# POTILASMONITORIVERKON JATKUVUUSSUUNNITELMA

Teemu Siitonen

Opinnäytetyö
Marraskuu 2012

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Tekijä(t):
SIITONEN, Teemu

Julkaisun laji
Opinnäytetyö

Päivämäärä
13.11.2012

Sivumäärä
74

Julkaisun kieli
Suomi

Verkkojulkaisulupa
myönnetty.

Työn nimi
POTILASMONITORIVERKON JATKUVUUSSUUNNITELMA

Koulutusohjelma
Tietotekniikka

Työnohjaaja
LEINO, Janne

Toimeksiantaja
Keski-Suomen sairaanhoitopiiri

Tiivistelmä
Opinnäytetyön tavoitteena oli kartoittaa potilasmonitoriverkon nykytilanne ja päivittää dokumentaatio vastaamaan nykytilannetta. Opinnäytetyön tavoitteena oli myös luoda suunnitelma KSSHP:n potilasmonitoriverkon uudistamiselle.

Nykytilanteessa uudistaminen oli välttämätöntä esimerkiksi kytkimien osalta laitteiston ikääntymisen takia. Myös nykyisen verkon rakennetta oli tarve tarkastella siten, että esimerkiksi monitoriverkko voidaan tulevaisuudessa tarvittaessa eristää muusta toiminnasta, jos muualla verkossa on ongelmia.

Työn aikana oli tarkoituksena myös oppia kaikki alueet jotka liittyvät nykyisen monitoriverkon rakenteeseen, toteutukseen ja ongelmakohtiin. Opiskelu toimi pohjana opinnäytetyön aikana luodulle dokumentaatiolle. Työn tekemisessä oli mahdollista käyttää hyödyksi KSSHP:n henkilökunnan asiantuntemusta sekä Ciscon dokumentointia.

Työ aloitettiin keräämällä tietoa useista eri lähteistä. Saaduista tiedoista kasaantui myöhemmin isompi kokonaisuus, joka kattaa koko potilasmonitorijärjestelmän selkeästi. Tämän jälkeen keskityttiin kuvailemaan tärkeimpiä tietoverkkopuolen ominaisuuksia, joista on apua järjestelmän selkeän kuvan saannissa. Lopuksi tehtiin järjestelmän toiminnallisuuden kannalta tarpeelliset toimintaohjeet sekä selvitykset.

Työssä oli haasteellista saada selkeä käsitys koko potilasmonitoriverkosta, mutta lopullinen dokumentaatio onnistui hyvin. Opinnäytetyöstä tuli paljon uutta dokumentaatiota liittyen potilasmonitorijärjestelmän toteutukseen ja vikatilanteiden hallintaan.

Avainsanat (asiasanat): potilasmonitori, ICS, valvonta, sairaala, tietoverkko

Muut tiedot

Author(s):
SIITONEN, Teemu

Type of publication
Bachelor's thesis

Date
13.11.2012

Pages
74

Language
Finnish

Permission for web publication (X).

Title
CONTINUITY PLAN FOR PATIENT MONITOR NETWORK

Degree Programme
Information Technology

Tutor
LEINO, Janne

Assigned by
Central Finland Health Care District

Abstract
The aim of thesis was to identify the situation of the patient monitor network and to update the documentation to match with the current patient monitor system. The purpose was also to create a plan to the KSSHP's patient monitor system renewal.

Nowadays reforming is necessary, for example on switches due the aging of the system. Additionally, the existing structure of the network needs to be reviewed, and if it is needed, the monitor network for example can be isolated from the network while the rest of the network is having problems.

The purpose of thesis was to learn about all the areas related to the current monitor network structure and its implementation and problems. This study will also be the basis for the documentation created during the thesis. During the study it was possible to benefit both from the expertise of the KSSHP's staff and Cisco's high-quality documentation.

The thesis was started with the gathering of the information from many different sources. Later a larger picture, which covers clearly the whole patient monitor network, was formed based on the information that had been gathered. After this the focus was on describing the most important features of the network, which are helpful when trying to see the whole system. Finally, all necessary action instructions and reports of the system's functionality were written.

It was challenging to get a clear insight of the whole patient monitor network; however, the final documentation was successful. A great deal of new documentation relating to the patient monitor network's implementation and problem management was brought out in the thesis.

Keywords
Patient monitor, ICS, Surveillance

Miscellaneous

**SISÄLTÖ**

## LIITTEET



## KUVIOT



## TAULUKOT

## LYHENTEET

| | |
|---|---|
| AP | Access Point |
| ACS | Cisco Secure Access Control Server |
| AGS | Alarm Group Service |
| CAPWAP | Control and provisioning of wireless access points -protokolla |
| CISCO IOS | Internetwork Operating System |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EKG | Elektrokardiogrammi |
| EOL | End-of-Life |
| EOS | End-of-Sale |
| GBIC | Gigabit Interface Converter |
| ICS | Infinity CentralStation |
| IEEE | The Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| KSSHP | Keski-Suomen sairaanhoitopiiri |
| LAN | Local Area Network |
| MAB | MAC autentication bypass |
| MEQUSOFT | Medical EQUipment SOFTware |
| NCS | Cisco Prime Network Control System |
| NMSRV | Name Service |
| PDS | Patient Data Service |
| RADIUS | Remote Authentication Dial In User Service -protokolla |
| RMA | Return Merchandise Authorization |
| SAS | Serial Attached SCSI |
| SSH | Secure Shell |
| SSID | Service set identifier |
| STP | Spanning tree -protokolla |
| TAC | Cisco's Technical Assistance Center |
| TACACS | Terminal Access Controller Access-Control System |
| VLAN | Virtual Local Area Network |
| WLAN | Wireless Local Area Network, |

| | |
|---|---|
| VSL | Virtual Switch Link |
| VSS | Virtual Switching System |
| VST | Vastasyntyneiden teho-osasto |
| VTP | VLAN Trunking Protocol |

# 1 OPINNÄYTETYÖN LÄHTÖKOHDAT

## 1.1 Lähtötilanne

Tämä opinnäytetyö tehtiin Keski-Suomen sairaanhoitopiirille. Työ oli suunniteltu ja toteutettu hyvin pitkälle omatoimisesti Keski-Suomen keskussairaalassa, lääkintätekniikan tiloissa.

Lääkintätekniikka on lääketieteellisen tekniikan palveluyksikkö tehtävänään erilaisten potilaan hoitoon ja tutkimukseen käytettävien laitteiden ja välineiden ylläpito- ja asiantuntijatehtävät sekä kyseisten toimitilojen varustelu- ja asiantuntijatehtävät. Lääkintätekniikka pyrkii osaltaan avustamaan sairaalan tutkimus- ja hoitotoimintaa laitteiden ja tilojen hankesuunnittelusta toteutukseen sekä huolehtii laitteen elinkaaren aikaisesta ylläpidosta aina laitteen poistamiseen saakka. Potilasmonitorijärjestelmien ylläpito ja huolto kuuluvat lääkintätekniikan vastuualueeseen Keski-Suomen keskussairaalassa. Lääkintätekniikassa työskentelee eri asiantuntijatehtävissä 19 henkilöä.

Opinnäytetyön aihetta mietittiin lääkintätekniikassa useampaan otteeseen, koska haluttiin löytää aiheen, joka olisi riittävän laaja ja josta olisi myös hyötyä KSSHP:lle. Keväällä 2012 tuli lääkintätekniikassa esille, että potilasmonitorijärjestelmässä voisi olla kehittämisen tarvetta ja tästä aiheesta olisi hyvä tehdä opinnäytetyö, koska työhön liittyi paljon selvitystyötä ja ammatillista kokemusta piti käyttää hyväksi.

Työnaihe antoi hyvät lähtökohdat ottaa myöhemmin vastuulle suurempaa kokonaisuutta potilasmonitoriverkon ylläpidosta ja vapauttaa näin muiden asiantuntijoiden kompetenssia muihin haasteellisiin tehtäviin.

## 1.2 Tehtävänanto

Opinnäytetyön tavoite oli luoda edellytykset KSSHP:n potilasmonitoriverkon uudistamiselle sekä parantamiselle tulevaisuudessa.

Keskussairaalan potilasmonitorijärjestelmä oli ajan saatossa kärsinyt heikosta dokumentoinnista. Tämä johtui useasta eri asiasta. Järjestelmät oli otettu käyttöön usean vuoden aikana, joista vanhimmat ovat tämän vuosituhannen alkupuolelta. Yksi syy on myös se, että potilasmonitorijärjestelmät eivät ole nykyään alkuperäisellä osastolla käytössä, vaan potilasmonitorijärjestelmiä on siirretty toiselle osastolle. Keskussairaalan potilasmonitorijärjestelmillä on myös useita eri toimittajia.

Tämän vuoksi opinnäytetyöhön kuului paljon selvitystyötä ja dokumentointia nykyisen potilasmonitorijärjestelmän nykytilanteesta. Ensimmäiseksi täytyi tutustua potilasmonitoriverkon rakenteeseen ja laitteisiin huolellisesti. Tämän selvityksen pohjalta luotiin kattava dokumentaatio laitteistosta ja verkkotopologiasta.

Opinnäytteen tavoitteisiin kuului myös tietoliikennelaitteiston ikääntymisen vuoksi tarkistaa laitteiston kunto sekä ikä ja varmistaa, että ikääntymisestä ei aiheudu haittaa. Tarvetta oli myös luoda suunnitelma laitteiston uusimiselle ja ryhtyä tarvittaviin toimenpiteisiin.

Lääkintätekniikkaan oli myös tarkoitus saada ohjeistus tarpeellisista potilasmonitoriverkon laitteista niin, että pienellä opastuksella lääkintätekniikasta asiantuntijat osaavat tehdä huoltotoimenpiteitä jotka liittyvät potilasmonitoriverkon tietoliikenneyhteyksiin.

Infrastruktuurista ei ollut todellista kuvaa tiedossa. Tiedot olivat erittäin monessa paikassa ja vaikeasti löydettävissä. Opinnäytteen aikana luotuja doku-

mentteja pitää pystyä myöhemmin käyttämään työssä avuksi sekä ylläpitämään niitä niin, että ne ovat aina ajan tasalla.

Potilasmonitorijärjestelmän toiminnan varmistamiseksi isomman tietoverkkoongelman sattuessa oli myös syytä tarkastella nykyistä verkkoa siten, että monitoriverkko voidaan tarvittaessa eristää muusta toiminnasta.

KSSHP:ssa on tarkoitus vuoden 2013 aikana ottaa laajemmin käyttöön dynaaminen VLAN, joten oli myös tarve ottaa selvää kuinka dynaamisen VLANin käyttöönotto vaikuttaa potilasmonitorijärjestelmän laitteisiin.

Työn aikana tuli myös esille, että Dräger Delta -potilasmonitoriverkon langattoman IP-osoitteistuksen kanssa on epäselvyyksiä, koska IP-osoitteiden jakamisen kanssa ei ollut yhtenäistä käytäntöä. Tästä syystä piti myös tehdä selvitys siitä, miten tällä hetkellä IP-osoitteet myönnetään ja miten sitä voidaan kehittää.

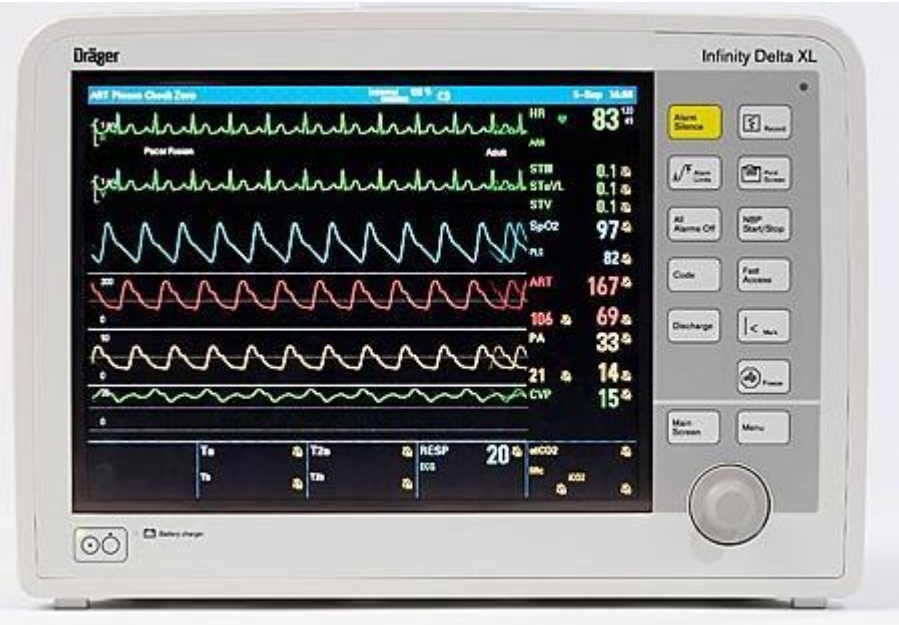
Työn aikana oli tarkoituksena myös oppia kaikki alueet, jotka liittyvät nykyisen monitoriverkon rakenteeseen, toteutukseen ja ongelmakohtiin. Näistä asioista on apua myöhemmin työelämässä. Opinnäyte keskittyi tietoliikennepuolen selvityksiin ja ongelmiin. Osa tehdystä dokumentaatiosta sisälsi IP-osoitteita tai muuta arvokasta tietoa. Tämän vuoksi nämä kohdat opinnäytetyöstä piti rajata lääkintätekniikan käyttöön ja eivät siten ole julkisia.

# 2 POTILASMONITORIJÄRJESTELMÄ

## 2.1 Mikä on potilasmonitorijärjestelmä ja mitä se sisältää?

Potilasmonitorijärjestelmä koostuu useammasta eri laitteesta, kuten potilasmonitorista, valvontakeskuksesta, telemetrialähettimistä ja tietoliikennekytkimistä.

Potilasmonitori on laite, joka seuraa yhtä tai useampaa fysiologista parametria. Potilasmonitorin ruudulta sairaalanhenkilökunta voi seurata potilaan vitaaliparametrien arvoja reaaliaikaisesti ja saada tietoa hoitopäätöksiin sekä seurata hoitojen vaikutuksia. Yksi yleisesti käytössä oleva malli on kuvion 1 Dräger Infinity Delta -potilasmonitori.




KUVIO 1. Potilasmonitori (Infinity Delta)

Yleensä potilasmonitori sijoitetaan huoneeseen potilaan viereen telakointiasemaan tai kiinteästi sängyn lähettyville. Potilasmonitorijärjestelmään voi myös kuulua keskusvalvontayksikkö, jonka avulla saadaan useamman potilasmonitorin tiedot yhdelle ruudulle esimerkiksi monitorityöasemalle. Lääkäri voi myös ottaa järjestelmään etäyhteyden, jonka kautta hän voi seurata tietyn monitorin tietoja reaaliaikaisesti. Lääkäri voi myös tätä kautta tarkastella historiaa. Etähallinta ei kuitenkaan ole välttämätön, joten potilasmonitori toimii myös ilman sitä. Telakoituvat potilasmonitorit ovat hyödyllisiä, koska niissä on langaton tiedonsiirtoyhteys ja akku. Tämä mahdollistaa potilaan elintoimintojen reaaliaikaisen seurannan, myös kun potilasta esimerkiksi siirretään eri osastolta toiselle.

## 2.2 Potilasmonitoriverkko KSSHP:ssä

Potilasmonitoriverkkoja on KSSHP:ssä kolmella leikkausosastolla, päivystyspoliklinikalla, sydänvalvonnassa, neurologian poliklinikalla, lastenosasto 1:llä, teho-osastolla sekä leikkaussalien heräämöissä. Laajin verkko on Drägerin tarjoama potilasmonitorijärjestelmä. Myös Philips ja GE/ Datex ovat edustettuina sairaanhoitopiirissä, mutta pienemmässä määrin. Drägerin verkko toimii osittain tietoliikennekytkimissä, joiden kautta kulkee myös muuta KSSHP:n verkon liikennettä. Myös GE:n, teho-osaston sekä Datexin heräämön potilasmonitorijärjestelmät ovat KSSHP:n tietoliikennekytkimien kautta kytketty.

## 2.3 Dräger

### 2.3.1 Yleistä

Dräger on toiminut vuodesta 1889 ja on johtava kansainvälinen sairaala- ja turvallisuusteknologia-alan konserni. Drägerin verkko on levittäytynyt kes-

kussairaalalla useisiin eri osastoihin, ja siihen kuuluu satoja laitteita. Keski-Suomen sairaanhoitopiirin verkkotopologiassa Dräger-potilasmonitoriverkko on eriytetty sairaanhoitopiirin muusta verkosta virtuaaliverkoilla. Dräger-potilasmonitoriverkko toimii omassa virtuaaliverkossaan ja Dräger-telemetriaverkko omassa virtuaaliverkossaan. (Patient Monitoring 2012)

Drägerin potilasmonitorijärjestelmän tietoverkon laitteisiin kuuluvat ICS-potilasvalvontakeskus, M300-telemetrialähettimet ja Dräger Delta -potilasmonitorit.

### 2.3.2 Liikenne Dräger-verkossa

Arviolta 99 % liikenteestä tulee monitoreilta ja suurin osa liikenteestä on multicast-liikennettä, mikä tarkoittaa sitä, että lähetys tapahtuu yhdeltä useammalle kohteelle. Multicast-liikennettä on potilasmonitoriverkossa noin 90 % kokonaisliikenteestä. Multicastia on esimerkiksi se, kun keskusvalvonta lähettää multicast-kehyksen, jonka sisällä on ICS:n kellonaika jokaiselle potilasmonitorille. (Ks. taulukko 1.)

Multicastia käytetään hälytyksille, potilasdatalle, järjestelmän kellolle sekä nimen levittämiselle. AGS-paketissa siirtyy potilaan tilatieto keskusvalvontaan. AGS vent –paketti lähetetään, kun monitori on kytketty MIB:n kautta ventilaattoriin. Name servicen avulla ICS tietää, että monitori on vielä verkossa. Aikapalvelun avulla monitori tietää, että sillä on vielä verkkoyhteys.

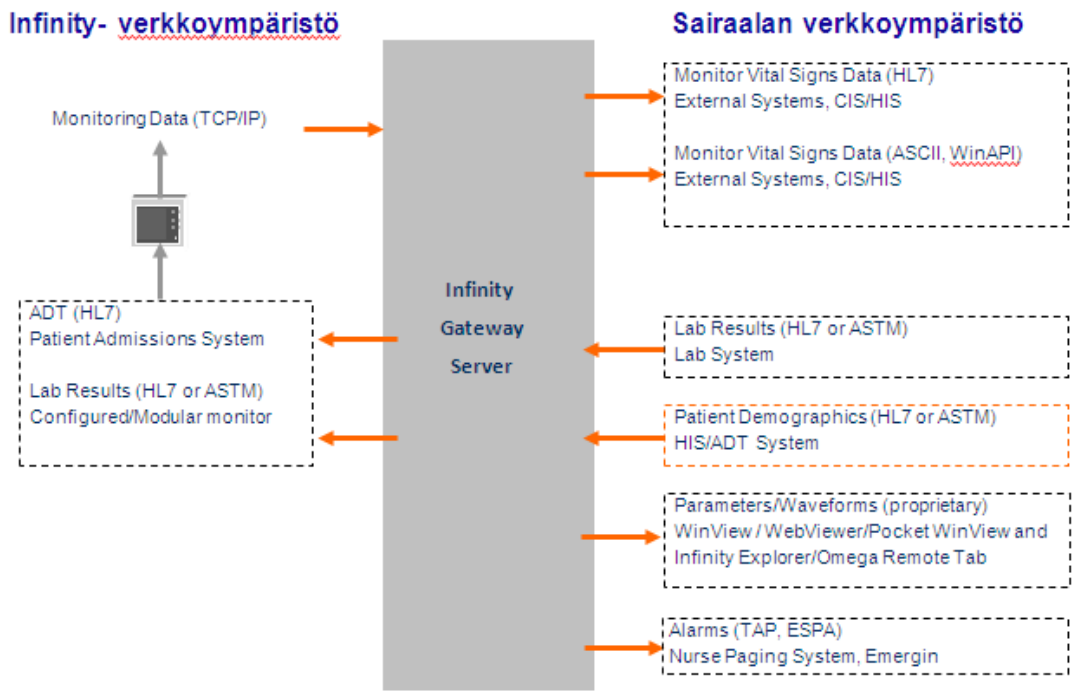
TAULUKKO 1. Potilasmonitoriverkon Multicast-liikenne

| Nimi | Multicast-osoite | Portti | Pakettien määrä |
|---|---|---|---|
| AGS | 224.127.Monitoriyksikkö .254 | 2000 | Yksi paketti jokaiselle monitorille. |
| AGS Vent | 244.127.Monitoriyksikkö .252 | 9250 | Yksi paketti jokaiselle monitorille. |
| NMSRV | 224.127.Monitoriyksikkö .Switch | 2150 | Jokainen laite mainostaa itseään yhdellä paketilla 20 sekunnin välein. |
| Time Service | 224.127.Monitoriyksikkö .253 | 2100 | ICS lähettää yhden paketin kymmenen sekunnin välein jokaiselle monitorille |
| PDS (monitorit) | 224.0.Monitoriyksikkö.Vuodepaikka | 2050 | Monitorit lähettävät kuusi pakettia sekunnissa. Sisältää käyrät ja parametrit. |
| PDS (telemetria) | 224.Vuodepaikka.Monitoriyksikkö.ID | 2050 | Telemetriat lähettävät kuusi pakettia sekunnissa. |

### 2.3.3 Dräger Infinity Gateway Server

Gatewayn kautta kulkee liikenne eri tietojärjestelmille kuten päivystyksen tietojärjestelmään, anestesiatietojärjestelmään sekä henkilötietojen haku henkilörekisteristä. Kuviossa 2 on kuvailtu Infinity Gateway Serverin lävitse menevä liikenne.

Nykyään Infinity Gateway sijaitsee konesalissa virtuaalipalvelimella. Ennen gateway oli fyysinen palvelin konesalissa, tämä muutos tapahtui syksyn 2012 aikana. Infinity Symphony -käyttöliittymä työaseman internet-selaimella antaa mahdollisuuden selata potilasvalvonnan historiatietoja ja reaaliaikaista dataa tietystä potilasmonitorista.




KUVIO 2. Gatewayn liikenne (Onemed, Koulutusmateriaali)

### 2.3.4 Dräger ICS

KSSHP:ssä on käytössä kahden mallisia ICS-keskusvalvontatietokoneita, mustia ja valkoisia. Väri kertoo keskusvalvontayksikön mallin. ICS on terveydenhoitoalan ammattilaisille, sairaaloihin ja terveyskeskuksiin tarkoitettu keskitetty seurantajärjestelmä, jonka käyttöjärjestelmä on Mandriva Linux 2009. Se soveltuu niin aikuisten, lasten kuin vastasyntyneidenkin tilan seurantaan Infinity-potilasseurantaverkossa.

ICS seuraa yhtä tai useampaa fysiologista parametria ja ilmoittaa niistä näkyvin ja kuuluvin hälytyksin. ICS ja sen lepo-EKG-näkymä selkeyttävät diagnoosien tekoa aikuis- ja lapsipotilaissa, jotka on kytketty EKG-seurantaan tarkoitettuun monitoriin. Yhtäaikaista informaatiota voidaan saada jopa 32 laitteelta. ICS muistaa 24 tuntia graafista ja numerollista trendiä. On myös mahdollista saada pitempiaikaista dataa, mutta tämä pitää katsoa gatewayn kautta. ICS:stä voidaan myös tulostaa arkistointikelpoista dataa. ICS lähettää seu-

rantaparametrit keskitetysti kliiniseen tietojärjestelmään, joka sijaitsee gatewaylla. (Infinity Central Station 05/ 2008)

### 2.3.5 Dräger Delta -potilasmonitori

Delta-potilasmonitori on tarkoitettu aikuisten, lasten ja vastasyntyneiden tilan seurantaan. Sitä voidaan käyttää yksinään erillisenä laitteena tai se voidaan kytkeä Infinity-verkkoon. Monitori on aina potilaskohtainen.

Monitori on varustettu ”poimi ja siirry” –ominaisuudella, eli monitorin voi irrottaa telakasta ja siirtää molemmat, sekä monitori että potilas toiseen sijaintiin. Potilasta ei tarvitse siis kirjata ulos ja uudelleen sisään toiseen monitoriin, sillä monitori kulkee aina potilaan mukana. Sen lisäksi, että tämä säästää aikaa, se myös auttaa seuraamaan potilaan tilaa siirron aikana.

Yhteys keskusvalvontaan toimii siirron aikana langattoman verkon kautta. Jos monitori siirron aikana epäonnistuu yhteyden siirtämisestä langattomasta tukiasemasta toiseen langattomaan tukiasemaan, katkos ei vaikuta monitorin toimintaan paikallisesti, vaan sairaanhoitohenkilökunta näkee edelleen potilaan lähellä monitorista tarvittavan tiedon. Yhteyden katkeaminen vaikuttaa vain yhteyteen potilasmonitorista keskusvalvontaan, jossa näkyy, että monitori ei enää välitä informaatiota keskusvalvomoon. (Infinity Delta 12/ 2012)

Jokaiselta monitorilta voidaan myös valvoa muita monitoreja, eli datan saa näkymään monitorista toiseen.

Telakka toimii myös potilasmonitorin laturina, kun potilasmonitori on kiinni telakassa. Telakassa ollessaan potilasmonitori käyttää telakan verkkokorttia langalliseen verkkoon pääsemisessä ja langaton yhteys ei ole käytössä.

Langaton verkko toimii, kun monitoriin on konfiguroitu delta-SSID sekä

verkkoon liittymiseen tarvittava salasana. Salaustapana on käytössä WPA2-PSK. WPA2 on langattomien 802.11-verkkojen viimeisin jaetunavaimen tietoturvastandardi. Salausavaimena käytetään 8-63 merkin mittaista salasanaa.

Heräämöjen potilasmonitorit lähettävät Dräger-verkossa sijaitsevan gatewayn kautta anestesiadatan anestesiatietojärjestelmään.

### 2.3.6 Dräger Infinity M300 -telemetrialähetin

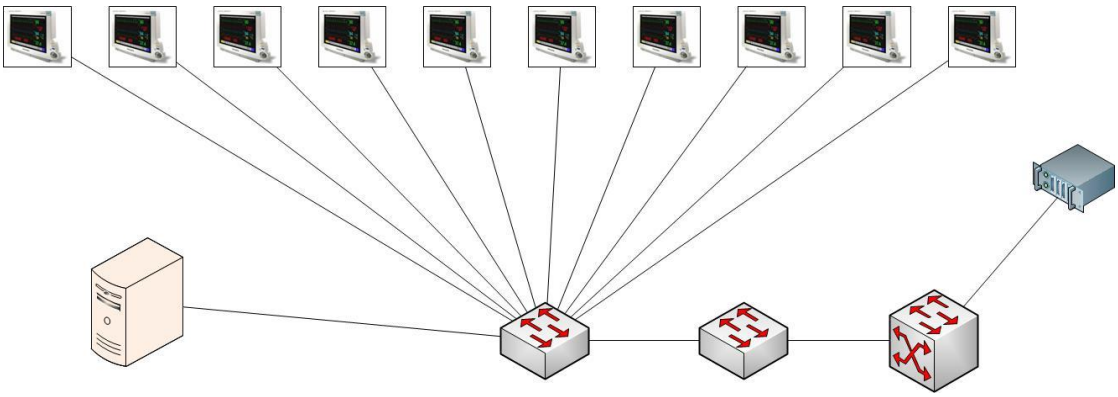
Dräger Infinity M300, WLAN-yhteydellä toimiva, värinäytöllinen telemetrialähetin, on terveydenhoitoalan ammattilaisille tarkoitettu telemetriajärjestelmä EKG:n ja pulssioksimetria-parametrien seurantaan. M300 on pieni, vedenkestävä, taskuun sopiva laite, jota potilas voi kuljettaa koko ajan mukanaan. Infinity M300 on tarkoitettu toimimaan langattomassa verkossa ICS:n kanssa. Langattomuus tuo vapautta liikkua. Telemetrialähetin lähettää reaaliaikaisesti parametrien arvot ICS:lle.

## 2.4 DATEX-potilasmonitorijärjestelmä GE S/5 iCentral

### 2.4.1 Yleistä

Datex-potilasmonitorijärjestelmä toimii omassa VLANissa ja on liitettynä KSSHP:n tietoliikenneverkkoon, koska anestesiadata lähetetään anestesiatietojärjestelmään. Järjestelmässä ei ole langatonta verkkoa eli kaikki laitteet ovat kiinni fyysisellä kaapeloinnilla. DATEX-potilasmonitorijärjestelmä koostuu keskusvalvontayksiköstä, potilasmonitoreista. Kuviossa 3 on Datex-verkon topologia, josta selviää tarkemmin, mitkä kytkimet kuuluvat Datex-potilasmonitorijärjestelmään ja mitä kautta liikenne kulkee gatewaylle.

Alun perin DATEX-potilasmonitorijärjestelmä sijaitsi teho-osastolla, mutta teho-osaston potilasmonitorien uusinnan myötä keväällä 2012 järjestelmä siirrettiin leikkausosastojen heräämö 2:een. Järjestelmä koostuu tietoliikennekytkimistä, potilasmonitoreista sekä keskusvalvonnasta.



KUVIO 3. DATEX-potilasmonitorijärjestelmän topologia

### 2.4.2 DATEX-keskusvalvontayksikkö

HP Compaq D530 CMT -työasema toimii keskusvalvontatietokoneena ja sillä voidaan tutkia reaaliaikaista dataa ja selata historiaa. Keskusvalvontayksikkö on konfiguroitu Clinisoftin VLANiin.

Keskusyksikkö vastaanottaa hälytyksiä potilaista, jotka ovat kytkeytyneet DATEX-potilasmonitorijärjestelmään. Työasema tukee kahta näyttöä, joista voidaan seurata yhtä aikaa maksimissaan 32 potilasta.

### 2.4.3 DATEX S/5 AM -potilasmonitorivalvontayksiköt

Datex S/ 5 AM -potilasmonitorit toimivat VLAN ***:ssa. Järjestelmässä on heräämö 2:lla 10 potilasmonitoria, joissa voi olla liitettynä moniparametrimo-

duuleja, relaksaatiomoduuleita, painemoduuleja ja monikaasumoduuleja tarpeen mukaan. Potilasmonitorit lähettävät mediamuuntimen kautta potilasdatan suoraan anestesiatietojärjestelmään, eli keskusvalvontaa ei tarvitse olla.

Potilasmonitoreja on sijoitettu myös muihin heräämöihin, mutta ilman keskusvalvontaa, jolloin ne toimivat itsenäisesti osastolla Dräger Delta -potilasmonitorien rinnalla.

## 2.5 Teho-osaston potilasmonitoriverkko

Uusittu teho-osaston potilasmonitoriverkko on toiminnassa, mutta koko järjestelmän käyttöönotto ei ole vielä täysin valmis. Käyttöönottoprojektia on tehty vuoden 2012 aikana ja käyttöönotto on tuonut mukanaan projektia viivästyttäviä haasteita. Potilasmonitorijärjestelmä toimii KSSHP:n kytkimien kautta ja niille on luotu omat VLANit.

Opinnäytetyön aikana teho-osaston kaapelointien merkinnät toteutettiin tarkasti. Kaapelimerkinnät potilaspaikalla on toteutettu niin, että kaapelissa sekä rasiassa on selkeät merkit, mihin mikäkin kaapeli tulee, ja tämän lisäksi kaapelit ovat erivärisiä.

Teho-osaston toiminnan kannalta potilasmonitoriverkon ympärivuorokautinen toiminta on erittäin tärkeää. Tästä johtuen kytkimiin on suunniteltu dynaamisen virtuaaliverkon käyttöönotto. Ristikytkentään on lisätty uusi tietoliikennekytkin, ja nyt portteja on vapaana niin paljon, että yhden kytkimen rikkoutuessa voitaisiin kaapelointi siirtää tyhjiin portteihin ja palauttaa toiminnallisuus teho-osaston työntekijöiden itsenäisellä toiminnalla.

## 2.6 Philips-potilasmonitorijärjestelmä

Philipsin potilasmonitorijärjestelmä on suljettu järjestelmä mikä toimii vastasyntyneiden teho-osastolla jossa hoidetaan tehohoitoa tai tehostettua hoitoa ja valvontaa tarvitsevia vastasyntyneitä.

Osastolla 3 keskusvalvonta sijaitsee tehohoitohuoneessa, ja tähän saadaan näkymään kahdeksan eri potilasmonitoria. Osastolla on käytettävissä keskusvalvontaan yhteensopivia monitoreja 10 kpl MP70, 2 kpl MP50 ja 1 kpl MP30.

M70 on selkeästi kookkain laite. Siinä ei ole akkua, ruudun koko on 15”, kun MP 50:ssä koko on 12” ja MP30:ssa koko on enää 10.4”. MP50 ja MP30 ovat siirrettäviä, mutta verkkoliitäntä on langallinen.

Keskusvalvontakoneena toimii Intellivue information center HP RP 5700, jossa on kiinni kaksi monitoria. (Philips IntelliVue 2012)

# 3 KSSHP:N VERKKOINFRASTRUKTUURI

## 3.1 Verkonhallinta

Potilasmonitorijärjestelmiin kuuluu oleellisena osana tietoverkko. Potilasmonitorit, telemetrialähettimet sekä keskusvalvontayksiköt kommunikoivat kaiken keskinäisen liikenteen KSSHP:n tietoliikennekytkimien ja langattomien tukiasemien kautta. Seuraavaksi on käyty yleisimpiä tietoliikennekytkimien käsitteitä ja tapoja toimia.

Keski-Suomen sairaanhoitopiirin tietoverkko on tietoliikenneinsinöörien vastuulla ja heidän toimipisteensä sijaitsee lääkintätekniikassa keskussairaalassa.

Verkon jokaiseen kytkimeen pääsee kiinni SSH-yhteydellä Putty- tai muun SSH-ohjelman avulla tai paikallisesti konsoliyhteydellä. Yhteyden muodostuksessa käytetään TACACS-autentikointia varmentamaan, että käyttäjällä on oikeus kirjautua kytkimelle. Tunnuksena käytetään henkilökohtaista hallintatunnusta.

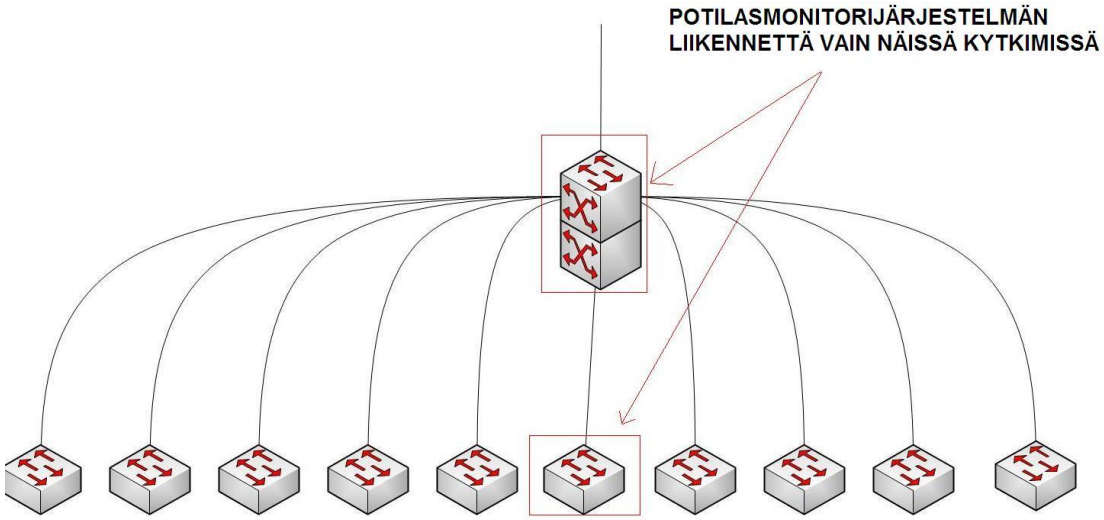
Potilasmonitoriverkossa on muutamia laitetoimittajan tarjoamia kytkimiä, joita ei voida hallita etäkäyttöisesti, mutta näiden kytkimien konfigurointi ei kuulu lääkintätekniikan henkilökunnalle. Sisä- ja ulkoverkon tietoliikennekytkimille on valmiit konfigurointipohjat, mutta esimerkiksi uuden potilasmonitoriverkon kytkimen lisääminen tai vaihtaminen on silti tehtävä tapauskohtaisesti toimintakuntoon.

## 3.2 Dokumentointi ja tietoverkkokuvat

Sairaalan potilasmonitoriverkko ei ollut tuttu insinöörityön alkaessa. Tästä johtuen yritin tukeutua olemassa olevaan dokumentointiin saadakseni hyvän kuvan potilasmonitoriverkosta. Tämä ei käytännössä onnistunut, koska tieto joka löytyi koski vain osaa järjestelmästä ja kokonaiskuva järjestelmästä jäi melko epäselväksi. Tietoverkosta oli KSSHP:ssä hyvät topologiakuvat, jotka olivat ajan tasalla, mutta ne eivät käsitelleet potilasmonitoriverkkoa erikseen. Kuviossa 4 on malli esimerkki verkon topologiasta kuinka alkutilanteessa potilasmonitoriverkon kytkimet oli kuvattu yhdessä topologia kuvassa.

Jotain tietoa potilasmonitorijärjestelmästä löytyi Mequsoftista, joka on KSSHP:ssä kehitetty lääkintälaiterekisteri. Mequsoft on nykyään Suomen keskussairaaloissa yleisesti käytössä, sillä yli puolet Suomen keskussairaaloista käyttää Mequsoftia laiterekisterinä. Mequsoft kattaa hyvin laitteet, joita on lisätty potilasmonitorijärjestelmään Keski-Suomen keskussairaalassa, mutta Mequsoftissa oikea tieto on vaikeasti noudettavissa ja mequsoftista on vaikea saada selkeää kuvaa koko järjestelmästä. Yksittäisestä laitteesta Mequsoftista saa hyvin tietoa, josta selviää laitteen tunnistamiseen, takuuseen, varusteluun sekä huoltoon liittyviä tietoja. Mequsoftin lisätiedot-kentästä löytyi joskus järjestelmään liittyviä dokumentteja joista sai lisäinformaatiota kyseisen järjestelmän toteutuksesta.

Lisätiedot-kenttään voidaan myös liittää liitetiedostoja. Tätä ominaisuutta käytettiin opinnäytetyön liitteiden tallentamiseen tietylle laitteistolle. Esimerkiksi järjestelmien topologiakuvat on nyt liitetty kyseiselle laitteistolle.




KUVIO 4. Potilasmonitorijärjestelmäkytkimet tietoverkkokuvissa.

## 3.3 Runko-, kuitu- ja työryhmäkytkimet

Verkon runkona toimii kaksi Ciscon WS-C6500–sarjan reitittävää kytkintä. Kytkimet sijaitsevat keskussairaalan konesalissa.

Runkoon on luotu VSS-pari yhdistämällä 6500-sarjan kytkimet porttikanavan avulla 10Gbit porteista ja luomalla Virtual Switching Link (VSL) niiden välille. Tämä luo kahdesta kytkimestä yhden laitekokonaisuuden. Näin ollen niiden hallinta ja valvonta helpottuu huomattavasti.

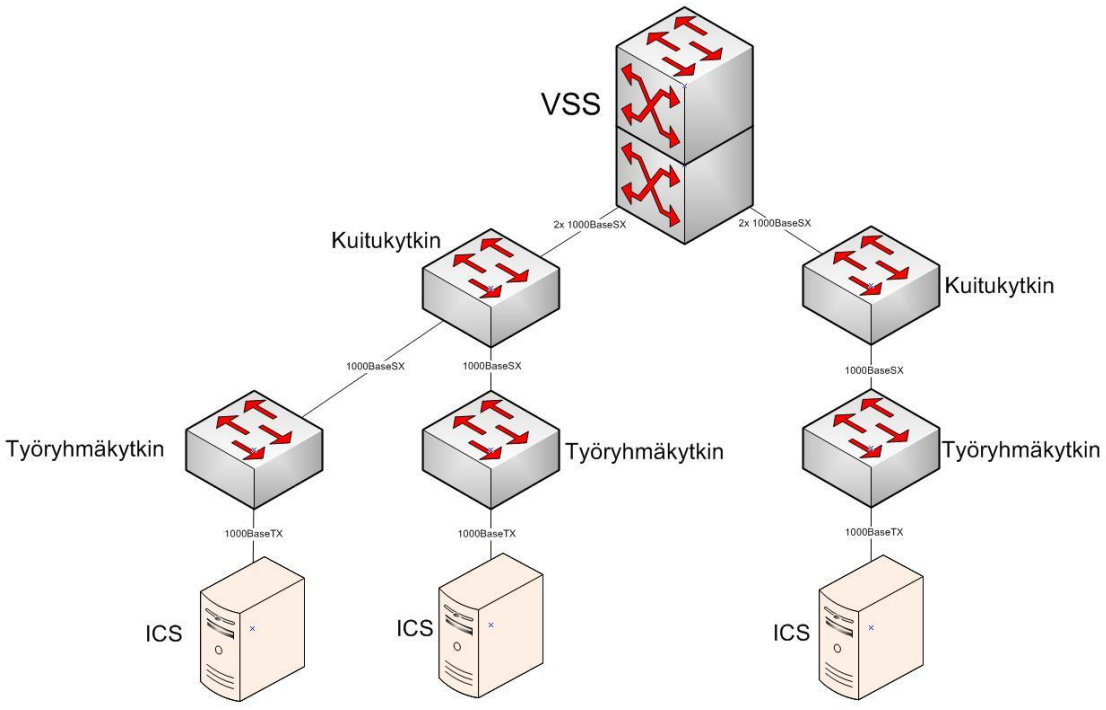
Kuitukytkimet ovat kiinni VSS-rungossa kahdella kuitukaapelilla, kaapeliksi käy joko 1000Base-SX tai 1000Base-LX kaapelit. Monimuotokuitu eli SX on tarkoitettu lyhyen matkan kuitukaapelivetoihin (enintään 500 metriä) ja yksimuotokuitu LX:llä voidaan päästä jo muutaman kilometrin pituuksiin.

Kuidut ovat kiinni GBIC-mediamuuntimen kautta kytkimissä, jolloin GBIC-muunnin tulee kytkimessä GBIC-moduulille varattuun paikkaan.

Kuitukytkiminä käytetään Ciscon WS-C3750G-12S-mallia, joka on yhteensopiva rungon kanssa sekä osoittautunut luotettavaksi. Verkon ylläpitäjillä on myös riittävästi kompetenssia Ciscon laitteiden ylläpitoon. Ohjelmistoversio on päivitetty jokaiseen kytkimeen samaksi yhteensopivuuden varmistamiseksi sekä konfiguraation yhtenäistämiseksi.

Kuitukytkimien fyysisen yhteyden kahdennus on toteutettu kytkemällä kuitukytkimestä kuitukaapeli kumpaankin VSS-parin kytkimeen. Tämä varmistaa verkon toiminnallisuuden, vaikka toinen VSS-kytkin, kuitukaapeli tai GBIC-mediamuunnin vikaantuisi.

KSSHP:n ristikytkentäkaapeissa on useita erimallisia työryhmäkytkimiä, jotka on valittu Ciscon tuotemallistosta. Tietoverkkotopologiasta kertoo kuvio 5. Suljettujen potilasmonitorijärjestelmien kytkimet voivat olla muiden valmistajien, koska ne eivät ole kiinni KSSHP:n verkossa. Näihin laitteiston toimittaja on voinut tuoda omat kytkimet.

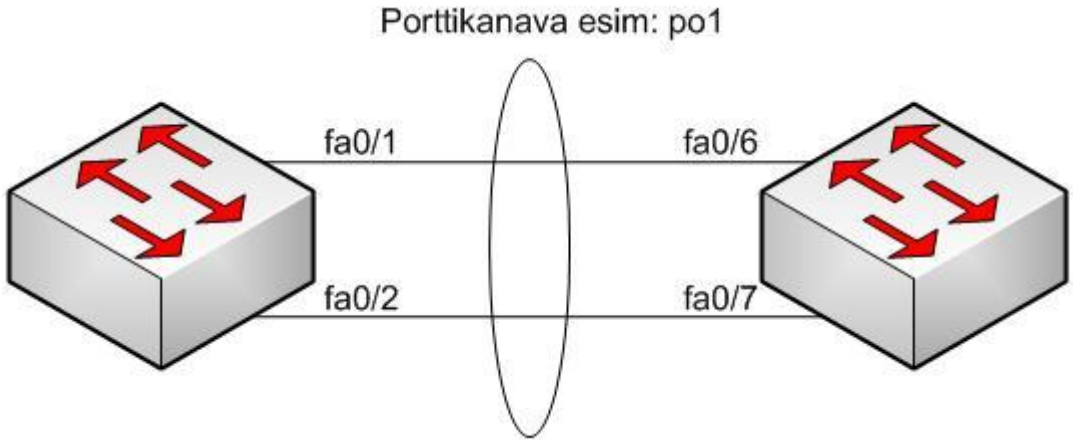



KUVIO 5. Verkkotopologia

## 3.4 Porttikanavat ja spanning tree

KSSHP:n tietoverkossa on käytössä porttikanavat kytkimien välillä. Porttikanavilla saadaan verkkoon redundanttisuutta, koska kytkimien väliset yhteydet ovat kahdennettu. Porttikanavassa kummastakin kytkimestä valitaan kaksi tai useampi portti, jotka ovat konfiguroitu normaalisti trunk-porteiksi. Tämän jälkeen näistä fyysisistä porteista tehdään yksi looginen kanava, jota kutsutaan porttikanavaksi, kuten kuviossa 6. on havainnollistettu.

Tämä tarjoaa vikasietoisen ja tavallista nopeamman linkin kahden laitteen välille. Jos yhden gigabitin portteja yhdistetään kaksi kappaletta, niin yhteysnopeus tulee olemaan kaksi gigabittiä.




KUVIO 6. Porttikanava

Jos toiseen porttikanavan linjaan tulee vikaa, niin potilasmonitoriverkko toimii vielä virheettömästi, koska toinen linja vielä hoitaa kytkimien välisen liikenteen. Huollettavuus on myös etu porttikanavassa, sillä esimerkiksi GBIC:n vaihtaminen onnistuu ilman yhteyden katkeamista.

Jos yhteys on kahdennettu ilman porttikanavaa, niin yhteyden katkeaminen aiheuttaisi Spanning treessa tilamuutoksen ja tulisi Spanning treen uudelleenlaskenta. Tämän uudelleenlaskennan estäminen onkin suurimpia etuja porttikanavan käytössä.

VSS-rungon kytkimien välinen layer 2-tasolla toimiva porttikanava luo runkoon silmukattoman topologian ja tästä johtuen spanning tree on käytössä ainoastaan virhekonfiguraation varalla. (Virtual Switching System 2012)

## 3.5 VLAN ja sen toteutus

KSSHP:ssä on potilasmonitoriverkon VLANit tarkoin rajoitettu niin, että potilasmonitoriverkkoon liittyvät virtuaaliverkot eivät ulotu muualle kuin kytkimiin, missä niillä on käyttöä. Tällä saadaan potilasmonitoriverkkoliikenteen broadcast-liikenne rajoitettua tietyn VLANin sisälle. Tämä vähentää kuormaa tietoliikennekytkimeltä sekä -reitittimeltä. Broadcast domainin pienentäminen auttaa myös rajoittamaan mistäpäin sairaalaa päästään potilasmonitoriverkkoon kiinni sekä vähentämään myös päätelaitteille saapuvien broadcast-kehysten määrää. Kehysten määrän vähentyminen tarkoittaa, että päätelaitteiden ei tarvitse käsitellä niin paljon turhia kehyksiä.

Virtuaaliverkot ovat KSSHP:ssä toteutettu porttikohtaisella konfiguraatiolla. Porttikohtainen VLAN toteutetaan konfiguroimalla kytkimien portteihin oikea VLAN, jonka jälkeen kyseiseen porttiin kytketty päätelaite liittyy kyseiseen VLANiin. Taulukossa 2. on esitetty potilasmonitoriverkon VLANit.

Virtuaaliverkkojen jakamiseen KSSHP:ssa käytetään VTP:tä. VTP on käytössä ainoastaan rungossa ja VTP välittää VLAN konfiguraation muutokset myös muille rungon kytkimille, jotka osallistuvat VTP:hen. Tämä auttaa siinä, että rungon VLAN-muutokset vaikuttavat jokaiseen rungon kytkimeen eli muutosta ei tarvitse tehdä jokaiseen erikseen.

Kuitu- ja työryhmäkytkimille on konfiguroitu transparent mode. Transparent modessa kytkin ei osallistu VTP:hen vaan VLAN-konfiguraatio on kytkinkohtainen. Esimerkiksi kytkimen portille voidaan kertoa käskyllä ”**switchport trunk allowed vlan 2,3**”, että tästä trunk-linjasta menee läpi vain VLANien 2 ja 3 VLAN-informaatio ja tämä mahdollistaa VLANien ulottamisen useamman kytkimen alueelle. Jokaiseen kytkimeen, jonka kautta esimerkiksi VLAN 2 välittyy, pitää olla luotu myös VLAN 2 eli pelkästään trunk-porttien konfigurointi ei riitä. (Software Configuration Guide 2012)

Käskyä ”**switchport trunk allowed vlan”** käyttäessä on erittäin tärkeää muistaa lisätä **add** sana ennen uutta VLAN numeroa. Käsky lisää uuden VLAN-numeron ja säilyttää myös vanhat sallitut VLANit. Jos **add**-sana puuttuu, niin käsky ylikirjoittaa vanhat VLANit. Tämä tarkoittaa, että vain lisätty VLAN toimii tämän trunk-yhteyden yli. (Software Configuration Guide 2012)

TAULUKKO 2. KSSHP:n potilasmonitorijärjestelmän VLANit

| Virtuaaliverkon numero | Virtuaaliverkon nimi |
|---|---|
| VLAN ** | Clinisoft |
| VLAN ** | Potilasmonitorit |
| VLAN ** | Telemetrialähettimet |
| VLAN ** | Datex |
| VLAN ** | teho_GE_MC |
| VLAN ** | teho_GE_monitorit |

## 3.6 DHCP

DHCP on verkkoprotokolla, joka jakaa IP-osoitteita lähiverkossa siihen liittyville laitteille. Lääkintätekniikassa tietoliikenneasiantuntijat ylläpitävät kahta DHCP-palvelinta, jotka jakavat IP-osoitteen oikeasta IP-osoiteryhmästä. Ryhmät ovat DHCP-palvelimella VLAN-kohtaiset. DHCP-palvelin jakaa myös oletusyhdyskäytävän sekä nimipalvelimien IP-osoitteet.

Laitetoimittajat suosittelevat kuitenkin, että potilasmonitoriverkossa käytetään staattisia IP-osoitteita, ja tästä johtuen DHCP ei ole käytössä potilasmonitoriverkossa. Potilasmonitorien telakoissa ei ole edes mahdollista laittaa DHCP:ta toimintaan. Poikkeuksena teho-osaston potilasmonitorijärjestelmä, jolle on varattu DCHP-palvelimelta omat IP-osoitealueet. Teho-osaston potilasmonitorit ovat silti kiinteällä IP-osoitteella toiminnassa, mutta siellä on muutamia IP-osoitteita varattu IP-poolista.

## 3.7 WLAN

KSSHP:ssä on kontrolleripohjainen langaton verkko toiminnassa. Kontrolleripohjaisessa verkossa tukiasemien konfigurointi ja hallinta tehdään keskitetysti. Juuri tämä on merkittävin ero muusta verkosta tietämättömistä tukiasemista rakennettuun lähiverkkoon. Kontrolleripohjainen ratkaisu on varmennettu redundanttisudella eli kontrollerin vikaantuminen ei vaikuta langattomanverkon toimivuuteen.

CAPWAP-protokolla mahdollistaa useamman tukiaseman samanaikaisen hallinnan. Tukiasemia ei tarvitse konfiguroida erikseen vaan tukiasemanohjain hoitaa oikean konfiguraation jakelun tukiasemiin. Myös vianhaku, tukiasemien tarkkailu sekä verkon liikenteen seuranta helpottuvat.

Kontrolleripohjaista WLAN-verkkoa hallitaan kontrollerin käyttöliittymästä tai erillisellä Ciscon Network Control System -ohjelmistolla, joista kumpikin ovat selainkäyttöliittymällä toimivia. KSSHP:llä on käytössä NCS, jonka kautta voidaan hallita ja valvoa kaikkia kontrollereja.

Langaton verkko kattaa koko keskussairaalan tilat ja tästä johtuen potilaita voidaan siirtää sairaalassa eri osastoille ilman, että yhteys keskusvalvontaan katkeaa. Siirron aikana potilaan potilasmonitori tai telemetrialähetin lähettää

tiedot keskusvalvontaan. Osastoilla voidaan potilasmonitori liittää telakkaan ja tämän jälkeen osaston omaan keskusvalvontaan. Potilasmonitoreille ja telemetrialaitteille on luotu omat SSID:t.

Telemetria- ja delta-verkoissa toimivien potilasmonitorilähettimien WLAN-asetusten konfigurointi päätelaiteille selvitetään myöhemmin tässä opinnäytetyössä.

# 4 POTILASMONITORIJÄRJESTELMÄN KEHITTÄMINEN

## 4.1 Potilasmonitorijärjestelmän lähtötilanne

Potilasmonitorijärjestelmät ovat toimineet KSSHP:ssä jo pitkän aikaa. Ensimmäiset potilasmonitorijärjestelmät tulivat käyttöön vuosituhannen alkupuolella ja dokumentaatio on arkistoitu Mequsoftin tietokantaan. Laitteita on kuitenkin vaihtunut ajan saatossa ja jopa osastot ovat vaihtaneet sijaintia. Tästä johtuen dokumentaatio piti käydä läpi. Järjestelmän vikaantuessa on hyvä, että dokumentaatiota on saatavilla järjestelmän eri osien korjauksesta. Samalla järjestelmän kehittäminen tulevaisuudessa helpottuu. Myös potilasmonitorijärjestelmän tietoliikennetarvikkeiden nykytilanne piti käydä läpi ja katsoa onko laitteiston välitön uusiminen tarpeellista.

## 4.2 Dokumentaation luominen

Järjestelmään tutustuminen aloitettiin niin, että kokenut lääkintätekniikan työntekijä esitteli eri osastot, joilla potilasmonitorijärjestelmiä oli käytössä keskussairaalalla. Näiden kierroksien aikana sain pohjatietoa laitteistosta, jota potilasmonitorijärjestelmään kuuluu. Näiden tietojen perusteella etsin lisää tietoa potilasmonitoriverkon laitteista ja dokumentoin löydetyt tiedot Excel-tiedostoon. Pikkuhiljaa tiedoista sain alkua rungolle, johon keräsin lisää tietoa ja lopulta tiedoista alkoi koostua isompi kokonaisuus.

Tarpeellisen informaation keräämiseen käytettiin avuksi kokemusta, joka oli tullut työn kautta. Informaation haussa käytettiin apuna Netdisco-ohjelmaa,

jolla voidaan kerätä eri verkkolaitteista tietoa SNMP-protokollan avulla. Tällä saatiin esimerkiksi listattua tietyn IP-osoite avaruuden kaikki verkossa näkyvät IP-osoitteet. Apuna olivat myös Cisco NCS ja Mequsoft-laitetietokanta. Lääkintätekniikan verkkotopologiakuvista oli myös apua kun selvityksessä.

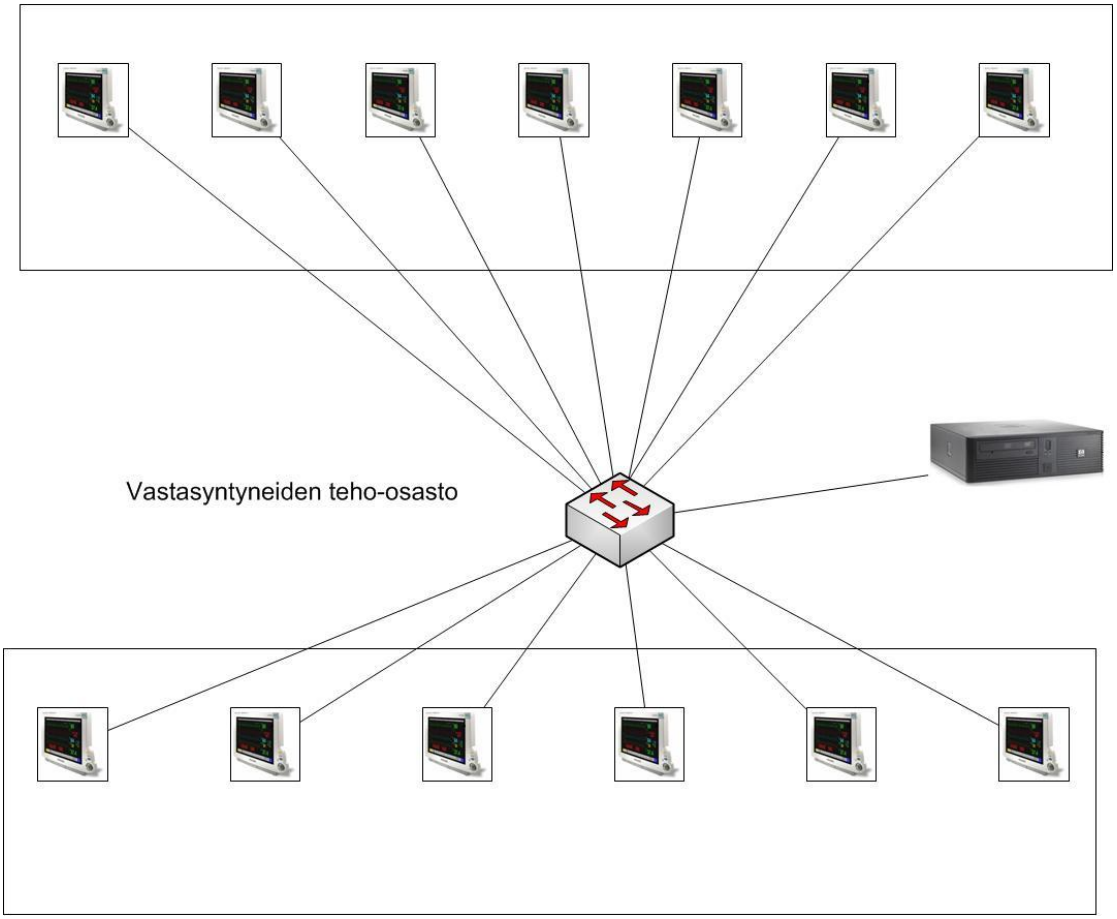
Verkkotopologiat olivat lääkintätekniikassa tallennettuna yhteiseen sähköiseen arkistoon ja tämän lisäksi tulostettu näkyville lääkintätekniikan osastolla. Näistä topologiakuvista ei kuitenkaan vielä nähnyt koko potilasmonitorijärjestelmää ja tästä johtuen nykyisestä potilasmonitoriverkosta piti saada selkeä dokumentaatio tehtyä Visio-ohjelmalla.

Selkeän dokumentaation luomiseen käytin apuna jo valmiiksi sairaanhoitopiirissä olevaa Microsoft VISIO- ohjelmaa. Visio on tarkoitettu 2D-objektikaavioiden esittämiseen ja soveltuu erittäin hyvin tähän käyttöön. Dokumentointikuvien päivittäminen onnistuu useammalta lääkintätekniikan henkilöltä, sillä Visiota oli jo entuudestaan käytetty sairaanhoitopiirin topologiaverkkokuvien tekemiseen. Tästä johtuen kuvien myöhempi päivittäminen onnistuu useammalta henkilöltä. Visiolla saadaan selvemmin esitettyä nykyinen potilasmonitoriverkko ja siihen kuuluvat laitteet. Kun laitteiden tiedot oli kerätty Excel-tiedostoon, tiedot päivittyvät automaattisesti Visio-kuvaan. Dokumentit tulee liittää Mequsoftin laitekorteille, jos dokumentaatio liittyy kyseiseen laitteeseen.

Opinnäytetyön aikana tehtyyn dokumentointiin on tuotettu kuusi eri topologiakuvaa:

- Dräger ICS -keskusvalvontatopologiaverkko
- Leikkausosastojen monitoriverkko
- Päivystysosastojen monitoriverkko
- Lastenosaston monitoriverkko
- Philips-potilasmonitorijärjestelmän topologiakuva
- Datex-potilasmonitorijärjetelmän topologiakuva

Opinnäytetyön aikana lasten teho-osasto muutti uuteen sijaintiin väistötila 2:een ja tämän mukana Philipsin valvontajärjestelmä siirtyi myös uusiin väistötiloihin. Tästä syystä suurin osa tämän järjestelmän dokumentaatiosta ei pitänyt enää paikkaansa ja VISIO- ja Excel -dokumentaatio piti luoda uudestaan. Uusittu vastasyntyneiden teho-osaston topologiakuva on esitetty kuviossa 7.




KUVIO 7. Vastasyntyneiden teho-osaston potilasmonitoriverkkotopologia

ICS-verkkotopologiakuva esittää koko verkkotopologian, johon kuuluu ICS-potilasvalvontakeskuksia. Kuvasta saadaan selville:

- ICS-keskuksen väri, josta selviää laitteen versio
- IP-osoite
- sijainti
- lääkintätekniikan ylläpitämä laitetunnus

- verkkoyhteys tyyppi
- uplink-kytkin.

Liikuteltavista laitteista eli telemetrialähettimistä (M300) sekä potilasmonitoreista saadaan kuvista selville seuraavat tiedot:

- IP-osoite
- MAC-osoite
- sijainti.

Potilasmonitorissa on potilaspaikoilla kiinteä telakka, jossa on verkkokortti. Kun potilasmonitori irrotetaan telakasta, se vaihtaa langattomaan verkkoon ja alkaa käyttää omaa IP-osoitettaan.

VISIO-kuvat käyttävät Excel-tiedostoa tietojen tallentamiseen. Tämä helpottaa kuvien ylläpitoa huomattavasti. Laitteen IP-osoitteen muuttuessa tarvitsee vain päivittää Excel-tiedostoon uusi osoite. Tuotetusta Excel -tiedostosta löytyy myös muita tärkeitä tietoja potilasmonitoriverkosta ja sen laitteista. Kuviossa 8. on malli kuinka exceliin on kerätty eri ICS-keskusvalvontalaitteistojen tietoja.

G23

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Verkkonimi | IP-osoite | L-tunnus | Huone | Malli | Kuvaus | ICS- |
| 2 | ICS 1 | 192.168.11.1 | L20121014 | D1.01.039 | Valk. | ICS | 00:15:17 |
| 3 | ICS 2 | 192.168.11.2 | L20121015 | D1.03.040 | Musta | ICS | 00:04:23 |
| 4 | ICS 3 | 192.168.11.3 | L20121016 | D1.01.041 | Valk. | ICS | 00:15:17 |
| 5 | ICS 4 | 192.168.11.4 | L20121017 | D2.01.042 | Valk. | ICS | 00:15:17 |
| 6 | ICS 5 | 192.168.11.5 | L20121018 | D3.02.043 | Musta | ICS | 00:04:23 |
| 7 | ICS 6 | 192.168.11.6 | L20121019 | D2.01.044 | Valk. | ICS | 00:0e:0c |
| 8 | ICS 7 | 192.168.11.7 | L20121020 | F2.01.045 | Musta | ICS | 00:04:23 |
| 9 | ICS 8 | 192.168.11.8 | L20121021 | F2.01.046 | Musta | ICS | 00:04:23 |
| 10 | ICS 9 | 192.168.11.9 | L20121022 | F2.01.047 | Musta | ICS | 00:04:23 |
| 11 | ICS 10 | 192.168.11.10 | L20121023 | O2.02.048 | Musta | ICS | 00:04:23 |
| 12 | ICS 11 | 192.168.11.11 | L20121024 | O2.02.049 | Musta | ICS | 00:04:23 |
| 13 | ICS 12 | 192.168.11.12 | L20121025 | O1.01.050 | Musta | ICS | 00:04:23 |
| 14 | ICS 13 | 192.168.11.13 | L20121026 | O2.01.051 | Musta | ICS | 00:04:23 |
| 15 | ICS 14 | 192.168.11.14 | L20121027 | N2.03.055 | Valk. | ICS | 001e.67 |
| 16 | HP | 192.168.11.15 | L20121028 | N2.04.056 | | | |
| 17 | ICS 15 | 192.168.11.16 | L20121029 | N2.02.057 | Valk. | ICS | |

KUVIO 8. Esimerkki Excelin rakenteesta

Kyseisessä tiedostossa on 5 välilehtitaulukkoa:

ICS:stä on seuraavat tiedot:

- verkkonimi
- IP-osoite
- L-tunnus
- huone
- osasto
- valmistaja
- malli
- kuvaus
- MAC-osoite
- missä tietoliikennekytkimessä kiinni
- missä tietoliikennekytkimen portissa on kiinni
- missä tietoliikennekytkin sijaitsee.

Kytkimistä on myös pitkä lista eri tietoja:

- verkkonimi
- IP-osoite
- L-tunnus
- sarjanumero
- sijainti
- valmistaja
- malli
- ohjelmistoversio
- tuotteen kuvaus
- aliverkkopeite
- ylläpitoliittymä
- porttimäärä
- uplink-portti
- uplink-kytkin
- käyttöönottovuosi

- takuuta jäljellä
- laitteistotuki loppuu
- ohjelmistotuki loppuu
- korvaava laite
- porttitilanne
- porttikanavat
- käyttötarkoitus.

Potilasmonitoreista sekä muista potilasmonitoriverkon laitteista on dokumentoitu:

- IP-osoite
- sijainti
- MAC-osoite
- missä tietoliikennekytkimessä laite on kiinni.

Telemetriasta on dokumentoitu seuraavat tiedot:

- IP-osoite
- sijainti
- MAC-osoite.

Dokumentaatiosta on suuri apu järjestelmän IP-osoitteiden hallinnan parantamisessa. Ongelmaahan ei olisi jos käytössä olisi DHCP-palvelu, mutta koska tämä ei ole mahdollista, vapaa IP-osoite uudelle laitteelle on selvitettävä itse. Aikaisemmin ei ole ollut mahdollista tukeutua dokumentaatioon ja katsoa Excel-tiedostosta suoraan tämän hetkisiä laitteita ja niille määriteltyjä IP-osoitteita.

## 4.3 Porttitilanne

Lääkintätekniikassa kytkimen kapasiteettisuunnittelussa on ollut tavoite, että uuden kytkimen asennuksen jälkeen kytkimissä on aina riittävä määrä vapai-

ta portteja. Vapaiden porttien riittäväksi määräksi on todettu noin kolmasosa kytkimen kokonaisporttimäärästä.

Jos todetaan, että kytkin on liian täynnä, tilanne on ratkaistavissa muutamalla eri tavalla. Ristikytkennän porttimäärää voidaan laajentaa asentamalla ristikytkentään uusi kytkin erillisenä kytkimenä tai liittämällä uusi kytkin stack-moduulin avulla olemassa olevaan kytkimeen. On myös mahdollista, että 24-porttisen kytkimen tilalle vaihdetaan 48-porttinen kytkin.

## 4.4 End-of-Sale ja End-of-Life

Koska Keski-Suomen sairaanhoitopiirin verkkoinfrastruktuuri on toteutettu Ciscon laitekannalla, Ciscon End-of-Sale ja End-of-Life -tiedotteet ovat hyvinkin tärkeitä verkon ylläpidolle. EOS tarkoittaa että kyseinen ilmoitettu päivämäärä on viimeinen myyntipäivä kyseiselle tuotteelle Ciscon myyntipisteistä. Pääsääntöisesti Cisco tarjoaa kuuden kuukauden ennakkoilmoituksen tuotteista, joihin EOS vaikuttaa. Cisco.com -nettisivuston ja tiedotuspalvelun (notification service) kautta on mahdollista saada tieto uudesta EOS- ja EOL-ilmoituksista sähköpostiin.

Cisco's Technical Assistance Center on käytettävissä 24 tuntia vuorokaudessa jokaisena viikonpäivänä viiden vuoden ajan EOS-päivästä laitteiston Cisco IOS -ongelmissa ja kolme vuotta laitteiston sovellusongelmissa. Varaosia EOS-ilmoituksen laitteille on saatavilla Ciscon tukemana viisi vuotta. Ohjelmistoon voidaan ensimmäisen vuoden aikana tehdä ohjelmistovirhekorjauksia, huoltojulkaisuja ja päivityksiä, jotka ovat tulleet Ciscon tietoon TAC:n tai cisco.com -verkkosivun kautta. Myös seuraavat neljä vuotta edellä olleet asiat voidaan korjata käyttöjärjestelmästä ja kaksi vuotta jos kyseessä on ohjelmisto, mutta on mahdollista, että kyseisen ongelman ratkaisu vaatii isomman ohjelmistopäivityksen kytkimelle. (End-of-Life Policy,2012)

Seuraaville potilasmonitoriverkon laitteille Cisco on ilmoittanut EOS- ja EOL-päivän ja sekä korvaavan tuotteen. Kytkimiä on kymmenen kappaletta, joihin EOS ja EOL vaikuttaa.

TAULUKKO 3. Korvaavat tuotteet

| **Tuote:** WS-C3750G-12S | **Korvaava:** WS-C3750X-12S-E | Määrä: 6 kpl | Päivämäärä: |
|---|---|---|---|
| End-of-Life Announcement Date | | | 31.1.2012 |
| End-of-Sale Date | | | 30.01.2013 |
| Last Ship Date: HW | | | 30.04.2013 |
| End of SW Maintenance Releases Date: HW | | | 30.01.2014 |
| End of Routine Failure Analysis Date: HW | | | 30.01.2014 |
| End of New Service Attachment Date: HW | | | 30.01.2014 |
| End of Vulnerability/ Security Support: OS SW | | | 30.01.2016 |
| End of Service Contract Renewal Date: HW | | | 30.04.2017 |
| Last Date of Support: HW | | | 31.01.2018 |

| **Tuote:** WS-C2960G-48TC-L | **Korvaava:** WS-C2960S-48TS-L | Määrä: 3 kpl | Päivämäärä: |
|---|---|---|---|
| End-of-Life Announcement Date | | | 01.08.2011 |
| End-of-Sale Date | | | 31.07.2012 |
| Last Ship Date: HW | | | 29.10.2012 |
| End of SW Maintenance Releases Date: HW | | | 31.07.2015 |
| End of Routine Failure Analysis Date: HW | | | 31.07.2013 |
| End of New Service Attachment Date: HW | | | 31.07.2013 |
| End of Service Contract Renewal Date: HW | | | 29.10.2016 |
| Last Date of Support: HW | | | 31.07.2017 |
| End-of-Life Announcement Date | | | 01.08.2011 |

| **Tuote:** WS-C3560-24PS-S | **Korvaava:** WS-C3560V2-24PS-S | Määrä: 1 kpl | Päivämäärä: |
|---|---|---|---|
| End-of-Life Announcement Date | | | 4.1.2010 |
| End-of-Sale Date | | | 5.7.2010 |
| Last Ship Date: HW | | | 3.10.2010 |
| End of SW Maintenance Releases Date: HW | | | 4.7.2013 |
| End of Routine Failure Analysis Date: HW | | | 5.7.2011 |
| End of New Service Attachment Date: HW | | | 5.7.2011 |
| End of Service Contract Renewal Date: HW | | | 30.9.2014 |
| Last Date of Support: HW | | | 31.7.2015 |
| End-of-Life Announcement Date | | | 4.1.2010 |

Taulukossa 3. olevat tietoliikennekytkimien mallit on dokumentoitu ja tiedostettu, että lähitulevaisuudessa kytkimien päivittäminen tulee ajankohtaiseksi. EOS-tiedote vaikuttaa myös seuraavien kytkin mallien tilaamiseen, koska nyt ei kannata tilata poistuvaa mallia. (Warranty Terms 2012)

## 4.5 Takuu

Laitteistolle Cisco tarjoaa rajoitetun elinkaaritakuun. Tämä tarkoittaa että laitteella on takuu niin kauan kuin alkuperäinen ostaja omistaa tuotteen, pois luettuna tuulettimet ja virtalähde. Näillä kahdella osalla on rajoitettu takuu viiteen vuoteen. Cisco lähettää korvaavan tuotteen normaalisti kymmenen arkipäivän aikana siitä hetkestä kun he ovat saaneet RMA-pyynnön.

Tällä hetkellä potilasmonitoriverkossa on 20 kytkintä ilman takuuta. Takuun puuttuminen ei sinänsä ole ongelma, koska korvaavia laitteita on saatavilla ja kytkimen vikaantuessa on mahdollista viedä tilalle uudemman mallin kytkin. Nykyisillä ostosopimuksilla saadaan uusi laite jo seuraavaksi päiväksi paikalle. Kriittisiin kohteisiin voidaan kuitenkin laiterikkoon reagoida tarvittaessa heti, koska lääkintätekniikassa on aina jotain Ciscon kytkinmallia varalla.

## 4.6 Dynaamisen VLANin käyttöönotto ja autentikointi

IEEE 802.1X porttikohtainen autentikointi on standardi, jota käytetään langallisessa ja langattomassa lähiverkossa ja tämän tarkoitus on autentikoida päätelaite, joka kytketään tietoverkkoon. Mahdollisia autentikointitapoja on useita erilaisia.

802.1X:n avulla voidaan verkossa ottaa käyttöön dynaaminen VLAN. Dynaamista virtuaaliverkkoa ei vielä ole laajamittaisesti käytetty KSSHP:ssä, mutta tavoite on että ensi vuonna dynaaminen VLAN tulee ulottumaan suureen osaan KSSHP:n tietoverkkoa.

Dynaamisessa virtuaaliverkossa tietoliikennekytkimen portti voi olla oletuksena esimerkiksi vierailijaverkon VLANissa, josta ei päästä sairaalan tietojärjestelmiin. Kun laite kytketään kytkimen porttiin, kytkin autentikoi laitteen RADIUS-protokollan avulla RADIUS-palvelimen kanssa. Autentikoinnin aikana tulee kytkimelle tieto siitä mihin virtuaaliverkkoon laitteen pitää kuulua ja kytkimen portti konfiguroituu dynaamisesti oikeaan virtuaaliverkkoon.

Hyötyä tästä on se, että laitteita voidaan siirtää helpommin ja kytkimien portteja ei tarvitse enää konfiguroida joka kerta, kun laitetta siirretään rasiasta toiseen. Dynaamisen VLANin ansiosta myös vikaantuneen kytkimen kaapelointi voidaan siirtää samassa ristikytkennässä olevien kytkimien vapaisiin portteihin.

Myös tietoturvallisuuteen tulee parannusta, koska porttiin liitetty tuntematon laite tulee aina autentikoida ennen kuin sille annetaan mitään palveluita, mitä kytkimen kautta on mahdollista saada. On myös mahdollista, että autentikoimaton laite laitetaan vierailijaverkon VLANiin vakiona.

Joskus järjestelmään voidaan yrittää murtautua väärentämällä MAC-osoite jostain tunnetusta laitteesta. Jos otetaan käyttöön dynaamiset access-listat, niin tämän jälkeen tunkeutuja pääsee kyllä liittymään verkkoon, mutta säännöt voivat määritellä että tietyn VLANin laitteille on auki vain esimerkiksi juuri Dräger-potilasmonitoriverkon portit, jotka on kuvattu aiemmin taulukossa. 2. Tämä estää tehokkaasti tunkeutujan pääsyn muihin järjestelmiin.

KSSHP:n tietoverkossa on käytössä 802.1x/ MAB open mode -autentikointi eli kun päätelaite kytketään kiinni porttiin niin päätelaite yrittää autentikoida RADIUS-palvelimen kanssa. MAB:ia käytettäessä laitteen tunnistukseen käy-

tetään laitteen MAC-osoitetta. Tämä toimii myös laitteissa joissa ei ole mahdollista käyttää varsinaista 802.1x autentikointia. Tällaisia laitteita on sairaalalla esimerkiksi osa lääkintälaitteista, IP-puhelimet sekä printterit. MAB:n käyttö vaatii tietokannan, jossa on MAC-osoitteet ja niille annetut oikeudet. Tätä tietokantaa ylläpitää tällä hetkellä lääkintätekniikan tietoliikenneasiantuntijat.

Open mode tarkoittaa että käytössä ei ole vielä rajoituksia, mutta onnistuneet ja epäonnistuneet todennukset jäävät ACS-palvelimelle talteen. Tällä saadaan arvokasta tietoa nykyisen verkon autentikointien määrästä ja siitä, kuinka päätelaiteet autentikoituvat oikein.

Tällä hetkellä lääkintätekniikassa ja leikkausosasto 3:n leikkaussaleissa on otettu käyttöön dynaaminen VLAN. Näillä osilla dynaamisen verkon toimintaa seurataan. Leikkaussaleissa on salikohtaiset työryhmäkytkimet. Salikohtaisilla kytkimillä saadaan koekäytön laajuutta rajattua tarkasti tietylle alueelle. Käytännössä on jo havaittu, että dynaamisen portin käyttöönotto ei tapahdu ilman ongelmia, joita pitää selvittää. Koekäytössä on havaittu, että erään lääkintälaitteen autentikointi ei satunnaisesti onnistu sillä laite ei ilmoita MAC-osoitetta kytkimelle. Kyseinen laite on erittäin vanha ja koska vika ei ilmene joka kerta kun laitetta käytetään, kyseistä vikaa on vaikea alkaa selvittelemään.

KSSHP:n tietoverkossa kiinni olevat potilasmonitorit ja telakat eivät tue 802.1x standardia, joten ne myös joudutaan autentikoimaan MAB:n avulla. Tämä on testattu testiympäristössä lääkintätekniikassa ja ACS:ssä on nyt valmis profiili potilasmonitorien VLANeille. Testissä kytkimen portti oli konfiguroitu liitteen 11 mukaan ja tarvittavat ACS-konfiguraatiot oli lisätty. Kun potilasmonitorin kytki porttiin niin potilasmonitori autentikoi oikein ja muutti portin oikeaan virtuaaliverkkoon. Tämän jälkeen potilasmonitorista oli yhteys samassa virtuaaliverkossa kiinni olevaan keskukseen. Autentikointi varmistettiin ACS:n logeista ennen konfigurointia ja konfiguroinnin jälkeen.

Ohjeistus Cisco Secure ACS:n käytöstä ja kytkimen portin konfiguraatiosta on liitteessä 11. Dynaamisen VLANin ohjeistus.

# 5 POTILASMONITORIJÄRJESTELMÄN YLLÄPITO

## 5.1 Potilasmonitorijärjestelmän palautumissuunnitelma

Seuraavaksi käydään läpi eri asioita mitkä ovat oleellisia potilasmonitorijärjestelmän toiminnan kannalta. On hyvä, että lääkintätekniikasta löytyy ohjeistusta eri tilanteisiin, jotka vaikuttavat potilasmonitorijärjestelmän toimintaan ja auttavat järjestelmän toiminnan palauttamisessa. Palautumissuunnitelma on toteutettu tietoliikennenäkökulmasta, joten tässä ei oteta kantaa itse potilasmonitorilaitteiden huoltamiseen.

Järjestelmän toiminnan kannalta oleelliset asiat tulevat olla läpikäyty ja ohjeistettu niin, että korjaustoimet olisivat vikatilanteessa mahdollisimman tehokasta.

Seuraavat asiat on otettu huomioon:

1. Kuinka toimitaan tietoliikennekytkimen vikaantuessa. ks. luku 5.2
2. Dräger ICS-potilasmonitorikeskuksen palautus ja konfigurointi. Liite 2
3. Dräger Potilasmonitorin konfigurointi, tärkeää uuden tuotteen paikalleen viemisen takia ja vianselvityksessä. Liite 3
4. Dräger Telemetrialähettimen konfigurointi, tärkeää uuden tuotteen paikalleen viemisen takia ja vianselvityksessä. Liite 4
5. Kuinka toimitaan laajemman verkkovian sattuessa että potilasmonitorijärjestelmän toiminta jatkuu. Liite 12

## 5.2 Tietoliikennekytkimen vaihtaminen

Nykyisistä tietoliikennekytkimistä löytyy konfiguraation varmuuskopio NetworkAuthority Inventorysta, joka sijaitsee lääkintätekniikan verkonvalvontapalvelimella. Inventoryssä on jokaisen tietoliikennekytkimen backup-konfiguraatio tallessa. Sieltä voidaan hakea esimerkiksi rikki menneen kytkimen startup-konfiguraatio josta kytkin lataa käynnistyessä konfiguraation. Backup-konfiguraatio voidaan siirtää suoraan uudelle laitteelle, kun korvaava kytkin asennetaan. Tässäkin tapauksessa on hyvä käydä läpi konfiguraatio ennen laitteen viemistä toimipisteelle. Toimipisteellä voidaan rikki menneestä kytkimestä siirtää kaapelit suoraan korvaavaan kytkimen vastaavaan porttiin.

KSSHP:n tietoverkosta löytyy pohjakonfiguraatiot eri kytkinmalleille korvaavan laitteen konfigurointia varten. Tämän pohjakonfiguraation päälle tulee vielä erikseen konfiguroida porttikohtaiset VLAN-asetukset, koska vakiona portit konfiguroidaan ennalta määriteltyyn virtuaalilaniin, esimerkiksi vierailijaverkkoon. Tämän lisäksi kytkimen nimi, kytkimen hallinta IP, oletus yhdyskäytävä sekä tieto kytkimen sijainnista pitää vaihtaa oikeaksi. Kaikki nämä löytyvät backup-konfiguraatiosta.

Aikaisemmin vuonna 2012 tietoliikennekytkimet päivitettiin uudempaan ja ennen kaikkea tärkeimpänä samaan ohjelmistoversioon.
Saman ohjelmistoversion etuja ovat yhteensopivuus laitteiden välillä, kytkinten ominaisuudet ja käskyjen rakenteet pysyvät samana.

Dynaamisen VLANin käyttöönotto tulee helpottamaan uuden tietoliikennekytkimen vaihtamista. Portteja ei tarvitse tämän jälkeen enää konfiguroida tietyille virtuaaliverkoille ja korvaavaan kytkimeen ei tarvitse enää laittaa rikkimenneen kytkimen kaapeleita vastaavaan porttiin.

## 5.3 Ristikytkentäkaappien siivous

Ristikytkennässä lähtökohtana on hyvä pitää, että nykyisien kytkimien rikkoutuessa uusi kytkin on helppo vaihtaa eikä kaapeleita tarvitse turhaan irrottaa. Tällä hetkellä tilanne ei ole näin vaan useissa kohteissa on tarvetta uudelleenjärjestelemiselle. Tätä ei kuitenkaan voida toteuttaa nopeasti koska osastoilla on ympärivuorokautista toimintaa ja kaapin siivouksessa joudutaan irrottamaan kaapeleita. Kesällä toteutettiin yhden kaapin täydellinen uudelleenjärjestely ja se onnistui hyvin, koska kyseisen osaston henkilökunta oli kesätauolla. Lääkintätekniikkaan on hankittu tarpeelliset kiinnitysraudat ja kaapeliohjurit, jotta mahdollisuuden tullen ristikytkennän siistiminen on mahdollista. NetworkAuthority Inventoryssä on myös mahdollisuus vanhan ja uuden konfiguroinnin vertailuun. Kytkimen asennuksen jälkeen voidaan vaikka verrata, että kaikki käskyt ovat menneet perille ja konfiguraatio näyttää samalta kuin vanha.

Ristikytkentäkaappeja on sijoitettu ympäri KSSHP:ta ja Excel-dokumentaatiosta löytyy osasto ja huone, joissa potilasmonitoriverkon tietoliikenneristikytkentäkaapit sijaitsevat. Leikkaussaleissa on salikohtaisia tietoliikennekytkimiä, jotka ovat yleensä 24-porttisia Ciscon tietoliikennekytkimiä.

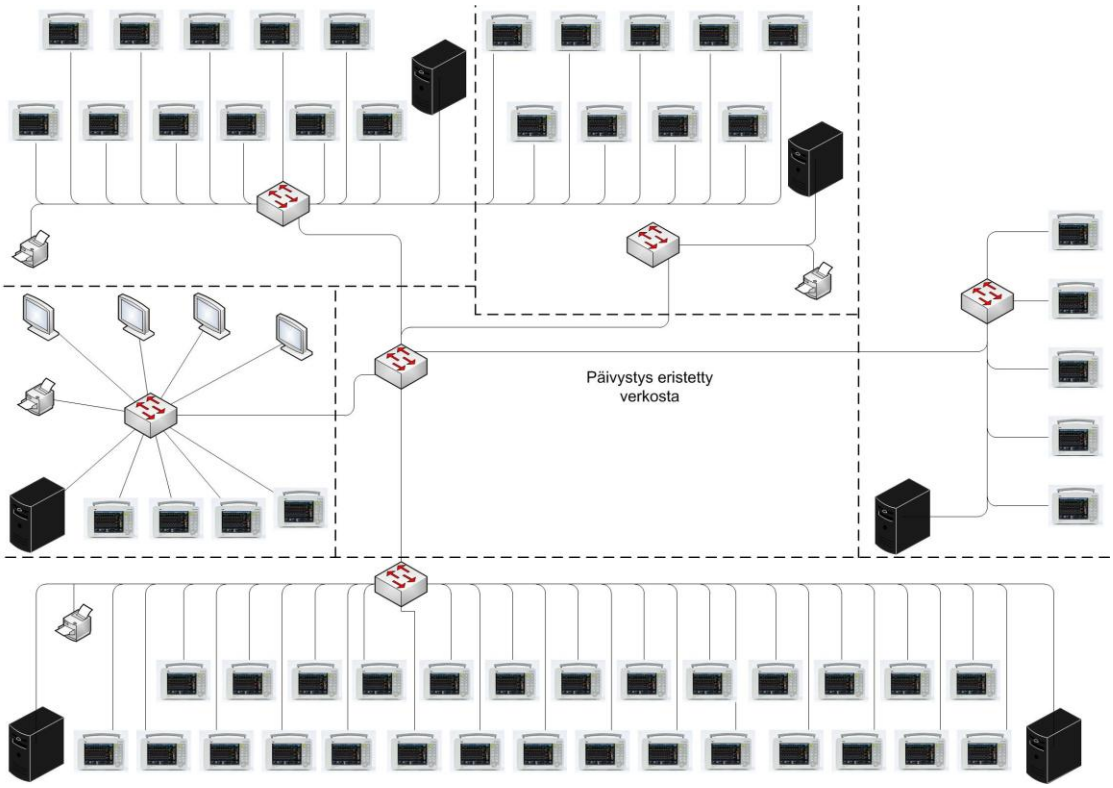
Kytkimet tulisi olla selkeästi merkitty virheiden minimoimiseksi. Kytkimiin tulee merkitä selkeälle paikalle Mequsoftin laitetunnus ja kytkimen nimi, esimerkiksi ksshp-c2960G-48-Koulu1-sw. Tästä johtuen ristikytkentäkaapit täytyy käydä läpi ja katsoa, että merkinnät ovat oikein ja johdot menevät järkevästi. Sivuille voidaan lisätä ohjausrautoja, jos niistä on hyötyä. On myös hyvä huolehtia, että tietoliikennekaapeissa on tarpeeksi vapaita sähköverkkorasioita.

## 5.4 Potilasmonitoriverkon eristäminen

Potilasmonitoriverkko on oltava mahdollista eristää niiltä osin, missä toiminta on kriittistä ympäri vuorokauden. Eristäminen tulee onnistua, kun KSSHP:n verkossa on liikennettä, joka vaikuttaa potilasmonitoriverkon toimintaan negatiivisesti. Mahdollisia eristystapoja on kaksi, fyysinen eristäminen tai kytkimen kuitulinkin sammuttaminen. Lääkintätekniikan tietoverkkoasiantuntijat voivat toteuttaa kytkimeltä kuitulinkin sammuttamisen, jos verkon toiminta sen vielä mahdollistaa. Monitoriverkon kuitukytkimen fyysinen eristys KSSHP:n verkosta voidaan toteuttaa VSS-runkoon menevien kuitukaapeleiden irrottamisella joko konesalista tai päivystysosastolla.

Eristetty alue on esitetty kuviossa 9. ja siihen kuuluvat seuraavat ICS:ät:

- Päivystyspoliklinikan huoneessa ** oleva ICS ja siinä olevat potilasmonitorit sekä tulostin.
- Päivystyspoliklinikan ICS, potilasmonitorit sekä tulostin.
- Toisessa kerroksessa sijaitsevan päivystys- ja infektio-osaston ICS:ät, potilasmonitorit sekä tulostin.
- Yöpäivystyksen ICS, potilasmonitorit ja tulostin.
- Triage / Shokkihoitohuoneen ICS, medical PC:t, potilasmonitorit sekä tulostin.




KUVIO 9. Eristetyn päivystysosaston potilasmonitoriverkkotopologia

Fyysinen eristys on toteutettu merkitsemällä päivystysosastolta potilasmonitoriverkon kuitukytkimeltä runkoon päin lähtevät kuitukaapelit. Konesalissa on merkitty tarralla päivystysosaston kuitukaapeleiden toinen pää eli irrottaminen onnistuu kummastakin päästä. Tarrassa lukee punaisella ”Potilasvalvontaverkko”. Ristikytkennässä on myös ohjeistus (liite 12.) tulostettuna.

## 5.5 ICS-potilasmonitorikeskuksen palautumissuunnitelma

### 5.5.1 Yleistä

Kun käytössä oleva ICS hajoaa toimipaikassa, se pitää tuoda lääkintätekniikkaan korjattavaksi. Lääkintätekniikassa henkilökunta ottaa selvää vian laadusta ja vakavuudesta.

Lääkintätekniikassa on varalla kumpaankin ICS-malliin varakovalevyt sekä imaget. Jos vika vaatii aikaa enemmän, eikä sitä ei voida heti korjata, viedään tilalle vara-ICS, joka on varalla lääkintätekniikassa. Liite 1 kertoo miten vara-ICS otetaan käyttöön.

### 5.5.2 ICS:n varaosat

ICS:n sisällä on kaksi kovalevyä. Mustassa ja valkoisessa ICS:ssä on erilaiset kovalevyt. Mustassa on Fujitsu MBA3073NC 73.5GB 15000 RPM 8MB Cache SCSI Ultra320 80pin 3.5". Kovalevyn liitäntä on rinnakkain kytketty SCSI Ultra 320 eli siirtonopeus on 320Mt/ s ja kovalevyn liittimessä on 80 pinniä. Kovalevyn väylän leveys on 16 bittiä. (Onemed, 05/ 2012)

Valkoisessa on Seagate® Constellation® ES SAS 6Gb/ s 500-GB Hard Drive, ST500NM0001 6-Gb/ s SAS 500GB 64MB. Kovalevyn liitäntä on SAS eli sarjankytketty SCSI. Kyseessä on tietokoneväylä, jota käytetään pääasiassa palvelinympäristöissä kiintolevyjen liittämiseksi järjestelmään. Väylännopeus on 375 Mt/ s. (Onemed, 05/ 2012)

Varmuuskopion tallennuspaikaksi on valittu USB kovalevy Lacie Rikiki 1000Gb USB3.0.

Kovalevyn tarkistaminen ja vaihtaminen:

1. Tuo ICS toimipisteeltä lääkintätekniikkaan.
2. Ensiksi aja PC-test -ohjelmistosta system stress test jolla voidaan testata järjestelmän eri osia kuten kovalevy, muistit.
3. Tämän jälkeen on kaksi eri vaihtoehtoa, joko Maxtor tai Seatools CD-levyt. Nämä levyt löytyvät lääkintätekniikasta.
4. Käynnistä ICS valitulta CD levyltä ja tarkista kovalevy.
5. Sammuta tietokone ja poista rikkinäinen kovalevy.

6. Uudelle kovalevylle voidaan palauttaa tiedostojärjestelmä Clonezillan varmuuskopiosta, joka sijaitsee Lacien Rikiki USB-kovalevyllä.

Lääkintätekniikkaan on hankittu varakovalevyjä neljä kappaletta kumpaankin ICS-malliin.

Virtalähde on FSP460-60PFN (460W) ja vastaavaa on myös saatavissa lyhyellä toimitusajalla paikallisista ATK-liikkeistä.

TAULUKKO 4. Varaosalista

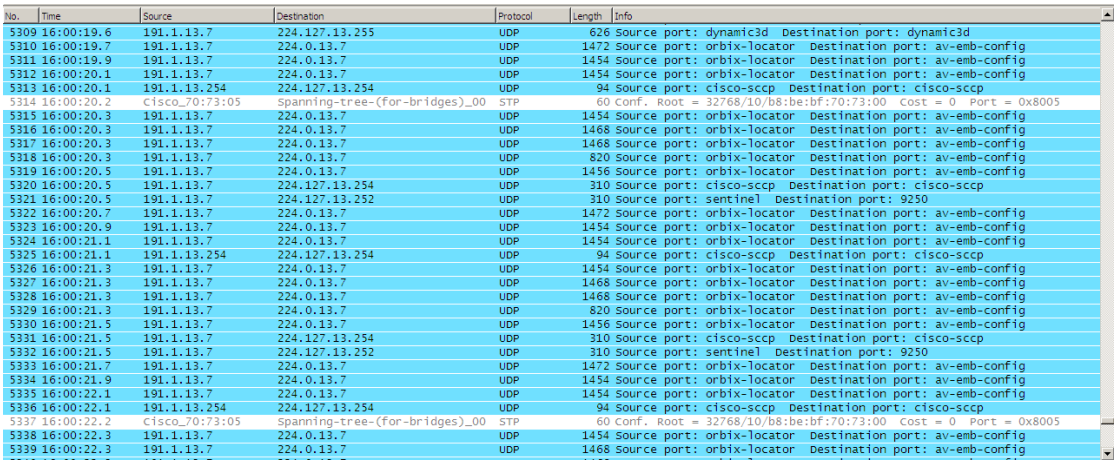
| **Drägerin varaosanumero** | **Varaosan nimi** |
|---|---|
| MS18842E581U | Etupuolella oleva tuuletin |
| MS18834E581U | DVD-Asema |
| MS18835E581U | Sisällä oleva tuuletin |
| MS18833E581U | Diskettiasema |
| MS18832E581U | Kovalevy |
| MS18829E581U | Äänikortti |
| MS18836E581U | Kaiutin |
| MS18830E581U | Näytönohjain |
| MS18837E581U | Kotelon vara-avaimet |
| MS18839E581U | 512MB SDRAM muisti |
| MS18831E581U | ATX virtalähde |
| MS16978E581U | Emolevyn patteri, 12V 21W IPS |

### 5.5.3 Potilasmonitoriverkon liikenteen tutkiminen

Kaappaamalla liikennettä potilasmonitoriverkosta voidaan syvemmin tutustua potilasmonitoriverkon liikenteeseen vikatilanteessa, esimerkiksi jos ICS ei

näe jotain verkossa olevaa potilasmonitoria ja sen pitäisi konfiguraation puolesta olla toiminnassa. Tästä johtuen opinnäytteen aikana on tutustuttu normaaliin potilasmonitoriverkon liikenteeseen jotta vikatilanteissa osataan tunnistaa epänormaali liikenne.

Liikennettä voidaan tutkia Ciscon kytkimen monitor-ominaisuuden avulla. Käskyllä **monitor session 1 source interface fastEthernet 0/2** valitaan interface 0/ 2 liikenne replikoitumaan. Tämän jälkeen käskyllä **monitor session 1 destination interface fastEthernet 0/1** voidaan merkata portti 0/ 1 vastaanottamaan 0/ 2:n replikoituvaa dataa. Tämän jälkeen portista 0/ 1 voidaan kaapata dataa esimerkiksi Wiresharkin avulla kuten kuviossa 10 on tehty.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5309 | 16:00:19.6 | 191.1.13.7 | 224.127.13.255 | UDP | 626 | Source port: dynamic3d Destination port: dynamic3d |
| 5310 | 16:00:19.7 | 191.1.13.7 | 224.0.13.7 | UDP | 1472 | Source port: orbix-locator Destination port: av-emb-config |
| 5311 | 16:00:19.9 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5312 | 16:00:20.1 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5313 | 16:00:20.1 | 191.1.13.254 | 224.127.13.254 | UDP | 94 | Source port: cisco-sccp Destination port: cisco-sccp |
| 5314 | 16:00:20.2 | Cisco_70:73:05 | Spanning-tree-(for-bridges)_00 | STP | 60 | Conf. Root = 32768/10/b8:be:bf:70:73:00 Cost = 0 Port = 0x8005 |
| 5315 | 16:00:20.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5316 | 16:00:20.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1468 | Source port: orbix-locator Destination port: av-emb-config |
| 5317 | 16:00:20.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1468 | Source port: orbix-locator Destination port: av-emb-config |
| 5318 | 16:00:20.3 | 191.1.13.7 | 224.0.13.7 | UDP | 820 | Source port: orbix-locator Destination port: av-emb-config |
| 5319 | 16:00:20.5 | 191.1.13.7 | 224.0.13.7 | UDP | 1456 | Source port: orbix-locator Destination port: av-emb-config |
| 5320 | 16:00:20.5 | 191.1.13.7 | 224.127.13.254 | UDP | 310 | Source port: cisco-sccp Destination port: cisco-sccp |
| 5321 | 16:00:20.5 | 191.1.13.7 | 224.127.13.252 | UDP | 310 | Source port: sentinel Destination port: 9250 |
| 5322 | 16:00:20.7 | 191.1.13.7 | 224.0.13.7 | UDP | 1472 | Source port: orbix-locator Destination port: av-emb-config |
| 5323 | 16:00:20.9 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5324 | 16:00:21.1 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5325 | 16:00:21.1 | 191.1.13.254 | 224.127.13.254 | UDP | 94 | Source port: cisco-sccp Destination port: cisco-sccp |
| 5326 | 16:00:21.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5327 | 16:00:21.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1468 | Source port: orbix-locator Destination port: av-emb-config |
| 5328 | 16:00:21.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1468 | Source port: orbix-locator Destination port: av-emb-config |
| 5329 | 16:00:21.3 | 191.1.13.7 | 224.0.13.7 | UDP | 820 | Source port: orbix-locator Destination port: av-emb-config |
| 5330 | 16:00:21.5 | 191.1.13.7 | 224.0.13.7 | UDP | 1456 | Source port: orbix-locator Destination port: av-emb-config |
| 5331 | 16:00:21.5 | 191.1.13.7 | 224.127.13.254 | UDP | 310 | Source port: cisco-sccp Destination port: cisco-sccp |
| 5332 | 16:00:21.5 | 191.1.13.7 | 224.127.13.252 | UDP | 310 | Source port: sentinel Destination port: 9250 |
| 5333 | 16:00:21.7 | 191.1.13.7 | 224.0.13.7 | UDP | 1472 | Source port: orbix-locator Destination port: av-emb-config |
| 5334 | 16:00:21.9 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5335 | 16:00:22.1 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5336 | 16:00:22.1 | 191.1.13.254 | 224.127.13.254 | UDP | 94 | Source port: cisco-sccp Destination port: cisco-sccp |
| 5337 | 16:00:22.2 | Cisco_70:73:05 | Spanning-tree-(for-bridges)_00 | STP | 60 | Conf. Root = 32768/10/b8:be:bf:70:73:00 Cost = 0 Port = 0x8005 |
| 5338 | 16:00:22.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1454 | Source port: orbix-locator Destination port: av-emb-config |
| 5339 | 16:00:22.3 | 191.1.13.7 | 224.0.13.7 | UDP | 1468 | Source port: orbix-locator Destination port: av-emb-config |

KUVIO 10. Wireshark

# 6 YHTEENVETO

Opinnäytetyön käynnistyminen oli hankala, koska tietoa potilasmonitorijärjestelmästä oli heikosti saatavilla dokumentaation muodossa ja aihe ei ollut ennestään tuttu. Olin kuitenkin työskennellessä KSSHP:n lääkintätekniikassa saanut paljon kokemusta eri asioista, mikä auttoi potilasmonitoriverkon rakenteen jäljittämisen ja kuvien piirtämiseen. Kuviin liittyvän Excel-tiedoston kasaamiseen meni mielestäni huomattavan paljon aikaa.

Sain opinnäytetyön aikana erittäin hyvin selville nykyisen potilasmonitorijärjestelmän rakenteen ja tiedän nykyään hyvin eri asioita potilasmonitoriverkosta, vaikka potilasmonitorijärjestelmiä on useita ja niihin liittyy useita eri alueita. Pidin kuitenkin opinnäytetyön tietoliikennepainotteisena ja karsin asioita, jotka eivät liittyneet mielestäni hyvin opinnäytetyön aiheeseen. Olen itse tyytyväinen opinnäytetyön aikaan saamaan dokumentaatioon. Mielestäni tästä on hyvä lähteä nyt ylläpitämään pysyvää hyvää dokumentaatiota ja kehittämään potilasmonitorijärjestelmää paremmaksi.

Tietoliikenteen osalta palautumissuunnitelma saatiin kattamaan useita tärkeitä ja ennen hieman ohuella pohjalla olleita kohteita ja tämän opinnäytetyöni on tuonut helpotusta potilasmonitorijärjestelmien ylläpitoon.
Myös opinnäytetyöni aikana luotu dokumentaatio ICS-järjestelmän palautuksesta on jo osoittautunut toimivaksi oikean vikatilanteen selvittämisessä.

# LÄHTEET

Infinity Delta. Dräger Medical Systems Inc. 12/ 2010, käyttöohjeet

Patient Monitoring. GE Healtcare www-sivut. Viitattu 11.09.2012
http:/ / www3.gehealthcare.com/ en/ Products/ Categories/ Patient_Monitoring#

Onemed. Dräger Infinity potilasvalvonta koulutusmateriaali. 05/ 2012

Infinity Central Station. Dräger Medical Systems Inc. 05/ 2008, käyttöohjeet

Philips IntelliVue, MP60 and MP70 patient monitors. Viitattu 10.11.2012
http:/ / www.healthcare.philips.com/ us_en/ products/ patient_monitoring/ products/ intellivue_mp70_mp60/

Virtual Switching System. 2012, Ciscon www-sivut. Viitattu 16.11.2012
http:/ / www.cisco.com/ en/ US/ prod/ collateral/ switches/ ps5718/ ps9336/ prod_qas0900aecd806ed74b.html

Software Configuration Guide. 2012. Ciscon www-sivut. Viitattu 12.11.2012
http:/ / www.cisco.com/ en/ US/ docs/ switches/ lan/ catalyst3750e_3560e/ software/ release/ 12.2_44_se/ configuration/ guide/ scg.html

End-of-Life Policy, 2012, Ciscon www-sivut. Viitattu 2.7.2012
http:/ / www.cisco.com/ en/ US/ products/ products_end-of-life_policy.html

Warranty Terms, 2012, Ciscon www-sivut. Viitattu 2.7.2012
http:/ / www.cisco.com/ en/ US/ docs/ general/ warranty/ English/ LH2DEN_ _.html

**LIITTEET**

**Liite 1. Vara-ICS:n käyttöönotto-ohje vikatilanteessa**

Tässä ohjeessa käydään läpi normaalit toimenpiteet mitkä pitää tehdä että vara-ICS on valmis vietäväksi toimipaikalle.

Jokaisessa ICS:ssä on sisällä USB-muisti missä on kyseisen ICS:n konfiguraatio, tikku löytyy vasemmanpuoleisesta kovalevytelakasta. Olisi hyvä että kyseinen USB-muisti laitetaan kaksipuoleisella tarranauhalla kiinni telakkaan.

ICS:stä on hyvä tietää seuraavia asioita:
Perussalasana = ”********”
Konsolipuolella su – salasana on ” ********”, tänne pääset Biomed valikon kautta järjestelmäkonsoli valinnasta.

/ sc3000/ -kansio tärkeimmät tiedostot ym. data ja lib, lib kansiossa on lisenssit ja konffiguraatiot.
Jos tarvetta niin konsolista pääsee normaali näkymään käskyllä login ja ****/ ****

ICS:n IP-osoitteen tarkistus tapahtuu komennolla cat / etc/ sysconf/ network-scripts/ ifcfg-eth0

Yksityiskohtainen ohjeistus:

1. Tarkista cat / proc/ partitions komennolla nykyiset osiot:
   root@ICS:~$ cat / proc/ partitions

| major | minor | #blocks | name |
|---|---|---|---|
| 251 | 0 | 771780 | ramzswap0 |
| 8 | 0 | 312571224 | sda |
| 8 | 1 | 308048896 | sda1 |
| 8 | 2 | 1 | sda2 |
| 8 | 5 | 4519936 | sda5 |

2. Laita USB-Muisti kiinni tietokoneeseen ja kirjoita hetkenpäästä uudelleen cat/ proc/ partitions niin näet että listaan tuli yksi laite lisää, tämä on USB-muisti

   root@ICS:~$ cat / proc/ partitions

   | major | minor | #blocks | name |
   |---|---|---|---|
   | 251 | 0 | 771780 | ramzswap0 |
   | 8 | 0 | 312571224 | sda |
   | 8 | 1 | 308048896 | sda1 |
   | 8 | 2 | 1 | sda2 |
   | 8 | 5 | 4519936 | sda5 |
   | 8 | 5 | 29531 | sdc1 |

3. Kirjoita käsky mount / dev/ sdc1 / mnt/ usb, tämä käsky liittää levyosioita tiedostojärjestelmään. Liittäminen on edellytys että kyseistä laitetta voidaan käyttää käyttöjärjestelmässä.

4. Nyt USB-muistilta voidaan kopioida tiedostoja vara-ICS:lle. Käskyllä restoreconfig, kopioidaan vara-ICS:lle USB-muistilta rikkimenneen ICS:n configuraatiot.

5. Irrota USB-muisti nyt, se pitää poistaa tiedostojärjestelmästä oikea oppisesti umount / dev/ sdc1 / mnt/ usb käskyllä. Tämän jälkeen USB-muisti voidaan laittaa takaisin telakan sisälle.

6. Edellinen käsky ylikirjoitti myös / sc3000/ lib/ locked_info.cfg tiedoston missä sijaitsi vara-ICS:n lisenssit, tämä tiedosto pitää nyt palauttaa vara-ICS:n USB tikulta.

   Pistä ensiksi vara-ICS:n USB-muisti windows koneeseen ja pura config.tar.gz paketista USB-muistin juureen locked_info.cfg tiedosto.

7. Laita vara-ICS:n USB tikku kiinni vara-ICS:sään, samalla tyylillä kuin äsken toinen tikku, eli etsi käskyllä cat / proc/ partitions oikea osio ja mount / dev/ sdc1 / mnt/ usb.

8. Kopioi vara lisenssitiedosto USB-muistilta / sc3000/ lib/ kansioon käskyllä cp / usb/ mnt/ locked_info.cfg / sc3000/ lib/

9. Nyt voidaan käskyllä restartcentral käynnistää keskus uudelleen.

10. Vie ICS toimipaikalle.

11. Lisää monitorit lisätä näytölle, tämä tapahtuu sivulta. Asennus/ keskusasettelu/ . Kannattaa kysyä henkilökunnalta kuka on valvomossa töissä että missä järjestyksessä he haluavat vuodepaikat näkymään ruudulla.
12. Tarkista sairaalan nimi, koska vuodepaikoilta voidaan ottaa EKG käyrä tulostimelle. Tulostus vaatii että sairaalan nimi on oikein asetuksissa. - Avaa konsoli ja käskyllä su – , superuserin oikeudet.
    Tämän jälkeen valitse lepo ekg asetukset komennolla rekgSelect, valitse 99 ja kirjoita sairaalannimi XXXX, tämän jälkeen valitse 7. eli 12 waves @5 sec (2 pages).

13. Sulje rekgSelect asetukset Q:lla.

14. Suorita uudelleen kirjautuminen ”logout tai login” ja sms_user / welcome

KAIKEN TÄMÄN JÄLKEEN: muista uudelleen käynnistää kaikkien deltamonitorien telakat, joko virta pois tai monitorin lukitussalpa auki ja kiinni.

HUOM: On mahdollista että käy niin että on 2 kappaletta näyttöjä kiinni ja uudelleenkäynnistyksen jälkeen kuva ilmestyy vain toiseen näyttöön.

Tämä näyttö voi olla hankalassa paikassa, esim. varastossa, eli voit varmistaa asennuksen jälkeen, että uudelleenkäynnistyksen jälkeinen kuva tulee oikeaan monitoriin. Jos kuva tulee väärään monitoriin, tulee monitorikaapelit vaihtaa ristiin.

**Liite 2 . ICS:n konfiguraatio**

Konfiguraatio löytyy USB-muistilta ja siksi ei yleensä tarvitse alkaa asettelemaan. Voi kuitenkin tulla tilanteita että konfiguraatiota pitää vaihtaa tai tarkistaa.

ICS:ssä:

1. Biomed → Määritä keskus
2. Laita salasana: ******
3. Sairaalan nimi: ****
4. Tulostinkytketty: Verkko – xx.xx.xx.240 (tarkista oikea IP)
5. Verkkotiedot: Sairaalan nimike: ****
6. Valvontayksikön nimike: näkee netInfo käskyllä (esim MON13)
7. Hoitoyksikön nimike: mihin hoitoyksikköön kuuluu.
8. Isännännimike:

**Liite 3. Deltan konfigurointi**

Telakan konfiguraatio:

1. Verkkotila: CPS/ IDS
2. Vuode: Vuodepaikan nimi. ICS:ssä oltava sama nimi, että tulee näkyviin (osasto lyhenne ja paikka numero)
3. CPS/ IDS: Samaksi kun vuodepaikan nimi
4. Hoitoyksikkö: Hoitoyksikön lyhenne, esim. sisat (sisätauti). Hoitoyksikkö voi koostua useammasta ICS:stä.
5. Tarkkailuyksikkö: ICS:n nimi, pitää tarkistaa ICS:n asetuksista
6. Sairaala: ****
7. Tallennin 1: tyhjä (ei käytössä, Paperitulostus)
8. Tallennin 2: tyhjä (ei käytössä, Paperitulostus)
9. Tallentimen käyttö: Verkkoyhteys (ei käytössä, Paperitulostus)
10. Isäntälaitteentunnus: deltan tunnus, vaikuttaa myös ip-osoitteeseen.
11. Tarkkailuyksikön tunnus: ICS:n tunnus, näkee netInfo käskyllä ICS:stä
12. IP-osoite: xx.xx.xx.isäntälaitteentunnus
13. Aliverkon peite 255.255.0.0
14. Oletusreititys
15. Etävaiennus: Kyllä
16. Etäohjain: Kyllä
17. Hälytysryhmä: 1
18. Keskusasema: Kyllä (Ottaako tietoja ICS:ltä vastaan, esim. kellon ajat)
19. Tallenna asetukset Näytönasetukset → Yksikköjärjestin → tallenna/ palauta

Deltassa on oma RJ45-liitin jonka kautta saadaan Delta langalliseen verkkoon kiinni ilman telakkaa, tämän konfiguraatio on sama kuin langattoman konfiguraatio. Deltaan on mahdollista lisätä langaton optio ja tämän mukana tulee langaton CompactFlash 54Mbps WLAN-kortti. Kortti asennetaan Deltan oikeaan laitaan. Langattoman verkon IP-osoite tulee olla eri kuin telakan konfiguraatiossa. Käytäntönä on nykyään että telakan IP-osoitteeseen lisätään 100. Jos IP-osoite olisi telakassa xx.xx.xx.43, niin langattoman IP-osoite on xx.xx.xx.143.

**Deltan langattoman sekä kiinteän verkon konfigurointi ilman telakkaa:**

1. Valikko → Näytön asetukset → Biomed → Huolto
2. Syötä salasana joka on ****
3. Verkkoasetukset → Langaton
4. Säilytä vuodemerkintä: Kyllä / Ei, katso kohta 12.
5. SSID: ****
6. Koodisuojaus ****
7. WPA2-tarkastuslauseke on: **********
8. Voimansiirto: 15
9. Maks. kanava 11
10. Valitse kanavat 1, 6, ja 11
11. Verkkotila: Suora verkkoyhteys
12. Vuode: MOBI1, Tuo tunnus pysyy siinä aina. Toinen vaihtoehto on pick&go toiminnallisuus, jossa monitori ottaa aina telekan tunnuksen mukaansa. Kohta 4.
13. Hoitoyksikkö: Hoitoyksikön lyhenne, esim. sisat (sisätauti). Hoitoyksikkö voi koostua useammasta ICS:stä.
14. Tarkkailuyksikkö: ICS:n nimi, pitää tarkistaa ICS:n asetuksista
15. Sairaala: ****
16. Isäntälaitteen tunnut: deltan tunnus, vaikuttaa myös ip-osoitteeseen.
17. Tarkkailuyksikön tunnus: ICS:n tunnus, näkee netInfo käskyllä ICS:stä
18. IP-osoite: xx.xx.xx.isäntälaitteentunnus
19. Aliverkon peite 255.255.0.0
20. Oletusreititys
21. Etävaiennus: Kyllä
22. Etäohjain: Kyllä
23. Hälytysryhmä: 1
24. Keskusasema: Kyllä
25. Tallenna asetukset Näytönasetukset → Yksikköjärjestin → tallenna/ palauta

**Liite 4. Dräger M300 -telemetrialähettimen konfigurointi**

Konfigurointi tapahtuu seuraavalla ohjeistuksella.

1. Virtajohto seinään tai varmista, että akun varaus on riittävä.
2. Tietokoneeseen pitää asentaa USB-Serial ajurit.
3. Otetaan ylös COM portti (Laitehallinta - USB Serial Port)
4. Konfigurointilaite kiinni USB kaapelin toiseen päähän.
5. Laite kytketään päälle painamalla nuolta ylös- ja alaspäin yhtä aikaa muutaman sekunnin ja vapauttamalla sen jälkeen napit.
6. Hyper Terminal / Putty tai vastaava ohjelma ja määritellään yhteys kyseiseen COM porttiin, portin nopeus pitää olla 115200.

Yhteyden ottaminen M300- laitteeseen (Service Menu)

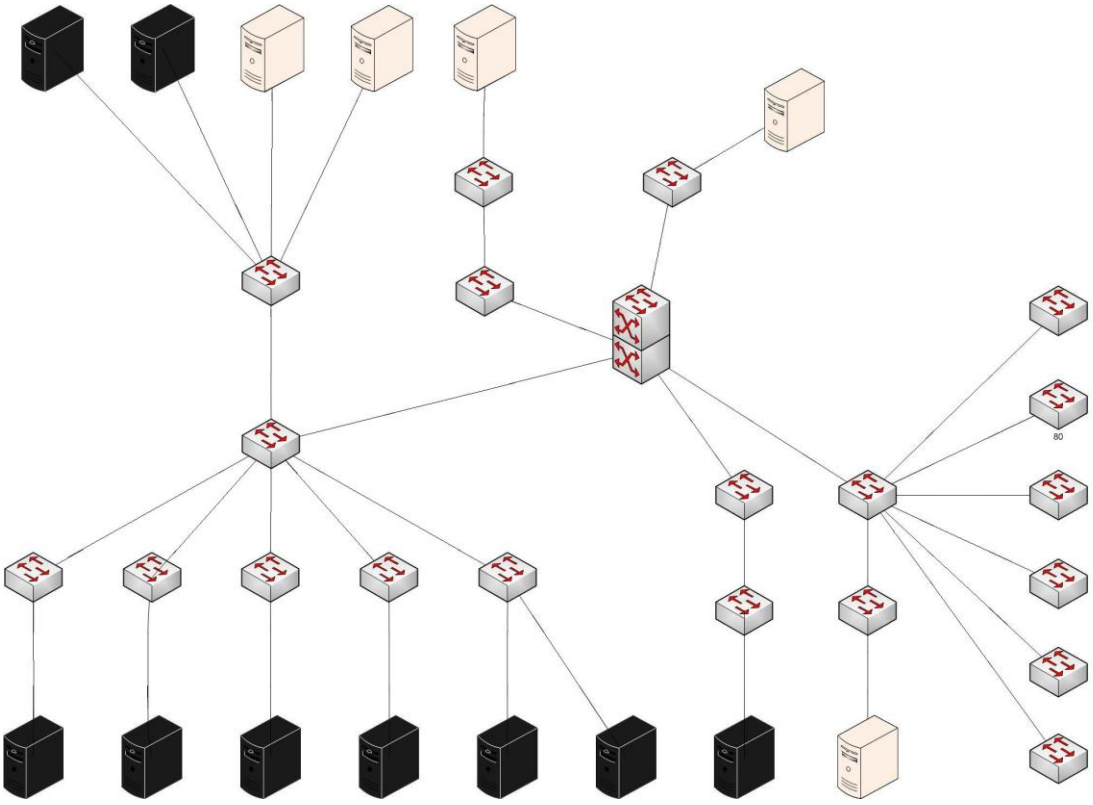
1. painetaan M300 laitteen kolmea nappia (ylärivi) yhtä aikaa ja heti perään tietokoneen ESC- näppäintä
2. Hyper Terminaaliin ilmestyy Service Menun salasana kysely ********* (uusissa laitteissa)
3. Valikoissa liikutaan kirjoittamalla valikosta haluttu toiminto ja enter (takaisin tullaan painamalla pelkästään enter)

IP osoitteen konfigurointi valikossa:

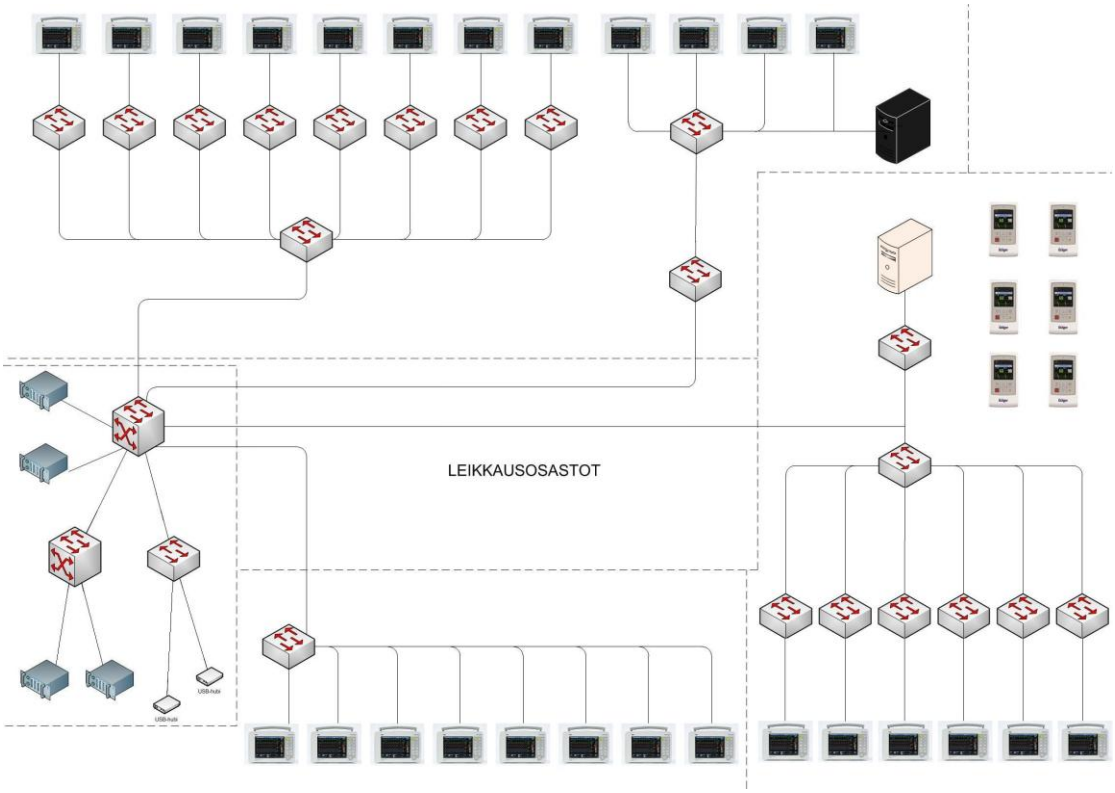
1. 2 + enter (Network menu)
2. 1 + enter (Network Setup Wizard) → Jos asetuksia on jo, niin wizard kysyy halutaan asetuksia muuttaa (Y/ N) → Y
3. Valitaan encryption modeksi → 2 (WPA2-PSK)
4. Valitaan encryption avaimeksi → ****
5. SSID:ksi valitaan → ****
6. Encryption key uudestaan → ****
7. Laitetaan oikea IP-osoite
8. Laitetaan oikea Maski
9. Laitetaan oikea Gateway
10. Kaikki tarvittavat konfiguraatiot on tehty. Asetukset voidaan tarkistaa valitsemalla 0 (Display Network Conf)

11. Enter painalluksilla voidaan kirjautua ulos.
12. Lopuksi reboot M300 laitteelle (nuolet yhtäaikaa)

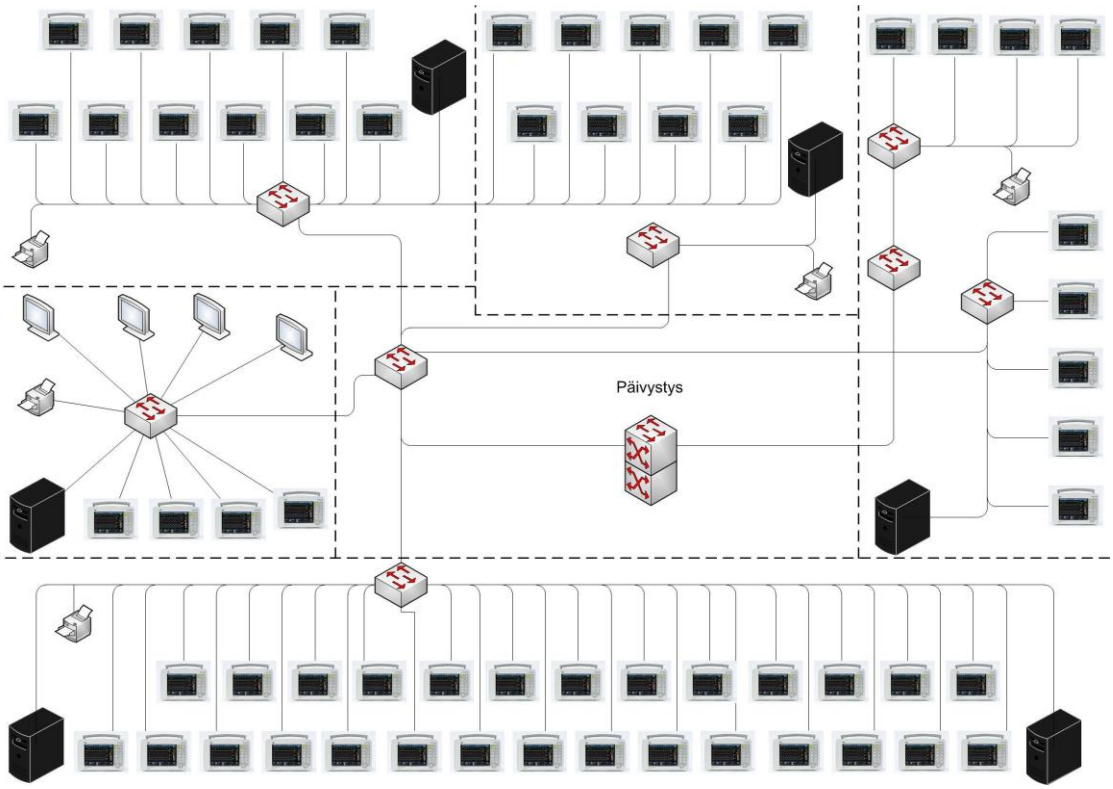
Muuta huomioitavaa:
Jos näyttö on "pimentynyt", painamalla ”menu” näppäintä muutama sekunti, näyttö aktivoituu.
Menu näppäimen takaa saadaan tarkistettua laitteelta.
1. Ensimmäinen painallus → potilaskaapeleiden tila
2. toinen painallus → potilastiedot ja paikka (ICS)
> kolme painallusta alaspäin-nuolinäppäin → saadaan verkkotiedot, signaali-voimakkuudet, mac ja jne...
3. kolmas painallus → voidaan säätää nuolinäppäimillä äänen voimakkuutta



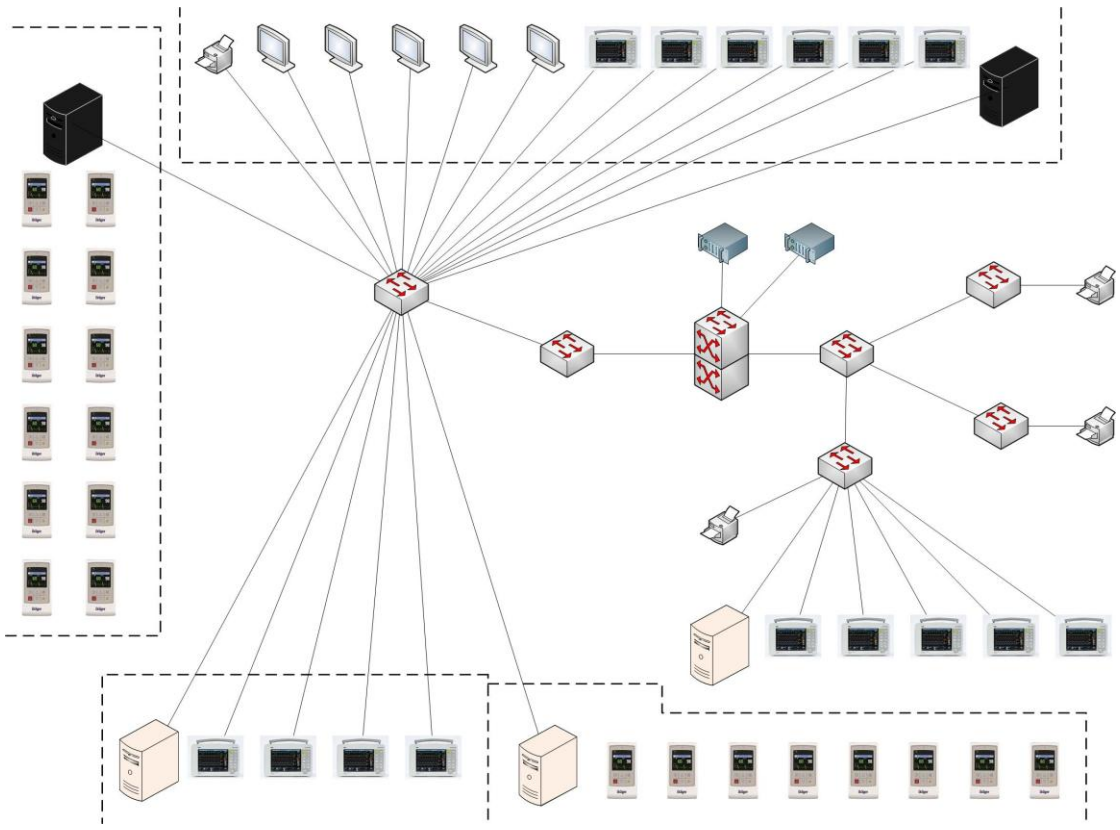
Liite. 5 ICS-keskusvalvontaverkkotopologia



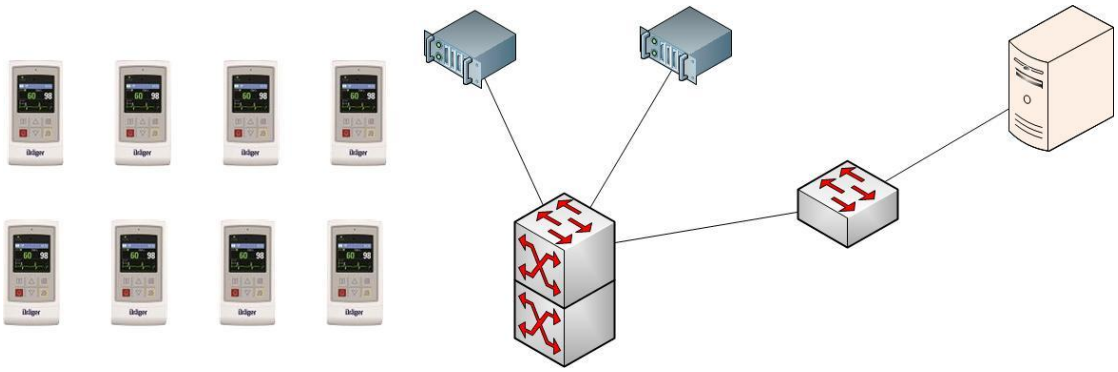

Liite.6 Leikkausosastojen potilasmonitoriverkkotopologia




Liite.7 Päivystysosaston potilasmonitoriverkkotopologia



Liite.8 Sydänvalvonnan potilasmonitoriverkkotopologia



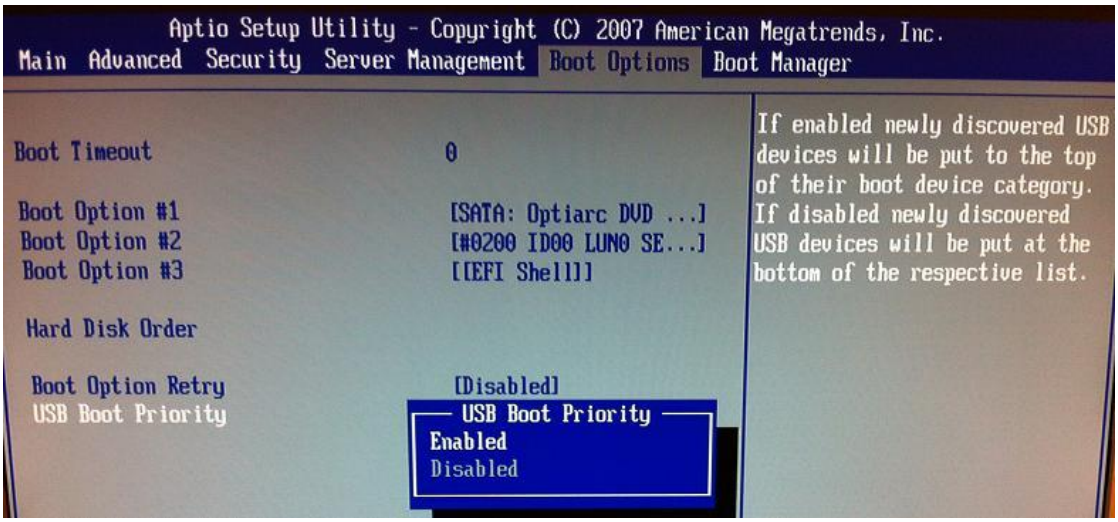
Liite.9 Lastenpoliklinikan potilasmonitoriverkkotopologia

**Liite 10. Varmuuskopion ottaminen Clonezilla-ohjelmalla**

Varmuuskopio Dräger ICS Potilasvalvontakeskuksen kovalevyistä otetaan Clonezilla-ohjelmistolla aina kun järjestelmään tulee muutoksia. USB-muisti, joka sisältää boottaavan Clonezilla-version löytyy lääkintätekniikasta tietotekniikkasalkusta, USB-muistissa on teksti CZ ja se on vihreä. Opinnäytetyön liite 10 on yksityiskohtainen ohje kuinka varmuuskopiointi suoritetaan.

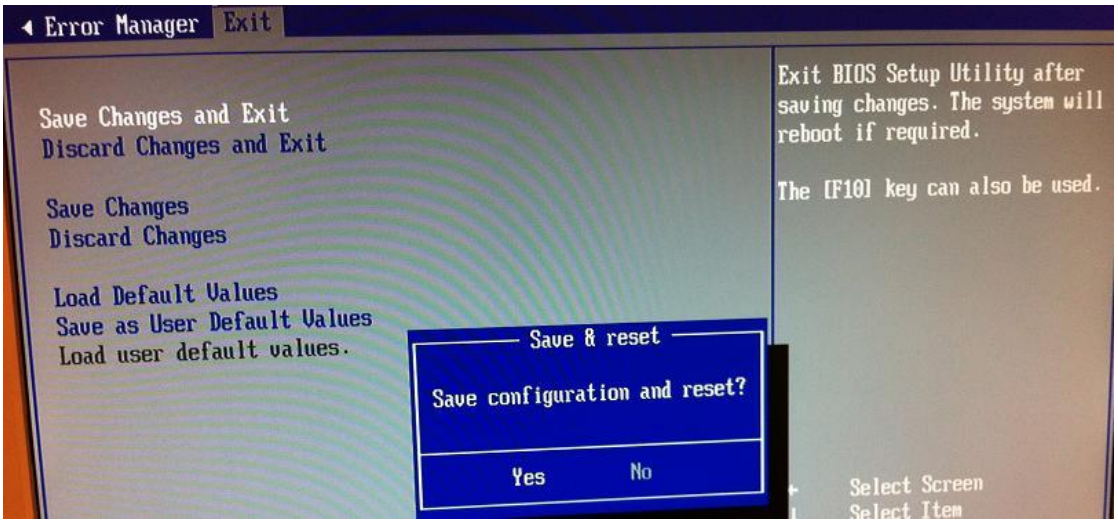
Varmuuskopioitava kone on käynnistettävä clonezilla USB- muistilta (merkitty CZ). Laita USB-muisti kiinni ja laita kone käyntiin, jos kone ei käynnisty USB-muistilta niin valitse F2.


Jos on tarpeellista mennä biossiin asettamaan USB-käynnistys mahdollisuus niin valitse Boot Options välilehdeltä USB- Priority = Enabled.

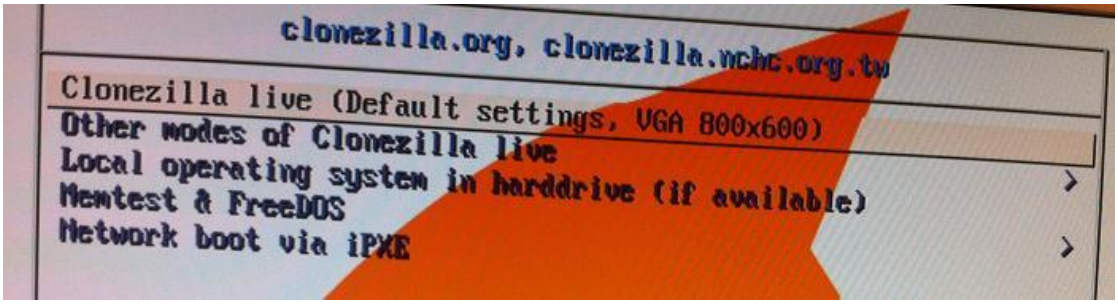



Tämän jälkeen mene Exit välilehdelle ja Save Changes and Exit.

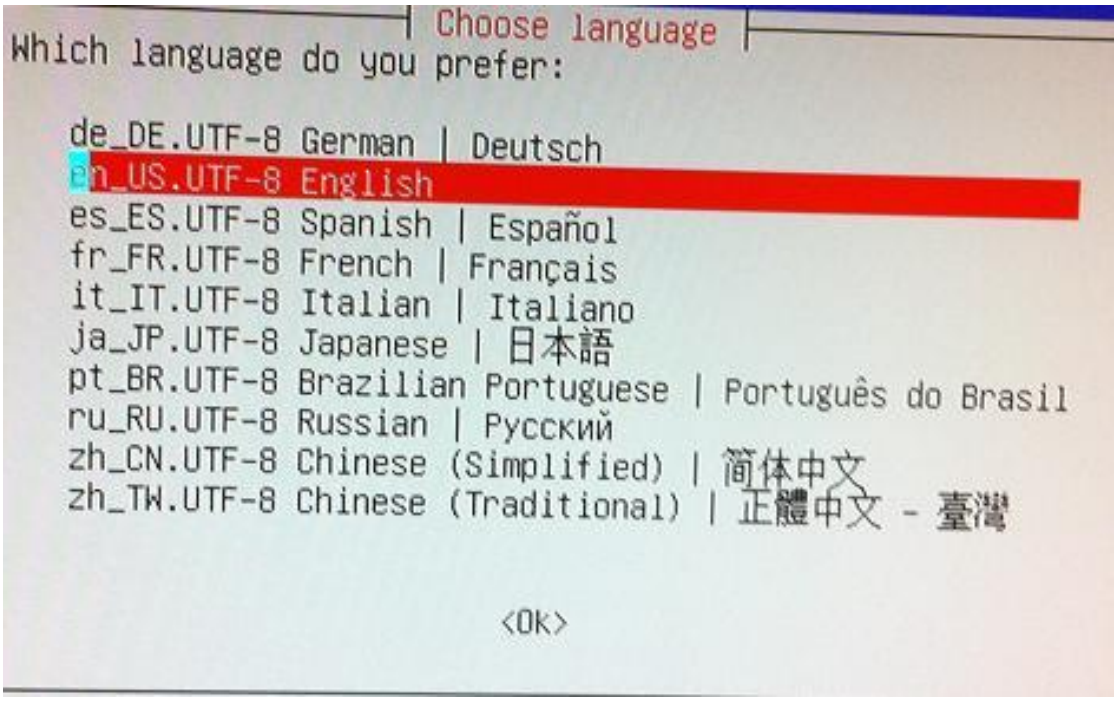
Tämän jälkeen koneen pitäisi käynnistyä USB-muistilta jos CZ USB-muisti on koneessa kiinni.



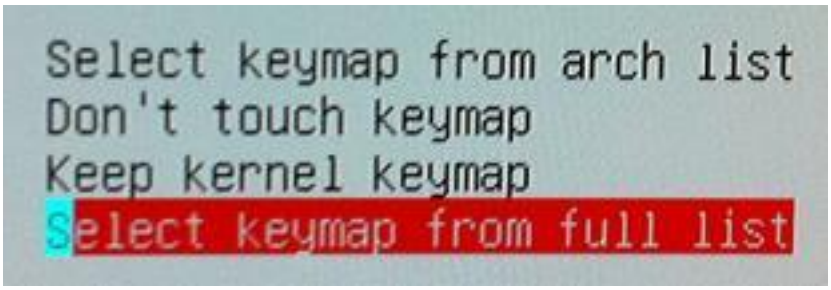

Valittavana näytön asetukset: 800x600 turvallisin vaihtoehto.



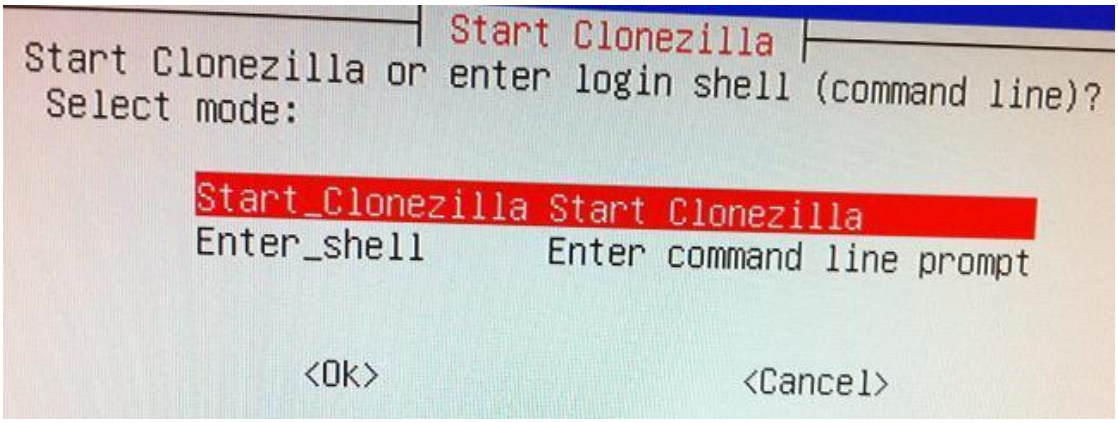
Ohjelman kielivalinta, valitse en_US.UTF-8 English



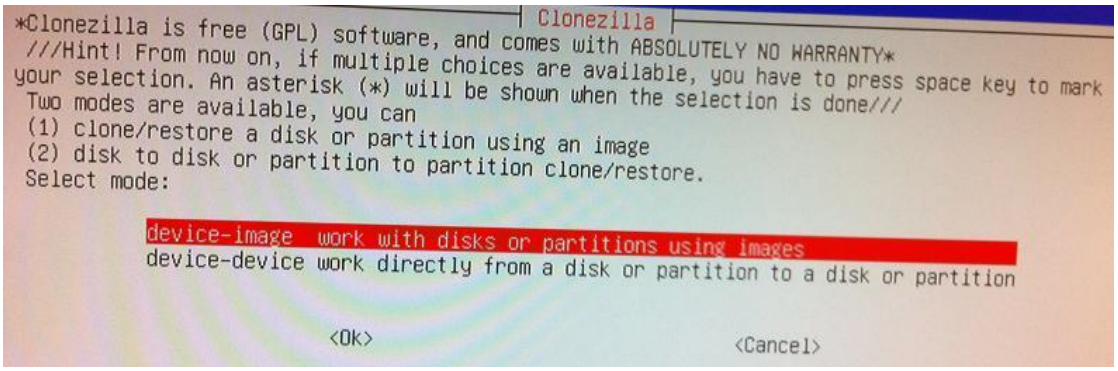

Keymap valittavana, normaalisti suomalainen kannattaa aina valita.



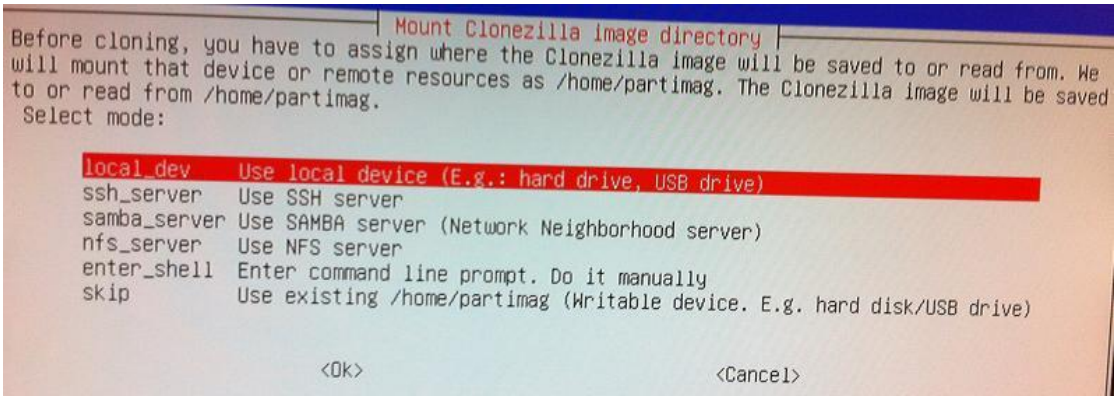

Käynnistä Clonezilla, Start_Clonezilla




Valitse device-image, levykuvien teossa valittava tämä.

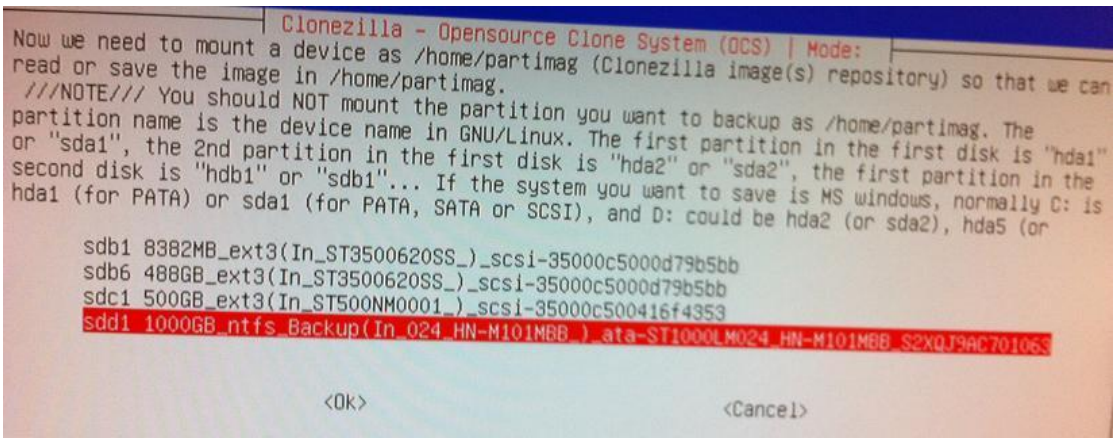



local_dev valitaan tämä koska käytämme USB-kiintolevyä jonne tallennetaan varmuuskopio image.

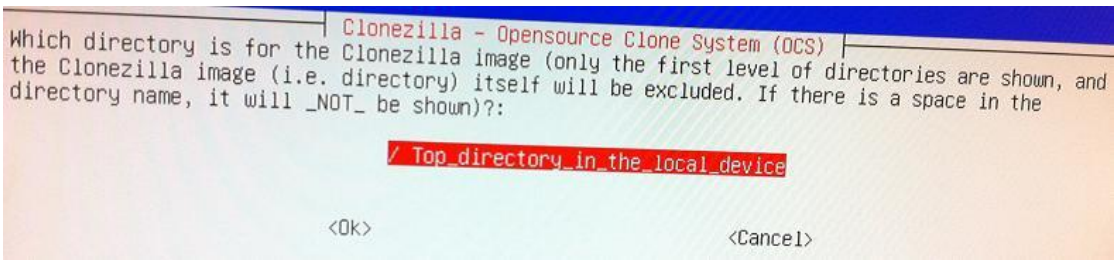


Kytke USB-kiintolevy vasta tässä vaiheessa koneeseen, clonezilla tunnistaa sen automaattisesti.

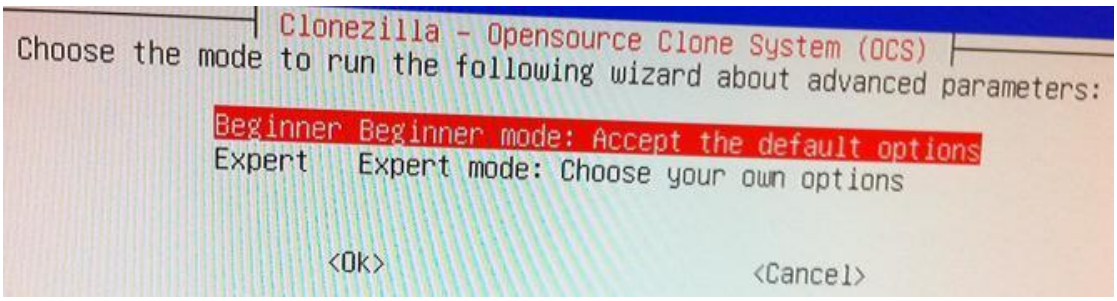

Valitse ulkoinen kiintolevy, yleensä alimmaisena ja LaCie merkkinen tällä hetkellä.




Tallenna kovalevyn juurihakemistoon eli valinta /

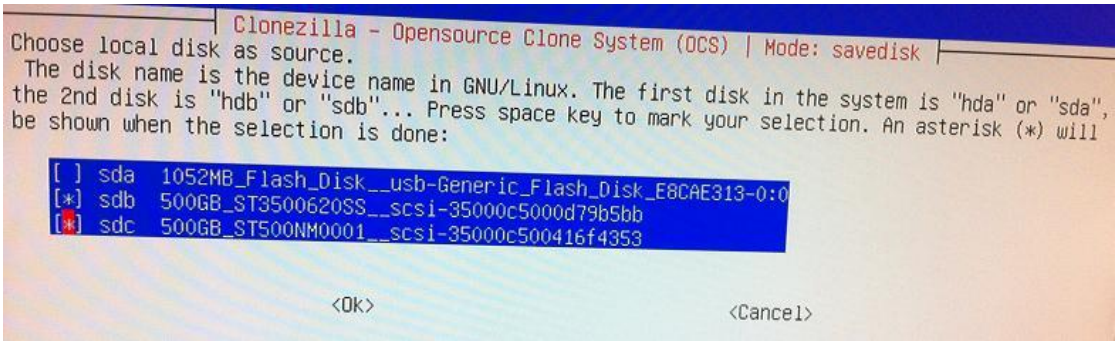



Valitse Beginner mode:

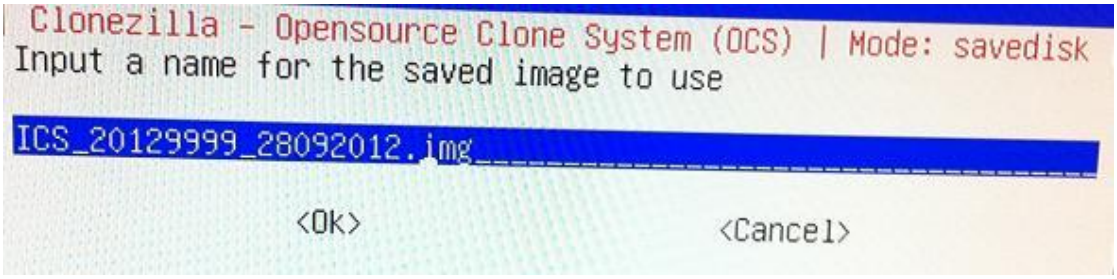



Savedisk, eli tallennetaan koko tallennettavan koneen levykuva ulkoiselle kiintolevylle.

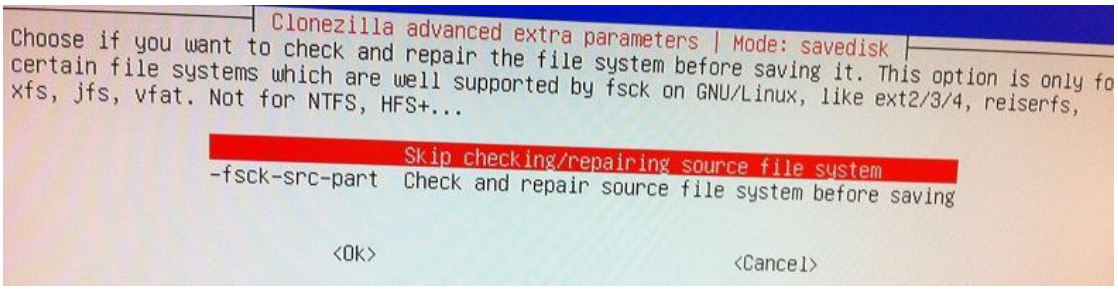

Valitse tallennettava kiintolevy, tässä varottava valitsemasta levyä jolla clonezilla käynnistetty. valinta tapahtuu viemällä punainen valitsin haluttuun kohtaan ja painamalla space, siirtymällä kohtaan ok ja painamalla enter.



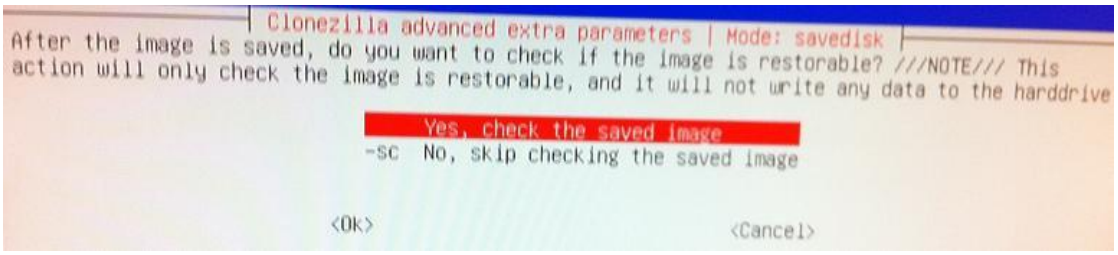

Kirjoita ICS_L-tunnus_päivämäärä.



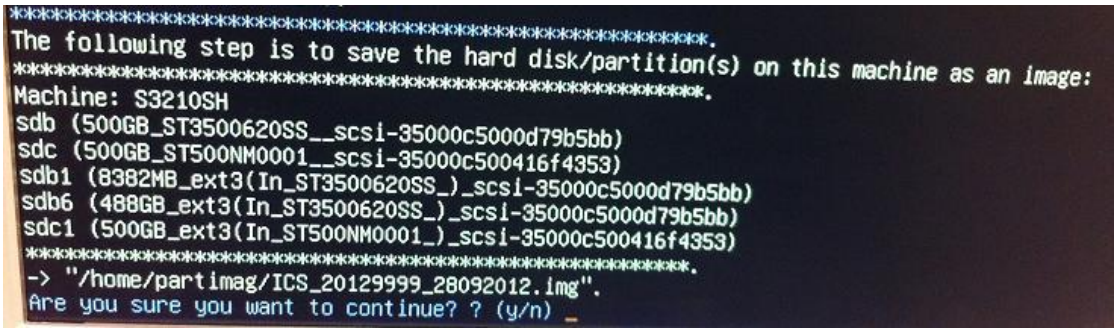

Ohita tämä kohta, emme halua tarkistaa ja korjata tiedostojärjestelmää ennen varmuuskopion ottamista.



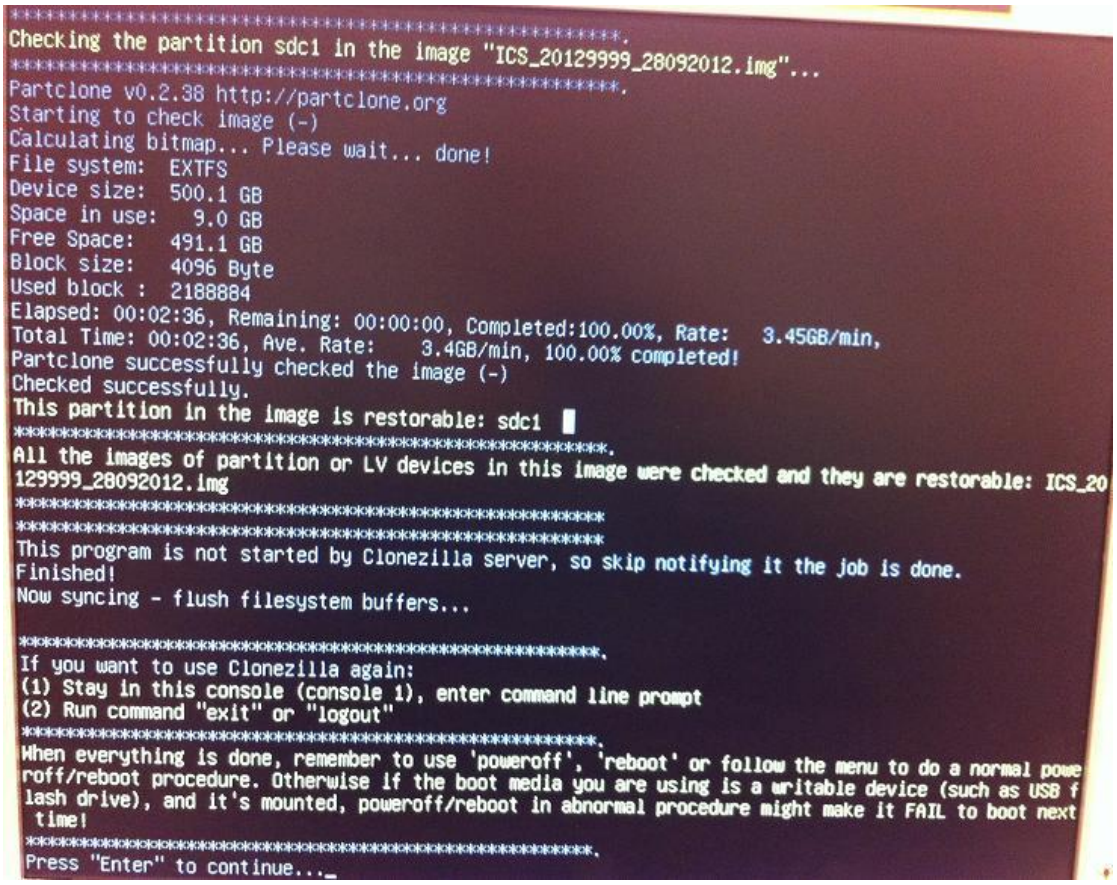

Tarkistettava tallennettu image jotta se on palautettava.




Jos nämä tiedot näyttävät oikealle valitse y




Lopuksi Clonezilla ilmoittaa että kopiointi ok ja tarkistus ok eli luotu image on toimintakuntoinen ja siitä voidaan palauttaa tiedot.




Irrota USB-kovalevy ja laita se takaisin oikeaan paikkaan ja muista myös irrottaa USB-muisti jossa on Clonezilla.

**Liite 11. Dynaamisen VLANin ohjeistus**

## Kytkimen portin asetukset.

Potilasmonitoriverkon laitteet voidaan liittää dynaamisesti verkkoon, kun alla oleva konfiguraatio on käytössä kytkimen portin konfiguraatiosta.

! Kytkimelle sisälle päin tuleva liikenne aktivoi autentikoinin, sallii verkosta päin tulevan liikenteen laitteelle. esim wake on lan
**authentication control-direction in**

! autentikointia on päällä mutta valvontamoodissa eli ei tehdä toimenpiteitä vaikka autentikointia epäonnistuisi.
**authentication open**

! autentikoinnin epäonnistuessa, käyttää seuraavaa autentikointi tapaa
**authentication event fail action next-method**

! Yhteensä kahdeksan laitetta voi autentikoitua yhdestä portista erikseen.
**authentication host-mode multi-auth**

! määrittelee missä järjestyksessä autentikointitapoja käytetään
**authentication order mab dot1x**

! aktivoi 802.1x autentikoinnin
**authentication port-control auto**

! uudelleen autentikointi kun autentikointi on epäonnistunut
**authentication timer restart 3600**

! aktivoi mab autentikoinnin
**mab**

! käsky liittyy portin 802.1x aktivointiin, tulee automaattisesti kun komento authentication port-control auto syötetään

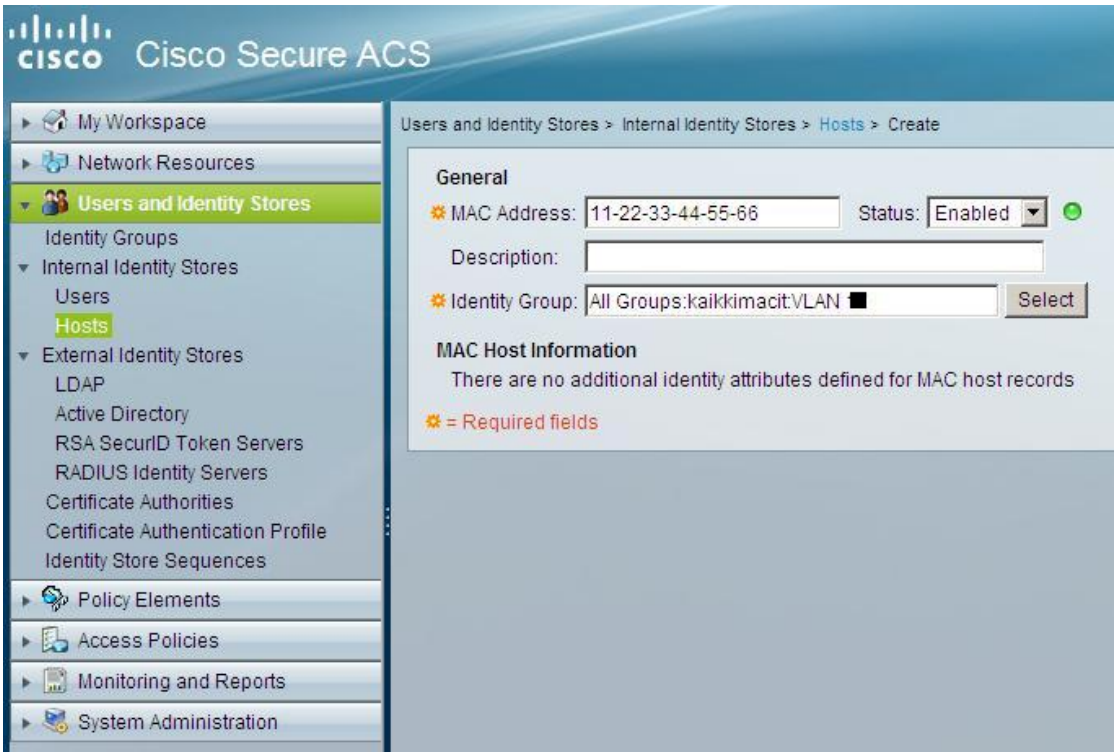
**dot1x pae authenticator**

## ACS ohjeistus.

Avaa Cisco Secure ACS

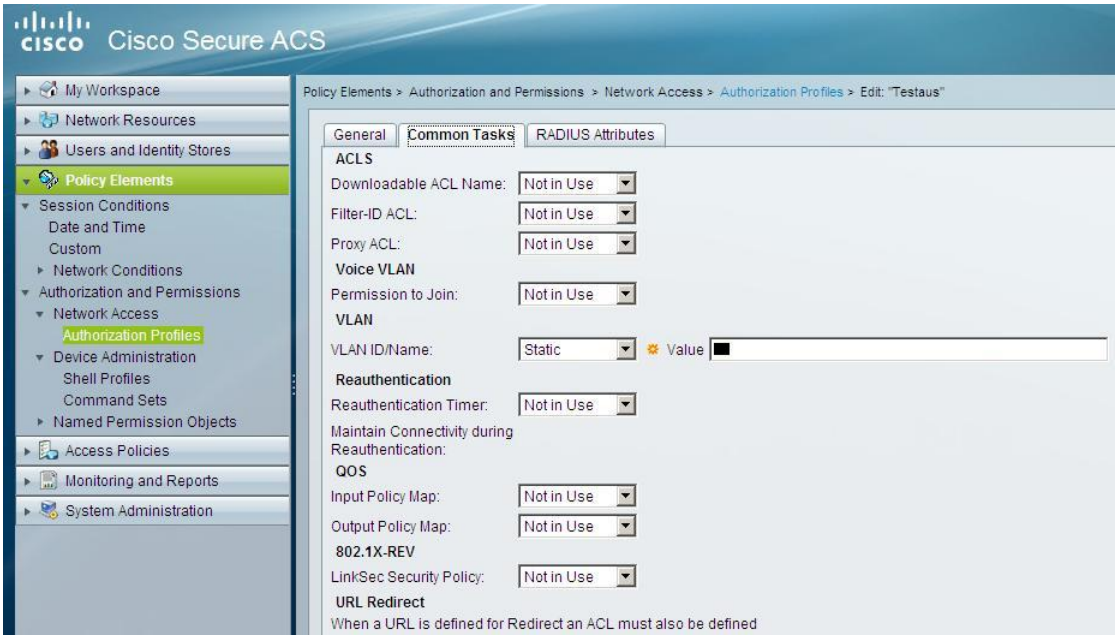
Luo uusi Identify Group alla olevalla tavalla, ohjeessa tehdään VLAN XX ryhmä


Tämän jälkeen liitetään Internal Identify stores → Hosts kohdassa laitteen MAC-osoitteen äsken luotuun VLAN XX ryhmään.



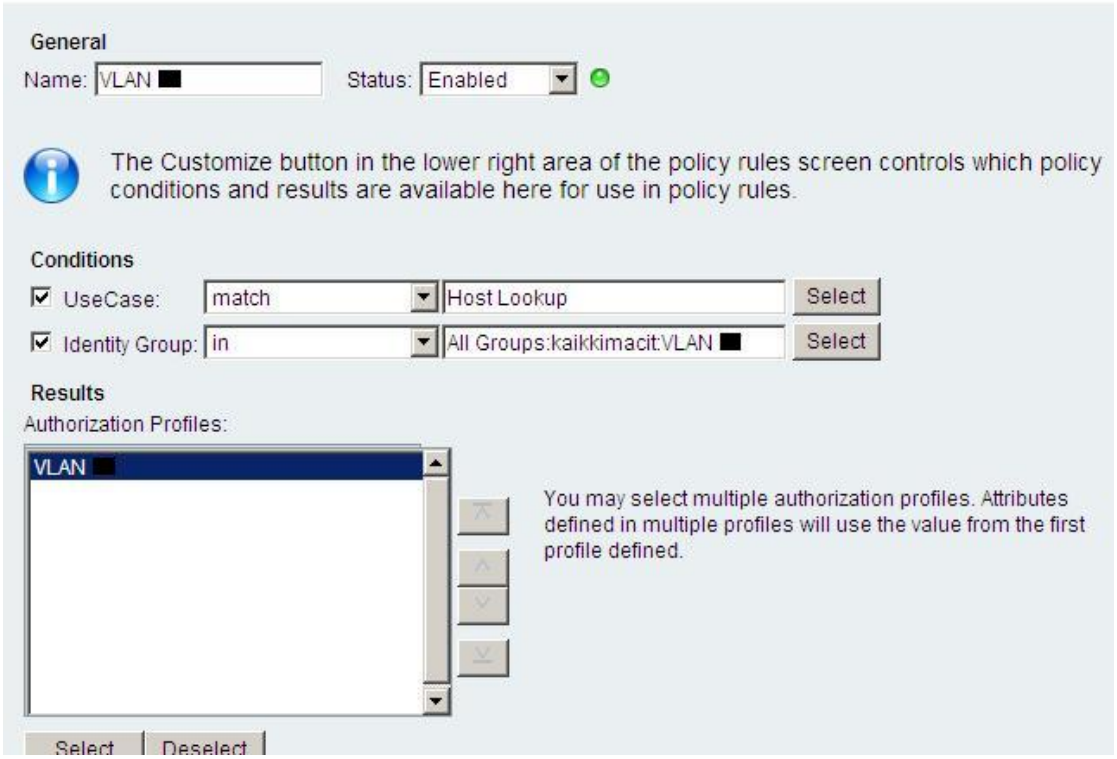

Authorization Progiles kohdassa luodaan uusi profiili VLAN XX

Sen jälkeen voidaan luoda tehtävä tälle profiilille common tasks kohdassa. Kun tätä profiilia käytetään, niin tällä tehtävällä on staattinen VLAN XX.




Lopuksi pitää mennä Access policies → Host lookup (MAB) ja luoda uusi access policy jossa käytetään edellä luotua Identify gruoppia ja authorization profiilia.


Näillä säännöillä tässä ohjeessa käytetyn MAC-osoitteen (11-22-33-44-55-66) omaava laite kun liittyy verkkoon, siihen porttiin vaihtuu oikea VLAN joka on XX.


General
Name: VLAN
Status: Enabled
The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.
Conditions
UseCase: match Host Lookup Select
Identity Group: in All Groups:kaikkimacit:VLAN Select
Results
Authorization Profiles:
VLAN
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.
Select
Deselect

## Liite 12. Päivystyspoliklinikan potilasmonitoriverkon eristäminen

Päivystyspoliklinikan potilasmonitoriverkon eristäminen muusta sairaalantietoverkosta tapahtuu seuraavalla tavalla. Etsi ristikytkentä kaappi RKT F.xx.x, Rak. xxx F xxxxxxxxx. Ristikytkentä sijaitsee xx-kerroksessa. Ristikytkennässä on kaksi kuitukaapelia, jotka on merkitty punaisella tekstillä POTILASMONITORIVERKKO. Tämä kaapelit irrottamalla voidaan potilasmonitoriverkko eristää muusta sairaalaverkosta. Kaapelit ovat kiinni ksshp-cxxxx_12_xxx_xxxx-sw tietoliikennekytkimessä.