

TARTU ÜLIKOOL
MATEMAATIKA-INFORMAATIKATEADUSKOND
Arvutiteaduse instituut
Informaatika eriala

Erkki Kukk

Multiedastus arvutivõrkudes

Magistritöö (60EAP)

Juhendaja: prof. E. Vainikko

Autor: “.....“ mai 2010

Juhendaja: “.....“ mai 2010

Lubada kaitsmisele

Õppetooli juhataja: “.....“ mai 2010

TARTU 2010

Sisukord

Sissejuhatus.....	3
1 Multiedastus	4
1.1 Multiedastuse IP aadressid.....	5
1.2 Multiedastuse MAC aadressid.....	7
2 Multiedastuse jaotuspuud	9
2.1 Lähtepuud.....	9
2.2 Jagatud puud.....	10
2.3 Kahesuunalised jagatud puud.....	11
2.4 Ühesuunalised jagatud puud	11
2.5 Lähtepuud vs jagatud puud.....	12
3 Multisaate edastamine.....	13
3.1 Vastandsuunaline edastus	13
3.2 TTL lävi.....	15
3.3 Administratiivselt hallatud piirid.....	16
4 Interneti grupi haldusprotokoll IGMP	18
4.1 IGMPv1	18
4.2 IGMPv2	21
4.3 IGMPv3	24
5 Multiedastus kommuteeritud võrgus.....	29
5.1 IGMP pealt kuulamine	31
5.2 Cisco grupihaldusprotokoll CGMP.....	38
6 Distant-vektor multiedastuse marsruutimis-protokoll DVMRP.....	41
6.1 DVMRP trimmitud levisaate puu	46
6.2 DVMRP pügamine.....	47
6.3 DVMRP pookimine	49
6.4 DVMRP infovahetuse käivitamine Cisco marsruuterites	49
7 Protokollist sõltumatu multiedastus - PIM	51
7.1 Tihedat laadi PIM.....	52
7.2 Hõredat laadi PIM.....	56
7.3 Hõre-tihe laadi PIM.....	65
7.4 Kahesuunaline PIM.....	66
7.5 Allika-spetsiifiline multiedastus PIM-SSM.....	69
8 Multiedastus Tartu Ülikooli arvutivõrgus	71
8.1 Multiedastuse käivitamine ja testimine	71
8.2 Digiteleviseiooni multiedastamine.....	75
8.3 Võrgutehnoloogia praktikumid Tartu Ülikoolis.....	79
Kokkuvõte	80
Multicast in Computer Networks	81
Kirjandus.....	82
Mõisted.....	84
Lisa 1. IGMP ja IGMP pealt kuulamine	88
Lisa 2. Hõre-tihe laadi PIM protokoll (PIM sparse-dense).....	90

Sissejuhatus

Töö sai alguse mitu aastat tagasi, kui kolleeg töö (töötan TÜ Infotehnoloogia osakonnas arvutivõrgu peaspetsialistina) juurest väitis, et TÜ arvutivõrgus multiedastus ei tööta. Tookord ei osanud seda väidet kinnitada ega tõestada ka vastupidist, sest puudusid vastavad teadmised. Nägime vaid seda, et ühendades ELIONi ADSL ruuteri neljanda porti arvutivõrguga, saime VLC multimeedia mängijaga teatud multiedastusgrupi aadressi pealt video voo avamisel pildi ette, aga see katkes alati mõne minuti möödudes ära.

Käesoleva magistritöö eesmärgiks ongi anda põhjalik ülevaade asutuse arvutivõrgus kasutatavatest multiedastusprotokollidest ja nendega seotud probleemidest, mida võib käsitleda ka õppematerjalina. Seejärel rakendada neid teadmisi TÜ arvutivõrgus: häälestada võrk multiedastuseks ja käivitada digiteleviseiooni vaatamise võimalus üle arvutivõrgu ning olla valmis teisteks üle multiedastuse pakutavateks teenusteks. Näiteks ülikoolisisesed videoülekanded TÜ Multimeedia osakonna poolt. Kuna tegelen Tartu Ülikoolis ka ainete “Võrgutehnoloogia I” ja “Võrgutehnoloogia II” õppejõuna, siis on eesmärgiks ka aine kuulajatega jagada saadud teadmisi praktikumide näol.

Oma töös piirdun asutuse siseselt kasutatavate multiedastustehnoloogiatega, mitte domeenidevaheliste protokollidega nagu MBGP (*MultiProtocol Border Gateway Protocol*) ja MSDP (*Multicast Source Discovery Protocol*). On olemas ka MOSPF (*Multicast Extensions to OSPF*) protokoll, mis, nagu nimigi ütleb, on üldlevinud OSPFv2 marsruutimisprotokollide laiendus ning seda võib kasutada nii autonoomse süsteemi piires kui ka mitme autonoomse süsteemi vahel. Kuid dünaamiliste ja paljude allikate, gruppidega võrkudes on MOSPF väga ressursimahukas. Seetõttu ei ole MOSPF heaks lahenduseks asutuse võrgus kasutamiseks ja edaspidi ma seda tehnoloogiat ei käsitle. MOSPF on kirjeldatud RFC-s 1584.

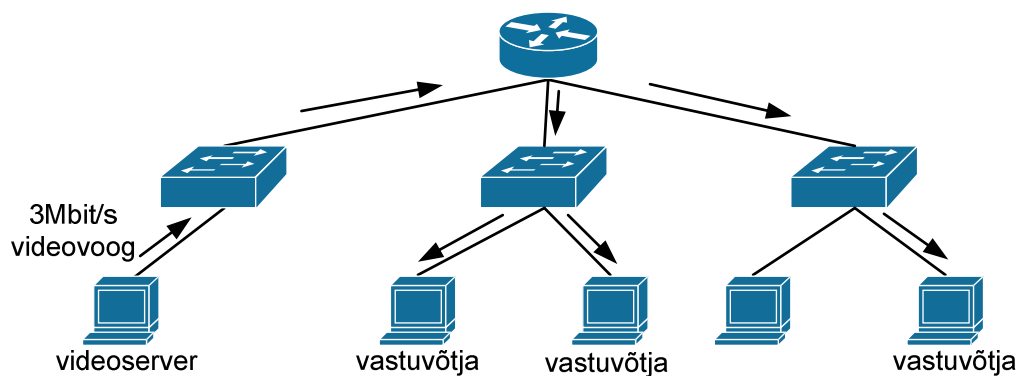
Kirjutasin oma magistritöö eesti keeles, sest antud tehnoloogia kohta puudub emakeelne materjal. Töö esimene pool on referatiivse iseloomuga, mida olen täiendanud omapoolsete näidete ja tähelepanekutega. Kõik konfigureerimise näited on seotud Cisco Systems seadmetega, sest tegu on andmeside võrguseadmete ja tarkvara tootjate seas turuliidriga ning ka TÜ magistraalvõrk ning paljude hoonete sisevõrgud on üles ehitatud Cisco Systems seadmetega. Töö teises pooles on kirja pandud see, kuidas ma saadud teadmisi rakendasin Tartu Ülikooli arvutivõrgus.

1 Multiedastus

Kui üks arvuti tahab suhelda teise arvutiga, siis ta üksikedastab pakette konkreetsele arvutile või leviedastab paketi igale arvutile lokaalses võrgus. Kuid on veel üks alternatiiv, see on multisaade, mis võimaldab pakette saata teatud arvutite grupile. See mudel on eriti kasulik rakenduste puhul, kus arvuti peab andmeid saatma mitmesse sihtkohta samaaegselt ja levisaate kasutamisel võib tekkida takistusi.

Näiteks videokonverentside puhul võib meile tunduda, et võiksime selleks kasutada leviedastust, mis tähendab, et iga arvuti lokaalses võrgus saab selles osaleda. See ei pruugi olla efektiivne lahendus, sest levisaade on kättesaadav iga arvuti jaoks lokaalses võrgus, kuid paketid ei jõua kaugvõrgu arvutiteni (enamik marsruutereid ei edasta levisaadet). Kui me seadistaksime marsruuteri levisaadet edastama, siis kogu levisaate paketid edastatakse ka kõigile neile kaugvõrgu arvutitele, mis ei ole nendest pakettidest huvitatud.

Multiedastusel on palju häid omadusi. Oletame, et meie arvutivõrgus on videosever, mis jagab 3 Mbit/s videovoogu. Selle asemel, et saata igale kliendile eraldi videovoog, nagu seda tehakse üksikedastuse puhul, saadetakse serverist välja ainult üks videovoog, mida marsruuterid ja kommutaatorid paljundavad vastavalt vajadusele nagu näidatud joonisel 1-1.



Joonis 1-1. Multiedastus üle arvutivõrgu.

Tegelikult nad isegi ei paljunda neid pakette, vaid edastamisel kasutatavad väljuvad liidesed jagavad ühist mäluühikut. Seega on multiedastus ribalaiust ning ka võrguseadmete ja serverite koormust säästev tehnoloogia.

Multiedastusel on ka negatiivseid omadusi. Kuna multiedastus eeldab üks-mitmele edastusmudelit, siis seal ei kasutata lõpp-punktide vahelisi kontrollmehhanisme nagu TCP puhul. Vaid multiedastus toimub üle UDP protokolliga ja ei garanteeri andmete kohale

jõudmist. Seega peavad multiedastuse rakendused hakkama saama mõningate pakettide kadumisega ning dubleeritud või vales järjestuses pakettide saamisega.

Siiski on olemas mõned eksperimentaalsed usaldusväärse multiedastuse transpordi protokollid, mis on toetatud mõningates võrguseadmetes ja operatsioonisüsteemides. Näiteks PGM (*Pragmatic General Multicast*), mis on kirjeldatud RFC-s 3208. Kui TCP kasutab jaatumärke (*ACK*), et teavitada saatjat mingi hulga pakettide vastuvõtmisest, siis PGM kasutab eitumärke (*Negative-ACK*) [1]. Kui vastuvõtja tuvastab paketi kadumise, siis ta üksikedastab allika suunas eitumärgi, mida ruuterid edastavad hüpe-hüppelt (et nad hiljem teaks, kuhu parandusi on vaja saata) ja kinnitavad eitumärgi saamist (*NAK Confirmation - NCF*). Parandusandmed (*RDATA*) saadab vastuvõtjale allikas või mõni vahepealne ruuter, mis on määratud parandajaks.

1.1 Multiedastuse IP aadressid

Erinevalt üksikedastuse IP aadressidest, mis identifitseerivad konkreetse hosti, määravad multiedastuse IP aadressid mingi juhusliku grupi hoste, mis on liitunud vastava grupiga ja soovivad saada sellesse gruppi edastatud liiklust. Multiedastuse tarbeks on IANA (*Internet Assigned Number Authority*) poolt eraldatud D klassi aadressruum. See tähendab seda, et binaarkujus on aadressi esimese okteti prefiksiks „1110“ ja kõik multisaate aadressid kuuluvad vahemikku 224.0.0.0 – 239.255.255.255.

IETF (*Internet Engineering Task Force*) on andnud IANA-le juhtnöörid multiedastusaadresside registreerimiseks (kirjeldatud RFC-s 3171). Kuid üldiselt on multiedastuse IP aadressid jagatud järgmisteks gruppideks:

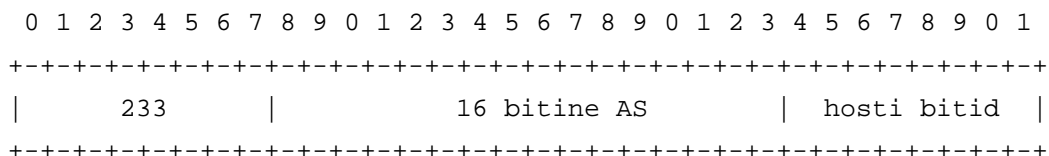
- 1) lokaalse skoobiga (lokaalse sideliini) aadressid (224.0.0.0 – 224.0.0.255);
- 2) globaalse skoobiga aadressid (224.0.1.0 – 238.255.255.255);
- 3) piiratud (administratiivse) skoobiga aadressid (239.0.0.0 – 239.255.255.255).

Lokaalse skoobiga aadresse 224/24 kasutatakse võrgu protokollide poolt lokaalse võrgusegmendi piires. Selle aadressruumi pakette edastatakse TTL (aega elada) väärtusega 1 ja marsruuterid neid edasi ei saada. Selle vahemiku aadresse registreerib IANA ning need on nähtavad veebiaadressil <http://www.iana.org/assignments/multicast-addresses>. Toon siinkohal mõned tuntumad registreeringud:

- 224.0.0.1 – kõik hostid antud kohtvõrgus;
- 224.0.0.2 – kõik marsruuterid antud kohtvõrgus;
- 224.0.0.4 – kõik DVMRP marsruuterid;
- 224.0.0.5 – kõik OSPF protokolliga kasutatavad marsruuterid;
- 224.0.0.6 – kõik OSPF määratud ja tagavara määratud marsruuterid (*DR – designated router; BDR – backup designated router*);
- 224.0.0.9 – kõik RIPv2 protokolliga kasutatavad marsruuterid;
- 224.0.0.10 – kõik IGRP protokolliga kasutatavad marsruuterid.

Multiedastuse adresseerimisel [2] on põhiküsimuseks, kas seda aadressi kasutatakse rangelt asutuse siseselt või globaalselt üle Interneti. Viimasel juhul tuleb kasutada globaalse skoobiga multiedastuse aadressi, mis ei satu konflikti mõne teise aadressiga. Globaalse skoobiga aadresse jagati algselt SDR protokolliga, hiljem hierarhiliselt üle interneti MASC (*Multicast Address Set-Claim*) protokolliga, mis on kirjeldatud RFC-s 2909.

Kuna globaalse skoobiga aadressid olid oma olemuselt dünaamilised ja multiedastuse algusaegadel ei olnud häid meetodeid aadresside jagamiseks, nii et nad konflikti ei satuks, siis loodi GLOP (GLOP ei ole akronüüm, vaid autori idee nimetada see vahemik nõnda) aadresside vahemik 233/8. GLOP vahemiku aadressid on globaalse skoobiga staatilised aadressid [3]. Iga autonoomse süsteemi AS numbrile on määratud 24-bitise maskiga aadressruum 233.x.y.0/24, kus oktetide x ja y väärtused saadakse AS numbrist. Valem on lihtne: kuna AS number on 16 bitine, siis ta sobib väga hästi kahe keskmise oktetiga täiteks nagu näidatud joonisel 1-2.



Joonis 1-2. GLOP aadressi tuletamine.

Näide 1-1.

Kui meil on kasutada AS nr 1234, siis binaarkujus on selle väärtus 0000010011010010, vasakpoolsed bitid täidetud nullidega. Jagame selle kaheks oktetiks: saame vastavalt "00000100" ja "11010010", mille väärtused kümnendsüsteemis on 4 ja 210. Seega on meil kasutada globaalse skoobiga võrguaadress 233.4.210.0/24.

Internetis on olemas ka kalkulaator, mis oskab tuletada AS numbrist põhjal globaalse skoobiga aadressi ja vastupidi: <http://www.shepfarm.com/multicast/glop.html>.

Saime teada, et igal asutusel (mil on olemas AS number) on kasutada maskiga /24 multisaate võrk. Aga kui asutus vajab suuremat aadressruumi või kui asutusel ei olegi AS numbrit? Tegelikult on veel üks kasutamata tükike globaalse skoobiga aadresside vahemikust [4]. Kuna RFC 1930 põhjal on olemas privaatsed AS numbrid 64512 kuni 65535, siis regionaalsetel Interneti registritel on suure vajaduse korral võimalik nende põhjal välja jagada lisa-aadresse.

Rangelt asutuse sisesel kasutamisel (rakendused, mis ei edasta üle Interneti) võime kasutada administratiivse skoobiga aadresse (239/8). Kuna need aadressid on lokaalse tähtsusega, siis ei pea nende kasutamist IANA-ga kooskõlastama. Administratiivse skoobiga aadressruumi võime autonoomse süsteemi piires omakorda jagada kaheks:

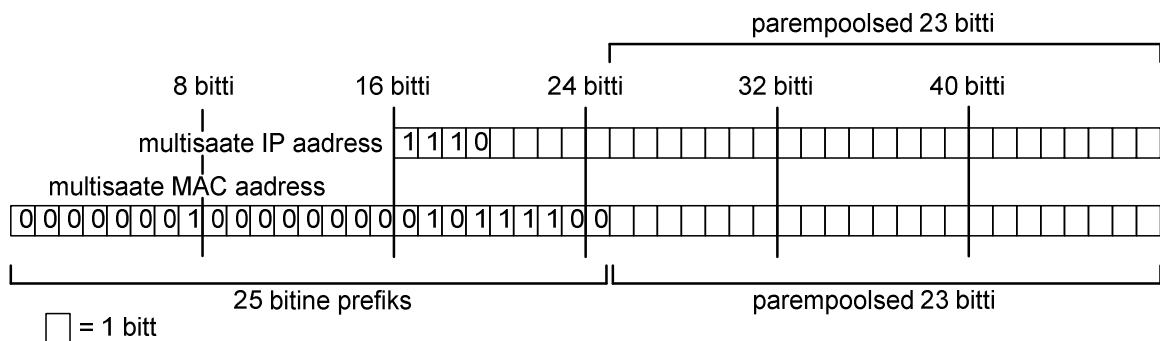
- 1) organisatsiooni skoobiga aadressid (239.192.0.0 – 239.251.255.255);
- 2) lokaalse võrgukoha (*site-local*) aadressid (239.255.0.0/16, vajadusel võimalik kasutada ka 239.252.0.0/16, 239.253.0.0/16 ja 239.254.0.0/16).

Lokaalse võrgukoha skoobiga aadressid võimaldavad aadresside taaskasutamist erinevates domeenides.

1.2 Multiedastuse MAC aadressid

Multiedastuse MAC aadresside esimese okteti madalaimad bitid on alati väärtusega 0x01. IANA omab MAC aadresside ploki prefiksiga 0100.5e. Pool sellest on eraldatud multiedastusele. Seega multiedastuse adresseerimiseks on kasutada 23 bitti ja selleks kasutatakse vahemikku 01.00.5e00.0000 kuni 0100.5e7f.ffff. Multiedastuse IPv4 aadressid on aga 32-bitised, millest esimesed neli on alati väärtusega “1110”, seega adresseerimiseks on kasutada 28 bitti.

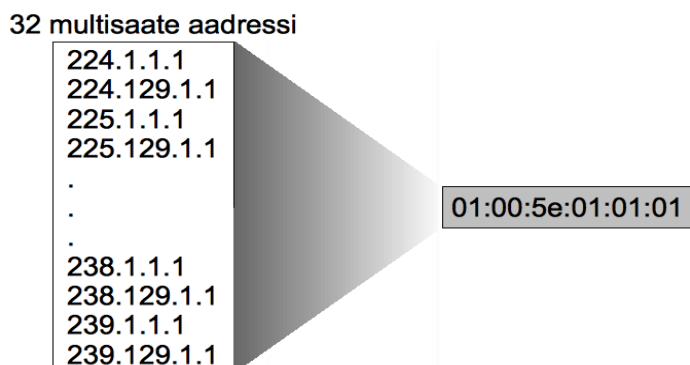
Kõik multiedastuse IP aadressid seotakse MAC aadressiga. Kuna 28 bitiga moodustatavaid IP multisaate aadresse ei saa kujutada 23 bitist moodustatavate MAC aadressidena, siis tehakse teisendus lihtsalt nii, et multisaate IP aadressi 23 parempoolset bitti kujutatakse 23 parempoolse bitina IEEE MAC aadressis, lisatakse 25-bitine prefiks ja 5 bitti infot läheb kaduma nagu näidatud joonisel 1-3.



Joonis 1-3. Multisaate IP aadressi kujutamine MAC aadressiks.

Ajaloost on teada [5], et see 5 biti info kaotamine ei olnud tahtlik. Kui 1990-ndate alguses Dr Steve Deering tegi uurimustööd IP multisaate kohta, siis ta soovis IEEE-lt 16 järjestikku OUI-d IP multiedastuse MAC aadresside tarbeks. Sest üks OUI annab 24 bitti aadressruumi ja 16 järjestikust OUI-d võimaldaks 1:1 sidumist multisaate IP aadresside ja MAC aadresside vahel. Sel ajal nõudis IEEE iga eraldatud OUI eest 1000\$, seega oleks juhendaja pidanud kulutama 16000\$, et uurimustööd jätkata. Kuna ressursid olid piiratud, nõustus juhendaja ostma ühe OUI ja andis pool sellest (23 bitti) Dr Deeringule ning teise poole reserveeris teiste teadustööde tarvis.

Seega vastab igale multisaate MAC aadressile 32 multisaate IP aadressi nagu näidatud joonisel 1-4.



Joonis 1-4. Multisaate MAC aadressi mitmesus [5].

Administraatorid peavad selle asjaoluga multiedastuse aadresside määramisel arvestama. Oletame näiteks, et üks vastuvõtja liitub multisaate grupiga A (224.1.1.1) ja teine vastuvõtja liitub multisaate grupiga B (225.1.1.1), siis andmelülikihi tasemel hakkavad nad mõlemad vastu võtma A ja B grupi liiklust, mis oleks masina ressursside raiskamine.

Kommutaatorid kasutavad tavaliselt IGMP pealt kuulamist (*IGMP snooping*), et piirata multiedastuse liiklust ainult nendesse portidesse, kus asuvad hostid, mis on avaldanud soovi liituda vastava multisaate grupiga. Kuid enamus L2 kommutaatoreid ujutavad võrgu üle (kaader edastatakse kõikidesse portidesse) multiedastuskaadritega, mille MAC aadressiks on 0100.5e00.00xx (vastav võrgukihi aadress kuulub lokaalse sideliini ploki). Lokaalse sideliini kaadrid ujutatakse üle võrgu seetõttu, et vastavatesse multiedastusgruppidesse ei saadeta liikmelisuse raporteid. Näiteks marsruuterid ei saada liikmelisuse raporteid „kõik OSPF marsruuterid“ grupile (224.0.0.5) kui OSPF marsruutimisprotsess on käimas. Kui kommutaatorid piiraks lokaalse sideliini grupi kaadreid ainult portidesse, kust tulevad liikmelisuse raportid, siis OSPF marsruutimisprotokoll ei töötaks.

Kuid peale lokaalse sideliini ploki (224.0.0.0/24) on MAC aadressiga 0100.5e00.00xx seotud veel teisigi aadressivahemikke ja seega ka nende gruppide liiklust ujutatakse üle kommuteeritud võrgu. Sel põhjusel tuleks kujul „x.0.0.y“ ja „x.128.0.y“ multiedastus-aadresside kasutamist vältida.

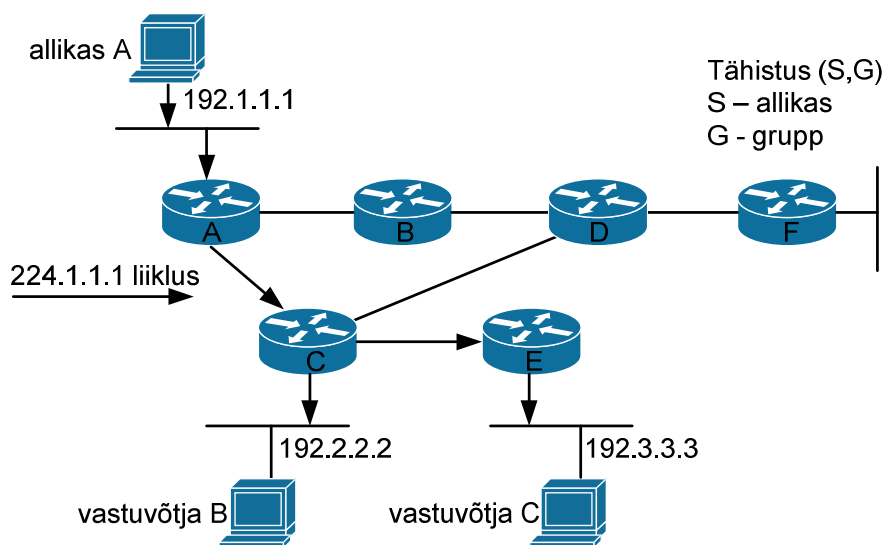
2 Multiedastuse jaotuspuud

Multisaate korral saadetakse andmed suvalisele grupile arvutitele, mis on esindatud multisaate grupi aadressiga. Andmete edastamisel üle ruuterite kõikide saajateni tekib nn multisaate jaotuspuu [5]. Multisaate jaotuspuid on kahte liiki: lähtepuu (*source tree*) ja jagatud puu (*shared tree*).

2.1 Lähtepuu

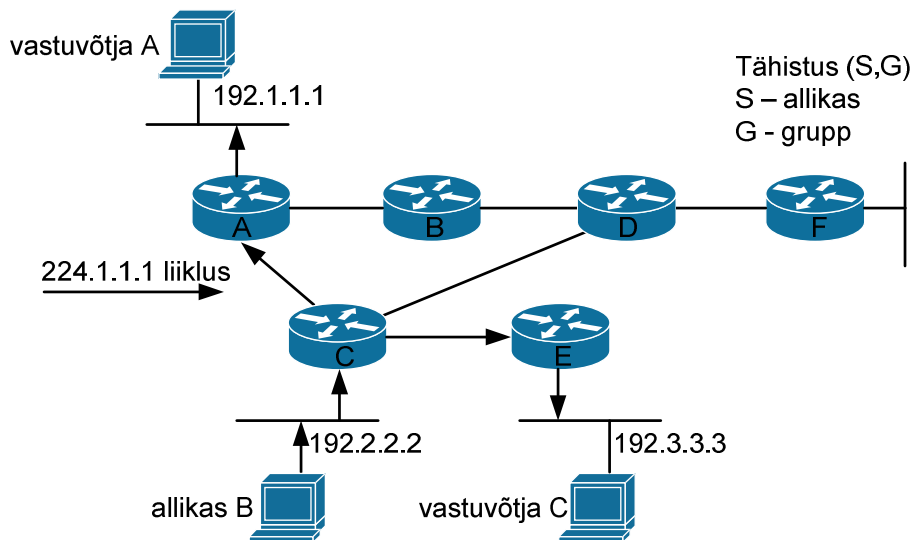
Lähtepuu on multisaate jaotuspuu lihtsaim vorm: tema juureks on multisaate allikas, hargnemiskohtadeks marsruuterid ja lehtedeks multisaate vastuvõtjad. Kuna see puu kasutab läbi võrgu lühimaid teid saajateni, siis nimetatakse seda puud ka lühima tee puuks SPT (*Shortest Path Tree*).

Joonisel 2-1 on SPT näide multisaate grupile 224.1.1.1, mille juureks on arvuti A ning vastuvõtjad B ja C.



Joonis 2-1. Host A lühima tee puu [5].

SPT tähistuseks on (S, G), kus S on allika IP aadress ja G on multisaate grupi aadress. Seega joonisel 2-1 toodud lähtepuu tähistuseks on (192.1.1.1, 224.1.1.1). Iga allika jaoks on olemas eraldi lähtepuu. Kui arvuti B samuti saadab andmeid grupi aadressile 224.1.1.1 ning A ja C on vastuvõtjad, siis leidub eraldi (S, G) lähtepuu tähistusega (192.2.2.2, 224.1.1.1) nagu näidatud joonisel 2-2.

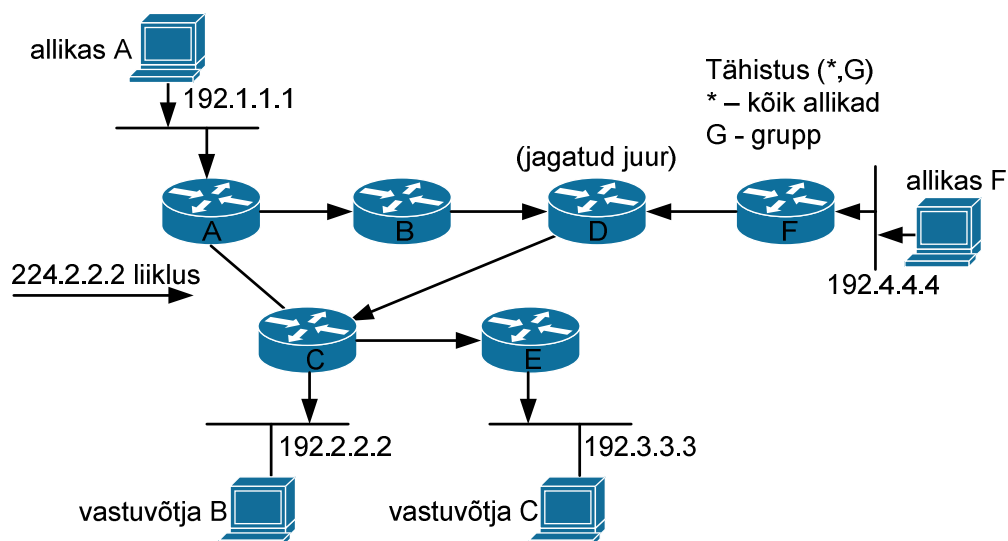


Joonis 2-2. Host B lühima tee puu [5].

2.2 Jagatud puud

Kui lähtepuu juureks oli multisaate allikas, siis jagatud puu korral kasutatakse ühte ühist juurt, milleks on võrgust valitud marsruuter. Sõltuvalt multisaate marsruutimisprotokollist nimetatakse seda juurt kohtumispunktiks RP (*Rendezvous Point*) või tuumaks (*Core*), millest tulenevad jagatud puude üldtuntud nimed RP puu RPT (*RP trees*) või tuumapõhised puud CBT (*Core-based trees*).

Joonisel 2-3 on kujutatud jagatud puu grupile 224.2.2.2, mille juureks on marsruuter D. Jagatud puu kasutamisel saadavad allikad oma liikluse juurele ja sealt edasi liigub liiklus vastuvõtjateni.

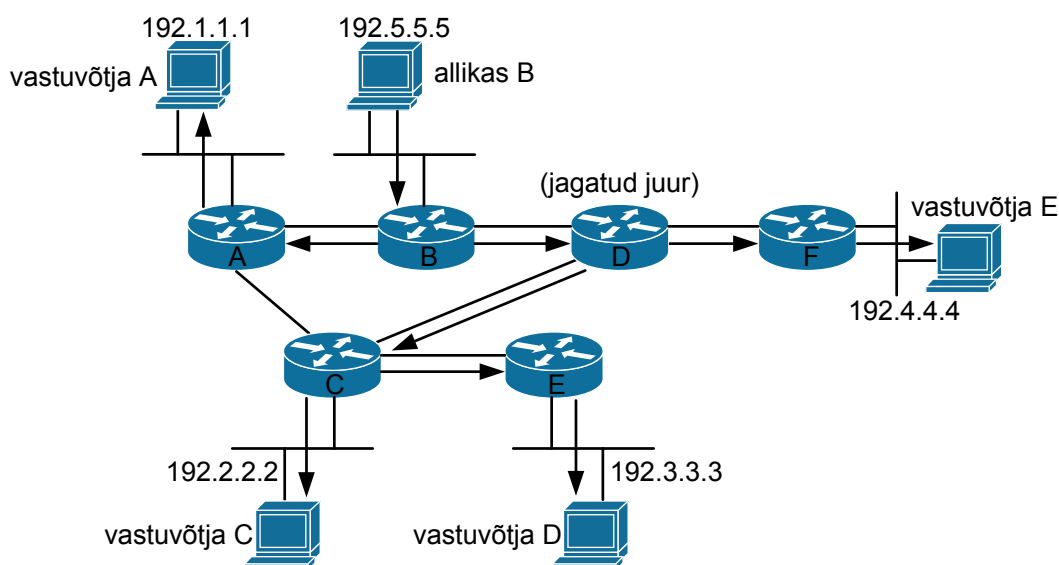


Joonis 2-3. Jagatud puu [5].

Kuna multisaate grupi kõik allikad kasutavad ühist jagatud puud, siis tähistatakse seda puud (*, G). Antud juhul * tähistab kõiki allikaid ja G multisaate gruppi. Seega on joonisel 2-3 kujutatud jagatud puu tähiseks (*, 224.2.2.2).

2.3 Kahesuunalised jagatud puud

Jagatud puud jagunevad omakorda kaheks: ühesuunalised ja kahesuunalised. Kahesuunalise jagatud puu (*Bidirectional shared tree*) korral võib multisaate liiklus voolata jagatud puus nii üles kui alla, et jõuda vastuvõtjateni. Joonisel 2-4 on kahesuunalise jagatud puu näide, kus allika B multisaate liiklus saadetakse esimese-hüppe marsruuteri poolt jagatud puu juure suunas ja seejärel vastupidises suunas tagasi vastuvõtjate poole (antud juhul vastuvõtja A suunas).



Joonis 2-4. Kahesuunaline jagatud puu [5].

2.4 Ühesuunalised jagatud puud

Ühesuunalised jagatud puud lubavad multisaate liiklusel voolata ainult juurest allapoole vastuvõtjateni. Seepärast peavad multisaate allikad liikluse juureni saatmiseks kasutama teisi meetodeid.

Esimeseks võimaluseks on lasta juurel eraldi liituda lähtepuuga, mille juureks on allikas ise, et tõmmata liiklus jagatud puu juureni ja seejärel mööda jagatud puud laiali saata. PIM (*Protocol Independent Multicast*) kasutab sellist meetodit allikast liikluse kättesaamiseks.

Teine võimalus multisaate liikluse juureni saamiseks on lasta see esimese-hüppe

marsruuteril üksikedastada otse üle IP-IP tunneli juurele, mis selle liikluse lahti kapseldab ja mööda jagatud puud edasi saadab. Seda meetodit kasutab CBT (*Core Based Trees*) multisaate marsruutimisprotokoll kui allikaks on ainult-saatev host, mis samas ei ole liitunud antud multisaate grupiga. CBT oli akadeemiline projekt, mida arendati mõned aastad, kuid ametliku versioonini ei jõutudki. Algsele versioonile CBTv1 (kirjeldatud RFC-s 2201) järgnes CBTv2 (kirjeldatud RFC-s 2189), mis ei olnud tagasiühilduv CBTv1-ga. Valmis ka CBTv3 kavand, mis ei olnud tagasiühilduv vanade versioonidega. Seetõttu CBT protokoll ei oma töös ei käsitle, kuid CBT-ga sarnaseid põhimõtteid kasutab kahe-suunaline PIM protokoll, mida tutvustan alapeatükis 7.3.

2.5 Lähtepuud vs jagatud puud

Nii lähtepuud kui jagatud puud on tsükli-vabad. Pakette paljundatakse ainult puu hargnemiskohtades. Mõlemad jaotuspuid tuleb dünaamiliselt hallata, sest multisaate grupi liikmed võivad liituda ja lahkuda grupist igal ajal. Kui mingis harus kõik aktiivsed vastuvõtjad enam ei soovi multiedastust saada, siis marsruuter püüab jaotuspuust vastava haru ja ei edasta sinna enam multisaadet.

Lähtepuudel on omadus tekitada optimaalne tee allika ja vastuvõtjate vahel [6]. See eelis garanteerib minimaalse latentsuse multiedastamisel. Kuid sellisel optimeerimisel on ka negatiivne pool: marsruuterid peavad mälu hoidma tee informatsiooni iga allika jaoks. Seega kui meie arvutivõrgus on tuhandeid multisaate allikaid ja grupe, tuleb tähelepanu pöörata marsruuteri mälu kasutusele.

Jagatud puude eeliseks on väga väike tee informatsiooni haldamise vajadus, mis tingib väiksema mäluvajaduse. Puuduseks on see, et allikate ja vastuvõtjate vahelised teed ei pruugi alati olla optimaalsed ning see omakorda võib põhjustada suuremat latentsust pakettide edastamisel.

Näiteks joonisel 2-4 on host A (allikas) ja host B (vastuvõtja) vaheliseks lühimaks teeks läbi ruuterite A ja B. Kuna jagatud puu juureks või kohtumispunktiks on ruuter D, siis multiedastuse liiklus peab liikuma allikast vastuvõtjani läbi ruuterite A, B, D ja C. Seega tuleb kohtumispunkti väga hoolikalt valida kui rakendada ainult jagatud puu keskkonda.

3 Multisaate edastamine

Üksiksaate korral edastatakse pakett läbi võrgu ühte teed pidi lähtekohast sihtkohta, mille IP aadress on kirjas paketi sihtaadressi väljal. Iga marsruuter sellel teel teeb edastamise otsuse, kasutades paketi sihtaadressi ja otsides vastavat sihtvõrku oma üksikedastuse marsruutimistabelist. Kui sihtvõrk leitakse siis pakett edastatakse marsruutimistabelis näidatud liidest pidi järgmisele hüppele sihtkoha suunas.

Multisaate korral saadab allikas infot teatud masinate grupele, mis on esindatud multisaate grupi aadressina IP paketi sihtaadressi väljal. Multisaate marsruuterid peavad kindlaks tegema, milline on ülesvoolu suund (allika poole) ja milline on allavoolu suund (suunad). Kui leidub mitu allavoolu suunda, siis marsruuter paljundab paketid ja edastab need allavoolu suunas. Multisaate edastamist pigem allikast eemale, kui vastuvõtjate suunas nimetatakse vastandsuunaliseks edastuseks RPF (*Reverse Path Forwarding*), mis on multisaate edastamise aluseks enamikes multisaate marsruutimisprotokollides.

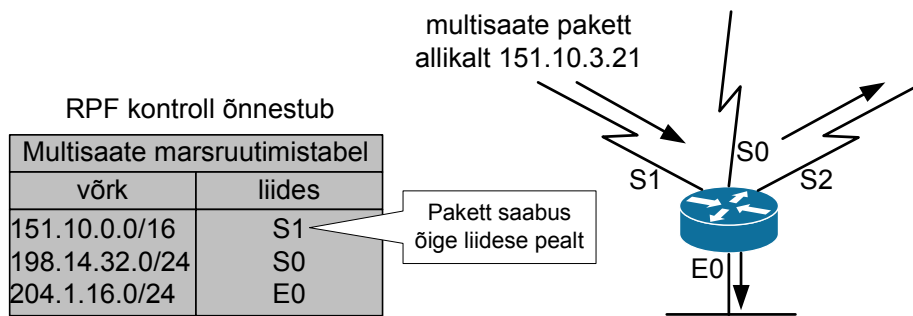
3.1 Vastandsuunaline edastus

Tegelikult kasutavad peaaegu kõik multisaate marsruutimisprotokollid mingil määral RPF kontrolli või sissetuleva liidese kontrolli, et otsustada kas pakett edasi saata või minema visata. Mõõda lähtepuud alla liikuva liikluse jaoks tähendab RPF kontroll järgmist:

- 1) marsruuter vaatab saabuva multisaate paketi lähteadressi ja teeb marsruutimistabeli järgi kindlaks kas pakett saabus liideselt, mis jääb tagasiteele allikani;
- 2) kui pakett saabus tagasi allikani viivalt liideselt, siis on RPF kontroll edukas ja pakett edastatakse;
- 3) kui RPF kontroll ebaõnnestub, siis pakett visatakse minema.

Allikani viiva liidese määramine sõltub kasutatavast marsruutimisprotokollist. Mõningad multisaate marsruutimisprotokollid peavad ülal eraldi multisaate marsruutimistabelit ja kasutavad seda RPF kontrolli jaoks (näiteks DVMRP). Teised kasutavad selleks aga üksiksaate marsruutimistabelit, nagu näiteks PIM ja CBT. Kuid PIM ja CBT oskavad kasutada ka teiste protokollide, nagu DVMRP ja MBGP marsruutimistabeleid või siis hoopis staatiliselt configureeritud RPF informatsiooni.

Joonisel 3-1 on toodud näide RPF kontrollist.



Joonis 3-1. RPF kontroll õnnestub [5].

Multisaate pakett allikalt 151.10.3.21 saabub liideselt S1. Antud olukorras eeldame, et tegu on DVMRP marsruutimisprotkolliga. Multisaate marsruutimistabelist on näha, et tagasiteel allikani peaksime kasutama liidest S1, seega RPF kontroll on edukas ja pakett edastatakse kõikidele väljuvate liideste nimekirjas olevatele liidestele (väljuvate liideste nimekiri ei pea tingimata sisaldama kõiki marsruuteri liideseid).

Oleme teada saanud, et multisaate liikluse edastamiseks üle võrgu kõikide vastuvõtjateni kasutatakse multisaate jaotuspuid. Lähtepuude ja jagatud puude hargnemiskohaks on tavaliselt marsruuter ning vastav puu on marsruuteris kirjeldatud multisaate edastamise puhvri (sageli viidatud kui multisaate marsruutimistabel) kirjena, kus sissetulev liides on seostatud null või enama väljuva liideselega.

Iga siseneva multisaate paketi korral RPF kontrolli teostamine oleks marsruuteri jaoks liiga koormav. Seepärast määratakse ära ka RPF liides, kui lisatakse kirje multisaate edastamise puhvrise. RPF liides saabki vastava kirje sissetulevaks liideseks. Vastava kirje väljuvate liideste määramine sõltub kasutatavast multisaate protokollist.

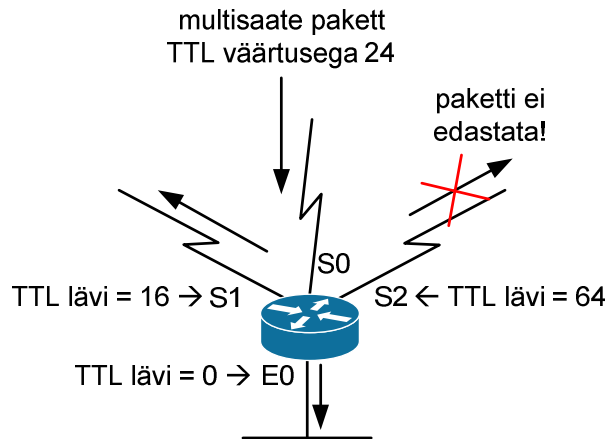
Näide 3-1. Cisco multisaate marsruutimistabeli kirje (**show ip mroute** väljundist).

```
(151.10.3.21/32, 224.2.127.254), 00:04:15/00:01:10, flags: T
  Incoming interface: Serial1, RPF nbr 171.68.0.91
  Outgoing interface list:
    Serial2, Forward/Sparse, 00:04:15/00:02:17
    Ethernet0, Forward/Sparse, 00:04:15/00:02:13
```

See (S, G) kirje kirjeldab joonisel 3-1 olevat SPT-d (151.10.3.21/32, 224.2.127.254). Lipp T näitab, et paketid saavad mööda lühima tee puud SPT. Sissetulev liides on Serial1 ja väljuvateks liidesteks on Serial2 ja Ethernet0, mis edastavad hõredas laadis. Ülesvoolu ruuteriks on 171.68.0.91.

3.2 TTL lävi

Marsruuterid vähendavad edastatavate pakettide IP päises olevat TTL väärtust ühe võrra. Kui paketi TTL väärtus on vähendatud 0-ni, siis pakett visatakse minema. Multisaate marsruuteri erinevatele liidestele on võimalik määrata TTL lävi, et vältida lävest väiksema TTL väärtusega pakettide edastamist.



Joonis 3-2. TTL läved [5].

Joonisel 3-2 saabub multisaate pakett TTL väärtusega 24 Serial0 liideselt. Oletame, et RPF kontroll on edukas ning Serial1, Serial2 ja Ethernet0 on kõik väljuvate liideste nimekirjas. Kuna liidestele on määratud TTL läved, siis peab marsruuter enne edastamist veenduma, et paketi TTL väärtus (mis on nüüd 23) on suurem või võrdne väljuva liidese TTL lävega. Pakett saadetakse välja Serial1 ja Ethernet0 liidestelt. Kui liidese TTL lävi on 0, siis sellel liidesel ei ole TTL läve määratud.

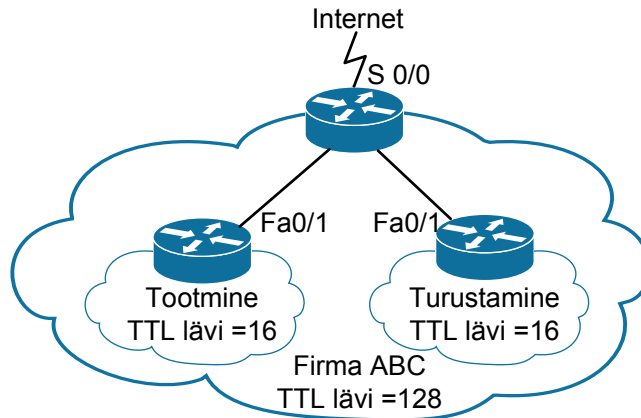
TTL läve kehtestamine aitab meil lihtsasti vältida multisaate liikluse edastamist väljapoole meie asutust või regiooni. Lisaks sellele aitab TTL lävi ära hoida pakettide lõputu ringlemise kui võrgus peaks ruutimistsükkel tekkima. TTL lävi määratakse liidesele, seega liidese konfigureerimise režiimis tuleb anda käsk:

```
ip multicast ttl-threshold <lävi>,
```

kus lävi on vahemikus 0 kuni 255. Vaikeväärtuseks on 0, mis tähendab et kõik multisaate pakettid edastatakse, sõltumata TTL väärtusest. Kehtivat TTL väärtust on võimalik vaadata käsuga:

```
show ip multicast interface <liides>.
```

Joonisel 3-3 on toodud näide TTL läve kasutamisest asutuses.



Joonis 3-3. TTL lävega piiritlemine.

Multisaate rakendused, mis tahavad oma liiklust piiritleda asutuse ABC võrgus, peavad saatma multisaate pakette TTL algväärtusega 127. Tootmise ja turustamise osakonnad on oma võrgu äärealadel kehtestanud TTL läve 16. Nii saavad nende võrkude multisaate rakendused vältida transmissioonide väljumist vastavatest võrkudest, kasutades TTL väärtust 15.

3.3 Administratiivselt hallatud piirid

Multiedastuse piiramine TTL läve kehtestamisega liidestel võib sageli osutada keeruliseks ja tülikaks, mõningatel juhtudel isegi problemaatiliseks [7]. Me võime multiedastust piirata ka aadresside põhjal. Me võime oma võrgus tekitada mitu saarekest, mis kasutavad administratiivse skoobiga aadressruumist lokaalse võrgukoha aadresse. Need aadressid ei pea olema unikaalsed, sest nad ei välju meie poolt hallatud piiridest.

Kui täiendada joonisel 3-3 toodud näidet, siis tootmise ja turustamise üksuste ruuteritele tuleks anda järgmised korraldused:

```
interface FastEthernet 0/1
    ip multicast boundary 1
    ip multicast ttl-threshold 16
access-list 1 deny 239.255.0.0 0.0.255.255
access-list 1 permit any
```

ja asutuse ABC ruuterile sellised korraldused:

```
interface Serial 0/0
    ip multicast boundary 10
    ip multicast ttl-threshold 16
access-list 10 deny 239.0.0.0 0.0.0.255
```

```
access-list 10 deny 224.0.1.39
access-list 10 deny 224.0.1.40
access-list 10 permit any.
```

Oleme loonud sellised pääsuloendid, et tootmise ja turustamise üksuste välise liidese pealt ei välju ega võeta vastu 239.255/16 võrgu liiklust ning asutuse ABC välisühenduse ruuteri liideselt ei välju ega võeta vastu võrkude 239/8, 224.0.1.39 ega 224.0.1.40 liiklust. Viimaseid kahte aadressi kasutab hõredat laadi PIM protokoll, millest tuleb juttu peatükis 7.

4 Interneti grupi haldusprotokoll IGMP

IGMP (*Internet Group Management Protocol*) peamine eesmärk on võimaldada arvutitel teavitada lokaalseid marsruutereid oma soovist saada mingi multisaate grupi liiklust ehk soovi liituda selle grupiga. Alates IGMPv2-st saavad masinad teavitada ka multisaate grupist lahkumist kui nad enam sellest liiklusest huvitatud ei ole. Multiedastuse marsruuterid kuulavad IGMP teateid ja saavad perioodiliselt päringuid, et teada saada, millised multisaate grupid on aktiivsed ja millised mitte.

4.1 IGMPv1

Kuna IGMPv1 võimalused on piiratud, siis tänapäeva rakendused seda enam ei kasuta. Kuid siiski on oluline teada kuidas see töötab ja millised need piirangud on. IGMP teateid edastatakse tavaliste IP pakettidena, mille IP protokoll number on 2 ja eluiga (TTL) on 1, seega on nad lokaalsed ja marsruuterid neid ei edasta.

0	4	7	15	23	31
Version	Tüüp	Kasutamata	Kontrollsumma		
Grupi aadress					

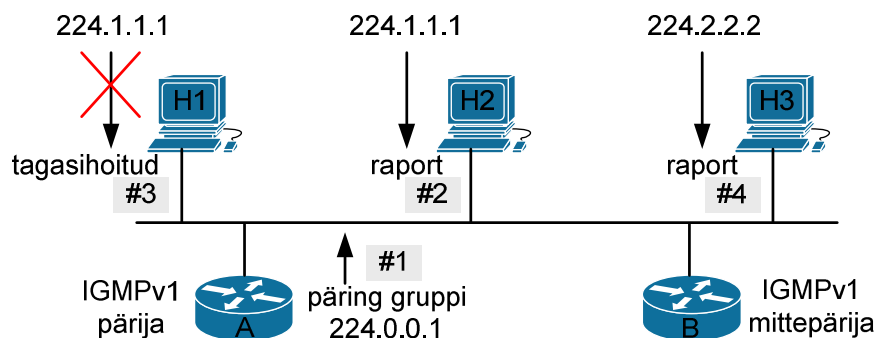
Joonis 4-1. IGMPv1 teate formaat [8].

Joonisel 4-1 on kujutatud IGMPv1 teate formaat, millel on järgmised väljad:

- versioon – IGMP versiooninumber ja seega väärtuseks on 1. IGMPv1 eelkäija versiooninumbriks oli 0 ja IGMPv2 puhul on väli elimineeritud;
- tüüp – IGMPv1 korral kasutatakse ainult kahte tüüpi teadet:
 - 1 = liikmelisuse päring;
 - 2 = liikmelisuse raport;
- kasutamata – kasutamata väli, nullitakse saatmisel ja ignoreeritakse vastuvõtmisel;
- kontrollsumma – 16-bitine kontrollsumma;
- grupi aadress – multisaate grupi aadress liikmelisuse raporti saatmisel, väli on nullitud liikmelisuse päringute korral ja ignoreeritakse hostide poolt.

4.1.1 IGMPv1 päring-vastus protsess

IGMP kasutab peamiselt päring-vastus tehnikat, mis aitab multisaate marsruuteril kindlaks teha aktiivsed multisaate grupid (grupid, milles on vähemalt üks vastuvõtja) lokaalses võrgus.



Joonis 4-2. IGMPv1 päring-vastuse protsess [5].

Joonisel 4-2 tahavad hostid H1 ja H2 saada multisaate grupi 224.1.1.1 liiklust. Host H3 on huvitatud grupist 224.2.2.2. Antud kohtvõrgus on marsruuter A IGMP pärija ning marsruuter B mitte-pärija, kes lihtsalt kuulab ja salvestab hostide vastuseid.

IGMPv1 päring-vastus süsteem antud näite korral töötab nii:

- 1) marsruuter A (IGMP pärija) multiedastab lokaalsesse võrku perioodiliselt (vaikimisi iga 60 sekundi järel) IGMPv1 liikmelisuse päringu “kõik-hostid” multisaate grupile (224.0.0.1). Kõik multisaate võimelised hostid peavad seda gruppi kuulama ja seega võtavad päringud vastu;
- 2) masin H2 jõuab esimesena vastata IGMPv1 liikmelisuse raportiga multisaate grupile 224.1.1.1, mille liige ta on. See raport annab kohtvõrgu marsruuterile teada, et leidub vähemalt üks host, mis on huvitatud grupi 224.1.1.1 multisaatest;
- 3) kuna host H1 kuulab multisaate gruppi 224.1.1.1, siis ta kuuleb ka H2 saadetud IGMPv1 liikmelisuse raportit ja keelustab oma raporti saatmise, sest marsruuter juba teab, et multisaate grupile 224.1.1.1 on vähemalt üks vastuvõtja olemas. Selline raporti tagasihoidmise mehhanism aitab vähendada lokaalse võrgu koormust;
- 4) host H3 on samuti saanud IGMPv1 liikmelisuse päringu ja ta multiedastab IGMPv1 liikmelisuse raporti grupile 224.2.2.2, mille liige ta on.

Selliste päring-vastuste vahetamistega teab marsruuter A, et on olemas aktiivsed kuulajad multisaate gruppidele 224.1.1.1 ja 224.2.2.2. Seda sama teab ka marsruuter B, sest ta kuulis kõike pealt.

4.1.2 Raporti tagasihoidmise mehhanism

IGMP raportite tagasihoidmise mehhanism aitab vähendada kohtvõrgu koormust ja ka hostide ressursse. Järgnevalt annan ülevaate kuidas seda tehakse:

- 1) kui host saab IGMP liikmelisuse päringu, siis ta käivitab raport-timeri iga multisaate grupi jaoks, millega ta on liitunud. Iga raport-timer algväärtustatakse juhusliku väärtusega vahemikust 0 kuni x , kus x on maksimaalne vastamise aeg (vaikimisi 10 sekundit);

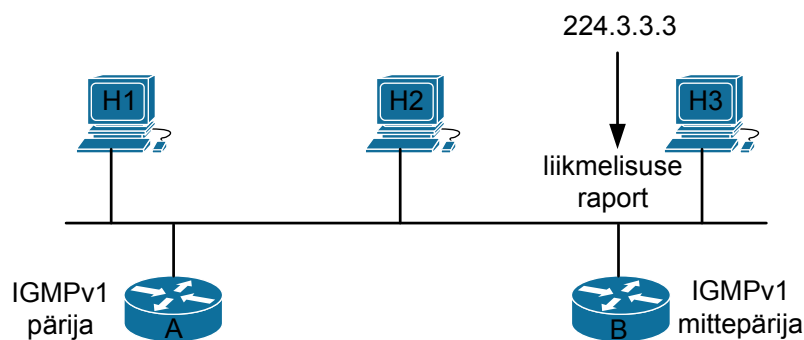
- 2) kui raport-taimer jõuab nulli, siis host saadab IGMP liikmelisuse raporti vastava raport-taimeriga seotud multisaate gruppi;
- 3) kui host kuuleb kedagi teist saatmas IGMP liikmelisuse raportit, siis ta katkestab vastava grupiga seotud taimeri ja keelustab sellega liikmelisuse raporti saatmise vastavasse gruppi.

4.1.3 IGMPv1 pärija

Kui ühte võrgusegmenti on ühendatud mitu multisaate marsruuterit, siis ei ole mõtet neil kõigil olla IGMP pärija rollis. IGMPv1 korral ei ole paraku spetsiaalset protsessi pärija valimiseks välja töötatud ja pärijaks saamine sõltub kasutatavast IP multiedastuse marsruutimise protokollist.

4.1.4 IGMPv1 grupiga liitumise protsess

Kui host soovib liituda mingi multisaate grupiga, siis ta ei pea ootama marsruuteri poolt saadetavat liikmelisuse päringut, vaid võib ise koheselt saata liikmelisuse raporti nagu näidatud joonisel 4-3.



Joonis 4-3. IGMPv1 liitumise protsess [5].

4.1.5 IGMPv1 grupist lahkumise protsess

Paraku on IGMPv1 puhul grupist lahkumine tehtud väga lihtsaks – nad lihtsalt lähevad minema. Ei ole olemas IGMPv1 grupist lahkumise teadet, millega teavitada marsruuterit, et host ei soovi enam saada mingi grupi multisaadet. Host lihtsalt ei võta enam multisaate grupi pakette vastu ja lõpetab IGMP päringutele vastamise vastavas grupis.

IGMP marsruuterid seovad iga multisaate grupiga taimeri. Kui vastavas grupis saadakse liikmelisuse raport, siis taimer algväärtustatakse. Tavaliselt on selleks algväärtuseks kolmekordne päringu intervall ehk 3 minutit. See aga tähendab seda, et marsruuter võib halvimal juhul jätkata multisaate edastamist lokaalsesse võrku kolmeks minutiks pärast viimase hosti lahkumist grupist. Selline latentsus võib tekitada probleeme. Oletame, et asutuses on viis erinevat gruppi multisaate allikaga, mis pakuvad kõrge kvaliteediga

videot. Kui kaugkasutaja (kelle võrguühendus on piiratud kiirusega) ei tea, millise kanali peal teda huvitav video jookseb, siis ta võib lihtsalt järjest kõik grupid läbi vaadata. Halvimal juhul on kasutaja liitunud viie multisaate grupiga leides huvipakkuva video ja lahkunud ilma teavitamata neljast grupist. See tähendab, et marsruuter võib edastada kaugkasutajale mittesoovitud nelja videovoogu kuni kolmeks minutiks ja kuigi kaugkasutaja näeb nüüd oma soovitud videot, võib esineda palju vigu suure ülekoormatuse tõttu.

Grupist lahkumise probleem oli peamine põhjus järgmise IGMP versiooni arendamiseks.

4.2 IGMPv2

IGMPv2 standard kinnitati IETF poolt 1997. a novembris (RFC 2236) ja on praegu enimkasutatav standard. IGMPv2 on tagasiühilduv IGMPv1-ga.

IGMPv2 protokollile lisati mõned uued omadused: pärija valimine, maksimaalne vastamise aeg, grupi-spetsiifilised päringud ja grupist lahkumise teated. Viimased kaks võimaldasid hostidel ja marsruuteritel vähendada grupist lahkumise latentsust minutitelt mõnele sekundile.

IGMPv2 päring-vastus protsess on sarnane IGMPv1-ga. Järgnevalt annan ülevaate uutest IGMPv2 lisavõimalustest:

- pärija valimine – võimaldab IGMPv2 marsruuteritel valida pärija sõltumata kasutatavast multiedastuse marsruutimisprotokollist;
- maksimaalse vastamise aja väli – uus väli päringu teadetes võimaldab pärijal määrata maksimaalse päring-vastuse aja;
- grupi-spetsiifilised päringud – võimaldab pärija marsruuteril saata päring konkreetsesse gruppi;
- grupist lahkumise teated – võimaldab hostidel teavitada marsruutereid oma soovist grupist lahkuda.

0	7	15	23	31
Tüüp	Max vastamise aeg	Kontrollsumma		
Grupi aadress				

Joonis 4-4. IGMPv2 teate formaat [9].

Joonisel 4-4 on toodud IGMPv2 teate formaat, millel on järgmised väljad:

- tüüp – IGMPv2 korral kasutatakse nelja tüüpi teateid:
 - liikmelisuse päring (kood 0x11) – liikmelisuse päringul on 2 alamtüüpi:
 - üldine päring – kasutatakse aktiivsete multisaate gruppide teada saamiseks nagu IGMPv1 korralgi. Grupi aadressi väli on nullitud;
 - grupi-spetsiifiline päring – et teada saada kas konkreetsel multisaate

grupil on aktiivseid liikmeid. Grupi aadressi väljal on päritava grupi aadress;

- versioon 1 liikmelisuse raport (kood 0x12) – tagasiühilduvuse tagamiseks IGMPv1 protokolliga;
- versioon 2 liikmelisuse raport (kood 0x16);
- grupist lahkumine (kood 0x17);
- maksimaalne vastamise aeg – kasutatakse ainult liikmelisuse päringu teadetes ja määrab maksimaalse lubatud aja (1/10 sekundit), mil host võib päringule vastata. Vaikeväärtuseks on 100 (10 sekundit). Teistes teadetes on väli nullitud ja ignoreeritakse vastuvõtjate poolt;
- kontrollsumma – 16 bitine kontrollsumma;
- grupi aadress – üldiste päringute korral on väli nullitud. Grupi-spetsiifiliste päringute, liikmelisuse raportite ja grupist lahkumise teadete korral sisaldab vastava grupi aadressi.

4.2.1 Päring-vastuse häälestamine

Selle asemel, et hostides päring-vastus intervall staatiliselt kirjeldada, lisati IGMPv2 päringutele lisaväli: “maksimaalne vastamise aeg”. Seega saame seda parameetrit kirjeldada IGMP pärijas, mis omakorda teavitab sellest hoste.

Maksimaalse vastamise aja häälestamine aitab kontrollida vastamise protsessi puhangulisust. See omadus on tähtis siis, kui meie võrgus on palju aktiivseid multisaate gruppe ja me soovime hajutada vastuseid pikemale ajaperioodile. Vastuste hajutamine saavutatakse sellega, et hostid valivad raport-timeri väärtuse suvaliselt vahemikust 0 kuni maksimaalne vastamise aeg.

Vastuste puhangu vähendamisel on ka halb külg. Kui me suurendame maksimaalset vastamise aega, siis me suurendame sellega ka grupist lahkumise latentsust, sest pärija marsruuter peab nüüd kauem ootama veendumaks, et ei ole jäänud ühtegi hosti multisaate gruppi.

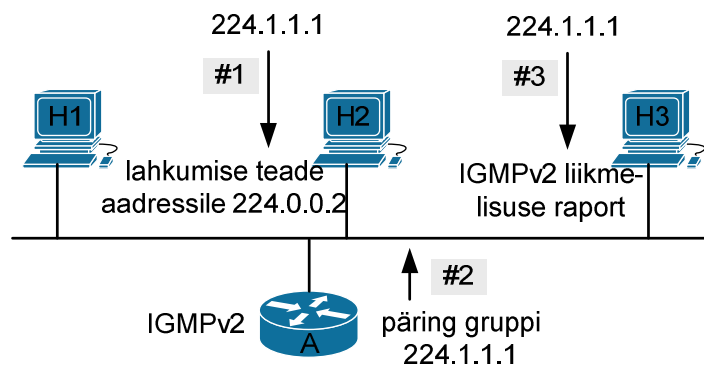
4.2.2 IGMPv2 grupi-spetsiifilised päringud

Grupi-spetsiifilised päringud võimaldavad marsruuteril pärida kõikide multisaate gruppide asemel ühte konkreetset gruppi. Selleks kasutatakse väljal “Grupi aadress” päritava grupi aadressi. IGMPv2 hostid vastavad nendele päringutele samamoodi nagu üldistele päringutele. Grupi-spetsiifilised päringud vähendavad veelgi grupist lahkumise latentsust, kasutades palju väiksemat maksimaalset vastamise aega (vaikimisi 1 sekund).

4.2.3 IGMPv2 grupist lahkumise protsess

IGMPv2 grupist lahkumise ja grupi-spetsiifilised teated, kombineerituna maksimaalse

vastamise ajaga, võimaldavad vähendada grupist lahkumise latentsuse vaid mõne sekundini. Tuletan meelde, et IGMPv1 puhul oli see halvimal juhul 3 minutit. Joonisel 4-5 on kujutatud IGMPv2 grupist lahkumise protsess.

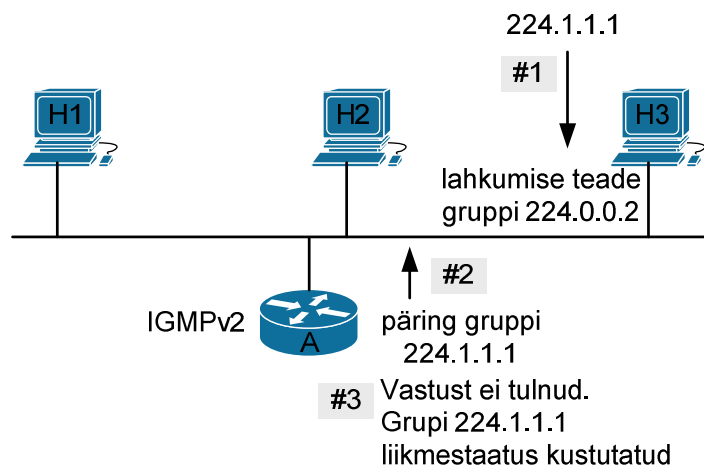


Joonis 4-5. IGMPv2 lahkumise protsess – H2 lahkub [5].

Hetkel on H2 ja H3 multisaate grupi 224.1.1.1 liikmed. Hosti H2 grupist lahkumise sündmused on järgmised:

- 1) H2 multiedastab IGMPv2 grupist lahkumise teate “kõik marsruuterid” grupile (224.0.0.2), et teavitada kõiki alamvõrgu marsruutereid oma lahkumisest;
- 2) marsruuter A (eeldades, et ta on IGMP pärija marsruuter) kuuleb H2 grupist lahkumise teadet. Kuna marsruuterid hoiavad endas ainult aktiivsete multisaate gruppide nimekirja, mitte individuaalseid liikmeksolevaid hoste, siis marsruuter A saadab grupi-spetsiifilise päringu veendumaks kas on veel mõni host jäänud gruppi 224.1.1.1. Kuna grupi-spetsiifiline päring saadetakse otse vastavale grupile, siis vastavad ainult hostid, mis asuvad grupis 224.1.1.1;
- 3) H3 on endiselt grupi 224.1.1.1 liige ja seega kuuleb grupi-spetsiifilist päringut ning vastab sellele IGMPv2 liikmelisuse raportiga.

Nüüd on host H3 ainuke grupi 224.1.1.1 liige. Oletame, et ka H3 tahab grupist lahkuda, nagu näidatud joonisel 4-6.



Joonis 4-6. IGMPv2 lahkumine - H3 lahkub [5].

Toimuvad järgmised sündmused:

- 1) H3 multiedastab IGMPv2 grupist lahkumise teate “kõik marsruuterid” grupile (224.0.0.2), et teavitada kõiki alamvõrgu marsruutereid oma lahkumisest;
- 2) seda kuuleb jällegi marsruuter A ja saadab grupi-spetsiifilise päringu vastavasse gruppi selgitamiseks kas on jäänud mõni liige gruppi 224.1.1.1;
- 3) kuna gruppi 224.1.1.1 ei ole jäänud ühtegi liiget, siis grupi-spetsiifilisele päringule ei vasta ükski host. Marsruuter A ootab “viimase liikme päringu intervalli” (vaikimisi 1 sekund) ja saadab veel ühe grupi-spetsiifilise päringu, millele ikka ei vastata (vaikimisi esitatakse päringut kaks korda). Seekord grupp aegub ja marsruuter lõpetab multisaate edastamise vastavasse alamvõrku.

4.2.4 Pärija valimine

Pärija valimine ei sõltu enam OSI mudeli ülemiste kihtide protokollidest, vaid IGMPv2 kasutab selleks üldise päringu teadetes IP aadressi. Protsess on selline:

- 1) kui IGMPv2 marsruuter käivitub, siis ta multiedastab IGMPv2 üldise päringu grupile “kõik multisaate hostid” (224.0.0.1), pannes teate lähteadressi väljale oma liidese IP aadressi;
- 2) kui IGMPv2 marsruuter saab üldise päringu kätte, siis ta võrdleb selle lähteadressi oma liidese aadressiga. Madalaima IP aadressiga marsruuter võrgusegmenendis valitakse IGMP pärijaks;
- 3) kõik mittepärijad marsruuterid käivitavad pärija-timeri, mis algväärtustatakse iga üldise päringu saamisel IGMP pärijalt. Vaikimisi pannakse selle timeri algväärtuseks kahekordne pärimisintervall või 250 sekundit. Pärija-timeri aegumisel oletatakse, et IGMP pärija on maas ja tehakse uus valimisprotsess.

4.3 IGMPv3

IGMPv3 on järgmiseks sammuks IGMP protokollide arengus. IGMPv3 lisab „allika filtreerimise“ omaduse. Multisaate vastuvõtja saab öelda ruuterile, milliste gruppide liiklust ja ainult konkreetse(te) allika(te) või kõikide allikate välja arvatud teatud allika(te) liiklust ta soovib saada. IGMPv3 ei ole veel standardiseeritud, spetsifikatsiooniga saate lähemalt tutvuda RFC-st 3376, kuid selle toetus on olemas pea kõigis tänapäeva operatsioonisüsteemides. Rakenduste programmeerijad peaksid juhinduma IGMPv3 API-liidestest.

IGMPv3 protokoll kasutab kahte tüüpi teateid:

- 1) liikmelisuse päring – tüübi kood 0x11;
- 2) liikmelisuse raport – tüübi kood 0x22.

Tagasiühilduvuse tagamiseks varasemate IGMP versioonidega toetatakse ka:

- 1) IGMPv1 liikmelisuse raport – tüübi kood 0x12;
- 2) IGMPv2 liikmelisuse raport – tüübi kood 0x16;
- 3) IGMPv2 grupist lahkumise teade – tüübi kood 0x17.

IGMPv3 vastuvõtjad ei saada enam liikmelisuse raporteid vastavatesse multisaate gruppidesse, mille liikmed nad on, vaid saadavad liikmelisuse raporti „kõik IGMPv3 marsruuterid“ aadressile 224.0.0.22. Ruuterid kuuluvad seda aadressi ja haldavad liikmelisuse staatust iga liikme kohta võrgusegmentis. Varasemates IGMP versioonides hallati liikmelisuse staatust võrgusegmentide kaupa. Hostid ise ei kuula 224.0.0.22 aadressi ja seega ei kuule teiste hostide liikmelisuse raporteid. Neil põhjustel ei kasuta IGMPv3 enam raporti tagasihoidmise mehhanismi. Et ära hoida IGMP raportite suurt tulva, on vastamise intervalli võimalik tuunida palju suuremas vahemikus kui varem.

Ruuterid saadavad välja liikmelisuse päringuid, et teada saada, milliste multisaate aadresside vastu huvi on võrgusegmentis. Perioodiliselt saadetakse välja (aadressile 224.0.0.1) üldisi päringuid värskendamaks multisaate gruppide liikmelisuste olekuid. Grupi-spetsiifilise päringuga teeb ruuter kindlaks huvi konkreetse grupi vastu ja grupi- ja allika-spetsiifilise päringuga teeb ruuter kindlaks huvi konkreetse allika edastusest vastavasse gruppi. Viimased kaks päringutüüpi saadetakse vastava grupi multisaate aadressile.

0	7	15	31
Tüüp		Max vastamise kood	Kontrollsumma
Grupi aadress			
	S	QRV	QQIC
Allikate arv (N)			
Allika aadress [1]			
Allika aadress [2]			
.			
.			
Allika aadress [N]			

Joonis 4-7. IGMPv3 päringu teate formaat [10].

Joonisel 4-7 on toodud IGMPv3 päringu teate formaat, millel on järgmised väljad:

- tüüp – tüübi kood päringu puhul 0x11;
- maksimaalne vastamise kood – maksimaalne lubatud aeg raportiga vastamiseks (1/10 s), kui väärtus on < 128, siis max vastamise aeg = max vastamise kood, kui väärtus > 128, siis väljendatakse ujukomaarvuna valemiga:

```

0 1 2 3 4 5 6 7
+-----+
|1| exp | mant |
+-----+
```

$$\text{Max vastamise aeg} = (\text{mant} | 0x10) \ll (\text{exp} + 3);$$

- grupi aadress – päritava grupi multisaate aadress grupi-spetsiifilise ning grupi- ja

- allika-spetsiifilise päringu korral, üldise päringu korral 0.0.0.0;
- lipp S – kui lipp püsti, siis ruuterid ei pea seda teadet menetlema;
- QRV – võrgu kvaliteeti näitav muutuja, mis aitab hostidel sättida taimerite ja korduste saatmise parameetreid;
- QQIC – kood, mis iseloomustab pärija pärimisintervalli sekundites, kui väärtus on <128, siis kood = intervall, vastasel juhul arvutatakse intervall sama valemiga, mida kasutatakse maksimaalse vastamise aja arvutamiseks;
- allikate arv (N) – päringus olevate allikate arv, üldise ja grupi-spetsiifilise päringu korral 0.

Järgneval joonisel 4-8 on toodud IGMPv3 raporti formaat.

0	7	15	31
Tüüp	Reserveeritud	Kontrollsumma	
Reserveeritud		Grupi kirjete arv (M)	
Grupi kirje [1]			
Grupi kirje [2]			
.			
.			
Grupi kirje [M]			

Joonis 4-8. IGMPv3 liikmelisuse raporti formaat [10].

IGMPv3 raportil on järgmised väljad:

- tüüp – kood raporti puhul on 0x22;
- reserveeritud – väljad nullitakse saatmisel ja vastuvõtmisel ignoreeritakse;
- grupi kirjete arv (M) – raportis olevate grupi kirjete arv.

Igal ülaltoodud grupi kirjel on järgmine formaat (näidatud joonisel 4-9):

0	7	15	31
Kirje tüüp	Lisaandmete pikkus	Allikate arv (N)	
Grupi aadress			
Allika aadress [1]			
Allika aadress [2]			
.			
.			
Allika aadress [N]			
Lisaandmed			

Joonis 4-9. Raporti sisese grupi kirje formaat [10].

- kirje tüüp – mitu erinevat tüüpi, kirjeldatud allpool koos vastava välja väärtusega;

- lisaandmete pikkus – grupi kohta käiva lisainfo suurus, praeguses spetsifikatsioonis lisaandmeid ei kasutata (mõeldud tuleviku jaoks) ja seega on väli saatmisel nullitud ning vastuvõtmisel ignoreeritakse;
- allikate arv (N) – näitab mitu allika aadressi on grupi kirjes.

Liikmelisuse raporti erinevad grupi kirjete tüübid (kus järjekorra number vastab kirje tüübi välja väärtusele):

- „hetke seisu kirje“ saadetakse vastuseks päringutele. See iseloomustab multisaate aadressile vastavat vastuvõtu olekut liidese peal ja neid olekuid on kaks:
 - 1) *INCLUDE* – filtri laad on kaasa arvav ehk vastava grupi kirjes olevate allikate liiklust soovitakse saada. Kui allikate list on tühi, siis lahkutakse vastavast multisaate grupist;
 - 2) *EXCLUDE* – filtri laad on välistav ehk vastava grupi kirjes olevate allikate liiklust ei soovita, aga ülejäänud allikate liiklust soovitakse. Kui allikate list on tühi, siis liitatakse multisaate grupiga ja võetakse vastu kõikide allikate liiklus nagu IGMPv2 puhul;
- „filtri laadi muutmise kirje“ saadetakse vastavast liidesest välja siis, kui multisaate rakenduse funktsioon *IPMulticastListen* põhjustab mingis multisaate grupis filtri laadi muudatuse (näiteks üleminek *INCLUDE* laadilt *EXCLUDE* laadile või vastupidi). „Filtri laadi muutmise kirjel“ on kaks väärtust:
 - 3) *CHANGE_TO_INCLUDE_MODE* – liidese filtri laad muudeti kaasa arvavaks antud multisaate grupis. Grupi kirje allikate aadressid on selle liidese uueks allikate listiks;
 - 4) *CHANGE_TO_EXCLUDE_MODE* – liidese filtri laad muudeti välistavaks antud multisaate grupis. Grupi kirje allikate aadressid on selle liidese uueks välistatud allikate listiks;
- „allikate listi muutmise kirje“ saadetakse vastavast liidesest välja siis, kui multisaate rakenduse funktsioon *IPMulticastListen* põhjustab mingis multisaate grupis allikate listi muudatuse ja filtri laadi ei muudeta. Raport saadetakse välja liideselt, mil muudatus toimus ning „allikate listi muutmise kirjel“ on kaks väärtust:
 - 5) *ALLOW_NEW_SOURCES* – grupi kirjes on lisa allikate aadressid, mille liiklust soovitakse vastu võtta. Kui muudatus tehakse *INCLUDE* laadi allikate listile, siis need aadressid lisatakse allikate listi ja kui muudatus tehakse *EXCLUDE* laadi allikate listile, siis need uued aadressid kustutatakse allikate listist;
 - 6) *BLOCK_OLD_SOURCES* - grupi kirjes on allikate aadressid, mille liiklust ei soovita enam vastu võtta. Kui muudatus tehakse *INCLUDE* laadi allikate listile, siis need aadressid kustutatakse allikate listist ja kui muudatus tehakse *EXCLUDE* laadi allikate listile, siis need uued aadressid lisatakse listi.

Kui allikate listi muudetakse uute allikate lisamisega ja teatud vanade allikate eemaldamisega, siis saadetakse multisaate gruppi kaks viimasena toodud grupi kirje tüüpi.

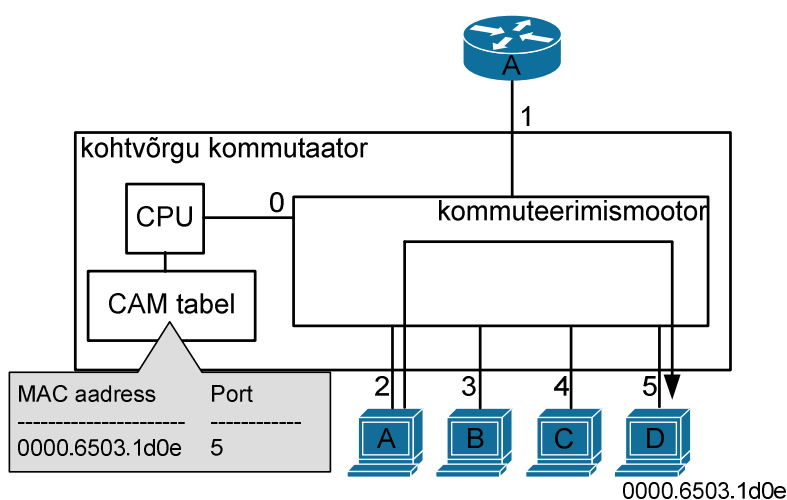
IGMPv3 leiab põhiliselt rakendust allika-spetsiifilise multiedastusprotokolli SSM puhul, millest tuleb hiljem juttu.

5 Multiedastus kommuteeritud võrgus

Teatavasti edastab kommutaator kaadreid sihtkoha MAC aadresside põhjal otsides vastava MAC aadressi üles oma edastustabelist, kus on kirjas edastamiseks kasutatav port. Edastustabelit täidetakse dünaamiliselt töötamise käigus saadavate kaadrite lähtekoha MAC aadressi ning siseneva pordi põhjal. Esimesed kommutaatorid kasutasid kommuteerimiseks keskprotsessorit. Kui protsessor sai kaadri ühest pordist, siis ta avas kaadri sihtkoha MAC aadressi, otsis selle oma edastustabelis üles ja edastas kaadri vastavas kirjes viidatud porti. Selle protsessi kiirendamiseks hakati edastustabelit hoidma spetsiaalses assotsiatiivmälus CAM (*Content Addressable Memory*), kus MAC aadressi kasutati viidana soovitud kirjeni.

Kuna nõudlus kommutaatorite suurema jõudluse järele pidevalt kasvas, siis vabastati protsessor kommuteerimisloogikast ja see funktsioon anti spetsiaalsele kommuteerimismootorile (*Switching Engine*), mis kasutas CAM tabelit ja edastas kaadreid sisenevast pordist väljuvasse porti „juhtmekiirusel“ (*wirespeed*). Sellise kiiruse saavutamiseks põhines kommuteerimismootor spetsiaalsel signaalprotsessoril ASIC (*Application-Specific Integrated Circuit*), mis võttis kaadri MAC aadressi (OSI mudeli 2. kihi info), otsis selle üles CAM tabelist ja edastas selle tabelis viidatud porti. Kuna ASIC protsessorite loogika signaliseering toimub ränis, siis see võimaldabki kaadrite kommuteerimist „juhtmekiirusel“.

Järgmisel joonisel 5-1 on toodud tüüpilise kohtvõrgu kommutaatori lihtsustatud plokkskeem.



Joonis 5-1. Kohtvõrgu kommutaatori arhitektuur [5].

Kommutaatori mikroprotsessor tegeleb haldusfunktsioonidega ja täidab CAM tabelit hostide MAC aadresside ja neile vastavate pordi numbritega. See protsessor on ühenduses kommuteerimismootori pordiga, mis on nagu iga teinegi kommutaatori port. Nii on võimalik kommutaatorile adresseeritud kaadrite edastamine protsessorile töötlemiseks (näiteks SNMP protokoll, telnet, ssh).

Kui kommutaator saab kaadri, mille sihtaadressi ei ole tema edastustabelis, siis ta saadab selle kaadri edasi kõikidesse teistesse portidesse. Tavaliselt juhtub see järgmistes situatsioonides:

- sihtkoha MAC aadress ei ole veel tuntud;
- sihtkoha MAC aadress on levisaate või multisaate aadress.

Esimene situatsioon ei ole probleemiks, sest niipea kui sihtkoht saadab vastu mõne kaadri, salvestab kommutaator vastava MAC aadressi oma CAM tabelisse. Sellest hetkest saadab kommutaator vastavasse sihtkohta kaadrid otse.

Teise situatsiooni korral tuleb levisaate kaadreid alati saata kõikidesse portidesse (va sissetulev port). Samamoodi on multisaatega: kommutaator ei tea milliste portide taga on multisaate vastuvõtjad.

Kuna kommuteeritud võrgud on muutunud väga populaarseks, siis on mõeldud välja ka mõned meetodid levisaate/multisaate ülejutamiste vastu. Üheks võimaluseks on ruuteris levisaate/multisaate osamäära piiramine (*rate limiting*). Idee seisneb piirangu kehtestamises, kui palju ribalaiusest võib tarbida levisaate/multisaate liiklus enne kui kaadreid hakatakse ära viskama. Vastav piiramise korraldus antakse Cisco marsruuterites liidese konfiguratsioonile:

```
ip multicast rate-limit in | out {[video] | [whiteboard]} [group-  
list <acl>] [source-list <acl>] [<kbps>],
```

kus valikulisi parameetreid on palju. Näiteks “video” ja “whiteboard” valikutega saame ainult vastavate voogude piirmäära kehtestada. Valikutega “group-list” ja “source-list” saame määrata, millistele gruppidele ja/või allikatele me piirmäära kehtestame, kuid parameetri ära jätmisel kehtestame piirmäära kogu liidest läbivale multiedastusele. Kui piirmäära (ühikutes Kbit/s) lõppu ei lisata, siis vaikeväärtuseks on “0”, mis tähendab et antud grupi või allikate multiedastuse paketid visatakse minema.

Kuid selgus, et selline suvaline teatud levisaate kaadrite ära viskamine põhjustab ebastabiilsusi, mis mõningatel juhtudel võib võrgu lausa katki teha. Üheks näiteks on sillaprotokolli andmeüksuste BPDU (*Bridge Protocol Data Unit*) kaadrid spetsiaalsele “kõik sillad” multisaate MAC aadressile. Kui neid kaadreid hakatakse ära viskama, võib võrk muutuda ebastabiilseks, sest täispuu protokoll STP (*Spanning Tree*) üritab pidevalt konvergeeruda ning siis võib omakorda BPDU kaadreid kaduma minna, mis lõpuks võib

tähendada võrgu mitte töötamist. OSPF „hello“ teated, mida multiedastatakse “kõik OSPF marsruuterid” multisaate MAC aadressile, on teiseks kriitiliste kaadrite näiteks. Kui neid kaadreid piisavalt palju ära kaotada, siis marsruuterid kaotavad OSPF mõttes külgnevuse ja see põhjustab ebastabiilsusi marsruutimises.

Ka mõnede tootjate kommutaatorites (näiteks Cisco) on võimalik kehtestada võrguressursi kasutamise piirangud (protsentides, bitti/s, paketti/s) nii üksikedastuse, leviedastuse kui ka multiedastuse liiklusele liidesele antava käsuga:

```
storm-control {broadcast | multicast | unicast} level <piirang>.
```

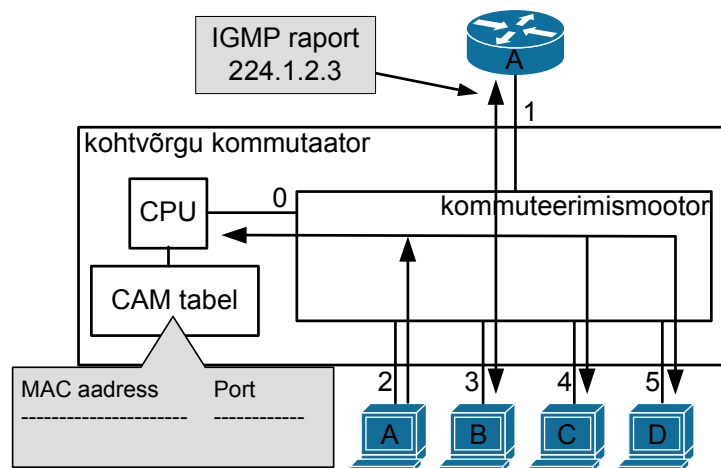
Piirmäära ületamisel pannakse vastav kommutaatori port kinni või saadetakse SNMP lõks, nii kuidas administraator soovib.

Veel üheks lahenduseks oleks käsitsi siduda multisaate MAC aadressid nende kommutaatori portidega, kus on vastuvõtjad. See lahendus töötab hästi, kuid ei ole mastabeeritav ja nõuab võrguadministraatorilt pidevat häälestamist. Seepärast on kommutaatorite edastustabelite dünaamiline häälestamine parem idee.

5.1 IGMP pealt kuulamine

Nagu nimigi ütleb, muutuvad kommutaatorid IGMP teadlikuks ja kuulavad hostide ja marsruuterite vahelist IGMP-suhtlust pealt. Kui kommutaator kuuleb hosti poolt saadetud IGMP liikmelisuse raportit mingile multisaate grupile, siis ta lisab hosti vastava pordi numbri vastava multisaate aadressi CAM tabeli kirjele. Kui kommutaator kuuleb hosti poolt saadetud IGMP grupist lahkumise teadet, siis vastav port eemaldatakse CAM tabelist.

Pealtnäha tundub olevat lihtne lahendus, kuid probleem on selles, et erinevate tootjate kommutaatorid käituvad erinevalt ja paljud odavamad kommutaatorid ei olegi IGMP teadlikud, mis võib põhjustada nende ülekoormuse. Järgnevalt vaatlemegi kuidas IGMP töötab erinevatel kommutaatoritel.



Joonis 5-2. Grupiga liitumine IGMP puhul [5].

Joonisel 5-2 on näide lihtsast L2 kommutaatorist (puudub spetsiaalne L3 riistvara), milles on käivitatud IGMP pealt kuulamine. Vaatleme, mis tavaliselt juhtub, kui leiduvad mõned multisaate grupiga liitujad:

- host A tahab liituda multisaate grupiga 224.1.2.3 ja multiedastab vastavasse gruppi MAC aadressiga 0x0100.5e01.0203 IGMP liikmelisuse raporti. Kuna algselt sellele multisaate MAC aadressile vastavaid kirjeid CAM tabelis ei ole, siis raport edastatakse kõikidesse kommutaatori portidesse (kaasa arvatud sisemisse porti, mis on ühenduses kommutaatori CPU-ga);
- kui CPU saab host A poolt saadetud IGMP raporti, siis ta kasutab selle informatsiooni ja tekitab CAM tabelisse kirje 0x0100.5e01.0203, mis on seotud host A pordiga 2, marsruuteri pordiga 1 ja kommutaatori CPU pordiga 0. Kommutaatori CPU peab ka edaspidi saama neid kaadreid, sest ta peab jälgima teisi sellele MAC aadressile adresseeritud IGMP teateid.

Tabel 5-1. CAM tabeli kirje pärast host A liitumist.

Sihtaadress	Pordid
0100.5e01.0203	0, 1, 2

Selle CAM tabeli kirje (tabelis 5-1) tulemusena on edaspidised multisaate kaadrid aadressiga 0x0100.5e01.0203 piiratud portidega 0, 1 ja 2 ning neid ei üleujutata kommutaatori teistesse portidesse.

Oletame nüüd, et ka host D tahab liituda sama grupiga ja saadab vastava IGMP liikmelisuse raporti. Vastavalt CAM tabeli kirjele tabelis 5-1, saadab kommutaator IGMP liikmelisuse raporti edasi välimistesse portidesse 1 ja 2. Kuna ka CPU-le edastatakse vastav raport, siis ta lisab pordi, millest raport saadi (antud juhul port 5), MAC aadressile 0x0100.5e01.0203 vastavale kirjele. Selle tulemusena saadakse tabelis 5-2 näidatud CAM tabel.

Tabel 5-2. CAM tabeli kirje pärast host D liitumist.

Sihtaadress	Pordid
0100.5e01.0203	0, 1, 2, 5

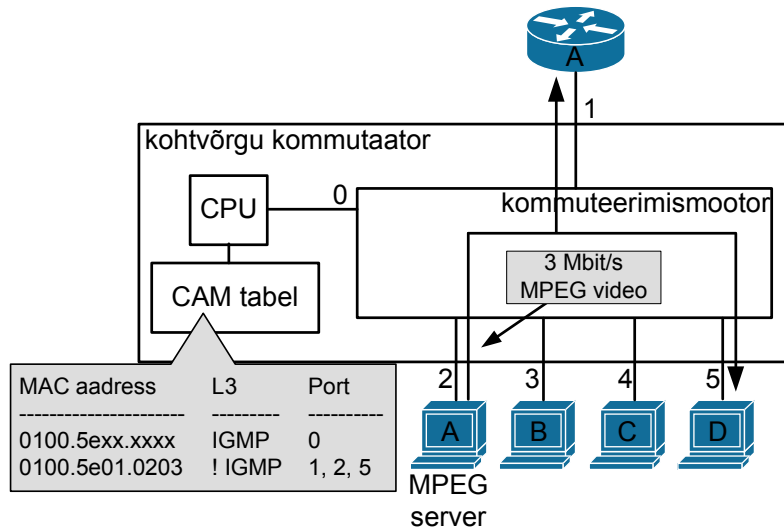
Nüüdest saadetakse kogu MAC aadressile 0x0100.5e01.0203 (mis vastab grupile 224.1.2.3) suunatud multisaate liiklus ainult hostidele A, D, marsruuterile ja kommutaatori CPU-le. Nagu näha, töötab liitumise protsess suurepäraselt. Kuid järgnevas lõigus räägime tõsisest probleemist, mis tekib siis, kui kasutada tavalist L2 kommutaatorit.

5.1.2 IGMP pealt kuulamise mõju jõudlusele

Eelnevalt jõudsimme tulemuseni, et ka CPU sisemine port on seotud multisaate gruppide MAC aadressiga nagu näidatud tabelis 5-1 ja 5-2. Võttes aluseks eelnevalt vaadeldud kommutaatori näite, oletame nüüd, et host A hakkab edastama 3 Mbit/s MPEG videovoogu multisaate grupile 224.1.2.3. See tähendab, et video kaadrite sihtkoha MAC aadressiks on samuti 0x0100.5e01.0203 ja seega edastatakse need muu hulgas ka kommutaatori CPU-le.

Kõikide kommutaatorit läbivate multisaate kaadrite läbivaatamine CPU poolt, selleks et leida IGMP pakette, põhjustab kommutaatori ülekoormuse ja mõnikord lausa kokkujooksu. Paraku kannatavad selle probleemi all enamuse madala hinnaga L2-taseme kommutaatorid, mis implementeerivad IGMP pealt kuulamist. Kommutaator võib isegi töötada lihtsamates ja vähemkoormatud võrkudes, kuid suurema koormuse all võib esineda nii multisaate kui üksiksaate pakettide aegajalist kadu. Teinekord aga jätkab kommuteerimismootor multisaate ja üksiksaate edastamist ilma kadudeta, kuid kaod tekivad pakettide edastamisel sisemisele CPU-le. See põhjustab IGMP pakettide vahele jäämisi, mis omakorda mõjutab grupiga liitumise ja lahkumise latentsust.

Ülaltoodud probleemide vältimiseks on vajalik, et kommutaatorites kasutataks selliseid ASIC protsessoreid ja CAM tabelleid, mis uurivad kaadreid sügavamalt ehk OSI mudeli L3 informatsiooni enne kaadrite edastamist. Kui kommutaator on sellise arhitektuuriga, siis on võimalik programmeerida CAM tabel, mis edastab CPU-le ainult IGMP teateid sisaldavaid kaadreid. Järgneval joonisel on lihtsustatult kujutatud uue L3 teadliku kommutaatori plokk skeem.



Joonis 5-3. L3 teadliku kommutaatori arhitektuur [5].

Kuna kommutaator on L3 teadlik, siis CAM tabeli kirjetel on nüüd lisaväli L3 informatsiooniga, mis mõjutab kommuteerimismootori käitumist. Joonisel 5-3 toodud CAM tabeli esimene kirje käsib kommuteerimismootoril edastada IGMP paketid ainult kommutaatori CPU-le. Teine kirje käsib edastada multisaate MAC aadressile 0x0100.5e01.0203 adresseeritud kaadrid, mis ei ole IGMP paketid, marsruuterile ja kahele grupiga liitunud hostile. Seega 3 Mbit/s videovoog ei katkesta enam CPU tööd ja talle edastatakse vaid mõned üksikud IGMP teated sekundis, millega CPU saab vabalt hakkama.

Uemates Cisco kommutaatorites on IGMP pealt kuulamine vaikimisi sisse lülitatud, aga seda saab ka vajadusel ise teha globaalse režiimi käsuga:

```
ip igmp snooping.
```

IGMP pealt kuulamise käivitust saame kontrollida käsuga:

```
show ip igmp snooping.
```

Pealt kuulamisega teada saadud multisaate gruppe (ning vastavaid edastusporte) saame vaadata korraldusega:

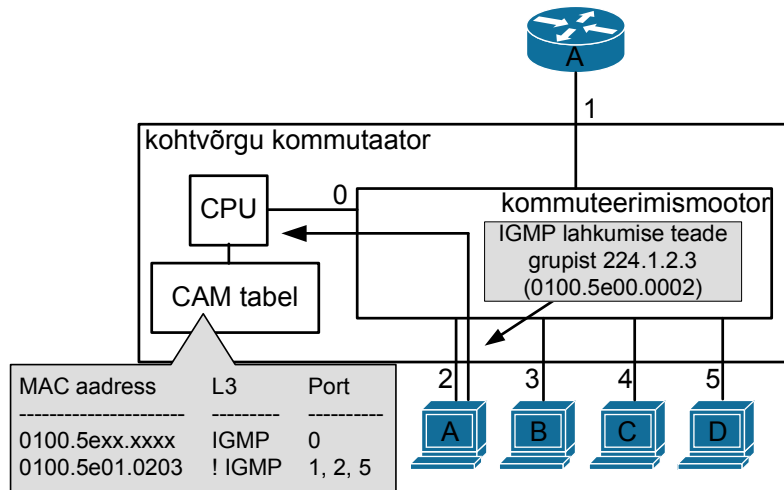
```
show ip igmp snooping groups.
```

Hosti liitumine grupiga L3 teadlikus kommutaatoris toimub sisuliselt samamoodi nagu lihtsas L2 kommutaatoris. Järgnevates lõikudes eeldame, et tegu on L3 teadliku kommutaatoriga.

5.1.3 Lahkumine grupist IGMP pealt kuulamisel

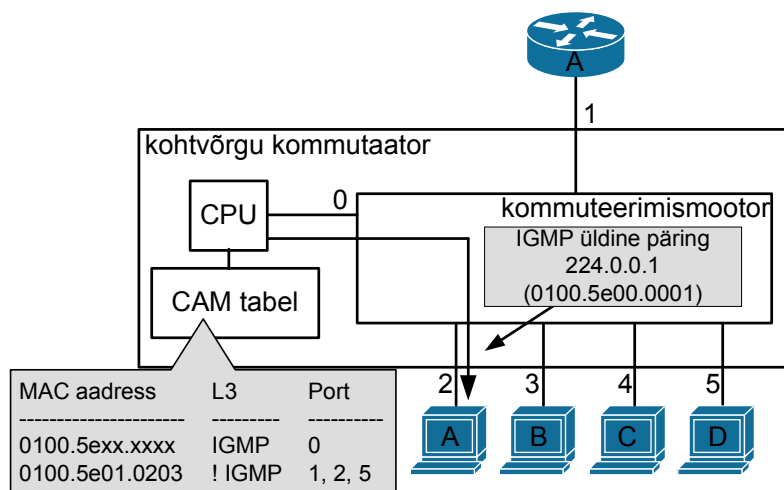
Oletame, et host A lahkub grupist. Toimuvad järgmised sündmused:

- 1) host A multiedastab grupist lahkumise teate "kõik marsruuterid" aadressile 224.0.0.2 (MAC aadress 0x0100.5e00.0002) nagu näidatud joonisel 5-4. Vastavalt kommutaatori CAM tabelile saadetakse see teade ainult CPU-le ja mitte ühtegi teise porti;



Joonis 5-4. IGMP korral grupist lahkumise samm 1 [5].

- 2) vastuseks lahkumise teatele saadab CPU IGMP üldise päringu porti 2 (joonis 5-5), et näha kas selles pordis on veel mõni antud grupi liige (tavaliselt juhtub see siis, kui mitu hosti on ühendatud kommutaatori porti jaoturi abil);



Joonis 5-5. IGMP korral grupist lahkumise samm 2 [5].

- 3) kui pordist 2 saadakse veel mõni IGMP raport, siis CPU lihtsalt heidab varem

saadud grupist lahkumise teate kõrvale. Kui pordist 2 IGMP raportit vastuseks ei saada, siis CPU kustutab vastava pordi oma CAM tabeli kirjes (tulemuseks saadakse tabelis 5-3 näidatud CAM tabel). Kuna CAM tabeli kirjes on veel mõni mitte-marsruuteri port, siis marsruuterile mingeid teateid ei saadeta;

Tabel 5-3. CAM tabel pärast host A lahkumist.

Sihtaadress	L3	Pordid
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 5

- 4) oletame nüüd, et ka host D lahkub grupist ja saadab vastava teate. Jällegi saadetakse see teade edasi ainult kommutaatori CPU-le;
- 5) vastuseks grupist lahkumise teatele saadab CPU IGMP üldise päringu porti 5, et näha kas selles pordis on veel mõni antud grupi liige;
- 6) kuna meie näites ei ole selles pordis rohkem hoste, siis IGMP raportit sellele grupile vastuseks ei saada ja kommutaator kustutab selle pordi oma CAM tabeli kirjes. Kuna see oli viimane mitte-marsruuteri port, siis kommutaator kustutab selle grupi CAM tabeli kirjed ja saadab pordist 1 välja IGMP grupist lahkumise teate marsruuterile.

5.1.4 Grupi haldamine IGMP pealt kuulamisega

Eelnevalt kirjeldatud grupist lahkumise protsess eeldab, et hostid alati saadavad grupist lahkumise teate. IGMPv3 puhul seda ka alati tehakse, kuid IGMPv2 spetsifikatsioon (RFC 2236) ütleb, et host võib (ei ole kohustuslik) saata grupist lahkumise teate. Tänapäeval sellega enam väga palju probleeme ei ole, kuid võib siiski juhtuda, et mõni host kasutab IGMPv1 (mis ei kasuta üldse grupist lahkumise teavitamise süsteemi) või läheb grupist lahkumise teade kommutaatori ülekoormuse tõttu kaduma. Selle probleemi lahendab üldise päringu-vastuse mehhanism.

Oletame, et host A ja D on eelnevalt liitunud multisaate grupiga 224.1.2.3 ning seega on kommutaatori CAM tabel selline nagu näidatud tabelis 5-4.

Tabel 5-4. CAM tabel, kui liikmeteks on host A ja D.

Sihtaadress	L3	Pordid
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2, 5

Siis toimuvad üldise päringu-vastuse mehhanismi käigus sellised sündmused:

- 1) marsruuter A saadab perioodiliselt üldise päringu "kõik hostid" multisaate grupile 224.0.0.1 (MAC aadress 0x0100.5e00.0001). Kommutaatori CPU näeb seda üldist päringut ja saadab selle oma kõikidesse portidesse edasi;
- 2) iga host vastab liikmelisuse raportiga gruppidesse, mille liige ta on. Kuna

kommutaatori CPU püüab kinni kõik IGMP teated, siis hostid ei kuule teineteise IGMP raporteid. See on vajalik selleks, et hostid ei kasutaks raporti tagasihoidmise mehhanismi ja kommutaator saaks teada kõik pordid, milles asuvad multisaate grupi liikmed;

- 3) kommutaator peab saatma ühe või mitu (tavaliselt ühe) IGMP raportitest edasi marsruuterile, et hoida elus IGMP grupi liikmelisuse staatust.

5.1.5 IGMP pealt kuulamine ja ainult-saatvad allikad

Multisaate allikad ei pea eelnevalt grupiga liituma, kui nad sinna infot saadavad ja seega ei pea nad saatma IGMP raportit. See tekitab probleeme kommutaatorites, mis kasutavad IGMP pealt kuulamist multisaate piiramiseks.

Oletame, et host A on ainult multisaate allikas ja ta on hakanud edastama 3 Mbit/s MPEG videovoogu multisaate gruppi 224.1.2.3 ilma IGMP liikmelisuse raportit saatmata. Oletame ka seda, et ükski host ei ole selle multisaate grupiga liitunud. Seega kommutaatori CAM tabel on selline nagu näidatud tabelis 5-5.

Tabel 5-5. CAM tabel ilma ühegi liikmeta.

Sihtaadress	L3	Pordid
0100.5exx.xxxx	IGMP	0

Odavamatel kommutaatoritel tekib selle olukorraga toimetulemisel probleeme. Sageli kommutaatori disainerid lihtsalt lubavad ainult-saatvate allikate liiklusega võrgu üleujutamise kõikidesse portidesse kuni mõni kommutaatori küljes olev host saadab IGMP liikmelisuse raporti. Ka CPU peab valimatult kuulama kõiki multisaate kaadreid, mis tekitab ülekoormuse.

Seevastu L3 teadlik kommutaator tuvastab vastava multisaate liikluse koheselt ja uuendab oma CAM tabeli kirjeid (tabel 5-6) nii, et allikast tulev multisaate voog edastatakse ainult marsruuterite portidesse.

Tabel 5-6. CAM tabel ainult-saatva allikaga.

Sihtaadress	L3	Pordid
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1

5.1.6 Marsruuterite tuvastamine IGMP pealt kuulamisega

Eelnevates näidetes oli marsruuteriga A ühendatud port automaatselt lisatud aadressile 0x0100.5e01.0203 vastavasse CAM tabeli kirjesse, sest marsruuterid peavad valimatult saama kõikide gruppide multisaadete liikluse. Tekib küsimus: kuidas kommutaator teadis lisada porti 1 CAM tabeli kirje 0x0100.5e01.0203 portide nimekirja? Ilmne vastus oleks,

et kommutaator kuulis eelmist IGMP üldist päringut marsruuterilt A ja jättis pordi meelde. Kui port peaks maha minema või kui kommutaatoril ei õnnestu kuulda IGMP üldiseid päringuid selles pordis, siis kommutaator oletab, et marsruuter ei ole enam ühendatud sellesse porti. Paraku selline tehnika ei ole piisavalt kindel.

Kui meil on näiteks mitu marsruuterit ühendatud kommutaatoriga, siis ainult üks nendest käitub IGMP pärijana ja teised marsruuterid ei saada IGMP üldisi päringuid ning kommutaator ei tea teistest marsruuteritest midagi.

Paremaks lahenduseks on lisaks IGMP päringutele kuulata ka teisi marsruutimisprotokolli pakette, mis vihjavad marsruuteri olemasolule. Cisco kommutaatorid, mis kasutavad IGMP pealt kuulamist, kuulavad OSPF, PIMv1 ja PIMv2 „hello“ pakette, DVMRP sonde, IGMP päringuid, CGMP liitumisi ja kuuma ooteseisundiga marsruutimisprotokolli HSRP (*Hot Standby Router Protocol*) teateid, mida marsruuterid saadavad välja perioodiliselt.

Cisco kommutaatorites saame multiedasruuteri asukohta kontrollida käsuga

```
show ip igmp snooping mrouter,
```

mis näitab igale virtuaalvõrgule (*VLAN*) vastavat pordi numbrit. Vajadusel saame ka ise määrata multiedastust toetava ruuteri asukoha käsuga

```
ip igmp snooping vlan <vlan_nr> mrouter interface <port>.
```

5.2 Cisco grupihaldusprotokoll CGMP

1996 aasta alguses tundsid Dino Farinacci ja Alex Tweedly firmast Cisco Systems vajadust alternatiivse multisaate piiramisvõimaluse järgi, sest uued L3 teadlikud ASIC-ud olid alles arendamisel ja odavamates kommutaatorites neid ei plaanitudki kasutada. Seega oli vaja mingit alternatiivi.

Nii sündiski lihtne protokoll, mis võimaldab marsruuteritel ja Cisco kommutaatoritel vahetada multisaate grupi liikmelisuse infot andmelülikihi tasemel. Seda uut protokollit hakati kutsuma CGMP (*Cisco Group Management Protocol*) ja on nüüd toetatud kõikides Cisco marsruuterites ja vanemates Cisco kommutaatorites.

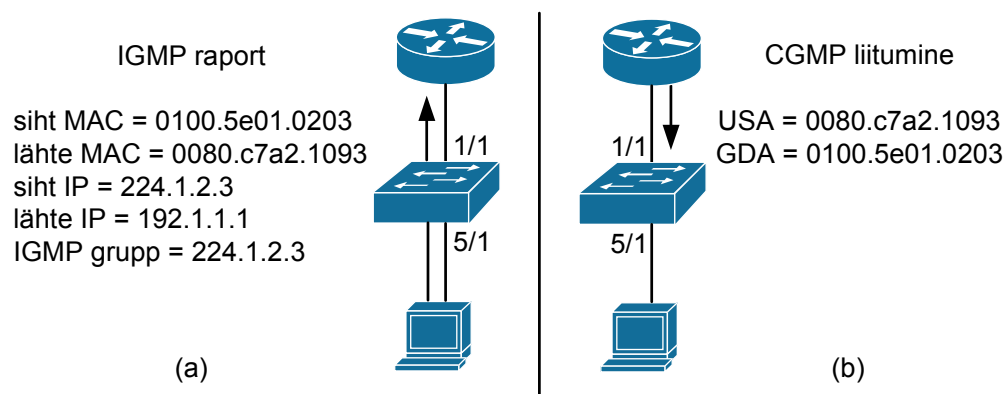
Kõik CGMP teated on OSI mudeli andmelüli kihi kaadrid, adresseeritud üldtuntud multisaate MAC aadressile 0x0100.0cdd.dddd. Kõik kommutaatorid, milles on CGMP lubatud, kuulavad seda aadressi. CGMP teadete multisaate MAC aadressil on oma tagamõte – nad edastatakse kommutaatorites vaikimisi kõikidesse portidesse olenemata sellest, kas kommutaator toetab CGMP-d või mitte. See võimaldab CGMP teadritel levida kogu kommuneeritud võrgu piires ja jõuda CGMP kommutaatoriteni isegi siis, kui teele

jäävad mitte-CGMP kommutaatorid.

CGMP kaardritel on järgmised väljad:

- versioon – 1 või 2;
- teate tüüp – liitumine või lahkumine;
- loendus – järgnevate multiedastuse/üksikedastuse aadresside paaride arv teates;
- GDA – multisaate grupi MAC aadress;
- USA (*Unicast Source Address*) – multisaate grupiga liituja MAC aadress.

CGMP tööpõhimõtte on kujutatud järgneval joonisel 5-6.



Joonis 5-6. CGMP tööpõhimõtte [5].

Host soovib liituda multisaate grupiga 224.1.2.3 ja saadab IGMP liikmelisuse raporti vastavasse gruppi. Kommutaator lihtsalt edastab raporti marsruuterile. Marsruuter (mille vastaval liidesel peab olema CGMP lubatud) töötleb IGMP liikmelisuse raportit nagu tavaliselt, kuid lisaks sellele koostab CGMP liitumise teate ja saadab selle üldtuntud MAC aadressile 0x0100.0cdd.dddd. CGMP-d kasutatav kommutaator võtab kaadri vastu ja saab teada kliendi MAC aadressi (USA väli) ning otsib sellele vastava pordi oma CAM tabelist ja teeb järgmist:

- tekitab CAM tabelisse uue kirje, kus GDA aadressiga on seotud kliendi port ja kõikide marsruuterite pordid või
- lisab kliendi pordi GDA-ga seotud portide nimistusse (kui vastav GDA kirje juba eksisteerib).

Järgnevas tabelis 5-7 on toodud erinevad CGMP teated.

Tabel 5-7. CGMP teated.

GDA	USA	Liitu/Lahku	Tähendus
Multisaate MAC	Kliendi MAC	Liitu	Lisa port gruppi
Multisaate MAC	Kliendi MAC	Lahku	Eemalda port grupist
0000...0000	Marsruuteri MAC	Liitu	Lisa marsruuteri port
0000...0000	Marsruuteri MAC	Lahku	Eemalda marsruuteri port
Multisaate MAC	0000...0000	Lahku	Kustuta grupp
0000...0000	0000...0000	Lahku	Kustuta kõik grupid

Esimesed kaks võimaldavad marsruuteril teavitada CGMP kommutaatorit, kui host liitub või lahku grupist. Kolmas ja neljas teade võimaldavad CGMP protokolliga kasutatavat kommutaatorit teavitada, et USA väljas olev MAC aadress kuulub marsruuterile ja vastav port (kust kaader siseneb kommutaatorisse) tuleb määrata marsruuteri pordiks (liitumisteade) või mitte marsruuteri pordiks (lahkumisteade). Kommutaator peab teadma, millistes portides marsruuterid asuvad, sest need pordid tuleb lisada CAM tabeli igasse multisaate kirjesse, et marsruuterid saaksid kätte kogu multisaate liikluse. Viimased kaks lahkumisteadet on spetsiaalsed haldamise funktsioonid. Näiteks Cisco marsruuteris antud käsk

```
clear ip cgmp <liides>
```

põhjustab marsruuteri poolt saadetud teate “kustuta kõik grupid” kommutaatoritele, mis eemaldab kõik CAM tabeli multisaate kirjed.

CGMPv2 on võimeline lokaalselt teostama klientide multisaate grupist lahkumist (ilma marsruuteri abita). Eelnevalt saime teada, et IGMPv2 grupist lahkumise teated saadetakse “kõik marsruuterid” multisaate aadressile 224.0.0.2, millele vastav MAC aadress on 0x0100.5e00.0002. Seega on kommutaatoritel lihtne neid teateid pealt kuulata, saates ainult nende sihtaadressidega kaadrid protsessorile, aga ülejäänud multiedastust mitte. Kui kommutaator saab grupist lahkumise teate, siis ta seda marsruuterile ei edasta, vaid saadab eelnevalt vastavasse porti IGMP üldise päringu veendumaks, et ei leidu teisi antud multisaate grupi huvilisi. Kui sellele päringule vastuseid ei tule, siis kommutaator lõpetab multisaate edastamise vastavasse porti. Kui see oli viimane port vastavas multisaate grupis, siis ta saadab vastava grupi marsruuterite portidesse grupist lahkumise teate.

Kui sama kohtvõrgu piires kasutatakse nii CGMP kui ka IGMP protokolliga [11], siis IGMP pealt kuulamist kasutavad kommutaatorid saavad sellest aru ja käivitavad spetsiaalse IGMP-CGMP laadi ning ei vahenda enam liikmelisuse raporteid, vaid saadavad need muutmata kujul marsruuteritele. See on CGMP töötamiseks hädavajalik, sest marsruuterid kasutavad raporti saatja MAC aadressi CGMP liitumise teate kokkupanemisel.

6 Distant-vektor multiedastuse marsruutimisprotokoll DVMRP

DVMRP (*Distance Vector Multicast Routing Protocol*) on üks esimesi laiemat kasutust leidnud multisaate ruutimisprotokolle. DVMRP on üsna sarnane RIP ruutimisprotokolliga ning seda toetavad enamasti kõikide tootjate võrguseadmed. Sageli kasutatakse DVMRP marsruuterina ka Unix-laadset tööjaama, millele on installeeritud *mrouterd* deemon. DVMRP protokoll on laialdaselt kasutusel virtuaalses multiedastuse magistraalvõrgus Mbone, mis ühendab tunnelitega üle Interneti erinevate ülikoolide, uurimisasutuste jt multiedastusvõimelised võrgud. Tänapäevaks on Mbone vananenud.

DVMRP andmevahetus toimub IGMP pakettide sees (IP protokoll nr 2) ning paketi struktuur on näidatud joonisel 6-1.

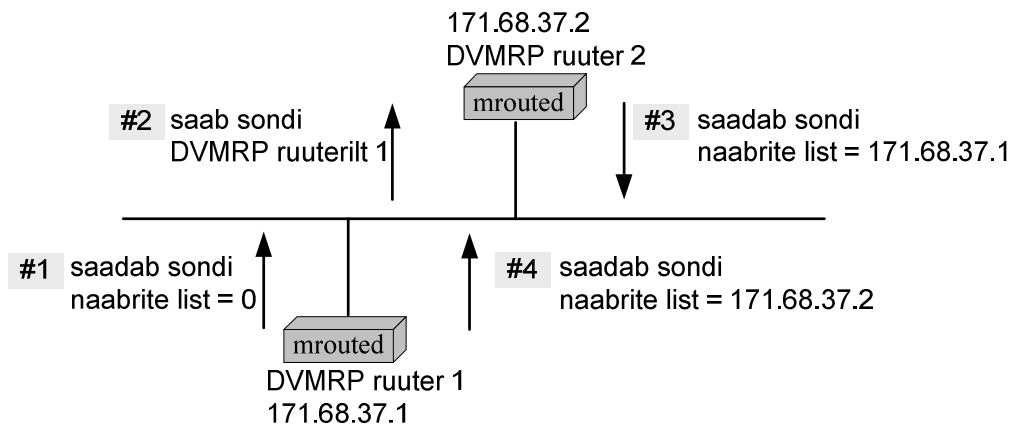
0	7	15	31
Tüüp	Kood	Kontrollsumma	
Reserveeritud		Alamversiooni nr	Põhiversiooni nr
Edasine osa sõltub DVMRP paketi tüübist ehk koodist (kuni 510 baiti)			
:			
:			

Joonis 6-1. DVMRP paketi formaat [12].

DVMRP paketi väljad:

- tüüp – väärtus 0x13 ütleb, et tegu on DVMRP paketiga;
- kood – määrab DVMRP paketi tüübi:
 - 0x1 – sond (naabrite avastamiseks);
 - 0x2 – raport (ruutingu info vahetamiseks);
 - 0x5 – küsi naabreid 2 (küside naabrite list);
 - 0x6 – naabrid 2 (vastus naabrite listiga);
 - 0x7 – pügamine (jaotuspuu pügamiseks);
 - 0x8 – pookimine (jaotuspuu pookimiseks);
 - 0x9 – pookimise kinnitus (pookimise teadete kinnitamiseks);
- kontrollsumma – kogu paketi 16 bitine kontrollsumma;
- alam-ja põhiversioon – vastavalt 0xFF ja 3 praeguse DVMRP versiooni juures.

DVMRP peab olema teadlik naabrite (teiste DVMRP-ruuterite) olemasolust. Selleks multiedastatakse perioodiliselt (iga 10 sekundi tagant, naabrussuhe aegub 35 sekundi jooksul) DVMRP sondeerimise teateid (*DVMRP Probe*) grupi “kõik DVMRP ruuterid” aadressile 224.0.0.4.



Joonis 6-2. DVMRP naabrite avastamine [5].

Joonisel 6-2 on kujutatud DVMRP naabrite avastamise protseduur. Kui ruuter saab sondeerimisteate, mille naabrite nimekirjas on tema enda IP aadress, siis on vastastikune naabrussuhe loodud.

DVMRP probleemide lahendamiseks mõeldud korraldus *mrinfo* (sisaldub *mrouterd* deemonis) kasutab “küsi naabreid 2” ja “naabrid 2” pakette. Pakett “küsi naabreid 2” üksikedastatakse DVMRP ruuterile, millele too vastab “naabrid 2” paketi (formaad näidatud joonisel 6-3).

0	7	15	31
Tüüp (0x13)	Kood (0x6)	Kontrollsumma	
Reserveeritud	Omadused	Alamversiooni nr	Põhiversiooni nr
Liidese aadress [1]			
Meetrika [1]	Lävi [1]	Lipud [1]	Naabreid [1]
Naaber [1]			
...			
Naaber [M]			
Liidese aadress [N]			
Meetrika [N]	Lävi [N]	Lipud [N]	Naabreid [N]
Naaber [1]			
...			
Naaber [K]			

Joonis 6-3. Paketi „Naabrid 2“ formaat [12].

Paketi päisele järgnevad vastaja ruuteri omadused, millele järgnevad seksioonid iga liidese kohta ning vastava liidese naaberruuterid [12]. Kui liides on maas või keelatud olekus, siis näidatakse naabrina aadressi 0.0.0.0 või tunneli puhul teise otsa IP aadressi.

Lokaalse ruuteri omaduste bittide tähendused:

bitt	lipp	Kirjeldus
0	leht	see ruuter on lehtruuter
1	pügamine	ruuter toetab pügamise teateid
2	genID	ruuter saadab generatsiooni ID-sid
3	mtrace	ruuter töötleb mtrace päringuid
4	snmp	ruuter toetab snmp protokoll (DVMRP mib).

Konkreetses liidesega seotud lipud:

bitt	lipp	kirjeldus
0	tunnel	naaber kättesaadav tunneli kaudu
1	source route	tunnel kasutab IP lähte marsruutimist (<i>source routing</i>)
2	reserveeritud	enam ei kasutata
3	reserveeritud	enam ei kasutata
4	maas	operatiivselt maas
5	keelatud	administratiivselt maas
6	pärija	pärija selles kohtvõrgus
7	leht	liidesel puuduvad allavoolu naabrid.

Näide 6-1. Ka Cisco ruuterid vastavad *mrinfo* päringutele. Cisco marsruuterile antud korraldus *mrinfo* väljastab iga liidese (millel on multiedastus konfigureeritud) IP aadressi koos seal nähtava naabriga, liidese meetrika (vaikimisi 1) ja TTL läve. Järgneda võib veel lisainfot: liidesel on käivitatud PIM protokoll, on pärija rollis, on lehtruuter.

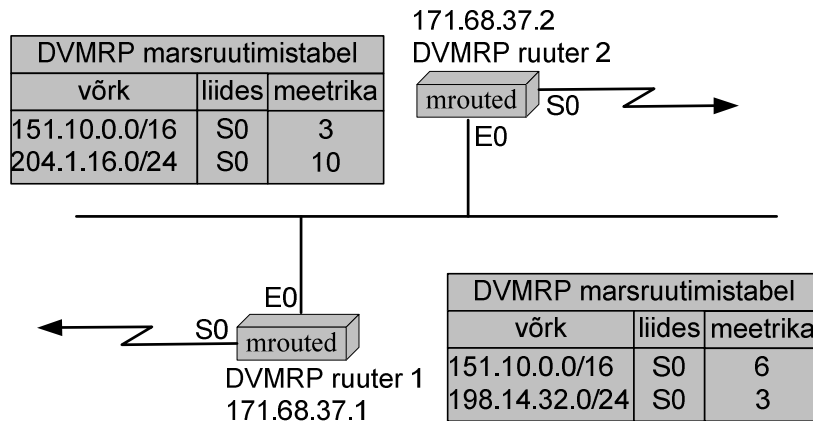
```
Router#mrinfo
193.40.12.52 [version 12.4] [flags: PMSA]:
  193.40.12.52 -> 193.40.12.49 (ak-gw.ut.ee) [1/0/pim]
  193.40.12.52 -> 193.40.12.53 [1/0/pim]
  172.17.200.1 -> 0.0.0.0 [1/0/pim/querier/leaf]
```

Esimesel real näidatakse päritud ruuteri IP aadressi (antud juhul iseenda), operatsioonisüsteemi versiooni ning ruuteri omadusi: P – konfiguratsioon toetab pügamist; M – *mtrace* toetatud; S – SNMP protokoll toetatud; A – auto-RP toetatud. Järgnevad liideste IP aadressid, kus DVMRP tunnelite puhul kuvatakse naabrina tunneli teise otsa IP aadress ning sõna “pim” asemel oleks sõna “tunnel”, PIM protokoll kasutava liidese puhul näidatakse PIM naabrit. Teades naabri aadressi, saame sama infot küsida ka naabri kohta.

DVMRP marsruutimisinfot vahetatakse nagu RIP puhulgi perioodiliselt iga 60 sekundi tagant otseühendatud naabritega. Ruutingu raporti teated sisaldavad lähtevõrke koos võrgumaskiga (seega on DVMRP klassideta ruutinguprotokoll) ja meetrikaks on hüpete loendamine. Marsruutimisinfot hoitakse üksikedastuse marsruutimisinfost eraldi tabelis ja seda kasutatakse:

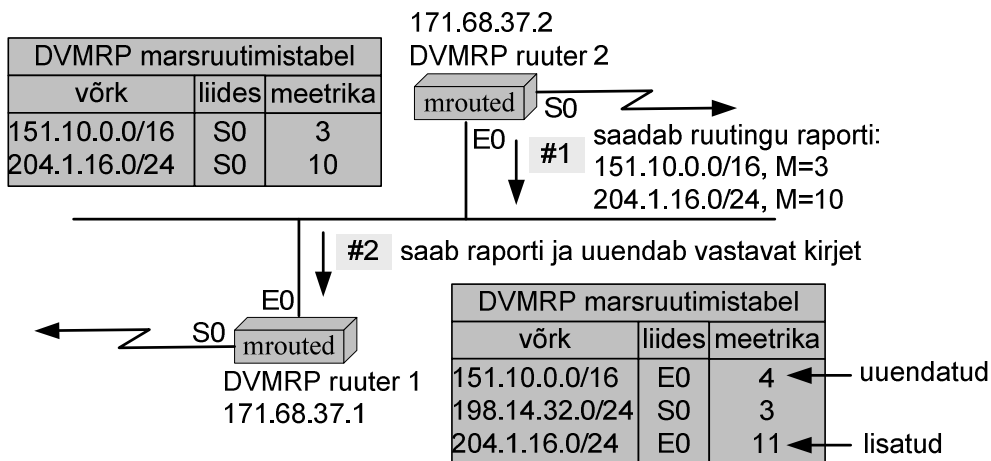
- 1) lähtepuude ehitamiseks;
- 2) multiedastusotsuste tegemiseks (RPF kontroll).

Ruutimisinfo vahetamise illustreerimiseks toon järgnevalt ühe näite, kus kaks DVMPR ruuterit (Unix tööjaamad, mis jooksuprotsessi *mrouterd*) on omavahel ühendatud ühisesse kohtvõrku nagu näidatud joonisel 6-4.



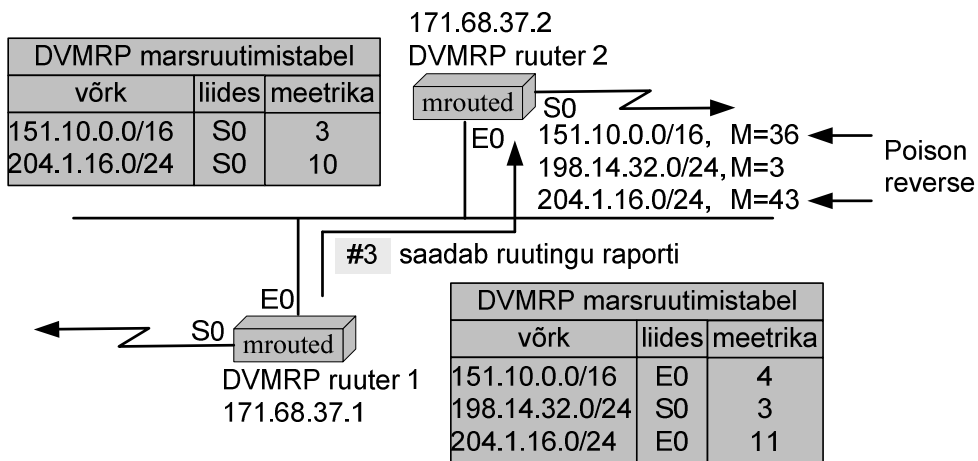
Joonis 6-4. DVMPR ruutimisinfo vahetamine – algseis [5].

Oletame, et mõlemad ruuterid on juba *serial* liideselt saanud ruutimisinfot enne kui nad omavahel infot vahetama hakkavad ning mõlemad omavad marsruuti võrku 151.10.0.0/16. Oletame, et ruuter 2 saadab oma raporti esimesena nagu näidatud järgmisel joonisel 6-5.



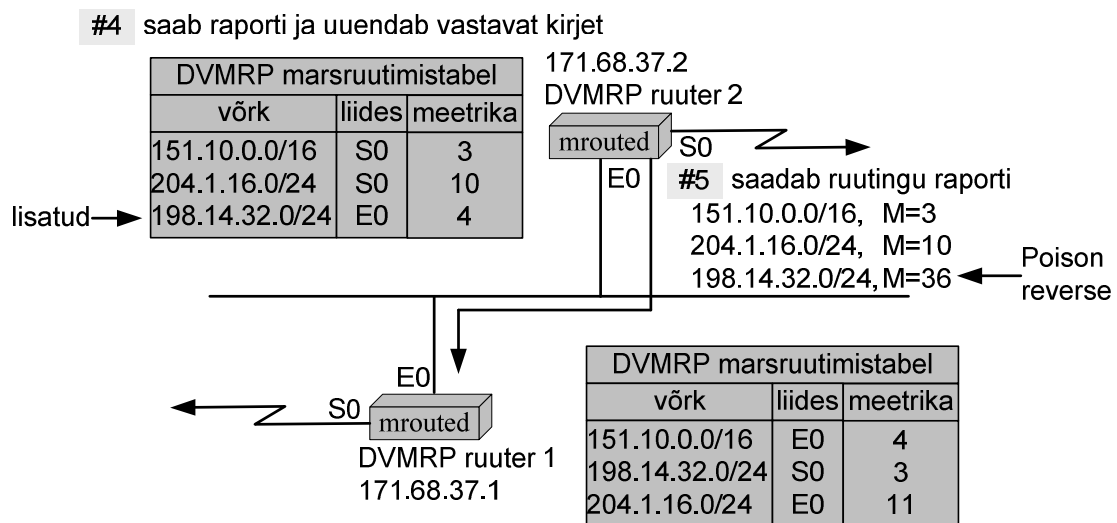
Joonis 6-5. DVMPR ruutimisinfo vahetamine – samm 1 ja samm 2 [5].

Ruuter 1 saab raporti ning lisab oma DVMPR ruutimistabelisse võrgu 204.1.16.0/24. Kuna ruuter 2 kaudu on võrgu 151.10.0.0 meetrika parem, siis uuendatakse ka vastavat kirjet uue meetrikaga 4 (välja kuulutatud meetrikale lisatakse 1 hüpe) ja väljuva liidesega E0. Järgnevalt vastab ruuter 1 omapoolse raportiga (joonis 6-6).



Joonis 6-6. DVMRP ruutimisinfo vahetamine – samm 3 [5].

Pange tähele, et ruuter 1 mürgitab (*Poison Reverse*) liideselt E0 saadud kaks marsruuti, lisades meetrikale lõpmatuse (32). See informeerib ruuterit 2, et ruuter 1 on ruuteri 2 alluv (multisaate jaotuspuus) ja ruuter 1 ootab vastavate võrkude multisaate liiklust ruuterilt 2. Ruuter 2 saab selle raporti kätte ja uuendab oma ruutimistabelit võrguga 198.14.32.0/24 (joonis 6-7, samm 4).



Joonis 6-7. DVMRP ruutimisinfo vahetamine – sammud 4 ja 5 [5].

Viimase sammuna saadab ruuter 2 raporti ja mürgitab ruuterilt 1 saadud marsruudi 198.14.32.0/24 lisades meetrikale lõpmatuse (32). See informeerib ruuterit 1, et ruuter 2 on alluv ning ootab võrgu 198.14.32.0/24 multiedastust ruuterilt 1.

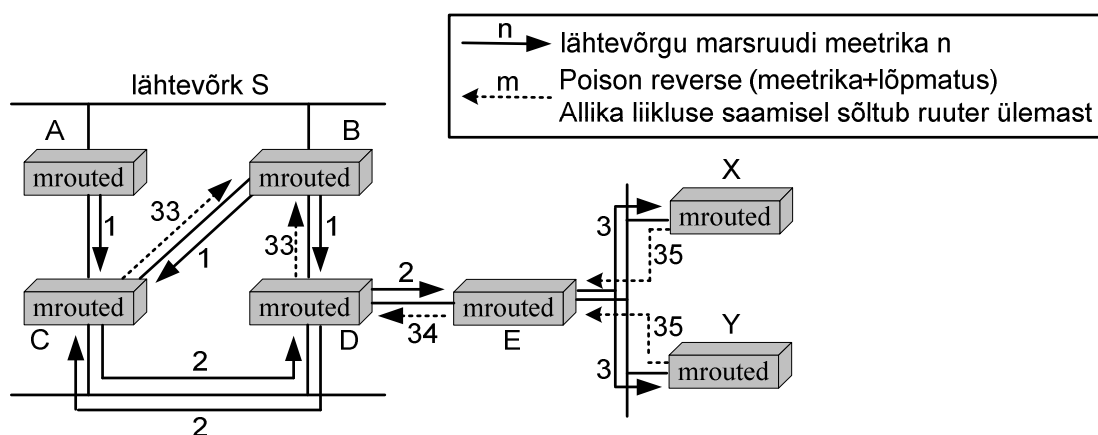
Toon siinkohal ühe näite DVMRP ruutimistabelist Cisco marsruuteris:

```
Router# show ip dvmrp route
DVMRP Routing Table - 1 entry
172.16.0.0/16 [100/11] uptime 07:55:50, expires 00:02:52
  via 192.168.0.0, Tunnel3
```

- 172.16.0.0/16 – lähtevõrk 16-bitise maskiga;
- [100/11] – administratiivne kaal on 100 ja meetrikaks 11 hüpet;
- uptime 07:55:50 – ruuting on olnud aktiivne 7 tundi ja 55 minutit;
- expires 00:02:52 – ruuting aegub 2 minuti ja 52 sekundi pärast, kui ei saada järgmist ruutimise raportit;
- via 192.168.0.0, Tunnel 3 – lähtevõrgu suunas järgmise hüppe IP aadress ja liides, millest paketid välja saata.

6.1 DVMRP trimmitud levisaate puu

DVMRP on oma olemuselt tihedat laadi marsruutimisprotokoll ja kasutab multisaate edastamiseks lähtepuid, mida tuntakse ka lühima tee puudena SPT. Need puud ehitatakse trimmitud levisaate puudest (*truncated broadcast tree*), mis omakorda luuakse DVMRP marsruutimisraportite abiga. Eelnevalt saime teada, et mürgitamise mehhanismiga öeldakse ülesvoolu ruuterile (ülemale), et antud lähtevõrgu liiklus tuleks ka sellest liidesest väljastada, et see jõuaks alluvani. Sisuliselt ütleb alluv ülemale, et teda lisatakse antud lähtevõrgu trimmitud levisaate puusse. Joonisel 6-8 on toodud illustreeriv näide.

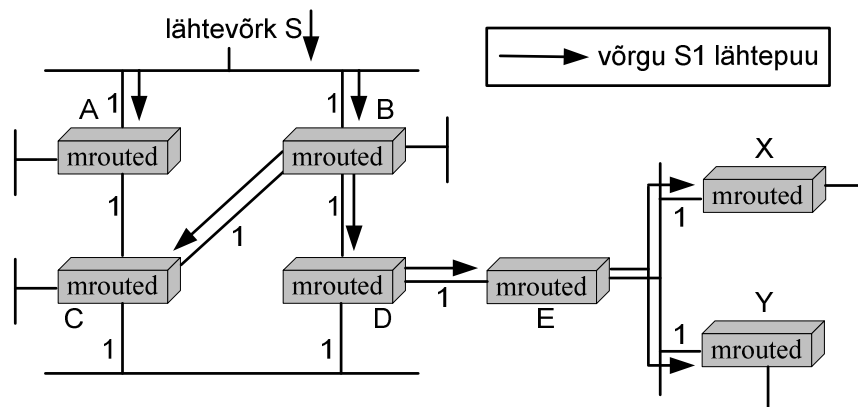


Joonis 6-8. DVMRP trimmitud levisaate puu koostamine [5].

Kui mingi ruuter saab mitmelt ruuterilt sama meetrikaga raporti (ruuter C saab raporti meetrikaga 1 nii ruuterilt A kui B), siis valitakse ülemaks väikseima IP aadressiga ruuter (oletame, et selleks on ruuter B) ning temale saadetud marsruut mürgitatakse. Ruuterid C ja D kuuluvad lähtevõrgu S marsruuti ühisesse kohtvõrku. Et vältida dubleeritud multisaate pakettide edastamist sellesse kohtvõrku, valitakse määratud edastajaks

(*designated forwarder*) ruuter, millel on lühim tee (väikseim meetrika) lähtevõrku S. Antud juhul on meetrikad võrdsed ja sellistel puhkudel valitakse määratud edastajaks väikseima IP aadressiga ruuter (oletame, et selleks on D).

Kui ruutimisinfo on levinud äärepealsete ruuteriteni ning alluvad on saatnud ülesvoolu ruuteritele mürgitatud marsruudi, mis ütleb neile, et antud liides tuleb lisada lähtevõrgu S väljuvate liideste nimekirja, siis ongi loodud trimmitud levisaate puu lähtevõrgu S jaoks nagu näidatud joonisel 6-9.



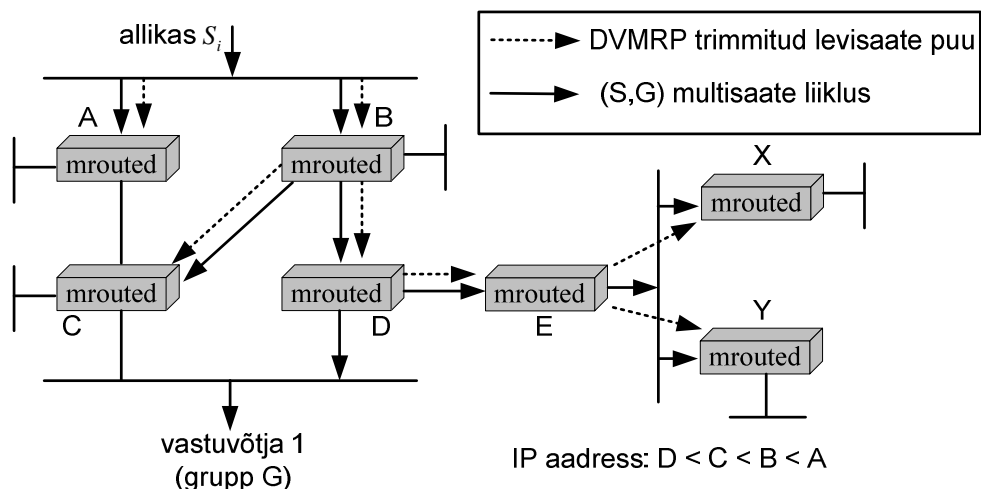
Joonis 6-9. Lähtevõrgu S trimmitud levisaate puu [5].

Iga lähtevõrgu jaoks leidub unikaalne trimmitud levisaate puu, kuid tegelikkuses hakatakse seda puud konstrueerima alles siis, kui leidub edastaja lähtevõrgus. Seega kui saadakse esimene pakett allikalt S_i , luuakse multisaate edastustabelisse (S_i , G) kirje (eeldades, et RPF kontroll õnnestub). Selline nõudmisel olekute loomine aitab kokku hoida ruuterite mäluressurssi.

6.2 DVMRP pügamine

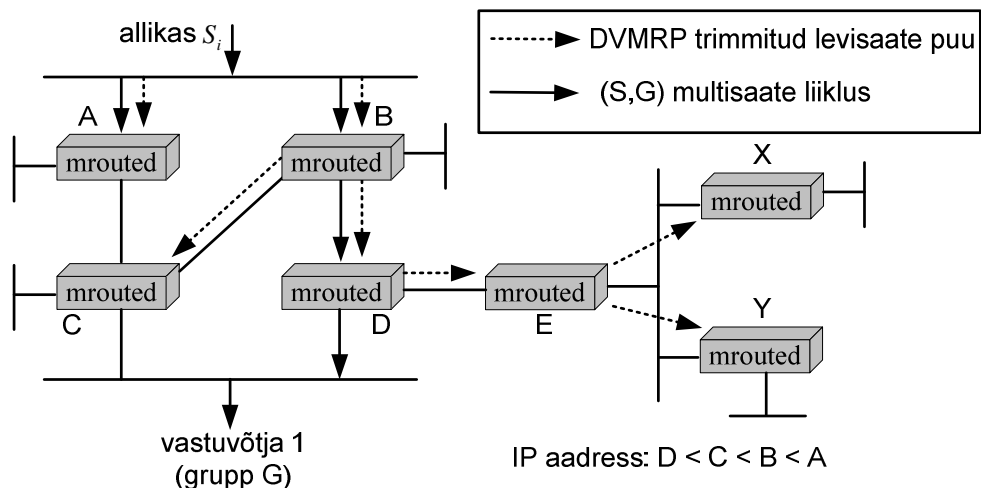
Algselt ujutatakse trimmitud levisaate puu multiedastuse kaadritega üle (olenemata vastuvõtjate olemasolust), et need jõuaksid kõikide ruuteriteni. Võrgu ressursside kokku hoidmiseks hakatakse pügama harusid, kus vastuvõtjaid ei ole. Seega lehtruuterid, mil ei ole otseühendatud vastuvõtjaid, saavad DVMRP pügamise teate trimmitud levisaate puus ülesvoolu. Pügamise tulemusena saadakse konkreetsele allikale vastav lühima tee puu SPT. Paraku on DVMRP "üleujuta ja püga" tüüpi protokoll ning lühima tee puu muutub taas trimmitud levisaate puuks kui pügamised aeguvad (tavaliselt 2 minuti pärast). Siinkohal pean selgitama asjaolu, et trimmitud levisaate puud ennast ei pügata, sest seda kirjeldavad kõikide ruuterite DVMRP marsruutimistabelite kirjed ning neid pügamise teated ei mõjuta. Selle asemel hoitakse pügamise teadete kaudu saadud infot eraldi andmestruktuuris, mille infot kasutatakse (S,G) liiklusvoo juhtimiseks mööda trimmitud levisaate puud.

Toon siinkohal ühe näite trimmitud levisaate puu pügamisest. Joonisel 6-10 on kujutatud võrku, kus allikas S_i edastab multisaadet gruppi G ning grupiga liitub vastuvõtja 1.



Joonis 6-10. DVMRP pügamine - algne üleujutamine [5].

Ruuter C ei ole määratud edastaja kohtvõrgus (kus asub vastuvõtja 1) ja on seega lehtruuter, mil ei ole otseühendatud vastuvõtjaid ning saadab pügamise teate ruuterile B. Ruuter B pügab ruuteri C haru. Kuna ruuterid X ja Y on lehtruuterid ilma vastuvõtjateta, siis ka nemad saadavad pügamise teate ülemale. Ruuter E on teadlik, et sellel liidesel on ainult kaks DVMRP naabrit (DVMRP sond teadete põhjal) ja seega ta võib sellele liidesele vastava haru pügada. Kuna ruuter E on allavoolu liidestest püganud (S_i, G) liikluse, siis ka tema saadab pügamise teate ülesvoolu ning ruuter D pügab liidese ruuterini E. Tulemuseks on joonisel 6-11 kujutatud edastuspuu.

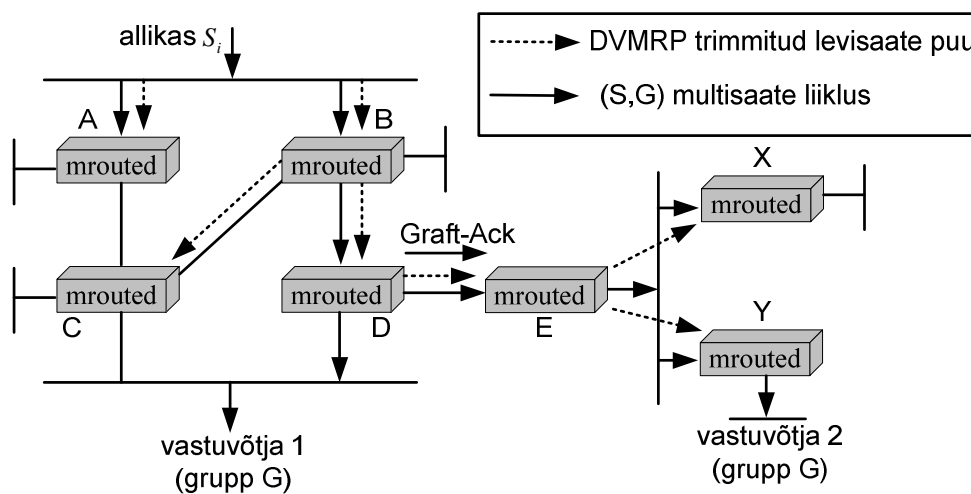


Joonis 6-11. DVMRP pügamine valmis [5].

6.3 DVMRP pookimine

DVMRP toetab usaldusväärset pookimise mehhanismi, mis poogib puule tagasi eelnevalt püगतud harud. Ilma selle mehhanismita peaksid uued vastuvõtjad ootama pügamiste aegumist, mis võib sõltuvalt võrgutopoloogiast aega võtta minuteid. Pookimisteadete kasutamine aitab liitumise latentsuse viia mõne millisekundini. Usaldusväärsus tagatakse sellega, et ülesvoolu ruuter saadab saadud pookimise teatele vastuseks pookimise kinnituse (*Graft-Ack*). Seega kui võrgu ülekoormusel vms põhjusel kaotatakse pookimise teade, siis ei väljastata ka kinnitust ning pookimise teadet korratakse.

Vaatleme eelmise näite peal pookimise mehhanismi. Oletame, et ruuteri Y kohtvõrku tekib vastuvõtja 2, kes liitub multisaate grupiga G. Ruuteris Y on endiselt (S_i, G) olek olemas, mis viitab sellele, et see ruuter püगतi trimmitud levisaate puust ja seega peab ruuter Y saatma ülesvoolu ruuterile pookimise teate. Kui ruuter E saab pookimise teate kätte, siis ta lisab püगतud haru tagasi lähtepuusse taastades liikluse ruuterile Y ning saadab talle pookimise kinnituse teate. Kuna ka ruuter E on eelnevalt (S_i, G) lähtepuust püगतud, siis ka tema saadab pookimise teate ülesvoolu ruuterile D. Kui ruuter D saab pookimise teate, siis ta paneb vastava liidese edastavas olekusse ning saadab tagasi pookimise kinnituse teate. Sellega on eelnevalt püगतud harud tagasi poogitud ning vastuvõtja 2 hakkab saama vastava grupi multiedastust nagu näidatud joonisel 6-12.



Joonis 6-12. DVMRP pookimine [5].

6.4 DVMRP infovahetuse käivitamine Cisco marsruuterites

DVMRP kasutamisse tänapäeva arvutivõrkudes tuleks suhtuda samamoodi nagu RIP protokollis kasutamisse. Kuna on olemas teisi efektiivsemaid ruutimisprotokolle, üksikedastuse puhul OSPF (*Open Shortest Path First*), EIGRP (*Enhanced Interior Gateway Routing Protocol*) jt ning multiedastuse puhul domeenisiseselt PIM, siis võiks

DVMRP protokoll käivitada ainult tagasiühilduvuse tagamiseks, et ühendada olemasolevate DVMRP infrastruktuuridega.

Tegelikult ei olegi Cisco marsruuteris võimalik käivitada eraldi DVMRP protokoll, vaid Cisco marsruutereid saab kasutada PIM-DVMRP lüüsidenä. DVMRP infovahetus aktiveeritakse automaatselt niipea, kui ruuter kuuleb mingi liidese peal DVMRP ruuteri poolt saadetud sond paketti. Eelduseks on muidugi see, et vastava liidese peal on käivitatud PIM protokoll.

Cisco ruuteri eripäraks on veel see, et ta omalt poolt ei vasta sond paketiaga. Seda sel põhjusel, et mitte segadusse ajada teisi võimalikke Cisco marsruutereid hulgiöördusega võrgusegmentides nagu Ethernet. Kuna Cisco marsruuter ei pea hulgiöördusega võrgusegmentides arvet teiste DVMRP naabrite kohta, siis ta ignoreerib ka pügamise teateid, sest Cisco marsruuter ei tea, kas vastavas võrgusegmendis leidub veel mõni DVMRP ruuter, mis endiselt soovib vastava grupi liiklust vastu võtta. Seega ei ole DVMRP ruuteritel võimalik mingi (S,G) grupi liiklust pügada. Seetõttu on soovitatav kasutada ka hulgiöördusega võrgus DVMRP naabriga ühendumiseks tunnelit, mis on punktist-punkti ühendus ja Cisco marsruuter aktsepteerib sel juhul pügamise teateid.

Näide 6-2. Cisco marsruuteri FastEthernet 0 liidesele on konfigureeritud DVMRP tunnel.

```
interface tunnel0
  ip pim unnumbered FastEthernet 0
  ip pim sparse-dense-mode
  tunnel source FastEthernet 0
  tunnel destination 192.168.1.10
  tunnel mode DVMRP
interface FastEthernet 0
  ip address 172.16.2.1 255.255.255.0
  ip pim sparse-dense-mode
```

Korraldus “tunnel mode DVMRP” tähendab, et kasutatakse IP-IP kapseldust (mis on DVMRP tunnelite puhul standardiks), kus lisatud IP päise lähteadressiks on FastEthernet 0 liidese aadress ning sihtaadressiks on 192.168.1.10. Tunneli lähteadressi võime määrata ka käsuga **tunnel source <ip_aadress>**.

Tunneli olekut saate hiljem kontrollida käsuga **show interface tunnel 0** ja ruutingute vahetamise töötamist **show ip dvmrp route**.

7 Protokollist sõltumatu multiedastus - PIM

PIM (*Protocol Independent Multicast*) sai oma nime selle järgi, et ta on IP marsruutimisprotokollist sõltumatu. Kuigi PIM-i kutsutakse multiedastuse marsruutimisprotokolliks, siis selle asemel, et hallata eraldi multisaate marsruutimistabelit, ta tegelikult kasutab RPF kontrolli teostamisel olemasolevaid üksikedastuse ruutimistabeli kirjeid (näiteks EIGRP, OSPF, BGP või staatilised ruutingud). Cisco seadmetes kasutatav PIM oskab kasutada ka DVMRP ja staatilisi multiedastuse ruutinguid (*mroutes*). Cisco IOS võimaldab konkreetse allika RPF kontrolli teostada ka käsurealt.

Näide 7-1. Küsin ruuterilt lühima tee puu (193.40.15.11, 239.100.0.0) allikani viiva liidese (RPF liides) ehk vastava marsruutimiskirje sissetuleva liidese.

```
Router#sh ip rpf 193.40.15.11
RPF information for digitv.ut.ee (193.40.15.11)
  RPF interface: Vlan50
  RPF neighbor: ak-gw.ut.ee (193.40.12.49)
  RPF route/mask: 0.0.0.0/0
  RPF type: unicast (static)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

Ülaltoodud näites on allikani viivaks liideseks „Vlan50“, ülesvoolu ruuteriks „ak-gw“ ning RPF kontrolli teostamisel kasutatakse üksikedastuse marsruutimistabeli vaike marsruudi kirjest (mis on määratud staatiliselt).

Kuna PIM ei pea tegelema ruutimisuuenduste saatmise/vastuvõtmisega, siis on PIM koormus marsruuteritele väike. Nagu DVMRP, kasutab ka PIM naabrite avastamise mehhanismi [5]. Naabrussuhete loomiseks kasutatakse perioodilisi (vaikimisi iga 30 sekundi tagant) “hello” teateid, mis multiedastatakse “kõik PIM marsruuterid” gruppi aadressiga 224.0.0.13. PIM “hello” teated sisaldavad ka säilitamise (*holdtime*) välja, mis ütleb vastuvõtjale, millal lasta vastava naabri külgnevusel aeguda. Tavaliselt on vaikimisi säilitamise ajaks kolmekordne PIM “hello” teadete periood ehk siis 90 sekundit.

Külgnevuste jälgimisel on oluline roll tihedat laadi PIM protokollis lähtepuude haldamisel nagu hiljem saame teada. PIM “hello” teateid kasutatakse ka võrgusegmendi jaoks määratud ruuteri (*Designated Router*) valimisel. Kõrgeima IP aadressiga marsruuter saab määratud marsruuteriks DR selles võrgus. Määratud ruuteri funktsionaalsust kasutatakse põhiliselt hõredat laadi PIM protokollis. Kuid kui mingis võrgusegmendis kasutatakse IGMPv1, siis on PIM-DR ühtlasi ka IGMP pärijaks-ruuteriks, sest IGMPv1 ei oma pärija-

ruuteri valimise mehhanismi.

Cisco marsruuterites saame PIM naabreid ja ühtlasi ka määratud ruuterit näha käsuga:

```
show ip pim neighbor.
```

Näide 7-2. PIM naabrite kohta info küsimine.

```
Router#sh ip pim neighbor
PIM Neighbor Table
Neighbor          Interface  Uptime/Expires  Ver  DR
Address                                     Prio/Mode
193.40.12.49      Vlan50    1d03h/00:01:32  v2   1 / S
```

Ülaltoodud käsu tulemusena väljastatakse meile PIM naabri IP aadress, liides, millelt naaber avastati, naabri püstitoleku aeg (*Uptime*), naabrussuhte aegumine, PIM naabri liidesel kasutatav PIM versioon, naabri liidese DR-prioriteet ning välja “Mode” lipud: DR – PIM naaber on määratud ruuter; B – toetab kahesuunalist PIM protokoll; S – olekute värskendamine toetatud.

Kui mingis võrgusegmendis on mitu marsruuterit, siis mõnikord tahab administraator ise otsustada, milline on määratud marsruuter DR. Eesmärgi saavutamiseks vajalik IP aadresside ümberhäälestamine on tüütu ja mõnikord ka võimatu. Seetõttu täiendati PIMv2 protokoll “hello” teateid DR-prioriteedi suvandiga (vaikeväärtus 1). DR-prioriteedi määramine liidesele toimub järgneva korraldusega:

```
interface <liides>
    ip pim dr-priority <prioriteet>,
```

kus prioriteedi väärtus võib olla vahemikust 0 kuni 4294967294.

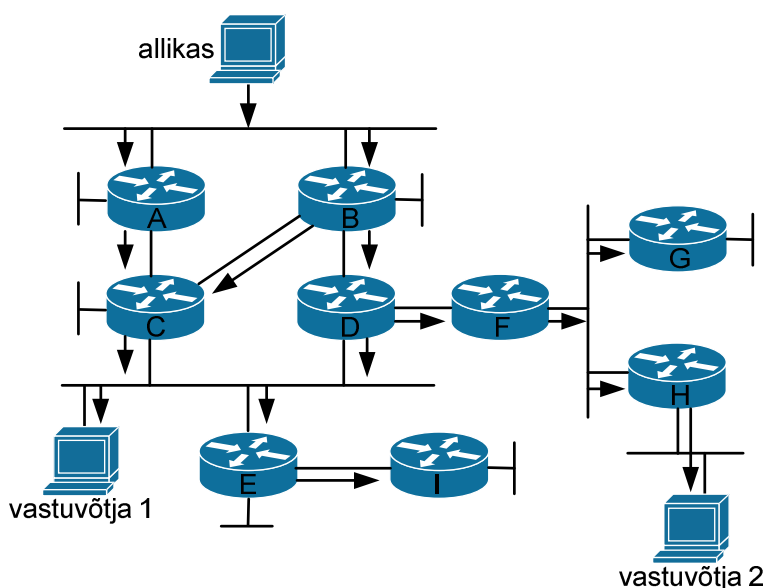
Suurima prioriteediga marsruuter valitakse määratud ruuteriks vastavas võrgusegmendis. Kui ruuteri “hello” teadetes ei ole prioriteeti kirjas, siis eeldatakse, et sel ruuteril on kõrgeim prioriteet. Kui mitmel ruuteril on sama DR prioriteet, siis võrreldakse IP aadresse. Kõrgeima IP aadressiga ruuter saab määratud ruuteriks.

7.1 Tihedat laadi PIM

Tihedat laadi protokoll PIM-DM (*PIM Dense Mode*) ujutab algselt kõik võrgusegmen did multisaate liiklusega üle, et kindlustada liikluse jõudmine kõikide huvilisteni. Seejärel hakkavad marsruuterid pügama puu harusid, kus puuduvad multisaate grupi liikmed. Protsess kordub iga 3 minuti tagant. Selline lähenemine on efektiivne ja mõttekas siis, kui

multisaate huvilised paiknevad arvutivõrgus väga tihedalt ning võrgu ribalaiusega probleeme ei ole.

PIM-DM kasutab multiedastamisel ainult lähtepuid ehk (S,G) kirjeid, mis ehitatakse jooksvalt niipea kui allikas edastama hakkab. Lähtepuu ehitamisel kasutatakse infot PIM naabrite kohta. Algselt on kõik PIM naabrid lühima tee puus SPT nii, et paketi sisendliides (teostatakse RPF kontroll üksikedastuse marsruutimistabeli abiga) on liides allika suunas ja kõik ülejäänud PIM-DM naabrid on allikast allavoolu ehk siis vastava ruuteri alluvad. Kui RPF kontrolli tulemusena leidub mitu sisendliidest (üksikedastuse ruutimistabelis on vastavasse võrku mitu võrdse maksumusega teed), siis peab ruuter valima ainult ühe liidese. Sel juhul kasutab PIM (nii tihedat kui hõredat laadi) RPF kontrolli teostamisel marsruutimiskirjet, mille järgmise hüppe IP aadress on kõrgeim.



Joonis 7-1. PIM-DM jaotuspuu - algne üleujutamine [5].

Joonisel 7-1 on kujutatud algset üleujutamist, sest puu pügamist ei ole veel toimunud. Marsruuterid A ja B võtavad allika liikluse vastu ja multiedastavad selle oma kõikidele PIM-DM alluvatele naabritele C ja D. Kuna pügamist ei ole veel toimunud, siis leidub puus ülemääraseid teid (ruuteril C on kaks sisendrada) ja dubleeritud edastajaid (ruuterid C ja D samas võrgusegmendis).

7.1.1 PIM-DM pügamine

PIM-DM ruuterid saavad pügamise teate järgmistel tingimustel:

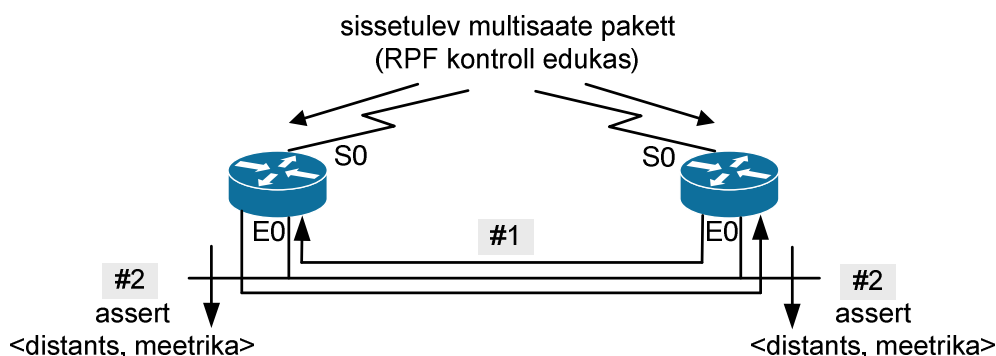
- liiklus saabub mitte-RPF punktist-punkti liideselt;
- ruuter on puu leheks ja tal ei ole vahetult ühendatud vastuvõtjaid;
- ruuter on puu tipuks (ei ole leht) punktist-punkti ühendusel ja ta saab pügamise teate oma naabrilt;
- ruuter on puu tipuks võrgu segmendis (tal ei ole vahetult ühendatud vastuvõtjaid)

ning ta sai pügamise teate naabrilt vastavast võrgu segmendist ja teised naabrid vastavas segmendis ei tühistanud pügamise teadet.

Seega joonisel 7-1 oleva puu pügamise sammud on järgmised:

- 1) ruuter C saadab ruuterile B pügamise teate, sest antud allika liiklus saabub sealtkaudu mitte-RPF liideselt (eeldusel, et marsruutimistabeli järgi on allika võrgu meetrika parem ruuteri A kaudu);
- 2) ruuter B pügab ühenduse ruuteriga C;
- 3) kuna ruuter I on puu leht, millel ei ole ühtegi vahetult ühendatud vastuvõtjat, siis ta saadab ruuterile E pügamise teate;
- 4) ruuter E pügab ühenduse ruuteriga I;
- 5) kuna ruuteril E ei ole ühtegi vahetult ühendatud vastuvõtjat ja alluvate ühendused on pügatud, saadab E pügamise teate ruuteritele C ja D;
- 6) kuna samas võrgusegmendis on vähemalt üks vastuvõtja (vastuvõtja1), siis ruuterid C ja D ignoreerivad pügamise teateid;
- 7) kuna ruuter G on puu leht, millel ei ole ühtegi vahetult ühendatud vastuvõtjat, ta saadab pügamise teate võrgusegmenti, kus asub ruuter F;
- 8) kuna pügamise teated multiedastatakse “kõik PIM ruuterid” grupile (224.0.0.13), siis ka ruuter H kuuleb pügamise teadet ning tühistab selle PIM liitumise teatega, sest tal on üks vahetult ühendatud vastuvõtja (vastuvõtja2).

Oleme saavutanud olukorra, kus allika liiklus jõuab ainult nendesse võrgu punktidesse, kus asuvad vastuvõtjad. Kuid lahendamata on veel dubleeritud liikluse probleem võrgusegmendis, kus asub vastuvõtja1 (mõlemad ruuterid C ja D edastavad sinna). PIM kasutab selle probleemi lahendamiseks PIM kinnitamise (*assert*) mehhanismi.

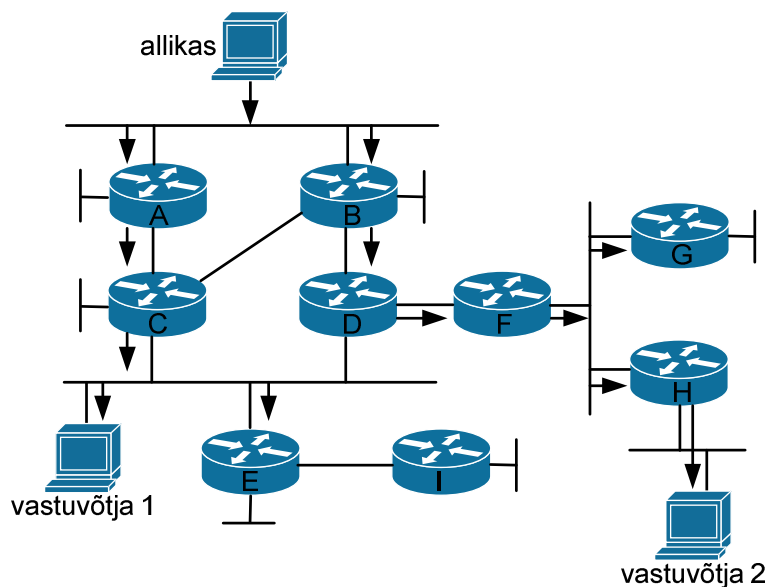


Joonis 7-2. PIM assert mehhanism [5].

Kui marsruuter saab multisaate allikalt paketi liidese pealt, mis on multisaate marsruutimistabelis vastava grupi (S, G) väljuvate liideste hulgas, siis ruuter saadab sellelt liideselt välja “PIM kinnitamise” teate nagu näidatud joonisel 7-2. Nende teadete põhjal selgitatakse välja multisaate edastaja vastavas võrgusegmendis. Võitjaks osutub marsruuter, mil on parim tee allikani. Kõigepealt ruuterid võrdlevad “kinnitamise” teates olevat allikani viiva marsruudi administratiivset kaalu (*administrative distance*). Mida

väiksem kaal seda parem, seejärel võrreldakse marsruudi maksimumust (mida väiksem seda parem). Kui need on võrdsed, siis saab võitjaks kõrgeima IP aadressiga marsruuter.

Oletame, et meie joonisel 7-1 osutus võitjaks ruuter C, mis jätkas pakettide edastamist ning ruuter D pügas oma liidese vastavast puust. Nüüdseks on PIM üles ehitatud allikast lähtuva täispuu, näidatud joonisel 7-3.



Joonis 7-3. PIM-DM täispuu [5].

PIM-DM on võimeline ka kiiresti tagasi pookima eelnevalt püगतud puu harud. Oletame, et ruuteri I tagusesse kohtvõrku ilmub kolmas vastuvõtja. Esmalt saab ruuter I uuel vastuvõtjalt IGMP liikmelisuse raporti ning seejärel ruuter I teab, et ruuterile E tuleb saata pookimise (*graft*) teade (ruuter I teab seda seetõttu, et ta säilitab allikate multisaate gruppide olekud (S, G), kuigi nad on eelnevalt püगतud). Marsruuter E kinnitab pookimise teate kätte saamist pookimise kinnituse (*graft-ACK*) teatega.

Tuletan meelde, et PIM-DM kordab üleujutamise ja pügamise protsessi iga 3 minuti tagant, mis raiskab asjatult võrgu ribalaiust. Seetõttu laiendati PIMv2 protokollile nn “oleku värskendamise” võimalusega [13]. Põhimõte on lihtne: esimese hüppe marsruuterid (allika poolt vaadatuna) saavad perioodiliselt (S,G) oleku värskendamise kontrollteateid mööda lähtepuud allavoolu, mis aitab ära hoida püगतud harude olekute aegumise. Cisco marsruuterites saab oleku kontrollteadete käsitlemist ja edastamist keelata globaalse konfigureerimise käsuga

```
ip pim state-refresh disable
```

ja lubada käsuga

```
no ip pim state-refresh disable.
```

Vaikimisi on oleku värskendamise kontrollteadete tekitamine keelatud, aga edastamine lubatud. Kontrollteadete algatuseks mingi liidese peal on vaja ruuterile anda järgmised käsud:

```
interface <liides>
    ip pim state-refresh origination-interval [intervall],
```

kus vaikimisi intervalliks pannakse 60 sekundit, kuid saab ka ise määrata vahemikust 1..100 sekundit.

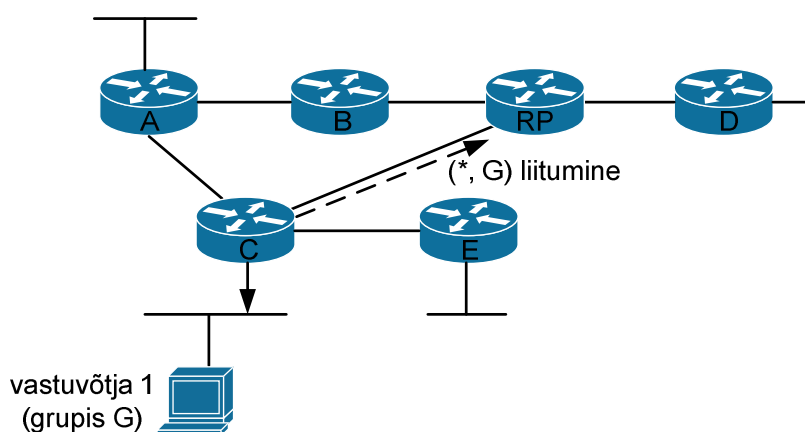
Olekute värskendamise häälestust saame kontrollida liidese detailvaatest:

```
show ip pim interface <liides> detail.
```

7.2 Hõredat laadi PIM

Hõredat laadi protokoll PIM-SM (*PIM Sparse Mode*) multiedastab liiklust ainult nendesse võrgu segmentidesse, kus asuvad aktiivsed vastuvõtjad. PIM-SM skaleerub hästi igasuguse suurusega võrgule, ka sellistele mis sisaldavad WAN ühendusi, sest liitumismehhanism aitab ära hoida WAN ühenduste koormamise soovimatu liiklusega. PIM-SM kasutab multisaate edastamiseks ühesuunalist jagatud puud, mille juureks on kohtumispunkt RP.

Oletame, et joonisel 7-4 liitub vastuvõtja 1 multisaate grupiga G (esimene liituja), seega ta saadab IGMP liikmelisuse raporti ruuterile C. Ruuter C tekitab (*,G) kirje oma multisaate ruutimistabelisse ja lisab kohtvõrgu liidese vastava kirje väljuvate liideste nimekirja.



Joonis 7-4. Jagatud puuga liitumine [5].

Kuna ruuteris C seda (*,G) kirjet ei olnud, siis ta edastab PIM (*,G) liitumise teate RP suunas (joonisel 7-4), et liituda jagatud puuga. (*,G) liitumise teade liigub hüpete kaupa grupi G kohtumispunkti RP suunas ning iga ruuteri läbimisel luuakse multisaate grupi G jaoks puu olek. Lõpuks jõuab (*,G) liitumise teade kohtumispunkti RP või ruuterisse, kus

on juba (*,G) puu olek olemas. Kui ruuter RP saab (*,G) liitumise teate ja ka temal puudub varasem info grupi G kohta, siis ta lisab oma multisaate marsruutimistabelisse (*,G) kirje ja lisab ühenduse ruuteriga C väljuvate liideste nimekirja. Sellisel moel ongi loodud multisaate grupi G jaoks jagatud puu (RP -> ruuter C -> vastuvõtja 1) ja vastava grupi multisaate liiklus, mis jõuab RP-sse saab voolata RP-st allavoolu.

Oletame, et liitub veel üks huviline multisaate grupiga G ruuteri E tagusest kohtvõrgust. Siis tehakse järgmised toimingud:

- 1) vastuvõtja 2 saadab ruuterile E IGMP liikmelisuse raporti;
- 2) ruuter E tekitab oma multisaate marsruutimistabelisse (*,G) kirje ja lisab kohtvõrgu liidese väljuvate liideste nimekirja;
- 3) ruuter E saadab (*,G) liitumise teate ruuterile C;
- 4) ruuter C saab liitumise teate ja kuna tema multisaate marsruutimistabelis juba on (*,G) kirje, siis lisab ühenduse ruuteriga E (*,G) väljuvate liideste nimekirja.

7.2.1 Jagatud puu pügamine

Kuna jaotuspuude ehitamisel kasutatakse liitumise teateid, siis puu harude eemaldamiseks kasutatakse pügamise teateid (on võimalik ka lihtsalt lõpetada puu olekute värskendamine liitumise teadete mitte saatmisega, kuid see ei oleks efektiivne võrguressursside kasutamine).

Oletame, et vastuvõtja 2 lahkub multisaate grupist G saates IGMP lahkumise teate ruuterile E. Kuna vastuvõtja 2 oli ainuke multisaate grupi G kuulaja selles kohtvõrgus, siis ruuter E eemaldab vastava kohtvõrgu liidese (*,G) väljuvate liideste nimekirjast. Kuna (*,G) väljuvate liideste nimekiri on nüüd tühi, siis ruuter E ei vaja enam grupi G multisaate liiklust ning saadab (*,G) pügamise teate ruuteri RP suunas. Ruuter C saab pügamise teate ja eemaldab kirje (*,G) väljuvate liideste nimekirjast ühenduse ruuteriga E. Kuna ruuteril C on endiselt olemas otseühendatud multisaate grupi G kuulaja (vastuvõtja 1), siis (*,G) väljuvate liideste nimekiri ei ole tühi ja pügamise teadet jagatud puu juure RP poole edasi ei saadeta.

7.2.2 PIM-SM lühima tee puud

PIM-SM peamisi eeliseid on see, et ta lubab multisaadet edastada ka mööda lühima tee puud SPT. Sama liitumise teadet, mida kasutatakse jagatud puuga liitumiseks (mille juureks on kohtumispunkt RP), saab kasutada ka SPT-ga liitumiseks (mille juureks on konkreetne allikas). SPT-ga liitumisel marsruuditakse multisaate liiklus otse vastuvõtjateni, ilma kohtumispunkti läbimata, saavutades sellega väiksema latentsuse ja efektiivsema võrgu ribalaiuse kasutamise ning ühtlasi vähendatakse ka RP koormust. Miinuseks on see, et SPT puus asuvad marsruuterid peavad haldama (S,G) olekuid multisaate marsruutimistabelis, kuid tavaliselt on see vähem ressurssinõudev kui tihedat laadi protokollide puhul, mil kõik marsruuterid peavad haldama (S,G) olekuid.

Ümberlülitust lühima tee puule määratakse marsruuterites parameetriga “spt-threshold” ribalaiuse ühikutes (Kbit/s). Kui see piirmäär ületatakse, siis vastuvõtjapoolne ruuter liitub lühima tee puuga. Cisco marsruuterites on vaikimisi piirmääraks 0, mis tähendab, et liitutakse lühima tee puuga esimese multisaate paketi saabumisel mööda jagatud puud. Kuid võrguadministraatoril on võimalus sundida liiklust jääma jagatud puule globaalse režiimi käsuga

```
ip pim spt-threshold infinity [group-list <acl>],
```

kus valikulise parameetri “group-list” pääsuloendiga määratakse, millistele gruppidele korraldus antakse. Parameetri ära jätmisel kehtib korraldus kõikidele multisaate gruppidele.

Lühima tee puu loomiseks saadab vastuvõtjaga otseühendatud marsruuter (S,G) liitumise teate allika S suunas. Kõik teele jäävad marsruuterid loovad oma multiedastustabelites (S,G) olekud, kus väljuvate liideste nimekirja lisatakse liides, millest liitumise teade saadi. Lõpuks jõuab (S,G) liitumise teade allika S kohtvõrgu marsruuterini, kus on juba (S,G) kirje olemas. Viimasel juhul täiendatakse (S,G) väljuvate liideste nimekirja liidesega, kust liitumine saadi ja multisaate paketid saavad hakata liikuma uue liituja suunas.

Sellest hetkest hakkab vastuvõtja (või temast ülesvoolu olev marsruuter) saama andmeid dubleerituna: nii lühima tee puust kui jagatud puust. Kui ruuter saab esimesed multisaate paketid SPT-st, hakkab ta ära viskama allikalt S gruppi G edastatud pakette, mis tulevad mööda jagatud puud RPT. Lisaks saadetakse spetsiaalne RP lipuga (S,G) pügamise teade RP suunas. Seda tuntakse kui (S,G,rpt) pügamise teatena. See teade liigub hüpete haaval RP suunas ja kõik teel olevad ruuterid saavad kohandada oma (S,G) kirjet nii, et allikalt S gruppi G edastatavat liiklust enam selles suunas ei edastataks. Nüüdsest saab vastuvõtja allikalt S grupi G multiedastust ainult mööda lühima tee puud.

7.2.3 PIM liitumise/pügamise teade

Siiani olen viidanud PIM liitumise ja pügamise teadetele kui erinevatele teadete tüüpidele. Tegelikult on tegemist ühe ja sama teatega. PIM liitumise/pügamise teate formaat on üksikasjalikumalt kirjeldatud RFC-s 4601. Iga liitumise/pügamise teade sisaldab muuhulgas multisaate gruppide nimekirja ning iga grupi kohta vastavat liitunud ja pügatud allikate nimekirja, millest kumbki võib olla ka tühi. Need nimekirjad on teatud ühise formaadiga, sisaldades muuhulgas järgmist informatsiooni:

- multisaate allika aadress – multisaate allika IP aadress, millega liitutakse või mida pügatakse (tegu on kohtumispunkti RP aadressiga, kui WC (*wildcard*) lipp on püsti);
- multisaate grupi aadress – multisaate grupi D klassi aadress, millega liitutakse või mida pügatakse;

- WC lipp – kui lipp püsti, on tegu jagatud puu (*,G) liitumise/pügamise kirjega;
- RP lipp – liitumise/pügamise info on rakendatav ainult jagatud puule ja tuleb edastada mööda seda ülespoole.
-

Näiteks PIM liitumise/pügamise teade, mille liitumise listis on kirje:

- allika aadress = 192.16.10.1;
- grupi aadress = 224.1.1.1;
- lipud = WC, RP;

tähendab, et tegemist on (*,G) liitumisega grupile 224.1.1.1 (sest WC ja RP lipud on püsti), mille kohtumispunkt RP on 192.16.10.1.

Aga PIM liitumise/pügamise teade, mille pügamise listis on kirje:

- allika aadress = 191.1.2.1;
- grupi aadress = 239.255.1.1;
- lipud = puuduvad;

tähendab, et tegemist on (S,G) (kuna WC ja RP lipud on maas) pügamisega allikale 191.1.2.1 grupis 239.255.1.1.

7.2.4 PIM-SM oleku värskendamine

Igal PIM-SM ruutimistabeli edastuskirjel (S,G) ja (*,G) on paika pandud lõplik eluiga (3 minutit), mille möödudes kirje kustutatakse. See aitab ära hoida kirjete rippuma jäämist, kui näiteks ülesvoolu ruuter ei saa pügamise teadet kätte võrgu ülekoormatuse tõttu. Seetõttu peavad allavoolu olevad ruuterid seda olekut perioodiliselt värskendama, saates ülesvoolu olevale ruuterile PIM liitumise/pügamise teateid.

Ruuterid värskendavad jagatud puid, saates iga minuti tagant (*,G) liitumise ülesvoolu ruuterile kohtumispunkti RP suunas. Ruuterid värskendavad lühima tee puid SPT, saates iga minuti tagant (S,G) liitumise ülesvoolu ruuterile multisaate allika suunas. Neid perioodilisi uuendusi saadetakse senikaua kuni ruuteri (*,G) või (S,G) väljuvate liideste nimekiri ei ole tühi.

7.2.5 Allika registreerimine

Kuna PIM-SM kasutab ühesuunalist jagatud puud, kus multisaate liiklus võib voolata juurest (RP) allavoolu, siis multisaate allikad peavad edastatava liikluse mingil muul viisil juureni toimetama. PIM-SM korral peab RP liituma allika lähtepuuga, kuid ennem peab RP allika olemasolust kuidagi teada saama. Selleks kasutatakse PIM registreerimise teateid.

7.2.6 PIM-SM registreerimise teated

PIM registreerimise teated saadetakse allikaga otseühendatud määratud ruuteri poolt RP suunas. PIM registreerimise teadetele on kaks eesmärki:

- 1) teatada RP-le, et allikas S on aktiivne multiedastaja grupis G;
- 2) toimetada allika S esialgsed multisaate paketid (kapseldatuna PIM registreerimise teadetesse) RP-le edastamiseks jagatud puust allavoolu.

Seega, kui multisaate allikas alustab edastamist, siis otseühendatud määratud marsruuter saab need andmed kätte ja tekitab oma multisaate ruutimistabelisse (S,G) kirje. Lisaks kapseldab määratud ruuter iga multisaate paketi PIM registreerimise teateks ja üksikedastab selle RP-le (kuidas määratud ruuter teab RP IP aadressi, sellest räägin hilisemas alalõigus “PIM kohtumispunktid”). RP saab PIM registreerimise teate kätte, kapseldab selle lahti ning saab multisaate paketi. Kui pakett on aktiivsele multisaate grupile (vastavale grupile on saadud jagatud puuga liitumise teateid), siis edastatakse pakett mööda jagatud puud allavoolu ning RP liitub allika S lähtepuuga, et saada (S,G) liiklust neitsilikul kujul, mitte kapseldatuna PIM registreerimise teadetesse. Kui aga vastavale grupile ei leidu aktiivset jagatud puud, siis multisaate paketid visatakse minema ja allika S lähtepuuga liitumist ei algatata.

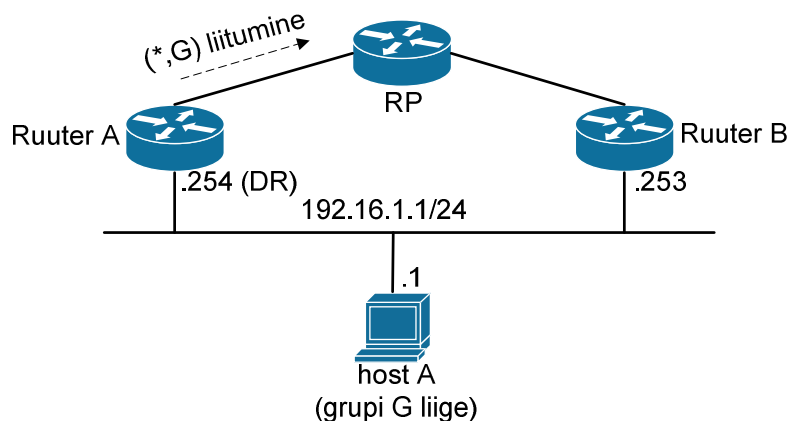
7.2.7 PIM-SM registreerimise peatamise teated

Kohtumispunkt RP üksikedastab PIM registreerimise peatamise (*PIM Register-Stop*) teated allikaga otseühendatud määratud marsruuterile (et ta lõpetaks (S,G) registreerimisteade saamise), kui on täidetud üks järgmistest tingimustest:

- RP hakkab saama multisaate pakette mööda allika S ja RP vahelist lühima tee puud;
- RP ei vaja vastava grupi liiklust, sest puudub aktiivne jagatud puu selle grupi jaoks.

7.2.8 PIM-SM määratud marsruuter

Eelnevalt (peatüki alguses) saime teada kuidas valitakse määratud ruuter mingis võrgusegmendis. Kui PIM-DM protokollis oli määratud ruuteril DR ainult IGMPv1 pärija roll, siis PIM-SM puhul on määratud ruuteril DR suurem tähtsus. Vaatleme joonisel 7-5 toodud olukorda.



Joonis 7-5. PIM-SM määratud ruuter [5].

PIM-SM ruuterid on ühendatud ühisesse võrgusegmenti, kus asub aktiivne multisaate grupi G vastuvõtja. Ainult määratud marsruuter DR (antud juhul ruuter A) peab saatma RP-le liitumise teateid, et ehitada grupi G jaoks jagatud puu. Kui mõlemad ruuterid saadaks (*,G) liitumisi kohtumispunktile, loodaks paralleelsed teed ja host A saaks multisaate liiklust dubleerituna.

Kui aga host A alustaks multisaate edastamist gruppi, siis DR (ruuter A) peab saatma PIM registreerimise teateid RP-le. Kui mõlemad ruuterid saadaks registreerimise teateid, siis saaks RP multisaate pakette topelt.

Kui määratud ruuter (ruuter A) lakkab töötamast, siis ruuter B märkab seda, kuna naabrussuhe ruuteriga A aegub ära. Sel juhul alustatakse uue määratud ruuteri valimise protsessi ja antud näites saaks selleks ruuter B, kes võtab ruuteri A ülesanded enda peale. Ruuter B juba teab, et kohtvõrgus leidub aktiivne vastuvõtja (host A), sest ka tema kuulis hosti saadetud IGMP liikmelisuse raportit ning saadab koheselt liitumise teate RP suunas. Peale seda hakkab multiedastus liikuma vastuvõtja suunas üle ruuteri B.

Kui host A oleks multisaate edastaja, siis järgmise paketi saamisel algatab ruuter B koheselt PIM registreerimise protsessi ja RP liitub host A lühima tee puuga üle ruuteri B.

7.2.9 PIM-SM kohtumispunktid

Kõik PIM-SM ruuterid peavad korrektseks töötamiseks teadma kohtumispunkti RP aadressi. Väikeses võrgus, kus kõikide multisaate gruppide jaoks kasutatakse sama kohtumispunkti, võime RP häälestada ruuterites käsitsi. Cisco ruuterites kasutatakse selleks käsku:

```
ip pim rp-address <aadress> [group-list <acl>],
```

kus valikulise parameetri “group-list” pääsuloendiga määratakse, millistele gruppidele antud kohtumispunkt on häälestatud.

Suurte võrkude korral või RP asukoha muutumiste korral muutub RP käsitsi häälestamine tülikaks. Lisaks on suurte võrkude puhul mõttekas kasutada erinevatel multisaate gruppidel erinevaid kohtumispunkte, et jagada viimaste koormust erinevatele ruuteritele ning ühtlasi ka optimeerida jagatud puid.

Cisco marsruuterid oskavad RP avastamiseks kasutada kahte mehhanismi:

- Cisco auto-RP;
- PIMv2 alglaadimisega ruuteri meetod BSR.

PIMv2 võttis kasutusele BSR mehhanismi, mis võimaldab PIM-SM marsruuteritel

dünaamiliselt teada saada grupp-RP vastavusi. Kuna PIMv2 oli alles visand, siis Cisco võttis oma PIM implementatsioonis kasutusele “auto-RP”, mis teeb sama asja. Viimase kasutamisel liituvad Cisco PIM ruuterid hästituntud multisaate grupiga “Cisco RP avastamine” (224.0.1.40), et saada grupp-RP vastavusi. Neid vastavusi edastavad sinna gruppi Cisco ruuterid, mis on konfigureeritud kaardistajaks (*Mapping Agent*). Kaardistajaid võib võrgus ka mitu olla, et tagada liiasust. Kaardistajad omakorda liituvad hästituntud multisaate grupiga “Cisco RP teadustamine” (224.0.1.39), et saada kätte võimalike RP kandidaatide kuulutused. RP kandidaadid teavitavad oma soovist olla mingi grupi või mitme grupi kohtumispunktiks “RP kuulutamise” (*RP Announce*) teadetega. Vaikimisi multiedastatakse neid teateid iga 60 sekundi tagant ning iga teade sisaldab ka kehtivuse (holdtime) väärtust (vaikimisi 180 sekundit), mis ütleb kui kaua on RP kuulutus kehtiv. Kaardistajad salvestavad grupp-RP vastavusi oma vahemällu (iga grupp-RP vastavuse kohta üks kirje, ka siis kui ühele grupile leidub mitu RP kandidaati). Kohtumispunkt valitakse kandidaatide IP aadressi põhjal. Suurima IP aadressiga kandidaat salvestatakse grupp-RP vastavuste vahemällu. Kaardistajad multiedastavad vahemälus olevad grupp-RP vastavused “RP avastamise” teadetes vaikimisi iga 60 sekundi tagant. Ka nendes teadetes kasutatakse kehtivuse parameetrit (vaikimisi 180 sekundit). Kui PIM ruuter ei saa “RP avastamise” teateid ja grupp-RP vastavus aegub, siis see ruuter lülitub ümber staatiliselt konfigureeritud kohtumispunktile. Kui kohtumispunkti staatiliselt häälestatud ei ole, siis edastatakse vastava grupi liiklust tihedat laadi režiimis.

Kohtumispunkti kandidaatideks võib seadistada ühe või mitu ruuterit järgneva globaalse režiimi käsuga:

```
ip pim send-rp-announce <liides> scope <ttl> [group-list <acl>],
```

kus liidesena kasutatakse sageli tagasisidestusliidest *Loopback* (siis on administraatoril lihtsam mõjutada kohtumispunkti valikut) ning grupp (või gruppide vahemik) määratakse pääsuloendiga. Kui valikuline parameeter “group-list” ära jätta, siis kuulutatakse ennast kõikide gruppide (224.0.0.0/4) kohtumispunktiks. Parameeter “scope” määrab RP kuulutuste ulatuse (levib vastava arvu hüpete kaugusele).

Näide 7-3. Ruuter kuulutab ennast RP kandidaadiks grupivahemikele 239.254.0.0 – 239.255.255.255 ja 224.0.0.0 – 231.255.255.255.

```
ip pim send-rp-announce loopback0 scope 16 group-list 10
access-list 10 permit 239.254.0.0 0.1.255.255
access-list 10 permit 224.0.0.0 7.255.255.255
```

Kaardistaja funktsioon käivitatakse ühes või mitmes ruuteris järgneva globaalse režiimi käsuga:

```
ip pim send-rp-discovery scope <ttl>.
```

Kaardistaja vahemälus olevaid grupp-RP kirjeid saame vaadelda käsuga:

```
show ip pim rp mapping.
```

Näide 7-4. Ruuteri “ak-gw” naaberruuteris grupp-RP kirjete vaatamine.

```
Router>sh ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 193.40.31.65 (ak-gw.ut.ee), v2v1
    Info source: 193.40.12.49 (ak-gw.ut.ee), elected via Auto-RP
    Uptime: 00:12:51, expires: 00:02:02
```

Antud näites on kõikide multiedastusgruppide kohtumispunktiks ruuter nimega „ak-gw“, aadressiga 193.40.31.65, mis on valitud auto-RP mehhanismiga.

7.2.10 PIMv2 alglaadimisega ruuteri meetod

Alglaadimisega ruuteri meetod BSR (*Bootstrap Router Method*) on oma nimetuse saanud sellest, et see tugineb ruuteril, mis algselt ujutab võrgu üle alglaadimise (*Bootstrap*) teadetega, et grupp-RP vastavused jõuaksid kõikide teiste ruuteriteni [5]. Nagu auto-RP puhulgi võib ühel multisaate grupil olla mitu RP kandidaati. Kandideerimiseks tuleb ruuteris anda käsk:

```
ip pim rp-candidate <liides> [group-list <acl>].
```

Ülaltoodud käsu sisestamisel hakkab ruuter üksikedastama PIMv2 kohtumispunktiks kandideerimise teateid hetkel kehtivale BSR ruuterile. Iga kuulutus sisaldab antud liidese IP aadressi (sageli kasutatakse tagasisidestusliidest) koos multisaate gruppidega, mis on määratud valikulise parameetri “group-list” pääsuloendiga. Kui viimane ära jätta, siis kuulutatud grupi vahemikuks on 224.0.0.0/4 ehk kandideeritakse kõikide multisaate gruppide kohtumispunktiks.

Näide 7-5. Ruuter kuulutab ennast RP kandidaadiks grupivahemikele 239.254.0.0 – 239.255.255.255 ja 224.0.0.0 – 231.255.255.255.

```
ip pim rp-candidate loopback0 group-list 10
access-list 10 permit 239.254.0.0 0.0.255.255
access-list 10 permit 239.255.0.0 0.0.255.255
access-list 10 permit 224.0.0.0 7.255.255.255
```

BSR funktsionaalsuse võime määrata ühele või mitmele BSR kandidaadile, kasutades järgmist globaalse režiimi käsku:

```
ip pim bsr-candidate <liides> <hash-mask-length> [prioriteet].
```

Selle käsu järgselt hakkab ruuter osalema BSR valimise protsessis, millest natuke hiljem. Kui ruuter osutub valituks, hakkab ta perioodiliselt (iga 60 sekundi järel) edastama BSR teateid kõikidesse liidestesse, kus asuvad PIMv2 naabrid. Need BSR teated sisaldavad järgmist informatsiooni:

- 1) kohtumispunkti RP aadress, mis on eelnevalt mainitud “bsr-candidate” käsus toodud liidesele vastav IP aadress;
- 2) RP räsi maski pikkus;
- 3) BSR prioriteet, mis on eelnevalt mainitud “bsr-candidate” käsus määratud valikulise parameetriga (vaikimisi kasutatakse 0, kui ei ole määratud);
- 4) kogu nimekiri kandidaatidest (RP-hulk), mis on teada saadud kõikidelt RP kandidaatidelt saadud kuulutamiste kaudu.

7.2.11 BSR valimine

BSR valitakse välja BSR kandidaatide hulgast. Valimisprotseduur on väga sarnane juurkommutaatori valimisele kommuteeritud võrkudes (täispuu protokoll). Valimisprotsess on järgmine:

- 1) kandidaat-BSR käivitab alglaadimise taimeri algse väärtusega 150 sekundit (*Bootstrap timeout*) ja ootab BSR teateid hetkel kehtivalt BSR ruuterilt;
- 2) kui ruuter saab eelistatud BSR teate (teates olev BSR prioriteet on kõrgem kui tema enda BSR prioriteet või võrdne prioriteet, kuid kõrgem BSR IP aadress), siis ta võtab selle vastu ja algseadistab alglaadimise taimeri 150 sekundile ning edastab teate kõikidesse teistesse liidestesse. Kui saadud teade ei ole eelistatud BSR teade, siis see visatakse minema;
- 3) kui alglaadimise taimer aegub, siis kandidaat-BSR eeldab, et tema ongi BSR ja hakkab perioodiliselt (iga 60 sekundi järel) kõikide liideste pealt välja saatma enda BSR teateid, kus on kirjas tema prioriteet ja RP-hulk;
- 4) kui ruuter on valitud BSR ja saab eelistatud BSR teate, siis see ruuter taandab ennast kandidaat-BSR ruuteriks ja protsess jätkub 1. sammuga.

7.2.12 BSR teadetega üleujutamine

BSR teateid multiedastatakse „kõik PIM ruuterid“ multisaate grupile (224.0.0.13) aega elada väärtusega (TTL) 1. Naaber PIMv2 ruuterid saavad BSR teated kätte ja taasedastavad need kõikide teiste liideste pealt TTL väärtusega 1. Niimoodi hüpete kaupa toimubki PIM domeeni üleujutamine BSR teadetega. Kuna BSR teated sisaldavad valitud BSR ruuteri IP aadressi, siis nii saavadki kandidaat-RP ruuterid teada valitud BSR IP

aadressi. See on vajalik, et kandidaat-RP ruuterid saaksid üksikedaastada oma kandideerimise kuulutusi valitud BSR-le.

Kandideerimise kuulutuse teateid saadetakse iga parameetri “C-RP-ADV-PERIOD” sekundi järel (vaikimisi 60 sekundit) ning iga kuulutus sisaldab ka säilitamise parameetrit “holdtime” (sekundites), mis annab BSR ruuterile teada kui kaua kuulutus kehtib. Vaikimisi on säilitamise ajaks 2,5 kordne kuulutamise intervall (150 sekundit).

7.2.13 RP valimine

Multisaate grupi jaoks kohtumispunkti valimisel kasutavad PIMv2 ruuterid räsifunktsiooni, mille sisenditeks on BSR teadetest saadud kandidaat-RP aadress C(i), grupi aadress G ja räsi mask M ning väljundiks on räsi.

$$F(G, M, C(i)) = (1103515245 * ((1103515245 * (G \& M) + 12345) \text{ XOR } C(i)) + 12345) \text{ mod } 2^{31} \quad [14].$$

Ruuter rakendab räsifunktsiooni antud grupi kõikidele kandidaatidele RP-hulgas ja vastava grupi G kohtumispunktiks saab väikseima räsiga kandidaat-RP. Kui kaks kandidaati annavad sama räsi, siis võitjaks valitakse suurema IP aadressiga kandidaat.

7.3 Hõre-tihe laadi PIM

Cisco võttis kasutusele veel ühe alternatiivse PIM liidese laadi – hõre-tihe laadi (*sparse-dense mode*) PIM [5], mis käivitatakse ruuteri liidesel järgmise käsuga:

```
ip pim sparse-dense-mode.
```

Sellisel juhul kasutab ruuter liidesel hõredat laadi multiedastust, kui ruuter omab edastatava multisaate grupi kohta RP infot (vastava grupi kohta leidub kirje grupp-RP vastavuste vahemälus). Kui edastatava multisaate grupi RP aadressi ei teata, siis kasutatakse tihedat laadi multiedastust. Hõre-tihe laadi kasutamine on ühtlasi ka eelistatuim PIM kasutusviis, sest võimaldab administraatoril multiedastamise laadi määrata pigem gruppide kaupa kui ruuteri liideste kaupa. Kui hallatava võrgu kõikides marsruuterites on kõik liidesed häälestatud hõre-tihe laadile, siis on administraatoril võimalik ühe ruuteri häälestamisega valida tihedat laadi ja hõredat laadi gruppe.

Oletame, et meie võrgus on ainult üks kandidaat-RP järgmise konfiguratsiooniga:

```
ip pim send-rp-announce loopback0 scope 16 group-list 10
access-list 10 permit 224.1.1.1.
```

See tähendab, et meie ruuter kandideerib kohtumispunktiks ainult multisaate grupile 224.1.1.1 ja kuna see on ainuke kandidaat-RP, siis ainult grupil 224.1.1.1 kasutatakse hõredat laadi ja kõikidel teistel tihedat laadi edastust. Sellist lähenemist on hea kasutada, kui administraator tahab arvutivõrgu üle viia tihedalt laadilt hõredale järk-järgult, tehes eelnevalt testgrupi peal kindlaks hõreda laadi korrektse töötamise. Arvutivõrgu täielikult üle viimiseks hõredale laadile, piisab ainult kandidaat-RP ruuteri(te) konfiguratsiooni muutmisest:

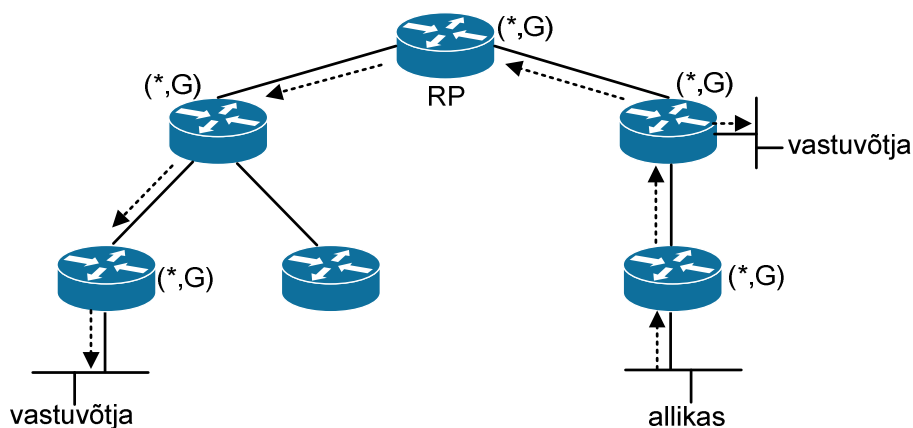
```
ip pim send-rp-announce loopback0 scope 16.
```

Valikulise parameetri “group-list” eemaldamine paneb ruuteri kandideerima kohtumispunktiks kõikidele multisaate gruppidele.

7.4 Kahesuunaline PIM

Kahesuunaline PIM (*Bidirectional PIM*) on PIM protokollide edasiarendus, et võimaldada efektiivselt mitu-mitmele suhtlust ühe PIM domeeni piires. Vastav Cisco poolt pakutud standard on kirjeldatud RFC-s 5015. Hõredat laadi PIM protokollide loodavad jagatud puud on ainult ühesuunalised ja seega allika liikluse toomiseks kohtumispunkti (jagatud puu juureni) kasutatakse lähtepuud. Kahesuunalise PIM korral kasutatakse liikluse edastamiseks ainult jagatud puud, mis on kahesuunalised ja juureks on vastava grupi kohtumispunkt RP.

Kahesuunaline PIM kasutab palju hõredat laadi PIM mehhanisme ja jagab lühima tee puu omadusi [15]. Allikate liiklus edastatakse tingimusteta ülesvoolu mööda jagatud puud ilma eelneva registreerimiseta nagu näidatud joonisel 7-6. PIM-SM ülesvoolu edastamist ei lubaks, sest pakette võetakse vastu ainult ühelt kohtumispunktini viiva lühima tee (RPF kontrolli põhjal) liideselt. Multisaate pakettide tsüklisse sattumise ära hoidmiseks on kasutusele võetud määratud edastaja DF valimine, mis aitab üles ehitada tsüklivaba lühima tee puu, mille juureks on kohtumispunkt.



Joonis 7-6. Kahesuunaline jagatud puu [15].

Sellised muudatused on vajalikud, et liiklust saaks edastada ainult (*,G) multisaate ruutimiskirjete põhjal. Selline omadus kaotab allika-spetsiifiliste olekute vajaduse ning protokoll skaleerub hästi suvalisele allikate arvule.

7.4.1 Määratud edastaja valimine

Igas võrgusegmendis ja punktist-punkti ühendusel valivad ruuterid määratud edastaja DF. See ruuter vastutab selle eest, et antud võrgusegmendist saadud multisaate paketid edastataks ülesvoolu kohtumispunktini RP. Iga kahesuunalise grupi kohtumispunkti kohta valitakse üks ruuter. Samas võib üks ruuter olla määratud edastajaks mitme liidese peal.

DF valitakse üksikedastuse marsruutimistabeli meetrikate põhjal ning viigi korral kasutatakse sama tehnikat mis PIM kinnitamise (*assert*) korral. Kohtumispunktini parima meetrikaga ruuter saab määratud edastajaks. Selle meetodi kasutamine kindlustab, et ainult üks paketi koopia jõuab RP-ni, isegi siis kui RP-ni leidub mitu võrdse maksumusega teed.

7.4.2 Kahesuunalise puu ehitamine

Kahesuunaline jagatud puu ehitatakse täpselt samuti kui hõredat laadi PIM puhulgi. Peamine erinevus on see, et määratud ruuteri DR rolli mängib määratud edastaja DF. Kui vastuvõtjatega kohtvõrgus ruuterid (kui neid on mitu) saavad IGMP liitumise, siis ainult määratud edastaja uuendab oma (*,G) ruutimiskirje väljuvate liideste nimekirja ning tegeleb vajadusel (*,G) liitumis- ja lahkumisteade saatisega ülesvoolu RP suunas. Kui ülesvoolu ruuter saab liitumis- või lahkumisteate ja ta ei ole määratud edastaja DF selle liidese peal, siis ta lihtsalt ignoreerib neid teateid. Vastasel juhul uuendatakse jagatud puud nii nagu hõredat laadi PIM puhulgi.

Võrgus, kus kõik ruuterid kasutavad kahesuunalisi jagatud puud ignoreeritakse (S,G) liitumis- ja lahkumisteateid. Ka ei ole vajalik PIM kinnitamise teadete saatmine, sest DF valimine välistab paralleelsete allavoolu teede tekkimise kohtumispunktist RP. Kohtumispunkt ei tegele puu ehitamisega allikani ega väljasta ka registreerimise peatamise teateid.

7.4.3 Pakettide edastamine

Kahesuunaliste puude korral kasutavad ruuterid ainult (*,G) ruutimiskirjeid, mille väljuvate liideste nimekiri sisaldab kõiki liideseid, millel ruuter on valitud määratud edastajaks ja on saanud kas IGMP või PIM liitumise teate. Ka ruuter, mis asub ainult saatmisega tegeleva multiedastaja harus tekitab endas (*,G) kirje, kuid selle väljuvate liideste nimekiri on tühi.

Kui saadakse multisaate pakett liideselt, mis asub tagasiteel kohtumispunkti (RPF kontrolli

põhjal), siis see edastatakse allavoolu vastavalt (*,G) ruutimiskirje väljuvate liideste nimekirjale. Teiste pakettide edastamisega ülesvoolu kohtumispunktile tegeleb ainult ruuter, mis on liidesel (kust pakett saadi) määratud edastaja ning kõik teised ruuterid peavad paketi ära viskama.

7.4.4 Kahesuunalise PIM käivitamine

Enne kahesuunalise PIM käivitamist tuleks veenduda, et antud võrgu piires kõik marsruuterid seda toetavad, sest osaliselt häälestatud võrgus tekivad koheselt marsruutimistsüklid.

Kahesuunalise PIM käivitamiseks tuleb globaalses režiimis sisestada käsk:

```
ip pim bidir-enable.
```

Järgnevalt tuleb määrata kohtumispunkt, kas staatiliselt või dünaamiliselt nagu PIM-SM puhulgi. Kohtumispunkti aadress ei pea olema füüsilise liidese aadress, vaid võib olla ka virtuaalne aadress omistatuna tagasisidestusliidesele. Lisaks sellele peab see aadress olema marsruuditud.

Staatiliselt määratakse kohtumispunkt järgmise käsuga:

```
ip pim rp-address <rp-aadress> [acl] bidir,
```

kus pääsuloend *acl* määrab aadressigrupid, mida käsitleme kahesuunalistena.

Kohtumispunkti infot võime jagada ka auto-RP funktsiooniga:

```
ip pim send-rp-announce <liides> scope <tvl> [group-list <acl>]  
[interval <intervall>] bidir,
```

kus valitud liidese IP aadress on kohtumispunkti IP aadressiks, valikulise parameetriga “group-list” määratakse multisaate grupid, mille kohtumispunktiks ennast kuulutatakse. Kuulutuste intervall on sekundites.

Kui soovime kasutada PIMv2 BSR mehhanismi, siis tuleb ruuterile anda käsk:

```
ip pim rp-candidate <liides> [group-list <acl>] bidir,
```

kus liidese nimega määratakse, millise IP aadressiga ruuter kohtumispunktiks kandideerib.

7.5 Allika-spetsiifiline multiedastus PIM-SSM

Allika-spetsiifiline multiedastus SSM (*Source Specific Multicast*) on IP multisaate laiendus, kus mingi grupi multisaate liiklust edastatakse saajatele ainult nendest allikatest, millega saaja on konkreetselt liitunud. Allika-spetsiifiline multiedastus ei ole standardiseeritud, kuid informatsiooni selle tehnoloogia kohta leiab RFC-st 3569. SSM edastust on hea kasutada üks-mitmele rakenduste puhul nagu audio ja video leviedastused. SSM vajab töötamiseks IGMPv3 olemasolu, sest see toetab allika filtreerimist. Cisco arendas välja ka kaks ülemineku lahendust: IGMP v3lite ja URD, mis võimaldavad kohest SSM teenuste kasutuselevõttu ootamata vastuvõtja poolse operatsioonisüsteemi ja rakenduste IGMPv3 toetatust [16]. Kuna IGMP v3lite ja URD ei ole IETF standardiseeritud ning on kasutatavad ainult Cisco IOS marsruuterites, siis nendel tehnoloogiatel siinkohal rohkem ei peatuks. Kuid soovi korral on lugejal võimalus nendega tutvuda Cisco dokumentatsioonidest.

Kui standardse multiedastuse puhul peab võrk teadma, millised on aktiivsed multiedastuse allikad, siis SSM puhul annavad selle info vastuvõtjad viimase hüppe ruuterile IGMPv3 protokolliga või IGMP v3lite või URD mehhanismiga. Standardse multiedastuse korral edastab suvaline hulk allikaid liiklust teatud grupile vastuvõtjatele (multisaate gruppi G) ning vastuvõtjad ei saa määrata, milliste allikate liiklust nad soovivad. SSM andmeedastus põhineb aga (S,G) kanalitel. Ühe (S,G) kanali liiklus koosneb üksikedastuse lähteadressist S ja sihtaadressiks on multisaate grupi aadress G. Vastuvõtjad saavad ainult nende kanalite liiklust, mida nad tellinud on. Kanalite tellimisel kasutatakse IGMPv3 INCLUDE tüüpi liikmelisuse raporteid. See aitab vältida ka teenusetõkestusründeid, sest standardse multiedastuse puhul võib gruppi edastama hakata suvaline allikas, mille liiklus hakkab võrku ning vastuvõtja ressursse koormama (häirides tegeliku allika edastuse vastuvõttu), sest vastuvõtja ei saa filtreerida allikaid.

SSM laiendab standardset multiedastust, mitte ei asenda seda ja saab seetõttu koeksisteerida tavalise multisaate võrguga. IANA on reserveerinud SSM rakenduste ja protokollide tarbeks aadresside vahemiku 232.0.0.0/8. Kuid Cisco ruuterite IOS tarkvara võimaldab kasutada suvalisi multiedastuse aadresside vahemikke. Kui vastuvõtja multisaate rakendused ei toeta (S,G) kanalite tellimist või URD lahendust, siis ta ei saa SSM vahemiku multiedastust.

SSM teenuseid saame käivitada võrkudes, mis kasutavad hõredat laadi PIM protokolliga. Kui me vajame ainult SSM teenuseid, siis piisab ruuterites ainult SSM häälestamisest ilma PIM-SM auto-RP või BSR mehhanismideta. Kui me paigaldame SSM juba olemasolevasse PIM-SM domeeni, siis ainult viimase hüppe ruuterid peavad toetama SSM ja teised ruuterid võivad kasutada PIM-SM protokolliga vastavate multisaate gruppide vahemikes.

Allika-spetsiifiline PIM käivitatakse globaalse režiimi käsuga:

```
ip pim ssm [default | range <acl>],
```

kus nurksulgudes oleva parameetriga määratakse ära vahemik, milles me SSM laadi kasutama hakkame. Sel käsul on ruuterile järgmine efekt:

- SSM vahemikus olevatele multisaate gruppidele võetakse (S,G) kanalite tellimusi IGMPv3 INCLUDE tüüpi liikmelisuse raportiga, IGMP v3lite või URD mehhanismiga (vastav meetod tuleb määrata administraatoril ruuteri liideste peal). IGMP v3lite ja URD mehhanismi ignoreeritakse väljaspool SSM vahemikku;
- SSM vahemikus olevate multisaate gruppide aadresside puhul kasutatakse PIM-SSM laadi. Selles laadis genereerib ruuter ainult PIM (S,G) liitumise ja pügamise teateid, (S,G,rpt) ja (*,G,rpt) teateid ei genereerita. Sissetulevaid jagatud puuga seotud toimingute teateid ignoreeritakse või lükatakse tagasi (reject) ja PIM registreerimisteadetele vastatakse koheselt registreerimise peatamise teatega. PIM-SSM on tagasiühilduv PIM-SM protokolliga, seega ruuterid, mis ei ole viimase hüppe ruuterid võivad SSM gruppide jaoks kasutada ka PIM-SM protokoll (näiteks kui nad veel ei toeta PIM-SSM protokoll);
- MSDP Source-Active (SA) teateid ei võeta vastu, ei genereerita ega edastata.

Lisaks peame käivitama vastavates võrgusegmentides PIM (*sparse* või *sparse-dense*) protokollis andes vastavatele liidestele korralduse:

```
ip pim {sparse-mode | sparse-dense-mode}.
```

Ning hostidega võrgusegmentides peame kasutama IGMPv3 protokollis või URD lahendust andes vastavatele liidestele käsu:

```
ip pim igmp version 3
```

või

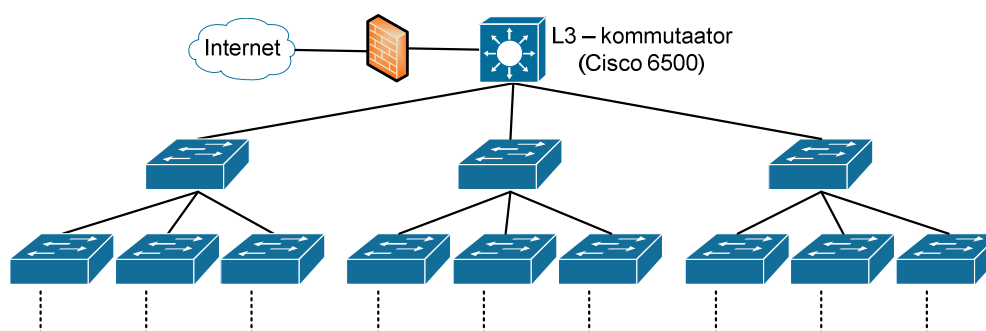
```
ip pim igmp v3lite
```

või

```
ip urd.
```

8 Multiedastus Tartu Ülikooli arvutivõrgus

Tartu Ülikooli arvutivõrk on arhitektuurilt kokkupandud magistraalvõrguga (*collapsed backbone*). Kõik võrgud koonduvad kokku ühte marsruuterisse, kus toimub kogu ülikooli võrgu marsruutimine. Tavaliselt on selleks keskseks marsruuteriks L3 funktsionaalsusega kommutaator. Tartu Ülikooli võrgus on selleks Cisco Catalyst 6500 seeria kommutaator (joonis 8-1).



Joonis 8-1. Kokkupandud magistraalvõrk.

Sellise arhitektuuriga võrk on väga kiire ja seda on lihtsam hallata. Kasutatakse palju ka virtaalseid kohtvõrke (*VLAN*), mis võimaldab sama töögrupi inimesi liita ühisesse kohtvõrku, kuigi nad paiknevad erinevates hoonetes. Samas on sellisel võrguarhitektuuril ka miinuseid: kogu koormus võrgus on koondatud keskele, kommuteeritud tsükli tekkimine mingis võrgusegmendis halvab kogu võrgu; keskse marsruuteri mittetöötamine põhjustab kogu võrgu mittetöötamise.

Ka multiedastust silmas pidades, oleks eelistatud võrguarhitektuuriks hierarhiline magistraalvõrk, mis võimaldaks erinevate multiedastusgruppide jaoks valida erinevaid kohtumispunkte kui me kasutame hõredat laadi PIM protokollit ja niimoodi magistraalvõrgu ruuterite koormust vähendada. Lokaalsed multiedastused ei koormaks magistraalvõrku, kui teistes majades vastava multiedastusgrupi liikmeid ei oleks.

8.1 Multiedastuse käivitamine ja testimine

Kokkupandud magistraalvõrgu korral ühenduvad kõikide majade kohtvõrgud keskse marsruuteri külge, seega asutuse siseseks multiedastuseks piisab selle ruuteri häälestamisest. Käivitasin TÜ keskses Cisco marsruuteris multiedastuse globaalse režiimi käsuga:

```
ip multicast-routing.
```

Seejärel käivitasin igal kohtvõrgu liidesel PIM protokoll, mis ühtlasi käivitas vastavatel liidestel ka IGMP protokoll. Kasutasin marsruuteri liidestel hõre-tihe laadi PIM protokoll käsuga (käsk antakse igale liidesele eraldi):

```
ip pim sparse-dense mode.
```

Vaikimisi käivitati liidestel IGMPv2, seda saame kontrollida käsuga:

```
show ip igmp interface <liides>.
```

Kuid soovi korral saame liidesel kasutatavat IGMP versiooni muuta käsuga

```
ip igmp version {3|2|1}.
```

Ruuteri liidestel jätsin kasutusele IGMPv2. Kuigi vaikimisi on tänapäeva Windows ja Linux operatsioonisüsteemides kasutusel IGMPv3. Kuid nad kohandavad kasutatavat versiooni vastavalt keskkonnale: kui host näeb võrgus IGMPv2 üldisi päringuid, siis ta hakkab ka automaatselt kasutama IGMPv2 raporteid.

Otsustasin kasutada kõikide multiedastuse gruppide marsruutimiseks hõredat laadi PIM protokoll, seega häälestasin järgmisena kohtumispunkti. Kuna meie topoloogias on ainult üks marsruuter, siis häälestasin kohtumispunkti RP staatiliselt:

```
ip pim rp-address 193.40.5.129.
```

Kuid testimiste käigus mitme ruuteriga katsetasin ka auto-RP funktsionaalsust, mis toimis suurepäraselt. Kui ruuter sai häälestatud, oli vaja üle kontrollida majade kommutaatorite seadistus. Enamike TÜ majade peakommutaatoriks on Cisco Catalyst 3550, 3560 või 3750 seeria kommutaator, millest edasi hargneb majasisene kommuteeritud võrk. Majasisesed võrgud on sõltuvalt teaduskondadest või struktuuriüksusest üles ehitatud kas Cisco Catalyst või HP Procurve kommutaatoritega. Lisaks sellele on väga palju mittehallatavaid kommutaatoreid, mis loomulikult ei tee multiedastusel ega leviedastusel vahet.

Cisco kommutaatorites on IGMP pealt kuulamine vaikimisi käivitatud. Seda on võimalik kontrollida käsuga

```
show ip igmp snooping,
```

mis näitab IGMP pealt kuulamise globaalset konfiguratsiooni, millele järgnevad seadistused iga VLANi kohta eraldi. Kui mingil põhjusel on IGMP pealt kuulamine välja

lülitatud, siis on seda võimalik sisse lülitada järgmise globaalse režiimi käsuga:

```
ip igmp snooping.
```

Selgus, et HP Procurve kommutaatorites on IGMP pealt kuulamine vaikimisi välja lülitatud, milles on võimalik veenduda käsuga:

```
show ip igmp.
```

Kui IGMP pealt kuulamine on välja lülitatud, siis kommutaator käsitleb multiedastuse kaadreid leviedastuskaadritena, mis tähendab seda, et kommutaatorisse sisenev kaader edastatakse kõikidesse portidesse (va sisenev port) edasi. Oletame nüüd, et sellise kommutaatori taga on 5 erinevat kasutajat, kes kõik vaatavad näiteks ülikooli arvutivõrgus pakutavat digitelevisiooni, igaüks erinevat TV kanalit. Kuna iga kanali kasutatav ribalaius on umbes 3 Mbit/s, siis kokku teeb see 15Mbit/s videovoogu, mis jõuab leviedastusena kõikide selle kommutaatori taga olevate arvutiteni olenemata sellest kas nad seda soovivad või mitte. Lisaks koormab mittesoovitud pakettide töötlemine ja ära viskamine arvutite protsessorit. Kõike eelnevat arvesse võttes, soovitan ka HP Procurve kommutaatorites IGMP pealt kuulamise käivitada. Selleks tuleb HP kommutaatoris igale VLAN konfiguratsioonile lisada käsk “ip igmp”.

Näide 8-1. HP Procurve kommutaatoris IGMP käivitamine.

```
configure terminal
    vlan <vlan-nr>
ip igmp
exit
```

Multiedastuse testimiseks on väga hea kasutada utiliiti “iperf”, mida on võimalik alla laadida nii Windowsile, Linuxile kui MacOS X-le. Näiteks liikluse edastamiseks aadressile 239.255.100.100 peame käivitama programmi “iperf” parameetritega:

```
iperf -c 239.255.100.100 -u -T 32 -t 100 -i 1
```

Näide 8-2. Edastame UDP liiklust gruppi 239.100.100.100 sekundilise raporteerimise intervalliga, 100-ks sekundiks, pakettide aega elada väärtusega 32.

```
iperf -c 239.100.100.100 -u -T 32 -t 100 -i 1
-----
Client connecting to 239.100.100.100, UDP port 5001
Sending 1470 byte datagrams
Setting multicast TTL to 32
UDP buffer size: 9.00 KByte (default)
-----
```

```

[ 3] local 169.254.201.232 port 58084 connected with 239.100.100.100 port 5001
[ ID] Interval          Transfer      Bandwidth
[ 3] 0.0- 1.0 sec        129 Kbytes   1.06 Mbits/sec
[ ID] Interval          Transfer      Bandwidth
[ 3] 1.0- 2.0 sec        125 Kbytes   1.02 Mbits/sec
[ ID] Interval          Transfer      Bandwidth
[ 3] 2.0- 3.0 sec        131 Kbytes   1.07 Mbits/sec

```

Vastuvõtmiseks peame käivitama programmi “iperf” parameetritega:

```
iperf -s -u -B 239.255.100.100 -i 1.
```

Näide 8-3. Võtame vastu UDP liiklust aadressilt 239.100.100.100, statistiliste raportitega iga sekundi tagant.

```

iperf -s -u -B 239.100.100.100 -i 1
-----
Server listening on UDP port 5001
Binding to local address 239.100.100.100
Joining multicast group 239.100.100.100
Receiving 1470 byte datagrams
UDP buffer size: 41.1 KByte (default)
-----
[ 3] local 239.100.100.100 port 5001 connected with 169.254.253.101 port 54422
[ ID] Interval      Transfer      Bandwidth      Jitter    Lost/Total Datagrams
[ 3] 0.0- 1.0 sec  129 Kbytes    1.06 Mbits/sec  0.080 ms   0/90 (0%)
[ ID] Interval      Transfer      Bandwidth      Jitter    Lost/Total Datagrams
[ 3] 1.0- 2.0 sec  128 Kbytes    1.05 Mbits/sec  0.109 ms   0/89 (0%)
[ ID] Interval      Transfer      Bandwidth      Jitter    Lost/Total Datagrams
[ 3] 2.0- 3.0 sec  128 Kbytes    1.05 Mbits/sec  0.171 ms   0/89 (0%)

```

Seejärel tegin esimesed videovoo edastamise testimised vabavaralise VLC multimeedia mängijaga, mis on alla laetav veebiaadressilt <http://www.videolan.org>. VLC on minu meelest üks parimaid meedia mängijaid, mis on võimeline mängima enamus audio ja video formaate (täpse loetelu võite leida VideoLAN kodulehelt) failist, füüsiliselt meedialt (DVD, video-CD, audio-CD), TV kaardilt või võrgust. Lisaks pakub VLC mängija palju erinevaid voogedastamise võimalusi.

Näiteks videofaili “video.avi” multiedastamiseks gruppi 239.255.100.100 võime Linuxi käsureal sisestada käsu[17]:

```
vlc "video.avi" --sout udp:239.255.100.100:5000 --ttl 2.
```

Sama saab teha ka Windowsi käsurealt või siis hoopis graafilise kasutajaliidese abiga. Antud käsk viskabki graafilise kasutajaliidese lahti. Kui te seda ei soovi, käivitage VLC deemonina, lisades käsule võtme “-d”. Kui soovite videofaili lõputult striimida, siis lisage ülaltoodud käsule parameeter „--loop”.

8.2 Digiteleviseiooni multiedastamine

Laiaulatuslikumaks testimiseks otsustasin hakata multiedastama tasuta levivaid digiTV kanaleid (ETV, KANAL2, TV3, TV11, ETV2) Tartu Ülikooli arvutivõrgus. Selleks otstarbeks ostsin pildil 8-1 oleva TV tuuneri “Avermedia Volar X USB”. See USB porti käiv tuuner on toetatud nii Windows XP/Vista/7, MacOS X kui ka Linux (alates 2.6.28 kernelist on draiver sisseehitatud) operatsioonisüsteemides. Spetsifikatsiooniga saate tutvuda Avermedia kodulehel <http://www.avermedia.com>.



Pilt 8-1. Avermedia Volar X USB TV tuuner.

Riistvaraliseks platvormiks valisin HP Compaq dc5700 MicroTower PC, millel on Intel Pentium 4 3,06GHz protsessor ja 2 GB RAM. Kuid ilmselt saab ka lihtsama arvutiga hakkama, sest kasutuskogemused näitavad, et masin seisab enamuse ajast jõude. Operatsioonisüsteemiks valisin Debian Squeeze distributsiooni.

Seejärel laadisin alla uusima TV tuuneri püsivara (*firmware*):

```
wget http://www.otit.fi/~crope/v41-dvb/af9015/af9015\_firmware\_cutter/firmware\_files/4.95.0/dvb-usb-af9015.fw.
```

Püsivara paigaldamine eeldas vähemalt 2.6.28 kerneli versiooni ja see nõue oli mul täidetud. Kopeerisin püsivara õigesse kataloogi:

```
sudo mv dvb-usb-af9015.fw /lib/firmware.
```

Televiseiooni voogedastamiseks otsustasin kasutada vabavaralist tarkvara MuMuDVB (*Multi Multicast DVB*). MuMuDVB on suuteline DVB allika (satelliit-TV, kaabel-TV, maapealse-TV) signaali voogedastama arvutivõrku multiedastuse või HTTP üksikedastuse

näol [18]. See tarkvara võimaldab transponderilt signaali vastu võtta ja panna iga kanali eraldi multiedastusgruppi. Samas on tarkvara vähese ressursivajadusega. Paigaldamiseks kasutasin Debiani pakihaldussüsteemi:

```
sudo apt-get install mumudvb.
```

Seejärel muutsin tarkvara käivitamise vaikeparameetreid failis “/etc/default/mumudvb”:

```
sudo vi /etc/default/mumudvb.
```

```
#Mumudvb init config file
#
# This file is used to specify the locations of mumudvb config
#files for each card
#
DONTSTARTMUMU=false

#If you want to launch a command before mumudvb (for example for
#automatic configuration generation)
#LAUNCH_BEFORE_MUMU=""

#Options for mumudvb
DAEMON_OPTS=""

#The user to launch mumudvb
DAEMONUSER=_mumudvb

#Change this line to reflect your configuration
#Ex : ADAPTERS="0 1 2 4"
ADAPTERS="0"

#Location of the config files
#Ex : MUMUDVB_CONF_1="/etc/mumudvb/card1.conf"
MUMUDVB_CONF_0="/etc/mumudvb/card0.conf"
```

Konfiguratsiooni jaoks tegin kataloogi “/etc/mumudvb” ja tekitasin sinna “card0.conf” nimelise faili järgmise sisuga [18]:

```
sudo vi /etc/mumudvb/card0.conf.
```

```

#----- TUNING -----
#The Transponder frequency
freq=626000
# ---- TERRESTRIAL (DVB-T) ----
#For DVB-T if the bandwidth is 8MHz you don't have to set other parameters
#----- AUTOCONFIGURATION -----
#We want the full autoconfiguration (ie we discover the channels and
#their pids)
autoconfiguration=2
#----- NETWORKING -----
#What is the "ip header"?
#The autoconfigured multicast ip have the form header.card.channelnumber
#The default header is 239.100
#autoconf_ip_header=239.10
#
#Do we want to change the default port (optional) ?
#common_port=4422
#
#Do we need to change the default multicast TTL (if you have routers,
#default value : 2) ?
multicast_ttl=10
#----- SAP ANNOUNCES -----
#The sap announces are sent automatically with full autoconfiguration
#Do we want NOT to send the announces ?
#sap=0
#
#What is the default playlist group for the SAP announces (optionnal) ?
sap_default_group=DigiTV
#Who is the organisation wich send the stream (optionnal) ?
#sap_organisation=m
#The interval between the SAP announces in second (default 5)
#sap_interval=10

```

Tartus peab TV tuuneri sageduseks määrama 626MHz [19]. Kanalite avastamiseks kasutasin automaathäälestust. Multiedastusaadresside prefiksi jätsin vaikeseadistusele ehk "239.100". Sel juhul kolmanda okteti väärtusena kasutatakse TV kaarti identifikaatorit (antud juhul 0) ja viimase okteti väärtuseks on TV kanali identifikaator. UDP pordi jätsin vaikimisi määratud 1234 peale. Kuna Eestis levib õhu kaudu 5 tasuta digiformaadis telekanalit, siis saan automaathäälestusena tabelis 8-1 näidatud multiedastusgrupid.

Tabel 8-1. Telekanalitele vastavad multiedastusgrupid, koos UDP pordi numbriga.

Kanali nr	IP aadress:port	Nimi
0	239.100.0.0:1234	ETV
1	239.100.0.1:1234	Kanal 2
2	239.100.0.2:1234	Kanal 11
3	239.100.0.3:1234	TV3
4	239.100.0.4:1234	ETV2

Suurendasin multiedastuse pakettide aega elada väärtuse 10-le, et leviks ka üle marsruuterite. Vaikimisi on multiedastuse sessioonide välja kuulutamine SAP (*Session Announcement Protocol*) protokolliga lubatud iga 5 sekundi tagant.

Sessioonide kuulutamise protokolliga on võimalik multiedastuse sessioonide kohta infot laiade jagada. SAP kuulutusi edastatakse üle UDP pordi 9875 multiedastusgruppi 224.2.127.254 aega elada väärtusega 255. SAP protokoll on kirjeldatud RFC-s 2974. Standardseks kuulutuse tüübiks on sessiooni kirjeldus SDP (*Session Description Protocol*) standardile vastavalt. SDP protokoll on kirjeldatud RFC-s 2327. Sessiooni kirjelduses on tavaliselt kirjas sessiooni nimi ja eesmärk, toimumise aeg, meedia tüüp ning vastuvõtmiseks vajalik info (aadressid, pordid, formaadid jne).

Kõige mugavam viis TÜ arvutivõrgus digiteleviseiooni vaatamiseks ongi VLC meedia mängijas SAP protokolliga käivitamine, mis tekitab mängija esitusloendisse eesti digikanalid. Selleks valige ülamenüüst “**Media → Teenuste kataloog → SAP announcements.**” Selle tulemusena liitub arvuti koheselt multiedastusgrupiga 224.2.127.254, et vastu võtta infot välja kuulutatud sessioonide kohta.

Seejärel avage oma esitusloend (ülamenüüst “**Vaade → Esitusloend**”), kuhu on ilmunud kataloog “SAP announcements”, mille peale klikkides ilmub kataloog “DigiTV”, milles asub eesti kanalite nimistu.

SAP kuulutuste vastuvõtmise seadistus unustatakse pärast meedia mängija sulgemist. Kuid seda on võimalik salvestada. Selleks valige ülamenüüst “**Tööriistad → Eelistused**”, eelistuste akna rubriigis “Kuva seaded” valige “Kõik”. Seejärel leidke vasakult “Esitusloend” alamenüüst “Services discovery”. Seal saate lisada linnukese kasti “SAP announcements” ning salvestage tehtud muudatus.

Digiteleviseiooni konkreetse kanali vaatamiseks võite avada voogedastuse ka otse, valides ülamenüüst “**Media → Ava voogedastus võrgust**”. Avanenud aknas valige protokolliks **UDP**, aadressilahtrisse kirjutage soovitud digikanalile vastav multiedastusgrupi aadress (vt tabel 8-1) ning pordi numbriks **1234** ja vajutage nupule **Play**.

Videovoogu on võimalik avada ka käsurealt, näiteks ETV kanali vaatamiseks tuleb sisestada käsk:

```
vlc udp://@239.100.0.0:1234.
```

VLC mängijal on huvitav omadus puhverdada vastuvõetavat videovoogu. See võimaldab telekanali vaatamise ajal pausi teha ja hiljem jätkata vaatamist pooleli jäänud kohast, kuigi arvutivõrk seda voogu enam ammu ei edasta.

Mõningatel klientidel esines probleeme multiedastuse vastuvõtmisega. Selgus, et neil masinatel oli mitu võrguliidest. Mõnikord võib võrguliides ka virtuaalne olla, mida tekitavad näiteks virtualiseerimistarkvarad *Vmware* ja *Virtualbox*. Kasutades *Wireshark* snifrit oli näha, et Windows saatis IGMP raporteid välja ainult ühe liidese pealt. Probleemi lahendas lisaliidese keelamine või hoopis liideste eelistusjärjekorra muutmine. Seda saab näiteks Windows Vistas ja Windows 7-s teha „**Control Panel → Network Connections → Advanced → Advanced Settings**“ menüüst.

8.3 Võrgutehnoloogia praktikumid Tartu Ülikoolis

Tartu Ülikool on liitunud ülemaailmse Cisco võrguakadeemia programmiga CNAP (*Cisco Networking Academy Program*), mis käivitus 1997. aastal ning millega on tänaseks liitunud üle 9000 akadeemia rohkem kui 165-st riigist. Lokaalse võrguakadeemiana on meil kasutada Cisco Systems poolt koostatud kaasaegsed CCNA (*Cisco Certified Network Associate*) õppematerjalid ning nende materjalide põhjal olen kokku pannud kaks TÜ Arvutiteaduse instituudis loetavat võrgutehnoloogia teemalist ainet:

- MTAT.08.003 – Võrgutehnoloogia I (6EAP);
- MTAT.08.004 – Võrgutehnoloogia II (6EAP).

Paraku ei käsitle kumbki neist aineist multiedastuse tehnoloogiat ja kuna Võrgutehnoloogia II aine praktikumideks lisaruumi on, siis otsustasin koostada praktikumilehed kahe praktikumi tarbeks. Esimene nendest käsitleb põhjalikumalt interneti grupi haldusprotokolle IGMP ning IGMP pealt kuulamist kommutaatoris ja teine praktikum keskendub rohkem multiedastuse marsruutimisele. Vastavad praktikumilehed on käesoleva magistritöö lisas.

Kokkuvõte

Antud magistritöö tulemusena valmis lugemismaterjal kõikidele arvutivõrgu spetsialistidele, kel on põhjalikum huvi multiedastustehnoloogia vastu. Töö annab ülevaate multiedastuse aadresseerimisest, erinevat liiki jaotuspuudest, millel multiedastuspakette edastatakse ning milliste kriteeriumite põhjal marsruuterid neid edastamisotsuseid teevad. Järgneb ülevaade multiedastusgrupi haldamisest hostide ja marsruuteri vahel, kasutades IGMP protokollid ning multiedastusgrupi haldamisest sageli nende vahele jäävas kommuteeritud võrgus olevates kommutaatorites, mis tegelevad IGMP protokollid pealt kuulamisega. Annan ülevaate ka asutuse võrgus kasutatavatest multiedastuse marsruutimisprotokollidest DVMRP ja PIM ning nende käivitamisest Cisco marsruuteritel.

Rakendasin saadud teadmisi TÜ arvutivõrgus, mis on nüüdsest multiedastusvõimeline ning käivitasin digitelevisiooni vaatamise võimaluse. Viimases peatükis annangi üldise ülevaate TÜ magistraalvõrgu arhitektuurist ning kuidas ma sellise arhitektuuri korral multiedastusteenuse käivitasin ning mõned olulised asjad, millele võiks tähelepanu pöörata. Seejärel tutvustan erinevaid võimalusi multiedastuse testimiseks programmi “iperf” abiga ja vabavaralise VLC multimeedia mängijaga. Järgnevalt kirjeldan kuidas ma alustasin õhu kaudu levivate digiformaadis tasuta telekanalite multiedastamist TÜ arvutivõrgus. Edastamiseks kasutasin vabavaralist tarkvara MuMuDVB ja digitelevisiooni kanalite vastuvõtmiseks soovitasin kasutada VLC multimeedia mängijat. Mitme kuu testimise tulemusel, millesse langes ka taliolümpiamängude periood, ei laekunud mulle ühtegi kaebust pildi seisma jäämise või kvaliteedi olulise halvenemise osas.

Kuna tegelen Tartu Ülikooli Arvutiteaduse instituudis ainete “Võrgutehnoloogia I” ja “Võrgutehnoloogia II” õpetamisega, mille õppeprogrammist puudub multiedastustehnoloogia, siis koostasid praktikumiülesannete lehed kahe praktikumi tarbeks, mida saan edaspidi kasutama hakata “Võrgutehnoloogia II” praktikumides.

Multicast in Computer Networks

Master thesis

Erkki Kukk

Abstract

IP multicast is a method of sending data packets to a group of interested receivers in a single transmission. It conserves bandwidth, saves server and network device resources and therefore it is wise to implement it on your enterprise networks. IP multicast is quite simple to configure on Cisco network devices but the true challenge is to understand what and why is going to happen in your network afterwards.

The purpose of this study was to get full understanding of intradomain multicast protocols, share the knowledge in the Estonian language and to implement it in the campus network of the University of Tartu. So the network can be ready for other multicast streams as well. For example, e-learning and live video broadcasts might benefit from it.

I am starting my thesis with general multicast topics, such as the multicast group concept, IP multicast addresses and Layer 2 multicast addresses. Thereafter I introduce the forwarding principles, distribution trees and protocol for managing multicast group membership. I also give an understanding how LAN switches handle IP multicast and which multicast routing protocols are suitable for use in enterprise networks. I also added some examples and configuration hints (based on Cisco devices) for better understanding.

The second part of my work gives a general overview of the backbone of the University of Tartu and how I implemented IP multicast on this network design. For testing purposes I used software like “iperf” and “VLC media player”, which are open source and very useful tools, and I introduce some multicast configuration verification commands on Cisco devices. After setting up IP multicast I started to stream Estonian digital terrestrial television channels over multicast. For this purposes I used Avermedia DVB-T tuner card and open source software MuMuDVB.

Finally, as a lecturer for subject “Network Technology II”, I made some practical worksheets on multicast technology, which I will be using in the future practice labs.

As a result of my research, the network in the University of Tartu is multicast capable. The two months testing period showed that the network was handling multicast very well and turned out to be stable.

Kirjandus

- [1] The Internet Protocol Journal, “Reliable Multicast Protocols and Applications”, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-2/reliable_multicast.html, 23.05.2010.
- [2] Cisco Technology White Paper, „Guidelines for Enterprise IP Multicast Address Allocation“, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/ps6592/prod_white_paper0900aecd80310d68.pdf, 24.05.2010.
- [3] „RFC 2770, GLOP Addressing in 233/8“, <http://www.ietf.org/rfc/rfc2770.txt>, 24.05.2010.
- [4] “RFC 3138, Extended Assignments in 233/8“, <http://www.ietf.org/rfc/rfc3138.txt>, 24.05.2010.
- [5] Beau Williamson. „Developing IP multicast Networks“. CiscoPress, 2000.
- [6] Cisco Technology White Paper, „IP multicast Technology Overview“, http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.pdf, 24.05.2010.
- [7] „RFC 2365, Administratively Scoped IP Multicast“, <http://www.ietf.org/rfc/rfc2365.txt>, 24.05.2010.
- [8] „RFC 1112, Host Extensions for IP Multicasting“, <http://www.ietf.org/rfc/rfc1112.txt>, 24.05.2010.
- [9] „RFC 2236, Internet Group Management Protocol, Version 2“, <http://www.ietf.org/rfc/rfc2236.txt>, 24.05.2010.
- [10] „RFC 3376, Internet Group Management Protocol, Version 3“, <http://www.ietf.org/rfc/rfc3376.txt>, 24.05.2010.
- [11] „Multicast in a Campus Network: CGMP and IGMP snooping“, http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a00800b0871.shtml#cgmp, 24.05.2010.
- [12] „Distance Vector Multicast Routing Protocol“, <http://tools.ietf.org/html/draft-ietf-idmr-dvmrp-v3-11>, 24.05.2010.
- [13] Cisco IOS Configuration Guide, „PIM Dense Mode State Refresh“, http://www.ciscosystems.lt/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_pim_dense_rfrsh_xe.pdf, 24.05.2010.
- [14] „RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)“, <http://www.ietf.org/rfc/rfc4601.txt>, 24.05.2010.
- [15] Cisco IOS Configuration Guide, „Configuring Bidirectional PIM“, http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbipim.pdf, 24.05.2010.
- [16] Cisco Configuration Guide, „Configuring Source Specific Multicast“, http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_cfg_ssm.pdf,

24.05.2010.

[17] VideLAN Wiki Documentation: Streaming Howto,

http://wiki.videolan.org/Documentation:Streaming_HowTo, 24.05.2010.

[18] MumuDVB tarkvara veebileht, <http://mumudvb.braice.net>, 24.05.2010.

[19] Levira saatejaamade tabel, <http://www.levira.ee/dyna/site/saatejaamad.pdf>,
24.05.2010.

Mõisted

- **ADSL** (*Asymmetric Digital Subscriber Line*) – asümmeetriline digitaalne abonendiliin. Tehnoloogia andmeedastuseks üle tavaliste telefoniliinide. Sõna "asümmeetriline" ehk ebasümmeetriline viitab sellele, et ADSL-i andmekiirused allavoolu ja ülesvoolu on erinevad;
- **ASIC** (*Application Specific Integrated Circuit*) – rakendus-spetsiifiline mikroskeem. Mingiks kindlaks otstarbeks, näiteks andmesideprotokolli, digikaamera või elektronmärkmiku jaoks projekteeritud kiip (pooljuht-mikroskeem);
- **BPDU** (*Bridge Protocol Data Unit*) – täispuuprotokolli andmeüksus, mis kirjeldab kommutaatori pordi atribuute nagu MAC aadress, prioriteetsus ja lingi maksumus. Sillaprotokolli andmeüksused võimaldavad täispuuprotokollis osalevatel kommutaatoritel koguda üksteise kohta;
- **CAM** (*Content Addressable Memory*) – assotsiatiivmälu. Mälukiip, milles iga bitikohta saab võrrelda. Tavalises dünaamilises muutmälus (DRAM) ja staatilises muutmälus (SRAM) adresseeritakse sisu bitiasukoha järgi ja siis kantakse sisu võrdlemiseks üle protsessori aritmeetika-loogikaplokki. CAM-kiipides võrreldakse sisu igas bitirakus, mis teeb võimalikuks väga kiired tabeliotsingud. Kuna võrreldakse kogu kiipi, siis on sageli lubatud andmeid salvestada juhuslikult, ilma et oleks vaja arvesse võtta adresseerimisskeemi. Paraku on CAM-kiipide mälu maht tunduvalt väiksem kui tavalistel mälukiipidel;
- **CBT** (*Core Based Trees*) – multiedastuse marsruutimisprotokoll, mis kasutab andmete edastamiseks jagatud juurega puud. Seda juurt nimetatakse ka tuumaks;
- **CGMP** (*Cisco Group Management Protocol*) – Cisco kommutaatorites ja marsruuterites kasutatav multiedastusgruppide haldusprotokoll;
- **DVB** (*Digital Video Broadcasting*) – digitaaltelevisioon, Euroopa Telekommunikatsiooni Standardite Instituudi (ETSI – European Telecommunications Standards Institute) poolt standardiseeritud digiteleviseiooni spetsifikatsioon satelliit-, kaabel- ja maapealse televisiooni jaoks;
- **DVMRP** (*Distance Vector Multicast Routing Protocol*) – kaugusvektoriga multiedastuse marsruutimisprotokoll, sarnaneb RIP protokolliga;
- **EIGRP** (*Enhanced Interior Gateway Routing Protocol*) – Cisco firmaomane klassideta kaugusvektoriga marsruutimisprotokoll. Täiustatud IGRP marsruutimisprotokoll;
- **HSRP** (*Hot Standby Routing Protocol*) – kuuma ooteseisundiga marsruutimisprotokoll, mis tagab marsruuteri varundamise selle tõrke korral. HSRP protokoll kasutamisel on marsruuterid ühendatud Etherneti, FDDI või lubaringvõrgu ühe ja sama segmendiga ning töötavad koos, nii et jääb mulje nagu oleks kohtvõrgus üksainus virtuaalne marsruuter. Kõigil marsruuteritel on sama virtuaalne IP ja

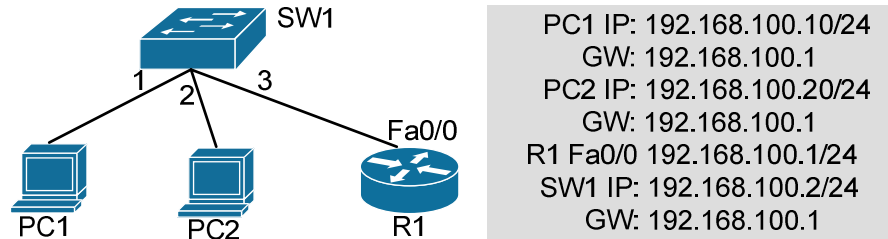
- MAC aadress, nii et kui üks marsruuter langeb rivist välja, siis kohtvõrku ühendatud hostid saavad jätkata pakettide edastamist samale IP ja MAC aadressile;
- **IANA** (*Internet Assigned Number Authority*) – üksus, mis korraldab ülemaailmselt IP aadresside jaotamist, domeeninimede süsteemi juurtsooni haldamist ja hoolitseb muude IP protokolliga seotud ülesannete lahendamise eest;
 - **IEEE** (*Institute of Electrical and Electronics Engineers, Inc*) – Elektri- ja Elektroonikainseneride Instituut. Ameerika Ühendriikides asuv maailma suurim erialaühing, mis asutati 1884 ja kuhu kuulub üle 320 tuhande liikme 147 riigist. IEEE toetab ülemaailmseid tehnikakonverentse ja seminare ning avaldab ligi 25% kõigist tehnilistest artiklitest elektrotehnika, elektroonika, arvutiehituse ja arvutiteaduse alal, pakub oma liikmetele täiendõppe programme ning toetab standardiseerimist. IEEE tegeleb lennunduse ja kosmosetehnikaga, arvutite ja sidega, biotehnoloogiaga, elektrotehnika ja elektroonikaga;
 - **IETF** (*Internet Engineering Task Force*) – Internetiehituse tööriühm. Peamine Interneti standardite alane organisatsioon. IETF on suur avatud rahvusvaheline ühendus, kuhu kuuluvad võrkude projekteerijad, operaatorid, teenusepakkujad ja teadlased, keda huvitab Interneti arhitektuuri areng ja Interneti tõrgeteta töö;
 - **IGMP** (*Internet Group Management Protocol*) – internetirühma haldusprotokoll. IP protokollide laiendus, mida kasutavad arvutid, et teavitada lokaalvõrgu marsruutereid oma kuuluvusest konkreetsesse multiedastuse gruppi;
 - **IGRP** (*Interior Gateway Routing Protocol*) – klassidega kaugusvektoriga marsruutimisprotokoll, mille meetrika koosneb sellistest komponentidest nagu ribalaius, koormus, viivitus ja usaldusväärsus;
 - **MAC** (*Media Access Control*) aadress – meediumipöörduse juhtimise aadress. Kohtvõrgus (või mõnes muus võrgus) on MAC aadress teie arvuti võrgukaardile tootja poolt omistatud unikaalne riistvaranumber;
 - **MASC** (*Multicast Address Set-Claim*) – protokoll, mida marsruuterid kasutavad multiedastusaadresside vahemiku liisimiseks oma domeeni tarbeks;
 - **MBGP** (*MultiProtocol Border Gateway Protocol*) – välislüüsi marsruutimisprotokollile BGP on lisatud erinevate protokollide toetus (Ipv6, IPX jne). See võimaldab ruuteritel paralleelset vahetada nii üksikedastuse kui ka näiteks multiedastuse topoloogiat;
 - **MOSPF** (*Multicast Extensions to OSPF*) – OSPF marsruutimisprotokoll, millele on lisatud multiedastuse toetus;
 - **MSDP** (*Multicast Source Discovery Protocol*) – PIM perekonda kuuluv multiedastuse marsruutimisprotokoll, mis ühendab omavahel mitu hõredat laadi PIM (PIM-SM) domeeni, võimaldades domeenidevahelist multiedastust;
 - **OSI** (*Open Systems Interconnection*) – avatud süsteemide sidumise arhitektuur. OSI on ISO ja ITU-T koostöös 1977 aastal valminud andmesideprotokollide kontseptuaalne mudel. OSI 7-kihilise arhitektuuriga baasmudel annab loogilise struktuuri konkreetsetele andmesidevõrkude standarditele;

- **OSPF** (*Open Shortest Path First*) – autonoomse süsteemi piires opereeriv siselüüsi marsruutimisprotokoll. On teadlik kogu võrgu linkide olekutest ning parima tee leidmisel kasutatakse linkide maksumust;
- **OUI** (*Organizationally Unique Identifier*) – 24-bitine prefiks MAC aadressis, mis identifitseerib vastava võrguseadme tootja, müüja vms organisatsiooni;
- **PIM** (*Protocol Independent Multicast*) – protokollist sõltumatu multiedastuse marsruutimisprotokoll, mis ei halda ise marsruutimisprotokoll, vaid kasutab edastamisotsuste tegemisel üksikedastuse marsruutimistabeleid;
- **RFC** (*Request For Comments*) – kommentaarinõue. Interneti kohta käivate dokumentide seeria, mille koostamist IETF alustas 1969. Kommentaarinõuete projekte võib IETF-le saata igal ajal ning IETF saadab need tutvumiseks asjast huvitatud osapooltele. Kui RFC muutub piisavalt populaarseks, võib sellest saada Interneti standard. Iga kommentaarinõudele omistatakse oma RFC number. Pärast avaldamist RFC enam ei muutu, vaid täiendatud ja parandatud RFC saab uue numbri;
- **RIP** (*Routing Information Protocol*) – kaugusvektoriga marsruutimisprotokoll. Andmete edastamiseks parima raja valikul arvestatakse hüpete arvu;
- **RP** (*Rendezvous Point*) – kohtumispunkt ehk jagatud juurega puu juur, kuhu multiedastuse allikad edastavad oma liikluse, mis edastatakse mööda puud vastuvõtjateni;
- **RPF** (*Reverse Path Forwarding*) – multiedastuse marsruutimisel kasutatav tehnika, millega tagatakse tsüklite-vaba pakettide edastus;
- **SAP** (*Session Announcement Protocol*) – multiedastuse sessioonide kuulutamise protokoll;
- **SDP** (*Session Description Protocol*) – multimeedia sessiooni kirjeldamise protokoll, mis annab lõpp-punktidele teada meedia tüübi, formaadi jm vajalikud omadused;
- **SDR** – sessioonikataloogi vahend (*Session Directory Tool*), mida kasutatakse Mbone multiedastuse konverentside välja kuulutamiseks ja nendega liitumiseks;
- **SNMP** (*Simple Network Management Protocol*) – lihtne võrguhalduse protokoll arvutite, marsruuterite, kommutaatorite jt võrguseadmete haldamiseks;
- **SSM** (*Source Specific Multicast*) – allika-spetsiifiline multiedastus, kus vastuvõtjatel on võimalik määrata, millisest grupist ja millistelt allikatelt multiedastus vastu võetakse;
- **STP** (*Spanning Tree Protocol*) – täispuuprotokoll. Võrguprotokoll, mis tagab sillatud kohtvõrgus silmustevaba topoloogia;
- **TCP** (*Transmission Control Protocol*) – edastusohje protokoll. Levinuim võrgu transpordikihi protokoll, mida kasutatakse Etherneti võrkudes ja Internetis. TCP on ühendusega edastuse protokoll, mis tagab töökindla sideühenduse ja andmevoo reguleerimise kahe osapoole vahel;
- **TTL** (*Time To Live*) – eluiga. Ettemääratud ajavahemik, mille vältel andmepaketil lubatakse võrgus liikuda, enne kui see kõrvale heidetakse;

- **UDP** (*User Datagram Protocol*) – kasutaja datagrammi protokoll. Ühenduseta sideprotokoll, mis erinevalt TCP-st ei taga töökindlat sideühendust ega reguleeri andmevoogu. Kui võrgust saabub datagrammideks jagatud sõnum, siis UDP datagramme ei reasta. See tähendab, et UDP-d kasutav rakendusprogramm peab ise suutma kontrollida, kas kogu sõnum on kohale jõudnud ja kas datagrammid on õiges järjestuses. OSI kontekstis asub UDP nagu ka TCP neljandas ehk transpordikihis;
- **URD** (*URL Rendezvous Directory*) – IGMPv3 protokollile ülemineku lahendus, kus marsruuter otsib HTTP liiklusest (S,G) kanalite tellimusi ning kui ruuter saab minuti jooksul vastavalt kliendilt ka (*,G) liitumise, siis ruuter liitub vastava grupi allika(te)ga;
- **VLAN** (*Virtual LAN*) – virtuaalkohtvõrk. Loogiliselt sõltumatu kohtvõrk. Ühe füüsilise silla taga võib olla korraga mitu virtuaalkohtvõrku;
- **WAN** (*Wide Area Network*) – laivõrk. Arvutivõrk, mis kasutab järjestikliine ja mille ulatus ületab 1 km.

Lisa 1. IGMP ja IGMP pealt kuulamine

Topoloogia



1. Ühenda seadmed nii nagu näidatud topoloogial ning häälesta IP aadressid vastavalt adresseerimisskeemile arvutites, kommutaatoris ja marsruuteris.

2. Testi ühendusi, pingides arvutitest ruuteri ja kommutaatori aadressi.

3. Sisesta kommutaatori käsureale käsk **show ip igmp snooping**

Kas IGMP pealt kuulamine on lubatud?

4. Käivita mõlemas arvutis *Wireshark* nimeline programm ja alusta pakettide kinnipüüdmist. Võite kasutada ka filtreid.

5. Alusta arvutis PC1 multisaate pakettide edastamist kasutades selleks **iperf** nimelist programmi järgmiste võtmetega:

```
iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1
```

Hiljem uuri, mis need võtmed tähendavad ja mis võimalused veel on olemas.

6. Kas PC1 edastus jõuab arvutisse PC2? Ja miks?

7. Anna kommutaatorile käsk **show ip igmp snooping groups**

Miks on väljund tühi?

a) Sisesta kommutaatorile käsk **show ip igmp snooping querier** ja **show ip igmp snooping mrouter**

8. Käivita marsruuteris multiedastuse marsruutimine globaalse režiimi käsuga

```
ip multicast-routing
```

ja Etherneti liidesel tihedat laadi PIM protokoll liidesele antava käsuga

```
ip pim dense-mode
```

9. *Wireshark* aknas peaksid nägema IGMP üldist päringut.

Vaata selle paketi IP aadresse ja MAC aadresse.

Kas keegi vastab sellele omapoolse raportiga ja miks?

9.1 Sisesta uuesti kommutaatorile käsk **show ip igmp snooping querier** ja **show ip igmp snooping mrouter**

10. Alusta uuesti arvutis PC1 multisaate pakettide edastamist:

```
iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1
```

11. Kas PC1 edastus jõuab arvutisse PC2? Ja miks?

12. Sisesta kommutaatori käsureale käsk **show ip igmp snooping groups**

13. Liitu arvutist PC2 grupiga 239.100.100.100, kasuta selleks iperf programmi järgmiste võtmetega:

iperf -s -u -B 239.100.100.100 -p 5000 -i 1

14. *Wireshark* aknas peaksid nägema PC2 poolt saadetud IGMP raportit.

Vaata selle paketi IP aadresse ja MAC aadresse.

15. Võid lisada ka marsruuteri grupi 239.100.100.100 liikmeks käsuga:

ip igmp join-group 239.100.100.100

Seejärel sisesta ruuteris käsk **show ip igmp membership**

Võid uurida ka silumiskäske **debug ip igmp** ja **debug ip packet**

16. Sisesta marsruuteris käsk:

show ip igmp interface FastEthernet 0/0

Millist IGMP versiooni vaikesel kasutatakse?

17. Muuda see IGMPv3-ks liidesele antava käsuga:

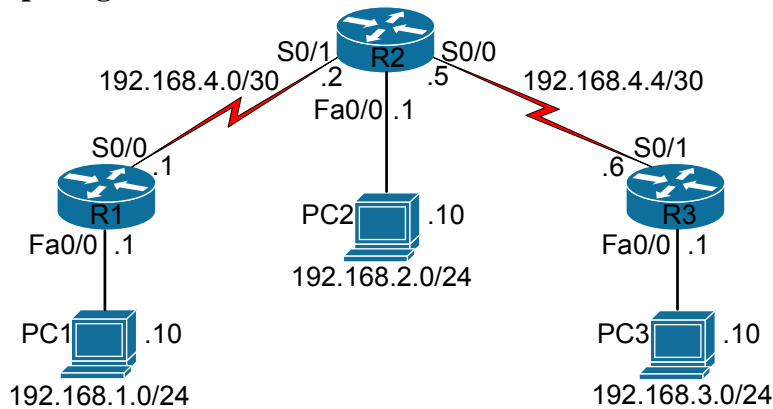
ip igmp version 3

18. Vaata *Wireshark* aknas, kas ka arvuti vahetab kasutatavat IGMP versiooni?

19. Muuda IGMP versioon tagasi IGMPv2 peale, kas ka arvuti vahetab kasutatavat IGMP versiooni?

Lisa 2. Hõre-tihe laadi PIM protokoll (PIM sparse-dense)

Topoloogia



1. Ühenda seadmed nii nagu näidatud topoloogial ning häälesta IP aadressid vastavalt adresseerimisskeemile arvutites ja marsruuterites.
2. Käivita marsruuterites EIGRP marsruutimisprotokoll ning lülitage marsruutide summeerimine välja (**no auto-summary**).
3. Testi ühendusi, pingides arvutist teisi arvuteid.
4. Käivita kõikides marsruuterites multiedastus globaalse režiimi käsuga
ip multicast-routing
5. Käivita kõikide ruuterite kõikidel liidestel hõre-tihe laadi PIM protokoll
ip pim sparse-dense-mode
6. Kuna kohtumispunkti RP ei ole määratud, siis kasutatakse kõikide multiedastusgruppide edastamiseks tihedat laadi PIM protokoll. Veendu selles, vaadates multiedastuse marsruutimiskirjeid käsuga **show ip mroute**
show ip pim rp
show ip mroute
7. Alusta arvutist PC2 multisaate pakettide edastamist:
iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1
8. Vaata vastava grupi marsruutimiskirjet ruuterites. Millist PIM laadi kasutatakse?
9. Alusta teistes arvutites multiedastuse vastu võtmist:
iperf -s -u -B 239.100.100.100 -p 5000 -i 1
Vaata uuesti marsruutimiskirjeid ja nende sisenevaid/väljuvaid liideseid.
10. Määra igas ruuteris kohtumispunkt RP staatiliselt globaalse režiimi käsuga
ip pim rp-address 192.168.2.1
11. Alusta seekord arvutist PC1 multisaate pakettide edastamist:
iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1
12. Alusta taas teistes arvutites multiedastuse vastu võtmist:
iperf -s -u -B 239.100.100.100 -p 5000 -i 1
Vaata uuesti marsruutimiskirjeid ja nende sisenevaid/väljuvaid liideseid.
Edastamiseks kasutatakse hõredat laadi PIM protokoll.
13. Eemalda marsruuteritest R1 ja R3 staatiline RP konfiguratsioon:

no ip pim rp-address 192.168.2.1

14. Alusta arvutist PC2 multisaate pakettide edastamist:

iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1

ja proovi teistest arvutitest vastu võtta:

iperf -s -u -B 239.100.100.100 -p 5000 -i 1

Ei tööta? Miks?

15. Eemalda ka ruuterist R2 staatiline RP konfiguratsioon:

no ip pim rp-address 192.168.2.1

16. Käivita marsruuterites auto-RP funktsionaalsus multiedastusgrupi vahemikule 239.100.100.0/24

a) Selleks lisa ruuteritele tagasisidestusliidesed:

Ruuter	Liides	IP aadress	Võrgumask
R1	Loopback 0	172.16.1.1	255.255.255.0
R2	Loopback 0	172.16.2.1	255.255.255.0
R3	Loopback 0	172.16.3.1	255.255.255.0

b) Käivita ka Loopback liidestel hõre-tihe laadi PIM

ip pim sparse-dense-mode

c) Lisa EIGRP konfiguratsiooni vastavad võrgud

d) Kuuluta näiteks ruuter R3 kohtumispunkti kandidaadiks gruppidele 239.100.100.0/24

ip pim send-rp-announce Loopback0 scope 4 group-list 1

ip pim send-rp-discovery Loopback0 scope 4

access-list 1 permit 239.100.100.0 0.0.0.255

e) Teistes ruuterites käivita ainult kaardistaja

ip pim send-rp-discovery Loopback 0 scope 4

17. Kontrolli ruuterites grupp-RP vastavusi käsuga

show ip pim rp

18. Alusta arvutist PC3 multisaate pakettide edastamist gruppi 239.100.100.100:

iperf -u -c 239.100.100.100 -p 5000 -T 10 -t 120 -i 1

19. Alusta teistes arvutites multiedastuse vastu võtmist:

iperf -s -u -B 239.100.100.100 -p 5000 -i 1

Vaata uuesti marsruutimiskirjeid ja nende sisenevaid/väljuvaid liideseid.

Veendu, et kasutatakse hõredat laadi PIM protokoll.

20. Alusta arvutist PC1 multisaate pakettide edastamist gruppi 239.100.200.1:

iperf -u -c 239.100.200.1 -p 5000 -T 10 -t 120 -i 1

21. Alusta teistes arvutites multiedastuse vastu võtmist:

iperf -s -u -B 239.100.200.1 -p 5000 -i 1

Vaata uuesti marsruutimiskirjeid ja nende sisenevaid/väljuvaid liideseid.

Veendu, et kasutatakse tihedat laadi PIM protokoll.

22. Võid proovida ka kahe ruuteri kohtumispunktiks kandideerimist. Mille põhjal RP valitakse?