ΤΕΙ ΗΠΕΙΡΟΥ

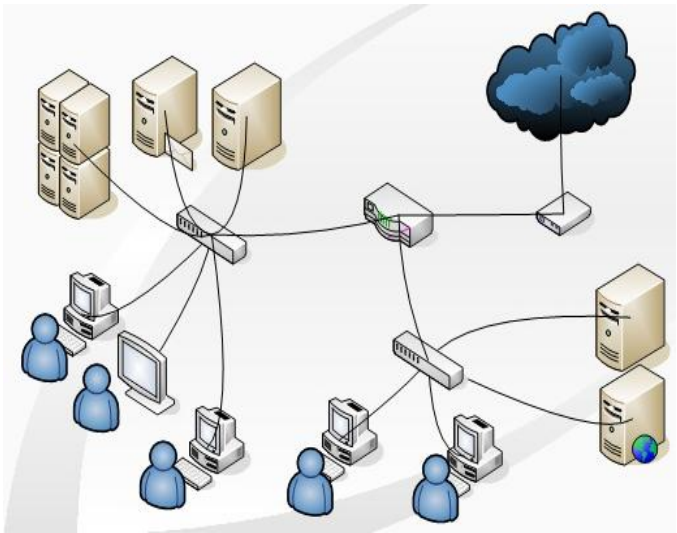
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΑΡΤΑ

«Περιγραφή Λειτουργίας & Συγκριτική Αξιολόγηση Τεχνικών Δρομολόγησης σε Δίκτυα Ευρείας Ζώνης Βασισμένα σε Πρωτόκολλα Ipv4 & IPv6»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Ι. Λάππας



Επιβλέπων:Καμπουράκη Αργυρώ
Εργαστηριακή συνεργάτης

Άρτα

Ιανουάριος 2009

Περιεχόμενα

Κεφάλαιο

1

1.1. Εισαγωγή στο IPv4

Η παρούσα έκδοση του πρωτοκόλλου IP (γνωστή ως έκδοση 4 ή IPv4) παραμένει ουσιαστικά ως έχει από τη δημοσίευση του εντύπου RFC 791 το 1981. Το πρωτόκολλο IPv4 αποδείχτηκε εύκολα υλοποιήσιμο και λειτουργικό ανεξαρτήτως πλατφόρμας υλοποίησής του.

Μία διεύθυνση IP (Ip address - Internet Protocol address), είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard.

Κάθε συσκευή που ανήκει στο δίκτυο, επίσης δρομολογητές (routers), υπολογιστές, time-servers, εκτυπωτές, μηχανές για fax μέσω Internet, και ορισμένα τηλέφωνα - πρέπει να έχει τη δική της μοναδική διεύθυνση. Μία διεύθυνση IP μπορεί να θεωρηθεί το αντίστοιχο μιας διεύθυνσης κατοικίας ή ενός αριθμού τηλεφώνου (σύγκριση με VoIP) για έναν υπολογιστή ή άλλη συσκευή δικτύου στο Διαδίκτυο. Όπως κάθε διεύθυνση κατοικίας και αριθμός τηλεφώνου αντιστοιχούν σε ένα και μοναδικό κτίριο ή τηλέφωνο, μια IP address χρησιμοποιείται για τη μοναδική αναγνώριση ενός υπολογιστή ή άλλης συσκευής που συνδέεται στο δίκτυο.

Μια διεύθυνση IP μπορεί να "μοιράζεται" σε πολλές συσκευές-πελάτες είτε επειδή αυτές είναι μέρος ενός shared hosting web server environment, είτε λόγω ενός proxy server (π.χ. ενός Παροχέα Υπηρεσιών Διαδικτύου (ISP) ή μιας υπηρεσίας για εξασφάλιση ανωνυμίας - anonymizer service) που λειτουργούν ως μεσολαβητές. Στην τελευταία περίπτωση (χρήση διακομιστή μεσολάβησης) η πραγματική διεύθυνση IP μπορεί να αποκρύπτεται απο το διακομιστή που δέχεται αίτηση. Η αναλογία στα τηλεφωνικά συστήματα θα ήταν η χρήση διεθνών ή τοπικών αριθμών κλήσης (proxy) και επεκτάσεων (shared).

1.1.1 Σκοπός

Το IPv4 είναι η τέταρτη έκδοση του πρωτοκόλλου Ίντερνετ, αλλά είναι το πρώτο που χρησιμοποιείται ευρέως. Χρησιμοποιεί ένα 32 bit σύστημα που επιτρέπει να δώσει 4.294.967.296 μοναδικές διευθύνσεις IP. Το IPv4 έχει τέσσερις διαφορετικές κλάσεις που είναι χωρισμένες στις παρακάτω κατηγορίες A, B, C και D. Μία διεύθυνση του πρωτοκόλλου IPv4 μοιάζει κάπως έτσι 207. 142. 131. 235. Το IPv4 χρησιμοποιεί μια μάσκα υποδικτύου, λόγω του μεγάλου αριθμού των υπολογιστών που χρησιμοποιούνται σήμερα. Η μάσκα υποδικτύου βοηθά στη μείωση του αριθμού των μοναδικών IP που χορηγούνται σε επιχειρήσεις, εταιρείες, πανεπιστήμια και σε κέντρα με πολλούς υπολογιστές.

Οι άνθρωποι έχοντας στη μνήμη τους το Σχήμα 1 και τον Πίνακα 3 μπορούν εύκολα και γρήγορα να αποφασίσουν σε ποια κλάση ανήκει μια IP και ποιο είναι το net id και ποιο το host id. Οι υπολογιστές, ωστόσο, για να βρούν το netid και το host id χρησιμοποιούν τη μάσκα. Αυτή είναι ένας 32-bit δυαδικός αριθμός, ο οποίος συνήθως γράφεται σε dotted-decimal μορφή όπως και η IP. Ο σκοπός που χρησιμοποιείται η μάσκα είναι για να ορίσει τη δομή μιας διεύθυνσης IP. Αυτό επιτυγχάνεται με το γεγονός ότι η μάσκα αναπαριστά το host id με 0s και το net id με 1s στο δυαδικό σύστημα, όπως φαίνεται παρακάτω, και πραγματοποιεί τη λογική πράξη AND με την IP προσδιορίζοντας έτσι το netid και το hostid.

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

Στο Πίνακα 4 συνοψίζονται οι προκαθορισμένες μάσκες για κάθε κλάση και τα μεγέθη των τμημάτων των net id και host id σε μια IP A, B, C κλάσης αντίστοιχα.

Πίνακας 4

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

Το Ipv4 είναι ιδιαίτερα περιορισμένο να παρέχει λειτουργίες, απαραίτητες για να μεταφέρουν ένα σύνολο bit (ένα IP datagram) από έναν αποστολέα στον προορισμό πάνω σ'ένα διασυνδεδεμένο σύστημα δικτύων. Δεν υπάρχουν μηχανισμοί να αυξάνουν άκρο προς άκρο την αξιοπιστία των δεδομένων, τη ροή ελέγχου, που ακολουθείται ή άλλες υπηρεσίες που συνήθως υπάρχουν σε host-to host πρωτόκολλα. Το Ipv4 μπορεί να εκμεταλλεύεται τις υπηρεσίες των υποστηρικτικών δικτύων για να παρέχει διαφόρων ειδών και ποιοτήτων υπηρεσίες.

1.1.2 Διεπαφές

Το Ipv4 επικαλείται το host-to-host πρωτόκολλο σε ένα περιβάλλον Internet. Το πρωτόκολλο αυτό παροτρύνει τα πρωτόκολλα τοπικών δικτύων να μεταφέρουν τα IP datagrams στην επόμενη πύλη ή τον εξυπηρετητή προορισμού. Για παράδειγμα, ένα TCP module (αυτοτελής μονάδα προγράμματος Η/Υ) επικαλείται την IP ενότητα (IP module) να πάρει ένα τμήμα του TCP (περιλαμβανομένου των TCP επικεφαλίδων και τα δεδομένα του χρήστη) σαν ένα τμήμα δεδομένων από ένα IP datagram. Ένα TCP module παρέχει τις διευθύνσεις και άλλες παραμέτρους της επικεφαλίδας στο IP module σαν συμφωνία στην κλήση. Έπειτα, το IP module θα δημιουργήσει ένα IP datagram και θα καλέσει την διεπαφή του τοπικού δικτύου για την μεταφορά του datagram. Για παράδειγμα, στην περίπτωση του ARPANET το IP module θα καλέσει το τοπικό net module το οποίο θα προσθέσει 1822 οδηγούς στο IP datagram δημιουργώντας ένα ARPANET μήνυμα που θα μεταφερθεί στο IMP. Η διεύθυνση ARPANET προέρχεται από την διεύθυνση Internet της διεπαφής του τοπικού δικτύου και είναι η διάταξη κάποιου εξυπηρετητή στο ARPANET ο οποίος μπορεί να είναι μια πύλη σε άλλα δίκτυα.

1.1.3 Λειτουργία

Το Ipv4 θέτει σε εφαρμογή δύο βασικές λειτουργίες : διευθυνσιοδότηση και κατάτμηση (addressing και fragmentation). Τα IP modules χρησιμοποιούν τις διευθύνσεις που μεταφέρουν στην επικεφαλίδα για την μετάδοση των IP datagrams προς τον προορισμό. Η επιλογή ενός μονοπατιού για μετάδοση καλείται δρομολόγηση (routing). Τα IP modules χρησιμοποιούν πεδία της επικεφαλίδας για να κατακερματίσουν και να επανασυναρμολογήσουν τα IP datagrams, όταν χρειάζεται για μεταφορά μέσω δικτύων

μικρών πακέτων. Το μοντέλο του εγχειρήματος είναι ότι ένα IP module ανήκει σε κάθε host που απασχολείται σε Internet επικοινωνία και κάθε πύλη που διασυνδέει δίκτυα. Αυτά τα modules μοιράζονται κοινούς κανόνες για την ερμηνεία των πεδίων διεύθυνσης και για κατάτμηση και επανασυναρμολόγηση των datagrams. Επιπρόσθετα, αυτά τα modules (ιδιαίτερα των πυλών) εκτελούν διαδικασίες για την λήψη αποφάσεων δρομολόγησης. Το Ipv4 συμπεριφέρεται σε κάθε datagram όπως σε μια ξεχωριστή οντότητα που δε συνδέεται με άλλο datagram. Δεν υπάρχουν συνδέσεις ή λογικά κυκλώματα (πραγματικά ή άλλου τύπου). Το Ipv4 χρησιμοποιεί τέσσερις μηχανισμούς κλειδιά για να παρέχει τις υπηρεσίες του, Type of Service, Time to Live, Options, και Header Checksum.

- **Type of Service**

Χρησιμοποιείται για να υποδηλώσει την ποιότητα των υπηρεσιών. Το είδος των υπηρεσιών είναι ένα αφηρημένο ή γενικευμένο σύνολο παραμέτρων οι οποίες χαρακτηρίζουν τις επιλογές των υπηρεσιών που παρέχονται στα δίκτυα που αποτελούν το Internet. Η παράμετρος Type of Service χρησιμοποιείται από τις πύλες για να συλλέξουν τις ακριβείς παραμέτρους μετάδοσης για ένα συγκεκριμένο δίκτυο, που χρησιμοποιείται για το επόμενο σκέλος (hop), ή την επόμενη πύλη όταν δρομολογείται ένα IP datagram.

- **Time to Live**

Ο χρόνος ζωής (Time to Live) είναι μια ένδειξη ενός ανώτερου ορίου στη διάρκεια ζωής ενός datagram. Ορίζεται από τον αποστολέα και περιορίζεται στα σημεία κατά μήκος της διαδρομής. Αν ο χρόνος ζωής αγγίξει το μηδέν πριν το IP datagram φτάσει στον προορισμό του τότε καταστρέφεται. Ο χρόνος ζωής μπορεί να χαρακτηριστεί σαν αυτοκαταστροφικό χρονικό όριο.

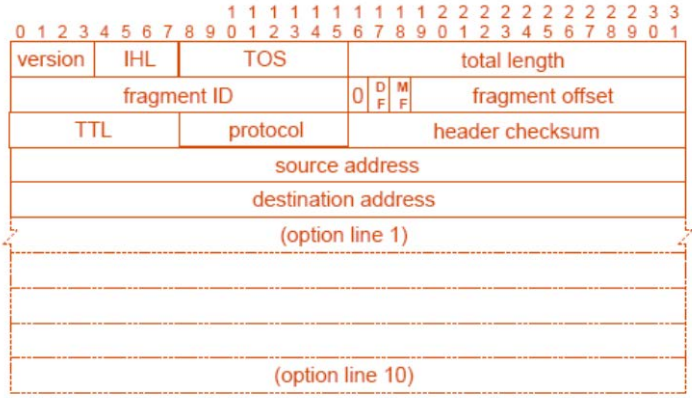
- **Options**

Οι επιλογές (Options) παρέχονται για λειτουργίες ελέγχου που χρειάζονται ή είναι χρήσιμες σε κάποιες περιπτώσεις αλλά δεν είναι απαραίτητες για τις περισσότερες κοινές επικοινωνίες. Οι επιλογές αναφέρονται σε timestamps, ασφάλεια και ειδικό δρομολόγηση.

- **Header Checksum**

Παρέχει την εξακρίβωση ότι οι πληροφορίες που χρησιμοποιήθηκαν στην επεξεργασία του datagram έχουν μεταφερθεί επιτυχώς. Τα δεδομένα μπορεί να περιέχουν λάθη, αν αποτύχει τότε απορρίπτεται αμέσως από την οντότητα που εντοπίζει το λάθος. Το Ipv4 δεν παρέχει μια αξιόπιστη ευχέρεια επικοινωνίας. Δεν υπάρχουν παραδοχές είτε end-to-end είτε hop-by-hop, δεν υπάρχει έλεγχος λάθους για τα δεδομένα μόνο ένας έλεγχος της επικεφαλίδας. Επίσης δεν υπάρχουν αναμεταδόσεις ούτε ροή ελέγχου. Τα λάθη που ανιχνεύονται μπορεί να

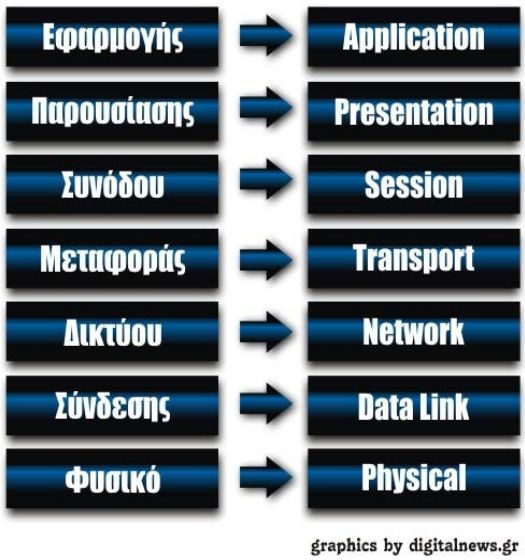
αναφερθούν μέσω του Internet Control Message Protocol (ICMP) το οποίο εφαρμόζεται στο Ipv4 module.



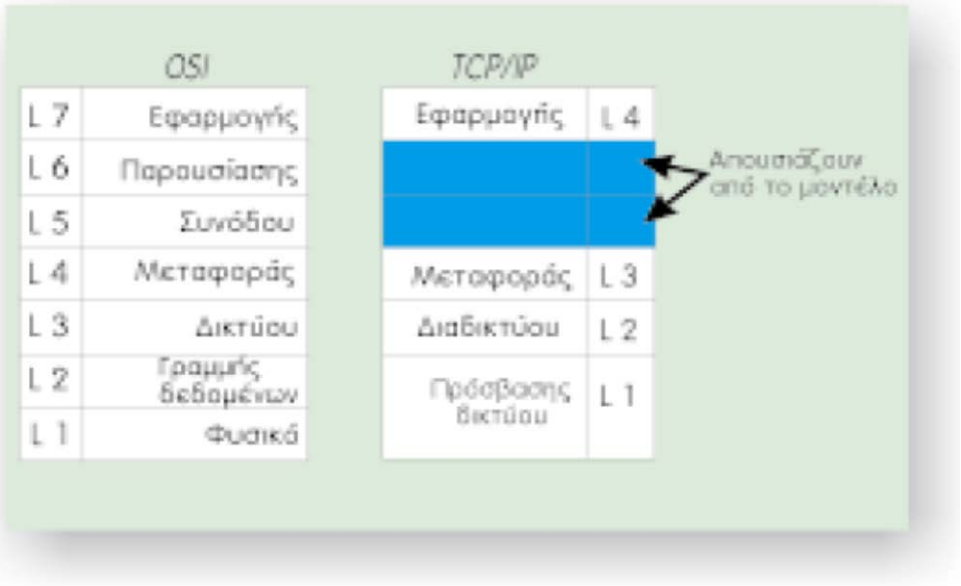
Εικόνα 1: Επικεφαλίδα IPv4

1.1.4 Το IP με το μοντέλο OSI

Το μοντέλο OSI
7. Επίπεδο Εφαρμογής
NNTP · SIP · SSI · DNS · FTP · Gopher · HTTP · NFS · NTP · SMPP · SMTP · SNMP · Telnet (more)
6. Επίπεδο Παρουσίασης
MIME · XDR
5. Επίπεδο Συνόδου
Named Pipes · NetBIOS · SAP
4. Επίπεδο Μεταφοράς
UDP · PPTP · SCTP · SSL · TLS
3. Επίπεδο Δικτύου
ICMP · IPsec · IGMP
2. Επίπεδο Σύνδεσης
CSLIP · SLIP · Ethernet · Frame relay · ITU-T G.hn DLL · L2TP · PPP
1. Φυσικό Επίπεδο
V.35 · V.34 · I.430 · I.431 · T1 · E1 · POTS · SONET/SDH · OTN · DSL · 802.11a/b/g/n PHY · ITU-T G.hn PHY



Το Ipv4 συνδέεται από τη μια πλευρά με το υψηλότερο πεδίο host-to-host πρωτοκόλλων και από την άλλη πλευρά με το πρωτόκολλο τοπικού δικτύου. Μέσα σε αυτό το πλαίσιο ένα τοπικό δίκτυο μπορεί να είναι ένα μικρό δίκτυο σε κτίριο ή ένα μεγάλο δίκτυο, όπως το ARPANET.



Σχήμα 5.35: Σύγκριση επιπέδων των μοντέλων αναφοράς OSI και TCP/IP

1.1.5 Μοντέλο λειτουργίας

Το μοντέλο της εφαρμογής της μετάδοσης ενός datagram από μια εφαρμογή προγράμματος σε άλλη επεξηγείται από το παρακάτω σενάριο :
Υποθέτουμε ότι αυτή η μετάδοση περιλαμβάνει μια ενδιάμεση πύλη.

Η απεσταλμένη εφαρμογή προγράμματος προετοιμάζει τα δεδομένα της και επικαλείται το τοπικό της IP module για να στείλει τα δεδομένα σαν datagram. Στην συνέχεια περνάει την διεύθυνση προορισμού και άλλες παραμέτρους σαν υποστήριξη της κλήσης.

Το IP module προετοιμάζει μία datagram επικεφαλίδα και σε αυτή επισυνάπτονται τα δεδομένα . Το IP module ερμηνεύει μια τοπική διεύθυνση δικτύου για αυτή την IP διεύθυνση, όπου σε αυτή την περίπτωση είναι η διεύθυνση της πύλης. Αυτό στέλνει το datagram και την τοπική διεύθυνση δικτύου στο τοπικό δίκτυο. Το τοπικό δίκτυο δημιουργεί μία επικεφαλίδα τοπικού δικτύου, επισυνάπτει το datagram και στέλνει τα αποτελέσματα.

Το datagram φτάνει στην πύλη του εξυπηρετητή, μέσα στην επικεφαλίδα τοπικού δικτύου, η διεπαφή τοπικού δικτύου αναλύει την επικεφαλίδα και γυρνάει το datagram πάνω

από το IP module. Το IP module προσδιορίζει από την IP διεύθυνση ότι το datagram θα προωθηθεί σε άλλο εξυπηρετητή σε ένα δεύτερο δίκτυο. Το IP module προσδιορίζει την τοπική net διεύθυνση του προορισμού. Έπειτα η διεπαφή τοπικού δικτύου αποστέλλει το datagram.

Αυτή η διεπαφή τοπικού δικτύου δημιουργεί μία επικεφαλίδα τοπικού δικτύου και επισυνάπτει το datagram στέλνοντας το αποτέλεσμα στον προορισμό.
Στον προορισμό το datagram αναλύει την επικεφαλίδα τοπικού δικτύου από την διεπαφή τοπικού δικτύου και μεταβιβάζεται στο IP module.

Το IP module καθορίζει ότι το datagram είναι για ένα πρόγραμμα εφαρμογής σε αυτόν τον εξυπηρετητή. Μεταφέρει τα δεδομένα στο πρόγραμμα εφαρμογής σε απάντηση της κλήσης περνώντας την διεύθυνση προέλευσης και άλλες παραμέτρους σαν αποτέλεσμα της κλήσης.

Η λειτουργία ή ο σκοπός του Ipv4 είναι να μετακινεί τα datagrams μέσω μιας διεπαφής δικτύων. Αυτό επιτυγχάνεται περνώντας τα datagrams από το ένα IP module στο άλλο μέχρι να φτάσουν στον προορισμό. Τα IP modules ανήκουν στους **δρομολογητές** και στις πύλες στο Internet. Τα datagrams δρομολογούνται από ένα IP module σε άλλο μέσω ξεχωριστών δικτύων βασισμένα στην ερμηνεία μιας IP διεύθυνσης. Κατά συνέπεια, ένας σημαντικός μηχανισμός του IPv4 είναι η IP διεύθυνση.

Στην επιλογή ενός μονοπατιού για μετάδοση (routing) των μηνυμάτων από το ένα IP module στο άλλο τα datagrams μπορεί να χρειαστεί να διασχίσουν ένα δίκτυο του οποίο το μέγιστο μέγεθος πακέτου είναι μικρότερο από το μέγεθος του datagram . Για να ξεπεράσουμε αυτή τη δυσκολία ο μηχανισμός της κατάτμησης παρέχεται στο IPv4.

1.2. Διευθυνσιοδότηση

Αν μια συσκευή επιθυμεί να επικοινωνήσει χρησιμοποιώντας το πρότυπο TCP/IP, χρειάζεται απαραίτητα μια IP. Όταν η συσκευή έχει μια IP διεύθυνση και το κατάλληλο λογισμικό και υλικό, μπορεί να στέλνει και να λαμβάνει πακέτα. Οποιαδήποτε συσκευή που μπορεί να στέλνει και να λαμβάνει IP πακέτα ονομάζεται IP host.

Μια IP διεύθυνση αποτελείται από 32 bits και χωρίζεται σε δυο κομμάτια, στη διεύθυνση δικτύου(network address ή netid) και στη διεύθυνση τερματικού (host address ή hostid). Η διεύθυνση δικτύου προσδιορίζει το δίκτυο και είναι κοινή για όλες τις συσκευές που βρίσκονται στο ίδιο δίκτυο ενώ η διεύθυνση τερματικού προσδιορίζει μια συγκεκριμένη

συσκευή που βρίσκεται στο δίκτυο. Μια IP διεύθυνση αναπαρίσταται με το συμβολισμό τεσσάρων δεκαδικών που μεταξύ τους έχουν τελείες (dotted-decimal notation) π.χ 172.16.81.100 δηλαδή τα 32 bits στο δυαδικό σύστημα διαιρούνται σε τέσσερις οκτάδες (8bits=1byte) και κάθε οκτάδα αναπαρίσταται στη δεκαδική μορφή και διαχωρίζεται από τις άλλες με τελεία π.χ

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

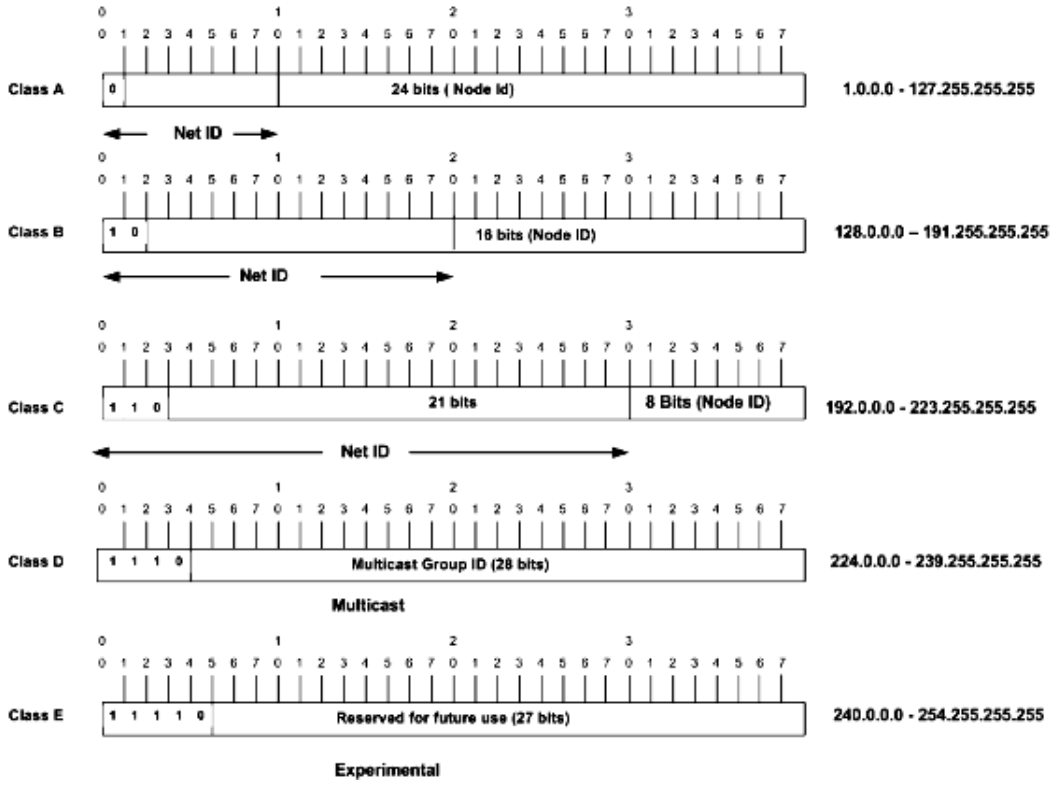
Εδώ θα δώσουμε ένα παράδειγμα πώς γίνεται η μετατροπή των δυαδικών οκτάδων σε δεκαδικό αριθμό: Το πιο δεξιό ψηφίο ή αλλιώς το λιγότερο σημαντικό ψηφίο μιας οκτάδας παίρνει τιμή 20 ενώ το bit που είναι στην αμέσως δεξιότερη θέση τη τιμή 21. Αυτό συνεχίζει μέχρι να φτάσουμε στο ψηφίο που είναι στην αριστερότερη θέση ή το πιο σημαντικό ψηφίο το οποίο παίρνει τη τιμή 2^7. Έτσι αν έχουμε έναν δυαδικό αριθμό που έχει όλα τα bit του 1 ο ισοδύναμος δεκαδικός θα είναι ο 255 όπως φαίνεται και στο παράδειγμα παρακάτω:

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)

Με βάση τα παραπάνω δημιουργείται το ερώτημα πόσα bits της IP διεύθυνσης θα προσδιορίζουν το δίκτυο και πόσα το τερματικό; Η λύση σ' αυτό το πρόβλημα δίνεται με τις κλάσεις. Υπάρχουν 5 κλάσεις εκ των οποίων 3 πρωτεύουσες, A, B, C και δυο για ειδικούς σκοπούς, οι D, E. Ανάλογα με τις απαιτήσεις που θέλουμε να ικανοποιεί και το σκοπό που θέλουμε να εξυπηρετεί το δίκτυο μας επιλέγουμε μια από τις 5 κλάσεις. Στο Σχήμα 1 φαίνεται αναλυτικά σε κάθε κλάση πόσα bit είναι το net id και πόσα bit το host id. Επισημαίνουμε ότι διαφορετική network address δηλώνει διαφορετικό φυσικό δίκτυο.

Σχήμα 1



Στο Σχήμα 1 παρατηρούμε ότι μια IP διεύθυνση που

1. Τα πρώτα 8 bits της, εκ των οποίων το πρώτο είναι 0, καθορίζουν το netid και τα υπόλοιπα 24 bits της το host id είναι κλάσης Α.
2. Τα πρώτα 16 bits της, εκ των οποίων το πρώτο και το δεύτερο είναι 1,0 αντίστοιχα, καθορίζουν το netid και τα υπόλοιπα 16 bits της το host id είναι κλάσης Β.
3. Τα πρώτα 24 bits της, εκ των οποίων τα τρία πρώτα έχουν τιμή 1,1,0 αντίστοιχα, καθορίζουν το netid και τα υπόλοιπα 8 bits της το host id είναι κλάσης C.

Βέβαια όταν μας δίνεται μια IP π.χ 8.5.1.3 για να καταλάβουμε σε ποια κλάση ανήκει και να αναλύσουμε πόσα bits είναι το netid και πόσα το hostid πρέπει να έχουμε υπόψη μας το Πίνακα 3.

Πίνακας 3

Class	**Leading bits**	**Start***	**End***	**Total number of Networks**	**Number of Hosts per Network**
Class A	0	1.0.0.0	127.255.255.255	2^7-2	2^{24}-2 (16.777.214)

Class B	10	128.1.0.0	191.254.255.255	2^{14}-2	2^{16}-2 (65.534)
Class C	110	192.0.1.0	223.255.254.255	2^{21}-2	2^{8}-2 (254)

Στην πραγματικότητα οι διευθύνσεις 0.0.0.0 ,127.255.255.255 όπως και οι 128.0.0.0, 191.255.255.255 αλλά και οι 192.0.0.0, 223.255.255.255 δεσμεύονται για δίκτυα A, B, C κλάσης αντίστοιχα αλλά δεν χρησιμοποιούνται .Οι διευθύνσεις που όλα τα bits του host id, όταν η IP είναι σε δυαδική μορφή, είναι 0 π.χ 8.0.0.0, 130.40.0.0, 196.120.80.0 ονομάζονται zero address και δηλώνουν όλο το δίκτυο ενώ οι διευθύνσεις που όλα τα bits του host id, όταν η IP είναι σε δυαδική μορφή, έχουν τιμή 1 π.χ 8.255.255.255,130.40.255.255, ονομάζονται broadcast address(ισχύει όταν παίρνουμε όλο το δίκτυο C κλάσης) και χρησιμοποιούνται όταν θέλουμε να στείλουμε ένα πακέτο σε όλες τις συσκευές του δικτύου. **Το πώς υπολογίζουμε τη broadcast address και τη zero address φαίνεται στο Πίνακα 5.

Πίνακας 5:*Με IP 8.1.4.5 και μάσκα 255.0.0.0 ο υπολογισμός της zero address και της broadcast address γίνεται ως εξής.*

Address	*8.1.4.5*	*0000 1000 0000 0001 0000 0100 0000 0101*
Mask	*255.0.0.0*	*1111 1111 0000 0000 0000 0000 0000 0000*
AND result *(zero address)*	*8.0.0.0*	*0000 1000 0000 0000 0000 0000 0000 0000*
Broadcast address	*8.255.255.255*	*0000 1000 1111 1111 1111 1111 1111 1111*

1.2.1 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.

1.2.2 Διαχείριση και Διαμόρφωση Δικτύου

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. Πόσο πιο ωραία δεν θα ήταν τα πράγματα αν απλά συνέδεες το μηχάνημα στο δίκτυο και αυτό διαμορφωνόταν 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 κει 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 η 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.

1.3. IPv4 Δρομολόγηση

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.

1.3.1 IPv4 Unicast Δρομολόγηση

Το IP (Internet Protocol), ένα μέρος του Transmission Control Protocol / Internet Protocol (TCP / IP), είναι το πρωτοκόλλο που επιτρέπει τη δρομολόγηση της κίνησης του δικτύου σε κάθε είδους Internetwork IP, συμπεριλαμβανομένων των Windows internetworks, UNIX internetworks, και τα μικτά περιβάλλοντα δικτύου. Το IP δίνει επίσης τη δυνατότητα επικοινωνίας μέσω του δημόσιου Διαδικτύου, το οποίο είναι ένα IP-based Internetwork.

Επί του παρόντος, η IP unicast δρομολόγηση λαμβάνει χώρα πάνω IPv4 internetworks. Ένα Internetwork αποτελείται από μικρότερα δίκτυα που ενώνονται με τις συσκευές διασύνδεσης γνωστές ως δρομολογητές. Η δρομολόγηση IP είναι η διαδικασία προώθησης των πακέτων IP από μια συσκευή δικτύου σε ένα μέρος ενός Internetwork σε μια συσκευή δικτύου σε ένα άλλο τμήμα του δικτύου (υποδίκτυο). Ένα πακέτο IP ή datagram είναι μια μονάδα πληροφοριών που αποστέλλονται μέσω δικτύου IP που περιλαμβάνει τα δεδομένα που προορίζονται για τον αποδέκτη, καθώς και μια επικεφαλίδα που περιέχει πληροφορίες δρομολόγησης (οι διευθύνσεις προέλευσης και προορισμού και σφάλμα-δεδομένα ελέγχου). Οι δρομολογητές IP προωθούν τα πακέτα μεταξύ των τμημάτων του δικτύου.

Η Unicast δρομολόγηση είναι η διαδικασία που δίνει τη δυνατότητα μοναδικής διανομής πακέτων από ένα κόμβο αποστολής σε ένα κόμβο προορισμό μέσω ενός ή περισσοτέρων ενδιάμεσων δρομολογητών. Ένας κόμβος είναι οποιαδήποτε συσκευή δικτύου που εκτελεί το πρωτόκολλο TCP / IP. Ο δρομολογητής είναι ένας κόμβος που εκτελεί δρομολόγηση. Δηλαδή, ένας δρομολογητής προωθεί πακέτα που δεν προορίζονται για την ίδια ρουτίνα(για τον δρομολογητή τον ίδιο), είτε απευθείας στον τόπο προορισμού ή σε άλλο δρομολογητή στη διαδρομή προς τον προορισμό.

1.3.2 Στατική και δυναμική δρομολόγηση

Ένας υπολογιστής που εκτελεί δρομολόγηση και κάποια υπηρεσία απομακρυσμένης πρόσβασης που έχει δύο ή περισσότερους προσαρμογείς δικτύου (καθένας ρυθμίστηκε με την κατάλληλη διεύθυνση IP και τη μάσκα υποδικτύου) είναι ένας δρομολογητής λογισμικού που μπορεί να προσφέρει ένα ευρύ φάσμα υπηρεσιών που υποστηρίζουν την δρομολόγηση IP.

Ένα σημαντικό μέρος αυτής είναι η υποστήριξη για στατική και δυναμική δρομολόγηση IP:

- Static IP δρομολόγηση. Ένας διαχειριστής ρυθμίζει χειροκίνητα τις πληροφορίες δρομολόγησης, και οι πληροφορίες δρομολόγησης δεν αλλάζουν εκτός αν ο διαχειριστής κάνει ενημερώσεις χειροκίνητα ή τις διαγράφει. Η στατική δρομολόγηση είναι κατάλληλη μόνο για ένα μικρό Internetwork.
- Δυναμική δρομολόγηση IP. Ένας διαχειριστής διαμορφώνει ένα δρομολογητή για να χρησιμοποιεί ένα πρωτόκολλο δυναμικής δρομολόγησης. Ο δρομολογητής που χρησιμοποιεί ένα πρωτόκολλο δυναμικής δρομολόγησης δημιουργεί αυτόματα πληροφορίες δρομολόγησης, μοιράζεται τις πληροφορίες με άλλους δρομολογητές, και ενημερώνει τις πληροφορίες δρομολόγησης όταν υπάρχουν αλλαγές. Ένα μεγάλο Internetwork που χρησιμοποιεί κατά κύριο λόγο δυναμική δρομολόγηση συνήθως χρησιμοποιεί επίσης μερικές χειροκίνητα στατικές διαδρομές.

Ένας υπολογιστής που εκτελεί δρομολόγηση και απομακρυσμένη πρόσβαση που έχει μόνο ένα interface είναι, εξ ορισμού, ένας μη-router υπολογιστής και μπορεί να παρέχει κάποια δρομολόγηση που σχετίζεται με τις υπηρεσίες δικτύωσης, όπως το φιλτράρισμα πακέτων IP ή να ενεργεί ως πράκτορας αναμετάδοσης DHCP.

1.3.3 DHCP Relay Agent

Το DHCP Relay Agent μεταφέρει μηνύματα μεταξύ πελατών DHCP και διακομιστών DHCP που βρίσκονται σε ξεχωριστά τμήματα του δικτύου. Κάθε υποδίκτυο IP που περιέχει υπολογιστές-πελάτες DHCP απαιτεί είτε έναν διακομιστή DHCP ή έναν DHCP μεταφορέα για την παροχή διευθύνσεων σε πελάτες DHCP. Χρησιμοποιώντας έναν ή περισσότερους φορείς αναμετάδοσης καθίσταται περιττό να εγκατασταθεί ένας ξεχωριστός διακομιστής DHCP σε κάθε υποδίκτυο σε ένα Internetwork.

1.3.4 ICMP router discovery

Χρησιμοποιείται για ICMP Router προσέλκυση πελατών και μηνύματα Router Advertisement για να επιτρέψει την αυτοματοποιημένη ανακάλυψη των δρομολογητών από hosts. Αν και δρομολογητές και οι hosts έχουν ρυθμιστεί να χρησιμοποιήσουν ICMP router

ανακάλυψη, το χαρακτηριστικό αυτό απλοποιεί τον τρόπο που οι IP hosts έχουν ρυθμιστεί με τις διευθύνσεις IP των τοπικών δρομολογητών και παρέχει έναν τρόπο για τους hosts να ανακαλύψουν τους δρομολογητές που βρίσκονται κάτω.

1.3.5 Unicasting, Broadcasting, και Multicasting

Εκτός από την προώθηση unicast πακέτων IPv4, οι IP δρομολογητές μπορούν επίσης να διαβιβάσουν και multicast πακέτα IP από μια συσκευή σε πολλαπλές συσκευές σε άλλο δίκτυο.

- Unicasting είναι ένας-προς-έναν επικοινωνία των πακέτων IP από τον κόμβο αποστολέα στον κόμβο που λαμβάνει. Τα Unicast πακέτα μπορεί να περάσουν μέσα από άλλες συσκευές, όπως αυτές μεταδίδονται σε όλη το Internetwork. Ωστόσο, unicast πακέτα, εξ ορισμού, στέλνονται πάντα από έναν μόνο κόμβο αποστολής σε έναν ενιαίο κόμβο προορισμού. Οποιαδήποτε τεχνολογία που αφορά την αποστολή πακέτων από έναν κόμβο σε έναν άλλο μέσω ενός IP-based Internetwork χρησιμοποιεί unicast δρομολόγηση.

- Broadcasting είναι ένας-προς-όλους επικοινωνία. Τα πακέτα IP στέλνονται από ένα κόμβο προς όλους τους άλλους κόμβους πρόσβασης στο ίδιο υποδίκτυο. Αν οι δρομολογητές έχουν ρυθμιστεί να διαβιβάσουν Internetwork μετάδοση, τότε προωθούνται τα πακέτα σε όλα τα άλλα τμήματα του δικτύου. Οι χρήστες της επικοινωνίας που μεταδίδονται σε ένα δευτερεύον δίκτυο περιλαμβάνουν την αναγγελία για τη διαθεσιμότητα των υπηρεσιών δικτύου, την επίλυση ονομάτων σε διευθύνσεις, καθώς και την επίλυση των διευθύνσεων IP σε Media Access Control (MAC)διευθύνσεις.
- Το Multicasting είναι ένας-προς-πολλούς επικοινωνία, μεταξύ ενός κόμβου σε πολλαπλούς κόμβους που επιλέγουν να συμμετάσχουν σε μια συγκεκριμένη ομάδα πολυεκπομπής. Η Multicast επικοινωνία χρησιμοποιείται κυρίως για πολλαπλές εφαρμογές πολυμέσων χρήστη, όπως η τηλεδιάσκεψη, μάθηση εξ αποστάσεως, και η συλλογική υπολογιστών.

1.4. Λειτουργία IPv4 Unicast Πρωτόκολλων Δρομολόγησης

Οι εφαρμογές της unicast δρομολόγησης IP μπορεί να είναι απλές ή σύνθετες, ανάλογα με τους παράγοντες όπως το μέγεθος των Internetwork, η χρήση του Dynamic Host Configuration Protocol (DHCP) για την κατανομή των διευθύνσεων IP, σύνδεση με το Διαδίκτυο, και η παρουσία των μη Windows hosts στο Internetwork.

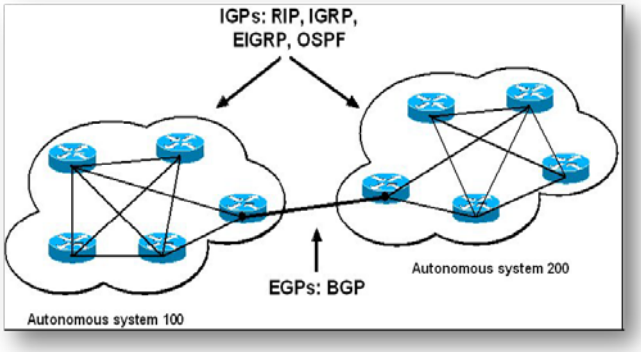
1.4.1 Εισαγωγή

Τα πρωτόκολλα δρομολόγησης (routing protocols) είναι υπεύθυνα για:

- την επιλογή του καλύτερου δρόμου προς οποιοδήποτε δίκτυο/υποδίκτυο προορισμού
- την κατάλληλη ενημέρωση των πινάκων δρομολόγησης
- την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των δρομολογητών ενός δικτύου.

Υπάρχουν δυο βασικά πρωτόκολλα δρομολόγησης:

- **τα εσωτερικά πρωτόκολλα πύλης IGP** (Interior Gateway Protocols) τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους σε ένα αυτόνομο σύστημα (autonomous system). (π.χ RIP, OSPF) Αυτόνομο σύστημα είναι ένα σύνολο δικτύων που εποπτεύονται από μια κοινή αρχή διαχείρησης.
- **τα εξωτερικά πρωτόκολλα πύλης EGP** (Exterior Gateway Protocols) τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους μεταξύ αυτόνομων συστημάτων. (π.χ BGP)



1.4.2 Αλγόριθμοι δρομολόγησης (Routing algorithms)

Βασική λειτουργία των πρωτοκόλλων δρομολόγησης είναι η εύρεση και η επιλογή του καλύτερου δρόμου για τα δίκτυα προορισμού με τη χρήση κατάλληλων αλγορίθμων δρομολόγησης (routing algorithms). Ο αλγόριθμος δρομολόγησης δημιουργεί έναν αριθμό, τον οποίο ονομάζουμε τιμή κόστους (metric), για κάθε διαδρομή στο δίκτυο. Η διαδρομή με το μικρότερο κόστος για τον ίδιο προορισμό καταχωρείται τελικά στον πίνακα δρομολόγησης. Ανάλογα με την υλοποίηση, ως κόστος μπορεί να χρησιμοποιηθεί ο αριθμός των δρομολογητών (hop count) που περνά το μήνυμα μέχρι να φτάσει στον προορισμό του, το εύρος ζώνης της γραμμής (bandwidth), η καθυστέρηση (delay), το φορτίο της γραμμής (load) και μια σειρά άλλων παραμέτρων ή ένας συνδυασμός από αυτές. Οι αλγόριθμοι δρομολόγησης χωρίζονται σε δυο κατηγορίες:

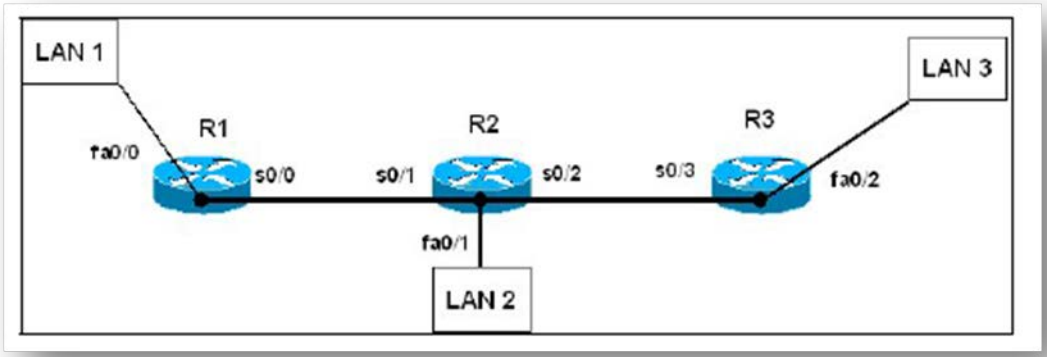
- **αλγόριθμοι διανύσματος απόστασης** (Distance Vector Algorithms), όπου οι πίνακες δρομολόγησης αποτελούνται από μια σειρά από προορισμούς (vectors) και κόστη τις αποστάσεις (distances) που διανύονται για την προσέγγιση του προορισμού.
- **αλγόριθμοι της κατάστασης της σύνδεσης (Link State Algorithms)**

1.4.3 RIP (Routing Information Protocol)

Το πρωτόκολλο RIP χρησιμοποιεί τον αλγόριθμο διανύσματος απόστασης και είναι κατάλληλο για τη λειτουργία μικρών δικτύων. Στους πίνακες δρομολόγησης που προκύπτουν υπάρχουν πληροφορίες για το δρόμο και το κόστος της απόστασης προς τα δίκτυα προορισμού. Ως κόστος χρησιμοποιείται ο αριθμός των ενδιάμεσων δρομολογητών μέχρι να φτάσουμε στο δίκτυο προορισμού (hop count). Ο αριθμός των ενδιάμεσων δρομολογητών μέχρι το δίκτυο προορισμού μπορεί να είναι μέχρι 15. Στο πρωτόκολλο RIP οι δρομολογητές περιοδικά (κάθε 30 δευτερόλεπτα), ανακοινώνουν ολόκληρο το περιεχόμενο του πίνακα δρομολόγησής τους, στους άμεσα γειτονικούς δρομολογητές. Ο πίνακας δρομολόγησης μπορεί να μεταδοθεί κι όταν υπάρξει κάποια αλλαγή στην τοπολογία του δικτύου. Έτσι επιτρέπεται στο κάθε δρομολογητή να βλέπει το δίκτυο του γειτονικού δρομολογητή και να προσθέτει το ανάλογο κόστος στην απόσταση που έχει ήδη προσθέσει ο δεύτερος. Το μειονέκτημα της προσέγγισης αυτής είναι ότι καθώς το δίκτυο μεγαλώνει, ανταλλάσσεται ένα μεγάλο ποσό πληροφορίας ανά τακτά χρονικά διαστήματα, ακόμα κι όταν η τοπολογία του

δικτύου δεν έχει αλλάξει, με αποτέλεσμα να περιορίζεται το διαθέσιμο εύρος ζώνης και να αυξάνεται ο χρόνος σύγκλισης.

Ως χρόνος σύγκλισης (convergence time), ορίζεται ο χρόνος που περνά μέχρι όλοι οι δρομολογητές να συμφωνήσουν σχετικά με την τοπολογία του δικτύου, από τη στιγμή που θα προκύψει μια αλλαγή. Όταν αλλάζει η τοπολογία του δικτύου, εκτελείται ο αλγόριθμος δρομολόγησης και σταματά η κίνηση των δεδομένων που μεταφέρει ο δρομολογητής προς τα διάφορα interfaces του, γιατί δεν γνωρίζει αν το δίκτυο προορισμού είναι διαθέσιμο ή όχι. Άρα, όσο πιο γρήγορα γίνεται η σύγκλιση τόσο πιο γρήγορα θα μεταφερθούν τελικά τα δεδομένα προς τον προορισμό τους.



Σύμφωνα με τα παραπάνω οι πίνακες δρομολόγησης που προκύπτουν στο παραπάνω δίκτυο θα είναι:

R1

network	next hop router	metric
LAN1	connected	0
LAN2	R2	1
LAN3	R3	2

R2

network	next hop router	metric
LAN1	R1	1
LAN2	connected	0
LAN3	R3	1

R3

network	next hop router	metric
LAN1	R2	2
LAN2	R2	1

LAN3	connected	0

Υπάρχουν δυο εκδόσεις του πρωτόκολλου RIP:
η έκδοση RIP-1, όπου δεν στέλνεται η μάσκα υποδικτύωσης μαζί με τους πίνακες δρομολόγησης (classful routing). Όλα τα δίκτυα πρέπει να έχουν τη default μάσκα,
η έκδοση RIP-2, όπου μαζί με τους πίνακες δρομολόγησης στέλνεται και η μάσκα υποδικτύωσης (classless routing)

1.4.4 OSPF (Open Shortest Path First)

Το OSPF είναι πρωτόκολλο δρομολόγησης IP δικτύων. Είναι ένα πρωτόκολλο τύπου IGP(Interior Gateway Protocol), δηλαδή διανέμει την πληροφορία εντός ενός αυτόνομου συστήματος παρότι μπορεί να στείλει και να λάβει διαδρομές και από άλλα. Βασίζεται στον αλγόριθμο του Dijkstra. Δεν υπάρχει περιορισμός στον αριθμό των hops, ενώ το RIP περιορίζεται στα 15 hops. Έχει τη δυνατότητα να σπάσει το IP δίκτυο σε πολλά υποδίκτυα διαφόρων μεγεθών, παρέχοντας μεγαλύτερη ευελιξία στον διαχειριστή και επίσης παρέχει λειτουργία αυθεντικοποίησης των μηνυμάτων δρομολόγησης. Τέλος επιτρέπει τη μεταφορά και το μαρκάρισμα των διαδρομών οι οποίες εισάγονται σε ένα αυτόνομο σύστημα από εξωτερικά πρωτόκολλα.

Πλεονεκτήματα

- Έχει καλύτερη - γρηγορότερη σύγκλιση, διότι οι αλλαγές προωθούνται άμεσα και όχι περιοδικά.
- Αλλαγές στη δρομολόγηση συμβαίνουν άμεσα και όχι περιοδικά
- Οι ενημερώσεις στέλνονται μόνο σε περίπτωση αλλαγής και γίνονται με ip multicast μετάδοση
- Λιγότερο overhead στο δίκτυο, ιδιότητα σημαντική για μεγάλα δίκτυα.
- Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση το κόστος των συνδέσεων και έτσι προτιμάται η αληθινά βέλτιστη διαδρομή
- Το αντίτιμο που πληρώνουμε για τις περισσότερες δυνατότητες του πρωτοκόλλου είναι η πολυπλοκότητα στην ρύθμιση και στην άρση βλαβών
- Επίσης απαιτείται περισσότερη επεξεργαστική ισχύς και μνήμη στους δρομολογητές.

1.4.5 BGP (Border Gateway Protocol)

Το Border Gateway Protocol (BGP) είναι ένα από τα πιο συνήθη και δοκιμασμένα routing protocols (χρησιμοποιείται ευρέως στο internet). Το bgp δημιουργεί έναν πίνακα από IP networks ή "prefixes" τα οποία δηλώνουν την προσβασιμότητα μεταξύ των Autonomous Systems. Πρόκειται για ένα path vector protocol, το οποίο δεν βασίζει τις αποφάσεις για τις διαδρομές σε IGP metrics (ping times ή latency), αλλά η δρομολόγηση γίνεται βασισμένη στην διαδρομή (hops), σε πολιτικές του δικτύου ή/και σε μια σειρά από κανόνες.
Τα βασικά χαρακτηριστικά του είναι:

- Τύπου EGP πρωτόκολλο δρομολόγησης ανάμεσα σε αυτόνομα συστήματα (interautonomous system routing protocol)
- Πρωτόκολλο τακτικής (Policy Based)
- Είναι το defacto EGP πρωτόκολλο στο διαδίκτυο (και μοναδικό)
- Σχετικά απλό σε λειτουργία
- Πολύπλοκο σε διάρθρωση
- Απαιτεί προσεκτική σχεδίαση αφού όλος ο κόσμος μπορεί να δει και να επηρεαστεί από τυχόν λάθη μας
- Στιβαρό
- Επιτρέπει εύκολη κλιμάκωση (περισσότερες από 100,000 διαδρομές στους πίνακες δρομολόγησης του BGP στο διαδίκτυο)
- Είναι το μόνο πρωτόκολλο που μπορεί να χρησιμοποιηθεί ανάμεσα σε AS αφού έχει εγγενή υποστήριξη σε τακτική δρομολόγισης
- Υποστηρίζει classless δρομολόγηση
- Τρέχει σε περισσότερους από 100K δρομολογητές
- Η δυναμική και οι αρχές κλιμάκωσης του δεν έχουν γίνει ακόμα κατανοητές.

Ποιο είναι το βασικό πρόβλημα που επιλύει το BGP;

- Το διαδίκτυο αποτελείται από πολύ μεγάλο αριθμό δικτύων.
- Πολλά από αυτά έχουν κάποιου είδους αστάθεια, γνωστή ή άγνωστη

στου διαχειριστές τους.

- Συνέχεια στοιχεία του δικτύου αλλάζουν λειτουργική κατάσταση.
- Κάτω από αυτές τις συνθήκες η ευστάθεια του πρωτοκόλλου γίνεται

πρωταρχικός στόχος.

- Το BGP σχεδιάστηκε έχοντας αυτό σαν πρωταρχικό στόχο.
- Επίσης βασικός στόχος της σχεδίασης του ήταν να επιτρέπει στους

πάροχους να παίρνουν αποφάσεις δρομολόγησης με βάση την τακτική
που επιθυμούσαν ή ήταν υποχρεωμένοι να έχουν.

1. *Πως θα βρούμε τη συντομότερη διαδρομή RIP, OSPF, IS-IS*
2. *Πως θα βρούμε τη σταθερότερη διαδρομή BGP*

1.4.6 IGRP (Interior Gateway Routing Protocol)

Το Interior Gateway Routing Protocol (IGRP) είναι ένα διανυσματικό πρωτόκολλο δρομολόγησης (IGP) που εφευρέθηκε από τη Cisco. Χρησιμοποιείται από τους δρομολογητές για να ανταλλάξει τα στοιχεία δρομολόγησης μέσα σε ένα αυτόνομο σύστημα.

Το IGRP είναι ένα ιδιόκτητο πρωτόκολλο. Το IGRP δημιουργήθηκε εν μέρει για να υπερνικήσει τους περιορισμούς RIP όταν χρησιμοποιείται μέσα στα μεγάλα δίκτυα. Το πρωτόκολλο αυτό υποστηρίζει τις πολλαπλάσιες μερτήσεις για κάθε διαδρομή, συμπεριλαμβανομένου του εύρους ζώνης, της καθυστέρησης, του φορτίου, το MTU και της αξιοπιστίας για να συγκρίνουν δύο διαδρομές που αυτές οι μετρήσεις συνδυάζονται μαζί σε έναν μετρητή, χρησιμοποιώντας έναν τύπο που μπορεί να ρυθμιστεί μέσω της χρήσης των προετοιμασμένων σταθερών. Η μέγιστη αρίθμηση hop των iGRP-καθοδηγημένων πακέτων είναι 255 (προεπιλογή 100), και οι αναπροσαρμογές δρομολόγησης είναι ραδιοφωνική μετάδοση κάθε 90 δευτερόλεπτα (εξ ορισμού).

Το IGRP θεωρείται ένα Classful πρωτόκολλο δρομολόγησης. Επειδή το πρωτόκολλο δεν έχει κανέναν τομέα για μια μάσκα υποδικτύου, ο δρομολογητής υποθέτει ότι όλη η διεπαφή εξετάζεται μέσα στην ίδια CLASS A, CLASS B ή CLASS C έχει την ίδια μάσκα υποδικτύου με τη μάσκα υποδικτύου που διαμορφώνεται για τις διεπαφές. Αυτό αντιπαραβάλλει με τα πρωτόκολλα δρομολόγησης που μπορούν να χρησιμοποιήσουν

τις μάσκες υποδικτύου μεταβλητού μήκους. Τα πρωτόκολλα Classful έχουν γίνει λιγότερο δημοφιλή δεδομένου ότι είναι σπάταλα του διαστήματος διευθύνσεων IP.

Προκειμένου να αντιμετωπιστεί τα ζητήματα του διαστήματος διευθύνσεων και άλλων παραγόντων, η Cisco δημιούργησε το EIGRP (ενισχυμένο εσωτερικό πρωτόκολλο δρομολόγησης πυλών). Το EIGRP προσθέτει την υποστήριξη για VLSM (μάσκα υποδικτύου μεταβλητού μήκους) και προσθέτει το Diffusing Update Algorithm (DUAL) προκειμένου να βελτιωθεί η δρομολόγηση και να παρασχεθεί ένα loopless περιβάλλον.

1.4.7 EIGRP (Enhanced Interior Gateway Routing Protocol)

Το EIGRP είναι η ανανεωμένη έκδοση του Distance Vector πρωτοκόλλου IGRP. Για να μπορέσει όμως το EIGRP πρωτόκολλο να ανταλλάξει πληροφορίες και να λειτουργήσει σωστά, πρέπει να έχει άμμεση γειτονία με τους γειτονικούς του routers.Αυτή την γειτνίαση την αναπτύσσει μέσω του Hello protocol. Εκτός όμως από το Hello Protocol που χρησιμοποιεί, ένας άλλος βασικός παράγοντας ζωτικής σημασίας για την σωστή διατήρηση του δικτύου, είναι και οι χρόνοι ανταλλαγής αυτών των πακέτων.

Οι τεχνικές και οι πληροφορίες του IGRP ισχύουν κατά τη χρήση του EIGRP, αλλά η χρήση του EIGRP είναι πιο αποτελεσματικη.
Τα δίκτυα υπολογιστών που διασυνδέονται με το πρωτόκολλο EIGRP είναι πιο αναπτυγμένα δομικά.

Οι διαφορές μεταξύ του EIGRP και του IGRP είναι:

- Συμβατικότητα
- Metric
- Hop Count
- Αναδόμηση του πρωτοκόλλου
- Route tagging
- Έτσι λοιπόν μπορούμε να αναφέρουμε πιο αναλυτικά λίγα στοιχεία για τις σημαντικότερες διαφορές μεταξύ των δυο πρωτοκόλλων.

Το EIGRP υποστηρίζει multiprotocols ενώ το IGRP όχι.Αυτή η λειτουργία στηρίζεται στο γεγονός ότι το EIGRP πρωτόκολλο δεν διακινεί τα πακέτα μέσω του TCP, αλλά μιας δικιάς του σουίτας του, την RTP.

Το metric του EIGRP έχει άμεση σχέση με το metric του IGRP και είναι 256 υποπολλαπλάσια του. Με αυτόν τον τρόπο η επικοινωνία μεταξύ των router που υποστηρίζουν EIGRP και αυτών που υποστηρίζουν IGRP είναι άμεση και ταχύτατη. Η παραπάνω σχέση που αναφέραμε πηγάζει από το γεγονός ότι το metric του EIGRP είναι 32bit long, ενώ του IGRP metric είναι 24bit long.

Το hot count του IGRP είναι 255 ενώ του EIGRP είναι 224. Αρκετά μεγάλος αριθμός που του δίνει την δυνατότητα να εφαρμόζεται και σε πολύ μεγάλα δίκτυα υπολογιστών.

Το EIGRP και το IGRP ανταλλάσσουν πληροφορίες όταν όμως η εφαρμόζονται πάνω στα ίδια Autonomous Systems (AS).

Το EIGRP μαρκάρει όλους τους routers που μαθαίνει εξωτερικά από το Autonomous System που ανήκει σαν external, ακόμα και τους IGRP router. Το IGRP δεν μπορεί να κάνει αυτόν τον διαχωρισμό. Έτσι λοιπόν κατά τη διαδικασία καταχώρησης των γνωστών router και Segment (περιοχές δικτύου) που κάνει στο routing table το EIGRP, μαρκάρει με το flag "D" όλους τους EIGRP Router, ενώ το flag "EX" τους external. Άρα μια καταχώρηση από το routing table της μορφής D EX 192.168.0.0 ..., σημαίνει ότι αυτός ο router είναι EIGRP και external.

Το EIGRP κάνει τις καταχωρήσεις για το υπόλοιπο δίκτυο και την δομή του, σε τρεις λίστες (tables).

- Neighbor Table
- Topology Table
- Routing Table
- Τα tables αυτά, το πρωτόκολλο EIGRP τα καταχωρεί στην μνήμη RAM του router ώστε να μπορεί να έχει γρήγορη και άμεση πρόσβαση του σε αυτά.

1.4.8 IPv4 πίνακας δρομολόγησης

Κάθε καταχώρηση στον πίνακα δρομολόγησης αντιστοιχεί σε μία διαδρομή. Όταν ένας κόμβος πρέπει να υποβάλει ένα πακέτο IP, γίνεται αναζήτηση του πίνακα δρομολόγησης για τον κόμβο και για μια διαδρομή που ταιριάζει καλύτερα με τη διεύθυνση προορισμού του

πακέτου. Συνήθως, η διαδικασία έχει ως εξής:
• **Για host**: Μπορεί να σταλεί ένα πακέτο είτε απευθείας στον προορισμό του, ή μπορεί να σταλεί το πακέτο καθ 'οδόν προς τον προορισμό με μια προεπιλεγμένη διαδρομή (Network ID: 0.0.0.0, Subnet Mask: 0.0.0.0) στα σημεία στην προεπιλεγμένη πύλη του. Μια προεπιλεγμένη πύλη είναι ένας δρομολογητής που συνδέει επιμέρους τμήματα του δικτύου IP.
• **Για ένα δρομολογητή:** Ο δρομολογητής προωθεί ένα πακέτο, είτε χρησιμοποιώντας στατική διαδρομή για ένα συγκεκριμένο τμήμα του δικτύου, μια διαδρομή υποδοχής, ή μια προκαθορισμένη διαδρομή.

1.4.9 Τύποι Διαδρομών σε ένα πίνακα δρομολόγησης

Τοπική διαδρομή δικτύου:

Μια διαδρομή σε ένα συγκεκριμένο τοπικό δίκτυο ID. Η διαδρομή αυτή προσδιορίζει ένα τμήμα του δικτύου που συνδέεται άμεσα με τον κόμβο. Για μια τοπική διαδρομή του δικτύου, η στήλη Gateway (μερικές φορές αποκαλείται Επόμενη Hop) μπορεί να είναι κενό ή μπορεί να περιέχει τη διεύθυνση IP του interface για το τμήμα του δικτύου.

Απομακρυσμένη διαδρομή δικτύου:

Μια διαδρομή σε ένα συγκεκριμένο απομακρυσμένο δίκτυο ID. Η διαδρομή αυτή προσδιορίζει ένα τμήμα του δικτύου που δεν συνδέονται άμεσα με τον κόμβο, αλλά είναι διαθέσιμη σε έναν ή περισσότερους δρομολογητές. Για μια απομακρυσμένη διαδρομή δικτύου, το Gateway (Next Hop) στήλη είναι η διεύθυνση IP του τοπικού δρομολογητή που βρίσκεται μεταξύ του κόμβου και το απομακρυσμένο δίκτυο.

Host διαδρομή.

Μια διαδρομή σε μια συγκεκριμένη διεύθυνση IP (αναγνωριστικό δικτύου + υποδοχής ID) για το Internetwork. Αντί για λήψη απόφασης δρομολόγησης με βάση μόνο το αναγνωριστικό δικτύου, όπως συμβαίνει στην περίπτωση είτε σε τοπικό είτε σε απομακρυσμένο δίκτυο, αποφασίζει για τη δρομολόγηση μιας διαδρομής κεντρικού υπολογιστή βασισμενη στο συνδυασμό της ταυτότητας δικτύου και υποδοχής ID. Για μια

Host διαδρομή, η στήλη Προορισμός Δικτύου είναι η διεύθυνση IP και η στήλη είναι Netmask 255.255.255.255. Συνήθως, μια Host διαδρομή χρησιμοποιείται για να δημιουργήσει μια διαδρομή προσαρμοσμένη σε ένα συγκεκριμένο υπολογιστή για να ελέγξουν ή να βελτιστοποιήσουν συγκεκριμένα είδη Internetwork κυκλοφορίας.

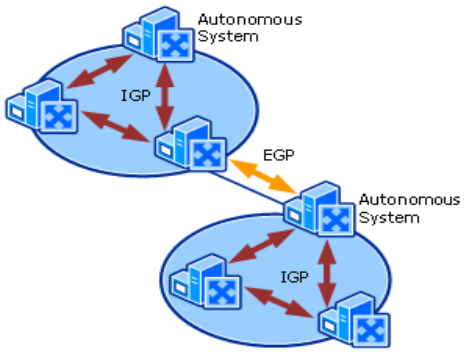
Προεπιλεγμένη διαδρομή:

Μια διαδρομή που χρησιμοποιείται όταν δεν υπάρχουν άλλες πιο κοντινές διαδρομές που να ταιριάζουν με τον προορισμό στον πίνακα δρομολόγησης. Συμπεριλαμβανομένης μιας προεπιλεγμένης διαδρομής στον πίνακα δρομολόγησης σημαίνει ότι ο πίνακας δρομολόγησης δεν χρειάζεται να αποθηκεύει διαδρομές για κάθε αναγνωριστικό δικτύου για το Internetwork. Χρησιμοποιώντας μια προκαθορισμένη διαδρομή, κατά συνέπεια, απλοποιείται η διαμόρφωση του host ή του δρομολογητή

1.4.10 Πρωτόκολλα δρομολόγησης μεταξύ και εντός των Αυτόνομων Συστημάτων

Τα αυτόνομα συστήματα χρησιμοποιούν δύο ειδών πρωτόκολλα δρομολόγησης για να ενημερώσουν τους δρομολογητές:

- Τα πρωτόκολλα που χρησιμοποιούνται για τη διανομή των πληροφοριών δρομολόγησης μεταξύ δύο ή περισσοτέρων αυτόνομα συστήματα είναι γνωστά ως Exterior Gateway πρωτόκολλα (EGPs).
- Τα πρωτόκολλα που χρησιμοποιούνται για τη διανομή των πληροφοριών δρομολόγησης μέσα σε ένα ενιαίο αυτόνομο σύστημα είναι γνωστό ως Interior Gateway πρωτόκολλα (IGPs).



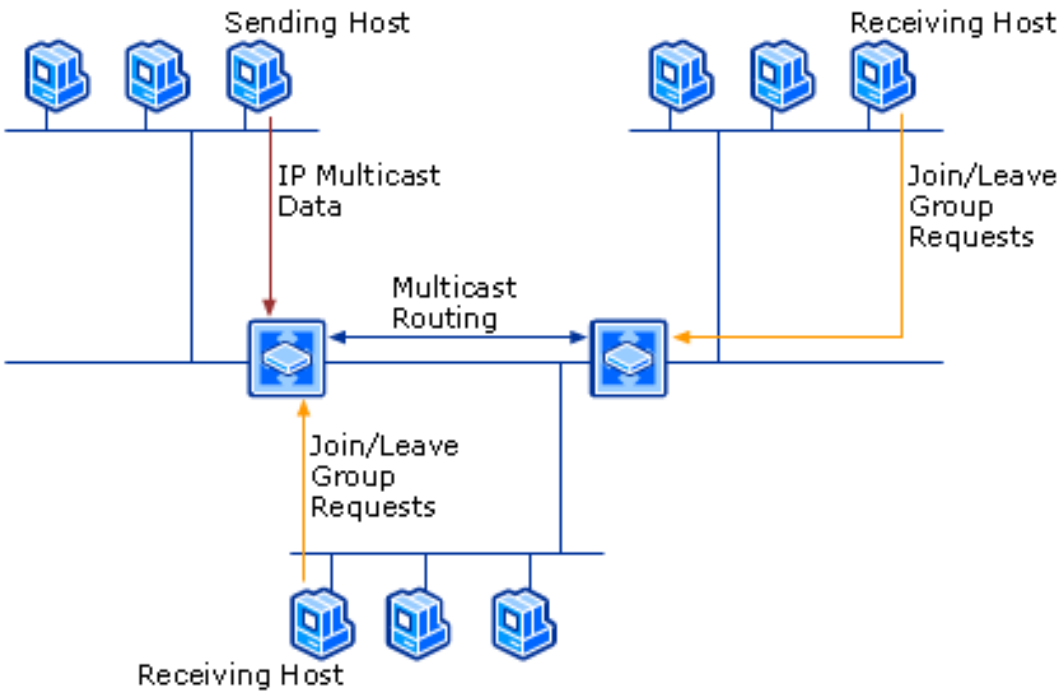
Εικόνα 2 Αυτόνομα συστήματα που χρησιμοποιούν εσωτερικά και εξωτερικά πρωτόκολλα επικοινωνίας

Τα EGPs είναι πρωτόκολλα δρομολόγησης μεταξύ του αυτόνομου συστήματος. Τα EGPs καθορίζουν τον τρόπο όπου όλες οι διαδρομές εντός του αυτόνομου συστήματος διαφημίζονται εκτός του αυτόνομου συστήματος. Οι δρομολογητές που συνδέουν αυτόνομα συστήματα με τη «σπονδυλική στήλη» του Internet χρησιμοποιούν EGP για να μεταδώσουν πληροφορίες δρομολόγησης ο ένας στον άλλο. Η ενημέρωση μπορεί να περιλαμβάνει τον κατάλογο των διαδρομών σε μια επίπεδη υποδομή δρομολόγησης ή τον κατάλογο των διαδρομών που συνοψίζονται σε μια ιεραρχική υποδομή δρομολόγησης.

1.5. IPv4 Multicasting

Η έννοια των μελών ενός group είναι βασική στο IP multicasting. Τα IP multicast datagrams στέλνονται σε ένα group και μόνο τα μέλη του group λαμβάνουν τα datagrams. Ένα group ταυτοποιείται από μια μοναδική IP multicast διεύθυνση η οποία είναι IP διεύθυνση στο Class D από 224.0.0.0 εώς 239.255.255.255. Αυτές οι Class D διευθύνσεις είναι γνωστές σαν group διευθύνσεις. Ένας host από την αφετηρία στέλνει multicast datagrams σε μια διεύθυνση group. Οι hosts προορισμού ενημερώνουν τον τοπικό δρομολογητή ότι χρειάζεται να συμμετάσχουν στο group.

Σε ένα IP multicast-enabled δίκτυο κάθε host μπορεί να στείλει IP multicast datagrams σε οποιαδήποτε group διεύθυνση και μπορεί να λάβει IP multicast datagrams από οποιαδήποτε group διεύθυνση ανεξάρτητα από την τοποθεσία του. Για να διευκολυνθεί αυτή η διαδικασία οι hosts και οι δρομολογητές του δικτύου πρέπει να υποστηρίζουν το IP multicasting. Οι hosts χρησιμοποιούν το Internet Group Management Protocol (IGMP) για να εγκαθιστούν τα μέλη του group. Ενώ οι δρομολογητές χρησιμοποιούν multicast πρωτόκολλα δρομολόγησης για την προώθηση των multicast δεδομένων. Το παρακάτω σχήμα επεξηγεί ένα multicast-enabled intranet:



Εικόνα 3 Multicast-Enabled Network

Στο παραπάνω σχήμα οι hosts και οι δρομολογητές είναι multicast-enabled έτσι ώστε να μπορούν να συμβούν τα παρακάτω :

- Ο host- αποστολέας στέλνει multicast datagrams σε μια σχεδιασμένη group διεύθυνση.
- Οι δρομολογητές προωθούν τα multicast datagrams σε οποιαδήποτε δικτυακά τμήματα που περιλαμβάνουν μέλη του group. Οι δρομολογητές μπορούν να προωθήσουν multicast κίνηση δια μέσου ενός δικτύου, μεταξύ δικτύων και διαμέσου του διαδικτύου.
- Οι hosts δέκτες πληροφορούν τον τοπικό δρομολογητή να πάρει μέρος στο group και έπειτα λαμβάνουν όλα τα επόμενα datagrams που στέλνονται στη διεύθυνση του group.
- Αν κάποιος host- δέκτης αφήσει το group και διακρίνει ότι μπορεί να είναι το τελευταίο μέλος του group στο υποδίκτυο, μπορεί να επικοινωνήσει με τον τοπικό δρομολογητή για να αφήσει το group πληροφορώντας τον να σταματήσει την προώθηση των multicast datagrams σε αυτό το υποδίκτυο.

1.5.1 Πλεονεκτήματα του IP Multicasting

Το Multicasting παρέχει ένα ικανό τρόπο να υποστηρίξει εφαρμογές του δικτύου με υψηλό εύρος ζώνης:

- Το Multicasting μπορεί να μειώσει εντυπωσιακά την κίνηση στο δίκτυο στέλνοντας ένα μοναδικό αντίγραφο δεδομένων.
- Οι hosts μπορούν να συντονίζουν τα λειτουργικά στοιχεία του multicasting χωρίς αναβαθμίσεις του hardware.
- Επειδή οι νεότεροι δρομολογητές ήδη υποστηρίζουν την multicast προώθηση και τα multicast πρωτόκολλα δρομολόγησης, αν χρησιμοποιείται multicasting σε ένα δίκτυο είναι πρακτικό και επικερδές.

Το Multicasting είναι χρήσιμο για πολλών ειδών εφαρμογών, όπως τα παρακάτω:

- Multimedia, όπως είναι οι video διασκέψεις και οι υνεργασίες μέσω υπολογιστών.
- Αυτόματη ανίχνευση πηγών σε ένα διαδίκτυο (για παράδειγμα, σε ένα Windows Server 2003, TCP/IP router discovery χρησιμοποιείται multicasting by default, και WINS χρησιμοποιεί multicasting κατά τη διάρκεια αυτόματης ανίχνευσης των αιτούμενων partners).
- Datacasting όπως είναι file distribution (διανομή αρχείων) ή συγχρονισμός database.
- Mobile computer υποστηρίζει για παράδειγμα remote address book updating.
- Διανομή των organizational publications.

1.5.2 Πώς λειτουργεί το IPv4 Multicasting

Το IP multicasting είναι αυτός που στέλνει ένα μοναδικό datagram σε πολλαπλούς hosts σε ένα δίκτυο. Από τις τρεις μεθόδους μεταφοράς που υποστηρίζονται από το IP ,το multicasting είναι η μέθοδος η οποία είναι η πιο πρακτική για μεταφορά από έναν-σε-πολλούς. Σε αντίθεση με το IP multicasting, το IP unicasting στέλνει ένα ξεχωριστό datagram σε κάθε host. Το IP broadcasting στέλνει ένα μοναδικό datagram σε όλους τους hosts σε ένα συγκεκριμένο τμήμα του δικτύου.

Πριν σταλούν ή ληφθούν IP multicast δεδομένα, ένα δίκτυο πρέπει να υποστηρίζει την λειτουργία multicasting, όπως παρακάτω:

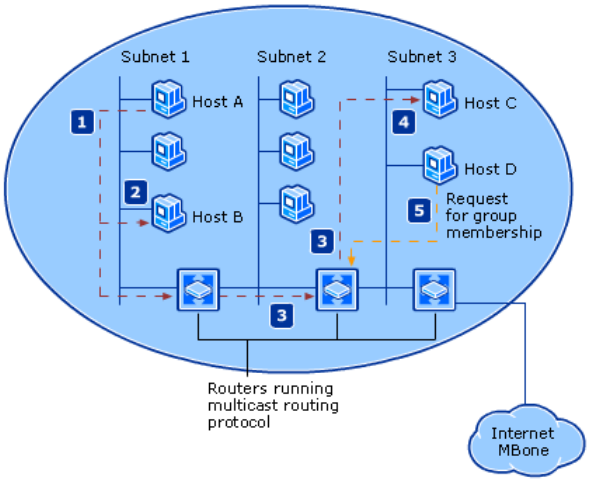
- Οι hosts πρέπει να συντονίζονται για να στείλουν και να λάβουν multicast δεδομένα.
- Οι δρομολογητές πρέπει να υποστηρίζουν το Internet Group Membership Protocol (IGMP), την multicast προώθηση και τα multicast πρωτόκολλα δρομολόγησης.

1.5.3 IP Multicasting αρχιτεκτονική

Για να υποστηριχτεί το multicasting σε ένα υπερδίκτυο, οι hosts και οι δρομολογητές πρέπει να είναι multicast-enabled. Σε ένα IP multicast-enabled δίκτυο κάθε host μπορεί να στείλει IP multicast datagrams και μπορεί να λάβει IP multicast datagrams, περιλαμβάνοντας αυτά που στέλνονται και λαμβάνονται μέσω του Internet.

Ο αποστολέας-host στέλνει multicast datagrams σε μια μεμονωμένη Class D IP διεύθυνση, γνωστή σαν διεύθυνση group. Κάθε host ο οποίος ενδιαφέρεται να λαμβάνει datagrams επικοινωνεί με ένα τοπικό δρομολογητή για να συμμετάσχει στο multicast group και έπειτα λαμβάνει όλα τα διαδοχικά datagrams που έχουν σταλεί σε αυτή τη διεύθυνση. Οι δρομολογητές χρησιμοποιούν ένα multicast πρωτόκολλο δρομολόγησης για να διευθύνει ποια υποδίκτυα συμπεριλαμβάνουν τουλάχιστον ένα μέλος multicast group που ενδιαφέρεται και για να προωθήσουν τα multicast datagrams μόνο σε αυτά τα υποδίκτυα τα οποία έχουν group μέλη ή σε ένα δρομολογητή ο οποίος έχει στο downstream group μέλη. Η επικεφαλίδα του multicast datagram συμπεριλαμβάνει μία Time-to-Live (TTL) τιμή η οποία καθορίζει πόσο μακριά μπορούν να προωθήσουν ένα multicast datagram οι δρομολογητές.

Το παρακάτω σχήμα δείχνει την αρχιτεκτονική του IPv4 Multicasting.



Εικόνα 4 IP Multicasting Architecture

Σε αυτό το σχήμα συμβαίνουν τα παρακάτω:

1. Ο Host A στο Subnet 1 είναι η multicasting πηγή και στέλνει τα multicast δεδομένα σε μια multicast group διεύθυνση.
2. Ο Host B στο Subnet 1 έχει ζητήσει να γίνει μέλος στο group από τον τοπικό δρομολογητή. Επειδή ο Host B έχει γίνει μέλος στο multicast group, ο adapter του δικτύου ακούει για datagrams που στέλνει στη multicast group διεύθυνση. Ο εναπομείναντος host στο Subnet 1 δεν έχει ζητήσει να συμμετάσχει στο group και σαν αποτέλεσμα ο adapter του δικτύου φιλτράρει την κίνηση που στέλνεται στη multicast διεύθυνση του group.
3. Οι δρομολογητές προωθούν τα multicast δεδομένα σε όποιο υποδίκτυο έχει μέλη του group ή σε κάποιον δρομολογητή ο οποίος έχει στο downstream μέλη. Σε αυτό το παράδειγμα ,οι δρομολογητές προωθούν multicast δεδομένα από το Subnet 1 στο Subnet 3.Επιπλέον, τα δεδομένα στέλνονται διαμέσου του Subnet 2, παρόλο που δεν υπάρχουν μέλη του group members, επειδή υπάρχουν μέλη στο downstream.
4. Ο Host C στο Subnet 3 έχει ζητήσει να γίνει μέλος του group και να λαμβάνει τα multicast δεδομένα.
5. Ο Host D στο Subnet 3 στέλνει μια αίτηση στον τοπικό δρομολογητή να πάρει μέρος στο group. Όταν ο Host D πάρει μέρος στο group, ο adapter του δικτύου θα περιμένει την κίνηση που στέλνεται στη multicast group διεύθυνση.

Εναλλακτικά, τα δεδομένα multicast μπορεί να προέρχονται από το multicast-enabled portion του Internet, γνωστό σαν MBone.

1.5.4 Μέλη του IP Multicasting

Host -λαμβάνων ή δέκτης	Είναι κάθε πελάτης ή server του διαδικτύου. Ένας **multicast-enabled** host που εναρμονίζεται για να στέλνει κα να λαμβάνει (ή μόνο να στέλνει) δεδομένα multicast.
Δρομολογητής	Ένας multicast δρομολογητής είναι ικανός να διαχειρίζεται τις απαιτήσεις του host και να συμμετάσχει ή να αφήσει το group και να προωθήσει τα δεδομένα multicast στα υποδίκτυα τα οποία περιέχουν μέλη του group.
Multicast διεύθυνση	Μία Class D IP διεύθυνση χρησιμοποιείται για να στέλνει IP multicast δεδομένα. Μία IP multicast πηγή στέλνει τα δεδομένα σε μια μοναδική

	multicast διεύθυνση. Μια συγκεκριμένη IP multicast διεύθυνση είναι επίσης γνωστή σαν group διεύθυνση.
Multicast group	Ένα multicast group είναι το σύνολο των hosts οι οποίοι «ακούν» μια συγκεκριμένη IP multicast διεύθυνση. Ένα multicast group είναι επίσης γνωστό σαν group των hosts.
MBone	Το IP multicast backbone, ή το τμήμα του διαδικτύου που υποστηρίζει την multicast δρομολόγηση.

Πίνακας 1 Στοιχεία του IPv4 Multicast

1.5.5 Σύγκριση Unicast και Multicast Δρομολόγησης

Χαρακτηριστικά ***Unicast Routing***	*Χαρακτηριστικά* ***Multicast Routing***
Η Unicast δρομολόγηση στέλνεται σε ένα παγκόσμιο μοναδικό προορισμό.	Η Multicast δρομολόγηση στέλνεται σε ένα «αόριστο» group προορισμό.
Οι Unicast διαδρομές στον πίνακα δρομολόγησης συνοψίζουν μια σειρά από παγκόσμιους μοναδικούς προορισμούς.	Επειδή οι διευθύνσεις group αντιπροσωπεύουν διαφορετικά group με διαφορετικά μέλη, οι group διευθύνσεις δεν μπορούν να γενικευθούν στον IP multicast πίνακα προώθησης.
Οι Unicast διαδρομές είναι συγκριτικά σταθερές έτσι ώστε ο πίνακας δρομολόγησης να χρειάζεται να ενημερωθεί μόνο όταν η τοπολογία του δικτύου αλλάζει. Τα Unicast πρωτόκολλα δρομολόγησης ενημερώνουν τον unicast πίνακα δρομολόγησης.	Η τοποθεσία των group μελών δεν είναι σταθερή, έτσι ώστε ο IP multicast πίνακας προώθησης ίσως χρειαστεί να ενημερώνεται όταν ένα μέλος του group συμμετέχει ή εγκαταλείπει ένα multicast group. Τα Multicast πρωτόκολλα δρομολόγησης ενημερώνουν τον IP multicast πίνακα προώθησης.

Πίνακας 2 Σύγκριση IPv4 unicast και multicast

1.6. IP Multicasting Protocols

Μια ποικιλία από πρωτόκολλα χρησιμοποιούνται για πολλές εφαρμογές του IP multicasting. Το παρακάτω σχήμα με συντομία προσδιορίζει τα πρωτόκολλα που περιγράφονται σε αυτό την παράγραφο.

Πρωτόκολλα που χρησιμοποιούνται για IP Multicasting:

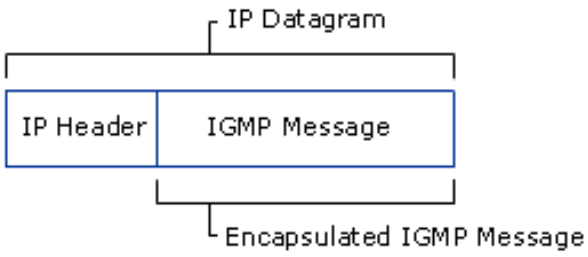
Πρωτόκολλο	*Περιγραφή*
IGMP	Internet Group Management πρωτόκολλο. Οι hosts χρησιμοποιούν αυτό το πρωτόκολλο για να κάνουν προτάσεις για μέλη group. Οι δρομολογητές χρησιμοποιούν αυτό το πρωτόκολλο για να ρωτήσουν για ενεργά μέλη group σε ένα υποδίκτυο. (Σημείωση: IPv6 χρησιμοποιεί Multicast Listener Discovery (MLD) αντί για IGMP για να διευθύνει τη συμμετοχή στο group .)
DVMRP	Distance Vector Multicast Routing Protocol. Είναι ένα multicast πρωτόκολλο δρομολόγησης.
MOSPF	Multicast Open Short Path First, multicast πρωτόκολλο δρομολόγησης.
PIM	Protocol Independent Multicast. Ανεξάρτητο πρωτόκολλο Multicast δρομολόγησης.
MADCAP	Multicast Address Dynamic Client Allocation Protocol. Αυτό το πρωτόκολλο καθιστά ικανό ένα host να ζητήσει μια IP multicast διεύθυνση από ένα multicast server.
PGM	Pragmatic General Multicast. PGM είναι ένα αξιόπιστο multicast πρωτόκολλο μεταφοράς. Τυπικά, τα multicast datagrams μεταφέρονται χρησιμοποιώντας UDP, το οποίο είναι ένα κληρονομικό μη αξιόπιστο πρωτόκολλο μεταφοράς. Οι hosts και οι δρομολογητές οι οποίοι είναι PGM- ικανοί μπορούν να ανακτήσουν χαμένα multicast datagrams.

Πίνακας 3 Πρωτόκολλα του IPv4 Multicasting

1.6.1 IGMP (Internet Group Management Protocol)

Το Internet Group Management Protocol (IGMP) συντηρεί host group μέλη σε ένα τοπικό υποδίκτυο. Οι hosts χρησιμοποιούν το IGMP για να επικοινωνήσουν τις αιτήσεις μελών με τον τοπικό multicast δρομολογητή. Οι δρομολογητές λαμβάνουν τις αιτήσεις των μελών και περιοδικά στέλνουν ερωτήματα για να καθορίσουν ποιοι hosts είναι ενεργοί ή ανενεργοί σε ένα τοπικό υποδίκτυο. Αυτό το πρωτόκολλο απαιτείται για να υποστηρίξει το

Level 2 multicasting. Τα IGMP μηνύματα συμπυκνώνονται σε IP datagrams και χρησιμοποιούν την τιμή 0x02. Το παρακάτω σχήμα επεξηγεί το datagram.



Εικόνα 5 Encapsulated IGMP Message

Υπάρχουν τρεις εκδόσεις του IGMP:

- IGMP version 1 παρέχεται από το TCP/IP για Microsoft Windows NT Server 4.0 Service Pack 3 και παλιότερα.
- IGMP version 2 παρέχεται από το TCP/IP για Microsoft Windows NT Server 4.0 Service Pack 4 και αργότερα για Windows 2000. Οι δρομολογητές χρησιμοποιώντας αυτή την έκδοση είναι συμβατοί με τους hosts που χρησιμοποιούν την IGMP version 1.
- IGMP version 3 παρέχεται από τοTCP/IP για Windows XP και Windows Server 2003. Οι Routers χρησιμοποιώντας αυτή την έκδοση είναι συμβατοί με τους hosts που χρησιμοποιούν την IGMP version 2 or IGMP version 1.

1.6.2 Πρωτόκολλα Multicast Routing: DVMRP, MOSPF, και PIM

Οι στόχοι των multicast πρωτοκόλλων δρομολόγησης περιλαμβάνουν τα παρακάτω:

- Προώθηση κίνησης μακριά από την πηγή για να αποτραπούν ατέρμονες επαναλήψεις.
- Μείωση ή ελαχιστοποίηση κίνησης στα υποδίκτυα που δεν χρειάζεται να λάβουν
- Ελαχιστοποίηση CPU και χρήση μνήμης στον δρομολογητή για να εξασφαλίζεται κλιμάκωση.
- Μείωση κίνησης πάνω από ένα πρωτόκολλο δρομολόγησης.
- Μείωση συμμετοχής στη λανθάνουσα κατάσταση, η οποία είναι ο χρόνος που χρειάζεται για το πρώτο μέλος group στο υποδίκτυο να αρχίσει να λαμβάνει group κίνηση.

Τα Multicast πρωτόκολλα δρομολόγησης χρησιμοποιούν μια ποικιλία από αλγόριθμους για να δημιουργήσουν ικανοποιητική μεταφορά μονοπατιών μέσω του υπερδικτύου. Οι Unicast δρομολογητές χρησιμοποιούν τον IP προορισμό διεύθυνσης για να προωθήσει τη κίνηση προς τον προορισμό. Επειδή η multicast κίνηση στέλνεται σε μια group διεύθυνση, multicast δρομολογητές χρησιμοποιούν την διεύθυνση αποστολέα για να προωθήσουν την κίνηση μακριά από την πηγή για να αποφύγουν looping την κίνηση πίσω στην πηγή .

1.6.3 Distance Vector Multicast Routing Protocol (DVMRP)

Το DVMRP είναι ένα multicast πρωτόκολλο δρομολόγησης το οποίο αναπτύσσεται από το Routing Information Protocol (RIP), ένα unicast πρωτόκολλο δρομολόγησης το οποίο προωθεί datagrams, βασισμένο σε πληροφορίες για την επόμενη μετάβαση προς τον προορισμό. Σε αντίθεση με το RIP, το DVMRP προωθεί τα datagrams βασισμένα σε πληροφορίες σχετικές με την προηγούμενη αναπήδηση προς τα πίσω στην πηγή.

Το DVMRP χτίζει ένα μεταφορικό δέντρο για να καθορίσει που να προωθηθούν τα datagrams. Πλημμυρίζει τα πρώτα multicast datagrams σε ένα multicast group μέσω του υπερδικτύου και έπειτα περικόπτει τα κλαδιά του δέντρου που οδηγούν στα υποδίκτυα τα οποία δεν περιλαμβάνουν μέλη group.

Το DVMRP είναι το πιο ικανοποιητικό σε περιβάλλοντα, όπου τα multicast μέλη groups απλώνονται πάνω στο υπερδίκτυο. Το DVMRP τρέχει στο υπερδίκτυο με multicast δρομολογητές και επίσης υποστηρίζει τη διάνοιξη σήραγγας, ενσωματώνοντας ένα multicast datagram σε ένα unicast datagram και προωθώντας το μέσω δρομολογητών.

1.6.4 Multicast OSPF (MOSPF)

Το MOSPF είναι ένα multicast πρωτόκολλο δρομολόγησης το οποίο επεκτείνει ένα Open Shortest Path First (OSPF). Αυτό το πρωτόκολλο χτίζει ένα δέντρο μεταφοράς για να καθορίσει που να προωθηθούν τα datagrams χρησιμοποιώντας πληροφορίες μελών group από την βάση δεδομένων της ζεύξης του IGMP και του OSPF. Τα δέντρα χτίζονται μετά από αίτηση κάθε ζευγαριού source-group.

Το MOSPF έχει ως στόχο για την οργάνωση του δικτύου και δεν ανεβαίνει κλίμακα. Το MOSPF απαιτεί το OSPF σαν βοήθημα σε unicast πρωτόκολλο δρομολόγησης. Μπορεί μερικές φορές να τοποθετήσει ένα βαρύ φορτίο στην CPU του δρομολογητή.

Το MOSPF είναι πιο ικανοποιητικό σε περιβάλλοντα όπου τα multicast group μέλη διασκορπίζονται πυκνά πάνω από το υπερδίκτυο. Δεν υποστηρίζει τη διάνοιξη σήραγγας αλλά μπορεί να εργαστεί σε multicast περιβάλλοντα με non-MOSPF δρομολογητές.

1.6.5 Protocol-Independent Multicast (PIM)

Το PIM αποτελείται από δύο πρωτόκολλα: PIM Dense Mode (PIM-DM) και PIM Sparse Mode (PIM-SM). Το PIM-DM είναι πιο ικανοποιητικό σε περιβάλλοντα όπου τα μέλη multicast group απλώνονται πυκνά πάνω στο υπερδίκτυο. Το PIM-SM είναι πιο ικανοποιητικό σε περιβάλλοντα όπου τα group μέλη απλώνονται αραιά. Ένα multicast group που χρησιμοποιεί PIM μπορεί να δηλωθεί το ίδιο ως αραιό ή πυκνό.

Το PIM protocol καθορίζει τις διαδρομές στα multicast groups των οποίων τα μέλη αναπτύσσονται σε ευρείες περιοχές και σε ενδιάμεσα υπερδίκτυα. Το PIM λειτουργεί ανεξάρτητα σε κάθε unicast πρωτόκολλο δρομολόγησης, παρόλο που χρησιμοποιεί τον υπάρχων unicast πίνακα δρομολόγησης.

1.6.5.1 PIM-DM

Αυτό το πρωτόκολλο σχεδιάστηκε για τα multicast groups των οποίων τα μέλη αaπλώνονται πυκνά πάνω από μια περιοχή όπου το bandwidth είναι άφθονο. Όπως το DVMRP, το PIM-DM πρώτα «πλημμυρίζει» την multicast κίνηση μέσω του υπερδικτύου και έπειτα περιορίζει σε έκταση τα υποδίκτυα τα οποία δεν έχουν group μέλη. Το PIM-DM χρησιμοποιείται με το PIM-SM. Το PIM-DM δεν έχει καλή κλιμάκωση.

1.6.5.2 PIM-SM

Το PIM-SM είναι το πιο ευρύ χρησιμοποιημένο multicast πρωτόκολλο δρομολόγησης. Σχεδιάστηκε για multicast groups με μέλη που απλώνονται αραιά σε μια μεγάλη περιοχή και είναι πιο ικανοποιητικό σε WAN περιβάλλον. Η μέθοδος flood-and-prune που χρησιμοποιείται από το PIM-DM μπορεί να προκαλέσει μη απαραίτητη κίνηση. Σε αντίθεση , το PIM-SM προωθεί την multicast κίνηση μόνο σε δρομολογητές που το ζητούν.

Με το PIM-SM, οι δρομολογητές πρέπει να συμμετέχουν και να αφήνουν τα multicast groups να λάβουν ή να σταματήσουν να λαμβάνουν multicast κίνηση.

1.6.6 MADCAP

Το Multicast Address Dynamic Client Allocation Πρωτόκολλο (MADCAP) είναι μία μέθοδος για τους hosts για να απαιτούν μία multicast διεύθυνση από έναν multicast server που διανέμει διευθύνσεις. Αν πολλαπλοί hosts χρησιμοποιούν την ίδια IP multicast διεύθυνση για διαφορετικές εφαρμογές, τότε η multicast κίνηση μπορεί να προωθηθεί σε λανθασμένο group. Το MADCAP εμποδίζει αυτό το πρόβλημα διανέμοντας μοναδικές Multicast διευθύνσεις. Αυτό υποστηρίζει δυναμική εκχώρηση και διευθέτηση των IP multicast διευθύνσεων σε δίκτυα βασισμένα στο TCP/IP.

Το MADCAP είναι μια επέκταση του Dynamic Host Configuration Protocol (DHCP), αλλά είναι ξεχωριστό από το DHCP. Μοναδικές multicast διευθύνσεις διανέμονται σε έναν DHCP πελάτη, όμοια όπως οι unicast διευθύνσεις εκχωρούνται στους πελάτες.

1.6.7 PGM

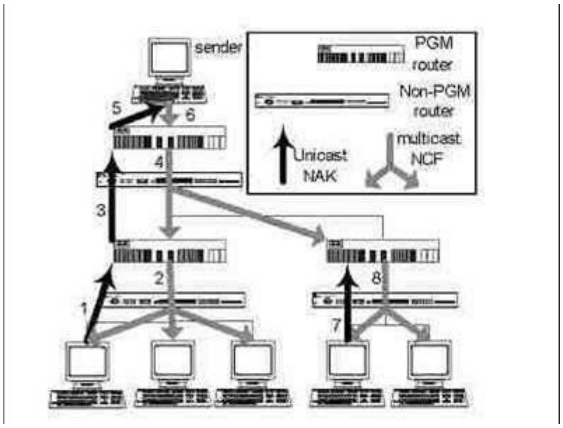
Το PGM- Pragmatic General Multicast έχει τα εξής γενικά χαρακτηριστικά :

- δημιουργείται μια δεντρική δομή από PGM-enabled δρομολογητές πάνω από το υπάρχον multicast enabled δίκτυο
- βασίζεται στη unicast αποστολή αρνητικών επιβεβαιώσεων από τους παραλήπτες (NAK) σε περίπτωση λάθους οι οποίες προωθούνται προς την πηγή
- μεταδίδει μόνο ένα NAK για κάθε χαμένο πακέτο σε κάποιο υποδέντρο
- Οι επαναμεταδόσεις γίνονται μόνο σε εκείνα τα υποδέντρα τα οποία έχουν παραλήπτες που έχουν εντοπίσει χαμένα πακέτα.

Η υποστήριξη του PGM από εταιρείες όπως CISCO, Microsoft, Talarian, Tibco, Nortel, η ελεύθερη διάθεση του κώδικα του που επιτρέπει την δημιουργία εφαρμογών που θα το

υποστηρίζουν καθώς και τα πολύ καλά χαρακτηριστικά του, το θέτουν ως το μηχανισμό reliable multicast που θα επικρατήσει.

Στην παρακάτω εικόνα ακολουθεί ενδεικτικό παράδειγμα λειτουργίας του PGM :



Εικόνα 6 Λειτουργία PGM

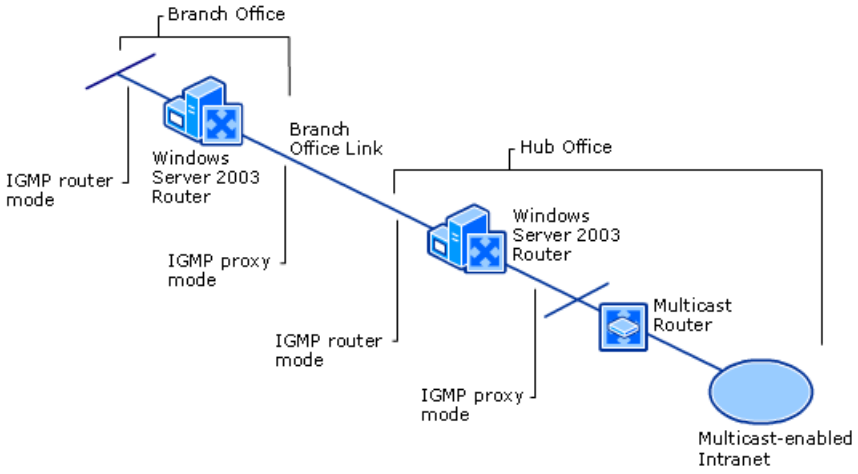
1. Ο δέκτης στέλνει ένα μήνυμα NAK (negative acknowledgement) για το χαμένο πακέτο.
2. Ο PGM δρομολογητής στέλνει με multicasts ένα NCF μήνυμα (NAK επιβεβαίωση)
3. Ο δρομολογητής στέλνει με unicast ένα NAK στον «γονιό» του, ο οποίος
4. στέλνει με multicast ένα NCF
5. Ένα unicast NAK στέλνεται στον αποστολέα,
6. ο οποίος αποκρίνεται με ένα multicast NCF
7. Αργότερα, κάποιος άλλος δέκτης εντοπίζει την απώλεια του ίδιου πακέτου και στέλνει με unicast δρομολόγηση ένα NAK στον PGM «γονιό»,
8. ο οποίος δρομολογεί με multicast ένα NCF
9. Ο «γονιός» δεν στέλνει προς την άνω ζεύξη NAK μήνυμα, γιατί έχει ήδη ειδοποιηθεί για την λήψη του αντίστοιχου NCF.

1.6.8 Προώθηση IP multicast κίνησης

Η διαδικασία της multicast προώθησης από τους hosts στην διεπαφή κάποιου δρομολογητή λειτουργεί ως εξής:

1. Ένας multicast host στέλνει multicast κίνηση σε μία συγκεκριμένη διεύθυνση group, και αν η διεύθυνση δεν είναι τοπική, ο IGMP δρομολογητής λαμβάνει την κίνηση.

2. Όταν ο δρομολογητής λαμβάνει το πρώτο datagram για κάποιο συγκεκριμένο multicast group, το IGMP πρωτόκολλο δρομολόγησης προσθέτει μία είσοδο στον IP multicast πίνακα προώθησης για να δηλώσει ότι υπάρχουν μέλη του group στην IGMP διεπαφή.
3. Η multicast κίνηση μεταβαίνει στην διαδικασία της προώθησης και βασισμένη στις εισόδους του πίνακα προώθησης, προωθείται χρησιμοποιώντας την IGMP διεπαφή.
4. Ο γειτονικός multicast δρομολογητής λαμβάνει την multicast κίνηση και προχωράει και αυτή στην διαδικασία προώθησης. Ο multicast δρομολογητής είτε προωθεί την κίνηση σε μέλη του group ή σιωπηλά την καταστρέφει ανάλογα με τα δεδομένα στον IP multicast πίνακα προώθησης.



Εικόνα 7 Multicast Προώθηση

Για τον κλάδο -branch office δρομολογητή, όλες οι διεπαφές προστίθενται στο IGMP πρωτόκολλο δρομολόγησης. Οι διεπαφές του κλάδου υποδικτύου- branch office, σχηματίζονται για τον IGMP δρομολογητή, και η διεπαφή που συνδέει το hub office δρομολογητή σχηματίζεται για τον IGMP proxy. Η διεπαφή που συνδέει τον hub office δρομολογητή μπορεί να είναι διεπαφή τοπικού δικτύου (LAN) ή διεπαφή κατ' απαίτηση.

Για τον hub office δρομολογητή, όλες οι διεπαφές προστίθενται στο IGMP πρωτόκολλο δρομολόγησης. Η διεπαφή που συνδέει τον branch office δρομολογητή σχεδιάζεται για τον IGMP δρομολογητή. Η διεπαφή μπορεί να είναι και αυτή μία διεπαφή LAN ή κατ' απαίτηση διεπαφή. Η διεπαφή που συνδέεται στο multicast-enabled δίκτυο σχηματίζεται για τον IGMP proxy.

Όταν κάποιος host συμμετέχει ή εγκαταλείπει ένα multicast group, αυτό στέλνει ένα IGMP μήνυμα μέλους. Το μήνυμα αντιγράφεται μέσω της ζεύξης του branch office στο multicast-enabled δίκτυο. Η Multicast κίνηση από τον branch office των hosts αντιγράφεται από το branch office υποδίκτυο μέσω της the branch office σύνδεσης στο multicast-enabled δίκτυο.

Αν η multicast κίνηση στέλνεται μεταξύ δύο hosts στο branch office δίκτυο, η κίνηση αντιγράφεται στην σύνδεση του branch office, με αποτέλεσμα χαμηλή χρήση του εύρους ζώνης. Μπορεί κάποιος να σχεδιάσει εφαρμογές και MADCAP servers να χρησιμοποιούν IP multicast διευθύνσεις (239.0.0.0 μέχρι 239.254.255.255) για να προστατεύσουν την τοπική branch office multicast κίνηση να αντιγραφεί. Σε αυτή την περίπτωση η διεπαφή στο hub office σχεδιάζεται σύμφωνα με τα κατάλληλα όρια.

1.7. Πρόβλημα του IPv4

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπ' όψη του τους παρακάτω παράγοντες:

- Την πρόσφατη, ταχύτατη –με εκθετικό ρυθμό- ανάπτυξη του διαδικτύου και τη συνακόλουθη εξάντληση του χώρου διευθύνσεων του πρωτοκόλλου IPv4. Οι IPv4 διευθύνσεις που έχουν απομείνει προς διάθεση είναι πλέον τόσο λίγες, ώστε κάποιοι οργανισμοί έχουν αναγκαστεί να χρησιμοποιούν το πρωτόκολλο NAT (Network Address Translator), το οποίο αντιστοιχεί πολλές ιδιωτικές («ψεύτικες», «αόρατες» για τους χρήστες των λοιπών δημοσίων IPv4 διευθύνσεων) IP διευθύνσεις σε μια δημόσια IPv4 διεύθυνση. Παρ' ότι όμως το πρωτόκολλο NAT επιλύει ένα μέρος του προβλήματος, έχει αρκετά μειονεκτήματα. Συγκεκριμένα, δεν υποστηρίζει την προτυποποιημένη ασφάλεια σε επίπεδο στρώματος δικτύου, η αντιστοίχιση των ιδιωτικών διευθύνσεων σε μια δημόσια δε γίνεται σωστά στα πρωτόκολλα που ανήκουν στα ανώτερα επίπεδα της στοίβας πρωτοκόλλων του δικτύου και μπορεί να δημιουργηθούν προβλήματα κατά τη διασύνδεση δύο οργανισμών, οι οποίοι χρησιμοποιούν ιδιωτικό χώρο διευθύνσεων. Τέλος ακόμα και αν δε ληφθούν υπ' όψη τα παραπάνω μειονεκτήματα, η εκθετική αύξηση των μηχανημάτων που απαιτούν IP διευθύνσεις, αργά ή γρήγορα θα οδηγήσει στην εξάντληση και των επιπλέον διευθύνσεων που προσφέρονται μέσω του πρωτοκόλλου NAT.

- Την ανάπτυξη του διαδικτύου και ικανότητα των δρομολογητών του δικτύου κορμού του διαδικτύου να διατηρούν μεγάλους πίνακες δρομολόγησης. Λόγω του τρόπου με τον οποίο διανέμονται οι διευθύνσεις δικτύου στο IPv4 υπάρχουν πάνω από 70000 καταχωρήσεις διαδρομών στους δρομολογητές του δικτύου κορμού του διαδικτύου. Η παρούσα υποδομή για τη δρομολόγηση στο πρωτόκολλο IPv4 είναι συνδυασμός επίπεδης και ιεραρχικής δρομολόγησης.
- Η ανάγκη για απλούστερη ρύθμιση παραμέτρων. Οι περισσότερες από τις παρούσες υλοποιήσεις του πρωτοκόλλου IPv4 απαιτούν η ρύθμιση των μηχανημάτων του δικτύου να γίνεται είτε με μη αυτόματο τρόπο, είτε με τη χρήση stateful address configuration protocols, όπως το πρωτόκολλο DHCP (Dynamic Host Configuration Protocol). Λόγω της παρουσίας πολύ περισσότερων μηχανημάτων που θα χρησιμοποιούν IP διευθύνσεις, υπάρχει ανάγκη να βρεθεί ένας απλούστερος και πιο αυτοματοποιημένος τρόπος ρύθμισης των IP διευθύνσεων και των άλλων παραμέτρων του δικτύου, ο οποίος δε θα επαφίεται στη διαχείριση μιας υποδομής βασισμένης στο πρωτόκολλο DHCP.
- Η αναγκαιότητα ασφάλειας στο επίπεδο IP της στοίβας πρωτοκόλλου δικτύου. Η προσωπική επικοινωνία πάνω από ένα δημόσιο μέσο, όπως είναι το διαδίκτυο απαιτεί υπηρεσίες κρυπτογράφησης, οι οποίες θα προστατεύουν τα δεδομένα που αποστέλλονται από υποκλοπή ή παραποίηση κατά τη μεταφορά τους. Παρ' όλο που υπάρχει ένα πρότυπο ασφαλείας στο πρωτόκολλο IPv4, γνωστό ως πρωτόκολλο (IPsec), το πρότυπο αυτό δεν είναι υποχρεωτικό να ακολουθείται και υπάρχουν συχνά διαφορετικές, μη συμβατές μεταξύ τους υλοποιήσεις.
- Η ανάγκη για καλύτερη υποστήριξη ροής δεδομένων σε πραγματικό χρόνο, γνωστή ως εξασφάλιση ποιότητας υπηρεσίας (QoS Quality of Service). Ενώ υπάρχει το πρότυπο για την υποστήριξη εξασφάλισης ποιότητας υπηρεσίας στο πρωτόκολλο IPv4, η υποστήριξη ροής δεδομένων σε πραγματικό χρόνο βασίζεται στο πεδίο είδος υπηρεσίας (TOS) του πρωτοκόλλου IPv4 και την ταυτοποίηση του φόρτου χρησιμοποιώντας μια θύρα του πρωτοκόλλου TCP ή UDP. Δυστυχώς, το πεδίο είδος υπηρεσίας του πρωτοκόλλου IPv4 έχει περιορισμένη λειτουργικότητα και ανά τα χρόνια υπήρξαν διάφορες τοπικές ερμηνείες του. Επίσης η ταυτοποίηση του φόρτου χρησιμοποιώντας θύρες των πρωτοκόλλων TCP και UDP δεν είναι δυνατή όταν το packet payload είναι κρυπτογραφημένο.

Για να αντιμετωπίσει αυτά τα ζητήματα, η επιτροπή Internet Engineering Task Force (IETF) έχει αναπτύξει μια σουΐτα πρωτοκόλλων και προτύπων γνωστά και ως IPv6 (Internet Protocol version 6 – Πρωτόκολλο Δικτύου έκδοση 6). Αυτή η καινούργια έκδοση, η οποία καλούνταν προηγουμένως ως IPng (IP next generation), ενσωματώνει τα θέματα πολλών προτεινόμενων μεθόδων για την αναβάθμιση του πρωτοκόλλου IPv4. Η σχεδίαση του IPv6 στοχεύει σκοπίμως τον ελάχιστο αντίκτυπο στα υψηλότερα και χαμηλότερα στρώματα πρωτοκόλλων αποφεύγοντας την τυχαία προσθήκη νέων χαρακτηριστικών.

Οι αυθεντικές IPv4 διευθύνσεις ήταν non-CIDR (Classless Inter Domain Routing). Οι διευθύνσεις διαιρούνταν σε A(/8) B(/16) C(/24) οι οποίες αντιστοιχούσαν σε διαφορετικές ανάγκες των χρηστών. Τα σύνολα των διευθύνσεων διαχειρίζονταν άλλοτε περισσότερο και άλλοτε λιγότερο αυθαίρετα. Στις αρχές του 1990 άρχισε ανησυχία ότι θα εξαντλούνταν οι IPv4 διευθύνσεις.

Το πρώτο βήμα για την βελτίωση του IPv4 έγινε με την εισαγωγή του CIDR.
Για παράδειγμα ένα συγκεκριμένο σύνολο διευθύνσεων μπορεί να έχει οποιοδήποτε μήκος. Αυτό περιγράφηκε από τα πρότυπα RFC1517 και RFC1519. Απαιτήθηκε επίσης ένα πρωτόκολλο διευθυνσιοδότησης το οποίο μπορεί να χειριστεί το BGP v4 (RFC1654). Παράλληλα το 1992 έγιναν συζητήσεις για κάποιο νέο μοντέλο διευθυνσιοδότησης. Η πρώτη πρόταση βασίστηκε στο ISO OSI μοντέλο, αλλά χρειάστηκε να αποσυρθεί.

Η IETF το 1992 έκανε μια εκτίμηση του μελλοντικού μεγέθους του Internet και των αναγκών σε διευθύνσεις και τα αποτελέσματα ήταν τα εξής:

- 2020, 10 δισεκατομμύρια άνθρωποι
- 100 υπολογιστές ανά άτομο

Αφήνοντας κάποιο περιθώριο για σφάλματα, αποφασίστηκε ότι οι ανάγκες θα ήταν
περίπου 10^15 υπολογιστές και περί τα 10^12 δίκτυα.

Έπειτα από αυτή την έρευνα, πριν από περίπου 15 χρόνια το 1994, εισήχθη ένας αριθμός προτάσεων με επικρατέστερη το IPng (next generation), το οποίο αποφασίστηκε να χρησιμοποιεί σαν βάση το IPv4και αυτή η νέα πρόταση ονομάστηκε IPv6.

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

Κεφάλαιο

2

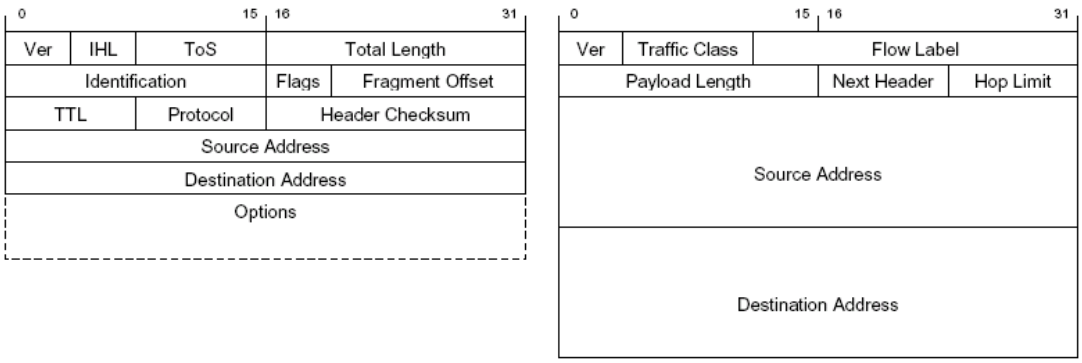
2.1 Εισαγωγή στο IPv6

Το πρωτόκολλο IPv6 έχει αναπτυχθεί έτσι ώστε να αντικαταστήσει το σημερινό πρωτόκολλο δικτύου IPv4. Το IPv4 έχει τις ρίζες του στις αρχές της δεκαετίας του 1970, όταν το διαδίκτυο απαρτιζόταν μόνο από περιορισμένο αριθμό ερευνητικών δικτύων. Το νέο πρωτόκολλο βρίσκεται υπό ανάπτυξη από το 1992, όταν οι ειδικοί του δικτύου διαπίστωσαν ότι η φύση του διαδικτύου είχε αλλάξει και βρισκόντουσαν στην ανάγκη μιας επικείμενης αναβάθμισης.

Το νέο πρωτόκολλο προσφέρει καινούρια λειτουργικότητα και υψηλότερες επιδόσεις στη διαδικτύωση σε διάφορα θέματα. Κατά τη σχεδίαση του IPv6, έγινε πολύ μεγάλη έρευνα, ώστε το IPv6 να μπορεί να χειριστεί την αναμενόμενη ανάπτυξη του διαδικτύου και όλες τις καινούριες προσφερόμενες υπηρεσίες που θα την ακολουθούσαν.

2.1.1 Η επικεφαλίδα του πρωτοκόλλου IPv6

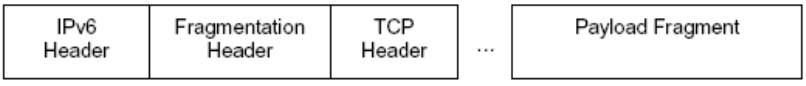
Το IPv6 παρουσιάζει σημαντικές βελτιώσεις σε σχέση με τον προκάτοχό του IPv4. Η μορφή της επικεφαλίδας στο IPv6 έχει αλλάξει από μια μεταβλητού μεγέθους επικεφαλίδα με δώδεκα πεδία και επιλογές σε μια σταθερού μεγέθους επικεφαλίδα μήκους 40 bytes, η οποία περιέχει μόνο οκτώ πεδία.



Εικόνα 8 IPv4 & IPv6 Επικεφαλίδα

Οι διαφορές μεταξύ των δύο εκδόσεων του πρωτοκόλλου IP αναφέρονται εν συντομία παρακάτω:

- Το πεδίο Type of Service (ToS) έχει αντικατασταθεί από το πεδίο Traffic Class, το οποίο μαζί με το καινούριο πεδίο Flow Label παρέχει δυνατότητες καθορισμού προτεραιότητας κυκλοφορίας πακέτων και ποιότητας υπηρεσίας (Quality Of Service).
- Το πεδίο Time To Live (TTL) έχει αντικατασταθεί από το πεδίο Hop Limit, το οποίο προσδιορίζει πιο σωστά τη σημασία του πεδίου.
- Το πεδίο Header Checksum έχει αποσυρθεί εντελώς στο IPv6, αφού ο έλεγχος σφαλμάτων στις περισσότερες περιπτώσεις πραγματοποιείται στα άλλα επίπεδα του TCP/IP. Αυτό δίνει μια μεγάλη ώθηση στις επιδόσεις των δρομολογητών και των firewalls, αφού δε χρειάζεται να ξαναϋπολογίσουν ένα Checksum, όταν κάτι αλλάξει στην επικεφαλίδα (π.χ. η διάρκεια ζωής του πακέτου στο πεδίο TTL).
- Τα πεδία Fragmentation Offset και Options έχουν αποσυρθεί εντελώς από την επικεφαλίδα του IPv6. Αντί αυτών, αυτή η πληροφορία τίθεται σε ξεχωριστές επικεφαλίδες επέκτασης (extension headers) που εισάγονται μεταξύ της επικεφαλίδας του IPv6 και του ωφέλιμου φορτίου (payload) . Η διαδικασία φαίνεται στο σχήμα 2.2. Κάθε επικεφαλίδα επέκτασης έχει ένα πεδίο Next Header (επόμενη επικεφαλίδα), το οποίο περιγράφει τον τύπο της επόμενης επικεφαλίδας. Αυτή η τεχνική διευκολύνει το χειρισμό επιπλέον επιλογών στην επικεφαλίδα καθώς και τις περιπτώσεις ειδικού τρόπου παράδοσης πακέτου. Επίσης παρέχει δυνατότητες εύκολης μελλοντικής επέκτασης με νέα είδη επικεφαλίδων.



Εικόνα 9 Κεφαλίδες επέκτασης (extension headers) στο IPv6

2.1.2 ICMPv6

Το IPv6 χρησιμοποιεί το Internet Control Message Protocol v6 (πρωτόκολλο μηνυμάτων ελέγχου δικτύου έκδοση 6), το οποίο είναι μια περαιτέρω ανάπτυξη του ICMP που είναι διαθέσιμο στο IPv4. Οι αλλαγές από την έκδοση 4 στην έκδοση 6 περιλαμβάνουν την αφαίρεση των σπάνια χρησιμοποιούμενων μηνυμάτων και την εισαγωγή των μηνυμάτων Internet Group Management Protocol (Πρωτόκολλο διαχείρισης ομάδων διαδικτύου) που χρησιμοποιείται για την είσοδο και την αποχώρηση από ομάδες πολλαπλής διανομής (multicast groups). Το ICMPv6 χρησιμοποιείται επίσης για διαγνωστικούς λόγους (π.χ. Ping) και autoconfiguration (αυτόματη απόκτηση ρυθμίσεων). Ο πίνακας παρουσιάζει τα μηνύματα του ICMPv6, τα οποία έχουν μέχρι στιγμής οριστεί.

ID	Message
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

Εικόνα 10 Τα μηνύματα του ICMPv6

2.1.3 Το IPv6 και τα ανώτερα στρώματα

Προσαρμογή πρωτοκόλλων ανώτερων επιπέδων

Το IP βρίσκεται στον πυρήνα της αρχιτεκτονικής του ARPANET (άρα και του Internet) και μια αλλαγή σε αυτό συνεπάγεται και κάποιες απαραίτητες προσαρμογές για τα ανώτερα επίπεδα.

Επίπεδο μεταφοράς (Transport Layer)

Το TCP και το UDP περιλαμβάνουν ένα 16-bit πεδίο ελέγχου (checksum) για να βεβαιώσουν την ακεραιότητα των δεδομένων. Πρέπει όμως επιπρόσθετα να βεβαιώσουν ότι τα δεδομένα φτάνουν και στον σωστό προορισμό. Για το λόγο αυτό προστέθηκε μία επιπλέον επικεφαλίδα, η **Pseudo header (ψευδο-επικεφαλίδα)**, η οποία περιέχει τις διευθύνσεις πηγής και προορισμού. Έτσι, ο υπολογισμός του checksum περιλαμβάνει την Pseudo επικεφαλίδα, την TCP ή UDP επικεφαλίδα, καθώς και τις επικεφαλίδες ανώτερων επιπέδων και τα δεδομένα. Η Pseudo επικεφαλίδα περιλαμβάνεται και στο ICMPv6 για τον υπολογισμό του δικού του checksum, με σκοπό την προστασία του ICMPv6 από λάθη στα πεδία της IPv6 επικεφαλίδα από την οποία εξαρτάται.

Προφανώς η Pseudo επικεφαλίδα πρέπει να αλλάξει προκειμένου να συμπεριλαμβάνει τις μεγαλύτερες διευθύνσεις των 128-bit. Έτσι θα έχει την παρακάτω μορφή :

<table>
<tr><td colspan="2">Source Address</td></tr>
<tr><td colspan="2">Destination Address</td></tr>
<tr><td colspan="2">Upper - Layer Packet Length</td></tr>
<tr><td>0</td><td>Next Header</td></tr>
</table>

Διάγραμμα 3 Pseudo Επικεφαλίδα

- Source Address : Η διεύθυνση του αποστολέα του πακέτου.

- Destination Address : Η διεύθυνση του προορισμού. Εάν το IPv6 πακέτο περιέχει Routing επικεφαλίδα, το πεδίο αυτό θα περιέχει την διεύθυνση του τελικού προορισμού.
- Upper-Layer Packet Length : Δίνει το μέγεθος της επικεφαλίδας του πρωτοκόλλου ανώτερου επιπέδου (π.χ. TCP) συν τα δεδομένα. Για ορισμένα πρωτόκολλα όπως το UDP τα οποία μεταφέρουν δική τους πληροφορία για το μήκος τους, αυτή η πληροφορία χρησιμοποιείται εδώ. Για άλλα όπως το TCP που δεν μεταφέρουν πληροφορία για το μήκος τους, το πεδίο ατό υπολογίζεται από το πεδίο Payload Length της IPv6 επικεφαλίδας μείον το μήκος τυχόν επεκτάσεων επικεφαλίδας ανάμεσα στην IPv6 επικεφαλίδα και αυτήν του ανώτερου επιπέδου.
- Next Header : Καθορίζει τον τύπο του πρωτοκόλλου του ανώτερου επιπέδου (π.χ 6 για TCP, 17 για UDP).

Μέγιστος χρόνος ζωής των πακέτων

Όπως είδαμε το πεδίο "Time-To-Live" στο IPv4, το οποίο μπορούσε να μετρήσει δευτερόλεπτα ή hops αντικαταστάθηκε από το "Hop Limit" στο IPv6, το οποίο μετράει μόνο hops. Έτσι, τυχόν πρωτόκολλο ανώτερου επιπέδου που στηριζόταν στο "Time-To-Live" πεδίο για να περιορίσει τη χρονική διάρκεια παραμονής ενός πακέτου στο δίκτυο πρέπει τώρα να έχει δικούς του μηχανισμούς. Στην πράξη πάντως σχεδόν κανένα πρωτόκολλο ανώτερου επιπέδου δεν μέτραγε το "Time-To-Live" σε δευτερόλεπτα.

Μέγιστο μέγεθος φορτίου ανώτερου επιπέδου

Σε αρκετές περιπτώσεις το μέγιστο μέγεθος φορτίου για τα δεδομένα των ανώτερων επιπέδων περιορίζεται από μηχανισμούς κατώτερων επιπέδων, όπως τον τύπο τοπικού δικτύου. Όταν επομένως υπολογίζεται το μέγιστο μέγεθος φορτίου που μπορεί να διατεθεί στα ανώτερα επίπεδα πρέπει να ληφθεί υπόψη το μεγαλύτερο μέγεθος της IPv6 διεύθυνσης σε σχέση με την IPv4.

2.2 Διευθυνσιοδότηση στο IPv6

Το μήκος των διευθύνσεων στο IPv6 είναι 128 bit, αντί των 32 bit που χρησιμοποιούνταν στο IPv4. Με 128 bit είναι θεωρητικά δυνατό να ανατεθούν περίπου 665,985,621,475,071,937 διευθύνσεις IP ανά τετραγωνικό χιλιοστό στην επιφάνεια της γης, έτσι το πρόβλημα της έλλειψης των IP διευθύνσεων φαίνεται να επιλύεται. Όμως στην πράξη, ο τεράστιος χώρος διευθύνσεων θα χρησιμοποιηθεί για να εισάγει μια πιο ιεραρχική δομή διευθύνσεων από αυτή του παρόντος πρωτοκόλλου IPv4. Μια ιεραρχική δομή επίσης θα βελτιστοποιήσει τη δρομολόγηση στα δίκτυα, αφού οι δρομολογητές δε θα χρειάζεται να εξετάζουν ολόκληρη τη διεύθυνση.

Καθορίζονται τρεις τύποι διευθύνσεων:

α) Μονής αποστολής (unicast). Ένα πακέτο που αποστέλλεται σε μία unicast διεύθυνση παραδίδεται στη διεπαφή που προσδιορίζεται από αυτή τη διεύθυνση

β) Μερικής αποστολής (anycast). Ένα πακέτο που αποστέλλεται σε μία διεύθυνση μερικής αποστολής δρομολογείται προς την πλησιέστερη διασύνδεση που ανήκει στο ‘anycast’ σύνολο διευθύνσεων (την «κοντινότερη», σύμφωνα με το μέτρο απόστασης του πρωτοκόλλου δρομολόγησης)

γ) Πολλαπλής αποστολής (multicast). Ένα πακέτο που αποστέλλεται σε μία διεύθυνση πολλαπλής αποστολής δρομολογείται προς όλες τις διασυνδέσεις που ανήκουν στο ‘multicast’ σύνολο διευθύνσεων

Η μορφή της IPv6 διεύθυνσης είναι: ‘x:x:x:x:x:x:x:x’, όπου το κάθε ‘x’ είναι ένας δεκαεξαδικός αριθμός, ο οποίος αντιστοιχεί σε ένα 16-bit τμήμα της 128-bit επικεφαλίδας. Επομένως η μέγιστη δυνατή τιμή μίας IPv6 διεύθυνσης είναι ‘FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF’, τάξεις μεγέθους μεγαλύτερη από την τιμή μίας IPv4 διεύθυνσης ‘FF:FF:FF:FF’

Οι διευθύνσεις στο IPv4 είναι γραμμένες στη λεγόμενη μορφή “four dotted decimal” (δεκαδική με τέσσερις τελείες) , όπως π.χ. η διεύθυνση 147.102.220.210. Με τα 128 Bits αντί των 32 bits αυτή η σημειογραφία θα απαιτούσε 16 δεκαδικούς ακεραίους για να σχηματιστεί μια IPv6 διεύθυνση, η οποία θα ήταν δύσχρηστη. Αντί για αυτό οι IPv6 διευθύνσεις γράφονται σαν 8 ομάδες 16-bit δεκαεξαδικών λέξεων, χωρισμένων μεταξύ τους με άνω και κάτω τελείες, όπως π.χ. οι διευθύνσεις:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

FE80:0000:0000:0000:0200:F8FF:FE22:26C8

Χρησιμοποιώντας δεκαεξαδικά ψηφία αυτή η μορφή είναι μικρότερη από τη μορφή με δεκαδικά ψηφία, αλλά ακόμα και έτσι η διεύθυνση παραμένει αρκετά μακροσκελής και δύσχρηστη. Για να μειωθεί ακόμα περισσότερο το μήκος υπάρχουν κάποιες περαιτέρω απλοποιήσεις.

Σε μια IPv6 διεύθυνση πιθανόν να υπάρχουν πολλά μηδενικά, λόγω του μεγάλου διαθέσιμου χώρου διευθύνσεων. Αφαιρώντας τα μηδενικά που βρίσκονται στην αρχή της λέξης και επομένως αντικαθιστώντας λέξεις όπως το 0200 με το 200, η διεύθυνση απλοποιείται. Επιπλέον οι λέξεις που απαρτίζονται ολοκληρωτικά από μηδενικά (0000) μπορούν να αντικατασταθούν από δύο συνεχόμενες άνω και κάτω τελείες (::) . Η διπλή άνω και κάτω τελεία μπορεί να αναπαριστά μια ή περισσότερες διαδοχικές λέξεις αυτού του είδους και μπορεί επομένως να απλοποιήσει περαιτέρω τη σημειογραφία των IPv6 διευθύνσεων. Η συμπιεσμένη μορφή της διεύθυνσης :

FE80:0000:0000:0000:0200:F8FF:FE22:26C8

γράφεται ως εξής :

FE80::200:F8FF:FE22:26C8.

Για να γραφεί μια IPv6 διεύθυνση αυτής της μορφής ξανά σε αναλυτική μορφή αρκεί να αντικατασταθούν οι δύο άνω και κάτω τελείες με τόσα μηδενικά όσα χρειάζονται για να συμπληρωθεί το απαιτούμενο μήκος της διεύθυνσης. Δεν είναι δυνατόν να υπάρχουν δύο φορές συνεχόμενες άνω και κάτω τελείες σε μια IPv6 διεύθυνση, γιατί αυτό θα καθιστούσε το συμβολισμό διφορούμενο.

Ένας βολικός τρόπος για να γραφούν IPv6 διευθύνσεις που προκύπτουν από IPv4 διευθύνσεις είναι ο ακόλουθος. Οι διευθύνσεις αυτές γράφονται σαν έξι δεκαεξαδικές ομάδες ακολουθούμενες από τη γνωστή “four dotted decimal” μορφή των IPv4 διευθύνσεων. Π.χ. η διεύθυνση :

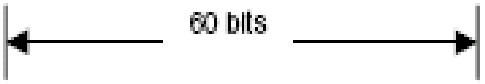
0:0:0:0:0:0:192.168.0.1

γράφεται σε συμπιεσμένη μορφή ως :

::192.168.0.1

Εκτός από τις IPv6 διευθύνσεις που ανατίθενται σε ξεχωριστούς υπολογιστές (hosts), το IPv6 καθιερώνει τα address prefixes (προθέματα διευθύνσεων). Το πρόθεμα διεύθυνσης

στο IPv6 είναι παρόμοιο με το network prefix (πρόθεμα δικτύου), το οποίο χρησιμοποιείται στο IPv4 και λειτουργεί με τον ίδιο τρόπο. Το πρόθεμα διεύθυνσης δηλώνεται σαν μια IPv6 διεύθυνση ακολουθούμενη από μια πλάγια γραμμή (/) και το μήκος του προθέματος σε bits. Τα επόμενα παραδείγματα παρουσιάζουν το ίδιο πρόθεμα γραμμένο με τρεις διαφορετικούς τρόπους:




```
3FFE:0000:0A12:1200:0000:0000:0000:0000/60
3FFE::A12:1200:0:0:0:0/60
3FFE:0:A12:1200::/60
```

2.2.1 Ανάθεση διευθύνσεων

Οι IPv6 διευθύνσεις ανατίθενται σε interfaces, όπως τα Ethernet NICs (κάρτες interfaces δικτύου), virtual interfaces PPP (εικονικές interfaces πρωτοκόλλου σημείου προς σημείο) κ.ο.κ. Παρ' όλα αυτά, μια διαπροσωπεία δεν περιορίζεται σε μια μοναδική διεύθυνση, όπως στο IPv4 αλλά στην πραγματικότητα μπορεί να έχει έναν άπειρο αριθμό διευθύνσεων ανατεθειμένων σε αυτή. Αυτό είναι πολύ χρήσιμο για το διαχωρισμό των διαφόρων ειδών κυκλοφορίας του δικτύου μέσα από το ίδιο interface.

2.2.2 Ο χώρος διευθύνσεων του IPv6

Ο χώρος διευθύνσεων του IPv6 είναι γιγάντιος. Η μετάβαση από 32 σε 128 bits μήκος διευθύνσεων σημαίνει δραστική αύξηση των διαθέσιμων διευθύνσεων. Επιπλέον, τα 128 bits δεν κάνουν μόνο δυνατή την ανάθεση εκατομμυρίων των εκατομμυρίων host, αλλά παρέχουν μεγαλύτερη ιεραρχική δομή από τα επίπεδα δικτύου, υποδικτύου και host που ορίζονται στο IPv4.

Στην κορυφή της ιεραρχίας του χώρου διευθύνσεων του IPv6, διάφοροι τύποι διευθύνσεων ορίζονται. Κάθε τύπος έχει το δικό του υποχώρο διευθύνσεων αναγνωρισμένο από ένα πρόθεμα διεύθυνσης όμοιο με αυτό που χρησιμοποιείται στο Classless Inter-domain Routing CIDR (Αταξική Δρομολόγηση μεταξύ Περιοχών). Ο πίνακας παρουσιάζει την αρχική ανάθεσή όπως έχει οριστεί στο RFC 2373. Ο πίνακας δείχνει την ονομαστική

ανάθεση μαζί με το αντίστοιχο πρόθεμα ακολουθούμενο από το κλάσμα του χώρου διευθύνσεων που κατανέμει.

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 δ/νσεις 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
δ/νσεις Unicast δεσμού-τοπικές	1111 1110 10	1/1024
δ/νσεις Unicast κόμβου-τοπικές	1111 1110 11	1/1024
δ/νσεις Multicast	1111 1111	1/256

Πίνακας 4

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. (Διευκρινήσεις στην 2.5.1)

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.

Όπως φαίνεται και στον πίνακα, περισσότερο από το 70% του χώρου διευθύνσεων παραμένει απροσδιόριστο. Αυτά τα απροσδιόριστα προθέματα μπορούν αργότερα να αντικατασταθούν από επιπλέον υπάρχοντες τύπους διευθύνσεων (π.χ. περισσότερες multicast και aggregatable διευθύνσεις) ή με καινούργιους. Υπάρχουν ήδη σχέδια να συμπεριληφθεί ένα γεωγραφικά βασισμένο σχέδιο όπου η διεύθυνση αντιστοιχεί σε μια γεωγραφική τοποθεσία και αντίστροφα.

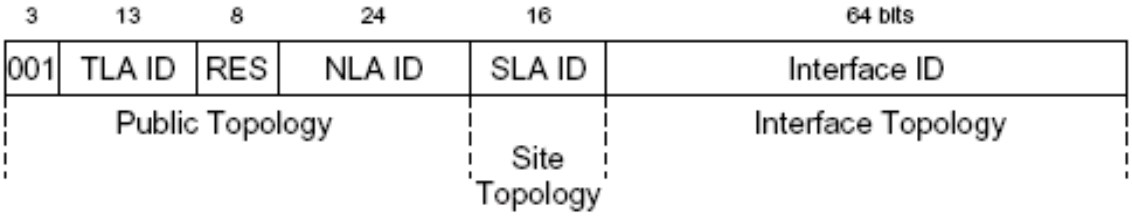
2.2.3 Διευθύνσεις Unicast (μόνης-μετάδοσης)

Μια unicast διεύθυνση προσδιορίζει ένα μοναδικό interface και πακέτα, τα οποία στέλνονται σε μια unicast διεύθυνση προορισμού παραδίδονται σε αυτό και μόνο το interface. Το IPv6 περιλαμβάνει διάφορους υποτύπους unicast διευθύνσεων.

2.2.3.1 Aggregatable unicast διευθύνσεις

Οι aggregatable global unicast διευθύνσεις είναι ένα ιεραρχικά δομημένο σχήμα διευθύνσεων, το οποίο αποτελεί το αρχικά χρησιμοποιούμενο πλάνο ανάθεσης διευθύνσεων για τους IPv6 κόμβους. Αυτή η μορφή διευθύνσεων έχει σχεδιαστεί για να βελτιστοποιήσει τη δρομολόγηση υψηλών ταχυτήτων στα δίκτυα κορμού του διαδικτύου εισάγοντας μια

πολυεπίπεδη τοπολογία διευθύνσεων χωρισμένες σε public, site, interface τοπολογίες. Η μορφή της διεύθυνσης είναι όπως στην εικόνα.



Εικόνα 11 Μορφή aggregatable unicast διευθύνσεων

Η μορφή της διεύθυνσης αποτελείται από τα τέσσερα πεδία ID για μια ιεραρχική δομή τεσσάρων επιπέδων :

- Top-Level Aggregation Identifiers (TLA ID) : χρησιμοποιούνται στην κορυφή της ιεραρχίας.
- Next Level Identifiers (NLA ID) : χρησιμοποιούνται από οργανισμούς
- Site Level Aggregation Identifiers (SLA ID) : αντιστοιχεί στα σημερινά υποδίκτυα του IPv4
- Interface ID : προσδιορίζει ένα μοναδικό Interface ενός IPv6 host

Υπάρχει επίσης ένα δεσμευμένο πεδίο (RES) , το οποίο είναι δυνατόν να προσφέρει μελλοντική αναβάθμιση των TLA ή/και NLA πεδίων.

2.2.3.2 Local Addresses (Τοπικές διευθύνσεις)

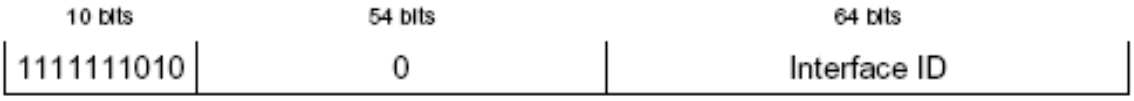
Το IPv6 προσδιορίζει τρεις τύπους διευθύνσεων για τοπική χρήση και μόνο, δηλαδή IP πακέτα που περιέχουν τοπική διεύθυνση πηγής ή προορισμού περιορίζονται σε μια φυσική περιοχή. Τα τοπικά πακέτα δε δρομολογούνται ποτέ έξω από αυτή τη φυσική περιοχή.

Η Loopback διεύθυνση, 0:0:0:0:0:0:0:1 (::1) αναφέρεται στο εικονικό Interface, το οποίο είναι ενσωματωμένο σε κάθε IPv6 host για τοπική εντός host επικοινωνία. Έχει την ίδια λειτουργικότητα με το localhost interface (127.0.0.1) του IPv4.

Οι Link local διευθύνσεις χρησιμοποιούνται για επικοινωνία σε ένα μοναδικό τμήμα (segment) του δικτύου IPv6. Αυτό θα μπορούσε να συμβαίνει σε ένα οικιακό δίκτυο, μια μικρή επιχείρηση ή σε 2 υπολογιστές συνδεδεμένους απ' ευθείας μεταξύ τους. Κάθε IPv6

interface απαιτείται να έχει τουλάχιστον μια link local διεύθυνση ανατεθειμένη και αυτόματα αναθέτει στον εαυτό του μια κατά τη στιγμή της εκκίνησής του. Το πώς πραγματοποιείται αυτή η ανάθεση εξαρτάται στο υποκείμενο μέσο (π.χ. Ethernet, ATM, IEEE 1394 κ.ο.κ.).

Μια link local διεύθυνση κατασκευάζεται με το πρόθεμα FE80::/10 και ένα 64 bit interface ID συμπληρωμένο με 54 μηδενικά bit ενδιάμεσα. Η μορφή της διεύθυνσης φαίνεται στο σχήμα.

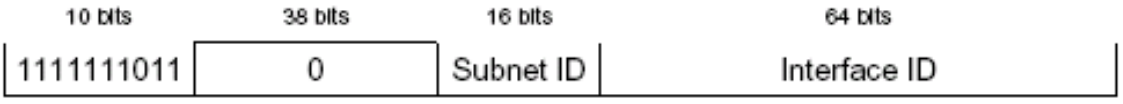


Εικόνα 12 link local διεύθυνση

Οι link local διευθύνσεις χρησιμοποιούνται ευρέως στις διαδικασίες αυτόματης ρύθμισης παραμέτρων (autoconfiguration) του IPv6.

Οι Site Local διευθύνσεις έχουν σχεδιαστεί για να επιτρέπουν σε τοποθεσίες με πολλαπλούς συνδέσμους ή τμήματα δικτύου να επικοινωνούν τοπικά χωρίς την ανάγκη ενός γενικού (global) προθέματος. Αυτή θα μπορούσε να είναι η περίπτωση ενός απομονωμένου εταιρικού δικτύου ή μιας κατοικημένης περιοχής χωρίς την ανάγκη γενικής (global) επικοινωνίας.

Η δομή μιας site local διεύθυνσης είναι όμοια με τη δομή της link local διεύθυνσης, εκτός από το καινούριο πρόθεμα FEC0::/10 και το καινούριο πεδίο subnet ID (αναγνωριστικό υποδικτύου). Η δομή φαίνεται στην εικόνα.

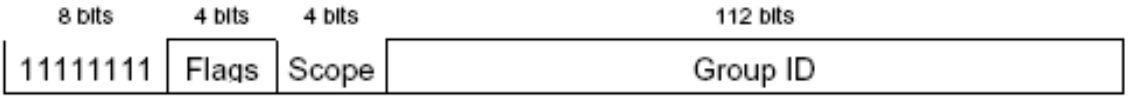


Εικόνα 13 site local διεύθυνση

2.2.4 Διευθύνσεις multicast (πολλαπλής διανομής)

Μια multicast διεύθυνση χρησιμοποιείται για να στέλνει πακέτα από μια πηγή σε πολλαπλούς προορισμούς. Το IPv6 θα κάνει το multicasting έναν πιο κοινό τρόπο επικοινωνίας, αφού κάθε IPv6 δρομολογητής απαιτείται να χειρίζεται τη δρομολόγηση

multicast. Μια multicast IPv6 διεύθυνση αποτελείται από το πρόθεμα διεύθυνσης 11111111 (FF::/8) ακολουθούμενο από μερικές σημαίες (flags), την εμβέλεια του multicast και τέλος ένα αναγνωριστικό της ομάδας στην οποία λαμβάνει χώρα το multicast (multicast group). Στην εικόνα φαίνεται η δομή της multicast διεύθυνσης.



Εικόνα 14 multicast διεύθυνση

Στο πεδίο flags, το τέταρτο bit υποδεικνύει, αν η multicast διεύθυνση είναι παροδική (transient) ή όχι. Οι παροδικές διευθύνσεις κατασκευάζονται για προσωρινές συνόδους (sessions) multicasting, όπως μια τηλεδιάσκεψη, ενώ μια μη παροδική διεύθυνση (non transient) είναι δεσμευμένη για ειδικές προκαταχωρημένες υπηρεσίες. Για παράδειγμα, το multicast group FF02::1 αναφέρεται σε όλους τους κόμβους στην τρέχουσα σύνδεση και το FF02::2 αναφέρεται σε όλους τους δρομολογητές. Μια πλήρης λίστα των καταχωρημένων multicast διευθύνσεων υπάρχει στο δικτυακό χώρο του IANA[1].

Το πεδίο scope (εμβέλεια) υποδεικνύει μέχρι πού μπορούν να δρομολογηθούν τα πακέτα που στέλνονται στο multicast group. Ο πίνακας παρουσιάζει τις μέχρι στιγμής ανατεθειμένες τιμές εμβέλειας όπως ορίζονται στο RFC 2373 [2].

Value	Definition Scope
0	Reserved
1	Node-local scope
2	Link-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

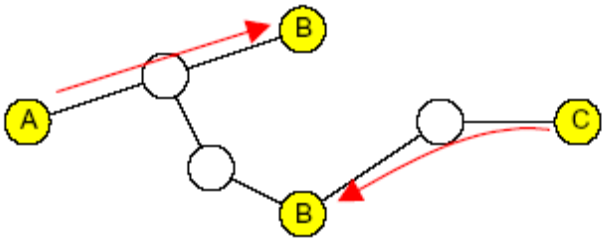
Εικόνα 15 Τιμές εμβέλειας του multicast

Οι τιμές που απουσιάζουν από τον πίνακα, δεν έχουν μέχρι στιγμής καταχωρηθεί και είναι διαθέσιμες στους διαχειριστές του δικτύου για να τις ορίσουν οι ίδιοι.

Τέλος, το πεδίο group identifier της διεύθυνσης διαχωρίζει μια multicast σύνοδο μέσα στην τρέχουσα εμβέλεια. Στο IPv6, το multicast θεωρείται σαν ένας κοινός τρόπος επικοινωνίας, σε αντίθεση με ότι συνέβαινε στο IPv4. Αυτό καθίσταται πολύ εύκολα αντιληπτό παρατηρώντας το αναγνωριστικό μήκους 112 bit του IPv6 σε σχέση με τα 28 bits που είναι διαθέσιμα στις διευθύνσεις τάξεως D του IPv4. Για παράδειγμα το multicast στο IPv6 αντικαθιστά το broadcast στο IPv4.

2.2.5 Διευθύνσεις anycast (μετάδοση σε οποιονδήποτε)

Το anycast είναι ένα καινούριο χαρακτηριστικό που παρουσιάζεται για πρώτη φορά στο IPv6. Μια anycast διεύθυνση είναι μια IPv6 διεύθυνση ανατεθειμένη σε πολλαπλά interfaces, η οποία συχνά ανήκει σε διαφορετικούς κόμβους. Οι anycast διευθύνσεις δε διακρίνονται από τις unicast και μπορεί να χρησιμοποιήσουν οποιοδήποτε σχήμα ανάθεσης unicast διεύθυνσης. Τα πακέτα που στέλνονται σε μια anycast διεύθυνση παραλαμβάνονται από το κοντινότερο, σύμφωνα με την απόσταση δρομολόγησης, στον αποστολέα interface. Η παρακάτω εικόνα απεικονίζει ένα απλό παράδειγμα με 2 hosts (A και C), όπου και οι δύο ορίζουν τον B σαν τη διεύθυνση προορισμού.



Εικόνα 16 Anycasting

Το anycasting μπορεί να χρησιμοποιηθεί για load balancing (εξισορρόπηση φόρτου δικτύου) μεταξύ πολλαπλών DNS, web ή database εξυπηρετητών. Η fuzzy (ασαφής) δρομολόγηση είναι άλλο ένα πιθανό χαρακτηριστικό με διευθύνσεις anycast όπου ο αποστολέας προσδιορίζει ότι τα πακέτα θα πρέπει να δρομολογηθούν μέσω οποιουδήποτε δρομολογητή σε ένα καθορισμένο δίκτυο. Επειδή είναι ένα νέο χαρακτηριστικό στον κόσμο του διαδικτύου, το anycast είναι ακόμα ένα θέμα προς έρευνα και καινούριες εφαρμογές εξελίσσονται συνεχώς.

2.2.6 Autoconfiguration (Αυτόματη απόκτηση παραμέτρων)

Το IPv6 εισάγει τον όρο autoconfiguration, δηλαδή την ικανότητα ρύθμισης ενός κόμβου χωρίς τη μεσολάβηση του ανθρώπινου παράγοντα. Αυτό είναι ένα ευπρόσδεκτο χαρακτηριστικό για τους διαχειριστές δικτύου, αλλά επίσης και για τους
άπειρους χρήστες.

2.2.6.1 Μηχανισμοί

Το IPv6 παρέχει τη λειτουργικότητα του autoconfiguration χρησιμοποιώντας τρεις μηχανισμούς:

- Neighbor discovery (ανακάλυψη γειτονικών κόμβων): Είναι ουσιαστικά ένα σύνολο από ICMPv6 μηνύματα, τα οποία αντικαθιστούν τις υπηρεσίες που παρέχονται από το ARP και το Router Discovery όπως αυτά ορίζονται στο IPv4.
- Stateless autoconfiguration: Αναθέτει μια παγκοσμίως νόμιμη διεύθυνση σε ένα interface συνδυάζοντας την link local διεύθυνσή του με την πληροφορία του προθέματος διεύθυνσης που δημοσιοποιείται (advertised) από τους κοντινούς δρομολογητές. Καμία αλληλεπίδραση από εξυπηρετητές ή ανθρώπους δεν απαιτείται για αυτή τη διαδικασία
- Stateful autoconfiguration: Παρέχει επιπρόσθετες παραμέτρους αυτόματης ρύθμισης, όπως τους εξυπηρετητές DNS χρησιμοποιώντας το πρωτόκολλο DHCP για το IPv6 (DHCPv6). Αυτή είναι και η προτιμώμενη μέθοδος ανάθεσης διευθύνσεων, αφού δίνει στους διαχειριστές πλήρη έλεγχο της διαδικασίας ανάθεσης.

Αυτοί οι μηχανισμοί μπορούν να χρησιμοποιηθούν μαζί ή ξεχωριστά αναλόγως της τοπολογίας δικτύου και των παραμέτρων δρομολογητή που ορίζονται από το διαχειριστή του δικτύου.

2.2.6.2 Διαδικασία αυτόματης ρύθμισης παραμέτρων

Η αυτόματη ρύθμιση παραμέτρων ενός κόμβου είναι μια διαδικασία που αποτελείται από πολλά βήματα. Η πλήρης διαδικασία είναι η ακόλουθη:

1) Το interface ενεργοποιείται
2) Μια link local διεύθυνση δημιουργείται (αλλά δεν ανατίθεται στο interface) συνενώνοντας το προκαθορισμένο πρόθεμα FE80::/10 με ένα 64-bit αναγνωριστικό του interface (interface identifier), όπως περιγράφεται στην ενότητα 2.3.4. Το αναγνωριστικό του interface μπορεί τυπικά να είναι η IEEE 802 διεύθυνση της κάρτας του interface δικτύου (π.χ. Ethernet, FDDI) ή ένας άλλος μοναδικός αριθμός που έχει ληφθεί από άλλα τμήματα του κόμβου (π.χ. ο σειριακός αριθμός της μητρικής πλακέτας).
3) Κατόπιν χρησιμοποιείται το neighbor discovery για να ελέγξει, αν η νέα διεύθυνση είναι μοναδική (στη ζεύξη). Αυτό γίνεται στέλνοντας μηνύματα αιτήσεις neighbor discovery με την διεύθυνση προορισμού να τίθεται στη διεύθυνση που ελέγχεται και τη διεύθυνση πηγής να τίθεται στην ακαθόριστη διεύθυνση (::). Αν μέσω μηνυμάτων neighbor discovery ληφθεί η πληροφορία ότι η διεύθυνση δεν είναι μοναδική, τότε χρειάζεται να επαναδημιουργηθεί είτε χειροκίνητα, είτε τυχαία και να επαναληφθεί η διαδικασία.
4) Όταν διαπιστωθεί ότι η link local διεύθυνση είναι μοναδική, η διεύθυνση ανατίθεται στο interface που ρυθμίζεται εκείνη τη στιγμή.
5) Χρησιμοποιώντας τη νέα link local διεύθυνση ως διεύθυνση πηγής, στέλνεται ένα μήνυμα αίτησης neighbor discovery για δρομολογητές στο multicast group «όλοι οι δρομολογητές» (FF02::2).
6) Προς απάντηση στις αιτήσεις neighbor discovery για δρομολογητές, οι δρομολογητές στέλνουν ένα unicast μήνυμα δημοσιοποίησης neighbor discovery για δρομολογητές προς τον κόμβο. Η δημοσιοποίηση ορίζει, αν ο κόμβος θα πρέπει να χρησιμοποιήσει stateless ή stateful autoconfiguration θέτοντας τη σημαία managed configuration κατάλληλα. Αν χρησιμοποιηθεί stateless autoconfiguration, κατασκευάζεται μια site local ή global διεύθυνση χρησιμοποιώντας ένα πρόθεμα διεύθυνσης, το οποίο συμπεριλαμβάνεται στη δημοσιοποίηση καθώς και την τρέχουσα link local διεύθυνση. Η νέα διεύθυνση ανατίθεται κατόπιν στο interface (το οποίο τώρα έχει δύο διευθύνσεις). Ο host τώρα ρυθμίζεται για επικοινωνία μέσα στο τμήμα του δικτύου ή ακόμα και σε όλο το διαδίκτυο.
7) Αν δεν υπάρχει καμία απάντηση από δρομολογητή, ή αν η σημαία managed configuration από το μήνυμα δημοσιοποίησης ορίζει ότι η διευθυνσιοδότηση δεν μπορεί να γίνει αυτόματα από το ίδιο το host, τότε χρησιμοποιείται stateful

autoconfiguration. Αυτό επιτυγχάνεται μέσω του πρωτοκόλλου DHCPv6 το οποίο ορίζει τύπους μηνυμάτων για τη ρύθμιση όλων των απαραίτητων παραμέτρων.

2.3 Πρωτόκολλα Δρομολόγησης στο IPv6

Εδώ μελετάμε τις διαδικασίες δρομολόγησης στο Επίπεδο Internet του ARPANET (Επίπεδο Δικτύου για ISO/OSI) και πώς αυτές επηρεάζονται από την εισαγωγή του IPv6.

Τα πρωτόκολλα δρομολόγησης χωρίζονται σε 2 κατηγορίες : **Interior Gateway Protocols (IGPs)**, τα οποία αναλαμβάνουν τη δρομολόγηση εντός **Αυτόνομων Συστημάτων (AS, Autonomous Systems)** και **Exterior Gateway Protocols (EGPs)** , τα οποία αναλαμβάνουν τη δρομολόγηση μεταξύ Αυτόνομων Συστημάτων. Ως Αυτόνομο Σύστημα ορίζεται ένα δίκτυο του οποίου τη διαχείριση έχει ένας φορέας. Τα σημαντικότερα πρωτόκολλα δρομολόγησης είναι τα RIP και OSPF (IGPs) και το BGP (EGP). Και τα τρία έχουν επεκταθεί ώστε να υποστηρίζουν το IPv6. Τις συγκεκριμένες τροποποιήσεις και επεκτάσεις θα εξετάσουμε στις επόμενες παραγράφους.

2.3.1 RIPng

Το πρωτόκολλο δρομολόγησης RIP είναι από τα πιο ευρέως χρησιμοποιούμενα IGPs και το πρώτο που υποστήριξε το IPv6 με την επέκτασή του RIPng. Η εύρεση του καλύτερου μονοπατιού βασίζεται στον αλγόριθμο Bellman-Ford. Το πρωτόκολλο είναι σχεδιασμένο για να τρέχει μόνο σε δρομολογητές, οι οποίοι διαθέτουν interfaces σε ένα ή περισσότερα δίκτυα. Η σχεδίαση του πρωτοκόλλου εμπεριέχει ορισμένους περιορισμούς, όπως :

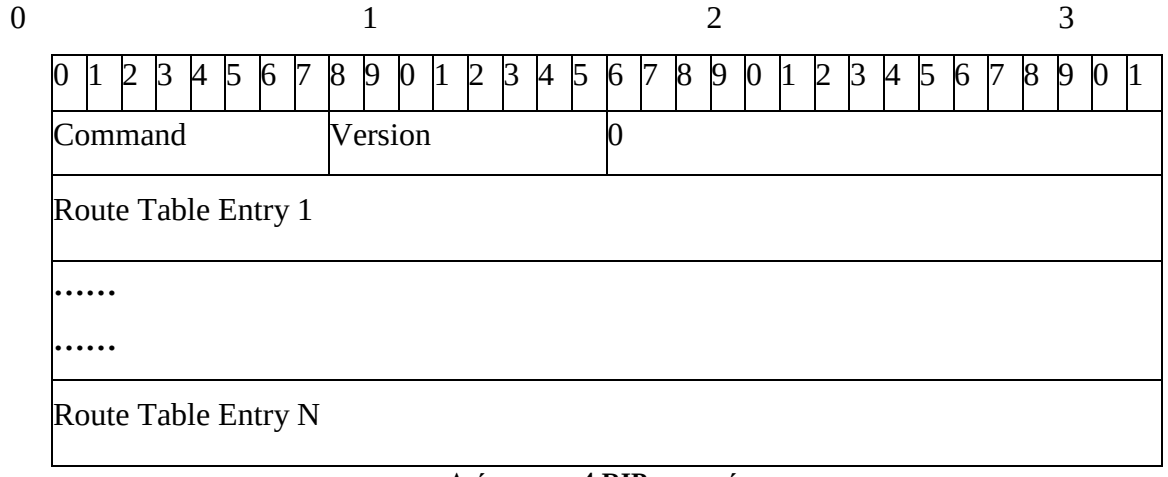
- Χρήση σε δίκτυα με **διάμετρο** (το μέγιστο μονοπάτι) το πολύ 15 hops.
- Την κατάσταση “counting to infinity” (μετρώντας το άπειρο), η οποία μπορεί να οδηγήσει σε μεγάλες καθυστερήσεις ή μεγάλη κατανάλωση bandwidth.
- Τον υπολογισμό του “βέλτιστου” μονοπατιού βάσει σταθερών μετρικών και άρα την αδυναμία προσαρμογής σε παραμέτρους όπως μέτρηση καθυστέρησης, φόρτο δικτύου ή αξιοπιστία γραμμών.

Κάθε δρομολογητής που υλοποιεί το RIPng πρέπει να διαθέτει έναν πίνακα δρομολόγησης (routing table), ο οποίος θα έχει εγγραφές για κάθε προορισμό σε όλο το

σύστημα που τρέχει το RIPng. Κάθε εγγραφή πρέπει να περιέχει τουλάχιστον την ακόλουθη πληροφορία :

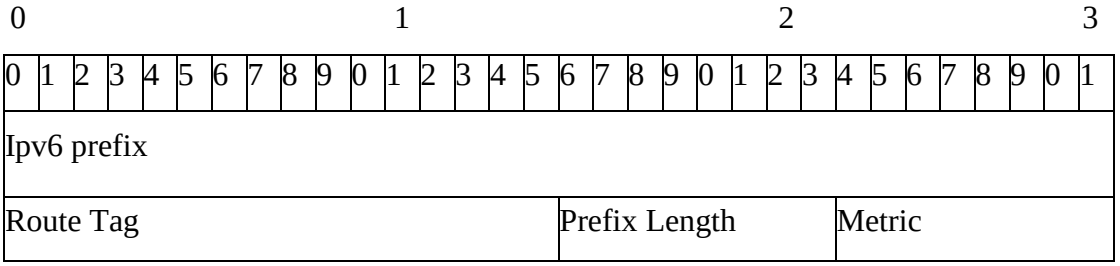
- Το IPv6 πρόθεμα του προορισμού.
- Μία μετρική που αντιπροσωπεύει το ολικό κόστος του να πάει ένα πακέτο από το router στον προορισμό, η οποία είναι το άθροισμα από τα κόστη για όλες τις γραμμές που πρέπει να διασχίσει για να φτάσει στον προορισμό.
- Την IPv6 διεύθυνση του επόμενου router πάνω στο μονοπάτι που πρέπει να ακολουθηθεί για τον προορισμό, εκτός και αν ο προορισμός βρίσκεται στο ίδιο δίκτυο με τον συγκεκριμένο δρομολογητή.
- Ένα flag που δείχνει αν η πληροφορία στον δρομολογητή έχει αλλάξει πρόσφατα.
- Μετρητές που σχετίζονται με τη δρομολόγηση.

Το RIPng βασίζεται στο UDP και χρησιμοποιεί το port 521. Τα πακέτα του έχουν την εξής μορφή:



Διάγραμμα 4 RIPng πακέτα

και κάθε Route Table Entry (RTE) έχει τη μορφή :



Διάγραμμα 5 Route Table Entry

Το πεδίο command καθορίζει τον τύπο του μηνύματος. Προς το παρόν υπάρχουν 2 είδη μηνυμάτων :

Request μήνυμα : Ζητά από τον αποδέκτη του μηνύματος να στείλει μέρος ή όλο τον πίνακα δρομολόγησης που διαθέτει.

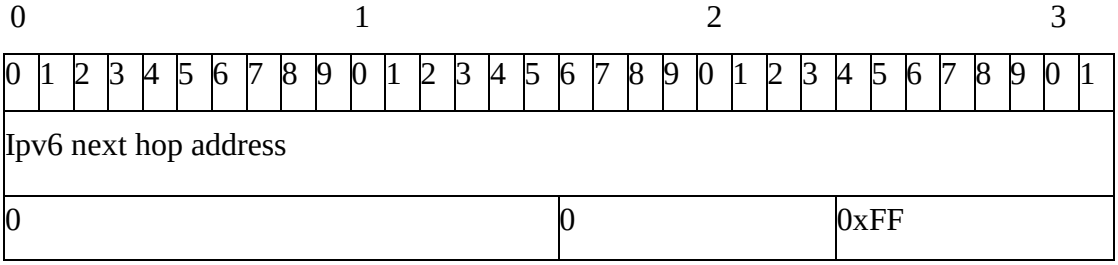
Response μήνυμα : Στέλνει μέρος ή όλο τον πίνακα δρομολόγησης του αποστολέα είτε ως απάντηση σε request μήνυμα είτε απρόκλητα ως ενημέρωση.

Η διεύθυνση του προορισμού είναι 128 bit όπως απαιτεί το IPv6, αποθηκευμένη ως 16 οκτάδες. Το route tag πεδίο παρέχει μία μέθοδο διαχωρισμού μονοπατιών εσωτερικών στο domain που διαχειρίζεται το RIPng και "εξωτερικών" , εισαγμένων από άλλο IGP ή από BGP.

Το πεδίο prefix length περιέχει το μήκος σε bits (0-128) του σημαντικού μέρους του προθέματος αρχίζοντας από αριστερά.

Το πεδίο metric περιέχει το συνολικό κόστος (1-15) για να φτάσει ένα πακέτο στον προορισμό. Αν η τιμή αυτή είναι 16 σημαίνει ότι δεν υπάρχει μονοπάτι για τον προορισμό.

Το RIPng παρέχει επίσης τη δυνατότητα να καθοριστεί η IPv6 διεύθυνση του επόμενου κόμβου (hop) στο μονοπάτι μέσω ενός ειδικού RTE, του **Next Hop Route Table Entry**. Το RTE αυτό αναγνωρίζεται από την τιμή FF στο πεδίο metric, έχει δηλαδή την παρακάτω μορφή :



Διάγραμμα 6 RTE με πεδία metric

Το πεδίο prefix καθορίζει τον επόμενο κόμβο που θα ακολουθηθεί, ενώ τα πεδία route tag και prefix length τίθενται μηδέν κατά την αποστολή και αγνοούνται κατά τη λήψη. Η τιμή 0:0:0:0:0:0:0:0 στο πεδίο prefix length δείχνει ότι η διεύθυνση του επόμενου κόμβου θα πρέπει να είναι ο αποστολέας του μηνύματος.

2.3.2 OSPF

Το ευρύτατα χρησιμοποιούμενο IGP πρωτόκολλο OSPF έχει επίσης τροποποιηθεί ώστε να υποστηρίζει το IPv6. Το OSPF χρησιμοποιεί τον αλγόριθμο **Dijkstra (Link State**

algorithm, LSA) ο οποίος προσφέρει ορισμένα πλεονεκτήματα σε σχέση με τον αλγόριθμο Bellman-Ford του RIP, όπως:

- Δυνατότητα για configuration ιεραρχικών και όχι μόνο επίπεδων διευθύνσεων.
- Χρήση σε μεγαλύτερα δίκτυα.
- Υπολογισμό πολλαπλών βέλτιστων μονοπατιών για καλύτερη εξισορρόπηση της κίνησης.
- Δυνατότητα χρήσης subnet masks μεταβλητού μήκους.

Το OSPF είναι ένα ιδιαίτερα ευέλικτο πρωτόκολλο, του οποίου τη λειτουργία δεν θα παρουσιάσουμε εδώ μιας και ξεφεύγει από τα πλαίσια της εργασίας. Θα εστιάσουμε αντίθετα στις αλλαγές που έγιναν στη νέα του έκδοση για να υποστηρίζει το IPv6.

Οι αλλαγές που έγιναν στο OSPF για να υποστηρίζει το IPv6 εστιάζονται κυρίως σε θέματα διαφορετικής σημειολογίας μεταξύ IPv4 και IPv6 και χειρισμού των μεγαλύτερων IPv6 διευθύνσεων. Οι θεμελιώσεις μηχανισμοί του πρωτοκόλλου (και του χρησιμοποιούμενου αλγορίθμου) παραμένουν ίδιοι. Οι διαφορές αυτής της έκδοσης του OSPF είναι οι εξής:

- Το πρωτόκολλο τρέχει τώρα πάνω στη λογική των συνδέσεων και όχι των υποδικτύων (subnets). Μία σύνδεση μπορεί να περιλαμβάνει περισσότερα του ενός υποδικτύων και δύο κόμβοι μπορούν να επικοινωνούν απευθείας αν βρίσκονται στην ίδια σύνδεση, ακόμα και αν ανήκουν σε διαφορετικά υποδίκτυα.
- Ο πυρήνας του πρωτοκόλλου έχει γίνει ανεξάρτητος του επιπέδου δικτύου, καθώς τα OSPF πακέτα δεν περιλαμβάνουν τις IPv6 διευθύνσεις. Τα αναγνωριστικά ID’s των router, area και link state παραμένουν στο μέγεθος των IPv4 διευθύνσεων, 32 bits, ενώ οι γειτονικοί routers αναγνωρίζονται πλέον μόνο από το router ID και όχι από την IPv4 διεύθυνση σε broadcast και NBMA δίκτυα.
- Η εμβέλεια στην οποία ο αλγόριθμος “πλημμυρίζει” την πληροφορία **(flooding scope)** γενικεύεται και κωδικοποιείται στο πεδίο LS type του LSA. Υπάρχουν 3 κατηγορίες flooding scope :
    - Link-local (τοπικό στη σύνδεση) : η πλημμύρα περιορίζεται στη σύνδεση.
    - Area scope : η πλημμύρα επεκτείνεται σε μία απλή OSPF περιοχή **(area)**.
    - AS scope : Πλημμυρίζεται όλο το domain.

- Υπάρχει η δυνατότητα να τρέχουν πολλαπλές OSPF διαδικασίες **(instances)** ταυτόχρονα στην ίδια σύνδεση, μέσω της χρήσης του Instance ID στο header του OSPF πακέτου και τις OSPF δομές στα interface. Αυτή η δυνατότητα επιτρέπει για παράδειγμα σε διαφορετικά OSPF domain που μοιράζονται κάποια σύνδεση να παραμένουν ξεχωριστά.
- Γίνεται χρήση των link-local διευθύνσεων του IPv6, οι οποίες όπως είδαμε χρησιμοποιούνται για autoconfiguration (Κεφάλαιο 4), neighbor discovery (Κεφάλαιο 3) κ.ά. μέσα σε μια σύνδεση, αλλά δεν έχουν ισχύ έξω από αυτήν. Το OSPF υποθέτει ότι κάθε δρομολογητής έχει link-local unicast διεύθυνση αποδοθείσα για κάθε φυσική του σύνδεση. Τα OSPF πακέτα στέλνονται χρησιμοποιώντας την link-local διεύθυνση του interface ως πηγή. Ένας δρομολογητής μαθαίνει τις link-local διευθύνσεις όλων των άλλων δρομολογητών στις συνδέσεις του και τις χρησιμοποιεί στην πληροφορία για τον επόμενο κόμβο κατά την προώθηση των πακέτων. Εξαίρεση αποτελούν τα **virtual links (εικονικές συνδέσεις)** στις οποίες χρησιμοποιούνται οικουμενικές διευθύνσεις ως πηγή.
- Δεν γίνεται πλέον authentication από το OSPF, μιας και το IPv6 έχει ενσωματωμένες τέτοιες δυνατότητες. Η επικεφαλίδα του OSPF πακέτου δεν έχει πια τα "AuType" και "Authentication" πεδία και όλα τα σχετικά με authentication πεδία των δομών του OSPF έχουν καταργηθεί. Το OSPF τώρα βασίζεται στο IP Authentication Header και το IP Encapsulating Security Payload (Κεφάλαια 1 και 6) για να εξασφαλίσει την ακεραιότητα, αυθεντικότητα και εμπιστευτικότητα των ανταλλασόμενων πληροφοριών δρομολόγησης. Για προστασία από αλλοίωση των δεδομένων λόγω λαθών χρησιμοποιείται το στάνταρτ 16-bit checksum του IPv6, το οποίο καλύπτει όλο το OSPF πακέτο και το προπορευόμενο IPv6 header.
- Το format του OSPF πακέτου έχει αλλάξει, έτσι ώστε να είναι ανεξάρτητο πρωτοκόλλου δικτύου. Συγκεκριμένα :

    - Ο αριθμός έκδοσης έχει αυξηθεί από 2 σε 3.
    - Το πεδίο Options στα πακέτα Hello και Database Description έχει αυξηθεί σε 24 bits.
    - Τα πεδία AuType και Authentication έχουν απομακρυνθεί από το header του OSPF πακέτου, όπως ήδη αναφέραμε.

- Το πακέτο Χαιρετισμού (Hello Packet) δεν περιέχει πλέον καθόλου πληροφορία διευθύνσεων, και περιλαμβάνει ένα Interface ID το οποίο ο δρομολογητής – αποστολέας του πακέτου έχει ορίσει για να αναγνωρίζεται μοναδικά ανάμεσα στα interfaces του το interface αυτό μέσα στη σύνδεση.
- Δύο bits επιλογών, τα R-bit και V6-bit έχουν προστεθεί στο πεδίο Options. Αν το R-bit είναι μηδέν ένας OSPF κόμβος μπορεί να συμμετάσχει στην κατανομή της τοπολογίας χωρίς να χρησιμοποιείται για την προώθηση κίνησης, ενώ το V6-bit εξειδικεύει τη λειτουργία του R-bit. Με το V6-bit στην τιμή 0 ο κόμβος μπορεί να συμμετέχει στην κατανομή της τοπολογίας χωρίς να προωθεί IPv6 datagrams, ενώ με το R-bit στην τιμή 1 και το V6-bit στην τιμή 0 τα IPv6 datagrams δεν προωθούνται αλλά τα datagrams άλλης οικογένειας πρωτοκόλλων μπορεί να προωθηθούν.
- Το header του OSPF πακέτου περιλαμβάνει τώρα ένα πεδίο Instance ID το οποίο όπως είδαμε προηγουμένως επιτρέπει πολλαπλά instances του OSPF να τρέχουν στην ίδια σύνδεση.

- Η επικεφαλίδα του LSA (Link-State Algorithm) δεν περιέχει σημειολογία διευθύνσεων, έτσι ώστε να είναι ανεξάρτητη πρωτοκόλλου δικτύου. Νέοι LSA έχουν προστεθεί για να διανείμουν την πληροφορία για τις IPv6 διευθύνσεις, και τα δεδομένα για τον προσδιορισμό του επόμενου hop. Συγκεκριμένα :

  - Το πεδίο Options έχει μετακινηθεί από τον LSA header στο body των Router-LSA, Network-LSA, Inter-Area-Router-LSA και Link-LSA, και έχει επεκταθεί στα 24 bits.
  - Το πεδίο LSA Type έχει επεκταθεί στα 16 bits, με τα τρία ανώτερα bits να κωδικοποιούν την εμβέλεια (scope) του flooding και το χειρισμό άγνωστων τύπων LSA (αναλυτικότερη επεξήγηση στην επόμενη παράγραφο).
  - Οι διευθύνσεις στα LSA κωδικοποιούνται ως [πρόθεμα, μήκος προθέματος] και όχι ως [διεύθυνση, μάσκα]. Η default δρομολόγηση (default route) εκφράζεται ως πρόθεμα μήκους μηδέν.
  - Τα Router-LSA και Network-LSA είναι τώρα ανεξάρτητα πρωτοκόλλου δικτύου, καθώς δεν περιέχουν πληροφορία για διευθύνσεις.
  - Η πληροφορία για τα interfaces του δρομολογητή μπορεί να εξαπλωθεί μεταξύ πολλαπλών Router-LSA. Οι αποδέκτες πρέπει όλοι να συμπεριλαμβάνουν τα

Router-LSA που δημιουργεί ένας δρομολογητής όταν τρέχουν τον SPF υπολογισμό.

- Υπάρχει ένα νέο LSA , το Link-LSA, το οποίο έχει τους εξής σκοπούς :
  - Να παρέχει την link-local διεύθυνση του δρομολογητή σε όλους τους άλλους δρομολογητές συνδεδεμένους στη σύνδεση.
  - Να πληροφορεί τους άλλους δρομολογητές της σύνδεσης για τη λίστα των IPv6 προθεμάτων που πρέπει να σχετίζουν με τη σύνδεση.
  - Να επιτρέπει στο δρομολογητή να συλλέγει Options bits τα οποία θα σχετίζει με το Network-LSA που δημιουργείται για τη σύνδεση.

- Το πεδίο Options στο Network-LSA είναι το λογικό OR των Options κάθε router στο Link-LSA.
- Τα τύπου-3 Summary-LSA μετονομάζονται Inter-Area-Prefix-LSA
  Τα τύπου-4 Summary-LSA μετονομάζονται Inter-Area-Router-LSA
- Το Link-State ID στο Inter-Area-Prefix-LSA, Inter-Area-Router-LSA και AS-external-LSA χρησιμοποιείται απλά για να ξεχωρίσει ανεξάρτητα κομμάτια της Link-State-Database. Οι διευθύνσεις ή τα Router ID που περιείχε μεταφέρονται τώρα από το body του LSA.
- Στα Network-LSA και Link-LSA το Link-State ID είναι το Interface ID του router που τα δημιούργησε, και γι' αυτό είναι τα μόνα LSA των οποίων το μήκος δεν μπορεί να περιορισθεί (μιας και το Network-LSA πρέπει να περιέχει όλους τους δρομολογητές της σύνδεσης, ενώ το Link-LSA όλες τις διευθύνσεις των δρομολογητών της σύνδεσης).
- Το νέο Inter-Area-Prefix-LSA μεταφέρει την IPv6 που στο IPv4 εμπεριέχεται στα Router-LSA και Network-LSA.
- Είναι προαιρετική η διεύθυνση προώθησης στο AS-external-LSA, όπως και το external route tag. Επιπλέον, τα AS-external-LSA μπορούν να αναφέρονται σε άλλο LSA, έτσι ώστε να μπορούν να χρησιμοποιηθούν επιπρόσθετα χαρακτηριστικά δρομολογήσεων έξω από την εμβέλεια του OSPF πρωτοκόλλου.

- Στη νέα έκδοση του OSPF έχει γίνει πιο ευέλικτος ο χειρισμός άγνωστων τύπων LSA. Στο παρελθόν τέτοιοι τύποι LSA απλά αγνοούνταν, ενώ τώρα μεταχειρίζονται είτε ως έχοντες link-local εμβέλεια, είτε αποθηκεύονται και προωθούνται σαν να ήταν

πλήρως κατανοητοί. Η συμπεριφορά αυτή καθορίζεται από το LSA Handling bit του Link-State header στο LS type πεδίο.

- Οι γειτονικοί δρομολογητές σε μία δεδομένη σύνδεση αναγνωρίζονται πάντοτε από το Router ID τους, ενώ στην προηγούμενη έκδοση αναγνωρίζονταν άλλοτε από το Router ID τους και άλλοτε από τις IPv4 διευθύνσεις των interfaces τους.

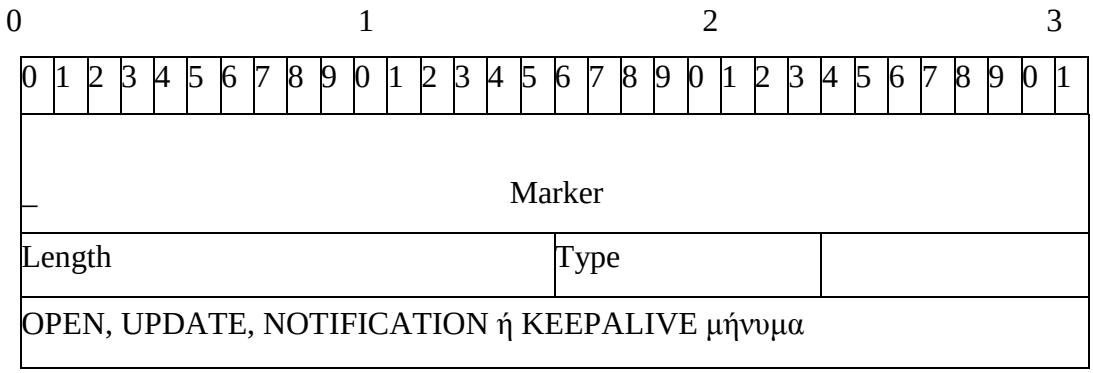
2.3.3 BGPv6

Το πιο διαδεδομένο EGP είναι το BGP. Η βασική λειτουργία του BGP είναι η ανταλλαγή πληροφορίας μεταξύ Αυτόνομων Συστημάτων ως προς το ποια δίκτυα μπορεί το καθένα να έχει πρόσβαση και κατά συνέπεια το σχηματισμό ενός γράφου που αναπαριστά όλα τα δυνατά μονοπάτια. Η τελευταία έκδοση του BGP είναι η BGP-4.

Η επικεφαλίδα του BGP υποστηρίζει τέσσερις δυνατούς τύπους μηνυμάτων :

- OPEN : αρχικοποιεί την BGP επικοινωνία.
- UPDATE : χρησιμοποιείται για τη μεταφορά πληροφορίας για τη δρομολόγηση.
- KEEPALIVE : ανταλλάσσεται σε τακτά χρονικά διαστήματα για να καθορίσει το αν είναι δυνατή η επικοινωνία.
- NOTIFICATION : στέλνεται όταν γίνει αντιληπτό κάποιο λάθος και προκαλεί τη διακοπή της BGP σύνδεσης.

Αρχικά ανοίγεται η TCP σύνδεση (connection) και το πρώτο μήνυμα είναι ένα OPEN μήνυμα. Αν αυτό γίνει αποδεκτό στο άλλο άκρο της BGP σύνδεσης, επιστρέφεται ένα KEEPALIVE μήνυμα ως επιβεβαίωση. Από εκεί και πέρα μπορεί να γίνει η ανταλλαγή UPDATE, KEEPALIVE και NOTIFICATION μηνυμάτων.



Διάγραμμα 7 Επικεφαλίδα BGP

Το BGP-4 αλλά και γενικότερα τα πρωτόκολλα της κατηγορίας του είναι γενικά ανεξάρτητα του πρωτοκόλλου δικτύου, και γι' αυτό το BGP-4 είναι κατάλληλο και για το IPv6, χωρίς την ανάγκη ιδιαίτερων μετατροπών. Η μόνη εξαίρεση είναι ότι το IPv6 όπως έχουμε δει ορίζει την εμβέλεια των unicast διευθύνσεων και το πότε πρέπει κάθε μία να χρησιμοποιείται (link-local, site-local, global – οικουμενική).

Αν και οι link-local διευθύνσεις χρησιμοποιούνται για να προσδιοριστεί το επόμενο hop κατά τη δρομολόγηση από το RIPng και το OSPF και κάθε δρομολογητής έχει μία link-local διεύθυνση επόμενου hop για όλους τους άμεσα συνδεδεμένους δρομολογητές (αυτούς δηλαδή που έχουν το ίδιο πρόθεμα υποδικτύου), δεν είναι κατάλληλες για να χρησιμοποιηθούν από το BGP για να ορίσουν το επόμενο hop κατά τη δρομολόγηση λόγω της φύσης του BGP ως EGP. Έτσι είναι ορισμένες φορές απαραίτητο να προσδιορίζεται το επόμενο hop από ένα πεδίο που περιέχει μία οικουμενική και μία link-local διεύθυνση. Αυτό επιτυγχάνεται από τον τρόπο κατασκευής του πεδίου "Network Address of Next Hop" στο MP_REACH_NLRI attribute.

Το πεδίο αυτό πρέπει να περιέχει υποχρεωτικά την οικουμενική διεύθυνση και μόνο όταν ο αποστολέας του BGP μηνύματος μοιράζεται κάποιο κοινό υποδίκτυο με την οντότητα της οποίας η οικουμενική διεύθυνση περιέχεται στο "Network Address of Next Hop" πεδίο πρέπει να περιέχεται και η link-local διεύθυνση. Το πεδίο "Length of Next Hop Network Address" το οποίο δείχνει το μήκος του "Network Address of Next Hop" θα έχει τιμή 16 αν υπάρχει μόνο η οικουμενική διεύθυνση και 32 αν υπάρχει οικουμενική και link-local.

Το Multiprotocol BGP (MP-BGP) Support για CLNS παρέχει τη δυνατότητα να κάνει κλίμακα διασύνδεσης με Network Service (CLNS) δίκτυα. Οι επεκτάσεις του Multiprotocol Border Gateway Protocol (BGP) έχει την ικανότητα να διασυνδέει το Open System Interconnection (OSI) domains δρομολόγησης δεν τη συγχώνευση των τομέων δρομολόγηση, παρέχοντας έτσι τη δυνατότητα για την κατασκευή πολύ μεγάλων δικτύων OSI.

2.3.4 IS-IS (System-to-Intermediate System Protocol)

Ένα άλλο σπουδαίο πρωτόκολλο κατάστασης ζεύξεων είναι το IS-IS (Intermediate System-Intermediate System), που σχεδιάστηκε για το DECnet και αργότερα το υιοθέτησε ο ISO για να το χρησιμοποιήσει στο πρωτόκολλο στρώματος δικτύου χωρίς σύνδεση, το CLNP. Από τότε έχει τροποποιηθεί για να χειρίζεται και άλλα πρωτόκολλα, με κυριότερο το

IP. Το IS-IS χρησιμοποιείται σε πολυάριθμα δίκτυα κορμού του Internet (συμπεριλαμβανομένου του παλιού δικτύου κορμού NSFNET) και σε μερικά ψηφιακά κυψελωτά συστήματα, όπως το CDPD. Το Novell NetWare χρησιμοποιεί μια ελαφρά παραλλαγή του IS-IS (NLSP) για τη δρομολόγηση των πακέτων IPX.

Βασικά το IS-IS διανέμει μια εικόνα της τοπολογίας δρομολογητών, από την οποία υπολογίζονται οι συντομότερες διαδρομές. Ο κάθε δρομολογητής, μέσα στις πληροφορίες κατάστασης ζεύξεων του, ανακοινώνει τις διευθύνσεις του στρώματος δικτύου στις οποίες έχει απ' ευθείας πρόσβαση. Οι διευθύνσεις αυτές μπορεί να είναι IP, IPX, AppleTalk ή οποιεσδήποτε άλλες διευθύνσεις. Το IS-IS μπορεί να υποστηρίξει ακόμη και πολλαπλά πρωτόκολλα στρώματος δικτύου ταυτόχρονα.

Πολλές από τις καινοτομίες που σχεδιάστηκαν για το IS-IS υιοθετήθηκαν από το OSPF (το OSPF σχεδιάστηκε αρκετά χρόνια μετά το IS-IS). Περιλαμβάνουν μία αυτοσταθεροποιούμενη μέθοδο πλημμύρας των ενημερώσεων των καταστάσεων ζεύξεων, την ιδέα ενός ονοματισμένου δρομολογητή σ' ένα LAN και τη μέθοδο υπολογισμού και υποστήριξης του τεμαχισμού διαδρομών και πολλαπλά κριτήρια. Ως συνέπεια, είναι πολύ μικρή η διαφορά ανάμεσα στο ISIS και το OSPF. Η σπουδαιότερη διαφορά είναι ότι το IS-IS είναι κωδικοποιημένο με τέτοιον τρόπο, ώστε να είναι εύκολο και φυσικό να μεταφέρει ταυτόχρονα πληροφορίες για πολλαπλά πρωτόκολλα στρώματος δικτύου, ένα χαρακτηριστικό που δεν το διαθέτει το OSPF. Το πλεονέκτημα αυτό είναι ιδιαίτερα χρήσιμο σε μεγάλα περιβάλλοντα πολλαπλών πρωτοκόλλων.

Τα χαρακτηριστικά γνωρίσματα IS-IS περιλαμβάνουν:

- Ιεραρχική δρομολόγηση
- Αταξική συμπεριφορά
- Γρήγορο flooding των νέων πληροφοριών
- Γρήγορη σύγκλιση
- Εύκαμπτος συντονισμός χρονομέτρων
- IOS της Cisco εφαρμογή για δρομολόγηση multi-area routing
- IOS της Cisco εφαρμογή για route-leaking
- IOS της Cisco εφαρμογή για overload-bit

Η δύο-επιπέδων ιεραρχία χρησιμοποιείται για να υποστηρίξει τις μεγάλες περιοχές δρομολόγησης. Μια μεγάλη περιοχή μπορεί να διαιρεθεί διοικητικά σε περιοχές. Κάθε σύστημα κατοικεί σε ακριβώς σε μία περιοχή. Η δρομολόγηση μέσα σε μία περιοχή

αναφέρεται στο Level 1. Η δρομολόγηση μεταξύ των περιοχών αναφέρεται ως επίπεδο 2. Ένα επίπεδο 2 Intermediate System (IS) κρατάει τις πορείες των περιοχών προορισμού. Ένα επίπεδο 1 IS κρατάει τις πορείες δρομολόγησης μέσα στην περιοχή του. Για ένα πακέτο που προορίζεται για μια άλλη περιοχή, ένα επίπεδο 1 IS στέλνει το πακέτο στο κοντινότερο επίπεδο 2 IS της περιοχής του, ανεξάρτητα από την περιοχή προορισμού. Κατόπιν το πακέτο ταξιδεύει μέσω του επιπέδου 2 καθοδηγώντας την περιοχή προορισμού, όπου μπορεί να ταξιδεψει μέσω του επιπέδου 1 καθοδηγώντας τον προορισμό. Πρέπει να σημειωθεί ότι η επιλογή μιας εξόδου από μια περιοχή βασισμένη στο επίπεδο 1 που καθοδηγεί στο πιό στενό επίπεδο 2 IS να οδηγήσει σε βέλτιστη δρομολόγηση.

Στα προσβάσιμα μέσα ραδιοφωνικής μετάδοσης (τοπικό LAN), ένα Designated Intermediate System (DIS) επιλέγεται να διευθύνει το flooding πέρα από τα μέσα. Το DIS είναι ανάλογο με τον οριζόμενο δρομολογητή στο Open Shortest Path First (OSPF), ακόμα κι αν και οι λεπτομέρειες συμπεριλαμβάνουνται στην εκλογική διαδικασία. Το DIS επιλέγεται από την προτεραιότητα. Η πιό υψηλή προτεραιότητα γίνεται το DIS. Αυτό ρυθμίζεται σε μία βάση διεπαφών. Στην περίπτωση ενός δεσμού, ο δρομολογητής με την υψηλότερη διεύθυνση SNPA (της MAC) θα γίνει το DIS.

2.3.4.1 IS-IS Πράξεις

Για ένα υψηλό επίπεδο, το IS-IS λειτουργεί ως εξής:

• Οι Δρομολογητές που τρέχουν το IS-IS θα στείλουν «hello» πακέτα σε όλες τις IS-IS διεπαφές για να ανακαλύψουν τους γείτονες και να δημιουργήσουν adjacencies.

• Οι Δρομολογητές που μοιράζονται μια κοινή σύνδεση δεδομένων θα γίνουν IS-IS γείτονες αν πακέτα «hello» περιέχουν πληροφορίες που πληρούν τα κριτήρια για τη διαμόρφωση ενός adjacency. Τα κριτήρια διαφέρουν ελαφρώς, ανάλογα με το είδος των μέσων που χρησιμοποιούνται (p2p ή εκπομπή). Τα κύρια κριτήρια είναι αντιστοίχιση ταυτότητας.

• Οι δρομολογητές που μπορούν να οικοδομηθεί μια σχέση-πακέτο κατάσταση (LSP) με βάση τις τοπικές διασυνδέσεις τους που έχουν ρυθμιστεί για το IS-IS και έμαθε προθέματα από άλλες όμορες δρομολογητές.

• Όλες οι δρομολογητές θα κατασκευάσουν τους δικούς τους link-state βάσεις δεδομένων από αυτές τις LSPs.

• Μια συντομότερη διαδρομή (SPT) υπολογίζεται από τον καθένα IS, και από το SPT πίνακα δρομολόγησης που είναι φτιαγμένο.

Κεφάλαιο

3

3.1 Ομοιότητες και διαφορές των IPv4 & IPv6

Το νέο πρωτόκολλο επιλύει πολλά από τα μεγάλα προβλήματα του προκατόχου του, ενώ εκμεταλλεύεται και υποστηρίζει τις νέες πιο απαιτητικές εφαρμογές. Πιο συγκεκριμένα:

- Δίνει οριστική λύση στο πρόβλημα των διευθύνσεων. Το μέγεθος της IPv6 διεύθυνσης είναι 16 bytes (128 bits), το τετραπλάσιο δηλαδή της μέχρι τώρα χρησιμοποιούμενης IPv4 διευθύνσεως. Αυτή υπολογίζεται ότι αντιστοιχίζει περίπου $6*10^{20}$ διευθύνσεις σε κάθε τετραγωνικό μέτρο της επιφάνειας της γης. Επομένως ο κάθε χρήστης μπορεί να έχει πολλαπλές IP διευθύνσεις, εκτός από τους υπολογιστές του, στα PDAs, στο κινητό τηλέφωνο, σε τηλεοράσεις ραδιόφωνα και γενικά σε όποια ηλεκτρική οικιακή συσκευή επιθυμεί, εφόσον παρέχεται αυτή η δυνατότητα. Ακόμα δεν υπάρχει κανένας λόγος συνέχισης της χρήσης λύσεων τύπου NAT που σήμερα χρησιμοποιούνται σε μεγάλο βαθμό.

  Η μορφή της Unicast IPv6 διευθύνσεως, η οποία χαρακτηρίζεται από το format 001, φαίνεται παρακάτω:

3bits	13bits	32bits	16bits	64bits
001	TLA	NLA	SLA	Interface ID

Διάγρμμα 2 Μορφή IPv6 Διευθύνσεως

Όπου το TLA ID (Top Level Aggregation IDentifier) καθορίζεται από κάποιον οργανισμό ο οποίος παρέχει συνδεσιμότητα δικτύου σε μεγάλη κλίμακα, το NLA ID (Next Level Aggregation IDentifier) το οποίο καθορίζουν οι οργανισμοί αυτοί για τους ISPs, και τα υπόλοιπα (64+16)bits για ιεράρχηση και διευθυνσιοδότηση μέσα στο site.

- Όπως φαίνεται και από το παραπάνω σχήμα, με αυτό τον τρόπο καθορίζεται μια πιο λειτουργική και ιεραρχική διευθυνσιοδότηση και δρομολόγηση στο IPv6, η οποία στηρίζεται στα πολλαπλά επίπεδα παροχών ISPs και οργανισμών. Επίσης υπολογίζεται ότι θα μειώσει κατά ένα ποσοστό 75% το σημερινό μέγεθος των πινάκων δρομολόγησης των δρομολογητών.
- Καλύτερη υποστήριξη της ποιότητας (QoS) με τα πεδία Traffic Class και Flow Label που έχουν προστεθεί στην IPv6 επικεφαλίδα. Το πρώτο πεδίο καθορίζει την προτεραιότητα για το κάθε πακέτο που δρομολογείται, ενώ το δεύτερο εισάγει την έννοια της ροής πακέτων (πακέτα από την ίδια προέλευση προς τον ίδιο προορισμό, που απαιτούν την ίδια επεξεργασία από τον δρομολογητή) και το οποίο αναμένεται να χρησιμοποιηθεί για real time μεταδόσεις, μειώνοντας σημαντικά την καθυστέρηση στους ενδιάμεσους δρομολογητές. Αυτό οφείλεται πρώτον στο ότι πλέον όλα τα δεδομένα που χρειάζεται ο δρομολογητής για την απαιτούμενη επεξεργασία και προώθηση του πακέτου υπάρχουν στην IPv6 επικεφαλίδα, χωρίς να χρειάζεται να παραβιάσει ανώτερα στρώματα άρα και να σπαταλήσει περισσότερη υπολογιστική ισχύ, προσθέτοντας επιπλέον καθυστέρηση στο χρόνο μετάδοσης. Δεύτερο και πιο σημαντικό, οι πιο πολλοί δρομολογητές θα διατηρούν ένα είδος κρυφής μνήμης στην οποία θα αποθηκεύουν τις ενέργειες που απαιτούνται για πακέτα της ίδιας ροής χωρίς να χρειάζεται πλέον επεξεργασία του κάθε πακέτου ξεχωριστά, μειώνοντας και με αυτό τον τρόπο σημαντικά την καθυστέρηση.
- Έχει γίνει εξ'αρχής σχεδιασμός με βάση την ασφάλεια. Το IPsec πρωτόκολλο ασφαλείας είναι ενσωματωμένο στο νέο πρωτόκολλο και αποτελεί αναπόσπαστο κομμάτι του παρέχοντας πιστοποίηση αυθεντικότητας και ακεραιότητας και κρυπτογράφηση.
- IPv6 Mobility, παρέχεται δηλαδή η δυνατότητα στους κινούμενους χρήστες να διατηρούν την σύνδεσή τους, ενώ μετακινούνται από το ένα δίκτυο στο άλλο. Συγκεκριμένα ο χρήστης διατηρεί την διεύθυνση του τοπικού του δικτύου και παράλληλα του αναθέτονται και οι διευθύνσεις των εκάστοτε δικτύων στα οποία εισέρχεται. Ένας δρομολογητής στο τοπικό δίκτυο (home agent), ενημερώνεται από τον χρήστη για τις εκάστοτε διευθύνσεις του κάθε φορά που ο τελευταίος αλλάξει δίκτυο. Στην περίπτωση που κάποιος άλλος χρήστης προσπαθήσει να επικοινωνήσει με τον κινούμενο χρήστη μέσω της τοπικής του διευθύνσεως τα πακέτα φτάνουν στον home agent, ο οποίος τα ενθυλακώνει και μέσω tunnel τα στέλνει στον κινούμενο

χρήστη-προορισμό. Στη συνέχεια ο ίδιος ο χρήστης ενημερώνει τον κόμβο προελεύσεως για την προσωρινή διεύθυνση του και η επικοινωνία γίνεται κατευθείαν μεταξύ των δύο, χωρίς την μεσολάβηση του home agent. Ο κινούμενος χρήστης κάθε φορά που αλλάζει διεύθυνση εκτός από τον home agent ενημερώνει και τους υπόλοιπους χρήστες με τους οποίους είχε ή έχει επικοινωνία, αλλά παράλληλα διατηρεί και τις προηγούμενες του διευθύνσεις για να δέχεται και τα πακέτα που καταφτάνουν σε αυτές.

- Παρέχει την δυνατότητα τόσο για Stateful Address Configuration με την παρουσία ενός DHCPv6 server, όσο για Stateless Address Configuration. Συγκεκριμένα οι διάφοροι κόμβοι του δικτύου καθορίζουν αρχικά τιςlink-local διευθύνσεις τους από το link-local πρόθεμα FE80::/64 και τον interface identifier που καθορίζουν οι ίδιοι και με ένα μήνυμα Neighbor Discovery ελέγχουν την μοναδικότητα της διευθύνσεως τους. Παρόμοια στην περίπτωση που δεν έχουν πάρει κάποιο μήνυμα router advertisement στέλνουν οι ίδιοι στον router μηνύματα router-solicitations απαιτώντας router advertisement. Αν δεν υπάρχει router, χρησιμοποιείται κάποιο stateful address autoconfiguration πρωτόκολλο. Εάν υπάρχει δρομολογητής, τότε απαντά με κάποιο router advertisement και από το πρόθεμα που διαφημίζεται σχηματίζεται η παγκόσμια και η site local διεύθυνση του κόμβου και τίθενται οι παράμετροι hop limit, reachable time, retransmission time, MTU και καθορίζεται το default route προς τον δρομολογητή που έστειλε τις διαφημίσεις.
- Απλοποίηση της διαχείρισης και του configuration του IPv6 multicast, παρέχοντας επιπλέον και καλύτερη κλιμάκωση με χρήση του Rendezvous Point (PR).
- Καλύτερες προϋποθέσεις για multihoming, λόγω των πολλαπλών unicast διευθύνσεων ανά interface, της χρήσης των site-local διευθύνσεων εντός του site και των πλέον καθορισμένων και διαχωρισμένων TLAs για τον κάθε ISP.

Το IPv6 βασίστηκε στο IPv4 ωστόσο υπάρχουν κάποιες βασικές διαφορές μεταξύ του IPv4 και του IPv6 πακέτου. Όλα τα πεδία έχουν ένα προκαθορισμένο και στατικό μέγεθος με αποτέλεσμα:

- Πιο γρήγορη επεξεργασία
- Δεν χρειάζεται επικεφαλίδα αρχικού μήκους (IHL-Initial Header Length)
- Ορίζεται ένας αριθμός επεκτάσεων-επικεφαλίδων

Στο νέο πρωτόκολλο η επικεφαλίδα ελέγχου αθροίσματος έχει αποσυρθεί επομένως τώρα έχουμε:

- Μεγαλύτερη ταχύτητα επεξεργασίας των πακέτων στους ενδιάμεσους κόμβους, αφού δεν χρειάζεται νέος υπολογισμός του αθροίσματος
- Τα πακέτα θεωρητικά μπορούν να σταλούν με κάποια λανθασμένα bits αλλά ο κίνδυνος είναι πολύ χαμηλός
- Η χρήσιμη πληροφορία συχνά έχει το δικός της έλεγχο

Πλέον το πακέτο δεν χρειάζεται κατάτμηση γιατί το IPv6 στέλνει πακέτα μόνο αφού πραγματοποιήσει έλεγχο μονοπατιού (Path maximum transmission unit discovery –PMTUD). Το IPv6 δεν έχει πεδίο TOS (Type of Service) και κάποια πεδία έχουν αλλάξει όνομα packet length =>payload length, protocol type => next header time to live => hop limit .

3.2 Σταδιακή μετάβαση από το IPv4 στο IPv6

Η μετάβαση από το IPv4 πρωτόκολλο στο IPv6 δεν είναι εύκολη υπόθεση, ιδιαίτερα αν αναλογιστεί κανείς το μέγεθος του διαδικτύου σήμερα, τον τεράστιο αριθμό των χρηστών και των sites. Πολλές εταιρείες και οργανισμοί σήμερα στηρίζονται αποκλειστικά στο διαδίκτυο για την λειτουργία τους και παροχή συνεχών υπηρεσιών, κάτι που καθιστά αδύνατη μια μετάβαση στο IPv6 πρωτόκολλο. Επίσης η τεράστια επένδυση που έχει γίνει στο IPv4 και ιδιαίτερα σε μηχανήματα που δεν μπορούν να αναβαθμιστούν όπως κινητά τηλέφωνα και δικτυακοί εκτυπωτές στέκεται εμπόδιο στην άμεση μετάβαση. Τέλος ίσως ο σημαντικότερος παράγοντας επιβράδυνσης της μετάβασης είναι η μέχρι στιγμής μικρή κατανόηση του IPv6 πρωτοκόλλου, των δυνατοτήτων του αλλά και των απαιτήσεων του. Η ανάγκη μετάβασης στο νέο πρωτόκολλο το οποίο θα λύσει πολλά από τα προβλήματα του προηγούμενου, δεν έχει γίνει κατανοητή σε όλους. Όλα τα παραπάνω δείχνουν ότι η μετάβαση δεν μπορεί να γίνει από τη μια στιγμή στην άλλη, ούτε υπάρχει κάποια συγκεκριμένη μέρα μέχρι την οποία θα έχει γίνει η μετάβαση. Η μόνη λύση για το πέρασμα στο νέο πρωτόκολλο είναι κάποιοι μηχανισμοί για σταδιακή και «ανώδυνη» μετάβαση.

Αυτό το γεγονός είχε ληφθεί υπόψη από την IETF κατά τον σχεδιασμό του πρωτοκόλλου, επομένως το IPv6 είναι κατά πολύ μεγάλο μέρος συμβατό με το IPv4.

Επιπλέον έχει συσταθεί ειδική ομάδα ερευνών για να ασχοληθεί αποκλειστικά με τα θέματα της μετάβασης. Η έρευνα που επιτελούνταν στο θέμα της μετάβασης είχε ως τελικό σκοπό κάποιους μηχανισμούς οι οποίοι να προσφέρουν:

- Δυνατότητα σταδιακής μετάβασης, έτσι ώστε οι IPv4 hosts και routers του κάθε δικτύου να μπορούν να αναβαθμίστουν σε IPv6 ο καθένας ξεχωριστά, χωρίς την απαίτηση να έχουν και οι υπόλοιποι κόμβοι του δικτύου εγκατεστημένο το IPv6.
- Ελάχιστες απαιτήσεις αναβάθμισης. Συγκεκριμένα το μόνο που απαιτείται είναι ένας DNS server που να χειρίζεται IPv6 εγγραφές στην περίπτωση των hosts και καμιά απαίτηση στην περίπτωση των routers.
- Απλότητα διευθυνσιοδότησης, δηλαδή να διατηρηθούν ιο IPv4 διευθύνσεις που είχε το μηχάνημα πριν την αναβάθμιση παράλληλα με τις IPv6 διευθύνσεις χωρίς να υπάρχει η ανάγκη επαναπροσδιορισμού αυτών.
- Καμιά προεργασία εγκατάστασης να μην απαιτείται για την αναβάθμιση από IPv4 σε IPv6.

Γι’ αυτούς τους λόγους, υλοποιήθηκε και ενσωματώθηκε στο νέο πρωτόκολλοένα σύνολο μηχανισμών, το SIT (Simple Internet Transition), που περιλαμβάνει κάποιους κανόνες και πρωτόκολλα, για την διευκόλυνση ης μετάβασης. Συγκεκριμένα το SIT παρέχει:

- Μία δομή IPv6 διευθύνσεων που μπορεί να προκύψει από τις IPv4 διευθύνσεις. Αυτές οι διευθύνσεις είναι IPv6 IPv4 compatible της μορφής ::ww.xx.yy.zz όπου ww.xx.yy.zz είναι η IPv4 διεύθυνση που είχε πριν την αναβάθμιση ο συγκεκριμένος κόμβος.
- Την δυνατότητα λειτουργίας των λειτουργικών συστημάτων με διπλή στοίβα πρωτοκόλλων ταυτόχρονα (dual stack). Δηλαδή το ένα πρωτόκολλο δεν επεμβαίνει στην λειτουργία του άλλου και το κάθε μηχάνημα συνήθως αναλόγως με το αποτέλεσμα της αναζήτησης DNS, επιλέγει ποια από τις δύο στοίβες θα χρησιμοποιήσει για επικοινωνία. Τα στρώματα ανωτέρου επιπέδου συνεργάζονται και με τα δυο πρωτόκολλα.
- Ένα μηχανισμό για την ενθυλάκωση των IPv6 πακέτων μέσα σε IPv4 πακέτα (tunneling) για μετάδοση τους πάνω από IPv4 σύννεφα. Οι μηχανισμοί αυτοί είναι οι πλέον χρησιμοποιούμενοι σήμερα.

- Προαιρετικά, δυνατότητα μετατροπής του IPv6 πακέτου σε IPv4, και αντίστροφα.

Στην παρούσα πτυχιακή εργασία, δεν θα ασχοληθούμε περισσότερο με τους μηχανισμούς που χρησιμοποιήθηκαν για να γίνει η μετάβαση από το IPv4 στο IPv6.

Βιβλιογραφία

1. RFC 791, “Internet Protocol Version 4 (IPv4) Specification”, September 1981
2. RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification’, December 1998
3. RFC 2365, “Administratively Scoped IP Multicast.”
4. RFC 1075, “Distance Vector Multicast Routing Protocol.”
5. RFC 1112, “Host extensions for IP multicasting.”
6. RFC 2236, “Internet Group Management Protocol, Version 2.”
7. RFC 3376, “Internet Group Management Protocol, Version 3.”
8. RFC 1584, “Multicast Extensions to OSPF.”
9. RFC 3208, “PGM Reliable Transport Protocol Specification.”
10. RFC 2117, “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification.”
11. RFC 1769, “Simple Network Time Protocol (SNTP).”
12. RFC 2373, “IP Version 6 Addressing Architecture”
13. RFC 1887, “An Architecture for IPv6 Unicast Address Allocation”
14. RFC 2374, “An IPv6 Aggregatable Global Unicast Address Format”
15. RFC 2375, “IPv6 Multicast Address Assignments”
16. RFC 2463, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”
17. RFC 2461, “Neighbor Discovery for IP Version 6 (IPv6)”
18. Dynamic Host Configuration Protocol for IPv6 (DHCPv6), draft-ietf-dhc-dhcpv6
19. RFC 2462, “IPv6 Stateless Address Autoconfiguration”
20. RFC 2080, “RIPng for IPv6”
21. RFC 2740, “OSPF for IPv6”
22. RFC 2545, “Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing”
23. RFC 2402, “IP Authentication Header”
24. RFC 1886, “DNS Extensions to support IP version 6”
25. Mobility Support in IPv6, draft-ietf-mobileip-ipv6
26. RFC 2466, “Management Information Base for IP Version 6 : ICMPv6 Group”
27. RFC 1933, “Transition Mechanisms for IPv6 Hosts and Routers”
28. RFC 2185, “Routing Aspects of IPv6 Transition”
29. RFC 2473, “Generic Packet Tunneling in IPv6 Specification”

30. *OSPF: Anatomy of an Internet Routing Protocol*, by John T. Moy, 1998, Reading, MA: Addison-Wesley.
31. *Routing in the Internet, Second Edition*, by Christian Huitema, 2000, Englewood Cliffs, NJ: Prentice Hall.
32. http://www.tcpipguide.com/free/t_TCPIPRoutingProtocolsGatewayProtocols.htm
33. TCP/IP Technical Reference.
34. IPv4 Multicasting Technical Reference.
35. http://technet.microsoft.com/en-us/library/cc738760(WS.10).aspx
36. IETF, http://www.ietf.org/
37. Andrew S. Tanenbaum, *«Δίκτυα Υπολογιστών»,* 2000