ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΑΘΗΝΑΣ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

Η ΥΠΗΡΕΣΙΑ IP MULTICASTING - ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΤΗΣ INTER-DOMAIN ΤΕΧΝΟΛΟΓΙΑΣ

ΕΙΣΗΓΗΤΗΣ ΚΑΘΗΓΗΤΗΣ:
Δρ. ΕΥΑΓΓΕΛΟΣ ΒΑΛΑΜΟΝΤΕ

ΣΠΟΥΔΑΣΤΗΣ:
ΜΙΧΑΛΗΣ ΚΟΚΚΙΝΗΣ

ΕΡΕΥΝΗΤΗΣ ΔΙΚΤΥΩΝ:
Δρ. ΙΩΑΝΝΗΣ ΚΟΡΟΒΕΣΗΣ

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ "ΔΗΜΟΚΡΙΤΟΣ"

Ευχαριστίες

Η συγκεκριμένη πτυχιακή εργασία ολοκληρώθηκε στα πλαίσια μελέτης που πραγματοποιήθηκε στο εργαστήριο Internet Systematics Lab, για την υλοποίηση της υπηρεσίας Multicasting του δικτύου “Αριάδνη” στο ΕΚΕΦΕ Δημόκριτος. Συνεπώς αισθάνομαι την ανάγκη να ευχαριστήσω τον Δρ.Γιάννη Κοροβέση, επιστημονικό υπεύθυνο του εργαστηρίου και του δικτύου Αριάδνη, για την πολύτιμη καθοδήγηση του και την ευκαιρία που μου έδωσε να γνωρίσω από κοντά πολλές από τις βασικές τεχνολογίες του διαδικτύου. Επίσης, θα ήθελα να ευχαριστήσω τους καθηγητές μου στο ΤΕΙ Αθήνας, Δρ. Ε.Βαλαμόντε και Δρ. Ι.Ράπτη, οι οποίοι με έφεραν σε επαφή με το εργαστήριο και παράλληλα μου στάθηκαν σε κάθε βήμα προς την ολοκλήρωση της εργασίας αυτής. Επίσης, θα ήθελα να εκφράσω τις ιδιαίτερες ευχαριστίες μου στον τεχνικό υπεύθυνο του δικτύου Χάρη Κουτσούρη, για το ιδιαίτερο ενδιαφέρον και ζήλο που έδειξε για το θέμα τόσο σε πρακτικό όσο και θεωρητικό επίπεδο. Ακόμα, θα ήθελα να ευχαριστήσω του συνεργάτες και φίλους Κ.Καραφασούλη, Κ.Μάγκο, Γ.Βιδάκη και Γ.Παπαπάνο για τις πολύ σημαντικές παρατηρήσεις και συμβουλές τους.
Κλείνοντας, θα ήθελα να διευκρινίσω ότι τυχόν λάθη και παραλείψεις σε σχέση με το θέμα βαρύνουν αποκλειστικά τον υπεύθυνο σπουδαστή.

Πρόλογος

Τα τελευταία χρόνια υπάρχει μεγάλη ανάπτυξη στην χρήση του διαδικτύου και ιδιαίτερα των εφαρμογών μετάδοσης πραγματικού χρόνου όπως είναι η ζωντανές μεταδόσεις ήχου και εικόνας σε πολλαπλούς αποδέκτες. Η χρησιμοποίηση των κλασικών μεθόδων αποστολής των πακέτων (unicasting) έχουν οδηγήσει στην μεγάλη σπατάλη των πόρων του Internet. Η τεχνολογία multicasting αποσκοπεί στην λύση αυτού του προβλήματος και παρουσιάζει μια συνεχής εξέλιξη και βελτίωση, που σε συνδυασμό με την αυξανόμενη χρήση από πολλούς παροχής υπηρεσιών Internet (Internet Service Provider) αποτελεί πρόκληση για τους μηχανικούς του Internet.Παρά τις δυνατότητές του, το multicasting έχει ακόμα πολλά προβλήματα να ξεπεράσει. Το multicasting είναι μια παλιά επινόηση, αλλά η ανάπτυξή του έχει γίνει με αργά βήματα. Αυτό θα το παρατηρήσουμε καλύτερα αν το συγκρίνουμε με το World Wide Web (WWW) και το Hyper Text Transform Protocol (HTTP). Το IP Multicasting πρωτοπαρουσιάσθηκε στην διδακτορική διατριβή του Steve Deering το 1988 και δοκιμάστηκε πρώτη φορά για μετάδοση ήχου το 1992 σε ένα συνέδριο της Internet Engineering Task Force (IETF) στο San Diego. Ο πρώτος WWW browser γράφτηκε το 1990 και το 1993 υπήρχαν 100 site στο WWW. Βλέπουμε λοιπόν ότι το multicasting έχει την ίδια ηλικία με το WWW αλλά πολύ μικρότερη ανάπτυξη και χρησιμοποίηση. Για πολλά χρόνια οι ρυθμίσεις που απαιτούνταν στους δρομολογητές ήταν αρκετά πολύπλοκες και η συντήρηση της multicast υποδομής κατέληξε σχεδόν αδύνατη. Αυτό έρχεται σε αντίθεση με το κλασικό μοντέλο του IP internet και περιορίζει τις δυνατότητες του IP multicasting.Με αυτά τα προβλήματα, η εικόνα του multicasting ίσως να μην φαίνεται καλή, όμως με τις τελευταίες τοπολογίες και τα πρωτόκολλα που έχουν αναπτυχθεί έχουν ξεπεραστεί πολλές αδυναμίες.

Η IP Multicast τεχνολογία χρησιμοποιείται σε περιπτώσεις που η ίδια πληροφορία πρέπει να σταλεί σε πολλαπλούς προορισμούς, με σκοπό την καλύτερη διαχείριση του Bandwidth και τον περιορισμό του φορτίου στους δρομολογητές. Εφαρμογές που εκμεταλλεύονται την τεχνολογία αυτή είναι: το video conference, οι ζωντανές μεταδόσεις ήχου και εικόνας και γενικότερα εφαρμογές πραγματικού χρόνου με πολλαπλούς αποδέκτες.Σε αυτή την πτυχιακή εργασία επιχειρείται μια μελέτη των βασικών τεχνολογικών εννοιών και των πρωτοκόλλων υλοποίησης της. Παρουσιάζονται εργαλεία με τα οποία μπορεί να την αξιοποιήσει ο τελικός χρήστης και την μέθοδο ενεργοποίησης της σε ένα δίκτυο. Παρουσιάζεται η υλοποίηση της τεχνολογίας Inter-Domain IP Multicasting του δικτύου Αριάδνη (Ε.Κ.Ε.Φ.Ε. «Δημόκριτος») με το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ). Συγκεκριμένα περιέχει τα εξής κεφάλαια:

1. Βασικές Έννοιες του IP Multicasting
2. Multicast Εργαλεία
3. Multicast Αλγόριθμοι δρομολόγησης και δέντρα διανομής
4. Intra-domain Multicasting (PIM-SM)
5. Interdomain Multicasting (MBGP, MSDP)
6. Configuring Routers for IP Multicasting
7. Multicast Debugging (εντολές show και το Mhealth)
8. SDP και SAP

Κεφάλαιο 1ο: Βασικές Έννοιες του IP Multicasting

1.1 Εισαγωγή

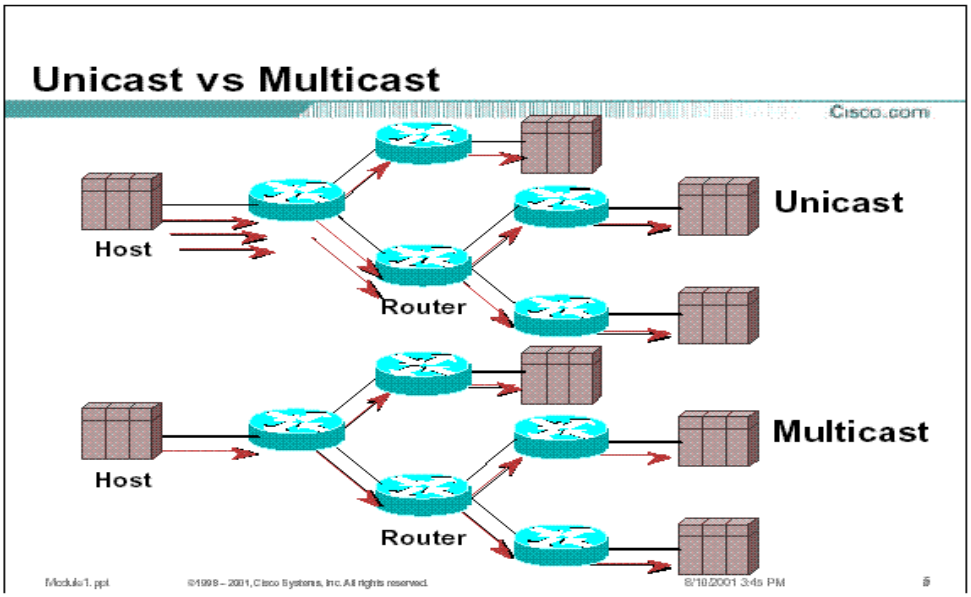
Πριν ξεκινήσουμε την ανάλυση της τεχνολογίας IP Multicasting, κρίνεται σκόπιμο να δοθούν κάποιες βασικές έννοιες, οι οποίες θα μας βοηθήσουν να κατανοήσουμε την παραπέρα ανάλυση. Συγκεκριμένα, θα εισάγουμε την έννοια του IP Multicasting και θα διακρίνουμε τις διαφορές του από το unicasting, την τεχνολογία που χρησιμοποιείται μέχρι τώρα ευρύτατα στο internet. Στη συνέχεια, θα αναφερθούμε πιο αναλυτικά στα πλεονεκτήματα και τα μειονεκτήματα της χρήσης του IP Multicasting, καθώς και στις εφαρμογές που αποκτούν πλεονέκτημα από αυτή. Επίσης θα δούμε την έννοια της multicast ομάδας, τις IP multicast διευθύνσεις, που χρησιμοποιούν οι ομάδες αυτές, και τέλος θα αναλύσουμε το Internet Group Management Protocol (IGMP), το πρωτόκολλο, δηλαδή, που χρησιμοποιούν τα PC's και οι δρομολογητές για να πετύχουν μεταξύ τους multicast επικοινωνία.

1.2 Τι είναι το IP Multicasting

Το IP Multicasting είναι μία από τις τρεις βασικές τεχνικές μετάδοσης στο IPv4, ενώ οι άλλες δύο είναι η unicast και η broadcast. Όμως, για να ορίσουμε την πρώτη τεχνική, θα διευκολυνθούμε καλύτερα, αν προηγηθούν οι ορισμοί των άλλων δύο.

Μια πηγή, με τη χρήση του unicasting, στέλνει ένα μήνυμα σε ένα και μόνο αποδέκτη, δηλαδή, ένα πακέτο μεταφέρεται από ένα αποστολέα σε ένα και μόνο παραλήπτη. Με το broadcasting μια πηγή στέλνει δεδομένα σε όλες τις μηχανές που καθορίζονται από την broadcast διεύθυνση προορισμού. Η multicast τεχνολογία, στη συνέχεια, βρίσκεται κάπου ανάμεσα στις δύο προηγούμενες. Με αυτή την τεχνική, μια ή περισσότερες πηγές στέλνουν δεδομένα σε μια καθορισμένη ομάδα αποδεκτών. Παρά το γεγονός ότι αυτό θα μπορούσε να γίνει αν η πηγή έστελνε με unicasting σε κάθε αποδέκτη χωριστά, υπάρχουν αρκετοί λόγοι να χρησιμοποιήσουμε την multicasting τεχνολογία. Ένας από αυτούς και ίσως ο βασικότερος είναι η κατά πολύ μικρότερη επιβάρυνση του δικτύου σε σχέση με το unicasting. Με το IP multicasting η πληροφορία μεταφέρεται στους multicast δρομολογητές, οι οποίοι αν είναι συνδεδεμένοι με πάνω από ένα ενδιαφερόμενο γι αυτήν, δημιουργούν ξανά τα δεδομένα και τα στέλνουν στους αποδέκτες. Έτσι έχουμε πολλαπλή αποστολή χωρίς να σπαταλούμε το bandwidth. Η εικόνα 1.1 δείχνει παραστατικά την διαφορά του unicast με το multicast.

Στην εικόνα 1.1 βλέπουμε ότι στο unicast η πηγή στέλνει τρία αντίγραφα των δεδομένων και το δίκτυο τα προωθεί σε τρεις διαφορετικούς αποδέκτες. Η πηγή δηλαδή, μπορεί να στέλνει μόνο σε ένα παραλήπτη τη φορά. Αντιθέτως, στο multicast η πηγή στέλνει ένα αντίγραφο και το δίκτυο κατασκευάζει πανομοιότυπα στο τελευταίο δυνατό hop για κάθε αποδέκτη. Έτσι, κάθε πακέτο υπάρχει μόνο μια φορά στο δίκτυο και παράλληλα η πηγή μπορεί να στέλνει σε πολλούς αποδέκτες ταυτόχρονα. Η σύγκριση θα ήταν πιο εντυπωσιακή και ο λόγος χρήσης του multicasting πιο εμφανής, στην περίπτωση ενός μεγάλου δικτύου με εκατοντάδες αποδέκτες.



Εικόνα 1.1: Διαφορά του multicast με το unicast

1.3 Πλεονεκτήματα και μειονεκτήματα του IP multicasting

Η multicast μεταφορά έχει αρκετά σημαντικά πλεονεκτήματα σε σχέση με την unicast, κυρίως όταν πρόκειται για αποστολή από μια πηγή σε πολλούς αποδέκτες ή από πολλές πηγές σε πολλούς αποδέκτες. Πρώτον, όπως αναφέραμε και προηγουμένως, χρησιμοποιεί καλύτερα το διαθέσιμο bandwidth του δικτύου. Επίσης, το γεγονός ότι λιγότερα δεδομένα χρειάζονται επεξεργασία και προώθηση αποτελεί κέρδος σε υπολογιστική δύναμη (σε υπολογιστές και δρομολογητές).

Μειονέκτημα του multicasting μπορεί να θεωρηθεί το γεγονός ότι βασίζεται στο UDP, οπότε έχει όλα τα μειονεκτήματα του συγκεκριμένου πρωτοκόλλου, σε αντίθεση με το unicasting που μπορεί να χρησιμοποιεί και το TCP. Έτσι, εφαρμογές πραγματικού χρόνου, όπως είναι οι εκπομπές ήχου και εικόνας, μπορεί να επηρεαστούν από τα χαμένα πακέτα, αφού δεν υπάρχει επανεκπομπή. Επίσης το UDP δεν υποστηρίζει έλεγχο της συμφόρησης, πράγμα που μπορεί να προκαλέσει προβλήματα, αν η χρήση του multicasting γίνει πιο ευρεία. Το πρόβλημα αυτό αντιμετωπίζεται από κάποιες εφαρμογές οι οποίες χρησιμοποιούν Real Time πρωτόκολλα (π.χ RTP[1]), που τρέχουν πάνω από το UDP.

1.4 Εφαρμογές που χρησιμοποιούν το IP multicasting

Οι εφαρμογές στις οποίες χρησιμοποιείται το multicasting μπορεί να είναι πραγματικού και μη πραγματικού χρόνου. Πραγματικού χρόνου εφαρμογές είναι οι ζωντανές μεταδόσεις ήχου και εικόνας, η αποστολή χρηματοοικονομικών δεδομένων και η video συνδιάσκεψη, ενώ μη πραγματικού χρόνου είναι η μεταφορά αρχείων, η απάντηση σε δεδομένα ή αρχεία και video-on-demand.

[1] Στο κεφάλαιο 7 αναφέρεται διεξοδικά το RTP.

1.5 Multicast Ομάδα (Group)

Το multicasting βασίζεται στην έννοια της ομάδας (group). Μια μηχανή (host) που θέλει να λάβει multicast δεδομένα συμμετέχει στην ομάδα, στην οποία η πηγή στέλνει αυτά τα δεδομένα. Οι ομάδες αυτές δεν έχουν γεωγραφικά και φυσικά όρια και έτσι ένας host μπορεί να βρίσκεται σε οποιοδήποτε σημείο στο internet. Επίσης, δεν υπάρχει περιορισμός στον αριθμό των hosts που μπορούν να συνδεθούν σε μια ομάδα, αλλά ούτε και στον αριθμό των ομάδων που μπορεί να συνδεθεί ένας host. Οι hosts που θέλουν να πάρουν συγκεκριμένα δεδομένα από κάποια multicast ομάδα πρέπει να γίνουν μέλη της ομάδας, ενώ για να στείλουν multicast δεδομένα στην ομάδα κάτι τέτοιο δεν είναι υποχρεωτικό. Ένας host που ανήκει σε ένα LAN αλλά ταυτόχρονα και σε μια multicast ομάδα παρακολουθεί την κίνηση και παίρνει τα multicast πακέτα που προορίζονται για αυτόν. Η συμμετοχή σε μια multicast ομάδα είναι δυναμική, πράγμα που δίνει τη δυνατότητα σε ένα host να συνδεθεί ή να αποσυνδεθεί όποτε αυτός επιθυμεί.

1.6 IP Multicast Διευθύνσεις

Κάθε ομάδα παίρνει μια διεύθυνση τάξης D, της οποίας τα τέσσερα πρώτα δυαδικά ψηφία είναι 1110 και κάθε διεύθυνση είναι μεταξύ 224.0.0.0 και 239.255.255.255 (224.0.0.0/4). Ο αποστολέας στέλνει πακέτα σε μια multicast ομάδα, χρησιμοποιώντας τις multicast διευθύνσεις σαν IP διευθύνσεις προορισμού των πακέτων αυτών.

1.6.1 Δεσμευμένα Πεδία Διευθύνσεων

Το εύρος των multicast διευθύνσεων χωρίζεται σε μικρότερα πεδία, που έχουν παρακρατηθεί για κάποιο συγκεκριμένο λόγο. Τα πεδία αυτά ανάλογα με το σκοπό διακρίνονται σε: i) τοπικού σκοπού (local scope), ii) γενικού σκοπού iii) περιορισμένου σκοπού (limited scope) ή σκοπού διαχείρισης (administrative scope) και iv) glop addressing.

- Τοπικού Σκοπού Διευθύνσεις

Οι διευθύνσεις 224.0.0.0 έως 224.0.0.255 είναι δεσμευμένες για χρήση από τα πρωτόκολλα δρομολόγησης και άλλες χαμηλού επιπέδου ενέργειες, όπως η ανακάλυψη του gateway και η αναφορά για συμμετοχή σε κάποια ομάδα. Τα πακέτα με τέτοιες διευθύνσεις προορισμού δεν προωθούνται ποτέ από δρομολογητές, χρησιμοποιούνται μέσα σε ένα LAN και έχουν πάντα time-to-live (TTL) 1. Μερικές γνωστές διευθύνσεις αυτού του πεδίου είναι:

Address	Usage
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet
224.0.0.5	OSPF Routers
224.0.0.6	OSPF Designated Routers
224.0.0.12	DHCP Server/Relay Agent
224.0.0.13	PIMv2
224.0.1.39	CISCO-RP-ANNOUNCE (Auto-RP)

224.0.1.40 CISCO-RP-DISCOVERY (Auto-RP)

- Διευθύνσεις Γενικού Σκοπού

Οι διευθύνσεις από 224.0.1.0 έως 238.255.255.255 είναι γενικού σκοπού και μπορούν να χρησιμοποιηθούν από οποιαδήποτε ομάδα στο internet. Μερικές από αυτές τις διευθύνσεις έχουν δεσμευτεί από την IANA για χρήση από multicast εφαρμογές. Για παράδειγμα η 224.0.1.1 έχει δεσμευτεί από το Network Time Protocol (NTP).

- Limited Scope ή Administrative Scope Addresses

Οι διευθύνσεις από 239.0.0.0 έως 239.255.255.255 λέγονται Limited Scope Addresses ή Administratively Scoped Addresses και δίνονται σε τοπικά group ή οργανισμούς. Οι δρομολογητές είναι ρυθμισμένοι με φίλτρα, που αποτρέπουν την προώθηση της multicast κίνησης έξω από ένα αυτόνομο σύστημα όταν τα πακέτα έχουν διεύθυνση προορισμού που αντιστοιχεί μέσα σε αυτό το εύρος διευθύνσεων.

- Glop Addressing

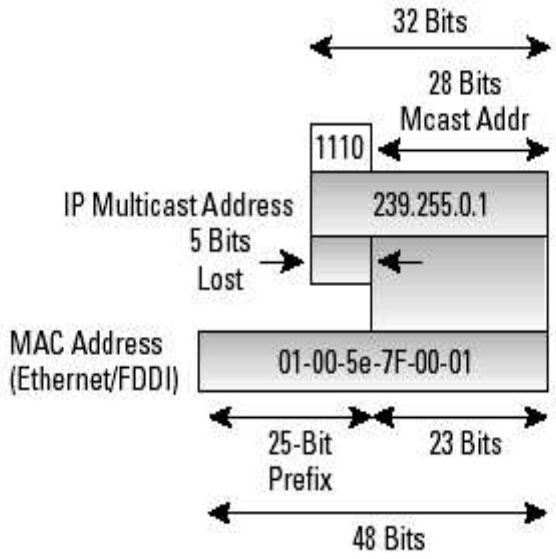
Οι multicast διευθύνσεις παραδοσιακά δεσμεύονται με την βοήθεια ενός δυναμικού μηχανισμού (πχ SDR). Όμως, πολλά αυτόνομα συστήματα και multicast εφαρμογές δε δέχονται αυτό το δυναμικό μηχανισμό. Η IANA έδωσε το πεδίο 233/8 για στατική δέσμευση multicast διευθύνσεων που ονομάζεται Glop Addressing. Το πεδίο των διευθύνσεων 233.0.0.0/8 είναι δεσμευμένο από τα αυτόνομα συστήματα που έχουν ένα AS νούμερο. Αυτό μπαίνει στην $2^{η}$ και $3^{η}$ οχτάδα της 233.0.0.0/8. Για παράδειγμα, ο AS 2546_{10} είναι $9F2_{16}$. Χωρίζεται σε δύο οχτάδες 09 και F2 και παίρνουμε 9 και 242 δεκαδικό. Αυτό μας δίνει το υποδίκτυο 233.9.242.0 που είναι δεσμευμένο από το AS 2546[1].

1.6.2 Ethernet Mac Address Mapping

Η IP multicast τεχνολογία επεκτείνεται και στο Ethernet. Για να υπάρξει επικοινωνία σε επίπεδο Ethernet πρέπει να μετατραπούν οι IP multicast διευθύνσεις σε Ethernet multicast διευθύνσεις.

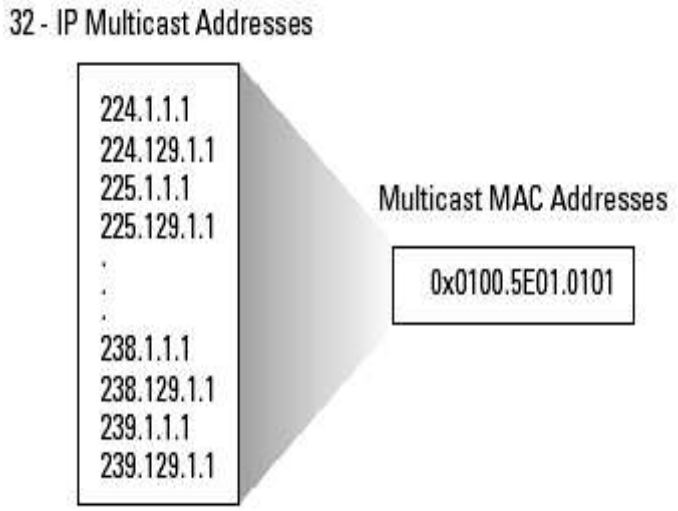
Η IANA διαχειρίζεται έναν αριθμό από Ethernet Mac διευθύνσεις, που αρχίζουν με το δεκαεξαδικό 01.00.5E. Οι μισές από αυτές τις διευθύνσεις είναι δεσμευμένες για multicast διευθύνσεις, οπότε το πεδίο που είναι διαθέσιμο για Ethernet Mac διευθύνσεις είναι από 01.00.5e.00.00.00 έως 01.00.5e.7f.ff.ff. Για την μετατροπή μιας IP multicast διεύθυνσης σε Ethernet multicast διεύθυνση τοποθετούμε τα 23 λιγότερο σημαντικά bits της IP multicast διεύθυνσης στα 23 λιγότερο σημαντικά bits της ειδικής multicast Ethernet διεύθυνσης που έχει καθοριστεί να είναι $01.00.5E.00.00.00_{16}$.

[1] Για περισσότερες πληροφορίες για τις γνωστές multicast διευθύνσεις δείτε το Παράρτημα ΙΙΙ.



Εικόνα 1.2: Ethernet Mac Address Mapping

Όπως φαίνεται και στην εικόνα 1.2, επειδή 5 bits της IP multicast διεύθυνσης δεν χρησιμοποιούνται στη μετατροπή, η διεύθυνση που προκύπτει δεν είναι μοναδική. Στην πραγματικότητα, 32 IP multicast διευθύνσεις αντιστοιχούν στην ίδια Ethernet Mac διεύθυνση (εικόνα 1.3).



Εικόνα 1.3: Η μετατροπή σε Ethernet δεν είναι μοναδική

1.7 Internet Group Management Protocol (IGMP)

Σε αυτή την παράγραφο θα δούμε τον τρόπο με τον οποίο επιτυγχάνεται η συμμετοχή μιας μηχανής (host) σε μια ομάδα. Το Internet Group Management Protocol (IGMP) χρησιμοποιείται από τους hosts για να αναφέρουν την συμμετοχή τους σε μια ομάδα, σε ένα κατευθείαν συνδεδεμένο multicast δρομολογητή[1]. Η κίνηση αυτή προτρέπει τους δρομολογητές να συνδεθούν σε ένα συγκεκριμένο multicast group για να

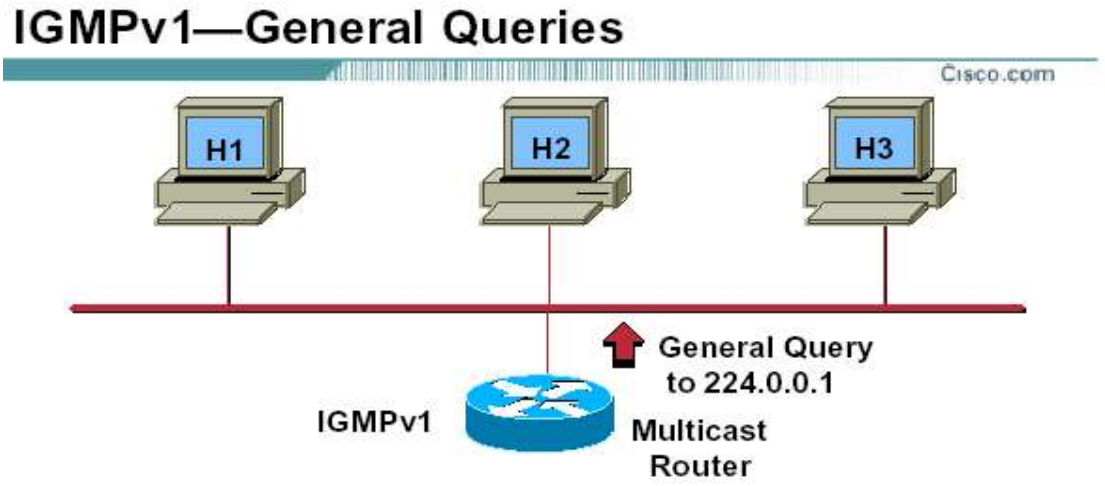
[1] Κατευθείαν συνδεμένο δρομολογητή ονομάζουμε το δρομολογητή που σε κάποιο interface του έχει συνδεμένο κάποιο PC. Συχνά τον ονομάζουμε και leaf δρομολογητή.

αρχίσουν να προωθούν κίνηση στο δίκτυο. Όπως το ICMP, έτσι και το IGMP είναι ένα τμήμα του IP. Υπάρχουν τρεις εκδόσεις του IGMP. Η πρώτη έκδοση παρουσίασε πολλά προβλήματα, γεγονός που το 1997 οδήγησε στην ανάπτυξη της δεύτερης έκδοσης. Η τρίτη έκδοση βρίσκεται ακόμα σε πειραματικό στάδιο.

1.7.1 IGMP έκδοση 1

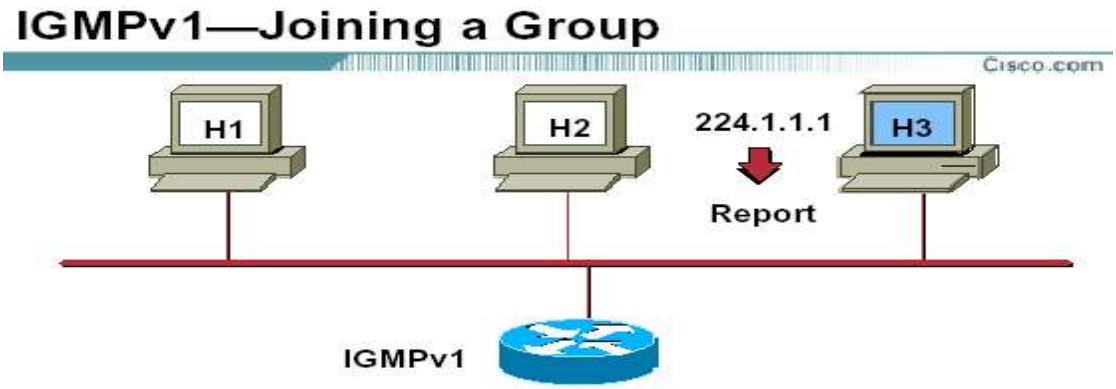
Στην έκδοση 1 του IGMP, όπως καθορίζεται από το Appendix 1 του RFC 1112, υπάρχουν δύο είδη μηνυμάτων: το μήνυμα-ερώτημα συμμετοχής και το μήνυμα-αναφορά συμμετοχής.

Οι multicast δρομολογητές στέλνουν μηνύματα-ερωτήματα συμμετοχής, για να ανακαλύψουν ποιες ομάδες έχουν μέλη που ανήκουν και στο τοπικό τους δίκτυο (εικόνα 1.4). Τα ερωτήματα στέλνονται στην all-hosts multicast διεύθυνση (224.0.0.1) και έχουν IP time-to-live 1. Ένας δρομολογητής του τοπικού δικτύου έχει την ιδιότητα να στέλνει τα ερωτήματα (querier) στους hosts. Δεν υπάρχει κάποια διαδικασία στο IGMPv1 για την εκλογή του δρομολογητή που κάνει τις ερωτήσεις. Κάθε multicast πρωτόκολλο δρομολόγησης χρησιμοποιεί διαφορετικούς μηχανισμούς. Αυτό συχνά έχει σαν αποτέλεσμα να στέλνονται πολλά ταυτόχρονα ερωτήματα από διαφορετικούς δρομολογητές. Τα ερωτήματα επαναλαμβάνονται κάθε 60-120 δευτερόλεπτα.



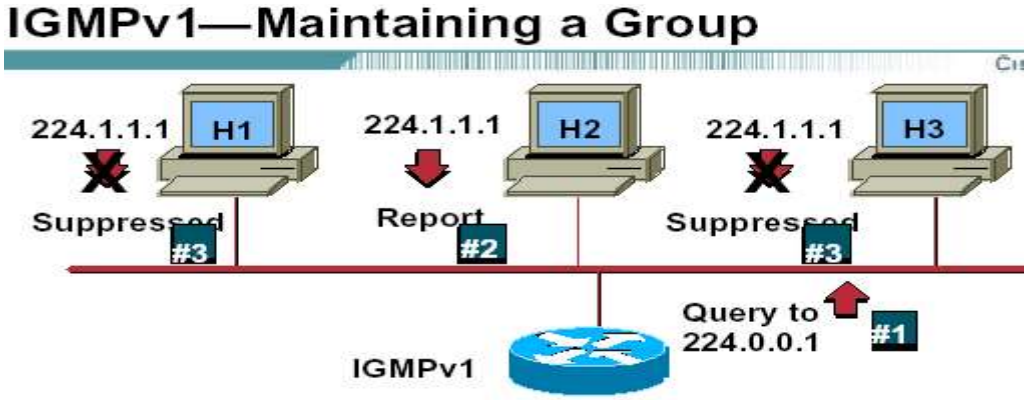
Εικόνα 1.4

Οι hosts στέλνουν IGMPv1 μηνύματα-αναφορές συμμετοχής εκφράζοντας την επιθυμία να λάβουν δεδομένα από μια συγκεκριμένη multicast ομάδα. Τα μηνύματα αυτά στέλνονται με TTL 1 στην multicast διεύθυνση του group, είτε μετά από ένα ερώτημα, είτε μόλις θελήσουν οι hosts να συνδεθούν στο group και χρησιμοποιούνται για να κρατηθεί το group ενεργό, έτσι ώστε η κίνηση να συνεχιστεί να προωθείται στο δίκτυο. Στην εικόνα 1.5 ο H3 στέλνει IGMPv1 αναφορά στο multicast group 224.1.1.1.



Εικόνα 1.5

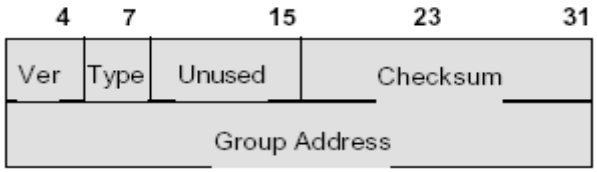
Για να αποφευχθεί μια πιθανή κατάρρευση λόγω αύξησης της κίνησης στο δίκτυο από ταυτόχρονες αναφορές, μόνο ένα μέλος για κάθε ομάδα απαντάει σε ένα ερώτημα. Όταν ένας host λάβει ένα ερώτημα, ένα χρονόμετρο τίθεται σε αντίστροφη μέτρηση για κάθε ομάδα που είναι μέλος. Μόλις λήξει ο χρόνος αυτός, ο host στέλνει την αντίστοιχη απάντηση. Αν όμως κάποιος host της ομάδας στείλει πρώτος απάντηση στον δρομολογητή, τότε η απάντηση λαμβάνεται και από τους άλλους hosts του δικτύου που αμέσως ακυρώνουν τη διαδικασία για να στείλουν απάντηση, μέχρι να ξαναδεχτούν νέο ερώτημα. Στο παράδειγμα της εικόνας 1.6, το χρονόμετρο του H2 τελείωσε πρώτο οπότε έστειλε απάντηση στον δρομολογητή και οι H1,H3 ακυρώνουν τις απαντήσεις τους.



Εικόνα 1.6

Στο IGMPv1 δεν υπάρχει κάποιος ιδιαίτερος μηχανισμός, με τη βοήθεια του οποίου ένας host να δηλώνει ότι θέλει να εγκαταλείψει την ομάδα. Άρα οι hosts εγκαταλείπουν μια ομάδα οποιαδήποτε στιγμή, χωρίς να ενημερώνουν τον τοπικό δρομολογητή. Κάτι τέτοιο δε δημιουργεί πρόβλημα, όταν στην ομάδα παραμένουν ενεργοί και άλλοι αποδέκτες. Όμως, αν και το τελευταίο μέλος της ομάδας στο LAN αποχωρήσει, υπάρχει μια χρονική περίοδος που ο δρομολογητής συνεχίζει να προωθεί άσκοπη multicast κίνηση, αφού δεν υπάρχουν μέλη να τη δεχτούν. Ο δρομολογητής, όμως, θα σταματήσει την προώθηση, αν μετά από μερικά ερωτήματα δε λάβει καμία απάντηση, γεγονός που δημιουργεί προβλήματα, αν ο αριθμός των ομάδων ή η κίνηση γι αυτές τις ομάδες είναι μεγάλη.

Η εικόνα 1.7 δείχνει την διαμόρφωση του IGMPv1 πακέτου.



Εικόνα 1.7

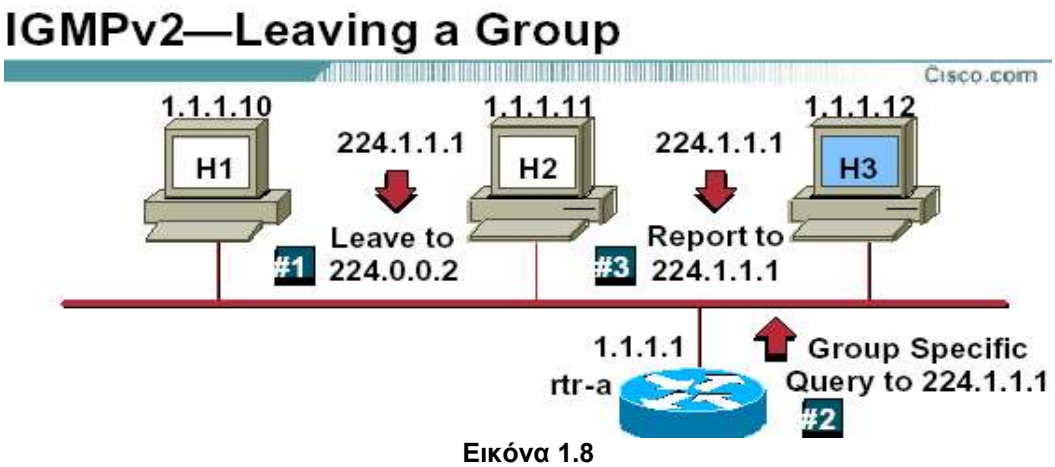
Τα πέντε πρώτα bit (ver) είναι η έκδοση του IGMP που μπορεί να είναι 0 ή 1. Τα επόμενα τρία (type) καθορίζουν το είδος του μηνύματος, δηλαδή αν είναι ερώτημα ή απάντηση και το πεδίο Group Address καθορίζει την IP διεύθυνση του group που στέλνονται τα μηνύματα-απαντήσεις.

1.7.2 IGMP έκδοση 2

Από τα παραπάνω φαίνεται ότι το IGMPv1 έχει μερικά μειονεκτήματα, τα οποία προσπάθησε να καλύψει η δημιουργία του IGMPv2. Οι περισσότερες από τις αλλαγές μεταξύ IGMPv1 και IGMPv2, έγιναν κυρίως για να διορθώσουν το πρόβλημα της καθυστέρησης που δημιουργείται κατά την σύνδεση και αποσύνδεση ενός host σε μια ομάδα.

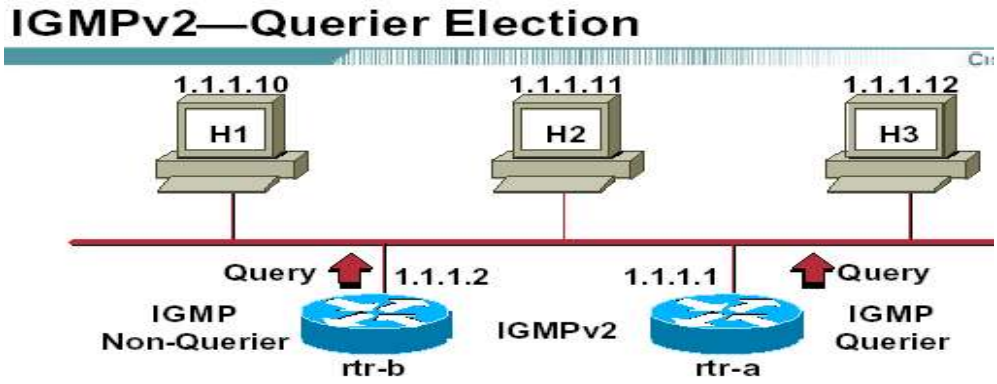
Στο IGMPv2 προστέθηκε ένα μήνυμα-ερώτημα που επιτρέπει στον δρομολογητή να ρωτάει μόνο μια συγκεκριμένη ομάδα και όχι όλες τις ομάδες, συντελώντας με αυτόν τον τρόπο στην ταχύτερη εύρεση μιας πιθανής αποχώρησης ενός μέλους από κάποια ομάδα, αφού πλέον δε χρειάζεται να ρωτηθούν όλες οι ομάδες. Το ερώτημα για συγκεκριμένη ομάδα δε στέλνεται στο ‘’All-Hosts’’ group (224.0.0.1), αλλά στη multicast διεύθυνση του group με TTL 1.

Επίσης στην έκδοση 2 δίνεται η δυνατότητα αποστολής μηνύματος εγκατάλειψης της ομάδας, που επιτρέπει σε τελικά συστήματα (π.χ hosts) να ενημερώνουν τους δρομολογητές ότι εγκαταλείπουν την ομάδα. Το μήνυμα αυτό στέλνεται στην “All-Routers” ομάδα (224.0.0.2), γεγονός που μειώνει την καθυστέρηση που δημιουργείται μέχρι ο δρομολογητής να εντοπίσει ότι δεν υπάρχει άλλο μέλος στην ομάδα. Στο παράδειγμα της εικόνας 1.8 ο H2 εγκαταλείπει την ομάδα και ο δρομολογητής στέλνει ερώτημα στην συγκεκριμένη ομάδα για να δει αν υπάρχει άλλο μέλος. Ο H3, όμως, που δεν έχει εγκαταλείψει την ομάδα στέλνει απάντηση.



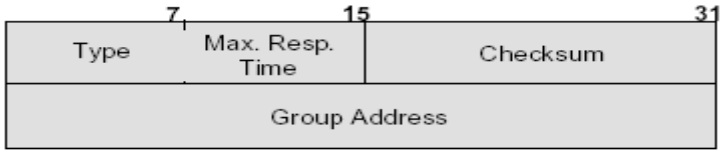
Εικόνα 1.8

Το IGMPv2 σε αντίθεση με το IGMPv1 έχει μηχανισμό εκλογής του δρομολογητή-ερωτώντος (querier router). Ο δρομολογητής με την χαμηλότερη unicast IP διεύθυνση, που υποστηρίζει IGMP, εκλέγεται να είναι ο ερωτών. Όλοι οι δρομολογητές του δικτύου αρχικά υποθέτουν ότι είναι ερωτώντες και αρχίζουν να στέλνουν ερωτήματα. Κάθε δρομολογητής βλέπει αυτά τα ερωτήματα και εξετάζει την IP διεύθυνση, ενώ τελικά ερωτών εκλέγεται αυτός με την μικρότερη διεύθυνση και όλοι οι άλλοι το αποδέχονται. Η εικόνα 1.9 δείχνει τον τρόπο λειτουργίας του μηχανισμού που μόλις περιγράψαμε.



Εικόνα 1.9

Το πακέτο του IGMPv2 έχει ως εξής:



Εικόνα 1.10

Στο IGMPv2, το παλιό πεδίο “ver” των 4 bit ενώθηκε με το πεδίο “Type” των 4 bit και δημιουργήθηκε ένα νέο “Type” πεδίο των 8 bit. Γενικότερα τα πεδία είναι:

Type:

0x11= Ερώτημα συμμετοχής
0x12= Έκδοση 1 αναφορά συμμετοχής
0x16= Έκδοση 2 αναφορά συμμετοχής
0x17= Μήνυμα εγκατάλειψης της ομάδας

Max. Resp. Time

Μέγιστος χρόνος μέχρι να σταλεί απάντηση

Group Address:

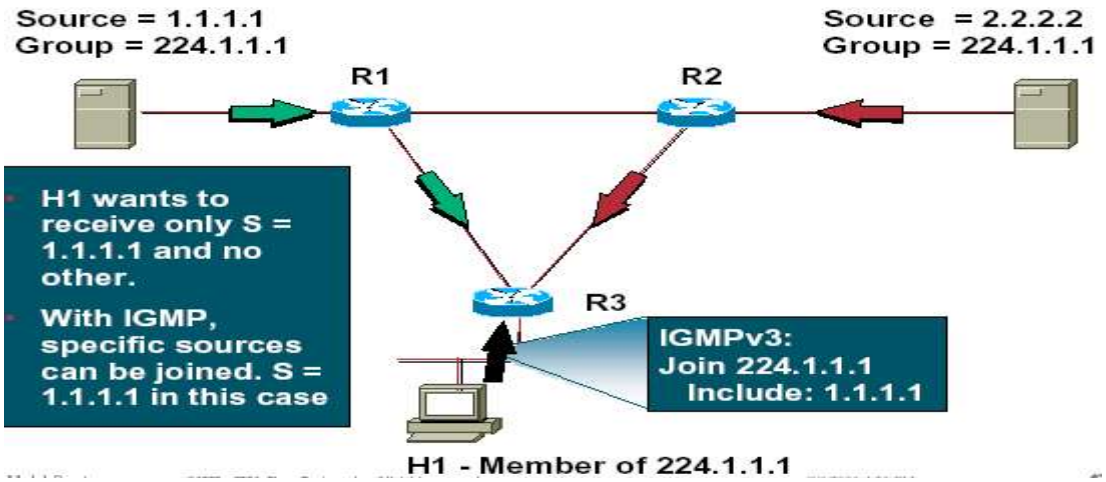
Η multicast διεύθυνση της ομάδας

Οι δρομολογητές που τρέχουν IGMPv1 δεν αναγνωρίζουν IGMPv2 αναφορές για συμμετοχή. Οπότε, όταν IGMPv2 hosts υπάρχουν στο ίδιο δίκτυο με ένα IGMPv1 δρομολογητή, οι hosts πρέπει να στέλνουν IGMPv1 αναφορές για να τους αναγνωρίζει ο δρομολογητής, ενώ σε μια τέτοια περίπτωση δεν υπάρχει λόγος οι hosts να στέλνουν μηνύματα αποχώρησης. Επίσης, συμβατότητα πρέπει να υπάρχει και στην περίπτωση που ο

δρομολογητής έχει έκδοση 2 και οι hosts έκδοση 1. Τέλος, όλοι οι δρομολογητές σε ένα δίκτυο πρέπει να τρέχουν την ίδια έκδοση του IGMP.

1.7.3 IGMP έκδοση 3

Η κύρια αλλαγή που επήλθε στο IGMPv3 είναι ότι κάθε ομάδα έχει μια λίστα από πηγές, από τις οποίες μπορεί να επιλέξει να λάβει δεδομένα ή όχι. Πιο συγκεκριμένα, ένας host του οποίου η ομάδα παίρνει δεδομένα από πολλές πηγές έχει το δικαίωμα να διαλέξει από ποιες πηγές θα λαμβάνει και από ποιες όχι. Οι IGMPv3 hosts δε στέλνουν τις αναφορές στην multicast group διεύθυνση, αλλά στην “All-IGMPv3 Routers” multicast διεύθυνση που είναι η 224.0.0.22. Οι δρομολογητές ακούν στην 224.0.0.22 για να δουν ποιοι hosts θέλουν να συνδεθούν στο group. Οι hosts δεν ακούν στην 224.0.0.22 οπότε δεν ξέρουν τις αναφορές για συμμετοχή των άλλων hosts. Η εικόνα 11 δείχνει ένα χαρακτηριστικό παράδειγμα του IGMPv3. Ο H1 επιθυμεί να συνδεθεί στο group 224.1.1.1, αλλά επιθυμεί τη λήψη δεδομένων μόνο από την πηγή 1.1.1.1. Τη δυνατότητα αυτή του τη δίνει το IGMPv3.



Εικόνα 1.11

Στη συνέχεια θα αναφερθούμε ξανά στο IGMPv3, όταν θα μιλήσουμε για Source Specific Multicasting.

1.8 Αναφορές 1ου Κεφαλαίου

1. Internetworking With TCP/IP. Douglas E. Comer
2. Cisco white paper. http://www.cisco.com/warp/public/cc/pd/iosw/tech/ipmu_ov.pdf
3. Παρουσίαση της Cisco. ftp://ftp-eng.cisco.com/ipmulticast/training/Module1.pdf
4. Παρουσίαση της Cisco. ftp://ftp-eng.cisco.com/ipmulticast/training/Module2.pdf
5. http://www.mbone.com/
6. http://www.ipmulticast.com
7. Introdaction to IP Multicast Routing. Internet draft. http://infocom.uniroma1.it/alef/rfc/draft-ietf-mboned-intro-multicast-03.txt
8. http://www.sprintlink.net/multicast/faq.html
9. http://www.merit.edu/~mbone/index/titles.html
10. http://www.cis.ohio-state.edu/~jain/cis788-97/ip_multicast/
11. http://www.iana.org/assignments/multicast-addresses
12. Introdaction to IP Multicast David Meyer Cisco Systems. http://www.nanog.org/mtg-9806/ppt/davemeyer/
13. http://www.grnet.gr/mbone/
14. http://www.nortelnetworks.com/products/02/papers/3584.html

RFCs:

15. RFC 2236: Internet Group Management Protocol, Version 2

Κεφάλαιο 2ο: Multicast tools

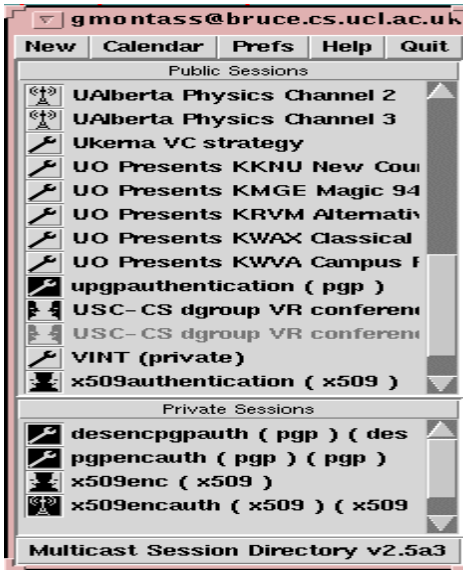
2.1 Εισαγωγή

Σε αυτή την ενότητα θα αναφέρουμε μερικά από τα εργαλεία που ένας χρήστης μπορεί να χρησιμοποιήσει προκειμένου να εκμεταλλευτεί την IP multicast τεχνολογία. Τα πιο γνωστά από αυτά είναι το *sdr,* που χρησιμεύει στην παρακολούθηση και δημιουργία των sessions -το οποίο ορίζεται στη συνέχεια-, το *rat* για την αποστολή και λήψη ήχου, το *vic* για την αποστολή και λήψη εικόνας και το wb που είναι εργαλείο συνδιάσκεψης.

Με τον όρο multimedia session ονομάζουμε κάθε multimedia εφαρμογή, την οποία παρέχει μια πηγή και στην οποία συμμετέχουν κάποιοι αποδέκτες. Η συνδιάσκεψη είναι ένα παράδειγμα ενός multimedia session. Ένα session μπορεί να είναι επίσης η εκπομπή ενός ραδιοφωνικού σταθμού (mp3 stream), ένα ντοκιμαντέρ με video και ήχο (όπως ακριβώς στην τηλεόραση), μια interactive συνδιάσκεψη, η εξ αποστάσεως εκπαίδευση κ.α.

2.2 Session Directory (SDR)

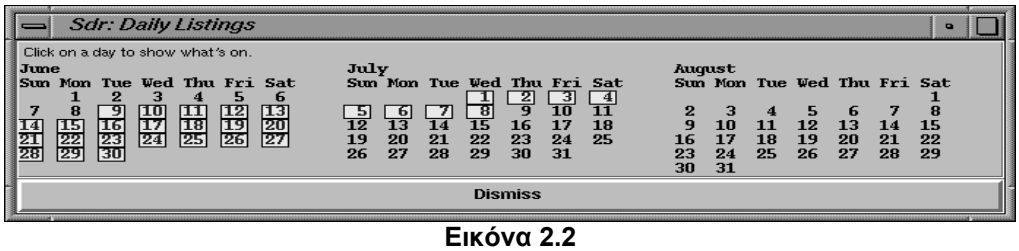
Το SDR είναι ένα εργαλείο που βοηθάει το χρήστη να συνδεθεί σε μια συνδιάσκεψη ή να δημιουργήσει μια νέα, που γίνεται με την multicast τεχνολογία. Οι συνδιασκέψεις που έχουν ανακοινωθεί από τους χρήστες τους στο SDR εμφανίζονται σε μια λίστα στο κυρίως παράθυρο με αλφαβητική σειρά (εικόνα 2.1).



Εικόνα 2.1: Το κυρίως παράθυρο του SDR

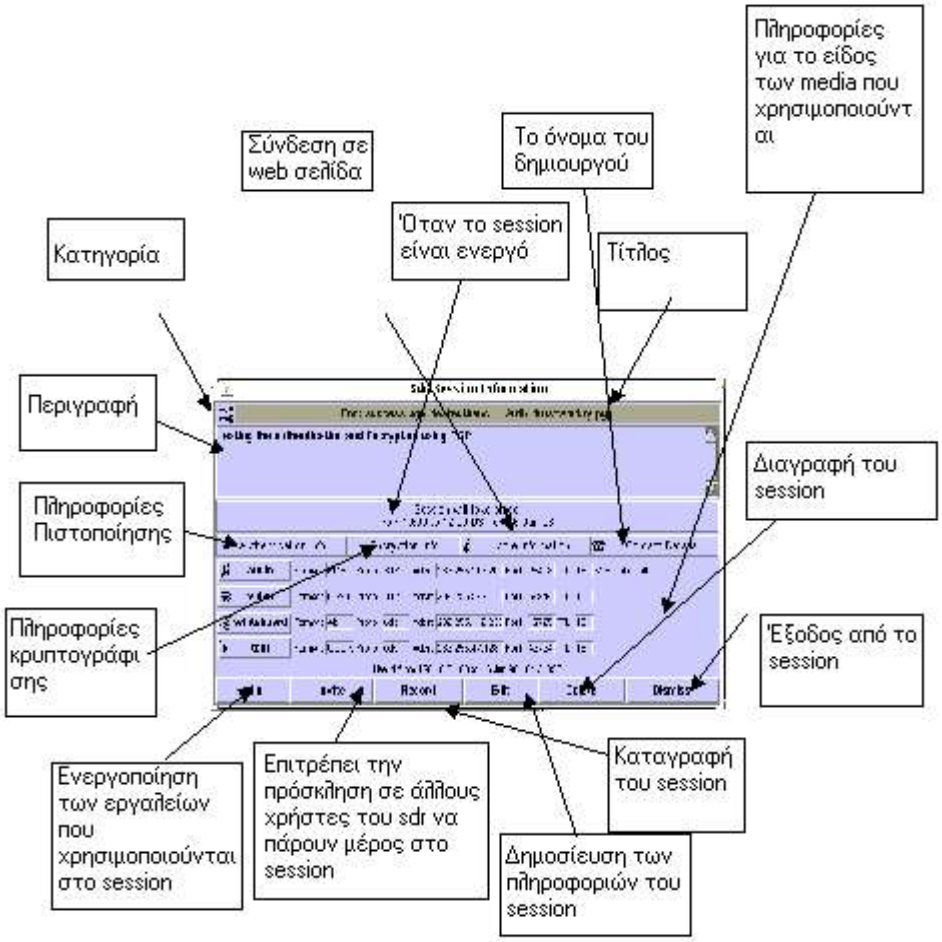
Επιλέγοντας το όνομα του session, ανοίγει ένα παράθυρο με περισσότερες πληροφορίες. Τα sessions που είναι γκρι, εκείνη την στιγμή δεν είναι ενεργά. Επιλέγοντας το εικονίδιο Daily Listing από το κυρίως παράθυρο, εμφανίζεται ένα νέο παράθυρο που παρουσιάζει όλα τα sessions σε καθημερινή βάση, με τη μορφή ενός οδηγού τηλεοπτικών προγραμμάτων. Οι ημερομηνίες που βρίσκονται σε κουτάκι είναι αυτές στις οποίες έχουν

προγραμματιστεί κάποια sessions, τα οποία εμφανίζονται επιλέγοντας πάνω σε κάθε ημερομηνία (εικόνα 2.2)



Εικόνα 2.2

Κατά την σύνδεση σε ένα session με το SDR τα αντίστοιχα εργαλεία αυτόματα ενεργοποιούνται με τις σωστές διευθύνσεις και τις σωστές παραμέτρους. Ένας τρόπος σύνδεσης σε ένα session είναι μέσω του παραθύρου Session Information επιλέγοντας το εικονίδιο join. Επίσης, ένας χρήστης μπορεί να διαλέξει να ενεργοποιήσει μερικά από τα εργαλεία του session επιλέγοντας το αντίστοιχο εικονίδιο (εικόνα 2.3).



Εικόνα 2.3

Το παράθυρο Session Information δίνει τις παρακάτω πληροφορίες για το session:

- Το εικονίδιο στην πάνω αριστερή γωνία δίνει το είδος του session: broadcast, συνδιάσκεψη και πειραματικό. Επιλέγοντας πάνω στην εικόνα, εμφανίζεται το είδος του session με λέξεις.

- Δεξιά του εικονιδίου υπάρχει το όνομα του session ακολουθούμενο από το είδος της ασφάλειας και το είδος της πιστοποίησης, αν υπάρχει αυτη, (PGP ή X.509), καθώς επίσης και το είδος της κρυπτογράφησης, αν το session είναι κρυπτογραφημένο (PGP, X.509, DES).
- Στο κουτί κάτω από το όνομα δίνεται μια περιγραφή του session.
- Το κουτί κάτω από την περιγραφή αναφέρει την χρονολογία που θα είναι ενεργό το session.
- Το εικονίδιο *Authentication Information* δίνει πληροφορίες πιστοποίησης, ενώ στην περίπτωση του PGP, δίνει το όνομα του προσώπου που δημιούργησε το session, και την ημερομηνία που δημιουργήθηκε.
- Το εικονίδιο *Encryption Information* δίνει το όνομα του χρήστη για τον οποίο η κρυπτογράφηση έγινε με επιτυχία.
- Το εικονίδιο *More Information* είναι ένα link σε μία web σελίδα και αυτό υπάρχει μόνο αν ο δημιουργός του session παρέχει το link.
- Το *Contact Details* εικονίδιο παρέχει πληροφορίες για το άτομο που δημιούργησε το session, όπως το όνομα, το τηλέφωνο και το e-mail, καθώς επίσης και την έκδοση του SDR που χρησιμοποίησε.
- Στην συνέχεια, ένα πεδίο εμφανίζει περισσότερες πληροφορίες για το μέσο επικοινωνίας που χρησιμοποιείται στο session. Υπάρχει μια γραμμή για κάθε εργαλείο (audio, video, text), όπου δίνεται η διαμόρφωση των media, το πρωτόκολλο που χρησιμοποιείται, η διεύθυνση και η πόρτα που θα χρησιμοποιήσει το session.
- Το εικονίδιο *join* ενεργοποιεί τα κατάλληλα εργαλεία και αρχίζει η συμμετοχή σε ένα session.
- Με το εικονίδιο *invite* μπορεί να προσκληθεί κάποιος χρήστης του SDR να συνδεθεί σε ένα session. Για να γίνει αυτό θα πρέπει ο δημιουργός να γνωρίζει το όνομα του χρήστη και το όνομα του υπολογιστή. Για παράδειγμα, για την πρόσκληση του χρήστη με username mkok που χρησιμοποιεί την μηχανή CW γράφουμε *mkok@CW*, το οποίο δεν έχει καμία σχέση με το e-mail του χρήστη.
- Αν έχει δημιουργηθεί ένα session αυτό μπορεί να διαγραφεί με το εικονίδιο *delete,* ενώ με το *edit* μπορούν να μετατραπούν τα στοιχεία που έχουν δοθεί στο session.

2.2.1 Δημιουργία ενός νέου session

Από το κυρίως παράθυρο του SDR επιλέγοντας το εικονίδιο *New* και στην συνέχεια *create advertise session* εμφανίζεται ένα νέο παράθυρο (εικόνα 2.4) όπου μπορεί να δημιουργηθεί μια ανακοίνωση. Σε αυτό το παράθυρο δίνεται το όνομα του session, μια περιγραφή του και ένα URL για κάποια web σελίδα.

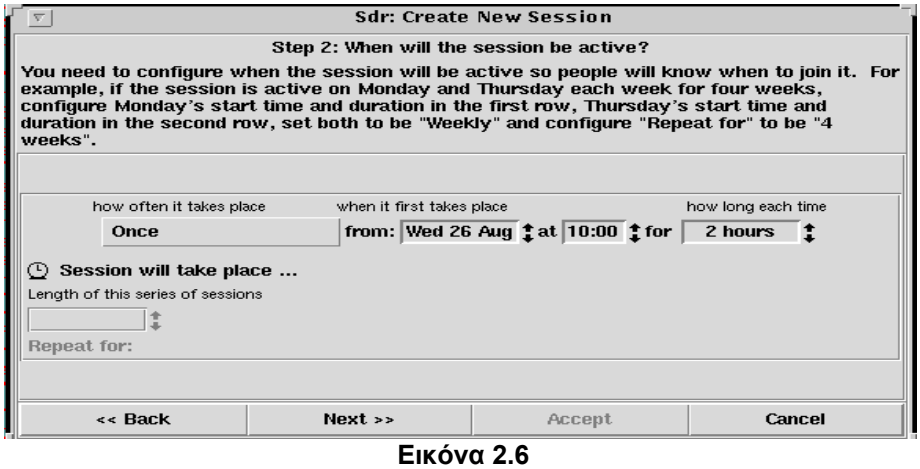
Εικόνα 2.4

Επιλέγοντας Next εμφανίζεται η εικόνα 2.5 όπου "κλικάροντας" στο Type μπορεί να επιλεχτεί το είδος του session (broadcast, meeting ή test).

Εικόνα 2.5

Στο επόμενο παράθυρο, εικόνα 2.6, επιλέγοντας το εικονίδιο *Once* εμφανίζεται μια λίστα με: *Once, Daily, Weekly, Every Two Weeks* όπου επιλέγεται το χρονικό διάστημα που θα είναι ενεργό το session. Δίπλα στο from δίνεται η χρονολογία, η ώρα που θα αρχίζει το session και για πόση ώρα θα είναι ενεργό.

Πρέπει να σημειωθεί, ότι το session θα ανακοινώνεται στο SDR όσο το SDR που το δημιούργησε τρέχει. Κλείνοντας το SDR, το session εξαφανίζεται από όλα τα SDR των χρηστών, μέχρι να ενεργοποιηθεί ξανά.



Εικόνα 2.6

Με Next εμφανίζεται η εικόνα 2.7.

Εικόνα 2.7

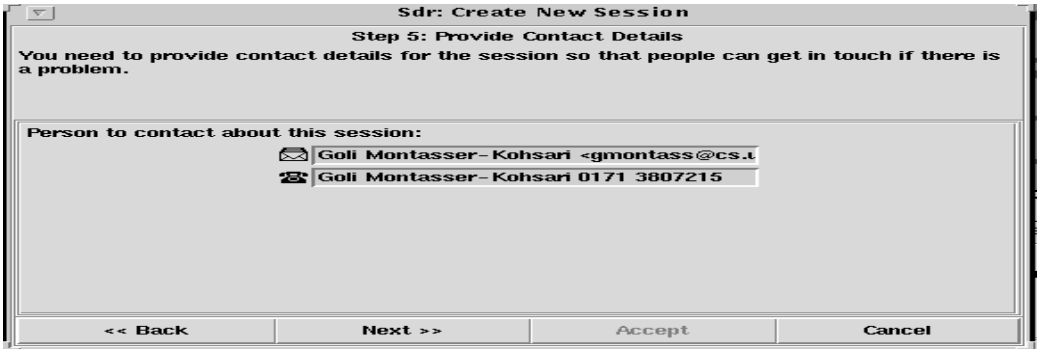
Στο πεδίο *Reached allows,* καθορίζεται πόσο μακριά θα φτάσει το session. Το *Local Scope,* επιτρέπει στο session να μεταδοθεί σε τοπικό επίπεδο π.χ μέσα σε μια πανεπιστημιούπολη. Το *Region* (ttl 63), καλύπτει περίπου μια ήπειρο και το *World* (ttl 127) όλο τον κόσμο.

Επιλέγοντας Next εμφανίζεται το παράθυρο της εικόνας 2.8.

Εικόνα 2.8

Εδώ πρέπει να επιλεχτεί το είδος του session που δημιουργείται. Τα διαθέσιμα είναι *audio, video, whiteboard και text.* Τα αντίστοιχα εργαλεία λογισμικού που απευθύνονται μπορεί να είναι το RAT, το VIC, το WB και το NTE.

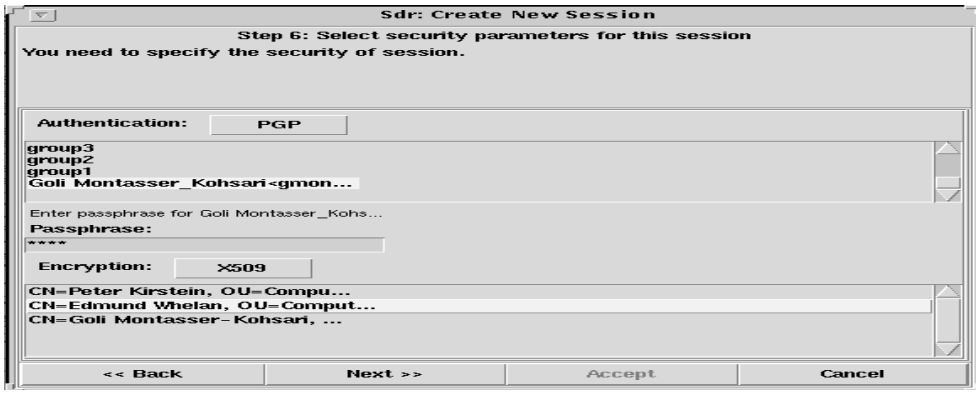
Επιλέγοντας Next εμφανίζεται η εικόνα 2.9.



Εικόνα 2.9

Στο βήμα 5 δίνονται τα στοιχεία του δημιουργού, ώστε αν κάποιος παραλήπτης έχει πιθανόν πρόβλημα να μπορεί να επικοινωνήσει μαζί του.

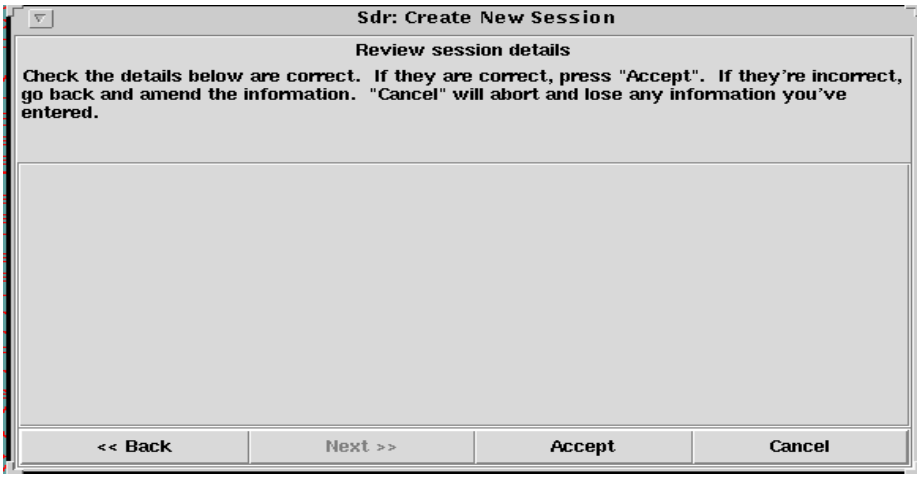
Στο επόμενο βήμα επιλέγονται παράμετροι ασφάλειας του session (εικόνα 2.10).



Εικόνα 2.10

Για την συμμετοχή σε ένα session υπάρχει δυνατότητα ο δημιουργός να φτιάξει μηχανισμό πιστοποίησης. Για πιστοποίηση υπάρχουν οι εξής επιλογές: “none”, PGP, X509, PGP+CERT, X509+CERT. Επίσης μπορεί να κρυπτογραφήσει την ανακοίνωση. Οι επιλογές που έχει είναι: “none”, PGP, DES, X509.

Στην τελευταία εικόνα, ο δημιουργός ελέγχει αν η πληροφορία που έδωσε στα προηγούμενα βήματα είναι σωστή.



Εικόνα 2.11

Επιλέγοντας *Accept*, δημιουργείται και στέλνεται η ανακοίνωση του session*.

2.3 Robust-Audio Tool (RAT)

Το RAT είναι ένα εργαλείο που επιτρέπει στους χρήστες του να συμμετέχουν σε συνδιασκέψεις ήχου στο internet. Μπορεί να χρησιμοποιηθεί είτε σε point-to-point (unicast) συνδιασκέψεις, είτε σε multicast συνδιασκέψεις όταν υπάρχουν πολλοί συμμετέχοντες σε διαφορετικές τοποθεσίες που συνδέονται με multicast δίκτυο.

* Για λεπτομέρειες για τις λειτουργίες του sdr βλ: http://www-mice.cs.ucl.ac.uk/multimedia/software/

Υπάρχουν δύο τρόποι για την ενεργοποίηση του RAT: από γραμμή εντολών και από το SDR. Με το SDR κατά την σύνδεση σε μια ομάδα όλοι οι παράμετροι ρυθμίζονται αυτόματα, ενώ από γραμμή εντολών δίνεται η εντολή

Prompt> rat [options] <address/port>

Η multicast διεύθυνση πρέπει να είναι μέσα στο πεδίο 224.2.0.0-224.2.255.255 (εκτός αν χρησιμοποιείται admin scope). Το νούμερο της πόρτας πρέπει να είναι μεγαλύτερο από 1024. Το RAT χρησιμοποιεί την πόρτα που του καθορίζει ο χρήστης και την αμέσως επόμενη.

Για παράδειγμα η παρακάτω εντολή θα ενεργοποιήσει το RAT με TTL 127, για την multicast διεύθυνση 224.2.3.50 και αριθμό πόρτας 5224.

Prompt>rat –t 127 224.2.3.50/5224

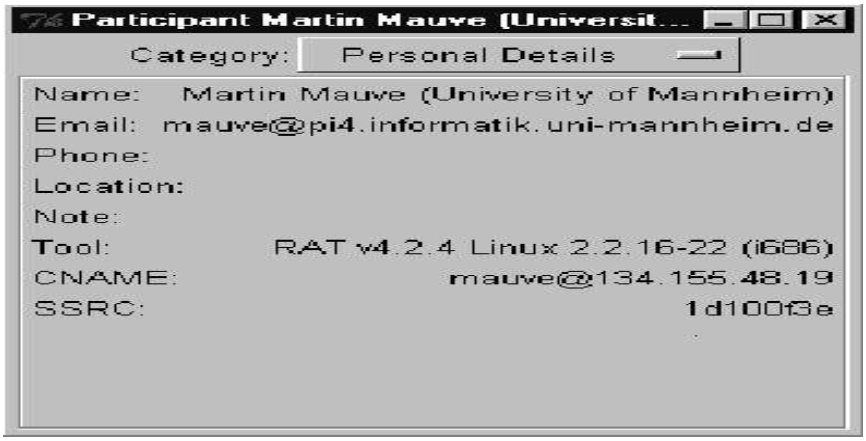
Το RAT αποτελείται από το κυρίως παράθυρο (main window), από το παράθυρο preferences και από μερικά παράθυρα που δίνουν πληροφορίες στο χρήστη. Παρακάτω θα δώσουμε μια περιγραφή τους.

2.3.1 Το Κυρίως Παράθυρο του RAT

Το κυρίως παράθυρο του RAT (εικόνα 2.12) χωρίζεται σε τρία μέρη. Στη μέση υπάρχει μια λίστα με τους συμμετέχοντες στο session. Το όνομα του χρήστη εμφανίζεται πάντα στην κορυφή της λίστας. Όταν κάποιος μιλάει εκείνη την στιγμή το όνομά του φωτίζεται.

Εικόνα 2.12:Το Κυρίως Παράθυρο του RAT

Κλικάροντας σε ένα από τα ονόματα, εμφανίζεται ένα παράθυρο επιλογών, με προεπιλεγμένη την κατηγορία Personal Details (εικόνα 2.13). Σε αυτό το παράθυρο μπορούν να εμφανιστούν άλλες τεχνικές λεπτομέρειες κάνοντας επιλογή μιας άλλης κατηγορίας από το μενού Category. Αυτές είναι: i) Playout, ii) Decoder, iii) Audio και iv) 3D Positions.



Εικόνα 2.13

Το πάνω μέρος του κυρίου παραθύρου χωρίζεται σε δύο μέρη, την είσοδο αριστερά και την έξοδο δεξιά. Επιλέγοντας τα κουτιά με την ονομασία Listen και Talk ενεργοποιούνται οι συσκευές που φαίνονται κάτω από αυτά. Εξ ορισμού, το Speaker είναι η συσκευή εισόδου και το Microphone η συσκευή εξόδου. Ανάλογα με το διαθέσιμο hardware, είσοδος μπορεί να είναι το Line in και το CD, ενώ έξοδος το Line out και το Headset. Πατώντας το τριγωνικό εικονίδιο από κάθε πλευρά, δίνεται η δυνατότητα επιλογής μεταξύ των παραπάνω εισόδων και εξόδων.

Κάτω από τις συσκευές εισόδου και εξόδου υπάρχει ένας δρομέας που μπορεί να μεταβάλλει την ένταση του ήχου από 0 έως 100. Η δυνατότητα αυτή είναι ιδιαίτερα χρήσιμη, γιατί σε μια συνδιάσκεψη επιτρέπει σε όλους τους χρήστες να προσαρμόζουν την ένταση του ήχου σε ένα ορισμένο και ίδιο για όλους επίπεδο.

Στο κάτω μέρος του παραθύρου εμφανίζεται το όνομα του session, η IP διεύθυνση της συνδιάσκεψης και το νούμερο της πόρτας, το TTL και πέντε εικονίδια ελέγχου. Από αριστερά στα δεξιά, αυτά τα εικονίδια έχουν τις εξής λειτουργίες:

1. Έλεγχος αρχείου, όταν παίζει από ή αντιγράφει σε αρχείο.
2. Εμφάνιση κειμένου βοήθειας.
3. Το εικονίδιο options εμφανίζει διάφορες επιλογές που μπορούν να δοθούν.
4. Το About δείχνει την καταχώρηση πνευματικής ιδιοκτησίας.
5. Το Quit κλείνει το RAT και το session.

2.3.2 Το Παράθυρο Options

Κάνοντας κλικ στο εικονίδιο options από το κυρίως παράθυρο του RAT εμφανίζεται ένα παράθυρο επιλογών που επιτρέπει την διαμόρφωση των λειτουργιών του RAT. Υπάρχουν διάφορες κατηγορίες επιλογών που μπορούν να διαμορφωθούν και εμφανίζονται από το μενού Category. Οι επιλογές αυτές μπορούν να αποθηκευτούν προσωρινά για το συγκεκριμένο session επιλέγοντας Apply Preferences ή να αποθηκευτούν για μελλοντικά sessions επιλέγοντας Save & Apply Preferences. Με το Cancel ακυρώνονται όλες οι αλλαγές που έχουν γίνει. Στην συνέχεια παραθέτονται μερικές επιλογές, στις οποίες συνήθως χρειάζεται να γίνεται αλλαγή.

1. Ο λόγος για τον οποίο ο ήχος κόβεται, δημιουργώντας έτσι πρόβλημα στους χρήστες, είναι η απώλεια πακέτων. Στην περίπτωση αυτή αυξάνουμε την ένταση του μικροφώνου και αν το πρόβλημα παραμένει, τότε κλείνουμε το Suppress Silence, ενώ κλείνουμε τον ήχο με mute όταν δεν μιλάμε, γιατί διαφορετικά θα μεταφέρεται ο θόρυβος του δωματίου.
2. Στην περίπτωση που η χρήση του εργαλείου γίνεται για λόγους αποκλειστικά ακουστικούς, για παράδειγμα αν θέλουμε να ακούσουμε μια διάλεξη, θα πρέπει να ενεργοποιούμε το Lecture Mode. Τότε το RAT καθυστερεί την έξοδο του ήχου για λίγο, αφήνοντας περισσότερο χρόνο στα πακέτα να φτάσουν. Το Lecture Mode απενεργοποιείται μόνο του, όταν αρχίζει η ομιλία.
3. Επιλέγοντας το εικονίδιο Name μπορεί να γίνει αλλαγή του ονόματος σε σχέση με αυτό που εμφανίζεται στο κυρίως παράθυρο. Επίσης μπορεί να γίνει αλλαγή του e-mail, του αριθμού του τηλεφώνου και της τοποθεσίας.[1]

2.4 VIC

Το VIC είναι ένα unicast και multicast εργαλείο βίντεο συνδιάσκεψης. Μπορεί να χρησιμοποιηθεί είτε για point-to-point βίντεο συνδιάσκεψη, δηλαδή κατευθείαν σύνδεση μεταξύ δύο μηχανών, είτε μεταξύ πολλών συμμετεχόντων, με τη βοήθεια του multicast.

Υπάρχουν δύο τρόποι για να ενεργοποιηθεί το VIC: από γραμμή εντολών και από το SDR. Από το SDR, για την σύνδεση σε μια συνδιάσκεψη το VIC ενεργοποιείται αυτόματα και έτσι όλες οι ρυθμίσεις γίνονται από το πρόγραμμα και όχι από το χρήστη. Όπως το RAT έτσι και το VIC μπορεί να ενεργοποιηθεί από γραμμή εντολών με τον παρακάτω τρόπο:

Prompt> vic [options] <address/port>

Η multicast διεύθυνση πρέπει να είναι μέσα στο πεδίο 224.2.0.0 – 224.2.255.255 (εκτός όταν χρησιμοποιείται admin scope). Το νούμερο της πόρτας πρέπει να είναι μεγαλύτερο από 5002.

Για παράδειγμα η παρακάτω εντολή θα ενεργοποιήσει το VIC με TTL 127, για την multicast διεύθυνση 224.2.3.50 και αριθμό πόρτας 5224.

Prompt>vic –t 127 224.2.3.50/5224

Το VIC αποτελείται από το κυρίως παράθυρο, το παράθυρο Menu και άλλα μικρότερα παράθυρα.

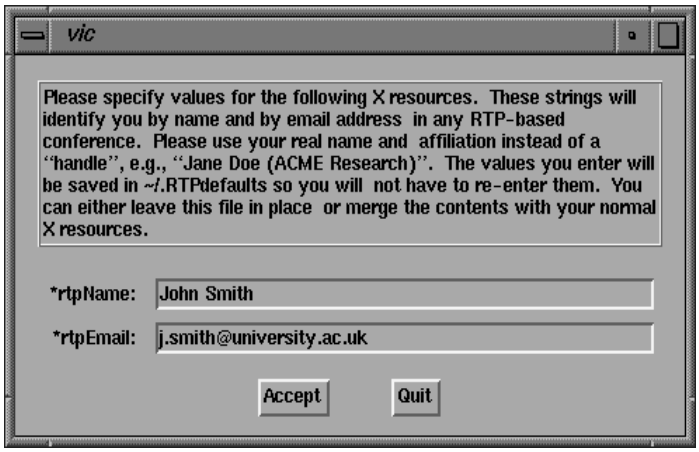
2.4.1 Το κυρίως παράθυρο του VIC

Στην εικόνα 2.13 φαίνεται το κυρίως παράθυρο του VIC.

[1] Για περισσότερες πληροφορίες: http://www-mice.cs.ucl.ac.uk/multimedia/software/rat/

Εικόνα 2.13 Το κυρίως παράθυρο του VIC

Την πρώτη φορά που ενεργοποιείται το VIC εμφανίζεται το παράθυρο της εικόνας 2.14, όπου πρέπει να δοθεί το όνομα του συμμετέχοντα και το e-mail. Αυτά αποθηκεύονται σε ένα αρχείο που λέγεται RTPdefaults. Το αρχείο αποθηκεύεται στον κατάλογο home του χρήστη. Αν ο χρήστης αυτός μεταδίδει βίντεο το όνομά του εμφανίζεται δίπλα στην εικόνα του στο κυρίως παράθυρο του VIC.



Εικόνα 2.14

Όταν ενεργοποιείται το VIC, στο κυρίως παράθυρο αυτόματα εμφανίζονται μικρά εικονίδια των videos που μεταδίδονται εκείνη την στιγμή από τους άλλους συμμετέχοντες. Πατώντας τα εικονίδια ανοίγει ένα κανονικό παράθυρο-video όπως δείχνει η εικόνα 2.15. Αυτό, μπορεί να αλλάξει μέγεθος από το εικονίδιο Size στο κάτω μέρος του παραθύρου. Υπάρχουν τρεις διαφορετικές κωδικοποιήσεις, CIF, NTSC και PAL. Το εικονίδιο Modes παρέχει τέσσερα διαφορετικά modes, που είναι α) το voice-switched που δείχνει την εικόνα εκείνου που μιλάει κάθε φορά, β) το timer-switched που αλλάζει την εικόνα μεταξύ όλων των συμμετεχόντων στη σειρά, με κάθε εικόνα να εμφανίζεται για 5 δευτερόλεπτα, γ) το Save-CPU και δ) το Use-Hardware, που χρησιμοποιεί έναν προσαρμογέα γραφικών για να αποκωδικοποιήσει την εικόνα. Με το Dismiss κλείνει το παράθυρο.

Εικόνα 2.15

Όταν καμιά πηγή δεν μεταδίδει στη διεύθυνση και στην πόρτα που το VIC ενεργοποιήθηκε, τότε το κεντρικό παράθυρο εμφανίζει το μήνυμα “Waiting for video…” (εικόνα 2.16).
8

Εικόνα 2.16

Επίσης, στο κεντρικό παράθυρο δίπλα στα videos υπάρχει κείμενο που αναφέρει το όνομα του συμμετέχοντα, την IP διεύθυνση της μηχανής και πληροφορίες για τη διαμόρφωση του βίντεο που ο συμμετέχοντας μεταδίδει. Το όνομα εμφανίζεται λιγότερο γκρι όταν κανένα μήνυμα δεν έχει ληφθεί για μερικά δευτερόλεπτα (κάθε VIC στέλνει περιοδικά session μηνύματα). Ακόμα, εμφανίζονται πληροφορίες για τη ροή του βίντεο που λαμβάνεται από το συγκεκριμένο συμμετέχοντα, πληροφορίες που αναφέρουν την ποσότητα των frames και των kilobits που λαμβάνονται το δευτερόλεπτο. Ο αριθμός στις παρενθέσεις δίνει το ποσοστό των χαμένων πακέτων.

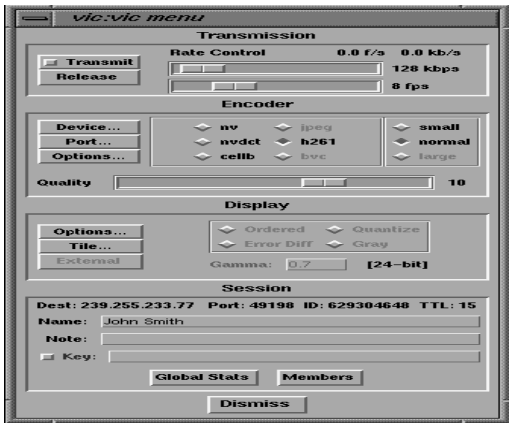
Επιλέγοντας το εικονίδιο mute, το VIC κάνει παύση στο βίντεο και η εικόνα εμφανίζεται παγωμένη στην οθόνη. Η πηγή μπορεί να κάνει mute την εικόνα που μεταδίδει όμως ο παραλήπτης δεν βλέπει παγωμένη εικόνα. Συνιστάται να γίνονται mute οι εικόνες για τις οποίες δεν ενδιαφερόμαστε, προκειμένου να ελαχιστοποιείται ο φόρτος στη μηχανή.

Το εικονίδιο color ελέγχει τις ρυθμίσεις των χρωμάτων για το εισερχόμενο βίντεο. Εξ ορισμού, το βίντεο εμφανίζεται με χρώμα αλλά μπορεί επίσης να εμφανιστεί και ασπρόμαυρο.

Επιλέγοντας το εικονίδιο info εμφανίζεται ένα μενού που περιέχει τα παρακάτω: Site info, RTP Stats, Decoder Stats, Mtrace from, Mtrace to.

2.4.2 Το παράθυρο menu του VIC

Επιλέγοντας το εικονίδιο Menu από το κυρίως παράθυρο του VIC εμφανίζεται ένα μενού το οποίο επιτρέπει στο χρήστη να αλλάξει τις ρυθμίσεις για τη μεταφορά του δικού του βίντεο (εικόνα 2.17).



Εικόνα 2.17: Το παράθυρο menu του vic

Οι ρυθμίσεις που συνήθως χρησιμοποιούνται είναι:

i) Τα εικονίδια Transmit και Release. Επιλέγοντας transmit αρχίζει η μετάδοση, ενώ για να σταματήσει η μετάδοση επιλέγουμε release ή transmit ξανά.

ii) Δίνεται η δυνατότητα αλλαγής του ονόματος που εμφανίζεται δίπλα στα μικρά video εικονίδια γράφοντας στο πεδίο Name.

iii) Ο χρήστης μπορεί να δει μια λίστα από όλους τους συμμετέχοντες που τρέχουν VIC σε μια διεύθυνση και πόρτα, επιλέγοντας το εικονίδιο Members.

iv) Μπορεί να καθοριστεί το μέγιστο bandwidth (kbits/s) που θέλει ο χρήστης να χρησιμοποιήσει και ο μέγιστος αριθμός των frames ανά δευτερόλεπτο αλλάζοντας το δρομέα δεξιά στα εικονίδια transmit και release[1].

2.5 WhiteBoard

Το WhiteBoard είναι ένα unicast και multicast εργαλείο συνεργασίας και παρέχει ένα χώρο εργασίας τον οποίο μπορούν να μοιραστούν όλοι οι συμμετέχοντες. Μπορεί να χρησιμοποιηθεί είτε για point-to-point συνδιάσκεψη, δηλαδή κατευθείαν σύνδεση μεταξύ δύο μηχανών, είτε μεταξύ πολλών συμμετεχόντων, με την βοήθεια του multicast. Το WB είναι μόνο διαθέσιμο για UNIX. Οι χρήστες των Windows μπορούν να χρησιμοποιήσουν το WBD. Το WB είναι κυρίως ένα εργαλείο συνδιάσκεψης- όχι εργαλείο ζωγραφικής. Μπορούμε να το φανταστούμε σαν ένα εργαλείο ζωγραφικής με μικρές δυνατότητες.

Και εδώ υπάρχουν δύο τρόποι για να ενεργοποιηθεί το WB: από γραμμή εντολών και από το SDR. Από το SDR, για την σύνδεση σε μια συνδιάσκεψη ενεργοποιείται αυτόματα, οπότε και όλες οι ρυθμίσεις γίνονται από το πρόγραμμα και όχι από τον χρήστη. Όπως το RAT και το VIC έτσι και

[1]Για περισσότερες πληροφορίες:http://www-mice.cs.ucl.ac.uk/multimedia/software/

το WB μπορεί να ενεργοποιηθεί από γραμμή εντολών με τον παρακάτω τρόπο:

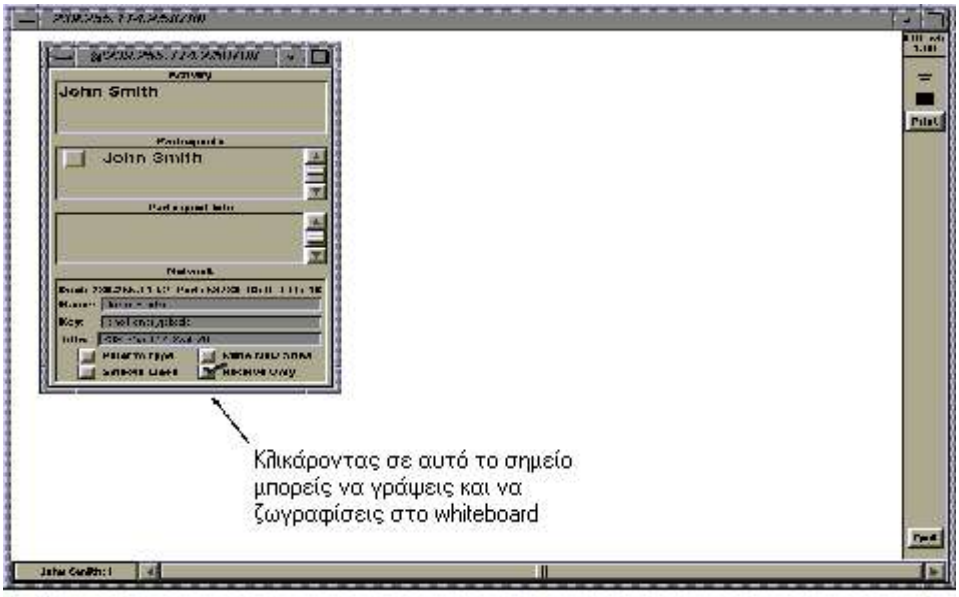
Prompt> wb [options] <address/port>

Η multicast διεύθυνση πρέπει να είναι μέσα στο πεδίο 224.2.0.0 – 224.2.255.255 (εκτός όταν χρησιμοποιείται admin scope). Ο αριθμός της πόρτας πρέπει να είναι μεγαλύτερος από 5002. Για παράδειγμα η παρακάτω εντολή θα ενεργοποιήσει το WB με TTL 48 στην multicast διεύθυνση 224.2.4.70 και αριθμό πόρτας 5004.

Prompt> wb –t 48 224.2.4.70/5004

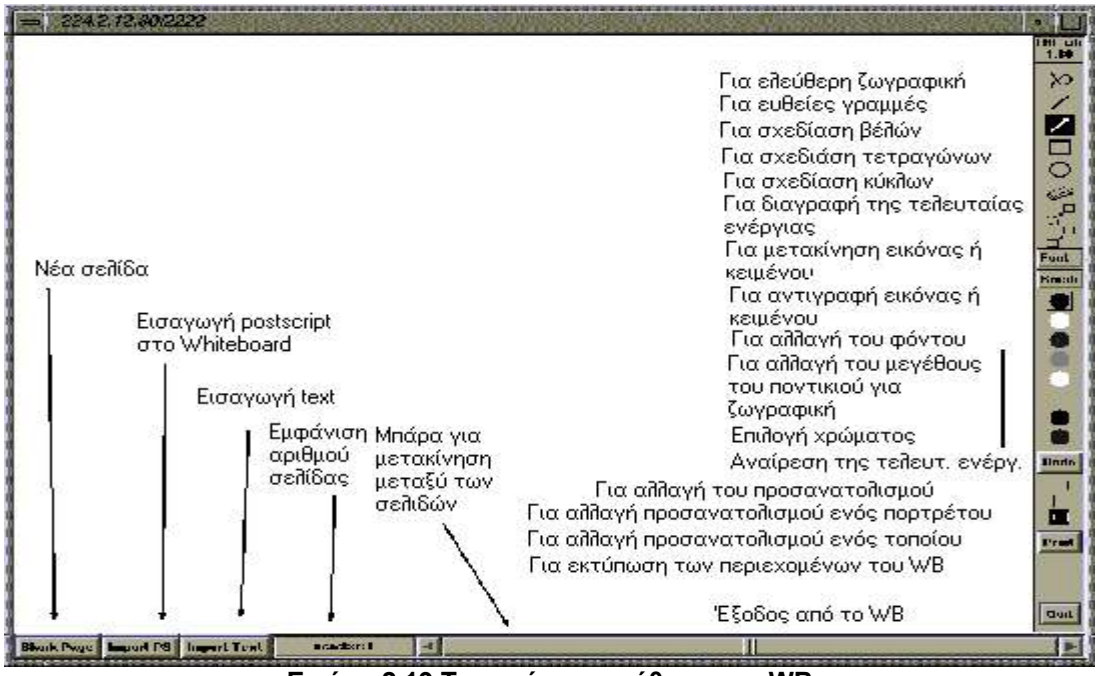
Στο παραπάνω παράδειγμα ο χρήστης χρησιμοποίησε την παράμετρο "-t" για να καθορίσει το TTL. Το TTL καθορίζει πόσο μακριά θα φτάσουν τα πακέτα. 48 TTL είναι αρκετό ώστε τα πακέτα να καλύψουν μια μεγάλη χώρα. Όλοι οι συμμετέχοντες πρέπει να χρησιμοποιούν την ίδια multicast διεύθυνση και πόρτα για να υπάρξει επικοινωνία.

Το WB αποτελείται από δύο παράθυρα, το κύριο και το παράθυρο ελέγχου. Αυτά εμφανίζονται στην οθόνη όταν ενεργοποιείται το WB (εικόνα 2.18).



Εικόνα 2.18

Τα κείμενα για δημοσίευση που δημιουργούνται από τους άλλους συμμετέχοντες εμφανίζονται στο κυρίως παράθυρο. Εξ ορισμού όταν ενεργοποιείται το WB μπορεί να λαμβάνει μόνο. Για να μπορέσει ο χρήστης να γράψει και να ζωγραφίσει, θα πρέπει να μην έχει γίνει επιλογή του εικονιδίου Receive only που βρίσκεται στην κάτω αριστερή γωνία του Control Panel (εικόνα 2.18). Σε μια τέτοια περίπτωση εμφανίζονται πολλά εικονίδια ελέγχου στο δεξιό μέρος του WB, δίνοντας την δυνατότητα στο χρήστη να γράψει και να ζωγραφίσει (εικόνα 2.19).



Εικόνα 2.19 Το κυρίως παράθυρο του WB

Με τα εικονίδια στα δεξιά της οθόνης μπορούν να γίνουν οι παρακάτω ενέργειες:

1. Να ζωγραφιστούν διάφορα σχήματα – γραμμές, τόξα, κύκλοι και τετράγωνα.
2. Να διαγραφούν οι τελευταίες ενέργειες.
3. Να διαγραφούν και να αντιγραφούν κείμενα και ζωγραφιές.
4. Να γίνει αλλαγή στο φόντο.
5. Να ρυθμιστεί το πάχος γραμμής στη ζωγραφική.
6. Να γίνει ρύθμιση του χρώματος που χρησιμοποιείται για ζωγραφική και γράψιμο.
7. Να γίνει αναίρεση της τελευταίας διαγραφής.

Με τα εικονίδια στο κάτω μέρος της οθόνης μπορούν να γίνουν οι παρακάτω ενέργειες:

1. Να ανοιχτεί καινούργια σελίδα.
2. Να εισαχθεί ένα PostScript και ένα text αρχείο.
3. Να κλειδωθεί μια σελίδα.
4. Να γίνει αναζήτηση μεταξύ των σελίδων αν είναι περισσότερες από μία σε ένα έγγραφο[1].

[1]Για περισσότερες πληροφορίες:http://www-mice.cs.ucl.ac.uk/multimedia/software/

2.6 Πηγές 2ου Κεφαλαίου

1. UCL Network and Multimedia Research Group. http://www-mice.cs.ucl.ac.uk/multimedia/software/
2. §http://imj.ucsb.edu/sdr-monitor/because.html

Κεφάλαιο 3ο:Τεχνικές Προώθησης Πακέτων και Δέντρα Διανομής

3.1 Εισαγωγή

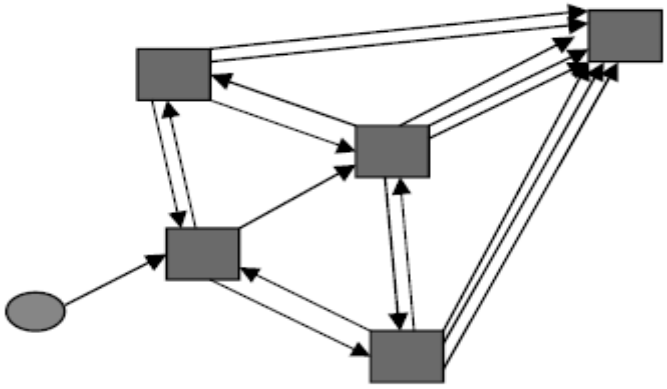
Στο 1ο κεφάλαιο αναφέραμε μερικές βασικές έννοιες του IP multicasting, τις διευθύνσεις που αυτό χρησιμοποιεί και τέλος γνωρίσαμε πώς ένας υπολογιστής επικοινωνεί με ένα δρομολογητή στα άκρα ενός δικτύου με την βοήθεια του IGMP. Σε αυτό το κεφάλαιο θα αναλύσουμε τις τεχνικές που χρησιμοποιούν οι multicast δρομολογητές για να προωθήσουν την κίνηση, καθώς επίσης και τους τύπους των δέντρων διανομής που δημιουργούν, από την πηγή προς τους αποδέκτες. Ο σχηματισμός των δέντρων γίνεται από τα multicast πρωτόκολλα δρομολόγησης που θα σχολιαστούν στο επόμενο κεφάλαιο. Για την προώθηση των multicast πακέτων, οι δρομολογητές πρέπει να ξέρουν την διεύθυνση της πηγής, σε αντίθεση με τα unicast όπου πρέπει να γνωρίζουν την διεύθυνση προορισμού. Ο προορισμός στο multicast είναι ένα group από άγνωστους αποδέκτες.

3.2 Τεχνικές Προώθησης Πακέτων

Τα multicast πρωτόκολλα δρομολόγησης χρησιμοποιούν δύο τεχνικές για την προώθηση των πακέτων: την Flooding και την Reverse Path Forwarding.

3.2.1 Flooding

Στην τεχνική Flooding ο δρομολογητής δεν απαιτείται να έχει καμιά πληροφορία δρομολόγησης. Ένα πακέτο που φτάνει σε ένα interface προωθείται σε όλα τα υπόλοιπα interfaces εκτός αυτού από το οποίο ήρθε. Η τελευταία ενέργεια μπορεί να οδηγήσει σε routing loops (εικόνα 3.1). Για να περιοριστεί το πρόβλημα των routing loops, ορίζεται ένας αριθμός σε hops τον οποίο όταν υπερβεί το πακέτο, αυτό απορρίπτεται.



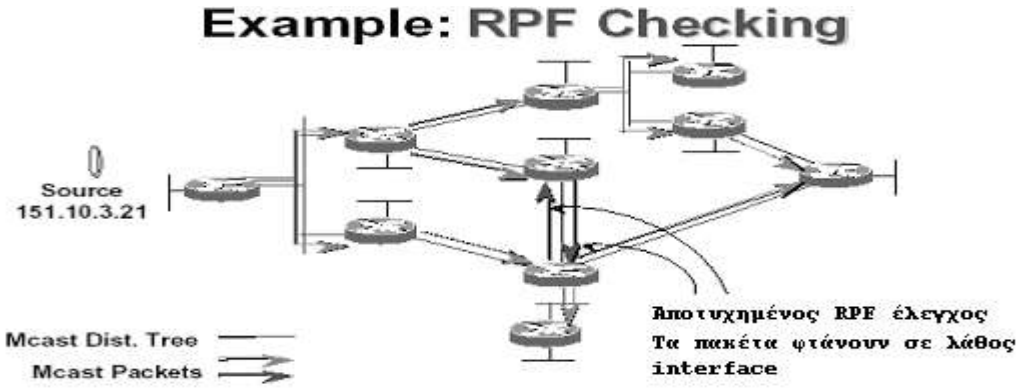
Εικόνα 3.1: Routing Loops

Η τεχνική flooding έχει τα εξής πλεονεκτήματα: i) είναι εύκολη στη διαχείριση και ii) οι δρομολογητές δεν απαιτείται να έχουν πίνακες δρομολόγησης. Μειονεκτήματα του flooding αποτελούν: i) το γεγονός ότι

αρκετές φορές δημιουργούνται routing loops και επομένως ii) η συμφόρηση που δημιουργείται στο δίκτυο είναι μεγάλη.

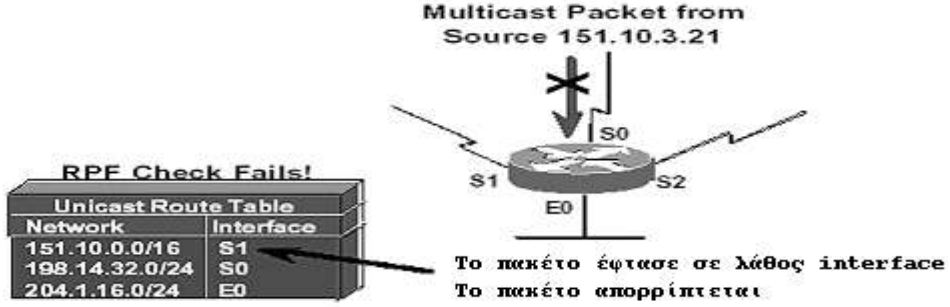
3.2.2 Reverse Path Forwarding (RPF)

Το Reverse Path Forwarding (RPF) είναι μια δεύτερη τεχνική που χρησιμοποιούν οι δρομολογητές για να προωθήσουν multicast πακέτα. Με αυτή την τεχνική, όταν ένα πακέτο φτάσει σε ένα από τα interfaces κάποιου δρομολογητή, εκείνος πραγματοποιεί ένα RPF έλεγχο για να διαπιστώσει αν το πακέτο έφτασε στο σωστό interface. Κατά τον έλεγχο αυτό εξετάζεται αν ο δρομολογητής θα χρησιμοποιούσε το interface για να προωθήσει unicast πληροφορία στην πηγή, δηλαδή αν θα επέλεγε τον ακριβώς αντίθετο δρόμο (Reverse Path). Αν ο έλεγχος γίνει με επιτυχία, δηλαδή η παραπάνω υπόθεση ελεγχθεί ότι ισχύει, το πακέτο στέλνεται από όλα τα εξερχόμενα interfaces, αλλά όχι και από το RPF interface, δηλαδή από αυτό στο οποίο έφτασε το πακέτο. Αν ο έλεγχος δεν είναι επιτυχής, το πακέτο απορρίπτεται.



Εικόνα 3.2: Παράδειγμα RPF ελέγχου

Η εικόνα 3.2 δείχνει ένα χαρακτηριστικό παράδειγμα του RPF, το οποίο έχει ως εξής: Η πηγή προωθεί στο δίκτυο multicast δεδομένα. Κάθε δρομολογητής του σχήματος, βάσει του πίνακα δρομολόγησής του, έχει ένα interface (RPF) το οποίο είναι το σωστό για να δεχτεί τα πακέτα από τη συγκεκριμένη πηγή. Οι δρομολογητές λαμβάνουν τα multicast πακέτα σε ένα ή περισσότερα interfaces, όμως με την εκτέλεση RPF ελέγχου αποτρέπονται τα routing loops. Στο παράδειγμα μας, ένας από τους δρομολογητές μετά από RPF έλεγχο απέρριψε την προώθηση πακέτων που έφταναν σε διαφορετικό από το RPF interface.



Εικόνα 3.3

Στην εικόνα 3.3 βλέπουμε με μια πιο κοντινή ματιά πώς γίνεται ο RPF έλεγχος. Ο δρομολογητής μπορεί να δεχτεί τα multicast δεδομένα που έρχονται από την πηγή 151.10.3.21 μόνο από το interface S1, γιατί ο unicast πίνακας δρομολόγησής του για το δίκτυο 151.10.0.0/16 έχει ως εξερχόμενο interface το S1. Τα δεδομένα που φτάνουν στο interface S0 απορρίπτονται.

Εικόνα 3.4

Αντίθετα η εικόνα 3.4 δείχνει έναν επιτυχημένο RPF έλεγχο, οπότε τα δεδομένα προωθούνται από τα εξερχόμενα interface S0 και E0.

3.3 Multicast Αλγόριθμος δρομολόγησης

Σε αυτή την παράγραφο θα αναφερθούμε στο γενικό αλγόριθμο δρομολόγησης που υλοποιείται από το IP για να προωθήσει τα multicast πακέτα. Στην συνέχεια παραθέτουμε τα βήματα του αλγόριθμου, από τα οποία τα πρώτα τέσσερα είναι γενικά, δηλαδή απευθύνονται για unicast, multicast και broadcast δρομολόγηση, ενώ τα επόμενα μόνο για multicast δρομολόγηση.

1. Ο δρομολογητής λαμβάνει το IP πακέτο από το επίπεδο σύνδεσης.
2. Ο δρομολογητής ελέγχει την επικεφαλίδα του IP πακέτου.
3. Ο δρομολογητής πραγματοποιεί τις διεργασίες για κάθε επιλογή (option) της επικεφαλίδας του IP.
4. Ο δρομολογητής εξετάζει την IP διεύθυνση προορισμού του IP πακέτου για να αποφασίσει ποιες θα είναι οι περαιτέρω ενέργειες του. Υπάρχουν τρεις περιπτώσεις που μπορούν να συμβούν:
   - Ο δρομολογητής να είναι ο προορισμός του πακέτου, οπότε αυτό μπαίνει στην ουρά για τοπική προώθηση και επίσης αν χρειάζεται επανασυνθέτεται.
   - Ο δρομολογητής να μην είναι προορισμός του πακέτου, οπότε αυτό μπαίνει στην ουρά για προώθηση.
   - Ο δρομολογητής να πρέπει να προωθήσει το πακέτο, αλλά ταυτόχρονα να προωθήσει και ένα αντίγραφό του στο τοπικό δίκτυο.

Στην συνέχεια αναφέρουμε τον αλγόριθμό δρομολόγησης στην περίπτωση που ο προορισμός είναι IP multicast. Υπενθυμίζουμε ότι οι κύριες διαφορές μεταξύ της προώθησης IP unicast και IP multicast πακέτων είναι:

- Τα IP multicast πακέτα συνήθως προωθούνται με βάση την IP διεύθυνση της πηγής και την IP διεύθυνση προορισμού.

- Τα IP multicast πακέτα προωθούνται σαν 2ου επιπέδου multicast πακέτα.
- Οι δρομολογητές δεν στέλνουν ICMP μηνύματα λάθους σαν απάντηση για τα IP multicast πακέτα.

Τα βήματα του IP multicast αλγόριθμου δρομολόγησης είναι:

5. Ο δρομολογητής βασίζεται στην IP διεύθυνση της πηγής και του προορισμού που βρίσκει στην επικεφαλίδα του πακέτου, για να ανακαλύψει αν το πακέτο έφτασε στο κατάλληλο για προώθηση interface. Η μέθοδος προσδιορισμού του κατάλληλου εισερχόμενου interface εξαρτάται από τον multicast αλγόριθμο δρομολόγησης που χρησιμοποιείται. Σε ένα από τους ποιο απλούς αλγόριθμους, τον Reverse Path Forwarding (RPF), το σωστό interface είναι αυτό που ο δρομολογητής θα χρησιμοποιούσε για να προωθήσει unicast πίσω στην πηγή του πακέτου.
6. Ο δρομολογητής βασίζεται στην IP διεύθυνση της πηγής και του προορισμού που βρίσκει στην επικεφαλίδα του πακέτου, για να ανακαλύψει τα εξερχόμενα interface του πακέτου αυτού. Για την αποφυγή των multicast routing loops, καθορίζεται μια TTL τιμή για κάθε εξερχόμενο interface. Ένα αντίγραφο του multicast πακέτου προωθείται από κάθε εξερχόμενο interface του οποίου η ελάχιστη τιμή στο TTL είναι μικρότερη ή ίδια με την τιμή του TTL που αναγράφεται στην επικεφαλίδα του πακέτου.
7. Ο δρομολογητής ελαττώνει την τιμή του TTL στο πακέτο κατά 1.
8. Ο δρομολογητής πραγματοποιεί κάθε IP επιλογή (option) που δεν μπορεί να υλοποιηθεί στο βήμα 3.
9. Ο δρομολογητής πραγματοποιεί κάθε αναγκαίο IP κατακερματισμό (IP fragmentation).
10. Ο δρομολογητής καθορίζει την επιπέδου σύνδεσης διεύθυνση που θα χρησιμοποιήσει για την ενθυλάκωση. Ο μηχανισμός για να γίνει το παραπάνω είναι ο Link Layer-dependent. Στα LANs, μέσα από ένα αλγόριθμο, μετατρέπονται οι IP multicast διευθύνσεις των πακέτων σε multicast διευθύνσεις επιπέδου σύνδεσης.
11. Ο δρομολογητής ενθυλακώνει το πακέτο στο αντίστοιχο, δευτέρου επιπέδου πλαίσιο (frame) και το τοποθετεί στην ουρά για έξοδο από το κατάλληλο interface.

3.4 Multicast Routing Πίνακας Δρομολόγησης

Κάθε δρομολογητής που συμμετέχει σε μια multicast επικοινωνία κατασκευάζει ένα πίνακα δρομολόγησης, δημιουργώντας (S:source, G:group) καταχωρίσεις για τα Source Path Trees και (“*”:star, G:group) καταχωρήσεις για τα Rendevous Point Trees (shared). Το star (*) αναφέρεται σε όλες τις πηγές από τις οποίες ο δρομολογητής δέχεται πακέτα, το “S” αναφέρεται σε μία πηγή και το “G” στην multicast ομάδα. Για την δημιουργία της (S,G) καταχώρισης χρησιμοποιείται ο κοντινότερος δρόμος για τα μέλη της ομάδας, τον οποίο εντοπίζει ο δρομολογητής από το δικό του unicast routing table (RPF).

Στην συνέχεια παραθέτουμε τρία πεδίο ενός multicast πίνακα δρομολόγησης.

(, 224.2.232.59), 00:02:28/00:02:59, RP 143.233.254.29, flags: SP*
Incoming interface: Ethernet0, RPF nbr 143.233.120.60
Outgoing interface list: Null

(128.223.230.9/32, 224.2.232.59), 00:02:28/00:00:31, flags: PT
Incoming interface: Ethernet0, RPF nbr 143.233.120.60
Outgoing interface list: Null

(, 224.2.127.254), 4w5d/00:02:59, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.28.6
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:20:35/00:02:53

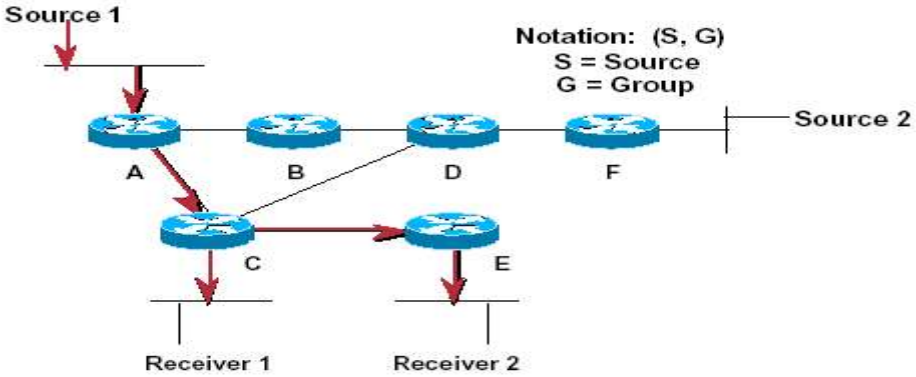
Οι (*,G) καταχώρηση που φαίνονται στο πρώτο πεδίο του πίνακα δρομολόγησης του παραδείγματος, χρησιμοποιείται για την προώθηση της multicast κίνησης προς τα κάτω, μέσο ενός Shared δέντρου δρομολόγησης. Το χρονόμετρο στην πρώτη γραμμή των καταχωρήσεων υποδεικνύει πότε η καταχώρηση θα διαγραφεί. Η κίνηση που φτάνει μέσο του Shared δέντρου προωθείται από το incoming interface στα outgoing interfaces. Η σημασία των flags παραμέτρων που φαίνονται στις καταχώρισης θα εξηγηθεί στο κεφάλαιο 7.

3.5 Multicast δέντρα διανομής

Με τον όρο δέντρο διανομής ονομάζουμε το μονοπάτι (path) που ακολουθούν τα δεδομένα από την πηγή μέχρι τους αποδέκτες. Τα δέντρα διανομής δημιουργούνται από τα multicast πρωτόκολλα δρομολόγησης και το κάθε ένα από τα πρωτόκολλα αυτά χρησιμοποιεί διαφορετικό μηχανισμό για την δημιουργία ενός δέντρου. Δύο είδη δέντρων διανομής μπορούν να δημιουργηθούν, το shortest path ή source distribution tree και shared path distribution tree, και στο καθένα από αυτά αναφερόμαστε χωριστά στη συνέχεια.

3.5.1 Shortest Path Trees

Τα Shortest Path Trees (SPTs) ή Source Path trees λέγονται έτσι, γιατί επιλέγουν τον κοντινότερο δρόμο από την πηγή προς τους αποδέκτες. Για κάθε multicast πηγή δημιουργείται ένα SPT multicast δέντρο δρομολόγησης που συνδέει άμεσα την πηγή με όλους τους αποδέκτες. Κάθε δρομολογητής που είναι μέλος ενός multicast SPT δέντρου έχει μια (S,G) καταχώρηση και μια λίστα από εξερχόμενα interfaces στο πίνακα δρομολόγησης του, όπου S είναι η διεύθυνση της πηγής και G της multicast ομάδας.

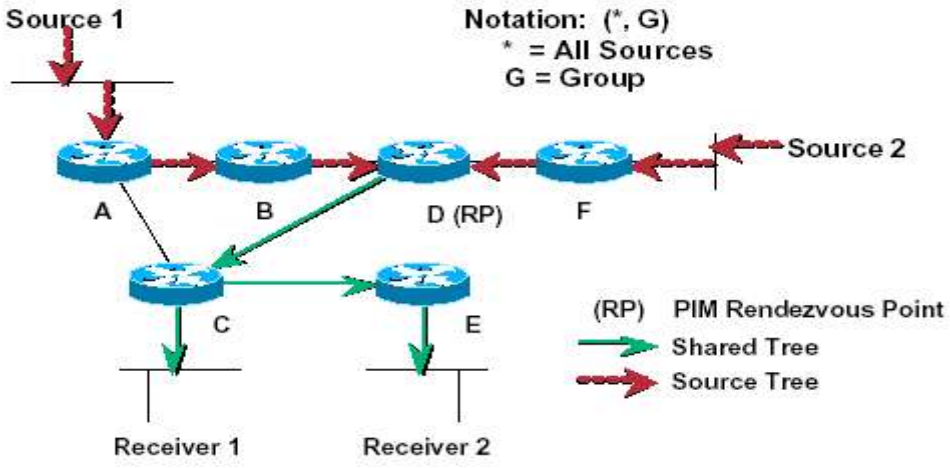


Εικόνα 3.5: SPT

Στο παραπάνω σχήμα παρατηρούμε ότι το δέντρο δημιουργήθηκε με τα λιγότερα δυνατά hops, ενώ θα μπορούσε να έχει δημιουργηθεί μέσω των δρομολογητών B,D,C, αλλά με περισσότερα hops. Το δέντρο αυτό ονομάζεται Shortest Path Tree.

3.5.2 Shared Trees

Τα shared trees λέγονται και RP trees γιατί βασίζονται σε ένα κεντρικό δρομολογητή που λέγεται rendezvous point (σημείο συνάντησης) για το PIM-SM. Ο RP συλλέγει όλη την κίνηση από τις πηγές και την προωθεί στους αποδέκτες. Οι leaf δρομολογητές* έχουν στείλει μηνύματα σύνδεσης στον RP οπότε αυτός είναι γνώστης των δρομολογητών, στους οποίους θα προωθήσει τα πακέτα. Αυτό έχει ως αποτέλεσμα σε ένα LAN να δημιουργείται ένα δέντρο για κάθε ομάδα ανεξάρτητα από το πλήθος των πηγών που στέλνουν στην ομάδα. Αν ένας αποδέκτης είναι και πηγή, δεν μπορεί να χρησιμοποιήσει το δέντρο για να στείλει πακέτα στον RP, όμως μπορεί να λάβει από το RP. Οι δρομολογητές των RPTs έχουν μια (*,G) καταχώρηση στον πίνακα δρομολόγησής τους, όπου "*" σημαίνει ότι λαμβάνουν από όλες τις πηγές και G είναι η IP multicast διεύθυνση της ομάδας.



Εικόνα 3.6: RPT

* Leaf ονομάζουμε το δρομολογητή που έχει συνδεμένους αποδέκτες. Επίσης ονομάζεται και last hop δρομολογητής. Ο πρώτος δρομολογητής από την πλευρά της πηγής ονομάζεται first hop.

Στο παράδειγμα της εικόνας 3.6, ο δρομολογητής D είναι το RP, οπότε συλλέγει την multicast κίνηση που στέλνουν οι πηγές 1,2 και την προωθεί στους αποδέκτες 1 και 2.

Η multicast κίνηση προωθείται μέσω του shared tree με δεδομένο μόνο την διεύθυνση της ομάδας G που τα πακέτα φέρουν, χωρίς οι δρομολογητές να παίρνουν υπόψη τους ποια είναι η πηγή.

3.5.3 Σύγκριση Shortest Path Tree (SPT) με Shared Path Tree (RPT)

Κάνοντας μια σύγκριση των δύο αυτών δέντρων διανομής, θα παρατηρήσουμε ότι τα RPTs προκαλούν μεγαλύτερες καθυστερήσεις στο δίκτυο (τα πακέτα πρέπει πρώτα να σταλούν στο RP πριν προωθηθούν), αλλά οι δρομολογητές πραγματοποιούν λιγότερη επεξεργασία και απαιτούν λιγότερη μνήμη. Αντίθετα τα SPTs παρέχουν μικρότερη απόσταση, μικρότερη καθυστέρηση, αλλά απαιτούν περισσότερη υπολογιστική δύναμη από τους δρομολογητές. Γενικότερα, όταν ο ρυθμός των πακέτων που μεταφέρονται είναι μεγάλος, χρησιμοποιείται SPT, ενώ αν είναι μικρός RPT.

Επίσης, υπάρχουν και περιπτώσεις, στις οποίες χρησιμοποιούνται και τα δύο δέντρα, όπως θα δούμε στο PIM-SM πρωτόκολλο, και όπου το δέντρο μπορεί από RPT να γίνει SPT. Μπορεί δηλαδή να ρυθμιστεί ένα όριο σε bits/sec που αν η κίνηση υπερβεί, το δέντρο μετατρέπεται από RPT σε SPT. Το προκαθορισμένο αυτό όριο είναί 0 bits/sec.

Τέλος, πρέπει να αναφερθεί ότι ο τρόπος δημιουργίας των δέντρων διανομής εξαρτάται από τα πρωτόκολλα δρομολόγησης, που θα εξετάσουμε στο επόμενο κεφάλαιο.

3.4 Πηγές 3ου Κεφαλαίου

1. Introdaction to IP Multicast Routing. Internet draft. http://infocom.uniroma1.it/alef/rfc/draft-ietf-mboned-intro-multicast-03.txt
2. http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/uni_rpf.htm. Cisco PDF.
3. IP Multicast Fundamentals. http://rdweb.cns.vt.edu/public/slides/ipm-1/
4. IP Multicast: Concepts, Algorithms and protocols. http://www.cis.ohio-state.edu/~jain/cis788-97/ip_multicast/
5. §Cisco White Paper. http://www.cisco.com/warp/public/cc/pd/iosw/tech/ipmu_ov.pdf
6. §Interdomain Multicast Fundamentals. http://www.pearsonptg.com/samplechapter/0201746123.pdf
7. §The Evolution of Multicast: From the MBone to Inter-Domain Multicast to Internet2 Deployment. Kevin C. Almeroth. http://macross.dynodns.net/idr/multicast_evolution.pdf
8. §http://www.comsoc.org/livepubs/surveys/public/1q00issue/ramalho.ht
9. §Windows White Paper. http://www.microsoft.com/windows2000/docs/pimsm2.doc
10. §http://www.uoregon.edu/~llynch/mcastwks/shep/
11. §www.nrg.cs.uoregon.edu/pubs/mct_icn01_talk.pdf
12. §http://www.tcm.hut.fi/Opinnot/Tik-110.551/1996/mcast.html
13. §RFC 1812: requirements for IPv4 routers.

Κεφάλαιο 4ο: Intra-domain Multicasting

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα ασχοληθούμε με το multicasting εντός ενός domain[1] και τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται σε αυτήν την περίπτωση για να δημιουργηθούν τα δέντρα διανομής. Πριν αναλύσουμε τα intra-domain πρωτόκολλα θα δούμε το Mbone, το πρώτο δίκτυο που χρησιμοποίησε multicasting, και από το οποίο δημιουργήθηκε η ανάγκη για δημιουργία intra-domain και inter-domain multicast τοπολογίας.

4.2 Το MBONE

Το MBONE ήταν το αποτέλεσμα των πρώτων δυο “audiocast” πειραμάτων του IETF, στα οποία στάλθηκαν ζωντανά εικόνα και ήχος ταυτόχρονα από την συνεδρίαση του IETF σε προορισμούς σε όλο τον κόσμο. Η ιδέα ήταν να κατασκευαστεί ένας ημι-μόνιμος IP multicast χώρος για να μεταφέρει τα αποτελέσματα και την εξέλιξη των πειραμάτων των συνεδριάσεων.

Το 1992 στον IETF αποφασίστηκε ότι το πρόβλημα της έλλειψης έξυπνων hardware συστημάτων (δρομολογητές) θα μπορούσε να ξεπεραστεί (προσωρινά) με τη χρήση ενός έξυπνου software. Για αυτό λοιπόν το λόγο, δημιούργησαν ένα "virtual network" -ένα δίκτυο το οποίο τρέχει πάνω από το Internet- και έγραψαν software που επιτρέπει σε multicast πακέτα να διασχίζουν το δίκτυο. Εφοδιασμένοι με το κατάλληλο software, οι δρομολογητές μπορούσαν να στέλνουν δεδομένα όχι μόνο σ' ένα κόμβο του Internet, αλλά σε πολλούς περισσότερους. Το δίκτυο αυτό που ονόμασαν MBONE είναι ένα virtual network, διότι μοιράζεται τα ίδια φυσικά μέσα με το Internet.

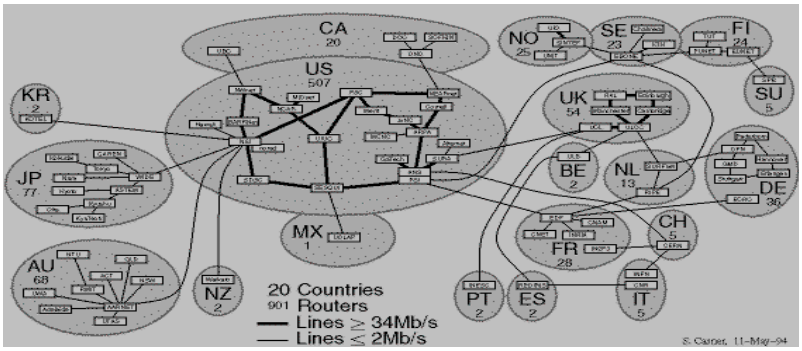
Το δίκτυο αποτελείτο από “νησιά”[2] που μπορούσαν απευθείας να υποστηρίζουν IP multicast και ήταν συνδεδεμένα από εικονικές point-to-point συνδέσεις που λέγονταν “tunnels”[3]. Στα άκρα των tunnels ήταν στην ουσία σταθμοί εργασίας που είχαν λειτουργικό σύστημα που υποστήριζε IP multicast και έτρεχε τον “mrouted”, multicast routing δαίμονα. Τα IP multicast πακέτα ενσωματώνονταν σε unicast για την μετάδοση τους μέσα από τα tunnels κι έτσι φαίνονταν σαν unicast πακέτα, πράγμα που τους βοηθούσε στο πέρασμα των τοπολογιών, οι οποίες διέθεταν δρομολογητές που δεν υποστήριζαν IP multicasting. Η δρομολόγηση μεταξύ των tunnels γινόταν με το Distance Vector Multicast Routing Protocol. Σε μια ήπειρο, η τοπολογία του MBONE ήταν συνδυασμός πλέγματος και αστέρα. Το backbone και τα περιφερειακά δίκτυα ήταν συνδεδεμένα με ένα πλέγμα από tunnels και mrouted μηχανές. Κάθε περιφερειακό δίκτυο είχε τοπολογία αστέρα και

[1] Domain στην περίπτωση μας, ονομάζουμε μια ομάδα από δρομολογητές που βρίσκονται κάτω από την ίδια διαχείριση.

[2] νησί στο MBone εννοούσαμε μια περιοχή που περιείχε δρομολογητές που υποστήριζαν ip multicasting. Στα άκρα αυτών των νησιών υπήρχαν υπολογιστές που έκαναν tunneling.

[3] Tunneling είναι η διαδικασία ενσωμάτωσης συγκεκριμένων πακέτων (εσωτερικό) μέσα σε ένα άλλο πακέτο (εξωτερικό), έτσι ώστε το εσωτερικό πακέτο να είναι αδιαφανής στο δίκτυο στο οποίο το εξωτερικό πακέτο δρομολογείται.

κρεμόταν στην άκρη ενός πλέγματος, στην οποία συνδέονταν όλα τα ενδιαφερόμενα δίκτυα. Η τοπολογία του MBONE το 1994 ήταν:



Εικόνα 4.1: Το MBONE

Σήμερα η πληθώρα των δρομολογητών του internet υποστηρίζει IP Multicasting και το MBONE έχει δώσει τη θέση του σε νέες αρχιτεκτονικές, όπως το Interdomain Multicasting.

4.3 Πρωτόκολλα δρομολόγησης

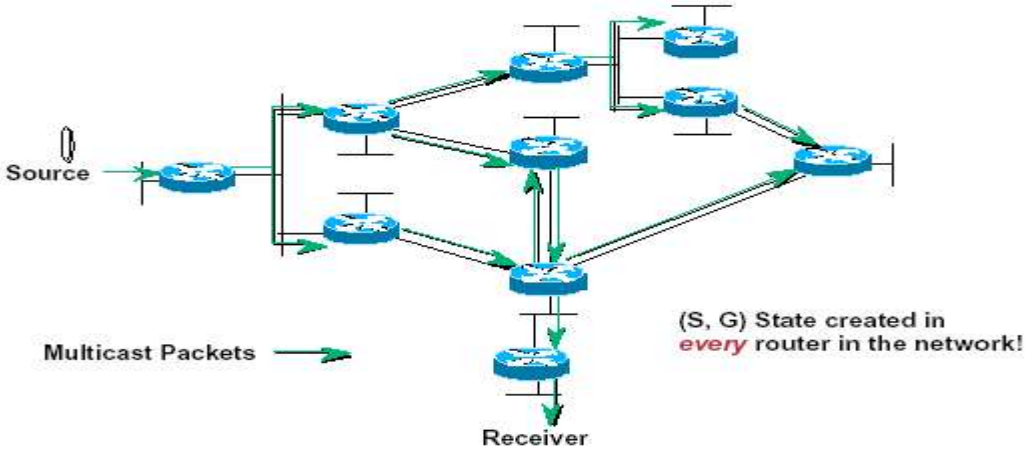
Από το 1992 έως το 1997, η χρήση του Mbone έγινε ιδιαίτερα ευρεία. Δεν ήταν πια ένα απλό εικονικό δίκτυο που υπήρχε πάνω από το internet, αλλά γρήγορα έγινε μέρος του δικτύου. Εκτός από τα απλά DVMRP tunnels, νέα πρωτόκολλα δρομολόγησης αναπτύχθηκαν και οι δρομολογητές άρχισαν να υποστηρίζουν εγγενώς το multicasting. Τα πρωτόκολλα αυτά χωρίζονται σε δύο κατηγορίες: τα dense mode και τα sparse mode πρωτόκολλα. Τα dense mode πρωτόκολλα είναι: i) το Distance Vector Multicast Routing Protocol (DVMRP), ii) το Multicast OSPF (MOSPF) και iii) το Protocol Independent Multicasting (PIM-Dense Mode). Τα sparse mode πρωτόκολλα είναι: i) το Protocol Independent Multicasting (PIM-Sparse Mode) και ii) το Core Based Trees (CBT). Στη συνέχεια θα αναλύσουμε το PIM-DM και το PIM-SM, τα οποία χρησιμοποιούνται στην πληθώρα των δικτύων που υποστηρίζουν multicasting σήμερα.

4.3.1 Protocol Independent Multicasting Dense Mode (PIM-DM)

Το PIM-DM λέγεται “protocol independent” γιατί μπορεί να χρησιμοποιήσει πληροφορίες δρομολόγησης από κάθε unicast πρωτόκολλο δρομολόγησης. Με τον όρο Dense Mode (πυκνής δρομολόγησης) εννοούμε ότι το πρωτόκολλο δημιουργήθηκε για περιπτώσεις όπου οι multicast ομάδες έχουν πολλά μέλη.

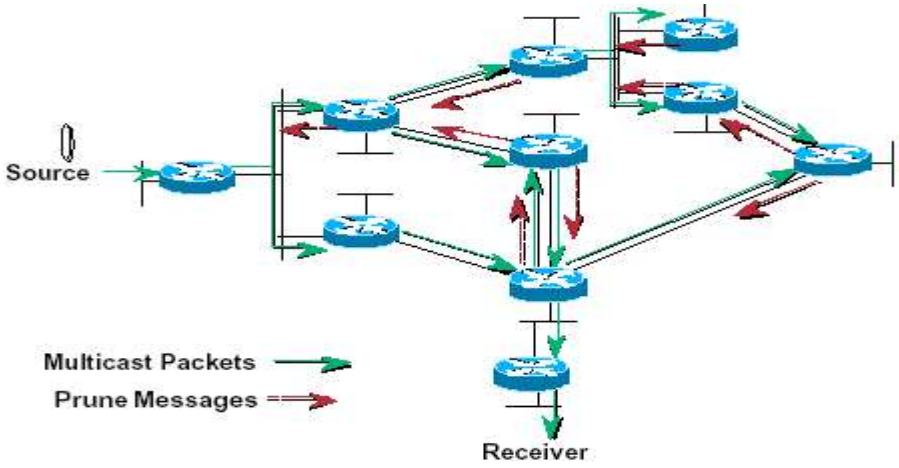
Το PIM-DM υποθέτει ότι όταν μια πηγή αρχίσει να στέλνει δεδομένα, όλες οι μηχανές (δρομολογητές, PCs) θέλουν να λάβουν multicast πακέτα. Αρχικά, τα multicast δεδομένα διασκορπίζονται σε όλες τις περιοχές του δικτύου. Κάθε δρομολογητής παίρνει την κίνηση από το RPF interface και την προωθεί σε όλους τους γειτονικούς του που τρέχουν PIM-DM, δημιουργώντας με αυτό τον τρόπο μια (S,G) καταχώρηση στον πίνακα

δρομολόγησής του. Αυτό έχει σαν αποτέλεσμα μερικά πακέτα να φτάνουν σε interfaces διαφορετικά του RPF στις περιπτώσεις που φαίνονται στην εικόνα 4.2.



Εικόνα 4.2

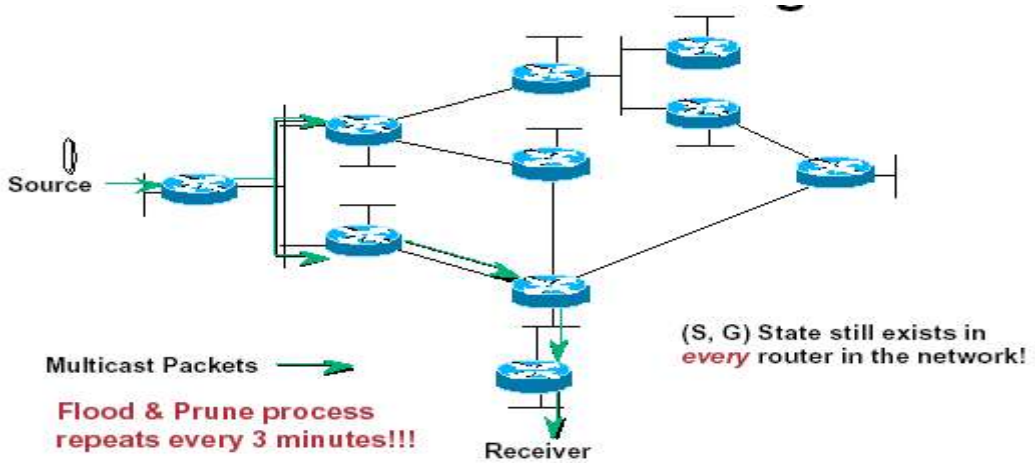
Το PIM-DM στέλνει μηνύματα αποκοπής της κίνησης (prune messages), για να σταματήσει την ροή άχρηστων δεδομένων. Τα μηνύματα αυτά στέλνονται στο RPF interface όταν ο δρομολογητής δεν έχει μέλη που ζητούν την multicast κίνηση. Επίσης, στέλνονται και στα άλλα interfaces, για να σταματήσει την ροή των δεδομένων που φτάνουν στο λάθος interface (RPF έλεγχος). Συνοψίζοντας, ένας δρομολογητής στέλνει μηνύματα αποκοπής στους πιο πάνω δρομολογητές του, i) όταν διαπιστώσει ότι δεν έχει συνδεμένους υπολογιστές ενδιαφερόμενους για την multicast κίνηση στα εξερχόμενα interfaces του και ii) όταν αποτύχει ο RPF έλεγχος. Η εικόνα 4.3 δείχνει τις δύο περιπτώσεις που οι δρομολογητές στέλνουν prune μηνύματα.



Εικόνα 4.3: Οι δρομολογητές στέλνουν μηνύματα αποκοπής

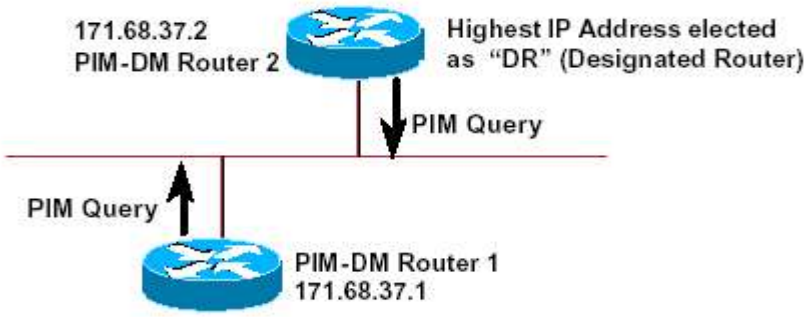
Μετά τα μηνύματα αποκοπής όλες οι συνδέσεις εκτός των απαραίτητων διακόπτονται. Έτσι δημιουργείται ένα Source Path Tree από την πηγή μέχρι τον αποδέκτη (εικόνα 4.4). Παρά το γεγονός ότι τα δεδομένα σταματούν να φτάνουν στους περισσότερους δρομολογητές του δικτύου, η (S,G) καταχώρηση συνεχίζει να υπάρχει σε όλους και παραμένει σε αυτούς μέχρι η πηγή να σταματήσει την εκπομπή. Η κατάσταση αποκοπής διαρκεί 3 λεπτά. Στη συνέχεια η κίνηση διασκορπίζεται ξανά σε όλους τους δρομολογητές, όπως είχε γίνει στην αρχή. Αυτός ο περιοδικός διασκορπισμός

και η αποκοπή πρέπει να λαμβάνονται υπόψη όταν σχεδιάζουμε να χρησιμοποιήσουμε το PIM-DM.



Εικόνα 4.4 Το αποτέλεσμα μετά την αποκοπή

Οι δρομολογητές, για να ανακαλύψουν άλλους γειτονικούς δρομολογητές που τρέχουν PIM-DM, στέλνουν PIM ερωτήματα (queries) στην “All-Routers” (224.0.0.2) multicast διεύθυνση. Όλοι οι PIM-DM δρομολογητές στέλνουν μηνύματα χαιρετισμού (“Hello Messages”) στην “All PIM Routers” διεύθυνση (224.0.0.13), για να δηλώσουν ότι τρέχουν PIM. Σε ένα τοπικό δίκτυο με πολλούς δρομολογητές αυτός με την μεγαλύτερη IP διεύθυνση εκλέγεται ως ο Designated Router (DR) (εικόνα 4.5). Στο PIM-DM ο DR δεν έχει κάποιο ιδιαίτερο ρόλο σε αντίθεση με τον αντίστοιχό του στο PIM-SM που θα εξετάσουμε στην επόμενη ενότητα. Εξαίρεση αποτελεί η περίπτωση, όπου χρησιμοποιείται IGMPv1, οπότε ο DR ενεργεί και σαν IGMP ερωτών δρομολογητής.



Εικόνα 4.5: Εκλογή του DR

4.3.2 Protocol Independent Multicasting Sparse-Mode

Το Protocol Independent Multicast Sparse-Mode (PIM-SM) δρομολογεί multicast πακέτα σε multicast ομάδες και σχεδιάστηκε για να δημιουργεί αποδοτικά δέντρα διανομής. Sparse Mode σημαίνει ότι το πρωτόκολλο δημιουργήθηκε για περιπτώσεις όπου οι multicast ομάδες δεν έχουν πολλά μέλη.

Το PIM-SM υποστηρίζει το παραδοσιακό IP multicast όπου οι πηγές απλά προωθούν πακέτα στο first-hop Ethernet, χωρίς να ενημερώνουν γι

αυτό. Οι αποδέκτες στέλνουν IGMP μηνύματα στους δρομολογητές με σκοπό να συνδεθούν στα multicast group και να πάρουν τα δεδομένα.

Το PIM-SM χρησιμοποιείται μεταξύ των δρομολογητών, κάτι που σημαίνει ότι οι hosts δε χρειάζεται να ρυθμιστούν για να το χρησιμοποιούν. Υποστηρίζει shared ή source δέντρα διανομής ή και τα δύο μαζί.

Στην εικόνα 4.6 βλέπουμε την επικεφαλίδα του PIM-SM έκδοση 2.

Ver	Type	Reserved	Checksum

Εικόνα 4.6

Ver: έκδοση του PIM. Για την έκδοση 2, η τιμή είναι 2.

Type: καθορίζει τι είδος είναι το πακέτο. Παίρνει τιμές από 0 έως 8. (εικόνα 4.7)

Type	**Description**
0	Hello
1	Register
2	Register-Stop
3	Join/Prune
4	Bootstrap
5	Assert
8	Candidate RP advertisement

Εικόνα 4.7

Θα εξετάσουμε κάθε μέρος του PIM-SM έκδοση 2 ξεκινώντας από το πώς γίνεται η ανακάλυψη των γειτονικών δρομολογητών και συνεχίζοντας με την σύνδεση στο shared δέντρο, την εγγραφή της πηγής στο RP, την μετατροπή σε SPT, την αποκοπή των interface και τέλος τον προσδιορισμό του RP. Τα έκδοση 2 μηνύματα ενσωματώνονται στα IP πακέτα με το πρωτόκολλο να παίρνει το νούμερο 103.

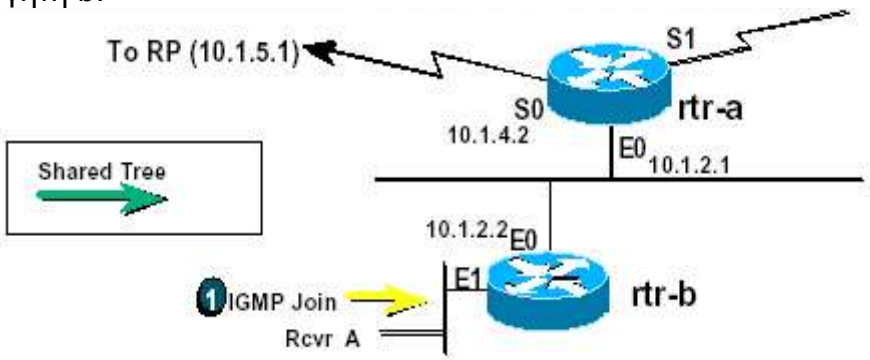
4.3.2.1 Ανακάλυψη των Γειτονικών Δρομολογητών

Όπως το PIM-DM, και το PIM-SM στέλνει περιοδικά PIM μηνύματα χαιρετισμού (PIM Hellos) για να ανακαλύψει την ύπαρξη άλλων PIM δρομολογητών στο δίκτυο και για να εκλέξει ποιος από αυτούς θα είναι ο designated (DR)(εικόνα 4.5). Σε ένα PIM-SM δίκτυο ο DR είναι υπεύθυνος να στέλνει μηνύματα σύνδεσης στον RP για τα μέλη και μηνύματα καταχώρησης στον RP για τις πηγές. Τα PIM-SM μηνύματα χαιρετισμού στέλνονται στην “All PIM-Routers” (224.0.0.13) multicast group διεύθυνση. Για τη εκλογή του DR, κάθε PIM δρομολογητής εξετάζει τα PIM μηνύματα χαιρετισμού που παίρνει από τους γειτονικούς και συγκρίνει την IP διεύθυνση του δικού του interface με την IP διεύθυνση κάθε PIM γειτονικού. Ο γειτονικός PIM δρομολογητής με τη μεγαλύτερη IP διεύθυνση εκλέγεται ως designated. Οι δρομολογητές δεν στέλνουν αναφορά ότι έλαβαν τα μηνύματα χαιρετισμού, ενώ αν για ένα χρονικό διάστημα (μπορεί να καθοριστεί) ο DR δε στείλει μηνύματα χαιρετισμού, ο μηχανισμός εκλογής του DR ξεκινάει την ίδια διαδικασία. Όταν λαμβάνεται ένα μήνυμα χαιρετισμού από ένα δρομολογητή, δεν προστίθεται

αυτόματα κάθε interface στη λίστα με τα εξερχόμενα interfaces, αλλά πρέπει πρώτα κάποιος αποδέκτης που βρίσκεται σε επόμενο δρομολογητή (downstream receiver) να συνδεθεί στην ομάδα, για να αρχίσει να προωθείται η κίνηση από αυτό το interface.

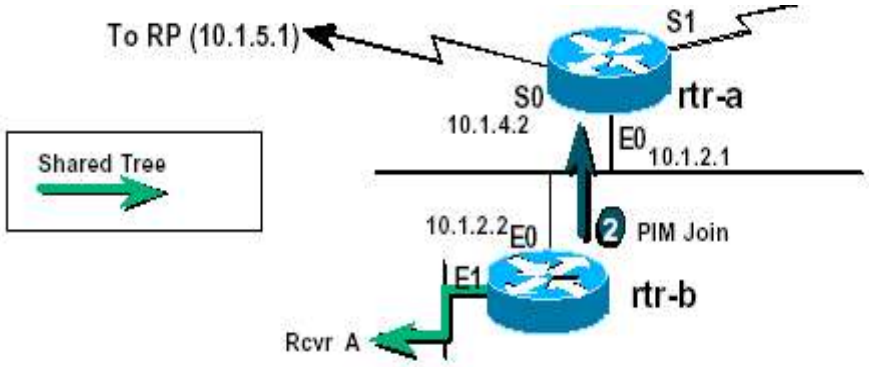
4.3.2.2 Σύνδεση στο Shared Δέντρο

Όπως έχουμε αναφέρει στην παράγραφο 1.6, όταν μια μηχανή θέλει να συνδεθεί σε μια multicast ομάδα, στέλνει ένα IGMP μήνυμα στον πρώτο δρομολογητή που συναντάει (upstream router). Αυτό σημαίνει ότι ο δρομολογητής πρέπει να αρχίσει να δέχεται multicast δεδομένα για αυτήν την ομάδα. Στην εικόνα 4.8 ο αποδέκτης A στέλνει IGMP μήνυμα στον δρομολογητή b.



Εικόνα 4.8

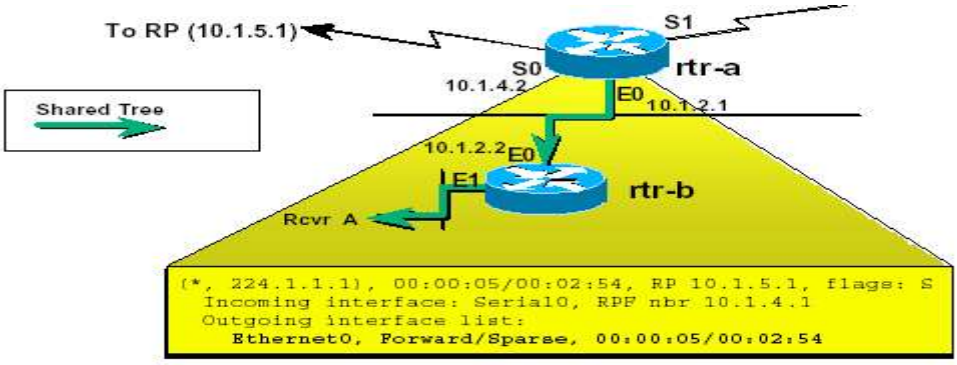
Για να λάβει ο δρομολογητής δεδομένα πρέπει να ενημερώσει το RP ότι επιθυμεί να συνδεθεί στο RPT. Αυτό το επιτυγχάνει στέλνοντας ένα PIM (*,G) μήνυμα σύνδεσης στον upstream PIM γειτονικό δρομολογητή, που βρίσκεται στην κατεύθυνση του RP. Τα μηνύματα σύνδεσης στέλνονται από τον ένα δρομολογητή στον άλλο στη διεύθυνση 224.0.0.13, που είναι η All-PIM-Routers ομάδα. Αυτό σημαίνει, ότι όλοι οι PIM γειτονικοί δρομολογητές είναι ενημερωμένοι για την σύνδεση, αλλά μόνο οι upstream δημιουργούν τη σύνδεση. Στην εικόνα 4.9 ο δρομολογητής b στέλνει PIM μήνυμα σύνδεσης στον upstream δρομολογητή a που βρίσκεται στο δρόμο για το RP.



Εικόνα 4.9: Ο δρομολογητής στέλνει PIM μήνυμα σύνδεσης

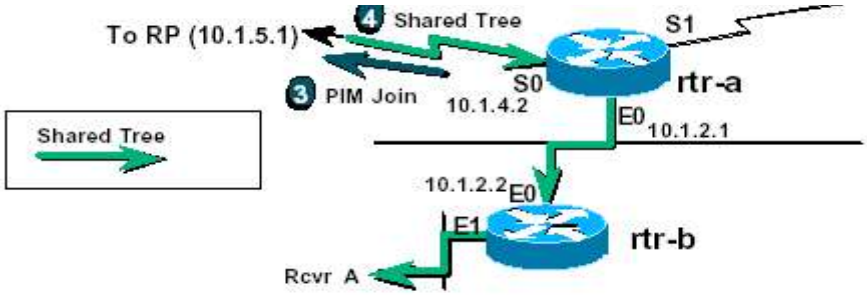
Όταν ένας PIM δρομολογητής δεχτεί ένα (*,G) μήνυμα σύνδεσης από ένα downstream δρομολογητή, ελέγχει αν η (*,G) καταχώρηση υπάρχει ήδη στον multicast πίνακα δρομολόγησής του. Αν η καταχώρηση υπάρχει, τότε το

μήνυμα σύνδεσης έχει φτάσει στο shared δέντρο και το interface, από το οποίο έφτασε το μήνυμα, προστίθεται στην λίστα με τα εξερχόμενα interfaces. Αν η καταχώρηση δεν υπάρχει, αυτή δημιουργείται από το δρομολογητή, το interface προστίθεται στη λίστα εξερχόμενων και το μήνυμα προωθείται προς το RP. Στην εικόνα 4.10 βλέπουμε την κατάσταση του multicast πίνακα δρομολόγησης του interface E0 του δρομολογητή a, μετά τη λήψη του μηνύματος σύνδεσης. Παρατηρούμε ότι ο δρομολογητής εδώ δημιούργησε (*,224.1.1.1) καταχώρηση και πρόσθεσε το interface E0 στη λίστα με τα εξερχόμενα interfaces. Στα υπόλοιπα πεδία του πίνακα δρομολόγησης θα αναφερθούμε σε επόμενο κεφάλαιο.



Εικόνα 4.10: Ο πίνακας δρομολόγησης του interface E0

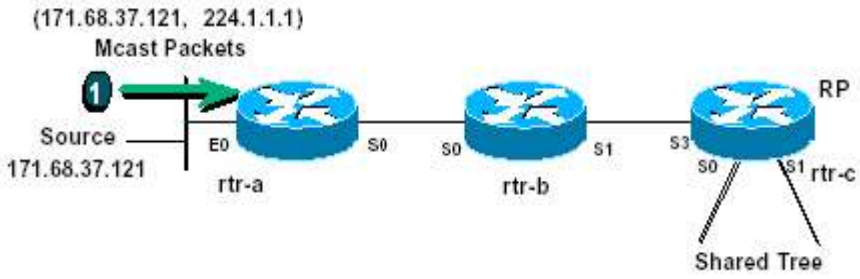
Το τελικό αποτέλεσμα του παραπάνω μηχανισμού είναι η δημιουργία μιας (*,G) καταχώρησης σε όλο το δρόμο από τον πρώτο στον αποδέκτη δρομολογητή μέχρι το RP, έτσι ώστε η multicast κίνηση για την ομάδα “G” να προωθηθεί μέσω του Shared δέντρου στον τελευταίο δρομολογητή, όπως φαίνεται στην εικόνα 4.11.



Εικόνα 4.11

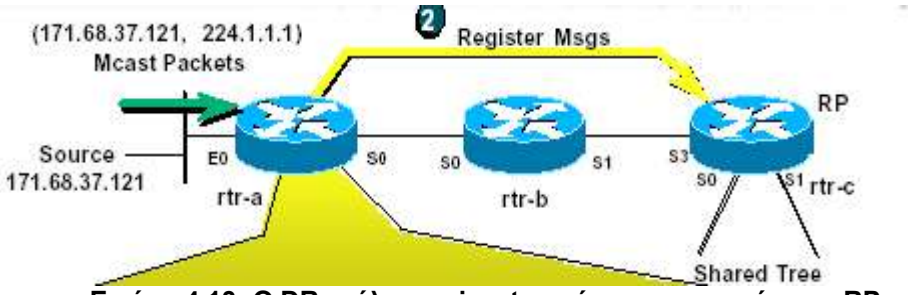
4.3.2.3 Εγγραφή της Πηγής στο RP (Source Register)

Οι πηγές δεν είναι υποχρεωτικώς μέλη της ομάδας που στέλνουν δεδομένα. Μια πηγή αρχίζει να στέλνει multicast κίνηση χωρίς προηγουμένως να έχει στείλει IGMP μήνυμα. Ο designated δρομολογητής μπορεί να αρχίσει να δέχεται δεδομένα από την πηγή, χωρίς να έχει (S,G) καταχώρηση στον πίνακα δρομολόγησής του. Αυτό σημαίνει ότι δεν έχει πληροφορία για το πώς να στείλει πακέτα στο RP μέσω ενός δέντρου. Στην εικόνα 4.12 η πηγή 171.68.37.121 στέλνει multicast πακέτα στο group 224.1.1.1. Ο δρομολογητής a προσθέτει στον πίνακα δρομολόγησης του την (S:171.68.37.121, G:224.1.1.1) καταχώρηση.



Εικόνα 4.12: Η πηγή στέλνει multicast πακέτα στον πρώτο δρομολογητή

Όταν ο DR δεχτεί το αρχικό multicast πακέτο, το ενθυλακώνει σε ένα PIM μήνυμα εγγραφής (Register message) και το στέλνει unicast στο RP της ομάδας για την οποία προορίζεται το μήνυμα (εικόνα 4.13).



Εικόνα 4.13: Ο DR στέλνει unicast μηνύματα εγγραφής στο RP

Μόλις ο RP λάβει το μήνυμα εγγραφής, το ανοίγει (decapsulate), εξετάζει το multicast πακέτο και αν αυτό το πακέτο έχει σταλεί για μια ομάδα για την οποία το RP έχει (*,G) καταχώρηση, το προωθεί από τα εξερχόμενα interface της λίστας. Επίσης, δημιουργεί μια (S,G) καταχώρηση και στέλνει ένα (S,G) μήνυμα σύνδεσης πίσω στην πηγή, με σκοπό τη δημιουργία ενός SPT από την πηγή στο RP (εικόνα 4.14).

Εικόνα 4.14: Ο RP στέλνει μήνυμα σύνδεσης στην πηγή

Αν δεν υπάρχουν συνδεδεμένοι αποδέκτες στον RP, αυτός δημιουργεί μια (S,G) καταχώρηση και απορρίπτει το πακέτο. Επίσης στέλνει ένα PIM register-stop μήνυμα στον πρώτο δρομολογητή για να σταματήσει να προωθεί άσκοπη κίνηση. Η ίδια διαδικασία επαναλαμβάνεται κάθε φορά που ο πρώτος δρομολογητής δέχεται από την πηγή ένα multicast πακέτο.

Μόλις ο πρώτος από την πηγή δρομολογητής δεχτεί το (S,G) μήνυμα σύνδεσης, που στέλνεται από δρομολογητή σε δρομολογητή ξεκινώντας από το RP και καταλήγοντας στην πηγή, προσθέτει το interface από το οποίο το

έφτασε το μήνυμα, στη λίστα με τα εξερχόμενα interfaces για την (S,G) καταχώρηση που ήδη υπήρχε. Ας θυμηθούμε ότι η (S,G) καταχώρηση δημιουργείται στον πρώτο δρομολογητή, όταν αυτός δεχτεί το πρώτο multicast πακέτο από την πηγή. Στη συνέχεια, ξεκινάει να προωθεί τα multicast δεδομένα από το SPT που δημιουργήθηκε, ενώ συνεχίζει να στέλνει και unicast μηνύματα εγγραφής στο RP. Μόλις ο RP αρχίσει να δέχεται κανονικά, όχι ενθυλακωμένα, multicast δεδομένα μέσω του SPT, στέλνει unicast ένα PIM (S,G) register-stop μήνυμα πίσω στον πρώτο δρομολογητή (εικόνα 4.15). Με αυτό ενημερώνει τον πρώτο δρομολογητή ότι η κίνηση φτάνει στο RP και του επιτρέπει να σταματήσει την ενθυλάκωση και να προωθεί την κίνηση κανονικά.

Εικόνα 4.15: Το RP στέλνει unicast ένα register-stop μήνυμα στον πρώτο δρομολογητή

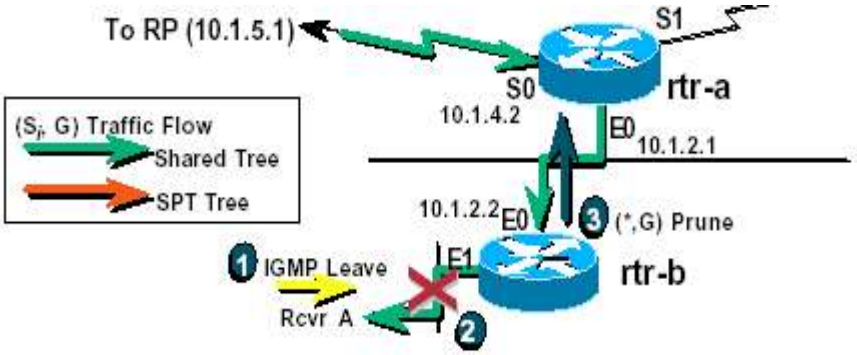
4.3.2.4 Μετατροπή σε SPT.

Στον leaf δρομολογητή μπορεί να καθοριστεί ένα όριο σε kilobits, το οποίο όταν υπερβεί η κίνηση, το δέντρο μετατρέπεται από Rendezvous Point Tree (RPT) σε Source Path Tree (SPT). Το προκαθορισμένο όριο είναι 0 kbps. Αυτό σημαίνει ότι όλα τα δέντρα άμεσα μετατρέπονται σε Shortest-Path Tree. Όταν λοιπόν η κίνηση υπερβεί το όριο, ο DR στέλνει ένα (S,G) μήνυμα σύνδεσης πίσω στην πηγή, δημιουργώντας έτσι ένα SPT από την πηγή στο δρομολογητή. Μετατροπή σε SPT σημαίνει ότι χρησιμοποιείται ο μικρότερος δρόμος για την μεταφορά της multicast κίνησης. Αυτή μπορεί να μειώσει τις καθυστερήσεις, κάτι που εξαρτάται όμως από την τοποθεσία της πηγής σε σχέση με τον αποδέκτη και το RP. Αρνητικό της μετατροπής στην οποία αναφερόμαστε είναι ότι περισσότερα δεδομένα χρειάζεται να αποθηκεύονται στους δρομολογητές.

4.3.2.5 Αποκοπή των Interface (Interface Pruning)

Όταν ένα RP λάβει ένα μήνυμα αποκοπής, παύει την προώθηση της κίνησης που έρχεται από την πηγή που δείχνει το μήνυμα. Τα μηνύματα αποκοπής δημιουργούνται από τον τελευταίο δρομολογητή. Αν το τελευταίο μέλος μιας multicast ομάδας στείλει στον δρομολογητή ένα IGMPv2 μήνυμα αποχώρησης (leave message), διαγράφονται το interface για την καταχώρηση (*,G) και για όλες τις (S,G) από την λίστα με τα εξερχόμενα interfaces για την ομάδα G. Αν κάθε interface για την ομάδα G διαγραφεί, τότε το μήνυμα αποκοπής στέλνεται προς τα πάνω, μέσω του shared tree, στο RP. Στην εικόνα 4.16 ο αποδέκτης A στέλνει ένα IGMP μήνυμα αποχώρησης στον δρομολογητή b. Αυτός αποκόπτει το interface E1 από τα

εξερχόμενα interfaces, γιατί δεν έχει άλλο αποδέκτη για την ομάδα G σε αυτό το interface. Όμως, επειδή γενικότερα δεν έχει άλλο ενδιαφερόμενο σε άλλο interface στέλνει μήνυμα αποκοπής στον πιο πάνω δρομολογητή από το interface E0 που είναι αυτό που δέχεται τα δεδομένα για την ομάδα G.



Εικόνα 4.16: Ο δρομολογητής στέλνει μηνύματα αποκοπής

Η ίδια διαδικασία γίνεται και στους επόμενους δρομολογητές μέχρι το RP εκτός και αν σε κάποιον από αυτούς υπάρχει ενδιαφερόμενος αποδέκτης σε κάποιο από τα interfaces του. Κάθε δρομολογητής καθυστερεί την αποκοπή των interfaces για 3 δευτερόλεπτα, καθώς περιμένει μήπως στο διάστημα αυτό τυχόν ενδιαφερόμενος συνδεθεί στην ομάδα.

4.3.2.6 Προσδιορισμός του RP

Οι αναφορές μας μέχρι εδώ στο RP παίρνουν ως δεδομένο τον τρόπο με τον οποίο οι δρομολογητές ενημερώνονται για την ύπαρξή του. Σε αυτήν την παράγραφο κρίνουμε σκόπιμο να αναφερθούμε στον τρόπο με τον οποίο γίνεται αυτό.

Αρχικά πρέπει να πούμε ότι υπάρχουν 3 τρόποι για τον προσδιορισμό του RP: i) ο Auto RP, ii) ο Static RP και iii)ο PIMv2 BSR. Στην Auto RP περίπτωση οι δρομολογητές μαθαίνουν αυτόματα για το ποιος είναι ο RP. Η Static RP είναι μια στατική μέθοδος, που απαιτεί από το διαχειριστή τη ρύθμιση για κάθε δρομολογητή με τη διεύθυνση του RP για μια ομάδα ή έναν αριθμό από ομάδες. Το PIM-SMv2 χρησιμοποιεί μια μέθοδο στην οποία ένας bootstrap δρομολογητής (BSR) δημιουργεί Bootstrap μηνύματα. Αυτά τα μηνύματα χρησιμοποιούνται για την εκλογή ενός bootstrap δρομολογητή, που είναι απαραίτητος για να διαδοθούν RP πληροφορίες, ενώ μεταδίδονται με multicast στην ALL-PIM-ROUTERS ομάδα.

4.4 Συμπεράσματα

Συνοψίζοντας, θα πρέπει να τονίσουμε ότι α) το MBONE δεν χρησιμοποιείται πλέον αφού νέες, περισσότερο αποδοτικές, τοπολογίες έχουν αναπτυχθεί, β) τα σημαντικότερα εσωτερικά (intra-domain) multicast πρωτόκολλα είναι το PIM-DM και PIM-SM.

Για την υλοποίηση της τεχνολογίας στο δίκτυο “Αριάδνη” χρησιμοποιούμε, σε δρομολογητές που τρέχουν IOS της CISCO, το PIM-SM επειδή πρόκειται για μικρή τοπολογία με λίγους αποδέκτες. Εξάλλου, για τον ίδιο λόγο έχουμε ορίσει ένα static RP.

Πηγές 4ου Κεφαλαίου

1. Cisco PDF. http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_2/pimv2.htm
2. http://www.nortelnetworks.com/products/02/papers/3584.html
3. Intra and Inter domain Multicast routing Protocols: Asarvey and Taxonomy. http://www.comsoc.org/livepubs/surveys/public/1q00issue/ramalho.html
4. White Paper. http://www.microsoft.com/windows2000/docs/intrdomain.doc
5. Παρουσίασης της Cisco. ftp://ftp-eng.cisco.com/ipmulticast/training/Module3.pdf
6. Παρουσίαση της Cisco. ftp://ftp-eng.cisco.com/ipmulticast/training/Module5.pdf
7. http://www.nanog.org/mtg-9806/ppt/davemeyer/
8. White Paper. http://www.microsoft.com/windows2000/docs/pimsm2.doc
9. http://cosmos.kaist.ac.kr/salab/activity/papers/iel_cgi.pdf
10. RFC 2117: Protocol Independent Multicast-Sparse Mode (PIM-SM)
11. RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM-SM)
12. draft: Bootstrap Router (BSR) Mechanism for PIM Sparse Mode
13. draft: Protocol Independent Multicast - Sparse Mode (PIM-SM)

ΚΕΦΑΛΑΙΟ 5^{Ο}: INTER-DOMAIN MULTICASTING

5.1 Εισαγωγή

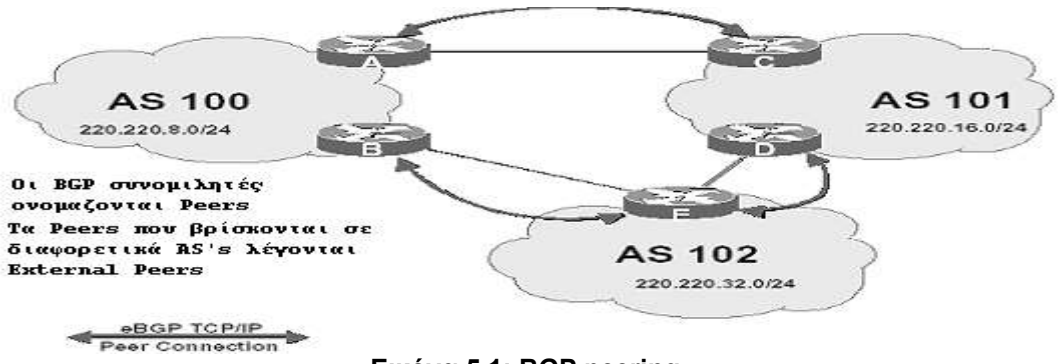
Ενώ η Intra-domain multicast δρομολόγηση έχει εδραιωθεί με το Protocol Independent Multicast-Sparse Mode (PIM-SM), η inter-domain multicast δρομολόγηση είναι ένα καυτό θέμα για τους διαχειριστές των παροχέων υπηρεσιών internet. Το επίκεντρο των προσπαθειών έχει μετατοπιστεί από τη διαχείριση των IP multicast υπηρεσιών μέσα σε ένα δίκτυο παροχής υπηρεσιών (service provider) προς την εύρεση του τρόπου με τον οποίο οι υπηρεσίες μπορούν να μοιρασθούν και να διανεμηθούν μεταξύ των providers (AS/domain). Προς την κατεύθυνση αυτή μείζον θέμα προκύπτει η επίλυση των εξής προβλημάτων:

- Διαχείριση διαφορετικών τοπολογιών και/ή πολιτικών για unicast και multicast υπηρεσίες.
- Αποφυγή εξαρτήσεων από τρίτους, δηλαδή οι providers δε θα πρέπει να βασίζονται σε rendezvous point (RP) που βρίσκεται εκτός του domain τους. (Αυτό βέβαια θα συμβεί με την προϋπόθεση ότι το PIM-SM είναι το εσωτερικό πρωτόκολλο).
- Τοποθέτηση του RP σε σημείο που εξυπηρετεί τις ανάγκες του domain στο οποίο βρίσκεται και όχι αναγκαστικά όπου διευκολύνει τη σύνδεση με άλλο domain.

Σε αυτό το κεφάλαιο θα αναλύσουμε το Multiprotocol Border Gateway Protocol (MBGP) και το Multicast Source Discovery Protocol (MSDP), τα οποία μαζί με το PIM-SM σαν intra-domain multicast πρωτόκολλο δρομολόγησης έχουν δώσει μια αρκετά επιτυχή λύση σε σχέση με τα αναφερθέντα προβλήματα. Πριν από αυτό θα κάνουμε μια μικρή αναφορά στο BGP, που θα μας βοηθήσει να εξηγήσουμε το MBGP.

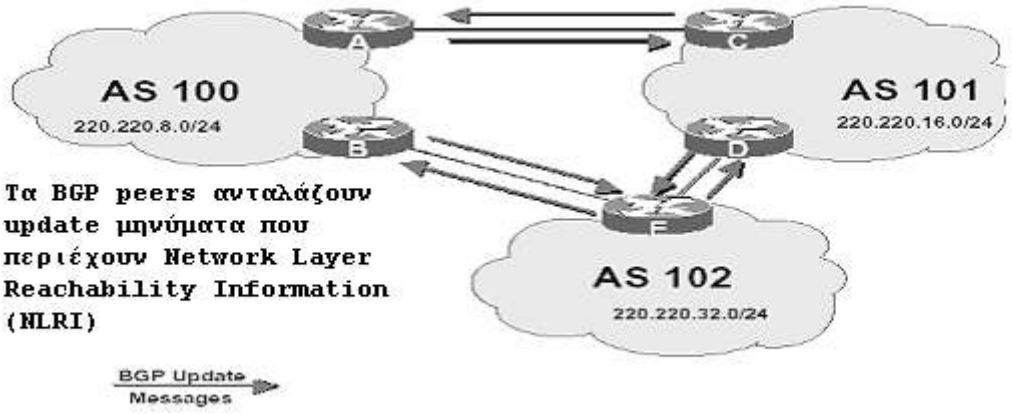
5.2 Βασικές Έννοιες του Border Gateway Protocol (BGP)

Το Border Gateway Protocol (BGP) είναι ένα πρωτόκολλο δρομολόγησης που χρησιμοποιείται από τους εξωτερικούς δρομολογητές των αυτόνομων συστημάτων (AS), με σκοπό την ανταλλαγή πληροφοριών δρομολόγησης για τα δίκτυα που δέχεται/μπορεί να δρομολογήσει ο καθένας. Οι δρομολογητές που ανταλλάσσουν μεταξύ τους BGP μηνύματα λέγονται *peers*. Δύο BGP peers που βρίσκονται σε διαφορετικά AS's λέγονται *external peers* (εικόνα 5.1).



Εικόνα 5.1: BGP peering

Για να δημιουργηθεί ένα external BGP peering πρέπει οι δρομολογητές να έχουν τουλάχιστον από ένα interface σε κοινό δίκτυο (LAN ή WAN). Οι BGP peers ανταλλάσσουν update μηνύματα (εικόνα 5.2) που περιέχουν πληροφορίες επίπεδου δικτύου για την ύπαρξη διαδρομής προς άλλα δίκτυα (Network Layer Reachability Information-NLRI) και έτσι δημιουργούνται και ανανεώνονται οι πίνακες δρομολόγησης και οι βάσεις πληροφοριών δρομολόγησης (Routing Information Base-RIB). Ένας εξωτερικός BGP peer ενός αυτόνομου συστήματος (ή μιας ομάδας από αυτόνομα συστήματα) πρέπει να έχει την ικανότητα να δημιουργεί ένα συνολικό (aggregate) δρόμο για μια ομάδα από διευθύνσεις προορισμού για τις οποίες έχει το διαχειριστικό έλεγχο, ακόμα και όταν δεν είναι όλες ταυτόχρονα προσβάσιμες. Με αυτό τον τρόπο μειώνεται το μέγεθος της πληροφορίας δρομολόγησης και η κατανάλωση μνήμης στους δρομολογητές[2] επιταχύνοντας ταυτόχρονα και την διαδικασία της δρομολόγησης. Το BGP προωθεί πληροφορίες δρομολόγησης που περιέχουν διαδρομές προς AS ανάλογα με τις πολιτικές που ο κάθε διαχειριστής καθορίζει.



Εικόνα 5.2

Αρκετή από την κίνηση που περνάει μέσα από ένα Αυτόνομο Σύστημα δημιουργείται ή τερματίζεται μέσα σε αυτό (όταν σε ένα πακέτο η IP διεύθυνση της πηγής ή IP διεύθυνση προορισμού αντιστοιχούν σε μια μηχανή που ανήκει στο AS). Η κίνηση που ταιριάζει σε αυτή την περιγραφή λέγεται τοπική κίνηση (local traffic). Η κίνηση που διέρχεται από ένα AS, χωρίς να ξεκινάει ή να καταλήγει εντός αυτού λέγεται “transit traffic”.

Ανάλογα με τις κατηγορίες κίνησης που δρομολογεί ένα AS αλλά και με το πλήθος των απευθείας συνδέσεων του με το internet μπορεί να κατηγοριοποιηθεί ως:

Stub AS: είναι τα AS’s που έχουν μόνο μια απλή σύνδεση με ένα άλλο AS, και μεταφέρουν μόνο local κίνηση.

Multihomed AS: είναι τα AS’s που έχουν συνδέσεις με περισσότερα από ένα AS, αλλά αρνούνται να μεταφέρουν transit κίνηση.

Transit AS: είναι τα AS’s που έχουν συνδέσεις με περισσότερα από ένα AS, και είναι σχεδιασμένα για να μεταφέρουν και transit και local κίνηση.

[2] Το υπέρογκο μέγεθος των πινάκων δρομολόγησης αποτελεί μέχρι και σήμερα πρόβλημα στην ανάπτυξη του Internet.

Το BGP παρέχει τη δυνατότητα να δημιουργηθούν πολιτικές δρομολόγησης, που μπορεί να είναι είτε προαιρετικές είτε υποχρεωτικές. Ακόμη, μπορεί να επέμβει στην επιλογή των δρόμων (paths) που θα δημοσιεύσει ο δρομολογητής στους άλλους δρομολογητές, καθώς επίσης και στις πληροφορίες δρομολόγησης που θα δεχτεί από τους άλλους δρομολογητές. Οι πολιτικές αποφασίζονται από το διαχειριστή του δικτύου. Μερικά παραδείγματα πολιτικών που μπορούν να εφαρμοστούν σε ένα AS είναι:

1. Ένα multihomed AS μπορεί να αρνηθεί να ενεργεί σαν ένα transit AS για άλλα AS's. (το πετυχαίνει δημοσιεύοντας τους δρόμους αποκλειστικά σε προορισμούς μέσα στο AS).
2. Ένα multihomed AS μπορεί να γίνει transit AS για ένα αριθμό AS's. Σε αυτή την περίπτωση μερικά AS που είναι συνδεμένο, μπορούν να το χρησιμοποιούν σαν transit AS (το πετυχαίνει δημοσιεύοντας τις πληροφορίες δρομολόγησής του μόνο σε αυτά τα AS's).

5.3 Multiprotocol Border Gateway Protocol (MBGP)

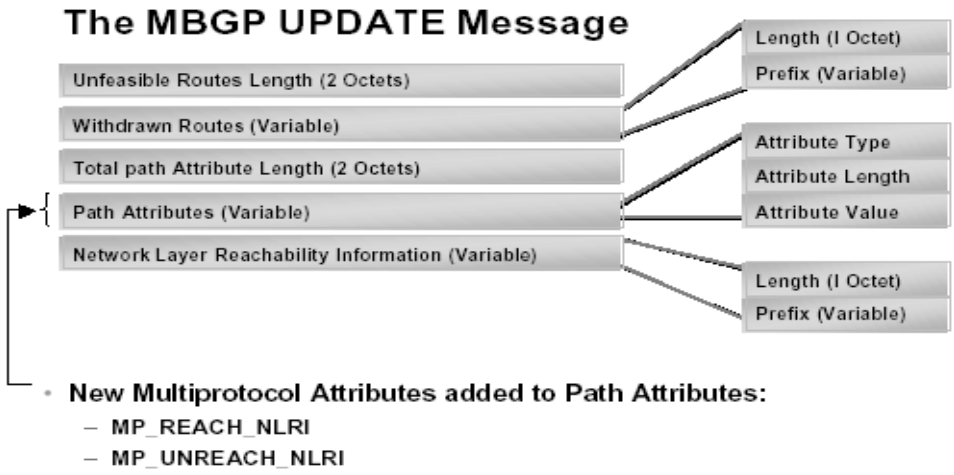
Το Multiprotocol Border Gateway Protocol (MBGP) καθορίζεται στο RFC 2283. Το MBGP είναι επέκταση του BGP, έτσι ώστε να υποστηρίζει και άλλες εκτός της IPv4 unicast δρομολόγησης, όπως π.χ την IP multicasting δρομολόγηση και την IPv6 δρομολόγηση.

Το MBGP δε δημιουργήθηκε για να αντικαταστήσει το PIM, αφού δεν αναπαράγει multicast πληροφορίες, ούτε χτίζει κανενός είδους multicast δέντρα διανομής. Ο ρόλος του είναι να διανέμει τις unicast πληροφορίες που χρησιμοποιούνται για το multicast RPF έλεγχο. Επειδή είναι επέκταση του BGP χρησιμοποιεί τους ίδιους κανόνες για την εκλογή των δρόμων επικοινωνίας.

Το BGP διατηρεί μόνο μια απλή βάση πληροφοριών δρομολόγησης (Routing Information Base-RIB) για IPv4 unicast επικοινωνία. Στη περίπτωση του MBGP, όμως, ξεχωριστές RIBs διατηρούνται για κάθε είδος πληροφορίας δρομολόγησης που ανταλλάσσεται. Έτσι, διαφορετική Unicast RIB (U-RIB) και Multicast RIB (M-RIB) διατηρείται από το MBGP. Η U-RIB περιέχει unicast πληροφορίες ουσιαστικά αυτές που είχε το BGP, ενώ η M-RIB περιέχει unicast πληροφορίες όπως και η U-RIB με τη διαφορά ότι οι πληροφορίες που αποθηκεύονται στη M-RIB χρησιμοποιούνται από το RPF για τον έλεγχο της εισερχόμενης multicast κίνησης. Για αυτό το λόγο είναι δυνατή η ύπαρξη διαφορετικών πολιτικών και τοπολογιών δρομολόγησης για unicast και multicast κίνηση.

Στην παρακάτω εικόνα εμφανίζονται τα πεδία του "update" μηνύματος του MBGP, που είναι ίδια με αυτά του BGP, με τη διαφορά ότι έχουν προστεθεί δύο νέες ιδιότητες:

- MP_REACH_NLRI
- MP_UNREACH_NLRI



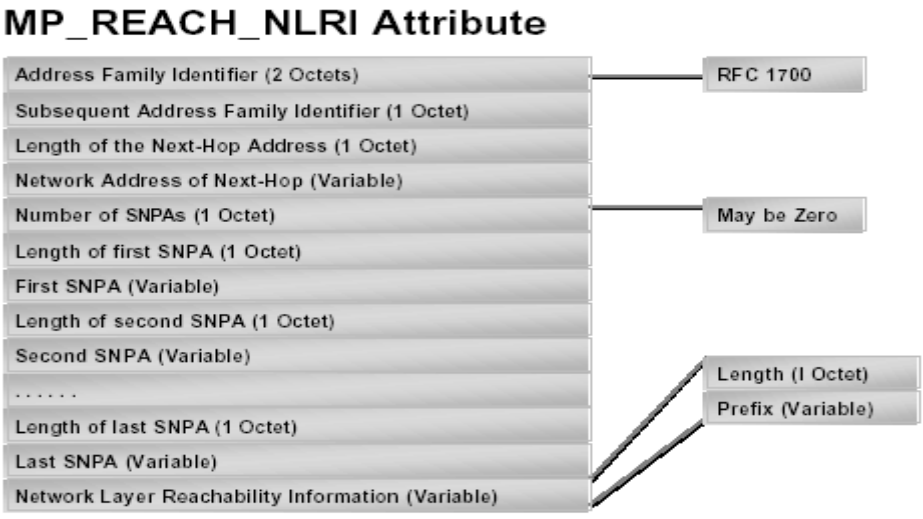
Εικόνα 5.3

Τα κύρια χαρακτηριστικά της MP_REACH_NLRI ιδιότητας είναι τα Address Family Identifier (AFI) και Sub-Address Family Identifier (Sub AFI) πεδία (εικόνα 5.4). Αυτά τα δύο πεδία καθορίζουν το είδος της πληροφορίας δρομολόγησης που μεταφέρεται μέσα στο NLRI πεδίο αυτής της ιδιότητας.

Η πληροφορία για τη διεύθυνση του επόμενου δρομολογητή (Next-Hop address) περιέχεται μέσα στο πεδίο που ακολουθεί μετά τα AFI και Sub-AFI.

Το πεδίο Address Family Information (AFI) βασίζεται στις address families που καθορίζονται από το RFC 1700, όπου AFI=1 είναι για IPv4 και AFI=2 είναι για IPv6. Το Sub-AFI πεδίο περιέχει περισσότερες πληροφορίες και εξαρτάται από το είδος της πληροφορίας δρομολόγησης που ανταλλάσσεται στο NLRI πεδίο. Για το IPv4 Address Family ισχύει:

- Αν Sub-AFI=1, τα NLRI χρησιμοποιούνται για unicast δρομολόγηση.
- Αν Sub-AFI=2, τα NLRI χρησιμοποιούνται για multicast RPF έλεγχο.
- Αν Sub-AFI=3, τα NLRI χρησιμοποιούνται και για unicast δρομολόγηση και για multicast RPF έλεγχο.



Εικόνα 5.4

Τέλος, το NLRI περιέχει πληροφορίες για το δρόμο προς το δίκτυο που θεωρείται προσβάσιμο (Εικόνα 5.3).

Συμπερασματικά, το MBGP έλυσε μέρος του inter-domain multicast προβλήματος, επιτρέποντας στα αυτόνομα συστήματα την ανταλλαγή

multicast RPF πληροφοριών μέσα στο NLRI. Η χωριστή αποθήκευση των unicast και multicast πληροφοριών επιτρέπει στην unicast και multicast κίνηση να ακολουθήσει διαφορετικούς δρόμους. Το PIM πρέπει να χρησιμοποιείται για το χτίσιμο των multicast δέντρων διανομής, για τον RPF έλεγχο και για την προώθηση της multicast κίνησης. Για intra-domain πρωτόκολλο προτιμάται το PIM-SM, γιατί επιτρέπει την χρήση του MSDP, το οποίο λύνει τα περισσότερα από τα υπόλοιπα προβλήματα της Inter-domain multicast δρομολόγησης πού έχουμε αναφέρει.

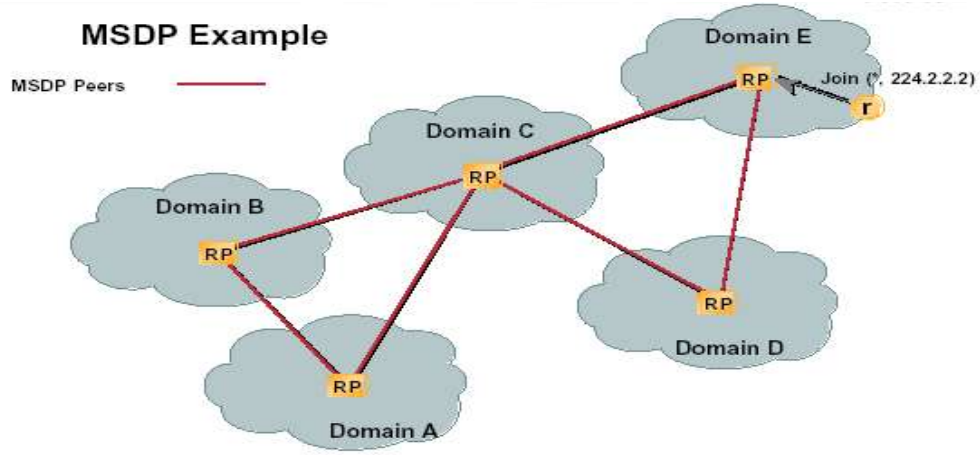
5.4 Multicast Source Discovery Protocol (MSDP)

Το MBGP, όπως είδαμε, έδωσε λύση σε κάποια προβλήματα που προέκυψαν με την ανάπτυξη της inter- domain τοπολογίας, όμως δεν έλυσε το πρόβλημα της εξάρτησης από τρίτους ή της ευελιξίας στην τοποθέτηση του RP. Έτσι, το MSDP αναπτύχθηκε ακριβώς για την αντιμετώπιση των πιο πάνω θεμάτων. Το MSDP χρησιμοποιεί inter-domain source path trees και όχι shared path trees για τη δρομολόγηση των πακέτων. Άρα τα RPs χρειάζονται μόνο το δρόμο προς τις ενεργές πηγές έξω από το δικό τους domain κι επομένως δεν υπάρχει η ανάγκη να χρησιμοποιηθεί το RP άλλου domain ή για κάποιο provider να τοποθετήσει το RP σε κάποιο συγκεκριμένο σημείο.

5.4.1 MSDP- Γενική Επισκόπηση

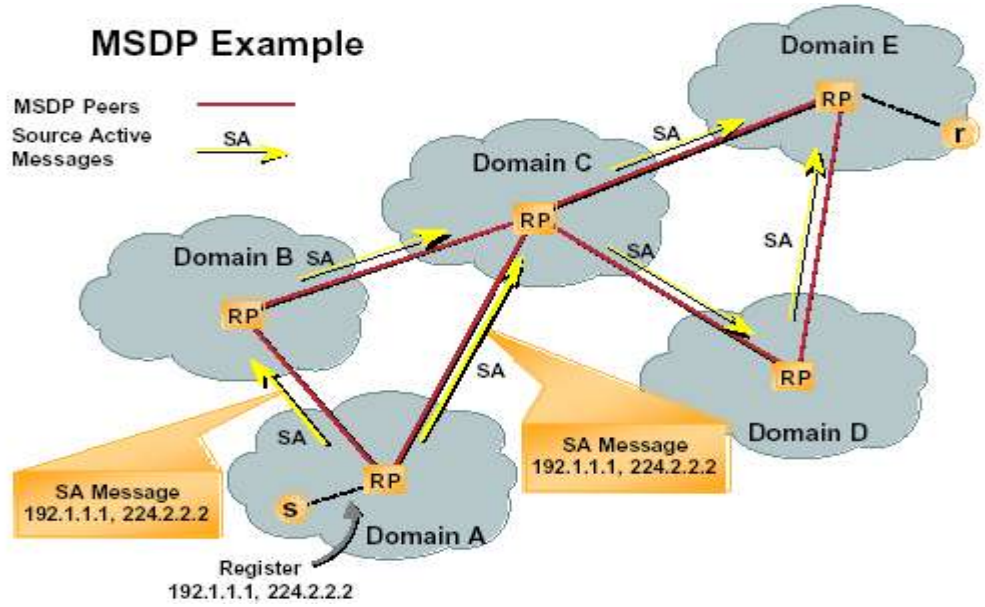
Το MSDP επιτυγχάνει την επικοινωνία των RPs που βρίσκονται σε inter-connected domains. Οπότε, το MSDP βασίζεται στην χρήση του PIM-SM σαν intra-domain multicast πρωτόκολλο δρομολόγησης. Όπως είδαμε στο κεφάλαιο 4 τα RPs γνωρίζουν όλες τις πηγές μέσα σε ένα PIM-SM domain. Άρα μπορούν να ενημερώσουν τα RPs των άλλων PIM-SM domains για την ύπαρξη ενεργής πηγής μέσα στο δικό τους τοπικό domain. Αυτό επιτυγχάνεται με την αποστολή MSDP Source Active (SA) μηνυμάτων. Επίσης, στο κεφάλαιο 4 είδαμε ότι τα RPs γνωρίζουν τους ενδιαφερόμενους αποδέκτες μέσα στο τοπικό domain. Οπότε όταν λαμβάνουν ένα SA μήνυμα που ανακοινώνει ότι μια ενεργή πηγή σε άλλο domain στέλνει multicast δεδομένα στην ομάδα που συμμετέχουν οι τοπικοί αποδέκτες, τότε τα RPs μπορούν να στείλουν ένα μήνυμα σύνδεσης πίσω στην πηγή που βρίσκεται εκτός του domain τους.

Τα RPs, μέσω του MSDP, περιοδικά δημιουργούν SA μηνύματα για τις πηγές που είναι ενεργές μέσα στο δικό τους τοπικό domain. Αυτά τα SA μηνύματα στέλνονται σε όλα τα ενεργά MSDP peers. Μόλις ένας MSDP δρομολογητής λάβει ένα SA μήνυμα από ένα από τα peers του, αφού κάνει ένα RPF έλεγχο, το προωθεί σε όλα τα άλλα peers. Ο δρομολογητής πραγματοποιεί τον RPF έλεγχο (χρησιμοποιώντας τη διεύθυνση του αρχικού RP) για να βεβαιωθεί ότι έφτασε από το σωστό AS-PATH. Μόνο αν ο έλεγχος είναι επιτυχής, το SA μήνυμα διασκορπίζεται (flooded) στα peers, κάτι που αποτρέπει τα routing loops. Η λειτουργία του MSDP θα γίνει καλύτερα κατανοητή με το παρακάτω παράδειγμα:



Εικόνα 5.5

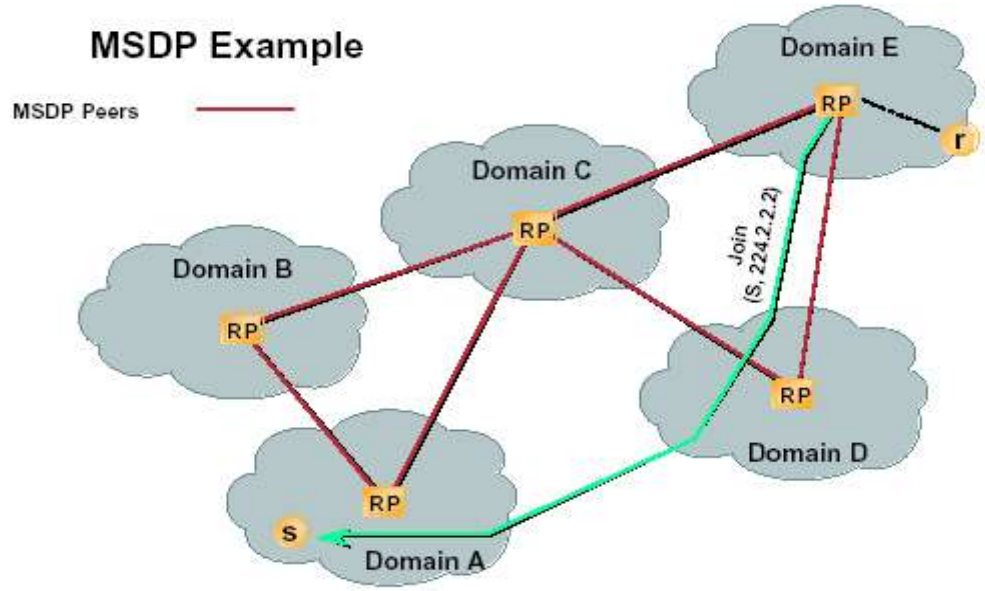
Στην εικόνα 5.5, έχουμε πέντε PIM-SM domains που το καθένα έχει ένα RP το οποίο τρέχει MSDP. Οι γραμμές μεταξύ των RPs δείχνουν την TCP σύνδεση των MSDP peers. Υποθέτουμε ότι ένας αποδέκτης μέσα στο domain E συνδέεται στη multicast ομάδα 224.2.2.2, δηλαδή προκαλεί τον DR του να στείλει (*,G) μήνυμα σύνδεσης στο RP. Αυτό, όπως είναι γνωστό, χτίζει ένα “κλαδί” στο shared δέντρο από το RP μέσα στο domain E μέχρι τον leaf δρομολογητή. Όταν μια πηγή γίνει ενεργή στο domain A (εικόνα 5.6), ο first-hop δρομολογητής στέλνει ένα PIM μήνυμα εγγραφής (PIM Register message) στο RP. Έτσι ενημερώνεται το RP του domain A ότι μια πηγή είναι ενεργή σε αυτό. Το RP (MSDP) δημιουργεί (S,G) SA μηνύματα για αυτή την πηγή και τα στέλνει στα MSDP peers των domain B και C. Θα συνεχίσει να στέλνει τα μηνύματα περιοδικά, όσο η πηγή παραμένει ενεργή. Όταν τα RP στα domains B και C λάβουν τα SA μηνύματα, κάνουν RPF έλεγχο και τα προωθούν στα επόμενα peers D και E (εικόνα 5.6).



Εικόνα 5.6

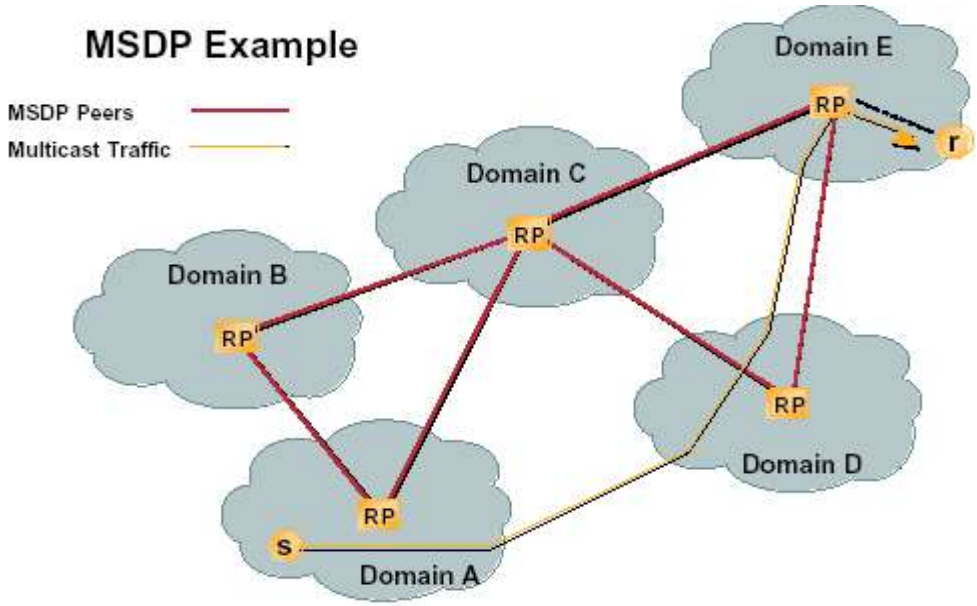
Μόλις το SA μήνυμα φτάσει στο RP του domain E, αυτό βλέπει ότι έχει ενδιαφερόμενους αποδέκτες για την ομάδα 224.2.2.2 πάνω στο shared δέντρο και απαντάει στο SA μήνυμα στέλνοντας ένα (S,G) μήνυμα (ΠΙΜ_ΣΜ

Ξοιν)σύνδεσης πίσω στην πηγή. Το (S,G) μήνυμα σύνδεσης θα ακολουθήσει τον λογικότερο inter-domain δρόμο από το RP στην πηγή, ο οποίος δεν είναι κατά ανάγκη ίδιος με αυτόν που χρησιμοποιήθηκε από τις MSDP συνδέσεις (εικόνα 5.7).



Εικόνα 5.7

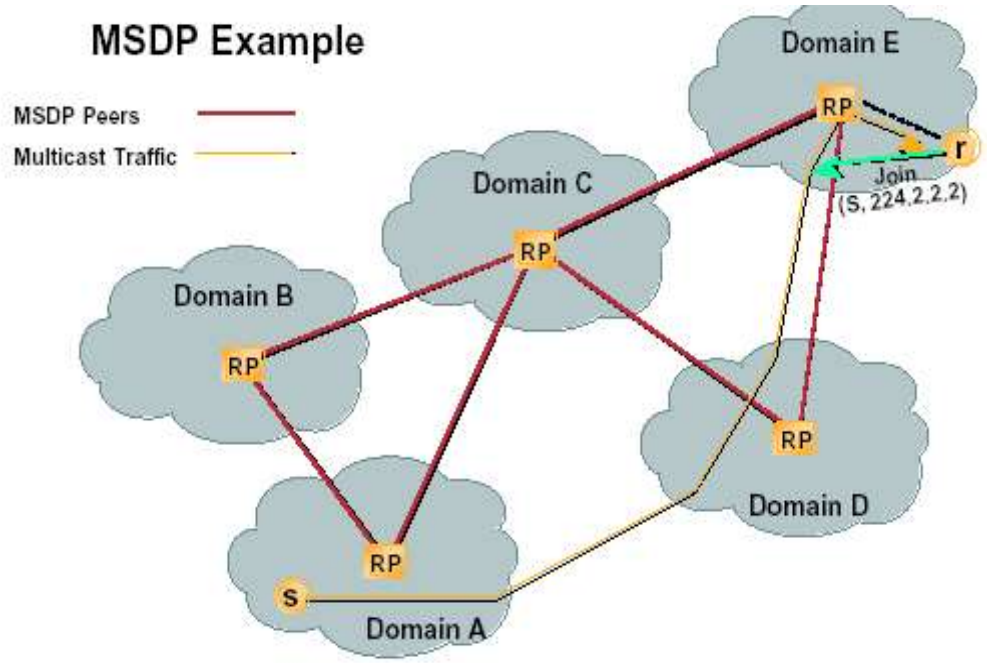
Μόλις το (S,G) μήνυμα σύνδεσης φτάσει στον first-hop δρομολογητή (S) στο domain A, η (S,G) κίνηση ξεκινάει προς το RP του domain E μέσω του source path δέντρου, που δημιουργήθηκε από τα μηνύματα σύνδεσης που μεταδόθηκαν από το leaf δρομολογητή στο first-hop δρομολογητή.



Εικόνα 5.8

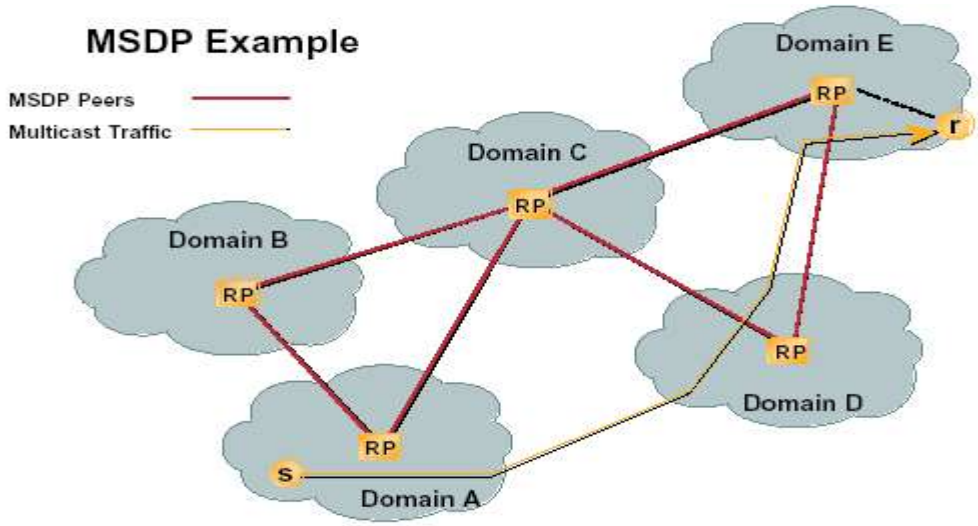
Όταν η (S,G) κίνηση φτάσει στον last-hop δρομολογητή (R) στο domain E, αυτός μπορεί αν θέλει να στείλει ένα (S,G) μήνυμα σύνδεσης στην

πηγή με σκοπό να αποφύγει το πέρασμα της κίνησης από το RP του domain E (εικόνα 5.9).



Εικόνα 5.9

Τελικά η (S,G) κίνηση φτάνει στον last-hop δρομολογητή μέσω του Source δέντρου χωρίς να περνάει από το RP του domain E (εικόνα 5.10).



Εικόνα 5.10

Από το παραπάνω παράδειγμα φαίνεται ότι οι απαιτήσεις που είχαν οι ISPs έχουν καλυφθεί με συνεργασία των PIM-SM, MBGP, MSDP. Χρειαζόταν ένα σαφές πρωτόκολλο σύνδεσης. Την απαίτηση αυτή κάλυψε το PIM-SM. Ακόμη, έπρεπε να χρησιμοποιηθεί το υπάρχον unicast μοντέλο λειτουργίας και η λύση ήρθε με την επέκταση του BGP σε MBGP (BGP+4), γεγονός που επέτρεψε στο διαχειριστή να ρυθμίζει και να διαχειρίζεται και τη unicast και τη multicast κίνηση χρησιμοποιώντας τα ήδη υπάρχοντα εργαλεία. Επιπλέον οι

ISPs δεν είναι πια υποχρεωμένοι να μοιράζονται τα RPs με τους ανταγωνιστές τους, αφού το MSDP επιτρέπει σε κάθε domain να έχει το δικό του RP για κάθε multicast ομάδα. Τέλος, τα RPs μπορούν να τοποθετηθούν οπουδήποτε μέσα σε ένα domain, αφού ενώνονται μέσω MSDP με τα άλλα RPs στα άλλα domain.

5.4.2 MSDP Peers

Το RP ενός domain, με το MSDP σαν inter-domain πρωτόκολλο, δημιουργεί peers (MSDP peers) με τα RPs των άλλων domains μέσω TCP σύνδεσης στην πόρτα 639. Το peer με τη μικρότερη IP διεύθυνση πρέπει να ξεκινήσει την TCP σύνδεση, ενώ το peer με τη μεγαλύτερη IP διεύθυνση περιμένει να δεχτεί την αίτηση σύνδεσης. Τα peer στέλνουν μηνύματα κάθε 60 δευτερόλεπτα για να κρατήσουν ζωντανή την σύνδεση (keepalive). Αν για 75 δευτερόλεπτα δεν ληφθούν πακέτα ή keepalives μηνύματα, η σύνδεση διακόπτεται.

Οι δρομολογητές που τρέχουν MSDP είναι απαιτούμενο να τρέχουν και MBGP αφού ο RPF έλεγχος για τα SA μηνύματα χρησιμοποιεί την AS-PATH πληροφορία που περιέχεται στα M-RIB και U-RIB του MBGP.

5.4.3 MSDP Μηνύματα

Υπάρχουν τέσσερα βασικά είδη MSDP μηνυμάτων, το καθένα από τα οποία είναι κωδικοποιημένο σε TLV[3] διαμόρφωση:

- Keepalives
- Source Active (SA)
- Source Active Request (SA-Req)
- Source Active Response (SA)

Τα Source Active (SA) μηνύματα χρησιμοποιούνται για τη δημοσίευση των ενεργών πηγών μέσα σε ένα domain. Επίσης, μπορεί να περιέχουν ένα αρχικό multicast πακέτο που έχει σταλεί από την πηγή, με σκοπό να βοηθήσει στην επίλυση προβλημάτων που δημιουργούνται, όπως είναι το bursty source[4] και ο χαμηλός ρυθμός μετάδοσης στις ανακοινώσεις του SDR. Ακόμα, τα SA μηνύματα περιέχουν την IP διεύθυνση του αρχικού RP, ένα ή περισσότερα (S,G) ζευγάρια για δημοσίευση και, τέλος, ίσως ενθυλακωμένα πακέτα δεδομένων.

Τα Source Active Request μηνύματα χρησιμοποιούνται για να ζητηθεί μια λίστα από ενεργές πηγές για μια συγκεκριμένη multicast ομάδα. Αυτά τα μηνύματα στέλνονται σε ένα δρομολογητή που λειτουργεί και ως MSDP SA Cache Server και αποθηκεύει μια λίστα από ενεργά (S,G) ζευγάρια. Έτσι, μπορεί να μειωθεί η καθυστέρηση σε μια σύνδεση, ζητώντας ο RP δρομολογητής τη λίστα με τις ενεργές πηγές για το group, παρά να περιμένει 60 δευτερόλεπτα για όλες τις ενεργές πηγές να δημοσιευτούν ξανά από το αρχικό RP.

Τα Source Active Response μηνύματα στέλνονται από τον MSDP SA Cache Server ως απάντηση σε ένα SA-Req μήνυμα. Αυτά περιέχουν την IP

[3] Αναφορά TLV
[4] bursty source

διεύθυνση του αρχικού RP, καθώς επίσης και ένα ή περισσότερα (S,G) ζευγάρια των ενεργών πηγών που βρίσκονται μέσα στο domain του RP.

Τα SA μηνύματα θα πρέπει να γίνονται δεκτά μόνο από το RPF interface του MSDP peer. Τα ίδια SA μηνύματα πρέπει να απορρίπτονται μέσω RPF ελέγχου, γιατί διαφορετικά θα δημιουργούνται loops. Για να γίνει RPF έλεγχος για ένα εισερχόμενο SA μήνυμα, θα πρέπει να είναι γνωστή η MSDP τοπολογία. Όμως το MSDP δε διανέμει πληροφορίες τοπολογίας κι επομένως εδώ δημιουργείται σχετικό πρόβλημα. Η λύση δίνεται μέσω της χρησιμοποίησης των MBGP δεδομένων δρομολόγησης, άρα η MSDP τοπολογία πρέπει να έχει την ίδια γενική τοπολογία με το BGP.

Για να προωθήσει ένας δρομολογητής ένα SA μήνυμα ακολουθεί τα παρακάτω βήματα:

- Αρχικά, χρησιμοποιώντας τη διεύθυνση της ομάδας “G” από το ζευγάρι (S,G) του SA μηνύματος, βρίσκει την αντίστοιχη (*,G) καταχώρηση στον multicast πίνακα δρομολόγησής του.
- Αν η (*,G) καταχώρηση βρεθεί και η λίστα με τα εξερχόμενα interfaces δεν είναι Null, τότε υπάρχουν ενεργοί αποδέκτες μέσα στο PIM-SM domain για την πηγή που δημοσιεύεται στο SA μήνυμα. Τότε φτιάχνει μια (S,G) καταχώρηση για την δημοσιευμένη πηγή.
- Στη συνέχεια, διασκορπίζει το SA μήνυμα σε όλα τα άλλα MSDP peers εκτός από αυτό από όπου έγινε δεκτό.

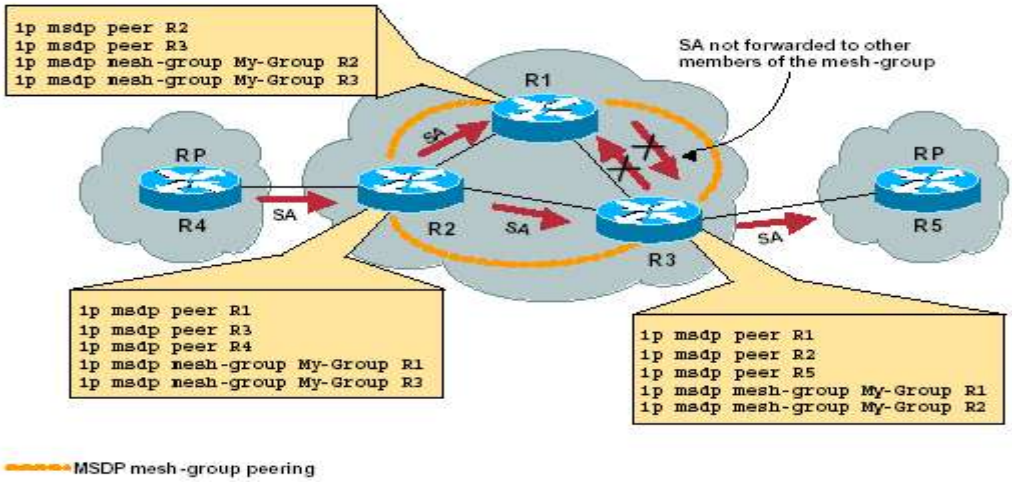
Ένα επιπλέον σημαντικό σημείο για τα SA μηνύματα είναι ότι μπορεί να φιλτραριστούν, έτσι ώστε να γίνονται δεκτά ή όχι από τους MSDP δρομολογητές. Τα φίλτρα ίσως χρησιμοποιούνται για τα εισερχόμενα ή εξερχόμενα SA μηνύματα και βασίζονται στα (S,G) ζευγάρια που καθορίζονται σε μια λίστα πρόσβασης (access list).

5.4.4 MSDP Mesh-Groups

Ένα MSDP peer μπορεί να ρυθμιστεί προκειμένου να ανήκει σε μια ομάδα από MSDP peers, γεγονός που έχει διπλό αποτέλεσμα. Πρώτον, μειώνει το SA flooding. Αυτό συμβαίνει γιατί όταν ένα MSDP peer της ομάδας δεχτεί ένα SA μήνυμα από ένα άλλο MSDP peer που ανήκει στην ίδια ομάδα (mesh-group), θεωρεί ότι αυτό το SA μήνυμα έχει σταλεί σε όλα τα άλλα MSDP peers που ανήκουν στην ομάδα. Οπότε, δεν είναι απαραίτητο για το peer που δέχτηκε το SA μήνυμα να το διασκορπίσει στα άλλα MSDP peers που ανήκουν στην ομάδα.

Επίσης, ένα δεύτερο αποτέλεσμα της συμμετοχής ενός MSDP peer σε ένα MSDP mesh-group είναι ότι τα MSDP mesh-groups μπορούν να χρησιμοποιηθούν για να μειώσουν την ανάγκη ενός δρομολογητή να τρέχει MBGP για να κάνει RPF έλεγχο. Αυτό συμβαίνει, γιατί τα SA μηνύματα ποτέ δεν διασκορπίζονται στα άλλα MSDP peers μέσα σε ένα mesh-group, οπότε δεν είναι απαραίτητο να γίνεται RPF έλεγχος.

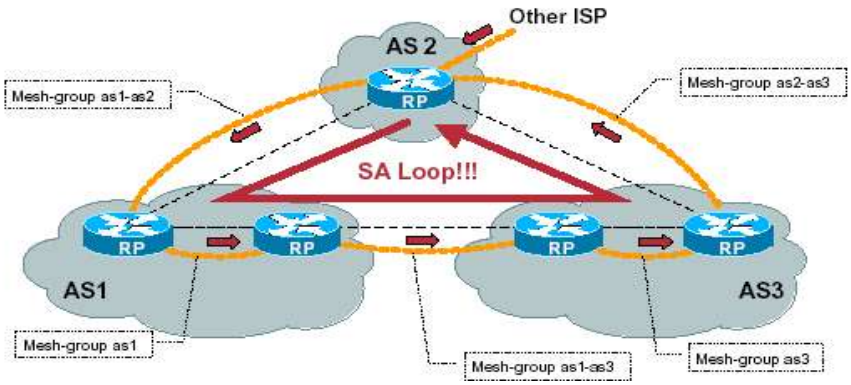
Η εικόνα (5.11) δείχνει παραστατικά την λειτουργία ενός MSDP mesh-group.



Εικόνα 5.11

Στο παράδειγμα, οι δρομολογητές R1,R2 και R3 είναι όλοι ρυθμισμένοι να είναι μέλη του ίδιου MSDP mesh-group. Επίσης, ο δρομολογητής R1 έχει MSDP σύνδεση με το δρομολογητή R4 και ο δρομολογητής R3 με το δρομολογητή R5. Οι R4 και R5 δεν ανήκουν στο mesh-group. Υποθέτουμε ότι ο R4 δημιουργεί ένα SA μήνυμα για μια πηγή που υπάρχει στο δικό του PIM-SM domain. Το μήνυμα στέλνεται στον R2, όπως φαίνεται στο σχήμα. Όταν ο R2 παραλάβει το μήνυμα, πρέπει να πραγματοποιήσει ένα RPF έλεγχο, γιατί το μήνυμα το έλαβε από ένα MSDP peer που δεν ανήκει στο mesh-group. Στο συγκεκριμένο παράδειγμα ο έλεγχος είναι επιτυχής, οπότε ο δρομολογητής R2 διασκορπίζει το SA μήνυμα σε όλα τα μέλη του mesh-group. Όταν οι R1 και R3 λάβουν το SA μήνυμα από τον R2, δεν είναι υποχρεωμένοι να πραγματοποιήσουν RPF έλεγχο, ούτε να το διασκορπίσουν μεταξύ τους, αφού και οι δύο είναι μέλη του mesh-group. Γνωρίζουν ότι τα άλλα μέλη θα έχουν λάβει το μήνυμα από τον R2, οπότε δεν το προωθούν. Για αυτό το λόγο, όλα τα μέλη πρέπει να είναι συνδεδεμένα μεταξύ τους, δημιουργώντας έτσι ένα πλέγμα (mesh). Τέλος, ο R3 διασκορπίζει το SA μήνυμα σε όλα τα MSDP peers που δεν είναι μέλη του mesh-group. Στο παράδειγμα, το SA διασκορπίζεται στον R5 για να συνεχιστεί η ροή μέχρι να φτάσει στο RP.

Στα mesh-groups οι ρυθμίσεις που δίνονται από κάθε διαχειριστή των δρομολογητών πρέπει να γίνονται με προσοχή, ώστε να αποφεύγονται τα routing loops, όπως αυτό της εικόνας 5.12.



Εικόνα 5.12

5.4.5 MSDP SA Caching

Όταν ένας MSDP δρομολογητής λάβει ένα SA μήνυμα, το αποθηκεύει σε μία SA cache. Αφού το προωθήσει στους MSDP γειτονικούς δρομολογητές, ενεργοποιεί ένα SA-expire χρονόμετρο διάρκειας 6 λεπτών, για την (S,G) καταχώρηση που έχει δημιουργήσει στον πίνακα δρομολόγησής του. Κάθε φορά που ένα (S,G) SA μήνυμα λαμβάνεται, το χρονόμετρο αρχίζει από την αρχή. Αν τα 6 λεπτά τελειώσουν, τότε η καταχώρηση διαγράφεται από το SA cache.

Όταν ένας δρομολογητής ρυθμιστεί να κάνει SA caching, αρχίζει να αποθηκεύει όλα τα (S,G) ζευγάρια που λαμβάνονται με τα SA μηνύματα. Αυτό μειώνει την αργοπορία σύνδεσης, αφού ο RP διατηρεί μια λίστα με όλες τις ενεργές πηγές. Άρα, όταν ο πρώτος αποδέκτης συνδεθεί στη multicast ομάδα, το RP δεν είναι υποχρεωμένο να περιμένει 60 δευτερόλεπτα για το επόμενο SA μήνυμα, πριν στείλει το (S,G) μήνυμα σύνδεσης.

Ένα ακόμα πλεονέκτημα του SA caching είναι ότι ο διαχειριστής του δρομολογητή έχει την δυνατότητα να δει τα περιεχόμενα της SA cache, οπότε μπορεί να ενημερωθεί για το ποιες πηγές είναι ενεργές στο internet, σε ποιο αυτόνομο σύστημα ανήκουν και από ποιο RP έχουν δημοσιευτεί.

Επίσης, επειδή τα SA’s δημοσιεύονται περιοδικά από την cache, και όχι από κάποιο γειτονικό δρομολογητή, μειώνεται η κίνηση στο δίκτυο, οι ουρές, δηλαδή, που πολλές φορές έχουν ως αποτέλεσμα να χάνονται οι TCP συνδέσεις μεταξύ των peers και γενικότερα να δημιουργείται αστάθεια στο MSDP.

Εξάλλου, η επίπτωση που προκαλεί το SA caching στη μνήμη των περισσοτέρων RPs είναι γενικά πολύ μικρή. Το τελευταίο draft για τον καθορισμό του MSDP από τον IETF απαιτεί τη χρησιμοποίηση του SA caching.

5.5 Πηγές 5ου Κεφαλαίου

1. Cisco PDF. http://www.cisco.com/warp/public/cc/pd/iosw/tech/ipmu_ov.pdf
2. Indrodaction to IP Multicast. http://www.nanog.org/mtg-9806/ppt/davemeyer/
3. http://www.dante.net/nep/GEANT-MULTICAST/
4. GEANT Multicast design MSDP&RP http://www.dante.net/nep/GEANT-MULTICAST/presentations/Nep-2001-129v7_multicast_msdp_rp_design.pdf
5. http://www.grnet.gr/mbone/
6. http://www.dante.net/mbone/guides/mdebug.html
7. http://www.dante.net/mbone/nop/tale/index.html
8. http://www.dante.net/mbone/guides/mmon/index.html
9. http://weathermap.geant.net/msdpmon/
10. http://taksometro.geant.net/GEANT/taksometro-topology.html
11. RFC2283 Multiprotocol Extensions for BGP-4 (obsoloted by 2858)
12. RFC2858 Multiprotocol Extensions for BGP-4 (PROPOSED STANDARD)
13. ftp://ftp-eng.cisco.com/ipmulticast/training/Module11.pdf
14. ftp://ftp-eng.cisco.com/ipmulticast/training/Module10.pdf
15. http://www.pearsonptg.com/samplechapter/0201746123.pdf
16. http://www.microsoft.com/windows2000/docs/intrdomain.doc
17. http://macross.dynodns.net/idr/multicast_evolution.pdf
18. http://www.comsoc.org/livepubs/surveys/public/1q00issue/ramalho.html
19. http://www.nossdav.org/2000/papers/28.pdf

Κεφάλαιο 6ο: Διαμόρφωση Δρομολογητών Για INTER-DOMAIN IP Multicast ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΜΕ ΤΟ ΕΔΕΤ.

6.1 Εισαγωγή

Μέχρι τώρα έχουμε αναφερθεί στις λειτουργίες των πρωτοκόλλων για intra-domain και inter-domain multicast, καθώς επίσης και στα software εργαλεία που χρησιμοποιούνται σε ένα σταθμό εργασίας για τη χρησιμοποίηση του IP multicast. Σε αυτό το κεφάλαιο θα περιγράψουμε τη διαμόρφωση που πρέπει γίνει στους IP multicast δρομολογητές. Θα αναφερθούμε σε ρυθμίσεις για Cisco δρομολογητές που τρέχουν λειτουργικό IOS. Οι ρυθμίσεις των πρωτοκόλλων που περιγράφονται, ενεργοποιήθηκαν στους δρομολογητές για την υλοποίηση της multicast υπηρεσίας εντός του δικτύου "Αριάδνη" και για την συνεργασία με την παρεχόμενη multicast υπηρεσία από το ΕΔΕΤ (εικόνα 6.1) . Συγκεκριμένα για την διασύνδεση με το ΕΔΕΤ είναι δυνατή η επιλογή από δύο διαφορετικές αρχιτεκτονικές multicasting :

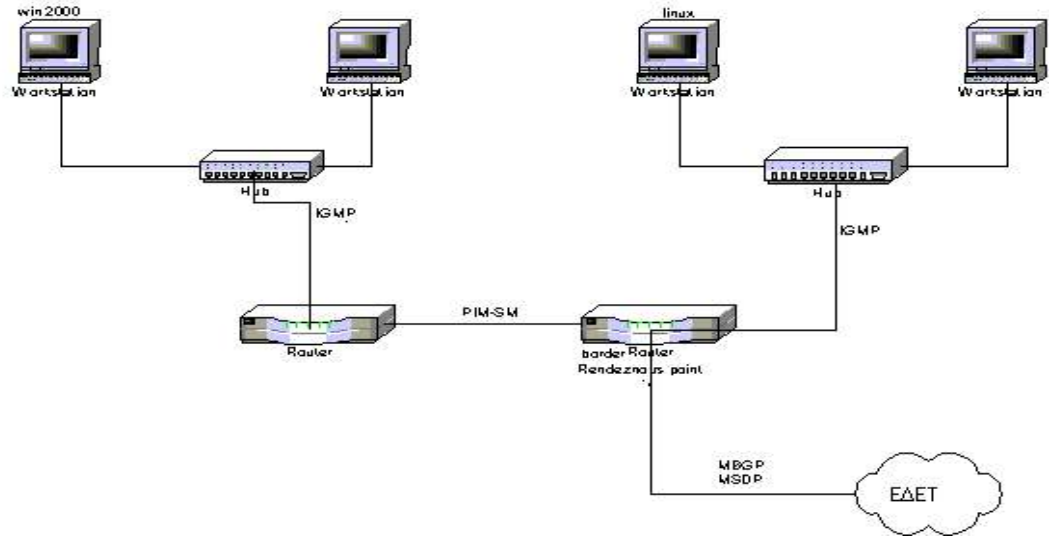
α) Inter-Domain Multicasting και

β) Απλή χρήση του RP που διαθέτει το ΕΔΕΤ.

Η αρχιτεκτονική α είναι η ποιο ολοκληρωμένη και παρέχει την μεγαλύτερη ευελιξία και για αυτό και επιλέχθηκε για την υλοποίηση.

Τα πρωτόκολλα που ενεργοποιήθηκαν είναι:

- Το Internet Group Management Protocol (IGMP) που χρησιμοποιείται μεταξύ των hosts πάνω σε ένα LAN και των δρομολογητών πάνω στο LAN και ελέγχει σε ποιες multicast ομάδες οι hosts είναι μέλη.
- Το Protocol – Independent Multicast (PIM) σε sparse και dense mode, που χρησιμοποιείται μεταξύ των δρομολογητών, έτσι ώστε να ελέγχουν ποια multicast πακέτα να προωθήσουν ο ένας στον άλλο και στα απευθείας συνδεδεμένα LANs μέσα στο ίδιο AS (Autonomous System).
- Το Multiprotocol BGP extension for ip Multicast για επικοινωνία των δρομολογητών σε διαφορετικά ASs.
- Το Multicast Source Discovery Protocol (MSDP) που χρησιμοποιείται από τα Rendezvous Points (RPs), τα οποία με σύνδεση TCP ανακαλύπτουν multicast πηγές σε άλλα domains.



Εικόνα 6.1

6.2 Διαμόρφωση Εσωτερικού Δρομολογητή

Για να προωθούν οι δρομολογητές multicast πακέτα, ενεργοποιούνται τα απαιτούμενα πρωτόκολλα και ρυθμίζονται οι αντίστοιχοι παράμετροι. Οι ρυθμίσεις που πρέπει ή μπορούν να γίνουν είναι:

- Ενεργοποίηση του IP Multicast Routing (απαιτείται).
- Ενεργοποίηση του PIM σε ένα interface (απαιτείται)
- Ρύθμιση του RP (απαιτείται)
- Ρύθμιση ενός δρομολογητή να είναι μέλος μιας ομάδας. (για debugging)
- Έλεγχος της πρόσβασης στα IP Multicast groups.
- Ρύθμιση του δρομολογητή σαν ένα στατικά συνδεμένο μέλος.
- Ενεργοποίηση του SAP Listener Support. (προτείνεται)
- Οριοθέτηση του χρόνου ύπαρξης μιας SAP Cache εισόδου. (προτείνεται)

6.2.1 Ενεργοποίηση του IP Multicast Routing

Αρχικά ενεργοποιούνται οι δρομολογητές προκειμένου να υποστηρίζουν IP multicasting. Για να γίνει, αυτό χρησιμοποιείται η παρακάτω εντολή σε global configuration mode:

router(config)# ip multicast-routing

6.2.2 Ενεργοποίηση του PIM σε ένα interface

Το επόμενο βήμα είναι η ενεργοποίηση του IGMP στους leaf δρομολογητές. Όταν όμως, ενεργοποιηθεί το PIM σε ένα interface, ενεργοποιείται και η IGMP λειτουργία σε αυτό το interface. Ένα PIM interface μπορεί να διαμορφωθεί να λειτουργεί σε dense mode, sparse mode ή sparse-dense mode. Το mode καθορίζει τον τρόπο με τον οποίο ο δρομολογητής χειρίζεται τον πίνακα δρομολόγησής του και τον τρόπο με τον οποίο προωθεί τα multicast πακέτα που δέχεται. Πρέπει να ενεργοποιηθεί ένα τουλάχιστον PIM interface σε ένα από τα παραπάνω modes, για να υπάρξει multicast δρομολόγηση.

Τα dense-mode interfaces πάντα προστίθενται στο multicast πίνακα δρομολόγησης, ενώ τα sparse-mode interfaces προστίθενται μόνο όταν λαμβάνοντα join μηνύματα από downstream δρομολογητές, ή όταν υπάρχει κατευθείαν συνδεδεμένο μέλος στο interface. Εξ ορισμού η προεπιλεγμένη διαμόρφωση σε ένα δρομολογητή είναι τέτοια ώστε η multicast δρομολόγηση να είναι ανενεργή σε κάθε interface. Στο δίκτυο της εικόνας που χρησιμοποιήθηκε για την υλοποίηση της multicast υπηρεσίας του δικτύου «Αριάδνη», τα interface των δύο δρομολογητών ρυθμίστηκαν σε sparse mode με την παρακάτω εντολή:

Router(config-if)#ip pim sparse-mode

Προσέξτε ότι η ενεργοποίηση του PIM / IGMP πρέπει να γίνει σε κάθε interface που θα υποστηρίζει multicasting

.

6.2.3 Ρύθμιση του RP

Αν ρυθμιστεί το PIM να λειτουργεί σε sparse mode, πρέπει να επιλεχτούν ένας ή περισσότεροι δρομολογητές να είναι RPs. Δεν χρειάζεται να ρυθμιστούν οι δρομολογητές να είναι RPs αφού στην περίπτωση του Auto-RP μαθαίνουν να γίνονται RPs μόνοι τους. Το Cisco IOS software μπορεί να ρυθμιστεί, έτσι ώστε τα πακέτα για μια multicast ομάδα να μπορούν να χρησιμοποιήσουν ένα ή περισσότερα RPs.

Η RP διεύθυνση χρησιμοποιείται από τους first-hop δρομολογητές για να στείλουν PIM register μηνύματα και από τους last-hop δρομολογητές για να στείλουν PIM join/prune μηνύματα. Η διεύθυνση του RP πρέπει να ρυθμιστεί σε όλους τους δρομολογητές όπως επίσης και στο ίδιο το RP. Ένας PIM δρομολογητής μπορεί να είναι RP σε περισσότερες από μια ομάδες ενώ μια ομάδα μπορεί να έχει πάνω από ένα RP. Σε αυτή την περίπτωση, ένα και μόνο RP μπορεί να χρησιμοποιείται από την ομάδα την φορά (δηλαδή όχι δύο ταυτόχρονα) μέσα σε ένα domain. Μια λίστα πρόσβασης μπορεί να καθορίσει για ποιες ομάδες είναι δρομολογητής είναι rendezvous point.

Για να δοθεί η διεύθυνση του RP σε ένα δρομολογητή, γράφουμε σε configuration mode:

router(config)#ip pim rp-address *rp-address [access-list]* ***[override]***

Ο παραπάνω τρόπος ρύθμισης του RP είναι ο πιο απλός. Όμως για τη χρησιμοποίηση πολλών RPs σε ένα δίκτυο πρέπει να ενεργοποιηθεί auto-RP.

6.2.4 Ρύθμιση ενός δρομολογητή να είναι μέλος μιας ομάδας.

Οι Cisco δρομολογητές μπορεί να ρυθμιστούν να είναι μέλη σε μια multicast ομάδα. Αυτή η στρατηγική είναι χρήσιμη για να ανακαλυφτεί αν μεταφέρονται τα multicast πακέτα σε ένα δίκτυο (debugging). Για παράδειγμα μπορεί ο δρομολογητής να απαντάει σε ping μηνύματα ή να χρησιμοποιεί τα multicast traceroute εργαλεία του Cisco IOS software.

Για να γίνει μέλος ένας δρομολογητής σε μια ομάδα και να ενεργοποιηθεί το IGMP, χρησιμοποιείται η παρακάτω εντολή σε interface configuration mode:

router(config-if)#ip igmp join-group *group-address*

6.2.5 Έλεγχος της πρόσβασης στα IP Multicast groups.

Οι multicast δρομολογητές στέλνουν IGMP ερωτήματα στους hosts για να ανακαλύψουν ποιες multicast ομάδες έχουν μέλη στο τοπικό δίκτυο. Στην συνέχεια, οι δρομολογητές προωθούν σε αυτά τα μέλη όλα τα πακέτα με διεύθυνση προορισμού την διεύθυνση της ομάδας. Μπορεί να τοποθετηθεί ένα φίλτρο σε κάθε interface που οι hosts είναι συνδεδεμένοι το οποίο να ελέγχει την πρόσβαση στις multicast ομάδες.

Για να γίνει έλεγχος των ομάδων που επιτρέπονται σε ένα interface, χρησιμοποιείται η παρακάτω εντολή σε interface configuration mode:

router(config-if)#ip igmp access-group *access-list*

6.2.6 Ρύθμιση του δρομολογητή σαν ένα στατικά συνδεμένο μέλος.

Μερικές φορές είτε δεν υπάρχει μέλος μιας ομάδας σε ένα δίκτυο, είτε όταν ένας host δεν μπορεί να αναφέρει την συμμετοχή του σε μια ομάδα μέσο του IGMP, όμως εμείς θέλουμε η multicast κίνηση να φτάσει σε αυτό το δίκτυο. Με την χρήση της παρακάτω εντολής, ο δρομολογητής δεν δέχεται τα πακέτα για τον εαυτό του αλλά μόνο τα προωθεί. Για να ρυθμίσουμε δηλαδή, ένα δρομολογητή να γίνει στατικά συνδεμένο μέλος μιας ομάδας χρησιμοποιούμε την παρακάτω εντολή σε interface configuration mode:

router(config-if)#ip igmp static-group *group-address*

6.2.7 Ενεργοποίηση του SAP Listener Support.

Οι εφαρμογές του Multicast (για παράδειγμα το vic, το rat και wb) βασίζονται στις πληροφορίες των multicast session που στέλνονται μέσο του δικτύου. Σε αυτές τις περιπτώσεις, χρησιμοποιείται ένα πρωτόκολλο που λέγεται Session Announcement Protocol (SAP)[1] για την μεταφορά των SDP session ανακοινώσεων[2].

Για να ενεργοποιηθεί το λειτουργικό Cisco IOS ώστε να ακούει τις Session Directory ανακοινώσεις, χρησιμοποιούμε την παρακάτω εντολή σε interface configuration mode:

router(config-if)#ip sap listen

6.2.8 Οριοθέτηση του χρόνου ύπαρξης μιας SAP Cache εισόδου.

Εξ ορισμού, οι είσοδοι διαγράφονται 24 ώρες μετά την τελευταία φορά που έλαβαν από το δίκτυο. Για να οριοθετήσουμε για πόσο χρόνο μια SAP cache είσοδος μένει ενεργεί στην cache, χρησιμοποιούμε την παρακάτω εντολή σε global configuration mode:

router(config-if)#ip sap cashe-timeout

Μέχρι τώρα είδαμε τις ρυθμίσεις που κάνουμε σε ένα εσωτερικό δρομολογητή ενός δικτύου προκειμένου να υποστηρίξει IP multicasting. Στο συγκεκριμένο δίκτυο το configuration του εσωτερικού δρομολογητή είναι:

```
Current configuration:
!
! Last configuration change at 13:10:23 EET Wed May 15 2002 by noc
! NVRAM config last updated at 13:10:29 EET Wed May 15 2002 by noc
!
version 11.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
```

[1] Περισσότερες πληροφορίες για τα SAP και SDP στο κεφ. 8
[2] Το SDR στέλνει και να λαμβάνει SDP/SAP πακέτα

```
!
hostname ***
!
no ip source-route
ip domain-name ariadne-t.gr
ip multicast-routing
ip sdr cache-timeout 5
no ip dvmrp route-limit
clock timezone EET 2
clock summer-time EET recurring last Sun Mar 3:00 last Sun Oct 4:00
!
interface ***
 description MulticastExp
 encapsulation isl 141
 ip address 143.233.41.1 255.255.255.0
 no ip redirects
 ip pim sparse-mode
 arp timeout 3600
 traffic-shape rate 64000 10000 5000 500
!
```

Από το configuration του δρομολογητή βλέπουμε ότι το IP multicasting είναι ενεργοποιημένο στο sub-interface ***.

6.3 Διαμόρφωση Εξωτερικού Δρομολογητή

Για την διαμόρφωση ενός εξωτερικού δρομολογητή πρέπει να γίνουν και οι ρυθμίσεις του εσωτερικού δρομολογητή. Στην συνέχεια θα αναφερθούμε στις ρυθμίσεις που πρέπει να γίνουν για τη διαμόρφωση ενός εξωτερικού (border) δρομολογητή. Αυτές είναι:

- Ρύθμιση ορίου multicast domain – multicast boundary.
- Ρύθμιση ορίου ελάχιστου TTL για εξερχόμενα πακέτα από το multicast domain.
- Ρύθμιση ορίου PIM Domain – PIM boundary.
- Καθορισμός του Rendezvou Point και των groups που εξυπηρετεί.
- Ρύθμιση ενός MSDP peer.
- Cashing SA State.
- Χρησιμοποίηση ενός MSDP φίλτρου.
- Ρύθμιση μιας MSDP mesh ομάδες.
- Ενεργοποίηση του MBGP.

6.3.1 Ρύθμιση multicast domain – multicast boundary.

Η ρύθμιση του ορίου ενός multicast domain επιτρέπει τον ορισμό multicast ομάδων οι οποίες δεν θα διαρρέουν αλλά ούτε και θα εισέρχονται από τα όρια (border router) του. Οι ομάδες που έχουν ορισθεί στην περίπτωση μας είναι οι προτεινόμενες από την CISCO Systems και το ΕΔΕΤ. Ποιό αναλυτικά είναι:

1) Εφαρμογές εντός LAN (local scope)

access-list 50 deny 224.0.1.35
access-list 50 deny 224.0.1.60
access-list 50 deny 224.0.2.2
access-list 50 deny 224.0.1.3
access-list 50 deny 224.0.1.2
access-list 50 deny 224.0.1.22
access-list 50 deny 224.0.1.24

2) Ομάδες για το auto-rp
access-list 50 deny 224.0.1.39
access-list 50 deny 224.0.1.40

3) Εφαρμογές εντός domain (Administrative scope)
access-list 50 deny 239.0.0.0 0.255.255.255

4) Επιτρεπόμενες ομάδες
access-list 50 permit 224.0.0.0 15.255.255.255

Η εφαρμογή του ορίου γίνεται ξεχωριστά ανά ακραίο (border) interface.

router(config-if)#ip multicast boundary access-list-number

6.3.2 Ρύθμιση ορίου ελάχιστου TTL για εξερχόμενα πακέτα από το multicast domain.

Η ρύθμιση του ορίου TTL είναι ένας δεύτερος να περιοριστεί μια ομάδα στο όρια του domain και έχει την τιμή των 16 hops. Σημειώστε ότι και αυτό το όριο τίθεται ανά ακραίο (border) interface.

***router(config-if)#ip multicast ttl-threshold** ttl*

6.3.3 Ρύθμιση ορίου PIM Domain – PIM boundary.

Ο περιορισμός των μηνυμάτων bootstrap είναι ο στόχος αυτού ορίου. Με αυτόν τον περιορισμό επιτυγχάνεται η εκλογή διαφορετικών bsr routers σε κάθε domain(όταν έχει ενεργοποιηθεί η δυνατότητα). Η εφαρμογή του περιορισμού γίνεται ανά ακραίο (border) interface.

router(config-if)#ip pim border

6.3.4 Στατικός καθορισμός του Rendezvou Point και των groups που εξυπηρετεί.

Για να καθοριστεί στατικά ο δρομολογητής που θα αναλάβει τον ρόλο του RP πρέπει να χρησιμοποιηθεί η εντολή που ακολουθεί. Η αυτή εντολή δίνει την δυνατότητα ορισμού και των groups που θα εξυπηρετεί ο συγκεκριμένος RP. Είναι σημαντικό η διεύθυνση που θα χρησιμοποιεί ο RP να ανήκει σε κάποιο από τα loopback interface του, έτσι ώστε να μην βασίζεται η πρόσβαση σε αυτόν στην διαθεσιμότητα σύνδεσης μέσω συγκεκριμένου φυσικού interface.

***router(config)# ip pim accept-rp** { address | **Auto-RP**} [access-list-number}*

6.3.5 Καθορισμός του Rendezvou Point και των groups που εξυπηρετεί.

Είναι δυνατό να καθοριστεί στους δρομολογητές η διεύθυνση του RP καθώς και οι ομάδες που εξυπηρετεί (μέσω Access-list) ώστε να αποφευχθούν προβλήματα από δυσλειτουργούντες δρομολογητές όπως φαίνεται στην συνέχεια:

router(config)# ip pim rp-address *ip-address [group-access-list-number}* [**override**]

6.3.6 Ρύθμιση ενός MSDP peer.

Οι δύο βασικές ρυθμίσεις είναι η ενεργοποίηση του MSDP και του MBGP. Το πρώτο γίνεται προσαρμόζοντας ένα MSDP peer στον τοπικό δρομολογητή. Για την διαμόρφωση ενός MSDP peer, χρησιμοποιείται η παρακάτω εντολή σε global configuration mode[1].

router(config)# ip msdp peer *{peer address | peer address}* ***[connect-source*** *type number]* ***[remote-as*** *as-number]*

Με τη λέξη-κλειδί **connect-source,** η κύρια διεύθυνση του καθορισμένου από τις τιμές του είδους και του αριθμού interface, χρησιμοποιείται ως πηγή για την TCP σύνδεση. Η connect-source συνιστάται κυρίως για ένα MSDP peer πάνω σε ένα εξωτερικό δρομολογητή, που κάνει peer με ένα εσωτερικό δρομολογητή σε ένα απομακρυσμένο domain.

Router(config)# ip msdp description *{peer name | peer-address} text*

Με την παραπάνω εντολή μπορεί να διαμορφωθεί μια περιγραφή για ένα καθορισμένο peer, έτσι ώστε να γίνεται ευκολότερα η αναγνώρισή του από την έξοδο μιας configuration ή show εντολής.

6.3.7 Cashing SA State.

Από default, ο δρομολογητής δεν αποθηκεύει τα (S,G) ζευγάρια που λαμβάνει από τα SA μηνύματα. Για να γίνει αυτό, χρησιμοποιείται η παρακάτω εντολή σε global configuration mode:

Router(config)# ip msdp cache-sa-state [list *access-list]*

Η παραπάνω εντολή μπορεί να παραληφθεί και να πετύχουμε το ίδιο αποτέλεσμα χρησιμοποιώντας sa-request μηνύματα. Τα τοπικά RPs μπορούν να στείλουν SA ερωτήματα (requests) και να πάρουν αμέσως απάντηση για όλες τις ενεργές πηγές για μια καθορισμένη multicast ομάδα. Οι δρομολογητές δεν έχουν προκαθορισμένη αυτή τη δυνατότητα. Για να επιτευχθεί αυτό, χρησιμοποιείται η παρακάτω εντολή σε global configuration mode:

[1] Ο δρομολογητής που καθορίζεται από το Domain Naming System (DNS) ή από την IP διεύθυνση, σαν ένα MSDP peer είναι συνήθως και MBGP peer neighbor.

Router(config)# ip msdp sa-request

Τα SA μηνύματα δημιουργούνται από τα RPs στα οποία οι πηγές έχουν εγγραφεί (register). Στα RPs είναι προεπιλεγμένο ότι κάθε πηγή που κάνει εγγραφή θα δημοσιευτεί σε ένα SA μήνυμα. Αυτό μπορεί να διαμορφωθεί με την παρακάτω εντολή, έτσι ώστε το RP να επιλέγει ποια πηγή να δημοσιευτεί και ποια όχι:

***Router(config)# ip msdp redistribute [list** access-list] [**asn** as-access-list] [**route-map** map-name]*[2]

6.3.8 Χρησιμοποίηση ενός MSDP φίλτρου.

Στα MSDP peers είναι προεπιλεγμένο να προωθούνται και να λαμβάνονται όλα τα SA μηνύματα. Όμως ο δρομολογητής μπορεί να διαμορφωθεί, έτσι ώστε να αποτρέπει την προώθηση εξερχόμενων μηνυμάτων και τη λήψη εισερχόμενων, χρησιμοποιώντας ένα φίλτρο ή δίνοντας ένα time-to-live. Το φίλτρο που προτείνεται από CISCO Systems και ΕΔΕΤ είναι:

1) Εφαρμογές εντός LAN (local scope)
access-list 150 deny ip any host 224.0.1.35
access-list 150 deny ip any host 224.0.1.60
access-list 150 deny ip any host 224.0.2.2
access-list 150 deny ip any host 224.0.1.3
access-list 150 deny ip any host 224.0.1.2
access-list 150 deny ip any host 224.0.1.22
access-list 150 deny ip any host 224.0.1.24

2) Ομάδες για το auto-rp
access-list 150 deny ip any host 224.0.1.39
access-list 150 deny ip any host 224.0.1.40

3) Εφαρμογές εντός domain (Administrative scope)
access-list 150 deny ip any 239.0.0.0 0.255.255.255

4) Περιορισμός από ΕΔΕΤ
access-list 150 deny ip any host 234.42.42.42
access-list 150 deny ip any host 229.55.150.208
access-list 150 deny ip any host 234.142.142.142

5) Περιορισμός πηγών με loopback, private διευθύνσεις
access-list 150 deny ip 10.0.0.0 0.255.255.255 any
access-list 150 deny ip 127.0.0.0 0.255.255.255 any
access-list 150 deny ip 172.16.0.0 0.15.255.255 any
access-list 150 deny ip 192.168.0.0 0.0.255.255 any

6) Πεδίο ομάδων SSM – αποτροπή χρήσης από MSDP
access-list 150 deny ip any 232.0.0.0 0.255.255.255

7) Επιτρεπόμενες ομάδες

[2] Η εντολή ip msdp redistribute μπορεί επίσης να χρησιμοποιηθεί για την δημοσίευση πηγών που είναι γνωστές στο RP αλλά δεν έχουν κάνει εγγραφή σε αυτό.

access-list 150 permit ip any 224.0.0.0 15.255.255.255
Για τα εξερχόμενα ή εισερχόμενα μηνύματα χρησιμοποιούνται οι παρακάτω εντολές σε global configuration mode:

Router(config)# ip msdp sa-filter out/in *{peer address | peer-name}*
Router(config)# ip msdp sa-filter out/in *{peer address | peer-name}* ***list*** *access-list*
Router(config)# ip msdp sa-filter out/in *{peer address | peer-name}* ***route-map*** *map-name*

Για να δοθεί ένα TTL όριο, δίνεται η εντολή:

Router(config)# ip msdp ttl-threshold *{peer address | peer-name} ttl-value*

6.3.9 Ρύθμιση μιας MSDP mesh ομάδες.

Για την δημιουργία ενός mesh-group, χρησιμοποιείται η παρακάτω εντολή σε global configuration mode:

Router(config)# ip msdp mesh-group *mesh-name {peer-address | peer-name}*

6.3.10 Ενεργοποίηση του MBGP

Μετά την έκδοση 11.1 το IOS χρησιμοποιεί NLRI (Network Layer Reachability Information) λέξεις-κλειδιά για την ενεργοποίηση Multiprotocol BGP πάνω από μια BGP σύνδεση και για να εισάγει τις unicast BGP συνδέσεις στην unicast βάση δεδομένων και τις multicast BGP συνδέσεις στην multicast βάση δεδομένων. Στην έκδοση 12.1, για τις παραπάνω ενέργειες το IOS χρησιμοποιεί ξεχωριστές address families.

Για τη ρύθμιση του Multiprotocol BGP μεταξύ δύο δρομολογητών χρησιμοποιούνται οι 4 παρακάτω εντολές ξεκινώντας σε global configuration mode:

Router(config)# ***router bgp*** *autonomous system*
Router(config-router)# ***neighbor*** *ip-address* ***remote-as*** *autonomous-system-number*
Router(config-router)# ***address-family ipv4 multicast***
*Router(config-router-af)#****neighbor*** *{ip-address | peer-group-name}* ***activate***

Αντίστοιχα οι παραπάνω εντολές έχουν την εξής σημασία:

- Διαμορφώνει μια BGP διαδικασία δρομολόγησης.
- Προσθέτει την IP διεύθυνση του γειτονικού δρομολογητή που ανήκει σε άλλο αυτόνομο σύστημα, στο Multiprotocol BGP neighbor πίνακα του τοπικού δρομολογητή.
- Καθορίζει την IPv4 address family και τοποθετεί τον δρομολογητή σε address family configuration mode
- Ενεργοποιείται ο γειτονικός δρομολογητής να ανταλλάσσει τα δεδομένα του πίνακα δρομολόγησης για το καθορισμένο είδος address family με τον τοπικό δρομολογητή.

Στο συγκεκριμένο δίκτυο το configuration του εξωτερικού δρομολογητή είναι:

*rb6#****sh run***
Building configuration...

```
Current configuration : 11022 bytes
!
! Last configuration change at 12:17:16 EET Tue May 21 2002 by ***
! NVRAM config last updated at 15:09:03 EET Tue May 14 2002 by ***
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname ***
!
!
ip domain-name ariadne-t.gr
!
ip multicast-routing
ip sap cache-timeout 5
call rsvp-sync
!
interface *** point-to-point
 bandwidth 14336
 ip address 194.177.209.190 255.255.255.252
 ip access-group 120 in
 ip access-group 121 out
 ip pim bsr-border
 ip pim sparse-dense-mode
 ip multicast ttl-threshold 16
 ip multicast boundary 50
 ip route-cache same-interface
 ip sap listen
 !
router bgp
 no synchronization
 bgp log-neighbor-changes
 network 143.233.0.0
 timers bgp 30 90
 neighbor xxx.xxx.xxx.xxx remote-as ***
 neighbor xxx.xxx.xxx.xxx soft-reconfiguration inbound
 neighbor xxx.xxx.xxx.xxx remote-as ***
 neighbor xxx.xxx.xxx.xxx send-community
 neighbor xxx.xxx.xxx.xxx soft-reconfiguration inbound
 neighbor xxx.xxx.xxx.xxx route-map *** in
 neighbor xxx.xxx.xxx.xxx route-map ***  out
 !
address-family ipv4 multicast
 neighbor xxx.xxx.xxx.xxx activate
 neighbor xxx.xxx.xxx.xxx send-community
 neighbor xxx.xxx.xxx.xxx soft-reconfiguration inbound
 network 143.233.0.0
 exit-address-family
!
ip classless
ip route 143.233.0.0 255.255.0.0 Null0 254
no ip http server
ip pim rp-address xxx.xxx.xxx.xxx
ip pim accept-rp xxx.xxx.xxx.xxx
ip mroute 143.233.0.0 255.255.0.0 Null0 254
ip msdp peer xxx.xxx.xxx.xxx connect-source ***
ip msdp sa-filter in xxx.xxx.xxx.xxx list 150
ip msdp sa-filter out xxx.xxx.xxx.xxx list 150
ip msdp cache-sa-state
ip msdp redistribute list 150
```

```
access-list 50 deny   224.0.1.35
access-list 50 deny   224.0.1.39
access-list 50 deny   224.0.1.40
access-list 50 deny   224.0.1.60
access-list 50 deny   224.0.2.2
access-list 50 deny   224.0.1.3
access-list 50 deny   224.0.1.2
access-list 50 deny   224.0.1.22
access-list 50 deny   224.0.1.24
access-list 50 deny   239.0.0.0 0.255.255.255
access-list 50 permit 224.0.0.0 15.255.255.255
access-list 150 deny   ip any host 224.0.1.35
access-list 150 deny   ip any host 224.0.1.39
access-list 150 deny   ip any host 224.0.1.40
access-list 150 deny   ip any host 224.0.1.60
access-list 150 deny   ip any host 224.0.2.2
access-list 150 deny   ip any host 224.0.1.3
access-list 150 deny   ip any host 224.0.1.2
access-list 150 deny   ip any host 224.0.1.22
access-list 150 deny   ip any host 224.0.1.24
access-list 150 deny   ip any 239.0.0.0 0.255.255.255
access-list 150 deny   ip any host 234.42.42.42
access-list 150 deny   ip any host 229.55.150.208
access-list 150 deny   ip any host 234.142.142.142
access-list 150 deny   ip 10.0.0.0 0.255.255.255 any
access-list 150 deny   ip 127.0.0.0 0.255.255.255 any
access-list 150 deny   ip 172.16.0.0 0.15.255.255 any
access-list 150 deny   ip 192.168.0.0 0.0.255.255 any
```

6.4 Αναφορές 6ου Κεφαλαίου

1. MSDP Configuring tasks Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/msdp.htm
2. §PIMv2 Configuring tasks Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_2/pimv2.htm
3. Multiprotocol BGP Extensions for IP Multicast Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/mbgp.htm
4. Using IP Multicast Tools Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/1cdtools.htm
5. Source Specific Multicast Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtssm.htm
6. Configuring Multicast Source Discovery Protocol Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfmsdp.htm
7. Υπηρεσία IP Multicast. Σελίδα του ΕΔΕΤ. http://www.grnet.gr/mbone/
8. Configuring IP Multicast Routing. Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1cmulti.htm
9. Cisco IOS Release 12.0 Configuration Guides and Command References. Cisco pdf.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/

Κεφάλαιο 7ο: Multicast Debugging

7.1 Εισαγωγή

Παρά την ανάγκη για καλύτερη διαχείριση της κίνησης στο Internet, ιδιαίτερα για τις απαιτητικές εφαρμογές όπως ο ήχος και το video, το multicasting δε χρησιμοποιείται αρκετά από τους ISPs. Ένας σημαντικός λόγος που συμβαίνει αυτό είναι η δυσκολία παρακολούθησης και αντιμετώπισης προβλημάτων. Σε αυτό το κεφάλαιο θα ασχοληθούμε με το multicast debugging, δηλαδή τις ενέργειες που πραγματοποιεί και τα εργαλεία που χρησιμοποιεί ο διαχειριστής ενός multicast δικτύου, για την διαπίστωση της ποιότητας μιας multicast σύνδεσης. Για το multicast debugging ο διαχειριστής μπορεί να χρησιμοποιήσει τις εντολές *show* και *debug* του λειτουργικού IOS[1] της Cisco στους δρομολογητές, καθώς επίσης και software εργαλεία που μπορούν να εγκατασταθούν σε σταθμούς εργασίας.

7.2 Εντολές Show

- **sh ip igmp group**

Παράδειγμα:

router>show ip igmp groups
IGMP Connected Group Membership

Group Address	*Interface*	*Uptime*	*Expires*	*Last Reporter*
239.255.255.255	*Fa0.41*	*01:54:48*	*00:02:33*	*143.233.41.10*
239.255.255.255	*Ethernet0*	*4w4d*	*00:02:00*	*143.233.150.13*
239.255.255.250	*Fa0.8*	*00:54:18*	*00:02:43*	*143.233.247.173*
239.222.255.224	*Fa0.41*	*01:52:48*	*00:02:35*	*143.233.41.10*
224.2.232.59	*Fa0.41*	*01:50:30*	*00:02:33*	*143.233.41.10*
224.2.158.51	*Fa0.41*	*01:52:46*	*00:02:37*	*143.233.41.10*
224.2.127.254	*Fa0.41*	*01:54:48*	*00:02:37*	*143.233.41.10*
224.2.127.254	*Ethernet0*	*4w4d*	*00:01:59*	*143.233.150.13*
224.0.1.75	*Fa0.41*	*01:54:47*	*00:02:35*	*143.233.41.10*
235.80.68.83	*Fa0.8*	*00:54:15*	*00:02:51*	*143.233.247.6*
224.2.163.249	*Fa0.41*	*01:50:30*	*00:02:31*	*143.233.41.10*
224.0.1.40	*Ethernet0*	*4w4d*	*never*	*143.233.160.7*
224.0.1.60	*Fa0.8*	*00:55:18*	*00:02:51*	*143.233.247.99*
224.0.1.11	*Fa0.41*	*01:52:02*	*00:02:31*	*143.233.41.10*
224.0.1.12	*Fa0.41*	*01:52:02*	*00:02:35*	*143.233.41.10*
224.0.1.24	*Fa0.8*	*00:55:20*	*00:02:47*	*143.233.247.3*

Group Address	IP διεύθυνση multicast ομάδας για την οποία υπάρχουν συμμετοχές (υπάρχουν hosts που θέλουν να λάβουν το traffic του group)
Interface	Σε ποιο interface είναι συνδεδεμένοι οι hosts.
Uptime	Πόσο χρόνο συμμετέχουν στην multicast ομάδα οι hosts.
Expires	Χρόνος λήξης της συμμετοχής στην ομάδα ένα δεν υπάρξει άλλη ανανέωση της από τους συμμετέχοντες hosts.
Last Reporter	***Η τελευταία μηχανή που έστειλε IGMP αναφορά.***

Πίνακας 7.1: περιγραφή των αποτελεσμάτων της εντολής **sh ip igmp group**

- **sh ip igmp interface**

[1] Όλες οι εντολές αναφέρονται στο λειτουργικό IOS, γιατί οι δρομολογητές που χρησιμοποιήθηκαν για την πραγματοποίηση των πειραμάτων ήταν Cisco.

Παράδειγμα:
*router#**sh ip igmp interface***
Fa0.41 is up, line protocol is up
Internet address is 143.233.41.1/24
IGMP is enabled on interface
Current IGMP version is 2
CGMP is disabled on interface
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Inbound IGMP access group is not set
IGMP activity: 173 joins, 164 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 143.233.41.1 (this system)
IGMP querying router is 143.233.41.1 (this system)
No multicast groups joined

Με την εντολή sh ip igmp interface μπορούν να εξαχθούν αρκετές πληροφορίες. Αρχικά, φαίνεται η κατάσταση του interface, δηλαδή αν αυτό και το line protocol είναι ενεργό. Η IP διεύθυνση και η μάσκα του interface είναι δύο επόμενα στοιχεία που λαμβάνουμε. Επίσης αναγνωρίζεται αν είναι ενεργό το IGMP και σε ποια έκδοση, κάτι που μπορεί να είναι σημαντικό στην περίπτωση που υπάρχουν στο LAN άλλοι δρομολογητές με διαφορετική έκδοση. Ακόμα πληροφορούμαστε για το χρονικό διάστημα μεταξύ δύο IGMP ερωτημάτων, το χρονικό διάστημα που περιμένει ο δρομολογητής μέχρι να αλλάξει ο ερωτών (querier time out), το μέγιστο χρονικό διάστημα μέχρι να απαντηθεί το ερώτημα, στατιστικά των IGMP ενεργειών (igmp activity) και, τέλος, για την IP διεύθυνση του DR και του ερωτώντος δρομολογητή.

- **sh ip pim neighbor**

Παράδειγμα:
*router>**sh ip pim neighbor***

PIM Neighbor Table

Neighbor Address	*Interface*	*Uptime*	*Expires*	*Mode*	
143.233.150.13	*Ethernet0*	*6d00h*	*00:01:13*	*Sparse*	
143.233.150.17	*Ethernet0*	*4w4d*	*00:01:17*	*Sparse*	*(DR)*
143.233.150.18	*Ethernet0*	*4w4d*	*00:01:22*	*Sparse*	

Neighbor Address	Η IP διεύθυνση των γειτονικών δρομολογητών που τρέχουν PIM.
Interface	Το interface από το οποίο έλαβε το PIM Hello από το συγκεκριμένο γειτονικό δρομολογητή.
Uptime	Για πόσο χρόνο αυτός ο PIM γειτονικός είναι ενεργός.
Expires	Πόσος χρόνος μένει για να γίνει ανενεργός ο γειτονικός δρομολογητής (τα PIM hellos ανανεώνουν αυτό το χρόνο).
Mode	Σε τι mode τρέχει το PIM σε αυτό το interface.

Πίνακας 7.2: περιγραφή των αποτελεσμάτων της εντολής **sh ip pim neighbor**

- **sh ip pim interface**

παράδειγμα:
*router >**sh ip pim interface***

Address	*Interface*	*Mode*	*Nbr Count*	*Query intvl*	*DR*
143.233.150.13	*Ethernet0*	*Sparse*	*3*	*30*	*143.233.150.17*
143.233.247.1	*FastEthernet0.8*	*Sparse*	*0*	*30*	*143.233.247.1*
143.233.5.5	*FastEthernet0.14*	*Sparse*	*0*	*30*	*143.233.5.5*
143.233.41.1	*FastEthernet0.41*	*Sparse*	*0*	*30*	*143.233.41.1*

Address:	Η IP διεύθυνση του interface του δρομολογητή που τρέχει PIM.
Mode:	Σε τι mode (sparse, dense ή sparse-dense) τρέχει το PIM.
Nbr Count:	Πόσοι γειτονικοί δρομολογητές τρέχουν PIM (στο ίδιο LAN).
Query intvl:	Πόσο είναι το χρονικό διάστημα σε δευτερόλεπτα μεταξύ δύο PIM ερωτημάτων.
DR:	Η IP διεύθυνση του DR, που βρίσκεται στο ίδιο LAN με το Interface.

Πίνακας 7.3: περιγραφή των αποτελεσμάτων της εντολής **sh ip pim interface**

- **sh ip rpf**

παράδειγμα:
router#show ip rpf 172.16.8.1
RPF information for R1 (172.16.8.1)
RPF interface: Ethernet0
RPF neighbor: R3 (172.16.6.1)
RPF route/mask: 172.16.8.0/255.255.255.0
RPF type: unicast

R4#sh ip rpf 172.16.12.2
RPF information for Source1 (172.16.12.2)
RPF interface: Ethernet0
RPF neighbor: R6 (172.16.11.1)
RPF route/mask: 172.16.12.0/255.255.255.0
RPF type: unicast

Τα παραπάνω δύο παραδείγματα δίνουν πληροφορίες για το RPF interface που χρησιμοποιείται για την επικοινωνία με τη συγκεκριμένη μηχανή. Το πρώτο παράδειγμα αφορά στην επικοινωνία με το δρομολογητή R1 και το δεύτερο στην επικοινωνία με την πηγή Source1.

- **sh ip mroute**

Η sh ip mroute είναι ίσως η πιο σημαντική debugging εντολή, αφού παρουσιάζει τα περιεχόμενα του IP multicast πίνακα δρομολόγησης. Το IOS φτιάχνει το multicast πίνακα δρομολόγησης δημιουργώντας (S:source, G:group) καταχωρίσεις για τα Source Path Trees και (“*”:star, G:group) καταχωρήσεις για τα Rendevous Point Trees (shared). Το star (*) αναφέρεται σε όλες τις πηγές, το “S” αναφέρεται σε μία πηγή και το “G” στην multicast ομάδα. Για τη δημιουργία της (S,G) καταχώρησης χρησιμοποιείται ο μικρότερος δρόμος προς την πηγή, που υπάρχει στο unicast routing table (RPF), ενώ για την περίπτωση (*,G) ο μικρότερος προς το RP.

Τα πεδία που υπάρχουν σε κάθε multicast routing entry όπως αυτές εμφανίζονται από την εντολή sh ip mroute περιγράφονται στην συνέχεια.

Παράδειγμα:
*router>**sh ip mroute***

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(, 239.255.255.255), 4w5d/00:02:57, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:20:34/00:02:57

(, 224.2.217.30), 05:10:08/00:02:59, RP 143.233.254.29, flags: SJCF*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:10:08/00:02:53

(143.233.41.10/32, 224.2.217.30), 00:05:39/00:00:26, flags: PCFT
Incoming interface: FastEthernet0.41, RPF nbr 0.0.0.0
Outgoing interface list: Null

(, 239.222.255.224), 05:10:10/00:02:59, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:10:10/00:02:59

(, 224.2.232.59), 00:02:28/00:02:59, RP 143.233.254.29, flags: SP*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list: Null

(128.223.230.9/32, 224.2.232.59), 00:02:28/00:00:31, flags: PT
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list: Null

(, 224.2.127.254), 4w5d/00:02:59, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:20:35/00:02:53

(128.59.244.235/32, 224.2.127.254), 00:23:04/00:02:59, flags: CJT
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 00:23:04/00:02:53

(128.112.232.101/32, 224.2.127.254), 00:22:11/00:02:56, flags: CJT
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 00:22:11/00:02:53

(, 224.0.1.75), 05:23:02/00:02:30, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.41, Forward/Sparse, 05:23:02/00:02:30

(, 224.0.1.40), 4w5d/00:00:00, RP 143.233.254.29, flags: SJPCL*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list: Null

(, 224.0.1.60), 1d04h/00:02:41, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.8, Forward/Sparse, 1d04h/00:02:41

(, 224.0.1.24), 1d04h/00:02:40, RP 143.233.254.29, flags: SJC*
Incoming interface: Ethernet0, RPF nbr 143.233.150.16
Outgoing interface list:
FastEthernet0.8, Forward/Sparse, 1d04h/00:02:40

Οι (*,G) καταχωρήσεις που φαίνονται στον πίνακα δρομολόγησης του παραδείγματος χρησιμοποιούνται για την προώθηση της κίνησης προς τα μέλη του group μέσω ενός Shared δέντρου δρομολόγησης, στην περίπτωση που δεν υπάρχει αντίστοιχη (S,G) καταχώρηση. Το χρονόμετρο στην πρώτη γραμμή της (*,G) υποδεικνύει πότε η καταχώρηση θα διαγραφεί. Η πληροφορία από το *incoming interface* πεδίο χρησιμοποιείται για τον RPF έλεγχο της εισερχόμενης (*,G) multicast κίνησης, που γίνεται σε σχέση με το RP. Η *outgoing interface list* αναφέρεται στα interfaces στα οποία έχουν σταλεί (*,G) μηνύματα σύνδεσης ή έχουν κατευθείαν συνδεδεμένα μέλη της ομάδας “G”. Η κίνηση που φτάνει μέσω του Shared δέντρου προωθείται από αυτά τα interfaces. Μια (*,G) καταχώρηση δημιουργείται, όταν λαμβάνεται μια (*,G) PIM σύνδεση ή μια IGMP αναφορά. Επίσης, οι (*,G) καταχωρήσεις δημιουργούνται αυτόματα, όποτε μια (S,G) καταχώρηση για την ομάδα “G” πρέπει να δημιουργηθεί. Η (*,G) καταχώρηση δημιουργείται αρχικά και στη συνεχεία η (S,G).

Οι (S,G) καταχωρήσεις χρησιμοποιούνται για κάθε multicast κίνηση που στέλνεται από την πηγή “S” στην ομάδα “G”. Όμοια με τις (*,G) καταχωρήσεις, στην πρώτη γραμμή υπάρχει ένα χρονόμετρο που δείχνει πόσο χρόνο θα υπάρχει η καταχώρηση. Η πληροφορία στο πεδίο *incoming interface* χρησιμοποιείται για τον RPF έλεγχο της εισερχόμενης (S,G) κίνησης. Αν ένα πακέτο δεν εισέλθει από αυτά τα interfaces, απορρίπτεται. Η λίστα με τα *outgoing interfaces* δείχνει τα interfaces από τα οποία τα (S,G) πακέτα προωθούνται. Μια PIM-SM, (S,G) καταχώρηση δημιουργείται, είτε όταν ο δρομολογητής λάβει ένα (S,G) μήνυμα σύνδεσης, είτε όταν γίνεται PIM-SM εγγραφή στο RP, που πραγματοποιείται από τον first-hop δρομολογητή.

Όταν μια (S,G) καταχώρηση πρέπει να δημιουργηθεί, ακολουθούνται τα παρακάτω βήματα:

- Αν η αντίστοιχη (*,G) καταχώρηση δεν υπάρχει, δημιουργείται.
- Ο RPF έλεγχος γίνεται με βάση την πηγή “S”. Αυτή η πληροφορία αποθηκεύεται στην (S,G) καταχώρηση για το πεδίο incoming interface και RPF neighbor (ο PIM γειτονικός προς την κατεύθυνση της πηγής).
- Για την περίπτωση της (S,G) καταχώρησης, η λίστα με τα εξερχόμενα interfaces παίρνει τα δεδομένα από την αντίστοιχη (*,G) καταχώρηση που έχει δημιουργηθεί. (Το εισερχόμενο interface δεν πρέπει να εμφανίζεται στην λίστα με τα εξερχόμενα, γιατί τότε δημιουργείται ένα loop).

Ένα interface προστίθεται στην λίστα με τα εξερχόμενα interfaces, όταν ένα μήνυμα σύνδεσης λαμβάνεται από το interface, ενώ κάθε φορά που συμβαίνει αυτό προστίθεται και στην αντίστοιχη (S,G) λίστα εξερχόμενων interfaces.

Τα interfaces διαγράφονται από τη λίστα εξερχόμενων interfaces, όταν το χρονόμετρο τελειώσει. Το χρονόμετρο ανανεώνεται κάθε φορά που το interface λαμβάνει ένα PIM μήνυμα σύνδεσης από ένα downstream δρομολογητή ή μια IGMP αναφορά από κάποιο κατευθείαν συνδεμένο μέλος. Επίσης, ένα interface διαγράφεται, όταν λάβει ένα Prune μήνυμα. Τα interfaces που διαγράφονται από την (*,G) λίστα, διαγράφονται από όλες τις αντίστοιχες (S,G) λίστες.

Οι παράμετροι του πεδίου flag στον πίνακα δρομολόγησης έχουν την εξής σημασία:

“S” Flag: υποδεικνύει ότι η ομάδα λειτουργεί σε sparse mode, και εμφανίζεται μόνο σε (*,G) καταχωρήσεις.

“D” Flag: υποδεικνύει ότι ή ομάδα λειτουργεί σε dense mode.

“C” Flag: υποδεικνύει ότι υπάρχει κατευθείαν συνδεδεμένο μέλος της ομάδας στο δρομολογητή.

“L” Flag: υποδεικνύει ότι ο δρομολογητής είναι ο ίδιος μέλος της ομάδας και λαμβάνει multicast κίνηση.

“P” Flag: υπάρχει όταν όλα τα εξερχόμενα interfaces της λίστας έχουν αποκοπεί (pruned). Αυτό σημαίνει ότι ο δρομολογητής θα στείλει prune μηνύματα στο RP για να σταματήσει την κίνηση.

“T” Flag: υποδεικνύει ότι τουλάχιστον ένα πακέτο έλαβε μέσω του SPT και αναφέρεται μόνο σε (S,G) καταχωρήσεις.

“J” Flag (Join SPT): α) όταν υπάρχει σε μια (*,G) καταχώρηση, υποδεικνύει ότι ο ρυθμός της κίνησης που διατρέχει το Shared δέντρο είναι μεγαλύτερος από το SPT όριο, οπότε το επόμενο πακέτο θα προκαλέσει την μετατροπή του δέντρου από Shared σε Source Path. β) όταν εμφανίζεται σε μια (S,G) καταχώρηση, υποδηλώνει ότι αυτή η καταχώρηση δημιουργήθηκε από shared δέντρο στο οποίο ο ρυθμός κίνησης πέρασε το καθορισμένο SPT όριο.

“F” Flag (Register): α) υπάρχει σε μια (S,G) καταχώρηση όταν η πηγή “S” είναι κατευθείαν συνδεδεμένη με τον δρομολογητή. Αυτό σημαίνει ότι ο δρομολογητής είναι first-hop δρομολογητής και είναι αυτός που στέλνει μηνύματα εγγραφής στο RP, για να τον ενημερώσει ότι η πηγή είναι ενεργή. β) υπάρχει επίσης σε μια (*, G) καταχώρηση αν εμφανίζεται σε κάποια από τις αντίστοιχες (S,G) καταχωρίσεις.

“R” Flag (RP-bit): Αυτή η παράμετρος υπάρχει μόνο σε (S,G) καταχωρήσεις και δείχνει ότι οι (S,G) πληροφορίες προώθησης της καταχώρησης είναι εφαρμόσιμες στην (S,G) κίνηση που διατρέχει το Shared δέντρο. Αυτό συμβαίνει όταν το interface λάβει ένα (S,G)RP-bit μήνυμα αποκοπής. Αυτά τα μηνύματα στέλνονται από τους downstream δρομολογητές του Shared δέντρου που θέλουν η συγκεκριμένη (S,G) κίνηση να αποκοπεί από το Shared δέντρο προς αυτούς. Αυτό γίνεται για να ελαττωθεί η πιθανότητα μεταφοράς διπλών πακέτων μετά την μετατροπή σε SPT. Όταν η “R” Flag εμφανίζεται σε μια (S,G) καταχώρηση, ο RPF έλεγχος πρέπει να γίνεται με βάση το RP και όχι την πηγή. Αυτό συμβαίνει λόγω της υπόθεσης (α).

“X” Flag (Proxy Join Timer Running): Αυτή η σημαία εμφανίζεται μόνο στις (S,G) καταχωρήσεις και χρησιμοποιείται για να δείχνει ότι ο “Proxy Join Timer” είναι ενεργός. Όταν συμβαίνει αυτό, ο δρομολογητής θα συνεχίσει να στέλνει (S,G) μηνύματα σύνδεσης προς την κατεύθυνση της πηγής ακόμα και αν η λίστα εξερχόμενων interfaces είναι NULL.

“M” Flag (MSDP created): εμφανίζεται μόνο στις (S,G) καταχωρήσεις και μόνο στο δρομολογητή που είναι ο RP για την ομάδα “G”. Υποδηλώνει ότι ο RP γνωρίζει για τη συγκεκριμένη πηγή μέσω ενός “Source Active” μηνύματος.

“A” Flag (Advertise Flag): εμφανίζεται μόνο στις (S,G) καταχωρήσεις και μόνο στο δρομολογητή που είναι ο RP για την ομάδα “G”. Δείχνει ότι αυτή η πηγή ανήκει στο τοπικό PIM-SM domain και είναι υποψήφια να δημοσιευτεί στα RPs άλλων δικτύων μέσω MSDP SA μηνυμάτων.

- **Sh ip mroute active**

Με την εντολή *sh ip mroute active* εμφανίζονται όλες οι ενεργές ομάδες στις οποίες οι πηγές στέλνουν με ρυθμό μεγαλύτερο από 4kbps.

Παράδειγμα:
router>sh ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (SAP.MCAST.NET)
Source: 128.223.83.33 (iptvhost.uoregon.edu)
Rate: 0 pps/0 kbps(1sec), 2 kbps(last 17 secs), 2 kbps(life avg

- **Sh ip mroute count**

Με την εντολή *sh ip mroute count* εμφανίζονται χρήσιμα στατιστικά για κάθε καταχώρηση.

Παράδειγμα:
router>sh ip mroute count
IP Multicast Statistics
34 routes using 13124 bytes of memory
12 groups, 1.83 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.255.255.255, Source count: 0, Group pkt count: 0
RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0

Group: 224.2.217.30, Source count: 1, Group pkt count: 0
RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Source: 143.233.41.10/32, Forwarding: 0/0/0/0, Other: 2399/0/2399

Group: 224.2.232.59, Source count: 2, Group pkt count: 24514
RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Source: 128.223.230.9/32, Forwarding: 24440/0/1112/0, Other: 61504/30749/6315
Source: 143.233.41.10/32, Forwarding: 74/0/75/0, Other: 150/75/1

- **Sh ip mroute summary**

Παράδειγμα:
router>sh ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(, 239.255.255.255), 2w0d/00:02:35, RP 143.233.254.29, flags: SJPC*
(, 224.2.127.254), 2w0d/00:02:59, RP 143.233.254.29, flags: SJPC*

(128.59.244.235/32, 224.2.127.254), 00:00:46/00:02:13, flags: PCT
(128.114.3.66/32, 224.2.127.254), 00:00:51/00:02:08, flags: PCT
(128.178.10.2/32, 224.2.127.254), 00:02:07/00:00:52, flags: PCT
(128.223.83.33/32, 224.2.127.254), 00:01:11/00:01:48, flags: PCT
(129.79.85.45/32, 224.2.127.254), 00:02:10/00:00:49, flags: PCT
(129.105.153.48/32, 224.2.127.254), 00:00:01/00:02:58, flags: PCT
(131.188.34.85/32, 224.2.127.254), 00:02:42/00:00:17, flags: PCT
(131.188.219.130/32, 224.2.127.254), 00:00:22/00:02:37, flags: PCT
(134.174.178.254/32, 224.2.127.254), 00:02:10/00:00:49, flags: PCT
(137.78.104.204/32, 224.2.127.254), 00:01:52/00:01:07, flags: PCT
(137.79.16.204/32, 224.2.127.254), 00:02:50/00:00:09, flags: PCT
(141.99.80.70/32, 224.2.127.254), 00:01:30/00:01:29, flags: PCT
(158.36.47.163/32, 224.2.127.254), 00:01:16/00:01:43, flags: PCT
(171.69.248.71/32, 224.2.127.254), 00:02:57/00:00:02, flags: PCT
(193.50.192.71/32, 224.2.127.254), 00:01:06/00:01:53, flags: PCT
(193.166.0.41/32, 224.2.127.254), 00:01:48/00:01:11, flags: PCT
(194.53.0.66/32, 224.2.127.254), 00:01:18/00:01:41, flags: PCT
(203.178.137.220/32, 224.2.127.254), 00:02:48/00:00:11, flags: PCT
(207.188.7.196/32, 224.2.127.254), 00:01:35/00:01:24, flags: PCT
(216.177.62.19/32, 224.2.127.254), 00:01:26/00:01:33, flags: PCT
(, 224.0.1.40), 2w0d/00:00:00, RP 143.233.254.29, flags: SJPCL*
(, 224.0.1.60), 2d01h/00:01:44, RP 143.233.254.29, flags: SJC*
(, 224.0.1.24), 2d01h/00:02:42, RP 143.233.254.29, flags: SJC*

Με αυτή την εντολή εμφανίζεται συνοπτικά ο multicast πίνακας δρομολόγησης του δρομολογητή.

- **Sh ip sdr**

Παράδειγμα:
router>sh ip sdr
SAP Cache - 67 entries

ANS AI Lunch Training
Causeries du FMBone
CNR Pisa Edificio A Stanza 17
Cognitive TeraNets
CRC TV
CSPAN via Nwstrn U.
FAU - Vorlesung Informationssysteme in der Dienstleistungswirtschaft
FAU - Vorlesung Office Management Systeme
FAU - Vorlesung OR IV (Netzplanmodelle)
FAU - Vorlesung OR V (Lagerhaltungsmodelle)
FAU-TV
FREE: iab-vbrick-1
FREE: My Name
FUNET-TV 1 (H.261)
FUNET-TV Eduskuntakanava
FUNET-TV Eduskuntaradio
FUNET-TV Test channel
HAX Hamster Cam
MBone-DE Chat
Nederland1
Nederland2
Nederland3
NRK Alltid Nyheter (mp3, 56 kbit, Hxgskolen i Xstfold)
NRK mPetre radio (mp3, 24 kbit, Hxgskolen i Xstfold)
NRK mPetre radio (mp3, 56 kbit, Hxgskolen i Xstfold)
NRK P2 Radio (MP3, 128 kbit, Hxgskolen i Xstfold)
NRK P2 radio (MP3, 24 kbit, Hxgskolen i Xstfold)

NRK Petre radio (mp3, 56 kbit, Hxgskolen Xstfold)
On-The-I SSM
On-The-I.com Channel-1 160kbs MP3 Audio
On-The-I.com Channel-1 32kbs MP3 Audio
On-The-I.com Channel-1 96kbs MP3 Audio
On-The-I.com Channel-1 MP3 Audio LSM
On-The-I.com Channel-2 160kbs MP3 Audio
On-The-I.com Channel-2 32kbs MP3 Audio
On-The-I.com Channel-2 MP3 Audio LSM
On-The-I.com Drum Logic 160kbs MP3 Audio
On-The-I.com Drum Logic 32kbs MP3 Audio
On-The-I.com Drum Logic 96kbs MP3 Audio
On-The-I.com Drum Logic MP3 Audio LSM
On-The-I.com Livecast 160k
On-The-I.com Livecast 32k
On-The-I.com Livecast 96k
On-The-I.com Livecast LSM
On-The-I.tv 300k
On-The-I.tv 56k
On-The-I.tv 800k
On-The-I.tv DIVX 800k
Orpheus vehicle main camera
Places All Over Renater2
Places all over the world
RealServer address announcement
Recipnet
Seal Cam surface camera
TAC/AES Chalktalks-Catalyst 4K SupIII
TU Darmstadt SWR3
Uni-TV (Kanal 1)
Uni-TV (Kanal 2)
Uni-TV (live)
UO Broadcasts OPB's Oregon Story
UO Medical Management of Biological Casualties (1)
UO Presents KWAX Classical Radio
USA WNY-HPNVI 24/7
UW-Milwaukee
Virtuelles Seminar Bayreuth, N|rnberg, Regensburg
Warriors of the Net
WirInNRW

Με την εντολή sh ip sdr εμφανίζονται όλα τα multicast sessions που ανακοινώνονται εκείνη τη στιγμή.

- **sh ip sdr detail**

παράδειγμα:
router>sh ip sdr detail
SAP Cache - 71 entries
Session Name: Broadway Local MPEG-2
Description: recording of 1/29/02 musical theater master class
Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
Uptime: 00:00:18, Last Heard: 00:00:18
Announcement source: 128.59.31.169, destination: 224.2.127.254
Created by: - 35029 1 IN IP4 128.59.31.169
Phone number: Network Operations <+1 212-854-1919>
Email: Network Operations noc@columbia.edu
URL: http://www.columbia.edu/acis/networks/advanced/broadway_local
Media: video 61552 RTP/AVP 32

Media group: 224.2.211.27, ttl: 127
Attribute: framerate:30
Attribute: x-iptv-svr:video iptvhost.cc.columbia.edu file 1 loop
Media: audio 21300 RTP/AVP 14
Media group: 224.2.241.169, ttl: 127
Attribute: x-iptv-svr:audio iptvhost.cc.columbia.edu file 1 loop

Η παραπάνω εντολή εμφανίζει λεπτομέρειες για τα sessions που υπάρχουν εκείνη τη στιγμή.

- **sh ip msdp peer**

παράδειγμα:
router>sh ip msdp peer
MSDP Peer 194.177.xxx.xxx , AS xxxx
Description:
Connection status:
State: Up, Resets: 28, Connection source: ATM1/0.1 (194.177.xxx.xxx)
Uptime(Downtime): 1d08h, Messages sent/received: 2117/526064
Output messages discarded: 0
Connection and counters cleared 7w0d ago
SA Filtering:
Input (S,G) filter: 150, route-map: none
Input RP filter: none, route-map: none
Output (S,G) filter: 150, route-map: none
Output RP filter: none, route-map: none
SA-Requests:
Input filter: none
Sending SA-Requests to peer: disabled
Peer ttl threshold: 0
SAs learned from this peer: 2029
Input queue size: 0, Output queue size: 0

Εμφανίζει τα στοιχεία των MSDP peers του δρομολογητή, δηλαδή την IP διεύθυνση, το domain name και το AS νούμερο. Επίσης, δείχνει την κατάσταση της σύνδεσης, από ποιο interface είναι συνδεδεμένος ο δρομολογητής (στο παράδειγμα ATM1/0.1), ο χρόνος που είναι ενεργό το peer, πόσα μηνύματα έχει στείλει και πόσα έχει λάβει, καθώς και πόσα εξερχόμενα μηνύματα έχει απορρίψει. Ακόμα, εμφανίζει τα εισερχόμενα και εξερχόμενα φίλτρα που μπορεί να υπάρχουν για τα SA μηνύματα. Τέλος, δείχνει πόσα SAs μηνύματα έχουν φτάσει σε αυτό το peer.

- **sh ip msdp summary**

Παράδειγμα:
*router>**sh ip msdp summary***
MSDP Peer Status Summary

Peer Address	*AS*	*State*	*Uptime/ Downtime*	*Reset Count*	*SA Count*	*Peer Name*
194.177.xxx.xxx	*xxxx*	*Up*	*2d18h*	*17*	*2221*	*xxxxxxx*

Η εντολή sh ip msdp summary δείχνει μια σύνοψη της εντολής sh ip msdp peer.

- **sh ip msdp count**

παράδειγμα:
*router>**sh ip msdp count***
SA State per Peer Counters, <Peer>: <# SA learned>

194.177.xxx.xxx

SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 2121
?: 4/2, 14: 10/9, 17: 8/6, 18: 5/4
24: 7/4, 25: 17/8, 26: 9/4, 32: 5/5
38: 6/4, 57: 1/1, 59: 14/3, 68: 1/1
70: 2/1, 73: 12/6, 81: 6/6, 87: 15/8
88: 3/2, 102: 7/2, 103: 8/7, 109: 74/52
111: 4/3, 127: 19/13, 131: 2/1, 137: 14/13
145: 1/1, 159: 3/2, 160: 4/2, 194: 15/4
195: 2/2, 210: 12/6, 224: 27/22, 237: 24/21
291: 12/5, 292: 11/3, 293: 17/6, 297: 4/4
376: 1/1, 549: 13/10, 557: 2/2, 559: 11/6
589: 1/1, 668: 3/2, 680: 51/20, 683: 36/13
776: 7/5, 777: 2/2, 786: 40/17, 803: 14/1
818: 13/11, 1103: 175/90, 1161: 26/9, 1224: 13/10
1239: 24/20, 1653: 46/42, 1657: 8/2, 1739: 3/2
1741: 4/4, 1798: 5/4, 1930: 1/1, 1938: 1/1
2072: 2/2, 2150: 12/10, 2381: 42/5, 2496: 8/4
2553: 2/1, 2603: 1/1, 2607: 1/1, 2611: 12/10
2637: 4/4, 2701: 9/8, 2831: 95/53, 2832: 2/2
2833: 29/9, 2841: 6/6, 2843: 9/1, 2852: 13/10
3112: 5/2, 3323: 1/1, 3390: 26/25, 3582: 69/50
3676: 1/1, 3685: 9/9, 3756: 1/1, 3807: 2/2
3912: 3/2, 3948: 59/59, 4201: 4/3, 4538: 11/4
5054: 6/5, 5408: 14/7, 5466: 2/2, 5470: 2/1
5640: 6/2, 5661: 10/6, 5663: 1/1, 5779: 434/423
6200: 4/2, 6263: 8/5, 6325: 1/1, 6356: 10/5
6366: 9/8, 6509: 8/5, 6867: 11/11, 7046: 1/1
7170: 4/3, 7212: 7/3, 7539: 4/4, 7571: 2/2
7660: 3/2, 7667: 2/2, 7774: 2/2, 7896: 4/2
8071: 11/5, 8158: 4/4, 8256: 1/1, 8365: 15/7
9112: 2/2, 9270: 4/4, 9406: 16/11, 10364: 3/2
10437: 5/4, 10490: 48/29, 10755: 5/5, 11078: 1/1
11422: 1/1, 12145: 2/2, 12173: 5/3, 13476: 1/1
13778: 19/7, 14077: 1/1, 14183: 4/3, 14878: 1/1
15474: 2/1, 16430: 4/3, 16517: 24/23, 17579: 1/1
19149: 4/2, 19770: 1/1, 20080: 2/2, 20130: 23/6
20894: 9/9, 20965: 17/5, 21320: 2/2, 22168: 5/3

Η εντολή sh ip msdp count εμφανίζει πληροφορίες για τον αριθμό των πηγών και των multicast ομάδων που δημοσιεύονται μέσα σε ένα αυτόνομο σύστημα (AS). Στο παράδειγμα οι συνολικές πηγές που έχουν δημοσιευτεί μέσω του MSDP είναι 2121. Το AS 14 δημοσιεύει 10 πηγές και 9 ομάδες, το AS 17 δημοσιεύει 8 πηγές και 6 ομάδες, το AS 18 δημοσιεύει 5 πηγές και 4 ομάδες κτλ.

- **Sh ip msdp sa-cache**

Παράδειγμα:
*router>**sh ip msdp sa-cache***
MSDP Source-Active Cache - 2217 entries
(128.100.102.201, 224.0.1.1), RP 205.211.94.253, MBGP/AS 549, 2d18h/00:05:38
(128.100.174.2, 224.0.1.1), RP 205.211.94.253, MBGP/AS 549, 2d18h/00:05:38
(128.149.33.218, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37
(128.149.33.219, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37
(128.149.68.100, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37

(128.240.3.15, 224.0.1.1), RP 212.219.85.217, MBGP/AS 786, 2d18h/00:05:38
(128.240.3.137, 224.0.1.1), RP 212.219.85.217, MBGP/AS 786, 2d18h/00:05:38
(129.237.117.7, 224.0.1.1), RP 129.237.1.1, MBGP/AS 2496, 00:09:06/00:00:52
(129.237.117.9, 224.0.1.1), RP 129.237.1.1, MBGP/AS 2496, 00:08:08/00:01:50
(129.241.110.78, 224.0.1.1), RP 128.39.0.86, MBGP/AS 224, 2d18h/00:05:38
(130.37.22.50, 224.0.1.1), RP 145.145.255.6, MBGP/AS 1103, 2d18h/00:05:38
(130.37.24.1, 224.0.1.1), RP 145.145.255.6, MBGP/AS 1103, 2d18h/00:05:38
(130.83.16.70, 224.0.1.1), RP 130.83.128.3, MBGP/AS 8365, 2d18h/00:05:37
(130.83.16.72, 224.0.1.1), RP 130.83.128.3, MBGP/AS 8365, 2d18h/00:05:37
(130.83.16.78, 224.0.1.1), RP 130.83.128.3, MBGP/AS 8365, 2d18h/00:05:37
(130.89.67.100, 224.0.1.1), RP 145.145.255.14, MBGP/AS 1103, 2d18h/00:05:38
(130.207.230.13, 224.0.1.1), RP 199.77.254.253, MBGP/AS 2637, 22:29:07/00:05:38
(131.188.3.220, 224.0.1.1), RP 131.188.1.1, MBGP/AS 680, 2d18h/00:05:37
(131.188.3.221, 224.0.1.1), RP 131.188.1.1, MBGP/AS 680, 2d18h/00:05:37
(131.188.3.222, 224.0.1.1), RP 131.188.1.1, MBGP/AS 680, 2d18h/00:05:37
(131.188.3.223, 224.0.1.1), RP 131.188.1.1, MBGP/AS 680, 2d18h/00:05:37
(137.78.8.23, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37
(137.78.170.33, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37
(137.79.94.56, 224.0.1.1), RP 192.138.85.65, MBGP/AS 127, 2d18h/00:05:37
(146.246.238.3, 224.0.1.1), RP 134.55.20.229, MBGP/AS 293, 2d18h/00:05

Τα περιεχόμενα της SA active cache είναι πολύ χρήσιμα για την αντιμετώπιση MSDP προβλημάτων σε ένα δίκτυο. Για αυτό το λόγο πολλοί διαχειριστές ενεργοποιούν την SA Cashing σε όλους τους MSDP δρομολογητές. Η παραπάνω εντολή βοηθάει στην εμφάνιση των περιεχομένων της SA Cache.

Στο παράδειγμα εμφανίζονται 2217 καταχωρήσεις μέσα στην SA Cache. Οι πληροφορίες από την πρώτη καταχώρηση είναι:

- (128.100.102.201, 224.0.1.1) = πηγή / ομάδα
- RP 205.211.94.253 = IP διεύθυνση του αρχικού RP.
- MBGP/AS 549 = Το RP βρίσκεται στο AS 549
- 2d18h/00:05:38 = Η πηγή είναι ενεργή για 2 μέρες και 18 ώρες, και θα σταματήσει να είναι σε 5 λεπτά και 38 δευτερόλεπτα.

Τα περιεχόμενα της SA Cache μπορούν να διαγραφούν με την εντολή:

clear ip msdp sa-cache [<group-address> | <group-name>]

7.3 Εντολές Debug

Εκτός από τις εντολές, show πολύ σημαντικές εντολές για debugging είναι και οι εντολές **debug** (debug commands). Οι εντολές debug δίνουν πολλές πληροφορίες για την εσωτερική λειτουργία των πρωτοκόλλων και παράγουν πολύ μεγάλο αριθμό εγγραφών(logs) που επιβαρύνουν σοβαρά τον φόρτο εργασίας του δρομολογητή και την λειτουργία του δικτύου ιδιαίτερα εάν χρησιμοποιείται απομακρυσμένος log server (syslog). Για αυτό και η χρήση τους πρέπει να περιορίζεται σε δύσκολες περιπτώσεις αποσφαλμάτωσης.

- **debug ip igmp**

παράδειγμα:

router#debug ip igmp
May 17 11:34:45 router-xx..ariadne-t.gr 54737: May 17 11:34:04.478 EET: IGMP: Received v2 Report from 143.233.41.10 (Fa0.41) for 224.0.1.12
May 17 11:34:47 router-xx.ariadne-t.gr 54738: May 17 11:34:06.478 EET: IGMP: Received v2 Report from 143.233.41.10 (Fa0.41) for 224.0.1.11

May 17 11:34:49 router-xx..ariadne-t.gr 54739: May 17 11:34:08.482 EET: IGMP: Received v2 Report from 143.233.41.10 (Fa0.41) for 224.2.252.33
May 17 11:34:49 router-xx.ariadne-t.gr 54740: May 17 11:34:08.482 EET: IGMP: Received v2 Report from 143.233.41.10 (Fa0.41) for 224.2.163.249

Με την εντολή debug ip igmp εμφανίζονται τα IGMP ερωτήματα (queries) και αναφορές (report) που στέλνονται και λαμβάνονται από τον δρομολογητή. Στο παράδειγμα ο δρομολογητής router στις 17 Μαΐου και ώρα 11:34:45 έλαβε ένα IGMPv2 report από τον host 143.233.41.10 μέσω του interface Fa0.41 για την multicast ομάδα 224.0.1.12. Από το επόμενο IGMP report που θα σταλεί από την ίδια μηχανή για το ίδιο group, μπορεί να ανακαλυφτεί το χρονικό διάστημα μεταξύ δύο reports.

- **debug ip mroute**

παράδειγμα:
router#debug ip mrouting
May 17 12:34:07 router-xx.ariadne-t.gr 56294: May 17 12:33:26.735 EET: MRT: Update (, 224.0.1.60), RPF Null, PC 0x6042F03C*
May 17 12:34:07 router-xx.ariadne-t.gr 56295: May 17 12:33:26.739 EET: MRT: Update (, 224.0.1.60), RPF Null, PC 0x6042F03C*
May 17 12:34:08 router-xx.ariadne-t.gr 56296: May 17 12:33:27.775 EET: MRT: Create (193.50.192.71/32, 224.2.127.254), RPF Ethernet0/143.233.100.50, PC 0x604373EC
May 17 12:34:31 router-xx.ariadne-t.gr 56297: May 17 12:33:50.895 EET: MRT: Delete (63.105.122.14/32, 224.2.127.254), PC 0x60439DE8
May 17 12:34:33 router-xx.ariadne-t.gr 56298: May 17 12:33:52.899 EET: MRT: Delete (207.75.164.44/32, 224.2.127.254), PC 0x6043

Με την εντολή debug ip mroute μπορεί να γίνει παρακολούθηση της κατάστασης του multicast πίνακα δρομολόγησης. Εμφανίζονται, δηλαδή, οι δημιουργίες, οι διαγραφές και οι ενημερώσεις που γίνονται στον πίνακα. Στο παράδειγμα στο δρομολογητή router στις 17 Μαΐου και ώρα 12:34:08 δημιουργήθηκε η (193.50.192.71/32, 224.2.127.254) καταχώρηση και έχει RPF interface το Ethernet 0/1 και RP των 143.233.100.50.

- **Debug ip pim**

Παράδειγμα:
router#debug ip pim
May 17 12:43:28 router-xx.ariadne-t.gr 57252: May 17 12:42:48.422 EET: PIM: For RP, Join-list: 143.233.254.29/32, RP-bit, WC-bit
May 17 12:43:28 router-xx.ariadne-t.gr 57253: May 17 12:42:48.422 EET: PIM: For RP, Prune-list: 143.233.41.10/32, RP-bit
May 17 12:43:29 router-xx.ariadne-t.gr 57254: May 17 12:42:48.422 EET: PIM: Send periodic Join/Prune to RP via 143.233.100.50 (Ethernet0)
May 17 12:43:29 router-xx.ariadne-t.gr 57255: May 17 12:42:48.422 EET: PIM: Send Join on Ethernet0 to 143.233.100.50 for (193.2.1.230/32, 224.2.127.254), S-bit
May 17 12:43:29 router-xx.ariadne-t.gr 57256: May 17 12:42:48.426 EET: PIM: Building Join/Prune message for 224.0.1.40
May 17 12:43:29 router-xx.ariadne-t.gr 57257: May 17 12:42:48.426 EET: PIM: For RP, Join-list: 143.233.254.29/32, RP-bit, WC-bit
May 17 12:43:29 router-xx.ariadne-t.gr 57258: May 17 12:42:48.426 EET: PIM: Send periodic Join/Prune to RP via 143.233.100.50 (Ethernet0)
May 17 12:43:30 router-xx.ariadne-t.gr 57259: May 17 12:42:50.242 EET: PIM: Send Join on Ethernet0 to 143.233.100.50 for (128.59.31.169/32, 224.2.127.254), S-bit

May 17 12:43:30 router-xx.ariadne-t.gr 57260: May 17 12:42:50.486 EET: PIM: Building Join/Prune message for 224.2.163.249
May 17 12:43:30 router-xx.ariadne-t.gr 57261: May 17 12:42:50.486 EET: PIM: For RP, Join-list: 143.233.254.29/32, RP-bit, WC-bit
May 17 12:43:30 router-xx.ariadne-t.gr 57262: May 17 12:42:50.486 EET: PIM: For RP, Join-list: 128.223.230.9/32
May 17 12:43:30 router-xx.ariadne-t.gr 57263: May 17 12:42:50.486 EET: PIM: For RP, Prune-list: 143.233.41.10/32, RP-bit
May 17 12:43:30 router-xx.ariadne-t.gr 57264: May 17 12:42:50.486 EET: PIM: Send periodic Join/Prune to RP via 143.233.100.50 (Ethernet0)
May 17 12:43:30 router-xx.ariadne-t.gr 57265: May 17 12:42:50.582 EET: PIM: Received Join/Prune on Ethernet0 from 143.233.28.7, not to us
May 17 12:43:30 router-xx.ariadne-t.gr 57266: May 17 12:42:50.582 EET: PIM: Prune-list: (128.59.31.169/32, 224.2.127.254)
May 17 12:43:31 router-xx.ariadne-t.gr 57267: May 17 12:42:50.582 EET: PIM: Set join delay timer to 3 seconds for (128.59.31.169/32, 224.2.127.254) on Ethernet0

Με την εντολή debug ip pim εμφανίζονται όλα τα PIM μηνύματα που στέλνει ο δρομολογητής. Αυτά είναι:

- μηνύματα-ερωτήματα για την ανακάλυψη των γειτονικών δρομολογητών
- Join και prune μηνύματα προς το RP
- Register και register-stop μηνύματα προς το RP.

- **debug ip msdp**

Παράδειγμα:
May 20 16:36:19 router-fa0-0.ariadne-t.gr 56708: 10w3d: MSDP: 194.177.209.189: Received 120-byte msg 17767677 from peer (1)
May 20 16:36:19 router-fa0-0.ariadne-t.gr 56709: 10w3d: MSDP: 194.177.209.189: SA TLV, len: 120, ec: 1, RP: 140.192.248.248, with data (2)
May 20 16:36:19 router-fa0-0.ariadne-t.gr 56710: 10w3d: MSDP: 194.177.209.189: Peer RPF check passed for 140.192.248.248, used MBGP peer (3)
May 20 16:36:23 router-fa0-0.ariadne-t.gr 56711: 10w3d: MSDP: (140.192.250.250/32 224.5.5.5/32), accepted (4)
May 20 16:36:23 router-fa0-0.ariadne-t.gr 56712: 10w3d: MSDP: 193.78.84.1: Forward 53-byte SA to peer (5)
May 20 16:36:25 router-fa0-0.ariadne-t.gr 56714: 10w3d: MSDP: 194.177.209.189: Received 52-byte msg 17767679 from peer
May 20 16:36:25 router-fa0-0.ariadne-t.gr 56715: 10w3d: MSDP: 194.177.209.189: SA TLV, len: 52, ec: 1, RP: 129.130.167.97, with data
May 20 16:36:25 router-fa0-0.ariadne-t.gr 56716: 10w3d: MSDP: 194.177.209.189: Peer RPF check passed for single peer
May 20 16:36:26 router-fa0-0.ariadne-t.gr 56717: 10w3d: MSDP: 194.177.209.189: Received 707-byte msg 17767680 from peer
May 20 16:36:26 router-fa0-0.ariadne-t.gr 56718: 10w3d: MSDP: 194.177.209.189: SA TLV, len: 707, ec: 1, RP: 145.145.255.6, with data
May 20 16:36:26 router-fa0-0.ariadne-t.gr 56719: 10w3d: MSDP: 194.177.209.189: Peer RPF check passed for single peer
May 20 16:36:28 router-fa0-0.ariadne-t.gr 56720: 10w3d: MSDP: 194.177.209.189: Received 577-byte msg 17767681 from peer
May 20 16:36:28 router-fa0-0.ariadne-t.gr 56721: 10w3d: MSDP: 194.177.209.189: SA TLV, len: 577, ec: 1, RP: 156.56.250.3, with data
May 20 16:36:28 router-fa0-0.ariadne-t.gr 56722: 10w3d: MSDP: 194.177.209.189: Peer RPF check passed for single peer
May 20 16:36:28 router-fa0-0.ariadne-t.gr 56723: 10w3d: MSDP: Forward decapsulated SA data for (129.79.85.45, 224.2.127.254) on FastEthernet0/0 (6)

Η εντολή debug ip msdp χρησιμοποιείται για την εξακρίβωση της ανταλλαγής μηνυμάτων και την εμφάνιση των αποτελεσμάτων του RPF ελέγχου που πραγματοποιείται κάθε φορά που λαμβάνεται ένα SA μήνυμα.

Από το παράδειγμα φαίνονται τα εξής debugging μηνύματα:

(1) Έλαβε ένα μήνυμα 120 byte από το MSDP peer 194.177.209.189.

(2) Αυτό το MSDP μήνυμα ήταν ένα SA που δημιουργήθηκε από το RP με IP διεύθυνση 140.192.248.248. Περιέχει επίσης ενσωματωμένα multicast πακέτα.

(3) Ο RPF έλεγχος ήταν επιτυχημένος και επίσης το MSDP peer = με το MBGP neighbor.

(4) Τα περιεχόμενα του SA μηνύματος περιέχουν μια (S,G) δημοσιοποίηση της πηγής για το (140.192.250.250/32 224.5.5.5/32).

7.4 Άλλες Χρήσιμες debugging IOS Εντολές

- **mrinfo**

παράδειγμα:

```
router>mrinfo
143.233.100.40 (router-xx.ariadne-t.gr) [version cisco 11.3] [flags: PMSA]:
  143.233.100.40 -> 143.233.28.3 (RB3-xx.ariadne-t.gr) [1/0/pim]
  143.233.100.40 -> 143.233.28.7 (RB7-xx-0.ariadne-t.gr) [1/0/pim]
  143.233.100.40 -> 143.233.100.50 (ROUTER-fa0-0.ariadne-t.gr) [1/0/pim]
  143.233.247.1 -> 0.0.0.0 [1/0/pim/querier/leaf]
  143.233.5.5 -> 0.0.0.0 [1/0/pim/querier/leaf]
  143.233.41.1 -> 0.0.0.0 [1/0/pim/querier/leaf]
```

Εντολή που δείχνει τους γειτονικούς multicast routers.

- **Ping**

Παράδειγμα:

```
router#ping 224.2.232.59

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.2.232.59, timeout is 2 seconds:

Reply to request 0 from 143.233.42.20, 16 ms
Reply to request 0 from l4.grnet.gr (194.177.210.227), 84 ms
Reply to request 0 from l4.grnet.gr (194.177.210.227), 84 ms
Reply to request 0 from 143.233.42.20, 76 ms
Reply to request 0 from 143.233.42.20, 76 ms
Reply to request 0 from l4.grnet.gr (194.177.210.227), 76 ms
Reply to request 0 from 143.233.42.20, 72 ms
Reply to request 0 from 143.233.42.20, 72 ms
                    Reply to request 0 from 143.233.42.20, 68 ms
Reply to request 0 from l4.grnet.gr (194.177.210.227), 64 ms
```

Η εντολή ping είναι ο ευκολότερος τρόπος για να δημιουργηθεί multicast traffic σε ένα δίκτυο και για να γίνει test του multicast δέντρου που

χτίζεται. Η χρήση της ping προϋποθέτει ότι υπάρχει μια ομάδα στην οποία συμμετέχουν οι δρομολογητές που μας ενδιαφέρει να ελέγξουμε, αυτή η συνθήκη μπορεί να επιτευχθεί με την διαδικασία της παραγράφου 6.2.5

7.5 Debugging Software Εργαλεία

Εκτός από τις εντολές του IOS που αναφέραμε, υπάρχουν αρκετά χρήσιμα multicast debugging software εργαλεία, που μπορούν να εγκατασταθούν σε ένα σταθμό εργασίας (Unix ή windows) και να παρέχουν σημαντική βοήθεια στην ανακάλυψη προβλημάτων. Τέτοια γνωστά εργαλεία είναι το MRM (Multicast Reachability Monitoring Protocol), το Mantra, το MHealth, το Mlisten, το Mrouted, το Mtrace, το sdr monitor, το Mwalk και το Multicast Beacon. Στη συνέχεια θα αναλύσουμε τη λειτουργία του MHealth.

7.5.1 MHealth

Το Mhealth είναι ένα γραφικό εργαλείο παρακολούθησης της multicast τοπολογίας. Σχεδιάστηκε για να καλύψει την ανάγκη για multicast debugging με ενέργειες που γίνονται πάνω σε σταθμό εργασίας και όχι πάνω σε δρομολογητή και είναι σχεδόν πραγματικού χρόνου. Το MHealth χρησιμοποιεί άλλα υπάρχοντα εργαλεία για να συλλέξει δεδομένα για sessions ήχου και εικόνας που βασίζονται στο Real-Time Protocol. Χρησιμοποιώντας ένα συνδυασμό από ένα πρωτόκολλο επιπέδου εφαρμογής για τις πληροφορίες των συμμετεχόντων και ένα multicast εργαλείο ανακάλυψης της διαδρομής για πληροφορίες τοπολογίας, το MHealth είναι ικανό να παρέχει μια multicast tree τοπολογία και πληροφορίες για την ποιότητα των συνδέσεων. Για το διαχειριστή ενός δικτύου ένα τέτοιο εργαλείο είναι πολύ χρήσιμο, γιατί είναι απαραίτητο να γνωρίζει αν το multicast traffic και τα δέντρα είναι “healthy” π.χ αν η κίνηση σε ένα group είναι αποδεκτής ποιότητας και αν το traffic φτάνει σε όλα τα μέλη του group και μόνο σε αυτά.

7.5.1.1 Ο τρόπος λειτουργίας του Mhealth

Το multicasting χρησιμοποιεί το UDP σαν πρωτόκολλο μεταφοράς. Εδώ όμως προκύπτει αυτόματα το εξής ερώτημα. Με ποιο τρόπο μπορούν να σταλούν πραγματικού χρόνου δεδομένα με multicast χωρίς καμιά από τις υπηρεσίες του TCP; Χωρίς connection-oriented τελικά σημεία για προώθηση δεδομένων, είναι δύσκολο να ανακαλυφθούν οι αποδέκτες ενός multicast stream και οι δρόμοι που τα δεδομένα πρέπει να ακολουθήσουν προκειμένου να φτάσουν στους αποδέκτες αυτούς. Επίσης, η real-time μεταφορά έχει πολύ ειδικές απαιτήσεις που ούτε το TCP μπορεί να παρέχει και, επειδή τα δεδομένα πρέπει να μεταφερθούν με τη μεγαλύτερη δυνατή ακρίβεια, απαιτείται επανεκπομπή των χαμένων πακέτων. Σα λύση του παραπάνω προβλήματος, τα δεδομένα πραγματικού χρόνου (unicast και multicast) χρησιμοποιούν ένα πρωτόκολλο επιπέδου εφαρμογής (Application Level Protocol), που ονομάζεται και Application Layer Framing (ALF). Ένα ALF πρωτόκολλο μπορεί να αποκτήσει τις ιδιότητες ενός ενδιάμεσου πρωτοκόλλου μεταξύ των πρωτοκόλλων του επιπέδου εφαρμογής και αυτών του επιπέδου μεταφοράς.

Ένα από τα πιο γνωστά ALF πρωτόκολλα που χρησιμοποιούνται για την real-time μεταφορά audio και video είναι το Real Time Protocol (RTP). Το RTP χρησιμοποιείται από τα εργαλεία του IP multicast αλλά και από άλλα streaming tools. Το πρωτόκολλο αυτό τρέχει πάνω από το UDP και παρέχει το είδος των δεδομένων, μια σειρά αρίθμησης και τη χρονική στιγμή μεταφοράς. Επίσης, περιέχει ένα πρωτόκολλο ελέγχου που λέγεται Real Time Control Protocol (RTCP), το οποίο επιτρέπει στους συμμετέχοντες σε ένα multicast group να αναφέρουν ότι είναι μέλη, ενώ επίσης παρέχει την ποιότητα της σύνδεσης τους.

Δύο είναι οι βασικές οντότητες από τις οποίες μπορεί ο χρήστης να λάβει πληροφορίες για ένα multicast group, οι δρομολογητές και οι συμμετέχοντες σε αυτό, τις οποίες το MHealth ενσωματώνει. Οι δρομολογητές μπορούν να ρωτηθούν από το Mhealth με τη βοήθεια ενός εργαλείου, όμοιου με το traceroute του unicasting, το mtrace. Επίσης, το MHealth βασίζεται στα RTCP πακέτα για να ανακαλύψει τη συμμετοχή σε μια multicast ομάδα και την ποιότητα της σύνδεσης για κάθε συμμετέχοντα.

7.5.1.2 Real Time Control Protocol

Το Real Time Control Protocol είναι ένα μέρος του Real Time Protocol. Το RTP κομμάτι εφαρμόζεται σε επίπεδο εφαρμογής framing για δεδομένα πραγματικού χρόνου, παρέχοντας το είδος των δεδομένων, τη σειρά αρίθμησης και το χρόνο. Το RTCP κομμάτι του πρωτοκόλλου είναι μια περιοδική μεταφορά πακέτων ελέγχου από όλους τους συμμετέχοντες σε όλους τους άλλους συμμετέχοντες στο session. Στο multicasting, τα RTCP πακέτα συνήθως στέλνονται στην ίδια multicast διεύθυνση με τα RTP δεδομένα, αλλά σε διαφορετική UDP πόρτα. Τυπικά αν η πόρτα δεδομένων είναι *κ* τότε η πόρτα για τα πακέτα ελέγχου είναι *κ+1*.

Το RTCP έχει τέσσερις λειτουργίες. Πρώτον, παρέχει πληροφορίες για την ποιότητα της μεταφοράς δεδομένων στο multicast group. Δεύτερον, μεταφέρει πακέτα που αναγνωρίζουν μια RTP πηγή, τα οποία λέγονται *canonical name.* Τρίτον, χρησιμοποιείται από κάθε συμμετέχοντα για να υπολογίσει το μέγεθος του group. Τέταρτον, διανέμει πληροφορίες για τη συμμετοχή στα group.

Το RTCP πακέτο αποτελείται από ένα ή περισσότερα τμήματα. Τα τμήματα-κλειδιά που χρησιμοποιούνται από το MHealth περιέχουν τα παρακάτω: την αναφορά του αποστολέα, την αναφορά του παραλήπτη, την περιγραφή της πηγής και το BYE τμήμα.

Είναι πολύ πιθανό οι παραλήπτες να μη λάβουν όλα τα RTCP πακέτα και αυτό οφείλεται εν μέρει στην παρεμβολή των firewalls, στην απώλεια των UDP πακέτων και στην ασυμβατότητα των εργαλείων με τα χαρακτηριστικά του RTP. Πάντως, τα RTCP πακέτα είναι ο μόνος τρόπος να ανακαλυφτεί η συμμετοχή ενός multicast session σε ένα group χωρίς να γίνει χρήση των στατιστικών των δρομολογητών. Γενικά, το RTCP είναι ο καλύτερος διαθέσιμος τρόπος για ένα εργαλείο όπως το MHealth.

7.5.1.3 Η Λειτουργία του Mtrace

Μόλις εξακριβωθούν οι συμμετέχοντες σε ένα multicast session, πρέπει να ανακαλυφθεί η τοπολογία. Το mtrace, μια multicast έκδοση του traceroute, μπορεί να δώσει αυτήν την πληροφορία. Ένα από τα αρνητικά του

mtrace είναι ότι δίνει το δρόμο μόνο από ένα αποδέκτη προς την πηγή. Έτσι, το MHealth πρέπει να εκτελέσει πολλά mtraces, ένα για κάθε παραλήπτη του session. Στη συνέχεια, το MHealth σχηματίζει το δέντρο ως αποτέλεσμα του συνδυασμού των κοινών σημείων, που βρίσκονται από το mtrace.

Δίνοντας μερικές επιπλέον πληροφορίες για το mtace, θα πρέπει να πούμε ότι πρόκειται για ένα χρήσιμο εργαλείο που βοηθάει στη διάγνωση των IP multicast προβλημάτων δρομολόγησης, καθώς επίσης και στη στατιστική επεξεργασία τους. Εφαρμόζεται στους multicast δρομολογητές με τη βοήθεια μιας επέκτασης του IGMP και έχει τη δυνατότητα να χαράζει δρόμους μεταξύ πηγής και αποδέκτη.

Ένα trace ερώτημα οδηγείται από δρομολογητή σε δρομολογητή μέσω του αντίστροφου δρόμου από τον αποδέκτη στην πηγή, συλλέγοντας IP διευθύνσεις, πληροφορίες για τον αριθμό των πακέτων που χάνονται και προβλήματα δρομολόγησης. Στη συνέχεια, τα στοιχεία αυτά περιέχονται σε μια απάντηση, η οποία και επιστρέφεται στο χρήστη του MHealth.

Για να τρέξει το mtrace, η μόνη παράμετρος που απαιτείται είναι το όνομα ή IP διεύθυνση της πηγής. Ο default αποδέκτης είναι η μηχανή που τρέχει το mtrace και το default group είναι το 0.0.0.0. Τα στοιχεία αυτά αρκούν στην περίπτωση που δεν απαιτούνται στατιστικά στοιχεία για τα πακέτα που χάνονται για μια συγκεκριμένη multicast ομάδα. Οι δύο όμως αυτοί προαιρετικοί παράμετροι πρέπει οπωσδήποτε να οριστούν, στην περίπτωση που αναφερόμαστε σε άλλο αποδέκτη (όχι τη μηχανή που τρέχει το mtrace) και σε κάποια συγκεκριμένη ομάδα. Επίσης, ξεχωρίζουν γιατί η διεύθυνση του αποδέκτη είναι unicast ενώ του group είναι multicast.

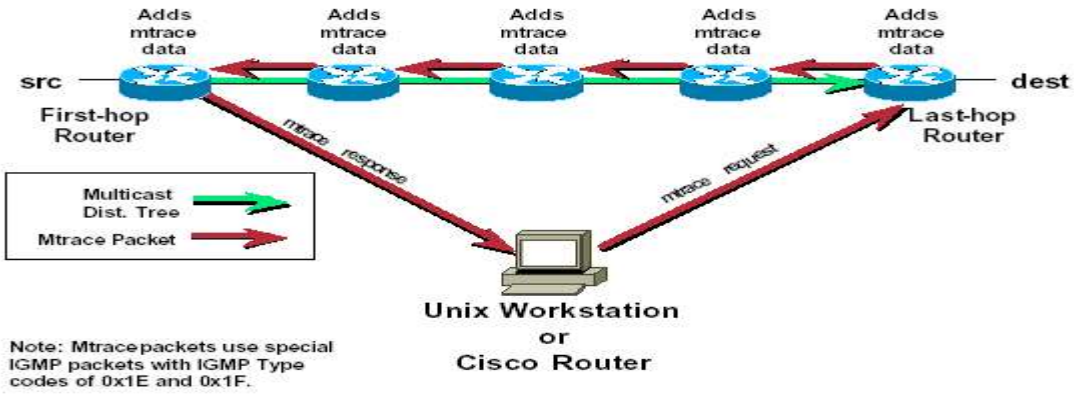
Αν η –g flag είναι καθορισμένη, η πηγή είναι ο host που τρέχει το mtrace και αποδέκτης ο δρομολογητής που καθορίζεται μαζί με το –g flag. Οι απαντήσεις γίνονται multicast στην ip διεύθυνση 224.0.1.32.

Παρά το γεγονός ότι η έξοδος από το mtrace είναι ανάλογη με αυτήν του traceroute, ο tracing μηχανισμός είναι εντελώς διαφορετικός. Ένα unicast traceroute στέλνει μια σειρά από πακέτα με αυξανόμενο TTL. Μόλις το TTL λήξει, ένα ICMP πακέτο, που δείχνει το δρομολογητή στον οποίο το TTL έληξε, επιστρέφεται στην πηγή. Έτσι, από τα ICMP μηνύματα μπορεί να εκτιμηθεί ο δρόμος από την πηγή στον προορισμό. Μια από τις πιο σημαντικές διαφορές μεταξύ mtrace και traceroute είναι ότι το πρώτο επιτρέπει από τρίτο μέλος (μηχανή που δεν συμμετέχει στο session) να κάνει mtrace.

Αφού το multicasting χρησιμοποιεί το reverse path forwarding, το ίχνος (trace) σχηματίζεται προς τα πίσω από τον αποδέκτη στην πηγή. Ένα trace query πακέτο (IGMP) στέλνεται στο last hop multicast δρομολογητή. Στην πραγματικότητα γίνεται multicast στην ALL-ROUTERS multicast διεύθυνση (224.0.0.2). Ο δρομολογητής αυτός φτιάχνει ένα trace request πακέτο, που περιέχει στοιχεία για το δικό του hop και το οποίο προωθεί unicast στο δρομολογητή που πιστεύει ότι είναι το προηγούμενο hop για τα πακέτα που δημιουργούνται από τη συγκεκριμένη πηγή. Κάθε δρομολογητής κατά μήκος του δρόμου προσθέτει τα στοιχεία που αφορούν το δικό του hop και προωθεί το πακέτο. Όταν το trace request πακέτο φτάσει στον first hop δρομολογητή (ο δρομολογητής που είναι πρώτος από την πηγή), αυτός στέλνει την ολοκληρωμένη απάντηση (response packet) σε μια καθορισμένη, από το trace query πακέτο, διεύθυνση. Αν ένας δρομολογητής κατά μήκος του reverse path έχει πρόβλημα στην επικοινωνία με τον upstream δρομολογητή, ο δημιουργός του mtrace θα στείλει τα trace δεδομένα πάνω από αυτό το

σημείο. Αν ο δρομολογητής δεν μπορεί να βρεθεί μέσα σε ένα χρονικό διάστημα, το mtrace θα τελειώσει και θα βγάλει ένα μήνυμα λάθους.

Όταν για πρώτη φορά το MHealth έτρεξε σε μεγάλα groups, υπήρχαν πολλά αποτυχημένα mtraces. Για αυτό το λόγο οι νέες εκδόσεις του MHealth πραγματοποιούν πάνω από τρία διαφορετικά mtraces για κάθε αποδέκτη πριν συνεχίσουν στον επόμενο. Αρχικά γίνεται το γνωστό mtrace από ένα αποδέκτη στην πηγή. Αν αυτό αποτύχει, ένα *gateway mtrace* πραγματοποιείται. Ένας από τους αρχικούς λόγους που το αρχικό mtrace αποτυγχάνει είναι γιατί το *Query* δεν μπορεί να βρει το last hop δρομολογητή. Αν ο δημιουργός του mtrace δεν ξέρει το last hop δρομολογητή, τον ανακαλύπτει κάνοντας mtrace από την μηχανή που τρέχει το MHealth στον παραλήπτη. Τέλος, αν το gateway mtrace αποτύχει, γίνεται ένα τελικό mtrace από την πηγή στον παραλήπτη. Η εικόνα 7.1 δείχνει την λειτουργία του mtrace.



Εικόνα 7.1

Παραθέτοντας ένα παράδειγμα, θα λέγαμε ότι τα αποτελέσματα που το mtrace βγάζει στην οθόνη χωρίζονται σε δύο μέρη. Το πρώτο είναι μια μικρή λίστα από τα hops με τη σειρά που ρωτούνται οι δρομολογητές, η οποία είναι η αντίθετη από τη σειρά, με την οποία μεταφέρονται τα data από την πηγή στον αποδέκτη.

Για κάθε hop τυπώνεται μια σειρά που δείχνει το νούμερό του (μετριέται αρνητικά για να δείξει ότι είναι ο αντίθετος δρόμος), το multicast πρωτόκολλο δρομολόγησης (DVMRP, MOSPF, PIM etc.), το όριο που απαιτείται για να γίνει η προώθηση των πακέτων και, τέλος, τη συνολική καθυστέρηση προκειμένου να φτάσει το query πακέτο σε αυτό το hop (υπάρχει μόνο αν τα ρολόγια είναι συγχρονισμένα). Αν κάποια από τις γραμμές τυπώσει “default” σημαίνει ότι ο δρομολογητής δεν έχει multicast route για αυτή την πηγή και βγάζει το unicast default route που είναι πιθανό να μην είναι το σωστό για mtrace.

Αυτό το μέρος τελειώνει με μια γραμμή που μας δείχνει το χρόνο που απαιτείται από την στιγμή που γίνεται το query μέχρι να δοθεί απάντηση. Και οι δύο αυτές τιμές του χρόνου δίνονται από το τοπικό ρολόι του συστήματος. Επίσης η γραμμή αυτή δείχνει το συνολικό ttl που απαιτείται για ένα πακέτο να ταξιδέψει από αυτό το path. Παρακάτω βλέπουμε τα αποτελέσματα του mtrace από τον αποδέκτη 128.26.0.170 στην πηγή 18.26.0.170 μέσω του group 224.2.0.3

oak.isi.edu 80# mtrace -l caraway.lcs.mit.edu 224.2.0.3
Mtrace from 18.26.0.170 to 128.9.160.100 via group 224.2.0.3

Querying full reverse path...
0 oak.isi.edu (128.9.160.100)
-1 cub.isi.edu (128.9.160.153) PIM-SM thresh^ 1 3 ms
-2 la.dart.net (140.173.128.1) PIM-SM thresh^ 1 14 ms
-3 dc.dart.net (140.173.64.1) PIM-SM thresh^ 1 50 ms
-4 bbn.dart.net (140.173.32.1) PIM-SM thresh^ 1 63 ms
-5 mit.dart.net (140.173.48.2) PIM-SM thresh^ 1 71 ms
-6 caraway.lcs.mit.edu (18.26.0.170)
Round trip time 124 ms

Το δεύτερο μέρος δείχνει εικονογραφημένα το δρόμο που ακολουθούν τα δεδομένα. Τα βέλη που δείχνουν προς τα κάτω, δείχνουν την κατεύθυνση της απάντησης, ενώ τα βέλη που δείχνουν προς τα πάνω δείχνουν το δρόμο που ακολουθεί το query πακέτο.

Για κάθε hop φαίνεται η διεύθυνση της εισόδου και εξόδου του δρομολογητή, μαζί με το ttl που απαιτείται για να φτάσει το πακέτο σε αυτό το hop, καθώς επίσης και η καθυστέρηση μέσα στο hop που δείχνει ότι οι δρομολογητές έχουν συγχρονισμένο ρολόι στις δύο άκρες τους. Το μεσαίο δεξιά μέρος της οθόνης έχει δύο set από στατιστικά. Το πρώτο περιέχει το μέσο ρυθμό μετάδοσης για όλη την κίνηση σε κάθε hop, ενώ το δεύτερο τον αριθμό των χαμένων πακέτων, τον αριθμό των πακέτων που έχουν σταλεί, το ποσοστό των χαμένων πακέτων, καθώς και το μέσο ρυθμό μετάδοσης σε κάθε hop. Στην συνέχεια, βλέπουμε το δεύτερο μέρος των αποτελεσμάτων για την ίδια πηγή και τον ίδιο αποδέκτη με προηγούμενα.

Waiting to accumulate statistics... Results after 101 seconds:

Source Response Dest Packet Statistics For Only For Traffic
18.26.0.170 128.9.160.100 All Multicast Traffic From 18.26.0.170
| __/ rtt 125 ms Lost/Sent = Pct Rate To 224.2.0.3
v / hop 65 ms ---------- ----------
18.26.0.144
140.173.48.2 mit.dart.net
| ^ ttl 1 0/6 = --% 0 pps 0/2 = --% 0 pps
v | hop 8 ms 1/52 = 2% 0 pps 0/18 = 0% 0 pps
140.173.48.1
140.173.32.1 bbn.dart.net
| ^ ttl 2 0/6 = --% 0 pps 0/2 = --% 0 pps
v | hop 12 ms 1/52 = 2% 0 pps 0/18 = 0% 0 pps
140.173.32.2
140.173.64.1 dc.dart.net
| ^ ttl 3 0/271 = 0% 27 pps 0/2 = --% 0 pps
v | hop 34 ms -1/2652 = 0% 26 pps 0/18 = 0% 0 pps
140.173.64.2
140.173.128.1 la.dart.net
| ^ ttl 4 -2/831 = 0% 83 pps 0/2 = --% 0 pps
v | hop 11 ms -3/8072 = 0% 79 pps 0/18 = 0% 0 pps
140.173.128.2

128.9.160.153 cub.isi.edu
| __ ttl 5 833 83 pps 2 0 pps
v \\ hop -8 ms 8075 79 pps 18 0 pps
128.9.160.100 128.9.160.100
Receiver Query Source

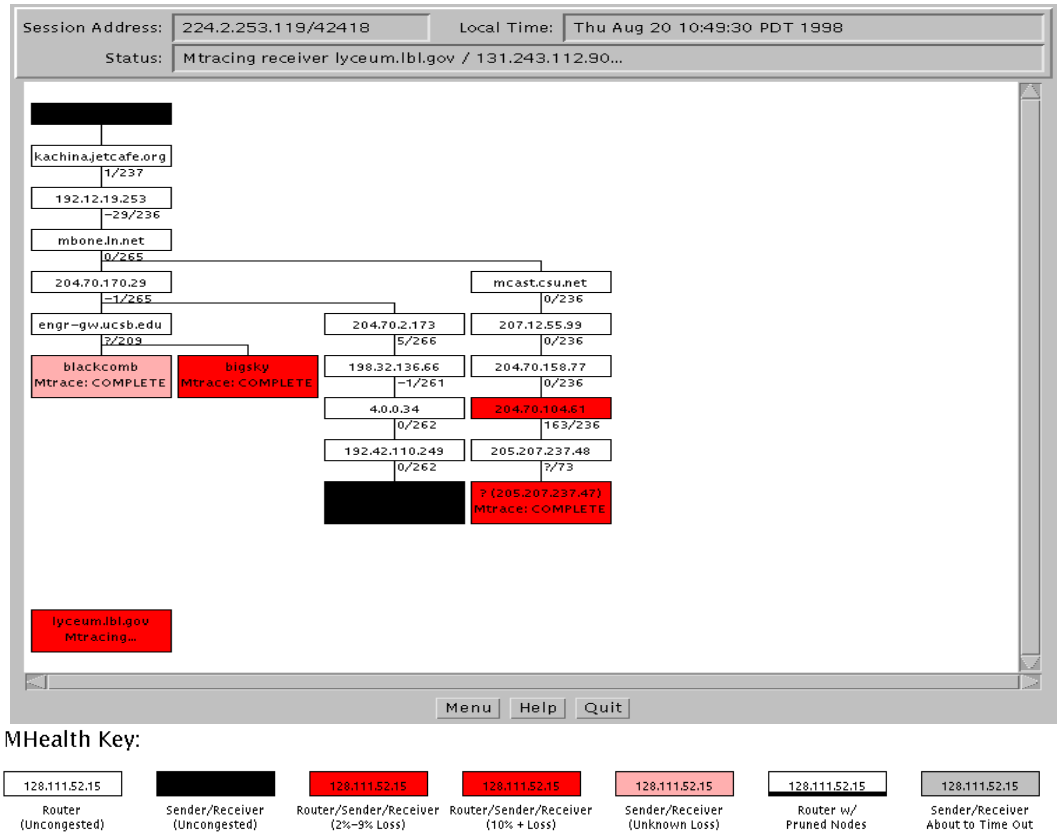
7.5.1.4 User Interface

Το user interface του MHealth είναι γραμμένο σε java. Όταν ο χρήστης τρέξει το MHealth, δίνει μια multicast IP διεύθυνση και ένα νούμερο πόρτας στην γραμμή εντολών ή στο αρχικό μενού. Επίσης σε αυτό το σημείο έχει την επιλογή να ενεργοποιήσει logging, δηλαδή να ορίσει ένα αρχείο όπου θα γραφούν όλα τα λαμβανόμενα RTCP πακέτα και τα mtraces που γίνονται στο session. Στη συνέχεια, το MHealth αρχίζει να παρακολουθεί τα RTCP πακέτα και βάσει αυτών φτιάχνει μια λίστα από πηγές και παραλήπτες. Οι πηγές εμφανίζονται στο πάνω μέρος της οθόνης και οι αποδέκτες στο κάτω, από αριστερά προς τα δεξιά με τη σειρά που εντοπίστηκαν. Το domain όνομα ενός host εμφανίζεται μόνο αν χωράει στο κουτί. Διαφορετικά εμφανίζεται η IP διεύθυνση. Τα κουτιά που αντιπροσωπεύουν ένα host χρωματίζονται ανάλογα με το ποσοστό των χαμένων πακέτων. Αυτό ανανεώνεται με κάθε RTCP πακέτο που λαμβάνεται.

Μόλις το MHealth έχει μια λίστα από πηγές και παραλήπτες, μπορεί να αρχίζει να χτίζει το multicast δέντρο. Όταν ένας δρόμος ανακαλυφθεί, σχηματίζεται γραφικά στην οθόνη. Στατιστικά των χαμένων πακέτων γράφονται κάτω από κάθε hop. Συγκεκριμένα δίνεται ένα κλάσμα που αποτελεί το λόγο των χαμένων πακέτων προς τα συνολικά που έστειλε η πηγή. Οι δρομολογητές παίρνουν τα ίδια χρώματα με τους hosts με την διαφορά ότι αν έχουν μικρές απώλειες παίρνουν άσπρο και όχι πράσινο.

Είναι πιθανό το mtrace να δείξει αρνητικό αριθμό χαμένων πακέτων όπως π.χ –5/265. Αυτό σημαίνει ότι ο δρομολογητής έλαβε 270 πακέτα ενώ περίμενε 265. Τα παραπάνω πακέτα οφείλονται σε άσκοπη αντιγραφή τους. Πρέπει να σημειωθεί ότι αρνητικό αποτέλεσμα μπορεί να κρύβει χαμένα δεδομένα π.χ το –5/265 μπορεί να σημαίνει ότι χάθηκαν 10 πακέτα και ξαναδημιουργήθηκαν 15.

Η παρακάτω εικόνα δείχνει το user interface του MHealth. Όταν το MHealth κάνει mtrace για όλους τους αποδέκτες ξεκινάει από την αρχή.



Εικόνα 7.2

Όσο τρέχει το Mhealth, η συμμετοχή των αποδεκτών στην ομάδα κι επομένως η τοπολογία μπορεί να αλλάξει. Αν νέα RTCP πακέτα ληφθούν από το MHealth, νέοι αποδέκτες προστίθενται στο κάτω μέρος του παραθύρου και το mtrace ενεργοποιείται ξανά. Αν ένα RTCP BYE πακέτο φτάσει, ο παραλήπτης και ο δρόμος που δημιουργήθηκε για αυτόν αφαιρείται.

7.5.1.5. Αλληλεπίδραση Χρήστη με MHealth

Το MHealth έχει τη δυνατότητα να δέχεται δεδομένα από το χρήστη. Κάθε κόμβος μπορεί να επιλεχθεί κάθε στιγμή και τότε βγάζει τις επιλογές: “View Stats”, που εμφανίζει στατιστικά στοιχεία, “Mtrace Next” που δίνει τη δυνατότητα στο χρήστη να αλλάξει τη σειρά του mtrace, “Prune” and “Expand” που παρέχει τη δυνατότητα στο χρήστη να αφαιρέσει όποιο δρομολογητή επιθυμεί από το δέντρο, “Make Root” , επιλογή που εμφανίζεται αν υπάρχουν πάνω από δύο πηγές, οπότε δίνεται η δυνατότητα στο χρήστη να διαλέξει μία για να δημιουργηθεί το συγκεκριμένο δέντρο.

7.6 Αναφορές 7ου Κεφαλαίου

1. Index of MBone Software by Category
   http://www.merit.edu/~mbone/index/titles.html
2. Basic Multicast Debugging. Παρουσίαση της Cisco
   ftp://ftp-eng.cisco.com/ipmulticast/training/Module4.pdf
3. Advance IP Multicast Features. Παρουσίαση της Cisco.
   ftp://ftp-eng.cisco.com/ipmulticast/training/Module7.pdf
4. Using IP Multicast Tools. Cisco
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/1cdtools.htm
5. MHealth:A Real-Time Multicast Tree Visualization and Monitoring Tool. David B. Makofske και Kevin C. Almeroth
   http://www.nossdav.org/1999/papers/53-1441030863.pdf
6. http://www.nmsl.cs.ucsb.edu/projects.html
7. Multicast Measurement Tools Taxonomy.
   http://www.nmsl.cs.ucsb.edu/projects.html

Κεφάλαιο 8ο: Session Description Protocol (SDP) και Session Announcement Protocol (SAP)

8.1 Εισαγωγή

Στο κεφάλαιο αυτό θα αναφερθούμε σε δύο σημαντικά πρωτόκολλα που στην περίπτωση του IP multicast βοήθησαν στην περιγραφή και δημοσίευση των multicast sessions. Το Session Description Protocol (SDP) κάλυψε την ανάγκη για περιγραφή των sessions και το Session Announcement Protocol (SAP) για δημοσίευση των session που δημιουργούν οι πηγές.

8.2 Session Description Protocol (SDP)

Στο IP Multicasting, ένα session directory εργαλείο, όπως για παράδειγμα το SDP, χρησιμοποιείται για τη δημοσίευση multimedia συνδιασκέψεων και φέρνει σε επικοινωνία τις διευθύνσεις της συνδιάσκεψης με τις ειδικές πληροφορίες του εργαλείου συνδιάσκεψης που είναι απαραίτητα για την συμμετοχή. Εδώ, θα αναλύσουμε ένα πρωτόκολλο περιγραφής των session, το Session Description Protocol (SDP), που χρησιμοποιείται σε τέτοιες περιπτώσεις. Το SDP δημιουργήθηκε για να παρέχει πληροφορίες στους συμμετέχοντες και η μορφή του διευκολύνει την περιγραφή των sessions. Επειδή δεν πραγματοποιεί μεταφορά δεδομένων, συνεργάζεται με διάφορα πρωτόκολλα μεταφοράς ανάλογα με την περίσταση. Για παράδειγμα αναφέρουμε το Session Announcement Protocol (SAP), το Session Initiation Protocol (SIP), το Real-Time Streaming Protocol (RTSP), το electronic mail με χρήση των MIME επεκτάσεων και το Hypertext Transport Protocol.

Η συνηθισμένη χρήση του SDP είναι η ανακοίνωση ενός session συνδιάσκεψης στέλνοντας, περιοδικά με την τεχνολογία multicast, ένα πακέτο ανακοίνωσης σε μια γνωστή multicast διεύθυνση και πόρτα χρησιμοποιώντας το Session Announcement Protocol (SAP).

Τα SAP πακέτα είναι UDP πακέτα με την παρακάτω διαμόρφωση:

SAP header
text payload …….

Η επικεφαλίδα είναι η επικεφαλίδα του SAP. Το text payload είναι μια περιγραφή ενός SDP session, το οποίο δεν μπορεί να είναι πάνω από 1 kbyte. Μία μόνο ανακοίνωση επιτρέπεται σε ένα απλό πακέτο SAP.

Τα sessions που βασίζονται στην τεχνολογία multicast διαφέρουν από τα unicast, γιατί κάθε ενδιαφερόμενος που θέλει να λάβει την κίνηση θα πρέπει να συνδεθεί στο session. Έτσι το SDP παρέχει δύο υπηρεσίες. Πρώτον, πιστοποιεί την ύπαρξη ενός session και δεύτερον, παρέχει πληροφορίες για να γίνει εφικτή η σύνδεση και η συμμετοχή σε ένα session.

Το SDP περιέχει:

- το όνομα και το σκοπό του session,
- χρονολογίες που το session είναι ενεργό,
- τα media που εμπεριέχονται στο session και
- πληροφορίες για την λήψη αυτών των media (διευθύνσεις, πόρτες, διαμορφώσεις κ.α).

Επίσης είναι πιθανό να περιέχει επιπρόσθετες πληροφορίες όπως:

- πληροφορίες για το bandwidth που χρησιμοποιείται από τη συνδιάσκεψη,
- πληροφορίες για την επικοινωνία με το άτομο που είναι υπεύθυνο για το session.

Για τις Media πληροφορίες το SDP περιέχει:

- το είδος των Media (βίντεο, ήχος κτλ),
- το πρωτόκολλο μεταφοράς (RTP/UTP/IP, H.320, κτλ),
- τη διαμόρφωση των media (H.261 video, MPEG video, κτλ),
- την multicast διεύθυνση και πόρτα για το media.

Τα sessions μπορεί να είναι περιορισμένα σε χρόνο. Για πληροφορίες χρόνου το SDP μπορεί να περιέχει:

- μια λίστα από χρονικές στιγμές αρχής και τέλους του session,
- επαναλαμβανόμενες περιόδους για κάθε όριο, όπως για παράδειγμα " κάθε Δευτέρα στις 10π.μ για 3 ώρες".

Μια περιγραφή ενός session πρέπει να περιέχει αρκετές πληροφορίες για να αποφασίζουν οι ενδιαφερόμενοι αν θέλουν να συμμετάσχουν σε αυτό. Το SDP μπορεί να περιέχει πρόσθετους δείκτες με τη μορφή των Universal Resources Identifiers (URIs) για περισσότερες πληροφορίες.

Οι περιγραφές του SDP είναι κυρίως σε μορφή κειμένου γραμματοσειρά ISO 10646 και κωδικοποίηση UTF-8. Μια SDP περιγραφή ενός session αποτελείται από μια σειρά γραμμών κειμένου που έχουν την μορφή <type>=<value>. Όπου <type> είναι πάντα ένας χαρακτήρας και <value> είναι ένα κείμενο. Η περιγραφή ενός session αποτελείται από την περιγραφή σε επίπεδο session και πιθανόν να περιέχει μερικές περιγραφές σε επίπεδο media. Μια ανακοίνωση περιέχει ένα τμήμα σε επίπεδο session και ακολουθούν μηδέν, ένα ή περισσότερα τμήματα σε επίπεδο media. Στο κομμάτι του session-level η πρώτη γραμμή ξεκινάει με "v=". Στην media περιγραφή η πρώτη γραμμή αρχίζει με "m=". Σε κάθε περιγραφή μερικές γραμμές απαιτούνται και άλλες όχι, αλλά όλες εμφανίζονται με τη σειρά που φαίνεται παρακάτω. Αυτές που δεν απαιτούνται σημειώνονται με ένα *.

Session description

v= (protocol version)
o= (owner/creator and session identifier).
s= (session name)
i=* (session information)
u=* (URI of description)
e=* (email address)
p=* (phone number)
c=* (connection information - not required if included in all media)
b=* (bandwidth information)
One or more time descriptions (see below)
z=* (time zone adjustments)
k=* (encryption key)
a=* (zero or more session attribute lines)

Time description

t= (time the session is active)
r=* (zero or more repeat times)

Media description
m= (media name and transport address)
i=* (media title)
c=* (connection information - optional if included at session-level)
b=* (bandwidth information)
k=* (encryption key)
a=* (zero or more media attribute lines)

Στη συνέχεια φαίνεται ένα παράδειγμα μιας SDP περιγραφής.

```
v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 3
m=application 32416 udp wb
a=orient:portrait
```

Οι παράμετροι έχουν την εξής σημασία:

"v": Δίνει την έκδοση του SDP.

"o": <username> <session id> <version> <network type> <address type> <address>: Όπου *username,* είναι το όνομα του χρήστη στη μηχανή που δημιούργησε το session. Το *session id* είναι ένα νούμερο που είναι μοναδικό και καθορίζει το session. Το Version καθορίζει την έκδοση της ανακοίνωσης. Το *network type* είναι ένα κείμενο που καθορίζει το είδος του δικτύου. Το "IN" στο συγκεκριμένο παράδειγμα σημαίνει "Internet". Το *address type* είναι ένα κείμενο που δίνει το είδος της διεύθυνσης που ακολουθεί. Στο παράδειγμα είναι "IP4". Το *address* δίνει τη διεύθυνση της μηχανής που δημιούργησε το session. Αν το domain name είναι διαθέσιμο, δίνεται. Διαφορετικά, όπως και στο παράδειγμα, δίνεται η IP διεύθυνση.

"s": Δίνει το όνομα του session.

"i": Δίνει μια περιγραφή του session.

"u": Δίνει ένα URI όπου ο ενδιαφερόμενος μπορεί να μάθει περισσότερες πληροφορίες για το session.

"e": Δίνει την e-mail διεύθυνση του υπεύθυνου του session.

"c": <network type> <address type> <connection address>. Το *network type* είναι ένα κείμενο που δίνει το είδος του δικτύου. Στο παράδειγμα είναι "IN" δηλαδή Internet. Το *address type* είναι και αυτό ένα κείμενο που καθορίζει το είδος της διεύθυνσης που ακολουθεί. Στο παράδειγμα είναι IP4. Τέλος το πεδίο *connection address* δίνει την IP multicast διεύθυνση που χρησιμοποιείται. Επίσης δίνει και το TTL με το οποίο στέλνονται τα πακέτα. Στο παράδειγμα είναι 127.

"t": <start time> <stop time>. Αυτό το πεδίο καθορίζει πότε αρχίζει και πότε τελειώνει το session.

"m": <media> <port> <transport> <fmt list>. Μια περιγραφή ενός session ίσως περιέχει μερικές media περιγραφές. Το πεδίο media καθορίζει το είδος του media. Στο παράδειγμα είχαμε audio, video και application. Το επόμενο πεδίο καθορίζει την πόρτα. Για το παράδειγμα, οι πόρτες που χρησιμοποιούνται είναι οι 49170, 51372 και 32416. Το πεδίο transport δείχνει το πρωτόκολλο μεταφοράς. Στο παραπάνω παράδειγμα, αυτό είναι το RTP για τα δύο πρώτα και το UDP για το τελευταίο media.

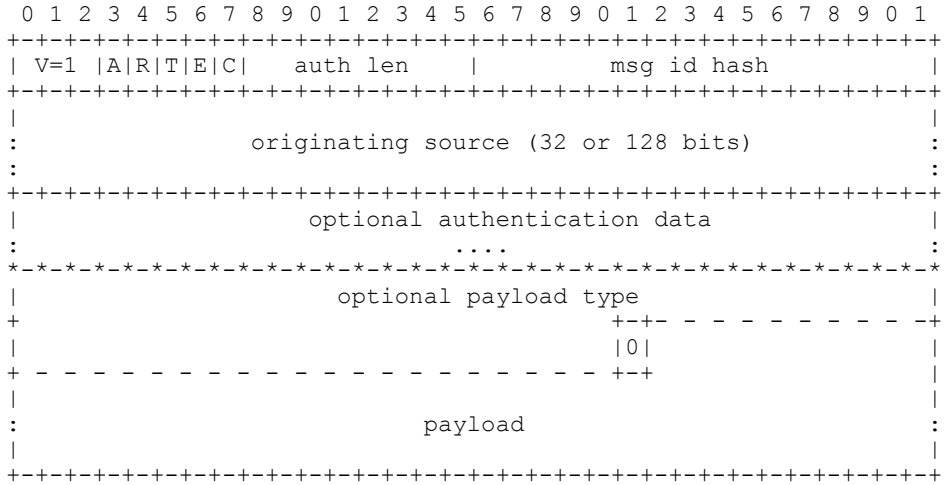
8.3 Session Announcement Protocol (SAP)

Το Session Announcement Protocol δημιουργήθηκε με σκοπό να βοηθήσει στη δημοσίευση των multicast multimedia sessions και να μεταφέρει πληροφορίες για τα sessions στους συμμετέχοντες. Το SAP στέλνει multicast, περιοδικά, ένα πακέτο ανακοίνωσης σε μια γνωστή multicast διεύθυνση και πόρτα. Η ανακοίνωση γίνεται multicast στο ίδιο καθορισμένο όριο (scope) που το session έχει ανακοινωθεί. Ένας SAP ακροατής ακούει στη γνωστή διεύθυνση και πόρτα που έχουν καθοριστεί για το συγκεκριμένο multicast όριο στο οποίο ανήκει (πχ. admin scope). Υπάρχουν οι εξής περιπτώσεις:

1) Τα IPv4 global scope sessions χρησιμοποιούν multicast διευθύνσεις που ανήκουν στο διάστημα 224.2.128.0 – 224.2.255.255 με τις SAP ανακοινώσεις να στέλνονται στην 224.2.127.254.

2) Τα IPv4 administrative scope sessions χρησιμοποιούν administrative scope multicast διευθύνσεις. Η multicast διεύθυνση που χρησιμοποιείται για τις ανακοινώσεις είναι η μεγαλύτερη multicast διεύθυνση της συγκεκριμένης administrative scope ζώνης. Για παράδειγμα, αν το καθορισμένο όριο είναι 239.16.32.0 –239.16.33.255, τότε η 239.16.33.255 χρησιμοποιείται για τις SAP ανακοινώσεις.

Οι SAP ανακοινώσεις πρέπει να γίνονται στην πόρτα 9875 και να στέλνονται με TTL 255. Η εικόνα 8.1 δείχνει τη διαμόρφωση ενός SAP πακέτου[1].



Εικόνα 8.1

Αναφορές 8ου Κεφαλαίου

1. Session Announcement Protocol (SAP). http://www.cs.ucl.ac.uk/staff/jon/mmbook/book/node184.html

[1] Για περισσότερες πληροφορίες συμβουλευτείτε το RFC 2974.

2. Session Description Protocol. http://smuhandouts.com/8393/ppt-JB-RFC2327.pdf
3. RFC 2327: SDP: Session Description Protocol
4. RFC 2974: Session Announcement Protocol

Παράρτημα Ι: Επεκτάσεις του Πρωτοκόλλου PIM

Ι.1 Εισαγωγή

Σε αυτό το παράρτημα θα αναλυθούν δύο επεκτάσεις του πρωτοκόλλου PIM: το Source Specific Multicast (SSM) και Bi-directional PIM.

Ι.2 Source Specific Multicast

Το Source Specific Multicast (SSM) είναι μια επέκταση του IP multicast όπου τα datagrams προωθούνται στους αποδέκτες μόνο από τις multicast πηγές στις οποίες οι αποδέκτες έχουν συνδεθεί. Για τις multicast ομάδες που είναι ρυθμισμένες για SSM δημιουργούνται μόνο source path δέντρα διανομής (όχι shared trees).

Ι.2.1 Συστατικά του SSM

Το SSM είναι ένα datagram μοντέλο διανομής που κυρίως υποστηρίζει one-to-many εφαρμογές. Εδώ θα σχολιάσουμε τα παρακάτω συστατικά του Cisco IOS που υποστηρίζουν SSM:

1. Protocol Independent Multicast source specific mode (PIM-SSM)
2. Internet Group Management Protocol Version 3(IGMPv3)
3. Internet Group Management Protocol Version 3 lite (IGMPv3lite)
4. URL Rendezvous Directory (URD)

Το PIM-SSM είναι ένα πρωτόκολλο δρομολόγησης που υποστηρίζει SSM και επηρεάζεται από το PIM-SM. ΤΟ IGMP version 3 υποστηρίζει φιλτράρισμα της πηγής, το οποίο απαιτείται για SSM. Για να τρέξει το SSM με IGMPv3, θα πρέπει να υποστηρίζεται από τους Cisco IOS δρομολογητές, τη μηχανή που τρέχει την εφαρμογή και από την ίδια την εφαρμογή. Το IGMPv3 lite και το URD είναι δύο λύσεις τις Cisco όπου δε χρειάζονται την full υποστήριξη από το IGMPv3 στις μηχανές και στις εφαρμογές που τρέχουν.

Ι.2.2 Διαφορές του SSM από το Standard Multicast

Το τρέχον IP multicasting στο internet αλλά και σε πολλά intranets βασίζεται στο PIM-SM πρωτόκολλο και στο Multicast Source Discovery Protocol (MSDP). Αυτά τα πρωτόκολλα είναι δοκιμασμένα και έχουν αποδείξει τη λειτουργικότητα τους. Παρόλα αυτά, έχουν κάποιες αδυναμίες για το Internet Standard Multicast (ISM) service μοντέλο. Για παράδειγμα, στο ISM το δίκτυο πρέπει να γνωρίζει ποιοι hosts στέλνουν multicast δεδομένα. Στην περίπτωση του SSM, αυτή η πληροφορία δίνεται από τους αποδέκτες, αφού το δίκτυο παρέχει τις διευθύνσεις των πηγών που μεταβιβάζονται στους last hop δρομολογητές μέσω του IGMPv3, IGMPv3 lite ή το URD. Γενικά, το SSM παρέχει καλύτερης ποιότητας IP multicast υπηρεσίες για εφαρμογές που υποστηρίζουν SSM.

Η ISM υπηρεσία παρέχει διανομή των IP datagrams από κάθε πηγή σε μια ομάδα από αποδέκτες. Αυτά τα datagrams έχουν μια IP unicast διεύθυνση πηγής S και την multicast διεύθυνση του group G σαν IP διεύθυνση προορισμού. Οι μηχανές θα δεχτούν την κίνηση αν γίνουν μέλη του group. Συμμετοχή στο group δηλώνουν με το IGMP version 1,2 ή 3.

Στο SSM, η μεταφορά των datagrams βασίζεται σε (S,G) κανάλια. Η κίνηση σε ένα (S,G) κανάλι αποτελείται από datagrams με μια IP unicast διεύθυνση πηγής S και την multicast group διεύθυνση σαν IP διεύθυνση προορισμού. Οι μηχανές θα δεχτούν αυτή την κίνηση, αν γίνουν μέλη του (S,G) καναλιού. Και στο SSM και στο ISM, μια μηχανή δεν χρειάζεται να στείλει κάποιο μήνυμα για να γίνει πηγή. Ωστόσο, στο SSM, οι αποδέκτες πρέπει να γραφτούν (να γίνουν συνδρομητές συνήθως) ή να ξεγραφτούν στο (S,G) κανάλι, για να δεχτούν ή να σταματήσουν να δέχονται δεδομένα από μια συγκεκριμένη πηγή. Με άλλα λόγια, οι αποδέκτες μπορούν να δέχονται δεδομένα μόνο από τα (S,G) κανάλια στα οποία είναι γραμμένοι, ενώ στην ISM οι αποδέκτες δεν χρειάζεται να γνωρίζουν τις IP διευθύνσεις των πηγών από τις οποίες παίρνουν δεδομένα. Η εγγραφή σε ένα κανάλι γίνεται με μετάδοση κάποιου πακέτου που υποστηρίζεται μόνο από το IGMPv3.

I.2.3 SSM πεδίο διευθύνσεων

Η Internet Assigned Numbers Authority (IANA) έχει δεσμεύσει το πεδίο διευθύνσεων 232.0.0.0 έως 232.255.255.255 για SSM εφαρμογές και πρωτόκολλα. Το Cisco IOS software επιτρέπει SSM configuration σε ένα αυθαίρετο υποσύνολο των IP multicast διευθύνσεων 224.0.0.0 έως 239.255.255.255. Όταν το SSM πεδίο βρεθεί, οι υπάρχοντες IP multicast αποδέκτες θα σταματήσουν να παίρνουν δεδομένα αν προσπαθήσουν να χρησιμοποιήσουν διευθύνσεις μέσα σε αυτό το πεδίο.

I.2.4 Λειτουργίες του SSM

Ένα δίκτυο που παρέχει multicasting και τρέχει PIM-SM μπορεί να υποστηρίξει SSM. Το SSM μπορεί επίσης να λειτουργήσει μόνο του σε ένα δίκτυο χωρίς τη βοήθεια των πρωτοκόλλων που απαιτούνται για interdomain PIM-SM. Εάν το SSM ενεργοποιηθεί σε ένα δίκτυο που τρέχει PIM-SM, πρέπει μόνο οι last-hop δρομολογητές να αναβαθμίσουν το software για να υποστηρίζουν SSM. Οι δρομολογητές που δεν είναι κατευθείαν συνδεδεμένοι με κάποιον αποδέκτη δεν πρέπει να ρυθμιστούν για SSM. Γενικά, αυτοί οι δρομολογητές πρέπει μόνο να τρέχουν PIM-SM στο SSM πεδίο και ίσως χρειάζονται επιπρόσθετες ρυθμίσεις, για να καταστέλλουν τα MSDP σήματα ή τις PIM-SM shared tree λειτουργίες που προσπαθούν να γίνουν μέσα στο SSM πεδίο.

Όταν ενεργοποιηθεί το SSM έχουμε τις παρακάτω επιπτώσεις:

1. Για τα groups που ανήκουν στο SSM πεδίο, η εγγραφή στα (S,G) κανάλια γίνεται με το IGMPv3 INCLUDE mode αναφορά για συμμετοχή, το IGMPv3 lite ή το URD.
2. Οι PIM λειτουργίες μέσα στο SSM πεδίο διευθύνσεων μετατρέπονται σε PIM-SSM. Σε αυτή την κατάσταση, μόνο PIM (S,G) join και prune μηνύματα δημιουργούνται από το δρομολογητή. Δε δημιουργούνται μηνύματα (S,G) rendezvous point tree (RPT) ή (*,G) RPT. Τα εισερχόμενα μηνύματα για RPT λειτουργίες αγνοούνται και τα εισερχόμενα PIM register μηνύματα αμέσως απαντώνται με register-stop μηνύματα. Το PIM-SSM είναι συμβατό με το PIM-SM, εκτός και αν ο δρομολογητής είναι last hop δρομολογητής. Οπότε, οι δρομολογητές που δεν είναι last hop μπορούν να τρέχουν PIM-SM για SSM ομάδες.

3. Τα MSDP source-active μηνύματα μέσα στο SSM πεδίο δε γίνονται δεκτά, δε δημιουργούνται και δεν προωθούνται.

I.2.5 IGMPv3

Το IGMPv3 είναι η τρίτη έκδοση του IGMP. Αυτό δίνει τη δυνατότητα στους hosts να στέλνουν στο group μηνύματα συμμετοχής, καθορίζοντας την πηγή από την οποία επιθυμούν να λάβουν δεδομένα. Ένας ενδιαφερόμενος μπορεί να στείλει μήνυμα δηλώνοντας, έτσι, την επιθυμία του να λάβει δεδομένα από όλες τις πηγές που στέλνουν στο group εκτός από κάποιες συγκεκριμένες (EXCLUDE mode). Επίσης μπορεί να δηλώσει ότι επιθυμεί να λάβει δεδομένα μόνο από κάποιες συγκεκριμένες πηγές που στέλνουν στο group. (INCLUDE mode). Το IGMPv3 μπορεί να λειτουργεί και με Internet Standard Multicast και με Source Specific Multicast. Στο ISM λειτουργεί και σε EXCLUDE και σε INCLUDE mode. Στο SSM μόνο οι INCLUDE mode αναφορές γίνονται δεκτές από το last hop δρομολογητή.

I.2.6 Πλεονεκτήματα του SSM

1. Στο ISM, οι εφαρμογές χρειάζονται μια μοναδική IP multicast group διεύθυνση γιατί η διανομή των δεδομένων βασίζεται μόνο στην IP multicast group διεύθυνση που χρησιμοποιείται. Αν δύο εφαρμογές με διαφορετικές πηγές και αποδέκτες χρησιμοποιούν την ίδια IP multicast group διεύθυνση, τότε οι αποδέκτες των δύο εφαρμογών θα δεκτούν δεδομένα από τους αποστολείς και των δύο εφαρμογών. Παρόλο που οι αποδέκτες έχουν τη δυνατότητα να απορρίψουν τα μη απαραίτητα δεδομένα, αυτή η κατάσταση δημιουργεί άσκοπη κίνηση.

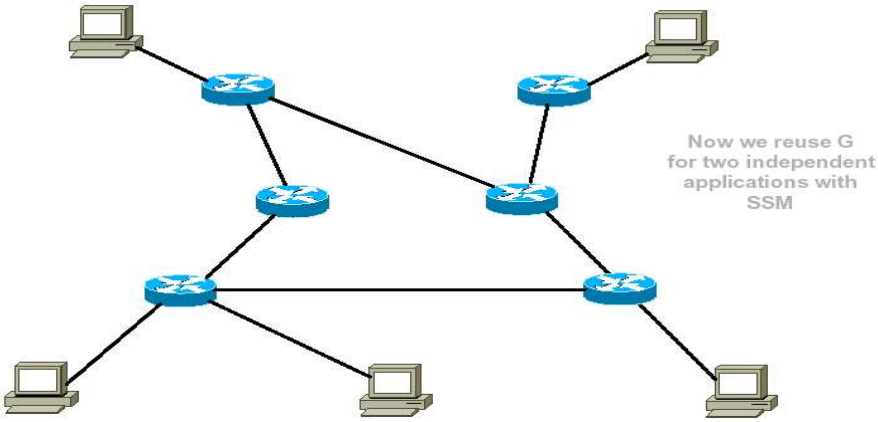
   Η δέσμευση μιας IP multicast διεύθυνσης για μια εφαρμογή είναι επίσης πρόβλημα. Οι περισσότερες μικρής διάρκειας εφαρμογές χρησιμοποιούν μηχανισμούς όπως το Session Description Protocol (SDP) και το Session Announcement Protocol (SAP) για να πάρουν τυχαίες διευθύνσεις, μια λύση που δεν λειτουργεί με επιτυχία όσο ο αριθμός των εφαρμογών αυξάνει στο internet. Η καλύτερη τρέχουσα λύση για μεγάλης διάρκειας εφαρμογές είναι αυτή των αυτόνομων συστημάτων, με μόνο μειονέκτημα ότι έχει μόνο 255 διευθύνσεις.

   Στο SSM, η κίνηση από κάθε πηγή προωθείται μεταξύ των δρομολογητών μέσα στο δίκτυο ανεξάρτητα από την κίνηση των άλλων πηγών. Έτσι, διαφορετικές πηγές μπορούν να χρησιμοποιούν ίδιες multicast group διευθύνσεις μέσα στο SSM πεδίο.
2. Στο SSM, η multicast κίνηση από κάθε πηγή θα μεταδοθεί στο δίκτυο, μόνο αν ζητηθεί από κάποιο αποδέκτη. Αντίθετα, στο ISM τα δεδομένα προωθούνται από την πηγή σε μια multicast ομάδα, δηλαδή σε όλους τους αποδέκτες που ζητούν αυτή την ομάδα. Έτσι, μια πηγή μπορεί εύκολα να δημιουργήσει πρόβλημα στη λειτουργία του δικτύου, απλά στέλνοντας δεδομένα χωρίς λόγο στην ίδια ομάδα. Με αυτό τον τρόπο μειώνεται το bandwidth από την πλευρά του αποδέκτη, αφού γεμίζει με άχρηστα δεδομένα και έτσι δημιουργείται ανωμαλία στην κανονική λειτουργία της μετάδοσης. Στο SSM, αυτή η επίθεση δεν μπορεί να συμβεί απλά στέλνοντας δεδομένα σε μια multicast ομάδα.

3. Το SSM είναι εύκολο να εγκατασταθεί σε ένα δίκτυο, αφού δεν απαιτείται η γνώση των ενεργών πηγών που στέλνουν στα multicast groups. Η standard λύση στο ISM είναι το PIM-SM και MSDP όπου το RP χρειάζεται μόνο για να γίνονται γνωστές οι ενεργές πηγές. Αυτό δεν απαιτείται στο SSM, για αυτό είναι ευκολότερο στην εγκατάσταση και στη διαχείριση. Επίσης είναι εύκολο να εγκατασταθεί και στην περίπτωση που ένα δίκτυο τρέχει ήδη multicasting, αφού χρειάζεται μόνο αλλαγή στον last-hop δρομολογητή να υποστηρίζει IGMPv3.

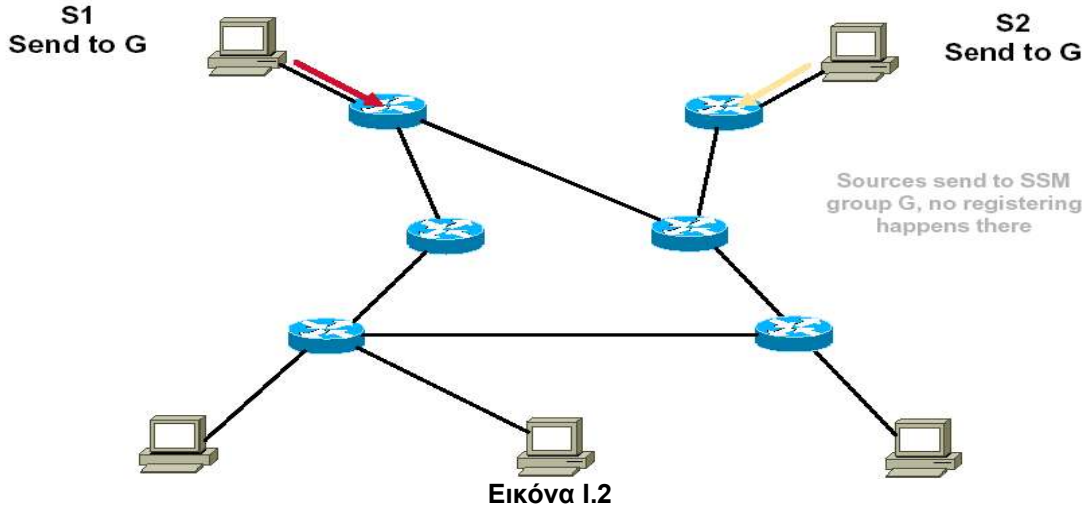
I.2.7 Παράδειγμα SSM

Παρακάτω παραθέτουμε ένα παράδειγμα του τρόπου μεταφοράς δεδομένων στο SSM



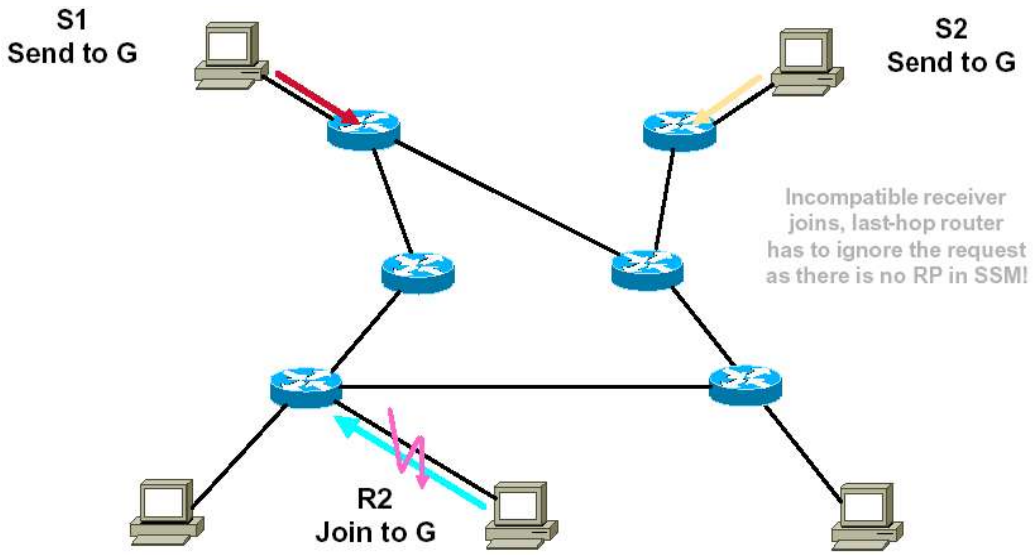
Εικόνα I.1

Έστω ότι έχουμε το παραπάνω δίκτυο και οι δύο πηγές στέλνουν διαφορετικές εφαρμογές στο G group με SSM.



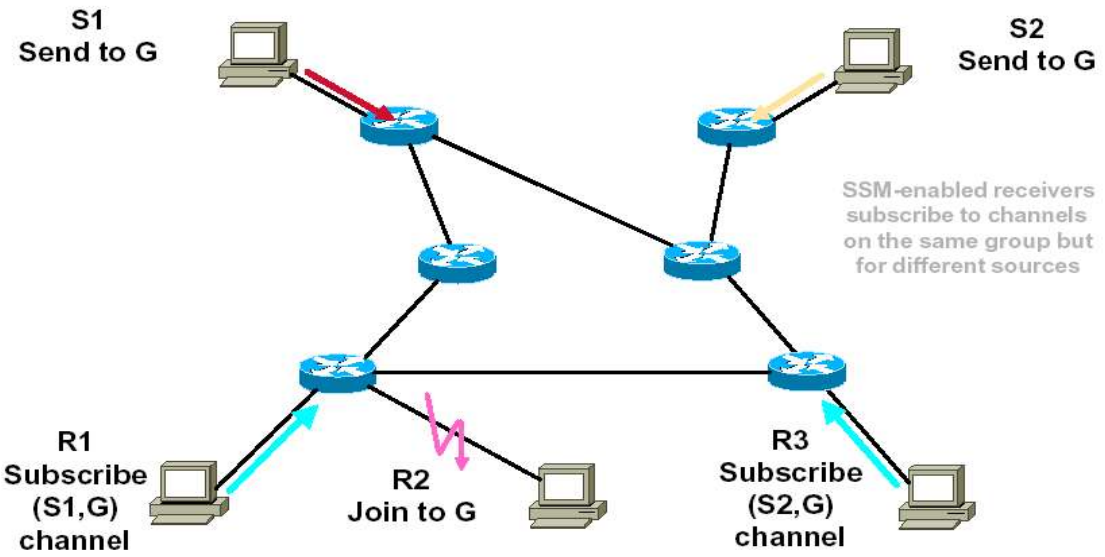
Εικόνα I.2

Οι πηγές στέλνουν στο SSM group G. Σε αντίθεση με το κανονικό multicasting οι παραλήπτες δεν κάνουν register σε κάποια ομάδα.



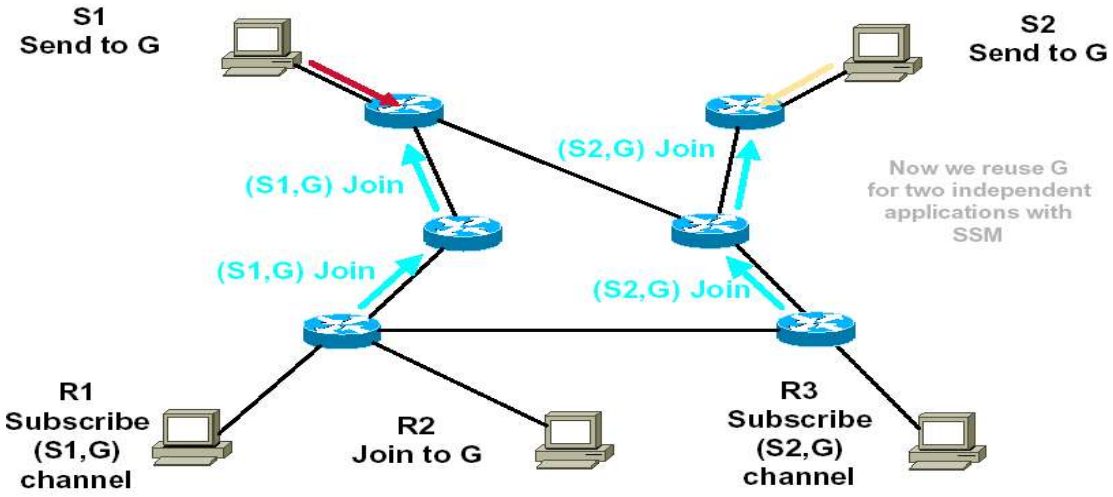
Εικόνα Ι.3

Κάποιος ενδιαφερόμενος που δεν είναι όμως συμβατός με SSM προσπαθεί να κάνει join στην ομάδα. Ο last-hop δρομολογητής αδιαφορεί αφού σε αυτή την περίπτωση δεν υπάρχει RP.



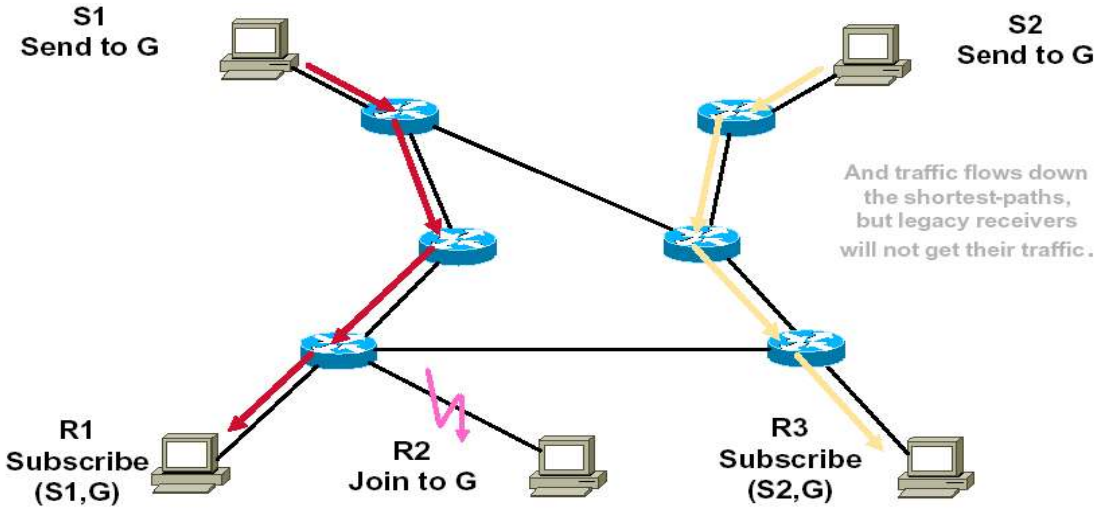
Εικόνα Ι.4

Οι ενεργοποιημένοι σε SSM αποδέκτες γράφονται σε κανάλια στο ίδιο group αλλά για διαφορετικές πηγές.



Εικόνα I.5

Χρησιμοποιείται δηλαδή το ίδιο group για δύο ανεξάρτητες εφαρμογές. Οι δρομολογητές όπως και στο ISM στέλνουν join μηνύματα στους upstream δρομολογητές.



Εικόνα I.6

Τελικά τα δεδομένα μεταφέρονται από το συντομότερο δυνατό τρόπο, αλλά οι «παραδοσιακοί» αποδέκτες δεν θα πάρουν δεδομένα.

I.3 Bi-directional (Bidir) PIM

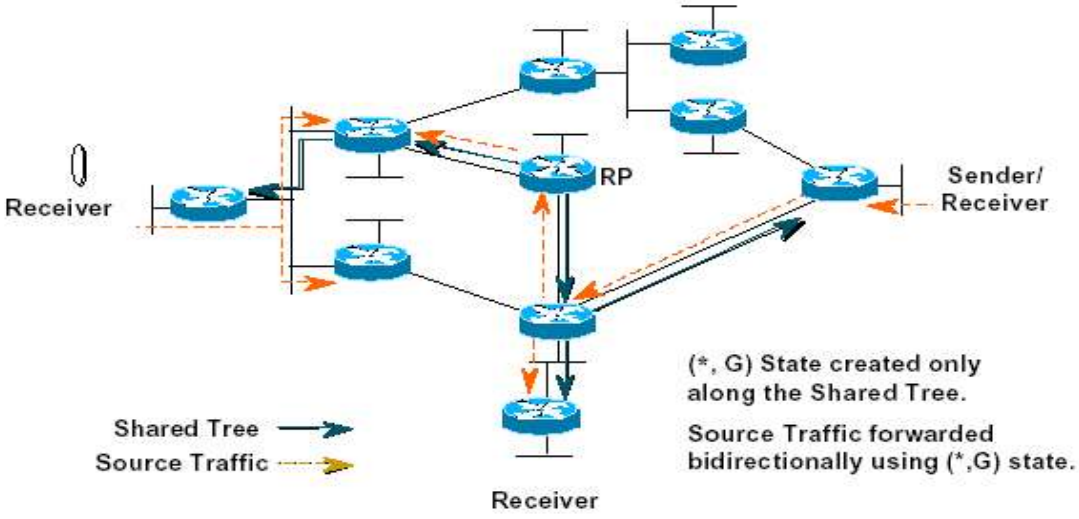
Όπως έχουμε αναφέρει, οι multicast εφαρμογές χωρίζονται στις εξής κατηγορίες: ένας αποστολέας σε πολλούς αποδέκτες (βίντεο, TV, Ραδιόφωνο), λίγοι σε λίγους (βίντεο/ ήχος συνδιασκέψεις), πολλοί σε πολλούς (παιχνίδια). Στην περίπτωση που έχουμε έναν αποστολέα και πολλούς αποδέκτες δημιουργείται μια (S,G) καταχώρηση στους δρομολογητές. Στην τελευταία όμως περίπτωση μπορεί να δημιουργηθούν απεριόριστες (S,G) καταχωρήσεις. Έτσι αυξάνονται οι απαιτήσεις σε υπολογιστική δύναμη στους δρομολογητές και η απόδοσή τους μειώνεται.

Το Bi-directional (αμφίδρομο) PIM μπορεί να δώσει λύση στο παραπάνω πρόβλημα, δημιουργώντας αμφίδρομα Shared δέντρα. Αυτά

επιτρέπουν στα δεδομένα να ρέουν το shared δέντρο προς τα πάνω. Η βασική ιδέα είναι να χρησιμοποιηθεί το ίδιο δέντρο για την κίνηση από τις πηγές στο RP και από το RP στους αποδέκτες.

Όπως είναι γνωστό, στο PIM-SM η κίνηση από τις πηγές στο RP αρχικά μεταφέρεται ενσωματωμένη στα μηνύματα εγγραφής στο RP, κάτι που επιφέρει επιπρόσθετο φόρτο. Επίσης, δημιουργείται ένα shortest path δέντρο από την πηγή στο RP, το οποίο έχει σαν αποτέλεσμα (*,G) και (S,G) καταχωρίσεις στο δρόμο μεταξύ του RP και της πηγής. Πολλές multicast εφαρμογές χρησιμοποιούν το μοντέλο πολλοί αποστολείς σε πολλούς αποδέκτες όπου κάθε μέλος είναι αποστολέας και αποδέκτης ταυτόχρονα. Σε μια τέτοια περίπτωση (*,G) και (S,G) καταχωρίσεις εμφανίζονται παντού στο δρόμο από τους συμμετέχοντες στο RP, με αποτέλεσμα την αύξηση της απαίτησης σε μνήμη. Επίσης είναι πιθανό να υπάρχει συμφόρηση στο δρόμο από το RP στην πηγή και αντίστροφα.

Το Bi-directional PIM παρακάμπτει την ενθυλάκωση των register μηνυμάτων επιτρέποντας στα πακέτα να προωθηθούν από μια πηγή στο RP χρησιμοποιώντας μόνο το shared δέντρο. Αυτό επιτρέπει την εμφάνιση μόνο των (*,G) καταχωρίσεων στους multicast πίνακες δρομολόγησης. Επίσης, ο δρόμος που χρησιμοποιούν τα πακέτα από τους συμμετέχοντες (πηγές και παραλήπτες) στο RP και αντίστροφα θα είναι ο ίδιος. Η εικόνα I.7 δείχνει ένα παράδειγμα ενός Bi-directional PIM δέντρου διανομής, όπου παρατηρούμε ότι η κίνηση προωθείται αμφίδρομα.



Εικόνα I.7

Στην περίπτωση του Bidir-PIM το ρόλο του designated δρομολογητή παίζει αντίστοιχα ο designated forwarder (DF), ο οποίος είναι ο μόνος δρομολογητής που προωθεί πακέτα προς την πηγή και προς τους αποδέκτες. Υπάρχει ένας DF για κάθε RP. Ο δρομολογητής με τον καλύτερο unicast δρόμο προς το RP εκλέγεται ως DF.

I.4 Αναφορές

1. Source-Specific Protocol Independent Multicast in 232/8. Internet draft Greg Shepherd, Juniper Network, Rob Rockell, David Mayer Φεβρουάριος 2002.
2. Bi-Directional Shared Trees in PIM-SM. Internet draft
3. PIM Protocol Extensions. Παρουσίαση της Cisco. ftp://ftp-eng.cisco.com/ipmulticast/training/Module12.pdf
4. Source Specific Multicast. Cisco configuration http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtssm.htm

Παράρτημα II: Πειραματικές Multicast Αρχιτεκτονικές

II.1 Εισαγωγή

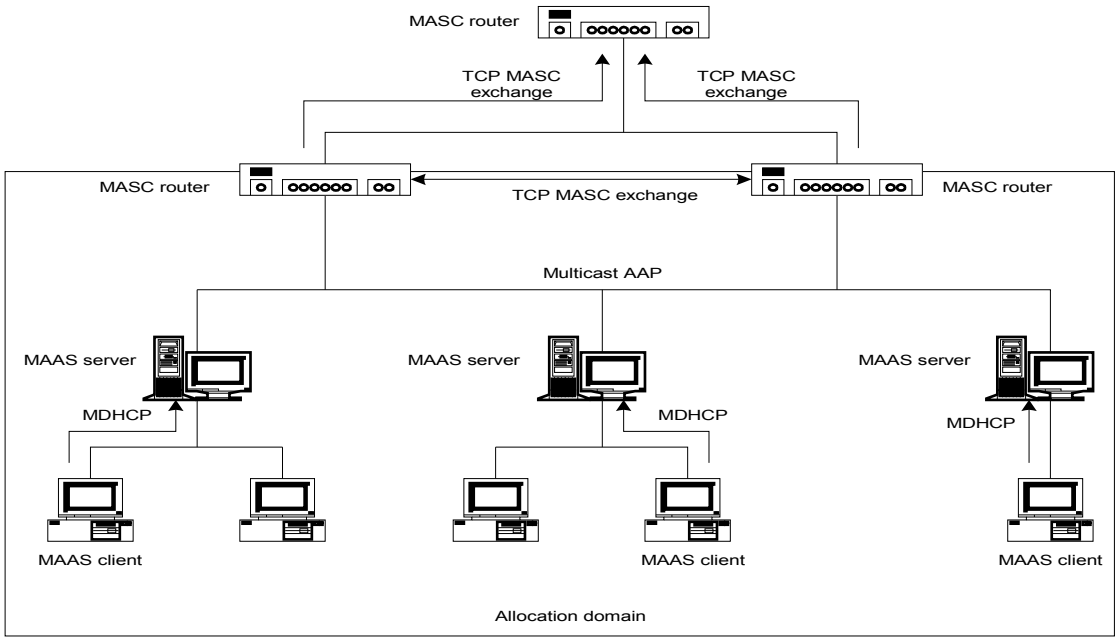
Ενώ τα πρωτόκολλα PIM-SM, MBGP και MSDP χρησιμοποιούνται με επιτυχία για interdomain multicast, νέες αρχιτεκτονικές έχουν αρχίσει να αναπτύσσονται. Σε αυτό το παράρτημα θα αναφερθούμε σε δύο πρωτόκολλα, το Border Gateway Multicast Protocol (BGMP) και το Multicast Address-Set Claim (MASC). Αυτά τα πρωτόκολλα χρησιμοποιούνται σε συνδυασμό με το MBGP και άλλα intra-domain multicast πρωτόκολλα δρομολόγησης. Η BGMP αρχιτεκτονική δουλεύει με τη βοήθεια του MASC, το οποίο είναι ένα πρωτόκολλο που παρέχει ιεραρχική διευθυνσιοδότηση (hierarchical addressing protocol). Παρόλο που το BGMP δεν εξαρτάται από το MASC, (άλλα πρωτόκολλα διευθυνσιοδότησης μπορούν να χρησιμοποιηθούν) το MASC είναι η καλύτερη λύση και τα δύο μαζί θεωρούνται σαν μία αρχιτεκτονική. Για να αναλύσουμε το BGP, θα πρέπει πρώτα να καταλάβουμε πώς γίνεται η διευθυνσιοδότηση. Πρώτα θα εξηγήσουμε το MASC, το οποίο είναι μέρος μιας αρχιτεκτονικής που παρέχει διευθυνσιοδότηση και λέγεται Multicast Address Allocation (MALLOC), και στη συνέχεια θα προχωρήσουμε στο BGMP.

II.2 Η αρχιτεκτονική Multicast Address Allocation (MALLOC)

Η MALLOC αρχιτεκτονική χρησιμοποιεί τρία πρωτόκολλα:

- Το Multicast Address-Set Claim (MASC), το οποίο ενεργεί ως υψηλού επιπέδου πρωτόκολλο διευθυνσιοδότησης και λειτουργεί μεταξύ των αυτόνομων συστημάτων.
- Το Address Allocation Protocol (AAP), το οποίο αναθέτει διευθύνσεις μέσα σε ένα domain.
- Το Multicast Address Dynamic Client Allocation Protocol (MADCAP), το οποίο χρησιμοποιείται από τους hosts για να ζητήσουν διευθύνσεις από ένα Multicast Address Allocation Server (MAAS).

Η MALLOC αρχιτεκτονική φαίνεται στην εικόνα II.1.

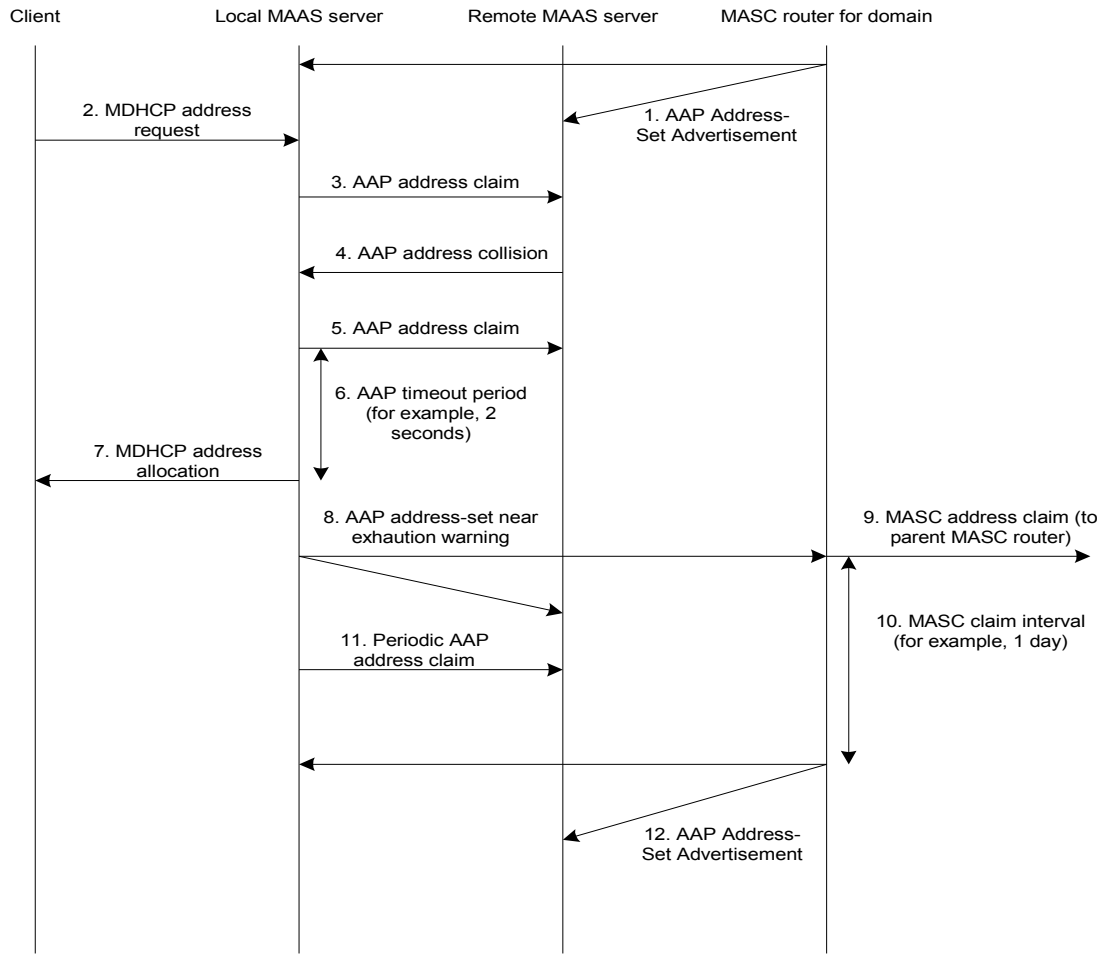


Η εικόνα δείχνει τα τρία επίπεδα της MALLOC. Το πρωτόκολλο MASC είναι η βάση της ιεραρχικής ανάθεσης διευθύνσεων της αρχιτεκτονικής. Αυτό αναθέτει δυναμικά, πεδία multicast διευθύνσεων από τα οποία τα groups που ανήκουν μέσα στο domain παίρνουν συγκεκριμένες multicast διευθύνσεις.

Το πρωτόκολλο AAP είναι ένα intra-domain πρωτόκολλο που χρησιμοποιείται για να παρέχει multicast διευθύνσεις μέσα στο domain. Χρησιμοποιείται από τους MAAS για να συντονίζει την ανάθεση, έτσι ώστε να μην παρέχονται διευθύνσεις δύο φορές. Αυτό το πρωτόκολλο λειτουργεί ακριβώς όπως το SDR, με τη διαφορά ότι ενεργεί μόνο μέσα σε ένα domain και δε δημοσιεύει τα sessions.

Το MADCAP είναι ένα απλό πρωτόκολλο αίτημα/απάντησης, το οποίο επιτρέπει στους clients να απαιτήσουν δυναμικά μια multicast διεύθυνση από το server.

Η εικόνα II.2 δείχνει τη σειρά των ενεργειών όταν παρέχονται multicast διευθύνσεις.



Εικόνα II.2

Το πρωτόκολλο MASC προμηθεύεται πεδία διευθύνσεων και τα διανέμει στους MAAS servers μέσο του AAP πρωτοκόλλου. Οι clients παίρνουν συγκεκριμένες διευθύνσεις από αυτά τα πεδία επικοινωνώντας με τον τοπικό MAAS server μέσο του MADCAP.

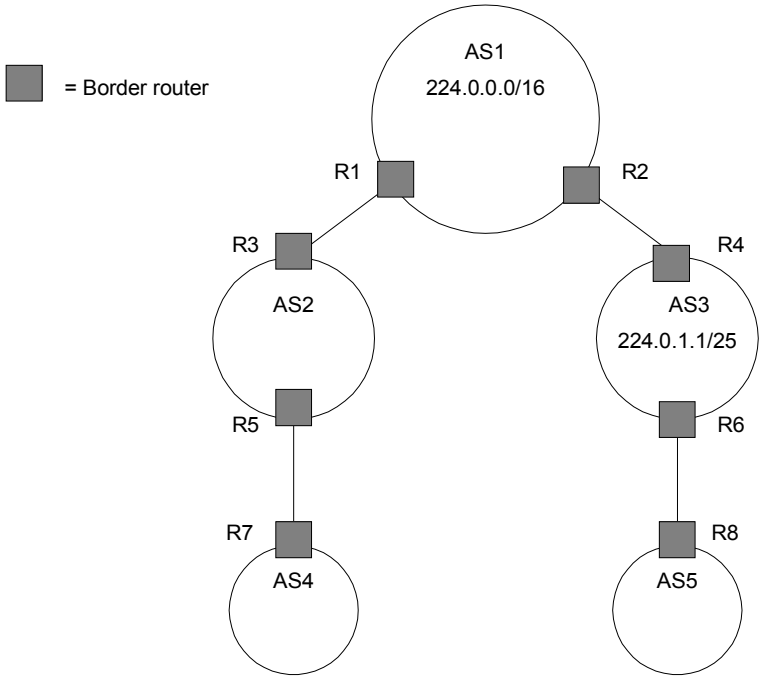
II.3 Το Πρωτόκολλο MASC

Το MASC τρέχει σε ένα ή περισσότερους εξωτερικούς δρομολογητές. Έχει την δυνατότητα να διανέμει δυναμικά πεδία διευθύνσεων σε domains που λειτουργούν σύμφωνα με την φράση «*άκουσε και απαίτησε με ανίχνευση συγκρούσεων*» (listen and claim with collision detection). Σύμφωνα με αυτή την τεχνική, τα domains “παιδιά”, ακούν στα multicast πεδία διευθύνσεων που έχουν επιλεχτεί από τα domains “γονείς”, απαιτούν υποπεδία από τα πεδία των γονέων, περιμένουν ένα χρονικό διάστημα για να κάνουν ανίχνευση συγκρούσεων, και αν δεν υπάρξει σύγκρουση, διαδίδει την πληροφορία στα άλλα domains παιδιά. Τα domains που δεν έχουν γονέα λέγονται top-level domains. Αυτά αποκτούν τις διευθύνσεις από το γενικό multicast πεδίο διευθύνσεων, 224.0.0.0/4.

Τα πεδία διευθύνσεων μεταδίδονται στον τοπικό MAASs με την χρήση του AAP και στα άλλα domains μέσο MBGP. Αυτά τα πεδία διευθύνσεων, όταν εισάγονται στο MBGP μέσο ενός δρομολογητή που τρέχει MASC,

λέγονται *group routes*. Ο πίνακας δρομολόγησης ενός MBGP δρομολογητή που περιέχει group routes λέγεται Group Routing Information Base (G-RIB).

Η εικόνα ΙΙ.3 δείχνει πως λειτουργεί το MASC.



Εικόνα ΙΙ.2

Σε αυτό το παράδειγμα, το αυτόνομο σύστημα 1 (AS1) είναι ένα top-level domain. Μπορούμε να θεωρήσουμε ότι είναι ένας κεντρικός παροχέας, ενώ τα MASC domains AS2 και AS3, τα οποία έχουν το AS1 σαν γονέα, είναι περιφερειακοί παροχείς. Τα AS2 και AS3 είναι “αδέρφια”(έχουν τον ίδιο γονέα). Τα AS2 και AS3 έχουν παιδιά τα AS4 και AS5. Ο κεντρικός παροχέας, AS1, έχει αποκτήσει το πεδίο των διευθύνσεων 224.0.0.0/16. Το παιδί του, AS3, έχει πάρει ήδη από αυτόν το πεδίο 224.0.1.1/25. Θα δούμε πως το AS2 θα αποκτήσει ένα πεδίο διευθύνσεων. Το MASC domain AS1 δημοσιεύει το πεδίο των διευθύνσεων του στα παιδιά του. Το παιδί domain AS2 ζητάει ένα πεδίο διευθύνσεων (για παράδειγμα το 224.0.1.0/24) από το πεδίο διευθύνσεων του γονέα, ενημερώνοντας τον γονέα για την αίτηση. Ο γονέας, AS1, διαδίδει αυτή την αίτηση για να ενημερώσει τα άλλα παιδιά του (σε αυτή την περίπτωση AS3). Αν κάποιο από τα αδέρφια του AS2 χρησιμοποιεί το πεδίο, ή μέρος αυτού, που το AS2 έχει επιλέξει, στέλνει πίσω μια ανακοίνωση σύγκρουσης.

Σε αυτό το παράδειγμα, επειδή το AS3 ήδη χρησιμοποιεί το πεδίο 224.0.1.1/25, στέλνει μια ανακοίνωση σύγκρουσης στο AS2. Αυτό τότε, εγκαταλείπει την αίτηση για το συγκεκριμένο το πεδίο διευθύνσεων και δημιουργεί νέα αίτηση για ένα διαφορετικό πεδίο, που πάντα όμως είναι υποσύνολο του πεδίου του γονέα, για παράδειγμα το πεδίο 224.0.128.0/24. Αν αυτή την φορά δεν υπάρξουν ανακοινώσεις συγκρούσεων, το AS2 παρέχει το πεδίο διευθύνσεων στον τοπικό του MAAS και μέσο του MBGP, στα άλλα domains σαν group routes.

Το domain γονέας, AS1, κρατάει στην μνήμη του πόσο από το πεδίο των διευθύνσεων του έχει δοθεί. Όταν αυτό υπερβεί κάποιο όριο, απαιτεί περισσότερο πεδίο, χρησιμοποιώντας το πρωτόκολλο MASC.

II.3.1 MASC και MBGP

Όπως είπαμε, όταν ένας MASC δρομολογητής αποκτήσει με επιτυχία ένα πεδίο διευθύνσεων, το εισάγει στον MBGP πίνακα δρομολόγησής του σαν ένα group route. Χρησιμοποιώντας το MBGP, τα multicast πεδία διευθύνσεων δημοσιεύονται στο internet.

Όταν ένας εξωτερικός δρομολογητής, X, δημοσιεύσει ένα group route σε ένα άλλο εξωτερικό δρομολογητή, Y, σημαίνει ότι ο Y μπορεί να χρησιμοποιήσει X σαν next hop για να προωθήσει multicast πακέτα στο root domain. Το root domain είναι αυτό που εισήγαγε το group route στον πίνακα δρομολόγησης.

Για παράδειγμα, στην εικόνα II.2, ο εξωτερικός δρομολογητής R3 δημοσιεύει το group route που αντιστοιχεί στο πεδίο διευθύνσεων 224.0.128.0/24, στον εξωτερικό δρομολογητή R1 του AS1. Επειδή όλοι οι MBGP δρομολογητές μέσα σε ένα domain επικοινωνούν μεταξύ τους για να ανταλλάξουν πληροφορίες που παίρνουν από τα εξωτερικά peers, ο εξωτερικός δρομολογητής R2 μαθαίνει το group route που έλαβε ο R1. Το group route που έλαβε ο R1 το αποθηκεύει στο G-RIB του σαν (224.0.128.0/24, R3), που σημαίνει ότι ο R3 είναι το next hop για τον R1 για να φτάσει στο root domain για το πεδίο 224.0.128.0/24. Ο R2 αποθηκεύει (224.0.128.0/24, R1) στο G-RIB του γιατί χρησιμοποιεί τον R1 σαν το next hop για το root domain γι αυτό το πεδίο διευθύνσεων.

II.3.2 Αρνητικά του MASC

Υπάρχουν δύο κύρια αρνητικά του MASC και είναι τα εξής:

- Είναι αρκετά πολύπλοκο, κάνοντας την εφαρμογή του δύσκολη και ακριβή.
- Δεν μπορεί να αναθέσει το multicast πεδίο διευθύνσεων δίκαια.

Το πρώτο δίνει εξήγηση από μόνο του. Ας δούμε όμως τι γίνεται στην περίπτωση του δεύτερου. Επειδή οι multicast ομάδες είναι περισσότερο δυναμικές από τις IP διευθύνσεις, είναι δύσκολο να υπολογιστεί εκ τον προτέρων πόσες διευθύνσεις θα χρειαστεί ένα domain. Αν οι δρομολογητές εκτιμήσουν μικρό πεδίο, πρέπει να ζητήσουν ξανά νέο πεδίο διευθύνσεων, που σημαίνει ότι το multicast πεδίο διευθύνσεων τεμαχίζεται. Ο τεμαχισμός παραβιάζει την απαίτηση ότι το πεδίο πρέπει να μοιραστεί λογικά. Επίσης αυξάνει το φόρτο στο MBGP, απαιτώντας την διανομή όλο και περισσότερης πληροφορίας όσο αυξάνει ο αριθμός των πεδίων. Από την άλλη αν ο δρομολογητής ζητήσει παραπάνω διευθύνσεις από ότι τελικά χρειάζεται, είναι πιθανό οι διευθύνσεις να τελειώσουν. Υπάρχουν 2^{28} multicast διευθύνσεις, που αν και φαίνεται μεγάλος αριθμός, αν κάθε domain αποκτάει ένα πεδίο αυτών χωρίς να το χρειάζεται, είναι πολύ πιθανό να εξαντληθούν.

II.4 Border Gateway Multicast Protocol (BGMP)

Οι εξωτερικοί δρομολογητές ενός domain τρέχουν BGMP για να χτίσουν ένα inter-domain shared δέντρο για μια multicast ομάδα. Οι ίδιοι δρομολογητές επίσης τρέχουν ένα intra-domain multicast πρωτόκολλο δρομολόγησης όπως π.χ το PIM-SM.

Τα shared δέντρα πάντα έχουν ένα root RP, το οποίο, για το BGMP, είναι ένα domain και όχι ένας απλός δρομολογητής. Η κύρια δουλειά του BGMP είναι να μάθει που βρίσκεται αυτό το RP. Όπως είπαμε, το root domain είναι το domain στο οποίο βρίσκεται ο δημιουργός του group. Οπότε, για να μάθει που είναι το root domain, το BGMP πρέπει να ξέρει ποιο domain κατέχει το πεδίο των διευθύνσεων που περιέχει την multicast διεύθυνση του group. Γι αυτό το λόγο το BGMP εξαρτάται από το MASC. Το MASC συσχετίζει τα multicast πεδία διευθύνσεων με συγκεκριμένα πεδία. Όταν το BGMP ξέρει το root domain, μπορεί να φτιάξει το ένα shared δέντρο για να διανέμει τα multicast δεδομένα.

Τα BGMP peers χρησιμοποιούν TCP συνδέσεις για να ανταλλάξουν πληροφορίες. Τα peers στέλνουν μεταξύ τους μηνύματα για να ανταλλάξουν πληροφορίες ελέγχου, όπως ποια μέλη έχουν συνδεθεί ή φύγει από μια ομάδα. Τα είδη των BGMP μηνυμάτων είναι όπως τα παρακάτω:

- Open, το οποίο χρησιμοποιείται για να ενεργοποιηθεί ένα session με ένα BGMP peer.
- Update, το οποίο μεταφέρει μηνύματα σύνδεσης, αποκοπής και προώθησης πληροφοριών μεταξύ των peers.
- Notification, το οποίο χρησιμοποιείται όταν ανιχνεύεται ένα λάθος.
- Keepalive, το οποίο χρησιμοποιείται για να κρατάει την TCP σύνδεση ζωντανή.

II.5 Αναφορές

1. The MASC/BGMP Architecture for Inter-domain Multicast Routing. Satish Kumart και Pavlin Radoslavov, David Thaler, http://netweb.usc.edu/cs551f00/papers/masc-bgmp-arch.pdf
2. An Overview of Inter-Domain Multicast Routing. White Paper. http://www.microsoft.com/windows2000/docs/intrdomain.doc

-

Παράρτημα III: Internet Multicast Addresses

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

224.0.0.0 Base Address (Reserved) [RFC1112,JBP]
224.0.0.1 All Systems on this Subnet [RFC1112,JBP]
224.0.0.2 All Routers on this Subnet [JBP]
224.0.0.3 Unassigned [JBP]
224.0.0.4 DVMRP Routers [RFC1075,JBP]
224.0.0.5 OSPFIGP OSPFIGP All Routers [RFC2328,JXM1]
224.0.0.6 OSPFIGP OSPFIGP Designated Routers [RFC2328,JXM1]
224.0.0.7 ST Routers [RFC1190,KS14]
224.0.0.8 ST Hosts [RFC1190,KS14]
224.0.0.9 RIP2 Routers [RFC1723,GSM11]
224.0.0.10 IGRP Routers [Farinacci]
224.0.0.11 Mobile-Agents [Bill Simpson]
224.0.0.12 DHCP Server / Relay Agent [RFC1884]
224.0.0.13 All PIM Routers [Farinacci]
224.0.0.14 RSVP-ENCAPSULATION [Braden]
224.0.0.15 all-cbt-routers [Ballardie]
224.0.0.16 designated-sbm [Baker]
224.0.0.17 all-sbms [Baker]
224.0.0.18 VRRP [Hinden]
224.0.0.19 IPAllL1ISs [Przygienda]
224.0.0.20 IPAllL2ISs [Przygienda]
224.0.0.21 IPAllIntermediate Systems [Przygienda]
224.0.0.22 IGMP [Deering]
224.0.0.23 GLOBECAST-ID [Scannell]
224.0.0.24 Unassigned [JBP]
224.0.0.25 router-to-switch [Wu]

224.0.0.26 Unassigned
[JBP]
224.0.0.27 AI MPP Hello
[Martinicky]
224.0.0.28 ETC Control [Polishinski]
224.0.0.29 GE-FANUC
[Wacey]
224.0.0.30 indigo-vhdp
[Caughie]
224.0.0.31 shinbroadband
[Kittivatcharapong]
224.0.0.32 digistar
[Kerkan]
224.0.0.33 ff-system-management
[Glanzer]
224.0.0.34 pt2-discover
[Kammerlander]
224.0.0.35 DXCLUSTER
[Koopman]
224.0.0.36 DTCP Announcement
[Cipiere]
224.0.0.37-224.0.0.68 zeroconfaddr (renew 12/02)
[Guttman]
224.0.0.69-224.0.0.100 Reserved
[IANA]
224.0.0.101 cisco-nhap
[Bakke]
224.0.0.102 HSRP
[Wilson]
224.0.0.103 MDAP
[Deleu]
224.0.0.104-224.0.0.250 Unassigned [JBP]
224.0.0.251 mDNS
[Cheshire]
224.0.0.252-224.0.0.255 Unassigned [JBP]

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

224.0.1.0 VMTP Managers Group [RFC1045,DRC3]
224.0.1.1 NTP Network Time Protocol
[RFC1119,DLM1]
224.0.1.2 SGI-Dogfight
[AXC]
224.0.1.3 Rwhod
[SXD]
224.0.1.4 VNP
[DRC3]
224.0.1.5 Artificial Horizons - Aviator
[BXF]
224.0.1.6 NSS - Name Service Server [BXS2]

224.0.1.7 AUDIONEWS - Audio News Multicast [MXF2]
224.0.1.8 SUN NIS+ Information Service [CXM3]
224.0.1.9 MTP Multicast Transport Protocol [SXA]
224.0.1.10 IETF-1-LOW-AUDIO [SC3]
224.0.1.11 IETF-1-AUDIO [SC3]
224.0.1.12 IETF-1-VIDEO [SC3]
224.0.1.13 IETF-2-LOW-AUDIO [SC3]
224.0.1.14 IETF-2-AUDIO [SC3]
224.0.1.15 IETF-2-VIDEO [SC3]
224.0.1.16 MUSIC-SERVICE [Guido van Rossum]
224.0.1.17 SEANET-TELEMETRY [Andrew Maffei]
224.0.1.18 SEANET-IMAGE [Andrew Maffei]
224.0.1.19 MLOADD [Braden]
224.0.1.20 any private experiment [JBP]
224.0.1.21 DVMRP on MOSPF [John Moy]
224.0.1.22 SVRLOC [Veizades]
224.0.1.23 XINGTV [Gordon]
224.0.1.24 microsoft-ds <arnoldm@microsoft.com>
224.0.1.25 nbc-pro <bloomer@birch.crd.ge.com>
224.0.1.26 nbc-pfn <bloomer@birch.crd.ge.com>
224.0.1.27 lmsc-calren-1 [Uang]
224.0.1.28 lmsc-calren-2 [Uang]
224.0.1.29 lmsc-calren-3 [Uang]
224.0.1.30 lmsc-calren-4 [Uang]
224.0.1.31 ampr-info [Janssen]
224.0.1.32 mtrace [Casner]
224.0.1.33 RSVP-encap-1 [Braden]

224.0.1.34 RSVP-encap-2
[Braden]
224.0.1.35 SVRLOC-DA [Veizades]
224.0.1.36 rln-server
[Kean]
224.0.1.37 proshare-mc
[Lewis]
224.0.1.38 dantz
[Zulch]
224.0.1.39 cisco-rp-announce
[Farinacci]
224.0.1.40 cisco-rp-discovery
[Farinacci]
224.0.1.41 gatekeeper
[Toga]
224.0.1.42 iberiagames
[Marocho]
224.0.1.43 nwn-discovery [Zwemmer]
224.0.1.44 nwn-adaptor
[Zwemmer]
224.0.1.45 isma-1
[Dunne]
224.0.1.46 isma-2
[Dunne]
224.0.1.47 telerate [Peng]
224.0.1.48 ciena
[Rodbell]
224.0.1.49 dcap-servers
[RFC2114]
224.0.1.50 dcap-clients [RFC2114]
224.0.1.51 mcntp-directory
[Rupp]
224.0.1.52 mbone-vcr-directory [Holfelder]
224.0.1.53 heartbeat [Mamakos]
224.0.1.54 sun-mc-grp [DeMoney]
224.0.1.55 extended-sys [Poole]
224.0.1.56 pdrncs
[Wissenbach]
224.0.1.57 tns-adv-multi
[Albin]
224.0.1.58 vcals-dmu
[Shindoh]
224.0.1.59 zuba
[Jackson]
224.0.1.60 hp-device-disc
[Albright]
224.0.1.61 tms-production
[Gilani]
224.0.1.62 sunscalar [Gibson]
224.0.1.63 mmtp-poll
[Costales]

224.0.1.64 compaq-peer
[Volpe]
224.0.1.65 iapp [Meier]
224.0.1.66 multihasc-com [Brockbank]
224.0.1.67 serv-discovery [Honton]
224.0.1.68 mdhcpdisover [RFC2730]
224.0.1.69 MMP-bundle-discovery1
[Malkin]
224.0.1.70 MMP-bundle-discovery2
[Malkin]
224.0.1.71 XYPOINT DGPS Data Feed [Green]
224.0.1.72 GilatSkySurfer [Gal]
224.0.1.73 SharesLive
[Rowatt]
224.0.1.74 NorthernData [Sheers]
224.0.1.75 SIP
[Schulzrinne]
224.0.1.76 IAPP
[Moelard]
224.0.1.77 AGENTVIEW
[Iyer]
224.0.1.78 Tibco Multicast1
[Shum]
224.0.1.79 Tibco Multicast2
[Shum]
224.0.1.80 MSP
[Caves]
224.0.1.81 OTT (One-way Trip Time) [Schwartz]
224.0.1.82 TRACKTICKER
[Novick]
224.0.1.83 dtn-mc
[Gaddie]
224.0.1.84 jini-announcement
[Scheifler]
224.0.1.85 jini-request
[Scheifler]
224.0.1.86 sde-discovery [Aronson]
224.0.1.87 DirecPC-SI [Dillon]
224.0.1.88 B1RMonitor [Purkiss]
224.0.1.89 3Com-AMP3 dRMON [Banthia]
224.0.1.90 imFtmSvc
[Bhatti]
224.0.1.91 NQDS4
[Flynn]
224.0.1.92 NQDS5
[Flynn]
224.0.1.93 NQDS6
[Flynn]
224.0.1.94 NLVL12
[Flynn]

224.0.1.95 NTDS1
[Flynn]
224.0.1.96 NTDS2
[Flynn]
224.0.1.97 NODSA
[Flynn] 224.0.1.98 NODSB
[Flynn]
224.0.1.99 NODSC
[Flynn]
224.0.1.100 NODSD [Flynn]
224.0.1.101 NQDS4R [Flynn]
224.0.1.102 NQDS5R [Flynn]
224.0.1.103 NQDS6R [Flynn]
224.0.1.104 NLVL12R [Flynn]
224.0.1.105 NTDS1R [Flynn]
224.0.1.106 NTDS2R [Flynn]
224.0.1.107 NODSAR [Flynn]
224.0.1.108 NODSBR [Flynn]
224.0.1.109 NODSCR [Flynn]
224.0.1.110 NODSDR [Flynn]
224.0.1.111 MRM
[Wei]
224.0.1.112 TVE-FILE
[Blackketter]
224.0.1.113 TVE-ANNOUNCE
[Blackketter]
224.0.1.114 Mac Srv Loc
[Woodcock]
224.0.1.115 Simple Multicast
[Crowcroft]
224.0.1.116 SpectraLinkGW
[Hamilton]
224.0.1.117 dieboldmcast [Marsh]
224.0.1.118 Tivoli Systems [Gabriel]
224.0.1.119 pq-lic-mcast [Sledge]
224.0.1.120 HYPERFEED
[Kreutzjans]
224.0.1.121 Pipesplatform
[Dissett]
224.0.1.122 LiebDevMgmg-DM
[Velten]
224.0.1.123 TRIBALVOICE
[Thompson]
224.0.1.124 Unassigned (Retracted 1/29/01)
224.0.1.125 PolyCom Relay1
[Coutiere]
224.0.1.126 Infront Multi1
[Lindeman]
224.0.1.127 XRX DEVICE DISC [Wang]
224.0.1.128 CNN
[Lynch]

224.0.1.129 PTP-primary
[Eidson]
224.0.1.130 PTP-alternate1
[Eidson]
224.0.1.131 PTP-alternate2
[Eidson]
224.0.1.132 PTP-alternate3
[Eidson]
224.0.1.133 ProCast
[Revzen]
224.0.1.134 3Com Discp
[White]
224.0.1.135 CS-Multicasting
[Stanev]
224.0.1.136 TS-MC-1
[Sveistrup]
224.0.1.137 Make Source [Daga]
224.0.1.138 Teleborsa [Strazzera]
224.0.1.139 SUMAConfig [Wallach]
224.0.1.140 Unassigned
224.0.1.141 DHCP-SERVERS
[Hall]
224.0.1.142 CN Router-LL [Armitage]
224.0.1.143 EMWIN [Querubin]
224.0.1.144 Alchemy Cluster
[O'Rourke]
224.0.1.145 Satcast One [Nevell]
224.0.1.146 Satcast Two [Nevell]
224.0.1.147 Satcast Three
[Nevell]
224.0.1.148 Intline
[Sliwinski]
224.0.1.149 8x8 Multicast
[Roper]
224.0.1.150 Unassigned
[JBP]
224.0.1.151 Intline-1
[Sliwinski]
224.0.1.152 Intline-2
[Sliwinski]
224.0.1.153 Intline-3
[Sliwinski]
224.0.1.154 Intline-4
[Sliwinski]
224.0.1.155 Intline-5
[Sliwinski]
224.0.1.156 Intline-6
[Sliwinski]
224.0.1.157 Intline-7
[Sliwinski]

224.0.1.158 Intline-8
[Sliwinski]
224.0.1.159 Intline-9
[Sliwinski]
224.0.1.160 Intline-10
[Sliwinski]
224.0.1.161 Intline-11
[Sliwinski]
224.0.1.162 Intline-12
[Sliwinski]
224.0.1.163 Intline-13
[Sliwinski]
224.0.1.164 Intline-14
[Sliwinski]
224.0.1.165 Intline-15
[Sliwinski]
224.0.1.166 marratech-cc
[Parnes]
224.0.1.167 EMS-InterDev
[Lyda]
224.0.1.168 itb301
[Rueskamp]
224.0.1.169 rtv-audio
[Adams]
224.0.1.170 rtv-video
[Adams]
224.0.1.171 HAVI-Sim
[Wasserroth]
224.0.1.172 Nokia Cluster [O'Rourke]
224.0.1.173 host-request
[K.Thompson]
224.0.1.174 host-announce
[K.Thompson]
224.0.1.175 ptk-cluster
[Hodgson]
224.0.1.176 Proxim Protocol
[Shukla]
224.0.1.177-224.0.1.255 Unassigned [JBP]
224.0.2.1 "rwho" Group (BSD) (unofficial)
[JBP]
224.0.2.2 SUN RPC PMAPPROC_CALLIT
[BXE1]

224.0.2.0 - 224.0.255.0 AD-HOC Block

224.0.2.064-224.0.2.095 SIAC MDD Service [Tse]
224.0.2.096-224.0.2.127 CoolCast [Ballister]
224.0.2.128-224.0.2.191 WOZ-Garage [Marquardt]
224.0.2.192-224.0.2.255 SIAC MDD Market Service [Lamberg]

224.0.3.000-224.0.3.255 RFE Generic Service [DXS3]
224.0.4.000-224.0.4.255 RFE Individual Conferences [DXS3]
224.0.5.000-224.0.5.127 CDPD Groups [Bob Brenner]
224.0.5.128-224.0.5.191 SIAC Market Service [Cho]
224.0.5.192-224.0.5.255 SIAC NYSE Order PDP protocol [Chan]
224.0.6.000-224.0.6.127 Cornell ISIS Project [Tim Clark]
224.0.6.128-224.0.6.255 Unassigned [IANA]
224.0.7.000-224.0.7.255 Where-Are-You [Simpson]
224.0.8.000-224.0.8.255 INTV [Tynan]
224.0.9.000-224.0.9.255 Invisible Worlds [Malamud]
224.0.10.000-224.0.10.255 DLSw Groups [Lee]
224.0.11.000-224.0.11.255 NCC.NET Audio [Rubin]
224.0.12.000-224.0.12.063 Microsoft and MSNBC [Blank]
224.0.13.000-224.0.13.255 UUNET PIPEX Net News [Barber]
224.0.14.000-224.0.14.255 NLANR [Wessels]
224.0.15.000-224.0.15.255 Hewlett Packard [van der Meulen]
224.0.16.000-224.0.16.255 XingNet [Uusitalo]
224.0.17.000-224.0.17.031 Mercantile & Commodity Exchange [Gilani]
224.0.17.032-224.0.17.063 NDQMD1 [Nelson]
224.0.17.064-224.0.17.127 ODN-DTV [Hodges]
224.0.18.000-224.0.18.255 Dow Jones [Peng]
224.0.19.000-224.0.19.063 Walt Disney Company [Watson]
224.0.19.064-224.0.19.095 Cal Multicast [Moran]
224.0.19.096-224.0.19.127 SIAC Market Service [Roy]
224.0.19.128-224.0.19.191 IIG Multicast [Carr]
224.0.19.192-224.0.19.207 Metropol [Crawford]
224.0.19.208-224.0.19.239 Xenoscience, Inc. [Timm]
224.0.19.240-224.0.19.255 HYPERFEED [Felix]
224.0.20.000-224.0.20.063 MS-IP/TV [Wong]

224.0.20.064-224.0.20.127 Reliable Network Solutions [Vogels]
224.0.20.128-224.0.20.143 TRACKTICKER Group [Novick]
224.0.20.144-224.0.20.207 CNR Rebroadcast MCA [Sautter]
224.0.21.000-224.0.21.127 Talarian MCAST [Mendal]
224.0.22.000-224.0.22.255 WORLD MCAST [Stewart]
224.0.252.000-224.0.252.255 Domain Scoped Group [Fenner]
224.0.253.000-224.0.253.255 Report Group [Fenner]
224.0.254.000-224.0.254.255 Query Group [Fenner]
224.0.255.000-224.0.255.255 Border Routers [Fenner]

224.1.0.0 - 224.1.255.255 (224.1/16) ST Multicast Groups [RFC1190,KS14]

224.2.0.0 - 224.2.255.255 (224.2/16) SDP/SAP Block

224.2.0.0 - 224.2.127.253 Multimedia Conference Calls [SC3]
224.2.127.254 SAPv1 Announcements [SC3]
224.2.127.255 SAPv0 Announcements (deprecated) [SC3]
224.2.128.0-224.2.255.255 SAP Dynamic Assignments [SC3]

224.3.0.0 - 224.251.255.255 Reserved [IANA]
224.252.000.000-224.255.255.255 DIS Transient Groups [IANA]
225.000.000.000-231.255.255.255 Reserved [IANA]
232.000.000.000-232.255.255.255 Source Specific Multicast [DRC3]
233.000.000.000-233.255.255.255 GLOP Block [RFC3180]
234.000.000.000-238.255.255.255 Reserved [IANA]

239.000.000.000-239.255.255.255 Administratively Scoped [IANA,RFC2365]

239.000.000.000-239.063.255.255 Reserved [IANA]
239.064.000.000-239.127.255.255 Reserved [IANA]

239.128.000.000-239.191.255.255 Reserved [IANA]
239.192.000.000-239.251.255.255 Organization-Local Scope [Meyer,RFC2365]
239.252.000.000-239.252.255.255 Site-Local Scope (reserved) [Meyer,RFC2365]
239.253.000.000-239.253.255.255 Site-Local Scope (reserved) [Meyer,RFC2365]
239.254.000.000-239.254.255.255 Site-Local Scope (reserved) [Meyer,RFC2365]
239.255.000.000-239.255.255.255 Site-Local Scope [Meyer,RFC2365]
239.255.002.002 rasadv [Thaler]