Opinnäytetyö YAMK

Teknologiaosaamisen johtamisen koulutusohjelma

YTEJOS16

2017

Tomi Lehtonen

MODERNIN TIETOLIIKENNEVERKON SUUNNITTELU SAIRAALAYMPÄRISTÖÖN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ YAMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Teknologiaosaamisen johtamisen koulutusohjelma

Huhtikuu 2017 | 48

Tomi Lehtonen

MODERNIN TIETOLIIKENNEVERKON SUUNNITTELU SAIRAALAYMPÄRISTÖÖN

Tietoliikenneverkkoon liitettävien laitteiden määrä kasvaa koko ajan sekä uusia laitevalmistajia ilmaantuu markkinoille. Vaatimukset tietoliikenneverkkoa kohtaan kasvavat, mutta keskeisemmät suunnittelutavoitteet sairaalaympäristössä toimivaan verkkoon säilyvät. Verkkoon on taattava toimintavarmuus, luotettavuus ja huollettavuus. Verkkosuunnittelussa pitää ottaa huomioon, että palvelut ja järjestelmät ovat aina käytettävissä riippumatta vuorokauden ajasta tai päivästä.

Opinnäytetyön tavoitteena oli kerätä kokemusperäistä tietoa, jota pysytään jatkossa hyödyntämään tulevissa sairaalaverkon laajennuksissa. Lisäksi opinnäytetyössä analysoitiin VAHTI-sisäverkko-ohjeen tarkistuslistoja nykyiseen verkkototeutukseen. Analysoinnissa löydetyt poikkeamat loivat pohjan asiantuntijahaastatteluiden aiheille, joissa kerättiin tietoa, miten tulevat verkkolaajennukset tulee suunnitella.

Tämä opinnäytetyö oli laadultaan kvalitatiivinen tutkimus ja opinnäytetyö suoritettiin yhteistyössä Medbitin Varsinais-Suomen ja Satakunnan sairaanhoitopiirien verkkoasiantuntijoiden kanssa. Tutkimusmetodeja olivat haastattelut, palaverit, keskustelut sekä kirjatutkimus.

Tutkimuksen tuloksena löytyi kehityskohteita verkkosuunnitteluun mm. verkkosegmentoinnin ja päätelaitteiden tunnistautumisen osalta. Lisäksi haastatteluiden tuotoksena saatiin kehityskohteita toimintatapoihin, joita tässä opinnäytetyössä ei tarkemmin lähdetty analysoimaan.

Sairaalaverkko tullaan auditoimaan VAHTIn tarkistuslistoja vastaan. Tutkimustulosten perusteella nykyinen sairaalaverkko täyttää pääosin sille asetetut vaatimukset. Sairaalaverkon segmentointia tulee jatkossa parantaa, jotta sairaalaverkko täyttää sille asetetut vaatimukset. Tulevissa suunnitteluissa tulee ottaa myös huomioon verkkoon liitettävien päätelaitteiden tunnistautuminen.

ASIASANAT:

Verkkosuunnittelu, sairaalaverkko, verkkosegmentointi, vaatimustenhallinta, kvalitatiivinen tutkimus, VAHTI-sisäverkko-ohje

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Technology Competence Management

April 2017 | 48 pages

Tomi Lehtonen

DESIGN OF A MODERN NETWORK IN A HOSPITAL ENVIRONMENT

A wide range of various devices will need a network connection to operate nowadays. New equipment manufacturers will enter the market. The requirements for network design are growing, but still the most important design rules apply when designing a network in a hospital environment. The network must guarantee operational reliability, provide the appropriate level of redundancy and tolerate maintenance operations. The network must maintain user access to services and applications all the time.

The aim of the present master's thesis is to gather the best practices and knowledge based information from previous network designs. Network specialists were interviewed to achieve this goal. Deviation analysis between the current network design and the requirements was conducted as part of the thesis. The structure of the specialist interviews was based on these findings.

The present thesis is qualitative in nature and the study was conducted in close co-operation with Medbit network specialists in the hospital districts of Southwest Finland and Satakunta. The research methods used were interviews, meetings, discussions and literature studies.

As a result, some development areas in the current network architecture, such as improvement needs in network segmentation and device authentications, were identified. In addition, some development ideas concerning the practices and daily operations were gathered as part of the interviews. These development ideas were, however, not analyzed in the context of this thesis.

Network design will be audited against VAHTI network guide in the near future. The current network design will meet most of the requirements. A major deviation point against the network requirements is in the network segmentation area, which will have to be improved in order to meet the requirements and, in addition, device authentication needs to be taken into account when designing new network expansions.

KEYWORDS:

Network design, hospital network, network segmentation, requirement management, qualitative research

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET

ACL	Access Control List
CAT5 / CAT6	Category 5 cable / Category 6 cable
CCNA	Cisco Certified Network Associate
DICOM	Digital Imaging and Communications in Medicine
HL7	Health Level Seven
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
PACS	Picture archiving and communication systems
PoE	Power over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RTLS	Real-Time Location System
SDN	Software-Defined Network
VAHTI	Valtiohallinnon tietoturvallisuuden johtoryhmä

VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSL	Virtual Switch Link
VSS	Virtual Switch System
VSSHP	Varsinais-Suomen sairaanhoitopiiri
WAN	Wide Area Network
WiSM2	Wireless Service Module 2
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

1 JOHDANTO

Elämme aikaa, jossa yhä useampi laite tullaan liittämään internetiin. Nykyinen verkkoinfrastruktuuri mahdollistaa esineiden internetiin (Internet of Things) liittyvän tiedon keräämisen, tallentamisen ja jakamisen. Jatkuva nettiyhteys ja esineiden internetiin liittyvät pilvipalvelut ovat oleellinen osa kokonaisuutta, koska kerättävä data on tallennettava paikkaan, josta se voidaan edelleen jakaa muille laitteille. Esineiden internetiin liittyviä laitteita on nykyään useita, esimerkiksi jääkaappi, pesukone tai televisio, mikäli ne vain täyttävät yleiset verkkovaatimukset. Tämä kehitys heijastuu osittain myös sairaaloiden verkkosuunnitteluun, mistä yhä useampi päätelaite tullaan liittämään sairaalaverkkoon.

Opinnäytetyössä perehdytään modernin tietoliikenneverkon suunnitteluun kuvaamalla sairaalaverkon nykytilaa. Verkkosuunnittelun kuvaus perustuu Varsinais-Suomen sairaanhoitopiirin (VSSHP) verkkoarkkitehtuuriin. Tulevaisuudessa suunniteltavat verkkolaajennukset on tarkoitus liittää osaksi kyseistä verkkorakennetta. Suunnittelussa tulee ottaa huomioon yhteensopivuus nykyiseen tietoliikenneverkkoon, uudet päätelaitteet sekä asiakkaan asettamat verkkovaatimukset. Suunnittelutyötä ohjaa vahvasti valtiovarainministeriön asettama VAHTI-sisäverkko-ohje, jonka tavoitteena on yhtenäistää menettelyitä sisäverkkojen rakentamisessa sekä tukea sopivan tietoturvatason käyttöönottoa organisaatioissa (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Taustatieto pohjautuu pääosin kirjaston lähdeaineistoon, jossa hyödynnettiin CCNA-kurssien (Cisco Certified Network Associate) kirjallisuutta. Kirjallisuuden tukena käytettiin internethakuja ja aihetta sivuavia opinnäytetöitä.

Aija Lindman käsittelee diplomityössään teollisen internetin, IoT:n ja Big datan testausta ja liiketoimintamahdollisuuksia. Työssään hän toteaa uusien järjestelmien ja digitalisaation murroksen tuovan uusia vaatimuksia, jotka kohdistuvat varsinkin järjestelmien integrointiin, turvallisuuteen ja datan oikeellisuuteen (Lindman 2016). Tämä muutos on myös nähtävissä, kun suunnitellaan modernia tietoliikenneverkkoa sairaalaympäristöön. Tietoliikenneverkkoon liitettävien laitteiden määrä kasvaa koko ajan sekä uusia laitevalmistajia ilmaantuu markkinoille. Vaatimukset tietoliikenneverkkoa kohtaan kasvavat, mutta keskeisemmät tavoitteet sairaalaverkon suunnittelulle säilyvät. Verkkoon on taattava toimintavarmuus, luotettavuus ja huollettavuus. Verkkosuunnittelussa pitää ottaa huomioon, että palvelut ja järjestelmät ovat aina käytettävissä riippumatta vuorokauden

ajasta tai päivästä. Tämä asettaa erityisvaatimuksia sähkönsyötölle, laitetiloille, kulunvalvonnalle, verkon ylläpidolle sekä ympärivuorokautiselle tuen saatavuudelle. Näitä edellä mainittuja kohtia ei tässä työssä käsitellä vaan keskitytään tietoliikenneverkon suunnitteluun.

2010-luvun puolella suurimmat verkkoyhtiöt, kuten Cisco, ovat tuoneet markkinoille omat ratkaisunsa ohjelmallisesti määriteltävistä verkoista, SDN (Software-Defined Network). Ohjelmallisesti määriteltävien verkkojen tarkoitus on vastata nykypäivän verkkohaasteisiin. Pilvessä tapahtuva tietojenkäsittely ja palveluiden saatavuus vaativat verkolta skaalattavuutta, joustavuutta ja nopeaa muutoskykyä. Reaaliaikaisen datan käyttö video- ja äänisovellusten kautta asettavat palvelun laadulle, QoS, nopeastikin muuttuvia haasteita (Cisco Systems Inc. 2014).

Thomas Paradis käsittelee laajasti omassa diplomityössään ohjelmallisesti määriteltävien verkkojen toimintaperiaatteita. Työssään hän toteaa, että verkkojen toimintaperiaate on yksinkertainen: kontrollitasolla verkon ylläpitäjä voi asettaa ohjelmallisesti verkon toiminnallisuuden muuttamalla dynaamisesti verkon rajapintoja niin, että ne täyttävät verkkoarkkitehtuurin vaatimukset. OpenFlow protokollan avulla verkon rajapintoja voidaan kontrolloida (OSI-mallin tasot 2 – 4: Ethernet, IP, TCP/UDP…) ja määrittää miten kyseinen verkon aktiivilaite, kuten kytkin, käsittelee datapaketin. Kontrollitaso pystyy hyödyntämään verkon resursseja, kuten tietokantoja ja hakemistopalveluja LDAP:n välityksellä (Lightweight Directory Access Protocol), käyttämään apuna palvelimia taaten muunneltavissa olevan, joustavan, skaalautuvan ja suorituskykyisen verkon aktiivilaitteen (Paradis 2014). Ohjelmallisesti määriteltävät verkot eivät ole varteenotettava vaihtoehto modernin sairaalaverkon suunnittelun pohjaksi, johtuen erilaisista vaatimuksista ja laitekannasta ja siksi ovat tämän opinnäytetyön ulkopuolella.

Opinnäytetyön tavoitteena on kerätä kokemusperäistä tietoa, jota pysytään jatkossa hyödyntämään tulevissa sairaalaverkon laajennuksissa. Lisäksi opinnäytetyössä pyritään vertailemaan VAHTIn tarkistuslistoja nykyiseen verkkototeutukseen ja löytämään poikkeamia, joita pitää ottaa huomioon tulevissa verkkolaajennuksissa.

Sairaalaverkon nykytilan arviointi pohjautuu VAHTIin, jonka tukena käytettiin yrityksen sisäisiä dokumentteja sekä asiantuntijoiden kanssa käytyjä keskusteluita ja haastatteluita. Haastatteluiden pohjaksi valittiin kvalitatiivinen tutkimus. Tutkimukset toteutettiin henkilöhaastatteluina, joissa haastateltiin verkkoasiantuntijoita Varsinais-Suomen sairaanhoitopiirin alueelta. Haastatteluiden pohjalta tehdystä yhteenvedosta valittiin kolme

keskeisintä aihealuetta. Näihin valittuihin aihealueisiin perehdyttiin tarkemmin erillisen jatkohaastattelun yhteydessä. Jatkohaastattelu pidettiin verkkotapaamisena, johon osallistui asiantuntijoita Varsinais-Suomen ja Satakunnan sairaanhoitopiiristä.

Tutkimuskysymykseen haettiin laajuutta taustamateriaaleja ja sairaalaverkon nykyistä verkkoarkkitehtuuria tutkimalla. Tutkimusten kautta havaittiin poikkeamia VAHTIn vaatimuksien ja nykyisen verkkoarkkitehtuurin välillä. Näiden havaintojen pohjalta esitettiin tutkimuskysymys:

Mitä hyviä käytäntöjä ja kokemuksia aikaisemmista verkkolaajennuksista voidaan soveltaa uusien verkkojen suunnittelussa?

Mitä parannuksia tulevissa verkkolaajennuksissa tulee tehdä?

Haastattelu jaettiin kolmeen eri osa-alueeseen: verkkosegmentointi ja tietoturva, verkon aktiivilaitteet sekä laitetilat ja kaapelointi. Jokaista osa-aluetta laajennettiin tarkentavilla kysymyksillä, joilla pyrittiin saamaan kaikki kokemusperäinen tieto kerättyä asiantuntijoilta.

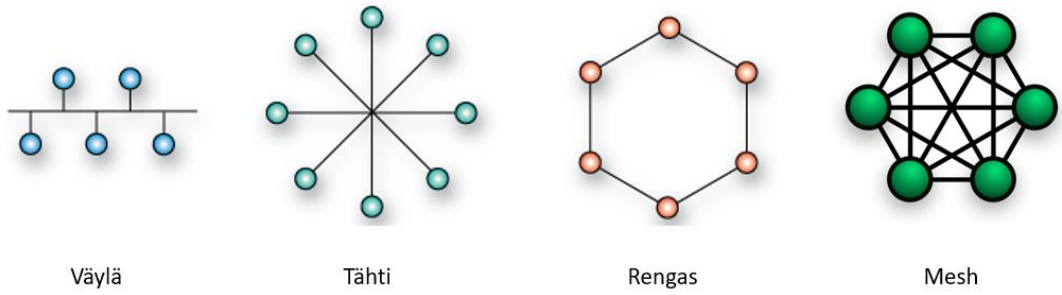
Opinnäytetyö vastaa tämän hetken tilannetta verkkosuunnittelun osalta. Opinnäytetyössä tehtyjä havaintoja voidaan hyödyntää tulevissa verkkolaajennuksissa. Kannattaa kuitenkin huomioida, että verkkoarkkitehtuuri saattaa muuttua tulevaisuudessa, jolloin on syytä analysoida verkon tila uudelleen. Tutkimuksessa havaitut hyvät käytännön kokemukset ovat silti hyödynnettävissä tulevaisuudessakin.

2 SAIRAALAVERKKO

Lähiverkkojen perustavoitteita ovat datan ja resurssien jakamisen sekä käyttäjien välisen viestinnän mahdollistaminen. Lähiverkon palveluita käytetään yhä enemmän etäyhteyksien kautta maantieteellisesti pitkienkin yhteyksien yli. Yksittäisellä organisaatiolla on myös useampia toimipisteitä, jotka verkkoarkkitehtuurisesti ovat yhtä ja samaa verkkoa. Tässä osiossa selvitetään yleistä teoriaa tietoliikenneverkon hierarkkisesta rakenteesta sekä verrataan sitä VSSHP:n tietoliikenneverkon rakenteeseen.

2.1 Hierarkkinen tietoliikenneverkko

Tietoverkolla on tarkoitus liittää yhteen verkon aktiivilaitteita, joilla mahdollistetaan tiedonsiirto eri päätelaitteiden välillä. Tietoverkon perusrakenne koostuu solmuista ja solmuja toisiinsa liittävistä yhteysväleistä. Solmupisteet ovat yleensä reitittimiä, kytkimiä tai langattomia tukiasemia. Tietoverkon kannalta solmut ja yhteysvälit muodostavat verkon topologian. Yleisimmin käytettyjä verkkotopologioita ovat väylä-, tähti-, rengas- ja mesh-topologiat (kuva 1).

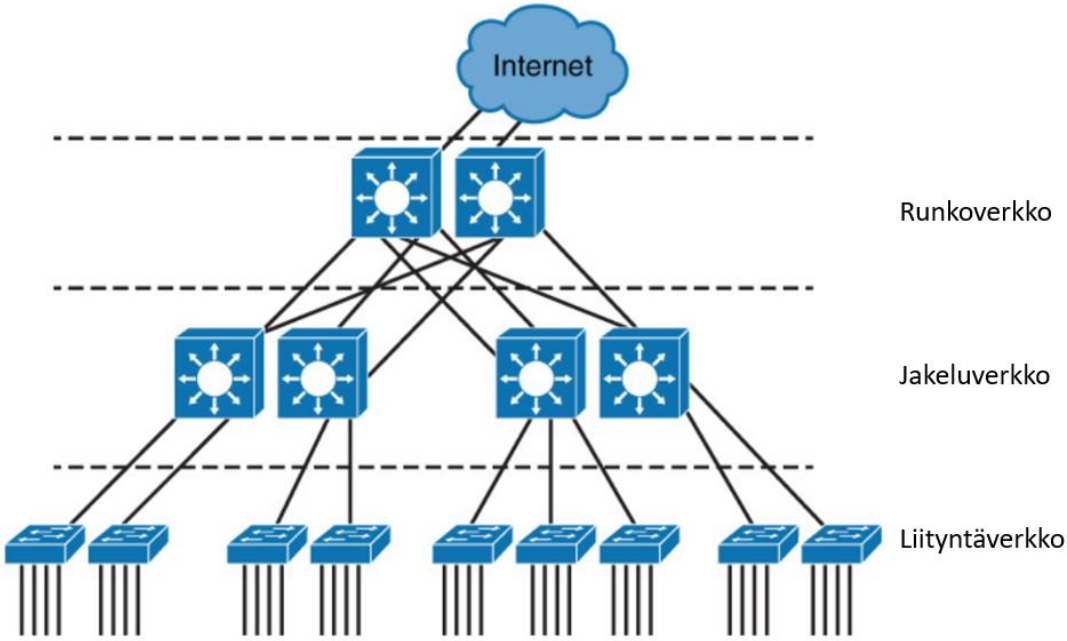


Kuva 1. Verkkotopologioiden yleisimmät mallit.

Verkkotopologiaa valittaessa on syytä miettiä verkon modulaarisuutta, joustavuutta ja skaalattavuutta. Rengastopologia saattaa olla helpoin toteuttaa ja laajentaa, kun taas mesh-topologialla saavutetaan paras vikasietoisuus. Verkkoa laajennettaessa rengastopologialla toteutetussa verkossa konfigurointityö kohdistuu vain naapurisolmuihin, kun taas mesh-topologialla toteutetussa verkossa konfigurointityö kohdistuu kaikkiin solmu-

pisteisiin. Tähtiverkkotopologia on yleisesti käytetty verkkotopologia, jossa solmupisteiden välisten yhteyksien kahdentamisella saadaan kohtuullisen hyvä vikasietoisuus samalla kuitenkin säilyttäen verkon joustavuus ja modulaarisuus (Sosinsky 2009).

Hierarkkisella tietoliikenneverkolla tarkoitetaan rakennetta, jossa verkko on jaettu toiminnallisiin tasoihin. Hierarkkisella rakenteella parannetaan verkon modulaarisuutta, joustavuutta sekä skaalattavuutta. Hierarkkinen verkko muodostuu runkoverkosta (engl. core layer), jakeluverkosta (engl. distribution layer) ja liityntäverkosta (engl. access layer) (Froom, Frahim 2015).



Kuva 2. Hierarkkinen lähiverkon rakenne (Academy 2014).

Liityntäverkolla tarkoitetaan verkon tasoa, jossa tarjotaan laitteille ja käyttäjille pääsy verkon tarjoamiin palveluihin ja toimintoihin. Tähän tasoon tullaan liittämään kaikki langallisen verkon päätelaitteet, kuten esimerkiksi tietokoneet, tulostimet, IP-puhelimet sekä langattoman verkon tukiasemat. Yleisesti liityntäverkkotasolla olevien kytkimien ja jakeluverkkotason kytkinten välinen yhteys on kahdennettu. Tällä pyritään takaamaan palvelujen saatavuus vikatilanteen ilmentyessä. Tämän verkkotason tarkoitus on myös yhdistää LAN-verkkoon erityyppiset verkonosat, kuten PoE-verkkoa käyttävät IP-puhelimet sekä langattoman verkon muodostavat WLAN-tukiasemat. Liityntäverkon kytkinten porttiasetuksien avulla pystytään luomaan perustason tietoturvaa, kuten esimerkiksi MAC-osoitteeseen perustuva tunnistaminen (Froom, Frahim 2015).

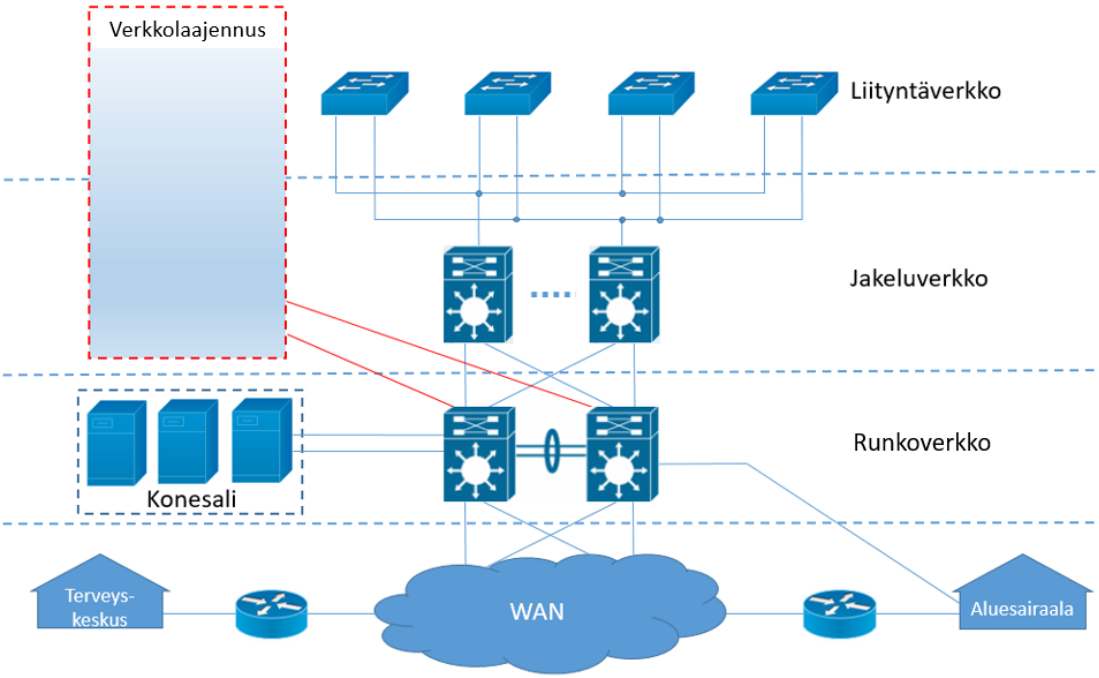
Jakeluverkon tehtävänä on kerätä liityntäverkon laitteilta tuleva data ja toimia reitittävänä rajapintana runkoverkon ja liityntäverkon välillä. Verkkopalvelujen saatavuus, nopea reitin palautuminen, kuorman tasaus ja palvelun laadun takaaminen ovat keskeisimpiä asioita jakelutasoa suunniteltaessa. Verkkopalvelujen keskeytymätön saatavuus pitkälti rakentuu kahdennettujen verkkoyhteyksien varaan. Tämä verkkoyhteyksien kahdennus tulee ottaa huomioon rakennusten sisäistä kaapelointia tehdessä. Jakelutason tarkoitus on usein myös reitittää dataliikennettä eri virtuaaliverkkojen (VLAN) välillä. Jakeluverkon kytkinten avulla voidaan edelleen tehostaa reititystä käyttämällä liityntäverkossa summaosoitetta kattamaan useamman VLAN-aliverkon (Froom, Frahim 2015).

Runkoverkossa kootaan yhteen kaikki verkon elementit. Se toimii rajapintana verkon tarjoamiin peruspalveluihin, kuten sähköposti, intranet, datatallennuspalvelut, ja ulkoiseen laajaverkkoon (WAN). Runkoverkon tarkoituksena on taata korkea vikasietoisuus- ja palautumiskyky yllättäville verkkomuutoksille. Tämänkaltaisia verkkomuutoksia saattavat olla vikaantuneen komponentin, kuten kytkimen, sähkönsyötön tai kaapeloinnin, aiheuttamat vikatilanteet. Verkon on myös taattava jatkuva toiminta tarvittavien komponentti- tai ohjelmistopäivitysten ajaksi. Tästä syystä runkoverkkoon ei yleensä luoda tarkkoja verkkokäytäntöjä tai siihen ei liitetä suoraan palvelimia tai päätelaitteita (Froom, Frahim 2015).

2.2 Sairaalaverkko VSSHP:n alueella

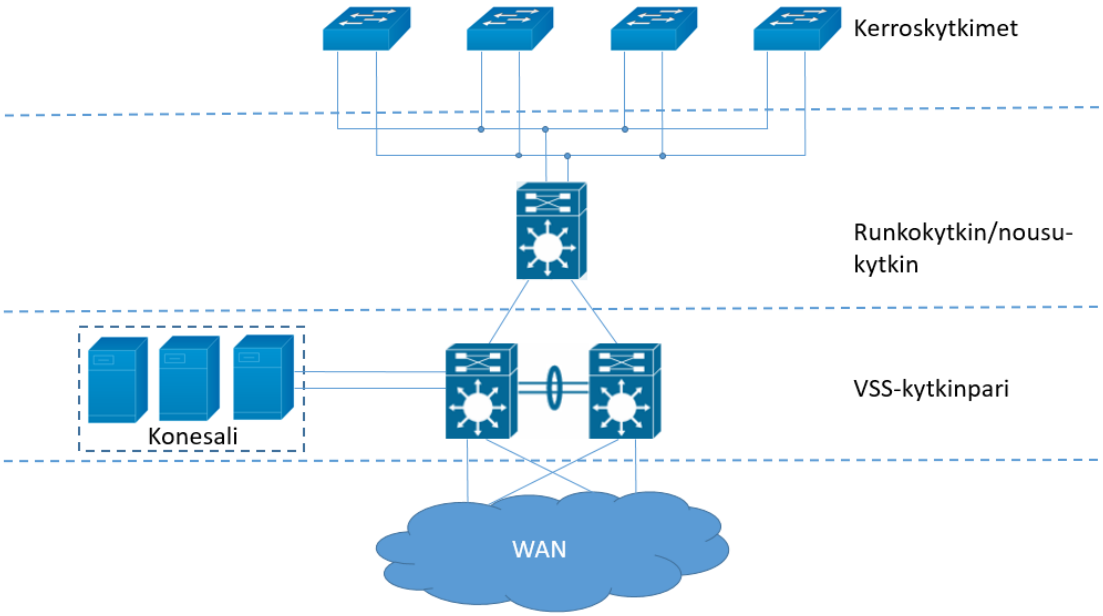
Varsinais-Suomen sairaanhoitopiirin alueella toimiva sairaalaverkko muodostuu Turun alueella toimivien sairaalarakennusten ja terveyskeskusten paikallisverkosta, toisten kaupunkien, kuten Salo tai Loimaa, alueella toimivien aluesairaaloiden paikallisverkoista sekä pienten alueiden terveyskeskusten muodostamista paikallisverkoista. Nämä sairaalaverkon osat liittyvät runkoverkon kautta toisiinsa. Alimman verkkotason muodostavat VSS-kytkinpari (Virtual Switch System), jonka kautta sairaalaverkon eri osat saavat käyttöönsä verkon peruspalvelut kuten potilastietojärjestelmät, sähköpostin, intranetin sekä käyttäjätietokanta- ja hakemistopalvelun (Active Directory).

Sairaalaverkon laajennustyöt kohdistuvat suurelta osin jakeluverkkoon ja liityntäverkkoon. Jakeluverkon osalta määritellään liityntätapa, jolla uusi laajennus tullaan liittämään nykyiseen sairaalaverkkoon runkokytkimen kautta. Liityntäverkko muodostaa loppukäyttäjärajapinnan, joka rakentuu sairaalarakennuksen sisäisistä kerroskytkimistä sekä langattomasta verkosta.



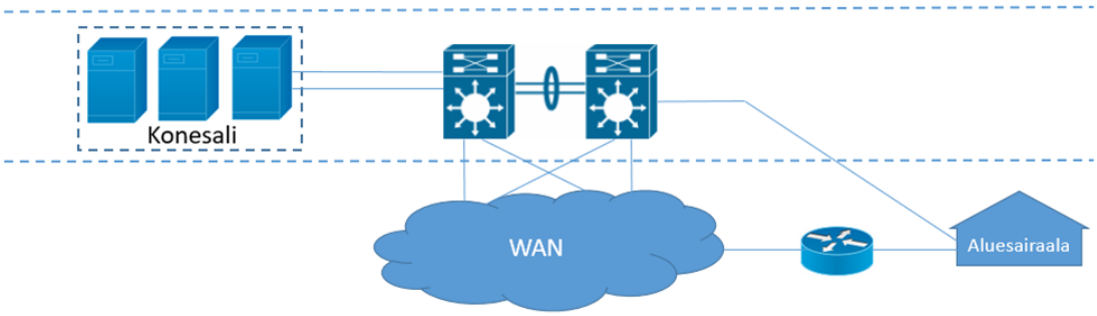
Kuva 3. Sairaalaverkon periaatekuva.

Turun alueella toimivat sairaalarakennukset ja terveyskeskukset liittyvät VSSHP:n sairaalaverkkoon runkokytkimen kautta VSS-kytkinparille. Yhteys runkokytkimen ja VSS-kytkinparin välillä on kahdennetut LACP-kanavilla (Link Aggregation Control Protocol) muodostettu valokuituyhteys. LACP-kanava on toteutettu yhdistämällä kaksi fyysistä porttia yhdeksi loogiseksi kanavaksi. Yhden LACP-kanavan nopeus on 2*10Gbps, jolloin kahdennetun kanavan tiedonsiirtokapasiteetti on 40Gbps. Valokuituverkko on osa VSSHP:n rakentamaa ja ylläpitämää tietoliikenneverkkoa. Rakennusten sisäisen verkko muodostuu runkokytkimestä, sekä siihen liitetyistä kerroskytkimistä. Kerroskytkimet toimivat rajapintana päätelaitteille ja tarjoavat niille tarvittavat palvelut sairaalaverkon konesaleissa sijaitsevilta palvelimilta. Runkokytkimen ja kerroskytkinten välinen yhteys on myös toteutettu valokuidulla käyttäen edellä mainittuja LACP-kanavia. Kaikki kuituyhteydet ovat kahdennettuja kuituyhteyksiä vikasietoisuuden parantamiseksi. Lisäksi valokuidut kulkevat eri reittiä verkon aktiivilaitteiden välillä. Tällä pyritään entisestään parantamaan verkon vikasietoisuutta.



Kuva 4. Yhden sairaalarakennuksen paikallisverkko.

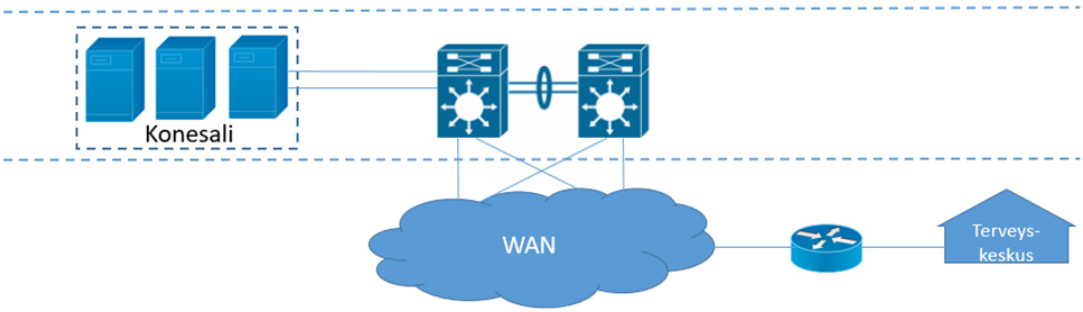
VSSHP:n alueella toimivat aluesairaalat, kuten Salon aluesairaala, ovat liitettyinä sairaalaverkkoon operaattorilta vuokratun valokuidun välityksellä. Vuokratun valokuidun kautta kulkee vain kyseisen aluesairaalan ja VSS-kytkinparin välinen liikenne. Aluesairaala saa VSS-kytkinparin kautta konesalin tarjoamat palvelut käyttöönsä. Edellä mainittu valokuituyhteys on varmennettu operaattorilta tilatun vuokraliittymän kautta. Varayhteydessä aluesairaala ja VSS-kytkinpari on yhdistetty reitittimien kautta toisiinsa, jolloin reitittimien välisessä yhteydessä kulkee myös muuta tietoliikennettä sairaaloiden välisen dataliikenteen lisäksi.



Kuva 5. Sairaalaverkko toiseen aluesairaalaan.

Joissain tapauksissa järkevin tapa liittää pienet terveyskeskukset sairaalaverkkoon on tehdä se vuokraliittymän kautta. Tällöin yhteys toimii samalla periaatteella kuin aluesai-

raalan varayhteys. Jos kuituyhteyttä ei ole saatavilla kyseiseen terveyskeskukseen, yhteys voidaan muodostaa myös käyttämällä LTE-reititintä ja muodostaa yhteys mobiiliverkon kautta. Varayhteydessä käytetyn LTE-reitittimen mobiiliyhteyttä voidaan parantaa käyttämällä kahden eri operaattorin datayhteyttä. Tällöin tietoliikenneverkko ei ole riippuvainen yhden operaattorin tarjoamista palveluista. Tämä ratkaisu on käytössä liikkuvissa sairaanhoitoyksiköissä, kuten esimerkiksi ambulansseissa. Molemmissa tapauksissa terveyskeskus liittyy VSS-kytkinparin kautta konesalin tarjoamiin palveluihin.



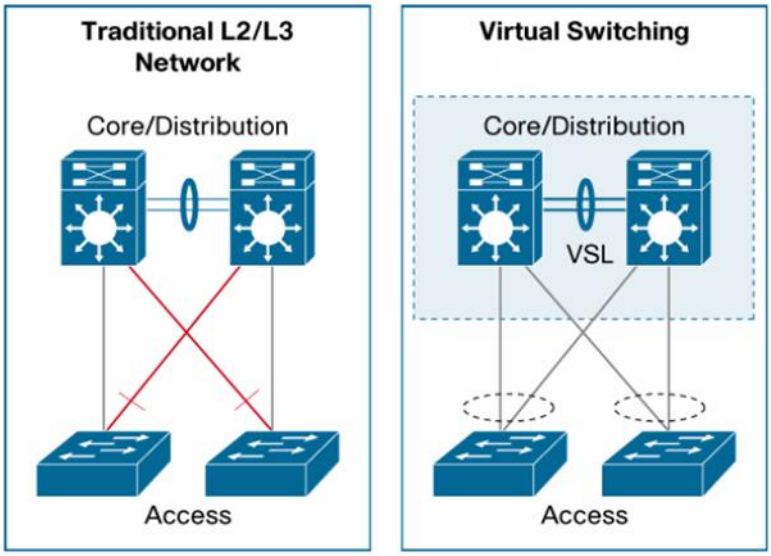
Kuva 6. Sairaalaverkko pieneen terveyskeskukseen.

VSSHP:n verkkorakenteesta voidaan havaita samat hierarkkiset verkkotasot kuin yleiskuvauksessa esitetyt. Jokainen verkkotaso on suunniteltu VAHTIn toimintaperiaatteen mukaisesti (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010). VAHTIa käsitellään tarkemmin myöhemmissä luvuissa. Käytössä oleva verkko on helposti skaalautuva ja siksi uuden sairaalarakennuksen liittäminen nykyiseen verkkoon aiheuttaa vain pieniä muutoksia sisäverkon VSS-kytkinparille. Uuden rakennuksen suunnittelussa tulee ottaa tarkoin huomioon yhteensopivuus olemassa olevaan verkkoon sekä asiakkaan verkkoon kohdistamat vaatimukset.

2.3 Sairaalaverkon toimintaperiaate

Runkoverkko rakentuu VSS-kytkinparin ympärille. VSS-kytkinparin kautta koko sairaalaverkko liittyy operaattorin tuomaan ulkoiseen internetyhteyteen, WANiin, sekä verkkopalveluihin, kuten potilastietojärjestelmiin, sähköpostiin, intranetiin sekä käyttäjätietokanta- ja hakemistopalveluihin. VSS-kytkinpari on Ciscon patentoima ratkaisu, jossa kaksi fyysistä kytkintä muodostavat yhden loogisen kytkimen. Kytkinpareina toimii Cisco Catalyst 6500 -sarjan kytkimet, jotka ovat liitettyinä toisiinsa VSL-linkin (Virtual Switch

Link) avulla. VSS-kytkinparit ovat sijoitettuina fyysisesti eri tiloihin, millä pyritään minimoimaan suurten vikatilanteiden, kuten tulipalon tai viemäreiden tulvimisesta aiheutuvien katkosten tuoma haitta. Toisen kytkimistä ollessa aktiivinen (Virtual Switch Active) on toinen kytkin valmiustilassa (Virtual Switch Standby). Aktiivinen kytkin kontrolloi kytkinten välistä kommunikointia ja kytkinparin toimintaa. Molemmat kytkimet kuitenkin osallistuvat aktiivisesti datan välittämiseen eteenpäin.



Kuva 7. Perinteinen kahden kytkimen verkkoratkaisu verrattuna VSS-kytkinparin ratkaisuun (Cisco Systems Inc. 2009b).

Yhden loogisen kytkimen rakenteella saavutetaan muutamia etuja kahden kytkimen ratkaisuun verrattuna. VSS-kytkinpari näkyy hallinnan kannalta yhtenä kytkimenä, jolloin konfigurointi on helpompaa. Samalla verkon skaalattavuus paranee, koska modulaarisen rakenteen kannalta VSS-kytkinpari muodostaa yhden 18-moduulipaikan rungon verrattuna kahteen 9-moduulipaikan runkoon. Yhdellä loogisella kytkimellä voidaan optimoida paremmin verkon kaistan käyttöä ja kuorman tasausta ja näin saavuttaa parempi verkon suorituskyky. Lisäksi mahdollisissa aktiivisen kytkimen vikatilanteissa parin toinen kytkin ottaa kytkinparin hallinnan minimoiden viasta aiheutuneen haitan, jolloin verkon vikasietoisuus paranee (Cisco Systems Inc. 2009a).

Jakeluverkon rakenne saattaa vaihdella toteutuksen osalta eri rakennuksissa VSSHP:n toimialueella. Uudempien rakennuksien jakeluverkon runkokytkin on toteutettu VSS-kytkinparilla, jonne on koottu liityntäverkon asiakasrajapinnan hoitavat kytkimet kahdennet-

tujen valokuituyhteyksien kautta. Vanhemmissa rakennuksissa jakeluverkon runkokytkimeen on liitettyinä sarja nousukytkimiä, joiden takana toimivat liityntäverkon asiakaskytkimet. Opinnäytetyössä on tarkoitus kerätä kokemusperäistä tietoa ja verkkovaatimuksia liittyen jakeluverkon ja liityntäverkon suunnitteluun. Tämänkaltaisia vaatimuksia ovat esimerkiksi yhteensopivuus olemassa olevaan sairaalaverkkoon, toimintavarmuus, vikatilanteesta toipuminen sekä huollettavuus ja ylläpito. Sairaalaverkko auditoidaan VAHTIa vastaan, jolloin kyseisen ohjeen vaatimukset ovat perustana verkon suunnittelulle. Vaatimustenhallintaa on kuvattuna tarkemmin opinnäytetyön myöhemmissä kappaleissa.

2.4 Sairaalaverkon segmentointi

VSSHP:n verkkosegmentointi perustuu rakenteeseen, jossa verkko on jaettu osiin niihin liitettyjen päätelaitteiden mukaan. Yksi segmentti pitää sisällään useampia virtuaaliverkon osia. VLAN-määritykset (Virtual Local Area Network) tullaankin tekemään tarpeen mukaan, johon osittain vaikuttavat esimerkiksi rakennuksen kerroskoot sekä liitettävät päätelaitteet. Verkon segmentoinnissa pitää ottaa huomioon voidaanko uusi laite liittää nykyiseen verkkosegmentointirakenteeseen vai pitääkö luoda uusi verkkosegmentti. Tulevaisuuden haasteena ovat IoT-laitteet, joita tullaan liittämään sairaalaverkkoon. IoT-laitteiden tietoturvaa ei välttämättä pystytä takaamaan, jolloin niille tarkoitettu verkkosegmentti on hyvä loogisesti irrottaa varsinaisesta sairaalaverkosta.

Verkon segmentoinnissa tulee ottaa huomioon myös tietoturva-asiat. Tietoturvan kannalta olisi hyvä rajoittaa päätelaitteiden pääsy ainoastaan niiden tarvitsemiin palveluihin. Nykyinen rakenne mahdollistaa päätelaitteiden pääsyn konesalin tarjoamiin palveluihin riippumatta siitä, mihin verkon segmenttiin päätelaite liitetään.

Nykyinen verkkosegmentointi jakaantuu kahdeksaan osaan, joissa pyritään erottelemaan verkkoon liitettävät päätelaitteet toisistaan (taulukko 1). Segmentoinnilla pyritään rajaamaan mahdollinen verkkovika kyseisen segmentin sisälle ja suojata muita verkon osia. Nykyisessä sairaalaverkossa kerroskytkimen vikaantuessa vika saattaa ulottua useampaan verkkosegmenttiin. Uutta sairaalaverkon osaa suunniteltaessa on hyvä miettiä, miten vika saadaan rajattua mahdollisimman pienelle alueelle.

Taulukko 1. Sairaalaverkon segmentointi.

Kohde	Verkosegmentin nimi
Potilasvalvonta, WLAN-potilasvalvonta	Potilasvalvonta
Lääkintälaite Potilashoitolaite Kuvantamislaite	Lääkintälaite
Liikuteltava lääkintälaite	Liikuteltava lääkintälaite
Hoitajakutsu	Hoitajakutsu
Valvontakamera	Video
Yleiskäyttöinen PC	Yleis PC
WLAN-tukiasemat	WLAN
VoIP-puhelin	Puhelin

2.5 Sairaalaverkkoon liitettävät päätelaitteet

Verkkoon liitettävät päätelaitteet voidaan jakaa kolmeen eri ryhmään. Yrityksen ylläpitämät päätelaitteet, joille annetaan täysi tuki niin laitteen, verkon ja verkon palveluiden osalta. Näistä päätelaitteista ja niiden käyttämistä ohjelmistoista on tarkka tieto yrityksen käyttäjätietokanta- ja hakemistopalvelussa. Näihin päätelaitteisiin lukeutuvat henkilökunnan tietokoneet, tabletit, matkapuhelimet ja VoIP-puhelimet. Muita verkon palveluita käyttäviä päätelaitteita ovat mm. tulostimet, kameravalvonta, kulunvalvonta- sekä hoitajakutsujärjestelmät. Toiseen ryhmään kuuluvat lääkintä- ja potilasvalvontalaitteet sekä kulunvalvonta- ja hoitajakutsujärjestelmät, joille annetaan tuki verkkoyhteensopivuudelle ja verkon tuottamille palveluille. Päätelaitteisiin kohdistuva tekninen tuki tulee laitevalmistajilta VSSHP:n teknisen osaston kautta ja yrityksen tehtävänä on taata verkkoyhteensopivuus kyseisille laitteille. Kolmas ryhmä koostuu laitteista, joille luodaan pääsy vierailijaverkon kautta internetin tarjoamiin palveluihin. Vierailijaverkosta ei ole suoraa pääsyä VSSHP:n sisäisiin verkkopalveluihin. Nämä laitteet ovat pääasiassa potilaiden tai omaisten mukanaan tuomia päätelaitteita, BYOD (Bring Your Own Device). Sairaalaverkko tulee suunnitella tukemaan kaikkia edellä mainittuja päätelaitteita. Tämä asettaa haasteita erityisesti tietoturvaan ja verkkoresurssien käytön kohdentamiseen.

Lääkintä- ja potilashoitolaitteet

Eri lääkintälaitteiden sekä potilastietojärjestelmien välinen tiedonsiirto perustuu standardoituun tapaan lähettää viestejä tietoliikenneverkon yli. HL7 työryhmä pyrkii luomaan viitekehyksen ja sitä tukevat standardit joilla määrittelemään tietosisällön viestit ja sanomat, joita terveydenhuollon järjestelmät toisilleen voivat standardien mukaisesti lähettää. HL7 standardit ovat jaettuina seitsemään eri osioon, joissa määritellään, miten tieto on paketoitu ja siirtyy eri järjestelmien välillä sekä yhteisen kommunikointikielen, rakenteen ja viestityypin joita käytetään eri järjestelmien yhteen integroinnissa. Standardeissa on luotu omat viestityyppinsä muun muassa laboratoriotuloksille, lähetteelle ja hoitopalautteelle. Terveyssektorin viestien lisäksi HL7:n standardit levittäytyvät osittain myös muille alueille, esimerkiksi tiedon esittämiseen (HL7 International 2016). Näitä standardeja kehittää kansainvälisesti Health Level Seven International ja kansallisella tasolla HL7 Finland ry, joissa jäseninä on mm. sairaanhoitopiirejä ja niille ICT-ratkaisuja tarjoavia yrityksiä (HL7 Finland ry 2016). Näitä standardeja ei tulla käsittelemään tarkemmin tässä opinnäytetyössä.

Kuvantamislaitteiden digitaalisen kuvan formaatti noudattaa DICOM-standardia. DICOM-standardin ansiosta eri valmistajien kuvaverkkoon liitetyt laitteet kykenevät yhteiseen käytännön tietojen välitykseen ja tiedon esitykseen. Se mahdollistaa eri valmistajien laitteiden yhteensopivuuden samassa järjestelmässä. Tavallisten röntgenkuvien lisäksi DICOM-standardi mahdollistaa tietokonetomografia-, magneettikuvaus- ja ultraäänitutkimuksien sekä lääketieteellisten valokuvien arkistoinnin samaan virtuaalisen arkistoon tavallisten röntgenkuvien kanssa. Kuvat tallennetaan PACS-arkistoon. Digitaalisen kuva-arkiston suuri etu on, että filmien kehittäminen jää kokonaan työprosessista pois. Digitaalisia kuvia voidaan myös muokata jälkeenpäin, joten uusintakuvauksien määrä pienenee. PACS-järjestelmän eräs ongelma on tietosuoja. Asiaankuulumaton henkilö voi päästä katselemaan kuvia esimerkiksi toisen ihmisen käyttäjätunnuksilla, koska niitä on vaivatonta siirtää paikasta toiseen (Reponen 2010). PACS-järjestelmää tai DICOM-standardia ei tulla käsittelemään tarkemmin tässä työssä. Tietosuojaan liittyvä näkökulma kannattaa ottaa huomioon verkkoa suunniteltaessa.

Osa lääkintä- tai potilashoitolaitteista tarvitsevat erillisen tietokoneen tukemaan toimintaa tai olemaan rajapintana verkon tarjoamien palveluiden suuntaan. Näiden tietokoneiden tulee täyttää sähköisille lääkintälaitteille säädetyn standardin, IEC 61010. Standardissa määritellään käyttöturvallisuusvaatimukset ja luotettavuusvaatimukset niiltä osin, kun ne

liittyvät laitteen käyttöturvallisuuteen. Laitteiden vaatimukset ovat tiukempia kuin perinteisten sähkölaitteiden vaatimukset ja niiden tulee sietää paremmin ulkoisia häiriölähteitä kuten säteilyä tai kemikaaleja. Lisäksi laitteet eivät saa häiritä muita laitteita, mikä on erityisen tärkeää esimerkiksi toimittaessa herkkien kuvantamislaitteiden läheisyydessä. Standardissa on otettu kantaa myös menetelmiin, joilla pienennetään mikroympäristön likaantumisastetta. Myöskään IEC 61010-standardia ei tässä työssä käsitellä, mutta tämä vaatimus on syytä ottaa huomioon hankittaessa tietokoneita lääkintälaitteiden yhteyteen.

WLAN tukiasemat ja paikannus

Langaton lähiverkko jaettu neljään eri verkkoalueeseen taulukon 2 mukaisesti. SSID-verkkojaon (Service Set Identifier) toteutus, hallinta ja valvonta on hoidettu keskitetysti WLAN-ohjaimen kautta. WLAN-ohjaimena on käytetty Ciscon WiSM2 (Wireless Service Module 2) moduulia, joka on sijoitettuna sisäverkon VSS-kytkinpariin. WLAN-ohjaimen kautta konfiguroidaan WLAN-verkko. WLAN-verkko pystyy tukemaan 1000 erillistä WLAN-tukiasemaa. Tuosta kapasiteetista on käytössä noin 780 WLAN-tukiasemaa. WLAN-ohjaimen kautta pystytään valvomaan langatonta verkkoa niin RF-häiriöiden (Radio Frequency) kuin palvelun laadun QoS (Quality of Service) kannalta (Cisco Systems Inc. 2016). Vierailijaverkon tiedonsiirtokapasiteettia on rajoitettu, kun taas muiden WLAN-verkko-osioiden kaistaa ei ole rajoitettu.

Taulukko 2. WLAN-verkko-ositus.

SSID	Kuvaus
VSSHP-Guest	Vierailijaverkko
eduroam	Yliopiston opetuskäyttöön tarkoitettu verkko.
VSSHP	Henkilökunnan käyttöön tarkoitettu WLAN-verkko.
VSSHP-medical	Liikuteltavien lääkintälaitteiden käyttöön tarkoitettu WLAN-verkko.

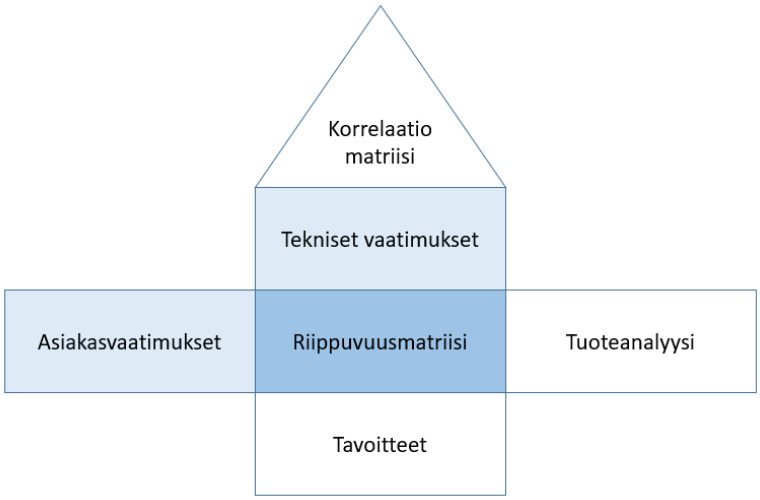
WLAN-verkon tukiasemat ovat Ciscon Aironet 2700 -sarjan tukiasemia, jotka tukevat IEEE 802.11ac -standardia. Tukiasemat toimivat 2,4 GHz:n ja 5 GHz:n taajuuksilla ja suurin kaistanopeus on 1,3 Gbps. WLAN-yhteydet on suojattu WPA2 enterprise (Wi-Fi Protected Access II) salausprotokollalla ja verkon käyttäjätunnistus todennetaan Microsoft AD:n ja RADIUS-palvelimen (Remote Authentication Dial-In User Service) kautta.

Sisätilanpaikannus on toteutettu Ekahaun RTLS (Real-Time Location System) langattomiin lähiverkkoihin perustuvan paikannusjärjestelmän avulla. Sisätilanpaikannuksessa käytetään pieniä ladattavalla akulla toimivia paikantimia. Paikantimet lähettävät WLAN-tukiasemien kautta paikkatietoa paikannusjärjestelmälle. Paikantimien ansiosta sairaaloissa tiedetään, missä henkilökunta tai potilaat kulloinkin ovat. Lisäksi hoitohenkilökunnan turvallisuus lisääntyy, kun kannettavalla paikantimella voi kutsua apuun vartijan lisäksi lähistöllä olevia kollegoita, jos potilas käyttäytyy aggressiivisesti. Potilaiden paikannus toimii sairaalassa esimerkiksi tilanteessa, jossa dementiapotilas vaeltaa epähuomiossa väärälle osastolle. Potilaan paikannusranneke tekee hälytyksen, jonka ansiosta hänet löydetään nopeasti.

2.6 Vaatimusten hallinta

Opinnäytetyö sijoittuu projektinhallinnan elinkaaressa projektin suunnitteluvaiheeseen. Vaatimustenhallinnan tavoitteena on luoda yhtenäinen näkemys hankkeeseen osallistuvien sidosryhmien välille siitä, mitä varten kyseinen hanke on olemassa ja mitä sillä pyritään saamaan aikaan. Vaatimustenhallinta on osa projektin laajuuden määrittelyä. Lisäksi vaatimustenhallinnan tarkoituksena on tukea hankintojen ohjausta sekä riskienhallintaa. Projektin laajuuden määrittelyssä tarkennetaan, mitä hyötyä projektista on yrityksen strategisten päämäärien saavuttamisen kannalta. Projektin laajuuden määritelmää taasen käytetään tulevien projektipäätösten perustana. Sen perusteella olisi myös viestittävä projektin tärkeydestä sekä hyödyistä, joita projektin onnistuneella toteuttamisella pitäisi saavuttaa. (ISO/TC 258 (SFS-julkaisut) Project, programme and portfolio management 2012)

Vaatimustenhallinnan kannalta kolme keskeisintä syötettä ovat sidosryhmät, dokumentit ja käytössä oleva järjestelmä (Pohl et al. 2011). Sidosryhmiltä kerättäviä vaatimuksia voidaan karkeasti luokitella sarjaksi prosesseja koostuen luetteloiden keräämisestä, asiakirjojen laadinnasta, katselmoinneista ja hyväksymisneuvotteluista (Kosola 2004). Yksi yleisesti käytetty malli vaatimusten keräämiseen on laadun talo eli House of Quality (kuva 8). Tässä prosessissa asiakkaan vaatimukset, järjestelmään kohdistuvat määräykset, tekniset vaatimukset ja kilpailevien tuotteiden analysoinnista saadut tiedot kootaan yhteen matriisiin, joka pisteytetään asiakkaalta saatujen ja projektin asettamien prioriteettien mukaisesti (Hauser, Clausing 1988).



Kuva 8. Laadun talo (Hauser, Clausing 1988)

Sairaalaverkkoon liittyvät asiakasvaatimukset tulevat valtaosin Varsinais-Suomen, Satakunnan ja Vaasan sairaanhoitopiireiltä, jotka toimivat työn tilaajina. Osa vaatimuksista taas saattaa tulla operaattoreilta, kuten DNA tai Elisa. Operaattoreilta tulevat vaatimukset kohdistuvat tietoliikenneverkon runkoverkkoon. Taulukossa 3 on eräs malli, jota voidaan käyttää pohjana vaatimusten keräämiseen sidosryhmiltä. Kyseisessä mallissa on listattuna projektin kaikki eri osa-alueet, joihin ammattialueeseen tai sidosryhmään kuuluvat henkilöt voivat koota oman alueensa vaatimukset. Eri ammattialueilta saadut vaatimukset kootaan yhteen matriisissa ja täten varmistetaan, että kaikki sidosryhmien vaatimukset tulee kerättyä. Kerätyistä vaatimuksista saatua listaa voidaan tarvittaessa tarkentaa ja priorisoida katselmointien ja hyväksymisneuvotteluiden kautta.

Taulukko 3. Malli vaatimusten keräämisestä.

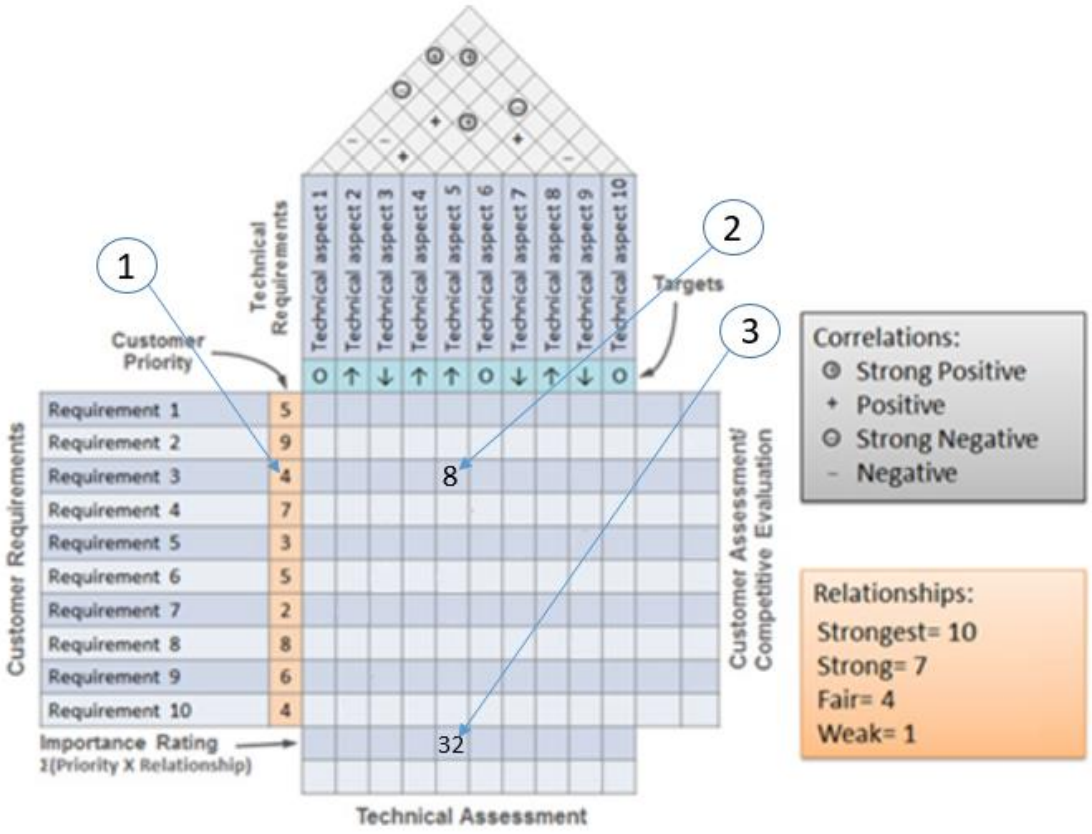
	Ammattialue A	Ammattialue B	Ammattialue C	... Ammattialue X	Yhteenveto
0: Taustaa ja yleistä asiaa					
1: Kokonaisuuden hallinta					
2: Sidosryhmien hallinta					
3: Laajuuden hallinta					
4: Resurssien hallinta					
5: Aikataulujen hallinta					
6: Kustannusten hallinta					
7: Riskienhallinta					
8: Laadunhallinta					
9: Hankintojen hallinta					
10: Viestinnän hallinta					
11: Yhteenveto ja muuta asiaa					

Sairaalaverkkoon kohdistuvat määräykset ja tekniset vaatimukset on listattu erinäisiin dokumentteihin, jotka suunnitteilla olevan tietoliikenneverkon laajennuksen tulee täyttää. Esimerkkejä dokumenteista saatavista vaatimuksista ovat projektiin keskeisesti liittyvät standardit, lakiasetukset sekä yrityksen sisäiset vaatimusmäärittelyt. Edellisissä luvussa oli kuvattuna lyhyesti lääkintälaitteisiin liittyviä standardeja, jotka osittain asettavat myös verkkosuunnittelulle vaatimuksia. Verkkosuunnittelun perustana voidaan käyttää valtiovarainministeriön luomaa VAHTI-sisäverkko-ohjetta. VAHTIssa on määritelty vaatimustasot esimerkiksi verkon kaapeloinnille, langattomille verkoille, aktiivilaitteille, sisäverkon yhteyksille, päätelaitteille, palveluille, tunnistautumiselle, verkon hallinnalle ja valvonnalle sekä jatkuvuussuunnittelulle. Lisäksi yrityksen sisäisistä vaatimuksista keskeisimpiä ovat potilas- ja lääkintätiedon saatavuus keskeytyksettä sekä vikatilanteista toipumisen nopeus. Käytössä olevat järjestelmät asettavat yhteensopivuuden kautta vaatimuksia uusien verkko-osien suunnittelulle. Uuden sairaalaverkko-osan tulee toimia saumattomasti olemassa olevan tietoliikenneverkon kanssa. Olemassa olevasta järjestelmästä saadut opit tulee hyödyntää uutta verkkoa suunniteltaessa.

Opinnäytetyö ei tule ottamaan kantaa siihen, minkä valmistajan verkkolaitteita tullaan laajennustöiden yhteydessä käyttämään. Verkon aktiivilaitteiden valintaan kuitenkin vaikuttavat niiden tekniset ominaisuudet, kuten kapasiteetti, porttinopeudet, tarvittaessa PoE (Power over Ethernet) ja reitityskyvykkyys. Yksi keskeisimmistä valintaperusteita on kuitenkin verkkolaitteiden elinkaareen kohdistuvat kustannukset, joihin vaikuttavat huoltosopimuksen laajuus, varalaitteiden saatavuus sekä takuun kattavuus.

Esimerkki laadun talon soveltamisesta

Asiakasvaatimukset ja järjestelmävaatimukset sekä kilpailevien tuotteiden analyysistä saadut vaatimukset pystytään tarvittaessa tuomaan kuvassa 9 olevaan matriisiin ja pisteyttämään tärkeysjärjestykseen. Kertomalla matriisin risteyskohdassa annettu laitteen tekniseen ominaisuuteen liittyvä, tärkeysjärjestykseen perustuva, numeraalinen arvo asiakaan prioriteetilla saadaan tavoitearvoille pisteytys. Esimerkissä yksi asiakasvaatimuksista on priorisoitu niin, että vaatimus numero 3 on saanut arvon 4 (kohta 1). Tähän kyseiseen asiakasvaatimukseen liittyy oleellisesti tekninen ominaisuus numero 5, joka on arvioitu tärkeäksi suunnittelun kannalta ja saanut arvon 8 (kohta 2). Kertomalla kyseiset arvot keskenään saadaan vaatimukselle tavoitearvoa kuvaava pisteytys 32 (kohta 3). Joissain tapauksissa tietty tekninen ominaisuus saattaa täyttää kaksi asiakkaan asettamaan vaatimusta, jolloin kyseisten tulojen summa merkitään tavoitearvon pisteiksi. Tätä menetelmää voidaan käyttää päätöksenteon tukena ja kommunikaatiovälineenä asiakkaiden kanssa. Mallia voidaan haluttaessa soveltaa myös sairaalan tietoliikenneverkon suunnittelun yhteydessä.



Kuva 9. Esimerkki laadun talo matriisin käytöstä (Hauser, Clausing 1988).

Tässä opinnäytetyössä keskitytään pääosin VAHTIn vaatimuksiin, nykyisen tietoliikenneverkon kautta tuleviin yhteensopivuusvaatimuksiin, vikasietoisuuteen ja palautumiskykyyn liittyviin yrityksen sisäisiin vaatimuksiin ja palautumiskykyyn, asiantuntijoiden lausuntoihin hyvistä suunnittelukäytännöistä sekä osittain sidosryhmiltä kerättäviin vaatimuksiin. Sidosryhmien vaatimukset tulevat tarkentumaan suunnittelutyön edetessä ja suurin osa vaatimuksista määräytyy vasta tämän opinnäytetyön valmistumisen jälkeen.

3 VAHTI-SISÄVERKKO-OHJEEN VAATIMUKSET

Varsinais-Suomen sairaanhoitopiiri vaatii, että sairaaloiden tietoliikenneverkon tulee täyttää VAHTIn perustason. Tässä kappaleessa verrataan sairaalaverkon nykytilaa VAHTIn eri vaatimustasoihin ja poimitaan kohtia, joita tulee ottaa huomioon uutta sairaalaverkkolaajennusta suunniteltaessa. Lisäksi VAHTI antaa hyvän pohjan asiantuntijahaastatteluiden tutkimuskysymyksille.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on luonut sisäverkko-ohjeen, jonka tavoitteena on parantaa tietoturvallisuuden tasoa yhtenäistämällä tietoturvavaatimuksia valtionhallinnon sisäverkoissa, joihin sairaalaverkko luetaan. Ohje tukee organisaatioita sisäverkkojen tietoturvallisuuden varmistamisessa ja kehittämisessä. Lisäksi ohje auttaa levittämään jo olemassa olevia hyviä käytäntöjä organisaatioihin. Ohjeessa on pyritty esittämään tuote- ja toimittajariippumattomasti sisäverkkojen tietoturvallisuutta edistävät toimenpiteet, koska tekniset ratkaisut kehittyvät jatkuvasti. Ohje on pyritty rakentamaan siten, että siitä on hyötyä myös uusien sisäverkkoteknologioiden käyttöönotossa. Ohje pyrkii vaikuttamaan siihen, että tietojärjestelmien tietoturvallisuudesta huolehtiminen kokonaisuutena olisi vakioitujen ja hyväksyttävien menettelytapojen mukaista (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010). Tämän ansiosta tietoturvallisuuden taso ei riipu yksittäisestä henkilöstä, mikä kokonaisuutena parantaa myös järjestelmien tietoturvallisuutta.

Sisäverkko-ohje jakaantuu verkkosuunnittelun kannalta eri osioihin, jota tullaan tässä kappaleessa käymään läpi tarkemmin. Jokainen osio sisältää omat tarkistuslistansa. Tarkistuslistojen avulla on tarkoitus kartoittaa sairaalaverkon nykytila. Yrityksen tulee täyttää sisäverkko-ohjeen asettamat perustason vaatimukset, jotka arvioidaan ulkoisilla auditoinneilla.

Verkon rakenteen vaatimukset

Verkon rakenteella tarkoitetaan verkon fyysisen tai loogisen rakenteen arkkitehtuuria, joka pitää sisällään langallisen ja langattoman verkon sekä virtuaaliverkkojaon. Vaatimuksissa tarkastellaan verkon omistajuutta, vastuujakoa verkon suunnittelusta, testauksesta sekä ylläpidosta sovittujen prosessien ja dokumentointikäytäntöjen mukaisesti. Lisäksi verkkoarkkitehtuurin tulee olla toteutettu tähtitopologialla hallinnan ja ylläpitämisen helpottamiseksi. Tämän topologian pohjalta verkosta tullaan määrittämään kriittiset komponentit, joihin osa verkkorakenteen vaatimuksista kohdentuu. Kriittisiksi komponenteiksi luetaan esimerkiksi tähden keskipisteessä oleva kytkin, joka vikaantuessaan vaikuttaa kaikkiin siihen liitettyjen laitteiden verkkoyhteyksiin. Näiden kriittisten komponenttien yhteydet tulee olla kahdennettuja. Vaatimuksissa viitataan myös ylläpitäjille säännöllisesti järjestettäviin tietoturvakoulutuksiin. Verkon rakenteen arviointi tehtiin tarkistuslistaa vasten. Taulukkoon 4 on poimittu tarkastuslistan osat, jonka vaatimukset koskevat myös uuden verkkolaajennuksen lisäämistä nykyiseen sairaalaverkkoon.

Taulukko 4. Osittainen verkon rakenteen tarkistuslista (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
5.5	Eri verkot tai niiden osat on eristetty toisistaan loogisesti tai fyysisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.6	Liikennettä sisä- ja ulkoverkon välillä rajoitetaan teknisesti siten, että vain tarpeellinen liikenne päästetään läpi.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.7	Ylläpitoon tarkoitetut etähallintayhteydet työasemiin on sallittu ainoastaan ylläpitohenkilöstölle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Taulukko 4 (jatkuu).

5.9	Verkkoliitännät yleisölle avoimissa tiloissa on suojattu siten, että organisaation sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.10	Muutokset verkkoon testataan, katselmoidaan ja toteutetaan muutoshallintaprosessin mukaisesti.	vahva suositus	vahva suositus	pakollinen vaatimus
5.11	Hallinta-/valvontatoiminta on erotettu muusta verkon liikenteestä esim. loogisesti erilliseen verkkoon.	suositus	vahva suositus	pakollinen vaatimus
5.12	Verkkojen väliset yhteydet on kartoitettu ja hyväksytty riskianalyysin kautta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.14	Vaihtoehtoiset tiedonsiirtoreitit ja -resurssit on toteutettu, dokumentoitu ja hyväksytetty asianmukaisilla tahoilla.	suositus	vahva suositus	pakollinen vaatimus
5.15	Kriittiset verkon komponentit on kahdennettu.	suositus	vahva suositus	pakollinen vaatimus
5.16	Suorat, ulkoverkosta sisäverkkoon otetut yhteydet on estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.19	Verkon rakenne on suunniteltu kestämään nykyinen ja arvioitu tuleva liikennemäärä.	suositus	vahva suositus	vahva suositus
5.20	Verkko on jaettu loogisesti erillisiin aliverkkoihin, joihin palvelut jaetaan käyttötarkoituksensa mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.23	Fyysinen verkko on jaettu vyöhykkeisiin eri käyttötarkoituksien mukaan.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Nykyinen sairaalaverkko täyttää pääosin edellä mainitut vaatimukset. Suurin epäkohta edellä mainittuihin vaatimuksiin tulee verkon segmentoinnin osalta. Nykyinen verkko ei täytä VAHTIn vaatimuksia 5.5 ja 5.23 (taulukko 4). Nämä kohdat tulee ottaa huomioon uusia sairaalaverkkolaajennuksia tehtäessä. Edellä mainittuja kohtia tullaan myös käsittelemään asiantuntijahaastatteluiden yhteydessä.

Suojattavien kohteiden vaatimukset

Sairaalaverkon tärkein suojauksen kohde on tieto ja sen luottamuksellisuus, eheys ja saatavuus. Järjestelmien, joihin tieto tallennetaan tai joissa sitä käsitellään, tulee olla suojattuja. Verkko ja sen osat ovat olemassa nykyistä ja tulevaa tiedonsiirtoa varten. Uutta sairaalaverkkoa tai sen osaa pystytettäessä verkko suojataan tietoturvallisuus huomioiden riippumatta siitä, onko se heti käytössä vai ei (taulukko 5). Näin toimitaan, jotta mahdolliset tietoturvaongelmat käytön aikana voidaan minimoida. Tiedon suojaaminen toteutetaan tiedon luokittelun mukaisesti siten, että kriittisimmät tiedot on suojattu paremmin. Verkossa olevan tiedon analyysiä käytetään verkon suunnittelun pohjana esimerkiksi verkon segmenttijaottelulle, liikenteen rajoittamiselle eri segmenttien välillä, tunnistautumiseen eri segmentteihin sekä pääsyrajoituksiin sisäverkon ja ulkoverkon välillä.

Taulukko 5. Osittainen suojattavien kohteiden tarkistuslista (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
6.1	Uutta verkkoa, verkkoaluetta tai segmenttiä pystytettäessä se suojataan tietoturvallisuus huomioiden, riippumatta siitä onko se heti käytössä vai ei.	vahva suositus	vahva suositus	pakollinen vaatimus
6.2	Verkon koko olemassaolon ajan analysoidaan säännöllisesti tietoturvaratkaisujen riittävyyttä suhteessa verkossa kulkevaan tietoon.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
6.3	Verkko on suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Nykyinen sairaalaverkko täyttää edellä poimitut vaatimukset. Riittävä tietoturva tulee ottaa huomioon jo heti alkuvaiheessa, kun uutta verkkolaajennusta aletaan pystyttää. Potilastiedot voidaan luokitella yhdeksi kriittisemmiksi tiedoiksi, joita verkon palvelimilla säilytetään. Varsinkin niiden suojaaminen tulee suunnitella tarkkaan.

Sisäverkkoon kohdistuvat uhat ja vaatimukset

Sairaalaverkon suojaaminen perustuu riskianalyysiin, jonka osana kartoitetaan verkossa olevaan tietoon liittyvät uhat ja vaatimukset sekä turvallisuustarpeet. Turvallisuustarpeiden pohjalta päätetään tarvittavat tekniset menetelmät, joiden avulla suojataan sairaalaverkon tietoa ja palveluita. Riskianalyysissä pyritään huomioimaan tiedon saatavuus, luottamuksellisuus ja eheys tietoturvallisuuden kannalta. Esimerkkejä yleisistä uhista ovat muun muassa haittaohjelmat, ulkopuoliset murtautujat, omat työntekijät, yhteistyökumppanit, erilaiset luonnonmullistukset ja muut fyysiset tapahtumat tai laiterikot, ohjelmistovirheet ja konfiguraatioviat. Edellä listattujen uhkien torjuminen on organisaation oman harkinnan mukaista ja verkkototeutus on hyvinkin vapaasti tehtävissä. Nämä vaatimukset koskevat koko sairaalaverkkoa eivätkä suoraan yksittäistä verkon osa-aluetta tai verkkolaajennusta, joten uhkien torjuminen noudattaa nykyistä käytäntöä.

Yhteistyö muiden toimijoiden kanssa

Sairaalaverkko toimintaympäristönä vaatii usein yhteistyökumppanien kanssa toimimista. Yhteistyökumppaneita toimii sairaalaverkon ylläpidon, palveluntuottajan sekä käyttäjän roolissa. Ennen yhteistyöhön ryhtymistä on hyvä arvioida yhteistyökumppanien aiheuttamat tietoturvariskit ja mahdolliset tarvittavat muutokset tietoturvallisuuden kannalta. Yhteistyökumppanin omat sisäiset tietoturvaohjeet ja menetelmät saattavat poiketa tai olla joiltain osa-alueilta heikommat kuin yrityksen omat menetelmät ja vaatimukset. On hyvän tarkistaa, että tietoturvavaatimukset ovat vähintäänkin samaa tasoa tai tiukemmat kuin sairaalaverkossa käytössä olevat tietoturvavaatimukset. Tässä opinnäytetyössä ei keskitytä vaatimuksiin, jotka kohdistuvat yhteistyökumppaneihin.

Kaapelointi

Päätelaitekaapeloinnit ovat lähes poikkeuksetta kierretystä parista tehtyjä CAT5- (vanhemmat verkonosat) tai CAT6-tason (uudet verkonosat) yleiskaapelointeja. Kerroksissa kaapelointi päättyy laitetiloissa sijaitseviin ristikytkentätelineisiin. Samassa laitetilassa sijaitsevat kerroskytkimet, joihin liitytään ristikytkentätelineen kautta. Ristikytkennässä on käytössä värikoodatut kaapelit, joilla on kuvattu verkon eri segmentit (taulukko 1). Sairaalaverkon aktiivilaitteiden väliset runkoyhteydet ovat valokuituyhteyksiä. Uusien verkko-osien osalta kaksi fyysisesti erillistä valokuituporttia muodostavat yhden loogisen kuitulinkin verkkolaitteiden välillä mahdollistaen suuremman tiedonsiirtokapasiteetit laitteiden välillä. Laitteiden välinen valokuituyhteys on kahdennettu yhteyksien turvaamiseksi. Yhteyksiä suunniteltaessa on hyvä varmistua, että kaapeloinnit kulkevat fyysisesti eri reittejä. Sairaalaverkon kaapeloinnit ovat sijoitettuna pääosin kaapelikouruihin tai -hyllyihin, ettei asiatonta kytkeytymistä kaapeleihin voi tehdä huomiota herättämättä, eivätkä kaapelit ole alttiina fyysiselle vaurioitumiselle. Taulukkoon 6 on poimittu tarkastuslistan osat, jonka vaatimukset koskevat myös uuden verkkolaajennuksen lisäämistä nykyiseen sairaalaverkkoon.

Taulukko 6. Kaapeloinnin tarkistuslista (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
9.1	Kaapelointi on hyväksytty ao. kaapeliluokalle määritellyn virallisen tyyppitestausmenettelyn mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.2	Kaapelit kulkevat kytkeytymistä ja fyysisiä vaurioita ehkäisevissä rakenteissa.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.3	Jakamot, ristikytkentäpaikat ja verkon aktiivilaitteet sisältävät telineet sijaitsevat lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.4	Kaapelointi on dokumentoitu ja näkösuojaan jäävät kaapelit on nimiöity dokumentteja vastaavasti molemmista päistään.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.5	Käyttämättömät liitäntäpisteet on irrotettu aktiivilaitteesta tai ao. laitteen portit estävät oletuksena uusien asemien vapaan liittämisen sisäverkkoon.	suositus	vahva suositus	pakollinen vaatimus

Nykyinen sairaalaverkko täyttää edellä mainitut vaatimukset. Laitetilojen kaapelointia tullaan käsittelemään osana asiantuntijahaastatteluita. Tarkoituksena on varmistaa, että hyvät käytännöt ja kokemukset siirtyvät uusiin sairaalaverkkolaajennuksiin sekä mahdolliset parannuskohteet tulee huomioitua.

Langattomat lähiverkot

Sairaalaverkon langaton lähiverkko on toteutettu käyttäen keskitettyä hallintaa, jonka kautta verkkoa voidaan konfiguroida ja valvoa. Langattomien lähiverkkojen haasteena saattaa olla niiden kuuluvuus rakennuksen ulkopuolelle sekä osittainen kuulumattomuus rakennuksen sisätiloissa, niin sanotut katvealueet. Tietoturvan kannalta langattomat verkot ovat ongelmallisia, koska langattomia verkkoja on helppo salakuunnella tai häiritä. Lisäksi ongelmana saattavat olla käyttäjien tahattomasti asentamat luvattomat tukiasemat, joiden kautta voi olla mahdollista päästä käsiksi verkon tarjoamiin palveluihin. Langaton vierailijaverkko on toteutettu niin, että siitä on yhteys vain internetiin. Langattomaan lähiverkkoon liittyvä käyttäjä ja laite on tunnistettava luotettavasti. Tämä on toteutettu RADIUS-palvelimen (Remote Authentication Dial In User Service) ja keskitetyn käyttäjätietokannan Microsoft AD:n avulla. Langattoman lähiverkon asetukset tehdään WLAN-ohjaimeen. Langatonta lähiverkkoa laajennettaessa tukiasemat hakevat asetukset suoraan WLAN-ohjaimelta. Langattomaan lähiverkkoon kohdistuvat vaatimukset on huomioitu WLAN-ohjaimen asetuksissa.

Verkon aktiivilaitteet

Verkon aktiivilaitteet ovat komponentteja, joilla sairaalaverkko luodaan. Sairaalaverkon keskeisimpiä laitteita ovat runko- ja nousukytkimet, internet-reitittimet, hakemistopalvelut, DNS-nimipalvelimet ja DHCP-osoitepalvelimet. Näille laitteille on järjestetty keskeytymätön virransyöttö, joka takaa laitteiden toiminnan virtakatkon aikana. Vaatimukset kattavat laitehallintaan liittyvät seikat, kuten hallintayhteyden salauksen, käyttäjän tunnistuksen ja hallintaverkon segmentoinnin. Verkon aktiivilaitteiden konfiguroinnissa on huomioitava, että niiden oletusasetuksissa saattaa olla myös tietoturvallisuutta heikentäviä asetuksia sekä automaattitoimintoja, jotka on poistettava käytöstä. Lisäksi verkon

aktiivilaitteista on hyvä kerätä lokitiedot talteen palvelimelle ja muutoinkin seurattava niiden toimintaa. Taulukkoon 7 on poimittu tarkastuslistan osat, jonka vaatimukset koskevat myös uuden verkkolaajennuksen lisäämistä nykyiseen sairaalaverkkoon.

Taulukko 7. Verkon aktiivilaitteiden tarkistuslista (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
11.1	Verkolle on tehty riskianalyysi ja tämän tuloksena keskeiset verkkolaitteet, niiden komponentit (esim. virtalähde) ja yhteydet on tarvittaessa kahdennettu.	vahva suositus	vahva suositus	pakollinen vaatimus
11.2	Keskeisillä laitteilla on UPS ja kaikki verkon laitteet palautuvat virtakatkon jälkeen normaalitoimintaan.	suositus	vahva suositus	vahva suositus
11.3	Sisäverkon tietoturvallisuudeltaan erilaiset vyöhykkeet on eristetty toisistaan palomuurilla tai reitittimen pääsylistoilla. DMZ on eristetty sisäverkosta palomuurilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.4	Sisäverkkoon liitetyt aktiivilaitteet tunnistetaan vahvasti esim. 802.1X-menettelyllä, jolla estetään tuntemattomien laitteiden liittäminen.	suositus	vahva suositus	pakollinen vaatimus

Taulukko 7 (jatkuu).

11.5	Verkkolaitteiden hallintaliitäntään pääsevät kytkeytymään vain hallinnasta vastaavat ennalta määritellyt henkilöt ja laitteet. Laitteiden hallintayhteydellä käytetään vahvaa salausta ja käyttäjän tunnistusta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
11.6	Verkkolaitteissa on vaihdettu tunnistukseen liittyvät toimittajien oletusparametrit.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.7	Hallintayhteydet (esim. SNMP) on eriytetty omaan verkkosegmenttiinsä.	suositus	vahva suositus	pakollinen vaatimus
11.8	SNMP-protokollasta on käytössä vähintään versio 3, jos laitteisiin tehdään muutoksia. Jos laitteista vain luetaan tietoa, SNMP-protokollan on oltava vähäntään versio 2c.	vahva suositus	vahva suositus	pakollinen vaatimus
11.9	SNMP-protokollalla on pienimmät mahdolliset oikeudet tai se on poistettu käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.10	Tarpeettomat palvelut, ohjelmat ja protokollat on poistettu verkon aktiivilaitteista käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.11	Verkkolaitteiden asetukset on tallennettu ja varmuuskopioitu mahdollista laitteen vaihtoa ja asetusten palauttamista varten.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Nykyinen sairaalaverkko täyttää edellä mainitut vaatimukset. Verkon aktiivilaitteita tullaan käsittelemään osana asiantuntijahaastatteluita. Tarkoituksena on varmistaa, että hyvät käytännöt ja kokemukset siirtyvät uusiin sairaalaverkkolaajennuksiin sekä mahdolliset parannuskohteet tulee huomioitua. Lisäksi tarkastuslistan kohta 11.4 tullaan ottamaan osaksi haastatteluita, koska nykyisessä sairaalaverkossa osaa laitteista, esimerkiksi tietyt lääkintälaitteet, ei pystytä tunnistamaan verkon toimesta (taulukko 7).

Sisäverkkojen väliset yhteydet

Sairaalaverkon sisällä eri sairaaloiden väliset yhteydet on muodostettu operaattorilta vuokratun valokuidun tai MPLS-tekniikan (Multiprotocol Label Switching) avulla, jolla pystytään muodostamaan toisistaan riippumattomista loogisista verkoista yksi yhteinen fyysinen verkko. Toimipisteiden väliset yhteydet ovat kahdennettuja samaan tapaan kuin lähiverkon komponentit ja yhteydet. Joissain tapauksissa varayhteys on tehty LTE-reitittimen avulla, kuten esimerkiksi saaristossa sijaitsevien terveyskeskusten varayhteydet.

Vaatimuksissa otetaan myös kantaa palvelun laatuun (QoS), tiedonsiirron salaukseen ja verkon turvallisuusluokitukseen. Nämä vaatimukset koskevat laajennuksia, jotka sijoittuvat etäälle sisäverkon VVS-kytkinparista, jolloin yhteyden muodostamiseen tarvitaan operaattorin vuokravalokuituja tai yhteyksiä. Tämä opinnäytetyö on rajattu niin, että kohteena oleva sairaalaverkon laajennus tullaan tekemään VSSHP:n kampusalueella ja yhteyden muodostus tapahtuu VSSHP:n omistamassa verkossa.

Sisäverkon päätelaitteet

Päätelaitteet tarjoavat käyttäjälle rajapinnan sairaalaverkon palveluihin. Työasemien, palvelinten ja älypuhelimien lisäksi päätelaitteita ovat mm. IP-puhelimet, tulostimet, lääkintälaitteet, kameravalvonta ja kulunvalvonta. Sairaalaverkon palveluiden käyttö on sallittu ainoastaan sisäverkosta tai VPN etäyhteyden (Virtual Private Network) kautta. Vaatimuksissa oletetaan päätelaitteiden olevan yksilöityjä ja verkon tunnistettavissa siten, että yksittäinen laite voidaan määrittää sisäverkkoon kuuluvaksi tai siihen kuulumattomaksi. Sairaalaverkkoon liitettäviä päätelaitteita käsiteltiin luvussa 2.5. Lääkintälaitteiden tunnistusta ei ole toteutettu sairaalaverkossa osittain siitä syystä, että laitekannan hankinta on VSSHP:n vastuulla ja Medbit antaa tuen verkkoyhteensopivuudelle. Medbitin hallinnoimille päätelaitteille suoritetaan automaattinen tarkastus ennen niiden liittämistä sairaalaverkkoon. Tarkastuksen avulla varmistetaan laitekohtaisen palomuurin ja virustorjunnan olemassaolo sekä päivitysten ajantasaisuus. Päätelaitteisiin kohdistuvat vaatimukset ovat tämän opinnäytetyön ulkopuolella.

Sisäverkon palvelut

Sisäverkon palveluilla tarkoitetaan sellaisia verkon palveluita, joiden avulla on mahdollista pystyttää itsenäisesti toimiva verkko. Kriittisten verkkopalveluiden eli osoite-, reititys- ja nimipalvelun toimivuus pyritään varmistamaan sekä toiminta suojaamaan tietoturvan näkökulmasta. Verkkopoikkeamia pyritään havaitsemaan IDS- (Intrusion Detection System) ja IPS-järjestelmien (Intrusion Prevention System) avulla. Osoitepalveluun liittyviä tietoturvariskejä ovat esimerkiksi avoimeksi määritelty osoitepalvelu, joka tarjoaa osoitetiedot kaikille verkkoon liittyville laitteille tunnistamatta niitä millään tavoin tai hallitsemattomasti käynnistetty DHCP-osoitepalvelu, esim. kotoa tuotu WLAN-tukiasema, voi aiheuttaa verkkoon häiriötilanteen. Nimipalvelu on myös verkon kannalta erittäin kriittinen

palvelu. Jos se ei ole käytettävissä, verkossa ei käytännössä voi liikennöidä. Tästä syystä yhteys DNS-nimipalveluun on hyvä olla kahdennettu. Verkon peruspalveluiden päälle on rakennettu arvoa tuottavia lisäpalveluita kuten sähköposti, IP-puhelin palvelut, intranet sekä levy- ja tulostinpalvelut. Tässä opinnäytetyössä ei käsitellä tarkemmin sairaalaverkon tuottamia palveluita.

Tunnistautuminen

Sisäverkossa on tarvetta niin laitteiden kuin käyttäjien tunnistautumiselle sisäverkon eri tasoilla. Tunnistautumisessa tärkeää on, että käyttäjältä vaaditaan mahdollisimman vähän toimia pitäen silti yllä korkea tunnistautumisen taso. Sairaalaverkon näkökulmasta tunnistautuminen voidaan toteuttaa esimerkiksi, kun päätelaite tai palvelin liittyy verkkoon tai kun käyttäjä tunnistautuu verkkoon tai verkon peruspalveluihin (taulukko 8). Sairaalaverkossa on käytössä Microsoft Active Directory, joka sisältää tietoja käyttäjistä, päätelaitteista ja verkon resursseista. Lisäksi potilastietokannassa on erillinen käyttäjähallinta. Potilastietokantaan tunnistautuminen tapahtuu kahdennettuna, erillisen toimikortin ja tietokannassa olevien käyttäjätietojen perusteella. VPN-etäyhteyksiä muodostettaessa tunnistautuminen perustuu Microsoft AD:n käyttäjätietoihin sekä tekstiviestivarmennukseen. Tässä opinnäytetyössä ei käsitellä tarkemmin tunnistautumista sairaalaverkkoon.

Taulukko 8. Tunnistautumisen tarkistuslistan osa (Valtiohallinnon tietoturvallisuuden johtoryhmä 2010).

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
15.4	Kaikki käyttäjät ja päätelaitteet ovat hallittujen tunnistautumisratkaisujen piirissä.	vahva suositus	vahva suositus	pakollinen vaatimus

Osa potilas- ja lääkintälaitteista ei ole hallittujen tunnistautumisratkaisujen piirissä. Tämä epäkohtaa tullaan ottamaan osaksi asiantuntijahaastatteluita.

Verkon hallinta/valvonta

Verkon toimintaa valvotaan, jotta voidaan varmistaa verkon palveluiden saatavuus ja verkon toiminta tietoturvanäkökulmasta. Valvonnalla pyritään varmistamaan, että lokeista saadaan tietoa siitä, mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Lisäksi verkon ja verkkolaitteiden kuormitustilannetta seurataan, jotta mahdolliset ongelmat havaittaisiin ja korjattaisiin ennen kuin ne ehtivät haittaamaan merkittävästi sairaalaverkon toimintaa. Verkon hallinnan yhteydessä jokaisesta muutoksesta otetaan varmuuskopio, jotta ongelmatilanteessa vikaantunut verkon laite saadaan korvattua nopeasti uudella laitteella samaan konfiguraatioon kuin vikaantunut laite oli. Osaa sairaalaverkon laitteista hallitaan yhteistyössä operaattorin kanssa. Verkkolaitteiden ohjelmistoista saatetaan löytää aika ajoin tietoturvaongelmia samalla tavalla kuin muistakin tietoteknisistä järjestelmistä. Verkkolaitteiden ohjelmistot päivitetään valmistajan suositusten mukaisesti, kuitenkin ajoittaen ohjelmistopäivitykset niin että verkkopalveluiden saatavuus ei keskeydy. Verkon hallinta ja valvonta tulee huomioida uutta verkkolaajennusta tehdessä. Vaatimukset kohdistuvat kuitenkin sairaalaverkkoon kokonaisuutena ja niitä ei tarkemmin käsitellä tässä opinnäytetyössä.

Jatkuvuussuunnittelu

Jatkuvuussuunnittelulla pyritään pienentämään ja lyhentämään toimintaa haittaavien tapahtumien vaikutusta ja aikaa. Sairaalaverkon palveluiden tulee olla saatavilla 24/7. Suunnittelu pitää sisällään järjestelmien rakenteeseen liittyviä toimenpiteitä, jotka parantavat niiden toimintaa häiriötilanteissa sekä toimenpiteitä, jotka parantavat toipumista ongelmatilanteista sekä mahdollisia varalaitejärjestelyitä. Sairaalaverkon kriittiset palvelut on kahdennettu tai monistettu niin, että kriittiset palvelut ovat saatavissa useamman kuin yhden palvelimen kautta, kuten laitteiden väliset yhteydet ja konesalipalvelut. Verkkolaitteiden ja -palveluiden varmuuskopiointi on järjestetty riittävän usein, että pystytään takaamaan verkkopalveluiden laatu ja nopea palautuminen häiriötilanteiden tapahtuessa. Jatkuvuussuunnittelun vaatimuksia ei käsitellä tässä opinnäytetyössä.

4 SAIRAALAVERKON SUUNNITTELU

Tutkimusaineisto kokoaminen sairaalaverkon suunnittelua varten jakaantui useaan eri vaiheeseen. Ensimmäiseksi luotiin haastattelurunko (liite 2), jota käytettiin asiantuntijahaastatteluissa. Asiantuntijahaastatteluiden ensimmäisessä vaiheessa haastateltiin neljää Varsinais-Suomen sairaanhoitopiirin asiantuntijaa Turun ja Loimaan alueilta. Näillä henkilöillä oli aikaisempaa suunnittelukokemusta sairaalaverkon laajennuksista. Haastatteluista laadittiin yhteenveto, josta poimittiin sairaalaverkon suunnittelun kannalta keskeisimmät aiheet. Nämä aiheet otettiin tarkempaan tarkasteluun erikseen järjestettävässä jatkohaastattelussa. Tähän jatkohaastatteluun valittiin asiantuntijat Varsinais-Suomen ja Satakunnan sairaanhoitopiirien alueilta. Henkilövalinnoilla pyrittiin saamaan mahdollisimman laaja näkökulma käsiteltäviin aiheisiin. Jatkohaastattelun tuloksena saatiin tutkimusaineistoa, jota voidaan jatkossa hyödyntää uusia sairaalaverkkolaajennuksia suunniteltaessa.

4.1 Haastattelurungon muodostaminen

Asiantuntijahaastatteluiden tarkoituksena on varmistaa, että hyvät käytännöt ja kokemukset siirtyvät uusiin sairaalaverkkolaajennuksiin sekä mahdolliset parannuskohteet tulee huomioitua. Haastatteluihin poimittiin vaatimuskohtia VAHTI-sisäverkko-ohjeesta, joita nykyinen sairaalaverkko ei täytä tai joihin tulee jatkossa kiinnittää huomiota. Tutkimuskysymykseksi muodostui:

Mitä hyviä käytäntöjä ja kokemuksia aikaisemmista verkkolaajennuksista voidaan soveltaa uusien verkkojen suunnittelussa?

Tarkentavissa kysymyksissä otettiin huomioon VAHTIsta tulleet kohdat. Haastattelu jakaantui kolmeen eri osioon: verkon segmentointiin, verkon aktiivilaitteiden valintaan sekä laitetilojen kaapelointiin.

Verkkosegmentointi

Haastatteluissa pyrittiin hakemaan asiantuntijoiden mielipidettä siihen, miten sairaalaverkon segmentointi tulisi jatkossa toteuttaa. Miten verkkosegmentointi vaikuttaa verkon

aktiivilaitteisiin, kuten mahdollisesti valittaviin reitittimiin tai reitittäviin kytkimiin? Tuovatko IoT-laitteet erityisvaatimuksia verkkosuunnittelulle ja miten IoT-laitteet tulee ottaa huomioon jo olemassa olevissa verkoissa? VAHTIn kohdissa 5.5, 5.23 (taulukko 4) ja 11.4 (taulukko 7) käsiteltiin verkon segmentointia ja päätelaitteiden tunnistamista. Nämä kohdat nostettiin myös mukaan haastatteluun, jossa käsiteltiin verkon tietoturvaa, segmentointia ja päätelaitteiden tunnistamista.

Verkon aktiivilaitteet

Uuden sairaalaverkkolaajennuksen suunnittelussa pyritään pitkälti hyödyntämään kokemuksia aikaisemmista verkkolaajennuksista. Verkon aktiivilaitteita valittaessa tulee ottaa huomioon laitteiden ominaisuudet ja nykyinen verkkoratkaisu. Kysymyksissä haluttiin hakea asiantuntijoilta mielipiteitä, miten ja millaisilla laitteilla verkkolaajennuksen runkoverkko-osa tulisi toteuttaa sekä mitä asioita pitää huomioida asiakaskytkimiä valittaessa. Lisäksi asiakaskytkimissä voidaan tarvittaessa lisätä sairaalaverkon tietoturvaa muuttamalla kytkinporttien asetuksia. Lisäksi haastatteluissa haettiin asiantuntijoiden kantaa tietoturvan toteutusta.

Kaapelointi laitetiloissa

Tutustumiskäynnin yhteydessä Varsinais-Suomen sairaanhoitopiirin T1/T2-sairaalan sairaalaverkon laitetiloihin nousi esille parannettavia kohtia laitetilan ristikytkentöjen toteutukseen liittyen. Lisäksi verkkolaitteiden ja ristikytkentäpisteiden sijoituksessa toisiinsa nähden laitekaapeissa oli kehitettävää. Haastattelun avulla pyrittiin keräämään nämä epäkohdat ylös ja hyödyntämään saadut kokemukset tulevien verkkolaajennusten yhteydessä. Lisäksi haastattelussa kysyttiin asiantuntijameilipiteitä laitetilojen ja kaapeleiden dokumentointiin liittyen.

4.2 Asiantuntijahaastatteluiden havainnot

Asiantuntijahaastattelut suoritettiin Medbitin toimitiloissa. Haastatteluiden kestot olivat noin tunnin mittaisia, joiden aikana haastatteluiden avainkohdat kirjattiin muistiin. Haastatteluista ei äänitetty digitaalista tallennetta asiantuntijoiden toivomuksesta. Jokaisen

haastattelun jälkeen kyseisistä haastatteluista kirjoitettiin yhteenveto, jonne nostettiin verkonsuunnittelun kannalta keskeisimmät asiat.

Verkon segmentointi ja tietoturva

Haastatteluissa nousi esille tarve sairaalaverkon tietoturvan lisäämiseksi. Suurimpana haasteena nähtiin tuntemattomien laitteiden liittyminen sairaalaverkkoon. Yhtenä esimerkkinä nousi esille erään käyttäjän tuoman laitteen aiheuttama verkkovika, jonka aiheutti kyseisen laitteen aktiivinen DHCP-palvelin. Kyseinen ongelma voidaan verkkosuunnittelussa ottaa huomioon aktivoimalla DHCP snooping -ominaisuus verkon aktiivilaitteesta. Kyseisellä ominaisuudella pystytään jakamaan tarvittaessa DHCP-palvelu ainoastaan ennestään tunnetuille päätelaitteille, rajaamaan DHCP-palvelu halutuille verkkosegmenteille ja torjumaan tuntemattomien verkkolaitteiden aiheuttamat ongelmat.

Asiantuntijoiden mielipiteissä nousi vahvasti esiin päätelaitteiden ja käyttäjien tunnistamiseen liittyvän 802.1x-menettelyn tuominen uusiin sairaalaverkkolaajennuksiin. Kyseisen palvelun avulla pystytään lisäämään verkon tietoturvaa. Tunnistamalla hyväksytyt päätelaitteet niiden liittyessä verkkoon ja ohjaamalla ne oikeaan verkko-osioon saadaan myös toteutettua verkkosegmentointia joka ei täyttänyt VAHTIn vaatimuksia 5.5 ja 5.23 (taulukko 4). 802.1x-menettelyn mahdollistamaan verkkosegmentointia voidaan tarvittaessa tukea myös palomuurien avulla. Samalla verkkoon liitettävät ennalta tuntemattomat laitteet voidaan ohjata omaan rajattuun verkkoon ja täten pienentää tuntemattomista laitteista aiheutuvia verkko-ongelmia.

ACL-listojen (Access Control List) laajamittaista käyttöä ei koeta järkeväksi vaihtoehdoksi. Tämä siitä syystä, että laajassa sairaalaverkossa ACL-listojen suuri määrä saattaa aiheuttaa työkuorman merkittävää lisääntymistä ACL-listojen ylläpitoon liittyen.

WLAN-verkko

Osa asiantuntijoista nosti esille tarpeen WLAN-verkon segmentoinnin tarkentamiselle. Nykyinen SSID-verkkoluokittelu on kuvattuna taulukossa 2. Varsinkin VSSHP-medical verkkoon liittyy useita eri tarkoituksiin kohdennettuja päätelaitteita. Tarkemman verkkojaon avulla pystyttäisiin parantamaan WLAN-verkon kapasiteettia ja ohjaamaan päätelaitteet tarvittaessa tarkemmin määritellyille verkko-osioille.

Toinen merkittävä huomio liittyi WLAN-verkon vikasietoisuuden parantamiseen. Ideana on kytkeä tiloissa olevat WLAN-tukiasemat laitetiloissa sijaitseviin PoE-kytkimiin niin, että esimerkiksi joka toinen käytävillä sijaitsevista WLAN-tukiasema on yhden PoE-kytkimen takana ja joka toinen toisen. Tällöin yhden PoE-kytkimen vikaantuessa WLAN-verkko on saatavissa suurimmilta osin, mutta signaalin taso tai sisätilan paikannus saattaa heiketä.

Verkon aktiivilaitteet ja verkkototeutus

Yhteinen mielipide asiantuntijoilta oli, että verkkolaajennuksissa runkoverkon toteutus tulisi toteuttaa reitittävien kytkinten avulla. Reitittimet eivät tuo lisäarvoa reitittäviin kytkimiin nähden ja usein niiden kustannus on huomattavasti suurempi. Reitittävien kytkinten ominaisuudet, kuten LACP-kanavien luominen vikasietoisuuden parantamiseksi, spanning treen käyttö kuormantasauksessa sekä reitityksen muodostamiseen, ovat riittävät vastaamaan VAHTIn ja nykyisen sairaalaverkon asettamiin vaatimuksiin.

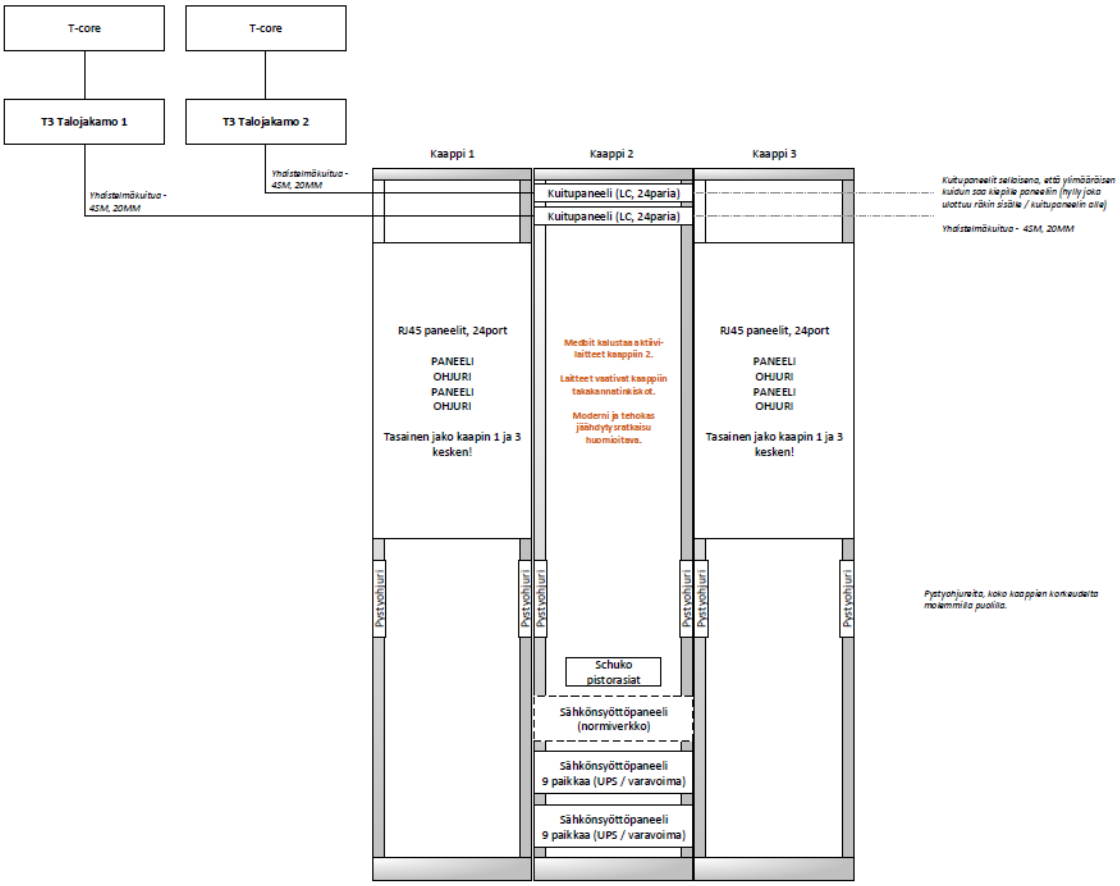
Liityntärajapinnassa asiantuntijat suosittelivat yksittäisten kytkinten käyttöä pinokytkinten sijasta. Yksittäisten kytkinten ylläpito ja huoltotoimenpiteet koetaan helpommiksi kuin pinokytkinten. Jossain tilanteissa pinokytkinten käyttö on perusteltua, esimerkiksi suuria porttimääriä tarvittaessa. Asiantuntijat nostivat myös esille spanning treen implementoinnin tuleviin verkkolaajennuksiin. Spanning treen avulla voidaan nopeasti ohjata vikaantunut verkkoyhteys kulkemaan toista reittiä ja täten parantaa verkon vikasietoisuutta.

Tietoturvaa voidaan parantaa myös kytkinporttien suojauksella. Esimerkiksi Ciscon kytkimissä olevan PortSecurity-ominaisuuden avulla kytkimen portti voidaan asettaa sallimaan vain tietty päätelaite. Vieraan päätelaitteen liittyessä kyseinen portti voidaan sulkea. Kyseinen ominaisuus voidaan halutessaan ottaa käyttöön harkitusti. Tämä ominaisuus ei kuitenkaan sovellu tilanteisiin, joissa useita eri päätelaitteita saatetaan liittää yhteen kytkinporttiin.

Tulevaisuudessa pitää ottaa huomioon PoE-kytkimestä sähkönsä saavat päätelaitteet. Tällaisia ovat esimerkiksi WLAN tukiasemat, valvontakamerat, VoIP-puhelimet sekä kannettavat tietokoneet. Tällä hetkellä PoE-kytkinten minimivaatimus on PoE+, jonka ominaisuudet määritellään tarkemmin standardissa IEEE 802.3at. PoE+ laitteen suurin tehontarve saa olla 25.5W. Tämä raja saattaa tulla vastaan, jos tulevaisuudessa halutaan WLAN-tukiaseman toimivan myös matkapuhelintukiasemana.

Laitetilat ja kaapelointi

Tuleviin verkkolaajennuksiin suositeltiin käytettäväksi kahta nousujakamoa, joihin kerroksissa sijaitsevien laitetilojen kaapeloinnit kerätään. Samanlainen ratkaisu on käytössä nykyisen T1/T2-sairaalan verkkototeutuksessa. Kahden nousujakamon avulla parannetaan merkittävästi verkon vikasietoisuutta. Suurten vikatilanteiden, kuten tulipalon, kohdistuessa toiseen nousujakamoon, toisessa nousujakamossa sijaitsevat verkon aktiivilaitteet tulevat hoitamaan verkossa tapahtuvat tiedonsiirrot esimerkiksi palvelimien ja päätelaitteiden välillä. Asiantuntijat laativat myös laitetilan kalustukseen liittyvän periaatekuvan (kuva 10), jossa havainnollistetaan liityntärajapinnan aktiivilaitteiden sekä ristikytkentäpaneelien suositellut sijoitukset laitetiloissa oleviin laitekaappeihin.



Kuva 10. Laitetilan mallikaappi sisäisestä ohjeesta.

Prosessin kehityskohteet

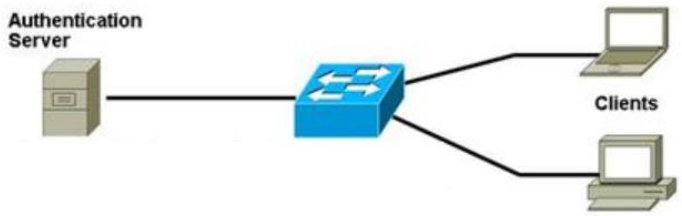
Haastatteluiden yhteydessä nousi esille muutamia kohteita, joihin asiantuntijat toivoivat tarkennettua tai määriteltyä toimintatapaa. Esimerkiksi uusien laitteiden, kuten potilas- ja lääkintälaitteiden, rekisteröimisen helpottamiseksi esitettiin portaalia, jonne laitteiden tiedot voidaan ilmoittaa.

Laitetiloissa tapahtuvien kaapelointien merkinnöissä, värikoodaamisessa ja dokumentoinnissa on sairaanhoitopiirikohtaisia käytäntöjä. Yhteiset käytännöt helpottaisivat tilannetta, jossa toisen sairaanhoitopiirin verkkoasiantuntija tulee suorittamaan työtehtävää toisen sairaanhoitopiirin alueelle. Tämän lisäksi laitetilojen nimeämiskäytännöt saattavat vaihdella sairaanhoitopiirien välillä.

Näitä prosessin kehittämiskohteita ei tulla käsittelemään tarkemmin tässä opinnäytetyössä.

4.3 Jatkohaastattelun havainnot

Asiantuntijahaastatteluiden yhteenveto käytiin läpi tapaamisessa Medbitin opinnäytetyön ohjaajan kanssa. Yhteenvedosta nousi esille kolme selkeää teemaa, jotka valittiin käsiteltäviksi erikseen järjestettävässä jatkohaastattelussa. Teemat, jotka valikoituivat jatkohaastattelun aiheiksi, olivat 802.1x-menettelyn implementointi verkkolaajennusten yhteydessä, verkkosegmentoinnin toteuttaminen sekä verkon aktiivilaitteet ja runkoverkon toteutus. Jatkohaastattelu järjestettiin Skype-palaverina Medbitin tiloissa, johon osallistui 8 asiantuntijaa Varsinais-Suomen ja Satakunnan sairaanhoitopiirien alueilta. Alustuksena käytettiin aikaisempien haastatteluiden yhteenvetoa, jonka havainnot esiteltiin osallistujille. Alustuksen jälkeen keskustelu avattiin asiantuntijoille, jonka ensimmäisenä aiheena oli 802.1x-menettelyn implementoiminen verkkolaajennusten yhteydessä.



Kuva 11. 802.1x-menettely päätelaitteen kannalta.

Toimintaperiaate 802.1x-menettelylle on kolmivaiheinen. Verkkoon liitetty päätelaite aloittaa tunnistautumisprosessin RADIUS-palvelimen kanssa (kuva 11). Jos päätelaitteessa on tuettuna 802.1x-menettelyn mukainen sertifikaatti, päätelaite pystytään tunnistamaan ja päätelaitteelle avataan pääsy sille kohdistettuihin verkkoresursseihin. Osissa päätelaitteista ei välttämättä ole tuettuna 802.1x-menettelyn sertifikaattia, jolloin päätelaitteen tunnistautumisessa käytetään laitteen MAC-osoitetta. Viimeisenä vaihtoehtona avataan sisäänkirjautumisikkuna päätelaitteen näytölle, jonka kautta tunnistautuminen voidaan suorittaa.

Pääosin sairaalaverkon aktiivilaitteet, asiakaskytkimet, tukevat suoraan 802.1x-menettelyä. Suurimman haasteen muodostavat suuri määrä lääkintä- ja potilaslaitteita, joissa 802.1x-menettelyn vaatimaa sertifikaattia ei ole. Näiden kaikkien lääkintä- ja potilaslaitteiden MAC-osoitteiden kirjaaminen RADIUS-palvelimelle olisi pitkä prosessi, johon ei ole järkevää ryhtyä. Lisäksi uusien laitteiden kirjaamiseen ja seurantaan tarvitaan selkeä toimintatapa, jota ei nykyisellään ole olemassa. Tärkeimpänä asiana verkkosuunnittelun kannalta on potilasturvallisuuden takaaminen. Lääkintä- ja potilaslaitteilla pitää olla pääsy verkon tarjoamiin palveluihin, jolloin 802.1x-menettelyn käyttö ei välttämättä sovellu käytettäväksi kyseisten päätelaitteiden kanssa. 802.1x-menettelyn osittainen käyttöönotto on kuitenkin mahdollista toteuttaa. Tällöin se kannattaa kohdistaa henkilöstön käyttämiin työasemiin, tietokoneisiin ja verkossa toimiviin tulostimiin. Edellä mainitut kohdat huomioiden verkon segmentointia ei voida pelkästään toteuttaa 802.1x-menettelyn avulla, vaan tueksi tarvitaan muita ratkaisuja.

Toisena aiheena siirryttiin käsittelemään verkkosegmentoinnin toteuttamista. Nykyinen verkko ei täytä VAHTIn vaatimuksia 5.5 ja 5.23 (taulukko 4). Koska 802.1x-menettelyä ei voida ottaa käyttöön kaikkien päätelaitteiden osalta, liityntärajapinnassa toteutettava verkkoresurssien jakoa ei voida täysimittaisesti toteuttaa. Tämä tarkoittaa sitä, että verkkosegmentointi tulee toteuttaa sairaalaverkon jokaisella verkkotasolla, jolloin sairaalaverkko tultaisiin jakamaan loogisiin osiin myös runkoverkon osalta. Asiantuntijoiden yhteinen mielipide oli, että verkkosegmentointi on suositeltavaa toteuttaa palomuurien avulla. Palomuurien avulla verkko pystytään jakamaan haluttuihin segmentteihin ja jaetuille segmenteille pystytään kohdistamaan niiden tarvitsemat verkkoresurssit. Muutostyö kuitenkin tarvitsee tarkempaa suunnittelua, koska muutokset kohdistuvat koko sairaalaverkkoon Varsinais-Suomen sairaanhoitopiirin alueella. Muutostyön aikana kaikille sairaalaverkkoon liitetyille päätelaitteille tulee turvata niiden tarvitsemat verkkopalvelut.

Näin laajat sairaalaverkkoon kohdistuvat muutokset ovat tämän opinnäytetyön ulkopuolella.

Viimeisenä aiheena käsiteltiin verkon aktiivilaitteita ja runkoverkon toteutusta verkkolaajennusten yhteydessä. Yleisesti hyväksi käytännöksi on muodostunut toteuttaa uuden rakennuksen liittäminen nykyiseen sairaalaverkkoon kahden nousujakamon kautta. Näihin nousujakamoihin sijoitettaviin reitittäviin kytkinpareihin tuodaan liityntärajapinnan asiakaskytkinten LACP-kanavat. Rakennusvaiheessa tulee huomioida riittävä valokuitukapasiteetti, jotta suurikin asiakaskytkinten määrä voidaan kahdennetusti kuljettaa kerroksissa sijaitsevista laitetiloista nousujakamoihin. Riittävällä valokuitukapasiteetilla pystytään välttämään verkon aktiivilaitteiden ketjuttamista. Tämä omalta osaltaan parantaa verkon vikasietoisuutta. Liityntärajapinnassa asiantuntijat suosittelivat yksittäisten kytkinten käyttöä pinokytkinten sijasta. Pinokytkimet todettiin huollon ja ylläpidon kannalta hankalammaksi vaihtoehdoksi kuin yksittäiset kytkimet, joten niiden käyttöä suositeltiin välttämään. Silti esimerkiksi rajallinen valokuitukapasiteetti laitetilojen välillä tai suuri porttimäärien tarve liityntärajapinnassa edelleen puoltavat pinokytkinten käyttöä.

Nykyisissä sairaalaverkkototeutuksissa on sairaanhoitopiirien välisiä eroja. Tulevaisuudessa on hyvä yhtenäistää verkkosuunnittelun hyväksi havaittuja käytäntöjä ja sopia yhteiset suunnitteluperiaatteet tulevien verkkolaajennuksien osalle.

5 YHTEENVETO

Työn tarkoituksena oli perehtyä modernin tietoliikenneverkon suunnitteluun sairaalaympäristössä ja kohteiksi valittiin tulevat sairaalaverkon laajennukset. Työ aloitettiin kuvaamalla nykyisen sairaalaverkon rakenne haastattelemalla asiantuntijoita, tutustumalla yrityksen dokumentaatioihin nykyisestä verkkototeutuksesta sekä kiertokäynnillä konesaleihin, runkoverkon ja osastojen laitetiloihin. Kuvauksen avulla saatiin hyvä ymmärrys sairaalaverkon nykytilasta ja sen suunnitteluperiaatteista.

Nykyisen verkkoarkkitehtuurin lisäksi suunnitteluun oleellisesti tulevat vaikuttamaan verkkoon liitettävät päätelaitteet. Tutkimuksissa kävi ilmi, että sairaalaverkkoon liitettävät päätelaitteet voidaan karkeasti jakaa kolmeen eri laiteryhmään. Ensimmäisen ryhmän muodostavat yrityksen ylläpitämät päätelaitteet, joille annetaan täysi tuki niin laitteiden kuin sairaalaverkon ja verkkopalveluiden osalta. Toisen ryhmän muodostavat laitteet, joille taataan verkkoyhteensopivuus ja pääsy verkon tuottamiin palveluihin. Kolmas ryhmä koostuu laitteista, joille luodaan pääsy vierailijaverkon kautta internetin tarjoamiin palveluihin. Vierailijaverkosta ei ole suoraa pääsyä VSSHP:n sisäisiin verkkopalveluihin. Nämä laitteet ovat pääasiassa potilaiden tai omaisten mukanaan tuomia päätelaitteita.

Yrityksen hallinnoima sairaalaverkko tullaan auditoimaan liitteessä 1 esitettyjä valtiovarainministeriön VAHTI-sisäverkko-ohjeen mukaisesti ja verkon tulee täyttää perustason vaatimukset. Verkon nykytilaa tutkimalla pystyttiin tekemään poikkeama-analyysi ohjeen tarkistuslistoja vastaan. Analyysissa havaittiin puutteita verkkosegmentoinnin toteuttamisessa sekä sairaalaverkkoon liitettävien päätelaitteiden tunnistautumisessa. Nämä kohdat nostettiin myös osaksi asiantuntijahaastatteluita.

Hyvien suunnittelukäytäntöjen ja kokemusperäisen tiedon hyödyntäminen tulevissa sairaalaverkkolaajennuksissa nähtiin oleelliseksi osaksi suunnitteluprosessia. Näitä tietoja pyrittiin keräämään asiantuntijahaastatteluiden yhteydessä. Haastattelun tutkimuskysymykseksi muodostui:

Mitä hyviä käytäntöjä ja kokemuksia aikaisemmista verkkolaajennuksista voidaan soveltaa uusien verkkojen suunnittelussa?

Tutkimuskysymystä tuettiin aihealueilla, jotka jakautuivat verkkosegmentointiin, verkon aktiivilaitteisiin ja verkon kaapelointiin. Haastatteluista saatiin hyviä huomioita tulevien

verkkolaajennusten suunnitteluun sekä muutamia ideoita toimintatapojen kehittämiseen ja yhdenmukaistamiseen.

Haastatteluista saadun tiedon pohjalta voidaan todeta, että verkon jakaminen loogisiin osiin tulisi toteuttaa kaikilla verkon tasoilla. Asiantuntijoiden yhteinen mielipide oli, että kyseinen jako kannattaa toteuttaa palomuurien avulla, jolloin jaetuille segmenteille pystytään kohdistamaan niiden tarvitsemat verkkoresurssit. Palomuureilla toteutettua verkkosegmentointia voidaan tarvittaessa tukea 802.1x-menettelyllä. Huomioitavaa kuitenkin on, että verkon loogista jakoa ei voida luoda pelkästään 802.1x-menettelyn avulla, koska päätelaitekannan monimutkaisuudesta johtuen kaikki päätelaitteita ei välttämättä pystytä tunnistamaan. Tämä saattaa johtaa tilanteeseen, jossa potilasturvallisuus saattaisi vaarantua.

Haastatteluiden kautta saatiin suunnittelusuositusten ohella hyviä aloitteita käytäntöjen yhdenmukaistamiseen toimipisteiden välillä. Työssä tarkasteltiin verkon suunnittelua yleisesti ja tästä johtuen työn todellinen hyöty ilmenee konkreettisesti vasta tulevaisuudessa tehtävien verkkolaajennusten yhteydessä. Opinnäytetyössä esitetyt asiat, kuten verkkosegmentoinnin ja 802.1x-menettelyn toteutuksen suunnitteleminen ovat seuraavia toimenpiteitä, joita tämän tutkimuksen pohjalta suositellaan aloitettaviksi.

LÄHTEET

Academy, C.N. 2014, *Scaling networks: companion guide,* Cisco Press.

Cisco Systems Inc. 2016, Aug 25,-last update*, Cisco Wireless Services Module 2 Controller data sheet*
. Available: http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/wireless-services-module-2-wism2/data_sheet_c78-645124.html [2017, Jan 22,].

Cisco Systems Inc. 2014, Jan 08,-last update*, Cisco Open Network Environment: Bring the Network Closer to Applications*. Available: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-1000v-switch-vmware-vsphere/white_paper_c11-728045.html [2016, Dec 15,].

Cisco Systems Inc. 2009a, Feb 25,-last update*, Integrate Cisco Service Modules with Cisco Catalyst 6500*
Virtual Switching System 1440. Available: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-virtual-switching-system-1440/109550-vss-svc-mod-integration.pdf.

Cisco Systems Inc. 2009b, Sep 17,-last update*, Virtual Switching System (VSS) Q&A*. Available: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod_qas0900aecd806ed74b.html.

Froom, R. & Frahim, E. 2015, *Implementing Cisco IP switched networks (SWITCH) foundation learning guide,* Cisco Press, Indianapolis, IN.

Hauser, J.R. & Clausing, D. 1988, May,-last update*, The House of Quality*. Available: https://hbr.org/1988/05/the-house-of-quality [2017, Mar 14,].

HL7 Finland ry 2016, *, HL7 Finland ry*
. Available: http://www.hl7.fi/ [2016, 16.12.].

HL7 International 2016, *, HL7 International*. Available: http://www.hl7.org/implement/standards/index.html [2016, 16.12.].

ISO/TC 258 (SFS-julkaisut) Project, programme and portfolio management 2012, *SFS-ISO 21500 Ohjeita projektinhallinnasta,* 1st edn, Suomen Standardisoimisliitto SFS ry, Helsinki.

Kosola, J.P., Pasi 2004, *Vaatimustenhallinnan soveltaminen puolustusvoimissa*
, 2nd edn, Edita Prima Oy, Helsinki.

Lindman, A. 2016, *Teollisen Internetin, IoT:n ja Big datan testaus ja liiketoimintamahdollisuudet*
, Lappeenrannan teknillinen yliopisto.

Paradis, T. 2014, *Software-Defined Networking*, KTH Royal Institute of Technology, Stockholm.

Pohl, K., Rupp, C., Weyer, T., Tenbergen, B. & Bednarczyk, M. 2011, *Requirements engineering fundamentals : a study guide for the certified professional for requirements engineering exam : foundation level, IREB compliant,* Rocky Nook, Santa Barbara (CA).

Reponen, J. 2010, *Teleradiology—changing radiological service processes from local to regional, international and mobile environment*, Oulun yliopisto.

Sosinsky, B. 2009, *Networking bible,* Wiley, Indianapolis, IN.

Valtiohallinnon tietoturvallisuuden johtoryhmä 2010, *Sisäverkko-ohje,* 1st edn, Juvenes Print, Tampereen yliopistopaino Oy, Helsinki.

VAHTI-SISÄVERKKO-OHJEEN TARKISTUSLISTAT

5.6 Verkon rakenteen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
5.1	Verkolle on määritelty omistaja.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.2	Verkon rakenne ja vastuu suunnittelusta ja ylläpidosta on selkeästi määritelty ja dokumentoitu.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.3	Verkkorakenne on dokumentoitu ja dokumentaatiota ylläpidetään.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.4	Verkkoinfrastruktuurin hankintaan ja kehittämiseen on olemassa määrämuotoinen prosessi.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.5	Eri verkot tai niiden osat on eristetty toisistaan loogisesti tai fyysisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.6	Liikennettä sisä- ja ulkoverkon välillä rajoitetaan teknisesti siten, että vain tarpeellinen liikenne päästetään läpi.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.7	Ylläpitoon tarkoitetut etähallintayhteydet työasemiin on sallittu ainoastaan ylläpitohenkilöstölle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.8	Sallitut yhteydet ulkoverkosta on dokumentoitu ja hyväksytetty organisaation tietoturvallisuudesta vastaavalla henkilöllä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.9	Verkkoliitännät yleisölle avoimissa tiloissa on suojattu siten, että organisaation sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.10	Muutokset verkkoon testataan, katselmoidaan ja toteutetaan muutoshallintaprosessin mukaisesti.	vahva suositus	vahva suositus	pakollinen vaatimus
5.11	Hallinta-/valvontatoiminta on erotettu muusta verkon liikenteestä esim. loogisesti erilliseen verkkoon.	suositus	vahva suositus	pakollinen vaatimus
5.12	Verkkojen väliset yhteydet on kartoitettu ja hyväksytty riskianalyysin kautta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.13	Ulkoiset yhteydet on rakennettu keskitettyjen pisteiden kautta.	suositus	vahva suositus	pakollinen vaatimus
5.14	Vaihtoehtoiset tiedonsiirtoreitit ja -resurssit on toteutettu, dokumentoitu ja hyväksytetty asianmukaisilla tahoilla.	suositus	vahva suositus	pakollinen vaatimus
5.15	Kriittiset verkon komponentit on kahdennettu.	suositus	vahva suositus	pakollinen vaatimus
5.16	Suorat, ulkoverkosta sisäverkkoon otetut yhteydet on estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.17	Ulkoverkkoon tarjottavat palvelut sijaitsevat sisäverkosta erotetussa DMZ-alueessa.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.18	Verkon ylläpitäjille järjestetään säännöllistä tietoturvakoulutusta.	suositus	vahva suositus	pakollinen vaatimus

5.19	Verkon rakenne on suunniteltu kestämään nykyinen ja arvioitu tuleva liikennemäärä.	suositus	vahva suositus	vahva suositus
5.20	Verkko on jaettu loogisesti erillisiin aliverkkoihin, joihin palvelut jaetaan käyttötarkoituksensa mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.21	Suorat, sisäverkosta ulkoverkkoon otetut yhteydet on oletuksena estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.22	Ulkoverkkoon otetaan yhteyttä erityisten välityspalvelinten (proxy) kautta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.23	Fyysinen verkko on jaettu vyöhykkeisiin eri käyttötarkoituksien mukaan.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

6.1 Suojattavien kohteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
6.1	Uutta verkkoa, verkkoaluetta tai segmenttiä pystytettäessä se suojataan tietoturvallisuus huomioiden, riippumatta siitä onko se heti käytössä vai ei.	vahva suositus	vahva suositus	pakollinen vaatimus
6.2	Verkon koko olemassaolon ajan analysoidaan säännöllisesti tietoturvaratkaisujen riittävyyttä suhteessa verkossa kulkevaan tietoon.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
6.3	Verkko on suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
6.4	Kaikille tiedoille, järjestelmille ja palveluille on määritelty omistaja. Omistaja on henkilö tai taho, joka on hallinnollisesti vastuussa ao. kohteen määritelmistä, kuten tietoaineiston luottamuksellisuuden tasosta.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
6.5	Verkossa talletettava tai kulkeva tieto on luokiteltu sen luottamuksellisuuden mukaan käyttäen olemassa olevaa ja hyväksyttyä tiedon luokittelun menetelmää.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
6.6	Verkon suunnittelu ja sen ratkaisut aloitetaan analyysillä siitä, mitä tietoa verkossa tallennetaan	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

7.1 Uhkien ja vaatimusten tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
7.1	Sisäverkon suojaaminen perustuu riskianalyysiin	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.2	Sisäverkon tietoturvallisuus auditoidaan säännöllisesti ulkopuolisen tahon toimesta	suositus	vahva suositus	pakollinen vaatimus
7.3	Yhteistyökumppanien pääsy verkkoon on rajattu tehokkaasti, erityisesti ylläpitoyhteyksien osalta.	vahva suositus	vahva suositus	pakollinen vaatimus
7.4	Päätelaitteiden ja palvelinten tietoturvallisuus on hoidettu riittävällä tasolla ja verkon ja sen tietoturvallisuuden vastuuhenkilö on nimetty	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.5	Verkosta vastuussa oleva henkilö pitää huolta siitä, että päätelaitteiden ja palvelinten tietoturvallisuus on vastuutettu ja hoidettu.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.6	Organisaation riskianalyysi kattaa yleisimmät uhat, joista kappaleen 7 alussa on esimerkkejä.	suositus	vahva suositus	pakollinen vaatimus
7.7	Verkosta vastuussa oleva henkilö on nimetty	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.8	Tietoverkko toteuttaa niitä periaatteita, joita ylempi johto on tietoturvallisuudelle asettanut.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.9	Päätelaitteet on kovennettu suojaustason edellyttämän tason mukaisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.10	Hajasäteilysuojausten on vastattava niille asetettuja vaatimuksia. *	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

* Lisätietoa hajasäteilysuojausten vaatimuksista voi kysyä Viestintäviraston NCSA-FI-yksiköstä.

8.1 Yhteistyöstä muiden toimijoiden kanssa tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
8.1	Yhteistyökumppanin kanssa tehdyssä sopimuksessa on selkeästi määritelty ainakin seuraavat asiat: SLA, sanktiot, seuranta, auditointi, taustaselvitykset, turvallisuussopimus ja vastuualueet	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.2	Keskeisille verkon laitteille, liitännöille ja palveluille on palvelusopimuksin (SLA) tai muuten ylläpitojärjestelyin taattava kohteen kriittisyyttä vastaava ylläpitotaso.	suositus	pakollinen vaatimus	pakollinen vaatimus
8.3	Palveluntarjoajan kanssa on sovittu henkilöt, jotka on kiinnitetty organisaation käyttöön ainakin normaaliolojen häiriötilanteiden aikana	suositus	vahva suositus	pakollinen vaatimus
8.4	Yhteistyökumppanin kanssa järjestetään säännöllisiä seurantapalavereja	suositus	vahva suositus	pakollinen vaatimus
8.5	Ulkoistuskumppanit on velvoitettu sitoutumaan vastaaviin tai tiukempiin tietoturvamenettelyihin lähiverkkoon liittyvissä asioissa kuin organisaatio itse sitoutuu	Vahva suositus	pakollinen vaatimus	pakollinen vaatimus
8.6	Ennen kilpailutusta on tehty riskianalyysi, jossa arvioidaan potentiaalisten yhteistyökumppanien aiheuttamat tietoturvariskit ja mahdolliset parannukset tietoturvallisuuden kannalta	suositus	vahva suositus	pakollinen vaatimus
8.7	Ennen kilpailutusta on selvitetty, missä maassa potentiaaliset yhteistyökumppanit käsittelevät salassa pidettäviä tietoja nyt ja tulevaisuudessa sekä selvitetään, vaikuttaako tietojen säilytyspaikka kilpailutuksen ehtoihin	suositus	pakollinen vaatimus	pakollinen vaatimus
8.8	Ulkoistuskumppania vaihdettaessa on varmistuttu siitä, että siirtovaiheessa tietoturvallisuuden taso ei laske.	suositus	pakollinen vaatimus	pakollinen vaatimus
8.9	Mikäli yhteistyökumppanilla on pääsy salassa pidettävään tietoon, määritellään sopimukseen henkilöstön tarvittavat turvallisuusselvitykset.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.10	Organisaation on varattava auditointioikeus verkkojen palveluntarjoajien toimintaan	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.11	Tietoturvapoikkeamien hallinta on suunniteltu, ohjeistettu, koulutettu, dokumentoitu ja erityisesti viestintäkäytännöt ja –vastuut on sovittu.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
8.12	Verkkojen tietoturvapoikkeamista on lisäksi ilmoitettava välittömästi turvallisuusviranomaiselle (esim. CERT-FI) tai tiedon omistajan (toimivaltaisen viranomaisen) hyväksymälle taholle.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

9.2 Kaapeloinnin tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
9.1	Kaapelointi on hyväksytty ao. kaapeliluokalle määritellyn virallisen tyyppitestausmenettelyn mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.2	Kaapelit kulkevat kytkeytymistä ja fyysisiä vaurioita ehkäisevissä rakenteissa.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.3	Jakamot, ristikytkentäpaikat ja verkon aktiivilaitteet sisältävät telineet sijaitsevat lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.4	Kaapelointi on dokumentoitu ja näkösuojaan jäävät kaapelit on nimiöity dokumentteja vastaavasti molemmista päistään.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.5	Käyttämättömät liitäntäpisteet on irrotettu aktiivilaitteesta tai ao. laitteen portit estävät oletuksena uusien asemien vapaan liittämisen sisäverkkoon.	suositus	vahva suositus	pakollinen vaatimus

10.2 Langattomien lähiverkkojen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
10.1	WLANia ei oteta käyttöön ilman riskianalyysiä	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.2	WLAN auditoidaan ulkopuolisen auditoijan toimesta	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.3	WLANin tietoturvallisuutta ja suorituskykyä valvotaan ja hallitaan keskitetysti tai muulla tavoin.	suositus	pakollinen vaatimus	Pakollinen vaatimus
10.4	Vierailijaverkko: Langaton vierailijaverkko on toteutettava siten, että se on fyysisesti tai loogisesti eriytetty sisäverkosta ja siitä on vain yhteys Internetiin.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.5	Vierailijaverkko: Langattoman vierailijaverkon Internet-yhteys on kytketty erillisen Internet-liittymän kautta tai muuten hallitusti rajoitetaan ja estetään sen mahdollisuus häiritä tai tutkia sisäverkon Internet-liikennettä	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.6	Vierailijaverkko: WLANin liikenne tulee olla vahvasti salattu.	vahva suositus	pakollinen vaatimus	Pakollinen vaatimus
10.7	Vierailijaverkko: WLANissa on käyttäjille vahva tunnistusmenettely.	vahva suositus	vahva suositus	Pakollinen vaatimus
10.8	Vierailijaverkko: WLANiin liittyvä laite ja WLAN tunnistavat toisensa luotettavasti.	vahva suositus	vahva suositus	Pakollinen vaatimus
10.9	Sisäverkkoon liitetty WLAN-verkko: WLANin liikenne tulee olla vahvasti salattu.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus

10.10	Sisäverkkoon liitetty WLAN-verkko: WLANissa on käyttäjille vahva tunnistusmenettely.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.11	Sisäverkkoon liitetty WLAN-verkko: WLANiin liittyvä laite ja WLAN tunnistavat toisensa luotettavasti.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus

11.2 Verkon aktiivilaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
11.1	Verkolle on tehty riskianalyysi ja tämän tuloksena keskeiset verkkolaitteet, niiden komponentit (esim. virtalähde) ja yhteydet on tarvittaessa kahdennettu.	vahva suositus	vahva suositus	pakollinen vaatimus
11.2	Keskeisillä laitteilla on UPS ja kaikki verkon laitteet palautuvat virtakatkon jälkeen normaalitoimintaan.	suositus	vahva suositus	vahva suositus
11.3	Sisäverkon tietoturvallisuudeltaan erilaiset vyöhykkeet on eristetty toisistaan palomuurilla tai reitittimen pääsylistoilla. DMZ on eristetty sisäverkosta palomuurilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.4	Sisäverkkoon liitetyt aktiivilaitteet tunnistetaan vahvasti esim. 802.1X-menettelyllä, jolla estetään tuntemattomien laitteiden liittäminen.	suositus	vahva suositus	pakollinen vaatimus
11.5	Verkkolaitteiden hallintaliitäntään pääsevät kytkeytymään vain hallinnasta vastaavat ennalta määritellyt henkilöt ja laitteet. Laitteiden hallintayhteydellä käytetään vahvaa salausta ja käyttäjän tunnistusta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
11.6	Verkkolaitteissa on vaihdettu tunnistukseen liittyvät toimittajien oletusparametrit.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.7	Hallintayhteydet (esim. SNMP) on eriytetty omaan verkkosegmenttiinsä.	suositus	vahva suositus	pakollinen vaatimus
11.8	SNMP-protokollasta on käytössä vähintään versio 3, jos laitteisiin tehdään muutoksia. Jos laitteista vain luetaan tietoa, SNMP-protokollan on oltava vähäntään versio 2c.	vahva suositus	vahva suositus	pakollinen vaatimus
11.9	SNMP-protokollalla on pienimmät mahdolliset oikeudet tai se on poistettu käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.10	Tarpeettomat palvelut, ohjelmat ja protokollat on poistettu verkon aktiivilaitteista käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.11	Verkkolaitteiden asetukset on tallennettu ja varmuuskopioitu mahdollista laitteen vaihtoa ja asetusten palauttamista varten.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

11.12	Kytkimen työasemaportit on erotettu toisistaan s.e. työasemat eivät voi nähdä toistensa liikennettä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
11.13	Käytössä on verkkotason tunkeilijan tunnistus- (IDS) ja estojärjestelmä (IPS)	suositus	vahva suositus	pakollinen vaatimus
11.14	Laiteiden lokitiedot kerätään keskitetysti ja niitä seurataan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus

12.2 Verkon aktiivilaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
12.1	Organisaation liiketoiminnan vaatimusten pohjalta on arvioitu yhteyksien kriittisyys ja sovittu palvelutasoista (SLA) palveluntarjoajan kanssa.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.2	Kriittiset toimipisteiden väliset tai internet-yhteydet on kahdennettu.	suositus	suositus	pakollinen vaatimus
12.3	Kriittiset sovellukset ja protokollat luokitellaan palvelulaatumäärittelyssä (QoS) muita sovelluksia korkeammalle tasolle.	suositus	vahva suositus	pakollinen vaatimus
12.4	Kansallisen salassa pidettävän tiedon siirrossa käytetään salausta, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	suositus	suositus	pakollinen vaatimus
12.5	Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.6	Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

13.2 Päätelaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
13.1	Internet-palveluiden käyttö on sallittu ainoastaan organisaation sisäverkosta tai etäyhteyden (VPN) kautta.	suositus	pakollinen vaatimus	pakollinen vaatimus
13.2	Kullakin päätelaitteella on yksilöity tunnus. Identtiset laitekokoonpanot erotetaan em. tunnuksen perusteella.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
13.3	Käyttäjille on laadittu lyhyet, selkeät ohjeet päätelaitteiden turvallisesta verkkokäytöstä - kullekin päätelaitetyypille omansa.	suositus	pakollinen vaatimus	pakollinen vaatimus
13.4	Tuntemattomien päätelaitteiden kiinnittäminen verkkoon on estetty kytkinporttien asetuksilla.	suositus	vahva suositus	pakollinen vaatimus
13.5	Työasemilta avatuissa etäyhteyksissä on automaattinen aikakatkaisu.	suositus	vahva suositus	pakollinen vaatimus
13.6	Päätelaitteissa on soveltuvilta osin käytössä laitekohtainen palomuuri.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

13.7	Päätelaitteille suoritetaan automaattinen terveystarkastus ennen niiden liittämistä sisäverkkoon.	suositus	suositus	suositus
13.8	Työasema- ja muu päätelaitekanta on yhtenäistetty.	suositus	suositus	vahva suositus
13.9	Mobiililaiteiden loppukäyttäjiä on ohjeistettu niiden turvalliseen käyttöön, esimerkiksi käyttäen pohjana ja muokaten Älypuhelinten turvallinen käyttö –ohjetta (VAHTI 2/2007, muokattava liite)	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
13.10	Työasemissa on käytössä työasemakohtainen palomuuri.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
13.11	Kannettavien työasemien kiintolevyt on salattu	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
13.12	Pöytätyöasemien kiintolevyt on salattu	suositus	vahva suositus	pakollinen vaatimus

14.3 Palveluiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
14.1	Sisäverkon reititysprotokollaksi on valittu suojattua tunnistautumista tukeva protokolla.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.2	Sovellusten tietoturvapäivitykset pidetään ajan tasalla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.3	Kriittisten infrapalveluiden, eli osoite-, reititys- ja nimipalvelun toimivuus on varmistettu tarkoituksen mukaisella palvelutasolla ja varautumisen tasolla	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.4	Ylimääräisten infrapalveluiden asentaminen sisäverkkoon on kielletty.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.5	DNSSEC on otettu käyttöön.	vahva suositus	vahva suositus	pakollinen vaatimus
14.6	Vastaanotetut ja lähetettävät sähköpostit skannataan virusten, haittaohjelmien ja roskapostien varalta.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.7	Resurssien jako (esim. kiintolevy, tulostin) on rajattu palvelinlaitteille. Työasemien resurssien jako on estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.8	Palveluiden määrä palvelimilla on minimoitu. Yksi palvelin (fyysinen tai virtuaalinen) hoitaa pääasiassa yhtä tehtävää (esim. WWW-palvelin, DNS-palvelin, tiedostopalvelin).	vahva suositus	vahva suositus	pakollinen vaatimus
14.9	Sisäverkossa on oma NTP-palvelin verkon laitteiden ajan synkronoimiseen. NTP-palvelin synkronoidaan joko ulkoisen NTP-palvelun tai palvelimeen liitetyn radiokellon kanssa.	suositus	vahva suositus	pakollinen vaatimus
14.10	DMZ-alueella käytetään pelkästään staattista reititystä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

15.2 Tunnistautumisen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
15.1	Tunnistautumisten lajeista on valittu sopivat menetelmät ja valinta perustuu analyysiin tunnistautumis-tarpeesta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.2	Käyttäjän tunnistamisessa käytetään henkilökohtaisia tunnuksia. Tämä koskee myös ylläpitotunnuksia.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.3	Etäyhteyksien muodostamiseen ei käytetä pelkkää käyttäjätunnus-/salasanaparia.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.4	Kaikki käyttäjät ja päätelaitteet ovat hallittujen tunnistautumisratkaisu-jen piirissä.	vahva suositus	vahva suositus	pakollinen vaatimus
15.5	Toimikorttia käytetään silloin, kun on tarve tehdä vahva tunnistaminen. Mikäli toimikortti ei ole käytössä, teh-dään vahva tunnistaminen käyttämäl-lä vaihtuvaa salasanaa.	vahva suositus	vahva suositus	pakollinen vaatimus
15.6	Käytettäessä käyttäjätunnus-/sala-sanaparia, luodaan salasanapolitiik-ka, joka koskee kaikkia palveluita ja käyttäjiä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.7	Tunnus lukkiutuu, mikäli järjestelmään yritetään epäonnistuneesti liian monta kertaa peräkkäin.	suositus	pakollinen vaatimus	pakollinen vaatimus
15.8	Pääsynvalvontalokeja säilytetään siten, että niitä ei päästä jälkikäteen muuttamaan.	suositus	vahva suositus	pakollinen vaatimus
15.9	Organisaatiolla on kirjallinen pääsyn-valvontapolitiikka	suositus	pakollinen vaatimus	pakollinen vaatimus
15.10	Varmenteiden myöntämiseen, käyt-töön ja uusimiseen on olemassa yksi-tyiskohtainen kirjallinen ohjeistus.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.11	Käytössä olevista varmenteista on ajantasainen lista.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.12	Epäonnistuneet kirjautumisyrityk-set sekä muut valtuuksien puutte-seen kariutuvat toimenpideyritykset kirjataan.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.13	Tunnistautumiseen ei yleisesti käytetä pelkkää käyttäjätunnus-/salasanapa-ria. Vain erityisen hyvin fyysisesti suo-jatussa ympäristössä voidaan kirjautua käyttäen käyttäjätunnus/ salasanaparia.	suositus	vahva suositus	pakollinen vaatimus
15.14	Kaikkien verkkotuotteiden ja muiden valmisohjelmistojen oletustunnusten salasanat on vaihdettu oletusarvosta tai oletustunnus on poistettu.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.15	Organisaatio on määritellyt käyttäjän-hallintaprosessin, jotta voidaan var-mistua, että käyttöoikeudet vastaavat kulloistakin tehtävää.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.16	Pelkän päätelaitetunnistautumisen perusteella annetaan verkkoon vain hyvin rajattu pääsy.	suositus	vahva suositus	pakollinen vaatimus

15.17	Tunnistautumisessa käytetään menetelmiä, joissa tunnistautumiseen käytettävät tiedot, kuten käyttäjätunnukset ja salasanat eivät kulje verkon yli salaamattomana.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.18	Tunnistautumismenetelmien riittävyys arvioidaan säännöllisesti	suositus	vahva suositus	pakollinen vaatimus
15.19	Verkon ylläpitämiseen käytettävät tunnukset sidotaan ylläpitovarmenteisiin tai ne kirjoitetaan ylös ja talletetaan turvalliseen paikkaan, kuten kassakaappiin. Yksittäinen henkilö ei saa ottaa tunnuksia kassakaapista.	suositus	vahva suositus	pakollinen vaatimus
15.20	Ylläpitäjät omaavat laajat valtuudet, joten avoimien verkkojen kautta toimittaessa heidän tunnistautumiseensa käytetään vahvaa tunnistautumista	suositus	pakollinen vaatimus	pakollinen vaatimus

16.2 Hallinnan/valvonnan tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
16.1	Lokit tallennetaan keskitetylle lokipalvelimelle.	suositus	vahva suositus	pakollinen vaatimus
16.2	Laitteiden lokiasetukset on määritetty sellaisiksi, että lokeista saadaan riittävästi tietoa verkon toiminnasta	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.3	Muutokset verkkoon tehdään suunnitteluvaiheiden periaatteiden mukaisesti.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.4	Hallintaliikenne salataan riittävällä tasolla, jotta ulkopuolinen henkilö ei pysty seuraamaan tehtäviä muutoksia eikä tunnistautumaan hallintakäyttäjänä	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.5	Verkon hallinnan yhteydessä jokaisesta muutoksesta otetaan varmuuskopio	vahva suositus	vahva suositus	pakollinen vaatimus
16.6	Etukäteen on määritelty, mitä asioita verkossa valvotaan.	vahva suositus	vahva suositus	pakollinen vaatimus
16.7	Hyökkäyksien havaitsemiseen ja hyökkäyksien torjumiseen käytetään niihin tarkoitettuja IDS/IPS laitteita ja ohjelmistoja	suositus	vahva suositus	vahva suositus
16.8	Lokit suojataan muutoksilta.	vahva suositus	vahva suositus	pakollinen vaatimus
16.9	Ulkoistettaessa verkon hallinta, • Määritellään hyvin tarkasti se, miten ja mitä toimenpiteitä ulkoistuskumppani tekee, miten ja millä toimenpiteillä valvontaa ja hallintaa tehdään • Säilytetään itsellä riittävä perusosaaminen verkoista, jotta voidaan ostaa siihen liityviä palveluita	vahva suositus	vahva suositus	pakollinen vaatimus

16.10	Verkkolaitteiden ohjelmistot päivitetään valmistajan suositusten mukaisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.11	Verkon hallintaan ja valvontaan on määritelty selkeät vastuuhenkilöt	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.12	Käytetyt hallintaprosessit on dokumentoitu.	suositus	vahva suositus	pakollinen vaatimus
16.13	Käytetyt valvontaprosessit on dokumentoitu.	suositus	vahva suositus	pakollinen vaatimus
16.14	Verkkolaitteiden kuormitustilannetta valvotaan.	suositus	vahva suositus	pakollinen vaatimus
16.15	Lokeista pystytään jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta (audit trail).	suositus	vahva suositus	pakollinen vaatimus
16.16	Verkon ylläpitoon ja tietoturvallisuuden määritysten muuttamiseen on käyttöoikeus vain niillä käyttäjillä, jotka tarvitsevat niitä työtehtävissään.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

16.17	Verkon etäylläpitoon käytetään vain turvallisinta osajoukkoa niistä välineistä, joita käytetään tavalliseen verkon ylläpitoon	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.18	Verkon lokeja ja erityisesti etäylläpidon lokeja käydään läpi säännöllisesti	suositus	pakollinen vaatimus	pakollinen vaatimus
16.19	Verkon fyysiset komponentit käydään säännöllisesti läpi tarkastaen, että niiden rakenne vastaa dokumentaatiota. Tarkoituksena on löytää mahdolliset merkit murtautumisyrityksistä. [merkkejä lukkojen väkivaltaisesta rikkomisesta tai ylimääräisiä verkkolaitteita ja kaapeleita]	suositus	vahva suositus	pakollinen vaatimus
16.20	Verkon hallinta ja valvonta tehdään laitteilla, jotka on fyysisesti erotettu muista työasemista.	suositus	vahva suositus	pakollinen vaatimus
16.21	Valvontaan ja hallintaan käytettävät sovellukset on määritelty	suositus	vahva suositus	pakollinen vaatimus
16.22	Verkon ylläpitäjä tarkistaa säännöllisesti verkon tietoturvallisuuden tason	suositus	vahva suositus	pakollinen vaatimus
16.23	Käyttäjät koulutetaan ilmoittamaan havaituista puutteista, ongelmista ja niiden epäilyistä esimiehelle, tietoturvavastaavalle tai verkon vastuuhenkilölle	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.24	Ylläpitopääsy verkon laitteille on rajoitettu verkon valvonta- ja hallintatyöasemille. Rajaus on toteutettu verkon sisällä sekä verkon ulkopuolella etäylläpidossa.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.25	Valvontaan käytetyillä tunnuksilla on vain lukuoikeus verkon lokitietoihin	suositus	vahva suositus	pakollinen vaatimus

17.3 Jatkuvuussuunnittelun tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
17.1	Organisaatiossa on toteutettu ja vastuutettu järjestelmien häiriöiden selvitys ja niistä toipuminen. Organisaation kaikki järjestelmät ja toiminnot on luokiteltu niiden kriittisyyden mukaan. Perustuen kriittisyysluokitteluun ja analyysiin eri järjestelmien ja toimintojen kokonaistarpeesta, on muodostettu jatkuvuussuunnitelma ja toipumissuunnitelma, joka on johdon hyväksymä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.2	Jatkuvuussuunnitelmissa on otettu huomioon sisäverkon erityispiirteet.	suositus	vahva suositus	pakollinen vaatimus
17.3	Jatkuvuussuunnitelma sisältää ennalta-ehkäisevät ja havaitsevat menetelmät ja ratkaisut sekä tilapäiseen korjaamiseen ja varsinaiseen normalisointiin liittyvät menetelmät ja ratkaisut.	suositus	vahva suositus	pakollinen vaatimus
17.4	Menetelmät ja ratkaisut on toteutettu niin, että tavoiteltu valmiustaso todellisuudessa saavutetaan.	vahva suositus	vahva suositus	pakollinen vaatimus
17.5	Jatkuvuussuunnitelman mukainen toiminta testataan ja koulutetaan.	vahva suositus	vahva suositus	pakollinen vaatimus
17.6	Jatkuvuussuunnitelma pidetään ajan tasalla ja päivitetään vähintään vuosittain	suositus	vahva suositus	pakollinen vaatimus
17.7	Varmuuskopioilta palauttamista testataan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus
17.8	Varmuuskopiotallenteista säilytetään riittävän monta varmuuskopiosukupolvea palo- ja murtoturvallisessa paikassa.	suositus	vahva suositus	pakollinen vaatimus
17.9	Verkon vastuuhenkilöstöllä on edellytykset saattaa verkko toimintakykyiseksi. Organisaatio pystyy itse toimimaan jatkuvuussuunnitelman mukaan ilman ulkopuolisten tahojen aktiivista toimintaa.	suositus	vahva suositus	pakollinen vaatimus
17.10	Verkon häiriö- ja keskeytystilanteisiin sekä verkkohyökkäyksiin on varauduttu, järjestelyt on dokumentoitu, testattu ja ylläpidetty. Järjestelyillä varmistetaan, että tilanteen korjaamisesta vastaava henkilöstö voi keskittyä ko. työhön.	vahva suositus	vahva suositus	pakollinen vaatimus
17.11	Poikkeusoloihin varautumisessa on otettu huomioon sisäverkkojen erityinen rooli ja haavoittuvuus tiedonsiirtoväylänä.	suositus	vahva suositus	pakollinen vaatimus
17.12	Järjestelmät luokitellaan tärkeysjärjestyksittäin perustuen ICT-varautumis- ja tietoturvatasoihin	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.13	Organisaatio pitää hallussaan tai varaa laitetoimittajilta varalaitteet kriittisimpien järjestelmien rikkoutumisen varalle.	vahva suositus	vahva suositus	pakollinen vaatimus

17.14	Organisaatiolla on kirjallinen varmuuskopiointipolitiikka ja -prosessi.	suositus	vahva suositus	pakollinen vaatimus
17.15	Tärkeimmistä järjestelmistä on otettu suojakopioita, jotka säilytetään eri palotilassa kuin varsinaiset varmuuskopiot.	suositus	vahva suositus	pakollinen vaatimus
17.16	Jatkuvuussuunnitelma sisältää sekä teknisen että hallinnollisen puolen.	suositus	vahva suositus	pakollinen vaatimus
17.17	Järjestelmien häiriöistä pidetään kirjaa ja käytetään tietoa hyväksi riskianalyyseissä ja palvelutasosopimusten teossa.	suositus	pakollinen vaatimus	pakollinen vaatimus
17.18	Jatkuvuussuunnitelman mukaisia toimia harjoitellaan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus
17.19	Varayhteydet ja -kapasiteetti pidetään jatkuvasti aktiivisena	suositus	suositus	vahva suositus
17.20	Toiminnan kannalta kriittiset palvelut on kahdennettu tai monistettu niin, että kriittiset palvelut saadaan useamman kuin yhden palvelimen kautta	suositus	vahva suositus	pakollinen vaatimus
17.21	Käyttäjiä ohjeistetaan säilyttämään työtiedostonsa palvelimilla	suositus	vahva suositus	pakollinen vaatimus
17.22	Mikäli sisäverkon toiminta on organisaation toiminnalle kriittistä, säilytetään riittävä osaaminen organisaation sisällä tai sopimuksin varmistettava, että riittävä osaaminen ulkoistuskumppanilta on aina saatavissa	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.23	Suunnittelussa ja sitä edeltävässä analysoinnissa on otettu huomioon muun muassa: • Organisaation toiminnan jatkuvuuden turvaaminen ja tehtävien suorittaminen • Välttämättömän tietojenkäsittelytoiminnan ylläpitäminenpoikkeusolojen vaikutuksista huolimatta • Valtiovallan asettamien kriisiajan valmiusvaatimusten täyttäminen • Tietojenkäsittelytoiminnan siirtojärjestelyihin varautuminen • Tietojenkäsittelytoiminnan supistamis- ja korvaamisjärjestelyihin varautuminen • Edellytysten luominen normaaliolojen tilanteeseen palaamiselle	vahva suositus	vahva suositus	pakollinen vaatimus
17.24	Normaaliolojen käytettävyyttä turvaavat varajärjestelyt on rakennettu niin, että ne tukevat myös poikkeusolojen vaatimuksia ja ratkaisuja	suositus	vahva suositus	pakollinen vaatimus
17.25	Varmuuskopioinnin onnistumista valvotaan systemaattisesti.	vahva suositus	vahva suositus	pakollinen vaatimus
17.26	Varmuuskopiot otetaan myös ennen olennaisia muutoksia ja niiden jälkeen.	vahva suositus	vahva suositus	pakollinen vaatimus

HAASTATTELURUNKO

Opinnäytetyön haastattelu aineiston keräämistä varten

Tutkimuskysymys:

Mitä hyviä käytäntöjä ja kokemuksia aikaisemmista verkkolaajennuksista voidaan soveltaa uusien verkkojen suunnittelussa?

1. Verkkosegmentoinnin toteuttaminen uusien verkkolaajennusten yhteydessä:

    - Miten verkon segmentointi tulisi mielestäsi toteuttaa?
    - Miten edellä mainittu verkkosegmentointi vaikuttaa verkon aktiivilaitteisiin?
        - Reitittävät kytkimet
        - Reitittimet
    - (Miten jakaisit verkkopalveluita verkkosegmenttien välillä?)
    - Miten IoT-laitteet tulee huomioida tulevaisuudessa?
    - Mitä tietoturva-asioita pitää huomioida uutta verkkolaajennusta suunniteltaessa?
        - 802.1x (tunnistautuminen)
        - Paikalliset palomuurit (toimipistekohtaiset palomuurit)
        - Uusien / tuntemattomien laitteiden liittäminen verkkoon? (Asiakkaat, ulkopuoliset)

2. Verkkolaitteet uudessa verkkolaajennuksessa:

    - Miten mielestäsi liityntä core-kytkimille kannattaisi toteuttaa?
        - Reitittävä kytkin
        - Reititin
    - Mitä ominaisuuksia pitää huomioida valittaessa asiakaskytkimiä?
        - Stacked, tarvitaanko jatkossa?
        - PoE, porttien määrä ja tehonkulutuksen tarve
        - Porttimäärät

    - Porttinopeudet
- Paljonko laajennusvaraa laitteisiin tulee varata?
- Miten tietoturva pitää huomioida asiakasverkkorajapinnassa?

3. Kaapelointi uusissa laitetiloissa:

- Miten ristikytkentä laitetiloissa pitäisi toteuttaa?
    - Ristikytkentäpanelien sijoitus?
    - PoE- vs. normaalikytkimet
- Mitä laitetilojen dokumentointi pitäisi mielestäsi toteuttaa?
    - Kaapelien värikoodauksen huomioiminen
    - Kytkentämuutosten kirjaaminen