LÄHIVERKON KÄYTTÖVARMUUDEN KEHITTÄMINEN KANTA-HÄMEEN SAIRAANHOITOPIIRISSÄ

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma

Syksy, 2016

Riku Salonen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Hämeen ammattikorkeakoulu

Tekijä Riku Salonen Vuosi 2016

Työn nimi Lähiverkon käyttövarmuuden kehittäminen Kanta-Hämeen sairaanhoitopiirissä

TIIVISTELMÄ

Opinnäytetyön tarve huomattiin Kanta-Hämeen sairaanhoitopiirin tieto- ja tietoliikennetekniikassa osana päivittäistä käyttövarmuutta. Kanta-Hämeen sairaanhoitopiirissä käytetään useita jatkuvasti käytössä olevia monitorointilaitteita ja kriittisiä järjestelmiä, joiden toiminta on turvattava mahdollisimman korkealla tasolla.

Opinnäytetyön tarkoituksena oli kehittää tietoliikenneyhteyksien toimintavarmuutta ja vähentää mahdollista käyttökatkon pituutta, jos lähiverkon reunakytkin rikkoutuisi. Opinnäytetyössä käytiin läpi Kanta-Hämeen sairaanhoitopiirin nykyinen tilanne ja toimintatapa vikatilanteen sattuessa. Käytännön osuudessa KHSHP:n verkkoympäristöön luotiin mallitoteutus, jossa reunakytkimille tehtiin hallittu päivityskäytäntö ja ajastetut varmuuskopiot.

Työn teoriaosuudessa käytiin läpi verkkotopologiat ja esiteltiin lähiverkon laitteisto. Yhdessä osuudessa keskityttiin KHSHP:lla käytössä olevien Cisco – merkkisten kytkinten perusteisiin ja konfiguroimiseen.

Työn lopputuloksena saatiin aikaan toimiva toteutus kytkimen päivittämiseen ja ajastettuun varmuuskopiointiin. Lopputuloksena aikaan saatua toimintatapaa aiotaan kehittää ja ottaa käyttöön Kanta-Hämeen sairaanhoitopiirissä vähitellen vuoden 2017 aikana.

Avainsanat Kytkin, cisco, lähiverkot, varmuuskopiointi, verkkotopolgia

Sivut 27 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Business Information Technology
Häme University of Applied Sciences

Author	Riku Salonen	Year 2016
Subject	Improving usage and reliability of the local area network for Kanta-Häme hospital district	

ABSTRACT

The topic of this thesis is to improve the usage and reliability of the local area network for the Kanta-Häme hospital district (KHSHP). At the Kanta-Häme hospital district there are many critical systems and monitoring devices that are working around the clock and those operations must be ensured at a high level.

The purpose of this thesis was to develop the reliability of the local network and reduce the downtime length in case of a switch hardware failure. This thesis discusses the current situation at KHSHP and how the hardware failure is solved out at the moment. In the practical part of the thesis, a switch operating system update and scheduled backups to the network environment were created.

The theoretical part deals with network topologies and network hardware. One of the main points was focusing on the Cisco – branded switches which are in use at KHSHP.

The final result was a working implementation which is a more effective and faster way to change the switch in case of failure. The result of this thesis will be developed and introduced at KHSHP during the year 2017.

Keywords Switch, reliability, cisco, local area network, backup, network topology

Pages 27 pages

SISÄLLYS

SANASTO

KHSHP – Kanta-Hämeen sairaanhoitopiiri

LAN – Local area network, lähiverkko

WAN – Wide are network, laajaverkko

TFTP – Trivial File Transfer Protocol, tiedonsiirtoprotokolla

PuTTY – SSH ja telnet -asiakasohjelma

VLAN – Virtual local area network, virtuaalilähiverkko

MAC – Message Authentication Code, verkkolaitteen yksilöivä koodi.

IEEE 802 – Standardointijärjestön työryhmä 802.

Ethernet - Lähiverkkoratkaisu

Mb/s – Megabittiä sekunnissa

Gb/s – Gigabittiä sekunnissa

Wi-Fi – Wireless Fidelity, WLAN yhteensopivuustestin sertifikaatti.

WLAN – Wireless LAN, langaton lähiverkko

IP-osoite – Internet Protocol address, on numerosarja verkkolaitteiden yksilöimiseen.

SNMP – Simple Network Management Protocol, tietoliikenneprotokolla, jonka avulla voidaan kysellä laitteiden tilaa.

Palomuuri – Firewall, järjestelmä joka tarkistaa ja suodattaa verkkoliikennettä.

DHCP – Dynamic host configuration protocol, verkkoprotokolla, joka jakaa IP-osoitteita lähiverkon laitteille.

IOS – Internetwork Operatin System, Cisco laitteiston käyttöjärjestelmä.

SSH – Secure Shell, on salattuun tietoliikenteeseen tarkoitettu protokolla.

Räkkiyksikkö – 19 tuuman räkki Standardisoitu laiteteline johon voidaan asentaa 19 tuumaa leveitä laitteita.
U-yksikkö – Viittaa räkeissä käytettävien laitteiden korkeuteen. 1U tarkoittaa 1,75 tuumaa eli 44,45mm.

Uplink-portti – Erillinen Ethernet-portti laitteessa, jota käytetään laitteiden keskenään linkittämisessä.

SFP-moduuli – small form-factor pluggable, SFP-moduuli, joka muuntaa signaalin parikaapelista valokuituun ja toisin päin.

LAN Base - Enterprise Access Layer 2 Switching, yrityskäyttöön L2-kytkin

CLI – Command-Line Interface, tekstipohjainen komentorivikäyttöliittymä.

ROM – Read Only Memory, lukumuisti on laitteessa oleva pysyvämuisti.

ICMP – Internet Control Message Protocol, protokolla jolla voidaan lähettää verkkolaitteesta toiseen paketteja varmistamaan laitteen toiminta.

1 JOHDANTO

Opinnäytetyön toimeksiantaja on Kanta-Hämeen sairaanhoitopiirin kuntayhtymä. Kanta-Hämeen sairaanhoitopiirin kuntayhtymään kuuluu 11 jäsenkuntaa ja se palvelee noin 180 000 asukasta. Kuntayhtymälle työskentelee yhteensä noin 2 000 ammattilaista eripuolilla Kanta-Hämettä. Opinnäytetyö toteutetaan Kanta-Hämeen keskussairaalan tiloissa ja ympäristössä. Kanta-Hämeen keskussairaala on otettu käyttöön vuonna 1979, ja se tarjoaa erikoissairaanhoidon palveluita ja osaamista. Kanta-Hämeen keskussairaala tarjoaa haastavan ja mielenkiintoisen ympäristön opinnäytetyön tekemiseen. (Häme-Wiki n.d.)

Valitsin aiheeksi lähiverkon käyttövarmuuden kehittämisen, koska olen kiinnostunut tietoliikennelaitteistosta ja tietoliikenteestä yleisesti. Opinnäytetyötä tehdessäni työskentelin Kanta-Hämeen sairaanhoitopiirin kuntayhtymässä tietoliikennetehtävissä. Oman työni ohessa huomasin kehittämisen kohteita, jotka jatkossa helpottaisivat ja parantaisivat Kanta-Hämeen sairaanhoitopiirin tietoliikenneratkaisuja.

Opinnäytetyössä käyteyt tutkimuskysymykset olivat seuraavat. Millä toimilla käyttökatkoa saadaan lyhennettyä vikatilanteissa? Pystytäänkö ongelmiin reagoimaan tarpeeksi nopeasti? Osataanko tehdä tarvittavat toimet?

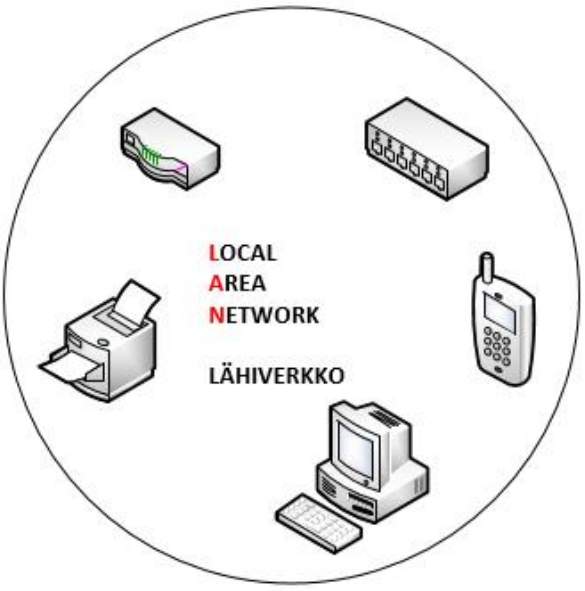
Tämän opinnäytetyön tarkoituksena oli kehittää lähiverkon toimintavarmuutta Kanta-Hämeen sairaanhoitopiirissä. Työssä käytiin läpi tietoliikenteeseen liittyviä menetelmiä ja laitteistoa. Tässä opinnäytetyössä esiteltiin perusteet verkkotekniikoista, verkkotopologioista ja lähiverkon laitteista. Työn yhtenä keskeisemmistä asioista oli Cisco-kytkinten käyttö ja konfigurointi.

Opinnäytetyö toteutettiin yhteistyössä Kanta-Hämeen sairaanhoitopiirin tietoliikenneinsinöörin kanssa. Tässä työssä on tutkittiin Kanta-Hämeen sairaanhoitopiirin nykyisiä toimintatapoja. Työn lopputuloksena toteutettiin Kanta-Hämeen keskussairaalan kytkinlaitteistolle uudistettu päivitys ja varmuuskopiointi tapa. Uudistetun toimintatavan avulla mahdollistetaan nopeampi ja helpompi ratkaisu mahdollisen laiterikon sattuessa Kanta-Hämeen sairaanhoitopiirissä.

2 VERKKOTEKNIIKAT

Erilaiset verkkotekniikat ovat yleistyneet kehityksen myötä. Verkkojen tarkoituksena on liikuttaa tietoa paikasta toiseen. Asiakirjat, valokuvat ja videot voidaan jakaa verkon välityksellä. Verkko lisää tiedonsiirron tehokuutta, eikä nykyään välttämättä tarvitse fyysisesti toimittaa asiakirjaa, vaan se voidaan skannata työasemalle tiedostoksi ja lähettää verkkoa pitkin eteenpäin. Yksinkertaisimmillaan verkko on kaksi fyysisesti toisiinsa liitettyä laitetta, jotka jakavat tietoa keskenään.

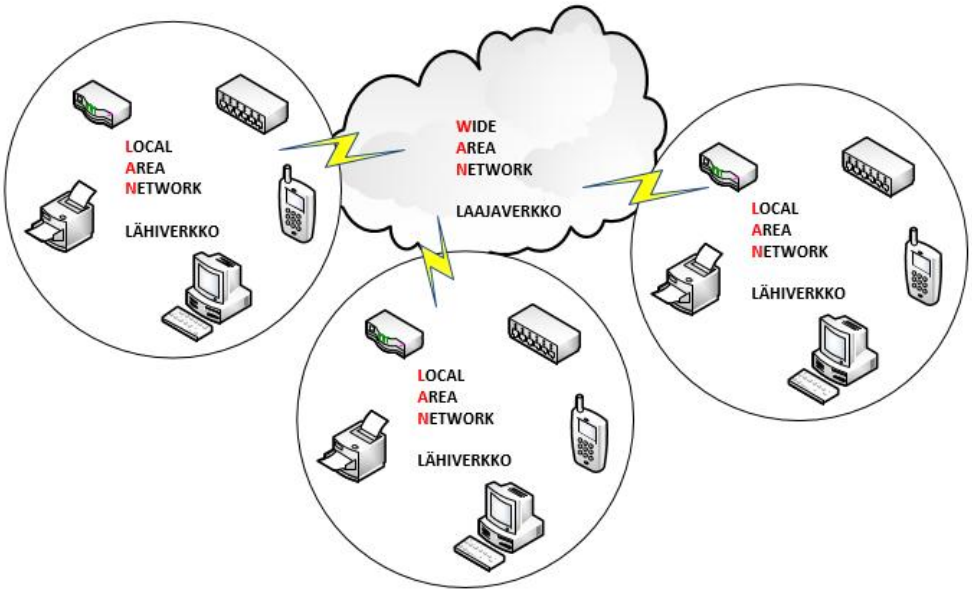
LAN (Local Area Network) eli lähiverkko tarkoittaa tietoliikenneverkkoa, joka toimii rajoitetulla maantieteellisellä alueella, jossa laitteet keskustelevat keskenään. Se voi olla rakennettu muutaman laitteen tai koko yrityksen laitteistosta. Lähiverkkoon voi kuulua muun muassa erilaiset verkkolevyt, pelikonsolit ja tulostimet. Lähiverkko voidaan rakentaa kaapeleilla tai langattomasti (WLAN Wireless Local Area Network). LAN käsitetään normaalisti verkkona, joka on fyysisesti toisiinsa liitettyjä verkkolaitteita yrityksen tai kodin rakennuksessa. Nykypäivän tekniikat, mahdollistavat lähiverkkojen yhdistämisen. LAN to LAN-tekniikan avulla voidaan lähiverkkoyhteys mahdollistaa kauas alkuperäisestä lähiverkosta. Perusrakenteet eli verkkotopologiat kertovat sen, kuinka lähiverkon laitteet ovat liitettyinä fyysisesti toisiinsa. Kuvassa 1 havainnollistetaan laitteet, jotka voivat keskustella keskenään ja ne muodostavat lähiverkon. (Okol n.d.)



Kuva 1. Yksinkertainen lähiverkko (Tyypillinen lähiverkko n.d.)

WAN (Wide Area Network) eli laajaverkko on tiedonsiirtoverkko, jonka tarkoituksena on yhdistää lähiverkot sekä kaupunkiverkot yhdeksi suureksi verkoksi. Laajaverkkoon voidaan liittää rajoittamaton määrä eri lähiverkkoja ja laitteita ympäri maailmaa. Esimerkiksi Internet on WAN. Ku-

vassa 2 havainnollistetaan, kuinka useasta lähiverkosta muodostuu laaja-verkko. (Okol, n.d.)



Kuva 2. Laajaverkko (NetPrivateer n.d.)

WLAN (Wireless Local Area Network) eli langaton lähiverkkotekniikka, joka nimensä mukaan toimii langattomasti. Langattomassa verkossa laitteet, jotka tukevat langatonta verkkoa voidaan yhdistää toisiinsa ilman fyysisiä kytkentöjä. WLAN-laitteet viestivät keskenään 2,4 Ghz:n ja 5,0 Ghz:n radiotaajuusalueilla. Kuitenkin kaikki WLAN-tekniikkaa hyödyntävät laitteet toimivat kaikissa WLAN-verkoissa. Langattomia yhteyksiä internettiin on nykyään hyvin saatavilla ja langaton verkkotekniikka on yleistynyt viimeisien vuosien aikana reilusti. Nykyään kotona ja työpaikoilla on useasti käytössä langaton lähiverkko. Riippuen WLAN:in käyttötarkoituksesta se voidaan suojata käyttäen erilaisia suojausmenetelmiä. WLAN:in suojaaminen on joka tapauksessa suositeltavaa, sillä ilman suojausta kuka tahansa voi liittyä langattomaan verkkoon, käyttää ja tehdä sillä luvattomasti mitä tahansa. Useat liikkeet, kahvilat ja ravintolat tarjoavat nykyään ilmaista pääsyä langattomaan verkkoon asiakkailleen, sillä langattoman verkon luonti on edullista ja helppoa. Yhä useammin nämäkin yhteydet ovat hyvin suojattuja ja niihin pääsyyn tarvittavat tunnukset annetaan asiakkaalle vasta kun asiakas asioi liikkeessä. (Viestintävirasto, 2014.)

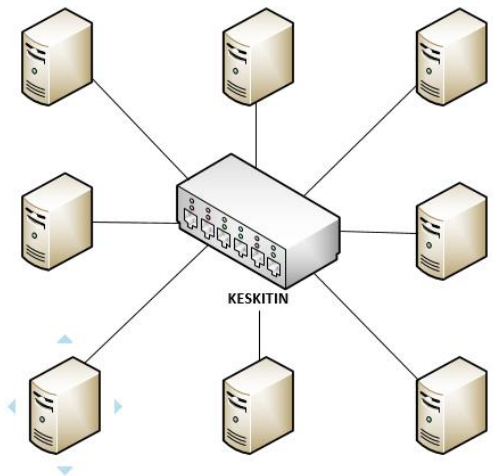
Langattoman lähiverkon luomisessa pitää ottaa huomioon yhteyksien kuuluvuus. Erilaiset rakennusmateriaalit vaikuttavat suuresti WLAN-yhteyksien toimintaan, jolloin WLAN-tukiasemia saatetaan joutua linkittämään toisiinsa signaalin vahvistamiseksi. Tukiasemien lähetystehoissa on laitekohtaisia eroja. Tehoa voidaan säätää manuaalisesti. Oletuksena lähetyssignaalin teho on usein suurin mahdollinen. (STUK 2015.)

3 VERKKOTOPOLOGIAT

Verkkotopologia on tapa, joka kuvaa lähiverkon perusrakennetta. Topologia kuvaa miten laitteet ovat fyysisesti kytkettynä toisiinsa. Verkkotopologia voi yksinkertaisimmillaan muodostua kahdesta laitteesta. Yleisimmät verkon topologiat, ovat tähti, rengas ja väylä. Muita topologioita ovat muun muassa puu ja mesh -topologiat. Jokainen verkkotopologia sisältää hyviä ja huonoja puolia. Topologiaa valitessa kannattaan miettiä tapauskohtaisesti kannattavin ratkaisu. Valittu verkkotopologia vaikuttaa pitkällä aikavälillä muun muassa siihen, kuinka verkon kasvua pystytään hallitsemaan jatkossa. Tässä luvussa esitellään yleisimmät käytössä olevat fyysiset verkkotopologiat. (Granlund 2007, 77.)

Tähtitopologiassa käytetään yhtä keskipistettä, jonka tehtävänä on välittää dataa verkon osapuolten välillä. Tämän topologian keskipisteenä voi toimia, joko keskitin tai älykkäämpi aktiivinen ohjain, jonka kautta kaikki tietoliikenne kulkee. Keskittimien käyttö keskipisteenä on nykyään vähentynyt, koska ne siirtävät datan kaikkiin keskittimeen kytkettyinä oleviin laitteisiin, joka aiheuttaa tietoverkossa ruuhkautumista. Tähtitopologiassa pyritään käyttämään kytkintä tai reititintä, jotka eivät pelkästään keskity siirtämään dataa, vaan huolehtivat myös tietoliikenteen suodattamisesta ja reitittämisestä, sekä valvovat verkkoliikennettä. Kuvassa 3 on kuvattu yksinkertainen tähtitopologia, jossa työasemat ovat fyysisesti liitettyinä keskittimeen. (Granlund 2007, 77.)

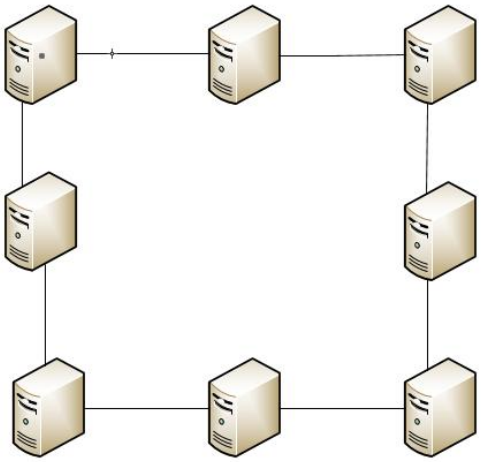
Perinteisen tähtitopologian heikkoutena on keskipisteenä toimiva laite. Laitteen rikkoutuessa, kaikki siihen kytketyt laitteet putoavat pois verkosta. Laitteen vaihto tai korjaus saattaa aiheuttaa pidempikestoisen katkoksen kaikkiin siihen kytkettyihin laitteisiin.



Kuva 3. Tähtitopologia muodostaa tähtimäisen rakenteen. (Granlund 2007, 78.)

Rengastopologiassa laitteet kytketään fyysisesti renkaan muotoon. Rengaskytkennässä jokaisella laitteella on kaksi yhteyttä. Toiselta laitteelta saadaan dataa ja se välitetään eteenpäin seuraavalle laitteelle. Rengasverkossa viedään liikennettä vain yhteen suuntaan, jossa se saattaa joutua lähettämään datan viereiselle laitteelle kiertämällä koko renkaan ympäri. (Granlund 2007, 78.)

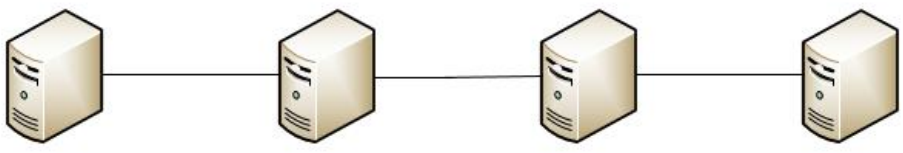
Rengastopologian heikkoutena on signaalin kulkeutuminen kaikkien laitteiden kautta. Häiriö yhdessä laitteessa saattaa vaikuttaa koko renkaan toimintaan. Kuvassa 4 esitetään, kuinka laitteet muodostavat renkaan eli rengastopologian.



Kuva 4. Rengastopologia. (Granlund 2007, 79.)

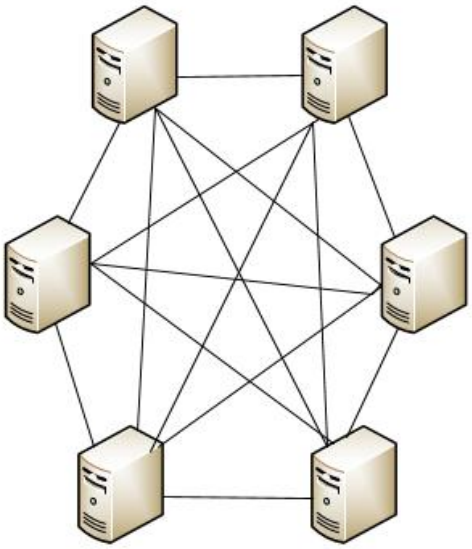
Väylätopologia on vanhin topologia. Väylätopologiassa kaikki laitteet ovat samassa väylässä niin, että kaikki laitteet voivat seurata ja osallistua tiedon välittämiseen. Väylätopologiassa vain yksi kone voi lähettää kerrallaan tietoja. Tieto lähetetään kaikille väylässä oleville laitteille sähköisinä signaaleina. Tiedon hyväksyy se laite, jonka osoite on sama kuin signaalissa. (Granlund 2007, 79.)

Väylätopologissa on monenlaisia ongelmia ja heikkouksia. Yhtenä ongelmista on osapuolten samanarvoisuus, jolloin kaksi laitetta saattavat lähettää signaalin samaan aikaan joista syntyy törmäyksiä ja ruuhkia verkossa. Mikäli väylätopologiassa hajoaa kaapeli, verkko jakaantuu kahdeksi, jolloin se ei ole enää toimintakuntoinen. Kuvassa 5 koneet ovat välylässä. (Okol n.d.)



Kuva 5. Väylätopologia (Okol n.d.)

Mesh-topologissa kaikki laitteet ovat yhteydessä keskenään. Tämä mahdollistaa erittäin vikasietoisen verkon. Yhden laitteen vikatilanteessa tieto välittyy perille vaihtoehtoista reittiä. Mesh-topologia on fyysisesti erittäin monimutkainen toteuttaa runsaiden kaapelointien takia ja sitä käytetään normaalisti vain tilanteissa, joissa laitekanta on pieni. Mesh-topologiaan käytetäänkin useimmiten laajojen langattomien verkkojen tekemisessä, ilman fyysisiä kytkentöjä. Kuvassa 6 esitetään Mesh-Topologia, jossa kaikki laitteet ovat yhteydessä toisiinsa. Mesh-topologian heikkoutena on kaapelointi ja siitä koituvat kustannukset. (Koudata n.d.)



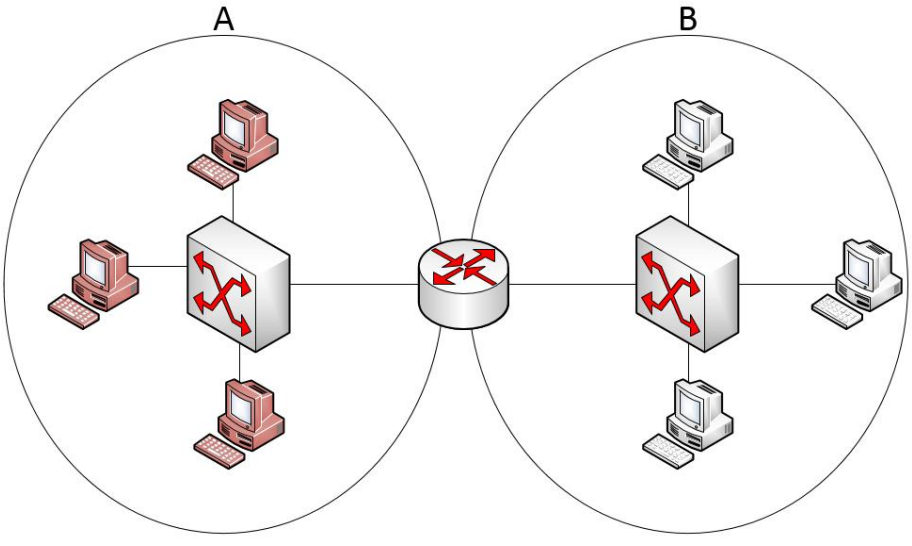
Kuva 6. Mesh-topologiassa kaikki laitteet keskustelevat keskenään. (Koudata n.d.)

4 LÄHIVERKON LAITTEISTO

Lähiverkko koostuu useista erilaisista laitteista, eikä ole olemassa yhtä oikeanlaista lähiverkkoa. Perinteiset lähiverkkoon liitettävät laitteet ovat työasemat, palvelimet ja oheislaitteet, kuten verkkotulostimet ja skannerit. Lähiverkkoon kuuluu myös tietoliikennettä ohjaavia laitteita, kuten kytkimiä ja reitittimiä. Tässä kappaleessa käydään läpi lähiverkon verkkoliikennettä ohjaavien laitteiden tärkeimmät tehtävät.

Reititin on laite, jolla pystytään yhdistämään tietoverkkoja toisiinsa. Reitittimen tarkoituksena on jakaa ja ohjata tietoa eteenpäin parasta mahdollista reittiä verkkokokonaisuuksissa. Reititin luo siirrettävälle tiedolle parhaan reittivalinnan, sen perusteella mitä topologiatietoa reititin on saanut reititysprotokollista ja ihmisavusteisesti. Laajoissa verkoissa reitittimien välille muodostuu useita eri reittejä, joista reititin itse valitsee tietojensa mukaan parhaan mahdollisen reitin. Reitittimien avulla pystytään tekemään hyvin vikasietoisia verkkokokonaisuuksia. Niiden avulla pystytään helpommin kiertämään esimerkiksi viallinen laite, koska ne osaavat vaihtaa liikenteen eri reitille, joko itsenäisesti tai saatujen sääntöjen mukaan. Reitittimien konfigurointi on monimutkaista, niiden tarjoamien useiden eri ominaisuuksien vuoksi. (Web-opas n.d.)

Reitittimen yksi tärkein tehtävä on jakaa verkko omiin verkkoalueisiin (broadcast domain) ja estää verkossa tapahtuvan yleislähetyksen eteneminen (broadcast-lähetys). Yleislähetyksellä voidaan kysellä tietoa verkon laitteista, lähettäjä lähettää yhden yleislähetyksen ja kaikki samassa verkossa olevat laitteet vastaavat. Jokainen reitittimeen kytketty laite muodostaa oman verkkoalueen, jonka avulla verkkoliikennettä rajataan. Kuvassa 7 esitetään omat broadcast domainit A ja B, kun kytkin lähettää yleislähetyksen reititin estää yleislähetyksen pääsemisen B puolelle. Kaikki lähettäjän puolen laitteet vastaanottavat lähetyksen. (TestOut, 2016.)



Kuva 7. Yleislähetys jää omiin broadcast domaineihin. (TestOut 2016.)

Kytkimen tehtävä on välittää liikennettä hallitusti eri kohteisiin. Kun kytkimelle saapuu tietopaketti, jos kytkin ei tiedä paketin vastaanottajaa se kaiuttaa paketin kaikkiin kytkimen porteista. Kun kytkin on saanut välitettyä tiedon oikeaan osoitteeseen, se tallentuu laitteen muistiin. Seuraavalla kerralla kytkin ohjaa tietopaketin suoraan oikeaan kohteeseen. Tämä vähentää huomattavasti tietoverkossa tapahtuvan liikenteen määrää ja vähentää yhteentörmäyksiä. Useita kytkimiä yhdistelemällä voidaan kasvattaa verkon kokoa tarpeen mukaan. Yhteen kytkimeen voidaan kytkeä useita laitteita ja verkkoliitinpaikkojen määrä vaihtelee laitekohtaisesti. Yrityksissä on useasti käytössä L2-tason kytkimiä. L2-kytkimiin voidaan määritellä eri virtuaaliverkkoja ja hallita niitä. (Helppari n.d.)

Keskittimen tehtävä on lähettää verkkoliikennettä eteenpäin. Keskitin lähettää tiedon aina kaikkiin siihen kytkettyihin laitteisiin ja sen vuoksi aiheuttaa turhaa ylimääräistä liikennöintiä verkossa. Keskittimien käyttö on vähentynyt verkkolaitteiden lisääntyessä, koska kulkevaa tietoa ei pystytä hallitsemaan keskittimen avulla. (Flyktman 2010, 322.)

5 CISCO

Cisco on maailmanlaajuinen IT-alan yhtiö, joka valmistaa reitittimiä, kytkimiä, verkkolaitteita ja palveluita. Cisco on perustettu vuonna 1984 ja se työllistää noin 75 000 työntekijää. Ciscolla on suurin markkinaosuus kytkin ja reititinlaitteiden markkinoista 56% prosentin osuudella. Ciscon myynnin viimeisen kolmen vuoden ajalta kokonaisliikevaihdosta kytkinten ja reititinlaitteiden osuus on noin 45%. Yhtiön lähimmät kilpailijat ovat Juniper, Huawei, HPE ja Alcatel-Lucent. Tässä kappaleessa käydään läpi Ciscon yrityskäyttöön tarkoitettujen kytkinten perusteet ja tutustutaan Cisco IOS-käyttöjärjestelmään, sekä IOS:n konfigurointiin. (Tivi, 2016.)

5.1 Cisco Catalyst

Catalyst on tuotemerkki Ciscon kytkinlaitteille. Yleisesti ottaen tuotemerkki on yhdistetty Ethernet-kytkimiin. Cisco on tuotteistanut Catalyst-tuotesarjan, hankkimalla muita yrityksiä. Alkuperäinen 5000 ja 6000 Catalyst-sarja pohjautui Crescendo Communications-yhtiön teknologiaan, jonka tuotannon Cisco hankki vuonna 1993.

Kaikissa nykyaikaisissa Catalyst-sarjan tuotteissa on verkkoliitäntä, jonka nopeus vaihtelee 10 Mbit/s ja 10 Gbit/s välillä mallista riippuen. Tuotesarja tarjoaa L2 ja L3-kytkimiä. Käytössä on kahta yleistä Catalyst-kytkin tyyppiä. Kiinteän kokoonpanon malli, joka on normaalisti 1U tai 2U-yksikköä. (WhatIs, 2016). Modulaarisia kytkimiä, joista pystytään vaihtamaan lähes jokainen osa, esimerkiksi virtalähde. Kytkimen tunniste alkaa yleensä WS-C kirjaimilla, jonka jälkeen esitetään mallinumero. Kirjaimilla mallinumeron perässä kuvataan erityispiirteitä ja numeroilla kuvataan verkkoliitäntöjen määrää. Kuvassa esitetään Cisco kytkimeltä show version –komennolla saatu mallinumero. (Wikipedia 2016.)

```
Switch Ports Model                     SW Version
------ ----- -----                     ----------
*    1 28    WS-C2960X-24TS-L          15.2(2)E5
```

Kuva 8. Cisco-kytkimen mallinumero

Kuva 8 mallinumeron selitys. (Fiber optic tutorial 2016.)

- W – IPSEC 40bit salaus
- S – kytkintaulu
- C – kiinteän kokoonpanon kytkin
- 2960 – mallinumero
- X – erottaa uudemman ja vanhemman 2960-sarjan
- 24 – porttien lukumäärä
- TS – Kytkimessä on SFP-portteja.
- L – LAN Base L2-kytkin

Ciscon Catalyt-sarjan kytkimet ovat erittäin suosittuja niiden hallittavuuden ja vikasietoisuuden takia. Laitteita pystytään konfiguroimaan käyttämällä eri liitäntätapoja kuten sarjaliitäntä, USB-liitäntä tai SSH-yhteydellä. Laitteiden konfigurointi tapahtuu tekstimuodossa, komentokehotteessa erilaisin komennoin. Ciscon laitteisiin kuuluu myös pienemmille organisaatioille suunniteltuja kytkimiä, joissa on luovuttu komentorivikäyttöliittymästä. Ne tarjoavat ainoastaan selainpohjaisen käyttöliittymän konfigurointiin ja hallintaan.

5.2 Cisco IOS

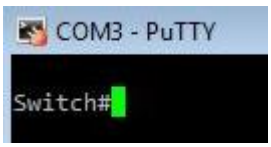
Cisco IOS (Internetwork Operating System) on Ciscon useimmissa reitittimissä ja kytkimissä käytetty käyttöjärjestelmä. IOS sisältää paljon käyttöominaisuuksia, joiden avulla voidaan parantaa verkkoliikenteen turvallisuutta ja suorituskykyä. IOS:n sisältämiä ominaisuuksia ovat muun muassa palomuuri, salaus ja todennus. (TechTarget n.d.)

Ciscon IOS käyttöjärjestelmä tarjoaa CLI:n eli komentorivikäyttöliittymän. CLI sisältää useita komentoja, joilla laitteita voidaan konfiguroida. IOS sisältää 5 eri komentotasoa, jotka ovat user exec mode, priviledged exec mode, global configuration mode, rom monitor mode ja setup mode.

User EXEC mode eli käyttäjätila on oletus tila IOS-laitteissa. Käyttäjätilassa on rajoitetut käyttöoikeudet. Käyttäjätilassa voidaan suorittaa yleisen tason komentoja, joilla voidaan suorittaa esimerkiksi yhteyden testausta tai listata järjestelmän tietoja. Käyttäjätilan laitetta käytettäessä tunnistaa kulmasulkeesta laitteen isäntänimen perässä.

Kuva 9. Kulmasulkeesta tiedetään, että käytössä on käyttäjätila.

Priviledged EXEC Mode eli etuoikeutettu tila, jossa pystytään suorittamaan kaikkia käyttöjärjestelmään määritettyjä komentoja. Etuoikeutettuun tilaan siirtymiseen määritetään normaalissa käyttötapauksessa salasana, jolloin lisätään laitteen tietoturvaa ja rajataan ketkä laitetta saavat konfiguroida ylemmällä tasolla. Etuoikeutetun tilan laitetta käytettäessä tunnistaa risuaita merkistä laitteen isäntänimen perässä.



Kuva 10. Risuaidasta tiedetään, että käytössä on etuoikeutettu tila

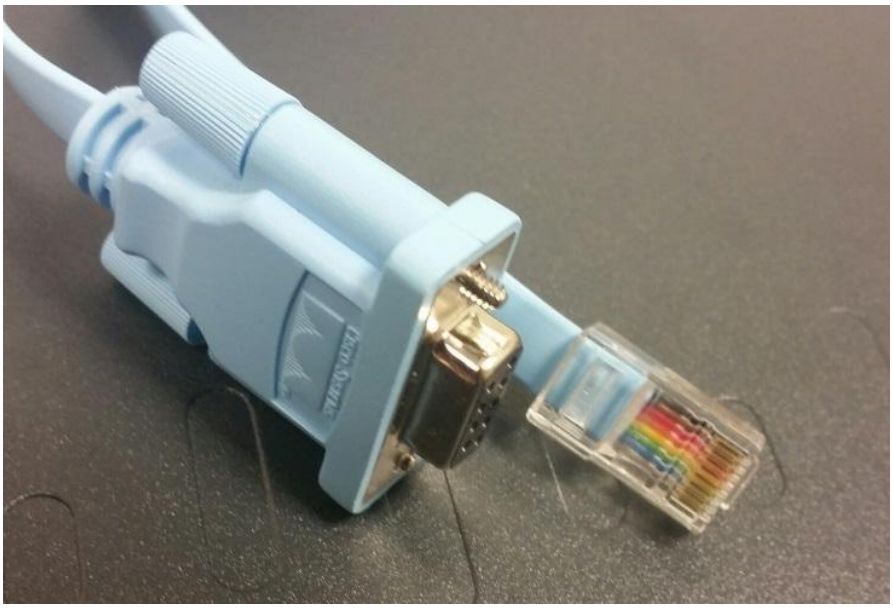
Global Configuration Mode eli globaali määritystila, jossa suoritetut komennot vaikuttavat koko laitteeseen yleisellä tasolla.

ROM Monitor Mode eli lukumuistitila toimii siten, että laite menee automaattisesti lukumuistitilaan, mikäli järjestelmä ei löydä kelvollista käynnistysmediaa.

Setup Mode eli asetustila. Asetustila on erilainen komentotila kuin muut tilat. Asetustilan avulla voidaan suorittaa reitittimen kokoonpanon konfiguraatio kun laite otetaan ensimmäisen kerran käyttöön. Asetustilassa on käytettävissä System Configuration Dialog, joka avustaa ja opastaa reitittimen asetusten määrittämisessä. (Cisco n.d.a.)

5.3 Konfigurointi

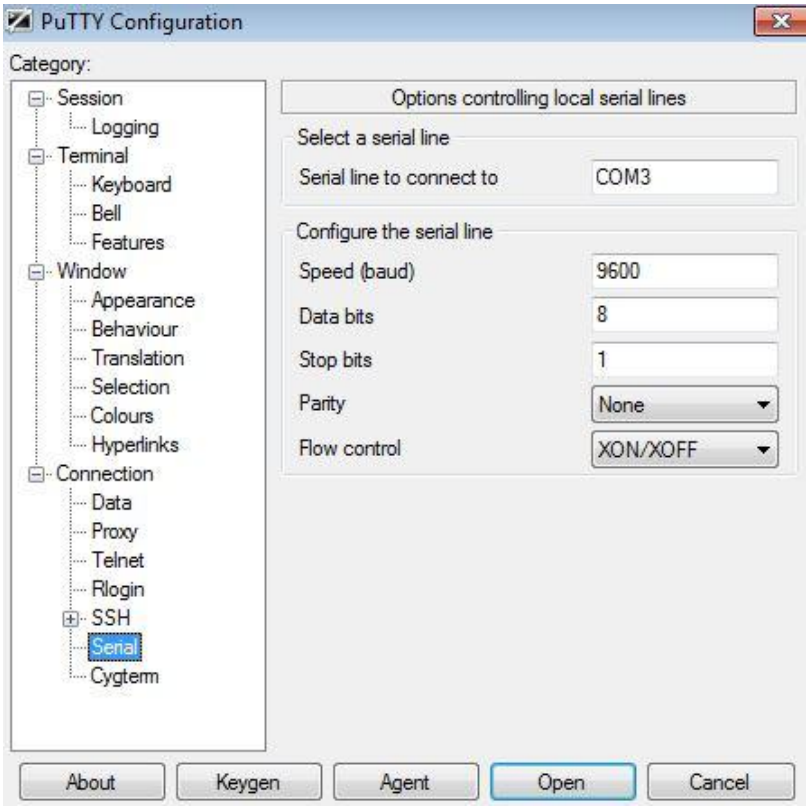
Laitteita voidaan konfiguroida käyttämällä suoraa fyysistä konsoli yhteyttä sarjakaapelilla tai uudemmissa laitteissa löytyvää USB konsoli yhteyttä. Kun kytkin on otettu käyttöön ja sille on asetettu tarvittavat verkon asetukset ja liitetty verkkoon laitteeseen voidaan ottaa yhteys käyttäen SSH-yhteyttä. Molempien tapojen yhdistämiseen tarvitaan sovellus, jolla tämä voidaan suorittaa. Sovelluksia on saatavilla useita, tässä opinnäyteyössä käytetty sovellus on PuTTY. Kuvassa 11 on esitettynä Cisco Systemsin sarjakaapeli, jolla voidaan ottaa konsoliyhteys. Toisessa päässä on naaras DB-9 liitin ja toisessa päässä uros RJ-45 liitin. (Cisco n.d.b.)



Kuva 11. Cisco Systemsin sarjakaapeli

PuTTY:llä ja sarjakaapelilla yhdistämisessä tarvitsee määritellä sarjaporttiasetukset oikein ja valita oikea COM-portti, johon sarjaliitin on liitetty tietokoneessa jota käytetään. Käytössä olevan sarjakaapelin COM-portti selviää Windows-käyttöjärjestelmissä laitehallinnan kautta. Sarjakaapelin

toisessa päässä oleva RJ-45 laitetaan kytkimessä osoitettuun konsoliporttiin. Kuvassa 12 kuvataan Cisco laitteelle soveltuvat konsoliyhteysasetukset.



Kuva 12. Asetukset Ciscon kytkimen sarjaporttiyhteydelle.

Suuressa osassa Ciscon laitteista konfigurointi tapahtuu CLI:llä. IOS:ssä on useita eri ominaisuuksia ja mahdollisuuksia, joten komentojakin on lukematon määrä. Ciscon CLI on tehty helppokäyttöiseksi. Konfiguroijan ei tarvitse aina muistaa koko komentoa ja riittää, kun muistaa komentojen ensimmäisen kirjaimen ja kirjoittaa sen perään kysymysmerkin. CLI listaa tämän komentotason alla olevat vaihtoehdot.

Jokaisella komentotasolla toimivat omat komennot. Esimerkiksi show-komentoa voidaan käyttää käyttäjätilassa ja etuoikeutetussa tilassa, mutta show-komentoa ei ole olemassa esimerkiksi globaalissa määritystilassa. Pelkästään show-komennolla ei vielä saada mitään tietoa ulos, vaan se tarvitsee toisen valinnaisen komennon toimiakseen. Listauksen show-komennon vaihtoehdoista saa kirjoittamalla show ? komentoriville. Show-komennoilla pystytään tarkastelemaan laitteiston tietoja, muuttamatta konfiguraatiota. Ciscon IOS version 15.2 esimerkiksi löytyy 174 erilaista show-komentoa.

Globaalissa määritystilassa tehdään muutoksia kytkimien asetuksiin. Tavallisella käyttäjätilalla ei pääse muokkaamaan laitteen asetuksia globaaliin määritystilaan, vaan käyttöoikeudet tarvitsevat korotusta etuoikeu-

tettuun tilaan. Configure terminal-komennolla päästään muokkaamaan laitteen asetuksia globaaliin määritystilaan. Tässä tilassa laitteen verkkoportteja voidaan muokata yksilöllisesti tai lisätä laitteelle uusia VLAN:ja. Globaalissa määritystilassa tarvitsee tietää mitä on tekemässä, koska esimerkiksi virheellisillä komennoilla saatetaan katkaista kytkimen verkkoyhteys, jolloin etäyhteys kytkimeen epäonnistuu eikä laitetta voida enää palauttaa etäyhteyden avulla. Tässä tapauksessa kytkimeen tarvitsee saada fyysinen yhteys, käyttämällä kytkimen USB tai COM-konsoli yhteyttä.

6 LÄHIVERKKO KANTA-HÄMEEN KESKUSSAIRAALASSA

Kanta-Hämeen keskussairaalan lähiverkosta ovat vastuussa sairaanhoitopiiri ja kolmannen osapuolen toimija. Kolmannen osapuolen vastuulla ovat runkolaitteet, reitittäminen ja palomuuri. Sairaanhoitopiiri vastaa reunakytkinten asennuksesta ja konfiguroinnista sekä langattoman verkon kuuluvuudesta.

Lähiverkko Kanta-Hämeen keskussairaalassa ja Kanta-Hämeen keskussairaalan Riihimäen yksikössä rakentuu pääsääntöisesti Ciscon verkkolaitteista. Hämeenlinnan yksikössä on noin 150 kytkintä ja Riihimäen yksikössä noin 35 kytkintä. Ciscon kytkinlaitteiden lukumäärä KHSHP:ssä on viimeisien vuosin aikana kasvanut tasaisesti. Ciscon mallistosta yleisin KHSHP:n käytössä oleva kytkinmalli on Ciscon WS-C2960S. Käytössä on myös runsaasti WS-C2960G ja uudemman sukupolven WS-C2960X kytkimiä. Käytössä olevat kytkimet ovat L2-tason kytkimiä, jotka osaavat käsitellä virtuaalilähiverkkoja. Osa kytkimistä on varusteltu PoE-ominaisuudella, joita käytetään paikoissa jossa tarvitsee liittää esimerkiksi valvontakameroita tai langattomia tukiasemia sairaalan verkkoon. Langattomia tukiasemia on yhteensä noin 160 kappaletta. Koko sairaanhoitopiirin kattavaa langattoman verkon kuuluvuutta ei ole, vaan langatonta verkkoa laajennetaan ja tukiasemia lisätään tarpeiden mukaan. Kuvassa 13 on kaksi Kanta-Hämeen sairaanhoitopiirin käytetyimmistä kytkinmalleista.

Kuva 13. Cisco Catalyst WS-C2960X-48TS-L ja WS-C2960X-24PS-L.

KHSHP:n kytkinten käyttöönotto tehdään manuaalisesti ja tämän takia vaatii huomattavan työpanoksen. Uutta kytkintä käyttöönottaessa tarvitsee tarkistaa kytkimen IOS-versio ja tarvittaessa päivittää. Kytkimelle konfirmoidaan aluksi hallintaverkon IP-osoite ja isäntänimeksi kytkimelle annetaan tulevan sijoituspaikan nimi, jotta etähallinnalla pystytään helposti varmistumaan käsittelyssä olevasta laitteesta. Kuvassa 14 esitetään nimeämistapaa kytkimen isäntänimeksi. Sijoituspaikka, tarkoitus tai tarkennettu sijainti ja numero, joka on kytkimelle määritetyn hallintaverkon IP-osoitteen viimeinen sarja.

```
Switch(config)#hostname hml-opinntaytetyo-1
hml-opinntaytetyo-1(config)#
Nov 16 12:06:39: %CNS IQ:0.1 ID:0 Changed:[hml-opinntaytetyo-1]
```

Kuva 14. Kytkin nimetään sijoituspaikan mukaan.

Sairaalassa on käytössä useita eri virtuaaliverkkoja. Eri laitteita on jaettu eri virtuaaliverkkoihin. VLAN:ien avulla jaotellaa fyysisesti yhtenäinen verkko omiksi virtuaaliverkoiksi. VLAN:ien avulla verkon hallittavuus paranee. Jokaisella VLAN:lla on oma IP-alue, joilta laitteet saavat osoitteen. Osassa verkoista on käytössä DHCP ja toisista VLAN:eista valitaan vapaa osoite, joka asetetaan manuaalisesti laitteelle. Suurimmat kokonaisuudet ovat jaettu omiin VLAN:eihin. Työasemat ovat jaoteltu 4 eri VLAN:iin. Työasemalle määritelty VLAN määräytyy työaseman sijainnin mukaan. Esimerkiksi Riihimäen toimipisteen työasemat ovat eri VLAN:ssa, kuin Hämeenlinnan yksikön. Verkkoon liitettävät tulostimet ja skannerit kuuluvat omaan VLAN:iin. Kiinteistövalvonnan valvontakamerat muodostavat oman VLAN:in ja hoitajakutsujärjestelmälle sekä lääkintälaitteille on omat VLAN:it.

```
hml-opinntaytetyo-1(config)#vlan 5
hml-opinntaytetyo-1(config-vlan)#name kytkinhallinta
```

Kuva 15. Kytkimelle konfiguroidaan hallintaverkon VLAN.

Kaikkien muutostöiden yhteydessä tulee muistaa tallentaa tehdyt konfiguraatiomuutokset. Konfiguraation tallennus onnistuu komennolla write memory tai copy running-config startup-config. Komennolla käynnissä oleva konfiguraatio tallennetaan käynnistyskonfiguraatioon. Tällä tavalla estetään tehtyjen muutosten häviäminen, kun laite käynnistyy uudelleen.

Muutostöitä tehdessä on otettava huomioon, että huoneiden verkkorasioita ei ole valmiiksi aktivoitu. Haluttu portti avataan kytkimeltä ja ristikytketään huoneeseen vasta, kun tiedetään mikä laite kyseiseen paikkaan liitetään. Toimiakseen optimaalisesti, jokaisen laitteen tulee olla sille kuuluvassa VLAN:ssa.

Langatonta verkkoa varten on käytössä Wireless LAN kontrolleri (WLC), jota käytetään langattoman verkon hallintaan. Kaikki käytössä olevat tukiasemat ovat Ciscon Aironet 2700-sarjaa. Tukiasemat saavat konfiguraation suoraan kontrollerilta. Langattoman verkon kautta on saatavilla sairaalan tuotantoverkko, asiakasverkko ja EKG-laitteille määritelty langaton verkko. Tuotantoverkko on salattu ja suojattu verkko, johon on pääsy sallittu vain sairaalan omistamilla laitteilla. Asiakasverkko on tarkoitettu asiakas käyttöön eri vuodeosastoilla ja oleskelutiloissa. Asiakasverkossa on käytössä web-pohjainen autentikointi, jonka jälkeen verkko on käytettävissä. Autentikoinnin avulla rajataan asiakasverkon verkkoliikennettä ja kuormaa. Laite joka on ollut 2 tuntia käyttämättä, pudotetaan pois sairaa-

lan asiakasverkosta. Kuvassa 16 Ciscon tukiasema, joita on noin 160 kappaletta koko sairaanhoitopiirin alueella.

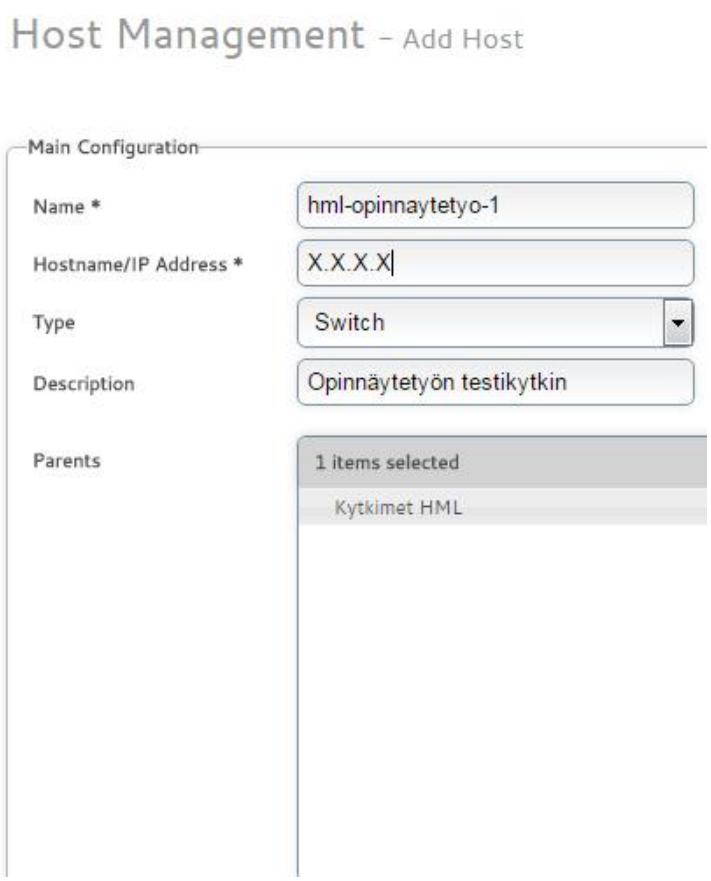
Kuva 16. Cisco AIR CAP 2701I-E-K9

Kytkinlaitteet ovat sijoitettuna kytkinkaappeihin, joihin pääsy on rajattu omalla erillisellä avaimella. Jokaiseen kerrokseen tai rakennuksen osaan on pyritty rakentamaan oma kaappi, joihin tulee kuituyhteys runkokytkimeltä. Normaalissa tilanteessa pyritään välttämään kytkimien ketjuttamista. Ketjuttamisen heikkoutena on jos yksi kytkin ketjussa hajoaa, silloin sen perään kytketyt laitteet menettävät myös yhteyden tietoliikenneverkkoon.

Kanta-Hämeen Sairaanhoitopiirin tietoliikennelaitteistoa valvotaan Cinian toimittamalla NetEye-ohjelmistolla. NetEye:lla valvotaan sairaanhoitopiirin palvelimia, kiinteistövalvontaa ja tietoliikennelaitteistoa Hämeenlinnassa sekä Riihimäellä. Ohjelmistolla valvotaan verkkoliikenteen laatua ja liikkuvan datan määrää verkossa. Ohjelmaan voidaan määrittää hälytykset sähköpostilla tai tekstiviestillä matkapuhelimeen. Tämän avulla pystytään reagoimaan poikkeukselliseen toimintaan tarvittaessa ympäri vuorokauden. Jos laite menettää yhteyden NetEye ilmoittaa siitä viestillä ja sähköpostilla. Ilmoituksesta selviää laitteen tiedot, IP-osoite ja varoituksen syy. Kun vika päättyy NetEye ilmoittaa, kuinka kauan kyseinen ongelma on ollut.

Uutta kytkintä NetEye:hin määriteltäessä se nimetään isäntänimen mukaan ja sille asetetaan IP-osoite. Valitaan valvottavan laitteen tyyppi alas-

vetovalikosta ja valitaan mihin osastoon laite kuuluu. Hälytys määritellään omalle ryhmälle, joita järjestelmään on luotu ja asetetaan aika, milloin hälytys lähtee. Kuvassa 17 perusnäkymä uuden kytkimen lisäämisestä NetEye:hin.

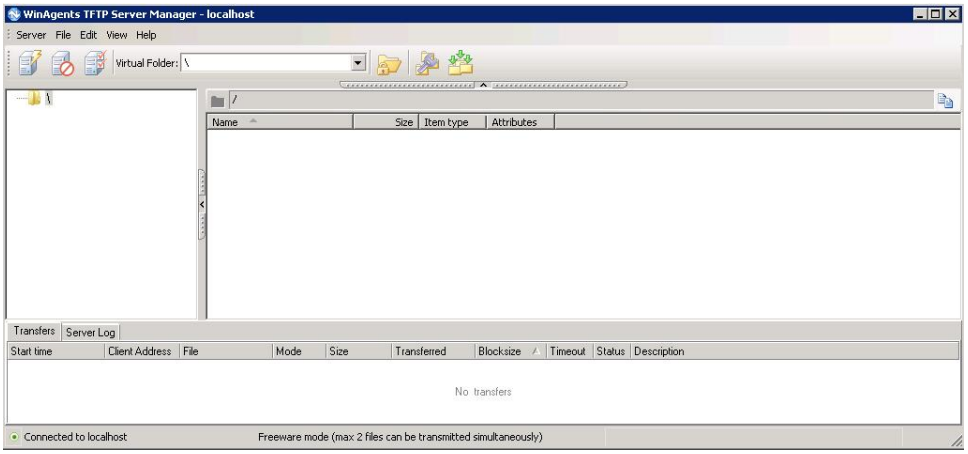


Kuva 17. Kytkin määritykset valvontaa varten.

NetEye:ssa on laaja valikoima valvontamahdollisuuksia. NetEye:n avulla voidaan asettaa valvontaan esimerkiksi palvelimen prosessorin käyttöaste tai levytilan käyttöaste. Reunakytkimen toiminnasta olennaisinta on tietää, että se vastaa verkossa ja sitä pystytään valvomaan ICMP-toiminnolla.

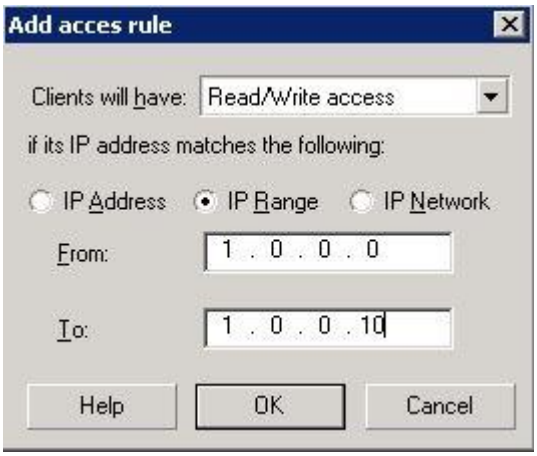
7 WINAGENTS TFTP-OHJELMA

Tässä työssä toteutetaan varmuuskopiointi ja päivitys käyttämällä WinAgents TFTP-ohjelmaa. Ohjelma on asennettuna KHSHP:n virtuaalipalvelimelle, jossa käytössä on Windows Server 2008 R2 Standard palvelin. TFTP-palvelun avulla voidaan hallitusti kerätä kytkimien konfiguraatiotiedostot yhteen paikkaan ja jakaa päivitykset. Kuvassa 18 on alkunäkymä hallinnointipaneelista, kun ohjelma on juuri asennettu.



Kuva 18. Yleisnäkymä hallinnointipaneelista.

Käyttöoikeudet määritellään siten, että sisältöä pystyy käsittelemään vain ne joille oikeudet ovat sallittu. Tämä parantaa tietoturvallisuutta. Kuvassa 19 määritellään IP-alue, joille myönnetään luku ja -kirjoitusoikeudet sovellukseen ja muilta IP-alueilta estetään pääsy TFTP:lle.

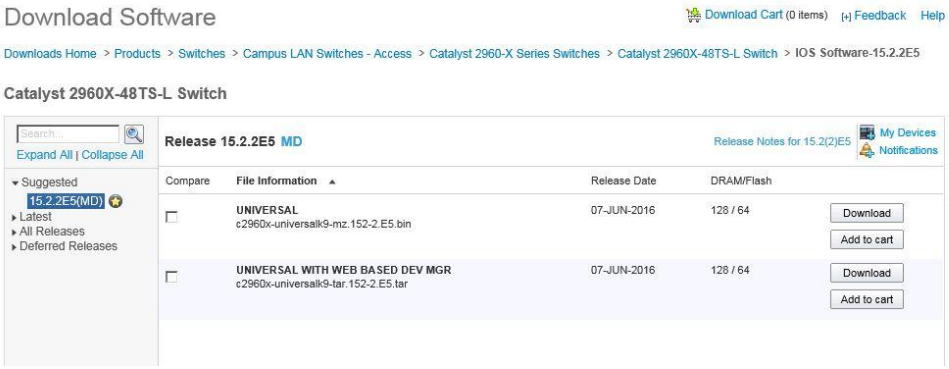


Kuva 19. Rajataan oikeudet vain halutulle joukolle kytkimiä.

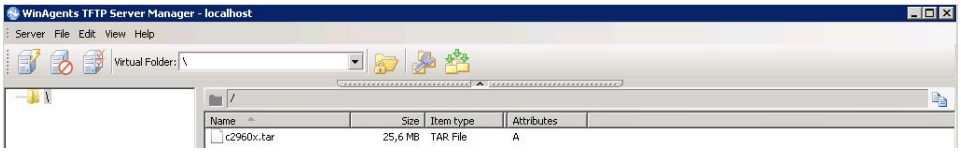
8 KYTKIMEN PÄIVITYS

Nykyisellä toimintatavalla päivitetään IOS-versio uudempaan, jos epäillään ongelmien johtuvan vanhentuneesta versiosta. Tavallisimpia syitä päivittää kytkimen IOS-versio, ovat versiossa ilmenneiden toimintaan vaikuttavien virheiden korjaus, uusien ominaisuuksien käyttöönotto tai mahdollisten tietoturvariskien paikkauspäivitykset. Päivitys toteutetaan USB-tikkua käyttämällä. USB-tikun kautta päivittämisen heikkous on sen tiedostojen huono hallinnointi ja pakottava tarve mennä fyysisesti kytkimen luo.

Kytkimen päivittäminen WinAgentsin kautta aloitetaan lataamalla haluttu IOS-versio Ciscon verkkosivuilta palvelimelle. Cisco tarjoaa kattavasti eri IOS-versioita omilla sivuillaan. Jotta IOS-versioita pystyy lataamaan, tarvitsee luoda käyttäjätili Ciscon verkkosivuille. Kuvassa 20 esitetään Ciscon verkkosivuston latausportaali, jossa on haettu Catalyst 2960X-48TS-L kytkimelle Ciscon suosittelema IOS-versio. Kytkimelle ladattu IOS-versio nimetään mallikohtaisesti. Kytkimen mallinumeron perään kirjoitetaan IOS-versionumero.



Kuva 20. Ciscon verkkosivusto.



Kuva 21. Ladattu tiedosto tuodaan ohjelmaan ja nimetään tunnistettavaksi.

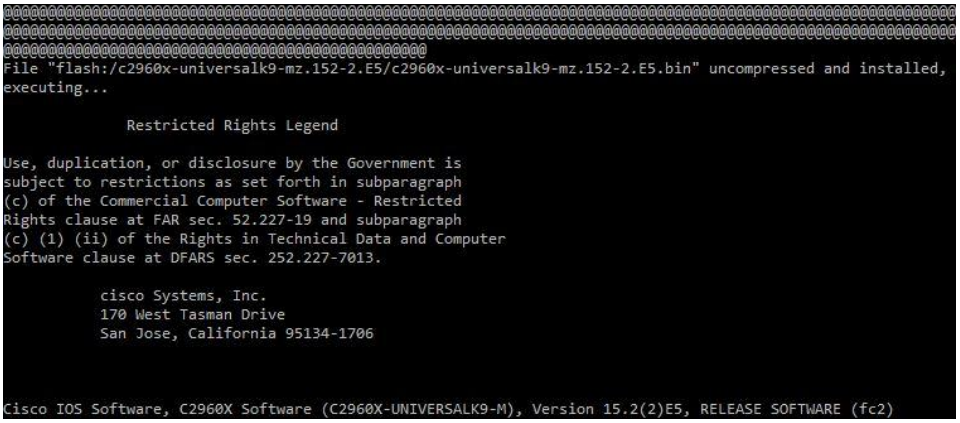
Kun päivittäminen aloitetaan tarkistetaan yhteys TFTP-palveluun. Yhteys tarkistetaan siitä kytkimestä, joka halutaan päivittää. Yhteyden testaaminen onnistuu ping-komennolla, jonka perään kirjoitetaan TFTP-palvelimen osoite.

Uusi versiopäivitys ladataan kytkimelle käyttämällä archive download-sw-komentoa. Komennon perään kirjoitetaan TFTP-palvelun IP-osoite ja nimi, joka uudelle versiolle annettiin. Lataus aloitetaan kytkimen hallintaverkon kautta, jonka sallimme WinAgentsin asetuksissa. Kuvassa 22 esitetään komento, jolla uusi IOS-versio ladataan kytkimelle.

Kuva 22. Ladataan IOS-versio kytkimelle.

Kun lataus on suoritettu, kytkin vaatii uudelleen käynnistyksen. Uudelleen käynnistyksen yhteydessä kytkin aloittaa ladatun version asennuksen. Uudelleen käynnistyksen voi tehdä reload-komennolla.

Uudelleen käynnistyksen yhteydessä kytkin käynnistyy muutaman kerran uudelleen ja päivitys kestää hetken. Kytkimen päivityksen edistystä voidaan seurata kehotteesta. Päivityksen valmistuttua kytkin käynnistyy. Aloituksen yhteydessä voidaan tarkistaa, onko oikea versio asentunut kytkimelle, kuten kuvassa 23 esitetään.



Kuva 23. Kytkin päivittynyt haluttuun IOS-versioon.

9 KYTKIMEN VARMUUSKOPIOINTI

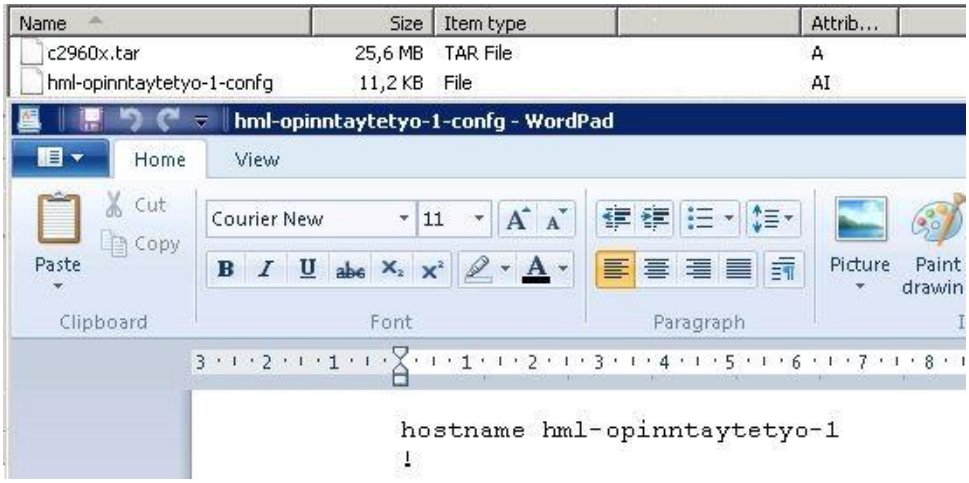
Kytkimen varmuuskopioinnilla saavutetaan nopeampi vasteaika vikaantuneen laitteen korjauksessa. Ilman kytkimen varmuuskopiota, vikaantuneen laitteen konfiguraatio voi olla mahdoton selvittää. Jos vikaantunutta laitetta ei saada enää kytkettyä päälle, edes fyysinen yhteys sarjakaapelilla ei auta. Kytkimen konfiguraatiossa saattaa olla useita eri VLAN:ja ja jokaisessa kytkimessä on oma konfiguraatio. Varmuuskopioimalla tasaisin väliajoin kytkimen konfiguraatiotiedosto, voidaan vikaantuneen kytkimen asetukset palauttaa paljon vähemmällä vaivalla.

Kytkimen varmuuskopiointi toteutetaan tallentamalla valmiiksi konfiguroidun kytkimen konfiguraatiotiedosto suoraan TFTP-palveluun, josta sitä voidaan nopeasti hyödyntää vikatilanteessa. Kopiointi manuaalisesti tapahtuu syöttämällä komento copy running-config tftp, jonka jälkeen pyydetään kirjoittamaan TFTP-palvelun IP-osoite. Kuvassa 24 kehote ilmoittaa, että tiedosto kopioitu.

```
hml-opinntaytetyo-1#copy running-config tftp
Address or name of remote host []? [redacted]
Destination filename [hml-opinntaytetyo-1-confg]?
!!
11531 bytes copied in 1.168 secs (9872 bytes/sec)
hml-opinntaytetyo-1#
```

Kuva 24. Kopioidaan konfiguraatio TFTP:lle.

Kun kytkimen konfiguraatio on siirretty onnistuneesti TFTP:lle, voidaan tiedostoa muokata ja käsitellä palvelimella. Varmuuskopioidun kytkimen konfiguraatio saadaan nopeasti tarvittaessa uudelle kytkimelle. Kuvassa 25 esitetään, kuinka kytkimen konfiguraatio saadaan auki käyttämällä esimerkiksi WordPad-ohjelmaa.



Kuva 25. Konfiguraatio TFTP:llä.

Jokainen kytkin tarvitsee varmuuskopioida säännöllisesti, koska niihin saatetaan tehdä satunnaisesti muutoksia. Jokaisen kytkimen varmuuskopioiminen säännöllisesti ilman automatisointia, on työlästä ja epäkäytännöllistä. Automaattisen varmuuskopioinnin avulla, jokaiseen laitteeseen tarvitsee vain kerran määritellä varmuuskopionti, jonka jälkeen laite pitää huolen varmuuskopioinnista.

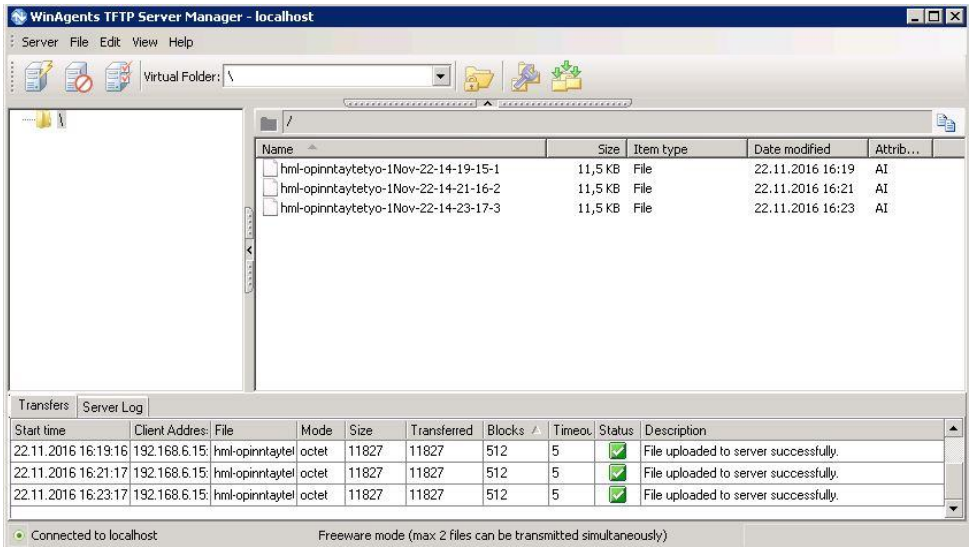
Automaattisesti kytkimen konfiguraation saaminen TFTP:lle vaatii aluksi toimivan yhteyden TFTP-palveluun, johon konfiguraatio halutaan viedä. Ciscon uudemmissa IOS-versioissa on käytössä archive-komento, jonka avulla kopiointi suoritetaan. Toisena varmuuskopioinnin käyttöönottoa helpottavana ominaisuutena, on käytössä oleva $h-muuttuja. $h-muuttujan avulla konfiguraatiotiedoston nimeksi saadaan isäntänimeä vastaava nimi.

Varmuuskopiointi onnistuu konfiguroimalla kytkimen konfiguraation arkistointiosioon polku, jossa TFTP-palvelu on. Käyttämällä $h-muuttujaa saadaan halutun kopion tiedoston nimeksi kyseessä olevan laitteen isäntänimi. Automaattinen varmuuskopio saadaan käyttämällä time-period-komentoa. Time-period-komennossa määritetään milloin varmuuskopio otetaan. Time-periodissa on käytössä vain minuutit, joten tarkkaa varmuuskopiointipäivää ei voida tämän komennon avulla suorittaa. Kuvassa 26 esitetään kytkimen konfiguraatioon lisätyt muutokset ja varmuuskopioiden tallennusväliksi on määritetty 2 minuuttia.

Kuva 26. Konfiguraatioon tarvittavat muutokset.

Kytkimen konfiguraation varmuuskopiointi voidaan tehdä tarvittaessa useastikin, riippuen organisaation tarpeesta. Koska yhdestä kytkimestä tuleva varmuuskopiotiedosto on pieni, ei nykypäivänä kiintolevytilan kanssa tule ongelmia. Jotta turhaa levytilaa palvelimella ei kuitenkaan käytetä, tarvittaessa kannattaa poistaa vanhoja varmuuskopioita.

WinAgents TFTP:stä nähdään palveluun automaattisesti tuodut konfiguraatiot. Konfiguraatiot ovat tulleen 2 minuutin välein ja niistä uusin selviää selkeästi järjestysnumerosta. WinAgentsin lokista voidaan tarkistaa, että konfiguraatio on toimitettu onnistuneesti palveluun. Kuvassa 27 nähdään, kuinka tiedostojen nimet ovat selkeät ja niitä erottaa päivämäärän ja kellonajan lisäksi järjestysnumero.



Kuva 27. Konfiguraatiotiedostot saatavilla uusimmasta vanhimpaan.

10 TOIMIMINEN VIKATILANTEESSA

Vikatilanne alkaa ilmoituksella. Ilmoitus viallisesta kytkimestä saadaan, joko NetEyen ilmoituksella tai käyttäjien toimesta. NetEye ilmoittaa ainoastaan, jos yhteys kytkimeen menetetään kokonaan, mutta käyttäjät saattavat ilmoittaa verkkoyhteyksien satunnaisesta katkoksista. Kun kytkinten vastuuhenkilö saa vikailmoituksen NetEye:sta, tarvitsee vastuuhenkilön etsiä kytkimen fyysinen sijainti.

Kytkimien kiireellisyys vaihtelee osastoittain. Kiireellisimmissä paikoissa kuten päivystys ja -synnytysosasto, saattaa kytkimen rikkoutuminen hankaloittaa huomattavasti hoitotyötä ja aiheuttaa vaaratilanteita, jos ei esimerkiksi saada potilastietoja nähtäville tarpeeksi nopeasti. Poliklinikoilla laiterikko saattaa aiheuttaa vastaanoton peruuntumisen, eikä vastaanottoa useasti pystytä jatkamaan ennen, kun vika on saatu korjattua.

Kun kytkin on löydetty fyysisesti, selvitetään tilanteen vakavuus. Ciscon laitteet ovat todella luotettavia. Pääsääntöisesti kun Ciscon kytkimeen katoaa yllättäen yhteys, kytkin on käyttökelvoton. Kytkin kannattaa kuitenkin koittaa käynnistää uudelleen ja samalla ottaa laitteeseen yhteyttä sarjakaapelilla. Jos kytkin todetaan käyttökelvottomaksi, tarvitsee hakea uusi vastaavaan käyttötarkoitukseen soveltuva kytkin.

Uusia kytkimiä pyritään pitämään kaikille tiedossa olevassa paikassa, josta kytkin on helposti saatavilla vikatilanteen sattuessa. Yleisimpiä Kanta-Hämeen keskussairaalassa käytettyjä kytkinmalleja on aina oltava saatavilla varalaitteina. Tarkoituksena on aina pyrkiä pitämään esikonfiguroituja kytkimiä valmiina hyllyssä. Näihin kytkimiin on valmiiksi konfiguroitu perusasetukset, kuten asetettu salasanat ja muut peruskäytänteet.

Uutta kytkintä vaihdettaessa paikalleen selvitetään, mitä laitteita kytkimeen on liitetty. Kytkimen verkkoportit kannattaa konfiguroida niin, että kaikki verkkoportit ovat työasemia varten. Normaalissa tilanteessa valtaosa kytkimeen liitetyistä laitteista ovat työasemia, poikkeuksena kiinteistövalvonnalle tai hoitajakutsujärjestelmälle varatuissa kytkimissä. Kuvassa 28 määritetään kaikki verkkoportit samaan VLAN:iin.

```
hml-opinntaytetyo-1(config-if-range)#interface range GigabitEthernet1/0/1-48
hml-opinntaytetyo-1(config-if-range)#switchport access vlan 10
hml-opinntaytetyo-1(config-if-range)#switchport mode access
```

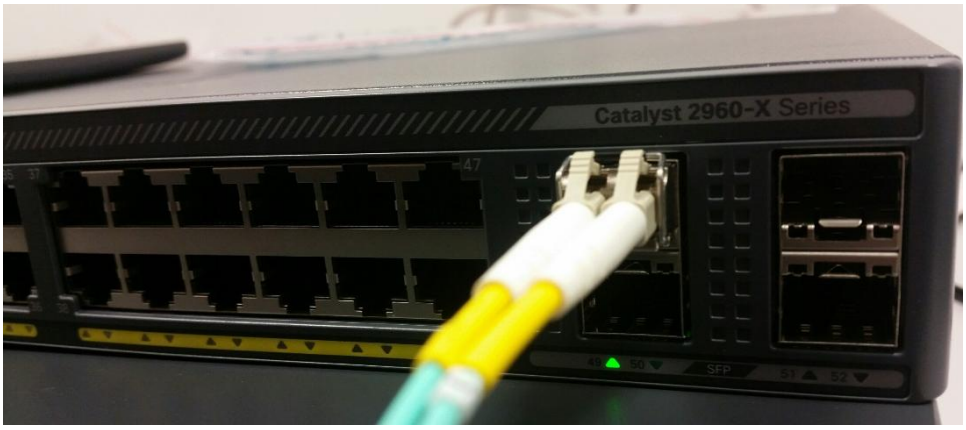
Kuva 28. 48 porttisen kytkimen verkkoportit määritelty kaikki samaan virtuaaliverkkoon.

Kytkimen SFP-portit määritellään oletuksena runkoyhteyksiksi, mitä kautta kytkin liitetään osaksi suurempaa lähiverkkoa. Tavallisissa verkkoporteissa pääsy on sallittu vain yhteen määriteltyyn VLAN:iin, kun taas runko määrityksellä kulkee kaikki VLAN:it. Kuvassa 29 konfiguroidaan kytkimen

SFP-portit runkoyhteykiksi ja kuvassa 30 porttiin numero 49 on kytkettynä SFP-moduuli.

```
hml-opinntaytetyo-1(config-if-range)#interface range GigabitEthernet1/0/49-52
hml-opinntaytetyo-1(config-if-range)#switchport mode trunk
```

Kuva 29. 48 porttisen kytkimen SFP-portit määritelty runkoyhteydeksi.



Kuva 30. Runkoyhteys kytkettynä SFP-moduulilla kytkimen porttiin numero 49.

Kun kytkin on vaihdettu ja selvitetty, mitä laitteita kytkimeen on liitettynä, pitää kytkimen porttien asetukset konfiguroida manuaalisesti. Porttiasetusten määrittämiseen menee huomattavan suuri osa ajasta, verrattuna muihin tehtäviin, kun kytkintä vaihdetaan. Manuaalisesti porttiasetusten määrittämisen lisäksi, tarvitsee tekijän myös tietää mihin VLAN:iin mikäkin laite kuuluu.

Kun kytkin on saatu paikalleen ja konfiguroitua se lisätään NetEye:n valvontaan. Jos kytkimelle on määritetty sama IP-osoite, kuin sillä jonka tilalle se on vaihdettu, niin lisäystä NetEye:hin ei tarvitse tehdä.

Tilanteessa jossa kytkimelle on ennalta määritetty automaattinen varmuuskopiointi, pystytään tilanteesta selviämään huomattavasti nopeammin. Kytkimen konfiguraation palauttaminen TFTP:lle kopioituneesta varmuuskopiosta, poistaa vaihtoprosessista kokonaan manuaalisten porttiasetusten määrittämisen.

Manuaalisten määritysten sijaan valitaan TFTP:ltä hajonneen kytkimen isäntänimeä vastaava konfiguraatiotiedosto. Konfiguraatiotiedostoa voidaan tarvittaessa vielä muokata tekstieditorilla ennen, kun se siirretään kytkimelle. Konfiguraation siirto kytkimelle suoritetaan kopioimalla koko konfiguraatiotiedoston sisältö esimerkiksi käyttämällä Windowsin pikakomentoja, ctrl+a valitsee koko tiedoston sisällön ja ctrl+c kopio tekstin leikepöydälle.

Uuteen paikalleen asennettu konfiguroimattomaan kytkimeen otetaan konsoliyhteys. Uusi kytkin on aina oletuksena käyttäjätilassa ja se vaatii korotuksen etuoikeutettuun tilaan enable-komennolla. Etuoikeutetusta tilasta siirrytään vielä config terminal-komennolla määritystilaan. Määritystilassa suoritetaan kytkimen konfigurointi painamalla hiiren oikeaa painiketta, joka tuo leikepöydällä olevan konfiguraation kytkimeen. Kytkin suorittaa konfiguraatiotiedoston mukaiset komennot automaattisesti. Kun kytkin on suorittanut konfiguroinnin, tarvitsee muistaa tallentaa kytkimelle tehdyt muutokset write memory-komennolla.

Kytkin on nyt konfiguroitu valmiiksi ja se voidaan tarvittaessa vielä päivittää. On huomioitava uutta laitetta vaihdettaessa vanhan tilalle, että vanhan laitteet verkkojohdot tulevat täsmälleen samoihin verkkoportteihin uudessa kytkimessä. Se onnistuu parhaiten laittamalla esimerkiksi uusi kytkin vanhan kytkimen alapuolelle ja siirtämällä johdot yksi kerrallaan laitteiden välillä.

11 YHTEENVETO

Opinnäytetyön lopputuloksena saavutettiin kehitetty ja nopeampi tapa toimia kytkimen vikatilanteessa. Kehitetyn varmuuskopioinnin ja päivitystavan myötä, koko prosessi on helpommin hallittavissa. Yksi tavoitteista oli nopeuttaa vikaantuneen laitteen vaihtoprosessia, joka toteutui uuden toimintatavan myötä hyvin. Toisena tärkeänä tavoitteena oli saada helpotettua prosessia siten, että kuka tahansa pystyisi tarvittaessa selviytymään vikatilanteesta. Tähän työ antaa hyvän pohjan, mutta vaatii vielä jatkokehitystä. Jatkosuunnittelussa pitäisi ainakin ottaa huomioon käyttöoikeudet, selkeämpi ohjeistus ja tarvittaessa koulutus.

Työssä käsiteltiin pintapuolisesti perusteet Ciscon konfiguroinnista ja selkeästä tavasta toteuttaa kytkimen varmuuskopiointi. Aiheeseen löytyy hyvin ohjeita internetistä ja kirjallisuudesta. Teoriaosuuden perusasiat eivät juuri ole ajansaatossa muuttuneet ja niihin löytyi useita samankaltaisia lähteitä. Työssä käytettyjen kytkinten konfiguraatioon ei perehdytty syvemmin, koska se olisi vaatinut valtavasti enemmän aikaa. Pyrittiin käymään läpi vain perusteet, jotka ovat olennaisia työn ja ominaisuuksien kannalta. Jos asiaan haluaa perehtyä syvemmin, Cisco tarjoaa hyvät tuki ja – ohjesivustot.

Toimeksiantajan puolesta ei annettu ennalta vaatimuksia, miten työ tulisi toteuttaa. Opinnäytetyössä syntyneeseen ratkaisuun päästiin ensin selvittämällä nykyinen toimintatapa ja tilanne Kanta-Hämeen sairaanhoitopiirissä. Ratkaisu ongelman korjaamiseen pohdittiin yhdessä KHSHP:n tietoliikenneinsinöörin kanssa. Toimeksiantaja on tyytyväinen opinnäytetyön lopputulokseen. Tätä opinnäytetyötä tullaan hyödyntämään ja jatkokehittämään tuotantokäyttöön asti.

Työn aikana opin paljon Cisco – laitteiden konfiguroinnista ja hallinnasta. Toteutuksen aikana käytin pääsääntöisesti Ciscon verkkosivuilta saatavia ohjeita ja dokumentteja. Tutustuin työssä vain yhteen pieneen osa-alueeseen, joka laitteilla voidaan tehdä. Se herätti minussa valtavaa mielenkiintoa jatkaa työskentelyä ko. laitteiden parissa ja kehittää omaa osaamista.

LÄHTEET

Cisco, n.d.a Cisco IOS Command Modes. Viitattu 18.10.2016
http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf019.html

Cisco, n.d.b Applying Correct Terminal Emulator Settings for Console Connections Viitattu 03.11.2016
http://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/9321-terminal-settings.html

Cisco, 30.lokakuuta 2013 Vip Perspectives. Viitattu 22.11.2016
https://learningnetwork.cisco.com/blogs/vip-perspectives/2013/10/30/understanding-cisco-auto-archive-feature-to-backup-configuration-file

Computer Hope, n.d. WAN. Viitattu 5.10.2016
http://www.computerhope.com/jargon/w/wan.htm

Daniweb, n.d. What does 10baseT means?. Viitattu 17.10.2016
https://www.daniweb.com/hardware-and-software/networking/threads/304394/what-does-10baset-means

Fiber optic tutorial, 2016. Explanation of The Model of Cisco Switches. Viitattu 21.11.2016
http://www.fiber-optic-tutorial.com/explanation-of-the-model-of-cisco-switches.html

Flyktman, R. 2010. Suuri PC-käsikirja – Windows 7. Porvoo: Ws Bookwell Oy

Granlund, K. 2007. Tietoliikenne. Jyväskylä: WSOYpro

Helppari n.d. Kytkimet ja reitittimet. Viitattu 14.10.2016
http://www.helppari.fi/fi/tuotteet/kytkimet-ja-reitittimet.html

Häme-Wiki, n.d. Kanta-Hämeen keskussairaala. Viitattu 30.9.2016
http://www.hamewiki.fi/wiki/Kanta-H%C3%A4meen_keskussairaala

Koudata, n.d. Topologiat. Viitattu 2.10.2016
http://koudata.fi/node/585

Ladu, n.d. VLAN-perusteet. Viitattu 5.11.2016
http://ladu.htk.tlu.ee/erika/lasse/switch2/vlanperusteet.html

NetPrivateer, n.d. WAN. Viitattu 28.11.2016
http://www.netprivateer.com/lanwan.html

Okol, n.d. Johdanto verkkotekniikkaan. Viitattu 8.10.2016
http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kaytto_ja_kehittaminen/lahiverkko_internet/lanjaint/johdanto_verkkotekniikkaan/johdanto3.htm

STUK, 14. lokakuuta 2015. Langaton lähiverkko. Viitattu 6.10.2016
http://www.stuk.fi/aiheet/kodin-ja-toimiston-sateilevat-laitteet/langaton-lahiverkko

TechTarget, n.d. Cisco IOS. Viitattu 18.10.2016
http://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System

TestOut, 2016. TestOut Routing and Switching Pro. Viitattu 22.11.2016
http://cdn.testout.com/client-v5-1-10-385/startlabsim.html?culture=en-us

Tivi, 6. maaliskuuta 2016. Verkkolaitteet. Viitattu 17.10.2016
http://www.tivi.fi/CIO/ciscon-ote-ei-heltia-reititinbisneksissa-6310879

Tyypillinen lähiverkko, n.d. Viitattu 28.11.2016
http://nmt82.tripod.com/tietoverkot/f.html

Viestintävirasto, 2. syyskuuta 2014. Langaton lähiverkko. Viitattu 5.10.2016
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409021705.html

Web-opas, n.d. Mikä on reititin. Viitattu 8.10.2016
http://www.webopas.net/mika_reititin.html

WhatIs, 2016. Rack Unit. Viitattu 17.10.2016
http://whatis.techtarget.com/definition/rack-unit

Wikipedia, 29. elokuuta 2016. Cisco Catalyst. Viitattu 17.10.2016
https://en.wikipedia.org/wiki/Cisco_Catalyst