Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Petteri Väisänen

Opinnäytetyö

Isoworks Oy - Tietoliikenteen etävalvonta

Työn ohjaaja Diplomi-insinööri Harri Hakonen
Työn tilaaja Isoworks Oy

Toukokuu 2010 Tampere
Tampereen ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

Tekijä	Petteri Väisänen
Työn nimi	Isoworks Oy - Tietoliikenteen etävalvonta
Sivumäärä	28
Valmistumisaika	Toukokuu 2010
Työn ohjaaja	Harri Hakonen
Työn tilaaja	Isoworks Oy

TIIVISTELMÄ

Tämä tutkintotyö käsittelee Isoworksin käyttöön ottamaa verkkopohjaista tietoliikenteen etävalvontaohjelmistoa. Työn tarkoituksena oli kerätä kattava kokonaisuus informaatiota sekä toimintaohjeita Isoworksin käyttöön. Pyrkimyksenä oli, että yrityksen työntekijät toimisivat oikein eri tilanteissa. Lisäksi tavoitteena oli saada helposti luettava ja ymmärrettävä kokonaisuus. Verkkopalvelun tarjoaa Isoworksille BaseN Oy, joka toimittaa räätälöityjä etävalvontapalveluita yrityksille. Lähtötilanteessa Isoworksilla ei ollut mitään ohjeistusta palvelun käytöstä tai toiminnasta, joten minun tehtäväkseni jäi selvittää ja kerätä kaikki mahdollinen tieto yritysten sisältä samoihin kansiin.

Etävalvontaohjelmiston avulla pystytään tehostamaan verkon toimintaa sekä laskemaan kustannuksia eri tilanteissa. Lisäksi esimerkiksi ongelmatilanteisiin reagoiminen tapahtuu nopeasti ennaltaehkäisevyyden vuoksi. Isoworks Oy on maanlaajuinen yritys, jonka toiminnalle on valtava hyöty siitä, että kaikkea verkon toimintaa pystytään valvomaan yhdestä sijainnista. Isoworks Oy:n liiketoiminnan lähtökohtana on tarjota asiakasyrityksille kokonaisvaltaisia tietotekniikan palveluratkaisuja, jotta yritykset voisivat näin keskittyä omiin ydintoimintoihinsa paremmin. Tätä kokonaisvaltaisuutta tuetaan BaseN-verkkopalvelulla. Sain toimeksiannon suoraan Isoworks Oy:ltä ja sekä Isoworks että BaseN Oy avustivat minua matkan varrella. Koko työ oli yrityksen puolelta teoriapainotteinen ja tämä esittely pohjautuukin kirjalliseen dokumenttiin.

Avainsanat verkonvalvonta, tietoliikenne, etähallinta

Tampere University of Applied Sciences
Business Information Systems

Author	Petteri Väisänen
Thesis	Isoworks Oy – Remote monitoring of telecommunication
Pages	28
Graduation time	May 2010
Supervisor	Harri Hakonen
Co-operating Company	Isoworks Ltd

ABSTRACT

This thesis handles web-based remote monitoring software of telecommunications, which was implemented by Isoworks. Meaning of this thesis was to collect inclusive packet of information and instructions for the company. Aim was that employees of the company would act right in different situations as well as understandability and easiness of packet. Network service is provided for Isoworks by BaseN Corporation, which delivers tailored remote monitoring services. Starting point was that Isoworks didn't have any kind of instructions how the service works or how to use it. My job was to collect all possible information and put it together.

Using remote monitoring program helps company optimize their network functionality. In addition they can lower expenses in different situations and reacting to problems occur faster due to proactive reacting. Isoworks Ltd is nationwide corporation which gains enormous benefit because they can monitor everything from one place. Baseline for Isoworks Ltd is to offer overall information technology solutions for corporations. This way customer corporations can focus on their own main activities. I got this assignment straight from Isoworks Ltd and both Isoworks and BaseN assisted me along the way. This whole assignment was theory based.

Keywords network monitoring, telecommunication, remote control

Sisällysluettelo

1 Johdanto

Tämän päivän yritysmaailmassa pyritään yleisesti siihen, että yritys voisi keskittyä tehokkaammin omiin ydintoimintoihinsa. Tämä johtuu kustannuksien ja hintojen yleisestä kasvusta jokaisella alalla, ja säästöjä tulee täten löytää jokaiselta osa-alueelta. Tähän päästäkseen on yrityksen usein selkeytettävä ja organisoitava uudelleen toimintaansa.

Palveluiden ulkoistaminen on tämän päivän yritysmaailmassa yleistä. Tämä tarkoittaa sitä, että yritys antaa ulkopuolisen toimijan hoitaa jonkin osa-alueen sen toiminnasta. Tämä selkeyttää yrityksen toimintamallia, ja on useissa tapauksissa johtanut tietoteknisten ratkaisuiden sekä palveluiden siirtämiseen ulkopuolisten yritysten hoidettavaksi.

Ulkoistettua palvelua hoitavan yrityksen on kehityttävä mukana. Pysyäkseen sopimuksissa ja taatakseen tulevaisuutensa, on pystyttävä kehittämään palveluita asiakkaan tyytyväisyyden takaamiseksi. Tällaisessa vaiheessa Isoworks Oy päätti kehittää tietoteknistä palveluaan asiakasyrityksille siten, että pystyttäisiin ennaltaehkäisemään verkkoon liittyviä ongelmia sekä nopeuttamaan niiden korjausta.

Suoritin opintoihin liittyvän viiden kuukauden työharjoittelujakson Isoworks Oy:n palveluksessa vuonna 2009. Tarkemmin sanottuna toimipisteeni oli HUS (Helsingin ja Uudenmaan sairaanhoitopiiri), joka on ulkoistanut palvelun Isoworksille. Isoworksin kautta sain myös aiheen ja toimeksiannon tutkintotyölleni. Yritys on ottamassa laajamittaisesti käyttöön BaseN Oy:n verkonvalvontaohjelmistoa. Tähän liittyen tehtäväkseni tuli selvittää ohjelmiston toimintaa, mahdollisuuksia, hyötyjä sekä etuja.

Tutkintotyöni koostuu teoria- ja käytännönosuudesta. Käytännön osuus koostui suurimmaksi osaksi tiedon keräämisestä sekä palavereissa ja tapaamisissa käymisestä yritysten edustajien kanssa. Työ on jaettu viiteen osaan. Ensin käydään läpi yritystietoa ja asiaan liittyvää teoriaa, jonka jälkeen käydään läpi järjestelmän ominaisuudet sekä käyttöönotto.

2 Toimintaympäristö

2.1 BaseN Oy

BaseN Oy on yksityinen palveluntarjoaja, joka on perustettu vuonna 2001 Espoossa. Yrityksen perusti joukko verkkoasiantuntijoita, joilla oli paljon osaamista operaattori- ja yritysmaailmasta. Yritys keskittyy vahvasti verkkojen suunnitteluun, optimointiin sekä hallinnointiin. BaseN:llä on pääkonttori Suomessa, jonka lisäksi toimintaa on Alankomaissa sekä Yhdysvalloissa. BaseN Oy:n ohjelmisto on samanniminen kuin yritys. Se on uniikki valvonta- ja vianetsintätyökalu mahdollistaen reaaliaikaisen verkon- ja vianhallinnan.

BaseN Oy keskittyy seuraavan sukupolven teknologioihin, tarjoten kustannustehokkaita verkonvalvontapalveluita yrityksille. Yritys tarjoaa asiakkailleen mahdollisuuden saada tarkkaa tietoa yksityisten ja julkisten verkkojen toiminnasta. Jokaiselle asiakasyritykselle räätälöidään tarpeelliset palvelut asiakkaan tarpeiden mukaan.

2.2 Isoworks Oy

Isoworks Oy on suomalainen, 40 paikkakunnalla toimiva tieto- ja viestintätekniikan palveluyritys. Isoworks tarjoaa asiakkailleen kokonaisvaltaisia tietotekniikan palveluratkaisuita. Pääasiallisesti Isoworks keskittyy pieniin ja keskisuuriin yrityksiin. Työntekijöitä yrityksellä on noin 600, ja se ratkaisee vuosittain noin 350 000 ongelmatapausta ympäri suomen. Isoworks Oy kuuluu Fujitsu Services Oy:n konserniin taaten näin laadukkaan ja luotettavan pohjan toiminnalleen.

Isoworks varmistaa yritysten tietotekniikka- ja viestintäratkaisuiden sujuvan toimivuuden ottamalla tarpeen mukaan vastuun yrityksen koko ICT-infrastruktuurista. Täten asiakasyritys voi keskittää voimavaransa pääasialliseen liiketoimintaansa.

3 Verkonhallinta

3.1 Yleistä verkonhallinnasta

Verkkolaitteiden määrä on kasvanut vuosittain. Tämä on aiheuttanut sen, että verkkojen ja laitteiden hallinnasta on tullut haastavampaa ja kriittisempää. Lisäksi erikokoisten ja -tyyppisten tietoverkkojen yhteen liittäminen on tuonut lisää monimutkaisuutta verkkojen hallintaan.

Aikaisemmin verkkojen hallinta pystyttiin hoitamaan pääasiassa paikallisesti ilman etähallintaa. Nykyään tietoverkkojen kasvu on aiheuttanut tilanteen, jossa verkkoja ja niihin kuuluvia laitteita on pystyttävä hallitsemaan helposti ja tehokkaasti etäyhteydellä. Yritykset ovat tulleet riippuvaisiksi verkoista, ja kehitys-suunta on isommissa sekä monimutkaisemmissa verkoissa. Tällöin verkonhallinnalle on asetettava vaatimuksia, jotta toiminnan tavoitteet tulevat täytetyiksi. (Karila 1999.)

3.2 Verkonhallinnan vaatimukset

Verkonhallinnan vaatimukset määriteltiin alunperin ISO:n (International Organization for Standardization) toimesta, mutta nykyään ne hyväksytään laajasti yleisessäkin mittakaavassa. (Stallings 1999, 2.) Verkonhallinnan tärkeimmät yleisesti hyväksytyt vaatimukset määritellään ISO:n Common Management Information Protocol (CMIP) – verkonhallintastandardissa seuraavasti:

- virheiden hallinta
- käytön hallinta
- kokoonpanon hallinta
- suorituskyvyn hallinta
- turvallisuuden hallinta.

3.2.1 Virheiden hallinta

Tietoverkon virhetilanteiden hallinnalla on oleellinen merkitys verkon toiminnalle. Kun verkossa sattuu virhetilanne, on erittäin tärkeää suorittaa seuraavat toimenpiteet:

- vian paikallistaminen
- varmistus ettei ongelma leviä
- verkon uudelleenkonfigurointi
- vian korjaus ja verkon palautus normaaliin toimintaan.

Vika määritellään verkossa tilaksi, joka aiheuttaa verkon normaalille toimivuudelle esteen, pois lukien pienet satunnaiset ja lyhytkestoiset ongelmat. Virhetilanteiden hallinta on tärkeää verkon luotettavuuden ja käytettävyyden kannalta. Yleisesti ottaen viat pitäisi pystyä korjaamaan siten, ettei niistä koidu suuria tai ylitsepääsemättömiä ongelmia loppukäyttäjälle. Lisäksi vikatilanteista tiedottaminen on tärkeässä osassa toimintaa. (Cisco: Network Management Basics.)

3.2.2 Käytön hallinta

Verkkojen määrän ja koon kasvaessa on verkonhallinnan tärkeää tarjota työkalut verkon resurssien seuraamiselle.Verkon ylläpitäjille on hyvin tärkeätä pystyä seuraamaan verkon resurssien käyttöä käyttäjä- tai ryhmätasolla. Tietoa tarvitaan esimerkiksi laskutukseen, verkon käytön tehokkuuden varmistamiseen sekä verkon laajennusten ja parannusten suunnitteluun.

Ylläpitäjän on kyettävä määrittelemään, mitä tietoa kerätään, mistä sitä kerätään sekä kuinka usein tieto kootaan yhteen. Käytön hallinnan ensisijainen etu on sen tarjoamassa mahdollisuudessa seurata verkon resurssien todellista käyttöä. Näin verkosta saadaan informaatiota, jota tarvitaan verkkoon suunnattavien investointien kohdistamisessa oikeisiin paikkoihin. (Hautaniemi 1994.)

3.2.3 Kokoonpanon hallinta

Verkon kokoonpanon ja konfiguroinnin merkitys korostuu verkkojen koon ja niiden muutosten vuoksi. Verkon konfiguroinnin tarkoituksena on asettaa verkon eri laitteet toimimaan tietyllä tavalla tietyssä ympäristössä.

Verkon rakenteen suunnittelun kautta on mahdollista määrittää verkon toiminnallisuus käyttötarkoituksen mukaan. Verkossa tapahtuvista pienistä kokoonpanomuutoksista ei välttämättä tarvitse informoida asiakasta, mutta suuremmista muutoksista on syytä välittää tieto käyttäjille. (Haikonen, Hlinovsky & Paju 2000.)

3.2.4 Suorituskyvyn hallinta

Verkon suorituskyvyn hallinta on todella tärkeää verkon kokonaiskapasiteetin hyödyntämiseksi. Nykyään verkoissa on monia erityyppisiä komponentteja, ja yritysten on saatava verkot toimimaan parhaalla mahdollisella tavalla.

Verkon suorituskyvyn hallinta voidaan jakaa kahteen osaan: verkkomonitorointiin sekä -kontrollointiin. Monitoroinnilla tarkoitetaan verkossa tapahtuvien aktiviteettien seurantaa. Verkon kontrolloinnilla vastaavasti tarkoitetaan suorituskykyyn liittyvien toimenpiteiden tekemistä. (Stallings 1999, 5.)

3.2.5 Turvallisuuden hallinta

Turvallisuuden hallinta liittyy tietojen suojaamiseen ja pääsyn hallintaan. Verkon tietoturvan hallinta on tärkeää verkon resurssien ja loppukäyttäjien tietojen suojaamiseksi. Verkon tietoturvafunktioiden käyttö pitäisi olla loppukäyttäjälle läpinäkyvää ja lisäksi tarjota heille riittävä luottamus verkon käyttämiseen. Verkon hallintafunktioiden käyttäminen vaatii käytännössä tunnistautumista, jolloin kriittisiin verkonhallintafunktioihin ei ole oikeuksia kuin erikseen määritellyllä joukolla. (Cisco: Network Management Basics.)

3.3 Verkonhallintajärjestelmät

Verkonhallintajärjestelmä käsittää joukon työkaluja verkon monitorointiin ja hallinnointiin. Työkalut ovat integroituja toisiinsa siten, että niiden käyttöön tarjotaan yksi rajapinta, jolla saadaan suurin osa tai kaikki verkonhallintatoimenpiteet suoritettua. Verkonhallintajärjestelmän perusarkkitehtuuri koostuu vähintään yhdestä verkonhallintasolmusta sekä yhdestä tai useammasta verkkoagentista. (Stallings 1999, 6.)

Vähintään yksi verkon solmuista on määritelty verkon hallintasolmuksi, joka sisältää verkonhallintaohjelmiston sekä rajapinnan verkonhallintatoimintojen suorittamiseen. Toiset verkon solmut ovat osa verkonhallintajärjestelmää, jotka vastaavat verkonhallintasolmun lähettämiin viesteihin. Tällaista verkkosolmua kutsutaan siis agentiksi.

Agentteja voivat olla täysimittaisten verkkopalvelimien ja -päätteiden lisäksi esimerkiksi reitittimet, sillat tai modeemit. Jos verkkolaite itsessään ei tue verkonhallintajärjestelmien käyttämistä, tilanne voidaan ratkaista käyttämällä erilaisia välipalvelimia verkkolaitteiden hallinnoimiseen. Nämä muuntavat verkonhallintakäskyt kyseisen laitteen ymmärtämään muotoon. (BaseN 2009.)

3.4 Verkonhallinnan perustoiminnot

Verkonhallinnan perustoiminnoiksi voidaan lukea verkon monitorointi verkkolaitteiden tila- ja asetustietojen lukemisen kautta sekä verkon kontrollointi, jolloin verkkolaitteiden parametreja sekä tiloja voidaan muuttaa verkonhallintajärjestelmän kautta.

3.4.1 Verkon monitorointi

Verkon valvonta on verkonhallintajärjestelmän tärkein osa-alue. Kaikki verkonhallintajärjestelmät tarjoavat verkon valvontaominaisuuden, mutta eivät välttämättä hallinnointiominaisuutta. Tämä johtuu usein käytetyn verkonhallintaprotokollan puutteellisista tietoturvaominaisuuksista

Esimerkiksi Isoworksin tapauksessa toimitaan siten, että asiakasyritykset saavat näkyviin joitakin mittareita verkon toiminnasta, mutta hallinnointi sekä muutokset tapahtuvat Isoworksilta käsin.

Verkon monitoroinnin perustarkoitus on kerätä informaatiota verkkolaitteiden tilasta ja toiminnasta. Jokaisessa verkonhallintajärjestelmän piirissä olevassa laitteessa on agentti, joka kerää ja tallentaa tietoa verkkolaitteen toiminnasta. Tiedot lähetetään tarvittaessa yhdelle tai useammalle monitorointiasemalle. Agenttien keräämä informaatio voidaan välittää joko monitorointiaseman pyynnöstä, tai automaattisesti määritetyin väliajoin.

3.4.2 Verkon kontrollointi

Verkon kontrolloinnin pääasiallinen tehtävä on verkkokomponenttien parametrien muuttaminen. Verkon kontrollointiin kuuluu erilaisia funktioita, kuten verkkolaitteen alustaminen, ylläpito sekä yksittäisten verkkokomponenttien alasajo. Verkon kontrollointiin liittyy kiinteästi tietoturvallisuus. Verkon toimintoja ja verkkolaitteiden parametreja ei voi muokata tai muuttaa kuka tahansa, sillä tällaisella toiminnalla voidaan saada aikaiseksi erittäin pahaa tuhoa verkon toiminnan ja luotettavuuden kannalta. (Stallings 1999, 55.)

4 Agenttipohjainen verkonvalvontapalvelu

4.1 Yleistä

Agenttipohjaisella tietoliikenneverkon valvontapalvelulla tarkoitetaan asiakkaan käyttämiin verkko-komponentteihin kohdistuvia valvontapalveluita, jotka toimittaja tuottaa palvelukeskuksestaan asiakkaan verkkoon sijoitettavilla valvonta-agenteilla. (IT & Security Portal 2006.)

Toimittaja tuottaa verkon valvontapalvelua esimerkiksi seuraaville verkon komponenteille:

- kytkimet
- reitittimet
- palomuurit
- palvelimet.

Verkkokomponentit voivat toimia joko yksittäisinä laitteina tai modulaarisina runkokomponentteina, joissa yksi fyysinen kehikko sisältää useita erilaisia verkkokomponenttirooleja. (Isoworks 2008.)

Palvelun tuottaminen edellyttää tietoliikenneyhteyttä palvelun kohteena olevaan verkkoon. Liikennöintiprotokollina ovat IP (Internet Protocol) ja HTTPs (Hypertext Transfer Protocol Secure), joista IP-protokolla huolehtii IP-tietoliikennepakettien toimittamisesta perille ja HTTPs on salattu hypertekstin siirtoprotokolla. Valvottavaan verkkoon asennetaan valvonta-agentti, joka kommunikoi HTTPs-protokollalla palvelukeskuksen valvontajärjestelmän kanssa. Agentti analysoi valvottavia laitteita käyttäen ICMP- ja SNMP-protokollaa (Simple Network Management protocol). ICMP-protokollalla (Internet Control Message Protocol) lähetetään viestejä koneelta toiselle ja SNMP-protokollaa käytetään verkkojen hallinnassa. (Isoworks 2008.)

4.2 Palvelun sisältö

Järjestelmälle tuotetaan palveluita, jotka koostuvat alla mainituista kahdesta palvelutasosta ja lisäpalveluista. Palvelutasot määritellään komponenttikohtaisesti palvelun käynnistyksen yhteydessä. Agenttipohjainen valvontapalvelu sisältää perusverkonvalvonnan, ilmoitukset asiakkaalle ongelmatilanteissa sekä raportoinnin. Toimittajan agentti-pohjainen valvontapalvelu sisältää seuraavat tehtävät:

- kohdekomponentin tilan seuranta valvonnan hälytyksiin perustuen
- ilmoitus asiakkaalle käsittää yhden tai useamman seuraavista, sovituista ilmoituksista: yksi sähköpostiviesti sovitulla jakelulla tai yksi tekstiviesti sovitulla jakelulla
- selainpohjainen ajantasainen historiaraportointi tietoliikenneverkon komponenttien tilatiedoista ja ongelmista.

4.2.1 Taso yksi - Saavutettavuuden valvonta

Tason yksi valvontapalvelu tarkoittaa verkkokomponentin saavutettavuuden valvontaa ICMP/PING -kyselyn avulla. Saavutettavuuden valvonta toteutetaan siten, että valvontaohjelmisto lähettää määrävälein saavutettavuuskyselyitä valvottavalle verkkokomponentille. (Isoworks 2008.)

Valvontaohjelmisto kirjaa verkkokomponentin saavuttamattomuustiedot tietokantaan, josta komponenttikohtaiset käytettävyystiedot on luettavissa myöhemmin kuvatuilla raportointimenettelyillä. (Isoworks 2008.)

4.2.2 Taso kaksi - Toimivuuden valvonta sekä liikenteen mittaus

Tason kaksi valvontapalvelu kattaa verkkokomponentin käytettävyyden valvonnan (taso yksi) lisäksi myös laajemman valvonnan, joka kerää tietoa verkkokomponentin toimivuudesta ja toiminnasta.

Valvonta toteutetaan siten, että valvontaohjelmisto suorittaa ennalta määriteltyjä, laitetyyppikohtaisesti parametroituja valvontakyselyitä valvottaville verkkokomponenteille.
Valvontaohjelmiston keräämät tiedot talletetaan tietokantaan, josta ne ovat luettavissa. Valvontaa suoritetaan Isoworksin toimesta porttikohtaisesti. (Isoworks 2008.)

4.2.3 Lisäpalvelut

Yhteydenottomenettely ja palveluraportointi

Asiakkaan nimeämien henkilöiden ensisijaisena yhteydenottopisteenä palvelutuotantoon toimii palvelun käynnistämisprojektin aikana sovittu yhteydenottopiste. Palvelu tunnistetaan palvelun käynnistämisen yhteydessä sovitulla asiointinumerolla. Yhteydenotto-oikeus sovittuun yhteydenottopisteeseen on asiakkaan nimeämillä, rajatuilla henkilöillä (esimerkiksi palvelukohteen pääkäyttäjillä). (Isoworks 2008.)

Palveluraportointi sisältää palvelun käynnistämisprosessin yhteydessä toteutettavan selainpohjaisen ja ajantasaisen näkymän verkko- tai verkkokomponenttikohtaisesti. (Isoworks 2008.)

Palvelun hinnoittelu

Käynnistysmaksu voi sisältää yhden tai useamman valvonta-agentin, palveluun liitettävät muut laitteet sekä porttien määritykset ja käyttöönoton. Palvelun hinnoittelu on yleensä verkkokomponenttipohjainen per kuukausi. Jokaiselle komponentille määritellään kumman tason palveluun se liittyy (palvelutasot yksi ja kaksi). (Isoworks 2008.)

Palvelun rajaukset

Palvelulle asetetaan rajat joiden mukaan toimitaan, sekä asiakkaalla että toimittajalla on tietyt tehtävät. (Isoworks 2008.)

Asiakas vastaa:

- palvelun vastuuhenkilön ja varahenkilön nimeämisestä asiakkaan organisaatiossa
- palveluun liittyvien muutosten ja poikkeustilanteiden tiedottamisesta toimittajalle ilman aiheetonta viivästystä
- palvelun tuottamiseen tarvittavasta tietoliikenneyhteydestä
- asiakkaan käyttäjien käyttäjätunnuksien hallinnasta toimittajan raportointijärjestelmässä
- valvonta-agenttilaitteen asennuksesta sovittuun paikkaan
- laitteiden ja palomuurin konfiguroinnista valvonnan varten
- asiakkaan tietoliikenneverkon toimivuudesta.

Toimittaja vastaa:

- palvelun vastuuhenkilön ja varahenkilön nimeämisestä toimittajan organisaatiossa
- palveluun liittyvien muutosten ja poikkeustilanteiden tiedottamisesta asiakkaalle ilman aiheetonta viivästystä
- sopimusvelvotteiden tiedottamisesta ja tarvittavasta kouluttamisesta toimittajan palveluun liittyvälle henkilöstölle
- palvelun tuottamisesta asiakkaalle palvelusopimuksessa sekä palvelukuvauksessa sovitulla tavalla.

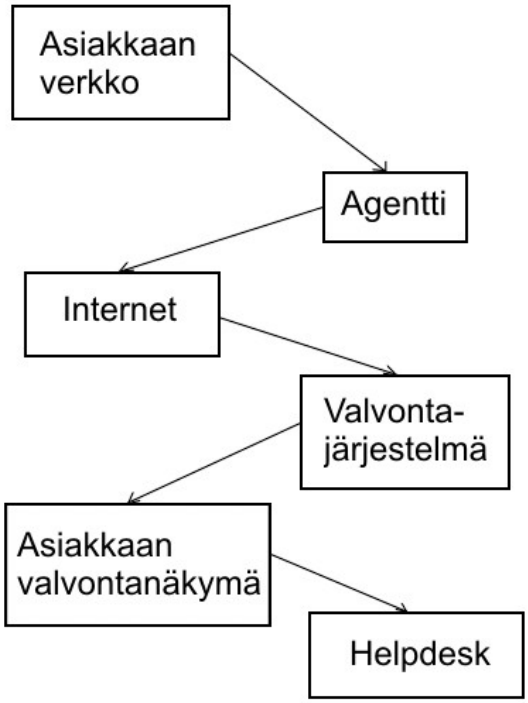
4.3 Palvelun hallinta

Palvelun käynnistäminen

Palvelun käynnistäminen vahvistetaan allekirjoittamalla palvelusopimus, jossa asiakas sitoutuu määriteltyyn palvelutasoon ja hinnoitteluun. Palveluiden käynnistyksen pohjana olevan työsuunnitelman tekee toimittaja. Suunnitelmassa kuvataan ne toimenpiteet, jotka ovat tarpeen palveluiden sujuvaan ja häiriöttömään siirtymiseen

toimittajan vastuulle siinä laajuudessa kuin asiakkaan ja toimittajan välisessä sopimuksessa on sovittu. (Isoworks 2008.)
Palvelun käynnistyksessä selvitetään palveluun liitettävät laitteet IP-osoitteineen ja valvottavat portit sekä määritellään niiden palvelutasot. Lisäksi määritellään palomuureihin tarvittavat konfiguraatiot, otetaan prosessit käyttöön sovittuine vastuineen, käynnistetään palvelukuvauksessa sovitut palvelut sekä nimetään asiakkaan ensisijainen yhteyshenkilö.

Käynnistyksen päättyessä toimittaja aloittaa palvelun tuottamisen sopimuksen mukaisesti (Kuva 1). Lisäksi asiakas voi lisätä ja poistaa laitteita valvontapalveluun ilmoittamalla muutoksista toimittajalle. (Isoworks 2008.)



Kuva 1. Palvelun tekninen kuvaus.

Palvelun päättyminen

Palvelun päättyessä puretaan käynnistyksen ja palvelutuotannon yhteydessä syntyneet palvelut, poistetaan asiakkaan tiedot ja lopetetaan palveluun liittyvien välineiden käyttö. Palvelun päättämisestä laaditaan suunnitelma, johon kuuluu tiedotus, käyttäjätunnusten

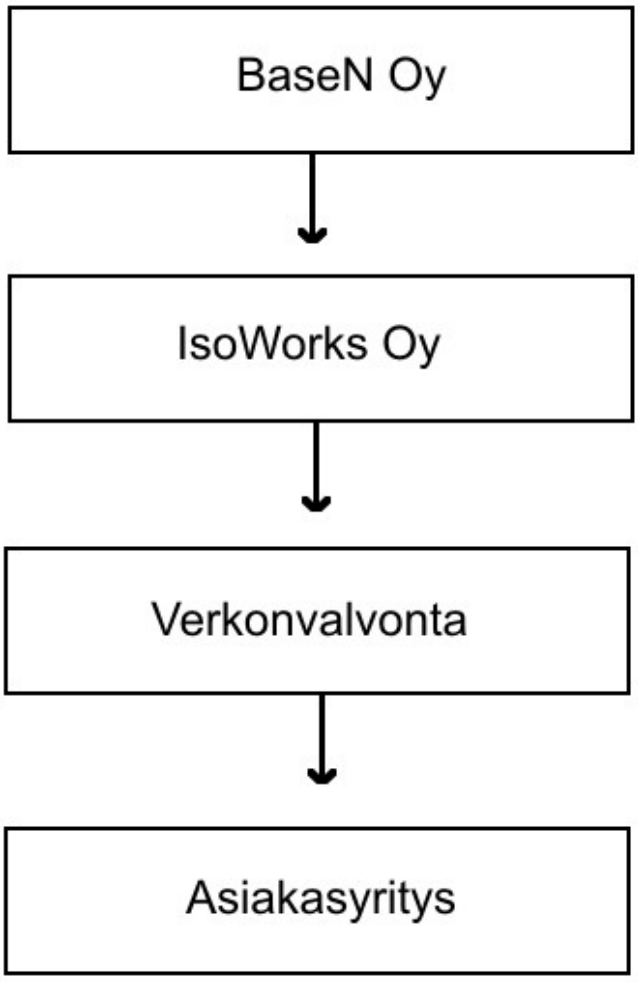
poisto, dokumentaation poisto, valvonta-agenttien palautus, laskutuksen lopetus sekä asiakkaan tietojen tuhoaminen. (Isoworks 2008.)

5 BaseN ohjelmiston esittely ja ominaisuudet

5.1 Ohjelmiston käyttötarkoitus

BaseN-alustan tarkoitus on tutkia verkkoliikennettä yrityksen tarpeiden mukaan. Se on ASP-pohjainen mittauspalvelu. Ohjelmaa käytetään verkon kautta keräämään tietoa, näyttämään visuaalisesti tuloksia sekä tuottamaan analyysejä.

BaseN toimii SaaS-mallilla, jolla tarkoitetaan sitä että BaseN tarjoaa ohjelmiston asiakasyrityksen käyttöön palveluna (Kuva 2). Ohjelmistoa voidaan käyttää ennaltaehkäisemään ongelmia ja reagoimaan niihin nopeasti. (BaseN: Services.)



Kuva 2. Palvelun toimintamalli.

5.2 Ohjelmiston hyödyt yritykselle

BaseN-palvelun käyttö ei vaadi asiakkaalta omaa laitteistoa, vaan tarvittavat laitteet toimitetaan osana palvelua. Asiakkaalta ei myöskään vaadita erikoisohjelmistoja tuotetta käyttäessä, vaan palvelua käytetään verkkosivustolla sijaitsevan ohjelman kautta. Ohjelmiston skaalautuvuus mahdollistaa uusien laitteiden lisäämisen yrityksen tarpeiden mukaan, jonka lisäksi verkkopohjaisuus mahdollistaa palvelun käytön mistä tahansa sijainnista.

Palvelun yhteensopivuus eri järjestelmien kanssa on laaja, käytännössä tarkoittaen sitä että ei ole väliä löytyykö verkkoympäristöstä Ciscon, HP:n, vai jonkin muun toimittajan laitteita.

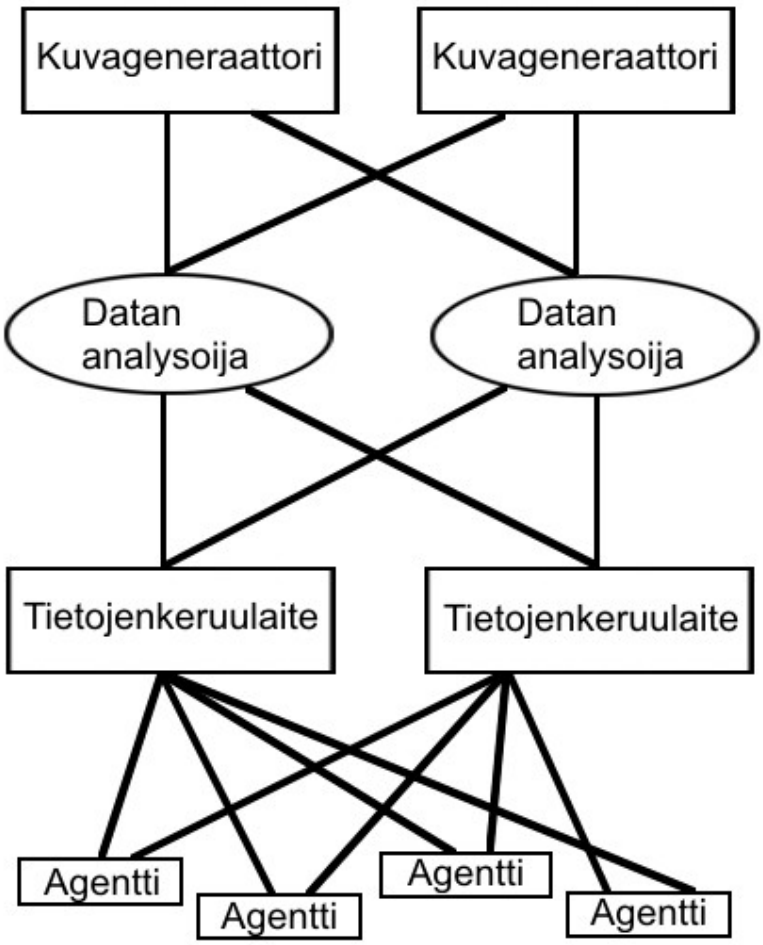
Ohjelmiston jatkuva reaaliaikaisuus mahdollistaa tiedon analysoinnin tapahtumahetkellä. Lisäksi verkkoportaalin helppokäyttöisyys nopeuttaa ja selkeyttää palvelua sekä lisää sen laatua. Verkosta kerätty tieto muokkaantuu keräämisen jälkeen helposti ymmärrettävään muotoon.

5.3 Arkkitehtuuri ja skaalautuvuus

BaseN-palvelun arkkitehtuuri on suunniteltu turvalliseksi ja skaalautuvaksi. Järjestelmä skaalautuu muutamista mittauskohteista aina miljooniin asti ilman arkkitehtuurin muutoksia.

Arkkitehtuurin virheensieto on mahdollista saada nostettua 50 prosenttiin tarpeen vaatiessa (laitteiden rikkoontuessa). Käytännössä tämä tarkoittaa kahdennusta, eli samaa mittausta suoritetaan vähintään kahdelta laitteelta samaan aikaan. Toisin sanoen fyysisellä tasolla pyritään siihen, että ongelmatilanteissa ylläpidetään katkeamaton toiminta.

Ohjelmiston tarvitsema tieto kerätään kokonaisuudessaan agenteilta (Agent machines), tietojenkeruulaitteilta (Loggers), datan analysoijilta (Data analyzers) sekä kuvageneraattoreilta (Distributed image generators) (Kuva 3). (BaseN 2009.)



Kuva 3. Järjestelmän arkkitehtuuri.

5.3.1 Agentit (Agent machines)

Arkkitehtuuri alkaa agenttilaitteista, jotka ovat asiakkaalla. Nämä laitteet keräävät varsinaisen datan yrityksen verkosta. Agenttilaitteet voivat tehdä sekä aktiivisia että passiivisia mittauksia. BaseN-ohjelmisto käyttää pääsääntöisesti näitä molempia mittauksia parhaan kattavuuden varmistamiseksi. Tämä tarkoittaa sitä, että mittauksia voidaan suorittaa joko reaaliajassa, tai vaihtoehtoisesti halutulla viiveellä. Mitattava

data kerätään usealta agenttilaitteelta, ja yksi agenttilaite pystyy säilyttämään kolmen kuukauden mittaustulokset datan säilyvyyden turvaamiseksi.

Agenttiprotokolla varmistaa sen, että normaalisti palvelun toiminta ei vie yrityksen verkon kaistanleveyttä yli 0,6 %. Agenttilaitteet ja BaseN-ohjelmisto kommunikoivat käyttäen HTTPs-protokollaa, eli mittaustulokset siirretään eteenpäin salattuina. Käytännössä toiminta menee niin, että ensin agentille ilmoitetaan mitä asioita verkosta halutaan mitata. Tämän jälkeen agentti suorittaa mittauksia ja lähettää niitä sitä mukaa eteenpäin. (BaseN 2009.)

5.3.2 Tietojenkeruulaitteet (Loggers)

Toinen palvelun osa-alueista on tietojenkeruulaitteet. Agenttilaitteet lähettävät mitatun datan tietojenkeruulaitteille, jotka ovat yhteydessä verkon kautta. Jos tietojenkeruulaitteen yhteys agenttiin katkeaa, säilyttää agentti datan siihen saakka kunnes yhteys palaa. Tämän jälkeen agentti lähettää datan tietojenkeruulaitteelle normaalisti.

Tietojenkeruulaitteet säilyttävät saadun datan yleensä yhden vuoden. Laitteet eivät tiedä toisistaan, joten jos tieto korruptoituu jollain laitteella, ei se vaikuta mitenkään palvelun toimintaan. (BaseN 2009.)

5.3.3 Datan analysoijat (Data analyzers)

Tietojenkeruulaitteet (Data analyzers) lähettävät mittaustiedot edelleen analysoijille. BaseN-ohjelmisto sisältää useita analysoijia, joilla on eri roolit, ja ongelmatilanteissa ne voivat omaksua toistensa rooleja. Analysoijat tuottavat reaaliaikaisia hälytyksiä ja visualisointia tarpeen mukaan. (BaseN 2009.)

5.3.4 Kuvageneraattorit (Distributed image generators)

Kuvageneraattorit (Distributed image generators) käyttävät analysoijilta saatua tietoa hälytysnäkymien ja kuvaajien luomiseksi. Tämän jälkeen yritys pystyy näkemään verkon tilan nopeasti. (BaseN 2009.)

5.4 Mitattavat laitteet

BaseN-palvelun avulla voidaan mitata lähes mitä tahansa verkossa olevaa laitetta. Yleensä mittaukset keskittyvät reitittimiin, kytkimiin, palomuureihin, verkon toimintaan sekä palvelinten fyysiseen toimintaan. Verkon laitteilta mitataan kaikkea, mitä tehokas valvonta edellyttää. Mittauksen suorittavat agenttilaitteet joilla on pääsy verkon tarvittaviin osiin. (BaseN 2009.)

5.5 Verkon vaatimukset

Yrityksen verkolta vaaditaan tiettyjä perusedellytyksiä palvelun toiminnan varmistamiseksi. Mittausten kohteena olevilla laitteilla tulee olla IP-osoite ping-toimintoa varten. Lisäksi agenteilta tulee olla pääsy mittauskohteisiin.

Agentteja varten tulee verkosta selvittää IP-osoite, verkkomaski, yhdyskäytävä, nimipalvelin (DNS) sekä aikapalvelin (NTP). Lisäksi verkon palomuurilta tulee sallia agentin pääsy ulkomaailmaan sekä ulkomaailmasta tietyistä kohteista pääsy agentille. Nämä sen vuoksi että agentin lähettämä data pääsee läpi, jonka lisäksi huolto- ja asetustoimenpiteitä varten yhteys tulee olla mahdollista saada ulkoverkosta. (BaseN 2009.)

5.6 Hälytykset

Hälytykset varoittavat kriittisistä ongelmista yrityksen verkossa tai palvelussa. Ne perustuvat yksilöllisiin määrittelyihin, jotka laukaisevat hälytyksen. Käyttäjä näkee yksilöidystä näkymästä mahdolliset ongelmat, mikä helpottaa niihin reagointia. Ohjelmiston päänäkymässä näkyy uusimmat virhetilanteet ja sijaintitiedot (Kuva 4).

Virheilmoitus kertoo, missä laitteessa ongelma on ja mikä on laitteen sijainti. Lisäksi graafinen kuvaaja kertoo, kuinka kauan ongelma on esiintynyt. Hälytykset jaetaan normaaleihin ja hiljaisiin hälytyksiin. Hiljaiset hälytykset tarkoittavat, ettei toimenpiteisiin ole välttämättä ryhdyttävä niin pikaisesti kuin normaalin hälytyksen tullessa. BaseN Oy:n asiakasyritykset määrittelevät itse toimintansa hälytys- ja ongelmatilanteissa siten, että se parhaiten palvelee toiminnan pikaista normalisointia.

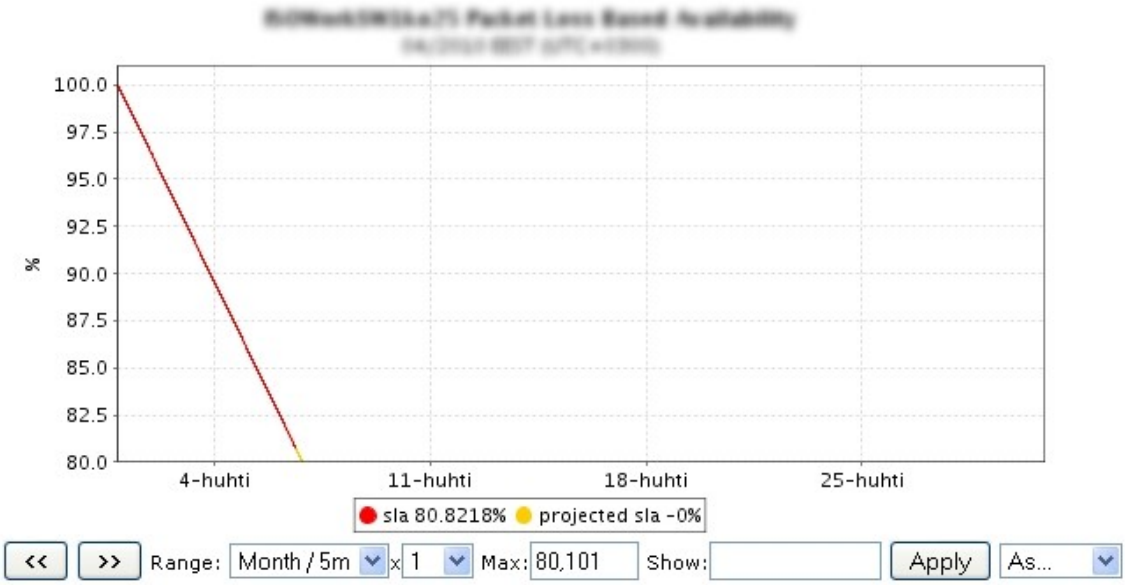
Kuva 4. Yleisnäkymä uusimmista virhetilanteista. (https://fortn.net/isoworks.)

5.7 Mittausten määrittelyt ja kuvaajat

Käyttöliittymän graafiset kuvaajat kertovat nopeasti verkon tilan halutulta osa-alueelta. Graafiset kuvaajat muuttuvat sen mukaan, miten mittauksen kohteena oleva laite käyttäytyy (Kuvaaja skaalautuu). Jos kohteessa tapahtuu suuria muutoksia, ne ovat nähtävissä kuvaajasta.

Mittausten raja-arvot määritellään tarpeiden mukaan. Mittauksissa on järkevää käyttää kuhunkin mittaukseen sopivia rajoja.
Yritys voi esimerkiksi määritellä, että tietty graafinen kuvaaja näyttää vain välin 98 – 100. Tällöin jos kuvaajan jana ylittää tai alittaa rajat, pysyy määritys muuttumattomana. On siis järkevää asettaa rajat mittauskohteisiin, joissa ei tapahdu suuria muutoksia.

Normaalia verkkoliikennettä kuvaavia graafeja ovat yleensä ainakin pakettien hukkuminen (packet loss) ja kiertoaika (round trip time). Alla olevassa kuvassa (Kuva 5) on pakettien hukkaamista kuvaava kuvaaja josta näkee pakettien hukkumisprosentin matkalla (kuvaaja määritelty näyttämään 80-100%).



Kuva 5. Graafinen kuvaaja pakettien hukkumisesta matkalla.
(https://fortn.net/isoworks.)

5.8 Uusien agenttien tilaus

Kun halutaan hankkia uusia agenttilaitteita, lähtökohtana on, että ensin käydään yhteydenpito BaseN:n myyjän kanssa. Tällöin selvitetään tuleeko kysymykseen pieni agentti vai räkkiversio. Lisäksi yrityksen tekniseltä yhteyshenkilöltä kysytään agentin toiminnan kannalta tärkeimmät verkon asetukset ja ajantasaiset palomuurisäädöt. Yrityksen tulee myös varmistaa, että agentilta on palomuurin näkökulmasta vapaa pääsy

tarvittaviin palveluihin ulkomaailmaan sekä ulkomaailmasta. Kun tarvittavat tiedot on saatu ja agentti asennettu, BaseN toimittaa laitteen yritykselle. Näin laite tarvitsee enää kytkeä ja käynnistää. Lopuksi BaseN varmistaa tuotteen toiminnan.

6 BaseN käyttöönotto Isoworksissa

6.1 Mitä Isoworks valvoo

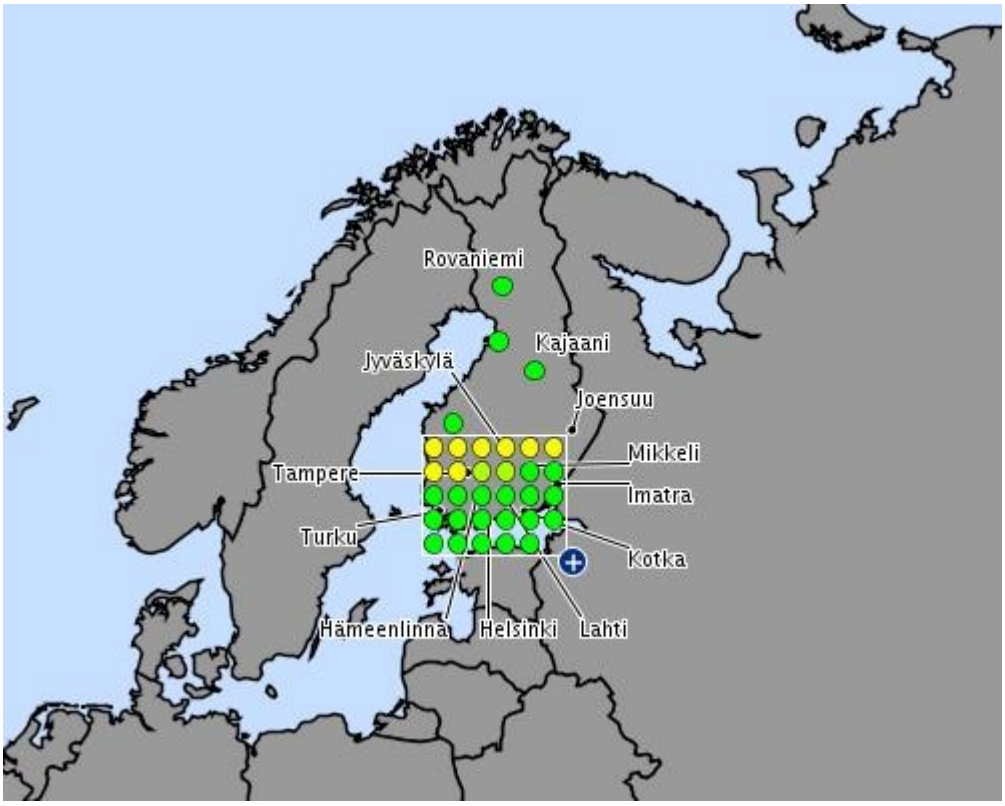
Valvonnan alaisuudessa ovat asiakkaan kanssa sovitut kytkimet. Asiakkaan kanssa sovitaan siitä, mitkä kytkimet ovat palvelun tuottamisen kannalta kriittisiä ja täten tulisi liittää valvonnan piiriin.

Tarpeen mukaan asiakkaan kanssa sovitaan mahdollisesta reitittimiin ja palomuureihin liittyvästä valvonnasta. Reitittimien valvontaa varten tarvitaan asiakkaan suostumus, sillä asiakas pyytää operaattorilta Isoworksin tarvitsemat määrittelyt.

6.2 Näkymä

Isoworks pyrkii siihen, että palvelupisteeltä (HelpDesk) käsin pääsee administrator-näkymään, jonka kautta pystyy muokkaamaan laitetietoja sekä graafisia kuvaajia. Isoworksin asiakkaalla tulee olemaan heidän omien laitteidensa perusnäkymä tarvittaessa.

Isoworksin näkymän vasemmassa reunassa nähdään asiakkaat, joita valitsemalla päästään asiakas- tai kaupunkikohtaisiin tietoihin. Kun valitsee asiakkaan nimen ja tämän jälkeen halutun kytkimen, niin näkee tietyn laitteen graafiset kuvaajat. Jos asiakasyritys on pieni tai keskikokoinen, saadaan yksinkertainen kattava näkymä kaikista mittauspisteistä. Oheisessa kuvassa (Kuva 6) pallot kuvaavat yrityksen kytkimiä.



Kuva 6. Maantieteellinen kuvaaja kytkimistä. (https://fortn.net/isoworks.)

6.3 Uusien verkkoon tulevien laitteiden päivitys

Kun halutaan mitattavaan verkkoon uusia kytkimiä tai muita verkkolaitteita, merkataan niiden tiedot excel-taulukkoon. Taulukkoon kirjataan uusien laitteiden nimet ja tiedot, minkä jälkeen sopimuksen mukaan joko lähetetään taulukko BaseN:lle tai ladataan tiedot itse palvelun sivujen kautta. Normaalisti palvelun alkuvaiheessa BaseN hoitaa laitteiden lisäämisen, jonka jälkeen asiakasyritys alkaa itse hoitaa lisäystä.

6.4 Palvelun käynnistäminen ja sen edistyminen

BaseN on luvannut, että sillä on aina agenttilaitteita valmiiksi varastossa. Kun BaseN saa asiakkaalta verkkoa varten tarvittavat tiedot, tapahtuu toimitus normaalisti kahdessa viikossa. Pikatoimituksena laitteet on mahdollista saada viikossa toimitettua.
BaseN palveluun kuuluu normaalisti kaksi vaihetta. Yhteistyön alkuvaiheessa pyritään siihen, että kaikki palveluun liittyvät muutokset ja lisäykset tehdään yhteistyössä. Asiakkuuden muuttuessa rutiiniksi BaseN vetäytyy sivummalle ja vastaa vain palvelun konfiguroinnista.

Ensimmäisten tilausten aikana Isoworks tekee standardin tilauksen ja toimittaa asiakkaan tiedot (kysytään BaseN lomakkeella), tämän jälkeen palvelu noudattaa seuraavaa kaavaa:

1) määritellään mittauspohjat ja konfiguroidaan asennettavat agentit
2) luodaan asiakaskohtainen sivusto (administrator ja normaali)
3) mittaukset laitetaan päälle
4) muutama päivä jälkimäärittelyä ja validointia
5) hyväksymispalaveri asennuksista.

Seuraavien tilausten aikana Isoworks tekee standardin tilauksen, jonka jälkeen:

1) Isoworks tekee itse konfiguroinnin (BaseN opeilla)
2) Isoworks tekee itse sivustot
3) mittaukset laitetaan päälle
4) BaseN ja Isoworks tekevät yhdessä jälkimäärittelyn ja validoinnin
5) asennukset hyväksytään palaverissa.

6.5 Ongelmatilanteet ja niihin reagointi

Ongelmatilanteissa hälytys lähtee Isoworksin palvelupisteeseen sekä nimetylle asiakkaan yhteyshenkilölle. Hälytykset toimitetaan sähköpostilla ja/tai tekstiviestillä

määrittelyiden mukaan. Normaalitilanteessa asiakas vastaa itse verkon ongelmien selvityksestä, ellei toisin ole sovittu. Isoworks reagoi hälytyksiin palveluajan puitteissa sopimuksen mukaan. Asiakkaan kanssa voidaan myös erikseen sopia, että ongelmatilanteisiin reagoidaan lähettämällä lähituki paikalle.

7 Loppusanat

Tätä opinnäytetyötä tehdessäni olin määräaikaisena työntekijänä Isoworks Oy:n palveluksessa. Työnkuvaani ei varsinaisesti kuulunut tähän työhön liittyvät asiat, mutta oli mielenkiintoista selvittää isommalla tasolla kuinka asiat toimivat. Suuren osan varsinaisen työn tiedoista sain yritysten sisältä eri henkilöiltä sekä erinäisistä dokumenteista.

Opinnäytetyön tavoitteena oli selvittää, kuinka Isoworks on ottamassa BaseN Oy:n etävalontapalvelun käyttöönsä. Lisäksi kartoitin palvelua Isoworksin päässä ylläpitäville henkilöille, kuinka erilaisissa tilanteissa tulee toimia. Tähän saakka yrityksellä ei ole ollut minkäänlaista tarkkaa toimintamallia kuinka toimia, ja tarkoituksena oli saada jokainen henkilö toimimaan oikealla tavalla. Tässä myös onnistuttiin kiitettävästi.

Työn haastavimpia puolia oli kahden yrityksen välissä toimiminen, käytännössä tarkoittaen sitä, että tarvitsin paljon informaatiota BaseN:ltä jota ei Isoworksilta vielä löytynyt. Lisäksi oli paljon asioita, mitä ei vielä oltu edes mietitty Isoworksin puolelta, ja näitä asioita jouduin käymään läpi lukuisissa palavereissa yritysten edustajien kanssa. Molemmat osapuolet olivat erittäin halukkaita avustamaan minua tiedoillaan. Lisähaasteen työntekoon toi se, että kaikki BaseN Oy:n materiaalit olivat käytännössä englanninkielisiä, ja niiden kääntäminen vei aikaa. Käytin paljon aikaa myös siihen kun tarkistin verkkolähteiden paikkansapitävyyttä William Stallingsin kirjasta.

Työn laajuus oli lopulta helppo rajata, sillä Isoworks teki hyvin selväksi mitä se haluaa ja milloin. Mielestäni tein hyvää työtä ottaen huomioon materiaalin määrän suhteessa pyydettyyn kompaktiin lopputulokseen. Aiheena tämä oli ajankohtainen, sillä yritykset siirtyvät koko ajan enemmän tämänkaltaisiin ulkoistettuihin ratkaisuihin toiminnassaan.

Työstä tulee yrityksen omien sanojen mukaan olemaan suuri hyöty yritykselle, joten olen iloinen että olen saanut olla osallisena tässä.

8 Lähteet

BaseN: Services. [www-sivu] [viitattu 14.03.2010].
https://www.basen.net/corporate/#Services

BaseN 2009. Service Reference Document.

Cisco Systems. Network Management Basics. [www-sivu] [viitattu 22.01.2010].
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/NM-Basics.html

Haikonen, Jarno; Hlinovsky, Jan; Paju, Antti 2000. Harjoitustyö:
Teletekniikan perusteet. [www-sivu] [viitattu 25.03.2010].
http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/47/index.shtml

Hautaniemi, Mika 1994. Diplomityö: TKK/Atk-keskuksen TCP/IP-verkon
valvonta ja hallinta. [www-sivu] [viitattu 10.12.2009].
http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhallinta.html

Isoworks Oy 2008. Agenttipohjainen tietoliikenneverkon valvontapalvelu.

IT & Security Portal 2006. Agent-based or Agent-less Network monitoring. [www-sivu]
[viitattu 22.01.2010].
http://www.it-observer.com/agent-based-or-agent-less-network-monitoring.html

Karila, Arto 1999. Tietokoneverkot luentomateriaali. [www-sivu] [viitattu 30.02.2010].

http://www.tml.tkk.fi/Opinnot/Tik-110.350/1999/Kalvot/TKV140499/index.htm

Stallings, William 1999. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Third Edition, 1999, Addison Wesley, ISBN 0-201-48534-6.