

Szakedolgozat

Dudics Zsolt

DE-IK
Informatikai Rendszerek és Hálózatok Tanszék
Debrecen
2008

Debreceni Egyetem

Informatikai Kar

Aktuális hálózati problémák megoldásainak
vizsgálata – IP Multicast

Témavezető:

Dr. Almási Béla
Egyetemi docens

Készítette:

Dudics Zsolt
mérnök informatikus (Bsc)

Debrecen, 2008

TARTALOMJEGYZÉK:

1. BEVEZETÉS	4
2. MI IS AZ A MULTICAST?	6
2.1 Hálózati címzés multicast adatforgalomnál.....	8
2.2 Ethernet címzés multicast adatforgalomnál.....	10
3. CSOPORTMENEDZSMENT	11
3.1 Internet Group Management Protocol (IGMP)	11
3.1.1 IGMP v1	11
3.1.2 IGMP v2	13
3.1.3 IGMP v3	15
3.2 Multicast Listener Discovery (MLD).....	17
4. MULTICAST TOVÁBBÍTÁSI ALGORITMUSOK.....	19
4.1 Naiv algoritmusok	20
4.1.1 Elárasztás	20
4.1.2 Adatkapcsolati szintű feszítő fák kiterjesztése multicast szintűre.....	21
4.2 Forrás alapú fa (Source-Based Tree) algoritmusok.....	21
4.2.1 Reverse Path Broadcasting (RPB).....	22
4.2.2 Truncated Reverse Path Broadcasting (TRPB)	23
4.2.3 Reverse Path Multicasting (RPM).....	23
4.3 Megosztott fa algoritmus	25
4.4 Steiner-fák	26
5. MULTICAST ÚTVÁLASZTÓ PROTOKOLLOK	27
5.1 Sűrű üzemmódú multicast útválasztó protokollok	27
5.1.1 Distance Vector Multicast Routing Protocol (DVMRP).....	28
5.1.2 Multicast Extensions to Open Shortest Path First (MOSPF)	32
5.1.3 Protocol Independent Multicast – Dense Mode (PIM-DM).....	36
5.2 Ritka üzemmódú multicast útválasztó protokollok	37
5.2.1 Protocol Independent Multicast – Sparse Mode (PIM-SM).....	38
5.2.3 Core Based Trees (CBT)	40
6. MULTICAST A GYAKORLATBAN – MBONE.....	42

6.1 Audió konferencia eszköz (Vat).....	43
6.2 Videó konferencia eszköz (Vic).....	45
6.3 Konferenciakatalógus (Session Directory).....	46
6.4 Osztott rajztábla (Whiteboard).....	47
7. ÖSSZEFOGLALÁS.....	49
8. IRODALOMJEGYZÉK.....	50
8.1 Szakirodalmak.....	50
8.2 Egyéb felhasznált irodalmak.....	53
9. KÖSZÖNETNYILVÁNITÁS.....	54

1. BEVEZETÉS

Napjainkban rohamos tempóban fejlődik a telekommunikáció, melynek szerves részét képezik az Internet és annak technológiái. A hagyományos, sok éves múltra visszatekintő élesen elkülönülő kommunikációs és hírközlő technológiákat mára felváltják az egységes, interneten keresztül megoldott technikák, mint például az IP-tévé vagy a VoIP szolgáltatások. Új szolgáltatásként megjelent a videokonferencia, mellyel a világ bármely pontján lévő ismerőseinkkel is tarthatjuk a kapcsolatot nem csak hang, de kép formájában, vagy akár üzleti megbeszéléseket is tarthatunk üzlettársainkkal. Az oktatás is nagy reformok előtt áll, egyre népszerűbb forma a távoktatás, ahol a hallgatók otthonról, számítógépük elől tudják elsajátítani a tananyagot élő előadásokon keresztül.

Ezen sokrétű, több területet is átfogó technológiák alapja a multicasting, mely arra hivatott, hogy egy időben több felhasználó is ugyanazt az információt szerezzék meg, földrajzi helytől függetlenül. A technológia nem új keletű, hiszen már a kilencvenes évek elején szabványosították, mégis csak napjainkban és a jövőben kerül szélesebb körben felhasználásra.

Napjainkban megnövekedett az adatforgalom, hiszen számos háztartásban jelenik meg az internet, egyre több ember használja a legújabb információs technológiákat, melyek sávszélesség-igénye napról napra növekszik. A multicast jellegű eljárások egyre nagyobb elterjedésével a megnövekedett adatforgalom kézben tartható sőt, jelentősen csökkenthető, mivel az egy időben ugyanazt az információt igénylő állomásoknak elegendő csupán egyszer, nem külön-külön elküldeni. Egy több résztvevős videokonferencia esetén pillanatok alatt eldugulna a hálózat, hiszen minden résztvevő audió és videó anyagát egyenként el kellene küldeni a hálózaton, ami tíz résztvevő esetén már százszoros forgalomműködést eredményezne.

A multicast technológia a mai napig nem megoldott kérdéseket vet fel, hiszen több összetevője az alap szabványon kívül nincs egyértelműen megfogalmazva. Alapvetően két problémakörrel beszélhetünk: az állomások megváltozott szerepköréről, illetve a multicast datagramok forgalomirányításáról a célállomás felé.

Dolgozatomban össze kívánom foglalni a multicast használatát, az általános bemutatáson keresztül, a ma használatos protokollokon át, egészen a gyakorlati megvalósításokig. Szeretnék külön kitérni az útválasztó algoritmusokra és gyakorlatban alkalmazott protokollokra, mivel ezek napjaink egyik legdinamikusabban fejlődő ágazatai az informatikai távközlésben. További motivációm, hogy magyar nyelven nem, vagy csak alig található a témával részletesen foglalkozó, egy helyen megtalálható írott anyag. Dolgozatom a későbbiekben nagy segítség lehet a magyar nyelven a témával foglalkozók számára, akik multicast jellegű problémákat szeretnének megoldani. A munkám tekinthető egyfajta, a Cisco Hálózati Akadémia tudását továbbvivő, másfajta protokollokat bemutató munkának is, mely egyben feltételezi is, hogy az olvasó némiképp jártas az informatikában, és a hálózati struktúrákban.

A dolgozat utolsó részében bemutatok néhány olyan multicast programot, amelyeket a gyakorlatban is alkalmazhatunk. Mint kiderül majd, ezek a programok nagymértékben multimédiás alkalmazások, melyek kényelmi vagy szórakoztató funkciókat látnak el.

2. MI IS AZ A MULTICAST?

„Az IP multicast technológia az Interneten való csoportos kommunikáció infrastrukturális háttérét hivatott biztosítani, megoldva a hálózati erőforrások hatékony és gazdaságos kihasználását.”¹

A multicast egy kommunikációs forma, amelyben egy adó (jelforrás) és tetszőleges számú vevő egy közös csatornát használva információt cserél. A legfontosabb tulajdonsága a pont-pont kommunikációval szemben, hogy az információmennyiség csak egy példányban áramlik át a hálózaton.

A multicastot az unicast és a broadcast közé szokás elhelyezni. Unicast esetében egy pont-pont kapcsolatról beszélünk, ahol az adó csak egy vevőnek küld üzenetet, az egyéni MAC cím alapján.

Broadcast estén az adó egy adott alhálózat minden állomásának elküldi az üzenetét, amit a MAC cím minden egyes bitjén csupa egyesekkel jelöl meg (FF-FF-FF-FF-FF-FF). Látható, hogy a túlzott broadcast üzeneteket kerülni kell, hiszen minden egyes ilyen módon feladott keretet az alhálózat összes gépének fel kell dolgoznia. A több címzettnek küldés másik, optimális esete a multicast, azaz a csoportos címzés. A multicast lehet az egyetlen megoldás olyan esetekben, ahol nagy sávszélességet igénylő adatforgalom zajlik nagyszámú, de hálózati szempontból egymáshoz közel elhelyezkedő gépek között. Ilyen esetekben ugyanis a multicast címzésnek megfelelően az adatokat nem kell minden gépnek külön-külön elküldeni, hanem elég csak egyszer a csoportcímre, ami jelentős sávszélesség megtakarítást eredményez az unicast móddal szemben.

Egy adó ilyen esetben úgy küld több vevőnek, hogy az csak egyszer jelenik meg a hálózatban. A multicast technológia tehát a felhasználók alkotta csoportokon belüli kommunikációt, adatközlést biztosít. A legtöbb esetben valamilyen multimédiával kapcsolatos alkalmazásokkal használatos, ahol általában nagy mennyiségű adatot kell párhuzamosan, egyszerre több számítógépnek eljuttatni. Ilyen esetekben a hagyományos unicast rendszerek könnyen telíthetik a rendelkezésre álló sávszélességet, mivel itt minden egyes résztvevőnek külön-külön el kell küldeni az adatokat, szemben a multicasttal, ahol lényegében egyetlen egy csoportos címre történik az adatok elküldése.

¹ NIIF intézet megfogalmazása szerint

Egy csoportnak tetszőleges számú tagja lehet, akár nulla is. A csoport tagsága dinamikus, azaz egy állomás bármikor elhagyhat vagy csatlakozhat egy csoporthoz, sőt, akár egyszerre többnek is tagja lehet. A felhasználók teljesen szabadon hozhatnak létre újabbakat is. Ha az egyik csoporttag kommunikálni szeretne a csoport összes többi tagjával, akkor az adatot a csoport címére kell elküldenie.

Az állomások három szintjét különböztetjük meg aszerint, hogy mennyire támogatják a multicast technológiát [3]:

0. szint: nem támogatott az IP Multicast

Ezek a gépek nem fogadhatnak és nem is küldhetnek multicast datagramokat.

1. szint: a küldés támogatott a fogadás viszont nem

Ez azt jelenti, hogy nem kell feltétlenül csatlakozni egy multicast csoporthoz, hogy tudjunk küldeni datagramokat a csoportnak

2. szint: teljesen támogatott az IP Multicast

Ezek az állomások ismerik a módját, hogy csatlakozzanak vagy kilépjenek multicast csoportokból, és képesek tudatni ezt az információt multicast útválasztókkal.

A mai operációs rendszerek közül az összes támogatja a multicast adatátvitelt.

Az állomásoknak valamilyen módszerrel jelezniük kell mind adatkapcsolati, mind hálózati rétegben, hogy jelenleg tagjuk-e valamelyik csoportnak, mivel csak így kaphatnak, illetve küldhetnek adatokat az éppen aktuális multicast csoportnak. Ehhez szükséges a korábbi unicast jellegű adatküldési formák kiterjesztése.

2.1 Hálózati címzés multicast adatforgalomnál

Multicast címzésre a hálózati rétegben a D osztályú IP címeket használhatjuk fel. Ezek első négy bitje mindig 1110, a további 28 bit nincs felosztva, azaz maradéktalanul a csoport azonosítására szolgál egy-két kivétellel. Az IP címek a 224.0.0.0 és 239.255.255.255 közötti tartományból kerülhetnek ki. Ezek a címek, mint célcímek szerepelnek, azaz egy csoport minden tagjának ugyanazzal a D osztályú címmel kell rendelkeznie. Amíg egy állomás tagja egy adott csoportnak, addig ideiglenesen D osztályú IP címmel rendelkezik, mellyel ugyanúgy küldhet és fogadhat datagramokat, mint a hagyományos IP címekkel. Ha elhagyja a csoportot, a D osztályú IP címe megszűnik, az operációs rendszer deaktiválja azt.

Kétféle csoportcímet különböztetünk meg: az ideiglenes és az állandó címeket. Az állandó címek egy jól meghatározott, létező csoportot címeznek. Ilyen cím például a 224.0.0.1 vagy a 224.0.0.2, melyeknek az összes állomás eleve tagja.

A tartomány további részekre osztott, ahol az egyes címek egyedi funkciókat látnak el. [14]

224.0.0.1	Összes IP rendszer (minden gazdagép) egy helyi hálózatban
224.0.0.2	Összes IP útválasztó egy helyi hálózatban
224.0.0.4	Összes DVMRP útválasztó (lásd. 27. oldaltól)
224.0.0.5	Összes OSPF útválasztó egy helyi hálózatban (lásd. 31. oldaltól)
224.0.0.6	Összes kijelölt OSPF útválasztó egy helyi hálózatban
224.0.0.13	Összes PIM útválasztó (lásd. 35. oldaltól)
224.0.1.1	Network Time Protocol [21]
239.0.0.0 - 239.255.255.255	adminisztratív terület

Az ideiglenes csoportok kialakítása a használatuk előtt történik. Ekkor a hosztok csatlakozhatnak a meghatározott csoporthoz. A multicast címtartomány egyes részei speciális célt szolgálnak. A 224.0.0.0/23 tartomány speciális alkalmazások számára van fenntartva, címeit az IANA osztja ki. Ennek első fele (224.0.0.0/24) a link-local tartomány, azaz ezeket a multicast csomagokat az útválasztók nem továbbítják, pontosan úgy, mintha a TTL mezőjük egyre lenne állítva.

Az unicast címekhez hasonlóan privát része is van a multicast címtartománynak, ez a 239.0.0.0/8. Ezeket a csoportokat minden szervezet önállóan, mindenféle korlátozás nélkül használhatja, de csak a saját rendszerén belül.

A címtartományból látszik, hogy valószínűleg nincs elegendő multicast cím az Internet összes, kamerával felszerelt gépéhez, melyek csoportot alkotnának társaikkal. Ez igaz is, viszont egyelőre nincs nagy érdeklődés iránta, másrészt az IPv6 bevezetésével ez a probléma megoldott lesz, mivel az IPv4 32 bites címzési rendszerét 128 bites rendszerré alakítják át, és a bevezetéséig nem várható, hogy a multicast dinamikus címei elfogynának.

Az IPv6-ban szintén léteznek multicast címzésre lefoglalt címek, melyek a 111 1111 (0xFF) formátumelőtagtól vannak kiosztva. [10]

- | | |
|-------------------|---|
| FF02::1 | Az össz-csomóponti cím, amelynek segítségével egy üzenetszórási tartomány összes csomópontja elérhető. |
| FF02::2 | Az össz-útvásztói cím, amelynek segítségével egy üzenetszórási tartomány összes útvásztója elérhető. |
| FF02::4 | Az össz-DVMRP (Distance Vector Multicast Routing Protocol) útvásztói cím, amelynek segítségével egy üzenetszórási tartomány összes DVMRP-csoportcímes útvásztója elérhető. |
| FF02::5 | Az össz-OSPF (Open Shortest Path First) útvásztói cím, amelynek segítségével egy üzenetszórási tartomány összes OSPF-útvásztója elérhető. |
| FF02::6 | Az össz-OSPF kijelölt útvásztói cím, amelynek segítségével egy üzenetszórási tartomány összes kijelölt OSPF-útvásztója elérhető. |
| FF02::1:FFXX:XXXX | A csomópont-megszólítási cím; a címfeloldási eljárásban ennek segítségével történik a kapcsolaton belüli csomópontok IPv6-címeinek feloldása kapcsolati rétegbeli címekre. A csomópont-megszólítási cím utolsó 24 bitje (XX:XXXX) azonos az egyedi IPv6-cím utolsó 24 bitjével. |

Egyetlen IPv6-csoportcím az összes csoporttagot egyidejűleg képes azonosítani, hasonlóan, mint az IPv4 esetében. Minden csoport fenntartott IPv6-címe a csoport összes tagállomása között meg van osztva, amelyek figyelik és fogadják a csoportcímre küldött összes IPv6-üzenetet.

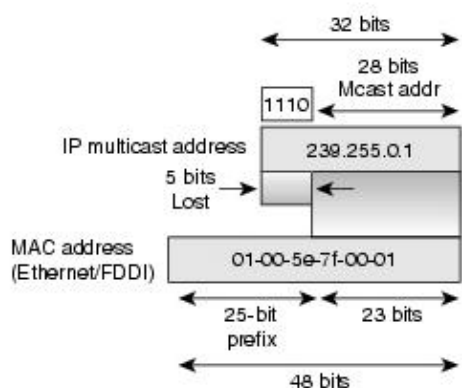
2.2 Ethernet címzés multicast adatforgalomnál

A második, adatkapcsolati rétegben szükséges a harmadik rétegbeli multicast címeket leképeznünk. Itt alapesetben az eszközök csak a saját MAC címükre, vagy a broadcast címmel ellátott üzenetek érkezésére reagálnak, a többi érkező keretet elutasítják, tehát nem megoldott, hogyan válogathatnák ki az adatkapcsolati hálózati eszközök, hogy az éppen érkezett keretet nekünk is címezték az egyik aktuális multicast csoportból vagy sem.

Erre a problémára megoldás a dinamikus MAC címek használata. Ekkor a gyári, eredeti MAC címen kívül további címek is beállíthatóak, amelyekre szintén reagál az eszköz. Ezt a lehetőséget kihasználva, és azt, hogy egy adott csoportnak ugyanaz legyen a dinamikus MAC címe, már megoldható a második rétegben is a multicast adatforgalom.

Ethernet és FDDI hálózatokban leképezés szükséges a harmadik és második rétegbeli multicast címek között, amely szabványban rögzített. [3] Kézenfekvő megoldás a már eleve közös IP címet felhasználni, ami négybájtos, a MAC viszont hat.

Legyen az első három bájton 01-00-5E. Ez a lefoglalt Ethernet címtartomány multicast címzésre van fenntartva. A további három bájton még 24 bitnyi információ fér el, de az IP cím 32 bites.



Mivel a D osztályú címek mindegyikének első négy bitje 1110, ezért a hasznos információ már csak 28 bit. Ha ezeken kívül még lemondunk néhány bitről, megkapjuk a közösen használható MAC címet.

Az IPv4 címből leképezett multicast Ethernet cím a következőképpen néz ki: 01:00:5e:0bbbbbbb:xx:xx, ahol az utolsó három byte megfelel a multicast IP cím utolsó három oktettjének, azzal a különbséggel, hogy az IP cím második oktettjének felső bitje elveszlik. Ezzel összesen öt bit veszlik el az IP címből, így jó pár különböző multicast csoport cím ugyanabba az adatkapcsolati címbe képződik le.

3. CSOPORTMENEDZSMENT

3.1 Internet Group Management Protocol (IGMP)

Az IGMP protokoll segítségével az állomások tagsági állapotra vonatkozó információcserét tudnak folytatni a csoportos küldést támogató IP-útválasztók és a multicast csoportok tagjai között, melynek megvalósítása mára kötelező az állomásokban, és az IPv6-ban már az ICMP szerves részét képezi majd. A multicast csoportokban szerzett tagságot az egyes tagállomások jelentik be, a tagsági állapot információt pedig a csoportos küldésű útválasztók rendszeresen lekérdezik. A csoport tagságaira vonatkozó információk alapján eldönthető, hogy az útválasztónak kell-e valamilyen multicast streamet továbbítania a hozzá közvetlenül kapcsolódó alhálózat felé.

Az IGMP hasonlóan az ICMP-hez, beépített része az IP protokollnak, az üzenetek a csomagokba ágyazódnak be. Sorozatos fejlesztések miatt mára három verziója is létezik a szabványnak.

3.1.1 IGMP v1

Az Igmp protokoll első verziója az RFC 1112-ben definiált. Minden egyes alhálózat útválasztója periodikusan „Host Membership Query” kérés üzenetet küld el, mellyel lekérdezi, hogy mely csoportnak vannak tagjai az alhálózaton. Az üzenet a 224.0.0.1 D osztályú címre címzett, és TTL értéke 1. Ez azt jelenti, hogy az üzenetet minden hoszt megkapja, de csak az adott alhálózaton belül lesz kézbesítve a datagram. Amikor egy állomás megkap egy ilyen kérést, egy úgynevezett „Host Membership Report” üzenettel válaszol rá, mely üzenetet minden egyes csoporttagnak címez. Lényeges különbség, hogy míg a kérés üzenetet minden egyes hoszt megkap az alhálózatban, addig a választ csupán a csoporttagok kapják meg. A riport-üzenet hasonlóan a kéréshez egyes TTL értékkel van feladva.

Mivel sok csoporttag esetén a riport üzenetek elárasztanák a hálózatot, ezért minden egyes hoszt, amely kérést kap, elindít egy pszeudo-random generátort, melynek lejártá után küldhet

csak választ a kérésre. Ha a várakozás közben egy másik riport üzenet érkezik a hoszthoz, akkor az időzítő újraindul. Ezzel a mechanizmussal elkerülhető, hogy riport üzenetek bombázzák meg egyidejűleg a hálózathoz tartozó útválasztót.

Az útválasztók egy egyszerű listát tartanak karban, amely csupán annyit tartalmaz, hogy mely csoportnak vannak jelen tagjai az alhálózatban. Nincs szükség részletes adatokra, mivel ha már csak egy csoporttag is van, akkor már szükséges az adott csoporthoz tartozó multicast adatokat továbbítani az alhálózat felé. Mivel a listának mindig aktuálisnak kell lennie, ezért az útválasztó periodikusan kéréseket küld ki, amelyekre válaszolva tartja karban a listát.

Ha nem érkezik riport meghatározott ideig egy adott csoportra vonatkozó kérésre, akkor az útválasztó számára már nincs jelen egy darab csoporttag sem, így a csoporthoz tartozó multicast adatok továbbítása megszűnik az adott interfészen. A csoport elhagyása tehát csendben történik, azaz ha egy hoszt már nem tagja egy csoportnak, akkor egyszerűen nem válaszol a kérésre tovább.

Új csoporttag, vagy esetleges új csoport esetén a hoszt közvetlenül egy IGMP Report üzenetet küld el az útválasztó felé, mellyel azonnal értesíti a routert, így nem szükséges kivárnia a kérés üzenet megérkezését.

Az IGMP üzenet az IP-csomagon belül 6 bájtot foglal el. Szerkezete a következő ábrán látható:

verzió	típus	használaton kívül	ellenőrző összeg
csoport cím			

Verzió: négy bit, itt tároljuk, hogy épp milyen verziójú IGMP üzenetet küldünk.

Típus: négy bit, ami háromféle értéket vehet fel: 1, ha az üzenet Host Membership Query, 2 ha az üzenet Host Membership Report vagy 3, ha DVMRP útválasztó üzenet

A második oktett használaton kívüli, ha a csomag küldött, akkor nullázott, ha fogadott, akkor figyelmen kívül hagyott.

A harmadik és a negyedik oktett egyben (16 bit) az ellenőrző összeg.

A csoport cím (32 bit) tartalmazza a multicast csoport címét abban az esetben, ha a csomag Host Membership Report, különben nullázott.

3.1.2 IGMP v2

Az IGMP protokoll második verziója az RFC 2236-ban található. A DVMRP (Distance Vector Multicast Routing Protocol) részeként határozták meg, az úgynevezett „mouted” forráskód implementálásában jelent meg először a gyakorlati alkalmazása, amely segítségével Unixos gépeken lehet a DVMRP útválasztó protokollt futtatni. Az implementáción felül további számos bővítést tartalmaz a protokoll, amely visszafelé kompatibilis az eredeti IGMP-vel.

Fontos változás, hogy az IGMP második verziójába bekerült egy szelekciós folyamat, amely segítségével, ha több útválasztó is található egy alhálózatban, mindig a legkisebb IP című router lesz a megbízott az IGMP kérések kiküldésére.

További lényeges különbség a megújított Query azaz kérés üzenet. A második verziós IGMP protokoll csoport specifikus kérés üzenetet vezetett be, melynek segítségével lehetősége van az útválasztónak egy megadott csoportnak kérést küldenie, mivel a kérések már nem a 224.0.0.1 összes hoszt címre lesznek kiküldve, hanem mindig egy megadott csoportcímre.

A csoportelhagyás módja is megváltozott az IGMP második verziójában. Ha egy hoszt már nem kíván tovább tagja lenni egy csoportnak, akkor ezentúl nem csupán nem válaszol a kérésekre, hanem egy úgynevezett „Leave” elhagyó üzenetet kell kiküldenie a 224.0.0.2 D osztályú IP címre, amely az összes útválasztót címzi. Ebben az üzenetben értesíti az útválasztókat a hoszt, hogy pontosan melyik csoportnak nem kíván tovább tagja lenni. Ha egy ilyen üzenetet kap egy útválasztó, fontos feladata eldönteni, hogy van-e még az adott csoportnak tagja az alhálózatban, vagy a „Leave” üzenetet feladó hoszt volt-e az utolsó csoporttag. Hogy ezt eldöntse, a beérkezést követően felad egy, a csoportnak címzett kérést, és ha megadott ideig nem érkezik rá riport, akkor úgy veszi, hogy már nincs a csoportnak aktív tagja az alhálózatban.

A csoportelhagyás módjának átdefiniálása „ésszerűbbé” teszi a protokoll alkalmazását. Az IGMP első verziójában, ha egy állomás el akar hagyni egy csoportot, egyszerűen nem tesz semmit, és majd az útválasztó dönti el hiányos információ alapján (várakozás), hogy van-e még tagja az adott csoportnak. Ezzel szemben az IGMP második változatában ez a beépített

mechanizmus gyorsabban és pontosabban meghatározza az aktív vagy éppen a már nem aktív csoporttagokat.

Végezetül az utolsó módosítás a protokollban, hogy az IGMP Query csomag szerkezete egy újabb mezővel egészült ki, a maximum várakozási idővel, amely megadja, hogy a hosztok maximálisan mennyi időt várakozhatnak, mielőtt riportot küldenek vissza. A várakozás közben történhető események nem változtak az első verzió óta.

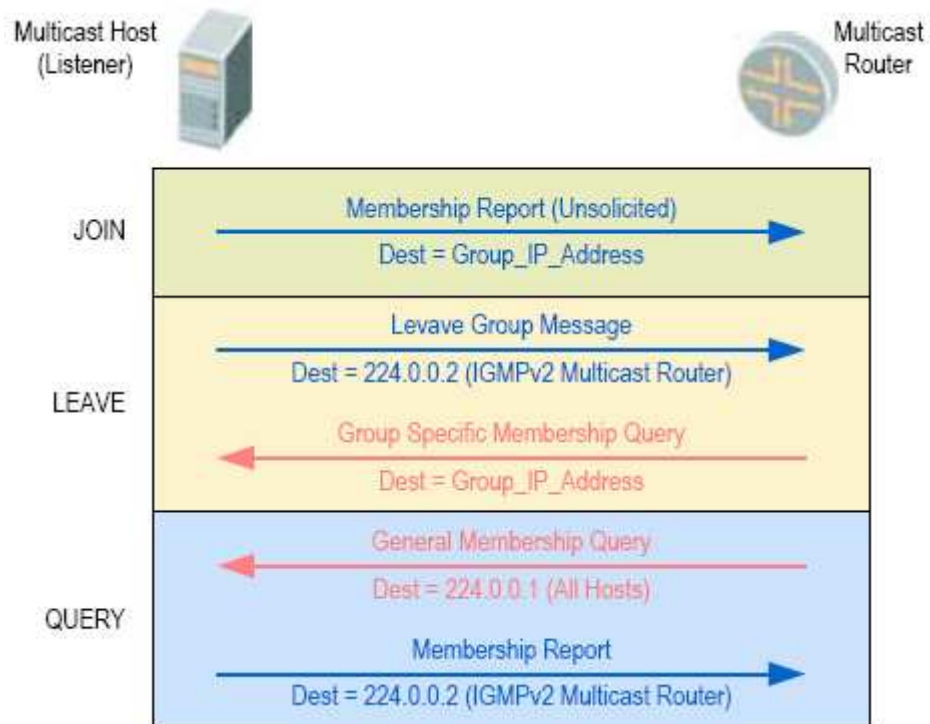
Az IGMP v2 csomagszerkezete a következő ábrán látható:

verzió	tipus	max válaszolási idő	ellenőrző összeg
csoport cím			

Ha egy szegmensben mindkét IGMP verziót használó eszközök is vannak, akkor a következő szabályok vannak érvényben:

- ha egy állomás IGMPv2-t tud, de a router csak IGMPv1-et, akkor a query üzenetre v1-es verziójú report üzenetet kell küldeni
- a csoport elhagyásakor nem kötelező Leave üzenetet küldenie az állomásnak, de ha küld nem gond
- ha a query-küldő router IGMPv2-t tud, akkor detektálnia kell, hogy van v1 hoszt a hálózatban, mivel a v1 hosztok nem tudnak a query response interval-lal mit kezdeni. Ebben az esetben a routernek ignorálnia kell a Leave üzeneteket, hiszen az erre válaszul küldendő group specific query-t nem fogják felismerni a v1 hosztok.
- ha több router van egy hálózatban, akkor minden routernek ugyanazon IGMP verziót kell futtatnia. Cisco routereknél ezt kézzel kell konfigurálni.

Az IGMP v2 működése szemléltetve:



3.1.3 IGMP v3

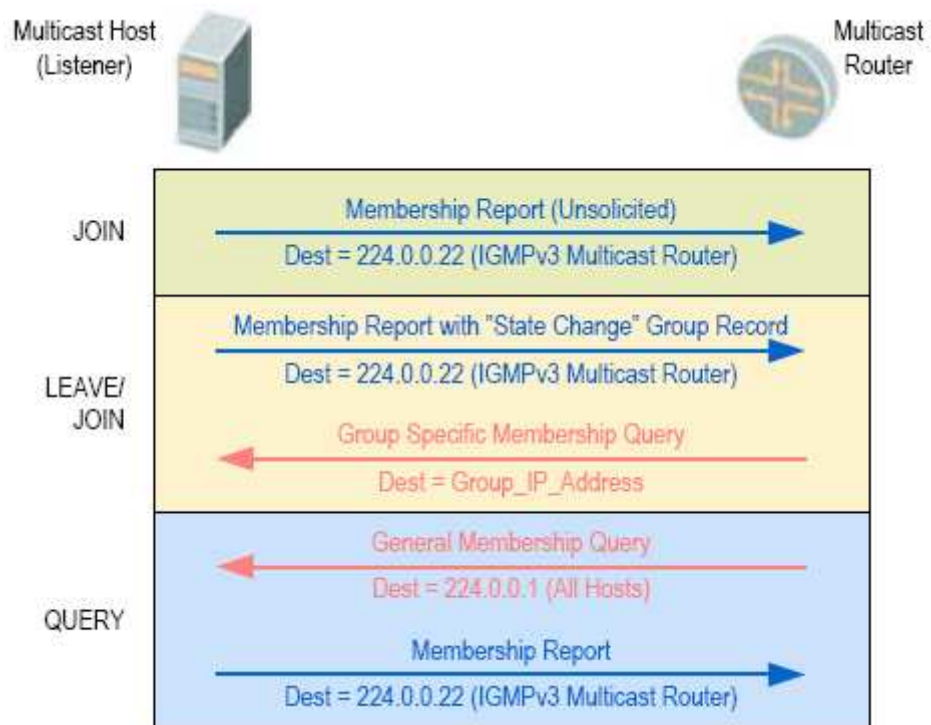
Az IGMP harmadik változata a legújabb, amely az RFC 3376-ban definiált, kisebb módosításokat tartalmaz a második verzióhoz képest. Az IGMP 3-as verziójának legfőbb újítása az SSM (Source-Specific Multicast) azaz a forrás-specifikus multicast lehetősége. Az SSM segítségével a multicast adatfolyamok forrás specifikusan lekérhetők, azaz a multicast csoportot a multicast IP cím és a forrás IP címe együttesen határozza meg.

A protokoll tartalmaz egy Group-Source Report üzenetet, amely segítségével minden egyes hoszt meghatározhatja, hogy a csoportban mely forrásoktól szeretnének multicast datagramokat fogadni. Egy úgynevezett beemelő (inclusion) Group-Source Report üzenet segítségével a hosztok megadhatják azoknak a forrásoknak az IP címeit, amelyektől szeretnének multicast datagramokat fogadni, és egy kizáró (exclusion) Group-Source Report

üzenet segítségével adhatják meg azoknak a forrásoknak a listáját, amelyet blokkolni szeretnének. Az IGMP első két verziójában, ha egy állomás multicast datagramokat szeretne fogadni, akkor a csoport összes forrásától megindul majd az adatforgalom az állomás felé. Ezzel a megoldással lényeges sávszélesség takarítható meg.

További módosítás a szabványban, hogy kiterjesztették a csoport-elhagyó üzeneteket, amit az IGMP második verziójában vezettek be. A harmadik verzióban bevezetésre került az úgynevezett csoport-forrást elhagyó (Group-Source Leave) üzenet, ami segítségével a hosztok elhagyhatnak egy teljes csoportot, vagy megadhatják azoknak a forrásoknak az IP címét, amely (forrás, csoport) párost el szeretnék hagyni.

Az IGMP v3 működése szemléltetve:



3.2 Multicast Listener Discovery (MLD)

Az MLD aszimmetrikus protokoll lehetővé teszi, hogy IPv6 esetében az állomások a tagsági állapotról vonatkozó információk cseréjét a csoportos küldést támogató IPv6-útválasztók felé jelezzék, illetve az útválasztók a tagsági állapot információt rendszeresen lekérdezhessék. Gyakorlatilag az IGMP csoportmenedzsment protokoll IPv6-os változata, az RFC 2710-ben definiált.

A routerek az MLD protokoll segítségével követik, hogy mely multicast címhez van az általuk felügyelt linkeken reprezentáns. Minden router a csatlakozó linkek viszonylatában listát vezet, amely tartalmazza, hogy mely multicast címhez van reprezentáns a kérdéses linken. Minden kapcsolódó link vonatkozásában valamely router kiválasztja egy lehetséges link lokális unicast címet, amelyet az általa küldött MLD csomagokban forrás címként használ az adott linken. Az IGMP üzenetekhez hasonlóan itt is Query és Report üzenetek vannak, melyek jelzik az útválasztók felé, hogy valamely állomás tagja-e épp egy multicast csoportnak.

Az MLD protokoll szerkezete a következő ábrán látható:

típus	kód	ellenőrző összeg
max válaszadási idő		foglalt
multicast cím		

Típus: nyolcbites, az MLD üzenet típusát határozza meg. Az alábbi értékeket veheti fel:

- 130: Multicast Listener Query
- 131: Multicast Listener Report
- 132: Multicast Listener Done
- 143: MLDv2 Multicast Listener Report

Kód: nyolcbites, további meghatározója az MLD üzenetnek. Nullázott a forrásnál, figyelmen kívül hagyott a vevő oldalon.

Ellenőrző összeg: 16 biten tárolódik.

Max válaszadási idő: 16 bites, ez a mező csak a Query üzenetknél jelentős, ahol meghatározza a maximális várakozási időt, mielőtt az állomás visszaküldene egy Report üzenetet az útválasztónak.

Foglalt: 16 bites, nullázott a forrásnál, figyelmen kívül hagyott a vevőnél. Későbbi, a protokoll megújítása során felhasználható mező.

Multicast cím: 128 bites, Query üzenetnél ez a mező nullázott, ha általános kérés, egyébként adott multicast IPv6 címet tartalmaz.

4. MULTICAST TOVÁBBÍTÁSI ALGORIMTUSOK

Az IGMP protokoll bevezetésével lehetővé vált, hogy multicast címekre küldjünk adatokat, ha azok egy alhálózaton belül helyezkednek el. Viszont egyáltalán nem biztosít semmilyen lehetőséget, ha összekapcsolt hálózatokon és útválasztókon át szeretnénk egy vagy több állomásra datagramokat küldeni. Ebben az esetben útválasztó algoritmusok és protokollok segítségével történik az adattovábbítás. Egy multicast útválasztó protokoll felelős a helyes továbbítási fák meghatározásáért illetve a csomagok továbbításáért. Minden szabványos, elfogadott protokoll mögött egy vagy több útválasztó algoritmus áll, melyek egyértelműen meghatározzák a működés feltételeit és alapjait.

Az algoritmusokat négy nagy csoportba sorolhatjuk bonyolultságuk és alapötletük szerint:

- Naiv algoritmusok:

- elárasztás
- adatkapcsolati szintű feszítő fák kiterjesztése multicast szintűre

- Forrás alapú fa (Source-Based Tree) algoritmusok:

- Reverse Path Broadcasting (RPB)
- Truncated Reverse Path Broadcasting (TRPB)
- Reverse Path Multicasting (RPM)

- Megosztott fa algoritmus

- Steiner-fák

4.1 Naiv algoritmusok

Az elárasztás és a feszítő fák kiterjesztése a legegyszerűbb algoritmusok. Primitívek, mivel nagy sávszélességet igényelnek, és viszonylag nagy számítási kapacitást a routerektől. Használatuk ezért elsősorban csak kis hálózatokban javallott, ahol kevés állomás található, és ezek is csak kevés csoport tagjai lehetnek egyszerre. Kiforratlansága miatt napjainkban nem használatosak.

4.1.1 Elárasztás

A legegyszerűbb módja annak, hogy a multicast datagramokat eljuttassuk a hálózat összes útválasztójának, és ezzel egyúttal a csoport összes tagjának. [11] A módszer lényege a következő: ha egy routerhez érkezik egy bejövő multicast csomag, amely belátható időn belül még nem érkezett hozzá, akkor azt az összes portján keresztül továbbküldi, kivéve azon, amelyiken megkapta. Ha már korábban megkapta a bejövő csomagot, akkor elutasítja. Ezzel a módszerrel biztosítható, hogy az összes útválasztóhoz elérjen a csomag rövid időn belül. A módszerhez mindössze egy olyan technikát kell biztosítani, mellyel a routerek vizsgálni tudják a bejövő csomagokat, hogy megkapták-e már őket korábban. Legegyszerűbben időbélyeggel lenne megoldható a vizsgálat, de IP csomagban nem lehet elhelyezni, ezért egyszerűen tárolni kell az utolsó „néhány” továbbított csomagot. A módszer hátránya éppen ez a lista, ami gyors hálózatokon meglehetősen hosszú lehet, és amelyek kezelése nagy erőforrások lefoglalásába kerül. Másfelől azt ugyan garantálja, hogy egy router nem küld el egy csomagot kétszer, azt viszont nem, hogy nem is kapja meg kétszer ugyanazt.

Magát az algoritmust nagyon egyszerű implementálni, mivel nem szükséges hozzá routing táblát fenntartani, csupán vizsgálatokat tartani. Egyszerűsége ellenére nem hatékony, alkalmazásával duplikálódott csomagok sokasága lepheti el a hálózatot, gyakorlati jelentősége nincs.

4.1.2 Adatkapcsolati szintű feszítő fák kiterjesztése multicast szintűre

Ez a módszer sokkal hatékonyabb megoldás, mint az elárasztás. Lényege, hogy mindig kiválasztunk egy, a hálózat részét képező feszítő fát. A feszítő fa egy olyan struktúra, ahol mindig csak egy aktív útvonal létezik bármelyik két pont között a hálózatban. [11]

Miután kialakult a feszítő fa, az útválasztó egyszerűen továbbítja a beérkezett multicast csomagokat az összes olyan portján, amely tagja a feszítő fának, kivéve azon, amelyiken beérkezett. A csomagok továbbítása az elágazások mentén garantálja, hogy duplikálódások nélkül eljutnak minden routerhez a hálózatban, mivel a fa körmentes és nem tartalmaz hurkokat.

Ez a technika szintén egyszerűen megvalósítható, mivel számtalan módszer létezik már feszítő fák kialakítására. Hátránya, hogy nagy, bonyolult hálózatban nagyon nagy számítási kapacitás szükséges a fa meghatározásához, illetve könnyen előfordulhat, hogy a hálózati forgalom csupán néhány központi linkre csoportosul, torlódásokat okozva a hálózaton.

4.2 Forrás alapú fa (Source-Based Tree) algoritmusok

Ezek az algoritmusok a feszítő fa elméletét viszik tovább, de annál sokkal eredményesebben. Minden egyes forráshoz külön meghatározásra kerül egy fa, így még hatékonyabbá tehető a multicast csomagok kézbesítése, mivel elkerülhető a forgalom centralizálása.

4.2.1 Reverse Path Broadcasting (RPB)

A forrás alapú fa algoritmusok legrégebbi tagja. A hálózat méretű fa helyett minden egyes potenciális forráshoz az alhálózatban külön feszítő fát határozunk meg, melyek közvetlenül kapcsolódnak a legközelebbi útválasztóhoz. Így mindig a forrástól függően más fa mentén kerül továbbításra az adat. [11]

Az RPB alap algoritmus meglehetősen egyszerű. Ha egy linken érkezik egy csomag, a router ellenőrzi, hogy a forráshoz képest az adott link a legközelebbi úton van-e. Ha igen, akkor az adott link kivételével az összesen keresztül továbbítja a multicast datagramot. Ha a csomag nem a legközelebbi interfészen keresztül érkezett a forrástól, akkor a router eldobja azt.

Azt a linket, amelyen keresztül fogadta a helyes csomagokat szülő linknek nevezik, míg azokat, melyeken továbbításra kerültek: gyerek linkek.

Az algoritmus egyszerűsége miatt könnyen redukálható szükségtelen duplikálódott csomagokat, viszont könnyen továbbfejleszthető, hogy csökkentsük ennek a valószínűségét. Ha egy helyi router a továbbítás mellett dönt, akkor meghatározhatja, hogy a gyerek linken lévő szomszédos útválasztó a legrövidebb úton található-e. Ezt gyakran nevezik „downstream” linknek. Ha valamelyik szomszédos útválasztó nem „downstream”, akkor felesleges továbbküldeni a multicast csomagokat azokba az irányokba, hiszen úgyis kiejti majd őket. Ezzel a módszerrel javítható az RPB hatékonysága.

Ezt az információt viszonylag könnyen megszerezhetjük, mivel a link-állapot alapú útválasztó protokolloknál az útválasztók eleve ismerik a teljes hálózat topológiáját, melyből könnyen meghatározható, hogy mely link mentén jutunk zsákutcába.

Ha távolság-vektor alapú protokollt használunk, akkor viszont a szomszédos router láthatja, hogy az előző ugrásnál jobb metrikával rendelkezik, így az útvonalak mérgezésével meggátolhatja a helytelen irányba való továbbítást.

Az RPB legnagyobb előnye, hogy meglehetősen hatékony, és könnyen implementálható. Nem szükséges, hogy a router tudja a teljes feszítő fát, és nincs szükség különböző speciális mechanizmusokra sem, hogy leállítsa a továbbítást, mint a hagyományos feszítő fáknál, mivel garantált, hogy eleve csak a legrövidebb úton haladhatnak a csomagok. Másik nagy előnye, hogy mivel a csomagok különböző fák mentén továbbítódnak, a forgalom eloszlik. Egyetlen hátránya, hogy nem veszi számításba a multicast csoport információkat a szórás fák

elkészítésénél, így olyan csoportoknak címzett datagramokat is továbbíthat a hálózatba, amely csoportnak épp nincs is tagja ott.

4.2.2 Truncated Reverse Path Broadcasting (TRPB)

A TRPB alapvetően az RPB hiányosságait javallott kiküszöbölni. Az IGMP információival ellátott, így a multicast routerek meghatározhatják a csoporttagságot minden egyes levél, azaz további útválasztókat nem tartalmazó alhálózatban. Így elkerülhető, hogy olyan datagramok is bekerüljenek a hálózatba, amelyeket olyan csoportnak címeztek, melynek jelenleg nincs is tagjuk épp ott.

A csoporttagság információi alapján az útválasztó csonkolhatja a levél szinten lévő alhálózatra vonatkozó feszítő fát, ha nincs aktív csoporttag, innen ered az algoritmus neve.

Ezzel a megoldással jelentősen továbbjavítható az RPB algoritmus, bár így is csak a problémák egy részét oldja meg. Bár kiküszöböli, hogy ne kerüljön felesleges forgalom a levél hálózatokba, nem szünteti meg a szükségtelen forgalmat a nem-levél hálózatok között.
[11]

4.2.3 Reverse Path Multicasting (RPM)

Az RPM algoritmus az RPB és a TRPB továbbfejlesztése, további ismert neve az RPB tisztítással.

Az RPM egy olyan kézbesítési fát alakít ki, amely csak a következőket íveli át:

- alhálózatok csoporttagokkal
- útválasztók és alhálózatok a legrövidebb út mentén a csoporttagokat tartalmazó alhálózatok felé

Az eljárás megengedi, hogy a forrás alapú legrövidebb utat tartalmazó kézbesítési fát megtisztítsuk, így a multicast datagramok csak azon elágazások mentén haladjanak előre, hogy végül csak az aktív csoporttagok felé kerülhessenek a hálózatban.

Amikor egy útválasztó megkap egy csomagot a (forrás, csoport) pártól, akkor az első csomagot TRPB módon továbbítja minden lehetséges routernek a hálózatban. A TRPB garantálja, hogy legalább az első csomagot a levél szinten elhelyezkedő útválasztók is megkapják. Ha van a levélszinten az adott csoportnak tagja, akkor továbbítja a multicast csomagokat a csoportmenedzsmenet információi alapján a tagoknak. Viszont ha nincs egyetlen tagja sem a csoportnak a levélszinten, akkor a levél- router a szülő linkjén keresztül visszaküld egy „tisztító” (prune) üzenetet, amely egy ugrásnyit visszafelé halad a feszítőfa mentén (upstream). Ez az üzenet tájékoztatja az eredetileg továbbküldő útválasztót, hogy ebben a (forrás, csoport) párban az adott linken keresztül nem található egyetlen csoporttag sem, így azon a gyerek-link mentén felesleges tovább küldenie az adott (forrás, csoport) multicast datagramokat. Ezt a tisztító üzenetet tárolnia kell a memóriájában az útválasztónak. Ha egy upstream router az összes linkjéről tisztító üzenetet kap vissza, akkor teljesen felesleges bármelyik linkjén keresztül továbbítani, így maga is generálhat egy tisztító üzenetet, amelyet az ő upstream routerének küldhet el az ő szülő linkjén keresztül.

A tisztító üzenetek kaszkádja egy nagyon hatékony multicast kézbesítési fát eredményez, amely kizárólag az aktív ágakból tevődik össze.

Minthogy a csoportmenedzselési és a hálózati topológiai információkat dinamikusan lehet cserélni, ugyanúgy lehetőség van rá, hogy a multicast kézbesítési fa letisztított állapotait is periodikusan frissítsük. Szabályos időközönként a tisztítási információk érvényüket veszítik a memóriában, és az ezt követő első datagramot megint az összes downstream routernek kézbesítik. Ezzel a módszerrel az esetlegesen inaktívvá vált tagokat is gyorsan ki lehet szűrni.

Minthogy a legtöbb algoritmusnak, az RPM-nek is vannak hátrányai. Az egyik, hogy a multicast csomagokat periodikusan broadcastolni kell minden útválasztón keresztül az összes levél alhálózat felé. Ez a sávszélesség pazarlásával jár mindaddig, amíg fel nem épül a letisztított állapotot jelző kézbesítési fa.

Mivel a hálózat összes routerének részt kell vennie az RPM algoritmusban, ezért az összesnek tárolnia kell minden egyes (forrás, csoport) párost, ami nagy hálózatokban viszonylag nagy erőforrást igényelhet. [11]

4.3 Megosztott fa algoritmus

A legkorszerűbb módja a multicast továbbítási technikáknak a megosztott kézbesítési fák használata. A legrövidebb út algoritmusokkal ellentétben, ahol minden egyes forráshoz, vagy (forrás, csoport) párhoz egy feszítő fa kerül meghatározásra, a megosztott fa algoritmus csupán egyetlen kézbesítési fát hoz létre, amelyet megoszt a csoport összes tagjával a hálózaton. Az alapelv meglehetősen hasonlít a feszítő fához, azzal a kivétellel, hogy meghatároz minden egyes csoport számára egy különböző megosztott fát. Ha egy állomás adatot szeretne fogadni egy multicast csoporttól, csatlakoznia kell a csoporthoz definiált megosztott fához, így az adatforgalom mindig csoporttól függően különböző feszítő fán keresztül halad azonos forrás esetén is.

A fa állhat egyetlen útválasztóból, vagy azok halmazából is, amelyek tartalmazzák a kézbesítési fa magját. Hasonlóan a többi multicast továbbító algoritmusokhoz, a megosztott fa algoritmus sem követeli meg a forrástól, hogy tagja legyen annak a csoportnak, melynek küldeni szeretne.

A skálázhatóság terén, a forrás alapú fákkal szemben lényegesen előnyösebb ez az algoritmus. Nincs szükség különösen nagyobb erőforrásokra, mivel elegendő csupán a csoport menedzseléséből származó információkat tárolni, szemben a forrás alapú fáknál alapvető jelentőségű információknál. Nem szükséges tárolni minden egyes forrást vagy (forrás, csoport) párost. Ezzel a javítással elérhető, hogy a küldők számának növekedése lényegesen ne befolyásolja az elérhető teljesítményt.

Másik nagy előnye az algoritmusnak, hogy nem szükséges periodikusan elárasztania az összes útválasztónak a hálózatot a levél szintű alhálózatok felé. Ezzel további értékes sávszélesség takarítható meg, különösen a kis sávszélességű WAN² linkeken keresztül.

Minden előny ellenére, mint mindennek, a megosztott fáknak is vannak hátrányaik. Mivel nem készül minden forráshoz külön kézbesítési fa, könnyen torlódás alakulhat ki a hálózaton, főleg a fa magját alkotó útválasztók közelében, mivel egy adott csoport minden egyes forrásától ugyanazonokon a linkeken keresztül történik a továbbítás.

További probléma, hogy egyáltalán nem garantált az optimális út meghatározása, és bár az algoritmus számos előnye miatt sávszélesség takarítható meg, szimulációkkal bizonyított,

² WAN: Wide Area Network

hogy a forrás alapú fákkal szemben 10 százalékkal nagyobb várakozási idő alakul ki, ha multimédia alkalmazásokra használjuk a multicast továbbítást. [11]

4.4 Steiner-fák

A forrás alapú fa algoritmusok a multicast csomagok kézbesítésére a legrövidebb utat keresik, ezzel biztosítva a lehető leggyorsabb kézbesítést, viszont egyáltalán nem foglalkoznak az erőforrások optimális kihasználásával.

Steiner-fának nevezzük az a fát, amely minimális költségű, azaz a csatlakozások száma minimális a feszítő fában.

A csatlakozások minimalizálásával erőforrást takaríthatunk meg, bár a csomagok lassabban jutnak célba, mivel esetenként jóval hosszabb útvonalon keresztül jutnak csak oda. Bár későbbiekben, ha nagyobb sáv szélesség érhető el széles körben, és az útválasztók is jóval nagyobb teljesítményűek lesznek, alkalmazható lesz ez a technológia, addig csupán elméleti szinten létezik, mivel hatalmas számítási kapacitás szükséges hozzá, nem beszélve arról, hogy nem elegendő csupán egyszer meghatározni a fát, minden egyes csoportba lépéskor illetve elhagyáskor újból számolni szükséges. Gyakorlati jelentősége ma még elhanyagolható.

5. MULTICAST ÚTVÁLASZTÓ PROTOKOLLOK

Az előbbieken tárgyalt, elméletben működő algoritmusoknak számos, a gyakorlatban használt implementációja létezik, melyekkel megvalósítható a tényleges multicast adattovábbítás a hálózat bármely pontjai között.

Alapvetően két csoportja létezik a multicast útválasztó protokolloknak: a sűrű és a ritka módú protokollok. A sűrű mód arra utal, hogy a csoport tagjai sűrűn helyezkednek el a hálózatban, illetve a rendelkezésre álló sávszélesség is viszonylag nagy. Ezzel szemben a ritka mód azt feltételezi, hogy a csoporttagok ritkán helyezkednek el, illetve a sávszélesség is csekély, azaz például sok, Interneten keresztül vezető út van a kézbesítési fában. Megjegyzendő, hogy a ritka mód nem jelenti azt, hogy a csoportnak kevés tagja van, csupán annyit, hogy a tagok nagy területen szóródnak szét a hálózatban.

5.1 Sűrű üzemmódú multicast útválasztó protokollok

Ezek a protokollok a nagy sávszélességgel, és a sűrűn elhelyezkedő csoporttagok esetén használatosak. Ebben az esetben feltételezhető, hogy majdnem minden gazdagép a hálózaton a csoporthoz tartozik.

Sűrű üzemmódú útválasztó protokollok a következők:

- DVMRP (Distance Vector Multicast Routing Protocol)
- MOSPF (Multicast Extensions to Open Shortest Path First)
- PIM-DM (Protocol Independent Multicast – Dense Mode)

5.1.1 Distance Vector Multicast Routing Protocol (DVMRP)

A DVMRP egy belső átjáró protokoll, mely, mint a neve is mutatja, távolság-vektor alapon továbbítja a datagramokat az egy autonóm rendszerhez tartozó hálózatban. Ez az első multicast útválasztással foglalkozó protokoll. A DVMRP egy forrás alapú kézbesítési fát hoz létre a Reverse Path Multicasting (RPM) algoritmus segítségével, és ez alapján hozza meg útválasztó döntéseit.

A protokoll eredetileg az RFC 1075-ben definiált, mára több változata is létezik. Az eredeti specifikációja a Routing Information Protocol (RIP) protokolltól származik, és kezdetekben még a TRPB algoritmust használta a multicast kézbesítési fa konstruálására. Az alapvető különbség a két protokoll között csupán annyi, hogy míg a RIP a következő ugrást határozza meg a célállomás felé, addig a DVMRP éppen az előző ugrást a forrás felé.

A DVMRP az IGMP protokollt alkalmazza az útválasztási információk cseréjéhez. A datagramok két részből tevődnek össze, egy rövid, fix hosszúságú IGMP fejlécszövegből, és egy változó hosszúságú adatrészből. Maga az üzenet nem lehet több 512 bajtnál, ami az IP fejlécszöveget is tartalmazza.

5.1.1.1 Fizikai és alagút interfészek

Egy DVMRP protokollal felkonfigurált útválasztónak kétféle interfészei lehetnek: fizikai, amely közvetlenül összekapcsolt multicast adatátvitelre képes alhálózatokat kapcsol össze, vagy úgynevezett alagút, mellyel más multicast-szigetek érhetőek el unicast módon (lásd későbbiekben Mbone). Minden interfészt konfigurálni kell egy metrikával és az interfészre vonatkozó TTL értékkel. Az alagút interfészeket további paraméterként a távoli interfész IP címével is konfigurálni kell. A TTL értékkel elérhető, hogy csak azok a csomagok továbbítódjanak az adott porton, melyeknek az IP fejlécszövegben lévő TTL értékei meghaladják az előre beállított értéket.

5.1.1.2 A protokoll működése

A DVMRP az RPM algoritmust implementálja. Minden egyes első érkező (forrás, csoport) párt az összes lehetséges interfészen kiküldi az útválasztó, feltéve, hogy a TTL értékek nagyobbak, mint az előre beállított érték. Rövid időn belül a levél szinten lévő routerek is megkapják a multicast csomagokat, majd vagy kézbesítik őket, vagy tisztító üzenetet küldenek vissza a forrás felé lévő útválasztónak, ha nincs az adott csoportnak tagja az alhálózatban. Ezek a tisztítási állapotot jelző információk periodikusan lejárnak, azaz egy idő múlva minden egyes beérkező (forrás, csoport) párost újra az összes lehetséges „downstream” interfészen továbbküldi az útválasztó. Ezzel biztosítható, hogy mindig a legrövidebb kézbesítési fa alakuljon ki a forrás-cél között. További oka a periodikus megújításnak, hogy az RPM implementációja nem teszi lehetővé a megbízható adatátvitelt a tisztítási információk megosztása során. A protokoll továbbá implementál egy kioltó üzenetet is, mellyel ignorálhatja az előzőleg elküldött tisztító üzenetét. Erre azért van szükség, mert ha egy levél szinten lévő útválasztó épp a tisztító üzenet elküldése után értesül az IGMP protokoll által egy új tagról, akkor üzenetet küldhet az előző ugrásra lévő útválasztónak, mely visszaállítja a megelőző tisztítási állapotot. Így nem szükséges megvárni, amíg lejár a periodikus idő, egyből megindulhat az adatforgalom az új csoporttag felé is.

Amikor egy vevő elhagy egy csoportot, akkor bonyolultabb a helyzet, mivel az utolsó szakaszbeli útválasztónak meg kell határoznia, hogy van-e még a kérdéses csoportnak további tagja az alhálózatban. Amikor egy gazdagép elhagyja a csoportot, és ezt jelzi IGMP üzenet segítségével az útválasztó felé, az útválasztó felgyorsítja a szokásos tagság lekérdező algoritmusát, mellyel gyorsan meghatározhatja, hogy maradt-e még az adott csoportnak tagja az alhálózatban. Ha felismeri, hogy nem maradtak tagok, akkor egy tisztító üzenetet küld a szórási fán „felfelé” a további adattovábbítás elnyomásának érdekében.

5.1.1.3 A DVMRP routing táblája

Minden egyes DVMRP útválasztó periodikusan routing-tábla frissítéseket cserél a szomszédos útválasztókkal, melyek teljesen függetlenek a hagyományos, unicast útválasztói

protokollok frissítéseitől, tehát egy időben egy router akár kétféle üzemmódban is szolgálhat. Egyrészt továbbítja a hagyományos unicast csomagokat, míg közben multicast adattovábbítást is végezhet. Természetesen lehetőség van rá, hogy csupán multicast csomagok továbbítására konfiguráljuk az eszközöket.

Egy lehetséges DVMRP routing tábla:

Source Prefix	Subnet Mask	From-Gateway	Metric	Status	TTL
128.1.0.0	255.255.0.0	128.7.5.2	3	Up	200
128.2.0.0	255.255.0.0	128.7.5.2	5	Up	150
128.3.0.0	255.255.0.0	128.6.3.1	2	Up	150
128.3.0.0	255.255.0.0	128.6.3.1	4	Up	200

Eltérően a hagyományos unicast protokollok tábláitól, a DVMRP routing táblája a forrás hálózatot, és a forrás átjáró címét tartalmazza, a célhálózat és a következő ugrás átjáró címei helyett.

A táblázat reprezentálja a forrás alapú legrövidebb út feszítő fáját minden egyes forrás hálózathoz, viszont nem tartalmazza a csoporttagsági információkat, illetve a fogadott tisztító üzeneteket.

A routing tábla oszlopai a következőket jelölik:

Source prefix: az az alhálózat, melyben az aktuális multicast datagram forrása található

Subnet mask: a forrás hálózatához tartozó alhálózati maszk. A DVMRP protokoll támogatja az osztály nélküli alhálózatokat.

From-Gateway: az előző ugrásban lévő útválasztó címe, mely visszavezet a forrás hálózatához

TTL: Time-to-Live mező, mely mutatja, hogy az aktuális bejegyzés hány másodpercig marad meg a táblában. Ennek a TTL értéknek semmi köze az IP fejlécben található TTL értékhez.

5.1.1.4 A DVMRP továbbítási táblája

Mivel a routing tábla nem tartalmaz semmilyen információt a csoporttagságról, ezért a protokoll egy másik, úgynevezett továbbítási táblát is létrehoz, amely a multicast routing tábla, az ismert csoportok, és a fogadott tisztító üzenetek információinak kombinációból jön létre. A továbbítási tábla reprezentálja a tényleges RPM által meghatározott aktuális funkcióját az útválasztónak.

Egy lehetséges DVMRP továbbítási tábla:

Source prefix	Multicast Group	TTL	InIntf	OutIntf(s)
128.1.0.0	224.1.1.1	200	1 Pr	2p3p
	224.2.2.2	100	1	2p3
	224.3.3.3	250	1	2
128.2.0.0	224.1.1.1	150	2	2p3

A továbbítási tábla oszlopai a következőket jelölik:

Source prefix: az az alhálózat, amely a specifikált csoportoknak multicast datagramokat küld

Muticast Group: D osztályú IP cím, ezekre a csoportcímekre címeztek datagramokat az adott alhálózatból

TTL: Time-to-Live mező, mely mutatja, hogy az aktuális bejegyzés hány másodpercig marad meg a táblában.

- InIntf: A (forrás, csoport) párhoz tartozó szülő interfész. A Pr jelölés azt jelzi, hogy ezen az interfészen már küldve lett tisztító üzenet az „upstream” router felé. (Ennek címe a routing táblában található.)
- OutIntf(s): A gyerek interfészek, amelyeken keresztül az adott (forrás, csoport) párt továbbítani kell. A p jelölés jelzi, hogy melyik porton érkezett egy, vagy esetleg az összes downstream routertől tisztító üzenet.

5.1.2 Multicast Extensions to Open Shortest Path First (MOSPF)

Az MOSPF protokoll a kapcsolatállapot alapú OSPF unicast útválasztó protokoll kiterjesztése multicast szintűre. A protokoll az RFC 1584-ben található meg. Hasonlóan a DVMRP-hez az MOSPF is belső átjáró protokoll, azaz az egy autonóm rendszerhez tartozó hálózaton belül alkalmazható hatékonyan.

„A kapcsolatállapot alapú irányító algoritmusok a topológiáról szerzett információkból összetett adatbázist készítenek. Míg a távolságvektor alapú algoritmusok nem rendelkeznek pontos információkkal a távoli hálózatokról, illetve semmilyen információjuk nincs a távoli forgalomirányítókról sem, a kapcsolatállapot alapú algoritmusoknak teljes képük van a távoli forgalomirányítókról és azok összekapcsolódásának módjáról. A kapcsolatállapot alapú irányító protokollok a hálózat egészéből vagy egy megadott részéből az összes többi forgalomirányítótól összegyűjtik az irányítási információkat. Miután az összes információt begyűjtötték, az egyes forgalomirányítók – egymástól függetlenül – a hálózat minden pontja felé meghatározzák a legjobb útvonalat. Mivel minden forgalomirányító a saját szemszögéből szemléli a hálózatot, kevésbé valószínű, hogy a szomszédjaitól származó hibás adatokat továbbadja. A kapcsolatállapot alapú irányító protokollok a hálózat egészéből vagy egy megadott részéből az összes többi forgalomirányítótól összegyűjtik az irányítási információkat. Miután az összes információt begyűjtötték, az egyes forgalomirányítók – egymástól függetlenül – a hálózat minden pontja felé meghatározzák a legjobb útvonalat.

Mivel minden forgalomirányító a saját szemszögéből szemléli a hálózatot, kevésbé valószínű, hogy a szomszédjaitól származó hibás adatokat továbbadja.” [20]

Az OSPF protokoll kiterjesztése multicast szintűre hasonló módon nyilvántart egy topológiai adatbázist a teljes hálózatról, melyet teljesen hasonló unicast módon hajtja végre, mint a hagyományos elődje. Az MOSPF nem támogatja az alagutakat, mint a DVMRP, így az Mbone-ban sem alkalmazzák.

Lehetőség van rá, hogy egy hálózatban keveredjenek az OSPF-et és az MOSPF-et támogató útválasztók.

5.1.2.1 A protokoll működése

A protokoll a legrövidebb útvonalat határozza meg hasonló módon, mint az OSPF, viszont a forrás felé. Az MOSPF adatbázisa ugyanazokat az információkat tartalmazza, mint az elődje, kiegészítve a csoportinformációit tartalmazó LSA-kkel.³

Amikor egy kezdeti, első (forrás, csoport) pár multicast datagram érkezik egy útválasztóhoz, akkor a forrás hálózata már biztosan szerepel az útválasztó kapcsolatállapot adatbázisában. Ezután az alap OSPF LSA, illetve a csoporttagság információit tartalmazó LSA segítségével a Dijkstra-algoritmus könnyedén meghatározza a forrás alapú legrövidebb elérési utat.

Miután a fa felépült, a csoporttagsági LSA segítségével megoldható a tisztító üzenetek küldése a többi útválasztónak. Az algoritmus végeredménye egy tisztított kézbesítési fa, melynek a gyökere a datagram forrása.

Hogy a forrástól minden csoporttag számára eljussanak a multicast datagramok, a kézbesítési fában található összes útválasztónak meg kell határoznia a saját helyét ebben a fában, azaz mindegyiknek le kell futtatnia a Dijkstra-algoritmust.

Az algoritmus minden egyes (forrás, csoport) párhoz külön kézbesítési fát hoz létre, melynek gyökere a forrás, és a levélszinten a csoport összes tagja megtalálható. Ha egy olyan (forrás, csoport) pár érkezik az útválasztóhoz, mely még korábban nem, akkor a router lefuttatja a bejövő interfészre a Dijkstra-algoritmust, melynek végeredménye a pároshoz tartozó

³ LSA: kapcsolatállapot-hirdetés

forrásalapú legrövidebb útvonal, illetve a kimenő interfész(ek) meghatározása, amelyeken a továbbítani kell majd a forráshoz tartozó datagramokat.

Néha előfordulhat, hogy bizonyos területek csoporttagsági információi ismeretlenek. Ekkor a MOSPF ezeknek a területeknek a határ-útválasztóit is hozzáadja a kézbesítési fához, mint esetleges kézbesítési cél.

A protokoll legnagyobb előnye a DVMRP-vel szemben, hogy itt, ha egy új csoporttag kezd el datagramokat küldeni, akkor nem szükséges első lépésként elárasztani az alhálózatokat a levél szintig.

Egyetlen hátránya az MOSPF-nek az OSPF-hez képest, hogy nem lehetséges a terheléselosztás, mivel ha két ugyanolyan költségű útvonalat határoz meg a Dijkstra-algoritmus, akkor is csak az egyik lesz kiválasztva aktív útvonalnak.

5.1.2.2 Továbbítási gyorsító tár

Minden egyes MOSPF útválasztó a döntései meghozatalához egy gyorsító tárat hoz létre és tart karban. A DVMRP-vel ellentétben nem RPB algoritmus dönt a továbbításról, hanem a legrövidebb elérési út minden egyes (forrás, csoport) pároshoz, és az útválasztó helyi csoporttagsági információi. Miután a router megtalálja a helyét a kézbesítési fában, a gyorsító tár tartalmazza a (forrás, csoport) páros upstream interfészét, és a szükséges downstream interfészeket, melyeken továbbítani kell a datagramokat.

Egy lehetséges MOSPF továbbítási gyorsító tár:

Destination Group	Source	Upstream	Downstream	TTL
224.1.1.1	128.1.0.2	11	12,13	5
224.1.1.1	128.4.1.2	11	12,13	2
224.1.1.1	128.5.2.2	11	12,13	3
224.2.2.2	128.2.0.3	12	11	7

Destination Group:	annak a csoportnak a címe, amelynek továbbítani kell a csomagokat
Source:	a datagram forrásának címe. Minden egyes (forrás, csoport) párhoz külön sor jelenik meg a gyorsító táblában.
Upstream:	az az interfész, melyen keresztül beérkezett a multicast datagram
Downstream:	azok az interfészek, amelyeken keresztül továbbítani kell a csomagokat
TTL:	az ugrások minimális száma, amelyen keresztül a datagram a csoport bármely tagjához elérhet a hálózaton. Az MOSPF útválasztó letilthatja azokat a datagramokat, amelyek TTL értékei annyira kevesek, hogy még a legközelebbi csoporttagot sem érhetik el.

A DVMRP-vel ellentétben a gyorsító táblák sorai nem évülnek el, és nem szükséges periodikusan megújítani őket, csupán akkor, ha topológiai változás történik a hálózatban.

5.1.2.3 Területek közötti multicast továbbítás

Az MOSPF lehetőséget ad rá, hogy hasonló módon, mint az OSPF, más területeken lévő csoporttagoknak is kézbesíteni tudjunk multicast datagramokat.

„A nagyméretű, OSPF alapú hálózatok tervezésekor hierarchikus elvet kell követni. Több terület csatlakozik egy elosztó területhez (0 sorszámmal), amit gerinchálózatnak is nevezünk. Ezt a szemléletet követve az útvonalfrissítések terjesztésének széles körű ellenőrzése válik lehetővé. A területek létrehozásával csökkenthető az irányítási többletterhelés, felgyorsítható a hálózat konvergenciája, a hibák hatása egy-egy kisebb területre korlátozható, illetve növelhető a teljesítmény.” [20]

Minden egyes területhatár útválasztónak megváltozik a feladata, területek közötti multicast továbbító szerepkört kell betölteniük, melyben alapvető feladatuk, hogy a területük összegzett csoporttagság információit továbbítsák a gerinchálózat felé. Ez a továbbítás aszimmetrikus, azaz a gerinchálózat felé érkehetnek tagsági üzenetek, de onnan visszafelé már nem.

A területek közötti továbbítás feltétele, hogy a határ útválasztók úgynevezett „wild-card” multicast-vevő szerepkört töltsenek be a kézbesítési fában, azaz az összes multicast forgalom az adott területből eljusson ehhez az útválasztóig, még akkor is, ha nincs a legrövidebb kézbesítési úton, vagy egyáltalán nem is lehet onnan tovább kézbesíteni majd. Ezzel garantálható, hogy az összes területen belüli multicast adatforgalom eljusson a területhatárig, és ha szükséges, akkor bekerül a hálózat gerincébe, majd onnan további területekre juthat át.

5.1.3 Protocol Independent Multicast – Dense Mode (PIM-DM)

A PIM útválasztó protokollt az IETF egyik részlege, az Inter-Domain Multicast Routing (IDMR) munkacsoport alkotta meg. Alapvető céljuk, hogy kidolgozzanak egy olyan szabványos, jól skálázható független protokollt, mely később az egész Interneten szabvánnyá léphet elő. Jelenleg kétféle PIM protokoll létezik, a sűrű, illetve a ritka módú. Bár nevük, és alapvető vezérlő utasításaik formája megegyezik, gyakorlatilag két különálló, független protokollról beszélhetünk. [6]

A nevét a protokoll arról kapta, hogy elméletileg nem függ semmilyen unicast jellegű útválasztó mechanizmustól, ennek ellenére az összes implementációjában szükséges valamilyen unicast protokoll működése a háttérben az információk cseréjéhez, illetve a topológia változások nyomon követéséhez.

A PIM-DM hasonlóan a DVMRP-hez, az RPM (Reverse Path Multicasting) algoritmust valósítja meg, néhány eltéréssel. A forráshoz tartozó út meghatározásához egy már meglévő unicast útválasztási táblájára hagyatkozik, ellentétben a DVMRP-vel, aminek egy beépített, RIP-szerű mechanizmusa van, ami magának készíti el az unicast jellegű táblázatot, amit később felhasznál. További ellentét, hogy míg a DVMRP minden egyes (forrás, csoport) párhoz meghatározza a gyerek portokat, a PIM-DM egyszerűen az összes nem bejövő portján továbbítja a multicast datagramokat egészen addig, míg tisztító üzenet nem érkezik rá. Ily módon folyamatosan az igényekhez igazodik hozzá a multicast továbbítási fa, lényeges műveletek nélkül. Ha tisztító üzenet érkezik vissza valamely portra, akkor az útválasztó azt az útvonalat levágja a kézbesítési fáról.

Hasonlóképp, mint a DVMRP-nél, a PIM-DM is tartalmaz egy oltvány üzenetet, melynek használatával visszaállítható egy korábbi állapot a kézbesítési fában, ha a tisztító üzenet elküldése után új csoporttagok jelentkeznek a levágott farészbe.

5.2 Ritka üzemmódú multicast útválasztó protokollok

A multicast útválasztó protokollok másik nagy csoportja a ritka üzemmódú protokollok. Ezek a megoldások a sűrű üzemmódúakkal szemben nem igényelnek nagy sávszélességet az optimális működéshez, illetve feltételezik, hogy a csoport tagjai nagy területen helyezkednek el a hálózatban, így nem feltétlenül alkalmazzák az elárasztás műveletét, mivel a nagy távolságok miatt ez hatalmas költségekkel járna, helyette új, sávszélesség-barát módokat fejlesztettek ki. Ezek a protokollok a legújabbak, fejlesztésük napjainkban is folyik, mivel ezek a leggyakorlatiasabbak a mindennapi, Interneten át zajló telekommunikációban, melyek kerülnek a folyamatos üzenetszórás.

Ritka üzemmódú protokollok:

- Protocol Independent Multicast – Sparse Mode (PIM-SM)
- Core Based Trees (CBT)

A PIM-SM egy független, az IETF által készített protokoll, mely széles körben alkalmazott napjainkban, a CBT pedig egy olyan eljárás, ami csak egyetlen fát készít el a csoport összes tagja számára.

5.2.1 Protocol Independent Multicast – Sparse Mode (PIM-SM)

A PIM egy független protokoll, melynek létezik egy sűrű, és egy ritka módú változata is. Bár hasonló felépítésűek, a gyakorlatban mégis két, teljesen független protokollról beszélhetünk. Olyannyira különbözőek, hogy bár teljesen megegyeznek a protokollvezérlő üzenetei, mégsem lehetséges, hogy egy régióban mindkét PIM fusson egy időben.

A PIM-SM alapvetően abban különbözik a sűrű módú társaitól, hogy a közvetlen szomszéd útválasztóknak egy csatlakozó üzenetet kell küldeniük, mielőtt megindulhatna az adatforgalom abba az irányba. Ha nem csatlakozik az előre kalkulált kézbesítési fához, akkor nem fogadhat multicast adatforgalmat sem az adott útválasztó.

Míg a sűrű módú protokollok alapelve, hogy a bejövő multicast datagramokat küldjük tovább a lehetséges összes irányba, amíg csak nem érkezik tisztító üzenet, addig a PIM-SM, és az összes ritka módú protokoll alapfilozófiája, hogy egészen addig blokkoljuk a forgalmat, amíg arra konkrét igény nem érkezik. [7]

Minden csoport rendelkezik egy találkozási ponttal (Rendezvous Point, RP), ennek küldenek csatlakozó üzenetet a csatlakozni vágyók, melyeket a közbeeső routerek PIM-Join segítségével feldolgoznak. A források mindegyike először az RP számára küldi el a multicast csomagjait, majd azok a helyek, amelyek szeretnének csatlakozni a csoporthoz, kérik egy alagút felállítását az RP és önmaga között. Ezáltal a PIM-SM a forgalmat unicast módon viszi át, nem multicast módon. Garantált módon csak egy RP lehet egyszerre egy PIM-SM tartományban.

5.2.1.1 Közvetlenül kapcsolódott állomás csatlakozása egy csoportba

Ha egy állomás csatlakozni szeretne egy csoporthoz, akkor IGMP üzenet segítségével jelzi ezt az adott alhálózat kiválasztott útválasztója (DR) felé. Ha egy alhálózatnak több útválasztója is van, akkor a legnagyobb IP című lesz a PIM szempontjából a kiválasztott router, mely küldhet csatlakozó és tisztító üzeneteket később. Miután a DR útválasztó IGMP Report üzenet segítségével értesül az új csoportról, egy speciális, többlépcsős művelet segítségével értesíti a

csoport RP útválasztóját erről, ami után megindulhat a multicast adattovábbítás az újonnan csatlakozott csoporttagok felé is, és csak abba az irányba. Először a DR útválasztó létrehoz egy új (*, csoport) továbbítási bejegyzést a memóriájába, majd unicast módon elküld egy PIM-Join üzenetet az RP útválasztó felé, az újonnan létrehozott bejegyzésről. A közbeeső útválasztók továbbítják a kérést az RP felé, és ha még nincs ilyen bejegyzésük a továbbítási táblájukban, akkor bejegyzik a megkapott (*, csoport) párost, így mire megkapja a csatlakozó üzenetet az RP is, már ki is alakult az egyéni továbbítási útvonal az új csoporttagok felé.

5.2.1.2 Egy közvetlenül kapcsolódott forrás datagram küldése csoportnak

Ha egy forrás először küld multicast csomagokat egy csoportnak, akkor a forráshoz tartozó DR útválasztó továbbítja ezeket a datagramokat a csoporthoz tartozó RP útválasztó felé a kézbesítési fa mentén. A DR útválasztó a kezdeti datagramokat egy PIM-SM-Register csomagba ágyazza be, és unicast módon továbbítja, ami értesíti a RP-t az új forrásról.

Ezek után az RP dönt arról, hogy visszaküld-e egy PIM-Join üzenetet a forráshoz tartozó DR felé, és így csatlakozik a DR legrövidebb kézbesítési fához, ami után már nem szükséges unicast módon beágyazva küldeni a multicast datagramokat.

Másik lehetőség, hogy saját maga csatlakozik a forrás legrövidebb kézbesítési fájához, melynek gyökere a forrás DR útválasztója. Ebben az esetben nem jönnek létre a közbeeső útválasztókon az adott (forrás, csoport) bejegyzések, illetve a DR útválasztó csak unicast módon, beágyazva tudja elküldeni a multicast datagramokat a RP felé, hasonlóan PIM-SM-Register segítségével. Ekkor a DR útválasztó akkor szakíthatja meg a multicast adatok küldését (unicast módon), ha a RP útválasztó egy PIM-SM-Register-Stop üzenetet küld ki a DR felé. Ez akkor történhet meg, ha már nincs egyetlen aktív csoporttag sem, akinek továbbítani kellene a multicast datagramokat.

Mint látható, a PIM-SM protokoll egyszerre használhatja a forrás alapú, és a megosztott fa algoritmusokat. Lényegében minden csoportnak lehetnek útválasztói a saját forrás alapú fájában, és lehetnek a megosztott fákban is egyidejűleg. Alapesetben a PIM-SM a megosztott fa algoritmust használja, melynek a gyökere a RP útválasztó. Függetlenül attól, hogy melyik fát alkalmazza, mindig csak a kellő irányokban jelenik meg a kívánt adatforgalom.

5.2.3 Core Based Trees (CBT)

A CBT, más néven mag alapú fa protokoll a PIM-SM-hez hasonlóan ritka üzemmódú, és a megosztott fa algoritmuson alapszik. Tervezésekor a legfőbb szempont volt, hogy a multicast programok szolgáltatásait ne csak az Interneten keresztül, hanem céges intranet hálózatokon keresztül is elérhetővé tegye. A protokoll független, azaz felhasználja bármelyik unicast útválasztó protokoll tábláit, hogy a saját kézbesítési fáját meghatározza, így nincs szüksége további speciális unicast algoritmusokra a működéséhez.

A protokoll alapelve hasonlóan a PIM-SM-hez, „önbetöltő” mechanizmusból tevődik ki, azaz jelezni kell az alhálózatoknak az igényt, ha multicast kérést észlelnek, és csak ezután indulhat meg az adattovábbítás. Ez a processzus lehet dinamikus, vagy manuális.

Minden egyes csoporthoz tartozik egy „mag” útválasztó, mely hasonló feladatot lát el, mint a PIM-SM esetében a RP router, egy mag viszont több csoportot is kiszolgálhat egyidejűleg.

5.2.3.1 A CBT működése

Ha egy állomás csatlakozni szeretne egy multicast csoporthoz, IGMP Report üzenet segítségével jelezheti ezt a helyi CBT útválasztó felé, mely informálja a routert, hogy új csoporttag van jelen az alhálózatban. Miután megérkezik az IGMP üzenet, a helyi CBT útválasztó egy Join-Request üzenetet küld el a csoport mag-útválasztója felé. Ha út közben olyan útválasztóhoz érkezik a kérés, mely már korábban tagja a csoport megosztott fájának, akkor ez az útválasztó visszaküld egy Join-ACK üzenetet a helyi CBT útválasztónak, mely eredetileg küldte ki a kérést. Ha út közben nincs olyan router, mely már tagja lenne a fának, akkor a mag-útválasztó küld vissza egy ACK üzenetet. Miközben visszafelé tart az ACK a helyi útválasztó felé, a közbeeső routerek egy úgynevezett aktív állapot-bejegyzést hoznak létre az adott csoporthoz, mely tartalmazza a down- és az upstream linkeket is. A linkek státuszát a CBT Echo protokollal tartja fent. A gyerek útválasztó a szülő felé periodikusan echo kéréseket küld ki unicast módon, melyre válaszolnia kell a szülő útválasztónak. Ha bármely okból megszakadna a kapcsolat a szülő és a gyerek útválasztó között, akkor a gyerek

router az ő saját gyerek linkjein keresztül egy úgynevezett Flush-Tree üzenetet küld ki, mely az adott irányban levágja a csoport kézbesítési fájának ágait. Ezek után a levélszinten lévő útválasztók a felelősek aktív tag esetén az újabb kézbesítési fa meghatározásához.

Miután a Join-ACK üzenet visszaérkezett az eredetileg küldő útválasztóhoz, megindulhat a csoport által létrehozott megosztott kézbesítési fán a multicast datagramok kézbesítése.

Természetesen lehetőség van rá, mint minden más protokoll esetében is, hogy egy olyan állomás küldjön egy csoportnak datagramokat, melynek épp nem is tagja. Ehhez szükséges, hogy a helyi útválasztó CBT kompatibilis legyen. Ha ilyen kérés érkezne hozzá, akkor unicast csomagokba ágyazva továbbküldi a csoporthoz tartozó mag útválasztónak. Ehhez szükséges, hogy minden CBT régióban az összes útválasztóban megtalálható legyen az összes (csoport, mag) összerendelés.

5.2.3.2 A CBT jövője

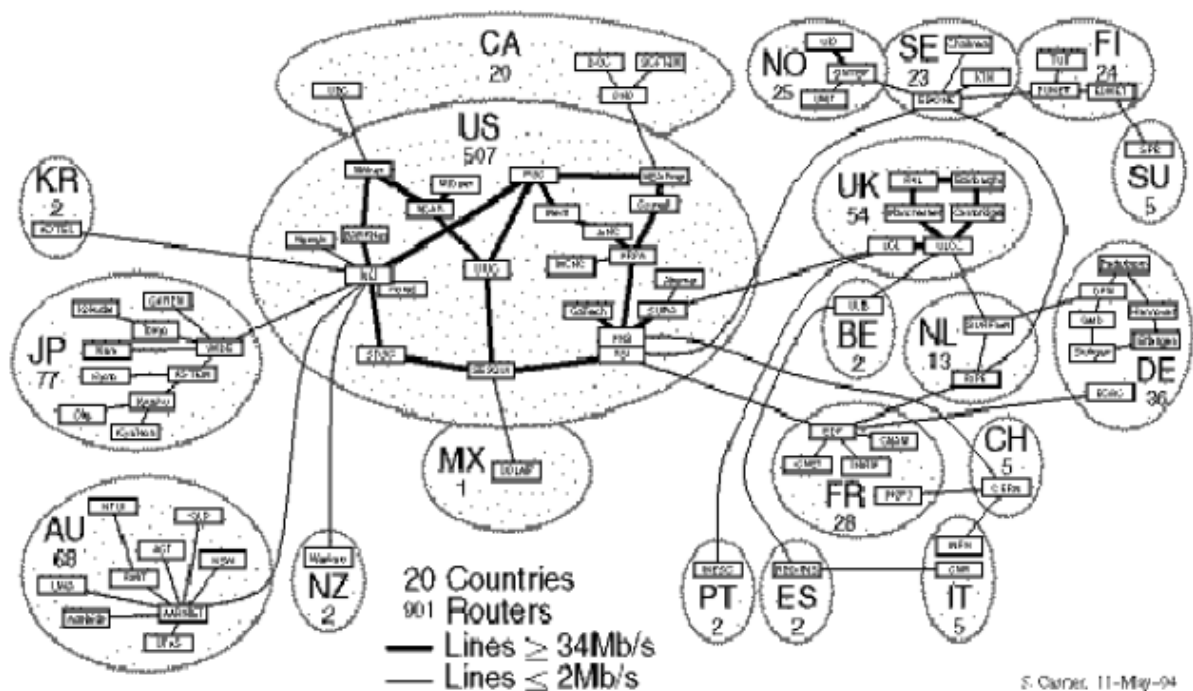
Bár manapság nem a CBT a legelterjedtebben használt megoldás multicast útválasztásra, a jövőben mégis nagy hangsúlyt kaphat ez a protokoll az autonóm területeken belüli forgalomirányításban. Jelenleg is fejlesztik a protokollt, meg szeretnék oldani, hogy DVMRP gerinchálózattal is össze lehessen kapcsolni CBT területeket. Ehhez olyan metódusokkal kell felszerelni a határ útválasztókat, hogy képesek legyenek mindkét protokollt egy időben összehangolva működtetni.

6. MULTICAST A GYAKORLATBAN – MBONE

Számtalan megoldás létezik már, mellyel több résztvevős, csoportos üzenetküldést valósíthatunk meg, a gyakorlatban azonban egyelőre sok probléma merülhet fel, ha az Interneten keresztül történik a csoportos kommunikáció. A multicast technológia hátránya, hogy ha csak egyetlen útválasztó nem támogatja a multicastos eljárásokat, akkor a két hálózat között már nem működik a szolgáltatás.

Ideiglenes megoldásként 1992-ben létrehozták az Internet Multicast Backbone (Mbone) virtuális gerinchálózatot, mely összekapcsolja azokat a részhálózatokat, amelyek támogatják a multicast adatátvitelt. A részhálózatokat szigeteknek nevezzük, melyek belsejében elérhető a szolgáltatás. Ha szigeten kívülre is címezzük a datagramokat, akkor a szigetek között unicast módon, beágyazva továbbítódnak a csomagok, kiküszöbölve a multicast hiányát az útválasztókban. Kezdetben négy ország 40 alhálózatával indult az Mbone, napjainkra több ezer hálózat a tagja. Gyakorlati haszna addig várható, amíg az Internet összes lényeges útválasztóját le nem cserélik úgynevezett m-útválasztókra.

Az Mbone térképe 1994 májusában:



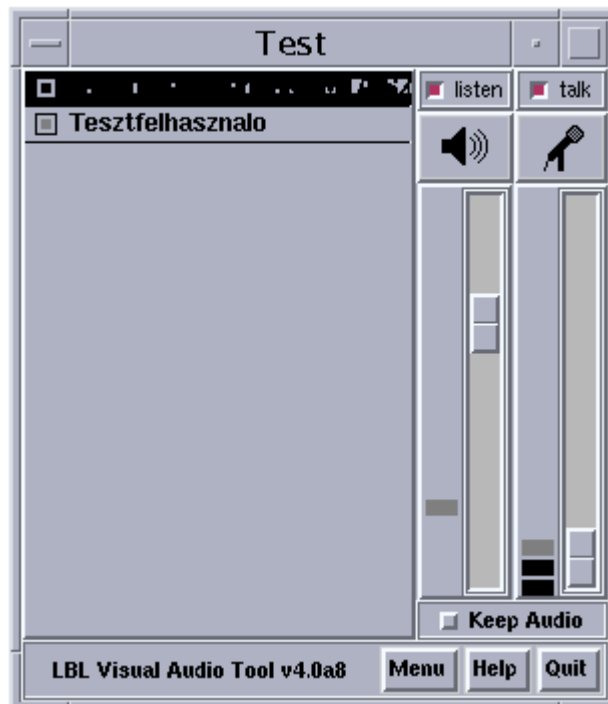
Alapvető műszaki igényként megadták a tervezők, hogy milyen követelményeknek kell megfelelnie egy vonalnak, hogy az Mbone hálózat része lehessen. Eszerint a vonali kapacitásnak meg kell haladnia a 128 kbps-t. Egy egyszerű audió multicasthoz legalább 16 kbps szabad kapacitásra van szükség, míg egy videó multicasthoz hozzávetőlegesen 150 kbps-hez. Ezek az értékek jellemzően napjainkban már sokszorosai az eredeti specifikációnak, mivel lényegesen javultak mind a hang, de inkább a képminőségek, amelyek a sáv szélesség igényekben is megmutatkoznak.

Az Mbone hálózatban alapvetően DVMRP útválasztó protokollt alkalmaznak, mivel képes alagutak kezelésére. Ha egy másik szigetre kell üzenetet továbbítani, akkor az alagút egyik végén lévő útválasztó a célcímként megadott multicast csoportcímet lecseréli az alagút másik oldalán található útválasztó egyedi unicast címére, és továbbítja a beágyazott csomagot. A túloldalon lévő útválasztó miután megkapta a beágyazott datagramokat, egyszerűen visszacseréli a célcímet az eredeti multicastos D osztályú IP címre, és továbbítja a szigeten belüli útválasztóknak a csomagokat.

Napjainkban az Mbone-t használhatjuk a legkülönbözőbb élő műsorok közvetítésére, audió és videó konferenciákra, vagy hálózati játékokra.

6.1 Audió konferencia eszköz (Vat)

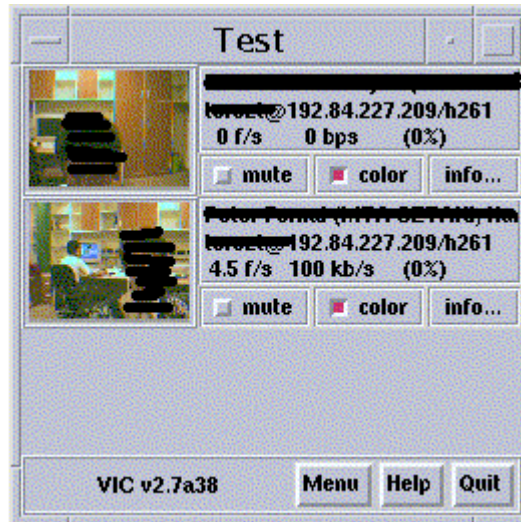
A Lawrence Berkeley Laboratories fejlesztette ki a Visual Audio Tool nevű programot. A vat lehetővé teszi, hogy a felhasználók szóban kommunikáljanak az Mbone egy tartományán. A vat egy munkaállomás beépített audió kapacitásait használja a felhasználói munkaállomásból jövő hang kódolására, és a vett anyag lejátszására is.



„A jobb oldali tolokákkal az adás és a vétel hangerejét szabályozhatjuk, amelyet a kivezérlés jelzők folyamatosan mutatnak. Megválaszthatjuk még azt is például, hogy a vett hang hangszóróból vagy a fülhallgatóból legyen hallható, illetve hogy külső vagy beépített mikrofont használunk. A VAT-ot CB-rádióhoz hasonló módon is tudjuk működtetni: ha az adás alapállapotban ki van kapcsolva, akkor a jobb egérgomb lenyomásával időlegesen leszünk csak hallhatóak. Hangátvitelre többféle formátumot használhatunk a PCM változataitól kezdve a GSM-ig. A bal oldali panelben vannak felsorolva a beszélgetés részvevői. Közülük bárkinek a hangja kikapcsolható, vagy éppen magánbeszélgetést lehet vele kezdeményezni egy külön csatornán, valamint a beszélgetőpartner hálózati elérhetőségét lehet tesztelni. Az eszköz egyéni és globális statisztikákat, grafikonokat is tud szolgáltatni a hálózati forgalomról.” [14]

6.2 Videó konferencia eszköz (Vic)

A Lawrence Berkeley Laboratories videó konferencia alkalmazása.

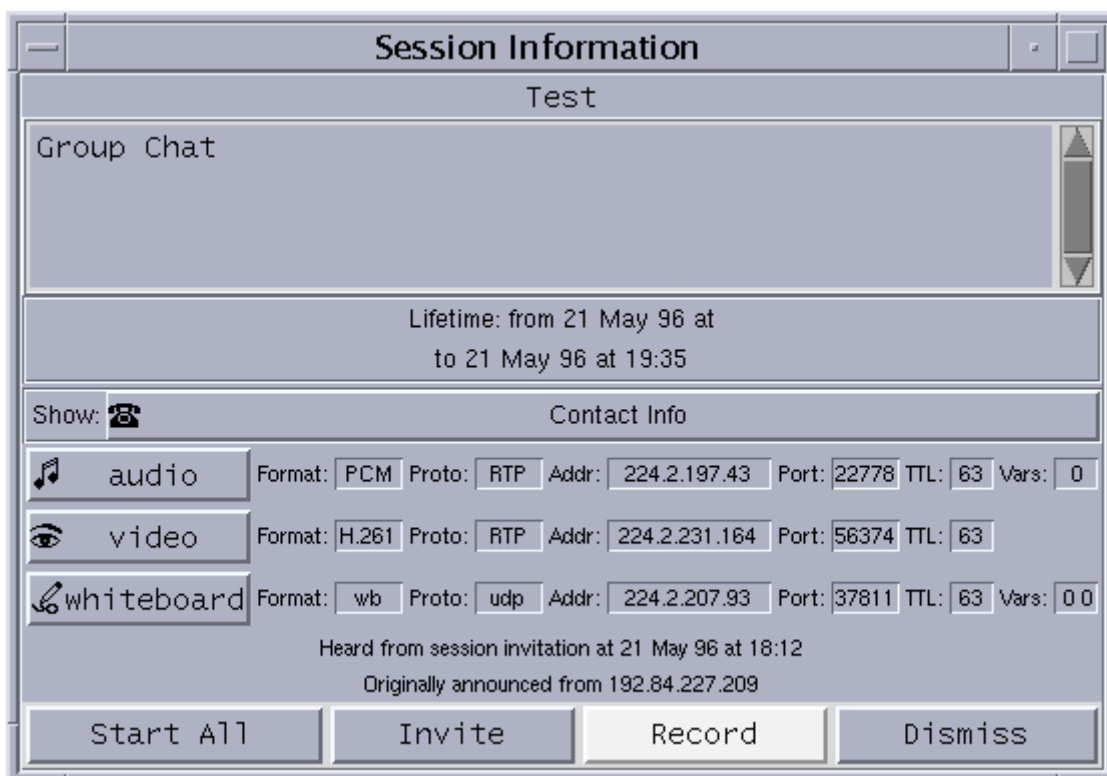


„A *vic* indulás után automatikusan megjeleníti a csatornán fogható összes mozgóképet kicsinyítve. Ugyanitt megtudhatjuk az adás illetve vétel címét, nevét, az éppen foglalt sávszélességet, a másodpercenkénti képváltások számát, valamint a vétel minőségére következtethetünk az elveszett adatcsomagok arányából. A kicsinyített videójeleket többféle méretre nagyíthatjuk ki. általában a H.261 CIF mérete (288x352 képpont) használatos. A QCIF ennek negyede (144x176), az SCIF pedig ennek négyszerese (576x704).” [14]

6.3 Konferenciakatalógus (Session Directory)

Új lehetőségként megjelenő módszer a konferenciakatalógus, amely az aktív konferenciák összefogására, és közlő konferenciák hirdetésére szolgál. Ilyen program az sdr.

„Az *sdr*-ben meghirdethetjük saját konferenciáinkat, ha kitöltjük az erre szolgáló űrlapot. A hirdetés addig zajlik, amíg nem töröljük ki a hirdetményt (ezt csak mi tehetjük meg), vagy nem lépünk ki az *sdr*-ből. További szolgáltatások: magántalálkozók támogatása (felhívhatunk egy személyt, aki ha éppen futtatja az *sdr*-t, fogadhatja a hívásunkat), és a konferenciák rögzítése (ez kissé helyigényes).” [14]



„Elindítása után kis késleltetéssel feltöltődik a program ablaka az aktuális konferenciák listájával. A teljes listára várjunk ilyenkor pár percet türelmesen, mivel a konferenciák hirdetése nem történik folyamatosan. A konferencia nevére kattintva megjelenik annak

részletes ismertetése, mely tartalmaz általában leírást, esetleg URL-t a rendezvény web lapjára, vagy e-mail címet. A legfontosabb azonban a háromféle konferenciaeszköz beállításainak leírása, és a kapcsolódó nyomógombok, melyek segítségével egyszerűen elindíthatjuk az eszközöket akár egyszerre, akár egyesével.” [14]

6.4 Osztott rajztábla (Whiteboard)

Az osztott rajztábla egy a konferenciateremben felállított rajztáblának felel meg, amire bárki rajzolhat, írhat, sőt akár előre elkészített rajzokat is megjeleníthet PostScript formátumból. Ilyen funkciókkal ellátott program a Lawrence Berkeley Laboratories által fejlesztett *wb*.



„Egy egyszerű rajzolóprogramban szokásos eszközkészletet találunk a *wb* nevű MBone alkalmazásban: különféle színű és vastagságú nyilak, vonalak, sokszögek és szövegek rajzolása, törlése, mozgatása. Mindenki csak a saját rajzrészleteit mozgathatja vagy törölheti, mások rajzainak csak a megjelenítését tilthatja meg. Így a kitiltott személyeknek semmilyen rajza nem jelenik meg a felhasználó számára. A rajzolás több oldalon is folyhat egyszerre, ilyenkor az eszköz automatikusan a legutolsó rajzot tartalmazó oldalra ugrik. Ha ez zavaró, akkor a felhasználó rögzítheti valamelyik oldalt a rajztábla alkalmazásban. Nyomon lehet követni a többi felhasználó tevékenységét az eszközhöz tartozó kontroll ablakban. Itt megjelennek, hogy kik voltak aktívak, kik a részvevői ennek a csoportnak, illetve itt adhatjuk meg saját nevünket, és a kapcsolat egyéb adatait.” [14]

7. ÖSSZEFOGLALÁS

Dolgozatomban a fellelhető külföldi, és némi magyar szakirodalmak felhasználásával sikerült ismertetnem a multicast technológiát, egészen az alapoktól megkezdve. Ismertettem a címleképzési módszereket, a csoportmenedzsment protokollok különböző verzióit, IPv4 és IPv6 tekintetében is. Bemutattam a különféle csoportküldési továbbítási algoritmusokat, majd ezek implementációit. Végezetül gyakorlati oldaláról mutattam betekintést a multicast világába, az Mbone hálózaton keresztül, illetve néhány egyszerűbb, kényelmi vagy szórakoztató program bemutatásával.

Munkám során nagyban támaszkodtam a protokollok hivatalos RFC dokumentumaira, melyek tanulmányozása után szerettem volna a lényegi információkat összeállítani, és itt bemutatni, hogy a későbbiekben a dolgozatomat olvasók egyszerűen átláthassák a protokollok működésének alapjait. Így tehát a multicast útválasztó protokollok a leírtakhoz képest jóval bonyolultabbak, egyes esetekben több szolgáltatást is nyújtanak, amelyek itt, ebben a dolgozatban nem kerültek megemlítésre.

Dolgozatom összefoglalásaként megemlíteném, hogy a munkám nem tért ki az OSI réteg harmadik, azaz a hálózati rétegbeli multicast megoldásoktól eltérő, más technikákra, amelyek a többi rétegbe beágyazódva látják el a feladatukat. Bár kétségtelen, hogy a hálózati rétegben mennek végbe a komplexebb feladatok a csoportküldési kézbesítések szempontjából, megemlítendő, hogy más rétegekben is léteznek elvétve multicasttal foglalkozó mechanizmusok.

A dolgozat lezárásaként úgy gondolom, sikerült egy aktuális hálózati probléma megoldásáról átfogó képet adnom, és talán ez a dolgozat adhat majd segítséget a későbbiekben a témával kapcsolatban foglalkozó lelkes érdeklődőknek.

8. IRODALOMJEGYZÉK

8.1 Szakirodalmak

- [1] Andrew S. Tanenbaum - Számítógép-hálózatok, Panem Kiadó, 2003.
- [2] McMahon, Richard A. – PC hálózatok a gyakorlatban, Panem Kiadó, 2004.
- [3] RFC 1112: S. Deering: Host Extensions for IP Multicasting
Stanford University, August 1989
<http://www.faqs.org/rfcs/rfc1112.html>
- [4] RFC 1075: D. Waitzman, C. Partridge, S. Deering: Distance Vector Multicast Routing Protocol
Stanford University, November 1988
<http://www.faqs.org/rfcs/rfc1075.html>
- [5] RFC 1584: J. Moy: Multicast Extensions to OSPF
Proteon, Inc., March 1994
<http://www.faqs.org/rfcs/rfc1584.html>
- [6] RFC 3973: A. Adams, J. Nicholas, W. Siadak: PIM-DM
NextHop Technologies, January 2005
<http://www.faqs.org/rfcs/rfc3973.html>
- [7] RFC 2117: D. Estrin, D. Farinacci, A. Helmy, S. Deering: PIM-SM
Cisco, USC, Xerox, June 1997
<http://www.faqs.org/rfcs/rfc2117.html>

- [8] RFC 4605: B. Fenner, H. He, H. Sandick: IGMP/ Multicast/MLD Proxying
AT&T, Nortel, August 2006
<http://www.faqs.org/rfcs/rfc4605.html>
- [9] RFC 2189: A. Ballardie: Core Based Trees Multicast Routing
Network Working Group, September 1997
<http://www.faqs.org/rfcs/rfc2189.html>
- [10] RFC 2460: S. Deering, R. Hinden: Internet Protocol, Version 6 (IPv6)
Cisco, Nokia, December 1998
<http://www.faqs.org/rfcs/rfc2460.html>
- [11] T. Maufer, C. Semeria: Introduction to IP Multicast Routing, July 1997
<http://tools.ietf.org/html/draft-ietf-mboned-intro-multicast-03>
- [12] Az IP multicast alapjai
http://nimrud.eet.bme.hu/hmk/ps/mc_ip.ps
- [13] A multicast útválasztó algoritmusok és protokollok
http://nimrud.eet.bme.hu/hmk/ps/mc_utval.ps
- [14] Kovács László, Micsik András: Mbone audió-videó konferenciarendszer pilot
MTA SZTAKI, Elosztott Rendszerek Osztály
www.sztaki.hu/~micsik/nws96-mbone/

[15] Internet Multicast Addresses

<http://www.iana.org/assignments/multicast-addresses>

[16] dr. Bakonyi Péter, dr. György András, Tóth Beatrix: Az Internet jövője

NHIT tanulmány, MTA SZTAKI, 2007

www.nhit-it3.hu/images/stories/tag_and_publish/Files/it3-4-2-6-1.ppt

[17] Visual Audio Tool, Lawrence Berkeley Laboratories

<http://www-nrg.ee.lbl.gov/vat>

[18] vic, Lawrence Berkeley Laboratories

<http://www-nrg.ee.lbl.gov/vic>

[19] wb, Lawrence Berkeley Laboratories

<http://www-nrg.ee.lbl.gov/wb/>

[20] Todd Lammle: CCNA Study Guide: Exam 640-802

Wiley Publishing Inc. 2007, ISBN: 978-0-470- 11008-9

[21] RFC 1305: David L. Mills: Network Time Protocol

University of Delaware, March 1992

<http://www.faqs.org/rfcs/rfc1305.html>

8.2 Egyéb felhasznált irodalmak

[22] IP Multicast

<http://www.szabilinux.hu/trendek/trendek74.html>

9. KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Almási Bélának, aki észrevételeivel, tanácsaival nagyban segítette munkámat, és e dolgozat létrejöttét.