

Ville Laitinen

Palvelutasosopimus ja verkonvalvonta yrityksen IT-toimintojen tukena

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

13.5.2014

Tekijä Otsikko Sivumäärä Aika	Ville Laitinen Verkonvalvonta ja palvelutasosopimus yrityksen IT-toimintojen tukena 36 sivua + 1 liite 13.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaajat	lehtori Erik Pätynen ICT Director Kai Niskanen
<p>Insinööritöiden tavoitteina oli toteuttaa yrityksen käyttöön soveltuva verkkonvalvontajärjestelmä ja laatia yrityksen käyttöön palvelutasosopimus. Tavoitteet tukevat toisiaan. Palvelutasosopimuksessa määritetään verkkonvalvonnan kohteet. Verkonvalvonta tarjoaa teknisen alustan palvelutasosopimuksen seurannalle.</p> <p>Verkonvalvonnan toteutus tehtiin kahdessa vaiheessa. Ensimmäisessä vaiheessa vertailtiin eri järjestelmiä, joista parhaat vaihtoehdot valittiin koekäyttöön. Koekäytön perusteella valittiin lopullinen käyttöön otettava järjestelmä. Toisessa vaiheessa järjestelmään mallinnettiin, palvelutasosopimuksen raameja hyväksi käyttäen, valvottavat järjestelmät ja palvelut sekä valvontamääreet niille. Valvontamääreillä tarkoitetaan hälytysten ja valvonnan yksityiskohtaista määrittelyä.</p> <p>Palvelutasosopimus määriteltiin kyselyn avulla. Kyselyyn vastanneet kertoivat käytössä olevat IT-palvelut, joille asetettiin palvelutasokriteerit. Näitä ovat esimerkiksi saatavuus, prioriteetti ja riippuvuudet.</p> <p>Palvelutasosopimuksessa sovitun tason toteutumista voidaan valvoa valitulla verkkonvalvontajärjestelmällä. Järjestelmä mahdollistaa liiketoiminnalle kriittisten järjestelmien toiminnan seuraamisen ja mahdollistaa vikoja ennaltaehkäisevät toimenpiteet. Palvelutasosopimus selkeyttää yrityksen IT-toimintojen roolia yrityksen sisäisenä palveluntarjoajana.</p> <p>Vastaisuudessa on mahdollista laajentaa verkkonvalvontajärjestelmän toimintaa kattamaan yhä suurempaa alaa yrityksen liiketoimintaprosesseista sekä syventää valvontaa esimerkiksi määrittelemällä palveluiden testaamiseen virtuaalikäyttäjiä. Lopputuloksena yrityksen IT-toimintojen on mahdollista seurata palveluiden tilaa proaktiivisesti ja samalla tietää muodolliset vaatimukset niiden toiminnalle.</p>	
Avainsanat	SNMP, verkkonvalvonta, SLA, palvelutasosopimus

Author Title Number of Pages Date	Ville Laitinen Using network monitoring and service level agreement to support enterprise IT operations 36 pages + 1 appendix 13 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Erik Pätynen, Senior Lecturer Kai Niskanen, ICT Director
<p>The goal of the project discussed in this thesis was to determine the requirements for IT services by forming service level agreement (SLA) and also to explore and implement suitable network monitoring system (NMS). Network monitoring and SLA hold many synergies, as SLA defines targets for network monitoring whereas network monitoring provides a technical platform to follow SLA.</p> <p>First, different network monitoring systems were compared, and the best alternatives were chosen for a trial. Secondly, NMS was defined in accordance with the SLA. The SLA was formed by data collected from questionnaires. IT services were formally recognized in the questionnaires and their service levels were defined.</p> <p>Finally, NMS was taken into use. The solution enables proactive monitoring of IT services which are prerequisites for a multitude of business processes. The SLA clearly defines the role of the IT department as an internal service provider.</p> <p>In the future, network monitoring can be extended to a wider range of business processes and also the current level of monitoring can be expanded for example by defining virtual users to test service function. In conclusion, it is possible for the IT department to proactively monitor services with the knowledge of clearly defined SLA.</p>	
Keywords	SNMP, network monitoring, SLA, service level agreement

Sisällys

Lyhenteet

1	Johdanto	1
2	Verkonvalvonnan teoriaa	3
2.1	Verkonvalvonnan osa-alueet	3
	Vikojen hallinta	4
	Käytön hallinta	4
	Kokoonpanon hallinta	4
	Suorituskyvyn hallinta	4
	Turvallisuuden hallinta	5
2.2	Verkonvalvonta järjestelmän eri tasoilla	5
2.3	Verkonvalvonnan käytännön toteutukset	5
2.4	SNMP-protokolla	6
	2.4.1 Roolit	7
	2.4.2 MIB-tietokanta	7
	2.4.3 SNMP-viestin muoto	9
	2.4.4 SNMPv1-viestin PDU-tyypit	11
2.5	Muut verkonvalvontaprotokollat	12
3	Verkonvalvonnan toteutus	14
3.1	Vaatimukset verkonvalvontajärjestelmälle	14
	Tekniset vaatimukset	14
3.2	Verkonvalvonnan suunnittelu	15
3.3	Verkonvalvontajärjestelmien vertailu	16
	3.3.1 Icinga	16
	3.3.2 Valhal	17
3.4	Vertailun tulos	19
3.5	Verkonvalvontajärjestelmän käyttöönotto	19
3.6	Verkonvalvontajärjestelmän testaus ja ongelmatilanteet	22
4	Palvelutasosopimus	23
	4.1 Saatavuus	23
	4.2 Palveluaika	25

4.3	Palvelujärjestys	25
4.4	Quality of Service	25
5	Palvelutasosopimuksen määrittäminen	27
5.1	Palvelutasosopimuksen määrittämissuunnitelma	27
5.2	Kyselyn toteutus	28
5.3	Kyselyn eri näkökulmat	29
5.4	Kyselyjen tulokset	30
5.5	Kyselyn ongelmakohdat	32
6	Yhteenveto	32
6.1	Verkonvalvonnan lopputila	32
6.2	Palvelutasosopimuksen lopputila	33
6.3	Verkonvalvonta ja palvelutasosopimus yhdessä	34
	Lähteet	35
	Liitteet	
	Liite 1. SLA-matriisi	

Lyhenteet

Lyhenteet

IETF	<i>Internet Engineering Task Force</i> . Avoin yhteisö, joka on monien nykyai- kaisten internet-tekniikoiden taustalla.
ISO	<i>International Organization for Standardization</i> . Kansainvälinen standardi- soimisjärjestö.
ITU	<i>International Telecommunication Union</i> . Kansainvälinen televiestintäliitto.
ITU-T	<i>ITU Telecommunication Standardization Sector</i> . Kansainvälisen televies- tintäliiton standardointiosasto.
MIB	<i>Management information base</i> . Tietokanta järjestelmien hallintaominai- suuksille.
MTBF	<i>Mean time between failures</i> . Keskimääräinen aika, jonka kuluessa laite vi- kaantuu.
MTTR	<i>Mean time to repair</i> . Keskimääräinen aika joka kuluu vikaantuneen laitteen korjaamiseen.
NMS	<i>Network monitoring system</i> . Verkonvalvontajärjestelmä.
OID	<i>Object identifier</i> . Hallittavan järjestelmän yksittäinen hallintamääre.
OSI	<i>Open Systems Interconnection</i> . ISO:n ja ITU-T:n hanke tietoverkkojen standardointiin.
RFC	<i>Request for Comments</i> . IETF:n julkaisemia muistioita, joista useat ovat muotoutuneet internetin standardeiksi.
RMON	<i>Remote Network Monitoring</i> . IETF:n liikennepohjainen verkonvalvontapro- tokolla.

SLA	<i>Service-level agreement.</i> Osapuolten välinen sopimus palvelutasosta.
SNMP	<i>Simple Network Management Protocol.</i> Verkkoprotokolla IP-verkkojen hallintaan.
UDP	<i>User Datagram Protocol.</i> Yhteydetön siirtoprotokolla, toinen internetin siirtoprotokollista yhteydellisen TCP:n rinnalla.
UPS	<i>Uninterruptible power supply.</i> Laite, jolla voidaan taata keskeyttämätön virransyöttö.

1 Johdanto

Nykyaikainen yritystoiminta on sidoksissa tietoverkkoihin ja sen toiminnasta riippuvaisiin IT-palveluihin. On vaikea kuvitella monenkaan yrityksen toimivan ilman näitä edellytyksiä. Pidemmät toimintakatkokset voivat jopa aiheuttaa jatkuvuusongelman yritystoiminnalle.

Miten tämän kaltaisia riskejä vastaan voidaan suojautua? Ongelma ei jää ilman ratkaisua, sillä tietoverkkojen ja IT-palvelujen toimintaa voidaan seurata systemaattisesti, verkonvalvontatyökaluilla.

Verkonvalvonta antaa näkymän yrityksen tietoverkon ja IT-palveluiden toimintaan, mahdollistaa ongelmien ennaltaehkäisyn ja edesauttaa niiden korjaamista. Se on myös oiva työkalu SLA:n (palvelutasosopimuksen) seurantaan.

Palvelutasosopimus määrittää tason yrityksen sisäisten ja ulkoisten palveluiden toiminnalle. Sopimus tehdään palvelun toimittajan kanssa, tavallisesti sisäisten IT-palveluiden tapauksessa sovitaan yrityksen sisäisten IT-toimintojen kanssa.

Palvelutasosopimus on olennainen, sillä onko muuten mahdollista tietää minkä palveluiden toiminta täytyy taata? Voidaanko sanoa, mikä on sopiva toimintataso palveluille? Palvelutasosopimus on vastaus näihin kysymyksiin ja se velvoittaa samalla osapuolet noudattamaan yhdessä sovittua tasoa.

Työ tehdään suomalaiselle (18.3.2014 japanilaisen luokituslaitos ClassNK:n omistukseen) Napa-yhtiöille. Napa-yhtiöt tarjoavat tietoteknisiä tuotteita ja palveluita merialusten suunniteluun ja operointiin. Napa-yhtiöt koostuu emoyhtiö Napa Oy:stä ja sen tytäryhtiö Onboard-Napa Oy:stä. Yritysten toiminta on maailmanlaajuista. Kuvassa 1 ovat kaikki yrityksen toimipisteet sekä muu palveluverkosto.



Kuva 1. Napa-yhtiöiden toimipisteet ja palveluverkosto [1].

Yrityksen toiminnan moninaistuminen ja laajeneminen maailmanlaajuiseksi asettaa erityiset haasteet verkonvalvonnan toteutukselle. Valvontaa ei enää ole tarkoituksenmukaista tehdä erillisillä komponenteilla, vaan on suunniteltava järjestelmäarkkitehtuuriin sopiva keskitetty valvontaratkaisu.

Sisäinen palvelutasosopimus tehdään IT-toimintojen roolin selkeyttämiseksi. Vastaavanlaista sopimusta ei ole ennestään olemassa. Sopimus määrittää yrityksen sisällä, IT-toimintojen ja yrityksen välille.

Työn tavoitteena on suunnitella ja ottaa käyttöön yrityksen vaatimukset täyttävä verkonvalvontaratkaisu ja palvelutasosopimus. Verkonvalvonnassa määritetään vaatimukset, jotka ratkaisuehdotusten tulee täyttää. Ratkaisuehdotukset otetaan koekäyttöön, jonka perusteella valitaan lopullinen järjestelmä. Lopulliseen järjestelmään määritellään perustoiminnallisuus. Palvelutasosopimuksen määrittämiseen vaadittavat tiedot hankitaan ensisijaisesti siitä suoritettavan kyselyn perusteella. Kyselystä kerättyjen tietojen pohjalta on mahdollista antaa ehdotus palvelutasosopimuksesta.

2 Verkonvalvonnan teoriaa

Verkonvalvonta käsitteenä ei ole kovinkaan yksiselitteinen. Se voidaan nähdä esimerkiksi aktiivisena seurantana tai passiivisempänä valvontana. Myös valvonnan kohteet vaihtelevat: usein seurataan verkkolaitteiden käytettävyyttä, mutta myös monimutkaisempien palveluiden seuranta on mahdollista.

Työssäni tarkoituksena on suunnitella ja ottaa käyttöön verkonvalvontajärjestelmä, jolla on tarkoitus suorittaa pääosin passiivista käytettävyyden valvontaa ja jonka toiminta on mahdollista laajentaa monimutkaisiin palvelukokonaisuuksiin.

2.1 Verkonvalvonnan osa-alueet

Miten verkonvalvontaa voidaan lähestyä kokonaisuutena? On eri lähtökohtia, mutta luonteva kulma asiaan on ITU-T:n (Telecommunication Standardization Sector) standardi x700. ITU-T on ITU:n (Kansainvälinen televiestintäliitto) alaisuudessa toimiva organisaatio [2], joka saa mandaattinsa suoraan YK:lta. Standardi kattaa erityisesti puhe-
linverkot, mutta se on myös sovellettavissa tietoverkkoihin. Standardi on hyödyllistä käsitellä, sillä se on yleisesti tunnettu ja tunnustettu.

ITU-T:n standardi jakaa verkonvalvonnan viiteen osa-alueeseen, joita ovat

- vikojen hallinta
- käytön hallinta
- kokoonpanon hallinta
- suorituskyvyn hallinta
- turvallisuuden hallinta [3, s. 3].

Seuraavaksi esittelen lyhyesti eri osa-alueiden tarkoituksen ja annan tietoverkkojen valvonnalle tyypillisen esimerkkisovelluksen alueesta. Verkonvalvonnan toteutuksessa keskityn pääosin vikojen- ja suorituskyvyn hallinnan näkökulmiin.

Vikojen hallinta

Vikojen hallinta on vikojen havaitsemista, eristämistä ja korjaamista [3, s. 4]. Vika tarkoittaa tässä yhteydessä muutosta tai tapahtumaa, jonka johdosta määrätty palvelu ei ole saatavilla.

Esimerkkisovellus: verkkolaite ei vastaa yhteydenottoihin määritellyssä ajassa. Verkonvalvontaohjelmisto antaa hälytyksen, jonka perusteella vika voidaan havaita ja korjata.

Käytön hallinta

Käytön hallinta kattaa verkon resurssien käytön seurannan, josta voidaan muun muassa johtaa laskutus käytön perusteella.

Esimerkkisovellus: yritys ostaa operaattorilta datayhteyden haarakonttoriinsa. Laskutus on sidottu liikennemäärään, ja yritys haluaa seurata yhteyden käytöstä koituvia kustannuksia ja mahdollisesti asettaa rajan yhteyden käytölle.

Kokoonpanon hallinta

Kokoonpanon hallinta on laitteiden asetusten hallintaa. Se sisältää laitteiden ja palveluiden asetusten tarkastelun, muokkaamisen ja palauttamisen.

Esimerkkisovellus: kaikkien verkkolaitteiden asetukset tallennetaan keskitetysti yrityksen järjestelmään. Rikkoutuneet laitteet ovat suoraan korvattavissa, kun käytetyt asetukset ovat tallessa.

Suorituskyvyn hallinta

Suorituskyvyn hallinta on verkkoresurssien suorituskyvyn ja käyttäytymisen valvontaa [3, s. 4]. Suorituskyvyn hallinta voidaan helposti sekoittaa käytön hallintaan. Osa-alueiden välillä on kuitenkin perustavan laatuinen eroavaisuus. Käytön hallinta mittaa määrää, kun taas suorituskyvyn hallinta määrän suhdetta aikaan (kuten esimerkiksi nopeuden ja matkan eroavaisuus fysiikassa).

Esimerkkisovellus: seurataan WWW-palvelimen vasteaikoja pyrkien takaamaan riittävä palvelunlaatu kaikkina aikoina. Vasteaikojen muuttuessa huonommiksi on mahdollista ryhtyä ennakoiviin toimiin tai esimerkiksi kirjata poikkeus ylös, mikäli se rikkoo sovittua palvelutasoa.

Turvallisuuden hallinta

Turvallisuuden hallinta tukee tietoturvamääräysten toteuttamista, tarkemmin tietoturvamääreiden luomista, levittämistä ja niiden raportointia [3, s. 4].

Esimerkkisovellus: määritellään verkkolaite kirjaamaan kaikki siihen kirjautuneet käyttäjät. Poikkeustilanteessa voidaan tarkastaa edellinen kirjautuminen laitteelle, ja selvittää poikkeuksen aiheuttaja.

2.2 Verkonvalvonta järjestelmän eri tasoilla

Osa-alueiden lisäksi on hyödyllistä jakaa verkonvalvonta eri tasoille. Tasot voidaan ymmärtää esimerkiksi OSI-mallin (Open Systems Interconnection model) tapaisiksi kerroksiksi. Osa-alueet jakavat verkonvalvonnan kohteet luokkiin valvonnan näkökulmasta, kun taas tasot määrittelevät kohteet valvottavan järjestelmän tason perusteella.

Tässä työssä jaan pääosan valvonnan kohteista palvelu- tai laitetasolle. Palvelut koostuvat lähes aina monesta valvottavasta laitteesta. On esimerkiksi helppo ymmärtää, että tietoverkko ei toimi ilman verkkolaitteita eikä verkkosivu ei toimi ilman WWW-palvelinta.

2.3 Verkonvalvonnan käytännön toteutukset

Miten verkonvalvonta tapahtuu käytännössä? Verkonvalvonta ei yksinomaan tarkoita suunniteltua, keskitetysti ohjattua kokonaisuutta, jolla valvonta suoritetaan. Lähes kuka tahansa voi käyttää verkonvalvonnan työkaluja päivittäin sitä varsinaisesti tietämättä.

Yksinkertaisimmillaan kyse on käyttöjärjestelmän sisäänrakennettujen toimintojen käytämisestä. Näistä yksi tunnetuimmista on ping-komento (ICMP echo request). Komenolla voidaan tarkistaa kohteen saatavuus [4, s. 1], eli onko kohde tavoitettavissa verkon

välityksellä. Tässä tapauksessa on kyseessä yhteyden testaaminen, joka on yksi yksinkertaisimmista tavoista toteuttaa verkonvalvontaa.

Usein järjestelmät eivät kuitenkaan ole näin yksinkertaisia, riippuvaisia vain yhden kohteen saatavuudesta. Järjestelmät koostuvat yhdestä tai useammasta palvelusta, joiden seuraaminen vaatii usein jo erikoistuneen sovelluksen. Miten pystytään tarkistamaan WWW-palvelimen toiminta? Verkkoselaimella voidaan testata, latautuuko sivu. Sivun latautuessa palvelu toimii.

Entä jos sivu ei lataudu? Selain antaa virheviestin, mutta tarkempaa virhekuvausta ei saada. Palveluita testaamalla saadaan tarkka tieto siitä, miksi palvelu ei ole toiminnassa. Usein palveluiden toiminta on riippuvainen myös muiden palveluiden toiminnasta. Riippuvaisuuksia voi olla edellisen esimerkin tapauksessa muun muassa tietokanta- ja tiedostopalvelimiin.

Palveluiden seuraaminen ja kokonaisuuksien muodostaminen muuttuu helposti monimutkaiseksi ja vaikeaksi ainoastaan palveluita seuraamalla. Yleinen tavoitetilä verkonvalvonnan toteutuksissa, kuten myös tässä työssä, on ottaa käyttöön erillinen verkonvalvontajärjestelmä.

Verkonvalvontajärjestelmät suorittavat yhteyden- ja palveluiden testaamista, mutta tukevat näiden lisäksi myös useita eri verkonvalvontaprotokollia. Näistä standardin asema [5] on SNMP-protokollalla (Simple Network Management Protocol), joka tästä syystä on seuraavan luvun aiheena. Järjestelmät helpottavat valvontakokonaisuuden luomista, kun kaikki valvontatieto on keskitetysti yhdessä järjestelmässä. Edellisen esimerkin WWW-palvelin voidaan mallintaa järjestelmään, jolloin vikatilanteessa on suoraan nähtävissä vikaantunut komponentti, eikä sen etsimiseen tarvitse käyttää ylimääräistä aikaa. Järjestelmät voivat lähettää hälytyksen esimerkiksi tekstiviestillä tai sähköpostilla ja ne tekevät näin valvonnasta proaktiivisempaa.

2.4 SNMP-protokolla

SNMP on melko vanha, jo vuonna 1988 ensimmäisen kerran julkaistu IP-verkkojen valvontaprotokolla [6, s. 1]. Sen ensimmäinen versio on määritelty kaksi vuotta myöhemmin IETF:n (Internet Engineering Task Force) Request for Comments -muodossa, RFC:ssä

numero 1157 [5, s. 2]. Protokollasta on tehty kolme pääversiota, joista kaikki ovat edelleen yleisesti käytössä. SNMP:n yleisyys takaa sen, että sillä voidaan hallita valtaisa laitekirjoa.

2.4.1 Roolit

SNMP-järjestelmissä osallistuvilla laitteilla voi olla kaksi roolia: agentti (agent) tai manageri (manager) [5, s. 3]. Agentti on verrattavissa client-server -malliin palvelimeen (server), manageri asiakasohjelmaan (client).

SNMP-agentti on ohjelmisto, joka tarjoaa rajapinnan SNMP-protokollan ja hallittavan laitteen välillä. Sen avulla voidaan kysellä tietoja hallittavasta laitteesta. Se vastaa SNMP-managerin pyyntöihin mutta voi myös tietyissä tapauksissa toimia ilman niitä (Trap ja InformRequest) [7, s. 21-22]. Usein agentti on sisäänrakennettu hallittavan laitteen ohjelmistoon, tai on saatavilla erillisenä komponenttina [5, s. 3].

SNMP-manageri on tavallisesti laitteessa, jossa on ajossa verkonhallintaohjelmisto. Se lähettää pyyntöjä SNMP-agenteille ottaen vastaan agenttien lähettämät vastaukset. SNMP-managerin avulla verkonvalvontajärjestelmä täydentää tietoja hallittavien laitteiden tilasta. Tietoa voidaan myös kirjoittaa SNMP-agenteille. On mahdollista muuttaa esimerkiksi laitteen kuvaustietoja.

Trap

SNMP Trap voidaan asettaa SNMP-agenttiin. Sen avulla voidaan määrittää verkkolaitte lähettämään viestejä määrätyissä olosuhteissa ilman, että SNMP-manageri ottaa ensin yhteyden [7, s. 21].

2.4.2 MIB-tietokanta

SNMP-protokolla ei sisällä tietoa kaikista sillä hallittavista laitteista, koska protokollan jatkuva päivittäminen jatkuvasti ei ole mahdollista. Tiedot hallittavista laitteista eli hallintamääreet ovat MIB-tietokannoissa.

MIB (Management Information Base) on tietokanta, joka sisältää kaikki yleiset hallint ominaisuudet. Mallinsa se saa ASN.1:n alakategoriasta SMIV2 (Structure of Management Information Version 2) [8, s. 2]. Mallien lähempi tarkastelu ei sisälly työn laajuuteen.



Kuva 2. MIB-tietokantojen puukaaviorakenne [5, s. 24].

MIB-tietokannat muodostavat loogisen puukaaviorakenteen. Kuvassa 2 nähtävät laatikot ovat MIB-moduuleita, ja kuvan ellipsi on MIB-objekti. Moduulit ovat kuin luokkia: ne si-

sältävät luokalleen yhteiset hallintamääreet ja muodostavat hierarkkisen rakenteen. Objektit ovat yksittäisiä hallintamääreitä. Esimerkiksi kuvan sysDescr-objekti sisältää järjestelmäkuvauksen.

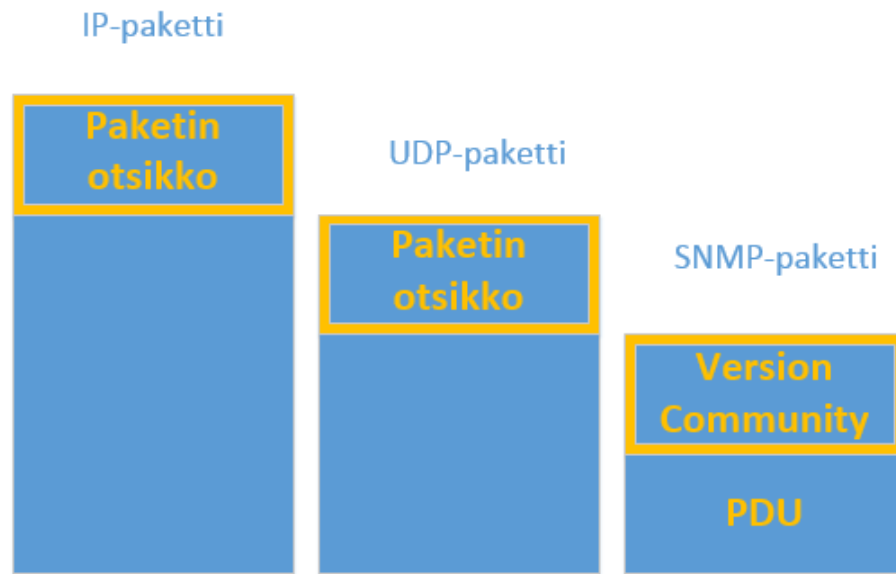
Erilaisia moduuleja on esimerkiksi eri laitetypyeille ja laitevalmistajille. Myös yksityinen yritys voi ehdottaa omaa moduuliaan tietokantaan.

Tietokantaan viitataan OID-tunnisteilla (object identifier). Tunniste muodostetaan seuraamalla polkua juuresta haluttuun puukaavion moduuliin tai objektiin. Esimerkiksi kuvan 3 Cisco-moduulin OID on 1.3.6.1.4.1.9. Verkonvalvontajärjestelmälle oleellisempi on kuitenkin tieto yksittäisistä objekteista. Esimerkiksi kuvan 3 sysDescr-objektin OID on 1.3.6.1.2.1.1.1. Sitä kutsumalla saadaan kohdejärjestelmän kuvaus.

2.4.3 SNMP-viestin muoto

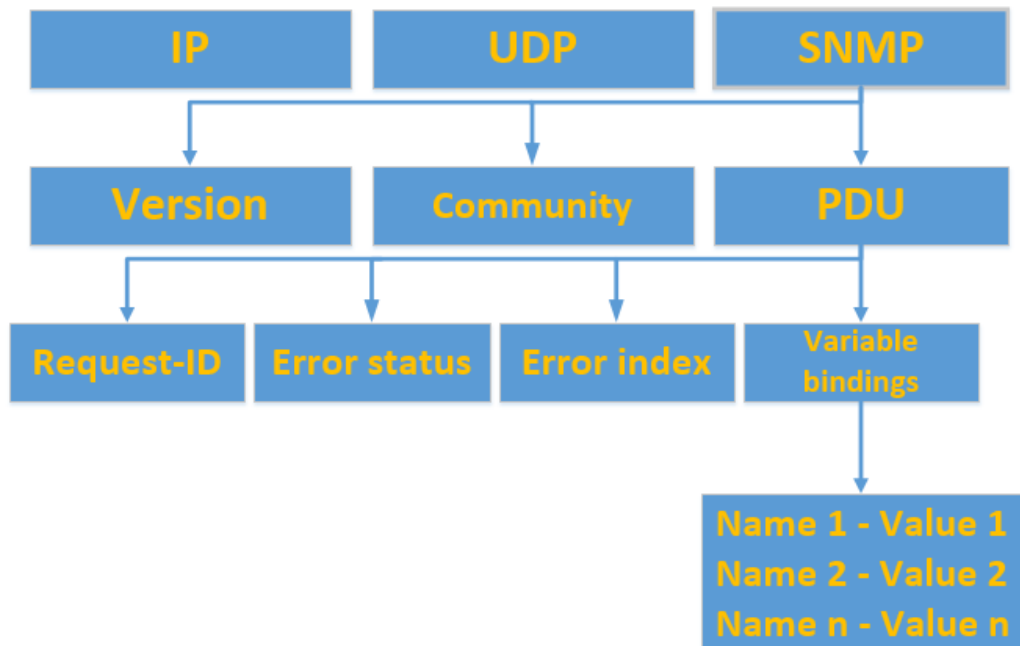
On tärkeää tarkastella protokollan toimintaa lähemmin, jotta edellä esitellyt kokonaisuudet voidaan asettaa käytännön asiayhteyteen. SNMP:n protokollapino sisältää SNMP:n lisäksi UDP:n ja IP:n (kuva 3) [5, s. 19].

Tarkastelussa on protokollan ensimmäinen versio. Se on protokollan versioista yksinkertaisin ja siksi myös helpoiten havainnollistettavissa.



Kuva 3. SNMP:n protokollapino [5, s. 19].

Mitä oikeastaan tapahtuu kun SNMP-manageri lähettää kyselyn SNMP-agentille? Muodostuu tavanomainen, monille verkkoprotokollille tyypillinen paketti, joka koostuu otsikosta (header) ja tietosisällöstä (PDU).



Kuva 4. SNMPv1-protokollan rakenne [9, s. 15].

Otsikkoa tarkastellessa tulee esille yksi SNMP:n todennusmenetelmistä, community-merkkijono. Se on yksinkertainen varmennusmenetelmä; sekä agentissa että managerissa on community-merkkijonon oltava sama, muutoin yhteys ei muodostu [9, s 8]. Toiminta on verrattavissa tavalliseen salasana-varmennukseen. Toinen otsikon kentistä on versio-kenttä, jossa määritellään, mitä protokollan versiota käytetään. Oletuksena community-merkkijono välitetään salaamattomana.

Viestin tietosisältö, PDU, sisältää haetun MIB-objektin sisällön (variable bindings) lisäksi kuvan 5 kentät Request-ID, Error Status ja Error Index. Näillä kentillä hallitaan virheitä: Request-ID sitoo kyselyn ja vastauksen yhteen, sillä muuten ei ole mahdollista varmistaa, mikä vastaus kuuluu millekin kyselylle. Error Status- ja Error Index -kenttien käyttö on riippuvainen PDU-tyypistä [9, s. 19–25].

2.4.4 SNMPv1-viestin PDU-tyypit

SNMP-protokollan ensimmäisessä versiossa on määritelty viisi erilaista PDU-tyyppiä.

- GetRequest PDU

- GetNextRequest PDU
- GetResponse PDU
- SetRequest PDU
- Trap PDU [9 s. 20–27].

GetRequest lukee MIB-objektin tiedot SNMP-agentilta. GetNextRequest tekee saman, mutta sen avulla voidaan hakea kokonaisten MIB-moduulien sisältävät tiedot [5, s. 43]. SetRequest-PDU on käytössä SNMP-agentin arvojen kirjoittamiseen. Näille PDU-tyypeille on yhteistä, että ne ovat ainoastaan SNMP-managerin käytössä.

GetResponse-PDU on SNMP-agentin lähettämä vastaus ja kuittaus. Trap-PDU on myös agentin lähettämä PDU, mutta poikkeuksellisesti agentti voi lähettää sen itsenäisesti, ilman SNMP-managerin yhteydenottoa.

Miten protokollan muut versiot eroavat ensimmäisestä? Protokollan 2c-versio toi näkyvimpänä ominaisuutenaan lisää PDU-tyyppejä tehokkaampaan tiedonhakuun (GetBulkRequest). Kolmas pääversio lisää protokollaan tärkeimpinä ominaisuuksinaan uusia todennusmenetelmiä ja salauksen.

2.5 Muut verkonvalvontaprotokollat

SNMP ei ole ainut laatuaan. Verkonvalvonnassa voidaan käyttää myös monia muita protokollia. Joukkoon kuuluvat sekä laitevalmistajien itse kehittämät että tiettyihin ympäristöihin erikoistuneet protokollat.

RMON

Remote Network Monitoring on, samaan tapaan kuten SNMP, IETF:n verkonvalvontaprotokolla. Toisin kuin SNMP, jonka valvonta keskittyy laitteisiin, RMON keskittyi alun perin lähes poikkeuksetta verkkoliikenteen valvontaan. Protokollan toiminnallisuutta on myöhemmin laajennettu [10, s. 2]. Toiminnaltaan RMON on osin verrattavissa SNMP:n Trap-toimintoon.

NetFlow

NewFlow on verkkolaittevalmistaja Ciscon verkonvalvontaprotokolla. Kuten RMON myös NetFlow on suunniteltu liikennepohjaiseen valvontaan.

Protokollasta on olemassa työn kirjoitushetkellä kymmenen versiota. Uusin versio, IP-FIX, on IETF:n standardi [11].

WMI

Windows Management Instrumentation rajoittuu nimensä mukaisesti Windows-ympäristöihin. Se mahdollistaa Windows-laitteiden hallinnan esimerkiksi skripteillä (PowerShell, VBScript) mahdollistaen verkonvalvonnan lisäksi myös järjestelmänhallinnan. WMI-käskyillä voidaan hallittavista järjestelmistä hakea sekä asettaa suuri määrä erilaisia arvoja kuten esimerkiksi tieto levyinkäytöstä [12].

Syslog

Syslog-protokollan avulla voidaan lähettää lokiin kirjautuneita tapahtumia eteenpäin, esimerkiksi hallintajärjestelmään tai erilliseen Syslog-palvelimeen. Syslog on vastikään määritelty IETF:n RFC:ssä 5424 [13]. Alun perin Syslog oli yksinomaan käytössä Sendmail-ohjelmassa. Sendmail on sähköpostinvälitysohjelma.

Verkonvalvontajärjestelmissä on tavallista määrittää SSH- sekä Telnet-protokollia valvontaan. Nämä protokollat eivät kuitenkaan ole verkonvalvontaprotokollia, vaan ne mahdollistavat etäkirjautumisen järjestelmiin. Kirjautumisen jälkeen järjestelmästä on mahdollista hakea tietoa suoraan komentoriviltä verkonvalvontajärjestelmän käyttöön.

Windows PowerShell, Microsoftin komentosarjakieli, on myös käyttökelpoinen yksinkertaisessa verkonvalvonnassa. Kielellä voidaan esimerkiksi määrittää yhteyksien tai palveluiden seuranta, jonka tuloksista julkaistaan HTML-pohjainen raportti suoraan verkkoon.

3 Verkonvalvonnan toteutus

Sopivan verkonvalvontajärjestelmän tulee kattaa yrityksen IT-toimintojen vaatimukset. Vaatimusten perusteella valittiin järjestelmiä koekäyttöön, jonka perusteella valittiin lopullinen järjestelmä.

3.1 Vaatimukset verkonvalvontajärjestelmälle

Verkonvalvontajärjestelmien yleisissä ominaisuuksissa painotettiin kattavaa tukea eri sensoreille sekä helppokäyttöistä hälytysjärjestelmää. Hälytysjärjestelmän on myös kyettävä lähettämään tekstiviestihälytyksiä.

Yleisissä ominaisuuksissa tärkeimmäksi nousi järjestelmän helppokäyttöisyys. On tärkeää, että ympäristön tila on helposti luettavissa järjestelmästä. Myös järjestelmän toiminnan tulee olla helposti ohjattavissa. Toiminnanohjaus tarkoittaa laitteiden määrittämistä valvontaan sekä esimerkiksi valvonnan keskeyttämistä väliaikaisesti. Helppokäyttöisyydellä tarkoitettiin lisäksi käyttöönoton helppoutta. Luonnollisesti kaikkeen liiketoimintaan sisältyy lisäksi vaatimus kustannustehokkuudesta.

Tekniset vaatimukset

Ympäristön erityispiirteet asettavat verkonvalvontajärjestelmälle tekniset vaatimukset, jotka valitun ratkaisun on täytettävä.

Valvonnan täytyy toimia sujuvasti myös yrityksen haarakonttoreissa, erityisesti Aasiassa. Valvonnan piiriin on liitettävä myös AWS:n (Amazon Web Services) pilvipalvelut, erityisesti EC2-instanssit (Amazon Elastic Compute Cloud) ja tarpeen mukaan myös Microsoft Online.

Verkkolaitteiden valvonnan on tuettava vähintään liikennemäärän lukemista sekä myös suorittimien ja muistin käyttöä.

Palvelimissa valvonnan on tuettava levytilan-, suorittimien- ja muistin käytön lukemista sekä Windows-palveluiden (services) tilan seuraamista.

Tulostimia ei haluttu valvonnan piiriin, sillä niiden toiminta on huoltosopimusten varassa. Huoltosopimuksen tarjoaja seuraa laitteiden tilaa automaattisesti. Tarvittaessa tulostinten toiminnasta voidaan ajaa raportteja.

Muiden laitteiden valvonnasta mainittiin erikseen UPS-laitteiden valvonta (akun tila, virransyöttö) sekä palvelinhuoneiden ympäristön valvonta (lämpötila ja ilmankosteus). Virtuaaliympäristöjen valvonnassa pitää olla tuettuina Microsoftin Hyper-V sekä VMwaren vSphere.

3.2 Verkonvalvonnan suunnittelu

Mitä ja miten verkossa halutaan valvoa? Tämä on verkonvalvontaa suunniteltaessa oleellinen kysymys, johon pyrin tässä luvussa vastaamaan toteutusympäristön suhteen.

Ympäristön monimutkaisuuden kasvaessa voi olla haastavaa määrittää tehokasta verkonvalvontaa. Palveluiden toiminnasta ei aina ole selkeää kuvaa. Jopa yksittäisten palvelimien rooli on saattaa olla hämärä. Miten voidaan päästä tehokkaaseen valvontaan saati laajempien palvelukokonaisuuksien määrittämiseen?

Ongelmaa voidaan lähestyä tuomalla verkon kaikki laitteet valvonnan piiriin. Tällöin verkonvalvontajärjestelmä rekisteröi jokaisen poikkeuksen, mutta voidaanko ongelma ratkaista näin? Ensimmäiseen ongelmaan törmätään heti valvontaa määriteltäessä. Mitä sensoreita yksittäisistä laitteista valvotaan? Tietoa voidaan hakea sadoista eri lähteistä. Sormien väsyessä kesken ensimmäisen laitteen määrittelyn otetaan asia uudelleen harkittavaksi. Määrittelyn rasittavuuden lisäksi rasite siirtyy myös verkkoon, sillä tiedon kerääminen sadoista sensoreista ei tapahdu ilman merkittävää kustannusta. Entä miten suuret resurssit vaaditaan tuhansien eri sensorien valvontaan? Tyypillisen IT-osaston resurssit tähän tuskin riittävät.

Toinen äärimmäinen lähestymistapa on määrittää valvontaa reaktiivisesti. Laitteita lisätään valvonnan piiriin vasta ongelmien ilmaantuessa. Tyyli on kenties toimiva, mutta eikö se riko verkonvalvonnan perusajatusta ongelmien havaitsemisesta ennen muita? Potentiaalisten ongelmien havaitsemisesta on turha puhua. Ympäristön kokonaiskuva jää hajanaiseksi ja sen ylläpito muuttuu hankalaksi.

Ratkaisu on varmasti löydettävissä näiden äärimmäisyyksien väliltä. Oma ratkaisuni perustuu osin ketterän kehityksen malleihin, osin muodolliseen palvelutasosopimukseen. Palvelutasosopimus määrittelee valvonnan suuret linjat: mille palveluille on taattava riittävä toiminnan taso? Eri palvelut rikotaan komponentteihin ja mallinnetaan verkonvalvontajärjestelmään. Ketterän kehityksen periaatteista [14] on apua ajatusmallina, joista tärkeimpiä ovat jatkuva muutokseen reagointi ja toimivan mallin luominen jo tekemisen varhaisessa vaiheessa.

Käytännössä toteutus tehdään aluksi mallintaen palvelut olemassa olevan dokumentaation ja muun tiedon perusteella. Mahdollisuuksien mukaan voidaan harkita autodiscovery ominaisuuksia (laitteiden automaattinen löytäminen) verkonvalvontasovelluksesta. Ympäristön yksittäisten laitteiden lisäämisen jälkeen voidaan niistä muodostaa palveluita ja muuta logiikkaa palvelutasosopimuksen perusteella. Toimivan verkonvalvonnan lisäksi saadaan ohessa dokumentaatio ajan tasalle sekä mahdollistetaan palvelutasosopimuksen seuraaminen.

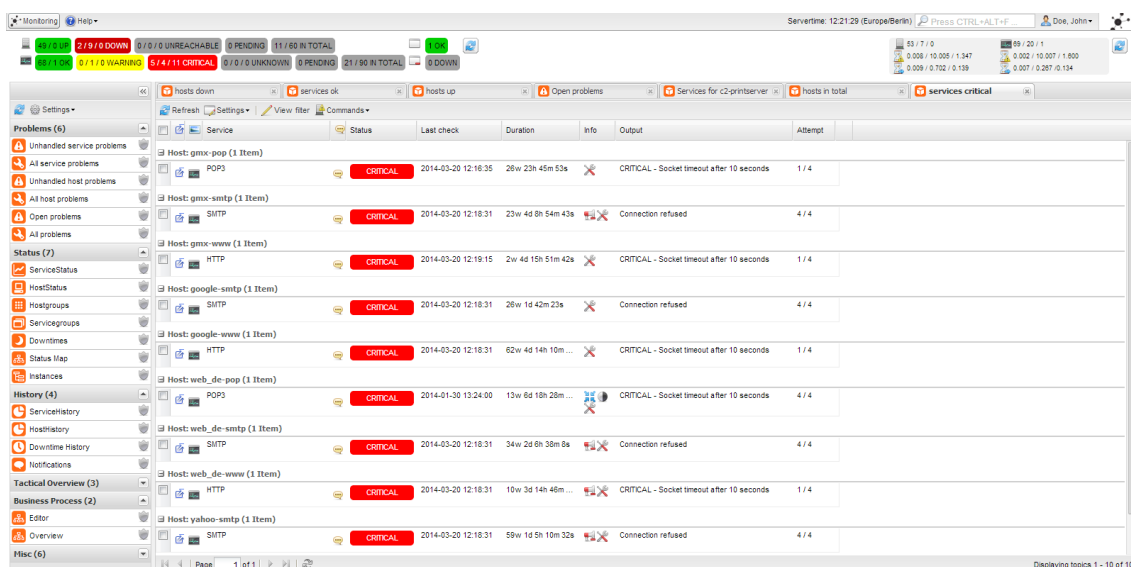
3.3 Verkonvalvontajärjestelmien vertailu

Lopulliseen koekäyttöön valikoitui kaksi verkonvalvontajärjestelmää. Lukuisia vaatimukset täyttäviä järjestelmiä arvioitiin, mutta koekäyttöön otettiin kaksi parasta ehdokasta.

3.3.1 Icinga

Icinga on avoimen lähdekoodin verkonvalvontajärjestelmä, joka perustuu tunnetumpaan Nagiokseen.

Asennus suoritettiin asennusohjeiden mukaisesti [15] virtuaaliympäristöön. Koekäyttöön otettiin versio 1.8.3. Helpompi tapa olisi ollut valmiin, Icingan kehitystiimin luoman virtuaalikoneen käyttäminen. Koekäytön aikaan valmiin virtuaalikoneen versio ei kuitenkaan ollut ajan tasalla.



Kuva 5. Icingan kotinäky (versio 1.11.0).

Kuvassa 5 on hallintänäkymän yleisasu. Ylhäällä vasemmalla on listattu valvottavien palveluiden ja sensorien tilat (esimerkiksi onko sensorin tila hyvä, onko se käyttämättömissä vai varoitusrajan alla). Ylhäällä oikealla on tietoja ympäristöstä: tiedot ajasta ja käyttäjästä sekä muun muassa tietoja palveluiden ja palvelimien määrästä. Palkki käyttöliittymän vasemmassa reunassa toimii kuten verkkoselaimista tunnettu suosikit-palkki. Siihen voi lisätä esimerkiksi eniten käytetyt valvontänäkymät. Loput näkymästä on varattu näytettävälle sivulle tai sivuille, jotka myös verkkoselaimista tuttuun tapaan näytetään eri välilehdillä.

Järjestelmä täytti lähes kaikki asetetut vaatimukset. Helppokäyttöisyysvaatimus täyttyi käyttöliittymän suhteen, mutta laitteiden lisääminen järjestelmään koettiin vaivalloiseksi. Kustannustehokkuudessa järjestelmä sai erityismaininnan, joskin epäilyjä heräsi järjestelmän konfiguroinnin vaatiman ajan sisäisistä kustannuksista.

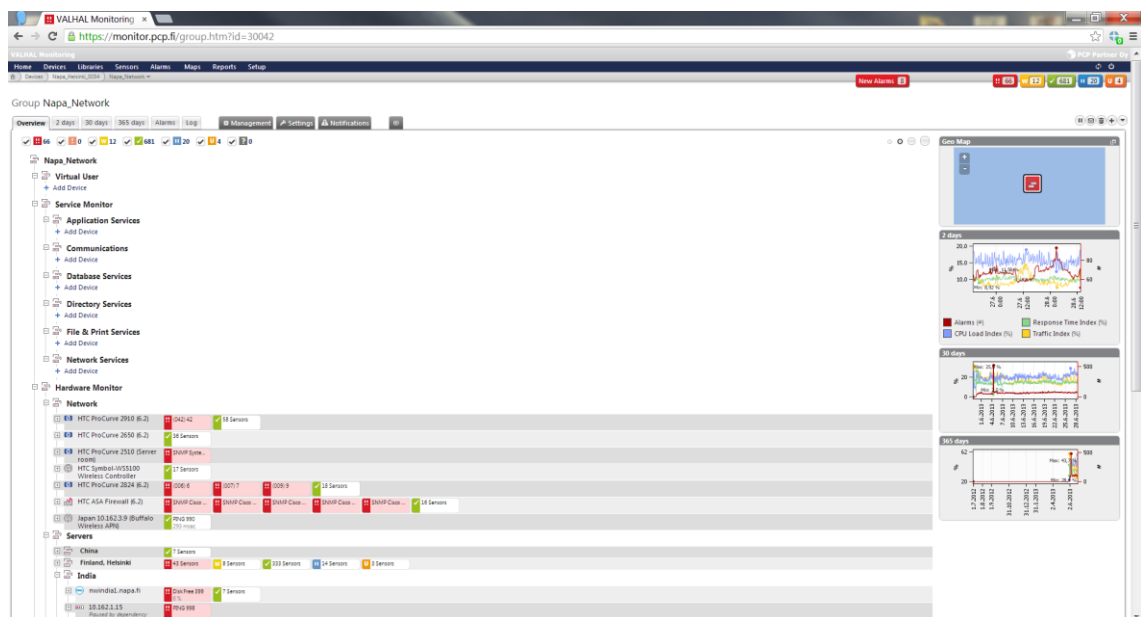
3.3.2 Valhal

Valhal (PCP ValHal) on PCP Partner Oy:n verkonvalvontapalvelu, jonka pohjana on Paessler PRTG. Palvelu toimii julkisessa verkossa. Asiakkaan tiloissa sijaitsee vain osa valvontainfrastruktuurista. Palvelu tilattiin testikäyttöön. Perusmäärittelyksistä vastasi palvelun toimittaja.

Valvonta luokitellaan neljään kerrokseen [16]: hardware monitor, service monitor, business logic ja virtual user.

Hardware monitor -kerrokseen sisältyy yksittäisten laitteiden tilan valvonta. Tyypillisesti valvotaan esimerkiksi verkkolaitteiden porttien tilaa ja levytilan käyttöä. Service monitor -kerros sisältää tiedot palveluiden tilasta. Esimerkiksi WWW-palvelimen http-palvelun tilaa voidaan valvoa. Business logic -kerroksen sisään voidaan määrittää liiketoiminnalle tärkeitä valvontamääreitä, jotta virheet liiketoimintaketjussa voidaan havaita.

Virtual user -kerros tarkoittaa verkon käytettävyyden testaamista virtuaalikäyttäjällä. Virtuaalikäyttäjä voidaan asettaa käymään läpi määritelty prosessi (esimerkiksi tiedon tallentaminen CRM-järjestelmään) ja tallentaa näin tietoja ympäristön käytettävyydestä suoraan yksittäisen testikäyttäjän näkökulmasta.



Kuva 6. Valhal:n kotinäky.

Kuvassa 6 on ValHal:n kotinäky. Oikealla ylhäällä näkyy valvottavien kohteiden tilat, joiden alla on Geo Map -kartta ympäristön maantieteellisestä sijainnista. Sen alla ovat taulukot ympäristön historiasta (ympäristön virheet, suoritinkäyttö, vasteaika- ja liikenneindeksit ajan suhteen). Muut osat käyttöliittymästä on pitkälti varattu valvottaville kohteille. Sivun keskellä ne nähdään ryhmiteltyinä. Käyttöliittymän yläosan valikosta kaikki toiminnot ovat saatavilla. Valikosta voidaan esimerkiksi ajaa raportteja ja näyttää loogisia kartoja ympäristöstä.

Järjestelmä täytti pitkälti kaikki vaatimukset. Järjestelmän toiminta palveluna herätti keskustelua. Haittapuolena pidettiin sitä, ettei järjestelmän kaikkia määrittäksiä voida tehdä itse. Hyvä puoli oli palvelun ylläpidossa: ostettua palvelua ei tarvitse itse ylläpitää tai päivittää. Hätätilanteessa palvelu on hyödyllinen: tietoja verkon tilasta saadaan myös katastrofin yllättäessä. Vaikkei tieto pahimmassa tapauksessa enää päivittyisikään, nähdään hätätilanteeseen johtanut tilannehistoria.

Vaatus palvelun helppokäyttöisyydestä toteutui. Vaadittuja laitteita pystyttiin valvomaan onnistuneesti. Suurimmaksi ongelmaksi jäi kehittyneimpien ominaisuuksien määrittely (kartat, raportit, virtuaalikäyttäjät, business logic) itse, eikä määrittelystä suoriutunut ilman apua.

3.4 Vertailun tulos

Toteutuksen järjestelmäksi valittiin PCP:n ValHal. Vertailun pääkriteeri, palvelun helppokäyttöisyys, toteutui parhaiten valitussa ratkaisussa (erityisestä lisätessä laitteita valvontaa).

Vertailun lopuksi päädyttiin myös siihen, että järjestelmä on parempi hankkia palveluna. Palveluna järjestelmän tekninen toiminta ei ole IT-toimintojen vastuulla. Voidaan luottaa siihen, että järjestelmä on sopimusehtojen mukaisesti käytettävissä. Päivitykset ovat myös toimittajan kontolla: niitä voidaan odottaa säännöllisiä. Päivitysten yhteensopivuutta ei tarvitse testata sisäisesti.

3.5 Verkonvalvontajärjestelmän käyttöönotto

Mittavin järjestelmän käyttöönottoa edeltävä tekninen toimenpide oli SNMP community-merkkijonon valitseminen ja määrittely kaikkiin SNMP:llä valvottaviin laitteisiin. Samalla valittiin käyttöön SNMP:n versio 2c. Kolmannen version parannetuille todennusominaisuuksille eikä salaukselle nähty tarvetta, sillä hallinta-aseman ja valvottavien laitteiden välinen liikenne kulkee suojatussa sisäverkossa. Ei myöskään ollut täyttä varmuutta, että kaikki valvottavat laitteet sisältäisivät tuen protokollan kolmannelle versiolle. Valvottavien laitteiden SNMP-agenttiin ei myöskään asetettu kirjoitustilaa päälle. Se tarkoittaa, että laitteista on mahdollista ainoastaan lukea tietoa.

Toinen valmistava tekninen toimenpide oli verkkoyhteyksien määrittely. Käyttöön otettiin osin myös valvontajärjestelmää varten erillinen hallintaverkko. Tämän lisäksi määritettiin palomuriin porttiavaukset ja NAT-säännöt (Network Address Translation) hallinta-asemalle, sillä sisäverkossa oleva hallinta-asema keskustelee julkisessa verkossa olevaan verkonvalvontapalveluun kanssa. Samalla hallinta-asema asennettiin yrityksen palvelinhuoneeseen.

Palvelu käyttöönotto tapahtui suunnitelman mukaisesti: valvontaan lisättiin olemassa olevan dokumentaation mukaiset laitteet ja palvelut. Myöhemmin, palvelutasokyselyiden edetessä, päivitettiin dokumentaatio niiden pohjalta. Autodiscovery (verkon laitteiden löytäminen ja lisääminen automaattisesti valvontajärjestelmään) suoritettiin, sillä dokumentaatio ei ollut täysin ajantasainen.

Hälytykset ja sensorit

Hälytykset määriteltiin sensorien tilan mukaan. Järjestelmä hälyttää ainoastaan sensorien olleessa poissa toiminnasta (down) poissa toiminnasta -tilaan sisältyy myös virhetila. Hälytyksenä voi lähteä myös tekstiviesti sähköpostin lisäksi riippuen valvottavan laitteen sensorin kriittisyydestä. Sensoreilla on lisäksi myös muita tiloja, näistä olennaisimpina

- varoitus (warning)
- epätavallinen (unusual)
- tuntematon (unknown)
- pysäytetty (paused).

Kuvassa 7 sensorit ovat järjestyksessä vasemmalta oikealle: poissa toiminnasta, poissa toiminnasta (tiedostettu), varoitus, normaali (ylhäällä), pysäytetty, epätavallinen ja tuntematon.



Kuva 7. Sensorien tilat.

Varoitus tapahtuu sensorin ylittäessä varoitusrajan mutta kuitenkin ennen sensorin poissa toiminnasta -tilaa. Epätavallinen-tila on hyödyllinen ongelmien ennaltaehkäisyssä. Voi esimerkiksi ilmetä, että verkkolaitteen tietyn portin liikennemäärä on epätavallisen alhainen. Tämän avulla on mahdollista löytää epätavallisen tilanteen aiheuttaja, ennen kuin tilanteesta muodostuu varsinainen ongelma. Sensorien pysäytys on tarpeellista muutoksien ja huoltokatkojen ajaksi. Pysäytetty sensori ei lähetä hälytyksiä. Ellei sensoriin saada yhteyttä, sen tila muuttuu tuntemattomaksi.

Näkymät

Vertailussa (luku 3.3.2) jo esitellyn kotinäkymän lisäksi voidaan järjestelmään lisäksi määritellä dashboard-näkymiä. Dashboardeihin voidaan määritellä valittuja osia järjestelmästä, esimerkiksi tietty näkymä sensoreista ja lokitiedosta. Palvelu on käytettävissä myös mobiilikäyttöliittymällä.

Sen lisäksi, että sensorit voidaan näyttää luokissa ja dashboard-näkymissä, niiden seuraaminen onnistuu lisäksi kartoista (maps) ja erillisistä sensorinäkymistä. Karttoja ei toteutukseen vielä määritelty, mutta erilliset sensorinäkymät ovat käytössä. Erillisiä sensorinäkymiä on kaksi: Tree Map ja Sunburst. Tree Map esittää valvonnan kohteet ruudukkona, jossa yhden ruudun koon määrittelee sen prioriteetti ja värin sen sisältämien sensorien tilat.



Kuva 8. Sunburst-näkymä.

Sunburst-näkymä (kuvassa 8) antaa hyvän yleiskatsauksen sensorien tilasta: siitä on nopeasti hahmotettavissa vikaantuneet laitteet sekä niiden riippuvuudet. Värit kuvastavat edellä esitettyjen sensorien värejä. Näkymästä huomataan myös eri tasot, joiden mukaan verkonvalvonta on määritelty. Hardware Monitor -luokan alla on yksittäisiä laitteita, kun taas Service Monitor -luokka sisältää lukuisia näistä koostuvia palveluita.

3.6 Verkonvalvontajärjestelmän testaus ja ongelmatilanteet

Järjestelmän lopullinen testaus tehtiin koekäytön aikana. Verkonvalvontajärjestelmä ei vaadi perusteellista testaamista, sillä sen toiminta on jatkuvassa muutoksessa. Verkonvalvontajärjestelmän toiminta on yhtä muuttuvaa kuin sen valvonnan kohteena olevat järjestelmät ja verkot. Nähtiin myös hyvin epätodennäköisenä, että verkonvalvontajärjestelmä voisi aiheuttaa ongelmia oman toimintansa ulkopuolella.

Ensimmäiseen ongelmaan törmättiin yrityksen Helsingin toimipisteen palomuurin NAT-määrittelyssä. Hallinta-asema ei saanut yhteyttä verkonvalvontapalveluun. Ongelma korjattiin määrittelemällä NAT-säännöt toisin. Muita ongelmia toteutuksessa aiheuttivat lähinnä yksittäisten sensorien ongelmatilanteet. Sensoriongelmien syynä olivat tavallisesti verkko-ongelmat tai ongelmat valvottavien laitteiden määrittelyssä. Osin oli myös tarpeen poistaa ja lisätä sensoreita uudelleen valvottaviin laitteisiin verkonvalvontajärjestelmän hallinnasta. Mikään toteutuksen ongelmista ei jäänyt ratkaisematta.

4 Palvelutasosopimus

Palvelutasosopimus (SLA) on palvelun tarjoajan ja käyttäjän välinen sopimus. Tyypillinen palvelutasosopimus määrittelee palvelun saatavuudelle vähimmäisajan mutta sisältäen usein myös muita määreitä. Sopimus ei ole muodoltaan määräinen, vaan se on täysin osapuolten määriteltävissä paikallisen lainsäädännön puitteissa. Sopimuksen perusteella osapuolten vastuiden tulisi olla selkeät [17, s. 157].

Keskeisiä käsitteitä sopimuksessa ovat luvattu palvelutaso sekä sanktiot sen rikkomisesta. Palvelutason tyypillinen mittari on saatavuus. Saatavuuskriteeri toteutuu, kun palvelu on käytettävissä sovituin ehdoin. Kun palvelu ei ole käytettävissä, on tapahtunut poikkeus [17, s. 74]. Esimerkiksi voidaan sopia internet-liittymästä nopeuden ehdoin: nopeuden laskiessa alle asetetun rajan ei palvelun katsota olevan saatavilla.

Palvelutasosopimuksen toteutumista seurataan valitulla verkonvalvontajärjestelmällä. Verkonvalvontajärjestelmään voidaan määrittää kaikki palvelutasosopimuksen piirissä olevat palvelut.

4.1 Saatavuus

Palvelun saatavuus mitataan usein prosenteissa. Sata prosenttia tarkoittaa palvelun olevan aina saatavilla. Tämä taso tosin on varsin teoreettinen, koska tyypilliset tietojärjestelmät ovat monimutkaisia ja ne koostuvat lukuisista komponenteista. Jos oletetaan, että kaikki komponentit sisältävät hajoamisriskin, on erityisen vaikea määritellä aina saatavilla olevaa järjestelmää.

Komponenttien saatavuuden mittaamisessa käytetyt luvut ovat MTTR (mean time to repair) ja MTBF (mean time between failure). MTTR sisältää keskimääräisen ajan, joka laitteen korjaamiseen kuluu, kun taas MTBF keskimääräisen ajan, jonka kuluessa ehjä laite vikaantuu. Saatavuuden yksinkertainen laskukaava on $MTBF / (MTBF + MTTR)$. Pelkän MTBF-arvon määrittely on usein monimutkaista. Vaikeus lisääntyy, kun saatavuuksia lasketaan laajemmille, useista laitteista koostuville järjestelmille. MTBF onkin lähes poikkeuksetta laitevalmistajan määrittelemä.

Komponenttien saatavuuden mittaaminen niiden ollessa sarjaan kytkettyinä on yksinkertaista: järjestelmän komponenttien saatavuus kerrotaan keskenään. Esimerkiksi jos järjestelmä koostuu kuudesta 99,9 %:n saatavuuden omaavasta komponentista, on sen saatavuus $0,999^6$. Rinnan kytketyillä komponenteilla sama kaava on $1 - (1 - 0,999)^6$, jossa 0,999 on 99,9 %:n saatavuus. Voidaan todeta, että yksinkertainen, rinnan kytketystä komponenteista koostuva järjestelmä on luotettavampi [18].

Monimutkaisissa järjestelmissä määrittelyä ei voida tehdä näin yksinkertaisesti. Komponentit voivat muodostaa kokonaisuuksia, jotka ovat samanaikaisesti sekä rinnan että sarjaan kytkettyjä. Edellisessä esimerkissä oletettiin rinnan kytketyn järjestelmän vaativan vain yhden komponentin toimiakseen. Entä jos toimintaan vaaditaankin kolme komponenttia?

Saatavuuteen liitetään usein, erityisesti reaaliaikaviestinnässä, yhteyden laadulliset ominaisuudet. Laadullisista ominaisuuksista tärkeimpiä ovat viive, siirtonopeus, jitter sekä siirtovirheet [19, s. 89–91]. Voidaan löytää useita esimerkkejä palveluista, joiden ei voida katsoa olevan saatavilla pelkästään palvelun ollessa tavoitettavissa. Tämänkaltaisia palveluita ovat esimerkiksi kaikki reaaliaikaiset puhe- ja videoviestintäpalvelut. Näiden palveluiden käyttö esimerkiksi sekunnin viiveellä on turhauttavaa. Keskustelijoiden puheenvuorojen ajoittaminen hankaloituu tai muuttuu mahdottomaksi. Palvelutasosopimuksessa voidaan erikseen määrittää rajat yhteyden laadullisille ominaisuuksille.

4.2 Palveluaika

Asetettu palveluaika määritellään usein SLA:n yhteydessä. Tyypillinen palveluaika voi olla esimerkiksi 8/5 (kahdeksan tuntia päivässä, viitenä päivänä viikossa) tai 24/7. Palvelutason mittaus tapahtuu vain palveluaikana. Palveluajan lisäksi voidaan määrittää aika, jolloin palvelun käyttäjätuki on saatavilla [20, s. 155].

On huomioitava myös palvelun saatavuuden palauttamisessa vaadittavat eri työn vaiheet. Vaiheet jaetaan usein havainto-, vaste-, korjaus- ja palautumisaikaan. Vaste-, korjaus- ja palautumisaika muodostavat ratkaisuaajan. Usein SLA:ssa määritellään vain vasteaika, mutta myös ratkaisuaika voidaan määrittää.

4.3 Palvelujärjestys

Palvelujärjestys tarkoittaa järjestystä, jossa palvelutasosopimuksessa määriteltyjen komponenttien vikaantumiset hoidetaan. Palvelujärjestys on oleellinen, mikäli palvelutasosopimus sisältää useita palveluita.

Käytännössä kyse on usein prioriteeteista, eri palveluille määritellyistä luokista kriittisyyden perusteella. Kriittisyyteen voivat vaikuttaa muun muassa vian laajuus ja vakavuus. Eri palveluiden tasot voidaan näin määrittää lisäksi asetettujen virheluokkien perusteella.

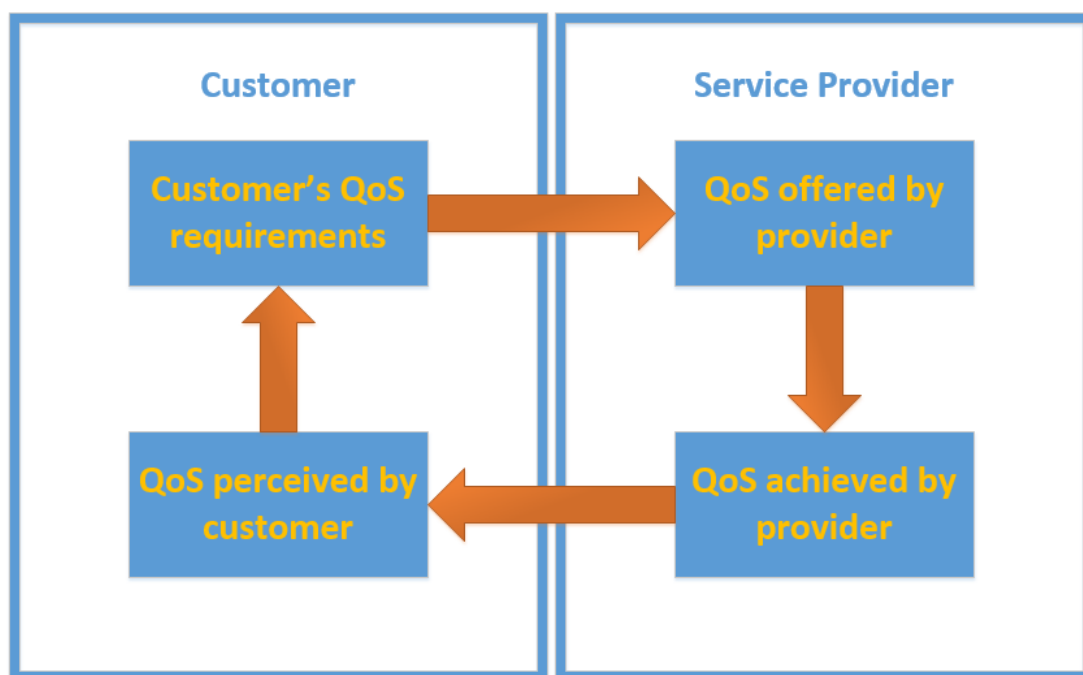
4.4 Quality of Service

Tavallisesti QoS (Quality of Service) on käytössä teknisenä käsitteenä verkkoliikenteen priorisoinnissa eri luokkien perusteella. Tavallinen toteutus on asettaa esimerkiksi reaaliaikaviestinnän liikenteelle muuta verkkoliikennettä korkeampi prioriteetti.

ITU:n standardi E.800 [21] määrittää QoS:lle hyödyllisiä yleisesti palvelunlaatua koskevia kuvauksia. Tärkeimpiä näistä ovat palvelunlaadun kuvaus päästä päähän ja palvelunlaadun näkökulmat.

Standardi kuvaa laadun komponentit päästä päähän käyttämällä neljää komponenttia: käyttäjää, terminaalilaitetta, jakeluverkkoa ja runkoverkkoa. Käyttäjä on yhteydessä terminaalilaitteella jakeluverkkoon ollen yhteydessä runkoverkon kautta toiseen samaan tapaan runkoverkkoon yhteydessä olevaan käyttäjään. Nämä komponentit ovat tavallisia lankapuhelinverkoille, mutta ne ovat myös tunnistettavissa IP-pohjaisessa liikenteessä (erityisesti reaaliaikaviestinnässä). Komponenttien erottelu korkealla tasolla on tärkeää, jotta laatuun voidaan kiinnittää huomioita järjestelmän kaikissa eri osissa.

E.800:ssa palvelunlaadulla on neljä eri näkökulmaa: asiakkaan havaitsema palvelunlaatu (QoS perceived by customer), asiakkaan vaatimukset palvelunlaadulle (Customer's QoS requirements), toimittajan tarjoaman palvelunlaadun taso (QoS offered by provider) ja palvelutaso, jonka toimittaja on saavuttanut (QoS achieved by provider).



Kuva 9. Palvelunlaadun eri näkökulmat [21].

Näkökulmien välinen yhteys muodostuu asiakkaan vaatimusten vaikuttaessa toimittajan tarjoamaan palvelunlaatuun. Toimittajan tarjoamalla palvelunlaadulla on luonnollisesti vaikutusta toimittajan saavuttamaan palvelutasoon, sillä lupaukset asiakasta kohtaan pyritään tavallisesti täyttämään. Asiakas tulkitsee toimittajan saavuttaman palvelutason omien kriteereidensä pohjalta: vaikutusketju alkaa lähtöpisteestään (kuten kuvassa 9).

Kun yritetään saavuttaa sovittua palvelutasoa, voidaan tarjontaa tarkastella eri näkökulmista ja samalla pyrkiä ottamaan selville, missä kohdassa ketjun toiminta katkeaa. Asiakkaan vaatimukset voivat esimerkiksi olla ristiriidassa toimittajan tarjoaman palvelunlaadun kanssa. Tässä tilanteessa on toimittajan joko nostettava palvelunlaatua tai asiakkaan laskettava vaatimuksiaan.

5 Palvelutasosopimuksen määrittäminen

Palvelutasosopimuksen ensisijainen tarkoitus on selkeyttää yrityksen IT-toimintojen roolia palveluntarjoajana. Tarkoituksena oli myös kartoittaa yrityksen sisäisiä palveluita ja niiden riippuvuuksia sekä sopia muodollisesti niiden toimintavaatimuksista.

Palvelutasosopimuksen vaatimukset

Vaatimukset täyttävä ratkaisu on palvelutasosopimusehdotus. Sen on täytettävä määrätty laajuus ja siitä tulee olla sovittu organisaation määrättyjen ryhmien edustajien kanssa.

5.1 Palvelutasosopimuksen määrittämissuunnitelma

Tiedot palvelutasosopimuksen määrittämiseksi hankittiin haastatteluilla, joihin sisältyy täytettävä matriisi (liite 1) sekä joukko avoimia kysymyksiä palvelutasosopimukseen liittyen. Kyselyn pääosa, matriisi, suunniteltiin täytettäväksi yhdessä haastattelijan kanssa. Kyselyn pääosa muistuttaa tyypiltään strukturoitua haastattelua. Vastausvaihtoehdot ovat kuitenkin ennalta määräämättömiä, joten kyse on puolistrukturoidusta haastattelusta [22, s. 86]. Kyselyn haastatteluosuus on tyypiltään teemahaastattelu. Yksittäiseen kyselyyn varattiin kolme tuntia aikaa ja haastatteluita tehtiin työn aikana kahdeksan.

Matriisi on jaettu kahteen osaan, joista toinen käsittelee yleisiä (common) palveluita ja toinen (haastateltavan) liiketoiminnalle erityisiä (business specific) palveluita. Sarakkeiden tiedot vasemmalta oikealle:

- Service on yksittäinen tunnistettu palvelu, esimerkiksi sähköposti.
- Category on palvelun luokka, esimerkiksi viestintä.

- Why on syy palvelun käytölle, esimerkiksi syy sähköpostin käytölle voi olla viestintä.
- Dependencies määrittää riippuvuudet muista palveluista. Palvelut voivat olla sidoksissa toisiinsa.
- Where on palvelun ajoympäristö, esimerkiksi tietty palvelin tai SaaS (software as a service).
- SLA priority on subjektiivinen prioriteetti palvelulle. Riippuen tunnistettujen palveluiden määrästä se on joko arvojärjestys tai arvojärjestys ryhmittäin. Suurin mahdollinen prioriteettiarvo on 1. Arvojärjestys voidaan mieltää esimerkiksi järjestyksenä, jossa palvelut käynnistetään kaikkien palveluiden ollessa poissa käytöstä.
- Availability on palveluaika (katso luku 3.3).
- Quality costs määrittää laatukustannukset, esimerkiksi hinnan menetetyistä työtunneista.
- Risk type for business on erityinen riski, joka aiheutuu palvelukatkosta, esimerkiksi imagohaitat.
- Risk severity on edellisen riskin vakavuus, joka ottaa huomioon sekä todennäköisyyden että vaikutuksen. Riski arvioidaan asteikolla 1–5, jossa suurin arvo on 5. Riskiin vaikuttavat sekä riskin todennäköisyys että sen vakavuus.

5.2 Kyselyn toteutus

Osallistujat kutsuttiin kyselyyn saatekirjeellä, jossa selitettiin lyhyesti kyselyn tavoitteet ja palvelutasosopimuksen yleiset käsitteet. Osallistujat pyrittiin valitsemaan tasaisesti organisaation eri ryhmistä, jotta käytössä olevista palveluista voitiin muodostaa kokonaisvaltainen kuva.

Kyselyn pääosa täytettiin sarakkeittain vasemmalta oikealle yhdessä haastateltavan kanssa. Aluksi kirjattiin ja eriteltiin käytössä olevat IT-palvelut palvelu-sarakkeeseen. Palveluiden erottelun jälkeen määriteltiin niille arvot kyselyn muiden kohtien mukaisesti. Yksi kyselyn tärkeimmistä tavoitteista oli saada tietoon käytössä olevat palvelut. Käytössä olevien palveluiden selvittäminen on yleinen edellytys kattavalle palvelutasosopimukselle [20, s. 47].

Yleisille palveluille ei määritelty kaikkia sarakkeita vaan ainoastaan palveluaika, prioriteetti ja laatukustannukset. Yleiset palvelut ovat kaikkien käytössä, joten myös kyselyn muiden sarakkeiden tulisi olla kaikille yhtenäisiä.

Haastattelija kirjasi kyselyä tukevien avointen kysymysten vastaukset. Avointen kysymysten rooli ei pelkästään ole palvelutasosopimuksen tarkka määrittely. Tarkoituksena on myös yhteisymmärryksen parantaminen, pidemmän tähtäimen toiminnan suunnittelu ja avoin palautekysely.

5.3 Kyselyn eri näkökulmat

Tiedon keräämisen yhteydessä on oleellista ottaa huomioon luvussa 4.4 esitetyt neljä palvelunlaadun näkökulmaa. Kyselyssä otetaan kantaa vaatimuksiin, joten vielä ei voida tarkastella saavutettua tai havainnoitua palvelutasoa. Toki myös nykyisen ympäristön palveluiden laatu vaikuttaa vaatimuksiin palvelutasosta.

Palveluntarjoajan eli yrityksen IT-toimintojen näkökulmasta kaikkia vaatimuksia voidaan tuskin toteuttaa ilman rajattomia resursseja. On määritettävä tarkasti palvelutaso, joka voidaan luvata käytössä olevilla resursseilla, sekä myös laskettava lisätyn palvelutason hinta. Ilman tarkkaa määrittelyä palvelutasoa ei voida varmistaa. Tämä näkökulma on aikaisemmin esitelty toimittajan tarjoamana palvelutasona.

Asiakkaan vaatimukset täytyy peilata toimittajan tarjoamaan palvelutasoon. Tarkan läpikäynnin jälkeen eritellään palveluista yksittäiset komponentit ja ehdotetaan palveluille parasta toteutettavissa olevaa palvelutasoa. Mikäli toteutettavissa oleva palvelutaso on riittämätön, esitetään arvio korotetun palvelutason kustannuksista.

Kriittiset palvelut vaativat erityisen tarkkaa läpikäyntiä. Mitkä ovat kriittisten palveluiden riippuvuudet? Kuinka laajaan käyttäjäjoukkoon kriittisen palvelun toimimattomuus vaikuttaa? Mistä syystä palvelu on kriittinen? Estääkö sen toimimattomuus työnteon vai onko sillä muita haittavaikutuksia?

Erityisen tarkka läpikäynti on tarpeen kahdesta syystä. Mikäli kriittisen palvelun toimintaa ei taata, voi sen toimimattomuudesta aiheutua vakavia haittavaikutuksia. Kaikkia palveluita ei kuitenkaan voida määritellä kriittisiksi: kriittisen palvelun toiminnan takaaminen voi vaatia huomattavasti resursseja.

Tarkastelussa voi myös esimerkiksi selvittää, että kriittinen palvelu on jo valmiiksi muulla tapaa varmennettu: käyttäjille lähetetyt sähköpostit eivät katoa pelkän sähköpostipalvelimen ollessa poissa toiminnasta vaan jäävät siitä huolimatta palvelujonoon.

5.4 Kyselyjen tulokset

Kyselyn tuloksien yksityiskohtainen tarkastelu työssä ei ole tarkoituksenmukaista eikä suotavaa yrityksen kannalta. Lisäksi syy siihen, ettei kaikkia yksittäisiä palveluita voida tuloksissa listata, on palveluiden suuri määrä ja vaihtuvuus. Kokonaiskuva katoaa nopeasti yksittäisiä palveluita listatessa, eikä se säily ajankohtaisena kovinkaan kauaa.

Kyselyn avoimien kysymyksien tuloksia ei käsitellä lainkaan. Olen muodostanut kyselyistä yksinkertaistetut koontitulokset (taulukko 1), jotka esittelen seuraavaksi. Yksittäisiä palveluita ei siis ole esitelty, vaan kaikki tulokset on yleistetty luokkiin:

- Development sisältää kaikki tuotekehityksen palvelut ja työkalut.
- Testing sisältää kaikki testaukset palvelut ja työkalut.
- Communications sisältää viestinnän palvelut.
- Support sisältää IT-toimintojen tarjoaman käyttäjätuen eri osa-alueet.
- CRM sisältää poikkeuksellisesti pelkän CRM-järjestelmän.
- Product sisältää yrityksen tuotteisiin liittyvät palvelut.
- License services tarkoittaa lisenssipalveluita.
- Financial software sisältää talousohjelmistot.
- Management sisältää työnhallintaohjelmistot, joihin sisältyy tuntiraportointi ja projektinhallinta.
- Company website sisältää toisena poikkeuksena ainoastaan yrityksen WWW-sivut.
- Document management sisältää dokumentinhallinnan palvelut.
- Infrastructure: core tarkoittaa verkon ja Windows-toimialueen perustoimintaa.
- Infrastructure: office tarkoittaa sisältää IT:n toimistopalveluita, esimerkiksi tulostin- ja työasemapalvelut.

Taulukko 1. SLA-kyselyjen koontitulokset.

Category	Dependencies	SLA priority (1-n)	Availability 8/5	Risk type for business	Risk severity 5 (5-1)
Development		4,25			
Testing	License services, development	4,67			
Communications		3,06	24/7	Reputation damage	2
Support		4,25			
CRM	Integrations to communications, development	2,50	24/7	Critical data	4
Product	Communications, infrastructure: core, license services	4,50	24/7	Customer dissatisfaction	
License services	Infrastructure: core	2,67	16/5		
Financial software	Infrastructure: office	3,75			
Management		3,75		Critical data	2
Company website		4,00	24/7	Reputation damage	2
Document management		4,00	24/7	Critical data	2
Infrastructure: core		1,58	24/7		
Infrastructure: office	License services	6,33			

Luokkien riippuvuudet on myös esitelty koontituloksissa. Riippuvuudet tarkoittavat palveluita, joita rivin palvelu vaati toimiakseen. Riippuvuuksilla voidaan helposti mallintaa laajempaa palveluiden riippuvuusketjua.

SLA-prioriteetti on edellä esitetty subjektiivinen arvostusmenetelmä. Yksittäisissä kyselyissä tunnistetut palvelut on jaettu luokkiin, minkä jälkeen luokille on laskettu prioriteetin keskiarvo. Kaikkien yksittäisten kyselyiden luokkien keskiarvoille on laskettu keskiarvo koontituloksiin.

Saatavuus (availability) kuvastaa tahtoa, milloin palvelun tulisi olla saatavilla. Koontituloksien saatavuuden arvoksi on merkitty yksittäisistä kyselyistä saatu korkeimman saatavuuden ajan ehdotus.

Liiketoimintariski (risk type for business) ja sen vakavuus ovat koontitulosten viimeisellä sarakkeella. Riskeihin on merkitty palvelukatkosta aiheutuva erityinen riski ja sen vakavuus.

Kyselyiden tuloksina löytyi yllättäviä riippuvuuksia kuten esimerkiksi lisenssipalvelun kohdalla koontituloksissa. Löydettiin useita palveluita, joiden toiminta riippuu lisenssipalveluista. Tämän johdosta lisenssipalveluiden varmentamiseen on nähty erityistä vaivaa.

Palveluiden arvostusjärjestys sen sijaan ei ollut yllättävä. Koontituloksissa esitetty arvostusjärjestys ei ole tarkka, sillä yksittäisten kyselyiden arvostusmenetelmät eivät ole yhtenäiset (arvojärjestys tai arvojärjestys ryhmittäin). Yksittäisten palveluiden jakaminen

luokkiin ei myöskään ollut suoraviivaista. Koontitulosten arvojärjestys antaa kuitenkin suuntaa palveluiden arvostukselle.

Erityisiä riskejä listattiin muutaman palvelun kohdalla erikseen. Riskeistä critical data tarkoittaa yritykselle kriittisten tiedon häviämistä tai vaurioitumista, kun taas reputation damage riskiä vahingosta yrityksen maineelle.

5.5 Kyselyn ongelmakohdat

Kyselyn pääosan, matriisin, läpikäynti aloitettiin listaamalla käytössä olevat IT-palvelut. Ongelmaksi koitui palvelujen erottelu ja luokittelu ja se, kuinka tarkasti palveluita tulisi listata. Suurin osa kyselyn käytetystä ajasta kului palveluiden määrittelyyn.

Saatavuus oli vaikea määritellä, sillä yrityksen toiminta on kansainvälistä. Palveluita olisi toivottavaa käyttää jatkuvalla saatavuudella, mutta nykyisellä palvelurakenteella jatkuvaa saatavuutta ei kuitenkaan voida tarjota kaikille palveluille ilman merkittävää lisäpanosta.

Kyselyn alkuperäinen prioriteettimäärittely tuotti haasteita. Alun perin määrittely tehtiin vaikutuksen ja kiireellisyyden perusteella. Haasteena oli vaikutuksen ja kiireellisyyden määrittelyn näkökulma – tulisiko se arvioida vain haasteltavan, haastateltavan yksikön vai koko liiketoiminnan kannalta? Lopulliseen kyselyyn otettiin käyttöön subjektiivinen arvostusmenetelmä.

6 Yhteenveto

Lopputuloksen arviointi on hyödyllistä tehdä molempien aihealueiden suhteen ja lisäksi tarkastella verkonvalvonnan ja palvelutasosopimuksen yhteistoimintaa.

6.1 Verkonvalvonnan lopputila

Toimivan verkonvalvonnan välittömiä hyötyjä ei voida kiistää. Alkutilanteen hajautettu valvonta on täysin korvattu yrityksen vaatimuksen täyttävällä keskitetyllä järjestelmällä.

Voidaan todeta useita eri tapauksia, joissa valvonnasta on ollut välitöntä apua sekä ongelmien ennaltaehkäisemissä että niiden korjaamisessa. Valvontanäkymä mahdollistaa kokonaisvaltaisen kuvan muodostamisen IT-toimintojen palveluntarjonnasta, jossa virheet ja poikkeukset ovat selkeästi erotettavissa.

Onko verkonvalvonta kuitenkaan koskaan valmiissa tilassa? Verkonvalvonnan kohteet ovat tavallisesti jatkuvassa muutoksessa, sillä laitteita päivitetään ja palveluiden määrityksen muuttuvat. On myös huomioitava verkonvalvontajärjestelmän ylläpito, päivitykset ja ongelmatilanteiden selvittäminen. Erityisesti järjestelmän ylläpito on selkeä jatkuvan kehityksen kohde myös vastaisuudessa. Toinen erikseen mainittava kehityskohde on valvonnan syventäminen. Valvontaa voidaan syventää valitun järjestelmän Virtual user -tasolla (luku 3.3.2). Virtuaalikäyttäjillä voidaan jäljitellä oikeiden käyttäjien toimintaa ja kerätä kaikki tieto eri palveluiden käytön eri vaiheista.

6.2 Palvelutasosopimuksen lopputila

Palvelutasosopimuksen edut eivät ole yhtä ilmeiset verkonvalvonnan hyötyihin verrattuna. Hyvä palvelutasosopimus on kuitenkin sisäisten IT-toimintojen palvelukehityksen kulmakivi. Sisäisten palveluiden tehokkaan tarjoamisen tärkein edellytys on tietää tarkasti liiketoiminnan asettamat vaatimukset. Ilman muodollisia vaatimuksia voidaan palveluiden käytön laajuutta ja tärkeysastetta vain arvioida. Alkutilanteessa tiedossa oli toki summittainen kuva käytetyistä palveluista, mutta tarkasti määriteltä kuvaa ei ollut lainkaan. Määrittelyn yhteydessä havaittiin myös palveluita, joiden toiminnasta ei aikaisemmin ollut tietoa.

Lopputilana annettiin ehdotus palvelutasosopimuksesta, joten seuraava kehityskohde on palvelutasosopimuksen muodollinen hyväksyntä. Muihin kehityskohteisiin sisältyy kyselyn avointen kysymysten mahdollinen käyttö yleisenä tyytyväisyyskyselynä ja myös palvelutasosopimuksen laajentaminen. Kyselyssä otettiin kantaan vain yrityksen kotimaan toimintojen vaatimuksiin. On olennaista laajentaa kysely kaikkiin haarakonttoreihin.

6.3 Verkonvalvonta ja palvelutasosopimus yhdessä

Työn alkuvaiheessa ei ollut helppoa muodostaa selkeää ajatusta siitä, miten verkonvalvonta ja palvelutasosopimus ovat yhteydessä toisiinsa. Loppuvaiheessa yhteys on selkeä.

Verkonvalvonnan suunnitteleminen puhtaalta pöydältä on haastavaa. Sisäisten IT-toimintojen tarkoitus on tukea liiketoimintaa, ei määrittellä sitä. Valvonnan määrittely ainoastaan IT-toimintojen näkökulmasta ei ole perusteltua. Palvelutasosopimuksen avulla saadaan liiketoiminnan näkökulma verkonvalvontaan. Apua on myös palveluiden tunnistamisesta: kaikki palvelut eivät ennestään olleet IT-toimintojen tiedossa.

Verkonvalvonnan tärkein etu palvelutasosopimuksen suuntaan on sen tarjoama tekninen alusta palveluiden tilan seuraamiseen. Yhteisesti sovittu järjestelmä on neutraali mitauspiste palveluiden toiminnalle. Saatavilla on myös historiatieto: on mahdollista verrata palvelutasosopimuksen ehtojen toteutumisen nykyhetkeä aikaisempiin ajankohtiin. Palvelutasosopimuksen automatisoitu seuranta on hyvä kehityskohde integraation edistämiseksi, ja se vahvistaa jo voimakasta yhteyttä verkonvalvonnan ja palvelutasosopimuksen välillä.

Lähteet

- 1 Service and Agent Network. 2013. Verkkodokumentti. Napa yhtiöt. <http://www.napa.fi/Contact-Us/Service-and-Agent-Network>>. 2013. Luettu 13.4.2014.
- 2 About ITU. 2014. Verkkodokumentti. International Telecommunication Union. <<http://www.itu.int/en/about/Pages/default.aspx>>. 4.1.2007. Luettu 13.4.2014.
- 3 Recommendation X.700. 1992. Verkkodokumentti. International Telegraph and Telephone Consultative Committee. <<http://www.itu.int/rec/T-REC-X.700-199209-1/en>>. 4.1.2007. Luettu 13.4.2014.
- 4 Internet control message protocol. 1981. Verkkodokumentti. IETF. <<http://tools.ietf.org/html/rfc792>>. Syyskuu 1981. Luettu 13.4.2014.
- 5 R. Mauro, Douglas – J. Schmidt, Kevin. 2005. Essential SNMP, Second Edition. O'Reilly Media: California, USA.
- 6 A Simple Network Management Protocol. 1988. Verkkodokumentti. IETF. <<https://www.ietf.org/rfc/rfc1067.txt>>. Elokuu 1988. Luettu 13.4.2014.
- 7 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). 2002. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc3416>>. Joulukuu 2002. Luettu 13.4.2014.
- 8 Structure of Management Information Version 2 (SMIv2). 1999. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc2578>>. Huhtikuu 1999. Luettu 13.4.2014.
- 9 A Simple Network Management Protocol (SNMP). 1990. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc1157>>. Toukokuu 1990. Luettu 13.4.2014.
- 10 Introduction to the Remote Monitoring (RMON) Family of MIB Modules. 2003. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc3577>>. Elokuu 2003. Luettu 13.4.2014.
- 11 Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. 2008. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc5101>>. Tammikuu 2008. Luettu 13.4.2014.
- 12 About WMI. 2014. Verkkodokumentti. Microsoft. <[http://msdn.microsoft.com/en-us/library/aa384642\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384642(v=vs.85).aspx)>. 2014. Luettu 13.4.2014.
- 13 The Syslog Protocol. 2009. Verkkodokumentti. IETF. <<https://tools.ietf.org/html/rfc5424>>. Maaliskuu 2009. Luettu 13.4.20

- 14 Beck, Kent - Grenning, James - C. Martin, Robert – Beedle, Mike - Highsmith, Jim - Mellor, Steve - Van Bennekum, Arie - Hunt, Andrew - Schwaber, Ken – Cockburn, Alistair - Jeffries, Ron - Sutherland, Jeff - Cunningham, - Kern, Jon - Thomas, Dave – Fowler, Martin – Marick, Brian. 2001. Principles behind the Agile Manifesto. Verkkodokumentti. <<http://agilemanifesto.org/principles.html>>. 2001. Luettu 13.4.2014.
- 15 Icinga Quickstart. 2009. Verkkodokumentti. Icinga Development Team. <<http://docs.icinga.org/latest/en/quickstart-icinga.html>>. 2014. Luettu 13.4.2014.
- 16 Valhal – Valvonta ja hallinta. 2013. Verkkodokumentti. PCP Partner Oy. <<http://www.pcp.fi/pilvipalvelut/valhal/>>. 2013. Luettu 13.4.2014.
- 17 Van Bon, Jan - De Jong, Arjen - Kolthof, Axel - Pieper, Mike - Tjassing, Ruby - Van der Veen, Annelies - Verheijen, Tienieke. 2008. Service Operation Based on ITIL V3: A Management Guide. Zaltbommel: Van Haren Publishing.
- 18 Calculating the Reliability of Series/Parallel and Non Series/Parallel Systems. 2001. Verkkodokumentti. Department of Electrical and Computer Engineering, University of Massachusetts. <<http://www.ecs.umass.edu/ece/koren/FaultTolerantSystems/simulator/NonSerPar/nsnpframe.html>>. Luettu 13.4.2014.
- 19 Kelly, Timothy. 2005. VoIP for Dummies. Wiley Publishing: Indiana, USA.
- 20 Van Bon, Jan - De Jong, Arjen - Kolthof, Axel - Pieper, Mike - Tjassing, Ruby - Van der Veen, Annelies - Verheijen, Tienieke. 2008. Service Design Based on ITIL V3: A Management Guide. Zaltbommel: Van Haren Publishing.
- 21 Recommendation E.800. Elokuu 1994. Verkkodokumentti. International Telecommunication Union. <<http://www.itu.int/rec/T-REC-E.800-200809-I/en>>. 30.4.2009. Luettu 13.4.2014.
- 22 Eskola, Jari – Suoranta, Juha. 2001. Johdatus laadulliseen tutkimukseen. Jyväskylä: Vastapaino.

SLA-matriisi

[illegible]