Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Joni Laaksonen

Ryhmälähetyssovellukset Metropolian laboratorioympäristössä

Insinöörityö 26.3.2010

Ohjaaja: yliopettaja Matti Puska
Ohjaava opettaja: yliopettaja Matti Puska

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä Otsikko Sivumäärä Aika	Joni Laaksonen Ryhmälähetyssovellukset Metropolian laboratorioympäristössä 100 sivua 26.3.2010
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja Ohjaava opettaja	yliopettaja Matti Puska yliopettaja Matti Puska

Tässä insinöörityössä käytiin läpi asioita joihin ryhmälähetysliikenne perustuu ja miten siitä voidaan tehdä sovelluksia koulun laboratorioympäristöön.

Teoriaosassa käytiin läpi ryhmälähetyssovelluksiin tarvittavat protokollat ja tekniikat. Myös tutustuttiin osa-alueihin, joissa käy ilmi ryhmälähetyksen idea, hyöty ja mahdolliset käytännönsovellukset. Työssä keskityttiin pitkälti multimediaan, videoon ja äänen suoratoistoon ja tutkittiin teoreettisesti kyseisten sovelluksien mahdollisuuksista.

Käytännön osuudessa mietitään, miten esimerkkiverkkojen kautta päästään ryhmälähetysliikenteeseen käsiksi. Multicast VRF:stä tuotiin esille vikasietoisuuteen ja liikenteen ohjautumiseen liittyvät edut. Lisäksi VRF:n tarvittavia määrittelyjä käytiin läpi. Myös pohditaan, miten liikennettä tulisi profiloida, jotta sovellukset tulisivat laitetasolla optimoiduksi.

Käytännön osuudessa tuli myös ilmi, kuinka ohjelmistopuolella päädyttiin tiettyyn mediantoistoympäristöön, VLC Media Playeriin. Erilaisten suoratoiston mahdollisuuksien toteuttamista katsotaan myös VLC-ohjelmiston ohella. Web-kameroiden tarjoamia ominaisuuksista tarkastellaan siten, miten ne sopivat eri ympäristöihin.

Lopuksi työssä tarjotaan esimerkkivisio siitä, miten koko työn sisältöä voidaan soveltaa eri toimipaikkojen välillä, ja keskitytään Metropolia Ammattikorkeakoulun Leppävaaran ja Bulevardin toimipisteiden välisiin verkkopalvelujen välittämiseen.

Hakusanat	IGMP, Multicast VRF, ryhmälähetys, VLC, VRF

Helsinki Metropolia University of Applied Sciences **Abstract**

Author Title Number of Pages Date	Joni Laaksonen Multicast applications for Metropolia school laboratory environment 100 26 March 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Matti Puska, Principal Lecturer Matti Puska, Principal Lecturer

The objective of this thesis work was to study what multicast traffic is based on and how it can be implemented in applications for the school laboratory environment.

The protocols and technologies needed for multicast applications were studied in the theoretical part Also, the different multicast uses were considered, which revealed the idea, potential benefits and practical applications of multicast transmission. The main focus was on multimedia video and audio streaming, whereby the possibilities of applications were theoretically approached.

The practical part is concerned with [finding out] how multicast transport access can be achieved by using example networks. Multicast VRF highlighted fault tolerance and gave insight into traffic interests. In addition, the VRF required specifications were reviewed. Another important consideration was how traffic should be profiled so that the applications would be optimized at device level.

The practical part also reveals how the software side ended up supporting a particular environment other than the media playback VLC Media Player. Different forms of streaming potential are also considered in the implementation of the software along with VLC. Webcam provided features shall be deemed based on how they fit different environments.

Finally, the thesis envisions how the entire content of my work can be applied to different facilities, principally focusing on the transmission network between Leppävaara and Bulevardi campuses.

Keywords	IGMP, Multicast, VRF, VLC, VRF

Sisällys

Lyhenteet

ABR	Area Border Router; alueen rajareititin
ALF	Application Layer Framing; sovellustason kehystys on tiedonsiirto-protokollan suunnitteluperiaate pakettiverkkoja varten
AS	Autonomous System; reititysalue
ASBR	Autonomous System Boundary Router; reititysalueen rajareititin
ASM	Any Source Multicast; ryhmälähetystekniikan nykyinen palvelumalli
BDR	Backup Designated Router; toimii DR-reitittimen varareitittimenä
CE	Customer Edge; asiakkaan reunalaite, joka kytkeytyy PE-reitittimeen
CEF	Cisco Express Forwarding; Ciscon lisensoima kolmostason kytkentätekniikka
CMOS	Complementary Metal Oxide Semiconductor; kanavatransistoreihin perustuva mikropiiritekniikka
DR	Designated Router; edustaa kaikkia saman verkkosegmentin reitittimiä
DVD	Digital Versatile Disc; optinen datan tallennusväline
DVMRP	Distance Vector Multicast Routing Protocol; ryhmälähetys-pohjainen reititysprotokolla
FPS	Frames per second; kuvataajuus eli näyttötekniikassa näytölle sekunnissa piirrettyjen kuvien määrää.
HD	High-definition; teräväpiirtotekniikka
HTML	Hypertext Markup Language; avoimesti standardoitu kuvauskieli
HTTP	Hypertext Transfer Protocol; protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon
IANA	Internet Assigned Numbers Authority; tahon, joka hallitsee osoitteita, porttinumeroita, protokollanumeroita ja muita Internetin parametreja
IGMP	Internet Group Management Protocol; TCP/IP-pinon protokolla, joka mahdollistaa asiakkaiden liittymisen lähetysryhmään
ILP	Integrated Layer Processing; tiedonsiirtoprotokollien toteutusmenetelmä

IP	Internet Protocol; internetissä käytettävä pakettimuoto
IPv4	Internet Protocol version 4; internetprotokollan yleisempi versio
IPv6	Internet Protocol version 6; kehittyneempi protokolla, joka on suunniteltu korvaamaan IPv4
IPTV	Internet Protocol television; internet-protokollan käyttöön perustuva teknologia niin televisio-ohjelman jakelussa kuin paluukanavassakin
IR	Internal Router; reitiysalueen sisäinen reititin
LAN	Local Area Network; lähiverkko
LSDB	Link State Database; linkkitilatietojen toiminnan tietokanta
MAC	Media Access Control; IEEE 802-verkoissa verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä
MBONE	Multicast Backbone; ryhmälähetysten runkoverkko
MOSPF	Multicast Open Shortest Path First; ryhmälähetyspohjainen reititysprotokolla
MPEG-TS	Moving Picture Experts Group- Tranport Stream; standardi, jonka tehtävä on suunnitella nykyaikaisia videonpakkaustapoja ja standardoida niitä.
MPLS	Multiprotocol Label Swithing; lippuinformaatiota käyttävä tiedonsiirtotapa
MSDP	Multicast Source Discovery Protocol; ryhmälähetyspohjaisien reititysprotokollien havaitsemiseen tarkoitettu protokolla
OS	Operating System; käyttöjärjestelmä
OSI	Open Systems Interconnection; tiedonsiirtoprotokollien yhdistelmä
OSPF	Open Shortest Path First; reititysprotokolla
P	Provider; palveluntarjoajan runkolaite
PE	Provider Edge; palvelun tarjoajan runkoreunalaitte
PIM	Protocol Independent Ryhmälähetys; ryhmälähetyspohjainen reititysprotokolla

PIM-DM	Protocol Independent Multicast Dense-Mode; ryhmälähetyspohjainen reititysprotokolla
PIM-SM	Protocol Independent Multicast Sparse-Mode; ryhmälähetyspohjainen reititysprotokolla
PoE	Power over Ethernet; tekniikka, jolla voidaan syöttää käyttöjännite esimerkiksi WLAN-tukiasemalle kierretyn parikaapelin avulla
QoS	Quality of Service; termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia
RAID	Redundant Array of Inexpensive Disks; tekniikka, jolla tietokoneiden vikasietoisuutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi
RD	Route Distinguisher; tunniste, jolla muunnetaan IPv4-osoite VPNv4-osoitteeksi.
RIP	Routing Information Protocol; reititysprotokolla
RP	Rendezvous Point; kohtauspaikka
RPF	Reverse Path Forwarding; tekniikka, jolla pyritään välttämään ryhmälähetys-reitityssilmukat.
RT	Route Target; väline reittien määritykseen VPN/VRF-yhteyksissä
RTP	Real-time Transport Protocol; tietoliikenneprotokolla tosiaikaisen datan, kuten äänen ja kuvansiirtoon pakettiverkoissa
SAP	Session Announcement Protocol; protokolla, joka lähettää ryhmälähetys-ryhmään mainostuksia säännöllisesti ryhmälähetysistunnoista
SDP	Session Description Protocol; protokolla, jolla voidaan kuvata internetin multimediaesityksiä tai -istuntoja
SPT	Shortest Path Tree; jakelupuumalli
TCP	Transmission Control Protocol; tietoliikenneprotokolla jolla luodaan yhteyksiä tietokoneiden välille sekä Internetiin
TTL	Time To Live; hyppyjen maksimimäärä siirtotiellä
UDP	User Datagram Protocol; yhteyskäytäntö, jolla sovellukset kommunikoivat

VGA	Video Graphics Array; IBM:n kehittämä näyttöstandardi
VLAN	Virtual Local Area Network; virtuaalinen lähiverkko
WLAN	Wireless Local Area Network; langaton lähiverkko
VLC	VLC media player; avoin ja alustariippumaton mediasoitin, joka on osa VideoLAN-projektia
VOD	Video On Demand; videotiedosto, joka ladataan katsojan tietokoneelle tai se esitetään suoratoistona
VPN	Virtual Private Network; virtuaalinen yksityisverkko
VRF	Virtual Routing and Forwarding; tekniikka, joka mahdollistaa usean reititystaulun käytön samanaikaisesti
WWW	World Wide Web; Internet-verkossa toimiva hajautettu hypertekstijärjestelmä

1 Johdanto

Opinnäytetyöni perustuu tietoverkkosovelluksiin, jota nykyisin käytetään multimedian välittämiseen verkon kautta. Työssäni perehdytään enimmäkseen ryhmälähetys-tekniikkaan, jota käytetään laajasti multimedian välittämiseen. Työn tavoitteena on toteuttaa sellaisia ryhmälähetyspohjaisia sovelluksia Metropolian laboratorioympäristöön, joita voidaan toteuttaa koulun resurssien puitteissa.

Sovelluksissa tulee ilmi, miten hallitaan tehokkaasti tietoliikenteen kuormitusta, videon tai äänen tiedonsiirtoa ja profiloidaan liikennettä. Työssäni käy ilmi myös, miten sopivat laitteet voidaan ottaa käyttöön ja tarjota niihen olevia median esitysympäristöjä.

Ryhmälähetys (Multicast) on tärkeä osa tietoliikennettä ja tarjoaa opiskelijoille hyvän pohjan ja tutustumisympäristön. Käytännön harjoituksien avulla opiskelijat voivat koulun laboratoriossa luoda multimediatestiverkkoja, joilla he pystyvät näkemään ja kokemaan ryhmälähetysten edut ja haitat. Opiskelija saa kuvan myös siitä, miten voidaan lisätä järjestelmän vikasitoisuutta ja oppia tekemään liikenteen ohjausta multicast VRF -pohjaisen (Virtual Routing and Forwarding) testiympäristön avulla.

Opinnäytetyön aiheen valitsin itse, koska aihe kiinnosti minua. Valintaan liittyi myös laaja ideointi ja ohjaajan opastus. Opinnäytetyöni pohjautuu sekä laajapuoliseen teoria- että käytännön osuuteen. Työssäni on sovelluksien rakentamista, toteuttamista ja testausta. Aiheen valinta tuli loppujen lopuksi helpoksi, koska se tarjosi haasteita ja sai sen kuulostamaan mielenkiintoiselta. Nykyisin ryhmälähetys tai suoratoisto tuntuu olevan jokapäiväistä multimediatietoliikennettä.

Ensimmäisessä luvussa käydään läpi ryhmälähetyssovelluksiin tarvittavat protokollat. Tämä on tarkeä osa-alue saada lukija perusymmärrykseen siitä, millaisen pohjan ryhmälähetysliikenne tarvitsee. Kolmannessa luvussa käsitellään tekniikat, joissa voidaan soveltaa ja monipuolistaa ryhmälähetysken käyttöönottoa. Luvussa 4 käydään ryhmälähetys perusteellisesti läpi, kuitenkin vain siten, että se liittyy työni sisältöön.

Kuitenkin mitään olennaista tai tärkeää ryhmälähetykseen liittyvää ei ole jätetty pois, joten lukija saa kattavan kuvauksen. Luvussa 5 käydään läpi virtuaalisuuden etuja.

Luku 6 lähestyy aihetta käytännön näkökulmasta, ja siinä puhutaan ryhmälähetys-pohjaisista sovelluksista. Seuraavassa luvussa lähdetään tutkimaan vaihe vaiheelta, mitä määrittelyjä ja esimerkkejä tarvitaan ryhmälähetysverkon luontiin. Luvussa 8 käydään läpi, miten tulisi suunnitella liikenteen profilointia verkossa, kun käytetään multimediaa, kuten videota ja ääntä. Luku 9 sisältää laajan perusmateriaalin siitä, miten saadaan VLC-mediasoittimella tehtyä ryhmälähetyssuoratoistoja myös etäkoneella. Luvussa 10 tarkastellaan web- ja verkkokameroita siinä mielessä, miten ne tekevät multimediasovelluksia ryhmälähetyksiä hyödyntäen. Lopuksi tarkastelen kokonaisuutta ja kommentoin yhteenvedossa mietteeni ja kokemukseni.

2 Ryhmälähetys- ja suoratoistoprotokollat

2.1 Internet Group Management Protocol

Internet Group Management Protocol (IGMP) on protokolla, jota käytetään hoitamaan jäsenyyksiä lähetysryhmään. IGMP:tä käyttävät isäntäkoneet ja vieressä olevat ryhmälähetysreitittimet. Protokolla kertoo vastauksena reitittimelle kaikki ryhmälähetys-osoitteet, joihin käyttäjän sovellukset ovat liittyneet. IGMP-protokolla myös toimii viestinnässä reitittimien välisessä siten, että määräajoin reitittimet lähettävät toisilleen tiedon, mitkä ryhmät ovat liittynyt verkkoon. IGMP Snooping toimii kytkimien ja työasemien välillä. [1.]

IGMP on olennainen osa IP-multicastia, jota käytetään verkkokerroksella, vaikka se ei varsinaisesti toimi reititysprotokollana. Se on samanlainen kuin ICMP täsmälähetys-yhteyksiä (unicast) varten. IGMP:tä voidaan käyttää verkossa oleviin suoratoisto-pohjaisiin video- ja peliympäristöihin ja mahdollistaa tehokkaammin resurssien käyttöä, kun tuetaan tämäntyyppisiä sovelluksia. IGMP:tä tarvitaan vain IPv4-verkkojen hallinnoimiseen, mutta ryhmälähetystä on käsiteltävä eri lailla IPv6-verkoissa [1.]

IGMP-versiot ja kehysrakenne

IGMP-versioita on kolme. IGMP-versio 1 kuvaa sen, kuinka IP-verkkojen (Internet Protocol, IP) koneet tekevät rekisteröintinsä lähetysryhmiin lähimmän ryhmälähetys-reitittimen avulla. Isäntäkoneet voivat liittyä ryhmälähetys-ryhmään, mutta tämä versio ei vielä pidä sisällään Leave Group -sanomaa. Ryhmästä poistuminen tapahtuu reitittimien aikarajan täyttyessä, kun se huomaa isäntäkoneen jättäneen ryhmän. IGMP-versio 2 ei myöskään ota kantaa siihen, mitä tapahtuu, eli kuinka rekisteröityminen tapahtuu, mitä viestejä menee minnekin, mitä osoitteita kukin käyttää, mistä ryhmälähetys tulee jne. IGMP-versio 3 sen sijaan ottaa kantaa siihen, miten näitä viestejä kulkee reitittimien ja koneiden välillä, mitä niille tehdään ja missä järjestyksessä niitä vastaanotetaan. [2.] Versioiden yleisyyteen en löytänyt lähdettä, mutta arvioin, että IGMPv3 alkaa olla yleisin, koska IGMPv3 julkaistiin jo vuonna

2002. Sitä kautta sen tietoturvan lisääminen ja myös valmistajien laitetuen saatavuus helpottavat sen toteuttamista käytännön ympäristöihin.

Kuvassa 1 on esitetty IGMP v2 -kehyksen rakenne.

+	Bits 0 - 7	8 - 15	16 - 23	24 - 31
0	Type	Max Resp Time	Checksum	
32	Group Address			

Kuva 1. IGMP v2 -kehyksen rakenne [1.]

Kuvassa olevat tietueet ovat seuraavat:

- Type eli sanoman tyyppi.
- Max. Response Time eli maksimivastausaika kyselyssä. Kun aika umpeutuu niin kyselyn kehys poistuu järjestelmästä, kunnes aloitetaan uusi kysely.
- Checksum eli tarkistussumman tarkoitus on tarkistaa kehyksen sisältö ja, kun summa ei täsmää niin kehys hylätään.
- Multicast Group Address eli ryhmälähetysosoite kertoo, mihin ryhmään IGMP-kehys on osoitettu.

IGMP-sanomat

IGMP-sanomia on kolmenlaisia: Membership Query, Report ja Leave Group. Membership Quarylla katsotaan, onko tiettyyn ryhmään kuuluvia tiettyjä ryhmiä olemassa tietyllä maksimivastausajalla (Time to Live, TTL). Membership Report antaa tiedon tapahtumasta, kun kone haluaa liittyä ryhmään tai on jo liittynyt ilmoitettuun ryhmään. Leave Group -sanoma antaa ilmoituksen siitä, että kone poistuu ryhmästä. Toisaalta, jos kone ei vastaa kyselyyn, tulee jäsenyydelle määritellä voimassaoloaika aikaraja. [3.]

IGMP Snooping

Kytkimet käsittelevät ryhmälähetys-liikennettä yleislähetysliikenteenä (broadcast), ellei käytetä IGMP Snooping-tekniikkaa. IGMP Snooping mahdollistaa vastaanottajan ja reitittimen välisten IGMP-sanomien tutkimisen kytkimen avulla. Kytkin kuuntelee IGMP-viestejä vastaanottajan ja reitittimen välillä ja viesteistä saamiensa tietojen perusteella päivittää MAC-tauluaan (Media Access Control, MAC). Kun kytkin kuulee vastaanottajan IGMP Leave -sanoman, se poistaa kyseisen MAC-taulumerkinnän. Näiden tietojen avulla kytkin osaa ohjata ryhmälähetysliikenteen oikeisiin portteihin. [4.]

2.2 Open Shortest Path First

Yleisin yhteystilareititysprotokolla ja oikeastaan IP-verkkojen lähes ainoa sellainen on OSPF (Open Shortest Path First). Linkkitilatietojen toiminnan perusta on LSDB- eli Link State Database -tietokannat. Sen ylläpito hoidetaan verkon kuormitusta säästävillä ryhmälähetyssanomilla aina kuin verkossa tuetaan ryhmälähetyksiä. [5, s. 94–95.]

Jos OSPF verkko kasvaa isoksi, ei ole enää tehokasta kasvattaa LSDB-tietokantaa. Tämän vuoksi OSPF-verkko voidaan jakaa alueiksi. Tällöin alueiden sisällä olevien reitittimien (Internal Router, IR) ei tarvitse käsitellä liian suurta määrää tietoa. Tällöin riittää, kun tiedetään minkä reitittimen kautta päästään naapurialueelle. Verkon täytyy olla melko suuri ennen kuin sitä kannattaa jakaa alueisiin. [5, s. 94–95.]

Aluejaon yhteydessä ABR-reitittimeksi (Area Border Router, ABR) valittujen reitittimien täytyy tietää tarkat tiedot kaikista alueista, joihin ne on liitetty. OSPF-verkon ja muilla reititysprotokollilla hallittujen verkkojen rajalla toimivia reitittimiä kutsutaan nimellä ASBR-reititin (Autonomous System Boundary Router, ASBR). [5, s. 94–95.]

OSPF-protokollan virheetön toiminta edellyttää, että saman OSPF-alueen sisällä olevien reitittimien LSDB-tietokannat ovat identtiset. Tämä varmistetaan luomalla ns.

täydellinen naapuruussuhde kaikkiin naapuri OSPF-reitittimiin. Täydellisen naapuruussuhteen edellytyksiä ovat muun muassa samat aliverkkopeitteet ja asetukset toipumiseen liittyvissä parametreissa ”hello interval” ja ”router dead interval”. [5, s. 94–95.]

Hello interval kertoo, kuinka usein OSPF-reititin lähettää naapurilleen Hello-viestejä. Nämä viestit kertovat reitittimien olevan toimintatilassa. Router dead interval on yleensä kolme kertaa niin suuri viive kuin hello interval. OSPF:n toipumisaikaa voidaankin säätää halutuksi muuntamalla ylläpitosanomien lähetystaajuutta. Neljä sekuntia on raja, jossa OSPF-verkko toipuu virheestä kuin virheestä, jos sanomia lähetetään niin usein kuin mahdollista. [5, s. 94–95.]

Vähänkin isoimmissa verkoissa syntyy melkoinen määrä liikennettä, jos kaikki reitittimet joutuisivat luomaan täydellisen naapuruussuhteen kaikkien muiden reitittimien kanssa. Tämän vuoksi multiaccess-pohjaisissa OSPF-verkoissa valitaan ns. Designated Router (DR), jonka kanssa täydellinen naapuruussuhde luodaan. Kun DR:llä on täydellinen naapuruussuhde kaikkiin reitittimiin, tiedetään, että kaikki reitittimet ovat toimintatilassa. Vahingon varalle DR:lle valitaan myös Backup Designated Router (BDR), joka ottaa DR:n tehtävät tämän vikaantumistilanteissa. [5, s. 94–95.]

2.3 Real-time Transport Protocol

RTP (lyhenne sanoista Real-time Transport Protocol) on tietoliikenneprotokolla tosiaikaisen datan, kuten äänen ja kuvansiirtoon pakettiverkoissa. RTP-protokollaa käytetään kolmannen sukupolven matkapuhelinverkkojen IP-pohjaisissa palveluissa, muun muassa puheluissa ja multimedian suoratoistossa. [6.]

RTP on erittäin yksinkertainen protokolla. Se tarjoaa sovellukselle tiedon sanoman sisältämästä tietotyypistä, sanoman ajastuksesta, sanoman häviämisestä ja sanoman sisältämän datan lähteistä. [6.]

RTP:n suunnitteluperiaatteina on ollut sovellustason kehystys ALF (Application Layer Framing, ALF), jossa sovellus jakaa itse datan verkon kannalta sopivanmittaisiin kehyksiin ja huolehtii uudelleenlähetyksistä tai toipuu kehysten häviämisestä muilla tavoin. RTP on ajateltu toteutettavaksi niin, että eri protokollakerroksiin kuuluva paketin käsittely yhdistetään yhteen tai kahteen silmukkaan eli käytetään yhdistettyä protokollakerrosten käsittelyä ILP (Integrated Layer Processing, ILP). RTP ei muodosta omaa protokollakerrostaan, vaan se tarjoaa sovellukselle puitteet reaaliaikaisen tiedon siirtoon. [6.]

Nimensä mukaisesti RTP pyrkii tarjoamaan siirtoyhteyden tosiaikaisuutta tarvitseville sovelluksille, kuten ääni ja video. RTP:tä voidaan käyttää sekä ryhmälähetys- että yleislähetystyyppisissä ympäristöissä. RTP:tä käytetään yleensä yhdessä UDP:n (User Datagram Protocol, UDP) kanssa. UDP on yhteydetön eikä tarjoa siten luotettavaa, sekventiaalista pakettien lähetystä. Täten RTP-protokolla itsessään ei myöskään takaa reaaliaikaisuutta itse median siirtopalvelussa. [5, s.158–159.]

2.4 Session Description Protocol

SDP (Session Description Protocol) on protokolla, jolla voidaan kuvata Internetin multimediaesityksiä tai -istuntoja, kuten internet-puheluja, elokuvien suoratoistoa tai puhelinneuvotteluja. SDP suunniteltiin alun perin MBONE:ssa (Ryhmälähetys Backbone, MBONE) välitettävien reaaliaikaisten multimediaesitysten kuvaamiseen. SDP-kuvauksessa luetellaan esityksen ajankohta, esitykseen kuuluvat mediat (ääni, video, grafiikkasovellus) ja niiden tarvitsemat parametrit (koodekit, siirtoprotokollat, porttinumerot). [7.]

2.5 Session Announcement Protocol

Session lähettäjä levittää tunnettuun lähetysryhmään säännöllisesti mainostuksia SAP-protokollan avulla ryhmälähetysistunnoista. SAP-mainostuksissa mukana kulkee kuvaus SDP lähetettävästä ohjelmasta. SDP-kuvauksessa esitetään esityksen ajankohta, käytettävät mediat ja parametrit, porttinumerot, siirtoprotokollat sekä IP-osoitteet. [8.]

Linux- ja Mac OS X -käyttöjärjestelmiin on saatavilla VideoLAN-kehittäjiltä Mini-SAP-palvelin. VLC-mediasoitin osaa vastaanottaa näitä SAP-mainostuksia ja tehdä niiden avulla listan mahdollisista lähetyksistä. Listasta käyttäjä voi valita haluamansa ohjelman nimen perusteella.

2.6 Hypertext Transfer Protocol

HTTP (lyhenne sanoista Hypertext Transfer Protocol eli hypertekstin siirtoprotokolla) on protokolla, jota selaimet ja WWW-palvelimet (World Wide Web) käyttävät tiedonsiirtoon. Protokolla perustuu siihen, että asiakasohjelma (selain, hakurobotti tms.) avaa TCP-yhteyden (Transmission Control Protocol, TCP) palvelimelle ja lähettää pyynnön. Palvelin vastaa lähettämällä sopivan vastauksen, tavallisimmin HTML-sivun (Hypertext Markup Language, HTML) tai binääridataa, kuten kuvia, ohjelmia tai ääntä. [9.]

3 Verkkotekniikat

3.1 Virtual Local Area Network

Virtuaalilähiverkko eli VLAN (Virtual Local Area Network) on tekniikka, jolla fyysinen Ethernet-verkko voidaan jakaa loogisiin osiin. Käytännössä tämä tarkoittaa sitä, että yrityksessä voidaan jakaa esimerkiksi eri osastot omiin verkkoihin riippumatta siitä, miten käyttäjät on jaoteltu rakennukseen. Virtuaalilähiverkkojen käyttöönotto vaatii tuen kytkimiltä ja reitittimiltä. [10.]

Virtuaalilähiverkkoja tukevat laitteet liittävät lähettämiinsä Ethernet-kehyksiin tunnuksia, joiden avulla vastaanottava laite tietää, mihin verkkoon vastaanotettu paketti kuuluu. Kun paketti lähetetään eteenpäin laitteelle, joka ei tue virtuaalilähiverkkoja, poistetaan siitä tunnus. [10.]

Laitteiden porttien määrityksissä käytetään termejä merkitty ja ei-merkitty riippuen siitä tukeeko vastaanottava laite virtuaalilähiverkkoja vai ei. Merkittyyn porttiin lähetettävään pakettiin liitetään virtuaalilähiverkkotunnus ja ei-merkittyyn porttiin lähetettävästä paketista poistetaan mahdolliset tunnukset. Laitteen portti voi olla vain yhden virtuaalilähiverkon ei-merkitty jäsen, mutta useamman virtuaalilähiverkon merkitty-jäsen. [10.]

3.2 Virtual Routing and Forwarding

Virtual Routing and Forwarding (VRF) on tekniikka, jonka sallii useita instasseja reititystaulukossa, joka toimii rinnakkain olemassa olevan saman reitittimen reititystaulun kanssa samaan aikaan. Koska reititysinstanssit ovat riippumattomia, samaa tai päällekkäisiä IP-osoitteita voidaan käyttää ilman, että osoitteet ovat ristiriidassa keskenään. [11.]

VRF-reititystaulut sijaitsevat ainoastaan PE-reitittimissä (Provider Edge, PE). Erillisiä VRF-tauluja voi PE-reitittimissä olla useampia kuin yksi. Yksinkertaisimmillään reititys sisältää yhden VRF-taulun jokaisessa PE-reitittimessä, mutta samaan reititykseen voi kuulua useampiakin VRF-tauluja. VRF-taulu sisältää omat reitit, jotka ovat käytössä tietylle ryhmälle verkkoja ja asemia. Käytännössä VRF-taulu sisältää tietyt reitit muihin saman reitityksen sisällä oleviin verkkoalueisiin. VRF-taulu asetetaan PE-reitittimen asiakkaan sisääntulo- tai aliliitynnälle, jolloin kyseisestä liitynnästä tulevat paketit reititetään VRF-taulun mukaan. Samalla kyseinen liityntä ja sen takana sijaitsevat asiakkaan verkot eivät enää esiinny reitittimen normaalissa IP-reititystaulussa vaan ainoastaan kyseisessä VRF-taulussa. Sitten, kun liitännästä tullut paketti on havaittu kuuluvaksi VRF:ään, se reititetään PE-reitittimeltä runkoverkon läpi toiselle PE-reitittimelle ja sieltä CE-laitteelle (Customer Edge, CE) ja edelleen kohdeosoitteeseen. [11.] Multicast VRF on samankaltainen kuin Unicast VRF. Ero vain on, että Multicast VRF on toteutettu käyttämään ryhmälähetysreititystä tavallisen täsmälähetysreitityksen sijaan.

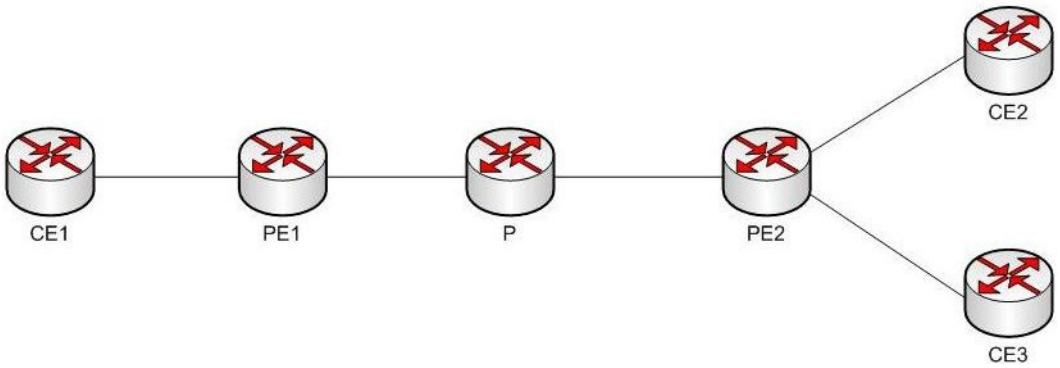
Palvelun tarjoajan runko- (P) ja reunalaitteet (PE)

Palveluntarjoajan reunalaitteita kutsutaan PE-reitittimiksi. Runkoverkon muita reitittimiä kutsutaan P-reitittimiksi (Provider, P), joihin luetaan runkoverkonydin-reitittimet (Core) sekä muut kuin PE- reitittimet. Käytännössä reititin luokitellaan P-reitittimeksi, jos reititin ei ylläpidä yhtään VRF-taulua. PE-reitittimet ovat yhteydessä asiakkaan CE-laitteeseen ja ylläpitävät VRF-tauluja. [11.]

Asiakkaan reunalaitteet (CE)

Asiakkaan reunalaitteita, jotka yhdistyvät suoraan palveluntarjoajan reunalaitteisiin kutsutaan CE-laitteiksi. CE-laitteisiin ei välttämättä tarvitse tehdä mitään muutoksia VRF:ä muodostettaessa vaan kaikki muutokset tapahtuvat PE-reitittimissä. CE-laitteiden tehtäväksi jää reitittää palvelun tarjoajan verkosta tulleet paketit kohdeosoitteisiin. PE-reitittimet huolehtivat siitä, että CE-laitteille ei pääse paketteja,

jotka eivät kuulu määriteltyyn VRF:ään. [11.] Kuvassa 2 esitetään PE-, P- ja CE-laitteet yhtenäisenä esimerkkitopologiana.



Kuva 2. VRF:n mukainen topologia [12.]

Route Distinguisher

RD (Route Distinguisher) määritellään VRF-taulujen tavoin PE-reitittimelle CE-laitteen sisääntuloliitynnälle. RD laajentaa CE-laitteelta opittujen reittien osoitteet VPNv4-osoitteiksi. Yksinkertaisimmillaan yksi VPN-yhteys (Virtual Private Network, VPN) käyttää yhtä RD:tä, jolloin kaikki sen IPv4-osoitteet laajennetaan samalla tunnuksella. Eri RD:n käyttö reiteille on pakollista siinä tapauksessa, että asiakkaiden verkot käyttävät samoja IPv4-osoitteita. Hyvä tapa on käyttää RD:nä asiakkaan tai VRF:n tunnusta, jolloin VPNv4-osoite on myös globaalisesti yksilöllinen osoite (olettaen että AS numero on yksilöllinen). [11.]

Route Target

Route Targetit määräävät, kenelle omia reittejä mainostetaan ja mitkä reitit tuodaan omaan VRF-tauluun. Jokaiselle VRF-taululle voidaan erikseen määritellä, mitkä reitit tauluun tuodaan (import) ja mitkä reitit viedään (export) muihin VRF-tauluihin. [11.]

OSPF-reitit

OSPF-protokollan tapauksessa asiakkaiden alueet kannattaa kukin määritellä omaksi OSPF-alueeksi (OSPF area), jolloin CE- ja PE-reitittimet ovat molemmat alueiden rajareitittimiä. Käytännössä palvelun tarjoajan verkko on oma OSPF-alueensa ja asiakkaan CE-laitteesta lähtien omansa. PE-reitittimen liityntä CE-reitittimelle määritellään kuuluvaksi asiakkaan OSPF-alueeseen. Tämän lisäksi PE-reitittimen VRF-tauluihin täytyy vielä tuoda tieto OSPF-reititystiedoista. [13.]

4 Virtualisointi

Virtuaalisointi tarkoittaa tietojenkäsittelyssä tekniikkaa, jolla jonkin fyysisen resurssin tekniset piirteet piilotetaan muilta järjestelmiltä, sovelluksilta ja loppukäyttäjiltä, jotka käyttävät näitä resursseja. Täten yksi fyysinen resurssi (kuten palvelin, käyttö-järjestelmä, sovellus tai tallennusväline) voi toimia monena loogisena resurssina, tai useat fyysiset resurssit (kuten tallennuslaitteet tai palvelimet) näkyvät yhtenä loogisena resurssina. Tätä uutta virtuaalista näkymää taustalla oleviin resursseihin ei rajoita niiden toteutus, maantieteellisen sijainti tai fyysinen määrittely. Useimmin virtuaalisoituja resursseja ovat laskenta- ja tallennuskapasiteetti. [14.]

Työasema- ja palvelinvirtualisointi

Virtuaalikone on ympäristö, joka näkyy toiselle käyttöjärjestelmälle erillisenä laitteena, mutta tätä laitetta itse asiassa simuloi isäntäjärjestelmässä toimiva ohjelmisto. Simuloinnin on oltava riittävän vahvaa siten, että toisen järjestelmän laiteajurit toimivat. Virtuaalikoneen muodostamiseen ja hallintaan viitataan usein termillä virtuaalipalvelin. [14.]

Virtuaalisovellus käsittää työpöytä- tai palvelinohjelmiston suorittamista paikallisesti ja paikallisia resursseja käyttäen ilman asentamista paikalliseen laitteeseen. Virtuaalisovellusta ajetaan omassa ympäristössään, joka sisältää sovelluksen

suoritukseen tarvittavat rekisteriasetukset, tiedostot ja muut komponentit. Tämä virtuaaliympäristö toimii välittäjäkerroksena sovellusohjelman ja käyttöjärjestelmän välissä. [14]

Laiteresurssien virtualisointi

Yhdistelemällä laiteresursseja suuremmiksi kokonaisuuksiksi voidaan muodostaa laajempia resursseja tai resurssivarantoja. Esimerkiksi RAID-levyjärjestelmät (Redundant Array of Inexpensive Disks, RAID) ja loogisten taltioiden hallintajärjestelmät yhdistelevät useita levyjärjestelmiä yhdeksi suureksi loogiseksi levytilaksi. Verkkolaitteet voivat käyttää useita rinnakkaisia kanavia ja antaa vaikutelman yhdestä laajempikaistaisesta yhteydestä. Pisimmälle vietynä tietokoneryppäät eli klusterit toteuttavat kaiken tämän. [14.]

Verkkolaitteiden virtualisointi

Verkkovirtuaalisointi on prosessi, joka yhdistää laitteiston ja ohjelmiston verkkoresurssit ja verkon toiminnot yhdeksi ohjelmistoon perustuvaan hallinnolliseen yksikköön. Verkkovirtuaalisointi liittyy yhteen alustan virtuaalisoinnin kanssa, usein yhdistettynä resurssien virtuaalisointiin. [15.]

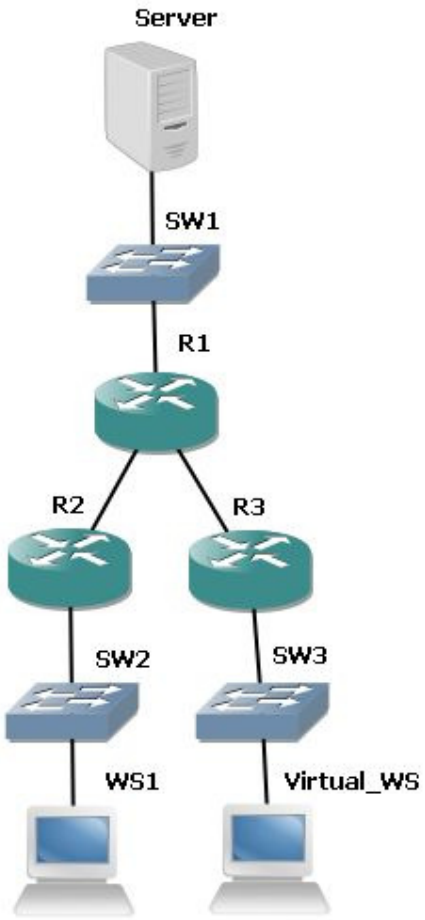
Verkkovirtuaalisointi on luokiteltu joko ulkoiseksi tai sisäiseksi. Ulkoisessa ratkaisussa yhdistyvät monet verkostot tai osia verkkojen osaksi olevaa virtuaalista yksikköä. Sisäinen ratkaisu tarjoaa verkkosuoritinohjelmiston klusteriin yhtenäisenä järjestelmänä. Onko virtuaalisointi sisäisesti tai ulkoisesti toteuttavissa, riippuu toimittajista, jotka tukevat teknologiaa. [15.]

Erilaiset laite- ja ohjelmistotoimittajat tarjoavat verkon virtuaalisoinnin yhdistämällä joitakin seuraavista:

- verkkolaitteita, kuten kytkimiä ja verkkokortteja, jotka tunnetaan myös nimellä verkkosovittimet

- verkkojan, kuten virtuaalinen LAN (VLAN) ja virtuaalikoneet
- verkon tallennuslaitteita
- verkkomediaa, kuten Ethernet- ja valokaapeli.

Kuva 3 esittää, miten WS1:ssa oleva virtuaalinen verkkokortti (Virtual_WS) tietokoneessa voi luoda yhteyksiä ilman, että oikeita tietokoneita otetaan käyttöön toisessa verkkosegmentissä.



Kuva 3. Virtuaalisen laiteresurssin hyödyntäminen verkossa

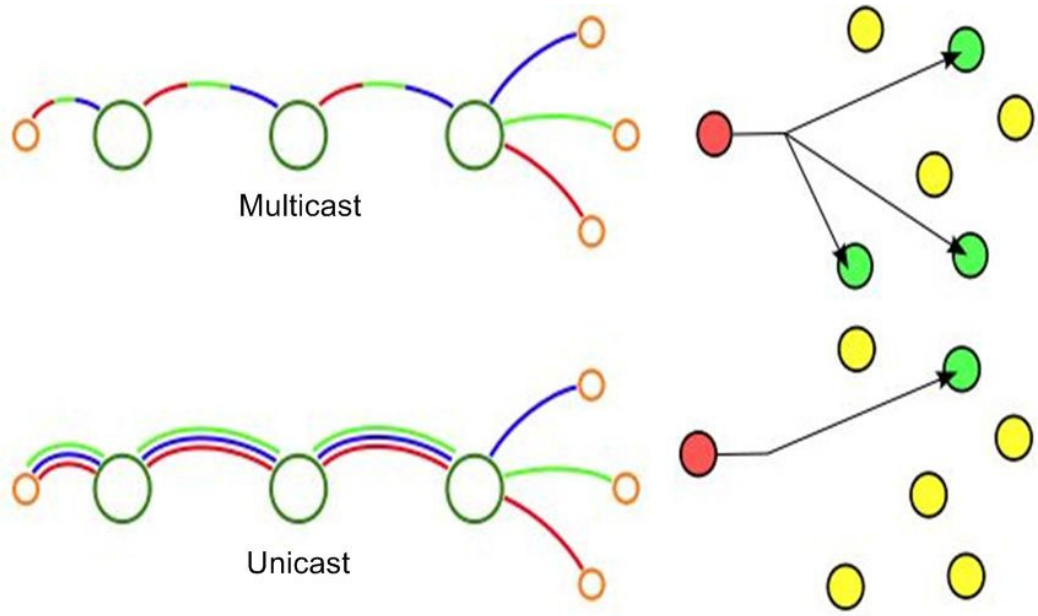
5 Ryhmälähetystekniikka

5.1 Ryhmälähetyksen perusteet

Ideana on, että ryhmälähetyspaketit lähetetään yhdeltä monelle. Kohde voi olla yksittäinen vastaanottaja tai tietty erikseen määritelty ryhmä. Halutessaan vastaanottaa ryhmälähetys-kehyksiä vastaanottaja tulee liittyä kyseiseen ryhmään. Ryhmälähetys-kehyksien lähettäminen on tehokkaampaa kuin täsmälähetyksessä, jossa on vain tietty lähettäjä ja vastaanottaja. [16.]

5.2 Ryhmälähetyksen edut

Ryhmälähetys vähentää verkon kuormitusta, koska jokaista datapakettia ei tarvitse lähettää erikseen kaikille vastaanottajille. Ryhmälähetyksen käyttö on perusteltua, kun lähetetään samaa dataa usealle vastaanottajalle, halutaan säästää tiedonsiirtokaistaa, vähentää verkon laitteiden kuormitusta tai ei tunneta vastaanottajien osoitteita. Ryhmälähetysverkkojen lisääntyminen ja kehittyminen tulevat auttamaan sovelluksia, joiden tarkoituksena on saada sama informaatio usealle vastaanottajalle. Kuva 4 esittää saman tiedon jakamista usealle vastaanottajalle perinteisen täsmälähetystekniikan avulla ja sen ohella saman tiedon jakelun toteutettuna ryhmälähetystekniikan avulla. Punainen ympyrä tarkoittaa lähettävää laitetta. Keltaiset ovat mahdollisia vastaanottajia, kun taas vihreät ympyrät kuvaavat lähettäjän vastaanottamia yhteyksiä. Viivalla kuvataan yhden lähetyksen luomista.



Kuva 4. Täsmälähetys- ja ryhmälähetyspohjaisen liikenteen ero [17.]

Ryhmälähetystekniikalla käytettävissä olevaa kaistanleveyttä hyödynnetään tehokkaammin, koska moninkertaiset saman datan lähetykset korvataan yhdellä lähetyksellä, joka monistetaan matkalla tarpeen vaatiessa.

5.3 Ryhmälähetyksen haitat

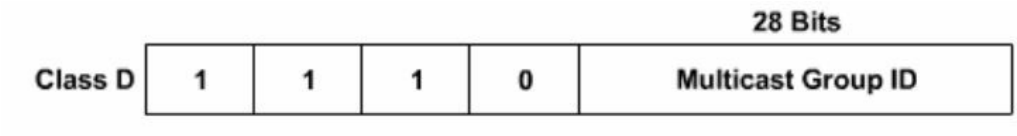
IP- multicast-tiedonsiirto on UDP-pohjaista. Yksi syy on UDP:n yleisrasite, joka on pienempi kuin TCP:n. UDP:ssä ei suoriteta alkukättelyä, pakettien kuittailua eikä kolmivaiheista yhteyden lopettamista. Satunnaista pakettien pois putoamista on odotettavissa, kun käytetään ”best-effort” -tyyppistä palvelua. Ryhmälähetystä ei tulisi käyttää, jos halutaan mahdollisimman luotettavaa tiedonsiirtoa. Pois pudonnutta pakettia ei ole mahdollista pyytää lähetettäväksi uudelleen, ja täten suuri pakettien pois jääminen reaaliaikaisissa sovelluksissa sotkee vastaanottajan saamaa informaatiota. Äänen siirrossa pudonneet paketit aiheuttavat äänen nykimisen vastaanottajalla, ja videokuvan siirrossa suuri pakettien pudonneisuus aiheuttaa kuvaan mosaiikkikuviota. Liikkuvan kuvan siirto sietää kuitenkin enemmän virheitä kuin äänen, ennen kuin vastaanotettavan informaation ymmärrettävyys heikkenee merkittävästi. Myös

käytettävän pakkausalgoritmin virheistä toipumiseen kuluva aika määrittelee, kuinka nopeasti informaatio menee epäselväksi vastaanottajan kannalta. [18.]

Pakettien ylimääräistä satunnaista monistumista saattaa ilmentyä, kun verkon topologia muuttuu. Ruuhkanhallintamahdollisuuden puuttuminen, toisin kuin TCP-liikenteessä, jossa on ikkunointi- ja ”slow-start”-ominaisuudet, voi aiheuttaa omalta osaltaan verkon tukkeutumisen, kun UDP-pohjaisen ryhmälähetys-liikenteen määrä kasvaa. [19.] Pakettien järjestys saattaa muuttua, koska käytössä ei ole sekvenssi-numerointia. Vastaanottoon käytettävän ohjelman tulisi huolehtia pakettien kaksoiskappaleiden, pakettien ruuhkaantumisen ja pakettien järjestyksen käsittelystä. Pakettien suodatuksessa ja turvallisuudessa voi tulla vaikeuksia. Ciscon mukaan luotettavan ryhmälähetystoteutuksen saralla on vielä paljon tutkittavaa, mutta kehitystä on odotettavissa. [20.]

5.4 Ryhmälähetysosoitteet

Ryhmälähetysosoitteille on varattu IP-osoiteavaruudesta luokka D, eli IP-osoitteet välillä 224.0.0.0–239.255.255.255. Verkon aktiivilaitteet tunnistavat ryhmälähetys-osoitteen katsomalla neljää merkitsevintä bittiä, jotka ovat 1110. Seuraavat 28 bittiä on varattu ryhmäosoitteille. Kuva 5 esittää osoitteen rakenteen.



Kuva 5. Ryhmälähetysosoitteen merkitsevimmät bitit ja group ID.

Verkkotunnusten ylin vastuu kuuluu IANA:lle (Internet Assigned Numbers Authority), joka on taas jakanut vastuun päätason tunnuksista eri tahoille. Esimerkiksi verkkotunnuksesta .fi ja sen IP-osoitteista vastaa Suomessa viestintävirasto. [21.] Ryhmälähetysosoiteavaruutta kuitenkin hallitsee suoraan IANA. Ryhmälähetys-

osoiteavaruus on jaettu kolmeen osoiteryhmään: paikallisiin, globaalisiin ja hallinnollisesti rajatuihin osoitteisiin. [22.]

Lista varatuista ryhmälähetysosoitteista löytyy IANA:n sivuilta: http://www.iana.org/assignments/ryhmälähetys-addresses.

Paikalliset osoitteet

IANA on varannut osoitteet 224.0.0.0–224.0.0.255 verkkoprotokollien käytettäväksi. Reitittimien ei pitäisi ohjata näistä osoitteista tulleita paketteja pois paikallisesta verkosta. Taulukossa 1 on listattu muutamia verkkoprotokollien käyttöön varattuja osoitteita. [23.]

Taulukko 1. Eräitä IANA:n varaamia ryhmälähetysosoitteita.

Osoite	Käyttö
224.0.0.1	All multicast systems on this subnet
224.0.0.2	All routers in this subnet
224.0.0.5	OSPF routers
224.0.0.6	OSPF designated routers

Globaalit osoitteet

Osoitteet 224.0.1.0–238.255.255.255 ovat tarkoitettu käytettäväksi organisaatioiden väliseen ja Internetissä tapahtuvaan ryhmälähetysliikenteeseen. Globaalien osoitteiden alueelta on IANA myös varannut muutamia osoitteita. Globaalien osoitteiden alue 224.2.X.X on varattu ryhmälähetysten runkoverkon (maailmanlaajuinen runkoverkko ryhmälähetyksille) käyttöön. [24.]

Hallinnollisesti rajatut osoitteet

Hallinnollisesti rajatut osoitteet on varattu organisaatioiden sisäiseen käyttöön. Näitä voidaan verrata A-. B- ja C-luokan osoiteavaruuksista löytyviin yksityisiin IP-osoitteisiin. RFC 2365 määrittelee osoitteet pidettäväksi organisaation sisällä.

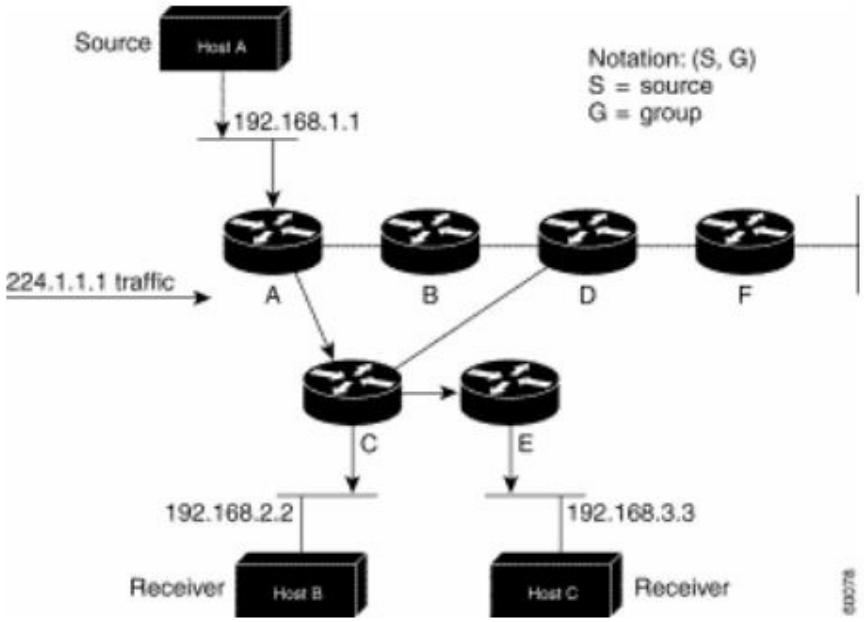
Hallinnollisesti rajattujen osoitteiden alue on 239.0.0.0–239.255.255.255. Reitittimien tulisi olla määritelty estämään liikenteen leviäminen tältä osoitealueelta toimialueen tai autonomisen järjestelmän ulkopuolelle. [24.]

5.5 Ryhmälähetysjakelupuut

Ryhmälähetysjakelupuiden avulla määritellään reitti lähteestä vastaanottajille. PIM-käytössä on kahta erilaista jakelupuumallia, Shortest Path Tree ja Shared Tree. Jakelupuiden tunnistaminen tapahtuu merkinnöistä (S,G) tai (*,G). Merkintä (S,G) ilmoittaa käytössä olevan SPT-mallisen puun (Shortest Path Tree, SPT) , jolloin polku on lyhin mahdollinen lähteestä vastaanottajalle. Merkintä (*,G) kertoo liikenteen tulevan kohtauspaikan (Rendezvous Point, RP) kautta, jolloin puu on Shared Tree -mallin mukainen.

Shortest Path Tree

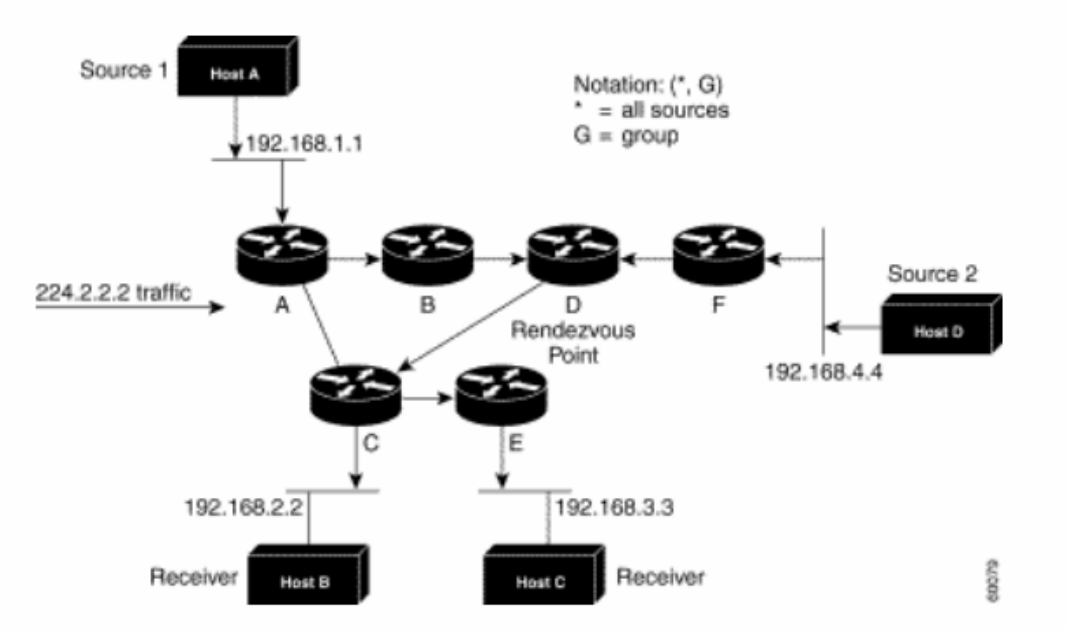
Shortest Path Tree (SPT) on yksinkertaisin ryhmälähetysten jakelupuumalli. SPT rakentaa jokaiselle lähteelle oman polun kohteeseen käyttäen lyhintä polkua (Shortest Path). Kuva 6 esittää SPT-mallista puuta. Ryhmät, joilla on vastaanottajia useassa verkon haarassa, tai verkot, joissa on monia ryhmiä, kuluttavat paljon verkon kapasiteettia käyttäessään Shortest Path -mallista puuta. Koska ryhmälähetyspakettien jakelu tapahtuu lyhintä mahdollista polkua pitkin vastaanottajille, viive on mahdollisimman vähäinen. Puun tunnistus tapahtuu merkinnästä (S,G): merkitty S (source) lähettää tiettyyn ryhmään G. [25.]



Kuva 6. SPT -puu (S,G), lyhin mahdollinen polku lähteestä vastaanottajalle. [24.]

Shared Tree

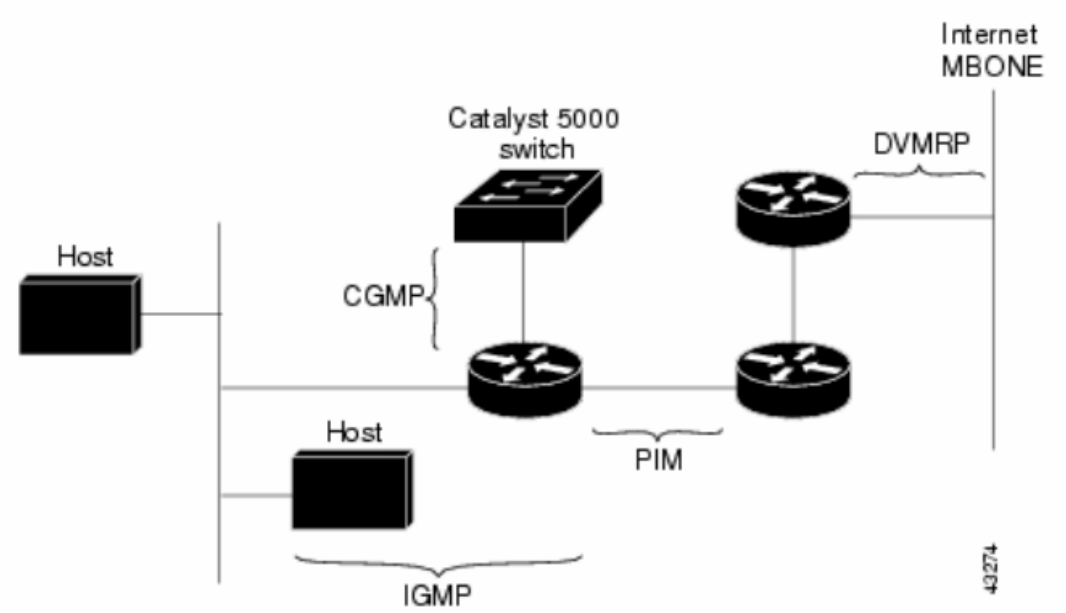
Shared Tree -mallisessa jakelupuussa käytetään liikenteelle kohtauspaikkaa (RP), joka toimii puun juurena. Kuva 7 esittää Shared Tree -muotoon rakentunutta jakelupuuta. Kaikki lähteet lähettävät ryhmälähetys-paketit kohtauspaikkaan, josta liikenne ohjataan puuta alaspäin kohden vastaanottajia. Puun tunnistus tapahtuu merkinnästä (*,G): mikä tahansa S (source) lähettää tiettyyn ryhmään G. Shared Tree -mallin etuna on sen kuluttama vähäinen muistintarve reitittimissä. Liikenne ei kuitenkaan kulje aina lyhintä reittiä kohteeseen, minkä vuoksi saattaa esiintyä häiritsevääkin viivettä. Kohtauspaikan valitseminen on tärkeässä roolissa suunniteltaessa Shared Tree -mallisen jakelupuun käyttöä. [25.]



Kuva 7. Shared Tree (,G), liikenne kulkee kohtauspaikan kautta.[25.]*

5.6 Ryhmälähetyksen reititys

Toimiva ryhmälähetysverkko tarvitsee muutamia protokollia ja prosesseja ennen kuin ryhmälähetykset ovat mahdollisia lähetettäväksi ja vastaanotettavaksi. Kuva 8 esittää IPv4:ssä käytettäviä ryhmälähetysreititysprotokollia. ASM-tyyppistä (Any Source Multicast) ryhmälähetys-jakelua käytettäessä reitittimien tulee tietää kohtauspaikan osoite. IPv4-käytössä kohtauspaikkojen reitittimien pitää pystyä keskustelemaan toisessa toimialueessa olevan kohtauspaikan kanssa, ja tämä onnistuu MSDP:n avulla (Multicast Source Discovery Protocol). PIM- (Protocol Independent Multicast) ja DVMRP-protokollien (Distance Vector Multicast Routing Protocol) avulla reitittimet keskustelevat toistensa kanssa; näistä kahdesta kuitenkin DVRMP alkaa olla korvattu tehokkaammalla PIM-SM-tekniikalla (Protocol Independent Multicast – Sparce Mode). Ilman IGMP:n apua kytkimet käsittelisivät ryhmälähetyssanomia kuin yleissanomina.



Kuva 8. Ryhmälähetysreititysprotokollia. [25.]

Ryhmälähetysreititys toimii täysin vastakkaisella periaatteella kuin täsmälähetys-reititys. Ryhmälähetyksessä tulee tietää, mistä paketti on tulossa, jonka jälkeen tehdään päätös, minne paketti ohjataan.

Protocol Independent Multicast

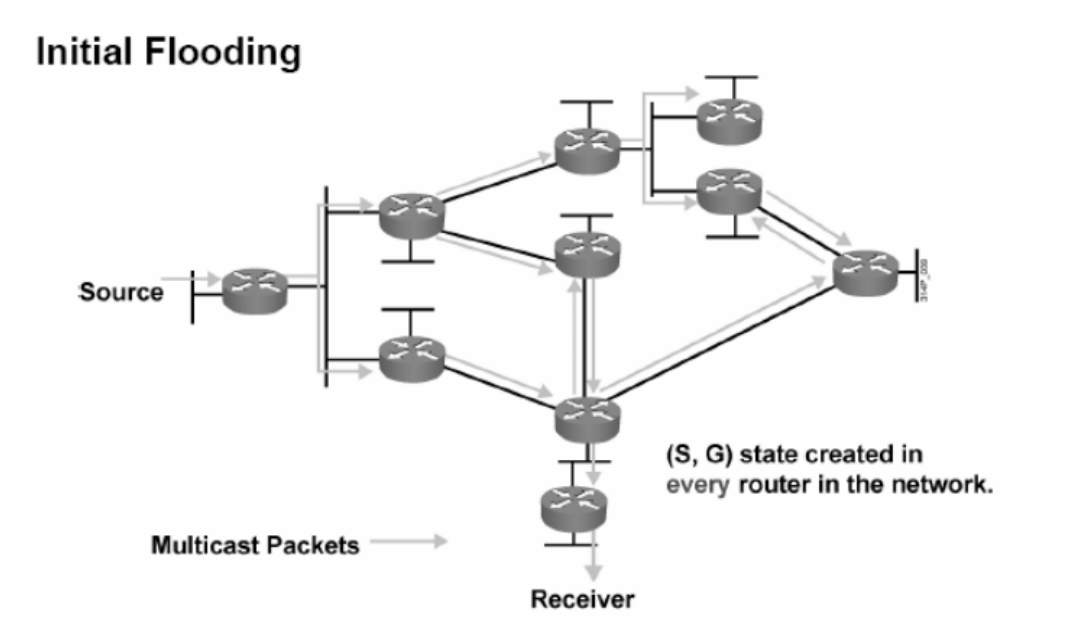
Protocol Independent Multicast (PIM) on ryhmälähetysreititystekniikka, jota joskus hieman väärin kutsutaan reititysprotokollaksi. PIM on protokollariippumaton tekniikka, joka hyödyntää käytössä olevaa täsmälähetysreititysprotokollaa ryhmälähetysliikenteen reititykseen. PIM käyttää RPF-tarkastusta (Reverse Path Forwarding) varmistamaan, että paketit saapuvat liitäntään, josta muodostuu lyhin matka lähteelle. RPF-testi tehdään olemassa olevaa täsmälähetysreititystaulua vasten. PIM ei lähetä eikä vastaanota reitityspäivityksiä kuten muun muasssa MOSPF (Multicast Open Shortest Path First). PIM voi toimia sparse- tai dense-muodossa. Dense-muodon käyttö on järkevää, kun vastaanottajia on paljon verkossa. Sparse-muodon käyttö toimii Dense-muotoa paremmin, kun vastaanottajia on harvakseltaan useassa osassa verkkoa kuten

Internetissä. Sparse-muodossa toimiessaan PIM tarvitsee kohtauspaikkoja, joiden kautta jakelupuu lähteen ja kohteen välille muodostetaan. [25.]

PIM dense -muoto

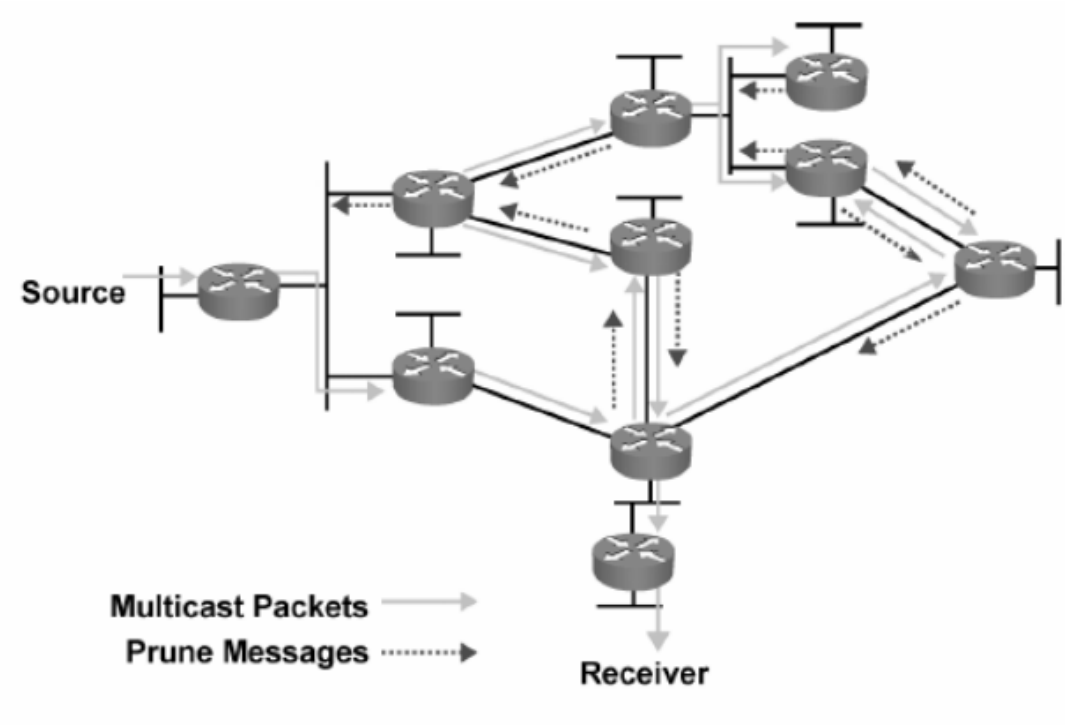
PIM dense -muoto toimii parhaiten, kun suurimmassa osassa verkon haaroja sijaitsee vastaanottajia ja tiedonsiirtokaistalla riittää tilaa. Dense- (suom. tiheä) tilan käyttöä suositellaankin ryhmälähetys-liikenteen levittämiseksi vain LAN-ympäristöissä (Local Area Network), sen käyttämän push-mallin vuoksi. Suurissa verkoissa, joissa vastaanottajia on vain vähän, dense-muodon käyttöä tulisi välttää, koska tiedonsiirtokapasiteettia tuhlautuu ryhmälähetyspakettien säännöllisen levityksen vuoksi. Kuva 9 esittää pakettien levitystä dense-tilassa. PIM-DM (Protocol Independent Multicast – Dense Mode) käyttää ainoastaan SPT-mallista menetelmää, joten se ei käytä kohtauspaikkaa kuten PIM-SM. Tämä tekee dense-muodosta helposti toteutettavan. PIM-DM on erittäin tehokas protokolla, kun suurin osa verkon laitteista on kiinnostuneita ryhmälähetysten vastaanotosta. [25.]

Liikenteen saapuminen reitittimeen aktivoi ryhmälähetysliikenteen elelleenohjauksen. dense-muodossa toimiva reititin levittää saapuvan liikenteen säännöllisesti liitäntöihin, joissa sijaitsee PIM-DM naapuri, suoraan liittynyt jäsen tai liitäntä on käsinmääritelty ryhmän jäseneksi. [25.]



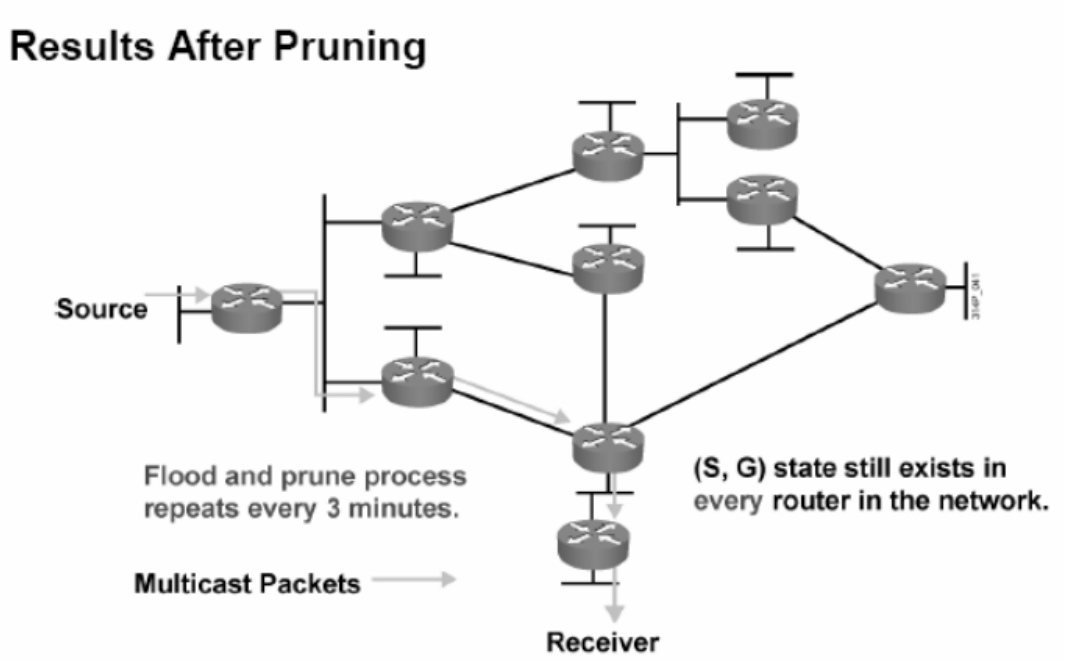
Kuva 9. Pakettien levitys dense-tilassa. [26.]

Jos paketti saapuu liitäntään, josta ei muodostu lyhintä reittiä lähteelle, niin se hylätään. Haarat, joissa ei sijaitse lähetyksen vastaanottajia lähettävät prune-viestin (karsinta) lähdettä kohden. Näin saadaan karsittua ei-toivottu liikenne. Kuva 10 esittää paketti-en levittämisen jälkeen tapahtuvaa karsintaa. Karsittu haara pysyy poissa reititystaulusta kolme minuuttia, jonka jälkeen tapahtuu uudelleen levitys ja mahdollinen karsinta, jos ei vastaanottajia vieläkään ole. Prune-viestejä lähetetään myös non-RPF-liitäntöihin, jotka eivät muodosta lyhintä polkua ryhmälähetyslähteelle. [25.]



Kuva 10. Levityksen jälkeinen karsinta ylimääräisistä reiteistä. [26.]

Prune-viestien jälkeen ryhmälähetyspaketit virtaavat vain vastaanottajalle, muut reitittimet säilyttävät (S,G) tilansa. Tila säilyy, kunnes lähde lopettaa lähetyksen tai lähteestä ei kuulla ennen tilan säilyttämiseksi käynnistetyn laskurin päättymistä. Kuva 11 esittää pakettien virtaa ylimääräisten reittien karsimisen jälkeen. [24.]



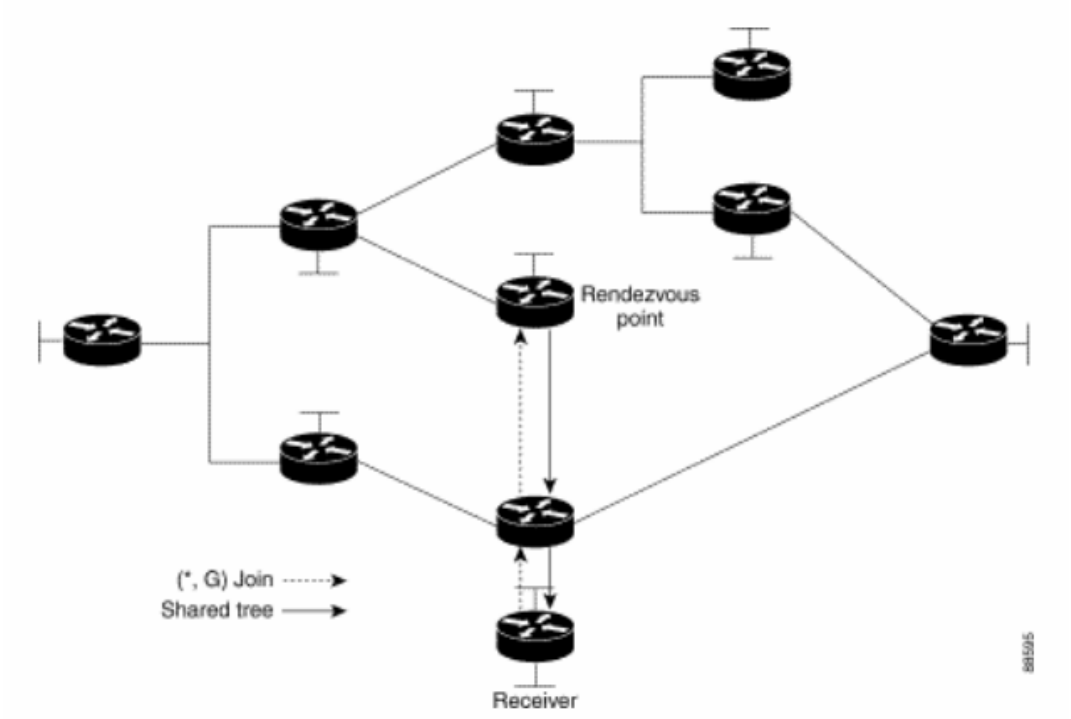
Kuva 11. Ryhmälähetys-pakettien virta karsimisen jälkeen. [26.]

PIM sparse -muoto

PIM sparse -muoto on Internetissä käytettävä ryhmälähetys-reitirysprotokolla. PIM-SM perustuu eksplisiittiseen pull-malliin, jolla tavalla liikenne ohjautuu oikeisiin verkon osiin. Se ei myöskään ole riippuvainen käytettävästä täsmälähetys-protokollasta. Shared Tree -jakelupuuta rakennettaessa käytetään kohtauspaikkaa (RP). PIM-SM osaa käyttää jakelupuina Shared Tree- ja Shortest Tree -mallia. [25.]

Kun vastaanottajia on eri puolilla verkkoa epätasaisesti, ryhmälähetyksen muodoksi suositellaan PIM-DM-muodon sijasta PIM-SM-muotoa. Dense-muoto levittää ryhmälähetyspaketit säännöllisesti, kun taas sparse-muodossa käytetään kohtauspaikkaa, jossa lähettäjä ja vastaanottaja tapaavat, eikä ylimääräistä pakettien tulvintaa tapahdu. PIM-SM-muoto skaalautuu hyvin verkkoon, jossa halutaan säästää tiedonsiirtokaistaa, koska paketit leviävät vain verkon osiin, joissa on halukkaita vastaanottajia. [25.]

Reitittimet liittyvät ryhmään lähettämällä kohtauspaikkaan IGMP join -viestin, jossa ilmoitetaan halusta liittyä tietyn ryhmän jäseneksi. Kun viesti saapuu kohtauspaikkaan, ohjataan ryhmälähetysliikenne porttiin, josta sanoma saapui. Liittymisviestit toimivat täsmälähetystekniikalla. Kohtauspaikan kautta muodostettu liikenne muodostuu aluksi Shared Tree -jakelupuumallin mukaisesti. Reitittimiin muodostuu tila (*,G) vain, kun ne ovat osana jakelupuuta. Kuva 12 esittää vastaanottajan lähettämää ilmoitusta halustaan liittyä ryhmään [24.].



Kuva 12. Vastaanottaja ilmoittaa IGMP join -viestillä halustaan liittyä ryhmään. [26.]

Kohtauspaikan on tiedettävä Join-viestissä ilmoitetun ryhmälähetysosoitteen lähteen sijainti. Kohtauspaikka saa tietoa ryhmälähetyslähteistä, kun se rekisteröityy lähettäjän verkon kohtauspaikan kanssa. Rekisteröityminen alkaa lähettäjän lähettäessä paketin ensimmäiselle reitittimelle, ja reitittimen tehtävänä on lähettää yksittäislähetyksellä rekisteröitymisviesti kohtauspaikan kanssa ja pyytää kohtauspaikkaa rakentamaan jakelupuu takaisin. Kohtauspaikan ja lähteen välille rakentuu SPT -mallinen jakelupuu. [24.]

Kohtauspaikan kautta muodostunut jakelupuu ei kuitenkaan ole välttämättä lyhin

reitti kohteen ja lähteen välillä, mikä saattaa aiheuttaa huonossa tapauksessa ylimääräistä viivettä lähetykseen. [24.]

PIM sparse-dense-muoto

Määrittelemällä reitittimen liitäntä sparse-dense-muotoon annetaan mahdollisuus yksittäisten ryhmien toimia joko sparse- tai dense-muodossa. Käytettävän muodon valinta riippuu saatavilla olevasta kohtauspaikkatiedosta kyseistä ryhmää varten. Jos reitittimellä on tietoa tiettyä ryhmää koskevasta kohtauspaikasta, käsitellään sitä Sparse-muodossa. Jos tietoa kohtauspaikasta ei ole, ryhmää käsitellään dense-muodossa. [25.]

MOSPF

Kun DVMRP on RIP-protokollan (Routing Information Protocol, RIP) varaan rakennettu ryhmälähetysprotokolla, MOSPF on OSPF-protokollaan perustuva protokolla. MOSPF-protokolla on siis yhteystilatietoihin perustuva ja sitä kautta monessa suhteessa parempi ryhmälähetysprotokolla kuin etäisyysvektoreihin perustuva DVMRP. [5, s. 144.]

5.7 Ryhmälähetyksen runkoverkko

Osa internetin reitittimistä ei tue vielä ryhmälähetysreititystä. MBONE muodostaa maailmanlaajuisen runkoverkon, joka yhdistää ryhmälähetys-lähetyksiin pystyvät verkot. Sana MBONE on alun perin tarkoittanut internetin ryhmälähetysverkkoa, joka toimii DVMRP-reitityksellä käyttäen tunnelointia, mutta se on jäänyt käyttöön, vaikka reititystekniikka on muuttunut. [27.]

Tällä hetkellä DVMRP ja PIM-DM ovat katoamassa ryhmälähetysrunkoverkon käytöstä ja korvaajaksi on noussut tehokas PIM-SM (protokollasta riippumaton ryhmälähetys-reititysprotokolla). [25.]

6 Ryhmälähetyssovelluksia

Web-kameran videon välitys

Web-kameran kautta voidaan tehdä erilaisia reaaliaikaesityksiä. ryhmälähetysliikenteen kannalta kameran ominaisuudet ja profilointi määrittelevät vaadittavat resurssit. Niin kuin aikaisemmin on mainittu, ryhmälähetys-liikenne ei vie täsmälähetys-verkko-liikenteestä kovin montaa prosenttia, vaikka olisi useitakin yhtäaikaisia suoratoisto-sessioita läpi verkon.

Ominaista kuitenkin web-kameroiden medialiikenteessä olisi, että laatu olisi hyvin siedettävä. Kun puhutaan reaaliaikasessiosta, lähettäjän kuvan ja äänen tulisi synkronoida. Tulisi myös huolehtia, etteivät kuva ja ääni siirtyisi eri vaiheessa tai altistuisi suuren kuormituksen ohella katselukelvottomaksi.

Asiaa voidaan tarkkailla muun muassa laskemalla mahdollinen kokonaisliikenne suurimmillaan. Kuitenkin tästä huolimatta lähiverkon tai suljetun Ethernet-pohjaisen verkon hallittavuus on hyvin helppoa. Ryhmälähetys liikenteeseen voidaan toteuttaa muun muassa pääsylistat, QoS (Quality of Service) ja siten voidaan varmistaa liikenteen saatavuus.

Itse sovelluksena tähän tarkoitukseen kouluympäristössä sopii muun muassa reaaliaikainen opetustunti tai vieläkin tehokkaampana ratkaisuna olisi valvontakamera-järjestelmä. Myös mainos- tai tiedotuskanavana käyttötarkoitus olisi erittäin kelvollinen.

Valmiin median välitys

Passiivinen media tarkoittaa jo olemassa olevaa mediatiedostoa. Tässäkin pätee samat säännöt kuin web-kameran kohdalla resurssien vaatimuksesta. Lähteenä käytetään joko videotiedostoa tai DVD-mediaa.

Resurssien puitteissakin passiivinen media poikkeaa luonnollisesti reaaliaikasessiosta siten, että käyttötarkoitus on hyvin erilainen. Passiivisella medialla voidaan luoda ns. jatkuva toisto, joka laitetaan pyörimään tietyssä ympäristössä. Vertailuesimerkkinä on PowerPoint-esitys, joka toimii koulun info-näyttönä. Ero kuitenkin on, että PowerPoint ei ole aina niin skaalautuva kuin erimuotoisten mediaformaattien yhdistelmä. Esimerkiksi DVD-media voidaan tehdä hyvin näyttäväksi, kun liikkuvan kuvan lisäksi saadaan tekstitystä ja ääntä yhtäaikaisesti.

IP-televisio

IPTV täytyy mainita erikseen, vaikka kyse on reaaliaikamuotoisesta sessiosta. Median lähetys tulee siitä huolimatta ulkoistettuna televisiojakeluverkon kautta.

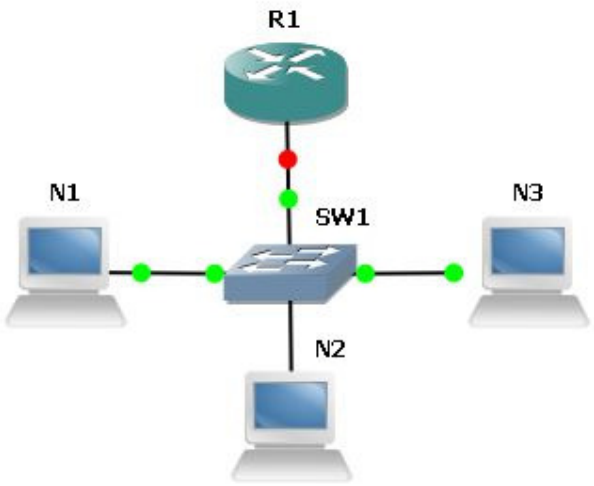
IPTV:tä ei varsinaisesti työssäni esiinny, mutta Bulevardin toimipisteessä on jo valmis järjestelmä siihen. Siten työhöni haluasin sisällyttää sen, miten kyseisen järjestelmän voisi tuoda Leppävaaran toimipisteeseen. Tähän palaan myöhemmin, kun puhutaan VLC-mediasoittimen sovelluksista.

7 Ryhmälähetyksen reititys ja runkoverkon toteutus

Ryhmälähetysrunkoverkon tavoitteena on nähdä, miten itse ryhmälähetysliikenne muodostuu eri OSI-tasojen (Open Systems Interconnection, OSI) mukaisesti. Verkkotopologioissa keskitytään siihen, miten testiympäristöjen avulla voidaan luoda tarvittava ryhmälähetystoiminta. Työssä käydään läpi olennaiset asiat, joita tarvitaan ryhmälähetysliikenteen luomiseen ja pohditaan niiden merkitystä. Myös VRF-teknikkaa sovelletaan ryhmälähetysliikenteeseen, jolloin voidaan luoda vikasietoisia verkkotopologioita. Työssäni käytetään Ciscon valmistamia laitteita.

7.1 OSI 2 -tason liikenteen ohjaus

Liikenteen ohjaus tapahtuu kytkintasolla IGMP-protokollan kautta ja VLANin määrittelyjen avulla. Ryhmälähetysliikenteen toiminta tällä tasolla on hyvin tärkeää. Aktiivisen liikenteen aikana voidaan tutkia IGMP:een sidettä porttien suhteen ja myös VLANin suhteen.



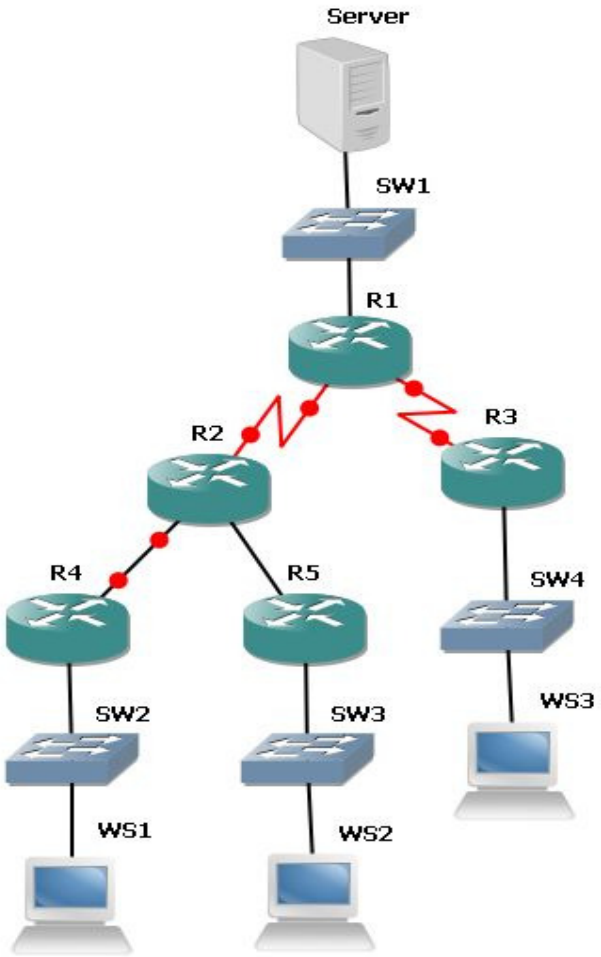
Kuva 13. IGMP:in toiminta

Kuvassa 13 olevat työasemat lähettävät pyynnön liittyä ryhmään ja siten kytkin käynnistää yhteyden, kun reititin reitittää pyynnön. Toisaalta, jos palvelin ja työasema olisivatkin samassa verkossa, niin silloin ryhmälähetysliikenne heijastuu suoraan työasemaan, joka pyytää lupaa liittyä ryhmään. Tällöin, jos ei VLAN:in määritelmiä ole tehty, varsinaista reititystä ei tapahdu. Reititin saa silti tiedon siitä, että kyseiseen ryhmään on liitytty.

VLANit hoitavat ryhmien jakamisen. Kuitenkaan VLANit eivät suoraan rajoita mitään ryhmälähetysliikenteen kannalta. Mutta jos OSI 3 -tason reititystä ei ole määritelty ryhmälähetysliikenne ei toimi VLANien välillä. VLANin etu on ryhmien hallinnoimisessa. Ryhmäosoitteita voidaan jo rajoittaa tälläkin tasolla, kuten pääsylistojen avulla.

7.2 OSI 3 -tason liikenteen ohjaus

Ryhmälähetyksen toiminnallisuuden kannalta reititys on äärimmäisen tärkeää lähiverkoissa. Lähtökohtana on kaksi mahdollisuutta, ja tässä yhteydessä painotetaan perusreititykstä. Perusreitityksen tavoitteena pitää olla se, että kunnollinen jakelupuurakenne on olemassa. Tällöin nähdään, miten ryhmälähetysreititys toimii ja miten ryhmälähetysliikenne muodostuu läpi verkon. Ryhmälähetysreitityksen toteutuksessa tarvitaan Ciscon omia laitekohtaisia määrittelyjä ennen kuin se alkaa toimia. Myös toinen erittäin tärkeä huomio on, ettei Ryhmälähetysreititys ole automaattisesti toimintatilassa. Ajatellaan, että meillä on kuvan 14 mukaisesti viiden reitittimen ja neljän kytkimen perusverkko, jossa on sekä sarja- ja Ethernet-liitäntöjä.



Kuva 14. Perusryhmälähetysreititetty verkkotopologia

Peruslaitemäärittelyjen kautta pitää ensimmäisenä asiana kaikissa reitittimissä aktivoida ryhmälähetys reititykseen kuuluva käsky globaalissa tilassa, jotta ryhmälähetys reititys aktivoituu: Tämä toisaalta ei vielä riitä siihen, että reititystä tapahtuu. Ryhmälähetys-liikenteeseen pitää sitoa PIM-protokolla haluttuun laitteen Ethernet- tai sarjaporttiin ja sitä kautta reitittyy ryhmälähetys. Kuten aikaisemmin kerrottiin, kyseisessä tilanteessa voidaan reitittimeen määritellä molemmat tavat hoitaa reititystä, jolloin ei myöskään tarvitse määritellä erikseen RP-pistettä.

Myös SAP-mainostuksia voidaan seurata laitepohjaisesti, jolloin sekin sidotaan tiettyyn laiteporttiin kuten itse ryhmälähetys liikenne. SAP antaa laitemäärittelyjä laittaessa sen edun, että SAP tutkii jo laitetasolla mitä SAP-mainoksia tulee tiettyihin porttien kautta. Kuvan 14 verkossa SAP-mainokset tulevat toimimaan läpi verkkotopologian. Etuna tässä on se, että jos halutaan tietää tarkalleen, mistä SAP-mainostus tulee, voidaan varmistua, että ryhmälähetysliikenne on toimintatilassa. Toisin sanoen SAP toimii tavallaan testaajana laitetasolla ja siitä SAP-mainostuksesta voidaan lukea kaikki olennainen sisältö. Ciscon reitittimet osaavat kuunnella SAP-sanomien sisältöä, mistä on esimerkki liitteessä 1.

Lopuksi on myös hyvä katsoa ja varmistaa, että kytkentä toimii. Toimivuutta voidaan todeta erilaisilla käskyillä. Toimivuuden kannalta tulee miettiä seuraavia tekijöitä:

- Tuleeko liittyneiden ryhmien tieto reitittimelle?
- Näkyykö voimassaoleva ryhmälähetysreititys läpi verkon?
- Menevätkö kaikki SAP-mainostukset perille saakka?
- Rakentuuko jakelupuurakenne aktiivisen ryhmälähetysliikenteestä oikean mallin mukaiseksi?

Tästä järjestelmästä on liitteessä 2 käskylistat, joilla kyseinen kytkentä saadaan aikaiseksi.

7.3 Liikenteen ohjaus multicast VRF -tekniikalla

Idea ja hyöty

Multicast VRF on oikeastaan yksi työn mielenkiintoisimpia teknisiä ratkaisuja. VRF:ään voidaan sitoa tarvittaessa vain osa verkkoyhteyksistä, joiden avulla tavallinen ryhmälähetysverkko on muodostettu. Ryhmälähetyksistä pystytään tekemään VRF:n avulla hyvin vikasietoinen. Toinen merkittävä asia on, että liikenne saa optimaalisen reitin.

VRF-alustukset

Ennen VRF käyttöönottoa pitää aktivoida Ciscon laitteessa CEF (Cisco Express Forwarding, CEF). Tämä aktivoi OSI 3 -tason kytkintekniikan, joka kiihdyttää pakettien käsittelyä. Itse VRF:n määrittely tapahtuu luomalla VRF tietyllä nimellä. Kerrotaan RD:lle, mihin VRF:ään osoite talletetaan pakettien kuljettamista varten. RD:een määrittelyyn on olemassa kolme keinoa:

- Järjestelmän AS-numero: asiakkaan VRF-tunnus, eli käytetään järjestelmän AS-numeroa, esimerkksi 64222 (yksityinen numero), ja sidotaan se asiakkaan tunnisteeseen, joka voi olla esimerkiksi 100.
- IP-osoite: asiakkaan VRF-tunnus, eli käytetään laiteen IP-osoitetta, esimerkiksi 172.16.1.0/30, ja sidotaan samalla tavalla asiakkaan tunnisteeseen kuin edellisessä tavassa.
- IP-osoiteasvaruus tai järjestelmän AS-numero: VRF-instanssi, eli käytetään järjestelmän AS-numeroa tai laitteen IP-osoitetta ja sidotaan se VRF-instansiin.

Ciscon reittimissä käytetään vain kahta ylintä tapaa VRF:iä määriteltäessä. [28.] Toisaalta tämä on ns. ohje, miten paketteja tulisi käsitellä, eikä se itsessään riitä ennen

kuin VRF toimii. Multicast VRF -reititykseen tarvitaan kuitenkin oma aktivointinsa, kuten tavallinenkin ryhmälähetysreititys, mutta siihen pitää lisätä luodun VRF:n nimi.

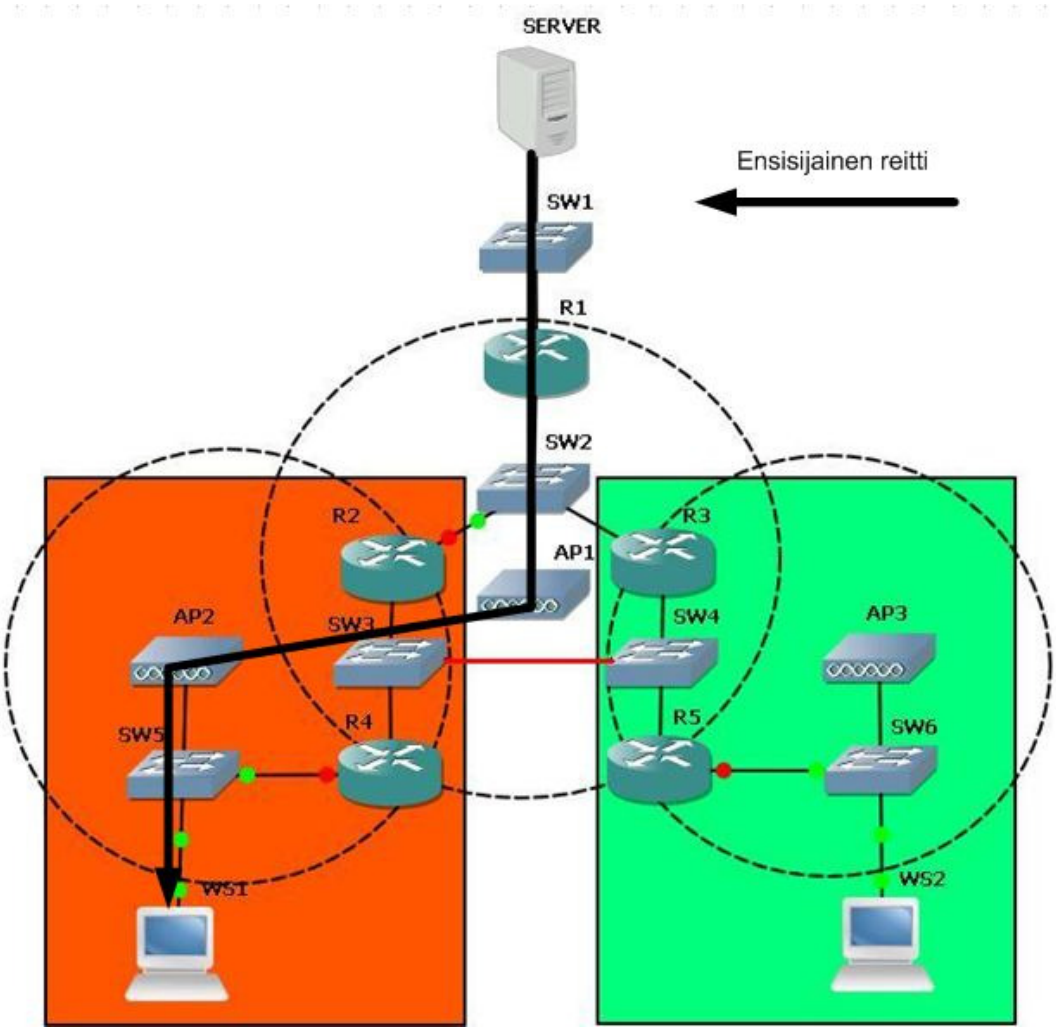
VRF:n määrittelyjen jälkeen luodaan virtuaaliportti (loopback), johon VRF-taulut otetaan käyttöön. Virtuaaliportti toimii reitittimen sisällä virtuaalisena rajapintana, ja se toimii myös ryhmälähetys VRF:in osoitetunnisteena. Virtuaaliportissa otetaan reitittimeen määritelty VRF-taulu, johon ryhmälähetys VRF-liikenne sidotaan. Tämän jälkeen siirrytään reitittimien portteihin, mutta loogisen portin sijasta käytetään aliliitäntäporttia, johon sidotaan olemassa oleva VRF-liikenne. Aliliitäntäportin merkitys on saada looginen portti pilkottua moneksi virtuaaliseksi portiksi, joihin voidaan luoda uusia reitityksen solmupisteitä ilman, että käytettäisiin reitittimessä uusi loogisia portteja. Ryhmälähetys VRF:ssä käytetään aliliitäntäportteja, jotka sidotaan tietyllä kapseloinnilla ja VLAN:lla. Aliliitäntäporttia työssäni käytetään siksi, että voidaan käyttää VLANin tuomia paketintunnisteita. Silloin kun VRF-tauluun kytketyt paketit saapuvat lähtevästä AS- tai IP-tunnisteesta, ne sitovat myös VLAN-tunnisteen ja reitittyvät eteenpäin toiseen aliliitäntäporttiin.

Lopuksi lisätään täsmälähetysreititysprotokolla toimimaan VRF:n kanssa, koska muuten ei VRF tule toimimaan itsenäisenä reitityksenä. Reititysprotokollaan sidotaan virtuaaliportin osoite ja aliliitännän osoite reitittymään saman reititysprotokollan alle. Tällöin nämä muodostavat uuden reititystaulun, joka erottuu tavallisesta reitityksestä ja toimii omana reitityksenä.

Nyt VRF-reititys alustukset on tehty valmiiksi. Pitää muistaa, että kaikkiin portteihin on syötettävä samat käskyt kuin edellisessä esimerkissä. Nämä vaiheet siis tulisi syöttää kaikkiin reitittimiin, jotka ovat mukana Multicast VRF -reitityksessä. Multicast VRF -reitityksen testaus ja toimintavalmiuden tulkinta voidaan suorittaa samankaltaisilla käskyillä kuin tavallinen ryhmälähetysliikennekin.

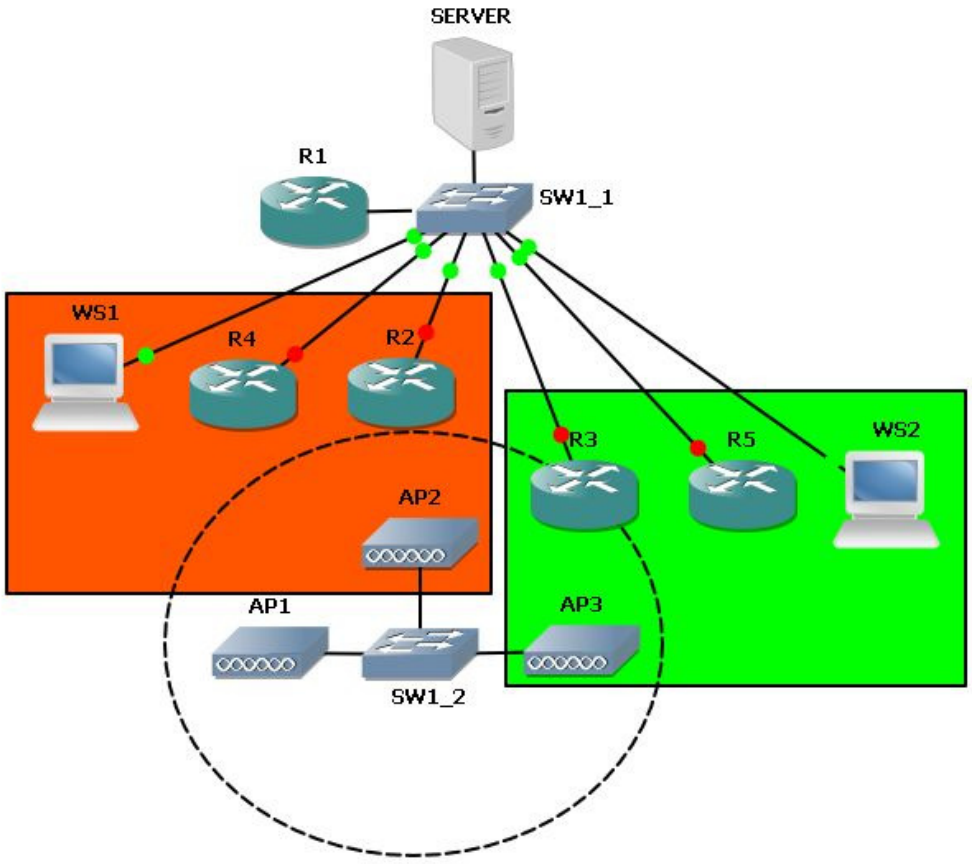
Viasta palautuminen

Viasta palautuminen on ehkäpä yksi tehokkaimmista tavoista hyödyntää Multicast VRF -tekniikkaa. Oletusajatus on se, että kaikki toimisi ja eikä tarvitsi olla mitään suurta huolta myöskään vikatiloista. Kuitenkin vikaantuminen on hyvin mahdollista missä ympäristössä tahansa, ja vikatilojen syntymiseen liittyvien riskien on oltava tiedossa. Sitä kautta järjestelmälle on mukavampi rakentaa nopea palautumisprosessi toimintatilaan. Seuraavaksi käydään läpi kuvan 15 mukaista esimerkkijärjestelmää.



Kuva 15. Vikasietoinen Multicast VRF -verkkotopologia

Aluksi pitää mainita, ettei fyysisiä laitteita ole todellisuudessa niin paljon, kuin kuvassa 15 esitetään. Kuvassa olevat SW1, SW2, SW3, SW4, SW5 ja SW6 ovat samaa fyysistä laitetta. Myöhemmin esitän, miltä kytkentä olisi tiivistettynä ja miksi esimerkkikytkentä on kuvan 16 esittämän näköinen. Kuitenkin kuvasta 15 on helpompi nähdä, miten kytkentä toimii. Topologianäyttäisi kuvan 16 laiselta supistettuna pelkkiin loogisiin laitteisiin. Erityisesti huomiota kannattaa kiinnittää siihen, että SW1 on jaettu kahteen laitteeseen.

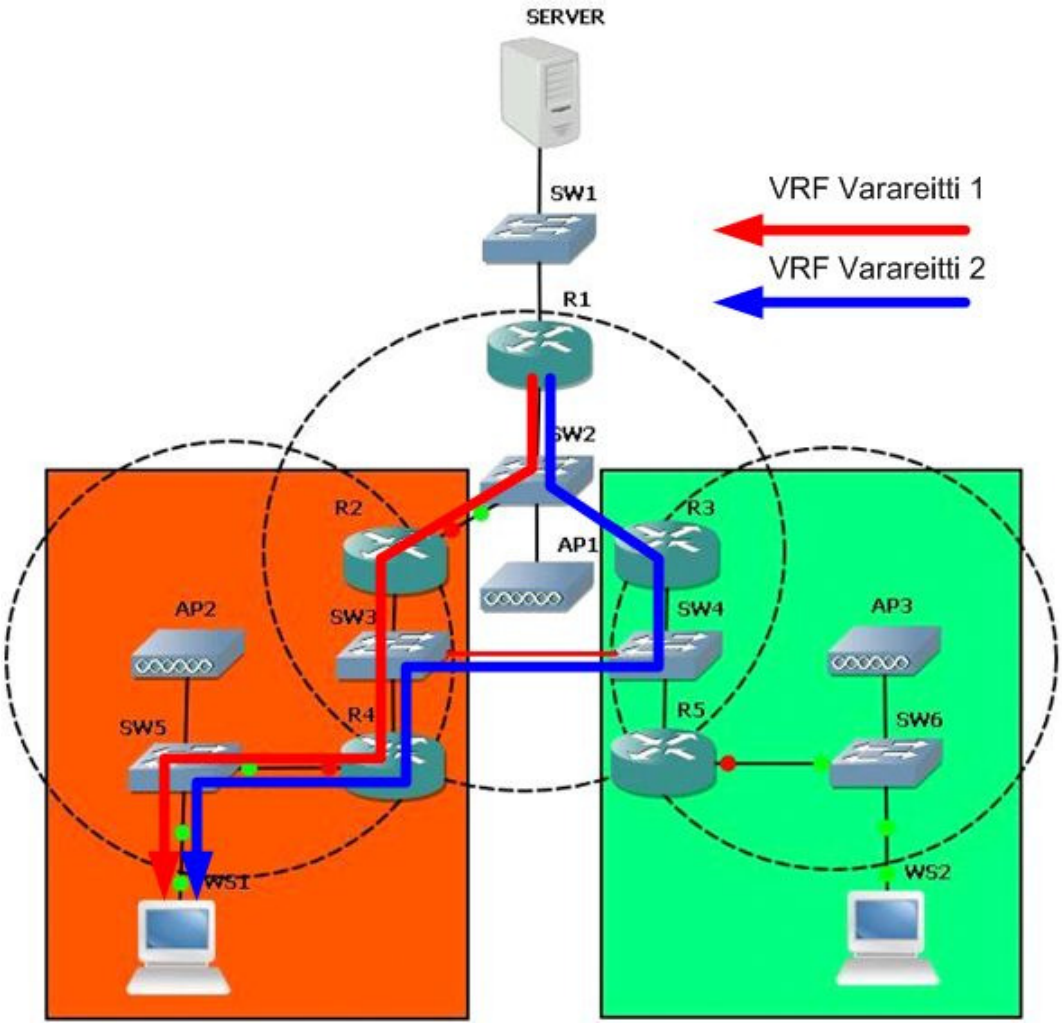


Kuva 16. Vikasietoinen Multicast VRF -verkkotopologia tiivistettynä

Ajatellaan, että WS1 haluaa liittyä palvelimen lähettämään materiaaliin. Nopeamman reitin tapauksessa oletusreitti kulkisi yhteyspisteestä toiseen R1:stä suoraan käyttäjälle kytkimen SW1 kautta.

Jos tapahtuu katkoksia, Multicast VRF tehtävä on palauttaa liikenne mahdollisimman nopeasti. Tavallinenkin ryhmälähetysreititys voi palauttaa liikenteen, mutta viive voi

olla hyvin pitkä riippuen verkkotopologiasta. Lähiverkossa viive on noin kymmenen sekunnin luokkaa. Joissakin tapauksissa ryhmälähetysliikenteen palautuminen toimintatilaan vaatii katkoksen korjauksen riippuen siitä, kuinka kriittiseen kohtaan topologiassa katkos tulee. Kuva 17 esittää, miten kyseisessä tapauksessa varareitit voisivat muodostaa.



Kuva 17. Vikasietoinen Multicast VRF:n varareititys

Kun katkos muodostuisi AP1:n ja SW2:n välille ensisijainen reititys ei toimisi, ja tällöin tulisivat seuraavat varareitit mahdollisiksi: Käytössä olisi toissijainen reitti R2:n, SW3:n ja R4:n kautta SW5-kytkimen alla olevaan työasemaan. Jos reititys lopettaisi toimintansa R2:sessakin, varareititys menisi R3:n, SW4:n, SW3:n ja R4:n kautta jälleen SW5-kytkimen työasemalle saakka.

VRF:n idea on jo kerrottu aikaisemmin, joten siihen en puutu tässä. Mutta ryhmälähetys VRF-reiteillä voidaan kiertää kytkentä nopeasti toista reittiä tai useampiakin reittejä. Multicast VRF ei kuitenkaan auta vikaantumisen ehkäisyssä, jos katkos tapahtuisi esimerkiksi yhden liitoksen varassa olevaa kytkentäpistettä.

Käskypolitiikka ei ole oikeastaan yhtään monimutkaisempi tai laajempi kuin jo edellä käydyt Multicast VRF:n käskyt. Tärkeintä on vain pohtia, miten haluaa rakentaa varareitit. Tähän liittyvät esimerkkijärjestelmän käskylistaukset ovat liitteessä 4.

7.4 WLAN-liikenteen ohjaus

WLAN-liikenne tavallisessa ryhmälähetysessä tai VRF:ssä ei tuo kovin suuria poikkeuksia. Jotta liikenne olisi mahdollisimman turvallista, tarvitaan tietoturvaa. Toinen asia, mikä tulee ottaa hyvin huomioon langattoman liikenteen tapauksessa, on liikenteen profilointi. Profiloinnista kerrotaan myöhemmin luvussa 9.4.

WLAN-ryhmälähetyksessä tulee olla mielellään salaus, jotta liikenne ei olisi avoinna kaikkialle. Jollei salausta ole, se olisi suuri uhka tiedon eheydelle. Hyvin määritellyn salauksen isäntäkone voi liittyä lähiverkkoon ja liittyä joko multicast VRF:ään tai tavalliseen ryhmälähetysliikenteeseen.

Salauksen lisäksi käyttäjien hallittavuutta on syytä miettiä. Esimerkiksi etäreitittimille olisi hyvä olla tietokanta käyttäjistä, jotka saavat liittyä verkkoon. Näin ollen kaikki olisi valmista langattomaan liikenteeseen käyttäjän näkökulmasta.

8 Liikenteen profilointi

Liikenteen profiloinnilla tarkoitetaan sitä, että halutaan tehdä tietynlaista ennalta määrittelyä ennen kuin liikenne luodaan. Liikenteen profilointi auttaa hallinnoimaan käyttäjiä sekä sitä, mistä ja millä he kytkeytyvät ryhmälähetysverkkoon.

Liikenteen profiloint sijainnin mukaan on todella tehokas tapa profiloida. Käyttäjät voivat päästä esimerkiksi vain tietystä paikasta, kuten tavallisesta toimistohuoneesta tietynlaiseen tarjontaan ryhmälähetysliikenteestä. Tällöin voidaan ajatella, että liikenne olisi aina tietynlaisissa loogisissa sektoreissa. Edellä mainittua profilointia hallitaan VLANien avulla, tai on jos tietty käyttäjä halutaan pitää tietyssä liikenteessä kiinni, niin käytetään Multicast VRF -tekniikkaa hyväksi. Esimerkkinä valvontakameralle voidaan osoittaa kiinteä sijainti, ja sitä pääsevät seuraamaan vain tietyt isäntäkoneet.

Profilointi laitteen tai laiteiden mukaan voi olla monimutkaista, koska siihen ei voi olla samanlaisia loogisia sektoreita kuin sijainnin mukaisella profiloinnilla. On olemassa etuja, joita ei saavuteta sijainnin mukaisella profiloinnilla. Laitteen mukaan voidaan mukauttaa palvelimien suoratoistomäärittelyjä, ja tietyn ryhmäosoitteen kautta voidaan määritellä hyvin optimaalinen verkkoresurssin tarve.

Langatonta liikennettä varten yleensä joudutaan tekemään oma profilointi. Syy perustuu lähinnä siihen, että siihen liittyvät työasemat voivat olla niin erilaisia toisiinsa nähden. Kyseessä ovat matkapuhelimet, kannettavat tietokoneet ja kämmentietokoneet, jotka hakevat yhteyttä. Tällöin laitteet voidaan profiloida omaksi liikenteekeeni. Ongelmanratkaisuun kuitenkin voi tarvita tietynlaista tietokantaa, joka olisi sidottu käyttäjäryhmiin.

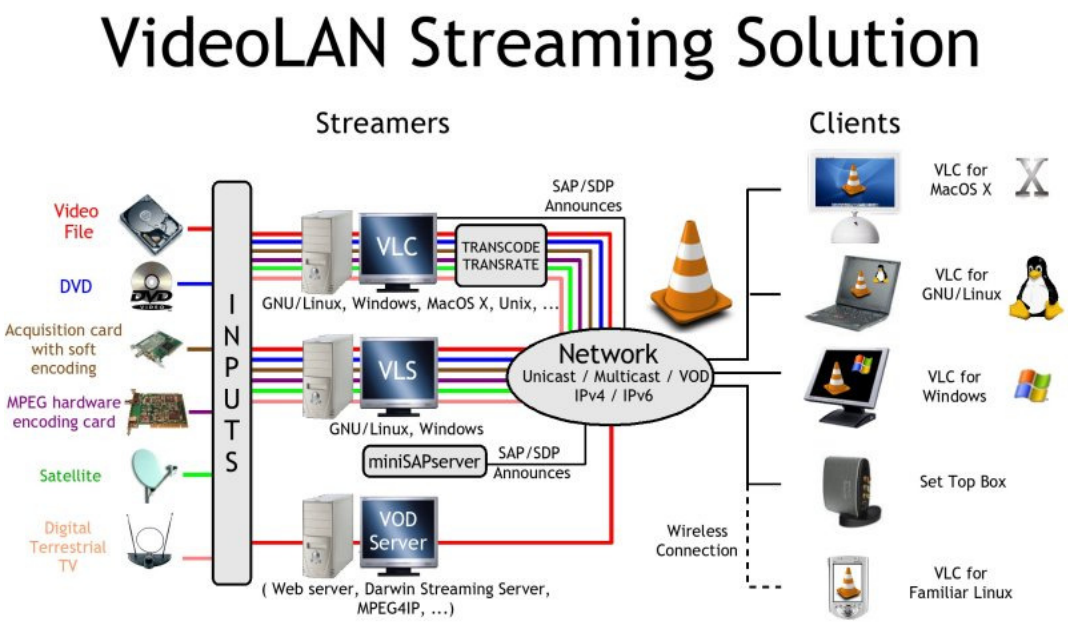
9 Videonjakelujärjestelmä VLC-ohjelmalla

9.1 Perusteet

VLC Media Player on tällä hetkellä varteenotettava mediantoisto-ohjelmisto. Se on ilmainen, joustava ja monipuolinen. VLC-mediasoittimeen löytyy kattava dokumentointi ja perusopasteita. VLC-mediasoitinta voidaan käyttää joko palvelimena tai isäntäkoneessa tavallisena soittimena. Yksi ohjelmisto sisältää molemmat toiminnallisuudet. Tavallisena soittimena sillä on hyvät videotoisto-ominaisuudet ja palvelimena käytettynä se tarjoaa hyvin laajat tavat luoda ja välittää videoita muille käyttäjille. Ohjelmisto myös tukee määrittelyjä, joita voidaan myös ajaa komentosarjana tai selainmuotoisena. Sitä kautta ryhmälähetysliikenteen saatavuus käyttäjille tehdään helpommaksi, ja käyttäjän tarvitsee hallita vain yhtä ohjelmistoa.

Edellä mainituilla perusteilla valitsin VLC-mediasoittimen testiympäristöön. Lähin vastaava vaihtoehto olisi ollut Darwin Streaming Server (DSS) [28.]. Se on hieman rajoittuneempi kuin VLC ja sisältää vain palvelinympäristön. Muitakin vaihtoehtoja olisi ollut, mutta ehtona on ottaa käyttöön vapaaseen lähdekoodiin perustuva soitin, joka sisältää laajat ominaisuudet ja jossa on palvelin- ja asiakastoiminnot.

Suoratoistoon liittyviä testituloksia esitetään liitteessä 4. Kuva 18 esittää, millaisia videonjakelukonsepteja VLC-mediasoitin pystyy hallitsemaan.



Kuva 18. VideoLAN-suoratoiston esimerkkijärjestelmä [29.]

9.2 SAP:n rooli VLC-soittimessa

SAP:n ideana on kertoa käyttäjälle, minkälaista liikennettä on tarjolla ja mainostaa suoratoiston olemassaoloa. SAP-julkaisu määritellään mielellään aina. SAP-julkaisun määrittelyn tavoitteena on saada katselijat tietoisuuteen siitä, mitä suoratoistoa verkossa on tarjolla. Voi olla syitä, miksi ei SAP-julkaisua määriteltäisi. Silloin ei olisi olemassa kyseistä palvelinta, joka huolehtisi julkaisujen olemassaolosta. VLC Media Player ei huolehdi SAP-julkaisujen mainostuksesta vaan siihen tarvitaan erillinen Mini-SAP-palvelin. Liitteessä 5 on esimerkki siitä, miten Mini-SAP asennetaan. VLC:ssä itse mediaan suoratoistoon voidaan määritellä SAP-tiedot erikseen, joten mainostustiedot tulevat VLC:n kautta, mutta vain niiden välittämiseen tarvitaan edellä mainittu Mini-SAP-palvelin. SAP-julkaisun määrittelyt toteutetaan suoratoiston määrittelyn loppuvaiheissa.

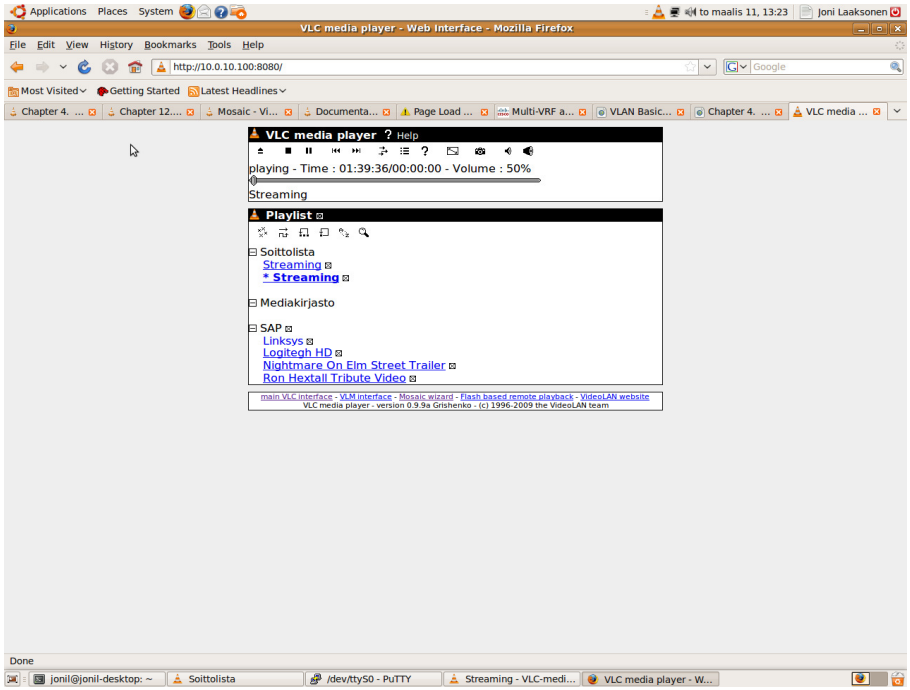
SAP-julkaisun tulisi kuvata liikennettä loppukäyttäjälle seuraavasti:

- SAP-ryhmän nimellä kuvataan parhaiten kanavapakettia, jossa on useita nimikkeitä eli ryhmän alaisuudessa olevia lähetyksiä. Ryhmän nimeksi voisi sopia vaikka ”Live-lähetykset” tai jonkun tietyn opettajan oma ”Opetuskanava”.
- SAP-viestin nimike kuvaa taas itse kanavan tai lähetyksen nimeä.

SAP-julkaisujen katselu vaatii, että VLC:ssä käynnistetään palvelujen haku. Palvelujen haun kautta VLC alkaa hakea verkosta saapuvia SAP-mainostuksia ja tulostaa ne sellaisenaan kuin ne on määritelty niiden suoratoistojen ohella. Kuten kuvassa 19 nähdään, SAP-mainostukset soittolistalla näkyvät selkokielellä ja esittävät tarkasti, mitä verkossa suoratoistetaan.

Kuva 19. SAP-palvelujen näkyminen VLC-mediasoitimessa

Kuvassa 20 nähdään paikallista suoratoistoa, joka ei ole SAP:n viestittämää. Myös HTTP-pohjaisessa soittimessa SAP-mainostamat suoratoistot tulevat omana listana. Tässä kohtaa on tärkeää mainita, että niin kuin tavallisessa soittimessakin vasta palveluiden haun kautta SAP-mainostukset näkyvät internet-selaimessa. Palveluiden haun jälkeen pitää myös sivusto päivittää, jotta SAP-mainokset tulevat näkyviin.

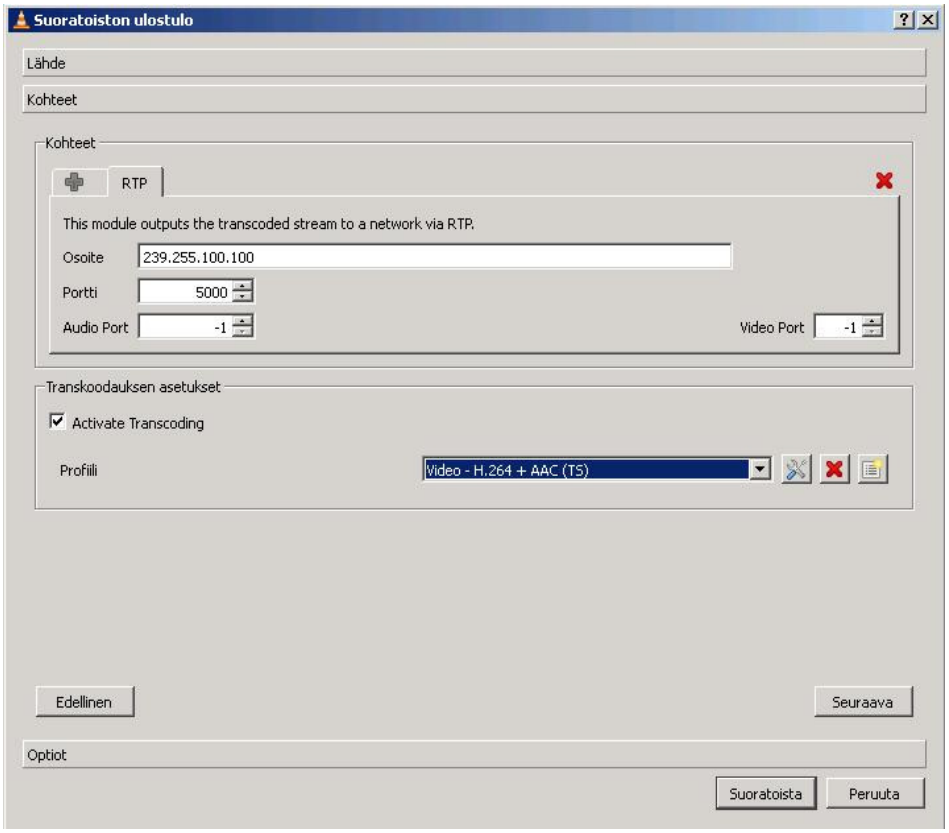


Kuva 20. Suoratoiston HTTP-pohjainen VLC mediasoitin

9.3 Suoratoiston lähetysmuotoja

Kun tehdään toisto omalle päätteelle voidaan todeta, että nähdään, toimiiko suoratoisto moitteettomasti ja onko se laadullisesti hyvä. Tämä toimii ikään kuin laaduntarkkailuna suoratoistolle ja helpottaa huomaamaan virheet.

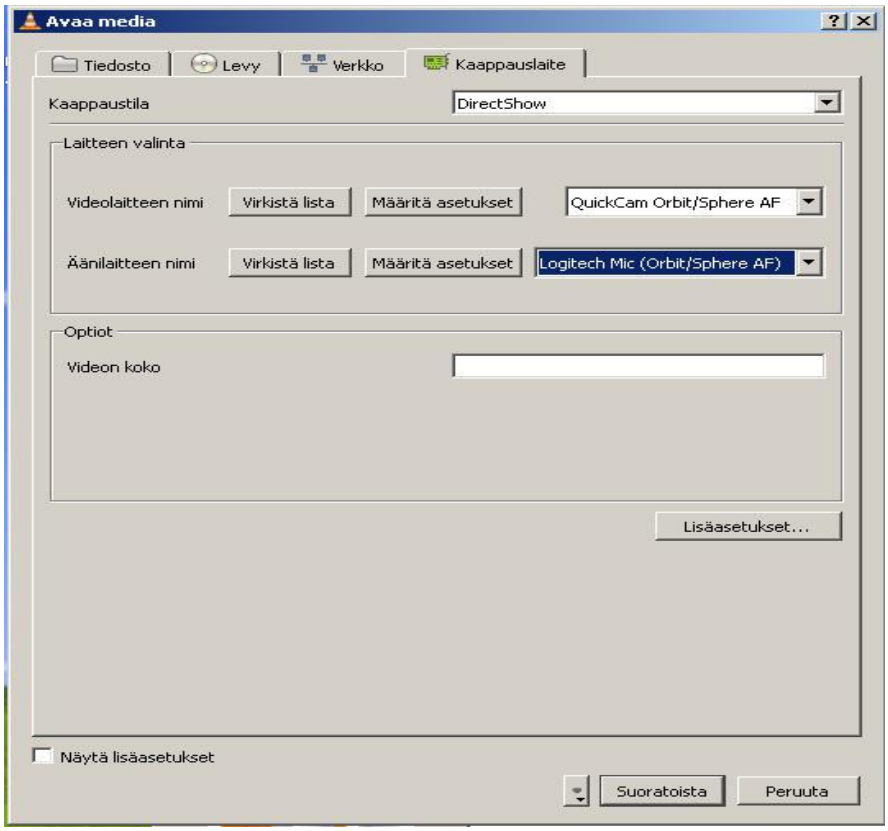
Suoratoisto voidaan toistaa monilla eri protokollilla kuten UDP:llä, RTP:llä ja RTSP:llä. Ryhmälähetyksen yhteydessä suoratoisto tulee käyttämään RTP-protokollaa. RTP:n valita perustuu siihen, että jo aikaisemmin mainittu UDP ei takaa muun muassa luotettavuutta ja sekvenssisyyttä. RTP antaa näihin teknisiin puuteisiin korjauksen. Tämän avulla suoratoiston paketit eivät tule perille vastaanottajalle epäjärjestyksessä tai eikä kuva katkeile protokollien takia. Kuvan 21 tapauksessa RTP-protokolla voidaan valita ja syöttää tarvittava ryhmälähetysosoite ja porttitiedot.



Kuva 21. Tyypillinen suoratoiston määrittelysivu

Suoratoistoa voidaan myös suorittaa Telnetin avulla VLC:ssä. Soittimen toimiessa palvelimena siihen voidaan yhdistyä Telnet-yhteydellä. Yhteyden ohella käynnistetään siihen mukautuva komentosarjatiedosto. Myös Interneissä käytettävä HTTP-pohjainen rajapinta on tuettu VLC-mediasoittimessa. Nämä ominaisuudet tuovat lisä-mahdollisuuksia, miten toteuttaa suoratoistoa. HTTP-pohjaisessa soittimessa on sekin etu, että sitä voidaan seurata Internet-selaimella ja silloin muun muassa matkapuhelimet ja kämmentietokoneet pystyvät helpommin seuraamaan VLC:llä välitettyä suoratoisto-tarjontaa.

VLC:ssä voidaan valita videonkaappauslaiteita kuten web-kameroita ja tehdä niillä suoratoistoa. Web-kameroilla voidaan käyttää kaikkia edellä mainittuja suoratoiston mahdollisuuksia. Suoratoisto web-kameroilla mahdollistaa erilaisia käytännön sovelluksia, joista kerrotaan seuraavassa luvussa. Kuva 22 esittää määrittelysivun, josta näkyy, miten koneeseen kytketyt kamerat näkyvät VLC-ohjelmassa.



Kuva 22. Suoratoiston videonkaappausvälisivu

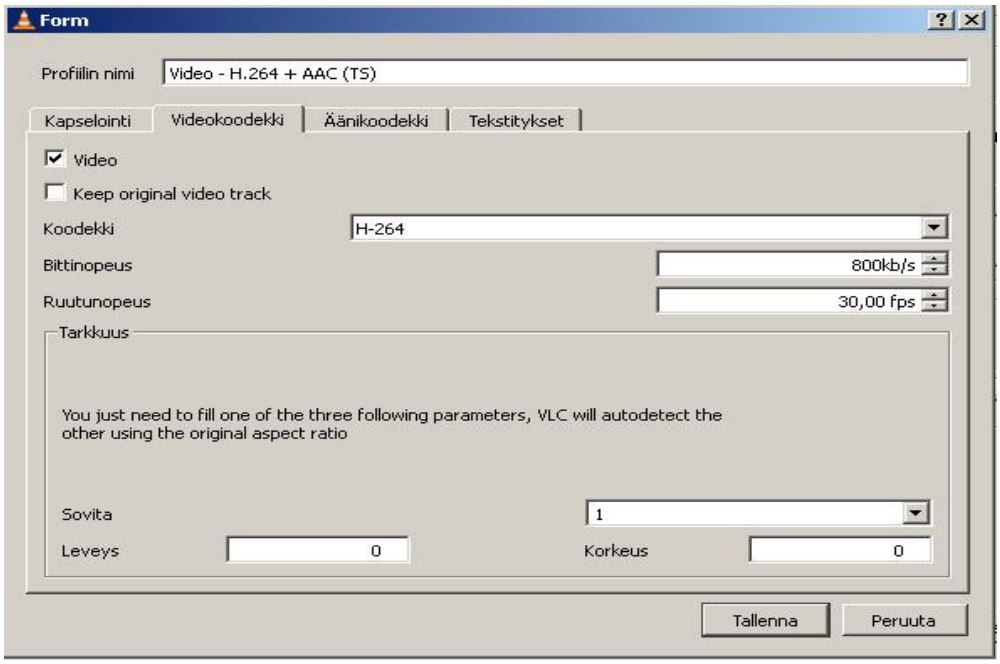
Eri suoratoistojen yhteydessä tulee määritellä TTL-arvo, koska se määrittelee maksimi-reitittimien hyppyjen määrän. Jokaisen hypyn kohdalla TTL-arvo vähenee yhdellä, ja kun sen arvo saavuttaa nollan reitittimessä ,liikenne lakkaa toimimasta. Näin ollen, jos TTL-arvoa ei ole määritelty tarpeeksi suureksi, suoratoisto ei saavuta tiettyjä aliverkkoja. Tarvittavan suuri TTL-arvo on alle 10:n lähiverkkojen kohdalla, ja sitä suurempi arvo riittää kattamaan jo valtavia tietoverkkoja.

9.4 Liikenteen profilointi VLC-ohjelmassa

Liikenteen profiloinnin määrittelyjä voidaan tehdä VLC:ssä. Tarpeellisuus yleensä vaaditaan, kun puhutaan matkapuhelimista tai kämmentietokoneista. Syynä tähän muun muassa tarve pienentää verkkokaistaa, jolloin tarvittavien kuvapisteiden määrää

kannattaa pienentää. Muitakin mahdollisia syitä voi olla. Profilointi edes auttaa suoratoiston mukautumista tiettyihin tietoverkkoympäristöihin.

Liikenteen profiloinnissa tulee esiin suoratoiston kapselointi. Sillä tarkoitetaan, sitä videostandardia, jota kyseisessä suoratoistossa käytetään. RTP-protokollaa käytettäessä on käytettävä MPEG-TS –kapselointia (Moving Picture Experts Group- Tranport Stream). Video- ja audioformaatti on ominaisuus, jolla muovataan kyseinen liikenne johonkin haluttuun muotoon. Tarjolla on useita eri formaatteja, ja niillä pystytään määrittelemään kaistamäärä, jolla audiota ja videota välitetään ja ruudunpäivitys videon kohdalla hoidetaan. Näiden profilointien vaiheiden kautta voidaan saavuttaa laadullisesti hyvä tai erinomainen suoratoisto. Kuva 23 esittää, millainen profilointi-ikkunan näkymä on.

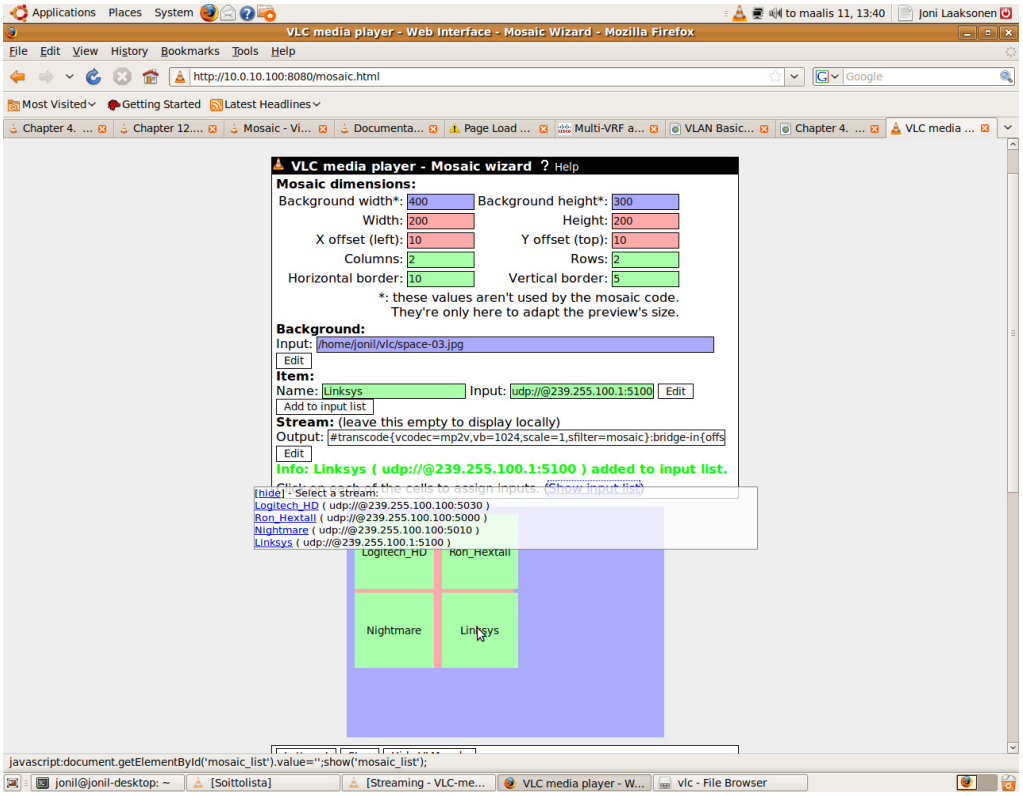


Kuva 23. Suoratoiston liikenteenprofilointi määrittelysivu

9.5 Suoratoiston luonti Mosaic-käyttöliittymä

Mosaic-rajapinta on hieman omaperäisempi tapa suoratoistojen näyttämiseen. Ideana se, että jos on tarjolla paljon kanavia, voidaan tehdä ns. kanavapaketti ja tuoda se ruudulle kerralla pieninä ikkunoina.

Etuna on, että käyttäjän ei tarvitse selailla kanavasta kanavaan, vaan hän voi tarkastella jo tarjontaa ennen kuin käynnistää suoratoiston tiettyyn kanavaan. Ominaisuus myös antaa verkonkaistalle vapautta, koska ei tule jatkuvia turhia suoratoiston käynnistyksiä. Ryhmälähetyksessä verkkokapasiteetin kuormitus ei ole mikään huolestuttava asia, mutta jos kyse olisikin täsmälähetyspohjaisesta eli Video-on-demand –suoratoistosta, konsepti olisi hyvä ratkaisu ehkäisemään verkkomedian ylikuormitusta. Kuva 24 esittää Mosaic-määrittelysivun, jossa on tehty profiileja, ja profiilit on asetettu tiettyihin ikkunoihin, joista tiettyä kanavaa voidaan seurata.



Kuva 24. Suoratoiston Mosaic-rajapinnan asetussivusäädöksien kanssa

10 Ryhmälähetyssuoratoiston sovellukset

Web-kameroita on kaksi luokkaa. Ensimmäinen luokka luetaan kameroihin, jotka tulee kytkeä suoraan työasemaan. Toinen luokka kameroista ovat työasemasta riippumatomia ja ne voidaan sijoittaa eri puolille verkkoa.

10.1 Tietokoneeseen kytkettävien kameroiden sovellukset

Aina, kun puhutaan tiettyyn tietokoneeseen kytkettävästä kamerasta, etäisyys kameran ja työaseman välillä on lyhyt ja katselukulmakin usein kapenee kohtuullisen pieneksi. Lyhyt etäisyys tietokoneesta johtuu USB-kaapelista, jonka pituus on useimmiten noin kaksi metriä. USB-kaapelin maksimipituus on viisi metriä. Syy, miksi laiteet tyytyvät lyhyempiin pituuksiin, ovat sähkömagneettiset kentät ja siirtolinjan rajoitteet. [30.] Myös katselukulma jää helposti pieneksi, koska sijoittelu kohdistuu joko pöydälle tai näytölle. Kameroiden käyttötarkoitus näillä kriteereillä on tulla kuvaamaan yhtä henkilöä pienen matkan päästä.

Sovellukset, jotka voisivat sopia parhaiten näille kameroille ovat:

- live-opetus, eli jostakin kiinteästä työasemasta voidaan tehdä suoratoistolla opetusmateriaalia oppitunnista
- videoneuvottelu, eli kahden tai useamman henkilön videokeskustelu verkon kautta
- laboratorion käytännön harjoituksiin, eli opiskelijoille työkalu, jolla voidaan tehdä reaaliaikaista suoratoistoa ja tehdä mittauksia.

Koneeseen kytkettävät kamerat sisältävät vertailussa kolme kameraa, jotka esitetään taulukossa 2.

Taulukko 2. Tietokoneeseen kytkettävät kamerat

Merkki	Logitech	Microsoft	Logitech
Malli	QC 3000 Business	LifeCam Cinema	QuickCam Sphere AF
Hinta	25 euroa	61 euroa	114 euroa
Tarkkuus	640x480,30fps	720p,2.0M,HD,30fps	1600x1200,2.0M,HD,30fps
Saatavuus	Verkkokauppa	Verkkokauppa	Verkkokauppa
Kennotyyppi	VGA CMOS	HD CMOS	HD CMOS
Yhteensopivuus	Windows, Linux	Windows	Windows
Lisäominaisuudet	Liikkeentunnistin	Laajakuva malli	Carl Zeiss-optiikka

Valintaperusteina käytettiin saatavuutta, hintaa ja ominaisuuksia. Tarjolla oli hyvin monta samankaltaista kameraa, mutta näiden kyseisten kameroiden kokonaiskuva verrattuna kilpailijoihin olivat optimaaliset. Valinnoissa haettiin kameroita kolme eri hintaluokassa halvasta, keskihintaiseen ja aina kallishintaisiin saakka. Valintakriteereinä näille edellä mainituille kameroille olivat seuraavanlaiset:

- Skaalautuvuus eli mahdollisimman erilaiset kamerat toisiinsa nähden. Näin ollen nähdään kameroiden erilaisuus.
- Käyttötarkoitus eli mihin käyttöön tarkalleen kamera sopii.
- Hinta-laatusuhde, joka esitetään suhteessa ominaisuuksien ja hinnan välillä. Pelkästään laadun tai hinnan mukaan ei voida tehdä vertailua yksipuolisesti, koska kamerat ovat niin erilaiset.

Tässä yhteydessä käytetään VLC-mediasoitinta laadullisien kriteereiden tarkasteluun ja lopuksi annetaan jokaiselle arvosana ja kirjataan päätelmät. Taulukossa 3 nähdään tulokset kyseisistä kameroista.

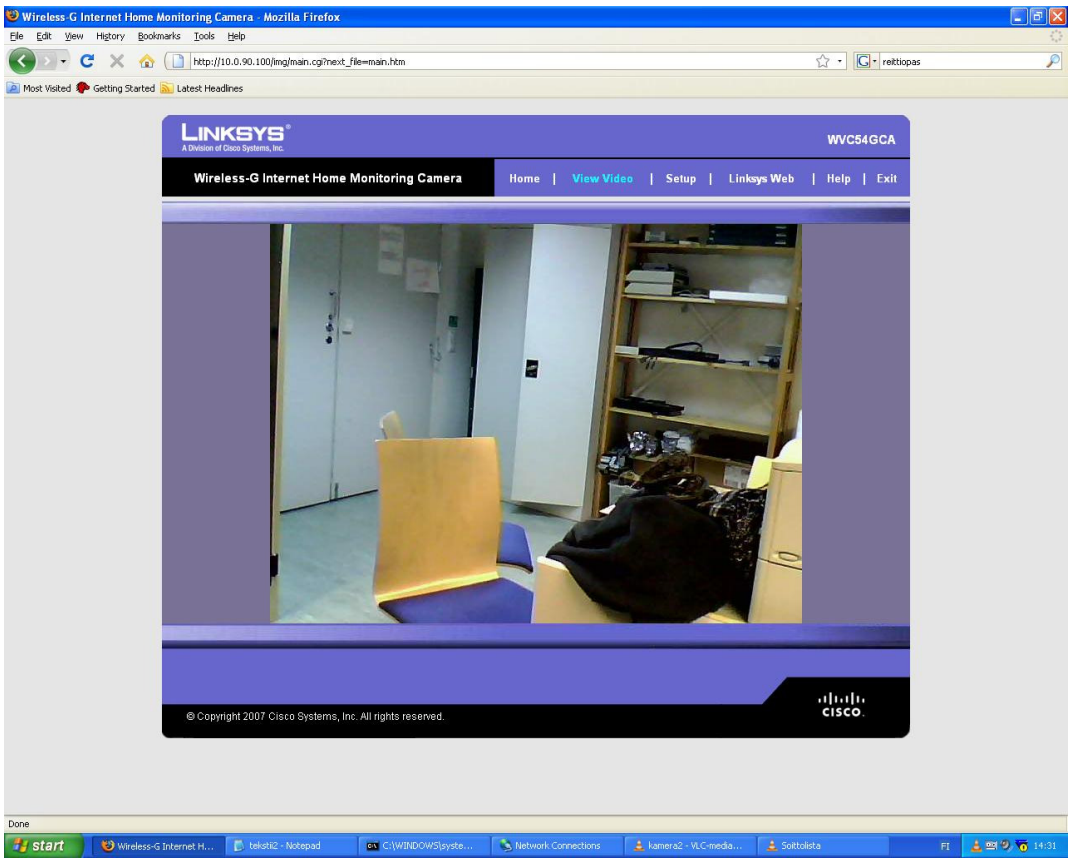
Taulukko 3. Tietokoneeseen kytkettävien kameroiden tulokset

Merkki	Logitech	Microsoft	Logitech
Malli	QC 3000 Business	LifeCam Cinema	QuickCam Sphere AF
Laatu / Tarkuus	Tyydyttävä, ruudun päivitys kohtuullinen, tarkuus riittävä henkilökasvojen näyttämiseen	Erittäin tyydyttävä, kuvan terävyys erittäin hyvä, mutta kuvanpäivitys heikkoluokkainen (tulee näkyviä vaakajuovia), tarkuus riittää muunkin ympäristön kuvaamiseen	Erittäin hyvä kokonaisuudessaan, erittäin terävä kuva ja kuvan-päivitys hyvä, tarkkuus riittävä kaikkiin valaistujen ympäristöjen kuvaamiseen
Käyttökohde	Näytölle / pöydälle, Laboratorio-harjoituskameraksi	Näytölle / pöydälle, Laboratorio-harjoituskameraksi	Näytölle / pöydälle, Laboratorio-harjoituskameraksi ja Live-opetus- ja videoneuvottelu-käyttöön
Hinta-laatusuhde	Hyvä, halpa hinta ja siitä huolimatta siedettävä kuva	Tyydyttävä, Tarkkuus luokaltaan loppujen lopuksi vain erittäin tyydyttävä, jolloin hinta on yli-hinnoteltu	Hyvä, tarkkuus kaikkiaan loistava, jolloin hinta on myös hyvin perusteltua.
Arvosana	8, Edullinen kamera, joka tarjoaa kaikki peruselementit, joita kameralta voi vaatia	7,5, Hieman kallis kamera, vaikka tarjoaakin HD-kuvan-laatua, ruudunpäivitys ongelmia	9+, Hieman korkea hinta, mutta tarkkuus on huippuluokkaa jolloin se sopii moneen eri käyttöön

Tuloksista voidaan päätellä, että halvan (Logitech QC 3000 Business) ja keskihintaisen kameran (Microsoft LifeCam Cinema) kokonaisero on hyvin pieni. Yleensä hinta on suurempi pääpaino hinta-laatusuhdetta katsottaessa, joten kyseisistä kameroista halvin olisi ideaalinen laboratorioharjoituskamera. Myös kun ajatellaan halvimman kameran rikkomis- tai häviämistapauksia, kamera ei tuottaisi suuria taloudellisia tappioita. Toisaalta vertailun kallein kamera (Logitech QuickCam Sphare AF) olisi hyvä vaihtoehto myös muihin suoratoistotarkoituksiin, kuten opetuskäyttöön, koska voisi siten näyttää muun muassa taulumerkintöjäkin tai muuta vastaavaa.

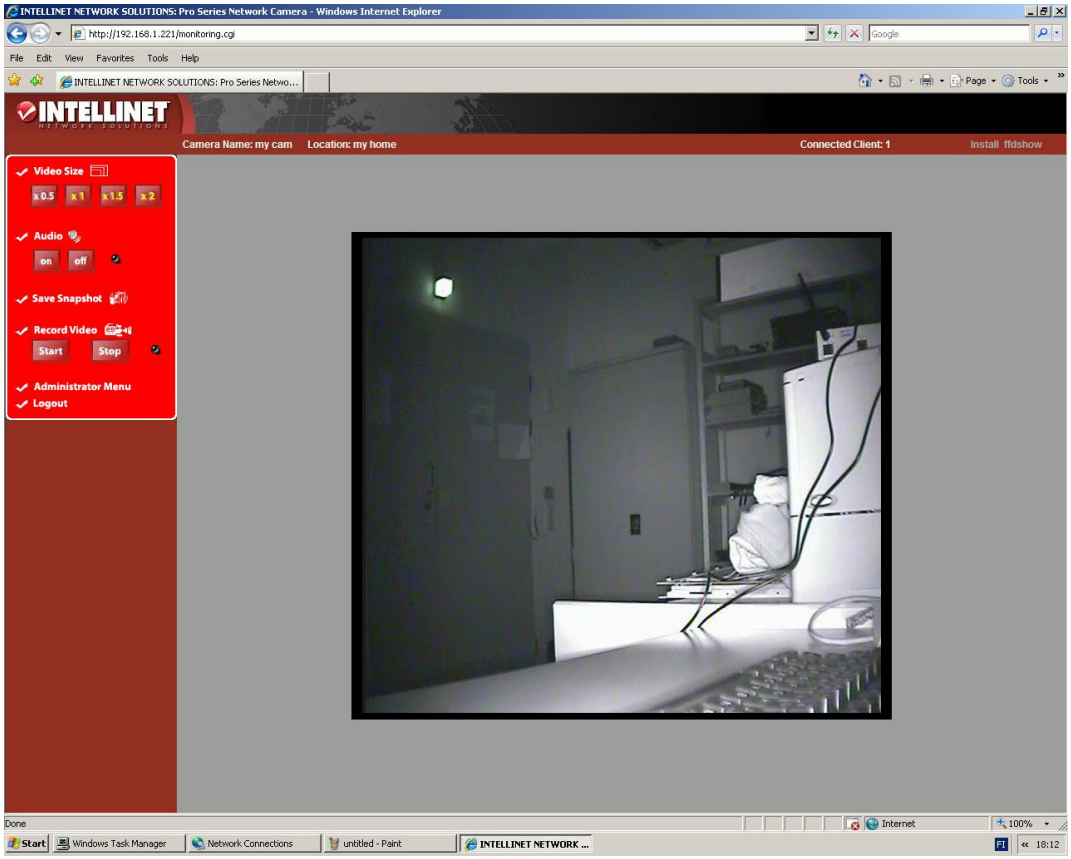
10.2 Verkkoon kytkettävien kameroiden sovellukset

Verkkopohjaiset kamerat ovat parempia kuin koneisiin kytkettävät, sillä niitä voidaan liittää ihan minne tahansa paikallista tietoverkkoa. Tämä antaa liikutettavuuden edun. Verkkopohjaiset kamerat tarjoavat myös oman sisäisen hallintasovelluksen, jolla tehdään kalibroinnit ja muut tarvittavat verkkomäärittelyt. Hallintasivustoon mennään Internet-selaimella, ja kamerat yleensä tarjoavat myös sisäisen käyttäjänhallinnan. Kuvassa 25 nähdään, kuinka selaimella voidaan nähdä suoraa videomateriaalia.



Kuva 25. Web-kameran Internet-selain- pohjainen katselusivusto

Sovellukset ovat oikeastaan hyvin samankaltaiset kuin koneeseen kytkettyissä kameroissa, mutta valvontakameraympäristön mahdollisuus on hyvin toteutettavissa verkkopohjaisilla kameroilla. Liikuteltavuus ja tietyt erikoisominaisuudet tarjoavat valvontakamera mahdollisuuden. Kuvassa 26 nähdään infrapunan näkymä, joka mahdollistaa myös pimeän tilan näyttämisen.



Kuva 26. Infrapunan näkyminen verkkopohjaisessa web-kamerassa

Verkkoon kytkettävien kameroiden vertailussa on kaksi kameraa, jotka esitetään taulukossa 4.

Taulukko 4. Lähiverkkoon kytkettävät kamerat

Merkki	Linksys	Intellinet
Malli	WVC54GCA-EU	550307
Hinta	98 euroa	377 euroa
Tarkkuus	640 x 480	640 x 480, 25 fps
Saatavuus	Multitronic	Notesco
Kennotyyppi	VGA CMOS	1/3” SONY Super HAD CCD
Sijoittelukohta	Sisätila (käytävä, luokat)	Sisätila (aulat, laajat tilat)
Lisäominaisuudet	WLAN, liikkeentunnistin	WLAN, PoE, IR, liikkeentunnistin, mikrofoni

Valintaperusteina käytettiin myös saatavuutta, hintaa ja ominaisuuksia. Varsinkin saatavuuden ja hinnan kannalta tavoitteeksi tuli etsiä kaksi mahdollisimman erilaista kameraa, koska joidenkin valmistajien kameroiden hintaluokka oli turhan suuri opinnäytetyötarkoitukseen. Toisaalta joillakin valmistajien kameroiden saatavuus oli hyvin kyseenalainen jälleenmyyjien kautta. Täten katsottiin parhaaksi ottaa huomioon samanlaisia valintakriteereitä kuin koneisiin kytkettävissä kameroissa. Valinnoissa haettiin kameroita halvoista ja keskihintaisista.

Tässäkin yhteydessä käytettiin VLC mediasoitinta laadullisien kriteereiden tarkasteluun ja lopuksi annetaan jokaiselle arvosana ja päätelmät. Taulukossa 5 nähdään tulokset kyseisistä kameroista.

Taulukko 5 Tietoverkkoihin kytkettävien kameroiden tulokset

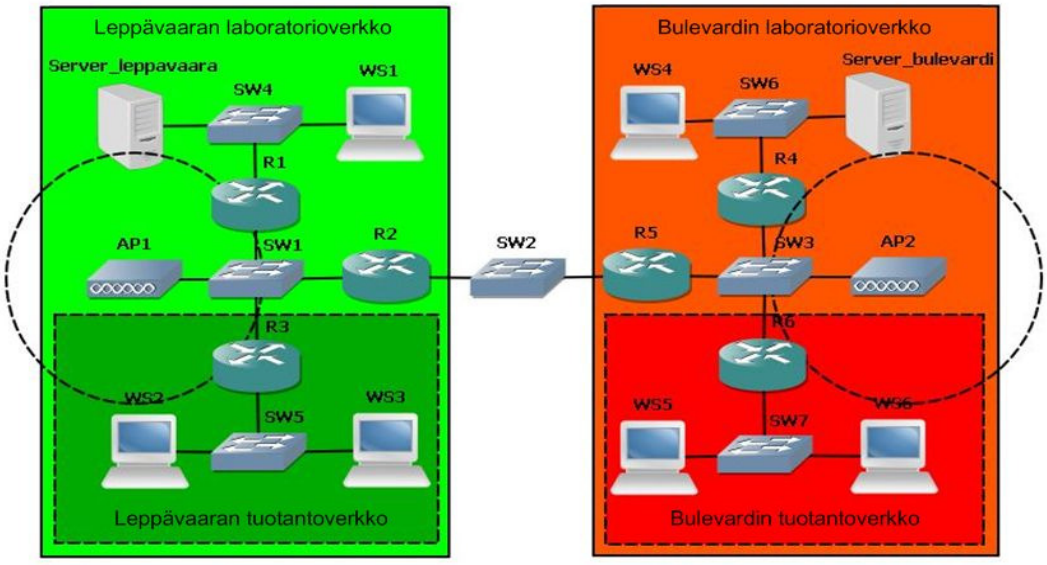
Linksys WVC54GCA-EU	Intellinet 550307
Hyvä tarkkuus ja ruudun päivitys kohtuullinen, tarkkuus riittävä ympäristön kuvaamiseen Kamerassa on WLAN-tuki ja liikeentunnustin	Hyvä tarkkuus ja ruudun päivitys hyväluokkanen, tarkkuus riittävä ympäristön kuvaamiseen päiväsaikaan ja yöaikaan (infrapuna). Kamerassa on WLAN-tuki ja liikeentunnustin
Pöydälle, laboratorio-harjoituskameraksi, live-opetus, videoneuvottelukäyttöön ja myös rajatussa mielessä valvontakameraksi	Pöydälle / seinään kiinteästi live-opetus, videoneuvottelu-käyttöön ja myös valvonta-kamerakäyttöön
Hyvä, halpa hinta ja siitä huolimatta hyvä kuva ja tarkkuus, myös langaton kamera	Hyvä, kohtuullisen halpa hinta valvontakameraksi, on myös langaton kamera
8+, edullinen kamera, joka tarjoaa kaikki peruselementit, joita verkko-kameralta voi vaatia. Ainoana "vika", ettei kamera oikein sovellu valvonta-kameraksi infrapunan puuttumisen takia	9+, Vvlvontakameraksi todella kilpailu-kykyinen hintainen, tarjoaa hyvät säätö-ominaisuudet, tarkkuus ja laatu tarjoavat monipuolisen kokonaisuuden.

Tuloksista voidaan päätellä, että halvan (Linksys) ja keskihintaisen kameran (Intellinet) kokonaisero on kohtuullisen pieni. Kuitenkin, jos kameraa ajatellaan sopivaksi valvontakäyttöön, vaatimukseen päästään vasta Intellinetin kamerassa. Infrapuna on vaatimus, että pimeässäkin voidaan nähdä selkeää kuvaa. Linksys kuitenkin soveltuu muuten kaikkiin muihin suoratoiston sovelluksiin, joita myös tietokoneisiin

kytkettävätkin kamerat tukevat. Toisaalta Linksyssä voidaan käyttää valvonta-kameraakin, mutta sen käyttö rajoittuisi luonnon- tai keinovalaistuihin tiloihin. Voidaan myös todeta, että valvontakameroissa hyvänä asiana on WLAN-tuki, jolloin voidaan päästä ylimääräisistä johdoista eroon. Toisaalta Intellinet-kameran PoE (Power over Ethernet, PoE) menettää WLAN-tapauksessa etua, koska langattomassa käytössä sen tulisi kuitenkin saada virtaa joko adapterin tai Ethernetin kautta. Lisäksi Intellinet-kamerassa Linksysiin verrattuna on hieman kehittyneempi hallintasovellus ja muutenkin enemmän ominaisuuksia. Kamera tarjoaa myös kuvankoon muutokset ja mikrofonin aktivoinin nauhoitustoiminnot jo katselutilassa. Tallennetut videoleikkeet voidaan tallentaa suoraan tai verkossa kytköksessä olevaan isäntäkoneeseen. Liikkeen-tunnistimen muutokset voidaan nähdä myös verkossa. Muita verkkomedian mittauksia esitetään liitteessä 6.

11 Toimipaikkojen välisten verkkopalvelujen välittäminen

Seuraavaksi visioin kuvassa 39, miten IPTV voisi tuoda Metropolian Leppävaaran toimipisteeseen jo olemassa olevan Bulevardin IPTV-palvelun ja päinvastoin sovellukset Bulevardille Leppävaarasta laboratorioympäristöstä.



Kuva 27. Kytkentäesimerkki toimipaikkojen välisestä palvelujen välityksestä

Ajatellaan, että palvelun tarjonta olisi kahdensuuntaista. Tämä auttaisi ensinnäkin siihen, että opiskelijoiden ei tarvitsi välttämättä hakeutua tiettyyn toimipaikkaan päästäkseen tekemään harjoituksia tai liittymään tarjottuun oppimateriaaliin.

Molemmissa toimipaikoissa olisi oma palvelin, joka olisi kiinni enimmäkseen laboratorioympäristössä ja myös sen käyttäjäryhmä. Kuitenkin molemmissa toimipaikoissa olisi mahdollisuus päästä palvelimeen langattomasti itse toimipaikalla. Jos haluttaisiin viedä kyseiset palvelut tuotantoverkkoon saakka, tarvittaisiin myös oma reititys.

Multicast VRF:ää voitaisiin käyttää siten, että vain aluksi ryhmälähetys-liikenne rajoittuisi tiettyyn osaan verkkoa, kuten toimipaikkojen väliseen laboratorio-ympäristöön. Toinen idea olisi myös tuoda valvontakamerajärjestelmä yli tuotantoverkon, jonka jälkeen sitä voidaan tarkastella tietyissä koneissa.

Jos tulevaisuudessa muidenkin toimipaikkojen välille tulisi omia yhteyksiä, VRF:n voisi soluttaa ympäri verkkoa. Toinen vaihtoehto olisi hyödyntää julkista verkkoa käyttämällä VPN-yhteyksiä.

12 Yhteenveto

Tämän insinöörityön tarkoitus on käsitellä ryhmälähetystekniikkaa ja siihen liittyviä sovelluksia. Ryhmälähetystiedonsiirto perustuu pieneen mediakaistan käyttöön eli liikennettä tulee vain sinne, mitkä isäntäkoneet sitä haluavat. Runkoverkon kannalta ryhmälähetys on ideallinen, koska se ei vie resursseja kuten täsmälähetykseen pohjautuvat multimediaverkot. Ryhmälähetys on yhteensopiva useiden protokollien kanssa, mutta MOSPF ja PIM ovat yleisimmin käytetyt reititysprotokollat paikallisissa verkoissa. [16.] Myös IGMP-protokollaa käytetään IPv4-pohjaisissa lähiverkoissa. [16.]

Ryhmälähetys mahdollistaa uusien sovelluksien, kuten live-opetuksen, IPTV:n ja valvontakameraympäristön käytön runkoverkossa. Palveluina voisi myös ajatella sisäistä TV-järjestelmää, josta tulisi ajankohtaista opetusohjelmaa. Ryhmälähetys on hyvin sulautuva runkoverkkoon, koska sillä voidaan ohjata VRF-tekniikan avulla liikenne paljon suppeampaan sektoriin verkossa, jolloin tärkeät verkon solmupisteet eivät kuormitu entisestään.

Suurin lisäys ryhmälähetykseen on VRF tekniikka, joka mahdollistaa liikenteen ohjautumaan virtuaalisesti toiseen reititystauluun, josta se reititetään omana liikenteenä. Multicast VRF ei kuitenkaan tuo tietoturvaa toisaalta, mutta siitä huolimatta multicast VRF parantaa runkoverkon huoltamista ja ylläpitoa. Pelkästään dynaamisen reitityksen osalta ja reitittimien linkkimäärän laskemalla, reitityksessä ei tule huomioon sitä, mitä muuta liikennettä siellä menee. Näin ollen, kun liikenne siirtyy muun muassa laitevian takia toiseen reititykseen, niin VRF:llä voidaan tehdä määrätty reititys pisteiden välille. Tällöin voidaan ennaltaehkäistä turha kuormitus sellaiselta sektorilta, jossa on vapaampaa kaistaa.

Ryhmälähetystekniikan käyttö on voimakkaassa kasvussa, ja se tulee kehittymään, koska lähes koko ajan pystytetään uusia verkossa olevia IPTV:eitä. Vielä, kun otetaan laiteresurssit ja tarvittavat verkkokaistojen optimointi huomioon, ryhmälähetys on lähes pakollinen. Toisaalta vaikka tietoverkkojen kaistat kasvavat kokoajan suuremmiksi, ryhmälähetyksen osuus tulee olemaan suhteellisen pieni tiedon kokonaismäärästä.

VLC-mediasoitin tuli todetuksi hyvin sopivaksi ratkaisuksi, ja se tarjoaa paljon ominaisuuksia mediantoistoon. VLC-mediasoitimella erilaisten suoratoistojen alustaminen oli vaivatonta. SAP-mainoksien näkyminen on tärkeää, koska sen avulla informoidaan käyttäjää olemassaolevista ryhmälähetys- tai muusta vastaavista multimedia suoratoistoista. Web-kameroiden suoratoisto tarjoaa erilaisia sovelluksia. Uskon, että ryhmälähetyksen avulla suoratoistamalla apuna käyttäen web-kameroita voidaan monipuolistaa nykyisiä olemassa olevia opetus-, mainonta- ja valvonta-ympäristöjä.

Tämän opinnäytetyöhön tavoitteet täyttyivät hyvin ja siihen liittyvät ryhmälähetys, VRF-tekniikka ja niiden sovelluksien mahdollisuudet tulivat todella opittua ja sisäistettyä. Opinnäytetyö antaa vahvaa osaamista ja tuntemusta kyseiseen aiheeseen, ja pidän hyvin tärkeänä tätä tietoa ja taitoa myös työmarkkinoilla.

Testiympäristössä lopputulos oli erittäin tyydyttävä, vaikka hieman ongelmia syntyi. Työni eteneminen oli sujuvaa ja ryhmälähetysliikenne toimi vaivattomasti. Ryhmälähetys antaisi vielä tuleville ja nyt opiskeleville mahdollisuuden jatkaa tätä pohjusta. Aiheiksi voisi kelvata muun muassa IPv6-toteutus tai ei-multimediapohjaiset ryhmälähetyssovellukset. Myös VPN- ja MPLS-tekniikkaa tulisi miettiä luotettavuuden lisäämisen kannalta ja lopuksi, miten WLAN-liikenteestä saataisiin kaikki irti.

Tästä opinnäytetyön sisällöstä voisi olla hyötyä opiskelijoille, jotka haluavat suuntautua tietoverkkoihin, koska ryhmälähetyksen ymmärtäminen on tärkeää. Suoratoisto-pohjaisten esimerkkisovelluksien kautta ryhmälähetystekniiikka voi tulla opituksi tehokkaammin, koska opiskelija saa hyvin käytännönläheisen tiedon siitä, kuinka hallita ja suunnitella ryhmälähetysverkkoa.

Lähteet

1 Internet Group Management Protocol. (WWW.-dokumentti.) Wikipedia. http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol. Luettu 14.8.2009.

2 IGMP: Internet Group Management Protocol Overview (IGMPv1, IGMPv2 and IGMPv3). (WWW-dokumentti) Javvin Technologies, Inc. http://www.javvin.com/protocolIGMP.html. Luettu 16.8.2009.

3 Fenner, W. RFC 2236. Internet Group Management Protocol Version 2. (WWW-dokumentti.) IETF. 1997. http://www.ietf.org/rfc/rfc2236.txt. Luettu 20.8.2009

4 Christensen, M. RFC 4541. Considerations for Internet Group Management Protocol (IGMP) and Ryhmälähetys Listener Discovery (MLD) Snooping Switches. (WWW-dokumentti.) IETF. 2006. http://tools.ietf.org/html/rfc4541. Luettu 23.9.2009.

5 Kaario, Kimmo. TCP/IP-verkot. Jyväskylä. Docendo. 2002.

6 Schulzrinne, H. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. (WWW-dokumentti.) IETF. 2003 http://tools.ietf.org/html/rfc3550. Luettu 2.9.2009.

7 Handley, M. & Jacobson, V. RFC 2327. SDP: Session Description Protocol. (WWW-dokumentti.) IETF. 1998. http://tools.ietf.org/html/rfc2327. Luettu 8.9.2009.

8 SAP (v1 & v2): Session Announcement Protocol. (WWW-dokumentti.) Javvin Technologies, Inc. http://www.javvin.com/protocolSAP.html. Luettu 15.9.2009.

9 Fielding, R. RFC 2616. Hypertext Transfer Protocol -- HTTP/1.1. (WWW-dokumentti.) IETF. 1999. http://tools.ietf.org/html/rfc2616. Luettu 18.9.2009.

10 Virtuaalilähiverkko. (WWW-dokumentti.) Wikipedia. http://fi.wikipedia.org/wiki/VLAN. Luettu 18.9.2009.

11 Introduction to Cisco MPLS VPN Technology. (WWW-dokumentti.) Cisco Systems. http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html. Luettu 15.10.2009.

12 CCIE SP Mini-Scenarios. (WWW-dokumentti.) Netzone. http://ccie18473.net/dynamips/dynamips.htm. Luettu 14.4.2010

13 OSPF Support for Multi-VRF on CE Routers. (WWW-dokumentti.) Cisco Systems Inc. http://www.cisco.com/en/US/docs/ios/12_0st/12_0st21/feature/guide/ospfvrfl.html. Luetttu 19.10.2009

14 Virtualisointi. (WWW-dokumentti.) Wikipedia. http://fi.wikipedia.org/wiki/Virtualisointi. Luettu 18.9.2009

15 Network virtualization. (WWW-dokumentti.) Wikipedia. http://en.wikipedia.org/wiki/Network_virtualization. Luettu 1.4.2010.

16 Quinn, B. RFC 3170. IP Ryhmälähetys Applications: Challenges and Solutions. (WWW-dokumentti.) IETF. 2003. http://tools.ietf.org/html/rfc3170. Luettu 2.10.2009

17 Ryhmälähetys. (WWW-dokumentti.) Wikipedia. http://en.wikipedia.org/wiki/Ryhmälähetys. Luettu 29.11.2009.

18. Overview of IP Ryhmälähetys (WWW-dokumentti).. Cisco Systems, Inc. http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00 80092942.shtml. Luettu 11.11.2009

19 Stevens, W. RFC 2001. TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms.(WWW-dokumentti.) IETF. 1997 http://www.ietf.org/rfc/rfc2001.txt?number=2001.Luettu 13.11.2009.

20 Quinn, B. RFC 3170. IP Ryhmälähetys Applications: Challenges and Solutions. (WWW-dokumentti.) IETF. 2001.http://www.ietf.org/rfc/rfc3170.txt?number=3170. 15.11.2009.

21 Tieteen tietotekniikan keskus CSC:n WWW-sivut. (WWW-dokumentti.). Funet. http://www.csc.fi/hallinto/funet/palvelut/dns/ficora. Luettu 26.11.2009.

22 Internet Ryhmälähetys Addresses. (WWW-dokumentti.) IETF. 2010. http://www.iana.org/assignments/ryhmälähetys-addresses. Luettu 13.4.2010

23 Albanna, Z. RFC 3171. IANA Guidelines for IPv4 Ryhmälähetys Address Assignments. (WWW-dokumentti.) IETF. 2001. http://www.ietf.org/rfc/rfc3171.txt?number=3171.Luettu 28.11. 2009.

24 Cisco IOS IP Ryhmälähetys Configuration Guide. (WWW-dokumentti.) Cisco systems Inc. 2008. https://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/12_4/imc_12_4_bo ok.pdf. Luettu 7.12.2009.

25 Celtdra, A. BSCI: IP Ryhmälähetys – PIM Routing Protocol. (WWW-dokumentti.) Route my world!. http://routemyworld.com/2009/01/22/bsci-ip-ryhmälähetys-pim-routing-protocol/. Luettu 18.12.2009.

26 Schulzrinne, H. Computer Science at Columbia University. Ryhmälähetys. (WWW-dokumentti.) http://www.cs.columbia.edu/~hgs/internet/ryhmälähetys.html. Luettu 19.12.2009..

27 Bhagat, A. Route Distinguisher & its types. (WWW-dokumentti.) Amit's Cisco Zone. http://sites.google.com/site/amitsciscozone/home/important-tips/mpls-wiki/route-distinguisher-its-types. Luettu 20.4.2010.

28 Darwin Streaming Server. (WWW-dokumentti.) Wikipedia. http://en.wikipedia.org/wiki/Darwin_Streaming_Server. Luettu 15.9.2009.

29 VideoLAN Streaming. (WWW-dokumentti.) VideoLAN. http://www.videolan.org/vlc/streaming.html. Luettu 20.9.2009.

30 Payne, M. What is the Maximum Length of a USB Cable?. (WWW-dokumentti.) eHow. http://www.ehow.com/about_5365028_maximum-length-usb-cable.html. Luettu 13.4.2010.

Liite 1: SAP-mainostukset Ciscon reitittimessä

Seuraavaksi tarkkaillaan esimerkkijärjestelmän tapauksessa käytettyjä SAP-mainoksia Ciscon reitittimessä.

```
R1#sh ip sap
SAP Cache - 3 entries
  Nightmare On Elm Street Trailer
  Ron Hextall Tribute Video
  RTSP Server - Linksys

R1#sh ip sap detail
SAP Cache - 3 entries
Session Name: Nightmare On Elm Street Trailer
  Description: N/A
  Group: 239.255.100.101, ttl: 255, Contiguous allocation: 0
  Uptime: 00:04:43, Last Heard: 00:00:03
  Announcement source: 10.0.10.100, destination: 239.255.255.255
  Created by: - 14947803663558281203 14947803663558281203 IN IP4 jonil-desktop
  Phone number:
  Email:
  URL:
  Media: video 5010 RTP/AVP 33
    Attribute: rtpmap:33 MP2T/90000

Session Name: Ron Hextall Tribute Video
  Description: N/A
  Group: 239.255.100.100, ttl: 255, Contiguous allocation: 0
  Uptime: 00:04:45, Last Heard: 00:00:03
  Announcement source: 10.0.10.100, destination: 239.255.255.255
  Created by: - 14947803324328939401 14947803324328939401 IN IP4 jonil-desktop
  Phone number:
  Email:
```

URL:
Media: video 5000 RTP/AVP 33
Attribute: rtpmap:33 MP2T/90000

Session Name: RTSP Server - Linksys
Description:
Group: 0.0.0.0, ttl: 0, Contiguous allocation: 0
Uptime: 00:10:40, Last Heard: 00:00:03
Announcement source: 10.0.90.100, destination: 224.2.127.254
Created by: - 000034107245104177 15324 IN IP4 10.0.90.100
Phone number:
Email:
URL:
Media: video 5100 RTP/AVP 96
Media group: 239.255.100.1, ttl: 32
Attribute: rtpmap:96 MP4V-ES/30000
Attribute: control:trackID=1
Attribute: fmtp:96 profile-level-id=1;
config=000001B001000001B509000001000000012000845D4C28A021E0A31F;decod
e_buf=76800
Attribute: x-framerate:30
Attribute: framerate:30.0
Media: audio 5102 RTP/AVP 97
Media group: 239.255.100.1, ttl: 32
Attribute: rtpmap:97 G726-16/8000/1
Attribute: control:trackID=2
Attribute: ptime:125

Yhteenvetona voidaan sanoa, että Ciscon reititin näkee lähestulkoon kaiken tiedon SAP-mainostuksien sisällöstä. Sieltä nähdään mm. lähettäjän osoite, ryhmälähetys-ryhmäosoite, RTP-porttinumerot ja kuinka kauan lähetys on ollut voimassa. Myös muitakin tietueita on nähtävissä. Joten kokonaisuudessaan Ciscon reitittimessä olevalla

SAP-viestien käsittelyllä saadaan kattava tietomäärä SAP-mainoksien sisällöstä. Kuitenkaan sitä Ciscon reititin ei kerro minkälainen todellinen kuvanlaatu kyseisillä suoratoistoilla, vaikka siinä mainitaankin käytetty videoformaatti.

Liite 2: Ryhmälähetys-konfiguraatiot Ciscon reittimessä

```
hostname R1
!
ip ryhmälähetys-routing
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.0.1.1 255.255.255.0
 clock rate 2000000
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.0.1.0 0.0.0.255 area 0
```

```
 network 10.0.2.0 0.0.0.255 area 0
!
end


hostname R2
!
ip ryhmälähetys-routing
!
interface FastEthernet0/0
 ip address 10.0.11.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.0.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
!
interface Serial0/1
 ip address 10.0.20.1 255.255.255.0
 clock rate 2000000
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
!
interface FastEthernet0/1
 ip address 10.0.12.1 255.255.255.0
```

```
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.12.0 0.0.0.255 area 0
!
end

hostname R3
!
ip ryhmälähetys-routing
!
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.30.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
```

```
 speed auto
!
interface Serial0/0
 ip address 10.0.20.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.0.2.0 0.0.0.255 area 0
 network 10.0.31.0 0.0.0.255 area 0
!
end

hostname R4
!
ip ryhmälähetys-routing
!
interface FastEthernet0/0
 ip address 10.0.11.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.40.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
```

```
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.40.0 0.0.0.255 area 0
!
end

hostname R5
!
ip ryhmälähetys-routing
!
interface FastEthernet0/0
 ip address 10.0.12.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.50.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
 no shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
```

```
 network 10.0.12.0 0.0.0.255 area 0
 network 10.0.50.0 0.0.0.255 area 0
!
end
```

Liite 3: Ryhmälähetys VRF-konfiguraatiot Ciscon reittimessä

```
hostname R1
!
ip cef
!
ip vrf VLC
 rd 100:100
 route-target import 100:100
 route-target export 100:100
!
ip ryhmälähetys-routing
ip ryhmälähetys-routing vrf VLC
!
interface Loopback1
 ip vrf forwarding VLC
 ip address 10.0.100.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0.2
```

```
 encapsulation dot1Q 10
 ip vrf forwarding VLC
 ip address 10.0.10.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
 encapsulation dot1Q 100
 ip vrf forwarding VLC
 ip address 10.0.20.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.3
 encapsulation dot1Q 200
 ip vrf forwarding VLC
 ip address 10.0.30.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
```

```
router ospf 100 vrf VLC
 log-adjacency-changes
 network 10.0.10.0 0.0.0.255 area 0
 network 10.0.20.0 0.0.0.255 area 0
 network 10.0.30.0 0.0.0.255 area 0
 network 10.0.40.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 capability vrf-lite
!
router ospf 1
 log-adjacency-changes
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.2.0 0.0.0.255 area 0
!
end

hostname R2
!
ip cef
!
ip vrf VLC
 rd 100:100
!
ip ryhmälähetys-routing
ip ryhmälähetys-routing vrf VLC
!
interface Loopback1
 ip vrf forwarding VLC
 ip address 10.0.100.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
```

```
interface FastEthernet0/0
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.2.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0.2
 encapsulation dot1Q 100
 ip vrf forwarding VLC
 ip address 10.0.20.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.3.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
```

```
 encapsulation dot1Q 300
 ip vrf forwarding VLC
 ip address 10.0.50.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.3
 encapsulation dot1Q 900
 ip vrf forwarding VLC
 ip address 10.0.220.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
router ospf 100 vrf VLC
 log-adjacency-changes
 network 10.0.20.0 0.0.0.255 area 0
 network 10.0.40.0 0.0.0.255 area 0
 network 10.0.50.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.220.0 0.0.0.255 area 0
 capability vrf-lite
!
router ospf 1
 log-adjacency-changes
 network 10.0.2.0 0.0.0.255 area 0
 network 10.0.3.0 0.0.0.255 area 0
!
end

hostname R3
!
ip cef
```

```
!
ip vrf VLC
 rd 100:100
!
ip ryhmälähetys-routing
ip ryhmälähetys-routing vrf VLC
!
interface Loopback1
 ip vrf forwarding VLC
 ip address 10.0.100.3 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.2.3 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0.3
 encapsulation dot1Q 200
 ip vrf forwarding VLC
 ip address 10.0.30.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
```

```
interface FastEthernet0/1
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.4.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
 encapsulation dot1Q 00
 ip vrf forwarding VLC
 ip address 10.0.60.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.3
 encapsulation dot1Q 800
 ip vrf forwarding VLC
 ip address 10.0.230.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
router ospf 100 vrf VLC
 log-adjacency-changes
 network 10.0.30.0 0.0.0.255 area 0
 network 10.0.60.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.230.0 0.0.0.255 area 0
```

```
 capability vrf-lite
!
router ospf 1
 log-adjacency-changes
 network 10.0.2.0 0.0.0.255 area 0
 network 10.0.4.0 0.0.0.255 area 0
!
end

hostname R4
!
ip cef
!
ip vrf VLC
 rd 100:100
!
ip ryhmälähetys-routing
ip ryhmälähetys-routing vrf VLC
!
interface Loopback1
 ip vrf forwarding VLC
 ip address 10.0.100.4 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
```

```
 encapsulation dot1Q 1 native
 ip address 10.0.3.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0.2
 encapsulation dot1Q 300
 ip vrf forwarding VLC
 ip address 10.0.50.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.3
 encapsulation dot1Q 800
 ip vrf forwarding VLC
 ip address 10.0.230.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.5.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
```

```
 encapsulation dot1Q 70
 ip vrf forwarding VLC
 ip address 10.0.70.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
router ospf 100 vrf VLC
 log-adjacency-changes
 network 10.0.50.0 0.0.0.255 area 0
 network 10.0.70.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.230.0 0.0.0.255 area 0
 capability vrf-lite
!
router ospf 1
 log-adjacency-changes
 network 10.0.3.0 0.0.0.255 area 0
 network 10.0.5.0 0.0.0.255 area 0
!
End

hostname R5
!
ip cef
!
ip vrf VLC
 rd 100:100
!
ip ryhmälähetys-routing
ip ryhmälähetys-routing vrf VLC
!
interface Loopback1
```

```
 ip vrf forwarding VLC
 ip address 10.0.100.5 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.4.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/0.2
 encapsulation dot1Q 400
 ip vrf forwarding VLC
 ip address 10.0.60.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
 encapsulation dot1Q 900
 ip vrf forwarding VLC
 ip address 10.0.220.2 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1
```

```
 no shutdown
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.6.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
interface FastEthernet0/1.2
 encapsulation dot1Q 80
 ip vrf forwarding VLC
 ip address 10.0.80.1 255.255.255.0
 ip pim sparse-dense-mode
 ip sap listen
!
router ospf 100 vrf VLC
 log-adjacency-changes
 network 10.0.60.0 0.0.0.255 area 0
 network 10.0.80.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.220.0 0.0.0.255 area 0
 capability vrf-lite
!
router ospf 1
 log-adjacency-changes
 network 10.0.4.0 0.0.0.255 area 0
 network 10.0.6.0 0.0.0.255 area 0
!
End
```

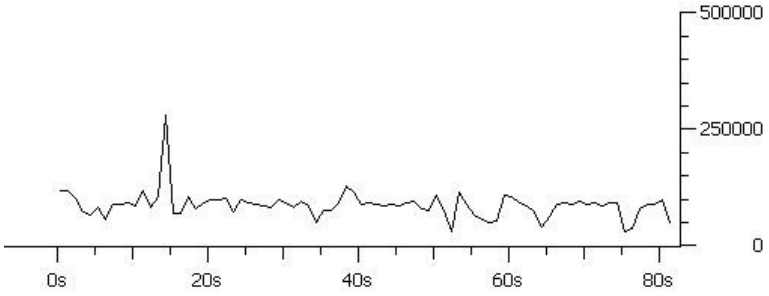
```
hostname SW1
!
interface FastEthernet0/1
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 100-200
!
interface FastEthernet0/2
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 100
!
interface FastEthernet0/3
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 200
!
interface FastEthernet0/4
!
interface FastEthernet0/5
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 300
 switchport trunk allowed vlan add 900
!
interface FastEthernet0/6
 switchport mode trunk
```

```
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 400
 switchport trunk allowed vlan add 800
!
interface FastEthernet0/7
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 300
 switchport trunk allowed vlan add 800
!
interface FastEthernet0/8
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 400
 switchport trunk allowed vlan add 900
!
interface FastEthernet0/9
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 10
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport mode access
 switchport access vlan dynamic
```

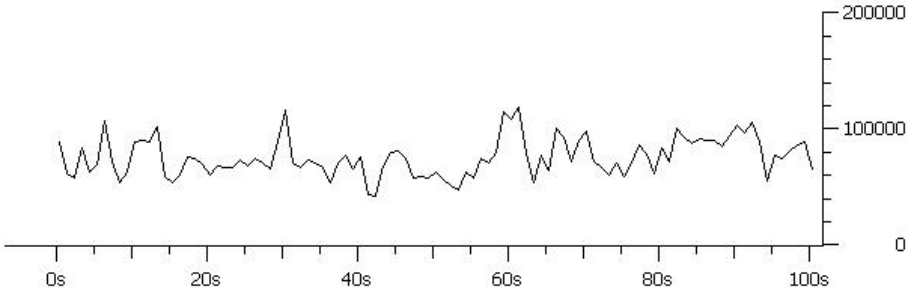
```
!
interface FastEthernet0/12
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan remove 2-1005
 switchport trunk allowed vlan add 70
!
interface FastEthernet0/13
 switchport access vlan 70
 switchport mode access
!
monitor session 1 source interface Fa0/15
monitor session 1 destination interface Fa0/24
!
end
```

Liite 4: Suoratoiston mittaustuloksia

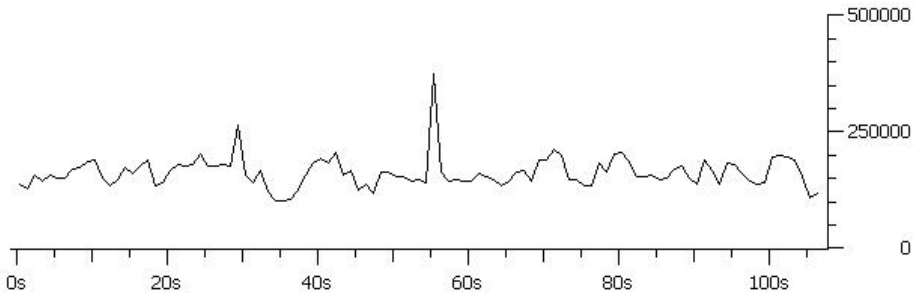
Seuraavat mittaukset on tehty Wireshark-analysaattorilla, jolla voidaan tutkia erilaisten verkkopakettien sisältöä ja mm. tehdä niistä kuvaajia. Seuraavaksi käydään neljä erilaista kuvaa läpi. Kuva 28 esittää esikäsiteltyä MPEG2-formaatia suoratoistettuna. Kuva 29 esitetään MPEG4-formaatissa olevaa suoratoistoa, jota ei ole esikäsitelty. Kuva 30 katsotaan mitä kaksi edellä mainittua suoratoistoa vievät verkkokaistaa yhteensä jolloin tulee todistetuksi ryhmälähetys-liikenne. Tärkeä tekijä tässä on, että suoratoistoa seuraa yhtä aikaa 2 isäntäkonetta. Kuva 31 kuvaa VRF tuoman viasta palautumisen. Lyhyempi katkos ei kuvaa VRF:än toiminnallisuutta vaan suoratoisto loppui ja alkoi uudestaan niin siitä tulee vain ns. lähetyksen katko. Kaikissa edellamainituissa kuvissa pystyakselin laatuna on tavu (byte).



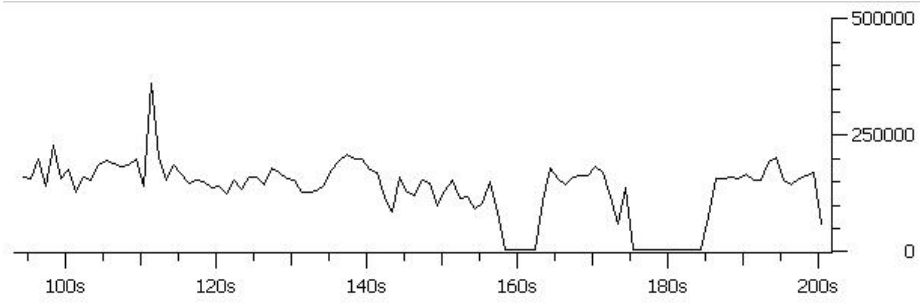
Kuva 28. Esikäsitetyllä MPEG2-formaattilla tehty suoratoisto



Kuva 29. Ei-esikäsitetyllä MPEG4-formaatilla tehty suoratoisto



Kuva 30. Edeltävät kaksi suoratoistoa yhtäaikaisesti



Kuva 31.VRF:än näkyminen suoratoistossa

Yhteenvetona näistä voin sanoa, että ryhmälähetys toimii moitteettomasti. Myös verkkoresurssien tarve kyseisillä videoformaateilla ei ole kovin suuri. Kuitenkin HD-videokuvaa (High-definition) suoratoistettaisiin niin kaistan määrä luonnollisesti nousisi tuntuvasti. Myös VRF-näkeminen toiminnassaan on tästä helppo nähdä. VRF:än viasta palautumisen toiminnallisuus on parhaiten nähtävissä mahdollisimman lähellä isäntäkonetta.

Liite 5: Telnet-liitännän määrittelyt

Telnet skriptitiedosto voi pitää sisällään useita kanavia, jotka käynnistetään yhtäaikaisesti. Skriptitiedostoa hallinnoidaan ihan tavallisella tekstieditorilla. Skrippitiedostoston sisältö on seuraavanlainen.

new channel1 broadcast enabled
setup channel1 input http://host.mydomain/movie.mpeg
setup channel1 output #rtp{mux=ts,dst=239.255.1.1,sap,name="Channel 1"}

new channel2 broadcast enabled
setup channel2 input rtp://@239.255.12.42
setup channel2 output #rtp{mux=ts,dst=239.255.1.2,sap,name="Channel 2"}

control channel1 play
control channel2 play

Jossa kanava jaotellaan tietynlaisina määrittelyinä. Kanavissa tulee mainita lähdemateriaalin sijainti ja sitten mihin tämä edelleen syötetään verkkoon. Lopuksi pitää olla kontrolli tietyssä tilassa kuten ”play” niin kanava toistuu. Kaikki asetukset kuvataan kuten komentopohjaisen käskyhierarkia ja siitä löytyy kattava dokumentointi VLC-kotisivuilta. Telnet-liitännän voi käynnistää graafisesti soittimen päävalikon kautta. Käynnistäminen voidaan myös tehdä komentokehotteeen kautta seuraavasti:

- **vlc--intf telnet**

Liite 6: Mosaic-esimerkin etenemismalli

Ajatellaan, että esimerkiksi 11 kanavaa on suoratoistossa, mutta 10 kanavaa olisi vain VOD-periaateella ja 1 kanavista näyttäisi ryhmälähetys:illa pienen ns. ennakkotarjonta videoleikkeen, mitä eri kanavalla esitetään. Siis tämä 1 kanava toimisi siis tällaisena mosaic-rajapinnan alla toimivana, joka toimisi vain kanava valitsimena.

Suoratoiston asetukset mosaic-rajapinalla on kaikesta erikoisuudesta huolimatta hyvin samankaltainen kuin muuutenkin suoratoiston käynnistäminen VLC mediasoittimella.

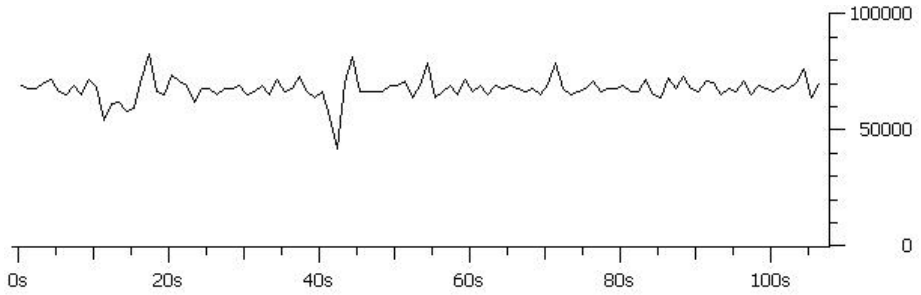
Poikkeuksellisena tehtävänä on tehdä ns. taustakuva. Kyseinen suoratoistokokoilma ikkunat tulostuvat kyseisen taustakuvan päälle halutussa kokooonpanossa. Sen jälkeen valitaan jälleen mitä halutaan suoratoistaan ja annetaan sille ikkunalle nimike. Nimike toimii ikäänkuin profiilina sille tietylle ikkunan suoratoistolle, johon sidotaan kaikki määritelmät

Seuraavaksi pitää tehdä profiili määrittelyt jotka ovat identtisiä kuten ihan tavallisena soittimessa tehtynä. Sitten luodaan suoratoistettavan median ryhmälähetys-osoite, enkapsulaointi ja SAP-määrittelyt. Asetuksien jälkeen niin tehdään tallennus kyseiseen profiiliin.

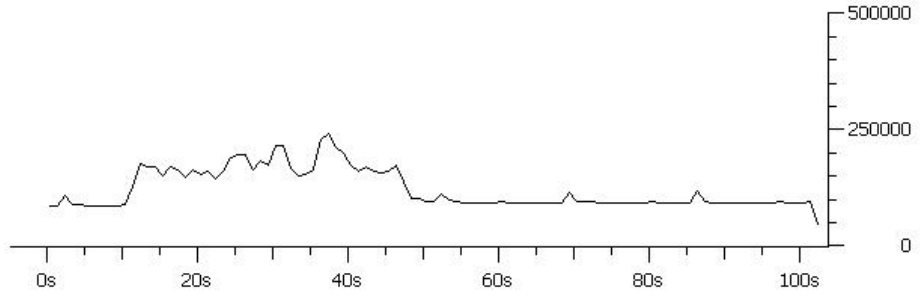
Profiileita Mosaic tapauksessa tulee useita, kun tarkoitus on tuota esiin useita erilaisia yhtäaikaisia mediantoistoja ruudulle. Kyseiset profiilit lopuksi liitetään tiettyihin ikkunoihin. Sen jälkeen suoratoisto voidaan käynnistää. Myös koko Mosaic-asetuksen saa samasta sivustosta ihan komentosarja-pohjaisenakin kopioitua varmuudeksi talteen.

Liite 7: Web-kameroiden mittaustuloksia

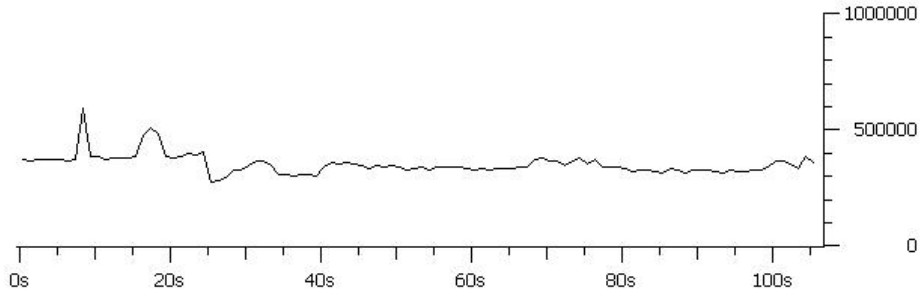
Seuraavat mittaukset on tehty Wireshark-analysaattorilla, jolla voidaan tutkia erilaisten verkkopakettien sisältöä ja mm. tehdä niistä kuvaajia. Seuraavaksi käydään neljä erilaista kuvaa läpi. Kuva 32 esittää Logitech QC 3000 Business-webkameralla tehtyä suoratoistoa. Kuva 33 esitetään Logitech QuickCam Sphere AF:an liikkeentunnistimen näkyminen suoratoistossa. Kuva 34 kuvaa mitä verkkopohjainen kamera Intellinet vie verkkokaistaa, kun sillä suoratoistetaan videota infrapunalla. Kaikissa edellamainituissa kuvissa pystyakselin laatuna on tavu (byte).



Kuva 32. Logitech QC 3000 Business-webkameralla tehtyä suoratoistoa



Kuva 33. Logitech QuickCam Sphere AF:an liikeentunnistimen näkyminen suoratoistossa



Kuva 34. Intellinet suoratoistaessa videota infrapunalla.

Yhteenvetona näistä voin sanoa, Logitech QC 3000 Business-webkamera vaatii hyvin pienen kaistan. Logitechin QuickCam Sphere AF muutos on nähtävissä aina siten, että kun kuvapisteiden muutos tapahtuu niin myös verkossa muuttuvien bittejen määrä kasvaa ja se nähdään suoraan kuvaajasta. Intellinet-webkamera vie suhteellisen paljon kaistaa infrapunaa käyttäessä. Sen käyttö vastaa samaa kuin Logitech kameroiden yhteensä tarvitsemaa verkkokaistaa.