KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Kim Vuorela

RYHMÄLÄHETYSTEN UUDET MENETELMÄT

Opinnäytetyö 2013

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

VUORELA, KIM	Ryhmälähetysten uudet menetelmät
Opinnäytetyö	48 sivua
Työn ohjaaja	yliopettaja Martti Kettunen
Toimeksiantaja	KYMP Oy
Huhtikuu 2013	
Avainsanat	IGMP, MLD, MLDP, multicast

Verkoissa tapahtuva liikenne kasvaa päivittäin valtavasti, mikä kuluttaa suuria määriä tietoliikennekapasiteettia. Liikenteen valtavan kuorman tasaamiseksi on kehitetty erilaisia ryhmälähetysprotokollia, joiden tehtävänä on vähentää tätä kuormaa. Ryhmälähetyksellä tarkoitetaan multicast-kehyksen lähettämistä yhdelle erikseen määritetylle ryhmälle, johon vastaanottajat voivat halutessaan liittyä. Ryhmälähetysprotokollien avulla mahdollistetaan datanjakelun kohdistamisen tehokkuus.

Tämän työn tarkoituksena oli perehtyä eri ryhmälähetys- eli multicast-protokolliin sekä niiden tapaan toimia osana IPv4- ja IPv6-verkkoa. Teoriaosuuden on tarkoitus antaa mahdollisimman kokonaisvaltainen ja selkeä kuvaus siitä, miten ryhmälähetys toimii. Erityisesti työn tarkoituksena oli tutustua uusiin ryhmälähetysmenetelmiin, jotka tarvitsevat uusia yhteyskäytäntöjä varsinkin siirryttäessä IPv6-protokollien käyttöön. Teoriaosuuden lisäksi tavoitteena oli saada rakennettua toimiva testikytkentä Kymenlaakson ammattikorkeakoulun laboratoriotiloissa ryhmälähetystekniikoihin perehtymistä varten.

Työtä varten rakennettiin IPTV-jakelutilannetta mallintava reititin- ja kytkinverkko. Datan lähteenä käytettiin joko oikean IPTV-operaattorin verkossa olevaa palvelua tai sitä mallintavaa omaa videopalvelinta. Videoliikenne ohjattiin testiverkon läpi asiakkaan lähiverkossa olevalle tietokoneelle, jota pitkin saapuva data kohdistettiin yhdelle päätteelle. Tässä testiympäristössä verkon osaksi liitettiin IPv4:ää sekä IPv6:tta tukevia ryhmälähetysprotokollia.

Työssä käytettyjen protokollien toimesta verkko todettiin toimivaksi. Kuitenkin tässä opinnäytetyössä esiintyvät protokollat ovat vain osa kaikista tarjolla olevista ryhmälähetys-protokollista. Mittavampien testituloksien saamiseksi testiympäristön olisi käsitettävä useita reititin- ja kytkinlaitteita, jotta ryhmälähetysprotokollien käyttäytyminen, sekä todellinen tehokkuus joutuisivat varsinaiseen testiin. Kuitenkin näiden testien avulla päästiin jo lupaaviin testituloksiin protokollien toiminnallisuudesta.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Information Technology

VUORELA, KIM	New Applications of Multicast
Bachelor's Thesis	48 pages
Supervisor	Principal Lecturer Martti Kettunen
Commissioned by	KYMP Oy
April 2013	
Keywords	IGMP, MLD, MLDP, multicast

In modern networks traffic grows enormously every day and it consumes a great deal of bandwidth. Different multicastprotocols have been invented to even the load that the traffic creates. Multicasting means sending a multicast-frame to only one separately determined group in which the recipients can join. With multicastprotocols the efficiency of sharing the targeted data is made possible.

The purpose of this study was to familiarize with different multicastprotocols, and their policy as a part of an IPv4- and IPv6-network. The theoretical part was to give as much comprehensive and explicit description as possible of how multicasting works. In addition theoretical part, a multicast modeling network was designed and implemented to experiment with different multicast technologies. The modeled network was built in Kymenlaakso University of Applied Sciences' laboratory.

For this study an IPTV-distribution situation modeling router- and a switch network was established. IPTV-operators service or a videoserver modeling environment was used as a source for data. The data was channeled through the test network to a single client PC which was located in a local area network. Multicastprotocols supporting IPv4- and IPv6 technologies were implemented as a part of this network.

The network was found working by the used protocols. However the protocols in this study were somewhat a small part of bigger whole of multicast-protocols. For more extensive test results the test environment should include several router- and switch devices to test the behavior and the actual effectiveness of these multicast-protocols. However the test results about the used multicastprotocols were promising.

LYHYENNELUETTELO

ADSL	*Asymmetric Digital Subscriber Line:* suosittu DSL:n muunnos. Verkkokytkintekniikka.
Anycast	IPv6:n määrittämä osoite, jota käytettäessä tietosähke toimitetaan yhdelle osoitteen määrittämään ryhmään kuuluvalle päätteelle.
BGP	*Border Gateway Protocol* on reititysprotokolla, jonka tehtävänä on hoitaa autonomisten järjestelmien välinen reititys.
CBT	*Core Based Tree*: tarveohjattu monilähetysreititysprotokolla, joka määrittelee jaettuja jakelupuita.
Cisco	Yritys, joka valmistaa tietoliikennelaitteita ja -tarvikkeita kuten reitittimiä ja kytkimiä.
Default route	Oletusreitti, jota käytetään, jos nimetyt reitit eivät johda haluttuun kohteeseen.
DHCP	*Dynamic Host Configuration Protocol*: protokolla, joka jakaa IP-osoitteita lähiverkolle määrätyltä alueelta.
DNS	*Dynamic Name System*: nimipalvelujärjestelmä, joka muuttaa verkkotunnukset IP-osoitteiksi.
DoSS	*Denial-of*-service *attack*: palvelunestohyökkäys tarkoittaa jonkun tietyn verkkopalvelun lamauttamista.
DVMRP	*Distance Vector Multicast Routing Procotol*: käytetään reitittimien väliseen ryhmälähetys-pakettien välitykseen.
Ethernet	Pakettipohjainen lähiverkkotekniikka.
Firefox	Mozilla-yhtiön verkkoselain.

FPS	*Frames Per Second*: näytön päivitysnopeus sekunteina.
GOP	*Group Of Pictures*: määrittää järjestyksen, jossa sisäinen ja ulkoinen kehys ovat.
HDTV	*High Definition Television*: teräväpiirtotelevisio.
ICMP	*Internet Control Message Protocol* on kontrolliprotokolla, jolla lähetetään viestejä koneista toisiin.
IGMP	*Internet Group Management Protocol* on protokolla, joka mahdollistaa asiakkaiden liittymisen ryhmälähetys-ryhmiin.
IGP	*Interior gateway protocol*: reititysporotokolla, jota käytetään informaation vaihdossa autonomisen järjestelmän kanssa,
IP	*Internet Protocol*: protokolla, joka huolehtii pakettien toimituksesta.
IPTV	*Internet Protocol Television*: Internet-protokollan avulla toimiva televisiolähetys.
LAN	*Local Area Network*: verkkoteknologia lyhyitä etäisyyksiä varten.
LSP	*Label-switched path*: MPLS:n läpi kulkeva polku.
Link-local address	IPv6 -osoite, joka on merkityksellinen yhdessä verkossa.
MLD	*Multicast Listener Discovery*: osa IPv6:n protokollaa. Vastaa IPv4:n IGMP:ä.
MLDP	*Multicast Label Distribution Protocol*: protokolla, jolla reitittimet kykenevät vaihtamaan Label Mapping -tietoja.

MPEG	*Moving Picture Experts Group*: ryhmä, joka suunnittelee videonpakkaustapoja.
MPLS	*Multiprotocol Label Switching* on menetelmä, jolla kuljetetaan IP -paketteja runkoverkon solmujen yli siten, että solmujen ei tarvitse tehdä erillistä reititystä.
Multicast	Osoite- ja reititysjärjestelmä, joka mahdollistaa IP -pakettien lähettämisen halutulle tietokonejoukolle.
MSDP	*Multicast Source Listener Protocol* on PIM -perheen protokolla, joka mahdollistaa PIM-SM:n rendezvous pointin.
NAT	*Network Address Translation*: osoitteenmuunnin.
OSI -malli	*Open Systems Interconnection Reference Model* on tiedonsiirtoprotokollien yhdistelmän kuvaava seitsemän kerroksinen kuvaus.
OSPF	*Open Shortest Path First* on TCP/IP-verkkojen reititysprotokolla.
PGM	*Pragmatic General Multicast*: lähetysprotokolla.
PIM	*Protocol Independent Multicast*: ryhmälähetysten lähde.
Ping	Tapa testata, onko kohde tavoitettavissa.
Plugin	Liitännäinen. Kevyt ohjelmallinen lisäosa, joka toimii yhteistyössä isäntäohjelman kanssa parantaakseen sen käytettävyyttä.
Protokolla	Sääntöjä koskeva määritys, joita tietokoneiden on noudatettava.

RIP	*Routing Information Protocol* on reititysprotokolla, joka laskee reitin hyppymäärillä.
Router	Laite, joka siirtää paketteja verkkojen välillä.
Route	Reitti, jota pitkin dataliikenne kulkee.
Server	Ohjelma, joka tarjoaa erilaisia palveluja verkon kautta.
SSM	*Single Source Multicasting* tai *Source-Specific Multicasting*: Kuljetuskerroksen viestipohjainen protokolla.
STB	*Set-top box*: laite, joka sisältää virittimen. Yhdistetään televisioon ja ulkoisen signaalin lähteeseen.
Switch	Laite, joka yhdistää pakettikohtaisen verkon osia.
UDP	*User Datagram Protocol*: yhteydetön protokolla, joka mahdollistaa tiedostojen siirron ilman laitteiden välistä yhteyttä.
VLAN	*Virtual Local Area Network*: tekniikka, joka mahdollistaa fyysisen tietoliikenneverkon jakamisen loogisiin osiin.
VLC	*Video Lan Client*: median toistoon tarkoitettu ohjelma, joka tukee monipuolisesti erilaisia tiedostomuotoja ja ominaisuuksia.
WAN	*Wide Area Network*, eli laajaverkko on tiedonsiirtoverkko, joka käsittää laajoja maantieteellisiä alueita.
Wireshark	Ohjelma, jolla pystytään lukemaan ja tulkitsemaan tietoliikennepaketteja sekä -liikennettä.

SISÄLLYS

1 JOHDANTO

Internet on kasvanut vuoden 2000 jälkeen valtavalla vauhdilla ja tällä hetkellä Internetkäyttäjiä on noin 2,5 miljardia eli noin kolmannes maailman väestöstä. Nopea tietoliikennemäärän kasvu on asettanut reititys- ja tietoliikennetekniikoiden kehityksen enemmän kuin tarpeelliseksi. Tietoliikenneverkkojen ongelmien ennaltaehkäisemiseksi käytettävissä olevien resurssien tehokas käyttäminen on elintärkeää.

Multicast eli ryhmälähetystekniikka tarjoaa helpotusta verkkojen valtaville kuormituksille. Kyseisellä tekniikalla lähettäjänä toimiva laite lähettää tiedon ainoastaan kerran eteenpäin. Reitin varrella olevat laitteet monistavat tarvittaessa lähettävän datan useisiin eri kohteisiin. Tämä on erinomainen keino säästää verkon resursseja ja keventää siinä esiintyvää kuormaa. Esimerkkinä ryhmälähetys-tekniikan toimivuudesta on IPTV, jonka avulla tiedonsiirtokaistaa kyetään käyttämään huomattavasti tehokkaammin kuin esimerkiksi unicast-tekniikkaa hyödyntämällä.

Ryhmälähetystekniikka on kasvussa vaikkakin sen perinpohjainen hyödyntäminen on edelleen alkutekijöissä. Lähiverkoissa ryhmälähetysten hyödyntäminen on paljon yleisemmässä käytössä kuin Internetin yli tapahtuvassa liikenteessä. IPv6:n kehittyessä tulee ryhmälähetysten käyttö helpottumaan. Lisäksi uuden IPv6:n myötä vanhat protokollat jäävät hitaasti pois, jolloin protokollien määrä vähenee, sekä uudet, tehokkaammat protokollat selkeyttävät ryhmälähetysten toteutusta.

Cisco Systemsin mukaan verkossa olevien päätelaitteiden ja yhteyksien määrä lähes kaksinkertaistuu seuraavan viiden vuoden aikana. Tämä tarkoittaa valtavaa kasvua Internetissä liikkuvan datan määrään. Ciscon ennusteen mukaan tämä tarkoittaa, että vuoteen 2016 Internet-liikkeen määrä tulee olemaan 1,3 tsetatavua, eli triljoona gigatavua. Lisäksi keskimääräinen Internet-liikenne tulee kasvamaan samaan vuoteen mennessä noin 150 petatavuun tunnissa. Tämä vastaa sitä, että 278 miljoonaa ihmistä katsoo samanaikaisesti teräväpiirtotasoista elokuvaa Internetin välityksellä. Teoriassa tästäkin liikenteessä osa tullaan hoitamaan ryhmälähetysliikenteenä, jolloin siirrettävän datan määrä on huomattavasti pienempi.

Tämän opinnäytetyön ensisijainen päämäärä oli perehtyä kasvussa olevien eri ryhmälähetysprotokollien perusominaisuuksiin sekä niiden tapaan toimia osana IPv4-, ja IPv6-verkkoa. Näitä protokollia ovat muun muassa IPv4:lle kehitetty IGMP eli Inter-

net Group Management Protocol, sekä PIM eli Protocol-Independent Multicast. Erityisesti IPv6-lähiverkkoympäristöön on tarkoitettu MLD eli Multicast Listener Discovery. Operaattoreiden MPLS-verkkoihin on puolestaan uutena yhteyskäytäntönä tullut MLDP eli Multicast Label Distribution Protocol. Työ suoritettiin Kymenlaakson ammattikorkeakoulun laboratoriossa liittämällä edellä mainitut protokollat suunniteltuun verkkoon.

Työn rajaus oli hetkittäin vaikeata johtuen ryhmälähetysprotokollien suuresta määrästä. Opinnäytetyössä tarkemman tarkastelun kohteeksi valittiin lopulta kolme protokollaa: IGMP, PIM sekä MLD. Multicast LDP laajuutensa vuoksi jätettiin työn loppuvaiheessa itse konfiguraatiosta pois. Siihen perehdyttiin vain teoriatasolla.

2 MUUTTUVA TIETOVERKKOYMPÄRISTÖ

Tietoverkoissa tapahtuu jatkuvaa muutosta. Viime aikojen suurimpiin muutoksiin, joka edelleen on käynnissä, voidaan laskea IP version päivittäminen 4:stä 6:een. Lisäksi Internet tarjoaa valtavia määriä erilaisia palveluja. Näistä potentiaalisimpana ehdokkaana on IPTV, joka yleistyy nopeasti helppokäyttöisyytensä vuoksi.

2.1 Internet Protocol version 6

Internet Protocol version 6 on IPv4:n seuraajaksi kehitetty protokolla. Ensisijainen syy IPv6:n kehittämiselle oli pelko siitä, että käytettävissä olevat IPv4-protokollan osoitteet loppuisivat, mikä tuntuu aika uskomattomalta, sillä IPv4:lle varattuja osoitteita on yli kolme miljardia. Mutta koska kaikki osoitteet eivät ole käytettävissä, ovat vapaat osoitteet ajan saatossa vähentyneet nopeasti, mikä taas lopulta johti uuden IP:n kehittämiseen.

IETF (Internet Engineering Task Force) päätti antaa IP:n uudelle versiolle numeron 6, joka erottaa sen edeltäjästä. Numero 5 päätettiin jättää väliin, koska se näytti aiheuttavan virheitä ja sekaannuksia.

2.1.1 IPv6 ominaisuudet

IPv6 sisältää monia erilaisia ominaisuuksia, jotka tekevät siitä tehokkaan ja todella käytännöllisen. Sen jopa luonnehditaan olevan perustaltaan sama kuin IPv4 muutamalla muutoksella. IPv6 tukee IPv4:n tapaan yhteydetöntä kuljetusta, sekä se sallii lähettäjän valitsevan viestin pituuden. Lisäksi se edellyttää, että lähettäjän on määriteltävä kuinka monta väliä viesti saa enintään kulkea, ennen kuin se on poistettava. IPv6:n suurimmat muutokset voidaan jakaa muutamiin pääryhmiin:

- *Pidemmät osoitteet*. Tärkein muutos on pidempi osoite. IPv6 kasvattaa osoitteen pituudeksi 128 bittiä, kun IPv4:llä se on ”vain” 32 bittiä. IPv6:n osoiteavaruus on niin suuri, että nykyisillään sen täyttäminen on silkka mahdottomuus.

- *Laajennettu osoitehierarkia.* Suurempi hierarkia mahdollistaa uusien, erilaisten tasojen lisäämisen, kuten esimerkiksi Internet-palveluntarjoajien toimipaikan sisäisen hierarkian määrittämisen.

- *Joustava otsikkorakenne.* IPv6:n tietosähke on uusittu, eikä se siis ole yhteensopiva IPv4:n kanssa.

- *Parannetut optiot.* IPv6 sallii ohjaustietojen lisäämisen tietosähkeisiin. IPv6 sisältää paljon uusia ominaisuuksia.

- *Mahdollisuus protokollan laajentamiseen.* Merkittävimpänä muutoksena on siirtyminen pois protokollasta, joka määrittää kaikki yksityiskohdat koskien uusia ominaisuuksia ja niiden lisäämistä. Käytännössä tämä tarkoittaa sitä, että halutessaan IETF voi tehdä muutoksia protokollan verkkolaitteisiin ja niiden sisäisiin muutoksiin.

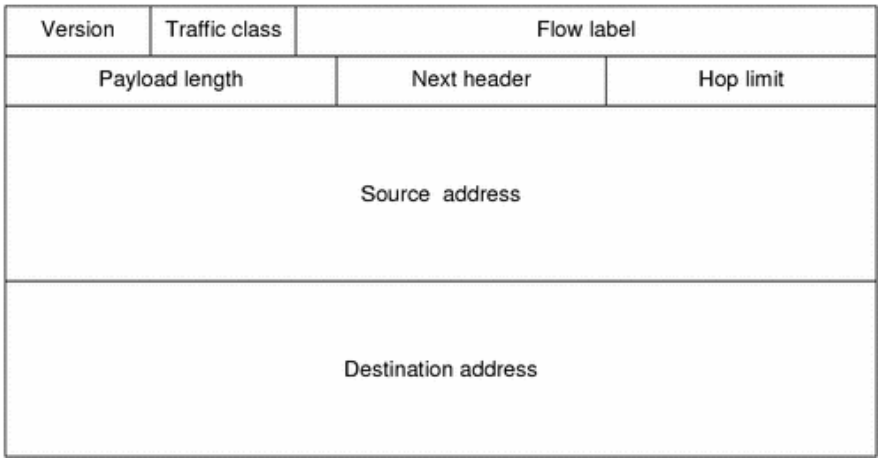
- *Automaattiset asetusmääritykset ja uudelleennumerointi.* IPv6 sisältää sellaisia ominaisuuksia, joiden avulla tietokone voi aloittaa suoran kommunikoinnin ilman asetusten manuaalista määrittämistä, tai ilman suoraa reititintukea.

- *Resurssien varaaminen.* Vuon käsite ja eriytettyjen palveluiden määritys mahdollistavat verkossa olevien resurssien varaamisen etukäteen. (Teare, D. 2010, 693-694).

2.1.2 IPv6 perusotsikon rakenne

IPv6:n perusotsikko sisältää vähemmän tietoa kuin IPv4:n perusotsikko, vaikkakin sen osoitteet ovat pidempiä. Jotkin optiot ja tietosähkeiden otsikot on siirretty IPv6:n laajennusotsikoihin. IPv6-otsikkokentät ovat:

- *Versio (Version)*, jonka pituus on 4 bittiä. Se sisältää IP:n versiomuodon.
- *Prioriteetti (Traffic Class)* antaa datagrammille prioriteettitason. Pituus 4 bittiä.
- *Vuon tunnus (Flow label)* sisältää tiedon siitä, minkä tasoiseen tietovuohon kyseinen datagrammi kuuluu. Vuon tunnus on pituudeltaan 16 bittiä.
- *Tietokuorman pituus (Payload lenght)* on pituudeltaan 16 bittiä. Sisältää tiedon varsinaisen tiedon sisällön pituudesta.
- *Seuraava otsikko (Next header)*, 8 bittiä. Määrittelee seuraavan otsikon tyypin.
- *Hyppymäärän rajoitin (Hop limit)* on pituudeltaan 8 bittiä. Hyppymäärän rajoitin kertoo, kuinka monta reititinhyppyä datagrammi voi maksimissaan käyttää. Tämä arvo vähenee aina yhdellä jokaisessa hypyssä. Jos paketti ei pääse perille ennen hop limit -arvon loppumista, pakettia katoaa tai kuolee.
- *Lähetettävä osoite (Source address).* Lähettäjänä toimivan koneen IP-osoite. Pituus 128 bittiä.
- *Vastaanottava osoite (Destination address).* Vastaanottajana toimivan koneen IP-osoite. Pituus myös 128 bittiä. (Comer 2002, 602–603.)



Kuva 1. IPv6-paketin otsikko. (Tunneling 2002.)

IPv6 käsittelee tietosähkeen pituutta koskevat määritykset uudella tavalla. Perusotsikko ei enää sisällä varsinaista pituuskenttää, koska perusotsikon pituus on aina 40 oktettia. Lisäksi IPv6 korvaa IPv4-tietosähkeen pituuskentän 16-bittisellä datan pituus kentällä, jolla määritetään tiedot tietosähkeiden tiedoista varsinaisten otsikkojen lisäksi. Käytännössä tämä tarkoittaa sitä, että IPv6-tietosähke voi sisältää maksimissaan 65 535 oktettia dataa. (Comer 2002, 602–603.)

2.1.3 IPv6 osoitteet ja esitystapa

IPv6-osoite on pituudeltaan 16 oktettia. Käytännössä se on siis neljä kertaa suurempi kuin IPv4-osoite. Tämän kokoinen osoiteavaruus varmistaa lähes minkä tahansa osoitejärjestelmän toteuttamisen. Eräs keino koettaa ymmärtää IPv6-osoiteavaruuden kokoa on seuraava: vaikka jokaisella maapallon asukkaalla olisi oma henkilökohtainen, nykyisen Internetin kokoinen verkko, riittäisi jokaiselle silti määrittelemättömän paljon osoitteita.

Uusi menetelmä ratkaisee osoitteiden riittävyyteen liittyvät ongelmat, mutta samanaikaisesti se luo täysin uusia ongelmia: yksinkertaisen osoitteen käsitteleminen on todella vaikeaa. Tämän ymmärtää, kun tarkastellaan 128 bittistä lukua pisteillä erotetussa muodossa:

104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255

Osoitteiden lyhentämiseksi sekä niiden kirjoittamisen helpottamiseksi päädyttiin kaksoispisteillä erotettuun heksadesimaalimuotoon. Tämä tarkoittaa, että osoite jaetaan 16-bittisiin osiin, jotka erotetaan toisistaan kaksoispisteillä. Alla sama osoite kuin yllä muutettuna heksadesimaalimuotoon:

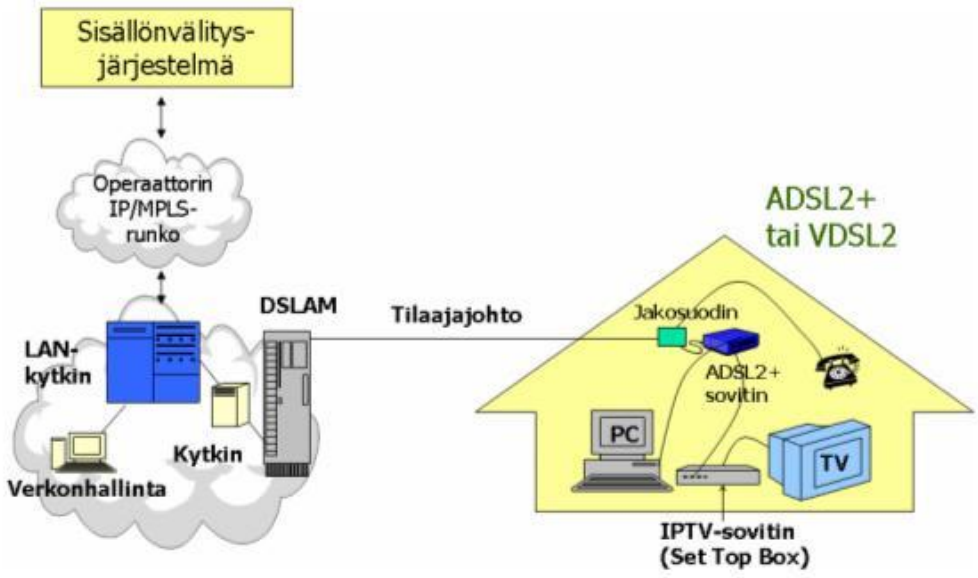
68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF

(Comer 2002, 610–611.)

2.2 IPTV

Paikallisten operaattorien tarjoama televisiopalvelu IPTV on järjestelmä, jonka kautta televisiopalvelut toimitetaan Internet-protokollien yli pakettikytkentäisenä ratkaisuna sen sijaan, että ne toimitettaisiin perinteisen maanpäällisen, satelliittisignaalin tai kaapelitelevision muodoissa. Tämä kyseinen tekniikka mahdollistaa muun muassa videoneuvottelut ja tv-ohjelmien jakelun.

IPTV mahdollistaa lähetyksen katselun missä ja milloin vain usealla päätteellä. Asiakas pystyy itse valitsemaan ohjelmistonsa sekä aikansa ja paikkansa, jolloin niitä haluaa hyödyntää. Normaalin tarjonnan lisäksi asiakkaan on mahdollista valita ohjelmistoonsa palveluita televisiotarjonnan ulkopuolelta. Lisäksi IPTV mahdollistaa terävä-piirtotelevision hyödyntämisen. (IPTV-järjestelmät 2007.)



Kuva 2. Esimerkki IPTV-ympäristöstä. (IPTV-järjestelmät 2007.)

IPTV:tä ei kuitenkaan pidä sekoittaa Internet-TV:seen. Internet-TV:ssä videosignaali välitetään yleisen Internetin ylitse. Lisäksi Internet-TV:stä puhutaan silloinkin, kun kyse on videoarkistosta, kuten YouTuben tai NetFlixin tapaisista palveluista. IPTV välitetään suljetussa operaattoriverkossa. Yleisesti ottaen IPTV on maksullinen palvelu, joka operaattorin puolesta osoitetaan palvelun tilaajille. Internet-TV on verkossa kaikkien saatavilla.

2.2.1 Toiminta ja laitteistovaatimukset

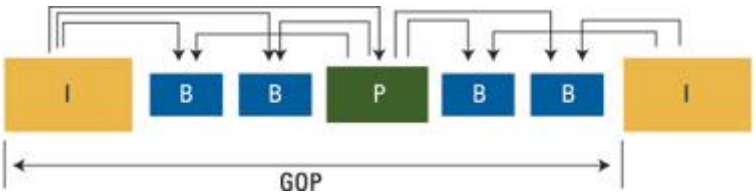
IPTV-palvelun vastaanottamiseen kuluttaja tarvitsee laajakaistayhteyden sekä ADSL-sovittimen. Koska yksi ohjelma vaatii siirtonopeudeksi vähintään kahdesta viiteen megabittiä sekunnissa, on palvelun käyttäjällä käytännössä oltava vähintään 8 megabitin laajakaistaliittymä. Teräväpiirtolähetykset vaativat yli 10 megabitin nopeuden ja useamman kanavan katselu samaan aikaan edellyttää jo 24 megabitin nopeutta. Suuret nopeudet puolestaan edellyttävät, ettei kuluttaja ole liian etäällä operaattorin tukiasemista. Myös kaapeli-tv:ssä on mahdollista käyttää IPTV-palvelua. (IPTV-järjestelmät 2007.)

Palvelu	Koodaus	Kapasiteettivaatimus Mbps	Huomioitavaa
HDTV	MPEG2	20	1080i, res.1920x1080
HDTV	MPEG2	16	720p, res. 1280x720
SDTV	MPEG2	5	
VoD	MPEG2	5	
HDTV	MPEG4 AVC/MS WM9	8	1080i, res.1920x1080
HDTV	MPEG4 AVC/MS WM9	6	720p, res. 1280x720
SDTV	MPEG4 AVC/MS WM9	2	
VoD	MPEG4 AVC/MS WM9	2	

Kuva 3. IPTV:n vaatimukset. (IPTV-järjestelmät 2007.)

Palvelua käyttääkseen on kuluttajalla oltava tarpeelliset laitteistot. Laajakaistamodeemi yhdistetään IPTV-sovittimeen (IP STB, Set-Top-Box), joka soveltuu pelkästään digitaalisen televisiopalvelun vastaanottoon. IP-sovitin puolestaan kytketään esimerkiksi televisioon ja stereolaitteistoon. Palveluita kuluttaja voi ohjata esimerkiksi kaukosäätimellä tai näppäimistöllä. Laitteiden määrä voi poiketa toisistaan asiakkaasta ja paikasta riippuen (IPTV-järjestelmät 2007.)

IPTV käyttää kuvanlähetykseen MPEG-koodekkia, jonka videovirta rakentuu yksittäisistä kuvista, jotka näytetään tietokoneen näytöllä nopeasti peräkkäin. Kyseessä on termi FPS, frames per second. Kukin kuvasarja koostuu kuvaryhmistä, joita kutsutaan Group Of Pictureksi, GOP:ksi. Ryhmän ensimmäinen kuva sisältää kyseisen kuvasarjan kaiken tiedon. Jos tämä kuva hajoaa tai katoaa, häviää tämän seurauksena koko kuvasarja. Mikäli paketin katoaminen osuu johonkin muuhun kuin ensimmäiseen kuvaan, ilmenee se videon pätkimisenä tai videon epäselvyytenä (Kankare 2009, 7.)



Kuva 4. MPEG-videovirran rakenne. (Kankare 2009, 7.)

Packet loss, eli pakettihävikki, voi johtua useasta eri syystä, mutta yleisimmin sen aiheuttaja on kaistan tukkeutuminen, ruuhkautuminen tai liian suuri viive. Näitä tekijöitä ei oikein voi ennalta ehkäistä, koska ruuhkautumista voi tapahtua myös runkoverkossa. Kuitenkaan tällaista vikaa ei saisi esiintyä runkoverkossa. Pakettien hävitessä pääte ei kykene puskuroimaan saapuvia paketteja tarpeeksi nopeasti, jolloin niitä putoaa välistä pois tai ne eivät saavu päätteelle ollenkaan. Tämä aiheuttaa kuvan pysähtelyä ja pätkimistä. Pahimmillaan kuva saattaa pysähtyä muutamiksi sekunneiksi (Kankare 2009, 8)(Rowe 2006, 1.)

Kuva 5. Pakettien häviämisten vaikutuksia. (Rowe 5/2006.)

2.2.2 Palvelut

Koska IPTV on todella nopeasti kasvava toimi, ovat sisällön palvelut sen tärkein asia. Jos ei ole tarjottavaa sisältöä, ei ole myöskään maksavia asiakkaita. IPTV tarjoaa useita erilaisia palveluita verrattuna tavalliseen televisioon.

IPTV:ssä palvelut jaetaan erilaisiin ryhmiin niiden interaktiivisuuden mukaan. Näitä palveluja ovat muun muassa seuraavat:

- True Video On Demand (T-VoD). Käyttäjä hallitsee istuntoa täysin. Käyttäjä hallitsee kaikkia ominaisuuksia: Hän pystyy kelaamaan videota eteenpäin ja taaksepäin, jäädyttämään kuvan tai suorittamaan satunnaisia tallennuksia.

- Near Video-On-Demand (N-Vod). Käyttäjän on mahdollista kelata videota. Tämä ominaisuus voidaan jakaa usealla kanavalla.

- Quasi Video-On-Demand (Q-VoD) on palvelu, jossa käyttäjät ryhmitellään heidän kiinnostuksiensa mukaisesti. Halutessaan käyttäjät voivat vaihtaa ryhmää helposti.

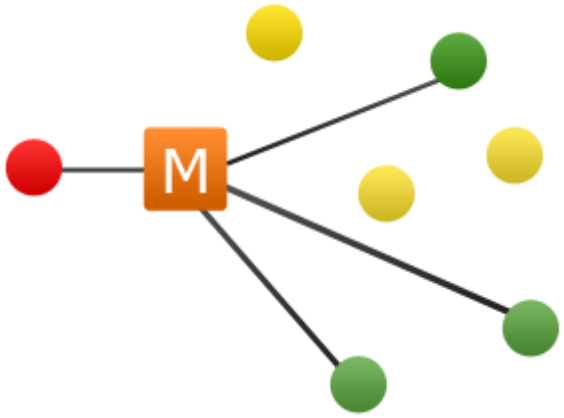
- Pay-Per-View (PPV). Käyttäjä kirjautuu palveluun ja maksaa tietystä ohjelmasta.

- Broadcast (No-VoD). Käyttäjällä ei ole mahdollisuutta vaikuttaa ominaisuuksiin palvelussa, vaan hän on passiivinen osallistuja. (Video-On-Demand 2000.)

3 RYHMÄLÄHETYSTEN PERINTEISET MENETELMÄT

Ryhmälähetyksellä tarkoitetaan tekniikkaa, joka mahdollistaa one-to-many-tietoliikenneinfrastruktuurin verkossa. Se jakautuu vastaanottimiin riippumatta multicast-viestejä vastaanottavien laitteiden määrästä. Ryhmälähetys käyttää verkkoinfrastruktuuria tehokkaasti vaatimalla, että paketti lähetetään vain kerran, vaikka se toimitetaankin usealle vastaanottajalle. Etuna muihin tekniikoihin verrattuna on se, ettei se vaadi tehokkaita laitteistoja, koska reititinverkko vastaa ja huolehtii viestien jakamisesta ja toimittamisesta. Ryhmälähetystä käytetään pääasiassa videoneuvotteluissa ja työryhmäohjelmissa.

”Ryhmälähetys-kehyksissä vastaanottajan ensimmäisen tavun vähiten merkitsevä bitti on 1.” (Jaakohuhta, 2005, 83). Yleisin ryhmälähetyksen hyödyntämä protokolla on User Datagram Protocol, UDP. UDP ei kuitenkaan ole kovin luotettava - viestit voivat katoilla, tai ne toimitetaan rikkinäisinä. Luotettavampi ryhmälähetysprotokolla on Pragmatic General Multicast, PGM. Se kehitettiin havaitsemaan UDP:n tapaista pakettien hävittämistä. Lisäksi se lähettää uudelleen epäonnistuneet paketit korkeammalla prioriteetilla varmistaakseen niiden perillepääsyn. (Overview of IP Multicast 2000.)



Kuva 6. Ryhmälähetyksen toiminta. (Multimedia Appliances 2013.)

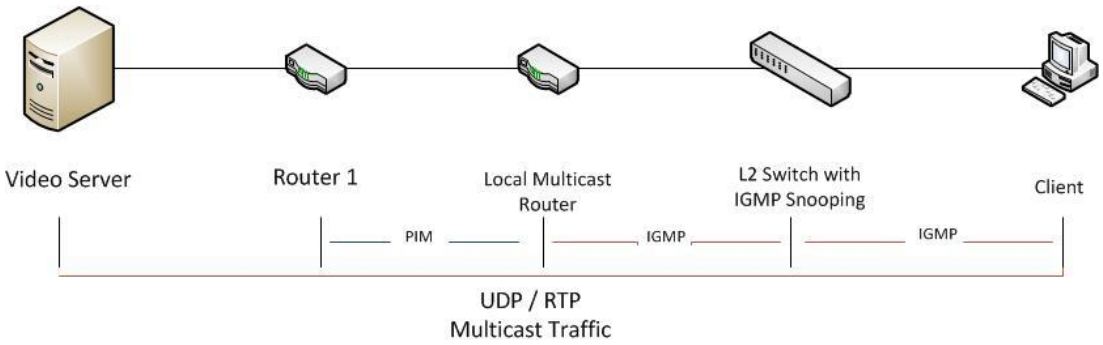
3.1 Internet Group Management Protocol (IGMP)

IGMP on protokolla, joka toimii TCP/IP-pinossa. Sen perimmäinen tarkoitus on asiakkaiden liittämisen mahdollistaminen eri ryhmälähetys-ryhmiin. Protokollaa hyödynnetään ryhmälähetys-reitittimien ja -kytkimien toimesta siten, että eri ryhmiä pystytään hallinnoimaan keskitetysti ja helposti. IGMP toimii yksinkertaisella tavalla ulkoverkon ja sisäverkon rajapintana: se kuuntelee ulkoverkon viestejä ja tarjoaa niitä halukkaille sisäverkon työasemille. Mikäli halukas työasema löytyy, pystytään sen viestit ohjaamaan automaattisesti takaisin ulkoverkon laitteille, jotka jatkavat yhteyden ylläpitämistä työaseman kanssa. IGMP-protokolla toimii vain IPv4-verkoissa.

IGMP -protokolla on ensisijaisesti tarkoitettu päätelaitteen ja sen oman yhdyskäytäväreitittimen väliseen liikenteeseen. Mikäli kuitenkin IGMP-viestien halutaan kulkevan yhdyskäytäväreitittimestä palveluntarjoajan seuraaville reitittimille, voidaan reitittimestä tehdä niin sanottu proxy, eli välityspalvelin. Välityspalvelin hoitaa tilaukset ja

luovuttamiset isäntäkoneiden pyyntöjen mukaisesti. Lisäksi IGMP-välityspalvelin välittää isäntäkoneiden viestejä isäntäkoneiden puolesta.

IGMP:tä käytetään lähiverkoissa itsenäisten käyttäjien dynaamiseen rekisteröintiin. Käytännössä käyttäjät voivat tunnistautua IGMP-ryhmän jäseneksi lähettämällä viestejä paikalliselle multicast-reitittimelle. IGMP:tä kuuntelevat reitittimet lähettävät säännöllisesti kyselyitä selvittääkseen ne ryhmät, jotka ovat aktiivisia.
(IGMP, Internet Group Management Protocol 2012.)



Kuva 7: IGMP-arkkitehtuuri.

3.1.1 IGMP toiminta ja viestittäminen

IGMP:n toiminta jakautuu kahteen vaiheeseen.

Vaihe 1: Tietokoneen liittyessä multicastryhmään, se tiedottaa omasta jäsenyydestään reitittimelle IGMP-sanomalla. Reititin vastaanottaa sanoman ja määrittää tarvittavat reitit levittämällä tietokoneen jäsenyystiedot muille reitittimille.

Vaihe 2: Paikalliset reitittimet tarkistavat kysymällä, onko ryhmissä vielä jäseniä lähettämällä niille kyselyitä säännöllisin väliajoin. Jos yksikään jäsen ei vastaa sanomaan, IGMP olettaa, että verkossa olevista tietokoneista mikään ei kuulu enää IGMP-ryhmään. Tällöin se lopettaa ryhmän mainostamisen muille reitittimille.
(Comer 2002, 328.)

3.1.2 IGMP toteutus

IGMP:n toteutus on suunniteltu niin, että se kuormittaa verkkoa niin vähän kuin mahdollista. Koska verkossa voi olla useita ryhmälähetys-reitittimiä, sekä useisiin eri ryhmiin kuuluvia tietokoneita, vain pieni osa niistä saa lähettää ohjausliikennettä.

IGMP vähentää liikennettä monella eri tavalla. Kaikessa tietokoneiden ja ryhmälähetys-reitittimien välisessä viestinnässä tarvitaan ryhmälähetystä. IGMP-sanomat kapseloidaan sähkeisiin lähetystä varten, minkä jälkeen kohdeosoitteeksi asetetaan ryhmälähetys-osoite. Tämän jälkeen reitittimet lähettävät IGMP-kyselyitä tietokoneille. Tällöin tietokone ja reitittimet lähettävät muille ryhmille oman IGMP-ryhmänsä osoitteeseen. Tämän jälkeen reititin lähettää kyselyn koskien reitittimien ja tietokoneiden jäsenyyksiä. Tämä viesti lähetetään vain kerran. Tämän niin sanotun kiertokyselyn lähetysväli on 125 sekuntia. Kun tietokoneet ovat vastaanottaneet sanoman IGMP-jäsenyydestä, ne valitsevat nopeasti yhden reitittimen, jonka tehtävänä on lähettää kiertokyselyt. Näin ollen IGMP-liikenteen määrä ei lisäänny, vaikka verkkoon liitettäisiin uusia ryhmälähetys-reitittimiä.

Tietokoneet eivät vastaa kyselyihin yhtä aikaa. Kukin IGMP:n tuottama kysely sisältää arvon, joka määrittää, kuinka kauan tietokone saa viivyttää vastaustaan. Kyselyn saapuessa tietokoneelle, se päättää mielivaltaisen arvon väliltä 0-N ja odottaa näin monta sekuntia. Lopuksi tietokoneet kuuntelevat, saavatko ne vastauksen joltakin muulta samaan ryhmään kuuluvalta jäseneltä. Jos vastaaminen ei ole tarpeen, tietokoneet eivät vastaa. (Comer 2002, 328–329.)

Yleiskysely	Selvitetään, onko segmentissä aktiivisia jäseniä missä tahansa ryhmässä.
Ryhmäkohtainen kysely	Selvitetään, onko segmentissä tiettyjä ryhmiä, joissa on aktiivisia jäseniä.
Raportti 1	Työaseman yhdistäminen jäseneen. Tiedon lähetys niille ryhmille, joissa asema on jäsenenä.
Viesti	Työasema vastaa kyselyyn ilmoittamalla, jääkö se pois ryhmälähetyksestä.
Raportti 2	Työaseman yhdistäminen jäseneen. Tieto lähetetään ryhmille, joissa työasema on jäsenenä. Työaseman yksilöinti.

Taulukko 1. IGMPv2 -viestityypit. (Jaakohuhta 2005, 173.)

3.1.3 IGMP version 1

IGMP Versio 1 on yksinkertainen protokolla, joka koostuu kahdesta viestistä: Membership Report ja Membership Query. Käyttäjän halutessa liittyä ryhmälähetysryhmään, he lähettävät Membership Report viestejä. Reititin vastaa Membership Query viesteillä varmistaakseen, että käyttäjä on edelleen kiinnostunut liittymään kyseiseen ryhmään. (IGMP, Internet Group Management Protocol 2011.)

3.1.4 IGMP version 2

IGMPv2 laajentaa toiminnallisuutta säilyttäen yhteensopivuuden IGMPv1:n kanssa. IGMPv2 käyttää yksinkertaista valintaprosessia valitakseen yksittäisen reitittimen jokaisesta aliverkosta, jotka lähettävät Membership Query -viestiä. Toisena uudistuksena on käyttäjien mahdollisuus lähettää paikalliselle reitittimelle Leave Group -viestejä. Muuten IGMPv2 toimii hyvin samalla tavalla kuin IGMPv1.
(IGMP, Internet Group Management Protocol 2011.)

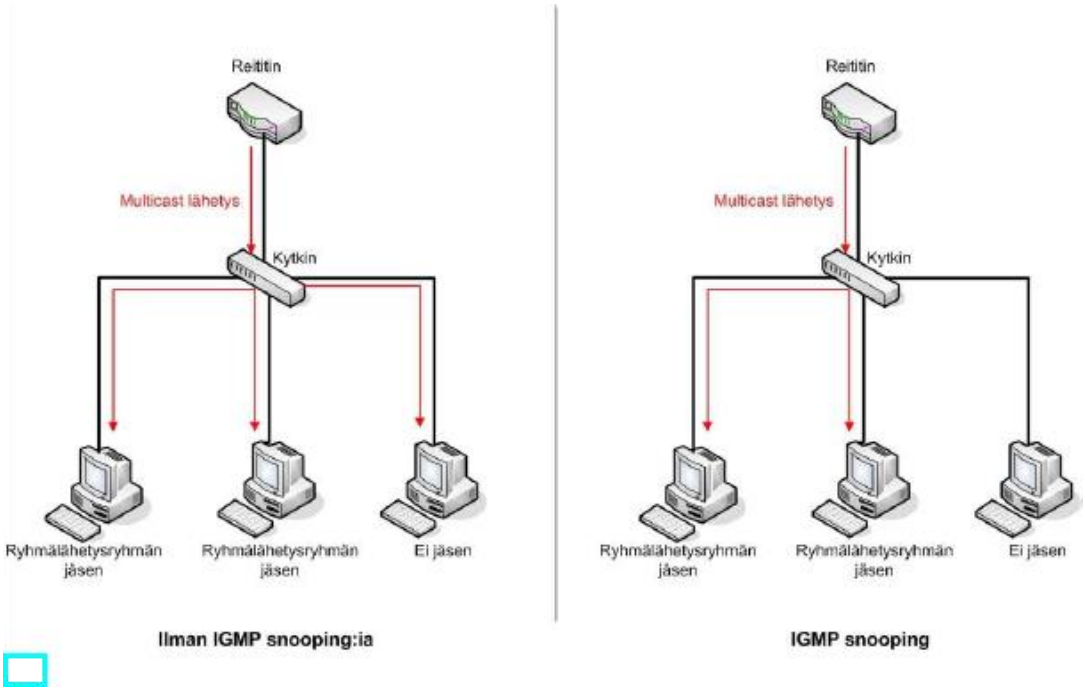
3.1.5 IGMP version 3

IGMPv3:n erona muihin on sen kyky lähettää viestejä niille ryhmälähetysryhmille, joihin se on halukas liittymään. (mm. SSM -tekniikka vaatii toimivuuden takaamiseksi

IGMPv3:sen.) Isäntäkone ilmoittaa halukkuutensa liittyä multicast-ryhmään liittymisviestillä, joka lähetetään IGMPv3-reitittimelle. (Internet Group Management Protocol 2002.)

3.1.6 IGMP Snooping

Johtuen siitä, että IGMP toimii IP-protokollan päällä, MAC-tasolla toimivat kytkimet eivät ole kykeneviä tietämään mitkä vastaanottajat kuuluvat mihinkin multicast-ryhmään. Tätä ongelmaa varten kehitettiin IGMP Snooping -tekniikka, jolla tutkitaan milloin verkossa liikkuu IGMP-viestejä. IGMP Snooping tallentaa nämä viestit omaan muistiinsa. IGMP Snooping -tekniikan avulla kytkin oppii aliverkon jäsenten ryhmät, jolloin se osaa lähettää paketit oikeille vastaanottajille. Ilman tätä tekniikkaa kytkin lähettää multicast-paketit yleis-, eli broadcast -lähetyksinä, jolloin jokainen aliverkon jäsen saa ryhmälähetyksen viestit vaikka ne eivät kuuluisikaan ryhmään. (IPTV ja lisäarvopalvelut laajakaistaverkossa 2006, 10–11.)



Kuva 8: Kytkimen toiminta eri tilanteissa. (IPTV ja lisäarvopalvelut laajakaistaverkossa 2006.)

3.2 PROTOCOL-INDEPENDENT MULTICAST (PIM)

Protocol-Independent Multicast on ryhmälähetys-reititysprotokollien perhe, joka on suunniteltu IP-verkkoihin. PIM on yksi niistä, jotka tarjoavat one-to-many ja many-to-many tiedonsiirtomahdollisuuksia LANin, WANin, tai Internetin yli.

PIM ei ole millään lailla riippuvainen käytettävästä reititysprotokollasta, joten PIM-verkossa voi olla käytössä mikä reititysprotokolla tahansa, koska PIM käyttää ryhmälähetysten välittämisen eteenpäin käyttäen unicastin reititysinformaatiota. Käytännössä PIM sisältää kaksi itsenäistä, toisistaan riippumatonta protokollaa. Näille protokollille yhteistä on ainoastaan nimen alkuosa, sekä sanomien otsikoiden rakenne. Näitä molempia protokollia tarvitaan, sillä varsinaisesti mikään protokolla ei toimi tarpeeksi hyvin kaikissa tilanteissa. PIM-DM on suunniteltu lähiverkkoihin, kun taas PIM-SM on ensisijaisesti tarkoitettu laaja-alueverkkoihin. (Comer 2002, 344.)

3.2.1 Sparse-mode (PIM-SM)

Sparse-Modea voidaan pitää CBT:n laajennuksena, joka tarvitsee tarkan kohteen, johon se voi liittymissanomansa osoittaa. Tämän vuoksi Sparse-Mode määrittää yhden reitittimen niin sanotuksi kohtauspaikaksi, rendezvous pointiksi. Ennen kuin tietokone liittyy ryhmälähetys-ryhmään, reititin suorittaa pyynnön ja lähettää sen rendesvouz pointille. Reitittimet, jotka sijaitsevat tämän pyyntöreitin varrella, tutkivat pyynnön ja kaikki jo aikaisemmin kyseiseen multicast-ryhmään liittyneet reitittimet vastaavat tähän viestiin. Tämän jälkeen Sparse-Mode pystyttää jakelupuun jokaista ryhmää varten, ja näiden puiden juuret ovat kohtauspaikkoja.

Sparse-Mode on kykenevä reittien optimointiin, mikäli jakelupuissa tapahtuu muutoksia. Sparse-Modea hyödyntävät reitittimet eivät tyydy vain yhden kohtauspaikan hyödyntämiseen, vaan ne laativat aina päivittyvän luettelon kaikista mahdollisista rendesvouz point -reitittimistä ja valitsevat niistä yhden kerrallaan. Jos yhteys käytössä olevaan reitittimeen päättyy, valitsee se itse luomastaan luettelosta toisen rendesvouz pointin ja luo nopeasti kaikkia verkon ryhmiä koskevat jakelupuut uudelleen.

Sen lisäksi, että PIM-SM voi valita toisen rendesvouz pointin, se voi vaihtaa jaetun puun SP-puuksi. (Shortest Path tree, lyhyimmän reitin puu). Protokolla mahdollistaa sen, että reititin voi päättää hyödyntääkö se SP:tä vai jo jaettua puuta. PIM-SM välit-

tää liikennettä vain niille verkon osille, joissa on aktiivisia vastaanottajia. (Comer 2002, 345.)

3.2.2 Dense-Mode (PIM-DM)

PIM-DM on optimoitu varmistamaan kuljetus, eikä niinkään minimoimaan verkon kuormitus, koska se on ensisijaisesti tarkoitettu kaistanleveydeltään suuriin ja nopeisiin verkkoihin. PIM-DM muistuttaa DVMRP:ä: se käyttää samanlaista yleislähetys- ja karsimisjärjestelmää. Aluksi tietosähkeet lähetetään kaikille ryhmille. Sen jälkeen niitä vähennetään sitä mukaa, kuin reitittimet kertovat karsimissanomallaan halunsa poistua ryhmästä. Tämä prosessi toistuu kolmen minuutin välein. Tällä keinolla reitittimet keräävät tietoa laitteista ja niiden tilasta. Näiden tietojen perusteella ne kasaavat oman ryhmälähetys-reititystaulunsa.

PIM-DM:n on tunnettava lyhin reitti kaikkiin kohteisiin. PIM-DM olettaakin, että reititin hyödyntää sellaista protokollaa, joka laskee lyhimmät mahdolliset reitit kohteisiin, tallentaa reitit reititystaulukkoon ja huolehtii niiden ylläpidosta. (Comer 2002, 344.)

3.2.3 Bi-Directional PIM

Bi-Directional PIM, eli kaksisuuntainen PIM, on kolmas PIM-protokolla. Se perustuu vahvasti PIM-SM:ään. Suurimpana Bi-Directional PIM:n erona Sparse-Modeen voidaan pitää sen menetelmää, jossa rendesvouz pointia käytetään datan lähettämisen lähteenä. BIDIR-PIM:ssä data virtaa RP:hen jaettua puuta pitkin, joka on kaksisuuntainen. Näin ollen tietovirrat kulkevat molempiin suuntiin.

BIDIR-PIM:ssä ei ole lähdekoodiin perustuvia puita. Sen vuoksi reitittimillä ei ole mahdollisuutta vaihtaa shared treestä lähdekoodiin perustuvaan puuhun. Lisäksi BIDIR-PIM ei tue SSM:ää, eikä BIDIR-PIM käytä kapselointia. (Pim Overwiev 2013.)

3.2.4 PIM Source-Specific Multicast (SSM)

PIM-SSM tukee ainoastaan one-to-many-mallia. SSM:ssä lähimpänä vastaanottajaa oleva reititin informoi jos se on halukas ottamaan ryhmälähetys-lähetyksiä vastaan. SSM:ssä pakettien lähetys perustuu (S, G)-kanaviin, jotka sisältävät lähteen unicast-

osoitteen ja ryhmälähetys-ryhmän kohdeosoitteen. Jotta vastaanottaja olisi kykenevä vastaanottamaan tällaista liikennettä, on sen liityttävä samojen kanavien jäseneksi.

SSM on erittäin tehokas ja mukautuva tapa lähettää esimerkiksi videokuvaa Internetissä useille vastaanottajille. Käytännössä se edellyttää Internetin kaikkien runkoreitittimien tukea toimiakseen vakaasti. (McFarland, Sambi, Sharma, Hooda 2011, 74–75.)

4 RYHMÄLÄHETYSTEN UUSIA MENETELMIÄ

Ryhmälähetysprotokollien on mukauduttava uuden IPv6:n mukanaan tuomaan muutoksiin. Seuraavassa esitellään kaksi uutta ryhmälähetysmenetelmää, joista toinen, MLD, toteutettiin myös käytännön tasolla. MLDP:hen perehdyttiin teoriatasolla.

4.1 Multicast Listener Discovery (MLD)

Multicast Listener Discovery on IPv6:n osa. IPv6-reitittimet käyttävät MLD:tä löytääkseen ryhmälähetys-kuuntelijoita. Se on ikään kuin IPv6-tekniikassa käytetty ryhmälähetysryhmien ylläpitäjä. MLD:tä käytetään reitittimien toimesta siten, että ne informoivat reitittimille, mikäli kullekin ryhmälle on kuuntelija.

MLD on hyvin samanlainen kuin IGMPv2. Tärkein ero näiden välillä on se, että MLD hyödyntää ICMP protokollaa, joka tekee MLD:n viesteistä ICMPv6:n datagrammeja. Kaikki MLD viestit on lähetettävä voimassa olevalla link-local -lähdeosoitteella, tai määrittämättömällä osoitteella mikäli rajapinnalla ei ole vielä link-local osoitetta.

Käyttämällä MLD:tä isännät voivat ilmoittaa, haluavatko he monilähetystä valituille ryhmille. Reitittimet voivat ohjata ryhmälähetyksen virtausta verkossa käyttämällä MLD:tä.

MLD käyttää kolmenlaisia viestejä: Query, Report ja Done. Done-viesti on kuin IGMPv2:ssa esiintyvä Leave Message: se osoittaa isännälle kun se ei enää halua vastaanottaa ryhmälähetyksen viestejä. Query-viestissä ryhmälähetyksen osoitekenttä nollataan kyselyä lähetettäessä, tai osoitteeksi valitaan IPv6:n ryhmälähetys-osoite. Report-viesti vastaa IGMPv2:ssa esiintyvää jäsenyysraportin viestiä. (Blanchet 2008, 267–268).

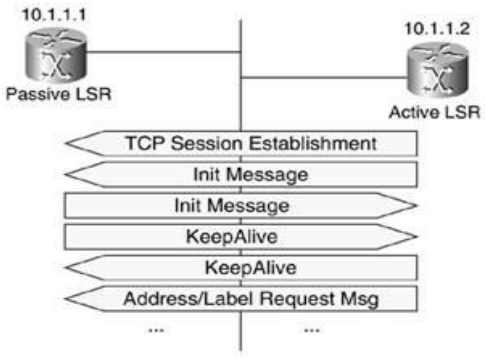
4.1.1 Multicast Listener Discovery Snooping

MLD Snooping -toiminnon periaate on täsmälleen sama kuin IGMP Snooping -toiminnolla. MLD Snooping -toiminnon avulla kytkin voi todeta ne portit, joissa on IPv6 multicast -lähetyksien vastaanottajia. Tämän seurauksena kytkin lähettää multicast kehykset vain niihin portteihin, joissa sitä tarvitaan sen sijaan, että se lähetettäisiin kaikille niillekin porteille, jotka sitä eivät halua.

4.2 Multicast Label Distribution Protocol (Multicast LDP)

Multicast LDP pohjautuu MPLS-tekniikkaan. MPLS-tekniikka poikkeaa normaalista IP-reitityksestä. MPLS käyttää lipuiksi kutsuttuja otsikkomerkintöjä, joiden avulla pakettien kytkentä, ja niiden kuljetus verkon läpi hoidetaan. Tämän ansiosta on mahdollista kuljettaa useita eri protokollia yhden verkkoinfrastruktuurin läpi. Lisäksi MPLS yhdistää Layer 2- ja Layer 3 -tekniikoiden parhaat ominaisuudet. MPLS-tekniikka luo ja ylläpitää LSP-polkuja verkon reunalaitteiden välillä. Tästä syystä pelkästään verkon reunalaitteiden on ymmärrettävä verkkoliikenne sen alkuperäisessä muodossa. Verkon loput laitteet toimivat vain välikappaleina koko reititysprosessissa. (RFC 3031 2001.)

Multicast Label Distribution Protocol on protokolla, jolla reitittimet kykenevät vaihtamaan label-mapping tietoja, vaikkakin sen tärkeimpänä tehtävänä on sidoksien mainostaminen naapurireitittimille. Normaalin LDP-viestittämiseen verrattuna se tarjoaa mahdollisuuden lähettää *point-to-multipoint* ja *multipoint-to-multipoint* -viestejä. *LDP*:n tarkoitus on rakentaa ja ylläpitää LSP tietokantoja, joita käytetään välittämään liikennettä MPLS-verkoissa. Kahden reitittimen istuntoa kutsutaan LDP-istunnoksi ja niiden tiedonvaihto on kaksisuuntaista. LDP tarvitsee IGP-reititysprotokollan toimiakseen, koska se toimii OSI-mallin kuljetuskerroksella. (Experience with the Label Distribution Protocol 2007.)



Kuva 9. LDP-istunnon muodustuminen. (Pignataro, Kazemi, Dry 2002.)

4.2.1 Multicast LDP kehysrakenne

LDP:n informaationvaihdot suoritetaan TCP-yhteyden välityksellä lähettämällä PDU:ja (Protocol Data Unit). Jokainen PDU sisältää yhden tai useamman viestin. Näiden ei tarvitse olla toisiinsa liittyviä viestejä. LDP-viestit ovat Type-Lenght-Value-kehysrakenteisia viestejä. Jokaisen viestin pitää siis olla kehystettynä Type-Lenght-Value-merkkausta käyttäen. TLV-kehys koostuu:

- Type-kentästä, jonka pituus on 14 bittiä. Se sisältää tiedon LDP-viestin tyypistä.

- Lenght-kentästä, jonka pituus on 16 bittiä. Lenght-kenttä sisältää LDP-viestin pituuden oktetteina.

- Value-kentästä, jonka pituus muuttuu. Tämä sisältää LDP-viestin arvot. (Vatanen 2010, 29.)

4.2.2 Multicast LDP viestittäminen

LDP hyödyntää neljää eri viestikategoriaa:

1. *Discovery-viesti*. Käytetään reitittimien mukanaolon ilmoittamiseen ja ylläpitämiseen verkossa.

2. *Session-viesti*. Käytetään LDP reitittimien välisten istuntojen muodostamiseen, ylläpitoon ja päättämiseen.

3. *Advertisement-viesti*. Käytetään leimojen luomiseen, muuttamiseen ja poistamiseen tietovuoista.

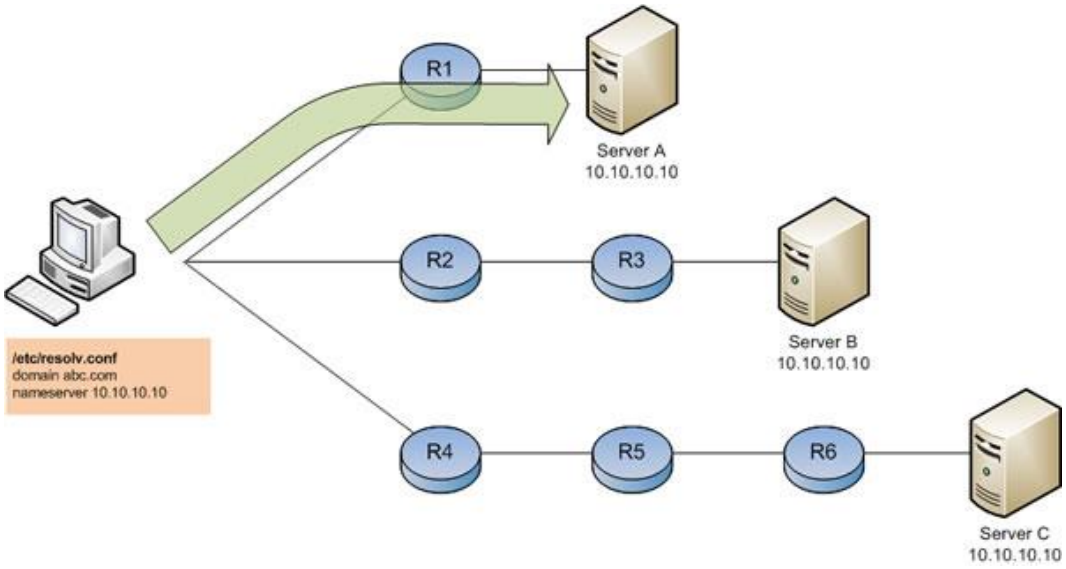
4. *Notification-viesti*. Käytetään lisäinformaation tuomiseen ja virheellisen tiedon havaitsemiseen.

Multicast LDP tarvitsee luotettavan ja järjestyksenmukaisen viestin siirron. Tämän vuoksi se käyttää TCP-yhteyttä advertisement- ja notification-viesteille. Discovery-

viesteissä, joita käyttämällä reitittimet lähettävät Hello-viestejä ilmoittaakseen läsnäolonsa verkossa, käytetään UDP-protokollaa. (Vatanen 2010, 28.)

4.3 Anycast

Anycastilla tarkoitetaan viestin lähettämistä ryhmälle siten, että lähetetty viesti päätyy tietyille ryhmän jäsenille. Perustuen reitityksen tietoihin, anycast tunnistaa lähimmän solmun ja kohdistaa viestin siihen. Tämän vuoksi oikea reititys on anycastin kannalta tärkeä verkon osa: se tarjoaa mahdollisuuden palvelujen vastaanottamisen useista eri lähteistä yhdellä IPv6-osoitteella. Anycastia voidaan käyttää kaikenkokoisissa verkoissa ja se on myös todella tehokas tapa jakaa verkossa esiintyvää kuormaa.



Kuva 10. Esimerkki anycastin käytöstä. Viesti välitetään lähimmälle päätteelle. (Anycast DNS - Part 1, Overview 2010.)

Anycast-osoitteita on lähes mahdoton erottaa unicast-osoitteista, koska anycast-osoitteet varataan unicastin osoitealueelta. Kun unicast-osoite määritetään usealle eri liityntäportille, siitä tulee anycast-osoite. Solmut, johon anycast-osoitteet on määritelty, on esitettävä erittäin selkeästi jotta niitä ei sekoiteta unicast-osoitteisiin. (Blanchet 2008, 273.)

4.3.1 Anycast Rendezvous Point (Anycast RP)

Anycast RP on hyödyllinen MSDP-sovellus, joka alun perin kehitettiin ryhmälähetys-sovelluksiin. Anycast RP:tä käytetään yleensä PIM-SM:n rinnalla täyttämään yhden ryhmälähetys-domainin vaatimukset.

Anycast RP:ssä kahdelle tai useammalle RP:lle on määritetty sama loopback-osoite, jonka tulisi olla 32-bittinen ollakseen isäntäosoite. Kaikkien muiden reitittimien pitäisi tietää, että kyseinen loopback-osoite on RP:n lokaali osoite. Reititys valitsee automaattisesti lähimmän RP:n osoitteen jokaista lähetystä ja vastaanottamista varten. Kun lähde rekisteröityy yhteen RP:hen, niin sanottu SA viesti lähetetään muille, että tämä reititin toimii nyt aktiivisena lähteenä. Tuloksena verkon jokainen RP oppii, että tietylle ryhmälähetys-ryhmälle on jo olemassa lähde. Mikäli tämä RP jostakin syystä epäonnistuu viestin lähettämisessä, voi toisesta RP:stä tulla aktiivinen. Näin jokaista lähetettävää ja vastaanotettavaa viestiä kohden on aina varalla vähintään yksi RP. (Anycast RP, 2013.)

4.3.2 Anycast Domain Name System (Anycast DNS)

Monet DNS-järjestelmät tukevat nykyisin anycast-menetelmää: juuripalvelimet, yksittäiset henkilöt ja suuret yritykset. Anycastin nimipalvelujärjestelmällä on useita etuja, kuten luotettavuus, palvelunestohyökkäyksien torjuminen, sekä suorituskyvyn parantaminen tuomalla käyttäjät lähemmäs palvelimia. Anycast Domain Name Systemillä on erilaisia vaatimuksia, jotta sen toiminta varmistetaan:

- Anycast-osoitteiden sisällyttäminen osaksi reititettyä verkkoa. Tämä voidaan toteuttaa käyttämällä joko staattisia reittejä, tai käyttäen eri reititysprotokollia, kuten BGP:tä, OSPF:ää tai RIP:iä.

- Nimipalvelimien pitäisi kuunnella anycast IP-osoitteiden DNS-pyyntöjä.

- Nimipalvelimiin pitäisi konfiguroida ainakin yksi anycast IP-osoite loopbackiin. Lisäksi palvelimiin pitäisi konfiguroida yksi hallinta-IP-osoite, joka voi olla fyysinen tai ylimääräinen loopback rajapinta.

- Ainakin yksi fyysinen IP-osoite on määriteltävä reititystietojen vaihdosta varten.

- Nimipalvelimet pitäisi konfiguroida käyttämään fyysistä tai hallinnon IP-osoitteistoa tiedonsiirtoja ja päivityksiä varten, jotta mahdolliset vastaukset eivät menisi väärille palvelimille. (Anycast DNS, 2010)

4.3.3 Anycast Domain Name Systemin hyödyt.

Lisääntynyt luotettavuus. Anycast parantaa luotettavuutta, koska saman IP-osoitteen takana on useita eri palvelimia maantieteellisesti eri alueilla. Redundanttisesti toimivat palvelimet parantavat palvelun saatavuutta ja luotettavuutta.

Kuormantasaus. Layer 3 -tason anycast-reitittäminen tasapainottaa tehokkaasti DNS-kyselyitä, jolloin viiveajat pienenevät.

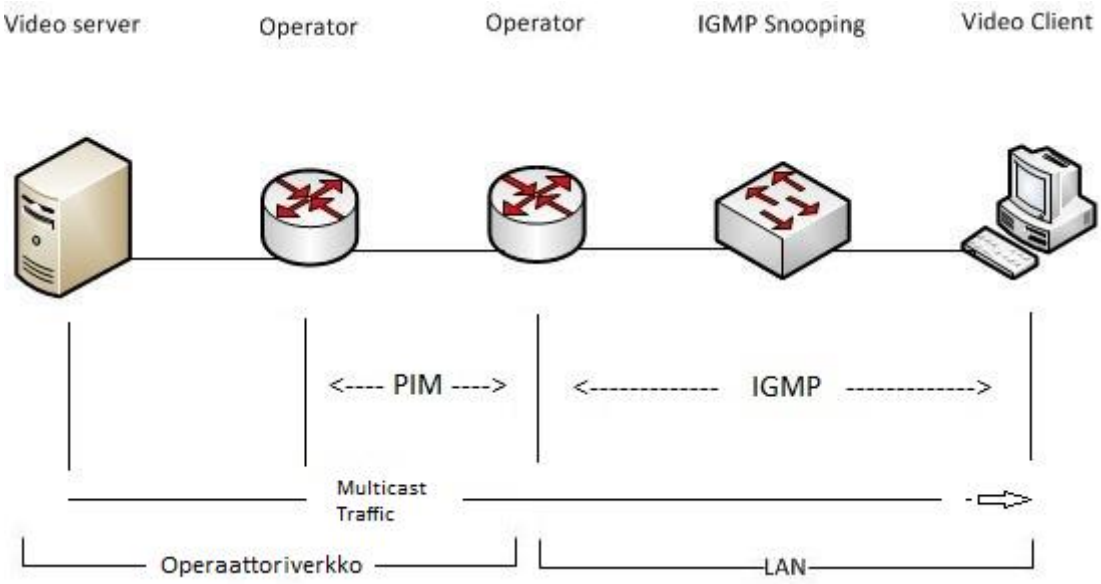
Parempi suorituskyky. Anycast DNS -palvelimille tarkoitetut paketit ohjautuvat lähimpään palvelimeen verkkotopologian mukaisesti. Tämä auttaa varmistamaan, että DNS-asiakkaat kohdistavat kyselyt paikalliseen palvelimeen.

Parempi turvallisuus. Maantieteellisesti hajallaan olevat
DNS-palvelimet, jotka toimivat käyttäen samaa IP-osoitetta tekevät palvelusta joustavampia DoS ja/tai DoSS hyökkäyksiä kohtaan, koska on huomattavasti vaikeampaa hyökätä verkkoon, jonka isännät käyttävät kahdennettua IP-järjestelmää. Mahdollisten hyökkäysten sattuessa ne ovat yleensä paikallisia ja vaikuttavat vain pieneen osaan koko Anycast DNS -ryhmästä.

Lisääntynyt saatavuus. Mikäli jokin palvelin ei ole käytettävissä esimerkiksi kunnossapidollisista syistä johtuen, on sillä erittäin pienet vaikutukset koko palveluun. Tällöin alhaalla olevat reitit poistetaan reititystaulusta. Lisäksi reititys määrittää hyvinkin nopeasti uuden vaihtoehtoisen reitin. (Anycast DNS 2010.)

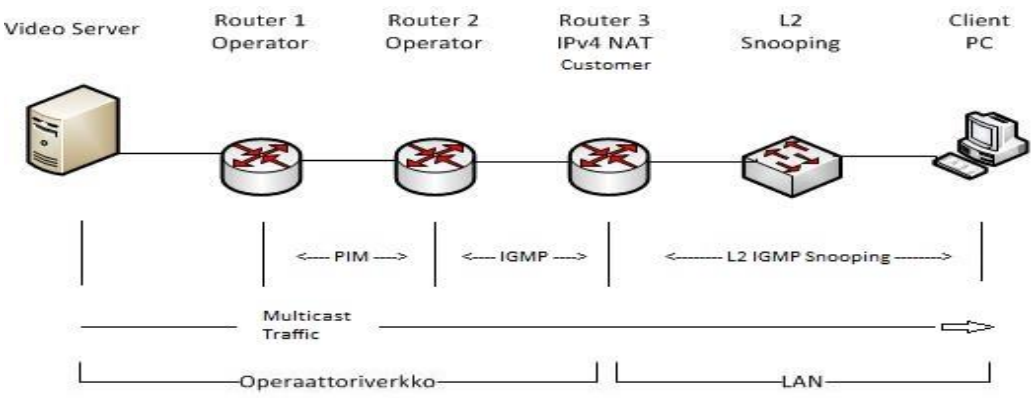
5 RYHMÄLÄHETYSTEN TESTAUSJÄRJESTELYT

Seuraavassa esitellään neljä erilaista ryhmälähetystilannetta. Kytkennät ovat samalla opinnäytetyössä varsinaisen työn perusta.



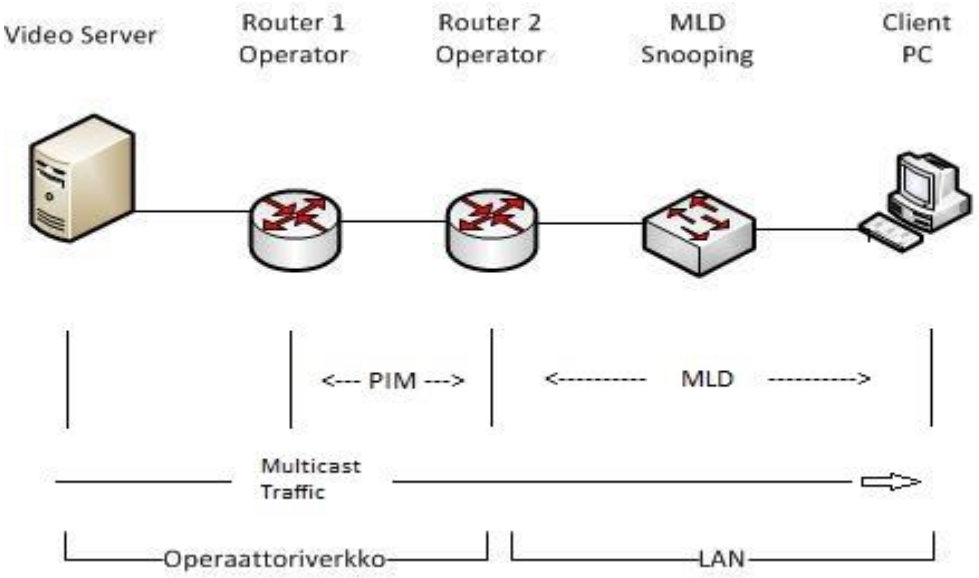
Kuva 11: IGMP verkon osana.

IGMP on tarkoitettu päätelaitteen ja sen oman yhdyskäytäväreitittimen väliseen liikenteeseen, eikä suinkaan ulkoverkkoon. Ilman IGMP Snooping -tekniikkaa kytkin lähettäisi kaikki paketit yleislähetyksinä. Tällöin kaikki aliverkon jäsenet saisivat multicast-viestin, vaikka ne eivät kuuluisikaan mihinkään ryhmään. IGMP Snooping -tekniikan avulla kytkin oppii ketkä aliverkon jäsenet kuuluvat mihinkin multicast-ryhmään. Näiden tietojen perusteella kytkin osaa lähettää paketit oikeille vastaanottajille.



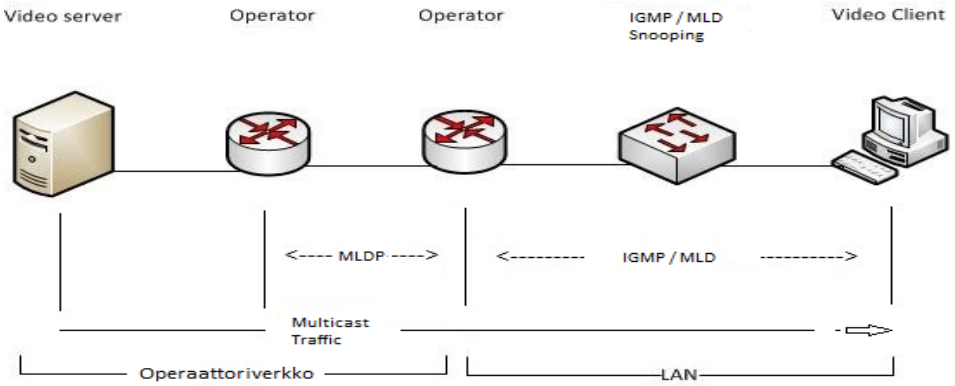
Kuva 12: IGMP proxy verkon osana.

Tässä laajennetussa verkkoratkaisussa IGMP proxy kuuntelee palveluntarjoajan reitittimiä. IPv4-maailmassa operaattoriverkkotasolla käytetään PIM-reititysprotokollaa. Operaattoritasolta siirryttäessä käyttäjän lähiverkkoon, PIMiä ei enää hyödynnetä, vaan käytössä on silloin IGMP, joka on tarkoitettu lähiverkkoratkaisuihin. Verkossa käyttäjää lähinnä oleva kytkin toimii IGMP-kuuntelijana.



Kuva 13: IGMP vaihdettuna MLD:hen.

Siirryttäessä IPv4-osoitteistosta IPv6-maailmaan, ensisijainen operaatio on vaihtaa IGMP MLD:hen. MLD Snooping -tekniikan avulla kytkin pystyy toteamaan ne portit, joissa on IPv6 Multicast -lähetyksen vastaanottajia. Tällä tavoin kytkin lähettää IPv6 Multicast -kehyksen niihin portteihin, joissa sitä tarvitaan. PIM on edelleen operaattoritasolla hyödynnetty protokolla.



Kuva 14: PIM korvattu Multicast LDP:llä.

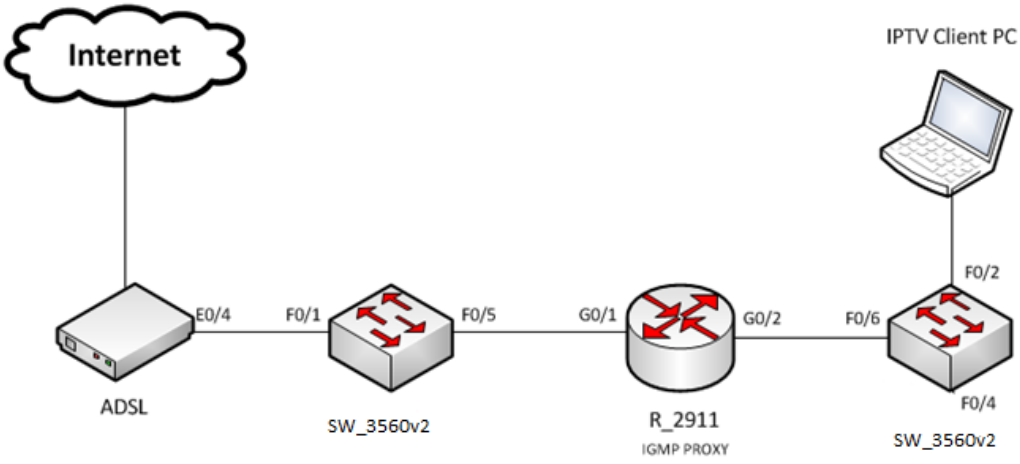
Multicast Label Distribution Protocol luo MPLS-lippukytkentäisen ryhmäjakeluverkon. Tämän vuoksi operaattoritasolla ei PIMiä enää tarvita. Lähiverkkotasolla käyttäjä voi halutessaan valita kumman tahansa protokollan, jolla se kuuntelee ulkoverkon lähetyksiä. Tässä työssä MLDP-protokollaa ei kuitenkaan käytetty vaan siihen perehdyttiin ainoastaan teoriatasolla.

6 RYHMÄLÄHETYKSEN KÄYTÄNNÖN TESTIT

Ensisijaisena työn tarkoituksena oli oppia ymmärtämään ryhmälähetysprotokollien tapaan toimia osana IPv4-, ja IPv6-verkkoja. Ryhmälähetyksen ollessa nopeassa kasvussa, on tärkeää ymmärtää sen toiminta sekä sen sisältämät ominaisuudet, jotka tehokkaasti vähentävät verkossa esiintyvää kuormaa. Kuormantasauksen ansiosta suuria datamääriä käsittelevät reitittimet eivät ruuhkaudu, joka edesauttaa pätkimisen ja yhteyksien takkuilun ennaltaehkäisemistä.

Tässä työssä saapuva data oli paikallisen palveluntarjoajan IPTV.

Ensimmäinen kytkentä näytti seuraavalta:



Kuva 15. Työn ensimmäinen kytkentä.

Työn edetessä, toimeksiantajan uusien toiveiden mukaan pyrittiin lisäämään laitteita sekä haluttuja määrityksiä reitittimiin ja kytkimeen.

6.1 Alkutilanne

Valittiin käyttöön yksi 2911-sarjan reititin, sekä 2800-sarjan kytkin. Lisäksi otettiin käyttöön yksi virtuaalikone, jolla toistettaisiin IPTV lähetystä VLC Media Playerin Firefox-pluginin avulla.

Konfigurointi aloitettiin määrittämällä isäntälaitteen nimi, sekä tarvittavat salasanat eri linjoille. Reitittimen käynnistyessä ensimmäistä kertaa verkon osana, se löysi itselleen ulkopuolen liityntäporttiin IP-osoitteen automaattisesti DHCP:n avulla. Sisäpuolen liityntäportin IP-osoite määritettiin manuaalisesti.

Määritettiin DHCP:lle nollareitti, sekä määritettiin DHCP jakamaan sisäpuolen työasemille IP-osoitteita seuraavalta alueelta: 172.16.14.100 - 172.16.14.200. NAT-määritykset tehtiin niin, että sisäpuolen työasemat kuuluivat NAT inside -puolelle ja reitittimen ulkoportti NAT outside -puolelle.

```
Router1(config)# ip dhcp pool OPPARI
Router1(dhcp-config)# network 172.16.14.0 255.255.255.0
Router1(dhcp-config)# default-router 172.16.14.1
Router1(dhcp-config)# dns-server 80.248.96.130
Router1(dhcp-config)# domain-name ictlab.kyamk.fi
Router1(config)# ip route 0.0.0.0 0.0.0.0 dhcp
Router(config)# ip dhcp excluded-address 172.16.14.1 172.16.14.100
Router(config)# ip dhcp excluded-address 172.16.14.200 172.16.14.254
```

Myöhäisemmässä vaiheessa työtä osa osoitteista vaihdettiin johtuen opinnäytetyön uusista ominaisuuksista. Seuraavaksi määritettiin NAT:

```
Router1(config)# access-list 1 permit 172.16.0.0 0.0.255.255
Router1(config)# ip nat inside source list 1 interface Gi0/1 overload
Router1(config)# interface Gi0/1
Router1(config-if)# ip nat outside
Router1(config-if)# exit
Router1(config)# interface Gi0/2
Router1(config-if)# ip nat outside
Router1(config-if)# exit
```

Komennolla *show ip nat translations* saatiin näkyviin NAT:n tulokset, jonka mukaan osoitteenmuunnin toimi halutulla tavalla.
Määritettiin vielä *domain-name* ja *name-server* kohdistumaan Kymen Puhelimeen:

```
Router1(config)# ip domain-name kymp.net
Router1(config)# ip name-server 80.248.96.130
```

Kytkimeen luotiin uusi VLAN, sekä määritettiin työn kannalta tarpeelliset portit hyväksymään liikenteen tietyn VLAN:n sisällä. Määritettiin myös *default-gateway*, jolla osoitettiin Router1:n sisäporttiin. Lisäksi määritettiin *name-serveriksi* Kymen Puhelimen DNS-palvelin, koska tässä vaiheessa haluttiin luoda yhteys vain Kymen Puhelimeen, ei muihin ulkoverkon osoitteisiin. Ihan ensimmäisenä kuitenkin määritettiin *Switch* käyttämään myös IPv6-osoitteistoa.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config#) reload

Switch(config)# ip name-server 80.248.96.130
Switch(config)# ip default-gateway 172.16.14.1

Switch(config)# interface Vlan14
Switch(config-if)# ip address 172.16.14.99 255.255.255.0
Switch(config-if)# no shutdown

Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 14

Switch(config)# interface FastEthernet0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 14
```

Virtuaalikone liitettiin Ethernet-kaapelilla kytkimen porttiin Fa0/6. Määriteltiin virtuaalikone hakemaan IP-osoite itselleen automaattisesti DHCP:n avulla. Virtuaalikone saikin osoitteekseen ensimmäisen vapaana olevan osoitteen rajatulta alueelta, joka oli *172.16.14.101*.

6.2 IGMP-ryhmälähetysprotokollan lisääminen osaksi verkkoa

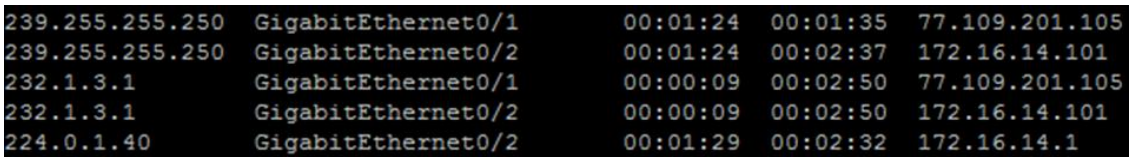
Peruskonfiguroinnin jälkeen oli vuorossa IGMP proxyn konfigurointi. Tämä toteutettiin asettamalla ensin *ip multicast-routing* päälle reitittimen peruskonfiguraatiotilassa. Tämän jälkeen lisättiin tarvittavat määritykset reitittimen liityntäportteihin, joilla

käynnistettiin IGMP, määritettiin sen tila ja osoitettiin se omasta liityntäportista toiseen liityntäporttiin. IGMP käyttää automaattisesti Version 2:sta, eikä sen muuttaminen ole tarpeen.

Router1(config)# interface Gi0/1
Router1(config-if)# ip igmp proxy-service
Router1(config-if)# ip pim sparse-dense-mode
Router1(config-if)# ip igmp mroute-proxy Gi0/2
Route1r(config-if)# exit

Router1(config)# interface Gi0/2
Router1(config-if)# ip igmp proxy-service
Router1(config-if)# ip pim sparse-dense-mode
Router1(config-if)# ip igmp mroute-proxy Gi0/1
Router1(config-if)# ip igmp helper-address 80.248.96.130

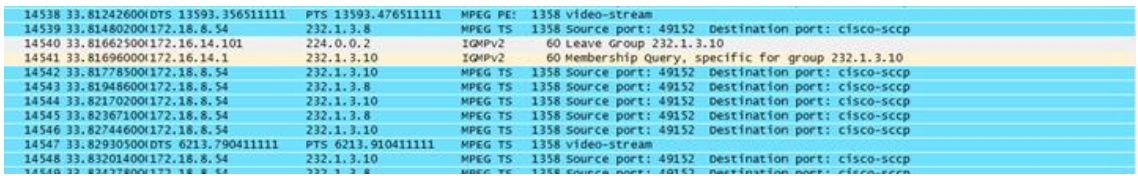
Komennolla *mroute-proxy* osoitettiin IGMP-palvelu ulkoportista sisäporttiin ja toisin päin. Ilman, että *mroute-proxy* -komento määritettiin molempiin portteihin, kuva pikselöityi pahasti, eikä IPTV:n katsominen olisi ollut mahdollista suurien kuvahäiriömäärien takia.



239.255.255.250	GigabitEthernet0/1	00:01:24	00:01:35	77.109.201.105
239.255.255.250	GigabitEthernet0/2	00:01:24	00:02:37	172.16.14.101
232.1.3.1	GigabitEthernet0/1	00:00:09	00:02:50	77.109.201.105
232.1.3.1	GigabitEthernet0/2	00:00:09	00:02:50	172.16.14.101
224.0.1.40	GigabitEthernet0/2	00:01:29	00:02:32	172.16.14.1

Kuva 16. IGMP-ryhmät. Kuvassa näkyy osoite, josta IPTV-palvelu lähetetään, ja sen reitti, sekä missä lähetystä vastaanotetaan.

IPTV-lähetys käynnistettiin osoitteessa **http://pctv.kymp.net**. Videolähetys saatiin onnistuneesti asiakaskoneen ruudulle. Tämän jälkeen tarkasteltiin vielä WireShark-ohjelmalla tietoliikennepakettien toimintaa. Ohjelmasta on selkeästi luettavissa kanavanvaihtoa koskevat tapahtumasarjat.



14538	33.81242600	DTS 13593.356511111	PTS 13593.476511111	MPEG PES	1358 video-stream
14539	33.81480200	172.18.8.54	232.1.3.8	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14540	33.81662500	172.16.14.101	224.0.0.2	IGMPv2	60 Leave Group 232.1.3.10
14541	33.81696000	172.16.14.1	232.1.3.10	IGMPv2	60 Membership Query, specific for group 232.1.3.10
14542	33.81778500	172.18.8.54	232.1.3.10	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14543	33.81948600	172.18.8.54	232.1.3.8	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14544	33.82170200	172.18.8.54	232.1.3.10	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14545	33.82367100	172.18.8.54	232.1.3.8	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14546	33.82744600	172.18.8.54	232.1.3.10	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp
14547	33.82930500	DTS 6213.790411111	PTS 6213.910411111	MPEG TS	1358 video-stream
14548	33.83201400	172.18.8.54	232.1.3.10	MPEG TS	1358 Source port: 49152 Destination port: cisco-sccp

Kuva 17. Wireshark-ohjelmalla kaapattu tilanne kanavanvaihdosta.

6.3 Siirtyminen IPv6-protokollaan

Kytkentä muutettiin kokonaan. Lisäksi se siirrettiin KyAMK:n ICTLAB-ympäristöön, jolloin *domain namet* sekä DNS-palvelimet piti vaihtaa globaaleihin osoitteisiin, jotta Internet toimisi. Kaikki *ip domain namet* vaihdettiin osoitteeseen *ictlab.kyamk.fi*. Lisäksi DNS-palvelimeksi määritettiin myös *ictlab.kyamk.fi*, jolloin reititin haki itselleen oikean dns-palvelimen osoitteen.

```
Router1(config)#ip dhcp pool OPPARI
Router1(dhcp-config)# domain-name ictlab.kyamk.fi
Router1(dhcp-config)# dns-server ictlab.kyamk.fi
```

Myös ip name-server jouduttiin vaihtamaan osoitteeseen *10.5.1.2*.

Kun kaikki IPv4:ään liittyvät osoitteet oli saatu korjatuksi, siirryttiin IPv6:een. ADSL-modeemin tilalle vaihtui KyAMK:n laboratorion oma kytkin, josta IPv6-osoitteet saatiin jaetuksi sisäverkkoon. Kun kytkentä oli korjattu, määritettiin molemmille GigabitEthernet-porteille omat IPv6-osoitteet.

```
Router2(config)# interface Gi0/1
Router2(config-if)# description Port to Outside
Router2(config-if)# ipv6 enable
Router2(config-if)# ipv6 address 2a00:1dd0:100:3003::2/64
Router2(config-if)# no shutdown
Router2(config-if)# exit

Router2(config)# interface Gi0/2
Router2(config-if)# description Port to Inside
Router2(config-if)# ipv6 address 2a00:1dd0:100:3003::1/64
Router2(config-if)# no shutdown
Router2(config-if)# exit
```

Määrityksellä *ipv6 unicast-routing* määritettiin, että myös IPv6 paketit liikkuvat reitittimien rajapintojen välillä. Lisäksi määritettiin IPv6 DHCP-palvelin reitittimen sisäporttiin, jotta sisäverkossa oleva pääte saisi myös IPv6-osoitteen IPv4:n rinnalle.

```
Router2(config)# ipv6 unicast-routing
Router2(config)# ipv6 dhcp pool OPPARI_ipv6
Router2(config-dhcp)# dns-server ictlab.kyamk.fi
Router2(config-dhcp)# domain-name ictlab.kyamk.fi
```

Viimeiseksi määritettiin molempiin reitittimen portteihin paikallinen *link-local* -osoite, sekä komento *nd other-config-flag*, jolla mainostetaan IPv6DHCP -määrityksiä. Lisäksi määritettiin Gi0/2 -portti jakamaan DHCP:n palveluja sisäverkkoon.

```
Router2(config)# interface Gi0/1
Router2(config-if)# ipv6 address FE80::1 link-local
Router2(config-if)# exit
Router2(config)# interface Gi0/2
Router2(config-if)# ipv6 address FE80::2 link-local
Router2(config-if)# ipv6 nd other-config-flag
Router2(config-if)# ipv6 dhcp server OPPARI_ipv6
Router2(config-if)# exit
```

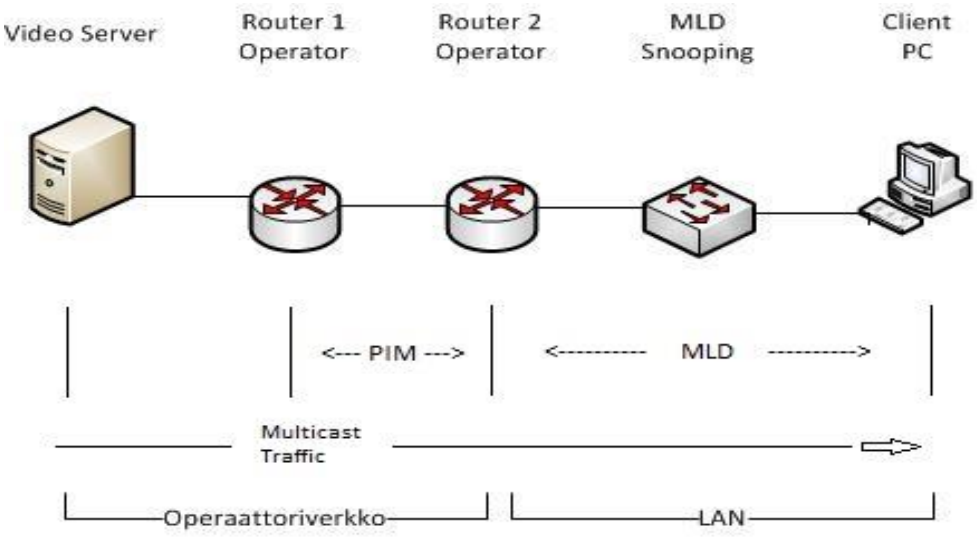
Kuvasta 19 ilmenee, että palvelin saa tiedot, jotka sille on määritetty antamaan.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : ictlab.kyamk.fi
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-89-FB-A2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2a00:1dd0:100:3003:4546:ad33:df2d:23e4(Pr
eferred)
   IPv6 Address. . . . . . . . . . . : 2a00:1dd0:100:3005:4546:ad33:df2d:23e4(Pr
eferred)
   Temporary IPv6 Address. . . . . . : 2a00:1dd0:100:3003:f96a:67c1:1d6d:16d3(Pr
eferred)
   Temporary IPv6 Address. . . . . . : 2a00:1dd0:100:3005:f96a:67c1:1d6d:16d3(Pr
eferred)
   Link-local IPv6 Address . . . . . : fe80::4546:ad33:df2d:23e4%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.14.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 19. maaliskuuta 2013 13:08:26
   Lease Expires . . . . . . . . . . : 20. maaliskuuta 2013 13:08:26
   Default Gateway . . . . . . . . . : fe80::ced5:39ff:fe41:ab41%11
                                       fe80::2%11
                                       172.16.14.1
   DHCP Server . . . . . . . . . . . : 172.16.14.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-D9-FF-82-00-0C-29-89-FB-A2

   DNS Servers . . . . . . . . . . . : 10.5.1.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Kuva 18. Virtuaalikoneen DHCP:ltä saamat IP-osoitteet.

6.4 MLD-ryhmälähetysprotokollan lisääminen osaksi verkkoa

MLD:tä varten verkko muutettiin vastaamaan testijärjestelyt-vaiheessa luotua verkkoa. Vaikka MLD on hyvin samanlainen protokolla kuin IGMP, ovat näiden protokollien määritykset kuitenkin hyvin erilaisia johtuen IPv4:n ja IPv6:n välisistä eroista. IGMP:n sijaan MLD hyödyntää IPv6:tta, joten kaikki määritykset oli tehtävä sen mukaisesti. MLD:n lisäysvaiheessa haluttiin hyödyntää testausjärjestely-vaiheessa käytettyä valmista pohjaa.



Kuva 19: MLD:n lisääminen verkon osaksi.

Varsinainen MLD:n määritys poikkeaa kuitenkin huomattavasti IGMP:n määrityksistä, vaikka nämä kaksi protokollaa ovat perustaltaan hyvin samanlaiset. MLD:tä varten sisäporttiin määritettiin seuraavia arvoja: Group, joksi valittiin sellainen yleinen multicast-osoite, jolla käsitetään lähiverkon kaikki segmentit. Lisäksi määritettii se enimmäisaika, jolla MLD-kyselyitä mainostetaan (*query-max-response-time)*, aika-arvo kyselylle, sekä se taajuus jolla MLD lähettää kyselyitä. Lisäksi määritettiin myös ryhmän maksimikoko. Versioksi valittiin MLD:n versio 2, joka on MLD:n oletusversio.

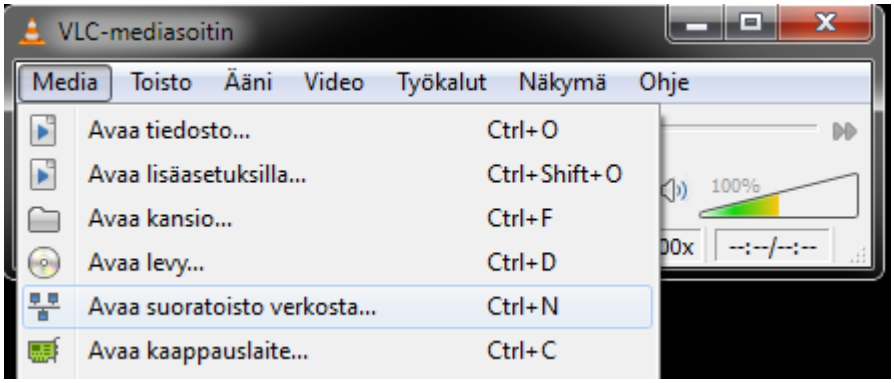
```
Router2(config)# interface Gi0/2
Router2(config-if)# ipv6 mld version 2
Router2(config-if)# ipv6 mld join-group FF02::1
Router2(config-if)# ipv6 mld query-max-response-time 20
Router2(config-if)# ipv6 mld query-timeout 150
Router2(config-if)# ipv6 mld query-max-response-time 15
Router2(config-if)# ipv6 mld query-interval 60
Router2(config-if)# ipv6 mld limit 100
Router2(config-if)# exit
```

Komennolla *show ipv6 mld interface* varmistettiin, että porttikohtaiset asetukset ovat kunnossa.

```
adsl-109-203-148#show ipv6 mld interface g0/2
GigabitEthernet0/2 is up, line protocol is up
  Internet address is FE80::2/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 60 seconds
  MLD querier timeout is 150 seconds
  MLD max query response time is 20 seconds
  Last member query response interval is 1 seconds
  Inbound MLD access group is: IPV6_MLD
  MLD activity: 57 joins, 49 leaves
  MLD Proxy is enabled for interface
```

Kuva 20: MLD:n porttikohtaiset asetukset.

Kun tarvittavat määritykset oli tehty MLD:tä vastaavaan porttiin, kytkettiin videota syöttävä palvelin päälle. Videopalvelimena toimivana koneella avattiin VLC Media Player -ohjelmalla suoratoisto verkosta. Suoratoisto ohjattiin IPv6:n mukaisesti videon lähteelle palvelimen IPv6-osoitteella. Satunnaisesti valittua videota pyöritettiin palvelimella varmistaakseen, että mitkään verkossa olevat laitteet eivät ruuhkaudu. Kun video lopulta suljettiin, tarkasteltiin arvoja ja paketteja, joita MLD oli saanut.



Kuva 21: Videostreamin avaus verkosta.

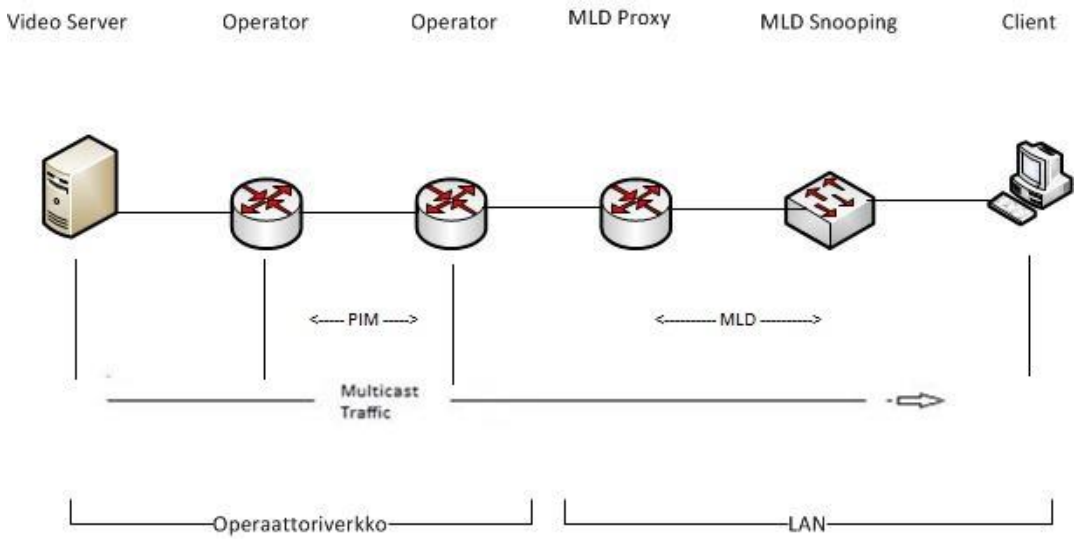
```
MLD Traffic Counters
Elapsed time since counters cleared: 04:45:05

                                Received      Sent
Valid MLD Packets                 1455         1095
Queries                           285          383
Reports                           1170         732
```

Kuva 22: Reitittimen välittämät MLD-paketit.

MLD:tä hyödyntämällä onnistuttiin saamaan kuva asiakaskoneen ruudulle. Videon aloitus kesti asiakaskoneella noin puoli minuuttia ennen kuin se sai yhteyden videopalvelinta mallintavaan koneeseen. Yhteyden saavutettua ei kuvassa esiintynyt häiriötekijöitä. IPv6:n yleistyessä tämä tekniikka tulee nostamaan päätään, mutta toistaiseksi se tuntui vaikeammalta kuin IGMP:n asetusten määrittäminen reitittimeen.

6.5 MLD Proxyn lisääminen verkon osaksi

MLD:n määritysten jälkeen verkkoon lisättiin vielä MLD Proxy. MLD Proxyn periaate on hyvin samanlainen kuin IGMP Proxy, nyt kyseessä on vain IPv6-maailmaan perustuva välityspalvelin. MLD Proxy tarjoaa mekanismin, jolla laite tuottaa MLD-jäsenraportteja käyttäen S, ja G -merkintöjä. MLD Proxy -toiminnon avulla laite on kykenevä oppimaan multicast-ryhmien jäsenyystiedot. Näiden tietojen perusteella se lähettää ryhmälähetyspaketit edelleen eteenpäin kohti sisäverkon laitteita.



Kuva 23: MLD Proxyn lisääminen verkon osaksi.

Ennen MLD Proxyn varsinaista määritystä, piti tässä työssä operaattoriverkon laitteita vastaavien laitteiden välille konfiguroida PIMv6-määritykset. Luotiin hyvin yksinkertainen sparse-dense-mode -yhteys kahden reitittimen välille. Molempiin reitittimiin asetettiin *ipv6 multicast-routing* -toiminto päälle. Ilman edeltävää komentoa PIMv6:n käyttö ei ole mahdollista. Lisäksi IPv6 PIMiä varten konfiguroitiin kiinteät IPv6-osoitteet, sekä rendesvouz point. Määritettiin myös *Hello* -viestien lähetysväli. Näiden määrityksien jälkeen PIMv6 löysi itselleen naapurin.

```
Router1#show ipv6 pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, G - GenID Capable
Neighbor Address          Interface          Uptime    Expires  Mode DR pri

FE80::21D:A1FF:FE4A:D858  Serial0/1/0        00:59:24  00:01:23 B G     1
```

Kuva 24: IPv6 PIM -naapuruussuhde.

Näiden jälkeen oli vuorossa vielä MLD Proxyn luonti. Verkkoon lisättiin kolmas reititin (Ks. kuva 23), joka vastasi asiakaspään reititintä. Tähän reitittimeen määritettiin MLD Proxyä koskevat asetukset. Tarkoituksena oli saada MLD Proxy toimimaan siten, että se oppisi multicast-ryhmien tiedot, ja välittäisi näitä tietoja eteenpäin edelleen kohti asiakaspään päätelaitteita.

Router3(config)# ipv6 mld host-proxy
Router3(config)# ipv6 mld host-proxy MLD_PROXY
Router3(config)# ipv6 mld host-proxy interface Gi0/2
Router3(config)# interface Gi0/2
Router3(config-if)# ipv6 mld query-max-response time 30
Router3(config-if)# ipv6 mld query-timeout 50

Edeltävillä komennoilla käynnistettiin MLD Proxy reitittimessä. Tämän jälkeen videopalvelinta mallintavalla laitteella käynnistettiin videostreami, johon asiakaskonetta vastaavalla laitteella yhdistettiin. Videon annettiin olla ruudulla hetken, jonka jälkeen tarkasteltiin Proxyn saamia arvoja komennolla *show ipv6 mld host-proxy*.

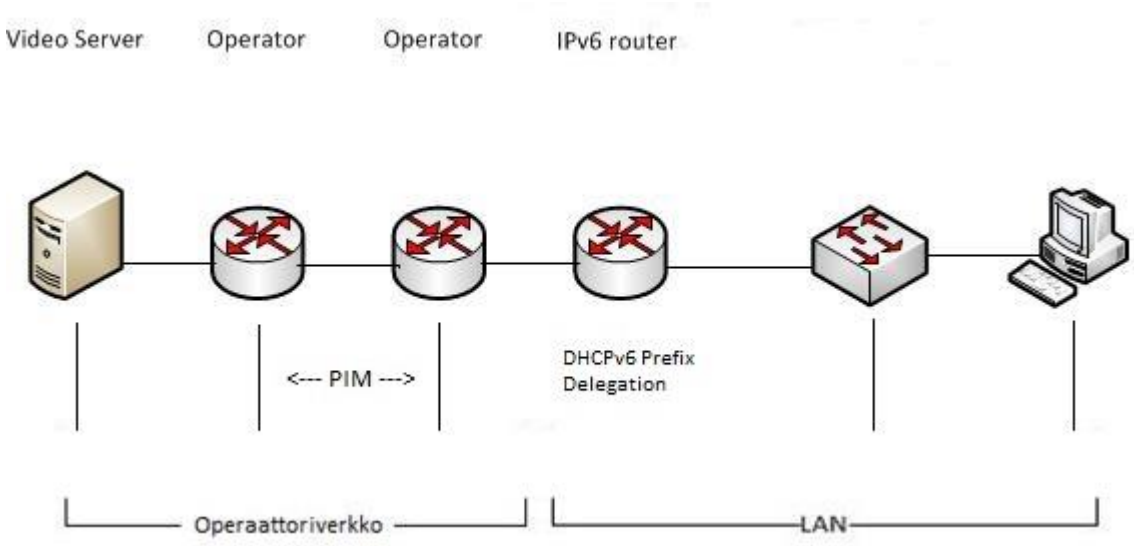
```
GigabitEthernet0/2 is up, line protocol is up
  Internet address is FE80::2
  Current MLD version is 2
  MLD querying router is FE80::2
  MLD max query response time is 30 seconds
  Current MLD proxy groups are 1
  Number of MLD queries received on interface is 5
  Number of MLDv1 reports sent are 0
  Number of MLDv2 reports sent are 12
  Number of MLDv1 leave sent are 0
  Number of MLDv2 leave sent are 4
```

Kuva 25: MLD Proxyn määritykset, ja ryhmiin liittymiset ja poistumiset.

Varmistaakseen, että MLD Proxy on toiminnassa, kirjoitettiin komento *show ipv6 mld interface gigabithethernet 0/2*, josta ilmenee että MLD Proxy on toiminnassa.

Videostreami avattiin samalla tavalla kuin aikaisemmassa vaiheessa. VLC:n asetusten mukaisesti videota toistettiin palvelimelta reaaliajassa. Tarkastellessa videon laatua ei mainittavia virheitä tapahtunut, kuten pätkimistä tai videon puuroutumista.

IPv6-maailmassa *Prefix Delegation* -komennon avulla asiakasryhmien reunalaitteille lähetetään niin sanottuja *prefiksejä* eli verkkotunnuksia. Nämä asiakaspään reitittimet jakavat prefixiltä saatuja IPv6-osoitteita edelleen sisäverkon päätelaitteille. *Prefix Delegation* -määrityksiä ei tähän opinnäytetyöhön kuitenkaan konfiguroitu.



Kuva 26: Prefix Delegation.

WireShark-ohjelmalla pystyttiin tutkimaan saapuvaa tietoliikennedataa helposti. Sen kautta pystyttiin näkemään linjalla tapahtuvat muutokset koskien multicast-protokollia, ryhmien vaihtoa, IPv4- ja IPv6 -osoitteiden muutoksia sekä reittiä, jota pitkin data kulkee.

IGMP-, eikä MLD Snooping -määrityksiä ei tässä opinnäytetyössä kytkimeen konfiguroitu johtuen verkon pienuudesta. Työn päämäärä oli teoriatasolla oppia miten tässä työssä käytetyt protokollat toimivat, sekä miten ne käytännössä määritetään laitteisiin silloin, kun niitä tarvitaan. Käyttäjän verkossa oli 2 päätettä, josta toisella tarkasteltiin IPTV-lähetystä, ja toisella saapuvaa dataa tarkkailtiin WireSharkilla.

7 YHTEENVETO

Työssä käytetyt elementit tarjoavat valtavasti erilaisia käyttömahdollisuuksia. Työ sisälsi monia erilaisia osa-alueita, joten oli tärkeätä rajata aiheet tarkasti, jotta työstä ei tulisi liian pitkä ja epäselvä. Työn edetessä sain uusia toiveita palveluntarjoajalta koskien lopullisen työni ominaisuuksia, kuten Multicast LDP:n ja anycastin lisäämisen verkon osaksi. Toiveiden ja vaatimusten kasvamisen vuoksi työ sisältää pintaraapaisun koskien protokollia, joita haluttiin hyödyntää. Kuitenkin voidaan todeta, että tässä työssä esiintyvien ryhmälähetysprotokollien perusajatukset tulivat selkeiksi, sekä ne lisättiin lopulliseen verkkoon onnistuneesti.

IGMP osoittautui suhteellisen helppokäyttöiseksi protokollaksi. Hyödyntämällä tätä protokollaa voidaan reitittimestä helposti tehdä välityspalvelin mille tahansa palvelulle. Tässä työssä sitä käytettiin, jotta reititin ja saapuva internetliikenne eivät tukehtuisi. Tässä onnistuttiin halutulla tavalla. IPTV toimi IGMP:n vuoksi moitteettomasti. Halutessaan IGMP -protokollaa hyödyntämällä voisi rakentaa verkon, johon sisältyisi useita reitittimiä ja kytkimiä. Mahdollisuuksien mukaan kyettäisiin testaamaan IGMP:n todellinen tehokkuus, sekä miten se käyttäytyy käsitellessään valtavia määriä sen lävitse kulkevia paketteja ja dataa.

Kun IPv6 lisättiin työhön, poikettiin hieman alkuperäisestä suunnitelmasta. IGMP ei tue lainkaan IPv6:tta, joten IGMP:n tilalle tarvittiin jokin muu protokolla. Protokollaksi valittiin Multicast Listener Discovery, joka vastaa IPv4:n IGMP:ä. MLD:llä rakennettiin kahden reitittimen välillä ryhmälähetysistunto ilman verkon ulkopuolisia lähteitä. Todettiin, että MLD toimii myös pienessä verkossa. Koska ulkopuoliset lähteet eivät olleet kuormittamassa kyseistä protokollaa, täydelliseen rasitustestiin ei päästy. Kuitenkin saatiin lupaavia tuloksia siitä, että MLD monimutkaisuudestaan huolimatta on tärkeä protokolla tulevaisuutta ajatellen, kun IPv6 jatkaa kasvuaan. Kuten IGMP:ssä, jatkona myös MLD:lle voitaisiin rakentaa suuri verkko, jossa liikkuvan datan määrä on valtava. Jotta saataisiin MLD varsinaiseen rääkkiin, pystyttäisiin toteamaan sen todellinen tehokkuus, sekä miten se käyttäytyy, kun joutuu taistelemaan valtavien pakettimäärien kanssa.

Multicast LDP eli Label Distribution Protocolin testaus suoritettiin myös pienessä verkossa kahden reitittimen väliin luodulla tunnelilla. Multicast LDP:llä on helppo luoda reitittimien välinen tunnelointi, joka perustuu MPLS:ään. Halutessaan kyseistä

tunnelointia voisi hyödyntää loputtomien reitittimien kanssa, joka mahdollistaisi MPLS-tekniikkaan perustuvat istunnot.

Anycastia käytettiin nopeaan testaamiseen. Työtä varten luotiin IPv6:lle omat rendezvous pointit sekä liityntäporteille omat anycast-osoitteet. Varsinainen testailu rajoittui anycast-osoitteiden toimivuuden kokeilemiseen, sekä rendezvous pointin määrittämiseen.

Jatkokehityksenä voisi tässä työssä käytettyjä protokollia ja ominaisuuksia hyödyntäen rakentaa suuremman verkon, jossa hyödynnettäisiin tehokkaasti esimerkiksi anycastin kohdistamista, ryhmälähetyksen rajausta tietyille tietokoneryhmille, sekä MPLS LDP:n ominaisuuksia usean eri verkon ja laitteen välillä. Tähän verkkoon luotujen MLD- ja LDP -ominaisuudet ovat suhteellisen pieni osa niiden kokonaiskuvaa, mutta kuitenkin niiden peruskäsitykset, sekä se, miten ne toimivat, tulevat hyvin ilmi. Kuitenkaan todelliseen testiin ne eivät päässeet. Multicast LDP:n osuus työssä jäi verrattain pieneksi, vaikka sen käyttömahdollisuudet ovat erittäin laajat. Sen perusajatus selvitettiin ja pieni osa sen tarjoamia ominaisuuksia lisättiin verkkoon. Pelkästään kyseisestä aiheesta saisi erittäin kattavan opinnäytetyön.

Lisäksi osana jatkokehitystä voisi olla Multicast LDP:n päivittäminen IPv4:stä IPv6:een. Toistaiseksi Ciscon laitteet eivät tue MLDP:tä IPv6-tekniikalla. Kun tämä mahdollistuu, voisi protokollaa hyödyntämällä rakentaa suuren verkon, joka perustuu Multicast LDP-protokollan hyödyntämiseen. Tällainen työ olisi esimerkiksi Kymenlaakson Ammattikorkeakoulun SimuNet-hanketta varten rakennettu, operaattoriverkkoa mallintava verkko. Sen kaikki PIM-protokollaa hyödyntävät operaatiot voitaisiin korvata täysin Multicast LDP:hen perustuvilla määrityksillä.

LÄHTEET

1. IPTV-järjestelmät. Saatavissa: http://www.tlu.ee/~matsak/telecom/lasse/ipTV/index.html [Viitattu 9.3.2013]

2. Suleva, L. 2011. IPTV:n asettamat vaatimukset verkolle ja palvelun toteutus SimuNetissä. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu. [Viitattu 22.3.2013]

3. Kankare, V. IPTV alueverkkojen näkökulmasta 12/2008. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/SimuNet_IPTV_aluedataverkossa_Kankare_20091207.PDF [Viitattu 22.3.2013]

4. Martin R. IPTV: Video's latest test frontier. 5/2006. Saatavissa: http://www.tmworld.com/design/design-and-prototyping/4386451/IPTV-Video-s-latest-test-frontier [Viitattu 22.3.2013]

5. Video-On-Demand. Saatavissa: http://www.cs.tut.fi/tlt/stuff/vod/VoDOverview/vod.html [Viitattu 14.3.2013]

6. IGMP, Internet Group Management Protocol. Saatavissa: http://www.networksorcery.com/enp/protocol/igmp.htm [Viitattu 20.3.2013]

7. Blanchet, M. 2008. Migrating to IPv6. Wiley Publishing, Inc. Eastbourne,

8. McFarland, S. Sambi, M. Sharma, N. Hooda, S. 2011. IPv6 for Enterprise Networks. Cisco Press. Indianapolis

9. Comer D. 2002. TCP/IP, IT Press. Helsinki.

10. Jaakohuhta, H. 2005, Lähiverkot - Ethernet. Ethernet-tekniikan soveltaminen käytännössä. IT-Press. Helsinki.

11. Casad, J. Willsey, B. 1999. TCP/IP Trainer. IT-Press. Helsinki.

12. Overview of IP Multicast. Saatavissa: http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080092942.shtml [Viitattu 22.3.2013]

13. Vatanen, M. 2010. Operaattoritasoisen reitityksen ja VPLS:n toteutus spidernetiin. Opinnäytetyö. Jyväskylän ammattikorkeakoulu.

14. Anycast RP - Cisco Systems. 2013. Saatavissa: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/anycast.html [Viitattu 22.3.2013]

15. Anycast DNS - Part 1, Overview. 2010. Saatavissa: http://www.netlinxinc.com/netlinx-blog/45-dns/118-introduction-to-anycast-dns.html [Viitattu 22.3.2013]

16. Multimedia Appliances. 2013. Saatavissa: http://www.vpod.tv/products/multimedia-appliances/ [Viitattu 25.3.2013]

17. Pignataro, C. Kazemi, R. Dry, B. 2002. Label Distribution Protocol (LDP): Overview. Saatavissa: http://flylib.com/books/en/4.280.1.44/1/ [Viitattu 25.3.2013]

18. Tunneling. 2002. Saatavissa: http://peiontrack.blogspot.fi/2012/04/tunneling_22.html [Viitattu 25.3.2013]

19. Teare, D. 2010. Implementing Cisco IP Routing (Route) [Viitattu 17.4.2013]

20. Internet Group Management Protocol. 2002. Saatavissa: http://tools.ietf.org/html/rfc3376 [Viitattu 17.4.2013]

21. RFC 3031, Multiprotocol Label Switching. IETF. Saatavissa: http://www.ietf.org/rfc/rfc3031.txt [Viitattu 18.4.2013]

22. Paananen, O. IPTV ja lisäarvopalvelut laajakaistaverkossa. 2006. Saatavissa: http://www.ad.jyu.fi/palhala/gradu_olavi.pdf [Viitattu 19.4.2013]