Διαχείριση Multicast Video σε non-Multicast Δίκτυα

Διπλωματική εργασία

Μιχάλης Τόλκας

Πανεπιστήμιο Δυτικής Μακεδονίας
Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών

Επιβλέποντες

Αγγελίδης Παντελής
Πανεπιστήμιο Δυτικής Μακεδονίας

Δημητρακόπουλος Γεώργιος
Πανεπιστήμιο Δυτικής Μακεδονίας

Μπλέτσας Μιχαήλ
MIT Media Lab

Κοζάνη, Μάρτιος 2011

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επίκουρο καθηγητή κ. Αγγελίδη Παντελή ο οποίος κατέστησε δυνατή τη μετάβασή μου στο Τεχνολογικό Ίδρυμα της Μασαχουσέτης για την εκπόνηση της παρούσης διπλωματικής εργασίας. Επίσης, ευχαριστώ θερμά τον κ. Μιχάλη Μπλέτσα, ερευνητή και διευθυντή του Network and Computing Systems του MIT Media Lab για την καθοδήγηση σε όλη την πορεία της εργασίας. Η συνεργασία μας σε αυτό το μοναδικό ακαδημαϊκό περιβάλλον αλλά και ευρύτερα έπαιξε σημαντικότατο ρόλο στη διεύρυνση των γνώσεών μου επί της εφαρμοσμένης πληροφορικής και της τεχνολογίας γενικότερα. Οφείλω επίσης να ευχαριστήσω ιδιαίτερα τους Will Glesnes και Peter Pflanz του NeCSys για τις πολύτιμες συμβουλές τους κατά τη διάρκεια της παρουσίας μου στο Media Lab, καθώς και τους Jon Ferguson, Tom Greene, Jane Wojcik, Josh Boughey, Elizabeth Harvey και Dan DeMore για την γόνιμη συνεργασία μας.

Περιεχόμενα

Διαχείριση Multicast Video σε non-Multicast Δίκτυα

Μιχάλης Τόλκας

Περίληψη

Η παρούσα διπλωματική εργασία επεξεργάζεται τις βασικές τεχνικές μετάδοσης video, εστιάζοντας κυρίως στην τεχνολογία Multicast η οποία όλο και περισσότερο εφαρμόζεται τα τελευταία χρόνια. Αν και ο συγκεκριμένος τρόπος μετάδοσης μπορεί να μειώσει σημαντικά τη χρήση πόρων ορισμένων δικτύων αλλά και να καταστήσει συνολικά αποδοτικότερη την προώθηση της κίνησης, οι προδιαγραφές τεχνολογιών όπως το IEEE 802.11, καθιστούν πρακτικά αδύνατη την εφαρμογή του. Στην εργασία αυτή, θα μελετήσουμε και θα χρησιμοποιήσουμε τεχνολογίες με τις οποίες θα υπερβούμε τα εμπόδια των προδιαγραφών και θα καταστίσουμε δυνατή την μετάδοση Multicast video σε οικογένειες δικτύων όπως αυτή του WiFi. Με αυτό τον τρόπο θα έχουμε τη δυνατότητα να δημιουργήσουμε μία χαμηλού κόστους, διαπλατφορμική υποδομή αξιόπιστης και αδιάλειπτης μετάδοσης video.

Εισαγωγή

Unicast, Broadcast, Multicast

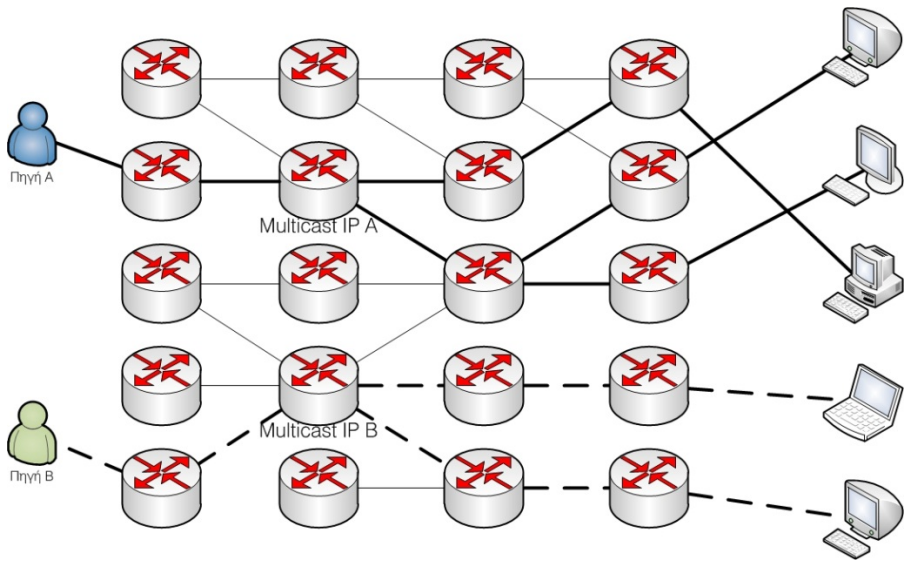
Το *Multicast* είναι μια μορφή επικοινωνίας με την οποία η πληροφορία παραδίδεται από μία ή περισσότερες πηγές σε πολλαπλούς δέκτες. Σε επίπεδο μετάδοσης πακέτων IP, το Multicast διαφέρει από το *Unicast* το οποίο είναι ένα-προς-ένα επικοινωνία και το *Broadcast* το οποίο είναι ένα-προς-όλους [1].

Το *Unicast* αποτελεί την πιο διαδεδομένη και απλή point-to-point επικοινωνία μεταξύ δύο συσκευών σε ένα δίκτυο, όπως ένα PC και έναν file server [2]. Το unicast είναι συνήθως αρκετό για την πλειοψηφία των εφαρμογών, αλλά υστερεί σε αρκετές περιπτώσεις όπου χρειάζεται συνεργασία μεταξύ των κόμβων ενός δικτύου. Για παράδειγμα, το unicast δεν θα ήταν κατάλληλο για την εκπαίδευση των υπαλλήλων μιας εταιρείας, διαδικασία κατά την οποία ο εκπαιδευτής χρησιμοποιεί μια collaborative, shared-whiteboard εφαρμογή για την αποστολή σε πραγματικό χρόνο, της εικόνας του δικού του υπολογιστή στα τερματικά 35 εκπαιδευόμενων. Στο unicast, η πληροφορίες της οθόνης του εκπαιδευτή θα πρέπει να μεταδοθούν ξεχωριστά σε κάθε τερματικό, κάτι που θα έχει σαν αποτέλεσμα σημαντικές καθυστερήσεις, καθώς κάθε νέα πληροφορία αποστέλλεται 35 φορές. Αυτό προφανώς αποτελεί σπατάλη bandwidth, καθώς η πληροφορία που λαμβάνει το κάθε τερματικό, είναι αντίγραφο της πληροφορίας που έλαβε ο προηγούμενος υπολογιστής. Θα ήταν φυσικά προτιμότερο αν και οι 35 εκπαιδευόμενοι μπορούσαν να ‘’ακούν’’ τον εκπαιδευτή ταυτόχρονα έτσι ώστε κάθε νέα πληροφορία να μεταδίδεται μόνο μία φορά.

Αυτό είναι κάτι που καταφέρνει ένα *Broadcast* δίκτυο. Το broadcast επιτρέπει σε ένα τερματικό ενός δικτύου να ‘’μιλάει’’ ταυτόχρονα σε όλες τις συσκευές που υπάρχουν στο ίδιο broadcast domain, ή subnet. Αλλά και τα broadcast δίκτυα έχουν τα δικά τους μειονεκτήματα. Για παράδειγμα, ο video server ενός τηλεοπτικού σταθμού θα μπορούσε να στέλνει μία ροή στο δίκτυο ενός πανεπιστημιακού campus, έτσι ώστε οποιοσδήποτε χρήστης να μπορεί να

συντονίζεται. Για να έχει όμως οποιοσδήποτε χρήστης του campus τη δυνατότητα να συντονίζεται, θα πρέπει να επιτραπεί στα broadcasts να ξεπερνούν τα όρια των επιμέρους subnets. Σε αυτό το σενάριο, τα broadcasts χρησιμοποιούν πολύτιμο bandwidth στα subnets κατά μήκους του campus. Επιπλέον, το broadcast επιβάλει σε όλα τα τερματικά και τον δικτυακό εξοπλισμό (όπως switches ή routers) να λάβουν και να επεξεργαστούν τα πακέτα, ακόμα και αν μόνο ένας μικρός αριθμός χρηστών επιθυμεί να λάβει την broadcast πληροφορία.

Την απάντηση στα παραπάνω προβλήματα δίνει το *IP Multicasting*. Πρόκειται για μια μέθοδο επικοινωνίας με την οποία ένα τερματικό μπορεί να στείλει πληροφορία σε πολλαπλούς χρήστες ταυτόχρονα, αλλά αντίθετα με τις δυνατότητες ‘’ένα ή όλα’’ που δίνουν τα unicast και broadcast αντίστοιχα, ο αποστολέας μπορεί να ορίσει τους χρήστες οι οποίοι θα λάβουν την πληροφορία. Αυτό επιτυγχάνεται με την αποστολή των πακέτων σε μια ‘’ειδική’’ IP multicast διεύθυνση, η οποία μπορεί να παρομοιαστεί με ένα τηλεοπτικό κανάλι. Οι χρήστες που ενδιαφέρονται να λάβουν την πληροφορία, απλά συντονίζονται (χρησιμοποιώντας το πρωτόκολλο IGMP το οποίο θα συζητήσουμε αργότερα) στην συγκεκριμένη διεύθυνση που περιέχει τα δεδομένα. Σε επίπεδο δρομολογητή, πριν την τελική προώθηση προς τους παραλήπτες πραγματοποιείται ο πολλαπλασιασμός των πακέτων (packet replication [53]), η γενική μορφή του οποίου φαίνεται στο σχήμα 1.

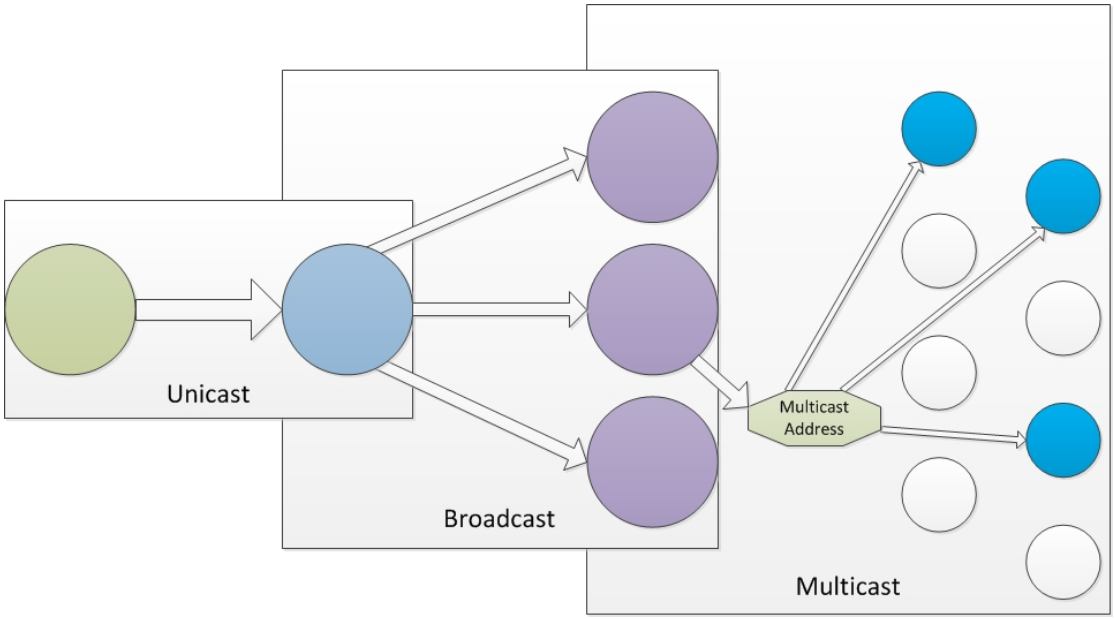


Σχήμα 1 – Packet Replication

Το IP multicasting, όταν υλοποιηθεί κατάλληλα, επιτρέπει κοινόχρηστες ροές δεδομένων να προωθηθούν μέσω του δικτύου μια μόνο φορά και αποκλειστικά στους χρήστες που επιθυμούν να λάβουν τη συγκεκριμένη ροή. Έτσι, αναφερόμενοι ξανά στο παράδειγμα του τηλεοπτικού video server, αν στο campus υπάρχουν συνολικά 40 subnets και οι χρήστες που θέλουν να λάβουν τη ροή ανήκουν σε μόνο 2 από αυτά, το bandwidth των υπόλοιπων 38 δεν θα επηρεαστεί, όπως θα συνέβαινε στην περίπτωση του broadcast.

Επιπλέον παραδείγματα εφαρμογών που επωφελούνται του IP multicasting είναι τα video (π.χ. η IPTV) και audio streaming, μετάδοση χρηματιστηριακών δεδομένων όπως οι τιμές μετοχών, αντίγραφα βάσεων δεδομένων, μεταφορά bulk data (για παράδειγμα παράλληλες αναβαθμίσεις λογισμικού σε εταιρικό περιβάλλον στο οποίο από έναν μόνο server μπορούν να αναβαθμιστούν ταυτόχρονα όσοι υπολογιστές χρήζουν αναβάθμισης, ανεξαρτήτως γεωγραφικής κατανομής), e-learning και κατανεμημένα (distributed) ηλεκτρονικά παιχνίδια.

Το Σχήμα 2 δίνει μια απλουστευμένη γραφική αναπαράσταση των χαρακτηριστικών των τριών τεχνολογιών.



Σχήμα 2 - Unicast, Broadcast, Multicast

Τα βασικά του Multicast

Multicast διευθυνσιοδότηση

Στη επικοινωνία μέσω multicast αντιμετωπίζουμε δύο βασικά προβλήματα: 1) πώς να προσδιορίσουμε τους δέκτες ενός multicast datagram και 2) πώς να διευθυνσιοδοτήσουμε το αποστελλόμενο multicast datagram [3]. Στην περίπτωση του unicast, η διεύθυνση IP του παραλήπτη (προορισμού) υπάρχει σε κάθε IP unicast datagram και προσδιορίζει τον μοναδικό παραλήπτη. Στην περίπτωση του broadcast όλοι οι κόμβοι του δικτύου θα λάβουν το broadcast πακέτο, άρα δεν χρειάζεται κάποια διεύθυνση προορισμού. Όμως στην περίπτωση του multicast έχουμε πολλαπλούς αποδέκτες.

Έχει νόημα, κάθε multicast πακέτο να φέρει την IP διεύθυνση όλων των παραληπτών; Αν και αυτή η προσέγγιση μπορεί να είναι εφαρμόσιμη για μικρό αριθμό παραληπτών, είναι πρακτικά αδύνατη σε περιπτώσεις δικτύων με εκατοντάδες ή χιλιάδες παραλήπτες. Η ποσότητα της πληροφορίας διευθυνσιοδότησης στο datagram θα υπερκάλυπτε την ποσότητα των πραγματικών δεδομένων στο πεδίο payload του πακέτου. Επίσης ο προσδιορισμός μεμονωμένων παραληπτών από τον αποστολέα προϋποθέτει ότι ο αποστολέας γνωρίζει την ταυτότητα και τις διευθύνσεις όλων των παραληπτών. Παρακάτω θα δούμε ότι υπάρχουν περιπτώσεις στις οποίες μια τέτοια γνώση από πλευράς αποστολέα δεν είναι θεμιτή.

Για τους παραπάνω λόγους, στην αρχιτεκτονική του Internet (και σε άλλες αρχιτεκτονικές δικτύων όπως τα ATM), ένα multicast datagram διευθυνσιοδοτείται χρησιμοποιώντας τη μέθοδο *address indirection.* Σύμφωνα με αυτή, ένα μοναδικό αναγνωριστικό (identifier) χρησιμοποιείται για την ομάδα των αποδεκτών και ένα αντίγραφο του πακέτου που προορίζεται για αυτή την ομάδα, παραδίδεται σε όλους τους παραλήπτες που συμμετέχουν στην ομάδα αυτή. Στο internet, αυτό το μοναδικό αναγνωριστικό που προσδιορίζει μια ομάδα αποδεκτών multicast πληροφορίας, είναι μια *Class D multicast IP διεύθυνση*. Η ομάδα αποδεκτών που προσδιορίζεται από μία Class D διεύθυνση, αναφέρεται ως *multicast group*.

Διευθύνσεις IP Multicast

Οι multicast διευθύνσεις προσδιορίζουν μια ομάδα με οποιονδήποτε αριθμό μελών (IP hosts). Οι hosts αυτοί έχουν προσχωρήσει στο multicast group και επιθυμούν να λάβουν την πληροφορία που αποστέλλεται σε αυτό το group [4].

Διευθύνσεις IP Class D

Η Αρχή για την εκχώρηση αριθμών στο Internet (Internet Assigned Numbers Authority - IANA) έχει καθορίσει ότι οι διευθύνσεις Class D (δηλαδή αυτές των οποίων τα πρώτα τέσσερα bit της διεύθυνσης είναι ''1110'') θα χρησιμοποιούνται για το IP Multicast. Αυτό σημαίνει ότι όλες οι διευθύνσεις των multicast groups θα ανήκουν στο εύρος: 224.0.0.0 – 239.255.255.255. Εδώ να σημειώσουμε πως αυτό το εύρος διευθύνσεων προορίζεται μόνο για τις διευθύνσεις των group ή την διεύθυνση προορισμού της ροής IP Multicast. Η διεύθυνση της πηγής (του αποστολέα) των multicast datagrams είναι πάντα η unicast IP διεύθυνσή του.

Επειδή το IP Multicast αναπτύχθηκε κυρίως μετά την αποδοχή από το IETF (Internet Engineering Task Force) των μοντέλων διευθυνσιοδότησης που δεν βασίζονται σε κλάσεις [με σημαντικότερο παράδειγμα το Classless Inter-Domain Routing (CIDR) σύμφωνα με το οποίο η σύνταξη μιας διεύθυνσης είναι της μορφής *192.168.100.1/24*], όλα πρωτόκολλα δρομολόγησης IP Multicast παρέχουν subnet masks στους πίνακες δρομολόγησής τους και συνήθως δεν αναφέρονται στις διευθύνσεις ως Class D [5].

Well-known IP Multicast διευθύνσεις

Η IANA έχει δεσμεύσει συγκεκριμένα εύρη IP διευθύνσεων για γνωστές (well-known) διαδικασίες. Αυτά τα εύρη διευθύνσεων ονομάζονται *permanent host groups* και η έννοιά τους είναι όμοια με τις well-know θύρες TCP και UDP (π.χ. η θύρα 80 προορίζεται για το http).

Reserved Link Local Address

Η IANA έχει δεσμεύσει το εύρος 224.0.0.0 έως 224.0.0.255 για χρήση από δικτυακά πρωτόκολλα σε επίπεδο τοπικού δικτύου. Τα πακέτα σε αυτό το εύρος διευθύνσεων δε θα πρέπει ποτέ να προωθούνται από τον δρομολογητή (router) [4] και θα πρέπει να παραμένουν εντός των ορίων ενός

συγκεκριμένου LAN (Local Area Network). Πάντα αποστέλλονται με τιμή time-to-live (TTL) ίση με 1. Τα διάφορα δικτυακά πρωτόκολλα χρησιμοποιούν αυτές τις διευθύνσεις για αυτόματη αναγνώριση δρομολογητών και για διαχείριση πληροφοριών δρομολόγησης. Ακολουθεί μια σύντομη λίστα με μερικές well-known τοπικές IP διευθύνσεις:

- 224.0.0.1 - Όλα τα συστήματα στο συγκεκριμένο subnet
- 224.0.0.2 - Όλοι οι δρομολογητές στο συγκεκριμένο subnet
- 224.0.0.12 - Dynamic Host Configuration Protocol (DHCP) server/relay agent

Globally Scoped Address

Το εύρος διευθύνσεων 224.0.0.1 έως 224.0.1.255 προορίζεται για ευρύτερη χρήση και οι δρομολογητές θα προωθούν τα αντίστοιχα πακέτα. Αυτές οι διευθύνσεις μπορούν να χρησιμοποιηθούν για την multicast αποστολή δεδομένων μεταξύ οργανισμών αλλά και στο internet.

Για τις δεσμευμένες διευθύνσεις και τις χρήσεις τους, ανατρέξτε στο Παράρτημα Α.

Administratively Scoped Addresses

Οι διευθύνσεις στο εύρος 239.0.0.0 έως 239.255.255.255 καλούνται Administratively Scoped διευθύνσεις και όπως καθορίζεται από το [6], περιορίζονται σε τοπικά δίκτυα και οργανισμούς. Οι διευθύνσεις αυτές μπορούν να θεωρηθούν ανάλογες με το εύρος 10.0.0.0/8 των Class A unicast διευθύνσεων [7].

Αν και η ιδέα του multicast group είναι απλή, γεννά ορισμένα ερωτήματα [3]:

- Πως αρχικοποιείται ένα group και πως τερματίζει η λειτουργία του;
- Πως επιλέγεται η διεύθυνση του group;
- Πως προστίθενται οι νέοι hosts στο group (είτε ως αποστολείς είτε ως αποδέκτες)
- Μπορεί ο οποιοσδήποτε να προσχωρήσει στο group (και να στείλει ή να λάβει από το group) ή η συμμετοχή στο group περιορίζεται και αν ναι, από ποιον;

- Γνωρίζουν τα μέλη του group τις ταυτότητες των υπόλοιπων μελών ως μέρος του network-layered πρωτοκόλλου;
- Πως επικοινωνούν μεταξύ τους οι κόμβοι του δικτύου για να παραδοθεί ένα multicast datagram σε όλα τα μέλη του group;

Για το Internet, τις απαντήσεις σε όλα αυτά τα ερωτήματα δίνει το Internet Group Management Protocol (IGMP) [8], το οποίο θα δούμε στη συνέχεια.

Internet Group Multicast Protocol (IGMP)

Ένα από τα πλεονεκτήματα του IP Multicasting είναι πως η multicast ροή είναι παρούσα μόνο στα subnets όπου ένας ή περισσότεροι hosts τη ζητούν [2]. Πριν την μετάδοση ενός multicast stream σε ένα subnet, ο δρομολογητής χρειάζεται να γνωρίζει αν υπάρχουν hosts σε αυτό το subnet που επιθυμούν να λάβουν το συγκεκριμένο stream. Για τα IP δίκτυα, το Internet Group Multicast Protocol (IGMP) αποτελεί το πρωτόκολλο με το οποίο δημιουργούνται δυναμικά και διατηρούνται οι λίστες με τα group memberships μεταξύ δρομολογητών και hosts.

Το *IGMP Version 1*, το οποίο περιγράφεται στο [10], ήταν η πρώτη ευρέως διαδεδομένη έκδοση του πρωτοκόλλου το οποίο έγινε και Internet Standard. Το *IGMP Version 2*, που περιγράφεται στο [11], εισήγαγε την υποστήριξη για το λεγόμενο "*low leave latency*". Το low leave latency είναι η ελάττωση στο χρόνο που χρειάζεται ένας multicast δρομολογητής για να μάθει πως δεν υπάρχουν πλέον μέλη ενός multicast group σε ένα συγκεκριμένο δίκτυο. Αυτό επιτρέπει στον δρομολογητή να μειώσει (prune) την group list πριν την αποστολή του επόμενου query, και άρα να μειώσει τον χρόνο ο οποίος σπαταλείται σε περιττές μεταδώσεις στο δίκτυο [12]. Το *IGMP Version 3* πρόσθεσε τη δυνατότητα για *"source filtering"*. Source filtering είναι η δυνατότητα ενός συστήματος:

- να ζητά τη λήψη των datagrams από μία και *μόνο* διεύθυνση, όπως απαιτείται για την υλοποίηση των Source-Specific Multicast (SSM). Τα δίκτυα SSM ακριβώς λόγω αυτού του περιορισμού, μειώνουν τις ανάγκες πόρων από το δίκτυο και παρέχουν μεγαλύτερη ασφάλεια.
- να ζητά τη λήψη των datagrams από *οποιανδήποτε* εκτός από συγκεκριμένες διευθύνσεις.

Το IGMP Version 3 είναι σχεδιασμένο για να υποστηρίζει τη συμβατότητα με τις εκδόσεις 1 και 2. Στην πράξη παρ' όλα αυτά, όπως θα δούμε και στο κομμάτι των εφαρμογών, υπάρχουν κάποιες ασυμβατότητες των εκδόσεων μεταξύ λειτουργικών συστημάτων. Το IGMP, το οποίο είναι ανάλογο του Internet Control Message Protocol (ICMP) των unicast επικοινωνιών, αποτελεί

μέρος του IP. Όπως και το ICMP, έτσι και τα IGMP μηνύματα αποστέλλονται encapsulated σε IP datagrams.

Υπάρχουν τρεις τύποι IGMP μηνυμάτων:

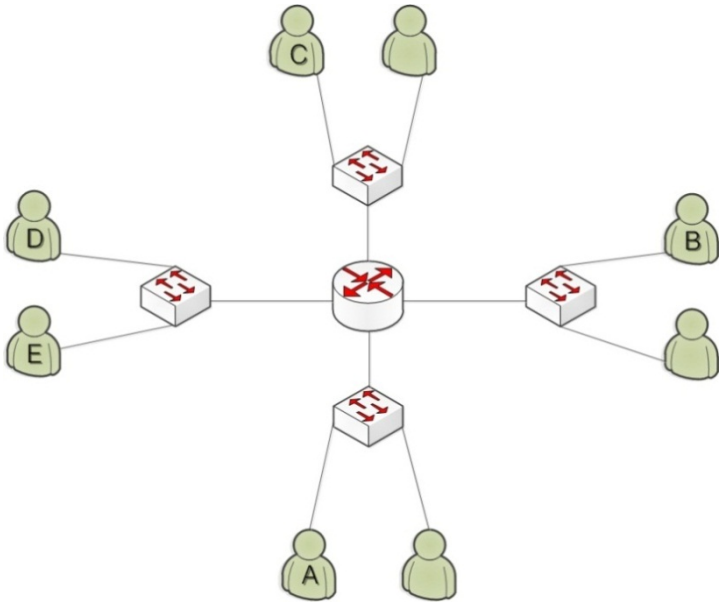
- *Membership Query* – τα μηνύματα αυτά χρησιμοποιούνται από τους multicast-enabled δρομολογητές για την ανακάλυψη μελών των multicast groups στα συνδεδεμένα δίκτυα. Τα Membership Queries στέλνονται στην multicast διεύθυνση 224.0.0.1 δηλαδή προς όλους τους παραλήπτες. Υπάρχουν δύο τύποι Membership Queries:
    - *General Query* το οποίο χρησιμοποιείται για τον προσδιορισμό του πια group έχουν μέλη σε ένα δίκτυο και
    - *Group-Specific Query* με το οποίο προσδιορίζεται αν ένα συγκεκριμένο group έχει συνδεδεμένα μέλη σε ένα δίκτυο
- *Membership Report* – Τα μηνύματα αυτά αποστέλλονται από έναν host όταν κάνει join ένα multicast group αλλά και ως απάντηση στα Membership Queries των multicast-enabled δρομολογητών
- *Leave Group* – Τα μηνύματα αποστέλλονται όταν ένας host αφήνει ένα multicast group. Τα Leave Group μηνύματα αποστέλλονται στην multicast διεύθυνση για όλους τους δρομολογητές (224.0.0.2). Στη συνέχεια ο δρομολογητής στέλνει ένα *group-specific membership query* στο δίκτυο για να επιβεβαιώσει αν έχει αποχωρήσει και το τελευταίο μέλος ενός multicast group.

Multicast σε switched περιβάλλον

Σε ένα περιβάλλον όπου χρησιμοποιούνται multicast-enabled δρομολογητές, η διαδικασία θα κυλά ομαλά και κάθε client θα λαμβάνει το multicast stream το οποίο ζήτησε μέσω των IGMP μηνυμάτων. Στην περίπτωση ενός switched (bridged) περιβάλλοντος (Layer 2), πρέπει να λάβουμε υπ' όψιν τους ακόλουθους περιορισμούς. Τα περισσότερα switched (bridges) είναι αυστηρώς Layer 2 συσκευές που εξετάζουν αποκλειστικά τις MAC διευθύνσεις [2]. Αγνοούν δηλαδή τα IGMP μηνύματα (τα οποία είναι Layer 3) και δεν γνωρίζουν ποια multicast group και streams οι hosts στις ports τους θέλουν να λάβουν. Υπό αυτό τον εγγενή περιορισμό, η προώθηση της

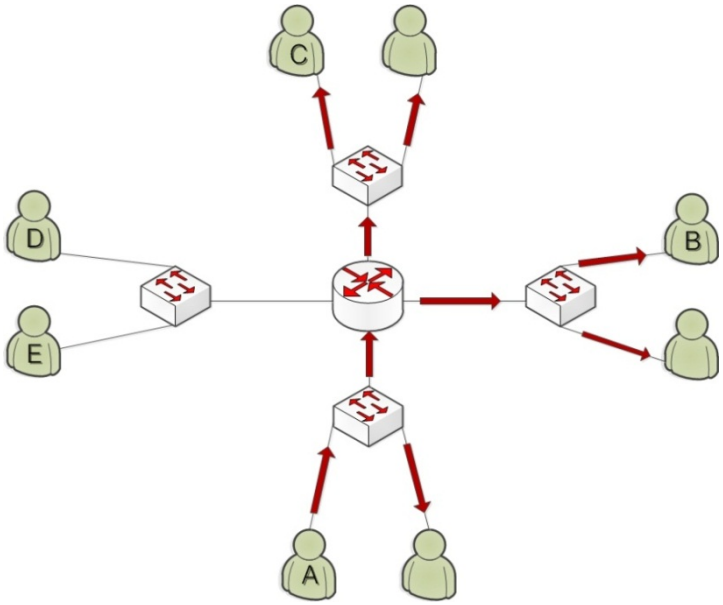
οποιασδήποτε κίνησης γίνεται προς όλες τις ports, *μετατρέποντας ουσιαστικά την multicast κίνηση σε broadcast* και αναιρώντας τον σκοπό του switch που είναι να περιορίζει την κίνηση στις ports που χρειάζονται τα δεδομένα. Τα σχήματα 3 και 4 απεικονίζουν το πρόβλημα του multicast σε switched περιβάλλον.

Έστω λοιπόν ότι έχουμε το παρακάτω δίκτυο με έναν router στο κέντρο και τέσσερα switches περιμετρικά να συνδέουν τους 8 χρήστες:



Σχήμα 3

Ας υποθέσουμε ότι ο χρήστης A είναι ο αποστολέας της Multicast ροής σε κάποια multicast διεύθυνση και οι χρήστες B και C συντονίζονται στο αντίστοιχο multicast group για να λάβουν τη ροή. Ο κεντρικός δρομολογητής όντας Layer 3 συσκευή θα προωθήσει σωστά τη ροή μόνο στα τμήματα του δικτύου στα οποία υπάρχουν hosts που τη ζήτησαν, αναλύοντας τα IGMP queries. Όταν όμως η multicast ροή φτάσει στα αντίστοιχα υποδίκτυα, τα Layer 2 switches προωθήσουν την ροή σε όλους τους hosts που υπάρχουν στις θύρες τους:



Σχήμα 4

Προφανώς σε ένα μεγαλύτερο δίκτυο, η παραπάνω διαδικασία θα οδηγήσει σε τεράστιες σπατάλες πόρων. Για την επίλυση αυτού του ζητήματος έχουν αναπτυχθεί ορισμένες μέθοδοι τις οποίες θα δούμε στη συνέχεια.

Μετατρέποντας τα Switches σε Multicast-Aware

Επειδή τα IGMP μηνύματα ελέγχου μεταδίδονται ως multicast πακέτα, δεν είναι διαχωρίσιμα από τα multicast δεδομένα στο Layer 2. Για την επίλυση αυτού του ζητήματος, έχουν αναπτυχθεί οι παρακάτω μέθοδοι [5]:

IGMP Snooping

Αυτή η τεχνική είναι εύκολη στην υλοποίηση της αλλά δύναται να υστερεί σε επίπεδο υποστήριξης, κυρίως από lower-end switches. Η προσέγγιση αυτής της μεθόδου προϋποθέτει πως το switch αποκωδικοποιεί το IP header (πληροφορία Layer 3) αναλύοντας το πεδίο “protocol” του IP datagram (για λεπτομέρειες σχετικά με τη δομή του πεδίου “protocol” και του IP datagram ανατρέξτε στο Παράρτημα Β’) ώστε να διαχωρίσει τα μηνύματα IGMP από την κανονική multicast κίνηση. Δίχως κάποια υποστήριξη σε επίπεδο hardware (Application-Specific Integrated Circuit - ASIC), αυτή η επιπλέον διαδικασία αποκωδικοποίησης μπορεί να αποδειχθεί πολύ ‘’βαριά’’ για τις επεξεργαστικές δυνατότητες ενός switch. Στην πράξη, το IGMP Snooping μπορεί να οδηγήσει σε αυθαίρετη απόρριψη πακέτων από το switch, ιδίως όταν υπάρχει αυξημένη multicast κίνηση. Παρ’ όλα αυτά, με τη χρήση του

κατάλληλου hardware το IGMP Snooping αποτελεί μια αξιόπιστη λύση. Επίσης τα snooping switches χρειάζεται να προσδιορίζουν τις ports στις οποίες είναι συνδεδεμένοι οι routers ώστε να γνωρίζουν που να στείλουν τα πακέτα [15]. Αυτό επιτυγχάνεται χρησιμοποιώντας:

- το πρωτόκολλο Multicast Router Discovery Protocol (MRDP) [16],
- αναλύοντας συγκεκριμένα IGMP queries [17] ή
- με manual ρύθμιση του switch

Η δυνατότητα του Snooping είναι διαθέσιμη σε μια μεγάλη ποικιλία από mid-ως-high end switches.

Το *IGMP proxying* [18] χρησιμοποιείται ορισμένες φορές είτε για την αντικατάσταση κάποιου multicast routing πρωτοκόλλου σε μικρά routers, είτε για την ανάλυση IGMP μηνυμάτων όταν χρησιμοποιείται μαζί με το IGMP Snooping.

Cisco's Group Management Protocol (CGMP)

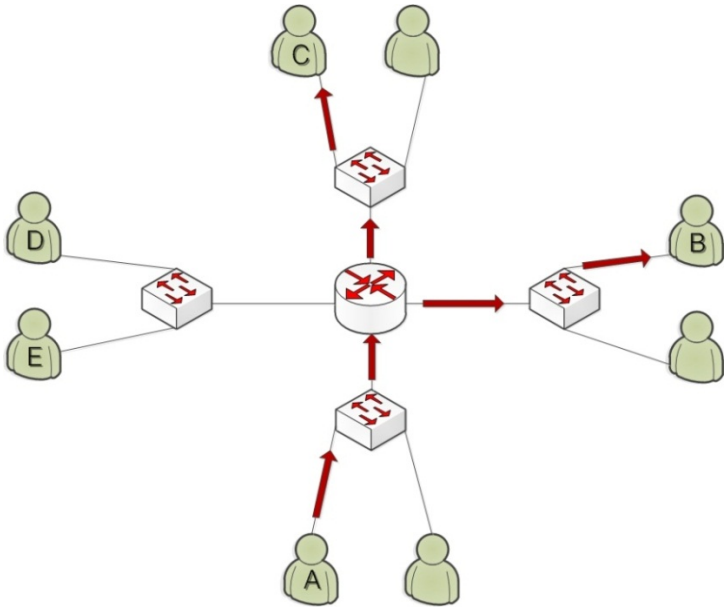
Η δεύτερη προσέγγιση, το CGMP, είναι μια proprietary λύση από τη Cisco και περιλαμβάνει τη χρήση ενός πρωτοκόλλου για την router-to-switch αποστολή των multicast group πληροφοριών. Η mid-to-high σειρά Catalyst των switches Cisco μπορεί να λαμβάνει multicast group join/leave μηνύματα από έναν multicast enabled δρομολογητή (σειρές 6000, 7000 κτλ.). Αυτά τα join/leave μηνύματα με τη σειρά τους χρησιμοποιούνται από τα switches για τη βελτιστοποίηση του multicast filtering. Το CGMP προσφέρει μηνύματα όπως "Add Port to Group," "Delete Port from Group," "Assign Router Port," "De-assign Router Port," "Delete Group," και "Delete All Groups."

Group Address Resolution Protocol (GARP)

Μια Τρίτη προσέγγιση είναι το πρωτόκολλο GARP της IEEE, βασικός σκοπός του οποίου είναι να συντηρεί πληροφορίες για groups σε επίπεδο Virtual LAN (VLAN). Το GARP μπορεί να επεκταθεί για να υποστηρίζει λίστες οι οποίες επιτρέπουν στο switch την αντιστοίχιση (mapping) των multicast groups σε συγκεκριμένες ports με τρόπο ανάλογο με τον οποίο ένα VLAN κρατά μια λίστα με MAC διευθύνσεις οι οποίες ανήκουν σε ένα συγκεκριμένο broadcast domain.

Αν και σε γενικές γραμμές οι παραπάνω τεχνικές έχουν αναπτυχθεί αρκετά, η δημοφιλέστερη είναι το CGMP κυρίως λόγω του μεγάλου αριθμού των υπαρχουσών υποδομών που χρησιμοποιούν multicast-enabled τεχνολογίες της Cisco. Ακολουθεί το IGMP Snooping με απόσταση από το GARP της IEEE για το οποίο χρειάζεται να γίνει πολύ δουλειά ώστε να θεωρηθεί αξιόπιστη λύση.

Σε συνέχεια του παραδείγματος με τους 8 χρήστες, όλες οι παραπάνω μέθοδοι στοχεύουν στην υλοποίηση του παρακάτω σχήματος (Σχήμα 5), όσον αφορά την σωστή παράδοση της multicast ροής στους hosts που την έχουν ζητήσει (υπενθυμίζουμε πως αποστολέας είναι ο host A ενώ παραλήπτες οι B και C):



Σχήμα 5

Multicast Δέντρα διανομής και Προώθηση

Δέντρα διανομής (Distribution Trees)

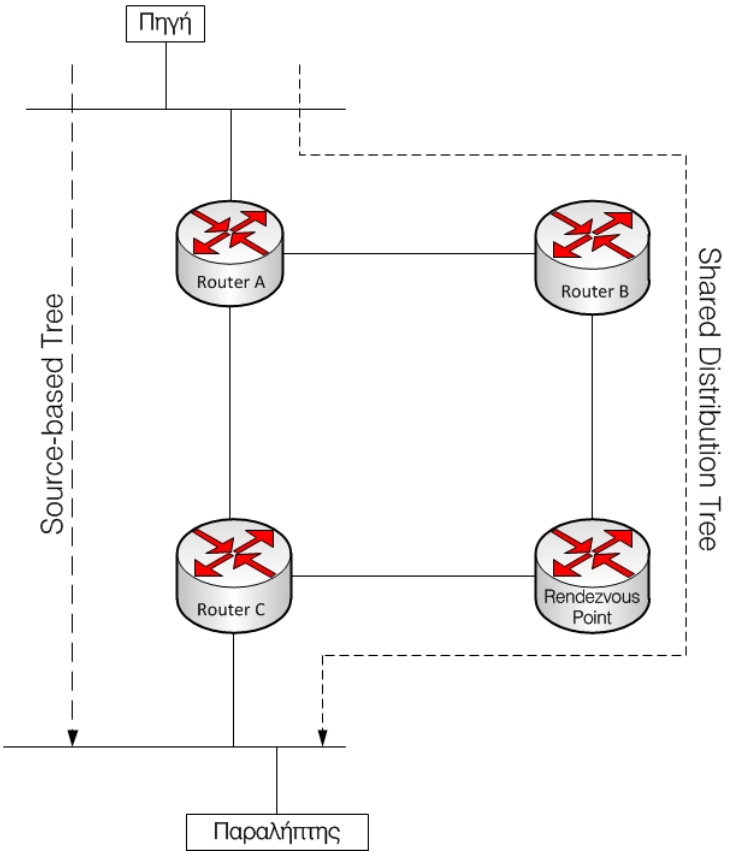
Οι multicast-capable δρομολογητές δημιουργούν δέντρα διανομής τα οποία ελέγχουν τη ροή της multicast πληροφορίας μέσω του δικτύου μέχρις ότου αυτή παραδοθεί σε όλους τους αποδέκτες [13]. Η δομή των δέντρων διανομής μπορεί να είναι είτε *source-based* είτε *shared distribution trees*.

Δομή Δέντρων Διανομής

Τα *source-based* δέντρα διανομής φτιάχνουν ένα βέλτιστο δέντρο *συντομότερου μονοπατιού* (optimal shortest-path tree) με ρίζα την πηγή της multicast ροής. Κάθε ζεύγος πηγής/group απαιτεί τη δική του πληροφορία κατάστασης (state information) το οποίο στη βιβλιογραφία συναντάται ως ''(S,G)'' [19] όπου το S αναφέρεται στην IP διεύθυνση της πηγής και το G στην διεύθυνση του multicast group. Έτσι, για groups με μεγάλο αριθμό πηγών ή για δίκτυα με μεγάλο αριθμό multicast groups όπου το κάθε group έχει μεγάλο αριθμό πηγών, η χρήση των source-based δέντρων μπορεί να οδηγήσει σε κορεσμό των αποθηκευτικών δυνατοτήτων των δρομολογητών.

Τα *shared distribution trees* δημιουργούνται γύρω από ένα κεντρικό δρομολογητή ο οποίος ονομάζεται *rendezvous point* [20] ή πυρήνας (core) από όπου κατανέμεται όλη η multicast ροή ανεξάρτητα από την τοποθεσία των πηγών. Το πλεονέκτημα των shared distribution trees είναι ότι δεν δημιουργούν μεγάλο αριθμό πληροφοριών κατάστασης (state information) στους δρομολογητές. Το μειονέκτημα είναι ότι το μονοπάτι από μία πηγή προς τους παραλήπτες μπορεί να είναι αρκετά μεγαλύτερο, κάτι το οποίο μπορεί να έχει σοβαρή επίπτωση για εφαρμογές ευαίσθητες στις καθυστερήσεις, για παράδειγμα μια live τηλεοπτική μετάδοση. Ακόμα, οι rendezvous δρομολογητές μπορεί να γίνουν σημεία traffic bottleneck αν υπάρχουν πολλές high data rate πηγές [21], όπως για παράδειγμα ένα High Definition τηλεοπτικό κανάλι (το οποίο εύκολα μπορεί να φτάσει τα 12 Mbps).

Το σχήμα 6 απεικονίζει τις παραπάνω δομές δέντρων:



Σχήμα 6 – Δομές δέντρων διανομής

Κατανομή Παραληπτών

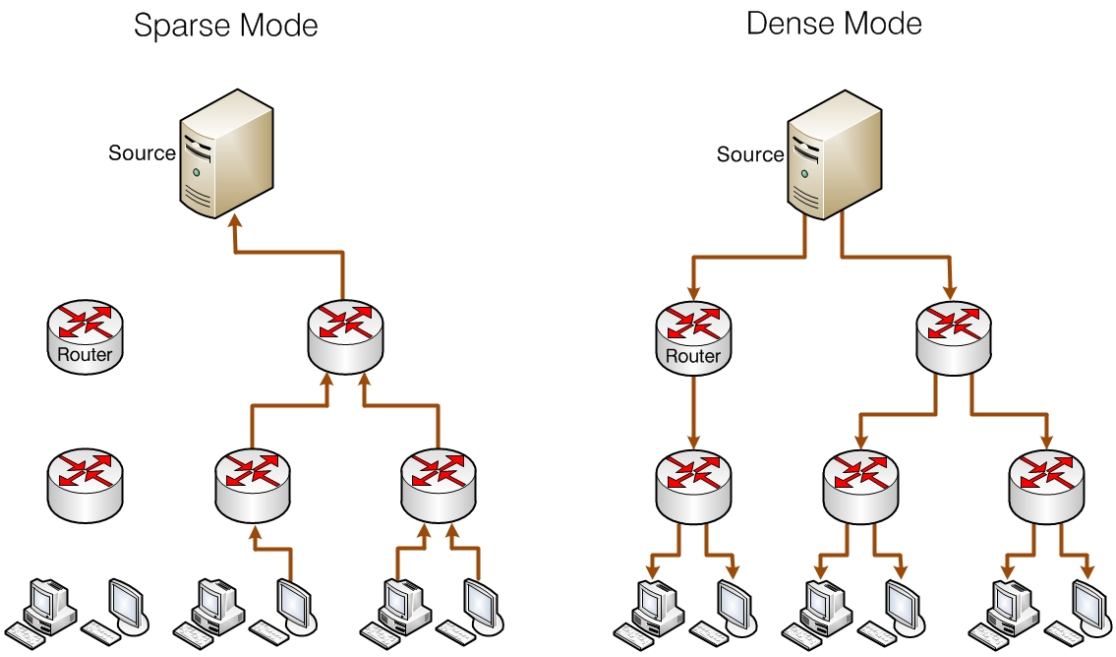
Ένα κριτήριο για την επιλογή ενός από τους δύο τύπους δέντρων, είναι το αν οι παραλήπτες είναι αραιά (sparse) ή πυκνά (dense) κατανεμημένοι μέσα στο δίκτυο (για παράδειγμα αν σχεδόν όλοι οι routers του δικτύου έχουν μέλη των multicast groups συνδεδεμένα στα ακριβώς γειτονικά τους υποδίκτυα) [21]. Αν το δίκτυο έχει παραλήπτες σε κάθε subnet ή οι παραλήπτες είναι χωρικά κοντά, τότε έχουν πυκνή κατανομή, Αν οι παραλήπτες βρίσκονται μόνο σε ορισμένα subnet ή είναι χωρικά μακριά μεταξύ τους, τότε έχουν αραιή κατανομή. Ο αριθμός τω παραληπτών δεν έχει σημασία. Ο *καθοριστικός παράγοντας είναι το πόσο κοντά είναι οι παραλήπτες μεταξύ τους αλλά και την πηγή*.

Τα *sparse-mode* πρωτόκολλα χρησιμοποιούν "join" μηνύματα για τη δημιουργία των δέντρων διανομής έτσι ώστε η κατάσταση και *οι λίστες των δέντρων να βρίσκονται μόνο στους routers του κατανεμημένου δέντρου* και τα πακέτα δεδομένων να προωθούνται μόνο στα LANs στα οποία βρίσκονται οι

παραλήπτες (η αρχικοποίηση της διαδικασίας ξεκινά από τους παραλήπτες). Έτσι τα sparse-mode πρωτόκολλα είναι κατάλληλα για μεγάλα δίκτυα όπου τα dense-mode πρωτόκολλα θα σπαταλούσαν bandwidth με το να προωθούν τα πακέτα σε όλα τα μέρη του δικτύου και εκ των υστέρων να κόβουν (prune) τις ανεπιθύμητες συνδέσεις. Τα sparse-mode πρωτόκολλα χρησιμοποιούν είτε shared είτε source-based δέντρα ή ακόμα και συνδυασμό των δύο. Τα sparse-mode πρωτόκολλα μπορούν να παρομοιαστούν με μία συνδρομή ενός περιοδικού, καθώς τα δέντρα διανομής *δεν* θα δημιουργηθούν ποτέ αν ο παραλήπτης (συνδρομητής) *δεν* κάνει join στο group [21].

Τα *dense-mode* πρωτόκολλα δημιουργούν μόνο source-based δέντρα διανομής. Τα dense-mode πρωτόκολλα καθορίζουν την κατανομή των παραληπτών με το flooding δεδομένων σε ολόκληρο το δίκτυο (ξεκινώντας από την πηγή, σε αντίθεση με τα sparse-mode) και έπειτα με την απομάκρυνση (pruning off) των τμημάτων του δικτύου που δεν περιλαμβάνουν παραλήπτες. Έτσι, *δημιουργούνται και κρατούνται πληροφορίες κατανομής σε όλους τους δρομολογητές του δικτύου* (σε αντίθεση με τα sparse-mode πρωτόκολλα που είδαμε προηγουμένως). Τα dense-mode πρωτόκολλα χρησιμοποιούν λιγότερα μηνύματα ελέγχου για την δημιουργία των λιστών κατάστασης από τα sparse-mode και μπορούν να είναι πιο αξιόπιστα ως προς τη παράδοση τα των δεδομένων τουλάχιστον σε ορισμένα μέλη των multicast group σε περίπτωση κάποιας αποτυχίας του δικτύου. Τα dense-mode πρωτόκολλα μπορούν να παρομοιαστούν με την ανεπιθύμητη αλληλογραφία (junk mail) με την έννοια ότι κάθε δίκτυο θα λάβει ένα αντίγραφο της πληροφορίας είτε το επιθυμεί είτε όχι.

Το Σχήμα 7 απεικονίζει την διαδικασία δημιουργίας των δέντρων σε sparse και dense mode:



Σχήμα 7 – Sparse και Dense δέντρα

Multicast Forwarding

Στο unicast forwarding, η δρομολόγηση της κίνησης στο δίκτυο γίνεται πάνω σε ένα μόνο μονοπάτι, από την πηγή στον προορισμό. Ένας unicast δρομολογητής δεν ενδιαφέρεται για την διεύθυνση της πηγής, παρά μόνο για τη διεύθυνση προορισμού και πώς να προωθήσει την κίνηση προς αυτό τον προορισμό. Ο router κάνει αναζήτηση στον πίνακα δρομολόγησής του και έπειτα προωθεί ένα αντίγραφο του unicast πακέτου προς την κατεύθυνση του προορισμού.

Στο multicast routing, η πηγή στέλνει την ροή προς ένας αυθαίρετο αριθμό group και μελών ο οποίος αντιπροσωπεύεται από την διεύθυνση του multicast group. Ο multicast δρομολογητής πρέπει να προσδιορίσει ποια κατεύθυνση είναι η upstream (προς την πηγή) και ποια ή ποιες η downstream. Αν υπάρχουν πολλαπλά downstream μονοπάτια, ο δρομολογητής δημιουργεί αντίγραφα (replicates) των πακέτων και προωθεί την κίνηση στα αντίστοιχα downstream paths. Η μέθοδοι προώθησης της multicast κίνησης *από την πηγή* και όχι *προς τον παραλήπτη* (όπως γίνεται στο unicast forwarding) βασίζονται στο *reverse path forwarding* (RPF).

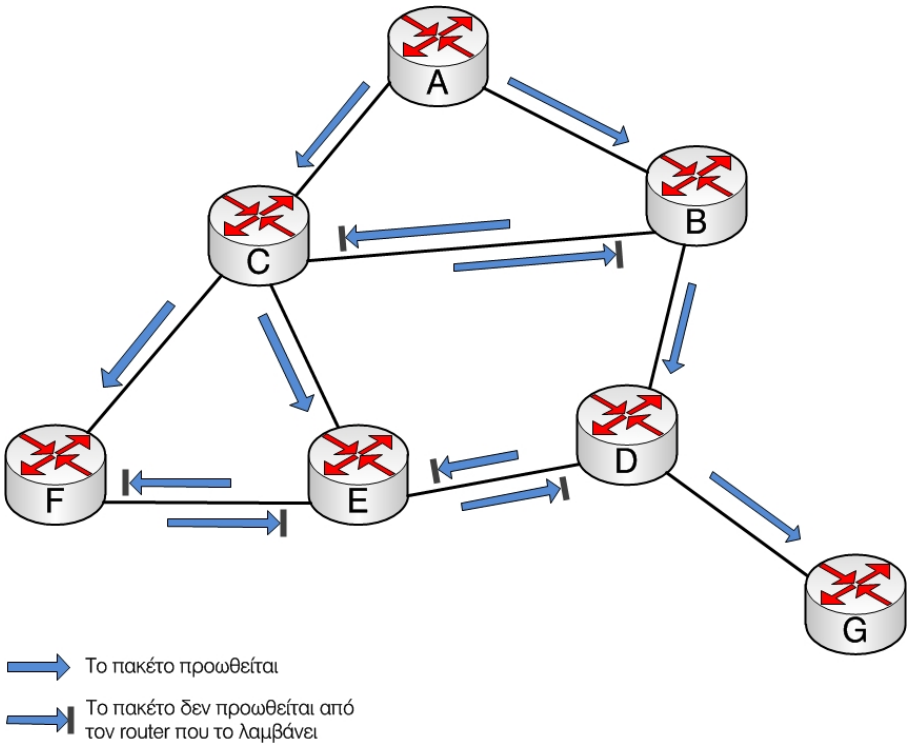
Reverse Path Forwarding

Η ιδέα πίσω από το RPF αν και απλή δεν παύει να είναι αποτελεσματική [3]. Η ιδέα αυτή είναι η εξής:

Όταν ένας δρομολογητής λαμβάνει ένα broadcast πακέτο με μία συγκεκριμένη διεύθυνση αποστολέα, αναμεταδίδει το πακέτο σε όλα τα εξερχόμενα link του (εκτός από αυτό στο οποίο αρχικά το έλαβε) μόνο αν το πακέτο που έφτασε αρχικά στο link, ανήκει στο δικό του συντομότερο (unicast) μονοπάτι προς την πηγή.

Διαφορετικά, ο δρομολογητής απλά απορρίπτει το εισερχόμενο πακέτο χωρίς να το προωθεί σε κανένα από τα εξερχόμενα link του. Η απόρριψη του πακέτου μπορεί να γίνει διότι ο δρομολογητής γνωρίζει ότι είτε ότι θα το λάβει είτε ότι το έχει ήδη λάβει στο link το οποίο ανήκει στο δικό του συντομότερο μονοπάτι προς τον αποστολέα.

Το Σχήμα 8 απεικονίζει τη λειτουργία του RPF [3]. Ας υποθέσουμε ότι οι σύνδεσμοι (μαύρες γραμμές) αναπαριστούν τα συντομότερα μονοπάτια από τους παραλήπτες προς την πηγή (router A). Αρχικά, ο κόμβος A κάνει broadcast ένα source-A πακέτο προς τους κόμβους B και C. Ο κόμβος B θα προωθήσει το source-A πακέτο που έλαβε από τον A προς τους κόμβους C και D, καθώς ο A ανήκει στο δικό του συντομότερο μονοπάτι προς τον A. Ο κόμβος B θα αγνοήσει (δηλαδή θα απορρίψει χωρίς να προωθήσει) οποιαδήποτε source-A πακέτα λάβει από οποιονδήποτε άλλο κόμβο, για παράδειγμα τους C ή D). Στη συνέχεια, ο κόμβος C, ο οποίος θα λάβει ένα source-A πακέτο απ' ευθείας από την πηγή A καθώς και από τον κόμβο B. Επειδή ο B δεν ανήκει στο συντομότερο μονοπάτι του C προς τον A, ο C θα αγνοήσει οποιοδήποτε source-A πακέτο λαμβάνει από το B. Από την άλλη, όταν ο C λάβει ένα source-A πακέτο απ' ευθείας από τον A, θα το προωθήσει στους κόμβους B, E και F.



Σχήμα 8 – Reverse Path Forwarding

Πρωτόκολλα δρομολόγησης IP Multicast

Τα πρωτόκολλα της multicast δρομολόγησης διακρίνονται σε δύο κατηγορίες: στα Dense-mode (DM) και Sparse-mode (SM). Τα DM πρωτόκολλα βασίζονται στην υπόθεση πως σχεδόν όλοι οι routers στο δίκτυο θα πρέπει να κατανείμουν την multicast ροή για κάθε multicast group (για παράδειγμα, όλοι οι hosts στο δίκτυο ανήκουν σε κάθε multicast group). Κατά συνέπεια, τα DM πρωτόκολλα δημιουργούν δέντρα διανομής ξεκινώντας με το flooding ολόκληρου του δικτύου και ύστερα με την απομάκρυνση (pruning) των, λίγων σε αριθμό, μονοπατιών χωρίς αποδέκτες. Τα SM πρωτόκολλα βασίζονται στην υπόθεση πως σχετικά λιγότερη δρομολογητές στο δίκτυο θα αναμειχθούν σε κάθε multicast και οι hosts που ανήκουν στα groups είναι εκτενώς διεσπαρμένοι, όπως πιθανότατα είναι αυτό που συμβαίνει για τα περισσότερα multicasts στο internet. Ως εκ τούτου, τα SM πρωτόκολλα ξεκινούν με ένα άδειο δέντρο διανομής και προσθέτουν κόμβους μόνο εφόσον έχουν δεχτεί requests από hosts για να συμμετάσχουν στην διανομή της multicast ροής. Τα DM πρωτόκολλα είναι καταλληλότερα για LAN περιβάλλοντα, καθώς αυτά παρέχουν τόσο την πυκνή κατανομή παραληπτών όσο και το απαραίτητο bandwidth για να ανεχτούν το flooding. Αντίστοιχα τα SM πρωτόκολλα είναι γενικά πιο κατάλληλα για WAN περιβάλλοντα [22].

Distance Vector Multicast Routing Protocol (DVMRP): Το DVMRP [23] ήταν το πρώτο πρωτόκολλο που σχεδιάστηκε για multicasting. Για την αποφυγή των αρχικών δυσκολιών υλοποίησης, υποστήριζε δυνατότητες tunneling, οι οποίες ήταν μέρος της multicast τοπολογίας του [24]. Το DVMRP χρησιμοποιεί source-based δέντρα με reverse path forwarding (RPF) και pruning [3]. Πλέον το DVMRP δεν χρησιμοποιείται πολύ συχνά καθώς έχει αντικατασταθεί από το πρωτόκολλο PIM-SM. Η πιο τυπική εφαρμογή του DVMRP είναι στα leaf networks για την προώθηση της κίνησης από ένα firewall που υποστηρίζει μόνο DVMRP, προς το εσωτερικό δίκτυο. Επιπλέον, επειδή το Generic Routing Encapsulation (GRE) [25] tunneling της Cisco έχει αποδειχτεί πιο λειτουργικό από το DVMRP, είναι σχετικά περιορισμένη η χρήση του, εκτός από τη συντήρησή του στα παλαιότερα συστήματα που το χρησιμοποιούν.

Protocol-Independent Multicast (PIM): Το PIM πρωτόκολλο δρομολόγησης, αποτελείται από δύο επιμέρους πρωτόκολλα, τα PIM Dense Mode (PIM-DM το οποίο πιθανότατα είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο multicast δρομολόγησης) και το PIM Sparse Mode (PIM-SM) [26]. Το PIM-SM [27] περιλαμβάνει τις λειτουργίες:

- *Any Source Multicast (ASM),* στην οποία μπορούν να υπάρχουν πολλαπλοί αποστολείς στο ίδιο group και
- *Source-Specific Multicast (SSM)* στην οποία καθορίζεται μία συγκεκριμένη πηγή για κάθε group.

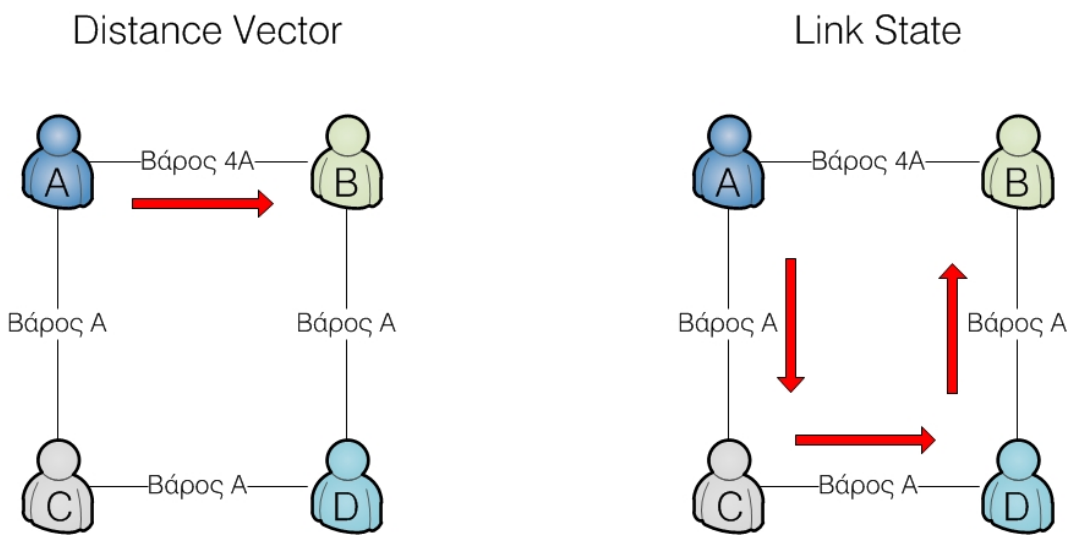
Το PIM-SSM είναι ένα υποσύνολο του PIM-SM το οποίο δεν χρησιμοποιεί Rendezvous Points (RPs) παρά προϋποθέτει πως ο παραλήπτης γνωρίζει το ζεύγος τιμών Πηγή/Group (S,G). Οι πιο πρόσφατες πλατφόρμες δρομολόγησης υποστηρίζουν PIM-SM [24]. Ενώ το PIM-SM έχει σχεδιαστεί για να αποφεύγει τα περιττά flooding των multicast δεδομένων, το PIM-DM [28] βασίζεται στην υπόθεση πως σχεδόν όλα τα subnets έχουν τουλάχιστον έναν παραλήπτη για κάποιο group. Το PIM-DM κάνει flood των multicast δεδομένων μέσα στο δίκτυο (παρόμοια με την μέθοδο “flood και prune” RPF που χρησιμοποιεί και το DVMRP) εκτός αν κάποια μέρη του δικτύου ενημερώνουν περιοδικά ότι δεν ενδιαφέρονται για το συγκεκριμένο group. Το PIM-DM είναι συνήθως αποδεκτό για ένα μικρό ή απλό δίκτυο στο οποίο η εγκατάσταση ενός Rendezvous Point θα ήταν περιττή και πιθανώς σε περιπτώσεις όπου ένα μεγάλο ποσοστό των χρηστών αναμένεται να θέλουν να λαμβάνουν τη ροή, έτσι ώστε η ποσότητα της πληροφορίας την οποία πρέπει να διατηρεί το δίκτυο ελαχιστοποιείται. Αρκετές υλοποιήσεις περιλαμβάνουν τη λεγόμενη “sparse-dense” λειτουργία, στην οποία το Sparse Mode είναι η προεπιλογή, αλλά το Dense Mode χρησιμοποιείται για προκαθορισμένα εύρη multicast group μόνο. Τελευταία , πολλά δίκτυα έχουν μεταπηδήσει από το sparse-dense mode σε sparse mode αποκλειστικά.

Bidirectional PIM: Το Bidir-PIM [29] είναι ένα πρωτόκολλο multicast δρομολόγησης, το οποίο εγκαθιστά ένα κοινόχρηστο μονοπάτι για όλες τις πηγές με μία μόνο ρίζα. Μπορεί να χρησιμοποιηθεί ως εναλλακτικό του PIM-SM μέσε σε ένα μόνο domain. Δεν προσφέρει data-driven events ή data-

encapsulation. Καθώς δεν κρατά πληροφορίες κατάστασης της πηγής, μπορεί να αποτελεί μία καλή λύση ιδίως σε δίκτυα με μεγάλο αριθμό πηγών. Αυτή τη στιγμή, δεν υπάρχει inter-domain λύση για τη χρήση bidirectional PIM σε ένα εύρος group.

Multicast Open Shortest Path First (MOSFP): Το πρωτόκολλο MOSFP [30] είχε αναπτυχθεί από διάφορες εταιρείες και είχε κάποια ανάπτυξη στα intra-domain δίκτυα. Το MOSFP βασίζεται στο *intra*-domain πρωτόκολλο Open Shortest Path First (OSPF) [31] το οποίο με τη σειρά του χρησιμοποιεί τη μία από τις δύο κύριες κατηγορίες πρωτοκόλλων δρομολόγησης, την *link state* (με τη δεύτερη να είναι τα *distance-vector* πρωτόκολλα). Σε αυτά τα πρωτόκολλα οι αλγόριθμοι δημιουργούν σε κάθε κόμβο, έναν ‘’χάρτη’’ διασύνδεσης του δικτύου με τη μορφή γραφήματος στο οποίο φαίνεται ποιοι κόμβοι συνδέονται με ποιους. Βάσει αυτού του χάρτη κάθε κόμβος υπολογίζει ξεχωριστά το βέλτιστο μονοπάτι σε κάθε δυνατό προορισμό του δικτύου. Αυτά τα βέλτιστα μονοπάτια αποτελούν τον *πίνακα δρομολόγησης* του κάθε κόμβου. Η διαφορά των link state πρωτοκόλλων με τα distance-vector είναι ότι στα δεύτερα, κάθε κόμβος μοιράζεται τον πίνακα δρομολόγησής του με τους γειτονικούς του κόμβους. Ακριβώς επειδή το MOSFP χρησιμοποιεί τους link-state αλγόριθμους, δεν είναι εύκολο να αναπτυχθεί σε *inter*-domain δίκτυα και για αυτό δεν έχει τύχει ευρείας αποδοχής από τους διαχειριστές δικτύων οι οποίοι προτιμούν τη χρήση ενός και μόνο πρωτοκόλλου τόσο για intra όσο και για inter domain δίκτυα.

Το σχήμα 9 δίνει μια απλουστευμένη απεικόνιση της λειτουργίας των link state και distance vector πρωτοκόλλων [34]. Στο σχήμα αυτό βλέπουμε πως αν χρησιμοποιηθεί το πρωτόκολλο Distance Vector, το route μεταξύ των κόμβων A και B που θα επιλεγεί είναι το 4A, παρόλο που έχει μεγαλύτερο βάρος από το A C D B. Αντίθετα, το πρωτόκολλο Link State, κρατώντας σε κάθε κόμβο το routing table με τα βέλτιστα μονοπάτια προς κάθε δυνατό προορισμό, θα επιλέξει το μονοπάτι A C D B καθότι έχει μικρότερο βάρος από το A B. Στο συγκεκριμένο παράδειγμα είναι προτιμότερη η χρήση του Link State. Αν όμως όλα τα μονοπάτια είχα το ίδιο βάρος, τότε η χρήση του Distance Vector θα αποτελούσε προφανώς καλύτερη προσέγγιση.



Σχήμα 9 – Distance Vector και Link State πρωτόκολλα δρομολόγησης

Border Gateway Multicast Protocol (BGMP): Το πρωτόκολλο BGMP [32] δεν είχε την απαραίτητη υποστήριξη από την κοινότητα των service providers ώστε να οδηγηθεί προς τα standards της IETF. Δεν υπάρχουν αναφορές εμπορικής υλοποίησης και ανάπτυξης.

Το πρωτόκολλο *Core Based Trees (CBT)* [33] ήταν ένα ακαδημαϊκό project το οποίο παρείχε την βάση για τα κοινόχρηστα δέντρα διανομής του PIM Sparse Mode. Από τη στιγμή που τα κοινόχρηστα δέντρα διανομής εισήχθησαν στις PIM υλοποιήσεις, δεν υπήρχε λόγος εμπορικής ανάπτυξης του CBT.

Ο πίνακας 1 δίνει μια συνοπτική περίληψη της τρέχουσας κατάστασης των παραπάνω τεχνολογιών:

	Inter-Domain	Intra-Domain	Κατάσταση
PIM-SM	Ναι	Ναι	Ενεργό
PIM-DM	Όχι πλέον	Όχι πλέον	Περιορισμένη χρήση
BIDIR-PIM	Όχι	Ναι	Υπό Ανάπτυξη
DVMRP	Όχι πλέον	Μόνο σε υπάρχοντα συστήματα	Αποσύρεται
MOSFP	Όχι	Όχι πλέον	Ανενεργό
CBT	Όχι	Όχι	Δεν υπήρξε ανάπτυξη
BGMP	Όχι	Όχι	Δεν υπήρξε ανάπτυξη

Πίνακας 1

Στατική Multicast δρομολόγηση (mroutes): Οι περισσότερες εταιρείες, μαζί με τον συνδυασμό κάποιον από τα παραπάνω IP-Multicast πρωτόκολλα δρομολόγησης, υλοποιούν και μεθόδους εισαγωγής στατικών πληροφοριών δρομολόγησης και προώθησης. Κάτι τέτοιο μπορεί να γίνει, για παράδειγμα, χρησιμοποιώντας την κονσόλα διαχείρισης του δρομολογητή για την απ' ευθείας ρύθμισης του ποια interfaces εισερχόμενης ροής επικοινωνούν με τις multicast πηγές και ποια interfaces εξερχόμενης ροής συνδέονται με το multicast group. Αν και σε αυτή την περίπτωση είναι απαραίτητη μια "brute force" προσέγγιση και απαιτούνται πολλές ώρες ρύθμισης και συντήρησης, η μέθοδος της στατικής δρομολόγησης είναι η πιο αξιόπιστη κάτω από συγκεκριμένα σενάρια και ως επί το πλείστον, σε περιπτώσεις αναγκών αυξημένης ασφάλειας (όπως firewall-to-internet, ασφαλείς περιοχές εταιρικού δικτύου, τεχνικών anti-hack και anti-spoofing και άλλα). Η Cisco αναφέρεται στη βιβλιογραφία της για τη στατική multicast δρομολόγηση, ως *mroutes*.

Multicast σε ασύρματα δίκτυα

Η σταθερότητα της τρέχουσας δομής του internet, οφείλεται σε μεγάλο βαθμό στον End-to-End μηχανισμό ελέγχου συμφόρησης (congestion control) που παρέχει το Transmission Control Protocol (TCP) [35]. Σήμερα, το TCP κυριαρχεί στο internet και αναπαριστά το 90% της κίνησης.

Με την ραγδαία αύξηση τον εφαρμογών multimedia, μια μεγάλη ποικιλία τέτοιον εφαρμογών (όπως το video conferencing, το broadcasting ειδήσεων, τα κατανεμημένα παιχνίδια και το e-learning) βασίζεται στο User Datagram Protocol (UDP) το οποίο δεν παρέχει τον έλεγχο συμφόρησης του αλλά και τους μηχανισμούς αξιόπιστης μετάδοσης του TCP. Η καλύτερη επιλογή για εφαρμογές που απαιτούν συνεργατική επικοινωνία είναι το multicasting διότι μπορεί να μεταδώσει παράλληλα και αποδοτικά τα multimedia δεδομένα σε πολλαπλούς χρήστες. Παρ' όλα αυτά, οι IP multicast εφαρμογές βασίζονται στην *best effort* παράδοση, η οποία δεν παρέχει καμία εγγύηση για αξιόπιστη μετάδοση δεδομένων ή quality of service.

Επιπλέον, τα πρότυπα IEEE 802.11 υποστηρίζουν την multicast μετάδοση απλώς με το broadcasting και χωρίς να παρέχουν κανένα feedback (π.χ. acknowledgement). Αυτό σημαίνει ότι ο αποστολέας του multicast εφαρμόζει μόνο *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) [36] πριν τη μετάδοση του Data frame. Δεν υπάρχει καμία ανάκτηση σε επίπεδο Media Access Control (MAC) για το multicast frame όπως γίνεται με το unicast. Ως αποτέλεσμα, η αξιοπιστία του multicast μειώνεται σημαντικά εξ αιτίας της αυξημένης πιθανότητας χαμένων frames ως αποτέλεσμα συγκρούσεων, παρεμβολών ή λοιπών σφαλμάτων [37].

Όπως αναφέρουν οι προδιαγραφές του 802.11 [38] για τη διαδικασία μεταφοράς του multicast MPDU (MAC protocol data unit):

> "*[...] only the basic access procedure shall be used. Regardless of the length of the frame,* ***no RTS/CTS*** *(Request to Send / Clear to Send) exchange shall be used. In addition,* ***no ACK shall be transmitted*** *by any of the recipients of the frame. [...] The broadcast/multicast message*

shall be distributed into the BSS (Basic Service Set). The STA (Station) originating the message shall receive the message as a broadcast/multicast message. Therefore, all STAs shall filter out broadcast/multicast messages that contain their address as the source address. Broadcast and multicast MSDUs(MAC service data unit) shall be propagated throughout the ESS (Extended service set).

There is no MAC-level recovery on broadcast or multicast frames[...]. As a result, the reliability of this traffic is reduced, relative to the reliability of individually addressed traffic, due to the increased probability of lost frames from interference, collisions, or time-varying channel properties. "

Όπως αναφέρεται στις ίδιες προδιαγραφές:

"[...]. There are no guarantees that the submitted MSDU will be delivered successfully. Broadcast and multicast transport is part of the data service provided by the MAC. Due to the characteristics of the WM(wireless medium), broadcast and multicast MSDUs may experience a lower QoS, compared to that of unicast MSDUs"

Η έλλειψη feedback οδηγεί σε τρία προβλήματα [39]:

1. Δεν υπάρχει ρύθμιση του λεγόμενου *Contention Window* (CW) το οποίο είναι μία καθυστέρηση στην μετάδοση των πακέτων
2. Δεν υπάρχουν αναμεταδώσεις
3. Δεν υπάρχει ρύθμιση του ρυθμού μετάδοσης (rate).

Αυτά τα προβλήματα προκαλούν θέματα δικαιοσύνης, αξιοπιστία και αποδοτικότητας αντίστοιχα.

Πρώτον, σε μια σύγκρουση, το multicast frame απλά απορρίπτεται χωρίς καμία αναμετάδοση στο επίπεδο MAC διότι δεν υπάρχει τρόπος να γνωρίζουμε για αυτή τη σύγκρουση, λόγω της έλλειψης acknowledgment. Τα τρέχοντα IEEE 802.11 πρότυπα υποστηρίζουν μόνο μη αξιόπιστες υπηρεσίες. Όσο ο αριθμός των ροών αυξάνεται, το ποσοστό χαμένων multicast frames αυξάνεται.

Δεύτερον, έλλειψη feedback σημαίνει πως ένα Access Point (AP) δεν μπορεί να συγκεντρώσει εύκολα τις πληροφορίες κατάστασης (state information) των hosts που συμμετέχουν σε ένα multicast group. Για το λόγο αυτό, τα περισσότερα Access Points χρησιμοποιούν έναν προκαθορισμένο, χαμηλό ρυθμό μετάδοσης (το λεγόμενο basic rate) για το multicast, προκειμένου να εγγυηθούν ότι θα μεταδοθούν επιτυχώς όσο το δυνατόν περισσότερα multicast πακέτα.

Έχουν προταθεί αρκετά πρωτόκολλα multicast μετάδοσης όπως και μηχανισμοί ελέγχου συμφόρησης, για να καταστίσουν δυνατή την αποδοτική μετάδοση δεδομένων σε συγκεκριμένο χρονικό διάστημα [35]. Αυτά επιδιώκουν την γρήγορη ανταπόκριση σε απώλειες, δικαιοσύνη και TCP-συμβατότητα. Μια από τις σημαντικότερες προκλήσεις που αντιμετωπίζει το End-to-End multicast, είναι η εξασφάλιση ενός κλιμακούμενου ελέγχου συμφόρησης που θα ανταποκρίνεται στην ετερογένεια των διάφορων groups παραληπτών. Η σχεδίαση ενός αξιόπιστου πρωτοκόλλου Multicast Congestion Control (MCC) το οποίο θα παρέχει υψηλή απόδοση, επεκτασιμότητα και TCP-συμβατότητα, είναι ένα δύσκολο έργο με το οποίο ασχολείται η ερευνητική κοινότητα την τελευταία δεκαετία.

Υπάρχουν δύο κατηγορίες MCC πρωτοκόλλων που διασφαλίζουν αξιόπιστη και αποδοτική μεταφορά δεδομένων [40]. Η πρώτη κατηγορία είναι η single rate MCC, όπου η πηγή προσαρμόζει το ρυθμό μετάδοσης της σύμφωνα με τον αργότερο παραλήπτη του session (γνωστός και ως Current Limiting Receiver – CLR). Η δεύτερη κατηγορία είναι η multi rate MCC [35], όπου η πηγή πρέπει να στείλει τα δεδομένα σε πολλαπλά επίπεδα και κάθε αποδέκτης μπορεί να συντονιστεί (subscribe) στο αντίστοιχο επίπεδο ανάλογα με τις δικές του δυνατότητες και ανάγκες. Στη πράξη, τα single rate MCC πρωτόκολλα είναι πολύ ευκολότερο να υλοποιηθούν και να αναπτυχθούν.

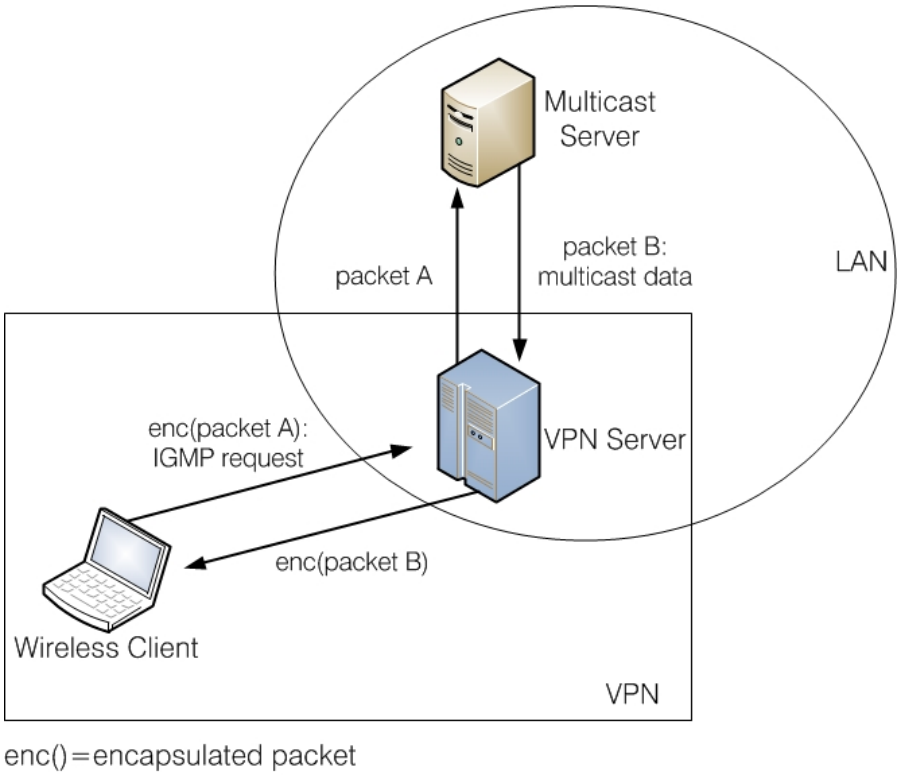
Packet encapsulation με χρήση VPN

Στις προηγούμενες ενότητες είδαμε τις αρχές λειτουργίας του multicast και τους περιορισμούς που αντιμετωπίζει η εφαρμογή του στα ασύρματα δίκτυα. Σε αυτή την ενότητα θα αναφερθούμε στην λύση που προτείνει η παρούσα διπλωματική εργασία για την επίτευξη της multicast μετάδοσης στα δίκτυα αυτά.

Η λύση που προτείνουμε, περιλαμβάνει την ‘’μετατροπή’’ (μέσω του encapsulation) των multicast frames σε unicast. Αφού η unicast μετάδοση περιλαμβάνει μηχανισμούς feedback στις προδιαγραφές του IEEE 802.11, μπορούμε εν τέλει να αποφύγουμε τους περιορισμούς που αναφέρθηκαν στην προηγούμενη ενότητα. Για τη διαδικασία του encapsulation θα χρησιμοποιήσουμε τα *Virtual Private Networks (VPNs)*.

Στα VPN, ο server δημιουργεί ασφαλή κανάλια επικοινωνίας με τους clients χρησιμοποιώντας unicast αναμεταδώσεις. Όταν ένας client ζητήσει μια multicast ροή, αρχικά στέλνει το IGMP request, αλλά αυτή τη φορά encapsulated σε VPN (unicast) πακέτο. Αφού ο server λάβει το IGMP request και με την προϋπόθεση ότι υποστηρίζει IGMP forwarding ή λειτουργεί ως IGMP proxy, θα προωθήσει την multicast ροή στον client. Ο multicast server (δηλαδή η πηγή της ροής) μπορεί να είναι είτε ο VPN server είτε οποιοδήποτε άλλος κόμβος σε κάποιο στο ο οποίο ανήκει ο VPN server (για παράδειγμα σε κάποιο άλλο LAN).

Το σχήμα 10 απεικονίζει την παραπάνω διαδικασία. Σε αυτή ο ασύρματος client στέλνει το encapsulated IGMP request ως unicast πακέτο στον server ο οποίος με τη σειρά του το στέλνει στον multicast server. Έτσι ο ασύρματος client συνδέεται με το multicast group για το οποίο έκανε το request. Έπειτα, ο multicast server στέλνει τα δεδομένα στον VPN server οποία θα κάνει το encapsulation για να τα στείλει πίσω στον client ως unicast πακέτα. Με αυτή τη μέθοδο, καταστήσαμε εφικτή την παράδοση της multicast ροής σε όλους τους client του VPN, είτε αυτοί είναι ενσύρματοι, είτε ασύρματοι.



Σχήμα 10 - Χρήση VPN για packet encapsulation

Πριν περάσουμε στα πρακτικά παραδείγματα, θα κάνουμε μια σύντομη αναφορά στους δύο τύπους VPN που χρησιμοποιήθηκαν για την υλοποίηση του παραπάνω σεναρίου, τα PPTP και OpenVPN.

Virtual Private Networks (VPNs)

Τα Virtual Private Networks είναι δίκτυα δεδομένων που χρησιμοποιούν το δημόσιο internet εξακολουθώντας να παρέχουν ασφάλεια μέσω της χρήσης πρωτοκόλλων κρυπτογράφησης και *tunneling*. Το VPN μπορεί να παρομοιαστεί με ένα ιδιόκτητο δίκτυο ή δίκτυο μισθωμένων γραμμών το οποίο χρησιμοποιείται μόνο από μια εταιρεία. Ο κύριος σκοπός του VPN είναι να δώσει στην εταιρία τις ίδιες δυνατότητες με αυτές του ιδιόκτητου δικτύου σε πολύ χαμηλότερο κόστος ακριβώς λόγω της χρήσης της δημόσιας υποδομής [41].

Οι διάφορες τεχνολογίες VPN χρησιμοποιούν δεκάδες πρωτόκολλα και μπορούν να διαφέρουν σε τομείς όπως [43]:

- Το πρωτόκολλο για το tunneling της κίνησης
- Το επίπεδο της προσφερόμενης ασφάλειας
- Το επίπεδο OSI που παρέχουν στη σύνδεση, για παράδειγμα Layer 2 ή Layer 3 επίπεδα

Πρωτόκολλα Tunneling

Η χρήση των πρωτοκόλλων tunneling στα δίκτυα υπολογιστών γίνεται όταν απαιτείται το encapsulation της κίνησης για τη μεταφορά του πάνω από το δίκτυο. Με το encapsulation επιτυγχάνεται η μεταφορά δεδομένων διαφορετικών πρωτοκόλλων από αυτά που μπορεί υποστηρίζει το εκάστοτε δίκτυο. Με την επιπλέον χρήση πρωτοκόλλων κρυπτογράφησης τα tunneling πρωτόκολλα, προσφέρουν την υποδομή για τα VPN.

Point-to-Point Protocol (PPP)

Το PPP είναι ένα data link πρωτόκολλο για την απευθείας σύνδεση δύο δικτυακών κόμβων. Παρέχει κρυπτογράφηση, authentication και συμπίεση δεδομένων. Δύο πολύ γνωστές μορφές PPP encapsulation, οι Point-to-Point Protocol over Ethernet (PPPoE) και Point-to-Point Protocol over ATM (PPPoA), χρησιμοποιούνται από τους Internet Services Providers για την σύνδεση των πελατών τους με την DSL υποδομή.

Point-to-Point Tunneling Protocol (PPTP)

Το PPTP είναι ένα tunneling πρωτόκολλο το οποίο χρησιμοποιεί βελτιωμένους μηχανισμούς του πρωτοκόλλου Generic Routing Encapsulation (GRE) για την παροχή ελέγχων ροής και συμφόρησης κατά το encapsulation και τη μεταφορά PPP πακέτων [42]. Οι προδιαγραφές του PPTP δεν περιλαμβάνουν λειτουργίες κρυπτογράφησης ή authentication και βασίζονται στους μηχανισμούς του PPP το οποίο μεταφέρει για τις υπηρεσίες ασφάλειας. Παρ' όλα αυτά, διάφορες υλοποιήσεις PPTP που ανήκουν στα προϊόντα της Microsoft προσφέρουν διάφορα επίπεδα κρυπτογράφησης και authentication καθώς αυτά υπάρχουν στο PPTP stack του λειτουργικού συστήματος Windows.

Generic Routing Encapsulation (GRE)

Το GRE είναι ένα tunneling πρωτόκολλο της Cisco το οποίο μπορεί να κάνει encapsulate διάφορους τύπους Layer 3 (network layer) πακέτων μέσα σε ένα IP tunnel, δημιουργώντας έτσι ένα point-to-point link μεταξύ διαφορετικών τύπων δρομολογητών.

Τα VPNs (και συγκεκριμένα τα *secure VPNs*) χρησιμοποιούν πρωτόκολλα κρυπτογράφησης και authentication για την ασφάλεια και την αξιοπιστία της επικοινωνίας (σε αντίθεση με τα *trusted VPNs* που στηρίζονται στην ασφάλεια της υποδομής του εκάστοτε δικτύου). Τα δύο πρωτόκολλα που χρησιμοποιούνται στις υλοποιήσεις αυτής της διπλωματικής εργασίας είναι τα:

- *Transport Layer Security* (SSL/TLS) το οποίο κάνει tunnel την κίνηση ολόκληρου του δικτύου, όπως συμβαίνει με το OpenVPN
- *Microsoft Point-to-Point Encryption* (MPPE) το οποίο κρυπτογραφεί την κίνηση του Point-to-Point Protocol (PPP) στις PPTP VPN υλοποιήσεις της εταιρίας, όπως θα δούμε για τα MS Windows Server 2003

OpenVPN

Το OpenVPN [44] είναι μια πλατφόρμα ανοιχτού κώδικα για την υλοποίηση virtual private networks το οποίο χρησιμοποιεί ασφάλεια και κρυπτογράφηση SSL/TLS μέσω της βιβλιοθήκης ανοιχτού κώδικα OpenSSL και λειτουργεί τόσο σε UDP όσο και σε TCP μεταδόσεις. Ακόμα, μπορεί να προσφέρει ακεραιότητα και authentication των πακέτων μέσω HMAC. Το authentication των χρηστών μπορεί να γίνει μέσω pre-shared κλειδιού, με πιστοποιητικά (το οποίο αποτελεί και την πιο αξιόπιστη μέθοδο) και με χρήση username/password.

Το OpenVPN υποστηρίζει δύο διαφορετικούς τρόπους για τη διασύνδεση των δικτύων [45]:

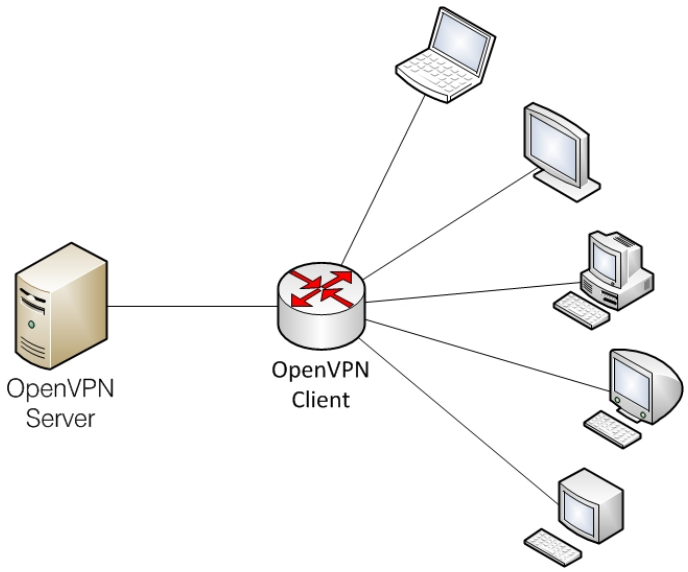
- Το *Routing* το οποίο αναφέρεται στο Layer 3 IP tunneling
- Το *Bridging* το οποίο αναφέρεται στην Layer 2 Ethernet διασύνδεση

Αυτές οι δύο λειτουργίες υλοποιούνται με χρήση των virtual network interfaces *TUN* και *TAP* [43] αντίστοιχα. Το TUN (εκ του network TUNnel) προσομοιώνει μία Layer 3 (network) συσκευή (όπως ένας router) και διαχειρίζεται layer 3 πακέτα όπως τα IP πακέτα. Από την άλλη, το TAP (εκ του network tap) προσομοιώνει μία Ethernet (Layer 2) συσκευή, όπως ένα switch/bridge και διαχειρίζεται αντίστοιχα layer 2 πακέτα (όπως τα Ethernet frames).

Το bridging mode εκ των πραγμάτων δε μπορεί να αξιοποιηθεί για το σενάριό μας στο οποίο θέλουμε την αποδοτική multicast παράδοση καθώς κάθε node του VPN θα λάμβανε τη ροή. Παρ' όλα αυτά ακόμα και στο Routing mode (τουλάχιστον στην έκδοση 2.1.3 του OpenVPN) στο οποία θα αναμέναμε την επιθυμητή λειτουργία, τα πειράματα έδειξαν πως το κάθε stream φτάνει σε όλους τους clients. Καταλήγουμε λοιπόν στο συμπέρασμα πως ο OpenVPN server χρησιμοποιεί ένα link για την αποστολή των δεδομένων προς όλους τους clients του VPN. Αντί λοιπόν για multicast καταλήγουμε να έχουμε και πάλι broadcast.

Έτσι, αν για παράδειγμα έχουμε 10 clients συνδεδεμένους στο VPN και κάθε client κάνει join σε διαφορετικό multicast group, το αποτέλεσμα θα ήταν ο server να στείλει και τις 10 διαφορετικές ροές σε όλους του clients. Ένα worst case σενάριο για αυτή την περίπτωση θα ήταν ο κάθε client να ζητά ένα High Definition κανάλι, όπου μια τέτοια ροή μπορεί εύκολα να φτάσει στα 11-12Mbs και να καταλήξει κάθε επιμέρους router να πρέπει να διαχειριστεί 110Mbps.

Ένα ακόμα πλεονέκτημα του OpenVPN είναι το ότι υποστηρίζεται από πολλά firmware δρομολογητών όπως το DD-WRT [46]. Έτσι ένας router με εγκατεστημένο το OpenVPN σε client mode και συνδεδεμένος σε έναν server, μπορεί να παρέχει όλα τα πλεονεκτήματα αυτού του VPN σε όλους τους clients που είναι συνδεδεμένοι με τον router, χωρίς να απαιτείται η εγκατάσταση του OpenVPN σε κάθε έναν από αυτούς τους clients ξεχωριστά. Αυτό το σενάριο φαίνεται στο σχήμα 11:



Σχήμα 11 – Router με εγκατεστημένο το OpenVPN σε client mode

Αν και αυτή η χρήση του OpenVPN είναι πρακτική, περιορίζεται από τις επεξεργαστικές δυνατότητες του δρομολογητή. Όπως έδειξαν τα πειράματα και οι μετρήσεις με χρήση του εργαλείου Iperf [54] κατά τη διάρκεια αυτής της εργασίας, είναι σχεδόν αδύνατο ακόμα και ένας σχετικά σύγχρονος δρομολογητής, να ανταπεξέλθει ικανοποιητικά στις απαιτήσεις της προώθησης video ακόμα και αν αυτό είναι Standard Definition.

OpenVPN σε bridging mode

Σε αυτή την ενότητα θα περιγράψουμε την bridging λειτουργία του OpenVPN σε ένα setup που περιλαμβάνει τον ενσύρματο server σε Microsoft Windows XP ο οποίος ανήκει στο ίδιο LAN με τον multicast server και clients τόσο με Windows όσο και με MacOS.

Δεν θα κάνουμε ιδιαίτερη αναφορά για την εγκατάσταση, τη δημιουργία πιστοποιητικών και το bridging των interface σε περιβάλλον Windows, καθώς το επίσημο tutorial στη διεύθυνση [47] είναι κατατοπιστικό.

Επιπλέον, στο συγκεκριμένο παράδειγμα κάνουμε το authentication των χρηστών μέσω Active Directory. Για το σκοπό αυτό θα χρησιμοποιήσουμε τα scripts που μπορούμε να βρούμε στη διεύθυνση [48].

OpenVPN Server

Το παρακάτω αποτελεί ένα ενδεικτικό και λειτουργικό configuration αρχείο για τον server σε bridging mode και συμπεριλαμβανομένου του Active Directory authentication:

```
################################################################
#
#You will only need to change the two uncommented lines below
to match your configuration
#local Your.IP.Address.Here
local 18.x.y.z

#server-bridge [subnet gateway] [subnet mask] [start IP] [end
IP]
server-bridge 18.x.x.x 255.x.x.x 18.x.x.x 18.x.x.x

#Go to: Run->cmd->ipconfig to find these values
#[start IP] [end IP] is the pool from which the client are
going to get IPs
################################################################
#

################################################################
#
#Don't change the following
mode server
#Here i use the script to connect to the Active Directory for
authentication
auth-user-pass-verify Auth4OpenVPN.vbs via-env
script-security 3
```

```
auth-user-pass-verify "C:/Windows/System32/cscript.exe
/H:cscript C:/Progra~1/OpenVPN/config/Auth4OpenVPN.vbs" via-env

client-to-client
username-as-common-name
duplicate-cn
port 1194
proto udp
dev tap
dev-node tap-bridge
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
dh dh1024.pem
push "redirect-gateway def1"
keepalive 10 120
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Τώρα μπορούμε να ‘’τρέξουμε’’ τον server.

OpenVPN Client

Τόσο ο client σε Windows όσο και σε Mac χρησιμοποιούν το ίδιο configuration file το οποίο παρατίθεται παρακάτω. Υπενθυμίζουμε πως οι clients των παραδειγμάτων είναι ασύρματοι μέσω Wifi.

Για το MacOS το ευκολότερο στη χρήση User Interface είναι το Tunnelblick [49] το οποίο και θα χρησιμοποιήσουμε. Μετά την εγκατάσταση, μετακινούμε τα πιστοποιητικά και τα αρχεία configuration στον αντίστοιχο φάκελο (συνήθως ΄Library/Application Support/Tunnelblick/Configurations)

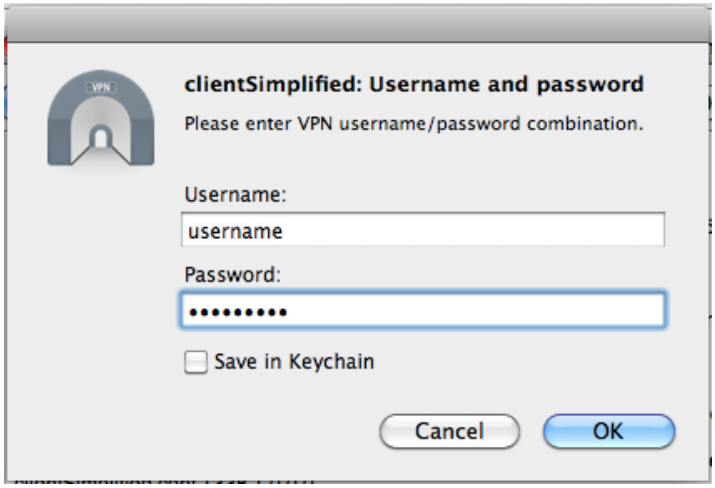
Το αρχείο configuration τόσο για MacOS όσο και Windows είναι:

```
##############################################################
#
#You will only need to change this uncommented line to match
your configuration
remote 18.x.x.x 1194


##############################################################
#
#Don't change the following
client
auth-user-pass
auth-retry interact
dev tap
proto udp
pull
```

```
float
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
verb 3
```

Αφού τρέξουμε και τον client, θα εμφανιστεί ένα παράθυρο όμοιο με της εικόνας 1, όπου θα συμπληρώσουμε τα κατάλληλα στοιχεία, στη συγκεκριμένη περίπτωση τα στοιχεία του Active Directory που μας αντιστοιχούν.



Εικόνα 1

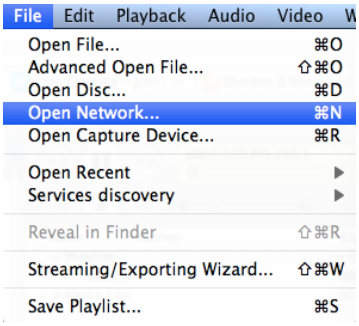
Πλέον είμαστε συνδεδεμένοι με τον server και ο client θα πρέπει να έχει αποκτήσει IP διεύθυνση η οποία να ανήκει στο domain του server καθώς είμαστε σε bridging mode.

Λήψη video

Τώρα που ασύρματοι client ανήκουν στο domain του server οποίος με τη σειρά του είναι στο ίδιο domain με τον multicast server, θα πρέπει να είναι δυνατή η λήψη της multicast ροής. Η λήψη του multicast ροής θα γίνει με τον open source VLC player [50] καθώς αποτελεί το πληρέστερο και πιο ευέλικτο εργαλείο για αυτού του είδους τις πολυμεσικές εφαρμογές.

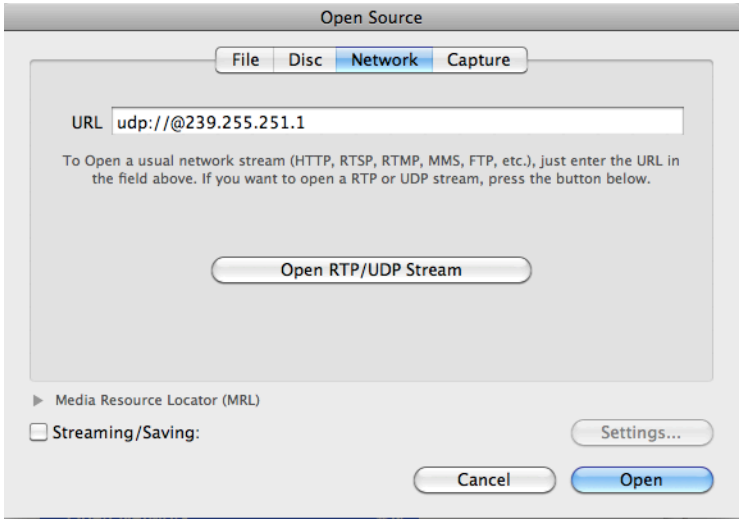
Τα βήματα για να λάβουμε το multicast video είναι τα εξής:

File -> Open Network



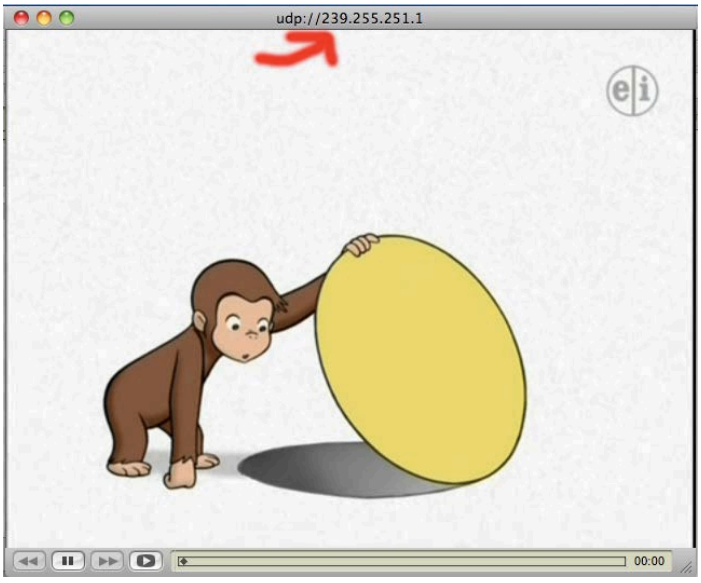
Εικόνα 2

Εισάγουμε την multicast διεύθυνση του group που θέλουμε να κάνουμε join, σε αυτή την περίπτωση η 239.255.251.1



Εικόνα 3

Πλέον θα πρέπει να μπορούμε να δούμε το video του multicast group

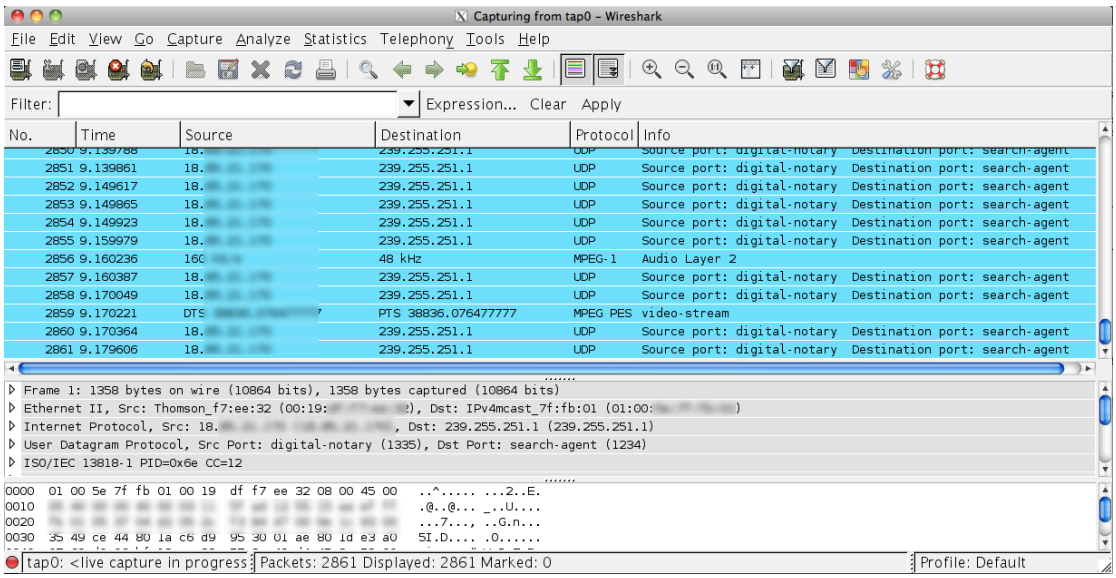


Εικόνα 4

Η διαδικασία για τον Windows client είναι όμοια.

Μεγάλο ενδιαφέρον έχει το να δούμε πως απεικονίζονται τα multicast UDP πακέτα που καταφτάνουν στο εκάστοτε virtual interface. Για το σκοπό αυτό θα χρησιμοποιήσουμε το πρόγραμμα Wireshark [51].

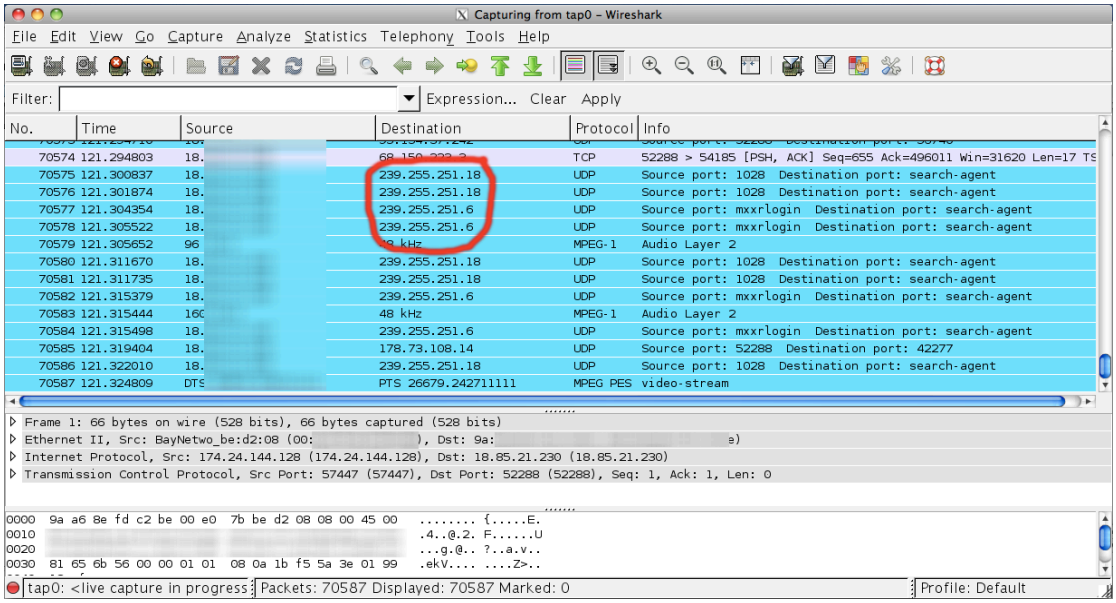
Τα πακέτα στο virtual interface (tap για τα Windows και τα tap0 για τα MacOS) θα έχουν την μορφή της εικόνας 5.



Εικόνα 5

Στη στήλη source είναι η διεύθυνση του multicast server ενώ στη στήλη destination είναι η διεύθυνση του multicast group στο οποίο κάναμε join.

Καθώς είμαστε σε bridging mode δεν υπάρχει καμία δρομολόγηση πακέτων από τον VPN server (ο οποίος δρα ως Layer 2 swtich/bridge) και έτσι κάθε client του εικονικού δικτύου θα λάβει, πέρα από τα δικά του πακέτα και τα πακέτα που έχει ζητήσει οποιοσδήποτε άλλος client του VPN. Αυτό μπορούμε να το δούμε πρακτικά στην εικόνα 6 κάνοντας δύο clients του VPN register σε δύο διαφορετικά multicast groups και ανιχνεύοντας τα πακέτα σε έναν από αυτούς.



Εικόνα 6

Όπως είναι αναμενόμενο, βλέπουμε πως ο client λαμβάνει τις ροές και από τα δύο multicast groups (*.6 και *.18)

OpenVPN σε routing mode

Όπως αναφέραμε και παραπάνω, τουλάχιστον για την έκδοση 2.1.3 του OpenVPN, ο server χρησιμοποιεί ένα link για την αποστολή των δεδομένων προς όλους τους clients και έτσι η multicast ροή καταλήγει να είναι broadcast. Παρ' όλα αυτά για λόγους πληρότητας, παραθέτουμε τα αρχεία configuration για τη routing λειτουργία.

Η διαδικασία εγκατάστασης είναι όμοια με αυτή του bridging mode. Επίσης σε αυτό το σενάριο δεν κάνουμε χρήση Active Directory authentication παρά μόνο χρήση πιστοποιητικών.

Server

Το παρακάτω είναι το αρχείο configuration για τον server:

```
local 18.x.x.x
proto udp
dev tun
dev-node tap-bridge
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
```

```
dh dh1024.pem
server 10.x.x.x 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 224.0.0.0 240.0.0.0"
client-to-client
duplicate-cn
keepalive 10 120
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Client

Ομοίως, το αρχείο configuration για τον client:

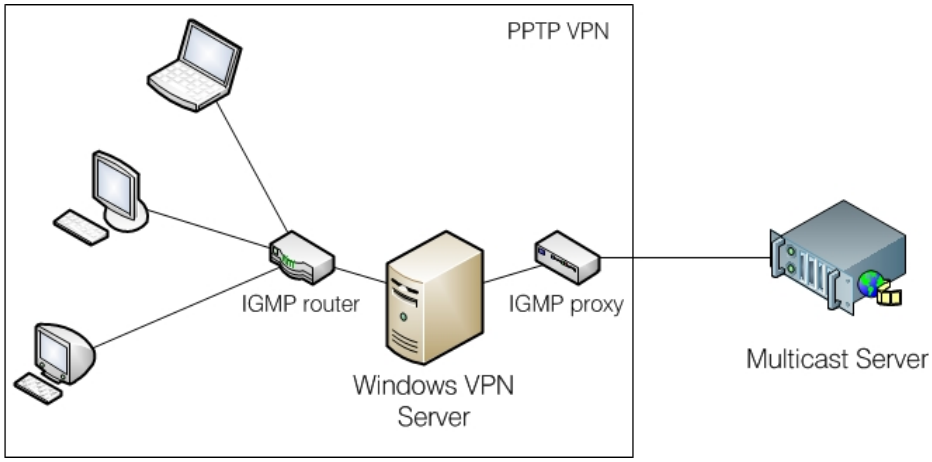
```
client
dev tun
proto udp
remote 18.x.x.x 1194
pull
float
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
verb 3
```

Εκτός από το command line περιβάλλον, το OpenVPN προσφέρει και γραφικό, web-based interface το οποίο απλοποιεί ακόμη περισσότερο τις διαδικασίες. Αν και το ζήτημα του ενός link για όλους τους clients παραμένει, αποτελεί έναν απλούστατο τρόπο για την εγκατάσταση ενός SSL VPN.

PPTP VPN

Η δεύτερη μέθοδος που προτείνεται από αυτή την διπλωματική εργασία, είναι η χρήση ενός PPTP VPN. Αυτό το δίκτυο θα υλοποιηθεί μέσα από τα Windows Server 2003 και όπως θα δούμε παρακάτω, θα προσφέρει το επιθυμητό multicast περιβάλλον. Το λειτουργικό σύστημα Windows Server περιλαμβάνει την υπηρεσία PPTP VPN και μαζί με τη χρήση ενός IGMP Proxy θα εγκαταστήσουμε το multicast δίκτυό μας.

Στον server θα χρειαστεί να προσθέσουμε τα εξής roles. Το "Remote Access/VPN Server" που περιέχει το PPTP και προαιρετικά το Domain Controller για το authentication των χρηστών μέσω του Active Directory. Αφού προσθέσουμε τον Access Role, πρέπει βεβαιωθούμε πως το φυσικό interface είναι ρυθμισμένο ως "IGMP proxy" και το virtual interface (αναφερόμενο ως internal) ρυθμισμένο ως "IGMP router". Έτσι, το φυσικό interface θα λάβει τη multicast ροή την οποία ως proxy θα προωθήσει στο virtual το οποίο με τη σειρά του θα δρομολογήσει τα πακέτα στους κατάλληλους hosts. Αυτή η διαδικασία φαίνεται στο σχήμα 12



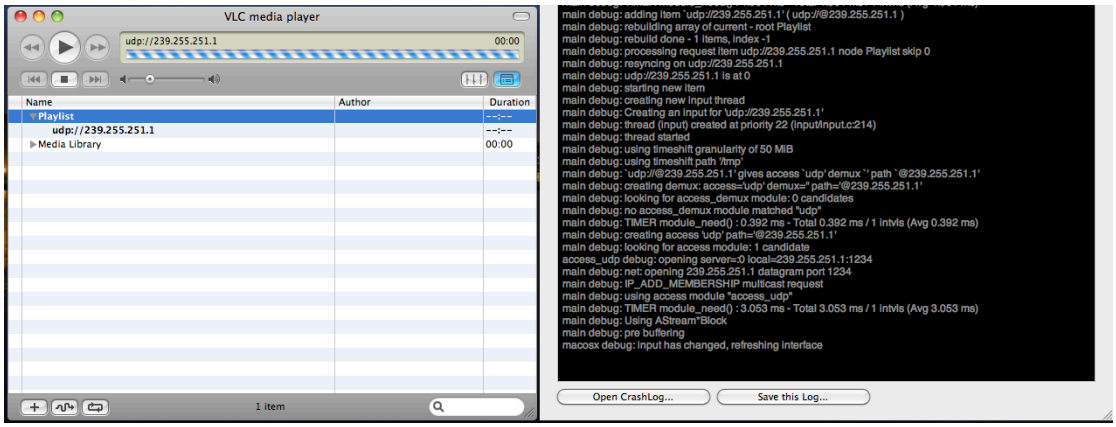
Σχήμα 12 – IGMP router και IGMP proxy

Επίσης, ανάλογα με το εκάστοτε setup του δικτύου μας, ίσως χρειαστεί να πειραματιστούμε με την έκδοση του IGMP που θα υποστηρίζει ο IGMP router. Για παράδειγμα, ρυθμίζοντας τον router στο IGMP Version 3, δεν υπήρχε συνεργασία με το λειτουργικό MacOS, κάτι που διορθώνονταν με την έκδοση 2.

Αφού ρυθμίσαμε τον server (ο οποίος βέβαια βρίσκεται στο ίδιο LAN ή ο ίδιος είναι ο multicast server), μπορούμε πλέον να συνδέσουμε τους clients. Παρακάτω θα δούμε παραδείγματα τόσο για MacOS X όσο και για Windows Clients.

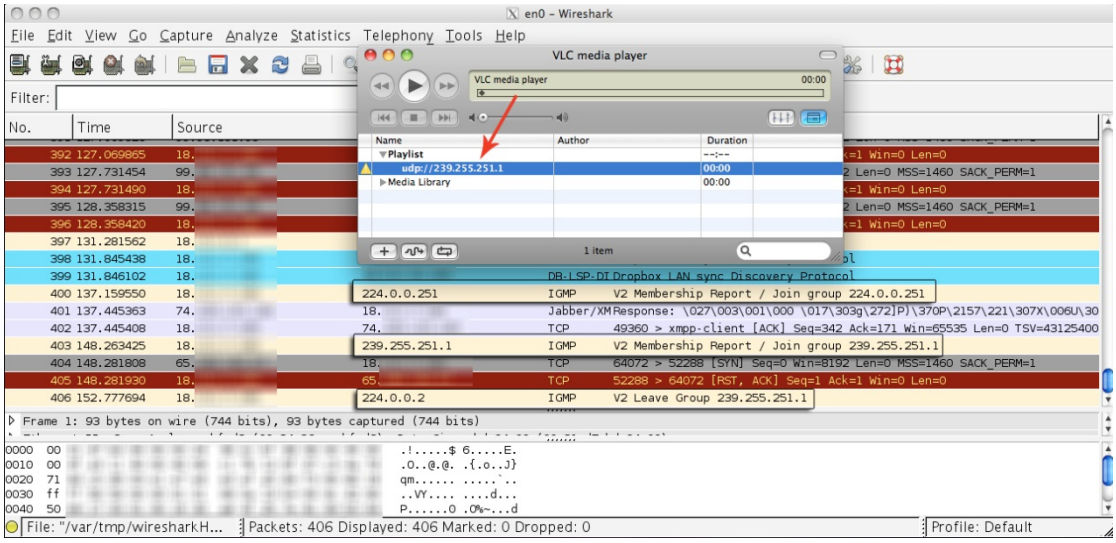
MaxOS X Client

Αρχικά, ας δούμε τη συμπεριφορά του client χωρίς να είναι συνδεδεμένος στο VPN. Αφού ανοίξουμε το υποθετικό stream θα έχουμε την παρακάτω εικόνα.



Εικόνα 7

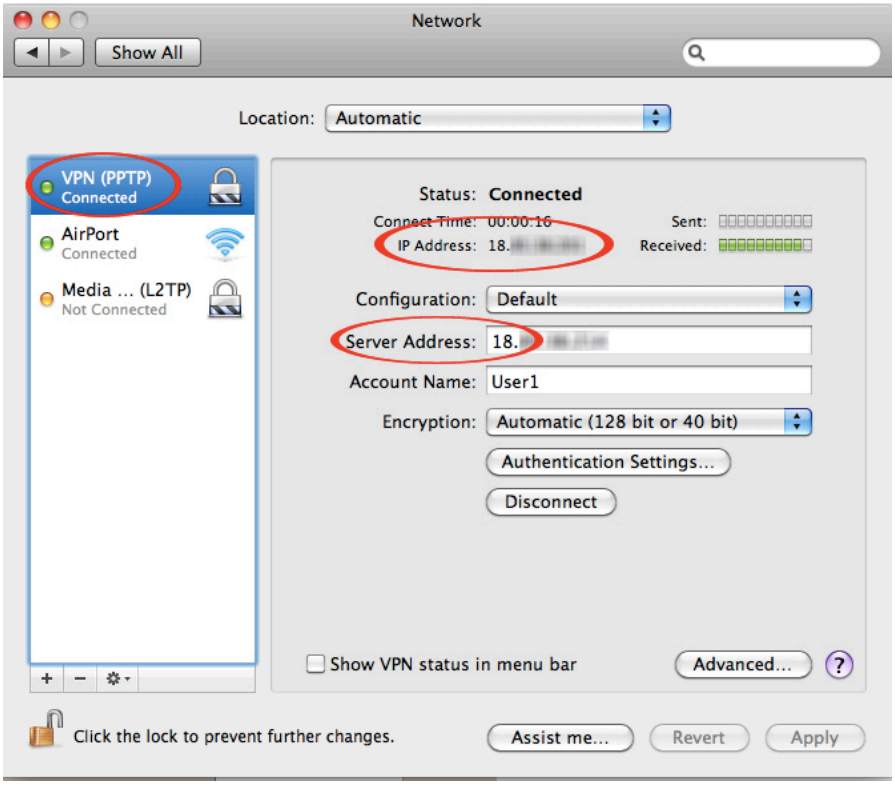
Ας δούμε τώρα τι συμβαίνει με τα πακέτα, πριν και μετά τη σύνδεση στο VPN. Το αποτέλεσμα του capturing των πακέτων στο φυσικό interface πριν την σύνδεση είναι αυτό της εικόνας 8:



Εικόνα 8

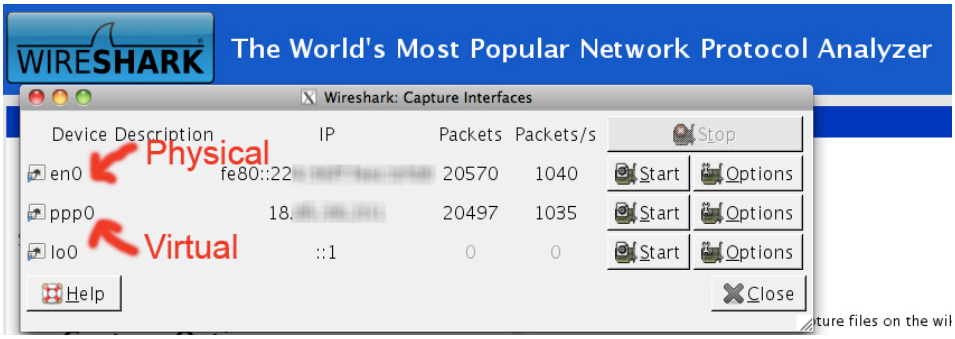
Παρατηρούμε πως όταν πατάμε το πλήκτρο Play στο VLC, η εφαρμογή στέλνει το IGMP Membership Report στον multicast server. Φυσικά, επειδή ο client είναι ασύρματος, δεν θα έχουμε κάποια λήψη, για τους λόγους που αναλύθηκαν στο θεωρητικό μέρος της εργασίας. Επίσης, όταν πατήσουμε το πλήκτρο Stop, ένα "Leave Group" IGMP μήνυμα θα σταλεί προς τον server.

Στη συνέχεια κάνουμε τη σύνδεση με το VPN.



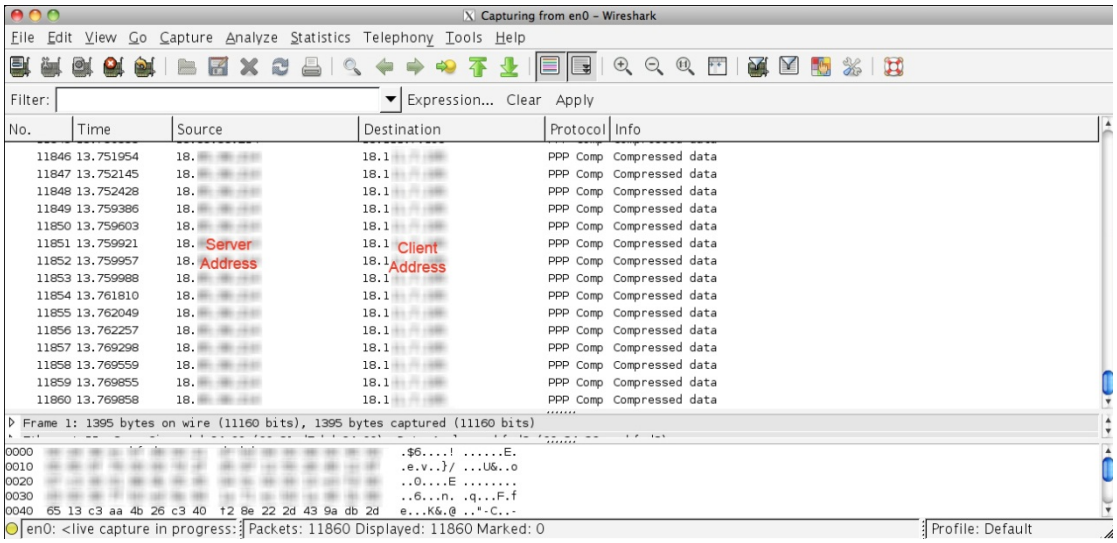
Εικόνα 9

Παρατηρούμε πως ο client έχει πάρει διεύθυνση IP από το pool που έχει ορίσει ο VPN server. Ας δούμε τώρα τα πακέτα, όπως φαίνονται στο Wireshark.



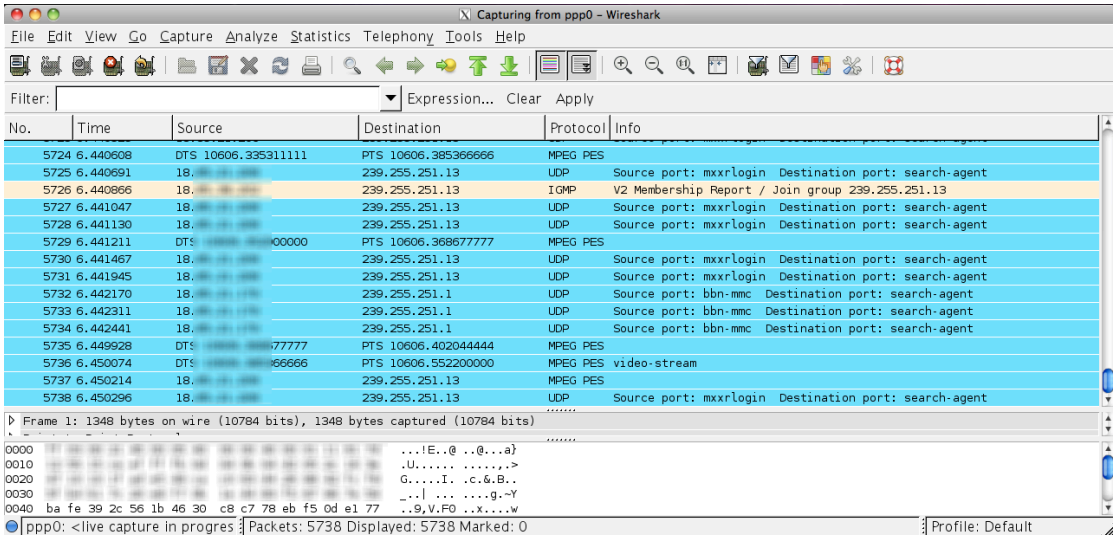
Εικόνα 10

Όπως είναι αναμενόμενο, στο φυσικό interface τα πακέτα λαμβάνονται ως encapsulated PPP πακέτα:



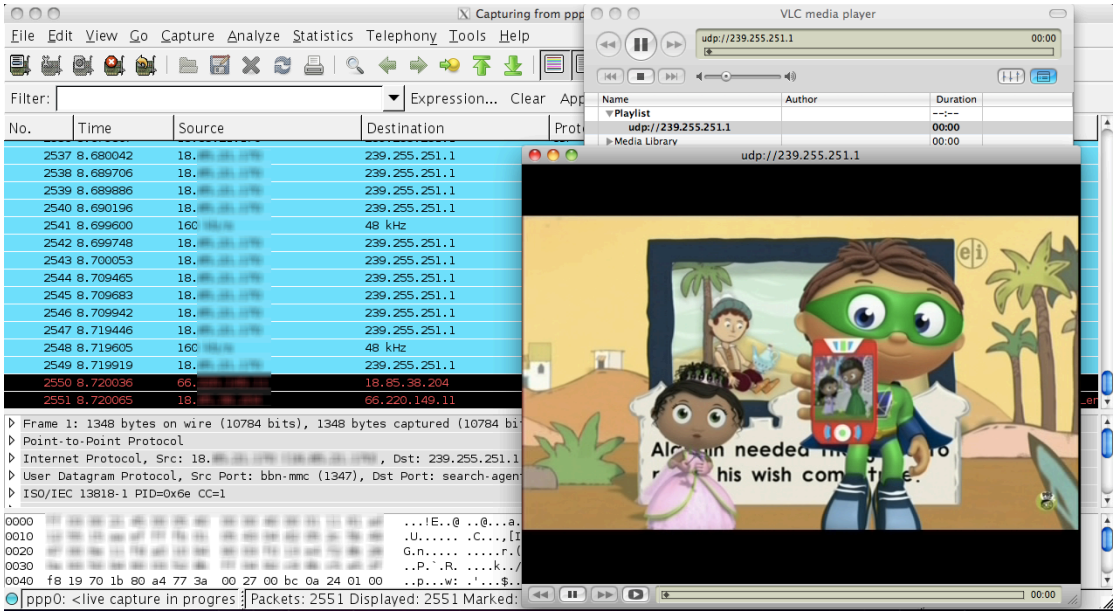
Εικόνα 11

Και αντίστοιχα στο virtual PPP interface βλέπουμε τα πραγματικά UDP πακέτα:



Εικόνα 12

Το αποτέλεσμα της σωστής multicast λήψης φαίνεται στην εικόνα 13:



Εικόνα 13

Με τη μέθοδο που παρουσιάσαμε σε αυτή την ενότητα δημιουργήσαμε την κατάλληλη υποδομή για την επίτευξη της multicast μετάδοση video σε ασύρματους clients. Στο link [52] μπορούμε να δούμε ακριβώς αυτή τη διαδικασία σε video. Σε αυτό το demo έχουμε δύο clients, έναν ασύρματο και έναν ενσύρματο οι οποίοι ζητούν δύο διαφορετικές multicast ροές από τον server. Χρησιμοποιώντας το Wireshark , βλέπουμε ότι όντως κάθε client λαμβάνει μόνο τα πακέτα του multicast group στο οποίο έχει κάνει join.

Συμπεράσματα – μελλοντικές επεκτάσεις

Στην παρούσα διπλωματική εργασία εξετάσαμε την τεχνολογία multicast, την μετάδοση video μέσω αυτής, καθώς και τους περιορισμούς που προκύπτουν από τις προδιαγραφές πρωτοκόλλων ασύρματης δικτύωσης όπως το IEEE 802.11. Έγινε μια εκτενής αναφορά στις ιδιότητες της συγκεκριμένης τεχνολογίας καθώς και στα εφαρμοσμένα πρωτόκολλα multicast προώθησης και δρομολόγησης. Επίσης, προτάθηκε και υλοποιήθηκε επιτυχώς η χρήση των Virtual Private Networks για την επίτευξη της αποδοτικής ασύρματης μετάδοσης multicast video σε περιβάλλοντα και δίκτυα που εξ αρχής δεν το επέτρεπαν.

Η αρκετά μικρή σε όγκο διαθέσιμη βιβλιογραφία επί του συγκεκριμένου ζητήματος, μας δείχνει πως αν και το multicast ως τεχνολογία είναι στο προσκήνιο της έρευνας για περισσότερο από μία δεκαετία, είναι ελάχιστες οι εφαρμόσιμες λύσεις που έχουν προταθεί και οι οποίες να είναι παράλληλα χαμηλού κόστους. Μετά από μία σειρά δοκιμών και πειραμάτων σε διάφορους τύπους δικτύων μπορούμε να συμπεράνουμε πως η προτεινόμενη λύση αποτελεί μια οικονομική αλλά και αξιόπιστη μέθοδο για την αποδοτική χρήση της τεχνολογίας multicast για μετάδοση video σε ασύρματα δίκτυα.

Ως μελλοντική επέκταση της ιδέας που επεξεργάστηκε αυτή η εργασία, αποτελεί ο σχεδιασμός μιας διαπλατφορμικής αρχιτεκτονικής για την υποστήριξη της ασύρματης μετάδοσης multicast video, ανεξάρτητα από τον τύπου συσκευής του αποδέκτη ή υλοποίησης του εκάστοτε ασύρματου δικτύου. Κάτι τέτοιο δύναται να επιτευχθεί μέσα από την λεπτομερή μελέτη των τρεχουσών προδιαγραφών των επικρατέστερων δικτυακών πρωτοκόλλων αλλά και συνδυασμό χαρακτηριστικών διαφορετικών καινοτόμων τεχνολογιών που μπορούν να δώσουν τα επιθυμητά αποτελέσματα σε επίπεδο εφαρμογής.

Παράρτημα Α’

Δεσμευμένες Multicast διευθύνσεις

Range	Mask	Description
224.0.0.0-224.0.0.255	224.0.0/24	Local Network Control Block
224.0.1.0-224.0.1.255	224.0.1/24	Internetwork Control Block
224.0.2.0-224.0.255.255	-	Ad hoc Block
224.1.0.0-224.1.255.255	-	Unassigned
224.2.0.0-224.2.255.255	224.2/16	SDP/SAP Block
224.3.0.0-231.255.255.255	-	Unassigned
232.0.0.0-232.255.255.255	232/8	Source Specific Multicast Block
233.0.0.0-233.255.255.255	233/8	GLOP Block
234.0.0.0-238.255.255.255	-	Unassigned
239.0.0.0-239.255.255.255	239/8	Administratively Scoped Block

IANA Multicast Address Assignments

Το εύρος διευθύνσεων 224.0.0.0 έως 224.0.0.255, είναι δεσμευμένο για χρήση από πρωτόκολλα δρομολόγησης και άλλα low-level πρωτόκολλα τοπολογικής αναζήτησης και συντήρησης όπως η εύρεση gateway και group membership reporting. Οι multicast δρομολογητές δεν πρέπει να προωθούν multicast datagrams με διευθύνσεις προορισμού που ανήκουν στο παραπάνω εύρος ανεξαρτήτως τιμής TTL.

Local Network Control Block (224.0.0.0 - 224.0.0.255 (224.0.0/24))

Address(s)	Description
224.0.0.0	Base Address (Reserved)
224.0.0.1	All Systems on this Subnet
224.0.0.2	All Routers on this Subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPFIGP OSPFIGP All Routers

224.0.0.6	OSPFIGP OSPFIGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IGRP Routers
224.0.0.11	Mobile-Agents
224.0.0.12	DHCP Server / Relay Agent
224.0.0.13	All PIM Routers
224.0.0.14	RSVP-ENCAPSULATION
224.0.0.15	all-cbt-routers
224.0.0.16	designated-sbm
224.0.0.17	all-sbms
224.0.0.18	VRRP
224.0.0.19	IPAllL1ISs
224.0.0.20	IPAllL2ISs
224.0.0.21	IPAllIntermediate Systems
224.0.0.22	IGMP
224.0.0.23	GLOBECAST-ID
224.0.0.24	OSPFIGP-TE
224.0.0.25	router-to-switch
224.0.0.26	Unassigned
224.0.0.27	Al MPP Hello
224.0.0.28	ETC Control
224.0.0.29	GE-FANUC
224.0.0.30	indigo-vhdp
224.0.0.31	shinbroadband
224.0.0.32	digistar
224.0.0.33	ff-system-management
224.0.0.34	pt2-discover
224.0.0.35	DXCLUSTER
224.0.0.36	DTCP Announcement
224.0.0.37-224.0.0.68	zeroconfaddr (renew 12/02)
224.0.0.69-224.0.0.100	Reserved
224.0.0.101	cisco-nhap

224.0.0.102	HSRP
224.0.0.103	MDAP
224.0.0.104	Nokia MC CH
224.0.0.105	ff-lr-address
224.0.0.106	All-Snoopers
224.0.0.107	PTP-pdelay
224.0.0.108	Saratoga
224.0.0.109	LL-MANET-Routers
224.0.0.110	IGRS
224.0.0.111	Babel
224.0.0.112-224.0.0.250	Unassigned
224.0.0.251	mDNS
224.0.0.252	Link-local Multicast Name Resolution
224.0.0.253	Teredo
224.0.0.254	RFC3692-style Experiment (*)
224.0.0.255	Unassigned

Internetwork Control Block (224.0.1.0 - 224.0.1.255 (224.0.1/24))

Address(s)	Description
224.0.1.0	VMTP Managers Group
224.0.1.1	NTP Network Time Protocol
224.0.1.2	SGI-Dogfight
224.0.1.3	Rwhod
224.0.1.4	VNP
224.0.1.5	Artificial Horizons - Aviator
224.0.1.6	NSS - Name Service Server
224.0.1.7	AUDIONEWS - Audio News Multicast
224.0.1.8	SUN NIS+ Information Service
224.0.1.9	MTP Multicast Transport Protocol
224.0.1.10	IETF-1-LOW-AUDIO
224.0.1.11	IETF-1-AUDIO
224.0.1.12	IETF-1-VIDEO
224.0.1.13	IETF-2-LOW-AUDIO

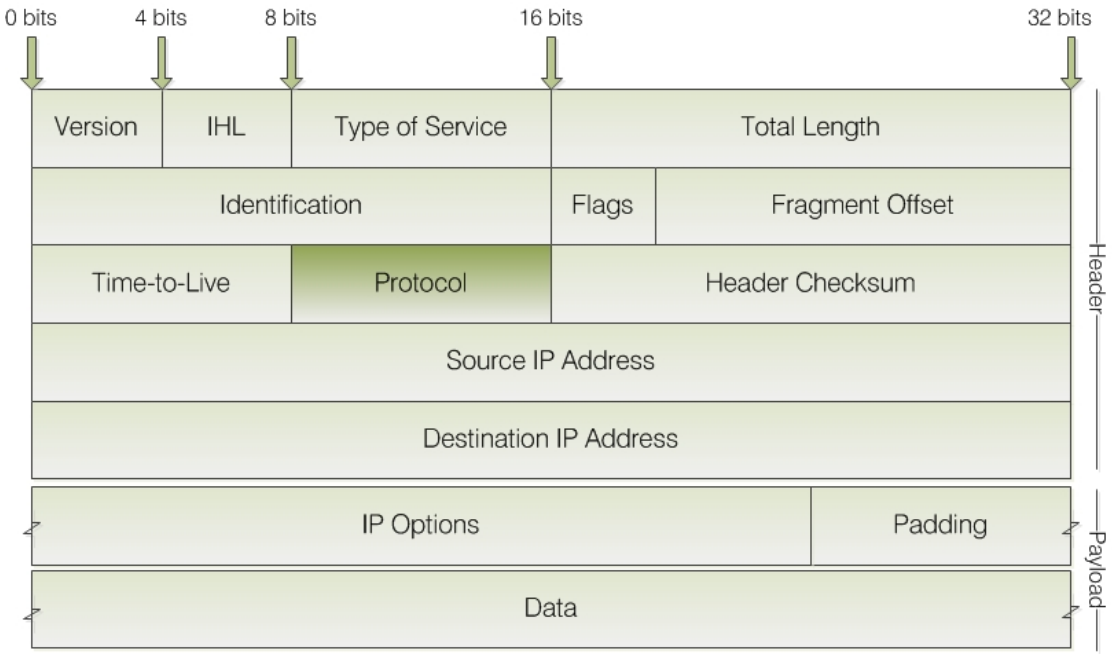
224.0.1.14	IETF-2-AUDIO
224.0.1.15	IETF-2-VIDEO
224.0.1.16	MUSIC-SERVICE
224.0.1.17	SEANET-TELEMETRY
224.0.1.18	SEANET-IMAGE
224.0.1.19	MLOADD
224.0.1.20	any private experiment
224.0.1.21	DVMRP on MOSPF
224.0.1.22	SVRLOC
224.0.1.23	XINGTV
224.0.1.24	microsoft-ds
224.0.1.25	nbc-pro
224.0.1.26	nbc-pfn
224.0.1.27	lmsc-calren-1
224.0.1.28	lmsc-calren-2
224.0.1.29	lmsc-calren-3
224.0.1.30	lmsc-calren-4
224.0.1.31	ampr-info
224.0.1.32	mtrace
224.0.1.33	RSVP-encap-1
224.0.1.34	RSVP-encap-2
224.0.1.35	SVRLOC-DA
224.0.1.36	rln-server
224.0.1.37	proshare-mc
224.0.1.38	unassigned
224.0.1.39	cisco-rp-announce
224.0.1.40	cisco-rp-discovery
224.0.1.41	gatekeeper
224.0.1.42	iberiagames
224.0.1.43	nwn-discovery
224.0.1.44	nwn-adaptor
224.0.1.45	isma-1
224.0.1.46	isma-2
224.0.1.47	telerate
224.0.1.48	ciena

224.0.1.49	dcap-servers
224.0.1.50	dcap-clients
224.0.1.51	mcntp-directory
224.0.1.52	mbone-vcr-directory
224.0.1.53	heartbeat
224.0.1.54	sun-mc-grp
224.0.1.55	extended-sys

Πηγή: IPv4 Multicast Address Space Registry – IANA

Παράρτημα Β’

Η δομή ενός IP Datagram - το πεδίο “Protocol”



Το πεδίο “protocol” του IP datagram περιγράφει το higher-level πρωτόκολλο το οποίο μεταδίδεται με το IP datagram. Αυτό συνήθως είναι είτε κάποιο transport layer είτε κάποιο encapsulated, network layer πρωτόκολλο [14]. Οι τιμές αυτού το πεδίου, που καθορίζονται από την IANA, είναι οι ακόλουθες:

Πρωτόκολλο	Τιμή (δεκαδική)
Reserved	0
ICMP	1
IGMP	2
GGP	3
IP-in-IP Encapsulation	4
TCP	6
EGP	8
UDP	17
Encapsulation Security Payload Extension Header	50
Authentication Header Extension Header	51

Αναφορές

[1] Matrawy, A.; Lambadaris, I.; , "A survey of congestion control schemes for multicast video applications," Communications Surveys & Tutorials, IEEE , vol.5, no.2, pp.22-31, Fourth Quarter 2003

[2] T. Tannenbaum; "IP Multicasting: Diving Through the Layers", Network Computing, November 15, 1996.

[3] Keith W. Ross, James F. Kurose; "Computer Networking: A Top-Down Approach (5th Edition)", Addison Wesley, 2009, ISBN-10: 0136079679

[4] IP Multicast Technology Overview - Cisco Systems

[5] IP-Multicasting Technology - http://www.intelligraphics.com/

[6] Administratively Scoped IP Multicast – RFC2365

[7] Address Allocation for Private Internets – RFC1918

[8] Internet Group Management Protocol – RFC3376

[9] Internet Group Management Protocol, Version 3 - The Internet Engineering Task Force

[10] Host Extensions for IP Multicasting – RFC1112

[11] Internet Group Management Protocol, Version 2 – RFC2236

[12] Overview of IP Multicast - Cisco Systems

[13] Internet Protocol (IP) Multicast - Cisco Systems

[14] IP Datagram General Format - http://www.tcpipguide.com

[15] RFC 5110 - Overview of the Internet Multicast Routing Architecture

[16] Multicast Router Discovery – RFC4286

[17] Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches – RFC4541

[18] Internet Group Management Protocol (IGMP) - Based Multicast Forwarding ("IGMP Proxying") – RFC4605

[19] Shortest-Pa7th Tree (SPT) for multicast - http://www.juniper.net

[20] Rendezvous Point Engineering - http://www.cisco.com

[21] IP Multicast Deployment Fundamentals - Cisco System

[22] White Paper, Overview of IP Multicast - Cisco Systems

[23] Distance Vector Multicast Routing Protocol – RFC1075

[24] Overview of the Internet Multicast Routing Architecture – RFC5110

[25] Generic Routing Encapsulation (GRE) – RFC2784

[26] Kaarle Ritvanen; "Multicast Routing and Addressing", 2004, Helsinki University of Technology, Seminar on Internetworking

[27] Protocol Independent Multicast - Sparse Mode (PIM-SM) – RFC4601

[28] Protocol Independent Multicast - Dense Mode (PIM-DM) – RFC3973

[29] Bidirectional Protocol Independent Multicast (BIDIR-PIM) – RFC5015

[30] Multicast Extensions to OSPF – RFC1584

[31] OSPF Version 2 – RFC2328

[32] Border Gateway Multicast Protocol (BGMP) – RFC3913

[33] Core Based Trees Multicast Routing – RFC2189

[34] Distance Vector vs. Link State Routing - http://www.inetdaemon.com

[35] Kammoun, W.; Youssef, H.; , "Improving the performance of End-to-End single rate Multicast Congestion Control," *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on* , vol., no., pp.1128-1132, 6-9 July 2008

[36] Min-Te Sun; Lifei Huang; Arora, A.; Ten-Hwang Lai; , "Reliable MAC layer multicast in IEEE 802.11 wireless networks," *Parallel Processing, 2002. Proceedings. International Conference on* , vol., no., pp. 527- 536, 18-21 Aug. 2002

[37] Xiaoli Wang; Lan Wang; Wang, Y.; Zhang, Y.; Yamada, A.; , "Supporting MAC Layer Multicast in IEEE 802.11n: Issues and Solutions," *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE* , vol., no., pp.1-6, 5-8 April 2009

[38] IEEE Standard for Information technology - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://standards.ieee.org/getieee802/802.11.html

[39] Nakjung Choi; Yongho Seok; Taekyoung Kwon; Yanghee Choi; , "Leader-Based Multicast Service in IEEE 802.11v Networks," *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE* , vol., no., pp.1-5, 9-12 Jan. 2010

[40] Kammoun, W.; Youssef, H.; , "Improving end-to-end multicast rate control in wireless networks," *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on* , vol., no., pp.643-648, 5-8 July 2009

[41] VPN Technologies - http://www.vpnc.org/

[42] Point-to-Point Tunneling Protocol (PPTP) – RFC2637

[43] http://wikipedia.org

[44] http://openvpn.net/

[45] Gibson's Research - http://www.grc.com

[46] http://www.dd-wrt.com

[47] OpenVpn HowTo and installation

[48] Active Directory Authentication for OpenVPN For Windows Implementations - http://sites.google.com/site/amigo4life2/openvpn

[49] Tunnelblick - http://code.google.com/p/tunnelblick/

[50] VLC media player - http://www.videolan.org/vlc/

[51] Wireshark - http://www.wireshark.org/

[52] PPTP VPN packet capturing demo - http://bit.ly/hIyhBa

[53] Liew, S.C.; , "A general packet replication scheme for multicasting in interconnection networks," INFOCOM '95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People. Proceedings. IEEE , vol., no., pp.394-401 vol.1, 2-6 Apr 1995

[54] Iperf - http://sourceforge.net/projects/iperf/

[55] IGMP Messages - http://www.inetdaemon.com