SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

VERKONVALVONTAJÄRJESTELMÄN KÄYTTÖÖNOTTO SIILINJÄRVEN KUNNALLE

Aruba Clearpass

TEKIJÄ: Lauri Kahari

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Lauri Kahari	
Työn nimi Verkonvalvontajärjestelmän käyttöönotto Siilinjärven kunnalle	
Päiväys 8.12.2020	Sivumäärä/Liitteet 20
Ohjaaja(t) Veijo Pitkänen / Pasi Liimatainen	
Toimeksiantaja/Yhteistyökumppani(t) Siilinjärven kunta	

Tiivistelmä

Opinnäytetyöni oli projektityö, jonka tavoite oli parantaa Siilinjärven kunnan verkkoympäristön hallittavuutta, luotettavuutta, käyttäjäystävällisyyttä ja tietoturvaa verkonvalvontajärjestelmän avulla. Clearpass on Aruba Networksin kehittämä ja hallinnoima verkonvalvontajärjestelmä.

Clearpass konfiguroitiin jokaiseen kunnan verkkokytkimeen. Sen ylläpito, muokkaus ja laite- tai käyttäjäkohtaiset määritykset tehdään Clearpassin omalla hallintasivulla. Clearpass hyödyntää 802.1X – autentikointia ja se tunnistaa Clearpass-kytkimiin liitetyt päätelaitteet ja niiden käyttäjät. Se todentaa käyttäjän oikeudet sekä tietokoneen määritykset, ja niiden perusteella määrittelee mihin verkkoon käyttäjällä on oikeus päästä. Clearpass osaa myös tunnistaa eri laitetyyppejä ja sen perusteella esimerkiksi sijoittaa tulostimet tulostusverkkoon.

Avainsanat
Tietoverkon monitorointi ja hallinta

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Lauri Kahari			
Title of Thesis Implementation of network access control software			
Date	8 December 2020	Pages/Appendices	20
Supervisor(s) Veijo Pitkänen / Pasi Liimatainen			
Client Organisation /Partners Municipality of Siilinjärvi			

Abstract

The goal of this project was to improve manageability, reliability, security, and user experience of network environment in municapility of Siilinjärvi. Clearpass is a network access control software, developed and managed by Aruba Networks.

Clearpass is configured on each switch in the network. Management, configuration, and device- or user specific settings are managed on its own maintenance site. Clearpass uses 802.1X -authentication and it identifies the devices and the users which are connected to clearpass switches. It inspects several different specifications from the device and the user, and determines on which network the user belongs to, or what rights does the user have. Clearpass can also identify different device types.

Keywords
Data network monitoring and management

SISÄLTÖ

Lyhenteet ja määritelmät

Kytkin	pakettikytkentäisen verkon yhdistämiseen käytetty laite
Kytkinportti	Yksi kytkimen Ethernet-porteista (RJ45)
IEEE 802.1X	porttikohtaisen todentamisen standardi (Ethernet ja wlan)
kofigurointi	Määritysten ja asetusten muokkaus
valokuitu	(valokaapeli), tiedonsiirtotekniikka
Ethernet	Lähiverkkotekniikka IEEE 802 – standardissa.
LAN	lähiverkko (tietoliikenneverkko, jolla on rajoitettu alue)
WLAN	Langaton lähiverkko IEEE 802 – standardissa
IEEE 802	LAN ja MAN –verkkojen standardi
DJK	Datajakamo, yhteydenjakokaappi
Trunk	uplink kytkinportti, jaetaan vlaneja kytkinten välillä
VLAN	Virtuaalilähiverkko, fyysinen verkko jaetaan loogisiin osiin
HUB	ethernet-muunnin, jakaa verkon useaan porttiin
PoE	Power over Ethernet, virransyöttö kytkimeltä päätelaitteelle datakaapelilla
Rima	RJ45-paneeli, johon tuodaan kaapelit kiinteistön datarasioista
Ohjuri	Kaapeliohjuri, johon sijoitetaan kytkimelle tulevat datakaapelit
SNMP	Simple Network Management Protocol, protokolla verkkolaitteiden etämonitorointiin

1 ARUBA CLEARPASS

Clearpass on Aruba Networksin kehittämä ja hallinnoima verkonvalvontajärjestelmä. Clearpass on kehitetty hallinnoimaan organisaation verkkoympäristöä, sekä vahvistamaan verkon suojausta.

Clearpass otettiin käyttöön kaikissa kunnan verkkokytkimissä. Sen ylläpito, muokkaus ja laite- tai käyttäjäkohtaiset määritykset tehdään Clearpassin omalla hallintasivulla. Yksittäisellä kytkimellä porttikohtainen käyttäjän todentaminen perustuu 802.1X – autentikointiin. Tietyissä tilanteissa käytetään mac-todennusta, jolla Clearpass tunnistaa päätelaitteen laitetyypin ja -mallin.

Verkonvalvonta käy läpi erilaisia parametreja liittyen laitteeseen ja käyttäjään, ja niiden perusteella määrittelee mihin verkkoon käyttäjällä on oikeus päästä. Clearpass tunnistaa laitetyypit mac-osoitteen perusteella, jolloin esim. tulostimet se osaa sijoittaa mahdolliseen tulostusverkkoon.

1.1 Käyttötarkoitus ja toiminta

Clearpassin käyttöönotolla on laaja vaikutus koko Siilinjärven verkkoympäristöön ja työntekijöiden päivittäiseen arkeen. Clearpassin käyttönotolle on monia perusteita, mutta päällimmäisenä niistä on sen tuoma verkon suojaus ja sitä kautta kehittyneempi tietoturva koko kunnassa. Siilinjärven verkkoympäristössä on käytössä useita eri virtuaalilähiverkkoja (vlania) ja niiden käyttötarkoitus on määritetty tarkasti.

Yhdessä toimistorakennuksessa saattaa työskennellä sosiaali- ja terveyspalveluiden, hallinnollisten palveluiden, sekä sivistyspalveluiden työntekijöitä. Näille kaikille palvelualoille on oma verkkonsa, mitä he tarvitsevat päivittäisessä työskentelyssään. Verkko toimistohuoneiden datarasioihin tulee kerroksen datajakamokaapilta, jossa on verkkokytkimiä. Datarasiaan voi tulla kerrallaan vain yksi verkko, joka kyseisen kytkimen kytkinporttiin on määritetty. Henkilöstöä vaihtuu ja työpiste saattaa muuttua. Jos työhuoneeseen tarvitaan eri verkkoa, tulee asiakkaan olla yhteydessä tietotekniikkapalveluihin ja pyytää vaihtamaan verkko. Clearpass tunnistaa käyttäjän, ja mihin verkkoon hänellä on oikeus päästä. Clearpass asettaa kytkinporttiin henkilölle oikean verkon automaattisesti.

Kullakin vlanilla on oma käyttäjäkuntansa, joten tiettyyn verkkoon tulee päästä vain käyttäjä, jolla on vaadittavat oikeudet. Myös muille käyttötarkoituksille, esim. verkkotulostukselle ja kytkinhallinnalle, on omat verkkonsa. Verkkoympäristö, jossa Clearpass toimii, on turvallinen ja ylläpitäjän näkökulmasta selkeä, sekä helppokäyttöinen. Käyttäjän ei tarvitse ottaa yhteyttä service deskiin, jos hän tarvitsee eri verkon mitä datarasiasta tulee. Tavoitteena on parantaa tietoturvaa, luoda työntekijöille parempi verkon käyttökokemus, sekä monitoroida verkon käyttöastetta ja laitekantaa.

1.2 Verkonvalvonta

Clearpassin verkonvalvonta ja pääsynhallinta perustuvat mm. 802.1X – autentikointiin ja mac-osoitteen avulla tehtävään laitetunnistukseen. Kun laite liittyy kunnan verkkoon, Clearpass määrittää laitteelle oikean verkon käyttäjätunnuksen oikeuksien ja roolin avulla.

802.1X – autentikointi tunnistaa päätelaitteen käyttäjän käyttäjätunnuksen, etsii sen kunnan Active Directorysta ja tarkastaa käyttäjän roolin, sekä oikeudet. Mikäli päätelaitteen käyttäjällä ei ole asianmukaista tunnusta, laite tunnistetaan mac-todennuksella. Tämän jälkeen näiden kahden todennuksen pohjalta voidaan määrittää käyttäjälle oikea verkko, jonka Clearpass sitten aktivoi kyseiseen kytkinporttiin.

Esim. kunnan lääkäri liittää työkoneen verkkoon ja kirjautuu tunnuksillaan, hänelle määritetään terveydenhuollon verkko. Mikäli käyttäjä on ns. vieras, eli hänellä ei ole oikeuksia päästä kunnan verkkoympäristöön, hänelle jaetaan kuitenkin avoin yhteys internetiin.

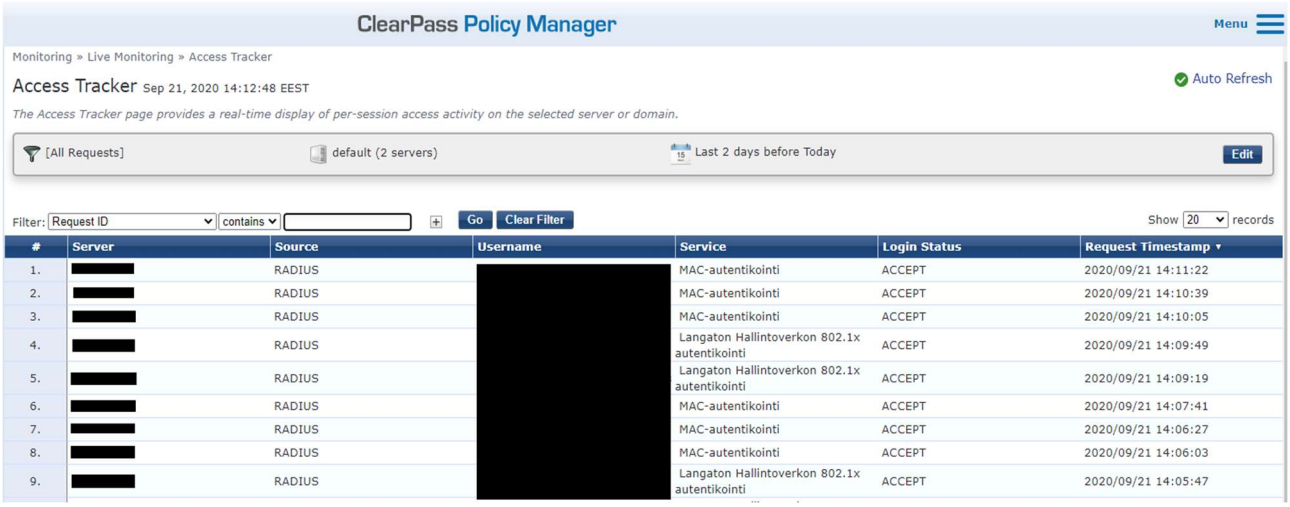
Kuva 1 / Kuvankaappaus Clearpassissa käyttöönotetusta vlanista, käytössä portissa 4.

1.2.1 Laitehallinta

Clearpass tunnistaa pääosan verkkoon liitetyistä päätelaitteista suoraan mac-osoitteen perusteella. Tunnistamisen avulla ylläpitäjät voivat monitoroida verkon laitekantaa ja käyttäjämieltymyksiä. Tämän avulla voimme taas räätälöidä muita palvelujamme käyttäjäkunnan tarpeiden mukaan.

1.3 Ylläpito ja määritykset

Clearpassia hallinoidaan sen omasta hallintaportaalista, Clearpass Policy Managerista. Tällä sivustolla ylläpitäjä voi muokata pääsynhallintamäärityksiä, laitehallinnan rekistereitä sekä Clearpassin toimintaa. Policy Managerista hallinnoidaan ainoastaan Clearpassin asetuksia, verkkolaitteiden määritykset tehdään eri kautta.



Kuva 2 / *Kuvankaappaus pääsynvalvonnan seurantanäkymästä.*

1.4 Aruba verkkokytkinten konfigurointi

Alla esimerkkejä ja selvityksiä joistakin Clearpassin konfiguraatioista. Nämä ovat siis laitekohtaisia asetuksia, jotka konfiguroidaan jokaiselle kytkimille erikseen.

radius-server host XXXX key XXXXX

avain on clearpassin autentikointipyyntöjä varten

radius-server host XXXX dyn-authorization

clearpass pystyy muuttamaan tällä asetuksella kytkinporttien vlaneja

radius-server host XXXX time-window plus-or-minus-time-window

radius-server host XXXX time-window 1000

Määritetään clearpass-palvelin + asetuksia

radius = autentikointimenetelmä kytkimen ja palvelimen välillä

radius-server dead-time 1

aikakatkaisu radius-palvelimeen yhdistämiselle

radius-server timeout 3

aikakatkaisu clearpassin autentikoinnille (käyttäjä)

radius-server retransmit 2

autentikoinnin uudelleenyritys 2kpl

aaa authentication port-access eap-radius authorized

määritetään radius ensisijaiseksi autentikointitavaksi (clearpass)

jos clearpass ei vastaa, autentikoinnissa käytetään porttiin määritettyä untagged vlania.

aaa accounting network start-stop radius

otetaan accounting käyttöön clearpassissa. Tunnistetaan kauanko sessio ollut aktiivinen + liikkuneen datan määrä

aaa accounting update periodic 2

accounting = pidetään kirjaa aktiivisesta sessiosta

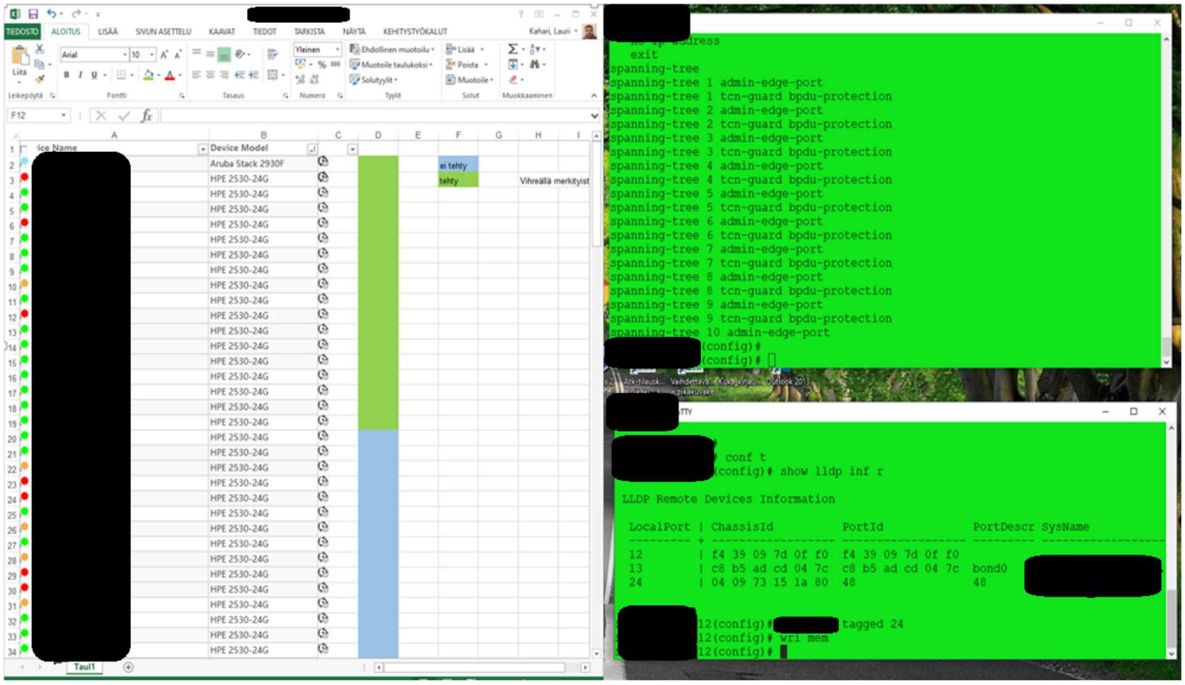
päivitetään accounting data 2 min välein

1.5 Käyttöönotto

Clearpassin käyttöönotto edellyttää, että kaikki kytkimet, jotka eivät ole Clearpass-yhteensopivia on vaihdettu asianmukaisiin kytkimiin. Laitevaihtojen jälkeen konfiguroimme tarpeelliset asetukset jokaiselle kytkimelle ja tukiasemalle. Tarkistusten jälkeen Clearpass aktivoidaan. Kaikki kytkimet vaativat useita konfiguraatiomuutoksia ennen Clerpassin varsinaista käyttöönottoa.

Ensimmäiseksi loimme verkkoympäristöön kokonaan uuden virtuaalisen lähiverkon, jota käytetään alustana laitetunnistukselle. Tämä vlan lisätään jokaiselle kytkimelle IMC:llä, mutta se täytyy käydä manuaalisesti lisäämässä jokaisella kytkimellä kaikkiin uplink-portteihin, jotka johtavat toiselle kytkimelle. Samalla tarkistettiin kokonaan kytkimen konfiguraatio, että kaikki määritykset ovat clearpassin käyttönottoa ajatellen kuten pitääkin.

Saatuani kaikki kytkimet vaihdettua, aloitimme käyttöönoton tukiasemien konfiguroinnista. Tukiasemat ovat langattoman verkon jakamiseen käytettäviä laitteita, joita on kytketty suureen osaan kytkimistä. Tukiasemien hallinnoinissa otettiin käyttöön PEAP-autentikointi.



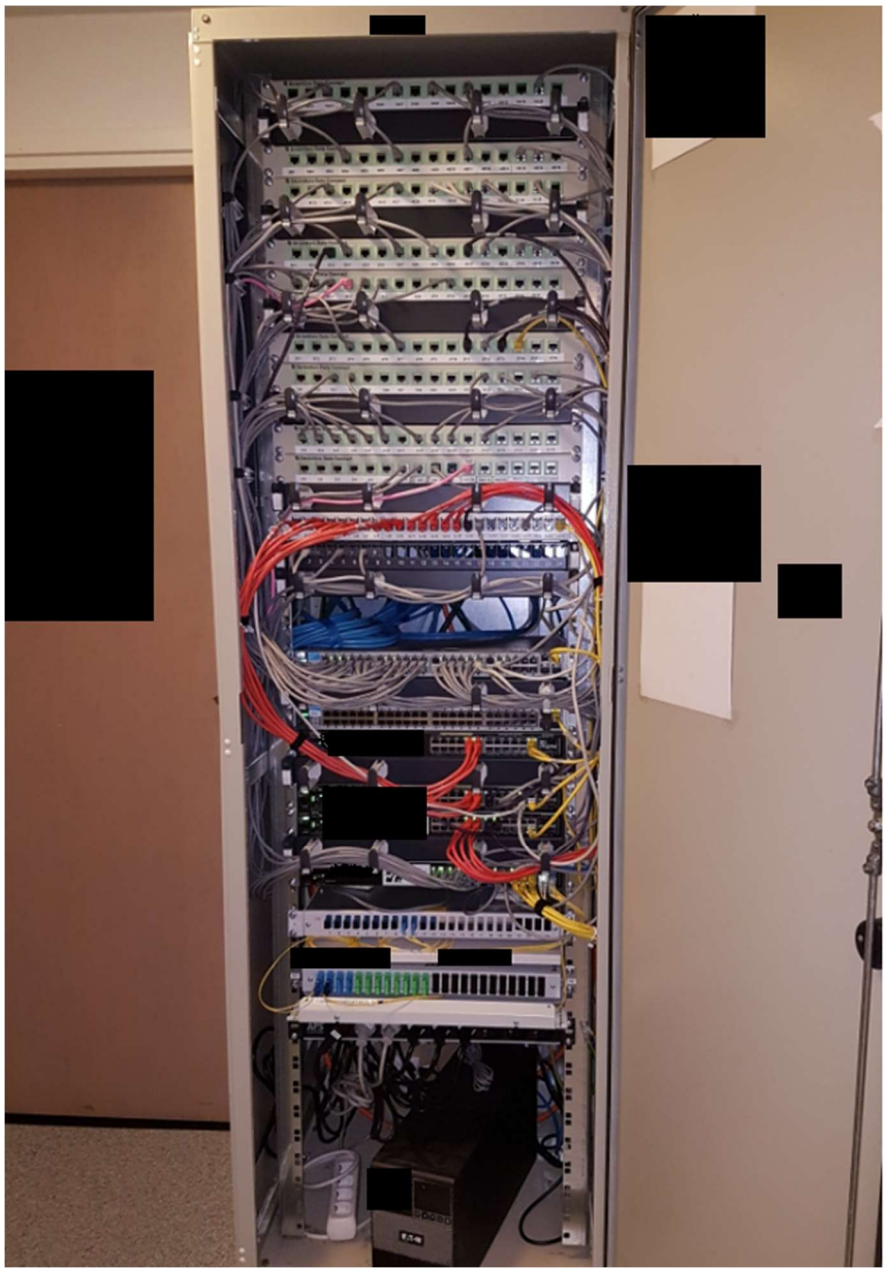
Kuva 3 / Uuden virtuaalisen lähiverkon lisäys kytkinten uplink-portteihin.
Lisäys tehtiin manuaalisesti lähes 200 kytkimeen.

2 VERKKOLAITTEET

Kunnan tietoverkossa on monenlaisia eri laitteita. Kytkimiä ja tukiasemia löytyy lähes jokaisen kiinteistön kaikista kerroksista. Kytkimet sijoitetaan räkkeihin ja nämä taas ovat useimmiten datajakamoissa, eli suljetuissa tietoliikennekaapeissa. Datajamoiden tyypillistä sisältöä ovat rimat, UPS:it, kytkimet, ja POE-injektorit.

2.1 Datajakamokaapit

Datajakamo (DJK) on siis tietoliikennekaappi, johon sijoitetaan tietoliikenteelle tarpeelliset laitteet. Isoissa kiinteistöissä jakamoita on usein yksi jokaisessa kerroksessa. Tietoliikennettä ohjataan kytkimillä, jos yhteyksille on kiinteistöissä paljon käyttöä, saattaa djk:ssa kulkea jopa satoja datakaapeleita.



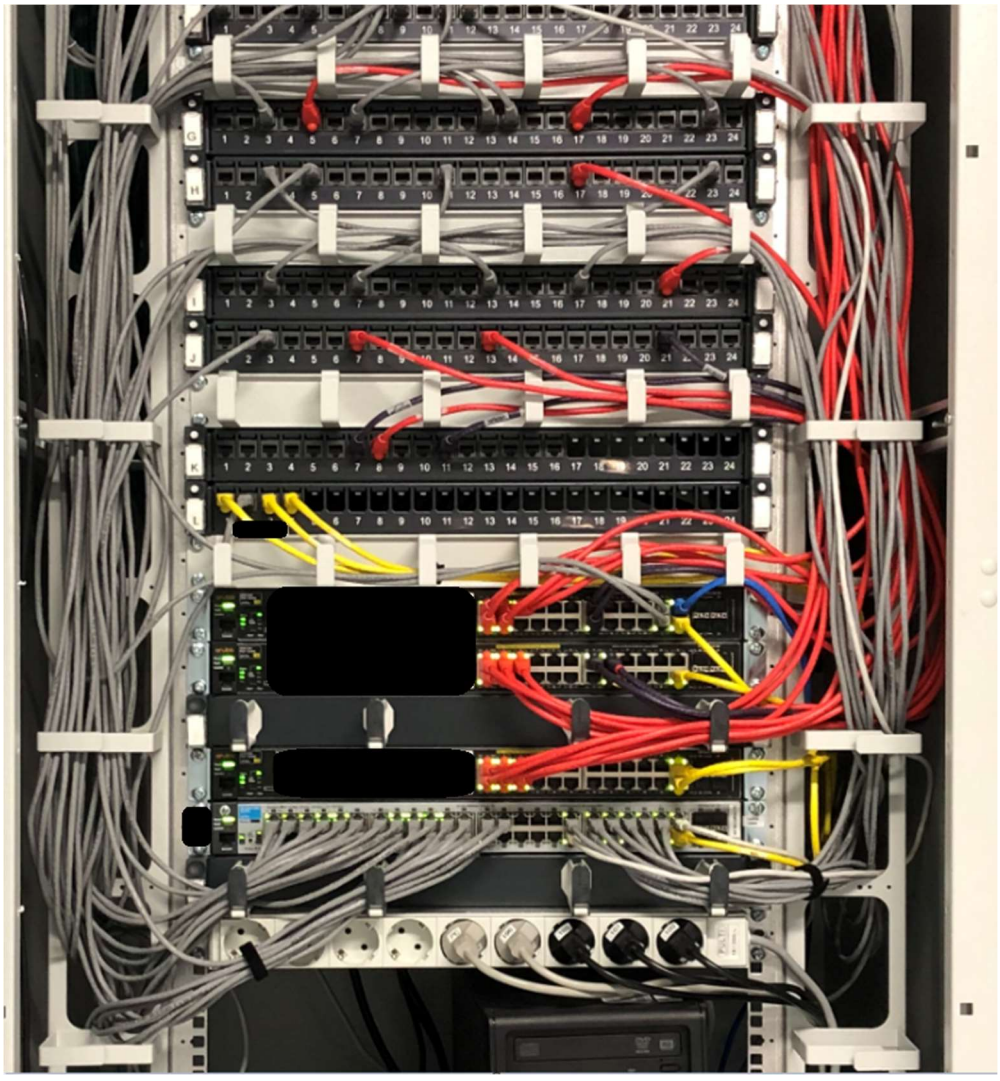
Kuva 4/ Kuvassa DJK, jossa useita kytkimiä, kaapelirimoja ja UPS

2.2 Kytkimet

Projektityöni oleellisin osa ovat kytkimet. Kytkin on laite, jolla yhdistetään paikallisverkon osia. Kytkin siis vastaanottaa tietoliikennepaketteja ja lähettää ne tietoverkossa eteenpäin paketin vastaanottajan mac-osoitteen mukaisesti. Siilinjärvellä käytetään Aruba Networksin valmistamia kytkimiä.

2.2.1 Kytkinmallit

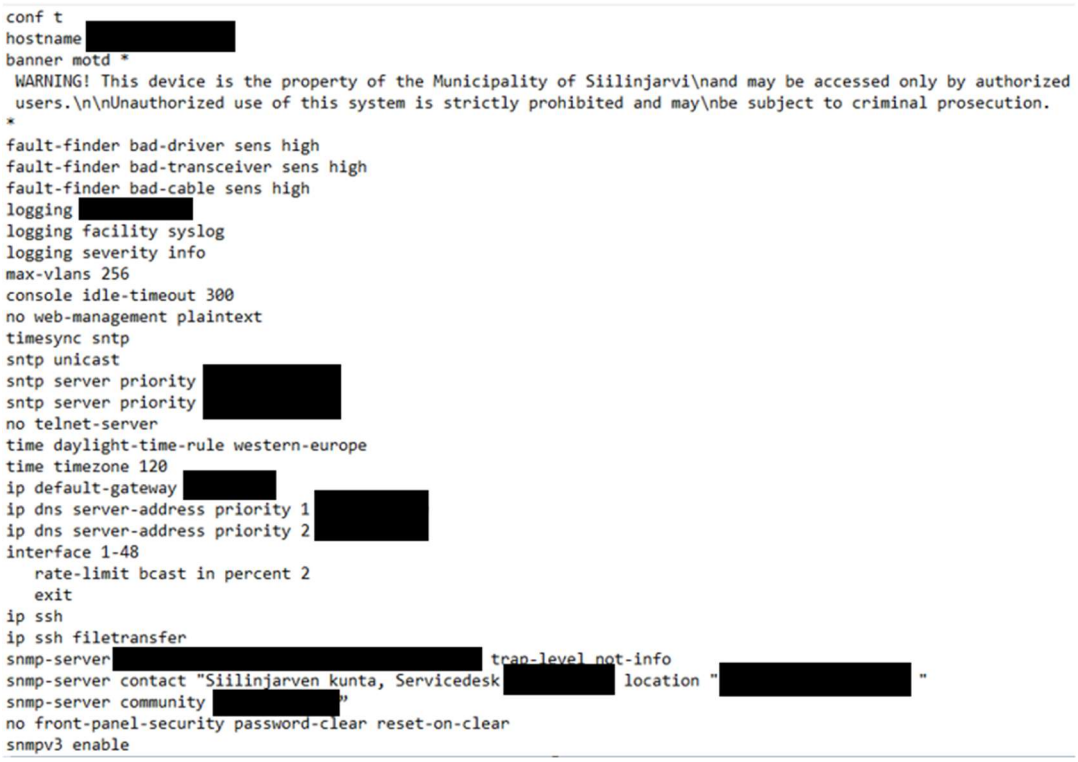
Kunnalla on käytössä useita erilaisia kytkimiä, merkittävin ero kytkimissä on kytkinporttien lukumäärä. Siilinjärvellä tyypillisimmät kytkimet ovat 24- ja 48-porttisia kytkimiä, mutta joihinkin tarkoituksiin voi olla esim. 8-porttisia kytkimiä. Toinen merkittävä ominaisuus kytkimillä on PoE (Power over Ethernet). PoE -kytkin pystyy syöttämään päätelaittelle virtaa datakaapelia pitkin. Tätä ominaisuutta hyödynnämme esim. tukiasemien ja valvontakameroiden kanssa. PoE ominaisuutta näkee Siilinjärvellä käytössä lähinnä 24 ja 8-porttisissa kytkimissä.



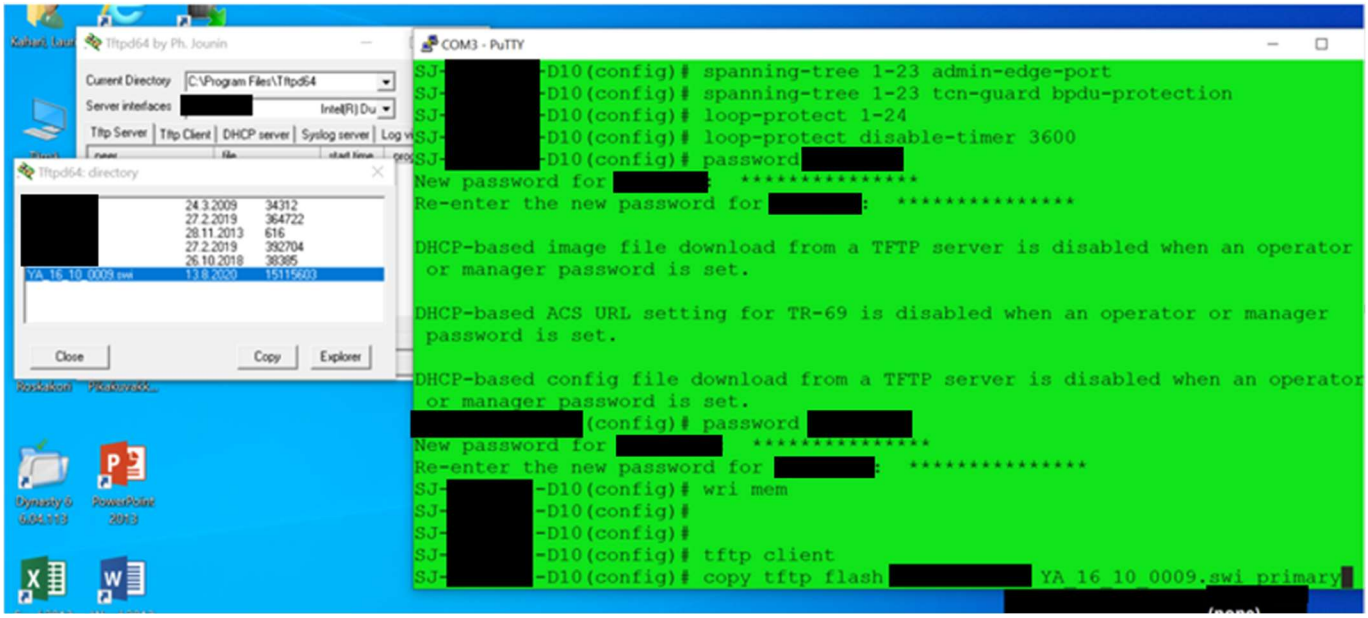
Kuva 2 / Kuva DJK:sta, jossa on 24-porttisia PoE-kytkimiä ja 48-porttinen kytkin.

2.2.2 Konfiguraatio

Kytkinten konfigurointi tapahtui projektissani kolmessa eri vaiheessa. Aluksi kytkimeen määriteltiin perusasetukset, eli konfiguraatio, joka määritetään jokaiseen kunnan tietoverkkoon tulevaan kytkimeen. Tässä konfiguraatiossa määritellään mm. yleisimmät vlanit, kytkimen tiedot, ylläpitäjän tunnukset, SNMP määritykset, tarvittavat ip-määritykset, spanning tree, yms. Alla esimerkkejä.



Kuva 3 | *Kuvankaappaus osasta "peruskonffia", eli konfiguraatiosta, joka ajetaan jokaiselle uudelle kytkimelle käyttöönoton alkuvaiheessa.*



Kuva 4 / *Kuvankaappaus laiteohjelmiston päivityksestä TFTP:llä*

3 LAITEVAIHDOT

Laitevaihdot olivat projektin isoin osa työajassa mitattuna. Vaihdettavia kytkimiä tuli loppujen lopuksi 36 kappaletta ympäri Siilinjärveä eri kiinteistöissä. Toimivan kytkimen vaihto toiseen on monivaiheinen projekti, joka täytyy suunnitella ja toteuttaa tarkasti, että kiinteistön työntekijöiden verkkokatko jäisi mahdollisimman lyhyeksi. Alla näkyy osa kytkinten vaihtolistastani.

3.1 Työvaiheet

Laitevaihtojen ensimmäinen työvaihe on sopia kiinteistön henkilöstön kanssa ajankohta kytkimen vaihdolle. Henkilöstöä tulee tiedottaa asianmukaisesti verkkokatkoista ja niiden vaikutuksista. Tämän jälkeen kartoitetaan vanhan kytkimen käyttöaste ja laitekanta. Jos kytkimellä on useita käyttäjiä, tukiasemia tai valvontakameroita, on tärkeää minimoida käyttökatkon kesto.

Tämän jälkeen konfiguroidaan uusi kytkin valmiiksi. Peruskonfiguraation lisäksi kytkin lisätään laitehallinta- ja monitorointijärjestelmiin sekä myös laiteohjelmisto tulee päivittää uusimpaan versioon. Lopuksi selvitetään, mitä vlaneja vanhalla kytkimellä on ja mitkä portit siellä ovat käytössä. Uudessa kytkimessä voi olla eri määrä valokuitu- ja/tai kuparikaapeliportteja, joten vanhat määritykset eivät välttämättä täsmää uuden kytkimen kanssa.

3.1.1 Suunnitelma

Jokaisen kytkimen vaihto tulee siis suunnitella tarkasti. Vaihdettava kytkin voi esim. viedä verkkoa muillekin kytkimille, jolloin vaihdon takia saattaa aiheutua verkkokatkos useassa eri kiinteistössä. Yhteensopivuusongelmia voi esiintyä myös kuituyhteyksien kanssa, vanha kuitusovitin ei välttämättä toimikkaan uudessa kytkimessä. Kytkinvaihdon ajankohta tulee sopia erikseen kiinteistön henkilöstön kanssa, ettei verkkokatko osu pahaan ajankohtaan kiinteistön henkilöstön työtehtävien näkökulmasta.

3.1.2 Valmistelut

Kytkinvaihdon valmistelut oli tehtävä huolellisesti, se on perusta sulavalle ja ongelmattomalle vaihdolle. Kaikki kytkinvaihtoni eivät sujuneet ongelmitta tai sulavasti ja usein sen syynä olivat puutteelliset tai huolimattomat valmistelut.

Vanhan kytkimen verkkoympäristön kartoitus tuli suorittaa huolellisesti. Monesti vanhoissa kytkimissä kytkennät on tehty huolimattomasti eli ne saattavat olla sotkussa, ilman värikoodeja tai ilman loogista järjestystä. Kytkimelle tulee kirjautua ja tarkastaa mitä verkkoja missäkin portissa kulkee ja mitä laitteita kytkimeen on liitetty.

Minun täytyi huolehtia, että värikoodit ovat kunnossa (esim. työasemakaapelit ovat harmaita, uplink-kaapelit keltaisia, UPS-kaapelit ovat siniset, jne.) ja että kytkentäjärjestys on suunnitelmamme mukainen, eli uplink-portit ovat kytkimen viimeisiä portteja. Mahdollisesti sotkuinen kaappi tulee myös järjestää uuden kytkimen asennuksen yhteydessä, eli suunnittelin mitä kautta kaapissa kaapelit vedetään, tulisiko asentaa uusi ohjuri, tai pitäisikö lyhyitä kaapeleita vaihtaa pidempiin.

3.1.3 Toteutus

Toteutus aloitetaan asentamalla uusi kytkin kytkinräkkiin. Uuteen kytkimeen myös kytketään virta ennen vaihdon suorittamista. Uuden kytkimen tulisi olla mahdollisimman lähellä vanhaa, että kaapelien pituus riittää suoraan siirtoon vanhasta kytkimestä uuteen.

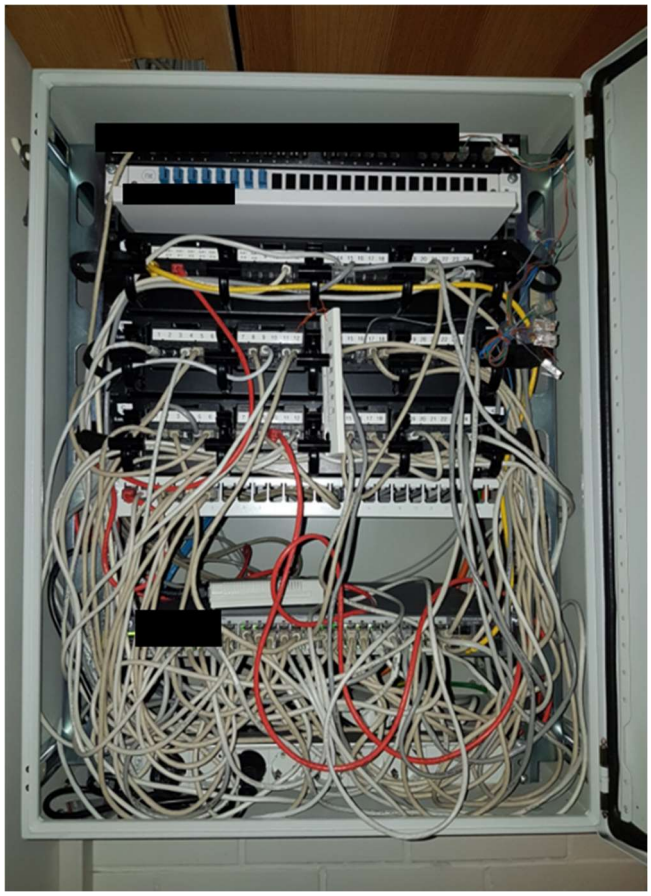
Kun uusi kytkin on asennettu ja päällä, varmistetaan, ettei kaapeleita tai muita irtaimistoa jää vaihdon aikana tielle. Usein jotkut kaapelit ovat liian lyhyitä kulkemaan kaapin sivussa, joten ne sattavat jäädä vaihdon jälkeen vanhan kytkimen eteen, jolloin vanhaa kytkintä ei saakkaan otettua pois räkistä ilman kaapeleiden irroitusta.

Kytkimet ovat nyt valmiita sulavaan vaihtoon, tässä kohtaa tulee varmistaa, että kiinteistön henkilöstö on tietoinen vaihdosta ja yhteyskatkosta. Mikäli käytössä on kuitukaapeleita, vaihdetaan kuitukaapeli ensin ja todennetaan, että uusi kytkin tunnistaa kuitumoduulin. Joskus moduuli saattaa olla niin vanhaa mallia, että uusi kytkin ei ole sen kanssa yhteensopiva. Tällöin poistetaan vanha moduuli, puhdistetaan kuitujohtojen päät kuituputsarilla ja liitetään kuitu uuteen moduuliin. Kuitujen jälkeen siirretään uplink-kaapelit ja todennetaan, että uusi kytkin pääsee verkkoon ja tarkastetaan yhteyden toimivuus. Seuraavaksi siirrämme kaikki loput kaapelit.

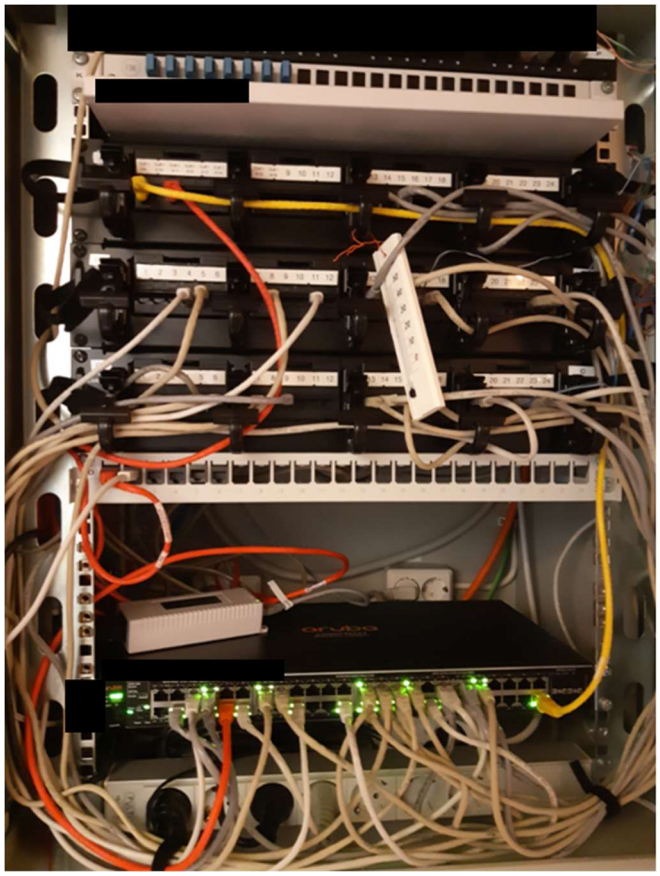
3.1.4 Jälkitarkastus ja muut toimenpiteet

Kun kaikki kaapelit saatiin onnistuneesti vaihdettua, tarkastettiin yhteyksien toimivuus. Hyvä käytäntö on varmistaa henkilöstöltä, että heidän työasemillaan toimii kaikki järjestelmät normaalisti. Tämän jälkeen aloitin kaapin siivouksen, aluksi poistin vanhan kytkimen, sekä sen mukana tarpeettomat kaapelit, kuten virtakaapeli, ja mahdolliset ylijääneet datakaapelit. Ennen vanhan kytkimen vaihtoa voi tarkastaa, paljonko portteja on ollut käytössä.

Esimerkiksi jos löytyy useita portteja, joissa on työasemakaapeli kiinni, mutta ei siirrettyä dataa yhtään useisiin kuukausiin, ei portti silloin ole käytössä. Tällaisista epäaktiivisista porteista tulee kerätä kaapelit pois, näin saadaan kaappiin lisää tilaa ja lopputulos on siistimpi.



Kuva 5 / DJK ennen kytkinvaihtoa



Kuva 6 / sama DJK kytkinvaihdon jälkeen

4 MUUT JÄRJESTELMÄT

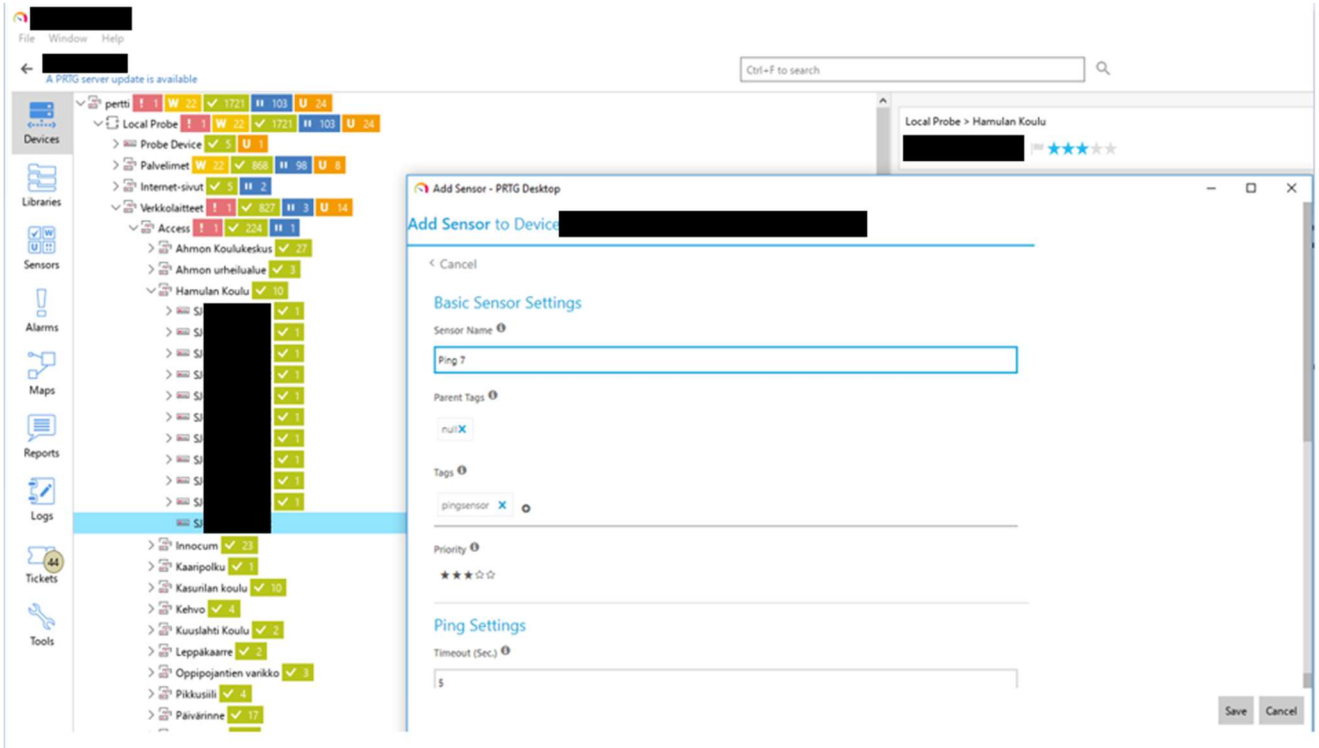
Tietoliikennelaitteiden ylläpidossa käytetään useita muitakin sovelluksia ja järjestelmiä. Reaaliaikainen monitorointi ja seuranta on tärkeää, etenkin vikatilanteiden sattuessa. Satojen laitteiden ylläpidossa yhteinen hallintasivusto parantaa kokonaiskuvaa ja tuo helppokäyttöisyyttä.

4.1 Laitehallinta ja monitorointi

Tärkeimmät järjestelmät ovat PRTG (laitemonitorointi) ja IMC (ylläpito). Uuden kytkimen käyttöönotossa tulee varmistua siitä, että uudet laitteet lisätään asianmukaisesti molempiin järjestelmiin, ja että poistettavat laitteet hävitetään asianmukaisesti kummastakin. Sekä PRTG, että IMC saavat monitorointidatansa kytkimiltä SNMP:n avulla, SNMP konfiguroidaan kytkimiin heti käyttöönoton yhteydessä, kun asennetaan ns. peruskonfiguraatio.

4.1.1 PRTG

PRTG on järjestelmä, jolla kunta monitoroi tietoteknisten laitteidensa kuntoa ja suorituskykyä etänä. Tietoliikennelaitteiden lisäksi PRTG:ssä on mm. palvelimet, UPS:it ja palomuurit.

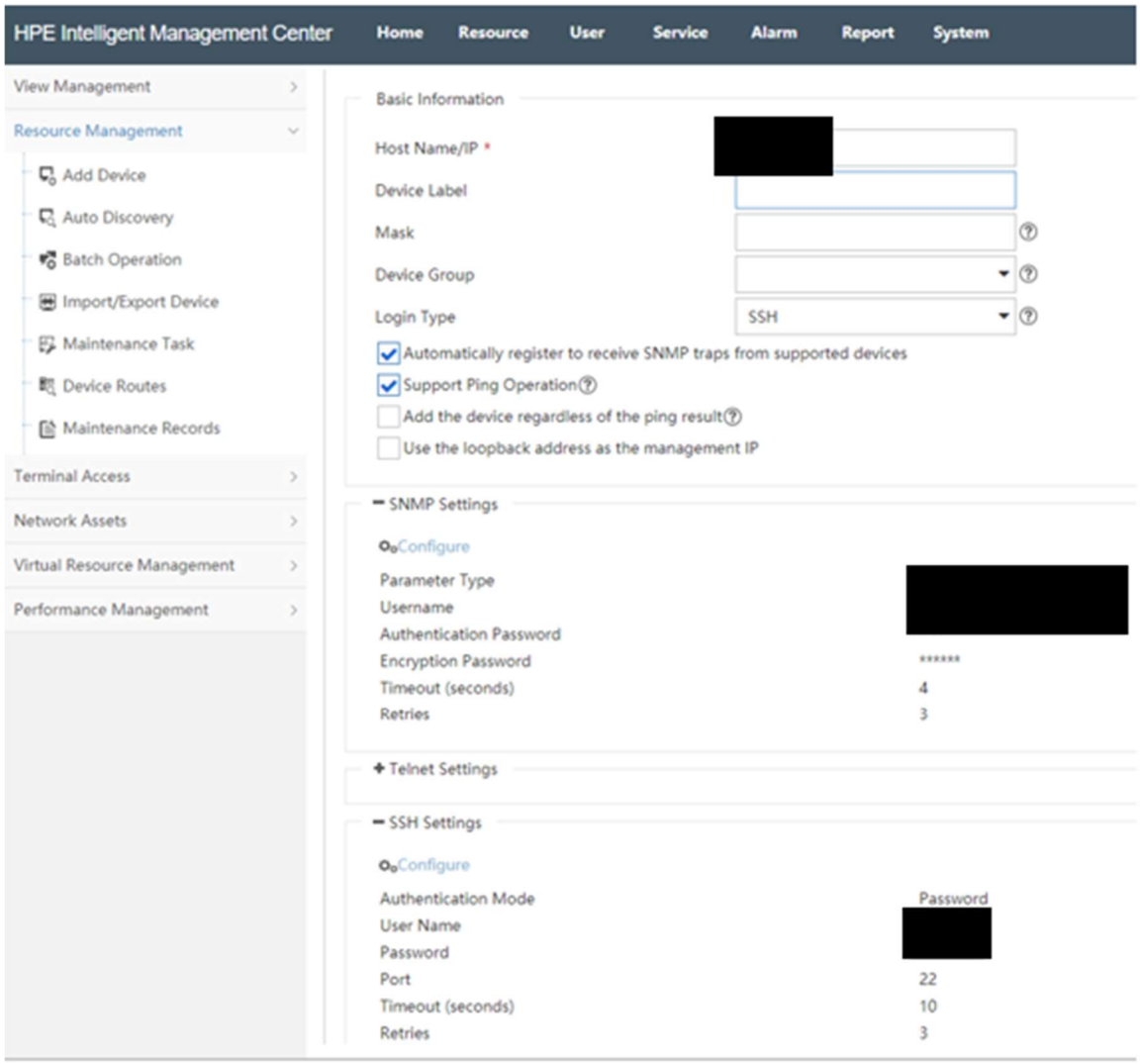


Kuva 7 / Kuvankaappaus PRTG:stä. Olen juuri lisännyt uuden kytkimen laitevalvontaan ja määritän laitteelle ping-sensoria.

4.1.2 IMC

Toinen tärkeä järjestelmä on HPE:n oma tuote, IMC (Intelligent Management Center). IMC:n kautta pystymme hoitamaan monia kytkinten monitorointiin ja ylläpitoon liittyviä tehtäviä, myös verkkotopologian ylläpito tapahtuu IMC:ssä. IMC:ssä on mahdollisuus esimerkiksi määrittää kytkimille yksinkertaisia konfiguraatiolisäyksiä tai muutoksia, joko yksitellen, tai useammalle kytkimelle kerrallaan.

Yksi IMC:n tärkeistä ominaisuuksista on varmuuskopiointi. IMC varmuuskopioi jokaisen kytkimen konfiguraation kerran päivässä, ajantasainen varmuuskopio verkkolaitteiden konfiguraatiosta on tärkeä mm. vikatilanteiden ja laitevaihtojen kannalta. Myös minun tekemissä laitevaihdoissa tarkistin jokaisen kytkimen vlan-konfiguraation, että osasin tehdä myös uudelle kytkimelle vastaavanlaisen.



Kuva 8 / Kuva IMC:stä, olen juuri lisäämässä konfiguroimaani uutta kytkintä palveluun, verkkotopologiakarttaan ja varmuuskopiointia varten.

5 LOPPUTULOS

Opinnäytetyöni tavoite oli ottaa Aruba Networksin Clearpass -verkonvalvontajärjestelmä käyttöön Siilinjärven kunnan verkkoympäristössä. Työ saatiin valmiiksi tavoiteajassa, ja projekti eteni suunnitelman mukaisesti jokaisessa vaiheessa.

Satunnaisia ongelmia esiintyi työni aikana, mutta ongelmatilanteisiin löytyi ratkaisu lähes joka tilanteessa nopealla aikataululla. Isoimmat haasteet esiintyivät laitevaihtojen yhteydessä, missä saattoi törmätä joko yhteensopivuus-, aikataulu-, tai laitekohtaisiin ongelmiin. Poistettavissa kytkimissä oli tapauskohtaisesti merkkitäviä eroja uuden kytkimen kanssa. Ongelmatilanteet ratkesivat kuitenkin nopeasti vianetsinnän ja asiantuntevan työtiimin ansiosta.

Opinnäytetyöni aikana kerrytin paljon arvokasta kokemusta verkkoympäristön ylläpidosta, laitteiden toiminnasta ja vikatilanteiden ratkaisusta. Kehityin työni aikana näillä osa-alueilla merkittävästi ja tästä kokemuksesta on varmasti hyötyä tulevaisuudessa. Työni tilaaja ja työn kirjoittaja olivat lopputulokseen tyytyväisiä.

LÄHDELUETTELO

Aruba Networks. (ei pvm). *Network Acces Control*. Haettu 20. Lokakuu 2020 osoitteesta https://www.arubanetworks.com/products/security/network-access-control/

Aruba Networks. (ei pvm). *Network Clearpass*. Haettu 18. Lokakuu 2020 osoitteesta https://www.arubanetworks.com/products/security/network-access-control/secure-access/

Wikipedia. (ei pvm). *Wikipedia*. Haettu 30. Syyskuu 2020 osoitteesta https://fi.wikipedia.org/wiki/IEEE_802.1X

Wikipedia. (ei pvm). *Wikipedia*. Haettu 10. Lokakuu 2020 osoitteesta https://fi.wikipedia.org/wiki/Ethernet

HPE. (ei pvm). *Hewlett Packard Enterprise.* Haettu 20. Marraskuu 2020 osoitteesta https://www.hpe.com/us/en/networking.html