Henri Sihvonen

SLA-monitorointi operaattoriverkoissa Echovault-sovelluksella

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

25.5.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Henri Sihvonen SLA-monitorointi operaattoriverkoissa Echovault-sovelluksella 40 sivua 25.5.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	lehtori Marko Uusitalo

Työn tarkoituksena oli luoda ohjeet kahden erilaisen verkon palveluntason mittausta varten Echovault-sovelluksella. Toinen verkoista olisi Ethernet-pohjainen ja toinen IP-pohjainen. Verkoista mitattaisiin kaikkia Echovaultin mahdollistamia suorituskyvyn mittareita, kuten viivettä ja jitteriä.

Työssä käydään läpi peruskäsitteitä, kuten mikä on palvelutasosopimus. Työssä läpikäydään myös peruskäsitteitä, joita tarvitaan verkon monitoroinnin ymmärtämiseksi. Tärkeimmässä osassa kuitenkin ovat Ethernetin OAM-standardit, jotka korjaavat Ethernetissä olevia puutteita verkonhallinnan ja verkon monitoroinnin osalta. Näiden parannusten avulla Ethernet lähestyy sitä pistettä, että siitä tulisi todellinen operaattoritasoinen teknologia.

Työn tarkoituksena olleet ohjeet saatiin koottua halutulla tavalla ja molempien ohjeiden pohjalta tehdyt testikonfiguraatiot toimivat.

Avainsanat	SLA, Ethernet, OAM, Echovault

Author(s) Title Number of Pages Date	Henri Sihvonen SLA Monitoring in Operator Networks Using Echovault Software 40 pages 25 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Computer Networks
Instructor(s)	Marko Uusitalo, Senior Lecturer

The purpose of this bachelor's thesis was to create instructions for two different kinds of network service level measurements for Echovault. One of the networks would be Ethernet based and the other would be IP based. Echovault would be used to measure network performance metrics, for example delay or jitter, in these networks.

This thesis goes through the fundamentals of a service level agreement and all the basics to understand network monitoring. The most important aspect of the thesis is the Ethernet OAM standards that fix deficiencies related to network management and network monitoring. With these improvements, Ethernet as a technology is closing in on becoming a true carrier grade technology.

The guides that were the purpose of this thesis were created as specified. Both were also tested to be functional in their respective networks.

Keywords	SLA, Ethernet, OAM, Echovault

Sisällys

Lyhenteet

SLA	Service Level Agreement. Palvelutasosopimus asiakkaan ja palveluntarjoajan välillä.
OAM	Operations, Administration and Management. Joukko työkaluja ja toimintoja verkon hallinnoimiseen ja monitoroimiseen.
EVC	Ethernet Virtual Connection. Virtuaalinen yhteys kahden toimipisteen Ethernet-verkkojen välillä.
UNI	User Network Interface. Demarkaatiopisteessä sijaitseva laite, johon palveluntarjoajan vastuu verkon toiminnasta loppuu.
EPL	Ethernet Private Line. Kahden toimipisteen välinen linkki, joka voi käyttää vain yhtä fyysistä yhteyttä laitteesta toiselle.
EVPL	Ethernet Virtual Private Line. Kahden toimipisteen välinen linkki, joka voi käyttää useampia virtuaalisia yhteyksiä laitteesta toiselle.
EFM	Ethernet First Mile. Asiakkaan ja palveluntarjoajan välinen verkkolinkki.
CFM	Connectivity Fault Management. IEEE 802.1ag -standardissa luotu malli monen operaattorin kattavan verkon vianselvityksen parantamista varten.
MEP	Maintenance End Point. Huollon toimialueen reunalaite.
MIP	Maintenance Intermediate Point. Huollon toimialueen välilaite.
CE	Customer Edge. Asiakkaan reunareititin.
PE	Provider Edge. Palveluntarjoajan reunareititin.
NID	Network Interface Device. Kts. UNI.
KPI	Key Performance Indicator. Avain suoritustekijä.

1 Johdanto

Tämän insinöörityön tarkoituksena on koota ohje Echovault-sovelluksen käyttöön, jotta tulevat Echovaultia käyttävät opiskelijat pystyvät oppimaan nopeammin Echovaultin peruskäytön. Tämän lisäksi työ sisältää tiedon kaikista peruskäsitteistä ja standardeista, jotka on hyvä ymmärtää, kun puhutaan verkon hallinnoimisesta. Työn pääasiallinen painopiste on verkonmonitorointi Ethernet-verkoissa, koska Ethernet-verkkojen suosio operaattorien keskuudessa on tällä hetkellä jatkuvassa kasvussa.

Työssä tarkastellaan, miten Echovaultia käyttämällä voidaan mitata verkon suorituskykyä Ethernet- ja IP-verkoissa. Tämän lisäksi työssä käydään läpi, miten Echovaultin tarvitsemat laitteet tulee konfiguroida sovellusta varten. Työssä keskitytään pääasiassa perusmittausten konfigurointiin kahdessa erillisessä testiverkossa, joista ensimmäinen on Ethernet-verkko ja toinen on IP-verkko.

2 SLA

Kun puhutaan verkonhallinnasta, niin tulee ymmärtää käsite Service Level Agreement (SLA) eli palvelutasosopimus, joka on dokumentti, jossa määritellään asiakkaan ja palveluntoimittajan välinen suhde ja sen yksityiskohdat. Jokainen palvelutasosopimus luodaan tapauskohtaisesti, mutta jokainen sopimus yleensä sisältää samat perusmääritelmät riippuen kuitenkin, millainen palvelu on kyseessä. Tässä dokumentissa keskitytään pääasiallisesti asioihin, jotka ovat olennaisia verkon SLA:n kannalta. (1.)

Aivan aluksi sopimusta luodessa määritellään tarkasti, mitä palveluntoimittajalta halutaan. Tämä voi sisältää palvelunkuvauksen ja siihen liittyviä erillisiä tarkentavia vaatimuksia. Toisin sanoen tässä vaiheessa sovitaan, mikä kuuluu palveluntoimittajalle toimitettaviin palveluihin ja mikä ei. Tämä on palveluntoimittajan kannalta tärkeää, jotta he voivat selkeästi rajata heidän vastuualueiseensa palvelun suhteen, koska on mahdollista, että tietyt osat esimerkiksi palvelun ylläpidosta jäävät asiakkaan vastuulle. (1.)

Jos palveluntoimittaja ei kuitenkaan pysty pitämään lupaustaan, ja sovittujen mittareiden arvot eivät pääse sovitulle tasolle, niin tällöin palveluntuottaja voi joutua maksamaan asiakkaalleen sanktioita. Riippuen sopimuksesta, tietyissä tapauksissa asiakas voi olla

myös oikeutettu lopettamaan sopimuksensa palvelutoimittajan kanssa. Sanktioiden määrät ovat myös riippuvaisia solmitusta sopimuksesta ja palveluntyypistä, mutta usein ne ovat joko korvausta menetetystä liikevaihdosta tai palveluntarjoajan saamasta korvauksesta. (1.)

Tällä hetkellä palvelutasosopimuksia solmitaankin paljon, koska monet yhtiöt eivät halua olla vastuussa pääosaamisensa ulkopuolella olevista palveluista, joten yhtiöt ostavat tietyt palvelut halvemmalla siihen erikoistuneilta kolmansilta osapuolilta (1). Verkon hallinnoiminen ja ylläpito onkin yksi palvelu, jota yhtiöt saattaisivat lähteä helpoiten ulkoistamaan. Yhtiö pystyy ostamaan palvelun kolmannelta osapuolelta halvemmalla ja paketoimaan sen yhteen verkkoyhteyksien vuokraamisen tai rakennuttamisen toimipisteiden välille.

Minkälaisia mittareita verkon SLA:ta varten sitten yleensä käytetään? Käytännössä SLA-mittareiksi voidaan määritellä melkein mitä tahansa riippuen tuotettavasta palvelusta, mutta tärkein ominaisuus millä tahansa SLA-mittarilla on, että sitä voidaan mitata luotettavasti ja helposti. Tämä saavutetaan yleensä automatisoimalla koko prosessi. Näitä mittareita ovat esimerkiksi käytettävyys ja viive. On kuitenkin olemassa myös SLA-mittareita kuten tietoturvallisuus ja muokattavuus, joita ei voida mitata automaatiolla vaan ne vaativat tarkempaa tarkkailua ihmisen toimesta. (2.)

Seuraavaksi käydään läpi yleisimmät asiat, joita käytetään verkon SLA-mittareina. Referenssinä on käytössä NTT Communications America Corporatedin, globaalin verkko-operaattorin, kotisivuillaan ilmoittamia SLA-lupauksia esimerkkinä siitä, mitä operaattorit voivat luvata asiakkailleen. Nämä käsitteet käydään läpi yksi kerrallaan selventäen hieman tarkemmin, mitä nämä arvot tarkoittavat. Heidän lupaamat SLA:t ovat vapaasti käännettynä seuraavat:

- Käytettävyys: NTT Com Globaal lupaa Globaalin IP verkon olevan 100 % vapaa katkoksista.
- Viive: Viive ei ylitä 50 ms Pohjois-Amerikan runkoverkossa, 90 ms Atlantin välisessä verkossa tai on 130 ms tai vähemmän Tyynenmeren yli kulkevassa verkossa.
- Pakettihäviö: Pakettihäviö ei ylitä 0,1 %.
- Jitter: Keskiverto viiveen vaihtelu eli jitter verkossa ei ylitä 250 mikrosekuntia eikä ylitä 10 millisekuntia enemmän kuin 0,1 % ajasta (http://www.us.ntt.net/support/sla/network.cfm)

2.1 Saatavuus/Käytettävyys

Käytettävyys on helpoin ja yksi tärkeimmistä palvelutason mittareista. Sitä kuvataan tyypillisemmin todennäköisyydellä, miten suurella prosentilla palvelu tai järjestelmä on toimintakykyinen asiakkaalle. Käytettävyyteen voidaan myös määritellä monia eri tekijöistä kuten esimerkiksi, miten nopeasti häiriöihin reagoidaan, kuinka paljon aikaa menee vikojen korjaukseen ja kuinka nopeasti voidaan palautua normaaliin toimintaan vikatilanteen jälkeen. (2.)

Käytettävyyttä yleensä mitataan kuukausi- tai vuositasolla tarkastamalla laitteiden päällä oloa eli uptimea. Tämä ei kuitenkaan kerro koko totuutta, koska kaikki verkon laitteet saattavat olla valvonnasta käsin täysin kunnossa, mutta jonkin verkon muutoksen tai konfigurointivirheen vuoksi käytettävyys saattaa olla loppukäyttäjällä kadonnut. (4.)

Tämän vuoksi, jos halutaan mitata todellista käytettävyyttä, niin tulisi käyttää verkonmittaukseen erillisiä työkaluja kuten tässä työssä esimerkkinä olevaa palvelunlaadun mittaus- ja monitorointijärjestelmää Echovaultia. Näin saadaan todellisempi kuva käytettävyydestä, ja mahdolliset ongelmatilanteet voidaan huomata nopeammin.

Palveluntarjoajat yleisemmin markkinoivat yhteyksiään lupaamalla tietyn käytettävyysprosentin asiakkailleen. Tämä prosentti on aina jotain 90 % ja 100 % välillä ja mitä lähemmäs 100 % mennään niin sitä suurempi hinta. Operaattorit tarjoavat yleisimmin lukuja, joissa on pelkkiä yhdeksiä peräkkäin ja tätä kutsutaankin yleisesti yhdeksien käytettävyydeksi. Prosentteja on kuitenkin hieman kömpelöä käyttää ja siksi on yleinen käytäntö ilmoittaa tämä luku käyttäen yhdeksien määrää. Esimerkkinä "kolmen yhdeksän käytettävyys" olisi 99,9 %. (4.)

Taulukosta 1 löytyvät yleisimmät käytettävyyden prosentit, joita operaattorit saattavat tarjota asiakkailleen.

Taulukko 1 Käytettävyyden ”yhdeksien” taulukko

Yhdek-sät	Prosentit	Katkot per kuukausi	Katkot per vuosi
3	99,9 %	43,8 min	8,75 tuntia
4	99,99 %	4,32 min	52 min
5	99,999 %	25,9 s	5 min
6	99,9999 %	2,59 s	31,5sek
7	99,999999 %	269,97 ms	3,15sek

Esimerkiksi asiakkaalle on mahdollisesti myyty lupaus kolmen 9:n eli 99,9 % käytettävyydestä tietylle verkolle tai sen tietylle segmentille ympäri vuoden. Tämä tarkoittaisi sitä, että jos verkon käyttäjillä olisi kuukauden aikana enemmän kuin 43,8 minuuttia käyttökatkoa, niin palveluntarjoaja joutuisi maksamaan sanktioita sopimusrikkomuksesta. Vaihtoehtoisesti, jos sama verkko olisi NTT American SLA:n alainen, niin verkon käyttäjille ei saisi esiintyä yhtään odottamatonta käyttökatkoa.

On kuitenkin tärkeää ottaa huomioon, että on olemassa kahdenlaisia käyttökatkoja. Nämä ovat odottamattomat katkot ja tiedossa olevat huoltokatkot. Molemmat voivat vaikuttaa asiakkaan saaman palvelun käytettävyyteen riippuen siitä miten sopimus on kirjoitettu eikä yleensä huoltokatkoja oteta huomioon SLA:ta laskettaessa. (4.) Tällainen huoltokatko voi olla asiakkaan erikseen pyytämä tai heidän kanssaan ennalta sovittu. Toisena vaihtoehtona on voitu myös sopia tietty ajanjakso, joka toimii huoltoikkunana, jolloin kaikki rutiinihuollot tulisi suorittaa. Nämä huoltotoimenpiteet kuitenkin pyritään toteuttamaan sellaisina ajankohtina milloin ne eivät aiheuta suurta haittaa asiakkaan palveluille. Huollot suoritetaan tässä tapauksessa yleensä yöaikaan tai viikonloppuisin.

Odottamattomat katkokset taas johtuvat yleensä laitevioista, väärästä konfiguraatiosta tai linkin välisen kaapelin katkeamisesta. Näissä tapauksissa SLA-lupauksen pitämistä varten ainoa vaihtoehto on pitää yllä toista vaihtoehtoista yhteyttä samaan pisteeseen eli kahdentaa yhteys. Näin voidaan poistaa mahdolliset yksittäiset verkon solmukohdat

jotka voivat aiheuttaa laajan verkon katkeamisen. Tällainen järjestely on kuitenkin kallis ja monesti käytössä vain korkeiden käytettävyyksien yhteydessä. Hinta tällaiselle palvelulle on huomattavasti korkeampi ja sen vuoksi sitä käytetäänkin harvemmin ja harkitusti. (4.)

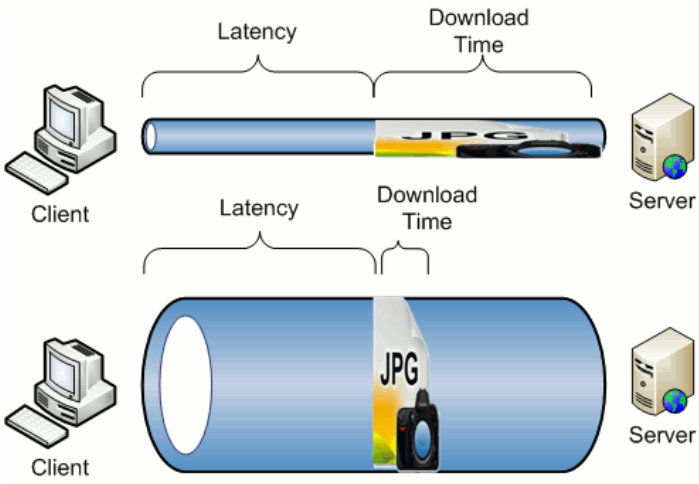
2.2 Viive

Seuraavaksi käyn läpi käsitteen viive eli latency, koska se on toinen suuri vaikuttaja verkon toimivuudessa. Kaikessa yksinkertaisuudessaan verkon viiveellä tarkoitetaan aikaa, mikä kuluu datan fyysisessä matkassa ja sen käsittelyssä kohteesta A kohteeseen B sellaiseen tilaan, että dataa voidaan käsitellä. Valitettavasti yhteyksiä ei voida todellisuudessa rakentaa niin, että jokaiseen kohteeseen olisi erillinen suora yhteys vaan joudutaan käyttämään muita laitteita reitittämään paketteja oikeaan osoitteeseen käyttäen käytössä olevaa verkkoinfrastruktuuria. (6.)

Viiveen ymmärtämiseksi on aluksi tärkeää ymmärtää, mitä tarkoittaa kaistanleveys eli yhteyden teoreettinen tiedonsiirron maksiminopeus. Voimme ajatella minkä tahansa verkon toiminnan käyttäen putkea vertauskuvana yhteydelle kahden pisteen välissä. Viive tässä tapauksessa olisi, kuinka pitkä putki on, ja kaistanleveys taas olisi putken halkaisija, joten mitä suurempi kaistanleveys sitä enemmän tietoa mahtuu kulkemaan putken läpi yhtäaikaisesti. Kuitenkin tulee huomioida, että putken halkaisijaa kasvattamalla emme vaikuta etäisyyteen, mitä tiedon täytyy kulkea vaan sen pitää silti kulkea yhtä pitkä matka, vaikka yhtäaikaisen tiedon määrää kasvatetaankin huomattavasti. Tämän vuoksi verkon kautta saapuvat resurssit latautuvat aina pienellä viiveellä, vaikka yhteyden nopeus eli kaistanleveys olisi kuinka suuri. (6.)

Aikaisemmin viivettä ei pidetty minkäänlaisena ongelmana, koska käytössä oleva kaistanleveys oli huomattavasti pienempi. Datan lataamisessa kesti paljon pitempään, jonka vuoksi vasteajalla ei ollut käytännössä merkitystä. Nykypäivänä verkkoyhteyksien nopeudet ovat kasvaneet niin paljon, että viiveen rooli on kasvanut huomattavasti yhteyksien optimoimisessa. Tavanomainen viive käytettäessä esimerkiksi internetiä voi olla 50–200 ms ja pienen kuvan itse lataamiseen kuluva aika saattaa olla vain muutamia millisekunteja. Tästä voidaankin suoraan nähdä, että viiveen vähentäminen on ainoa tapa käytännössä pienentää latausaikoja. Kuvassa 1 tämä on esitetty graafisesti. Ylem-

mässä osiossa kuvaa on esimerkki yhteydestä, jossa tiedostoa ladataan pienellä kaistanleveydellä ja alemassa ladataan sama tiedosto käyttäen suurempaa kaistanleveyttä. (6.)



Kuva 1 Kaistanleveyden ja viiveen vaikutus tiedoston lataamisennopeuteen (6)

Pörssikauppa on alue, joka vaatii viiveen pudottamista mahdollisimman alas, koska nykyään kaupankäyntiä tehdään niin nopeasti. Millisekuntien ja joskus jopa mikrosekuntien ylimääräisellä viiveellä on suuri merkitys kaupankäynnissä. Tällaista kaupankäyntiä kutsutaan korkean frekvenssin kaupankäynniksi. Tämän menetelmän idea on suorittaa kymmeniä tuhansia kauppoja päivässä, jossa nopeilla ostoilla ja myynneillä haalitaan muutamia senttejä tai murto-osia senteistä per osake. Tämä pieni määrä kuitenkin kerrotaan muutamien satojen osakkeiden myynnillä per kauppa, jolloin mahdollisen tuoton määrä alkaa avautua selkeämmin. (7.)

Tällainen kaupankäynti on vain mahdollista silloin, kun tietoa osakkeiden hinnoista voidaan päivittää lähes reaaliajassa. Pelkästään viiveen lyhentämiseen ollaan valmiit tekemään satojen miljoonien ja jossain tapauksissa jopa miljardien investointeja. Tämä tehdään pelkästään siksi, että etäisyyksien viivettä saataisiin vähennettyä muutamilla prosenteilla. Viiveen vähennys on yleensä luokkaa 2-10 ms riippuen siitä, miten suoraksi yhteys voidaan parantaa ja mitä teknologiaa käytetään. Tämä pieni parannus viiveessä kuitenkin voi olla monien miljoonien arvoinen korkean frekvenssin meklareille, koska näin he pääsevät olemaan varmemmin ensimmäisenä suorittamaan kauppoja, kun tietokone havaitsee mahdollisuuden rahantekoon. (7)

Hyväksi esimerkiksi tästä trendistä löysin New Yorkin ja Chicagon välisistä yhteyksistä, jotka näkyvät kuvassa 2. Toisin kun voisi kuvitella, niin kaikki kaupankäynti ei olekaan keskittynyt New Yorkiin, vaan Chicagon pörssi on myös suuri keskus tietylle osalle Yhdysvaltojen kaupankäyntiä ja näitä kauppoja voi suorittaa vain kyseisestä pörssistä.

Kuva 2 Chicagon ja New Yorkin väliset verkkoyhteydet. Sininen ja oranssi yhteys on toteutettu radiolinkeillä ja punainen ja vihreä on toteutettu valokuidulla (7)

Kaupunkien väliin oli asennettu 80-luvun puolessa välissä valokuitukaapeli, jonka viive oli parhaimmillaan 14,5 ms. Vuonna 2010 Spread Networks suoritti kauppoja tietoliikenne yhteyksien ostamisesta heidän yksityiseen käyttöön kaupunkien välille, jotta he pystyisivät tarjoamaan asiakkailleen yhteyden, missä viiveen määrä näiden kaupunkien välillä olisi parhaimmillaan 13,1 ms. Vuonna 2012 kaksi muuta yhtiötä, McKay Brothers ja Tradeworkx, lähtivät mukaan kilpailemaan paremman viiveen omaavan yhteyden tarjoamisesta, ja he lähtivät rakentamaan mikroaaltoyhteyttä kaupunkien välille. McKay Brothers lupasi 9 ms viivettä parhaimmillaan ja Tradeworkx 8,5 ms. Näiden yhteyksien hinnat ovat yleensä kovin salaisia, mutta Tradeworkx on paljastanut heidän yhteytensä vuosittaisen hinnan olevan 250 000 dollaria per vuosi.

Mikä sitten aiheuttaa viiveen? Viiveellä on 4 päälähdettä, jotka ovat seuraavat: paketin kulkemiseen kuluva aika eli etenemisviive, sarjoitus, dataprotokollien aiheuttama viive, pakettien käsittely ja jonotusaika. (5.)

Etenemisviive

Etenemisviive on aika, joka tiedolla kuluu kulkea valonnopeutta mediassa lähtöpisteestä kohteeseen, ja tämä on suurin tekijä mitattaessa verkon viivettä. Tyhjiössä tämä nopeus on noin 300 000 km/s, mutta kupari- tai kuitukaapeleissa valonnopeus on hitaampaa, koska valonnopeus on riippuvainen siitä mitä välittäjäainetta käytetään. Esimerkiksi kuparijohdoissa valonnopeus vaihtelee 40 % - 80 % välillä tyhjiön nopeudesta riippuen,

miten johto on suunniteltu, kun taas tyypillisessä valokuitukaapelissa nopeus on yleensä 70 %:n luokassa. Kolmantena vaihtoehtona tieto voidaan myös välittää radioaalloilla, jolloin tieto kulkee valonnopeutta. (5.)

Etenemisviive on helppo laskea, kun tiedetään välimatka ja kuinka nopeasti valo kulkee käytettävässä mediassa. Se lasketaan seuraavalla kaavalla:

$$Etenemisviive(s) = \frac{Välimatka(m)}{Valonnopeus\ välittäjäaineessa(\frac{m}{s})}$$

Kaavaa käyttäen saadaan yhteen suuntaan kuluva viive, mutta todellisen viiveen saamiseksi meidän tarvitsee kertoa tämä tulos kahdella. Paketinhan tulee ensin saapua kohteeseen ja tämän jälkeen kohteelta pyydetyn vastauksen tulee palata takaisin alkuperäiselle lähettäjälle.

Havainnollistavaksi esimerkiksi taulukkoon 1 on laskettu, kuinka suuri viive kuparilla, kuidulla ja mikroaaltolinkillä olisi, jos näillä medioilla olisi suora yhteys Helsingistä New Yorkiin. Kuparikaapeleiden nopeus vaihtelee runsaasti rakenteen ja materiaalien mukaan. Tämän vuoksi laskuissa on käytetty tyypillistä 66 %:n arvoa. (5.)

Taulukko 2 Välittäjäaineen vaikutus viiveeseen.

Välittäjäaine	**Yksisuuntainen viive**	**Kaksisuuntainen viive**
Kupari	$\frac{6628\ km}{299\ 792\frac{\text{km}}{\text{s}} * 0{,}66} = 0{,}0334979s \approx 33{,}49\ ms$	66,98 ms
Kuitu	$\frac{6628\ km}{299\ 792\frac{\text{km}}{\text{s}} * 0{,}7} = 0{,}0315838\ s \approx 31{,}58\ ms$	63,16 ms

Mikroaaltolinkki	$\frac{6628\ km}{299\ 792\ \frac{km}{s}} = 0{,}0221086\ s \approx\ 22{,}11\ ms$	44,22 ms

Näistä laskuista voidaan selkeästi nähdä, että eri välittäjäaineen käyttäminen voi vaikuttaa huomattavasti etenemisviiveen määrään, mutta tämä ei ole kuitenkaan ainoa keino vähentää etenemisviivettä. Toinen tapa etenemisviiveen minimoimiseen on lyhentää yhteyden pituutta. Alun perin verkkoja rakennettiin rautatieyhteyksien tai muiden vastaavien projektien yhteydessä. Monesti näillä yhteyksillä ei ollut suoria reittejä, vaan ne saattoivat kiertää jopa satoja kilometrejä. (7)

Hyvä esimerkki tästä on aikaisemmassa New York – Chicago -välisistä verkkoyhteyksistä (kts. kuva 2). Tämän valokuituyhteyden alkuperäinen pituus oli yli 1600 km, mutta pelkästään ostamalla oikeuksia tietyille verkon reiteille Spread Networks onnistui lyhentämään etäisyyttä noin 400 kilometrillä, ja näin he saivat viivettä vähennettyä millisekunnin verran. McKay Brothers ja Tradeworkx vähensivät mikroaaltolinkeillä yhteyden etäisyyttä noin 100 kilometrillä lisää ja saivat viivettä laskettua vielä noin neljällä millisekunnilla. Tähän on kuitenkin laskettu 30 %:n nopeuslisä, joka saadaan käytettäessä mikroaaltolinkkejä valokuidun sijaan. (7.)

On kuitenkin hyvä ottaa huomioon, että näitä toimenpiteitä ei kannata suorittaa kaikille yhteyksille erinäisten syiden vuoksi. Tärkein tekijä on käytettävän rahan määrä verrattuna saatuun hyötyyn. Yhteyksiä ei usein lähdetä parantamaan tai luomaan uudelleen ilman että niistä voidaan saada tarpeeksi hyötyä. New York – Chicago -kuituverkon yhteydestä saatiin tiputettua 400 km matka pois ja sillä voitettiin 1,4 ms vähemmän viivettä ja tämä arvo on jo huomattava parannus alkuperäiseen yhteyteen. Jos matkaa olisikin saatu lyhennettyä vain 100 km, niin etenemisviive vähenisi 0,35 ms:lla. Tämä parannus ei todennäköisesti olisi kannattava syy kuluttaa miljoonia yhteyden parantamiseen.

Tämän syyn vuoksi esimerkiksi Suomen olosuhteissa yhteyksien parantaminen ei ole kovin kannattavaa. Jos oletetaan Helsinki – Oulu -välillä kulkevan verkkoyhteyden olevan kuituyhteys, joka kulkee junaratoja seuraten, niin yhteyden etäisyydeksi saataisiin noin 590 km ja sen etenemisviive olisi 2,81 ms. Kaupunkien etäisyys toisistaan suoralla

linjalla olisi noin 540 km ja tämän yhteyden etenemisviive olisi 2,57 ms. Yhteyden suoristaminen siis vähentäisi etenemisviivettä 0,24 ms:lla, mutta vaatisi kokonaan uuden yhteyden vetämisen kaupunkien välille. Tämän viiveen vähennyksen määrällä yhteyden rakentaminen ei olisi lainkaan kannattavaa, koska uuden yhteyden vetäminen maksaisi miljoonia

Tietyissä tapauksissa, kun langalliset yhteydet tai mikroaaltolinkit koetaan liian kalliiksi tai niiden rakentaminen ei vain ole mahdollista tietyllä alueella, niin alueella voidaan ottaa käyttöön satelliittilinkki. Satelliittilinkkejä käytettäessä mikroaallot välitetään eteenpäin maata kiertäviä satelliitteja käyttäen. Satelliittilinkkien ongelma kuitenkin on, että satelliitit käyttävät vielä yleisesti geostationääristä kiertorataa, joka sijaitsee päiväntasaajan yläpuolella noin 35 786 km päässä maanpinnalta. Lisäksi tämä etäisyys tulee kaksinkertaistaa, koska radioaaltojen tulee kulkea tämä etäisyys kahteen kertaan. Ensin radioaallot kulkevat satelliitille ja tämän jälkeen ne kulkevat saman etäisyyden päästäkseen seuraavalle verkon osuudelle maan pinnalla. Tämän vuoksi näitä satelliitteja käyttävä henkilö kokee pelkästään tältä osuudelta noin 500 ms viiveen. (5.)

Satelliittilinkkien viivettä voidaan kuitenkin pienentää käyttämällä matalampaa kiertorataa ja esimerkiksi O3b Networks käyttää satelliitteja 8063 kilometrin Middle Earth Orbit (MEO) -kiertoradalla. Tämä muutos vähentääkin satelliittilinkin viiveen noin 100 ms:n luokkaan, joka tarpeeksi pitkään kuituyhteyteen verrattuna on erittäin lähellä kuidun viivettä. (5)

Sarjoitusviive

Sarjoitusviive tapahtuu, kun dataa muutetaan tietokoneen muistin biteistä tavuiksi (yksi tavu = 8 bittiä) ja tämä bittien sarja lähetetään käytössä olevan verkkoyhteyden yli tietyn kokoisina paketteina. Tämä muutos tarvitaan, jotta dataa voidaan lähettää verkkomedian yli. Sarjoituksessa kuluu aina määrätty aika, ja se voidaan laskea seuraavaa kaavaa käyttäen. (5.)

$$Sarjoitusviive(s) = \frac{Paketin\ koko\ (bittiä)}{Kaistanleveys\ (\frac{bitttiä}{s})}$$

Tästä kaavasta voidaankin nähdä, että kun pakettien koko pidetään alhaalla ja kaistannopeus on korkea, niin silloin sarjoitusviive on pienin mahdollinen. Esimerkkinä jos datapaketin koko on 1500 tavua (12000 bittiä), niin vanhan 56K-modeemin kaistanleveydellä sarjoitusviive olisi 214 ms ja 2 Mbs kaistanleveydellä tämä viive olisi 0,6 mikrosekuntia. (5) Koska nyky-yhteyksien kaistanleveydet ovat yleisesti vähintään 2 Mbs tai korkeampia, niin sarjoitusviiveen vaikutus jää huomattavasti etenemisviiveen varjoon, ja korkeimmilla nopeuksilla sarjoitusviive voidaan käytännössä unohtaa.

Verkkolaitteiston viive

Kun dataa välitetään mitä tahansa laajempaa verkkoa pitkin, kuten internetissä, niin paketit kulkevat aina reitittimien tai kytkinten kautta. Näitä laitteita kutsutaan runkolaitteiksi, ja ne keskustelevat toistensa kanssa ja selvittävät, mikä reitti datapaketille on parhain, jotta päästään kohteeseen. Laitteet päivittävät tietoja näistä reiteistä jatkuvasti, koska aikaisemmin nopein reitti voi olla poikki tai se voi olla tukossa liian suuren pakettimäärän vuoksi, joka voi sitten vaikuttaa kyseisen verkko-osuuden viiveeseen. (5.)

Laitteet itsessään lisäävät myös viivettä verkkoon. Korkean suorituskyvyn reitittimet ja kytkimet lisäävät viivettä noin 200 mikrosekuntia yhdellä yhteysvälillä, koska laitteiden tarvitsee lukea datapaketit aina, kun ne saapuvat, ja sen jälkeen ohjata paketti oikeaan suuntaan. Esimerkkinä viiveen vaikutuksesta voidaan olettaa internetin runkoverkossa olevan 800 km välein reitittimiä. Viive vastaisi silloin 40 km pidempää kuituyhteyttä. Tämän esimerkin mukaisesta tilanteesta voidaankin havaita, että viive kasvaa noin 5 % laitteiden vaikutuksesta. (5) Jos tätä viivettä haluttaisiin pienentää niin, käytännön kannalta parhain ratkaisu olisi saada laitteista tehokkaampia, mutta taas voitettu vähennys viiveeseen ei ole vielä tässä vaiheessa mielestäni kannattavaa.

Laitteiston viiveen jälkeen on myös mahdollisuus, että datapaketti jääkin odottamaan laitteessa vuoroa jatkolähetystä varten. Tätä kutsutaan jonotus viiveeksi. Joskus laitteesta ulos menevää dataa on liikaa, ja reititin tai kytkin joutuu odottamaan jonossa laitteen käsittelyviiveen jälkeen. Tässä vaiheessa viivettä voi tulla 20 ms lisää. (5)

2.3 Pakettihäviö

Pakettihäviötä tapahtuu kuin yksi tai useampi data paketti ei saavuta kohdettaan tietoliikenneverkossa. Pakettien tippuminen on yleensä merkki ongelmista verkkoyhteydessä, mutta on myös tilanteita, joissa paketteja tiputetaan tarkoituksella. (8.) Pakettihäviön havainnollistamiseksi käymme läpi, miten Internet on suunniteltu ja millä eri tavoilla pakettihäviötä käsitellään IP eli Internet-protokollan tasolla.

Wikipedia määrittelee Internet-protokollan seuraavasti:

> IP on TCP/IP-mallin Internet Kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkennäisessä Internet-verkossa. Se on myös koko internetin ydin ja ainoa asia, mikä kaikkia Internetiin liitettyjä tietokoneita yhdistää. (9.)

Yksinkertaistettuna IP yhdistää eri verkoissa olevat laitteet IP-osoitteella, jotta ne voivat keskustella keskenään.

Internet-protokolla suunniteltiin sillä ajatuksella että verkkolaitteiden toiminta voitaisiin pitää mahdollisimman yksinkertaisena. Protokolla pyrkiikin vain lähettämään datapaketit eteenpäin kohti sen määränpäätä parhaansa mukaan, mutta ei ota millään tavalla kantaa, saapuvatko paketit perille. Protokolla jättää tämän osuuden datan pyytäjän ja kohteen vastuulle. Tätä varten IP:seen onkin erikseen määritelty datapakettien kuljetusprotokollia, jotka ovat TCP eli Transmission Control Protocol ja UDP eli User Datagram Protocol. Molemmat protokollat huolehtivat tiedon saapumisesta, mutta hieman eri tavoin. TCP pyrkii varmistamaan luotettavuutta uhraten nopeutta, ja UDP keskittyy enemmän pakettien saapumiseen ajallaan tiputtamalla paketteja, jos ne ovat myöhässä. (8.)

Pakettien tippumista voi siis tapahtua, jos käytettävä kuljetusprotokolla huomaa, että paketissa on jotain ongelmaa tai se on myöhässä. Tämä ei kuitenkaan ole tyypillisin syy pakettien tippumiseen. Tyypillisin syy on verkon ruuhkautuminen eli network congestion. Tämä tukkeutuminen monesti johtuu joko tietyn verkon osan tai tietyn laitteen ylikuormittumisesta. Laitteet tässä tapauksessa vain saavat välitettäväksi liian paljon datapaketteja ja joutuvat tämän vuoksi tiputtamaan osan näistä paketeista, jos tilanne jatkuu tarpeeksi pitkään. (8.)

Tukkeutumisen lisäksi verkossa voi mahdollisesti olla fyysisiä vikoja, jotka myös voivat aiheuttaa pakettien tippumista. Esimerkkejä näistä vioista ovat: rikkinäiset johdot, radio-

aallon signaalin heikkous, sähkömagneettiset häiriöt, vialliset laitteet tai mahdolliset virheelliset asetukset verkkolaitteissa. (8.)

Pakettien tippumisen vaikutusta ei tavallinen verkon käyttäjä välttämättä huomaa lainkaan. Yleisin näkyvin tekijä voi olla verkon nopeuden hidastuminen, koska paketteja täytyy ladata uudelleen monia kertoja. Käyttäen aikaisempaa viiveen putki esimerkkiä (kts kuva 1) pakettien häviötä voi verrata putken vuotamiseen. Jos putken läpi halutaan tietty määrä dataa, ja on tiedossa, että tietty määrä dataa ”vuotaa” ulos putkessa kulkiessaan putken läpi, niin tämä määrä joudutaan korvaamaan. Tämän vuoksi saman datamäärän läpikulkuun putken läpi kuluisi pitempi aika.

Kaikki datapaketit eivät kuitenkaan ole samanarvoisia verkossa. TCP:tä käyttävät paketit ovat yleisemmin tärkeämpiä, koska niiden on välttämättä saavuttava perille, mutta protokolla huolehtii niiden saapumisesta perille, vaikka paketteja tippuisikin. TCP:tä voitaisiin käyttää esimerkiksi tiedostojen lataamisessa, jossa yksikin tiputettu paketti tarkoittaa käyttökelvotonta tiedostoa. UDP:tä käytetään taas suoratoistosovelluksien pakettien kuljetuksessa kuten videon tai VoIP (Voice over IP) -puheluiden välittämisessä, jossa pakettien tulisi saapua ajallaan tai ei lainkaan. Tämän vuoksi laadun takaamiseksi tukkeutumisen aikana saatetaankin tiputtaa vain TCP-paketteja, jotta suoratoistoa vaativien sovellusten palvelun taso voidaan pitää korkeana. Kun paketteja priorisoidaan tällä tavalla, niin puhutaan verkon Quality of Servicestä (QoS) eli palvelun laadusta.

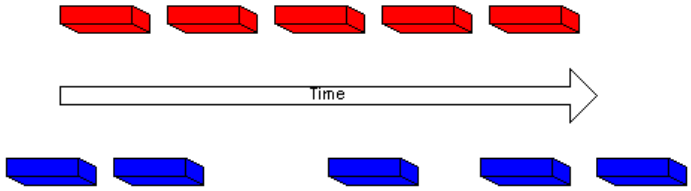
Minkälainen pakettihäviö on sitten hyväksyttävissä? Tämä riippuukin vahvasti siitä, millaista dataa ollaan siirtämässä. Muutaman paketin häviö VoIP-puhelu aikana ei aiheuta minkäänlaista heikkenemistä puhelun laatuun, mutta jos häviö kasvaa 5-10 %:n tasolle niin puhelun osapuolia voi olla melkein mahdoton ymmärtää. (8.)

Käytännössä verkossa on aina pientä pakettihäviötä, mutta vasta kun tämä häviö kasvaa tarpeeksi suureksi, sillä alkaa olla vaikutusta verkkoa käyttävien sovellusten toimintaan. Esimerkiksi TCP-protokolla käyttää liukuvaa ikkunaa pakettien lähettämisessä, jota protokolla muokkaa jatkuvasti. Tämä liukuva ikkuna määrittelee, kuinka paljon paketteja voi olla yhtäaikaisesti matkalla lähteen ja kohteen välillä. Kun paketti häviää TCP-yhteyttä käytettäessä, niin tämä aiheuttaa paketin uudelleenlähetyksen ja ikkunakoon pienenemisen, jolloin yhteyden efektiivinen nopeus pienenee. (5.)

2.4 Jitter

Pakettipohjaisissa verkoissa datapaketteja lähetetään säännöllisin väliajoin, jotta pakettien saapuminen olisi mahdollisimman tasaista. Viive vaikuttaa näiden pakettien saapumiseen kohteeseensa, mutta joskus verkon ongelmien vuoksi on myös mahdollista, että yksittäiset paketit saattavat kulkea pitemmän ajan samalla reitillä. Tätä eroa pakettien välisessä viiveessä kutsutaan nimellä jitter tai packet delay variation. (10.)

Kuvassa 3 olevat punaiset paketit ovat alkuperäisen lähettäjän säännöllisin välein lähettämät paketit verkkoon. Siniset paketit ovat samat paketit sen jälkeen, kun niihin on vaikuttanut verkon tukkeutuminen tai jokin muu häiriöntekijä. (10.)



Kuva 3 Jitteriä pääasiassa mitataan VoIP-puheluiden tai suoratoistosovellusten laadun parantamista varten, koska näissä palveluissa viiveen vaihtelu on huomattava. (9)

Perustiedonsiirrossa ei yleensä ole suurta merkitystä, milloin yksittäinen paketti saapuu, mutta VoIP-puhelun aikana kuitenkin monen paketin jatkuva myöhästyminen aiheuttaisi kuultavan puheeseen selkeitä kuultavia virheitä. On kuitenkin tapoja korjata verkon aiheuttamaa jitteriä. Ciscon reitittimissä tämä jitterin korjaus hoidetaan playout delay bufferilla, joka on oletuksena dynaaminen. Käytännössä tämä on välimuisti, johon reititin säilöö saapuneet paketit ja lähettää ne uudelleen sillä aikavälillä, millä paketit olivat alun perin lähetetty. Välimuistin dynaamisuus taas vaihtelee välimuistin koosta riippuen kuinka paljon jitteriä laite havaitsee pakettien saapuessa. (10.)

Tämän välimuistin käytöllä on kuitenkin pieni hinta. Jos jitterin määrä on suuri ja välttämättä halutaan säilyttää kaikki datapaketit, joita VoIP-puhelu käyttää, niin välimuistin käyttäminen lisää puhelun kokonaisviivettä. Tämä tapahtuu, koska jitterin poistoa varten reitittimen täytyy säilöä dataa sen ajan, että paketit voidaan lähettää halutulla säännöllisellä aikavälillä eteenpäin. Jos jitter on huomattavan suuri, niin välimuistin käyttö ei ole yksin riittävää, vaan laite joutuu tiputtamaan paketin. (10.)

Paketteja tiputetaan, koska aika, jota paketit odottavat välimuistissa, on lisätty puhelun kokemaan viiveeseen ja ylimääräisen viiveen lisääminen ei ole tietyn pisteen jälkeen enää sen arvoista. Laitteilla onkin parempia vaihtoehtoja korvata yksittäisiä aukkoja, jotka ovat syntyneet pakettien tiputuksen vuoksi. Esimerkiksi Ciscon reitittimillä on digitaalinen signaaliprosessori, joka pystyy laskemaan ”arvauksen” puuttuvien pakettien sisällöstä saapuneiden pakettien perusteella. (10) Tämä laskettu signaali sitten sijoitetaan aukon tilalle ja monissa tapauksissa pakettihäviön ollessa pieni, kukaan puhelun osapuolista ei edes huomaa, että paketteja olisi pudonnut.

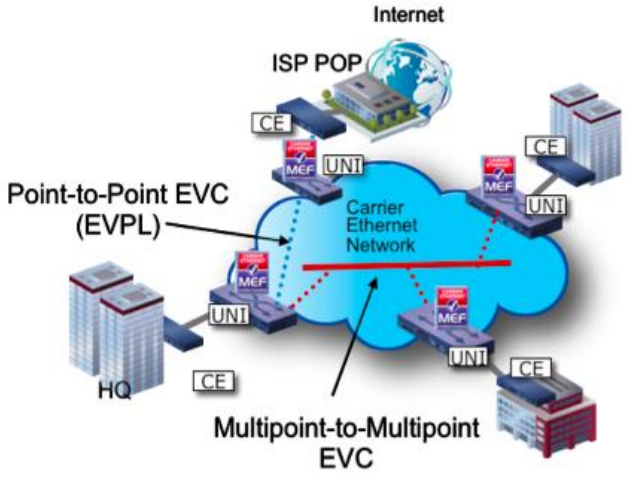
3 Operaattoritason Ethernet

Ethernet on pitkään ollut yleisimmin käytetty teknologia lähiverkkoja (LAN) rakentaessa, ja yhteyksien nopeudet ovat 30 vuoden aikana kasvaneet 10 Mb/s nopeudesta 100 Gb/s nopeuteen. Ethernet onkin kasvanut kaupunkiverkkojen (MAN) teknologiaksi ja on nyt laajenemassa myös laajaverkkojen (WAN) teknologiaksi sen halvan hinnan ja yhä kasvavan nopeuden vuoksi. Vielä tällä hetkellä IP on yleisin tapa tarjota verkon palveluja operaattori tasolla, mutta operaattorit ovat nyt huomanneet Ethernetin potentiaalin ja ovat alkaneet kehittää näitä palveluita.

Tärkein ero tavallisen Ethernetin ja operaattori-Ethernetin välillä on, että operaattoritasolle siirryttäessä tarvitaan paljon standardeja, joita LAN-tason Ethernet ei vaadi. Operaattori Ethernetiä varten Metro Ethernet Forum (MEF) on määritellyt kaksi standardoitua tapaa toimittaa palveluita operaattoritasolla. Ensimmäinen standardi on nimetty E-LINE:ksi, ja se on point-to-point-yhteys kahden toimipisteen välillä. Tämä yhteys muodostetaan Ethernet Virtual Connectionin (EVC) avulla, jolla voidaan yhdistää kaksi Ethernet-verkkoa toisiinsa toimipisteiden User Network Interface (UNI) -laitteilla. Nämä kyseiset laitteet toimivat operaattorin ja asiakkaan verkkojen välillä mahdollistaen verkkojen keskustelun keskenään. E-LINE -palvelussa on kaksi eri vaihtoehtoa toteuttaa tämä virtuaalinen yhteys, ja nämä ovat Ethernet Private Line (EPL) ja Ethernet Virtual Private Line (EVPL). (11.)

EPL:n ja EVPL:n erot ovat suhteellisen pienet. Käytännössä molemmat yhteydet ovat putkia verkon yli paikasta A paikkaan B, mutta EPL:n tapauksessa asiakkaalle on myyty fyysinen yhteys. EVPL:n tapauksessa taas on käytössä virtuaalinen yhteys, jossa on

mahdollisuutena käyttää montaa yhtäaikaista EVC:tä yhtä asiakkaan UNI:a kohtaan, jolloin laitteita tarvitaan vähemmän. Tällä menetelmällä voidaankin jakaa kulkevat paketit eri EVC:hin, joihin myös voidaan määritellä erilaiset palveluntasot. Kuvassa 4 löytyy esimerkki asiakkaan yhteydestä internettiin, joka on toteutettu EVPL:ää käyttäen. (11.)



Kuva 4 E-LINE (sininen yhteys) ja E-LAN (punainen yhteys)

Toinen MEF:n määrittelemä standardi operaattori Ethernetille on E-LAN. E-LAN on multipoint-to-multipoint EVC-palvelu, joka mahdollistaa liikenteen välittämisen monen eri toimipisteen UNI:en välillä yhtäaikaisesti. (11) Esimerkki tällaisesta yhteydestä toimipisteiden välillä löytyy aikaisemmasta kuvasta 4.

Operaattori Ethernetin hyvänä ominaisuutena tulee myös mainita, että sitä voidaan käyttää muiden vanhojen kuljetusteknologioiden ylitse käyttäen esimerkiksi virtuaalisia privaattiverkkoja (VPN:iä) (11). Tämä jo yksinään kasvattaa operaattori Ethernetin kustannuustehokkuutta, koska operaattorin ei tarvitse välttämättä uusia koko verkkoaan Operaattori Ethernetin käyttöönotossa. Sama tilanne myös pätee asiakkaisiin ja kannustaa asiakkaitakin vaihtamaan kyseisen teknologian käyttöön.

Kuitenkaan perus-LAN-tyypin hallinta- ja vianselvitystyökalut eivät ole riittäviä hallinnoimaan MAN- tai WAN-tason yhteyksiä eikä SLA:ta. Näitä työkaluja on kuitenkin lisätty Ethernet OAM -standardien avulla. (11.)

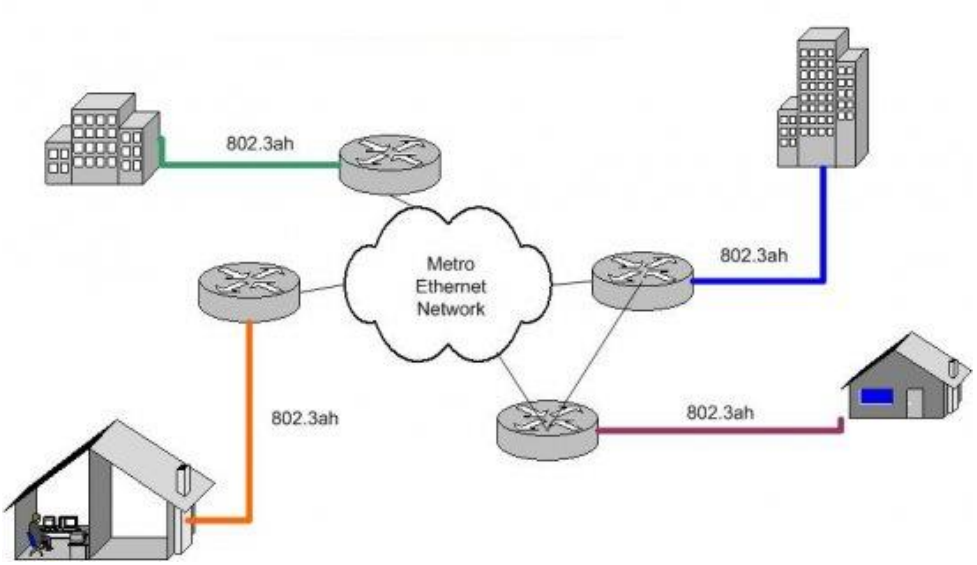
3.1 OAM

Operations, administration ja management eli OAM sisältää joukon erilaisia toimintoja ja työkaluja, joita verkkoa hallinnoiva taho tarvitsee operaattoritasoisen verkon hallinnoimiseen ja monitoroimiseen. OAM:n tärkeimmät toiminnot liittyvät yhteyksien varmistukseen, vikojen havaitsemiseen, suorituskyvyn valvontaan ja palvelunlaadun valvontaan. Palvelunlaadun valvontaan Ethernet-tasolla erityisesti on lisätty työkaluja saatavuuden, viiveen, jitterin ja pakettihäviön mittaamiseen, joita on kipeästi tarvittu. Nämä mittarit antavat valmiudet huomata nousevia vikoja koko verkon tasolla ennen kuin ne kasvavat sille tasolle, että ne vaikuttaisivat verkon käyttäjiin. (12.)

Näitä standardeja on ollut työstämässä seuraavat tahot: Insitute of Electrical and Electronics Engineers (IEEE), International Telecommunications Union (ITU), ja aikaisemmin mainittu MEF. Nämä kolme tahoa ovat työstäneet Ethernet OAM:n standardeja yhteistyössä, jotta standardit eivät aiheuta suurempia päällekkäisyyksiä. Jokainen erillinen standardi lisää uusia ominaisuuksia ja rakentaa OAM-standardista laajemman kokonaisuuden. (12.)

3.2 Ethernet Link OAM

Ethernet Link OAM on määritelty IEEE 802.3 -standardin momentissa 57 ja standardi oli alun perin kehitetty Ethernet in the First Mile (EFM) -välisen yhteyden monitorointiin ja sitä kutsutaan monesti sen vanhalla nimellä ”802.3ah”. EFM:llä viitataan linkkiin, joka on operaattorin ja asiakkaan laitteiden välillä. Ensimmäisestä asiakkaan laitteesta myös käytetään nimitystä demarkaatiopiste, koska vastuu verkontoiminnasta siirtyy asiakkaalle tästä laitteesta eteenpäin. Ennen tämän standardin kehitystä Ethernet-tasolla ei ollut lainkaan keinoja hallinnoida fyysisiä linkkejä. (13) Esimerkkejä tästä yhteysvälistä löytyy kuvassa 5.



Kuva 5 802.3ah eli Ethernet First Mile

Ethernet Link OAM:n toimimiseksi protokolla käyttää erikseen määriteltyjä datapaketteja OAM Protocol Data Uniteja (OAMPDU), jotka voivat kulkea vain yhden linkin ylitse Ethernet-verkossa. Jotta paketit eivät veisi huomattavasti yhteyden kaistanleveyttä, pakettien lähetysnopeus on rajoitettu protokollassa kymmeneen pakettiin per sekunti. (13.)

Tärkeimpiä ominaisuuksia Link OAM:ssä ovat:

- Laitteiden havainnointi – Linkin laitteiden ja OAM-ominaisuuksien havaitseminen.

- Linkin monitorointi – Linkin vikojen paikallistaminen ja datapakettien virheiden raportointi.

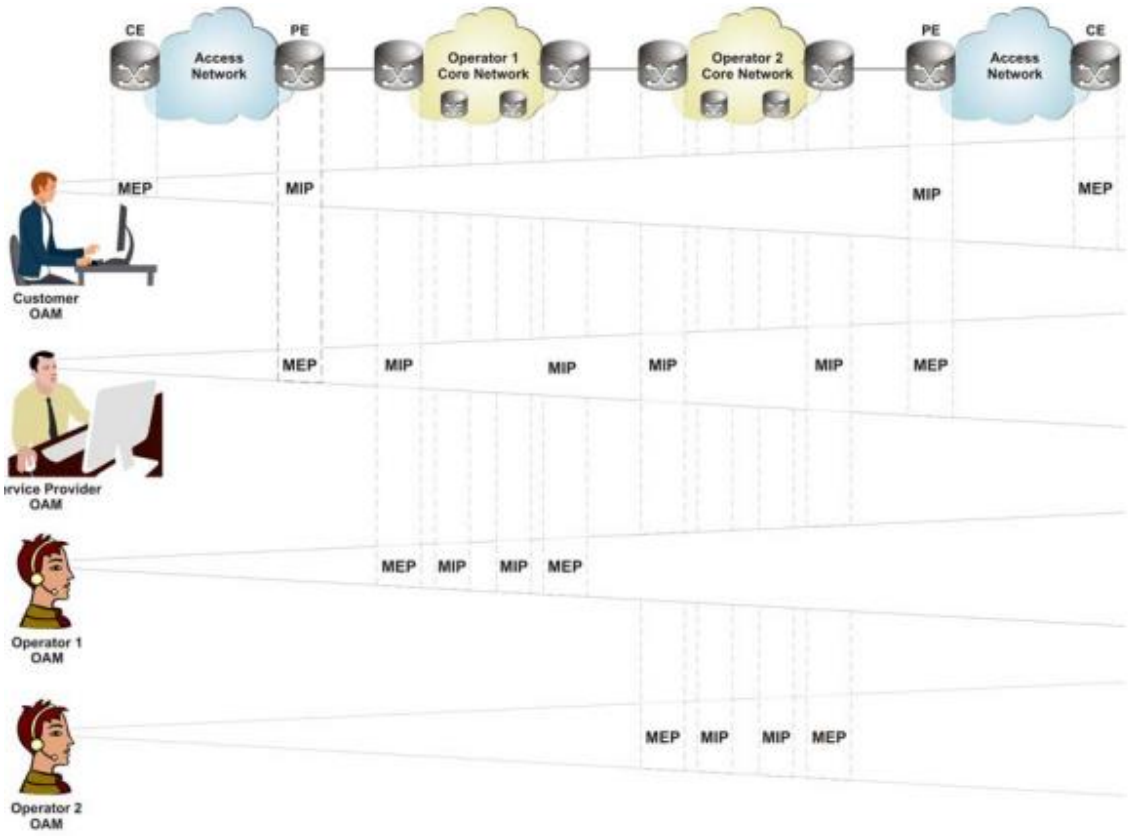
- Remote Failure Indication – Toiminto jolla laite ilmoittaa linkin toiseen päähän laiteviasta kuten virtalähteen hajoamisesta ja muista kriittisistä vioista. Laitteen viimeisestä ilmoituksesta käytetään termiä dying grasp. Nämä viestit kulkevat OAMPDU:n sisällä olevilla tietyillä merkkibitin arvoilla.

- Remote Loopback – Toiminto jolla laite pystyy loopback control OAMPDU:n avulla asettamaan linkin sellaiseen tilaan missä toinen laite palauttaa kaikki sille lähetetyt datapaketit. Toiminto on tärkeä linkin vianetsinnässä ja asennusvaiheessa. (13.)

3.3 Ethernet Connectivity Fault Management

Connectivity Fault Management (CFM) on IEEE 802.1ag -standardissa luotu malli monen operaattorin kattavassa verkossa päästä päähän riippumatta, missä vika todellisuudessa onkaan. CFM:ssä verkko on jaettu erillisiin huollon toimialueisiin, jotka on luokiteltu erillisille tasoille toimialueen laajuudesta riippuen. Kun verkko on jaettu eri toimialueisiin, niin CFM määrittelee jokaisen toimialueen lopussa olevan laitteen linkin portin maintenance end pointiksi (MEP). Kaikki toimialueen sisälle jäävät laitteiden portit, jota kautta yhteys kulkee, määritetään maintenance intermediate pointeiksi (MIP). Tämän tarkoitus on auttaa määrittelemään huollon vastuualueet ja parantamaan jokaisen vastuullisen tahon vianselvitysmahdollisuuksia. (12.)

CFM:ssä määritellyt toimialueet on aina määritelty tietynlaisen hierarkian mukaan, ja standardi antaa valmiudet enintään 8 eri tason käyttöön. Kuvassa 6 on esimerkki tällaisesta verkon hierarkiasta. Se alkaa operaattoreista, jotka voivat vain tarkkailla omia laitteitaan. Tämän jälkeen tulee palveluntarjoaja, joka omien laitteidensa lisäksi pystyy myös näkemään operaattorien laitteet MIP:einä. Viimeiseksi tasoksi jää asiakas ja hänen laitteensa. Asiakas omalla tasollaan pystyy näkemään omat laitteensa, joita kutsutaan Customer Edge (CE) laitteiksi ja palveluntarjoajan laitteet, joista käytetään nimitystä Provider Edge (PE). (13.)



Kuva 6 Esimerkki CFM:n määrittelemästä OAM hierarkiasta (12)

CFM:n kaikki paketit on määritelty Ether-tyypiksi (0x8902). Tämä määritys on tehty sen vuoksi, että jokainen verkon laite pystyy välittämään CFM:n viestit eteenpäin, vaikka viestin vastaanottanut laite ei tukisi lainkaan CFM:ää. Kohde MEPin vastaanottaessa paketin se ei välitä sitä enää eteenpäin, koska CFM:n paketit liikkuvat vain niiden oman toimialueen sisällä. Tähän on kuitenkin yksi poikkeus. Jos kyseinen MEP on myös MIP korkeamman toimialueen sisällä, niin se välittää tämän toimialueen paketit eteenpäin kyseisen korkeamman toimialueen MEP:lle. (13.)

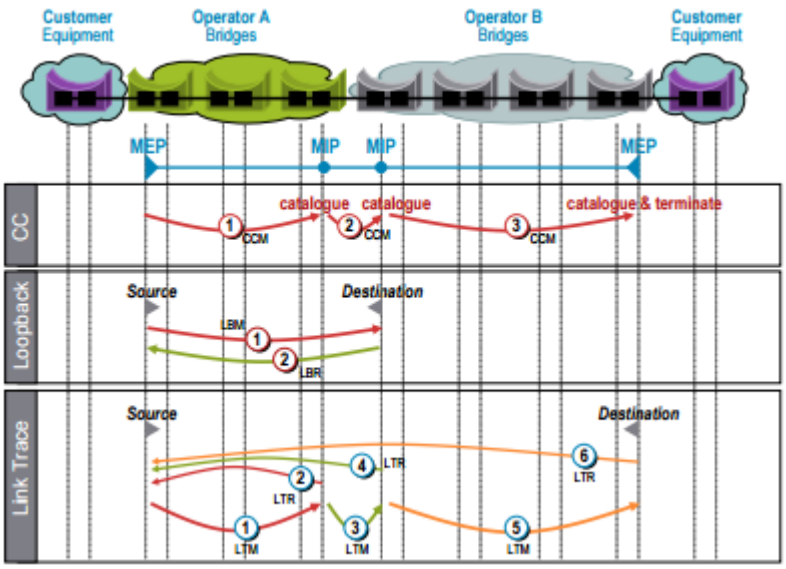
CFM sisältää myös seuraavat tärkeät ominaisuudet Ethernet-verkon vianselvitystä varten: Connectivity Check (CC), Loopback-viestit ja Link Trace -viestit.

Connectivity Check toimii MEP:ien Connectivity Check Messageilla (CCM), jotka lähetetään toimialueen kaikille laitteille multicast-lähetyksenä MAC-osoitteen perusteella. Näiden viestien avulla MEP:it voivatkin itse havaita yhteysongelmia toimialueensa sisällä. Tätä ominaisuutta kutsutaankin yleisesti heartbeat-viestiksi, koska laitteet lähettävät viestejä säännöllisesti siitä lähtien, kun CC aktivoidaan. Tällä samalla ominaisuudella MEP:t myös löytävät toisensa verkossa ja MIP:it saavat tiedon toimialueen

MEP:stä. CC:tä joudutaan kuitenkin käyttämään tarkkaan, koska jos viestien väliaika on pieni ja verkko sisältää paljon MEP:tä, CC voi aiheuttaa verkkoon huomattavan kuorman. (13.)

Loopback viestillä voidaan tarkistaa reitti tiettyyn kohteseen järjestelmänvalvojan näin halutessa. Tätä varten MEP lähettää Loopback Message (LBM) kohteelle ja kohteen saadessa tämän viestin niin se vastaa Loopback Reply (LBR) viestin lähettäneelle MEP:lle. (13.)

Link Trace viestejä käytetään, kun verkon ylläpitäjä haluaa tietää mitä reittiä tiettyyn MEP:iin kulkevat paketit käyttävät. Link Trace toimii Link Trace Message (LTM) ja Link Trace Reply (LTR) viestien avulla. MEP lähettää LTM viestin kohti kohdetta ja aina kun viesti saavuttaa uuden MIP:n tai MEP:n niin kyseinen laite lähettää alkuperäisen viestin lähettäneelle MEP:lle LTR vastauksen. (13.)



Kuva 7 Connectivity Checkin, Loopbackin ja Link Tracen toiminta (13)

3.4 Performance Monitoring

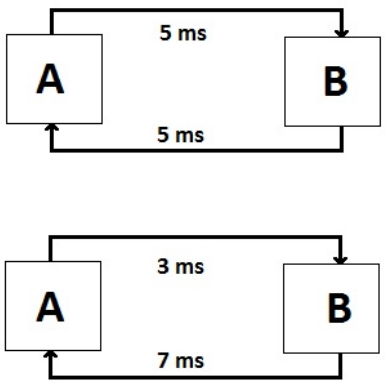
Y.1731 Performance Monitoring (PM) on standardi Ethernet-verkkon suorituskyvyn mittausta varten. PM mahdollistaa mitata Ethernet-pakettien viivettä, jitteriä, pakettihäviötä ja verkon yli kulkevien pakettien määrää.(14) Y.1731 sisältää myös osittain samoja ominaisuuksia kuin IEEE 802.1ag -standardi, mutta kuitenkin Y.1731:n tärkein ominaisuus

on PM. Ilman PM:n antamia toimintoja laadunvalvonta Ethernet-verkossa olisi äärimmäisen rajallinen.

PM:n suorittamat mittaukset, kuten viiveen ja jitterin mittaus, tehdään lähettämällä synteettisiä paketteja toimialueen MEP:ien välillä, ja vastaanottava MEP lähettää vastauksen alkuperäiselle lähettäjälle. CFM ja PM toimivat samoilla periaatteilla, mutta PM tarvitsee huomattavasti enemmän paketteja jotta mittausten tarkkuus voidaan pitää korkeana ja ajantasaisena. (15.)

Y.1731-standardissa verkon viiveen, jitterin, pakettihäviön mittaaminen on määritelty toteutettavaksi kahdella eri menetelmällä. Nämä ovat yhdensuuntainen ja kahdensuuntainen mittaus. Menetelmien suurin ero on, että yksisuuntaisella mittauksella laitteiden välinen kello on oltava synkronoitu ja kaksisuuntaisessa mittauksessa tätä ei tarvita. Tämä synkronointi suoritetaan Network Time Protokollaa (NTP) käyttäen. Yksisuuntaisella mittauksella toinen MEP:stä toimii lähettävänä osapuolena ja toinen MEP:stä vastaanottajana. MEP lähettää aikaleimatun paketin ja vastaanottava MEP vertaa tätä aikaleimaa omaan kelloonsa ja suorittaa tarvittavat laskutoimitukset. Kaksisuuntaisessa mittauksessa taas MEP:n vastaanottaessa paketin vastaanottava MEP lähettää saman paketin takaisin alkuperäiselle lähettäjälle, joka huolehtii tiedon käsittelystä. (15.)

Yksisuuntaisessa mittauksessa on myös se hyöty, että tällä mittaustavalla voidaan tarkastella, mikä linkin viive todellisuudessa on. On aina mahdollista, että linkissä ei ole samaa viivettä datapaketin palatessa, kun sillä oli alun perin saapuessa. Esimerkki tällaisesta tapauksesta löytyy kuvasta 8. Kaksisuuntaisessa mittauksessa tulos olisi molemmissa tapauksissa 10 ms. (15.)



Kuva 8 Esimerkki viiveestä mikä voidaan huomata vain yksisuuntaisella mittauksella

Y.1731 myös määrittelee uuden tavan mitata pakettihäviötä. Standardissa on määritelty ominaisuus nimeltä Synthetic Loss Measurement (SLM). Aikaisemmin pakettihäviön mittaamista varten on jouduttu käyttämään verkon yli liikkuvaa dataa mittauksia varten. Nyt kuitenkin SLM:ää käyttäen voidaan verkon yli lähettää synteettisiä, ETH-SLM-paketteja, joiden perusteella voidaan laskea pakettihäviö. (15.)

3.5 Network Interface Device

Operaattoritasoisen Ethernet-verkon hallinnointi ei kuitenkaan onnistu pelkkien uusien standardien avulla vaan tarvitaan myös laitteita, jotka tukevat näitä käytössä olevia standardeja. Tämän korjaamiseen on onneksi vaihtoehto käyttää Network Interface Deviceja (NID) jotka mahdollistavat kaikkien Ethernet OAM -toimintojen käytön verkon päästä päähän. (16.)

Tällä hetkellä verkon yleisimmät demarkaatiopisteissä olevat laitteet eivät pysty käyttämään 802.1ag/Y.1731-standardeja EFM:llä. Tämä tarkoittaa, että NID:jä käytettäessä voidaan joko käyttää 802.3ah-standardia ja saada muutamia OAM-ominaisuuksia käyttöön tai tälle välille ei saada lainkaan OAM:ää, ja SLA:n mittaaminen ei onnistu lainkaan. Demarkaatiopisteen laitteen vaihtaminen NID:iin taas muuttaa tilanteen täysin, koska laite on varta vasten suunniteltu mittaamaan OAM:ää ja käyttämään 802.1ag/Y.1731-standardin ominaisuuksia. Tämän avulla todellinen päästä päähän monitorointi on mahdollista, koska NID:t toimivat asiakkaan OAM-tason MEP:nä. (16.)

NID:en käytössä on myös muitakin hyviä ominaisuuksia, jotka parantavat OAM:n mittaamista verrattuna tavallisiin verkkolaitteisiin. Verkkolaitteet on pääasiassa suunniteltu suorittamaan toimenpiteitä datapakettien kuljettamisessa ja käsittelyssä, jonka vuoksi OAM-toiminnot tapahtuvat näillä laitteilla sekundäärisellä prioriteetilla riippuen, miten paljon verkko on kuormittunut. Saman syyn vuoksi tavalliset verkkolaitteet voivat vain tarkkailla muutamia SLA:oita kerralla riippuen laitteen kuormituksesta NID:eissä taas on oma prosessori, jonka tehtävä on pelkästään laskea laitteeseen määritellyt SLA:t. Tämän prosessorin avulla NID pystyy laskemaan sataa yhtäaikaista SLA:ta ilman vaikutusta laitteen suorituskykyyn. (16.)

Kuva 9 Accedian EtherNID (vasen) ja MetroNID (oikea) (15)

NID:t myös lisäävät tiettyjen SLA-mittausten tarkkuutta. Tavallinen verkkolaite pystyy mittaamaan vain kaksisuuntaista viivettä 1 ms:n luokassa vaihtelevalla tarkkuudella. Laitteiden käyttämä SLM-pakettihäviö mittaaminen ei myöskään ole tarpeeksi tarkka, koska laskennoissa käytetään vain OAM-paketteja. NID:t taas pystyvät suorittamaan molemman suuntaisia mittauksia 1 µs:n tasolla. Mittausten virheen marginaali on luokkaa < 20 µs ja tämän lisäksi NID pystyy mittaamaan pakettihäviötä Real Frame Loss (RFL) -ominaisuudella. RFL on laitteiston avulla toteutettu ratkaisu, joka mahdollistaa reaaliaikaisen pakettihäviön mittaamisen. (16.)

4 Echovault

Echovault on suomalaisen Creanord-yhtiön luoma sovellus operaattoritason SLA:n mittaamista, mittauslaitteiden konfigurointia ja verkon monitorointia varten. Echovaultin arkkitehtuuri koostuu yhdestä pääkontrollerista, vaihtoehtoisista paikalliskontrollereista ja NID:eistä, joihin on asennettu Echoagent-sovellus. Lisäksi Echovault sisältää paljon erilaisia työkaluja SLA-raporttien luomiseen asiakkaita varten.

SLA:n mittaamisessa Echovaultin kaikki konfigurointi tehdään selainpohjaisesta käyttöliittymästä. Täältä voidaan valita kaikki Key Performance Indikaattorit (KPI), joita halutaan mitata tiettyjen NID:en väliltä. Nämä KPI:t vastaavat aikaisemmin käsiteltyjä SLA-mittareita, kuten viivettä tai jitteriä. Echovault käsittelee KPI-datan sellaiseen muotoon, että siitä saadaan toimintaa kuvastavia SLA:ita.

Näitä KPI:ta mitataan Echovaultissa määritettyjen testi policyjen avulla. Echovault lähettää XML-muotoiset konfiguraatiot NID:eille, joihin on määritelty lähettävät ja vastaanot-

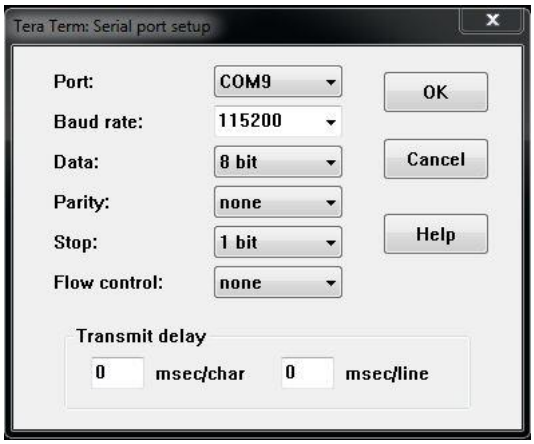
tavat NID:t ja myös, mitä KPI:ta halutaan tarkkailla. NID:en vastaanotettua nämä konfiguraatiot ne aloittavat mittaamisen ja raportoivat mittauksien tuloksista takaisin Echovaultille.

5 Työ

Työn toteuttamisessa käytettiin kahta eri verkkoa ja Leppävaaran kampukselle asennettua Echovault-sovellusta. Ethernet tason konfigurointi tehtiin verkkoon, jossa oli kaksi Cisco Catalyst 2960 -kytkintä ja yksi Cisco Catalyst 3560 -kytkin. Testilaitteina käytettiin kahta Accedianin EtherNID NID:iä. IP-tason konfigurointi tehtiin yhden Cisco 2811 -reitittimen läpi. Molempien mittausten konfigurointi suoritettiin Metropolian laboratorioluokassa, ja konsoliyhteys laitteisiin on otettu Tera Term sovellusta käyttäen.

5.1 NID:en yleiset asetukset

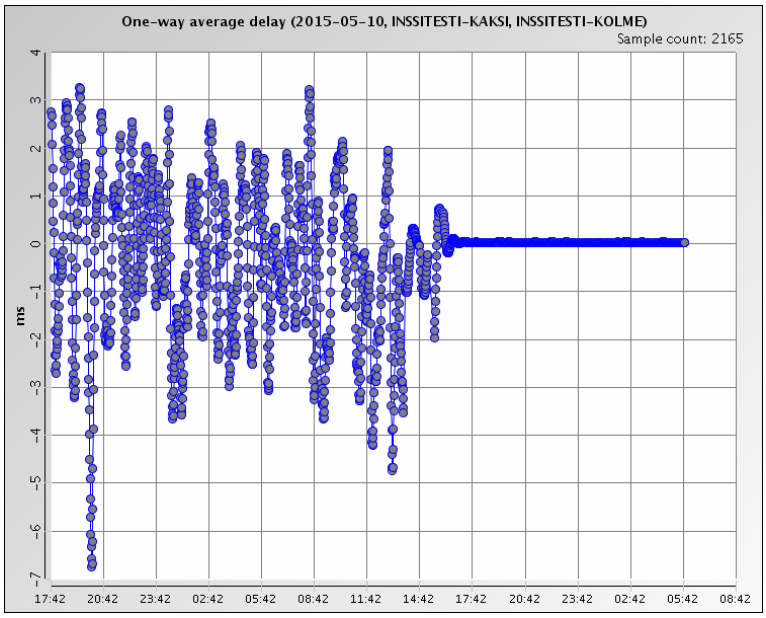
Ennen kuin mittauksia voidaan tehdä, täytyy NID:t saada yhdistettyä Echovaultiin. Tämä onnistuu helpoiten yhdistämällä NID:n management-portti koulun laboratorioverkkoon, josta laite hakee DHCP:ltä IP-osoitteen automaattisesti. Laitteet konfiguroidaan helpoiten konsoliportin kautta. Konsoliyhteyden muodostaminen tehdään sarjaportin kautta ja siihen tarvitaan kuvassa 10 olevat asetukset. Port-asetus kuitenkin riippuu käytössä olevasta tietokoneesta, ja tämä tulee vaihtaa siihen COM-porttiin, mihin kaapeli on tietokoneessa kytketty.



Kuva 10 Tera Term -sarjaportin asetukset

Kun yhteyden muodostaminen laitteeseen onnistuu, niin laite pyytää käyttäjätunnusta ja salasanaa. Kirjautumisen jälkeen NID kannattaa resetoida tehdasasetuksille komennolla ”Configuration reset”. Tämä on suositeltavaa, koska laitteessa voi mahdollisesti olla vanhoja konfigurointeja.

Tämän toimenpiteen jälkeen yhdestä NID:stä tulee määritellä NTP-palvelin, joka päivittää kelloaan koulun NTP:ltä muille NID:lle. Tämä prosessi on äärimmäisen tärkeä, koska jos NID:t asetetaan päivittymään suoraan koulun NTP:ltä, niin kellojen synkronointi ei ole riittävän tarkka yksisuuntaisten mittausten toteuttamiseksi. Kuvassa 11 näkyykin, millainen vaikutus mittauksiin on, kun NID:n NTP-palvelin otettiin käyttöön ja synkronointi oli valmis noin klo 17:00. Aikaisemmin arvot vaihtelivat -7 ms ja 3 ms välillä, mutta muutoksen jälkeen mittaustulokset pysyivät 0,032 ms:n (± 0,002 ms) arvossa.



Kuva 11 NTP-palvelimien tarkkuuden ero

NTP-palvelimen konfigurointia varten NID:lle lisätään koulun NTP-palvelin, jotta saamme laitteen mahdollisimman lähelle Echovaultin aikaa. Tämän jälkeen laitteen NTP-palvelinominaisuus tulee aktivoida, ja tämä vaatii, että laiteelle asetetaan normaali resoluutio korkean resoluution sijaan. Muuten palvelinta ei saada aktivoitua. Kaikki komennot NTP-palvelimen konfigurointiin löytyy kuvasta 12.

```
ntp edit sync-mode normal
ntp add 10.95.254.253
ntp enable 10.95.254.253
ntp enable-server
ntp utc-hour 3
```

Kuva 12 NTP-palvelimen konfigurointi NID:lle.

Palvelimen aktivoinnin jälkeen muille NID:lle riittää, että NTP NID:n Management-portin IP-osoite lisätään laitteen NTP palvelinlistalle ja NTP aktivoidaan käyttöön. NTP client NID:ien konfiguraatio löytyy kuvasta 13.

```
ntp add "NTP NIDn Management portin IP-osoite"
ntp enable "NTP NIDn Management portin IP-osoite"
ntp utc-hour 3
```

Kuva 13 NTP clientin aktivoiminen.

NTP-konfiguraatioita tehdessä tulee kuitenkin ottaa huomioon, jos käytössä on kesäaika. Utc-hour 3 -komennolla laitteet määritellään Suomen aikavyöhykkeelle kesäaikaan, mutta talviajassa ajan tulisi olla tunnin vähemmän. Tämän vuoksi jos laitteiden kellot heittävät tunnilla, niin helpoin keino tämän korjaamiseen on vain muuttaa ”ntp utc-hour 3” -komennossa arvo kakkoseksi. Laitteessa on mahdollista konfiguroida automaattinen talviajan muutos, mutta se ei ole laitteen perustuntemuksen kannalta olennainen ominaisuus.

Kun kaikkien laitteiden NTP-asetukset ovat kunnossa, niin tulee odottaa jonkin aikaa kunnes ”ntp show” -komennolla voidaan varmistaa, että ”Sync status”-kohdassa lukee ”Syncronized” kaikissa laitteissa. Alla olevasta kuvasta 14 löytyy esimerkki onnistuneesta synkronoinnista.

```
INSSITESTI-KAKSI: ntp show

NTP client     : Enabled
NTP server     : Disabled
TAI offset     : 34
DSCP           : 0
VLAN priority  : 0
Sync mode      : High resolution
Sync status    : Synchronized
```

Kuva 14 Onnistunut NTP-synkronointi

Kellonajan päivittymisen jälkeen NID:t ovat valmiit Echovaultiin yhdistämiseen. NID tarvitsee yhteyden muodostamista varten tietoon Echovault-kontrollerin IP-osoitteen, käytössä olevan protokollan, käytettävän portin ja lopuksi salasanan, jolla yhteys voidaan muodostaa. Komennot näiden tietojen lisäämiseen NID:eihin löytyy kuvasta 15.

```
echoagent edit controller_1 195.148.98.185
echoagent edit communication_protocol https
echoagent edit port 443
echoagent edit password "Kontrollerin salasana"
echoagent enable
```

Kuva 15 Echoagent aktivointi

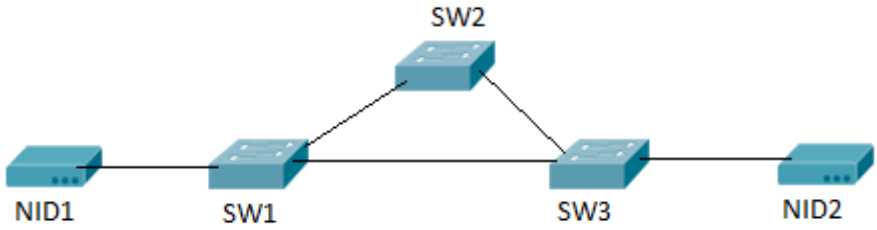
Kun echoagentin konfigurointi on kunnossa, niin ”echoagent show” -komennolla tulisi näkyä kuvaa 16 vastaava tilanne ja tämän jälkeen laitteen tulisi päivittyä Echovaultiin.

```
EchoAgent status:
Mon May  4 15:46:04 2015 : Agent start(ID:E005C9699).
Mon May 18 13:48:19 2015 : Agent status(connected).
-----------------------------------------------------
Mon May 18 13:48:19 2015 : https://195.148.98.185:443/
Mon May 18 13:48:02 2015 : https://195.148.98.185:443/
```

Kuva 16 Echoagent yhteydessä Echovaulttiin

5.2 Ethernet-tason SLA-mittaus

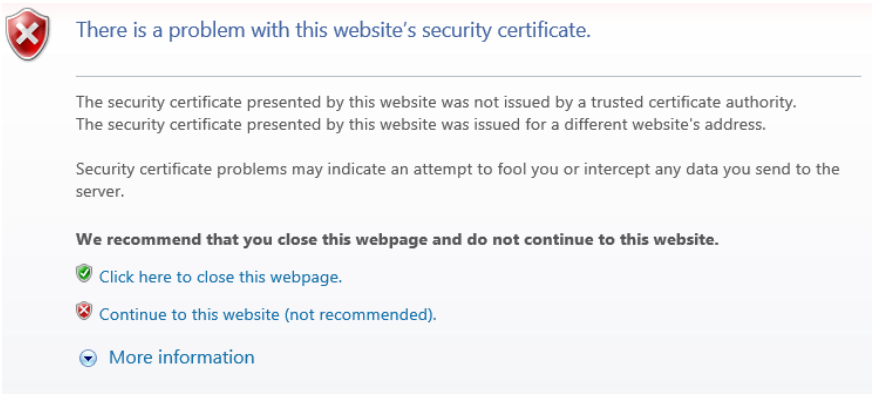
Ethernet-tason mittaukset toteutettiin kolmen kytkimen verkossa, missä kaikki kytkimet on yhdistetty toisiinsa muodostaen ringin. Verkon rakentamisessa kytkimet eivät vaadi erillistä konfiguraatiota, ja molemmat NID:t on yhdistetty verkkoon laitteiden RJ-45 B eli network-porttien kautta. Verkko on havainnollistettu kuvassa 17. Laitteet on myös erikseen yhdistetty koulun laboratorio-verkkoon niiden Management-portin kautta, jotta laitteet voivat lähettää mittausten tiedot Echovaultille.



Kuva 17 Ethernet-mittausten testiverkko

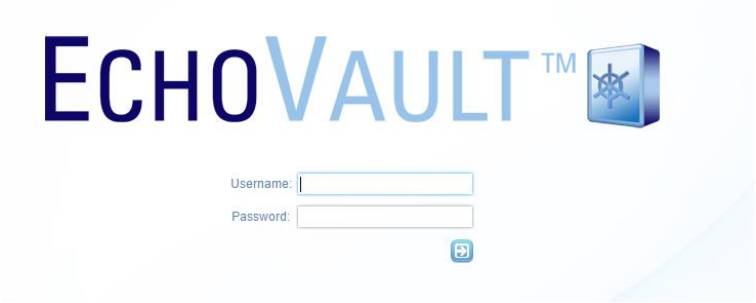
Ethernet-tason mittauksissa laitteille ei tarvitse tehdä mitään erillisiä konfiguraatioita, jotta mittaukset onnistuvat. Riittää että laitteet kytketään verkkoon ja mittaukset konfiguroidaan Echovaultin kautta oikein.

Echovaulttiin voidaan muodostaa yhteys internetselaimesta käyttämällä osoitetta https://195.148.98.185/. Ennen sivustolle pääsyä selain ilmoittaa ongelmasta sivuston sertifikaatin kanssa, koska se ei ole luotettava. Tästä virheestä ei kuitenkaan tarvitse välittää tässä tapauksessa, koska kyseessä on koulun ylläpitämä palvelu eikä tuntematon Internet-sivu.



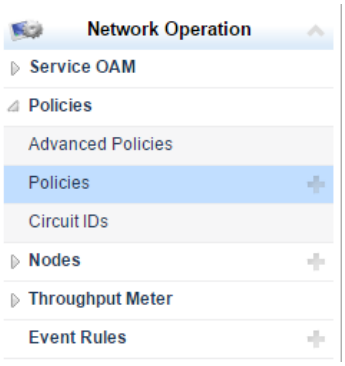
Kuva 18 Sertifikaattivirhe Internet Explorerissa

Tämän jälkeen avautuu Echovaultin kirjautumisikkuna, johon tarvitaan Echovaulttiin määritelty erillinen käyttäjätunnus ja salasana.



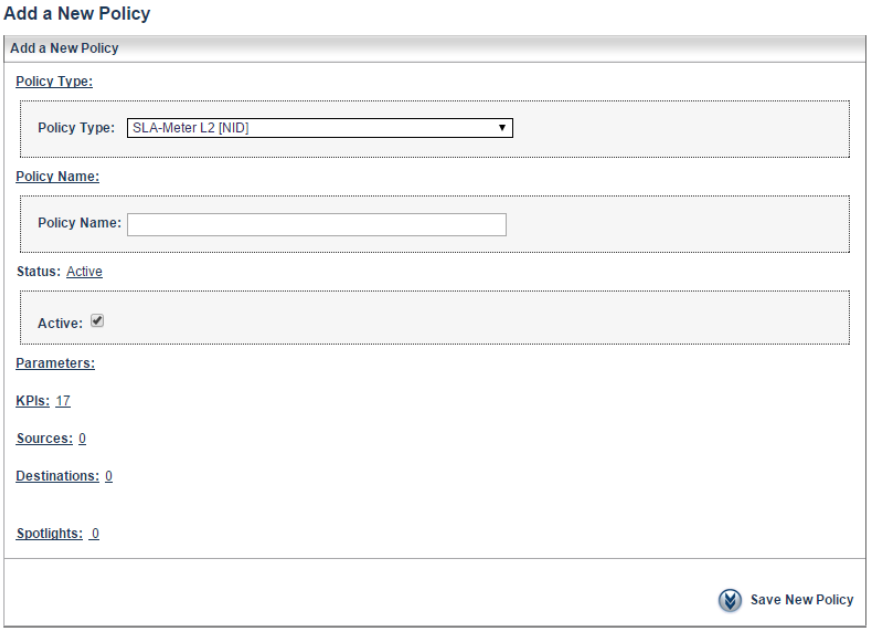
Kuva 19 Echovault kirjautumisikkuna

Mittauksen konfiguraation määrittäminen aloitetaan Policies-valikosta, joka löytyy Network Operations-osuuden alta päävalikossa (kts kuva 20). Policyn luonnin voi aloittaa joko Policies-otsikon vieressä olevasta plus-merkistä tai policies-sivuston ylälaidassa olevasta ”Add a New Policy” -linkistä.



Kuva 20 Policies-valikko

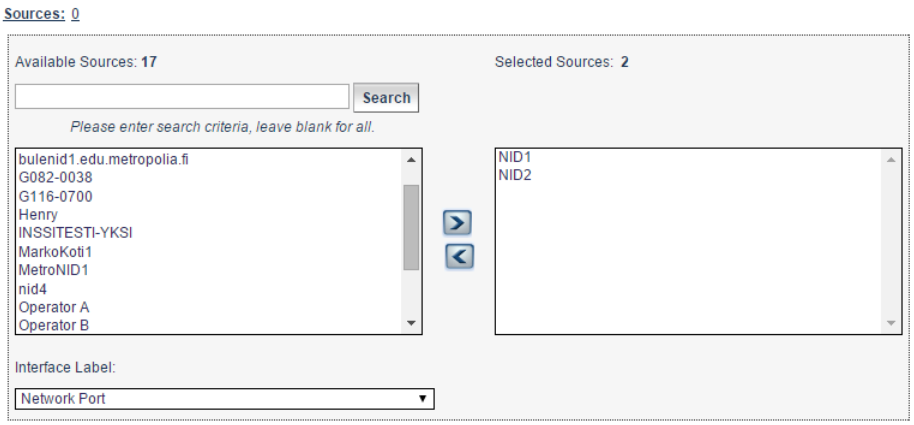
Seuraavaksi tulee määritellä, mitä tarkalleen halutaan mitata. Koska tarkoituksena on mitata Ethernet-verkon SLA:ta, niin Policy type -alasvetovalikosta tulee valita vaihtoehto ”SLA-Meter L2 [NID]”. Tämän valinnan jälkeen sivustolle ilmestyy policyn määrittämisen eri vaihtoehdot (kts kuva 21). Tärkeimmät kohdat, jotka vaativat muutoksia tällä sivulla ovat policy name, sources ja destinations. Policy name kohtaan voi keksiä minkä vaan kutsumanimen, jotta policyn voi tunnistaa helposti.



Kuva 21 Policyn määritys

Seuraavaksi source- ja destination-osioihin tulee määritellä, mitä laitteita halutaan käyttää lähteinä ja vastaanottajina. Source-osiossa määritellään, mikä NID lähettää paketteja ja destination-kohdassa löytyy pakettien vastaanottajat. Tässä esimerkissä konfigurointi

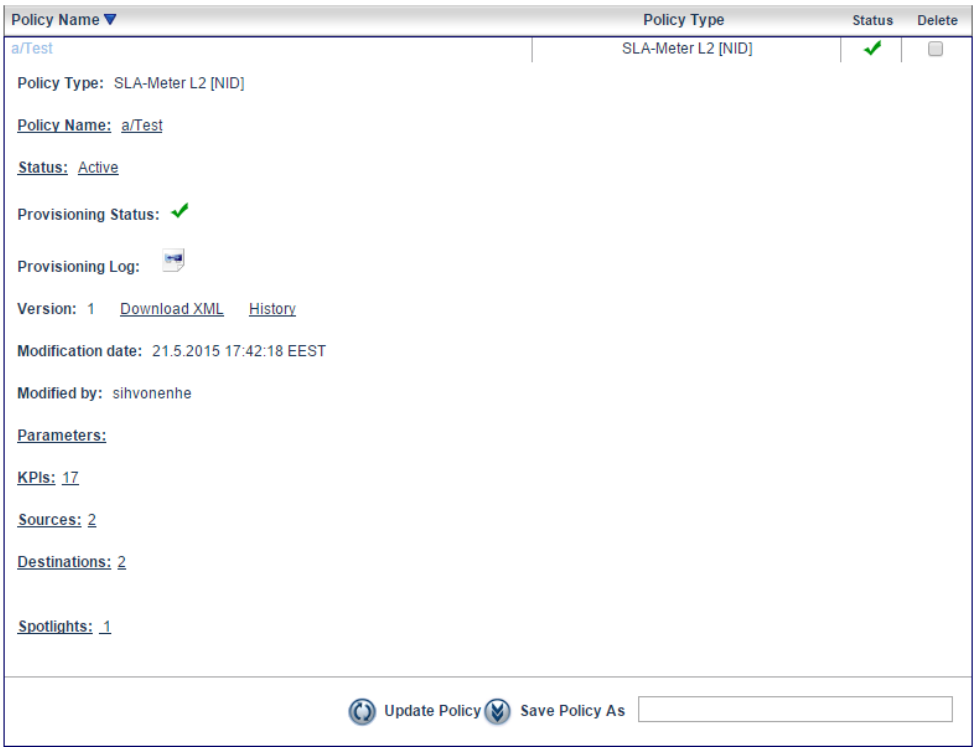
määritellään niin, että molemmat laitteet lähettävät ja vastaanottavat mittauksien paketteja. Kuvassa 22 on esimerkki, miltä molempien osioiden tulisi näyttää. Käyttöön tulevat NID:t valitaan yksi kerrallaan vasemmasta valikosta ja siirretään oikeaan painamalla oikealle osoittavaa nuolta. Kun NID:t on valittu, niin pitää myös valita osion alalaidasta, mitä interface labelia tullaan käyttämään. Tähän voi valita oletusvaihtoehdon ”Network port”.



Kuva 22 Kohde-NID:n määritys

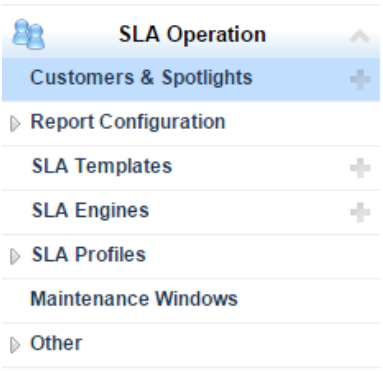
Kun source- ja destination-osioihin on lisätty halutut NID:t, niin policyn konfiguraatio on valmis. Tämän jälkeen sivuston alalaidasta voi painaa ”Save New Policy” nappia, joka tallentaa policyn käyttöä varten.

Tämän jälkeen policy-konfiguraatioiden lähettämisen onnistuminen on hyvä tarkistaa Policies-valikosta, onko luodun policyn konfiguraatio mennyt NID:lle asti. Tämän voi tarkistaa avaamalla policyn tiedot ja sieltä tarkistamalla, onko ”Provisioning status” valmistunut vai ei. Sininen kuvake viittaa, että konfiguraatio on meneillään ja oranssi merkki viittaa ongelmaan. Kun statuksena on vihreä merkki, niin silloin konfiguraatio on onnistunut (kts. kuva 23).



Kuva 23 Onnistunut policyn asetusten määritys

Nyt mittausta varten käytettävä policy on määritelty, niin tarvitaan vielä spotlight, jotta mittauksen tuloksia voidaan päästä tarkastelemaan. Uuden spotlightin määritys onnistuu päävalikon SLA Operations alivalikosta Customers & Spotlights -otsikon viereisestä plus merkistä, joka näkyy kuvassa 24 valittuna. Samalle sivustolle pääsee myös painamalla kyseistä otsikkoa ja käyttämällä uudelta sivustolta ”Add a new Spotlight” -linkkiä.



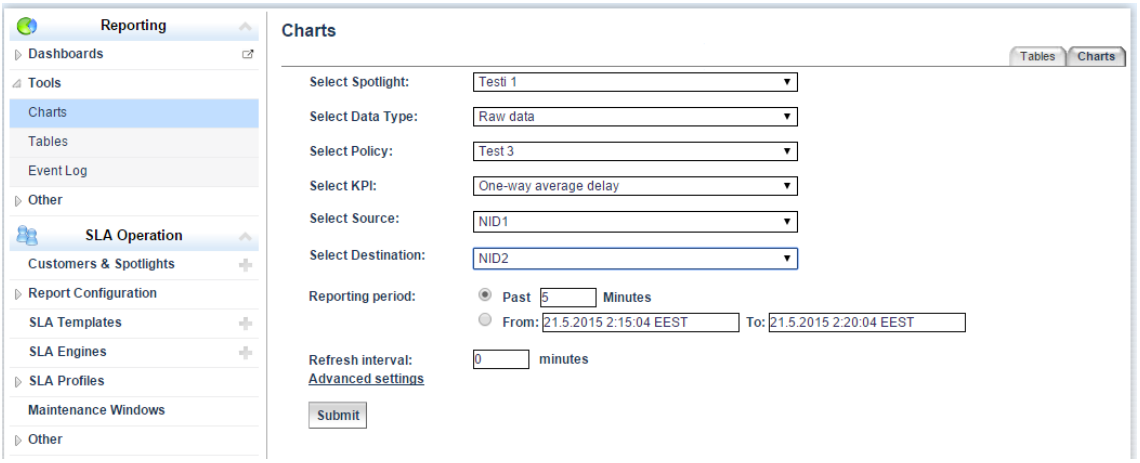
Kuva 24 Customer & Spotlights -valikko

Seuraavaksi spotlightille tulee antaa nimi ja tarkemmin määritellä sen asetuksia. Tässä vaiheessa tulee määrittää, mitä NID:jä ja mitä policyjä halutaan lisätä spotlightiin

”nodes”- ja ”policies”-osioissa (kts kuva 25). Osoiden määrittäminen tapahtuu samalla prosessilla kuin policyssä määriteltiin käytettävät NID:t. Nodes-kohdassa käytettävät NID:t siirretään oikeaan valikkoon ja policies-osiosta valitaan aikaisemmin luotu policy. Näiden asetusten määrittämisen jälkeen tallenna Spotlight ”Save New Spotlight” -painikkeesta.

Kuva 25 Uuden Spotlightin luonti

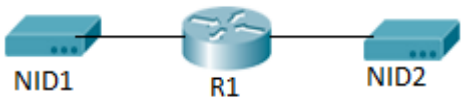
Nyt kun Spotlight on luotu, niin yksittäisen KPI:n mittauksen tarkastelu onnistuu joko taulukkona tai kuvaajana. Molemmat näistä toiminnoista löytyy Reportingin alavalikosta Tools. Kuvassa 26 löytyy esimerkki, miten saadaan yksisuuntaisen keskivertoviiveen kuvaaja viiden minuutin sisällä tehdyistä mittauksista. Jos tietystä aikavälistä halutaan kuvaaja tai taulukko, niin ”past” kentän alapuolella on valinta, jolla kuvaajan tai taulukon voi saada miltä tahansa aikaväliltä. Aikaväliin voi määritellä aloitus- ja lopetusajankohdat sekuntien tarkkuudella.



Kuva 26 Yhdensuuntaisen viiveen kuvaajan asetukset

5.3 IP-tason SLA-mittaus

IP-tason mittaukset toteutettiin yhden reitittimen ylitse omassa verkossaan. Kuten Ethernet mittauksissa niin NID:t oli yhdistetty koulun verkkoon Managament-porttien kautta ja laitteet on kytketty reitittimeen Network-portin kautta. Verkko on havainnollistettu kuvassa 27.



Kuva 27 IP-mittauksia varten käytetty verkko

IP-tason mittauksia varten NID:hin pitää konfiguroida lisää, jotta laitteet voivat muodostaa yhteyden toisiinsa reitittimen ylitse. Tämä on tarpeen, koska testiverkossa ei ole DHCP:tä, jolla laitteille tulisivat IP-osoitteet automaattisesti. Tähän testiverkkoon ei ole myöskään konfiguroitu automaattisesti toimivaa reititystä verkosta toiseen, koska halusin pitää verkon määritykset äärimmäisen yksinkertaisina.

Verkko on konfiguroitu niin, että NID1 on verkossa 192.168.1.0/24 ja NID2 on verkossa 192.168.2.0/24 ja NID:ille tarvitsee asettaa IP-osoitteet kommunikointia varten. Tämä onnistuu konsoliyhteyden avulla laitteen interface-asetuksia muuttamalla. Kuvassa 28 on molempien laitteiden Network-portin konfiguroinnit testiverkkoa varten.

```
NID1
interface edit Network address 196.168.1.2 netmask 255.255.255.0
NID2
interface edit Network address 196.168.2.2 netmask 255.255.255.0
```

Kuva 28 NID:en IP-osoitteiden määritys

Porttien IP-osoitteiden asettamisen jälkeen on hyvä tarkistaa ”interface show” -komennolla, että Network portin asetukset ovat oikein. Interface-taulukon tulisi näyttää NID1:llä kuten kuvassa 29.

```
INSSITESTI-KOLME: interface show

Interface name    State    DHCP     IP address      Netmask         Gateway
    Info
----------------- -------- -------- --------------- --------------- ------------
--- --------------
Management        Enabled  Enabled  10.95.129.21    255.255.255.192 10.95.129.1
    ---
Network           Enabled  Disabled 192.168.1.2     255.255.255.0   ---
    ---
Auto              Enabled  Enabled  ---             ---             ---
    Auto interface
```

Kuva 29 Oikein määritelty Network-portti

Tämän jälkeen molemmille laitteille tulee määritellä kiinteät reitit, jotta laitteet tietävät minne lähettää pakettejaan. Määritys tulee tehdä molemmille laitteille siten, että lähde on laitteen Network portin IP-osoite ja kohde on toisen NID:n verkko. Kuvassa 30 oleva komento reitin määrittämistä varten on kirjoitettava samalle riville.

```
route add NID1 type net destination 192.168.1.2 netmask 255.255.255.0 gateway
192.168.2.2 interface Network
```

Kuva 30 Reitin lisäys NID:lle

Kun konfiguraatiot ovat kunnossa, niin ”route show active” komennon kautta voi tarkistaa, onko reititystiedot oikein. NID1:lle on asetettu reitti NID2:lle 192.168.2.0 verkkoon (kts kuva 31). Destination tulisi olla kohde NID:n verkko ja gatewayn tulisi olla tarkasteltavan laitteen Network portin IP-osoite.

```
INSSITESTI-KOLME: route show active

Flags: U - Route is up              H - Destination is a host
       G - Use a gateway            D - Dynamically installed

Destination     Gateway         Netmask         Flags Interface
--------------- --------------- --------------- ----- -----------------
10.95.129.0     ---             255.255.255.192 U     Management
192.168.2.0     192.168.1.2     255.255.255.0   UG    Network
192.168.1.0     ---             255.255.255.0   U     Network
default         10.95.129.1     0.0.0.0         UG    Management
```

Kuva 31 Oikein konfiguroitu reitti NID:lle

Kun route-tieto näyttää olevan oikein, niin lopuksi kannattaa tarkistaa, että laitteet vastaavat verkosta. Tämä voidaan toteuttaa ping-komennolla. Komento on täysin sama kuin tietokonetta käytettäessä. Esimerkkiverkossa komento olisi NID1-laitteelta NID2-laitteelle ”ping 192.168.2.2”. Komento jatkaa viestien lähettämistä määriteltyyn kohteeseen niin pitkään, kunnes konsolissa painetaan ctrl+c-näppäinyhdistelmää, joka katkaisee viestien lähetyksen. Tämän jälkeen ruudulle tulee yhteenveto kuinka nopeasti paketit kulkivat ja kuinka monta pakettia pääsi perille asti. Tästä tiedosta pystyy näkemään, ovatko paketit päässeet perille vai eivät. Onnistuneen testauksen jälkeen NID:t ovat valmiina mittausten suorittamiseen.

IP-tason mittausten suorittamiseksi Echovaultin asetusten määritys tehdään samalla tavalla kuin Ethernet-tason mittauksissa. IP-mittauksen ainoana erona on, että policy tyypeksi tulee valita IP:llä toimiva policy ”Add a New Policy” valikossa. Toimiva policy IP-mittauksia varten on SLA-Meter UDP[NID].

6 Yhteenveto

Insinöörityön tarkoituksena oli tutkia, miten Echovault-sovellusta käyttäen voidaan mitata verkon SLA:ta ja tämän selvityksen pohjalta tuli luoda ohjeet Echovaultin mittausten luomiseen. Ohjeiden tuli olla sellaiset, että niiden perusteella pystyisi kuka tahansa opiskelija tekemään SLA-mittauksia Ethernet- sekä IP-verkoissa.

Ohje on testattu ensin konfiguroimalla NID:t ohjeen mukaisesti. Tämän jälkeen näitä NID:jä on käytetty luomaan SLA-mittauksia Echovaultissa onnistuneesti Ethernet- ja IP-verkoissa. Tästä voidaan päätellä, että insinöörityö on toteuttanut tavoitteensa.

Haasteita työn suorittamisessa aiheutti hieman puutteellinen alkuperäinen dokumentaatio. Creanordilta saaduissa ohjeissa ei esimerkiksi ollut erillistä mainintaa, mitä kaikkea NID:hin tarvitsee konfiguroida, että laitteita pystyisi käyttämään Echovaultissa. Tämän vuoksi heti työn alkuun oli pitkä selvitys, minkä vuoksi NID:t eivät suostuneet vastaanottamaan SLA-mittausten konfigurointeja vastaan. Lopulta kuitenkin selvisi, että vikana olivat virheelliset kellonajat NID:en päässä.

Lähteet

1 Service Level Agreements on IP Networks. Verkkodokumentti. IBM. <www.research.ibm.com/people/d/dverma/papers/SLAOverview.pdf> Luettu 28.9.2014.

2 Service Level Agreements in Service-Oriented Architecture Environments. Verkkodokumentti. Software Engineering Institute. <http://resources.sei.cmu.edu/asset_files/technicalnote/2008_004_001_14951.pdf> Luettu 19.4.2015.

3 The myth of the nines. Verkkodokumentti. Evan Marcus <http://searchstorage.techtarget.com/tip/The-myth-of-the-nines> Luettu 19.4.2015.

4 High availability. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/High_availability> Luettu 19.4.2015.

5 What is Network Latency and Why Does It Matter. Verkkodokumentti. O3b Networks. <http://www.o3bnetworks.com/wp-content/uploads/2015/02/white-paper_latency-matters.pdf> Luettu 19.4.2015 (Päivitetty 4.5.2015).

6 Bandwith, Latency, and the ”Size of your pipe”. Verkkodokumentti. Billy Hoffman. <http://zoompf.com/blog/2011/12/i-dont-care-how-big-yours-is> Luettu 19.4.2015.

7 Raging bulls: How wall street got addicted to light-speed trading. Verkkodokumentti. Jerry Adler. <http://www.wired.com/2012/08/ff_wallstreet_trading/> Luettu 19.4.2015.

8 Packet loss. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Packet_loss> Luettu 19.4.2015.

9 IP. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/IP>Luettu 19.4.2015.

10 Understanding Jitter in Packet Voice Networks. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html> Luettu 25.4.2015.

11 What is Carrier Grade Ethernet. Verkkodokumentti. Brocade. <http://www.brocade.com/downloads/documents/white_papers/Carrier_Grade_Ethernet_WP_00.pdf> Luettu 25.4.2015.

12 Ethernet OAM Standards. Verkkodokumentti. RAD data communications. <http://www.rad.com/Media/5361_Ethernet_OAM_Guide.pdf> Luettu 25.4.2015

13 Ethernet OAM Overview: Making Ethernet Manageable. Verkkodokumentti. Frank Brockners. <https://www.dfn.de/fileadmin/3Beratung/DFN-Forum1/104-1645-1715.pdf> Luettu 3.5.2015.

14 Ethernet Operations, Administration, and Management. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7-2/theory/operations/TheoryofOperations/eoam_theory.html> Luettu 3.5.2015

15 Y.1731 Performance Monitoring. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/y-1731PM.pdf> Luettu 11.5.2015

16 Accedian Ethernet OAM Overview. PDF. Accedian Networks.