Korkean käytettävyyden tietoliikenneverkon toteutus erikoissairaanhoidon tarpeisiin

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tekniikan ammattikorkeakoulututkinto opinnäytetyö

Tieto- ja viestintätekniikka, HAMK Riihimäki

Syksy 2021

Erno Paju

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka Tiivistelmä

Riihimäki

Tekijä	Erno Paju	Vuosi 2021
Työn nimi	Korkean käytettävyyden tietoliikenneverkko sairaanhoidossa	
Ohjaajat	Teemu Järvenpää	

TIIVISTELMÄ

Opinnäytetyössä käsitellään uuden suuren sairaalaympäristön kriittisen verkon suunnitteluperiaatteita ja toteutusta. Koska tämän päivän sairaalassa lähes kaikki laitteet ovat liitettynä tietoverkkoon on sairaalaympäristön suunnittelun lähtökohtana hoitotoiminnan varmistaminen kaikissa tilanteissa.

Jatkuvan toiminnan varmistamiseksi suunnittelussa ja toteutuksessa kiinnitetään erityistä huomiota verkon kahdennuksiin, tietoturvaan ja huoltovarmuuteen, sekä skaalautuvuuteen. Sairaalaympäristön erityispiirteenä on se, että useat lääkintälaitteet eivät tue uusimpia verkon standardeja, kuten sertifikaattipohjaista autentikointia. Opinnäytetyön sairaalan ympäristö päädyttiin näistä lähtökohdista toteuttamaan Juniper Networks ja Cisco Systems teknologioilla.

Opinnäytetyössä kuvataan tietoliikenneverkon arkkitehtuuri ja keskeiset suunnitteluperiaatteet fyysisen ja loogisen toteutuksen osalta. Lisäksi esitellään valmistajien arkkitehtuurin malleja kampusverkkojen toteutukselle.

Työn lopputuloksena toteutettiin onnistuneesti verkkoinfra uuden ison suomalaisen erikoissairaanhoitoa tuottavaan sairaalaan. Opinnäytetyö tehtiin Istekki Oy:lle, joka suunnitteli ja toteutti hankkeen.

Avainsanat Tietoverkko, korkea käytettävyys, kriittinen ympäristö

Sivut 38 sivua ja liitteitä 2 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technology
Riihimäki

Abstract

Author Erno Paju
Subject High availability network in a medical care
Supervisors Teemu Järvenpää

Year 2021

ABSTRACT

The thesis studies the design principles and implementation of a critical network for a large new hospital environment. Since in today's hospitals almost all devices are connected to a computer network the starting point for designing a hospital environment is to ensure care operations in all situations.

To ensure continuous operation, special attention is paid to network duplication, data security and security of supply, as well as scalability in the design and implementation. A special feature of the hospital environment is that many medical devices do not support the latest network standards such as certificate-based authentication. From this starting point, it was decided that the hospital environment presented in this thesis was implemented with Juniper Networks and Cisco Systems technologies.

The thesis describes the architecture of the telecommunication network and the main design principles in terms of physical and logical implementation. In addition, manufacturers' architectural models for the implementation of campus networks are presented in this thesis.

As a result of the work, network infrastructure for a new large Finnish hospital providing special medical care was successfully implemented. The thesis was done for Istekki Oy which designed and implemented the project.

Keywords Network, high availability, critical environment

Pages 38 pages and appendices 2 pages

Lyhenteet

AD	Active Directory
ADC	Application Delivery Controller
AP	Access Point
BGP	Border Gateway Protocol
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EVPN	Ethernet VPN
ICMP	Internet Control Message Protocol
IPS	Intrusion Prevention System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
PAT	Port Address Translation
PEAP	Protected Extensible Authentication Protocol
PoE	Power over Ethernet
PSK	Pre Shared Key
RADIUS	Remote Authentication Dial In User Service
SNMP	Network Management Protocol
SSID	Service Set Identifier
TLS	Transport Layer Security
VLAN	Virtual LAN
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN
WLC	Wireless LAN Controller

Termit

802.1X	Porttikohtaisen todentamisen standardi
MAC-osoite	Laitteen verkkokortin uniikki tunnistus osoite

MPLS-L3VPN VPN reittien BGP-mainostuksiin perustuva teknologia

Sisällys

Kuvat, taulukot ja kaavat

Liitteet

Liite 1 Tietoliikenteen vaatimukset liitettäville järjestelmille

1 Johdanto

Nykyaikaisen sairaanhoidon nopean kehittymisen ja paperittomaan toimintamalliin siirtymisen myötä on verkkoon liitettävien laitteiden määrä ja kriittisyys lisääntynyt viime vuosina merkittävästi. Verkkoon liitetään hoitotoimintaan liittyvien lääkinnällisten laitteiden lisäksi esimerkiksi kiinteistöjen talotekniikka, kannettavat- ja pöytätyöasemat, mobiililaitteet ja tabletit, sekä potilasviihtyvyyteen ja opastuksiin liittyvät laitteet, kuten televisiot ja infonäytöt. Tämä asettaa verkolle ja sen toimintakyvylle monenlaisia vaatimuksia, jotka tulee huomioida verkon suunnittelussa.

Tärkeitä suunnittelun lähtökohtia on verkon segmentoinnin toteutus huomioiden skaalautuvuuden ja tietoturvan, mutta samalla mahdollistaen riittävän liitettävyyden verkossa huomioiden eri laitevalmistajien järjestelmien ja laitestandardien vaatimukset. Sairaalamaailman erityispiirre on se, että lääkintälaitteet eivät monesti tue uusimpia verkon standardeja lääkintälaitteiden sertifiointien takia.

Sairaalaympäristön suunnittelun lähtökohta on jatkuvan toiminnan varmistaminen kaikissa tilanteissa. Jatkuvan toiminnan varmistamiseksi suunnittelussa kiinnitetään erityistä huomiota verkon kahdennuksiin ja siihen, ettei verkossa ole yksittäisiä pisteitä, jotka vikaantuessaan estävät koko verkon toiminnan. Toiminnan varmistamiseksi laitteet on kyettävä myös huoltamaan ja päivittämään mahdollisimman pienin vaikutuksin verkon toimintaan.

Tässä opinnäytetyössä käsitellään Istekki Oy:n toteuttamaa uuden sairaalan verkon suunnitteluperiaatteita ja toteutusta. Opinnäytetyössä käsitellään erityisesti sitä, miten saavutetaan verkon riittävä kapasiteetti, käytettävyys, tietoturvallisuus, hallittavuus ja skaalautuvuus tulevaisuuden tarpeisiin, sekä verkon saatavuus myös vika ja huoltotilanteissa.

Toteutusta ei tehty yhden valmistajan parhaiden käytäntöjen mukaan vaan toteutuksessa yhdisteltiin eri valmistajien tekniikoiden toimiviksi todetut parhaat puolet.

Verkon tietoturva on myös erittäin tärkeässä roolissa. Tässä avaintekijöitä ovat verkon segmentointi, sekä verkkoon autentikointi.

Työssä keskitytään sairaalan tietoliikenneverkon fyysisen ja loogisen toteutuksen, sekä tietoliikenneverkosta tuotettavien palveluiden kuvaukseen. Työn rajaamiseksi, sekä tietoturvasyistä esimerkiksi palomuurien konfiguraatiota ja konfiguraatioiden yksityiskohtia ei ole lähdetty käsittelemään, vaikka ne ovatkin luonnollisesti tärkeä osa verkkoa ja sen toimintaa.

2 Keskeiset suunnitteluperiaatteet

Sairaalaympäristön suunnittelun lähtökohta on jatkuvan toiminnan varmistaminen kaikissa tilanteissa. Jatkuvan toiminnan varmistamiseksi suunnittelussa kiinnitetään erityistä huomiota käytettävyyteen, skaalautuvuuteen, huolettavuuteen ja verkon tietoturvallisuuteen.

Käytettävyys eli verkon saatavuus on verkon tärkein suunnittelun periaate ja lähtökohtaisesti sairaalassa verkko on oltava aina käytettävissä myös huoltokatkojen aikana. Verkossa sijaitsevat palvelut ovat haastavia luokiteltavia kriittisyyksien mukaan potilaan hoidon kannalta, joten lähtökohtaisesti kaikki verkkoon liitettävät järjestelmät käsitellään toteutuksen osalta kriittisinä.

Verkon muuntojoustavuus eli skaalautuvuus on otettava huomioon ja suunnitteluvaiheessa. Tietoliikenneverkon tulee kyetä mukautumaan käyttöiän aikana tuleviin käyttötarpeen muutoksiin ja mahdollistaa uusien palveluiden, sekä teknologioiden katkoton käyttöönotto tulevaisuudessa. Verkon tulee myös skaalautua, niin fyysiseltä kapasiteetiltaan, kuin loogiselta kapasiteetiltaan ylös ja alaspäin tarpeiden mukaisesti.

Huollettavuus on verkon jatkuvan palvelun edellytys. Käytettävyyden ja tietoturvan saavuttamiseksi on tietoliikennelaitteiden ohjelmistojen oltava aina ajan tasalla. Uudet ohjelmistoversiot tuovat myös uusia ominaisuuksia ja parannuksia olemassa oleviin kyvykkyyksiin. Verkkoon on siis pystyttävä tekemään päivityksiä, joiden aikana verkko pitäisi olla sairaalan hoitotoiminnan kannalta käytettävissä tai vaikutuksien oltava mahdollisimman

näkymättömiä tai vähintään rajattavissa tiettyyn osaan verkkoa. Huollettavuus on yksi merkittävä lisäarvo uuden verkon toimintakykyä parantava tekijä.

Tietoturva on oleellinen vaatimus mille tahansa verkolle. Sairaalan verkossa liikkuvan arkaluonteisen henkilötiedon välitys ja eheys on pysyttävä turvaamaan ja huomioimaan, sekä sisäiset, että ulkoiset uhkatekijät.

3 Verkolle asetetut vaatimukset ja valittu ratkaisu

Sairaalaverkolle asetetaan erityisiä vaatimuksia verraten yleisiin lähtökohtiin, koska verkkopalveluiden tulee käytännössä olla saatavilla 24/7 vuoden jokaisena päivänä. Tämän saavuttamiseksi käytetään standardoitu ratkaisuja useamman valmistajan tekniikoilla toteutettuna. Ratkaisun periaatteella pyritään vähentämään erillisten järjestelmäkohtaisten ratkaisujen määrää ja saavuttamaan käyttöiän aikaisia kustannussäästöjä ylläpitämällä aina vain yhtä toimivaa kokonaisuutta verkon eri osakokonaisuuksissa.

3.1 Käytettävyys

Kaikki sairaalan tietoliikenneyhteydet rakennetaan kahdennetusti siten, ettei yksittäisen laitteen tai yhteyden vikaantuminen aiheuta katkosta sairaalan toiminnalle. Jokaisen yksittäisen osaston päätelaitteet, langattoman verkon tukiasemat sekä talotekniikka hajautetaan vähintään kahteen erilliseen jakamokytkimeen, jotta yksittäisen kytkimen vikaantuminen ei aiheuta täydellistä katkosta osaston tietoliikenneyhteyksien toimintaan.

Sairaalan tietoliikenneverkko segmentoidaan MPLS-EVPN ja MPLS-L3VPN palveluilla, sekä järjestelmäkohtaisella aliverkotuksella pienempiin osiin. Tällä saavutetaan se, että mahdolliset vika-alueet pysyvät rajattuina, eivätkä pääse vaikuttamaan koko sairaalan alueelle. Kaikki kiinteän verkon tietoliikennelaitteet on varustettu vähintään kahdella toisiaan varmistavalla ja käytön-aikaisesti vaihdettavalla virtalähteellä. Jokainen verkon laite kytketään myös aina vähintään kahdella kytkennällä, joten yhden liitäntäportin tai optiikan vikaantuminen ei aiheuta liikenteeseen katkosta.

3.2 Skaalautuvuus

Sairaalaympäristön MPLS runkoverkossa käytetään laajoissa toteutuksissa toimiviksi todettuja operaattoritason ratkaisuja, jotka mahdollistavat palveluiden laajentamisen tulevaisuudessa myös sairaalan ulkopuolelle. Sairaalaan toteutettava MPLS runkoverkko mahdollistaa erittäin suuren skaalautuvuuden, sekä mahdollistaa verkkopalveluiden tuottamisen optimaalisilla ratkaisuilla erilaisiin yhteystarpeisiin. MPLS tekniikalla toteutettu verkko on myös automaattisesti reitittyvä, joten tällä saadaan yhden reitityspisteen vikaantumisesta aiheutuvat vaikutukset käytännössä rajattua millisekunteihin tai pahimmillaan pieniin pakettihävikkeihin, joista päätelaitteet toipuvat.

Nopeudet kaikilla verkkoliitännöillä ovat reunakytkimien porteissa vähintään 1G ja runkoyhteyksillä vähintään 10G ja reitittimien välillä 100G.

3.3 Huollettavuus

Tietoliikenneverkko suunnitellaan siten että jokaisen yksittäisen laitteen päivitys- ja huoltotoimenpiteet voidaan suorittaa toiminnan keskeytymättä. Yksittäisen laitteen päivitys- tai huoltotoimenpiteestä aiheutuva välityskapasiteetin lasku on huomioitu sairaalan tietoliikenneverkon yhteyskapasiteettien mitoituksessa, joten edes palvelutason laskua ei tule huoltotoimenpiteiden aikana.

3.4 Tietoturvallisuus

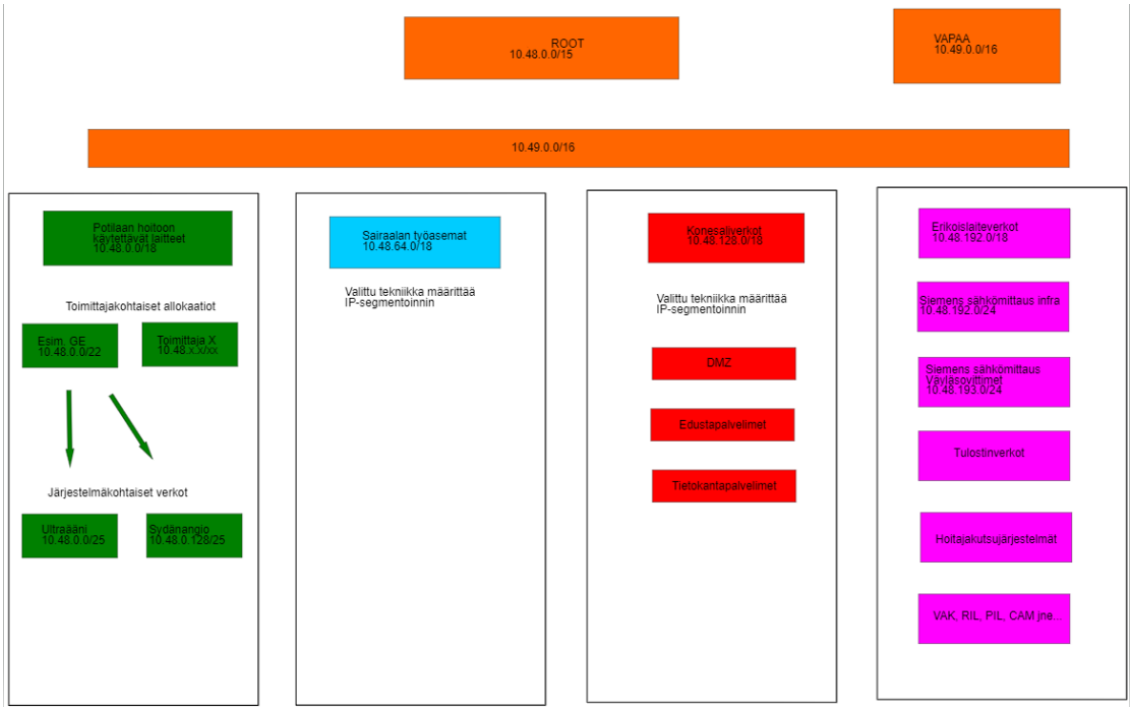
Tietoturvallisuus saavutetaan verkon kattavalla segmentoinnilla, sekä konesaliverkossa, että lähiverkossa. Verkkoon otetaan 802.1X radius pohjainen autentikointi käyttöön kaikkien kerroskytkinten portteihin, sekä langattomaan verkkoon liitettäessä. Näin laitteet tunnistetaan verkkoon liitettäessä ja voidaan luokitella esimerkiksi laitetyypeittäin. Tunnistettu laite siirretään automaattisesti oikeaan verkkosegmenttiin ja tunnistamattomia laitteita ei päästetä verkkoon ollenkaan. Verkkoon autentikoidutaan laitesertifikaatin perusteella kaikissa päätelaitteissa, jotka tätä tukevat. Muiden laitteiden osalta tunnistetaan laite MAC-osoitteen perusteella.

Langattomassa lähiverkossa ei käytetä perinteiseen yhteiseen esijaettuun avaimeen (Pre shared key) perustuvaa verkkoon autentikoimistekniikkaa.

Palomuureilla toteutetaan säännöstöt käyttäjätietoisesti ja avaukset tehdään sovellustietoisina vain tarvittaville porteille ja protokollille, käyttäen palomuuritoimittajan valmiita ja itse mallinnettuja sovellustunnisteita.

Verkon segmentoinnin periaate on havainnollistettu kuvassa 1.

Kuva 1 Verkon segmentointi



4 Verkkopalveluiden keskeiset toteutustekniikat

Verkkopalveluiden toteutustekniikat on valittu huomioiden verkolle asetetut vaatimukset. Kappaleessa käydään läpi kokonaisuuden kannalta oleellisimmat toteutustekniikat, jotka osaltaan mahdollistavat verkolle asetettujen vaatimuksien toteutumisen.

4.1 BGP MPLS-Based Ethernet VPN

Sairaalan tietoliikenneverkon useaan pisteeseen ulottuvat layer2 Ethernet palvelut toteutetaan MPLS runkoverkon Ethernet VPN tekniikalla BGP MPLS-Based Ethernet VPN

(RFC 7432). Ethernet VPN tekniikka mahdollistaa aktiivisten kahdennettujen layer2 palveluiden toteuttamisen turvallisesti ja skaalautuvasti koko sairaalan alueella, mahdollistaen nopean uudelleen reitityksen esimerkiksi laiterikko tilanteessa.

4.2 BGP MPLS Virtual Private Networks

Sairaalan tietoliikenneverkossa järjestelmäkohtainen liikenteen erottelu toteutetaan BGP MPLS Virtual Private Networks (RFC 4364) tekniikalla. Järjestelmäkohtaisen MPLS IP-VPN verkon sisällä laitteet sijoitetaan useisiin IP-aliverkkoihin, jotka voivat liikennöidä keskenään unicast ja multicast reitityksellä. Verkkojen välinen liikennöinti toteutetaan palomuurin kautta ja näin varmistetaan verkon näkyvyys ja tietoturva.

4.3 802.1X

IEEE 802.1X Port Based Authentication, eli porttikohtainen todentaminen on IEEE:n 802.1X-standardi. 802.1X:n tarkoituksena on tunnistaa verkkoon liitetyt laitteet ja ohjata radiukselle määritellyn politiikan mukaisesti laitteet oikeaa verkkoon tai vastaavasti estää verkkoon pääsy.

4.4 LACP

Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces eli suomeksi porttikanava on tekniikka, jonka johdosta on mahdollista käyttää kahta tai useampaa fyysisestä liitäntää yhtenä loogisena porttina. Tekniikka mahdollistaa sen, että kaikki liitännät saadaan tehtyä kahdella tai useammalla fyysisellä kytkennällä ja ne toimivat porttikanavana yhdessä ja näin fyysisen linkin katkeaminen yhdestä portista ei aiheuta verkon liikennöinnissä liikennöinnin näkökulmasta katkosta.

5 Valittujen toteutustekniikoiden edut

Valitut toteutustekniikat mahdollistavat kaikkien verkkopalveluiden toteuttamisen kahdennettuina MPLS runkoverkon palveluina suoraan MPLS runkolaitteista jakamokytkimille. Tällöin kaikki palvelut voivat käyttää MPLS runkoverkon yleisiä

ominaisuuksia, kuten liikennesuunnittelua, nopeaa uudelleenreititystä, kuormanjakoa, ja palvelunlaatuluokkia. Toteutuksessa on selkeitä etuja esimerkiksi perinteiseen hajautetun arkkitehtuurin kytkinratkaisuun nähden.

Layer2-palvelut voidaan tuottaa kahdennettuna MPLS-EVPN palveluna suoraan kaikkiin jakamokytkimiin. Eri virtuaalilähiverkkoja (vlan) ei tässä toteutustekniikassa tarvitse kuljettaa suoraan jakamokytkimien välillä, jolloin vika-alueet saadaan rajattua mahdollisimman pieniksi ja mahdollistetaan vikasietoisten layer2 palveluiden toteuttaminen ilman välityssilmukoiden riskiä. MPLS-EVPN käyttää kontrolloitua MAC osoitteiden oppimista BGP protokollan avulla. Ominaisuus vähentää layer2 palveluissa runkoverkon yli välitettävän BUM liikenteen eli verkon aktiivi- ja asiakaslaitteiden tuottamaa broadcast-, unicast- ja multicast-liikennettä, joka näin laajassa ympäristössä alkaisi jo kuormittamaan verkon runkolaitteita.

Layer3 palveluissa jokaisen aliverkon oletusreititin sijaitsee paikasta riippumatta lähimmässä MPLS verkon runkolaitteessa. Tämä tarkoittaa, että mikäli yhtä aliverkkoa on useammassa kerroksessa, sama oletusreititin toimii hajautetusti kaikissa runkoreitittimissä, joiden takana kyseistä aliverkkoa on käytössä.

MPLS-L3VPN palvelu mahdollistaa järjestelmäkohtaisten reititettyjen virtuaaliverkkojen toteuttamisen sairaalan verkossa. Reititettyjen virtuaaliverkkojen käyttäminen layer2 virtuaaliverkkojen sijasta mahdollistaa huomattavasti suuremman skaalautuvuuden ja käytettävyyden, sekä pienentää merkittävästi vikojen vaikutusalueita ja parantaa tietoturvaa mahdollistaen aliverkkokohtaisen segmentoinnin, sekä yksinkertaistamalla tietoturva-arkkitehtuuria.

Kaikki sairaalan tietoliikennelaitteet toimivat itsenäisesti, eikä niillä ole suoria keskinäisiä riippuvuussuhteita, jotka vaatisivat esimerkiksi saman ohjelmistoversion ajamista tai laiteparien yhtäaikaista päivittämistä. Tämä mahdollistaa tietoverkon päivittämisen laite kerrallaan siten, että päivityksen ajan palvelut toimivat varmentavien laitteiden kautta, eikä täydellistä palvelukatkoa pääse syntymään. Tämä on yksi sairaalan kannalta kaikista oleellisen arkkitehtuurin ominaisuus.

6 Valmistajien kampus arkkitehtuurimallit

Valmistajat tarjoavat valmiita kampusverkkototeutuksen arkkitehtuurimalleja. Arkkitehtuurit sinällään perustavat samanlaiseen ajatukseen, jossa core, distribution ja access tasot erillisillä laitteilla toteutettuna ja linkit kahdentaen.

Toteutuksessa valittiin eri verkon alueisiin ominaisuuksiltaan parhaaksi katsotut laitemerkit, joiden katsottiin ominaisuuksiltaan tuovan parhaat kyvykkyydet verkkoon nyt ja tulevaisuuden tarpeisiin.

Tekniikat valittiin toimittajien parhaita tekniikoita hyödyntäen ja lopputuloksessa Juniper MX-reitittimet hoitavat runko (core) ja kerrosreititystä (distribution). Juniper tekniikan valintaa näihin verkon toimintoihin perustui erityisesti MPLS BGP reititystekniikoiden kyvykkyyksiin ja käsitykseen laitteiden vahvuuksiin reitityksen tuottamisesta juuri kriittisen runko palveluiden reitityksen tuottamisessa.

Cisco Catalyst 9300 48-port PoE+, kytkinmalli valittiin langallisen lähiverkon access kytkimeksi. Langaton verkko on toteutettu Cisco Catalyst 9800–40 langattoman verkon kontrollerilla ja Cisco Aironet 4800 tukiasemilla. Radius palvelu tuotetaan Ciscon Identity Services Enginellä.

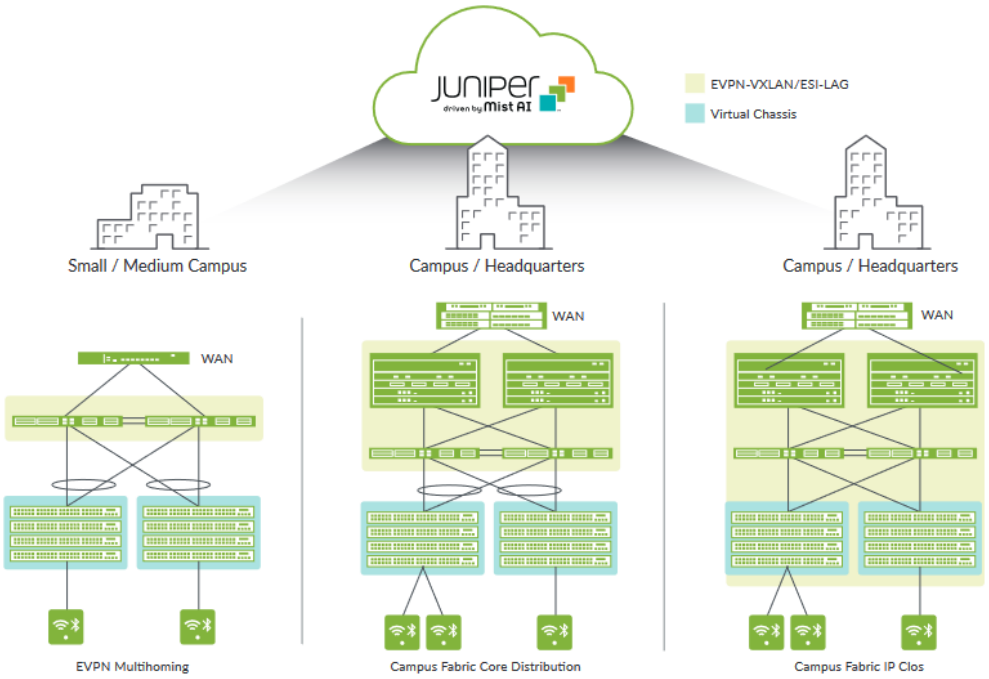
Cisco valittiin access kerroskytkinten ja wlan-verkon laitevalmistajaksi muun muassa seuraavin perustein.

- Pystyy toimittamaan langallisen ja langattoman lähiverkon ratkaisut
- Iso tukiorganisaatio myös Suomessa
- Huomattava määrä referenssejä sairaalaympäristöistä
- Lähiverkon kytkimien fyysinen koko ja hiljaisuus
- Mahdollisuus ottaa käyttöön tietoturvaa, näkyvyyttä ja hallintaa parantavia ohjelmistoja (mm. Stealthwatch, DNA Assurance, DNA Center)
- Tuki tulevaisuuden SDN tekniikoille, SD-Access kyvykkyyksiltään BGP-reititysprotokollaa käytettäessä.

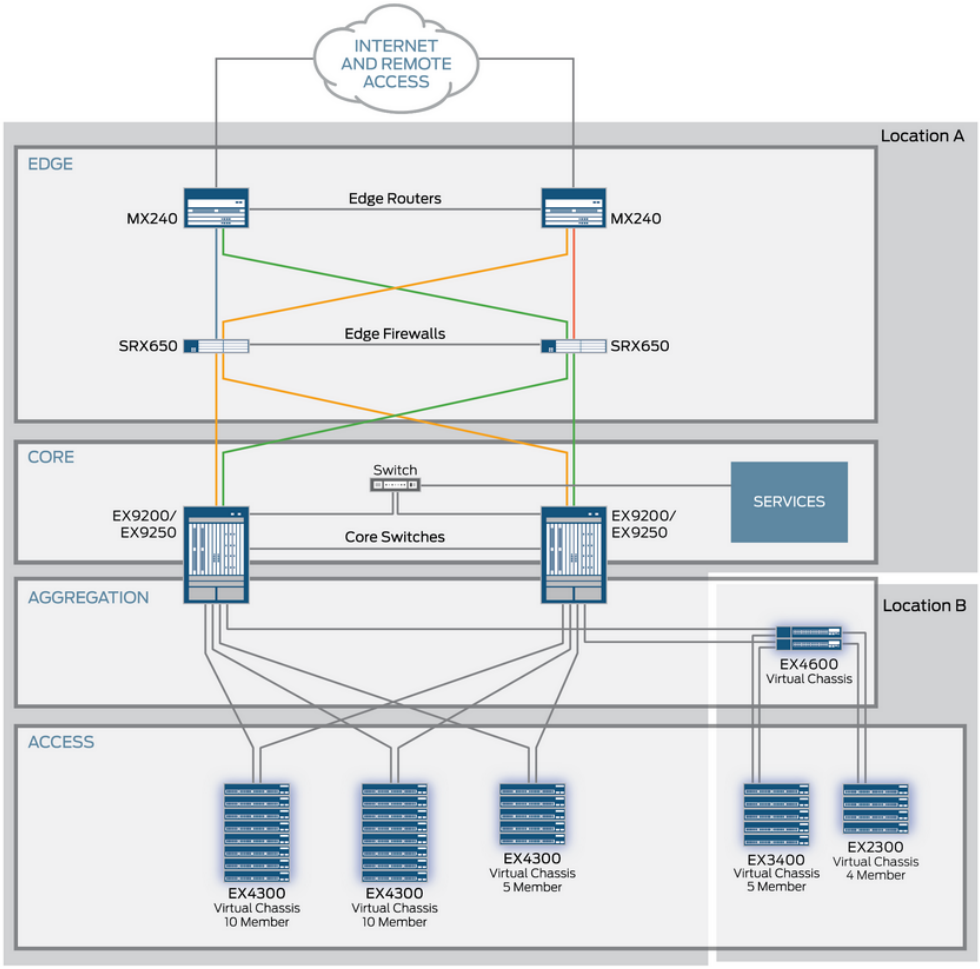
Itse topologia on kuitenkin toteutettu eri valmistajien topologia mallien periaatteilla, jotka on esitetty kuvissa 2 ja 3 Juniper Networksin toteutuksella ja kuvassa 4 Cisco Systemsin core, distribution ja access tasoihin hajautettu kampusarkkitehtuuri.

Ciscon kampus topologia on vastaava kuin Juniperilla, mutta core taso perustuu Ciscon Catalyst kytkimiin.

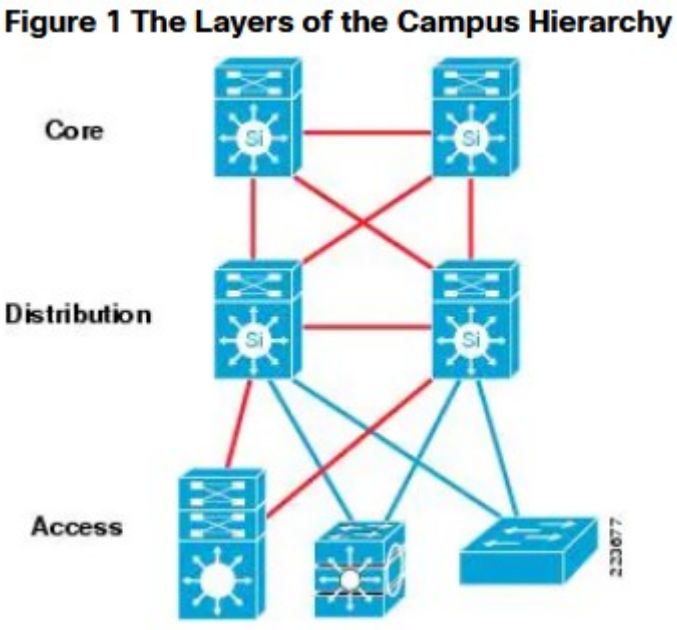
Kuva 2 Juniper kampus arkkitehtuurin malli (Juniper Networks, Inc, 2021)



Kuva 3 Juniper verkkotopologia malli (Juniper Networks, Inc, 2021)



Kuva 4 Cisco Kampus hierarkian arkkitehtuuri malli (Cisco Systems, Inc 2008)

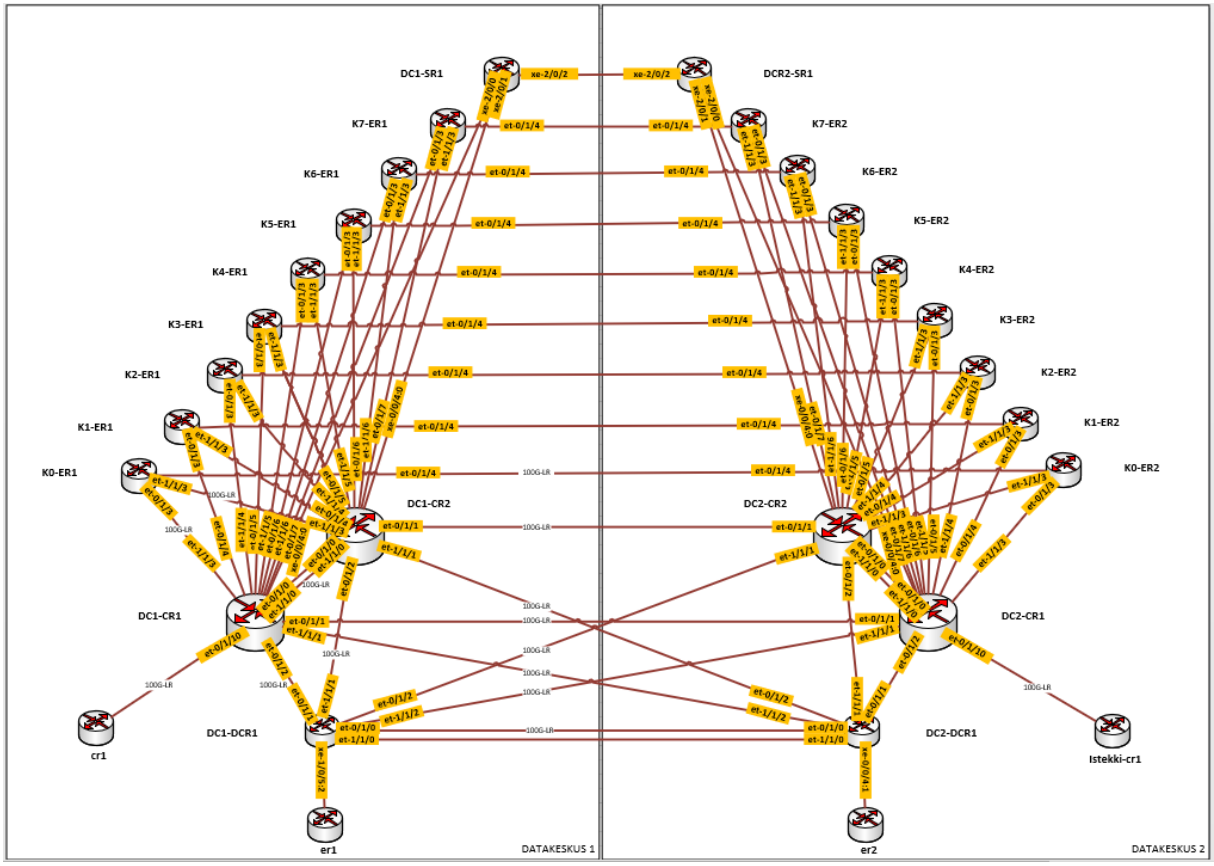


7 Verkkopalveluiden liitynnät kampuksella

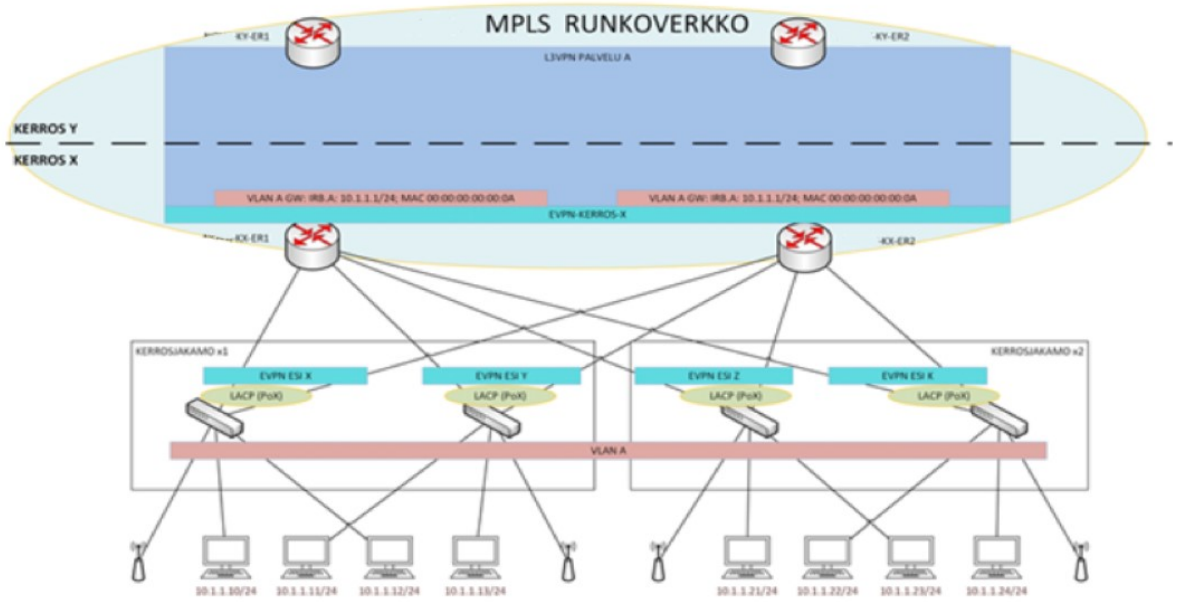
Kerroksessa käytetään kerroskohtaisia Ethernet vpn-instansseja, joista allokoidaan verkkopalvelun päätelaitteille kerroskohtaiset virtuaaliverkot. Yhdelle verkkopalvelulle allokoitu kerroskohtainen vlan on sama jokaisessa kerroksessa, mutta kerroksia ei oletusarvoisesti yhdistetä L2-tasolla toisiinsa. Kerroskohtaisille virtuaaliverkoille allokoidaan yksilölliset ip-aliverkot, joiden aktiivisina kahdennettuina oletusreitittiminä toimivat kerroskohtaiset MPLS runkolaitteet. Oletusreitittimien aktiivinen kahdennus toteutetaan MPLS EVPN tekniikalla.

Kunkin verkkopalvelun IP-aliverkot yhdistetään palvelukohtaiseksi virtuaaliverkoksi MPLS-L3VPN tekniikalla. Tällöin jokaiselle verkkopalvelulle muodostuu sairaalan verkon sisälle täysin erillinen reititetty virtuaaliverkko. Kampuksen verkkopalveluiden liitynnän periaate on esitetty kuvissa 5 Kampuksen verkkopalveluiden liitynnät kampuksen runko- ja kerrosreitittimillä ja 6 Kampuksen verkkopalveluiden liitynnän periaate.

Kuva 5 Kampuksen verkkopalveluiden liitynnät kampuksen runko- ja kerrosreitittimillä



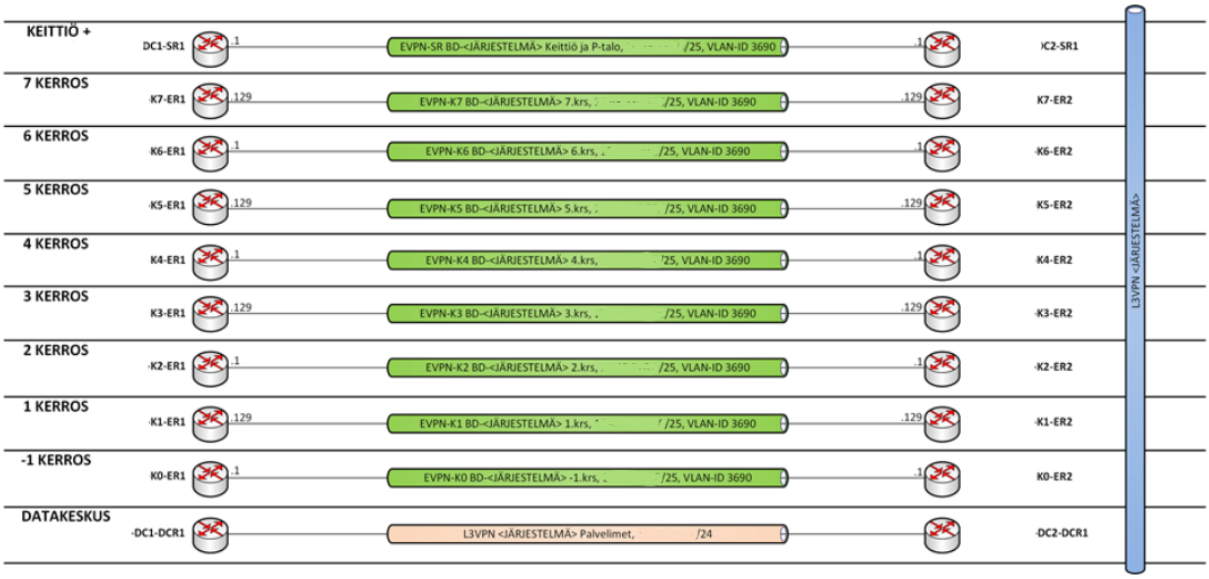
Kuva 6 Kampuksen verkkopalveluiden liitynnän periaate



7.1 Verkkopalveluiden yhteistoiminta

MPLS-EVPN tekniikalla rakennetaan kerrosten sisäiset L2-yhteydet, sekä mahdollistetaan oletusreitittimien aktiivinen kahdennus. MPLS-L3VPN tekniikalla muodostetaan järjestelmäkohtainen virtuaaliverkko sijoittamalla järjestelmän aliverkot erilliseen reititystauluun ja mahdollistamalla reititetyt yhteydet virtuaaliverkkojen välillä. Verkkopalveluiden yhteistoiminnan periaate on esitetty kuvassa 7 Verkkopalveluiden yhteistoiminnan periaate.

Kuva 7 Verkkopalveluiden yhteistoiminnan periaate



7.2 Runkoyhteyksien kapasiteetti, suorituskyky ja varmennukset

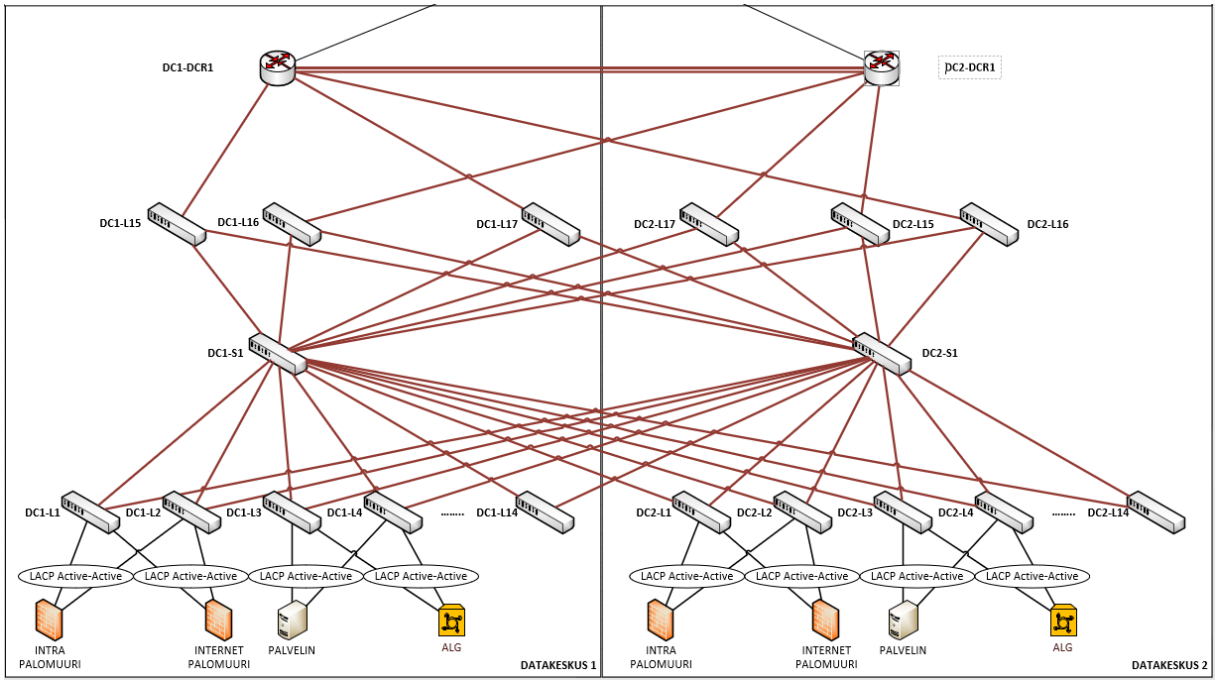
Runkoverkon fyysinen topologia ja laitteiden väliset kuitureitit on suunniteltu siten, ettei yksittäisen laitteen tai yhteyden vikaantuminen aiheuta katkosta sairaalan toimintaan. Runkoyhteyksien määrä ja kapasiteetti on mitoitettu huomioiden mahdollisista vikatilanteista aiheutuva lisäkuormitus, sekä lähitulevaisuudessa tapahtuva liikennemäärien kasvu. Verkossa ei siis näin ollen ole yhtään yksittäistä pistettä, joka vikaantuessaan aiheuttaisi verkon toiminnan kannalta merkittävää heikentymistä.

8 Verkon fyysinen topologia

Datakeskuksiin sijoittavat laitteet, kuten palvelimet, palomuurit, ja kuormantasauslaitteet liitetään vähintään kahdella fyysisellä yhteydellä kahteen konesalin kytkimeen. Yhteyksistä muodostetaan loogisesti yksi aktiivinen yhteys LACP protokollaa käyttäen.

Toisiaan varmentavat laitteet hajautetaan fyysisesti kumpaankin datakeskukseen, jolloin yhden datakeskuksen vikaantuminen ei aiheuta palvelukatkoa. Verkon datakeskusten fyysiset kytkennät on tehty kuvan 8 havainnollistamalla mallilla.

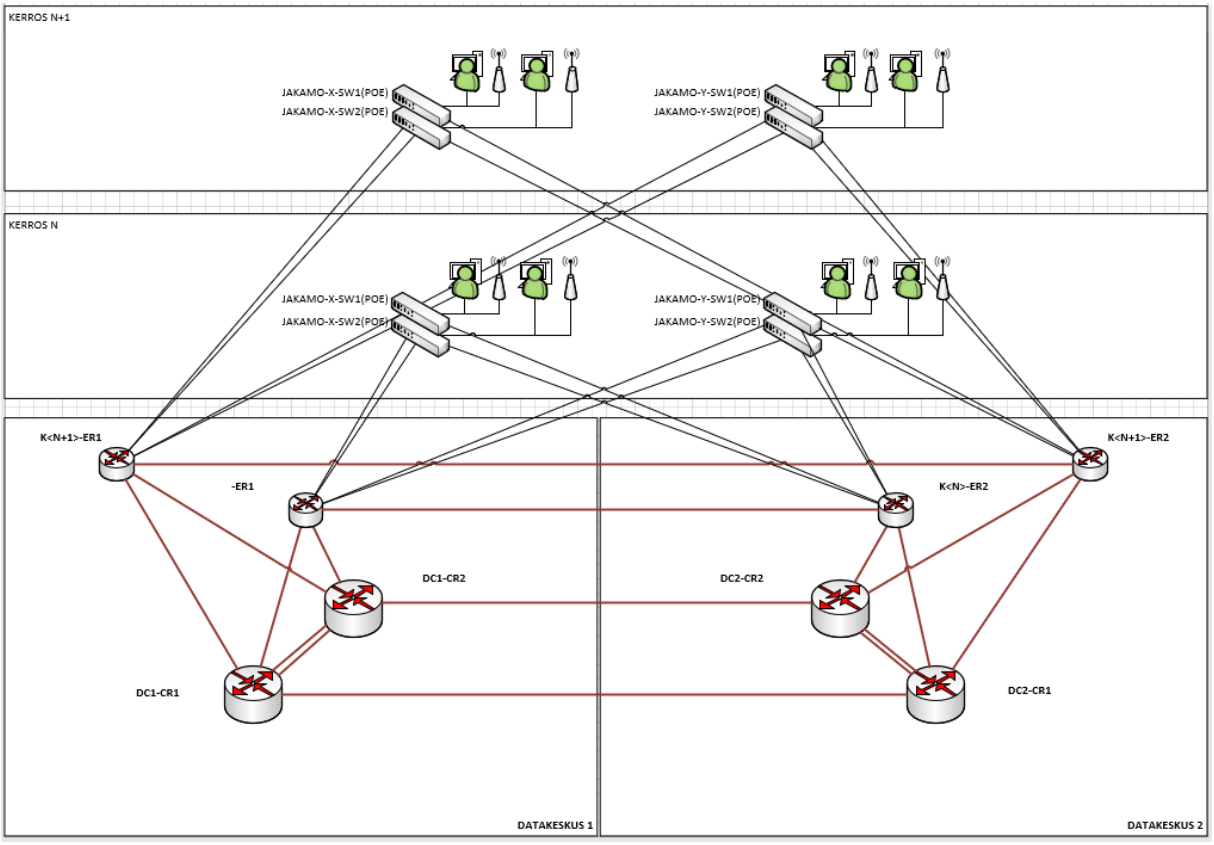
Kuva 8 Verkon fyysiset kytkennät



Jokaisen yksittäisen osaston päätelaitteet, langattoman verkon tukiasemat, sekä talotekniikka hajautetaan vähintään kahteen erilliseen jakamokytkimeen, jotta yksittäisen kytkimen vikaantuminen ei aiheuta täydellistä katkosta osaston tietoliikenneyhteyksien toimintaan.

Jokainen yhteys on kytketty vähintään kahdella kuitudulla ja näiden reitit ovat fyysisesti erillään toisistaan kuvan 9 mukaisesti.

Kuva 9 Kampusverkon fyysinen topologia



Runkoverkon ja kerrosreitittimien kuitukytkennät on toteutettu 100G liitännöillä. Kerrosjakamokytkimet ovat liitettynä kahdella erillisellä 10G kuituyhteydellä kerroskohtaisiin runkolaitteisiin, joista on muodostettu yksi looginen yhteys LACP protokollaa käyttäen näin kerrosreitittimien ja kerroskytkimien välinen kapasiteetti on 20GB/s. Kerroskytkimien porttien nopeus on 1GB/s ja ne syöttävät Poe+ virtaa kaikista porteistaan. Kerroskytkimeen on mahdollista ottaa myös kuituliitäntöjä aina 100GB/s nopeuteen asti lisämoduulilla.

8.1 Runkoverkko

Runkoverkko ja kerrosreititys on toteutettu Juniper MX10003 reitittimillä, jonka etupaneelin näkymä on kuvassa 10. Jokaista sairaalan kerrosta kohden on kaksi erillistä MPLS runkolaitetta. Jokainen kerrosjakamokytkin liitetään kahdella erillisellä 10G kuituyhteydellä kerroskohtaisiin runkolaitteisiin. Jokainen aktiivilaite on varustettu vähintään kahdella virtalähde moduulilla, jotka voidaan vaihtaa ilman laitteen sammutus tarvetta.

Kerrosjakamokytkimessä runkolaitteisiin menevistä yhteyksistä muodostetaan loogisesti yksi aktiivinen 20G yhteys LACP protokollaa käyttäen. Runkolaitteissa hajautettu looginen yhteys kerrosjakamokytkimen suuntaan muodostetaan MPLS-EVPN aktiivisen kahdennustekniikan ja LACP protokollan avulla.

Kerrosreitittimet ja datakeskusreitittimet on kytketty toisiinsa 100G liitännöillä suorituskyvyn ja kapasiteetin riittävyyden varmistamiseksi myös tulevaisuudessa.

Runkoverkon fyysinen topologia ja laitteiden väliset kuitureitit on suunniteltu siten, ettei yksittäisen laitteen tai yhteyden vikaantuminen aiheuta katkosta sairaalan toimintaan. Runkoyhteyksien määrä ja kapasiteetti on mitoitettu huomioiden mahdollisista vikatilanteista aiheutuva lisäkuormitus sekä lähitulevaisuudessa tapahtuva liikennemäärien kasvu.

Kuva 10 Juniper Networks MX10003

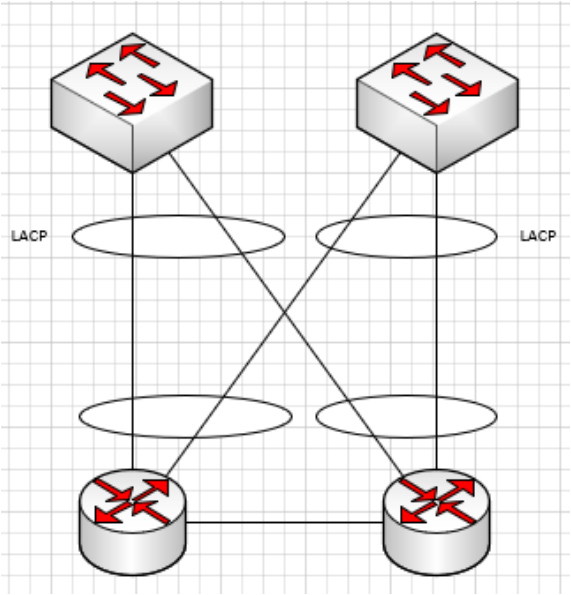
8.2 Langallinen lähiverkko

Langallinen lähiverkko on toteutettu Cisco Catalyst 9300 48-porttisilla Poe+ mallilla. Kytkimessä on 48 kappaletta Poe+ virransyöttöön kykeneviä 1GB kupariportteja, sekä modulaarinen 8 paikkainen optinen uplink-kortti. Kytkimet on varustettu kahdella virtalähteellä. Kytkimen ulkoasu on esitetty kuvassa 11.

Kuva 11 Cisco Catalyst 9300 PoE

Jokainen kytkin on kytketty kahteen eri kerrosreitittimeen kahdella erillisellä kuitukytkennällä 10G liitännöillä. Näitä kahta liitäntä ajetaan LACP porttikanavana ja kapasiteetiksi saadaan näin 20Gbit/s kerrosreitittimen ja reunakytkimen välillä. Kytkennän periaate esitetty kuvassa 12.

Kuva 12 Kerroskytkimen liitäntä kerrosreitittimiin



Kerroksessa olevat päätelaitteet sekä WLAN-tukiasemat hajautetaan aina vähintään kahteen kerrosjakamokytkimiin siten, että yhden kerrosjakamokytkimen vikaantuminen tai huoltotyö ei aiheuta laajaa häiriötä alueen palveluiden toimintaan. Päätelaitteet on kytketty CAT6-verkkokaapelilla.

8.3 Langaton lähiverkko

Langaton lähiverkko toteutettiin Cisco WLC 9800-K40 kontrollerilla ja Cisco Aironet 4800 tukiasemilla. Ympäristö koostuu neljästä fyysisestä laitteesta. Verkon primääri kontrolleri on kahdennettu HA-pari ja lisäksi on yksi kolmas kontrolleri, jolle WLAN-hallinta voidaan siirtää primäärin klusterin vikaantuessa. Neljännellä kontrolleri laitteella tehdään ohjelmistojen ja asetusten testaukset, jotta estetään uusien ohjelmistoversioiden ennakoimattomat vaikutukset sairaalan tuotanto langattomaan-verkkoon.

Langattoman verkon salaus toteutetaan WPA2-Enterprise tekniikalla käyttäen AES salausta ja EAP-TLS tunnistusprotokollaa. Langattoman verkon käyttäjien liikenne voidaan valikoiden joko tunneloida kontrollerin kautta tai siirtää tukiasemasta suoraan paikalliseen langalliseen lähiverkkoon. Langattomissa verkoissa pyritään käyttämään sairaalan omille päätelaitteille mahdollisimman pientä määrää eri SSID:tä ja sijoittamaan laitteet oikeaan virtuaaliverkkoon langallista verkkoa vastaavalla toteutustavalla. Vierailijoiden laitteille langattomaan verkkoon on toteutettu erillinen SSID, jonka liikenne ohjataan suoraan Internetiin.

Verkossa olisi ideaalista käyttää vain 5 GHz taajuusalueita, mutta päätelaitteiden 5 GHz tuen puutteiden takia on 2,4 GHz taajuudet jouduttu ottamaan käyttöön. SSID:t ja niiden käyttämät taajuudet on esitetty kuvassa 13.

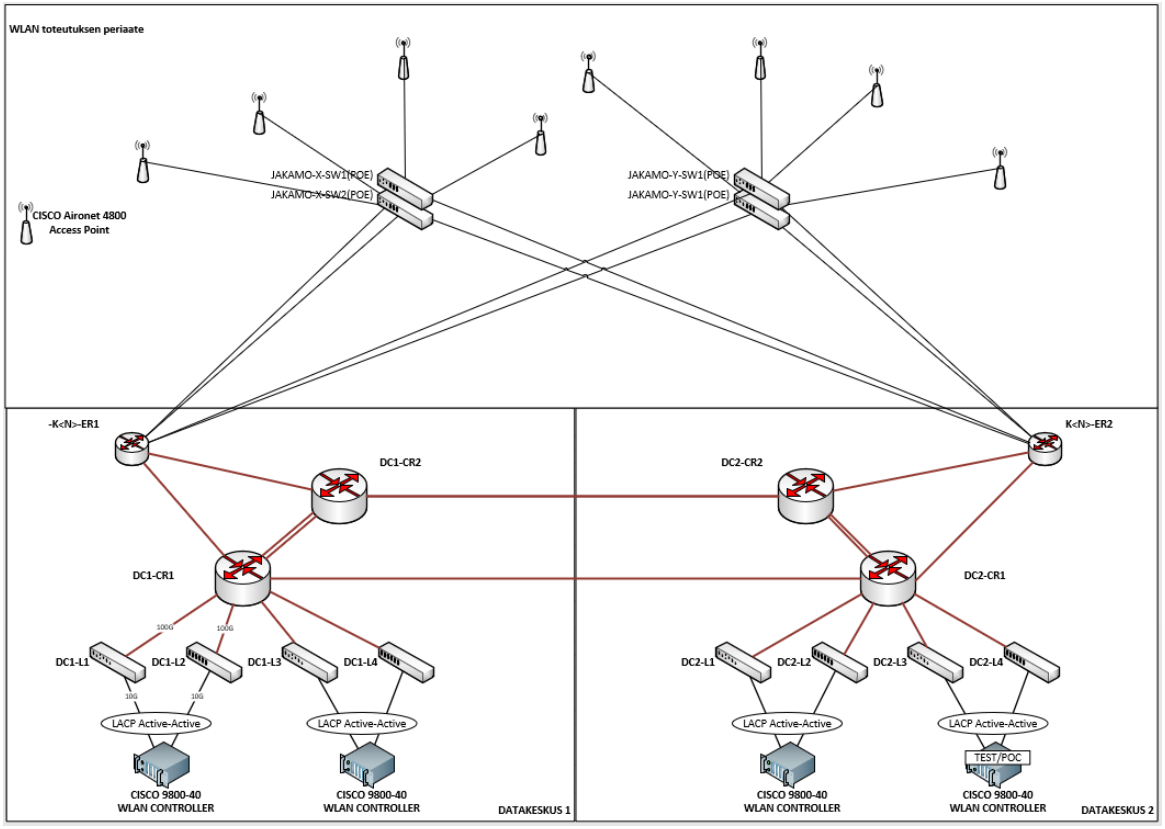
Kuva 13 Wlan SSID ja taajuudet

SSID	Autentication	Encryption	Radio Band
wlan	802.1X EAP-TLS & EAP-PEAP	AES	5G
wlan1	WPA/WPA2-iPSK	AES	2.4G + 5G
wlan2	WPA/WPA2-iPSK	AES	2.4G + 5G
open	Open	AES	2.4G + 5G

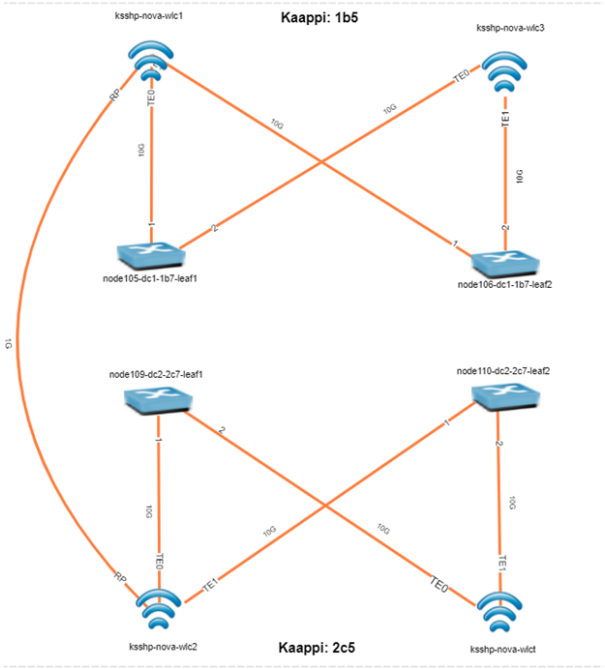
Sairaalan omat työasemat tunnistautuvat SSID ”wlan” langattomaan verkkoon automaattisesti laitesertifikaatin perustella ja ne ohjataan tunnistamisen perusteella oikeaan aliverkkoon. Työasemat saavat IPv4 osoitteet automaattisesti DHCP protokollan avulla, IPv6 osoitteita eivät ole käytössä. Jokaisen aliverkon sisällä tapahtuva työasemien välinen liikennöinti on oletusarvoisesti estetty ja jokainen aliverkko on eriytetty omaksi

reititysalueekseen, joten kaikki aliverkon ulkopuolelle tapahtuva liikennöinti kulkee Intra-palomuurin läpi. Wlan toteutuksen on kuvattu kuvissa 14 WLAN toteutuksen periaate, WLC kytkennät kuvassa 15 ja työasemat langattomassa verkossa kuvassa 16.

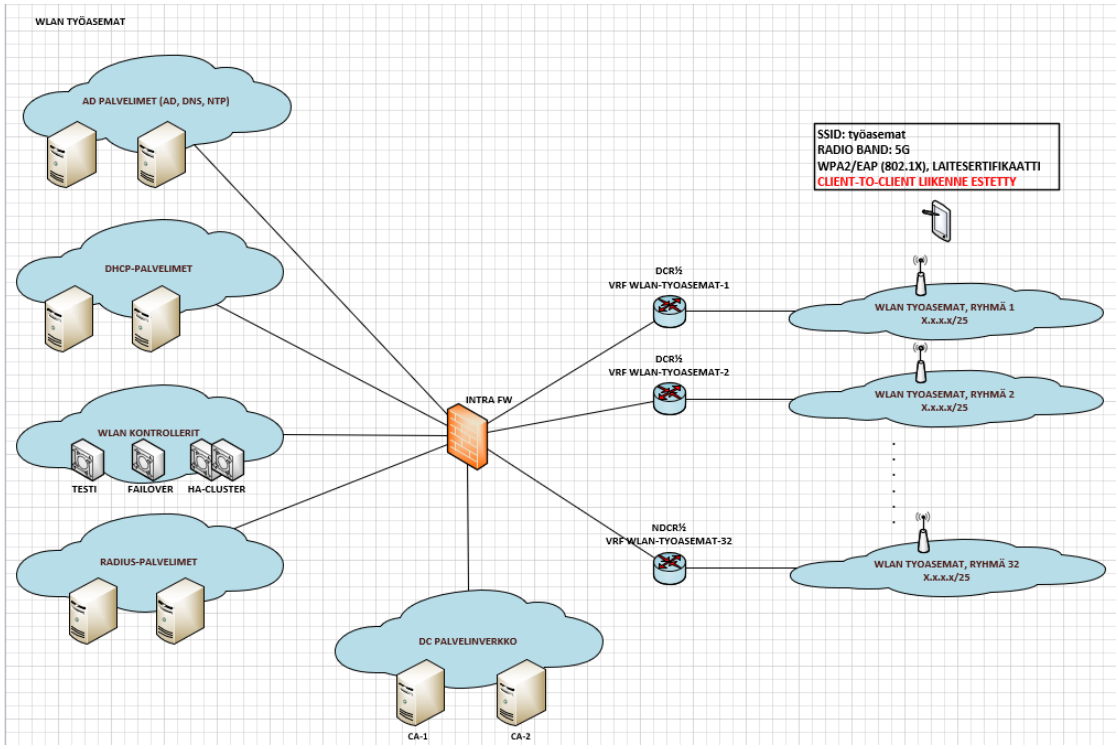
Kuva 14 WLAN toteutuksen periaate



Kuva 15 WLC kytkennät



Kuva 16 Wlan työasemat



8.3.1 Langattoman verkon päivitys

Ciscon 9800 kontrollerissa on kyvykkyys Software Maintenance Updates (SMU) päivitykseen ja tukiasemille rolling AP update toiminto ja näin ollen koko wlan-verkko voidaan päivittää, ilman katkoa wlan-verkkoa käyttävien päätelaitteiden verkkoyhteydessä.

Kontrollerin päivitys on havainnollistettu kuvassa 17 Cisco WLC Software Maintenance Updates. Päivitys tehdään ensin HA-parin passiiviselle standby laitteelle, jonka jälkeen tapahtuu tukiasemien ja yhteyksien siirto päivitetylle laitteella, josta tulee näin olleen aktiivinen laite. Tämän jälkeen päivitys tehdään alussa aktiivisena olleelle laiteparin laitteelle.

Kuva 17 Cisco WLC Software Maintenance Updates

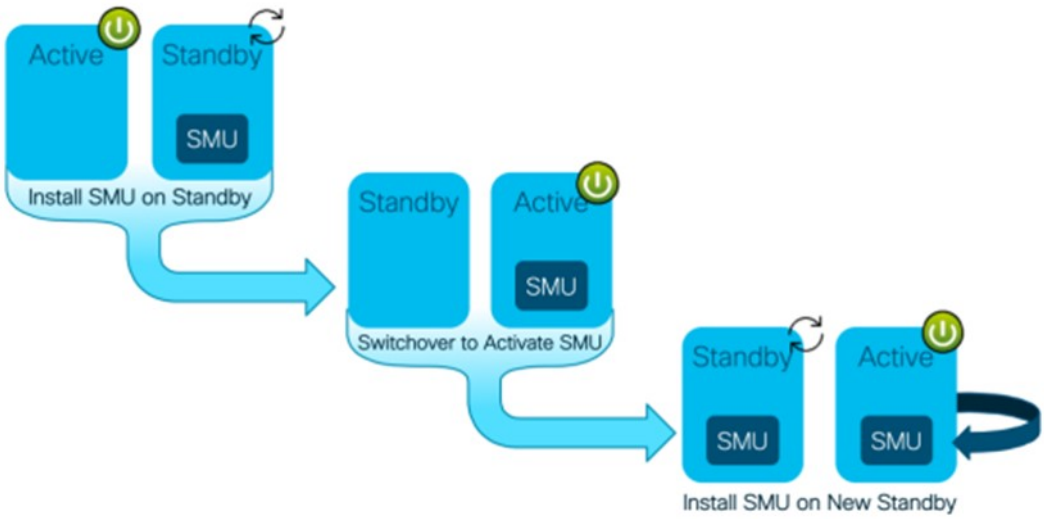
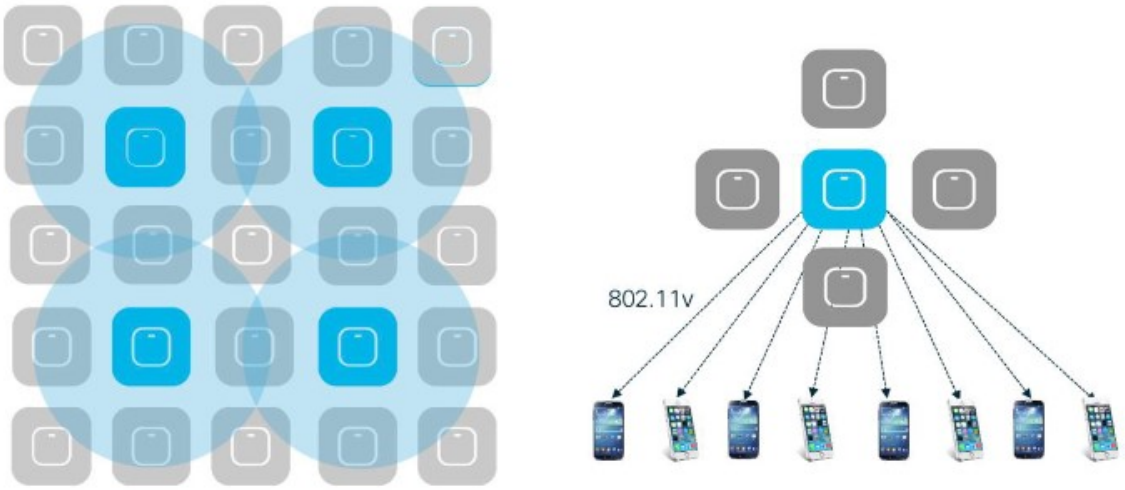


Figure 1 Active Standby Cold Patch Activation

Tukiasemien päivittämiseksi Ciscon 9800 kontrolleri tukee Rolling AP Upgrade toimintoa, joka mahdollistaa kaikkien tukiasemien päivittämisen ympäristössä ilman verkkoa käyttävien päätelaitteiden verkkokatkoa. Ideana päivitystavassa on se, että langattoman verkon kontrolleri tuntee tukiasemien naapuruus suhteet ja voi näin ollen siirtää tukiasemassa kiinni olevat päätelaitteet toiselle kuuluvuuden piirissä olevalle tukiasemalle käyttäen 802.11v protokollaa ja suorittaa sitten tyhjennetyn tukiaseman ohjelmistopäivityksen. Jos päätelaite ei tue kyseistä protokollaa, niin kontrolleri pakottaa laitteen uudelleen autentikoitumaan verkkoon, jolloin päätelaite poistuu hetkeksi verkon piiristä. Päätelaitteen kannalta

tapahtumassa oli kyseessä roaming tilanne tukiasemasta toiseen. Rolling update päätelaitteiden siirto toiselle kuuluvalle tukiasemalle havainnollistettu kuvassa 18.

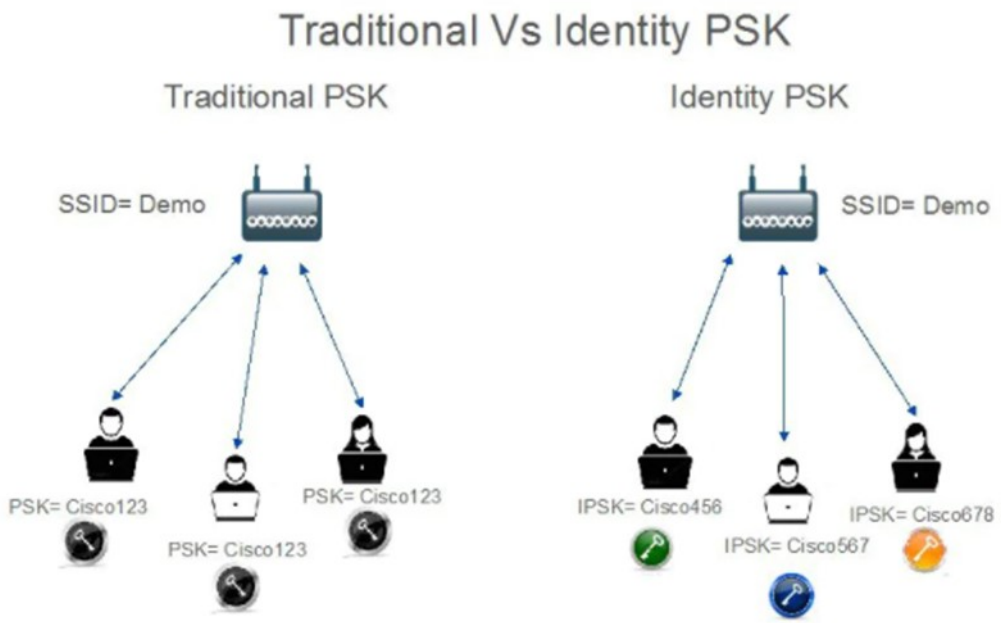
Kuva 18 Cisco Rolling AP upgrade (Cisco Systems, Inc, 2020)



8.3.2 Cisco Identity PSK

Cisco Identity PSK (iPSK) autentikointi ratkaisu mahdollistaa sertifikaatti pohjaista autentikointia tukemattomien laitteiden turvallisen autentikoinnin verkkoon. Identity PSK:t ovat uniikkeja avaimia joko yksittäisille laitteille tai laiteryhmille ja revokointi yksittäiselle laitteelle tai laiteryhmälle tapahtuu PSK radius palvelimelta. iPSK:n ja perinteisen PSK:n ero havainnollistettu kuvassa 19.

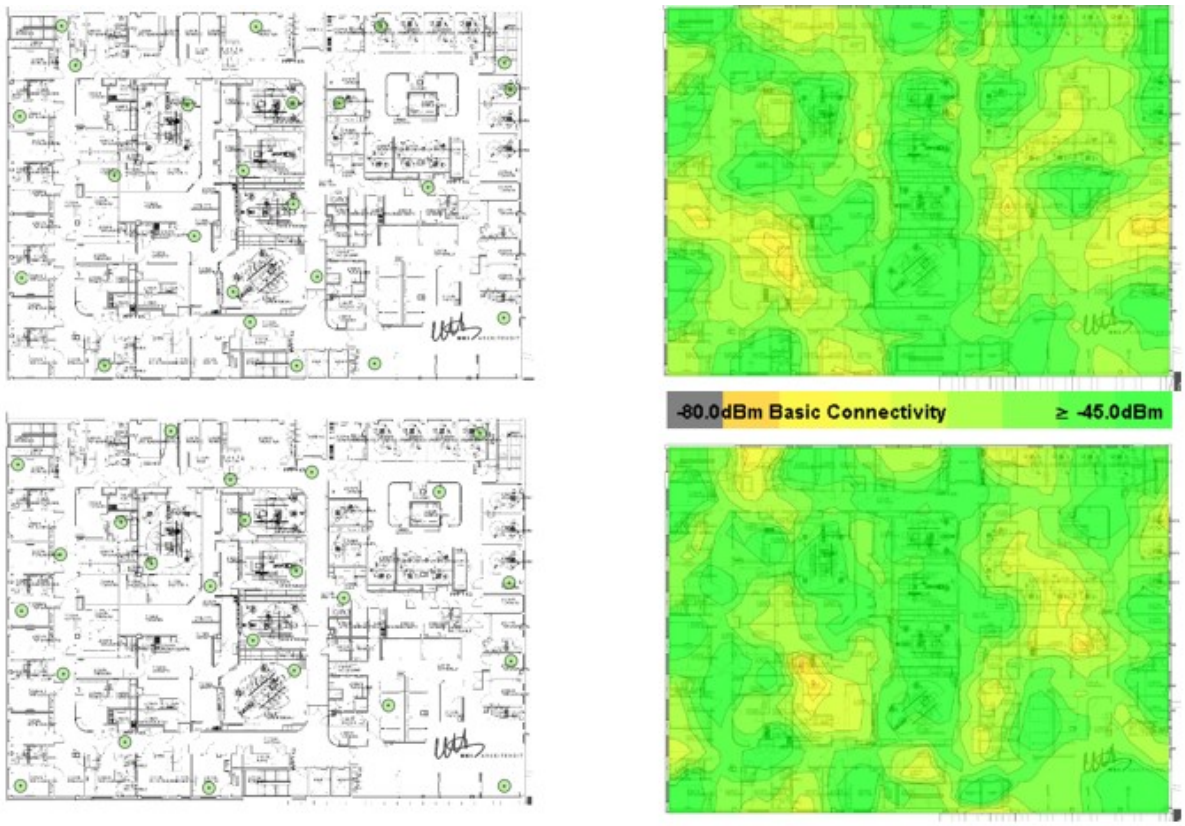
Kuva 19 Perinteinen ja identity PSK (Cisco Systems, Inc, 2017)



8.3.3 Redundanttinen wlan-verkko

WLAN-verkon peitto on suunniteltu redundanttiseksi eli kuuluvuuden alueella päätelaite kuulee aina vähintään kahden tukiaseman verkon mainostuksen. Näin ollen missään sairaalan alueella ei yhden tukiaseman hajoaminen aiheuta wlan verkon merkittävää heikkenemistä loppukäyttäjän kannalta. Kuva 20 Signaalin voimakkuudet, havainnollistaa tätä tilannetta kuuluvuus voimakkuuden karttoina.

Kuva 20 Signaalin voimakkuudet, kun vain puolet tukiasemista on käytössä



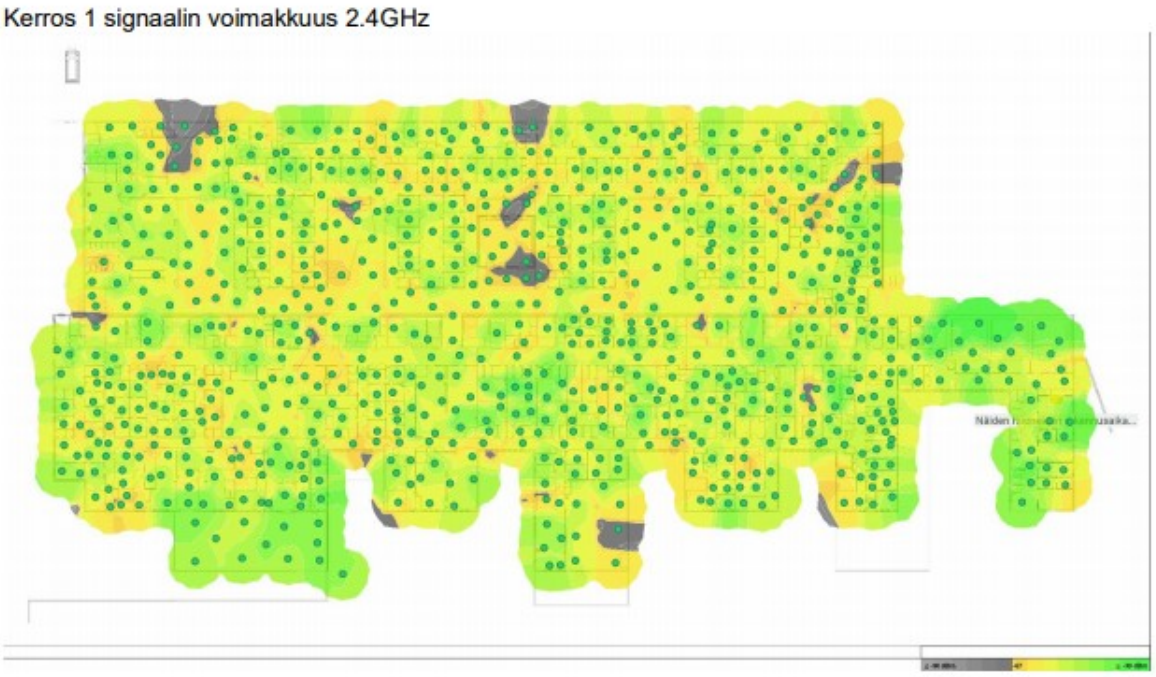
Tukiasemien sijoittelu on suunniteltu käyttäen tähän tarkoitukseen suunniteltua Ekahau sovellusta. Sijoittelu on esitetty kuvassa 18 WLAN-verkon suunnitelma. Tukiasemien sijoittelu esitetty kuvassa 21.

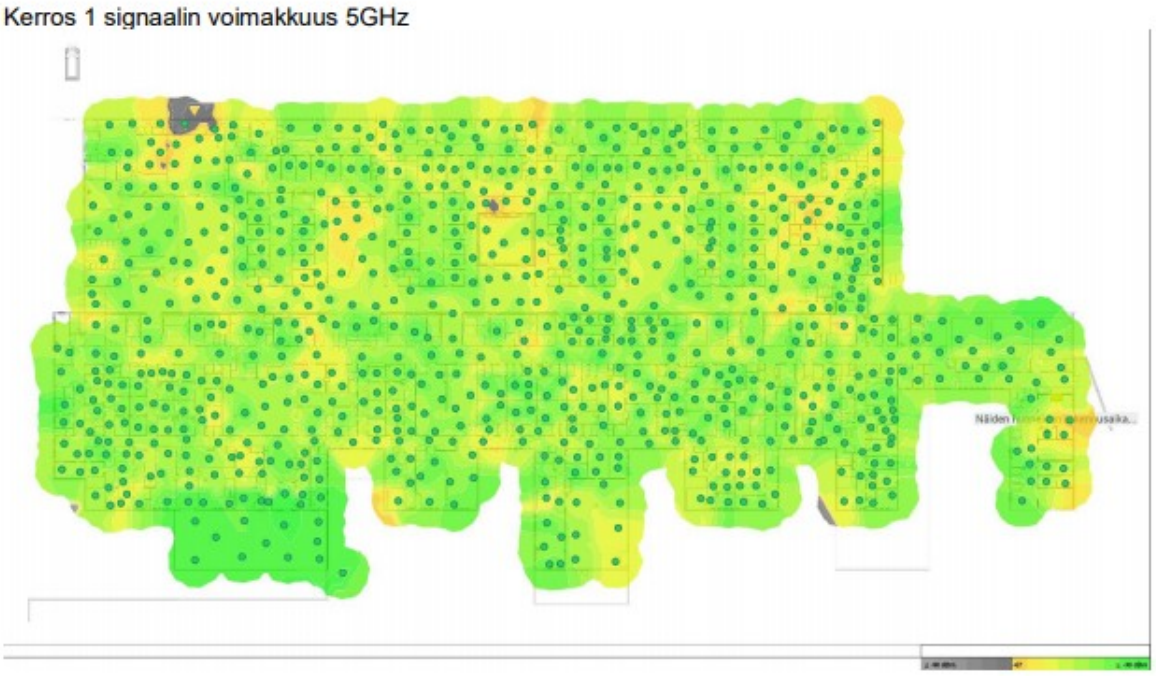
Tukiasemat saavat virransyöttönsä Cisco Catalyst 9300 kytkinten Power over ethernet (PoE) virransyötöstä, joten erillisiä injektoreita tai sähköpisteitä ei tarvittu pisteisiin.

Kuva 21 WLAN-verkon suunnitelma

Tukiasemien asennuksien ja käyttöönoton jälkeen verkko käytiin tarkistusmittaamassa 2,4 GHz ja 5 GHz taajuusalueilta, jotta voitiin olla varmoja, ettei esimeriksi suunnitteluun ilmoitetut seinärakenteet ja vahvuudet olisi muuttuneet rakennuksen aikana. Myös muut laitteet saattavat aiheuttaa kuuluvuuteen heikentymistä, jota ei ilman mittausta voida ottaa huomioon. Tarkistusmittaukset tulokset esitetty kuvassa 22.

Kuva 22 WLAN-verkon tarkistusmittaus





9 Verkon looginen topologia

Sairaalassa on kaksi toisiaan varmentavaa, aktiivista datakeskusta. Kummassakin datakeskuksessa on erillinen MPLS verkon runkolaite, josta on kahdennetut yhteydet sekä sairaalan MPLS runkoverkkoon, että datakeskusten yhteiseen sisäiseen runkoverkkoon.

Datakeskusten sisäinen runkoverkko on fyysisesti spine-leaf topologia, ja kaikki laitteiden väliset loogiset yhteydet on rakennettu reititettyinä.

Datakeskuksen palvelimien väliset yhteydet rakennetaan VXLAN kehystettyinä yhteyksinä leaf-kytkinten välille. VXLAN kehystys mahdollistaa datakeskuksen virtuaaliverkkojen pitämisen toisistaan erillään sekä leaf-kytkimissä toteutettujen palvelukohtaisten reititystaulujen yhdistämisen siten että datakeskusten sisälle voidaan muodostaa palvelukohtaisia virtuaaliverkkoja.

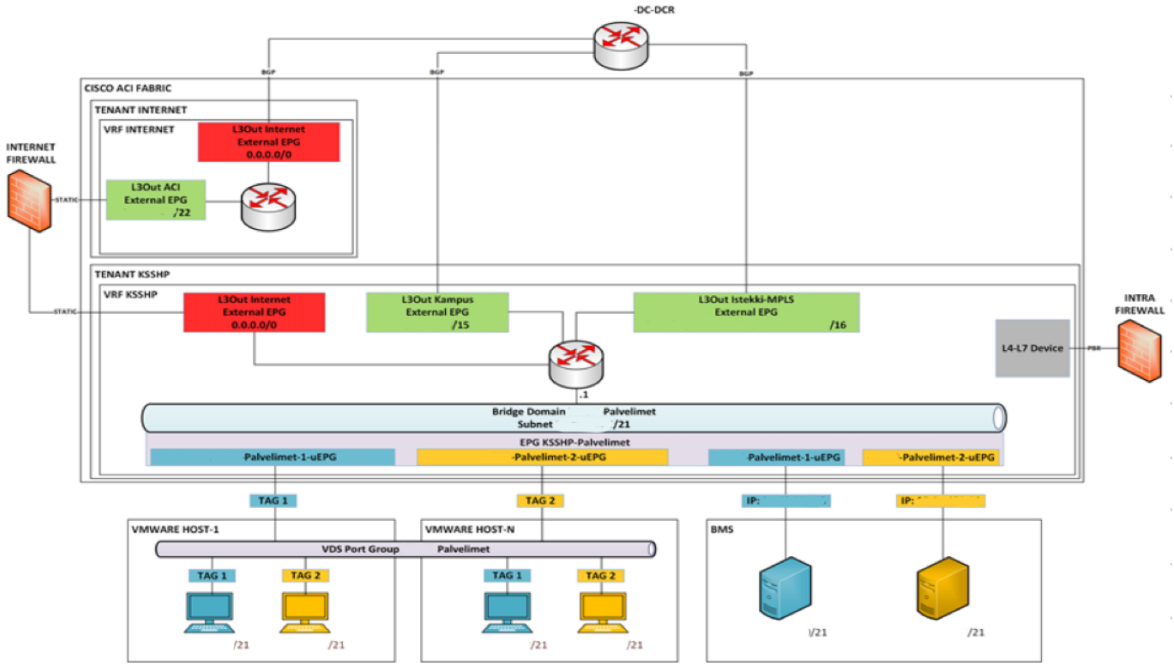
Datakeskusten sisällä palvelinten välinen liikennöinti voidaan estää tai sallia sovelluskohtaisesti palvelimen loogisesta sijainnista riippumatta. Datakeskusten sisällä liikennettä voidaan ohjata poikkeussäännöillä siten että vältetään liikenteen tarpeeton välitys esimerkiksi kahden peräkkäisen palomuuriklusterin läpi.

Datakeskusten ja kampuksen virtuaaliverkkojen keskinäinen liikennöinti voidaan sallia joko suoraan tai datakeskuksessa sijaitsevien palomuurien kautta.

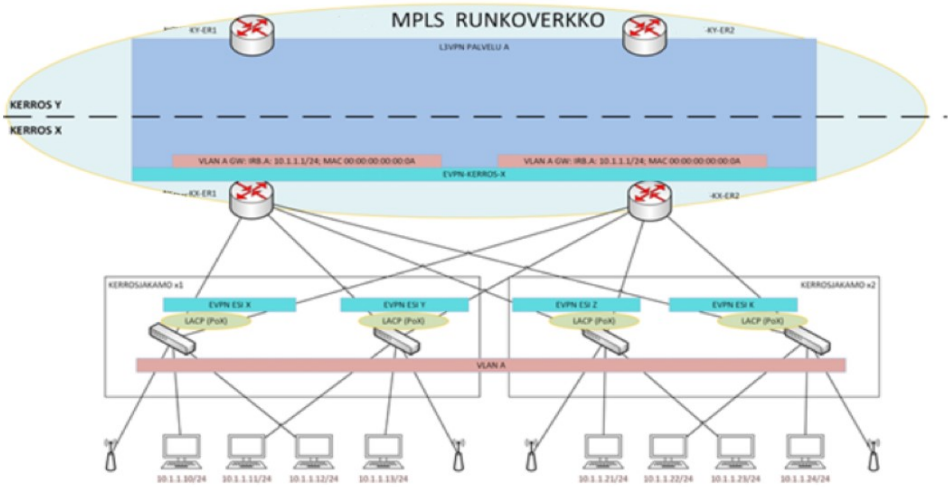
Verkon looginen topologia perustuu järjestelmäkohtaiseen liikenteen erotteluun, joka on toteutettu BGP MPLS Virtual Private Networks tekniikkaan. Järjestelmäkohtaisen MPLS IP-VPN verkon sisällä laitteet sijoitetaan useisiin IP-aliverkkoihin, jotka voivat liikennöidä keskenään unicast ja multicast reitityksellä. Verkkojen välinen liikennöinti toteutetaan palomuurin kautta ja näin varmistetaan verkon joustavuus ja tietoturva.

Verkon looginen topologia on kuvattu kuvissa 23 Verkon looginen topologia, 24 Kampusverkon looginen topologia ja 25 Runkoverkon looginen topologia ja IP-osoitteet.

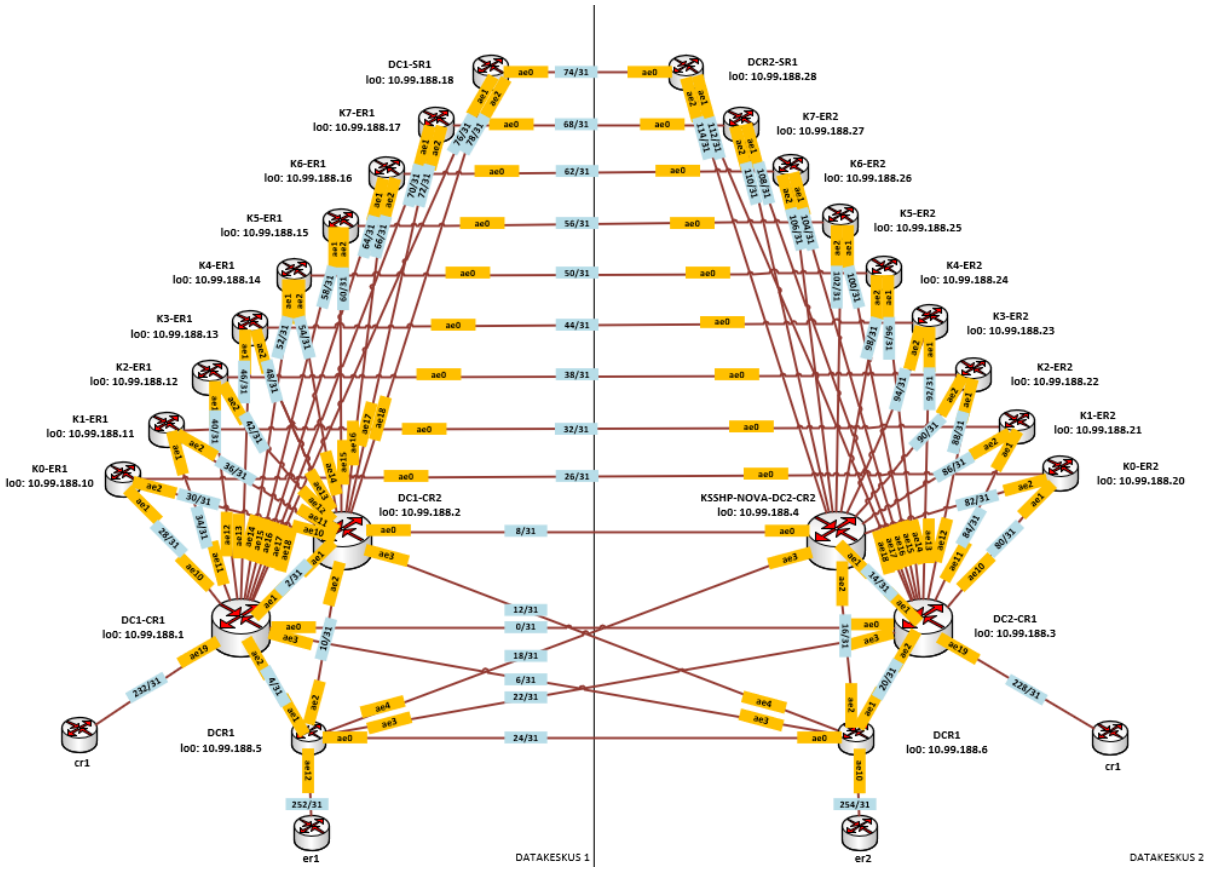
Kuva 23 Verkon looginen topologia



Kuva 24 Kampusverkon looginen topologia



Kuva 25 Runkoverkon looginen topologia ja IP-osoitteet



9.1 Verkon reititys ja segmentointi

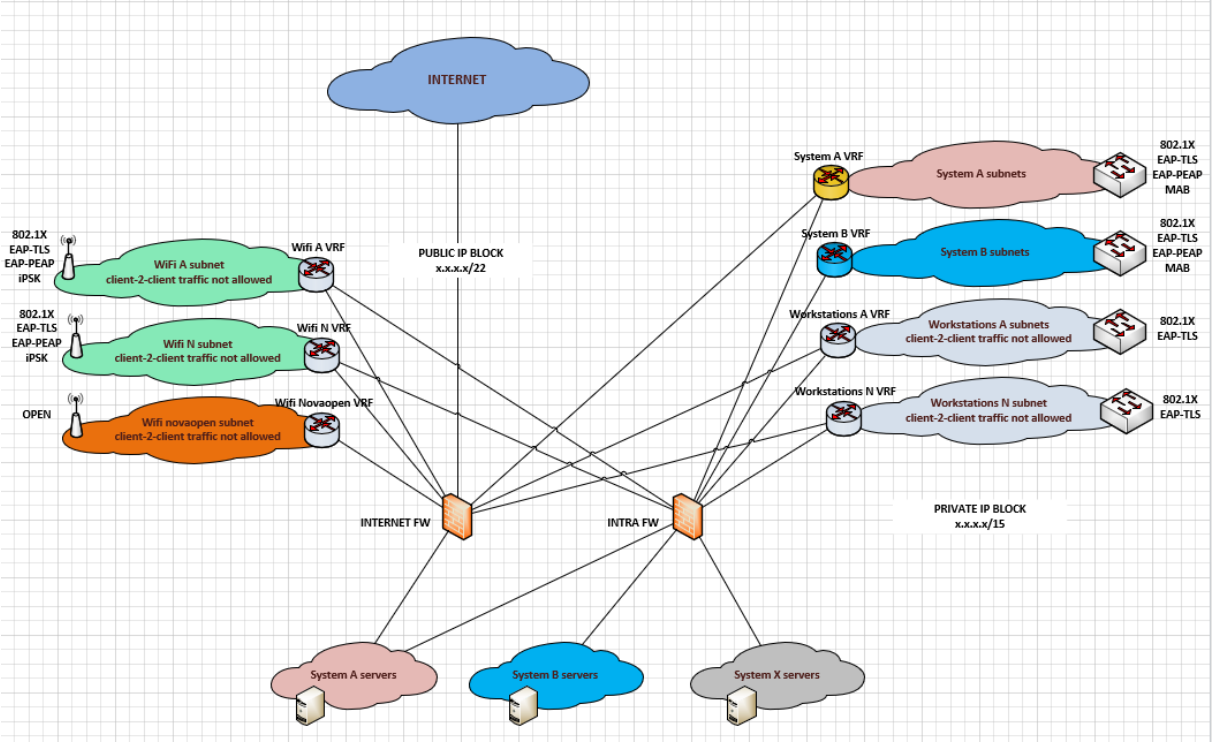
Sairaalan sisäisten virtuaaliverkkojen reititys toteutetaan sairaalan runkoverkossa MPLS-VPN tekniikalla. MPLS-VPN ratkaisu rakennetaan siten, että virtuaaliverkkojen välinen liikenne kulkee sairaalan Intra-palomuurin kautta ja on oletusarvoisesti kielletty. Tällöin sairaalan työasemat eivät voi liikennöidä virtuaaliverkkojen välillä suoraan keskenään. Verkot reititetään jokaisessa sairaalan kerroksessa paikallisesti ja jokaiselle yksittäiselle verkolle allokoidaan oma paikallinen VLAN ID. Työasemaverkot pidetään kerroskohtaisina, eikä niitä laajenneta kerroksesta toiseen muuten kuin erityistapauksessa. Myös kaikki sairaalan erikoislaiteverkot, sekä alueelliset ratkaisut toteutetaan lähtökohtaisesti reititettyinä.

Jokaiselle järjestelmäkohtaiselle virtuaaliverkolle toteutetaan erilliset tietojärjestelmäverkot palomuurilla erotettuna. Jokaiselle virtuaaliverkolle toteutetaan lisäksi mahdollisuus tarvittavien tietoliikenteen peruspalveluiden käyttöön mukaan lukien etäkäyttö, VPN ja ADC-palvelut.

Sairaalan virtuaaliverkoissa käytetään oletuksena privaattiosoitteita (RFC 1918). Julkisissa palveluissa sekä Internetiin liikennöitäessä käytetään sairaalan käyttöön varattuja julkisia IP-osoitteita.

Sairaalan verkossa ei tämän suunnitelman perusteella käytetty IPv6-osoitteita. Kaikissa tietoliikenneverkon laitteissa tulee olla IPv6 tuki tule vaisuuden varalle. Verkon segmentointi havainnollistuu kuvassa 26.

Kuva 26 Verkon segmentoinnin periaate



9.2 Palomuurit

Sairaalan Intra- ja Internet-palomuurit toteutetaan kahdella vikasietoisella, sairaalan datakeskuksiin hajautetuilla palomuuriklustereilla. Kummassakin klusterissa jokaiselle virtuaaliverkolle voidaan toteuttaa erilliset palomuurialueet, joissa käytetään seuraavan sukupolven (Next Generation) palomuuriominaisuuksia sairaalan tietoturvapolitiikan edellyttämällä tavalla. Palomuurit ympäristössä on havainnollistettu kuvassa 27.

Sisäisten verkkojen suojaus hoidetaan Intra-palomuuriklusterilla siten, että Internet-palomuuriklusterin vikaantuminen tai mahdollinen palvelunestohyökkäys ei lamaannuta intra-palomuuriklusterin toimintaa. Palomuuriklusterit tukevat palomuurien virtualisointia siten, että yhdelle klusterille voidaan tarvittaessa tehdä erillisiä loogisia palomuureja sairaalan eri toimijoiden käyttötarkoituksiin.

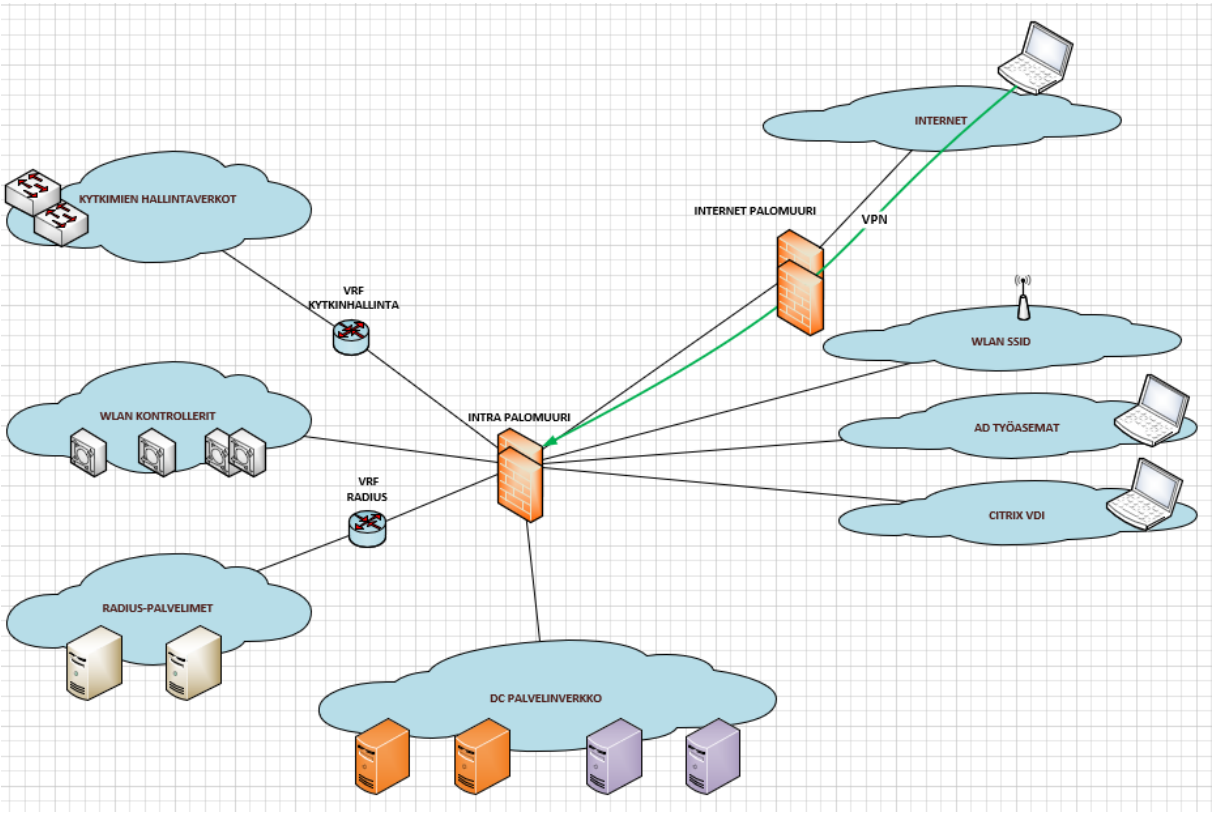
Sekä Intra- että Internet-palomuureissa käytetään sovellus- ja käyttäjätietoisia palomuurisääntöjä, sekä tunkeutumisenesto-ominaisuuksia (IPS). Sovellusten tunnistuksen avulla palvelussa voidaan määritellä palomuurisäännöstö palveluihin ja sovelluksiin riippumatta kommunikoinnissa käytetystä portista tai protokollasta. Sovelluspohjaisella säännöstöllä voidaan hallinnoida muun muassa erilaisia web-palveluita perinteistä palomuuria hienojakoisemmin. Käyttäjäkohtaiset palomuurisäännöt perustuvat AD-palvelimella määriteltyyn käyttäjäryhmään ja kyseiselle ryhmälle rakennettuihin roolipohjaisiin palomuurisääntöihin.

Internetin suuntaan tehtävä palomuuraus tehdään erillisellä palomuuriklusterilla (Internet-palomuuri). Internet muurin tehtävänä on tarkistaa ja suodattaa internetin suuntaan liikennöitäessä. Internet-palomuurille otetaan käyttöön lisäksi tukevia tietoturvaominaisuuksia, kuten haittaohjelma-suodatus, Bot-verkkojen tunnistus, uhkapilveen perustuva analyysipalvelu ja webliikenteen URL-kategorioihin perustuva sisällönsuodatus. Web-liikenteen sisällönsuodatuksella voidaan havaita ja estää sairaalan toiminnalle haitallinen liikenne. Sisältökategoriat päivittyvät dynaamisesti ja ne valitaan tietoturvapolitiikan mukaisesti. Palomuureilla voidaan tarvittaessa purkaa ja salata uudelleen SSL-salattua tietoliikennettä hienojakoisesti URL-kategoriaan tai sovellukseen perustuen.

Osoitemuunnoksiin (NAT/PAT, Network Address Translation/Port Address Translation) käytetään Internet-palomuuriklusteria. Pääsäätöisesti osoitemuunnoksia tarvitaan privaattisoitteiden muuntamiseksi julkiseksi osoitteeksi Internetin suuntaan liikennöitäessä. Sairaalan Internet-liikenteelle tehdään lähdeosoitteen ja -portin muunnos ulospäin menevälle liikenteelle. Sairaalan sisäisessä liikenteessä pyritään ensisijaisesti välttämään osoitemuunnosten käyttöä. Tarvittaessa osoitteenmuunnoksia voidaan kuitenkin tehdä myös intra-palomuurilla, mikäli jokin sisäinen liikenne sitä esimerkiksi muutosvaiheessa vaatii.

Käyttäjätietoiset palomuurisäännöt on tehty AD-käyttäjätunnuspohjaisesti. Näin ollen siis verkosta verkkoon staattiset avaukset on saatu pidettyä minimissään ja palomuuri sallii käyttäjälle AD-ryhmien perusteella luvitetun liikenteen, käyttäjän verkkosijainnista riippumatta.

Kuva 27 Intra ja internet palomuurit



9.3 Verkon autentikointi

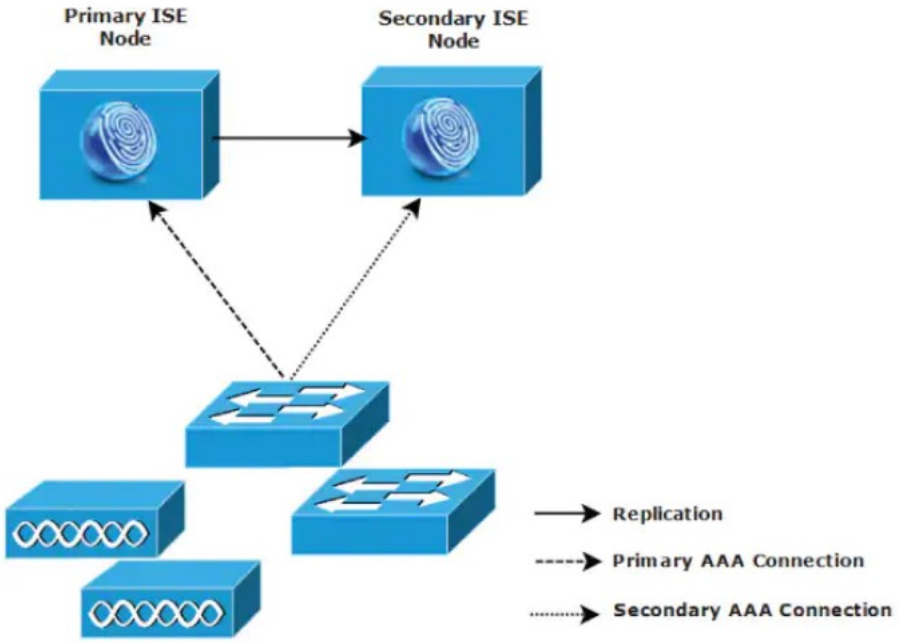
Sairaalan langallisessa lähiverkossa käytetään lähtökohtaisesti kaikissa kytkinporteissa 802.1X-standardin mukaista porttikohtaista tunnistamista. Tunnistaminen pohjautuu käyttäjän päätelaitteen laitesertifikaattiin (EAP-TLS), laitteen verkkoasetuksissa määriteltyyn käyttäjätunnus/salasana pariin (EAP-PEAP) tai käyttäjän AD käyttäjätilin käyttäjätunnus/salasana pariin (EAP-PEAP). Laite siirretään automaattisesti oikeaan virtuaaliverkkoon laitesertifikaatin tai käyttäjätunnuksen AD-ryhmäjäsenyyden perusteella. Mikäli käyttäjän laite ei tue 802.1X-tunnistusta laitesertifikaateilla, autentikointi voidaan tehdä laitteen MAC-osoitteen perusteella. Mikäli laitteen tunnistaminen epäonnistuu, käyttäjän liikennöinti oletuksena estetään.

Palvelussa voidaan automaattisesti profiloida MAC-osoitteiden, erilaisten ohjelmallisten lisäosien ja DHCP-kyselyn perusteella laitteita sekä tarvittaessa sallia tiettyjen tunnettujen laitteiden pääsy verkkoon ilman MAC-osoitteen manuaalista syöttämistä.

Vastaava toteutus on käytössä myös langattomassa lähiverkossa, jossa kontrolleri välittää autentikointitiedon RADIUS-palveluun. Langattomissa verkoissa pyritään käyttämään sairaalan omille päätelaitteille mahdollisimman vähän SSID:tä ja sijoittamaan laitteet oikeaan virtuaaliverkkoon langallista verkkoa vastaavalla toteutustavalla. Vierailijoiden laitteille langattomaan verkkoon toteutetaan erillinen SSID.

Verkon autentikointi on toteutettu Cisco ISE radius virtuaalisella klusterilla. Radius palvelu toimii HA-parina ja oletuksena autentikointipyynnöt menevät aktiiviselle jäsenelle, josta autentikointi kannan tiedot päivittyvät automaattisesti passiiviselle jäsenelle ja on näin valmis ottamaan aktiivisen jäsenen roolin milloin tahansa. ISE radius topologian periaate on esitetty kuvassa 28.

Kuva 28 Cisco ISE radius arkkitehtuuri (Cisco Systems, Inc. 2021)

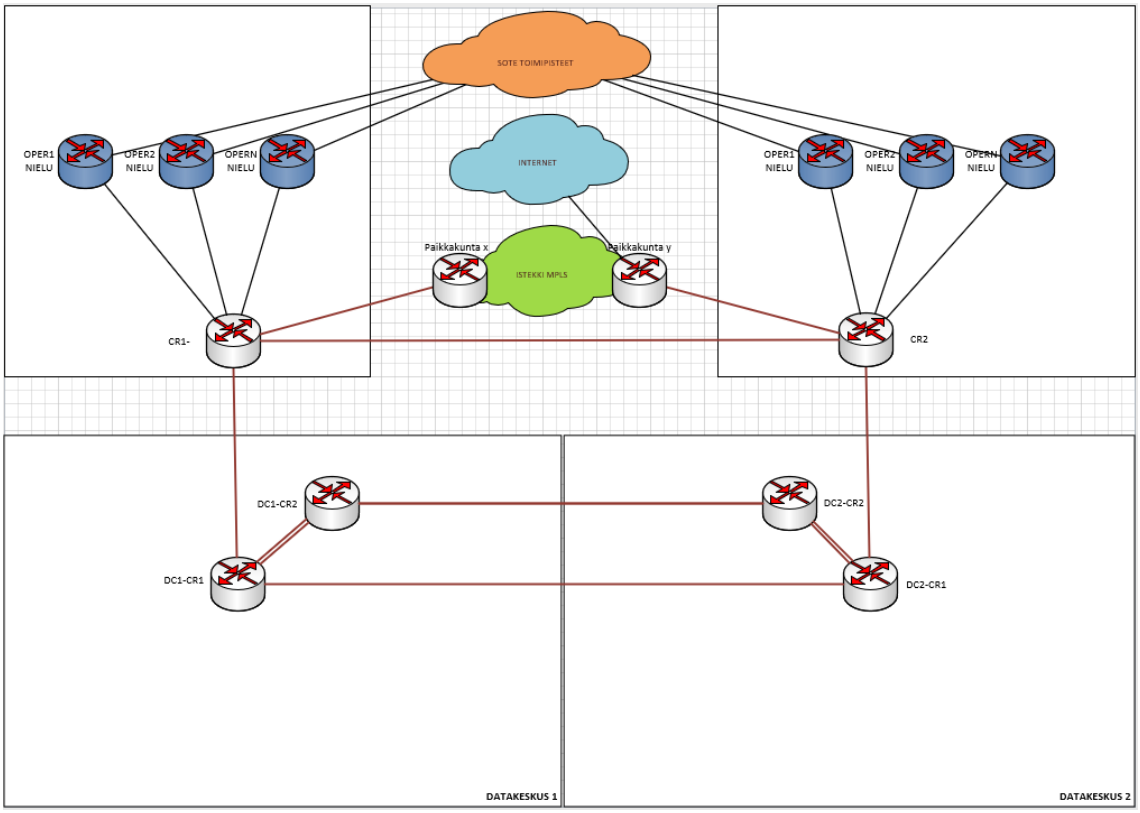


.

10 Ulkoiset yhteydet

Sairaalan ulkoiset yhteydet rakennetaan erillisten operaattoritilojen kautta. Operaattoritiloihin sijoitetaan runkoreitittimet, joista rakennetaan fyysisesti erillisiä kuitureittejä käyttäen varmennetut yhteydet sairaalan datakeskusten runkoreitittimiin. Operaattoritilojen käyttö mahdollistaa useiden operaattorien yhteyksien liittämisen sairaalan verkkoon kahdennettujen operaattorinielujen kautta. Operaattori-tiloista on yhteydet useiden operaattorien runkoverkkoihin, joten BGP-varmennetut Internet-peeraukset, sekä yhteydet ulkoisiin toimijoihin ovat helposti järjestettävissä. Sairaalan ulkoisien yhteyksien toteutuksen periaate on esitetty kuvassa 29.

Kuva 29 Ulkoiset yhteydet



11 Verkonvalvonta

Verkonvalvonta on toteutettu laitteiden lähettämällä SNMP (Simple Network Management Protocol) trap viesteillä, sekä ICMP-pollauksella. Laitteista saadaan siis verkon valvontaan tieto ja tarvittaessa hälytys esimerkiksi prosessori kuormituksista, lämpötiloista ja vaikka BGP

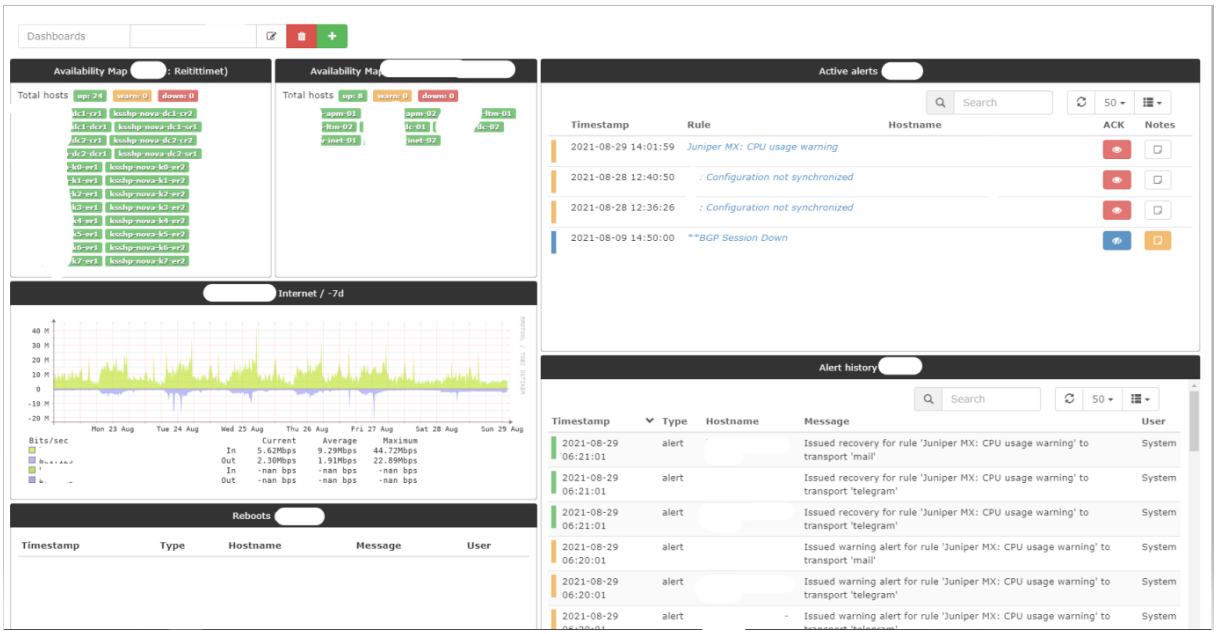
sessioiden virheilystä, jo ennen kuin ICMP-pollauksiin vastaaminen lakkaa ja laitteen todetaan pudonneen verkosta.

Valvontanäkymästä saadaan myös porttikohtaiset liikennemäärän kuvaajat graafisina näkyviin ilman itse laitteelle tarvittavaa kirjautumista ja tiedon hakemista.

Verkonvalvonta on tärkeä osa verkon käytettävyyden turvaamista ja snmp tiedot auttavat ennakoimaan mahdollisiin tuleviin ongelmiin, ennen kuin ne näkyvät verkon loppukäyttäjille.

Verkonvalvonnan näkymä on esitetty kuvassa 30. Näkymässä on oletuksena esitetty graafisesti väreillä esitettynä eri laiteryhmien tila. Vihreä väri tarkoittaa tilanteen olevan laitteella normaali, keltainen laitteella olevan varoitustilanne, kuten korkea lämpötila tai prosessorin kuorma ja punainen väri tarkoittaa laitteen tippuneen valvonnasta. Verkon valvonnan oletusnäkymässä on myös esitetty graafisena internetin käyttö sisään ja ulospäin kulkevan liikenteen osalta. Laitteiden uudelleen käynnistymiset ilmoitetaan omassa kentässään. Oleellisimpia ovat aktiiviset hälytykset näkymä, johon tulevat laitteiden varoitukset ja hälytykset, sekä hälytyksien historia tieto. Valvontanäkymään on mahdollista luoda näkymiä tarpeen mukaan esimerkiksi linkkien käyttöasteesta, mikäli ne ovat sairaalan toiminnan kannalta oleellisia.

Kuva 30 Verkonvalvontanäkymä



12 Johtopäätökset ja pohdinta

Kriittisen sairaalaympäristön tietoverkko on koko hoitotoiminnan kannalta elintärkeä tämän päivän sairaanhoidossa, sanan varsinaisessa merkityksessä. Sairaalan tietoliikenneverkkoon liitetään laitteita ja järjestelmiä hyvin laidasta laitaan, joten yhteensopivuus ja tietoturvan ylläpitäminen on jatkuva prosessi, mutta hyvät vakioidut topologiamallit ja uuden teknologian hyödyntäminen antavat tähän hyvät lähtökohdat.

Opinnäytetyöprosessi oli pitkältä toteutetun kokonaisuuden dokumentointi, valmistajien arkkitehtuurimalleihin syventävää tutustumista, sekä pohdintaa valituista teknologioista ja ratkaisuista.

Itse projektissa oli haasteena varsinkin yllättävät verkkotarpeet, sekä verkkolaitteiden pitkät toimitusajat kansainvälisestä puolijohteiden pulasta johtuen. Näin ollen aikataulu oli koko toteutusvaiheen suurin haaste ja yllättäviä verkkotarpeita ilmeni lähes viikoittain. Hanke saatiin kuitenkin määräajassa valmiiksi ja ennalta asetetuissa verkon määrittelyissä ja tahtotilassa pystyttiin haasteista huolimatta pysymään.

Ylläpidettävyydestä ja verkon saatavuudesta on jo ehditty sairaalan käyttöönoton jälkeen saamaan erittäin hyviä kokemuksia, kun konesalin runkokytkimet, konesaliverkko,

palomuurit ja langaton lähiverkko on kertaalleen suoritettu ohjelmistoversion päivitys ilman käyttäjille näkyviä vaikutuksia.

Myöskään käytönoton jälkeen suunnittelemattomia katkoja tai häiriöitä ei ole ollut, joten voidaan todeta hankkeen olleen onnistunut ja tavoitteiden täyttyneen.

Lähteet

Cisco Systems, Inc. (2017). *Perinteinen ja identity PSK*. Cisco Identity PSK Feature Deployment Guide. Haettu 16.8.2021 osoitteesta https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Cisco Systems, Inc. (2021). *Cisco ISE radius arkkitehtuuri.* Cisco Identity Services Engine Installation Guide, Release 2.4. Haettu 16.8.2021 osoitteesta https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/install_guide/b_ise_InstallationGuide24/b_ise_InstallationGuide24_chapter_00.html

Juniper Networks, Inc. (2021). *Juniper verkkotopologia malli*. Juniper midsize-enterprise-campus-ref-arch-design-considerations. Haettu 23.8.2021 osoitteesta https://www.juniper.net/documentation/en_US/release-independent/solutions/topics/concept/midsize-enterprise-campus-ref-arch-design-considerations.html#jd0e192

Juniper Networks, Inc. (2021). *Juniper kampus arkkitehtuurin malli*. THE AI-DRIVEN CAMPUS Using artificial intelligence for the campus networks of the next decade. Haettu 12.9.2021 osoitteesta https://www.juniper.net/content/dam/www/assets/white-papers/us/en/the-ai-driven-campus-architecture.pdf

Cisco Systems, Inc. (2008). *Cisco Kampus hierarkian arkkitehtuuri malli*. Cisco Enterprise Campus 3.0 Architecture: Overview and Framework. Haettu 23.8.2021 osoitteesta https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html

Cisco Systems, Inc. (2020). *Cisco Rolling AP upgrade*. Cisco High Availability using Patching and Rolling AP Upgrade on Cisco Catalyst 9800 Wireless Controllers. Haettu 11.9.2021 osoitteesta https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-3/deployment-guide/c9800-ha-rau-apsp-apdp-issu-dg-rel-17-3.pdf

Liite 1: Tietoliikenteen vaatimukset liitettäville järjestelmille

Sairaalan liitettäville järjestelmille tarjotaan tilaajan tietoliikenneverkosta tarpeen mukaan Ethernet kytkinportteja, langattoman verkon verkkonimen (SSID), sekä IP-osoitteet. Järjestelmän toimittajan ei siis tule tarjota järjestelmän mukana lähiverkon kytkimiä eikä langattoman verkon tukiasemia.

Jokaiselle järjestelmälle rakennetaan tilaajan tietoliikenneverkkoon järjestelmäkohtainen MPLS IP-VPN (RFC4364) verkko, jonka sisällä järjestelmän liikenne pysyy erillään muiden järjestelmien liikenteestä. Järjestelmäkohtaisen MPLS IP-VPN verkon sisällä laitteet sijoittuvat useisiin IPv4 aliverkkoihin, joiden välille tilaaja järjestää unicast ja multicast reititykset sekä tarvittavat palomuuripalvelut. Tilaaja järjestää lisäksi tarvittavat rajoitetut yhteydet järjestelmäkohtaisesta IP-VPN verkosta muihin järjestelmiin. Broadcast liikenteen välitys ei ole sallittua aliverkkojen välillä.

Tilaaja tarjoaa järjestelmän palvelimille virtualisointialustan kahdennetusta datakeskuksesta. Mikäli järjestelmän mukana toimitetaan palvelinrautaa, tilaaja osoittaa niille laitetilat datakeskuksesta tai muusta soveltuvasta laitetilasta. Tilaaja allokoi järjestelmän palvelimissa käytettävät IP-osoitteet.

Tilaaja tarjoaa liitettäville järjestelmille tarpeen mukaan NTP ja DNS palvelut.

Tilaaja järjestää tarvittaessa salatun etätyöpöydän, jonka kautta on mahdollista saada etäyhteys järjestelmään. Järjestelmän toimittajalla on mahdollista saada etäyhteys järjestelmään myös toimittamalla järjestelmäkohtainen IPSEC-VPN salauslaite tilaajan tiloihin. Tilaaja sijoittaa toimitetun salauslaitteen ja järjestelmän väliin palomuurin, jossa järjestelmään tulevia etäyhteyksiä valvotaan ja rajoitetaan.

Vaatimuksia laitteiden liitettävyydelle:

LAN: Pakolliset vaatimukset

- 10/100Base-T ethernet (Auto-Negotiation, Full Duplex)

- IPv4 DHCP Client

LAN: Vapaaehtoiset, hyväksi katsottavat lisävaatimukset

- 10/100/1000Base-T ethernet (Auto-Negotiation, Full Duplex)

- 802.1X

- LLDP

WLAN: Pakolliset vaatimukset

- 802.11n 5GHz, 20Mz Channel width

- IPv4 DHCP Client

- WPA2-PSK (AES Encryption)

- 1 WLAN verkkonimi (SSID) / system

WLAN: Vapaaehtoiset, hyväksi katsottavat lisävaatimukset

- 802.11n 5GHz, 40Mz channel width

- 802.11ac, 20, 40, and 80MHz channel width

- WPA2-ENT (802.1X + EAP-TLS, AES Encryption)

- Working without SSID broadcasting (hidden SSID)