University of Macedonia
Master Information System
Networking Technologies

Professor: A.A. Economides

Subject:

IPV6, MBONE, MOBILE IPV6, ICMPV6, IGMPV6, IPV6 OVER ATM, IPMULTICASTING OVER ATM

MAVROUDI MAGDALINI

THESSALONIKI 2002

Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων

Υπεύθυνος Καθηγητής: Α.Α. Οικονιμίδης

Θέμα:

IPV6, MBONE, MOBILE IPV6, ICMPV6, IGMPV6, IPV6 OVER ATM, IPMULTICASTING OVER ATM

Μαυρουδή Μαγδαληνή

ΘΕΣΣΑΛΟΝΙΚΗ 2002

ΠΕΡΙΕΧΟΜΕΝΑ-CONTENTS

Περίληψη

Με το Διαδίκτυο που διπλασιάζεται στο μέγεθος κάθε 10 έως 12 μήνες και η αγορά που απαιτεί όλο και περισσότερο τη ζωντανή ηχητική και τηλεοπτική μετάδοση μέσω του Διαδικτύου, ο καιρός έχει έρθει για μια επόμενη γενεά Internet πρωτοκόλλου που θα είναι σε θέση να αντιμετωπίσει αυτή την αυξητική κλιμάκωση των απαιτήσεων των χρηστών. Στη παρούσα εργασία αρχικά αναφέρονται τα χαρακτηριστικά του IPv6 και οι πέντε σημαντικές αλλαγές οι οποίες αφορούν την επέκταση της διεύθυνσης, την απλοποίηση της επικεφαλίδας, τη βελτίωση της επεκτασιμότητας, την υποστήριξη ετικετών προτεραιότητας και ροής πακέτων και τέλος τους μηχανισμούς για την ασφάλεια και την πιστοποίηση. Στη συνέχεια παρουσιάζονται τα πεδία τα οποία περιλαμβάνουν οι επικεφαλίδες του IPv6 οι οποίες είναι οργανωμένες σε λέξεις των 64 bits και το συνολικό μέγεθος των επικεφαλίδων είναι 40 bytes.Επίσης στο IPv6 μπορούν να υπάρχουν προαιρετικά επικεφαλίδες επέκτασης που θα πρέπει να εμφανίζονται με συγκεκριμένη σειρά. Η κάθε επικεφαλίδα αναφέρει ποια είναι η επόμενη που ακολουθεί ή αν είναι η τελευταία.

Στο IPv6 υπάρχουν τρεις κατηγορίες διευθύνσεων οι unicast, multicast και anycast (μόνο οι δρομολογητές επιτρέπεται να έχουν anycast διεύθυνση) ενώ έχουν καταργηθεί οι broadcast.Το Ipsec πρότυπο ορίζει τους μηχανισμούς ασφάλειας που μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξάρτητα από την έκδοση έτσι ώστε να επιτυγχάνεται ασφάλεια στο επίπεδο δικτύου. Ο έλεγχος πρόσβασης, η ακεραιότητα δεδομένων, η πιστοποίηση του αποστολέα, η προστασία εναντίον επιθέσεων τύπου packet replay, η κωδικοποίηση των δεδομένων και η εξασφάλιση του απορρήτου της ροής των δεδομένων είναι οι κυριότερες υπηρεσίες του Ipsec.

Ένας από τους πιο συγκεκριμένους στόχους του Ipv6 ήταν να υποστηρίζει την αρχή “Plug and Play” ώστε να είναι δυνατή η σύνδεση ενός σταθμού χωρίς να απαιτείται η ανθρώπινη παρέμβαση. Βασισμένο σε αυτή τη δυνατότητα της αυτόματης ρύθμισης των σταθμών εργασίας το Mobile IPv6 παρουσιάζει σημαντικά πλεονεκτήματα.

Στη συνέχεια αναπτύσσονται οι τεχνικές μετάβασης του διαδικτύου στο πρωτόκολλο IPv6 μια και η μετάβαση μπορεί και πρέπει να γίνει σταδιακά.

Το Mbone είναι μια εφαρμογή η οποία έχει το χαρακτηριστικό ότι επιτρέπει σε multicast πακέτα να ταξιδεύουν και μέσω των δρομολογητών οι οποίοι έχουν δημιουργηθεί για να διαχειρίζονται μόνο unicast κίνηση. Πιστεύετε ότι όταν το multicasting θα γίνει ένα στάνταρ χαρακτηριστικό στους δρομολογητές του Internet αυτή η εφαρμογή θα γίνει απαρχαιωμένη.

Το ICMPv6 είναι ενσωματωμένο στοιχείο του IPv6 και πρέπει να μπορεί να υλοποιηθεί από κάθε κόμβο για να αναφέρουν τα λάθη σε πακέτα που διαχειρίστηκαν και να πραγματοποιήσουν άλλες λειτουργίες πχ. διαγνωστικά. Όπως το ICMPv6 και το IGMPv6 είναι ένα τμήμα του Ip και όλοι οι υπολογιστές που θέλουν να λαμβάνουν IP multicasting πρέπει να το έχουν εγκατεστημένο. Με αυτό το πρωτόκολλο οι host επικοινωνούν με τους τοπικούς mrouters για να ανταλλάσσουν την πληροφορία ότι ενδιαφέρονται να λαμβάνουν multicasting μηνύματα που στέλνονται σε συγκεκριμένες ομάδες.

Τα δυο πρωτόκολλα ATM και Ipv6 γιατί όχι μόνο αλληλοσυμπληρώνουν το ένα το άλλο, αλλά επίσης εξυπηρετούν εντελώς διαφορετικούς ρόλους στο διαδίκτυο και έτσι δεν υπάρχει θέμα επιλογής ανάμεσα τους.
Τέλος η δυνατότητα υποστήριξης IP multicasting θεωρείται ένα από τα σημεία που θα κρίνουν σε μεγάλο βαθμό την καταλληλότητα του ATM ως μέσο μεταφοράς κίνησης

Summary

With the Internet doubling in size every 10 to 12 months and the market increasingly demanding live audio and video transmission over the Internet, the time has come for a next generation Inernet Protocol that will be able to cope with these rapidly ascalating user volume and traffic demands. In the present work are initially reported the characteristics of IPv6 and five the important changes which concern the extension of address, the simplification of heading, the support of labels of priority and flow of packets and finally the mechanisms for the safety and the certification. Then are presented the fields which include headings of JPv6 what are organized in words the 64 bits and total size of headings are 40 bytes. Also in the IPv6 can exist optionally headers of extension that will be supposed to present itself with concrete order. Each header reports which is next that follows or if she is the last one.

In the IPv6 exist three categories of addresses unicast, multicast and anycast (only the routers it is allowed they have anycast address) while have been suppressed broadcast. The Ipsec model fix the mechanisms of safety that can be used from the IP protocol independent from the version so as to is achieved safety in the level of network. The control of access, the integrity of data, the certification of sender, the protection against attacks of type packet replay, the coding given and the guarantee of secrecy of flow of data are the more important services of Ipsec.

One from the most particular objectives of Jpv6 it was supports the beginning “Plug and Play” so that is possible the connection of station without is required the human intervention. Based on this possibility of automatic regulation of stations of work Mobile IPv6 presents important advantages. Then are developed the techniques of passage of internet in protocol IPv6 one and the passage can and it should it becomes progressively. The Mbone is a application which has the characteristic that it allows in multicast packets to travel also via the routers which have been created in order to they only manage unicast movement. Believe that when multicasting becomes a standard characteristic in the routers of Internet this application will become out of date.

The ICMPv6 is incorporated element of IPv6 and it should it can be materialized from each node in order to they report the errors in parcels that were managed and they realize other operations eg. Diagnostics. Like the ICMPv6 and the IGMPv6 are a department of Ip and all the computers that want to receive IP multicasting it should him they have installed. With this protocol host they communicate with local mrouters in order to they exchange the information that they interest to receive multicasting messages that are sent in concrete teams.

The two protocols ATM and Ipv6 because not only supplement the one the other, but also they serve completely different roles in the internet and thus does not exist subject of their choice between them.
Finally the possibility of support IP multicasting is considered one of the points that will to a large extent judge the appropriateness of ATM as means of transport of movement.

Εισαγωγή

Το διαδίκτυο αυτήν τη στιγμή χρησιμοποιεί την έκδοση τέσσερα (4) του Internet πρωτοκόλλου, γνωστή συνοπτικά σαν IPv4. Πρόκειται αναμφίβολα για το πιο πετυχημένο πρωτόκολλο με χρήση του οποίου συνδέθηκαν χιλιάδες κόμβοι εκατοντάδων διαφορετικών δικτύων δημιουργώντας αυτό που σήμερα ονομάζουμε διαδίκτυο. Αρκετές δεκάδες εκατομμυρίων υπολογιστών και εκατοντάδες εκατομμυρίων χρηστών είναι συνδεμένοι στο διαδίκτυο.
Η πρώτη έκδοση του IP έγινε τα μέσα του 1970 και στη δεκαετία που διανύουμε είναι πλέον φανερά τα σημάδια γήρατος κάτι που σημαίνει ότι απαιτείται σύντομα η αναβάθμισή του. Αυτό όμως σημαίνει ότι μία αναβάθμιση του πρωτοκόλλου αυτόματα θα επηρεάσει εκατομμύρια χρηστών και οργανισμών και θα πρέπει να γίνει με τον καλύτερο δυνατό τρόπο ώστε να ελαχιστοποιηθούν οι πιθανότητες προβληματικής λειτουργίας.

Οι βασικοί λόγοι που απαιτείται η αναβάθμιση είναι οι παρακάτω:

1 Θέματα έλλειψης διευθύνσεων: Αν και οι χρήστες πιστεύουν ότι αυτός εμφανίζεται σαν ο βασικότερος λόγος αναβάθμισης του IPv4, ουσιαστικά πρόκειται μόνο για ένα από τα προβλήματα που απασχολούν την κοινότητα του διαδικτύου.

2 Θέματα απόδοσης: Παρ' όλο που το IP λειτουργεί αποδοτικά τα 20 και πλέον χρόνια που χρησιμοποιείται, υπάρχουν πάρα πολλές βελτιώσεις που μπορούν να γίνουν. Οι διαχειριστές γνωρίζουν καλύτερα από όλους το κόστος διαχείρισης των routing entries εξαιτίας της έλλειψης επιπέδων ιεραρχίας στις IP διευθύνσεις. Επίσης αρκετές εφαρμογές απαιτούν υποστήριξη ποιότητας εξυπηρέτησης (QoS) από το IPv4 και προσπαθούν να ξεπεράσουν αυτή του την αδυναμία με χρήση άλλων πρωτοκόλλων σε υψηλότερα επίπεδα, μην πετυχαίνοντας όμως τα αναμενόμενα.

3 Θέματα ασφάλειας: Μετά την τεράστια εξάπλωση που γνώρισε το διαδίκτυο και τη χρήση του σε κάθε είδος οικονομικής συναλλαγής διαπιστώθηκε ότι η ασφάλεια δεν μπορεί να απασχολεί μόνο τις εφαρμογές, αλλά το ίδιο το IP θα πρέπει να έχει μηχανισμούς ασφάλειας.

4 Θέματα αυτόματης ανάθεσης διεύθυνσης: Είναι γνωστό ότι οι ρυθμίσεις του IPv4 στους κόμβους είναι σχετικά πολύπλοκη διαδικασία. Οι χρήστες θα επιθυμούσαν μία λειτουργία "plug and play" με την έννοια του να μπορεί κάποιος να συνδέει τον υπολογιστή του στο δίκτυο IP και αυτός να μπορεί αυτόματα να βρίσκει τις ρυθμίσεις του. Οι ανάγκες των συνεχώς αυξανόμενων χρηστών που δεν έχουν σταθερό χώρο εργασίας (mobile users) απαιτούν αυτόματες ρυθμίσεις ανεξάρτητα του δικτύου που χρησιμοποιούν κάθε φορά για να συνδεθούν.

1Τα χαρακτηριστικά του Ipv6

1.1Οι προδιαγραφές του Ipv6

Η αναβάθμιση από το IPv4 στο IPv6 αρχικά περιγράφηκε σε δύο RFCs. Το RFC 1883 [1] ορίζει το ίδιο το πρωτόκολλο (που αργότερα αντικαταστάθηκε από το RFC 2460 [2]) και το RFC 1884 [3] (που αργότερα αντικαταστάθηκε από το RFC 2373). Τα νέα αυτά χαρακτηριστικά αναφέρουν πέντε σημαντικές αλλαγές και αφορούν την επέκταση της διεύθυνσης, την απλοποίηση της επικεφαλίδας, τη βελτίωση της επεκτασιμότητας, την υποστήριξη ετικετών προτεραιότητας και ροής πακέτων και μηχανισμούς για την ασφάλεια και την πιστοποίηση. Πιο αναλυτικά το IPv6 έχει [4],[5]:

1 Νέες δυνατότητες αριθμοδότησης: Με δεδομένο τον κίνδυνο για έλλειψη των υπαρχόντων διευθύνσεων του IPv4 υιοθετήθηκαν διευθύνσεις μεγέθους 128 bits σε σχέση με τις υπάρχουσες διευθύνσεις των 32 bits. Καταργείται η έννοια της κλάσης δικτύου και υπάρχουν δυνατότητες ιεραρχικής αριθμοδότησης και δρομολόγησης. Με το νέο τρόπο ο αριθμός των διευθύνσεων είναι: 4δις x 4 δις (= 2^{96}) x [το μέγεθος του σημερινού Διαδικτύου (2^{32})]. Το αποτέλεσμα είναι: 340.282.366.920.938.463.463.374.607.437.68.211.456 [6]. Αυτός είναι ένα πολύ μεγάλο σύνολο διευθύνσεων το οποίο αντιστοιχεί σε 665.570.793.348.866.943.898.599 διευθύνσεις ανά τετραγωνικό μέτρο της γης. Ακόμη όμως και με τις πιο δυσοίωνες πρακτικές για αριθμοδότηση θα ήταν δυνατόν να έχουμε περίπου 3.000 διευθύνσεις / τετραγωνικό μέτρο. Έχουν δεσμευθεί διευθύνσεις για κατευθείαν απόδοση από πάροχο υπηρεσιών, διευθύνσεις για αριθμοδότηση με βάση τις NSAP διευθύνσεις του OSI, multicast διευθύνσεις, διευθύνσεις για δίκτυα IPX, τοπικές διευθύνσεις κλπ. Γενικά το 15% των διευθύνσεων είναι δεσμευμένο ενώ το υπόλοιπο 85% φυλάσσεται για μελλοντική χρήση.

2 Ορίζονται διευθύνσεις με τοπική (link local) ή υπερτοπική (site local) μοναδικότητα οι οποίες δεν είναι μοναδικές και δεν δρομολογούνται στο διαδίκτυο αλλά διευκολύνουν την αυτόματη ρύθμιση σταθμών (βλέπε συνέχεια).

3 Υιοθέτηση διευθύνσεων τύπου anycast για την αντιστοίχιση ενός συνόλου σταθμών σε μία διεύθυνση. Παράλληλα καταργούνται οι διευθύνσεις τύπου broadcast. Αποστολή ενός πακέτου σε διεύθυνση anycast σημαίνει την παράδοσή του σε ένα οποιοδήποτε σταθμό του συνόλου (κατά αναλογία με ATM). Μόνο οι δρομολογητές επιτρέπεται να έχουν τέτοιες διευθύνσεις, ενώ επιτρέπεται να χρησιμοποιούνται μόνο ως διεύθυνση αποστολής.

4 Κατάργηση διάφορων απαρχαιωμένων τύπου επικεφαλίδων με αποτέλεσμα το σύνολο μήκος της επικεφαλίδας των πακέτων IPv6 να είναι το διπλάσιο μόνο από αυτό του IPv4 όταν οι αντίστοιχες διευθύνσεις είναι τετραπλάσιες σε μήκος. Δυναμική επέκταση της επικεφαλίδας μόνο όταν απαιτείται από τις συνθήκες λειτουργίας. Πιο συγκεκριμένα οι επικεφαλίδες στο IPv6 αποτελούνται από οχτώ (8) πεδία (δύο εκ των οποίων είναι οι διευθύνσεις αποστολέα και προορισμού) και έχουν μέγεθος σαράντα (40) bytes. Σε αντίθεση οι επικεφαλίδες στο IPv4 που περιλαμβάνουν τουλάχιστον δώδεκα (12) πεδία και το μέγεθός τους μπορεί να κυμαίνεται από είκοσι (20) bytes αν δεν έχουν χρησιμοποιηθεί τα πεδία Options μέχρι και εξήντα (60) bytes αν χρησιμοποιηθούν. Η απλοποίηση της επικεφαλίδας επιτρέπει πιο εύκολη και γρήγορη επεξεργασία από τους δρομολογητές και άρα

μεγαλύτερη ταχύτητα στη δρομολόγηση. Για παράδειγμα η συνθήκη όλες οι επικεφαλίδες να έχουν το ίδιο μέγεθος καταργεί την ανάγκη να υπάρχει πεδίο μεγέθους επικεφαλίδας. Επίσης η κατάργηση της κατάτμησης του πακέτου από τους ενδιάμεσους κόμβους (μόνο ο αποστολέας έχει αυτό το δικαίωμα) καταργεί αρκετά πεδία που χρησιμοποιούνταν για αυτό το σκοπό. Τέλος η κατάργηση του πεδίου checksum δεν επηρεάζει την αξιοπιστία αφού υπάρχουν οι αντίστοιχοι έλεγχοι στα ανώτερα πρωτόκολλα (TCP & UDP).

5 Καλύτερη υποστήριξη των IP Options και βελτίωση του μηχανισμού των επεκτάσεων (Extension). Ενώ στο IPv4 τα IP Options προσθέτονταν στο τέλος της IP επικεφαλίδας, στο IPv6 προσθέτονται σε ξεχωριστές επικεφαλίδες επέκτασης. Έτσι μόνο οι κόμβοι που απαιτείται να ελέγξουν αυτές τις επικεφαλίδες πρέπει να τις διαβάσουν. Για παράδειγμα οι επικεφαλίδες κατάτμησης (fragmentation headers) χρειάζονται να επεξεργαστούν μόνο από τον κόμβο αποστολέα και τον κόμβο παραλήπτη. Όλοι οι υπόλοιποι κόμβοι αγνοούν αυτές τις επικεφαλίδες κάτι που οδηγεί σε ταχύτερη επεξεργασία. Επιπλέον αν απαιτείται κάποια Options να ελεγχθούν από όλους τους ενδιάμεσους κόμβους, τότε αυτό μπορεί να γίνει με χρήση της επικεφαλίδας Hop by Hop Options.

6 Δυνατότητες για παροχή υπηρεσίας ποιότητας (Quality of service) μέσω του ορισμού ετικέτας προτεραιότητας και ροής πακέτων (flow label). Η ροή πακέτων (flow) ορίζεται ως ένα σύνολο πακέτων που ξεκινούν από μία συγκεκριμένη διεύθυνση αφετηρίας με προορισμό μια απλή unicast ή multicast διεύθυνση και για την οποία η αφετηρία απαιτεί ιδιαίτερη μεταχείριση από τους δρομολογητές του μονοπατιού μέχρι τον παραλήπτη. Με βάση αυτήν την ετικέτα η αφετηρία μπορεί κάνει αίτηση για εκχώρηση χωρητικότητας μέσω του πρωτοκόλλου RSVP. Μία άλλη περίπτωση είναι η χρησιμοποίηση της ετικέτας προτεραιότητας ροής στα πρωτόκολλα δρομολόγησης με στόχο την βελτιστοποίηση της δρομολόγησης. Είναι προφανές ότι αυτός ο μηχανισμός είναι ιδιαίτερα χρήσιμος για τις εφαρμογές πραγματικού χρόνου. Οι δρομολογητές κρατούν πληροφορία για κάθε ροή πακέτων η οποία αφορά το σύνολο των πακέτων της ροής. Έτσι δεν χρειάζεται να ελέγχουν κάθε επικεφαλίδα πακέτου ξεχωριστά και αυτό οδηγεί σε αύξηση της ταχύτητας επεξεργασίας.

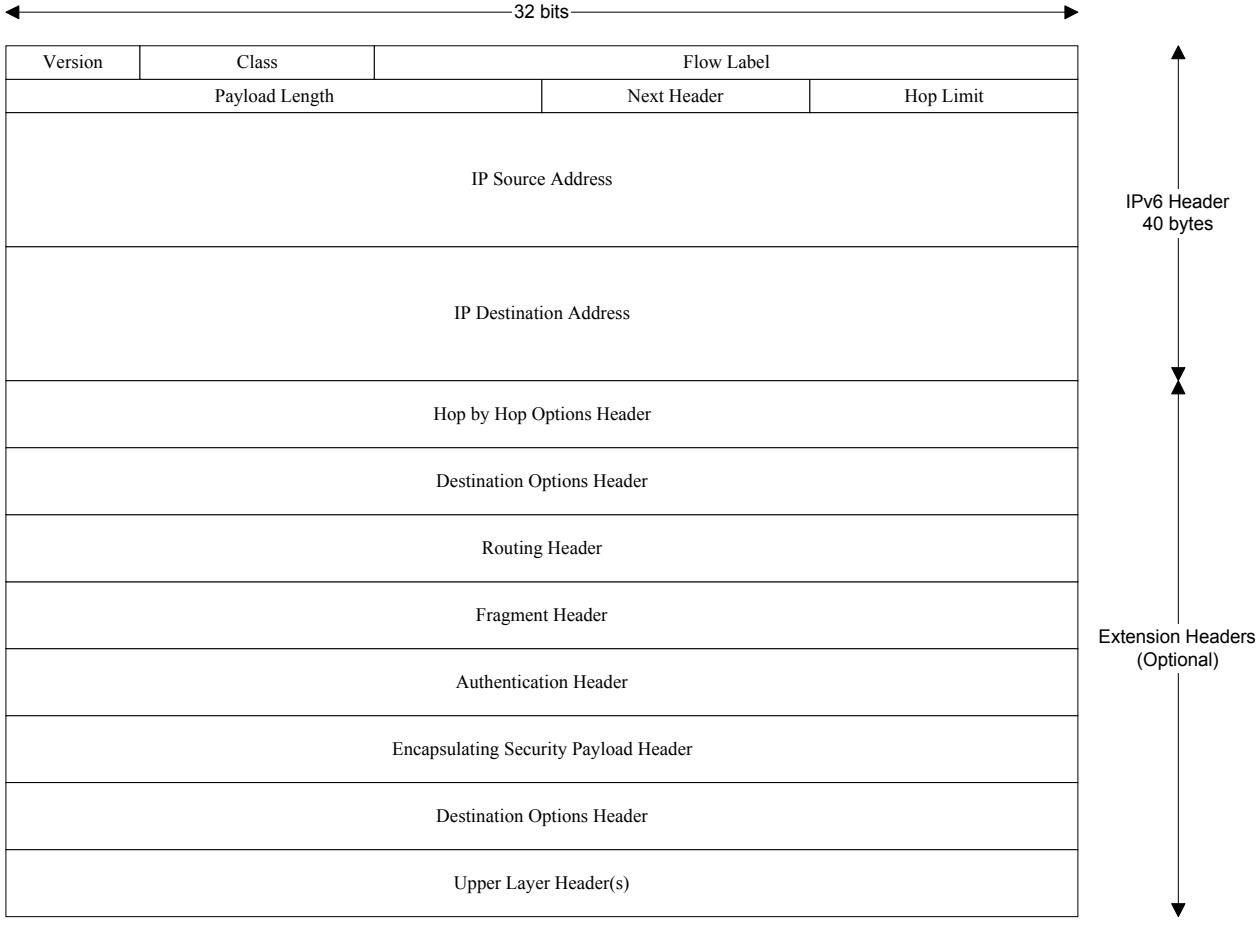
7 Ενσωματωμένες δυνατότητες για αυξημένη ασφάλεια με επιλεκτική κρυπτογράφηση ολόκληρου του πακέτου ή μόνο της επικεφαλίδας του. Δυνατότητα για επαλήθευση της ταυτότητας του αποστολέα και παραλήπτη σε περιπτώσεις κρυπτογραφημένων ή απλών πακέτων. Το IPv6 χρησιμοποιεί όλες τις τεχνικές για ασφάλεια που είχαν ενσωματωθεί στο IPv4 και επιπλέον παρουσιάζει και δύο επεκτάσεις το IP Authentication Header (AH) και το IP Encapsulating Security Payload (ESP). Η πρώτη εξασφαλίζει ότι το πακέτο δεν έχει αλλαχθεί κατά τη διαδρομή του από την αφετηρία στον παραλήπτη, βάζοντας ένα checksum του πακέτου στη θέση του AH. Η δεύτερη παρέχει ένα μηχανισμό με τον οποίο μπορεί να κωδικοποιηθούν είτε τα δεδομένα του πακέτου (payload) είτε να κωδικοποιηθεί ολόκληρο το πακέτο και στη συνέχεια να γίνει tunnel πάνω από το διαδίκτυο. Αυτός ο μηχανισμός είναι απαραίτητος γιατί μπορεί να αποτελέσει τη βάση δημιουργίας ιδεατών ιδιωτικών δικτύων (VPNs) ώστε να μπορέσουν οι οργανισμοί να χρησιμοποιήσουν το διαδίκτυο για να χτίσουν τα δικά τους ασφαλή backbone.

8 Αυτόματη ρύθμιση σταθμών. Η αυτόματη ρύθμιση σταθμών επιτρέπει την αυτόματη συγκρότηση (configuration) και ρύθμιση των υπολογιστών όταν

συνδέονται στο διαδίκτυο. Η δυνατότητα αυτή ισχύει εφόσον τα άκρα διασύνδεσης (interfaces) έχουν ένα μοναδικό χαρακτηριστικό (πχ link layer address) διεύθυνσης. Η αυτόματη ρύθμιση σταθμών είναι ένα σημαντικό χαρακτηριστικό στην περίπτωση που χρειάζεται ομαδική αλλαγή της αριθμοδότησης σε ένα ολόκληρο δίκτυο (πχ λόγω αλλαγής πάροχου υπηρεσιών). Σε περίπτωση που η αυτόματη ρύθμιση των σταθμών δεν είναι επιθυμητή, συνίσταται η δυναμική ρύθμιση με χρήση του πρωτοκόλλου DHCP. Η αυτόματη ρύθμιση γίνεται με χρήση των διευθύνσεων τοπικού και υπερτοπικού χαρακτήρα.

1.2 Η δομή της επικεφαλίδας στο IPv6

Στο IPv4 όλες οι επικεφαλίδες είναι οργανωμένες σε λέξεις των 32 bits. Στο IPv6 οι επικεφαλίδες είναι οργανωμένες σε λέξεις των 64 bits και το συνολικό μέγεθος των επικεφαλίδων είναι 40 bytes. Επιπλέον στο IPv6 μπορούν να υπάρχουν προαιρετικά επικεφαλίδες επέκτασης που θα πρέπει να εμφανίζονται με συγκεκριμένη σειρά. Η κάθε επικεφαλίδα αναφέρει ποια είναι η επόμενη επικεφαλίδα που ακολουθεί ή αν είναι η τελευταία.



Σχήμα 1 Η δομή μιας IPv6 επικεφαλίδας

Το πρωτόκολλο IPv6 περιλαμβάνει τα ακόλουθα πεδία στις επικεφαλίδες του[7]:

1 Έκδοση: Αναφέρεται η έκδοση του IP που χρησιμοποιείται (για το IPv6 είναι ίση με έξι (6).

2 Κλάση: Ορίζει το είδος υπηρεσίας, που ανήκει στο μοντέλο των differentiated υπηρεσιών, που πρέπει να δοθεί στο πακέτο. Είχε οριστεί για πρώτη φορά στο RFC 1883 [1] σαν πεδίο προτεραιότητας. Κατόπιν το όνομα αλλάχτηκε σε κλάση και πρόσφατα χαρακτηρίζεται σαν κλάση κίνησης. Δεν έχει προς το παρόν οριστεί πώς θα χρησιμοποιείται αυτό το πεδίο.

3 Ροή πακέτων: Χρησιμοποιείται για να αναγνωριστούν τα πακέτα της ίδιας ροής. Ένας κόμβος μπορεί να έχει περισσότερες από μία ροές πακέτων. Στο RFC 1883 [1] είχε οριστεί με μεγαλύτερο μέγεθος, αλλά κατόπιν της αύξησης του πεδίου κλάσης μειώθηκε το μέγεθός της.

4 Μήκος πακέτου: Είναι ένας αριθμός που δηλώνει το μήκος του πακέτου των δεδομένων –δηλαδή του πακέτου μετά το τέλος των επικεφαλίδων– (payload) σε bytes. Περιλαμβάνει και το μέγεθος των IPv6 header extensions που τυχόν υπάρχουν.5Επόμενη επικεφαλίδα: Αναφέρει πιο πρωτόκολλο χρησιμοποιείται στην επικεφαλίδα μετά το IPv6 πακέτο. Εκτός από το να αναφέρεται σε κάποιο ανώτερου επιπέδου πρωτόκολλο όπως τα TCP και UDP, μπορεί να αναφέρει την ύπαρξη IPv6 extension headers.

5 Hop limit: Κάθε φορά που ένας κόμβος προωθεί το πακέτο, μειώνει το μέγεθος του hop limit κατά ένα. Όταν αυτό μηδενιστεί το πακέτο διαγράφεται από το δίκτυο. Δεν είναι απίθανο να καταργηθεί αυτό το πεδίο, μιας και η τρέχουσα αίσθηση θέλει αντίστοιχες λειτουργίες να μεταφερθούν σε πρωτόκολλα ανώτερων επιπέδων.

6 Διεύθυνση αποστολέα: Είναι η IPv6 διεύθυνση του κόμβου που δημιούργησε το πακέτο.

7 Διεύθυνση παραλήπτη: Είναι η IPv6 διεύθυνση του ή των κόμβων που πρόκειται να παραλάβουν το πακέτο. Μπορεί να είναι διεύθυνση τύπου unicast, multicast ή anycast. Εάν στο πακέτο υπάρχει και routing extension που ορίζει το μονοπάτι που πρέπει να ακολουθήσει το πακέτο, τότε η διεύθυνση προορισμού μπορεί να είναι ένας από τους ενδιάμεσους κόμβους αντί αυτής που αναφέρεται στο πεδίο διεύθυνση παραλήπτη.

8 Hop-by-Hop Options Header: Αυτή η επικεφαλίδα ακολουθεί πάντα την επικεφαλίδα του IPv6 πακέτου. Περιλαμβάνει δεδομένα που κάθε κόμβος θα πρέπει να επεξεργαστεί.

9 Destination Options Header: Περιέχει πληροφορίες που θα πρέπει να ελεγχθούν από τον πρώτο παραλήπτη που αναφέρεται στη διεύθυνση προορισμού και στις διευθύνσεις που περιλαμβάνονται στο Routing Header.

10 Routing Header: Αναφέρονται οι διάφοροι κόμβοι που θα επισκεφτεί το πακέτο κατά τη διαδρομή από τον αποστολέα στον παραλήπτη. Ο κάθε κόμβος που παραλαμβάνει το πακέτο ελέγχει ποιος είναι ο επόμενος παραλήπτης στη λίστα και προωθεί το πακέτο σ’ αυτόν.

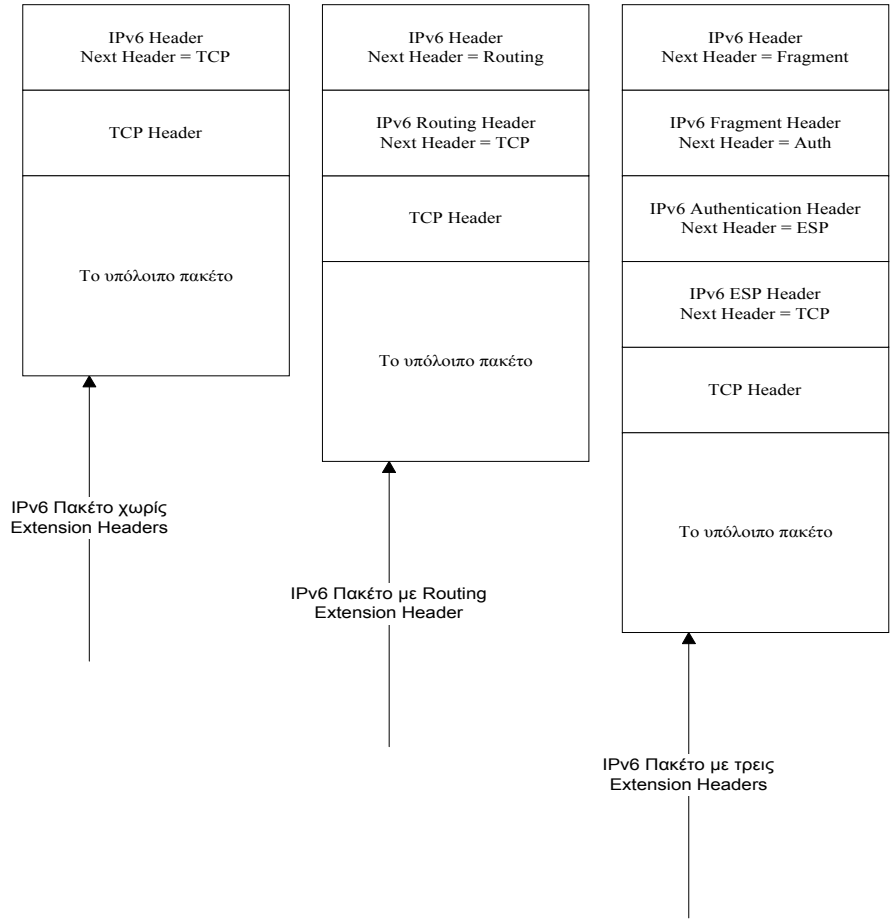
11 Fragment Header: Χρησιμοποιείται από τον κόμβο αποστολέα προκειμένου να μεταδώσει πακέτα με μέγεθος μεγαλύτερο από το μέγιστο επιτρεπόμενο μέγεθος πακέτου (Path MTU) στο μονοπάτι από τον αποστολέα στον παραλήπτη.

12 Authentication Header: Χρησιμοποιείται προκειμένου να εξασφαλιστεί ότι τα δεδομένα δεν έχουν αλλαχτεί κατά τη μετάδοση του πακέτου στο μονοπάτι από τον αποστολέα στον παραλήπτη. Η μέθοδος που χρησιμοποιείται για αυτό είναι ένα κρυπτογραφημένο checksum κάποιων από τις επικεφαλίδες του IPv6 και των δεδομένων (payload).

13 Encapsulating Security Payload Header: Πρόκειται για την τελευταία επικεφαλίδα που μπορεί να υπάρξει στη σειρά των επικεφαλίδων επέκτασης που δεν έχει κωδικοποιηθεί (αν έχει επιλεγεί από τον κόμβο αποστολέα η κωδικοποίηση των δεδομένων που μεταδίδει). Χρησιμοποιείται προκειμένου να δείξει ότι ολόκληρο το πακέτο έχει κωδικοποιηθεί και παρέχει πληροφορία για τον κόμβο παραλήπτη για τη διαδικασία αποκρυπτογράφησης.

14 Destination Options Header: Αντιστοιχεί στο πεδίο IP Options του IPv4. Ο κόμβος παραλήπτης επεξεργάζεται αυτήν την επικεφαλίδα αφού παραλάβει το πακέτο. Προς το παρόν δε χρησιμοποιείται καθόλου αυτό το πεδίο και απλώς συμπληρώνεται με bits (padding).

Όλες οι επικεφαλίδες στο IPv6 έχουν το ίδιο μέγεθος και την ίδια μορφοποίηση. Η διαφορά τους βρίσκεται στο πεδίο που αφορά την επόμενη επικεφαλίδα. Η σειρά με την οποία μπορούν να εμφανίζονται οι επικεφαλίδες είναι αυστηρά καθορισμένη.



Σχήμα 2 Παράδειγμα χρήσης IPv6 Extension Headers στο IPv6 πακέτο

1.3 Αλλαγές των πεδίων της επικεφαλίδας του IPv6

Οι τέσσερις μεγάλες αλλαγές που εισήγαγε το IPv6 στα πεδία της επικεφαλίδας ενός πακέτου αφορούν:

- την ύπαρξη ετικετών ροής και προτεραιότητας των πακέτων (Flow Labels)
- την ύπαρξη κλάσεων κίνησης (Traffic Classes)

- την αλλαγή στη φιλοσοφία της κατάτμησης του πακέτου (Fragmentation)
- την ύπαρξη επικεφαλίδων επέκτασης (Extension Headers)

1.3.1 Ετικέτες ροής

Οι προδιαγραφές του IPv4 προκειμένου να πετύχει σαν πρωτόκολλο σε δίκτυο μεταγωγής πακέτων ήταν να μπορεί κάθε πακέτο να βρίσκει το δικό του δρόμο προς τον προορισμό, πρόκειται δηλαδή για πρωτόκολλο χωρίς σύνδεση. Το προφανές πλεονέκτημα είναι ότι δύο πακέτα από τον ίδιο αποστολέα προς τον ίδιο παραλήπτη μπορούν να ακολουθήσουν διαφορετικά μονοπάτια μέχρι να καταλήξουν στον κόμβο προορισμό. Αυτό αυξάνει την ευρωστία του δικτύου και την ευελιξία σε περίπτωση που κάποιο από τα μονοπάτια παρουσιάσει πρόβλημα λειτουργίας.

Παρ' όλα αυτά η αντιμετώπιση αυτή δεν είναι αποδοτική, ειδικά στην περίπτωση που τα πακέτα δεν είναι αυτόνομα αλλά πρόκειται για τμήματα από μία ροή δεδομένων μεταξύ εφαρμογών. Τότε ο κάθε δρομολογητής στο μονοπάτι αποστολέας – παραλήπτης θα πρέπει να επεξεργάζεται αυτό το πακέτο εισάγοντας επιπλέον καθυστέρηση που είναι γνωστή σαν latency. Αυτή η καθυστέρηση δε δημιουργούσε προβλήματα σε παραδοσιακές εφαρμογές όπως το ftp, το email κλπ αλλά στις νέες προηγμένες υπηρεσίες που απαιτούν μεταφορά αλληλεπιδραστικού ήχου και κινούμενης εικόνας κάτι τέτοιο επηρεάζει σημαντικά την απόδοσή τους.

Ένα ακόμη πρόβλημα της φιλοσοφίας αυτής του IPv4 είναι η αδυναμία να δρομολογηθεί συγκεκριμένος τύπος κίνησης σε μονοπάτια που το κόστος τους είναι χαμηλό. Για παράδειγμα η μεταφορά πακέτων ηλεκτρονικού ταχυδρομείου που δεν είναι εφαρμογή πραγματικού χρόνου και μπορεί να γίνει στο παρασκήνιο θα μπορούσε να γίνει πάνω από μία σύνδεση χαμηλής ταχύτητας άρα και κόστους, αφιερώνοντας έτσι τις συνδέσεις υψηλών ταχυτήτων (που έχουν και μεγάλο κόστος) σε εφαρμογές πραγματικού χρόνου.

Στο IPv6 αυτό το πρόβλημα έχει αντιμετωπιστεί και μία ροή πακέτων με ίδιους αποστολέα και παραλήπτη θεωρείται ότι ανήκουν στην ίδια ροή και φυσικά έχουν την ίδια τιμή στο πεδίο της ετικέτας ροής και προτεραιότητας.

1.3.2 Κλάση κίνησης

Στην πρώτη έκδοση του IPv6 στο RFC 1883 υπήρχε ορισμένο ένα πεδίο προτεραιότητας τεσσάρων bits όπου μπορούν να οριστούν δεκαέξι διαφορετικές κλάσεις προτεραιότητας. Αργότερα το πεδίο αυτό μετονομάστηκε σε κλάση κίνησης με συνολικό μέγεθος ένα byte.

Η ακριβής χρήση αυτού του πεδίου δεν έχει ακόμα καθοριστεί. Ο στόχος της ύπαρξης και χρήσης αυτού του πεδίου είναι να επιτρέπει στους κόμβους αποστολείς και στους δρομολογητές να μαρκάρουν τα πακέτα που επιθυμούν να έχουν διαφορετική επεξεργασία από τη συνήθη. Να έχουν δηλαδή ειδική επεξεργασία όσον αφορά το κόστος, το εύρος ζώνης και το χρόνο latency ή και κάποια άλλα χαρακτηριστικά των συνδέσεων πάνω από τις οποίες δρομολογούνται.

1.3.3 Κατάτμηση πακέτων

Όπως προαναφέρθηκε στο IPv6 η κατάτμηση των πακέτων επιτρέπεται μόνο μεταξύ του κόμβου αποστολέα και του κόμβου παραλήπτη, απλοποιώντας έτσι την επικεφαλίδα του πακέτου και μειώνοντας το χρόνο δρομολόγησης. Η δυνατότητα να γίνεται κατάτμηση των πακέτων στο IPv4 από οποιονδήποτε κόμβο του μονοπατιού είναι ιδιαίτερα επιζήμια

γιατί πιθανά είναι μία διαδικασία που θα πρέπει να γίνει αρκετές φορές καθώς επίσης η απώλεια ενός τμήματος (fragment) του πακέτου συνεπάγεται επανάληψη όλων των τμημάτων.

Για παράδειγμα έστω στο IPv4 ένας κόμβος μεταδίδει ένα πακέτο μεγέθους 1500 bytes προς έναν παραλήπτη στο διαδίκτυο. Το πακέτο μεταδίδεται πάνω από το τοπικό δίκτυο Ethernet προς το δρομολογητή του δικτύου. Ο δρομολογητής αυτός το δρομολογεί πάνω από τη σειριακή του σύνδεση με τον πάροχο διαδικτύου. Σε κάποιον ενδιάμεσο κόμβο της διαδρομής διαπιστώνεται ότι κάποια δικτυακή σύνδεση δεν μπορεί να χειριστεί πακέτα αυτού του μεγέθους. Τότε ο δρομολογητής που έχει αυτήν τη δικτυακή σύνδεση θα «σπάσει» το πακέτο σε μικρότερα ανάλογα με το μέγιστο μέγεθος πακέτου (Maximum Transmission Unit – MTU) για τη συγκεκριμένη δικτυακή σύνδεση. Έστω ότι το MTU είναι στη συγκεκριμένη περίπτωση 1280 bytes, οπότε ο δρομολογητής δημιουργεί δύο πακέτα, ένα με μέγεθος 1260 bytes (και 20 bytes της επικεφαλίδας = 1280 bytes) και ένα μεγέθους 240 bytes (και 20 bytes της επικεφαλίδας = 260 bytes). Αυτή η διαδικασία θα επαναληφθεί όσες φορές χρειαστεί και ο κόμβος παραλήπτης θα ενώσει τα διαφορετικά τμήματα για να φτιάξει το πακέτο.

Αυτό αρχικά θεωρήθηκε σαν πλεονέκτημα του σχεδιασμού του IPv4. Όμως θέτει σημαντικά θέματα απόδοσης στους δρομολογητές καθώς η διαδικασία στοιχίζει αρκετά τόσο σε επεξεργασία όσο και σε χρόνο.

Για να λυθεί αυτό το πρόβλημα θα πρέπει να είναι εκ των προτέρων γνωστό το MTU του μονοπατιού). Δύο είναι οι λύσεις σε αυτό το πρόβλημα. Η μία που χρησιμοποιείται και στο IPv4 είναι ο δρομολογητής να στέλνει ένα πακέτο με μέγεθος όσο είναι το MTU της σύνδεσής του στον παραλήπτη. Εάν κάποια στιγμή αυτό το πακέτο πρέπει να «σπάσει» τότε με χρήση του πρωτόκολλο Internet Control Message Protocol (ICMP) ο δρομολογητής που έχει το πρόβλημα θα ενημερώσει τον αρχικό δρομολογητή για το δικό του MTU. Η διαδικασία επαναλαμβάνεται μέχρι να βρεθεί το MTU του μονοπατιού. Η τεχνική αυτή λέγεται Path MTU Discovery. Η άλλη τεχνική είναι να υπάρχει ένα ελάχιστο μέγεθος MTU που να πρέπει να υποστηρίζεται από όλα τα είδη συνδέσεων.

Το IPv6 υποστηρίζει και τις δύο λύσεις. Αρχικά μάλιστα το ελάχιστο MTU ήταν 576 bytes, αργότερα έγινε 1500 και κατόπιν 1280. Ο λόγος των αλλαγών είναι ότι το ελάχιστο MTU ουσιαστικά ορίζει ποιες τεχνολογίες θα εγκαταλείπονταν ενώ παράλληλα είναι και ένας από τους παράγοντες που επηρεάζει την απόδοση ενός δικτύου. Για να αντιμετωπίσει αυτό το πρόβλημα το IPv6 ορίζει ότι όλοι οι IPv6 κόμβοι πρέπει να υλοποιούν την τεχνική του Path MTU Discovery. Με χρήση του “Don’t Fragment” bit θα αναγκάζονται οι ενδιάμεσοι δρομολογητές να επιστρέφουν ICMP μηνύματα λάθους αναφέροντας ότι το μέγεθος του πακέτου είναι μεγάλο. Οι κόμβοι που δε θα χρησιμοποιούν αυτήν την τεχνική θα πρέπει να χρησιμοποιούν το ελάχιστο μέγεθος για το MTU.

1.3.4 Οι επικεφαλίδες επέκτασης

Στο IPv4 το πρόβλημα με το πεδίο IP Options είναι ότι επειδή αλλάζει η μορφή των επικεφαλίδων θα πρέπει να αντιμετωπίζονται σαν ειδικές περιπτώσεις από τους δρομολογητές. Οι δρομολογητές όμως θα πρέπει να είναι βέλτιστοι για τα συνήθη πακέτα και άρα τα IPv4 χειρίζονται σαν ειδικές περιπτώσεις που αφήνονται να εξεταστούν αργότερα. Οι επικεφαλίδες επέκτασης στο IPv6 αντιμετωπίζουν αυτό το πρόβλημα γιατί έχουν μεταφερθεί από το κομμάτι της επικεφαλίδας του πακέτου στο κομμάτι των δεδομένων του πακέτου (payload). Έτσι αναγκάζουν τους δρομολογητές να αντιμετωπίζουν το ίδιο άμεσα ένα πακέτο με options και ένα πακέτο χωρίς options.

Εξαίρεση σε αυτό αποτελούν οι Hop By Hop options που θα πρέπει να επεξεργάζονται από όλους τους ενδιάμεσους δρομολογητές.

1.4 Η διευθυνσιοδότηση στο IPv6

Η αρχιτεκτονική διευθυνσιοδότησης στο IPv6 περιγράφεται στο RFC 2373 [10]και η οποία αποτελεί βελτίωση της αρχικά προτεινόμενης αρχιτεκτονικής που περιγράφονταν στο RFC 1883.
Η πρώτη βασική διαφορά που διαπιστώνει κανείς είναι ότι το μέγεθος μιας διεύθυνσης στο IPv6 είναι 128 bits σε σχέση με τα 32 bits στο IPv4. Αυτό δίνει το πλεονέκτημα μία IPv6 διεύθυνση να περιλαμβάνει αρκετά πεδία που μπορεί να βελτιώνουν τη δρομολόγηση. Επίσης στο IPv6 υπάρχουν τρεις κατηγορίες διευθύνσεων: unicast, multicast και anycast ενώ καταργήθηκαν οι διευθύνσεις broadcast [3]. Οι δύο πρώτες κατηγορίες ακολουθούν το ίδιο σκεπτικό όπως και στο IPv4 ενώ οι διευθύνσεις τύπου anycast [11] χρησιμοποιούνται για την αντιστοίχιση ενός συνόλου σταθμών σε μία διεύθυνση. Αποστολή ενός πακέτου σε διεύθυνση anycast σημαίνει την παράδοσή του σε ένα οποιοδήποτε σταθμό του συνόλου (κατά αναλογία με ATM). Μόνο οι δρομολογητές επιτρέπεται να έχουν τέτοιες διευθύνσεις, ενώ επιτρέπεται να χρησιμοποιούνται μόνο ως διεύθυνση αποστολής. Αντί των διευθύνσεων τύπου broadcast υπάρχει η multicast address “all nodes” και ένας σταθμός που ενδιαφέρεται να παρακολουθεί τα πακέτα που μεταφέρονταν με τα broadcast θα πρέπει να γραφτεί στο συγκεκριμένο multicast group, απαλλάσσοντας έτσι τους κόμβους που δεν ενδιαφέρονται για τα broadcasts από περιττή πληροφορία.
Η αναπαράσταση μίας IPv6 διεύθυνσης είναι της μορφής X:X:X:X:X:X:X:X όπου κάθε X είναι ένας δεκαεξαδικός αριθμός με μέγεθος 4 bits. Οι διευθύνσεις IPv6 χωρίζονται σε δύο τμήματα, το κομμάτι που αφορά το υποδίκτυο και το κομμάτι που αφορά τον κόμβο. Για αυτόν το λόγο είναι απαραίτητη για την περιγραφή μιας IPv6 διεύθυνσης και ένας αριθμός που δηλώνει πόσα bits είναι το πρώτο τμήμα της διεύθυνσης. Για παράδειγμα μία διεύθυνση της μορφής `1030:0:0:0:C9B4:FF12:48AA:1A2B/60` δηλώνει ότι τα πρώτα 60 bits της διεύθυνσης αφορούν το κομμάτι του υποδικτύου.
Το μοντέλο διευθυνσιοδότησης του IPv6 χρησιμοποιεί πολλά χαρακτηριστικά του αντίστοιχου μοντέλου του IPv4. Έτσι μία διεύθυνση unicast αντιστοιχεί σε ένα interface ενός κόμβου. Η διαφορά είναι ότι στο IPv6 δεν απαιτείται για τις point to point συνδέσεις να αφιερώνονται αποκλειστικές διευθύνσεις πετυχαίνοντας έτσι οικονομία διευθύνσεων. Επιπλέον στο IPv6 είναι δυνατόν να αντιστοιχιστεί μία διεύθυνση σε πολλά interfaces. Αυτό είναι σημαντικό πλεονέκτημα σε περιπτώσεις που ένας εξυπηρετητής έχει πολλά interfaces και είναι επιθυμητό το μοίρασμα του φόρτου (load balancing). Οι multicast και οι anycast διευθύνσεις μπορούν επίσης να αντιστοιχιστούν με πολλά interfaces. Τέλος ένα δικτυακό interface μπορεί να αντιστοιχιστεί με πολλές διευθύνσεις όλων των κατηγοριών.
Στο IPv6 δεν υπάρχουν κλάσεις διευθύνσεων όπως στο IPv4, το μοντέλο μοιάζει περισσότερο με το CIDR του IPv4, απλά τα πρώτα bits στο αριστερό μέρος της διεύθυνσης χαρακτηρίζουν τον τύπο της διεύθυνσης όπως φαίνεται στον πίνακα που ακολουθεί[12]:

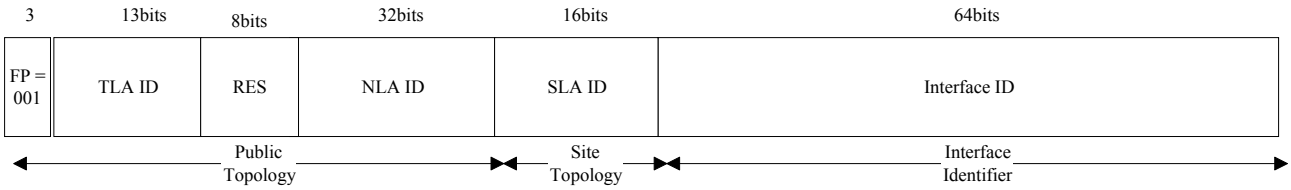
Πίνακας 1 Η σημασία των high order bits μιας IPv6 διεύθυνσης

Allocation	Format Prefix
Reserved Unassigned	0000 0000 0000 0001
Reserved for NSAP Reserved for IPX	0000 001 0000 010
Unassigned Unassigned Unassigned	0000 011 0000 1 0001
Aggregatable Global Unicast Address	001
Unassigned Unassigned Unassigned Unassigned Unassigned Unassigned Unassigned Unassigned Unassigned	010 011 100 101 110 1110 1111 0 1111 10 1111 1110 0
Link-local unicast address Site-local unicast address	1111 1110 10 1111 1111 11
Multicast address	1111 1111

Αυτά τα υψηλής τάξης (high order) bits λέγονται format prefix και χρησιμοποιούνται για τη δρομολόγηση. Έτσι αν τα 3 πρώτα υψηλής τάξης bits είναι ίσα με 001 τότε η διεύθυνση λέγεται Aggregatable global unicast address, εάν τα πρώτα 8 υψηλής τάξης bits είναι ίσα με 11111111 τότε πρόκειται για multicast διεύθυνση κλπ.
Ένα ακόμη χαρακτηριστικό της αρχιτεκτονικής διευθύνσεων στο IPv6 είναι ότι δεσμεύει κάποιες διευθύνσεις για διευθύνσεις τύπου NSAP και IPX ώστε δίκτυα βασισμένα στο OSI ή στο NetWare να μπορούν να ενσωματωθούν εύκολα στην αρχιτεκτονική του IPv6.
Η αρχιτεκτονική του IPv6 απαιτεί την ύπαρξη ενός interface identifier σε κάθε IPv6 unicast διεύθυνση. Το interface identifier είναι κάτι σαν τις 48 bits media access control (MAC) διευθύνσεις των καρτών δικτύου. Οι IPv6 διευθύνσεις των κόμβων βασίζονται στο IEEE EUI-64 πρότυπο [13] για τα interface identifiers. Από τις MAC διευθύνσεις δημιουργούνται οι 64 bits interface identifiers που χαρακτηρίζουν μοναδικά ένα δικτυακό interface. Αυτό σημαίνει ότι μπορούν να υπάρξουν 2^{64} διαφορετικά φυσικά interfaces, αριθμός που κρίνεται ικανοποιητικός.

1.4.1 Οι διευθύνσεις της μορφής Aggregatable Global Unicast

Η πιο κοινή μορφή μιας IPv6 διεύθυνσης είναι η Aggregatable Global Unicast Address που ξεκινά με το πρόθεμα 001. Αυτές οι διευθύνσεις θα αντικαταστήσουν τις κλάσεις διευθύνσεων A, B και C του IPv4. Η μορφοποίηση αυτών των διευθύνσεων περιγράφεται στο RFC 2374 [14] και φαίνεται στο ακόλουθο σχήμα:



Σχήμα 3 Η IPv6 Aggregatable Global Unicast Address

Τα πεδία της Aggregatable Global Unicast Address είναι:FP: Είναι το πρόθεμα (format prefix) μεγέθους 3-bit των IPv6 διευθύνσεων που για τη συγκεκριμένη μορφή ισούται με 001.

TLA ID: Τα αρχικά του σημαίνουν Top Level Aggregation Identifier και αποτελεί το υψηλότερο επίπεδο με πληροφορία δρομολόγησης μιας διεύθυνσης. Έχει μέγεθος 13 bits κάτι που σημαίνει ότι το πολύ 8192 διαφορετικές top-level δρομολογήσεις μπορούν να υπάρξουν. Το 6Bone έχει δεσμεύσει το δεκαεξαδικό αριθμό 0x1FFE.

RES: Πρόκειται για τα επόμενα 8 bits τα οποία είναι δεσμευμένα για μελλοντική χρήση. Μπορούν να χρησιμοποιηθούν είτε για επέκταση του προηγούμενου πεδίου (TLA) είτε του επόμενου πεδίου (NLA).

NLA ID: Τα αρχικά του σημαίνουν Next Level Aggregation Identifier και σκοπός του είναι να χρησιμοποιηθεί από οργανισμούς που ελέγχουν τα TLA Ids για να οργανώσουν το διαθέσιμο εύρος διευθύνσεων. Τέτοιοι οργανισμοί (που πιθανά μπορούν να είναι μεγάλοι πάροχοι διαδικτύου – ISPs) μπορούν να «μοιράσουν» το πεδίο των 24 bits προκειμένου να διευκολύνουν τη δική τους ιεραρχική διευθυνσιοδότηση. Για παράδειγμα να χρησιμοποιηθούν 2 bits για τον ορισμό 4 top level routes και να αποδοθεί το πεδίο διευθύνσεων των 20 bits σε άλλες οντότητες όπως μικρότερης κλίμακας πάροχοι δικτύου. Οι τελευταίοι μπορούν να επαναλάβουν την ίδια διαδικασία κλπ.

SLA ID: Τα αρχικά σημαίνουν Site Level Aggregation και χαρακτηρίζει το πεδίο διευθύνσεων που δίνεται στους οργανισμούς για να αναπτύξουν τις δικές τους δικτυακές υποδομές. Τα 16 bits αυτού του πεδίου μπορούν να χρησιμοποιηθούν για τη δημιουργία εσωτερικών δικτυακών υποδομών με τη δημιουργία υποδικτύων όπως και στο IPv4. Έτσι μπορούν να υπάρξουν 65535 διαφορετικά υποδίκτυα αν δεν υπάρξει διαχωρισμός των 16 bits, ενώ με χρήση των πρώτων 8 bits για high level routing δημιουργούνται 255 high level subnets καθένα με 255 υποδεέστερα υποδίκτυα.

Interface ID: Πρόκειται για τα 64 bits που χαρακτηρίζουν το (τα) δικτυακό interface ενός κόμβου.

1.4.2 Ειδικές κατηγορίες IPv6 διευθύνσεων

Εκτός της κατηγορίας των Aggregatable Global Unicast διευθύνσεων υπάρχουν ειδικές κατηγορίες που περιλαμβάνουν:

Unspecified Address: Πρόκειται για μία διεύθυνση της οποίας όλα τα bits ισούνται με 0 και χρησιμοποιείται όταν δεν υπάρχει έγκυρη διεύθυνση. Για παράδειγμα όταν ένας κόμβος βρίσκεται στη διαδικασία της εκκίνησης από το δίκτυο και δεν έχει λάβει ακόμα την κανονική του διεύθυνση.

Loopback Address: Πρόκειται για μία διεύθυνση της οποίας όλα τα bits εκτός του τελευταίου ισούνται με 0. Χρησιμοποιείται ακριβώς για τον ίδιο λόγο όπως και στο IPv4.

IPv4 Mapped IPv6 Address: Πρόκειται για διευθύνσεις που επιτρέπουν σε εφαρμογές IPv6 να λειτουργούν σε κόμβους που υποστηρίζουν και IPv4 και IPv6 για να επικοινωνούν με κόμβους που υποστηρίζουν μόνο IPv4. Θα παίξουν σημαντικό ρόλο κατά τη μετάβαση από το IPv4 στο IPv6 όπου θα πρέπει να συνυπάρξουν τα δύο δίκτυα με τις εφαρμογές τους. Αυτές οι διευθύνσεις δίνονται για παράδειγμα αυτόματα από τους εξυπηρετητές της υπηρεσίας DNS όταν μία IPv6 εφαρμογή ζητά την IPv6 διεύθυνση ενός κόμβου που υποστηρίζει μόνο IPv4. Τα 80 πρώτα bits της διεύθυνσης αυτής ισούνται με 0, τα επόμενα 16 ισούνται με 1 και τελευταία 32 είναι η IPv4 διεύθυνση.

IPv4 Compatible IPv6 Address: Πρόκειται για διευθύνσεις που θα χρησιμοποιηθούν επίσης στο μεταβατικό στάδιο από το IPv4 στο IPv6. Αυτές οι διευθύνσεις δίνονται σε κόμβους που υποστηρίζουν και IPv4 και IPv6 αλλά δεν έχουν γειτονικό δρομολογητή που να υποστηρίζει IPv6. Ένας άλλος κόμβος που υποστηρίζει IPv6 και θέλει να ανταλλάξει δεδομένα με τον πρώτο κόμβο θα ενσωματώσει το IPv6 datagram σε μία IPv4 επικεφαλίδα και θα το στείλει στην IPv4 Compatible IPv6 διεύθυνση δημιουργώντας έτσι αυτόματα κανάλια (automatic tunnel). Τα 96 πρώτα bits αυτής της διεύθυνσης ισούνται με 0.

Link Local Address: Πρόκειται για διευθύνσεις που χρησιμοποιούνται για να αριθμήσουν κόμβους σε μια δικτυακή σύνδεση. Τα πρώτα 10 bits του προθέματος αυτών των διευθύνσεων ειδοποιούν το δρομολογητή ώστε να αγνοεί τα πακέτα που περιέχουν αυτές τις διευθύνσεις είτε στα πεδία προορισμού είτε στα πεδία αποστολέα. Το επόμενο κομμάτι έχει και τα 54 bits να ισούνται με 0. Πιθανοί χρήστες τέτοιων διευθύνσεων είναι όσοι συνδέονται στα δίκτυα των οργανισμών του μέσω τηλεφωνικών γραμμών (Voice, ISDN κλπ).

Site Local Address: Πρόκειται για διευθύνσεις που μπορούν να χρησιμοποιηθούν από ένα οργανισμό χωρίς να υπάρχει η ανάγκη να αποκτήσουν ένα prefix μοναδικό. Αυτές οι διευθύνσεις έχουν πρόθεμα 10 bits ίσο με το δεκαεξαδικό αριθμό FEC0 που ειδοποιεί τους δρομολογητές ώστε να μη δρομολογούν αυτές τις διευθύνσεις στην εξωτερική σύνδεση με το διαδίκτυο. Ουσιαστικά πρόκειται για διευθύνσεις αντίστοιχες με τις NAT διευθύνσεις στο IPv4. Σε περίπτωση όμως που ο οργανισμός θελήσει να αποκτήσει έγκυρες IPv6 δίκτυο δεν απαιτείται η αλλαγή των διευθύνσεων όλων των σταθμών εργασίας όπως στο IPv4, παρά αλλαγή του Site Local προθέματος με ένα έγκυρο πρόθεμα.

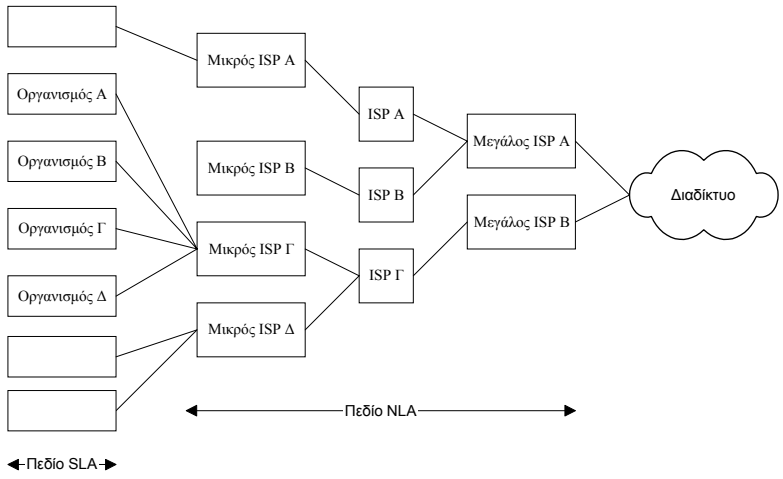
OSI NSAP and IPX addresses: Πρόκειται για ένα εύρος διευθύνσεων που έχει δεσμευτεί προκειμένου να χρησιμοποιηθεί για τη διαλειτουργικότητα με δίκτυα OSI και IPX.

Multicast addresses: Πρόκειται για διευθύνσεις που χρησιμοποιούνται από το μηχανισμό multicast προκειμένου να γίνει μετάδοση πακέτων σε πολλούς κόμβους ταυτόχρονα. Η φιλοσοφία τους είναι η ίδια με αυτή του IPv4, όμως καθώς δεν υπάρχει περιορισμός στο χώρο των διευθύνσεων multicast μπορούν να δημιουργηθούν πολλές ομαδοποιήσεις multicast σταθμών, να υπάρξουν είτε εσωτερικά ενός δικτύου είτε ενός υποδικτύου, είτε σε όλα το διαδίκτυο. Αυτές οι διευθύνσεις έχουν πρόθεμα 8 bits ίσο με τη μονάδα [15].

Anycast addresses: Είναι διευθύνσεις που απευθύνονται σε πολλούς κόμβους, αλλά μόνο ένας από αυτούς θα λάβει το πακέτο που στάλθηκε. Είναι πολύ χρήσιμες για υπηρεσίες όπως αυτή της ονοματολογίας (DNS) ή της κεντρικής ώρας (TS). Έτσι ένας κόμβος απευθύνεται με μία διεύθυνση στο σύνολο των εξυπηρετητών αυτών των υπηρεσιών και δεν θα διακοπεί η ομαλή λειτουργία της υπηρεσίας εξαιτίας της αποτυχίας ενός εξυπηρετητή.

1.5 Η δρομολόγηση στο IPv6

Κάνοντας χρήση της αρχιτεκτονικής διευθύνσεων που προαναφέρθηκε το IPv6 πετυχαίνει να απλουστεύσει αρκετά τη διαδικασία της δρομολόγησης πετυχαίνοντας τη μέγιστη δυνατή μείωση στους πίνακες δρομολόγησης των δρομολογητών. Επιπλέον πετυχαίνει να γνωρίζει όχι μόνο πώς θα μεταφέρει ένα πακέτο στον προορισμό του, αλλά να γνωρίζει και φυσικά που βρίσκεται αυτός ο οργανισμός. Ο μηχανισμός που ακολουθήθηκε είναι αυτός που προτάθηκε στο RFC 2008 [16] που ανέφερε τα προβλήματα δρομολόγησης στο διαδίκτυο καθώς και κάποιες τεχνικές που μπορούσαν να περιορίσουν το πρόβλημα. Η βασική οδηγία αυτού του RFC ήταν η μετάβαση των δικτύων IPv4 από την κατάσταση «ιδιοκτησίας διευθύνσεων» στην κατάσταση «δανεισμού διευθύνσεων». Πιο συγκεκριμένα πρότεινε στους οργανισμούς αντί να ζητούν ένα πεδίο διευθύνσεων από τις εξουσιοδοτημένες αρχές (πχ RIPE, ARIN κλπ) να το δανείζονται από τους διάφορους παρόχους (ISPs). Με αυτόν τον τρόπο πετυχαίνεται μείωση των διαφημιζόμενων δρομολογήσεων (aggregation). Το μεγάλο πρόβλημα που εισήγαγε κάτι τέτοιο είναι ότι οι οργανισμοί θα ήταν αναγκασμένοι να ρυθμίσουν ξανά το δίκτυό τους εάν αποφάσιζαν να αλλάξουν πάροχο.
Αυτό ακριβώς πετυχαίνει και το IPv6 και μάλιστα χωρίς να παρουσιάζει τα προβλήματα της λύσης του RFC 2008. Το συνολικό εύρος των IPv6 διευθύνσεων έχει κατανεμηθεί γεωγραφικά στους μεγάλους πάροχους μέσω του πεδίου NLA ID. Αυτοί μπορούν να χρησιμοποιήσουν μέρος αυτού του πεδίου για να διευκολύνουν τη δική τους ιεραρχική διευθυνσιοδότηση και να «μοιράσουν» ένα μέρος από το πεδίο διευθύνσεων σε μικρότερους ISPs. Αυτή η διαδικασία μπορεί να επαναληφθεί αρκετές φορές μέχρι να φτάσουμε στους οργανισμούς που μπορούν να συνεχίσουν την ιεραρχική διευθυνσιοδότηση μέσω του πεδίου SLA ID.



Σχήμα 4 Η ιεραρχική δρομολόγηση πετυχαίνει route aggregation στο IPv6

Στο πρωτόκολλο IPv6 καταργήθηκε η έννοια της κλάσης των διευθύνσεων. Αυτό ήταν πολύ φυσιολογικό αφού ακόμα και στο IPv4 με την τεχνική CIDR είχε στην ουσία καταργηθεί η χρήση των κλάσεων A,B,C. Έτσι οι IPv6 διευθύνσεις επιτρέπεται να χαρακτηρίζονται με όσο το δυνατόν λιγότερη μάσκα bits διευκολύνοντας στο μέγιστο βαθμό τη δρομολόγηση αφού οι κεντρικοί δρομολογητές δε θα χρειάζεται να έχουν αναλυτικά όλους τους αριθμούς των δικτύων προκειμένου να δρομολογήσουν τα πακέτα τους.

1.5.1 Τα πρωτόκολλα δρομολόγησης

Αυτό που δεν έχει αλλάξει πολύ στη μετάβαση από το IPv4 στο IPv6 είναι η φιλοσοφία των πρωτοκόλλων δρομολόγησης. Αυτό είναι συνέπεια του γεγονότος ότι περιορίστηκε το μέγεθος των καταχωρήσεων στους πίνακες δρομολόγησης και επομένως οι υπάρχοντες αλγόριθμοι δρομολόγησης απαιτούν ελάχιστη τροποποίηση για να επιτευχθεί βέλτιστη απόδοση. Οι περισσότερες ρυθμίσεις μάλιστα απλώς επεκτείνουν τα υπάρχοντα πρωτόκολλα στο να χειρίζονται τις διευθύνσεις IPv6 που έχουν μεγαλύτερο μέγεθος ενώ παράλληλα καταργήθηκαν διαδικασίες που αντάλλασσαν πληροφορίες πιστοποίησης (το authentication γίνεται από την αντίστοιχη επικεφαλίδα του IPv6 πακέτου) και πληροφορίες που αφορούν επικεφαλίδες του IPv4 πακέτου που έχουν καταργηθεί (όπως η επικεφαλίδα Type of Service).
Έτσι για τη δρομολόγηση εντός του δικτύου ενός οργανισμού (Interior Routing) έχουν ήδη σχεδιαστεί το Distance Vector πρωτόκολλο RIPng που περιγράφεται στο RFC 2080 [17], ενώ είναι σε φάση εξέλιξης το Link State πρωτόκολλο OSPF [18]. Τέλος για τη δρομολόγηση στο εξωτερικό του δικτύου ενός οργανισμού (Exterior Routing) είναι σε φάση εξέλιξης το πρωτόκολλο BGP στο οποίο έχουν γίνει οι κατάλληλες προσθήκες προκειμένου να υποστηρίζει πολλαπλά δικτυακά πρωτόκολλα [19].

1.6 Η ασφάλεια στο IPv6

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπόψη του κανένα θέμα ασφάλειας λόγω της φύσης του δικτύου (επιδίωκε να συνδέσει ακαδημαϊκά ιδρύματα). Μετά την τεράστια εξάπλωση που γνώρισε το διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε ένα από τα πιο απαιτητικές ανάγκες στο διαδίκτυο. Για να καλύψει τις ανάγκες αυτές η IETF δημιούργησε το IP Security Working Group με στόχο να σχεδιάσει μία αρχιτεκτονική ασφαλείας και τα αντίστοιχα πρωτόκολλα ώστε να παρέχεται ασφάλεια βασισμένη στην κρυπτογραφία για το IPv6 πρωτόκολλο [20]. Η αρχιτεκτονική αυτή είναι γνωστή και ως IPsec και περιγράφεται στο RFC 1825 [21]. Καθώς προχωρούσαν οι εργασίες διαπιστώθηκε ότι η προτεινόμενη αρχιτεκτονική ασφαλείας για το IPv6 μπορούσε να ενσωματωθεί και στο IPv4 και έτσι το τελευταίο ορίστηκε σαν επιπλέον στόχος. Πρέπει να τονιστεί ότι αυτή η αρχιτεκτονική αφορά το πρωτόκολλο IP και δεν προτείνει μία αρχιτεκτονική ασφάλειας για το διαδίκτυο. Ορίζει τις υπηρεσίες ασφάλειας που μπορούν να χρησιμοποιηθούν στο επίπεδο δικτύου τόσο από το IPv4 όσο και από το IPv6. Η υλοποίηση βέβαια αυτών των υπηρεσιών διαφέρει, αφού στο IPv4 θα πρέπει να υπάρχουν οι κατάλληλες AH και ESP επικεφαλίδες στο πεδίο IP Options, κάτι που είναι αρκετά πιο δύσκολο σε σχέση με το IPv6 που αυτές οι λειτουργίες υλοποιούνται εύκολα γιατί έλαβε υπόψη του αυτές τις απαιτήσεις στο σχεδιασμό του.

1.6.1 Η ασφάλεια που ορίζει το IPsec

Το IPsec πρότυπο ορίζει τους μηχανισμούς ασφάλειας που μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξαρτήτως έκδοσης ώστε να επιτυγχάνεται ασφάλεια στο επίπεδο δικτύου. Ένα σύστημα χρησιμοποιεί το IPsec για να απαιτήσει από τους κόμβους που επικοινωνεί να κάνουν χρήση συγκεκριμένων αλγορίθμων και πρωτοκόλλων ασφαλείας. Το IPsec παρέχει και τα εργαλεία με τα οποία ένα σύστημα μπορεί να διαπραγματευτεί με άλλα συστήματα για να καταλήξουν για παράδειγμα σε κοινή χρήση ενός αλγορίθμου κωδικοποίησης.
Οι υπηρεσίες που μπορούν να θεωρηθούν μέρος του IPsec περιλαμβάνουν:

1 Έλεγχο πρόσβασης: Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί τον κατάλληλο κωδικό. Υπάρχουν διάφορα πρωτόκολλα ασφάλειας που μπορούν να χρησιμοποιηθούν για να ορίσουν μία ασφαλή ανταλλαγή κλειδιών.

2 Ακεραιότητα δεδομένων: Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου χωρίς την ανάγκη να ελεγχθεί άλλο πακέτο πριν ή μετά από το πακέτο που πρέπει να ελεγχθεί. Αυτό μπορεί να επιτευχθεί με χρήση τεχνικών hashing.

3 Πιστοποίηση του αποστολέα: Είναι δυνατή η πιστοποίηση του αποστολέα με χρήση των κατάλληλων αλγορίθμων ψηφιακών υπογραφών.

4 Προστασία εναντίον επιθέσεων τύπου packet replay: Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις όπου ο επιτιθέμενος προσπαθεί να βλάψει τη διαθεσιμότητα του συστήματος, υποκλέπτοντας ένα πακέτο και στέλνοντάς το πολλές φορές στον αποστολέα.

5 Κωδικοποίηση των δεδομένων: Παρέχονται μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων.

6 Εξασφάλιση απορρήτου της ροής των δεδομένων: Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων ώστε ο επιτιθέμενος να μην μπορεί να βγάλει συμπεράσματα παρακολουθώντας ένα προς ένα τα πακέτα (που μπορεί να είναι κωδικοποιημένα).

1.7 Αυτόματη ρύθμιση των σταθμών

Ένα από τα σοβαρότερα μειονεκτήματα του IPv4 όπως αναφέρθηκε σε προηγούμενο κεφάλαιο είναι η πολυπλοκότητα των ρυθμίσεων που απαιτούνται από το διαχειριστή του δικτύου προκειμένου να συνδέσει ένα σταθμό εργασίας στο διαδίκτυο. Παρ' όλο που προτάθηκαν διάφοροι μηχανισμοί (όπως τα BOOTP και DHCP πρωτόκολλα) οι ρυθμίσεις του IP εξακολουθούν να παραμένουν ένα σοβαρό πρόβλημα.
Ένας από τους πιο σημαντικούς στόχους για το IPng ήταν να υποστηρίξει την αρχή του "Plug and Play" ώστε να είναι δυνατή η σύνδεση ενός σταθμού εργασίας στο IPv6 δίκτυο και η λειτουργία του χωρίς να απαιτείται ανθρώπινη παρέμβαση. Το IPv6 χρησιμοποιεί τους δύο μηχανισμούς που «κληρονόμησε» από το IPv4 (BOOTP και DHCP) οι οποίοι ανήκουν όμως στην κατηγορία των statefull αυτόματων ρυθμίσεων, δηλαδή θα πρέπει σε κάποιον εξυπηρετητή να υπάρχουν πλήρως ορισμένες όλες οι ρυθμίσεις για κάθε σταθμό εργασίας, η πολιτική με την οποία δίνονται οι διευθύνσεις στους σταθμούς εργασίας, το χρονικό διάστημα για το οποίο μπορεί να δοθεί σε έναν

σταθμό εργασίας μία διεύθυνση κλπ. Το πρόβλημα με τις statefull αυτόματες ρυθμίσεις είναι ότι η συντήρηση και η διαχείρισή τους είναι αρκετά πολύπλοκη για το διαχειριστή του δικτύου. Είναι προτιμότερη η λύση των stateless αυτόματων ρυθμίσεων, κάποιων μηχανισμών δηλαδή που να επιτρέπουν στον κάθε κόμβο να ανακαλύπτει μόνος του τις ρυθμίσεις IP που θα πρέπει να έχει χωρίς να απαιτείται να ρωτήσει κάποιον εξυπηρετητή για αυτήν την πληροφορία.
Ένας σταθμός εργασίας μπορεί εύκολα να μάθει τη διεύθυνση του επιπέδου σύνδεσης και αφού αυτή είναι μοναδική (για τις περισσότερες αρχιτεκτονικές) να σχηματίσει την IEEE EUI-64 διεύθυνση και επομένως το κομμάτι host ID της διεύθυνσης IPv6. Με αυτόν τον τρόπο το μόνο που χρειάζεται είναι και η IPv6 διεύθυνση του υποδικτύου του. Για να το μάθει αυτό απλώς ρωτάει τον πλησιέστερο δρομολογητή που είναι διαθέσιμος και έτσι έχει πλέον σχηματίσει την IPv6 διεύθυνσή του [22],[23].

1.8 Μεθοδολογία μετάβασης από τα δίκτυα IPv4 στα δίκτυα IPv6

Είναι φανερό ότι δεν είναι δυνατή η άμεση ή η ταυτόχρονη μετάβαση του διαδικτύου στο πρωτόκολλο IPv6. Κάτι τέτοιο θα δημιουργούσε πολλά προβλήματα στα εκατομμύρια χρηστών και θα απαιτούσε τη συνεργασία των διαχειριστών δικτύου για την επίλυσή των προβλημάτων, την αναβάθμιση του λογισμικού τόσο στις δικτυακές συσκευές τους όσο και στους κόμβους τους. Επίσης η αναβάθμιση αυτή προϋποθέτει και αντικατάσταση εξοπλισμού που δεν θα μπορούσε να υποστηρίξει τη νέα κατάσταση αυξάνοντας υπερβολικά το κόστος.
Η μετάβαση λοιπόν στο IPv6 μπορεί και πρέπει να γίνει σταδιακά. Θα υπάρξει αναγκαστικά ένα μεγάλο χρονικό διάστημα όπου τα δύο πρωτόκολλα δικτύου (IPv4 και IPv6) θα συνυπάρχουν. Αυτός ήταν άλλωστε και ένας από τους στόχους του IPv6: η σταδιακή αναβάθμιση των κόμβων, η σταδιακή εξάπλωση των IPv6 δικτύων, η ευκολία στη διευθυνσιοδότηση των IPv4 κόμβων που αναβαθμίζονται ώστε να υποστηρίζουν και IPv6 και το χαμηλό κόστος της μετάβασης των υπαρχόντων IPv4 συστημάτων σε IPv6. Έτσι στο διάστημα της μετάβασης οι διαχειριστές θα προχωρούν σταδιακά στην αντικατάσταση του λογισμικού καταρχήν στις δικτυακές τους συσκευές και κατόπιν στους κόμβους τους. Παράλληλα παρωχημένος εξοπλισμός θα αντικαθίστανται από νέας τεχνολογίας που θα υποστηρίζει εξαρχής το IPv6.
Οι περισσότερες τεχνικές μετάβασης βασίζονται στην τεχνική της ενθυλάκωσης (protocol tunneling) και τη δημιουργία νησίδων IPv6. Τα πακέτα IPv6 ενθυλακώνονται σε πακέτα IPv4 και μεταδίδονται μεταξύ των νησίδων (επειδή μεσολαβούν IPv4 κόμβοι).

Στην αρχή της μετάβασης αυτή η τεχνική θα είναι πολύ δημοφιλής μέχρι να μεταβούν ένας μεγάλος αριθμός δικτύων στο IPv6. Κατόπιν η επικοινωνία μεταξύ των δικτύων IPv6 θα γίνεται κανονικά χωρίς ενθυλάκωση και η τεχνική αυτή θα χρησιμοποιείται μόνο για τα δίκτυα IPv4 που δεν έχουν μεταβεί στο IPv6.
Μία άλλη κατηγορία τεχνικών βασίζεται στην παράλληλη υποστήριξη των δύο πρωτοκόλλων (IPv4 και IPv6). Προϋπόθεση είναι ότι τόσο οι δρομολογητές όσο και οι κόμβοι θα μπορούν να λειτουργούν και με τις δύο αρχιτεκτονικές πρωτοκόλλων κάτι που είναι ιδιαίτερα δύσκολο τουλάχιστον στην αρχή της μετάβασης.
Πολύ χρήσιμες κατά τη διάρκεια της μετάβασης θα είναι οι διευθύνσεις συμβατότητας (Compatibility Addresses) που έχει ορίσει το IPv6. Υπάρχουν δύο τέτοιου τύπου διευθύνσεις:

1 Οι IPv4-compatible IPv6 διευθύνσεις που χρησιμοποιούνται από δρομολογητές ή κόμβους που υποστηρίζουν το IPv6 και πρέπει να επικοινωνήσουν «πάνω» από μία υποδομή που υποστηρίζει IPv4 (δεν υπάρχουν δρομολογητές που να υποστηρίζουν IPv6 στο υποδίκτυο). Τότε οι συσκευές στα άκρα της IPv4 υποδομής χρησιμοποιούν αυτού του τύπου τις unicast διευθύνσεις που περιέχουν την IPv4 διεύθυνση στα τελευταία 32 bits ενώ όλα τα προηγούμενα 96 bits είναι ίσα με 0. Χρησιμοποιούνται με την τεχνική των αυτομάτων καναλιών.

2 Οι IPv4-mapped IPv6 διευθύνσεις που χρησιμοποιούνται από τους κόμβους που υποστηρίζουν μόνο IPv4 και όχι IPv6. Ένας IPv6 κόμβος χρησιμοποιεί μία τέτοια διεύθυνση για να επικοινωνήσει με έναν κόμβο που υποστηρίζει μόνο IPv4. Αυτή τη διεύθυνση την επιστρέφει στον IPv6 κόμβο η υπηρεσία ονοματολογίας για τους IPv4 κόμβους. Αυτού του τύπου οι unicast διευθύνσεις έχουν τα πρώτα 80 bits ίσα με το 0, τα επόμενα 16 ίσα με 1 και τα τελευταία 32 bits περιέχουν την IPv4 διεύθυνση.

1.9 Σύγκριση των χαρακτηριστικών των δύο πρωτοκόλλων

Συγκρίνοντας τα δύο πρωτόκολλα γίνεται φανερό ότι η μετάβαση στο IPv6 είναι απλώς ζήτημα χρόνου. Ουσιαστικά η μετάβαση θα «ανοίξει» και το δρόμο ώστε το IP να αποτελέσει το παγκόσμιο δίκτυο πάνω στο οποίο θα αναπτυχθούν και να ολοκληρωθούν όλες οι υπόλοιπες υπηρεσίες που αυτή τη στιγμή βασίζονται σε πρωτόκολλα που δεν έχουν πετύχει την ανάπτυξη του IP. Το IPv6 δεν αποτελεί μόνο τη λύση στο πρόβλημα της έλλειψης IPv4 διευθύνσεων. Πρόκειται για ένα πρωτόκολλο που έχει σχεδιαστεί από την αρχή έχοντας λάβει υπόψη του τις εμπειρίες από την εικοσαετή χρήση του IPv4, τις απαιτήσεις των υπηρεσιών που αναπτύχθηκαν και στηρίχτηκαν στο IPv4, και την ανάγκη να υπάρξει ένα πρωτόκολλο πάνω από το οποίο θα μπορούν να αναπτυχθούν χωρίς προβλήματα οι νέες υπηρεσίες. Συνδυάζει την απλότητα, την ευκολία στην εγκατάσταση, την ασφάλεια, την υποστήριξη των κινητών σταθμών και την ποιότητα υπηρεσιών.

2 Η υποστήριξη Mobile Networking στο IPv6

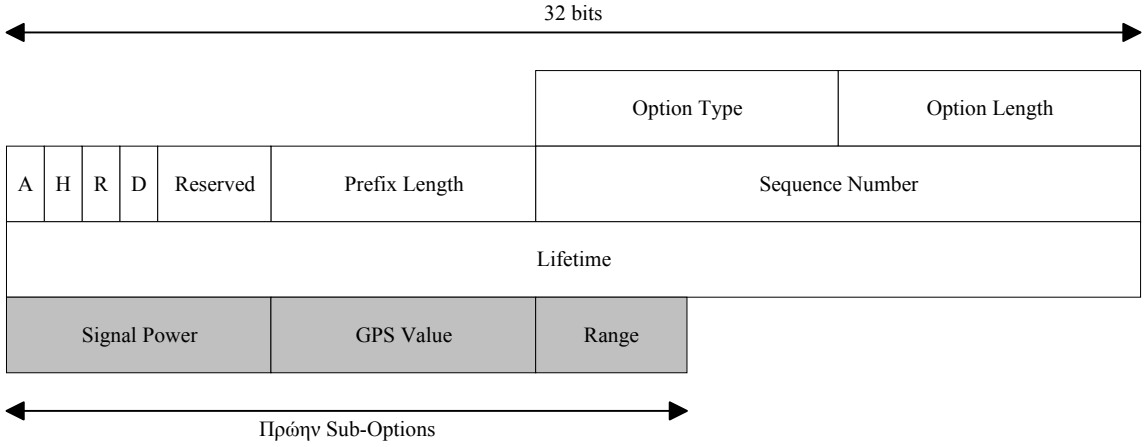
Για την υποστήριξη των κινητών χρηστών το IPv6 υιοθέτησε το βασικό κορμό του Mobile IP που είχε σχεδιαστεί για το IPv4. Η εφαρμογή του Mobile IP μάλιστα στο IPv6 παρουσιάζει σημαντικά πλεονεκτήματα λόγω των μηχανισμών του τελευταίου σε θέματα όπως τη δυνατότητα αυτόματης ρύθμισης των σταθμών εργασίας. Επιπλέον είναι σε φάση σχεδιασμού διάφορες επεκτάσεις του Mobile IP και μηχανισμών του IPv6 ώστε η ολοκλήρωση να είναι η καλύτερη δυνατή [25]
Σε αναλογία με το Mobile IP για το IPv4 κάθε κινητός σταθμός έχει μία μόνιμη διεύθυνση που λέγεται home address και η οποία παραμένει σταθερή ανεξάρτητα από τα δίκτυα που συνδέεται ο κινητός κόμβος. Το υποδίκτυο που αντιστοιχεί η home address λέγεται home subnet. Οποιοσδήποτε κόμβος επικοινωνεί με τον κινητό κόμβο λέγεται correspondent node. Ο κινητός κόμβος όταν δεν βρίσκεται στο home subnet χρησιμοποιεί την care-of address που είναι μία κανονική IPv6 διεύθυνση που λαμβάνει με το μηχανισμό της αυτόματης ρύθμισης στο foreign subnet. Ο συνδυασμός της home address με την care-of address και το χρόνο που σημειώνει τη χρονική διάρκεια που είναι έγκυρος αυτός ο συνδυασμός λέγεται binding. Όταν ο κινητός κόμβος βρίσκεται εκτός του home subnet, ο δρομολογητής του home subnet λέγεται home agent και συντηρεί την εγγραφή με το binding του κινητού κόμβου. Επίσης δεσμεύει όλα τα πακέτα που απευθύνονται στη home address του κινητού κόμβου και τα δρομολογεί μέσω καναλιών στην care-of address του κινητού κόμβου. Όταν ο correspondent κόμβος μάθει την care-of address του κινητού κόμβου μπορεί να στείλει σε αυτόν κατευθείαν τα πακέτα χωρίς την παρέμβαση του home agent με χρήση της IPv6 επικεφαλίδας δρομολόγησης (IPv6 Routing Header).
Μία πολύ σημαντική λειτουργία προκειμένου η υποστήριξη των κινητών κόμβων να είναι αξιόπιστη είναι η όσο το δυνατόν γρηγορότερη ενημέρωση των κόμβων για την τρέχουσα care-of διεύθυνση του κινητού κόμβου. Έτσι αποφεύγεται ένα από τα σημαντικότερα προβλήματα δρομολόγησης που είναι γνωστό σαν triangle routing. Το πρόβλημα δημιουργείται όταν κάθε correspondent κόμβος θα πρέπει να στείλει τα πακέτα του στο home agent και αυτός να τα προωθήσει στον κινητό κόμβο, ο οποίος απαντά απευθείας στον correspondent κόμβο. Αυτό έχει σαν αποτέλεσμα να αυξάνεται ο φόρτος του δικτύου, να παρουσιάζεται σημαντική καθυστέρηση στην παράδοση των πακέτων και να αφιερώνει μεγάλο μέρος της επεξεργαστικής ισχύος του ο home agent. Για αυτό το λόγο το IPv6 εισήγαγε δύο νέες Destination Options που λέγονται Binding Update και Binding Acknowledgement οι οποίοι χρησιμοποιούνται από το Mobile IPv6. Με αυτόν τον τρόπο μεταφέρεται η πληροφορία για το τρέχον binding στους IPv6 κόμβους. Κάθε IPv6 κόμβος διαθέτει ένα μέρος της μνήμης του για να κάνει caching αυτών των δεδομένων. Πριν στείλει κάποια πακέτα κάθε κόμβος ελέγχει την cache με τα bindings και αν υπάρχει κάποιο binding για τη συγκεκριμένη διεύθυνση προορισμού τότε ο κόμβος δρομολογεί το πακέτο κατευθείαν στον κινητό κόμβο στην care-of διεύθυνσή του. Η δρομολόγηση χρησιμοποιεί την επικεφαλίδα IPv6 Routing αντί κάποια ενθυλάκωση ώστε να μην αυξηθεί το κόστος λόγω της αύξησης του μήκους του πακέτου. Η care-of διεύθυνση δηλαδή είναι η διεύθυνση προορισμού για το πακέτο και η home διεύθυνση είναι η διεύθυνση στη routing επικεφαλίδα. Όταν ο κινητός κόμβος λάβει το πακέτο θα επεξεργαστεί την επικεφαλίδα routing και το πακέτο θα παραδοθεί στο επίπεδο μεταφοράς με διεύθυνση τη home διεύθυνση του κινητού κόμβου.
Για την απλοποίηση της λειτουργίας του home agent οι κινητοί κόμβοι μπορούν να ανακαλύπτουν μόνοι τους τη διεύθυνση του home agent με το να στέλνουν ένα Binding Update στην IPv6 διεύθυνση τύπου anycast στο home subnet. Αυτό το πακέτο θα

παραληφθεί από έναν και μόνο δρομολογητή ο οποίος θα απαντήσει με Binding Acknowledgement στο οποίο θα αναφέρει ότι το μήνυμα Binding Update απορρίφθηκε. Στο πακέτο αυτό θα περιλαμβάνει τη δική του unicast IPv6 διεύθυνση. Κατόπιν ο κινητός κόμβος επαναλαμβάνει το Binding Update μη χρήση της unicast διεύθυνσης του δρομολογητή.

3 Προτάσεις για επεκτάσεις στο Ipv6

Αν και το πρωτόκολλο IPv6 δεν έχει ολοκληρωθεί και τεκμηριωθεί πλήρως υπάρχουν κάποια θέματα τα οποία μπορούν να βελτιωθούν ώστε να ανταποκρίνονται καλύτερα στις ανάγκες τις οποίες καλείται να εξυπηρετήσει το συγκεκριμένο πρωτόκολλο.
Μία από αυτές τις ανάγκες αφορά το Mobile IP στο IPv6. Προκειμένου να υποστηριχτεί όσο το δυνατόν καλύτερα η ποιότητα υπηρεσίας στους κινητούς χρήστες θα πρέπει η μετάβαση του κινητού κόμβου από ένα δίκτυο σε κάποιο άλλο να διαρκεί το λιγότερο δυνατό χρόνο. Αυτή τη στιγμή σύμφωνα με τις προδιαγραφές που έχουν οριστεί για το Mobile IPv6 ο κινητός κόμβος μπορεί να χρησιμοποιεί περισσότερες της μίας διευθύνσεις τη στιγμή που αλλάζει δίκτυο. Τόσο ο κινητός κόμβος όσο και ο δρομολογητής στο δίκτυο που φιλοξενούνταν ο κινητός κόμβος έχουν μηχανισμούς με τους οποίους διαπιστώνουν ότι ο κινητός κόμβος έχει αλλάξει δίκτυο. Οι μηχανισμοί αυτοί βασίζονται στο πρωτόκολλο του Neighborhood Discovery το οποίο χρησιμοποιεί ICMPv6 πακέτα με κατάλληλο περιεχόμενο ώστε να διαπιστωθεί ότι ο ζητούμενος κόμβος δεν είναι πλέον διαθέσιμος στο συγκεκριμένο υποδίκτυο. Στην ουσία μόλις οι κόμβοι λάβουν το μήνυμα Destination Unreachable θεωρούν ότι ο κόμβος τον οποίο αναζητούν έχει αλλάξει δίκτυο.
Αυτό το χρονικό διάστημα μπορεί να είναι αποδεκτό για εφαρμογές που δεν έχουν υψηλές απαιτήσεις όπως η υπηρεσία του ηλεκτρονικού ταχυδρομείου αλλά μπορεί να αποδειχτεί μοιραίο για εφαρμογές πραγματικού χρόνου που έχουν προκαθορισμένες απαιτήσεις για τις μετρικές jitter, delay.
Μία λύση στο παραπάνω πρόβλημα μπορεί να αποτελέσει η χρήση του Global Positioning System (GPS). Απαραίτητη προϋπόθεση για την προτεινόμενη λύση είναι οι δρομολογητές που έχουν οριστεί να υποστηρίζουν τους κινητούς κόμβους και οι ίδιοι οι κινητοί κόμβοι θα πρέπει να διαθέτουν GPS terminal.
Μέχρι στιγμής ο αλγόριθμος που περιγράφεται στο Mobile IPv6 αναφέρει τα ακόλουθα: Όταν ο κινητός κόμβος συνδέεται σε ένα δίκτυο ανταλλάσσει μηνύματα τύπου Router Discovery και Router Advertisement με το δρομολογητή του υποδικτύου για να μάθει το πρόθεμα του δικτύου του και να υπολογίσει τη νέα IPv6 διεύθυνσή του για το συγκεκριμένο υποδίκτυο. Ο κινητός κόμβος επιλέγει από τη λίστα με τις care-of διευθύνσεις του μία να είναι η primary care-of διεύθυνση την οποία διαφημίζει τόσο στο home agent όσο και στους correspondent κόμβους. Κατόπιν ο κινητός κόμβος ανταλλάσσει τόσο με το δρομολογητή του στο νέο υποδίκτυο όσο και με το home agent και με τους correspondent κόμβους μηνύματα Binding Update. Τα μηνύματα αυτά στην αρχή ανταλλάσσονται μεγάλο ρυθμό ο οποίος βαίνει μειούμενος προς μία ελάχιστη τιμή όσο η care-of διεύθυνση του κινητού κόμβου παραμένει σταθερή.
Η προτεινόμενη επέκταση βασίζεται στην προσθήκη πληροφορίας στα μηνύματα Binding Update μεταξύ του κινητού κόμβου και των δρομολογητών των δικτύων που είναι συνδεμένος ο κινητός κόμβος. Συγκεκριμένα προτείνεται η ανταλλαγή πληροφορίας που αφορά την ισχύ του σήματος που λαμβάνει ο κινητός κόμβος, οι GPS συντεταγμένες του και η εμβέλεια του κινητού κόμβου σε σχέση με τις GPS συντεταγμένες. Με το συνδυασμό αυτών των δύο παραμέτρων ο κινητός κόμβος μπορεί εύκολα να διαπιστώσει ότι σύντομα ο προκαθορισμένος του δρομολογητής δε θα είναι

προσπελάσιμος και άρα θα σύντομα θα πρέπει να αλλάξει δίκτυο και προκαθορισμένο δρομολογητή. Έτσι μπορεί να επιλέξει με βάση τις παράμετρες που έχει συγκεντρώσει από τα υπόλοιπα δίκτυα στα οποία είναι συνδεμένος ποιος θα είναι ο επόμενος προκαθορισμένος δρομολογητής και η primary care-of διεύθυνση. Κατόπιν τούτου ο κινητός κόμβος ενημερώνει το home agent και τους correspondent nodes για τη νέα care-of διεύθυνσή του.
Τα πλεονεκτήματα αυτής της επέκτασης είναι καταρχήν ότι μειώνεται στο ελάχιστο ο χρόνος που απαιτείται για την ενημέρωση των ενδιαφερόμενων κόμβων για την care-of διεύθυνση του κινητού κόμβου. Επιπλέον ελαχιστοποιείται ο φόρτος του δικτύου αφού δεν απαιτούνται οι συχνές ενημερώσεις των κόμβων με Binding Update και Binding Acknowledgment μηνύματα.
Πρέπει να τονιστεί ότι για τις περιπτώσεις που η πληροφορία ισχύος σήματος δεν είναι δυνατή θα πρέπει ο κινητός κόμβος και ο προκαθορισμένος δρομολογητής του δικτύου που φιλοξενείται να διαπιστώσουν την ανάγκη αλλαγής δικτύου από τις παράμετρες GPS και μόνον. Για αυτό το λόγο θα πρέπει να έχει ελεγχθεί η παράμετρος που αφορά την εμβέλεια του δικτύου.
Επιπλέον ο κινητός κόμβος θα πρέπει να ελέγχει εάν το νέο υποδίκτυο στο οποίο συνδέεται είναι διαφορετικό από το προηγούμενο με απλό έλεγχο του προθέματος δικτύου. Αν τα δύο προθέματα είναι ίδια τότε ο κινητός κόμβος απλώς αλλάζει κόμβο σε επίπεδο σύνδεσης και επομένως δεν απαιτείται να προχωρήσει σε διαδικασία αλλαγής των δικτυακών ρυθμίσεων.



Σχήμα 5 Προτεινόμενες αλλαγές στο μήνυμα Binding Update

4 MBONE

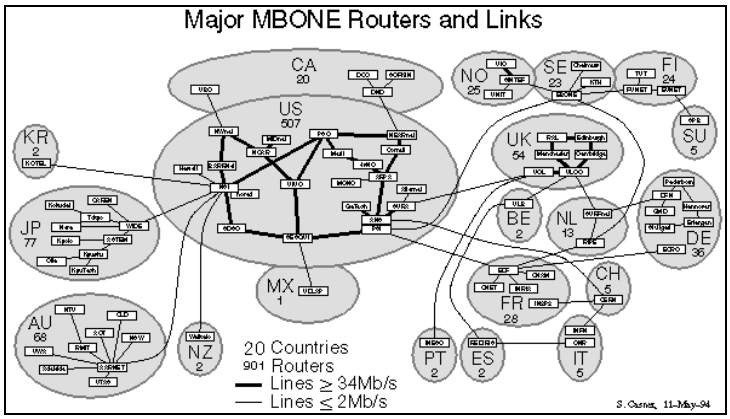
Το MBONE(Multicast Backbone on the Internet)[27] είναι μια τεχνολογία, η οποία επιτρέπει τη διακίνηση και προσπέλαση διαλογικών πολυμέσων σε πραγματικό χρόνο στο Internet χρησιμοποιώντας έξυπνους τρόπους διαχείρισης πληροφορίας κατά μήκος του δικτύου με αποτέλεσμα να είναι δυνατή η μείωση της περιττής αναπαραγωγής και η μερική αποφόρτιση του δικτύου. Το Mbone είναι ένα παράγωγο των δύο πρώτων Internet Engineering Task Force (IETF) "audiocast" πειραμάτων στα οποία τα live audio και video γίνονταν multicast από το site συνάντησης του IETF προς προορισμούς σε όλο

τον κόσμο. Η ιδέα ήταν να κατασκευαστεί μία προσωρινή IP multicast πλατφόρμα για test με σκοπό να μεταφέρει τα IETF transmissions και να υποστηρίζει συνεχόμενα πειράματα μεταξύ των meetings. Αυτό θα είναι μία εθελοντική δουλεία με συνεργασία.

Το 1992 μέσα στο IETF αποφασίσθηκε ότι η έλλειψη έξυπνων hardware συστημάτων (mrouters) θα μπορούσε να ξεπεραστεί (προσωρινά) με χρήση έξυπνου software. Γι' αυτό λοιπόν, δημιούργησαν ένα "virtual network" -ένα δίκτυο το οποίο τρέχει πάνω από το Internet- και έγραψαν software που επιτρέπει σε multicast πακέτα να διασχίζουν το δίκτυο. Εφοδιασμένοι με το κατάλληλο software, μπορούσαν να στέλνουν δεδομένα όχι μόνο σ' ένα κόμβο του Internet, αλλά σε πολύ περισσότερους. Το δίκτυο αυτό που ονομάσανε 1MBONE είναι ένα virtual network διότι μοιράζεται τα ίδια φυσικά μέσα με το Internet.Σήμερα έχει το μέγεθος που είχε περίπου το Internet το 1990(1700 δίκτυα σε 20 χώρες περίπου)

4.1 Τοπολογία του MBONE

Μέσα σε μία περιοχή, η τοπολογία του Mbone θα είναι ένας συνδυασμός από mesh και star: το backbone και τα regional (ή μεσαίου επιπέδου) networks θα σχετίζονται μέσω a mesh of tunnels μεταξύ mrouted μηχανές τοποθετημένες κυρίως στα σημεία επικοινωνίας των backbones και regionals. Μερικά εφεδρικά tunnels μπορεί να ρυθμιστούν με υψηλότερες μετρικές για robustness. Τότε κάθε regional network θα έχει μία ιεραρχία star κρεμάμενο από τον κόμβο του mesh για να συνδέεται με άλλα customer networks που θέλουν να συμμετέχουν.



Μεταξύ περιοχών υπάρχουν συνήθως μόνο ένα ή δύο Tunnels, που κατά προτίμηση τερματίζονται στο κοντινότερο σημείο στο Mbone Mesh.

4.2 Mbone-IPMulticasting

Ίσως να μην έχει γίνει μέχρι τώρα κατανοητή η διαφορά, αλλά και η σχέση του IP multicasting με το MBONE[28]. Το IP multicasting είναι μια υπηρεσία routing του δικτύου - μια μέθοδος του να στέλνεις πακέτα σε περισσότερα από ένα site κάθε φορά. Το MBONE είναι μια χαλαρή ομοσπονδία από sites που συγχρόνως υλοποιούν IP multicasting. Για να καταλάβει όμως κανείς την έννοια του MBONE θα πρέπει να γνωρίζει την multicast υπηρεσία. Η υπηρεσία αυτή παρέχει την δυνατότητα της ταυτόχρονης μεταφοράς πληροφορίας σε πολλούς αλλά συγκεκριμένους χρήστες. Το multicasting μπορεί να εφαρμοστεί μόνο όταν υπάρχουν και οι αντίστοιχοι multicast routers που υποστηρίζουν τέτοια δυνατότητα.

Το χαρακτηριστικό του MBONE είναι ότι επιτρέπει σε multicast πακέτα να ταξιδεύουν και μέσω των routers οι οποίοι έχουν δημιουργηθεί για να διαχειρίζονται μόνο unicast κίνηση. Με χρήση ειδικού software που χρησιμοποιεί το MBONE, τα multicast πακέτα μετατρέπονται σε παραδοσιακά unicast πακέτα έτσι ώστε οι unicast routers να μπορούν να τα διαχειριστούν. Η διαδικασία αυτή καλείται tunneling. Μελλοντικά, οι περισσότεροι εμπορικοί routers θα υποστηρίζουν το multicasting, χωρίς να χρειάζεται το tunneling.Όταν τα multicast πακέτα (που είναι κρυμμένα σε unicast πακέτα) φτάσουν σ' ένα router που μπορεί να τα καταλάβει, ή σ' ένα workstation με το κατάλληλο software, τότε αυτά αναγνωρίζονται και επεξεργάζονται σαν multicast πακέτα όπως πράγματι είναι. Οι μηχανές (workstations ή routers) εκείνες που είναι εφοδιασμένες στο να υποστηρίζουν multicast IP (πρωτόκολλα δικτύου - Internet Protocol) καλούνται mrouters (multicast routers).

Η τεχνολογία του MBONE δεν εγγυάται ότι με την υπάρχουσα υποδομή και την αύξηση των χρηστών και των απαιτήσεών τους δεν θα έχει προβλήματα. Αντίθετα τα πρώτα προβλήματα είναι ήδη εντοπισμένα και αποτελούν αντικείμενο προς έρευνα.

4.3 Επίκαιρα προβλήματα του Mbone-Πιθανές Λύσεις

Αυτή τη στιγμή το MBONE δεν είναι Plug and Play. Μέχρι ο αριθμός των χρήσεων της μεθόδου tunneling μειωθεί θα υπάρχουν πάντα περιορισμοί στην αυτόματη χρήση του MBONE. Η χρήση των tunnels απαιτεί ανθρώπινη μεσολάβηση και στις δύο άκρες, και μερικές φορές εβδομάδες ή μήνες μπορεί να περάσουν μεταξύ της στιγμής που μια τοποθεσία αποφασίσει να προχωρήσει στο MBONE και της στιγμής που η τοποθεσία αυτή θα μπορέσει να το χρησιμοποιήσει αποτελεσματικά. Εκτιμάται όμως ότι αυτό το πρόβλημα θα λυθεί σταδιακά από μόνο του αφού θα εγκαθίστανται όλο και περισσότεροι πραγματικοί multicast routers.

Επίσης το πρόβλημα του εύρους ζώνης(bandwith) θα συνεχίσει να υπάρχει αλλά και να αυξάνεται συνεχώς όσο κρατώντας το ίδιο maximum bandwidth (500Kps) αυξάνονται οι χρήστες του δικτύου. Το αποτέλεσμα θα είναι η υπερφόρτωση του δικτύου και όσες παρενέργειες μπορούν να υπάρξουν από χρήση μη αρκετού εύρους.

Ένα άλλο μεγάλο πρόβλημα χρησιμοποιώντας το MBONE είναι ότι έχει μια πιο τεχνική φύση. Συγχρόνως, τα πρωτόκολλα δικτύου του Internet δεν εξασφαλίζουν την απαραίτητη υποστήριξη που απαιτείται για real-time video. Αυτό σημαίνει ότι το MBONE δεν μπορεί να δουλέψει όσο καλά θα μπορούσε. Real time traffic απαιτεί ελάχιστες (μηδαμινές) καθυστερήσεις ανάμεσα στον πομπό και στον δέκτη και low packet loss. Το Internet, επί του παρόντος, δεν έχει τις δυνατότητες να εξασφαλίσει ότι η real-time traffic θα διανέμεται με μηδαμινές καθυστερήσεις και χαμηλούς ρυθμούς χασίματος (low loss rates). Ο ρυθμός χασίματος πακέτων επηρεάζει έντονα την ποιότητα εξυπηρέτησης την οποία μπορείς να πάρεις από το MBONE.

Μια μερική λύση των παραπάνω προβλημάτων καλείται IPng ή IPV6. Η IPng (Internet Protocol, Next Generation) είναι η επόμενη έκδοση του IP πρωτοκόλλου και οι αρχές της έχουν ήδη υιοθετηθεί. Η μετάβαση στο νέο IP πρωτόκολλο αναμένεται να

πραγματοποιηθεί στα επόμενα 10 χρόνια. Αυτό το νέο πρωτόκολλο θα εξασφαλίσει το MBONE μαζί με τα εφόδια που αυτό χρειάζεται για να υποστηρίξει την real-time traffic. Για να το κάνει αυτό, το νέο IP πρωτόκολλο θα είναι ικανό να προσδιορίζει τις ανάγκες της real-time traffic και έπειτα να λαμβάνει υπ' όψιν υπό θεώρηση όταν δρομολογεί τα διάφορα ήδη της κυκλοφορίας.

Το MBONE είναι μια χαλαρή συμμαχία από sites που τα οποία συγχρόνως υλοποιούν IP multicasting. Το MBONE είναι στην καλύτερη περίπτωση μια προσωρινή εφαρμογή, η οποία τελικά θα γίνει απαρχαιωμένη όταν το multicasting θα είναι ένα στάνταρ χαρακτηριστικό στους routers του Internet.

5 Πρωτόκολλο Μηνυμάτων ελέγχου Διαδικτύου (Internet Control Message Protocol) για το IPv6

Το πρωτόκολλο Μηνυμάτων διαδικτύου για το IPv6 (ICMPv6) χρησιμοποιείται από κόμβους IPv6 για να αναφέρουν λάθη που διαπίστωσαν σε πακέτα που διαχειρίσθηκαν και να πραγματοποιήσουν άλλες λειτουργίες σε επίπεδο διαδικτύου, όπως διαγνωστικά[26]. Το ICMPv6 είναι ενσωματωμένο στοιχείο του IPv6 και πρέπει να μπορεί να υλοποιηθεί από κάθε κόμβο.

5.1 Μορφή Γενικού Μηνύματος

Τα μηνύματα στο IPv6 είναι ομαδοποιημένα σε δύο κατηγορίες: μηνύματα λάθους και μηνύματα πληροφορίας. Τα μηνύματα λάθους αναγνωρίζονται σαν τέτοια επειδή φέρουν ένα μηδενικό στο bit υψηλότερου επιπέδου στο πεδίο Τύπος Μηνύματος. Με αυτόν τον τρόπο τα μηνύματα λάθους έχουν τύπους από 0 έως 127 και τα μηνύματα πληροφορίας 128 έως 255.

Παρακάτω θα αναφέρουμε και θα αναλύσουμε μερικά ενδεικτικά μηνύματα.
Μηνύματα λάθους:

1 Προορισμός Απρόσβατος - Destination Unreachable
2 Πακέτο ιδιαίτερα μεγάλο - Packet too big
3 Το χρονικό περιθώριο εξαντλήθηκε - Time Exceeded
4 Πρόβλημα Παραμέτρου - Parameter Problem

Μηνύματα πληροφορίας
128 Αίτηση Echo - Echo Request
129 Απεστάλη Echo - Echo Reply

Κάθε μηνύματος προηγείται ένας προπομπός (header) IPv6 και ένα μηδενικό ή περισσότεροι προπομποί. Ο προπομπός ICMPv6 αναγνωρίζεται από την τιμή 58 στην θέση Τιμή Επομένου Προπομπού (Next Header Value) του προηγούμενου προπομπού.
Τα μηνύματα ICMPv6 έχουν την ακόλουθη γενική μορφή:

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Code								Checksum															
Message Body																															

Το πεδίο τύπου (type) δείχνει τον τύπο του μηνύματος. Η τιμή του υποδεικνύει την μορφή της υπόλοιπης πληροφορίας.
Το πεδίο κωδικός (code) εξαρτάται από το πεδίο τύπου. Χρησιμοποιείται για να δημιουργήσει ένα επιπρόσθετο επίπεδο τμηματοποίησης του μηνύματος.
Το πεδίο άθροισμα ελέγχου (checksum) χρησιμοποιείται για την διαπίστωση ενδεχόμενης καταστροφής της πληροφορίας και μέρους του προπομπού.

5.2 Διαπίστωση της διεύθυνσης της πηγής του μηνύματος

Ένας κόμβος που στέλνει ένα μήνυμα ICPMv6 έχει να διαπιστώσει και την διεύθυνση του αποστολέα και την διεύθυνση του παραλήπτη πριν υπολογίσει το άθροισμα. Εάν ο κόμβος έχει περισσότερες από μία unicast διευθύνσεις, πρέπει να επιλέξει την διεύθυνση αποστολέα του μηνύματος ακολούθως:

1. Εάν το μήνυμα είναι απόκριση σε ένα μήνυμα που είχε σταλεί σε μια από τις διευθύνσεις unicast του κόμβου, η διεύθυνση αποστολές της απάντησης πρέπει να είναι η ίδια.
2. Εάν το μήνυμα είναι απόκριση σε ένα μήνυμα που είχε σταλεί σε μια multicast ή anycast ομάδα, της οποίας ο κόμβος είναι μέλος, η διεύθυνση αποστολέα της απάντησης πρέπει να είναι μια unicast διεύθυνση που ανήκει στην διεργασία που παρέλαβε το multicast ή anycast πακέτο.
3. Εάν το μήνυμα είναι απόκριση σε ένα μήνυμα που έχει σταλεί σε μια διεύθυνση που δεν ανήκει στον κόμβο, η διεύθυνση του αποστολέα θα πρέπει να είναι εκείνη η unicast διεύθυνση που θα ανήκει σε κόμβο ο οποίος θα είναι ο πιο κατάλληλος για την διάγνωση του λάθους. Για παράδειγμα, αν το μήνυμα είναι η απόκριση σε μια ενέργεια προώθησης πακέτου που δεν ολοκληρώθηκε επιτυχώς, η διεύθυνση αποστολέα θα είναι μια διεύθυνση unicast ανήκουσα στην διεργασία στην οποία προωθήθηκε το πακέτο.
4. Διαφορετικά, ο πίνακας δρομολόγησης του κόμβου πρέπει να ερευνηθεί για να διαπιστωθεί η διεργασία που θα χρησιμοποιηθεί για να μεταδοθεί το μήνυμα στον προορισμό του ώστε μια unicast διεύθυνση ανήκουσα σε αυτήν να χρησιμοποιηθεί σαν διεύθυνση αποστολέα του μηνύματος.

6 Group Internet Management Protocol (IGMP)

Οι hosts που επιθυμούν να λαμβάνουν multicast μηνύματα πρέπει να ενημερώσουν τους απευθείας γειτονικούς routers ότι ενδιαφέρονται να λαμβάνουν multicast μηνύματα που στέλνονται σε συγκεκριμένες ομάδες. Το πρωτόκολλο μέσω του οποίου οι hosts επικοινωνούν με τους τοπικούς m-routers για να ανταλλάξουν αυτήν την πληροφορία λέγεται Internet Group Management Protocol[26]

Όπως το ICMPv6 έτσι και το Internet Group Management Protocol (IGMP) είναι ένα τμήμα του IP.Λεπτομέρειες για το IGMP βρίσκονται στο RFC 1112.
Όλοι οι υπολογιστές που θέλουν να λάβουν IP multicasting πρέπει να έχουν εγκατεστημένο το IGMP.
Οι υπολογιστές που έχουν το IGMP μπορούν να κάνουν τα ακόλουθα:

- Να γνωστοποιήσουν την ομάδα στην οποία ανήκουν σε όλους τους multicast routers με τους οποίους συνδέονται άμεσα
- Να καθορίσουν της ομάδες ανάμεσα στους host και στους routers

Κάθε δρομολογητής που ανήκει σε ένα multicast group λειτουργεί και σα host και σα router.Εάν ο router έχει πολλές κάρτες δικτύου θα χρειαστεί να τρέξει το IGMP μόνο για μια από αυτές τις κάρτες. Επίσης οι routers που έχουν το IGMP μπορούν να μάθουν ποιοι από τους υπολογιστές των ομάδων συνδέονται στις κάρτες δικτύου τους.
Τα πακέτα IGMP βρίσκονται μέσα στα πακέτα IP και περιέχουν στην IP επικεφαλίδα τους το IP Alert Option(RFC 2113).Αυτή η επιλογή είναι χρήσιμη σε πρωτόκολλα όπως το IGMP τα οποία στέλνουν πακέτα συγκεκριμένο υπολογιστή αλλά απαιτούν σχετικά πολύπλοκη επεξεργασία όσο αναφορά τους αλγόριθμους δρομολόγησης.
IGMP Message Format
Τα μηνύματα IGMP έχουν το παρακάτω σχήμα

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Max Response Time								Checksum															
Group Address																															

*Type field:*Οι ακόλουθες τιμές τοποθετούνται στην επικεφαλίδα του ICMP πρωτοκόλλου αλλά αναφέρονται στον τρόπο λειτουργίας του IGMP

Type	**Message**
130	Group membership query
131	Group membership report
132	Leave Group membership

Max Response Time Field:Αυτό το πεδίο χρησιμοποιείται μόνο από τα μηνύματα που ασχολούνται μόνο με μηνύματα membership query και για όλους τους άλλους τύπους μηνυμάτων έχει την τιμή 0. Αυτό το πεδίο καθορίζει την χρονική διάρκεια που μεσολαβεί ανάμεσα στη χρονική στιγμή που το τελευταίο μέλος κάποιας ομάδας εγκαταλείπει την ομάδα μέχρι τη χρονική στιγμή που αυτό γίνεται γνωστό στο πρωτόκολλο δρομολόγησης.
Checksum Field: Χρησιμοποιείται για αναγνώριση λαθών (RFC 2236)
Group Address Field :Καθορίζει τη διεύθυνση της ομάδας.

IGMP Message Type
Υπάρχουν τρεις τύποι από IGMP message όσον αναφορά την αλληλεπίδραση ανάμεσα στους δρομολογητές και τους υπολογιστές.
IGMP Multicast Group Membership Query

Υπάρχουν δυο υποκατηγορίες από τα membership query message: το general και το group-specific.Το IGMP χρησιμοποιεί το general για να μάθει ποιες ομάδες έχουν μέλη στο τοπικό δύκτυο.Για να είναι έγκυρο ένα query message θα πρέπει να έχει τουλάχιστον μήκος 8 bytes και τη σωστή τιμή στο πεδίο checksum.Η διεύθυνση ομάδας (group address) θα πρέπει να είναι έγκυρη αλλά εναλλακτικά μπορεί να έχει και τη τιμή 0.Η διεύθυνση ομάδας είναι εκείνο το πεδίο που διαφοροποιεί τις δυο κατηγορίες μηνυμάτων. Στο membership query message η διεύθυνση ομάδας παίρνει την τιμή 0 όταν αναφερόμαστε σε ένα general query ενώ όταν αναφερόμαστε σε ένα specific query δέχεται ως όρισμα την διεύθυνση αυτού του group.Το max Response Time τις περισσότερες φορές είναι 100msec.

IGMP Multicast Membership Report

Όταν ένας υπολογιστής δέχεται ένα membership query (general ή group specific) πραγματοποιεί τις ακόλουθες ενέργειες:

Πρώτα από όλα ο υπολογιστής εντοπίζει τις ομάδες της κάρτας δικτύου από την οποία έλαβε το query και θέτει μετρητές χρονικής καθυστέρησης (delay timers) για κάθε ομάδα της οποίας είναι μέλος. Εάν για κάποια ομάδα χρησιμοποιείται ήδη κάποια μετρητής αρχικοποιείται ανάλογα με την τιμή του πεδίου max response time

Όταν ο δρομολογητής λάβει το μήνυμα αναφοράς κάνει τα ακόλουθα:

1)προσθέτει την ομάδα από την οποία έλαβε την αναφορά στη λίστα των μελών των ομάδων από το οποίο έλαβε την αναφορά

2)Θέτει το χρονικό μετρητή για τη συμμετοχή στο group membership interval στη τιμή της χρονικής διάρκειας που θα πρέπει να περάσει πριν ένας multicast router αποφασίσει ότι δεν υπάρχουν μέλη στην ομάδα. Εάν ο router δεν παραλάβει αναφορές για μια συγκεκριμένη ομάδα πριν τη λήξη του χρονικού μετρητή υποθέτει ότι η ομάδα δεν έχει τοπικά μέλη. Σε αυτή τη περίπτωση ο router δεν επεξεργάζεται μηνύματα που απευθύνονται στα μέλη αυτής της ομάδας.

IGMP Multicast Leave Group Membership

Όταν ένας υπολογιστής εγκαταλείπει ένα multicast group στέλνει ένα ειδικό μήνυμα η δομή του οποίου καθορίζεται από την έκδοση του IGMP που χρησιμοποιεί ο υπολογιστής. Ορισμένοι υπολογιστές στέλνουν ένα τέτοιο μήνυμα μόνο όταν είναι οι τελευταίοι υπολογιστές οι οποίοι έχουν απαντήσει σε ένα membership report query ενώ σε άλλες υλοποιήσεις του πρωτοκόλλου το μήνυμα αυτό στέλνεται πάντα και άσχετα με το αν ο υπολογιστής έχει στείλει ένα membership report ως απάντηση σε κάποιο query.

7 Ipv6 Over ATM

7 Ipv6 Over ATM [35]

Το ATM είναι μία τεχνολογία που χρησιμοποιείται τόσο σε δίκτυα τύπου campus όσο και για δίκτυα τύπου backbone. Παρ' όλα αυτά δεν μπορεί να αναιρέσει την ανάγκη για δρομολόγηση πακέτων. Υπάρχει μια παρεξήγηση που χρειάζεται να αποσαφηνιστεί όταν εξετάζουμε το Ipv6 αναφορικά με το ATM μεταγωγή κυψελίδας και άλλες μεθόδους μεταβίβασης ως πιθανές μεθόδους αντικατάστασης για δρομολόγηση πακέτων. Πιστεύετε ότι το ATM έχει τη θέση του στο χώρο του διαδικτύου, αλλά δεν μπορούμε να αντικαταστήσουμε τη δρομολόγηση πακέτου από αυτό το ίδιο. Έτσι δεν υπάρχει θέμα επιλογής του να έχουμε ATM ή Ipv6 γιατί τα δυο πρωτόκολλα όχι μόνο αλληλοσυμπληρώνουν το ένα το άλλο, αλλά επίσης εξυπηρετούν εντελώς διαφορετικούς ρόλους στο διαδίκτυο.

Γιατί να μη χρησιμοποιούμε το ATM ως μέσο μετάδοσης για υψηλής ταχύτητας IPv6 backbone(ραχοκοκαλιά) δίκτυα? Αυτή είναι μια ερώτηση που έχει δώσει το έναυσμα σε πολλά στάνταρτ και αναπτυξιακή δουλειά με στόχο την ενσωμάτωση του ATM και του Ipv6. Πιο πιθανή είναι η σύγκλιση και η ολοκλήρωση του ATM με το IPv6 παρά η εξάλειψη του ενός από το άλλο.Το Ipv6 όμοια με το Ipv4, προσφέρει δικτυακές υπηρεσίες για όλους τους κυριότερους τύπους συνδέσεων, συμπεριλαμβανομένων του ATM, Ethernet,Token Ring, Frame Relay και T1.

8 IPMulticasting Over ATM [34]

Multicasting όπως έχει ήδη αναφερθεί είναι η μετάδοση πακέτων σε ένα υποσύνολο σταθμών του δικτύου οι οποίοι στα πλαίσια αυτής της μετάδοσης απαρτίζουν μια ομάδα από παραλήπτες. Αντί να μεταδίδεται ένα ξεχωριστό αντίγραφο των δεδομένων για κάθε παραλήπτη ο αποστολέας στέλνει ένα μόνο αντίγραφο σε όλους τους παραλήπτες. Τα τελευταία χρόνια πολλές multicasting εφαρμογές έχουν μεγάλες απαιτήσεις σε εύρος ζώνης και έτσι το ATM θεωρείται μια ιδανική λύση. Το ATM είναι μια τεχνολογία προσανατολισμένη σε σύνδεση(connection oriented) δηλαδή για να επικοινωνήσουν δυο σταθμοί πρέπει να εγκατασταθεί ένα νοητό κύκλωμα(VC). Υπάρχουν δυο βασικές τεχνικές για multicasting IP πακέτων σε ένα υποδίκτυο ATM οι οποίες βασίζονται και οι δυο στη χρήση ενός Εξυπηρετητή Ανάλυσης Multicast Διευθύνσεων(MARS).Η πρώτη χρησιμοποιεί ένα σύνολο από νοητά κυκλώματα ενός σημείου προς πολλά καθένα από τα οποία έχει τη ρίζα του σε μια πηγή multicast και η άλλη χρησιμοποιεί ένα διαμοιραζόμενο δέντρο ενός σημείου σε πολλά που έχει τη ρίζα του σε έναν Multicast Server. Η απουσία, διευθύνσεων multicast από τις προδιαγραφές του ATM δημιουργεί την ανάγκη ενός μηχανισμού μετατροπής μιας IP multicast διεύθυνσης σε ένα αντίστοιχο σύνολο ATM διευθύνσεων των μελών της ομάδας. Ο εξυπηρετής MARS διατηρεί την αντιστοιχία μεταξύ των IP διευθύνσεων multicast ομάδων και των ATM διευθύνσεων των μελών.

ΒΙΒΛΙΟΓΡΑΦΙΑ -ΑΝΑΦΟΡΕΣ

[1] Deering S and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification,* RFC 1883 (December 1995)

[2] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460 (December 1998)

[3] Hinden R. and Deering S., *IP Version 6 Addressing Architecture,* RFC 1884 (December 1995)

[4] Steve King, Ruth Fax, Dimitry Haskin, Wenken Ling, Tom Meehan, Robert Fink, Charles E. Perkins, *The Case for IPv6,* Internet Draft, draft-iab-case-for-ipv6-05.txt, (October 1999)

[5] Παραδοτέα 1,2,3,4 του πιλοτικού έργου *Υλοποίηση δικτύου τεχνολογίας IPv6,* του έργου Greek University Network (GUnet) (Αθήνα 1998)

[6] Miller Mark, *Finding Your Way Through the New IP,* Network World (December 1996)

[7] W. Stallings, *IPv6: The New Internet Protocol,* IEEE Communications Magazine, (July 1996)

[8] Stewart S. Miller, *IPv6 The Next Generation Internet Protocol,* Digital Press (New York 1998

[9] Deering S and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification,* RFC 1883 (December 1995)

[10] S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification,* RFC 2460 (December 1998

[11] Partridge C., T. Mendez and W. Milliken, *Host Anycasting Service,* RFC 1546, (November 1993)

[12] Rekhter Y. & T. Li, *An Architecture for IPv6 Unicast Address Allocation,* RFC 1887 (December 1995)

[13] IEEE, *Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority,* http://standards.ieee.org/db/oui/tutorials/EUI64.html, (March 1997)

[14] R. Hinden, M.O'Dell, S. Deering, *An IPv6 Aggregatable Global Unicast Address Format,* RFC 2374, (July 1998)

[15] R. Hinden, S. Deering, *IPv6 Multicast Address Assignments,* RFC 2375, (July 1998)

[16] Y. Rekhter, T. Li, *Implications of Various Address Allocation Policies for Internet Routing,* RFC 2008, (October 1996)

[17] G. Malkin, R. Minnear, *RIPng for IPv6,* RFC 2080, (January 1997)

[18] R. Coltun, D. Ferguson, J. Moy, *OSPF for IPv6,* Internet draft, draft-ietf-ospf-ospfv6-06.txt, (June 1999)

[19] T. Bates, R. Chandra, D. Katz, Y. Rekhter, *Multiprotocol Extensions for BGP-4,* RFC 2283

[20] Rolf Oppliger, *Security at the Internet Layer,* IEEE Computer Magazine, (September 1998)

[21] R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 1825, (August 1995)

[22] S. Thomson, T. Narten, *IPv6 Stateless Address Autoconfiguration,* RFC 1971, (August 1996)

[23] S. Thomson, T. Narten, *IPv6 Stateless Address Autoconfiguration,* RFC 2562, (December 1998)

[24] Charles E. Perkins, *Mobile Networking in the Internet,* Mobile Networks & Applications, Volume 3, (January 1999)

[25] Gilligan R. and E.Nordmark, Transition Mechanisms for Ipv6 Hosts and Routers, RFC 1933

[26] Ipv6 Networks Marcus Goncalves and Kitty Niles

[27] http://www.savetz.com/mbone

[28] http://www.mbone.come

[29] http://www.technologie.pl/atm/atmlnk.html

[30] http://alternic.org/rfcs/search (RFC Search Engine)

[31] IP Multicasting Goncalves ISBN: 0-07-913791-1

[32] http://cell-relay.indiana.edu/mhonarc/ipatm/1995-Oct/msg00029.html

[33] http://www.experteach.de/pdf/ki/ki_IPMC.pdf

[34] Rajesh R.Talpade, Mostafa H.Ammar,Multicasting Server Architectures for Supporting IP Multicast over ATM

[35] http://www.ipv6forum.com/navbar/events/birmingham00/presentations/PDF/PatrickGrossetete.pdf