



**LAHDEN AMMATTIKORKEAKOULU**  
*Lahti University of Applied Sciences*

# PORTTIKOHTAINEN AUTENTIKOINTI

LAHDEN  
AMMATTIKORKEAKOULU  
Tekniikan ala  
Tietotekniikan koulutusohjelma  
Tietoliikennetekniikka  
Opinnäytetyö  
Kevät 2015  
Jarno Mäkelä

Opinnäytetyön tavoitteena oli suunnitella ja pilotoida porttikohtainen autentikointiympäristö Päijät-Hämeen sosiaali- ja terveysyhtymälle. PHSOTEY:llä on ympäri Päijät-Hämeen aluetta toimipaikkoja muuallakin kuin pelkästään Päijät-Hämeen keskussairaalan tiloissa. Näissä toimipaikoissa on myös muita yrityksiä samassa rakennuksessa ja siellä sijaitsee eri yritysten kanssa yhteisiä ristikytkenäkaappeja. Alueelle täytyisi siis suunnitella tietoturallinen ratkaisu, jotta vieraiden yritysten laitteet eivät pääse luvattomasti kytkeytymään PHSOTEY:n verkkoon.

Tietoturva muodostuu yleisesti monesta eri tekijästä. Tämän takia opinnäytetyön teoriaosuudessa käsitellään tietoturvaa, lähiverkon toimintaa, autentikointimenetelmiä sekä porttikohtaisessa autentikoinnissa käytettäviä eri protokollia. Opinnäytetyössä tehtiin pilottiympäristö porttikohtaiselle autentikoinnille, jossa käytettiin asiakaspäätettä, muutamaa erilaista kytkintä sekä RADIUS-palvelinta. Pilottiympäristössä mallinnettiin PHSOTEY:n tuotantoa ja testataan ympäristön toimivuutta eri kytkimillä, jolla varmistetaan autentikoinnin toimivuus myös työn tullessa tuotantoympäristöön. Autentikointimenetelmäksi valittiin IEEE 802.1x porttikohtainen autentikointi. Valinta oli IEEE 802.1x-autentikointi, koska IEEE 802.1x-autentikointi on tietoturvallinen ja käytännöllisin ratkaisu toteuttaa vertailluista autentikointimenetelmistä.

Kevään 2015 aikana työ pilotoitiin PHSOTEY:n tiloissa. Pilotoinnin jälkeen huomattiin, että alueella on myös muitakin laitteita kuin vain työasemia, jolloin IEEE 802.1x porttikohtaisen autentikoinnin ohelle täytyy ottaa vaihtoehtoinen autentikointimenetelmä käyttöön. Varmimmaksi tavaksi tulee MAC-autentikoinnin liittäminen IEEE 802.1x-autentikoinnin rinnalle, jolloin voidaan myös sellaisia laitteita liittää autentikoinnin piiriin, jotka eivät IEEE 802.1x-autentikointia tue. Valmis työ tulee tulevaisuudessa PHSOTEY:n tuotantoon. Porttikohtainen autentikointi on ollut jo suunnitteilla, mutta sitä ei ole vielä ehditty pilotoimaan.

Asiasanat: tietoturva, lähiverkko, IEEE 802.1x, MAC-autentikointi, RADIUS

Lahti University of Applied Sciences  
Degree Programme in Information Technology

MÄKELÄ, JARNO:

Port-Based Authentication

Bachelor's Thesis in Telecommunications Technology, 53 pages, 7 pages of  
appendices

Spring 2015

## ABSTRACT

---

The goal of this thesis was to create and test a port based authentication system for the Päijät-Häme's Social and Health Group. They have offices in various locations in Päijät-Häme. In these buildings there are also other companies and there should be a plan for a secure method how to block computers of other businesses accessing the Päijät-Häme Social and Health Group's network.

Information security usually depends on various factors. This is why the theory part of the thesis contains several topics such as information security, local area networks, authentication methods and different protocols used in port-based authentication. In the thesis, a pilot environment was made and it consisted of a client, a couple of switches and a RADIUS server. In the pilot phase the Päijät-Häme Social and Health Group's production design was modeled. The functioning of the switches was tested in order to secure the functioning of the environment when the pilot turns into production. The IEEE 802.1x authentication method was chosen, because it is the most secure and practical method to implement.

During spring 2015 the port-based authentication environment was piloted in the IT area of the Päijät-Häme Social and Health Group. After the pilot phase it was found that all the devices in the areas network are not just computers that support the IEEE 802.1x port-based authentication, and therefore in the future production phase, there should be some other authentication method to be attached to the IEEE 802.1x authentication. The most secure way is MAC authentication, because you can authenticate devices not supporting the IEEE 802.1x authentication with it.

Key words: information security, LAN, IEEE 802.1x, MAC authentication, RADIUS

## SISÄLLYS

1	JOHDANTO	2
2	TIETOTURVALLISUUS	3
2.1	Tietoturvan määritelmä	3
2.2	Tietoturva ennen ja nyt	4
3	LÄHIVERKKO	5
3.1	OSI-malli	5
3.2	Virtuaalinen lähiverkko	8
4	YHTEYSPROTOKOLLAT	10
4.1	PPP	10
4.1.1	LCP-protokolla	11
4.1.2	NCP-protokolla	12
4.2	PAP	12
4.3	CHAP	13
4.4	EAP	15
4.4.1	EAP-autentikointiprosessi	17
4.4.2	EAPOL	18
4.5	PEAP	19
5	AUTENTIKOINTIPROTOKOLLAT	21
5.1	AAA	21
5.2	RADIUS	21
6	AUTENTIKOINTIMENETELMÄT	23
6.1	IEEE 802.1x	23
6.2	IEEE 802.1x:n vaatimukset	24
6.3	MAC-autentikointi	26
6.4	Portaali-autentikointi	27
6.5	Autentikointimenetelmien vertailu	28
7	PILOTTIYMPÄRISTÖ	31
7.1	Palvelimet	31
7.2	Kytkimet	32
8	AUTENTIKOINNIN TOTEUTUS	34
8.1	Sertifikaatin luominen	34

8.2	RADIUS	38
8.3	Kytkimien konfiguroinnit	42
8.4	Ympäristön testaus	44
8.5	Autentikoinnin toiminta	48
9	YHTEENVETO	50
	LÄHTEET	51
	LIITTEET	54

# 1 JOHDANTO

Maailmassa tietotekniikan määrä kasvaa jatkuvasti ja yhä useammat työtehtävät tehdään joko tietokonetta tai vastaavaa päätelaitetta käyttäen. Yritysten harmiksi muodostuu usein tehokkaan ja hallittavan tietoturvan ylläpitäminen, sillä tietoturvan suunnittelemiseen ja ylläpitämiseen kuluu yhä enemmän aikaa ja resursseja. Monissa yrityksissä vierailee myöskin ulkopuolisia henkilöitä, joilla on oma päätelaite käytössä. Jos yrityksen verkko on vielä julkinen, niin ulkopuolinen käyttäjä voi lisätä oman päätelaitteensa yrityksen sisäverkkoon ja mahdollisesti saastuttaa ja lamauttaa osan verkosta.

Kohdeympäristössä Päijät-Hämeen sosiaali- ja terveisyhtymässä on otettu vierailijoille käyttöön vieras WLAN, mutta pöytätöasemien pääsyä ei ole yhtymässä estetty. Ongelmaksi pöytätöasemien kohdalla muodostuu sellaisten toimipisteiden tietoturvallisuus, missä on myös muita yrityksiä samassa rakennuksessa.

Opinnäytetyön aiheena on porttikohtaisen autentikoinnin suunnittelu ja pilottiympäristön toteutus. Työn tavoitteena on saada toimiva ympäristö, jossa jokainen työasema joutuu todistamaan jäsenyytensä yhtymän toimialueeseen niin sanotun AAA:n eli todennuksen, valtuutuksen ja tilastoinnin avulla (*Authentication, Authorization, Accounting*).

Porttikohtainen autentikointi on tietoturvaa lisäävä ominaisuus, joka on ollut suunnitteilla PHSOTEY:ssä, mutta sitä ei ole vielä toteutettu käytännössä. Porttikohtaisella autentikoimisella pystytään estämään ulkopuolisten käyttäjien liittyminen yhtymän sisäverkkoon. Tällä saadaan lisättyä tietoturvan tasoa merkittävästi yhtymässä.

Toimintaympäristön suunnittelu ja pystyttäminen on teknillisesti haastava ja vaatii tekijältä tuntemusta palvelinympäristöstä sekä aktiivilaitteista. Teoriaosuudessa käydään läpi lyhyesti tietoturvaa, lähiverkon teknologiaa, työssä käytettäviä protokollia sekä sitä, mitä pilottiympäristön suunnitteleminen ja toteuttaminen vaatii.

Kohdeympäristönä toimii Päijät-Hämeen Sosiaali- ja Terveysyhtymä. Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymä, jonka käyttönimi on Päijät-Hämeen sosiaali- ja terveysyhtymä ja se aloitti toimintansa 1.1.2007. Yhtymän toimialat ovat erikoissairaanhoidon, sosiaali- ja perusterveydenhuolto sekä ympäristöterveydenhuolto. Päijät-Hämeen Sosiaali- ja Terveysyhtymässä työskentelee noin 4000 henkilöä. Sosiaali- ja terveysyhtymä antaa erikoissairaanhoidon palveluja 14 jäsenkunnalle (Asikkala, Hartola, Heinola, Hollola, Hämeenkoski, Iitti, Kärkölä, Lahti, Myrskylä, Nastola, Orimattila, Padasjoki, Pukkila, ja Sysmä), joiden asukasluku oli 31.12.2013 yhteensä 213 428. (Päijät-Hämeen sosiaali- ja terveysyhtymä 2015.)

## 2 TIETOTURVALLISUUS

### 2.1 Tietoturvan määritelmä

*”Tietoturva mielletään usein tekniseksi ongelmaksi, vaikka ihminen on heikoin lenkki”*. Tietoturvallisuus yrityksessä on osa organisaationsa toiminnan laatua. Tietoturvalla tarkoitetaan tietoaaineistojen, tietojärjestelmien ja palveluiden suojausta, jossa otetaan huomioon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyviä riskejä (Pietikäinen 2013; Albrecht 2015.)

Käytännössä tietoturvallisuudella tarkoitetaan tietojen ja tietojärjestelmien pysymistä vain niihin oikeutettujen saatavilla. Ulkopuolisille ei anneta mahdollisuutta päästä käsiksi yrityksen tietoihin, koska heille se tieto ei kuulu. Tietojen käsittelyynkin oikeutetut henkilöt saavat käsitellä tietoja vain asianmukaisissa työtehtävissään. Minkään asiattoman toiminnan, haittaohjelman, laitteisto- tai ohjelmistovian tai muiden vahinkojen, tapahtumien tai häiriötilanteiden vuoksi tieto ei saa paljastua, muuttua tai tuhoutua. (Pietikäinen 2013.)

Tietojärjestelmien tai palveluiden on pysyttävä toiminnassa ja oltava saatavilla silloin, kun niitä tarvitaan. Sellaiset palvelut ovat lisääntyneet, joissa palvelun käyttö on ympärivuorokautista, kuten sähköisissä asiointipalveluissa. Tällaisten palveluiden on kyettävä tunnistamaan palvelua käyttävä henkilö luotettavasti sekä pidettävä lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää. (Pietikäinen 2013.)

Tietoturvatoimenpiteillä turvataan tietoa käyttävän henkilön etuja. Suuri osa yhteiskunnan toiminnoista ovat joiltakin osin riippuvaisia tietojen käsittelystä tai siirrosta. Harva organisaatio on enää verkottuneessa toimintaympäristössä itse vastuussa omasta tietoturvallisuudestaan. Suurimmat tietoturvallisuuden vaarantumiseen liittyvät ongelmat johtuvatkin yleisesti kiireestä, huolimattomuudesta, osaamattomuudesta tai tietojärjestelmien toteutuksen ja käytön laadullisista tekijöistä. (Pietikäinen 2013.)



## 2.2 Tietoturva ennen ja nyt

Tietoturvan osalla ongelmia on ollut aina olemassa. Internetin aikakaudella ennen kaikkea sähköisen tiedon joutuminen väärin käsiin on tullut yhä yleisemmäksi ja tätä kautta myös tietoturva käsite on yhä yleisempi puheenaihe kuin ennen.

Nykyisin yritysten myyntiartikkelit perustuvat tutkimuksiin ja kokeiden avulla saatuihin tietoihin, tästä syystä myös tiedosta on tullut varkaille kiinnostava aihe. Sähköisen tiedon varastaminen on myös helpompi ja kiinnostavampi tapa toteuttaa tietovarkaus, sillä se ei vaadi fyysisiä toimenpiteitä. Tiedot voidaan varastaa sähköisesti Internetin välityksellä paikasta riippumatta. (Lindström 2015.)

Nykypäivän liikkuvassa sekä mobiilipainotteisessa maailmassa tietoturvallisuuden merkitys vain korostuu. Tietoturvallisuutta ei tulisi tarkastella enää pelkästään erillisenä osa-alueena vaan tietoturvallisuus tulisi ymmärtää osaksi kaikkea mitä yrityksessä tapahtuu. Tietoturvallisuus ei tarkoita pelkästään ulkoisia uhkia, kuten haittaohjelmistoja ja verkkohyökkäyksiä tietojärjestelmiä kohtaan, vaan myös työntekijöiden itsessään mukana pidettäviä tietoja, jotka saattavat vahingossa kadota. (Kinnunen 2015.)

Tietoturvaan sisältyy teknisten laitteiden ja ohjelmien lisäksi myös suuri määrä koulutusta ja asioiden ohjeistusta. Tietoturvallisuutta tulisikin tarkastella kokonaisuutena, jota tarpeen mukaan pystyttäisiin mittaamaan. Tietoturvariskit ovat koko yrityksen yksi liiketoimintariskeistä, joten yrityksen johdolla tulisi olla vastuu riskin hallinnasta. Riittävällä koulutuksella ja ohjeistuksella riskiä voidaan helposti pienentää ja samalla yrityksen johto saa paremman kuvan siitä, miten asioita yrityksessä käytännön tasolla hoidetaan. (Kinnunen 2015.)

### 3 LÄHIVERKKO

Lähiverkko (*Local Area Network*) on tietoliikenneverkko, jossa tietokoneet ja muut laitteet ovat yhteydessä toisiinsa ja sijaitsevat maantieteellisesti suhteellisen pienellä alueella, yhdessä tai useammassa rakennuksessa, kuten koulu- tai työympäristössä. Lähiverkko on hyödyllinen resurssien jakamisessa, kuten tiedostojen, tulostimien tai ohjelmien jakamisessa. Lisäksi nämä voidaan lähiverkon lisäksi yhdistää laajaverkkoon tai Internetiin. (Mitchell 2015.)

Useimmat lähiverkot rakennetaan suhteellisen halvoista materiaaleista, kuten ethernet kaapeleista, verkkoadapttereista ja hubeista. Myös langattomia laitteita, kuten reitittimiä, voidaan käyttää lähiverkossa ja näin laajentaa lähiverkkoa langattomasti. (Mitchell 2015.)

#### 3.1 OSI-malli

OSI (*Open Systems Interconnection Reference Model*) on ISO-järjestön (*International Organization for Standardization*) kehittämä tiedonsiirtoprotokollien viitemalli, joka kuvaa tietoliikennejärjestelmän jakamista seitsemään kerrokseen. OSI-mallin seitsemän eri kerrosta on esitetty kuviossa 1. OSI-malli kehitettiin 1980-luvun alussa. OSI-malli kehitettiin, jotta eri tietoliikennejärjestelmät suunniteltaisiin yhtäläisesti. OSI-malli toimii pyramidin tavoin, eli jokainen kerros käyttää aina yhtä alemman kerroksen palveluja ja tarjoaa palveluja aina yhtä kerrosta ylemmäs. (OSI-malli 2015.)



KUVIO 1. OSI-mallin kerrokset (OSI-malli 2015.)

OSI-mallissa on seitsemän päällekkäistä kerrosta, jossa jokaisella on oma tehtävänsä:

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

Fyysinen kerros (*Physical layer*), eli OSI-mallin alin kerros, hoitaa kaiken tiedonsiirtoon liittyvät loogiset, sähköiset ja mekaaniset asiat. Fyysisellä tasolla voidaan tietoa siirtää kahdella eri tavalla joko sarjamuotoisella tiedonsiirrolla, tai rinnakkaismuotoisella tiedonsiirrolla. Sarjamuotoisessa tiedonsiirrossa siirretään dataa peräkkäin yksi bitti kerrallaan, kun taas rinnakkaismuotoisessa tiedonsiirrossa yhden merkin kaikki bitit siirretään yhtäaikaan jokainen omaa johdintaan pitkin. Rinnakkaismuotoinen tiedonsiirto on tietysti paljon nopeampaa,

mutta monien rinnakkaisten johtimien vuoksi rinnakkainen tiedonsiirto ei ole niin kannattavaa langattomissa yhteyksissä eikä pitkillä matkoilla sen mahdollisten tiedonsiirtovirheiden vuoksi. (OSI-malli 2015.)

Siirtoyhteyseros (*Data Link Layer*) on OSI-mallin toinen kerros, joka hoitaa yhteyden luomisen, virheiden korjaamisen sekä yhteyden purkamisen. Yhteyden luominen ja purkaminen tapahtuu fyysisestä kerroksesta riippuen.

Siirtoyhteyseros hoitaa niin sanotun vuonohjauksen, eli se pitää huolen siitä, ettei tietoa lähetetä nopeammin, kuin vastaanottaja sitä pystyy käsittelemään. Siirtoyhteyseros pitää myös huolen siitä, ettei sen läpi kulkeva tieto sisällä virheitä, ja jos se havaitsee virheen, lähettää se virheellisen datan uudelleen eteenpäin. (OSI-malli 2015.)

Verkkokerros (*Network Layer*) on OSI-mallin kolmas kerros, joka tarjoaa verkon rakenteesta ja kytkentätekniikasta riippumattoman tiedonsiirron. Tämän kerroksen tarkoituksena on piilottaa tiedonsiirrossa käytettävien fyysisten toteutuksien piirteet, kuten IP-osoitteet. Verkkokerroksen tarkoituksena on myös valita, mitä reittiä data lähetetään monihaarisessa tietoliikenneverkossa. (OSI-malli 2015.)

Kuljetuseros (*Transport layer*) vastaa tiedonsiirtoyhteyden päästä-päähän (*Point-to-Point*) -yhteyksistä tietoliikenneverkossa. Tietoliikenneverkossa saattaa tapahtua laitteiden hajoamisia tai muuten yhteyden katkeamisia, joten kuljetuseroksen tehtävänä on huolehtia, että vian sattuessa käytetään vaihtoehtoisia reittejä määränpäähän. (OSI-malli 2015.)

Istunto- tai yhteysjaksokerroksen (*Session layer*) tehtävänä on huolehtia, että fyysisten yhteyksien katketessa ei tiedonsiirto sekoja vaan se hoitaa yhteyden jatkamisen katkon jälkeen. Istuntokerros järjestää yhteyden kahden ohjelman välille hoitaen yhteyden muodostamisen, ylläpidon ja purkamisen.

Istuntokerroksen toinen tehtävä on muodostaa keskusteluyhteys istuntojen välille. Tämä voidaan toteuttaa kahdella eri tavalla: joko molemmat lähettävät ja vastaanottavat samanaikaisesti dataa tai siten, että vuorotellen vain toinen lähettää ja toinen vastaanottaa. (OSI-malli 2015.)

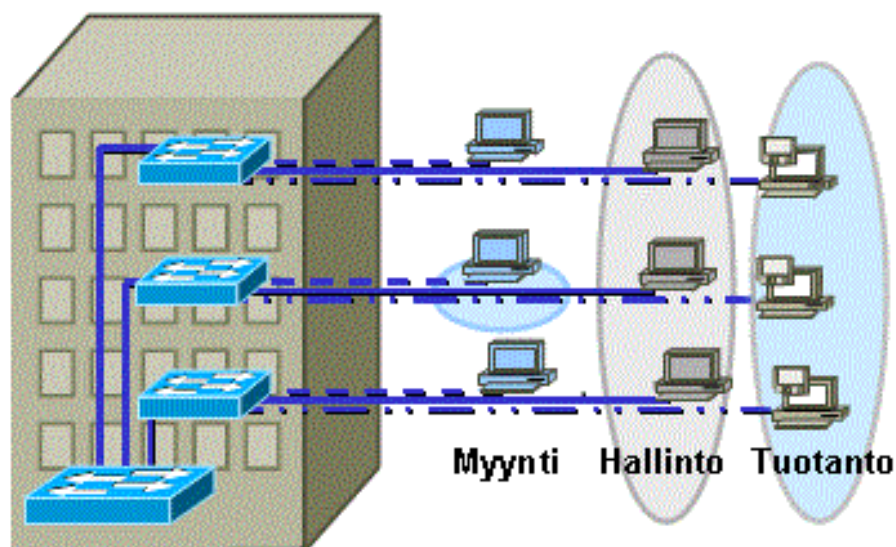
Esitustapakerros (*Presentation layer*) ratkoo mahdollisia ongelmia jos niitä tulee vastaan koneiden kommunikoidessa keskenään. Esitustapakerros ei liity enää

varsinaiseen tiedonsiirtoon, vaan on kerros, jolla sovitaan laitteiden välisestä yhteisestä tiedon esitystavasta. (OSI-malli 2015.)

Sovelluskerroksen (*Application layer*) tehtävänä on eri protokollien tarjoaminen sovellusten käyttöön. Sovelluskerros toimii niin sanottuna linkkinä siihen ohjelmaan, joka tiedonsiirtoa tarvitsee, kuten esimerkiksi sähköposti. (OSI-malli 2015.)

### 3.2 Virtuaalinen lähiverkko

Virtuaalinen lähiverkko eli VLAN (*Virtual LAN*) on looginen ryhmä tietokoneita, palvelimia tai verkkolaitteita, jotka ovat samassa lähiverkossa huolimatta niiden maantieteellisestä sijainnistaan. VLAN sallii ryhmän koneita tai käyttäjiä kommunikoidaan simuloidussa ympäristössä, jossa ne luulevat kuuluvansa yhteen samaan lähiverkkoon. Useimmiten virtuaalisia lähiverkkoja käytetään toiminnallisista syistä ja esimerkiksi myynti, hallinto ja tuotanto halutaan pitää erillisissä verkoissaan. Tämä on havainnollistettu kuviossa 2. Virtuaalisilla lähiverkoilla saavutetaan parempaa skaalautuvutta verkossa. VLAN:lla voidaan myös parantaa tietoturvaa, käyttäjien hallintaa sekä tehostaa koneiden hallittavuutta. Myös verkossa tapahtuvat muutokset on nopea ja helppo ottaa virtuaalisessa lähiverkossa käyttöön. (Janssen 2015.)



KUVIO 2. VLAN-segmentointi (VLAN-perusteet 2015.)

VLAN-jäsenyys määritellään joko kytkimien porttien mukaan tai päätelaitteen verkkokortin eli sen MAC-osoitteen mukaan. Jos VLAN-jäsenyys määritellään kytkimen portin mukaan, kuuluu kytkimen porttiin liitetty laite aina samaan VLAN:iin riippumatta laitteesta. Tätä kutsutaan staattiseksi VLAN:ksi. Jos käyttäjä ja työasema siirtyvät toiseen paikkaan, joudutaan kytkin konfiguroimaan uudestaan. Jos taas kytkimelle määritellään VLAN verkkokortin mukaan, ei muutoksia tarvitse tehdä, jos työasema siirtyy toiseen paikkaan. Tätä tapaa kutsutaan dynaamiseksi VLAN:ksi. Muuttuvissa ympäristöissä dynaaminen VLAN on huomattavasti järkevämpi tapa toteuttaa ylläpidon kannalta. (VLAN-perusteet 2015.)

VLAN mahdollistaa turvallisen ja joustavan liikkumisen käyttäjälle. Esimerkiksi jos työasema on liitetty tiettyyn VLAN:iin, yhdistää se aina tuohon samaan VLAN:iin riippumatta sen sijainnista. Tämä helpottaa varsinkin langattomien verkkojen käyttäjiä. Langallisella puolella tämä vaatii käyttäjän tunnistusta, kuten 802.1x-protokollaa, joka ohjaa työaseman siihen VLAN:iin, johon se on määritelty kuuluvan.

802.1x-autentikoinnilla voidaan käyttää RADIUS-palvelinta ja Windowsin Active Directorya määrittämään käyttäjän tai työaseman kuuluvan johonkin tiettyyn VLAN:iin. Ilman porttikohtaista autentikointia käyttäjä liittyy siihen VLAN:iin, johon se ethernetpiuhalla liittyy ja johon kytkimen porttiin se kuuluu. Langattomissa verkoissa SSID määrittää sen, mihin verkkoon käyttäjä liittyy. (Ozlak 2012.)

## 4 YHTEYSPROTOKOLLAT

Yhteysprotokollat ovat käyttäjille näkymättömiä protokollia, joita tarvitaan verkkolaitteiden välillä kulkevan tiedonsiirron siirtämiseen. Aiemmin esitelty verkkoteknologiat tarvitsevat toimiakseen jonkin yhteisen yhteysprotokollan, jolla määritetään tekniikka, millä tavalla paketit liikkuvat verkossa ja mikä on tiedonsiirron tietoturvan taso.

Opinnäytetyössä käytiin läpi muutamia yhteysprotokollia, jotka liittyivät opinnäytetyöhön. Todellisuudessa yhteysprotokollia on muitakin, mutta ovat tekniikaltaan jo sellaisia, joita ei nykyaikana enää käytetä.

### 4.1 PPP

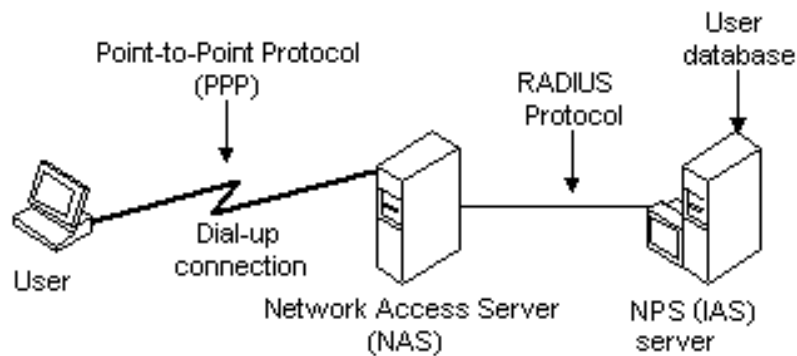
PPP (*Point to Point Protocol*) on tiedonsiirrossa käytettävä protokolla, jota käytetään muodostamaan suora yhteys verkossa olevien laitteiden välille. PPP-protokolla kehitettiin lähinnä puhelinverkko- ja modeemiyhteyksissä käytettäväksi protokollaksi, mutta sitä käytetään myös laajakaistayhteyksissä. PPP-protokolla on kehittyneempi versio SLIP-protokollasta (*Serial Line Internet Protocol*), joka kehitettiin samaan tarkoitukseen kuin mitä PPP-protokolla on, mutta käytettävyyden ja rajoitteidensa takia SLIP-protokolla on poistunut jo lähes kokonaan käytöstä. (Wikipedia 2015b.)

PPP-protokollalla on kolme pääkomponenttia, joiden mukaan se toimii:

1. Kapselointi, jota käytetään lähettämään datagrammeja määritellyn fyysisen kerroksen yli.
2. LCP (*Link Control Protocol*), jota käytetään yhteyden muodostamiseen, konfiguroimiseen ja testaamiseen.
3. NCP (*Network Control Protocol*), jota käytetään eri verkkoprotokollien yhteyden muodostamiseen sekä konfiguroimiseen.

Muodostaakseen point-to-point-yhteyden täytyy jokaisen PPP-linkin ensin lähettää LCP paketti konfiguroidakseen datalinkki yhteyden muodostamisvaiheessa. Kun yhteys on muodostettu, tarjoaa PPP valinnaisen

autentikointivaiheen ennen jatkamista verkkoprotokollan valintaan. (Simpson 1992.)



KUVIO 3. PPP-yhteys verkkolaitteiden välillä (RADIUS Authentication, Authorization, and Accounting 2015)

#### 4.1.1 LCP-protokolla

Ollakseen riittävän monipuolinen ympäristössä, jossa tapahtuu muutoksia sekä käytetään erilaisia tekniikoita, tarjoaa PPP siirtoyhteysprotokollan itsessään eli LCP-protokollan. LCP on PPP-protokollan yksi osa, ja sen tehtävänä onkin muodostaa, konfiguroida ja testata yhteyden toimivuutta. (Simpson 1992.)

Laitteet eivät voi käyttää PPP-protokollaa lähettämään dataa ennen kuin LCP-paketti on määrittänyt yhteyden eheyden. LCP-paketit on sulautettu PPP-paketteihin, ja siksi PPP yhteys on muodostettava ennen kuin LCP voi uudelleenkonfiguroida yhteyden. (Simpson 1992.)

LCP-protokollan tehtävät:

1. kapselointitavan tunnistus ja hyväksyntä verkossa
2. pakettikoon määrittäminen ja hoitaminen
3. loputtomasti kiertävien silmukoiden havaitseminen sekä muiden väärinkonfiguroitujen ongelmien havaitseminen
4. autentikointimenetelmien päättäminen.



#### 4.1.2 NCP-protokolla

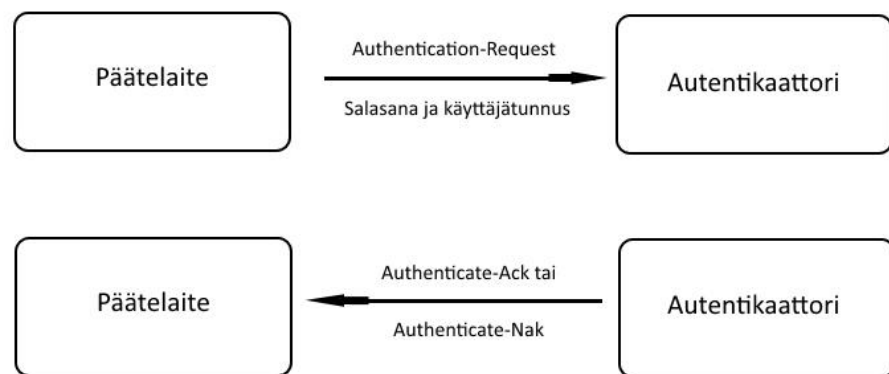
NCP-protokolla on yksi osa PPP-protokollaa aivan kuten LPC. NCP-protokollan tehtävinä on eri verkkokerrosprotokollien yhteyden muodostaminen sekä konfiguroiminen PPP-yhteyksissä. NCP-protokolla kehitettiin, sillä PPP-yhteyksien konfigurointi muodostui ongelmalliseksi. (Simpson 1992.)

LCP-protokollan on suoritettava verkon tarkistus ja määrittää perusasetukset verkkolaitteille ja niiden väliselle yhteyksille ennen kuin NCP-protokolla pystyy konfiguroimaan verkon asetuksia. NCP-protokolla pystyy hoitamaan nämä konfiguroinnit automaattisesti. (Simpson 1992.)

#### 4.2 PAP

PAP (*Password Authentication Protocol*) on autentikointiprotokolla, joka käyttää salasanaa autentikoimiseen. PPP-protokolla käyttää PAP:ia tunnistukseen käyttäjät ennen kuin he voivat muodostaa yhteyden palvelimien tarjoamiin palveluihin. (Simpson 1992.)

PAP tarjoaa yksinkertaisen tavan käyttäjän tunnistukseen käyttämällä kaksivaiheista kättelyä, kuvattu kuviossa 4. Kun PAP-protokollan käytössä linkkiyhteys on muodostettu, lähetetään käyttäjätunnus/salasana-yhdistelmää autentikaattorille niin kauan, että yhteys muodostuu tai linkki laitteen ja autentikaattorin välillä katkeaa. PAP ei ole vahva autentikonititapa, sillä salasanat lähetetään selvänä tekstinä eteenpäin eikä niitä ole salattu mitenkään. (Simpson 1992.)

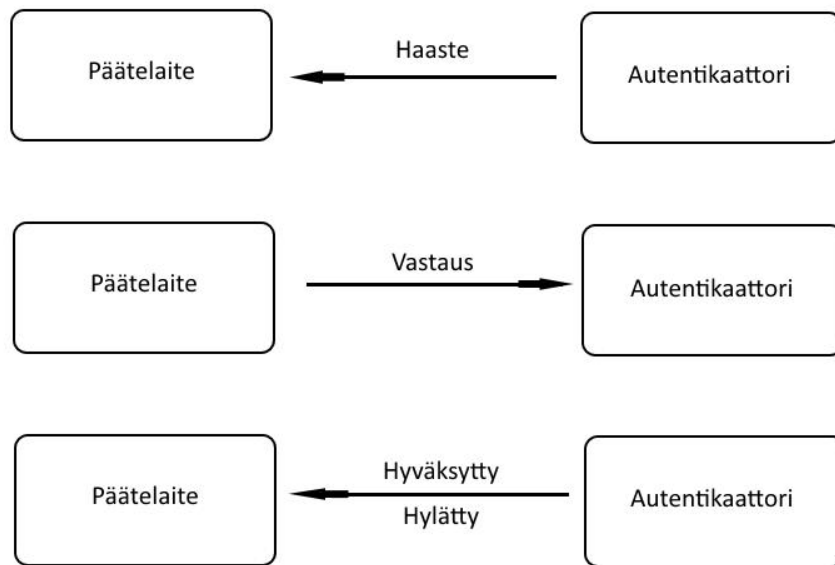


KUVIO 4. PAP-autentikoinnin toiminta

Salasanojen lähettäminen selväkielisenä verkossa ei ole tietoturvallinen ratkaisu, joten PAP-protokollan käyttöä tulisi välttää. Sitä on käytettävä vain ja ainoastaan varotoimenpiteenä, jos käytössä on vanhaa teknologiaa, joka ei tue vahvempia autentikointiprotokollia, kuten CHAP:ia tai EAP:ia.

### 4.3 CHAP

CHAP-protokolla (*Challenge-Handshake Authentication Protocol*) on autentikointiprotokolla, joka on kehitetty PAP-protokollan pohjalta. CHAP käyttää kolmivaiheista kättelyä autentikointiin ja on PAP-autentikointia tietoturvaisempi ratkaisu. Lisäksi CHAP-autentikoinnissa autentikointikättely saattaa toistua, vaikka yhteys päätelaitteen ja autentikaattorin välillä olisi jo muodostettu. Kuviossa 5 on kuvattuna CHAP-autentikointiprotokollan toiminta. (Simpson 1996.)



KUVIO 5. CHAP-autentikointiprotokolla

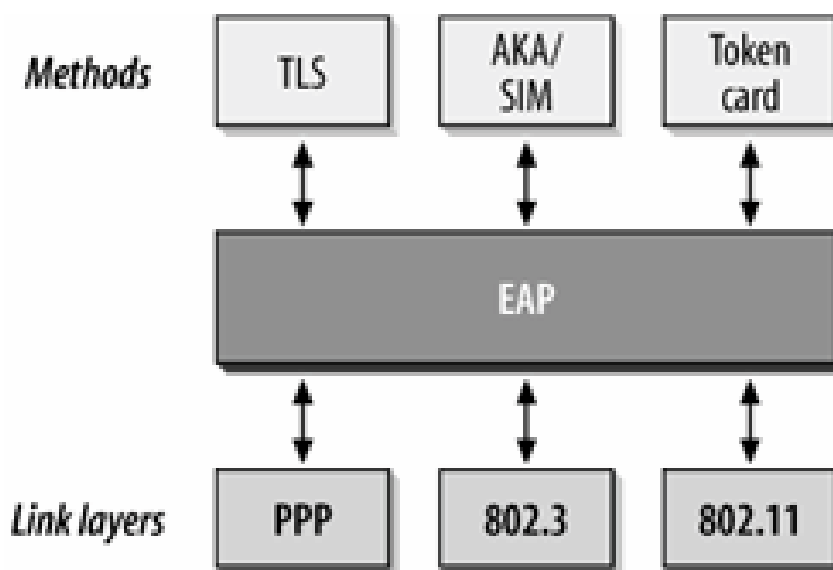
CHAP-protokollan toiminta perustuu seuraaviin vaiheisiin:

1. Yhteyden muodostamisen jälkeen autentikaattori lähettää ”haaste”-viestin päätelaitteelle.
2. Päätelaitte vastaa pyyntöön arvolla, joka on laskettu yksisuuntaisella tiivistefunktiolla.
3. Autentikaattori tarkistaa vastatun arvon ja vertaa sitä itse laskemaan arvoonsa. Jos luvut täsmäävät, niin autentikointi on onnistunut. Jos luvut eivät täsmää, yhteys katkeaa.
4. Satunnaisin väliajoin autentikaattori lähettää uuden ”haaste”-viestin päätelaitteelle ja vaiheet 1 – 3 toistuvat.

CHAP-protokollan autentikointimenetelmä perustuu salaiseen avaimen tai salasanaan, jotka vain autentikaattori ja päätelaite tietävät. Vaikka autentikointi on käytännössä vain yksisuuntainen, voi autentikointia toisaalta pitää molemminsuuntaisena autentikointina CHAP-kättelyn kolmivaiheisuuden ja jaetun salaisen avaimen takia. (Simpson 1996.)

#### 4.4 EAP

EAP-protokolla (*Extensible Authentication Protocol*) on nykyisistä autentikointiprotokollista kehittynein. EAP-protokolla on esitetty RFC 2284-dokumentissa. EAP on alun perin suunniteltu PPP-protokollan pohjalta ja PPP-protokollan kanssa käytettäväksi. EAP-autentikointikehys on kehitetty joustavaksi, ja se sopiikin monien autentikointimetodien kanssa käytettäväksi. Kuviossa 6 on esitetty EAP-protokollan arkkitehtuuria. (Hassell 2002, 108)



KUVIO 6. EAP-arkkitehtuuri (Hassell 2002, 108)

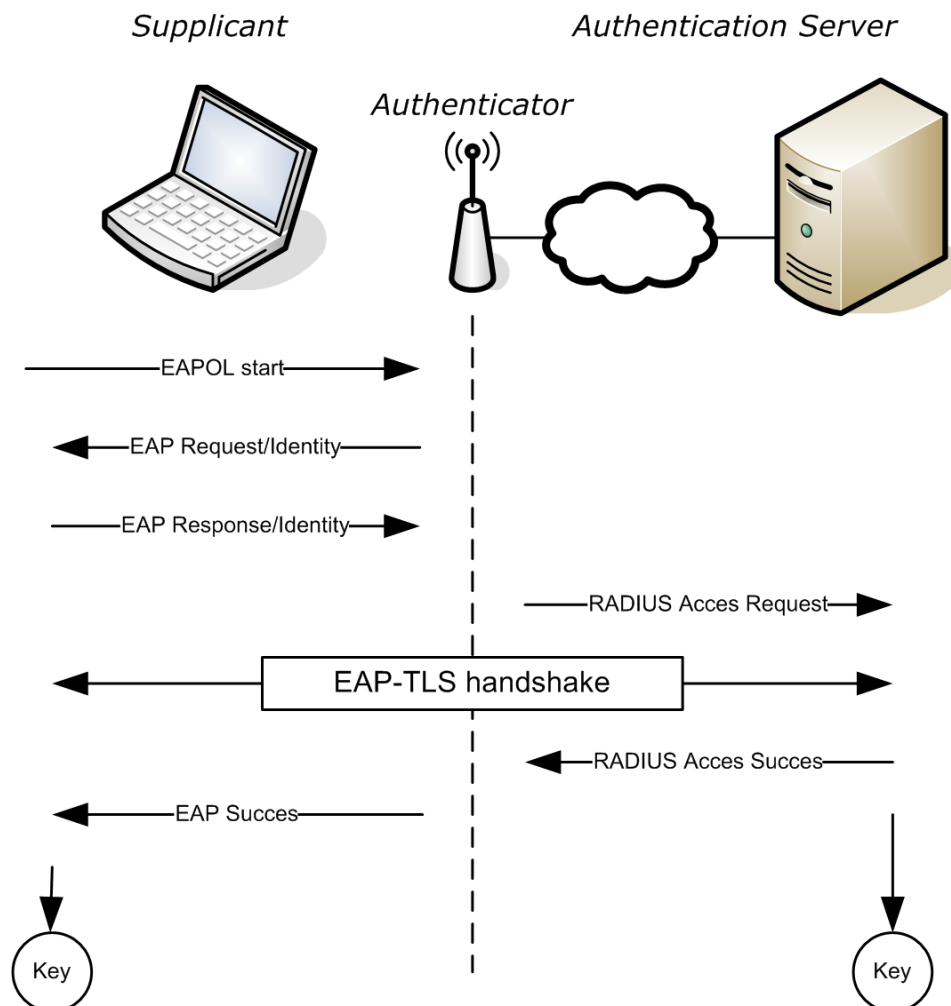
EAP-viestit kulkevat siirtoyhteyskerroksella eli OSI-mallin 2. kerroksella, kuten PPP tai IEEE 802, eikä se vaadi IP-tietoja käyttöönsä. EAP:ia käytetään autentikointimenetelmän valitsemiseen, tyypillisesti sen jälkeen kun autentikaattori pyytää lisätietoja päättääkseen, mitä tiettyä autentikointimenetelmää autentikoinnissa käytetään. EAP-protokolla ei itsessään ole autentikointimenetelmä, mutta se tarjoaa kuljetuspohjan valitsemalle autentikointimenetelmälle. (Aboba 2004.)

EAP-protokollan vahvuutena on sen arkkitehtuurin mahdollistava laajennettavuus ja se on laajalti käytössä verkkoympäristöissä. Esimerkiksi IEEE 802.11 WPA- ja WPA2-standardit ovat hyväksyneet IEEE 802.1x -autentikoinnin yli sadan virallisen EAP-autentikointimenetelmän kanssa. Tunnettuja EAP-

autentikointimenetelmiä ovat muun muassa. EAP-TLS, EAP-TTLS, EAP-MD5 ja LEAP. (Wikipedia 2015a.)

EAP-TLS käyttää TLS-kättelyä autentikoimiseen, ja asiakaskoneiden autentikointi tapahtuu digitaalisten sertifikaattien vaihdolla, kuvattu kuviossa 7.

Verkkoympäristössä sertifikaatteja käytetään tuottamaan autentikointi molempiin suuntiin palvelimen ja asiakaskoneen välillä. Palvelin esittää sertifikaattinsa asiakaskoneelle, ja kun sertifikaatti on vahvistettu esittää asiakaskone palvelimelle sertifikaattinsa. Normaalisti sertifikaatti on suojattu asiakaskoneella salasanalla, PIN-koodin tai älykortin taakse salauksesta riippuen. EAP-TLS:n heikkouksena on, että tunnistevaihdon aikana tieto ei kulje salattuna ennen varmenteen vaihtoa. (Hassell 2002, 108)



KUVIO 7. EAP-TLS-kättely (802.1x 2014)

#### 4.4.1 EAP-autentikointiprosessi

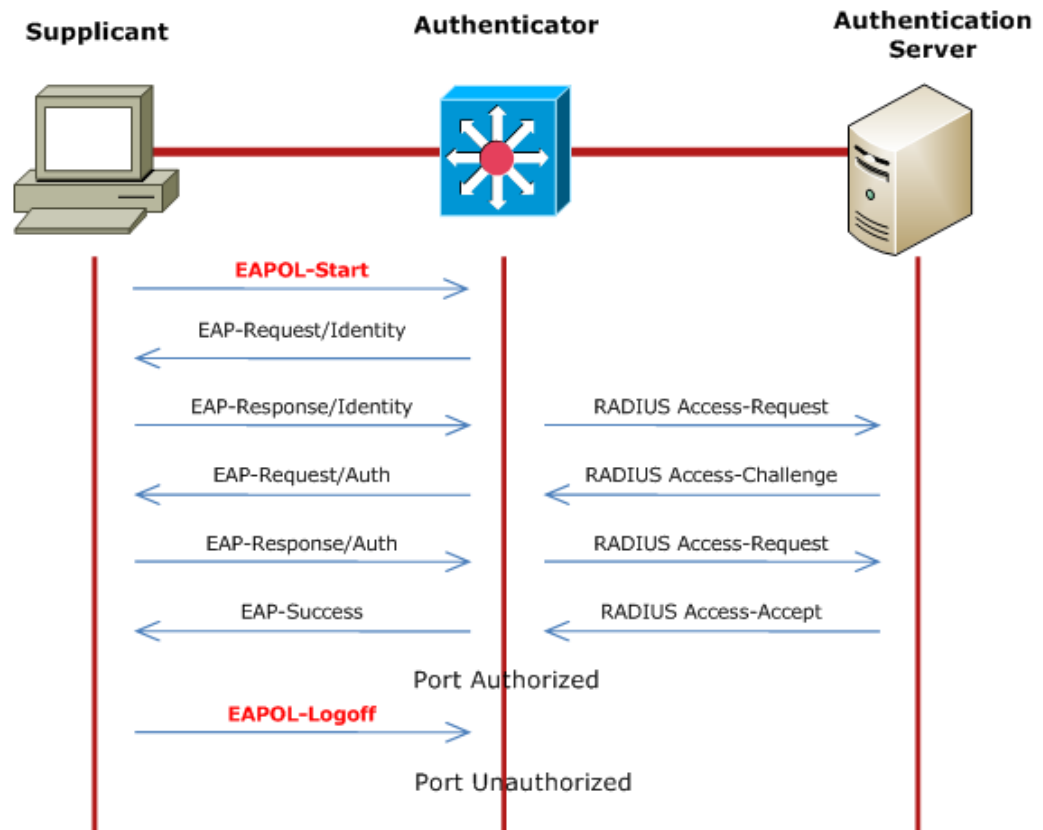
EAP-prosessi sisältää seuraavat vaiheet: alustus, aloitus, neuvottelu ja autentikointi. Ennen varsinaista autentikoinnin aloitusta autentikaattorin portit ovat luvaton-tilassa, joten mikään liikenne ei pääse portista läpi ennen kuin autentikointi on tapahtunut. Vain 802.1x-verkkoliikenne on sallittu tässä vaiheessa ja kaikki muu liikenne kuten UDP ja TCP liikenne estetään. (802.1x 2014.)

Autentikointi alkaa, kun autentikaattori lähettää EAP-Request Identity-kehyksen OSI-malli kerroksen 2, eli siirtoyhteyskerroksen yli. Asiakas avaa kuunteluyhteyden, kun se vastaanottaa EAP-Request Identity-kehyksen ja vastaa EAP-Response Identity-kehyksellä autentikaattorille. Tämä kehys sisältää asiakkaan tunnistustiedot. Autentikaattori kapsuloi tämän tiedon RADIUS Access-Request-pakettiin ja edelleenlähettää sen autentikointipalvelimelle. Tässä vaiheessa asiakas voi aloittaa alusta autentikointiprosessin tai käynnistää uuden istunnon lähettämällä EAPOL-Start-kehyksen autentikaattorille. Jos tämä tapahtuu, autentikaattori lähettää EAP-Request Identity-kehyksen uudelleen. Autentikointiprosessi näkyy kuviosta 8. (802.1x 2014.)

Neuvotteluvaihetta kutsutaan myös nimellä EAP-neuvotteluksi. Tässä vaiheessa autentikointipalvelin lähettää kapseloidun uudelleenlähetyksen autentikaattorille. Tämä uudelleenlähetyks sisältää EAP Requestin, joka täsmentää käytetyn EAP-menetelmän. Autentikaattori kapsuloi EAP-pyyynnön EAPOL-kehykseen ja toimittaa sen asiakkaalle. Tässä vaiheessa asiakas voi käyttää EAP-menetelmää, jota autentikointipalvelin pyysi, tai vaihtaa Negative Acknowledgement (NAK)-menetelmään ja vastata EAP-menetelmällä, jonka tunnistus haluaa suorittaa. (802.1x 2014.)

Autentikointi tapahtuu, kun asiakas ja autentikointipalvelin pääsevät yhteisymmärrykseen EAP-menetelmästä. EAP-vastaukset asiakkaan sekä autentikointipalvelimen välillä kulkevat autentikaattorin kautta. Tätä jatkuu, kunnes autentikointipalvelin vastaa EAP Success-kehyksellä, joka sisältää RADIUS Access-Accept-paketin tai EAP Failure-kehyksellä, joka sisältää RADIUS Access Reject-paketin. Jos autentikointiprosessi menee onnistuneesti läpi, asettaa autentikaattori fyysisen tai loogisen portin lupa-tilaan ja sallii

normaalin verkkoliikenteen portin kautta. Jos autentikointiprosessi ei mene onnistuneesti läpi, jättää autentikaattori portin vielä luvaton-tilaan ja blokkaa liikenteen asiakkaalta eteenpäin. (802.1x 2014.)

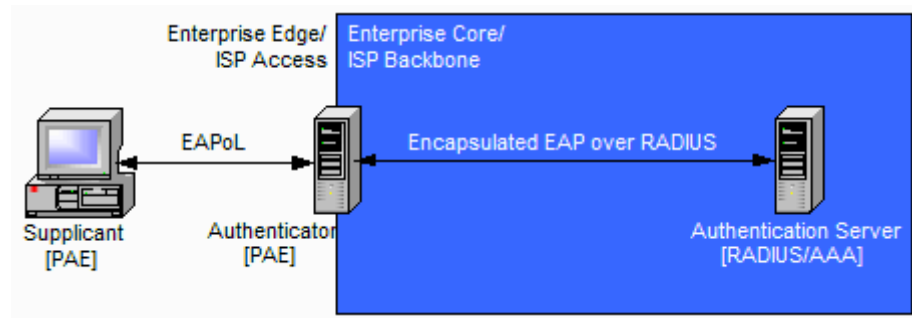


KUVIO 8. EAP autentikointiprosessi (802.1x 2014)

#### 4.4.2 EAPOL

EAPoL (*Extensible Authentication Protocol over LAN*) on paketoititekniikka, jota käytetään IEEE 802.1x-protokollan EAP-viestien kuljettamiseen.

Molemmissa EAPoL:ssa sekä EAP:ssa käytetään samaa kolmea pääkomponenttia autentikoimiskeskusteluun, jotka ovat asiakas, autentikaattori sekä autentikointipalvelin. Kuviossa 9 kuvataan kuinka lähiverkon laitteet ovat yhdistettyinä lähiverkkoympäristössä. (EAPoL 2015.)



KUVIO 9. EAPoL-arkkitehtuuri (EAPoL 2015)

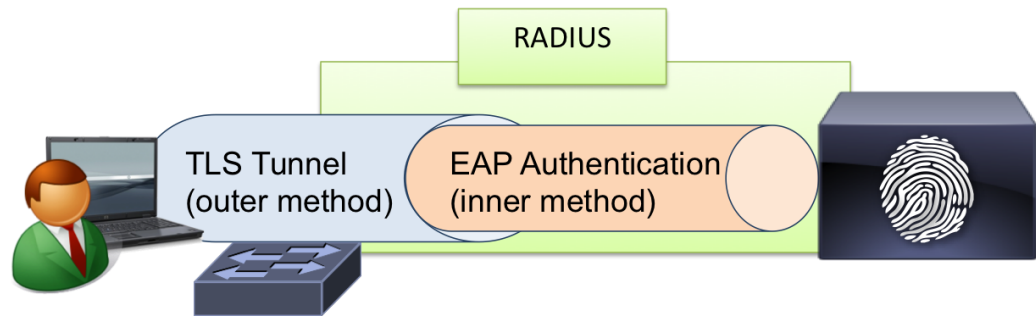
EAPoL-viestejä on viittä erilaista, ja kaikki kehykset eivät sisällä EAP-viestejä. Viestejä, joista EAP puuttuu, käytetään hallinnolliseen käyttöön, kuten autentikoinnin käynnistykseen tai sen lopettamiseen. Ensimmäinen EAPoL-Start-viesti sisältää yhteyden avauspyynnön. Ensimmäisen kerran, kun asiakas liittyy tietoverkkoon, se ei tiedä autentikaattorin MAC-osoitetta. Lähettämällä EAPoL-Start-viestin multicastina verkkoon asiakas saa vastauksena autentikaattorilta EAP-Request/identity-viestin. EAPoL-Key-viesti sisältää salatut avaintiedot, jotka autentikaattori lähettää asiakkaalle, kun sille on annettu pääsy verkkoon. EAPoL-Packet-kehys sisältää EAP-viestit. Yksinkertaisesti se on paketti, jossa EAP-viestit kulkevat lähiverkossa. EAPoL-Logoff-viesti tiedottaa autentikaattorille haluavansa poistua verkosta, minkä jälkeen autentikaattori blokkaa asiakkaan pois verkosta. EAPoL-Encapsulated-ASF-Alertia käytetään ASF-viestien (*Alert Standard Forum*) kuljettamiseksi portin läpi, mikäli asiakas on luvaton-tilassa autentikaattorille. (Understanding 802.1X 2015.)

#### 4.5 PEAP

PEAP eli Protected Extensible Authentication Protocol toimii samalla periaatteella kuin EAP-protokolla. PEAP käyttää EAP-TLS:n tavoin Transport Level Securityä (TLS) luodakseen salatun tunnelin PEAP:ia käyttävän asiakkaan ja PEAP-autentikaattorin, kuten Internet Authentication Service (IAS) tai Remote Authentication Dial-In User Service (RADIUS)-palvelimen välille. PEAP ei itsessään ole autentikointimenetelmä, mutta tarjoaa lisäturvaa muille EAP-protokollille. (PEAP 2015.)



PEAP tarjoaa hyötyinä suojaa EAP-neuvottelumetodille asiakkaan ja palvelimen välille kuljettamalla tiedon salatussa TLS-tunnelissa. Tämä estää mahdollisia verkkohyökkäyksiä vastaan ja hyökkääjä ei pääse saastuttamaan datapaketteja asiakkaan työaseman ja palvelimen välillä kuten EAP-protokollalla on mahdollista. Salatun TLS-tunnelin avulla myös estetään DoS (*Denial of Service*)-hyökkäyksiä vastaan. (PEAP 2015.)



KUVIO 10. TLS-tunnelissa kulkeva EAP-viesti (Woland 2013)

EAP-protokollaan erona on myös pakollinen molemminpuoleinen autentikointi. PEAP protokollaa käyttäessä siis myös palvelin autentikoi työaseman ja näin myös välissä -hyökkäyksiä (*man-in-the-middle attack*) voidaan ennaltaehkäistä. PEAP:n asiakkaan ja autentikaattorin luoma TLS:n master secrettiä ei jaeta tukiaseman tai kytkimen kanssa. Tämän takia välissä oleva tukiasema ei voi purkaa PEAP-salausta. (PEAP 2015.)

## 5 AUTENTIKOINTIPROTOKOLLAT

### 5.1 AAA

AAA-protokolla on menetelmä, jolla varmistetaan laitteen identiteetti, annetaan pääsy tai seurataan käyttäjän tekemisiä tietoverkossa. Lyhenne AAA tulee sanoista autentikointi (*Authentication*), valtuutus (*Authorization*) ja tilastointi (*Accounting*). (Cisco 2015.)

Autentikointi tunnistaa käyttäjän käyttäjätunnuksella tai salasanalla, haaste-vastaus-menetelmällä, kertakäyttöisellä avaimella tai digitaalisella sertifikaatilla. Tämä riippuu siitä, mikä suojausprotokollaa päätetään käyttää. (Cisco 2015.)

Valtuutuksella annetaan käyttäjälle mahdollisuus käyttää tietoverkossa tiettyjä palveluita tai estää käyttäjiä niitä käyttämästä. Käyttäjän käyttämät palvelut voidaan antaa tai kieltää niitä käyttämästä esimerkiksi kellonajan tai sijainnin perusteella. (Cisco 2015.)

Tilastointi tarjoaa menetelmän tiedon keräämiseen. Tietoa voidaan tallentaa lokeihin lokaalisti ja lähettää tieto AAA-palvelimelle laskutusta, tilintarkastusta tai raporttia varten. (Cisco 2015.)

### 5.2 RADIUS

RADIUS (*Remote Authentication Dial In User Service*) on tietoliikenne-protokolla, jonka tarkoituksena on tarjota tietourvaa, kuten käyttäjien tunnistusta ja hallintaa. RADIUS mahdollistaa AAA-mallin käyttäjän tunnistuksen, valtuutuksen sekä käyttäjätietojen tilastoinnin. (RADIUS Authentication, Authorization, and Accounting 2015.)

RADIUS-protokolla on alun perin Livingston Enterprisesin vuonna 1991 suunnittelema sisäänsoittopalveluiden tunnistusprotokolla, ja nykypäivänä sitä käytetään edelleen samaan käyttötarkoitukseen. IETF (*Internet Engineering Task Force*) toi RADIUS-protokollan yhdeksi vakio standardikseen jälkeenpäin. RADIUS-protokollan nykyinen määrittely tunnistuksen ja valtuutuksen kohdalla esitetään RFC 2868-dokumentissa ja uusien tilastoinnin määrittely esitetään RFC

2867-dokumentissa. Nykyisin RADIUS-protokollaa käytetään lähinnä yrityksen sisäisessä verkossa, jolloin tietoverkkoa voidaan pitää luotettavana sekä yhden toimijan ylläpitämänä. (Wikipedia 2015c.)

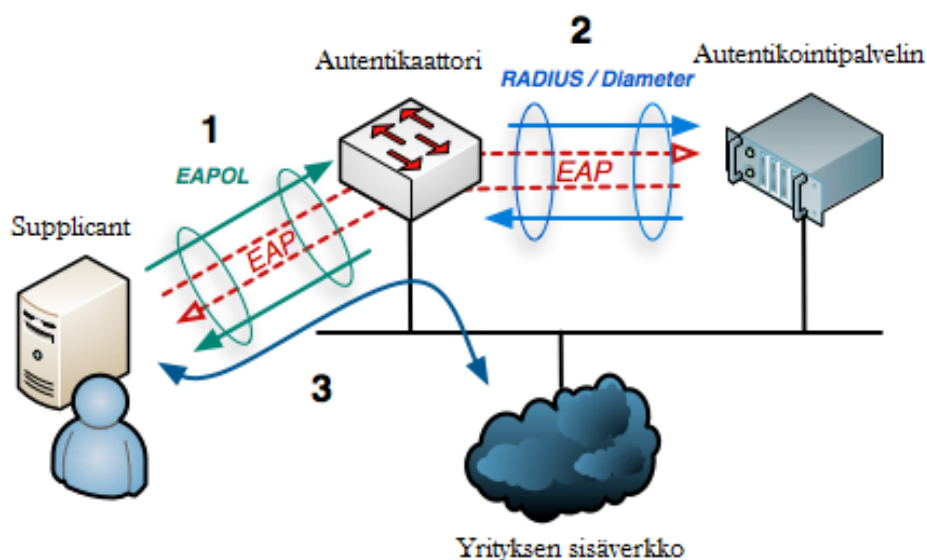
AAA-palveluiden käyttö vaatii, että lähiverkolla on oltava RADIUS-palvelin, johon WLAN-tukiasemat tai ethernet-kytkimet ottavat RADIUS-protokollalla yhteyttä. Kytkimen tai WLAN-tukiaseman sekä RADIUS-palvelimen välille on konfiguroitava oma yhteinen salasana, jolla ne tunnistavat toisensa tietoverkossa ja pitävät toisiaan luotettavina laitteina. RADIUS-palvelin itsessään voi sisältää tietokannan käyttäjänimille ja salasanoille, mutta se osaa myös käyttää olemassa olevia tietokantoja hyväkseen, kuten Windows 2000 Active Directorya. (Wikipedia 2015c.)

## 6 AUTENTIKOINTIMENETELMÄT

### 6.1 IEEE 802.1x

IEEE 802.1x:n (*Institute of Electrical and Electronics Engineers*) määrittelemä standardi perustuu porttikohtaiseen autentikointiin, jota käytetään ethernet- ja wlan-verkoissa. IEEE 802.1x porttikohtaista autentikointia käytetään estämään luvattomilta laitteilta ja käyttäjiltä pääsy verkkoon ja näin parantaa yrityksen tietoturvaa. 802.1x-standardi käyttää kolmea komponenttia todentamiseen. Komponentit ovat asiakas (*supplicant*), autentikointipalvelin (*authentication server*) sekä autentikaattori (*authenticator*). (802.1x 2014.)

Tietokonetta tai muuta asiakaslaitetta kutsutaan supplicantiksi eli anojaksi tai asiakkaaksi. Asiakas on autentikoiva päätelaite, joka haluaa pääsyn verkkoon langallisesti tai langattomasti. Asiakas voi myös tarkoittaa sovellusta, joka on päätelaitteella käytössä ja tarjoaa sen kautta tarvittavat käyttäjä- ja kirjautumistiedot autentikointipalvelimelle. Autentikointipalvelimena toimii yleensä RADIUS-palvelin, joka suorittaa asiakkaan autentikoinnin. Tunnistaja eli autentikaattori toimii näiden kahden välissä, ja se on yleensä joko reititin tai kytkin. Kuviossa 11 näkyy 802.1x-autentikoinnin arkkitehtuuri. (802.1x 2014.)



KUVIO 11. 802.1x-autentikointi (802.1x 2014)

Autenttikaattori pakottaa LAN-porttiin kytketyn laitteen tunnistautumaan ennen kuin se avaa laitteelle pääsyn eteenpäin. Kytkimen fyysiset portit eivät päästä liikennettä lävitsensä ennen kuin asiakas on autentikoitunut palvelimelle. (802.1x 2014.)

802.1x-autentikointi perustuu joko sertifikaattiin tai salasanasuojaukseen. Jos sertifikaattia käytetään todentamiseen, voidaan AD:n Group Policyllä jakaa sertifikaatit päätelaitteisiin. Sertifikaattien tuominen päätelaitteisiin voidaan hoitaa automaattisesti Group Policyn Auto-Enrollment-tavalla. Tämä tarkoittaa, että kun tietokone käynnistyy, Group Policy eli ryhmäkäytäntö, suoritetaan ja sertifikaatti asentuu automaattisesti tietokoneen lokaaliin sertifikaattimuistiin. (Loos 2012.)

Jos käytetään EAP-TLS-protokollaa, tarvitsee RADIUS-palvelin myös oman sertifikaattinsa. Tätä sertifikaattia käytetään todentamaan RADIUS-palvelimen identiteetti asiakaslaitteelle ja luomaan salattu tunneli näiden välille. Ensimmäisen yhteyden aikana muodostetaan RADIUS-palvelimen ja asiakaslaitteen välille tunneli, joka varmistaa, että kaikki liikenne näiden välillä on salattua. On suositeltavaa käyttää PEAP-protokollaa langallisen verkon autentikoinnissa sen tuoman lisäturvan takia. (Loos 2012.)

## 6.2 IEEE 802.1x:n vaatimukset

IEEE 802.1x autentikointia voidaan käyttää kahdella eri autentikointimenetelmällä. Riippumatta kumpaa autentikointimenetelmää käytetään, salasanaa vai sertifikaattia, vaatii IEEE 802.1x autentikointi vähintään seuraavat komponentit:

1. asiakas
2. autentikaattori
3. autentikointipalvelin.

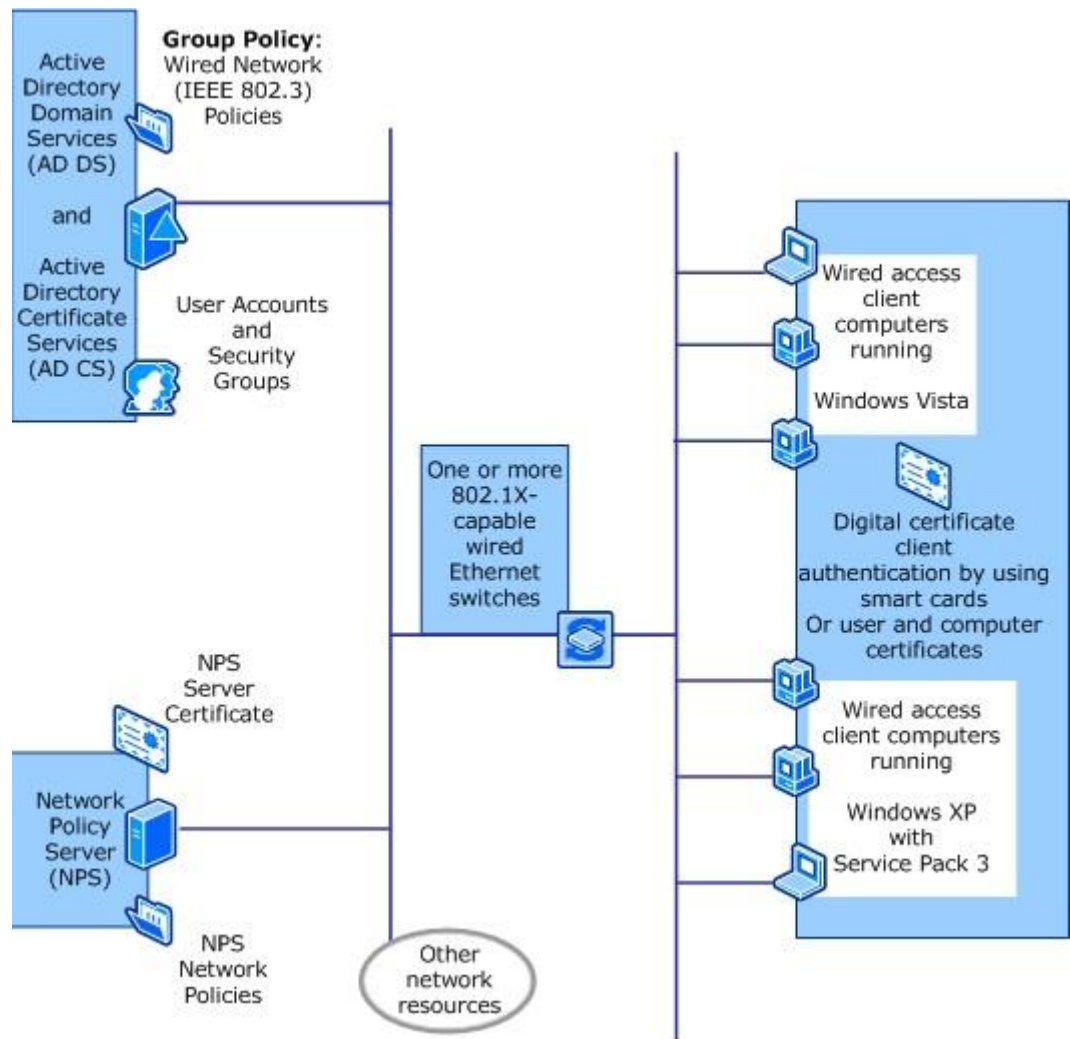
Lisäksi tarvitaan yksi tai useampi 802.1x yhteensopiva kytkin joka on yhteensopiva myös RADIUS-protokollan kanssa. Kytkimen täytyy tukea 802.1x-

standardia ja pystymään keskustelemaan RADIUS-palvelimen kanssa. Tuen voi tarkistaa kytkimen flash imagesta. (Loos 2012.)

Active Directoryn toimialuepalvelu tarvitaan käyttäjä- sekä ryhmähallintaan. AD:hen voidaan tehdä käyttäjille oikeutettuja ryhmiä, jos valittavaksi autentikointitavaksi tulee salasanakohtainen autentikointi. Jos valitaan taas sertifikaattisuojaus, voidaan asiakaskoneille myös tehdä omia ryhmiä, joihin sertifikaatit jaetaan automaattisesti. (Loos 2012.)

Active Directoryn sertifikaattipalvelu tarvitaan sertifikaattien hallinnalle. Sertifikaattipalveluita käytetään sertifikaattien luomiseen asiakaskoneille sekä RADIUS-palvelimelle. Suositus julkisen PKI (*Public Key Infrastructure*) -avaimen rakenteeseen on kaksipuolinen rakenne, juuri (*Root*) sekä alempi (*Subordinate*) varmenne. (Loos 2012.)

Lisäksi tarvitaan NPS (*Network Policy Server*)-palvelin, joka tuottaa itse autentikoinnin, valtuutuksen ja tilastoinnin. NPS-palvelin toimii RADIUS palvelimen roolissa, ja sitä käytetään käyttäjien ja koneiden todennukseen riippuen kumpaa autentikointimenetelmää käytetään, käyttäjäkohtaista tai konekohtaista. RADIUS-palvelin on yhteydessä AD:n Domain Controlleriin, josta se saa tiedon käyttäjä- tai asiakaskoneiden valtuudesta. Kuviossa 12 on kuvattuna 802.1x-ympäristö. (Loos 2012.)



KUVIO 12. 802.1x-autentikoinnin ympäristö (Loos 2012)

### 6.3 MAC-autentikointi

Media Access Control (MAC) -autentikointia käytetään autentikoimaan päätelaitteet niiden fyysisen MAC-osoitteen perusteella. MAC-autentikointi vaatii, että päätelaitteen fyysisen MAC-osoitteen on oltava täysin sama kuin manuaalisesti määritellyssä luettelossa. Tämä autentikointimuoto on hankala toteuttaa, jos laitteita on useita kymmeniä, koska MAC-osoitteiston luonti on työlästä. Lisäksi MAC-osoitteen muutos, vastaamaan hyväksyttyä MAC-osoitetta, on helppo väärentää. Tämän takia pelkkää MAC-autentikointia ei ole järkevää käyttää yksittäisenä autentikointinamenetelmänä, jos halutaan tietoturvallista ratkaisua. (MAC Authentication 2015.)

MAC-autentikointia voidaan käyttää myös jonkin toisen autentikointimenetelmän ohella, kuten 802.1x:n tai WEP:n rinnalla. 802.1x-autentikoinnin rinnalla MAC-autentikointia voidaan käyttää kolmella eri tapaa.

Ensimmäisellä tavalla MAC-autentikointi suoritetaan ennen 802.1x-autentikointia. MAC-autentikointi jakaa kaikki samat autentikointipalvelimen konfiguroinnit kuin 802.1x. Jos langallinen tai langaton asiakas yhdistää verkkoon, tehdään MAC-autentikointi ensin. Jos MAC-autentikointi epäonnistuu, ei 802.1x-autentikointi toteudu myöskään. Jos MAC-autentikointi onnistuu, siirrytään 802.1x-autentikointiin. Jos 802.1x-autentikointi onnistuu, asiakas saa yhteyden verkkoon, ja jos taas 802.1x-autentikointi epäonnistuu, asiakas siirretään deny-all- tai mac-auth-only-rooliin. (MAC Authentication 2015.)

MAC authentication only-roolissa käytetään pelkkää MAC autentikointia. Järjestelmänvalvoja voi luoda mac-auth-only-roolin, jos 802.1x-autentikoinnissa on MAC-autentikointi sallittuna. Mac-auth-only-rooli assosioituu asiakkaalle silloin jos MAC-autentikointi onnistuu, mutta 802.1x-autentikointi epäonnistuu. Jos 802.1x-autentikointi onnistuu myös, se yliajautuu viimeisen roolin toimesta. Mac-auth-only-roolia käytetään pääsääntöisesti vain langallisilla asiakkailla. (MAC Authentication 2015.)

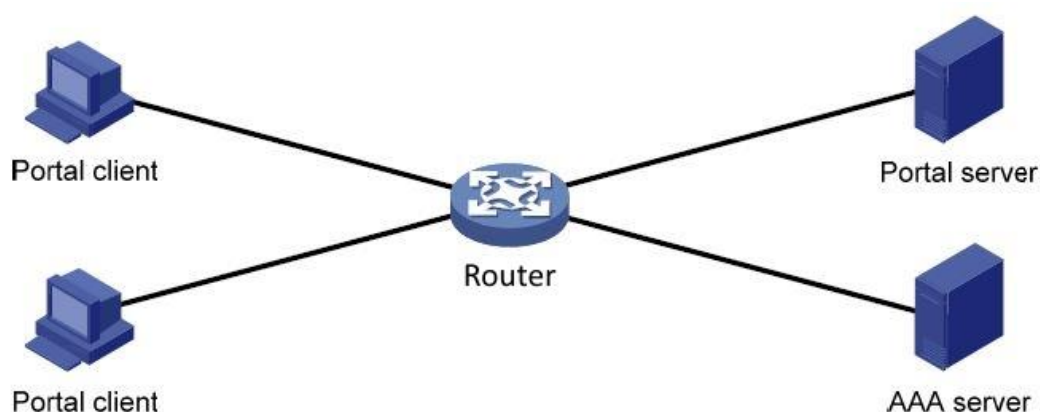
#### 6.4 Portaali-autentikointi

Portaali-autentikointi auttaa hallitsemaan käyttäjien pääsyä Internetiin tunnistautumisportaalien avulla. Portaali autentikointia kutsutaan web-autentikoinniksi ja verkkosivua, joka tarjoaa portaali autentikoinnin, kutsutaan portaali verkkosivuksi. Portaali-autentikoinnissa käyttäjien päätelaitteet pakottavat käyttäjät kirjautumaan portaali verkkosivulla. Ennen kirjautumista käyttäjät voivat käyttää palveluita, joita portaali verkkosivu tarjoaa, mutta pääsy Internetiin avautuu vasta kirjautumisen jälkeen. (Portal Authentication Technology White Paper 2008.)

Hyvänä puolena portaali-autentikoinnissa on joustavuus ja helppous. Portaali-autentikointi ei tarvitse taakseen asiakasohjelmaa vaan autentikoi käyttäjän suoraan verkkosivun kautta. Autentikointi voidaan määrittää tietyille koneille



VLAN:n, portin ja IP-osoiteavaruuden perusteella. Portaali-autentikoinnilla voidaan toteuttaa käyttäjän autentikointi verkon yli ja sallia pääsy yrityksen verkkoon myös ulkopuolelta talon omaa sisäverkkoa. Tyypillinen portaalijärjestelmä muodostuu neljästä eri peruskomponentista, jotka ovat asiakaspääte, portaali-palvelin, reititin sekä AAA-palvelin. Kuviossa 13 on esitetty tyypillinen portaalijärjestelmä. (Portal Authentication Technology White Paper 2008.)



KUVIO 13. Tyypillinen portaalijärjestelmä (Portal Authentication Technology White Paper 2008)

Autentikointi käynnistyy, kun tunnistamaton käyttäjä avaa selaimen ja kirjoittaa jonkin verkkosivun osoitteen osoitekenttään. Http pyyntö luodaan ja lähetetään reitittimelle, joka uudelleenohjaa http-pyyntöä käyttäjälle takaisin portaali-palvelimen autentikointisivulle. Autentikoinnin kotisivulle käyttäjä syöttää käyttäjänimen sekä salasanan, jotka portaali-palvelin lähettää reitittimelle. Käyttäjän syöttämät tiedot reititin välittää AAA-palvelimelle, joka onnistuneen autentikoinnin seurauksena hyväksyy pyynnön ja ilmoittaa tästä reitittimelle. Tämän jälkeen reititin sallii käyttäjän pääsyn Internetiin. (Portal Authentication Technology White Paper 2008.)

## 6.5 Autentikointimenetelmien vertailu

Opinnäytetyössä haetaan tietoturvallista ja käytännöllistä ratkaisua toteuttaa autentikointi pöytätyöasemille. Valinnaksi muodostui IEEE 802.1x porttikohtainen autentikointi. Verrattuna MAC-autentikointiin ja portaali-

autentikointiin, IEEE 802.1x-autentikointi on sekä tietoturvallisempi että käytännöllisempi tapa toteuttaa autentikointi.

MAC-autentikoinnin heikkoutena on helppo murrettavuus sekä ylläpitäminen. MAC-osoitteen vaihto on helppo tehdä, ja tarvittavan MAC-osoitteen saaminen ei vaadi suuria toimenpiteitä. Kaikki autentikoivat laitteet on myös käsin liitettävä kytkimelle sekä RADIUS-palvelimelle ja poistaa ne molemmista, kun laite poistuu verkosta.

Portaaliautentikoinnin murrettavuus on jo eri luokkaa kuin MAC-autentikoinnissa on, mutta tietoturvallinen ratkaisu tämä ei ole. Verkkoon pääsyyn vaaditaan käyttäjätunnus ja salasana, jotka voivat helposti päätyä väärin käsiin. Tällä tavalla verkkoon kuulumaton henkilö voi tiedot saatuaan liittyä verkkoon. Käytettävyys ei ole IEEE 802.1x-autentikointiin verrattuna samaa luokkaa. Jokaisen käynnistyksen yhteydessä käyttäjän on ensin avattava selaimensa ja kirjauduttava sisään verkkoon ennen kuin verkon palveluita voi käyttää. Taulukossa 1 on esitetty autentikointimenetelmien vertailu. Paras vaihtoehto saa 3 pistettä, toiseksi paras 2 pistettä ja huonoin 1 pisteen.

TAULUKKO 1. Autentikointimenetelmien vertailu

	802.1x autentikointi	MAC- autentikointi	Portaali autentikointi
Tietoturva	3p	1p	2p
Ympäristön asennus	3p	1p	2p
Ylläpito	3p	1p	2p
Poistuvien laitteiden hallinta	3p	1p	2p
Yhteensä	12p	4p	8p

Taulukosta näkee, että 802.1x-autentikointi oli paras autentikointiratkaisu kolmesta vertailluista menetelmästä. Portaali-autentikointi oli jokaisella osa-alueella toisena, ja MAC-autentikointi sijoittui kaikissa viimeiseksi.

## 7 PILOTTIYMPÄRISTÖ

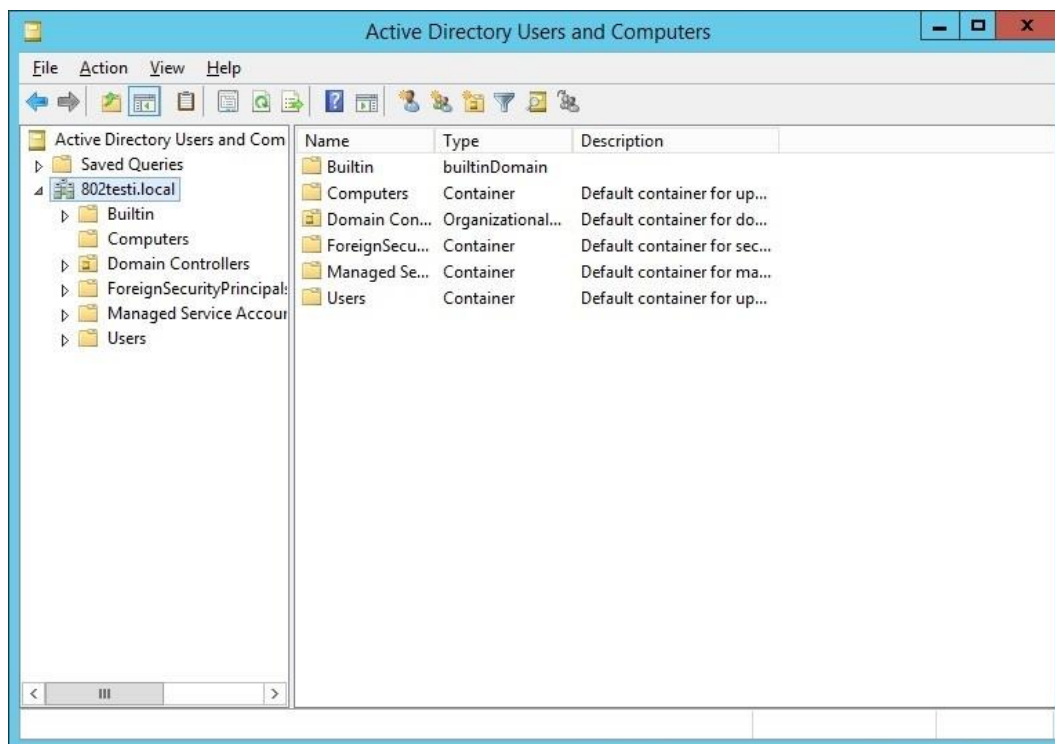
Pilottiympäristö pystytettiin PHSOTEY:n tietoliikenteen tiloihin, joissa käytössä oli kolme kytkinmallia sekä kolme virtuaalipalvelinta, joihin kullekin asennettiin oma roolinsa. Työn olisi voinut tehdä myös yhdellä virtuaalipalvelimella, mutta se ei olisi mallintanut PHSOTEY:n omaa tuotantoympäristöä. PHSOTEY:n tuotannossa käytetään rooleille eri palvelimia kuormantasauksen vuoksi.

Aktiivilaitteista kytkimiä oli käytössä kolmea eri mallia, joita tuotannossakin käytetään. Näin saatiin myös kytkimien toimivuus ympäristön kanssa pilotoitua. Työasemina käytettiin Windows 7 -käyttöjärjestelmällä olevia laitteita. Molempia PHSOTEY:n tuotannossa olevia, 64-bittistä sekä 32-bittistä Windows 7 -käyttöjärjestelmää.

### 7.1 Palvelimet

Testiympäristöön oli varattuna 3 kpl virtuaalipalvelimia, joissa jokaisessa pyöri Windows Server 2012 R2. Tarkoituksena oli ottaa yhdelle palvelimelle AD (*Active Directory*) käyttöön, jossa mallinnettiin PHSOTEY:n toimialuetta. Toiselle palvelimelle otettiin RADIUS käyttöön, jossa itse autentikointi hoidetaan, ja kolmannesta palvelimesta tehtiin sertifikaattipalvelin. Kaikki nämä toiminnot voitaisiin asentaa myös samalle palvelimelle, mutta testiympäristö mallintaa näin yhtymän tuotantoympäristöä paremmin pitämällä palvelimet ja roolitukset niissä erillään. Jatkossa toteutus on helpompi tuoda tuotantoon, kun pilotointi on tehty samankaltaisessa ympäristössä.

Ensimmäiselle virtuaalipalvelimelle asennettiin AD- ja DNS-roolit, ja tämä palvelin toimi yhtymän omaa toimialuetta vastaavana palvelimena. Palvelimelle lisättiin testauksessa käytettäviä käyttäjiä ja kaksi eri testikonetta, joilla testattiin pilotin toimivuutta. Oma toimialue nimettiin 802testi.local-nimellä.



KUVIO 14. 802.1x.local-toimialue

Toiselle virtuaalipalvelimelle asennettiin NPS-rooli. Virtuaalipalvelin toimi pilottiympäristössä RADIUS-palvelimena, jossa autentikointiin tarvittavat konfiguroinnit sijaitsevat ja josta voidaan lukea lokeja vikatilanteiden selvittämiseksi. Kolmas virtuaalipalvelin toimi sertifikaattipalvelimena, johon luotiin sertifikaatti, jotta työasemat pääsevät autentikoitumaan RADIUS-palvelimelle.

## 7.2 Kytkimet

Käytössä oli kolme kytkinmallia, jotka vastaavat PHSOTey:n tuotannossa käytettäviä kytkimiä. Jokaista kytkinmallia on testattava erikseen, sillä tuotantoon siirryttäessä tulee muuten ongelmia, jos jokin malli ei tue 802.1x-todennusta. Mahdollista on myös, että kytkimen konfiguroiminen vaatii sellaisia toimenpiteitä, jotka katkaisevat loppukäyttäjältä yhteyden ennen kuin autentikointi on suoritettu onnistuneesti. Kuvioissa 15, 16 ja 17 on esitettyä pilotissa käytetyt kytkimet.



KUVIO 15. Extreme Summit X450a-48t (Summit X450a 48t 2011)



KUVIO 16. HP Procurve 2650-48 (HP ProCurve 2650 2015)



KUVIO 17. HP Procurve 2610-24 (HP ProCurve 2610-24 2015)

## 8 AUTENTIKOINNIN TOTEUTUS

Käytännön toteutuksessa päädyttiin 802.1x-autentikointiin joka oli myös toimeksiantajan visio porttikohtaisessa autentikoinnista. 802.1x on tietoturvallinen ratkaisu, joka on myös suhteellisen helppo ottaa tuotantoon. Lisänä 802.1x:n käyttöönottoaminen on käyttäjälle näkymätön toimenpide eikä loppukäyttäjä välttämättä edes huomaa autentikoinnin olemassaoloa. Kaikista käytännön kuvista sekä liitteistä on poistettu tai sumennettu IP-osoitteet tietoturvalisistä syistä.

Työ alkoi palvelimien roolitusten asentamisesta. Kaikki kolme palvelinta olivat puhtaita asennuksia, eivätkä ne sisältäneet mitään toimintoja valmiiksi.

Palvelimien roolien asennuksessa oli aluksi ongelmia, koska aikaisempaa kokemusta palvelimien toiminnasta ja roolien lisäämisestä ei ollut kovinkaan paljoa. Palvelimien konfigurointia piti tutkia Internetistä sekä kysellen PHSOTEY:n järjestelmäasiantuntijoilta niiden toiminnasta ja vaadittavista asetuksista. Palvelinroolien asennuksiin ei tässä työssä perehdytä sen syvemmin vaan keskitytään itse autentikointijärjestelmän ympärille.

### 8.1 Sertifikaatin luominen

Ennen kuin 802.1x-autentikointia voidaan käyttää, tarvitsee päätelaitteille ja palvelimille luoda molemmille omat sertifikaatit. PEAP-EAP-TLS-protokollaa käytettäessä tarvitaan myös palvelimille myös oma sertifikaatti, sillä sen on todistettavasti oltava luotettava palvelin päätelaitteelle. Näille sertifikaateille on kuitenkin valmiina omat pohjat, joten niistä otetaan vain kopiot ja muokataan omaan tarpeeseen mukautuviksi.

Koska käytettiin konekohtaista autentikointia, tehdään sertifikaatit koneille ja palvelimille eikä käyttäjille. Konekohtainen autentikointi valittiin sen takia, koska silloin voidaan autentikointiprosessi pitää näkymättömänä käyttäjälle. Myös päätelaitteiden lisääminen AD:ssa oikeaan ryhmään on helpompi kuin käyttäjien, sillä käyttäjät saattavat työskennellä eri toimipaikoissa eri päivinä ja pöytäkoneet ovat vain omilla kiinteillä paikoillaan.

Avataan sertifikaatti palvelimelta Certificate Authority ja valitaan Certificate Templatesta Manage. Tämän jälkeen tehdään duplikaatti RAS and IAS Server

certificate Templatesta ja muokataan se haluttuun muotoon. Muutetaan nimi kuvaavaksi ja valitaan *Validity Period* eli se, kuinka kauan sertifikaatti on voimassa, tämä on kuvattu kuviossa 18. Yleensä voimassaoloaika rajataan yhteen vuoteen, mutta pilottiympäristössä tällä valinnalla ei ollut merkitystä.

802.1x sertifikaatti koneille Properties

Subject Name Issuance Requirements

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Template display name:  
802.1x sertifikaatti koneille

Template name:  
802.1xsertifikaattikoneille

Validity period: 5 years Renewal period: 6 weeks

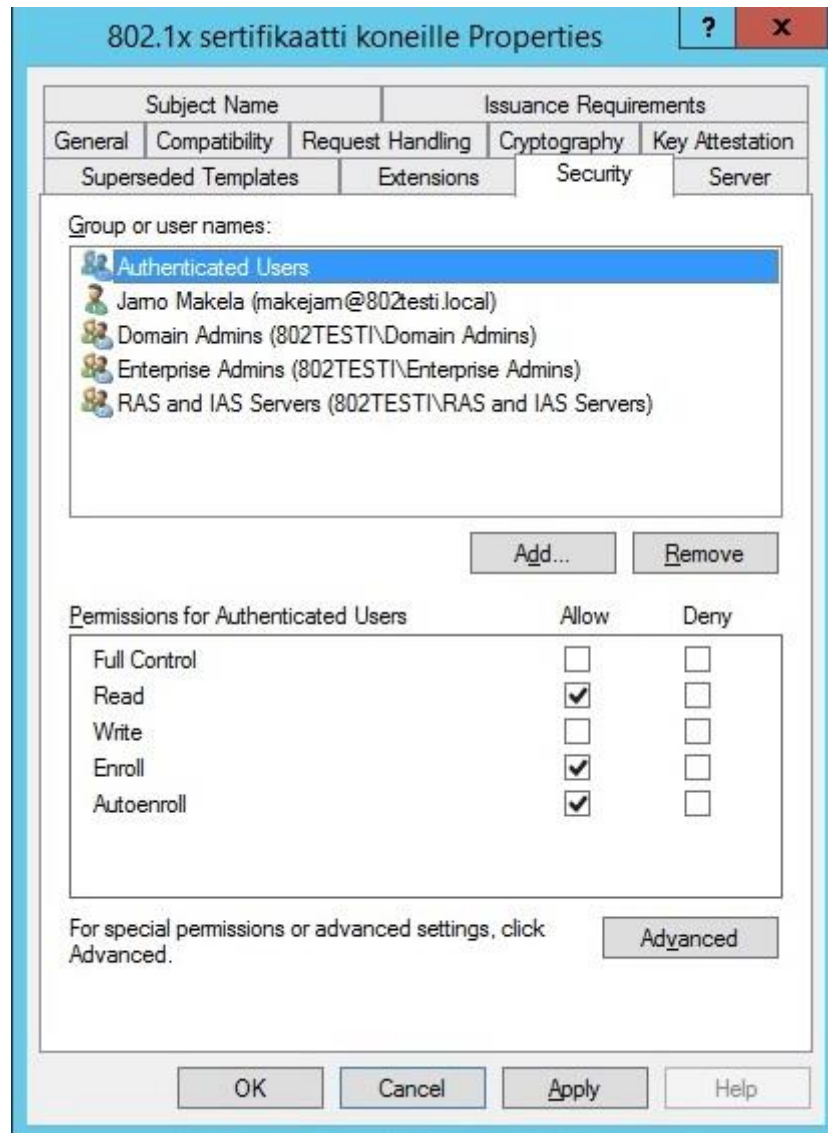
☒ Publish certificate in Active Directory:  
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

KUVIO 18. Sertifikaatin ominaisuudet

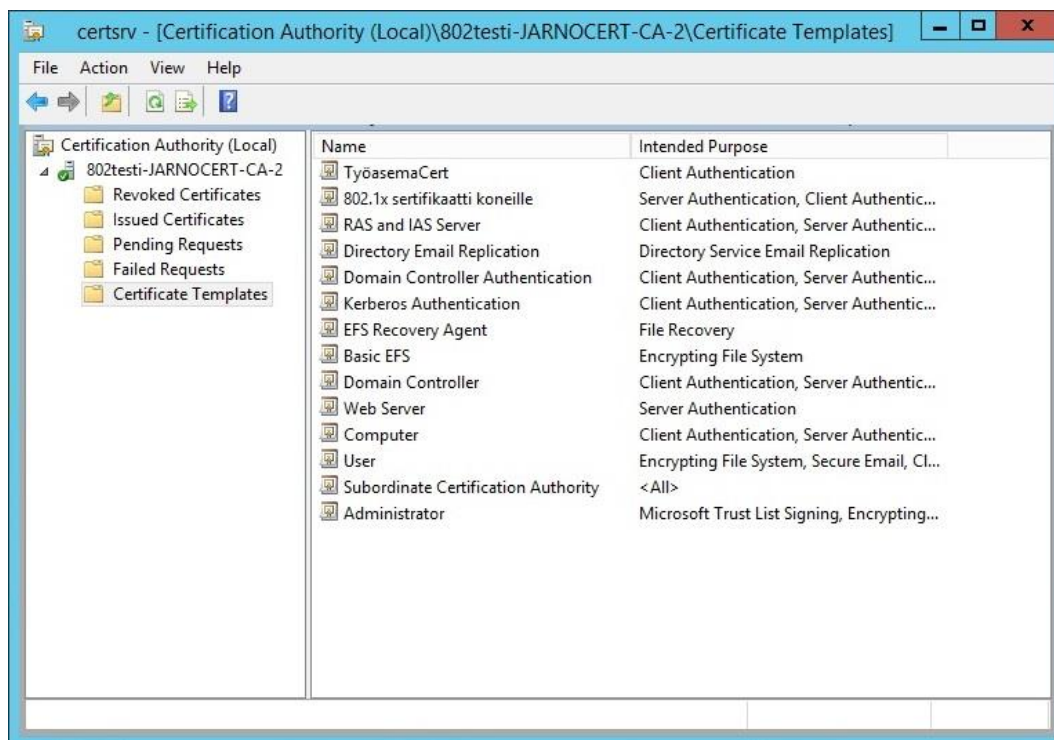
Katsotaan vielä *Securityn* alta, että *enroll* ja *autoenroll* on varmasti päällä, jottei testauksessa tule ongelmia sertifikaatin automaattisen tuomisen kanssa. Tämä vaihe näkyy kuviossa 19.





KUVIO 19. Sertifikaatin ominaisuudet

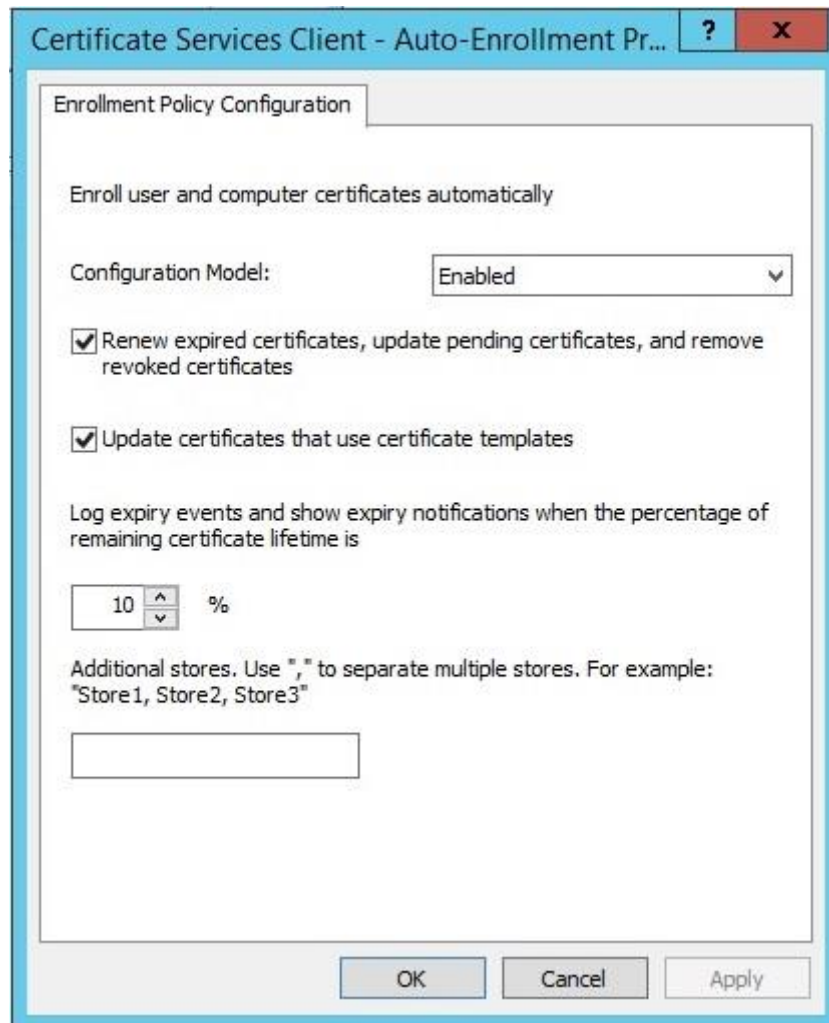
Kuviossa 20 on kuvattu, kuinka tuodaan luodut sertifikaatit käyttöön valitsemalla *Certificate Authority* ja sieltä taas *Certificate Templates* ja valitaan *New – Certificate Template to Issue*. Valitaan luotu *802.1x-sertifikaatti* koneille.



KUVIO 20. 802.1x-sertifikaatti koneille

Jotta sertifikaatin jakelussa ei tule ongelmia, voidaan se automaattisesti tuoda tiettyyn ryhmään kuuluvalla koneelle. Otetaan yhteys AD-palvelimeen ja avataan *Administrative Toolseista - Group Policy Management*. Valitaan ryhmä, johon autentikoivat koneet kuuluvat, ja tehdään uusi *Group Policy Object*, joka nimetään mahdollisimman kuvaavaksi. Käytetään *802\_Client\_Asetukset*-nimeä, joka on jatkossakin kuvaava nimi päätelaitteiden asetuksille. Valitaan luotu objekti ja muokataan *Computer Configuration – Policies – Windows Settings – Security Settings – Public Key Policies* ja *Auto-Enrollment properties*, nämä muutokset näkyvät kuviossa 21. Otetaan sääntö *Enablella* käyttöön.

Ongelmatilanteiden välttämiseksi valitaan vielä *System Services*-kohdasta *Wired AutoConfig Properties*-kohdasta sääntö automaattiseksi; näin käyttäjä ei itse voi mennä vaihtamaan asetuksia.



KUVIO 21. Auto-Enrollmentin käyttöönotto

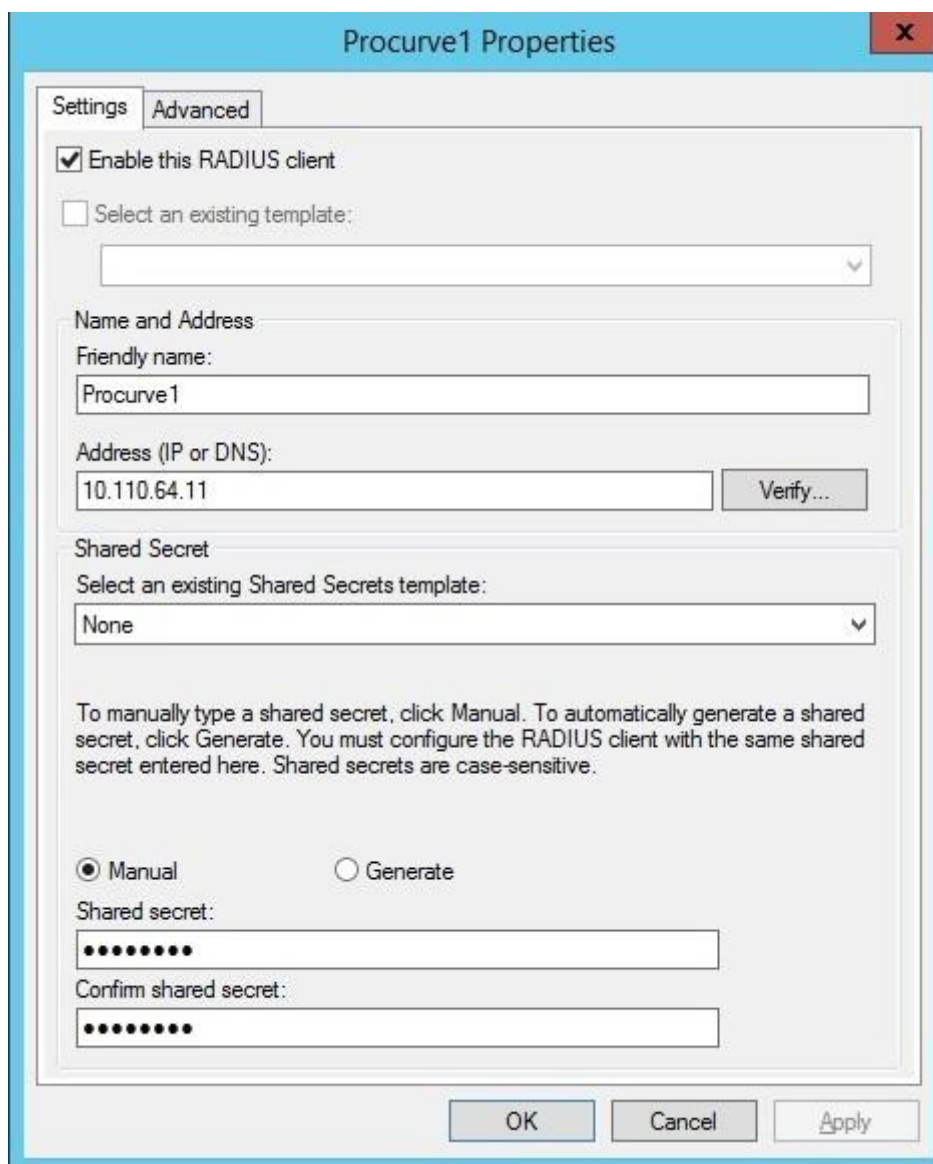
Luotu sääntö otetaan käyttöön luodulle *802testi*-ryhmälle, johon testikoneet liitettiin. Näin ryhmäkäytäntö tulee automaattisesti voimaan niille koneille, jotka ryhmään kuuluvat, ja luotu sertifikaatti latautuu koneelle automaattisesti ja autentikointi onnistuu.

## 8.2 RADIUS

RADIUS-palvelin on suoraan kytkimiin yhteydessä, joten jokainen kytkin on lisättävä palvelimelle käsin. Jos kytkintä ei lisätä palvelimelle, ei autentikointia kyseisellä kytkimellä voida suorittaa.

Aloitetaan RADIUS-palvelimen konfiguroiminen ottamalla yhteys RADIUS-palvelimeen. Valitaan palvelimelta *Administrative Tools* ja sen alta *Network*

*Policy Server*. Otetaan *RADIUS Clients* ja lisätään *New RADIUS Client*illä uusi kytkin listaan. Annetaan kytkimen nimi ja sen IP-osoite ja lisätään kytkimien ja palvelimen välille salainen avain, joka täytyy molemmilla olla täysin sama, jotta yhteys muodostuu niiden välille. Tietoturvallisesti tämän avaimen tulisi erittäin pitkä ja monimutkainen isojen ja pienten kirjainten sekä numeroiden sarja, mutta testauksessa käytettiin varsin lyhyttä ja helppoa salasanaa, jotta voidaan minimoida mahdollisten virheiden syntyminen. Tehdyt asetukset näkyvät kuviosta 22.



Procurve1 Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:  
Procurve1

Address (IP or DNS):  
10.110.64.11 Verify...

Shared Secret

Select an existing Shared Secrets template:  
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:  
.....

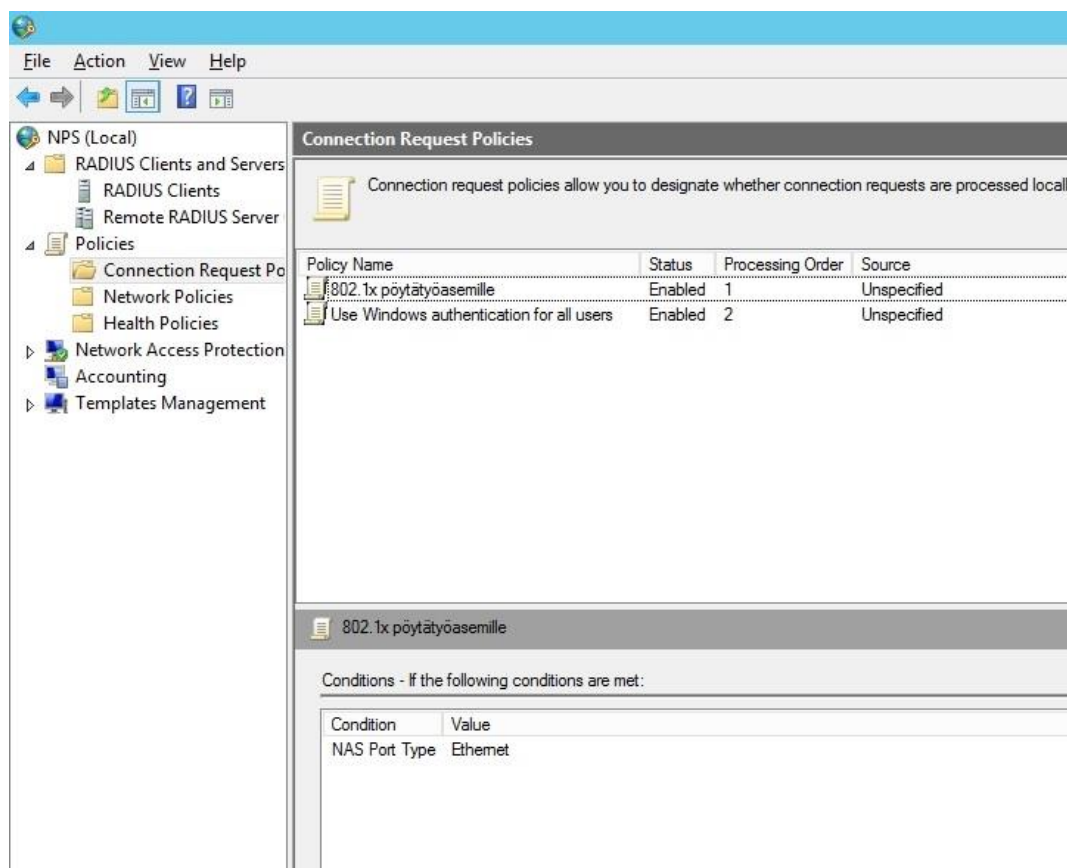
Confirm shared secret:  
.....

OK Cancel Apply

KUVIO 22. Kytkimen lisääminen palvelimelle

Seuraavaksi täytyy tehdä säännöt eli policyt palvelimelle. Tässä vaiheessa määritetään, mitä autentikointimenetelmää halutaan käyttää, ja työssä valintana oli

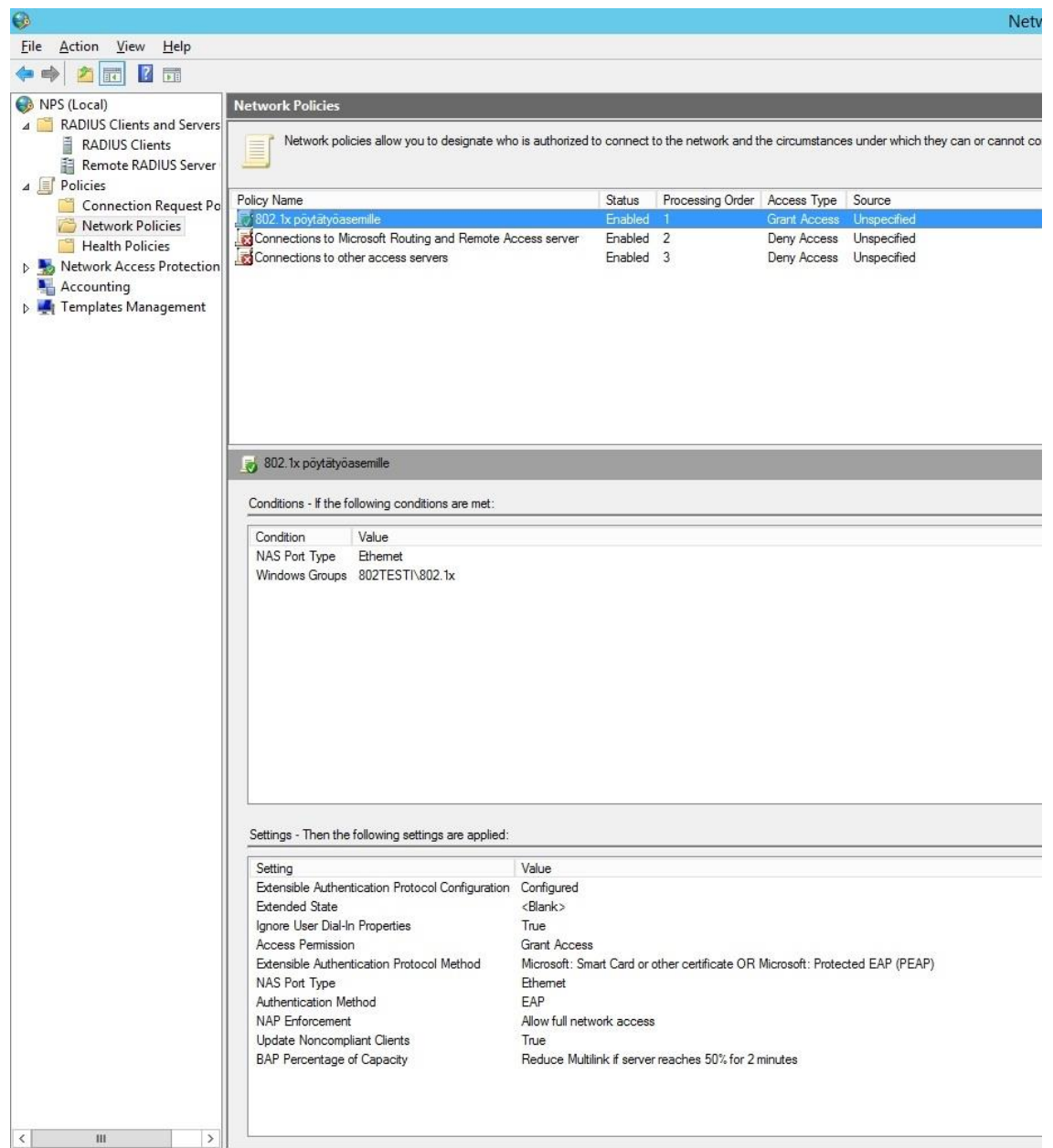
PEAP sen tuoman tietoturvan takia. Aluksi avataan *Network Policy Server*-konsoli jossa luodaan uusi sääntö *Connection Request Policies*-kohdassa. Annetaan policylle kuvaava nimi, kuten *802.1x pöytätyöasemille*, ja valitaan edellytykseksi IPv4 osoitteisto. Valitaan vielä *Settings*-välilehdeltä *Authenticate requests on this server*, sillä käytetään tätä palvelinta autentikointiin. Muita asetuksia ei tällä hetkellä tarvitse tehdä, joten suljetaan ohjattu asennustoiminto klikkaamalla OK. Alla oleva kuvio 23 havainnollistaa tehtyjä asetuksia.



KUVIO 23. Connection Request Policy

Luodaan palvelimella vielä säännöt verkkoliikenteelle ja tehdään *Network Policies*-kohtaan uusi sääntö. Annetaan säännölle kuvaava nimi, kuten *802.1x pöytätyöasemille*, ja tehdään sääntöön vaadittavat muutokset. *Conditions*-välilehdeltä lisätään *NAS Port Typeksi Ethernet*, sillä halutaan käyttää langallista yhteyttä pelkästään pilottiympäristössä. Tässä voidaan määrittää käytettäväksi myös langatonta 802.11-standardia, jos sitä tarvittaisiin. Tässä kohtaa täytyy vielä lisätä toimialueelle luotu ryhmä 802.1x, jotta sääntö astuu voimaan kaikille ryhmässä oleville koneille.

*Constraints*-välilehdeltä valitaan nyt haluttu autentikointimenetelmä. Otetaan ruksit pois kaikista kohdista, sillä ei haluta ottaa käyttöön heikompia autentikointimenetelmiä, ja lisätään *Add* painikkeella *Protected EAP* sekä *Smart Card or other certificate*. Edit-painikkeella valitaan vielä sertifikaatiksi työn alussa luomamme *802.1x sertifikaatti koneille*. Tämän jälkeen voidaan ohjattu asennustoiminto sulkea OK:lla. Tässä vaiheessa on tärkeää muistaa siirtää luotu sääntö ensimmäiseksi valikossa, tai muuten ensimmäinen sääntö Deny Access estää liikenteen kokonaan. Alla kuviossa 24 vielä havainnollistettu asetukset, jotka juuri tehtiin.



KUVIO 24. Network Policies-asetukset

### 8.3 Kytkimien konfiguroinnit

Työ jatkui kytkimien konfiguroinnista. Käytössä oli kahden eri valmistajan kytkmiä: Extremer Summit X450a-48t kytkin sekä HP:n Procurve 2610-24 sekä Procurve 2650-48. Kytkimissä oli jätetty vanhat konfiguraatiot, joten ne täytyi ensin resetoida ja ladata niihin uusimmat firmware-versiot.

HP:n kytkimissä konfiguroinnit olivat melkein täsmälleen samat, suurimmat erot olivat porttien määrissä näissä kahdessa mallissa. Extremen kohdallakaan mitään suurta eroa ei ole. Extremen konfiguroimisessa käytetään vain erityylistä kieltä, mutta perustoiminnot näissä kaikissa kytkimissä ovat samanlaiset. Kytkimien peruskonfiguroimisen, kuten kellonaikojen hakeminen palvelimelta, oletusyhdyskäytävän määrittäminen sekä haluttujen aliverkkojen ja protokollien pääsy kytkimeen, jälkeen luotiin ”testiws” VLAN kytkimelle tagilla 1100. VLAN luotiin, jotta siihen kuuluvat portit kuuluisivat autentikoinnin piiriin. Tagged-portti on varattu kytkimien väliselle yhteydelle ja *write memory*-komennolla tallennetaan asetukset kytkimen muistiin. Alla Kuviossa 25 konfiguraatio, siitä kuinka VLAN luodaan.

```
Pro1# conf t
Pro1 (config)# vlan 1100
Pro1 (vlan-1100)# untagged 1-25
Pro1 (vlan-1100)# tagged 26
Pro1 (vlan-1100)# exit
Pro1(config)# write mem
```

#### KUVIO 25. Kytkimen konfiguraatio

VLAN:n luonnin jälkeen täytyi määrittää itse autentikointimenetelmän käyttö sekä määrittää sitä käyttävät portit. Tämän jälkeen täytyy määrittää myös itse RADIUS-palvelimen osoite sekä kytkimen ja palvelimen välinen salattu avain, jotta kytkin osaisi kommunikoida palvelimen kanssa ja hakea sieltä tarvittavat autentikointitiedot. Komennot näkyvät Kuviossa 26.



```
Pro1(config)# radius-server host x.x.x.x key "802testi"
```

```
Pro1(config)# aaa authentication port-access eap-radius
```

```
Pro1(config)# aaa port-access authenticator 1-10
```

```
Pro1(config)# aaa port-access authenticator active
```

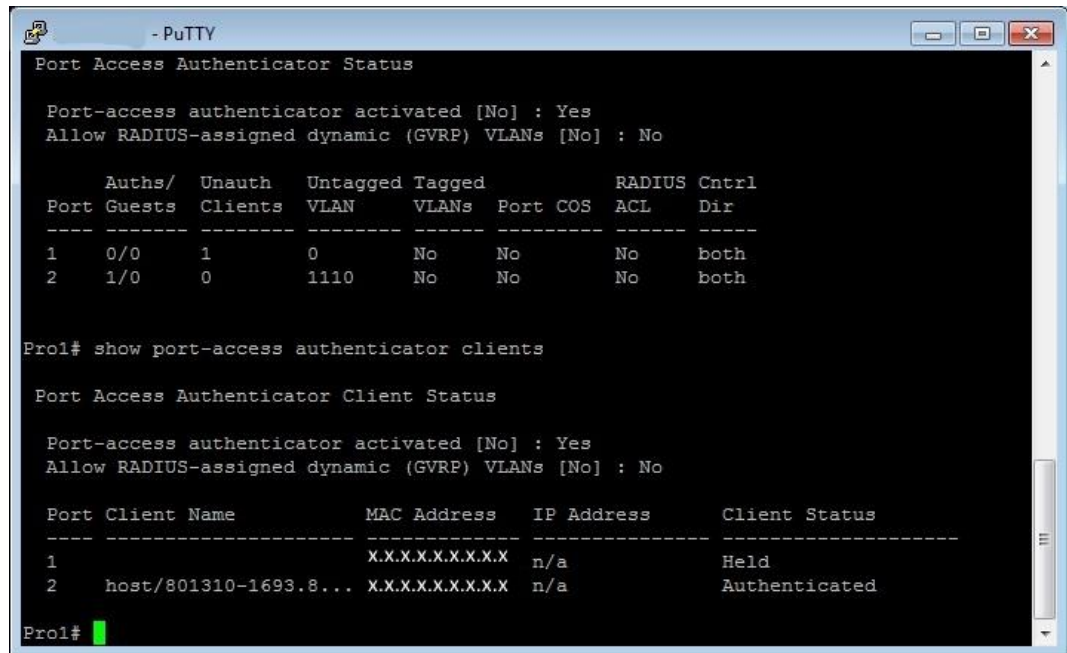
```
Pro1(config)# write mem
```

## KUVIO 26. RADIUS-palvelimen määrittäminen

Nyt kytkimelle oli luotu tarvittavat konfiguroinnit autentikoinnille. Käyttöön otettiin vain portit 1-10, jotta autentikoinnin toimivuutta voidaan testata vaihtamalla päätelaite autentikoivasta portista sellaiseen porttiin, jossa ei autentikointia ole käytössä, ja tästä voidaan tehdä tarvittavia muutoksia. Samat konfiguroinnit tehtiin kaikille kolmelle kytkimelle ja niiden konfiguraatiot löytyvät liitteistä.

### 8.4 Ympäristön testaus

Nyt kun palvelimet ja kytkimet on konfiguroitu, voidaan siirtyä ympäristön testausvaiheeseen. Toinen testikoneista 801310-1693 laitetaan toimialueella oikeaan ryhmään *802.Ix*, jonka kanssa autentikointi pitäisi toimia automaattisesti eikä käyttäjän pitäisi huomata päätelaitteen käytössä mitään eroa. Toinen testikone 801310-1901 jätetään ryhmästä pois, ja koneen ei pitäisi saada yhteyttä ollenkaan Internetiin. Otetaan samalla etäyhteys kytkimeen, josta myös voidaan tarkkailla tilannetta. Porttikohtaisen autentikoinnin tilaa voidaan tarkastella *show port-access authentication*-komennolla ja numeroilla voidaan määritellä halutut portit, joita halutaan tarkkailla. Kuviosta 27 nähdään, että toinen päätelaitteista on jo autentikointunut ja sillä pitäisi olla yhteys Internetiin ja toisella koneella on ongelmia autentikoinnin kanssa.



```

- PuTTY
Port Access Authenticator Status

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Port  Auths/  Unauth  Untagged Tagged  RADIUS Cntrl
-----
Port  Guests  Clients  VLAN    VLANs  Port COS  ACL    Dir
-----
1     0/0      1        0        No     No       No     both
2     1/0      0       1110     No     No       No     both

Pro1# show port-access authenticator clients

Port Access Authenticator Client Status

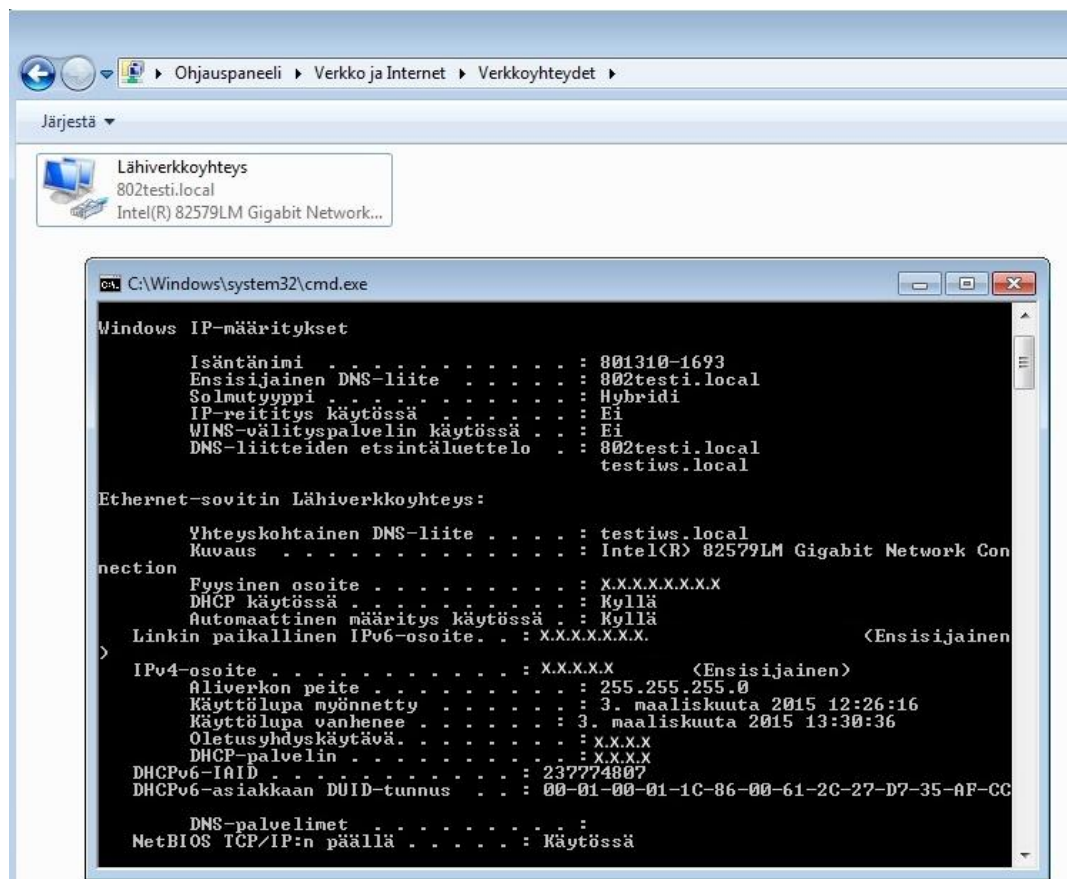
Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Port Client Name          MAC Address      IP Address      Client Status
-----
1     host/801310-1693.8... X.X.X.X.X.X.X.X n/a            Held
2     host/801310-1693.8... X.X.X.X.X.X.X.X n/a            Authenticated

Pro1#

```

KUVIO 27. Kytkimen porttien status



Ohjauspaneeli > Verkko ja Internet > Verkkoyhteydet >

Järjestä ▼

Lähiverkkoyhteys  
802testi.local  
Intel(R) 82579LM Gigabit Network...

```

C:\Windows\system32\cmd.exe
Windows IP-määritykset

Isäntänimi . . . . . : 801310-1693
Ensisijainen DNS-liite . . . . . : 802testi.local
Solmutyyppi . . . . . : Hybridi
IP-reititys käytössä . . . . . : Ei
WINS-välityspalvelin käytössä . . . . . : Ei
DNS-liitteiden etsintäluettelo . . . . . : 802testi.local
testiws.local

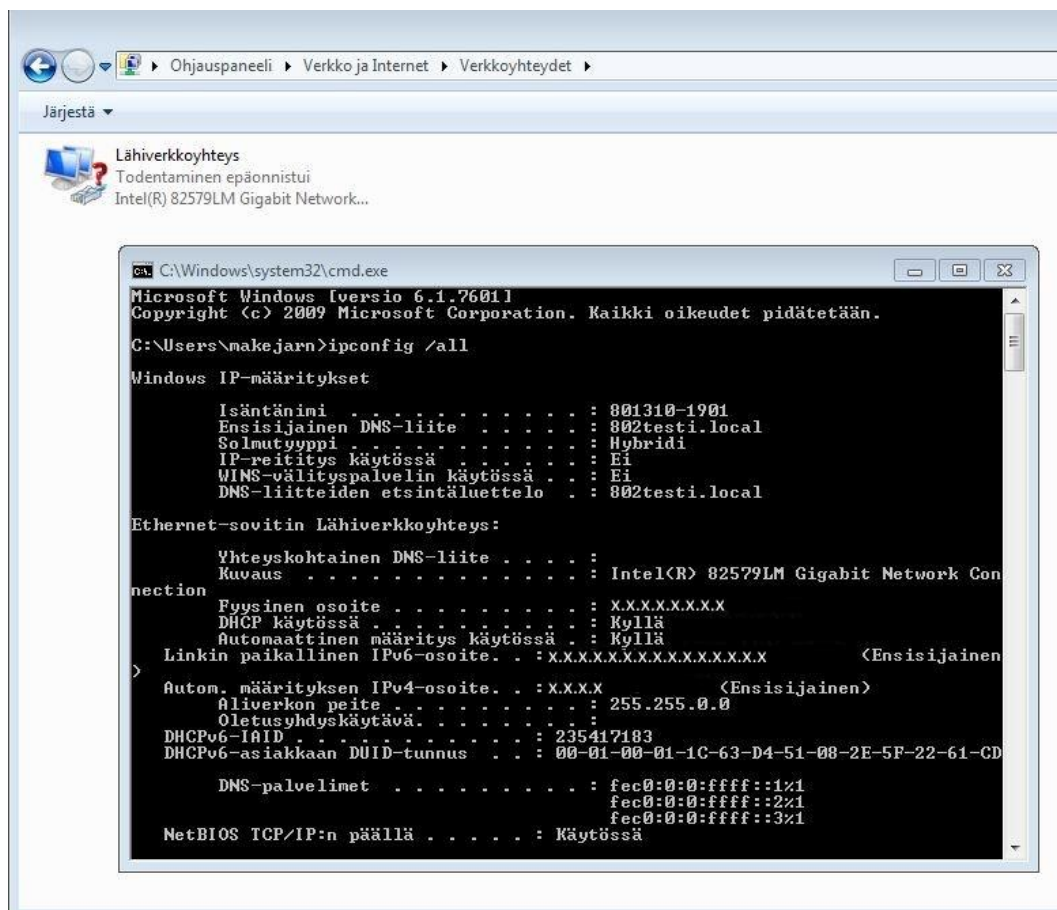
Ethernet-sovitin Lähiverkkoyhteys:

Yhteyskohtainen DNS-liite . . . . . : testiws.local
Kuvaus . . . . . : Intel(R) 82579LM Gigabit Network Con
nection
Fyysinen osoite . . . . . : X.X.X.X.X.X.X
DHCP käytössä . . . . . : Kyllä
Automaattinen määrittely käytössä . . . . . : Kyllä
Linkin paikallinen IPv6-osoite . . . . . : X.X.X.X.X.X.X <Ensisijainen>
IPv4-osoite . . . . . : X.X.X.X.X <Ensisijainen>
Aliverkon peite . . . . . : 255.255.255.0
Käyttöluupa myönnetty . . . . . : 3. maaliskuuta 2015 12:26:16
Käyttöluupa vanhenee . . . . . : 3. maaliskuuta 2015 13:30:36
Oletusyhdistyskäytävä . . . . . : X.X.X.X
DHCP-palvelin . . . . . : X.X.X.X
DHCPv6-IAID . . . . . : 237774807
DHCPv6-asiakkaan DUID-tunnus . . . . . : 00-01-00-01-1C-86-00-61-2C-27-D7-35-AF-CC

DNS-palvelimet . . . . . :
NetBIOS TCP/IP:n päällä . . . . . : Käytössä

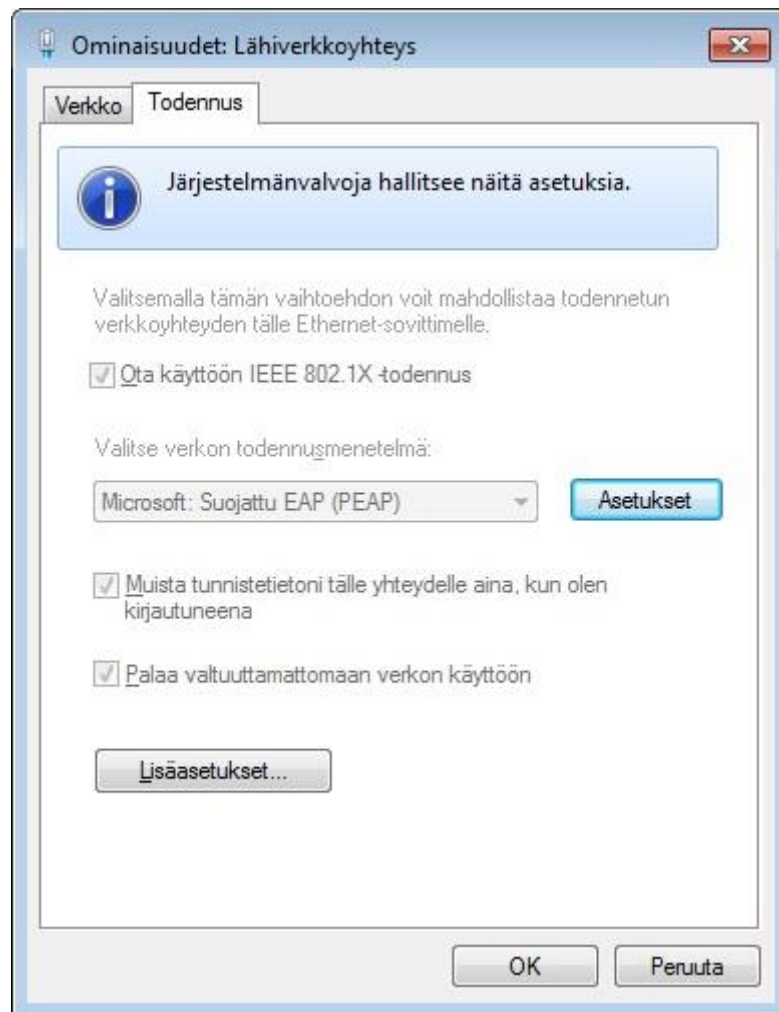
```

KUVIO 28. Työasemalla yhteys Internetiin

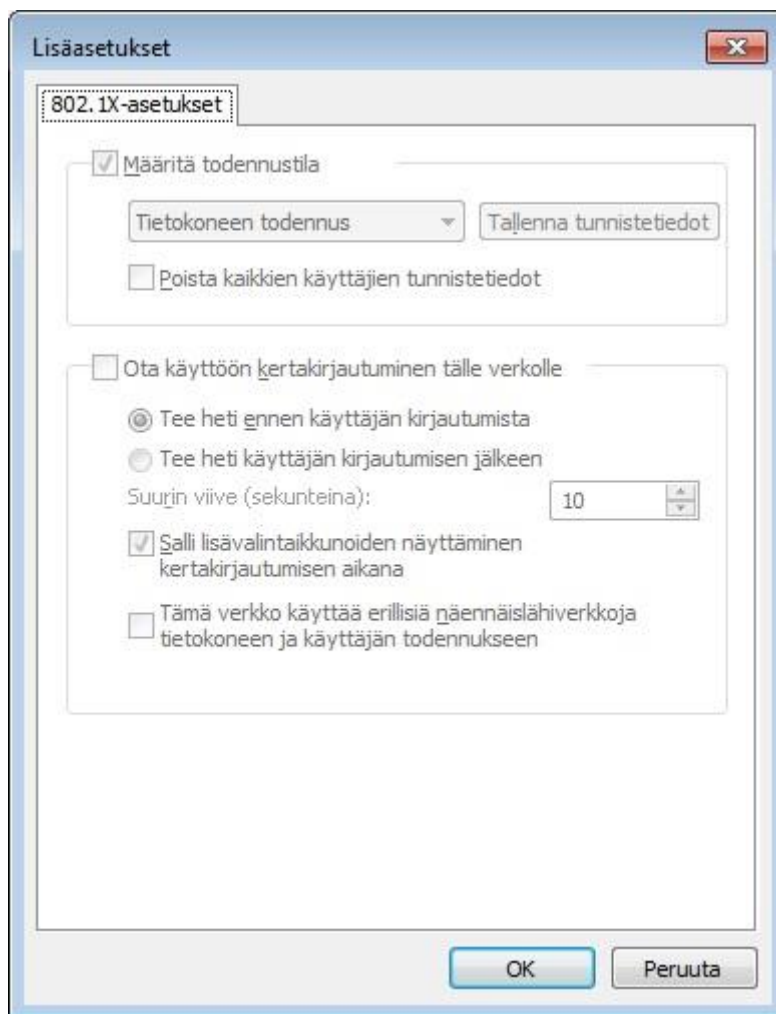


KUVIO 29. Työasemalla ei yhteyttä Internetiin

Katsotaan vielä, että tehdyt muutokset näkyvät myös lähiverkkoyhteyden ominaisuuksissa. Työssä haluttiin, ettei käyttäjä pääse muokkaamaan itse asetuksia, jotta tulevaisuudessa välttyään ongelmilta. Kuvioista 30 ja 31 nähdään, ettei käyttäjä voi muokata todennuksen asetuksia ja asetukset tulevat ryhmäkäytännön myötä automaattisesti.



KUVIO 30. Todennuksen asetukset



KUVIO 31. Todennuksen asetukset

## 8.5 Autentikoinnin toiminta

Pilottiympäristössä tehty autentikointiratkaisu toimii täysin automaattisesti ilman, että käyttäjä edes huomaa autentikoinnin olemassaoloa. Kun uusia koneita asennetaan, saa kone automaattisesti ryhmäkäytännön avulla autentikointitiedot, joilla se pääsee kirjautumaan PHSOTEY:n verkkoon. MAC-autentikoinnilla sekä portaali-autentikoinnilla tämä ei olisi ollut mahdollista. Ympäristön on oltava mahdollisimman yksinkertainen, sillä 4 000 henkilön yhtymässä ohjeistaminen jokaiselle on erittäin hankalaa.

Ympäristön asennus ja toteutus onnistuivat ilman suurempia ongelmia, mutta pilottiympäristön pystyttämisen jälkeen tuli ongelmaksi sellaiset laitteet, jotka 802.1x autentikointia eivät tue. Tällaisia laitteita ovat verkkotulostimet,

terveydenhuollon verkkolaitteet, IP-puhelimet sekä IP-kamerat. Näiden toimintaa ei pilotissa testattu lainkaan ja tuotantoon siirryttäessä on 802.1x-autentikoinnin ohelle otettava myös MAC-autentikointi. 802.1x-autentikointia tukemattomia laitteita on todennäköisesti erittäin vähän, joten MAC-autentikoinnin käyttöönoton ja ylläpidon ei pitäisi olla kovin suuritöinen.

## 9 YHTEENVETO

Opinnäytetyö perustui toimeksiantoon, jossa tarkoituksena oli pystyttää pilotointiympäristö porttikohtaiselle autentikoinnille. Koska valinnanvaraa autentikointitavoista on sen verran vähän, päädyttiin melkeinpä suoraan 802.1x-autentikointiin. Vertailussa olevista autentikointimenetelmistä 802.1x-autentikointi on myös tietoturvalisin ja käytännöllisin vaihtoehto.

Opinnäytetyössä käytiin läpi tietoturvaa, lähiverkon toimintaa, autentikointimenetelmiä sekä porttikohtaisessa autentikoinnissa käytettäviä eri protokollia. Pilottiympäristössä mallinnettiin PHSOTY:n tuotantoa ja testattiin ympäristön toimivuutta eri kytkimillä, millä varmistettiin autentikoinnin toimivuus myös työn tullessa tuotantoympäristöön.

Pilottiympäristössä testattiin vain työasemia. Todellisuudessa verkossa on muitakin laitteita kuin pelkästään tietokoneita, kuten esimerkiksi verkkotulostimet, IP-kamerat, IP-puhelimet ja verkossa olevat terveydenhuoltolaitteet. Näiden laitteiden toimintaa ei pilottiympäristössä testattu lainkaan. MAC-autentikoinnin lisääminen 802.1x-autentikoinnin rinnalle ei ole kuitenkaan suuritöinen muutos, mutta sen testaus olisi ollut hyödyllinen tuotantoa silmälläpitäen.

Jos ympäristöt ovat sellaisia, joissa joudutaan ottamaan MAC-autentikointi käyttöön, laskee tietoturvan taso, sillä kuka vain voi väärentää oman MAC-osoitteensa. Tulostimelta voidaan kopioida autentikoidun laitteen MAC-osoite ja ottaa se käyttöön omalla koneella ja näin saada yhteys yhtymän sisäverkkoon. Kuitenkin MAC-autentikoinnin käyttäminen on paljon tietoturvalisempaa kuin autentikoinnin pois jättäminen kokonaan.

Porttikohtaisen autentikoinnin tuoma hyöty yrityksen tietoturvaan nähden on erittäin suuri. Ulkopuoliset käyttäjät voidaan pienellä vaivalla saada yrityksen verkosta kokonaan estettyä ja tietoturvan taso yrityksessä nousee huomattavasti. Tulevaisuudessa tietoturvan merkitys kasvaa ja on tärkeää pitää henkilökohtainen ja arkaluontoinen tieto vain niiden käsissä, joille se kuuluu. Vaikka autentikoinnin lisääminen yritykselle ei kuulosta suurelta asialta, on todellisuudessa tietoturvan näkökulmasta autentikoinnin lisäämisellä erittäin suuri vaikutus koko yritykselle.

## LÄHTEET

Painetut lähteet:

Gast, M. 2002. 802.11® Wireless Networks: The Definitive Guide

Hassell, J. 2002. RADIUS. O'Reilly & Associates

Sähköiset lähteet:

802.1x. 2014. [viitattu 29.2.2015]. Saatavissa: <http://www.tech-faq.com/8021x.html>

Aboba, B. 2004. Extensible Authentication Protocol [viitattu 16.4.2015]. Saatavissa: <https://tools.ietf.org/html/rfc3748>

Albrecht, M. 2015. F-Securen Hyppönen: Haittaohjelmat usein Venäjältä ja Baltiasta – "Taitoja ja kykyjä, mutta ei töitä" [viitattu 28.2.2015]. Saatavissa: <http://www.yrittajat.fi/fi-FI/uutisarkisto/a/uutisarkisto/f-securen-hypponen-haittaohjelmat-usein-venajalta-ja-baltiasta-taitoja-ja-kykyja-mutta-ei-toita>

Cisco 2015a. 2015 [viitattu 5.3.2015]. 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#wp1259589](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#wp1259589)

EAPoL. 2015. [viitattu 22.3.2015]. Saatavissa: <http://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/>

HP ProCurve 2610-24. 2015. Saatavissa: <https://kauppa.lanwan.fi/cgi-bin/nph-cgi/~0YTRx0000001/?Y999=PIF&Y104=J9085A%23ABB>

HP ProCurve 2650. 2015. Saatavissa: [http://www.powersourceonline.com/buy-equipment/hp\\_parts-J4899C-cy-en.jsa](http://www.powersourceonline.com/buy-equipment/hp_parts-J4899C-cy-en.jsa)

Janssen, C. 2015. Virtual Local Area Network (VLAN). [viitattu 25.3.2015]. Saatavissa: <http://www.techopedia.com/definition/4804/virtual-local-area-network-vlan>



Kinnunen, N. 2015. Tietoturva osana yrityksen liiketoimintaa. [viitattu 28.2.2015]. Saatavissa: <http://www.turvallisuusopas.fi/tietoturva/tietoturva-osana-yrityksen-liiketoimintaa>

Lindström, A. 2015. Tietoturva [viitattu 28.2.2015]. Saatavissa: <http://www.lindstorm.org/tietoturva/tietoturva.html>

Loos, J. 2012. Implementing IEEE 802.1x for Wired Networks [viitattu 25.3.2015]. Saatavissa: <http://www.sans.org/reading-room/whitepapers/authentication/implementing-ieee-8021x-wired-networks-34520>

MAC authentication. 2015. [viitattu 26.3.2015]. Saatavissa: [http://www.arubanetworks.com/techdocs/InstantMobile/Advanced/Content/Instant%20User%20Guide%20-%20volumes/MAC\\_Authentication.htm#authentication\\_586225611\\_1027641](http://www.arubanetworks.com/techdocs/InstantMobile/Advanced/Content/Instant%20User%20Guide%20-%20volumes/MAC_Authentication.htm#authentication_586225611_1027641)

Mitchell, B. 2015 LAN – Local Area Network. [viitattu 25.3.2015]. Saatavissa: [http://compnetworking.about.com/cs/lanvlanwan/g/bldef\\_lan.htm](http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm)

Olzak, T. 2012. End-user Device Security [viitattu 26.3.2015]. Saatavissa: <http://resources.infosecinstitute.com/end-user-chapter-6/>

Olzak, T. 2012. VLAN Network Segmentation and Security [viitattu 26.3.2015]. Saatavissa: <http://resources.infosecinstitute.com/vlan-network-chapter-5/>

OSI-malli. 2015. [viitattu 16.4.2015]. Saatavissa: [http://fi.at02.wikia.com/wiki/OSI\\_malli](http://fi.at02.wikia.com/wiki/OSI_malli)

PEAP. 2015. [viitattu 26.3.2015]. Saatavissa: <https://technet.microsoft.com/en-us/library/cc757996%28v=ws.10%29.aspx>

Pietikäinen, S. 2013. Tietoturvallisuus – Mitä se on? [viitattu 28.2.2015]. Saatavissa: <https://www.vahtiohje.fi/web/guest/691>

Portal Authentication Technology White Paper. 2008. [viitattu 6.4.2015]. Saatavissa: [www.h3c.com/portal/download.do?id=675250](http://www.h3c.com/portal/download.do?id=675250)

Päijät-Hämeen sosiaali- ja terveysyhtymä. 2015. [viitattu 28.2.2015]. Saatavissa: <http://www.phsotey.fi/sivut/?vy=9987&ryhma=253>

RADIUS Authentication, Authorization, and Accounting. 2015. [viitattu 16.4.2015]. Saatavissa: <https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb892012%28v=vs.85%29.aspx>

Simpson, W. 1992. PPP Authentication Protocols [viitattu 16.4.2015]. Saatavissa: <http://www.faqs.org/rfcs/rfc1334.html>

Simpson, W. 1996. PPP Challenge Handshake Authentication Protocol [viitattu 16.4.2015]. Saatavissa: <http://www.faqs.org/rfcs/rfc1994.html>

Summit X450a 48t. 2011. Saatavissa: <http://assets.extremenetworks.com/?q=node/51>

Szilagyi, A., Sood, A. & Singh, T. 2009. RADIUS: A Remote Authentication Dial-In User Service. [viitattu 8.4.2015]. Saatavissa: <https://www.rivier.edu/journal/ROAJ-Fall-2009/J286-RADIUS-Sood.pdf>

Understanding 802.1X. 2015. [viitattu 22.3.2015]. Saatavissa: <https://sites.google.com/site/amitsciscozone/home/switching/802-1x>

VLAN-perusteet. 2015. [viitattu 25.3.2015]. Saatavissa: <http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html>

Wikipedia. 2015a. Extensible Authentication Protocol [viitattu 25.3.2015]. Saatavissa: [http://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

Wikipedia. 2015b. PPP. [viitattu 16.4.2015]. Saatavissa: <http://fi.wikipedia.org/wiki/PPP>

Wikipedia. 2015c. Radius. [viitattu 16.4.2015]. Saatavissa: <http://en.wikipedia.org/wiki/RADIUS>

Woland, A. 2013. EAP Primer. [viitattu 16.4.2015]. Saatavissa: <http://blog.woland.com/?p=9>

## LIITTEET

Kytökimen 1 konfigurointi:

Pro1(config)# sho run

Running configuration:

; J9085A Configuration Editor; Created on release #R.11.107

hostname "Pro1"

time timezone 120

time daylight-time-rule Western-Europe

ip default-gateway x.x.x.x

timesync sntp

snmp-server community "public" Unrestricted

vlan 1

    name "DEFAULT\_VLAN"

    untagged 27-28

    no ip address

    no untagged 1-26

    exit

vlan 1110

    name "testiws"

    untagged 1-25

    ip address x.x.x.x x.x.x.x

    tagged 26

    exit

ip authorized-managers x.x.x.x x.x.x.x

ip authorized-managers x.x.x.x x.x.x.x

radius-server host x.x.x.x acct-port 1813 key "802testi"

sntp unicast

sntp server x.x.x.x

aaa authentication port-access eap-radius

aaa port-access authenticator 1-10

aaa port-access authenticator active

ip ssh

Kytkimen 2 konfigurointi:

```
Pro2# show running-config
```

Running configuration:

```
; J4899A Configuration Editor; Created on release #H.10.115
```

```
hostname "Pro2"
```

```
time timezone 120
```

```
time daylight-time-rule Western-Europe
```

```
interface 1
```

```
    no lacp
```

```
exit
```

```
interface 2
```

```
    no lacp
```

```
exit
```

```
interface 3
```

```
    no lacp
```

```
exit
```

```
interface 4
```

```
    no lacp
```

```
exit
```

```
interface 5
```

```
    no lacp
```

```
exit
```

```
interface 6
```

```
    no lacp
```

```
exit
```

```
interface 7
```

```
    no lacp
```

```
exit
```

```
interface 8
```

```
    no lacp
```

```
exit
```

```
interface 9
```

```
    no lacp
```

```

exit
interface 10
    no lacp
exit
ip default-gateway x.x.x.x
snmp server x.x.x.x
timesync snmp
snmp unicast
snmp-server community "public" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    no ip address
    no untagged 1-50
    exit
vlan 1110
    name "testiws"
    untagged 1-47
    ip address x.x.x.x x.x.x.x
    tagged 48-50
    exit
ip authorized-managers x.x.x.x x.x.x.x
ip authorized-managers x.x.x.x x.x.x.x
aaa authentication port-access eap-radius
radius-server host x.x.x.x 802testi
aaa port-access authenticator 1-10
aaa port-access authenticator active
ip ssh

```

Kytökimen 3 konfigurointi:

```

Extreme1.1 # sho configuration
# Module devmgr configuration.
configure snmp sysName "Extreme1"

```

```

configure timezone name EET 120 autodst name EET begins every last sunday
march at 3 0 ends every last sunday october at 4 0
configure sys-recovery-level switch reset
# Module vlan configuration.
configure vlan default delete ports all
configure vr VR-Default delete ports 1-50
configure vr VR-Default add ports 1-50
configure vlan default delete ports 1-48
create vlan "testiws"
configure vlan testiws tag 1110
create vlan "turha2"
configure vlan Default add ports 49-50 untagged
configure vlan testiws add ports 47-48 tagged
configure vlan testiws add ports 1-11 untagged
configure vlan testiws ipaddress x.x.x.x x.x.x.x
# Module fdb configuration.
configure iparp vr VR-Default max_entries 4096
configure neighbor-discovery vr VR-Default timeout 10
configure neighbor-discovery vr VR-Mgmt timeout 10
# Module rtmgr configuration.
configure iproute add default x.x.x.x
# Module mcmgr configuration.
# Module aaa configuration.
configure radius netlogin primary server x.x.x.x 1812 client-ip x.x.x.x vr VR-
Default
configure radius netlogin primary shared-secret encrypted ":%lt;;~orvm"
enable radius netlogin
configure account admin encrypted "ilH35T$nJrfMNIaOD5q/f73QnfrS."

# Module acl configuration.
configure access-list zone DOS application Dos application-priority 1
configure access-list zone SYSTEM application NetLogin application-priority 3
# Module bfd configuration.
# Module ces configuration.

```

```
# Module cfgmgr configuration.
# Module dosprotect configuration.
# Module dot1ag configuration.
# Module eaps configuration.
# Module edp configuration.
# Module elrp configuration.
# Module ems configuration.
# Module epm configuration.
enable cpu-monitoring interval 20
# Module erps configuration.
# Module esrp configuration.
# Module ethoam configuration.
# Module etmon configuration.
# Module exsshd configuration.
enable ssh2
# Module hal configuration.
# Module idMgr configuration.
# Module ipSecurity configuration.
# Module ipfix configuration.
# Module lldp configuration.
# Module mrp configuration.
# Module msdp configuration.
# Module netLogin configuration.
configure netlogin vlan turha2
enable netlogin dot1x
enable netlogin ports 1-11 dot1x
configure netlogin ports 1 mode port-based-vlans
configure netlogin ports 1 no-restart
configure netlogin ports 2 mode port-based-vlans
configure netlogin ports 2 no-restart
configure netlogin ports 3 mode port-based-vlans
configure netlogin ports 3 no-restart
configure netlogin ports 4 mode port-based-vlans
configure netlogin ports 4 no-restart
```

```
configure netlogin ports 5 mode port-based-vlans
configure netlogin ports 5 no-restart
configure netlogin ports 6 mode port-based-vlans
configure netlogin ports 6 no-restart
configure netlogin ports 7 mode port-based-vlans
configure netlogin ports 7 no-restart
configure netlogin ports 8 mode port-based-vlans
configure netlogin ports 8 no-restart
configure netlogin ports 9 mode port-based-vlans
configure netlogin ports 9 no-restart
configure netlogin ports 10 mode port-based-vlans
configure netlogin ports 10 no-restart
configure netlogin ports 11 mode port-based-vlans
configure netlogin ports 11 no-restart
# Module netTools configuration.
configure sntp-client primary x.x.x.x vr VR-Default
enable sntp-client
# Module ospf configuration.
configure ospf vlan testiw priority 0
# Module ospfv3 configuration.
# Module pim configuration.
# Module poe configuration.
# Module rip configuration.
# Module ripng configuration.
# Module snmpMaster configuration.
# Module stp configuration.
configure mstp region 00049627c409
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
# Module synce configuration.
# Module telnetd configuration.
# Module tftpd configuration.
# Module tftttd configuration.
```



# Module vmt configuration.

# Module vrrp configuration.

# Module vsm configuration.