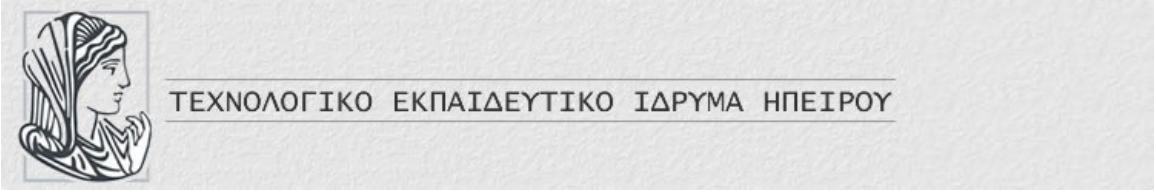


Α.Τ.Ε.Ι. ΑΡΤΑΣ
Τμήμα Τηλεπληροφορικής και Διοίκησης

ΜΕΘΟΔΟΙ ΚΑΙ ΕΡΓΑΛΕΙΑ ΓΙΑ ΤΗΝ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ Ipv6

ΓΕΩΡΓΙΟΣ ΤΣΙΤΣΙΡΟΥΔΗΣ
ΕΞΑΜΗΝΟ :ΠΤΥΧΙΟ
Α.Μ. 3557

ΑΡΤΑ 2006

Περιεχόμενα

Εισαγωγή

Το IPv6 είναι το νέο πρωτόκολλο που προορίζεται να αντικαταστήσει το κυρίαρχο εδώ και δεκαετίες IPv4. Το IPv6 προσφέρει μια σειρά από βελτιώσεις έναντι του IPv4, με κυριότερη αυτή της αύξησης του χώρου διευθύνσεων (128 bits αντί 32), αλλά και με νέα πεδία για παροχή Quality of Service (QoS), έλεγχο ροής, ασφάλεια στο επίπεδο δικτύου, autoconfiguration, ευελιξία και επεκτασιμότητα. Στόχος των βελτιώσεων αυτών είναι να μπορέσει το πρωτόκολλο να ανταποκριθεί στις νέες ανάγκες όπως αυτές διαμορφώνονται σήμερα στο Internet.

Η μετάβαση από το IPv4 στο IPv6 είναι μια μακρά και πολυέξοδη διαδικασία. Στο προσεχές μέλλον και για μεγάλο χρονικό διάστημα προβλέπεται η συνύπαρξη και των δύο πρωτοκόλλων στο Internet. Απαραίτητο στάδιο για την υιοθέτηση του IPv6 είναι η ύπαρξη δικτυακών εφαρμογών που θα βασίζονται σε αυτό, είτε κάνοντας port κάποιες από τις υπάρχουσες για IPv4 εφαρμογές είτε γράφοντας νέες από την αρχή.

1.1 Επισκόπηση των αλλαγών της επικεφαλίδας

Οι αλλαγές από το IPv4 στο IPv6 μπορούν να συνοψισθούν στις παρακάτω κατηγορίες:

• **Εκτεταμένη δυνατότητα διευθυνσιοδότησης:** Το IPv6 αυξάνει το μέγεθος της επικεφαλίδας από 32 σε 128 bits, προσφέροντας δυνατότητες για περισσότερα επίπεδα διευθυνσιοδότησης, “ανεξάντλητο” χώρο διευθύνσεων και απλούστερη αυτοδιαμόρφωση των διευθύνσεων (autoconfiguration). Η διαβαθμισιμότητα της δρομολόγησης multicast έχει βελτιωθεί, προσθέτοντας το πεδίο scope στη διεύθυνση που πληροφορεί το δρομολογητή για την περιοχή των host που “ακούνε” (π.χ. LAN, WAN, Internet).

• **Απλοποιημένη επικεφαλίδα:** Ορισμένα πεδία του IPv4 απουσιάζουν από το IPv6 ή έχουν γίνει προαιρετικά. Αυτό βοηθά στη μείωση του κόστους δρομολόγησης για κάθε πακέτο και του κόστους σε εύρος ζώνης που καταναλώνει η επικεφαλίδα. Η επικεφαλίδα, επίσης, έχει σταθερό μήκος, και οι δρομολογητές έχουν καλύτερη απόδοση για τέτοιες επικεφαλίδες.

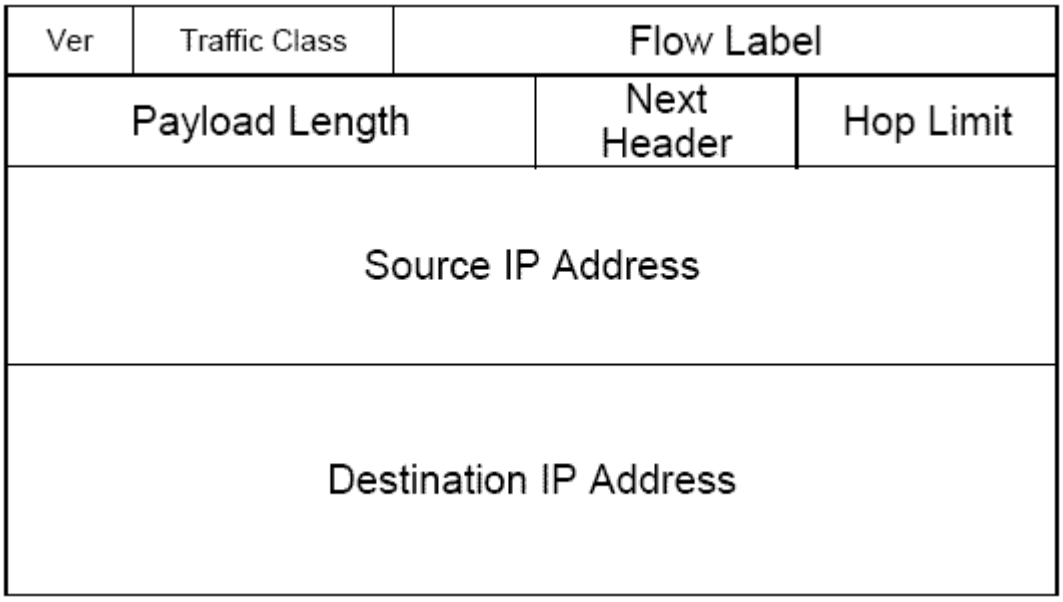
• **Βελτιωμένη υποστήριξη για επεκτάσεις και επιλογές της επικεφαλίδας:** Το IPv6 διαθέτει υποστήριξη προαιρετικών πεδίων σε ξεχωριστές επικεφαλίδες. Αυτό διευκολύνει την απόδοση της απλής δρομολόγησης, αφού δεν χρειάζεται κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία, αν κάτι τέτοιο δεν είναι αναγκαίο.

• **Έλεγχος ροής στο επίπεδο IP:** Μια καινούρια λειτουργία έχει προστεθεί που κατηγοριοποιεί τα πακέτα ενός αποστολέα σε μια συγκεκριμένη ροή (flow). Αυτή η ροή μπορεί να αντιμετωπιστεί με κάποιο ειδικό τρόπο (π.χ. μια ροή δεδομένων live streaming video).

• **Ασφάλεια στο επίπεδο IP:** Το IPv6 προσφέρει, μέσω των επικεφαλίδων επέκτασης, ασφάλεια και απόκρυψη δεδομένων.

1.2 Η βασική επικεφαλίδα του IPv6

Το Σχήμα 1 δείχνει τη δομή της βασικής επικεφαλίδας του IPv6.



Σχήμα 1 Η βασική IPv6 επικεφαλίδα

• **Version (Έκδοση):** Έχει μήκος 4 bits και για το IPv6 πρέπει να είναι ίσο με 6.

• **Traffic Class (Τάξη Κυκλοφορίας):** Έχει μήκος 8 bits και προσδιορίζει ότι μια συγκεκριμένη υπηρεσία παρέχεται σ' αυτό το πακέτο. Η προκαθορισμένη τιμή του είναι με όλα μηδέν.

• **Flow Label (Ετικέτα Ροής):** Έχει μήκος 20 bit και χρησιμοποιείται για να γνωστοποιεί ποια πακέτα ανήκουν σε μια συγκεκριμένη ροή. Ένας κόμβος μπορεί να είναι η αφετηρία για πάνω από μια ροές ταυτόχρονα. Γι αυτό η ετικέτα ροής σε συνδυασμό με τη διεύθυνση της αφετηρίας μπορούν να αναγνωρίσουν μονοσήμαντα μια ροή.

• **Payload Length (Μήκος Πακέτου):** Αυτό το πεδίο καταλαμβάνει 16 bits και περιέχει μια δυαδική τιμή ίση με το μήκος του πακέτου σε bytes. Το μήκος αυτό αφορά το μέρος του πακέτου που ξεκινά αμέσως μετά τη βασική επικεφαλίδα. Δηλαδή οι επικεφαλίδες επέκτασης συνυπολογίζονται σ' αυτό το μέγεθος.

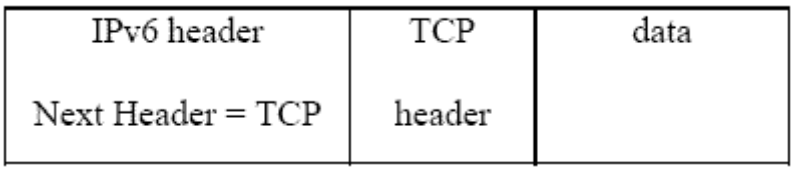
• **Next Header (Επόμενη επικεφαλίδα):** Ένα πεδίο των 8 bit που η τιμή του δείχνει το είδος της επόμενης επικεφαλίδας. Η επόμενη επικεφαλίδα μπορεί να είναι η επικεφαλίδα του επιπέδου μεταφοράς (TCP, UDP) ή μια επικεφαλίδα επέκτασης.

• **Hop Limit (Όριο βημάτων):** Αυτό το 8 bit πεδίο μειώνεται κατά ένα κάθε φορά που το πακέτο προωθείται στον επόμενο κόμβο. Αν το Hop-limit φτάσει το μηδέν το πακέτο απορρίπτεται. Αντίθετα με το IPv4, όπου το πεδίο "time-to-live" παίζει παρόμοιο ρόλο, η πρόθεση στο IPv6 είναι να μην καθορίζεται ο χρόνος ζωής ενός πακέτου στο επίπεδο δικτύου, αλλά σε ανώτερα επίπεδα.

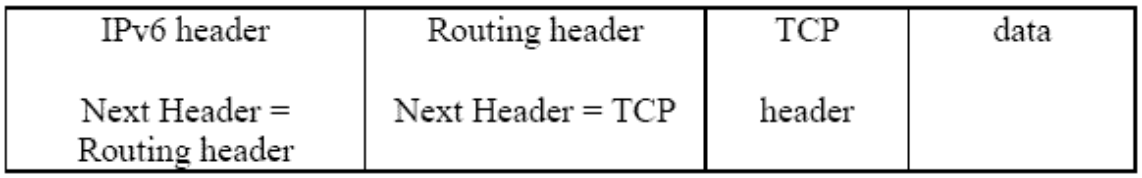
• **Source / Destination Address (Διεύθυνση Αφετηρίας / Προορισμού):** Οι 128 bit διευθύνσεις αφετηρίας και προορισμού του πακέτου. Όσον αφορά τη δεύτερη, αυτή μπορεί να είναι μια unicast, multicast ή anycast διεύθυνση. Αν χρησιμοποιείται επικεφαλίδα δρομολόγησης (που καθορίζει μια συγκεκριμένη διαδρομή που πρέπει να ακολουθήσει το πακέτο), η διεύθυνση προορισμού μπορεί να είναι ένας από τους κόμβους της διαδρομής και όχι απαραίτητα ο τελικός κόμβος.

1.3 Οι επικεφαλίδες επέκτασης του IPv6

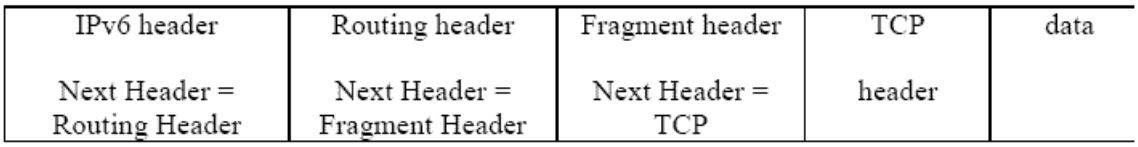
Στο IPv6, προαιρετικές πληροφορίες του επιπέδου δικτύου βρίσκονται σε ξεχωριστές επικεφαλίδες, που τοποθετούνται μεταξύ της βασικής επικεφαλίδας του IPv6 και της επικεφαλίδας του επιπέδου μεταφοράς. Κάθε μία από τις επικεφαλίδες επέκτασης προσδιορίζεται από μια συγκεκριμένη τιμή του πεδίου Next header. Όπως φαίνεται στα παρακάτω παραδείγματα, ένα πακέτο IPv6, μπορεί να μην έχει καμία, να έχει μια ή περισσότερες επικεφαλίδες επέκτασης. Κάθε μια από αυτές προσδιορίζεται από το πεδίο Next Header της προηγούμενης επικεφαλίδας.



Σχήμα 2 Καμιά επικεφαλίδα επέκτασης



Σχήμα 3 Μια επικεφαλίδα επέκτασης



Σχήμα 4 Δυο επικεφαλίδες επέκτασης

Με μια εξαίρεση, οι επικεφαλίδες επέκτασης δεν εξετάζονται ή επεξεργάζονται από τους ενδιάμεσους κόμβους, που βρίσκονται πάνω στη διαδρομή του πακέτου. Αυτό γίνεται μόνο όταν φτάσουν στον κόμβο ή κόμβους (περίπτωση multicast) προορισμού. Εκεί η μετάφραση του πεδίου Next header της βασικής επικεφαλίδας του IPv6, οδηγεί στην επεξεργασία της πρώτης επικεφαλίδας επέκτασης ή της επικεφαλίδας επιπέδου μεταφοράς. Το περιεχόμενο και τα πεδία κάθε επικεφαλίδας επέκτασης καθορίζουν αν πρέπει να προχωρήσουμε στην επόμενη επικεφαλίδα. Γι' αυτό, οι επικεφαλίδες επέκτασης πρέπει να επεξεργάζονται με την ακριβή σειρά με την οποία συναντώνται στο πακέτο. Οπότε, ένας παραλήπτης δεν μπορεί να ψάξει στο πακέτο για να βρει μια συγκεκριμένη επικεφαλίδα πριν επεξεργαστεί τις προηγούμενες.

Η εξαίρεση που αναφέραμε στην προηγούμενη παράγραφο αφορά την επικεφαλίδα επέκτασης Hop-by-Hop (Βήμα-προς-βήμα), η οποία περιέχει πληροφορίες που πρέπει να εξεταστούν από όλους τους κόμβους πάνω στη διαδρομή του πακέτου, συμπεριλαμβανομένων και των κόμβων αφετηρίας και προορισμού. Η επικεφαλίδα Hop-by-Hop όταν υπάρχει πρέπει να ακολουθεί αμέσως μετά από τη βασική επικεφαλίδα. Η παρουσία της δηλώνεται με την τιμή μηδέν στο πεδίο Next header της βασικής επικεφαλίδας του IPv6.

Αν κάποιος κόμβος επεξεργαζόμενος ένα IPv6 πακέτο χρειάζεται να μεταβεί στην επόμενη επικεφαλίδα, αλλά δεν μπορεί να μεταφράσει το πεδίο Next header της προηγούμενης, τότε πρέπει να απορρίψει το πακέτο. Κατόπιν αυτού πρέπει να στείλει ένα ICMP (Internet Control Message Protocol) μήνυμα στην πηγή του πακέτου με κωδικό 2 ("Μη αναγνωρίσιμος τύπος Next Header"), που θα περιέχει την τιμή του πεδίου Next Header που δεν μπόρεσε να αναγνωρίσει. Το ίδιο θα πρέπει να γίνεται αν ένας κόμβος συναντήσει τιμή μηδέν

στο πεδίο Next Header κάποιας άλλης επικεφαλίδας εκτός από την επικεφαλίδα του IPv6.

Η κάθε επικεφαλίδα επέκτασης είναι ακέραιο πολλαπλάσιο των 8 bytes. Τα πεδία τους που έχουν μήκος πάνω από ένα byte ευθυγραμμίζονται στα φυσικά τους όρια, π.χ. ένα πεδίο των n bytes τοποθετείται σε ένα ακέραιο πολλαπλάσιο των n bytes από την αρχή του πακέτου, για n = 1, 2 ,4 ή 8.

Μια πλήρης υλοποίηση του IPv6 περιλαμβάνει τις εξής επικεφαλίδες επέκτασης:

Next Header Value	Description
0	Hop-by-Hop Header
43	Routing Header (RH)
44	Fragmentation Header (FH)
51	Authentication Header (AH)
52	Encapsulated Security Payload (ESP)
59	No Next Header
60	Destination Options Header

Πίνακας 1 Οι επικεφαλίδες επέκτασης του IPv6

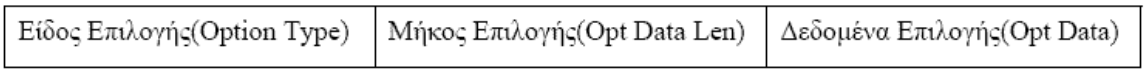
Όταν περισσότερες από μια επικεφαλίδα επέκτασης χρησιμοποιείται στο ίδιο πακέτο, προτείνεται αυτές οι επικεφαλίδες να εμφανίζονται με την εξής σειρά:

• IPv6 header
• Hop-by-Hop Options header
• Destination Options header (επεξεργάζεται από τον τελικό προορισμό, καθώς επίσης και οποιοδήποτε άλλο προορισμό που περιέχεται στην routing header)
• Routing header
• Fragment header
• Authentication header
• Encapsulation Security Payload (ESP) header
• Destination Options header (επεξεργάζεται μόνο από τον τελικό προορισμό όταν γίνεται χρήση routing header)
• Upper-layer header

Όπως φαίνεται παραπάνω η επικεφαλίδα επέκτασης προορισμού(Destination Options header) μπορεί να εμφανίζεται δυο φορές σε ένα πακέτο, όταν χρησιμοποιείται επικεφαλίδα δρομολόγησης(Routing header).

1.4 Επικεφαλίδες Επέκτασης Επιλογών (Options Extension Headers)

Κάθε μια από τις επικεφαλίδες επέκτασης επιλογών περιέχει έναν αριθμό επιλογών μεταβλητού μήκους. Τέτοιες επικεφαλίδες είναι οι επικεφαλίδες Hop-by-Hop και Προορισμού. Οι επιλογές τους ακολουθούν την εξής μορφή:



Σχήμα 5 Μορφή των επιλογών των επικεφαλίδων επέκτασης

• **Option Type:** 8-bit προσδιοριστής του είδους επιλογής.

• **Opt Data Len:** 8-bit unsigned integer, που περιέχει το μήκος της επιλογής σε bytes.

• **Opt Data:** Μεταβλητού μήκους δεδομένα της επιλογής.

Οι επιλογές μέσα στην επικεφαλίδα πρέπει να επεξεργάζονται με την αυστηρή σειρά με την οποία εμφανίζονται. Οπότε, ο παραλήπτης δεν πρέπει να ψάξει στην επικεφαλίδα για την επιλογή που τον ενδιαφέρει και να την επεξεργαστεί, χωρίς να έχει επεξεργαστεί πριν τις προηγούμενες επιλογές.

Ο αριθμός Option Type έχει κωδικοποιηθεί με τέτοιο τρόπο ώστε τα δυο υψηλότερα bits να προσδιορίζουν την ενέργεια που θα πρέπει να ληφθεί αν ο IPv6 κόμβος δεν αναγνωρίζει το είδος της επιλογής:
• 00 – προσπέρασε την επιλογή και συνέχισε την επεξεργασία της επικεφαλίδας
• 01 – απόρριψε το πακέτο
• 10 – απόρριψε το πακέτο και στείλε μήνυμα ICMP, με κωδικό 2, στην αφετηρία, ενημερώνοντάς την για το είδος της επιλογής
• 11 – απόρριψε το πακέτο και μόνο όταν ο προορισμός δεν είναι multicast στείλε ICMP μήνυμα στην πηγή

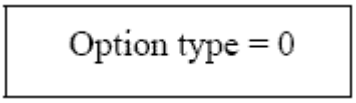
Το τρίτο ψηλότερο bit στο Option Type, προσδιορίζει το αν μπορεί το περιεχόμενο της επιλογής να αλλάξει κατά τη δρομολόγηση. Όταν χρησιμοποιείται επικεφαλίδα Authentication στο πακέτο, για κάθε επιλογή, της οποίας το περιεχόμενο μπορεί να αλλάξει κατά τη δρομολόγηση, το περιεχόμενό της δεν πρέπει να λαμβάνεται υπόψη κατά τον υπολογισμό της τιμής authentication.
• 0 – Η επιλογή δεν αλλάζει κατά τη δρομολόγηση
• 1 – Η επιλογή μπορεί να αλλάξει κατά τη δρομολόγηση

Ορισμένες επιλογές απαιτούν ιδιαίτερη μεταχείριση, ως προς τη θέση τους μέσα στηνεπικεφαλίδα. Οι απαιτήσεις θέσης της κάθε επιλογής προσδιορίζονται χρησιμοποιώντας των τύπο xn+y. Αυτό σημαίνει ότι πεδίο Option Type της επιλογής πρέπει να εμφανίζεται σε ένα ακέραιο πολλαπλάσιο του x συν y bytes ακόμα από την αρχή της επικεφαλίδας.
Για παράδειγμα :

• 2n: σημαίνει ότι η επιλογή ξεκινά σε οποιοδήποτε αριθμό bytes από την αρχή του πακέτου που είναι πολλαπλάσιο του δύο.

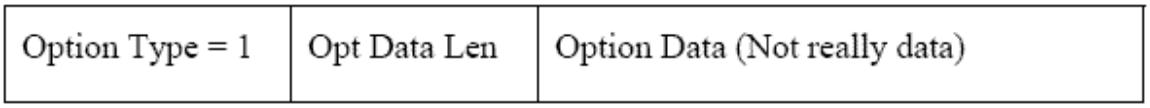
• 8v+2: η επιλογή ξεκινά σε οποιοδήποτε πολλαπλάσιο του οχτώ συν δύο bytes.

Για να ικανοποιείται η συνθήκη xn+y για κάθε επιλογή υπάρχουν οι επιλογές γεμίσματος, που οι ίδιες δεν έχουν απαιτήσεις θέσης. Η μία είναι η επιλογή γεμίσματος Pad1 που έχει κωδικό 0 και δεν έχει άλλα πεδία εκτός του Option type.



Σχήμα 6 Pad1

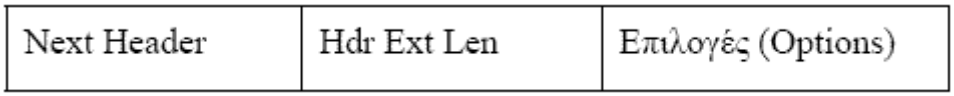
Η άλλη είναι επιλογή γεμίσματος PadN που έχει μήκος δύο byte και πάνω:



Σχήμα 7 PadN

1.5 Η επικεφαλίδα επέκτασης Hop-by-Hop

Η επικεφαλίδα Hop-by-Hop χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες, που πρέπει να εξεταστούν από κάθε κόμβο της διαδρομής. Η επικεφαλίδα αυτού του τύπου έχει κωδικό 0 στο πεδίο Next header της επικεφαλίδας IPv6 και ακολουθεί την παρακάτω μορφή:



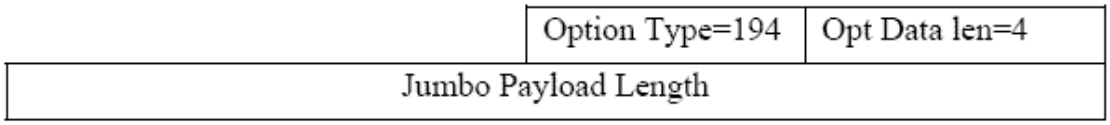
Σχήμα 8 Η επικεφαλίδα Hop-by-Hop

• **Next Header:** Επιλογέας των 8 bit, που προσδιορίζει το είδος της επόμενης επικεφαλίδας.

• **Hdr Ext Len:** Ένας αριθμός των 8 bit που περιέχει το μήκος της επικεφαλίδας σε bytes, χωρίς να συνυπολογίζει το πεδίο Next Header στο μήκος αυτό.

• **Options:** Περιέχει επιλογές μεταβλητού μήκους, της μορφής που προσδιορίσαμε παραπάνω.

Μια από τις επιλογές που έχουν οριστεί για την επικεφαλίδα Hop-by-Hop είναι η επιλογή μεγάλου πακέτου (Jumbo Payload Option), που έχει απαιτήσεις θέσης 4n+2.



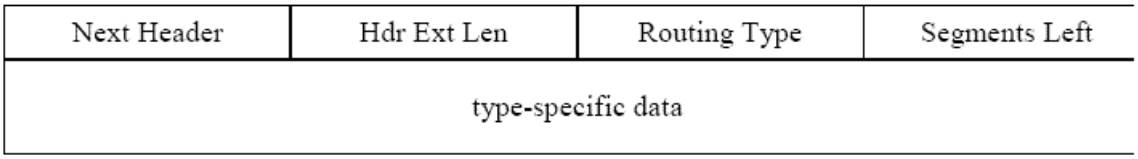
Σχήμα 9 Jumbo Payload Option

Η επιλογή μεγάλου πακέτου χρησιμοποιείται για να στείλει IPv6 πακέτα με μέγεθος μεγαλύτερο των 65,535 bytes. Το πεδίο Jumbo Payload Length είναι το μέγεθος του πακέτου σε bytes εξαιρώντας τη βασική επικεφαλίδα IPv6, και πρέπει να είναι μεγαλύτερο του 65,535. Αν ληφθεί πακέτο με Jumbo Payload μικρότερο ή ίσο του 65,535 στέλνεται ICMP μήνυμα στην αφετηρία με κωδικό 0, ενημερώνοντάς την για το λάθος.

Το πεδίο Payload Length της επικεφαλίδας IPv6 πρέπει να τίθεται ίσο με μηδέν όταν το πακέτο έχει Jumbo Payload. Σε διαφορετική περίπτωση χειριζόμαστε το λάθος στέλνοντας ICMP στην αφετηρία. Παρομοίως όταν ένα πακέτο που έχει επικεφαλίδα Fragment και Jumbo Payload (κάτι που δεν επιτρέπεται), στέλνουμε ICMP στην αφετηρία. Τέλος ένα network interface που δεν υποστηρίζει Jumbo Payload, δε μπορεί να διασυνδεθεί με network interfaces των οποίων το MTU (Maximum Transfer Unit – Μέγιστη μονάδα Μεταφοράς) σύνδεσης είναι μεγαλύτερο του 65,575 (40 bytes IPv6 Header συν 65,535 bytes payload).

1.6 Επικεφαλίδα Δρομολόγησης (Routing Header)

Η επικεφαλίδα δρομολόγησης χρησιμοποιείται όταν η πηγή θέλει το πακέτο να περάσει από έναν ή περισσότερους ενδιάμεσους (συγκεκριμένους) κόμβους στην πορεία του προς τον προορισμό. Η επικεφαλίδα δρομολόγησης έχει κωδικό στο πεδίο Next Header της αμέσως προηγούμενης επικεφαλίδας ίσο με 43. Η γενικότερη μορφή της επικεφαλίδας δρομολόγησης έχει ως εξής:



Σχήμα 10 Η επικεφαλίδα δρομολόγησης

• **Routing Type:** 8-bit πεδίο που προσδιορίζει το είδος της επικεφαλίδας δρομολόγησης.

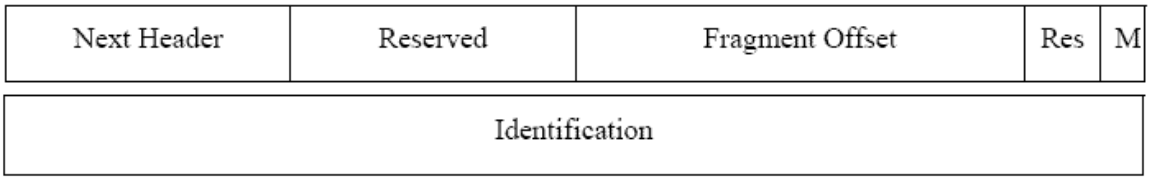
• **Segments Left:** 8-bit πεδίο που περιέχει το πλήθος των ενδιάμεσων κόμβων που το πακέτο πρέπει να επισκεφτεί, ακόμα για να φτάσει στον τελικό προορισμό.

• **type-specific data:** Πεδίο μεταβλητού μήκους, με μορφή που καθορίζεται από την τιμή του πεδίου Routing Type, και μέγεθος τέτοιο ώστε το συνολικό μήκος της επικεφαλίδας να είναι ακέραιο πολλαπλάσιο των 8 bit.

Αν κατά την επεξεργασία της επικεφαλίδας δρομολόγησης, ένας κόμβος συναντήσει Routing Type άγνωστο σ' αυτόν, η αντίδρασή του εξαρτάται από την τιμή του πεδίου Segment Left. Όταν αυτό είναι μηδέν ο κόμβος αγνοεί την επικεφαλίδα δρομολόγησης και προχωρά στην επόμενη επικεφαλίδα. Αν είναι διάφορο του μηδέν τότε ο κόμβος απορρίπτει το πακέτο και στέλνει το αντίστοιχο ICMP μήνυμα στην αφετηρία.

1.7 Επικεφαλίδα Διάσπασης (Fragment Header)

Η Επικεφαλίδα Διάσπασης χρησιμοποιείται από την πηγή για να στείλει πακέτα μεγαλύτερα από το MTU του μονοπατιού (το μέγιστο μήκος πακέτου που υποστηρίζεται από όλους τους συνδέσμους της διαδρομής). Πρέπει να σημειωθεί εδώ πως αντίθετα με το IPv4 η διάσπαση (fragmentation) γίνεται μόνο από την πηγή και όχι από τους δρομολογητές που βρίσκονται πάνω στη διαδρομή. Η Επικεφαλίδα Διάσπασης έχει κωδικό 44 στο πεδίο Next Header της αμέσως προηγούμενης επικεφαλίδας και ακολουθεί την παρακάτω μορφή.



Σχήμα 11 Η επικεφαλίδα διάσπασης

• **Reserved:** αχρησιμοποίητο πεδίο των 8 bit

• **Fragment Offset:** unsigned integer των 13 bits. Περιέχει την απόσταση των δεδομένων που ακολουθούν αυτήν την επικεφαλίδα από την αρχή του αρχικού πακέτου μετρημένη σε λέξεις των 64 bit.

• **Res:** 2-bit αχρησιμοποίητο πεδίο. Αρχικοποιείται σε μηδέν κατά τη μετάδοση και αγνοείται κατά τη λήψη.

• **M flag:** 1 = κι άλλα κομμάτια, 0=τελευταίο κομμάτι.

• **Identification:** Πεδίο μήκους 32 bits. Θα αναφερθούμε σ' αυτό παρακάτω.

Για να μπορέσει να στείλει ένα πακέτο αρκετά μεγάλο για να χωρέσει στο MTU μονοπατιού, η αφετηρία μπορεί να χωρίσει το πακέτο σε κομμάτια και να στείλει το κάθε ένα από αυτά ως ξεχωριστό πακέτο. Το αρχικό πακέτο θα επανενωθεί από τον προορισμό.

Για κάθε πακέτο προς διάσπαση, η πηγή δημιουργεί μια τιμή Identification. Η τιμή αυτή πρέπει να είναι διαφορετική από το Identification κάθε άλλου πρόσφατου πακέτου με την ίδια πηγή και προορισμό (όταν εδώ αναφέρουμε πρόσφατο πακέτο, εννοούμε ότι θα θέλαμε το προηγούμενο πακέτο με το ίδιο Identification να έχει φτάσει στον προορισμό, γιατί δεν θα ήταν καθόλου καλό δυο fragments με το ίδιο Identification να βρίσκονται την ίδια στιγμή καθ' οδόν). Αν το πακέτο διαθέτει επικεφαλίδα δρομολόγησης ο προορισμός που μας ενδιαφέρει είναι ο τελικός προορισμός. Το ίδιο το πεδίο Identification γι' αυτό το σκοπό έχει επιλεγεί να έχει τόσο μεγάλο εύρος τιμών, έτσι ώστε με μια απλή

διαδικασία μέτρησης από το μηδέν μέχρι τη μέγιστη τιμή (2_{32}=4 δισεκατομμύρια περίπου) να διασφαλίζεται η παραπάνω απαίτηση για μοναδικό Identification.

Το αρχικό, πριν τη διάσπαση, πακέτο θεωρούμε ότι αποτελείται από δυο μέρη:

Μη διασπώμενο μέρος	Διασπώμενο μέρος

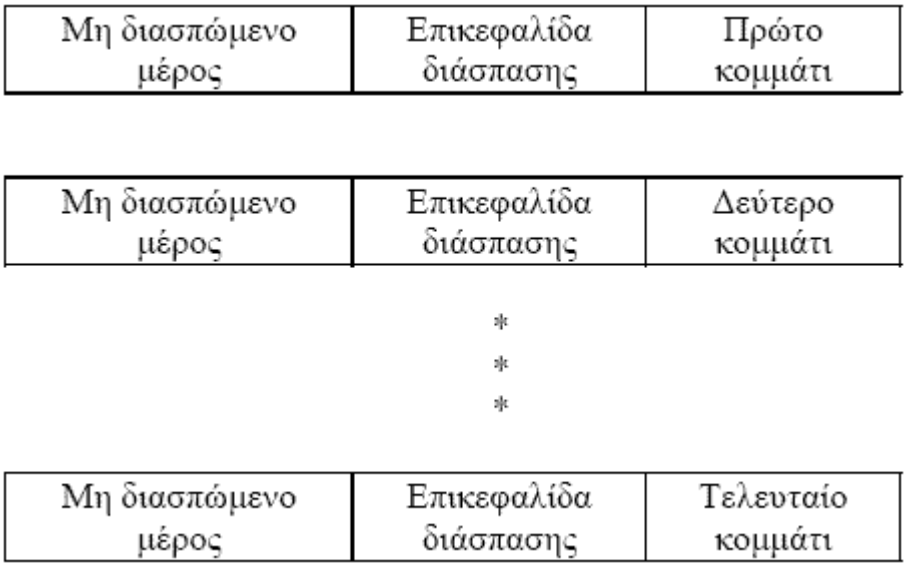
Σχήμα 12 Αρχικό πακέτο

Το μη διασπώμενο μέρος αποτελείται από την επικεφαλίδα του IPv6 συν όποιες επικεφαλίδες επέκτασης χρειάζεται να επεξεργαστούν από τους ενδιάμεσους κόμβους της διαδρομής. Οπότε θα είναι όλες οι επικεφαλίδες μέχρι την Επικεφαλίδα Δρομολόγησης αν το πακέτο διαθέτει μία, ή η Επικεφαλίδα Hop-by-Hop αν το αρχικό πακέτο διαθέτει μία, αλλιώς δεν θα είναι καμία επικεφαλίδα επέκτασης.

Το διασπώμενο μέρος αποτελείται από το υπόλοιπο του πακέτου, δηλαδή τις επικεφαλίδες επέκτασης που δε χρειάζεται να επεξεργαστούν από τους ενδιάμεσους κόμβους, την επικεφαλίδα ανωτέρου επιπέδου και τα δεδομένα. Το διασπώμενο μέρος διαιρείται σε κομμάτια, όπου το καθένα(ίσως εκτός από το τελευταίο) έχει μήκος ίσο με ένα ακέραιο πολλαπλάσιο των 8 bytes. Κατόπιν τα κομμάτια μεταδίδονται με τη μορφή πακέτων κομματιών (fragment packets) όπως φαίνεται παρακάτω:

Μη διασπώμενο μέρος	Πρώτο κομμάτι	Δεύτερο κομμάτι	.....	Τελευταίο κομμάτι

Σχήμα 13 Αρχικό πακέτο σε κομμάτια



Σχήμα 14 Διάσπαση και μεταφορά ενός πακέτου

Κάθε πακέτο κομματιού αποτελείται από:

1. Το μη διασπώμενο μέρος του αρχικού πακέτου με το πεδίο μήκους πακέτου (Payload Length) της επικεφαλίδας IPv6 να περιέχει τώρα το μέγεθος του κομματιού, και το πεδίο Next header της τελευταία επικεφαλίδας του μη διασπώμενου μέρους να έχει αλλαχθεί σε 44.

2. Μια Επικεφαλίδα Διάσπασης (Fragmentation Header) που περιέχει :

• Το πεδίο Next Header που αντιστοιχεί στην πρώτη επικεφαλίδα, που ανήκει στο διασπώμενο μέρος του αρχικού πακέτου. Το Fragment Offset που περιέχει την απόσταση του κομματιού, μετρημένη σε λέξεις των 8 bytes, από την αρχή του διασπώμενου μέρους του αρχικού πακέτου (Το Fragment Offset του πρώτου κομματιού είναι μηδέν).

• Η flag M που έχει τιμή 0 αν το κομμάτι είναι το τελευταίο, αλλιώς έχει τιμή 1

• Το πεδίο Identification που αντιστοιχεί στο αρχικό πακέτο.

3. Το ίδιο το κομμάτι(fragment) του διασπώμενου μέρους του αρχικού πακέτου Τα μήκη των κομματιών, είναι ευνόητο πως έχουν επιλεχθεί, μετά από κάποιο μηχανισμό με τον οποίο η αφετηρία έμαθε το MTU του μονοπατιού. Τέλος, στον προορισμό τα πακέτα επανασυντίθενται με βάση την πληροφορία που βρίσκεται στους Fragment headers.

1.8 Επικεφαλίδα Επιλογών Προορισμού (Destination Options Header)

Η Επικεφαλίδα Επιλογών Προορισμού χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες, που χρειάζεται να εξεταστούν μόνο από τους κόμβους προορισμού. Η επικεφαλίδα αυτή αντιπροσωπεύεται από τον κωδικό 60 στο πεδίο Next Header της αμέσως προηγούμενης επικεφαλίδας και έχει την ακόλουθη μορφή :

Σχήμα 15 Επικεφαλίδα Επιλογών Προορισμού

Η μορφή της επικεφαλίδας επιλογών προορισμού είναι εφάμιλλη αυτής της επικεφαλίδας Hop-by-hop.

1.9 Authentication Header

Αυτή η επικεφαλίδα [12] προσφέρει ένα μηχανισμό υπολογισμού ενός κρυπτογραφικού αθροίσματος ελέγχου πάνω σε κάποια μέρη της επικεφαλίδας IPv6, των επικεφαλίδων επέκτασης και των δεδομένων.

1.10 Encapsulation Security Payload

Αυτή η επικεφαλίδα [13] θα είναι πάντα η τελευταία, μη κρυπτογραφημένη επικεφαλίδα, οποιουδήποτε πακέτου. Δείχνει ότι το υπόλοιπο μέρος του πακέτου είναι κρυπτογραφημένο, και προσφέρει αρκετές πληροφορίες για τον εξουσιοδοτημένο προορισμό να το αποκρυπτογραφήσει.

1.11 Ζητήματα που αφορούν το μέγεθος πακέτου

Το IPv6 προϋποθέτει ότι κάθε σύνδεσμος στο διαδίκτυο έχει ένα MTU μεγαλύτερο από ή ίσο με 576 bytes. Για κάθε σύνδεσμο που δεν υποστηρίζει το παραπάνω μέγεθος πακέτου, θα πρέπει το πρόβλημα να λυθεί τοπικά. Η λύση είναι ο τεμαχισμός και η επανασύνθεση των πακέτων ένα επίπεδο χαμηλότερα από το IPv6.

Για κάθε σύνδεσμο στον οποίο ένας κόμβος είναι απευθείας συνδεδεμένος, ο κόμβος αυτός πρέπει να μπορεί να αποδέχεται πακέτα με μέγεθος όσο είναι το MTU του συνδέσμου. Οι σύνδεσμοι που έχουν καθοριζόμενο MTU (π.χ. PPP σύνδεσμοι) πρέπει να τους έχει καθοριστεί MTU τουλάχιστο ίσο με 576 bytes, αν και προτείνεται ένα μεγαλύτερο MTU. Έτσι θα μπορούμε να χειριστούμε πιθανά encapsulations (π.χ. tunneling) χωρίς να χρειαστεί να κάνουμε τεμαχισμό.

Προτείνεται, ιδιαίτερα, οι κόμβοι του IPv6 να υποστηρίζουν εύρεση MTU μονοπατιού, ώστε να κάνουν πλήρη αξιοποίηση μονοπατιών με MTU μεγαλύτερο από 576 bytes. Ωστόσο μια απλοποιημένη υλοποίηση του IPv6 θα μπορούσε να υιοθετήσει ως path MTU τα 576 bytes, και να μην χρειάζεται να υλοποιεί εύρεση MTU μονοπατιού.

Για να μπορέσει να στείλει ένα πακέτο μεγαλύτερο από το path MTU, ένας κόμβος αφετηρίας μπορεί να χρησιμοποιήσει την επικεφαλίδα τεμαχισμού, για να διασπάσει το πακέτο σε κομμάτια και να το στείλει στον προορισμό, όπου θα γίνει η επανασύνθεση. Ωστόσο, η χρήση τεμαχισμού σ' αυτήν την περίπτωση αποθαρρύνεται, αν το επίπεδο εφαρμογής μπορεί να καθορίσει το μήκος των πακέτων του ώστε να ικανοποιούν το path MTU.

Κάθε κόμβος πρέπει να έχει τη δυνατότητα να επανασυνθέτει τεμαχισμένα πακέτα, που μετά την επανασύνθεση έχουν μέγεθος μέχρι 1500 bytes, συμπεριλαμβανομένης και της επικεφαλίδας του IPv6. Οπότε ένας κόμβος αφετηρίας δεν πρέπει να στέλνει τεμαχισμένα πακέτα που επανασυντίθενται σε μέγεθος μεγαλύτερο από 1500 bytes, εκτός κι αν γνωρίζει ότι ο προορισμός μπορεί να επανασυνθέσει πακέτα τέτοιου μεγέθους.

Σε απάντηση σε ένα IPv6 πακέτο που στέλνεται σε ένα IPv4 προορισμό (π.χ. ένα πακέτο που υφίσταται μετάφραση από IPv6 σε IPv4), ο IPv6 κόμβος της αφετηρίας μπορεί να λάβει ένα ICMP μήνυμα "πακέτο πολύ μεγάλο" αναφέροντας MTU επόμενου βήματος μικρότερο από 576 bytes. Σ' αυτήν την περίπτωση, ο κόμβος IPv6 δεν χρειάζεται να μειώσει το μέγεθος των επόμενων πακέτων σε λιγότερο από 576, αλλά πρέπει να συμπεριλάβει μια επικεφαλίδα τεμαχισμού στα πακέτα αυτά. Έτσι ο κόμβος μετάφρασης από IPv6 σε IPv4 θα έχει λάβει το πεδίο Identification, το οποίο μπορεί να χρησιμοποιήσει για να φτιάξει τα αντίστοιχα IPv4 fragments.

Τέλος, όσον αφορά το μηχανισμό εύρεσης του MTU path, αυτό στο IPv4 επιτυγχάνεται στέλνοντας ένα πακέτο με συγκεκριμένο μέγεθος και με την επιλογή "Don't Fragment" και περιμένοντας κάποιο ICMP μήνυμα αν το πακέτο δεν καταφέρει να "περάσει". Τότε μειώνουμε το μέγεθος και ξαναστέλνουμε κ.ο.κ. Κάτι αντίστοιχο μπορεί να γίνει και με το IPv6, μόνο που εδώ δεν υπάρχει το πεδίο "Don't Fragment" γιατί τα IPv6 πακέτα εξ ορισμού δεν τεμαχίζονται από τους ενδιάμεσους κόμβους.

1.12 Ετικέτα Ροής (Flow Label)

Το 24-bit πεδίο Flow Label [2] της επικεφαλίδας του IPv6 μπορεί να χρησιμοποιηθεί από ένα κόμβο αφετηρίας για να προσδιορίσει εκείνα τα πακέτα για τα οποία επιθυμεί ειδική διαχείριση από τους δρομολογητές IPv6. Όπως για παράδειγμα ξεχωριστή ποιότητα υπηρεσίας ή υπηρεσία πραγματικού χρόνου. Αυτό το χαρακτηριστικό του IPv6 είναι προς το παρόν πειραματικό και επιδέχεται αλλαγών, καθώς οι απαιτήσεις για υποστήριξη ροής στο διαδίκτυο γίνονται πιο σαφείς. Οι κόμβοι που δεν υποστηρίζουν τις λειτουργίες της Ετικέτας Ροής πρέπει να αρχικοποιούν το πεδίο αυτό σε μηδέν όταν στέλνουν, να μην το αλλάζουν όταν προωθούν και να το αγνοούν όταν λαμβάνουν ένα πακέτο.

Μια Ροή είναι μια ακολουθία από πακέτα, που προέρχονται από μια συγκεκριμένη πηγή και κατευθύνονται προς ένα συγκεκριμένο (unicast ή multicast) προορισμό, για την οποία η πηγή επιθυμεί ιδιαίτερη μεταχείριση από τους ενδιάμεσους κόμβους. Η φύση της ιδιαίτερης μεταχείρισης μπορεί να γνωστοποιηθεί στους δρομολογητές από ένα πρωτόκολλο ελέγχου, όπως είναι ένα πρωτόκολλο δέσμευσης πόρων, ή από πληροφορία μέσα στα πακέτα της ροής (π.χ. ως μια επιλογή της επικεφαλίδας Hopby-Hop).

Μπορεί να υπάρχουν περισσότερες της μιας ροές από μια πηγή σε ένα προορισμό, όπως επίσης και κίνηση που δεν ανήκει σε κάποια ροή. Μια ροή προσδιορίζεται μονοσήμαντα από τη διεύθυνση προορισμού και τη μη μηδενική ετικέτα ροής. Τα πακέτα που δεν ανήκουν σε κάποιο ροή, έχουν ετικέτα ροής ίση με μηδέν. Γενικότερα, η ιδέα της ροής είναι μια καλή ιδέα. Γιατί παρ' όλη την ανεξαρτησία που έχουν τα πακέτα μέσα σε ένα IPv4 δίκτυο, σπάνια αυτό είναι αληθές στην πραγματικότητα. Πάντα υπάρχουν πακέτα που αντιστοιχούν, π.χ. σε ένα αρχείο που ανακτάται μέσω FTP ή HTTP ή ανήκουν σε ένα live streaming video και ήχου, ή που ανήκουν σε μια interactive δικτυακή εφαρμογή.

2.1 Διευθυνσιοδότηση IPv6

Οι διευθύνσεις στο IPv6 [9], [10] είναι ορίσματα 128-bit για διεργασίες και σύνολα διεργασιών. Υπάρχουν τρεις τύποι διευθύνσεων:

• Unicast: Όρισμα μεμονωμένης διεργασίας. Ένα πακέτο που αποστέλλεται σε διεύθυνση τύπου unicast παραδίδεται στην διεργασία που προσδιορίζεται από την διεύθυνση αυτή.

• Anycast: Όρισμα συνόλου διεργασιών (που ανήκουν συνήθως σε διαφορετικούς κόμβους). Ένα πακέτο που αποστέλλεται σε μια διεύθυνση anycast παραδίδεται στην διεργασία που προσδιορίζεται από την διεύθυνση αυτή (τον πλησιέστερο, σύμφωνα με τον υπολογισμό απόστασης των πρωτοκόλλων δρομολόγησης)

.

• Multicast: Όρισμα συνόλου διεργασιών (που ανήκουν συνήθως σε διαφορετικούς κόμβους). Ένα πακέτο που αποστέλλεται σε μια διεύθυνση multicast παραδίδεται σε όλες τις διεργασίες που προσδιορίζονται από την διεύθυνση αυτή. Δεν υπάρχουν διευθύνσεις broadcast στο IPv6, η λειτουργία τους επιτυγχάνεται μέσω multicast διευθύνσεων. Στο IPv6, όλα μηδενικά και όλα άσοι είναι νομότυπες τιμές για ένα πεδίο, εκτός εάν έχουν ευκρινώς εξαιρεθεί. Ειδικώς, τα προθέματα, είναι δυνατόν να περιέχουν πεδία μηδενικής τιμής ή πεδία που καταλήγουν σε μηδενικά.

2.2 Μοντέλο διευθυνσιοδότησης

Οι διευθύνσεις IPv6 [9], όλων των τύπων, αποδίδονται σε διεργασίες και όχι σε κόμβους. Μια IPv6 unicast διεύθυνση αναφέρεται σε μία μοναδική διεργασία. Εφόσον κάθε διεργασία ανήκει σε ένα μοναδικό κόμβο, κάθε unicast διεύθυνση μιας διεργασίας αυτού του κόμβου μπορεί να χρησιμοποιηθεί σαν όρισμα του. Όλες οι διεργασίες απαιτείται να έχουν τουλάχιστον ένα link – τοπική unicast διεύθυνση. Σε μια διεργασία μπορεί επίσης να αποδοθούν πολλαπλές IPv6 διευθύνσεις κάθε τύπου (unicast, anycast, και multicast) και τάξης. Σε διεργασίες που δεν χρησιμοποιούνται σαν αφετηρία ή τερματισμός, προς ή από μη γειτονικές δεν απαιτείται διευθυνσιοδότηση τάξης μεγαλύτερης από την τοπική, το οποίο είναι μερικές φορές χρήσιμο για point to point διεργασίες.

Υπάρχει μια εξαίρεση σε αυτό το μοντέλο διευθυνσιοδότησης: Μια διεύθυνση unicast ή ένα σύνολο από διευθύνσεις unicast μπορεί να αποδοθεί σε πολλαπλές φυσικές διεργασίες εάν η υλοποίηση μεταχειρίζεται τις διεργασίες αυτές σαν μια μοναδική διεργασία όπως αυτό εμφανίζεται από την πλευρά του επιπέδου διαδικτύου. Αυτό είναι χρήσιμο για τον καταμερισμό φορτίου επάνω σε πολλαπλές φυσικές διεργασίες. Το IPv6 συνεχίζει το μοντέλο του IPv4 όπου ένα πρόθεμα μάσκας (subnet prefix) συσχετίζεται με ένα link. Πολλαπλά προθέματα μπορούν να συσχετιστούν με το ίδιο link.

2.3 Απεικόνιση των διευθύνσεων σαν κείμενο

Υπάρχουν τρεις συμβατικές φόρμες απεικόνισης διευθύνσεων IPv6 ως συμβολοσειρές κειμένου:

1. Η προτιμώμενη φόρμα είναι X:X:X:X:X:X:X:X, όπου τα X αντιστοιχούν σε δεκαεξαδικές τιμές των 8 16-bit κομματιών της διεύθυνσης.

Παραδείγματα:
o FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
o 1080:0:0:0:8:800:200C:417A
Να σημειωθεί ότι δεν είναι απαραίτητο να γραφούν τα αρχικά μηδενικά σε κάθε

πεδίο (εκτός της περίπτωσης που περιγράφεται παρακάτω).

2. Λόγω ορισμένων μεθόδων απεικόνισης διευθύνσεων IPv6, είναι σύνηθες οι διευθύνσεις αυτές να περιέχουν μεγάλες συμβολοσειρές μηδενικών bits. Για τις περιπτώσεις αυτές είναι διαθέσιμη μια ειδική σύνταξη για την συμπίεση των μηδενικών. Η χρήση του «::» προσδιορίζει πολλαπλές ομάδες μηδενικών 16-bits πεδίων. Το «::» μπορεί να εμφανιστεί μόνο μια φορά σε μια διεύθυνση. Μπορεί επίσης να χρησιμοποιηθεί για την συμπίεση των αρχικών και / ή των τελικών μηδενικών μιας διεύθυνσης. Ο Πίνακας 2 δείχνει κάποια χαρακτηριστικά παραδείγματα.

Τύπος	Κανονική μορφή	Μπορεί να αποδοθεί ως
μια διεύθυνση unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
μια διεύθυνση multicast	FF01:0:0:0:0:0:0:101	FF01::101
η διεύθυνση loopback	0:0:0:0:0:0:0:1	::1
η απροσδιόριστη διεύθυνση	0:0:0:0:0:0:0:0	::

Πίνακας 2 Συμπίεση μηδενικών στις IPv6 διευθύνσεις

3. Μια εναλλακτική φόρμα, που είναι μερικές φορές πιο κατάλληλη σε περιπτώσεις μεικτού περιβάλλοντος IPv6 – IPv4 κόμβων, είναι η X:X:X:X:X:X:D.D.D.D, όπου τα X είναι οι δεκαεξαδικές τιμές των έξι, υψηλής τάξης, πεδίων της διεύθυνσης και τα D οι δεκαδικές τιμές των τεσσάρων, χαμηλής τάξης 8-bit πεδίων, της διεύθυνσης (IPv4 απόδοση).

Παραδείγματα:
0:0:0:0:0:0:13.1.68.3 ή σε συμπυκνωμένη μορφή ::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38 ή σε συμπυκνωμένη μορφή ::FFFF:129.144.52.38

2.4 Απεικόνιση των προθεμάτων διεύθυνσης σε μορφή κειμένου

Μια διεύθυνση IPv6 αναπαρίσταται από την αναφορά:
ipv6-address/prefix-length όπου:
• ipv6-address: μια διεύθυνση IPv6 οποιασδήποτε μορφής

• prefix-length: μια δεκαδική τιμή που προσδιορίζει πόσα από τα αριστερότερα bits της διεύθυνσης απαρτίζουν το πρόθεμα

Για παράδειγμα, νομότυπες αναπαραστάσεις του 60μπιτου προθέματος 12AB00000000CD3 είναι οι:
• 12AB:0000:0000:CD30:0000:0000:0000:0000/60
• 12AB::CD30:0:0:0:0/60
• 12AB:0:0:CD30::/60

Ο Πίνακας 3 δείχνει κάποιες απεικονίσεις που δεν είναι σωστές.

Διεύθυνση	Λάθος
12AB:0:0:CD3/60	αποκόπτει τα αρχικά αλλά όχι τα τελικά μηδενικά από οποιοδήποτε 16 μπιτ κομμάτι της διεύθυνσης
12AB::CD30/60	η διεύθυνση αριστερά του "/" γίνεται 12AB:0000:0000:0000:0000:000:0000:CD30
12AB::CD3/60	η διεύθυνση αριστερά του "/" γίνεται 12AB:0000:0000:0000:0000:000:0000:0CD3

Πίνακας 3 Λάθος τρόποι απεικόνισης προθεμάτων IPv6 διευθύνσεων

Όταν γράφονται η διεύθυνση ενός κόμβου και το πρόθεμα της, μπορούν και τα δύο να συνδυαστούν όπως δείχνει ο Πίνακας 4.

Η διεύθυνση του κόμβου	και το πρόθεμα
12AB:0:0:CD30:123:4567:89AB:CDEF	12AB:0:0:CD30::/60
ενσωματώνονται σε	
12AB:0:0:CD30:123:4567:89AB:CDEF/60	

Πίνακας 4 Συνδυασμός IPv6 διεύθυνσης με πρόθεμα

2.5 Απεικόνιση τύπου διεύθυνσης

Ο τύπος μιας IPv6 διεύθυνσης προσδιορίζεται από τα πρώτα bits της. Το μεταβλητό μήκους πεδίο που σχηματίζουν αυτά τα bits καλείται πρόθεμα τύπου – Format Prefix (FP). Η σημασία του κάθε προθέματος δίδεται στον Πίνακας 5.

Σημασία	**Πρόθεμα (δυαδικό)**	**Τμήμα του χώρου διευθύνσεων**
Δεσμευμένο	0000 0000	1/256
μη δεσμευμένο	0000 0001	1/256
Δεσμευμένο για απόδοση NSAP	0000 001	1/128
Δεσμευμένο για απόδοση IPX	0000 010	1/128
μη δεσμευμένο	0000 011	1/128
μη δεσμευμένο	0000 1	1/32
μη δεσμευμένο	0001	1/16
επίσημες διευθύνσεις Unicast	001	1/8
μη δεσμευμένο	010	1/8
μη δεσμευμένο	011	1/8
μη δεσμευμένο	100	1/8
μη δεσμευμένο	101	1/8
μη δεσμευμένο	110	1/8
μη δεσμευμένο	1110	1/16
μη δεσμευμένο	1111 0	1/32
μη δεσμευμένο	1111 10	1/64
μη δεσμευμένο	1111 110	1/128
μη δεσμευμένο	1111 1110 0	1/512
διευθύνσεις Unicast δεσμού-τοπικές	1111 1110 10	1/1024
διευθύνσεις Unicast κόμβου-τοπικές	1111 1110 11	1/1024
διευθύνσεις Multicast	1111 1111	1/256

Πίνακας 5 Σημασία των προθεμάτων στις IPv6 διευθύνσεις

Σχόλια:

1. Η “απροσδιόριστη” διεύθυνση, η διεύθυνση “ανατροφοδότησης” (loopback) και οι διευθύνσεις IPv6 με ενσωματωμένη την IPv4 διεύθυνση ορίζονται εκτός του προθέματος 0000 0000.

2. Τα προθέματα 001 έως 111, εκτός αυτό των διευθύνσεων Multicast (1111 1111), απαιτείται να έχουν ορίσματα 64-bit σύμφωνα με το EUI-64.

Αυτός ο διαχωρισμός υποστηρίζει τον άμεσο διαχωρισμό των επισήμων διευθύνσεων, των τοπικών διευθύνσεων και των multicast διευθύνσεων. Έχει δεσμευτεί χώρος για διευθύνσεις NSAP και IPX. Ο υπόλοιπος χώρος είναι διαθέσιμος για μελλοντική χρήση. Αυτό μπορεί να γίνει σαν επέκταση των υπαρχόντων χρήσεων ή για νέες χρήσεις. Η αρχική αυτή κατανομή αφορά το 15% του χώρου των διευθύνσεων. Το υπόλοιπο 85% αφορά μελλοντική χρήση.

Οι διευθύνσεις unicast διακρίνονται από τις multicast από την τιμή τής υψηλής τάξης οκτάδας της διεύθυνσης: η τιμή FF (11111111) ορίζει μια διεύθυνση ως multicast, οποιαδήποτε άλλη τιμή ορίζει unicast διεύθυνση. Οι διευθύνσεις anycast αντλούνται από των χώρο των unicast διευθύνσεων, και δεν είναι συντακτικά διακρίσιμες από αυτές.

2.6 Διευθύνσεις unicast

Υπάρχουν διάφοροι τύποι διευθύνσεων unicast στο IPv6: η επίσημη διαδικτυακά δεσμευμένη διεύθυνση, η NSAP διεύθυνση, η IPX ιεραρχική διεύθυνση, η τοπική διεύθυνση κόμβου, η τοπική διεύθυνση δεσμού (link-local) και η IPv4 συμβατή διεύθυνση. Νέοι τύποι διευθύνσεων μπορούν να προστεθούν στο μέλλον.

Οι κόμβοι IPv6 μπορεί να έχουν σχετική ή μηδαμινή γνώση της εσωτερικής δομής της διεύθυνσης IPv6, αναλόγως με τον ρόλο που παίζουν (π.χ. server με δρομολογητή). Κατ' ελάχιστον, ένας κόμβος μπορεί να «πιστεύει» ότι οι διευθύνσεις unicast (της δικής του συμπεριλαμβανομένου) δεν έχουν εσωτερική δομή:

128 bits
Διεύθυνση κόμβου

Πίνακας 6 Ipv6 διεύθυνση χωρίς γνώση της δομής της

Ένας ελαφρώς πιο προχωρημένος server (αλλά πάντα απλής μορφής) θα μπορούσε επί προσθέτως να είναι ενήμερος για τα προθέματα υποδικτύου των δεσμών που είναι προσκολλημένος, όπου διαφορετικές διευθύνσεις μπορούν να έχουν διαφορετικές τιμές για n:

n bits	128-n bits
Πρόθεμα υποδικτύου	ID διεργασίας

Πίνακας 7 Ipv6 διεύθυνση με γνώση του προθέματος υποδικτύου

Ακόμη πολυπλοκότεροι servers μπορεί να είναι ενήμεροι για περισσότερα πεδία των διευθύνσεων unicast. Αν και ένας απλούστατος δρομολογητής μπορεί να μην έχει γνώση για την εσωτερική δομή των διευθύνσεων unicast, οι δρομολογητές, γενικά, γνωρίζουν τα ιεραρχικά γνωρίσματα των πρωτοκόλλων δρομολόγησης. Τα όρια γνώσης θα διαφέρουν από δρομολογητή σε δρομολογητή, ανάλογα με την θέση που αυτοί κατέχουν στην ιεραρχία δρομολόγησης.

2.6 Ορίσματα διεργασιών

Τα ορίσματα διεργασιών στις διευθύνσεις unicast χρησιμοποιούνται για να ορισθούν οι διεργασίες ενός link. Απαιτείται να είναι μοναδικά στο link αυτό. Επίσης μπορεί να είναι μοναδικά και από ευρύτερης άποψης. Αρκετές φορές ένα όρισμα θα ταυτίζεται με την διεύθυνση του επιπέδου του link της διεργασίας. Το ίδιο αυτό όρισμα της διεργασίας μπορεί να χρησιμοποιηθεί σε πολλαπλές διεργασίες ενός κόμβου. Να σημειωθεί ότι η χρήση κοινού ορίσματος διεργασίας σε πολλαπλές διεργασίες ενός κόμβου δεν επηρεάζει την παγκόσμια μοναδικότητα του ορίσματος ή την παγκόσμια μοναδικότητα της διεύθυνσης που προκύπτει από την χρήση του ορίσματος αυτού.

Σε αρκετούς τύπου προθέματος τα ορίσματα διεργασιών απαιτούνται να είναι μήκους 64 bits και σύμφωνα με το IEEE EUI-64 format [EUI64]. Τα ορίσματα αυτά μπορεί να έχουν παγκόσμια ή τοπική προοπτική (scope) αναλόγως με τι χρειάζεται. Είναι απαραίτητο το «u» bit (universal/local bit στην IEEE EUI-64 ορολογία) να αντιστρέφεται. Για παγκόσμια προοπτική τίθεται σε 1 και για τοπική σε 0. Το κίνητρο αναστροφής του u bit κατά τον σχηματισμό του ορίσματος είναι η διευκόλυνση των διαχειριστών συστημάτων κατά την διαμόρφωση ορισμάτων τοπικής προοπτικής . Το εναλλακτικό θα ήταν η χρήση της μορφής: 0200:0:0:1, 0200:0:0:2 αντί του απλούστερου ::1,::2, κτλ.

Η χρήση του universal/local bit στο IEEE EUI-64 όρισμα είναι για την μελλοντική ανάπτυξη τεχνολογίας που να μπορεί να αξιοποιήσει τα ορίσματα διεργασιών παγκόσμιας προοπτικής.

2.7 Η απροσδιόριστη διεύθυνση

Η διεύθυνση 0:0:0:0:0:0:0:0 καλείται απροσδιόριστη διεύθυνση. Δεν πρέπει ποτέ να αποδοθεί σε κόμβο. Καταδεικνύει την απουσία διεύθυνσης. Ένα παράδειγμα της χρησιμότητας της είναι το πεδίο διεύθυνσης του αποστολέα κάθε

πακέτου που αποστέλλεται από έναν server σε φάση αρχικοποίησης πριν αυτός ενημερωθεί για την διεύθυνση του. Δεν μπορεί να χρησιμοποιηθεί ως διεύθυνση παραλήπτη ή για δρομολόγηση.

2.8 Η διεύθυνση ανατροφοδότησης (loopback)

Η διεύθυνση unicast 0:0:0:0:0:0:0:1 καλείται διεύθυνση ανατροφοδότησης. Χρησιμοποιείται ώστε κάποιος κόμβος να στείλει IPv6 πακέτο στον εαυτό του. Δεν πρέπει ποτέ να αποδοθεί σε διεργασία. Πρέπει να αντιμετωπίζεται σαν να συσχετίζεται με μια εικονική διεργασία .

Η διεύθυνση ανατροφοδότησης δεν πρέπει να χρησιμοποιείται σαν διεύθυνση αποστολέα πακέτου που στέλνεται έξω από τον κόμβο και ένα τέτοιο πακέτο ποτέ δεν πρέπει να προωθείται από δρομολογητή.

2.9 Διευθύνσεις IPv6 με ενσωματωμένες IPv4 διευθύνσεις

Οι μηχανισμοί μεταφοράς IPv6 (transition mechanisms-TRAN) περιέχουν μια τεχνική ώστε εξυπηρέτες και δρομολογητές να προωθούν πακέτα IPv6 σε IPv4 υποδομή. Αυτό επιτυγχάνεται με διευθύνσεις unicast που φέρουν την διεύθυνση IPv4 στα 32 χαμηλότερης τάξης bits. Αυτού του τύπου η διεύθυνση ορίζεται ως «IPv4- συμβατή διεύθυνση IPv6» και έχει την μορφή που δείχνει ο Πίνακας 8.

80 bits	16	32 bits
0000.....0000	0000	IPv4 address

Πίνακας 8 IPv4-compatible IPv6 διεύθυνση

Ένας δεύτερος τύπος διεύθυνσης IPv6 που περιέχει μια ενσωματωμένη διεύθυνση IPv4 επίσης ορίζεται. Αυτή η μορφή χρησιμοποιείται στην απεικόνιση διευθύνσεων κόμβων που υποστηρίζουν μόνο IPv4 σαν IPv6 διευθύνσεις. Αυτός ο τύπος διεύθυνσης καλείται IPv4-χαρτογραφημένη IPv6 διεύθυνση και έχει την μορφή που δείχνει ο Πίνακας 9.

80 bits	16	32 bits
0000.....0000	FFFF	IPv4 address

Πίνακας 9 IPv4 mapped IPv6 διεθυνση

2.10 Διευθύνσεις NSAP

Γενικά συστήνεται οι σχεδιαστές δικτύων που έχουν σχεδιάσει ή αναπτύξει ένα σχέδιο διευθυνσιοδότησης OSI NSAP να το επανασχεδιάσουν σε IPv6. Παρ' όλα αυτά έχει οριστεί ένα σύνολο μηχανισμών υποστήριξης διευθύνσεων NSAP σε IPv6 δίκτυο, το οποίο περιλαμβάνει επίσης μια αντιστοίχηση IPv6 διευθύνσεων στην OSI μορφή διευθύνσεων.

2.11 Διευθύνσεις IPX

Η μετατροπή διευθύνσεων IPX σε IPv6 γίνεται όπως δείχνει ο Πίνακας 10.

7 bits	121 bits
0000010	Υπό μελέτη

Πίνακας 10 Μετατροπή IPX σε IPv6 διευθύνσεις

2.12 Επίσημες διαδικτυακά δηλωμένες διευθύνσεις Unicast

Οι επίσημες διαδικτυακά δηλωμένες διευθύνσεις Unicast (Aggregatable Global Unicast Addresses) έχουν την μορφή που δείχνει ο Πίνακας 11. Το μήκος της unicast διεύθυνσης μιας διεργασίας διαδικτυακού τύπου πρέπει να είναι 64 bits.

3	13	8	24	16	64 bits
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID

Πίνακας 11

- **001**: Πρόθεμα μορφής (Format Prefix) (3 bit)
- **TLA ID**: Όρισμα υψηλού επιπέδου (Top-Level Aggregation Identifier)
- **RES**: Δεσμευμένο για μελλοντική χρήση
- **NLA ID**: Όρισμα επομένου επιπέδου (Next-Level Aggregation Identifier)
- **SLA ID**: Όρισμα επιπέδου κόμβου (Site-Level Aggregation Identifier)
- **INTRFCE ID**: Όρισμα διεργασίας (Interface Identifier)

Αναλυτικά:

• Το όρισμα υψηλού επιπέδου (Top-Level Aggregation Identifier) βρίσκεται στην κορυφή της ιεραρχίας δρομολογήσεων. Όλοι οι δρομολογητές θα πρέπει να έχουν ένα πίνακα δρομολογήσεων για κάθε ενεργό TLA ID και, πιθανώς, θα έχουν επίσης καταχωρήσεις για τα TLA ID στα οποία βρίσκονται. Είναι δυνατόν να έχουν επιπρόσθετες καταχωρήσεις για την συγκεκριμένη τοπολογία της οποίας αποτελούν μέρος, αλλά γενικά η συνολική τοπολογία πρέπει να είναι τέτοια ώστε να ελαχιστοποιείται ο αριθμός καταχωρήσεων στους γενικούς πίνακες δρομολόγησης. Αυτή η πολιτική διευθυνσιοδότησης υποστηρίζει 8192 (2_{13}) ορίσματα TLA. Επιπρόσθετα ορίσματα μπορούν να προστεθούν, είτε επεκτείνοντας το πεδίο προς τα δεξιά προς το πεδίο RES, ή χρησιμοποιώντας νέας μορφής προθέματα.

• Το πεδίο RES είναι για μελλοντική χρήση και πρέπει να τίθεται σε 0. Επιτρέπει την μελλοντική επέκταση των πεδίων TLA, NLA, αν απαιτηθεί.

• Το όρισμα επομένου επιπέδου (Next-Level Aggregation Identifier) χρησιμοποιείται από οργανισμούς που τους έχει αποδοθεί ένα όρισμα TLA για να οργανώσουν την εσωτερική δομή του δικτύου τους. Για αυτό το σκοπό χρησιμοποιούν το ανώτερο μέρος του NLA ορίσματος και το υπόλοιπο μπορεί να χρησιμοποιηθεί για τον ορισμό τόπων του δικτύου τους:

n	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interface ID

Κάθε οργανισμός που δεσμεύει όρισμα TLA, αποκτά 24 bits χώρο NLA. Ο χώρος αυτός αντιστοιχεί περίπου με τον χώρο που ολόκληρο το τρέχον IPv4 Internet μπορεί να καλύψει. Μπορεί να αποδώσει NLA ορίσματα σε άλλους οργανισμούς που είτε παρέχουν, είτε δεν παρέχουν με την σειρά τους υπηρεσίες. Σε περίπτωση που παρέχουν υπηρεσίες μπορούν να αποδώσουν με την σειρά τους ορίσματα NLA σε άλλους οργανισμούς όπως φαίνεται στο Σχήμα 16.

N	24-n bits			16	64 bits
NLA1	Site ID			SLA ID	Interface ID
	m	24-n-m bits		16	64 bits
	NLA2	Site ID		SLA ID	Interface ID
		o	24-n-m-o	16	64 bits
		NLA3	Site ID	SLA ID	Interface ID

Σχήμα 16 Απόδοση NLA ορισμάτων

Η κατανομή του χώρου NLA είναι στην αρμοδιότητα του οργανισμού που είναι υπεύθυνος για το TLA. Αντίστοιχα αρμόδιος οργανισμός για κάθε NLA όρισμα είναι αυτός που κατέχει το NLA του προηγούμενου επιπέδου.

• Το όρισμα επιπέδου τόπου (Site-Level Aggregation Identifier) χρησιμοποιείται από κάθε οργανισμό για την ιδιαίτερη δομή διευθύνσεων και τα υποδίκτυά του. Το 16-bit SLA πεδίο παρέχει 65535 ανεξάρτητα υποδίκτυα. Η δομή αυτή μπορεί να είναι ενός επιπέδου είτε δύο ή και περισσοτέρων επιπέδων ιεραρχίας (που οδηγεί σε μικρότερους πίνακες δρομολόγησης) όπως φαίνεται στο Σχήμα 17.

n	16-n		64 bits
SLA1	Subnet		Interface ID
	m	16-n-m	64 bits
	SLA2	Subnet	Interface ID

Σχήμα 17 Δομή SLA

Ο υποστηριζόμενος αριθμός υποδικτύων που μπορούν να δημιουργηθούν κρίνεται επαρκής για την συντριπτική πλειοψηφία φορέων και οργανισμών. Πάντα υπάρχει, βεβαίως, η προοπτική να αποκτηθούν από τον παροχέα υπηρεσιών επιπρόσθετα ορίσματα SLA για την επέκταση του αριθμού υποδικτύων.

• Το όρισμα διεργασίας (Interface Identifier) χρησιμοποιείται για να ορίσει μια διεργασία σε ένα δεσμό, το όρισμα αυτό πρέπει να είναι μοναδικό σε σχετικά με αυτόν τον δεσμό, αλλά μπορεί να είναι μοναδικό και σε ευρύτερη περιοχή. Σε πολλές περιπτώσεις ένα όρισμα διεργασίας είναι δυνατόν να είναι ταυτόσημο ή να βασίζεται σε αυτό της διεύθυνσης της διεργασίας επιπέδου δεσμού.

2.13 Τοπικής χρήσης διευθύνσεις Unicast

Υπάρχουν δύο είδη τοπικής χρήσης διευθύνσεις Unicast (Local-Use IPv6 Unicast Addresses), οι τοπικού δεσμού (Link-Local) και οι τοπικού κόμβου (Site-Local). Οι πρώτες είναι για χρήση σε ένα δεσμό και οι δεύτερες για χρήση σε ένα μοναδικό κόμβο.

Οι διευθύνσεις τοπικού δεσμού έχουν την μορφή που δείχνει ο Πίνακας 12.

10 bits	54 bits	64 bits
1111111010	0	Όρισμα διεργασίας

Πίνακας 12 Link-Local διευθύνσεις

Οι διευθύνσεις τοπικού δεσμού σχεδιάστηκαν για την χρήση σε διευθυνσιοδότηση απλού δεσμού με στόχους την διαμόρφωση αυτοδιευθυνσιοδότησης, ανακάλυψη γείτονα ή όταν δεν υπάρχουν δρομολογητές. Οι δρομολογητές δεν πρέπει να δρομολογούν πακέτα με διεύθυνση τοπικού δεσμού ως διεύθυνση αποστολέα ή παραλήπτη.

Οι διευθύνσεις τοπικού κόμβου έχουν την ακόλουθη μορφή:

10 bits	38 bits	16 bits	64 bits
1111111011	0	Όρισμα υποδικτύου	Όρισμα διεργασίας

Πίνακας 13 Site-Local διευθύνσεις

Οι διευθύνσεις τοπικού κόμβου σχεδιάστηκαν για την χρήση εσωτερικά σε κόμβους χωρίς την χρήση παγκόσμιου προθέματος. Οι δρομολογητές δεν πρέπει να δρομολογούν πακέτα με διεύθυνση τοπικού κόμβου ως διεύθυνση αποστολέα ή παραλήπτη.

2.14 Διευθύνσεις Anycast

Η διεύθυνση Anycast είναι μια διεύθυνση που μπορεί να αποδοθεί σε περισσότερες από μία διεργασίες (οι οποίες ανήκουν σε διαφορετικούς κόμβους), με την ιδιότητα ότι το πακέτο που αποστέλλεται σε μια anycast διεύθυνση προωθείται στην «κοντινότερη» διεργασία με αυτήν την διεύθυνση, σύμφωνα με τα πρωτόκολλα μέτρησης αποστάσεως.

Οι διευθύνσεις anycast αντλούνται από τον χώρο των unicast διευθύνσεων, με όποια από τις καθορισμένες unicast μορφές. Έτσι τα δύο είδη διευθύνσεων είναι συντακτικά ταυτόσημα. Όταν μια unicast διεύθυνση αποδοθεί

σε περισσότερες από μια διεργασίες, οι κόμβοι που φιλοξενούν τις διεργασίες αυτές πρέπει απαραιτήτως να ενημερωθούν πως πρόκειται για anycast διευθύνσεις.

Για κάθε διεύθυνση ορισμένη ως anycast, υπάρχει ένα μέγιστο πρόθεμα διεύθυνσης P που ορίζει την τοπολογική περιοχή στην οποία βρίσκονται όλες οι διεργασίες που ανήκουν στην διεύθυνση αυτή. Μέσα στην περιοχή του P, κάθε μέλος του συνόλου unicast πρέπει να δηλώνεται με ξεχωριστή καταχώρηση στο σύστημα δρομολόγησης. Εκτός της περιοχής που ορίζεται από το P, η anycast διεύθυνση πρέπει να προστεθεί στην καταχώρηση δρομολόγησης του P.

Να σημειωθεί ότι στην χειρότερη περίπτωση, το πρόθεμα P ενός συνόλου anycast μπορεί να είναι το null π.χ. όταν τα μέλη του συνόλου δεν έχουν τοπολογική συγκέντρωση. Σε αυτήν την περίπτωση, η διεύθυνση anycast πρέπει να διανεμηθεί σαν ξεχωριστή καταχώρηση σε όλο το διαδίκτυο, το οποίο και εμφανίζει το αυστηρό όριο των παγκοσμίων διευθύνσεων anycast που μπορούν να υποστηριχθούν. Μια από τις συνεπαγόμενες χρήσεις των διευθύνσεων anycast είναι να ορισθεί το σύνολο των δρομολογητών που ανήκουν σε έναν οργανισμό. Αυτές οι διευθύνσεις μπορεί να χρησιμοποιηθούν σαν ενδιάμεσες διευθύνσεις σε ένα IPv6 σύστημα δρομολόγησης που θα οδηγεί το πακέτο να παραδοθεί μέσα από μια συγκεκριμένη διαδρομή ή σύνολο διαδρομών. Άλλες πιθανές χρήσεις είναι να καθορίσουν το σύνολο των δρομολογητών ενός συγκεκριμένου υποδικτύου, ή ενός συγκεκριμένου domain.

Γενικά, υπάρχει μικρή εμπειρία στην διασπορά στο διαδίκτυο διευθύνσεων anycast, και μερικές γνωστές επιπλοκές και κολλήματα όταν αυτές χρησιμοποιούντα ανεξέλεγκτα. Έως ότου περισσότερη εμπειρία αποκτηθεί πάνω στο θέμα οι διευθύνσεις unicast θα υπόκεινται στους παρακάτω περιορισμούς:

• Μια διεύθυνση anycast δεν πρέπει να χρησιμοποιείται σαν διεύθυνση αποστολέα σε ένα πακέτο IPv6.

• Μια διεύθυνση anycast δεν πρέπει να αποδίδεται σε κόμβο IPv6 παρά μόνο σε δρομολογητή IPv6.

2.15 Απαιτούμενη διεύθυνση anycast

Η anycast διεύθυνση δρομολόγησης υποδικτύου είναι ορισμένη με τη μορφή που δείχνει ο Πίνακας 14.

N bits	128-n bits
Πρόθεμα υποδικτύου	00000000000000

Πίνακας 14 Anycast IPv6 διεύθυνση

Το πρόθεμα υποδικτύου (subnet prefix) σε μια διεύθυνση anycast είναι το πρόθεμα που ορίζει ένα συγκεκριμένο link. Αυτού του είδους η διεύθυνση anycast είναι συντακτικά όμοια με μια διεύθυνση unicast διεργασίας σε δεσμό με την διαφορά ότι το όρισμα διεργασίας είναι 0.

Τα πακέτα που αποστέλλονται σε διεύθυνση anycast με πρόθεμα υποδικτύου θα προωθηθεί σε έναν μόνο δρομολογητή του υποδικτύου. Όλοι οι δρομολογητές απαιτείται να υποστηρίζουν τις διευθύνσεις αυτού του είδους για τα υποδίκτυα στα οποία έχουν διεργασίες.

Η διεύθυνση anycast με πρόθεμα υποδικτύου έχει σκοπό να χρησιμοποιηθεί σε εφαρμογές όπου κάποιος κόμβος χρειάζεται να επικοινωνήσει με ένα σύνολο δρομολογητών σε απομακρυσμένο υποδίκτυο.

2.16 Διευθύνσεις Multicast

Μια διεύθυνση multicast είναι ένα όρισμα συνόλου κόμβων. Ένας κόμβος μπορεί να ανήκει σε οποιονδήποτε αριθμό ομάδων multicast. Οι διευθύνσεις multicast έχουν την μορφή που δείχνει ο Πίνακας 15.

8	4	4	112 bits
11111111	Flgs	Scop	Group id

Πίνακας 15 Multicast IPv6 διευθύνσεις

• 11111111 στην αρχή της διεύθυνσης δηλώνει ότι πρόκειται για διεύθυνση Multicast

• Flgs είναι ένα σύνολο 4 flags: Τα πρώτα 3 είναι δεσμευμένα και πρέπει να είναι 0. Το τέταρτο flag T, με T=0 δείχνει μια μονίμως ορισμένη διεύθυνση multicast, υποδεικνυόμενη από την παγκόσμια διεύθυνση διευθυνσιοδότησης διαδικτύου, ενώ με T=1 δείχνει μια όχι μονίμως ορισμένη διεύθυνση multicast.

• Scop είναι μια 4-bit τιμή πολλαπλού σκοπού που χρησιμοποιείται για να ορίσει το εύρος της ομάδας multicast. Οι τιμές είναι:
ο δεσμευμένη
ο τοπικού δεσμού
ο τοπικού κόμβου
ο μη ορισμένη
ο μη ορισμένη
ο τοπικού τόπου
ο μη ορισμένη
ο μη ορισμένη
ο τοπικού οργανισμού

o μη ορισμένη
o A μη ορισμένη
o B μη ορισμένη
o C μη ορισμένη
o D μη ορισμένη
o E παγκόσμια
o F δεσμευμένη

• Group id καθορίζει την ομάδα multicast, είτε μόνιμη είτε προσωρινή.
Η έννοια της μονίμως ορισμένης διεύθυνσης multicast είναι ανεξάρτητη του εύρους της ομάδας της. Για παράδειγμα, αν στην ομάδα εξυπηρετών NTP έχει αποδοθεί μια μόνιμη διεύθυνση multicast με όρισμα ομάδας το 101 (hex) τότε:

• FF01:0:0:0:0:0:0:101 ορίζει σαν αποστολέα όλους τους NTP servers του κόμβου

• FF02:0:0:0:0:0:0:101 ορίζει σαν αποστολέα όλους τους NTP servers του link

• FF05:0:0:0:0:0:0:101 ορίζει σαν αποστολέα όλους τους NTP servers του site

• FF0E:0:0:0:0:0:0:101 ορίζει σαν αποστολέα όλους τους NTP servers του Διαδικτύου

Η μη μονίμως ορισμένες διευθύνσεις multicast έχουν έννοια μόνο σε περιορισμένο εύρος ομάδας. Για παράδειγμα, ένα σύνολο ορισμένο με την μη μόνιμη, τοπικού τόπου διεύθυνση multicast FF15:0:0:0:0:0:0:101 σε κάποιον τόπο δεν έχει καμία σχέση με άλλο σύνολο σε άλλον τόπο με ακριβώς ίδια διεύθυνση, ούτε με ένα σύνολο σε άλλο τόπο με διαφορετικό εύρος ομάδας, ούτε με ένα μόνιμο σύνολο με το ίδιο όρισμα. Οι διευθύνσεις multicast δεν πρέπει να χρησιμοποιούνται σε πακέτα στο πεδίο αποστολέας ή να εμφανίζονται σε προθέματα δρομολόγησης.

2.17 Προκαθορισμένες Διευθύνσεις Multicast

Οι ακόλουθες διευθύνσεις multicast είναι προδεσμευμένες και δεν επιτρέπεται να αποδοθούν σε κανένα σύνολο multicast:
• FF00:0:0:0:0:0:0:101
• FF01:0:0:0:0:0:0:101
• FF02:0:0:0:0:0:0:101
• FF03:0:0:0:0:0:0:101
• FF04:0:0:0:0:0:0:101
• FF05:0:0:0:0:0:0:101
• FF06:0:0:0:0:0:0:101

• FF07:0:0:0:0:0:0:101
• FF08:0:0:0:0:0:0:101
• FF09:0:0:0:0:0:0:101
• FF0A:0:0:0:0:0:0:101
• FF0B:0:0:0:0:0:0:101
• FF0C:0:0:0:0:0:0:101
• FF0D:0:0:0:0:0:0:101
• FF0E:0:0:0:0:0:0:101
• FF0F:0:0:0:0:0:0:101

Οι ακόλουθες διευθύνσεις multicast αντιπροσωπεύουν όλους τους IPv6 κόμβους με εύρος 1 (τοπικές κόμβου) και 2 (link-local).
• FF01:0:0:0:0:0:0:1
• FF02:0:0:0:0:0:0:1

Οι ακόλουθες διευθύνσεις multicast αντιπροσωπεύουν όλους τους IPv6 δρομολογητές με εύρος 1 (τοπικές κόμβου), 2 (link-local) και 3 (site-local).
• FF01:0:0:0:0:0:0:2
• FF02:0:0:0:0:0:0:2
• FF05:0:0:0:0:0:0:2

Για την μετατροπή διευθύνσεων unicast ή anycast σε multicast προστίθονται τα 24 χαμηλότερης τάξης bits της διεύθυνσης με το πρόθεμα FF02:0:0:0:0:1:FF00::/104 επιστρέφοντας διεύθυνση multicast της περιοχής από FF02:0:0:0:0:1:FF00:0000 έως FF02:0:0:0:0:1:FFFF:FFFF. Για παράδειγμα η αναλυμένη multicast για την διεύθυνση 4037::01::800:200E:8C6C είναι η FF02::1:FF0E:8C6C. Κάθε κόμβος απαιτείται να υπολογίζει την εκφρασμένη multicast διεύθυνση για κάθε unicast, anycast διεύθυνση που του αποδίδεται.

2.18 Απαιτούμενες διευθύνσεις κόμβου

Ένας κόμβος υποχρεούται να αναγνωρίζει τις ακόλουθες διευθύνσεις για τη αυτοαναγνώριση του:

• Την διεύθυνση τοπικού δεσμού για κάθε διεργασία
• Την αποδοσμένη unicast διεύθυνση του
• Την διεύθυνση ανατροφοδότησης
• Τις διευθύνσεις multicast όλων των κόμβων
• Την εκφρασμένη unicast διεύθυνση για κάθε unicast, anycast διεύθυνση που του έχει αποδοθεί.

3.1 IPv6 και εφαρμογές πραγματικού χρόνου

Το Internet σχεδιάστηκε για να προσφέρει best effort κίνηση και βασίζεται στην ιδέα ότι το δίκτυο θα κάνει όλες τις δυνατές προσπάθειες για να παραδώσει ένα πακέτο, χωρίς όμως να παρέχει κάποια εγγύηση για την επιτυχή παραλαβή του πακέτου ή τον πραγματικό χρόνο που αυτή θα γίνει.

Οι εφαρμογές πραγματικού χρόνου (real time applications) παράγουν τη λεγόμενη κίνηση πραγματικού χρόνου (real time traffic). Η κίνηση πραγματικού χρόνου είναι ένα είδος κίνησης ευαίσθητο στις καθυστερήσεις και τις απώλειες κατά τη διάρκεια της μετάδοσης των πακέτων. Επιπλέον, η κίνηση πραγματικού χρόνου συχνά απαιτεί την ύπαρξη ενός ελάχιστου εγγυημένου bandwidth. Η εισαγωγή των υπηρεσιών πραγματικού χρόνου (real time services) στα δίκτυα έχει κάνει επιτακτική την ανάγκη για υποστήριξη Quality of Service (QoS). Η υποστήριξη για Quality of Service θα πρέπει επίσης να παρέχεται και για τη multicast μετάδοση δεδομένων, γιατί η multicast μετάδοση δεδομένων χρησιμοποιείται συχνά από τις εφαρμογές πραγματικού χρόνου.

Η παροχή εγγυήσεων ποιότητας στις εφαρμογές πραγματικού χρόνου συνδέεται στενά με την δυνατότητα διαχείρισης των δικτυακών πόρων (δηλ. το bandwidth). Για να μπορεί το δίκτυο να παρέχει εγγυήσεις ποιότητας, πρέπει να ενσωματωθούν στο δίκτυο μηχανισμοί που χειρίζονται τους δικτυακούς πόρους και μηχανισμοί που δέχονται ή απορρίπτουν αιτήσεις (Admission Control).

Η multimedia επικοινωνία επηρεάζεται από αρκετά χαρακτηριστικά του IPv6:

• Χαρακτηριστικά που προσφέρει το IPv6 για την παροχή QoS σε εφαρμογές πραγματικού χρόνου.
• Ενσωματωμένη υποστήριξη IP Multicast.
• Μεγάλος χώρος διευθύνσεων.
• Χαρακτηριστικά που επιτρέπουν το autoconfiguration.
• Αποτελεσματική και γρήγορη δρομολόγηση.
• Υποστήριξη μηχανισμών ασφάλειας στο επίπεδο δικτύου.

Μερικά από τα χαρακτηριστικά του IPv6 μπορούν να βελτιώσουν σημαντικά την υποστήριξη για εφαρμογές πραγματικού χρόνου, και ειδικότερα τα δύο νέα πεδία επικεφαλίδας:

• Το μήκους 8 bit πεδίο Traffic Class
• Το μήκους 20 bit πεδίο Flow Label

Το πεδίο Traffic Class αναμένεται να έχει ανάλογη λειτουργικότητα με τα πεδία Type Of Service και Precedence του IPv4. Το πεδίο Flow Label μπορεί να

χρησιμοποιηθεί για να διαφοροποιήσει πακέτα που ανήκουν σε διαφορετικές ροές δεδομένων.

Επιπλέον, τα πρωτόκολλα που συνοδεύουν το IPv6 όπως το ICMPv6 (το οποίο συμπεριλαμβάνει λειτουργικότητα για τη διαχείριση multicast groups) και το OSPFv6 (το οποίο διαχειρίζεται multicast δέντρα) επίσης συνεισφέρουν στη βελτίωση της υποστήριξης εφαρμογών πραγματικού χρόνου.

Οι βελτιώσεις που προσφέρει το IPv6 δεν είναι βέβαια δυνατόν να υποστηρίξουν όλες τις εφαρμογές πραγματικού χρόνου πάνω από ένα δίκτυο best-effort όπως το Internet. Έτσι το IPv6 ήταν αρχικά μέρος του φιλόδοξου σχεδίου Integrated Services, το οποίο στοχεύει στην επέκταση της αρχιτεκτονικής του Internet ώστε να μπορεί να υποστηρίζει και κίνηση πραγματικού χρόνου. Επιπλέον, ο τελικός καθορισμός της χρήσης των Traffic Class και Flow Label πεδίων δεν έχει γίνει ακόμα.

Το πεδίο Traffic Class μπορεί να χρησιμοποιηθεί για να διαφοροποιηθεί ο χειρισμός της κίνηση βάσει της τιμής κάθε πακέτου σε αυτό το πεδίο. Όταν εμφανίζεται συμφόρηση, μπορεί να χρησιμοποιηθεί ένας προκαθορισμένος κανόνας βασισμένος στο Traffic Class πεδίο, ώστε κάποια πακέτα να πετάγονται. Επομένως το πεδίο μπορεί να αποβεί χρήσιμο για την υλοποίηση QoS μηχανισμών βασισμένων στην DiffServ αρχιτεκτονική (για παράδειγμα η Thomson edge device χρησιμοποιεί το πεδίο Traffic Class για την υλοποίηση QoS βασισμένου στην DiffServ αρχιτεκτονική).

Το πεδίο Flow Label στην επικεφαλίδα των IPv6 πακέτων σχεδιάστηκε ώστε να μπορεί μία ροή κίνησης να αναγνωριστεί, και άρα να μπορούν οι ενδιάμεσοι κόμβοι να χρησιμοποιήσουν την ετικέτα αυτή για να αναγνωρίσουν ροές κίνησης και να τις χειριστούν ανάλογα (χρησιμοποιώντας για παράδειγμα ένα πρωτόκολλο κράτησης πόρων όπως το RSVP). Η χρήση του πεδίου Flow Label στα IP πακέτα μπορεί να βοηθήσει τους ενδιάμεσους κόμβους ώστε να επεξεργαστούν την κίνηση ταχύτερα, αν τα μονοπάτια και οι κρατήσεις για συγκεκριμένες ομάδες ροών έχουν νωρίτερα καθοριστεί στους ενδιάμεσους αυτούς κόμβους. Η τιμή του πεδίου Flow Label αρχικοποιείται από τις πηγές των ροών. Αυτό σημαίνει ότι το πεδίο Flow Label μπορεί να χρησιμοποιηθεί για την υλοποίηση QoS σχημάτων βασισμένων στην IntServ αρχιτεκτονική (για παράδειγμα ο Lancaster RSVP media server χρησιμοποιεί το πεδίο Flow Label για την υλοποίηση QoS βασισμένου στην IntServ αρχιτεκτονική).

Το IPv6 προσφέρει επίσης τη δυνατότητα χρήσης επιπλέον επικεφαλίδων μέσω του πεδίου Next Headers. Αυτή η δυνατότητα μπορεί να χρησιμοποιηθεί για την υλοποίηση Quality of Service σχημάτων βασισμένων σε νέες επικεφαλίδες. Η χρήση του IPv6 έχει το μειονέκτημα της μεταφοράς μιας σημαντικά μεγαλύτερης επικεφαλίδας, η οποία συνεπάγεται μεγαλύτερο RTP / UDP / IP overhead. Αυτό το overhead μπορεί να επηρεάσει αρνητικά τα χαμηλής ταχύτητας δίκτυα και άρα πρέπει να χρησιμοποιηθούν κάποιοι αποτελεσματικοί μηχανισμοί συμπίεσης.

Το IPv6 συμπεριλαμβάνει επίσης μηχανισμούς ασφάλειας μέσω δύο επικεφαλίδων επέκτασης, των Authentication Header (AH) και Encrypted Security Payload (ESP).

Η Authentication Header προσφέρει τη δυνατότητα για εξακρίβωση αυθεντικότητας χρήστη (user authentication) και διασφάλιση ακεραιότητας IP πακέτων (IP packet integrity), και προλαμβάνει την μη εξουσιοδοτημένη τροποποίηση ενός πακέτου ή την ψευδή αποστολή πακέτων (packet spoofing). Η Encrypted Security Payload επικεφαλίδα προσφέρει ενθυλάκωση ρυπτογραφημένων δεδομένων (encrypted data encapsulation) έτσι ώστε μόνο ο επιθυμητός κόμβος αποστολής να μπορεί να διαβάσει τα δεδομένα του πακέτου. Οι δύο αυτές επικεφαλίδες χρησιμοποιούν την έννοια του Security Association (SA), σε Transport και Tunnel mode.

Κατά την χρήση της Authentication Header σε tunnel mode, η ασφάλεια παρέχεται για τμήματα της εξωτερικής IP επικεφαλίδας και ολόκληρο το εσωκλειόμενο πακέτο (το οποίο περνάει μέσα από το tunnel), ενώ όταν χρησιμοποιείται η Encrypted Security Payload, προστατεύεται μόνο το εσωκλειόμενο πακέτο. Αν έχει εγκαθιδρυθεί Security Association μεταξύ των δύο επικοινωνούντων κόμβων, τότε είτε transport είτε tunnel mode μπορεί να χρησιμοποιηθεί. Αν μία από τις ακμές είναι ένα security gateway τότε μόνο tunnel mode μπορεί να χρησιμοποιηθεί.

4.1 Γιατί η μετακίνηση από το IPv4 στο IPv6 είναι αναγκαία

Θα έλεγε κανείς ότι το IPv4 δουλεύει αρκετά καλά, ιδιαίτερα λαμβάνοντας υπόψη την ηλικία του. Σχεδόν κάθε σύστημα στον κόσμο χρησιμοποιεί IPv4 (εκτός ίσως από λίγα πειραματικά δίκτυα που χρησιμοποιούν από τώρα IPv6). Οπότε κάθε σύστημα στον κόσμο θα πρέπει να αναβαθμιστεί, προκειμένου να υποστηρίζεται το IPv6. Πρόκειται για ένα αριθμό συστημάτων της τάξης των 100 εκατομμυρίων, που χρησιμοποιούν διάφορες εκδόσεις δικτυακού λογισμικού για TCP/IP, που τρέχουν σε μια πληθώρα λειτουργικών συστημάτων και υλικού.

Υπάρχει το ερώτημα αν θα μπορούσε να αποφευχθεί το κόστος που μια ενδεχόμενη αναβάθμιση στο IPv6 θα μπορούσε να επιφέρει. Βασικά όλα εξαρτώνται από το βαθμό που ένα νέο πρωτόκολλο είναι αναγκαίο. Αν το μόνο πρόβλημα που αντιμετώπιζε το IPv4 ήταν η έλλειψη διευθύνσεων, θα μπορούσε να επιβιώσει για κάμποσο ακόμα χρησιμοποιώντας τεχνικές όπως το NAT (Network Address Translation), το CIDR (Classless Inter-Domain Routing) και το subnetting. Φυσικά αυτές είναι βραχυπρόθεσμες λύσεις που χρησιμοποιούνται χρόνια τώρα. Η ανάπτυξη του διαδικτύου στο απώτερο μέλλον δεν θα είναι δυνατή αν το πρωτόκολλο IP δεν αναβαθμιστεί.

Το IPv4 επιδέχεται κι άλλες βελτιώσεις εκτός από την αύξηση του χώρου διευθύνσεων. Αυτές έχουν να κάνουν με τη διαχείριση (administration), με τη δρομολόγηση (routing), την ποιότητα υπηρεσιών, την ιεραρχία και την ασφάλεια. Μετά από χρόνια εμπειρίας πάνω στο IPv4 είναι γνωστό τι δουλεύει καλά, τι απλά δουλεύει και άρα επιδέχεται βελτιώσεων, τι θα ήταν επιθυμητό να προστεθεί και τι είναι πραγματικά περιττό. Οπότε η μετάβαση από το IPv4 δεν έχει να κάνει με την αντικατάσταση μιας γνωστής ποσότητας με μια άγνωστη. Οι σχεδιαστές του IPv6 έχτισαν το καινούριο πρωτόκολλο πάνω στο IPv4,

κρατώντας ότι δούλευε καλά, βελτιώνοντας ότι δούλευε, αφαιρώντας ότι ζημίωνε την λειτουργικότητα και την απόδοση, ενώ προσέθεσαν καινούρια χαρακτηριστικά που ήταν φανερό ότι χρειάζονταν.

Στο υπόλοιπο του κεφαλαίου εξετάζονται τα μέτρα που προς το παρόν έχουν παρθεί για την αντιμετώπιση των προβλημάτων του IPv4 και καταλήγοντας απαντάται το ερώτημα του γιατί η μετάβαση είναι αναγκαία.

4.2 IPv4 Routing

Ένα πακέτο που ταξιδεύει στο διαδίκτυο πρέπει να δρομολογηθεί μεταξύ δικτύων για να φτάσει στον προορισμό του. Όλη η δρομολόγηση τελικά γίνεται από κάποιους δρομολογητές (routers) που συνδέουν τα δίκτυα μεταξύ τους. Ο δρομολογητής ελέγχει μια λίστα με διαφορετικές διαδρομές και αποφασίζει πού θα στείλει το πακέτο. Όταν η λίστα του δρομολογητή είναι πολύ μεγάλη (π.χ. οι δρομολογητές του backbone που έχουν λίστα διαδρομών για πάνω από 100.000 διαφορετικές διευθύνσεις) η δρομολόγηση μπορεί να επιφέρει μεγάλη καθυστέρηση. Εδώ υπεισέρχεται η έννοια της ιεραρχικής διευθυνσιοδότησης, όπου συνενώνοντας διαδρομές απλοποιούμε τη δρομολόγηση.

4.3 Subnetting & Classless Inter-Domain Routing (CIDR)

Το Subnetting και το CIDR είναι τεχνικές ιεραρχικής διευθυνσιοδότησης, που προσφέρουν λύσεις τόσο στην αποδοτικότερη δρομολόγηση όσο και διανομή διευθύνσεων. Το Subnetting έχει να κάνει με τη διάσπαση ενός Class A, Class B ή Class C δικτύου σε μικρότερα υποδίκτυα ίσου μεγέθους. Αυτό επιτυγχάνεται με την επέκταση της διεύθυνσης δικτύου κατά κάποια bits παραπάνω, που ονομάζονται μάσκα υποδικτύου (subnet mask). Η επέκταση αυτή δεν είναι ορατή εξωτερικά, αλλά ο δρομολογητής που συνδέει την κλάση δικτύου με το διαδίκτυο αναλαμβάνει να στείλει τα εισερχόμενα πακέτα στο αντίστοιχο υποδίκτυο. Οπότε αυτός ο δρομολογητής δεν χρειάζεται να διατηρεί λίστες δρομολόγησης για όλες τις διευθύνσεις, που αντιστοιχούν στην κλάση. Απλά στέλνει το εισερχόμενο πακέτο στο υποδίκτυο με την αντίστοιχη subnet mask. Αυτό με τη σειρά του αναλαμβάνει να στείλει το πακέτο πιο χαμηλά στην ιεραρχική οργάνωση της κλάσης, είτε είναι ο προορισμός είτε κάποιο ακόμα υποδίκτυο.

Είναι φανερό πως αν διανεμηθούν οι κλάσεις δικτύων ως έχουν, πολλές διευθύνσεις θα μείνουν αχρησιμοποίητες. Π.χ. μια εταιρία που θέλει να συνδέσει 20 μηχανήματα με το διαδίκτυο είναι λάθος να της δοθεί μια ολόκληρη Class C. Ενώ θα ήταν σωστότερο να της δοθεί ένα υποδίκτυο μιας Class C.
Το CIDR από την άλλη κάνει ακριβώς το αντίστροφο με το subnetting. Δηλαδή συνενώνει συνεχόμενα δίκτυα μιας συγκεκριμένης κλάσης σε μια μεγαλύτερη οργάνωση υπερδικτύου (supernet). Ενώ λοιπόν το subnetting λειτουργεί εσωτερικά το CIDR λειτουργεί εξωτερικά αφαιρώντας κάποια bits από τη διεύθυνση της κλάσης, που ονομάζονται μάσκα υπερδικτύου (supernet mask).

Όλη η κίνηση, που εισέρχεται στο υπερδίκτυο δρομολογείται από ένα μόνο δρομολογητή, με αποτέλεσμα να ελαφρύνονται οι πίνακες δρομολόγησης των κόμβων που βρίσκονται απ' έξω.

Παρά το ότι οι παραπάνω τεχνικές κάνουν τη διανομή διευθύνσεων αποδοτικότερη, δεν κάνουν τίποτα για την αύξηση των διευθύνσεων. Πρόκειται δηλαδή για βραχυπρόθεσμες λύσεις που απλά δίνουν λίγο χρόνο ζωής παραπάνω στο IPv4.

4.4 Network Address Translation (NAT)

Υπάρχουν περιπτώσεις δικτύων, τα οποία δεν είναι συνδεδεμένα στο διαδίκτυο. Ένας πολύ σημαντικός λόγος γι' αυτό είναι η ασφάλεια. Τα δίκτυα αυτά δεν είναι λογικό να δεσμεύουν IP διευθύνσεις, αν και στο παρελθόν, που δεν υπήρχε έλλειψη διευθύνσεων, κάτι τέτοιο ενθαρρυνόταν. Αντίθετα, τώρα, κάτι τέτοιο μάλλον αποθαρρύνεται. Φυσικά το πλεονέκτημα των μοναδικών διευθύνσεων είναι ότι όταν κάποτε ένα τέτοιο δίκτυο θελήσει να συνδεθεί με ένα άλλο δίκτυο ή το διαδίκτυο δεν θα χρειαστεί να επανακαθοριστούν οι διευθύνσεις του.

Ο μηχανισμός NAT έρχεται να προσφέρει μια λύση γι' αυτά τα δίκτυα, σε περίπτωση που θέλουν να συνδεθούν με το διαδίκτυο. Αυτό το επιτυγχάνει με τη χρήση ενός μεσολαβητή (firewall) που μεταφράζει τις διευθύνσεις του δικτύου σε μοναδικές διευθύνσεις διαδικτύου, επιτρέποντας την έμμεση επικοινωνία με το διαδίκτυο. Δεν δίνει λύση, όμως, για την περίπτωση σύνδεσης δυο δικτύων, όπου ίσως χρειαστεί να αλλαχτούν οι διευθύνσεις για να επιτευχθεί η σύνδεση.

Το NAT, ουσιαστικά, έρχεται να δελεάσει μικρούς οργανισμούς προσφέροντας τους ένα τρόπο να διαμορφώσουν μόνοι τους το δικό τους χώρο διευθύνσεων, χωρίς να βασίζονται στις αρμόδιες αρχές να τους δώσουν μοναδικές διευθύνσεις. Αυτό έχει ως αποτέλεσμα τα δίκτυα που δεν είναι συνδεδεμένα στο διαδίκτυο να μην καταναλώνουν άσκοπα πολύτιμο χώρο διευθύνσεων. Απ' την άλλη αν το NAT χρησιμοποιηθεί χωρίς σύνεση, αυτό μπορεί να οδηγήσει στο να χρειαστεί να αριθμηθούν ξανά τα μηχανήματα του δικτύου, κάπου στην πορεία. Επιπλέον, ένα μηχάνημα που βρίσκεται πίσω από NAT, έχει συνήθως μεγάλη δυσκολία στο να μπορέσει να δουλέψει σωστά με πολλά από τα πρωτόκολλα που τρέχουν πάνω από το Internet, ή να λειτουργήσει ως server.

4.5 Network Administration and Configuration

Στο παρελθόν ένα σύστημα που έτρεχε IPv4 έπρεπε να διαμορφωθεί κατάλληλα με μια σειρά από αρκετά πολύπλοκες παραμέτρους. Μερικές από αυτές είναι το host name, η IP διεύθυνση, η μάσκα δικτύου και η διεύθυνση του δρομολογητή. Δηλαδή ένα σύστημα για να συνδεθεί στο δίκτυο απαιτούσε γνώσεις και χρόνο. Προέκυψε, λοιπόν, η ιδέα ότι θα ήταν πραγματικά καλό αυτή

η διαδικασία να απλοποιηθεί. Το ιδανικό θα ήταν να συνδέεται ένα μηχάνημα στο δίκτυο και αυτό να παίρνει το configuration που πρέπει να κάνει αυτόματα.

Το πρώτο βήμα προς αυτή την κατεύθυνση έγινε με το πρωτόκολλο BOOTP (Boot Protocol). Το πρωτόκολλο αυτό παρέχει ένα μηχανισμό για ένα host, που συνδεόμενος με ένα BOOTP εξυπηρετητή (server) λαμβάνει από αυτόν τις αναγκαίες IP παραμέτρους. Το BOOTP χρησιμοποιήθηκε για να αντιστοιχεί IP διευθύνσεις σε διευθύνσεις επιπέδου σύνδεσης (link layer addresses). Ενώ δεν προσφέρει αυτό που λέμε πραγματικό plug & play.

Ένα ακόμα βήμα προς τα εκεί έγινε με το πρωτόκολλο DHCP (Dynamic Host Configuration Protocol). Το DHCP χτίστηκε πάνω στο BOOTP και χρησιμοποιεί κι εκείνο μοντέλο πελάτη / εξυπηρετητή (client / server). Κι εδώ ο host μπορεί να ζητήσει από ένα DHCP server τις πληροφορίες παραμετροποίησης. Ωστόσο, το DHCP προσφέρει μεγαλύτερη ευελιξία, τόσο για το είδος των πληροφοριών παραμετροποίησης, όσο και για τον τρόπο που θα εκχωρηθούν οι IP διευθύνσεις. Υπάρχουν τρεις μηχανισμοί για εκχώρηση διευθύνσεων:

• Αυτόματη εκχώρηση (automatic allocation), όπου ο host ζητάει μια IP διεύθυνση και του δίνεται μια μόνιμη, που θα χρησιμοποιεί κάθε φορά που θα συνδέεται.

• Προκαθορισμένη εκχώρηση (manual allocation), όπου ο server δίνει συγκεκριμένη IP σε κάθε host, σύμφωνα με μια λίστα που παρέχει ο διαχειριστής του δικτύου. Αυτές οι IP διευθύνσεις δεσμεύονται, ανεξάρτητα από το αν ο κάθε host τις χρησιμοποιεί.

• Δυναμική εκχώρηση (dynamic allocation), όπου ο server μοιράζει διευθύνσεις σε όποιον host προλάβει να τις ζητήσει. Οι host έχουν δικαίωμα να χρησιμοποιούν αυτές τις διευθύνσεις για ένα συγκεκριμένο χρονικό διάστημα, μετά από το οποίο λήγουν.

Τόσο ή αυτόματη όσο και η προκαθορισμένη εκχώρηση, έχουν ως αποτέλεσμα οι διευθύνσεις να δεσμεύονται από τους hosts ες αεί. Αυτό είναι κακό, διότι οι host που μπορεί να συνδέεται σπάνια θα δεσμεύουν άδικα διευθύνσεις. Ενώ η δυναμική εκχώρηση επιτρέπει σε ένα σχετικά μεγάλο πλήθος hosts να μοιράζονται ένα σχετικά μικρό αριθμό IP διευθύνσεων.

Δυστυχώς ούτε το DHCP επιτυγχάνει να δώσει μια πραγματικά αυτοματοποιημένη λύση. Κι αυτό γιατί ο DHCP server πρέπει να έχει καθοριστεί ρητά ώστε να περιέχει πληροφορίες για τους hosts, ενώ κάθε host πρέπει να γνωρίζει ποιος είναι ο κοντινότερος DHCP server. Το πραγματικό plug & play, το οποίο είναι προϋπόθεση για τη μεταφερσιμότητα (portability), δεν υποστηρίζεται από το IPv4. Κι αυτός είναι ένας ακόμα λόγος για την αναβάθμιση σε IPv6.

4.6 Type of Service (TOS)

Το IP χρησιμοποιεί μεταγωγή αυτόνομου πακέτου. Αυτό σημαίνει ότι ένα πακέτο μπορεί να πάρει ένα πλήθος από διαφορετικές διαδρομές για να φτάσει στον προορισμό του. Αυτές οι διαδρομές διαφέρουν ως προς το κόστος, την καθυστέρηση, το εύρος ζώνης και την αξιοπιστία τους. Το IPv4 έχει στην επικεφαλίδα το πεδίο τύπου υπηρεσίας (Type of Service) που επιτρέπει στις εφαρμογές να λένε στο IP πώς να χειριστεί τη ροή δεδομένων τους. Π.χ. μια εφαρμογή που απαιτεί μεγάλο throughput, όπως το FTP, μπορεί να αναγκάσει τη ροή δεδομένων του να περάσει από συνδέσεις με υψηλό εύρος ζώνης. Ενώ μια εφαρμογή που απαιτεί μικρούς χρόνους απόκρισης, όπως είναι τα δικτυακά παιχνίδια πραγματικού χρόνου, μπορεί να το δηλώσει στο TOS, ώστε να ευνοήσει την επιλογή διαδρομών με μικρή καθυστέρηση.

Το TOS ήταν μια πραγματικά καλή ιδέα, που όμως δεν λειτούργησε τόσο καλά στην εφαρμογή της. Απ' τη μια, τα πρωτόκολλα δρομολόγησης πρέπει να λαμβάνουν υπόψη το TOS και απ' την άλλη να κρατάνε πληροφορίες σε σχέση με το κόστος, την καθυστέρηση, το εύρος ζώνης και την αξιοπιστία των διαδρομών. Απ' την άλλη οι σχεδιαστές των εφαρμογών πρέπει να τις σχεδιάσουν έτσι ώστε να χρησιμοποιούν το TOS. Εν τέλει το Type of Service είναι η επιλογή ενός μόνο από τα επιθυμητά χαρακτηριστικά της διαδρομής. Π.χ. μπορείς να δηλώσεις ότι θέλεις ταχύτητα, αλλά όχι ταχύτητα και αξιοπιστία κ.ο.κ.

4.7 IP Options

Η επικεφαλίδα του IPv4 περιλαμβάνει ένα μεταβλητού μήκους πεδίο προαιρετικών επιλογών. Οι επιλογές αυτές μπορεί να χρησιμοποιούνται στη δρομολόγηση, όσο και στην ασφάλεια του πακέτου. Το πρόβλημα τώρα είναι ότι αυτές οι επιλογές είναι ειδικές περιπτώσεις. Τα IP πακέτα χωρίς προαιρετικές επιλογές είναι η συντριπτική πλειοψηφία και είναι το είδος των πακέτων για τα οποία έχουν καλή απόδοση οι δρομολογητές. Η επικεφαλίδα χωρίς προαιρετικές επιλογές έχει πάντα μήκος πέντε λέξεων των 32 bits και άρα είναι πιο εύκολο να επεξεργαστεί. Μην ξεχνάμε ακόμα πως η ταχύτητα είναι το κλειδί για τις πωλήσεις δρομολογητών. Γι ' αυτό οι κατασκευαστές δρομολογητών φτιάχνουν τα μηχανήματά τους έτσι ώστε να αντιμετωπίζουν τις προαιρετικές επιλογές της επικεφαλίδας IP ως εξαιρέσεις. Κάνοντάς τις στην άκρη για να τις επεξεργαστούν όποτε είναι πιο βολικό, κρατώντας τη γενικότερή τους απόδοση σε υψηλά επίπεδα.

Παρά τα οφέλη της χρήσης προαιρετικών πεδίων στην επικεφαλίδα του IPv4, το μειονέκτημά τους ως προς την απόδοση περιορίζει πολύ τη χρήση τους.

4.8 IPv4 Security

Η ασφάλεια, με την έννοια της απόκρυψης των μεταδιδόμενων δεδομένων, παλιότερα χειριζόταν από τα ανώτερα επίπεδα από αυτό του δικτύου. Όπως για παράδειγμα το πρωτόκολλο SSL (Secure Socket Layer) που ανήκει στο επίπεδο μεταφοράς. Πιο πρόσφατα η ασφάλεια κατέβηκε και στο επίπεδο δικτύου με την εμφάνιση του VPN (Virtual Private Network). Τα προϊόντα που χρησιμοποιούν VPN βασίζονται στη χρήση ενός μηχανισμού που ονομάζεται tunneling. Σύμφωνα με αυτό το μηχανισμό το IP πακέτο περιτυλίγεται μέσα σε ένα άλλο IP πακέτο με διαφορετικές πληροφορίες διαδρομής. Δηλαδή το αρχικό IP πακέτο γίνεται το τμήμα δεδομένων του καινούριου πακέτου –μια τεχνική γνωστή και ως encapsulation. Συνηθίζεται επίσης να κρυπτογραφείται το αρχικό IP πακέτο πριν τη διαδικασία του tunneling.

Το τμήμα IPsec (IP security) της IETF δουλεύει πάνω στην εξεύρεση μηχανισμών ασφαλείας τόσο για το IPv4 όσο και για το IPv6. Αν και είδη υπάρχουν τέτοιοι μηχανισμοί για το IPv4 μέσω των προαιρετικών πεδίων της επικεφαλίδας, στην πράξη δεν υπήρξαν ιδιαίτερα επιτυχείς. Η IPsec σκοπεύει να υλοποιήσει την ασφάλεια καλύτερα στο IPv6.

4.9 Συμπέρασμα

Είναι φανερό πια ότι η εξάντληση των διευθύνσεων δεν είναι το μοναδικό πρόβλημα του IPv4. Αυτό που δεν είναι ίσως απόλυτα φανερό είναι το γιατί να είναι απαραίτητη μια τόσο ακραία λύση, όπως η αντικατάσταση του με το IPv6. Μια άλλη λύση θα ήταν, για παράδειγμα, να μεγαλώσει η διεύθυνση του IPv4 και να αφεθεί το πρωτόκολλο κατά τα άλλα ως έχει. Αυτό θα σήμαινε ότι οι στοίβες του TCP/IP έπρεπε να ενημερωθούν όλες την ίδια στιγμή. Τελικά το κόστος μιας τέτοιας απλής αλλαγής θα ήταν συγκρίσιμο με αυτό της ολοκληρωτικής αντικατάστασης του με το IPv6. Οπότε είναι προτιμότερο να γίνει η μετάβαση και να υπάρχει ένα καινούριο και καλύτερο πρωτόκολλο δικτύου όπως το IPv6.

Μιλώντας για τη μετάβαση πρέπει να γίνει σαφές ότι αυτή δεν μπορεί να γίνει σε μια στιγμή. Αντίθετα θα διανυθεί μια μεταβατική περίοδος όπου το IPv6 θα συνυπάρχει με το IPv4.

5.1 Διαδικασίες μετάβασης στο IPv6

Για να δουλέψει το IPv6, δεν χρειάζεται να αναβαθμιστούν όλα τα interfaces που είναι συνδεδεμένα στο δίκτυο την ίδια στιγμή. Φυσικά κάτι τέτοιο δεν είναι εφικτό ούτως ή άλλως, λόγω του μεγέθους και των πολλών ειδικών περιπτώσεων του προβλήματος. Οι άνθρωποι που εργάζονται πάνω στη μετάβαση στο IPv6 έχουν εφεύρει μηχανισμούς για να γίνει αυτή σταδιακά και με μικρό κόστος. Η αναβάθμιση των είδη υπαρχόντων δικτύων σε δίκτυα IPv6

μπορεί να γίνει με σχετικά μικρές επιπτώσεις, εφόσον χρησιμοποιηθεί μεθοδικότητα και ακολουθηθούν έξυπνες λύσεις. Παρακάτω περιγράφονται μερικοί από τους μηχανισμούς που θα οδηγήσουν σε μια ομαλή μετάβαση στο IPv6.

Εκτός από το γεγονός ότι η μετάβαση στο IPv6 θα γίνει σταδιακά, θα γίνει επίσης και σχετικά αργά, καθώς λίγοι θα είναι αρχικά οι “τολμηροί” χρήστες που θα έχουν μεγάλη ανάγκη από τις λύσεις που προσφέρει το IPv6. Γιατί είναι γνωστό πως κάθε τι καινούριο ενδέχεται να έχει bugs και γενικότερα προβλήματα. Τα πράγματα θα αλλάζουν σιγά-σιγά καθώς οι σχεδιαστές υλικού και λογισμικού θα αποκτούν πείρα πάνω στο IPv6 και θα προσφέρουν ολοκληρωμένες και bug-free λύσεις για IPv6. Αναμένεται, δηλαδή, ότι το IPv6 θα συνυπάρχει με το IPv4 για πολύ καιρό –ίσως και για πάντα.

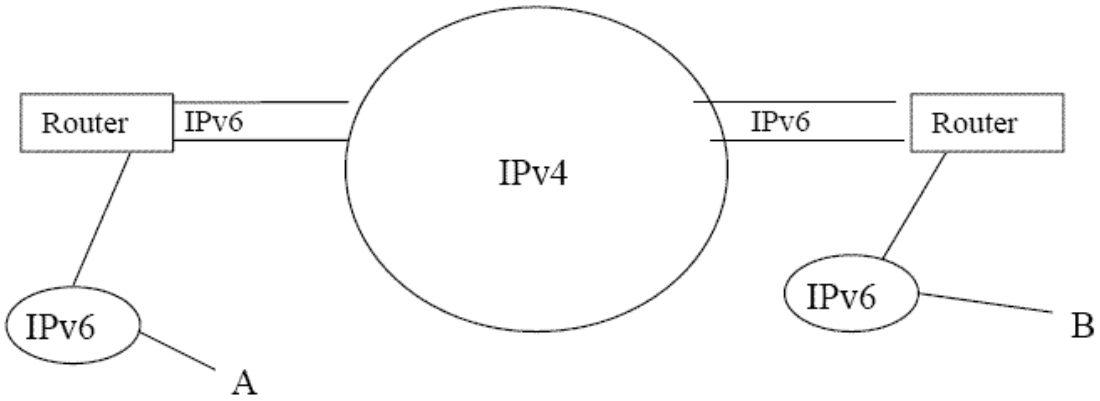
Οι περισσότερες στρατηγικές για τη μετάβαση βασίζονται σε μια προσέγγιση δύο κατευθύνσεων. Η μια χρησιμοποιεί protocol tunneling, όπου τα IPv6 πακέτα ενθυλακώνονται μέσα σε IPv4 πακέτα για τη μετακίνηση τους μεταξύ απομονωμένων IPv6 δικτύων διαμέσου του IPv4 διαδικτύου. Ακόμα και στα προχωρημένα στάδια της μετάβασης, η ενθυλάκωση (encapsulation) του IPv6 θα συνεχίσει να είναι χρήσιμη για να προσφέρει σύνδεση διαμέσου των εναπομεινάντων IPv4-only backbones. Η άλλη κατεύθυνση της στρατηγικής είναι η προσέγγιση διπλής στοίβας (dual stack), όπου οι hosts και οι routers θα τρέχουν και IPv4 και IPv6 στοίβες πάνω στα ίδια network interfaces. Με αυτόν τον τρόπο, ένας κόμβος διπλής στοίβας θα μπορεί να δέχεται και να μεταδίδει IPv4 και IPv6 πακέτα, ώστε τα δυο πρωτόκολλα να συνυπάρχουν πάνω στο ίδιο δίκτυο.

5.2 Η προσέγγιση του IPv6 Protocol Tunneling

Αυτή η προσέγγιση [16] είναι χρήσιμη για τη σύνδεση απομονωμένων IPv6 νησιών μέσα σε ένα IPv4 ωκεανό, όπως φαίνεται στο Σχήμα 18. Το tunneling απαιτεί να υπάρχει ένας κόμβος IPv6, που να μπορεί να μεταδώσει IPv4 πακέτα (κόμβος διπλής στοίβας) σε κάθε μια από τις δυο άκρες του tunnel. Η ενθυλάκωση ενός IPv6 πακέτου μέσα σε ένα IPv4 πακέτο βασικά λειτουργεί όπως η ενθυλάκωση πρωτοκόλλου (protocol encapsulation). Ο κόμβος στην μια άκρη του tunnel παίρνει το IPv6 πακέτο και το μεταχειρίζεται ως τμήμα εδομένων ενός IPv4 πακέτου, που πρέπει να φτάσει στον κόμβο που βρίσκεται στην άλλη άκρη του tunnel. Το αποτέλεσμα είναι μια ροή από IPv4 πακέτα, που περιέχουν IPv6 πακέτα.

Όπως φαίνεται στο Σχήμα 18, ο κόμβος Α και ο κόμβος Β είναι IPv6 κόμβοι. Για να πάει ένα πακέτο από τον Α στον Β, ο κόμβος Α απλά τοποθετεί στο πεδίο διεύθυνσης προορισμού του πακέτου την IPv6 διεύθυνση του κόμβου Β. Κατόπιν το πακέτο πηγαίνει στον δρομολογητή Χ, που ενθυλακώνει το IPv6 πακέτο που προορίζεται για τον κόμβο Β και το στέλνει στην IPv4 διεύθυνση του δρομολογητή Υ. Ο δρομολογητής Υ λαμβάνει το IPv4 πακέτο και το ξετυλίγει.

Έτσι ανακτά το αρχικό IPv6 πακέτο το οποίο προωθεί κατάλληλα στον κόμβο B.



Σχήμα 18 Διασύνδεση απομονωμένων IPv6 δικτύων διαμέσου ενός IPv4 διαδικτύου με τη βοήθεια ενός tunnel που έχει στις άκρες του διπλής στοίβας δρομολογητές IPv4/IPv6

5.3 IPv4-compatible IPv6 διευθύνσεις

Υπάρχει μία κατηγορία IPv6 διευθύνσεων που περιέχουν IPv4 διευθύνσεις. Διακρίνουμε δύο είδη μεταξύ αυτών. Τις IPv4-compatible και τις IPv4-mapped διευθύνσεις. Οι IPv4-compatible διευθύνσεις είναι απλά διευθύνσεις των 128 bit από τα οποία τα ψηλότερα 96 είναι μηδέν και τα χαμηλότερα 32 περιέχουν μια IPv4 διεύθυνση. Οι διευθύνσεις αυτές χρησιμοποιούνται από κόμβους διπλής στοίβας ικανούς να κάνουν αυτόματο tunneling IPv6 πακέτων μέσα από IPv4 δίκτυα.

Ο κόμβος διπλής στοίβας θα λέγαμε τότε ότι χρησιμοποιεί την “ίδια” διεύθυνση τόσο για IPv4 όσο και για IPv6 πακέτα. Οι IPv4 κόμβοι μπορούν να στέλνουν πακέτα στον κόμβο διπλής στοίβας χρησιμοποιώντας την IPv4 διεύθυνσή του, ενώ οι IPv6 κόμβοι μπορούν να στέλνουν πακέτα στην IPv6 διεύθυνση (που ουσιαστικά είναι η IPv4 διεύθυνση συμπληρωμένη με μηδενικά από αριστερά ώστε να έχει μήκος 128 bits).

Γενικά αυτό το είδος του κόμβου θα είναι ένας δρομολογητής που θα συνδέει IPv6 δίκτυα με αυτόματο tunneling διαμέσου IPv4 δικτύων. Ο δρομολογητής αυτός δέχεται IPv6 πακέτα από το τοπικό του IPv6 δίκτυο και θα τα ενθυλακώνει σε IPv4 πακέτα που προορίζονται για ένα άλλο κόμβο διπλής στοίβας, που επίσης θα χρησιμοποιεί IPv4-compatible διεύθυνση, και βρίσκεται κάπου στην άλλη άκρη του IPv4 διαδικτύου. Ο κόμβος αυτό θα ξετυλίγει τα πακέτα, όπως περιγράψαμε και προηγουμένως, και θα τα στέλνει στον IPv6 προορισμό τους.

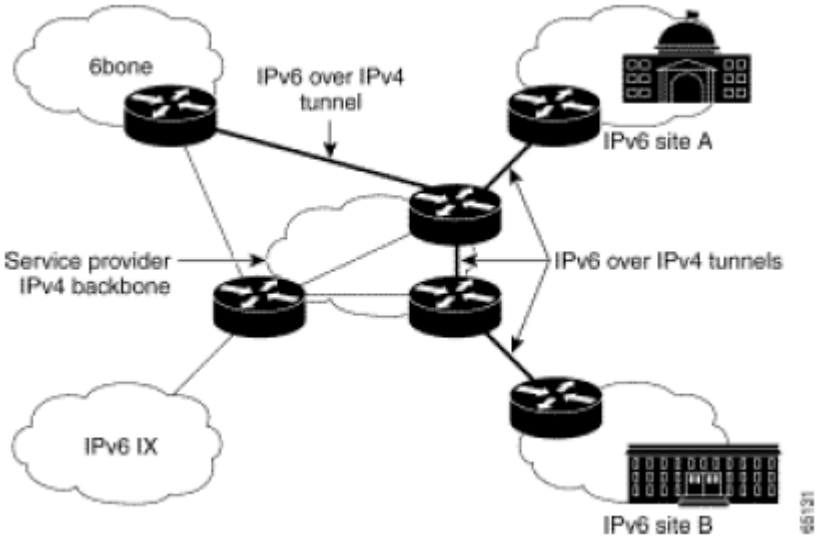
5.4 Configured Tunneling και Αυτόματο Tunneling

Η διαφορά μεταξύ configured και αυτόματου tunneling έγκειται κυρίως στο γεγονός ότι το αυτόματο tunneling χρησιμοποιεί δρομολογητές διπλής στοίβας με IPv4- compatible διευθύνσεις στις άκρες του tunnel. Τα αυτόματα tunnels δεν χρειάζονται παραμετροποίηση για να δουλέψουν οι IPv4 διευθύνσεις των δρομολογητών διπλής στοίβας. Αντίθετα στο configured tunneling οι IPv4 διευθύνσεις των κόμβων διπλής στοίβας πρέπει να παρέχονται μέσω κάποιου μηχανισμού (για παράδειγμα, μέσω DHCP ή μέσω των διαχειριστών του δικτύου).

5.5 Configured Tunnels

Με τον όρο Configured Tunnel εννοείται το tunnel στο οποίο σε κάθε άκρο ορίζεται ρητά η IPv4 διεύθυνση του απέναντι άκρου. Η τεχνική της διασύνδεσης IPv6 νησίδων πάνω από το IPv4 δίκτυο με την χρήση configured tunnels είναι ο τρόπος που καταρχήν χρησιμοποιήθηκε για την δημιουργία των IPv6 δικτύων. Η τεχνική αυτή στηρίχτηκε στις τεχνικές tunneling που ήδη υπήρχαν και είναι ευρέως γνωστές. Για το λόγο αυτό παρακάτω ακολουθεί μια αρκετά σύντομη περιγραφή της λειτουργίας της.

Τα IPv6 πακέτα προκειμένου να διασχίσουν το IPv4 δίκτυο ενθυλακώνονται σε IPv4 πακέτα των οποίων το πεδίο Identification έχει την τιμή 41, τιμή η οποία χρησιμοποιείται για να δηλώσει ότι το IPv4 πακέτο περιέχει ένα άλλο IPv6. Εννοείται πως το δίκτυο που διασχίζουν τα IPv6 πακέτα πρέπει να επιτρέπει την διέλευση των IPv4 πακέτων με τιμή 41 στο αντίστοιχο πεδίο.
Η διεύθυνση προορισμού των IPv4 πακέτων είναι αυτή που ρητά έχει δηλωθεί κατά την δημιουργία του tunneling interface στον δρομολογητή (tunnel destination) ενώ αντίστοιχα η διεύθυνση αποστολέα είναι η IPv4 διεύθυνση του interface. Με αυτόν τον τρόπο οι δρομολογητές χτίζουν point-to-point links πάνω από την IPv4 υποδομή και τα οποία χρησιμοποιούν για την μεταφορά των IPv6 πακέτων. Πάνω από τα tunneling interface οι δρομολογητές μπορούν και τρέχουν διάφορα IPv6-enabled routing πρωτόκολλα Μία κλασική περίπτωση εφαρμογής της συγκεκριμένης τεχνικής παρουσιάζεται στο Σχήμα 19.



Σχήμα 19 Εφαρμογή των configured tunnels

Η χρησιμότητα της συγκεκριμένης τεχνικής είναι πολύ μεγάλη καθώς επιτρέπει την παράλληλη ανάπτυξη του IPv6 δικτύου χωρίς να απαιτεί την δαπάνη κονδυλίων για την χρήση ξεχωριστών φυσικών διασυνδέσεων.

5.6 Automatic Tunnels

Η Τεχνική Automatic Tunneling κάνει χρήση των IPv4 συμβατών (compatible) IPv6 διευθύνσεων. Από τον τρόπο που είναι δομημένες οι διευθύνσεις αυτές, ο σταθμός μπορεί εύκολα να καταλάβει ποιο είναι το άλλο άκρο του tunnel που πρόκειται να δημιουργήσει, για να επικοινωνήσει με τον απέναντι IPv6 σταθμό. Έτσι για να εφαρμοστεί η συγκεκριμένη τεχνική χρειάζεται μόνο να εγκατασταθεί στους σταθμούς των χρηστών το κατάλληλο λογισμικό, το οποίο να εφαρμόζει την τεχνική αυτή.

Το συγκεκριμένο λογισμικό δεν είναι τίποτα άλλο παρά ένα pseudo-interface, το οποίο αναλαμβάνει να κάνει την ενθυλάκωση των IPv6 πακέτων μέσα σε IPv4 και την προώθηση τους πάνω από το IPv4 interface. α IPv4 πακέτα έχουν type code 41, διεύθυνση προορισμού την IPv4 διεύθυνση που είναι κωδικοποιημένη μέσα στο IPv6 πακέτο και ως πηγαία (source) διεύθυνση την IPv4 διεύθυνση του σταθμού - αποστολέα. Εννοείται πως οι σταθμοί που χρησιμοποιούν αυτήν την τεχνική πρέπει να έχουν ενεργοποιημένες και τις δύο stack των πρωτοκόλλων.

Προκειμένου να λειτουργήσει ο μηχανισμός αυτός, πρέπει οι IPv4 διευθύνσεις των σταθμών να είναι globally routable, δηλαδή αποκλείονται private διευθύνσεις.

Συνήθως η τεχνική των αυτόματων tunnels χρησιμοποιείται σε συνδυασμό με κάποιο configured tunnel, προκειμένου ο IPv6 σταθμός να είναι ικανός να επικοινωνήσει με το σύνολο των IPv6 σταθμών (δηλαδή των native IPv6 σταθμών και των σταθμών που χρησιμοποιούν 6to4 τεχνική) και όχι μόνο με όσους χρησιμοποιούν automatic tunneling.

Έτσι οι σταθμοί χρησιμοποιώντας automatic tunnels, επικοινωνούν με ανάλογους σταθμούς. Επίσης με την χρήση κάποιου configured tunnel, προωθούν πακέτα που έχουν σαν IPv6 διεύθυνση προορισμού κάποια, που ανήκει στο σύνολο των native διευθύνσεων, προς ένα router, ο οποίος έχει σε κάποιο από τα interfaces του IPv4- compatible IPv6 διεύθυνση. Επισημαίνεται πως configured tunnel ονομάζεται εκείνο, που η IP του άλλου endpoint παρέχεται από configuration πληροφορία και μπορεί να χρησιμοποιεί οποιουδήποτε τύπου IPv6 διευθύνσεις, native, IPv4-compatible. Ο router ο οποίος χρησιμοποιείται ως tunnel endpoint στην συγκεκριμένη περίπτωση, πρέπει να έχει σύνδεση με το native IPv6 δίκτυο.

Η αντίστροφη φορά της επικοινωνίας επιτυγχάνεται ως εξής: Ο native IPv6 host πρέπει, αφού διαπιστώσει πως η source διεύθυνση ανήκει στην κλάση των IPv4- compatible διευθύνσεων, να προωθήσει τα πακέτα (destination address IPv4 compatible) προς ένα router, ο οποίος μπορεί να εφαρμόσει την τεχνική automatic tunneling.

Γενικά θεωρείται σαν αρχή να αποφεύγεται η εισροή των IPv4 routing entries στο IPv6 Backbone. Υπάρχουν όμως περιπτώσεις, στις οποίες αυτό είναι αναπόφευκτο. Μια από αυτές είναι για παράδειγμα η περίπτωση που η τεχνική automatic tunneling χρησιμοποιείται στο τμήμα μεταξύ του router και ενός host, ο οποίος έχει IPv4- compatible διεύθυνση.

Ας θεωρήσουμε την περίπτωση όπου ο source host A έχει native IPv6 διεύθυνση και έχει σύνδεση με κάποιο τοπικό IPv6 enable router, ενώ ο destination host B δεν έχει πρόσβαση σε κανένα router συνδεδεμένο στο 6bone και χρησιμοποιεί IPv4- compatible IPv6 διευθύνσεις. Παρατηρούμε πως ο μόνος τρόπος για να επιτευχθεί η επικοινωνία A→B, είναι μέσω ενός router, ο οποίος έχει σύνδεση στο IPv6 δίκτυο και ταυτόχρονα εκτελεί automatic tunneling. Έτσι επιτυγχάνεται επικοινωνία χρησιμοποιώντας IPv6 routing μέχρι τον router και Router-to-Host automatic tunnel. Όμως προκειμένου τα πακέτα που προορίζονται για το σταθμό B (και γενικά για σταθμούς με IPv4-compatible διευθύνσεις) να προωθούνται μέχρι τον συγκεκριμένο router, πρέπει να διαφημίζει μέσα στην IPv6 routing υποδομή, το τμήμα των IPv4- compatible διευθύνσεων που μπορεί να εξυπηρετήσει. Σε αυτή την περίπτωση έχουμε εισροή των IPv4 routing entries στο IPv6 δίκτυο.

Γενικά οι συστάσεις είναι: Όπου δεν μπορεί να αποφεύγεται η συγκεκριμένη τακτική, να εφαρμόζεται με πολύ προσοχή και πιο συγκεκριμένα να φιλτράρονται οι IPv4 routing entries, έτσι ώστε να “διαρρέουν” μόνο αυτές που οδηγούν σε IPv6 –capable δίκτυα.

Συνοψίζοντας, επειδή η συγκεκριμένη τεχνική tunneling επιτρέπει σε απομονωμένους σταθμούς να έχουν πρόσβαση στο IPv6 δίκτυο και ο τρόπος λειτουργίας της είναι αρκετά απλός και ευέλικτος, μπορεί να συνδυαστεί με αρκετές άλλες τεχνικές προκειμένου να επιτευχθεί end-to-end επικοινωνία.

5.7 Τα είδη των IPv6 Tunnels

Υπάρχουν αρκετοί διαφορετικοί συνδυασμοί κόμβων που μπορεί να παίζουν το ρόλο των ακραίων σημείων ενός tunnel. Ως αποτέλεσμα υπάρχουν διαφορετικά είδη tunneling τα οποία έχουν ως εξής :

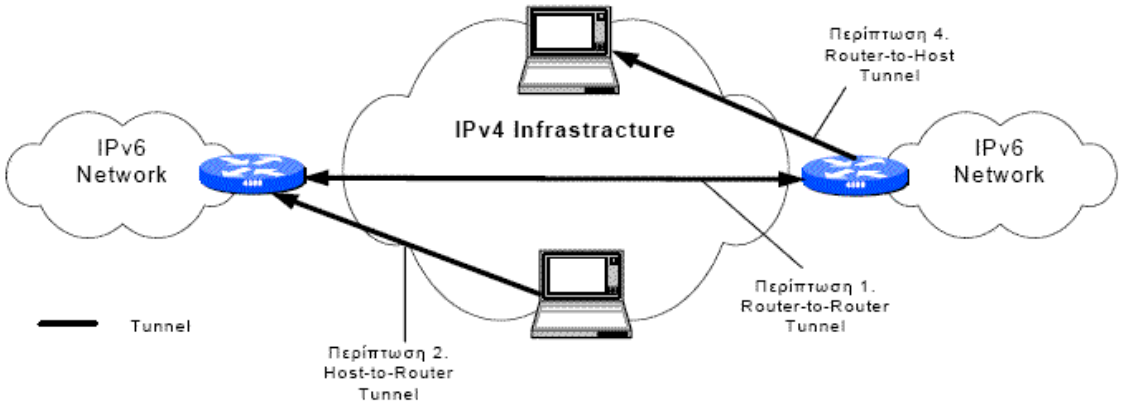
• **Router-to-router tunneling:** IPv4/IPv6 routers που συνδέονται μεταξύ τους μέσω μιας IPv4 δομής που κάνουν tunneling IPv6 πακέτων μεταξύ τους. Σ' αυτήν την περίπτωση το tunnel αντιστοιχεί σε ένα μεσαίο τμήμα της συνολικής διαδρομής του IPv6 πακέτου.

• **Host-to-router tunneling:** IPv4/IPv6 hosts που κάνουν tunneling IPv6 πακέτων προς ένα ενδιάμεσο IPv4/IPv6 router, στον οποίο έχουν πρόσβαση μέσω μιας IPv4 δομής. Σ' αυτήν την περίπτωση το tunnel αντιστοιχεί στο αρχικό τμήμα της συνολικής διαδρομής.

• **Host-to-host tunneling:** IPv4/IPv6 hosts που είναι συνδεδεμένοι μεταξύ τους μέσω μιας IPv4 δομής κάνουν tunneling IPv6 πακέτων μεταξύ τους. Σ' αυτήν την περίπτωση το tunnel αντιστοιχεί στη συνολική διαδρομή.

• **Router-to-host:** IPv4/IPv6 routers που κάνουν tunneling IPv6 πακέτων στον τελικό τους προορισμό, που είναι ένας IPv4/IPv6 host. Σ' αυτήν την περίπτωση το tunnel αντιστοιχεί στο τελικό τμήμα της συνολικής διαδρομής.

Οι παραπάνω περιπτώσεις απεικονίζονται στο Σχήμα 20.



Σχήμα 20 Περιπτώσεις εφαρμογής Tunnels

Στις δύο πρώτες από τις περιπτώσεις που αναφέρθηκαν παραπάνω (router-to router και host-to-router), το τέλος του tunnel είναι ένας router, ο οποίος είναι μεν ενδιάμεσος κόμβος και όχι ο τελικός προορισμός της

μεταδιδόμενης πληροφορίας. Η λειτουργία αυτού του κόμβου είναι απλώς να απενθυλακώσει τα IPv6 πακέτα και να τα προωθήσει προς τον τελικό προορισμό τους. Έτσι η IPv6 διεύθυνση των πακέτων που ενθυλακώνονται, δεν μπορεί να παρέχει καμιά πληροφορία σχετικά με την IPv4 διεύθυνση του τέλους του tunnel και συνεπώς αυτή η πληροφορία πρέπει να γίνει διαθέσιμη μέσω configuration. Τα tunnels που χρειάζονται απευθείας χειρωνακτικό ορισμό της διεύθυνσης τέλους τους ονομάζονται configured tunnels.

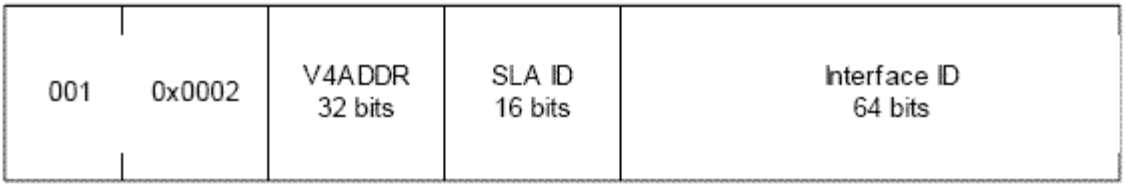
Αντίθετα στις δύο τελευταίες περιπτώσεις (host-to-host και router-to-host), τα IPv6 πακέτα ενθυλακώνονται προς έναν σταθμό, ο οποίος αποτελεί και τον τελικό αποδέκτη της μεταδιδόμενης πληροφορίας. Δηλαδή, τόσο η IPv6 διεύθυνση όσο και η IPv4 δείχνουν προς τον ίδιο σταθμό. Αυτό το γεγονός μπορεί να χρησιμοποιηθεί με την εφαρμογή κατάλληλων τεχνικών, έτσι ώστε η IPv4 διεύθυνση του τελικού σταθμού προορισμού να κωδικοποιείται μέσα στην IPv6 διεύθυνση του πακέτου. Αποτέλεσμα αυτού είναι, να μπορεί ο κόμβος που κάνει την ενθυλάκωση (δημιουργεί το tunnel) να καταλαβαίνει αυτόματα την IPv4 διεύθυνση του σταθμού προορισμού. Αυτό φυσικά έχει ως σημαντικό όφελος τη μείωση του διαχειριστικού κόστους, σε σχέση με αυτό που θα απαιτούνταν για τον άμεσο (χειρωνακτικό) ορισμό των tunnels.

5.8 Μηχανισμός μετάβασης 6to4

Ο μηχανισμός μετάβασης 6to4 [24] είναι μια τεχνική που μπορεί να χρησιμοποιηθεί για την επίτευξη connectivity μεταξύ IPv6-enabled hosts ακόμα και αν δεν υπάρχει IPv6 υποστήριξη στο δίκτυο που ανήκουν. Το γεγονός ότι δεν κάνει χρήση configured tunnels, δίνει μεγάλη ευελιξία στον τρόπο εφαρμογής, αφού το χαρακτηριστικό αυτό εξασφαλίζει ελάχιστο διαχειριστικό κόστος. Περιγράφεται στο RFC 3056.

Γενικά η τεχνική 6to4 χρησιμοποιεί και αυτή την IPv4 υποδομή, προκειμένου να επιτύχει τη διασύνδεση απομακρυσμένων IPv6 sites. Συγκεκριμένα, βλέπει το IPv4 δίκτυο σαν ένα unicast point to point link layer και χρησιμοποιώντας τεχνικές ενθυλάκωσης, υλοποιεί το IPv6 δίκτυο. Για τον μηχανισμό 6to4 έχει αποδοθεί από τις αρμόδιες αρχές διαχείρισης του IPv6 address space, ένα 13bit IPv6 top level Aggregator identifier (TLA) κάτω από το IPv6 prefix 001. Η δεκαεξαδική του αναπαράσταση είναι 0x0002 και συνεπώς το IPv6 prefix που έχει αποδοθεί είναι 2002::/16(hex).

Κάθε site που έχει τουλάχιστον μια routable IPv4 διεύθυνση, μπορεί να κάνει χρήση του μηχανισμού 6to4. Οι IPv6 διευθύνσεις που μπορεί να χρησιμοποιήσει, είναι αυτές που παράγονται από το IPv6 prefix 2002:V4ADDr::/48. Η μορφή των διευθύνσεων που χρησιμοποιούνται είναι αυτή που φαίνεται στο Σχήμα 21.

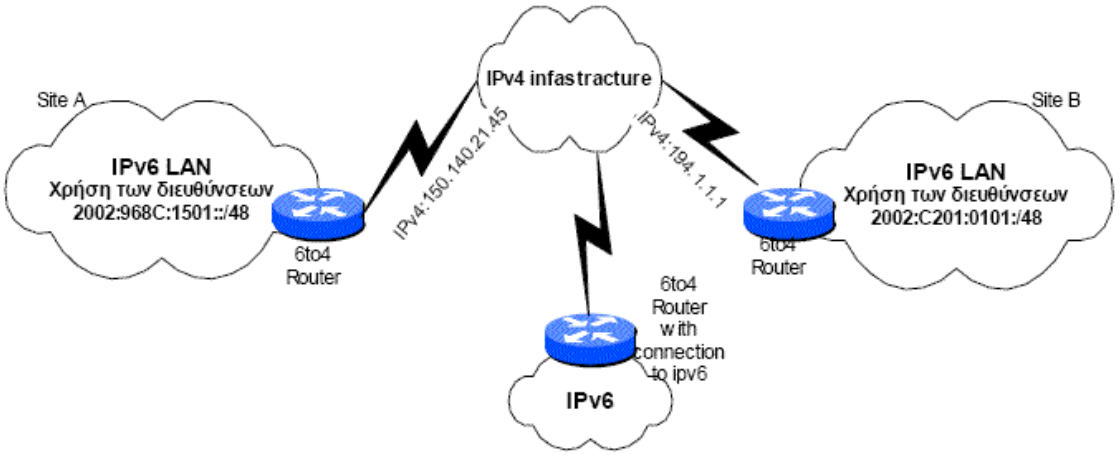


Σχήμα 21Δομή IPv6 διεύθυνσης που χρησιμοποιείται στην 6to4 τεχνική

Οι διευθύνσεις αυτές είναι κανονικές IPv6 διευθύνσεις (όχι της μορφής IPv4- compatible) και συνεπώς μπορούν να χρησιμοποιηθούν σε διαδικασίες auto configuration (stateless/state full), DHCP, κλπ. πό τα παραπάνω φαίνεται πως όλα τα sites που χρησιμοποιούν τον 6to4 μηχανισμό, δημιουργούν μια "κλάση" στο σύνολο των IPv6 διευθύνσεων, αυτών που η διεύθυνση τους αρχίζει με το prefix 2002::. ταν ένας σταθμός σε ένα 6to4 site θέλει να επικοινωνήσει με άλλον IPv6 σταθμό, εκτός του site για τον οποίον ξέρει ότι έχει διεύθυνση που ανήκει στην κλάση των 6to4 διευθύνσεων, τότε απλώς προωθεί τα IPv6 πακέτα προς εκείνο τον router/host που έχει το interface, το οποίο έχει την IPv4 που βγαίνει προς το Internet. Σε αυτό το interface είναι ορισμένο ένα 6to4 pseudo-interface, το οποίο και κάνει το encapsulation των IPv6 πακέτων μέσα σε IPv4 και τα προωθεί προς το αντίστοιχο IPv4 interface που εξυπηρετεί το απέναντι 6to4 site. Η IPv4 διεύθυνση του απέναντι interface είναι γνωστή, αφού είναι κωδικοποιημένη πάνω στην διεύθυνση προορισμού του IPv6 πακέτου. Έτσι δεν χρειάζεται ο άμεσος ορισμός της IP του απέναντι interface (automatic tunneling). Επίσης πρέπει να τονιστεί πως μεταξύ των 6to4 routers δεν απαιτείται να υπάρχει κάποιο IPv6 exterior routing πρωτόκολλο. Όλη η απαιτούμενη routing διαδικασία γίνεται από το IPv4.

Στο σημείο αυτό πρέπει να τονιστεί πως η σωστή λειτουργία του 6to4 μηχανισμού εξαρτάται από τον τρόπο, με βάση τον οποίο οι σταθμοί επιλέγουν ποια διεύθυνση θα χρησιμοποιήσουν, από αυτές που επιστρέφονται στο σταθμό από την DNS υπηρεσία.

Δηλαδή, έστω ένας σταθμός που έχει 6to4 διεύθυνση και ρωτάει για την IPv6 διεύθυνση ενός άλλου σταθμού. Εάν η υπηρεσία DNS του επιστρέψει δύο IPv6 διευθύνσεις που αντιστοιχούν σε δύο IPv6 interfaces, μία native και μια 6to4, είναι αναγκαίο ο σταθμός να χρησιμοποιήσει την 6to4 διεύθυνση στην προσπάθεια του να επικοινωνήσει με τον άλλο σταθμό. Στην περίπτωση που ο άλλος σταθμός έχει μόνο native IPv6 διεύθυνση, τότε η επικοινωνία μπορεί να επιτευχθεί μόνο με την χρήση ενός relay router δηλαδή ενός router που έχει connectivity και με το native IPv6 δίκτυο αλλά και με το 6to4. Ο τελευταίος τρόπος είναι και ο μοναδικός, με τον οποίο μπορεί να επιτευχθεί η επικοινωνία μεταξύ των 6to4 IPv6 δικτύων και αυτών που χρησιμοποιούν native IPv6 διευθύνσεις. Δηλαδή ο 6to4 router ενός site πρέπει να έχει μια τουλάχιστον σύνδεση με κάποιον router, ο οποίος να είναι 6to4 router, αλλά επιπλέον να διαθέτει και σύνδεση με το native IPv6 δίκτυο.



Σχήμα 22 Τυπική περίπτωση εφαρμογής 6to4 τεχνικής

Προκειμένου να γίνει πιο κατανοητή η λειτουργία και τα χαρακτηριστικά της συγκεκριμένης τεχνικής, παρουσιάζεται ένα σενάριο λειτουργίας στο Σχήμα 22. Στην περίπτωση που ένας σταθμός στο site A θέλει να επικοινωνήσει με κάποιον άλλον που βρίσκεται στο site B, τότε έχουμε μια τυπική περίπτωση 6to4 IPv6 επικοινωνίας όπως αυτή περιγράφηκε ανωτέρω. Στην περίπτωση που σταθμοί είτε από το site A είτε από το site B θέλουν να επικοινωνήσουν με IPv6 σταθμούς, που έχουν native IPv6 διευθύνσεις, τότε όπως προαναφέρθηκε πρέπει να διαμεσολαβήσει ένας IPv6 relay router, ο οποίος δεν είναι τίποτε άλλο παρά ένας IPv6 router, ο οποίος όμως έχει ορισμένο πάνω του ένα 6to4 pseudo-interface, σύνδεση με το IPv4 δίκτυο και τουλάχιστον ένα native IPv6 interface.

Στο παραπάνω σενάριο πρέπει να θεωρήσουμε τρία διαφορετικά routing domains:

1. Το εσωτερικό routing domain καθενός 6to4 site: Όπως προαναφέρθηκε, η δρομολόγηση εσωτερικά σε ένα 6to4 δίκτυο γίνεται με τους γνωστούς τρόπους, όταν πρόκειται για εσωτερικές IPv6 (6to4) διευθύνσεις και με χρήση κάποιου default ή έμμεσου route που να δείχνει προς τον 6to4 router του site.

2. Το εξωτερικό routing domain που διασυνδέει ένα σύνολο από border 6to4 routers και το οποίο περιλαμβάνει και τους 6to4 relay routers: Στην περίπτωση αυτή υπάρχουν δυο διαφορετικές επιλογές για να υλοποιηθεί το σχήμα δρομολόγησης:

ο Χωρίς την χρήση κάποιου IPv6 πρωτοκόλλου δρομολόγησης, αφού και τα πρωτόκολλα δρομολόγησης που τρέχουν για το IPv4 μπορούν να εξασφαλίσουν τη διασύνδεση μεταξύ των 6to4 sites.
ο Με χρήση κάποιου εξωτερικού IPv6 πρωτοκόλλου δρομολόγησης. Ένα σύνολο 6to4 routers, εάν έχουν διασύνδεση με κάποιον 6to4 router, από τον οποίον μπορούν να μαθαίνουν τα native IPv6 routes, μπορούν να τρέχουν μεταξύ τους κάποιο IPv6 capable routing πρωτόκολλο όπως το BGP4+.

Προϋπόθεση για το παραπάνω αποτελεί ο relay router να διαφημίζει τις απαραίτητες native IPv6 routes (IPv6 prefixes) πάνω στο 6to4 pseudointerface του. Ουσιαστικά με αυτόν τον τρόπο δηλώνει για ποιο κομμάτι του IPv6 δικτύου είναι διαθέσιμος ως relay router. Αν και αυτή η προσέγγιση είναι διαχειριστικά πιο πολύπλοκη, εντούτοις δίνει το πλεονέκτημα ότι παρέχει εργαλεία για τον έλεγχο της πολιτικής.

3. Το εξωτερικό IPv6 routing domain από κάθε IPv6 δίκτυο: Κάθε relay router πρέπει να διαφημίζει το 2002::/16 prefix πάνω στην native IPv6 διεύθυνση που διαθέτει. Είναι θέμα routing πολιτικής πόσο μακριά μέσα στο native IPv6 routing σύστημα θα φτάσει αυτή η διαφήμιση (advertisement). Δεδομένου ότι γενικά θα υπάρχουν πολλοί 6to4 relay routers, οι οποίοι θα διαφημίζουν το συγκεκριμένο prefix, είναι θέμα πολιτικής, ποιους θα επιλέγει κάθε native IPv6 site. Απαιτείται η εφαρμογή προσεκτικού filtering από τους διαχειριστές των δικτύων.
Πιο λεπτομερή 2002:: prefixes (π.χ. 2002::/48) δεν πρέπει να διαδίδονται μέσα στο IPv6 routing σχήμα, προκειμένου να μην μολύνεται αυτό από routing entries του IPv4 δικτύου και απαιτείται από τους διαχειριστές των δικτύων να φιλτράρουν και να απορρίπτουν τέτοια prefixes.

Γενικά ο μηχανισμός 6to4 παρέχει την δυνατότητα για άμεση σύνδεση στο IPv6 δίκτυο οποιουδήποτε το επιθυμεί χωρίς να υπάρχει αντίστοιχη υποστήριξη στο πρωτόκολλο από τον παροχέα (provider) του φορέα.
Το μεγάλο πλεονέκτημα που παρέχει είναι, ότι επιτρέπει την πρόοδο της διαδικασίας μετάβασης, χωρίς να απαιτείται η εγκατάλειψη άλλων μηχανισμών ή πρωτοκόλλων. Επιτρέπει το σταδιακό migration από IPv4 σε 6to4 και έπειτα σε native IPv6. Αυτό γίνεται ακολουθώντας τα παρακάτω βήματα:

1. Εφαρμογή του IPv6 εσωτερικά στο δίκτυο του φορέα ή στο σταθμό, αν πρόκειται για μεμονωμένο χρήστη. Η εφαρμογή οποιουδήποτε μηχανισμού είναι επιτρεπτή όπως native IPv6, 6over4 και tunnels.

2. Ρύθμιση ενός router, ο οποίος είναι συνδεμένος με το Internet, έτσι ώστε να υποστηρίζει 6to4. Το χαρακτηριστικό αυτό ήδη παρέχεται από τους περισσότερους κατασκευαστές δικτυακών συσκευών π.χ. Cisco. Ο συγκεκριμένος δρομολογητής πρέπει επίσης να διαφημίζει προς τα έξω το 2002::/16 prefix. Τέλος, πρέπει να ενημερωθούν οι DNS entries, έτσι ώστε να περιλαμβάνουν αυτό το prefix. Σ' αυτό το σημείο ο μηχανισμός 6to4 είναι ήδη διαθέσιμος και το site κάνει χρήση ενός 2002:IPv4ADDR::/48 prefix.

3. Εάν η διασύνδεση με το native IPv6 δίκτυο είναι επιθυμητή, τότε πρέπει το site/host να βρει έναν διαθέσιμο relay router, ο οποίος θα τον διασυνδέει με το native IPv6 δίκτυο. Ο relay router μπορεί να ανήκει είτε σε κάποιο άλλο συνεργαζόμενο 6to4 site είτε να προσφέρεται ως υπηρεσία από τον provider.

Όσον αφορά τα θέματα δρομολόγησης, εάν δεν χρησιμοποιείται κάποιο exterior routing πρωτόκολλο από το 6to4 site, τότε πρέπει να υπάρχει ένα default route που να δείχνει προς τον relay router. Εάν αντίθετα χρησιμοποιείται κάποιο exterior routing πρωτόκολλο, όπως BGP, τότε το site πρέπει να ρυθμιστεί έτσι ώστε να δημιουργήσει τα κατάλληλα BGP peerings με αυτόν.

4. Όταν κάποια στιγμή μία native IPv6 σύνδεση γίνει διαθέσιμη, τότε πρέπει να προστεθεί ένα δεύτερο (native) prefix στον 6to4 router, όπως επίσης να ενημερωθεί και ο DNS.

5. Όταν αργότερα διαπιστωθεί πως έχει ολοκληρωθεί η μετάβαση σε native IPv6, τότε μπορεί πολύ εύκολα να απομακρυνθεί το 6to4 configuration.

Σημαντικό πλεονέκτημα επίσης του 6to4 μηχανισμού αποτελεί το γεγονός ότι μπορεί να χρησιμοποιηθεί σε δίκτυα, τα οποία χρησιμοποιούν private IPv4 διευθύνσεις και μόνο μια routable. Επίσης δεν επηρεάζεται καθόλου από την παρουσία firewalls ή NAT boxes στο δίκτυο.

5.9 6over4

Η μέθοδος 6over4 έχει αναπτυχθεί με κύριο σκοπό να επιτρέψει σε κάποιον απομονωμένο σταθμό IPv6, ο οποίος βρίσκεται πάνω σε φυσικό σύνδεσμο (link) χωρίς την παροχή native IPv6 υποστήριξης, να γίνει ένας πλήρως λειτουργικός IPv6 σταθμός με πρόσβαση στο IPv6 δίκτυο. Ο μηχανισμός 6over4 περιγράφεται στο RFC 2529.

Ο μηχανισμός 6over4 κάνει χρήση του IPv4 multicast domain, το οποίο θεωρείται ως το link layer πάνω από το οποίο δομείται η IPv6 Stack. Προκειμένου να χρησιμοποιηθεί η 6over4 μέθοδος, πρέπει το IPv4 domain να υποστηρίζει multicast. Επίσης, εάν απαιτείται να υπάρχει σύνδεση με εξωτερικά sites (IPv6), πρέπει απαραίτητα να υπάρχει και κάποιος router που να εφαρμόζει την ίδια μέθοδο στο link που συνδέεται με το multicast domain. Η 6over4 μέθοδος είναι εφαρμόσιμη στα όρια του ίδιου site και εξαιτίας του γεγονότος ότι δεν χρησιμοποιεί IPv4-compatible IPv6 διευθύνσεις ή configured tunnels, παρέχει μεγάλη ανεξαρτησία, όσον αφορά την τεχνολογία των links που χρησιμοποιούνται αλλά και την τοπολογία του IPv6 δικτύου που επιχειρείται να εφαρμοστεί. Συχνά η μέθοδος 6over4 αναφέρεται και ως virtual Ethernet.

Ο τρόπος λειτουργίας της συγκεκριμένης τεχνικής είναι σχετικά απλός: Για κάθε IPv6 LAN ορίζεται ένα multicast session, το οποίο “ακούν” τόσο οι hosts που συμμετέχουν στο IPv6 subnet, όσο και ο router που δρομολογεί την κίνηση του προς τα έξω (λειτουργίες IPv6 neighbour/router discovery). Απαραίτητη προϋπόθεση και πάλι αποτελεί ο router να έχει υλοποιημένες και τις δύο stack στο interface που εξυπηρετεί το virtual LAN.

Προκειμένου οι hosts που χρησιμοποιούν την συγκεκριμένη τεχνική να μπορούν να υποστηρίξουν stateless auto configuration, έχει οριστεί ότι το συμπλήρωμα του prefix FE80:0000/64 (χρησιμοποιείται στην stateless auto

configuration διαδικασία) θα είναι η unicast IPv4 διεύθυνση του link, συμπληρωμένη (padded) από τα αριστερά με 32 bits, προκειμένου να συμπληρωθεί το σύνολο των 128 bits που αποτελούν την IPv6 διεύθυνση.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην τιμή TTL που δίνεται στα multicast IPv4 πακέτα που μεταφέρουν την IPv6 κίνηση, έτσι ώστε η τιμή του να είναι αρκετά μικρή προκειμένου να μην υπάρχουν διαρροές IPv6 κίνησης έξω από το Multicast domain.

5.10 Η Προσέγγιση IPv4 / IPv6 Διπλής Στοίβας

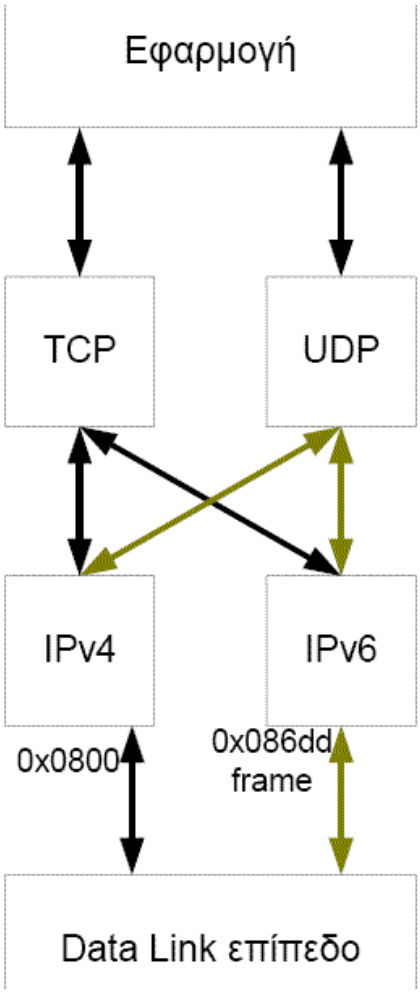
Αναμφισβήτητα το IPv4 θα είναι μαζί μας για πολύ καιρό ακόμα. Γιατί πάνω από όλα η αναβάθμιση σε IPv6 κοστίζει, τόσο σε καινούριο λογισμικό όσο και υλικό. Όλο αυτό τον καιρό τα αναβαθμισμένα συστήματα θα πρέπει να διατηρήσουν την επικοινωνία τους με τα IPv4 συστήματα. Αυτό θα επιτευχθεί με τη χρήση συστημάτων που υποστηρίζουν και τα δυο IP πρωτόκολλα (IPv6, IPv4). Η ιδέα της διπλής στοίβας δεν είναι καινούρια. Χρησιμοποιήθηκε και χρησιμοποιείται για τη διασύνδεση LAN, που τρέχουν παλιό δικτυακό λογισμικό της Novell (που υλοποιούσε το πρωτόκολλο δικτύου IPX), με το internet(TCP/IP). Η σύνδεση με το internet γίνεται μέσω της στοίβας TCP/IP, ενώ η σύνδεση με το δίκτυο Novell γίνεται μέσω της IPX στοίβας. Καθώς πακέτα λαμβάνονται στο επίπεδο σύνδεσης δεδομένων και ξετυλίγονται, οι επικεφαλίδες τους δηλώνουν αν το πακέτο προορίζεται για την TCP/IP στοίβα ή την IPX στοίβα –και το πακέτο επεξεργάζεται από την αντίστοιχη στοίβα.

5.11 Κόμβοι Διπλής Στοίβας

Οι κόμβοι διπλής στοίβας IPv4/IPv6 δουλεύουν περίπου με τον ίδιο τρόπο που δουλεύουν και άλλα είδη κόμβων πολλαπλής στοίβας. Καθώς πακέτα λαμβάνονται στο επίπεδου δικτύου από το επίπεδο σύνδεσης, ξετυλίγονται και εξετάζονται οι επικεφαλίδες τους. Αν το πεδίο έκδοσης (version) της επικεφαλίδας είναι τέσσερα, τότε το πακέτο επεξεργάζεται από την IPv4 στοίβα. Ενώ αν είναι έξι τότε επεξεργάζεται από την IPv6 στοίβα.

Ο μηχανισμός ουσιαστικά αναφέρεται στην ενεργοποίηση και των 2 πρωτοκόλλων στο δίκτυο και βασίζεται στη πολύ απλή ιδέα της ενεργοποίησης και των δύο stacks των πρωτοκόλλων στα δικτυακά interfaces του εξοπλισμού. Με τον τρόπο αυτό επιτυγχάνεται σχετικά απλά η επικοινωνία των κόμβων του δικτύου με άλλους, είτε αυτοί χρησιμοποιούν το IPv4 πρωτόκολλο είτε το IPv6 ή και τα δύο. Η επιλογή για το ποιο από τα δύο πρωτόκολλα θα χρησιμοποιήσει κάθε εφαρμογή εξαρτάται είτε από εσωτερική επιλογή (από τον κατασκευαστή

του λογισμικού) είτε από την απάντηση της υπηρεσίας ονοματολογίας του δικτύου (DNS).
Η λειτουργία του μηχανισμού φαίνεται παραστατικά στο Σχήμα 23.



Σχήμα 23 Κόμβος διπλής στοίβας

5.12 Προβλήματα –Απαιτούμενες διευκρινίσεις

Στην υλοποίηση της dual stack τεχνικής εισέρχονται κάποια θέματα και προβλήματα,τα οποία πρέπει να διευκρινιστούν προκειμένου να γίνει η εφαρμογή της αποδοτική.

Το πρώτο από αυτά είναι η Υπηρεσία Ονοματολογίας (DNS) και ο τρόπος με τον οποίο αυτή επηρεάζει την “προτίμηση” που θα έχουν οι dual stack σταθμοί προς το ένα ή το άλλο πρωτόκολλο. Επίσης σημαντική είναι η επίδραση της στην απόδοση του δικτύου.

Για την υλοποίηση της Υπηρεσίας Ονοματολογίας, έτσι ώστε να υποστηρίζει το IPv6, έχει εισαχθεί και οριστεί ένα νέο είδος record για την βάση

δεδομένων του DNS, το A6 record το οποίο αποτελεί συνέχεια / εξέλιξη του AAAA record. Έτσι προκειμένου ένας σταθμός να είναι ικανός να επικοινωνεί χρησιμοποιώντας και τα δύο πρωτόκολλα, πρέπει να διαθέτει τις απαιτούμενες βιβλιοθήκες, για να “ρωτάει” την Υπηρεσία Ονοματολογίας για την IP address σταθμών IPv4, IPv6 και IPv4/IPv6. Με άλλα λόγια, οι βιβλιοθήκες αυτές να είναι ικανές να χειρίζονται τα A records (IPv4) αλλά και τα AAAA/A6 records (IPv6).

Για να αποσαφηνιστεί περισσότερο η επίδραση της Υπηρεσίας Ονοματολογίας στην εφαρμογή τεχνικών Dual Stack, ας θεωρήσουμε την περίπτωση κατά την οποία ένας dual stack σταθμός “ρωτάει” την Υπηρεσία Ονοματολογίας για την IP διεύθυνση ενός σταθμού και βρίσκει ότι στο συγκεκριμένο όνομα αντιστοιχεί τόσο μια IPv4 address οσο κ μια IPv6. Σε αυτή την περίπτωση οι βιβλιοθήκες που διαθέτει ο σταθμός για το DNS έχουν τις εξής επιλογές ως προς την απάντηση που θα επιστρέψουν στην εφαρμογή:

1. Να επιστρέψουν μόνο την IPv4 διεύθυνση

2. Να επιστρέψουν μόνο την IPv6 διεύθυνση

3. Να επιστρέψουν και τις 2 διευθύνσεις διαταγμένες σε μία σειρά IPv4 – IPv6 ή Αντίστροφα

Σε κάθε περίπτωση η επιλογή που γίνεται από τις DNS βιβλιοθήκες καθορίζει και το πρωτόκολλο που θα χρησιμοποιηθεί. Η σύσταση που έχει γίνει προτείνει ότι η επιλογή αυτή πρέπει να γίνεται από τις εφαρμογές και όχι αυθαίρετα από τις βιβλιοθήκες resolve των σταθμών.
Για την Υπηρεσία Ονοματολογίας κατά την διάρκεια της μετάβασης από IPv4 σε IPv6, έχει γίνει η εξής σύσταση προκειμένου να αποφευχθούν διάφορα δυσάρεστα φαινόμενα:

Ένα AAAA/A6 record για ένα host θα πρέπει να καταχωρείται στη DNS database μόνο όταν και οι τρεις παρακάτω προτάσεις είναι αληθείς.

1. Η IPv6 διεύθυνση έχει αποδοθεί σε ένα interface του host

2. Η IPv6 διεύθυνση έχει γίνει configured στο interface του host

3.Το συγκεκριμένο interface έχει σύνδεση προς το IPv6 δίκτυο

Τα παραπάνω έχουν αντίστοιχη εφαρμογή κατά τα τελευταία στάδια της μετάβασης και πιο συγκεκριμένα για το πότε το record που αντιστοιχεί σε μια IPv4 διεύθυνση, η οποία έχει απενεργοποιηθεί από το Interface ενός σταθμού, αφαιρείται από την DNS βάση.

5.13 Dual Stack Transition Mechanism (DSTM)

Η Τεχνική Dual Stack Transition Mechanism (DSTM) [26] έχει αναπτυχθεί, προκειμένου να επιτρέψει την επικοινωνία μεταξύ των IPv6 σταθμών και των IPv4 only δικτύων που υπάρχουν σήμερα. Είναι μια εναλλακτική πρόταση στις τεχνικές μετάφρασης επικεφαλίδας.

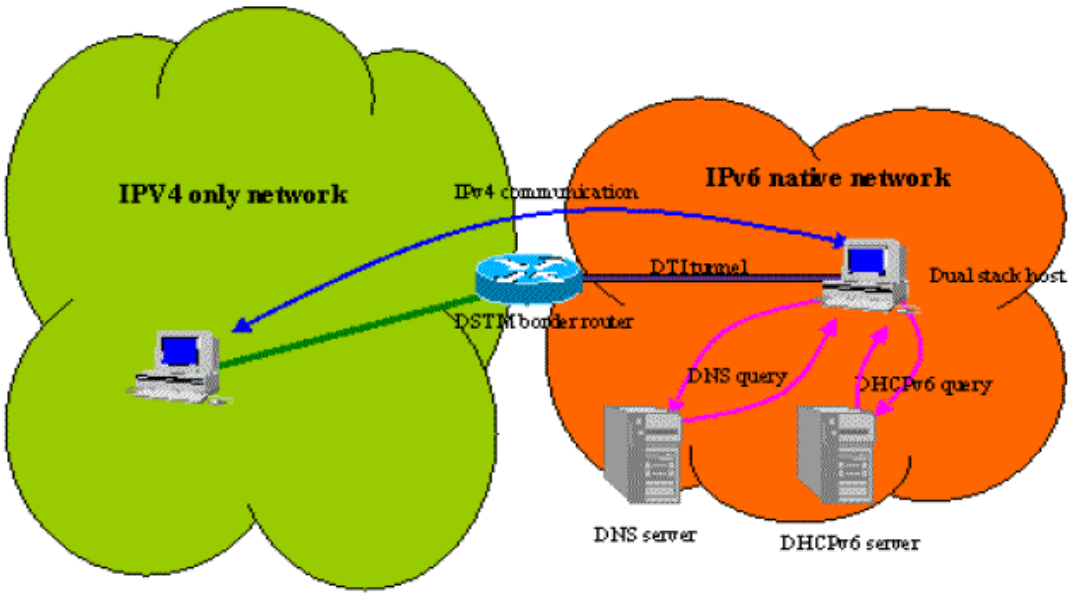
Ο DSTM ουσιαστικά αποτελεί ένα μηχανισμό, ο οποίος προκύπτει από το συνδυασμό τεχνικών απόδοσης IPv4 διευθύνσεων σε IPv6 hosts και Dynamic Tunneling Interfaces (DTI).

Η τεχνική DSTM βασίζεται στη χρήση ενός DHCPv6 server, ο οποίος αποδίδει προσωρινά global IPv4 διευθύνσεις στους IPv6 σταθμούς που θέλουν να επικοινωνήσουν με κάποιον IPv4 only σταθμό. Τα IPv4 πακέτα ενθυλακώνονται σε IPv6 μέσω ενός DTI interface και μεταφέρονται μέσα στο IPv6 δίκτυο μέχρι τον Border Router που το διασυνδέει με το IPv4 δίκτυο.

Η λειτουργία του μηχανισμού είναι δικατευθυντήρια (bi-directional), δηλαδή η αρχικοποίηση της επικοινωνίας μπορεί να γίνει είτε από την πλευρά του IPv6 host είτε από την πλευρά του IPv4. Αυτό αποτελεί και σημαντικό πλεονέκτημα της συγκεκριμένης μεθόδου σε σχέση με άλλες τεχνικές, οι οποίες επιτρέπουν την επικοινωνία των IPv6 σταθμών με το IPv4 δίκτυο και απαιτούν την αρχικοποίηση της επικοινωνίας μόνο από τον IPv6 host.
Ο τρόπος λειτουργίας της συγκεκριμένης τεχνικής επεξηγείται αναλυτικά στη συνέχεια για τις εξής δύο περιπτώσεις: **I)** η επικοινωνία αρχικοποιείται από τον IPv6 host και **II)** η επικοινωνία αρχικοποιείται από τον IPv4 host.

I. Στην πρώτη περίπτωση ο IPv6 σταθμός στέλνει IPv4 πακέτα στον απέναντι σταθμό μέσω του DTI interface, το οποίο υλοποιεί την ενθυλάκωση σε IPv6 πακέτα και στη συνέχεια τα προωθεί προς το άλλο άκρο του Tunneling interface (συνήθως είναι ένας DSTM router που βρίσκεται στα όρια του IPv6 δικτύου και του IPv4 κόσμου). Εκεί τα πακέτα απενθυλακώνονται και προωθούνται πλέον κανονικά προς τον IPv4 προορισμό τους. Με βάση τα ανωτέρω συμπεραίνεται ότι για να έχει αποτέλεσμα ο παραπάνω μηχανισμός, θα πρέπει ο border router, που εξυπηρετεί την επικοινωνία των δύο δικτύων IPv4 και IPv6, να διαφημίζει προς το IPv4 δίκτυο το τμήμα των IPv4 διευθύνσεων που χρησιμοποιούνται για προσωρινή απόδοση στους σταθμούς. Ένα ακόμη σημείο στο οποίο πρέπει να δοθεί προσοχή, είναι ο τρόπος που λειτουργεί η υπηρεσία DNS και οι βιβλιοθήκες resolve των clients, αφού η επιλογή της χρήσης της μεθόδου εξαρτάται από αυτό Αναλυτικότερα, στην αρχή ο IPv6 host ρωτάει την υπηρεσία DNS για ένα AAAA record για τον IPv4 host και προφανώς παίρνει ως απάντηση ένα μήνυμα λάθους. Στη συνέχεια ρωτάει την υπηρεσία για ένα A record, που αντιστοιχεί στην IP του και παίρνει ως απάντηση την διεύθυνση του σταθμού. Αφού πλέον καταλαβαίνει πως ο σταθμός είναι IPv4, ρωτάει τον DHCPv6 server για μια προσωρινή IPv4 διεύθυνση, προκειμένου να την χρησιμοποιήσει στην

επικοινωνία του με τον σταθμό. Το ανωτέρω σενάριο περιγράφεται στο Σχήμα 24.



Σχήμα 24 Λειτουργία μηχανισμού DSTM

II. Στην περίπτωση κατά την οποία η επικοινωνία αρχικοποιείται από την πλευρά του IPv4 host, λαμβάνει χώρα η εξής σειρά ενεργειών: Ο IPv4 σταθμός ρωτάει την υπηρεσία DNS για την IPv4 διεύθυνση του IPv6 σταθμού. Με την σειρά του ο DNS server ενημερώνει τον AIIH(Assignment of IPv4 global addresses to IPv6 Hosts) server ότι πρέπει να αποδώσει μια διεύθυνση στον IPv6 σταθμό και αφού συμβεί αυτό, στη συνέχεια πρέπει να την δηλώσει στη βάση της DNS Υπηρεσίας. Ο IPv6 host ενημερώνεται για την διεύθυνση που του αποδίδεται και πλέον η επικοινωνία μπορεί να αρχικοποιηθεί.
Ο DSTM μηχανισμός βασίζεται στην χρήση ενός DHCP server και προαιρετικά στην χρήση ενός DNS server. Συνεπώς ο σχεδιασμός του ταιριάζει αρκετά σε μικρού και μεσαίου μεγέθους οργανισμούς που ήδη χρησιμοποιούν ένα DHCP server προκειμένου να μοιράσουν τις global IPv4 διευθύνσεις.
Η κύρια δυσκολία εφαρμογής του έγκειται στο γεγονός της μη διαθεσιμότητας του DHCPv6 server, δεδομένου ότι η διαδικασία προτυποποίησης του δεν έχει ακόμα ολοκληρωθεί.

6.1 Υποστήριξη του IPv6 σε επίπεδο λειτουργικών συστημάτων και εφαρμογών

Παρά όλη την προχωρημένη φάση στην οποία βρίσκεται η διαδικασία προτυποποίησης του πρωτοκόλλου, δεν υπάρχει αντίστοιχη υποστήριξη σε επίπεδο εφαρμογών από την μεριά του χρήστη. Η Microsoft ενσωματώνει στα Windows XP την IPv6 stack, κάτι που δεν ισχύει για τα Windows 2000, στα οποία μεν εγκαθίσταται η IPv6 stack αλλά η λειτουργικότητα της είναι αρκετά περιορισμένη και προκαλεί αρκετά προβλήματα στη όλη λειτουργία του σταθμού. Σημαντικότερα καλύτερη είναι η αντίστοιχη υποστήριξη στο IPv6 από τους κλώνους του Unix και ειδικότερα από τις διάφορες εκδόσεις του Linux και του BSD. Για το τελευταίο ιδιαίτερα υπάρχει μεγάλη ποικιλία εφαρμογών τόσο σε επίπεδο εξυπηρετητή όσο και σε επίπεδο πελάτη(client). Αυτό συμβαίνει γιατί το BSD είναι το λειτουργικό πάνω στο οποίο κυρίως εργάζεται το KAME Group από την Ιαπωνία, που είναι από τις σημαντικότερες προσπάθειες για την προώθηση του IPv6.

7.1 Βιβλιογραφία

[1] C. Bouras, A. Gkamas, K. Stamos, “From IPv4 to IPv6: The case of OpenH323 Library”, SAINT 2003, Orlando, Florida, 27-31 January 2003, pp. 196-199
[2] S. Josset, C. Bouras, A. Gkamas, K. Stamos, “Adding IPv6 support to H323: Gnomemeeting/openH323 port”, IST Mobile & Wireless Communications Summit 2003, 15-18 June 2003, Aveiro – Portugal (submitted)
[3] Ch. Bouras, A. Gkamas, A. Karaliotas, D. Primpas, K. Stamos, “Issues for the performance monitoring of an open source H.323 implementation ported to IPv6-enabled networks with QoS characteristics”, The 4th International Conference on Internet Computing (IC 2003), June 23th - 26th, 2003, Monte Carlo Resort, Las Vegas, Nevada, USA (submitted)
[4] C. Bouras, P. Ganos, A. Karaliotas, “Transition Strategies from IPv4 to IPv6: The case of GRNET”, 3rd International Network Conference-INC 2002, Plymouth, UK, July 16-18 2002, pp. 89-96
[5] C. Bouras, P. Ganos, A. Karaliotas, “The deployment of IPv6 in an IPv4 world and Transition Mechanisms”, Internet Research: Electronic Networking, Applications and Policy, Emerald, 2003, (to appear)
[6] RFC 1809 “Using the Flow Label Field in IPv6” C. Partridge, June 1995
[7] RFC 1889 “RTP: A Transport Protocol for Real-Time Applications”, H. Shculzrinne, S. Casner, R. Frederick, V. Jacobson, January 1996
[8] RFC 2292 “Advanced Sockets API for IPv6”, W. Stevens, M. Thomas, February 1998
[9] RFC 2373 “IP Version 6 Addressing Architecture” R. Hinden, S. Deering, July 1998
[10] RFC 2374 “An IPv6 Aggregatable Global Unicast Address Format” R. Hinden, M. O’Dell, S. Deering, July 1998
[11] RFC 2375 “IPv6 Multicast Address Assignments” R. Hinden, S. Deering, July 1998
[12] RFC 2402 “IP Authentication Header” S. Kent, R. Atkinson, November 1998
[13] RFC 2406 “IP Encapsulating Security Payload (ESP)” S. Kent, R. Atkinson, November 1998
[14] RFC 2460 “Internet Protocol, Version 6 (IPv6) Specification” S. Deering, R. Hinden, December 1998
[15] RFC 2463 “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification” A. Conta, S. Deering, December 1998
[16] RFC 2473 “Generic Packet Tunneling in IPv6 Specification” A. Conta, S. Deering, December 1998
[17] RFC 2474 “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers” K. Nichols, S. Blake, F. Baker, D. Black, December 1998
[18] RFC 2529 “Transmission of IPv6 over IPv4 Domains without Explicit Tunnels” B. Carpenter, C. Jung, March 1999
[19] RFC 2546 “6Bone Backbone Routing Guidelines” A. Durand, B. Buclin, March 1999

[20] RFC 2553 “Basic Socket Interface Extensions for IPv6”, R. Gilligan, S.,Thomson, J. Bound, W. Stevens, March 1999
[21] RFC 2710 “Multicast Listener Discovery (MLD) for IPv6” S. Deering, W. Fenner, B. Haberman, October 1999
[22] RFC 2732 “Format for Literal IPv6 Addresses in URL's”, R. Hinden, B. Carpenter, L. Masinter, December 1999
[23] RFC 2893, “Transition Mechanisms for IPv6 Hosts and Routers”, R. Gilligan, E. Nordmark, August 2000
[24] RFC 3056 “Connection of IPv6 Domains via IPv4 Clouds” B. Carpenter, K. Moore, February 2001
[25] RFC 3175 “Aggregation of RSVP for IPv4 and IPv6 Reservations” F. Baker, C. Iturralde, F. Le Faucheur, B. Davie, September 2001
[26] “Dual stack deployment using DSTM and 6to4” Tsirtsis, draft-ietf-ngtrans-6to4-dstm-00.txt
[27] “Application Aspects of IPv6 Transition”, Myung-Ki Shin, Yong-Guen Hong, Sookyoung Jeny Lee, Joo-Chul Lee, Yong-Jin Kim, draft-shin-ngtransapplication-transition-01.txt
[28] MSDN Library, Windows Sockets Version 2
[29] Microsoft IPv6 Technology Preview for Windows 2000, http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp
[30] Compaq IPv6 Porting Assistant, http://www.tru64unix.compaq.com/internet/ipv6portingassistant/
[31] Solaris IPv6, http://wwws.sun.com/software/solaris/ipv6/
[32] “Adding IPv6 capability to Windows Socket Applications”, Microsoft Corporation
[33] “Porting Networking Applications to the IPv6 APIs”, Sun Microsystems
[34] “Guidelines for migration of collaborative work applications”, Eva Castro, Tomas P. de Miguel, LONG project, June 2002
[35] “Network Programming, Volume 1”, 2nd Edition, W. Richard Stevens
[36] “TCP/IP Illustrated - Volume 2” W. Richard Stevens, Gary Wright
[37] “Implementing IPv6” Mark A. Miller
[38] “IPv6 Clearly Explained” Pete Loshin
[39] “IPv6 : The Next Generation Internet Protocol” Stewart S. Miller
[40] “IPv6 Document Library” http://www.sumitomo.com/htmls/randd/ipv6/doc.html
[41] Guide to DIGITAL UNIX IPv6, http://www.ipv6.zk3-x.dec.com/userguide/TITLE.HTM
[42] Ian Sommerville, “Software Engineering Fifth Edition” Addison-Wesley 1995
[43] IPv6 Forum, http://www.ipv6forum.com/
[44] IPv6 Information Page, http://www.ipv6.org/
[45] IPv6 Resource Centre, http://www6.cs-ipv6.lancs.ac.uk/
[46] IPv6.com, http://www.ipv6.com/
[47] 6bone Home Page, http://www.6bone.net/
[48] 6REN Project, http://www.6ren.net/
[49] 6NET project, http://www.sixnet.org
[50] 6INIT project, http://www.6init.org/presentations.html

[51] KAME project, http://www.kame.net/
[52] Euro6IX project, http://www.euro6ix.net
[53] Lancaster VideoServer, http://www.cs-IPv6.lancs.ac.uk/IPv6/videoserver
[54] UCL Mbone tools, http://www-mice.cs.ucl.ac.uk/multimedia/software/
[55] EAITY, http://www.cti.gr

8.1 Ακρωνύμια

AAL ..... Atm Adaptation Layer
ACF..... Admission control ConFirm
AH..... Authentication Header
ANSI .....American National Standards Institute
ARJ ..... Admission control ReJect
ARQ.....Admission control ReQuest
ASN.1..... Abstract Syntax Notation number One
ATM.....Asynchronous Transfer Mode
BCF..... Bandwidth control ConFirm
BGP.....Border Gateway Protocol
BOOTP ..... BOOT Protocol
BRJ..... Bandwidth control ReJect
BRQ .....Bandwidth control ReQuest
BSD..... Berkeley Software Distribution
CCITT.....Comité Consultatif International Téléphonique et Télégraphique
CIDR..... Classless Inter-Domain Routing
CODEC.....COder / DECoder
CTI ..... Computer Technology Institute
DHCP..... Dynamic Host Configuration Protocol
DNS.....Domain Name Service
DS .....Differentiated Services
DSTM .....Dual Stack Transition Mechanism
DTI.....Dynamic Tunneling Interfaces
ESP.....Encapsulation Security Payload
FTP..... File Transfer Protocol
GCF..... Gatekeeper discovery ConFirm
GRQ..... Gatekeeper discovery ReQuest
HTTP..... HyperText Transmission Protocol
ICMP..... Internet Control Message Protocol
IEEE.....Institute of Electrical and Electronic Engineers
IETF .....Internet Engineering Task Force
IGMP..... Internet Group Memebership Protocol
I/O .....Input / Output
IP.....Internet Protocol
IPX ..... Internetwork Packet eXchange
ISDN .....Integrated Services Digital Network

ISO .....International Standardisation Organisation
ITU-T ..... International Telecommunication Union
LAN .....Local Area Network
MCU ..... Multipoint Control Unit
MLD.....Multicast Listener Discovery
MODEM..... MOdulator / DEModulator
MPL ..... Mozilla Public License
MTU..... Maximum Transfer Unit
NAT ..... Network Address Translation
NLA ..... Next-Level Aggregation
NSAP .....Network Service Access Point
NTP.....Network Time Protocol
OSI ..... Open Systems Interconnection
OSPF..... Open Shortest-Path First
PDU..... Protocol Data Unit
PIM .....Protocol-Independent Multicast
POP3 .....Post Office Protocol (level/version) 3
POTS.....Plain Old Telephone Service/System
PSN ..... Packet Switched Network
PSTN.....Public Switch(ed) Telephone Network
QoS ..... Quality of Service
RAS.....Registration Admission Status
RFC.....Request For Comments
RSVP.....Resource reSerVation (setup) Protocol
RTCP..... Real-Time Transport Control Protocol
RTP ..... Real-Time Transport Protocol
SCN.....Switched Circuit Network
SCP .....Session Control Protocol
SDES..... Source DEScription
SMTP.....Simple Mail Transfer Protocol
SNMP.....Simple Network Management Protocol
SPX .....Sequenced Packet Exchange
SSL..... Secure Socket Layer
TCP ..... Transmission Control Protocol
TLA.....Top-Level Aggregation
TOS..... Type Of Service
TTL .....Time-To-Live
UDP.....User Datagram Protocol
URL..... Uniform Resource Locator
VoIP ..... Voice over IP
VPN.....Virtual Private Network
WAN.....Wide Area Network
ΕΑΙΤΥ..... Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών