ΤΕΙ ΜΕΣΟΛΟΓΓΙΟΥ

ΤΜΗΜΑ ΤΗΛΕΠ/ΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μηχανισμοί Μετάβασης του Διαδικτύου από το πρωτόκολλο IPv4 στο IPv6

ΟΝΟΜΑΤΕΠΩΝΥΜΟ

Φιορεντίνος Ιωάννης

Επιβλέπων: Τάσος Νταγιούκλας, Ph.D.
Ναύπακτος 2010

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΧΗΜΑΤΑ-ΠΙΝΑΚΕΣ

ΠΕΡΙΛΗΨΗ

Σκοπός της πτυχιακής εργασίας είναι η παρουσίαση του τρόπου μετάβασης του διαδικτύου από το πρωτόκολλο IPv4 στο πρωτόκολλο IPv6. Για να γίνει καλύτερα αντιληπτό το θέμα αρχικά γίνεται μια παραουσίαση του πρωτοκόλλου IPv4 και των χαρακτηριστικών του. Αναλύονται τα ζητήματα που προέκυψαν από την χρησιμοποίηση του , το πρόβλημα της εξάντλησης των IPv4 διευθύνσεων το οποίο τελικά μας οδηγεί στην σταδιακή αντικατάσταση του, καθώς και κάποιες τεχνικές που αναπτύχθηκαν οι οποίες έδωσαν «παράταση ζωής» στο IPv4. Στην συνέχεια παρουσιάζεται το πρωτόκολλο IPv6 , τα χαρακτηριστικά του και οι βελτιώσεις του σε σχέση με το IPv4. Γίνεται παρουσίαση των μηχανισμών μετάβασης που θα οδηγήσουν σταδιακά στην μετάβαση καθώς και σε ποιες περιπτώσεις πρέπει να χρησιμοποιηθεί κάποιος μηχανισμός έναντι κάποιου άλλου.Στο τέλος παρουσιάζεται ο σχεδιασμός ενός δικτύου προσομοίωσης το οποίο χρησιμοποιήθηκε για να γίνουν κάποιες μετρήσεις και συγκρίσεις μεταξύ των δύο πρωτοκόλλων.

ABSTRACT

The goal of the thesis is the presentation of the way that Internet will transit from IPv4 to IPv6. For a better understanding of the subject at first it is presented the currently main protocol IPv4 and its characteristics. Also the subject of the depletion of IPv4 addresses that led the transition is being analyzed and the techniques that extended the life of IPv4. Later it is presented the IPv6 protocol, its features and its improvements in comparison with the IPv4 protocol. Also there is a presentation of the transition mechanisms its features and in which case should be used each of those. Lastly it is presented the design of a simulation network that was used for some scenario measurements.

ΕΙΣΑΓΩΓΗ

Η ολοένα και αυξανόμενη εξέλιξη στον τομέα της τεχνολογίας της πληροφορικής και ιδιαίτερα στα δίκτυα ηλεκτρονικών υπολογιστών που με τον καιρό αντικαθιστούν τις παραδοσιακές μορφές επικοινωνίας φανέρωσε τις αδυναμίες του υπάρχοντος πρωτοκόλλου επικοινωνίας IPv4 να ικανοποιήσει τον ολοένα αυξανόμενο αριθμό των χρηστών και κατ' επέκταση δικτύων που αποτελούν σήμερα το διαδίκτυο, όπως επίσης και τις ανάγκες τους σε θέματα διευθυνσιοδότησης και διαχείρισης του μεγάλου όγκου νέων εφαρμογών που συνεχώς εμφανίζονται με αυξημένες απαιτήσεις. Για τον λόγο αυτό η IETF (Internet Engineering Task Force) το 1994 παρουσίασε ένα νέο πρωτόκολλο επιπέδου δικτύου το IPv6 ή IPng (IP next generation) με σκοπό την σταδιακή αντικατάσταση του κυρίαρχου πρωτοκόλλου IPv4.

Το νέο αυτό πρωτόκολλο δίνει λύσεις σε αρκετά προβλήματα του προκατόχου του και προσδίδει μια νέα δυναμική στο internet και τις δικτυακές επικοινωνίες γενικότερα. Ωστόσο η διαδικασία της μετάβασης είναι αρκετά δύσκολη αν αναλογιστεί κανείς το μέγεθος του internet σήμερα και το τι αντίκτυπο έχει αυτό στην καθημερινότητα μας. Η μετάβαση αυτή θα γίνει σταδιακά και σε βάθος χρόνου.

Για τον σκοπό αυτό υλοποιήθηκαν κάποιοι μηχανισμοί με σκοπό την ομαλή και σταδιακή μετάβαση από το κυρίαρχο σήμερα πρωτόκολλο IPv4 στο νέο IPv6. Οι πιο διαδεδομένοι μηχανισμοί στο παρών στάδιο μετάβασης είναι οι μηχανισμοί tunneling οι οποίοι παρουσιάζονται σε αυτή την εργασία. Η εργασία συνοπτικά περιλαμβάνει :

- Παρουσίαση του πρωτοκόλλου IPv4 και συνοπτική παρουσίαση της σουίτας πρωτοκόλλων TCP/IP της οποίας αποτελεί μέρος.
- Ανάλυση των τεχνικών που χρησιμοποιούνται σε συνδυασμό με το IPv4 για την προσωρινή λύση του προβλήματος της αυξημένης ζήτησης δημοσίων IP διευθύνσεων και κατά συνέπεια παράταση ζωής του IPv4.
- Αναλυτική Παρουσίαση του πρωτοκόλλου IPv6.
- Ανάλυση των μηχανισμών μετάβασης.
- Σύγκριση των δύο πρωτοκόλλων με βάση σενάρια που υλοποιήθηκαν σε λογισμικό προσομοίωσης και σε πραγματικό εξοπλισμό

Η δομή της εργασίας είναι η εξής. Στο Κεφαλαιο 1 γίνεται ανάλυση του κυρίαρχου αυτή την στιγμή πρωτοκόλλου IPv4. Περιγράφονται τα χαρακτηριστικά του και επίσης το πρόβλημα που προκύπτει με τις διαθέσιμες διευθύνσεις καθώς το IPv4 μπορεί να διαθέσει μέχρι και 4.294.967.296 μοναδικές διευθύνσεις.

Στο 2^{ο} Κεφάλαιο ακολουθεί αναλυτική παρουσίαση τουπρωτοκόλλου IPv6. Επίσης γίνεται σύγκριση με το πρωτοκόλλο IPv4 τόσο σχετικά με τις επικεφαλίδες των πρωτοκόλλων (headers) όσο και μεταξύ των χαρακτηριστικών τους. Επίσης στην αρχή του κεφαλαίου 2 γίνεται αναφορά στις τεχνικές που έδωσαν παράταση ζωής στο IPv4 (NAT,VSLM) καθώς χωρίς αυτές οι διαθέσιμες IPv4 διευθύνσεις θα είχαν ήδη εξαντληθεί.

Το 3^{ο} κεφάλαιο είναι αφιερωμένο στους μηχανισμούς μετάβασης που θα οδηγήσουν σταδιακά το διαδικτύο να βασίζεται στο πρωτόκολλο IPv6. Οι κύριες κατηγορίες των μηχανοσμών αυτών είναι Translation Mechanisms , Dual Stack Mechanisms και Tunneling Mechanisms.

Στο 4^{ο} κεφάλαιο παρουσιάζεται μια πλατφόρμα προσομοίωσης που σχεδιάστηκε μέσω λογισμικού και τα αποτελέσματα των μετρήσεων ενός σεναρίου.

.

1 Το πρωτόκολλο IPv4

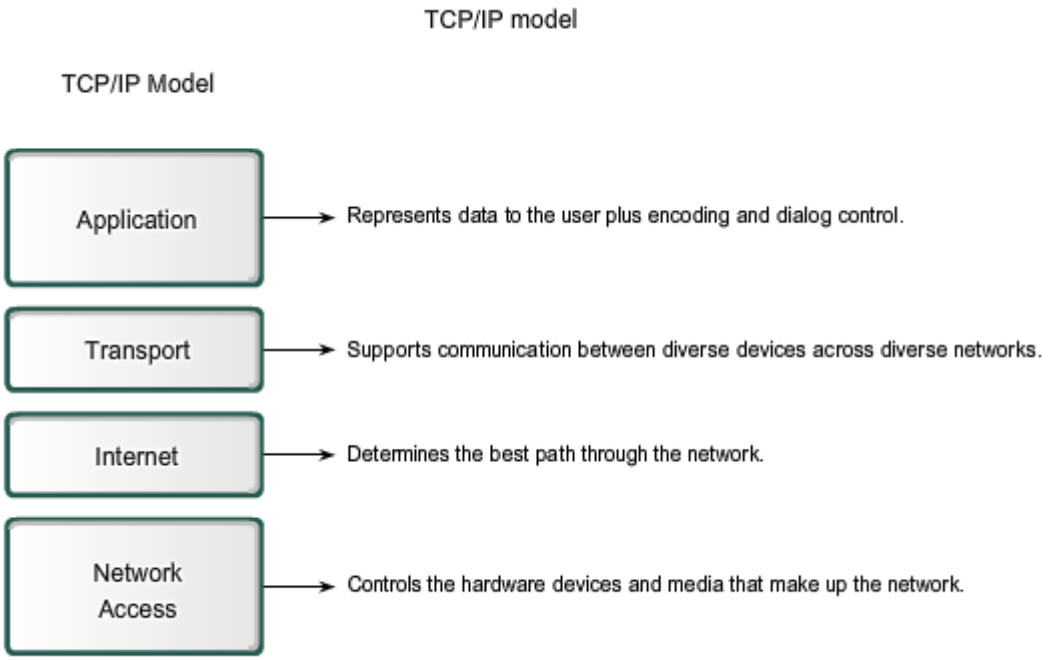
1.1 Η Στοίβα Πρωτοκόλλων TCP/IP και το πρότυπο OSI

Το πρώτο ιεραρχικό μοντέλο πρωτοκόλλων για διαδικτυακή επικοινωνία δημιουργήθηκε το 1970 και αναφέρεται και ως το μοντέλο διαδικτύου (The Internet Model) . Καθορίζει τέσσερις κατηγορίες λειτουργιών οι οποίες πρέπει να συμβούν έτσι ώστε η επικοινωνία μεταξύ των κόμβων να είναι επιτυχής. Η αρχιτεκτονική της στοίβας πρωτοκόλλων TCP/IP ακολουθεί την δομή αυτού του μοντέλου. Εξ' αιτίας αυτού , το μοντέλο του διαδικτύου αναφέρεται και ως το TCP/IP μοντέλο. Η στοίβα πρωτοκόλλων TCP/IP δεν περιλαμβάνει μόνο αυτά τα δύο πρωτόκολλα αλλά πήρε το όνομα της από τα δύο ποιο γνωστά και ευρέως χρησιμοποιούμενα πρωτόκολλα στις δικτυακές επικοινωνίες :

Το πρωτόκολλο επιπέδου μεταφοράς TCP (Transfer Control Protocol) και το πρωτόκολλο επιπέδου δικτύου IP (Internet Protocol).

Τα περισσότερα μοντέλα πρωτοκόλλων περιγράφουν μια στοίβα πρωτοκόλλων ενός συγκεκριμένου κατασκευαστή. Όμως το γεγονός ότι το TCP/IP μοντέλο είναι ένα ανοιχτό πρότυπο, μια εταιρεία-κατασκευαστής δεν μπορεί να ελέγξει τον καθορισμό του μοντέλου. Αυτός είναι και ο σκοπός του μοντέλου αυτού : να καθορίσει κάποιους κανόνες λειτουργικότητας και επικοινωνίας μεταξύ υπολογιστικών συστημάτων ανεξαρτήτως αρχιτεκτονικής της υποδομής του κάθε δικτύου.

Ο καθορισμός των προτύπων και των TCP/IP πρωτοκόλλων γίνεται θέμα συζήτησης σε δημόσια forum και καθορίζονται σε δημοσίως διαθέσιμα έγγραφα. Τα έγγραφα αυτά ονομάζονται RFCs (Request For Comments). Συμπεριλαμβάνουν τα επίσημα χαρακτηριστικά των πρωτοκόλλων επικοινωνίας δεδομένων και περιγράφουν την χρήση του κάθε πρωτοκόλλου. Τα RFCs περιλαμβάνουν επίσης τα τεχνικά χαρακτηριστικά και τις πολιτικές σχετικά με το Internet του IETF (Internet Engineering Task Force) ενός οργανισμού που απαρτίζεται από περισσότερες από 80 ομάδες εργασίας υπεύθυνες για την ανάπτυξη προτύπων για το διαδίκτυο.



Σχήμα 1.1 Το Μοντέλο TCP/IP

1.2 Το Μοντέλο OSI

Αρχικά το μοντέλο OSI σχεδιάστηκε από τον οργανισμό International Organization for Standardization (ISO) ώστε να παρέχει ένα πλαίσιο εργασίας για την ανάπτυξη πρωτοκόλλων που να διασφαλίζουν την διαλειτουργικότητα.

Σαν μοντέλο αναφοράς το OSI αποτελείται από επτά διακριτά επίπεδα και παρέχει εκτενή λίστα με τις λειτουργίες που μπορούν να συμβούν σε κάθε επίπεδο του. Επίσης περιγράφει την αλληλεπίδραση ενός επιπέδου με αυτό που βρίσκεται ακριβώς από πάνω και κάτω του. Τα επτά επίπεδα που απαρτίζουν το μοντέλο OSI είναι τα εξής :

7. **Application Layer** (Επίπεδο Εφαρμογών ή Επίπεδο 7): Παρέχει στον χρήστη την διεπαφή μεταξύ των εφαρμογών που επικοινωνούν και του δικτύου πάνω από το οποίο μεταφέρονται τα μηνύματα. Τα πρωτόκολλα επιπέδου εφαρμογών χρησιμοποιούνται για την ανταλλαγή δεδομένων μεταξύ των προγραμμάτων που τρέχουν τόσο στον αποστολέα όσο και στον παραλήπτη. Κάποια από τα ποιο γνωστά πρωτόκολλα επιπέδου εφαρμογών είναι τα εξής :

-Domain Name System (DNS) : Χρησιμοποιείται για την μετάφραση domain names σε IP διευθύνσεις.

-HTTP (Hypertext Transfer Protocol) : Χρησιμοποιείται για την επικοινωνία πάνω από το World Wide Web .

-SMTP (Simple Mail Transfer Protocol) : Χρησιμοποιείται για την μεταφορά e-mail μέσω του διαδικτύου.

-POP (Post Office Protocol) : Χρησιμοποιείται για την ανάκτηση e-mail.

-Telnet : Χρησιμοποιείται για την απομακρυσμένη πρόσβαση σε δικτυακές συσκευές.

-DHCP (Dynamic Host Configuration Protocol) : Χρησιμοποιείται για την αυτόματη απόδοση παραμέτρων όπως IP Address , Default Gateway , DNS Server σε μια δικτυακή συσκευή.

-FTP (File Transfer Protocol) : Χρησιμοποιείται για την μεταφορά αρχείων σε ένα περιβάλλον client – server.

6. Presentation Layer (Επίπεδο Παρουσίασης ή Επίπεδο 6)

Το επίπεδο παρουσίασης έχει τρεις κύριες λειτουργίες :

-Την κωδικοποίηση και μετατροπή των δεδομένων των εφαρμογών του επιπέδου 7 , ώστε να διασφαλίσει ότι τα δεδομένα του αποστολέα ερμηνευτούν σωστά από την κατάλληλη εφαρμογή στον παραλήπτη.

-Την συμπίεση των δεδομένων με τέτοιο τρόπο ώστε να είναι δυνατή η αποσυμπίεσή τους στον παραλήπτη.

-Την κρυπτογράφηση των δεδομένων και την αποστολή τους και την αποκρυπτογράφηση τους μετά την λήψη τους στην κατάλληλη συσκευή.

5.Session Layer (Επίπεδο Συνόδου ή επίπεδο 5) : Είναι υπεύθυνο για την διαχείριση και δημιουργία συνόδων μεταξύ δύο εφαρμογών που επικοινωνούν. Το επίπεδο συνόδου χειρίζεται την ανταλλαγή πληροφοριών για την έναρξη συνόδων , την διατήρησή τους ή την επανέναρξή τους εάν έχουν υπάρξει ανενεργές.

4.Transport Layer (Επίπεδο Μεταφοράς ή Επίπεδο 4) : Κάνει δυνατή την επικοινωνία πολλών εφαρμογών που τρέχουν στο ίδιο τερματικό να επικοινωνούν ταυτόχρονα μέσω του ίδιου δικτύου. Αυτό επιτυγχάνεται με την χρησιμοποίηση ports. Επίσης εάν είναι απαραίτητο μπορεί να εγγυηθεί την αξιόπιστη ανταλλαγή πακέτων την χρησιμοποίηση μηχανισμών διαχείρισης λαθών (error handling). Τα ποιο γνωστά πρωτόκολλα του επιπέδου 4 είναι το **TCP** και **UDP**.

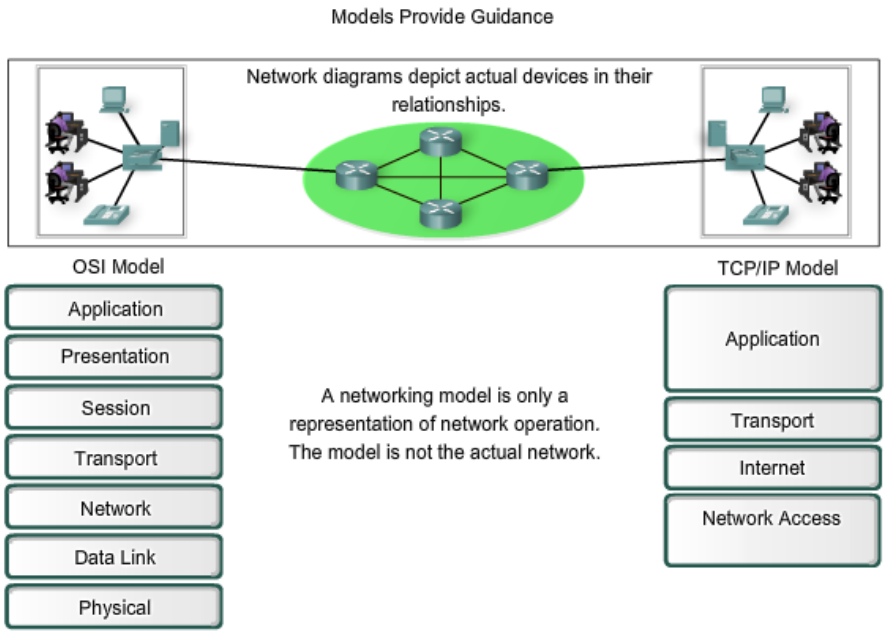
3.Network Layer (Επίπεδο Δικτύου ή επίπεδο 3): Το επίπεδο 3 παρέχει στις υπηρεσίες την ανταλλαγή πακέτων μεταξύ των τερματικών συσκευών. Για να επιτύχει αυτήν την από άκρο σε άκρο επικοινωνία χρησιμοποιεί τις εξής λειτουργίες : Διευθυνσιοδότηση , ενθυλάκωση , δρομολόγηση , απενθυλάκωση. Το πρωτόκολλο IPv6 που είναι το βάσικο θέμα της εργασίας αυτής όπως και τα πρωτόκολλα IPv4 είναι πρωτόκολλα επιπέδου 3 . Άλλα πρωτόκολλα του ίδιου επιπέδου είναι τα IPX , Connectionless Network Service (CLNS/DECNet) και AppleTalk. Συσκευές όπως οι router λειτουργούν σε αυτό το επίπεδο.

2.Data Link Layer (Επίπεδο Διασύνδεσης ή επίπεδο 2) : Το επίπεδο 2 καθορίζει τον τρόπο με τον οποίο γίνεται ανταλλαγή πακέτων σε ένα κοινό τοπικό μέσο. Εκτελεί δύο βασικές υπηρεσίες :

-Επιτρέπει στα ανώτερα επίπεδα να έχουν πρόσβαση στο φυσικό μέσο χρησιμοποιώντας τεχνικές όπως το framing.

-Ελέγχει τον τρόπο με τον οποίο γίνεται η τοποθέτηση και η λήψη των δεδομένων στο φυσικό μέσο χρησιμοποιώντας τεχνικές όπως media access και error detection. Τα switch λειτουργούν κατά βάση στο επίπεδο αυτό λαμβάνοντας τις αποφάσεις τους σχετικά με την προώθηση του κάθε πακέτου με βάση την επιπέδου 2 (MAC Address) διεύθυνση την οποία προορίζεται το πακέτο.

1.Physical Layer (Φυσικό επίπεδο ή επίπεδο 1): Το φυσικό επίπεδο παρέχει τα μέσα για την μεταφορά μέσω του δικτύου των bits τα οποία απαρτίζουν ένα Layer 2 frame. Ο σκοπός του φυσικού επιπέδου είναι η δημιουργία των ηλεκτρικών , οπτικών ή μικροκυματικών σημάτων τα οποία αναπαριστούν τα δεδομένα πάνω στο φυσικό μέσο.



Σχήμα 1.2 Τα μοντέλα OSI και TCP/IP

1.3 IPv4 – Διευθυνσιοδότηση στο Δίκτυο

Το πρωτόκολλο IPv4 είναι αυτή την στιγμή το πιο διαδεδομένο πρωτόκολλο επιπέδου δικτύου και το μοναδικό που χρησιμοποιείται για την μετάδοση δεδομένων μέσω του Internet. Σε κάποια εσωτερικά δίκτυα χρησιμοποιούνται και άλλα layer 3 πρωτόκολλα όπως το IPX, το Appletalk ή το CLNS . Επίσης το IPv6 έχει ήδη αρχίσει και εφαρμόζεται σε κάποιες περιοχές. Το IPv6 λειτουργεί ταυτόχρονα με το IPv4 και μελλοντικά θα αντικαταστήσει το μεγαλύτερο μέρος του. Οι υπηρεσίες που παρέχονται από το IP καθορίζονται από την έκδοση που είναι σε χρήση σε κάθε περίπτωση. Οι υπηρεσίες και η δομή των πακέτων χρησιμοποιούνται για την ενθυλάκωση των TCP Segments ή UDP Datagrams για το ταξίδι τους μέσα στο δίκτυο.

Το IP σχεδιάστηκε ως ένα πρωτόκολλο με χαμηλό φόρτο (overhead). Παρέχει μόνο τις αναγκαίες λειτουργίες για την παράδοση πακέτων και όχι για να διαχειρίζεται την ροή των πακέτων. Οι λειτουργίες αυτές παρέχονται από άλλα πρωτόκολλα άλλων επιπέδων. Τα βασικά χαρακτηριστικά του IPv4 είναι :

- Connectionless – Δεν χρειάζεται η εγκατάσταση σύνδεσης πριν την αποστολή πακέτων.

- Best Effort (unreliable) – Δεν χρησιμοποιείται καμία επιβάρυνση στο δίκτυο που να εγγυάται την παράδοση πακέτων. (όπως πχ. στην περίπτωση του TCP με την χρησιμοποίηση των Acknowledgements).
- Media Independent – Λειτουργεί ανεξάρτητα από το μέσο που χρησιμοποιείται για την μετάδοση των δεδομένων (χαλκός, οπτική ίνα, αέρας).

Στις δικτυακές επικοινωνίες για να είναι δυνατή η επικοινωνία δύο συσκευών κάθε συσκευή θα πρέπει με κάποιο τρόπο να αναγνωρίζεται μοναδικά μέσα στο δίκτυο. Θα πρέπει δηλαδή να έχει μια ταυτότητα η οποία να είναι μοναδική μέσα στο δίκτυο ώστε να μπορεί να αναγνωρίζεται. Η ποιο γνωστή διεύθυνση τέτοιου τύπου είναι η IP Address .

1.4 Η διεύθυνσης IPv4 και η δομή ενός IPv4 πακέτου

Σε επίπεδο δικτύου τα πακέτα για να φτάσουν στον προορισμό τους και να είναι επιτυχής η επικοινωνία πρέπει να περιέχουν μια source address και μια destination address (διεύθυνση αποστολέα και παραλήπτη αντίστοιχα). Χρησιμοποιώντας το IPv4 αυτό σημαίνει ότι κάθε πακέτο έχει μια 32-bit source address και μια 32-bit destination address στην επικεφαλίδα του IP πακέτου. Οι διευθύνσεις αυτές στο δίκτυο χρησιμοποιούνται σε δυαδική μορφή καθώς οι δικτυακές συσκευές χρησιμοποιούν ψηφιακή λογική. Για τον άνθρωπο μια ακολουθία 32 bit είναι δύσκολο να απομνημονευτεί και για τον λόγω αυτό τις αναπαριστούμε με την λεγόμενη dotted decimal μορφή. Για παράδειγμα η διεύθυνση **10101100000100000000010000010100** σε dotted decimal μορφή εκφράζεται και ως **172.16.4.20**. Η IPv4 διεύθυνση αποτελείται από τέσσερα πεδία , το καθένα μεγέθους 8-bit . Ανάλογα με την μάσκα δικτύου που χρησιμοποιείται μπορούμε να καταλάβουμε ποιο μέρος της διεύθυνσης αναφέρεται στο δίκτυο και ποιο μέρος στον host. Υπάρχουν τρεις τύποι διευθύνσεων :

- **Network Address**: Η διεύθυνση με την οποία αναφερόμαστε στο δίκτυο.
- **Broadcast Address:** Μια ειδική διεύθυνση η οποία χρησιμοποιείται για αποστολή δεδομένων σε όλους τους host του δικτύου.
- **Host Address :** Η διεύθυνση του host.

Για παράδειγμα έστω ότι η IP Address ενός υπολογιστή είναι η 192.168.10.1 με μάσκα 255.255.255.0 (/24). Τότε η Host Address είναι η 192.168.10.1 η διεύθυνση δικτύου η 192.168.10.0 και η διεύθυνση broadcast η 192.168.10.255 .
Όταν μια εφαρμογή που εκτελείται σε ένα τερματικό προσπαθεί να επικοινωνήσει με μια άλλη που εκτελείται σε ένα άλλο υπολογιστικό σύστημα το επίπεδο εφαρμογών στέλνει τα δεδομένα στα χαμηλότερα στρώματα του μοντέλου OSI . Όταν αυτά φτάσουν στο επίπεδο μεταφοράς , αυτό με την σειρά του και με την διαδικασία της ενθυλάκωσης (encapsulation) προσθέτει στα δεδομένα μια επικεφαλίδα στην οποία ορίζει την εφαρμογή-αποστολέα και την εφαρμογή-παραλήπτη μέσω των ports (source port – destination port). Ουσιαστικά αυτό που κάνει είναι να διαχωρίζει τα δεδομένα διαφορετικών εφαρμογών. Όταν για παράδειγμα ένα πακέτο φτάνει με destination port 80 ξέρει ο παραλήπτης ότι το πακέτο προορίζεται για HTTP εφαρμογή και όχι για e-mail (SMTP).

Μετά το επίπεδο μεταφοράς τα δεδομένα (TCP Segment ή UDP Datagram) μεταφέρονται στο επίπεδο δικτύου όπου και αυτό με την σειρά του εκτελεί την διαδικασία της ενθυλάκωσης. Προσθέτει δηλαδή στο πακέτο ένα IP header το οποίο συν τοις άλλης περιέχει τις πληροφορίες source IP address και destination IP address οι οποίες βοηθάνε στην δρομολόγηση του πακέτου από τους ενδιάμεσους κόμβους και επίσης όταν ένας host παραλάβει ένα πακέτο απαντάει στο source IP address του πακέτου.

1.5 Η επικεφαλίδα ενός IPv4 πακέτου (IPv4 packet header)

Στο σχήμα που ακολουθεί φαίνεται το πρωτόκολλο IPv4 καθορίζει διαφορετικά πεδία στην επικεφαλίδα. Τα πεδία αυτά περιλαμβάνουν δυαδικές τιμές (binary values) στις οποίες αναφέρονται διάφορες υπηρεσίες καθώς προωθούν πακέτα μέσω του δικτύου. Τα έξη σημαντικότερα πεδία είναι τα εξής :

- IP Source Address (Διεύθυνση Αποστολέα)
- IP Destination Address (Διέυθυνση Παραλήπτη)
- Time to Live (TTL)
- Type of Service (ToS)
- Protocol
- Fragment Offset

IP Source Address

Περιλαμβάνει μια δυαδική τιμή μεγέθους 32-bit που υποδηλώνει την διεύθυνση του αποστολέα του πακέτου

IP Destination Address

Περιλαμβάνει μια δυαδική τιμή μεγέθους 32-bit που υποδηλώνει την διεύθυνση του παραλήπτη του πακέτου

Time to Live

Περιλαμβάνει μια δυαδική τιμή μεγέθους 8-bit που υποδηλώνει τον εναπομείναντα «χρόνο ζωής του πακέτου». Η τιμή αυτή μειώνεται τουλάχιστον κατά ένα κάθε φορά που το πακέτα προσπελαύνεται από ένα router. Όταν η τιμή αυτή γίνει ίση με μηδέν τότε ο router απορρίπτει
το πακέτο. Ο μηχανισμός αυτός αποτρέπει πακέτα τα οποία δεν μπορούν να φτάσουν στον προορισμό τους από το να δρομολογούνται για άπειρο χρονικό διάστημα (το πρόβλημα των routing loops).

Protocol

Η τιμή αυτή μεγέθους 8-bit υποδηλώνει τον τύπο πακέτου που έχει ενθυλακωθεί μέσα στο IPv4 πακέτο. Το πεδίο αυτό δίνει την δυνατότητα στο επίπεδο δικτύου (Network Layer) να στείλει τα δεδομένα στο κατάλληλο ανώτερο επίπεδο.

Παράδειγμα:

01 ICMP

04 TCP

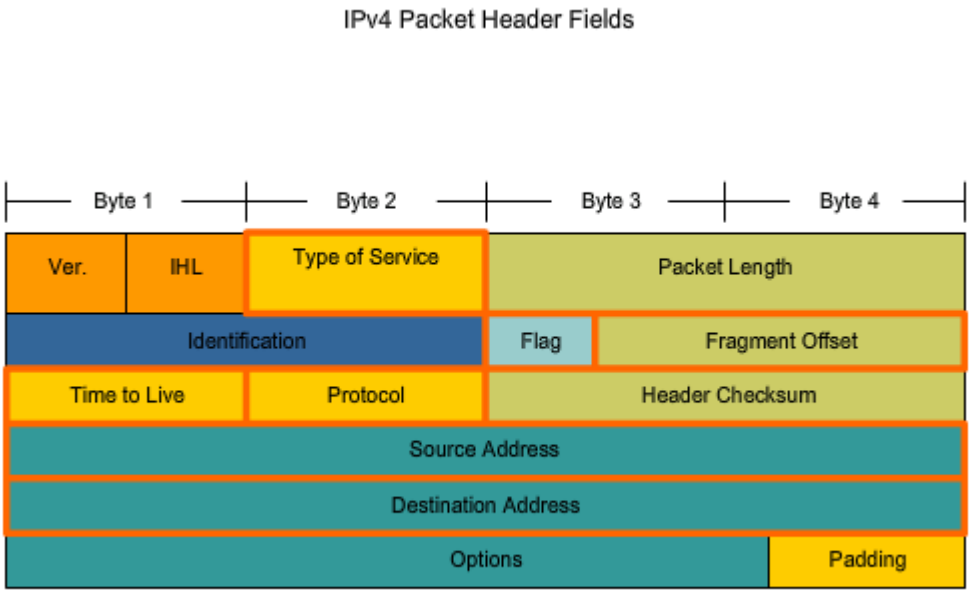
17 UDP

Type of Service

Το πεδίο αυτό περιλαμβάνει μια δυαδική τιμή μεγέθους 8-bit που χρησιμοποιείται για τον καθορισμό της προτεραιότητας τους κάθε πακέτου. Η τιμή αυτή ενεργοποιεί ένα μηχανισμό QoS (Quality of Service) για τα πακέτα με υψηλή προτεραιότητα.

Fragment Offset

Ένας router μπορεί να χρειαστεί να «τεμαχίσει ένα πακέτο» σε μικρότερα πριν την προώθηση
του. Όταν συμβαίνει ο «τεμαχισμός» το πακέτο χρησιμοποιεί το πεδίο Fragment Offset για την ανακατασκευή του πακέτου όταν αυτό φτάσει στον προορισμό του.



Σχήμα 1.3 Τα πεδία της επικεφαλίδας ενός IPv4 πακέτου

Άλλα πεδία της IPv4 επικεφαλίδας

Version

Υποδηλώνει το ποια έκδοση του πρωτοκόλλου χρησιμοποιείται (4 ή 6)

IHL

Υποδηλώνει το μέγεθος της επικεφαλίδας του πακέτου.

Packet Length

Το πεδίο αυτό υποδηλώνει το συνολικό μέγεθος του πακέτου συμπεριλαμβανομένου επικεφαλίδας και δεδομένων σε bytes.

Identification

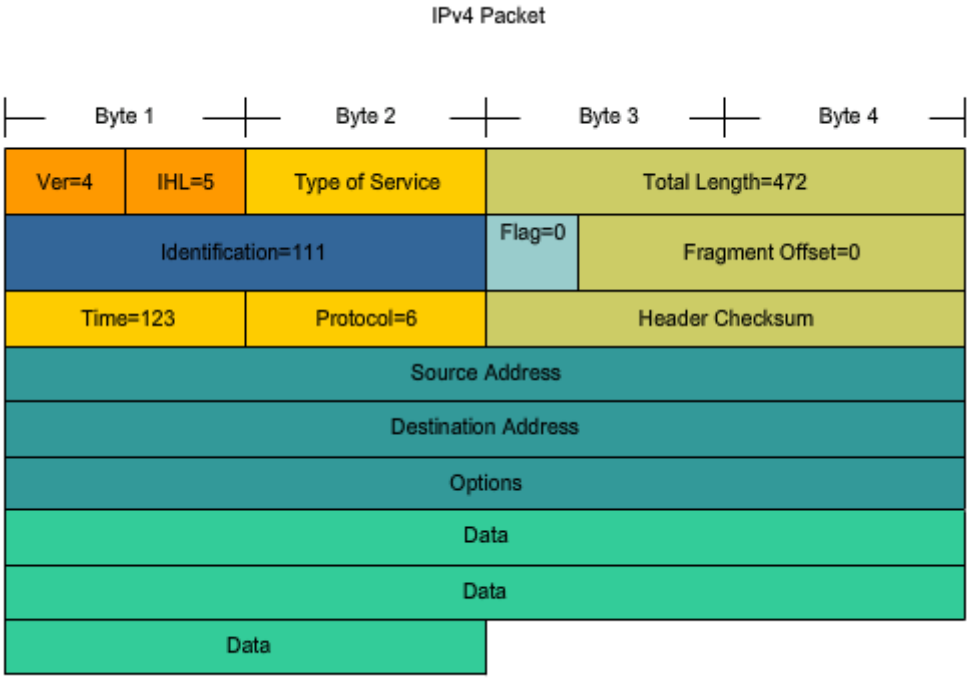
Χρησιμοποιείται για να αναγνωρίζεται μοναδικά ένα fragment ενός πακέτου.

Header Checksum

Χρησιμοποιείται για έλεγχο λαθών της επικεφαλίδας

Options

Υπάρχει πρόβλεψη για επιπλέον πεδία στην επικεφαλίδα τα οποία θα παρέχουν άλλες υπηρεσίες αν και πολύ σπάνια χρησιμοποιούνται.



Σχήμα 1.4 Ένα τυπικό πακέτο

2 Το πρωτόκολλο IPv6

2.1 Ανάγκη για νέο πρωτόκολλο δικτύου

Το ήδη υπάρχον πρωτόκολλο IPv4 (Internet Protocol version 4) που ορίστηκε στο RFC 791 το 1981 αποδείχτηκε ένα σταθερό και δυνατό πρωτόκολλο που κάλυψε σε μεγάλο βαθμό τις απαιτήσεις για τις οποίες σχεδιάστηκε και επικράτησε τελικά στο παγκόσμιο Internet. Εδώ και μερικά χρόνια όμως είχαν αρχίσει να φαίνονται κάποια σημαντικά προβλήματα στα οποία το συγκεκριμένο πρωτόκολλο αδυνατούσε να δώσει λύση. Η ολοένα και αυξανόμενη εξέλιξη της τεχνολογίας στον τομέα των δικτυακών επικοινωνιών και οι νέες εφαρμογές που εμφανίστηκαν στο προσκήνιο δεν μπορούσαν να υποστηριχτούν στον απαιτούμενο βαθμό από το IPv4. Ακολουθούν οι σημαντικότεροι λόγοι που κατέστησαν επιτακτική την ανάγκη για την μελλοντική αντικατάσταση του IPv4 από ένα νέο πρωτόκολλο δικτύου.

- Ο τεράστιος αριθμός των νέων διασυνδέσεων υπολογιστών και δικτύων και γενικότερα η επέκταση του internet σήμερα που ξεπέρασε κάθε αρχική προσδοκία οδήγησαν στην εξάντληση των IPv4 διευθύνσεων. Το πρόβλημα είχε κάνει την εμφάνιση του πολλά χρόνια πριν, το 1994 περίπου όταν και ο αριθμός των διασυνδεδεμένων δικτύων αυξανόταν με μαθηματική πρόοδο. Προτάθηκαν και υλοποιήθηκαν διάφορες λύσεις για την αντιμετώπιση του προβλήματος , αρχικά δρομολόγηση τύπου classless CIDR (Classless Interdomain Routing) η οποία έδωσε κάποια παράταση ζωής στο IPv4 και αργότερα ο μηχανισμός NAT (Network Address Translation) με δίκτυα ιδιωτικών διευθύνσεων κάτω από μια ή περισσότερες δημόσιες IP διευθύνσεις. Όμως η τελευταία δημιούργησε άλλα προβλήματα όπως μείωση της απόδοσης , αδυναμία peer-to-peer επικοινωνιών και εκμετάλλευση των σχετικών εφαρμογών όπως και καθώς και προβλήματα ασφάλειας από άκρο σε άκρο .

- Η ανάγκη για υποστήριξη εφαρμογών πολυμέσων και μετάδοσης δεδομένων σε πραγματικό χρόνο με επιπλέον απατήσεις για ποιότητα υπηρεσίας (QoS – Quality of Service) . Αν και θεωρητικά υπάρχει το πεδίο TOS (Type of Service) στην επικεφαλίδα του IPv4 πακέτου , πρακτικά δεν υλοποιείται και ουσιαστικά η όλη διαδικασία ελέγχου γίνεται σε ανώτερα επίπεδα του μοντέλου OSI (πχ επίπεδο μεταφοράς) και έγκειται στον διαχωρισμό των TCP από τις UDP επικεφαλίδες με τα προβλήματα που αυτό επιφέρει όπως σπατάλη της υπολογιστικής ισχύς στους δρομολογητές και αδυναμία για την πιο πάνω διάκριση εάν χρησιμοποιείται κρυπτογράφηση.

- Η εξάπλωση των ασύρματων δικτύων , τα οποία συνεχώς αυξάνονται με πολύ γρήγορους ρυθμούς. Όμως οι κινούμενοι χρήστες που υποστηρίζουν το IPv4 πρωτόκολλο δεν έχουν την δυνατότητα να διατηρήσουν την συνοδό και την διεύθυνση τους όταν μετακινούνται μεταξύ υποδικτύων (πρόβλημα Mobility).

- Η αδυναμία των δρομολογητών κορμού (backbone routers) να κρατήσουν στους πίνακες δρομολόγησης τον τεράστιο αριθμό δικτύων που υπάρχουν σήμερα στο internet. Σε πολλούς σήμερα border routers ο αριθμός των εγγραφών ξεπερνάει τις ογδόντα με εκατό χιλιάδες και προβάλλεται επιτακτικά η ανάγκη για καλύτερη διευθυνσιοδότηση και ιεράρχηση. Αν και οι νέες γενιές router αντιμετωπίζουν το

θέμα αυτό αποτελεσματικά, λόγω αυξημένων υπολογιστικών δυνατοτήτων , η δυνατότητα που προσφέρει το IPv6 για καλύτερη ιεραρχική δρομολόγηση και συνεπώς λιγότερη υπολογιστική ισχύ στους δρομολογητές το καθιστά βέλτιστη λύση.

- Η ανάγκη για πιο απλή ρύθμιση (configuration). Οι IPv4 διευθύνσεις πρέπει είτε να ανατεθούν manual είτε να γίνει χρήση ενός stateful address configuration protocol όπως το DHCP (Dynamic Host Configuration Protocol). Το πρόβλημα γίνεται εντονότερο όσο προστίθενται καινούργιοι υπολογιστές στο δίκτυο και το μέγεθος του αυξάνεται.

- Η απαιτήσεις σε ασφάλεια σε επίπεδο IP. Αν και ήδη υπάρχει το IPsec (Internet Protocol Security) , είναι προαιρετικό και όχι ενσωματωμένο στο IPv4 πρωτόκολλο. Όμως λόγω του ότι σήμερα μέσω της χρήσης του Internet πραγματοποιούνται διάφορες συναλλαγές οικονομικού και όχι μόνο χαρακτήρα, είναι αδιαμφισβήτητη πλέον η ανάγκη για ασφάλεια σε επίπεδο δικτύου.

Πριν αναφερθούμε στα χαρακτηριστικά του νέου πρωτοκόλλου θα παρουσιάσουμε κάποιες τεχνικές και τεχνολογίες που χρησιμοποιήθηκαν για να δώσουν προσωρινή λύση στο πρόβλημα της μη ύπαρξης διαθέσιμων IPv4 διευθύνσεων ώστε να ικανοποιήσουν τις ανάγκες ζήτησης που υπάρχουν.

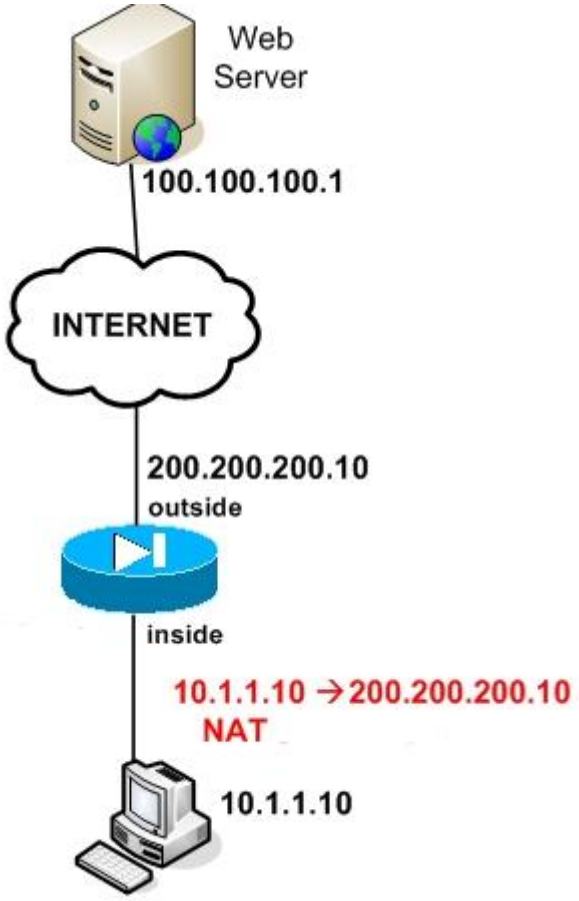
2.2 Το πρωτόκολλο NAT

Όταν το ARPANET ιδρύθηκε το 1969 σαν ένα ερευνητικό project κανένας δεν μπορούσε να αντιληφθεί ότι θα υπήρχε τέτοια τεράστια εξέλιξη. Μέχρι το 1989 το ARPANET είχε μετατραπεί σε αυτό που σήμερα όλοι γνωρίζουμε ως INTERNET. Μέσα στην επόμενη δεκαετία ο αριθμός των hosts στο Internet αυξήθηκε προοδευτικά από 159.000 τον Οκτώβρη του 1989 σε πάνω από 72 εκατομμύρια στο τέλος της χιλιετίας. Τον Ιανουάριο του 2007 υπήρχαν 443 εκατομμύρια hosts στο Internet. Χωρίς την εισαγωγή στο VLSM και CIDR το 1993 (RFC 1519), NAT το

1994 (Network Address Translator-RFC 1631) και την ιδιωτική διευθυνσιοδότηση το 1996 (RFC 1918) οι IPv4 διευθύνσεις θα είχαν εξαντληθεί προ πολλού.

Η βασική φιλοσοφία σχετικά με το NAT είναι η εγκατάσταση ενός εσωτερικού δικτύου , με ιδιωτικές IP διευθύνσεις. Όταν κάποιος host του δικτύου θέλει να επικοινωνήσει με το Internet τότε του «δανείζεται» μια δημόσια IP διεύθυνση. Όταν δεν χρειάζεται πια επικοινωνία με το Internet τότε η ίδια διεύθυνση μπορεί να ανατεθεί σε κάποιον άλλο host. Με αυτό τον τρόπο επιτυγχάνεται η επικοινωνία με το Internet πολλών host χρησιμοποιώντας λιγότερες δυνατές διευθύνσεις.

Με τον καιρό αναπτύχθηκαν καινούργιες εκδόσεις του NAT οι οποίες προσέφεραν παραπάνω δυνατότητες, όπως για παράδειγμα το Port Sharing NAT ή αλλιώς NAT-PT το οποίο επιτρέπει τον διαμοιρασμό περιορισμένου αριθμού διευθύνσεων σε μεγαλύτερο αριθμό host επιτρέποντας την ανάθεση της ίδιας διεύθυνσης σε δύο ή περισσότερους host **ταυτόχρονα.**



Σχήμα 2.1 Επικοινωνία με NAT

Πλεονεκτήματα του NAT

Διαμοιρασμός δημοσίων IP διευθύνσεων : Ένας μεγάλος αριθμός host μπορεί να μοιραστεί ένα μικρό αριθμό διευθύνσεων. Με αυτόν τον τρόπο μειώνεται το κόστος αλλά και δεν σπαταλούνται διευθύνσεις.

Ευκολότερη επέκταση του δικτύου : Αφού δεν είναι απαραίτητη η ανάθεση δημοσίων διευθύνσεων είναι ευκολότερη η πρόσθεση νέων δικτυακών συσκευών.

Ευκολότερη μετάβαση σε άλλον ISP: Το μόνο που αλλάζει είναι η δημόσια διεύθυνση. Δεν χρειάζεται η αλλαγή διευθύνσεων των host του δικτύου.

Αυξημένη Ασφάλεια: Με την χρήση του NAT δημιουργείται ένα είδος firewall μεταξύ του ιδιωτικού δικτύου και του Internet. Είναι πολύ πιο δύσκολο κάποιος μη-εξουσιοδοτημένος να έχει πρόσβαση σε ένα host του ιδιωτικού δικτύου επειδή οι host αυτοί χρησιμοποιούν ιδιωτικές διευθύνσεις.
Transparent: Η υλοποίηση του NAT λαμβάνει μέρος σε ένα ή το πολύ λίγο περισσότερους router. Έτσι δεν χρειάζεται να αλλάξουν οι ρυθμίσεις στους τελικούς χρήστες.

Μειονεκτήματα

Πολυπλοκότητα: Η εγκατάσταση , παραμετροποίηση και διαχείριση ενός δικτύου που χρησιμοποιεί NAT είναι πιο πολύπλοκη σε σχέση με ένα που δεν χρησιμοποιεί. Επίσης κάνει το troubleshooting δυσκολότερο λόγω της αντικατάστασης των διευθύνσεων.

Θέματα Ασφάλειας : Πρωτόκολλα όπως το IPSec έχουν σχεδιαστεί ώστε να εντοπίζουν τροποποιήσεις στις επικεφαλίδες , κατά συνέπεια εμποδίζουν τις αλλαγές που επιφέρει το NAT καθώς δεν μπορούν να τις ξεχωρίσουν από ένα «ύποπτο πακέτο».

Θέματα Πρόσβασης: Η έλλειψη δημοσίων διευθύνσεων σε κάθε host έχει διπλό αντίκτυπο. Ναι μεν είναι πολύ δύσκολο κάποιος κακόβουλος χρήστης να έχει πρόσβαση σε ένα NAT host από εξωτερικό δίκτυο, αλλά είναι δημιουργούνται προβλήματα όταν θέλει να έχει πρόσβαση και κάποιος νόμιμος χρήστης. Για παράδειγμα η εγκατάσταση μιας peet-to-peer εφαρμογής γίνεται δυσκολότερη. Το πρόβλημα είναι ότι το NAT δεν επιτρέπει να εγκατασταθούν συνδέσεις εάν κάνει την αίτηση κάποιος host από εξωτερικό δίκτυο. Το πρόβλημα μπορεί να λυθεί εάν παρέμβει ο administrator κάνοντας ρυθμίσεις που έχουν σχέση με το port forward. Το port forward είναι μια τεχνική η οποία επιτρέπει την επιτρέπει την πρόσβαση από εξωτερικούς host σε συγκεκριμένα ports που βρίσκονται σε κάποιο host του εσωτερικού δικτύου.

Μείωση Απόδοσης: Κάθε φορά που γίνεται τροποποίηση σε ένα πακέτο του ιδιωτικού δικτύου που έχει κάποιον εξωτερικό προορισμό χρειάζεται να γίνει address translation. Επίσης πρέπει να υπολογιστούν ξανά κάποιες τιμές όπως το checksum συνεπώς όλα αυτά προσθέτουν φόρτο στο δίκτυο.

2.3 Εισαγωγή στο IPv6

Η δυνατότητα αποτελεσματικής επέκτασης των δικτύων έχει ως βασική προϋπόθεση την απεριόριστη διαθεσιμότητα IP διευθύνσεων. Το IPv6 ή IP version 6 ή IPng (Next Generation) συνδυάζει επεκταμένη διευθυνσιοδότηση με αποτελεσματικότερη και περισσότερα χαρακτηριστικά επικεφαλίδα , ώστε να ικανοποιήσει τις ανάγκες για μελλοντική επέκταση των δικτύων.

Το IPv6 ικανοποιεί τις αυξανόμενες ανάγκες για ιεραρχική διευθυνσιοδότηση κάτι το οποίο δεν μπορεί να παρέχει το IPv4 σε ικανοποιητικό βαθμό. Ένα βασικό χαρακτηριστικό είναι ότι το IPv6 μπορεί να επαναδημιουργήσει συνδέσεις από άκρο σε άκρο χωρίς την ανάγκη να παρέμβασης από το NAT (Network Address Protocol).

Το Internet θα μεταμορφωθεί μετά την σχεδόν ολική αντικατάσταση του IPv4 από το IPv6, αν και το IPv4 δεν θα εξαφανιστεί μέσα σε μια νύχτα. Αντιθέτως θα

συνυπάρξει και σταδιακά θα αντικατασταθεί από το IPv6. Η αλλαγή αυτή έχει ήδη ξεκινήσει σε Ευρώπη , Ιαπωνία , Η.Π.Α. κτλπ. Στις περισσότερες από αυτές τις περιοχές έχει εξαντληθεί το εύρος των διαθέσιμων IPv4 διευθύνσεων που τους έχει ανατεθεί , κάτι το οποίο κάνει το IPv6 πολύ ελκυστικό. Επιπλέον το IPv6 παρέχει απεριόριστες διευθύνσεις .

Το πιο προφανές στοιχείο που κάνει το IPv6 να ξεχωρίζει είναι η χρήση πολύ μεγάλων διευθύνσεων. Το μέγεθος μιας IPv6 διεύθυνσης είναι 128-bit δηλαδή τέσσερις φορές μεγαλύτερη από την 32-bit IPv4 διεύθυνση. Μια διεύθυνση 32 bit προσφέρει 2^32 διαθέσιμες διευθύνσεις (4.294.967.296 διευθύνσεις) ενώ μια 128 bit διεύθυνση προσφέρει 2^128 (340,282,366,920,938,463,463,374,607,431,768,211,456 διευθύνσεις).

Στα τέλη της δεκαετίας του 1970 όταν σχεδιάστηκε το εύρος διευθύνσεων του IPv4 φαινόταν αδύνατο να εξαντληθεί . Ωστόσο λόγω τεχνολογικών αλλαγών και πρακτικές αποδόσεων διευθύνσεων οι οποίες δεν είχαν προβλέψει την τεράσια ζήτηση που θα ακολουθούσε το εύρος διευθύνσεων συρρικνώθηκε τόσο ώστε το 1992 φαινόταν καθαρά πως η αντικατάσταση θα ήταν αναγκαία μελλοντικά.

Με το IPv6 είναι δύσκολο ακόμα και να υποθέσουμε πως κάποτε οι διευθύνσεις θα εξαντληθούν. Η χρησιμοποίηση μιας 128 bit διεύθυνσης δεν αποσκοπεί μόνο στις άπειρες διευθύνσεις αλλά έχει σκοπό και την διαίρεση σε ιεραρχικά routing domain τα οποία απεικονίζουν την εικόνα του σημερινού Internet. Η χρήση των 128 bit επιτρέπει πολλαπλά επίπεδα ιεραρχίας και ευελιξίας στον σχεδιασμό ιεραρχικής διευθυνσιοδότησης και δρομολόγησης κάτι το οποίο λείπει από το IPv4

Το IPv6 δεν θα υπήρχε εάν δεν είχε προκύψει το θέμα εξάντλησης των διαθέσιμων IPv4 διευθύνσεων. Ωστόσο εκτός από το μεγαλύτερο εύρος διευθύνσεων , η ανάπτυξη του IPv6 έδωσε την ευκαιρία να δημιουργηθεί ένα νέο πρωτόκολλο με καινούργια και βελτιωμένα χαρακτηριστικά τα οποία αντιμετωπίζουν κάποιους από τους περιορισμούς του IPv4

2.3.1 Τα χαρακτηριστικά του πρωτοκόλλου IPv6

- Η απλοποιημένη επικεφαλίδα (header) και λειτουργία του πρωτοκόλλου αυτόματα μεταφράζεται σε μικρότερο φόρτο στο δίκτυο. Επίσης καθορίζεται μια πιο λειτουργική και ιεραρχική διευθυνσιοδότηση και δρομολόγηση η οποία στηρίζεται στα πολλαπλά επίπεδα ISPs και οργανισμών και που σύμφωνα με υπολογισμούς θα μειώσει το μέγεθος των πινάκων δρομολόγησης των δρομολογητών κατά 75%.

- Καλύτερη Υποστήριξη της Ποιότητας Υπηρεσίας (QoS) με τα πεδία Flow Label και Traffic Class. Το πεδίο Flow Label εισάγει την έννοια της ροής πακέτων (πακέτα από την ίδια προέλευση προς τον ίδιο προορισμό που χρειάζονται την ίδια επεξεργασία από τον δρομολογητή) και το οποίο αναμένεται να χρησιμοποιηθεί για την μετάδοση real time δεδομένων τόσο audio αλλά και video streaming μειώνοντας σημαντικά την καθυστέρηση στους ενδιάμεσους δρομολογητές. Αυτό οφείλεται πρώτον στο ότι όλα τα δεδομένα που χρειάζεται ο δρομολογητής βρίσκονται στην επικεφαλίδα και έτσι δεν χρειάζεται να «παραβιάσει» ανώτερα στρώματα , και κατά συνέπεια χωρίς να εισάγει περεταίρω καθυστέρηση στην μετάδοση. Και το δεύτερο και σημαντικότερο είναι ότι οι δρομολογητές θα διατηρούν μια κρυφή μνήμα cache στην οποία θα διατηρούν τις ενέργειες που απαιτούνται για πακέτα της ίδιας ροής , χωρίς πλέον να χρειάζεται η επεξεργασία του κάθε πακέτου ξεχωριστά μειώνοντας με αυτό τον τρόπο σημαντικά την καθυστέρηση. Το πεδίο Traffic Class καθορίζει την προτεραιότητα για το κάθε πακέτο που δρομολογείται.

- Έχει γίνει εξ' αρχής ο σχεδιασμός με βάση την ασφάλεια. Το IPsec πρωτόκολλο ασφάλειας είναι ενσωματωμένο στο νέο πρωτόκολλο και αποτελεί αναπόσπαστο κομμάτι του , παρέχοντας Πιστοποίηση Αυθεντικότητας και Ακεραιότητας , και Κρυπτογράφηση. Το IPsec περιέχει τα εξής στοιχεία τα οποία παρέχουν ασφάλεια:

- Authentication Header (AH): Η επικεφαλίδα Authentication παρέχει αυθεντικότητα και ακεραιότητα των δεδομένων.
- Encapsulating Security Payload Header (ESP): Η ESP επικεφαλίδα παρέχει αυθεντικότητα δεδομένων, ακεραιότητα δεδομένων και εμπιστευτικότητα δεδομένων για πακέτα στα οποία έχει γίνει ενθυλάκωση (encapsulation).
- Το πρωτόκολλο Internet Exchange Key (IKE): Διαπραγματεύεται τις ρυθμίσεις του IPsec.

- IPv6 Mobility , παρέχει δηλαδή τη δυνατότητα σε κινούμενους χρήστες να διατηρούν την σύνδεση τους ενώ κινούνται μεταξύ διαφορετικών δικτύων.

Συγκεκριμένα ο χρήστης διατηρεί την διεύθυνση του τοπικού δικτύου (home address και παράλληλα του αναθέτονται οι νέες διευθύνσεις από τα δίκτυα στα οποία εισέρχεται. Ένας δρομολογητής στο τοπικό δίκτυο ο home agent ενημερώνεται από τον χρήστη για τις διευθύνσεις του κάθε φορά που ο τελευταίος αλλάζει δίκτυο και στην περίπτωση που κάποιος προσπαθήσει να επικοινωνήσει με τον κινούμενο χρήστη , μέσω τις τοπικής του διευθύνσεως , τα πακέτα φτάνουν στον home agent , ο οποίος τα ενθυλακώνει και μέσω tunnel τα στέλνει στον κινούμενο χρήστη-προορισμό. Στην συνέχεια ο ίδιος ο χρήστης ενημερώνει τον κόμβο που του έστειλε τα πακέτα για την προσωρινή του διεύθυνση και η επικοινωνία γίνεται άμεσα μεταξύ των δύο χωρίς την διαμεσολάβηση του home agent. Ο κινούμενος χρήστης κάθε φορά που αλλάζει διεύθυνση εκτός από τον home agent ενημερώνει και τους υπόλοιπους χρήστες με τους οποίους είχε ή έχει επικοινωνία αλλά παράλληλα διατηρεί και τις υπόλοιπες διευθύνσεις για να δέχεται τα πακέτα που έρχονται σε αυτές. Η δυνατότητα αυτή παρέχεται και για το IPv4 όμως όχι αυτόματα. Κάτι που σημαίνει πως χρειάζονται παραπάνω ρυθμίσεις για να μπορέσει κάποιος να επιτύχει mobility.

- Παρέχει την δυνατότητα για Stateful και Stateless Address Configuration. Με το IPv4 για να ρυθμιστούν δυναμικά οι host χρησιμοποιούσαν ένα DHCP sever και περίμεναν ένα μικρό χρονικό διάστημα για να πάρουν τις ρυθμίσεις που αφορούσαν την διευθυνσιοδότηση τους. Με το Stateles Address Configuration ένας host έχει την

δυνατότητα να ρυθμίσει αυτόματα την IP διεύθυνση του στο link. Αυτού του είδους οι διευθύνσεις λέγονται link-local διευθύνσεις και μπορούν να χαρακτηριστούν και ως το "host portion" της IPv6 διεύθυνσης. Οι link-local διευθύνσεις μπορούν να ρυθμιστούν και χωρίς την παρέμβαση ενός δρομολογητή. Έτσι η επικοινωνία μεταξύ γειτονικών συσκευών μπορεί να γίνει άμεσα.

- Απεριόριστες επικεφαλίδες επέκτασης (extension headers): Με την εισαγωγή extension headers μετά την IPv6 header μπορεί κάποιος να επεκτείνει το πρωτόκολλο με καινούργια χαρακτηριστικά.

- Το πρωτόκολλο Neighbor Discovery (ND) για διαχείριση συσκευών που βρίσκονται πάνω σε ένα κοινό μέσο : Το Neighbor Discovery Protocol είναι μια σειρά από ICMPv6 μηνύματα που χρησιμοποιούνται σε IPv6 περιβάλλον για να αναγνωρίσουν την σχέση μεταξύ γειτονικών κόμβων. Το ND δίνει την δυνατότητα σε ένα host να δει διαδρομές (routes) , διευθύνσεις και prefix διευθύνσεων σε ένα κομμάτι δικτύου. Τα πρωτόκολλο ARP(Address Resolution Protocol) , τα μηνύματα ICMPv4 router discovery και ICMPv4 Redirect Message αντικαθιστούνται από τα πιο αποδοτικά multicast και unicast ND μηνύματα.

- Νέα διαμόρφωση της επικεφαλίδας όπου χρησιμοποιούνται τα απολύτως απαραίτητα πεδία , χωρίς να υπάρχει η επιβάρυνση των αχρησιμοποίητων πεδίων όπως το options στο IPv4 όπου σχεδόν ποτέ δεν χρησιμοποιούταν όμως ο δρομολογητής ήταν υποχρεωμένος να το ελέγχει σπαταλώντας έτσι υπολογιστική ισχύ. Όλα τα επιπλέον πεδία που συμπεριλαμβάνονται στις δευτερεύουσες επικεφαλίδες που ακολουθούν σαν προέκταση της πρώτης και η ύπαρξη τους δηλώνεται στο πεδίο *Next Header.* Έτσι η επικεφαλίδα του IPv6 πακέτου έχει μόλις το διπλάσιο μέγεθος από αυτήν του IPv4 αν και το μήκος της IPv6 διεύθυνσης είναι τετραπλάσιο από το αντίστοιχο της IPv4. Συγκεκριμένα στην IPv6 επικεφαλίδα υπάρχουν το πεδίο *Version* που υποδηλώνει εάν πρόκειται για IPv6 ή IPv4 πακέτο, τα πεδία *Traffic Class* και *Flow Label* που επεξηγήθηκαν προηγουμένως , το πεδίο *Next Header* που υποδηλώνει εάν κάποιες επιπλέον extension headers υπάρχουν μετά την επικεφαλίδα , το πεδίο *Hop Limit* που είναι αντίστοιχο με το πεδίο *TTL (Time to Live)*

στο IPv4 δηλαδή μετά από πόσα hops θα απορριφθεί το πακέτο. Επίσης η διεύθυνση πηγής (source address) και προορισμού (destination address).

- Πολλές επιλογές μετάβασης.

➢ Ρύθμιση μιας συσκευής ως Dual Stack (δηλαδή να υποστηρίζει και IPv4 και IPv6)

➢ Τεχνικές όπως IPv6 over IPv4 (tunneling)

➢ NAT-PT επιτρέπει μετάφραση πρωτοκόλλων μεταξύ IPv6 και IPv4. Αυτό δίνει την δυνατότητα απ' ευθείας επικοινωνίας μεταξύ συσκευών που χρησιμοποιούν διαφορετικά πρωτόκολλα.

2.3.2 Η επικεφαλίδα ενός IPv6 πακέτου

Η IPv6 επικεφαλίδα περιέχει τα εξής πεδία :

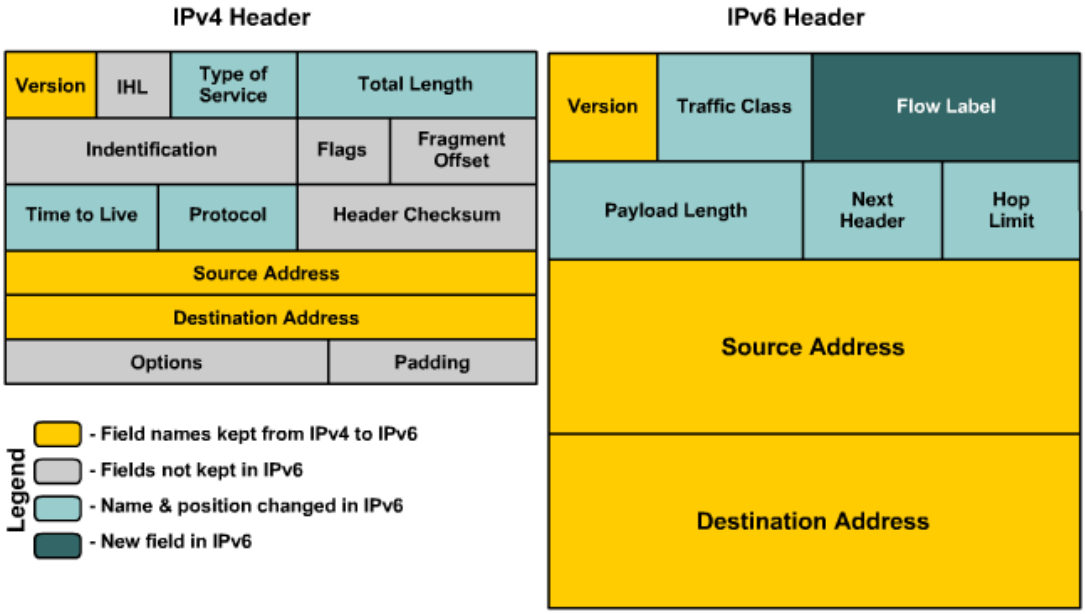
- **Version :** Πεδίο μεγέθους 4 bit. Το ίδιο με το IPv4. Περιέχει τον αριθμό 4 αντί του 6.
- **Traffic Class :** Πεδίο μεγέθους 8-bit παρόμοιο με το ToS (Type of Service) στο IPv4.
- **Flow Label :** Πεδίο μεγέθους 20-bit που επιτρέπει σε μια συγκεκριμένη ροή πακέτων να

«σημαδευτεί». Μπορεί να χρησιμοποιηθεί για τεχνικές multilayer switching και για αυξημένη απόδοση packet switching.

- **Payload Length :** Παρόμοιο με το πεδίο Total Length στο IPv4. Καθορίζει το συνολικό μέγεθος σε bytes. Έχει μέγεθος 16 bit.
- **Next Header :** Καθορίζει το τι είδους επικεφαλίδα ακολουθεί. Μπορεί να είναι ένα πακέτο επιπέδου μεταφοράς TCP ή UDP για παράδειγμα. Το πεδίο αυτό είναι παρόμοιο με το πεδίο Protocol στο IPv4. Έχει μέγεθος 8 bit.
- **Hop Limit :** Καθορίζει τον μέγιστο αριθμό hops που μπορεί να διασχίσει ένα πακέτο. Κάθε hop ή router μειώνει το πεδίο αυτό κατά ένα (ομοίως με το πεδίο TTL στο IPv4) . Έχει μέγεθος 8 bit.

Επειδή δεν υπάρχει το πεδίο checksum στο IPv6 ο router μπορεί να μειώσει την τιμή του πεδίου χωρίς να υπολογίσει ξανά το checksum. Ο μη υπολογισμός αυτός εξοικονομεί σημαντικό υπολογιστικό χρόνο σε ένα router.

- **Source Address :** Έχει μέγεθος 128 bit. Προσδιορίζει την πηγή απ' όπου προέρχεται το πακέτο.
- **Destination Address :** Έχει μέγεθος 128 bit . Προσδιορίζει τον προορισμό του πακέτου.



Σχήμα 2.2 Σύγκριση των επικεφαλίδων IPv4 – IPv6

Στον παρακάτω πίνακα γίνεται μια σύγκριση μεταξύ των κύριων χαρακτηριστικών των 2 πρωτοκόλλων.

ΘΕΜΑ	**IPv4**	**IPv6**	**Πλεονέκτημα IPv6**
Εύρος Διευθύνσεων	4 Δισεκατομμύρια Διευθύνσεις	2^128	79 Οκτάκις φορές το εύρος διεθύνσεων του IPv4
Ρύθμιση	Manual ή χρησιμοποιώντας DHCP	Universal Plug and Play (UPnP) με ή χωρίς DHCP	Μικρότερο λειτουργικό κόστος και λιγότερα λάθη
Broadcast/Multicast	Χρησιμοποιεί και τα Δύο	Δεν χρησιμοποιεί Broadcast και έχει διαφορετικές μορφές multicast	Ποιο αποδοτική Χρησιμοποίηση του Bandwidth
Υποστήριξη Anycast	Όχι	Αποκλειστική υποστήριξη Anycast	Νέες εφαρμογές σε Mobility
Δικτυακή Ρύθμιση	Κυρίως manual	Διευκολύνει την Επαναδιευθυνσιο δότηση των host και router	Μικρότερο λειτουργικό κόστος και διευκόλυνση στην μετάβαση
Υποστήριξη QoS	ToS χρησιμοποιώντας DIFFServ	Flow Classes και Flow Labels	Πιο αποδοτικός έλεγχος του QoS
Ασφάλεια	Χρησιμοποιεί IPsec για την προστασία των IP πακέτων	Το IPsec γίνεται η κυρίαρχη τεχνολο-γία για την προστασία και τον έλεγχο πακέτων	Ασφαλέστερο δικτυακό Περιβάλλον
Mobility	Χρησιμοποιεί Mobile IPv4	Το Mobile IPv6 παρέχει γρήγορη μεταβίβαση και router optimization	Συμβατό με τις τελευταίες 3G τεχνολογίες

Πίνακας 1 Σύγκριση των δύο πρωτοκόλλων

2.3.3 Τύποι IPv6 Διευθύνσεων

Η αναπαράσταση μιας IPv6 διεύθυνσης γίνεται χωρίζοντας την σε πεδία των 16-bit. Κάθε
πεδίο γράφεται σε δεκαεξαδική μορφή μεταξύ 0x000 και 0xFFF τα οποία χωρίζονται με άνω και κάτω τελεία (:). Κάποιο γενικοί κανόνες για την αναπαράσταση μιας IPv6 διεύθυνσης είναι:

Εάν ένα πεδίο ξεκινάει με μηδενικά δεν είναι υποχρεωτικό να αναφερθούν. Για παράδειγμα 09C0=9C0 και 0000=0.

Συνεχόμενα πεδία αποτελούμενα από μηδενικά μπορούν να αναπαρασταθούν ως «::» μόνο μια φορά.

Μια μη καθορισμένη διεύθυνση γράφεται ως «::» καθώς αποτελείται μόνο από μηδενικά.

Το σύμβολο «::» μειώνει αρκετά το μέγεθος των περισσότερων διευθύνσεων. Για παράδειγμα FF01:0:0:0:0:0:0:1=FF01:1.

Η δομή της IPv6 διευθυνσιοδότησης καθορίζονται σε διάφορα RFCs όπως στο 3513 και 4291.
Σε κάθε RFC καθορίζονται τρεις τύποι διευθύνσεων:
Unicast Address : Υποδηλώνει μια μοναδική συσκευή μέσα στο δίκτυο. Ένα πακέτο που αποστέλλεται σε μια unicast address παραδίδεται στο αντίστοιχο interface που του έχει αποδοθεί η συγκεκριμένη διεύθυνση. Υπάρχουν δύο τύποι Unicast διευθύνσεων :

1.Link Local Unicast Address: Είναι διευθύνσεις δικτύου οι οποίες χρησιμοποιούνται για επικοινωνία εντός του δικτύου ή μιας point to point ζεύξης. Οι δρομολογητές δεν προωθούν πακέτα με Link Local διευθύνσεις. Οι διευθύνσεις αυτές χρησιμοποιούνται συχνά όταν δεν υπάρχει εξωτερική πηγή διευθυνσιοδότησης (πχ. DHCP Server). Η διευθυνσιοδότηση εκτελείται από το λειτουργικό σύστημα του host χρησιμοποιώντας μια διεργασία που λέγεται stateless address autoconfiguration. Στο IPv6 οι διευθύνσεις αυτές είναι απαραίτητες και χρησιμοποιούν το prefix f380::/10.

2.Global Unicast Address: Είναι μοναδική globally ώστε να μπορεί να δρομολογηθεί χωρίς τροποποίηση. Τα πακέτα με global διευθύνσεις πηγής και προορισμού δρομολογούνται από τους router του διαδικτύου στον τελικό προορισμό τους.

Όλα τα interfaces πρέπει να έχουν τουλάχιστον μία Link Local Address αν και ένα βασικό χαρακτηριστικό του IPv6 είναι ότι ένα interface μπορεί επίσης να έχει πολλαπλές IPv6 διευθύνσεις οποιουδήποτε τύπου (unicast , anycast ή multicast).

Σημείωση: Υπάρχει επίσης και η site local unicast address άλλα ο οργανισμός IETF πρόκειται να την καταργήσει ή να την αντικαταστήσει οπότε δεν θα γίνει αναφορά σε αυτή.

Multicast Address: Το IPv6 δεν έχει broadcast address. Το Broadcasting στο IPv4 μπορεί να επιφέρει διάφορα προβλήματα. Δημιουργεί σε κάποιες περιπτώσεις καθυστέρηση σε κάθε συσκευή στο δίκτυο μειώνοντας την απόδοση του και σε κάποιες άλλες μπορεί να κάνει το δίκτυο να καταρρεύσει. Το φαινόμενο αυτό είναι γνωστό και ως broadcast storm. Οι broadcast διευθύνσεις έχουν αντικατασταθεί από τις Multicast διευθύνσεις. Το Multicast επιτρέπει αποδοτικότερη λειτουργία του δικτύου ομαδοποιώντας κάποιες συσκευές (multicast groups) , στέλνοντας με αυτό τον τρόπο πακέτα σε ένα περιορισμένο αριθμό συσκευών αντί των broadcast πακέτων τα οποία λαμβάνονται από όλες τις συσκευές που ανήκουν σε ένα δίκτυο.

Anycast Address : Είναι μια καινούργιου τύπου διεύθυνση η οποία υποδηλώνει μια λίστα συσκευών δηλαδή αναφέρεται σε πολλαπλά interfaces. Ένα πακέτο με προορισμό μια anycast address παραδίδεται στο interface το οποίο βρίσκεται πιο κοντά στον προορισμό σύμφωνα με το πρωτόκολλο δρομολόγησης που χρησιμοποιείται. Η διαφορά με το multicast είναι η εξής : Και στις δύο περιπτώσεις υπάρχει μια σχέση ένα-προς-πολλά μεταξύ της διεύθυνσης προορισμού και των παραληπτών. Στην περίπτωση του multicast όλες οι συσκευές που ανήκουν στο multicast group που υποδηλώνει η διεύθυνση παραλαμβάνουν το πακέτο , ενώ στο anycast επιλέγεται μόνο ένας κάθε φορά από τις συσκευές που ανήκουν στο group.

Σημείωση : Οι anycast διευθύνσεις μπορούν να χρησιμοποιηθούν μόνο ως διευθύνσεις προορισμού! (destination address)

Οι διευθύνσεις Global Unicast και Anycast

Οι δύο αυτοί τύποι διευθύνσεων έχουν την ίδια μορφή. Οι anycast διευθύνσεις προκύπτουν από το εύρος διευθύνσεων των Global Unicast Address.

Όταν μια unicast address ρυθμίζεται σε πάνω από μια συσκευές αυτό την κάνει αυτόματα μια anycast address. Όταν ένα πακέτο έχει προορισμό μια unicast address τότε το πακέτο αυτό ακολουθεί την διαδρομή εκείνη η οποία οδηγεί στην κοντινότερη συσκευή στην οποία έχει αποδοθεί η διεύθυνση αυτή.

Μια χρήση του unicast είναι όταν ένα LAN «πέφτει» πάνω σε πολλούς router. Οι router αυτοί μπορεί να έχουν την ίδια anycast διεύθυνση. Έτσι οι απομακρυσμένες συσκευές το μόνο που πρέπει να γνωρίζουν είναι μια anycast διεύθυνση αντί τις διαφορετικές διευθύνσεις του κάθε router. Οι ενδιάμεσες συσκευές μπορούν να επιλέξουν το κοντινότερο μονοπάτι το οποίο οδηγεί στην συσκευή με την anycast address.

Οι IPv6 global unicast addresses είναι αντίστοιχες με τις IPv4 global unicast addresses. Μια IPv6 global unicast διεύθυνση αποτελείται από ένα global routing prefix , ένα subnet ID και ένα interface ID. Το πεδίο διευθύνσεων τους είναι όλο το πεδίο του εύρους των IPv6 διευθύνσεων εκτός του FF00::/8 το οποίο χρησιμοποιείται για multicast διευθύνσεις.

2.3.4 Interface Identifier

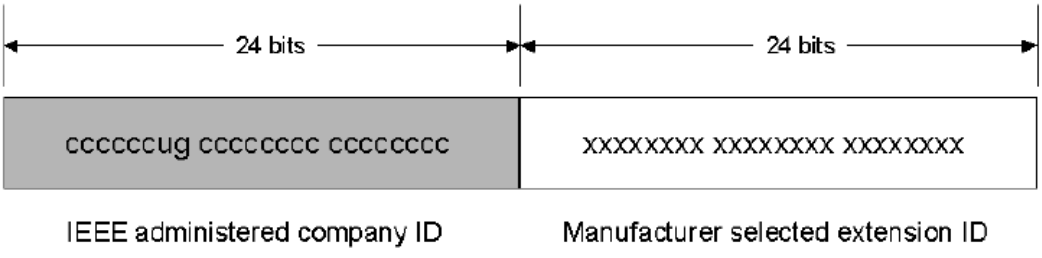
Στο IPv4 οι IP διευθύνσεις δεν σχετίζονται με κάποιο τρόπο με τις φυσικές διευθύνσεις (MAC Address) που χρησιμοποιούνται στο επίπεδο διασύνδεσης δεδομένων (data link layer). Ένας host που συνδέεται πάνω σε ένα TCP/IP δίκτυο χρησιμοποιώντας μια Ethernet κάρτα δικτύου, έχει μια mac διεύθυνση και μια IP διεύθυνση αλλά οι δύο αυτές διευθύνσεις είναι διαφορετικές και δεν έχουν κάποια σχέση μεταξύ τους.

Εξετάζοντας τον τρόπο διευθυνσιοδότησης στο IPv6, παρουσιάζεται μια ευκαιρία συσχέτισης των IPv6 unicast διευθύνσεων με τις mac διευθύνσεις. Με μέγεθος διεύθυνσης 128-bit όπως είδαμε προηγουμένως , ακόμα και με 48 bit δεσμευμένα για το network prefix και 16 υποδικτύωση , υπολείπονται 64 bit τα οποία μπορούν να χρησιμοποιηθούν για το interface identifier. Μπορεί κάποιος να συσχετίσει το interface ID με την φυσική διεύθυνση του host με τον μόνο περιορισμό να μην

ξεπερνάει σε μέγεθος τα 64 bit (υπενθυμίζουμε ότι οι MAC διευθύνσεις είναι 48 bit – η MAC διεύθυνση είναι μοναδική για κάθε host). Έτσι δεν υπάρχει κάποιο πρόβλημα ώστε να χρησιμοποιηθεί η φυσική διεύθυνση ενός host ως interface identifier της IP διεύθυνσης του. Η μέθοδος αυτή έχει το εξής πλεονέκτημα : διευκολύνει τον διαχειριστή ενός δικτύου καθώς δεν υπάρχει λόγος να γίνει καταγραφή δύο διαφορετικών και άσχετων μεταξύ τους διευθύνσεων που ανήκουν σε ένα host. Η IP διεύθυνση μπορεί να προκύψει από την MAC διεύθυνση και το Network Identifier. Αυτό σημαίνει ότι κάποιος μπορεί να υποθέσει την IP διεύθυνση από την MAC διεύθυνση και το αντίθετο.

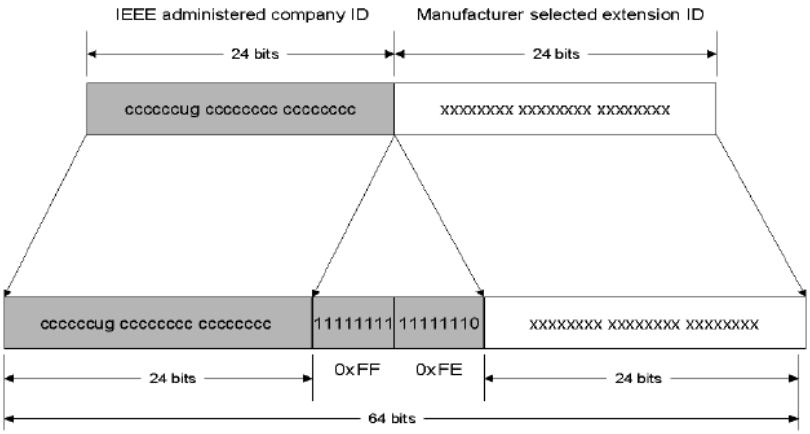
Η μέθοδος συσχέτισης των δύο αυτών διευθύνσεων εξαρτάται από την τεχνολογία που χρησιμοποιείται. Φυσικά είναι απαραίτητο όλες οι συσκευές που ανήκουν στο ίδιο δίκτυο να χρησιμοποιούν την ίδια μέθοδο συσχέτισης διευθύνσεων. Όπως αναφέρθηκε παραπάνω μια MAC διεύθυνση είναι μεγέθους 48-bit με τα πρώτα 24 bit αναφέρονται στον κατασκευαστή (OUI - organizationally unique identifier) και τα υπόλοιπα 24 να αναφέρονται στην συσκευή.

Ο οργανισμός IEEE έχει καθορίσει το οποίο ονομάζεται 64-bit extended unique identifier ή EUI-64. Είναι παρόμοιο με το 48 bit – MAC. Τα πρώτα 24 bit αναφέρονται στον κατασκευαστή του hardware αλλά στην συσκευή αναφέρονται 40 αντί για 24 bit. Μια μορφή του EUI-64 έχει υιοθετηθεί για το IPv6 με την ονομασία modified EUI-64. Ακολουθεί ένα παράδειγμα υπολογισμού του imterface identifier. Παρακάτω φαίνονται τα 48 bit μιας MAC διεύθυνσης.



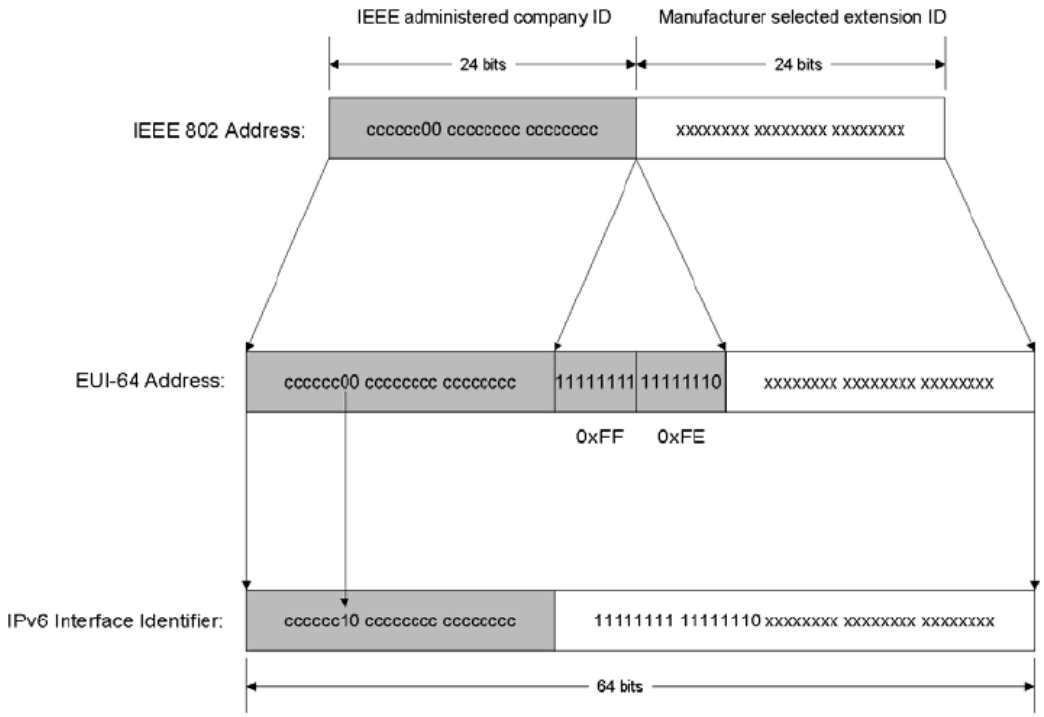
Σχημα 2.3 Σχηαμτισμός του Interface Identifier (1)

Με το γράμμα u συμβολίζεται το U/L (universal/local) bit το οποίο είναι το προτελευταίο bit του πρώτου byte. Επειδή το interface ID όπως αναφέρθηκε και προηγουμένως έχει μέγεθος 64-bit και η MAC Address έχει μέγεθος 48 bit , 16 επιπλέον bit με την τιμή 11111111 11111110
(0xFFFE) εισέρχονται στην MAC διεύθυνση μεταξύ του company ID και του extension ID όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 2.4 Σχηματισμός Interface Identifier (2)

Και τέλος παίρνεται το συμπλήρωμα του U/L (εάν η τιμή του είναι 0 τότε γίνεται 1 και εάν είναι 1 γίνεται 0). Όλοκληρη η διαδικασία φαίνεται στο σχήμα που ακολουθεί.



Σχήμα 2.5 Σχηματισμός Interface Identifier (3)

2.3.5 DHCPv6

Ένα από τα χαρακτηριστικά του πρωτοκόλλου IPv6 είναι η δυνατότητα ευκολότερης παραμετροποίησης και διαχείρισης του δικτύου σε θέματα διευθυνσιοδότησης. Υπάρχουν δύο βασικές μέθοδοι για την παραμετροποίηση των IPv6 hosts.

1.Stateless Autoconfiguration : Είναι μια μέθοδος η οποία επιτρέπει σε ένα host να κάνει ρυθμίσεις αυτόματα.

2.Stateful Autoconfiguration : Σε αυτή την περίπτωση οι πληροφορίες που χρειάζεται ένας host του παρέχονται από ένα server.

Το ποια από τις δύο μεθόδους θα χρησιμοποιηθεί εξαρτάται από τα χαρακτηριστικά του εκάστοτε δικτύου. Το πώς ένας host κάνει χρήση της μεθόδου Stateless

Autoconfiguration περιγράφεται σε επόμενη ενότητα. Σε αυτή θα γίνει αναφορά στην μέθοδο Stateful Autoconfiguration.

Η μέθοδος αυτή παρέχεται μέσω DHCPv6. Όπως και στην περίπτωση του DHCP για το πρωτόκολλο IPv4 , το DHCPv6 μπορεί να χρησιμοποιηθεί για να λάβει ένας host IP διεύθυνση και άλλες πληροφορίες παραμετροποίησης. Η λειτουργία του DHCPv6 είναι παρόμοια με αυτή του DHCPv4 αν και το πρωτόκολλο έχει οριστεί από την αρχή. Δεν βασίζεται στα παλαιότερα DHCP και BOOTP εκτός από κάποιες κοινές έννοιες. Χρησιμοποιεί το πρωτόκολλο UDP αλλά με διαφορετικά port numbers, νέα μορφή μηνύματος και καινούργιες επιλογές. Όλα αυτά σημαίνουν πως το DHCPv6 δεν είναι αυστηρά συμβατό με τα DHCPv4 και BOOTP αν και γίνεται προσπάθεια για τον ορισμό μιας μεθόδου που θα επιτρέπει στους DHCPv6 servers να δουλεύουν με IPv4 hosts.

Επίσης το DHCPv6 είναι προσανατολισμένου γύρω από την IPv6 μέθοδο διευθυνσιοδότησης και ειδικά της χρήσης link local multicast addresses. Αυτό επιτρέπει επιτυχή επικοινωνία ακόμα και χωρίς να έχει αποδοθεί σε ένα client IP διεύθυνση. Όταν ένας έχει διεύθυνση και γνωρίζει την ταυτότητα του server , τότε μπορεί να επικοινωνεί με αυτόν χρησιμοποιώντας unicast διευθυνσιοδότηση.

Η διαδικασία που ακολουθείται είναι η εξής :

1. Ο client στέλνει ένα multicast Solicit μήνυμα για να βρει κάποιον DHCP server από τον οποίο θα δανειστεί μια διεύθυνση.

2.Οποιοσδήποτε server μπορεί να απαντήσει στέλνοντας ένα Advertise μήνυμα.

3.Ο client επιλέγει ένα server και στέλνει ένα Request μήνυμα στο οποίο ζητάει από τον server να επιβεβαιώσει την διεύθυνση που πρόσφερε και άλλες παραμέτρους.

4. Ο server απαντάει με ένα Reply μήνυμα με το οποίο τερματίζεται και η διαδικασία.

Υπάρχει και μια πιο σύντομη διαδικασία με την οποία ο client στέλνει solicit μήνυμα και υποδεικνύει στον server ότι πρέπει να απαντήσει αμέσως με ένα Reply μήνυμα.

Ένας DHCPv6 client μπορεί να ανανεώσει την διεύθυνση στέλνοντας ένα Renew μήνυμα , μια διαδικασία που γίνεται και στο DHCPv4 .

2.3.6 IPv6 και DNS

Οι IP διευθύνσεις τον τύπο εγγραφής AAAA. Ο τύπος αυτός παρέχει ένα πλήρες domain name σε μια IPv6 διεύθυνση. Η δομή του τύπου εγγραφής είναι ως εξής :
Name In AAAA Address
Ένας κόμβος μπορεί να έχει περισσότερες από μια AAAA εγγραφές.

Για παράδειγμα βλέπουμε πως η υπηρεσία της google για IPv6 έχει τις εξής εγγραφές:

```
Non-authoritative answer:
ipv6.google.com canonical name = ipv6.l.google.com
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::63
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::67
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::68
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::69
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::6a
ipv6.l.google.com       AAAA IPv6 address = 2a00:1450:8006::93
> _
```

Το πρόβλημα του Διαμοιρασμού των Ονομάτων

Ένας resolver που ψάχνει για ένα όνομα ξεκινάει κοιτάζοντας στους root server και ακολουθεί παραπομπές μέχρι να φτάσει σε ένα name server ο οποίος έχει καταγεγραμμένη την εγγραφή για αυτό το όνομα. Εάν κάπου μέσα στην διαδρομή ο resolver παραπεμφθεί σε ένα name server ο οποίος μπορεί να γίνει προσβάσιμος από μια διαδρομή που ο resolver δεν μπορεί να ακολουθήσει τότε δεν μπορεί να ολοκληρώσει την «αποστολή» του.

Όταν το διαδίκτυο μετατραπεί σε ένα μείγμα τόσο από IPv4 αλλά και IPv6 κόμβους, τότε το παραπάνω σενάριο θα συμβαίνει αρκετά συχνά. Ολόκληρη η ιεραρχία του

DNS θα διαχωριστεί σε ένα σχήμα όπου κάποιοι name servers θα είναι προσβάσιμοι μόνο πάνω από μια συγκεκριμένη διαδρομή. Η ανησυχία είναι πως ένας resolver που χρησιμοποιεί μια συγκεκριμένη έκδοση IP και ψάχνει για την διεύθυνση ενός άλλου κόμβου που χρησιμοποιεί την ίδια έκδοση, δεν θα μπορεί να το κάνει διότι κάπου μέσα στο «μονοπάτι» κάποιος server θα χρησιμοποιεί άλλη έκδοση IP.

Με όλα τα DNS δεδομένα διαθέσιμα μέσω IPv4 η διαδικασία είναι απλή. Οι IPv4 resolvers ξεκινούν να ψάχνουν από τους root servers και κάτω στην ιεραρχία, ενώ οι IPv6 resolvers χρειάζονται έναν translator καθώς δεν έχουν άμεση πρόσβαση στα DNS δεδομένα.

Το ίδιο συμβαίνει και σε ένα περιβάλλον που τα DNS δεδομένα θα είναι διαθέσιμα μέσω IPv6. Παρόμοια διαδικασία θα ακολουθούν οι IPv6 resolvers , ενώ οι IPv4 resolvers θα χρειάζονται κάποιον translator για να γίνεται η προώθηση των ερωτημάτων τους.

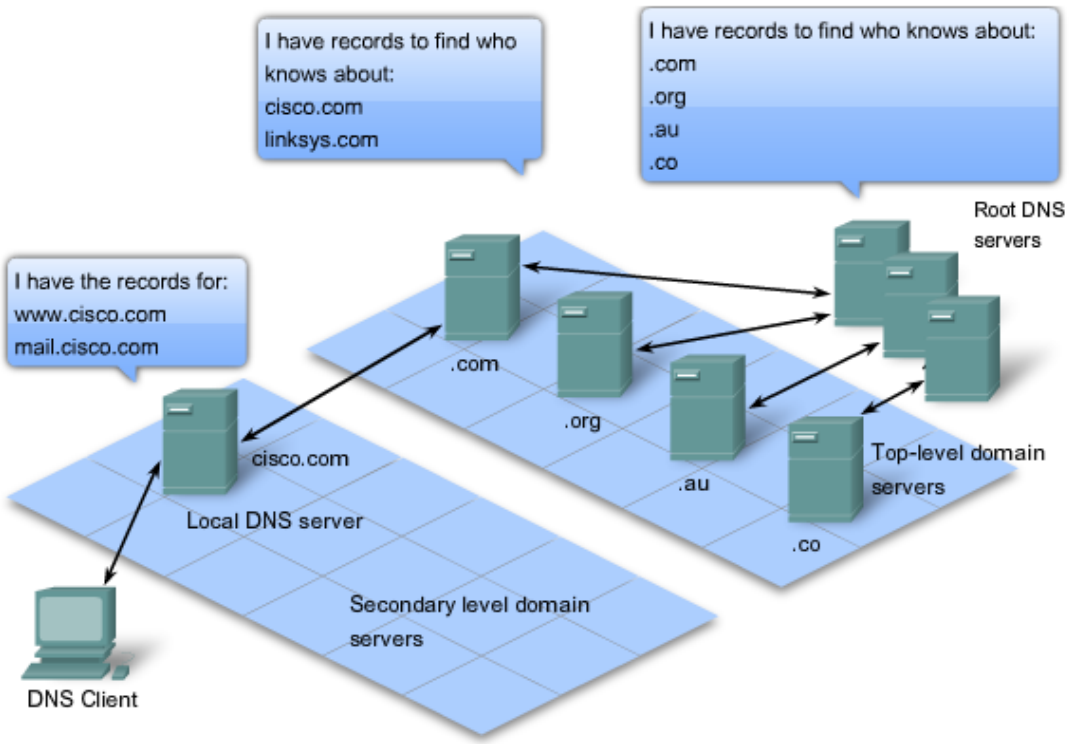
Το δεύτερο σενάριο δεν είναι πολύ πιθανό στο άμεσο μέλλον καθώς όπως έχουμε αναφέρει κατά την διάρκεια της μετάβασης τα δύο πρωτόκολλα θα συνυπάρξουν , και ο αριθμός των κόμβων που θα χρησιμοποιούν τα δύο πρωτόκολλα θα είναι διαμοιρασμένος. Έτσι θα υπάρχουν τρεις κατηγορίες DNS δεδομένων , με βάση αν τα δεδομένα θα είναι διαθέσιμα μέσω IPv4 μόνο, μέσω IPv6 μόνο ή μέσω και των δύο πρωτοκόλλων.

Το να είναι τα DNS δεδομένα διαθέσιμα μέσω και των δύο πρωτοκόλλων είναι η καλύτερη περίπτωση. Το ερώτημα είναι πως θα διασφαλιστεί μια τέτοια περίπτωση όσο το δυνατόν συντομότερα. Αν και είναι προφανές πως κάποια DNS δεδομένα θα είναι διαθέσιμα μόνο μέσω IPv4 για αρκετό καιρό, είναι επίσης σημαντικό να μην διαμοιραστούν οι εγγραφές που είναι διαθέσιμες στους IPv4 hosts.

Σήμερα υπάρχουν λίγες DNS “ζώνες” στο διαδίκτυο που είναι διαθέσιμες μέσω IPv6 και αρκετές από αυτές μπορούν να θεωρηθούν και πειραματικές. Βέβαια, όσο το γρηγορότερο τα root και top level domain γίνουν διαθέσιμα μέσω IPv6 είναι λογικό να περιμένουμε πως θα υπάρξουν πολλές ζώνες οι οποίες θα εξυπηρετούνται από

IPv6 servers. Αυτό θα χωρίσει το IPv4 name space και πρέπει να βρεθεί ένας μηχανισμός ο οποίος θα αποτρέπει κάτι τέτοιο.

Κάποιες γενικές οδηγίες για την αποφυγή του παραπάνω προβλήματος είναι οι εξής :
-Κάθε name server θα πρέπει να είναι είτε IPv4-only είτε dual stack.
-Κάθε DNS ζώνη θα πρέπει να εξυπηρετείται από ένα τουλάχιστον name server ο οποίος είναι διαθέσιμος μέσω IPv6.



Σχήμα 2.6 Ιεραρχία των DNS Servers

3 Μηχανισμοί Μετάβασης

Η μετάβαση από το IPv4 στο IPv6 δεν είναι εύκολη υπόθεση , αναλογιζόμενοι του μεγέθους του διαδικτύου σήμερα και τον αριθμό των χρηστών του. Πολλές εταιρίες και οργανισμοί σήμερα στηρίζονται στο internet για την λειτουργία τους και την παροχή υπηρεσιών κάτι που καθιστά αδύνατη μια μετάβαση στο IPv6 με κατέβασμα των συστημάτων τους έστω και για ελάχιστο χρονικό διάστημα. Ο σημαντικότερος παράγοντας επιβράδυνσης της μετάβασης , είναι η μέχρι στιγμής μικρή κατανόηση των απαιτήσεων του πρωτοκόλλου αλλά και των δυνατοτήτων που προσφέρει. Η ανάγκη για μετάβαση στο νέο πρωτόκολλο το οποίο θα λύσει πολλά από τα προβλήματα του προκατόχου του δεν έχει γίνει κατανοητή από όλους. Όλα αυτά δείχνουν ότι δεν μπορεί να γίνει η μετάβαση από την μια στιγμή στην άλλη ούτε έχει οριστεί μια "D-Day" μέχρι την οποία θα έχει γίνει η μετάβαση. Η λύση είναι η μετάβαση να γίνει σταδιακά και "ανώδυνα".

Το γεγονός αυτό είχε ληφθεί υπ' όψιν από την IETF το νέο πρωτόκολλο είχε σχεδιαστεί ώστε να είναι συμβατό με το IPv4. Επίσης είχε συσταθεί μια ομάδα η οποία θα ασχολούταν αποκλειστικά με τα θέματα της μετάβασης. Η έρευνα που επιτελούταν στο θέμα της μετάβασης είχε ως στόχο κάποιους μηχανισμούς οι οποίοι να πρσφέρουν:

- **Δυνατότητα σταδιακής μετάβασης ,** έτσι ώστε οι IPv4 hosts και routers του κάθε δικτύου να μπορούν να αναβαθμιστούν σε IPv6 ο καθένας ξεχωριστά χωρίς να υπάρχει η απαίτηση το πρωτόκολλο να έχει εγκατασταθεί και στους υπόλοιπους κόμβους.
- **Ελάχιστες απαιτήσεις αναβάθμισης ,** και συγκεκριμένα το μόνο που απαιτείται είναι ένας DNS server να χειρίζεται τις εγγραφές στην περίπτωση των host , στην περίπτωση των router δεν υπάρχει καμία απαίτηση.
- **Απλότητα διευθυνσιοδότησης ,** και συγκεκριμένα δυνατότητα να διατηρηθούν οι IPv4 διευθύνσεις που είχε το μηχάνημα πριν την αναβάθμιση παράλληλα με τις νέες IPv6 διευθύνσεις.

Για τους λόγους αυτούς καθορίστηκαν ένα σύνολο κανόνων SIT (Simple Internet Transition) για την διευκόλυνση της μετάβασης. Συγκεκριμένα το SIT παρέχει :

-Μια δομή IPv6 διευθύνσεων που μπορεί να προκύψει από τις ήδη υπάρχουσες IPv4 διευθύνσεις. Οι διευθύνσεις αυτές είναι οι IPv6 IPv4 compatible της μορφής ::ww.xx.yy.zz όπου ww.xx.yy.zz η IPv4 διεύθυνση του κόμβου.

-Την δυνατότητα λειτουργίας των λειτουργικών συστημάτων ως dual stack. Δηλαδή ταυτόχρονη υποστήριξη και των δύο πρωτοκόλλων χωρίς το ένα πρωτόκολλο να επεμβαίνει στην λειτουργία του άλλου και το κάθε μηχάνημα συνήθως αναλόγως της αναζήτησης που κάνει μέσω DNS επιλέγει ποια στοίβα θα χρησιμοποιήσει.

-Ένα μηχανισμό για την ενθυλάκωση IPv6 πακέτων μέσα σε IPv4 πακέτα (tunneling) για την μετάδοση πάνω από IPv4 backbone συσκευών δικτύου. Οι μηχανισμοί αυτοί είναι οι πλέον χρησιμοποιούμενοι σήμερα και θα αναλυθούν στην συνέχεια.

-Προαιρετικά μετατροπή του IPv6 πακέτου σε IPv4 και αντίστροφα.

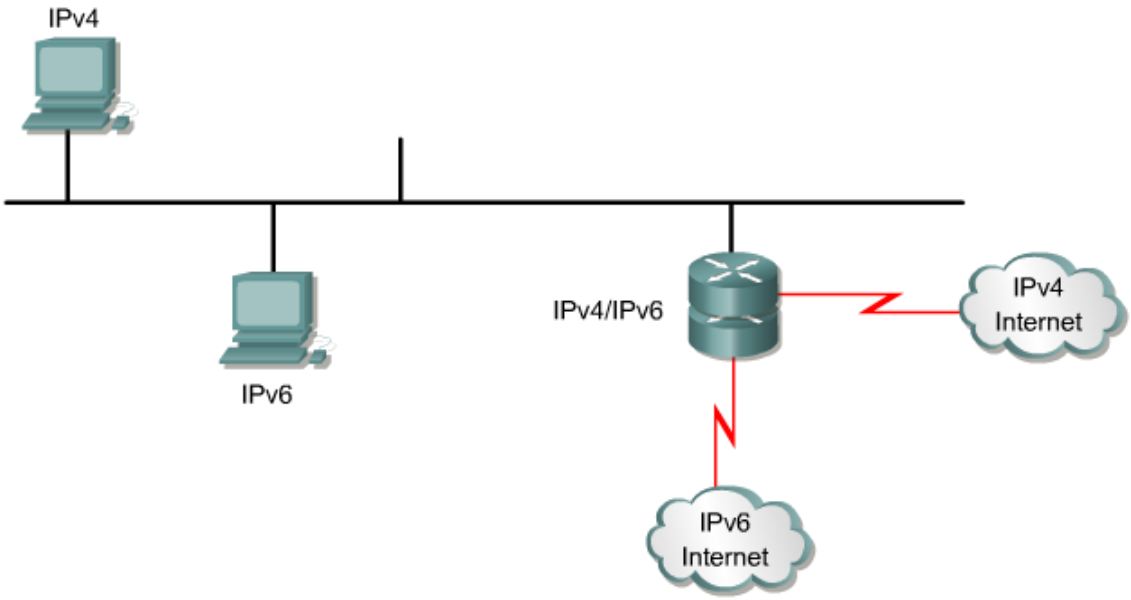
Βάση των δυνατοτήτων αυτών που προσφέρει το SIT , προέκυψαν σε αυτό το διάστημα συνύπαρξης των δύο πρωτοκόλλων αρκετοί μηχανισμοί μετάβασης που μπορούν αν ταξινομηθούν στις κάτωθι κατηγορίες.

- Μηχανισμοί Dual Stack (διπλής στοίβας)
- Μηχανισμοί Tunneling
- Μηχανισμοί Translation

3.1 Μηχανισμοί Dual Stack

Οι μηχανισμοί αυτοί είναι σχετικά απλοί στην υλοποίηση τους , η οποία έγκειται απλώς στην εγκατάσταση και των δύο πρωτοκόλλων στα λειτουργικά συστήματα (OS) των συσκευών του δικτύου.

Έτσι οι συσκευές οι οποίες είναι dual stack μπορούν να λάβουν και να προωθήσουν πακέτα και από τα δύο πρωτόκολλα. Η επιλογή του πρωτοκόλλου που θα χρησιμοποιηθεί γίνεται κατά βάση από την DNS αναζήτηση.
Αν ο κόμβος που θα γίνει η επικοινωνία έχει καταγεγραμμένη μόνο IPv6 διεύθυνση , επιλέγεται η IPv6 στοίβα , αν έχει μόνο IPv4 επιλέγεται η αντίστοιχη IPv4 στοίβα ενώ εάν είναι dual stack τότε η default συμπεριφορά είναι να χρησιμοποιηθεί το IPv6. Για να εγγράψει κάποιος κόμβος την IPv6 σύνδεση του πρέπει με κάποιο τρόπο να του παρέχεται IPv6 συνδεσιμότητα (είτε native είτε μέσω tunnel) εκτός από την εγκατάσταση της IPv6 στοίβας. Αυτή είναι και η αδυναμία της συγκεκριμένης κατηγορίας μηχανισμών στο παρών στάδιο μετάβασης. Δηλαδή απομονωμένοι dual stack κόμβοι στους οποίους δεν παρέχεται IPv6 συνδεσιμότητα πρέπει να συνεργαστούν με κάποιο άλλο μηχανισμό μετάβασης (πχ tunneling) ώστε να είναι δυνατή η μεταξύ τους επικοινωνία.



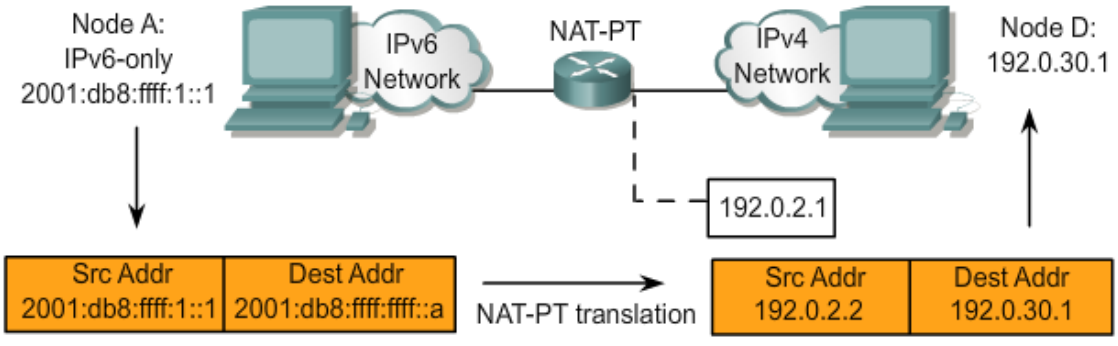
Σχήμα 3.1 Dual Stack Δρομολογητής

3.2 Μηχανισμοί Translation

Οι μηχανισμοί αυτοί επιτρέπουν την επικοινωνία κόμβων που υποστηρίζουν μόνο IPv4 (IPv4 only) με κόμβους που υποστηρίζουν αντίστοιχα μόνο IPv6 (IPv6 only) και ουσιαστικά μεταφράζουν την κίνηση μεταξύ των δύο πρωτοκόλλων. Εκτιμάται ότι θα χρησιμοποιηθούν πολύ στα τελευταία στάδια της μετάβασης και ειδικά για εκείνες τις συσκευές που δεν θα είναι δυνατή η αναβάθμισή τους.

3.2.1 NAT-PT

Ο κυριότερος μηχανισμός translation είναι το NAT-PT (NAT-Protocol Translator). Το NAT-PT είναι ένας μηχανισμός translation ο οποίος εγκαθίσταται μεταξύ ενός IPv4 only και ενός IPv6 only δικτύου. Ο ρόλος του είναι να «μεταφράζει» IPv6 πακέτα σε IPv4 και το αντίστροφο. Το static NAT-PT χρησιμοποιεί static translation ώστε να αντιστοιχήσει μια IPv6 διεύθυνση σε μια IPv4 (σχέση 1:1). Οι κόμβοι στο IPv6 δίκτυο επικοινωνούν με εκείνους του IPv4 κάνοντας χρήση της αντιστοίχησης των διευθύνσεων σύμφωνα με το configuration που έχει γίνει στο NAP-PT router που παρεμβάλλεται μεταξύ των δύο δικτύων. Στο παρακάτω σχήμα φαίνεται πως ένας IPv6 only κόμβος (Node A) μπορεί να επικοινωνήσει με έναν IPv4 only (Node D) χρησιμοποιώντας τον μηχανισμό NAT-PT.



Σχήμα 3.2 Επικοινωνία μέσω NAT-PT

Ο NAT-PT router έχει ρυθμιστεί ώστε να αντιστοιχεί την διεύθυνση IPv6 του Node A 2001:0db8:ffff:1::1 στην

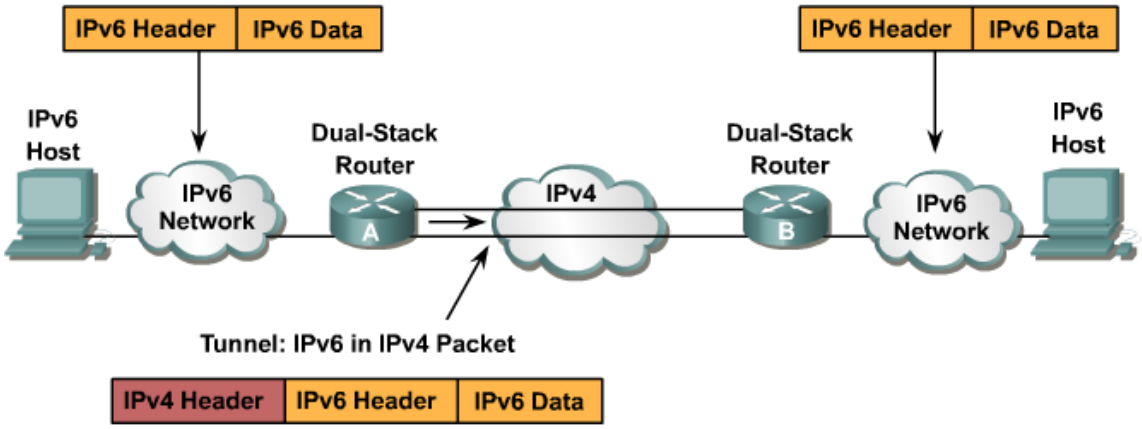
IPv4 192.0.2.2 αντίστοιχα η IPv4 διεύθυνση του Node D 192.0.30.1 να αντιστοιχεί στην IPv6 2001:0db8:ffff:ffff::a. Όταν ο NAT-PT router λαμβάνει πακέτα τα οποία προέρχονται από τον Node A μεταφράζονται ώστε να έχουν διεύθυνση προορισμού αυτή που ανταποκρίνεται στο Node D. Ο Node A από την μεριά του βλέπει ότι εγκαθιστά επικοινωνία με IPv6 συσκευή.

3.3 Μηχανισμοί Tunneling

Για όσο διάστημα διευρύνεται η χρήση του IPv6 είναι χρήσιμο αλλά και αναγκαίο τουλάχιστον στο στάδιο μετάβασης , η IPv4 υποδομή να παραμείνει λειτουργική και να χρησιμοποιηθεί επίσης για την μετλαδοση πληροφορίας. Η πιο διαδεδομένη τεχνική , με την οποία γίνεται εκμετάλλευση της IPv4 υποδομής για την μεταφορά IPv6 πακέτων είναι η μηχανισμοί tunneling.

Το tunneling γενικότερα είναι ένας μηχανισμός που χρησιμοποιείται ευρέως σήμερα και στηρίζεται στην ενθυλάκωση (encapsulation) ενός πρωτοκόλλου δικτύου σε πακέτα άλλου πρωτοκόλλου για την μετάδοση τους πάνω από ένα κανάλι (πχ το GRE – Generic Routing Encapsulation που χρησιμοποιείται σε αρκετές περιπτώσεις σήμερα). Η τεχνική αυτή χρησιμοποιείται και στο μεταβατικό στάδιο από το IPv4 στο IPv6. Συγκεκριμένα IPv6 hosts και routers έχουν την δυνατότητα να ανταλλάσουν IPv6 πακέτα τα οποία εχουν ενθυλακωθεί σε IPv4 πακέτα μεταδίδοντας τα με αυτό τον τρόπο πάνω από το ήδη υπάρχον δίκτυο (internet). Έτσι οι ενδιάμεσοι backbone routers αν και δεν υποστηρίζουν το IPv6 πρωτόκολλο προωθούν τα ενθυλακωμένα πακέτα σαν να πρόκειται για κανονικά IPv4 πακέτα.

Για την λειτουργία των μηχανισμών tunneling πρέπει και οι δύο κόμβοι στα άκρα του tunnel – οι κόμβοι δηλαδή που εκτελούν την διαδικασία της ενθυλάκωσης και απενθυλάκωσης των πακέτων – να είναι dual stack δηλαδή να υποστηρίζουν και τις δύο στοίβες πρωτοκόλλων.



Σχήμα 3.3 Tunnel Μεταξύ δύο απομονωμένων IPv6 δικτύων

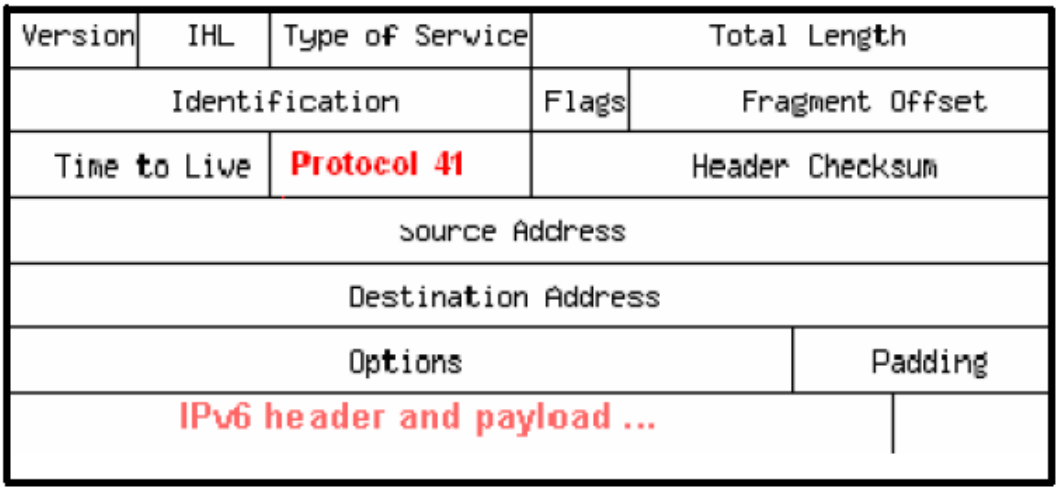
3.3.1 Είδη Μηχανισμών Tunneling

Οι μηχανισμοί tunneling χωρίζονται σε κατηγορίες με βάση τον μηχανισμό με τον οποίο ο κόμβος εισόδου που πραγματοποιεί την ενθυλάκωση ορίζει την διεύθυνση του κόμβου εξόδου (του άλλου άκρου του tunnel), σε μηχανισμούς manually configured tunneling και automatic tunneling.

Στο **manually configured tunneling** η IPv4 διεύθυνση του άλλου άκρου του tunnel , καθορίζεται από τις πληροφορίες που έχει ο router που εκτελεί την ενθυλάκωση μέσω του configuration που του έχει γίνει από τον διαχειριστή του. Για το κάθε tunnel που υλοποιεί ο συγκεκριμένος κόμβος πρέπει να έχει αποθηκευμένη την αντίστοιχη διεύθυνση του άλλου άκρου του tunnel . Όταν ένα πακέτο μεταδίδεται μέσω του tunnel , η διεύθυνση του άλλου άκρου του tunnel τίθεται ως η διεύθυνση προορισμού (destination address) στο IPv4 πακέτο μέσα στο οποίο ενθυλακώνεται το IPv6 πακέτο.

Στο **automatic tunneling** η IPv4 διεύθυνση του άκρου του tunnel , μπορεί να προκύψει από την IPv6 διεύθυνση προορισμού του πακέτου που πρόκειται να

μεταδοθεί μέσω του tunnel. Δηλαδή στην περίπτωση αυτή με κάποιο τρόπο η IPv4 διεύθυνση περιέχεται μέσα στην IPv6. Στην περίπτωση αυτή οι IPv6/IPv4 κόμβοι επικοινωνούν πάνω από την IPv4 υποδομή χωρίς να χρειάζεται να έχουν γίνει εκ των προτέρων configured τα tunnel που θα χρησιμοποιηθούν.



Σχήμα 3.4 Ενθυλακωμένο IPv6 πακέτο

3.3.2 Λειτουργία Μηχανισμών Tunneling

Τα κύρια χαρακτηριστικά και για δύο κατηγορίες tunnels (manually configured , automatic) είναι ίδια.

-Ο κόμβος στον οποίο γίνεται η ενθυλάκωση (encapsulation) δημιουργεί την IPv4 επικεφαλίδα με την τιμή 41 στο πεδίο protocol κάτω από την οποία ενθυλακώνει το IPv6 πακέτο, και στην συνέχεια δρομολογεί το πακέτο με IPv4 δρομολόγηση , θέτοντας ως διεύθυνση προορισμού την IPv4 διεύθυνση του κόμβου εξόδου όπου θα γίνει η απενθυλάκωση (decapsulation).

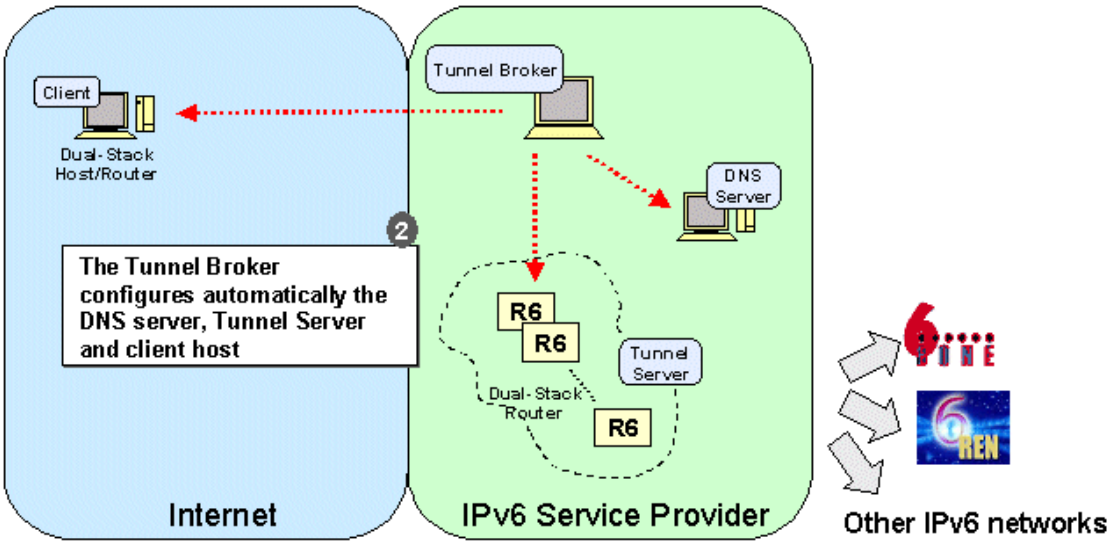
-Στο άλλο άκρο του tunnel όπου γίνεται η απενθυλάκωση , ο κόμβος παραλαμβάνει το ενθυλακωμένο πακέτο το επανασυναρμολογεί εάν έχει προκύψει κατακερματισμός του (fragmentation) και αφού δει την τιμή 41 στο πεδίο protocol αφαιρεί την IPv4 επικεφαλίδα. Στην συνέχεια εάν η διεύθυνση προορισμού είναι διαφορετική από την δικιά του δρομολογεί αντιστοίχως το πακέτο με κανονική IPv6 δρομολόγηση. Κατά την διάρκεια της απενθυλάκωσης δεν μεταβάλεται η IPv6 επικεφαλίδα παρά μόνο μειώνεται η τιμή του πεδίου hop limit κατά ένα σε περίπτωση περαιτέρω προώθησης του πακέτου.

-Υπάρχει η περίπτωση ο κόμβος εισόδου να χρειάζεται να κρατά πληροφορίες για κάποιες παραμέτρους όπως MTU (Maximum Transfer Unit) και Hop Limit ώστε να μπορεί να προωθήσει τα πακέτα μέσα στο tunnel.

3.4 Μηχανισμοί Automatic Tunneling

3.4.1 Tunnel Broker

Ο συγκεκριμένος μηχανισμός προσφέρει τον απλούστερο τρόπο σε ένα dual stack host που αποτελεί μέρος ενός IPv4 δικτύου να επικοινωνήσει με IPv6 κόμβους. Η ιδέα του βασίζεται στην παροχή dedicated servers που λέγονται Tunnel Brokers οι οποίοι διαχειρίζονται αυτόματα τις αιτήσεις των χρηστών που απαιτούν IPv6 συνδεσιμότητα. Η προσέγγιση αυτή προσδοκάται ότι θα υποκινήσει αρκετούς χρήστες να αποκτήσουν πρόσβαση σε IPv6 δίκτυα λόγω της απλότητας της. Η βασική διαφορά του Tunnel Broker και άλλων μηχανισμών όπως πχ. 6to4 που θα αναφερθούν στην συνέχεια, είναι ότι εξυπηρετούν διαφορετικά κομμάτια της IPv6 κοινότητας. Το tunnel broker είναι κατάλληλο για μικρά απομονωμένα IPv6 δίκτυα και ακόμα καλύτερα για hosts οι οποίοι αποτελούν κομμάτι του ήδη υπάρχοντος IPv4 internet και θέλουν να έχουν επικοινωνία με κάποιο IPv6 δίκτυο. Το 6to4 έχει σχεδιαστεί ώστε να επιτρέπει σε απομονωμένα IPv6 δίκτυα να έχουν επικοινωνία μεταξύ τους , χωρίς να περιμένουν από τους ISPs να τους παρέχουν IPv6 υπηρεσίες. Αυτό είναι κατάλληλο για δίκτυα extranet και vpn.



Σχήμα 3.5 Το μοντέλο Tunnel Broker

Το Tunnel Broker που φαίνεται στο σχήμα είναι το σημείο που ο χρήστης συνδέεται για να δηλώσει και να ενεργοποιήσει τα tunnels (συνήθως είναι κάποια site που προσφέρουν την υπηρεσία , οπότε η σύνδεση γίνεται σε ένα web server). Στέλνει οδηγίες για την δήλωση , ενεργοποίηση , παραμετροποίηση ή διαγραφή ενός tunnel στον αντίστοιχο tunnel server. Το tunnel broker μπορεί επίσης να δηλώσει το όνομα και την IPv6 διεύθυνση του χρήστη στο DNS.

Ένας tunnel server είναι ένας dual stack δρομολογητής ο οποίος έχει σύνδεση με το διαδίκτυο. Όταν λάβει οδηγίες παραμετροποίησης από τον Tunnel Broker τότε δημιουργεί αλλάζει ή διαγράφει το tunnel από την μεριά του. Μπορεί επίσης να διατηρεί στατιστικά χρήσης για κάθε ενεργό tunnel.

Ο χρήστης της υπηρεσίας από την μεριά του έχει ένα dual stack router ή απλό host ο οποίος έχει σύνδεση στο Internet. Όταν ζητήσει IPv6 συνδεσιμότητα αρχικά πρέπει να διαθέσει τις εξής πληροφορίες:

-Την IPv4 διεύθυνση του που θα έχει το tunnel από την μεριά του.

-Ένα όνομα που θα χρησιμοποιηθεί στην δήλωση της IPv6 διεύθυνσης του tunnel από την μεριά του client στο DNS.

Επίσης εάν ο client είναι ένας router ο οποίος θέλει να εξυπηρετήσει αρκετούς host τότε αντί για μια IPv6 διεύθυνση μπορεί να ζητήσει όσες χρειάζεται ανάλογα με τον αριθμό των host που θα εξυπηρετεί.

Το tunnel broker διαχειρίζεται τις αιτήσεις των clients ως εξής :

1.Αρχικά υποδεικνύει ένα Tunnel Server ο οποίος θα ενεργεί ως tunnel endpoint.

2.Επιλέγει το IPv6 prefix το οποίο θα αποδοθεί στον client. Το μέγεθός του μπορεί να είναι οποιοδήποτε μεταξύ 0 και 128. Τα πιο συνηθισμένα είναι τα /48 (site prefix) /64(subnet prefix) και /128 (host prefix).

3.Δηλώνει στο DNS τις public IPv6 διευθύνσεις που έχουν ανατεθεί στα δύο άκρα του tunnel.

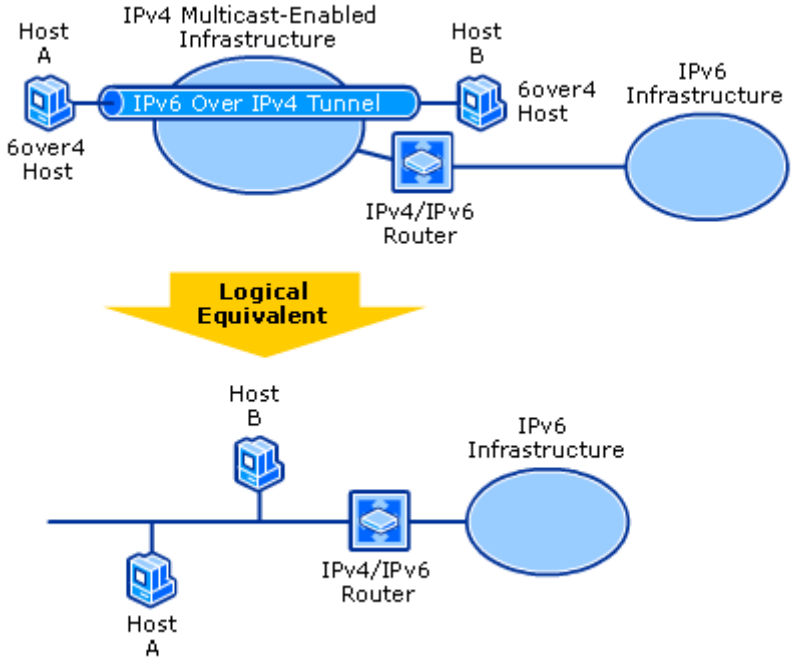
4.Κάνει τις απαραίτητες ρυθμίσεις του tunnel από την μεριά του server.

5.Στέλνει στον client πληροφορίες σχετικά με το tunnel και κάποιες οδηγίες για να κάνει το configuration που χρειάζεται στον υπολογιστή του. Μετά την ολοκλήρωση ο χρήστης μπορεί να συνδεθεί σε IPv6 δίκτυα.

Ο μηχανισμός αυτός είναι ο απλούστερος για home users οι οποίοι επιθυμούν σύνδεση στο IPv6 Ιντερνετ στις περισσότερες περιπτώσεις παρέχεται δωρεάν. Κάποια από τα πιο γνωστά site που προσφέρουν την υπηρεσία είναι : *www.tunnelbroker.net* , *www.sixxs.net*,

3.4.2 6over4

Ο μηχανισμός αυτός επιτρέπει την επικοινωνία αποκομμένων IPv6 host που βρίσκονται μέσα σε ένα IPv4 domain το οποίο υποστηρίζει IPv4 multicast να επικοινωνούν μέσω αυτόματων tunnel. Η ιδέα για την μέθοδο αυτή είναι να είναι δυνατή η επικοινωνία αυτών των host χωρίς να είναι απαραίτητη η παρουσία IPv6 router στο δίκτυο που ανήκουν. Για να επιτευχθεί αυτό πρέπει να γίνει χρήση ενός IPv4 multicast domain σαν εικονική σύνδεση. Με αυτόν τον τρόπο τουλάχιστον ένας IPv6 router που χρησιμοποιεί την ίδια μέθοδο πρέπει να συνδεθεί στο IPv4 domain ώστε να αναλάβει την δρομολόγηση των IPv6 πακέτων όπου είναι απαραίτητο.
Ο μηχανισμός αυτός είναι γνωστός και ως multicast tunneling , χρησιμοποιεί την IPv4 υποδομή σαν να επρόκειτο για ένα τμήμα φυσικής ζεύξης δηλαδή ένα LAN όπως φαίνεται και στο παρακάτω σχήμα.



Σχήμα 3.6 Μηχανισμός 6over4

Οι κόμβοι στους οποίους έχει εγκατασταθεί 6over4 κάνουν configure μόνοι τους την link local διεύθυνση τους FE80::wwxx:yyzz (όπου wwxxyyzz η IPv4 διεύθυνση τους) και χρησιμοποιούν τις διεργασίες του Neighbor Discovery όπως γίνεται σε μια φυσική ζεύξη με δυνατότητες multicast. Για παράδειγμα ένας host με την διεύθυνση 192.0.2.142 θα χρησιμοποιήσει την fe80::c000:028e σαν την link local διεύθυνση του (το c000:028e είναι η δεκαεξαδική αναπαράσταση του 192.0.2.142). Εαν γνωρίζει την αντιστοιχία link local διεύθυνσης και multicast διεύθυνσης ένας host μπορεί να χρησιμοποιήσει το ICMPv6 για την διαδικασία Neighbor Discovery και στην συνέχεια να εκτελέσει stateless autoconfiguration.

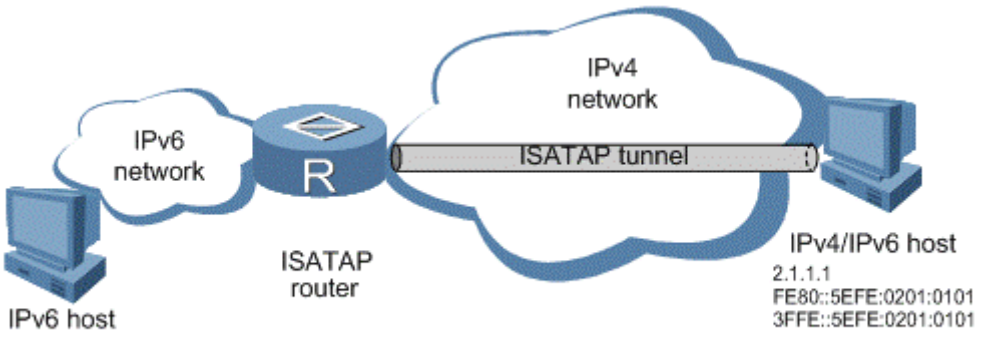
Ο συγκεκριμένος μηχανισμός δεν χρησιμοποιήθηκε πολύ λόγω της απαίτησης σου για IPv4 multicast κάτι που οι περισσότεροι ISP και διαχειριστές δεν το παρέχουν.

3.4.3 ISATAP

Το ISATAP (Intra Site Automatic Tunneling Addressing Protocol) είναι η εναλλακτική επιλογή στο πρόβλημα που δημιουργείται με το 6over4. Χρησιμοποιεί την IPv4 υποδομή σαν ένα εικονικό link δεν θέτει όμως την προϋπόθεση για υποστήριξη IPv4 multicast. Επίσης και σε αυτή την περίπτωση ο μηχανισμός λειτουργεί και κάτω από NAT (Network Address Translation).

Χρησιμοποιεί σαν link local πρόθεμα το fe80::/64 και interface identifier 0:5efe:w.x.y.z (όπου w.x.y.z η IPv4 διεύθυνση του interface είτε public είτε private). Έτσι σχηματίζεται η link local διεύθυνση για επικοινωνία με τον ISATAP router. Για παράδειγμα ένας host με διεύθυνση 192.0.2.143 θα χρησιμοποιήσει την link local διεύθυνση: fe80:0000:0000:0000:0000:5efe:c000:028f όπου c000028f η δεκαεξαδική αναπαράσταση της 192.0.2.143 που για λόγους συντομίας γράφεται και ως fe80::5efe:c000:28f . Λόγω της έλειψης υποστήριξης multicast δεν είναι δυνατή η αυτόματη διαδικασία Router Discovery. Έτσι κάθε ISATAP host πρέπει να ρυθμιστεί με PRL. Μόλις αρχικοποιηθεί ένας ISATAP κόμβος ψάχνει μέσω DNS για το όνομα ISATAP λαμβάνοντας έτσι τις διευθύνσεις όλων των ISATAP routers και φτιάχνει την PRL (Potential Router List). Καθένας από αυτούς τους router ελέγχονται ανά μεγάλα χρονικά διαστήματα μέσω ICMPv6 Router Discovery ώστε να καθοριστεί ποιοι από αυτούς τους router λειτουργούν για την εκτέλεση unicast-only autoconfiguration. Αρχικά ο host στέλνει μήνυμα Router Solicitation και ο router απαντάει με router advertisement στον host , όπου μέσα περιέχεται το site prefix έτσι ώστε ο host να φτιάξει την δική του μοναδική public διεύθυνση.

Στην περίπτωση επικοινωνίας μέσα στο ίδιο site τα πακέτα ενθυλακώνονται μέσα στον ISATAP host και ως IPv4 διεύθυνση προορισμού η διεύθυνση που προκύπτει από τον Interface Identifier της διεύθυνσης προορισμού (τα τελευταία 4 bytes). Σε περίπτωση που η επικοινωνία γίνεται με ISATAP ή IPv6 native κόμβο που βρίσκεται σε άλλο site τα πακέτα ενθυλακώνονται και στέλνονται στον ISATAP router.
Ο μηχανισμός αυτός παρέχει υλοποίηση του IPv6 σε διασκορπισμένους κόμβους που βρίσκονται μέσα σε IPv4 domains , υποστηρίζεται στα περισσότερα λειτουργικά συστήματα και επιπλέον δουλεύει και κάτω από NAT.



Σχήμα 3.7 Ο μηχανισμός ISATAP

3.4.4 Teredo

Ο μηχανισμός Teredo σχεδιάστηκε με στόχο να εγγυηθεί IPv6 συνδεσιμότητα σε κόμβους που βρίσκονται πίσω από NAT συσκευές οι οποίες δεν έχουν γνώση της ύπαρξης IPv6. Καθορίζει ένα τρόπο ενθυλάκωσης IPv6 πακέτων μέσα σε IPv4 UDP Datagrams τα οποία μπορούν να δρομολογηθούν μέσω NAT στο IPv4 Internet.

Ο μηχανισμός 6to4 όταν χρησιμοποιείται, απαιτεί στα άκρα του tunnel να υπάρχουν στατικές δημόσιες διευθύνσεις . Οι περισσότεροι host όμως σήμερα, επικοινωνούν με το Internet μέσω NAT. Σε αυτή την περίπτωση η μοναδική δημόσια IPv4 διεύθυνση ανατίθεται στην συσκευή που εκτελεί το NAT έτσι ως άκρο του 6to4 tunnel πρέπει να τεθεί η συσκευή αυτή. Δεν είναι δυνατή όμως η αναβάθμιση όλων αυτών των συσκευών ώστε να υποστηρίζουν 6to4 είτε για τεχνικούς είτε για οικονομικούς λόγους.

Το Teredo δίνει λύσει σε αυτό το πρόβλημα με την ενθυλάκωση των IPv6 πακέτων μέσα σε UDP/IPv4 datagrams τα οποία το NAT μπορεί να τα προωθεί χωρίς πρόβλημα. Έτσι οι IPv6 host που βρίσκονται πίσω από το NAT μπορούν να

χρησιμοποιηθούν ως η άκρη του tunnel ακόμα και αν δεν διαθέτουν δημόσιες στατικές IPv4 διευθύνσεις. Στην πραγματικότητα ένας host που υλοποιεί Teredo μπορεί να αποκτήσει IPv6 συνδεσιμότητα χωρίς να κάνει χρήση του τοπικού δικτυακού εξοπλισμού (πχ ένα dual stack router). Ένα μειονέκτημα του είναι πως δουλεύει κάτω από συγκεκριμένα είδη NAT (για παράδειγμα δεν λειτουργεί εάν ο host βρίσκεται πίσω από symmetric NAT).

Το πρωτόκολλο Teredo εκτελεί διάφορες λειτουργίες:

-Αναγνωρίζει την επικοινωνία UDP over IPv4 και το είδος του NAT που χρησιμοποιείται.

-Αναθέτει σε κάθε Teredo host IPv6 διευθύνσεις οι οποίες είναι δρομολογήσιμες.

-Ενθυλακώνει IPv6 πακέτα μέσα σε UDPv4 datagrams για την μετάδοση τους πάνω από το IPv4 δίκτυο.

-Δρομολογεί την κίνηση μεταξύ Teredo hosts και native (non Teredo) IPv6 hosts.

Είδη Teredo κόμβων

Το Teredo καθορίζει διάφορα είδη κόμβων:

Teredo Client : Είναι ένας host ο οποίος έχει IPv4 συνδεσιμότητα με το Internet μέσω NAT και χρησιμοποιεί το Teredo ώστε να έχει πρόσβαση στο IPv6 Internet. Σε ένα Teredo Client ανατίθεται μια IPv6 διεύθυνση η οποία έχει το εξής prefix 2001:0000::/32 .

Teredo Server : Είναι ένας host που χρησιμοποιείται για την αρχική παραμετροποίηση ενός Teredo Tunnel. Δεν προωθεί κίνηση με προορισμό τον client (εκτός των IPv6 pings) , οπότε οι απαιτήσεις του για bandwidth δεν είναι πολύ μεγάλες κάτι που επιτρέπει σε ένα server να υποστηρίζει πολλούς host.

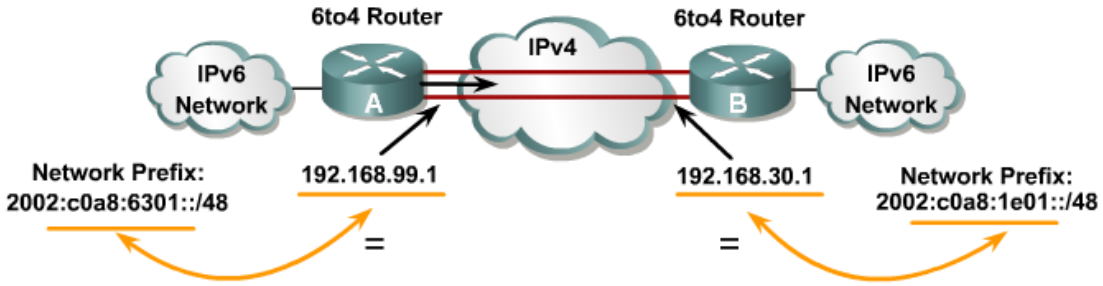
Teredo Relay : Παίζει το ρόλο του απομακρυσμένου άκρου του tunnel. Ένα Teredo Relay πρέπει να προωθεί όλα τα δεδομένα για τον client που εξυπηρετεί. Οπότε έχει μεγάλες απαιτήσεις σε bandwidth και μπορεί να εξυπηρετήσει ταυτόχρονα περιορισμένο αριθμό clients.
Κάθε Teredo Relay εξυπηρετεί ένα συγκεκριμένο εύρος από IPv6 hosts και προωθεί την κίνηση μεταξύ των Teredo ή απλών IPv6 clients που ανήκουν σε αυτό το εύρος.

Teredo Host-Specific Relay : Είναι ένα Teredo Relay ο οποίος εξυπηρετεί μόνο τον host στον οποίο τρέχει. Έτσι δεν υπάρχει καμία ιδιαίτερη απαίτηση για bandwidth. Ένας host με Teredo Host-Specific Relay θα χρησιμοποιήσει το Teredo για την επικοινωνία του με άλλους Teredo Clients αλλά για την επικοινωνία του με το υπόλοιπο IPv6 Internet θα στηριχτεί στον πάροχο του.

3.4.6 Ο Μηχανισμός 6to4

Το 6to4 είναι ένας μηχανισμός αυτόματου tunneling που παρέχει την δυνατότητα σε απομονωμένα IPv6 Sites, στα οποία δεν υπάρχει ευρύτερη IPv6 συνδεσιμότητα και υπηρεσίες από κάποιον πάροχο ISP να απικοινωνούν μεταξύ τους πάνω από το ήδη υπάρχον IPv4 δίκτυο. Επιπλέον δίνεται η δυνατότητα να επικοινωνούν με sites τα οποία ανήκουν στο native IPv6 δίκτυο. Ο μηχανισμός αυτός σχεδιάστηκε για το μεταβατικό στάδιο από τις IPv4 στις IPv6 διευθύνσεις, κατά την περίοδο δηλαδή που οι δύο διευθύνσεις θα συνυπάρχουν. Σκοπός του μηχανισμού είναι οι απομονωμένες IPv6 νησίδες που έχουν πρόσβαση στο IPv4 wide area network, το οποίο δεν υποστηρίζει IPv6 να επικοινωνούν μεταξύ τους με εύκολο και αυτόματο τρόπο.

Με τον 6to4 μηχανισμό κάθε site το οποίο έχει μια παγκόσμια μοναδική unicast διεύθυνση μπορεί χρησιμοποιώντας ενθυλάκωση με automatic tunneling να μεταδώσει πακέτα πάνω από το παγκόσμιο IPv4 internet χρησιμοποιώντας ένα μοναδικό prefix (2000::/16). Εκτός του 6to4 router , οι υπόλοιποι τοπικοί host και router δεν χρειάζεται να υλοποιούν τον 6to4 μηχανισμό και οι διάφορες λειτουργίες του εσωτερικού δικτύου γίνονται όπως ορίζει το IPv6 πρωτόκολλο.



Σχήμα 3.8 Ο μηχανισμος 6to4

Ο μηχανισμός 6to4 επικράτησε των υπόλοιπων μηχανισμών μετάβασης και αντικατέστησε τα configured tunnels τα οποία χρησιμοποιούνταν αρχικά τόσο λόγω της ευκολίας υλοποίησης του αλλά και των ελάχιστων απαιτήσεων που θέτει, οι οποίες είναι :

-Ο border router του site ο οποίος είναι ο μόνος που υλοποιεί τον μηχανισμό πρέπει να είναι dual stack.

-Το site πρέπει να διαθέτει μια public IPv4 address για την επικοινωνία του με το IPv4 internet.

Έτσι απλά υλοποιώντας τον 6to4 μηχανισμό στον border router του 6to4 site προσφέρεται σε όλους τους hosts που ανήκουν στο site IPv6 συνδεσιμότητα χωρίς να χρειάζεται να υλοποιούν οι ίδιοι τον μηχανισμό. Το μόνο που χρειάζεται από την μεριά των host είναι να καθορίσουν στο default route τους ως next hop την διεύθυνση του 6to4 δρομολογητή.

Η διαδικασία που εκτελείται για την δημιουργία του site prefix είναι η εξής : Όπως αναφέρθηκε παραπάνω για να εφαρμοστεί ο μηχανισμός 6to4 το site θα πρέπει να έχει μια τουλάχιστον public IPv4 διεύθυνση. Η IANA (Internet Assigned Numbers Authority) – που επιτηρεί την ανάθεση των IP διευθύνσεων – έχει ορίσει το unicast 6to4 prefix (TLA) 2002::/16 για την αποκλειστική χρήση από τον 6to4 μηχανισμό. Το 6to4 prefix μαζί με την IPv4 διεύθυνση σχηματίζουν το /48 site prefix, 2002:IPv4/48 το οποίο είναι και αυτό μοναδικό για τον λόγο ότι προκύπτει από την μοναδική public

IPv4 διεύθυνση. Για παράδειγμα έστω ότι το site έχει public IP Address την **62.157.9.98 .**

Μετατρέποντας την στην δεκαεξαδική μορφή είναι **3e 9d 9 62 .** Οπότε σύμφωνα με τα παραπάνω το πρόθεμα του 6to4 site θα διαμορφωθεί ως εξής **2002:3e9d:0962::/48 .** Επιπλέον με αυτόν τρόπο γίνονται διαθέσιμα 2^16 υποδίκτυα με prefix /64 το οποίο το καθένα έχει χωρητικότητα μέχρι 2^64 hosts , κάτω από μια μοναδική IPv4 διεύθυνση. Αφότου καθοριστεί το 6to4 πρόθεμα του site (/48), καθορίζονται τα διάφορα υποδίκτυα του site, τα οποία παίρνουν το καθένα διαφορετική τιμή για το SLA ID , έτσι που τελικά σχηματίζεται το μοναδικό

2002:IPv4:SLA ID:://64 πρόθεμα του υποδικτύου (site prefix). Το πρόθεμα αυτό διαφημίζεται από τους 6to4 δρομολογητές με μηνύματα router advertisement όπως ορίζει το πρωτόκολλο Neighbor Discovery έτσι ώστε οι hosts να σχηματίσουν μόνοι τους την public διεύθυνση τους με Stateless Address Autoconfiguration. Συγκεκριμένα οι hosts υπολογίζουν μόνοι τους τα τελευταία 64 bit τα οποία είναι ο μοναδικός για κάθε host interface identifier (η διαδικασία υπολογισμού του interface identifier περιγράφτηκε προηγουμένως) και σε συνδυασμό με τα 64 bit του site prefix που περιέχονται στα μηνύματα Router Advertisements των δρομολογητών σχηματίζεται η public IPv6 (6to4) διεύθυνση τους.

Η διεύθυνση αυτή χρησιμοποιείται για την εγγραφή τους σε DNS records , κάτι το οποίο τους καθιστά αναγνωρίσιμους και από άλλους IPv6 κόμβους κάνοντας με αυτόν τον τρόπο δυνατή την επικοινωνία τόσο με άλλους 6to4 κόμβους ή και με native IPv6 κόμβους.

Bits : 0-16	Bits : 17-48	Bits : 49-64	Bits : 65-128
2002	IPv4 Address	SLA ID	Interface ID

Πίνακας 2 Σχηματισμός της διεύθυνσης 6to4

Έχουν θεσπιστεί κάποιοι κανόνες ώστε να διασφαλιστεί η εύρυθμη λειτουργία τους 6to4 μηχανισμού. Σύμφωνα με αυτούς κατά την διάρκεια μιας επικοινωνίας πρέπει να

υλοποιηθεί κατάλληλα η σωστή επιλογή διεύθυνσης πηγής (source address) και προορισμού (destination address).
-Εάν ένας host έχει μόνο 6to4 διεύθυνση και ο άλλος έχει 6to4 και native IPv6 διεύθυνση τότε και οι δύο θα χρησιμοποιήσουν την 6to4 διεύθυνση τους.
-Εάν και οι δύο έχουν 6to4 διεύθυνση και native IPv6 διεύθυνση , τότε σε αυτή την περίπτωση χρησιμοποιείται η native IPv6 διεύθυνση.

Η διαδικασία ενθυλάκωσης-απενθυλάκωσης 6to4 πακέτων (Encaspulation/Decapuslation process)

Τα IPv6 πακέτα ενθυλακώνονται όταν φτάσουν στον 6to4 δρομολογητή ώστε να μεταδοθούν πάνω από την ήδη υπάρχον IPv4 υποδομή δικτύου (IPv4 Backbone). Όσα IPv6 πακέτα φτάσουν στον 6to4 δρομολογητή τα οποία έχουν σαν διεύθυνση προορισμού κάποιον host ο οποίος δεν ανήκει στο site προωθούνται στο tunnel interface του δρομολογητή και μέσω αυτού γίνεται η μετάδοση τους. Τα IPv6 πακέτα ενθυλακώνονται μέσα σε IPv4 πακέτα τα οποία στην επικεφαλίδα τους στο πεδίο protocol θέτουν την τιμή 41 ώστε να γίνεται αντιληπτό από τους ενδιάμεσους κόμβους ότι έχει γίνει ενθυλάκωση. Επίσης στην IPv4 επικεφαλίδα περιέχεται η διεύθυνση η IPv4 διεύθυνση πηγής και η αντίστοιχη διεύθυνση προορισμού. Εάν πρόκειται για καθαρή 6to4 επικοινωνία τότε οι δύο διευθύνσεις είναι οι public IPv4 διευθύνσεις του κάθε site. Εάν πρόκειται για 6to4 με native IPv6 επικοινωνία η διεύθυνση προορισμού στην IPv4 επικεφαλίδα του Relay Router που έχει καθοριστεί από διαχειριστή στον πίνακα δρομολόγησης του 6to4 router (Relay Router έιναι ένας δρομολογητής ο οποίος προωθήσει πακέτα τα οποία δεν έχουν ως προορισμό κάποιον 6to4 host).

Για την ακρίβεια μόλις τα πακέτα προωθηθούν στο tunnel interface γράφεται στο πεδίο source address της IPv4 επικεφαλίδας , η IPv4 διεύθυνση του δικτύου. Στην συνέχεια εάν τα πρώτα 16 bits της διεύθυνσης προορισμού αντιστοιχούν σε 2002::/16 (δηλαδή ο προορισμός είναι ένας 6to4 host) και το prefix /48 διαφέρει του τοπικού (δηλαδή ο προορισμός είναι εκτός του site) , τίθεται ως destination address η IPv4 διεύθυνση του site προορισμού.
Εάν η διεύθυνση προορισμού δεν αντιστοιχεί σε 6to4 , τότε τίθεται σαν διεύθυνση προορισμού στην IPv4 επικεφαλίδα , η διεύθυνση του relay router που έχει

καθοριστεί. Κατόπιν αφότου γίνει η ενθυλάκωση , προωθούνται μέσω tunnel τα IPv4 πακέτα (τα οποία περιέχουν IPv6 επικεφαλίδα και δεδομένα) , με IPv4 δρομολόγηση πάνω από το IPv4 δίκτυο.

Από την άλλη μεριά του tunnel ο 6to4 δρομολογητής του site , αν δει τιμή 41 στο πεδίο protocol της επικεφαλίδας προωθεί τα πακέτα στο δικό του 6to4 interface όπου και απενθυλακώνει την επικεφαλίδα του ipv4 πακέτου , βλέπει την 6to4 διεύθυνση προορισμού και προωθεί κατάλληλα το πακέτο με κανονική IPv6 δρομολόγηση. Παρόμοια διαδικασία ακολουθεί και ο relay router.

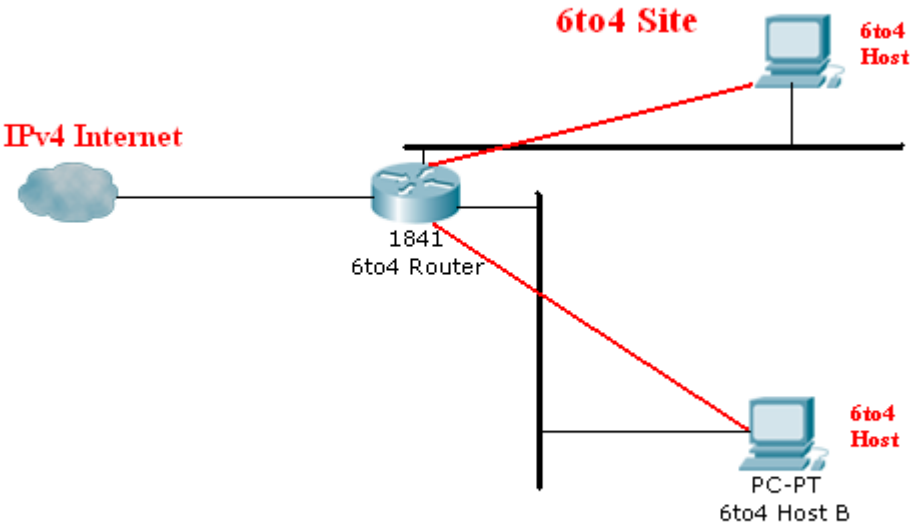
Ο 6to4 μηχανισμός δεν πρέπει να στέλνει πακέτα σε broadcast ή multicast IPv4 διευθύνσεις. Γενικά πρέπει να απορρίπτει τα πακέτα που οι IPv4 και IPv6 διευθύνσεις δεν είναι global unicast.

Επίσης όταν γίνεται χρήση του μηχανισμού 6to4 δεν είναι απαραίτητη η ύπαρξη link local διεύθυνσης για το 6to4 interface. Σε περίπτωση που επιθυμείται ο καθορισμός της , τότε χρησιμοποιείται το πρόθεμα fe80::/64 και τίθεται στα πρώτα 32 bit του Interface ID η IPv4 διεύθυνση και στα υπόλοιπα το 0. Σε αυτήν την περίπτωση μπορεί να χρησιμοποιηθεί το πρωτόκολλο Neighbor Discovery για να εκτελέσει ο host Stateless Address Autoconfiguration.

3.4.7 Σενάρια χρήσης του μηχανισμού 6to4

(i)Επικοινωνία δύο 6to4 host που ανήκουν στο ίδιο site

Στην περίπτωση αυτή χρησιμοποιείται μόνο IPv6 δρομολόγηση μέσα στο ίδιο το site και οι hosts συμπεριφέρονται σαν απλοί IPv6 κόμβοι. Γενικά μέσα στο site χρησιμοποιείται κάποιο πρωτόκολλο δρομολόγησης πχ. RIPng (RIP next generation) ή OSPFv3 και η μόνη διαφορά με τα άλλα native IPv6 sites είναι μια εγγραφή στους πίνακες δρομολόγησης των host του προθέματος 2002::/16 με next hop την διεύθυνση του 6to4 router που έστειλε τα advertisements για να δημιουργήσουν οι host τις 6to4 διευθύνσεις τους. Σε αυτό το σενάριο επικοινωνίας δεν
χρησιμοποιείται το 6to4 interface.

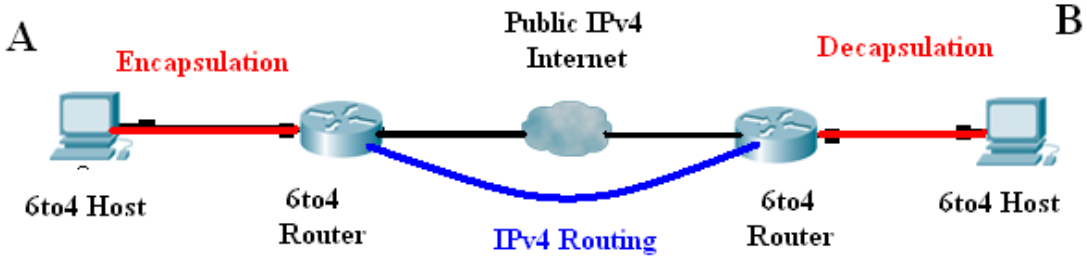


Σχήμα 3.9 6to4 Επικοινωνία μέσα στο ίδιο site

(ii) Επικοινωνία μεταξύ δύο διαφορετικών 6to4 site

Στην περίπτωση αυτή είναι αναγκαίο τα δύο sites που λαμβάνουν μέρος στην επικοινωνία να έχουν μια public routable IPv4 διεύθυνση. Το σενάριο αυτό χρησιμοποιείται για τα sites που χρησιμοποιούν IPv6 αλλά δεν έχουν πρόσβαση σε native ISP Services. Μέσα στο κάθε site όλοι οι hosts υλοποιούν το IPv6 πρωτόκολλο και οι ρυθμίσεις των διευθύνσεων γίνονται μέσω stateless address autoconfiguration. Οι hosts έχουν τις DNS εγγραφές τους έτσι ώστε να είναι δυνατό κάποιος host που ανήκει σε άλλο site να μπορεί να βρει την διεύθυνση τους. Σε αυτή την περίπτωση το tunnel εγκαθίσταται μεταξύ των δρομολογητών των δύο site που πρόκειται να επικοινωνήσουν και τα πακέτα δρομολογούνται απ' ευθείας μεταξύ τους χωρίς να παρεμβαίνει κάποιος άλλος δρομολογητής ενδιάμεσα. Η διαδικασία που εκτελείται ώστε να λάβει μέρος η επικοινωνία είναι η εξής :

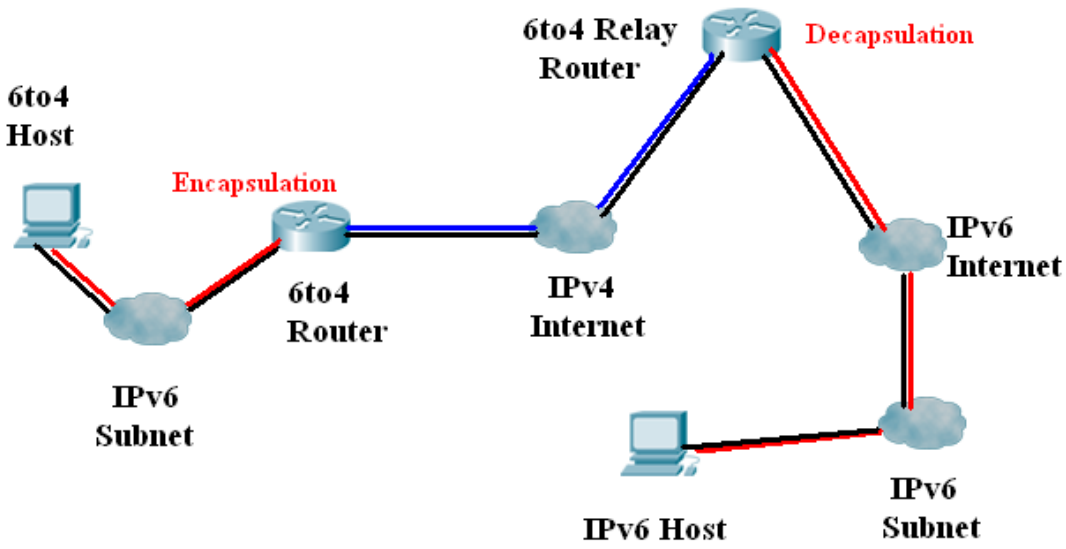
Ο 6to4 host που ανήκει στο ένα site μαθαίνει μέσω αναζήτησης DNS την διεύθυνση του 6to4 host με τον οποίο θέλει να επικοινωνήσει. Μέσα στο site εκτός από τις διευθύνσεις της μορφής 2002:IPv4::/48 διευθύνσεις οι υπόλοιπες χειρίζονται σαν οποιεσδήποτε μη τοπικές διευθύνσεις και στέλνονται μέσω του default route στον 6to4 δρομολογητή. Όταν ο router δει το πρόθεμα 2002::/16 και διεύθυνση προορισμού η οποία δεν ανήκει στο τοπικό site τότε στέλνει τα πακέτα στο 6to4 pseudo-interface όπου γίνεται η ενθυλάκωση σε IPv4 πακέτα. Στο πεδίο protocol της IPv4 επικεφαλίδας τίθεται η τιμή 41 και στην συνέχεια τα πακέτα προωθούνται με IPv4 δρομολόγηση. Η IPv4 διεύθυνση προορισμού προκύπτει από το πρόθεμα 2002:**IPv4**::/48. Όταν τα πακέτα φτάσουν στον 6to4 δρομολογητή του site προορισμού , εκείνος μόλις εντοπίσει την τιμή 41 στο πεδίο protocol της IPv4 επικεφαλίδας εκτελεί απενθυλάκωση (decapsulation) και προωθεί το πακέτο με IPv6 δρομολόγηση μέσα στο site.



Σχήμα 3.10 6to4 Επικοινωνία μεταξύ δύο site

(iii)Επικοινωνία 6to4 site με site συνδεδεμένο στο native IPv6 δίκτυο

Στην περίπτωση αυτή χρειάζεται ένας relay router. Η συσκευή αυτή ουσιαστικά είναι ένας κανονικός IPv6 router ο οποίος έχει και ένα 6to4 pseudo interface στο οποίο εκτελούνται οι διαδικασίες της ενθυλάκωσης και απενθυλάκωσης. Θα γίνει αναφορά ενός σεναρίου στο οποίο δεν χρησιμοποιείται εξωτερικό πρωτόκολλο δρομολόγησης αλλά ο 6to4 router του site ξέρει την διεύθυνση του relay router που θα χρησιμοποιηθεί. Η διεύθυνση αυτή μπορεί να είναι είτε IPv4 unicast address είτε η anycast διεύθυνση 192.88.99.1 όπως ορίζεται στο RFC 3068 “An Anycast Prefix for 6to4 Relay Routers” ώστε να προωθούνται τα πακέτα στον κοντινότερο relay router. Η διαδικασία επικοινωνίας σε ένα τέτοιο σενάριο είναι η εξής:
Αφού βρεθεί μέσω DNS η διεύθυνση του host προορισμού, ο 6to4 host στέλνει μέσω default route τα πακέτα στον 6to4 router. Ο 6to4 router με την σειρά του αφού δει την διεύθυνση προορισμού προωθεί το πακέτο στο 6to4 interface όπου γίνεται η ενθυλάκωση του IPv6 πακέτου κάτω από την IPv4 επικεφαλιδα. Ως διεύθυνση προορισμού τίθεται η διεύθυνση του relay router που υπάρχει σαν next hop στον πίνακα δρομολόγησης για την συγκεκριμένη διαδρομή. Όταν ο relay router παραλάβει τα πακέτα και δει την τιμή 41 στο πεδίο protocol του IPv4 header εκτελεί απενθυλάκωση και προωθεί τα πακέτα στον προορισμό τους με IPv6 δρομολόγηση.



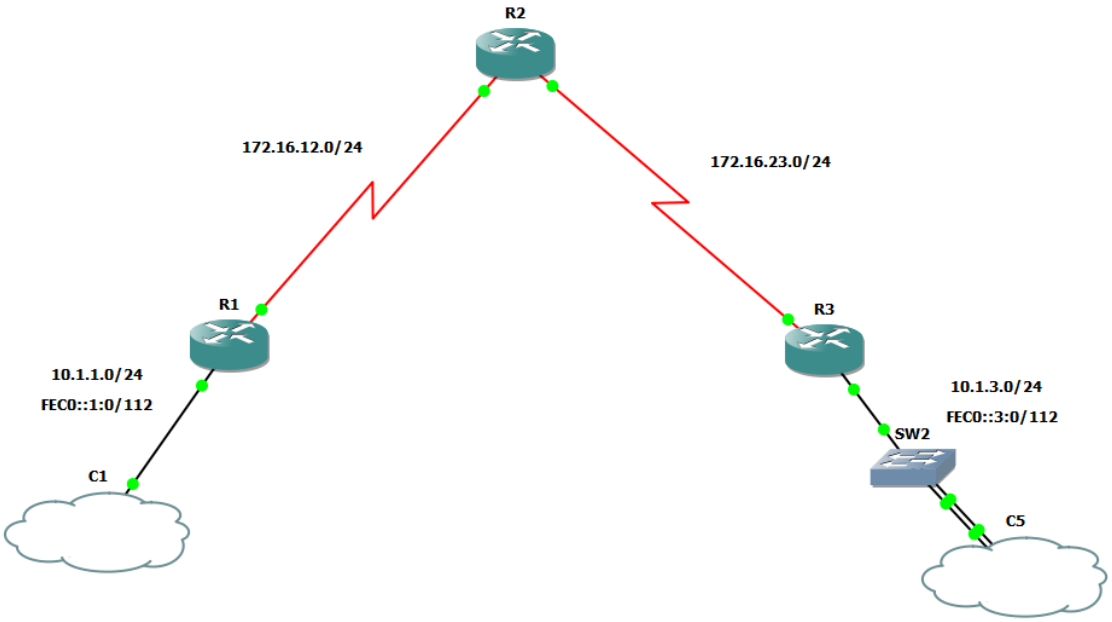
Σχήμα 3.11 Επικοινωνία 6to4 site με Native IPv6 Site

4 Σενάριο Προσομοίωσης

Μετρήσεις

Το σενάριο υλοποίησης είναι το εξής : Σε ένα δίκτυο θα τρέξουμε μια ftp εφαρμογή και θα γίνουν διάφορες μετρήσεις σχετικά με την απόδοση του εκάστοτε πρωτοκόλλου που χρησιμοποιηθήκε σε κάθε μια από τις περιπτώσεις.
Θα μετρήσουμε την απόδοση της εφαρμογής, το πόσο επιβαρύνε το δίκτυο κτλπ.
Στην συνέχεια θα ακολουθήσει εκτενής ανάλυση
Το software που χρησιμοποιήθηκε είναι τα ακόλουθα προγράμματα :
1.Graphical Network Simulator 3 v0.7 (www.**gns3**.net*) , προσομοιωτής δικτύου ο οποίος έχει την δυνατότητα πιστής προσομοίωσης σε περιβάλλον Cisco και Juniper. Στην συγκεκριμένη περίπτωση χρησιμοποιηθήκαν Cisco δρομολογητές της σειράς 3700.*
*2.Vmware Workstation (www.**vmware**.com), πρόγραμμα virtualization . Με την βοήθεια του προγράμματος αυτού δημιουργήθηκαν δύο virtual workstation (με λειτουργικό σύστημα windows xp). Το ένα workstation λειτούργησε ως client και το άλλο ως server.*
*3.Xlight Ftp Server (www.**xlightftp**d.com) , υποστηρίζει τα πρωτόκολλα IPv6 και IPv4 , έχει αρκετές δυνατότητες και είναι πολύ εύκολο στην εγκατάσταση , διαχείρηση και παραμετροποίηση.*
*4.Wireshark (www.**wireshark**.org), network protocol analyzer , πολύ χρήσιμο με αρκετές δυνατότητες , δίνει στον χρήστη την ικανότητα να κάνει ανάλυσει σε επίπεδο πρωτοκόλλου την κίνηση που περνάει πάνω από το δίκτυο βγάζοντας χρήσιμα συμπεράσματα.*
5.Cace Pilot (http://www.cacetech.com/products/cace_pilot.html), είναι πλήρως συμβατό με τα δεδομένα του wireshark (.pcap files) , δίνει στον χρήστη την δυνατότητα περαιτέρω ανάλυσης των trace files που προκύπτουν από το wireshark.

Στο σενάριο αυτό έχει στηθεί ένα 6to4 tunnel μεταξύ των Router 1 και Router 3 οι οποίοι είναι dual stack. Υλοποιούν δηλαδή και τις δύο στοίβες πρωτοκόλλων (IPv4 και IPv6). Πίσω από τον Router 1 υπάρχει ο ftp server και πίσω από τον Router 2 υπάρχουν 2 ftp client.



Σχήμα 4.1 Τοπολόγία Δικτύου Προσομοίωσης

Πίνακες Διευθυνσιοδότησης

Router 1

Interface	IPv4 Address	IPv6 Address
Fast Ethernet 0/0	10.1.1.1/24	Fec0::1:1/112
Serial 0/0	172.16.12.1/255	----------
Tunnel 0 (6to4 Tunnel)	----------	2002:AC10:C01:1::1/64

Router 2

Interface	IPv4 Address	IPv6 Address
Serial 0/0	172.16.12.2/24	----------
Serial 0/1	172.16.23.2/24	----------

Router 3

Interface	IPv4 Address	IPv6 Address
Fast Ethernet 0/0	10.1.3.1/24	Fec0::3:2/112
Serial 0/0	172.16.23.3/24	----------
Tunnel 0	----------	2002:AC10:1703:1::3/64

Host 1 (Server)

Interface	IPv4 Address	IPv6 Address
Fast Ethernet	10.1.1.2/24	Fec0::1:2/112

Host 2 (Client 1)

Interface	IPv4 Address	IPv6 Address
Fast Ethernet	10.1.3.2/24	Fec0::3:2/112

Host 3 (Client 2)

Interface	IPv4 Address	IPv6 Address
Fast Ethernet	10.1.3.3/24	----------

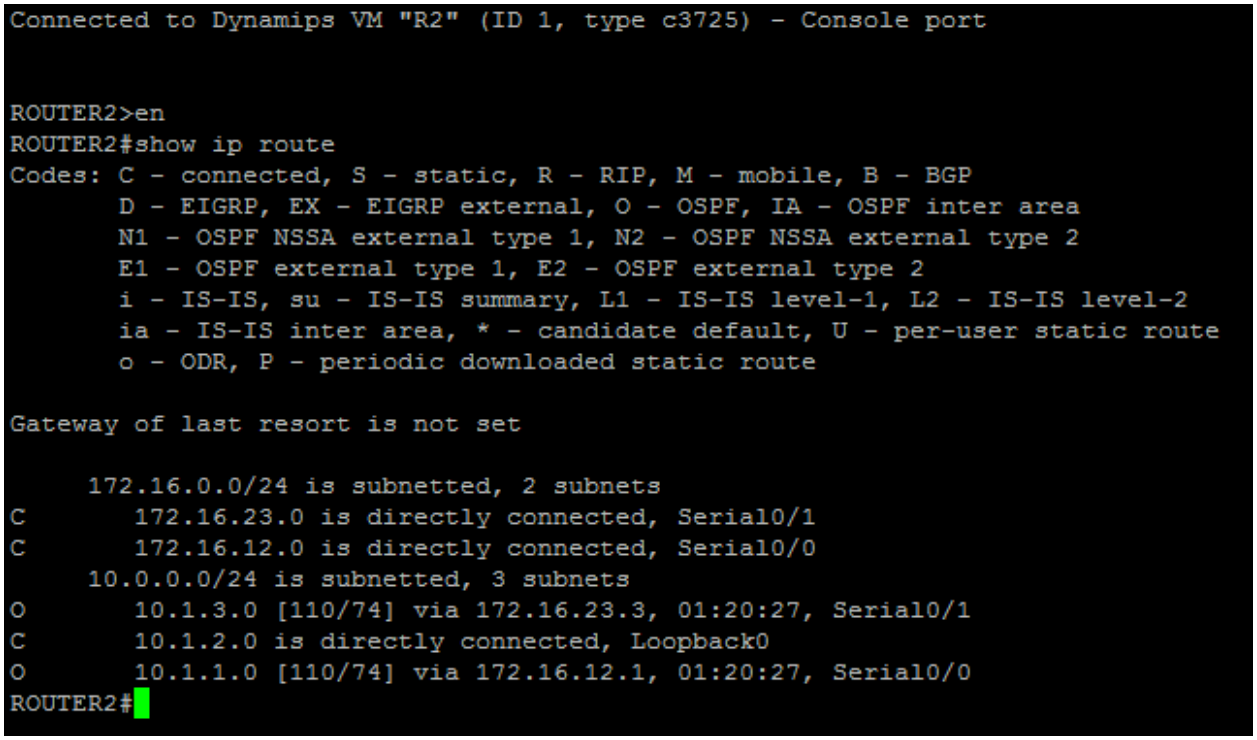
Παρατηρούμε πως τα Tunnel Interfaces των Router 1 και Router 3 έχουν τις διευθύνσεις 2002:AC10:1703:1::1/64 και 2002:AC10:1703:1::3/64 αντίστοιχα. Ας εξετάσουμε τι σημαίνουν οι διευθύνσεις αυτές.
Το 2002 είναι το πρόθεμα μιας 6to4 διεύθυνσης.
AC10:C01 είναι η δεκαεξαδική αναπαράσταση της IPv4 διεύθυνσης 172.16.12.1.
Όπως έχει αναφερθεί νωρίτερα , στο automatic tunneling η IPv6 διεύθυνση σχετίζεται με την IPv6.
Σχετικά με την δρομολόγηση των πακέτων μέσα στο δίκτυο ισχύουν τα εξής:

Για την δρομολόγηση των IPv4 πακέτων , έχουν ρυθμιστεί οι router ώστε να χρησιμοποιούν το πρωτόκολλο OSPF . Ενώ για IPv6 πακέτα έχουν ρυθμιστεί static routes.

Σχήμα 4.2 Router 1 Routing Table

```
Connected to Dynamips VM "R1" (ID 0, type c3725) - Console port


ROUTER1>en
ROUTER1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O       172.16.23.0 [110/128] via 172.16.12.2, 01:13:37, Serial0/0
C       172.16.12.0 is directly connected, Serial0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.1.3.0/24 [110/138] via 172.16.12.2, 01:13:37, Serial0/0
O       10.1.2.1/32 [110/65] via 172.16.12.2, 01:13:37, Serial0/0
C       10.1.1.0/24 is directly connected, FastEthernet0/0
ROUTER1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2002::/16 [1/0]
     via ::, Tunnel0
C   2002:AC10:C01:1::/64 [0/0]
     via ::, Tunnel0
L   2002:AC10:C01:1::1/128 [0/0]
     via ::, Tunnel0
L   FE80::/10 [0/0]
     via ::, Null0
C   FEC0::1:0/112 [0/0]
     via ::, FastEthernet0/0
L   FEC0::1:1/128 [0/0]
     via ::, FastEthernet0/0
S   FEC0::3:0/112 [1/0]
     via 2002:AC10:1703:1::3
L   FF00::/8 [0/0]
     via ::, Null0
ROUTER1#
```

Σχήμα 4.3 Router 2 Routing Table



Σχήμα 4.4 Router 3 Routing Table

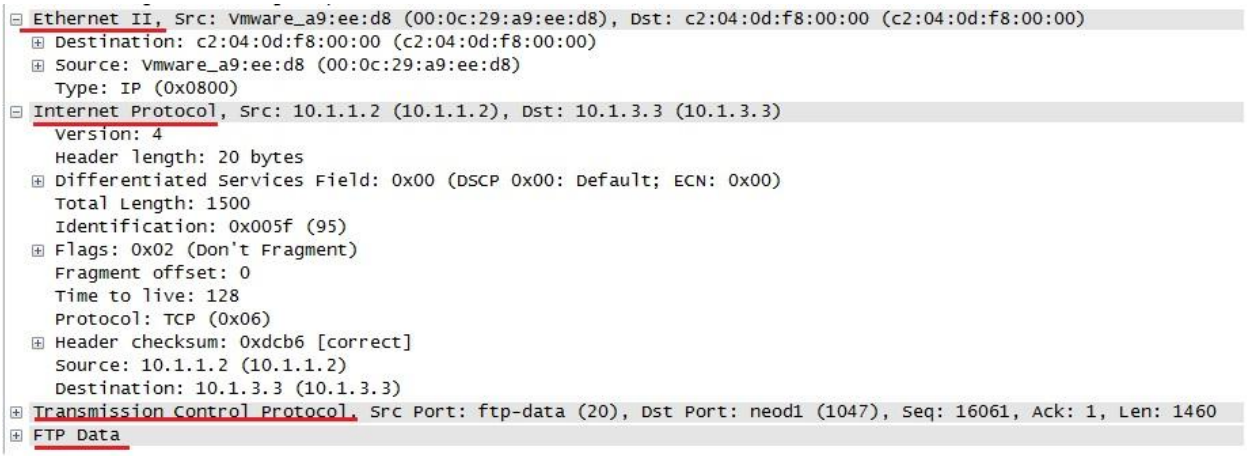
```
ROUTER3>en
ROUTER3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.23.0 is directly connected, Serial0/0
O       172.16.12.0 [110/128] via 172.16.23.2, 01:23:15, Serial0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.3.0/24 is directly connected, FastEthernet0/0
O       10.1.2.1/32 [110/65] via 172.16.23.2, 01:23:15, Serial0/0
O       10.1.1.0/24 [110/138] via 172.16.23.2, 01:23:15, Serial0/0
ROUTER3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2002::/16 [1/0]
     via ::, Tunnel0
C   2002:AC10:1703:1::/64 [0/0]
     via ::, Tunnel0
L   2002:AC10:1703:1::3/128 [0/0]
     via ::, Tunnel0
L   FE80::/10 [0/0]
     via ::, Null0
S   FEC0::1:0/112 [1/0]
     via 2002:AC10:C01:1::1
C   FEC0::3:0/112 [0/0]
     via ::, FastEthernet0/0
L   FEC0::3:1/128 [0/0]
     via ::, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
ROUTER3#
```

Στο κόκκινο πλαίσιο βλέπουμε πως η δρομολόγηση των 6to4 πακέτων γίνεται μέσω του Tunnel Interface των δρομολογητών Router 1 και Router 3.
Τα γράμματα αριστερά των routes έχουν την εξής ερμηνεία
Connected**:** Το δίκτυο αυτό είναι φυσικά συνδεδεμένο πάνω στον router (πχ μέσω καλωδίου).
Static**:** Ο router έχει μάθει την διαδρομή για αυτό το δίκτυο μέσω μιας στατικής εγγραφής (static route) την οποία έχει ορίσει ο διαχειρηστής του router.
OSPF: Ο router έχει μάθει την διαδρομή για αυτό το δίκτυο μέσω του πρωτοκόλλου OSPF.

Στον Server υπάρχει ένα αρχείο 191 Mbytes. Ξεκινάμε την ταυτόχρονη μεταφορά του αρχείου στους 2 client. Με τον Client 1 συνδεόμαστε στον server μέσω IPv6 και με τον Client 2 μέσω IPv4.
Η ιεραρχία των πρωτοκόλλων σε ένα πακέτο είναι η εξής :

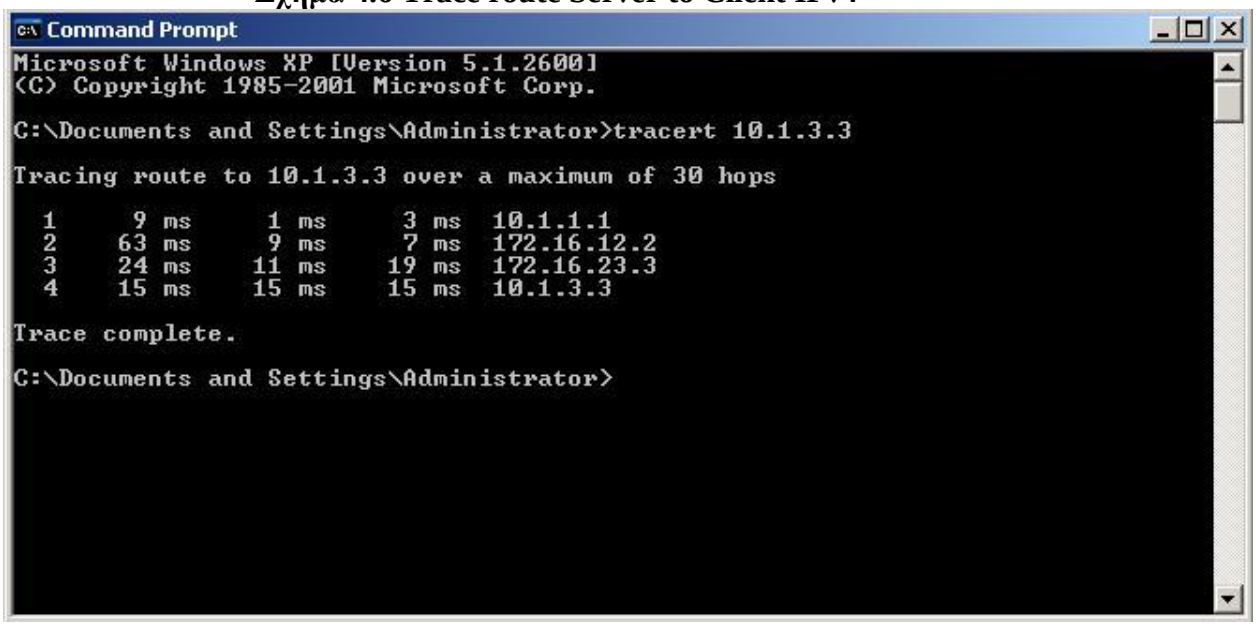
Aplication Layer : FTP (File Transfer Protocol)
Transport Layer : TCP (Transmission Control Protocol)
Network Layer : IPv4 (Internet Protocol version 4) και αν το πακέτο είναι 6to4 τότε μέσα στο IPv4 ενθυλακώνεται ένα IPv6 πακέτο.
Data Link Layer : Ethernet

Σχήμα 4.5 Πακέτο καταγεγραμμένο με το Wireshark



Με κόκκινη υπογράμιση φαίνεται η ιεραρχία των πρωτοκόλλων όπως αναφέρθηκε νωρίτερα. Ας δούμε την συμβαίνει σε αυτή την περίπτωση. Μια εφαρμιογή FTP παράγει δεδομένα (ftp-data). Τα δεδομένα αυτά ενθυλακώνονται σε ένα TCP Segment του οποίου η επικεφαλίδα περιέχει τα πεδία source port και destination port. Παρατηρούμε την τιμή 20 στο πεδίο source port η οποία είναι η default τιμή για το FTP. Στην συνέχεια το TCP Segment ενθυλακώνεται μέσα σε ένα IPv4 packet το οποίο στην επικεφαλίδα του περιέχει εκτός των άλλων τα πεδία source address και destination address. Εδώ βλέπουμε πως το πακέτο αποστέλεται απο τον server (Source Address:10.1.1.2) προς τον client (Destination Address:10.1.3.2). Ακολούθως το IP Packet ενθυλακώνεται μέσα σε ένα Ethernet Frame το οποίο περιέχει τις φυσικές διευθύνσεις – mac addresses. Στην συνέχεια το ethernet frame μετατρέπεται σε bits για την μεταδοσή του πάνω από το φυσικό επίπεδο.

Σχήμα 4.6 Trace route Server to Client IPv4



Ένα πακέτο για να μεταφερθεί από τον Server στον Client ακουλουθεί την διαδρομή που φαίνεται στην εικόνα
Δηλαδή από τον server πάει : Router1→ Router2 → Router3 → Client. Το πακέτο διασχίζει μια διαδρομή τεσσάρων hops. Αυτό συμβαίνει στην περίπτωση χρησιμοποιείται το IPv4 . Σε περίπτωση που χρησιμοποιείται το IPv6 η δρομολόγηση γίνεται μέσω tunnels οπότε το δίκτυο προορισμού φαίνεται σαν directly connected.

ΣΤΑΤΙΣΤΙΚΑ

Σχήμα 4.7 Γενικά Στατιστικά Καταγραφής

Statistic Name	Value
Total Number of Bits	4,022,493,208
Total Number of Bytes	502,811,651
Total Number of Packets	479,738
Number of Broadcast Packets	9
Number of Multicast Packets	136

Καταγράφονται συνολικά κατά την μεταφορά 479.738 πακέτα και 502.811.651 bytes ή 479.5 περίπου megabytes.
Ο χρόνος ολοκλήρωσης της μεταφοράς του αρχείου στην περίπτωση που χρησιμοποιήθηκε το IPv4 ήταν 741 seconds (12,31min) με ρυθμό μετάδοσης 270 kbytes /sec .
Στην περίπτωση χρησιμοποίησης του IPv6 ο χρόνος ολοκλήρωσης της μεταφοράς του αρχείου ήταν 233 seconds (3,8 min) με ρυθμό μετάδοσης 858 kbytes/sec .
Με μια πρώτη ματιά παρατηρούμε ότι στην περίπτωση που χρησιμοποιήθηκε το IPv6 ο χρόνος μεταφοράς ήταν σημαντικά λιγότερος όπως επίσης και το ότι ο ρυθμός μετάδοσης ήταν μεγαλύτερος.

Από τα 479.738 πακέτα , τα 368.360 ήταν IPv4 και τα 111.310 ήταν IPv6 όπως προκύπτει από την ανάλυση των trace files του wireshark με το Cace Pilot.

Σχήμα 4.8 Κατανομή πρωτοκόλλων δικτύου – Πακέτα

Παρατηρούμε πολλά περισσότερα IPv4 πακέτα σε σχέση με τα IPv6.
Από τα 111.310 IPv6 πακέτα ο αριθμός πακέτων που περιέχουν FTP data είναι 89.060 όπως προκύπτει από το Wireshark και έχουμε μόνο 8 αναμεταδόσεις πακέτων με FTP data. Τα πακέτα αυτά φαίνονται στην επόμενη εικόνα.

No.	Time	Source	Destination
36321	60.407002	fec0::1:2	fec0::3:2
56781	70.405944	fec0::1:2	fec0::3:2
57177	71.114259	fec0::1:2	fec0::3:2
65027	84.350422	fec0::1:2	fec0::3:2
72445	106.697235	fec0::1:2	fec0::3:2
73951	108.680627	fec0::1:2	fec0::3:2
76851	114.492141	fec0::1:2	fec0::3:2
82337	122.544960	fec0::1:2	fec0::3:2

Protocol	Info
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1440 bytes

Τα καθαρά δεδομένα σε ένα πακέτο είναι μεγέθους 1440 bytes . Το IPv6 λόγω του μεγέθους της επικεφαλίδας του προσθέτει 40 bytes overhead. 20bytes overhead προσθέτει η TCP επικεφαλίδα οπότε φτάνουμε στην τιμή του MTU (Maximum Transmission Unit) λίγο μεγαλύτερο από 1500 bytes αν συνυπολογίσουμε και το overhead που προσθέτει το πρωτόκολλο Ethernet.

Από τα 368.360 IPv4 πακέτα ο αριθμός πακέτων που περιέχουν FTP data είναι 249.941 όπως προκύπτει από το wireshark εκ των οποίων 87.239 αναμεταδόσεις , κάτι που σημαίνει πως υπάρχουν αρκετά TCP λάθη. Ένα μέρος των αναμεταδόσεων φαίνεται στην επόμενη εικόνα.

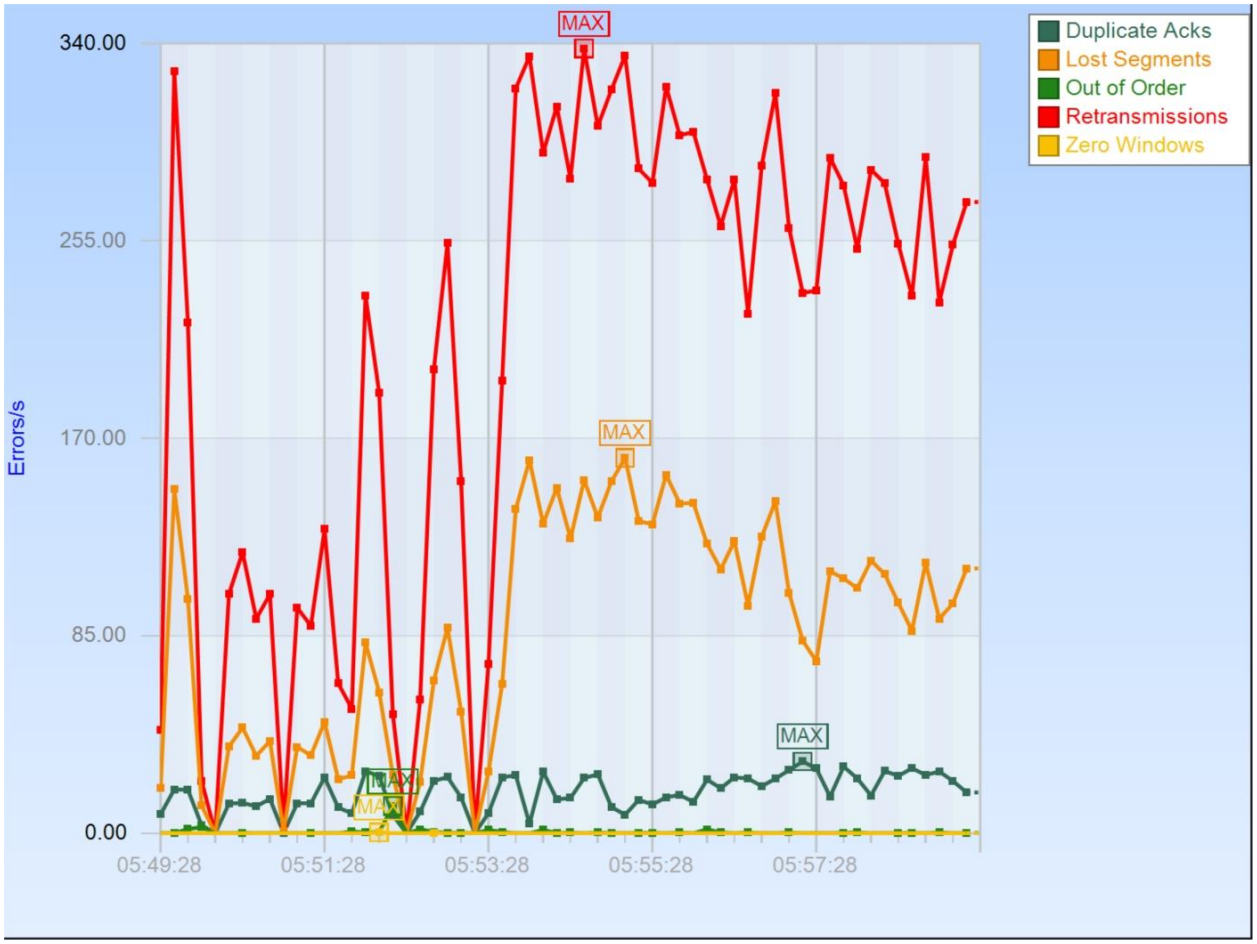
No.	Time	Source	Destination
36278	60.319392	10.1.1.2	10.1.3.3
36279	60.321588	10.1.1.2	10.1.3.3
36285	60.325870	10.1.1.2	10.1.3.3
36294	60.332072	10.1.1.2	10.1.3.3
36295	60.333967	10.1.1.2	10.1.3.3
36296	60.335869	10.1.1.2	10.1.3.3
36297	60.337816	10.1.1.2	10.1.3.3
36298	60.339695	10.1.1.2	10.1.3.3
36299	60.341608	10.1.1.2	10.1.3.3
36300	60.343562	10.1.1.2	10.1.3.3
36301	60.345868	10.1.1.2	10.1.3.3
36302	60.347775	10.1.1.2	10.1.3.3
36349	60.413541	10.1.1.2	10.1.3.3
36350	60.415818	10.1.1.2	10.1.3.3
36352	60.418205	10.1.1.2	10.1.3.3

FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes
FTP-DATA	[TCP Retransmission] FTP Data: 1460 bytes

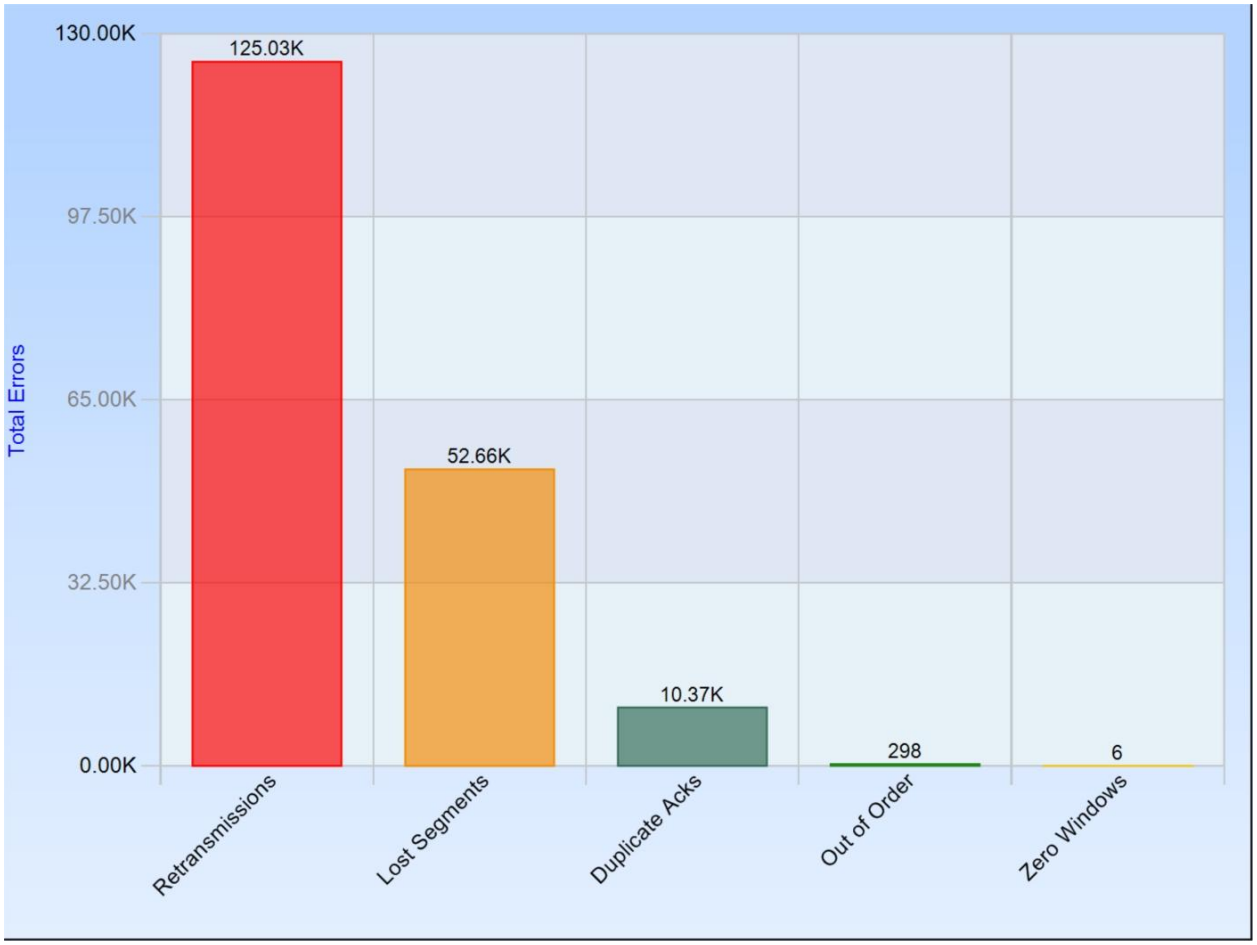
Παρατηρούμε ότι τα καθαρά ftp data σε ένα IPv4 πακέτο είναι μεγέθους 1460bytes , 20 bytes δηλαδή παραπάνω απ' ότι σε ένα IPv6 FTP πακέτο. Αυτό συμβαίνει για τον

εξής λόγο. Η IPv4 επικεφαλίδα είναι μεγέθους 20bytes αντί 40 bytes που είναι του IPv6. Τα υπόλοιπα 20 bytes λοιπόν μπορούν να χρησιμοποιηθούν από τα ftp δεδομένα.

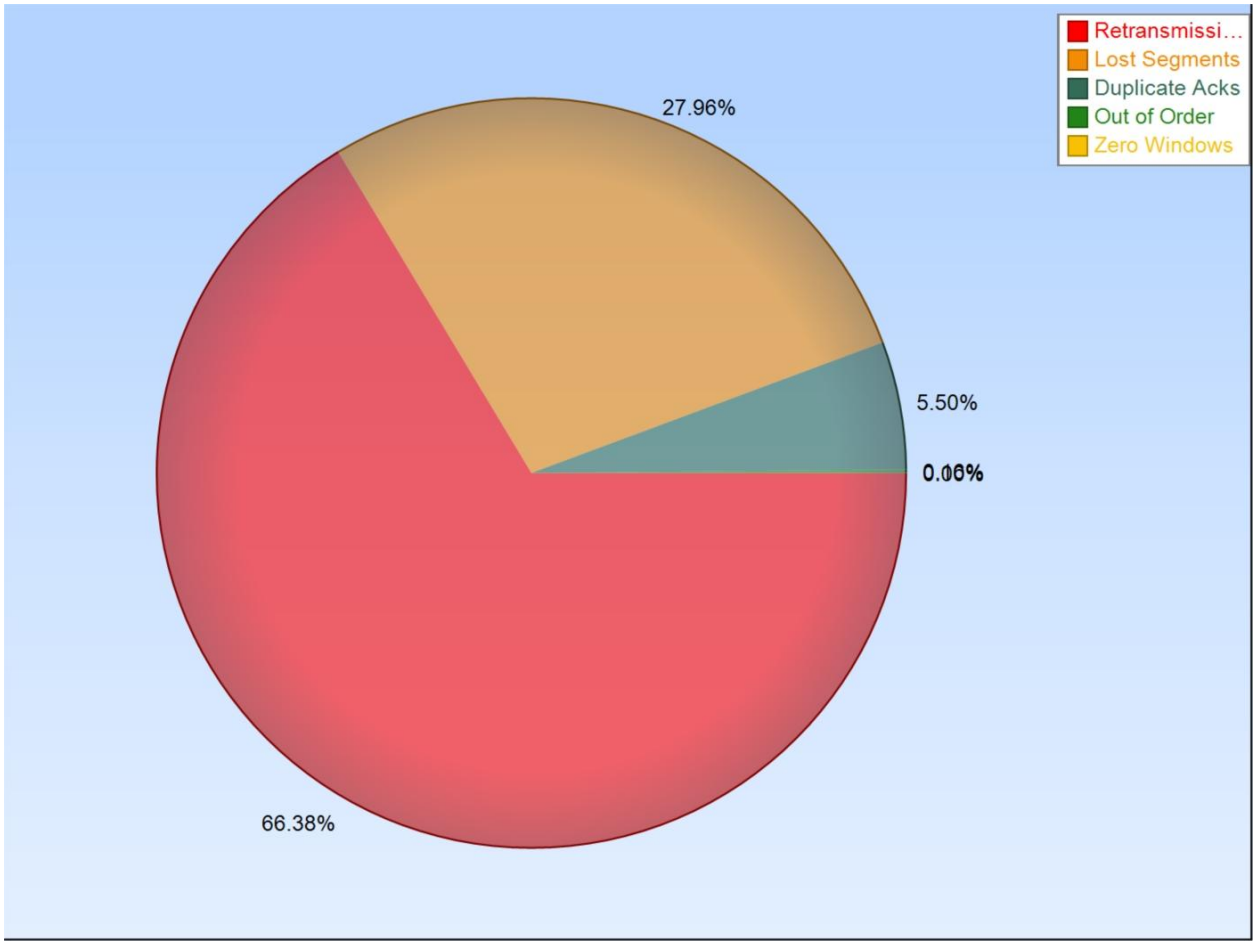
Ας δούμε σε τι οφείλονται οι αναμεταδόσεις αυτές .



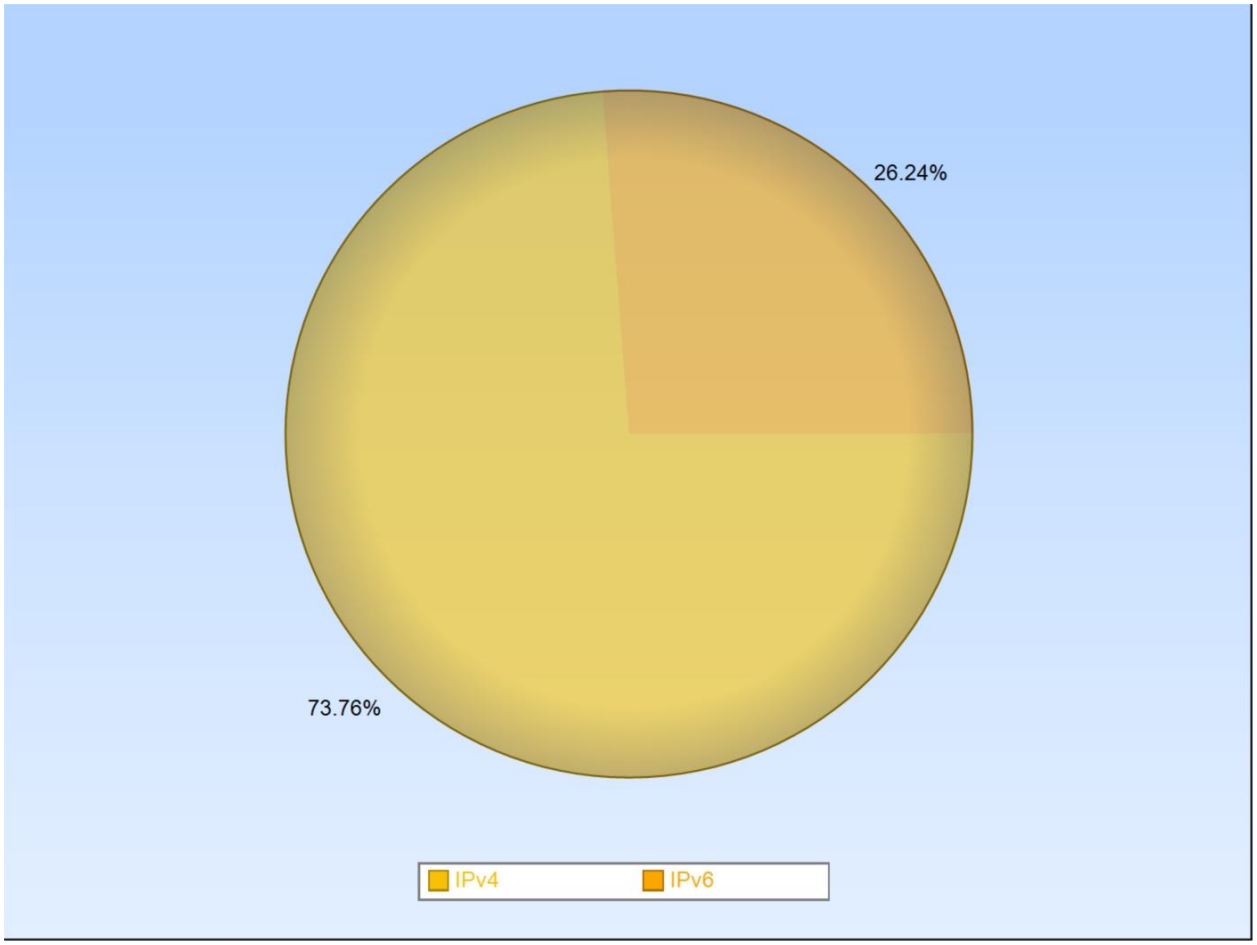
Σχήμα 4.9 Αναμεταδόσεις Πακέτων



Στις παραπάνω και στις επόμενες εικόνες έχουμε μια εικόνα των TCP Errors που προκύπτουν κατά την μεταφορά τουν αρχείου.

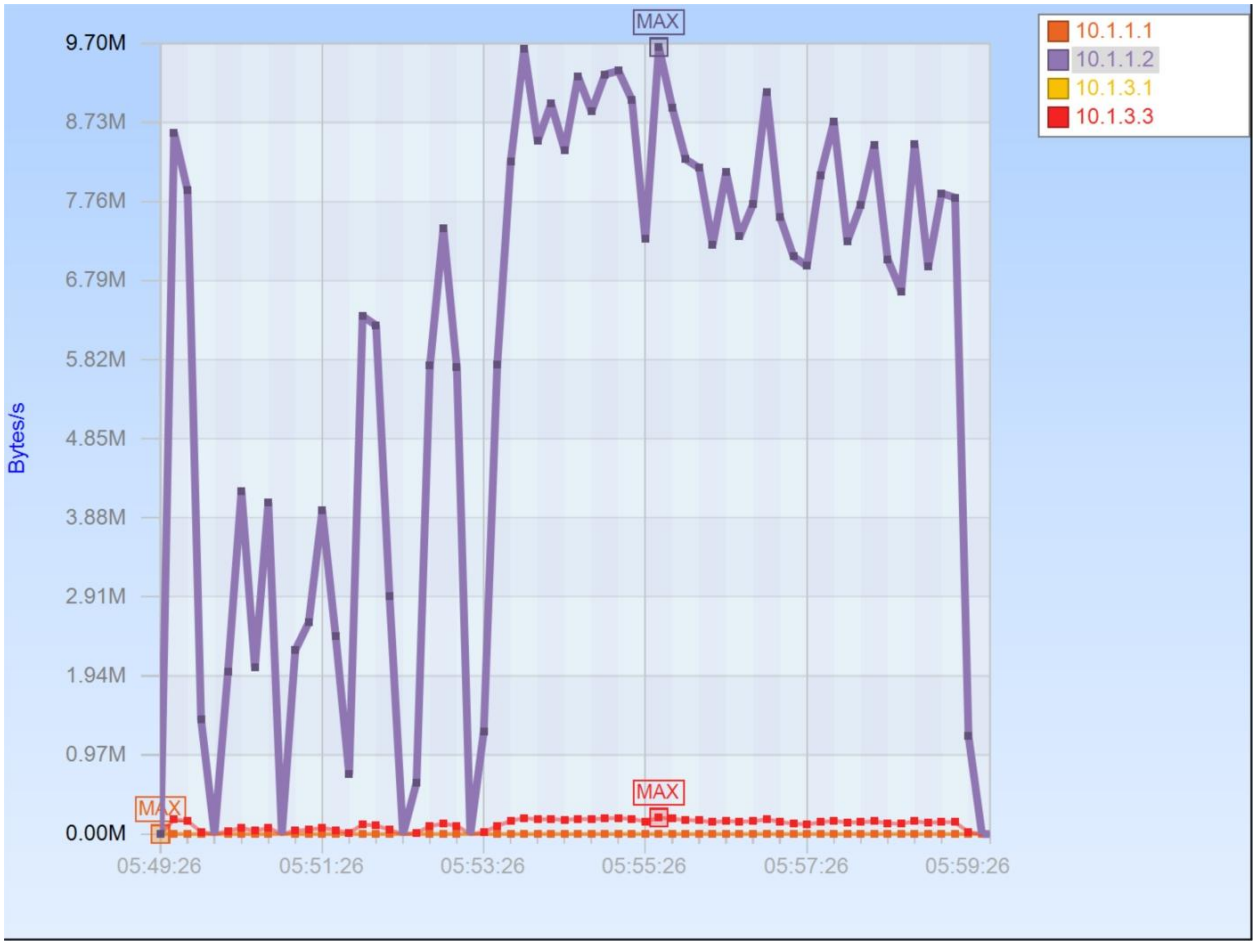


Συνοπτικά μέχρι στιγμής έχουμε τα εξής:
Με το IPv6 είχαμε μικρότερο χρόνο μεταφοράς , μεγαλύτερο ρυθμό μετάδοσης. Επίσης συνολικά επιβάρυνε λιγότερο το δίκτυο. Όπως φαίνεται και στο παρακάτω σχήμα η IPv4 κίνηση κατέλαβε το 73,76% της συνολικής κίνησης , ενώ η IPv6 κίνηση το 26,24 %.



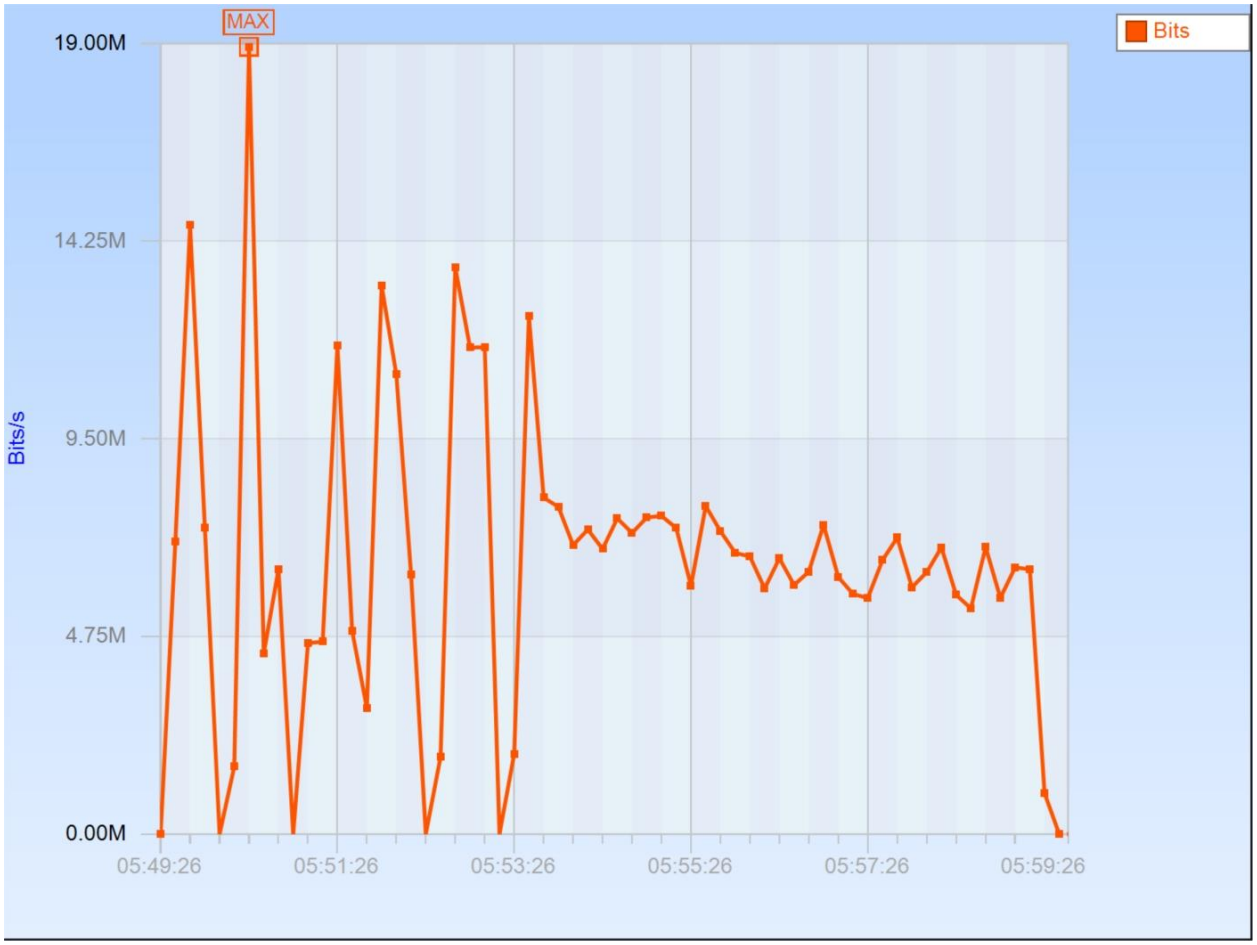
Σχήμα 4.10 IPv4 vs IPv6 Traffic

Όπως είναι φυσικό σχεδόν όλο το μέρος της κίνησης (IPv4 && IPv6) είχε πηγή τον ftp server ο ο οποίος έστελνε ταυτόχρονα δεδομένα στους δύο clients, κάτι που φαίνεται στην παρακάτω εικόνα. Το μικρό ποσοστό κίνησης που οφείλεται στους δύο clients αφορά τα ACKS που έστελναν σε κάθε σωστή παραλαβή πακέτου όπως επίσης και κάποια requests.

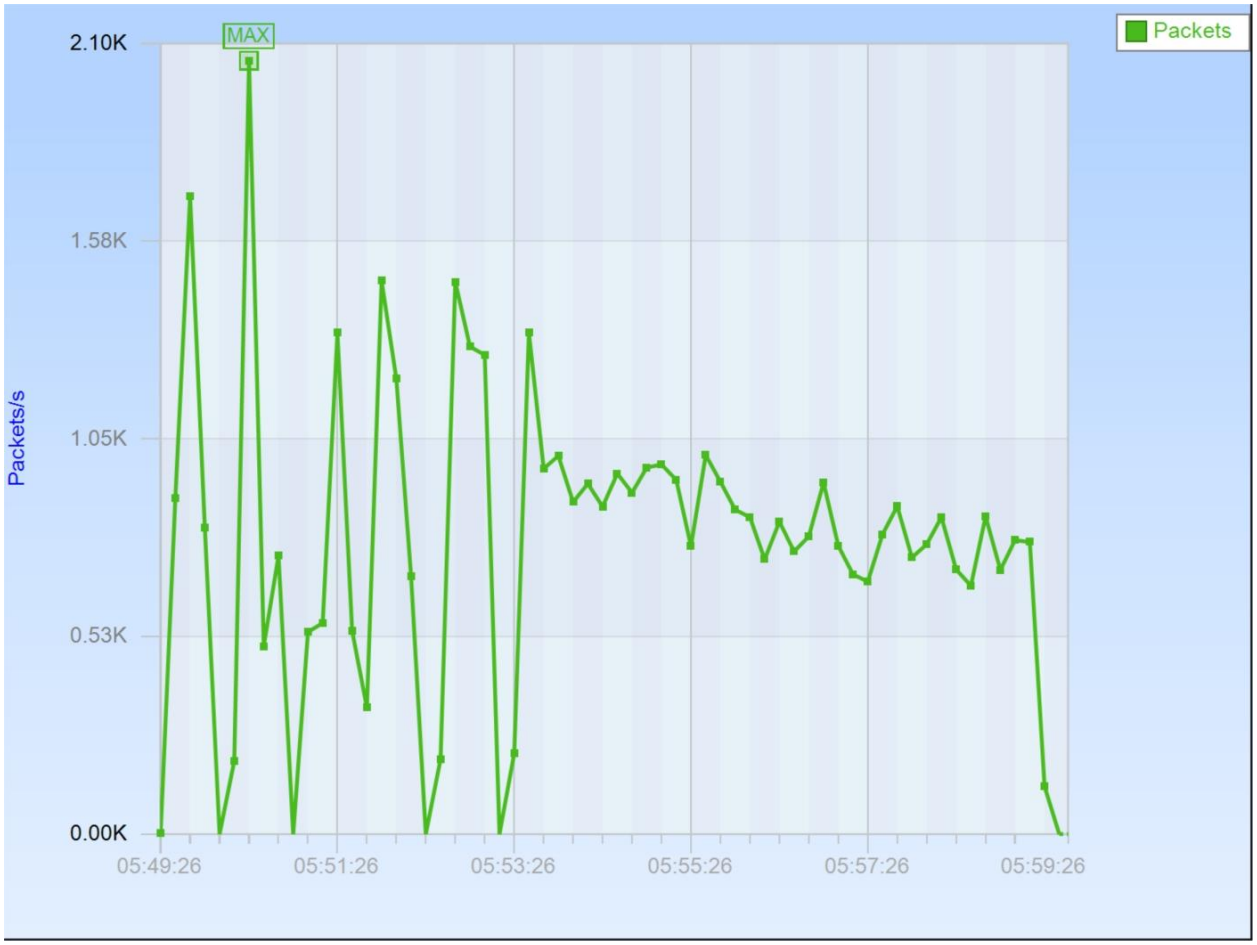


Σχήμα 4.11 Throughput Statistics

Στις παρακάτω εικόνες βλέπουμε στατιστικά που αφορούν το throughput



Σχήμα 4.12 Throughput over time – Bits/second



Σχήμα 4.13 Throughput over time – Packets /second

Στην μέγιστη τιμή του , όπως φαίνεται στην πρώτη εικόνα, το throughput παίρνει την μέγιστη τιμή των 18,9 Megabit. Στην μέγιστη τιμή του δηλαδή έχουμε χρησιμοποίηση της γραμμής (utilization0 19% περίπου.

Τέλος παραθέτω τα configuration files των τριών δρομολογητών

ROUTER 1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
```

```
 no ip address
 no ip redirects
 ipv6 address 2002:AC10:C01:1::1/64
 tunnel source Serial0/0
 tunnel mode ipv6ip 6to4
!
interface Loopback0
 no ip address
 shutdown
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FEC0::1:1/112
!
interface Serial0/0
 ip address 172.16.12.1 255.255.255.0
 clock rate 64000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.255 area 0
!
ip classless
!
!
ip http server
no ip http secure-server
!
ipv6 route 2002::/16 Tunnel0
ipv6 route FEC0::3:0/112 2002:AC10:1703:1::3
!
!
!
!
control-plane
```

```
!
!
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0
 password cisco
 login
line vty 1 4
 login
!
!
end
```

ROUTER 2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

```
!
resource policy
!
memory-size iomem 5
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.16.12.2 255.255.255.0
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 ip address 172.16.23.2 255.255.255.0
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/3
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 network 172.16.12.0 0.0.0.255 area 0
 network 172.16.23.0 0.0.0.255 area 0
!
ip classless
```

```
!
!
ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

ROUTER 3

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
 no ip redirects
```

```
 ipv6 address 2002:AC10:1703:1::3/64
 tunnel source Serial0/0
 tunnel mode ipv6ip 6to4
!
interface Loopback0
 no ip address
 shutdown
!
interface FastEthernet0/0
 ip address 10.1.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FEC0::3:1/112
!
interface Serial0/0
 ip address 172.16.23.3 255.255.255.0
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.3.0 0.0.0.255 area 0
 network 172.16.23.0 0.0.0.255 area 0
!
ip classless
!
!
ip http server
no ip http secure-server
!
ipv6 route 2002::/16 Tunnel0
ipv6 route FEC0::1:0/112 2002:AC10:C01:1::1
!
!
!
!
control-plane
!
!
```

```
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
End
```

Αναφορές – References

[1] “Understanding IPv6” , J.Davies , Microsoft Press ,2008

[2] “Deploying IPv6 Networks” , Patrick Grossetete, Eric Levy-Abegnoli, Ciprian P. Popoviciu, Cisco Press, 2006

[3] IPv6 Essentials (2nd Edition) Silvia Hagen, O'Reilly & Associates, 2006

[4] RFC2460 - Internet Protocol, Version 6 (*IPv6*) Specification , S. Deering , R.Hinden , 1998

[5] RFC3053 – IPv6 Tunnel Broker , A.Durand , P.Fasano , I.Guardini , D.Lento , 2001

[6] RFC3056 – Connection of IPv6 domains via IPv4 Clouds , B.Carpenter, K.Moore , 2001

[7] RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers , R. Gilligan , E. Nordmark , 2001

[8] RFC2080 - RIPng For IPv6 , G. Malkin , R. Minnear , 1997

[9] IPv6: Το Πρωτόκολλο και οι Τεχνικές Μεταβάσεως και Μεταφερσιμότητας Απ. Γκάμας, Π. Γανός, Αν. Καραλιωτας, Χρ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, Ελληνικά Γράμματα, 2005

[10] CCNP Curriculum , Building Scalable Internetworks , Cisco Press

[11] “Global IPv6 Strategies- From Business Analysis to Operational Planning” , by Patrick Grossetete, Ciprian P. Popoviciu, Fred Wettling , Cisco Press , 2008

[12] Cisco IOS IPv6 Configuration Guide , Release 12.4, 2008

[13] Μηχανισμοί Μετάβασης από το IPv4 στο IPv6 , Δημήτριος Φιλιππίδης

[14] www.tcpipguide.com