LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Network Access Control

Aruba Clearpass

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Antti Ketoluoto

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KETOLUOTO, ANTTI: Network Access Control
Aruba ClearPass

Tietoliikennetekniikan opinnäytetyö, 38 sivua

Kevät 2017

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli selvittää, voidaanko Aruba ClearPass-järjestelmällä suorittaa Ethernet-verkkoon liitettävien päätelaitteiden VLAN-konfiguraation automatisointi. Selvityksen jälkeen järjestelmä toteutettiin tulostin- ja kiinteistövalvonnan verkkoihin. Kohdeympäristönä on Lahden kaupungin verkko, jota työn toimeksiantaja Lahden Tietotekniikka ylläpitää.

Aruba ClearPass on verkkoon pääsyn hallinnassa käytettävä järjestelmä, joka suorittaa päätelaitteiden RADIUS-autentikointia. Järjestelmällä voidaan myös toteuttaa IEEE 802.1X -standardin mukaista porttikohtaista autentikointia. Porttikohtaisen autentikoinnin tavoitteena on estää luvattomien päätelaitteiden liikenne verkon liityntäpisteen kautta. RADIUS on AAA-mallin mukainen tietoliikenneprotokolla, jolla verkkoon pyrkivän päätelaitteen tunnistautumistiedot välitetään autentikointipalvelimelle autentikointia varten.

Opinnäytetyön käytännön osuudessa tutkitaan jo kaupungin langattomissa verkoissa käytössä olevaa ClearPass-järjestelmää ja sitä, miten VLAN-konfiguraation automatisointi voitaisiin sillä toteuttaa. Toteteutuksessa päädyttiin hyödyntämään IPAM-serverin tietokantaa olemassa olevista laitteista. Tietokannan avulla muodostettiin ClearPassiin palvelu, joka automatisoi verkkoon liitettävien tulostimien, kiinteistönvalvonnan ja vieraiden laitteiden VLAN-konfiguraation. Palvelussa hyödynnettiin IEEE 802.1X porttikohtaista autentikointia ja RADIUS-CoA toiminnon tarjoamaa kytkinportin VLANin muuttamista.

Testiympäristössä järjestelmä saatiin toimimaan sunnitellulla tavalla. Verkkoon kytketyt laitteet saivat aikaan kytkinportin siirtymisen haluttuun VLANiin ja tuotantoon otettaessa järjestelmä säästäisi merkittävästi järjestelmän ylläpitoon käytettävää aikaa siirrettäessä laitteita tai lisättäessä uusia laitteita verkkoon.

Asiasanat: VLAN, IEEE 802.1X, RADIUS, Ethernet, Aruba ClearPass

Lahti University of Applied Sciences
Degree Programme in Information Technology

KETOLUOTO, ANTTI: Network Access Control
Aruba ClearPass

Bachelor's Thesis in Telecommunications, 38 pages

Spring 2017

ABSTRACT

The objective of this thesis was to examine whether the Aruba ClearPass system can be used for the automatization of VLAN configuration in network interfaces. The system was implemented into printer, guest and property monitoring networks. The network environment used in the implementation is the City of Lahti's network. The network is managed by Lahden Tietotekniikka, which commissioned this thesis.

Aruba ClearPass is a Network Access Control solution which provides RADIUS authentication to appliances. It is also used for IEEE 802.1X port-based authentication. The purpose of port-based authentication is to prevent unauthorized access to a network. RADIUS is a networking protocol providing AAA model authorization, authentication and accounting services. It is used for delivering supplicant's authentication information between the network access device and the authentication server.

Before implementing the solution to the network, the Aruba ClearPass system was thoroughly examined to determine whether it is suitable for automatization of VLAN configuration. The ClearPass system was chosen because it is already used in the network for authentication of wireless clients. During the implementation, it was discovered that using the database from the IPAM server, which contains the information of all devices in the network, would be the best solution. The database was used to make a service to the ClearPass system which configures a switch port where the device is connected to the correct VLAN according to the type of the device and its authorization status from the IPAM database. This service also utilized IEEE 802.1X RADIUS CoA property for changing switchport VLAN.

While testing the system, it was found to be working as expected. Connecting a device to a switch triggered the correct ClearPass service and the switch port was automatically configured to the correct VLAN. If implemented into production, this solution would save a considerable amount of time from the IT management when new devices are introduced to the network or old devices are moved around.

.

Key words: VLAN, IEEE 802.1X, RADIUS, Ethernet, Aruba ClearPass

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, Authorization, Accounting. Protokolla tunnistamiseen, valtuuttamiseen ja tilastointiin.
CoA	Change of Authorization. RADIUS-protokollan ominaisuus, jolla voidaan aloittaa autentikointi uudelleen tai määrittää uusia käytäntöjä.
CPPM	ClearPass Policy Manager. Aruba ClearPass järjestelmän hallintanäkymä.
DHCP	Dynamic Host Configuration Protocol. IP-osoitteiden jakamisessa käytetty verkkoprotokolla.
EAP	Extensible Authentication Protocol. Käyttäjien tunnistamisessa käytettävä protokolla.
EAPOL	Extensible Authentication Protocol Over Local area network. Protokolla autentikoitavan käyttäjän ja verkon liityntäpisteen väliseen liikennöintiin.
HP	Hewlett-Packard. Maailmanlaajuinen tietotekniikka-alan yritys.
HTTP	HyperText Transfer Protocol. Internetselainten käyttämä tiedonsiirtoprotokolla.
HTTPS	HyperText Transfer Protocol Secure. Suojattu versio HTTP-protokollasta.
IEEE	Institute of Electrical and Electrics Engineers. Kansainvälinen tekniikan alan järjestö.
IKE	Internet Key Exchange. Protokolla salausavaimien vaihtamiseen IP-verkon yli.
IP	Internet Protocol. Yleisesti käytetty

	tietoliikenneprotokolla.
IPAM	IP Address Management. Järjestelmä IP-osoitteiden hallintaan.
LLC	Logical Link Control. OSI-mallin siirtoyhteyskerroksen ylempi alikerros.
NAS	Network Access Server. Verkon liityntäpiste, jonka kautta asiakas liittyy verkkoon.
MAB	Mac Address Bypass. Porttikohtainen autentikointi MAC-osoitteen perusteella.
MAC	Media Access Control. OSI-mallin siirtoyhteyskerroksen toinen alikerros.
OSI	Open Systems Interconnection Reference Model. Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PEAP	Protected Extensible Authentication Protocol. Ciscon ja Microsoftin kehittämä suojattu EAP-protokolla.
RADIUS	Remote Authentication Dial In User Service. Verkon liityntäpisteen ja autentikointipalvelimen väliseen liikennöintiin käytetty protokolla.
RFC	Request For Comments. Kokoelma Internetiä koskevia standardeja.
SQL	Structured Query Language. Standardoitu kyselykieli relaatiotietokannan hallintaan.
TCP	Transmission Control Protocol. Tiedonsiirtoprotokolla.
TLS	Transport Layer Security. Salausprotokolla, jolla

	salataan liikenne IP-verkkojen yli.
UDP	User Datagram Protocol. Tiedonsiirtoprotokolla.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
VOIP	Voice Over Internet Protocol. Äänen siirtäminen reaaliaikaisesti internetin yli.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Nykyaikaisessa yhteiskunnassa tietoverkot ovat osa jokapäiväistä elämää. Lähes kaikki tiedonsiirto tapahtuu erilaisissa verkoissa. Näiden verkkojen rakentaminen, ylläpito ja korjaaminen kuormittavat niistä vastaavia organisaatioita ja pienillä toimenpiteillä on mahdollista vaikuttaa esimerkiksi ylläpidon kuormittavuuteen.

Työn tavoitteena on toteuttaa verkkolaitteiden VLAN-konfiguraation automatisointi Aruba Clearpass -järjestelmällä. Kohdeympäristönä on Lahden Tietotekniikan ylläpitämä Lahden kaupungin verkko, jonka loppukäyttäjiä ovat esimerkiksi kunnallishallinto, sosiaali- ja terveyspalvelut sekä muut kaupungin toimialat.

Nykytilanteessa, kun esimerkiksi uusi tulostin lisätään kaupungin verkkoon, tulee kytkinportti, johon tulostin liitetään, konfiguroida manuaalisesti oikeaan VLANiin. Konfiguroiminen kuormittaa rajallisia henkilöstöresursseja ja aiheuttaa ylimääräistä työtä. Lisäksi automatisointi mahdollistaa myös laitteiden siirron toimipisteellä huoneiden välillä ilman IT-tuen toimenpiteitä.

2 LÄHIVERKKO

Lähiverkolla tarkoitetaan tietoliikenneverkkoa, jossa verkon laitteet ovat maantieteellisesti rajattu pienen alueen sisälle. Esimerkiksi yrityksen yhden toimipisteen työasemat, tulostimet, palvelimet, kaapelit ja verkkolaitteet muodostavat lähiverkon.

Lähiverkko mahdollistaa resurssien, kuten tulostimien, tiedostojen ja ohjelmien, jakamisen useiden käyttäjien kesken. Lähiverkko voidaan toteuttaa myös langattomasti IEEE 802.11 -standardissa määritettynä WLAN-lähiverkkona. Työssä keskitytään kuitenkin vain langalliseen lähiverkkoon.

2.1 OSI-Malli

OSI eli Open Systems Interconnection Reference Model on tiedonsiirtoprotokollien viitemalli, jossa tietoliikennejärjestelmä on jaettu seitsemään kerrokseen. OSI-malli kehitettiin mahdollistamaan tietoliikennejärjestelmien yhtäläinen suunnittelu.

OSI-malli on kehitetty alun perin ISO-järjestön toimesta 1980-luvun alussa. OSI-malli toimii pyramidin tavoin, jossa ylempi kerros käyttää aina alemman kerroksen tarjoamia palveluja. (Microsoft 2017.)

2.2 OSI-kerrokset

OSI-malli jaetaan kuviossa 1 esitetyn mukaisesti seitsemään kerrokseen. OSI-mallin seitsemän kerrosta, joista jokaisella on oma tehtävänsä ovat

1. Fyysinen kerros
2. Siirtokerros
3. Verkkokerros
4. Kuljetuskerros
5. Istuntokerros
6. Esitystapakerros
7. Sovelluskerros.

KUVIO 1. OSI-mallin kerrokset (Wikipedia 2016)

Kuten aiemmin kerrottiin, näistä jokainen kerros käyttää alemman kerroksen palveluita mahdollistaakseen oman palvelunsa. Esimerkiksi kuljetuskerroksen tarjoamia TCP- ja UDP-tiedonsiirtoprotokollia käytetään yleisimmin verkkokerroksen tarjoaman IPv4:n ja yleistymässä oleva IPv6:n mukaisessa tiedonsiirrossa. (Microsoft 2017b.)

2.2.1 Fyysinen kerros

Fyysinen kerros määrittää tiedonsiirrossa käytettävän fyysisen median kuten kaapelin, valokuidun tai radiotien. Fyysisellä tasolla tietoa siirretään joko sarja- tai rinnakkaismuotoisella tiedonsiirrolla. (Microsoft 2017b.)

Sarjamuotoisessa tiedonsiirrossa data siirretään peräkkäin yksi bitti kerrallaan. Rinnakkaismuotoisessa tiedonsiirrossa voidaan dataa siirtää useampi bitti kerrallaan rinnakkaisia siirtoteitä pitkin. (Microsoft 2017b.)

2.2.2 Siirtokerros

Siirtokerroksen tehtävänä on kehystää ylempien kerrosten paketin siirrettäväksi fyysisellä kerroksella. Siirtokerroksella tiedonsiirrossa puhutaan kehyksistä. Siirtokerros hoitaa yhteyden luomisen ja purkamisen, yhteyden vuonohjausta, sekä yhteyden virheenkorjausta. (Microsoft 2017b.)

Yhteyden luominen ja purkaminen suoritetaan fyysisen kerroksen siirtotiestä riippuvalla tavalla. Vuonohjauksella tarkoitetaan sitä, että tietoa ei lähetetä nopeammin kuin vastaanottaja pystyy sitä käsittelemään. Virheenkorjauksessa havaittu virheellinen data lähetetään uudelleen. (Microsoft 2017b.)

Siirtokerros jaetaan kahteen alikerrokseen, MAC- eli Media Control Access -tasoon sekä LLC- eli Logical Link Control -tasoon. Näistä tasoista MAC-tasolla kontrolloidaan, kuinka laitteet saavat pääsyn verkkoon ja luvan tiedonsiirrolle. LLC-tasolla tunnistetaan verkkokerroksen protokollat ja hoidetaan niiden enkapsulointi sekä suoritetaan virheenkorjausta ja kehysten synkronointia. (Microsoft 2017b.)

2.2.3 Verkkokerros

Verkkokerroksen tehtävänä on jakaa ylemmiltä kerroksilta saatu data paketteihin ja toimittaa ne perille vastaanottajalle erilaisten verkkoratkaisujen yli. Verkkokerroksella suoritetaan myös liikenteen reititystä, eli valitaan mitä reittiä data siirtyy tietoverkossa. (Microsoft 2017b.)

Verkkokerroksella liikennöinti tapahtuu käytetyn protokollan mukaisella osoitteistuksella. Nykyään käytössä on melkein yksinomaan Internet-protokolla eli IP ja sen versiot IPv4 ja IPv6. (Microsoft 2017b.)

2.2.4 Kuljetuskerros

Kuljetuskerros huolehtii käyttäjän tarvitseman tiedonsiirtotavan toteutumisesta. Kuljetuskerroksin tehtäviin kuuluu myös ruuhkautumisen hallinta. (Cisco 2016c.)

Siirtotapoja ovat esimerkiksi virheettömyyden takaava TCP eli Transmission Control Protocol. TCP:tä käytettäessä jokainen lähetetty paketti kuitataan saapuneeksi vastaanottajan toimesta. Toinen yleinen siirtotapa on User Datagram Protocol eli UDP, jossa ei lähettäjälle ilmoiteta millään tavalla tiedon saapumisesta perille. (Cisco 2016c.)

2.2.5 Istuntokerros

Istuntokerros järjestää yhteyden, eli istunnon kahden ohjelman välille. Kerroksen tehtävänä on myös mahdollistaa yhteyden jatkaminen sen katkeamisen jälkeen. (Cisco 2016c.)

OSI-mallissa istuntokerroksen vastuulla on myös yhteyksien sulava katkaisu. Lisäksi sekä tallennuspisteiden luominen, että yhteyksien päättäminen ja palauttaminen ovat istuntokerroksen vastuulla. (Cisco 2016c.)

2.2.6 Esitystapakerros

Esitystapakerroksen tehtävänä on ratkoa ongelmia erilaisten päätelaitteiden kommunikoidessa keskenään. Esitystapakerros ei siis vastaa tiedon siirtämisestä. (Cisco 2016c.)

Esitystapakerros määrittää siis formaatit datan esittämiselle. Esimerkiksi äänentoistossa käytetty MIDI-, videotoistoon tarkoitettu MPEG- ja kuvien esittämiseen tarkoitettu GIF-protokolla ovat esimerkkejä esitystapakerroksella käytettävistä formaateista. (Microsoft 2017b.)

2.2.7 Sovelluskerros

Sovelluskerroksen tehtävä on tarjota tiedonsiirtoprotokollia sovellusten käyttöön. Esimerkiksi WWW-sivujen siirtämiseen käytetään HTTP- ja HTTPS-protokollia.

Sovelluskerros on kerroksista siis lähimpänä loppukäyttäjää. Kerros toimiikin linkkinä käyttäjän käyttämän sovelluksen ja sovelluksen tarvitseman tiedonsiirtoprotokollan välillä. (Microsoft 2017b.)

2.3 Ethernet

Nykyään yleisin lähiverkossa käytetty tekniikka on IEEE 802.3 -standardissa määritelty Ethernet. Ethernetin nousu sen nykyään hallitsevaan asemaan lähiverkoissa perustui hyvään hinta-laatusuhteeseen, helppokäyttöisyyteen ja laitevalmistajien tukeen. Ethernet oli ensimmäinen lähiverkon toteutustapa, joka on teollisuusstandardi, eikä valmistajakohtainen toteutustapa.

Nykyään yleisimmät lähiverkoissa käytössä olevat standardit ovat jo väistymässä oleva 100 Mbit/s siirtonopeuden tarjoava FastEthernet, 1 Gbit/s siirtonopeuteen pystyvä GigabitEthernet sekä aluksi vain kuituverkoissa käytössä ollut, mutta nyt myös parikaapelilla toteutettava TenGigabitEthernet. (IEEE 2015.)

Ethernet verkko voidaan fyysisesti rakentaa joko väylä- tai tähtitopologian mukaan. Väylätopologian mukaan toteutetussa verkossa kaikki laitteet ovat käytännössä yhden kaapelin varrella ja käyttävät samaa siirtotietä tiedonsiirtoon. Tähtitopologiassa verkossa on keskuslaite, esimerkiksi kytkin. Keskuslaitteelta on oma kaapelinsa verkon kaikille muille laitteille, eikä siirtotie ole jaettu muiden käyttäjien liikenteen kanssa. Lisäksi tähtitopologian mukainen verkko on väylätopologiaa vikasietoisempi. Siinä missä katkennut kaapeli väylätopologian mukaisessa verkossa estää liikenteen verkon kaikilta käyttäjiltä, tähtitopologialla toteutetussa verkossa

katkennut kaapeli aiheuttaa verkon toimimattomuuden vain laitteelle, jonka kaapeli on katkennut. Koko tähtitopologialla toteutetun verkon voi lamauttaa vain keskuslaitteen hajoaminen. (IEEE 2015.)

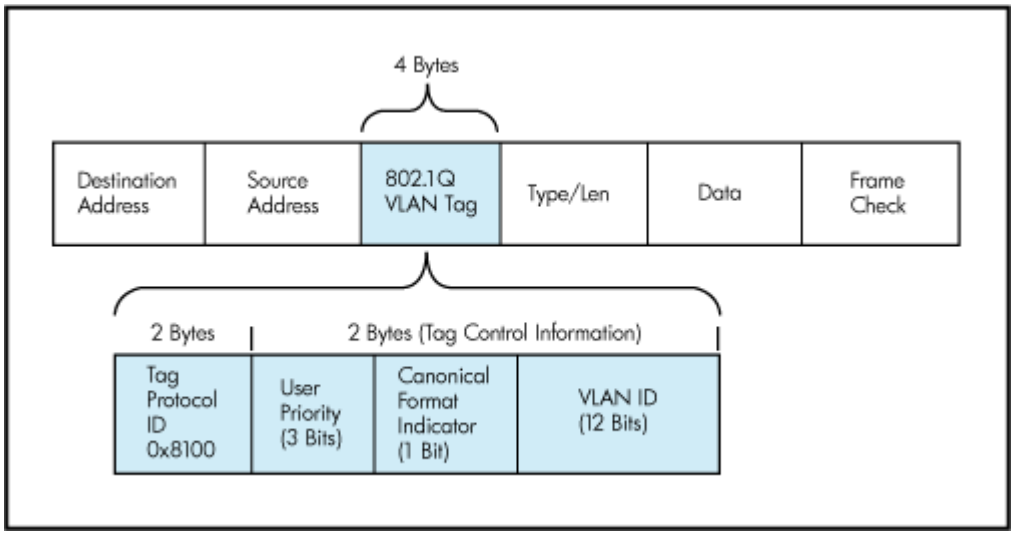
2.4 Virtuaalinen lähiverkko

VLAN eli virtuaalinen lähiverkko on joukko laitteita yhdessä tai useammassa maantieteellisessä sijainnissa, jotka on konfiguroitu liikennöimään kuin ne olisivat yhdessä fyysisessä lähiverkossa. VLANit käyttävät loogisia yhteyksiä fyysisten sijaan, joten ne ovat erittäin mukautuvia.

Virtuaalisia lähiverkkoja käytetään esimerkiksi jakamaan yrityksen eri osastot omiin verkkoihinsa, jakamaan erilaisten laitteiden, kuten VOIP-puhelimien, tulostimien ja tietokoneiden, liikenne omiin verkkoihinsa yhdessä fyysisessä verkossa sekä rajoittamaan broadcast-liikennettä suurissa verkoissa. Virtuaalinen lähiverkko on määritelty IEEE-standardeissa 802.1Q ja 802.1p. (Cisco 2017.)

2.4.1 IEEE 802.1Q

IEEE 802.1Q -standardi lisää Ethernet-kehykseen mahdollisuuden virtuaaliverkkoihin kuvion 2 mukaisella neljän tavun kokoisella lisäkentällä.



KUVIO 2. 802.1Q VLAN Tag (Ciscohite 2013)

Lisäkenttä koostuu TAG-protokollatunnisteesta ja TAG-ohjaustiedosta, jotka molemmat ovat kahden tavun kokoisia. Protokollatunniste määrittää kehyksen 802.1Q-kehykseksi ja tunnisteen arvo Ethernet verkoissa on heksaluku 0x8100. Ohjaustiedossa ensimmäiset 3 bittiä osoittavat kehyksen prioriteettitason, jotka on määritelty IEEE 802.1p -standardissa. Seuraava CFI-kenttä on yhden bitin kokoinen, ja sitä käytetään Ethernet ja Token Ring -verkkojen yhteensopivuudessa. Ethernet-verkoissa kentän arvo on 0. Viimeinen 12 tavua on varattu merkitsemään mihin VLANiin kehys kuuluu. Arvolla 0 kehys ei kuulu mihinkään VLANiin. Virtuaalisten lähiverkkojen suurin mahdollinen lukumäärä on 4094. (IEEE 2014.)

2.4.2 IEEE 802.1p

IEEE 802.1p -standardi mahdollistaa liikenteen priorisoinnin. Priorisointi toimii OSI-mallin toisella kerroksella MAC-tasolla. Otsikko sisältää kolmen bitin kentän, jonka perusteella liikennettä jaetaan eri luokkiin. Mahdollisia luokkia on kahdeksan. Arvolla 000 liikenne on alimmalla mahdollisella prioriteetilla ja arvolla 111 liikenne on suurin mahdollinen prioriteetti. Yleensä pientä latenssia vaativat palvelut kuten VOIP-liikenne ja verkonhallinta sijoitetaan korkealle prioriteetille. Esimerkiksi sähköposti ei ole niin riippuvainen yhteyden latenssista, joten sähköpostiliikenne voidaan siirtää pienemmällä prioriteetilla. (Transition networks 2017.)

3 AUTENTIKOINTIPROTOKOLLAT

Autentikointiprotokollien tehtävänä on toteuttaa kahden eri osapuolen välisen identiteetin tunnistautuminen. Yksinkertaisimmillaan tämä tarkoittaa salasanan lähettämistä rajapinnan yli.

Autentikointiprotokollista käytetään yleensä puhuttaessa myös termiä AAA-protokollat. Termissä käsitettä on laajennettu kattamaan myös muita toimintoja, kuin vain identiteetin tunnistaminen.

3.1 AAA

AAA-protokollalla tarkoitetaan protokollia, joita käytetään käyttäjän todentamiseen, valtuutusten antamiseen sekä käytön seurantaan tietoverkoissa. Lyhenne muodostuu sanoista Authentication eli todentaminen, Authorization eli valtuutus ja Accounting eli tilastointi.

AAA-protokollan toiminta voidaan tiivistää kolmeen peruskysymykseen:

- Kuka käyttäjä on?

- Mihin resursseihin käyttäjällä on oikeuksia?

- Mitä käyttäjä tekee oikeuksillaan?

Yleisimpiä käytettyjä AAA-protokollia ovat RADIUS, siitä uudistettu DIAMETER ja TACACS+. Työssä käytetään RADIUS-protokollaa.

3.1.2 Todentaminen

Authentication eli todentaminen tarkoittaa palvelua, jolla tunnistetaan verkkoon kirjautuvan käyttäjän tai laitteen identiteetti. Tunnistamisessa voidaan käyttää esimerkiksi käyttäjätunnus-salasana-yhdistelmää, sertifikaattia tai laitteen MAC-osoitetta. Autentikointiprosessi suoritetaan ennen käyttäjän pääsyä verkkoon. (Cisco 2013.)

Käyttäjän tunnistamisessa yleisin käytetty menetelmä on salasanan perusteella. Menetelmän yleisimpänä ongelmana ovat liian yksinkertaiset

tai helposti arvattavat salasanat. Lisäksi vahvimmatkaan salasanat eivät kuitenkaan suojaa järjestelmää, jos ne päätyvät muiden kuin käyttäjän itsensä tietoon. (Cisco 2013.)

Salasanaan perustuvan tunnistuksen ongelmia on pyritty korjaamaan kehittämällä esinepohjainen käyttäjäntunnistus. Siinä käyttäjä kirjautuu järjestelmään käyttäen omaa käyttäjätunnustaan sekä esimerkiksi vaihtuvaa salasanaa, joka löytyy käyttäjän hallussa olevasta listasta. Esinepohjaisesta käyttäjätunnistuksesta hyvänä esimerkkinä toimivat pankkien verkkopankeissa käyttämät tunnuslistat. (Cisco 2013.)

Kehittynein käyttäjätunnistus saavutetaan biometrisellä käyttäjätunnistuksella. Biometrinen autentikointi perustuu käyttäjän yksilölliseen fyysiseen ominaisuuteen. Yleisimmin käytetyt biometriset tunnistusmenetelmät ovat sormenjälki ja silmän iirikseen perustuva tunnistus. Biometrisen tunnistuksen käyttö on myös haastavinta sen vaatiman ylimääräisen apuvälineen, kuten sormenjälkiskannerin vuoksi. (Turun TKK 2011.)

Vahvin suojaus saavutetaan yhdistämällä eri tunnistusmenetelmiä. käyttäjän on esimerkiksi salasanan lisäksi syötettävä tunnuslistasta löytyvä koodi. Yhdistämällä menetelmiä esimerkiksi tunnuslistan joutuminen muiden haltuun ei vielä riitä pääsyn saamiseksi järjestelmään. (Cisco 2013.)

3.1.3 Valtuutus

Authorization eli valtuutusprosessissa käyttäjälle tai laitteelle annetaan verkon resursseja käyttöön. Valtuutus suoritetaan autentikoinnin jälkeen, kun käyttäjä on onnistuneesti kirjautunut verkkoon. Valtuutus perustuu ennalta määrättyyn protokollaan, eli tietyillä käyttäjillä on tietyt oikeudet tehdä toimintoja verkossa. (Cisco 2013.)

Tietyille käyttäjille voidaan esimerkiksi sallia pääsy julkisen verkon palveluihin kuten internettiin, mutta estää pääsy yrityksen sisäverkon jaettuihin resursseihin. Tämä on yleinen käytäntö esimerkiksi yritysten WLAN-verkoissa, joissa vierailijat saavat internet-yhteyden käyttöönsä, mutta eivät voi käyttää yrityksen omia verkkolevyjä tai tulostimia. Samalla kuitenkin yrityksen työntekijöiden laitteet voivat käyttää sisäverkon palveluita samoja WLAN-tukiasemia käyttäen. (Cisco 2013.)

3.1.4 Tilastointi

Accounting, eli kirjaaminen tarkoittaa tiedon keräämistä verkon käyttäjistä. Käyttäjistä voidaan kerätä muun muassa yhteysaikoja, tietoa käytetyistä palveluista, kuten jaettujen verkkolevyjen käytöstä, tai käyttäjän toimista, kuten verkkolaitteiden asetusten muuttamisesta. (Cisco 2013.)

Tilastointi suoritetaan valtuutuksen jälkeen, kun käyttäjä on ensin tunnistettu sekä käyttäjälle on annettu sille kuuluvat oikeudet. Tallennettuja tietoja voidaan hyödyntää esimerkiksi ongelmatapauksissa, kun tarvitsee selvittää mitä on tehty, koska se on tehty tai kuka sen teki. (Cisco 2013.)

3.2 RADIUS

RADIUS eli *Remote Authentication Dial In User Service* on käyttäjien tunnistusta ja hallintaa tarjoava AAA-protokolla. RADIUS tarjoaa AAA-mallin mukaiset tunnistautumis-, valtuutus- ja tilastointipalvelut. (Microsoft 2017a.)

RADIUS-protokolla kehitettiin Livingston-yhtiön toimesta sisäänsoittopalveluihin tarjoamaan käyttäjän tunnistusta. Nykyisin RADIUS-protokollaa käytetään pääasiassa yritysten sisäisissä verkoissa. (Microsoft 2017a.)

Nykymuodossaan RADIUS on määritelty RFC 2867-dokumentissa. Määritykseen kuuluivat tunnistukseen ja valtuutukseen liittyvät

toimenpiteet. Tilastointi on määritelty osaksi protokollaa myöhemmin RFC 2868-dokumentissa. (Microsoft 2017a.)

3.2.2 RADIUS-protokollan toiminta

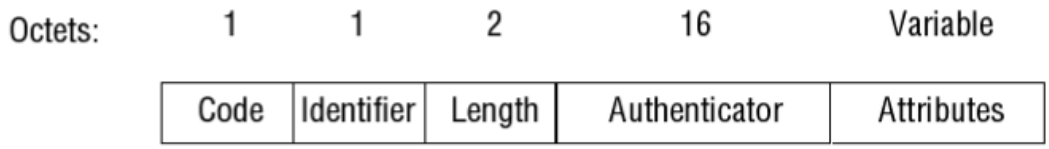
RADIUS-prosessiin kuuluu neljä osapuolta:

- autentikoitava käyttäjä
- NAS-liityntäpiste
- RADIUS-palvelin
- käyttäjätietokanta.

Autentikoitava käyttäjä on laite, joka tarvitsee pääsyn verkkoon, esimerkiksi kytkimeen kytketty tietokone. Tietokone lähettää pyynnön verkkoon pääsystä kytkimelle eli NAS-liityntäpisteelle. Liityntäpiste kysyy käyttäjältä tunnistetietoja jotka ovat yksinkertaisimmillaan käyttäjätunnus ja salasana. Liityntäpiste toimii seuraavaksi RADIUS-asiakkaana ja välittää tunnistetiedot eteenpäin RADIUS-palvelimelle. Palvelin tarkastaa ne käyttäjätietokantaa vasten ja suorittaa käyttäjän tunnistuksen, sekä antaa käyttäjälle valtuutuksen. (Microsoft 2017a.)

3.2.3 RADIUS-viestin rakenne

Kaikilla RADIUS-viesteillä on sama kuvion 3 mukainen perusrakenne. Viestit koostuvat tyyppi-, tunniste-, pituus-, tunnistetieto- ja attribuutti-kentistä. Tyyppikenttä kertoo RADIUS-viestin tyypin. Esimerkiksi arvolla 1 kyseessä on Acces-Request viestityyppi, jolla pyydetään palvelinta suorittamaan autentikointi. Tunnistekenttää käytetään tunnistamaan toisiinsa liittyvät viestit. Pituus kenttä määrittää viestin pituuden. Tunnistetietoa käytetään salaamaan viestin sisältö ja attribuutti-kentässä välitetään käyttäjän tunnistautumistiedot kuten käyttäjänimi ja salasana. (Geier 2008, 72.)



KUVIO 3. RADIUS-viestin rakenne (Geier 2008, 72)

3.2.4 RADIUS-viestityypit

RADIUS-viestejä on kahdeksaa eri tyyppiä, joista kuusi on yleisesti käytössä. Seuraavassa taulukossa on listattu eri viestityypit.

TAULUKKO 1. RADIUS-viestityypit

Koodi	Tyyppi
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

Access-Request viestiä käytetään käyttäjän liittyessä verkkoon NAS-liityntäpisteen kautta. Liityntäpiste lähettää Access-Request viestin RADIUS-palvelimelle pyytäen käyttäjän autentikointia. Palvelin vastaa joko Access-Accept-, tai Access-Reject-viestillä, riippuen onnistuiko käyttäjän autentikointi. Access-Request-viesti sisälsi autentikoitavan käyttäjän

käyttäjätiedot, laitteen IP-osoitetiedot sekä tiedon miltä NAS-liityntäpisteeltä kirjautumista yritetään. Käyttäjän salasana salataan käyttämällä MD5-salausta. (Geier 2008, 76.)

Jos käyttäjän tunnistaminen ei onnistu käyttäen vain Access-Request-viestin sisältämiä tietoja, voi RADIUS-palvelin pyytää lisää kirjautumistietoja Access-Challenge tyyppisellä viestillä. Liityntäpiste välittää kyselyn takaisin autentikoitavalle käyttäjälle ja saatuaan vaaditut lisätiedot, lähettää se uuden täydennetyn Access-Request-viestin RADIUS-palvelimelle. (Geier 2008, 77.)

Kun käyttäjälle on myönnetty pääsy verkkoon, aloitetaan tilastointi. Tilastoinnissa liityntäpiste lähettää RADIUS-palvelimelle Accounting-Request-viestin arvolla Start, jolla ilmoitetaan käyttäjän verkkoon pääsyn aloitus. Palvelin kuittaa saaneensa tiedon käyttäjän pääsystä verkkoon Accounting-Response-viestillä. Käyttäjän päättäessä istuntonsa, lähettää liityntäpiste taas Accounting-Request-viestin arvolla Stop kertoakseen käyttäjän istunnon päättyneen. RADIUS-palvelin vastaa taas Accounting-Response viestillä. Lisäksi käyttäjän istunnon aikana voidaan päivittää käyttäjän toimia verkossa esimerkiksi siirretyn datan määrää tai verkkolaitteille tehtyjä muutoksia, jos käyttäjällä on niihin tarvittavat oikeudet. Näihin päivityksiin käytetään myös Accounting-Request tyyppisiä viestejä, joihin palvelin vastaa Accounting-Response-viesteillä. (Geier 2008, 79.)

4 IEEE 802.1X

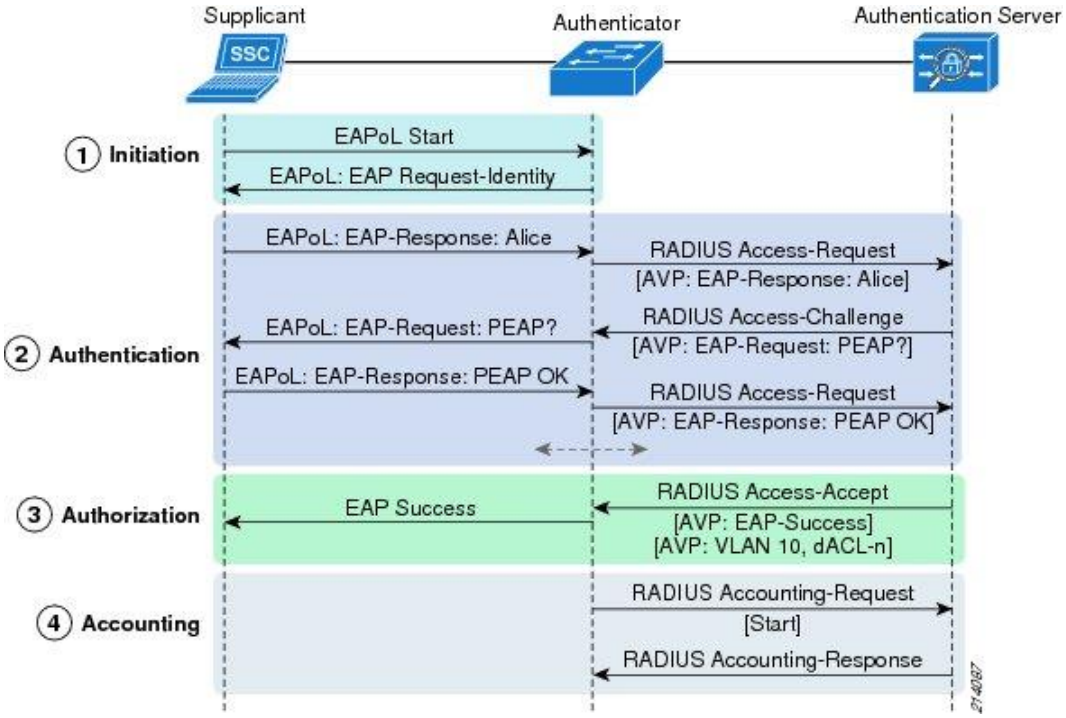
IEEE 802.1x -standardissa määritellään porttikohtaisen autentikoinnin käyttö ethernet- ja wlan-verkoissa. Porttikohtaista autentikointia käytetään estämään luvattomien laitteiden pääsy verkkoon ja näin parantamaan verkon tietoturvaa. 802.1x porttikohtainen autentikointi perustuu EAP-protokollaan. (Cisco 2016a.)

Autentikoinnissa on kolme osapuolta, jotka ovat asiakas, autentikointipalvelin ja autentikaattori. Prosessissa verkkoon liitettävää autentikoitavaa päätelaitetta kutsutaan asiakkaaksi. Autentikointipalvelimena käytetään yleensä RADIUS-palvelinta, joka suorittaa asiakkaan autentikoinnin. Autentikaattorilla tarkoitetaan verkon liityntäpistettä, yleensä kytkintä, jonka kautta asiakas liittyy verkkoon. (Cisco 2016a.)

4.1 Protokollat

IEEE 802.1x -standardin mukaisessa porttikohtaisessa autentikoinnissa käytetään useita eri protokollia. Näitä käytetään niin tiedon siirtämiseen, kuin salaamiseenkin.

Protokollista oleellisimpia ovat erityisesti EAP, aiemmin esitelty RADIUS sekä EAPOL. RADIUSta käytetään liityntäpisteen ja autentikointipalvelimen väliseen liikennöintiin, kun taas liikennöinti asiakkaan ja liityntäpisteen välillä käydään EAPOL-protokollalla kuvion 4 mukaisesti. (Cisco 2016b.)



KUVIO 4. Porttikohtaisen todennuksen liikennöinti (Cisco 2011)

4.1.1 EAP

Extensible Authentication Protocol on tietoturvaprotokolla, jota käytetään todentamiseen. Se toimii OSI-mallin 2. kerroksen MAC-alikerroksella, eikä se ole riippuvainen Internet Protokollasta. EAP-protokolla ei ole autentikointimenetelmä, mutta se tarjoaa kuljetusmetodin valitulle autentikointimenetelmälle. Yleisimpiä EAP-autentikointimenetelmiä ovat muun muassa EAP-TLS, LEAP, EAP-MD5, EAP-TTLS, EAP-IKEv2. (Geier 2008, 223.)

EAP soveltuu käytettäväksi kaikissa siirtoyhteyskerroksissa tahansa. Työssä käytössä on IEEE 802.3 mukainen 100BASE-T Fast Ethernet ja 1000BASE-T Gigabit Ethernet parikaapeliverkko. (Geier 2008, 223.)

4.1.2 PEAP

Protected Extensible Authentication Protocol toimii kuten EAP-protokolla. PEAP käyttää Transport Layer Securityä luodakseen salatun tunnelin asiakkaan ja autentikointipalvelimen välille. PEAP ei ole

autentikointimenetelmä, vaan sen tarkoituksena on tarjota lisäturvaa muille EAP-protokollille. (Geier 2008, 112.)

Erona EAP-protokollaan on pakollinen molemminpuolinen autentikointi. Näin pystytään estämään liikenteen kaappaamista ja man-in-the-middle hyökkäyksiä. (Geier 2008, 112.)

4.1.3 EAPOL

Extensible Authentication Protocol over LAN on tietoliikenneprotokolla, jolla enkapsuloidaan 802.1x protokollan EAP-viestit ethernet kehykseen. Protokollaa käytetään välittämään asiakkaan ja autentikointipalvelimen välistä EAP-liikennettä. (Geier 2008, 55.)

EAPOL kehitettiin alun perin käytettäväksi IEEE 802.3 ethernet verkoissa. Myöhemmin EAPOLin huomattiin soveltuvan käytettäväksi myös muissa verkkotekniikoissa, kuten IEEE 802.11 WLAN-verkoissa. (Geier 2008, 55.)

4.1.4 MAB

MAC Authentication Bypass on IEEE802.1x -standardin laajennus. Sitä käytetään, jos päätelaite ei tue 802.1x-autentikointia. Näitä laitteita ovat yleensä verkkotulostimet, kamerat sekä muut sulautetut järjestelmät. (Cisco 2016a.)

Kun kytkimen porttiin on konfiguroitu MAB käyttöön, toimii se seuraavalla periaatteella. Kun laite kytketään verkkoon ja kytkin ei saa EAPOL-vastausta päätelaitteelta, lähettää kytkin RADIUS Access-Request-viestin autentikointipalvelimelle. Tässä viestissä käyttäjätunnus ja salasana kentät täytetään autentikoitavan laitteen MAC-osoitteella. (Cisco 2016a.)

4.2 Porttikohtaisen autentikoinnin toiminta

Porttikohtaista autentikointia käytettäessä kytkimen portti on aluksi unauthorized- eli luvaton tilassa. Tässä tilassa kaikki normaali TCP- ja UDP-liikenne on estetty ja vain EAPOL-liikenne on sallittu. (Cisco 2016a.)

Kuvion 4 mukainen autentikointiprosessi alkaa, kun asiakas, eli päätelaite kytketään porttiin. Autentikaattori eli kytkin lähettää EAP-Request Identity-kehyksen OSI-mallin 2 kerroksen MAC-alikerroksella. Asiakas avaa kuunteluyhteyden vastaanotettuaan EAP-Request Identity-kehyksen ja lähettää vastauksena EAP-Response Identity-kehyksen autentikaattorille. Kehys sisältää asiakkaan tunnistustiedot, jotka autentikaattori enkapsuloi edelleen RADIUS Access-Request-paketiksi ja lähettää sen edelleen autentikointipalvelimelle. (Cisco 2016b.)

Neuvotteluvaihetta kutsutaan myös EAP-neuvotteluksi. Neuvotteluvaiheessa autentikointipalvelin lähettää EAP Requestin sisältävän uudelleenlähetyksen autentikaattorille, jolla täsmennetään käytetty EAP-autentikointimenetelmä. Autentikaattori enkapsuloi pyynnön EAPOL-kehykseen ja lähettää sen edelleen asiakkaalle. Nyt asiakas voi käyttää autentikaatiopalvelimen pyytämää EAP-autentikaatiomenetelmää, tai antaa Negative ACknowledgement vastauksen ja valita EAP-menetelmän, jolla haluaa tunnistuksen suorittaa. (Cisco 2016b.)

Autentikointi tapahtuu asiakkaan ja autentikaatiopalvelimen sovittua käytetystä EAP-menetelmästä ja asiakkaan toimitettua RADIUS-autentikointiin vaadittavat tiedot valitulla EAP-menetelmällä. Autentikaatiopalvelin vastaa RADIUS Access-Accept-paketin sisältävällä EAP Success-kehyksellä, tai autentikoinnin epäonnistuessa RADIUS Access Reject-paketin sisältävällä EAP Failure-kehyksellä. Autentikoinnin onnistuessa asettaa kytkin portin sallittu-tilaan, jossa kaikki normaali verkkoliikenne sallitaan. Portti pysyy sallittu-tilassa EAPOL Logoff-kehyksen vastaanottamiseen asti. (Cisco 2016b

5 VLAN KONFIGURAATION AUTOMATISOINTI

Opinnäytetyön tavoitteena oli löytää ratkaisu uusien laitteiden lisäämiseen Lahden kaupungin verkkoon sekä olemassa olevien laitteiden siirtymiseen fyysisesti eri portteihin. Nykytilassa esimerkiksi tulostimen siirto toiseen huoneeseen vaatii kytkimen portin konfiguroimisen Tulostus-VLANiin. Usein tiloissa on myös useampi verkkoliitäntä ja käyttäjät saattavat itse siirtää laitteita liitännästä toiseen, jolloin toimimattoman verkkotulostimen vianselvitys aiheuttaa turhaa työtä.

Järjestelmä tulisi automatisoida niin, että liitettäessä laite kytkimen porttiin ei se vaatisi manuaalista asetusten muokkaamista kytkimellä. Samalla laitteet voidaan myös todentaa ja estää verkon luvatonta käyttöä.

Lahden kaupungilla on käytössä Aruba Clearpass -ohjelmisto, jolla kaupungin työasemat todennetaan langattomaan lähiverkkoon liityttäessä. Työssä tutkittiin, soveltuuko olemassa oleva järjestelmä käytettäväksi myös verkkotulostinten sekä kiinteistönvalvonnan laitteiden liittämiseksi kaupungin verkkoon.

5.1 Testiympäristö

Testaamista varten käytössä oli HP 2530-48G-PoE+ -kytkin, Canon LBP6070 tulostin sekä kaksi HP elitebook 840 kannettavaa tietokonetta. Lisäksi käytettävissä oli Lahden kaupungin Microsoft IPAM-palvelin sekä Aruba ClearPass 6.6.0 -palvelin. Palvelimet olivat tuotantokäytössä, eikä niiden asennus ja käyttöönotto sisälly tämän työn laajuuteen.

5.1.1 Kytkimen konfiguraatio

Kytkimen perusasetusten kuten VLAN- ja etähallinta-asetusten lisäksi tuli kytkimelle määrittää RADIUS-palvelimeksi ClearPass palvelin komennoilla:

radius-server host x.x.x.x key "yyyyyyyy"

radius-server host x.x.x.x dyn-authorization

radius-server host x.x.x.x time-window 0

Ensimmäinen komento asettaa ClearPass palvelimen RADIUS-palvelimeksi. Toinen komento ottaa käyttöön RADIUS CoA -toimimnallisuuden. Kolmannella komennolla kytkimen sallitaan ottavan vastaan CoA-viestejä milloin tahansa. Seuraavaksi otetaan käyttöön RADIUS Accounting 2 minuutin päivitysvälillä:

aaa accounting network start-stop radius

aaa accounting update periodic 2

Määritetään kytkimelle käyttöön porttikohtainen 802.1x todentaminen ja otetaan 802.1x käyttöön:

aaa authentication port-access eap-radius

aaa port-access authenticator active

Lopuksi 802.1x todentaminen on otettava käyttöön porttitasolla. Testikäytössä käytettiin kytkimen portteja 11 ja 12. Sallitaan vain yksi todennetun käyttäjän portissa ja asetetaan 30 sekunnin aika, jolloin vain EAP-paketit sallitaan. Näin toimimalla 802.1x päätelaitteilla on tarpeeksi aikaa tunnistautua ja estetään laitteita saamasta IP-osoitteita DHCP-palvelimelta väärästä VLANista kesken tunnistautumisprosessin.

aaa port-access authenticator 11-12 client-limit 1

aaa port-access authenticator 11-12 unauth-period 30

Koska esimerkiksi käytetyssä tulostimessa ei ole tukea 802.1x autentikoinnille, on kytkimelle otettava käyttöön myös porttikohtainen MAC-pohjainen todentaminen. Jos laite ei läpäise MAC-pohjaista tunnistautumista laitetaan portti oletus VLANiin, joksi on asetettu HALLINTO VLAN 51.

aaa port-access mac-based 11-12

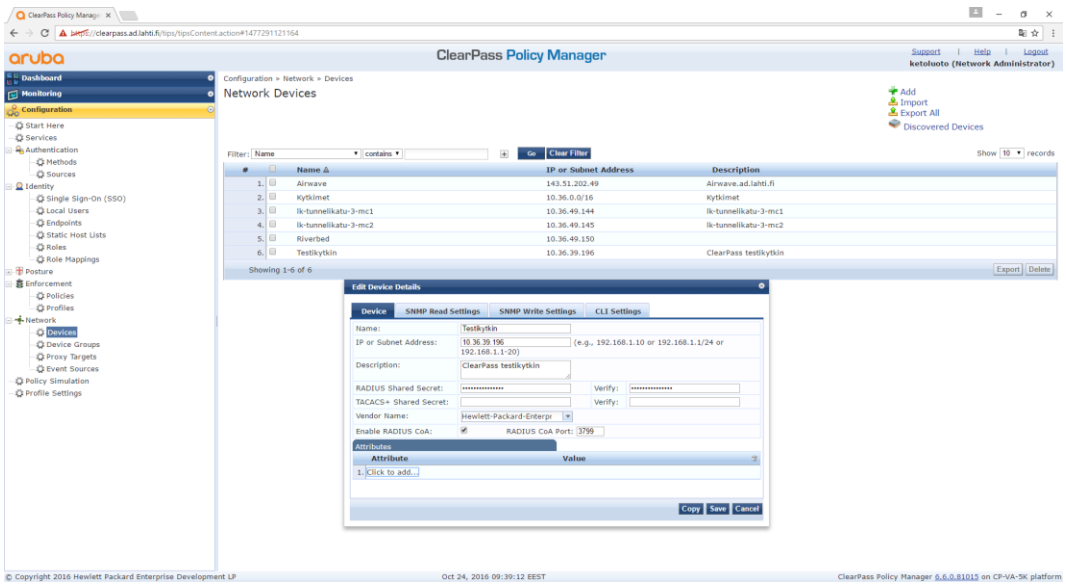
aaa port-access mac-based 11 unauth-vid 51

aaa port-access mac-based 12 unauth-vid 51

Tuotantokäytössä tunnistautumattoma laitteet laitetaan VIERAS VLANiin, mutta toistaiseksi vain HALLINTO VLANiin on konfiguroitu DHCP-kyselyt ohjautumaan ClearPass palvelimelle laitteiden profilointia varten. Jos järjestelmä otetaan käyttöön, pyydetään operaattoria tekemään muutokset myös VIERAS verkkoon.

5.1.2 Kytkimen lisääminen Aruba ClearPass Policy Manageriin

Kytkin lisätään ClearPass järjestelmään Configuration välilehdeltä löytyvältä Network devices sivulta. Kuviossa 5 käytetty kytkin lisätään siihen etähallintaa varten asetetulla IP-osoitteella, sekä aiemmin annetun radius-server komennossa esiintyvän Pre-shared keyn avulla. Lisäksi voidaan määrittää RADIUS CoA portti, mutta työssä käytetään vakio arvoa 3799.



KUVIO 5. Kytkimen lisääminen ClearPass Policy Manager -järjestelmään

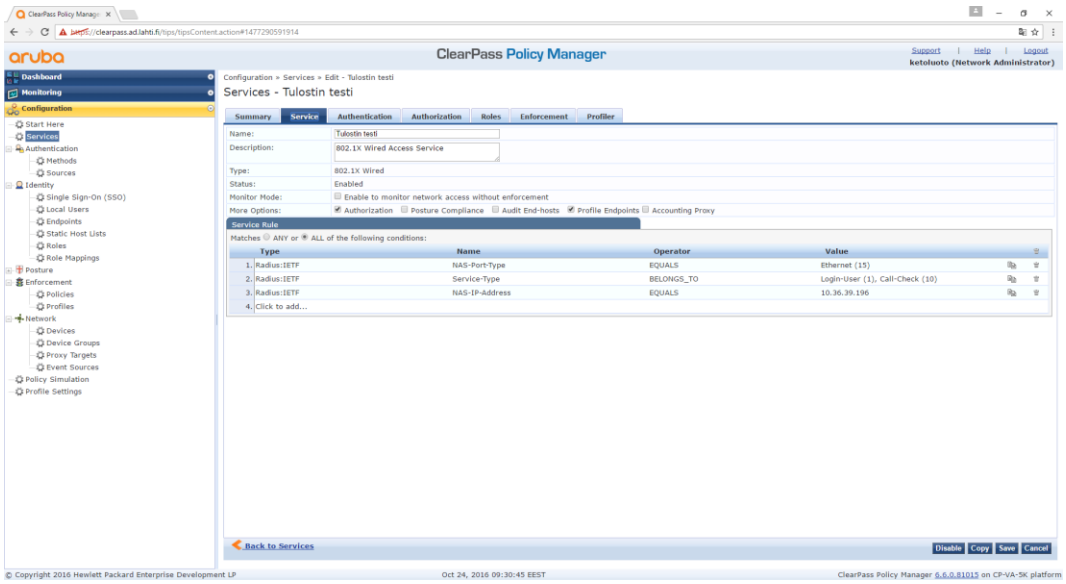
5.2 Aruba Clearpass Policy Manager

Aruba Clearpass Policy Manager eli CPPM on Hewlett Packard Enterprise -yrityksen sovellus verkkoon pääsyn valvontaan. Sen ominaisuuksia ovat enterprise-tason RADIUS ja TACACS -palvelut, tuki kaikkien valmistajien verkkolaitteille, sisäänrakennettu päätelaitteiden profilointi-palvelu sekä verkon käytäntöjen toimeenpano. (Aruba Networks 2016.)

5.2.1 CPPM-palvelu

Aluksi luodaan ClearPass-järjestelmään kuvion 6 mukainen uusi palvelu testausta varten. Palvelun tarvitsee ottaa kantaa vain testikäytössä olevan kytkimen portteihin liitettyihin laitteisiin, jottei verkon muu toiminta häiriintyisi. Niinpä yhdeksi säännöksi, jonka perusteella ClearPass käyttää luotua palvelua saapuviin RADIUS-pyyntöihin määritettiin käytettävän verkkolaitteen IP-osoitteen.

Palveluun otettiin käyttöön myös päätelaitteiden profilointi. Profilointia käytettäessä kytkimen porttiin liitetty laite voidaan automaattisesti tunnistaa esimerkiksi tulostimeksi.



KUVIO 6. ClearPass service

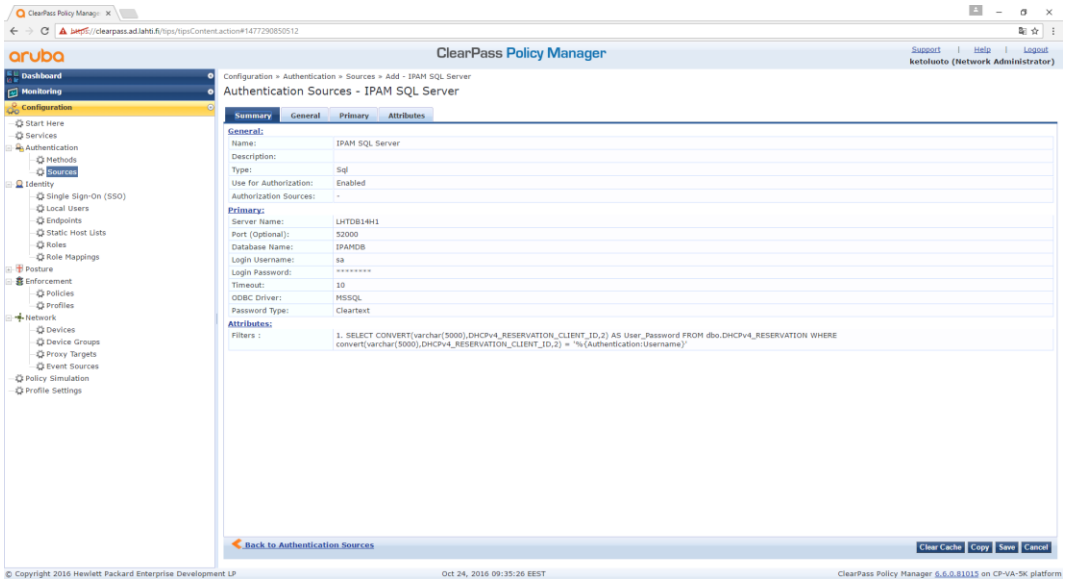
5.2.2 Todennus

Todennuksessa käytettiin “Allow All MAC AUTH”-menetelmää. Menetelmä toimii niin, että laitteen todennuksen epäonnistuessa, sallitaan sille silti pääsy omaan rajoitettun VLAN-verkkoonsa, jossa laite voidaan profiloida. Profiloinnin jälkeen on mahdollista suorittaa toimintoja laitteen sijoittamiseksi uuteen VLAN-verkkoon.

Menetelmässä käytetään IPAM-serverin tietokantaa tunnetuista laitteista. Tietokantaan lähetetään kysely, jossa verkkoon liitetyn laitteen MAC-

osoitetta verratan IPAM-serverin tietokannasta löytyvien laitteiden MAC-osoitteisiin. Kuvion 7 mukaista kyselyä varten jouduttiin selvittämään, missä muodossa IPAM-palvelin tallentaa MAC-osoitteet tietokantaan sekä taulu josta ne löytyvät.

Lahden kaupungin tapauksessa verkkotulostimet lisätään IPAM-serverille tulostusjonoa luodessa, joten niiden MAC-osoite löytyy tietokannasta todennusta varten. Kiinteistönvalvonnan laitteiden verkossa ei ole DHCP-palvelinta vaan laitteille on annettu manuaalisesti staattiset IP-osoitteet. Näiden osoitteiden listaa ylläpidetään myös IPAM-serverillä.



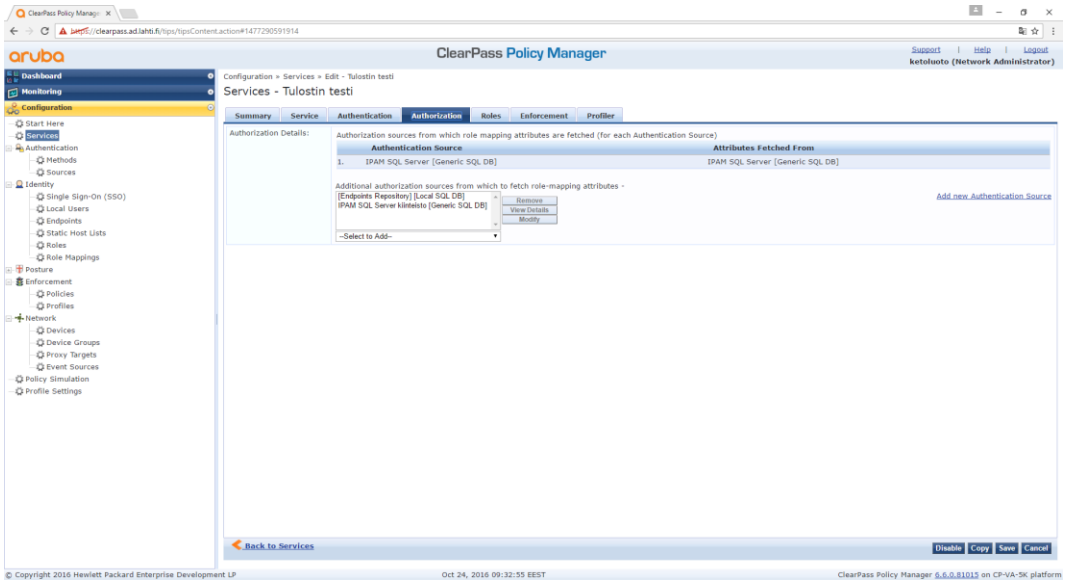
KUVIO 7. IPAM SQL-kysely

5.2.3 Valtuutus

Laitteiden valtuutusta varten tarvitaan IPAM-tietokannan lisäksi muitakin kuvion 8 mukaisia lähteitä. Tulostimien kanssa yksinkertaisimmaksi tavaksi tunnistaa laitteet todettiin ClearPass:in oma profilointi ja päätelaitelista.

Liitettäessä tulostin verkkoon sen DHCP-kysely välitetään myös ClearPass-palvelimelle. Tämän kyselyn sisältämästä datasta ClearPass profiloi laitteen tulostimeksi ja tallentaa sen päätelaitelistalle. Käytettäessä päätelaitelistaa valtuutukseen, voidaan eri laitteille antaa eri valtuudet tai

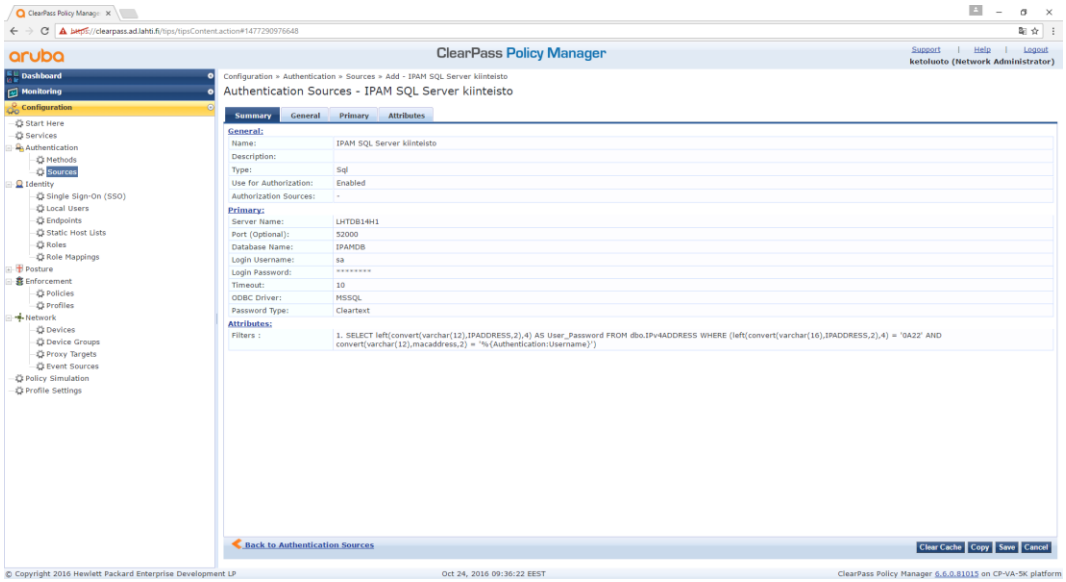
määrittää VLAN laitetyyppin perusteella. Tässä tapauksessa, kun laite on profiloitunut tulostimeksi ja sen MAC-osoite löytyy IPAM-serverin tietokannasta, asetetaan portti johon tulostin on kytketty tulostus VLANiin.



KUVIO 8. Valtuutuslähteet

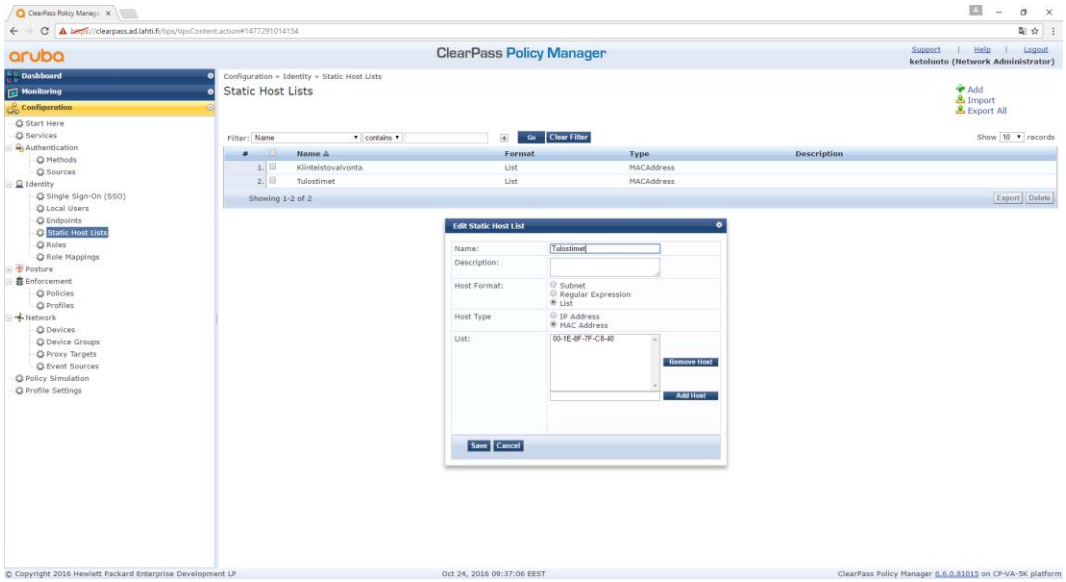
Automaattisen profiloinnin käyttö kiinteistövalvonnan laitteiden tunnistamiseen osoittautui mahdottomaksi. Laitteita on paljon erilaisia ja valmistajat vaihtelevat. Lisäksi osa laitteista on tietokoneita, jotka profiloituvat työasemiksi tai palvelimiksi. Laitteita varten luotiin oma SQL-kysely IPAM-serverin tietokantaan. Koska tietokannassa vain staattisesti määritetyt IP-osoitteet ovat kiinteistövalvonnan verkossa, voidaan todeta tämän tiedon riittävän laitteen tunnistamiseksi kiinteistövalvonnan laitteeksi.

Kuvio 4 mukaisessa SQL-kyselyssä tarkastetaan tietokannasta laitteet, joiden MAC-osoite löytyy tietokannasta ja IP-osoitteen alkuosa kuuluu kiinteistövalvonnan verkkoon. Koska IP-osoitteet tallennetaan IPAM-serverin SQL-tietokantaan Binary(4) muodossa jouduttiin kyselyä varten selvittämään käytetyn verkon osoite Binary(4) muodossa vertailua varten.



KUVIO 9. Kiinteistövalvonnan laitteiden SQL-kysely

ClearPass-järjestelmästä löytyy myös sisäänrakennettu kuviossa 10 esitetty staattinen laitteiden MAC-osoitteiden lista, jonka perusteella laitteille voidaan antaa erilaisia valtuutuksia. Listan käyttäminen tarkoituksena laitteiden siirtämiseen oikeaan VLANiin ilman verkkolaitteiden asetusten manuaalista muuttamista olisi mahdollista. Staattisen listan käyttö ei kuitenkaan olisi mielekästä, sillä listaa pitäisi ylläpitää manuaalisesti ja tiedot kaupungin verkon laitteista löytyy jo IPAM-serverin tietokannasta, joten niiden syöttäminen toiseen listaan manuaalisesti ei olisi mielekästä.



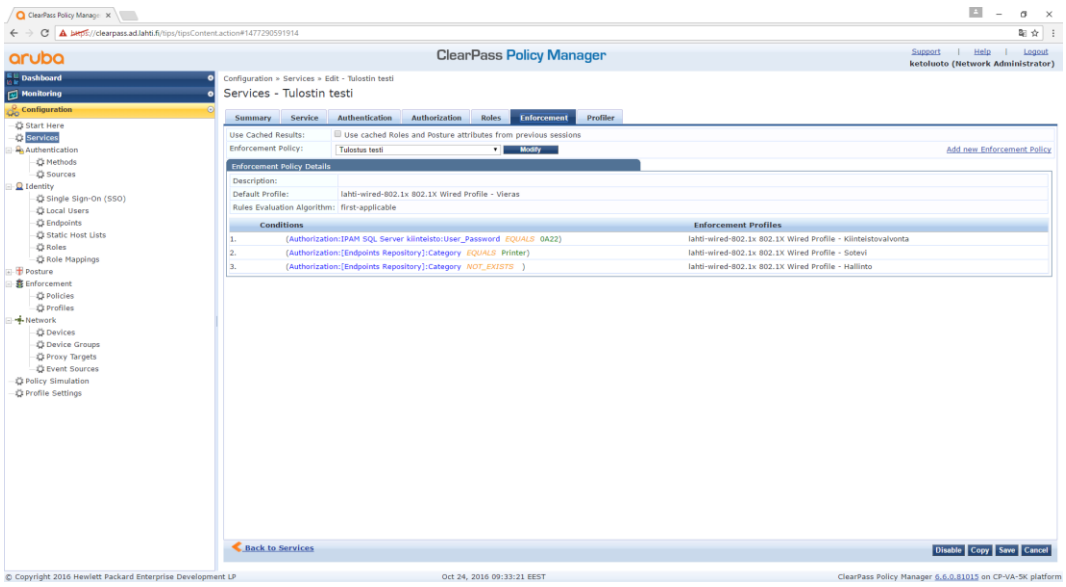
KUVIO 10. Static Host List

5.2.4 Toimeenpano

Laitteen todennuksen ja valtuutuksen jälkeen tulee määrittää halutut toimenpiteet. Työssä on tavoitteena automatisoida kytkimen VLAN asetukset, joten Clearpass piti saada määrittämään portti haluttuun VLANiin kytketyn laitteen perusteella. Tämä tapahtuu kuvion 11 Toimeenpano välilehdeltä löytyvillä säännöillä.

Aluksi määritetään, mitä kaikille tunnistautuneille laitteille tapahtuu. Koska käytetty tunnistusmenetelmä salli kaikki laitteet huolimatta siitä, mihin verkkoon ne olivat valtuutettuja, määritettiin vakioasetukseksi Lahden kaupungin vieras-verkon. Kaikki laitteet sallitaan pääsyn takaamiseksi vieras-verkkoon vieraille sekä laitteiden ClearPass päätelaitetietokantaan profiloimista varten.

Seuraava askel on käyttää valtuutusmenetelmiä laitteiden asettamiseen haluttuihin VLANeihin. Testipalvelussa lisättiin myös loppuun sääntö kaikkien muiden kuin tulostimien ja kiinteistövalvonan laitteiden ohjaamiseksi Hallinto-VLANiin, jossa laitteiden profiloiminen testivaiheessa oli mahdollista.

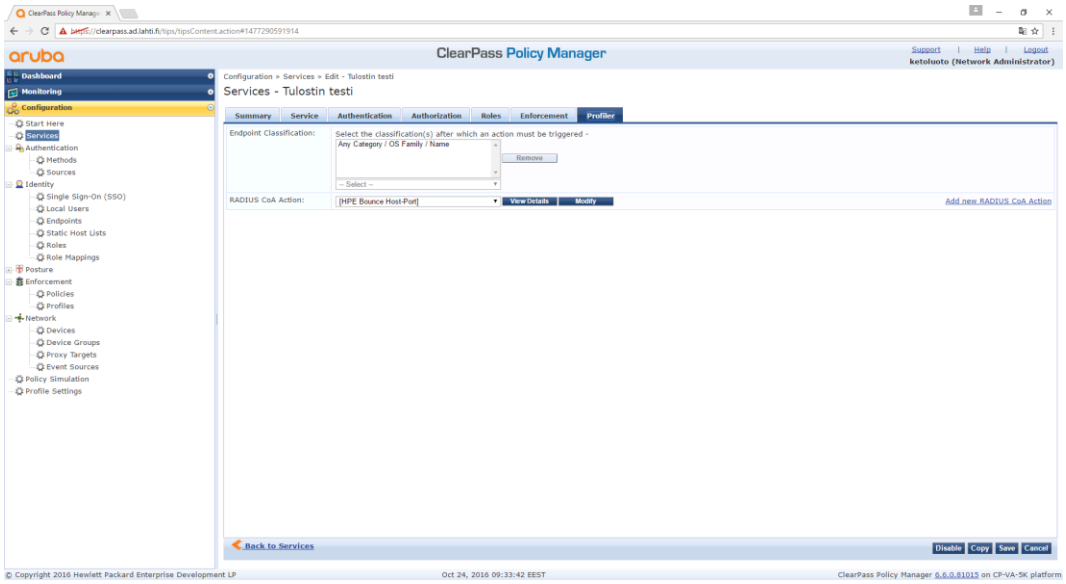


KUVIO 11. Toimeenpano välilehti

5.2.5 Profilointi

Profilointi välilehdellä voidaan muokata, miten toimitaan laitteiden profiloituessa. Esimerkiksi jos laite profiloituisi Windows työasemaksi, voitaisiin kytkimen portti poistaa käytöstä. Halutun toimimnallisuuden takaamiseksi laitteen profiloituessa valittiin kuvion 12 mukaisesti Bounce Host-Port toiminto. Tämä takaa sen, että 802.1x autentikointiprosessi alkaa alusta laitteen profiloiduttua, eikä esimerkiksi tulostimen käyttämä portti jää vieras-VLANiin.

Radius CoA bounce port viesti palvelimelta aiheuttaa kytkimen portin alustuksen ja siihen liitettyjen laitteiden DHCP-prosessin uudelleen suorituksen. Näin esimerkiksi tulostimet, jotka itsessään eivät sisällä ominaisuuksia VLANin vaihtumisen havaitsemiseksi, noutavat itselleen IP-osoitteen oikean VLANin DHCP-palvelimelta.



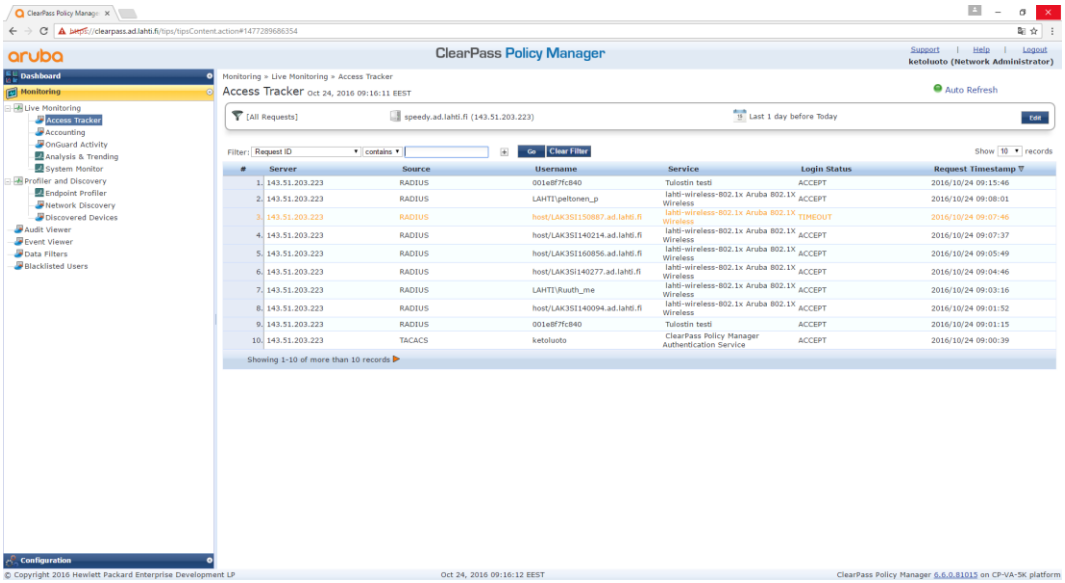
KUVIO 12. Profilointi toiminnon valinta

5.3 Testaus

Valmiin palvelun testaamiseksi käytössä oli Canon LBP6070 tulostin ja kaksi HP Elitebook 840 kannettavaa tietokonetta. Tulostinta käytettiin testaamaan laitteen profiloitumista tulostimeksi sekä päätymistä oikeaan

verkkoon. Kannettavat tietokoneet simuloivat testissä kiinteistövalvonnan päätelaitetta sekä vierasta tietokonetta.

ClearPass Policy Managerista löytyvän listauksen perusteella voidaan tarkastella kaikkia sille saapuvia kirjautumiskyselyitä. Listaus näyttää myös minkä palvelun alle kysely on luokiteltu ja työssä keskityttiin omaan ”Tulostin testi” -palveluun osuvista kyselyistä. Kuviosta 13. nähdään saapunut RADIUS-kysely, joka on osunut haluttuun palveluun kyselyn lähettäneen kytkimen perusteella.



KUVIO 13. Access tracker

5.3.1 Tulostimen testaus

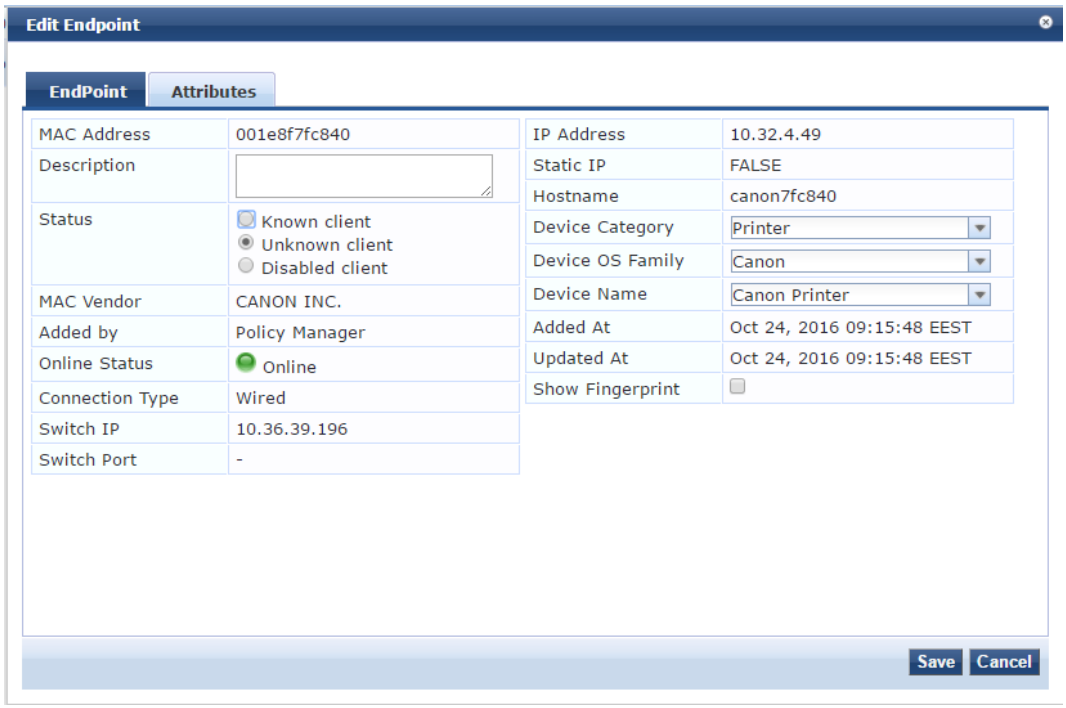
Testausta varten kytkettiin Canon LBP6070 tulostin kytkmen 11. porttiin. Koska tulostimella ei ole tukea 802.1x tunnistautumiselle, käyttöön tulee porttiin asetettu MAC-pohjainen todennus. Tässä todennusviestissä lähetetään laitteen MAC-osoite käyttäjätunnuksena ja salasanana RADIUS-palvelimelle.

Kuviossa 14. nähdään ClearPass-palvelimelle saapuneen RADIUS-pyynnön. Pyynnön perusteella laite profiloituu tulostimeksi, jonka voimme todeta mukana olevasta RADIUS CoA -välilehdestä. Tulostin sijoitetaan palvelun mukaan oikeaan VLAN-verkkoon, joka näkyy valitusta

käytäntöönpanoprofiilista. Testikäytössä jouduttiin käyttämään Hallinto-VLANia profiloimiseen.

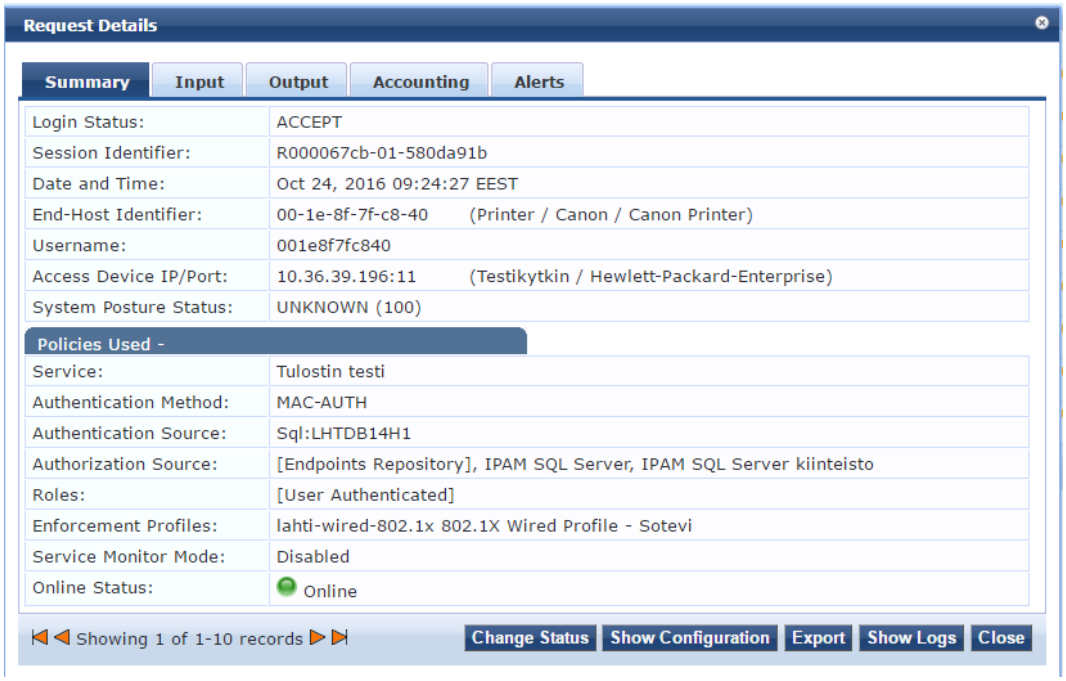
KUVIO 14. Tulostimen RADIUS-pyyntö ennen profilointia

Lisäksi voidaan todeta kuvion 15 mukaisesti tulostimen tallentuneen profiloituneena myös ClearPass:in päätelaitteiden listalle. RADIUS-CoA Bounce host port toiminnon seurauksena tulostimelta tulee palvelimelle uusi RADIUS-pyyntö.



KUVIO 15. Tulostimen tiedot tallennettuna päätelaiteluettelossa

Uuden kyselyn tarkastelussa kuviossa 16 voidaan todeta laitteen päätyneen oikeaan VLAN-verkkoon. Testissä käytettiin tulostusverkon sijaan Sotevi-verkkoa. Lisäksi laitteen ollessa jo profiloitu, ei sen uusi RADIUS-pyyntö laukaise RADIUS-CoA toimintoa.



KUVIO 16. Tulostimen RADIUS-pyyntö profiloinnin jälkeen

5.3.2 Kiinteistövalvonnan testaus

Kiinteistövalvonnan verkossa ei ole käytössä DHCP-palvelinta. Kun verkkoon lisätään laite, sen MAC-osoite lisätään IPAM-serverille ja sille määritetään manuaalisesti IP-osoite. Testausta varten lisättiin HP Elitebook 840 kannettavan tietokoneen MAC-osoite ”70:5A:0F:D3:D6:17” kiinteistövalvonnan verkkoon omalla IP-osoitteellaan.

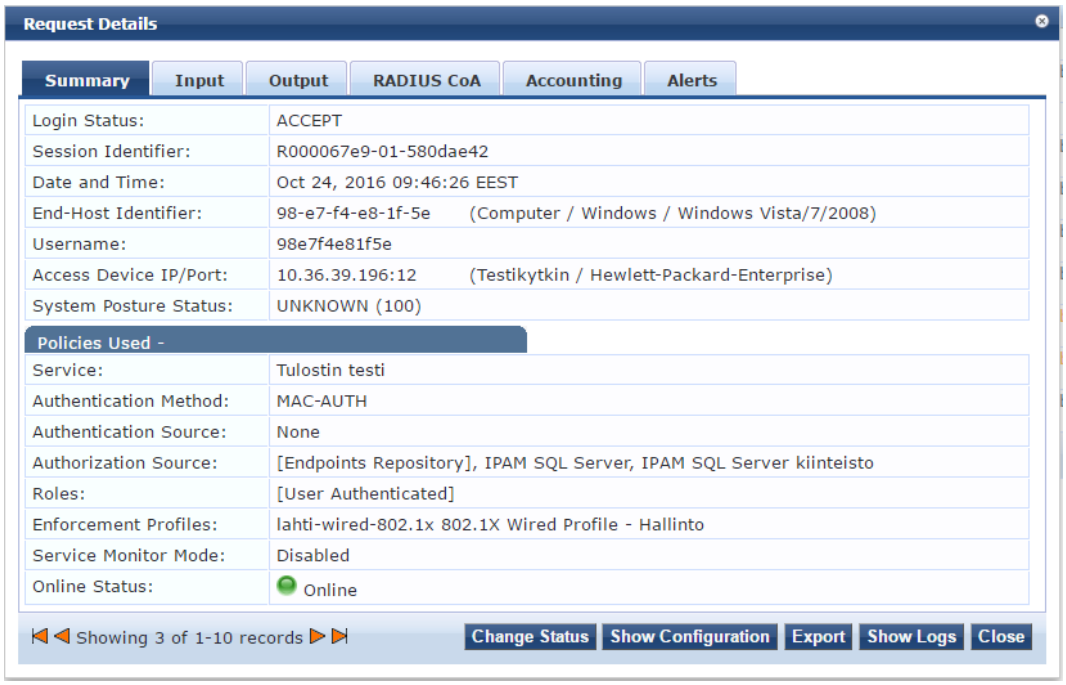
Kytkettäessä laite testikytkimen 12. porttiin voidaan ClearPass access trackerista löytää kuvion 17 mukainen RADIUS-pyyntö. Kuvasta havaitaan palvelun määrittävän kytkimen portin oikeaan VLANiin. Näin voidaan siis todeta kiinteistövalvonnan laitteiden tunnistaminen toimivaksi.

KUVIO 17. Kiinteistövalvonnan testaus

5.3.3 Vieraan laitteen testaus

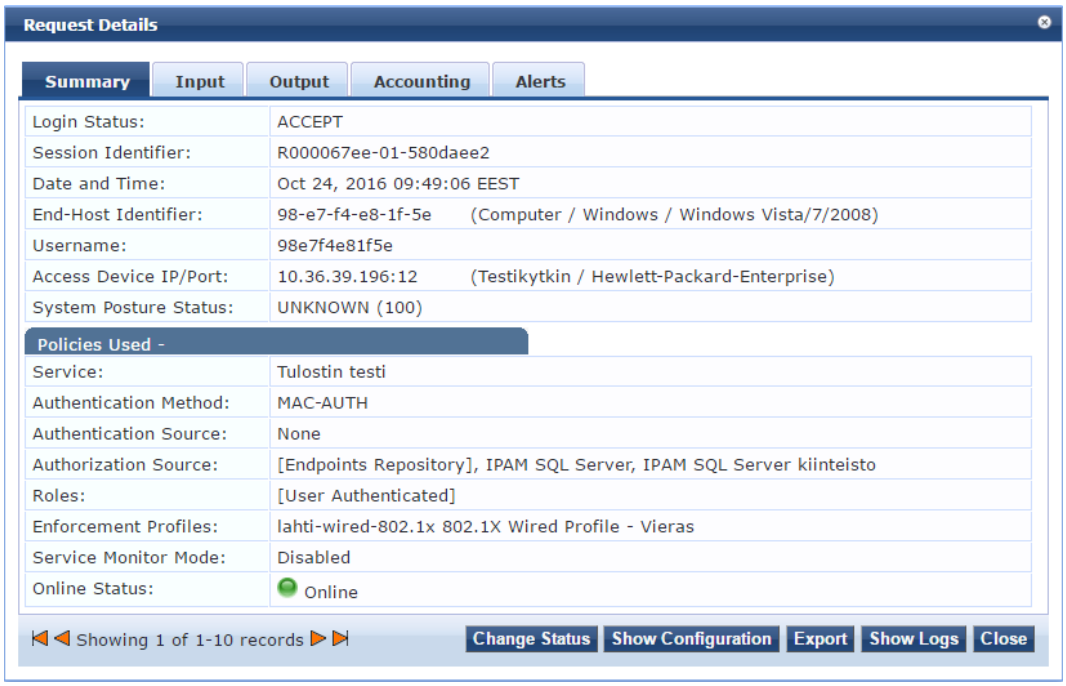
Palvelun toimintaa vieraan laitteen kohdalla testattiin käyttämällä toista HP Elitebook 840 kannettavaa tietokonetta. Konetta ei ollut aiemmin käytetty Lahden kaupungin verkossa, eikä koneen MAC-osoitetta myöskään löydy IPAM-serverin tietokannasta.

Kuviosta 18 nähdään laitteen RADIUS-pyyntö. Kuvasta voidaan havaita, että tunnistautumislähdettä ei ole. Laite sijoitetaan siis suoraan profilointia varten varten oikeaan VLAN-verkkoon. Lisäksi lähetetään RADIUS-CoA viesti takaisin kytkimelle profiloinnin seurauksena.

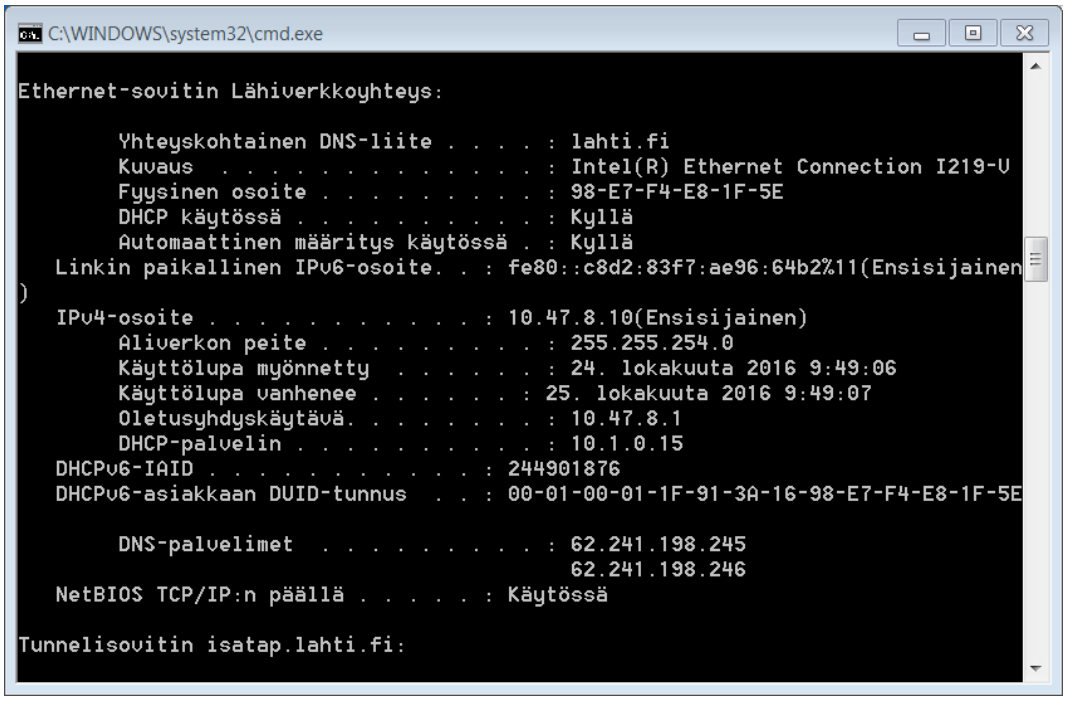


KUVIO 18. RADIUS-pyyntö ennen laitteen profiloimista

Kun portti johon laite on kytketty resetoidaan, saapuu kuvion 19 mukainen uusi RADIUS-pyyntö. Pyynnöstä nähdään kyseessä olevan edelleen vieras laite ilman tunnistautumista. Koska laite on profiloitu työasemaksi, sijoitetaan se nyt palvelun mukaisesti vieras-VLANiin. Lisäksi työasemalta voidaan tarkastaa sen päätyneen oikeaan verkkoon tarkastamalla työaseman saama IP-osoite. Kuviosta 20. nähdään IP-osoitteen tulleen vieras-verkon palvelimelta.



KUVIO 19. RADIUS-pyyntö profiloinnin jälkeen

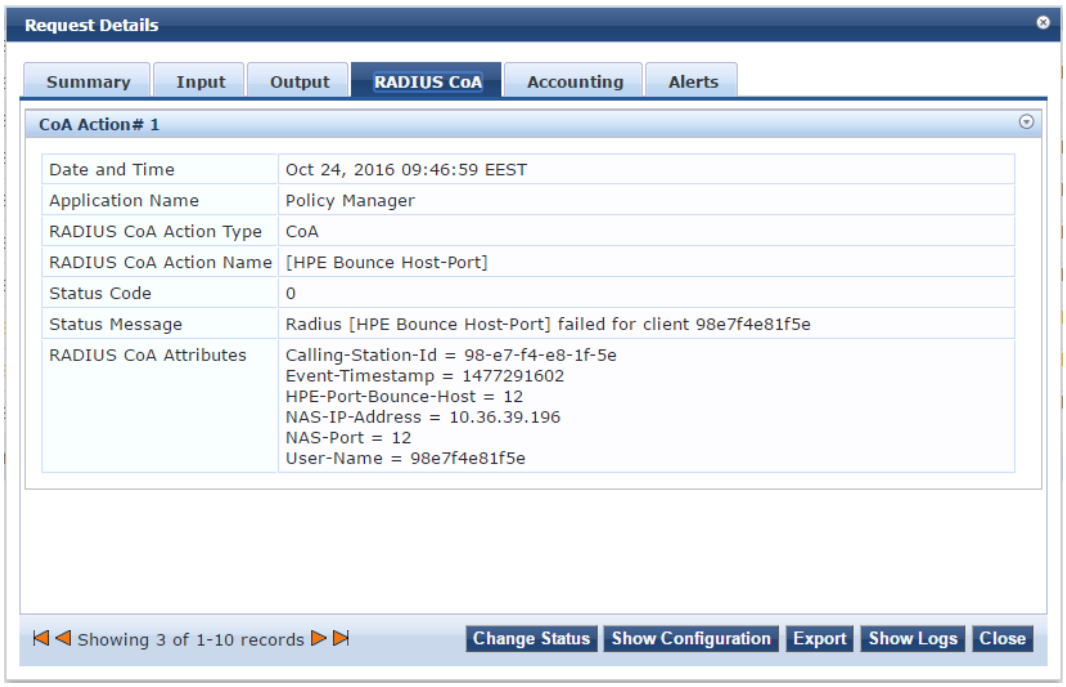


KUVIO 20. Työaseman saama IP-osoite

5.3.4 Testauksen ongelmat

Testauksessa törmättiin ongelmaan RADIUS-CoA-ominaisuuden kanssa. Kun kytkimeen kytketty laite saatiin profiloitua, ei ”Bounce Host-Port”-toiminto tuntunut toimivan, kuten kuvio 21 osoittaa. Ongelmaa tutkiessa

selvisi, ettei käytetty kytkimen malli HP 2530-48G-PoE+ (J9772A) tue RADIUS-CoA toiminnallisuutta. Niinpä testeissä toimintoa simuloitiin irrottamalla laitteen kaapeli ja kytkemällä se porttiin uudelleen profiloinnin jälkeen.



KUVIO 21. RADIUS-CoA ongelma

6 YHTEENVETO

Opinnäytetyön tavoitteena oli verkkolaitteiden VLAN konfiguraation automatisoiminen. Lisättäessä verkkoon uusi laite tai siirtämällä vanha laite uuteen kytkinporttiin, aiheutuu siitä ylimääräistä työtä, kun kytkimen portti tulee konfiguroida oikeaan VLANiin riippuen liitetyn laitteen tyypistä. Työssä käytettävät laitteet on rajattu verkkotulostimiin, kiinteistövalvonnan laitteisiin ja vieraslaitteisiin.

Työn tilaajana toimi Lahden Tietotekniikka, joka ylläpitää Lahden kaupungin tietoverkkoa. Verkossa on käytössä Aruba ClearPass-järjestelmä hallitsemassa langattomien päätelaitteiden verkkoon pääsyä. Työssä tutkittiin, soveltuuko olemassa oleva järjestelmä käytettäväksi myös langallisessa Ethernet lähiverkossa.

Työn teoriaosuudessa käydään läpi keskeisimmät aiheeseen liittyvät protokollat ja tekniikat. Näitä ovat lähiverkko, autentikointiprotokollat ja IEEE 802.1x porttikohtainen autentikointi.

Käytännön osuudessa tutkitaan, soveltuuko Aruba ClearPass-järjestelmä käytettäväksi VLAN-konfiguraation automatisoimiseen. Tutkittaessa löydetään useampi tapa saavuttaa haluttu lopputulos. Löydetyistä tavoista päädytään käyttämään IPAM-serverin tietokantaa laitteiden valtuuttamiseen staattisen listan vuoksi, sillä listan ylläpitäminen vaatisi manuaalisia toimenpiteitä, kun taas kaupungin päätelaitteet löytyvät jo valmiiksi IPAM-serverin tietokannasta.

Toteutuksessa luodaan ClearPassiin palvelu, joka rekisteröi vain testikytkimelle liitettävät laitteet. Liitetty laite profiloidaan laitteen tyypin selvittämiseksi, ja lisäksi sitä verrataan tietokannasta löytyviin laitteisiin. Kun laite täyttää halutut ehdot, eli se on esimerkiksi tulostin, joka löytyy tietokannasta, konfiguroidaan kytkinportti automaattisesti tulostus VLANiin.

Työssä päästiin haluttuun tavoitteeseen ja järjestelmää testatessa sen toiminta vastasi odotuksia. Kytkettäessä verkkotulostin kytkimeen, siirtyi tulistimen käyttämä kytkinportti automaattisesti tulostus-VLANiin. Samoin

myös kiinteistövalvonnan laitteen kohdalla kytkinportti siirtyi kiinteistövalvonnan-VLANiin. Kytkettäessä vieras laite porttiin siirtyi portti vieras-VLANiin. Testauksessa törmättiin myös ongelmiin. Käytössä ollut kytkin ei tukenut Radius CoA toimintoa, joten järjestelmää tuotantoon otettaessa on huomioitava kytkinten tuki toiminnolle, jotta järjestelmä toimisi täysin automaattisesti.

Kun järjestelmä päästään ottamaan tuotantoon ja kaikki verkon kytkimet tukevat vaadittuja ominaisuuksia, tulee se säästämään merkittävästi työtunteja ylläpidolta. Työtunteja säästyy niin uusia laitteita lisättäessä, kuin vanhojen siirroista aiheutuvien vikailmoitusten jäämisellä historiaan.

Jos järjestelmä otetaan käyttöön Lahden kaupungin verkossa, säästää järjestelmä kaupungin tietoliikenneasiantuntijoiden työaikaa automatisaatiolla vältettävissä olevilta työtehtäviltä. Lisäksi säästetään työaikaa myös Helpdesk puolella, kun laitteiden siirroista johtuvat vikailmoitukset poistuvat.

Porttikohtaisen autentikoinnin käyttö yrityksissä yleistyy koko ajan. Sen tuoman tietoturvan lisäksi yritykset voisivat kartoittaa myös tarvetta käytetyn järjestelmän soveltuvuudesta VLAN-konfiguraation automatisoinnille. Mikäli yritys on ratkaisussaan päätynyt käyttämään Aruba ClearPass -järjestelmää, mahdollistaa se nyt tutkitun mukaisesti tietyissä ympäristöissä VLAN-konfiguraation automatisoimista. Jatkossa tulisi kuitenkin tutkia myös järjestelmän soveltuvuutta konfiguraation automatisoimiseen erilaisissa ympäristöissä. Pientenkin työvaiheiden automatisaatio säästää arvokasta työaikaa ja organisaatiokoon kasvaessa myös säästetty aika kasvaa samassa suhteessa.

LÄHTEET

Aruba Networks 2016. Aruba ClearPass Policy Manager solution overview [viitattu 18.1.2017]. Saatavissa: http://www.arubanetworks.com/assets/so/SO_ClearPass.pdf

Cisco 2011. Wired 802.1X Deployment Guide [viitattu 28.5.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html

Cisco 2013. Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1 [viitattu 18.1.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_aaa.html

Cisco 2016a. 802.1X Authentication Services Configuration Guide, Cisco IOS Release 15E, Chapter: Configuring IEEE 802.1X Port-Based Authentication [viitattu 28.5.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-e/sec-usr-8021x-15-e-book/config-ieee-802x-pba.html

Cisco 2016b. Catalyst 6500 Release 12.2SX Software Configuration Guide, Chapter: IEEE 802.1X Port-Based Authentication [viitattu 28.5.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html

Cisco 2016c. Internetworking Basics [viitattu 16.4.2017]. Cisco. Saatavissa: http://docwiki.cisco.com/wiki/Internetworking_Basics

Cisco 2017. Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW, Chapter: Understanding and Configuring VLANs [viitattu 20.2.2017]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Ciscohite 2013. Difference between ISL & 802.1q [viitattu 1.3.2017]. WordPress. Saatavissa: https://ciscohite.wordpress.com/2013/05/14/difference-between-isl-802-1q/

Geier, J. 2008. Implementing 802.1X Security Solutions for Wired and Wireless Networks. Indianapolis: Wiley Publishing, Incorporated.

IEEE 2014. 802.1Q-2014 - IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks [viitattu: 20.2.2017]. Saatavissa: http://standards.ieee.org/getieee802/download/802-1Q-2014_mibs.zip

IEEE 2015. 802.3 IEEE Standard for Ethernet [viitattu 12.2.2017]. IEEE. Saatavissa: http://standards.ieee.org/about/get/802/802.3.html

Microsoft 2017a. RADIUS Protocol and Components [viitattu 2.2.2017]. Saatavissa: https://technet.microsoft.com/en-us/library/cc726017%28v=ws.10%29.aspx

Microsoft 2017b. The OSI Model's Seven Layers Defined and Functions Explained [viitattu 16.4.2017]. Microsoft. Saatavissa: https://support.microsoft.com/fi-fi/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Wikipedia 2016. OSI-malli [viitattu 16.4.2017]. Saatavissa: https://fi.wikipedia.org/wiki/OSI-malli

Transition networks 2017. Quality of Service (QoS) in High-Priority Applications [viitattu. 20.2.2017]. Saatavissa: https://www.transition.com/wp-content/uploads/2016/05/qos_wp.pdf

Turun TKK 2011. Biometriikka [viitattu 18.1.2017]. Saatavissa: http://sec.cs.tut.fi/maso/teksti.php?id=201