OULUN SEUDUN
AMMATTIKORKEAKOULU

Mika Watilo

# KOKONAISKÄYTETTÄVYYDEN HALLINTA OTTK:N TIETOLIIKENNEVERKOSSA

# KOKONAISKÄYTETTÄVYYDEN HALLINTA OTTK:N TIETOLIIKENNEVERKOSSA

Mika Watilo
Opinnäytetyö
Kevät 2012
Hyvinvointiteknologian koulutusohjelma
Oulun seudun ammattikorkeakoulu

# TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Hyvinvointiteknologian koulutusohjelma

---

Tekijä(t): Mika Watilo
Opinnäytetyön nimi: Kokonaiskäytettävyyden hallinta OTTK:n tietoliikenneverkossa
Työn ohjaaja(t): Veijo Väisänen
Kevät 2012 Sivumäärä: 65

---

Työn taustalla oli Oikeushallinnon tietotekniikkakeskuksen ja BaseN-yrityksen välinen pilottiprojekti. Projektin tarkoituksena oli mitata tietoliikenneverkon laatua ja toimintaa BaseN:n tarjoamalla ratkaisulla. Tilaajana työssä toimii Oikeushallinnon tietotekniikkakeskus OTTK.

Lyhyen aikavälin tavoitteena OTTK:n ja BaseN:n välisellä projektilla pyrittiin löytämään järjestelmien ja kokonaisuuksien ongelmia ja pullonkauloja. Pitkän aikavälin tavoitteena oli parantaa toiminnan laatua lisäämällä palvelun tasojen läpinäkyvyyttä

Opinnäytetyö käsitti kolme päävaihetta: Mittauksen suunnittelu kustannustehokkaasti, raporttien laadinta tietohallinnon käyttöön, sekä loppukäyttäjien kannalta ohjelmien toiminta ja niiden kriittiset pisteet. Tavoitteena oli mittausrungon suunnittelu, mittauksen integrointi ja toimivuuden tarkistus, käyttäjäkyselyt, tulosten keräys ja analysointi, sekä lopputulosten kokoaminen.

Työn tuloksena saatiin käsitys tietoliikenneverkon kapasiteetin ja laitteistovaatimusten riittävyydestä organisaation tarpeisiin. Ongelmat joita kohdattiin, olivat peräisin organisaation sisäisestä sovelluskannasta ja sen päällekkäikksyyksistä.

---

Asiasanat: käytettävyys, SNMP, verkonhallinta

# ALKULAUSE

Tämä työ on tehty Oikeushallinnon tietotekniikkakeskuksen toimeksiannosta. Työ aloitettiin syyskuussa 2010 ja mittaukset saatettiin päätökseen kesäkuussa 2011.

Opinnäytetyön yhteyshenkilönä tilaajan puolelta toimi ATK-suunnittelija Ulla Mansikka-aho Oulun käräjäoikeudesta. Valvovana opettajana työssä toimi Veijo Väisänen Oulun seudun ammattikorkeakoulusta.

Kiitokset Ulla Mansikka-aholle työn aiheesta ja avustuksessa työn eri vaiheissa ja Minttu Uusimaalle kannustamisesta työn aikana.

24.5.2012

Mika Watilo

# SISÄLTÖ


TIIVISTELMÄ 3
ALKULAUSE 4
SISÄLTÖ 5
SANASTO 7
1 JOHDANTO 9
2 OIKEUSHALLINNON TIETOTEKNIIKKAKESKUS 10
3 VERKONHALLINTA 13
3.1 FCAPS-malli 14
3.1.1 Vikatilanteiden hallinta 14
3.1.2 Kokoonpanon hallinta 15
3.1.3 Käytön hallinta 16
3.1.4 Suorituskyvyn hallinta 16
3.1.5 Turvallisuuden hallinta 18
3.2 SNMP 19
3.3 SNMP:n versiot 20
3.3.1 SNMPv1 20
3.3.2 SNMPv2 21
3.3.3 SNMPv3 21
3.4 MIB 21
3.5 ICMP-Ping 25
4 BASEN-PLATFORMI 26
4.1 BaseN:n idea 27
4.2 Arkkitehtuuri 27
4.3 Agenttikoneet 28
4.4 Loggerit 30
4.5 Data analysaattorit 30
4.6 Image Generators 31
4.7 Web-serverit 31
4.8 Web-portaalit 32

4.9 Järjestelmän integrointi 33
5 MITTAUKSEN LÄHTÖKOHTA 35
5.1 Perustiedot 35
5.2 Luokittelu 35
5.3 Lisäämismenettely 36
5.4 Raportointi 37
6 MITTAUSRUNGON SUUNNITTELU 38
6.1 Mittausrungon rakenne 39
6.2 Mittauspisteet 40
7 MITTAUSPISTEET 42
7.1 Mitattavat palvelimet 42
7.2 Mitattavat työasemat virastoittain 44
7.3 Mitattavat työsovellukset 45
7.4 Mitattavat virastotyypit 47
7.5 Loppukäyttäjäkysely 47
8 SAADUT TULOKSET 49
8.1 Käyttäjäkyselyt 49
8.2 Käyttäjäkyselyn arviointi 59
9 YHTEENVETO 61
LÄHTEET 63

## SANASTO

ASN.1 – Abstract Syntax Notation One

BER - Bit Error Rate/Ratio, virhearvot (tässä työssä)

FCAPS – Kehys verkonhallintaan. Akronyymi hallintaryhmien sanoille, fault, configuration, accounting, performance, security

Ho – Hovioikeus

HTTP – Hypertext Transfer Protocol, protokolla jota selaimet ja www-palvelimet käyttävät tiedonsiirtoon

ICMP – Internet Control Message Protocol. TCP/IP kontrollointiprotokolla, jolla lähetään viesetejä koneesta toiseen

IETF – Internet Engineering Task Force. Organisaatio joka vastaa Internet-protokollien standardoinnista

IP – Internet Protocol

Ko – Käräjäoikeus

KkO – Korkein oikeus

MIB – Management Information Base. Laitteen tietojen kuvaus järjestelmä

RMON – Remote Network Monitoring. IETF:n kehittämä hallintatietojen tarjoaja

SMI – Structure of Management Information. Hallinnointi-informaation rakenne.

SNMP – Simple Network Management Protocol. TCP/IP-verkkojen hallinnan tietoliikenneprotokolla

TCP – Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille, jotka ovat yhteydessä Internetiin

UDP – User Datagram Protocol. Niin sanottu yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tietojen siirron

Uo – Ulosotto

# 1 JOHDANTO

Työn taustalla oli Oikeushallinnon tietotekniikkakeskuksen (OTTK) ja BaseN-yrityksen välinen pilottiprojekti. OTTK:n päätehtävänä projektissa oli selvittää pääkohdat tietoliikenneverkosta, jotka sisällytettiin osaksi projektia sekä selvittää olennaisimmat fyysiset laitteet, jotka otetaan mukaan projektiin.

Opinnäytetyön aiheena oli OTTK:n ja BaseN:n välisen projektin pohjalta tarkastella OTTK:n tietoliikenneverkon käytettävyyttä, sen toimintavarmuutta ja käyttöastetta saatujen mittaustulosten ja käyttäjäkyselyiden avulla. Keskeisin kohde opinnäytetyön kannalta oli suunnitella yhdessä tilaajan kanssa mittauspisteet, toisin sanoen valita fyysiset laitteet, joita tarkkaillaan. Valintakriteerinä oli valita laitteet, joista saadaan maksimaalinen hyötysuhde, niin taloudellisesti, kuin tietoliikenneverkon kattavuuden kannalta. Lisäksi opinnäytetyössä suunniteltiin käyttäjäkyselylomakkeet ja suoritettiin käyttäjäkyselyt kahtena eri kertana. Kyselyissä keskityttiin loppukäyttäjän kokemaan tietoliikenneverkon, sekä työsovellusten ja laitteiden käytettävyyteen. Viimeisenä kerättiin BaseN-portaaleista saadut mittaustulokset ja verrattiin niitä käyttäjäkyselyn tuloksiin.

Työ rajattiin pääasiassa mittausrungon suunnitteluun, mittauspisteiden valintaan, sekä vastaavuuksien etsintään BaseN-laitteiston keräämien tulosten ja käyttäjäkyselyiden välillä.

# 2 OIKEUSHALLINNON TIETOTEKNIIKKAKESKUS

Oikeushallinnon tietotekniikkakeskus tuottaa ministeriölle ja hallinnonalan muille virastoille ja muille valtion virastoille tietotekniikan kehittämis-, asiantuntija-, tuotanto-, hankinta- ja tukipalveluja. Oikeushallinnon tietotekniikkakeskuksen päätehtävänä on tietojärjestelmien ylläpito ja kehittäminen oikeusministeriön ja sen hallinnonalan virastojen ja laitosten toimintaa ja johtamista varten, sekä oikeushallinnon tieto- ja viestintäteknisen infrastruktuurin ylläpito. Oikeushallinnon tietotekniikkakeskus osaltaan koordinoi yhdessä ministeriön tietohallintoyksikön kanssa oikeushallinnon tietohallinto- ja tietopalveluyhteistyötä. Oikeushallinnon tietotekniikkakeskus toimii koko oikeusministeriön ja sen hallinnonalan virastojen ja laitosten tietohallintopalvelujen organisoijana, toimittajana ja asiantuntijana. Se valvoo asiakkaidensa valtuuttamana ulkoisten palveluntuottajien toimittamien palvelujen laatutasoa ja käytettävyyttä. Keskeinen valvontatehtävä on myös palvelujen, järjestelmien ja verkkojen käytön toimintakriittisyyden mukaisesta tietoturvallisuudesta ja varautumisesta huolehtiminen. (1, s. 9).

Vuosittain mitattavan asiakastyytyväisyyden keskiarvo vuonna 2009 oli 3,4. Tavoitteeksi asetettiin keskiarvon nostaminen 3,8:aan vuonna 2009 (1, s. 4). Tavoitetta ei saavutettu, kuten taulukosta 1 voidaan todeta. Kehitys on ollut päinvastainen, sillä asiakastyytyväisyys on ollut laskusuuntainen.

*TAULUKKO 1. Asiakastyytyväisyyskyselyjen keskiarvot vuosina 2008 ja 2009*

| Asiakastyytyväisyys asteikolla 1 - 5 | 2008 | 2009 |
|---|---|---|
| Keskiarvo | 3,7 | 3,4 |

Tavoite vuodelle 2009 oli, että kohta ”tietotekniset häiriöt ovat haitanneet työskentelyä jatkuvasti” olisi 0,0% (2, s. 7).Tavoitetta ei saavutettu millään mittauksen piiriin kuuluvalla virastolla, kuten taulukosta 2 voidaan todeta.

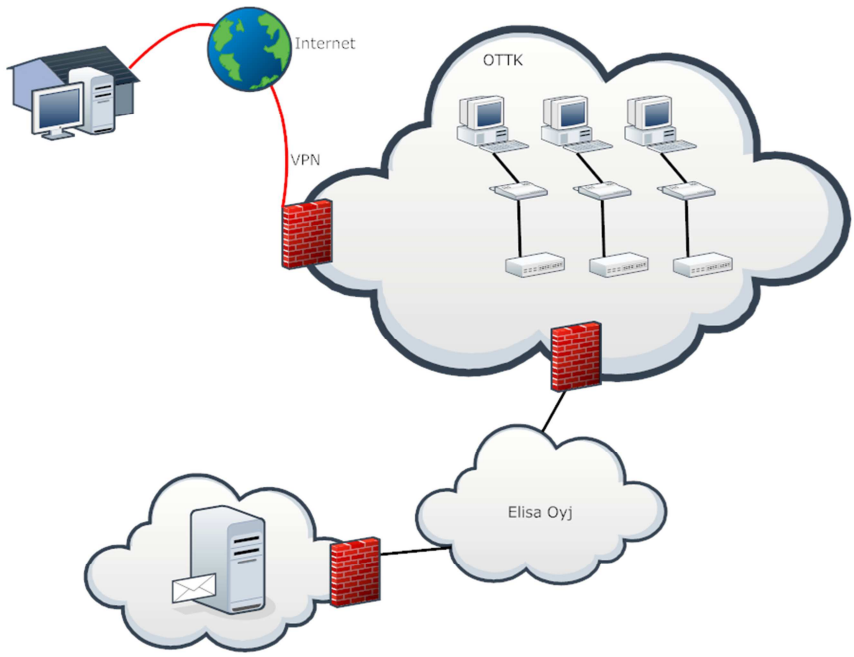
*TAULUKKO 2. Tietotekniset häiriötilanteet ovat haitanneet työtehtävien hoitamista mittauksen piiriin kuuluneissa virastoissa vuonna 2009 (2, s. 7).*

| | Käräjäoikeudet 2009 | Ulosotto 2009 | KKO ja HO 2009 | KHO ja HaO 2009 | Syyttäjä 2009 |
|---|---|---|---|---|---|
| Ei koskaan | 0,0 % | 0,4 % | 1,2 % | 0,0 % | 0,0 % |
| Harvoin | 19,2 % | 35,0 % | 19,3 % | 30,3 % | 20,4 % |
| Sillon tällöin | 56,4 % | 54,0 % | 50,6 % | 34,9 % | 50,0 % |
| Usein | 18,2 % | 8,4 % | 24,1 % | 25,7 % | 24,1 % |
| Jatkuvasti | 6,2 % | 2,1 % | 4,8 % | 9,2 % | 5,6 % |

Tavoitteeksi asetettu satunnaisotantaan pohjautuva tekninen menetelmä käytettävyyden mittaamiseksi kilpailutettiin ja kehitettiin tavoitteiden mukaisesti. Järjestelmä otettiin osittain käyttöön vuonna 2009. Käytettävyysmittauksen kehittämistä ja raportoinnin kehittämistä jatkettiin vuonna 2010.

Oikeushallinnon tietotekniikkakeskuksen tulostavoitteisiin vuodelle 2011 on merkitty seuraavasti: ”Otetaan käyttöön palveluiden kokonaiskäytettävyyden mittaus, jonka avulla tilaajille, asiakkaille ja tietohallinnon johdolle, sekä myös tekniselle henkilöstölle raportoidaan palveluiden laadusta ja määrästä neljännesvuosittain. Kehitetään vika- ja poikkeamatilanteiden hallintaa.”(2, s. 3).

OTTK:n tietoliikenneverkon palveluntarjoajana toimii Elisa Oyj. Tietoliikenneverkon toimivuudesta on pääasiallisessa vastuussa palveluntarjoaja. Tietoliikenneverkon piiriin kuuluvat kaikki Oikeusministeriön ja Oikeushallinnon alaisuudessa toimivat virastot ja toimipaikat sekä mahdolliset kotityöasemat, jotka ovat käytettävissä VPN-yhteyden kautta. Lisäksi tietoliikenneverkkoon on yhdistetty eri palveluntarjoajien palvelinkoneita. Tietoliikenneverkon perusrakenne on esitetty kuvassa 1.




*KUVA 1. Periaatekuva OTTK:n tietoliikenneverkon rakenteesta ja sen kytköksistä*

OTTK:n verkko käsittää reilut 10 000 kappaletta työasemia ja kannettavia työkoneita. Lisäksi verkkoon kuuluvat virastoiden omat verkkotulostimet, VOIP-puhelimet ja joitain viraston sisäisiä palvelimia.

# 3 VERKONHALLINTA

Verkonhallinnan kannalta on olennaista monitoroida avainpalveluita ja infrastruktuureja. Verkonhallinnan kannalta on olemassa kolme keskeisintä asiaa joihin kannattaa keskittyä

- Suorituskyky: ovatko resurssit riittävät.
- Käyntiaika: kauanko järjestelmä on ollut yhtäjaksoisesti käytettävissä
- Saatavuus: onko resurssit käytettävissä vai kaatuneena (3, s. 8).

Verkonhallinnan avulla on mahdollista seurata satoja yksittäisiä resursseja verkon välityksellä, kuten palvelimien virtalähteitä, kiintolevyjä, CPU-varauksia, verkkokorttien kuormitusta jne. verkonhallintasovelluksissa käytetäänkin liipaisin-hälytyskonseptia. (3, s. 8).

Liipaisin-hälytyskonsepti toimii seuraavasti: jollekin muuttujalle, esimerkiksi kiintolevyn täyttöasteelle, asetetaan liipaisinarvoksi 80 %, jolloin tämän arvon ylittyessä verkonhallintasovellus antaa hälytyksen kyseiseltä resurssilta. Verkon monitorointi toimii tällä perusperiaatteella.

Verkonhallintaa tarvitaan nykypäivänä, koska tietoliikenneverkot ovat kasvaneet todella suuriksi ja työntekijät ovat monesti täysin riippuvaisia tietoliikenteen ja siihen yhteyksissä olevien laitteiden toiminnasta. Verkonhallintaan liittyvät olennaisesti erilaiset automaattiset verkonhallintatyökalut, sillä manuaalisesti toteutettu verkonhallinta vaatii resursseja kohtuuttomasti.(3, s. 6).

Tässä luvussa keskitytään ISO:n FCAPS-malliin sekä sen osa-alueisiin. FCAPS-malli toimii ohjeistuksena sille, mitä osa-alueita tehokkaan verkonhallinnan tulisi sisältää.

### 3.1 FCAPS-malli

FCAPS-malli on osa ITU:n Telecommunications Management Network (TMN) standardia (4). FCAPS-malli tarjoaa kehysrakenteen dataverkon ylläpitoon ja hallinnointiin.

Mallin viisi pääkohtaa ovat seuraavat:

- Fault Managment (Vikatilanteiden hallinta).
- Configuration Managment (Asetuksien hallinta ja provisiointi).
- Accounting Managment (Käytön hallinta).
- Performance Managment (Suorituskyvyn seuranta ja optimointi).
- Security Managment (Turvallisuuden hallinta ja pääsynvalvonta).

Tässä työssä keskityttiin erityisesti vikatilanteiden hallintaan, tiedon keruuseen verkosta sekä suorituskyvyn seurantaan ja optimointiin.(5).

#### 3.1.1 Vikatilanteiden hallinta

Vianhallinnan (Fault management) tehtävä on yksinkertaisimmillaan havaita tai löytää vikoja verkosta ja antaa siitä tarvittavaa tietoa. Päätehtävänä on siis vastata vian hallinnasta ja mahdollisesta korjauksesta.(5; 10 s. 11).

Verkon toiminnan kannalta on olennaista, että jokainen itsenäinen verkkoon kytketty laite ja järjestelmä kokonaisuutena on toimiva. Vikojenhallintatekniikat ovat oiva työkalu verkon ylläpitäjälle. Niiden avulla on mahdollista paikantaa ja ratkaista ongelmat nopeammin kuin ilman näitä työkaluja. Vian ilmetessä suoritetaan seuraavat asiat:

- Ongelma on paikallistettava.
- Ongelma on eristettävä.
- Ongelma korjataan, jos se vain on mahdollista. (3, s. 8-9).

Perinteisessä ongelmatapauksessa käyttäjä pyrkii käyttämään sovellusta, jonka palvelin on toisella puolen Suomea. Kyseisessä tapauksessa tietoliikenne kulkee monen laitteen kautta päätepisteeseen. Ongelmana ilmenee seuraavaa: käyttäjä ei pääse sisälle sovellukseen omilla tunnuksillaan. Seuraavaksi ylläpitäjä alkaa paikallistaa ongelmaa. Selvitetään, onko vika käyttäjälähtöinen, esimerkiksi väärin kirjoitettu tunnus tai onko käyttäjällä oikeudet käyttää kyseistä sovellusta. Vian syy ollessa edelleen selvittämättä aletaan ongelmia etsiä laitteista. Pääsääntönä on että laitteita selvitetään käyttäjästä poispäin. Ongelman löytyessä laitteesta se korjataan, jos vain mahdollista.

Vianhallinnan hyödyt ovat varsin konkreettiset. Parhaassa tapauksessa verkonhallintasovellus antaa tiedon viasta, ennen kuin käyttäjät ovat sitä huomanneet, ja näin selvitään ilman minkäänlaista haittaa ongelmasta, jos se vain onnistutaan ratkaisemaan nopeasti. Tämä jättää aikaa verkon kehittämiselle sen sijaan, että ylläpitäjien aika menisi etsiessä verkon ongelmia ja niitä korjatessa.

### 3.1.2 Kokoonpanon hallinta

Kokoonpanon hallinnan (Configuration management) keskeisempänä tehtävänä on kerätä ja ylläpitää verkon laitteiden konfiguraatio- ja ohjelmistoversiodataa tietokantaan tallennettuna. Kokoonpanon hallinnalla voidaan pitää yllä myös laitteiden inventaariotietoja, joista voi olla hyötyä esimerkiksi haluttaessa tietää laitteiston rakenne versioineen. Kokoonpanon hallinnan tehtäviä on myös käynnistää ja pysäyttää verkon laitteita. On toivottavaa että tehtävä voidaan suorittaa automaattisesti esimerkiksi tiettynä viikonpäivänä. Ylläpitäjän silmistä katsottuna kokoonpanon hallinnan on tarjottava laitteiden tunnistetiedot sekä kuvata laitteiden väliset yhteydet käyttäjien tarpeita vastaaviksi.(5).

Yksinkertaisen verkonhallinnan konfiguraatiotyökalun tulisi tarjota vähintään seuraavat tiedot kokoonpanosta: verkko-osoitteet, laitteiden fyysiset sijainnit, sarjanumerot sekä muut yleiset laitetiedot. Työkalun tulisi myös kerätä tietoja

laitteista automaattisesti (autodiscovery-ominaisuus), sillä tällöin voitaisiin olla varmoja tietokannan ajantasaisuudesta.

Kokoonpanon hallinnan ensisijainen etu on mahdollisuus muuttaa verkon loogista rakennetta. Kuten aiemmin mainittiin etuna on myös laitekannan tunteminen, joka helpottaa esimerkiksi eri ohjelmistoversioiden yhteensopimattomuudesta johtuvien ongelmien ratkaisua.

### 3.1.3 Käytön hallinta

Käytön hallinnassa (Accounting management) päämääränä on hallita verkkojen ja järjestelmien resursointia: kuka käyttää, mitä käyttää ja miten käyttää. Informaatiota saadaan esimerkiksi levyresurssien, verkkopalveluiden tai CPU-kuormituksen käytöstä käyttäjäkohtaisesti.(5).

Jotta vältytään liian suurelta kerätyltä datamäärältä on pystyttävä määrittelemään se, mitä tietoa kerätään, mistä kerätään ja kuinka paljon kerätään. Lisäksi on määriteltävä käyttäjäkohtaiset raja-arvot verkon resurssien kuormittamiseen sekä on määrättävä toimenpiteet, jotka suoritetaan arvon ylittyessä.

Käytön hallinnan myötä saadaan tieto verkon resurssien todellisesta käyttömäärästä sekä verkon ja sen laitteiden todellisesta kuormitusasteesta. Tämän myötä saadaan informaatiota, jota voidaan käyttää hyväksi verkkoon suunnattavien investointien kohdistamisesta tarvittaviin kohteisiin. Verkon laajentamista ajatellessa on tärkeää tietää, mitä yhteyksiä ja palveluita todellisuudessa kuormitetaan ja käytetään eniten. Käytön hallinta on avuksi organisaatioille, joilla on tulosvastuu, sillä käytön hallinta antaa mahdollisuuden jakaa verkosta aiheutuvat kustannukset todellisen käytön mukaan.

### 3.1.4 Suorituskyvyn hallinta

Suorituskyvyn hallinnalla (Performance management) pyritään mittaamaan ja auditoimaan verkon, järjestelmien ja sovellusten suorituskykyä. Suorituskyvyn

hallinnalla saadaan selville tietoverkkojen pullonkauloja, sekä saadaan ennustettavuutta ja keinoja kapasiteettisuunnitteluun.(5).

Yleisesti tietoliikenneverkkoon yhteydessä olevat laitteet käyttävät jaettuja resursseja, esimerkiksi verkkolevyjä. Näiden jaettujen resurssien ja toimintojen kannalta voi olla kriittistä se että verkon suorituskyky on riittävällä tasolla.

Tietoverkon suorituskyvyn hallinta koostuu kahdesta pääkohdasta: valvonta (monitoring) ja hallinta (controlling). Liikenteen tarkkailu suoritetaan valvonnan avulla ja hallinta antaa mahdollisuuden suorituskyvyn tehostamisen tarjoamalla välineet verkon asetusten säätämiseksi. (3, s. 13).

Mietittäessä verkon suorituskykyä keskeiset esille tulevat kysymykset ovat yleensä seuraavanlaisia:

- Mikä on verkon käyttöaste?
- Onko verkko ruuhkautunut joiltakin osin?
- Onko jonkin linkin välityskyky liian alhaisella tasolla?
- Onko jossain pullonkauloja?
- Ovatko vasteajat tarvittavalla tasolla?

Jotta edellä mainittuihin kysymyksiin saataisiin vastaukset, on verkon ylläpitäjän tarkkailtava jotain tiettyä blokkia tietoliikenneverkosta voidakseen arvioida suorituskyvyn tasoa. Blokki sisältää tietyn tietoliikenneverkon osan laitteineen. (3, s. 13).

Jotta olisi mahdollista suorittaa suorituskyvyn hallintaa, on tietoliikenneverkosta ja sen sovelluksista kerättävä tietoa ennen toiminnan aloittamista. On siis tunnettava tarvittavalla tasolla verkon suorituskyky. Tämä voidaan suorittaa siten että selvitetään verkon keskimääräiset ja huonoimmat vasteajat ja verkon palvelujen luotettavuus. Nämä tiedot auttavat verkon suunnittelussa, hallinnassa ja ylläpitämisessä. Suorituskykytilastojen avulla voidaan selvittää esimerkiksi tietoliikenneverkon pullonkauloja. Tämän avulla voidaan suorittaa

toimenpiteitä, jolloin pullonkauloja ei pääse enää syntymään. Voidaan hajauttaa tietoliikennettä ruuhka-aikoina tai havaittaessa voimakkaasti kasvavaa liikennettä jollain verkon alueella.(3, s. 13).

Suorituskyvyn hallinta antaa tietoa eri laitteiden käyttöasteesta. Käyttöasteen avulla voidaan päättää, onko palvelujen kannalta tarpeen ryhtyä äärirajoilla toimivien resurssien laajentamiseen. Lisäksi suorituskyvyn hallinta antaa arvokasta tietoa historiatietojen ja liikenteenmäärän analysoinnilla suunniteltaessa tulevia laajennuksia.

### 3.1.5 Turvallisuuden hallinta

Turvallisuuden hallinnassa (Security management) tehtävänä on estää luvaton pääsy verkkoihin ja järjestelmiin, sekä havainnoida niiden mahdollinen väärinkäyttö.(5).

Tärkeä osa turvallisuuden hallintaa ovat erilaiset lokeihin kerätyt tiedot. Tästä johtuen suurin osa turvallisuuden hallintaa ovatkin erilaiset lokimerkinnät, niiden tallennus, sekä niiden analysointi. Turvallisuuden hallinnan päätehtävänä on keskittyä siihen kenellä, ja mistä on oikeus päästä käsiksi eri laitteisiin ja niistä saataviin palveluihin.

Turvallisuuden hallinnan on annettava välineet verkon resurssien ja käyttäjien tiedon turvaamiseen. Käyttäjät on pidettävä tietoisina siitä että turvallisuuskäytännöt ovat luotettavia ja toimivia ja turvallisuuden hallinta on itsessään suojattu, eli ainoastaan valtuutetut henkilöt pääsevät käsiksi turvallisuuden hallinnan tarjoamiin työkaluihin. (6, s. 503-504).

Turvallisuuden hallinnan avulla on mahdollista vähentää murtautumisyrityksiä järjestelmiin, koska pääsy tiettyihin laitteisiin, joiden kautta sovellukse toimivat on rajoitettu esimerkiksi toimipaikka/käyttäjä kohtaiseksi. Monesti myös pelkkä tieto turvallisuuden hallinnasta on tehokas keino vähentää murtautumisyrityksiä. Voidaan verrata hyvin kaupan videovalvontalaitteisiin. Esimerkiksi varkauden estämiseksi riitää monesti ilmoitus tiloissa olevasta videovalvonnasta.

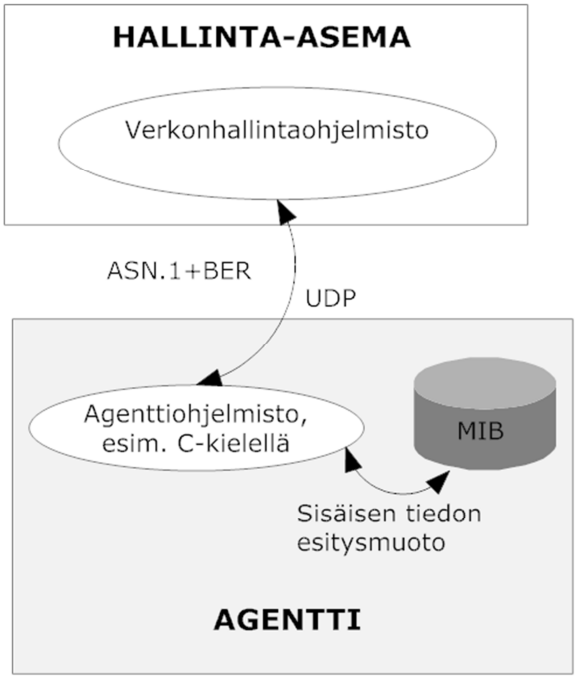
### 3.2 SNMP

Yleisin TCP/IP-verkkojen hallintaan käytetty protokolla on SNMP, sillä on nykyään mahdollista valvoa ja hallita lähes minkälaisia verkkolaitteita tahansa. SNMP (Simple Network Managment Protocol) käsittää joukon erilaisia standardeja, jotka rakentuvat varsinaisen SNMP-protokollan ympärille, näihin protokolliin kuuluu sovellustason protokolla OSI-mallissa, tietokantamalli, sekä joukko hallintaobjekteja eli olioita. Perusidea kaikessa SNMP-protokollaan perustuvassa verkonhallinnassa on se, että verkossa on joukko SNMP:llä hallittavia laitteitta, SNMP-agentteja, joiden tilaa voidaan tutkia ja joita voidaan konfiguroida SNMP-verkonhallinta-aseman avulla. Liikennöinti tapahtuu IP-protokollan päällä UDP-protokollan avulla, jotta SNMP-laitteiden aiheuttama rasitus verkkoa kohtaan olisi mahdollisimman pieni. Huonona puolena UDP-protokollan käytöstä seuraa SNMP-viestien mahdollinen katoaminen, joten SNMP-viestien perille menosta ei ole takeita.(7).

SNMP määritellään joukossa RFC-dokumentteja. Varsinaisen verkonhallintaprotokollan lisäksi oleellisia ovat tiedon rakenteen ja tiedon tunnistamisen standardit.

Nimensä mukaisesti verkonhallinta-asema huolehtii SNMP-verkon hallinnasta. Verkonhallinta-asema suorittaa tarvittavat kyselyt SNMP-agentilta. Kaikki hallintotietokanat on kuvattu samalla kielellä ASN.1:llä, tästä syystä erilaisilla käyttöjärjestelmillä varustetut agentit ja hallintajärjestelmät on helppoa saada ymmärtämään toisiaan. Yleisimmin laitteet saadaan keskustelemaan keskenään BER-koodaussääntöjen avulla. SNMP-verkonhallinassakin käytetään edellä mainittua menetelmää.(5).

BER-koodaus koodaa ASN1. kuvausten muuttujat ja tietorakenteet SNMP-viesteihin siten, että viestin vastaanottaja, jonka tulee ymmärtää BER-koodausta osaa purkaa viestin omaa sisäistä tiedon esittämistapaa vastaavaan muotoon.




*KUVA 2. SNMP-verkon koostumus, pakettien koodaus ja siirto (8)*

### 3.3 SNMP:n versiot

Tällä hetkellä SNMP:stä on käytössä kolme eri versiota: SNMPv1, SNMPv2, sekä SNMPv3.

#### 3.3.1 SNMPv1

SNMP-versio1 (SNMPv1) on alkuperäinen toteutus SNMP protokollasta ja se on yleisin käytössä oleva verkkohallinnan protokolla. SNMPv1 siirtää dataa seuraavien protokollien yli: UDP, IP, CLNS, DDP ja IPX. Ensimmäinen versio on saanut osakseen kritiikkiä sen huonosta turvallisuudesta. Salasanan sijaan liikennöinti SNMP-agentteihin ja MIB-dataan käydään selkokielisillä community-stringeillä (yhteisönimillä). Nykyisissä laitteissa on mahdollista parantaa tietoturvaa communityihin lisättävilla access-listoilla, joilla liikennöintiä voidaan rajoittaa IP-tasolla siten, että määritellään sellaiset IP-osoitteet, jotka saavat olla yhteyksissä kyseisiin laitteisiin. (4).

### 3.3.2 SNMPv2

SNMP-versio 2 parantui versioon 1 nähden muun muassa: suorituskyvyssä, tietoturvassa ja luotettavuudessa. Versiossa 2 on mukana myös GetBulkRequest-operaatio, joka voi siirtää suurempia määriä dataa yhdellä kyselyllä verrattuna version 1 iteratiiviseen GetNextRequest-operaatioon. Uudistettu tietoturva oli kuitenkin monen mielestä liian kompleksinen joten toisesta versiosta ei tullut laajalti suosittua. SNMPv2:sta on olemassa myös muutettu versio nimeltään SNMPv2c, joka perustuu SNMPv1:en community-periaatteseen. SNMPv2c toimii samalla tietoturvakäytännöllä kuin SNMPv1. Virallisesti SNMPv2c toimii Draft-standardina, mutta sitä pidetään tehokkaampana ja monipuolisempana de-facto standardina version 1 rinnalla. (4).

### 3.3.3 SNMPv3

SNMPv3 on tuotettu pelkästään tietoturvallisuutta silmälläpitäen. Siihen ei sisälly minkäänlaisia toiminnallisia uudistuksia verrattuna SNMPv2:een. Tietoturvauudistuksen myötä SNMPv3 mahdollistaa autentikoinnin, yksityisyyden, sekä pääsyn kontrolloinnin. SNMPv3 on luokiteltu IETF:n mukaan nykyiseksi standardiksi vuodesta 2004 lähtien ja se onkin antanut aiemmille versioille statukseksi ”historiallinen”. Käytännössä SNMP toteutukset tukevat useita versioita: yleisimmin SNMPv1, SNMPv2c ja SNMPv3. Toisaalta useimmat toimijat ovat jättäneet SNMPv3 pois käytöstään koska on olemassa toimittajia jotka eivät käännä MIB:ejään kunnolla versioon 3. (4).

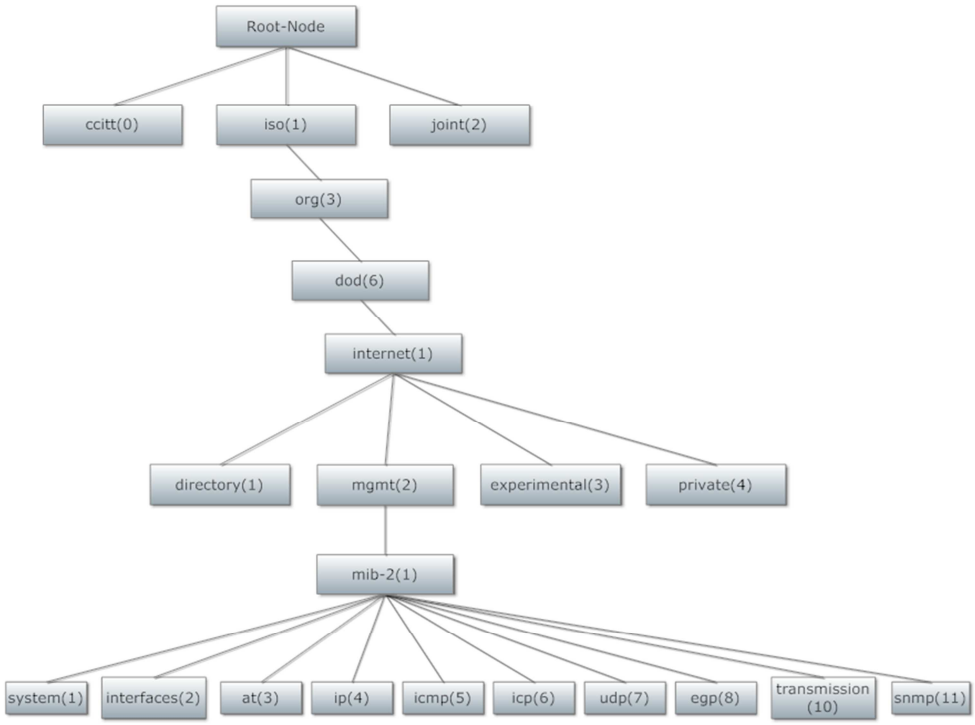
## 3.4 MIB

Verkonhallinta protokollan lisäksi tarvitaan hallintatietokantojen määrittely MIB (Management Information Base), sekä tieto-olioiden määrittely SMI (Structure of Management Information).

Yleisimmin SNMP:llä hallittavat tiedot ovat MIB-1, MIB-II- tai RMON-määrittelyissä löytyviä kokonaisuuksia.

MIB on hierarkkinen datarakenne, joka kuvaa kaikki muuttujat, joista luetaan tietoja. On myös mahdollista että joissain tapauksissa MIB:t asettavat arvoja. MIB:en rakenne on kuvattu SNMP-sukuisessa standardissa RFC 1155 ”Structure and Identification of Management Information for TCP/IP-based Internets”, joka määrittää miten MIB tiedot on järjestyneet ja mitkä tietotyypit ovat sallittuja, sekä miten MIB:in sisäiset resurssit ovat esitetty ja nimetty. MIB sisältää nimen, objektin tunnisteen (numeerinen arvo), data tyypin ja viittauksen objektiin josta luetaan tai kirjoitetaan tietoja. MIB:n ylimmät kerrokset on ennalta määrätyn kaltaisia, kun taas alemmat oksat on määritelty IETF:n ja muiden organisaatioiden toimesta. (9, s. 153).

MIB:n hierarkian juuritasolla on yleistiedot tietoliikenneverkosta, ja mitä alemmille tasoille liikutaan, sitä tarkempia tietoja saadaan tietyistä laitteista ja palveluista. Juuritason alla on kolme alihaaraa, jonka jälkeen puu laajenee internetalaoksaan, joka jakautuu neljään alipuuhun, kuten kuvassa 3 on osoitettu.




*KUVA 3. MIB-hierarkian perusrakenne, sekä MIB-II:n objektiryhmät.(10)*

Puun tärkeimpinä haaroina pidetään mgmt-haaraa, sekä private-haaraa. Mgmt-haara on varattu yleiskäyttöön määriteltävää MIB-dataa varten ja private-haara on varattu laitevalmistajien omia MIB-toteutuksia varten.(10).

MIB-puun jokainen objekti on nimetty ASN.1:n määrittelemällä oid:lla eli Object identifierilla. Oid:t käsitellään järjestelmässä numeerisin arvoin ja niistä on olemassa rinnalle myös nimetty muoto. Esimerkiksi MIB-2:n hallintaobjektiivit alkavat oid:lla .iso.org.dod.internet.mgmt.mib-2, jonka vastaava numeerinen arvo on .1.3.6.1.2.1..(10).

**MIB-II**

MIB-II on tärkeä hallintaobjektiryhmä, koska jokaisen laitteen joka tukee SNMP:tä tulee tukea myöskin MIB-II:ta.

MIB-II:n pää oid:t on määritelty dokumentissa RFC1213-MIB, mib-2 alapuulle seuraavasti (10):

```
mib-2        OBJECT IDENTIFIER ::= { mgmt 1 }
```

```
system       OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces   OBJECT IDENTIFIER ::= { mib-2 2 }
at           OBJECT IDENTIFIER ::= { mib-2 3 }
ip           OBJECT IDENTIFIER ::= { mib-2 4 }
icmp         OBJECT IDENTIFIER ::= { mib-2 5 }
tcp          OBJECT IDENTIFIER ::= { mib-2 6 }
udp          OBJECT IDENTIFIER ::= { mib-2 7 }
egp          OBJECT IDENTIFIER ::= { mib-2 8 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
snmp         OBJECT IDENTIFIER ::= { mib-2 11 }
```

Taulukossa 3 on kuvattu lyhyesti mitä MIB-II:n eri hallintaryhmät sisältävät.

*TAULUKKO 3. Kuvaus MIB-II:n hallintaryhmistä (10)*

| Alipuu | OID | Kuvaus |
|---|---|---|
| *system* | *1.3.6.1.2.1.1* | Sisältää listan objekteista, jotka kuvaavat järjestelmän up timeä , kontakteja sekä järjestelmän nimen |
| *interfaces* | *1.3.6.1.2.1.2* | Kuvaa rajapintojen toimintaa, seuraamalla mitkä niistä ovat toiminnassa; katsomalla lähetettyjen ja vastaanotettujen tavujen määrää, sekä seuramalla rajapintojen virheitä sekä hylkäyksiä |
| *at* | *1.3.6.1.2.1.3* | Osoitteen kääntäjä "address tranaslation" (at) on väheksytty ja on yhteensopiva vain vanhempien versioiden kanssa. Tullaan todennäköisesti poistaamaan MIB-III:sta |
| *ip* | *1.3.6.1.2.1.4* | Seuraa ip-tason toimintaa esimerkiksi ip:n reititystä |
| *icmp* | *1.3.6.1.2.1.5* | Seuraa ICMP:n virheitä, hylkäyksia jne. |
| *tcp* | *1.3.6.1.2.1.6* | Seuraa monen muun asian lisäksi TCP-yhteyksien tilaa (esim. Katkaistu, odottaa, synSent, jne) |
| *udp* | *1.3.6.1.2.1.7* | seuraa UDP:n tilastoja, datagrammeja sisään ja ulos, jne. |
| *egp* | *1.3.6.1.2.1.8* | Seuraa eri EGP-tilastoja sekä pitää taulukkoa EGP-naapureista |
| *transmission* | *1.3.6.1.2.1.10* | Tälle tasolle ei ole tällä hetkellä määritelty objekteja |
| *snmp* | *1.3.6.1.2.1.11* | Mittaa pohjalla toimivan SNMP-implementaation suorituskykyä, kuten lähetettyjen ja vastaanotettujen SNMP-pakettien määrää |

### 3.5 ICMP-Ping

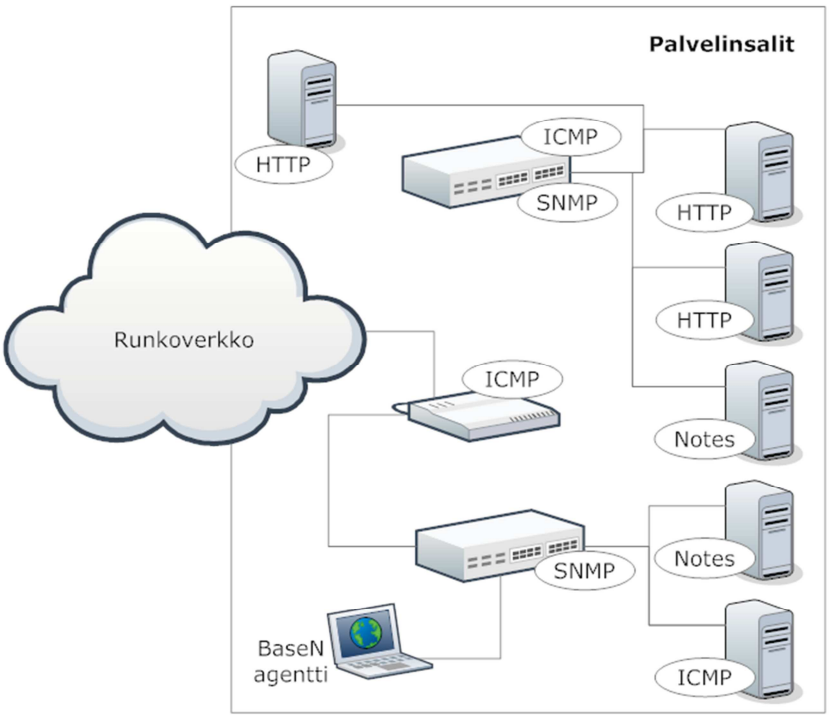
Ping on TCP/IP-protokollan työkalu, joka kokeilee määrätyn laitteen saavutettavuutta. Ping lähettää laitteelle ICMP-echo request -paketin, johon etätietokone vastaa omalla echo reply -paketilla. Tyypillisesti työkalu tulostaa sekä lähetettyjen ja vastaanotettujen pakettien määrän että latenssin. (11).

Mittauksessa ICMP-pingillä saadaan selville mitattavan kohteen käytettävyys. Nähdään kadonneiden pakettien määrä tietyllä aikavälillä, esimerkiksi kuukausitasolla. Pingillä selvitetään myös laitteiden Round Trip Time.

# 4 BASEN-PLATFORMI

OTTK:n projektissa verkonhallinta suoritettiin BaseN-yrityksen tuottamalla verkonhallintasovelluksella. BaseN on Helsingissä pääkonttoriaan pitävä, maailmanlaajuisesti toimiva, verkon ja palveluiden mittaukseen erikoistunut yritys.

Mittaukset on toteutettu BaseN:n agenttikoneella, joka kerää tietoja OTTK:n-tietoliikenneverkosta. Agenttikoneet muodostavat yhteyden verkon eri fyysisiin laitteisiin ja tekevät niihin kyselyjä, joiden avulla saadaan tietoa tietoliikenneverkon toiminnasta ja laitteen kapasiteetista. (12).




*KUVA 4. BaseN agenttikone palvelinsalissa*

Valvonta suoritetaan ICMP-pingein sekä SNMP-kyselyiden avulla. Kyselyjä suoritetaan seuraavasti: esimerkiksi windows-palvelimelta kysytään levytilojen täyttöastetta ja yksittäisen prosessin viemää suoritinaikaa. Järjestelmällä on mahdollista valvoa myös yksittäisiä sovelluksia, kuten HTTP, Lotus Notes jne.

Tällöin on mahdollista tarkastella esimerkiksi kirjautumisen vasteaikaa Notes palveluun. (12).

### 4.1 BaseN:n idea

BaseN:n tarjoama ratkaisu toimii mittauspohjana datalle, sekä se tuottaa mittausdatan järkeväksi kokonaisuudeksi.

Arkkitehtuuri mahdollistaa miljoonien objektiivien seuraamisen hajautetun verkkolaskennan avulla. Tämä toteutetaan agenttikoneilla, jotka voivat purkaa tietoa MIB:stä tai passiivisesti Syslogeista tai SNMP-trapeista. Loggerit pystyvät vastaanottamaan tietoja N määrältä agentteja ja jalostamaan tiedon jotta ei rasitettaisi tietokantoja turhalla informaatiolla. Analyzerit toimivat pareittain ja siirtävät datan valmiiksi näytettävällä ”ready to display” -formaatilla. Kun raportti tuotetaan käyttäjälle Analyzerit kokoavat datan ja siirtävät sen edelleen Image Generaattoreille. Nämä kuvaajat voidaan esittää reaaliaikaisina ja informaatio virta Image generaattoreiden Analyzereiden välillä on interaktiivista. Loppunäkymä tuotetaan authentication-layerin läpi, joka mahdollistaa useiden käyttäjäryhmien pääsyn dataan heidän oman toiminta kenttänsä kannalta. (13).

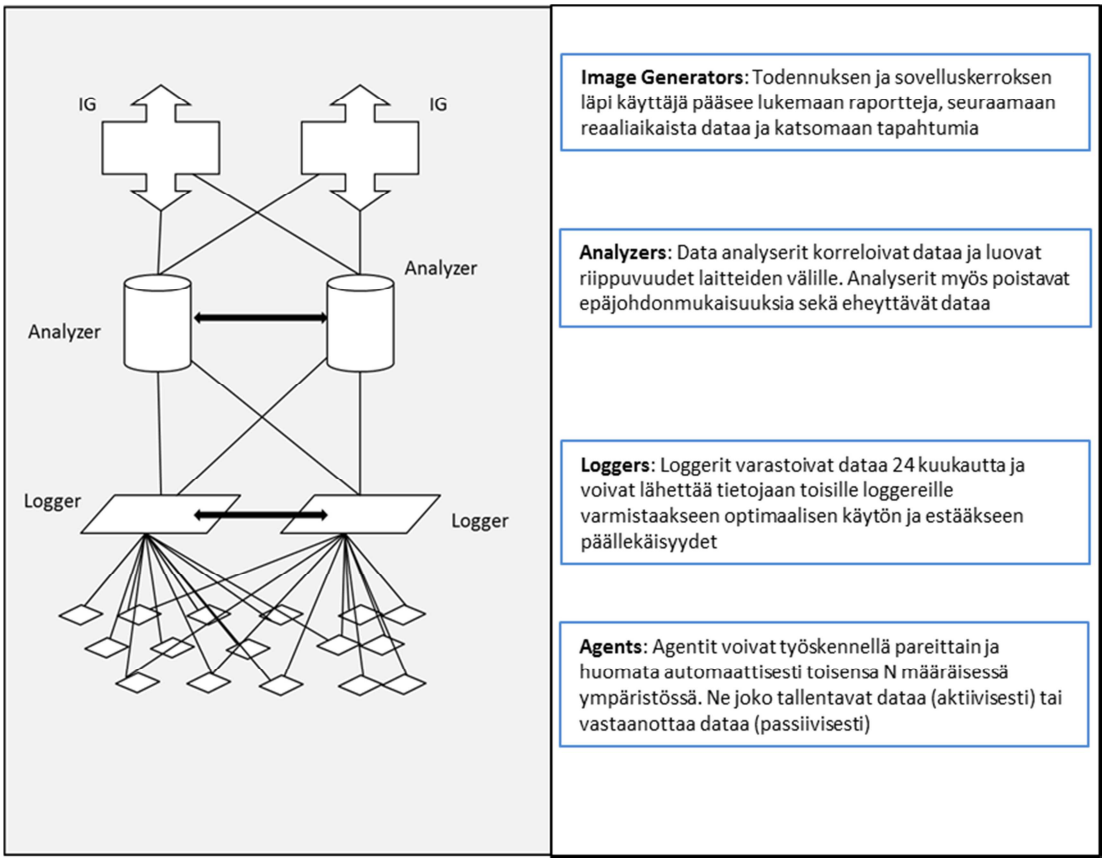
Lopputuloksena on tiivis helposti ymmärrettävä näkymä tuotetusta mittausdatasta. Yleiskuva tietoliikenneverkon tilasta saadaan näin näkyville vilauksella. Dataan on pääsy monilla eri käyttäjillä monien erilaisten alustojen kautta. (13).

### 4.2 Arkkitehtuuri

Perustana on erittäin skaalautuva ja joustava ratkaisu. BaseN-sovellusalusta eroaa muista ratkaisuista sen grid-arkkitehtuurin ansiosta. Sovellusalustan komponentit ovat erittäin neutraaleja toisilleen, sillä ne jokainen ovat huomaamattomia toisilleen, mutta toimivat silti yhteen ja jakavat resurssejaan. Ne ovat myös automaattisesti konfiguroitavissa muiden koneiden kautta jos uusi tai vioittunut laite tulee liittää osaksi verkkoa. (13).

Kaikki funktiot voidaan suorittaa useilta koneilta. Katkos yhdessä paikassa tai yhden komponentin hajoaminen ei näin ollen kaada koko järjestelmää. Järjestelmä on suunniteltu kestämään jopa 50% hajoamistoleranssi säilyttäen toimintakykynsä, vaikkakin nopeus kärsii. (13).

Kuvassa 5 on esitetty BaseN-alustan yleiskuva ja laitteiden tehtävät ja toimintatavat.




*KUVA 5. BaseN-alustan yleiskuva*

### 4.3 Agenttikoneet

Agenttikoneet tuottavat aktiivista ja passiivista mittausta. Ratkaisu käyttää kumpaakin tapaa saadakseen aikaan mahdollisimman suuren kattavuuden. Useampi agenttikone kerää talteen mitatun datan, jotta hävikki tai isolaatio yhdessä agenttikoneessa ei vaikuta lopputulokseen. Agenttikone varastoi tietoja kolmen kuukauden ajalta varmistuakseen siitä että data on jaettu ja varmistettu

useaan kertaan. Seuraavien askeleiden virheiden varalta tieto saadaan lähetettyä uudestaan, jotta historiatietoja ei katoa. (13).

BaseN-hosted implementoinnissa Agenttikone on ainut fyysinen laite, jonka tarvitsee olla asiakkaan laitetiloissa. Hyvinä puolina BaseN-hosted ratkaisussa on: lyhyt implementointi aika, kustannustehokkuus ja järjestelmä on kokonaan hallittu BaseN:n taholta. Miinus puolina ratkaisussa on: hankala integroida muihin järjestelmiin, kuin suunniteltuun ja järjestelmä on tällöin hyvin standardisoitu. (13).

Toisaalta on myös mahdollista että kaikki kuvassa 5 esitetyt laitteet ovat asiakkaan tiloissa tällöin on kyse In-house asennuksesta. In-House asennuksessa replika BaseN:n-platformista implementoidaan asiakaan nopeaan data centeriin osaksi heidän verkkoaan. In-House asennusta suositellaan käytettäviksi erittäin suurissa verkoissa tai silloin kun verkon koon oletetaan kasvavan todella nopeasti. Ratkaisun plussapuolet ovat kokonaisvaltainen hallinta, muokattavuus ja mahdollisuus integroida osaksi muita järjestelmiä. Miinuspuolina ratkaisussa ovat: pitkä implementointi aika ja kalliimpi ylläpito kuin BaseN-hosted ratkaisussa. (13).

Agenttikoneet kommunikoivat muiden järjestelmässä olevien laitteiden kanssa http-protokollassa TCP-portteihin 80 ja 8080. Mitattu data lähetetään BaseN enkryptatyn protokollan kautta. Kaikki kommunikaatio agentin ja järjestelmän välillä on lähtöisin agentilta eikä koskaan järjestelmästä agenttiin. (13).

Agentit lähettävät mittaustulokset järjestelmän tallennin servereille. Tietyin väliajoin agentti noutaa uudet konfigurointi tiedot tältä serveriltä. (13).

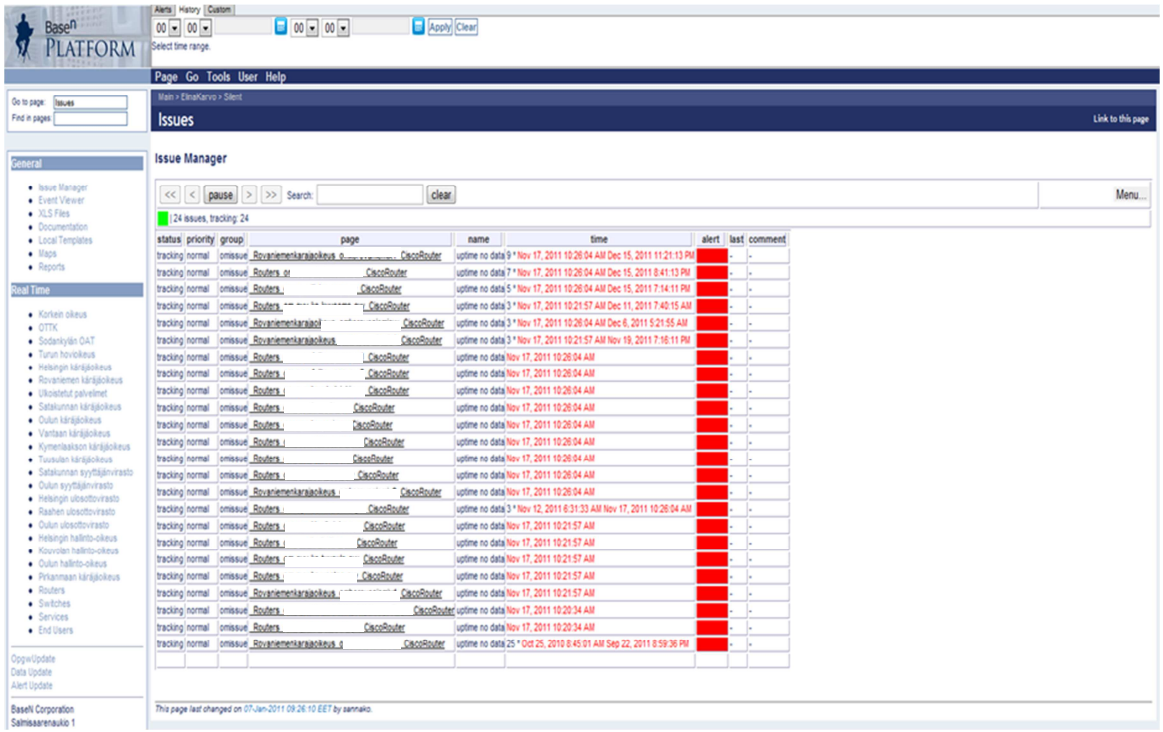
Agenttikoneissa on paikallinen kovalevy sisäistä tallennusta varten. Mittauksen aikana agentit tallentavat tiedot paikalliselle levylle. Jos yhteydessä tallennin serverille on ongelmia, tiedot ovat tallessa agenttikoneen paikallisella levyllä. Yhteyden jälleen toimiessa agenttikone lähettää tiedot paikalliselta levyltä tallennin serverille. (13).

### 4.4 Loggerit

Agentit lähettävät mittausdatan loggereille, jotka ovat yhteydessä IP-verkon kautta agentteihin. Loggerit säilyttävät tietoja yleisesti vuodesta kahteen vuoteen. Loggerit eivät ole tietoisia toisistaan, joten tiedon häviäminen yhdestä loggerista ei vaikuta toiseen. Tällä tavoin voidaan varmistua tiedon eheydestä. (13).

### 4.5 Data analysaattorit

Loggereiden tehtävänä on lähettää data analysaattoreille. Järjestelmässä on erilaisia analysaattoreita, joilla jokaisella on omanlaisensa tehtävä. Jotkin huolehtivat tapahtumista ja käsittelevät niistä saadun tiedon relevanttiin kontekstiin. Toiset taas suorittavat erilaisia tukitehtäviä. Analysaattorit voivat ottaa toistensa rooleja vian varalta. Verkossa on aina useampia analysaattoreita. Analysaattoreilla voidaan toteuttaa reaaliaikaisia hälytyksiä ja visualisointeja näin haluttaessa. Kuvassa 6 on esitetty esimerkki analysaattoreiden luomista hälytyksistä. (13).

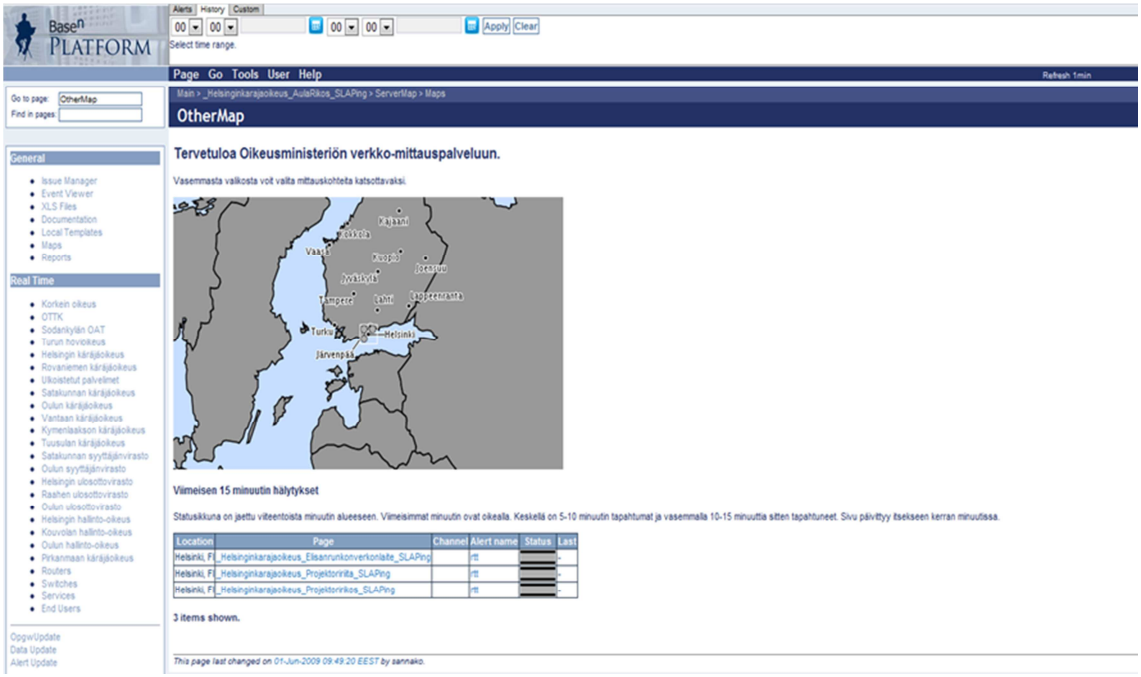



*KUVA 6. Lista annetuista hälytyksistä BaseN-nettiportaalissa*

Jokaiselle hälytykselle voidaan antaa oma liipaisuarvonsa ja tämän ylittyessä hälytys ilmestyy näkyviin nettiportaalin tai haluttaessa siitä voidaan antaa myös sms- tai sähköpostihälytys. Hälytykset voidaan liittää myös osaksi yritysten omia tikettijärjestelmiä.

### 4.6 Image Generators

Image generaattorit (käytetään tästä eteenpäin nimeä IG) tuottaa analysaattoreilta saadun tiedon pohjalta hälytysnäkymiä kuten kuvassa 6 on osoitettu, lisäksi IG:t tuottavat graafisia näkymiä saadusta datasta. IG:t tuottavat myös maantieteelliseen sijaintiin pohjautuvia hälytys ja laitekuvia kuten kuvassa 7 on osoitettu. Kuvasta voidaan valita tietyn paikkakunnan hälytykset ja tarkentaa kohdetta aina tiettyyn yksittäiseen laitteeseen asti. (13).




*KUVA 7. IG:n tuottama karttakuva hälytyksistä Etelä-Suomen alueella.*

### 4.7 Web-serverit

Web-serverit mahdollistavat mittausdataan käsiksi pääsyn IP-verkon kautta. Dataa voidaan tarkastella PC:llä sekä erilaisin mobiililaittein. Toimivuus on

taattu useilla servereillä, joten jos yksi kaatuu on data saatavilla toisen serverin kautta. (13).

### 4.8 Web-portaalit

Käytössä on kaksi eri portaalia: hallinnointiportaali ja ns. käyttäjäportaali. Hallinnointiportaalin kautta on mahdollista tehdä muutoksia mitattaviin kohteisiin, sekä ulos saataviin raportteihin ja graafeihin. Käyttäjäportaalin kautta on mahdollista vain tarkastella mittauksesta saatuja tuloksia.

Mittausjärjestelmän hallinnointi ja mittauspisteiden lisääminen suoritetaan hallinnointiportaalin kautta. Lisäksi portaalissa on mahdollista tarkastella mittaustietoja. Hallinnointiportaalin on käytössä lukuoikeus-tyyppiset tunnukset, portaalin teknisille käyttäjille tai vaihtoehtoisesti olisi mahdollista tehdä tiimikohtaisia geneerisiä tunnuksia. Kirjoitusoikeudellisia tunnuksia myönnetään vain BaseN:n kouluttamille pääkäyttäjille. Hallinnointiportaaliin on jokaisella käyttäjällä henkilökohtaiset tunnukset.

Tietojen ja raporttien katselu tapahtuu loppukäyttäjäportaalin kautta. Mittaustiedot järjestetään portaaliin halutun hierarkian mukaisesti. Kuvassa 8 mittausdata on järjestetty ensin virastotyypin mukaan ja tämän jälkeen laitemallin mukaan.

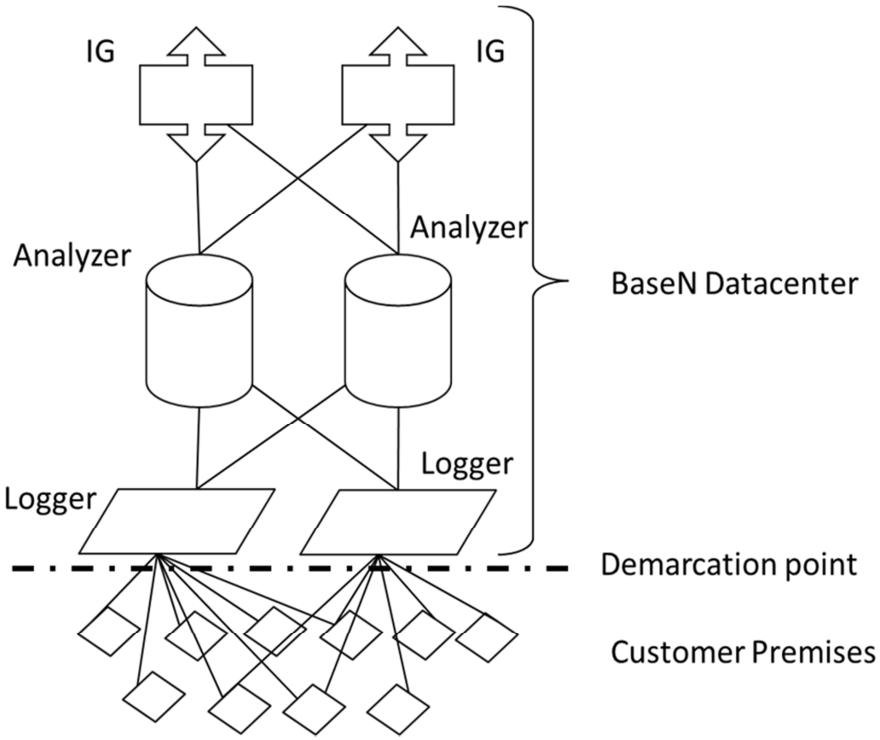

*KUVA 8. Esimerkki mittausdatan jaottelusta.*

Portaaliin on käytössä yksi yleinen käyttäjätunnus. Mittausdataa ei ole rajoitettu millään muotoa, sillä kyseessä on läpinäkyvyyden lisäämiseen tähtäävä järjestelmä, joka kertoo vain käytettävyyden tilasta.

### 4.9 Järjestelmän integrointi

Tässä luvussa käydään läpi ainoastaan työssä käytetty BaseN-hosted-integrointi. Toinen käytössä oleva mahdollisuus on In-House-integrointi, jossa kaikki laitteet ovat asiakkaan tiloissa.

BaseN-hosted ratkaisussa kaikki muut laitteet paitsi agentti-koneet ovat BaseN:n tiloissa, kuvassa 9 on esitetty BaseN-hosted ratkaisu.




*KUVA 9. BaseN-hosted integrointi. Agenttikoneita lukuun ottamatta kaikki muut järjestelmän fyysiset laitteet sijaitsevat BaseN:n omassa datacenterissä.*

# 5 MITTAUKSEN LÄHTÖKOHTA

Verkonhallinnan mittauskohteet ovat yksittäisiä mittauspisteitä (fyysisiä laitteita), joista kerätään ennalta määriteltyä tietoa. Tyypillisin mittauskohde on IP-osoitteella tunnistettu kytkin.

## 5.1 Perustiedot

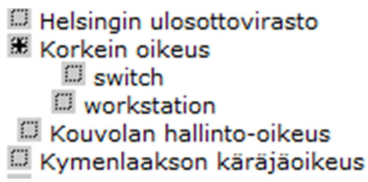
Mittauspisteille tulee määritellä joukko erilaisia perustietoja, jotta mittaus voidaan toteuttaa, luokittelutieto saadaan jalostettua ja raportit ja näkymät voidaan rakentaa järkevästi. Mittauskohteiden perustiedot on esitetty taulukossa 4.

*TAULUKKO 4. Mittauskohteiden vaaditut tiedot (12)*

| | |
|---|---|
| **ID** | Yksilöllinen ID, jolla laite tunnistetaan, (entityID) |
| **Nimi** | Yksilöivä nimi (entity nick) |
| **IP-osoite** | Verkon IP-osoite |
| **Template** | BaseN-mittausmenetelmä, (esim: Cisco Switch, Windows Server) |
| **Tunnukset** | SNMP community ja muut tarvittavat tunnukset |

## 5.2 Luokittelu

Mittaustulosten hierarkkisuus mahdollistaa mittausdatan käyttämisen dynaamisissa näkymissä. Esimerkkinä kaikki tiettyyn tietojärjestelmään tai virastoon liittyvät mittaustulokset. Luokittelu suoritettiin laitteille seuraavasti; Virasto → laitemalli → laitenimi tai työasemanimi + käyttäjän nimi. Kuvassa 10 on näkymä BaseN-nettiportaalista jossa näkyy laitteiden jaotteluperiaate.




*KUVA 10. Malli laitteiden hierarkkisesta jaottelusta.*

### 5.3 Lisäämismenettely

Mittauspisteiden lisääminen tulee tehdä hallitusti ja monivaiheisesti, jotta raportit ja tulokset ovat kokonaisuudessaan yhtäläiset. Mikäli mittauspisteitä lisätään suunnittelematta on vaarana tilanne, jossa jokaisella käyttäjällä on omanlaisensa raportit ja tulokset. Taulukossa 5 on esitetty mittauspisteiden lisääminen vaihe vaiheelta, sekä esitetty myös jokaisen vaiheen vastuuhenkilö(t).

*TAULUKKO 5. Järjestelmään tehtävien muutosten kulku vaihe vaiheelta (12)*

| Vaihe | Tehtävät | Vastuu |
|---|---|---|
| **Tarve** | Tarve mittaukselle ilmenee. -> Tarvitsija lähettää viestin mittauksesta vastuussa olevalle taholle. Viestistä tulee ilmetä tarve mittaukselle ja sen aikataulu | "Tarvitsija" |
| **Arviointi** | Mittaustarve arvioidaan seuraavasti:<br>- Onko tieto jo saatavissa<br>- Yleiset suunnitelmat<br>- Saatavan tiedon arvo<br>- Onko vastaavia mittauksia toteutettu<br>- Kustannustehokkuus | Mittausryhmä |
| **Toteutuksen suunnittelu** | Tekninen ylläpito selvittää parhaan tavan mitata vaadittua tapahtumaa. Samalla valmistellaan miten mittauksien vaatimat protokollat otetaan käyttöön ja kuka tämän tekee. | Vastuussa olevat järjestelmän tekniset osaajat |
| **Hyväksyntä** | Mittausryhmä hyväksyy mittaustavan toteutuksen ja valtuuttaa tilauksen | Mittausryhmä |
| **Tilaus** | Mittausryhmä tilaa muutoksen BaseN:ltä ja valtuuttaa muilta tahoilta tehtävät muutokset | Mittausryhmä |
| **Toteutus** | BaseN toteuttaa muutokset ja raportoi niiden valmistuttua | BaseN |
| **Tiedotus** | Mittausryhmä huolehtii tarvittavasta tiedotuksesta muutoksista johtuen. Samalla toimitetaan ohjeet uuden datan tarkasteluun | Mittausryhmä |
| **Tulosten tarkastelu** | Tarvitsija arvoio saamaansa tietoa ja tarvittaessa pyytää tarkennuksia | Mittausryhmä ja tarvitsija |

Mikäli tarvittava muutos on pieni voidaan se hyväksyä jo ennen toteutuksen suunnittelu vaihetta.

### 5.4 Raportointi

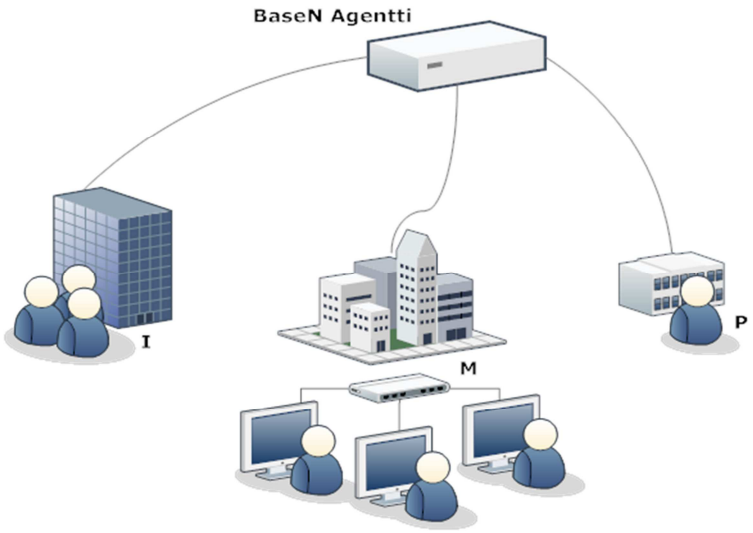
Järjestelmään kerätään mittaustapahtuman avulla erilaista tietoa tietoliikenteen ja laitteiden käyttäytymisestä sekä kuormituksesta. Tietoa hyödynnetään monella eri tasoilla. Taulukossa 6 on esitetty mittaustulosten raportoinnin jaottelu.

*TAULUKKO 6. Mittaustulosten jaottelu (12)*

| | |
|---|---|
| **Välitön hyödyntäminen** | Mittaustuloksia voidaan tarkastella kattavasti portaaleista. Yksittäisistä mittaustuloksista on portaalin työkaluilla mahdollista tehdä erilaisia kuvaajia ja hakea tietoa taulukkolaskennan edelleen muokkausta varten. |
| **Hälytykset** | Järjestelmään voidaan määritellä halutuille mittauskohteiden arvoille hälytysrajoja (liipaisuarvoja), joiden ylityksistä voidaan lähettää tarvittavat viestit joko sähköpostina tai SMS-viestinä. |
| **Raportointi** | Raportteja on mahdollista luoda ja lähettää halutun aikataulun mukaisesti. |

# 6 MITTAUSRUNGON SUUNNITTELU

Opinnäytetyön kannalta mittauspisteiden suunnitelmaa lähdettiin rakentamaan alkutilanteen mukaan, joka on esitetty kuvassa 11. Työssä mittauspisteet suunniteltiin mahdollisimman kattavaksi OTTK:n tietoliikenneverkon suhteen. Työasemat valittiin kolmesta erilaisesta toimipaikasta. **I** = iso toimipaikka, jossa paljon käyttäjiä, sekä oma tietoliikenne. **P** = pieni toimipaikka, jossa vähän käyttäjiä. **M** = monitoimipaikka, virastotalo jossa useita virastoja (käräjäoikeus, syyttäjä, ulosotto) saman tietoliikenteen päässä.




*KUVA 11. Mittausrungon suunnitelman lähtökohta.*

Valitsemalla mitattavaksi erilaisia virastoja saatiin tietoliikenneverkosta mahdollisimman kattava kuva. Näin saatiin selvitettyä käyttäjämäärän vaikutus ohjelmistojen käytettävyyteen. Toisekseen voitiin vertailla tietoliikenneverkon toimintaeroja sellaisten virastojen välillä, joilla on erilaiset tietoliikennerakenteet. Hyödyt jotka suunnitellulla mittausrungolla saavutettiin:

- Verkkojen suunniteltavuus helpompaa tulevaisuudessa, kun tiedetään tarkkaan käyttäjien ja verkon rakenteen vaikutus käytettävyyteen.

- Katettiin suuri määrä käyttäjiä mahdollisimman pienillä kustannuksilla.
- Saatiin mahdollisimman kattava ja monipuolinen kuva tietoliikenteeseen vaikuttavista tekijöistä.
- Mittauksen vaikutusalueeseen saatiin 62 % kiinteistä työasemista.
- Valituilla virastotyypeillä voitiin verrata tietoliikennekaistan riittävyyttä tai riittämättömyyttä.
- Saatiin selville ylimitoitetut verkkopalvelut, jos sellaisia oli olemassa.

### 6.1 Mittausrungon rakenne

Taulukossa 7 on esitetty mitattavaksi valitut organisaatiot ja niiden suhteellinen osuus koko oikeushallinnon työasemamäärästä

*TAULUKKO 7. Mitattavat organisaatiot ja niiden suhteellinen osuus.*

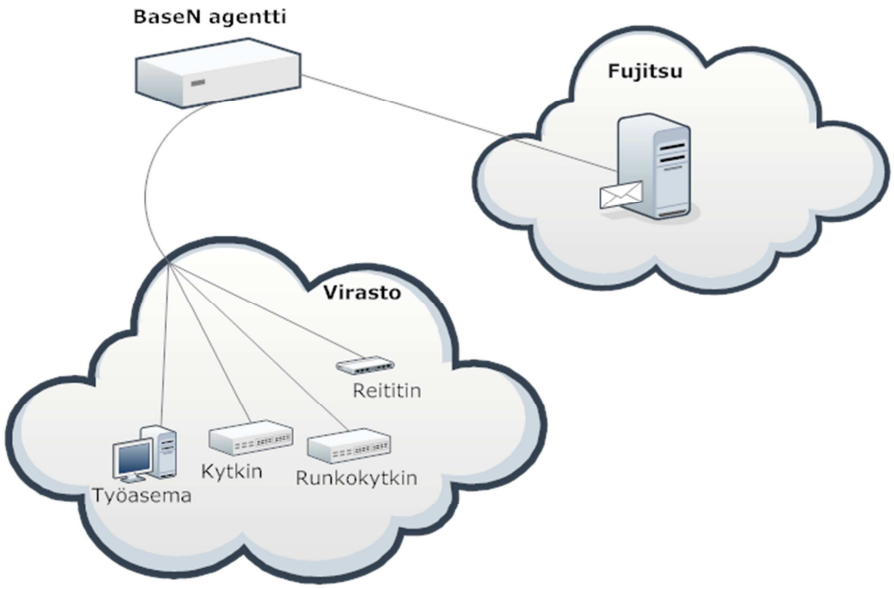
| Sektori / sovellukset | Työasemia | Suhteellinen osuus | Valittujen työasemien suhteellinen osuus | Mitattavat sovellukset |
|---|---|---|---|---|
| | 9461 | | | |
| KARAJAOIKEUS/Desktops/ | 2566 | 27,1 | 27,1 | Tuomas, Sakari |
| Vankilat/Desktop | 1646 | 17,4 | | |
| ULOSOTTO/Desktops/ | 1540 | 16,3 | 16,3 | Uljas |
| OIKEUSAPU/Desktops/ | 705 | 7,5 | | |
| HOVIOIKEUS/Desktops/ | 606 | 6,4 | 6,4 | Notes asianhallinta |
| SYYTTAJA/Desktops/ | 471 | 5,0 | 5,0 | Sakari |
| HALLINTO-OIKEUS/Desktops/ | 443 | 4,7 | 4,7 | Notes asianhallinta |
| KRIMINAALIHUOLTOLAITOS/Desktops/ | 305 | 3,2 | | |
| OM/MINISTERIO/Desktops/ | 225 | 2,4 | | |
| OM/OPK/Desktops/ | 145 | 1,5 | | |
| OM/OTTK/Desktops/ | 130 | 1,4 | | |
| VAKUUTUSOIKEUS/Desktops/ | 95 | 1,0 | | |
| OM/ERAAT VIRASTOT/Desktops/ | 79 | 0,8 | | |
| VHL/RISE/Desktops/ | 78 | 0,8 | | |
| KORKEIN HALLINTO-OIKEUS/Desktops/ | 72 | 0,8 | 0,8 | Notes asianhallinta |
| KORKEIN OIKEUS/Desktops/ | 67 | 0,7 | 0,7 | Notes asianhallinta |
| VHL/RSKK/Desktops/ | 65 | 0,7 | | |
| OM/ORK/Desktops/ | 55 | 0,6 | | |
| VALTAKUNNANSYYTTAJANVIRASTO/Desktops/ | 46 | 0,5 | 0,5 | Sakari |
| KULUTTAJARIITALAUTAKUNTA/Desktops/ | 33 | 0,3 | | |
| MARKKINAOIKEUS/Desktops/ | 32 | 0,3 | 0,3 | Notes asianhallinta |
| KRIMINAALIHUOLTOLAITOS/Notebooks/ | 31 | 0,3 | | |
| TYOTUOMIOISTUIN/Desktops/ | 13 | 0,1 | 0,1 | Notes asianhallinta |
| VALTAKUNNANVOUDINVIRASTO/Desktops/ | 8 | 0,1 | 0,1 | Uljas |
| KYOSTI KIOSKI/Desktops/ | 3 | 0,0 | | |
| TUOMARINVALINTALAUTAKUNTA/Desktops/ | 2 | 0,0 | | |
| | | 100,0 | 62,0 | |

Kuten taulukosta ilmenee, mittauksen vaikutuspiiriin saatiin 62 % kaikista työasemista, eli lukumäärällisesti mittauksen vaikutukseen saatiin ~5866 työasemaa. Listasta on vähennetty kannettavat tietokoneet, koska niitä ei ollut mahdollista saada mukaan mittaukseen. Syynä tähän on se että jokainen mitattava työasema tarvitsi kiinteän IP-osoitteen ja tätä ei voitu toteuttaa etäkannettavien osalta.

### 6.2 Mittauspisteet

Mittauspisteinä toimi, kuten kuvasta 12 nähdään palvelin, reititin, runkokytkin (jos virastossa on sellainen), kytkin ja työasema. Jokaisesta mittauspisteestä kertyi kuluja 8 € kuukautta kohden.

Palvelimen puolelta ei päästy mittaamaan reititintä tai kytkintä, mutta se ei liene oleellista tulosten oikeellisuuden kannalta, koska tietoliikenne kulkee monen reitittimen ja kytkimen kautta, joihin ei ollut mahdollisuutta päästä käsiksi. Tärkeimpänä osana pidettiinkin itse viraston sisäisen tietoliikenteen seuraamista sekä sen toimivuutta. Palvelimelta mitattiin vain sen kuormitusta.




*KUVA 12. Esimerkki mittauspisteistä*

# 7 MITTAUSPISTEET

Mittauspisteinä toimi palvelimia, työasemia, reitittimiä ja kytkimiä. Näillä valinnoilla saatiin suoritettua mittaus end-to-end -periaatteella, eli saatiin kuva koko tietoliikenneputken päästä päähän (työasemalta palvelimelle).

Seuraavassa luvussa on lueteltu mitattavat palvelimet, työasemat virastoittain, mitattavat työkalusovellukset ja mittauksessa mukana olevat virastotyypit. Lisäksi valinnat on perusteltu.

## 7.1 Mitattavat palvelimet

Alla on listattu mittauksessa mukana olleet palvelimet ja niiden lukumäärä. Kappaleessa on myös perusteltu palvelimien mukanaolo mittauksessa.

- Zenworks, 4 kpl
- Notes posti, 4 kpl
- Notes sovellus/asianhallinta, 1 kpl
- Notes sovellus/sykä, 1 kpl
- Notes data, 6 kpl
- Sakari, 1 kpl
- Tuomas, 1 kpl
- Uljas/sovellus, 1 kpl
- Uljas/tietokanta, 1 kpl
- Dataklusteri, 1 kpl
- AD Tieto, 5 kpl
- AD Virasto, 3 kpl
- Skannaus M-levy, 1 kpl
- Skannaus, 1 kpl

Luettelossa mainituilla palvelimilla saatiin suurin kustannustehokkuus käytettävyysmittaukselle. Taulukossa 8 on esitetty palvelinten tehtävät ja niiden vaikutusalueet. Valinnoilla katettiin suurimmat virastotyypit ja mahdollisimman suuri määrä työasemia sekä työkaluja.

*TAULUKKO 8. Mitattavat palvelimet, niiden tehtävä ja mittauksen tarkastelupiste*

| **Palvelin** | **Tehtävä** | **Vaikutus** |
|---|---|---|
| Zenworks | Järjestelmän hallinta, työasemien päivitys, ohjelmistojen asennukset yms. | Työasemien toiminta |
| Notes postipalvelin | Sähköposti palvelut | Työntekijöiden pääsääntöisen viestintäkanavan toimivuus ja luotettavuus |
| Notes sovelluspalvelimet | Notesin pohjalla toimivien sovellusten toiminta | Suuri osa työkalusovelluksista toimii palvelimien kautta |
| Notes data | Henkilöstön Notes profiilien ylläpito | Palvelimien kuormitus hidastaa kirjautumista |
| Uljas | Ulosoton sovellus | Uljaksen toimintavarmuus |
| Dataklusteri | Uusi ratkaisutapa tietojen hallinnointiin. Verkotettu malli | Ratkaisun haitat ja hyödyt verrattuna aikaisempaan hajautettuun järjestelmään |
| AD | Käyttäjätunnusten, niiden salasanojen ja käyttäjätunnusten oikeuksien hallinta | Palvelinten luotettaavuuden selvitys |
| Skannaus | Skannatujen tiedostojen säilytys | Palvelinten kuormitus ja käyttöaste |

Kaikkien mainittujen palvelimien osalta mitattiin niiden kuormitusta ja vasteaikaa. Kuormituksella tarkoitetaan prosessori-, keskusmuisti- ja levytilan käyttöä. Mittaus antoi tietoa siitä, jos jokin palvelin ylikuormittuu esimerkiksi prosessoritehon riittämättömyyden johdosta.

### 7.2 Mitattavat työasemat virastoittain

Alla mittauksessa mukana oleet työasemat virastoittain, sekä mittauksessa mukana olleiden työasemien kappalemäärä virastotyyppiä kohden:

- Satakunnan käräjäoikeus, Pori 2 kpl
- Oulu käräjäoikeus, Oulu 2 kpl
- Oulu käräjäoikeus, Kuusamo 2 kpl
- Vantaan käräjäoikeus 1 kpl
- Kymenlaakson käräjäoikeus Kouvola 1 kpl
- Kymenlaakson käräjäoikeus, Kotka 1 kpl
- Tuusulan käräjäoikeus 2 kpl
- Satakunnan syyttäjä 1 kpl
- Oulun syyttäjä 2 kpl
- Helsinki ulosotto 2 kpl
- Raahe ulosotto, Ylivieska 1 kpl
- Oulu ulosotto, Oulu 2 kpl
- Oulu ulosotto, Liminka 1 kpl
- Korkein oikeus 1 kpl
- Helsinki hao 1 kpl
- Kouvola hallinto-oikeus 2 kpl
- Oulu hallinto-oikeus 1 kpl

Työasemat valittiin seuraavien ehtojen mukaisesti. Työasemia tulee olla käyttäjämäärältään ja tietoliikennerakenteeltaan kolmesta erilaisesta virastosta (iso toimipaikka, pieni toimipaikka ja monitoimipaikka. Kuva 11). Jokaisesta

mittauksessa mukana olevasta virastotyypistä oli mukana vähintään yksi kappale työasemia. Työasemien määrät organisaatioittain painotettiin suhteelliseen osuuteen kaikista työasemista. Käyttäjämäärältään suuremmista virastoista valittiin useampi työasema mittaukseen, esimerkkinä Oulun käräjäoikeus ja Helsingin Ulosottovirasto.

Työasemalta vaadittiin mittaukseen kiinteä IP-osoite, SNMP-palveluiden tuli olla koneessa käynnissä ja SNMP-community oikein määritelty, jotta työasemasta pystyttiin lukemaan tietoja.

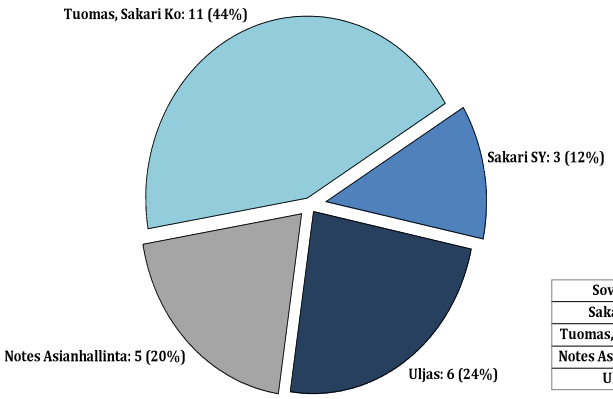
### 7.3 Mitattavat työsovellukset

Alla on listattu mittauksessa mukana olleet sovellukset, joita virastojen henkilökunta käyttää päivittäiseen työntekoon.

- Tuomas
- Sakari
- Uljas
- Notes asianhallinta

Kuten kuvasta 13 käy ilmi, käräjäoikeuksista mitattiin Tuomasta ja Sakaria 11 työasemasta, joka kattoi 44 % kaikista mitattavista työasemista. Käräjäoikeuksissa on suhteellisesti eniten työasemia, joten tämä selittää korkean prosenttilukeman. Syyttäjänvirastosta mittauksessa mukana oli yhteensä 3 työasemaa, joka kattoi 12 % mitattavista työasemista. Ulosottovirastoista mittaukseen kuului kuusi työasemaa, joista mitattiin Uljaksen toimintaa. Prosenttimäärällisesti ulosoton työasemia on 24 % mitattavista työasemista.

Notes asianhallintaa mitattiin viidestä työasemasta, jotka kattavat mittauksessa mukana olevista työasemista 20 %. Notesin-asianhallintaa, mitattiin seuraavista virastoista, Korkein oikeus sekä Hallinto-oikeus.




| Sovellus | Työasemat (kpl) |
|---|---|
| Sakari SY | 3 |
| Tuomas, Sakari Ko | 11 |
| Notes Asianhallinta | 5 |
| Uljas | 6 |

*KUVA 13. Sovellusten suhteellinen jakautuminen käytettävyysmittauksessa.*

Mitattavien työasemien määrä virastoittain perusteltiin työasemien suhteellisella määrällä. Virastot joissa oli suurempi suhteellinen määrä työasemia koko oikeushallinnon työasemiin nähden, sai osakseen suuremman määrän mittauspisteitä, kuin virastot joissa oli pienempi työasemamäärä.

Taulukossa 9 on sovellusten keskeisimmät tiedot käyttäjämääristä ajoista ja riippuvuuksista

*TAULUKKO 9. Mitattavien sovellusten keskeisimmät tiedot*

| Sovellus | Käyttävä virasto | Käyttöaika | Kriittisyys* | Käyttäjämäärä | Tapahtumat/päivä | Riippuvuudet/Liittymät |
|---|---|---|---|---|---|---|
| Notes | Oikeushallinto | 8:00-16:15 | 2 | n. 7500 | | Notes-posti ulkopuolelle ei toimi, jos w01 ei toimi |
| Sakari | Syyttäjät ja käräjäoikeudet | 7.00-21.30 | 3 | n. 1500, joista yhtäaikaisia 200 | 2000-2500 kirjautumista/ pvä 300 000-400 000 tapahtumaa/ pvä | Tilasto- ja raportointijärjestelmä Riki, Tietokanta -> DBZ, Asiakirjat -> Lotus Notes |
| Tuomas | Käräjäoikeus | 7:00-21:30 | 3 | n. 1500 | | Santra3 tiedonsiirtojärjestelmä, DW-raportointijärjestelmä |
| Uljas | Ulosotto | ? | 3 | n. 1600 | Tuxedo-palvelupyyntöjä 1 000 000 kpl/päivä, vasteaika n. 0,12 s | "Atkos" postipalvelut, sähköiset hakijat, ORK/RAJSA, VTJ, pankki, DW-Uljas |
| | | | | | | |
| Kriittisyys: | | | | | | |
| 2= Palvelun puuttuminen aiheuttaa merkittävää häiriötä | | | | | | |
| 3= Viraston toiminta täysin riippuvainen palvelusta | | | | | | |

### 7.4 Mitattavat virastotyypit

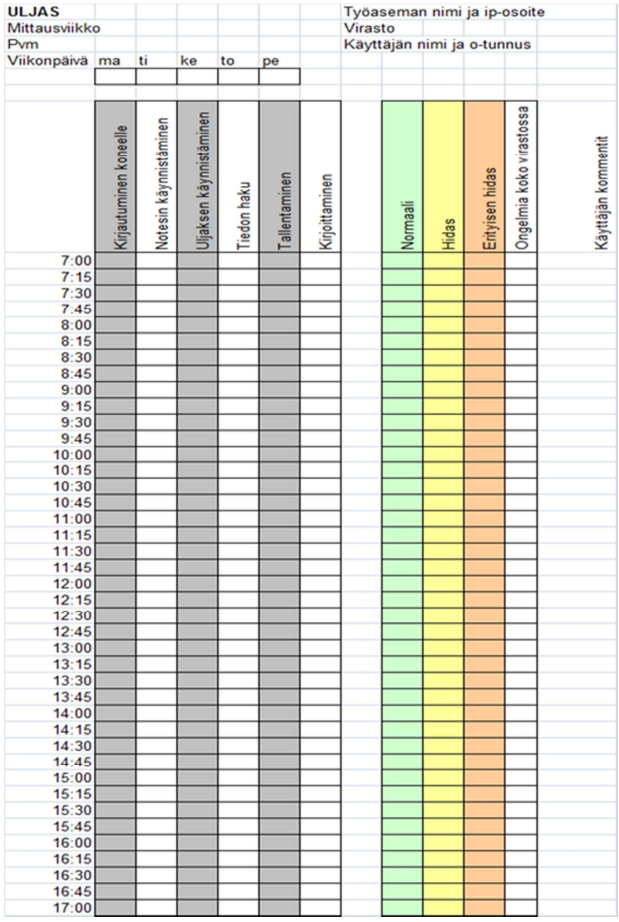
Alla on lueteltu mittauksen piiriin kuuluneet virastotyypit

- Käräjäoikeus
- Syyttäjä
- Ulosotto
- Korkein oikeus
- Hallinto-oikeus

Mitattavat virastotyypit määräytyivät mittauksessa mukana olleiden sovellusten perusteella.

### 7.5 Loppukäyttäjäkysely

Mittauksen alkuvaiheessa suoritettiin loppukäyttäjäkysely, jonka tarkoituksena oli kerätä tietoa loppukäyttäjän kokemasta käytettävyydestä. Loppukäyttäjän kokemalla käytettävyydellä tarkoitetaan sitä, miten työaseman käyttäjän mielestä ohjelmistot ja itse työasema hänen mielestään toimivat. Käyttäjä täyttivät lomaketta (Kuva 14) viiden peräkkäisen työpäivän ajan. Kysely suoritettiin kaksi kertaa, jotta saadaan luotettavammat ja kattavammat tulokset käyttäjiltä. Loppukäyttäjän kokemalla käytettävyydellä on tärkeä osa käytettävyysmittauksessa koska tärkeimpänä asiana mittauksessa on, työntekijöiden työkalujen ja laitteiston luotettava ja nopea toimivuus.




*KUVA 14. Loppukäyttäjäkyselylomake*

Käyttäjät täyttivät lomaketta viitenä peräkkäisenä työpäivänä, ja merkitsivät siihen rastin sen kellonajan kohdalle, jolloin kysytty tehtävä on suoritettu. Seuraavaksi käyttäjä arvioi tapahtuman nopeuden ja merkitsi sen lomakkeeseen. Esimerkiksi, jos työntekijä oli käynnistänyt Notesin kello 8.30, hän laittoi rastin Notesin käynnistäminen kello 8.30 kohdalle. Jos käynnistyminen oli ollut käyttäjän mielestä hidas, tuli rasti samalle vaakariville kohtaan hidas.

Kyselystä saatuja tuloksia verrattiin itse käytettävyysmittauksesta saatuihin tuloksiin. Näin saatiin kartoitettua mittauksen tasoja kohdalleen. Toisin sanoen tiedetään, paljonko on paljon ja minkä arvojen sisällä lukemien tulisi pysyä.

# 8 SAADUT TULOKSET

Työssä keskityttiin ainoastaan käyttäjäkyselyistä esille nousseiden ongelmien selvittämiseen ja mittaustulosten tarkasteluun ongelmien aikana.

## 8.1 Käyttäjäkyselyt

Käyttäjäkysely suoritettiin kahdessa osassa. Ensimmäinen kysely tehtiin marraskuun 2010 lopusta joulukuun 2010 alkuun ja toinen helmikuun 2011 alussa. Kyselyllä pyrittiin kartoittamaan käyttäjän kokemaa käytettävyyttä ja verrata niistä saatuja tuloksia, BaseN:n kautta saatuihin mittaustuloksiin. Tässä dokumentissa on käsitelty pääasiassa vain sellaisia tapahtumia, jotka käyttäjä on kokenut toiminnaltaan erittäin hitaana.

Kyselyyn valituiden käyttäjien tuli täyttää käyttäjäkyselylomaketta viiden perättäisen päivän ajan. Käyttäjät merkitsivät lomakkeeseen tehdyn tehtävän kohdalle rastin, siihen kellonaikaan kun he olivat tehtävän tehneet ja toiseen sarakkeeseen rastin miten tehtävä oli toiminut heidän mielestään.

Käyttäjäkyselyyn osallistui yhteensä 25 käyttäjää. Käyttäjät olivat samoja jotka ovat mukana käytettävyysmittauksessa. Käyttäjät täyttivät kiitettävästi kyselylomakkeita ja niistä saatiinkin hyvää vertailuaineistoa BaseN:n raporteille.

Suurin osa käyttäjäkyselyn tuloksista oli hyviä, eli käyttäjät tunsivat käytettävyyden olevan hyvä. Eniten hitautta koettiin työasemalle kirjautumisissa, notesin käynnistymisessä ja Sakarin käytössä. Taulukoissa 10 ja 11 on lueteltu kummastakin kyselystä esille nousseet erittäin hitaana, tai koko viraston ongelmana koetut tapahtumat.

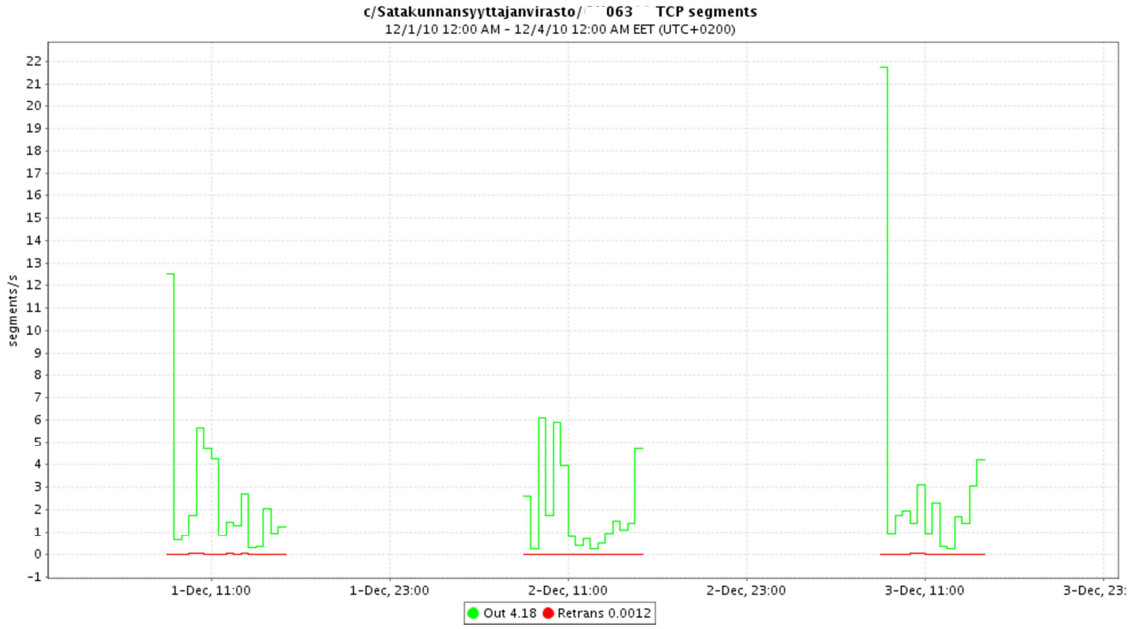
Kuvaajat on haettu BaseN portaalista osoitteesta fortn.net/om.

*TAULUKKO 10. Ensimmäisessä käyttäjäkyselyssä havaitut ongelmat*

| Virasto | Työasema | Ongelma | Laatu* | PVM | KLO |
|---|---|---|---|---|---|
| Satakunnan sy, Pori | 063 | Notesin käynnistys | EH | 3.12.2010 | 8:30 |
| Satakunnan ko, Pori | 200 | Notesin ongelmia | KV | 2.12.2010 | 11:30-13:30 |
| Vantaan ko | 192 | Kirjautumisen hitaus | EH | 9.12.2010 | 9:15 |
| Vantaan ko | 192 | Tuomaksesta haku hidasta | EH | 9.12.2010 | 11:00 |
| Vantaan ko | 192 | Kirjautuminen hidasta | EH | 9.12.2010 | 12:30 |
| Vantaan ko | 192 | Kirjautuminen hidasta | EH | 10.12.2010 | 12:30 |
| Vantaan ko | 192 | Sakarin käynnistyminen todella hidasta | EH | 11.12.2010 | 10:30 |
| Oulun hao | 111 | Notesin käynnistys | EH | 3.12.2010 | 7:30 |

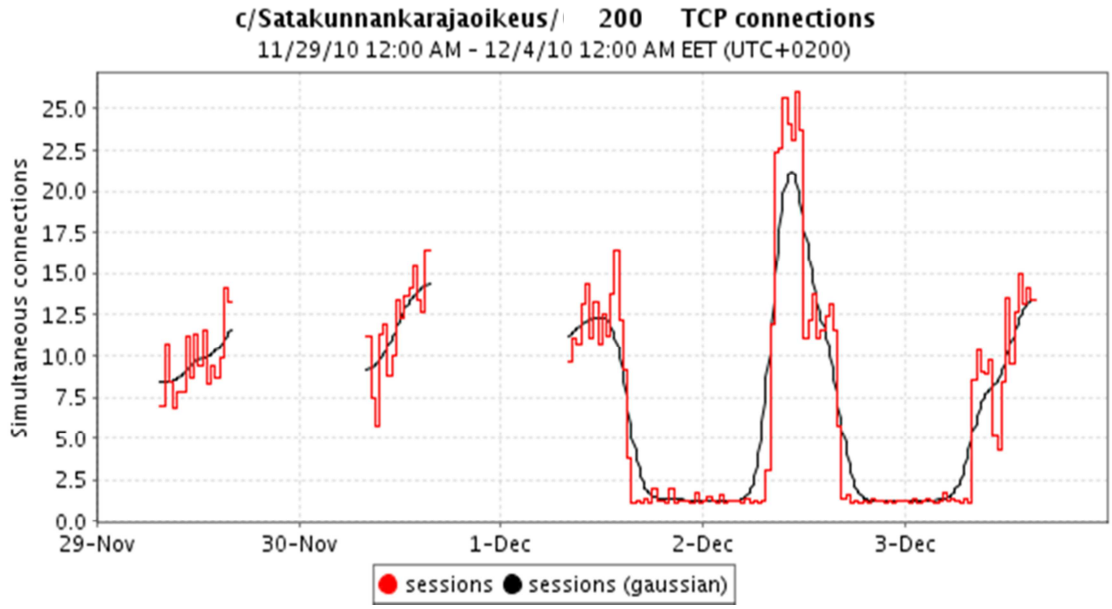
* EH = Erittäin hidas
KV = Koko viraston ongelma

Satakunnan syyttäjänviraston työasemassa 063 oli ilmennyt hitautta Notesin käynnistyksessä 3.12.2010 kello 8.30. Ainoa poikkeavuus normaalin käyttäytymiseen pitemmällä aikavälillä löytyy TCP-segmenttien määrässä tuohon kyseiseen aikaan. Segmenttien määrä on ollut kyseiseen aikaan hieman alle 22 segmenttiä per sekunti. Kyseessä voi siis olla vastaanottopään kuittaamattomuus, jolloin segmentit lähetetään uudelleen, ja tämä on näkynyt käyttäjälle hitautena. Notes-palvelimelta ei löytynyt kyseisellä hetkellä kuitenkaan normaalista poikkeavaa toimintaa.



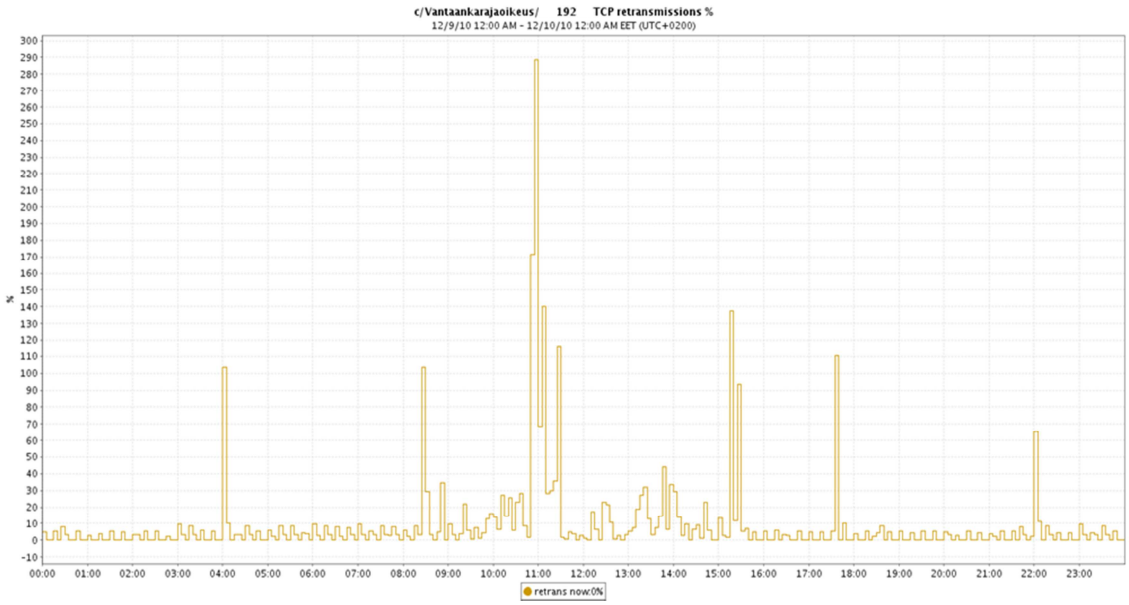

*KUVA 14. Työaseman 063 TCP-segmenttien määrä aikavälillä 1.– 3.12.2010*

Satakunnan käräjäoikeudessa oli ollut koko viraston kattava ongelma 2.12.2010 kello 11.30-13.30 Notesin käytössä. Ainoa eroavuus normaaliin oli mittausdatasta löytyvä yhtäaikaisten yhteyksien määrä, mittauksessa mukana olevalla työasemalla 200. Tietoliikenteen määrässä ei kuitenkaan tähän aikaan ollut merkittävää piikkiä. Toisaalta mittauksessa on mukana myös toinen työasema samasta virastosta, jolla ei käyttäjän mukaan kuitenkaan ilmennyt hitautta. Kuvassa 15 on esitetty työaseman 200 yhtäaikaisten yhteyksien määrä.



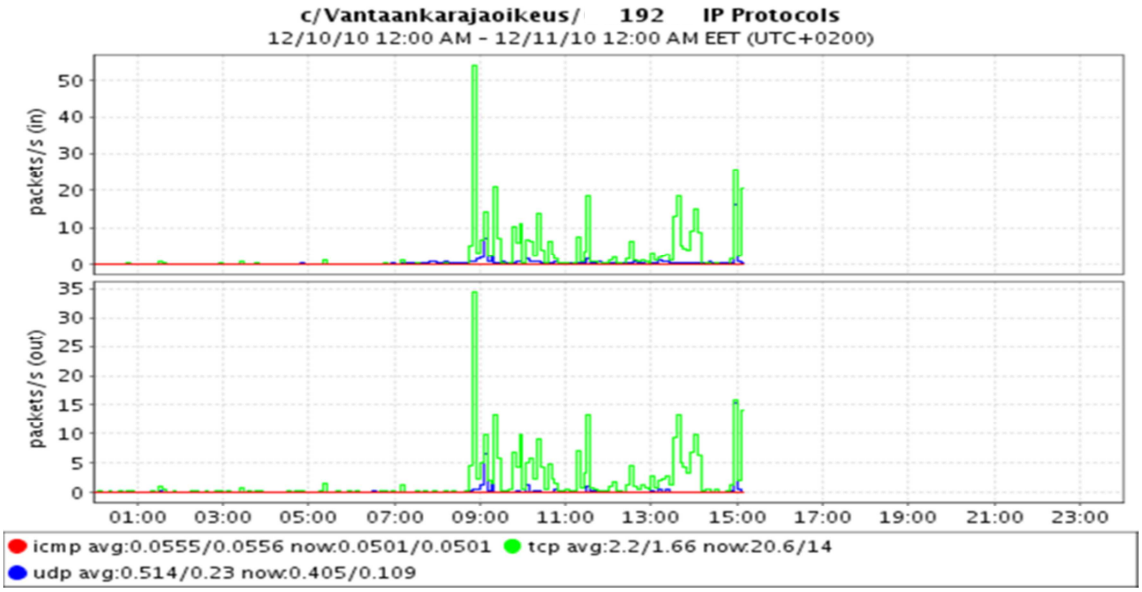

*KUVA 15. Työaseman 200 yhtäaikaisten TCP-yhteyksien määrä 29.11. - 3.12.2010*

Vantaan käräjäoikeudessa oli ollut työasemalla 192 hitautta käytännöllisesti katsoen koko päivän ajan. Hitautta oli ilmennyt kirjautumisessa ja Tuomaksen haussa, ja tietoliikenneyhteys oli ollut takkuista kello 9.15 – 12.30. Ongelma näkyi TCP retransmissions -kuvaajassa, jossa arvot olivat huomattavasti koholla koko päivän ajalta. Pahimmillaan uudelleenlähetyksiä oli yli 120 %, normaalin arvon ollessa alle 10 %. Kyseinen tapahtuma kertonee tietoliikenneyhteyden ruuhkautumisesta, josta johtuu koneen toimintojen hidastuminen. Kuvassa 16 on esitetty työaseman TCP–uudelleen lähetykset




*KUVA 16 Työaseman 192 TCP-uudelleen lähetykset*

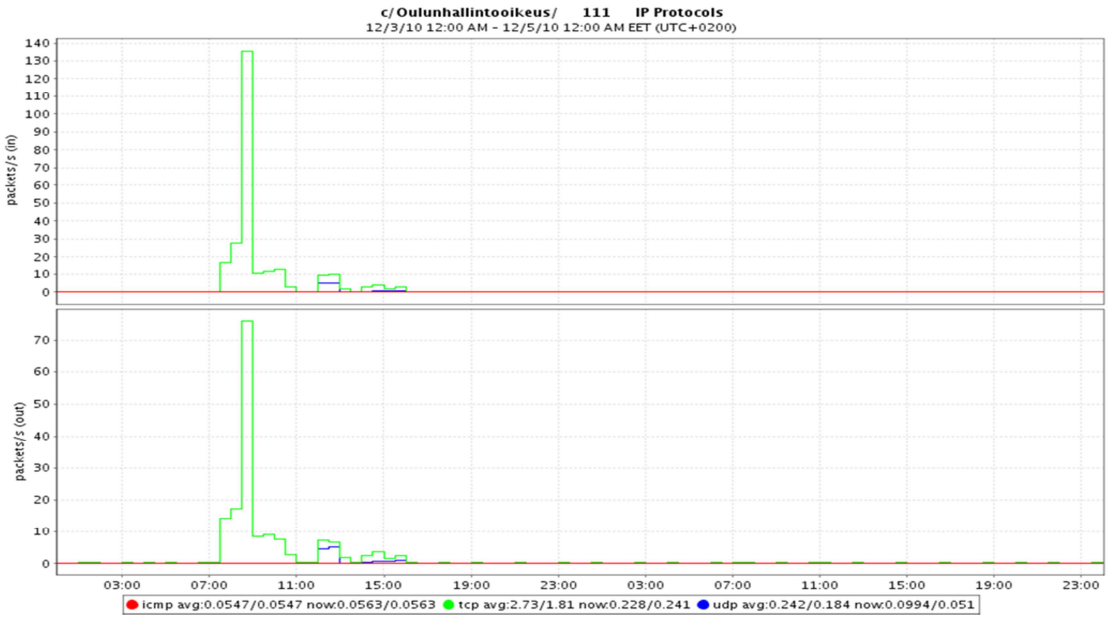
Samassa työasemassa myös TCP-pakettien määrä on ollut erittäin suuri johtuen uudelleen lähetyksistä. BaseN-palvelussa on asetettu hälytyksen rajaksi 50 pakettia/sekunti, joka on ylittynyt sinä aikana kun hitautta on esiintynyt. Arvo on ollut koholla koko päivän ajan. Kuvassa 17 on esitetty TCP-pakettien määrä työasemalta ulos ja sisään.




*Kuva 17. TCP-pakettien määrä per sekunti työasemalla 192 aikavälillä 10. - 11.12.2010*

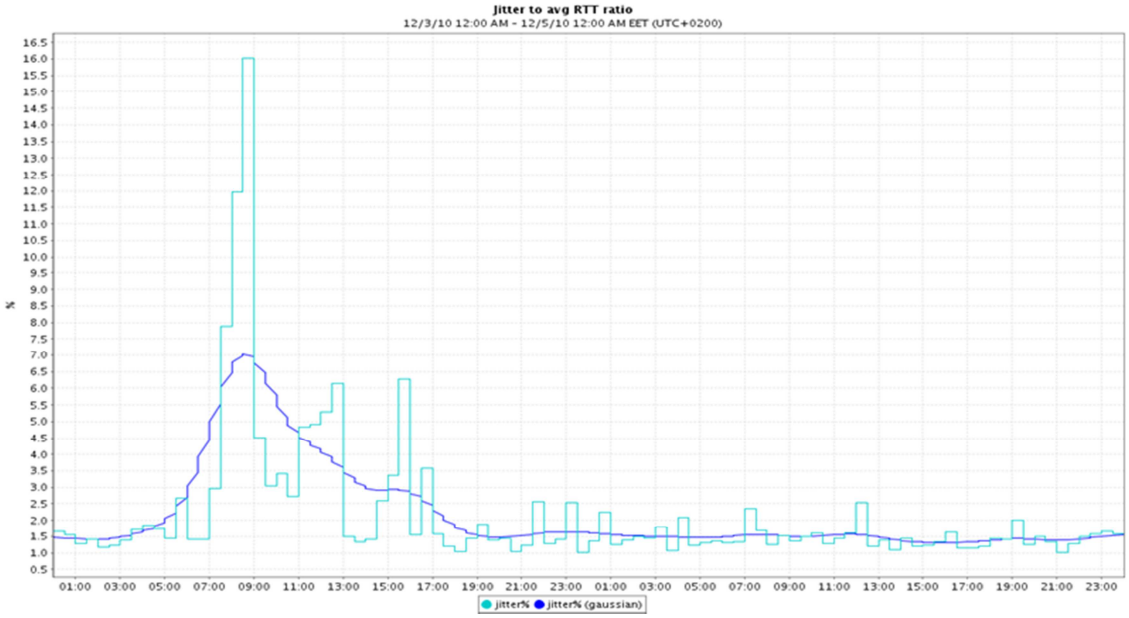
Samalla työasemalla on esiintynyt samanlaisia ongelmia myös seuraavana päivänä hieman lievempänä. Seuraavan päivän kuvaajista kävi ilmi että hitaus johtuu samasta syystä.

Oulun hallinto-oikeuden työasemalla 111 hitautta oli ilmennyt 3.12.2010 Notesin käynnistyksessä kello 7.30. Kuvaajista ilmeni edellisen tapauksen kaltainen ongelma ja pakettien liikennemäärä oli erittäin suuri, kuten kuvasta 18 käy ilmi.




*KUVA 18. Työaseman 111 TCP-pakettien määrä sekunnissa 3. - 5.12.2010.*

Myös Round Trip Timen heilahteluarvossa on piikki samalla kohtaan kuin yllä olevassa kuvassa. Työasemalta ei jostain syystä ole kyseisellä ajanhetkellä tallentunut TCP-pakettien uudelleenlähetysarvoja.




*KUVA 19. RTT:n heilahteluarvo työasemalla 111*

Ensimmäisen käyttäjäkyselyn tulokset saatiin kohtuullisen hyvin selvitettyä. Tietoliikenteessä on ollut jonkin verran ongelmia, mutta niiden syyt eivät selvinneet tässä yhteydessä. Palvelinpäässä ei näkynyt ongelmia, jotka selvittäisivät tietoliikenteen ongelmia.

Toisen käyttäjäkyselyn tulokset on esitetty taulukossa 11.

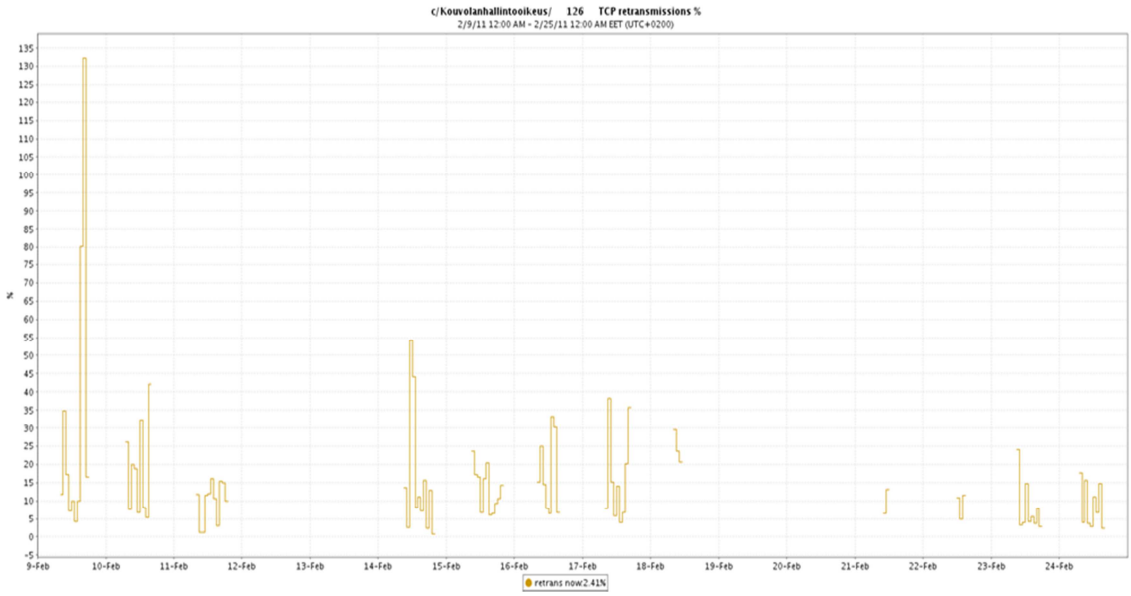
*TAULUKKO 11. Toisen käyttäjäkyselyn tulokset*

| Virasto | Työasema | Ongelma | Laatu* | PVM | KLO |
|---|---|---|---|---|---|
| Oulu Hao | 111 | Kirjautuminen ja Notes | EH | 9.2.2011 | 8:30 |
| Oulu Hao | 111 | Kirjautuminen | EH | 10.2.2011 | 8:30 |
| Oulu Hao | 111 | Kirjautuminen | EH | 11.2.2011 | 8:00 |
| Kouvola Hao | 126 | Netti hidastellut ja verkkotulostus ei onnistunut | KV | 9.2.2011 | koko pvä. |
| Tuusulan Ko | 132 | Kirjautuminen | EH | 9.2.2011 | 8:45 |
| Oulun Sy | 147 | Sakarin ongelma | EH | 9.2.2011 | 15:30 |
| Vantaan Ko | 192 | Notes-ongelmia OpenOfficen avautuminen hidas | EH | 10.2.2011 | ei merkitty |
| Satakunnan Ko, Pori | 200 | Notes ei auennut | KV | 9.2.2011 | 8:00 |
| Helsinki Hao | 218 | Asianhallinta ja Notes ongelma | | 9-11.2.2011 | koko pvä. |

* EH=Erittäin hidas
KV= Koko viraston ongelma

Oulun hallinto-oikeuden työasemalla OH111 ilmeni ongelmia kirjautumisessa sekä Notesin käytössä aikavälillä 9. - 11.2.2011. Ongelma ilmeni aina kello 8.00-8.30, eli päivällä kirjautumisessa ei ongelmia ollut. BaseN-kuvaajista ongelmalle ei kuitenkaan selitystä löytynyt. Oletettavaa on että tuohon vuorokaudenaikaan on hyvin paljon sisäänkirjautumisia, joten se voidaan kokea hitaana. Notesin käynnistymisen hitaus johtunee samasta syystä. Kaikki kuvaajat jota kyseiseltä työasemalta tarkasteltiin pitkältä aikaväliltä noudattivat normaalia käyttäytymistä.

Kouvolan hallinto-oikeuden työasemalla ilmeni ongelmia tietoliikenteen hidastumisena ja verkkotulostaminen ei onnistunut 9.2.2011. Ongelmia oli ilmennyt koko päivän ajan. Kyseisessä tapauksessa oli ongelmia TCP pakettien liikenteessä. Pakettien uudelleenlähetysmäärä oli erittäin suuri, kuten kuvasta 20 voidaan todeta.

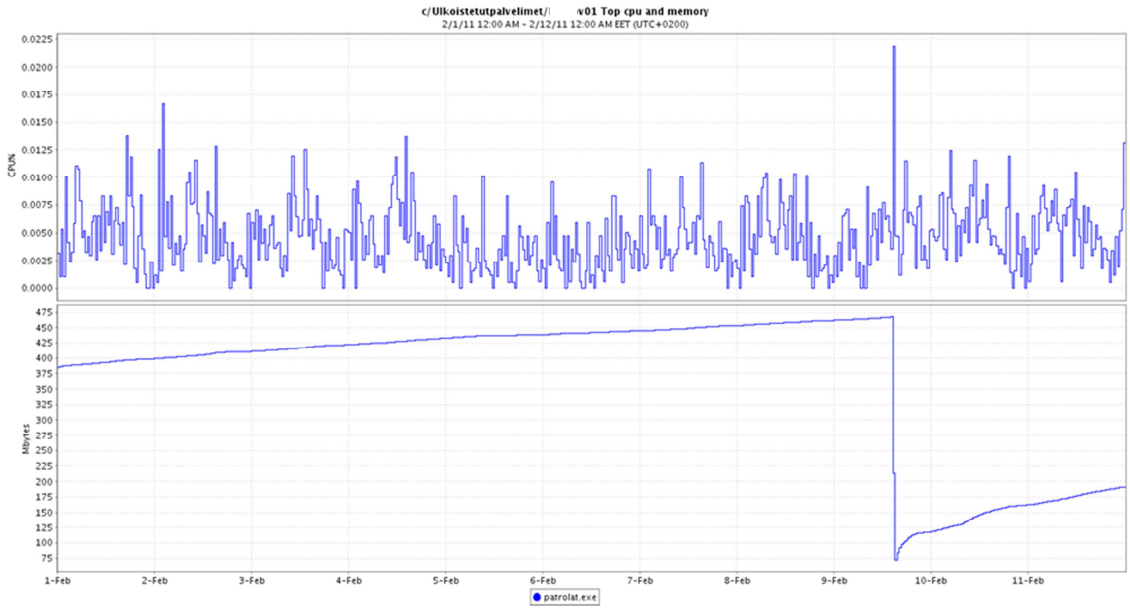



*KUVA 20. Työaseman 126 TCP-pakettien uudelleenlähetys-suhde. Aikaväliltä 9. - 25.2.2011*

Kuva 20 todistaa sen että 9.2.2011 TCP-paketteja on lähetetty moninkertaisesti uudestaan verrattuna normaalikäyttäytymiseen. Tietoliikenteessä on siis ollut tukkoisuutta kyseisenä päivänä.

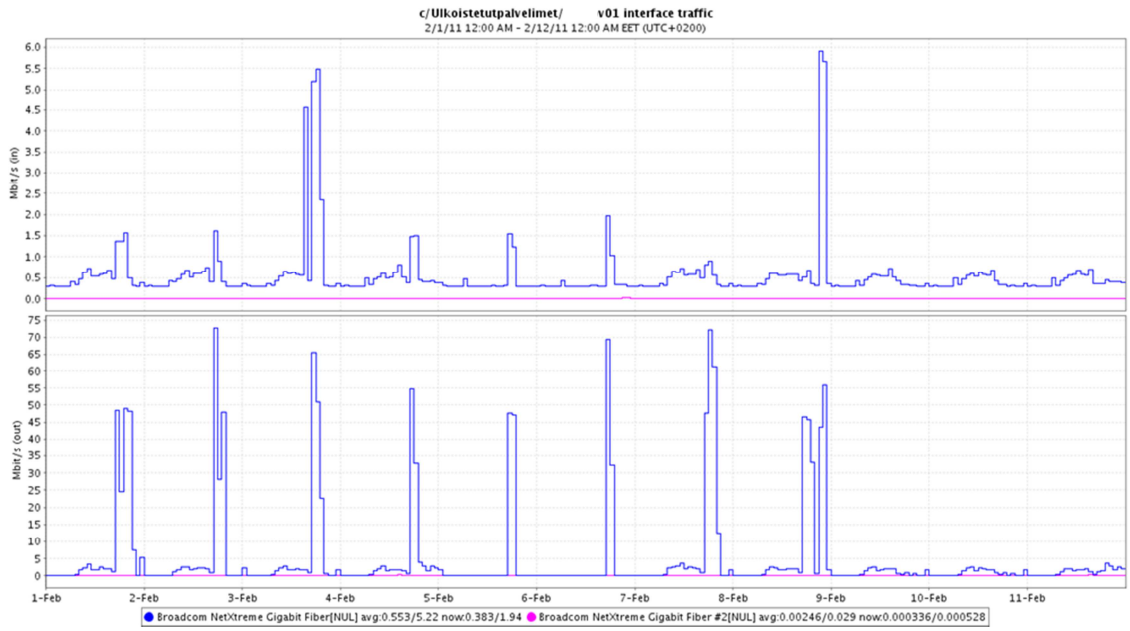
Helsingin hallinto-oikeudessa oli ollut ongelmia Notesin asianhallinnan osalta 9. - 11.2.2011 itse työasemalta ei löytynyt ongelmalle mitään selitystä, mutta tarkasteltaessa asianhallinnan palvelinta ilmeni että ongelma johtunee sieltä. Kuvissa 21, 22 ja 23 on esitetty kuvaajat jotka poikkesivat reilusti normaalista käyttäytymisestä.

Kuten kuvasta 21 nähdään, patrolat.exe on lopettanut täyden toimintansa 9. - 10.2.2011 välisenä aikana.



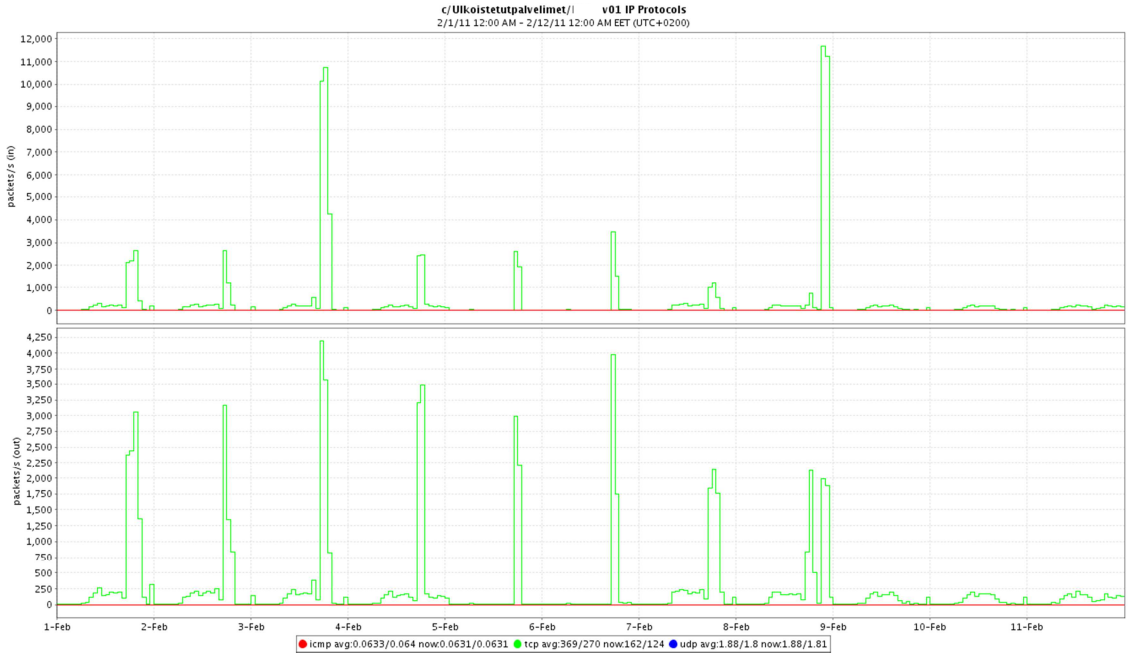

*KUVA 21. v01 palvelimen suorittimen ja muistin käyttö patrolat.exe sovelluksen osalta aikavälillä 1. - 12.2.2011*

Kuvasta 22 käy ilmi että tietoliikenteen kunnollinen toiminta on loppunut samaan aikaan, kun patrolat.exe on lopettanut toimintansa.




*KUVA 22. Palvelimen tietoliikenteen määrä aikavälillä 1. - 12.2.2011*

Kuva 23 tukee teoriaa, jonka mukaan palvelimen tietoliikenne on melkein pysähdyksissä 9. – 12.2.2011




*KUVA 23. Palvelimen TCP-pakettien liikennemäärät aikavälillä 1. - 12.2.2011*

Palvelimella on siis selvästikin ollut ongelmia aikana, jolloin käyttäjä on kokenut hidasta käytettävyyttä asianhallinnan osalta.

Toisen käyttäjäkyselyn muut ongelmat eivät selvinneet BaseN raporttien pohjalta. Kirjautumisen ongelmat jäivät siis selvittämättä työasemalta 132. Työaseman 147 Sakari ongelmalle ei myöskään löytynyt selitystä. Notes ongelmat työasemilta 192 ja 200 eivät myöskään ratkenneet.

### 8.2 Käyttäjäkyselyn arviointi

Käyttäjäkyselyn tulokset helpottivat BaseN raporttien lukemista ja kyselyn myötä saatiin myös tietoa siitä mitkä ovat raja-arvot toiminnan varmuuden kannalta. Kyselyn tulokset helpottivat siis huomattavasti löytämään reilusti koholla olevat arvot normaaleista arvoista. Toisaalta osa tuloksista ei tukenut millään tavalla käyttäjän kokemaa käytettävyyttä. Tämä johtunee siitä, ettei kaikki tarvittavat laitteet olleet mukana mittauksessa, kun ensimmäinen

käyttäjäkysely suoritettiin. Laitteista ei vielä sillä hetkellä ollut mukana kytkimet ja reitittimet, joten niiden käyttäytymistä ei voitu tutkia. Erityisesti TCP-pakettien katoamisen ja uudelleenlähetyksen kannalta näiden tarkastelu olisi voinut olla mielenkiintoista. Mittauksen mukaan työasemien suorituskyky on riittävä organisaation tarpeiden kannalta.

# 9 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää Oikeushallinnon tietotekniikkakeskuksen tietoliikenteen kokonaiskäytettävyyttä BaseN-yrityksen tarjoamalla ratkaisulla. Päätavoitteina oli suunnitella ja integroida mittaustapahtuma osaksi OTTK:n tietoliikenneverkkoa. Suunnittelun pääongelmina olivat kustannustehokkuus, laitteiden ja sovellusten valinta eri sektorien tarpeiden mukaisesti, sekä ohjelmien toiminta ja niiden kriittisten pisteiden selvittäminen loppukäyttäjän kannalta.

Ongelmat jotka asetettiin ratkaistavaksi työn aikana, saatiin suoritettua ilman suurempia ongelmia. Mittauspisteet saatiin valittua tarkan suunnittelun ansiosta kustannustehokkaasti, sillä suhteellinen osuus kaikista työasemista saatiin 62 %:iin. Luku merkitsee epäsuoraa kuuluvuutta mittaukseen. Rajatulla määrällä mittauspisteitä tämä tavoitti alkuperäisen tavoitteen. Mitattavat laitteet saatiin valittua helposti tarkan mittaustapahtuman suunnittelun avulla.

Tällä hetkellä projekti on vielä käynnissä, mutta siitä tullaan todennäköisesti luopumaan. Projekti antoi kattavan kuvan tietoliikenneverkon ja laitteiston toiminnasta, mutta projektin päätavoitteena oli tarkastella käytettävyyttä. BaseN-yrityksen ratkaisu ei ollut optimaalinen käytettävyyttä tarkasteltaessa. Työn tilaajalla on sopimus tietoliikenteen tarjoajan kanssa häiriötilanteiden valvontaan ja niihin reagoimiseen.

Raportoinnissa tehtävä muuttui hieman, sillä BaseN toimitti raportit valmiina ja niitä lukemaan valitut henkilöt olivat ammattitaitoisia tulkitsemaan kuvaajia. Loppukäyttäjille suoritettiin käyttäjäkyselyä ja päiväkirjan pitoa. äistä saatuja tietoja verrattiin mittauksesta saatuihin tuloksiin. Tulokset olivat hieman hataria, sillä joihinkin tuloksiin ja ongelmiin löytyi jonkinlainen selitys, muttei jokaiseen.

Itse käytettävyydestä kyseinen ratkaisu ei antanut kovinkaan hyvää kuvaa. Mittauksista saatujen tulosten mukaan itse laitteiden suorituskyvyssä ei ollut puutteita ja myös tietoliikenneyhteydet toimivat pääsääntöisesti hyvin. Ongelmat

johtunevat sovelluskannan arkkitehtuuriongelmista ja päällekäikksyyksistä, jotka hidastavat ohjelman käyttöä ja toimintaa.

# LÄHTEET


1. Oikeushallinnon tietotekniikkakeskuksen toimintakertomus 2009. Luotu 30.3.2009. Saatavissa: http://www.om.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=Toimintakertomus_2009.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1277813047851&blobheadername1=Content-Disposition&ssbinary=true&blobheader=application/pdf. Hakupäivä 24.2.2011

2. Oikeushallinnon tietotekniikkakeskuksen tulostavoitteet ja voimavarat vuodelle 2011. Luotu 9.12.2010. Saatavissa: http://www.om.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=Tulossopimus%202011_001.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1290611387890&blobheadername1=Content-Disposition&ssbinary=true&blobheader=application/pdf. Hakupäivä 20.11.2011

3. Lempinen, Esa 2006. Verkonhallinta tutkimusverkossa. Verkonhallintajärjestelmä Nagios. Tampere: Tampereen ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. Saatavissa:https://publications.theseus.fi/bitstream/handle/10024/10167/TMP.objres.834.pdf?sequence=2. Hakupäivä 24.4.2012

4. Telecommunications Management Network (TMN) standardi. Saatavissa: http://www.drivehq.com/file/df.aspx/publish/rayan_xeon/MYpdf/TMN.pdf

5. Simple Network Management Protocol (SNMP), Saatavissa: http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol. Hakupäivä 12.2.2012

6. Hautaniemi, Mika 2004. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Helsinki, Teknillinen korkeakoulu. Tietotekniikan osasto. Diplomityön tiivistelmä. Saatavissa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhallinta.html. Hakupäivä 1.4.2012

7. Jaakohuhta, Hannu & Lahtinen, Tapani 1997. Tietoliikenneverkot ñ Tehokäyttäjän opas. Jyväskylä: Gummerrus Kirjapaino Oy

8. Seppänen ,Marko 2008. Verkonhallinta Dna Oy Pohjois-Suomen alueella. Raahe: Oulun seudun ammattikorkeakoulu, tietotekniikan koulutusohjelma. Opinnäytetyö

9. SNMP-verkon koostumus Saatavissa: http://docs.oracle.com/cd/E13161_01/tuxedo/docs10gr3/snmpmref/1tmib.html. Hakupäivä 3.3.2012

10. Leinwald, Allan & Fang Conroy Karen 1996. Network Management A Practical Perspective. Addison Wesley Longman Inc.

11. MIB-II objektiryhmät. Saatavissa: http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_05.htm.Haku päivä 3.3.2012

12. ICMP-Ping kuvaus. Saatavissa: http://fi.wikipedia.org/wiki/Ping. Haku päivä 29.5.2012

13. Kokonaiskäytettävyyden hallinta M.Hållfast 21.6.2010. OTTK:n sisäinen dokumentti

14. BaseN Platform Technical Information, Sujit Wings. Helsinki 20.11.2008. BaseN:n tekninen informaatio dokumentti.

15. Ballew, Scott M 1997. Managing IP Networks with Cisco Routers. USA: O´Reilly & Associates.

16. FCAPS-mallin perusteet. Saatavissa: www.tml.tkk.fi/Opinnot/T-110.2100/2007/Luennot/10.Management-Billing-6.pdf. Hakupäivä 10.2.2012

17. McGinnins, Evan – Perkins David 1997. Understanding SNMP MIBs. New Jersey: Prentice Hall PTR