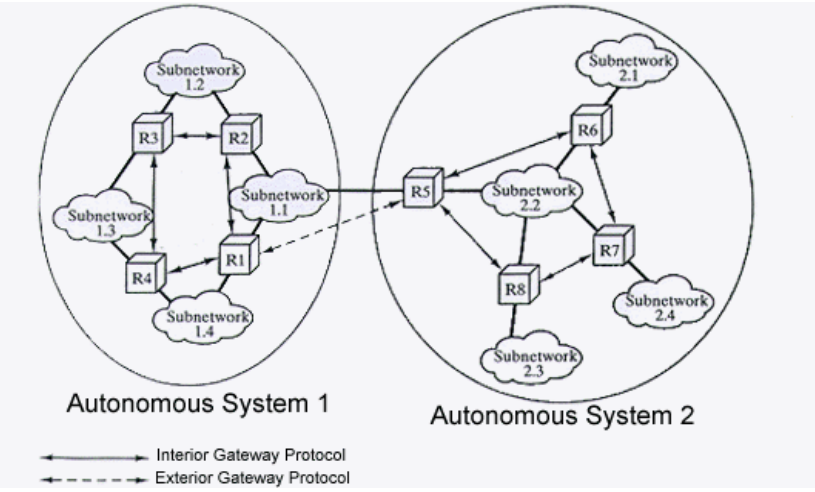
ΔΡΟΜΟΛΟΓΗΣΗ

ΠΡΩΤΟΚΟΛΛΑ – ΤΕΧΝΙΚΕΣ



ΕΡΓΑΣΙΑ ΠΟΥ ΠΑΡΑΔΟΘΗΚΕ ΣΤΑ ΠΛΑΙΣΙΑ ΤΟΥ ΜΑΘΗΜΑΤΟΣ
ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΚΤΥΩΝ

ΜΙΜΙΛΙΔΗΣ ΑΧΙΛΛΕΑΣ
ΜΙΧΕΛΑΚΟΣ ΓΙΑΝΝΗΣ
ΜΟΥΤΑΦΙΔΗΣ ΓΙΩΡΓΟΣ
ΜΠΙΜΠΙΚΑΣ ΔΗΜΗΤΡΗΣ

Κεφάλαιο 1

1.1 Εισαγωγή στη δρομολόγηση

Δρομολόγηση ονομάζεται η επιλογή των καλύτερων διαδρομών που πρέπει να ακολουθήσουν τα πακέτα πληροφορίας σε ένα δίκτυο υπολογιστών. Αυτή η επιλογή γίνεται συνήθως από το δίκτυο με βάση τις πληροφορίες που είναι αποθηκευμένες στους κόμβους. Η πηγή μπορεί επίσης να καθορίσει το μονοπάτι εφόσον έχει την απαραίτητη πληροφορία.

Για να επιλέξουν οι αλγόριθμοι δρομολόγησης την καλύτερη διαδρομή προς έναν προορισμό χρησιμοποιούν διάφορες μετρικές όπως π.χ. το μήκος της διαδρομής. Για να διευκολύνεται η εύρεση της διαδρομής αποθηκεύονται στους κόμβους πίνακες δρομολόγησης (routing tables) που περιέχουν πληροφορίες για τις διαδρομές. Το είδος της πληροφορίας που αποθηκεύεται στους κόμβους εξαρτάται από τον αλγόριθμο δρομολόγησης αλλά και από τη μέθοδο μεταφοράς που χρησιμοποιείται.

Για μεταφορά αυτοδύναμων πακέτων κάθε κόμβος διατηρεί έναν πίνακα δρομολόγησης οργανωμένο όπως φαίνεται στον πίνακα 1. Οι πίνακες δρομολόγησης του κόμβου βασίζονται σε εκτιμήσεις της συμφόρησης του δικτύου. Στους πίνακες υπάρχουν συσχετίσεις της μορφής προορισμός / επόμενος κόμβος (next hop) που λένε στον κόμβο ότι για να φτάσει ένα πακέτο σε έναν συγκεκριμένο προορισμό θα πρέπει να σταλεί στον επόμενο κόμβο. Όταν ένα πακέτο φτάσει σε έναν κόμβο τότε αυτός ελέγχει τη διεύθυνση του κόμβου προορισμού και συσχετίζει αυτή τη διεύθυνση με έναν επόμενο κόμβο.

Η ενημέρωση των πινάκων δρομολόγησης γίνεται με ανταλλαγή μηνυμάτων μεταξύ των κόμβων. Ένα τέτοιο παράδειγμα μηνύματος είναι το routing update που περιέχει ένα μέρος ή και ολόκληρο πίνακα δρομολόγησης. Αναλύοντας ένας κόμβος τα routing updates που λαμβάνει, μπορεί να δημιουργήσει μια εικόνα της τοπολογίας του δικτύου. Από τη στιγμή που γίνεται αντιληπτή η τοπολογία του δικτύου μπορούν να προσδιοριστούν βέλτιστες διαδρομές προς τους διάφορους προορισμούς [1].

Προορισμός	Επόμενος κόμβος (next hop)
D1	Node A
D2	Node B
D3	Node C
D4	Node A
D5	Node A
D6	Node B

Πίνακας 1: Πίνακας δρομολόγησης για μεταφορά αυτοδύναμων πακέτων

Η επιστήμη των υπολογιστών ασχολείται με τη δρομολόγηση για πάνω από δύο δεκαετίες αλλά η δρομολόγηση έγινε εμπορικά δημοφιλής στα μέσα περίπου της δεκαετίας του 1980 όταν δηλαδή έγινε δημοφιλής η μεγάλης κλίμακας διαδικτύωση (internetworking). Ο κύριος λόγος που συνέβη αυτό είναι η φύση των δικτύων υπολογιστών κατά τη δεκαετία του 1970 αφού κατά τη διάρκεια αυτής της περιόδου τα δίκτυα ήταν σχετικά απλά και ομογενή.

Η δρομολόγηση δεν είναι μια εύκολη διαδικασία. Τα σημερινά δίκτυα συνήθως αποτελούνται από έναν μεγάλο αριθμό κόμβων και συνεπώς οι δυνατές διαδρομές που συνδέουν τον κόμβο-αφετηρία με τον προορισμό είναι πολλές. Τα πράγματα γίνονται δυσκολότερα εξαιτίας του γεγονότος ότι η κατάσταση του δικτύου μεταβάλλεται με την πάροδο του χρόνου. Έτσι μπορεί λόγω βλάβης ορισμένες συνδέσεις ή και κόμβοι να πέφτουν και να μην μπορούν να αποτελούν μέρος μιας διαδρομής. Επιπλέον μπορεί κόμβοι ή συνδέσεις που προηγουμένως είχαν υποστεί βλάβη να επιδιορθώθηκαν και να ξαναγίνονται διαθέσιμες.

Οι συσκευές που υλοποιούν την διαδικασία της δρομολόγησης και παρέχουν τη φυσική σύνδεση μεταξύ των κόμβων ονομάζονται δρομολογητές (routers). Επιπρόσθετα της παροχής φυσικής σύνδεσης μεταξύ δικτύων, οι routers έχουν την ικανότητα να διακινούν πληροφορία μεταξύ πολλαπλών δικτύων προωθώντας datagrams βασιζόμενοι στις δικές τους διευθύνσεις Επιπέδου Δικτύου (Network Layer). Σε αυτήν την περίπτωση το επίπεδο του δικτύου είναι το τρίτο επίπεδο στο 7-επιπέδων μοντέλο διασύνδεσης ανοικτών συστημάτων (Open Systems Interconnection, OSI). Ο όρος datagram χρησιμοποιείται για να περιγράψει κάθε

πληροφορία που παράγεται από ένα υψηλότερου επιπέδου πρωτόκολλο ή εφαρμογή και την οποία χειρίζεται το επίπεδο δικτύου στο μοντέλο αναφοράς OSI [2].

1.2 Εσωτερική και εξωτερική δρομολόγηση

Ένα αυτόνομο σύστημα (autonomous system) είναι ένα δίκτυο συνδεδεμένο με routers που χρησιμοποιούν μια ενιαία διαδικασία δρομολόγησης, κάτω από ένα διαχειριστικό έλεγχο μιας απλής οντότητας [1].

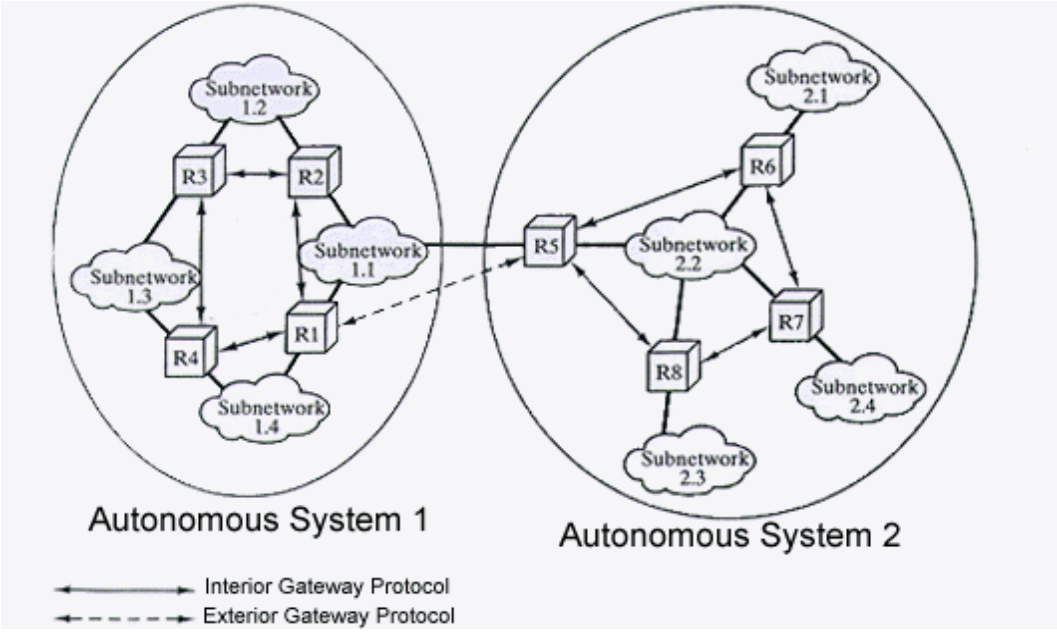
Ένα πρωτόκολλο εσωτερικής δρομολόγησης (Interior Routing Protocol, IRP) περνάει πληροφορία δρομολόγησης διαμέσου ενός αυτόνομου συστήματος και δεν χρειάζεται να εκτελεστεί έξω από το σύστημα. Αυτή η ευελιξία επιτρέπει στα IRPs να χρησιμοποιούνται σε συγκεκριμένες εφαρμογές και απαιτήσεις.

Συνήθως ένα διαδίκτυο κατασκευάζεται με περισσότερα από ένα αυτόνομα συστήματα. Το πρωτόκολλο που περνάει πληροφορία δρομολόγησης μεταξύ των routers σε διαφορετικά αυτόνομα συστήματα αναφέρεται σαν πρωτόκολλο εξωτερικής δρομολόγησης (Exterior Routing Protocol, ERP). Είναι λογικό ένα ERP να χρειάζεται να περάσει λιγότερη πληροφορία και να είναι πιο απλό από ένα IRP για τον λόγο ότι αν τα δεδομένα είναι να μεταφερθούν από έναν host ενός αυτόνομου συστήματος, σ' έναν host ή σε ένα άλλο αυτόνομο σύστημα, ο router στο πρώτο σύστημα χρειάζεται μόνο να τερματίσει το υπό στόχο αυτόνομο σύστημα και να συσκευάσει μια δρομολόγηση για να μπει στο σύστημα. Όταν μια φορά τα δεδομένα μπουν στο υπό στόχο αυτόνομο σύστημα οι routers μπορούν να συνεργαστούν για να μεταφέρουν τελικά τα δεδομένα.

Στο Internet οι routers (καλούνται και Gateways στην ορολογία του Internet) που διακινούν πληροφορία μέσα σε ένα αυτόνομο σύστημα καλούνται Interior Routers (IR) και το πρωτόκολλο που χρησιμοποιούν Interior Gateway Protocol (IGP). Αντίθετα, οι routers που διακινούν πληροφορία μεταξύ αυτόνομων συστημάτων καλούνται Exterior Routers (ER) και το πρωτόκολλο που χρησιμοποιούν Exterior Gateway Protocol (EGP) (Σχ. 1-1).

Στις επόμενες παραγράφους θα εξεταστεί η εσωτερική δρομολόγηση και θα περιγραφούν με όσο το δυνατόν απλούστερο τρόπο τα πιο γνωστά IGPs που

χρησιμοποιούνται στο Internet. Επίσης, θα γίνει αναφορά στην εξωτερική δρομολόγηση και στο πρωτόκολλο BGP που πρώτο χρησιμοποιήθηκε για την υλοποίησή της.



Σχήμα 1-1: Παράδειγμα χρήσης των Interior Gateway Protocols και των Exteriors Gateway Protocols

1.3 Routing σε διαδίκτυο

1.3.1 Στατική Δρομολόγηση (Static Routing)

Η απλούστερη μορφή δρομολόγησης είναι η στατική δρομολόγηση (Static Routing)η οποία προγραμματίζει εκ των προτέρων τα δρομολόγια. Η διαδικασία εύρεσης δρομολογίων και η διάδοσή τους στο δίκτυο αποτελεί έργο του internetwork administrator. Ο router ο προγραμματισμένος για στατική δρομολόγηση κάνει forward τα πακέτα μέσω προσχεδιασμένων ports. Αφού δημιουργηθεί η σχέση σύνδεσης μεταξύ διεύθυνσης προορισμού (destination address) και router port, δεν υπάρχει επιπλέον ανάγκη για περαιτέρω προσπάθεια των δρομολογητών να ανακαλύψουν καινούρια δρομολόγια ή να επικοινωνήσουν με άλλους routers προκειμένου να ενημερώσουν για τα υπάρχοντα δρομολόγια του δικτύου.

Η χρήση στατικών δρομολογίων παρουσιάζει αρκετά πλεονεκτήματα. Για παράδειγμα, προγραμματισμένα στατικά δρομολόγια προσφέρονται για την επίτευξη μεγαλύτερης ασφάλειας στο δίκτυο (more secure network) και μπορεί να είναι είτε

απλά, δηλαδή μοναδικά, ή πολλαπλά στατικά μονοπάτια συνδεδεμένα από και πρός το δίκτυο.

Ένα άλλο πλεονέκτημα είναι το γεγονός ότι το static routing είναι πολύ πιο αποδοτικό όσον αφορά τους πόρους που ξοδεύει. Το Static routing ξοδεύει αρκετά λιγότερο bandwidth κατά μήκος της διάδοσης, δεν ξοδεύει CPU cycles προσπαθώντας να υπολογίσει δρομολόγια, και απαιτεί πολύ λιγότερη μνήμη.
Ωστόσο, η στατική δρομολόγηση παρουσιάζει ένα αλλά πολύ σημαντικό μειονέκτημα. Σε περίπτωση δικτυακής βλάβης (network failure) ή τοπολογικής αλλαγής, όλο το βάρος πέφτει στον διαχειριστή του δικτύου ο οποίος θα πρέπει να προσαρμόσει «χειρωνακτικά» το δίκτυο στις τρέχουσες αλλαγές [1].

1.3.2 Δυναμική Δρομολόγηση (Dynamic Routing)

Η δυναμική δρομολόγηση (Dynamic Routing) αναφέρεται σε διαδρομές που μαθαίνονται μέσω ενός internal ή external routing protocol. Η προσέγγιση κάποιου δικτύου εξαρτάται από την ύπαρξη και την κατάσταση αυτού του δικτύου. Αν ο προορισμός είναι εκτός λειτουργίας (down), τότε το route θα εξαφανιστεί από τον πίνακα δρομολόγησης και το φορτίο δε θα στέλνεται προς αυτό τον προορισμό.

Οι routers σ' ένα διαδίκτυο είναι υπεύθυνοι για να λαμβάνουν και να προωθούν πακέτα διαμέσου του διασυνδεδεμένου συνόλου των υποδικτύων. Ο κάθε router οδηγεί αποφάσεις οι οποίες βασίζονται στη γνώση της τοπολογίας και στην κατάσταση του διαδικτύου. Σ' ένα απλό διαδίκτυο ένα σταθερό σχέδιο προώθησης είναι πιθανό. Λεπτομερώς, ο router πρέπει να αποφύγει τα μέρη του δικτύου τα οποία έχουν αποτύχει καθώς και να αποφασίσει για τα μέρη του δικτύου τα οποία προξενούν συμφόρηση. Προκειμένου να παρθούν τέτοιες δυναμικές αποφάσεις δρομολόγησης οι routers αλλάζουν την πληροφορία δρομολόγησης που χρησιμοποιεί ένα ειδικό πρωτόκολλο δρομολόγησης για την περίσταση. Η πληροφορία χρειάζεται για την κατάσταση του δικτύου, σε περιόδους που κάποια δίκτυα μπορούν να προσεγγιστούν από κάποιες διαδρομές και σε περιόδους καθυστέρησης των χαρακτηριστικών σε μεταβαλλόμενες διαδρομές.Για τη λειτουργία της δρομολόγησης των routers είναι απαραίτητο να διακρίνουμε δύο θέσεις:
Πληροφορία δρομολόγησης. Πληροφορία για την τοπολογία και τις καθυστερήσεις του διαδικτύου.

Αλγόριθμος δρομολόγησης. Ο αλγόριθμος παίρνει μια απόφαση δρομολόγησης για διάφορα δεδομένα, βασισμένα στην τωρινή πληροφορία δρομολόγησης. Στη συνέχεια θα εξετάσουμε τις δύο σημαντικότερες οικογένειες αλγορίθμων που χρησιμοποιούν τα πρωτόκολλα δρομολόγησης.

Distance-Vector Routing

Στο routing που βασίζεται στους distance-vector αλγορίθμους, που είναι γνωστοί και ως Bellman-Ford αλγόριθμοι, οι αλγόριθμοι περνάνε περιοδικά αντίγραφα των πινάκων δρομολόγησής τους άμεσα στους δικτυακούς γείτονές τους. Κάθε παραλήπτης προσθέτει ένα διάνυσμα απόστασης (distance vector) το οποίο είναι, η δικιά του τιμή απόστασης (distance value) στον πίνακα και το προωθεί (κάνει forward) στους γείτονες του με τους οποίους έχει άμεση πρόσβαση. Αυτή η βήμα-προς-βήμα διαδικασία έχει ως αποτέλεσμα κάθε router να μαθαίνει τη σχέση του με τους άλλους routers και να συσσωρεύει τις δικτυακές αποστάσεις (network distances).

Ο συσσωρευτικός πίνακας (cumulative table) χρησιμοποιείται τότε για να ενημερώνει τους πίνακες δρομολόγησης κάθε router. Μόλις η διαδικασία ολοκληρωθεί, κάθε router έχει μάθει την αόριστη πληροφορία σχετικά με τα distances προς τα δικτυακά resources. Δεν μαθαίνει τίποτα εξειδικευμένο σχετικά με άλλους routers, ή την ακριβή δικτυακή τοπολογία (RFC 1058, Hedrick 1988, [4]).

Link-state Routing

Οι Link-state routing αλγόριθμοι διατηρούν μια πολύπλοκη βάση δεδομένων της τοπολογίας του δικτύου. Σε αντίθεση με τα distance-vector πρωτόκολλα, τα link-state πρωτόκολλα παρουσιάζουν και διατηρούν μια πλήρη γνώση των δρομολογητών του δικτύου για το τρόπο με τον οποίο αυτοί διασυνδέονται. Αυτό επιτυγχάνεται μέσω της ανταλλαγής με άλλους routers στο δίκτυο link-state advertisements (LSAs), δηλαδή μηνυμάτων που πληροφορούν τους παραλήπτες για την κατάσταση των συνδέσεων του αποστολέα. Η πληροφορία για την κατάσταση των συνδέσεων μπορεί να χρησιμοποιηθεί για να κατασκευαστεί μια εικόνα της τοπολογίας του δικτύου.

Κάθε router ο οποίος έχει ανταλλάξει LSAs κατασκευάζει μία τοπολογική βάση δεδομένων χρησιμοποιώντας όλα τα λαμβανόμενα LSAs. Ένας αλγόριθμος

χρησιμοποιείται τότε για να υπολογίσει τη δυνατότητα προέκτασης (reachability) μέχρι τους προορισμούς. Αυτή η πληροφορία χρησιμοποιείται για να ενημερώνει τα routing tables. Αυτή η διαδικασία μπορεί να ανακαλύψει τις τοπολογικές αλλαγές στο δίκτυο που προκάλεσε μια βλάβη σε ένα τμήμα του δικτύου (component failure) ή μια ανάπτυξη του δικτύου.

1.3.3 Σύγκριση

Το static routing είναι καλό μόνο για πολύ μικρά δίκτυα τα οποία διαθέτουν μόνο ένα απλό μονοπάτι προς οποιοδήποτε δοσμένο προορισμό. Σ'αυτές τις περιπτώσεις, το static routing αποτελεί τον πιο αποτελεσματικό μηχανισμό διότι δεν καταναλώνει bandwidth προσπαθώντας να ανακαλύψει καινούρια δρομολόγια ή να επικοινωνήσει με άλλους routers. Καθώς το μέγεθος και η πολυπλοκότητα των δικτύων αυξάνονται και επομένως επιπλέον μονοπάτια προς τους προορισμούς προστίθενται, το static routing γίνεται ευαίσθητο και αποφεύγεται η χρησιμοποίησή του εκτός συγκεκριμένων περιπτώσεων (πχ σχηματισμός στατικών δρομολογίων που να υποστηρίζουν ασφάλεια).

Όσον αφορά στο dynamic routing, οι distance-vector αλγόριθμοι εφρμόζονται σε απλά πρωτόκολλα τα οποία είναι εύκολο να σχηματιστούν, διατηρηθούν, και να χρησιμοποιηθούν. Συνεπώς, αποδεικνύονται αρκετά χρήσιμα στα μικρά δίκτυα τα οποία έχουν λίγα εναλλακτικά μονοπάτια και όχι αυστηρές απαιτήσεις στην απόδοση του δικτύου.

Το link state routing αποτελεί εγγύηση ανεξαρτήτως των αποτελεσμάτων που θα επέφερε μία τοπολογική αλλαγή. Παράλληλα, υπάρχει περισσότερο bandwidth το οποίο είναι πολύ πιο χρήσιμο σε περιπτώσεις routing traffic και όχι τόσο σε περιπτώσεις συντήρησης του δικτύου, γεγονός που οδηγεί στον καταλληλότερο σχεδιασμό του τελευταίου. Γίνεται, λοιπόν, εύκολα αντιληπτό ότι η link state δρομολόγηση είναι καλύτερη για μεγάλα και πιο περίπλοκα δίκτυα αν και πρέπει να σημειωθεί ότι απαιτεί περισσότερο καλά σχεδιασμένους και συνεπώς ακριβότερους δρομολογητές.

1.4 Πρωτόκολλα εσωτερικής δρομολόγησης

Τα σημαντικότερα πρωτόκολλα εσωτερικής δρομολόγησης είναι:

i. Routing Information Protocol (RIP).
ii. Routing Information Protocol 2 (RIP 2) (αποτελεί επέκταση του RIP).
iii. Interior Gateway Routing Protocol (IGRP).
iv. Enhanced Interior Gateway Routing Protocol (EIGRP).
v. Open Short Path First (OSPF).

1.4.1 Routing Information Protocol (RIP)

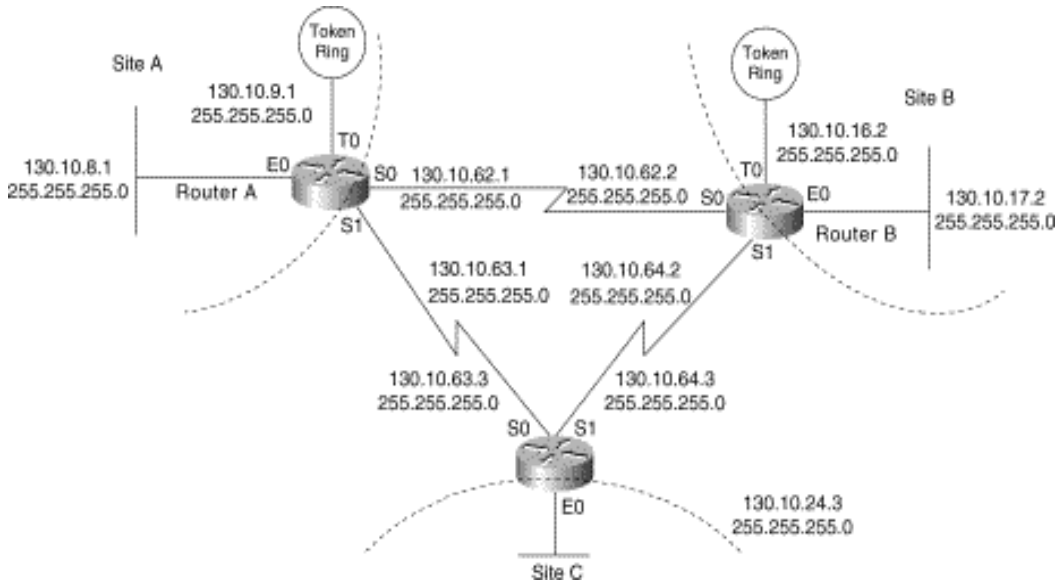
1.4.1.1 Ιστορική Αναδρομή

Το RIP είναι ένα πρωτόκολλο δρομολόγησης που χρησιμοποιήθηκε αρχικά στην Xerox Network Systems (XNS) οικογένεια πρωτοκόλλων με την ονομασία GWINFO. Μια επόμενη έκδοσή του, γνωστή ως "routed" περιλαμβανόταν στο Berkeley Standard Distribution (BSD) Unix to 1982 οπότε και έγινε δημοφιλές μέσω της χρησιμοποίησής του στην TCP/IP οικογένεια. Παράλληλα, υιοθετήθηκε στα δικτυακά προϊόντα αρκετών εταιριών κατασκευαστών προσωπικών υπολογιστών, όπως τη Novell, την Banyan (RTP), την 3COM, την AppleTalk (RTMP) κ.α. [3]. Η πρώτη υλοποίηση του IP RIP περιγράφεται στο Request For Comments (RFC) 1058 [4].

1.4.1.2 Περιγραφή λειτουργίας

Το routing με το RIP γίνεται μέσω αλγόριθμου distance vector. Ως εκ τούτου, τα βασικά σημεία της λειτουργίας του είναι αυτά που περιγράφηκαν στην παράγραφο 1.3.2.1. Ο πίνακας δρομολόγησης ενός host που υλοποιεί το RIP έχει μία είσοδο για κάθε προορισμό, η οποία πρέπει να περιλαμβάνει την IP διεύθυνση του προορισμού, μια μετρική (το συνολικό κόστος μεταφοράς ενός datagram από τον host σε αυτόν τον προορισμό), μια σημαία (flag) που να υποδεικνύει αν η πληροφορία για τον route

έχει αλλάξει πρόσφατα και διάφορα χρονόμετρα (timers) [4]. Ένα δίκτυο RIP φαίνεται στο σχήμα 1-2.



Σχήμα 1-2: Ένα δίκτυο RIP

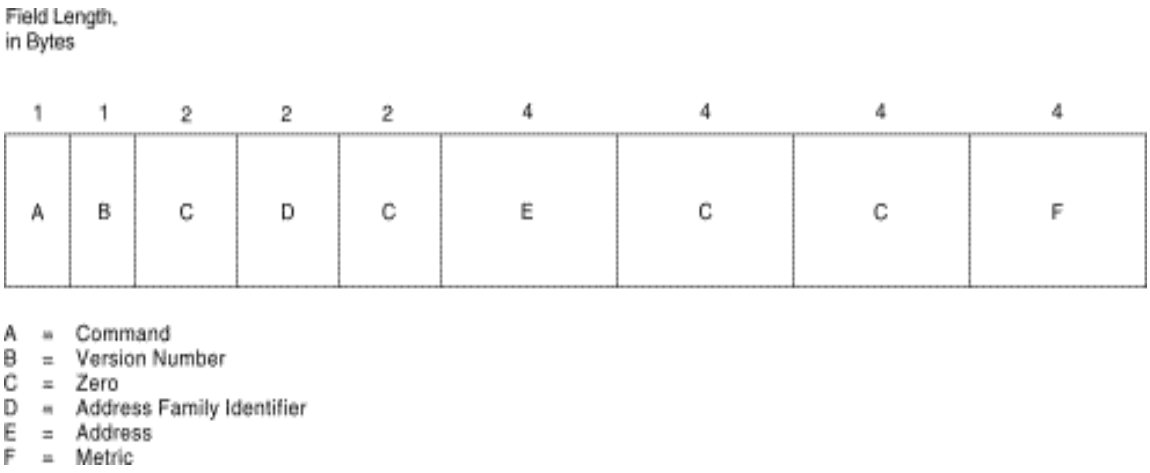
Αναλυτικότερα, η λειτουργία του RIP περιλαμβάνει [1]:

- **RIP Updates** Το RIP στέλνει updates ανά τακτά διαστήματα και κάθε φορά που αλλάζει η τοπολογία του δικτύου. Όταν ένας router λαμβάνει ένα update μεταβάλλει τον πίνακα δρομολόγησής του εξαιτίας της νέας εισόδου. Στη συνέχεια, ο router στέλνει με τη σειρά του updates στους γειτονικούς του routers πληροφορώντας τιυς για την αλλαγή. Αυτά τα updates είναι ανεξάρτητα από τα προγραμματισμένα updates που στέλνουν οι RIP routers.
- **RIP Metrics** Για το RIP η μετρική είναι ο αριθμός των κόμβων μεταξύ της πηγής και του προορισμού. Κάθε τέτοιος κόμβος έχει τιμή 1 οπότε όταν ένας router λαμβάνει ένα update η τιμή της μετρικής αυξάνεται κατά 1 και ο αποστολέας υποδεικνύεται ως το επόμενο hop ενώ ο router διατηρεί μόνο την καλύτερη διαδρομή (αυτή με τη μικρότερη μετρική) για έναν προορισμό. Ο μέγιστος αριθμός κόμβων για το RIP είναι 15, με το 16 να παριστάνει ένα άκυρο δρομολόγιο (μια άπειρη μετρική). Σε μια τέτοια περίπτωση, βέβαια, ο προορισμός θεωρείται ανέφικτος.

- **RIP Stability Features** Προκειμένου να προσαρμοστεί σε γρήγορες και συχνές δικτυακές μεταβολές, το RIP έχει κάποια χαρακτηριστικά σταθερότητας (Stability Features). Πιο συγκεκριμένα, το RIP υλοποιεί την τεχνική split-horizon, η οποία προστατεύει από την αποστολή της πληροφορίας δρομολόγησης στο σύστημα από το οποίο μαθεύτηκε η ίδια πληροφορία. Επίσης, χρησιμοποιείται ο hold-down μηχανισμός ώστε να μην πιστεύουν οι routers λανθασμένη πληροφορία δρομολόγησης που προέρχεται από συσκευές που δεν έχουν ακόμα ενημερωθεί για μια τοπολογική αλλαγή.
- **RIP Timers** Για την υλοποίηση του RIP χρησιμοποιούνται αρκετά χρονόμετρα (timers). Το update timer είναι ο χρόνος μεταξύ δύο updates και είναι θεωρητικά 30 sec, αλλά συνήθως είναι αυξημένος κατά κάποια δευτερόλεπτα ώστε να συγχρονίζονται τα updates μεταξύ τους και να αποφεύγονται οι συγκρούσεις (collisions) [3]. Το invalid timer (ή route timeout) είναι ο χρόνος μεταξύ δύο updates από έναν συγκεκριμένο γειτονικό router και ο οποίος αν παρέλθει ενεργοποιείται ο hold-down μηχανισμός. Για το RIP ο χρόνος αυτός είναι 180 sec. Όταν συμβαίνει ένα failure τρέχει και ένα άλλο χρονόμετρο, το flush timer (240 sec). Αν παρέλθει και αυτός ο χρόνος, η διαδρομή όχι μόνο είναι άκυρη αλλά, επιπλέον, απομακρύνεται από τον πίνακα δρομολόγησης.

Το IP RIP packet format αποτελείται από 9 πεδία και φαίνεται στο Σχήμα 1-3 ενώ οι παρακάτω περιγραφές είναι απαραίτητες για την κατανόηση του σχήματος.

- **Command** Δείχνει αν το πακέτο είναι request ή response. Το request ζητάει από έναν router να στείλει ολόκληρο ή μέρος του πίνακα δρομολόγησής του ενώ το response μπορεί να είναι η απάντηση σε ένα request ή ένα τακτικό update.
- **Version Number** Καθορίζει την χρησιμοποιούμενη έκδοση του RIP.



Σχήμα 1-3: Το packet format του RIP

- **Zero** Δεν χρησιμοποιείται
- **Address Family Identifier (AFI)** Καθορίζει την οικογένεια διευθύνσεων (Address Family) που χρησιμοποιείται. Για το IP το AFI είναι 2.
- **Address** Καθορίζει την IP address για την είσοδο του πίνακα δρομολόγησης.
- **Metric** Αριθμός των κόμβων από την πηγή. Όπως ειπώθηκε παραπάνω, είναι μεταξύ 1-15 για έγκυρη διαδρομή και 16 για ανέφικτη.

1.4.1.3 Επίλογος

Με την χρησιμοποποίηση του RIP, όταν ένας δρομολογητής μαθαίνει για τις αλλαγές στις διαδρομές από κάποιον γείτονά του, δίνει αυτή την πληροφορία στους άλλους γείτονές του ώστε να ανανεωθούν οι πίνακες δρομολόγησης. Έτσι, αν ένα μέρος του δικτύου αποτύχει, τότε το άλλο μέρος του δικτύου υπολογίζει πώς, αν είναι δυνατόν, να εργαστεί παρά την αποτυχία αυτή. Όταν η βλάβη αποκατασταθεί, τότε το δίκτυο επιστρέφει στον αρχικό τρόπο λειτουργίας του.

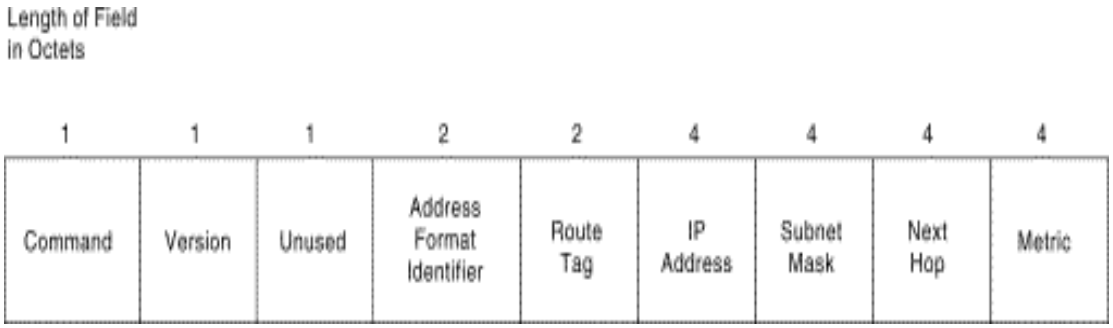
Θα λέγαμε ότι το RIP είναι ο «παππούς» των πρωτοκόλων δρομολόγησης [1]. Αποτελεί ένα πολύ καλό παράδειγμα αλγοριθμοποίησης distance vector ενώ ο σχηματισμός του είναι απλός και εύκολος και, ως εκ τούτου, αποτελεί ιδανική επιλογή για μικρά και απλά δίκτυα. Ωστόσο, το γεγονός ότι η μετρική του δεν μπορεί να είναι πάνω από 16 περιορίζει το μέγεθος των δικτύων στα οποία μπορεί να εφαρμοστεί.

1.4.2 Routing Information Protocol Version 2 (RIP 2)

Η δεύτερη έκδοση του RIP αποτελεί μαι αναβάθμιση της αρχικής και έχει χαρακτηριστικά που απαιτούν τα μοντέρνα πρωτόκολλα δρομολόγησης. Περιλαμβάνει μεγαλύτερη ποσότητα πληροφορίας δρομολόγησης και περιγράφεται στα Request For Comments (RFCs) 1388 [5] και 1721-1723.

Η βασική καινοτομία που εισάγει το RIP 2 είναι η δυνατότητα ενσωμάτωσης της μάσκας υποδικτύου (subnet mask) και κατά συνέπεια η χρησιμοποίησή του σε Μεταβλητού Μήκους Μάσκας Υποδικτύου (Variable Length Subnet Mask) περιβάλλοντα. Επίσης, έχει προστεθεί ένα πεδίο πιστοποίησης (authentication field) στο packet format του RIP ώστε να μην επιτρέπεται σε μια μη εξουσιοδοτημένη οντότητα να εγχέει λανθασμένη πληροφορία δρομολόγησης στο δίκτυο.

Μία άλλη σημαντική αλλαγή είναι η πρόσθεση μιας νέας διεύθυνσης επόμενου κόμβου (next-hop address) ώστε ο router να μπορεί να καθορίσει έναν γειτονικό του ως τον καλύτερο επόμενο κόμβο για κάποια διαδρομή. Το packet format του RIP 2 αποτελείται από πεδία όμοια με αυτά του RIP και απεικονίζεται στο σχήμα 1-4.



Σχήμα 1-4: Το packet format του RIP 2

- **Command** Δείχνει αν το πακέτο είναι request ή response. Το request ζητάει από έναν router να στείλει ολόκληρο ή μέρος του πίνακα δρομολόγησής του ενώ το response μπορεί να είναι η απάντηση σε ένα request ή ένα τακτικό update.
- **Version Number** Καθορίζει την χρησιμοποιούμενη έκδοση του RIP (δηλ. 2).
- **Unused** Μηδενική τιμή.

- **Address Family Identifier (AFI)** Καθορίζει την οικογένεια διευθύνσεων (Address Family) που χρησιμοποιείται. Για το IP το AFI είναι 2. Αν το AFI για την πρώτη είσοδο στο μήνυμα είναι 0xFFFF, το υπόλοιπο της εισόδου περιέχει πληροφορία πιστοποίησης (πχ κάποιο password).
- **Route Tag** Παρέχει μια μέθοδο διαχωρισμού μεταξύ εσωτερικών (μέσω του RIP) και εξωτερικών (μέσω άλλων πρωτοκόλλων) διαδρομών.
- **IP Address** Καθορίζει την IP address για την είσοδο του πίνακα δρομολόγησης.
- **Subnet Mask** Περιέχει τη μάσκα υποδικτύου για την είσοδο. Αν είναι 0 δεν έχει καθοριστεί μάσκα υποδικτύου.
- **Next Hop** Υποδεικνύει την IP address του επόμενου κόμβου στον οποίο πρέπει να προωθηθούν τα πακέτα για μια είσοδο.
- **Metric** Αριθμός των κόμβων από την πηγή. Όπως ειπώθηκε παραπάνω, είναι μεταξύ 1-15 για έγκυρη διαδρομή και 16 για ανέφικτη.

Η δεύτερη έκδοση, λοιπόν, του RIP παρέχει περισσότερες δυνατότητες σε σχέση με την αρχική και αποτελεί καλή λύση όμως και πάλι μόνο για μικρά δίκτυα ή για μικρά τμήματα μεγάλων δικτύων.

1.4.3 Interior Gateway Routing Protocol (IGRP)

1.4.3.1 Ιστορική Αναδρομή

Το IGRP είναι ένα πρωτόκολλο δρομολόγησης που αναπτύχθηκε στα μέσα της δεκαετίας του ’80 από την εταιρία Cisco Systems η οποία είχε ως αρχικό στόχο να κατασκευάσει ένα δυνατό πρωτόκολλο για δρομολόγηση στο εσωτερικό αυτόνομων συστημάτων. Δημιουργήθηκε για να καλύψει τις αδυναμίες του RIP αφού αυτό δεν μπορούσε να χρησιμοποιηθεί σε πολύπλοκα και μεγάλου μεγέθους δίκτυα και πραγματικά η σθεναρότητά του οδήγησε πολλούς μεγάλους οργανισμούς να αντικαταστήσουν το RIP με το IGRP [6].

1.4.3.2 Δομή - Χαρακτηριστικά

Το IGRP είναι ένα distance vector πρωτόκολλο με στοιχεία όμως και link-state αλγορίθμων. Ένα από τα βασικά του πλεονεκτήματα είναι ότι απαιτεί έναν αριθμό αυτόνομου συστήματος (autonomous system number) ο οποίος πρέπει να αντιστοιχεί σε όλους τους γειτονικούς routers με τους οποίους αναμένεται να γίνει ανταλλαγή πληροφορίας δρομολόγησης. Ένα update με διαφορετικό αριθμό αυτόνομου συστήματος αγνοείται. Με αυτόν τον τρόπο αποφεύγεται η έγχυση λανθασμένης πληροφορίας δρομολόγησης [1].

Επίσης, ένα άλλο χαρακτηριστικό που προσφέρει μεγάλη ευελιξία στο IGRP είναι ότι υπολογίζει όχι μόνο ένα (όπως το RIP) αλλά πολλαπλά μονοπάτια (multipath) προς τον ίδιο προορισμό. Το πλεονέκτημα είναι ότι αυξάνει η αξιοπιστία και η απόδοση αφού μπορεί να γίνει διαχωρισμός της κυκλοφορίας σε πολλές διαδρομές για να ελαττωθεί το φορτίο σε καθεμιά από τις γραμμές επικοινωνίας. Για να καθορίσει το IGRP ότι ένα μονοπάτι είναι χρησιμοποιήσιμο χρησιμοποιεί δύο κριτήρια. Πρώτον, ο γειτονικός router πρέπει να είναι πιο κοντά στον προορισμό από τον τοπικό. Έτσι εξασφαλίζεται ότι ο γειτονικός router δεν έχει ένα λανθασμένο μονοπάτι για τον προορισμό. Δεύτερον, η μετρική του γειτονικού router πρέπει να είναι μικρότερη από το γινόμενο της μετρικής του τοπικού router επί τον συντελεστή διακύμανσης [1]. Τα πολλαπλά μονοπάτια μπορούν να χρησιμοποιηθούν ακόμα και όταν οι μετρικές είναι διαφορετικές. Δηλαδή, αν ένα μονοπάτι έχει τρεις φορές μικρότερη μετρική από ένα άλλο, θα χρησιμοποιηθεί τρεις φορές περισσότερο. Εξάλλου, μόνο οι διαδρομές με μετρικές εντός συγκεκριμένων ορίων κοντά στη βέλτιστη χρησιμοποιούνται ως πολλαπλά μονοπάτια [6].

- **IGRP Metrics** Το IGRP χρησιμοποιεί ένα συνδυασμό μετρικών στα updates του. Εύρος (bandwidth), καθυστέρηση (delay), αξιοπιστία (reliability) και φορτίο (load) συνυπάρχουν στην πληροφορία δρομολόγησης. Οι μετρικές αυτές μπορούν να παίρνουν τιμές σε μεγάλη σχετικά έκταση κάτι που συμβαίνει συχνά σε διαδίκτυα με μεταβαλλόμενα χαρακτηριστικά ενώ, παράλληλα, ο συνδυασμός των αλγορίθμων μπορεί να γίνει από τον ίδιο τον network administrator.

- **IGRP Stability Features** Το IGRP χρησιμοποιεί τις τεχνικές spilt-horizon και hold-down όπως ακριβώς και το RIP που είδαμε νωρίτερα.
- **IGRP Timers** Το IGRP έχει τα ίδια χρονόμετρα με το RIP με την διαφορά ότι κάθε χρονόμετρο έχει διαφορετική τιμή απ' ότι στο RIP. Το update timer είναι 90 sec, το invalid timer (ή route timeout) είναι 270 sec ενώ το flush timer είναι 630 sec.

1.4.3.3Επίλογος

Το IGRP είναι ένα πολύ πετυχημένο πρωτόκολλο. Το πλεονέκτημα της χρησιμοποίησης πραγματικών χαρακτηριστικών για τον υπολογισμό της μετρικής του μονοπατιού είναι πολύ χρήσιμο και δουλεύει καλά στην πράξη. Ωστόσο, νεότερα πρωτόκολλα έχουν καλύτερα χαρακτηριστικά σύγκλισης και για το λόγο αυτό το αντικαθιστούν σε μεγάλα δίκτυα. Ένα από αυτά είναι το Enhanced IGRP το οποίο θα εξετάσουμε στην επόμενη παράγραφο.

1.4.4 Enhanced Interior Gateway Routing Protocol

1.4.4.1 Πρόλογος

Το EIGRP αποτελεί τη μετεξέλιξη του IGRP η οποία προήλθε από την διαφοροποίηση των δικτυακών απαιτήσεων εξαιτίας της σημαντικής ανάπτυξης των διαδικτύων και κυρίως του Internet. Το EIGRP ενοποιεί τα χαρακτηριστικά και τις ικανότητες των link-state στα distance-vector πρωτόκολλα. Είναι συμβατό με IGRP routers οπότε μπορεί να προστεθεί σταδιακά σε ήδη υπάρχοντα IGRP δίκτυα. Επίσης, χρησιμοποιεί ακριβώς τις ίδιες μετρικές με το IGRP με αποτέλεσμα να είναι απολύτως συγκρίσιμες, σαν να πρόκειται για διαδρομές από το ίδιο Αυτόνομο Σύστημα. Το EIGRP θεωρεί τις IGRP διαδρομές εξωτερικές, δίνοντας, έτσι, την δυνατότητα στο διαχειριστή του δικτύου να τις προσαρμόσει σύμφωνα με τις απαιτήσεις του συστήματος [7].

1.4.4.2 Χαρακτηριστικά – Ιδιότητες

- Επιτυγχάνεται γρήγορη σύγκλιση (fast convergence) αφού ένας EIGRP router αποθηκεύει τους πίνακες δρομολόγησης των γειτονικών του ώστε να υιοθετεί γρήγορα εναλλακτικές διαδρομές. Αν δεν υπάρχει εναλλακτική διαδρομή ο EIGRP router στέλνει queries στους γειτονικούς του μέχρι να βρεθεί τουλάχιστον μία.
- Οι διαδρομές συνοψίζονται αυτόματα αφού το EIGRP πρωτόκολλο υποστηρίζει μάσκες υποδικτύου μεταβλητού μήκους (variable length subnet masks).
- Στο EIGRP δεν στέλνονται περιοδικά updates σε όλους τους routers αλλά μόνο όταν αλλάζει η μετρική για μια διαδρομή και μόνο στους routers που χρειάζεται να μάθουν την πληροφορία αυτή. Έτσι, μειώνεται σημαντικά σε σχέση με το IGRP το εύρος ζώνης που καταναλώνεται.
- Το EIGRP χρησιμοποιεί πακέτα τύπου hello and acknowledgement, τύπου update και τύπου query and reply.

1.4.4.3 Θεμελιώδεις τεχνολογίες

Προκειμένου να παρέχει καλή απόδοση στη δρομολόγηση το EIGRP χρησιμοποιεί τις παρακάτω τεχνολογίες οι οποίες συνδυαζόμενες, το κάνουν να διαφέρει από τα άλλα πρωτόκολλα [7].

- **Neighbor discovery/recovery** Μέσω αυτής της διαδικασίας οι routers λαμβάνουν πληροφορίες για τους γειτονικούς τους και μαθαίνουν αν είναι εφικτή η σύνδεση μαζί τους.
- **Reliable Transport Protocol (RTP)** Το πρωτόκολλο αυτό είναι υπεύθυνο για την σωστή παράδοση των EIGRP πακέτων στους γειτονικούς routers που ζήτησαν πληροφορία. Το RTP προβλέπει να στέλνονται γρήγορα multicast πακέτα όταν δεν έχει επιβεβαιωθεί η λήψη ώστε να διατηρείται ο χρόνος σύγκλισης σε χαμηλά επίπεδα προκειμένου για συνδέσεις διαφορετικών ταχυτήτων.

- **DUAL finite-state machine** Η τεχνολογία αυτή συστηματοποιεί την διαδικασία υπολογισμού των διαδρομών που γνωστοποιούνται από τους γειτονικούς routers με προφανή θετική επίδραση στο χρόνο σύγκλισης.
- **Protocol-dependent modules** Τα modules αυτά έχουν την ευθύνη της μεταφοράς των EIGRP πακέτων για απαιτήσεις επιπέδου δικτύου.

1.4.4.4 Βασικές αρχές

Το EIGRP βασίζεται στις παρακάτω αρχές [1]:

- **Neighbor Table** Όταν ένας router ανακλύπτει έναν καινούριο γειτονικό του, καταγράφει την διεύθυνσή του σαν είσοδο στον γειτονικό πίνακα (Neighbor Table). Παράλληλα, σε αυτήν την είσοδο περιέχεται πληροφορία που απαιτείται από το RTP.
- **Topology Table** Ο πίνακας τοπολογίας (Topology Table) περιέχει τους προορισμούς που γνωστοποιούνται από τους γειτονικούς routers.
- **Route State** Η είσοδος στον πίνακα τοπολογίας για έναν προορισμό μπορεί να είναι σε μία από τις εξής δύο καταστάσεις (states): ενεργή (active) ή όχι (passive). Ένας προορισμός είναι ενεργός όσο ο router όσο πραγματοποιεί την διαδικασία υπολογισμού των αντίστοιχων διαδρομών.

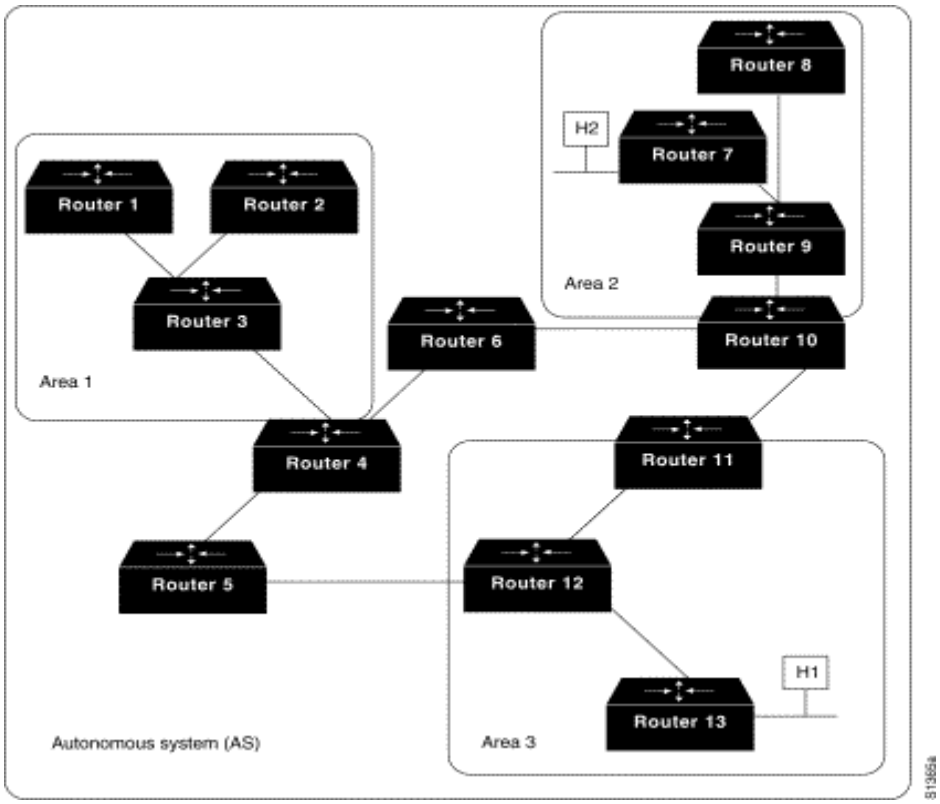
1.4.5 Open Short Path First (OSPF)

1.4.5.1 Εισαγωγή

Το OSPF είναι ένα πρωτόκολλο εσωτερικής δρομολόγησης που αναπτύχθηκε στις αρχές της δεκαετίας του ’90 για να αντικαταστήσει το RIP το οποίο είχε αρχίσει να μην καταφέρνει να καλύψει τις ολοένα αυξανόμενες ανάγκες των μεγάλων, ετερογενών διαδικτύων. Το OSPF προτυποποιήθηκε το 1988 και από τότε χρησιμοποιείται ευρύτατα σε TCP/IP δίκτυα. Είναι ένα link state πρωτόκολλο και βασίζεται στον Shortest Path First (SPF) αλγόριθμο του Dijkstra [2] οι προδιαγραφές του περιγράφονται στο Request For Comments (RFC) 1247 [8].

1.4.5.2 Δομή – Λειτουργία

Το OSPF μπορεί να λειτουργεί μέσα σε ένα ιεραρχικό περιβάλλον όπου το αυτόνομο σύστημα μπορεί να χωρίζεται σε περιοχές, οι περιοχές σε υποπεριοχές και ούτω καθεξής (Σχ. 1-5) [9].



Σχήμα 1-5: Αυτόνομο σύστημα χωρισμένο σε περιοχές

Το OSPF είναι link - state πρωτόκολλο. Έτσι κάθε router στέλνει πληροφορίες για την κατάσταση των links του (Link State Advertisements - LSA) σε όλους τους άλλους που βρίσκονται στο ίδιο επίπεδο ιεραρχίας με αυτόν. Τα μηνύματα αυτά είναι μικρά και έτσι δεν καταναλώνουν μεγάλο εύρος ζώνης. Αρχικά ένας router αρχικοποιεί τις δομές δεδομένων του και περιμένει από τα πρωτόκολλα των χαμηλότερων επιπέδων να διαπιστώσει ποια από τα links του, είναι λειτουργικά. Έπειτα με τη χρήση Hello μηνυμάτων προσπαθεί να βρει τους γειτονικούς του routers. Τα Hello μηνύματα χρησιμοποιούνται και στη συνέχεια για να ελέγχει ο router αν οι γείτονές του είναι ακόμη σε λειτουργία. Κάθε router στέλνει περιοδικά LSAs με την κατάσταση των links του. Ακόμη LSAs στέλνονται και όταν αλλάζει η κατάσταση ενός router.

Ένας router διατηρεί την τοπολογία όλου του επιπέδου του δικτύου που ανήκει (η οποία μπορεί να εκφραστεί σαν κατευθυνόμενος γράφος) και προσπαθεί να την διατηρεί ενημερωμένη από τα LSAs που λαμβάνει. Όταν λαμβάνει LSAs και ενημερώνει την τοπολογία, τρέχει ο αλγόριθμος SPF. Αυτός υπολογίζει τις καλύτερες διαδρομές για τα δίκτυα προορισμού, και έπειτα αποθηκεύεται στον routing πίνακα το πρώτο hop κάθε διαδρομής, για να χρησιμοποιηθεί για τη διαδικασία προώθησης (forwarding) [1].

1.4.5.3Χαρακτηριστικά

- **Message Format** Τα OSPF μηνύματα ξεκινούν με μια επικεφαλίδα (header) 24-byte:

(Σε παρένθεση ο αριθμός των byte)

Version Number (1)	Type (1)	Packet length (2)	Router ID (4)	Area ID (4)	Check sum (2)	Authent ication type (2)	Authentication (8)

Η σημασία των πεδίων της OSPF header είναι:

- Version number Η υλοποίηση του OSPF που χρησιμοποιείται.
- Type Προσδιορίζει ένα από τους 5 τύπους των OSPF μηνυμάτων:

Hello Στέλνεται σε τακτά χρονικά διαστήματα για να ιχνηλατήσει την κατάσταση των γειτονικών routers.

Database Description Περιγράφει τα περιεχόμενα της τοπολογικής βάσης ενός router και στέλνεται κατά την αρχικοποίηση μιας σύνδεσης με ένα γειτονικό router.

Link State Request Με το μήνυμα αυτό ένας router ζητά ένα κομμάτι του τοπολογικού πίνακα ενός γειτονικού του router, επειδή έχει ανακαλύψει ότι μέρος της δικής του τοπολογικής βάσης είναι μη ενημερωμένο.

Link State Update Απαντάει σε link state request μηνύματα. Επιπλέον χρησιμοποιείται για την περιοδική μετάδοση των LSAs.

Link State Acknowledgment Στέλνεται για acknowledgment στα link state update μηνύματα. Τα link state update μηνύματα πρέπει να φτάσουν σε όλους τους προορισμούς του επιπέδου ιεραρχίας του δικτύου, μέσα στο οποίο στέλνονται.

- Packet length Το συνολικό μέγεθος του πακέτου.
- Router ID Προσδιορίζει το router που έστειλε το μήνυμα.
- Area ID Προσδιορίζει την περιοχή (area) στην οποία το πακέτο ανήκει.
- Checksum Ελέγχει το περιεχόμενο του πακέτου για πιθανές αλλοιώσεις.
- Authentication type Περιέχει ένα τύπο απόδοσης εξουσιοδότησης (Authentication type) για παράδειγμα «simple password». Όλα τα OSPF μηνύματα πρέπει να περιέχουν μια τιμή στο πεδίο αυτό.
- Authentication Περιέχει την authentication πληροφορία (το ίδιο το password) μήκους 64 bits.

- **Multipath Routing** Το OSPF υποστηρίζει multipath routing, καθώς και δρομολόγηση βασισμένη σε πληροφορία των πρωτοκόλλων των υψηλότερων επιπέδων (type of service (TOS) πεδίο στην IP header). Για παράδειγμα, μια εφαρμογή μπορεί να προσδιορίσει ότι η μετάδοση κάποιων δεδομένων είναι επείγουσα. Αν στο OSPF έχουν τεθεί κάποια links σαν υψηλής προτεραιότητας τότε μπορούν να χρησιμοποιηθούν αυτά για την μετάδοση της επείγουσας πληροφορίας.
- **Metrics** Το OSPF υποστηρίζει μία ή περισσότερες μετρικές (καθορίζεται από τον network administrator). Αν υποστηρίζει μόνο μία, τότε δεν υποστηρίζει το TOS IP πεδίο που αναφέρθηκε προηγουμένως. Αν υποστηρίζει περισσότερες από μία τότε το TOS υποστηρίζεται. Πιο συγκεκριμένα υποστηρίζονται οι οχτώ συνδυασμοί που δημιουργούν τα τρία IP TOS bits τα οποία αντιστοιχούν στο delay, στο throughput και στη reliability (καθένα από αυτά έχει δύο τιμές). Κάθε συνδυασμός π.χ. low delay, low throughput, high reliability, θεωρείται μια ξεχωριστή μετρική για την οποία υπάρχει ξεχωριστός πίνακας δρομολόγησης. Άρα όταν ζητείται ένας από τους οχτώ συνδυασμούς TOS η δρομολόγηση γίνεται με τη χρήση του αντίστοιχου πίνακα.

- **Support VLSM** Τα μηνύματα του πρωτοκόλλου μπορούν να περιέχουν IP μάσκες υποδικτύου μεταβλητού μεγέθους.

1.4.5.4Επίλογος

Το OSPF είναι ένα πολύ καλό λειτουργικό πρωτόκολλο αφού η σύγκλιση επιτυγχάνεται αρκετά γρήγορα. Παράλληλα, υπάρχουν πολλά εργαλεία [1] που επιτρέπουν στο OSPF να χρησιμοποιείται σε μεγάλα και απαιτητικά δίκτυα. Εν γένει, το OSPF έχει πολλά χαρακτηριστικά και απαιτεί περισσότερη σκέψη προκειμένου να σχεδιαστεί και να λειτουργήσει από τα υπόλοιπα IGP πρωτόκολλα που εξετάσαμε. Ωστόσο, οι πολλές παράμετροι και παράγοντες υλοποίησης το καθιστούν εκτός από πολύπλοκο, ένα πολύ ισχυρό και γρήγορο πρωτόκολλο που αναμένεται να εξελιχθεί ακόμα περισσότερο στα επόμενα χρόνια.

1.5 Εξωτερική Δρομολόγηση

Σαν παράδειγμα εξωτερικής δρομολόγησης θα περιγραφεί το Border Gateway Protocol (BGP) το οποίο έχει γίνει το standard EGP στο Internet. Οι αρχές του μπορούν να εφαρμοστούν σε όλα τα δίκτυα ανεξαρτήτως οικογένειας πρωτοκόλλων που χρησιμοποιούν.

1.5.1 Border Gateway Protocol

Με τη χρήση του BGP, routers διαφορετικών αυτόνομων συστημάτων ανταλλάσσουν πληροφορία δρομολόγησης και από αυτήν υπολογίζουν καλύτερες διαδρομές. Το BGP αποτελείται από 4 (open, keepalive, update, notification) μηνύματα τα οποία στέλνονται πάνω από TCP συνδέσεις που ανοίγουν οι routers μεταξύ τους.

Οι βασικές διαδικασίες του πρωτοκόλλου είναι τρεις:

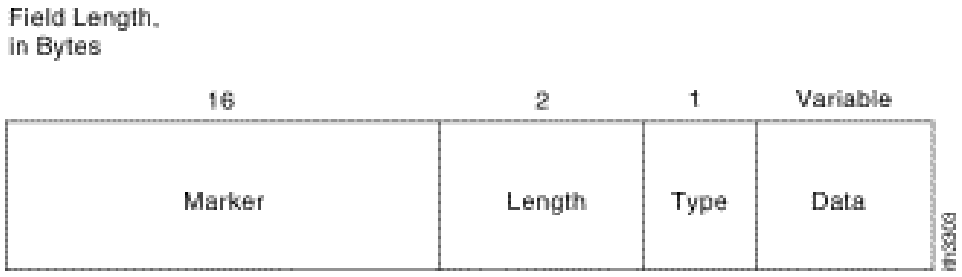
- Neighbor acquisition (Απόκτηση Γειτόνων)
- Neighbor reachability (Προσβασιμότητα στους γείτονες)

- Network reachability (Προσβασιμότητα σε κάποιο υποδίκτυο)

Η διαδικασία neighbor acquisition έχει να κάνει με τη συμφωνία δύο δρομολογητών που ανήκουν σε διαφορετικά αυτόνομα συστήματα αλλά συνδέονται στο ίδιο υποδίκτυο (subnetwork), ότι θα ανταλλάσσουν routing πληροφορία όποτε αυτό είναι απαραίτητο. Η διαδικασία αυτή είναι απαραίτητη γιατί μπορεί οι δύο routers να συνδέονται στο ίδιο υποδίκτυο και να είναι γείτονες αλλά μπορεί ο ένας από αυτούς να είναι φορτωμένος με την δρομολόγηση μέσα στο αυτόνομο σύστημα στο οποίο ανήκει, και να μην θέλει να αναλάβει κίνηση πακέτων προερχόμενων από άλλο. Η διαδικασία αυτή του πρωτοκόλλου δεν προβλέπει με ποιο τρόπο οι routers γνωρίζουν τις διευθύνσεις των γειτόνων τους ή πως δύο routers αποφασίζουν να ανταλλάξουν πληροφορία δρομολόγησης. Κάτι τέτοιο μπορεί να ρυθμιστεί από τον διαχειριστή του δικτύου. Για να πραγματοποιηθεί η διαδικασία αυτή ένας router στέλνει ένα Open μήνυμα στον άλλο. Αν ο router προορισμού δεχτεί την αίτηση, απαντά με ένα Keepalive μήνυμα.

Η διαδικασία neighbor reachability διατηρεί μια σχέση γειτονικότητας την οποία έχουν συμφωνήσει οι δύο routers με την προηγούμενη διαδικασία. Η σχέση αυτή διατηρείται με την αποστολή Keepalive μηνυμάτων ανά τα τακτά χρονικά διαστήματα. Η τελευταία διαδικασία network reachability σκοπό έχει οι routers να διατηρούν πληροφορία για την προσπέλαση των υποδικτύων. Έτσι κάθε router διατηρεί μια βάση δεδομένων με τα υποδίκτυα τα οποία μπορεί να προσπελάσει και την καλύτερη διαδρομή προς αυτά. Όταν συμβαίνει κάποια αλλαγή στη βάση δεδομένων, ο router, στέλνει (broadcast) Update μηνύματα σε όλους τους routers που υλοποιούν το BGP. Με τον τρόπο αυτό οι BGP routers ενημερώνονται για αλλαγές που συμβαίνουν στο δίκτυο και προσαρμόζουν τις καλύτερες διαδρομές στους routing πίνακές τους [10].

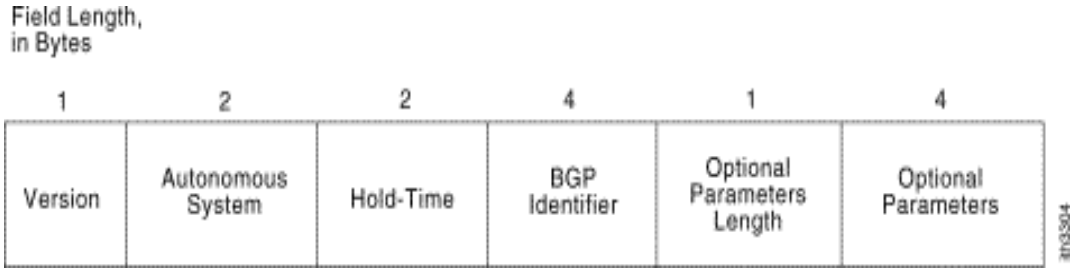
- **Message Format** Όλοι οι τύποι των BGP μηνυμάτων χρησιμοποιούν την βασική επικεφαλίδα (header) που φαίνεται στο σχήμα 1-6.



Σχήμα 1-6 Επικεφαλίδα ενός BGP πακέτου

- ♦ Marker Χρησιμοποιείται για authentication. Ο αποστολέας μπορεί να εισάγει μια τιμή σε αυτό το πεδίο, η οποία θα χρησιμοποιηθεί κατά τη διαδικασία αναγνώρισης της ταυτότητάς του από τον παραλήπτη.
- ♦ Length Το μήκος του μηνύματος σε bytes.
- ♦ Type Ο τύπος του μηνύματος (open, keepalive, update, notification).

Open message



Σχήμα 1-7 Ένα BGP open μήνυμα

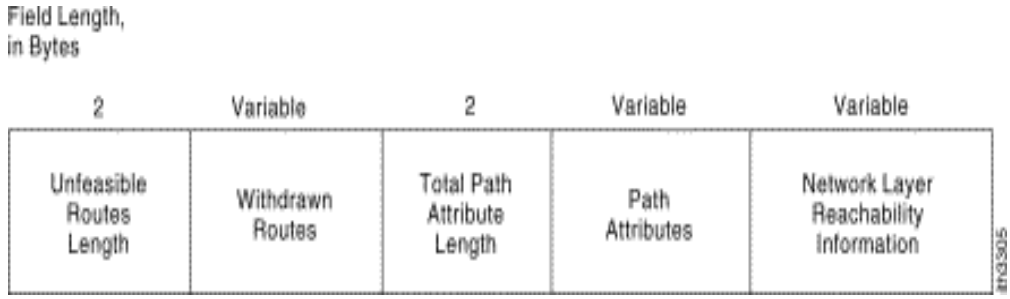
Το Open μήνυμα (Σχ. 1-7) περιέχει ένα πεδίο με το AS στο οποίο ανήκει ο αποστολέας router και ένα με την IP διεύθυνσή του (BGP identifier). Ακόμη περιέχει και ένα πεδίο Hold time το οποίο δηλώνει τον μέγιστο αριθμό των δευτερολέπτων, που προτείνει ο αποστολέας, για το χρονικό διάστημα μεταξύ δύο επιτυχημένων

Keepalive ή Update μηνυμάτων του. Ο παραλήπτης υπολογίζει το μικρότερο από το δικό του Hold time και το Hold time που λαμβάνει και αυτό τίθεται στον Hold timer.

Keepalive message

Τα Keepalive μηνύματα αποτελούνται μόνο από το header.

Update message



Σχήμα 1-8 Ένα BGP update μήνυμα

Το update μήνυμα (Σχ. 1-8) μπορεί να περιέχει δύο είδη πληροφορίας:
Α) Πληροφορία για μία διαδρομή του δικτύου. Η πληροφορία αυτή προστίθεται στη βάση δεδομένων των routers που τη λαμβάνουν, ή/και
Β) Μια λίστα από διαδρομές που είχαν προταθεί από το router, οι οποίες τώρα αποσύρονται.

Σχετικά με το πρώτο είδος πληροφορίας εμπλέκονται τα εξής πεδία. Το Network Layer Reachability Information (NLRI), το Total Path Attributes Length, το Path Attributes. Το NLRI περιέχει τις IP διευθύνσεις (το μέρος των IP διευθύνσεων που δηλώνει ένα συγκεκριμένο υποδίκτυο) των υποδικτύων που μπορούν να προσπελαστούν από τη συγκεκριμένη διαδρομή. Το πεδίο Path Attributes περιέχει μια λίστα από χαρακτηριστικά (attributes) της συγκεκριμένης διαδρομής: Αυτά είναι:

Origin: Καθορίζει αν η πληροφορία για τη συγκεκριμένη διαδρομή δημιουργήθηκε από ένα interior gateway protocol π.χ. OSFP, ή από ένα exterior gateway protocol (το BGP).

AS_Path: Περιέχει όλα τα αυτόνομα συστήματα που διασχίζει η διαδρομή. Με τη χρήση του πεδίου αυτού ένας router μπορεί να επιλέξει ή να απορρίψει μια διαδρομή

ανάλογα με την πληροφορία που έχει για τα αυτόνομα συστήματα που αυτή διασχίζει. Για παράδειγμα αν γνωρίζει ότι ένα αυτόνομο σύστημα είναι μικρής απόδοσης μπορεί να απορρίψει τη διαδρομή. Επίσης το πεδίο αυτό βοηθά στο να τερματίζεται η μετάδοση ενός Update μηνύματος αποτρέποντάς το από το να κάνει κύκλους ασταμάτητα. Όταν ένας router λάβει ένα update μήνυμα και το αυτόνομο σύστημα στο οποίο ανήκει περιέχεται στο AS_Path πεδίο του μηνύματος, σταματά την επαναμετάδοσή του.

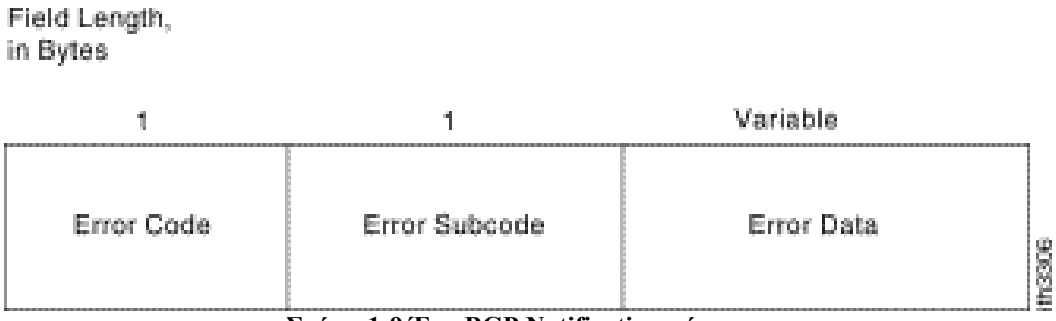
Next_hop: Περιέχει την IP διεύθυνση του border router που προτείνεται να χρησιμοποιηθεί σαν next hop για όλους του προορισμούς στο NLRI πεδίο.

Multi_Exit_Disc: Χρησιμοποιείται για την επιλογή ενός BGP router, όταν υπάρχουν περισσότεροι από ένα που συνδέονται με το γειτονικό αυτόνομο σύστημα.

Local_Pref: Χρησιμοποιείται από ένα router για να πληροφορήσει άλλους που βρίσκονται στο ίδιο αυτόνομο σύστημα για το βαθμό στον οποίο προτιμά μια συγκεκριμένη διαδρομή. Δεν επηρεάζει routers σε άλλα αυτόνομα συστήματα.

Atomic_Aggregate, Aggregator: Αυτά τα δύο πεδία υλοποιούν την ιδέα της ομαδοποίησης (aggregation) των διαδρομών.

Notification message



Σχήμα 1-9 Ένα BGP Notification μήνυμα

Το Notification μήνυμα στέλνεται όταν υπάρξει κάποιο λάθος. Τα λάθη αυτά μπορεί να είναι:

Message header error: Περιλαμβάνει λάθη συντακτικά και αναγνώρισης ταυτότητας

Open message error: Περιλαμβάνει λάθη συντακτικά και τιμές πεδίων μη αναγνωρίσιμες στο Open μήνυμα. Ακόμη μπορεί να σημαίνει ότι το Hold time που προτάθηκε από τον αποστολέα δεν είναι αποδεκτό.

Update message error: Περιλαμβάνει λάθη στο Update μήνυμα.

Hold timer expired: Αν ένας router δεν έχει λάβει Keepalive ή Update ή Notification μήνυμα μέσα σε χρόνο Hold time τότε το λάθος αυτό στέλνεται και η σύνδεση διακόπτεται.

Finite state machine error: Περιλαμβάνει διάφορα μη προσδοκώμενα λάθη.

Cease: Χρησιμοποιείται από ένα router για να κλείσει μια σύνδεση χωρίς να έχει συμβεί κάποιο λάθος [10].

- **Exchange of routing information**

Η ανταλλαγή routing πληροφορίας από τους BGP routers μπορεί να γίνει αρκετά πολύπλοκη ανάλογα με τις αλλαγές που συμβαίνουν στα κόστη των συνδέσεων στο δίκτυο (το BGP χρησιμοποιεί μια μετρική που ορίζεται από τον διαχειριστή του δικτύου και μπορεί να είναι delay, cost, ταχύτητα, σταθερότητα, αριθμός hops). Παρακάτω δίνεται ένα απλό παράδειγμα με βάση το δίκτυο του σχήματος 1.

Έστω ο router R1 του AS1. Ένας router που υλοποιεί το BGP, υλοποιεί επίσης και ένα interior gateway protocol π.χ. το OSPF. Με τη χρήση του OSPF, ο R1 μπορεί να ανταλλάσσει πληροφορία με τους άλλους routers μέσα στο AS1, να χτίσει την εικόνα της τοπολογίας των υποδικτύων και των routers του AS1, και να σχηματίσει τον routing πίνακα. Μετά μπορεί να στείλει ένα Update μήνυμα στον R5 του AS2, με την εξής πληροφορία:

AS_Path = AS1.
Next Hop = IP διεύθυνση του R1.
NRLI = οι διευθύνσεις των υποδικτύων του AS1.

Το μήνυμα αυτό πληροφορεί τον R5 ότι όλα τα υποδίκτυα του πεδίου NLRI προσπελαύνονται μέσω του R1 και το μόνο AS που διασχίζεται είναι το AS1. Αν υποτεθεί ότι ο R5 έχει ένα γειτονικό BGP router R9 σε ένα άλλο αυτόνομο σύστημα

AS3. Τότε ο R5 θα προωθήσει την πληροφορία που έλαβε από τον R1 στον R9 με ένα νέο Update μήνυμα. Το μήνυμα αυτό περιέχει:

AS_Path = AS2, AS1.
Next Hop = IP διεύθυνση του R5.
NRLI = οι διευθύνσεις των υποδικτύων του AS1.

Το μήνυμα αυτό πληροφορεί τον R9 ότι όλα τα υποδίκτυα του πεδίου NLRI προσπελαύνονται μέσω του R5, διασχίζοντας τα αυτόνομα συστήματα AS2, AS1. Ο R9 πρέπει τώρα να αποφασίσει αν η διαδρομή που έλαβε με το Update μήνυμα είναι η καλύτερη για την προσπέλαση των υποδικτύων του AS1, ή γνωρίζει κάποια καλύτερη. Αν αποφασίσει ότι είναι καλύτερη, ενημερώνει την βάση δεδομένων του και στέλνει ένα Update μήνυμα στους άλλους γείτονές του. Το μήνυμα αυτό περιέχει:

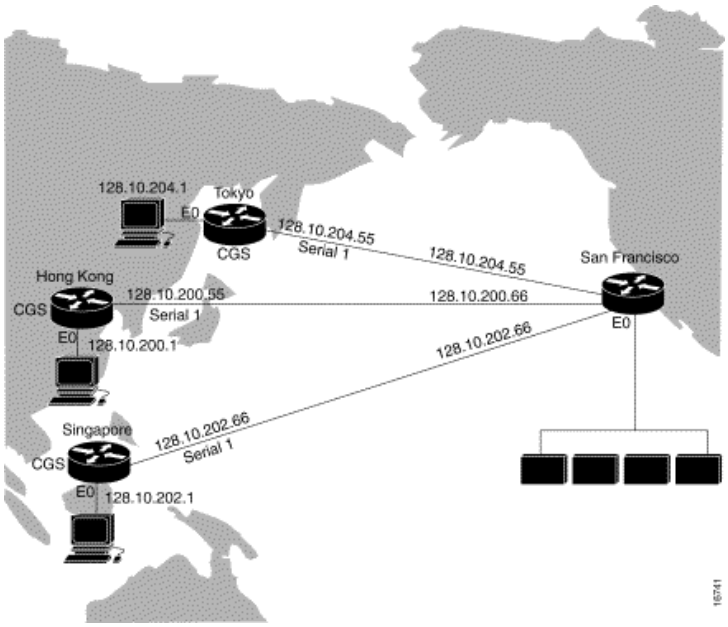
AS_Path = AS3,AS2, AS1.
Next Hop = IP διεύθυνση του R9.
NRLI = οι διευθύνσεις των υποδικτύων του AS1.

Το παραπάνω παράδειγμα είναι απλό και δεν καλύπτει όλη τη λειτουργία του BGP. Μερικές φορές μπορεί και routers μέσα στο ίδιο AS να ανταλλάζουν BGP μηνύματα (εσωτερικοί γείτονες). Σε αυτή την περίπτωση το AS_Path μένει κενό. Ακόμη όταν ένας router επιλέξει μια νέα καλύτερη διαδρομή για κάποιον εξωτερικό προορισμό στέλνει αυτή τη διαδρομή σε όλους τους εσωτερικούς του γείτονες. Ο καθένας από αυτούς μετά αποφασίζει αν αυτή είναι καλύτερη διαδρομή. Αν είναι, προστίθεται στη βάση δεδομένων του και ένα νέο Update μήνυμα στέλνεται.

Αν υπάρχουν πολλά σημεία εισόδου (BGP routers) σε ένα AS και αυτά είναι διαθέσιμα σε ένα BGP router ενός άλλου AS, το πεδίο Multi_Exit_Disc χρησιμοποιείται για να επιλεχθεί ένα από αυτά. Αυτό περιέχει μια μετρική για την προσπέλαση κάποιου προορισμού στο AS. Για παράδειγμα έστω ότι οι R1, R2 υλοποιούν το BGP και συνδέονται με σχέση γειτονικότητας με τον R5. Ο καθένας από αυτούς στέλνει Update μηνύματα στον R5 σχετικά με το υποδίκτυο 1.3, η οποία περιέχει και κάποια μετρική δρομολόγησης που χρησιμοποιείται εσωτερικά στο AS1, π.χ. τη μετρική που χρησιμοποιεί το OSPF. Ο R5 μπορεί να χρησιμοποιήσει αυτές τις δύο μετρικές για να αποφασίσει μεταξύ των δύο.

Κεφάλαιο 2

Dial-on-Demand Routing (DDR)



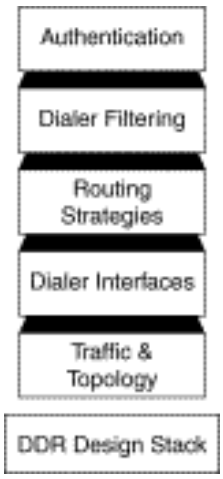
2.1 Εισαγωγή

Η Dial-on-Demand Routing (DDR) αποτελεί μια σχετικά καινούργια τεχνική δρομολόγησης όπου ένας δρομολογητής μπορεί δυναμικά να διαχειριστεί την έναρξη και τον τερματισμό circuit-switched περιόδων λειτουργίας (sessions) για την κατα παραγγελία (on-demand) παροχή υπηρεσιών.Οι περίοδοι αυτοί λειτουργίας υλοποιούνται μέσω του δημόσιου τηλεφωνικού δικτύου (PSTN).Ο δρομολογητής (router) διαμορφώνεται με τέτοιο τρόπο ώστε να θεωρεί κάποια συγκεκριμένη κίνηση (traffic) ως «ενδιαφέρουσα» (π.χ την κίνηση ενος συγκεκριμένου πρωτόκολου) και όλες τις άλλες ώς «αδιάφορες».Πρωτόκολλα όπως τα IP, Novell IPX , X.25 , Frame Relay και SMDS μπορούν να χρησιμοποιηθούν για την επιλογή της «ενδιαφέρουσας» κίνησης.Μόλις ο δρομολογητής λάβει ένα πακέτο και αποφανθεί οτι αυτό είναι ενα «ενδιαφέρον» πακέτο τοτε αποκαθίσαται μια τηλεφωνική σύνδεση με το δίκτυο προορισμού όπως αυτό αναφέρεται στο πακέτο.Αν κατα τη διάρκεια αυτή ο δρομολογητής λάβει ένα «αδιάφορο» πακέτο τότε και αυτό το πακέτο μεταδίδεται.[11],[12].

2.2 Το DDR Μοντέλο

Αν και η DDR δεν αποτελεί κατ'ουσία μια αρχιτεκτονική δικτύου παρ'ολα αυτά για την καλύτερη κατανόηση της η εταιρεία Cisco εισήγαγε ένα μοντέλο σχεδίασης (όμοιο με αυτό του OSI)που περιγράφει τα δίκτυα DDR και βοηθά τους σχεδιαστές δικτύων στην υλοποίηση τους. Μια προσέγγιση αυτού του μοντέλου παρουσιάζεται εποπτικά στην παρακάτω εικόνα [12].

Εικόνα 2-1: Το DDR μοντέλο



2.2.1 DDR Dialer Clouds

Το δίκτυο που αποτελείται απο όλες τις διασυνδεμένες DDR συσκευές (devices) γενικά αποκαλείται «σύννεφο καλούντων» (dialer cloud) .

Τα Dialer clouds είναι η συλλογή τόσο των ενεργών (σημείο προς σημείο (point-to-point) οσο και των δυνιτικών συνδέσεων και επιρεάζουν τη σχεδίαση του DDR σε κάθε του στάδιο. [13]

2.2.2 Traffic και Τοπολογία (Topology) του DDR

Το πιο σημαντικό κριτίριο επιλογής της τοπολογίας που θα χρησιμοποιήσει κανεις είναι θα πρέπει να είναι ο αριθμός των θέσεων - δρομολογητών (sites) που θα υποστηριχθούν. Αν οι θέσεις αυτές είναι δυο τότε επιλέγεται η τοπολογία point-to-point topology. Αν οι θέσεις είναι περισσότερες τότε συνήθως επιλέγεται η τοπολογία hub-and-spoke. Για μικρό αριθμό θέσεων με μικρό φόρτο κίνησης η τοπολογία fully meshed topology ίσως αποτελεί την καλύτερη επιλογή.

Οι τοπολογίες του DDR είναι:

- Point-to-point
- Fully meshed
- Hub-and-spoke

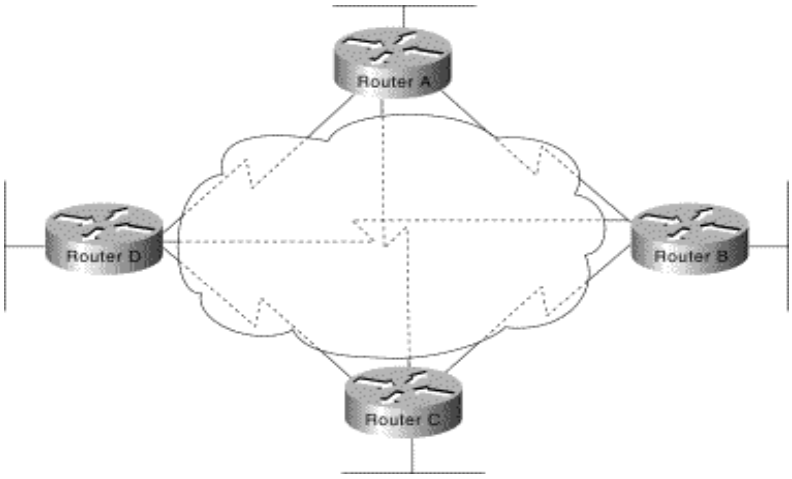
Point-to-Point Topology

Στην τοπολογία point-to-point (Εικόνα 2-2) οι δύο δρομολογητές αλληλοσυνδέονται και αντιστοιχούν ο καθένας απο τη μεριά του τις διευθυνσεις του άλλου σε ένα τηλεφωνικό νούμερο.Αν απαιτείται περισσότερο bandwidth τότε μπορούν να επιτευχθούν πολλαπλές συνδέσεις με τη χρήση Multilink PPP.

Εικόνα 2-2: Point-to-point topology.

Fully Meshed Topology

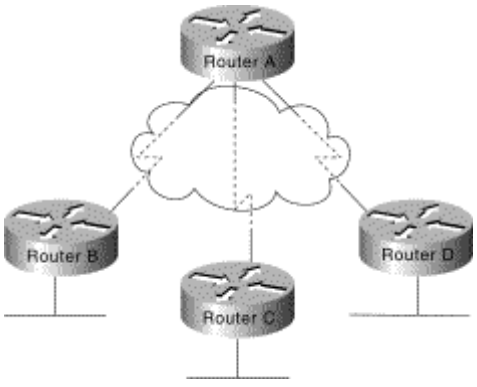
Στις fully meshed τοπολογίες ο κάθε δρομολογητής έχει απευθείας πρόσβαση στους υπόλοιπους δρομολογητές (any-to-any connectivity) του δικτύου τους οποίους μπορεί να καλέσει χωρίς τη βοήθεια κάποιου ενδιάμεσου σταθμου (Εικόνα 2-4)



Εικόνα 2-4 : Fully meshed τοπολογία

Hub-and-Spoke DDR τοπολογία

Στην τοπολογία hub-and-spoke (βλ.Εικόνα 2-5), ένας κεντρικός δρομολογητής είναι συνδεδεμένος με αρκετούς άλλους απομακρυσμένους δρομολογητές . Οι απομακρυσμένοι δρομολογητές επικοινωνούν απευθείας με τον κεντρικό και δεν επικοινωνούν μεταξύ τους όπως στην προηγούμενη τοπολογία. [13]



Εικόνα 2-5: Hub-and-spoke τοπολογία

2.3 Υπηρεσία Κλήσης

Τα μέσα για την επίτευξη μιας DDR σύνδεσης είναι προσβάσιμα μέσω της ιδιότητας «διασύνδεση καλούντος». Οι δρομολογητές μπορούν να υποστηρίξουν ISDN B κανάλια (channels), σύγχρονες σειριακές διεπαφές (Synchronous Serial interfaces) καθώς και ασύγχρονες σαν τέτοιες διεπαφές.

2.3.1 Υποστηριζόμενες φυσικές διεπαφές.

- ISDN Interfaces
- Synchronous Serial Interfaces
- Asynchronous Modem Connections

2.3.2 Μέθοδοι ενθυλάκωσης

Οι μέθοδοι ενθυλάκωσης (encapsulation methods) που είναι διαθέσιμοι εξαρτώνται απο τη φυσική διεπαφή που έχει επιλεγχθει προηγουμένως.

Point-to-Point Protocol (PPP)

Το πρωτοκολλο PPP είναι η κατάλληλη μέθοδος encapsulation γιατί υποστηρίζει πολλαπλά πρωτόκολλα και χρησιμοποιείται για σύγχρονες , ασύγχρονες και ISDN συνδέσεισand .

High-Level Data Link Control (HDLC)

Το HDLC υποστηρίζεται μόνο απο τις συνδέσεις σύγχρονων σειριακών γραμμών και τις συνδέσεις ISDN . Το HDLC υποστηρίζει πολλαπλά πρωτόκολλα. Δε διαθέτει όμως μηχανισμούς πιστοποίησης.

Serial Line Interface Protocol (SLIP)

Το πρωτόκολλο SLIP δουλεύει μόνο στις ασύγχρονες συνδέσεις και υποστηρίζεται μόνο απο το IP , οι διευθύνσεις πρέπει να ρυθμιστούν και δε διαθέτει μηχανισμούς πιστοποίησης.

X.25

Το X.25 υποστηρίζεται μόνο απο τις συνδέσεις σύγχρονων σειριακών γραμμών και απο τις συνδέσεις απλών ISDN B καναλιών.[13]

2.3.3 Dialer rotary groups

Πολλαπλές DDR διεπαφές μπορούν να συνδιαστούν ωστε να αποτελέσουν a dialer rotary group. Οι τοπολογίες hub-and-spoke και fully meshed μπορούν να εκμεταλευθούν αυτή τη δυνατότητα. Η DDR υποστηρίζει το συνδιασμό διαφορετικών φυσικών διεπαφών , δίνοντας τη δυνατότητα σε μια φυσική διεπαφή να είναι απασχολημένη ενω μια άλλη να θέτει μια σύνδεση.

2.3.4 Dialer profiles

Χρησιμοποιώντας αυτά τα προφίλ (profiles) ξεχωρίζεται το λογικό απο το φυσικό επίπεδο κάτι που προσθέτει σχεδιαστική ευελιξία. Η ιδιότητα αυτή επιτρέπει σε πολλαπλές διεπαφές να χρησιμοποιούν το ίδιο προφιλ ταυτόχρονα .

2.3.4.1 Addressing Dialer Clouds

Υπάρχουν δύο τρόποι διευθυνσιοδότησης στα dialer clouds :

Χρήση υποδικτύων στο dialer cloud

Κάθε δρομολογητής που είναι συνδεδεμένος στο dialer cloud παίρνει μια μοναδική διεύθυνση κόμβου σε ένα κοινό υποδίκτυο για να το χρησημοποιήσει στο δικό του dialer interface.

Χρήση μη αριθμημένων διασυνδέσεων

Οπως και στην περίπτωση χρήσης μη αριθμημένων διασυνδέσεων στις μισθωμένες γραμμές και στις διασυνδέσεις point-to-point , η διευθυνση ενος άλλου interface στο router δανείζεται για να χρησιμοποιηθεί στο dialer interface. Η μέθοδος αυτή εκμεταλεύεται το γεγονός οτι υπάρχουν μόνο δυο συσκευές στη point-to-point σύνδεση. Ο πίνακας δρομολόγησης (routing table) δείχνει σε ένα interface (the dialer interface) και σε μια next-hop διευθυνση (η οποία πρέπει να ταιριάζει σε ενα dialer map: στατικά ή δυναμικά).

Dialer Maps

Κατά την διαδικασία αυτή μεταφράζονται οι next-hop διευθύνσεις σε τηλεφωνικά νούμερα. [13]

2.4 Στρατηγικές Δρομολόγησης (Routing Strategies)

Στα DDR δίκτυα η δρομολόγηση καθώς και κάποια directory services tables πρέπει να τυγχάνουν διαχείρισης ακόμα και όταν δεν υπάρχει δραστηριότητα. Οι DDR σχεδιαστές μπορούν να χρησιμοποιήσουν τεχνικές στατικής , δυναμικής ή δρομολόγησης στιγμυότυπου (snapshot) καθώς και συνδιασμό αυτών.

Στατική Δρομολόγηση (Static Routing)

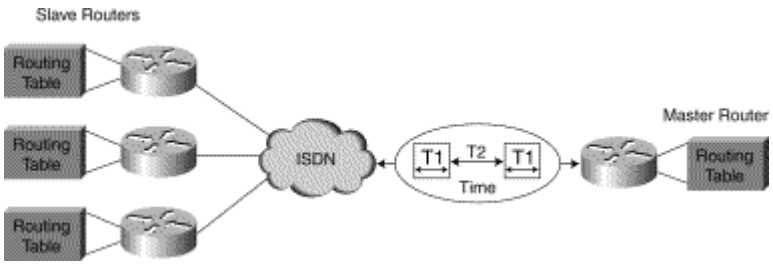
Στη στατική δρομολόγηση οι διευθύνσεις εισάγονται απο τους σχεδιαστές και με τον τρόπο αυτό δεν υπάρχει ο λόγος ανταλλαγής ενημερώσεων (updates) απο το πρωτόκολλο δρομολόγησης σε μια DDR σύνδεση. Αυτού του τύπου η δρομολόγηση αποδυκνείεται αποτελεσματοκή σε μικρού μεγέθους δίκτυα που δεν αλλάζουν συχνα.

Δυναμική Δρομολόγηση (Dynamic Routing)

Τα δυναμικά πρωτόκολλα δρομολογησης είναι RIP,RIP2,EIGRP,IGRP και OSPF.Οταν χρησιμοποιούνται τα πρωτόκολλα αυτά οι ανανεώσεις δρομολόγησης (routing updates) ανταλάσονται μεταξύ των DDR δρομολογητών μόλις μιά DDR σύνδεση επιτευχθεί.

Snapshot Δρομολόγηση

Η Snapshot δρομολόγηση χρησιμοποιεί το μοντέλο client-server . Ο server και οι clients ανταλλάσουν πληροφορίες δρομολόγησης στη διάρκεια μιας ενεργής περιόδου. Σρην αρχή αυτής , ο client router καλεί τον server router για να ανταλαξουν πληροφορίες. Στο τέλος της ενεργής περιόδου κάθε δρομολογητής παίρνει ένα στιγμυότυπο (snapshot) των εγγραφών του routing table. Οι εγγραφές αυτές παραμένουν παγωμένες κατα τη διάρκεια της ύσηχης περιόδου. Στο τέλος της περιόδου αυτή μια άλλη ενεργή περίοδος αρχίζει και ο client router καλεί τον server router για να αποκτήσει τις τελευταιές πληροφορίες δρομολόγησης. [12]

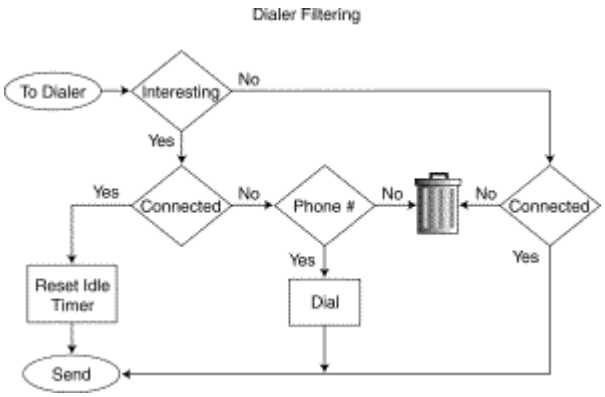


Εικόνα 2-6: Snapshot δρομολόγηση

2.5 Dialer Filtering

Dialer filtering (δες Εικόνα 2-7) χρησιμοποιείται για να πιστοποιήσει όλα τα πακέτα που διατρέχουν μια DDR σύνδεση είτε ως «ενδιαφέροντα» είτε ως «αδιάφορα» χρησιμοποιώντας Λίστες Ελέγχου Πρόσβασης (Access Control Lists (ACLs)). Μόνο τα «ενδιαφέροντα» πακέτα μοπορύν να ενεργοποιήσουν και να διατηρήσουν μία DDR σύνδεση. Κύριο μέλημα των σχεδιαστών μιας DDR υλοποίησης είναι να αποφανθούν ποιά πακέτα θα χαρακτηρίσουν ώς «αδιάφορα» και να αναπτύξουν τις κατάλληλες ACLs για να τα εμποδίσουν να δημιουργούν ανεπιθυμητες DDR συνδέσεις.

Αν ένα πακέτο είναι «αδιάφορο» και δεν υπάρχει κάποια ενεργή σύνδεση το πακέτο απορρίπτεται. Αν το πακέτο είναι «αδιάφορο» αλλά υπάρχει μια ενεργή σύνδεση τότε το πακέτο αποστέλλεται αλλά ο χρόνος αναμονής δεν μηδενίζεται. Αν το πακέτο είναι «ενδιαφέρον» και δεν υπάρχει σύνδεση διαθέσιμη ο δρομολογητής θα επιχειρίσει να αποκαταστήσει μια.



Εικόνα 2-7: Dialer filtering

2.8 Πιστοποίηση

Η πιστοποίηση σε ένα DDR δίκτυο παρέχει δύο λειτουργείες : την ασφάλεια και την dialer state. Μιας και τα DDR δίκτυα συνδέονται στο PSTN , το θέμα της ανάπτυξης ενος καλού μοντέλου ασφάλειας που θα αποτρέπει την μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες κρίνεται πρωταρχικής σημασίας. Επίσης υπάρχει η δυνατότητα να γνωρίζουμε κάθε στιγμή ποιοι δρομολογητές είναι συνδεδεμένοι.Ας δούμε μερικές επιλεγμένες μεθόδους.

PPP Πιστοποίηση

Η PPP πιστοποίηση μέσω CHAP ή PAP πρέπει να χρησιμοποιείται για να παρέχεται ασφάλεια στις DDR συνδέσεις. Η PPP πιστοποιήση πραγματοποιείται σαν μια is negotiated as an LCP option, και είναι αμφίδρομη ,δηλαδή κάθε πλευρά μπορεί να πιστοποιήσει την άλλη.

ISDN Security

Οι ISDN DDR συνδέσεις μπορούν να χρησιμοποιούν την αναγνώριση κλήσης (caller-ID) για την παροχή αυξημένου επιπέδου ασφάλειας. Οι εισερχόμενες κλήσεις φιλτράρονται για να διαπιστωθεί αν προέρχονται απο κάποια αναμενόμενη περιοχή.

2.9 Περίληψη

Οταν πρόκειται να σχεδιάσουμε ένα DDR internetwork, θα πρέπει να αποφασίσουμε τον τύπο της τοπολογίας που θα χρησιμοποιήσουμε: point-to-point, hub-and-spoke, and fully meshed. Με τον τύπο της τοπολογίας στο μυαλό θα σκεφτούμε τη μέθοδο διευθυνσηιοδότησης που θα χρησιμοποιήσουμε και τα θέματα ασφαλείας. Η επόμενη απόφαση μας θα πρέπει να είναι η μέθοδος δρομολόγησης (δυναμική ή στατική) και το πως τα πακέτα θα φτάνουν στον προορισμό τους (αντιστοίχιση διευθύνσεων σε τηλεφωνικά νούμερα). Τελικως η σημαντικότερη απόφαση που θα πρέπει κάποιος σχεδιαστής δικτύου να πάρει είναι να καθορίσει τα «ενδιαφέροντα» και τα «αδιάφορα» πακέτα.

Κεφάλαιο 3

3.1 Distance Vector Multicast Routing Protocol

Τα πρωτόκολλα Distance Vector επιλέγουν τη δρομολόγηση με βάση το κόστος που έχουν οι διπλανοί δρομολογητές. Στις περισσότερες περιπτώσεις το κόστος είναι η απόσταση ενός δρομολογητή με τον άλλον, τα λεγόμενα hops. Αυτή η πληροφορία παρέχεται από τους συγκοινωνούντες δρομολογητές. Η τεχνική αυτή βασίζεται στον αλγόριθμο Bellman-Ford. Ένα πολύ διαδεδομένο πρωτόκολλο τύπου Distance Vector είναι το RIP (Routing Information Protocol).

Οι δρομολογητές ανταλλάσσουν μεταξύ τους πληροφορίες περίπου κάθε τριάντα λεπτά. Από αυτές τις πληροφορίες δημιουργούν τις βάσεις δεδομένων στις μνήμες τους οι οποίες αντιστοιχούν σε στοιχεία όπως οι IP διευθύνσεις , τα λεγόμενα metrics, τις «πόρτες» των διπλανών δρομολογητών. [14]

Το multicast είναι ένας τρόπος να μεταδίδονται δεδομένα όπως κείμενο, ήχος και εικόνα στο Internet ή σε ένα τοπικό δίκτυο σε έναν ορισμένο αριθμό ατόμων. Αντί ο αποστολέας να στέλνει ξεχωριστά τα δεδομένα σε κάθε παραλήπτη, ένα μόνο μήνυμα στέλνεται κάθε φορά σε μια ομάδα παραληπτών που αποτελούν το λεγόμενο multicast group. Με άλλα λόγια, το multicasting είναι μια μορφή επικοινωνίας «ένας προς πολλούς». Σε αντίθεση, ο παραδοσιακός τρόπος μετάδοσης δεδομένων στο Internet ονομάζεται unicast και είναι ένας τρόπος μετάδοσης «ένας προς έναν». [15]

Το πρωτόκολλο Distance Vector Multicast Routing Protocol είναι ένα από τα πρώτα multicast πρωτόκολλα που εμφανίστηκαν στο Internet. Η κύρια λειτουργία του είναι να επιτρέπει δρομολογητές που είναι «multicast aware» να ανταλλάσσουν πληροφορίες δρομολόγησης μεταξύ τους. Το DVMRP μοιάζει πολύ με το RIP αλλά έχει περισσότερες λειτουργίες οι οποίες έχουν να κάνουν με το multicast. Ουσιαστικά αυτό που κάνει το πρωτόκολλο είναι να μεταφέρει πληροφορίες για να multicast groups και το κόστος που έχει η μεταφορά των δεδομένων από δρομολογητή σε δρομολογητή. Οι δρομολογητές κατασκευάζουν στη μνήμη τους μια τοπολογία δέντρου. Έτσι, όταν φτάνει σε έναν δρομολογητή μια πληροφορία multicast αυτός στέλνει ένα αντίγραφο σε όλους τους δρομολογητές αυτής της τοπολογίας. [16]

Το πρωτόκολλο DVMRP είναι αρκετά παλιό και πλέον δεν χρησιμοποιείται. Στη θέση του υπάρχουν πιο εξελιγμένα πρωτόκολλα όπως το MBGP που έχει όλα τα χαρακτηριστικά του γνωστού πρωτοκόλλου BGP και προσφέρει υπηρεσίες multicast.

Κεφάλαιο 4

Το πρωτόκολλο PIM (Protocol Independent Multicast).

4.1 Εισαγωγή

Το Protocol Independent Multicast (PIM) είναι ένα πρωτόκολλο δρομολόγησης που αναπτύχθηκε από την Inter-Domain Multicast Routing (IDMR) που είναι ομάδα εργασίας του οργανισμού Internet Engineering Task Force. Σκοπός της IDMR ήταν να αναπτύξει ένα πρωτόκολλο δρομολόγησης πολλαπλής εκπομπής (multicast) το οποίο να μπορεί να προσφέρει κλιμακωτή δρομολόγηση μέσα στο διαδίκτυο (Internet). Το PIM σχεδιάστηκε έτσι ώστε να διορθώσει τα προβλήματα κλιμάκωσης στην δρομολόγηση που παρουσιάζει το Distance-Vector Multicast Routing Protocol (DVMRP)όπως και τα προβλήματα στην απόδοση των Core-Based Trees (CBT). [17]

Το PIM ονομάζεται έτσι λόγω του γεγονότος ότι δεν εξαρτάται από τους μηχανισμούς που προσφέρονται από κάποιο συγκεκριμένο πρωτόκολλο απλής (unicast) δρομολόγησης (σε αντίθεση π.χ. με το DVMRP το οποίο έχει ενσωματωμένο ένα πρωτόκολλο απλής δρομολόγησης). Ωστόσο οποιαδήποτε υλοποίηση χρησιμοποιεί το PIM απαιτεί την ύπαρξη ενός πρωτοκόλλου απλής δρομολόγησης (ή ενός συνόλου αυτών) για να προσφέρει πληροφορίες για τον πίνακα δρομολόγησης και για την προσαρμογή σε αλλαγές της τοπολογίας. Οποιοσδήποτε συνδυασμός πρωτοκόλλων απλής δρομολόγησης είναι επαρκής για τον σκοπό αυτό, όπως : OSFP, Integrated IS-IS, RIPv1, RIPv2, BGP-4, IGRP, E-IGRP κ.α.

Το PIM έχει δύο βασικές υλοποιήσεις:

1) PIM – DENSE MODE (PIM –DM)
2) PIM – SPARSE MODE (PIM – SM)

Παρόλο που αυτές οι δύο υλοποιήσεις έχουν το ίδιο όνομα και έχουν συσχετιζόμενα μηνύματα ελέγχου, είναι ανεξάρτητες μεταξύ τους. Η πρώτη υλοποίηση υποστηρίζει την υποστήριξη πυκνής δρομολόγησης σε ορισμένες ομάδες πολλαπλής εκπομπής και η δεύτερη την υποστήριξη αραιής δρομολόγησης σε ομάδες πολλαπλής εκπομπής.

4.2 Το πρωτόκολλο PIM – Dense Mode (PIM – DM).

Όταν μιλάμε για υποστήριξη πυκνής δρομολόγησης δεν εννοούμε έναν μεγάλο αριθμό από παραλήπτες (Group Members), αλλά ένα επιχειρησιακό πεδίο όπου στο οποίο οι Group Members καταλαμβάνουν ένα μεγάλο κλάσμα των διαθεσίμων υποδικτύων.[18]

Παρόλο που η αρχιτεκτονική του πρωτοκόλλου PIM οδηγήθηκε αρχικά από την ανάγκη για ένα πρωτόκολλο που θα παρείχε αποδοτικά, κλιμακωτά δέντρα μεταβίβασης για αραιή δρομολόγηση (scalable sparse-mode delivery trees), (κυρίως για να εφαρμοστεί πάνω σε δίκτυα ευρείας περιοχής -WAN's- , τα οποία απαιτούν μεγάλη αποδοτικότητα), το PIM, επίσης προσδιόρισε ένα καινούριο πρωτόκολλο πυκνής δρομολόγησης. Απώτερος σκοπός ήταν το PIM-DM να εφαρμοσθεί πάνω σε περιβάλλοντα πλούσια σε πόρους, όπου οι Group Members καταλαμβάνουν ένα μεγάλο ποσοστό των υποδικτύων και υπάρχει μεγάλο εύρος ζώνης διαθέσιμο. Σύμφωνα με τον σχεδιασμό τους τα μηνύματα ελέγχου (control messages) είναι τα ίδια για το PIM-DM και το PIM-SM.

Το PIM-DM είναι βασισμένο στον αλγόριθμο του ανάστροφου μονοπατιού για το multicast (Reverse Path Multicast -RPM- algorithm) όπως και το DVMRP v3. Αξιοπρόσεκτη είναι η απουσία ενός ενσωματωμένου πρωτοκόλλου δρομολόγησης unicast το οποίο χρησιμοποιείται για την χρησιμοποίηση του πίνακα δρομολόγησης έτσι ώστε να μπορούν να γίνουν οι έλεγχοι για την διάδοση στο αντίστροφο μονοπάτι (Reversed-Path Forwarding –RPF- check).

Το PIM-DM χρησιμοποιεί ένα απλό μοντέλο ώθησης της πολλαπλά εκπεμπόμενης κυκλοφορίας (multicast traffic), σε όλα τα σημεία του δικτύου, έως ότου συγκεκριμένα μηνύματα αποκοπής του Group Member από το δέντρο μεταβίβασης φτάσουν στον αποστολέα. Αυτή είναι μια βίαιη μέθοδος μεταβίβασης των δεδομένων στους παραλήπτες, αλλά σε συγκεκριμένες εφαρμογές αυτό μπορεί να

αποδειχθεί ένας αποτελεσματικός μηχανισμός εάν υπάρχουν ενεργοί παραλήπτες σε κάθε υποδίκτυο (subnet) στο δίκτυο. Το PIM-DM αρχικά κατακλύζει το δίκτυο με την multicast κυκλοφορία. Οι δρομολογητές που δεν έχουν στην κατεύθυνση διάδοσης της κυκλοφορίας γειτονικούς δρομολογητές που να χρειάζονται την κυκλοφορία, τους αποκόβουν από το δέντρο μεταβίβασης λαμβάνοντας ένα μήνυμα αποκοπής (Prune Message) το οποίο ισοδυναμεί με ένα λάθος στον RPF έλεγχο. Όταν ένας δρομολογητής θέλει να συνεχίσει να συμμετάσχει στο δέντρο μεταβίβασης αποστέλλει ένα μήνυμα ένωσης (Join Message) το οποίο ισοδυναμεί με επιτυχία του RPF ελέγχου. Αυτή η διαδικασία επαναλαμβάνεται κάθε 3 λεπτά.[18],[20]

Για τις περιπτώσεις όπου παραλήπτες εμφανίζονται ξαφνικά σε ένα προηγουμένως αποκομμένο κλαδί του δέντρου μεταβίβασης, το PIM-DM, κατέχει μηνύματα επανένωσης του παραλήπτη, στο δέντρο μεταβίβασης.

Με αυτόν τον μηχανισμό διάδοσης και αποκοπής οι δρομολογητές αντιλαμβάνονται την κατάσταση τους λαμβάνοντας το ρεύμα των δεδομένων. Αυτό το ρεύμα δεδομένων περιέχει την απαραίτητη πληροφορία για τον αποστολέα και τον παραλήπτη των δεδομένων έτσι ώστε οι δρομολογητές που διαδίδουν στους γειτνιάζοντες δρομολογητές δεδομένα να μπορούν να δημιουργήσουν τους δικούς τους πίνακες διάδοσης της εκπεμπόμενης πληροφορίας.

Το PIM-DM μπορεί να υποστηρίξει μόνο πηγαία δέντρα (source trees – (S,G) entries) και δεν μπορεί να χρησιμοποιηθεί για την δημιουργία ενός διαμοιραζόμενου κατανεμημένου δέντρου.

4.3 Το πρωτόκολλο PIM – Sparse Mode (PIM – SM).

Το πρωτόκολλο PIM-SM αναπτύχθηκε για να προσφέρει ένα πρωτόκολλο πολλαπλής εκπομπής (multicast protocol) το οποίο να προσφέρει αποδοτική επικοινωνία μεταξύ μελών ομάδων που είναι αραιά κατανεμημένες, τον τύπο των ομάδων δηλαδή που συναντάμε συνήθως σε δίκτυα ευρείας περιοχής (WAN). Οι σχεδιαστές του παρατήρησαν καταστάσεις κατά τις οποίες διάφοροι οικοδεσπότες (hosts) που επιθυμούσαν να συμμετάσχουν σε μια σύσκεψη πολλαπλής εκπομπής (multicast conference) δεν είναι θεμιτό να κατακλύζουν όλο το δίκτυο με περιοδικά

εκπεμπόμενη πληροφορία προς όλους τους συμμετέχοντες. Υπήρχε ο φόβος ότι με τα υπάρχοντα πρωτόκολλα δρομολόγησης πολλαπλής εκπομπής θα παρουσιάζονταν προβλήματα κλιμάκωσης εάν γινόταν πολλές μικρές συσκέψεις, δημιουργώντας μεγάλους όγκους συνολικά αθροιζόμενης κυκλοφορίας, η οποία ενδεχομένως να δημιουργούσε σοβαρά προβλήματα στις περισσότερες συνδέσεις μέσω WAN στο διαδίκτυο. Για να καταπολεμηθούν αυτά τα ενδεχόμενα προβλήματα κλιμάκωσης σχεδιάστηκε το PIM-SM. Το PIM-SM, περιορίζει την κυκλοφορία κατά τέτοιο τρόπο ώστε μόνο όσοι δρομολογητές ενδιαφέρονται στο να παραλάβουν κυκλοφορία για μια συγκεκριμένη ομάδα να την «βλέπουν». [19]

Το PIM-SM διαφέρει από τα υπάρχοντα πρωτόκολλα πολλαπλής εκπομπής σε δύο σημαντικά σημεία:

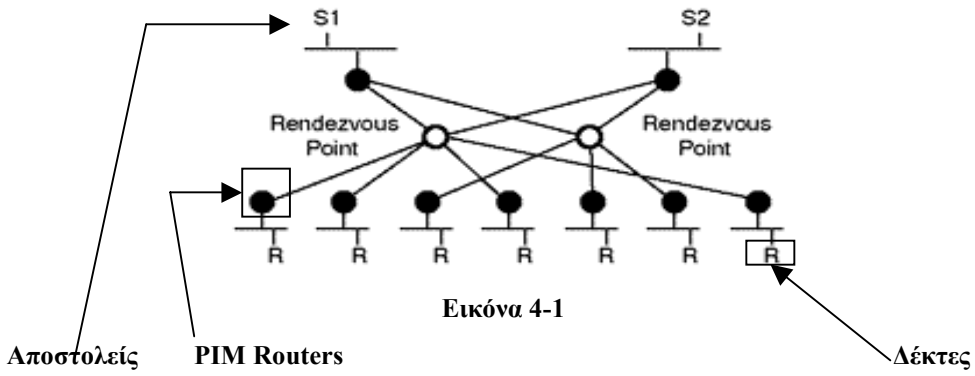
- Το PIM-SM δημιουργεί κοινόχρηστα δέντρα μεταβίβασης της κυκλοφορίας με τα οποία πρέπει να ενωθούν οι δρομολογητές που βρίσκονται στην κατεύθυνση διάδοσης της κυκλοφορίας.

  Δρομολογητές με παρακείμενα μέλη ομάδων είναι υποχρεωμένοι να ενωθούν στο δέντρό μεταβίβασης της πληροφορίας μεταδίδοντας ένα μήνυμα ένωσης τους (Join Message) σε ένα σημείο που ονομάζεται «σημείο συνάντησης» (Rendezvous Point). Ένα ένας δρομολογητής δεν έχει ενωθεί στο δέντρο μεταβίβασης όταν μέχρις ότου αρχίσει η μετάδοση των δεδομένων δεν μπορεί να παραλάβει καμιά κυκλοφορία η οποία απευθύνεται στην ομάδα.

  Η προκαθορισμένη ενέργεια διαβίβασης ενός ενδεχομένου-ένωσης πρωτοκόλλου είναι η αποστολή όλης της κυκλοφορίας από τον αποστολέα προς όλους (π.χ. PIM-DM και DVMRP), ενώ ενός πρωτοκόλλου αραιής δρομολόγησης είναι να στείλει την κυκλοφορία εκεί ακριβώς που ζητήθηκε.

- Το PIM-SM αποτελεί μια εξέλιξη της προσέγγισης των δέντρων βασισμένων σε πυρήνα (CBT Trees –Core Based Trees-) αφού χρησιμοποιείται η ιδέα ενός πυρήνα όπου οι παραλήπτες «συναντούν» τους αποστολείς των δεδομένων (RP –Rendezvous Points- στην ορολογία του PIM-SM).

Όταν πρόκειται για συνένωση σε μια ομάδα, ο δέκτης χρησιμοποιεί το IGMP (Internet Group Management Protocol) για να ειδοποιήσει τον δρομολογητή στον οποίο είναι άμεσα συνδεμένος, ο οποίος δρομολογητής με την σειρά του στέλνει ένα σαφές μήνυμα ένωσης (PIM Join Message) στο RP της ομάδας για να συμπεριληφθεί στο δέντρο διαβίβασης της κυκλοφορίας. Ο δρομολογητής του αποστολέα ξέρει πώς να προωθήσει την πληροφορία στο RP, και αφού μεταφερθεί εκεί η κυκλοφορία αυτή προωθείται σε όλα τα μέλη της ομάδος. (Εικόνα 4-1).

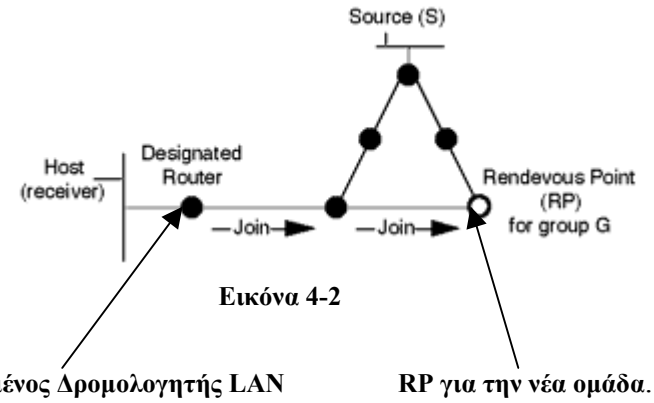


Εικόνα 4-1

Αυτό το μοντέλο προϋποθέτει πως κάθε PIM δρομολογητής θα πρέπει εκτός από μια κατάσταση των μελών που θα προωθήσει την κυκλοφορία, να έχει και μια κατάσταση με εναλλακτικά RP's. Για κάθε ομάδα υπάρχει μόνο ένα ενεργό κάθε φορά RP. Ο αποστολέας χρησιμοποιεί το RP επίσης για να γνωστοποιήσει την παρουσία του στους αποδέκτες και να ενωθούν άμα ενδιαφέρονται στην ομάδα που θα παραλάβει τα δεδομένα. Άμα συμβεί ένα συμβάν αποτυχίας σύνδεσης με το RP, δημιουργείται μια νέα κατάσταση η οποία δεν συμπεριλαμβάνει το συγκεκριμένο RP. Αν υπήρχε μόνο ένα μόνο RP στην κατάσταση τότε η επικοινωνία των μελών της ομάδας δεκτών, δεν είναι δυνατή. Για αυτό τον λόγο χρησιμοποιείται και η κατάσταση των RP's η οποία αυξάνει την αξιοπιστία του πρωτοκόλλου.

Όταν περισσότεροι από ένας PIM δρομολογητές είναι ενωμένοι σε ένα πολλαπλής πρόσβασης τοπικό δίκτυο, ο δρομολογητής με την υψηλότερη IP

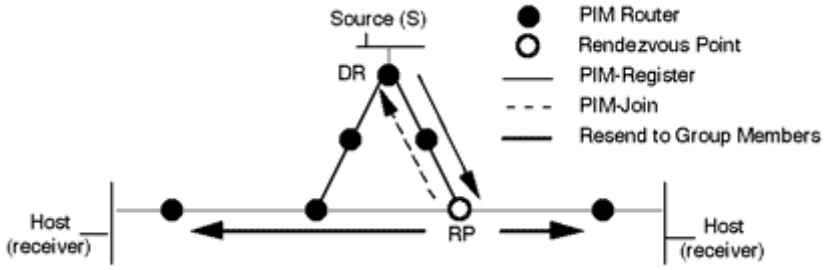
διεύθυνση επιλέγεται σαν ο ορισμένος δρομολογητής για το τοπικό δίκτυο (Designated Router –DR-). Ο DR είναι αυτός που αποστέλλει τα σήματα ένωσης-αποκοπής (Join-Prune messages) για το τοπικό δίκτυο. Όταν λαμβάνεται ένα σήμα αναφοράς για μια καινούρια ομάδα (IGMP Host Membership Report Message) ο DR, εκτελεί μια διαδικασία για να οριστεί μοναδικά το RP για την καινούρια αυτή ομάδα και αποστέλλει ένα μήνυμα ένωσης στο RP της καινούριας ομάδας. (Εικόνα 4-2)



Εικόνα 4-2

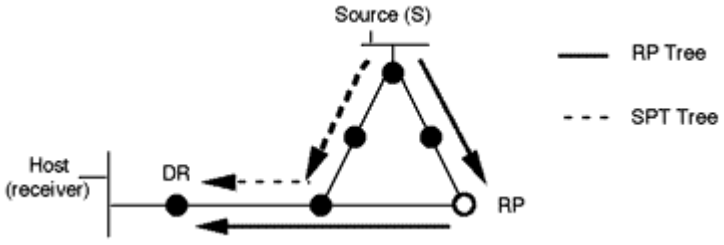
Εκλεγμένος Δρομολογητής LAN **RP για την νέα ομάδα**.

Στην περίπτωση που ένας αποστολέας μεταδίδει ένα πακέτο πολλαπλής εκπομπής σε μια ομάδα, ο DR του αποστολέα πρέπει να προωθήσει το πακέτα στο πρωτεύον (ενεργό) RP για διανομή στο δέντρο μεταβίβασης της ομάδας. Ο DR μαζεύει τα αρχικά πακέτα πολλαπλής εκπομπής του αποστολέα και τα αποστέλλει σαν πακέτα καταχώρησης PIM-SM (PIM-SM Register Packets) μέσω απλής εκπομπής (unicast) στο RP της ομάδας. Αυτή η ενέργεια έχει σαν αποτέλεσμα το RP να αποστείλει ένα μήνυμα ένωσης πίσω στον DR του αποστολέα. Οι δρομολογητές έτσι ανάμεσα στον DR του αποστολέα και το RP ξέρουν πια πώς να δρομολογούν από εδώ και στο εξής τα επόμενα πακέτα από το υποδίκτυο του αποστολέα στο RP της ομάδας και από εκεί στα μέλη που ανήκουν στο δέντρο μεταβίβασης μέσω πακέτων πολλαπλής εκπομπής πια (multicast packets).
(Εικόνα 4-3)



Εικόνα 4-3

Τα κοινόχρηστα δέντρα που χρησιμοποιούνται από τα RP (RP-shared trees) προσφέρουν διασύνδεση για τα μέλη της ομάδας αλλά δεν βελτιστοποιούν το μονοπάτι μεταβίβασης (delivery path) διαμέσου του δικτύου. Έτσι το PIM-SM επιτρέπει στους δρομολογητές είτε α) να συνεχίσουν να λαμβάνουν πολλαπλά εκπεμπόμενη κυκλοφορία διαμέσου των δέντρων των RP's είτε b) να ακολουθήσουν το μικρότερο μονοπάτι με βάση τον αποστολέα (Shortest Path Tree –SPT-) που δημιουργεί επακόλουθος ο παραλήπτης μειώνοντας έτσι την καθυστέρηση μετάδοσης ανάμεσα σε αυτόν και μια συγκεκριμένη πηγή. Ένας PIM δρομολογητής με τοπικούς παραλήπτες έχει την δυνατότητα να χρησιμοποιήσει το SPT αμέσως μόλις αρχίσει να λαμβάνει πακέτα από έναν αποστολέα στέλνοντας ένα μήνυμα ένωσης στον αποστολέα των πακέτων και ταυτοχρόνως ένας άλλος μηχανισμός εγγυάται την άμεση αποστολή ενός μηνύματος αποκοπής για τον ίδιο αποστολέα στο ενεργό RP. Ειδάλλως μπορεί να συνεχίσει να χρησιμοποιεί το βασισμένο στο RP δέντρο μεταβίβασης. (Εικόνα 4-4)



Εικόνα 4-4

Κεφάλαιο 5

Το πρωτόκολλο RSVP (Resource ReserVation Protocol)

5.1 Εισαγωγή

Το πρωτόκολλο RSVP είναι ένα πρωτόκολλο επικοινωνίας του Internet το οποίο έχει σκοπό να μεταδίδει δεδομένα στο σωστό χρόνο και στη σωστή σειρά. Ο παραδοσιακός τρόπος μετάδοσης δεδομένων στο Internet είναι αυτός «της καλύτερης προσπάθειας» (best effort delivery) και δεν παρέχει καμία εγγύηση για τη σωστή μεταφορά των δεδομένων αφού το πρωτόκολλο IP που χρησιμοποιείται ευρέως δεν είναι προσανατολισμένο στη σύνδεση (connectionless oriented). Από την άλλη μεριά, το πρωτόκολλο TCP που χρησιμοποιείται σε συνδυασμό με το IP μπορεί να εγγυηθεί τη σωστή μεταφορά των δεδομένων αλλά όχι στο σωστό χρόνο. Η μεταφορά των δεδομένων στο χρόνο που πρέπει είναι κάτι το πολύ σημαντικό για τις εφαρμογές τηλεματικής. Για αυτό ακριβώς το λόγο το IETF έχει σχεδιάσει το πρωτόκολλο RSVP.

Με λίγα λόγια το πρωτόκολλο RSVP είναι μια προσπάθεια να αναπτυχθεί η «ποιότητα υπηρεσίας» (Quality of Service) στο Internet αλλά και σε όλα τα δίκτυα που χρησιμοποιούν το μοντέλο TCP/IP. Αυτό που μπορεί να πραγματοποιήσει το RSVP είναι να «κρατήσει» (reserve) ένα ορισμένο εύρος ζώνης (bandwidth) ανάμεσα σε δίκτυα που συνδέονται μεταξύ τους με τη βοήθεια δρομολογητών (routers). Ο κάθε δρομολογητής που γνωρίζει το RSVP διαθέτει ένα μέρος του εύρους ζώνης του για μια συγκεκριμένη ροή δεδομένων. Η ποιότητα υπηρεσίας (QoS) είναι χαρακτηριστικό των ATM δικτύων. Αυτό ακριβώς προσπαθεί να «μιμηθεί» το RSVP για παραδοσιακά δίκτυα TCP/IP.

Η δουλεία του RSVP, δηλαδή, είναι να εγγυάται εύρος ζώνης από το ένα σύστημα (πηγή δεδομένων) ως το άλλο (παραλήπτης δεδομένων). Το πρωτόκολλο λειτουργεί από τον ένα δρομολογητή προς τον επόμενο και δεν είναι στην πραγματικότητα ένα πρωτόκολλο δρομολόγησης, αλλά ένα πρωτόκολλο ελέγχου. Αν κάποιος δρομολογητής από το ένα σύστημα (πηγή) στο άλλο (παραλήπτης) δεν γνωρίζει το RSVP πρέπει να βρεθεί ένα άλλο μονοπάτι ανάμεσα στα δύο συστήματα.

Σήμερα, σχεδόν όλοι οι κατασκευαστές δρομολογητών υποστηρίζουν το RSVP. [14][15]

5.2 Η ροή δεδομένων στο RSVP

Η ροή δεδομένων μέσω του RSVP χαρακτηρίζεται από «συνόδους» (sessions) οι οποίες αναλαμβάνουν να μετακινήσουν τις πληροφορίες από τον πομπό στον/στους δέκτη/ες. Άρα, μία RSVP σύνοδος είναι μια μετάδοση δεδομένων από ένα αποστολέα προς έναν ή πολλούς παραλήπτες. Το RSVP υποστηρίζει και τη ταυτόχρονη μετάδοση δεδομένων από έναν ορισμένο αριθμό αποστολέων σε ένα ορισμένο αριθμό παραληπτών. Δηλαδή, ο παραλήπτης μπορεί να είναι μια ειδική IP που είναι δυνατό να αντιστοιχεί σε πολλούς παραλήπτες (περίπτωση multicast). Στην περίπτωση, λοιπόν, του multicast, υπάρχει ένα αντίγραφο των δεδομένων που στέλνει ο αποστολέας το οποίο παραδίδεται σε όλους τους παραλήπτες. Στην περίπτωση του unicast, ο αποστολέας στέλνει ξεχωριστά τα δεδομένα σε καθένα από τους παραλήπτες.

5.3 Το RSVP και η Ποιότητα Υπηρεσίας

Η ποιότητα υπηρεσίας στο RSVP καθορίζει τη συνδιαλλαγή δεδομένων ανάμεσα σε δρομολογητές αλλά και συγκεκριμένους υπολογιστές που λαμβάνουν μέρος σε κάποια RSVP σύνοδο. Οι υπολογιστές χρησιμοποιούν το RSVP για να καθορίσουν μία συγκεκριμένη στάθμη ποιότητας υπηρεσίας για μια συγκεκριμένη εφαρμογή, για παράδειγμα ένα λογισμικό τηλεδιάσκεψης. Παράλληλα, οι δρομολογητές χρησιμοποιούν το RSVP για να ζητήσουν από τους διπλανούς τους δρομολογητές το απαιτούμενο εύρος ζώνης για να μπορέσει να ικανοποιηθεί η αίτηση του προηγούμενου υπολογιστή. Ο δρόμος που τελικά συνδέει έναν αποστολέα και έναν παραλήπτη RSVP ροής δεδομένων λέγεται μονοπάτι (RSVP PATH).

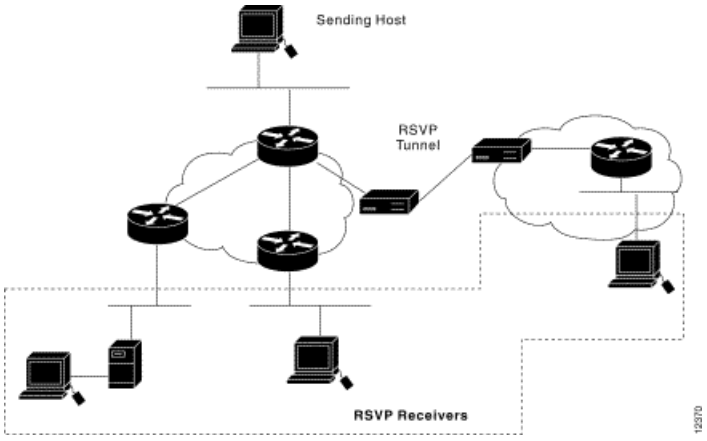
5.4 Η αρχή της RSVP συνόδου

Το ενδιαφέρον με το πρωτόκολλο RSVP βρίσκεται στις συνδέσεις multicast. Και αυτό γιατί τις περισσότερες φορές οι εφαρμογές που έχουν δεδομένα ευαίσθητα στο χρόνο είναι κυρίως λογισμικά τηλεδιασκέψεων στις οποίες λαμβάνουν μέρος πολλά άτομα. Για να πάρει μέρος κάποιος παραλήπτης σε μία RSVP multicast

σύνοδο πρέπει να πάρει μια multicast IP μέσω του πρωτοκόλλου IGMP (Internet Group Member Protocol). Στην περίπτωση της unicast συνόδου η δρομολόγηση γίνεται πάλι μέσω του IGMP με τη βοήθεια του PIM (Protocol Independent Multicast). Αφού ο παραλήπτης έχει μπει μέσα στην παραπάνω ομάδα, ο αποστολέας αρχίζει να στέλνει μηνύματα τα οποία θα δημιουργήσουν το RSVP μονοπάτι (PATH) προς την IP του παραλήπτη (multicast). Η εφαρμογή του παραλήπτη λαμβάνει τα παραπάνω μηνύματα και στέλνει πίσω απαντήσεις η οποίες αιτούνται κάποια στάθμη ποιότητας υπηρεσίας. Αφού τελικά η εφαρμογή του αρχικού αποστολέα έχει λάβει τις απαντήσεις των παραληπτών – η οποίες έχουν τη μορφή αίτησης κάποιου εύρους ζώνης – αρχίζει να μεταδίδει τα δεδομένα της εφαρμογής (audio, video κλπ). [20]

Περιγραφικά η δημιουργία μιας RSVP συνόδου είναι η παρακάτω:

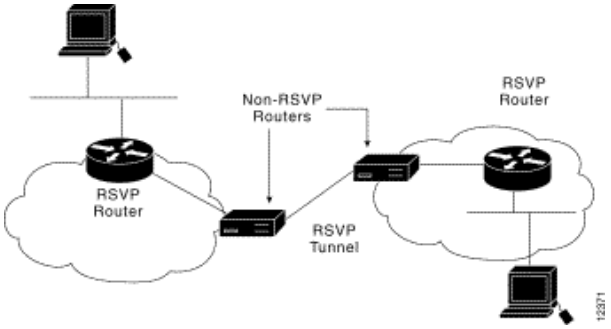
Η διαδικασία ξεκινά από τη μεριά του αποστολέα . Αυτός δίνει μια εντολή τύπου PATH, η οποία ταξιδεύει με τη βοήθεια των δρομολογητών σε έναν ή περισσότερους τελικούς αποδέκτες. Το μονοπάτι συνήθως συνδέει πάνω από έναν δέκτες και η σύνοδος είναι multicast. Κάθε δρομολογητής μπορεί να υποστηρίζει πολλές RSVP συνόδους. Όμως, η κάθε μία σύνοδος διαθέτει μία μοναδική «ταυτότητα» (ID) έτσι ώστε να μην συγχέονται τα δεδομένα της μίας με της άλλης. Αυτό το ID δίνεται από τον αποστολέα στη φάση της έκδοσης της εντολής για τη δημιουργία του RSVP μονοπατιού (RSVP PATH). Η προηγούμενη εντολή περιέχει και πληροφορίες για το είδος των δεδομένων που θα μετακινηθούν αλλά και το απαιτούμενο εύρος ζώνης που θα χρειαστεί. Η εντολή PATH ταξιδεύει από δρομολογητή σε δρομολογητή και δίνει τις απαραίτητες πληροφορίες που έχει ζητήσει ο αποστολέας. Το εύρος ζώνης που έχει ζητήσει δεν έχει αποδοθεί ακόμα. Όταν κάποιος παραλήπτης λάβει την εντολή PATH, μπορεί να ζητήσει να συμμετέχει στην RSVP σύνοδο στέλνοντας πίσω μια εντολή τύπου RESV. Η απάντηση των συμμετεχόντων πρέπει να ακολουθήσει την ίδια διαδρομή με αυτή της εντολής PATH του αποστολέα. Κάθε δρομολογητής που λαμβάνει την εντολή RESV εγγυάται το απαιτούμενο εύρος ζώνης. Αν κάποιος δρομολογητής λάβει πολλαπλές RESV εντολές από πολλούς διαφορετικούς παραλήπτες, τότε δεν διαθέτει ξεχωριστό εύρος ζώνης για κάθε σύνοδο, αλλά τις συνδυάζει αφού γνωρίζει το μοναδικό ID της RSVP συνόδου. [14]



Το πρωτόκολλο RSVP έχει ένα ακόμα ενδιαφέρον χαρακτηριστικό το οποίο ονομάζεται soft state. Με τη βοήθεια αυτού του χαρακτηριστικού μπορούν να γίνονται δυναμικές αλλαγές στις ομάδες των παραληπτών των RSVP δεδομένων. Με άλλα λόγια, το ίδιο το δίκτυο το οποίο «γνωρίζει» το πρωτόκολλο RSVP είναι δυνατό να πραγματοποιεί αλλαγές χωρίς να συμβουλεύεται τους τελικούς αποδέκτες των μηνυμάτων. Αυτό σε αντίθεση με τα δίκτυα circuit switched στα οποία ο τελικός κόμβος είναι υπεύθυνος για τη δημιουργία όλων των συνδέσεων. Όλοι οι συμμετέχοντες σε μία σύνοδο RSVP (δρομολογητές και υπολογιστές) είναι υποχρεωμένοι να στέλνουν περιοδικά κάποια μηνύματα τα λεγόμενα reservation states. Με αυτά τα μηνύματα οι δρομολογητές και οι συμμετέχοντες δηλώνουν την παρουσία τους στη συγκεκριμένη σύνοδο. Αν κάποιος αργήσει να στείλει ένα τέτοιο μήνυμα στην ώρα του, τότε το δίκτυο το θεωρεί ανενεργό. Σε περίπτωση που έχει αλλάξει η δρομολόγηση σε μία RSVP σύνοδο ο νέος δρομολογητής αναλαμβάνει να ανανεώσει το μονοπάτι που συνδέει όλους τους συμμετέχοντες.

Πολλές φορές δύο σταθμοί εργασίας που θέλουν να δημιουργήσουν μια σύνοδο RSVP συνδέονται με δρομολογητές που δεν γνωρίζουν το πρωτόκολλο. Αυτό είναι συχνό φαινόμενο όταν οι δύο σταθμοί χωρίζονται από μεγάλη γεωγραφική περιοχή και ανάμεσά τους βρίσκονται πολλοί δρομολογητές. Για αυτό το σκοπό, λοιπόν, το πρωτόκολλο RSVP έχει το χαρακτηριστικό που ονομάζεται tunneling. Το tunneling

είναι το φαινόμενο κατά το οποίο ένας δρομολογητής λαμβάνει μια εντολή PATH αλλά δεν γνωρίζει το πρωτόκολλο RSVP. Στην περίπτωση αυτή η εντολή περιέχει την τελευταία IP του δρομολογητή που γνώριζε το πρωτόκολλο RSVP και η αίτηση περνά αυτόματα στον διπλανό δρομολογητή ο οποίος γνωρίζει το συγκεκριμένο πρωτόκολλο. [20]



Στο κομμάτι της εγγύησης του απαιτούμενου εύρους ζώνης υπάρχουν διάφορα θέματα. Ένα πολύ σημαντικό στοιχείο είναι να μην μπορεί ο κάθε χρήστης να «κρατήσει» οσοδήποτε μεγάλο εύρος ζώνης για μια εφαρμογή που θα επιθυμεί να τρέξει στο δίκτυο. Σε τοπικά δίκτυα η διαχειριστική ομάδα μπορεί να εγκαταστήσει ορισμένους εξυπηρετητές οι οποίοι θα κρατούν πληροφορίες για το ποιος μπορεί να αιτηθεί εύρος ζώνης, πότε μπορεί να το κάνει, πόσο διάστημα θα το έχει στη διάθεσή του και πόσο θα είναι αυτό το εύρος ζώνης. Σε επίπεδο Internet το πρωτόκολλο RSVP θα υπάγεται στην τιμολογιακή στρατηγική των Internet Service Providers.

Ένα άλλο ζήτημα είναι με ποιο τρόπο οι δρομολογητές διαχειρίζονται τις προτεραιότητες. Ένας δρομολογητής μπορεί την ίδια στιγμή να υποστηρίζει πολλές συνόδους RSVP με διαφορετικά ID και με ξεχωριστές απαιτήσεις για εύρος ζώνης. Σίγουρα, κάποιες από αυτές θα έχουν μεγαλύτερες απαιτήσεις και κάποιες άλλες μικρότερες. Ένας τρόπος για να διαχειριστεί ο δρομολογητής αυτές τις ξεχωριστές συνόδους είναι να δημιουργήσει μια «ουρά» (queue) που να περιέχει όλες τις συνόδους που περιμένουν να εξυπηρετηθούν και να δώσει σε καθεμία μια ξεχωριστή προτεραιότητα. Κάθε πακέτο κάθε συνόδου περιέχει μία «ταμπέλα» (tag) η οποία καθορίζει την προτεραιότητά του. Ο δρομολογητής προωθεί τα πακέτα με την

μεγαλύτερη προτεραιότητα πρώτα. Σε αυτόν τον αλγόριθμο διασφαλίζεται ότι ακόμα και τα πακέτα με τη χαμηλότερη προτεραιότητα θα προωθηθούν. [21][22]

Για την υλοποίηση μιας RSVP συνόδου θα πρέπει να λαμβάνουν μέρος πολύ ισχυροί και σύγχρονοι δρομολογητές, διότι από το σχεδιασμό του το πρωτόκολλο RSVP απαιτεί πολύ μεγάλη υπολογιστική ισχύ από τους ενδιάμεσους δρομολογητές για την δημιουργία και συνεχή εποπτεία της συνόδου. [14]

Κεφάλαιο 6

Το πρωτόκολλο PNNI (Private Network-to-Network Interface)

6.1 Εισαγωγή

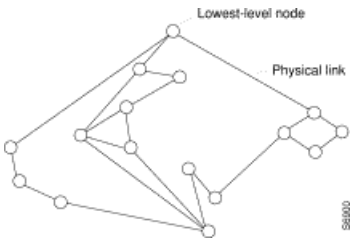
Το PNNI είναι ένα πρωτόκολλο δρομολόγησης που χρησιμοποιείται στα δίκτυα ATM. Είναι ένα δυναμικό link state πρωτόκολλο που υλοποιείται συνήθως σε δίκτυα campus. Χαρακτηρίζεται ως δυναμικό γιατί έχει σχεδιαστεί έτσι ώστε οι μονάδες (switches) να μαθαίνουν σχεδόν αυτόματα την τοπολογία και τη διασυνδεσιμότητα του δικτύου. Ένα χαρακτηριστικό του PNNI είναι ότι κάθε μονάδα ενός τέτοιου δικτύου υπολογίζει ολόκληρη τη διαδρομή που θα πρέπει να ακολουθήσει το σήμα για να συνδέσει δύο σταθμούς εργασίας σε ένα ATM δίκτυο. Αυτό σε αντίθεση με το συνηθισμένο «hop by hop» τρόπο σύνδεσης κατά τον οποίο κάθε μονάδα στέλνει το σήμα στην επόμενη χωρίς να γνωρίζει ολόκληρη τη διαδρομή που αυτό τελικά θα ακολουθήσει. Ένα τυπικό ATM δίκτυο μπορεί να αποτελείται από μερικά ATM switches τα οποία επικοινωνούν με κάποιο πρωτόκολλο το οποίο το έχει σχεδιάσει ο κατασκευαστής τους (NNI Network to Network Interface). Το πρωτόκολλο PNNI έρχεται να συνδέσει όλα αυτά τα switches με τρόπο ώστε να επιτρέπεται η άμεση επικοινωνία τους.

Με άλλα λόγια, το PNNI προσφέρει ένα ενιαίο τρόπο επικοινωνίας ανάμεσα σε διαφορετικά – από κατασκευής switches – έτσι ώστε να μπορούν να ανταλλάσουν πληροφορίες σχετικά με την τοπολογία του δικτύου. Σε κάποια μεγάλα ATM δίκτυα μπορεί να υπάρχουν εκατοντάδες ή χιλιάδες ATM switches τα οποία, βέβαια, πρέπει να επικοινωνούν μεταξύ τους για να παρέχουν τη σύνδεση από έναν σταθμό εργασίας στον άλλον. Με τη βοήθεια του PNNI βρίσκεται το κατάλληλο μονοπάτι που συνδέει δύο υπολογιστές μέσα σε ένα ATM δίκτυο και από εκεί και πέρα το ίδιο το ATM αναλαμβάνει να δημιουργήσει το VC (virtual circuit). [14] [23]

Θέματα σχεδιασμού και λειτουργίας

Το PNNI δημιουργεί μια ιεραρχία από συνδεόμενα ATM switches. Με αυτό τον τρόπο ελαχιστοποιείται η πληροφορία που πρέπει να ανταλλάσσουν οι συσκευές μεταξύ τους. Σε μεγάλα ATM δίκτυα δεν έχει νόημα όλες οι συσκευές να

επικοινωνούν με όλες, αντίθετα τα switches με τη βοήθεια του PNNI χωρίζονται σε



ομάδες έτσι ώστε να υπάρχει ιεραρχική διαχείρισή τους. Τα επίπεδα αυτής της ιεραρχίας φτάνουν μέχρι και τα 105, αν και είναι απίθανο ένα ATM δίκτυο να χρειαστεί πάνω από μερικές δεκάδες.

Στην κορυφή της ιεραρχίας βρίσκεται το Private ATM Network ή PAN, το οποίο καθορίζει με ποιο τρόπο λειτουργεί η ιεραρχία παρακάτω και με ποιο τρόπο οι συσκευές που βρίσκονται στα κατώτερα στρώματα της ιεραρχίας παρέχουν πληροφορίες στα ανώτερα. Το μοντέλο γενικά είναι αναδρομικό, άρα ότι ισχύει στα ανώτερα στρώματα ισχύει και στα κατώτερα. Κάθε στρώμα του μοντέλου αποτελείται από λογικές μονάδες που συνδέονται λογικά μεταξύ τους. Στα κατώτερα στρώματα του μοντέλου υπάρχουν οι φυσικές συσκευές (ATM switches) ή ένα κλειστό ATM δίκτυο που αποτελείται από πολλά ATM switches, το χρησιμοποιεί κάποιο ιδιαίτερο πρωτόκολλο NNI για εσωτερική επικοινωνία και το PNNI για την επικοινωνία του με τα υπόλοιπα στρώματα του μοντέλου.

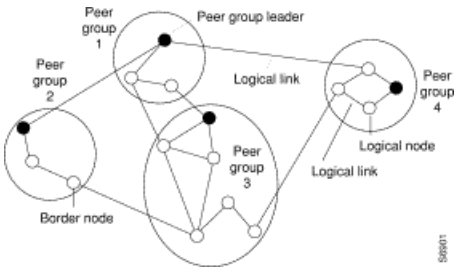
Μια ομάδα από μονάδες (switches) μέσα στο ίδιο επίπεδο της ιεραρχίας ονομάζεται peer group ή Private ATM switches (PASs). Ο ορισμός του peer group είναι μια ομάδα από switches τα οποία ανταλλάσσουν την ίδια τοπολογική βάση δεδομένων μεταξύ τους και τις ίδιες πληροφορίες για την κατάσταση σύνδεσης (link state information). Εφόσον κάθε μονάδα σε ένα peer group έχει τις ίδιες πληροφορίες με της υπόλοιπες, η ομάδα δεν είναι καλό να αποτελείται από πολύ μεγάλο αριθμό από μονάδες (switches), διότι θα υπάρχει πολύ μεγάλη άσκοπη κίνηση από την ανταλλαγή αυτών των πληροφοριών και βάσεων δεδομένων. Για αυτό στις περιπτώσεις των peer groups, υπάρχει μια ιεραρχική δομή η οποία ξεκινά με το γονιό – group (parent group). Ο γονιός βλέπει κάθε «παιδί» του ως μία λογική μονάδα η οποία στην πραγματικότητα αποτελείται από πολλές ξεχωριστές μονάδες (ATM switches). Κάθε τέτοιο «παιδί» ονομάζεται logical group node. Τα παιδιά

επικοινωνούν με τους γονείς τους σε αυτό το ιεραρχικό μοντέλο και ανταλλάσσουν πληροφορίες μαζί τους σαν να ήταν μία ενιαία μονάδα.

Το ιεραρχικό αυτό σχήμα χρησιμοποιεί τις ειδικές ATM διευθύνσεις για να ξεχωρίζει τα διάφορα επίπεδα μεταξύ τους.

Κάθε peer group εκλέγει ένα μοναδικό κόμβο ο οποίος ορίζεται ως υπεύθυνος όλης της μονάδας. Αυτός ο κόμβος ονομάζεται peer group leader (PGL). Κάθε PGL χαρακτηρίζεται από μια μοναδική ATM διεύθυνση. Αρμοδιότητες του κόμβου αυτού είναι να ενημερώνει τα ανώτερα στρώματα για τη διαθεσιμότητα του επιπέδου στο οποίο βρίσκεται ο ίδιος, αλλά και μεταφέρει πληροφορίες από τα ανώτερα επίπεδα στα κατώτερα. Με αυτό τον τρόπο οι πληροφορίες διαχέονται σε όλη την ιεραρχία και κατασκευάζονται αξιόπιστοι δρόμοι ανάμεσα στις λογικές και φυσικές μονάδες.

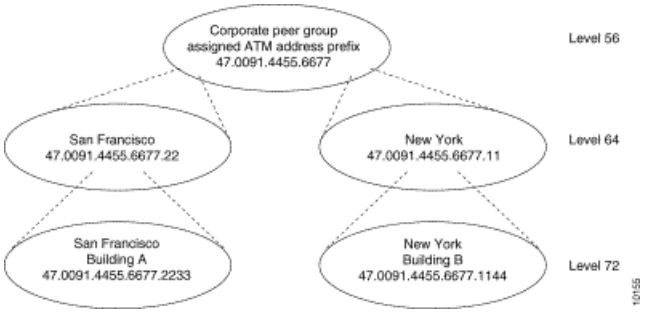
Όσο η πληροφορία μεταφέρεται από τα ανώτερα επίπεδα στα κατώτερα τόσο ελαχιστοποιείται. Με άλλα λόγια, στο κατώτερο επίπεδο της ιεραρχίας οι μονάδες – οι οποίες αποτελούνται από φυσικές οντότητες (switches) – γνωρίζουν όλες τις πληροφορίες για τις ομάδες του ίδιου επιπέδου, λιγότερες πληροφορίες για τις ομάδες που βρίσκονται ένα επίπεδο πιο πάνω κοκ.



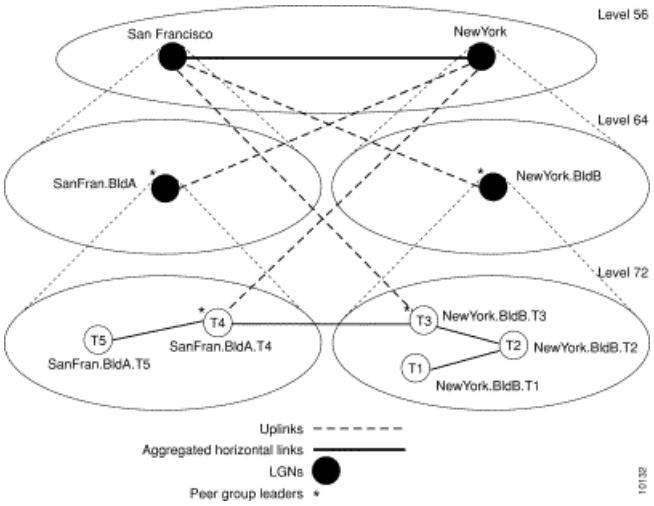
Οι εσωτερικές συνδέσεις μεταξύ των κόμβων σε ένα peer group ονομάζονται οριζόντιες.

Οι κόμβοι ανακαλύπτουν ο ένας τον άλλον μέσα από ειδικά μηνύματα επικοινωνίας τα λεγόμενα hello. Αυτά είναι πακέτα που ανταλλάσσονται σε τακτά χρονικά διαστήματα ανάμεσα σε δύο γειτονικούς κόμβους. Στην περίπτωση κατά την οποία δύο κόμβοι καταλάβουν ότι βρίσκονται στο ίδιο peer group, τότε ανταλλάσσουν τις βάσεις δεδομένων τους για τη δρομολόγηση μέχρι να έχουν ακριβώς τα ίδια στοιχεία. Αμέσως μετά στέλνουν και στα υπόλοιπα μέλη του ίδιου peer group αυτές τις πληροφορίες έτσι ώστε να μεταφερθεί η πληροφορία όσο το δυνατό γρηγορότερα.

Οι κόμβοι που αναλαμβάνουν να ανακαλύψουν άλλα peer groups ονομάζονται border nodes και συνδέονται φυσικά με τις υπόλοιπες ομάδες. Η επικοινωνία πραγματοποιείται και σε αυτή την περίπτωση με τα hello πακέτα. Οι δύο border nodes ανταλλάσσουν πληροφορίες και καταλαβαίνουν ότι ανήκουν σε δύο διαφορετικά peer groups, ανακαλύπτουν τους κοινούς «γονείς» αλλά και μοιράζουν πληροφορίες για τις γειτονικές ομάδες που τυχόν θα βρίσκονται συνδεδεμένοι. Ο σκοπός πάντα της ανταλλαγής πληροφοριών είναι να γνωρίζουν όλοι οι κόμβοι για τη διαθεσιμότητα όλων των υπολοίπων. Τα border nodes ανταλλάσσουν πληροφορίες και για τους PGLs κάθε group έτσι ώστε να γνωρίζει ο κάθε leader τους διπλανούς του.



Μόλις η κυκλοφορία όλων των πληροφοριών έχει ολοκληρωθεί και κάποιος σταθμός εργασίας στείλει μία αίτηση σε κάποιο κόμβο (switch) για να συνδεθεί με κάποιον άλλον σταθμό εργασίας πραγματοποιείται το εξής: ο κόμβος που θα λάβει το σήμα θα δημιουργήσει ένα δρόμο που θα έχει κάθε λεπτομέρεια για την αποστολή της αίτησης μέσα στο ίδιο peer group, θα έχει λιγότερες πληροφορίες για το πώς θα συνεχίσει το σήμα εκτός του group κοκ. Με άλλα λόγια, όσο απομακρύνεται το σήμα από το πρώτο switch τόσο πιο αδύναμη είναι η πληροφορία. Όμως, όταν η αίτηση περάσει εκτός του πρώτου peer group θα την παραλάβει ο border node του επόμενου στην ιεραρχία peer group και θα ακολουθηθεί η ίδια διαδικασία. Αυτό θα συνεχιστεί μέχρι η αίτηση να φτάσει στο τελικό peer group και με τη βοήθεια αυτού να δημιουργηθεί η τελική σύνδεση ανάμεσα στους δύο σταθμούς εργασίας.



Με αυτό τον τρόπο τα PANs μπορούν να επεκταθούν σε μεγάλες γεωγραφικές αποστάσεις και να λαμβάνουν μέρος στην ιεραρχία πολλά switches. Όμως, πρέπει να θυμάται κανείς ότι στο ATM ο κύριος σκοπός είναι να υπάρχει ικανοποιητική ποιότητα υπηρεσίας (Quality of Service). Καθώς η πληροφορία γίνεται όλο και πιο συγκεντρωτική όσο ανεβαίνει στην ιεραρχία του PNNI, τόσο συγκεντρωτικές γίνονται και οι απαιτήσεις των σταθμών εργασίας για QoS. Άρα, όσο μεγαλώνει η ιεραρχία του PNNI, τόσο μειώνεται η απόδοση του ATM δικτύου σε ότι αφορά το QoS.

Για να λύσει αυτό το πρόβλημα το PNNI έχει μια λειτουργία η οποία δίνει τη δυνατότητα στους κόμβους των ανώτερων επιπέδων να γνωρίζουν με λεπτομέρεια όλη την τοπολογία του δικτύου, ακόμα και τους κόμβους των κατώτερων επιπέδων.

Ένα ακόμα χαρακτηριστικό του πρωτοκόλλου PNNI είναι ότι έχει τη δυνατότητα να δημιουργεί permanent virtual connections. Αυτό σημαίνει το «άνοιγμα» ενός PVC με καθαρές λειτουργίες PNNI οι οποίες υποστηρίζουν QoS. [16]

Το πρωτόκολλο PNNI είναι μια μέτρια λύση για υλοποίηση ενός ATM δικτύου σε τοπική διάσταση, για παράδειγμα ένα LANE. Το PNNI είναι υπερβολικά πολύπλοκο και αποτελεί πολύ κακή επιλογή για δημιουργία ATM WAN δικτύων. Ο καλύτερος τρόπος για τη δημιουργία ενός ATM δικτύου είναι να θεωρηθούν τα switches «μαύρα κουτιά» και να δρομολογούν την κίνηση σύμφωνα με την τοπολογία που θα λάμβανε υπόψη του ένας δρομολογητής του τρίτου επιπέδου του OSI και όχι σύμφωνα με την ιεραρχία και τη λειτουργία του PNNI. [20][24][25]

Κεφάλαιο 7

Routing Over Large Clouds

Το ROLC αποτελεί μία ομάδα εργασίας στην IETF που δημιουργήθηκε για να αναλύσει και να προτείνει λύσεις στα προβλήματα που παρουσιάζονται όταν θέλουμε να διεξάγουμε IP δρομολόγηση πάνω σε μεγάλα και κοινά δίκτυα όπως τα ATM, Frame Relay, SMDS, και X.25. [26]

7.1 MultiProtocol Over ATM MPOA / Next Hope Resolution Protocol

Το MPOA πρωτόκολλο είναι μια λύση για τη μεταφορά όλων των πρωτοκολλων σε ένα δίκτυο ATM.Τα σημαντικότερα πλεονεκτήματα του MPOA είναι :

- Inter-VLAN “cut-through” που μεγιστοποιεί το bandwidth και τον κατακερματισμό (segmentation) του δικτύου.
- Robust Layer 3 QoS χαρακτηριστικά για την υποστήριξη packetized κίνησης (π.χ video ή φωνή), ενω εγγυάται και τις υπηρεσίες επιπέδου δεδομένων (data service levels)
- Μία software-only αναβάθμιση (upgrade) , που ελαχιστοποιεί το κόστος και απλοποιεί την υλοποίηση.

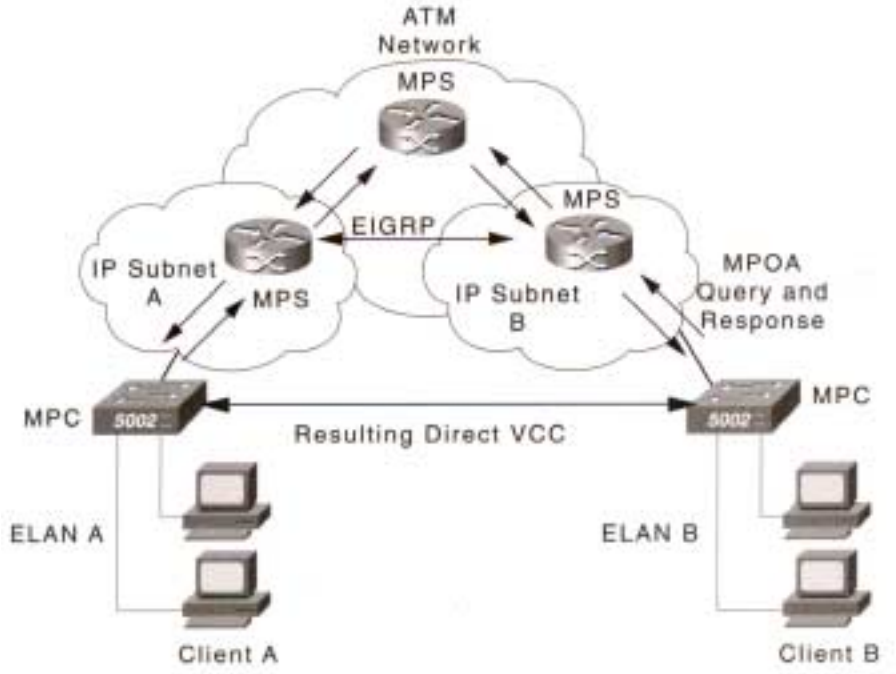
Η αρχιτεκτονική του MPOA έχει τέσσερα δομικά στοιχεία

- MPOA client (MPC)
- MPOA server (MPS)
- Next Hope Resolution Protocol (NHRP)

- LAN Emulation (LANE)

Το MPOA χρησιμοποιεί μια απευθείας εικονική σύνδεση καναλιού (virtual channel connection (VCC)) μεταξύ της εισόδου και της εξόδου. Η VCC επιτρέπει την προώθηση των πακέτων του επιπέδου 3 (Layer 3), που συνίθως μεταδίδονται μέσω ενδιάμεσων δρομολογητών , απο τον αρχικό στον τελικό δρομολογητή αυξάνοντας έτσι την αποδοτικότητα και μειώνοντας την καθυστέρηση.

Η εικόνα 7-1 απεικονίζει τη χρήση MPC , MPS και του NHRP για την επίτευξη μιας VCC μεταξύ των δύο άκρων ενος ATM δικτύου.



Εικόνα 7-1: Επίυευξη απευθείας σύνδεσης μεταξύ των δύο άκρων ενός ATM δικτύου

Η χρήση του NHRP γίνεται στον MPS. Ας δούμε λοιπόν τη λειτουργεία του.

7.1.1 Multiprotocol Server (MPS)

Ο MPS παρέχει όλες τις πληροφορίες προώθησης που χρησιμοποιούν οι MPCs. Ο MPS διαχειρίζεται την πληροφορία χρησιμοποιώντας το NHRP. Ο MPS αλληλεπιδρά με το NHRP σύμφωνα με τα παρακάτω :

1. Ο MPS μετατρέπει την αίτηση που δέχεται απο το MPOA για επίλυση σε μια NHRP αίτηση. Επειτα ο MPS στέλνει την αίτηση αυτή είτε στον Next Hop MPS είτε στον Next Hop Server (NHS). Ο MPS εξασφαλίζει επίσης τη σωστή ενθυλάκωση σύμφωνα με τον τύπο του NHS.
2. Αν ο επόμενος κόμβος (hop) αποδειχθεί οτι θα είναι σε ένα LANE cloud ο NHS στέλνει τις αιτήσεις επίλυσης στον MPS. Διαφορετικά ο NHS στέλνει τις αιτήσεις επίλυσης όταν ο προορισμός των πακέτων είναι άγνωστος. Ο MPS μπορεί επίσης να ζητήσει απο τον NHS να απορίψει το πακέτο.
3. Αν οι απαντήσεις τερματίσουν στο δρομολογητή ή η διασύνδεση του επόμενου κόμβου χρησιμοποιεί LANE οι απαντήσεις ανάλυσης αποστέλλονται απο τον NHS στον MPS.
4. Οταν λάβει ο MPS τις απαντήσεις επίλυσης απο τον NHS τότε στέλνει μια MPOA αίτηση επίλυσης στον MPC.

Ο MPS χρησιμοποιεί μια ταυτότητα δικτύου (network ID). Η προεπιλεγμένη της τιμή για όλους τους MPS είναι ένα.Αυτό βοηθά τους σχεδιαστές του δικτύου στο να επιτρέπουν ή οχι τις συνδέσεις που επιθυμούν. Η network ID ενός MPS και του NHRP πρέπει να είναι ίδια στον ίδιο δρομολογητή για να μπορούν να συνεργασθούν[12].

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] “Advanced IP Routing in Cisco Networks”, Slattery & Burton, McGraw-Hill, 1999

[2] “Δίκτυα Υπολογιστών”, Tannenbaum, Παπασωτηρίου, 1992

[3] “Routing Information Protocol”
http://www.cisco.com/press/cc/td/cpress/fund/ith2nd/it2444.htm

[4] http://www.cis.ohio-state.edu/htbin/rfc/rfc1058.htm

[5] http://www.cis.ohio-state.edu/htbin/rfc/rfc1388.htm

[6] “Interior Gateway Routing Protocol”
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

[7] “Enhanced Interior Gateway Routing Protocol”
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm

[8] http://www.cis.ohio-state.edu/htbin/rfc/rfc1247.htm

[9] “Open Shortest Path First Protocol”
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm

[10] “Border Gateway Protocol”
http://www.cisco.com/univercd/cc/td/doc/csintwk/ito_doc/bgp.htm

[11] “Designing Cisco Networks” ,Diane Teare ,Cisco Press ,1999

[12] “Cisco Router Handbook”, George Sackett , McGraw Hill , 1999

[13]”Designing DDR Internetworks”
http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2010.htm

[14] “Encyclopedia of Networking”, Tom Sheldon, εκδ. McGraw-Hill, 1998

[15] “Top-Down Network Design, Priscilla Oppenheimer”,εκδ. Macmillan Technical Publishing, 1999

[16] “LAN, ATM and LAN Emulation Technologies”, Daniel Minoli Anthony Alles, εκδ. Artech House, 1996

[17] “Deploying IP Multicast In The Enterprise”,Thomas A. Maufer, Prentice Hall,1998

[18] “Protocol Independent Multicast Version 2, Dense Mode Specification”, draft-ietf-idmr-pim-dm-spec-05.ps, S. Deering, D. Estrin, D. Farinacci, V. Jacobson, A. Helmy, and L.Wei, May 21, 1997

[19] “Protocol Independent Multicast-Sparse Mode (PIM-SM): Motivation and Architecture”, draft-ietf-idmr-pim-arch-04.ps, S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C. Liu and L.Wei, November 19, 1996

[20] http://www.knowcisco.com

[21] http://www.informit.com

[22] http://www.baynetworks.com

[23] “OSPF Network Design Solutions”, Thomas M. Thomas II, εκδ. Macmillan Technical Publishing, 1998

[24] http://www.cisco.com

[25] http://www.atmforum.com

[26]Acronyms Explanation – Cisco Webopedia

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm