Saimaan ammattikorkeakoulu
Tekniikka, Lappeenranta
Tietotekniikan koulutusohjelma
Organisaation It-palvelut

Lauri Repo

Premekon Oy:n tietoliikenneverkon uudistus

Opinnäytetyö 2015

Tiivistelmä

Lauri Repo
Premekon Oy:n tietoliikenneverkon uudistus, 36 sivua
Saimaan ammattikorkeakoulu
Tekniikka Lappeenranta
Tietotekniikan koulutusohjelma
Organisaation IT-palvelut
Opinnäytetyö 2015
Ohjaajat: lehtori Mikko Huhtanen, Saimaan ammattikorkeakoulu, tietojärjestelmäasiantuntija Asko Rupponen, Premekon Oy

Tämän opinnäytetyön aiheena on Premekon Oy:n tietoliikenneverkon uudistaminen. Työn tavoitteena oli tuottaa yrityksen aikaisemman tietoliikenneverkon korvaajaksi nykyaikainen, vikasietoinen ja tietoturvallinen tietoliikenneverkko sekä laajentaa sen ominaisuuksia ja käytettävyyttä.

Opinnäytetyö koostuu opinnäytetyön kohteena olevan uudistuksen kannalta olennaisten ITIL-mallin osa-alueiden esittelystä, lähtötilanteen kartoituksesta, uudistuksen suunnittelusta, toteutus- ja testausvaiheesta sekä jatkokehitysajatusten ja muiden pohdintojen osuudesta. Lisäksi työn lopussa käsitellään hieman riskienhallintaa uudistukseen ja verkkolaiteympäristöön liittyen.

Työn käytännön osuus valmistui ajallaan ja tavoitteet saavutettiin. Vikasietoisuus saavutettiin verkon kriittisimmissä osa-alueissa ja verkon tietoturvaa parannettiin segmentoimalla verkko käyttökohteiden mukaisiin alueisiin. Käytettävyyttä parannettiin saumattomasti toimivalla langattoman verkon ratkaisulla sekä DHCP:n käyttöönotolla.

Asiasanat: tietoliikenneverkko, TCP/IP, LAN, VLAN, WLAN

Abstract

Lauri Repo
Improvement of a local area network for Premekon Oy, 36 pages
Saimaa University of Applied Sciences
Technology Lappeenranta
Information technology
IT services
Bachelor´s Thesis 2014
Instructors: Mr Mikko Huhtanen, Senior Lecturer, Saimaa University of Applied Sciences, Mr Asko Rupponen, Technical Specialist, Premekon Oy

The purpose of the thesis was to design and implement a new and segmented local area network to replace the previous network implementation. The work was commissioned by Asko Rupponen for Premekon Oy. The main focus of the design was in fault tolerance, security and usability. An extensible WLAN network was also in the scope of the work.

A new local area network was designed, tested and implemented side by side with the previous one during the working period. The main themes of ITILv3 model were used when suitable while designing and fulfilling the actual reformation of the network.

The final result of this thesis was a completely new, extensible and secure local area network with basic supervision implemented for the critical elements of the network infrastructure. The objectives of the work were achieved and the network is currently operational on the premises. Some key notes about future development projects were also documented for later use.

Keywords: Local Area Network, TCP/IP, LAN, VLAN, WLAN

Sisällys

Termit

802.1Q protokolla	IEEE standardi, joka mahdollistaa VLAN:ien käytön Ethernet-lähiverkoissa
802.1X protokolla	IEEE standardi Ethernet-lähiverkoissa käytettävälle porttikohtaiselle tunnistamiselle
CARP	Common Address Redundancy Protocol. Reitittimien kahdennusprotokolla, jonka avulla IP-osoite voidaan jakaa reitittävien laitteiden välillä virtuaalisen verkkoliitännän avulla.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka tehtävänä on jakaa verkkoasetusparametrejä, esimerkiksi IP-osoitteita, tietoliikenneverkkoon kytketyille laitteille
FreeRADIUS	Avoimen lähdekoodin RADIUS-palvelinsovellus. Mahdollistaa esimerkiksi 802.1X protokollan käyttämisen
IEEE	Institute of Electrical and Electronics Engineers -järjestö
LAN	Local Area Network, lähiverkko
NAT	Network Address Translation. Mahdollistaa osoitemuunnokset esimerkiksi ei-julkisten ja julkisten osoitteiden välillä.
pfSense	Avoimen lähdekoodin palomuurikäyttöjärjestelmä, joka on asennettavissa esimerkiksi tavalliselle PC-raudalle
Spanning Tree Protocol	IEEE 802.1D standardin mukainen protokolla, jonka tarkoituksena on lähiverkkokytkinten välisten silmukoiden estäminen
VLAN	Virtual Local Area Network, virtuaalinen verkkoalue
VLAN Tag	IEEE 802.1Q standardin mukainen merkintä Ethernet-paketissa, joka mahdollistaa virtuaalisten verkkoalueiden käytön tietoliikenneverkossa.
VLAN Trunk	Tietoliikennelaitteiden välinen linkki, jossa voidaan kuljettaa usean VLAN:in liikennettä laitteelta toiselle
VTP	Cisco Systemsin patentoima protokolla, jonka avulla samaan VTP domainiin liitetyt lähiverkkokytkimet voivat siirtää VLAN-tiedot kytkimeltä toiselle automaattisesti

1 Johdanto

Tämä opinnäytetyö käsittelee Premekon Oy:lle toteutettua tietoliikenneverkon uudistusta. Työssä pyritään käsittelemään muutostyön läpivientiä ITILv3-mallin kehityspolun mukaisesti. Työssä esitellään työn kannalta olennaisten, tietoliikenneverkon rakenteeseen ja palveluihin liittyvien termien tarkoitus sekä käyttökohteet.

Tietoliikenneverkkojen toimintavarmuus ja tietoturva ovat nykyään jokaisen yrityksen perustoiminnan kulmakiviä. Jos verkossa tapahtuu häiriö tai verkon tietoturva vaarantuu, saattaa seurauksena olla yrityksen toiminnan halvaantuminen tai ainakin toiminnan heikkeneminen. Tietoturvaongelmat saattavat johtaa erilaisiin ongelmiin yritysten asiakkaiden kanssa ja menetettyä luottamusta on vaikea saada takaisin. Tästä syystä onkin erittäin tärkeää, että yritysten käytössä olevat verkkoratkaisut on suunniteltu ja toteutettu käyttäen parhaita mahdollisia toimintatapoja, kuitenkin järkevään kustannustasoon pyrkien.

Aihe on varsinkin pienten yritysten osalta mielenkiintoinen, sillä monessa yrityksessä yrityksen henkilökunnan tietotaito perustuu lähinnä yksityisenä henkilönä hankittuun osaamiseen, eikä tietoa osata välttämättä soveltaa yritysmaailman ratkaisuihin. Ratkaisuissa saatetaan keskittyä joskus liikaakin kustannusten minimoimiseen, unohtaen tai jättäen huomioimatta esimerkiksi yhteyden vikaantumisesta aiheutuvat välilliset kustannukset ja niiden minimointi.

1.1 Kohdeyritys: Premekon Oy

Premekon Oy on Lappeenrannan Joutsenossa toimiva metallialan yritys, joka suunnittelee ja valmistaa erilaisia metallirakenteita ja tuotteita teollisuuden tarpeisiin. Yritys on perustettu vuonna 1984 nimellä Insinööritoimisto Premekon Oy ja se erikoistui 1990-luvun alussa teollisuuden hoitotasojen valmistukseen. Premekon Oy työllistää 60–70 henkilöä, joista noin 20 henkilöä työskentelee suunnittelun, työnjohdon ja hallinnon työtehtävissä ja noin 50 henkilöä valmistustehtävissä. Suurin osa yrityksen valmistamista tuotteista viedään ulkomaille. Referenssiasiakkuuksina yrityksen verkkosivuilla mainitaan Metso Paper sekä Andritz, joille on toimitettu yrityksen suunnittelemia ja toteuttamia teollisuusympäristöjen hoitotasoja.

1.2 Työn tavoitteet

Työn tavoitteena oli tuottaa Premekon Oy:lle aiempaa tehokkaampi ja turvallisempi tietoliikenneverkko, vuosien saatossa rakennetun verkkoratkaisun tilalle. Aiempi ratkaisu oli toiminut lähiverkon nopeuden osalta melko hyvin, mutta muita näkökulmia, kuten eri verkkoalueiden eriyttämistä tietoturvasyistä, ei oltu juurikaan huomioitu. Käyttäjämäärän kasvaessa ja uusia toimintatapoja suunnitellessa oli huomattu, että verkon rakennetta oli tarve muuttaa, jotta puuttuvat ominaisuudet saataisiin käyttöön.

Verkon rakennetta uudistaessa oli tarkoitus ottaa käyttöön myös muita uusia ominaisuuksia, kuten esimerkiksi useiden WLAN-tukiasemien avulla toteutettu saumaton langaton verkkoyhteys, toisistaan eriytetyt virtuaaliverkot (VLAN) sekä porttikohtaisen todentamisen (IEEE 802.1X-protokolla) avulla tapahtuva käyttäjän tunnistaminen hallintaverkkoon liityttäessä. Lisäksi tavoitteena oli myös ottaa käyttöön raportointiin ja valvontaan liittyviä sovelluksia, joiden avulla verkon kehitystä ja muutostarpeita voitaisiin suunnitella ja seurata. Valvonnan ja raportoinnin avulla olisi mahdollista kerätä tärkeää dataa siitä, miten verkko toimii kokonaisuutena ja valvoa verkon aktiivilaitteita yleisellä tasolla. Valvontajärjestelmään on lisäksi mahdollista määritellä myös palvelinten ja muiden laitteiden valvontaa, tarpeiden kasvaessa.

Verkkouudistuksen suunnittelu- ja toteutusvaiheiden läpiviennissä oli erittäin tärkeää se, että uuden verkon toimivuutta voitiin ensin testata erillisen testiryhmän avulla, vaarantamatta alkuperäisen verkon toimivuutta. Tällöin päivittäiseen liiketoimintaan liittyvät toimet eivät häiriintyisi verkkouudistukseen liittyvistä muutoksista eikä muutoksesta aiheutuisi yrityksen toiminnalle ongelmia.

Työssä käytetyt menetelmät ja määritykset dokumentoitiin yrityksen myöhempää käyttöä sekä mahdollista jatkokehitystä varten. Samalla luotiin myös lähtöasetelma jatkuvalle palvelun parantamiselle, hyödyntäen verkonvalvonnan ja seurannan tuottamaa dataa.

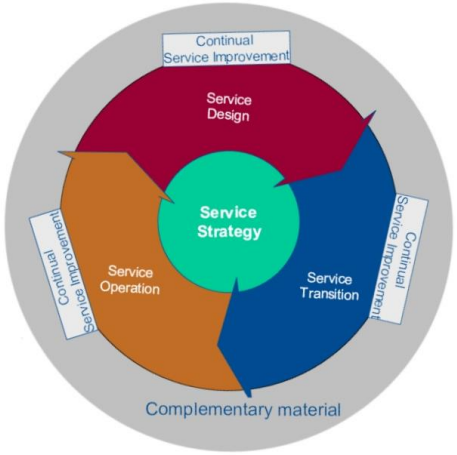
Käytännön kehitystehtäviä opinnäytetyössä olivat:

- Verkko- ja IP-suunnitelman teko

- Verkkoalueiden eriyttäminen erillisiksi virtuaaliverkoiksi
- Kahdennetun palomuurikoneparin asetusten määrittely virtuaalisten verkkoalueiden ja muiden asetusten osalta kokonaisuuteen sopivaksi (palomuuriparin rakentaminen toteutettiin erillisenä projektina)
- Lähiverkkokytkimien asetusten määrittely
- Yhtenäisen langattoman verkon suunnittelu, toteutus ja käyttöönotto
- Verkkolaitteiden valvonnan määrittely

2 ITIL-mallista lyhyesti

ITIL–mallilla tarkoitetaan OGC:n eli Office of Government Commercen (UK) kehittämää, nykyisin IT Service Management Forumin (itSMF) ylläpitämää kokoelmaa, joka käsittelee IT-palveluiden hallintaan ja johtamiseen liittyviä parhaita käytäntöjä. Malli sisältää suuren määrän erilaisia toimintoja ja prosesseja, joista organisaatio voi poimia sopivat osat käyttöönsä. Mallin laajuuden vuoksi kaikkia toimintoja ei ole välttämättä mahdollista tai järkevää yrittää soveltaa sellaisenaan, vaan mallin ideaa täytyy muokata kohdeorganisaation toimintaan ja resursseihin sopivaksi. Esimerkiksi palvelupistetoiminnon järjestäminen pienissä yrityksissä on usein resurssimielessä haastavaa, mutta tukijärjestelmiä ja itsepalvelumahdollisuuksia sekä yhdessä sovittuja ja hyvin kuvattuja prosesseja hyödyntämällä toiminnan voi saada alkuun. (1 s. 13; 2.)



Kuva 1: ITILv3 Elinkaarimallin rakenne (1.)

ITILv3–mallissa palveluiden tuottamiseen liittyy viisi pääaihealuetta (kuva 1):

1. Palvelustrategia - Service Strategy
2. Palvelusuunnittelu - Service Design
3. Palvelutransitio - Service Transition
4. Palvelutuotanto - Service Operation
5. Jatkuva palvelun parantaminen - Continual Service Improvement

Mallin ytimenä toimii palvelustrategia, joka ohjaa palveluiden suunnittelua, palvelutransitiota sekä palvelutuotantoa. Palvelustrategian tärkeimpänä tarkoituksena on määrittää yrityksen tarjoamien palveluiden sisältö, kohderyhmät sekä kehitystarpeet. Palvelustrategian avulla tuotetaan yrityksen palveluportfolio, joka yhdessä palvelusuunnittelun tuottaman palvelukatalogin avulla kuvaa yrityksen tuottamat ja ulkopuolelta hankittavat IT-palvelut. (1 s. 23; 2; 3.)

Palvelusuunnittelu keskittyy tuottamaan palvelukatalogin tueksi myös palveluiden riskienhallintaan, saatavuuteen, kapasiteetinhallintaan, tietoturvaan sekä jatkuvuuden hallintaan liittyvää tietoa. Palvelusuunnittelun yhteydessä suunnitellaan myös palveluiden arkkitehtuuri sekä tarvittavat prosessit palvelun tuottamiseksi. (1 s. 31; 4.)

Palvelutransition tavoitteena on mahdollistaa ja varmistaa palveluiden tehokas ja turvallinen käyttöönotto, sekä uusien että muuttuvien palveluiden osalta. Palvelutransitio tähtää siis palveluiden käyttöönottoon ja se koostuu muun muassa erillisistä suunnittelu ja valmisteluvaiheista, testaus- ja pilotointivaiheista sekä varsinaisesta käyttöönottovaiheesta. (1 s. 39; 5.)

Palvelutuotanto keskittyy varmistamaan ja hallitsemaan palveluiden keskeytyksetöntä tuottamista palveluiden käyttäjille. Palvelutuotannon tukena käytetään palveluille määriteltäviä palvelutasoja (Service Level Agreement, SLA), joiden avulla määritellään palveluiden saavutettavuuden tavoitetasot. Palvelutuotanto koostuu herätteiden, häiriöiden ja ongelmien hallinnasta sekä erillisten palvelupyyntöjen hallinnasta. Palvelutuotannon työkaluna käytetään usein tukipyyntöjen käsittelyyn tarkoitettua tikettijärjestelmää. (1 s. 45.)

Jatkuvalla palvelun parantamisella pyritään nimensä mukaisesti seuraamaan ja kehittämään palveluiden ja prosessien laatua, tehokkuutta sekä varmistamaan, että palvelut vastaavat palveluiden käyttäjien odotuksia. Pienten yritysten mittakaavassa jatkuva palvelun parantaminen voi tarkoittaa esimerkiksi sisäisten IT-

palveluiden toimivuuden seuraamista ja kehittämistä palautteen tai tehtyjen huomioiden perusteella. Toisaalta myös sovittujen toimintamallien ja prosessien noudattamisen seuranta sekä prosessien kehittäminen ympäristössä tapahtuvien kehityshankkeiden ja muutosten perusteella on osa jatkuvaa palveluiden parantamista. Kehitysaskeleiden ei välttämättä aina tarvitse olla suuria, kyse voi olla esimerkiksi uuden työaseman käyttöönottoon liittyvien haasteiden vähentämisestä. Jotta kehitystä voitaisiin seurata ja mitata, on kehitysideat kirjattava ylös ja niiden edistymistä seurattava. (1 s. 53; 6.)

Tässä opinnäytetyössä pyrittiin keskittymään työn kannalta olennaisiin ITIL-mallin osiin. Koska kohdeyritys oli henkilöstömäärältään melko pieni metallialan yritys, eivätkä sen henkilöstöresurssit mahdollistaneet esimerkiksi kaikkien ITIL:in mukaisten toimintojen toteuttamista, pyrittiin työssä soveltamaan tietoa parhaan mahdollisen toiminnan takaamiseksi. Mallin päätason otsikot (palvelustrategia, palvelusuunnittelu, palvelutransitio, palveluiden operointi sekä jatkuva palveluiden parantaminen) pyrittiin huomioimaan ja tietoliikenneverkon uudistusta käsiteltiin mallin vaiheiden mukaisesti. Suunnitteluvaiheessa pyrittiin luomaan yrityksen IT-palveluista palveluportfolio sekä palvelukatalogi ja kuvaamaan IT-palveluita näiden avulla. Palveluportfolion ja palvelukatalogin tietojen pohjalta lähdettiin kehittämään eri osa-alueita tietoliikenneverkon uudistustarpeiden tavoitteiden mukaiseen suuntaan.

3 Lähtötilanne

Opinnäytetyön aloitushetkellä Premekon Oy:n tietoliikenneverkon rakenne oli muotoutunut vuosien saatossa, tarpeiden kasvaessa pikkuhiljaa. Koska verkkoa ja sen palveluita oli rakennettu pala kerrallaan aina uuden tarpeen ilmetessä, ei yritykseltä löytynyt varsinaista verkkosuunnitelmaa, eikä kaikkia osa-alueita ollut dokumentoitu kunnolla. Lisäykset oli tehty parhaan osaamisen ja resurssien puitteissa ja yrityksen tietojärjestelmäasiantuntija oli kyllä tietoinen verkon rakenteesta, mutta muuten tilanteesta ei ollut olemassa selkeää kuvausta. Lisäksi osa yrityksen lähiverkossa toimivista palveluista alkoi olla elinkaarensa päässä, joten opinnäytetyönä tehtävä, verkon rakennetta, palveluita ja hallintaa käsittelevä työ oli enemmän kuin tervetullut yrityksen näkökulmasta katsottuna.

Ensimmäisessä vaiheessa työtä aloittaessa pyrimme yhdessä tietojärjestelmäasiantuntijan kanssa kartoittamaan lähiverkon nykytilanteen ja tarkastelemaan verkon rakennetta sekä siihen sisältyviä palveluita yleisellä tasolla. Vaikka yrityksen tärkeimpänä tavoitteena oli alun perin opinnäytetyötä suunniteltaessa saumattoman langattoman verkon käyttöönotto, huomattiin lähtötilannetta tutkiessa, että koko tietoliikenneverkon rakenne olisi hyvä suunnitella ja toteuttaa uudelleen. Tällöin verkon rakenne, palvelut ja muut kriittiset komponentit saataisiin yhtenäistettyä ja dokumentoitua ja samalla uudistus mahdollistaisi myös uusien, vikasietoiseen toteutukseen tähtäävien laitekokonaisuuksien ja asetuskokonaisuuksien käyttöönoton.

4 Tietoliikenneverkon uudistus, suunnitteluvaihe

Suunnitteluvaihe käynnistettiin lähtötilanteen kartoituksella. Kartoitusvaiheessa pyrittiin muodostamaan kuva verkon rakenteesta sekä verkon erilaisista palveluista ja niiden riippuvuuksista. Käytännössä kartoitusvaiheessa käytiin yrityksen verkon laitteet sekä toteutustavat läpi yhdessä yrityksen IT-vastaavan kanssa ja tutkittiin niiden asetuksia. Kun kartoitusvaihe saatiin päätökseen, aloitettiin varsinainen uudistuksen suunnittelu. Suunnittelu jaettiin erilaisten aihealueiden perusteella useaan osaan.

4.1 Lähtötilanteen tarkempi kartoitus

Uudistuksen suunnitteluvaiheen ensimmäisenä tehtävänä oli tarkastella lähtötilanteen verkon rakennetta, verkossa toimivia palveluita ja muita resursseja. Tilannetta käytiin läpi yhdessä yrityksen tietojärjestelmäasiantuntijan kanssa, tarkastelemalla laitteita ja kytkentöjä fyysisellä tasolla sekä keskustelemalla rakenteesta ja konfiguraatioista yleisellä tasolla.

Verkon rakenne vaikutti melko yksinkertaiselta: kaikki laitteet olivat samassa sisäverkossa ja verkkosegmentissä, lähiverkko oli toteutettu yhdellä Ciscon ja kahdella D-Linkin kytkimellä. Pääosa yrityksen työasemista oli kytkettynä Ciscon laitteeseen, laitteen konfiguraatio oli tehdasasetuksilla. Myös D-Linkin laitteet olivat tehdasasetuksillaan. Yrityksen kanssa samoissa tiloissa toimivan sisaryrityksen laitteet oli kytketty samaan lähiverkkoon yrityksen laitteiden kanssa

ja yritykset jakoivat keskenään muun muassa verkkotulostimet. Myös verkkolevykapasiteetti oli yhteistä laitetasolla, eri käyttäjille oli määritelty eri verkkolevyasemat tarpeiden mukaisesti.

Verkon palomuurina toimi vanha Linux-palvelin, joka hoiti palomuurisääntöjen toteutuksen lisäksi myös reitityksen julkisen sekä ei-julkisen verkon välillä. Palomuurikone oli kaapeloitu yksittäisellä verkkokaapelilla operaattorin päätelaitteeseen, kahdennettua kytkentää ei ollut käytössä. Palomuuriin oli tehty muutamia 1:1 NAT-osoitemuunnossääntöjä tiettyjen sisäverkossa sijaitsevien laitteiden käyttöä varten sekä sallittu liikennettä tarpeen mukaisesti, jotta laitteisiin pystyttiin saamaan yhteys myös määritetyistä osoiteavaruuksista julkisen verkon yli.

Verkossa ei ollut käytössä IP-osoitteiden ja muiden tarpeellisten verkkoasetusten automaattisesta jakamisesta huolehtivaa DHCP-palvelinta, vaan kaikille verkon laitteille oli määritelty IP-osoitteet manuaalisesti. DHCP päätettiin ottaa uudistuksen yhteydessä käyttöön ja se päätettiin sijoittaa palomuuriparin kylkeen. Tällöin palvelu pystyttiin samalla kahdentamaan ja toteuttamaan vikasietoisesti.

Langaton verkko oli toteutettu kahdella WLAN -tukiasemalla. Toinen laitteista oli liitetty suoraan yrityksen sisäverkkoon, toinen tarjosi vierailijaverkkoa ja liikennöi suoraan julkiseen verkkoon operaattorin toimittaman päätelaitteen kautta. Vierasverkko oli salaamaton.

Yrityksellä ei ollut lähiverkossaan Microsoftin Active Directory-hakemistopalveluita tai muita hakemistopalveluita, joiden avulla tunnushallintaa tai työasemien keskitettyä hallintaa olisi voitu tehdä. Käyttäjien työasemat oli asennettu yksitellen ja käyttäjätunnukset olivat paikallisesti asetettuja, työ-asemat olivat liitettynä yrityksen työryhmään (workgroup). Uusia tai muuttuvia asetuksia ei siis voitu jakaa työasemille keskitetyn konfiguraatio- tai asetushallinnan kautta (esimerkiksi Group Policy Object -määritykset tai Microsoft System Center Configuration Managementin avulla toteutetut jakelut), joten jokaiselle työasemalle oli määriteltävä asetukset manuaalisesti työasema kerrallaan. Tämän todettiin hidastavan esimerkiksi työn lopputuloksena käytettävien verkkoasetusten muuttamista

työasemilla, joten asetusten manuaaliseen muuttamiseen varattiin käyttöönotto-suunnitelmassa aikaa.

Palveluiden, laitteiden ja asetusten hallinta tapahtui tietotojärjestelmäasiantuntijan toimesta, erillisiä dokumentteja hyödyntämällä. Varsinaisia keskitettyjä dokumenttien tai tiedonhallinnan työkaluja ei ollut käytössä, mutta eräänlainen tiedotusväline oli rakennettu yhdelle lähiverkon virtuaalipalvelimista. Lisäksi yrityksen työntekijöillä oli käytössään Mozillan kalenterisovellus, johon oli rakennettu integraatio yrityksen tuntikirjausjärjestelmään.

Palveluiden osalta kirjasimme yrityksen tietojärjestelmäasiantuntijan kanssa yhdessä selvityksen, josta muodostimme ITIL-mallin mukaisen palveluportfolion palvelukatalogin. Palvelukatalogissa huomioimme palvelustrategian mallin; määrittelimme, mitä palveluita haluttiin ja voitiin tuottaa järkevästi yrityksen omasta verkosta, omilla resursseilla ja mitkä palvelut hankittiin muilta palvelun-tarjoajilta.

4.2 Verkon rakenteen suunnittelu

Verkon rakenteen suunnittelussa lähdettiin siitä, että verkon käyttäjät ja resurssit piti pystyä eriyttämään toisistaan ja vain erikseen määritellyt yhteydet haluttiin sallia verkkoalueiden välillä. Verkko täytyi siis jakaa erillisiin virtuaalisiin VLAN-verkkoalueisiin ja virtuaaliset verkkoalueiden välinen liikenne kierrättää verkon reitittimenä toimivan palomuurilaitteen kautta. Tällöin verkkoliikenteen suodatusta verkkoalueiden välillä olisi mahdollista tehdä palomuurisääntöjä hyödyntämällä ja eri virtuaaliverkoissa olevat laitteet eivät näkisi toisiaan, vaikka olisivatkin kytkettyinä samaan lähiverkon kytkimeen.

Tarvittavia verkkoalueita suunnitellessa tunnistettiin seuraavat kokonaisuudet:

- julkinen verkkoalue
- yrityksen varsinainen verkkoalue
- sisaryrityksen verkkoalue
- vierasverkko
- hallintaverkko
- julkiseen verkkoon altistettavien laitteiden verkkoalue (optio)

Julkiselle verkolle ei tarvinnut luoda VLAN-verkkoa palomuurilaitteelle ja lähiverkon kytkimille, sillä julkiset IP-osoitteet oli mahdollista sitoa palomuurilaitteelle ja luoda palomuurille sopivat NAT-osoitemuunnossäännöt liikenteen läpivientiä varten. Muille verkkoalueille oli luotava omat VLAN-alueet ja määriteltävä ne sekä palomuurilaitteelle että lähiverkon kytkimille.

Yritykselle rakennettiin samaan aikaan erillisenä projektina kahdennettu, pfSense-palomuurikäyttöjärjestelmällä varustettu palomuurikokonaisuus. Palomuuriparia suunnitellessa ja toteuttaessa oli huomioitu myös tietoliikenneverkon uudistukseen liittyvät vaatimukset, joten palomuurilaitteen hyödyntäminen tässä kokonaisuudessa oli mahdollista. Palomuurilaitteet oli kahdennettu, jotta yksittäisen palomuurikoneen mahdollinen käyttökatkos ei estäisi koko verkon liikennöintiä eikä esimerkiksi muurin päivityksestä aiheutuisi loppukäyttäjille näkyvää katkosta. Jotta lähiverkko olisi todellisuudessa vikasietoinen, täytyisi myös tärkeimpien lähiverkkolaitteiden välille rakentaa kahdennettuja verkkokytkentöjä siten, että yksittäisen laitteen poistaminen verkosta ei kaataisi koko verkon toimintaa. Esimerkiksi tärkeimmät palvelinlaitteet voitaisiin tällöin kytkeä useampaan lähiverkkokytkimeen, jolloin myös palvelinten tietoliikennekytkennät saataisiin vikasietoisiksi. Tavallisen työaseman tai muun vastaavan laitteen ollessa kytkettynä vain yhteen lähiverkkokytkimeen ei vikasietoisuutta olisi tarjolla, mutta työaseman käyttämän verkkoportin voisi tarvittaessa vaihtaa esimerkiksi lähiverkkokytkimen vikatilanteessa manuaalisesti kytkimestä toiseen.

4.3 Tiedon hankinta

Koska toteutettavat muutokset vaativat erilaisten teknologioiden ja resurssien käyttöönottoa, mutta muutokseen käytettävissä oleva budjetti oli rajallinen, oli muutos suunniteltava myös resurssimielessä tarkkaan. Aiempien kokemusteni perusteella tiesin, että tiettyjen laitevalmistajien laitteilla (Cisco, Juniper, HP) kokonaisuuden olisi saanut rakennettua melko varmasti tarpeiden mukaiseksi. Näiden laitevalmistajien käyttämisen negatiivisena puolena voitiin nähdä laitteiden korkea hinta sekä konfiguroinnin vaatimukset ylläpitäjältä, joten oli tutkittava muita vaihtoehtoja. Samantapaisia lähiverkkokokonaisuuksia oli varmasti rakennettu aikaisemmin, hyödyntäen erilaisia laitekombinaatioita sekä laitteiden

käyttöjärjestelmävaihtoehtoja. Tietoa täytyi vain osata etsiä oikeista paikoista ja muokata tilanteeseen sopivaksi.

Käytössäni oli pfSense-palomuuriparin asennus- ja käyttöönottoprojektin yhteydessä hankittu, pfSensen kultatason tukijäsenilleen julkaisema asennus- ja konfigurointiopas. Aiemmin hankkimastani Ciscon CCNA Portable Command Guide -opaskirjasta sekä Ciscon verkkosivuilta ladattavista kytkinten pikaoppaista löytyi paljon käytännön apua kytkinten asetusten ja verkon rakenteen suunnittelun tueksi.

4.4 Tietoliikennelaitteiden käytön suunnittelu

Käytettävien laitteiden suunnittelussa oli huomioitava yrityksen käytössä olleiden laitteiden uudelleenkäyttömahdollisuudet sekä yhteensopivuus hankittavien laitteiden kanssa. Lähtötilanteen kokonaisuudessa oli käytössä 2 kpl D-Link DGS1210-24 kytkimiä sekä 1 kpl Cisco Catalyst WS-2948G-GE-TX kytkimiä. Laitteiden asetukset olivat tehdasasetusten mukaiset, sillä niitä ei ollut verkon yksinkertaisesta rakenteesta johtuen muutettu lainkaan. Tavoitteena oli pystyä käyttämään kyseisiä laitteita myös uudistetussa tietoliikenneverkossa. Yrityksestä löytyi yksi D-Link DGS1210-24 varalaite, jonka avulla konfiguraatiomahdollisuuksia pystyi tutkimaan. Lisäksi vanhempia Cisco Catalyst 2950–48 -laitteita oli käytettävissä 2 kpl, sillä olin hankkinut niitä muutaman aiemmin omaan käyttööni.

Tärkeimmät vaatimukset uudistetun tietoliikenneverkon laitteille olivat seuraavat:

- laitteiden täytyi olla hallittavia
- laitteen täytyi tukea virtuaalisia verkkoalueita (VLAN)
- laitteiden täytyi tukea tietoliikennepakettien merkitsemistä (VLAN Tag)
- laitteiden täytyi tukea usean VLAN:in läpivientiä (VLAN Trunk)
- laitteissa täytyi olla tuki SNMP:lle (valvonta)
- laitteiden olisi hyvä ymmärtää myös 802.1X-protokollaa (hallintaverkko)

Lähiverkkokytkinten osalta tilanne vaikutti olemassa olevia laitteita tutkittaessa hyvältä, sekä Ciscon että D-linkin kytkimistä löytyi tuki vaadituille ominaisuuksil-

le. D-linkin kytkimen manuaali löytyi valmistajan verkkosivuilta ja sen avulla pystyin varmistamaan laitteen tukemat ominaisuudet. Myös Ciscon lähiverkkokytkimiin löytyi hyviä pikaoppaita Ciscon verkkosivuilta.

Laitteiden konfigurointi erosi toisistaan jonkin verran, sillä Ciscon laitteita konfiguroitiin sarjaporttiyhteyden (mahdollisuus myös Telnet- ja SSH-yhteyksiin) kautta, kun taas D-linkin hallinta perustui web-käyttöliittymään. Ciscon laitteiden konfigurointi oli itselleni tuttua, joten D-linkin käyttöliittymää täytyi tutkia hieman testilaitteen avulla. Myös Ciscon laitteiden välisiä eroja täytyi tutkia, sillä Cisco Catalyst 2948G -laitteessa oli muista käytettävissä olevista Ciscon laitteista poiketen CatOS-käyttöjärjestelmä, joka käyttäytyi hieman Cisco IOS:stä poikkeavalla tavalla.

Sopivan WLAN-tukiaseman löytäminen osoittautui suurimmaksi haasteeksi laitesuunnittelun osalta. Koska laitehankinnoissa täytyi varautua tulevaan langattoman verkon laajentamiseen jopa viidellätoista tukiasemalla, oli laitteen hintaluokka pyrittävä pitämään mahdollisimman matalana. Langatonta verkkoa oli tarkoitus koekäyttää tämän opinnäytetyön tulosten perusteella viidellä tukiasemalla ja laajentaa myöhemmässä vaiheessa siten, että verkko kattaisi koko yrityksen tehdasalueen sisätilat. Koska edullisissa WLAN-tukiasemissa ei yleensä ole ainakaan laitevalmistajan käyttöliittymässä tarjolla tietoliikenneverkon uudistuksen kannalta tarpeellisia VLAN TAG ja VLAN Trunking-ominaisuuksia, oli tutkittava muita vaihtoehtoja. Useisiin WLAN-tukiasemiin on mahdollista ladata valmistajan ohjelmistoversion tilalle jokin korvaava ohjelmistoversio, joka sisältää usein alkuperäistä ohjelmistoa laajemman skaalan erilaisia ominaisuuksia. Olin aikaisemmin käyttänyt DD-WRT-nimistä laiteohjelmistoa muutaman erilaisen WLAN-tukiaseman kanssa onnistuneesti, joten lähdin tutkimaan sen käyttömahdollisuutta ensimmäisenä. Testausta varten yritykseltä löytyi kaksi erilaista tukiasemamallia, D-Link DIR-300 sekä Buffalo Airstation N300. Korvasin D-Linkin tukiaseman ohjelmiston DD-WRT:llä ja tutkin muutoksen aiheuttamia vaikutuksia. Web-käyttöliittymän puolella näkyi kyllä muun muassa VLAN-asetuksiin liittyviä valintoja sisältävä sivu, mutta valinnat eivät tallentuneet laitteen muistiin eivätkä vaikuttaneet laitteen toimintaan millään tavalla. DD-WRT:n tukifoorumeita selattuani löysin viestiketjun, jossa neuvottiin määrittelemään

VLAN-asetukset Telnet-yhteyden avulla. Telnet-yhteyden muodostus onnistui lähiverkkokaapelin ja PuTTY-sovelluksen avulla, mutta myöskään tällä tavalla määritellyt asetukset eivät tuntuneet toimivan. D-Link DIR-300-laitteen käyttömahdollisuudet tulevassa ympäristössä vaikuttivat melko huonoilta. Laitemallin vaihto toiseen D-Linkin tukiasemaan (DIR-615) tai Buffalon tukiasemaan eivät tuottaneet tulosta, eikä ongelma tuntunut ratkeavan millään. Kokeilin myös erilaisia DD-WRT:n versioita, tuloksetta.

Lopulta löysin DD-WRT:n tukifoorumia selatessani vihjeen tarkistaa laitemallin käyttämän WLAN-piirin valmistajan. Useat foorumin käyttäjät olivat kertoneet Broadcomin valmistaman piirin sisältävien laitteiden tukevan haluttuja ominaisuuksia. D-Link DIR-300 pohjautuu Atheroksen WLAN-piiriin, joten selitys vaikutti uskottavalta. Sopivaa, Broadcomin piiriin perustuvaa laitetta etsiessäni törmäsin Netgearin WNR3500Lv2-laitteeseen, jonka ominaisuudet vaikuttivat lupaavilta. Laitteen ominaisuuksia sekä ohjelmistotukea tutkiessani huomasin, että kyseiseen laitteeseen oli mahdollista asentaa laitevalmistajan firmwaren tilalle DD-WRT:tä vastaava Tomato-firmware. Tomaton ominaisuuslistauksissa oli mainittu kaikki vaadittavat ominaisuudet ja linksysinfon (7) tukifoorumeilta löytyi aiheeseen liittyviä viestiketjuja. Pyysin yrityksen tietojärjestemäasiantuntijaa tilaamaan kaksi kappaletta Netgearin laitteita koekäyttöä varten.

Laitteiden saavuttua asensin Netgearin ohjelmiston tilalle ensin DD-WRT:n ohjelmiston ja tutkin sen avulla saataville tulleita ominaisuuksia. Kaikkia toteutuksen kannalta olennaisia ominaisuuksia ei pystynyt käyttämään luotettavasti, joten asensin Tomaton ohjelmistoversion laitteeseen. Tomaton ohjelmistoversiolla tarvittavat asetukset ja ominaisuudet toimivat, joten päätimme käyttää kyseistä laitetta ja ohjelmistoversiota.

4.5 IP-suunnittelu

IP-suunnittelu on osa verkkosuunnittelua ja sen avulla pyritään helpottamaan verkonhallintaa sekä parantamaan kuvaa yrityksen verkosta. Hyvin toteutettuna IP-suunnittelulla voidaan myös säästää IP-osoitteita sekä parantaa verkon hallittavuutta. Minimissään IP-suunnittelu tuottaa kuvan yrityksen käyttämistä osoit-

teista ja osoitealueista, ennaltaehkäisten päällekkäisyyksien ja ongelmatilanteiden syntymistä.

Yrityksellä oli olemassa listaus muun muassa julkisista IP-osoitteistaan, mutta suunnitelma oli osittain puutteellinen. Uudessa verkossa oli lisäksi erillisiä verkkoalueita, joten koko verkkosuunnitelma oli syytä tehdä uudelleen. Verkkosuunnitelma päätettiin dokumentoida ensin Excel-taulukkoon, mutta tulevaisuudessa sen ylläpitopaikaksi suunniteltiin keskitettyä dokumentointisovellusta. Taulukkoon kirjattiin ylös jokaisen verkkosegmentin kiinteästi varatut IP-osoitteet ja niiden käyttötarkoitukset sekä verkkojen DHCP-palvelimen jakamat osoitteet. Jokaisen verkkosegmentin osalta pyrittiin käyttämään samanlaista jakoa, jossa osoitealueen alkupää varattiin kiinteästi osoitteita käyttävien laitteiden käyttöön ja loppupää DHCP:llä jaettavaksi.

Myös VLAN-verkkojen VLAN TAG -arvot oli suunniteltava käytössä olevien laitteiden rajoitusten mukaisesti. VLAN TAG on IEEE 802.1Q-standardin mukainen, Ethernet-tietoliikennepaketin kehyksen mukana kulkeva merkintä, jonka avulla eri verkkoalueiden liikenteen IP-paketit voidaan tunnistaa. Käytännössä VLAN TAG-merkityt tietoliikennepaketit kulkevat verkkoliikenteen mukana laitteelta toiselle ja eri VLAN TAG -merkinnän omaavat tietoliikennepaketit eivät voi kohdata toisiaan ilman reitittävän laitteen apua. Langattomien tukiasemien muistirajoituksen vuoksi niiden käyttämien verkkoalueiden VLAN TAG -arvojen oli oltava maksimissaan 16 arvon päässä toisistaan, joten verkon VLAN TAG -arvoiksi päätettiin määritellä taulukossa 1 esitellyt arvot.

VLAN TAG	**VLAN -verkon nimi**	**Verkon käyttötarkoitus**
VLAN 3	Premekon-LAN	Yrityksen oma verkkosegmentti
VLAN 11	Modustep-LAN	Sisaryrityksen verkkosegmentti
VLAN 12	Guest-LAN	Vierasverkon verkkosegmentti
VLAN 15	Management-LAN	Hallintaverkon verkkosegmentti
VLAN 100	DMZ	Optio, ei vielä käytössä

Taulukko 1: VLAN-määritykset

DMZ-verkkoalueen VLAN TAG -arvo määriteltiin kauemmas muista verkoista, sillä sitä ei tarvitse missään pohditussa skenaariossa viedä WLAN-tukiasemille.

Kun verkkoalueet oli saatu suunniteltua, siirryttiin määrittelemään verkkoalueiden IP-osoitealueita. Osoitealueet valittiin VLAN TAG -arvon perusteella 192.168.0.0/16 verkkoalueesta taulukon 2 mukaisesti.

VLAN TAG	Verkkoalue ja verkkomaski	DHCP:n jakama osoitealue
VLAN 3	192.168.3.0 / 255.255.255.0	192.168.3.128 - 254
VLAN 11	192.168.11.0 / 255.255.255.0	192.168.11.128 - 254
VLAN 12	192.168.12.0 / 255.255.255.0	192.168.12.128 - 254
VLAN 15	192.168.15.0 / 255.255.255.0	192.168.15.128 - 254
VLAN 100	192.168.100.0 / 255.255.255.0	

Taulukko 2: Verkkoalueet

4.6 WLAN-tukiasemien sijoittelu ja roaming tukiasemien välillä

Jotta langattoman verkon käyttö olisi saumatonta ja mahdollisimman helppoa, on WLAN-tukiasemat sijoitettava ja niiden asetukset määriteltävä siten, että päätelaitteet kykenevät vaihtamaan tukiasemaa päätelaitetta liikuttaessa automaattisesti. Tukiasemasta toiseen siirtymistä kutsutaan roamingiksi ja oikein toteutettuna tukiaseman vaihtamisesta ei aiheudu näkyvää katkosta verkon käyttöön. Langattomien tukiasemien kantomatkaa mitattiin kannettavan tietokoneen wlan-sovittimen sekä Android-matkapuhelinkäyttöjärjestelmälle asennetun langattomien verkkojen signaalitasoa mittaavan sovelluksen avulla. Mittaustulosten perusteella arvioitiin tukiasemien sijoituspaikat testausta varten.

Ensimmäisessä vaiheessa langatonta verkkoa piti pystyä käyttämään toimiston tiloissa. Myöhemmin verkkoa haluttiin laajentaa myös valmistustiloihin siten, että verkon kantoalue kattaisi koko rakennuksen. Testausvaiheessa kaksi tukiasemaa kiinnitettiin yrityksen toimiston ylemmän kerroksen kattorakenteisiin ja kaksi tukiasemaa sijoitettiin alemman kerroksen huoneiden pöydille. Tukiasemille määriteltiin manuaalisesti kanavavalinnat siten, että tukiasemat asetettiin kanaville 1, 6 ja 11 sijoituspaikkojen mukaisesti. Tällöin kanavaväli on tarpeeksi suuri ja päätelaite ymmärtää vaihtaa tukiasemasta toiseen, päätelaitteen liikkuessa kantoalueen rajalle. Kun laitteita lisätään myöhemmässä vaiheessa myös tuotantotiloihin, on kanavamääritykset asetettava kuuluvuuden perusteella ristiin

siten, että päällekkäisyyksiä ei pääse syntymään. Myös hallin tukirakenteiden vaikutus verkon kuuluvuuteen on tarkistettava verkkoa laajentaessa.

5 Tietoliikenneverkon uudistus, käytännön toimenpiteet

Käytännön toimenpiteet koostuivat seuraavista kokonaisuuksista:

- Laitehankinnat
- Laitteiden asetusten määrittely ja muut asennustoimet
- Uuden verkkoympäristön testaus testikäyttäjien toimesta
- Yliheittovaiheen toimenpiteiden ja aikataulun suunnittelu
- Käyttöönoton toteutus
- Verkkolaitteiden valvonnan määrittely

Valvontaohjelmistona käytetty Nagios-sovellus oli asennettu virtuaalipalvelimelle muun työn ohessa. Nagioksen asennusprosessia ei kuvata tässä dokumentissa, mutta verkkolaitteiden valvonnan määrittelyyn liittyvät asiat on kuvattu perustasolla.

5.1 Resurssit ja laitehankinnat

Laitehankinnat pystyttiin pitämään yrityksen aiempien laitteiden ominaisuuksien johdosta melko vähäisinä, hankittavia laitteita olivat ainoastaan Netgearin WLAN-tukiasemat sekä omasta käytöstäni yli jääneet kaksi Ciscon lähiverkkokytkintä. Ciscon kytkimet lahjoitin yrityksen käyttöön ja Netgearin laitteet tilattiin kahdessa erässä eräästä verkkokaupasta. Ensimmäiset laitteet tilattiin testausvaiheessa ja loput laitteiden yhteensopivuuden varmistuttua. Laitteiden saatavuus näytti tilaushetkellä hyvältä, mutta koska varastosaldot ja saatavuustiedot saattavat muuttua ajan kuluessa, tilattiin laitteita varmuuden vuoksi jo hieman käyttöönottohetken tarvetta useampi.

5.2 Verkkolaitteiden konfigurointi

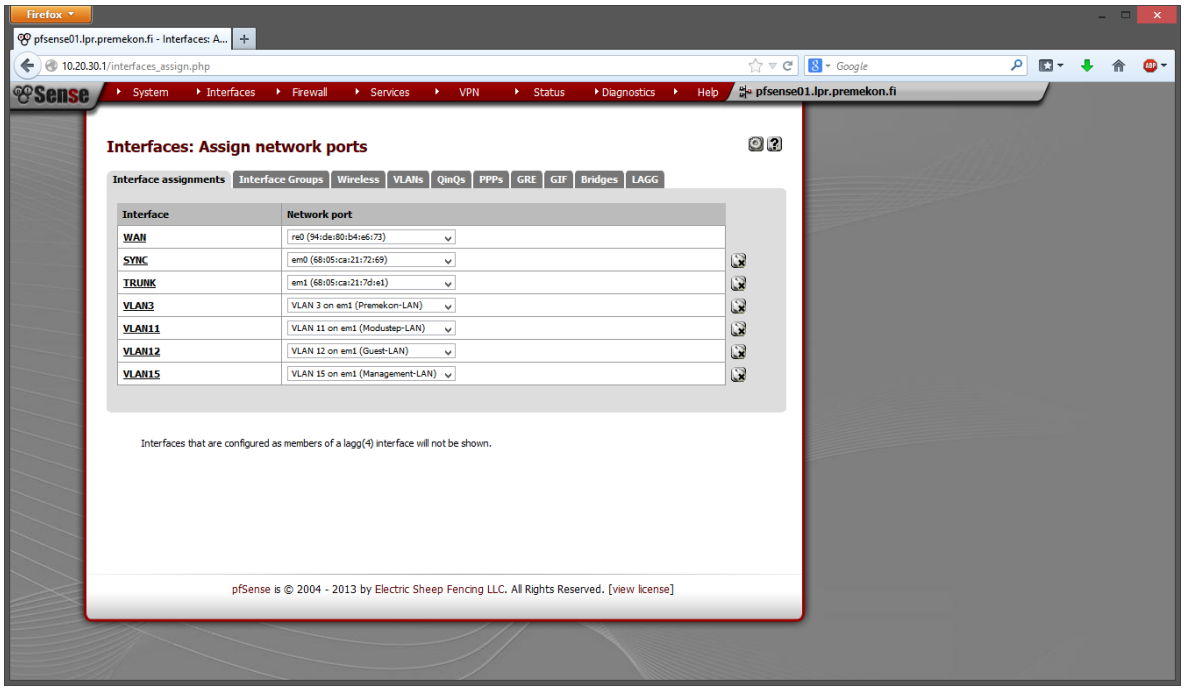
Verkkolaitteiden konfigurointi tuotantokäyttöön tehtiin asteittain, verkon topologian mukaisesti. Ensimmäisenä määriteltiin tarvittavat asetukset vielä tässä vaiheessa testikäytössä olleelle pfsense-palomuurilaiteparille, sitten testikäytössä

olleille lähiverkkokytkimille ja seuraavaksi WLAN-tukiasemille. Aivan viimeisenä, niin sanottuna yliheittoviikonloppuna, tehtiin tarvittavat määrittelyt myös aiemmassa tuotantokäytössä olleille, Ciscon Catalyst sekä D-linkin lähiverkkokytkimille. Lähiverkkokytkinten VLAN-määrittelyistä tehtiin erillinen porttikartta, jossa näkyi selkeästi, mikä kytkinportti oli määritelty mihinkin VLAN-verkkoon. Verkkolaitteiden asetukset ja asennustavat dokumentoitiin yrityksen myöhempää käyttöä varten, esimerkiksi mahdollisen vikatilanteen yhteydessä tapahtuvaa laitevaihtotarvetta ajatellen. Verkkolaitteiden asetusten tärkeimmät määrittelyt on kuvattu seuraavien otsikoiden alla.

5.2.1 pfSense

pfSense -palomuurilaiteparin konfigurointi tapahtui web-käyttöliittymän avulla. Määriteltävät asetukset liittyivät pääasiassa VLAN-verkkojen asetuksiin, CARP-virtuaaliosoitteiden luontiin, DHCP-poolien määrittelyihin, palomuurisääntöjen luontiin sekä FreeRADIUS-asetusten määrittelyyn. Virtuaalisella CARP-osoitteella mahdollistetaan saman IP-osoitteen käyttö kahden reitittävän palomuurilaitteen eri noodien välillä, lisäten vikasietoisuutta. DHCP-poolien avulla määriteltiin palomuurilaitteiden DHCP-palvelinten jakamat osoiteavaruudet, jokaiselle erilliselle verkkosegmentille. FreeRADIUS-palvelun avulla hallintaverkkoon kytkettäviin lähiverkkoportteihin pystyttiin lisäämään erillinen 802.1X -protokollan mukainen verkkoon liittyvän laitteen tunnistaminen, jolloin hallintaverkon väärinkäyttö vaikeutuu.

Testauksen yhteydessä päätettiin rajoittaa vierasverkon liikennenopeutta, joten vierasverkon palomuurisääntöjä varten määriteltiin erillinen rajoitin. Varsinaisia palomuurisääntöjä ei ole tietoturvasyistä dokumentoitu tämän työn liitteeksi, ne on toimitettu yritykselle erillisenä dokumenttina. Palomuurilaitteille luotiin tarvittavat VLAN-verkot *Interfaces → Assign → VLANS* -valikon kautta ja jokaisen VLAN-verkon asetukset määriteltiin IP-suunnitelman mukaisiksi. Kuvassa 2 näkyy pfSensen VLAN-verkkoalueiden luonnissa käytetty tyyli.



Kuva 2: pfSensen verkkoadapterimääritykset

Molemmissa palomuuriparin laitteissa määriteltiin TRUNK-verkkoliitännän alle VLAN:it 3, 11, 12 sekä 15. Jos erillinen DMZ-verkkoalue otetaan tulevaisuudessa käyttöön, lisätään verkkoliitännän alle VLAN100. Palomuurilaitteet jakavat jokaisen VLAN:in osalta oletusyhdyskäytävän osoitteen virtuaalisena CARP IP-osoitteena laitteiden välillä. Esimerkiksi VLAN3:n osalta palomuuriparin ensimmäiselle laitteelle on määritelty osoite 192.168.3.2 ja toiselle laitteelle 192.168.3.3, laiteparin jakama virtuaalinen osoite on 192.168.3.1. Kun verkkomäärityksissä käytetään oletusyhdyskäytävänä osoitetta 192.168.3.1, voidaan kumpi tahansa palomuurilaite sammuttaa ilman että siitä aiheutuu katkoksia liikenteeseen. Laitteet kommunikoivat keskenään SYNC-verkkoliitännän läpi pfsync -tekniikalla. Jos Slave-palomuuri ei saa Master-palomuurilta statustietoa, se olettaa Master-laitteen olevan poissa käytöstä ja alkaa toimia itse Master-laitteena. Kun toinen palomuuriparin laite palaa linjoille, neuvottelevat laitteet roolijakonsa uudelleen.

Lisäksi pfsenselle asennettiin FreeRADIUS-lisäpaketti ja määriteltiin sen asetukset lähiverkon tunnistautumista ajatellen sopiviksi. pfSensen asetusten tarkempi määrittely on kuvattu erillisenä projektina toteutetun kahdennetun pfsense -palomuurikokonaisuuden käyttöönottodokumentaatiossa, joka on toimitettu yritykselle omana kokonaisuutenaan.

5.2.2 Cisco IOS

Cisco Catalyst 2950G -sarjan kytkimissä on IOS-käyttöjärjestelmä, joten konfigurointi kytkimen ollessa tehdasasetuksilla aloitetaan konsolikaapelin sekä terminaalisovelluksen avulla. Koska nykyaikaisissa kannettavissa työasemissa ei ole enää sarjaporttiliitäntää, käytin konsoliyhteyden muodostamiseen USB-sarjaporttisovitinta sekä PuTTY-sovellusta. Kun konsoliyhteys saadaan muodostettua, voidaan kytkimen asetukset määritellä siten, että kytkimeen pääsee kiinni myös telnet ja SSH-protokollalla lähiverkkoyhteyden läpi. Lähiverkkokytkimet oli testausvaiheessa palautettu tehdasasetuksille ja perusasetukset oli määritelty laitteille käsin. Laitteille täytyi luoda VLAN-verkkoalueet sekä määritellä kytkinporteille niiden käyttämät VLAN:it.

Käytännössä VLAN-verkkojen luonti toteutettiin komennoilla:

```
cata02# vlan database
cata02(vlan)# vlan 3 name Premekon-LAN
VLAN 3 added:
   Name: Premekon-LAN
cata02(vlan)# vlan 11 name Modustep-LAN
VLAN 11 added:
   Name: Modustep-LAN
cata02(vlan)# vlan 12 name Guest-LAN
VLAN 12 added:
   Name: Guest-LAN
cata02(vlan)# vlan 15 name Management-LAN
VLAN 15 added:
   Name: Management-LAN
```

Lisäksi kytkinporttien määrittelyt haluttuihin VLAN-verkkoihin toteutettiin komennoilla:

```
cata02# configure terminal
cata02(config)# interface range FastEthernet 0/17 - 32
cata02(config-if-range)# switchport mode access
cata02(config-if-range)# switchport access vlan 3
cata02(config-if-range)# exit
cata02(config)# interface range FastEthernet 0/33 - 38
cata02(config-if-range)# switchport mode access
cata02(config-if-range)# switchport access vlan 11
cata02(config-if-range)# exit
cata02(config)# interface range FastEthernet 0/39 - 44
cata02(config-if-range)# switchport mode access
cata02(config-if-range)# switchport access vlan 12
cata02(config-if-range)# exit
cata02(config)# interface range FastEthernet 0/45 - 48
cata02(config-if-range)# switchport mode access
cata02(config-if-range)# switchport access vlan 15
cata02(config-if-range)# exit
```

```
cata02(config)# interface range FastEthernet 0/17 - 48
cata02(config-if-range)# spanning-tree portfast
cata02(config-if-range)# end
```

Configure terminal -komento siirtää käyttäjän konfigurointimoodiin ja *interface range FastEthernet 0/17 - 32* -komento valitsee portit 17 - 32 konfiguroitaviksi. Komento *switchport mode access* määrittää portit VLAN:in jäsenporteiksi ja *switchport access vlan* 3 määrittelee portit VLAN3-verkkoon. Sama toistettiin porteille 33 - 38, 39 - 44 sekä 45 - 48, eri VLAN-määrityksiä käyttäen. Lopuksi kaikille access-porteille komennettiin *Spanning-tree portfast* -komennolla porttien spanning-tree -asetukset siten, että portit eivät neuvottele kytkinportin tilaa vastapuolen laitteen kanssa, vaan siirtyvät suoraan access-porteiksi.

Jotta kaikille kytkimille ei tarvitsisi luoda VLAN:eja manuaalisesti, hyödynnettiin Ciscon kytkimissä valmistajan Virtual Trunkin Protocol (VTP)-määrityksiä. Ensisijaisella kytkimellä määriteltiin VTP domain sekä sen salasana ja määriteltiin kytkin VTP palvelimeksi:

```
cata02# configure terminal
cata02(config)# vtp mode server
cata02(config)# vtp domain vtp_domain_example
cata02(config)# vtp password secret_password_example
cata02(config)# end
```

Tämän jälkeen muut kytkimet voitiin lisätä VTP-domainiin, jolloin kytkimet hakevat VLAN-määritykset VTP-palvelimena toimivalta kytkimeltä. Jos verkkoon halutaan lisätä uusi VLAN, määritellään se VTP-palvelimeksi konfiguroidulla kytkimellä, jolloin myös VTP-clienteiksi määritellyt kytkimet oppivat uuden VLAN:in. Muita lähiverkon Cisco-kytkimiä konfiguroidessa määriteltiin kytkimet VTP-clienteiksi ja syötettiin kytkimille VTP-domainin tiedot:

```
cata03# configure terminal
cata03(config)# vtp mode client
cata03(config)# vtp domain vtp_domain_example
cata03(config)# vtp password vtp_password_example
cata03(config)# end
```

Lähiverkon kytkinten väliset ja kytkimestä palomuurilaitteelle kytketyt portit konfiguroitiin 802.1Q (VLAN Trunk) -porteiksi ja sallittiin porttien liikennöidä VLAN:it 3, 11, 12 ja 15 verkkojen osalta:

```
cata02# configure terminal
cata02(config)# interface range FastEthernet 0/1 - 16
```

```
cata02(config-if-range)# switchport mode trunk
cata02(config-if-range)# switchport trunk allowed vlan 3,11,12,15
cata02(config-if-range)# end
```

Muut tarvittavat määrittelyt ja kytkinkonfiguraatiot on dokumentoitu erikseen tarkemmalla tasolla yrityksen käyttöä varten. Vikatilanteesta palautumista varten kytkinten asetukset voi siirtää vastaavaan laitemalliin, joko määrittelemällä asetukset käsin tai rakentamalla verkkoon TFTP- tai FTP-palvelimen ja kopioimalla asetukset talteen. Kopiointi onnistuu komentamalla kytkimeltä *copy tftp* tai *copy ftp* ja syöttämällä pyydetyt tiedot. FTP:tä käytettäessä täytyy kytkimille lisätä FTP-palvelimen käyttäjätiedot (käyttäjänimi ja salasana), jotta kytkin kykenee kirjautumaan palvelimelle asetuksia siirtäessä (8). Kytkinkonfiguraatioiden varmistukset TFTP- tai FTP-palvelimille on kirjattu yhtenä kehitysehdotuksena kehityskohdelistalle.

5.2.3 Cisco CatOS

Cisco CatOS -käyttöjärjestelmä on erillinen, tietyissä kytkinmalleissa käytetty käyttöjärjestelmäversio, jota ei enää nykyään kehitetä. Se perustuu alun perin Crescendo Communications -nimisen yrityksen kehittämään XDI-nimiseen käyttöjärjestelmään, josta tuli myöhemmin CatOS, Ciscon ostettua Crescendon liiketoiminta itselleen. CatOS-käyttöjärjestelmällä varustetun kytkimen asetusten määrittely poikkeaa hieman IOS:n asetusmäärittelyistä. Perusajatus on sama, mutta komennoissa ja toimintalogiikassa on eroja. Esimerkiksi VTP client -määrittelyt komennettiin seuraavalla tavalla:

```
cata01> (enable) set vtp domain vtp_domain_example
cata01> (enable) set vtp passwd vtp_password_example
cata01> (enable) set vtp mode client
```

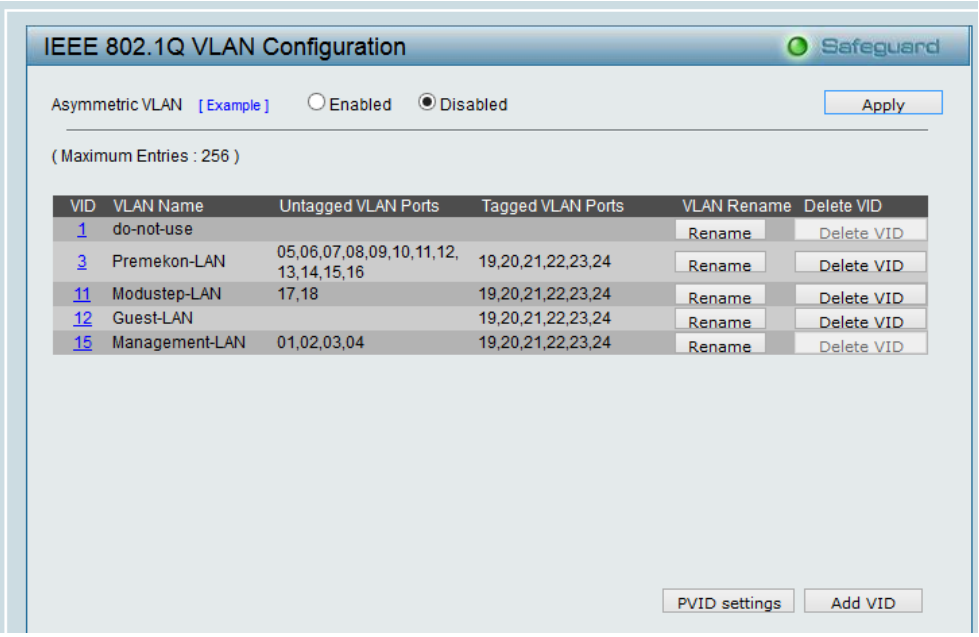
Porttien 2-4 määrittelyt 802.1Q Trunk -porteiksi, porttien 17–48 määrittely työasemien ja palvelinten käyttämiksi accessporteiksi VLAN 3:een sekä access-porttien 17–48 spanningtree portfast -määrittelyt toteutettiin komennoilla:

```
cata01> (enable) set trunk 2/2 on 3,11,12,15
cata01> (enable) set trunk 2/2 on dot1q
cata01> (enable) set trunk 2/3 on 3,11,12,15
cata01> (enable) set trunk 2/3 on dot1q
cata01> (enable) set trunk 2/4 on 3,11,12,15
cata01> (enable) set trunk 2/4 on dot1q
cata01> (enable) set vlan 3 2/17-48
cata01> (enable) set spantree portfast 2/17-48 enable
```

Ciscon internetsivuilta ladattu *Quick Software Configuration Guide* -opas (9) on lisäksi toimitettu yritykselle myöhempää käyttöä varten.

5.2.4 D-Link DGS1210-24

D-linkin kytkinten asetuksia pääsi muokkaamaan kirjautumalla kytkimen web-hallintaan internetselaimella. Kytkimille määriteltiin tarvittavat 802.1Q VLAN -asetukset kuvan 3 mukaisesti.



Kuva 3: D-Linkin kytkimen VLAN-määritykset

Portit 19-24 määriteltiin Tagged-porteiksi (vrt. 802.1Q Trunk Ciscon kytkimissä) VLAN 3, 11, 12 ja 15 osalta, muut portit määriteltiin tarpeiden mukaisesti sopiviin VLAN-verkkoihin access porteiksi. Vierasverkon VLAN vietiin kytkimille Tagged -portteja ja WLAN-tukiasemia ajatellen, mutta yhtäkään porttia ei D-Linkin kytkimissä määritelty vierasverkon accessportiksi.

Kaikkien kytkinten porttimääritykset dokumentoitiin myöhempää käyttöä varten erilliseen taulukkoon, jotta tietoihin pääsisi helposti käsiksi ilman kytkimelle kirjautumista. Kehityskohteena kytkinten konfiguraatioiden tarkasteluun liittyen kirjattiin verkkolaitekonfiguraatioita esimerkiksi SNMP:llä lukevan sovelluksen käyttöönottotarve, jotta verkkolaitteiden asetuksia voisi tutkia keskitetysti reaaliajassa.

5.2.5 Netgear (tomato)

Langatonta verkkoa suunnitellessa ja testatessa päädyttiin käyttämään Netgearin 3500Lv2 WLAN-tukiasemaa, johon asennettiin alkuperäisen ohjelmiston tilalle tomato-niminen käyttöjärjestelmä. Tomatoa käyttämällä Netgearin edullisesta tukiasemasta saatiin käyttöön sellaisia ominaisuuksia, joita Netgearin alkuperäinen ohjelmistoversio ei tukenut. Esimerkiksi erillisiä virtuaalisia WLAN-verkkoja ja niiden liikenteen ohjausta tiettyyn VLAN:iin ei pystynyt Netgearin ohjelmistolla tekemään, mutta tomaton firmwaren avulla tämä onnistui.

Suunnitteluvaiheessa todettiin, että ohjelmistopäivitys täytyi tehdä DD-WRT firmwaren avulla. Netgearin tukiaseman oman ohjelmiston tilalle asennettiin ensin DD-WRT:n ohjelmisto ja sen jälkeen DD-WRT:n päälle Tomaton ohjelmistoversio. Jos päivitystä yritti tehdä suoraan Netgear → Tomato, ei päivitys onnistunut.

Ohjelmistovaihdoksen jälkeen tukiasemien asetukset määriteltiin verkon rakenteen mukaisiksi. Laitteen LAN - br0 -verkkosovittimelle määriteltiin kiinteä IP-osoite hallintaverkosta, jotta laite pystyy kommunikoimaan hallintaverkon kanssa oikein. Jokaista VLAN:ia varten luotiin oma silta ja sille määriteltiin osoite verkkosegmentistä. Sillat sidottiin VLAN-määrityksiin kuvassa 4 näkyvällä tavalla.

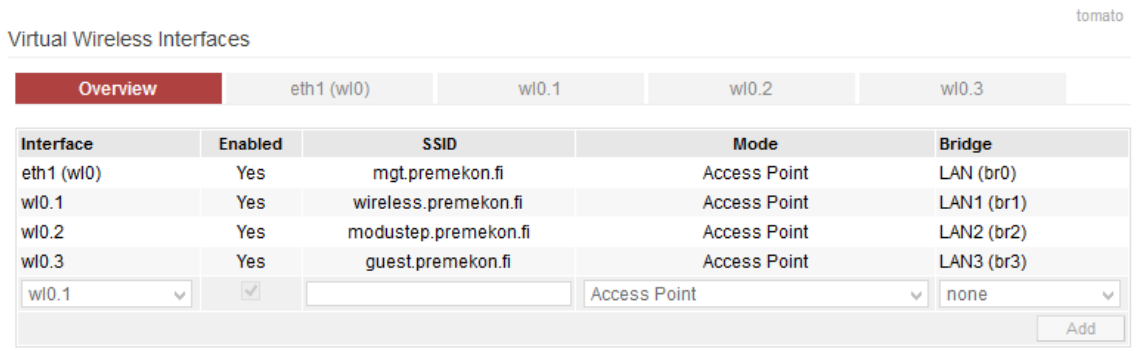
VLAN

VLAN ▲	VID	Port 1	Tagged	Port 2	Tagged	Port 3	Tagged	Port 4	Tagged	WAN Port	Tagged	Default	Bridge
1	1							Yes				*	
2	2									Yes			WAN
3	3	Yes	On			Yes							LAN1 (br1)
11	11	Yes	On										LAN2 (br2)
12	12	Yes	On										LAN3 (br3)
15	15	Yes	On	Yes									LAN (br0)
0	0	☐		☐		☐		☐		☐			none

Add

Kuva 4: Netgearin VLAN- ja porttimääritysten asetukset (Tomato)

VLAN:it 1, 3, 11 ja 15 määriteltiin Tagged-asetuksella (VLAN TAG) laitteen ensimmäiseen verkkoporttiin ja jokaiseen VLAN:iin määriteltiin silta. Lisäksi laitteelle luotiin langattomat verkot jokaista verkkoaluetta varten ja ne kiinnitettiin sopiviin verkkosiltoihin kuvan 5 mukaisesti.



Kuva 5: Netgearin WLAN-VLAN -sidossuhdeasetukset (Tomato)

Näiden asetusten avulla verkkoliikenne pystyttiin sitomaan tietystä WLAN-verkosta tiettyyn VLAN:iin. Tarkemmat ohjelmiston asennusohjeet sekä laitteiden konfigurointiohjeet dokumentoitiin erikseen yrityksen käyttöä varten ja toimitettiin myöhempää käyttöä varten tietojärjestelmäasiantuntijalle.

5.3 Testaus

Testausvaiheessa testikäyttäjien työasemat sekä muun työn ohessa uusittu tiedostopalvelin kytkettiin uuden tietoliikenneverkon testilaitteisiin. Testikäyttäjinä toimivat pääasiassa sisaryrityksen käyttäjät, mutta myös yrityksen omia työasemia ja liikennöintiä testattiin uudessa verkossa tietojärjestelmäasiantuntijan sekä oman testityöasemani avulla. Työasemien verkkoasetuksissa vaihdettiin verkkoasetusten automaattinen haku päälle ja DHCP:n toimivuutta testattiin eri verkkosegmenteissä. Verkkoalueiden välistä liikennettä, liikenteen läpimenoon vaikuttavia verkkoalueiden välisiä palomuurisääntöjä sekä verkon nopeutta testattiin erilaisten testitapausten avulla. Muutamia esimerkkitapauksia olivat:

- DHCP-asetusten testaus ja DHCP:n käyttöönotto työasemilla
- Liikenteen toimivuus julkiseen verkkoon
- Sisäverkon palveluiden toimivuus (saman vlanin sisällä)
- Liikenteen toimivuus sisaryrityksen vlanista yrityksen vlanissa sijaitseville palvelimille (palomuurisäännöt)
- Liikenteen suodatus liikennöidessä vierasverkosta muihin vlaneihin (palomuurisäännöt)
- Toisen palomuurikoneen sammutuksen vaikutus (vikasietoisuuden testaus)

Testien aikana ei huomattu käyttöönottoon vaikuttavia puutteita tai muita kriittisiä toimimattomuuksia. Palomuurisääntöjä määriteltiin hieman alkuperäistä suunnitelmaa tarkemmalla tasolla ja vierasverkon liikennenopeutta päätettiin rajoittaa pfSensen avulla siten, että vierasverkon liikennekapasiteetti rajattiin kymmenesosaan yrityksen 20M/20M -liittymän kapasiteetistä. Liikennerajoitukseen liittyvä Limiter-rajoitus määriteltiin pfSensen *Firewall → Traffic Shaper → Limiter* -valikon kautta. Lisäksi rajoitin sidottiin vierasverkon liikenteen palomuurisääntöihin. Tämän jälkeen rajoitusta testattiin käytännössä liittämällä kaksi testityöasemaa vierasverkkoon ja ajamalla nopeustestiä sekä lataamalla noin 100MB testipakettia verkon yli.

Koska testitapaukset osoittivat uuden verkon toimivan halutulla tavalla, varsinaista käyttöönottoa voitiin alkaa aikatauluttaa.

5.4 Käyttöönotto

Varsinainen käyttöönotto sovittiin aloitettavaksi perjantaina 4.4.2014. Työt päätettiin aloittaa heti työntekijöiden lähtiessä viikonlopun viettoon, sillä käyttöönoton suunnittelun yhteydessä oli arvioitu yliheiton ja sen yhteydessä toteutettavien muiden muutosten läpiviennin kestävän useita tunteja. Töiden valmistumisen takarajana pidettiin sunnuntai-iltaa, sillä yrityksen tuotannon oli jatkuttava maanantaiaamuna normaalisti.

Verkon yliheiton suunnitelma koostui seuraavista vaiheista:

1. kytkinten ja palomuurin välisten kytkentöjen sekä liikenteen toimivuuden tarkistus
2. aiemmassa verkossa olleiden kytkinten asetusten muuttaminen uuden konfiguraation mukaiseksi
3. verkkokytkentöjen ja kaapelointien muutokset, kytkinten välisten linkkien kahdennus
4. verkkolaitteiden asetus- ja kytkentämuutosten jälkeinen testaus
5. verkkolevypalvelinten siirto uuteen verkkoon, verkkoasetusten muutokset
6. työasemien verkkoasetusten muutokset
7. tulostimien ja muiden verkon aktiivilaitteiden siirto uuteen verkkoon, verkkoasetusten muutokset

8. palveluiden toimivuuden testaus
9. vanhojen, tarpeettomiksi jääneiden laitteiden purku

Verkon yliheiton yhteydessä toteutettiin samalla myös vanhan verkkolevypalvelimen tiedostojen lopullinen kopiointi uudelle ja uuden palvelimen asetusten jako työasemille. Vanha verkkolevypalvelin jätettiin varmuuskopiokäyttöön ja sille asetettiin uuden verkkoalueen mukaiset asetukset.

Mahdollisten ongelmatilanteiden varalle tehtiin myös lyhyt rollback-suunnitelma, joka perustui vanhan palomuurilaitteen verkkoon palauttamiseen sekä alkuperäisten kytkinkonfiguraatioiden palauttamiseen. Toimenpiteet olisivat olleet verkkolaitteiden osalta yksinkertaisia, sillä lähiverkkokytkimet olisi palautettu tehdasasetuksille ja kaapeloitu takaisin vanhaan palomuurilaitteeseen.

5.5 Valvonta

Verkkolaitteiden ja muiden verkon resurssien valvonta toteutettiin Nagios -valvontaohjelmistolla. Valvonnan perustasoksi määriteltiin ICMP Ping -valvonta, joka tarkistaa vastaako laite Internet Control Message Protocol (ICMP) -määritelmän mukaiseen Ping -pakettiin. Tällä tasolla valvottaessa nähdään onko laite ylipäänsä verkossa ja kykeneekö se liikennöimään perustasolla. Lisäksi lähiverkon kytkimille määriteltiin myös SNMP-protokollaa hyödyntävää valvonta porttitason tietoja ajatellen. SNMP, eli Simple Network Management Protocol on TCP/IP-pohjaisissa tietoliikenneverkoissa yleisesti käytettävä verkkolaitteiden hallintaprotokolla, jonka avulla voidaan esimerkiksi lukea verkkolaitteiden asetustietoja suoraan laitteelta. SNMP:n toiminta perustuu laitteille määriteltävään SNMP yhteisötietoon (SNMP community) ja sen hyödyntämiseen tietoja käsittelevän sovelluksen avulla. Laitteille määritellään lähes poikkeuksetta kaksi yhteisötunnusta, read- ja write -tason tunnukset. Read-tason tunnuksella voidaan vain lukea asetuksia, write-tason tunnuksella voidaan myös ylikirjoittaa aiempia asetuksia.

Jokaista verkkolaitetyyppiä varten luotiin Nagioksen asetustiedostoihin sopivat skannausasetukset, määrittelemällä muun muassa skannattavan laitteen nimi sekä IP-osoite, jota skannataan. Lähiverkon verkkolaitteille määriteltiin sama SNMP-ryhmämääritys asetusten lukemista varten ja kyseinen ryhmä lisättiin

Nagioskonfiguraatioissa verkkolaitteen skannausasetuksiin. Laitteiden sidossuhteet määriteltiin asetustiedostoihin, jotta Nagios osaa piirtää topologiakuvan laitteiden hierarkiasta.

Valvontasovelluksen toimivuutta testattiin muun muassa määrittelemällä yksittäisen lähiverkkokytkimen tietty lähiverkkoportti statusvalvontaan ja ottamalla verkkokaapeli irti kyseisestä portista. Portin statustiedon muuttuminen aiheutti hälytyksen ja kaapelin takaisinkytkentä palautti statustiedon normaaliksi.

6 Jatkokehitys ja varautuminen tulevaisuuden tarpeisiin

Jatkokehityksen ja tulevaisuuden tarpeisiin varautumisen osalta työn suunnittelu- ja toteutusvaiheessa kirjattiin ylös muutamia kehityskohteita ja rakenteellisia puutteita. Kohteet on esitelty lyhyen selostuksen kera seuraavien otsikoiden alla.

6.1 Dokumentaatiojärjestelmän käyttöönotto

Yrityksellä ei ole käytössään dokumenttienhallintajärjestelmää tai tarkemmin sovittua dokumentaatiotapaa esimerkiksi tietoliikenneverkon laitteiden, verkon palveluiden tai muiden tarpeellisten osa-alueiden dokumentointia varten. Esimerkiksi virtuaalipalvelimelle asennettava Mediawiki, phpmyfaq, Atlassian Confluence tai joku muu web-pohjainen sovellus, jonka avulla tieto voidaan tallentaa järkevässä muodossa verkkoon, helpottaisi dokumentaation hallintaa ja parantaisi palveluiden hallittavuutta. Lisäksi dokumentaatiojärjestelmä parantaisi palveluiden käyttäjien mahdollisuuksia ratkaista yleisimpiä ongelmatilanteita itsenäisesti dokumentaation perusteella ja kannustaisi kehittämään niin sanottua Knowledge Base -tietovarastoa työn tueksi.

6.2 Microsoft Active Directory -hakemistopalveluiden käyttöönotto

Nykyinen työryhmäpohjainen ratkaisu on erittäin työläs ja hankala ylläpitää, varsinkin muutostilanteissa. Työasema- ja palvelinlaitemäärän kasvaessa ongelma tulee entistä ajankohtaisemmaksi. Hakemistopalvelun ja keskitetyn hallinnan avulla helpotettaisiin toimialueen työasemien, tunnusten ja muiden asetusten päivittäistä ylläpitoa. Koska yrityksen käyttämille työasemille on asennettu pää-

asiassa Microsoft Windows -käyttöjärjestelmien uusimpia versioita, olisi Microsoft Server -tuoteperheen tarjoama Active Directory Domain Services -tuote luonnollisin ja helppokäyttöisin valinta toiminnan tueksi. Myös lähiverkkoon liitettävien laitteiden tunnistaminen ja vain toimialueen työasemien salliminen yrityksen omaan verkkosegmenttiin voidaan toteuttaa Microsoft Windows Server -tuoteperheen ratkaisujen avulla, FreeRADIUS-palvelun tapaan.

6.3 Virtuaalipalvelinten siirto oikealle palvelinraudalle

Nykyiset työasemaraudalla toteutetut palvelimet ovat varsinaiseen palvelinrautaan verrattuna epävakaampia, eikä palvelimia ole palomuuriparia lukuun ottamatta kahdennettu. Mahdollisessa vika- tai ongelmatilanteessa palvelimen hajoaminen voi aiheuttaa yrityksen toimintakyvyn alentumisen tai halvaantumisen. Palvelinten läpikäynti ja luokittelu sekä kriittisimpien palvelinten kahdennus parantaisi toipumismahdollisuuksia. Esimerkiksi HP:n Microserver-tuoteperheen edulliset ja pienet palvelimet voisivat olla sopiva ratkaisu, mikäli palvelimia hankittaisiin vähintään kaksi ja kriittiset palvelut kahdennettaisiin kahdelle erilliselle fyysiselle alustalle.

6.4 Varavirtasyötön rakentaminen

Verkon kriittiset pisteet, kuten palomuurilaitteet, lähiverkkokytkimet sekä palvelimet olisi syytä suojata sähkökatkoilta ja virtapiikeiltä. Kahdennettujen laiteparien eri laitenoodien kytkennät olisi syytä sijoittaa eri sulakkeiden takana olevien kytkentöjen taakse. Tällöin ongelmatilanteessa lyhyt sähkökatkos ei aiheuttaisi koko verkon kaatumista.

6.5 Tukipyyntöjen ja kehitysideoiden käsittely

Pienimuotoisen tikettijärjestelmän ja FAQ tai Knowledge base -tyylisten ratkaisujen avulla tukipyyntöjen määrää sekä yleisten ongelmatilanteiden ratkaisutietokantaa olisi mahdollista kasvattaa ja samalla pienentää tietojärjestelmäasiantuntijan työkuormaa. Tukipyyntöjen määrän ja laadun seuranta on olennainen osa jatkuvaa palvelun parantamista, joten tukipyynnöstä ja sen käsittelystä pitäisi saada selkeää dataa.

6.6 Verkkolaitteiden konfiguraatiotietoa lukeva sovellus

Esimerkiksi Nedi-nimisen verkon aktiivilaitteiden asetuksia SNMP-protokollan avulla lukevan sovelluksen käyttöönotto helpottaisi laitteiden asetusten tutkimista vikatilanteessa. Samalla laitteiden asetustietojen varmuuskopiointi olisi mahdollista automatisoida.

6.7 Valvontasovelluksen uusiminen ja valvonnan jatkokehitys

Valvontasovelluksen mahdollinen uusiminen, Nagioksen korvaaminen Icingalla (10) tai muulla uudemmalla versiolla, mahdollistaisi uusien ominaisuuksien käyttöönoton. Myös palvelinten valvontaa olisi syytä määritellä tarkemmalle tasolle ja hyödyntää palvelimelle erikseen asennettavan valvontakomponentin mahdollistamaa lisävalvontaa. Tällöin esimerkiksi levytilan täyttyessä valvonta-agentti kykenisi ilmoittamaan lähestyvästä ongelmatilanteesta ennen levyn täyttymistä.

6.8 Lähiverkon kytkimien varalaitemenettelyn huomiointi

Lähiverkon kytkimen vikaantuessa vain D-Linkin lähiverkkokytkimille löytyy yritykseltä yksittäinen varalaite. Muiden laitemallien osalta varalaitteita ei ole, mutta niille on saatavilla korvaavia, eri laitevalmistajan vastaavilla ominaisuuksilla varustettuja laitteita. Haasteita laitevalmistajan ja laitteen käyttöjärjestelmän vaihtuessa voi tuottaa laitteen konfiguraation sovittaminen vanhan ja uuden laitteen välillä. Yksittäisten varalaitteiden hankkiminen myös Ciscon lähiverkkokytkinten osalta pienentäisi ongelmatilanteesta palautumiseen kuluvaa aikaa.

7 Yhteenveto ja pohdinta

Tietoliikenneverkon yliheittovaihe sujui ongelmitta ja liikenne toimi laitteiden välillä. Suurimpia haasteita yliheittovaiheessa olivat CatOS-käyttöjärjestelmällä varustetun Ciscon lähiverkkokytkimen asetusten määrittely sekä työasemien asetusten manuaalisesta muuttamisesta sekä testaamisesta aiheutunut työmäärä. CatOS-kytkimen konfiguraatiota ei ollut varalaitteen puuttumisesta johtuen mahdollista testata ennen yliheittoa, mutta yliheiton asetusmuutosten jälkeen ei kuitenkaan havaittu ongelmia. Työasemien verkkoasetukset muutettiin

verkkosuunnitelman mukaisiksi yksitellen, eikä muutoksia tehdessä havaittu ongelmia.

Uudistetun lähiverkon nopeus yllätti yrityksen työntekijät positiivisesti, nopeuden muutos oli havaittavissa esimerkiksi tiedostopalvelinta käytettäessä. Vaikka palomuurisääntöihin jouduttiin tekemään jälkikäteen pieniä korjauksia, eivät segmentoinnin jälkeiset rajoitukset häirinneet työntekoa. Pääasiassa muutos onnistui kaiken kaikkiaan sujuvasti. Tavoitteet saavutettiin ja kehitysehdotukset toimitettiin yritykselle jatkokehitystä varten.

Verkon segmentointi erillisiin VLAN-virtuaaliverkkoihin osoittautui toimivaksi ratkaisuksi. Kahdennettu palomuuripari toimi hyvin vikasietoisena verkon reitityspisteenä ja kykeni rajoittamaan verkkoalueiden välistä liikennettä sekä vierasverkon kapasiteettiä halutulla tavalla. Yksittäisen palomuurilaitteen sammuttaminen kesken käytön ei aiheuttanut loppukäyttäjille näkyvää katkosta verkon liikenteeseen.

Kuvat

Taulukot

Lähteet

1. ITIL v3 taskukirja, Zaltbommel: Van Haren Publishing 2009

2. www.mitre.org, IT Service Management: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/enterprise-technology-information-and-infrastructure/it-service-management Luettu huhtikuussa 2015

3. ITILv3, palvelustrategia, Wakaru: https://www.wakaru.fi/etusivu/lue-lisaa/itil3/palvelustrategia Luettu huhtikuussa 2015

4. ITILv3, palvelusuunnittelu, Wakaru: https://www.wakaru.fi/etusivu/lue-lisaa/itil3/palvelusuunnittelu Luettu huhtikuussa 2015

5. ITILv3, palvelutransitio, Wakaru: https://www.wakaru.fi/etusivu/lue-lisaa/itil3/palvelutransitio Luettu huhtikuussa 2015

6. ITILv3, jatkuva palvelun parantaminen, Wakaru: https://www.wakaru.fi/etusivu/lue-lisaa/itil3/jatkuva-palvelun-parantaminen Luettu huhtikuussa 2015

7. Linksysinfo.org -tukifoorumi: http://www.linksysinfo.org/index.php?forums/tomato-firmware.33/

8. Ciscon kytkinkonfiguraation backup-toiminnon määrittely: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-122-mainline/46741-backup-config.html

9. Quickstart-opas Cisco CatOS:lle: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/quick/software/guide/quicksw.pdf

10. Icinga
https://www.icinga.org/

Kuva 1: (Timo Hyvönen - OGC, Wikipedia: http://fi.wikipedia.org/wiki/ITIL#/media/File:Itil3.jpg)