Teemu Salo

IP-videon suoratoistoon optimoidun tietoliikenneverkon nopeuden päivitys ja testaus

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
19.5.2011

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Teemu Salo IP-videon suoratoistoon optimoidun tietoliikenneverkon nopeuden päivitys ja testaus 58 sivua + 3 liitettä 19.5.2011
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Ohjaajat	tekninen johtaja Pasi Makkonen yliopettaja Harri Ahola

Työssä päivitettiin Asiakas Oy:n kameravalvontajärjestelmä vastaamaan tulevaisuuden tarpeita. Koska tietoliikenneverkkoa käytetään pääasiassa IP-videon suoratoistoon, suunnittelussa haluttiin varmistua hankintojen ja suoritettavien toimenpiteiden tarkoituksenmukaisuudesta kameravalvontajärjestelmän käytettävyyden kannalta.

Työssä asennettiin kuusi HP A5800 -kytkintä sekä tehtiin tarvittavat asetukset ja vanhojen kytkinten vaihdossa vaaditut yliheitot. Työssä tutkittiin HP:n kytkimissä käytettäviä RRPP- ja IRF-tekniikoita (RRPP, Rapid Ring Protection Protocol; IRF, Intelligent Resilient Framework) ja niitä sovellettiin toteutuksessa. Työssä kuvataan myös IP-videon kannalta tärkeää ryhmälähetystoimintoa verkon suunnittelun näkökulmasta. RRPP-tekniikan testaamiseksi asennettiin kolmen kytkimen testirengas, ja verkon palautumista tutkittiin eri lähetysmenetelmillä. Lisäksi kamerajärjestelmän videoviive mitattiin kameroiden ohjattavuuden tutkimiseksi.

Työssä havaittiin, että RRPP-verkko palautui valmistajan antamien tietojen mukaisesti 50 ms:ssa. Ryhmälähetyksen palautuminen RRPP-renkaan katkoksen yhteydessä oli kuitenkin riippuvainen reitittimen PIM-Hello -viestien (PIM, Protocol Independent Multicast) lähetysvälistä. Eri verkkojen välillä mitattu HD 720p -videoviive asettui noin 200 ms:iin. Videoviive aiheutui pääasiallisesti videon H.264-enkoodauksesta ja -dekoodauksesta.

Työssä havaittiin, että verkon videoviiveen mittaamiseen käytetty menetelmä soveltui hyvin tarkoitukseensa. Toisaalta havaittiin myös, että parempia menetelmiä tulisi kehittää suurten datamäärien käsittelemiseen pakettikaappaustesteissä.

Avainsanat	IP-video, ryhmälähetys, RRPP, IRF

Helsinki Metropolia University of Applied Sciences **Abstract**

Author Title Number of Pages Date	Teemu Salo Upgrading and optimizing IP video network 62 (total number of pages including appendices) 19 May 2011
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Pasi Makkonen, Chief Technology Officer Harri Ahola, Principal Lecturer

The object of this thesis work was to upgrade Guest Ltd's camera surveillance network to meet future needs. Since the network is mainly used for streaming IP video, it was essential to ensure that the purchase and the upgrade process of the surveillance system's network components were appropriate in terms of usability.

The Intelligent Resilient Framework (IRF) and Rapid Ring Protection Protocol (RRPP) functionalities of HP switches were studied and the findings were implemented in the practical part of the work. The thesis also describes the multicast technique, which is an important feature of any IP video system, focusing on practical network design considerations.

Six HP A5800 switches were installed and the necessary configurations were made as well as the required switch-overs during the exchange process. A 10 Gbit/s backbone was installed to accommodate future growth. Also a three node RRPP test ring was built and network convergence was studied using different delivery methods. In addition, the video latency of the system was measured to ensure proper usability during PTZ (Pan Tilt Zoom) camera control.

During the tests it was observed that the RRPP network converged within 50 ms after link failure. However, since RRPP did not cause multicast flood during topology change, multicast convergence was dependent on the router's PIM Hello message interval. The measured video latency settled around 200 ms while streaming HD 720p video. Video latency was mainly caused by encoding and decoding H.264.

Keywords	IP CCTV, multicast, IRF, RRPP

Sisällys

Lyhenteet

10GbE	*10-Gigabit Ethernet*. Ethernet yhteys, jonka nopeus on 10 Gbit/s.
ACL	*Access Control List*. Pääsylista.
BPDU	*Bridge Protocol Data Unit*. STP:n käyttämä sanomarakenne.
CAT6	*Category 6*. Yleiskaapeloinnin kaapeli- ja liitinkategoria 6.
DVMRP	*Distance Vector Multicast Routing Protocol*. Ryhmälähetyksen reitityksessä käytettävä protokolla, jota myös kytkimet kuuntelevat multicast-reititinportin tunnistamiseen.
DVR	*Digital Video Recorder*. Tallennin, joka muuntaa analogisen videon digitaaliseksi sekä enkoodaa ja tallentaa sen.
GRE	*Generic Routing Encapsulation*. Tunnelointiprotokolla, joka tukee mm. ryhmälähetystä.
HD	*High Definition*. Teräväpiirtotekniikka.
IANA	*Internet Assigned Numbers Authority*. IP-osoitteistuksesta vastaava järjestö.
ICMP	*Internet Control Message Protocol*. Tietoliikenneverkon ongelmien raportointiin ja diagnosointiin käytettävä protokolla.
IEEE	*Institute of Electrical and Electronics Engineers*. Kansainvälinen tekniikan alan järjestö, joka mm. laatii standardeja.
IETF	*Internet Engineering Task Force*. Laatii RFC-dokumentteja Internet-protokollien standardoimiseen.
IGMP	*Internet Group Management Protocol*. Ryhmiin liittymiseen käytettävä protokolla.
IP	*Internet Protocol*. Internetin yhteyskäytäntö.
IPv6	*Internet Protocol version 6*. Uusi versio IP-protokollasta.
IPsec	*IP security*. Tekniikka Internet-yhteyksien suojaamiseen.
IRF	*Intelligent Resilient Framework*. HP:n kytkimissä käytettävä virtualisointitekniikka.
LAN	*Local Area Network*. Lähiverkko.

LACP	*Link Aggregation Control Protocol*. IEEE 802.3ad standardin määrittelemä kytkentöjen kahdentamiseen ja kuorman jakamiseen käytettävä protokolla.
MAC	*Media Access Control*. IEEE 802-verkoissa verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä, joka toimii siirtokerroksen yhteydessä.
MTBF	*Mean Time Between Failures*. Laitteiden vikatiheyttä kuvaava arvo.
NVR	*Network Video Recorder*. Tallennin, joka tallentaa enkoodattua videota tietoliikenneverkosta.
OM3	*Optical Multimode 3*. ISO/IEC 11801 Ed 2.1:2009 standardissa määritelty monimuotokuitu 10 Gbit/s -yhteyksiin.
OSPF	*Open Shortest Path First*. Sisäinen reititysprotokolla, joka käyttää Dijkstran algoritmia optimaalisimman reitin löytämiseen.
PIM	*Protocol Independent Multicast*. Ryhmälähetyksen reititykseen käytettävä protokolla.
QoS	*Quality of Service*. Palvelunlaatu. Tietoliikenteen luokitteluun käytettävä tekniikka.
RADIUS	*Remote Access Dial-In User Service.* Autentikointiprotokolla, joka toimii autentikointipalvelimessa.
RFC	*Request for Comments*. RFC-dokumentit ovat asiakirjoja, jotka määrittelevät Internetin yhteyskäytäntöjä.
RGMP	*Router-Port Group Management Protocol*. Ciscon protokolla, jolla pyritään välttämään ryhmälähetysliikenteen leviäminen kytkimen reititinporttiin.
RIP	*Routing Information Protocol*. Yksinkertaisin sisäinen reititysprotokolla.
RPF	*Reverse Path Forwarding*. Ryhmälähetyksen reitityksessä käytettävä protokolla.
RRPP	*Rapid Ring Protection Protocol*. HP:n kytkimissä käytettävä rengasverkkotekniikka.
RRPPDU	*Rapid Ring Protection Protocol Data Unit.* RRPP:n käyttämä sanomarakenne.
RTCP	*Real-time Transport Control Protocol*. RTP-yhteyden signalointiin käytettävä protokolla.

RTP	*Real Time Protocol*. Reaaliaikaisen datan siirtoon käytettävä yhteyskerroksen protokolla.
SD	*Standard Definition*. Tavallinen tarkkuus televisio-ohjelmissa.
SFP	*Small Formfactor Pluggable*. Modulaarinen Ethernet-portti.
SMS	*Short Message Service*. Matkapuhelinten lyhytviestipalvelu.
SNMP	*Simple Network Management Protocol*. Tietoliikenneverkon komponenttien monitoroimiseen ja hallintaan käytettävä protokolla.
SSH	*Secure Shell*. Salaava tiedonsiirtoprotokolla, jota käytetään erityisesti pääteyhteyksien salaamiseen.
STP	*Spanning Tree Protocol*. Virityspuualgoritmi verkon silmukoiden estämiseksi.
TCP	*Transmission Control Protocol*. Yhteydellinen kuljetuskerroksen protokolla.
TFTP	*Trivial File Transfer Protocol*. Yksinkertainen protokolla tiedostojen siirtoon tietoliikenneverkossa.
UDP	*User Datagram Protocol*. Yhteydetön kuljetuskerroksen protokolla.
UPS	*Uninterruptible Power Supply*. Varavirtalähde lyhyiden sähkökatkoksien varalle.
VLAN	*Virtual Local Area Network*. Virtuaalinen lähiverkko.
VPN	*Virtual Private Network*. Tekniikka organisaation eri toimipisteiden verkkojen turvalliseen yhdistämiseen Internet-yhteydellä.
WAN	*Wide Area Network*. Laajaverkko.

1 Johdanto

Tarve kameravalvonnan lisäämiselle kasvaa jatkuvasti rikollisuuden ja omaisuuteen kohdistuvan ilkivallan lisääntyessä sekä väkivallan uhan kasvaessa. Myös järjestyksenvalvojien ja yritysten henkilökunnan oikeusturvan kannalta on tärkeää, että saatavilla on hyvälaatuista kameravalvontajärjestelmän tuottamaa tallennekuvaa todellisen tapahtumakulun osoittamiseksi ristiriitatilanteissa. Ei ole ennenkuulumatonta, että rikollista taustaa omaava henkilö tekee saamastaan kohtelusta perättömän ilmiannon poliisille. Onkin tärkeää saada tallennettua paitsi itse rikos, myös koko tapahtumaketju sisältäen epäillyn kiinnioton ja kuljetuksen aina poliisin saapumiseen asti.

IP-pohjaisen (IP, Internet Protocol) kameravalvontatekniikan kehittyminen on osaltaan vastannut kameravalvonnan muuttuviin tarpeisiin ja lisääntyneisiin laatuvaatimuksiin. Yhä useammin tallennetaan sujuvaa kuvaa jollakin teräväpiirtotarkkuudella (HD, High Definition), esimerkiksi 25 kuvaa sekunnissa HD 720p -tarkkuudella. Teräväpiirtotarkkuuksiin siirrytään, sillä kuvan vaakajuovien lisäämisellä ja lomittamattomalla kuvalla saadaan laadukkaampaa pysäytyskuvaa kuin vähitellen käytöstä poistuvilla tavallisilla tarkkuuksilla (SD, Standard Definition).

Lisääntynyt kuvainformaatio sekä kameroiden lisääminen tarkoittaa puolestaan potentiaalisesti suurempaa tietoliikenneverkon kuormitusta ja kasvavaa tallennustilan tarvetta. Tähän on vastattu kehittämällä edistyneitä koodaus- ja lähetystekniikoita. Ensinnäkin tehokkaampaa koodausta käyttämällä voidaan pienentää suoratoistojalanjälkeä. Nykyään H.264-enkoodauksen käyttö lisää merkittävästi kameravalvontajärjestelmän kustannustehokkuutta aiemmin käytössä olleisiin koodaustapoihin verrattuna. Toiseksi ryhmälähetystä (multicast) käyttämällä voidaan vähentää tietoliikenneverkon kuormitusta tilanteissa, joissa vastaanottajia on enemmän kuin yksi.

Yritys Oy tuottaa Asiakas Oy:lle IP-pohjaisia kameravalvontapalveluja, jotka perustuvat IndigoVision Ltd:n järjestelmään ja siihen integroitaviin lisälaitteisiin. Kameroina käytetään joko analogisia kameroita, jotka liitetään erilliseen H.264-enkooderiin, tai digitaalisia IP-kameroita, joissa koodaus tehdään paikallisesti. Koodattu suoratoisto

lähetetään tietoliikenneverkossa valvomoihin ja tallennettavaksi. Nimityksiä Asiakas ja Yritys käytetään tietoturvasyistä.

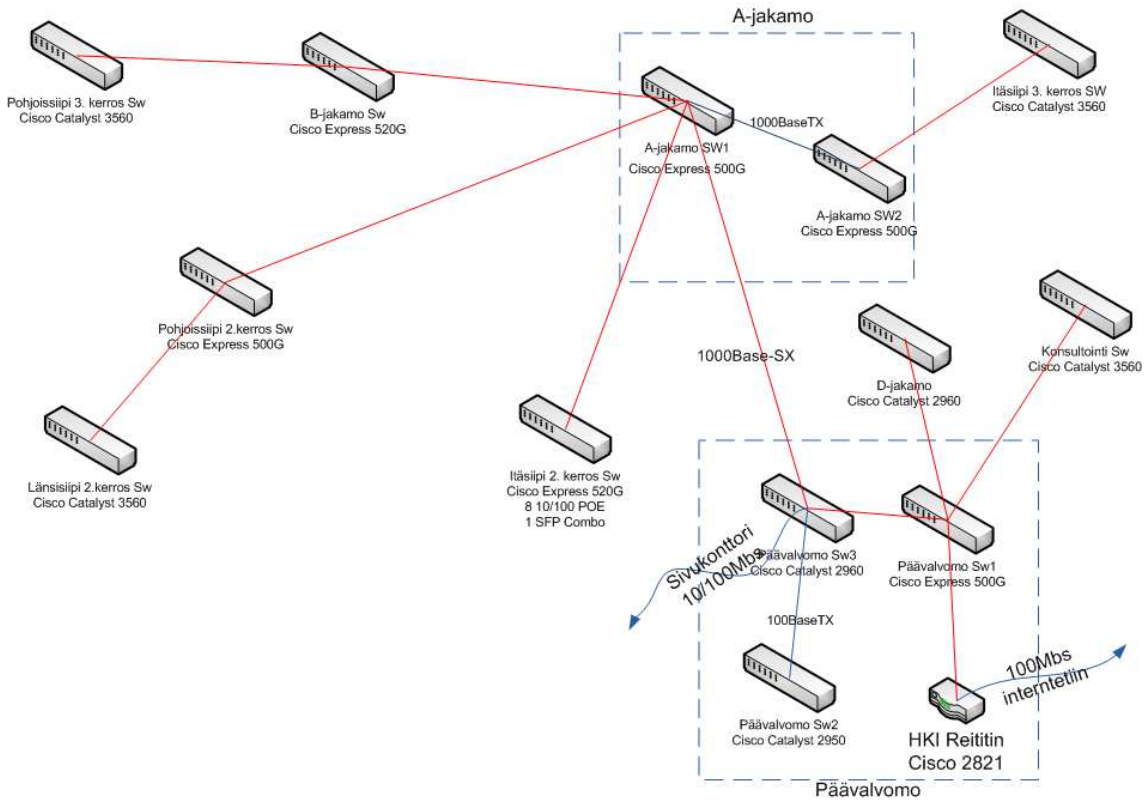
Yritys aloitti kameravalvonnan uudistamisen Asiakkaan Helsingin toimipisteessä noin viisi vuotta sitten. Tuolloin käytössä oli DVR-tekniikkaan (DVR, Digital Video Recorder) perustuva järjestelmä, jossa kukin analoginen kamera oli yhdistettynä suoraan tallentimena toimivaan tietokoneeseen. Kamerajärjestelmän ohjaamiseen käytettiin analogista videomatriisia. Järjestelmää uudistettiin: nyt jokainen kamera on yhteydessä tietoliikenneverkkoon omalla IP-osoitteellaan. Videota voidaan tallentaa joustavasti eri NVR-tallentimille (NVR, Network Video Recorder) tarpeen mukaan, samoin kameravalvontanäkymiä voidaan tietokoneen näytöllä muokata tilanteeseen sopivaksi.

Aluksi Asiakkaan kameravalvontajärjestelmässä oli vain noin 70 kameraa. Sittemmin kameroiden määrä on lisääntynyt koko järjestelmässä noin 500:aan. Lisäksi rikkoutuneiden SD-kameroiden tilalle on asennettu HD-kameroita. IP-pohjaisen järjestelmän edut on myös haluttu hyödyntää mahdollisimman hyvin. Samaan järjestelmään onkin otettu käyttöön useita etäkohteita, joiden kamerajärjestelmiä on uusittu ja liitetty samaan valvomoympäristöön. Valvomoja on myös lisätty. Lisäksi kamerakuvaa välitetään yhteistyökumppaneille ja viranomaisille tietyin ehdoin, mikä myös lisää kameraverkon kuormaa ja monimutkaisuutta. Asiakkaan Helsingin toimipisteen kameraverkkoa päätettiinkin päivittää vastaamaan paremmin uusia vaatimuksia.

Tässä insinöörityössä kuvataan kameraverkon lähtötilanne sekä luodaan yleiskatsaus suoratoistoon liittyviin tekniikoihin. Työssä kuvataan myös laitteiden hankintaprosessia, uusien kytkimien ominaisuuksia, verkon suunnittelua ja asennetun verkon testausta.

2 Lähtötilanne

Kamerajärjestelmän käyttöön on alusta alkaen rakennettu erillinen tietoliikenneverkko, joka palvelee vain videon siirtoa. Vanha kameraverkko on esitelty kuvassa 1. Kuvasta voidaan havaita, että kameraverkossa käytettiin Ciscon Catalyst Express 500G- ja 520-sarjan laitteita. Näissä kytkimissä tiedonsiirtonopeutta ei voi kasvattaa käytössä olleesta 1 Gbit:stä/s. Lisäksi IGMP-ryhmien (Internet Group Management Protocol) määrä on kytkimissä rajoitettu 256 ryhmään. Oli ennakoitavissa, että tuettujen IGMP-ryhmien määrä tultaisiin pian ylittämään kameraverkon suunniteltujen laajennusten vuoksi. Catalyst Express -sarjan hallintaominaisuudet ovat myös hyvin rajallisia. Kytkimet eivät tue kahdennettua virransyöttöä. Verkon topologia ei myöskään ollut vikasietoinen.



Kuva 1. Kameraverkon vanha topologia.

Helsingin toimipisteen kytkinverkon kaapelointina käytetään monimuotokuitu-kaapelointia, joka on tehty OM3-kategorian (Optical Multimode 3) valokuidulla. Yhteydet sivukonttoreihin ja Internetiin on toteutettu yksimuotokuidulla.

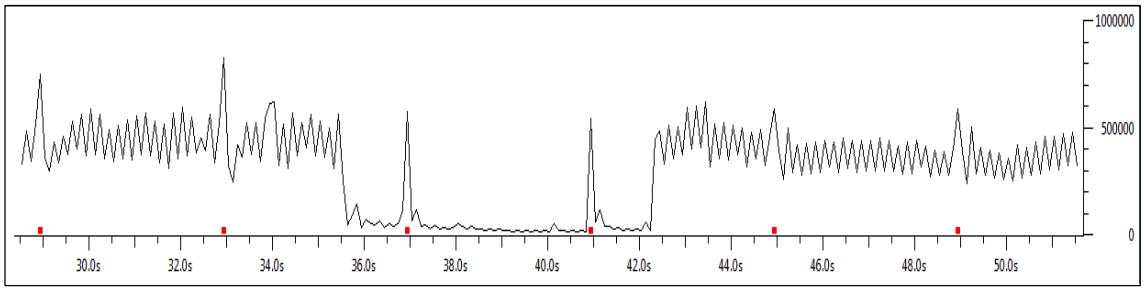
3 Suoratoistoverkon teoriaa

3.1 H.264-koodaus

H.264-standardissa määritellään joukko videon koodaukseen käytettäviä menetelmiä. Enkooderien valmistajille on annettu vapaus käytettävien menetelmien valintaan. Menetelmät on jaettu profiileihin niiden monimutkaisuuden mukaan. [1, s.16.]

H.264-suoratoiston keskeisessä osassa on avainkuva, joka toimii aloituskuvana sitä seuraavalle muutoskuvien sarjalle. Muutoskuvien koodauksessa käytetään hyödyksi perättäisten kuvien samankaltaisuutta. Muutoskuvien koodauksessa voidaan käyttää esimerkiksi liikkeenestimointia, jolla voidaan vähentää liikkuvan kohteen koodaukseen tarvittavaa datamäärää. [2, s. 2.]

Kuvassa 2 on esitetty kamerakiertoa tekevän kameran H.264-koodatun suoratoiston liikenneprofiili. Avainkuvat näkyvät selvinä piikkeinä liikenneprofiilissa, erityisesti silloin, kun kamera on paikallaan, jolloin kuvassa tapahtuu vain vähän muutosta. Tällöin peräkkäiset kuvat ovat hyvin samankaltaisia, joten muutoskuvien koodaamiseen tarvittava datamäärä on vähäinen.



Kuva 2. H.264-koodattu, automaattista kamerakiertoa tekevän kameran suoratoisto. Kameran tarkkuus on HD 720p, suoratoisto on asetettu 4 Mbit:iin/s ja kuvatahti on 25 kuvaa sekunnissa. Pystyasteikko on 0–10 Mbit/s. Avainkuvat lähetetään 4 s:n välein: lähetysajankohdat on merkitty punaisella pisteellä. Kamera on paikallaan 36–42 s:n kohdalla.

3.2 Real-time Transport Protocol

RTP-protokolla (Real-time Transport Protocol) on yhteyskerroksen protokolla, jolla ylläpidetään suoratoistettavan videon tahdistusta. RTP-otsikko sisältää suoratoistopaketin aikaleiman ja sekvenssinumeroinnin. Näiden tietojen avulla video voidaan toistaa alkuperäisessä järjestyksessä, vaikka pakettien järjestys olisi muuttunut siirron aikana. Sekvenssinumerointi mahdollistaa myös pakettihäviön havaitsemisen. Lisäksi aikaleiman avulla voidaan kompensoida viiveen vaihtelua suoratoistossa. [3, s. 14]

RTCP-protokollaa (Real-time Transport Control Protocol) käytetään RTP-yhteyden tilan signalointiin. Pakettihäviötä havaitessaan suoratoiston vastaanottaja voi lähettää avainkuvapyynnön videolähteelle RTCP-protokollalla. Avainkuvapyynnön lähettäminen nopeuttaa suoratoiston palautumista. [4, s. 12.]

3.3 Suoratoisto täsmälähetyksenä

RTP-enkapsuloitua videota voidaan kuljettaa TCP- (Transport Control Protocol) tai UDP-protokollalla (UDP, User Datagram Protocol). UDP-protokollalla voidaan lähettää suoratoistoa joko täsmälähetyksenä (unicast) tai ryhmälähetyksenä (multicast). TCP-protokollan etuna on se, että kunkin dataikkunan perille saapuminen varmistetaan kuittauksin [5]. Toisaalta kuittausmenettely lisää verkon kuormitusta erityisesti silloin, kun joudutaan tekemään uudelleenlähetyksiä pakettien menettämisen vuoksi. Lisäksi saman datan uudelleenlähettäminen lisää viivettä verkossa.

TCP on usein huono valinta suoratoistoon sen viivealttiuden vuoksi. Toisaalta TCP sopii hyvin paikalliseen tallennukseen, jolloin varmistutaan siitä, ettei videovirrasta menetetä kuvia. Tallennin järjestää paketit RTP-otsikon sisältämän aikaleiman mukaan, minkä ansiosta tallennettu video toistuu sujuvasti.

UDP-protokollan etuna taas on se, että ylimääräistä kuittauksista ja uudelleenlähetyksestä johtuvia viiveitä ja verkon kuormitusta ei synny. UDP-videota

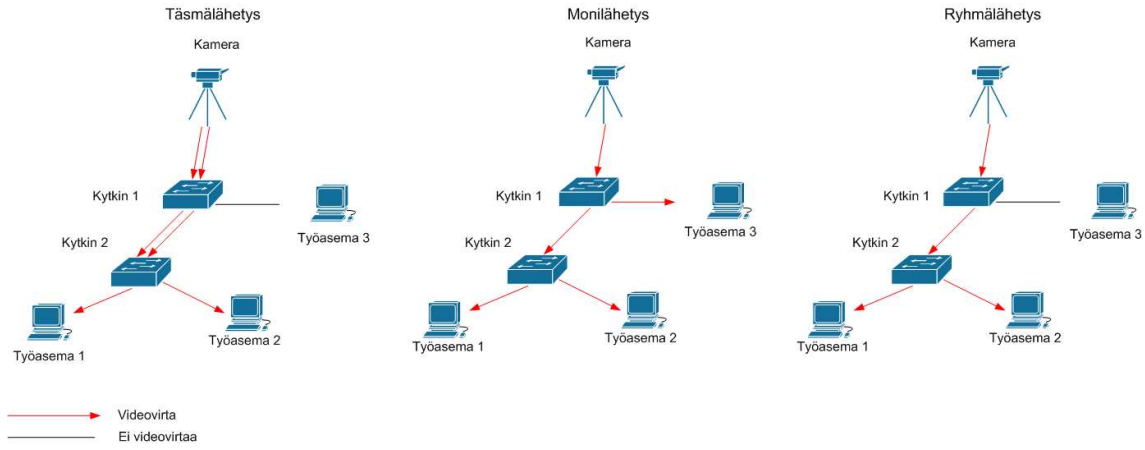
voidaan suoratoistaa varsin hitaalla yhteydellä. Uudelleenlähetyksen puuttuminen kuitenkin aiheuttaa sen, että kuvainformaatiota voidaan menettää. UDP-protokollaa käyttävässä suoratoistossa pakettihäviö näkyy kuvan katkonaisena toistona. Valvomokäytössä satunnainen pakettihäviö ei juuri haittaa, sillä tavallisesti katsojalle on tärkeintä nähdä tilanne reaaliajassa. Toisaalta tallennuskäytössä tilanne on ikävämpi, sillä saattaisihan olla, että juuri ne puuttuvat kuvat olisivat olleet tallenteen käytön kannalta tärkeitä.

UDP-protokollan otsikkokentästä puuttuu sekvenssinumerointi. Tämän vuoksi pakettihäviön tai väärän pakettien saapumisjärjestyksen havaitseminen ei UDP-protokollalla onnistu. RTP täydentää UDP:n toimintaa tarjoten sekvenssinumeroinnin, jonka ansiosta yhteyden luotettavuus paranee. [6, s.15.]

3.4 Suoratoisto ryhmälähetyksenä

3.4.1 Ryhmälähetyksen perusteet

Ryhmälähetystä käytetään tilanteessa, jossa useat käyttäjät haluavat vastaanottaa samaa reaaliaikaista tietoa. Tällöin vaikuttaa turhalta lähettää sama data useaan kertaan laitteelta verkkoon ja siirtää tämä sama data runkoverkossa useana kopiona, kunnes päätelaitteiden luona lähetykset erkanevat. Sen sijaan lähetetäänkin reaaliaikainen tieto vain kerran laitteelta verkkoon ja runkoverkossa siirretään jatkuvasti vain yhtä originaalia, kunnes topologian niin vaatiessa reitittimet ja kytkimet kopioivat sen tarvittaviin portteihin. Kuvassa 3 on havainnollistettu täsmälähetyksen, monilähetyksen (broadcast) ja ryhmälähetyksen välistä eroa. [7.]



Kuva 3. Suoratoisto eri lähetystavoilla.

Kuvassa työasemat 1 ja 2 haluavat vastaanottaa videota kameralta. Täsmälähetyksessä kamera lähettää suoratoiston kahdesti. Monilähetyksessä suoratoisto lähetetään vain kerran, mutta sen vastaanottaa myös työasema 3, jonka ei ole tarpeen vastaanottaa videota. Ryhmälähetyksessäkin suoratoisto lähetetään vain kerran, mutta erona monilähetykseen on se, että ainoastaan ryhmään liittyneet työasemat 1 ja 2 vastaanottavat videota.

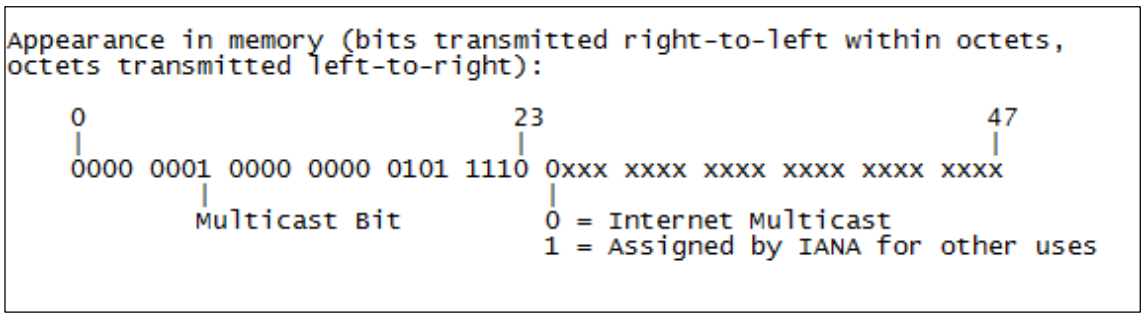
Ryhmälähetystoiminto on tärkeä paitsi verkon kapasiteetin säästämiseksi, myös kameran tai enkooderin suorituskapasiteetin säästämiseksi. Esimerkiksi IndigoVision on ilmoittanut HD-kameroidensa läpäisyksi 32 Mbit/s [8]. Tämä on helppo ylittää, mikäli videota suoratoistetaan 8 Mbit:n/s maksimilaadulla useissa valvomoissa ja lisäksi tallennetaan. Ryhmälähetystoiminnallisuutta käytettäessä myös nämä ongelmat vältetään, sillä tällöin voidaan lähettää videota valvomokäyttöön ryhmälähetyksenä, jolloin kyseinen video lähetetään vain kerran ja tallennukseen video lähetetään tarvittaessa erikseen täsmälähetyksenä.

Haasteet ryhmälähetyksen kanssa johtuvat siitä, että kun tavallisesti kamera tietää, mihin dataa ollaan lähettämässä, niin tässä tapauksessa dataa lähetetään ryhmäosoitteeseen ja luotetaan siihen, että dataa tarvitsevat saavat sen käyttöönsä. Näin vastuu vastaanottajien tietojen keräämisestä siirretään kameralta tietoliikenneverkolle.

3.4.2 Ryhmäosoitteet

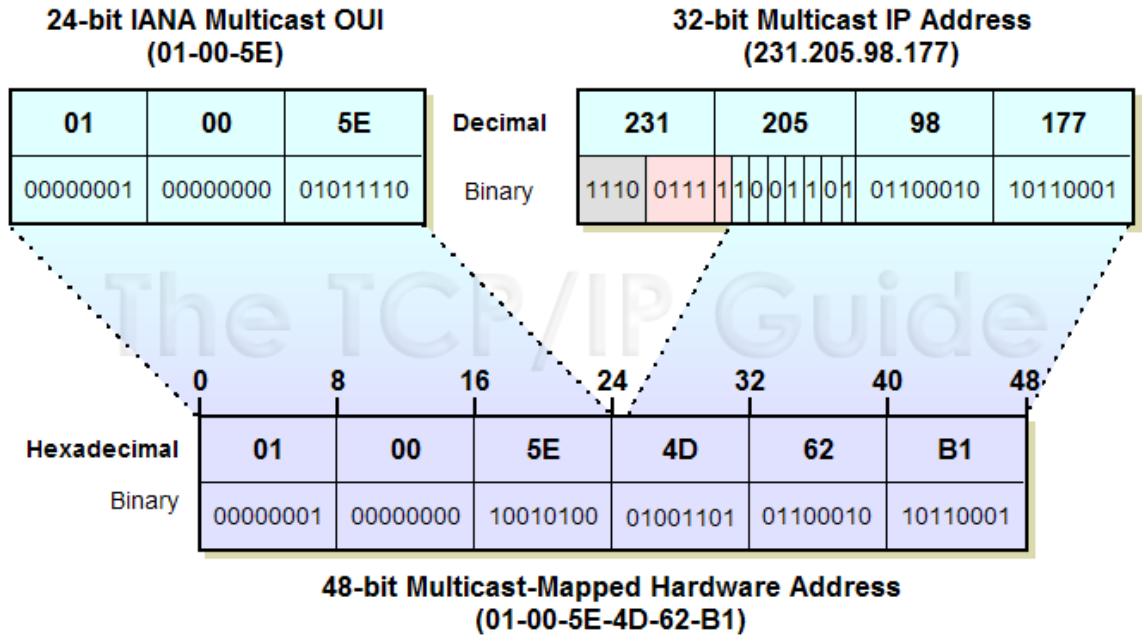
Ryhmälähetykselle on määritelty oma IP-osoitealueensa, jonka tiedot löytyvät sivustolta www.iana.org. Osoitealueeksi on määritetty 224.0.0.0–239.255.255.255 [9]. RFC 2365 -dokumentissa (RFC, Request For Comments) on annettu omat suosituksensa ryhmälähetysosoitteiden käytöstä yksityisessä verkossa. Käytännössä verkko 239.0.0.0/8 on varattu yksityiseen ryhmälähetyskäyttöön, mutta suositus on, että käyttö aloitetaan osoitealueelta 239.255.0.0/16 [10, s. 2].

Ryhmälähetyksen MAC-osoitealue (MAC, Media Access Control) on IANA:n mukaan 01-00-5E-00-00-00...01-00-5E-7F-FF-FF. Muunnos lähettävän kameran verkkokerroksen ryhmäosoitteesta siirtokerroksen osoitteelle suoritetaan siten, että verkkokerroksen ryhmäosoitteen ensimmäinen oktetti korvataan 01-00-5E:llä ja loput kolme oktettia muodostuvat verkkokerroksen ryhmäosoitteesta. IANA (Internet Assigned Numbers Authority) on kuitenkin merkinnyt varatuksi ryhmälähetyksen MAC-osoitteesta bitin 24. Tämän vuoksi jälkimmäisen osan (kolme viimeistä oktettia) eniten merkitsevä bitti muutetaan nollaksi (bitti 24). Osoitteen muodostus on esitetty kuvassa 4. [11.]



Kuva 4. Ryhmälähetyksen MAC-osoite [11].

Kuvassa 5 on esitetty verkkokerroksen ryhmäosoitteen 231.205.98.177 muuntaminen siirtokerroksen ryhmäosoitteeksi.



Kuva 5. IP-ryhmäosoitteen muuntaminen MAC-ryhmäosoitteeksi [12].

Muunnos tehdään seuraavasti: muunnetaan 231.205.98.177 heksadesimaalimuotoon, jolloin saadaan E7-CD-62-B1. Ensimmäinen oktetti EF korvataan 01-00-5E:llä. Näin saadaan 01-00-5E-CD-62-B1. Muutetaan vielä bitti 24 nollaksi, jolloin lopputulokseksi muodostuu MAC-ryhmäosoite 01-00-5E-4D-62-B1. [12.]

Edellä kuvattu osoitteiden muuttuminen tulee ottaa huomioon ryhmäosoitealueiden määrittämisessä. Koko käytettävän verkon ryhmäosoitealueet tulisi määritellä samaan x.x.x.x/9 -osoitealueeseen, koska kytkin ei osaa erottaa esimerkiksi ryhmäosoitteita 239.1.1.1 ja 238.1.1.1 tai 239.1.1.1 ja 239.129.1.1 toisistaan. Verkon 224.0.0.0/24 ryhmäosoitteet on varattu verkon signalointiin. Näihin ryhmäosoitteisiin lähetettävä data leviää oletuksena koko verkossa. Kytkinten ryhmäosoitteiden erottelukyvyn puutteellisuudesta seuraa, että mitään ryhmälähetysverkkoja x.0.0.0/24 tai x.128.0.0/24 ei tule käyttää, tai muuten lähetettävä ryhmälähetys leviää koko verkkoon. [13.]

3.4.3 Internet Group Management Protocol

Työasemat, jotka haluavat vastaanottaa ryhmälähetystä lähettävät multicast-reitittimelle ryhmäänliittymispyynnön IGMP-protokollalla (IGMP, Internet Group Management

Protocol). Reititin lähettää verkkoon säännöllisin väliajoin IGMP-kyselyitä. Kyseilyillä varmistetaan, että verkossa on vielä ryhmälähetystä vastaanottavia työasemia. [7.]

3.4.4 Internet Group Management Protocol Snooping

Ryhmälähetysliikenteen toiminnan ymmärtämiseksi siirtoverkossa on tiedettävä kytkinten toiminnan perusperiaatteet. Kytkin pitää yllä verkon MAC-osoitetietoja kytkintaulussa. Aina kun kytkin vastaanottaa datakehyksen, kytkin tarkistaa kehyksestä lähettäjän MAC-osoitteen. Lähettäjän MAC-osoite lisätään kytkintauluun, mikäli tätä ei ole jo tehty aiemmin. Kytkintauluun merkitään myös, mistä portista kehys saapui ja mihin VLAN:iin (Virtual Local Area Network) osoite kuului. Mikäli kytkintaulussa on MAC-osoitteesta aiempi merkintä, mutta portti on vaihtunut, korvataan vanha merkintä uudella. Näin ollen sama MAC-osoite ei voi esiintyä kytkintaulussa samaan aikaan eri porteissa. Kytkintaulua on havainnollistettu kuvassa 6. [14.]

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.5900.ba06    DYNAMIC     Fa0/24
   1    000c.8593.f7c0    DYNAMIC     Fa0/24
   1    000c.8593.f7d8    DYNAMIC     Fa0/24
   1    000f.e207.f2e0    DYNAMIC     Gi0/1
   1    0015.992e.a0eb    DYNAMIC     Fa0/12
   1    0018.fe65.145a    STATIC      Fa0/11
   2    000c.8593.f7d8    DYNAMIC     Fa0/24
   2    0012.fb1d.79a5    DYNAMIC     Fa0/24
```

Kuva 6. Kytkimen MAC-osoitetaulu.

Kytkin tekee välityspäätökset kytkintaulun perusteella. Ryhmälähetyksen MAC-osoitteita ei kuitenkaan esiinny lähettäjän MAC-osoitteena. Tästä seuraa, että kytkin ei voi oppia ryhmäosoitteita normaalilla oppimismenetelmällä. Näin ollen ryhmälähetys on oletuksena levitettävä joka porttiin. [15, s. 2.]

IGMP snooping (Internet Group Management Protocol snooping) on tekniikka, jota kytkimet käyttävät lähetysryhmien hallintaan. IGMP snooping -tekniikkaa käyttävä kytkin tarkastelee verkkokerroksen IGMP-liikennettä ja erittelee liikenteestä ryhmiä

koskevat liittymisviestit samoin kuin poistumisviestit. Kun kytkin vastaanottaa ryhmäänliittymisviestin, kytkin merkitsee kytkimen IGMP-ryhmätauluun ryhmälähetysosoitteen ja portin, josta viesti saapui. Jos kytkin vastaanottaa liittymisviestin samaan ryhmään jostakin muusta portista, lisätään portti ryhmätauluun ryhmäosoitetta vastaavien porttien listaan. Toisin kuin täsmälähetyksessä, jolloin yhtä osoitetta vastaa yksi portti, ryhmälähetyksessä yhtä lähetysryhmää vastaa ryhmä portteja. Kytkimen IGMP-ryhmätaulua on havainnollistettu kuvassa 7. [16, s. 413–417]

Vlan	Group	Type	Version	Port List
1	224.0.1.127	igmp	v1	Fa0/12, Gi0/1
1	239.255.1.79	igmp	v2	Fa0/24, Gi0/1
1	239.255.1.95	igmp	v2	Fa0/24, Gi0/1
1	239.255.1.112	igmp	v2	Fa0/14, Gi0/1
2	224.2.127.254	igmp	v2	Gi0/1
2	239.255.255.255	igmp	v2	Gi0/1
21	224.2.127.254	igmp	v2	Gi0/1
21	239.255.1.12	igmp	v2	Fa0/1, Gi0/1
21	239.255.1.62	igmp	v2	Fa0/1, Gi0/1

Kuva 7. IGMP-ryhmätaulu Cisco Catalyst 2960 -kytkimeltä. Kytkin lukee IGMP-ryhmäosoitteet verkkokerroksen IGMP-otsikkotiedoista.

Vaikka ryhmätaulun ryhmäosoitteet esitetään verkkokerroksen ryhmäosoitteina, kytkin välittää varsinaisen ryhmälähetysliikenteen käyttäen ryhmälähetyksen MAC-osoitteita. Kun kytkimeen saapuu ryhmälähetyskehys, kytkin lähettää sen jokaiseen ryhmään kuuluvaan porttiin. [16, s. 413–417.]

3.4.5 Ryhmälähetyksen leviäminen siirtokerroksessa

Kuten aiemmin todettiin, ellei IGMP snooping -toimintoa ole asetettu käyttöön siirtokerroksen laitteisiin, suoratoistettava ryhmälähetys tavallisesti toimii monilähetyksen tavoin ja leviää jokaiseen kytkimen porttiin. Samoin mikäli STP:tä (Spanning Tree Protocol) käyttävässä verkossa tapahtuu topologiamuutos, ryhmälähetys leviää oletuksena, kunnes kytkinten IGMP-taulut päivittyvät [17, s. 7, 8]. Tämä on erittäin epätoivottavaa, koska se voi aiheuttaa suurta kuormitusta koko verkolle.

Kaikki siirtokerroksen segmentissä siirrettävä ryhmälähetysliikenne leviää aina myös verkossa sijaitsevalle multicast-reitittimelle. Kytkimet kuuntelevat tämän reitittimen

lähettämiä PIM-DVMRP-viestejä (PIM, Protocol Independent Multicast; DVMRP, Distance Vector Multicast Routing Protocol) ja kirjaavat sen perusteella reitittimelle vievän portin multicast-reititinportiksi [18, s. 143]. Kaikki kytkimelle saapuva ryhmälähetys leviää tähän multicast-reititinporttiin. Kyseinen reititin tarkistaa mitkä ryhmälähetyksistä tulee reitittää eteenpäin. Mikäli tämä IGMP snooping -tekniikan rajoittuneisuudesta aiheutuva toiminta jätetään huomioimatta, saatetaan alimitoittaa verkon reitittimen kapasiteetti. Esimerkiksi sellaisen verkon suunnittelussa, jossa ryhmälähetystä virtautetaan 20 Mbit/s etäkohteisiin ja 120 Mbit/s paikallisesti, voi helposti tehdä sen virheen, että hankkii reitittimen etäkohteisiin lähetettävän datamäärän mukaan. Tällöin reitittimen kapasiteetti ylittyy paikallisesta verkosta sille leviävästä ryhmälähetysliikenteestä. Toki on kehitelty sellaisia protokollia kuin RGMP (Router-port Group Management Protocol) tämän ongelman ratkaisemiseksi, mutta sitä tukevat laitteet ovat erittäin kalliita, eivätkä siten useinkaan kustannustehokkaita. [19, s. 2.]

3.5 10 Gigabit Ethernet

IEEE 802.3ae eli 10 Gigabit Ethernet (10GbE) hyväksyttiin standardiksi vuoden 2002 kesäkuussa. Sen nopeusluokka on nimensä mukaisesti 10 Gbit/s. Aiemmista Ethernet-standardeista poiketen se on määritelty toimimaan vain kaksisuuntaisessa tilassa, jolloin törmäysten havainnointia ei tarvita. 10GBase-SR on monimuotokuidulle tarkoitettu lyhyen aaltopituuden (850 nm) media 10 Gbit/s -yhteyksille. 10GBase-SR-yhteys voidaan muodostaa enintään 300 m pitkällä OM3-kategorian (Open Multimode 3) kuidulla. 10GBase-LR-yhteys (pitkä aallonpituus, 1310 nm) voidaan muodostaa 10 km:iin asti yksimuotokuidulla. [20, s. 10; 21, s. 742.]

4 Laitteiden valinta

4.1 Kameravalvontajärjestelmän keskeiset vaatimukset

Kameravalvontajärjestelmän tarkoitus on ylläpitää turvallisuutta. Turvajärjestelmän käyttöön tarkoitetun tietoliikenneverkon suunnittelussa tulee varmistua siitä, että järjestelmän käytettävyys säilyy hyvänä myös poikkeusoloissa. Käytettävyyden vaatimuksen vuoksi verkon on noudatettava seuraavia keskeisiä vaatimuksia.

Alhainen viive

Kameravalvonnassa käytettävän suoratoistoverkon viiveen tulee olla alle 300 ms mukaan lukien kameran kuvan koodaus, lähetys ja dekoodaus. Tämä johtuu siitä, että käyttäjä ohjaa kameraa reaaliaikaisesti ja pitkät viiveet tekevät sujuvan ohjauksen mahdottomaksi. Viiveelle asetettu 300 ms:n raja perustuu ihmisen kykyyn reagoida näkökyvyn välityksellä saatuihin herätteisiin [22, s. 66]. Suoratoistoa ei tulisi puskuroida tarpeettomasti reaaliaikaisuuden vaatimuksen vuoksi [23, s. 2].

Ympärivuorokautinen käyttö

Palvelutaso on määritetty 99,8 %:iin, mikä tarkoittaa noin neljän tunnin katkosta kolmen kuukauden tarkastelujaksolla. Normaalissa toimistoverkossa palvelutaso määräytyy vain työajan mukaan. Tällöin tietoliikenneverkkoa voi huoltaa yöllä sen vaikuttamatta palvelutasoon. Valvontajärjestelmää kuitenkin käytetään vuorokauden ympäri, ja sen tärkeys korostuu öisin [23, s. 2]. Katkosten tulisikin olla mahdollisimman lyhyitä. Toteutunut palvelutaso selvitetään SNMP-valvontajärjestelmän (Simple Network Management Protocol) tuottamien raporttien avulla.

Nopea toipuminen

Järjestelmän tulee toipua nopeasti yhden jakeluverkon kytkimen vikaantumisesta tai jakeluverkon yhteyden katkeamisesta. Verkon tulee toipua 50 ms:ssa, mikä vastaa noin

yhden kuvan menettämistä suoratoistossa. Toipumisen jälkeen jakeluverkon muiden osien kuin suoraan katkoksen aiheuttaneen kytkimen tai yhteyden, tulee olla käytettävissä.

Keskuslaiteriippumattomuus

Turvajärjestelmän tulee olla keskuslaiteriippumaton. Yhden laitteen vikaantuminen ei saa johtaa koko järjestelmän käytettävyyden menettämiseen. Keskuskytkimen tuleekin olla kahdennettavissa eri laitetiloihin, jottei yhdessä laitetilassa tapahtunut onnettomuus, kuten tulipalo tai vesivahinko, aiheuta koko järjestelmän käytettävyyden menettämistä. Verkon aktiivilaitteiden tulee tukea myös kahdennettuja virtalähteitä, jotteivät lyhyet sähköverkon viat tai yksittäisen UPS-ryhmän (Uninterruptible Power Supply) vikaantuminen aiheuta katkosta järjestelmän toimintaan.

Tietoturva

Turvajärjestelmän tulee olla suojattu ilkivallalta ja verkkoon tunkeutumiselta. Ylläpidon tulee myös saada reaaliaikaisesti tieto mahdollisista tunkeutumisyrityksistä. Käyttäjien toimet, esimerkiksi tallenteiden haku, tulee myös kirjata lokiin.

Edellä lueteltujen perusperiaatteiden mukaisesti kameraverkon kytkimille asetettiin vaatimukset, jotka on esitetty taulukossa 1. Vaatimusten pohjalta tutustuttiin eri laitevalmistajien muun muassa Ciscon ja HP:n tuotteisiin ja tekniikoihin.

Taulukko 1. Kytkinten vähimmäisvaatimukset.

Vähäinen viive	Estoton kytkin 10GbE-tuki QoS-tuki (Quality of Service)
Vikasietoisuus	Kahdennettu - verkko - virransyöttö - keskuskytkin
IGMP-tuki	IGMP v1,v2 (Internet Group Management Protocol) IGMP snooping Jakelukytkimillä vähintään 1000 IGMP-ryhmää
Reititys	Routing Information Protocol v2 (RIPv2), Open Shortest Path First (OSPF),Protocol Independent Multicast Sparse Mode (PIM-SM)
Hallinta	Simple Network Management Protocol (SNMP) Secure Shell v2 (SSH)
Tietoturva	Remote Authentication Dial In User Service (RADIUS) Port security

4.2 Vertailu

Laitevalmistajien evaluoinnin jälkeen HP Networking (HP, Hewlett Packard) valittiin uuden jakeluverkon laitetoimittajaksi. Erityisesti edistyneet IRF- (Intelligent Resilient Framework) ja RRPP-tekniikat (Rapid Ring Protection Protocol) vaikuttivat valintaan. HP:n kytkimistä valittiin kolme 10 Gbit/s -yhteyksiä tukevaa kytkintä edelleen vertailuun.

Vertailuun valittiin HP:n A5120-, A5500- ja A5800-kytkimet. Kun laitteita vertailtiin keskenään, havaittiin, että A5120 ei täyttänyt kaikkia jakeluverkon laitteille asetettuja ensisijaisia vaatimuksia. A5120- ja A5500-sarjan laitteisiin joutuisi myös hankkimaan laajennuskortin 10 Gbit/s -nopeuksia varten. Kun vertailtiin kustannuksia eri mallien välillä, tultiin siihen tulokseen, että oli kustannustehokasta hankkia A5800-sarjan laitteita, joissa on suoraan 10 Gbit/s -tuki. Taulukossa 2 on esitelty yhteenveto vertailun

tuloksista. Hintavertailu on tehty kokoonpanoilla, joihin kuuluu kytkin, mahdollisesti tarvittava 10 Gbit/s -kortti sekä kaksi 10GBase-SR-moduulia. Laitteiden vertailussa teknisten ominaisuuksien ja hinnan välinen suhde oli 50/50. Pisteytys oli laitteiden hankintapäätöksen perustana.

Taulukko 2. Jakelukytkinten pisteytys. Hintavertailu on tehty 10 Gbit/s -kokoonpanoilla.

Laite	**HP A5120-24G-PoE EI**	**HP A5500-24G-PoE EI**	**HP A5800-24G-PoE EI**
Ensisijaiset vaatimukset	1050	1380	1470
Toissijaiset vaatimukset	200	200	230
YHTEENSÄ	**1250**	**1580**	**1700**
Tekninen toteutus, paras 50 pistettä	37	46	50
Hinta, halvin 50 pistettä	50	43	44
LOPPUTULOS	**87**	**89**	**94**

Vertailun perusteella A5800-sarjan kytkimet valittiin keskuskytkimiksi ja jakeluverkon kytkimiksi. Kaikki jakeluverkon laitteet valittiin samasta tuoteperheestä.

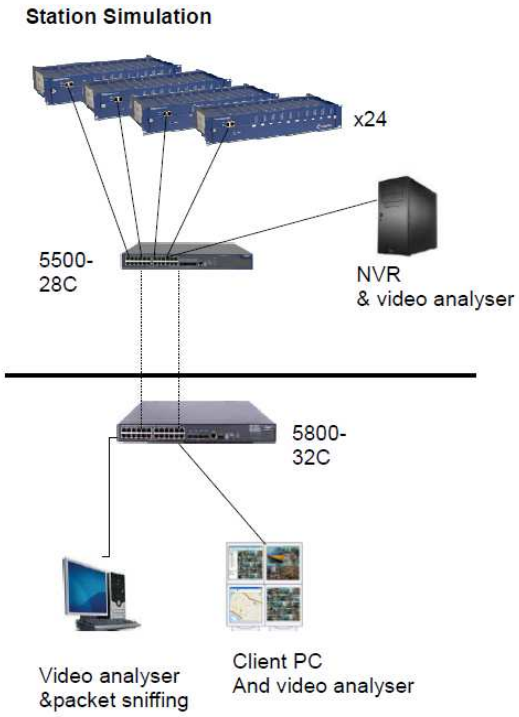
Reunaverkon kytkimiksi valittiin edullisemmat A5120-kytkimet. Peruskokoonpanolla ne olivat huomattavasti edullisempia kuin muut vertailun kytkimet, ja reunakytkimiksi niissä oli runsaasti ominaisuuksia. Taulukossa 3 on esitelty tiivistelmä reunakytkimien pisteytyksestä, ja kokonaisuudessaan taulukko on liitteessä 1.

Taulukko 3. Reunakytkinten pisteytys. Hintavertailu on tehty 1 Gbit/s -kokoonpanoilla.

Laite	**HP A5120-24G-PoE EI**	**HP A5500-24G-PoE EI**	**HP A5800-24G-PoE EI**
Ensisijaiset vaatimukset	765	765	795
Toissijaiset vaatimukset	210	210	230
YHTEENSÄ	**975**	**975**	**1025**
Tekninen toteutus, paras 50 pistettä	48	48	50
Hinta, halvin 50 pistettä	50	34	23
LOPPUTULOS	**98**	**82**	**73**

Jakeluverkon kytkinten toiminnan varmistamiseksi järjestettiin vielä testi yhteistyössä VideoGen Ltd:n, IndigoVisionin ja HP:n kanssa. HP toimitti yhden A5800- ja yhden A5500-kytkimen VideoGenille. VideoGen testasi kytkinten toimintaa IndigoVisionin

laboratoriossa Skotlannissa. Testattujen kytkinten ohjelmistoversio oli 5.20-2202P19. Testijärjestelyt on esitetty kuvassa 8.



Kuva 8. Kytkimien testijärjestelyt. Kussakin 5500-28C- kytkimeen liitetyssä yksikössä on neljä enkooderia [23].

Testillä haluttiin varmistua siitä, että kytkimet kykenevät 96 kameran yhtäaikaiseen ryhmälähetykseen valvomotietokoneelle ja täsmälähetykseen TCP-yhteydellä tallentimelle. Kutakin kameroista suoratoistettiin ja tallennettiin 4 Mbit/s -kuvayhteydellä. Kytkimet suoriutuivat testistä hyvin.

Testin jälkeen kytkimet päätettiin hankkia. Hankinnan yhteydessä edellytettiin, että ostettavien kytkinten ohjelmistoversio on sama kuin testeissä käytetyillä kytkimillä.

4.3 Valittujen kytkimien erityisominaisuudet

4.3.1 Rapid Ring Protection Protocol

IEEE 802.1D -standardissa määritelty STP-protokolla (Spanning Tree Protocol) on kytkinten siirtokerroksen vikasietoisuutta parantava tekniikka. HP:n omalla RRPP-protokollalla (Rapid Ring Protection Protocol) on STP:n kanssa toimintatavaltaan useita samankaltaisuuksia, mutta myös keskeisiä eroavuuksia. Kummassakin protokollassa perusajatus on sama: tarjota mahdollisuus kahdennettuihin reitteihin siirtokerroksen laitteiden välillä ja samalla kuitenkin estää silmukoiden muodostuminen. Siirtokerroksen laitteiden välille ei nimittäin saa muodostua silmukkaa, koska muutoin koko verkkosegmentin toiminta romahtaa leviävästä liikenteestä. Näin ollen täytyy olla keino sen varmistamiseksi, ettei näitä silmukoita muodostu. Toisaalta vikatilanteesta tulisi saada tieto, jotta voidaan tarvittaessa ottaa estetty yhteys jälleen käyttöön.

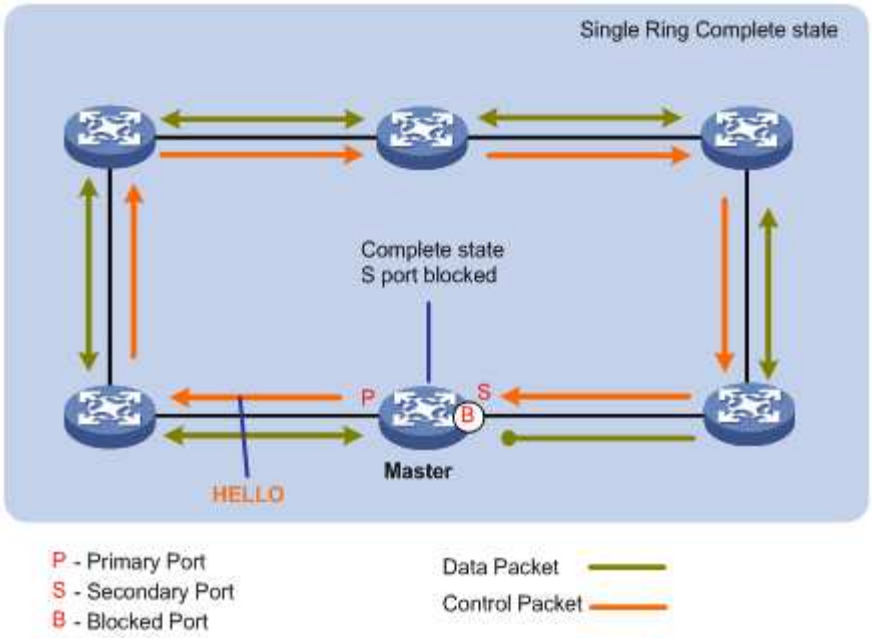
Molemmissa protokollissa on isäntälaite, joka lähettää verkkoon statusviestejä, joiden mukaan päätellään verkon tila ja informoidaan verkon muita laitteita mahdollisesti tarvittavista toimenpiteistä. STP-protokollassa isäntälaite on nimeltään juurisilta, ja informointiin käytetään BPDU-viestejä (Bridge Protocol Data Unit). RRPP-protokollassa taas isäntälaite on nimeltään isäntä ja informaatioviestit ovat RRPPDU-viestejä (Rapid Ring Protection Protocol Data Unit). [24; 25.]

STP-protokollassa perusajatus on se, että kytkökset voivat mennä hyvin monimutkaisesti kytkinten välillä niin, että kytkinten väliset yhteysnopeudet ja kytkinten määrä voi vaihdella dynaamisesti. Myös juurikytkin voi vaihtua alkuperäisen juurikytkimen mennessä epäkuntoon. Muodostunut kytkentöjen verkko levitetään auki puumaiseksi rakenteeksi ja siitä karsitaan kaikki silmukat pois. Käyttöön jäävässä virityspuussa pyritään optimoimaan käytettävät yhteydet, jotta kehykset voisivat kulkea nopeinta reittiä määränpäähänsä. Tämän tehtävän suorittamiseksi tarvitaan monimutkaisia proseduureja, joiden läpikäymiseen tarvitaan aikaa sitä enemmän, mitä enemmän verkossa on kytkimiä ja niiden välisiä yhteyksiä. STP-protokollassa palautuminen topologiamuutoksen yhteydessä voi kestää useita sekunteja. Verkon läpimitta on

rajoitettu, ja se vaikuttaa palautumisaikaan. Toisaalta STP on standardi ja siksi tuettu useimmissa kytkimissä. [24.]

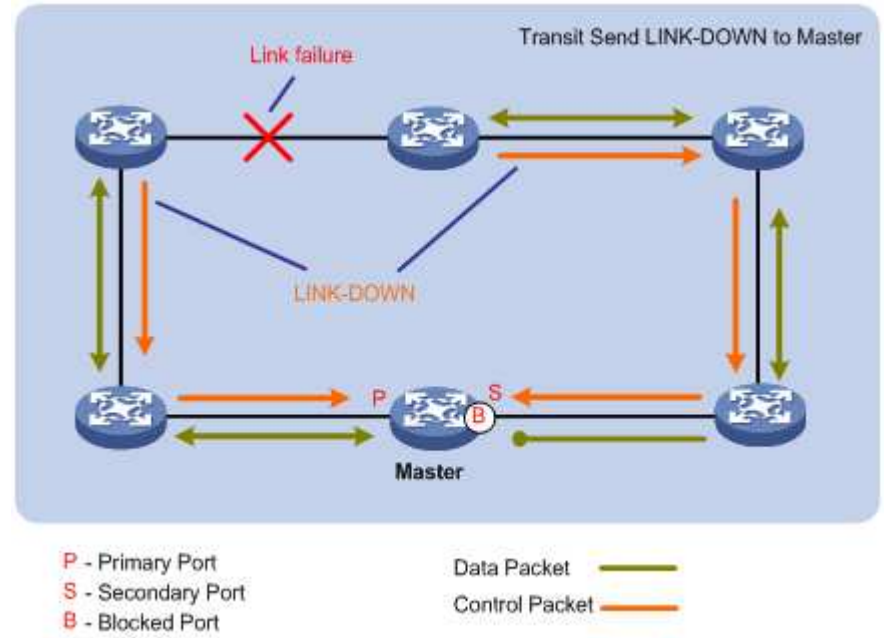
RRPP-protokollassa puolestaan lähdetään siitä, että verkko on suunniteltu rengasmaisesti tai rengaslinkeiksi. Verkkoon määritetään käsin isäntäkytkin ja välityskytkimet, samoin kuin mahdollisesti tarvittavat avustavat kytkimet eri renkaita yhdistäviin solmukohtiin. Samalla määritetään myös oletustilassa suljetut portit. Koska normaalitila on verkon topologiassa tehty staattisesti, voidaan topologiamuutoksiin vastata nopeasti riippumatta verkon koosta. Toisaalta tämä merkitsee enemmän ylläpitotyötä kytkimiä lisätessä ja poistaessa. Lisäksi RRPP-renkaaseen ei kannata lisätä kuin sellaisia kytkimiä, joissa RRPP on tuettu, tai muuten muutoksiin vastataan hitaammin tai virheellisesti. Kun RRPP-renkaassa käytetään useita VLAN-verkkoja, kuormitusta voidaan jakaa linkkien kesken. [25.]

RRPP soveltuu hyvin käytettäväksi esimerkiksi runkoverkossa silloin, kun muutoksia runkoverkkoon tarvitsee tehdä harvoin, kun runkoverkko muodostaa luonnollisesti ketjumaisen tai rengasmaisen rakenteen ja kun on tarpeen varautua vain yhden kytkimen tai linkin vikaantumiseen. Tällöin saavutetaan erittäin nopea palautumisaika vikatilanteissa. Kuvassa 9 on kuvattu yhden RRPP-renkaan topologia. [25.]



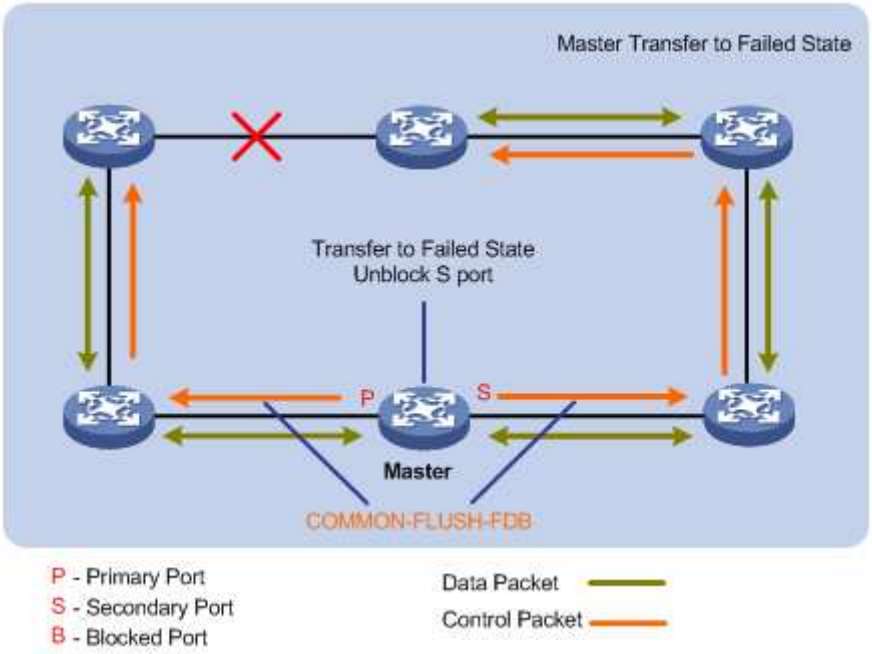
Kuva 9. Yhden RRPP-renkaan topologia [25].

Kuvassa on isäntäkytkin (Master) ja loput ovat välityskytkimiä (Transit). Oletustilassa isäntälaite pystyy vastaanottamaan ensisijaisesta portista (kuvassa P-kirjaimella merkitty portti) lähetetyt Hello-viestit toissijaisen portin kautta (kuvassa S-kirjaimella merkitty portti). Tämän vuoksi isäntäkytkimen toissijainen portti estetään, mikä estää silmukan syntymisen. Kuvassa 10 on esitetty yhden linkin katkeaminen. [25.]



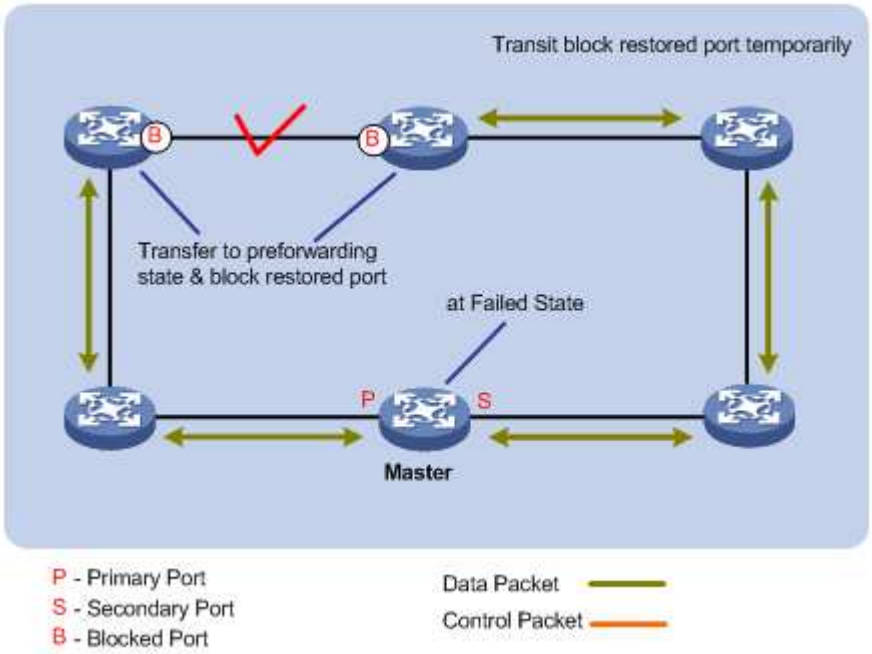
Kuva 10. Linkin katkeaminen RRPP-renkaassa [25].

Kun linkki katkeaa, linkin molemmin puolin olevat laitteet havaitsevat katkoksen ja lähettävät isäntälaitteelle tiedon *Link Down* -viestillä. Isäntälaite siirtyy vikatilaan ja avaa toissijaisen portin liikenteelle, mikä on esitetty kuvassa 11. [25.]



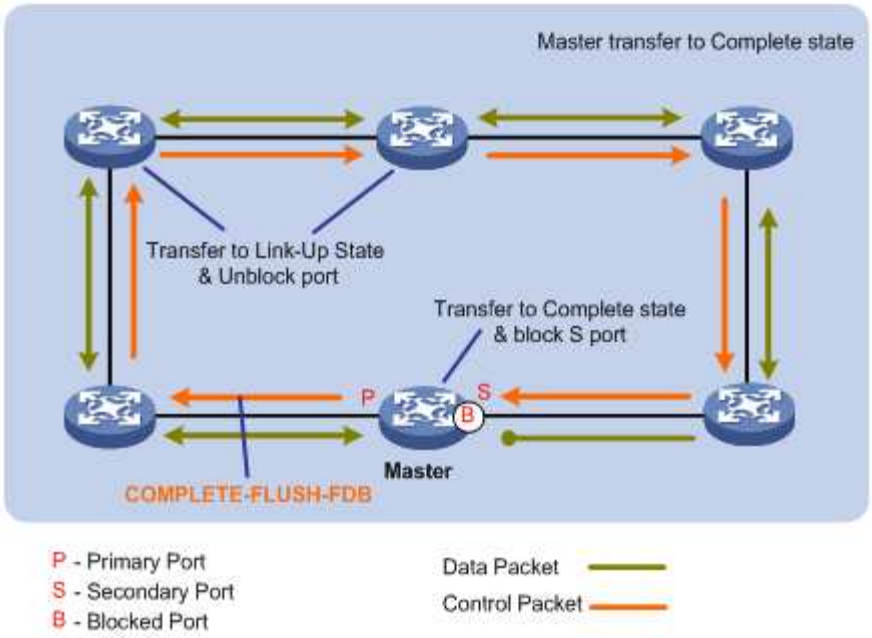
Kuva 11. Isäntälaite siirtyy vikatilaan [25].

Toissijainen portti avataan myös, mikäli jostain syystä isäntälaite ei saa Hello-viestiään toissijaisesta portista. Isäntälaite lähettää renkaan kytkimille tiedon topologiamuutoksesta *Common Flush FDB* -viestillä, ja kytkimet päivittävät MAC-osoitetaulunsa. Kun linkki palautuu välityskytkinten välillä, molemmat välityskytkimet estävät palautuneen linkin portit, koska isäntälaite ei ole vielä tietoinen muutoksesta. Tämä on esitetty kuvassa 12. [25.]



Kuva 12. Välityskytkimet estävät palautuneen linkin käyttöönoton [25].

Koska linkki on noussut ylös, isäntälaite voi jälleen vastaanottaa lähettämänsä Hello-viestit. Tällöin isäntälaite poistaa käytöstä toissijaisen porttinsa ja lähettää päivityskäskyn välityskytkimille, mikä on esitetty kuvassa 13. [25.]



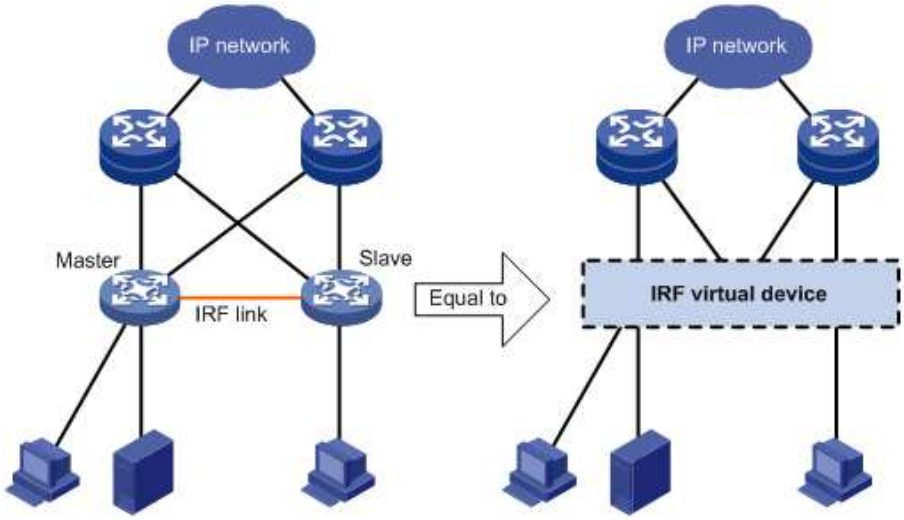
Kuva 13. Verkko palaa normaaliin tilaansa [25].

Saadessaan isäntäkytkimeltä *Complete Flush FDB* -viestin välityskytkimet avaavat estetyt porttinsa käyttöön. Verkko on näin palautunut normaaliin tilaansa. [25.]

Edellä esitelty RRPP-topologia vastaa tässä insinöörityössä testattavaa verkon rakennetta. Erityisesti kiinnostaa se, palautuuko yhteys 50 ms:ssa niin kuin valmistaja ilmoittaa.

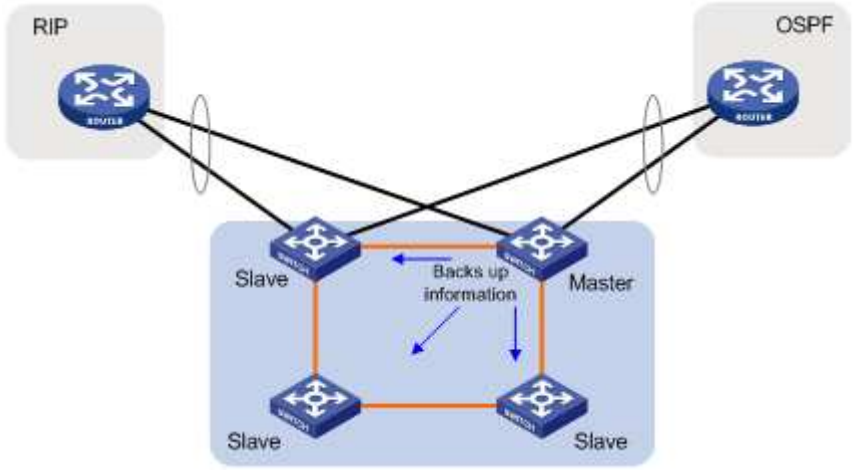
4.3.2 Intelligent Resilient Framework

Yksi kehittyneimmistä HP:n tekniikoista on IRF-tekniikka (Intelligent Resilient Framework), jolla voidaan yhdistää useita saman sarjan kytkimiä 10GbE-linkkien avulla yhdeksi virtuaaliseksi kytkimeksi. IRF-pinoon yhdistetyt kytkimet näkyvät verkkoon kaikin tavoin vain yhtenä kytkimenä. Tämä mahdollistaa valvomokoneiden LACP-linkkien (Link Aggregation Control Protocol) liittämisen erillisiin fyysisiin laitteisiin. Näin valvomokoneen yhteys tietoliikenneverkkoon säilyy toisen kytkimen rikkoutuessa. IRF-toteutusta on esitelty kuvassa 14. [26.]



Kuva 14. IRF-tekniikka muodostaa virtuaalisen kytkimen [26].

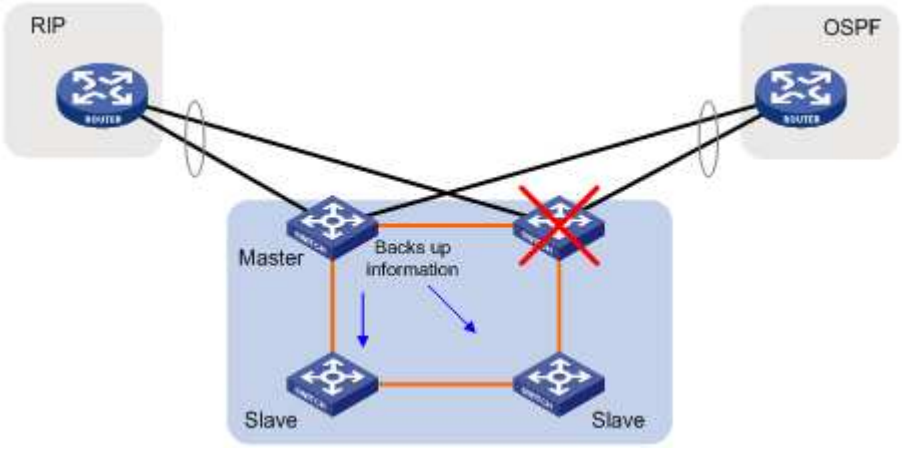
Kytkimet liitetään toisiinsa 10GbE-yhteydellä ja portit määritetään IRF-porteiksi. Mikäli kytkimien välille kytketään useampi IRF-yhteys, voidaan linkkejä käyttää kuorman tasaamiseksi. Samaan IRF-kytkökseen voidaan määrittää enintään neljä porttia 5800-sarjan laitteissa. Näin saavutetaan potentiaalisesti nelinkertainen yhteysnopeus IRF-laitteiden välillä. [26.]



Kuva 15. Asetusten kopiointi IRF-kokoonpanossa [26].

IRF-pinossa olevat kytkimet synkronoivat asetustiedoston keskenään. Kytkimiä voidaan pitää yllä yhdellä yhteisellä asetustiedostolla. Tämä on esitetty kuvassa 15. Isäntälaite kopioi asetukset muihin pinon kytkimiin. Jonkin pinon kytkimen vikaantuessa sen tilalle asennettavaan laitteeseen ladataan automaattisesti oikeat asetukset. Mikäli isäntälaite

vikaantuu, valitaan uusi isäntälaite automaattisesti, mikä on esitetty kuvassa 16. Valintaan vaikuttavat muun muassa laitteen prioriteetti ja käynnissäoloaika. [26.]

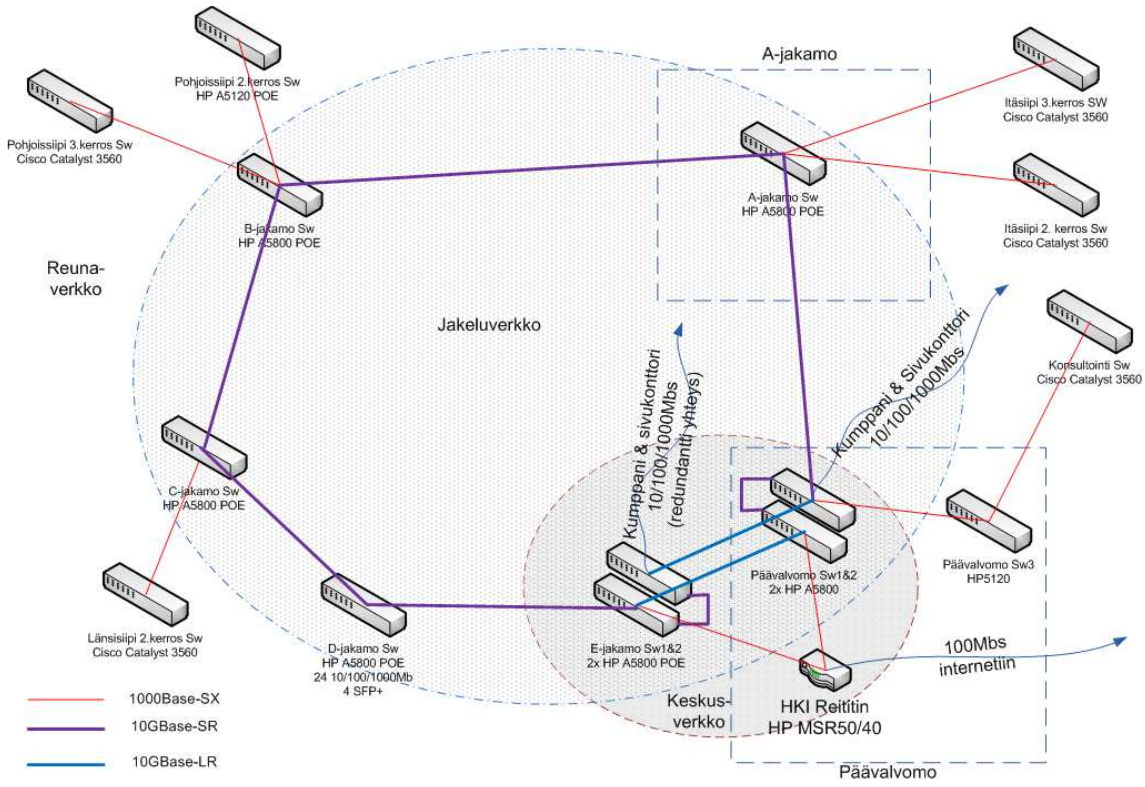


Kuva 16. IRF-kokoonpanon palautuminen isäntälaitteen vikaantuessa [26].

Koska IRF-pino voidaan toteuttaa normaaleilla 10GbE-yhteyksillä, pino voidaan muodostaa myös sellaisten laitteiden välillä, jotka ovat eri laitetiloissa. Insinöörityössä toteutetaan yksi IRF-virtuaalikytkin kahdesta 5800-sarjan kytkimestä. Lopullisessa toteutuksessaan samassa IRF-pinossa tulee olemaan neljä kytkintä.

5 Verkon toteutussuunnitelma

5.1 Verkkosuunnitelma



Kuva 17. Asiakkaan Helsingin toimipisteen kameraverkon suunniteltu topologia.

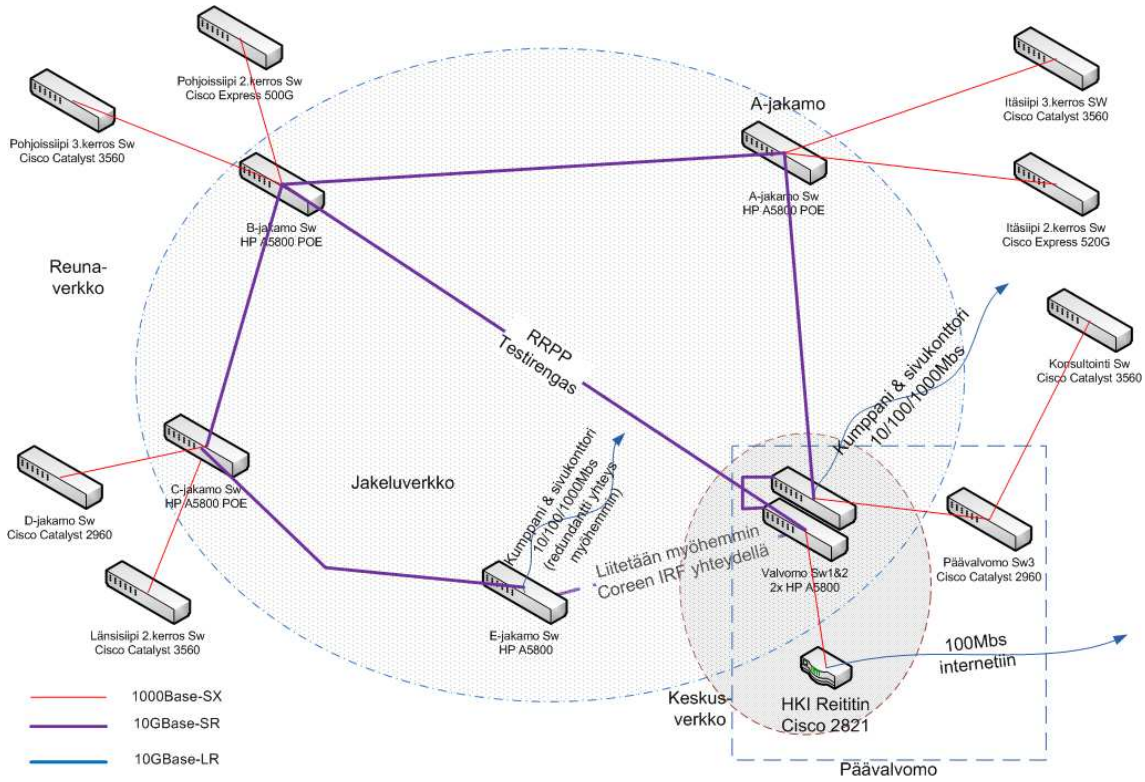
Suunnitelman mukaan siirrytään nykyisestä tähtimallisesta topologiasta rengasmalliseen, jossa keskuskytkiminä palvelee päävalvomossa ja E-jakamossa sijaitsevat yhteensä neljä HP A5800 -kytkintä. Kytkimet määritetään IRF-pinoon niin, että kumpaankin laitetilaan asennettavat kytkinparit liitetään toisiinsa kahdella 10GBase-LR-yhteydellä. 10GBase-LR-yhteydet kulkevat eri reittiä E-jakamon ja päävalvomon välillä, jotta voidaan minimoida kaapelivaurion aiheuttaman katkoksen riski. Lisäksi rakennetaan RRPP-renkaaksi 10GbE-jakelukerros neljästä 5800-sarjan kytkimestä, jotka ovat edelleen yhteydessä reunatason kytkimiin. Kaksi reunakytkintä tullaan vaihtamaan uusiin HP A5120 -sarjan kytkimiin. Jakelukytkimet ovat yhteydessä toisiinsa 10Gbase-SR-yhteyksillä. Reunakytkimet ovat yhteydessä jakelukytkimiin 1000Base-SX-yhteyksillä. Suunnitelma on esitelty kuvassa 17.

Jotta videon viive voitaisiin pitää mahdollisimman alhaisena, jakeluverkon nopeus Helsingin toimipisteessä päätettiin nostaa 10 Gbit:iin/s. B- ja C-jakamoiden välisen kuituosuuden matkaksi tulisi nykyisellään yli 330 m. B-jakamon laitepaikan sijainti on kuitenkin päätetty muuttaa 50 m lähemmäksi C-jakamoon nähden. Nämä suunnitelmat toteuttamalla kuituyhteyden kokonaispituus näiden jakamoiden välillä saadaan lyhennettyä 10GBase-SR-standardin mukaiseksi. Samalla saadaan tulevia tarpeita ajatellen vedettyä myös nykyisen 6-kuituisen tilalle 12-kuituinen kaapeli.

Koska uudet kytkimet tukevat useampia SFP-paikkoja (SFP, Small Fromfactor Pluggable) kuin osa tällä hetkellä käytettävissä olevista kytkimistä, verkon rakennetta voidaan muuttaa käytännöllisemmäksi niin, ettei tarvitse tehdä epäjohdonmukaisia ristikytkentöjä seuraavalle SFP-paikkoja vapaana olevalle kytkimelle. Vanhojen kytkinten SFP-paikkojen rajallisuus on osaltaan aiheuttanut alkuperäisen varsin kaoottisen kytkinasetelman.

Lopullisessa suunnitelmassa virtuaalinen keskuskytkin asetetaan toimimaan oletusreitittimenä Helsingin toimipisteen kameraverkolle ja se asetetaan Asiakkaan kameraverkon ryhmälähetysten kohtaamispisteeksi. Näin vältetään tilanne, jossa kuormitetaan varsinaista WAN-yhteyksiin (WAN, Wide Area Networks) käytettävää reititintä liikaa, ja lisäksi voidaan ehkäistä tilanne, jossa reitittimen 1 Gbit/s -portit kuormittuisivat Helsingin kameraverkosta ja muista siihen kytköksissä olevista verkoista suuntautuvasta ryhmälähetysliikenteestä. WAN-reitittimen tehtävinä ovat pääasiassa vain tunneloinnit etätoimipisteisiin ja tunneloidun liikenteen salaus. Etäyhteydet toteutetaan GRE-tunnelein (GRE, Generic Routing Encapsulation), joilla saadaan ryhmälähetystoiminnallisuus Internet-yhteydellä etätoimipisteille, ja data salataan IPsec VPN -toteutuksella (IPsec, IP security; VPN, Virtual Private Network).

Asennus toteutetaan budjetointisyistä kahdessa osassa, joista vain ensimmäinen osuus kuuluu tämän insinöörityön piiriin. Toteutus on esitelty kuvassa 18.



Kuva 18. Insinöörityössä toteutettava topologia.

Insinöörityössä toteutettavassa topologiassa D-jakamon laitetilan kytkin jätetään vaihtamatta. D-jakamon kytkin jätetään reunakytkimeksi ja se yhdistetään jakeluverkkoon 1000Base-SX-yhteydellä C-jakamon kytkimen kautta. Lisäksi toinen E-jakamon kytkimistä jätetään toistaiseksi asentamatta ja E-jakamon kytkös päävalvomon IRF-pinoon jätetään tekemättä. Myös suunnitellut reunakytkinten vaihdot A5120-sarjan kytkimiin jätetään toteuttamatta. Samoin kahdennetut virtalähteet asennetaan vasta myöhemmin, UPS-järjestelmän päivityksen yhteydessä.

Asiakkaan kameraverkossa ryhmäosoitteet määräytyvät siten, että ryhmälähetysdataa lähettävän kameran IP-osoitteen kaksi ensimmäistä oktettia korvataan 239.255:llä ja loput kaksi oktettia vastaavat kameran IP-osoitetta. Kytkimistä tarkistetaan, että niissä on IGMP snooping -toiminnallisuus käytössä. Lisäksi tarkistetaan, että IGMP-ryhmät kirjautuvat kytkimelle.

Koska asiakkaalle on tässä tapauksessa asennettu erillinen kameraverkko, jonka pääasiallinen liikenne on nimenomaan videodataa, ei ole mielekästä asettaa videolle

muita korkeampaa prioriteettia. Sen sijaan kameran ohjausdatalle annetaan normaalia korkeampi prioriteetti.

HP:n kytkimissä on mahdollisuus muokata puskureiden käyttöä varsin monipuolisesti. Kytkimissä käytetään sekä porttikohtaisia puskureita että jaettua puskuria, joita käytetään porttikohtaisten puskureiden loputtua kesken. Kytkimissä otetaan käyttöön ns. burst-mode. Tällöin kytkin tekee päätöksiä dynaamisesti muuttuvien olosuhteiden mukaan. Burst-mode otetaan käyttöön komennolla *burst-mode enable.* [27.]

5.2 Testaus

Testausta tehdään silmämääräisin havainnoin, pakettikaappauksin sekä tarkastelemalla kytkinten loki- sekä statistiikkatietoja. Lisäksi testataan kamerajärjestelmän videoviive kuvakaappauksin.

Myös RRPP-renkaan toiminta halutaan testata. Testaukseen käytetään kolmen RRPP-kytkimen testirengasta, johon kuuluvat virtuaalinen keskuskytkin sekä A- ja B-jakamot, jolloin kussakin yhteydessä pysytään 10GBase-SR-yhteyden asettamassa 300 m:n rajoissa.

5.3 Projektin vastuunjako

Projekti on jaettu seuraaviin osioihin: suunnittelu, hankinta, kytkinasennukset, kaapeloinnit, kytkinasetukset, testaus, reititinasetukset ja projektin johto. Mikäli tarvitaan vaativia reititinasetusten muutoksia, niiden tekemiseen käytetään alihankkijaa. Tarvittavissa kuitukaapelointiasennuksissa ja -hitsauksissa käytetään myös alihankkijaa. Kaikki muut projektin osa-alueet kuuluvat tämän insinöörityön tekijälle.

5.4 Ylläpito

Laitteiden tilan seurantaan käytetään SNMP-protokollaa (SNMP, Simple Network Management Protocol). Laitteiden prosessorikuormitusta, muistin käyttöä, lämpötilaa ja

porttien käyttöastetta seurataan. Lisäksi kytkimet ilmoittavat statusmuutoksista SNMP-Trap-viestein. SNMP-järjestelmä ilmoittaa virhetilanteista sähköpostilla tikettijärjestelmään ja lähettää myös tarvittaessa SMS-viestit (SMS, Short Message Service) ylläpidon matkapuhelimiin. Kaikki järjestelmän tuottama lokitieto kerätään syslog-palvelimelle. Lopullisessa toteutuksessa kytkinasetuksia ylläpidetään TFTP-palvelimella (TFTP, Trivial File Transport Protocol). Kytkimien tuuletusritilät puhdistetaan pölystä puolivuosittain ja samalla tarkistetaan, että johdot ja liittimet ovat kunnolla kiinni laitteissa.

Ylläpidossa käytetään myös HP:n omaa hallintasovellusta, jolla voi hallita sekä HP:n että Ciscon laitteita. Kytkimillä on elinikäinen Next Business Day -vaihtotakuu. HP A5800-24G-PoE EI -kytkimen vikaantumistiheyttä kuvaava MTBF-arvo (MTBF, Mean Time Between Failures) on valmistajan mukaan 35 vuotta.

6 Verkon asennus

6.1 Laiteasennukset

Asennukset sujuivat hyvin suunnitelman mukaisesti. Merkittävin havaitsemani ero HP:n ja aiemmin käyttämieni Ciscon kytkinten asennuksissa oli se, että kun Ciscon kytkimissä STP ja IGMP snooping ovat oletuksena käytössä, niin HP:n kytkimissä ne tuli ottaa erikseen käyttöön. Kun aluksi asensin HP:n kytkimen verkkoon ottamatta STP:tä kytkimellä käyttöön, Ciscon kytkin asetti HP:n kytkimeen vievän portin estettyyn tilaan. Kun otin HP:n kytkimellä STP:n käyttöön, alkoi verkko toimia ongelmitta. Yhteyksien nopeuden nostot eivät aiheuttaneet ongelmia, vaan kaikki 10GBase-SR-yhteydet lähtivät toimimaan alusta alkaen hyvin.

Eniten työtä jouduttiin tekemään B-jakamon kytkimen asennuksessa, koska samalla laitekaappia siirrettiin 50 m. Nämä työvaiheet esitetään seuraavaksi.

Ennen B-jakamon kytkimen asennusta alihankkija oli asentanut uuden laitekaapin paikalleen, vetänyt OM3-valokuitukaapelin valmiiksi A-jakamosta uuteen laitekaappiin ja hitsannut kuidut. Alihankkija oli myös asentanut kameroita varten CAT6-kaapelit (CAT6, Category 6) uuteen laitekaappiin. Ongelmallisinta oli toteuttaa kuituyhteyksien vaihdos niin, että palvelulle tulisi mahdollisimman pieni katkos.

Asensin ensin uuden B-jakamon kytkimen uuteen laitekaappiin ja yhdistin sen A-jakamon kytkimeen uudella valokuitukaapelilla. Sitten vaihdoin kamerayhteydet uudelle kytkimelle. Tämän jälkeen siirsin kaikki vanhan B-jakamon kautta kulkevat yhteydet, muun muassa C-jakamon yhteyden, kulkemaan toista kuitureittiä. Asensin pohjoissiiven toiseen kerrokseen oman tallentimen yliheiton ajaksi, koska sinne vedetty valokuitukaapeli oli päätetty ainoastaan B-jakamon vanhaan laitetilaan. Muutoin tallennusyhteyteen olisi tullut tuntien katkos kuitukaapelin siirtämisen ja kuituhitsauksien ajaksi.

Tallentimen asentamisen jälkeen katkaisin B-jakamon vanhassa laitekaapissa C-jakamon ja pohjoissiiven toisen kerroksen valokuitukaapelit. Sitten vedin katkaistut kuitukaapelit uuteen tilaansa B-jakamossa. Alihankkija hitsasi ja mittasi kuidut. Kuitujen mittausten yhteydessä alihankkija havaitsi, ettei yhdessä kaapelissa olleita kuituja oltu alun perin järjestetty kaapelivalmistajan värikoodien mukaan. Kuitujen järjestys vaihdettiin vastaamaan valmistajan ohjeita. Tämän jälkeen nämä kuituyhteydet otettiin jälleen käyttöön. Yhteydet alkoivat toimia ja kuituyhteys C-jakamoon palautettiin kulkemaan B-jakamon kautta.

6.2 Asetusten teko

6.2.1 Intelligent Resilient Framework -asetukset

Liitin suunnitelman keskuskytkinkokoonpanoon kuuluvat kytkimet omaksi virtuaaliseksi laitteeksi HP:n IRF-ohjelmointiohjeen mukaisesti. Valitsin isäntäkytkimeksi päävalvomoon ensimmäisenä asentamani kytkimen. Asetin isäntäkytkimen jäsennumeron (MemberID) 1:ksi ja asetin sille korkeimman prioriteetin. Tein kytkennän IRF-porttien välillä. Ohjelmoinnit tein laitteiden sarjaporttien kautta.

Näin muodostunut virtuaalinen kytkin alkoi toimia ongelmitta. Kaikki tämän jälkeen suoritettavat ohjelmointitoimenpiteet koskevat molempia kytkimiä.

6.2.2 Palvelunlaatuasetukset

Määritin valvomokoneiden kytkinportteihin palvelunlaatuasetukset (QoS, Quality of Service) siten, että kameran ohjausdatalle asetetaan ylennetty prioriteetti. Tässä tapauksessa prioriteetiksi asetetaan 6, 7:n ollessa ylin ja 0:n ollessa alin prioriteetti. Videolle varasin prioriteetin 5 jatkoa ajatellen. Käytin priorisointiin IEEE 802.1p -toteutusta.

Aluksi loin pääsylistan (ACL, Access Control List), johon valvomokoneen porttiin tulevaa dataa verrataan. Määritin pääsylistaan TCP-portin 1443 auditointiyhteyttä varten

sekä kameran kontrolliportit TCP 49500–49509. Näiden komentojen suorittaminen on esitelty kuvassa 19.

```
[Asiakas-hki-C-jakamo-sw] acl number 3000 name Control-QoS
[Asiakas-hki-C-jakamo-sw-acl-adv-3000-Control-QoS] rule permit tcp
destination-port eq 1443
[Asiakas-hki-C-jakamo-sw-acl-adv-3000-Control-QoS] rule permit tcp
destination-port range 49500 49509
```

Kuva 19. ACL-määritysten tekeminen liikenteen luokittelua varten.

Määrittelin tämän jälkeen ”liikenteen luokittelijan” komennolla *traffic-classifier* ja määritin sille ehdoksi edellä mainitun pääsylistan. Määrittelin myös ”käyttäytymisen” *traffic behavior* -komennolla ja asetin sille prioriteetiksi 6. Nämä toimenpiteet on esitelty kuvassa 20.

```
[Asiakas-hki-C-jakamo-sw]traffic classifier Control-Class
[Asiakas-hki-C-jakamo-sw -classifier-Control-Class]if-match acl name
Control-Qos
[Asiakas-hki-C-jakamo-sw]traffic behavior Control-Behavior
[Asiakas-hki-C-jakamo-sw-behavior-Control-Behavior] remark dot1p 6
```

Kuva 20. Prioriteetin määrittäminen.

Seuraavaksi loin QoS-käytännön ja linkitin aiemmin luodun luokittelijan ja käyttäytymismallin käytäntöön. Lopuksi liitin luodun QoS-käytännön valvomokoneen käyttämään kytkimen porttiin kuvassa 21 esitetyin komennoin.

```
[Asiakas-hki-C-jakamo-sw] qos policy Control-Policy
[Asiakas-hki-C-jakamo-sw-qospolicy-Control-Policy] classifier
Control-Class behavior Control-Behavior
[Asiakas-hki-C-jakamo-sw -GigabitEthernet1/0/1] qos apply
policy Control-Policy inbound
```

Kuva 21. QoS-käytännön luominen ja käyttöönotto.

Näin QoS-määritykset on otettu käyttöön päävalvomokoneen portissa ja siihen tulevat kontrollikomennot lähetetään eteenpäin ylennetyllä prioriteetilla.

6.2.3 Rapid Ring Protection Protocol -asetukset

RRPP vaatii STP:n poistamisen käytöstä niistä porteista, joissa käytetään RRPP-protokollaa. Tämän takia suljin ensin ohjelmallisesti testirenkaassa keskuskytkimeltä A-jakamoon johtavan kytkinportin. Sitten poistin STP:n käytöstä testirenkaan porteista.

Seuraavaksi tein RRPP-renkaan toimialueasetukset keskuskytkimellä RRPP-ohjeen mukaisesti. Valitsin keskuskytkimen isäntälaitteeksi *node-mode master* -komennolla. Määritin A-jakamoon johtavan portin ensisijaiseksi portiksi ja B-jakamoon johtavan toissijaiseksi. Lopuksi otin RRPP-protokollan käyttöön juurikomennolla *rrpp enable.* Komennot on esitelty kuvassa 22.

```
[Asiakas-Helsinki-Core]  rrpp domain 1
Info: Create a new domain.
[Asiakas-Helsinki-Core-rrpp-domain1] control-vlan 101
[Asiakas-Helsinki-Core-rrpp-domain1] protected-vlan reference-
instance 0 to 32
[Asiakas-Helsinki-Core-rrpp-domain1] ring 1 node-mode master primary-
port Ten-GigabitEthernet 2/0/25 secondary-port Ten-GigabitEthernet
1/0/28 level 0
[Asiakas-Helsinki-Core-rrpp-domain1] ring 1 enable
[Asiakas-Helsinki-Core] rrpp enable
```

Kuva 22. RRPP-porttien määrittäminen isäntäkytkimellä.

Tein samat toimenpiteet myös A- ja B-jakamoiden kytkimien renkaaseen liittyville porteille poistamalla niistä STP:n käytöstä. Erona oli se, että nämä kytkimet asetettiin välityskytkimiksi *node-mode transit* -komennolla.

Kun olin ohjelmoinut kaikki kolme kytkintä, avasin keskuskytkimeltä ohjelmallisesti suljetun A-jakamon portin. Tämän jälkeen tarkistin keskuskytkimeltä RRPP-tilatiedot. Tarkistin ensin tilastotiedot, jotka on esitelty liitteessä 2 kuvassa 1.

Tilastotiedoista voidaan havaita, että keskuskytkin on alkanut vastaanottaa lähettämiään RRPP Hello -viestejä toissijaisesta portistaan. Lisäksi RRPP-linkin asettuminen normaalitilaan on aiheuttanut *Common Flush FDB* -viestin lähetyksen kytkimeltä välityskytkimille. Liitteen 2 kuvasta 2 voidaan myös havaita, että RRPP-linkki on

toiminnassa. Isäntäkytkimen toissijainen portti on estettynä normaalitilanteessa. Renkaan tilatiedoksi on merkitty *Complete*, mikä tarkoittaa normaalia tilaa.

7 Verkon testaus

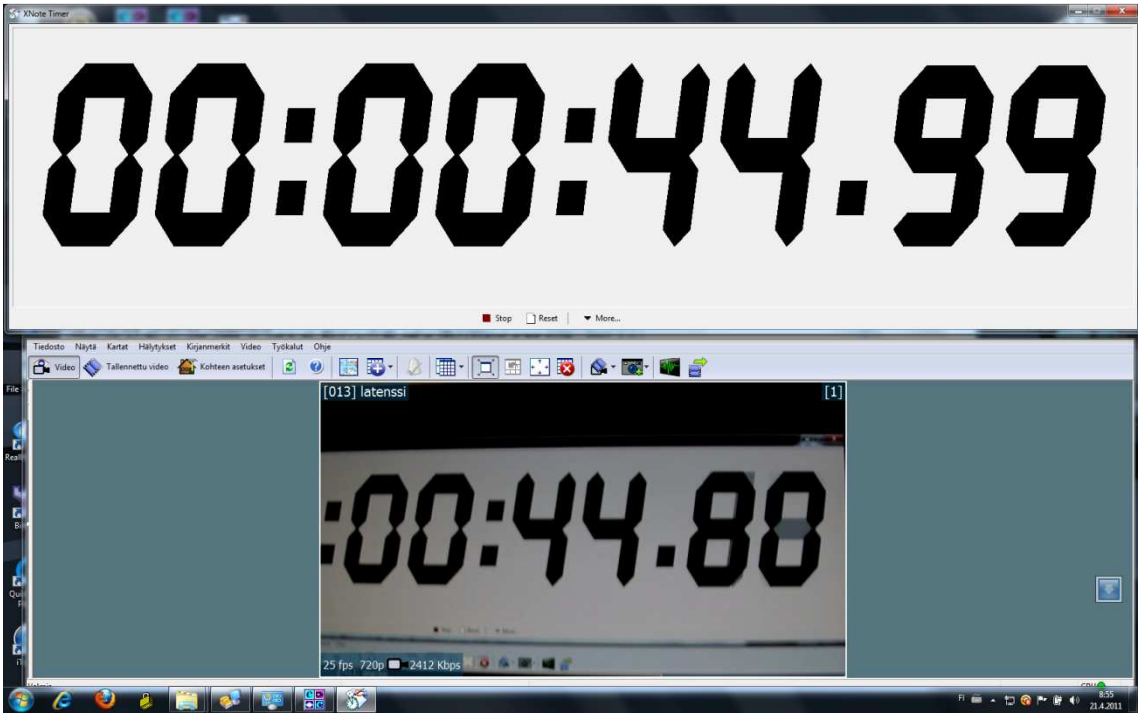
7.1 Viiveen testaus

Mittasin videon koodauksen, lähetyksen ja dekoodauksen viivettä seuraavasti: laitoin kameran ja kannettavan tietokoneen E-jakamossa eri VLAN-verkkoihin (VLAN, Virtual Local Area Netework). Käynnistin kannettavassa tietokoneessa ajanottosovelluksen ja asetin kameran kuvaamaan tietokoneen ruudulla tätä ajanottoa. Sitten käynnistin valvomosovelluksen, jolla näytettiin kameran kuvaamaa aikaa ajanottosovelluksen alla. Ajanottosovelluksen näyttämä aika vastasi testissä reaaliaikaa ja valvomosovelluksen näyttämä aika viiveellistä aikaa. Näin ajanottosovelluksen näyttämän ajan ja valvomosovelluksen näyttämän ajan erotuksesta saadaan videon viive. Otin näistä aikapareista kuvakaappauksia viiveen mittaamiseksi. Testiasetelma on esitelty kuvassa 23.

Kuva 23. Viiveen mittaamiseen käytetty testiasetelma.

Käytin kamerana IndigoVisionin 11000HD-kameraa. Suoratoistin videota 4 Mbit/s -virtana 25 kuvaa sekunnissa HD 720p -tarkkuudella ja H.264-enkoodauksella. Käytin valvomosovelluksena IndigoVisionin Control Center -ohjelmistoa versiolla 3.19.4. Tietokone oli HP 6730b -merkkinen. Ajanottosovellus oli XNote Timer, jonka versio oli 1.11.

Pienensin valvomosovelluksen niin, että sain kamerakuvan sopivasti ajanottokellon alle. Testissä suoratoistettu video siirtyi koko 10 Gbit/s -kytkinverkon yli reitittimelle ja takaisin. Tein testit käyttäen UDP-täsmälähetystä.



Kuva 24. Videoviiveen referenssikuva. Ylempi kuva vastaa reaaliaikaa ja alempi viiveellistä aikaa.

Kuvasta 24 voidaan havaita, että viive testissä on 19 sadasosasekuntia, kun ylempi kuva (reaaliaika) on 44,99 s ja alempi kuva (viiveellinen aika) on 44,80 s eli aikaero on 190 ms. Eri kuvapareja vertailemalla sain 10 kuvakaappauksen otoksella videoviiveen keskiarvoksi 206 ms, keskiarvon keskivirheen ollessa 6 ms. Mittaustulokset on esitelty taulukossa 4. Tämän johdosta voidaan todeta, että järjestelmä täyttää sille asetetun 300 ms:n maksimiviivevaatimuksen.

Taulukko 4. Videoviive kameraverkossa.

Mittaus	Kello (ms)	Kamera (ms)	Erotus (ms)
1	10440	10260	180
2	9730	9510	220
3	9780	9580	200
4	57370	57190	180
5	5000	4790	210
6	44990	44800	190
7	10450	10220	230
8	20530	20310	220
9	43780	43550	230
10	12120	11920	200
		Keskiarvo	206
		Keskihajonta	18.97366596
		Keskivirhe	6.00

Vertailun vuoksi tein vastaavan testin myös laittamalla kameran suoraan kannettavaan tietokoneeseen kiinni. Tein myös tästä testistä 10 kuvaparin otoksen. Tässä testissä sain videoviiveen keskiarvoksi 202 ms, keskiarvon keskivirheen ollessa 6 ms. Tämän mittauksen arvot on esitelty taulukossa 5.

Taulukko 5. Videoviive kameran ollessa suoraan yhteydessä tietokoneeseen.

Mittaus	Kello (ms)	Kamera (ms)	Erotus (ms)
1	10750	10530	220
2	45180	44950	230
3	4880	4680	200
4	33810	33590	220
5	13350	13160	190
6	8800	8620	180
7	10340	10140	200
8	17270	17060	210
9	14160	13980	180
10	12510	12320	190
		Keskiarvo	202
		Keskihajonta	17.51190072
		Keskivirhe	5.537749242

Tämän testin perusteella voidaan todeta, että suurin viive videoon aiheutuu enkoodauksessa ja dekoodauksessa.

7.2 Kiertoaikatestit

Tein kiertoaikatestit samalla kokoonpanolla ja samassa sijainnissa kuin edellä mainitut viivetestit. Testasin kiertoaikoja eri VLAN-verkoissa olevien kameran ja kannettavan tietokoneen välillä ICMP-kaiutuspyyntöjä (ICMP, Internet Control Message Protocol) käyttäen. Käytin kiertoaikatesteihin pieniä 32 tavun paketteja ja fragmentoituvia 5000 tavun paketteja. Molempia paketteja lähetettiin 100 kappaletta. Tein jälleen vertailun vuoksi samat testit myös kytkemällä kameran suoraan tietokoneeseen kiinni.

Kun testasin kiertoaikoja 32 tavun paketeilla, en havainnut käytännössä mitään eroa kiertoajoissa lähetettäessä ICMP-kaiutuspyyntöjä verkossa tai suoraan kameralle. Molemmissa testeissä 100 paketin otoksella kiertoajan keskiarvoksi tuli 2,6 ms keskiarvon keskivirheen ollessa 0,2 ms.

Kun testasin kiertoajat 5000 tavun paketeilla, sain eroa näkyviin. Suoraan kameraan kytkettynä keskiarvoksi muodostui 3,9 ms ja keskiarvon keskivirhe oli 0,2 ms. Verkossa lähetettynä kiertoajan keskiarvo oli 8,7 ms keskiarvon keskivirheen ollessa 0,3 ms.

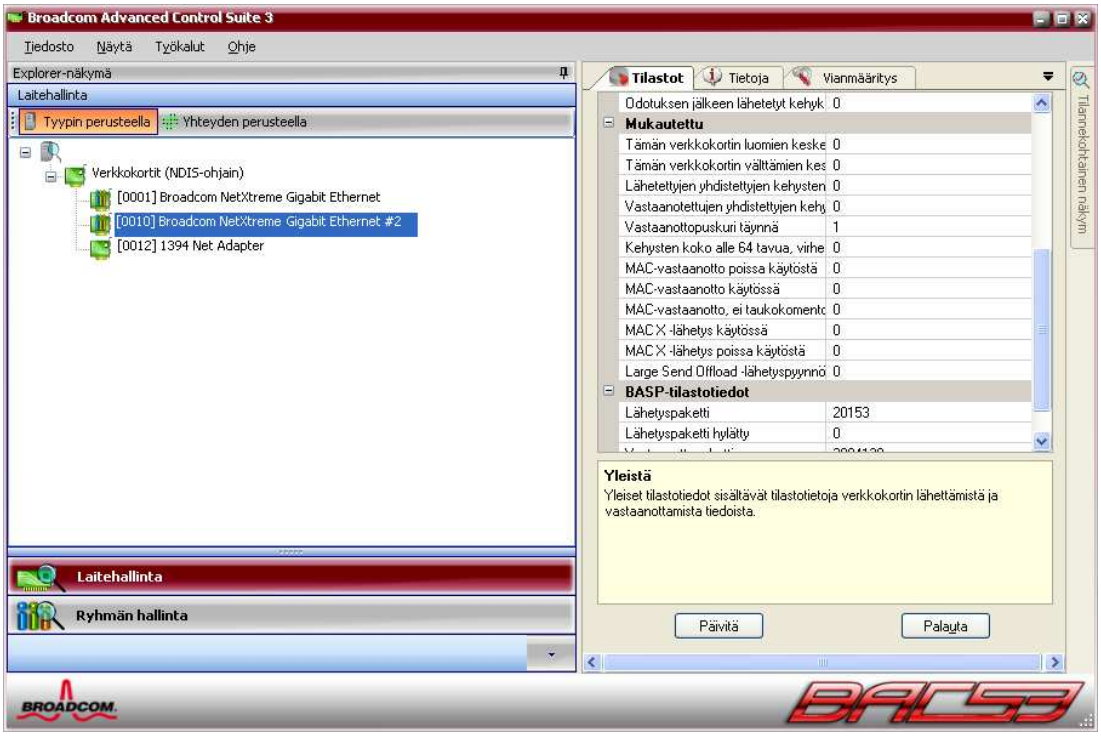
Kiertoaikatestin tulos on verkon vaatimuksia ajatellen riittävän hyvä, sillä videoviivetestien perusteella viivebudjetiin jäi varaa noin 100 ms kameran ohjausviiveelle.

7.3 Pakettikaappaukset valvomokoneelta

Otin valvomokoneelta pakettikaappauksia mahdollisten verkon ongelmien löytämiseksi. Valvomokoneella vastaanotettiin 26 H.264-enkoodattua suoratoistoa. Tällä pyrittiin tarkistamaan tietokoneen vastaanottamaa dataa normaalissa valvontakäytössä. Myös tietoliikenneverkko oli muutenkin normaalissa tuotantokäytössä. Valvomotietokoneena käytettiin HP:n XW8600-työasemaa kahdella 2,83 GHz:n neliydinprosessorilla. Käyttöjärjestelmänä oli Windows XP Professional 32-bittisellä versiolla. Vastaanotettaessa 26 suoratoistoa kukin kahdeksasta ytimestä oli noin 80 %:n kuormituksessa. Testeillä pyrittiin saamaan selville, jääkö kameroiden lähettämiä paketteja saapumatta

valvomokoneelle normaalissa tuotantokäytössä. Otin pakettikaappaukset valvomokoneelta WireShark-ohjelmistolla.

Koska kukin suoratoisto oli noin 4 Mbit:n/s luokkaa, tuli pakettikaappauksista hyvin suuria tiedostoja, ja siksi kaappaukset täytyi pitää lyhyinä, noin kolmen minuutin mittaisina. En havainnut näissä pakettikaappauksissa mitään poikkeamia enkä pakettihäviötä. Kun kaappausaikaa pidennettiin yli kolmeen minuuttiin, tapahtui kaappauksen aiheuttaman ylimääräisen kuormituksen vuoksi valvomokoneen vastaanottopuskurin ylivuoto, minkä vuoksi joitakin paketteja menetettiin pakettikaappauksesta. Ylivuoto on esitetty kuvassa 25. Ylivuoto-ongelma toistui testeissä systemaattisesti. En kuitenkaan havainnut ylivuodon yhteydessä kuvassa ylimääräistä nytkähdystä, eikä vastaanoton puskurin ylivuotoa tapahtunut tuotanto-käytössä silloin, kun pakettikaappaus ei ollut käynnissä.



Kuva 25. Valvomokoneen verkkokortin vastaanottopuskurin ylivuoto.

Valvomokoneessa käytössä olleen Broadcomin verkkokortin vastaanottopuskurin kokoa ei valitettavasti päässyt säätämään toisin kuin joidenkin muiden verkkokorttien, mutta

ainakaan se ei silmämääräisen havainnon perusteella ollut liian suuri aiheuttaakseen merkittävää viivettä videoon.

Pakettikaappaustesti osoitti, että suunniteltu testiympäristö ei ollut tarkoituksenmukainen, koska itse testi aiheutti virheen järjestelmän toimintaan. Laitteiden suorituskyky tuli vastaan liian suurten lähetysnopeuksien vuoksi. Jatkossa tulisikin kehittää muita menetelmiä 10 Gbit/s -verkon virheiden mittaamiseen.

Pyrin selvittämään myös ohjausviivettä valvomon pakettikaappauksin. Havaitsin pakettikaappauksesta, että kameralta tuli kuittausviesti ohjauskomennosta 9 ms:ssa ohjausyhteyden aloittamisesta, TCP-kättely mukaan lukien. Tulos sijoittui hyvin 100 ms:n varmuusrajoihin. Toisaalta on hyvä olla runsaasti varmuusrajaa, sillä kaikki viiveen tyypit suurenevat reititettäessä videota etätoimipisteisiin.

7.4 Kytkinten tilastotiedot

Kun kameraverkko oli ollut normaalissa käytössä yli vuorokauden, tarkastelin kytkinten runkoporttien tilastotietoja. En havainnut jakeluverkon tilastotiedoissa mitään virheitä tarkastelujaksolla. Yhden kytkinportin tilastotiedot on esitelty liitteessä 3. Tarkastellessani päävalvomon kytkimen IGMP-tietoja havaitsin, että siihen oli kirjattuna 127 IGMP-ryhmää, kuten voidaan havaita kuvasta 26, joten IGMP snooping toimi kytkimissä odotetusti.

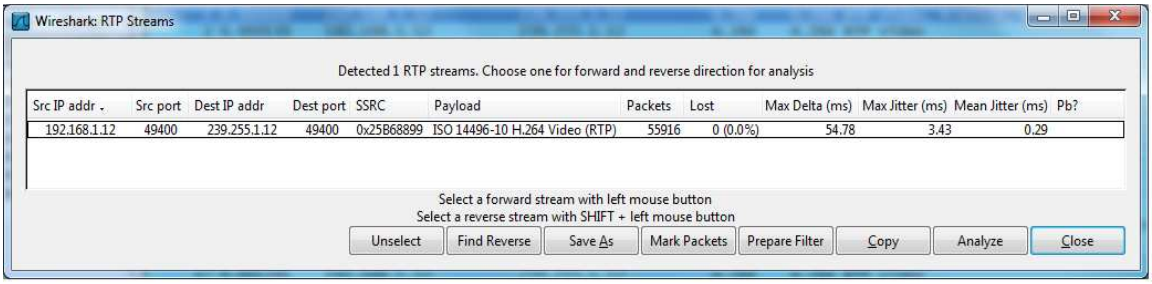
```
[Asiakas-Helsinki-Core]display igmp-snooping group
  Total 127 IP Group(s).
  Total 127 IP Source(s).
  Total 127 MAC Group(s).
```

Kuva 26. IGMP-ryhmien lukumäärä keskuskytkimellä.

7.5 Rapid Ring Protection Protocol -testit

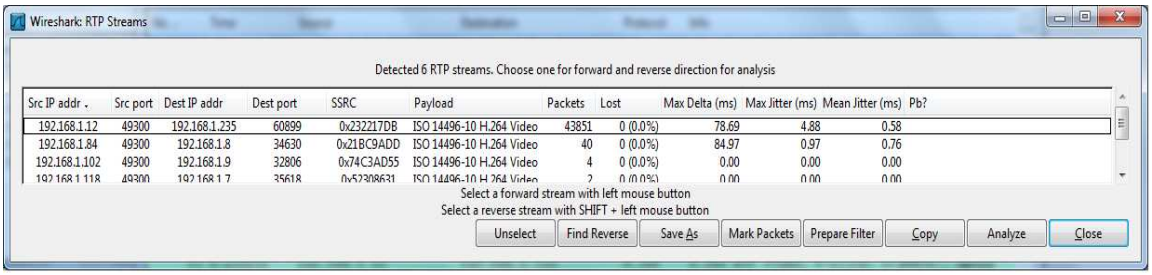
7.5.1 Täsmälähetyksen palautuminen renkaassa

Testasin myös asennetun RRPP-renkaan toimintaa pakettikaappauksin. Suoratoistin testissä videota kameralta, joka sijaitsi A-jakamossa, keskuskytkimeen kytketyllä kannettavalla tietokoneella. Käytin pakettikaappauksessa WireShark-ohjelmiston versiota 1.0.8. Testasin RRPP-renkaan palautumista vikatilanteessa irrottamalla kuituyhteyden A- ja B-jakamoiden välillä sekä sulkemalla kyseisen yhteyden *shutdown*-komennolla A-jakamon kytkimeltä. Testasin samoin RRPP-renkaan palautumisen normaaliin tilaan. Tein testit sekä UDP-täsmälähetyksenä että -ryhmälähetyksenä. HD-kameran videota suoratoistettiin 4 Mbit/s, kuvatahti oli 25 kuvaa sekunnissa. Aluksi tein noin kolme minuuttia kestävän testin normaalissa tilassa suoratoistamalla videota UDP-ryhmälähetyksenä ilman katkoksia. Pakettikaappauksen antama tilastotieto on kuvassa 27. Kaikissa kuvakaappauksissa mustalla kehystetty rivi on testin osalta oleellinen.



Kuva 27. Yhden kameran videovirran tiedot normaalissa tilassa.

Statistiikkatiedoista voidaan havaita pakettien maksimivälin olevan normaalitilanteessa likimäärin 50 ms:n luokkaa. Koska RRPP-linkki palautuu valmistajan mukaan 50 ms:ssa, *Max Delta* -arvon ei tulisi ylittää 100 ms:a. Seuraavaksi suoratoistin kuvaa UDP-täsmälähetyksenä ja irrotin A- ja B-jakamoiden välisen linkin. Tämän testin pakettikaappauksen statistiikkatiedot on esitelty kuvassa 28.



Kuva 28. Välityskytkimien välinen kuituyhteys irrotettu täsmälähetystestissä.

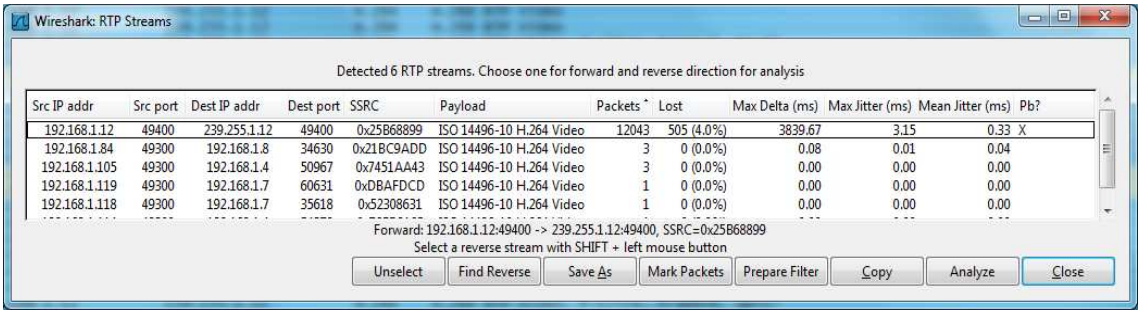
Kuvakaappauksen kehystetystä rivistä voidaan havaita, että *Max Delta* -arvo oli noussut 78,69 ms:iin, mikä osoittaa, että katkos aiheutti pienen viiveen saapuvien pakettien välillä. Yhtään pakettia ei kuitenkaan menetetty katkoksen takia. Tarkistin RRPP-renkaan tiedot isäntäkytkimeltä. Listaus on esitelty liitteessä 2 kuvassa 3. Tiedoista voidaan havaita, että isäntälaite on tunnistanut, että rengas on vikatilassa ja aktivoinut toissijaisen portin käyttöön. Tarkistin myös RRPP-tilastotiedot. Nämä tiedot on esitetty liittessä 2 kuvassa 4. Tilastotiedoista voidaan todeta, että isäntälaite oli saanut yhteyden katkeamisesta tiedon sekä B-jakamon että A-jakamon kytkimiltä *Link Down* -viestillä, sillä se on kirjautunut molempien porttien tietoihin.

Seuraavaksi testasin yhteyden palautumista kytkemällä takaisin välityskytkimien välisen kuituyhteyden. Tässä pakettikaappauksessa *Max Delta* -arvo oli 83,66 ms ja paketteja oli menetetty yhteyden palautuessa 11.

Kokeilin samat asiat vertailun vuoksi sulkemalla ja avaamalla A- ja B-jakamoiden välisen yhteyden komentokehotteelta *shutdown*-komennolla. Tällöin yhteyden sulkeminen ei käytännössä aiheuttanut vikaa suoratoistossa. Katkos oli lähes olematon *Max Delta* -arvon ollessa 59,51 ms. Samoin kävi yhteyden palautuessa: *Max Delta* -arvo oli 54,81 ms. Yhteyden palautumisen yhteydessä menetettiin 11 pakettia.

7.5.2 Ryhmälähetyksen palautuminen renkaassa

Seuraavaksi oli ryhmälähetystestin vuoro. Tein ryhmälähetykselle samat testit kuin täsmälähetykselle. Ensimmäisenä testasin yhteyden palautumista irrottamalla kuidun A- ja B-jakamoiden välillä, mistä on esitetty pakettikaappauksen tilastotiedot kuvassa 29.



Kuva 29. Välityskytkimien välinen kuitu irrotettu ryhmälähetystestissä.

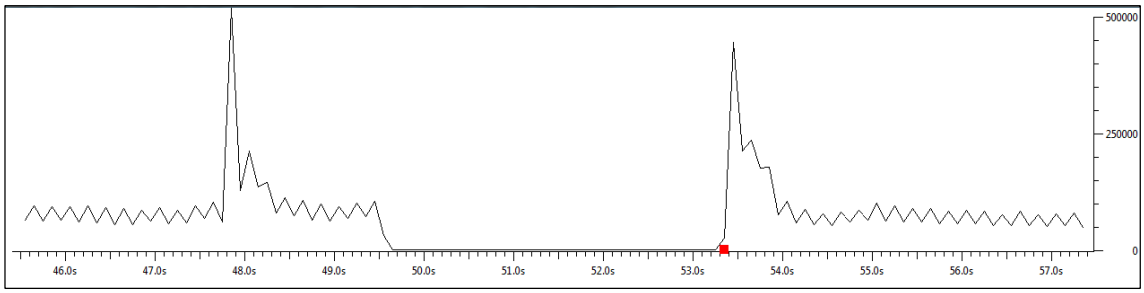
Nyt ilmeni selvä vikatilanne. *Max Delta* -arvo oli lähes neljä sekuntia. Paketteja menetettiin 505. Jälleen testasin palautumisen myös kytkemällä kuituyhteyden takaisin. Tilanne yhteyden kytkemisen yhteydessä oli jopa pahempi kuin irrotettaessa, ryhmälähetysvirta keskeytyi yli seitsemäksi sekunniksi.

Ryhmälähetyksenkin kohdalla samat testit tehtiin myös sulkemalla ja avaamalla yhteys komentokehotteelta. Molemmissa testeissä ryhmälähetykseen aiheutui hieman yli sekunnin katkos.

Yhteenvetona tehdyistä testeistä voidaan ensinnäkin todeta, ettei katkoksen aiheuttamistavalla ollut käytännössä merkitystä yhteyden palautumisajan kannalta. Toisaalta 50 ms:n palautuminen koskee vain täsmälähetystä. Koska täsmälähetystä käytetään tallennuksessa ja ryhmälähetystä pääsääntöisesti vain valvonnassa, ei ryhmälähetyksen palautuminen yli 50 ms:ssa ole kriittinen vika. Toisaalta kameravalvontajärjestelmän käytettävyyden kannalta on tärkeää, että myös ryhmälähetys palautuisi niin nopeasti kuin mahdollista, vähintään alle sekunnissa. Päätinkin tutkia asiaa lisää.

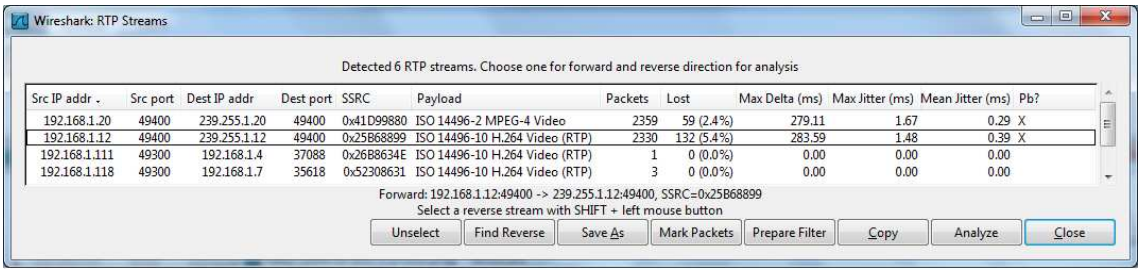
Havaitsin pakettikaappauksista, että katkon jälkeen ryhmälähetysyhteys palautui välittömästi seuraavan PIM Hello -viestin jälkeen. Kuvassa 30 on esitetty ryhmälähetyksen palautuminen PIM Hello -viestin jälkeen. PIM Hello -viestejä, joita toisinaan nimitetään myös PIM Query -viesteiksi, lähetetään Cisco-reitittimeltä oletuksena 30 sekunnin välein. Näin ollen *query-interval*-arvoa pienentämällä voidaan nopeuttaa ryhmälähetysyhteyden palautumista topologiamuutoksen jälkeen. Kokeilin nopeuttaa

palautumista muuttamalla reitittimen LAN-portin (LAN, Local Area Network) *query-interval*-arvoksi 500 ms komennolla *ip pim query-interval 500 msec*. [28.]



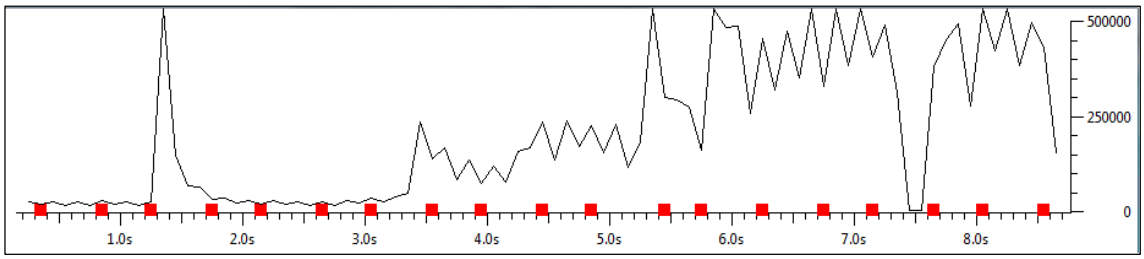
Kuva 30. Ryhmälähetys palautuu välittömästi PIM Hello -viestin jälkeen. PIM Hello -viesti on merkitty punaisella pisteellä.

Query-interval-arvon muuttaminen nopeutti huomattavasti ryhmälähetysyhteyden palautumista. Tein kolme testiä sulkemalla sekä palauttamalla A- ja B-jakamoiden välisen yhteyden komentokehotteelta: jokaisessa testissä ryhmälähetysyhteys palautui alle 500 ms:ssa. Kuvassa 31 on esitetty yksi esimerkki, jossa testi on tehty kahdella kameralla.



Kuva 31. Ryhmälähetyksen palautuminen katkoksesta query-interval-*arvon muuttamisen jälkeen.*

Kuten kuvasta voidaan havaita, palautuminen oli nyt alle 500 ms. Kuvassa 32 on esitetty PIM Hello -viestien lähetys suhteessa katkokseen. Katkos tapahtuu noin 7,5 s:n kohdalla.



Kuva 32. Ryhmälähetyksen palautuminen muutoksen jälkeen. PIM Hello -viestien lähetysväliksi on asetettu 500 ms. PIM Hello -viestit on merkitty punaisella pisteellä.

Katkos on selvästi aiempaa lyhyempi, koska PIM Hello -viestejä lähetetään nyt useammin. *Query-interval*-arvoa voitaisiin vieläkin pienentää, mutta se jätettiin 500 ms:iin toistaiseksi reitittimen ylimääräisen kuormituksen välttämiseksi. Ryhmälähetyksen palautuminen vasta PIM Hello -viestin yhteydessä osoittaa, että toisin kuin STP, RRPP ei levitä ryhmälähetystä topologiamuutoksen yhteydessä.

8 Yhteenveto

Insinöörityössä rakennettiin 10 Gbit/s -jakeluverkko onnistuneesti. Alkuperäistä suunnitelmaa ei voitu kokonaisuudessaan toteuttaa insinöörityön puitteissa budjetti- ja aikataulusyistä johtuen. Sen vuoksi RRPP-toteutusta kokeiltiin alkuperäistä suunnitelmaa suppeammalla kolmen kytkimen testirenkaalla. Testeissä havaittiin, että UDP-täsmälähetyksessä verkon palautumisaika oli odotusten mukaisesti 50 ms:n luokkaa. Toisaalta ryhmälähetyksessä palautumisaika oli suurempi ja suoraan riippuvainen PIM Hello -viestien lähetysvälistä. Pienentämällä PIM Hello -viestien lähetysväliä 30 s:n oletusarvosta 500 ms:iin, saatiin ryhmälähetys palautumaan huomattavasti nopeammin. Videoviive oli testien mukaan 200 ms:n luokkaa, mikä sekin asettui hyvin 300 ms:n vaatimukseen. Kiertoaikatesteissä samoin kuin pakettikaappauksin suoritetuissa testeissä ei havaittu poikkeamia. Myöskään kytkinten tilastotietoihin ei kirjautunut lähetyksen tai vastaanoton virheitä jakeluverkon osalta.

Tarkoitus on edelleen jatkaa alkuperäisen suunnitelman toteutusta jatkamalla RRPP-rengasta sekä liittämällä E-jakamon laitetilan kytkimet virtuaaliseen keskuskytkimeen. Keskuskytkin muutetaan kameraverkon oletusreitittimeksi ja ryhmälähetysten kohtauspisteeksi. Lisäksi nykyinen reititin tullaan vaihtamaan uuteen ja kytketään LACP-yhteydellä virtuaalisen keskuskytkimen eri jäsenkytkimiin. Näin saadaan vielä etäyhteyksien vikasietoisuutta parannettua nykyisestä.

Opin paljon työtä tehdessäni. Havaitsin ensiksikin, että videoviivetesteissä käytetty menetelmä soveltui hyvin tarkoitukseensa. Toisaalta valvomokoneella suoritetut pakettikaappaustestit epäonnistuivat suorituskykyongelmien vuoksi. PIM Hello -viestien merkitys siirtoverkon ryhmälähetysliikenteen palautumisen kannalta oli myös tärkeä uusi oivallus, jota varmasti tarvitsen vielä työssäni myöhemminkin. Lisäksi opin paremmin ymmärtämään IGMP snooping -tekniikan toimintaa siirtoverkossa. Tutustuin myös ensimmäistä kertaa HP:n uusiin kytkinperheisiin. Sain näin arvokasta tietoa ja kokemusta HP:n laitteiden asentamisesta ja ohjelmoinnista sekä HP:n tekniikoista. Tulen käyttämään HP:n IRF- ja RRPP-toteutuksia myös jatkossa.

Lähteet

1 Sullivan, G., Topiwala, P. & Luthra, A. The H.264/AVC Advanced Video Coding Standard: Overview and Introduction to the Fidelity Range Extensions. (WWW-dokumentti.) FastVDO LLC. <http://www.fastvdo.com/spie04/spie04-h264OverviewPaper.pdf>. August, 2004. Luettu 14.5.2011.

2 Viitanen, Marko. H.264 liikkeenestimoinnin testaus ja optimointi. Kandidaatintyö. (WWW-dokumentti.) TTY. <http://fador.be/kandityo_Marko_Viitanen_2010.pdf>. Kesäkuu 2010. Luettu 14.5.2011.

3 H. Schulzrinne, S. Casner, R. Frederick & V. Jacobson. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. (WWW-dokumentti). IETF. <http://tools.ietf.org/html/rfc3550>. July, 2003. Luettu 4.5.2011

4 Wenger, S., Chandra, U., Westerlund, M. & Burman, B. RFC 5104. Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF). (WWW-dokumentti). IETF. <http://tools.ietf.org/html//rfc5104>. February, 2008. Luettu 4.5.2011

5 Kojo, Markku. TCP-ruuhkanvalvonta (RFC 2581). Luentomateriaali. (WWW-dokumentti.) <http://www.cs.helsinki.fi/u/kojo/tiliII/TiliIIs05_L2.pdf>. 2004. Luettu 7.5.2011.

6 Kiviniemi, Teemu. Implementation of an IPv4 to IPv6 Multicast Translator. Master's Thesis. (WWW-dokumentti.) HUT. <http://www.elisanet.fi/teemuki/translator/thesis.pdf>. October 25, 2009. Luettu 15.5.2011.

7 Harju, Jarmo. Multicast. Kurssimateriaali. (WWW-dokumentti.) TTY. <http://www.cs.tut.fi/kurssit/TLT-2600/t2005-06/TLT-2600-VTJ-luento-multicast.pdf>. Luettu 16.4.2011.

8 IndigoVision 11000 HD IP camera range. (WWW-dokumentti.) IndigoVision, Ltd. <http://www.indigovision.com/documents/public/datasheets/11000%20Fixed%20Camera%20Datasheet-Letter.pdf>. Luettu 27.4.2011.

9 IPv4 Multicast Address Space Registry. (WWW-dokumentti.) IANA. <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>. Updated 26.4.2011. Luettu 27.4.2011.

10 Meyer, David. RFC 2365. Administratively Scoped IP Multicast. (WWW-dokumentti.) IETF. <http://www.ietf.org/rfc/rfc2365.txt>. July 1998. Luettu 30.3.2011.

11 Ether types. (WWW-dokumentti.) IANA. <http://www.iana.org/assignments/ethernet-numbers>. Updated 5.4.2010. Luettu 28.3.2011.

12 Kozierok, Charles M. TCP/IP Address Resolution For IP Multicast Addresses. (WWW-dokumentti.) <http://www.tcpipguide.com/free/t_TCPIPAddressResolutionForIPMulticastAddresses.htm>. The TCP/IP Guide v.3.0, 20.9.2005. Luettu 30.3.2011.

13 Guidelines for Enterprise IP Multicast Address Allocation. (WWW-dokumentti.) Cisco Systems Inc. <http://www.cisco.com/warp/public/cc/techno/tity/prodlit/ipmlt_wp.pdf>. 2004. Luettu 1.4.2011.

14 Understanding VLANs by understanding MAC table operation. (WWW-dokumentti.) Cisco Systems Inc. <https://learningnetwork.cisco.com/servlet/JiveServlet/download/4080-12-3569/Understanding_VLANs_by_understanding_MAC_table_operation_021-CN.pdf>. 2008. Luettu 8.5.2011.

15 Multicast in a Campus Network: CGMP and IGMP Snooping (WWW-dokumentti.) Cisco Systems Inc. <http://www.cisco.com/image/gif/paws/10559/22.pdf > Updated: December 17, 2008. Luettu 8.5.2011.

16 Williamson, Beau. Developing IP Multicast Networks. Volume 1. Cisco Systems Inc. Indianapolis: Cisco Press, 2000.

17 Understanding and Configuring IGMP Snooping. (WWW-dokumentti.) Cisco Systems, Inc. <http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/11/configuration/guide/multi.pdf>. Luettu 15.4.2011.

18 McQuerry, S., Jansen, D. & Hucaby, D. Cisco LAN Switching Configuration Handbook. 2nd ed. Indianapolis: Cisco Press, 2009.

19 Wu, I. & Eckert, T. RFC 3488. Router-port Group Management Protocol (RGMP).. (WWW-dokumentti.) IETF. <http://www.ietf.org/rfc/rfc3488.txt >. February 2003. Luettu 2.4 .2011.

20 Hietavirta, Petteri. Ethernet (Kytkinperustaiset). Seminaarityö. (WWW-dokumentti.) LUT. <http://www2.it.lut.fi/kurssit/02-03/010626000/palautukset/seminaarit/Ethernet.doc>. 9.2.2003. Luettu 15.5.2011.

21 Gilmore, Michael Charles. Multimode fiber bandwidth – its true value for high bit rate networks within plug-and-play data centre infrastructures. Qualification thesis. (WWW-dokumentti.) <http://www.fia-online.co.uk/pdf/QS/thesis050001.pdf>. The Fiberoptic Industry Association. 16.4.2006. Luettu 27.3.2011.

22 Globisch, J., Hamm A. O., Esteves, F. & Öhman, A. Fear appears fast: Temporal course of startle reflex potentiation in animal fearful subjects. Psychophysiology, 1999. Vol. 36, s. 66–75.

23 Frame, Tom. Network Design Proposal – v1.52. VideoGen Ltd, 28.3.2011.

24 Understanding Spanning-Tree Protocol. (WWW-dokumentti.) Cisco Systems, Inc. <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm>. 1997. Luettu 20.4.2011.

25 RRPP Technology White Paper. (WWW-dokumentti.) Hangzhou H3C Technologies Co., Ltd. <http://www.h3c.com/portal/Products___Solutions/Technology/LAN/Technology_White_Paper/200810/618495_57_0.htm>. 2008. Luettu 26.3.2011.

26 IRF2.0 Technology White Paper. (WWW-dokumentti.) Hangzhou H3C Technologies Co., Ltd. <http://www.h3c.com/portal/Products___Solutions/Technology/IRF/Technology_White_Paper/200901/624932_57_0.htm >. 2010. Luettu 26.3.2011.

27 H3C S5820X&S5800 Series Ethernet Switches IRFConfiguration Guide. (WWW-dokumentti.) <http://www.h3c.com/portal/download.do?id=1039958>. 2010. Luettu 5.5.2011.

28 Settey, Vladimir. Fast convergence and load splitting. (WWW-dokumentti.) Cisco Systems, Inc. <http://www.ciscoexpo.sk/slides/02c_vlsettey_0x_mcast_fc_ecmp.pdf>. 2008. Luettu 17.4.2011.

Taulukko 1. Keskus / jakelukytkinten pisteytys.

Keskus / jakelukytkimet						
TEKNINEN TOTEUTUS						
Ensisijaiset vaatimukset						
Laite	**HP A5120-24G-PoE EI**		**HP A5500-24G-PoE EI**		**HP A5800-24G-PoE EI**	
Täyttääkö vaatimukset	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet
Vähintään 1000 IGMP-ryhmää	Kyllä	100	Kyllä	100	Ylittää, 4000 ryhmää	120
Tuki 10 Gbit/s -nopeuksille	Kyllä	100	Kyllä	100	Kyllä	100
Suorituskyky vähintään 128 Gbit/s	Kyllä	100	Kyllä	100	Ylittää, 208Gbit/s	120
Rengasmallinen vikasietoinen; palautuminen 50 ms:ssa	Kyllä, RRPP	100	Kyllä, RRPP	100	Kyllä, RRPP	100
Pinoaminen käyttäen 10GbE yhteyksiä	Kyllä, IRF	100	Kyllä, IRF	100	Kyllä, IRF	100
Kahdennetut virtalähteet	Kyllä	100	Kyllä	100	Kyllä	100
Siirtokerroksen ryhmälähetys: IGMPv1/2/3, MVR	Kyllä	100	Kyllä	100	Ylittää, MVR+	110
Verkkokerroksen ryhmälähetys: PIM-DM, PIM-SM	Ei	0	Ylittää, PIM-SSM, MSDP, MBGP	110	Ylittää, PIM-SSM, MSDP, MBGP	110
Verkkokerroksen reititys: RIP, OSPF	Ei	0	Ylittää, BGP, VRRP	110	Ylittää, BGP,VRRP, IS-IS	120
YHTEENSÄ		700		920		980
Painokerroin	**1.5**	**1050**		**1380**		**1470**
Laite	**HP A5120-24G-PoE EI**		**HP A5500-24G-PoE EI**		**HP A5800-24G-PoE EI**	
Toissijaiset vaatimukset	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet
Kytkimessä neljä SFP-paikkaa	Kyllä	100	Kyllä	100	Ylittää, neljä SFP+ paikkaa	120
Laajennettavuus kortein	4 SFP/SFP+ paikkaa	100	4 SFP/SFP+ paikkaa	100	16 SFP/ 4 SFP+ paikkaa	110
YHTEENSÄ		200		200		230
Painokerroin	**1**	**200**		**200**		**230**
TEKNINEN TOTEUTUS YHTEENSÄ		**1250**		**1580**		**1700**
Tekninen toteutus, paras 50 pistettä		**37**		**46**		**50**
Hintavertailu 10Gbit/s kokoonpanolla, halvin 50 pistettä		**50**		**43**		**44**
LOPPUTULOS		**87**		**89**		**94**

Taulukko 2. Reunakytkinten pisteytys.

Reunakytkimet						
TEKNINEN TOTEUTUS						
Ensisijaiset vaatimukset						
Laite	**HP A5120-24G-PoE EI**		**HP A5500-24G-PoE EI**		**HP A5800-24G-PoE EI**	
Täyttääkö vaatimukset	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet
Vähintään 256 IGMP-ryhmää	Ylittää, 1000 ryhmää	110	Ylittää, 1000 ryhmää	110	Ylittää, 4000 ryhmää	120
Tuki 10 Gbit/s -nopeuksille	Kyllä	100	Kyllä	100	Kyllä	100
Pinoaminen käyttäen 10GbE yhteyksiä	Kyllä, IRF	100	Kyllä, IRF	100	Kyllä, IRF	100
Kahdennetut virtalähteet	Kyllä	100	Kyllä	100	Kyllä	100
Siirtokerroksen ryhmälähetys: IGMPv1/2/3, MVR	Kyllä	100	Kyllä	100	Ylittää, MVR+	110
YHTEENSÄ		510		510		530
Painokerroin	**1.5**	**765**		**765**		**795**
Laite	**HP A5120-24G-PoE EI**		**HP A5500-24G-PoE EI**		**HP A5800-24G-PoE EI**	
Toissijaiset vaatimukset	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet	Kyllä/Ei/Ylittää	Pisteet
Kytkimessä kaksi SFP-paikkaa	Ylittää, neljä SFP-paikkaa	110	Ylittää, neljä SFP-paikkaa	110	Ylittää, neljä SFP+ paikkaa	120
Laajennettavuus kortein	4 SFP/SFP+ paikkaa	100	4 SFP/SFP+ paikkaa	100	16 SFP/ 4 SFP+ paikkaa	110
YHTEENSÄ		210		210		230
Painokerroin	**1**	**210**		**210**		**230**
TEKNINEN TOTEUTUS YHTEENSÄ		**975**		**975**		**1025**
Tekninen toteutus, paras 50 pistettä		**48**		**48**		**50**
Hintavertailu 1Gbit/s kokoonpanolla, halvin 50 pistettä		**50**		**34**		**23**
LOPPUTULOS		**98**		**82**		**73**

```
[Asiakas-Helsinki-Core]display rrpp statistics domain 1
Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Active Status : Yes
Primary port  : Ten-GigabitEthernet2/0/25
 Packet           Link      Common     Complete   Edge      Major
Packet
 Direct Hello     Down      Flush FDB  Flush FDB  Hello     Fault
Total
-------------------------------------------------------------------------
---------
 Send   158       0         0          1          0         0
159
 Rcv    0         0         0          0          0         0
0
Secondary port: Ten-GigabitEthernet1/0/28
 Packet           Link      Common     Complete   Edge      Major
Packet
 Direct Hello     Down      Flush FDB  Flush FDB  Hello     Fault
Total
-------------------------------------------------------------------------
---------
 Send   0         0         0          0          0         0
0
 Rcv    34        0         0          1          0         0
35
```

Kuva 1. Keskuskytkimen RRPP-statistiikkatiedot. Kytkin merkitty isäntälaitteeksi.

```
[Asiakas-Helsinki-Core]display rrpp verbose domain 1
Domain ID     : 1
Control VLAN  : Major 101    Sub 102
Protected VLAN: Reference Instance 0 to 32
Hello Timer   : 1  sec  Fail Timer : 3  sec

Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : Ten-GigabitEthernet2/0/25  Port status: UP
Secondary port: Ten-GigabitEthernet1/0/28  Port status: BLOCKED
```

Kuva 2. Keskuskytkimen RRPP-tilatiedot normaalissa tilassa (tilaksi merkitty Complete).

```
[Asiakas-Helsinki-Core]display rrpp verbose domain 1
Domain ID      : 1
Control VLAN   : Major 101    Sub 102
Protected VLAN: Reference Instance 0 to 32
Hello Timer    : 1  sec  Fail Timer : 3  sec

Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Enable Status : Yes    Active Status: Yes
Primary port   : Ten-GigabitEthernet2/0/25  Port status: UP
Secondary port: Ten-GigabitEthernet1/0/28  Port status: UP
```

Kuva 3. RRPP-rengas "Failed" -tilassa.

```
[Asiakas-Helsinki-Core]dis rrpp statistics domain 1
Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Active Status : Yes
Primary port   : Ten-GigabitEthernet2/0/25
 Packet           Link      Common     Complete   Edge      Major
Packet
 Direct Hello     Down      Flush FDB  Flush FDB  Hello     Fault
Total
-------------------------------------------------------------------
---------
 Send   385       0         1          0          0         0
386
 Rcv    0           1         0          0          0         0
1
Secondary port: Ten-GigabitEthernet1/0/28
 Packet           Link      Common     Complete   Edge      Major
Packet
 Direct Hello    Down      Flush FDB  Flush FDB  Hello     Fault
Total
-------------------------------------------------------------------
---------
 Send   0           0         1          0          0         0
1
 Rcv    100       1         0          0          0         0
101
```

Kuva 4. RRPP-statistiikkatiedot renkaan vikaannuttua. Isäntälaite on vastaanottanut Link Down -viestin vikaantumisen yhteydessä.

[Asiakas-Helsinki-Core-Ten-GigabitEthernet2/0/25]display interface Ten-GigabitEthernet 2/0/25
Ten-GigabitEthernet2/0/25 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 3ce5-a67a-e541
Description: A-jakamo 10GbE
Loopback is not set
Media type is optical fiber,Port hardware type is 10G_BASE_SR_SFP
10Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 1
Link delay is 0(sec)
Port link-type: trunk
VLAN passing : 1(default vlan), 2-3, 10, 21, 899
VLAN permitted: 1(default vlan), 2-4094
Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Peak value of input: 13381196 bytes/sec, at 2011-04-05 12:15:47
Peak value of output: 460627 bytes/sec, at 2011-04-05 12:19:57
Last 300 seconds input: 13702 packets/sec 13344185 bytes/sec 1%
Last 300 seconds output: 561 packets/sec 419888 bytes/sec 0%
Input (total): 14554357 packets, 14133353906 bytes
1856875 unicasts, 198 broadcasts, 12696739 multicasts, 0 pauses
Input (normal): 14553812 packets, - bytes
1856875 unicasts, 198 broadcasts, 12696739 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
- ignored, - parity errors
Output (total): 632300 packets, 456882861 bytes
82705 unicasts, 5706 broadcasts, 543889 multicasts, 0 pauses
Output (normal): 632300 packets, - bytes
82705 unicasts, 5706 broadcasts, 543889 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, - no carrier