Janne Kangas

Sertifikaattipohjaisen autentikoinnin käyttöönotto langallisessa työasemaympäristössä

Seinäjoen ammattikorkeakoulu

Opinnäytetyö
Kevät 2020
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Tekniikka

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Janne Kangas

Työn nimi: Sertifikaattipohjaisen autentikoinnin käyttöönotto langallisessa työasemaympäristössä

Ohjaaja: Alpo Anttonen

Vuosi: 2020 Sivumäärä: 66

Porttikohtainen autentikointi on yksi turvallisimmista vaihtoehdoista suojata tietoliikenneverkkoa riippumatta siitä, kuinka suuri käyttäjäkunta kyseisellä verkolla on. Tässä opinnäytetyössä käydään läpi porttikohtaisen autentikoinnin teoriaa ja siihen liittyviä vaatimuksia ja ominaisuuksia.

Opinnäytetyössä luodaan pieni testiympäristö hyödyntäen Seinäjoen ammattikorkeakoulun laitteita ja ohjelmistoja. Porttikohtaisesta autentikoinnista käydään läpi siihen kuuluvista protokollista EAP, RADIUS ja PEAP. Työssä luotiin PEAP-EAP-TLS-pohjainen autentikointiratkaisu, jonka avulla käyttäjien ei tarvitse huolehtia ylimääräisistä salasanoista vaan autentikointi suoritetaan automaattisesti työaseman ja autentikointipalvelimen välillä hyödyntämällä sertifikaattipohjaista autentikointia. Tällä autentikointimenetelmällä poistetaan inhimilliset virheet ja lisätään tietoturvaa.

Työssä käytettiin Ciscon verkkolaitteita, Windows Server 2016 -käyttöjärjestelmän omaavaa palvelinta ja kolmea työasemaa, joihin oli asennettu Windows 10. Työssä käytetyt IP-osoitteet ovat keksittyjä ja niiden jakamisesta vastasi palvelin. Teoriaosa rajattiin käsittelemään opinnäytetyössä tarvittavia malleja, protokollia ja esimerkkejä, jotka tarvitaan toimivan porttikohtaisen autentikointikokonaisuuden konfiguroimiseen.

802.1X, EAP, PEAP-EAP-TLS, RADIUS, tietoturva

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Network Technology

Author: Janne Kangas

Title of thesis: Deployment of a Certificate-based Authentication in a Wired Workstation Environment

Supervisor: Alpo Anttonen

Year: 2020 Number of pages: 66

Port-based authentication is one of the safest methods to secure a telecommunications network regardless of the size of the userbase that the network holds. This thesis focused on the theory regarding port-based authentication along with its requirements and features.

A small test environment was created for the thesis using the equipment and software provided by Seinäjoki University of Applied Sciences. From all port-based authentication protocols EAP, RADIUS and PEAP were the ones that were discussed. In the thesis a PEAP-EAP-TLS-based authentication solution was implemented, so that users do not have to deal with extra passwords since authentication is carried out automatically by the computer and authentication server by using certificate-based authentication. This authentication method removes the possibility of human errors and increases security.

The practical part of the thesis was done using Cisco network equipment, a physical server running Windows Server 2016 operating system, and three computers that had Windows 10 operating system installed on them. The IP addresses used in the thesis were made up and they were distributed by the server. The theory part of the thesis concentrated on the models, protocols and examples needed to configure a functioning port-based authentication in its entirety.

802.1X, EAP, PEAP-EAP-TLS, RADIUS, information security

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

AAA	Authentication Authorization Accounting. AAA/AAA-mallilla viitataan protokollien joukkoon, joka vastaa verkkoon pääsystä.
AD	Active Directory. Microsoftin kehittämä hakemistopalvelu käyttäjä- ja työasematileille. Aktiivihakemiston avulla verkonvalvojat luovat ja hallinnoivat toimialueita, käyttäjiä ja erilaisia objekteja verkossa.
CS	Certification Services. Microsoftin Windows-palvelinympäristössä pyörivä palvelu, joka vastaa sertifikaattien jakamisesta.
CryptoAPI	Cryptographic Application Programming Interface. Microsoftin kehittämä sovellusohjelmointirajapinta, jonka avulla voidaan kehittää Windows-pohjaisia sovelluksia kryptografisesti.
DHCP	Dynamic Host Configuration Protocol. Protokolla, jonka avulla jaetaan IP-osoitteita dynaamisesti verkossa sijaitseville laitteille.
DNS	Domain Name System. Nimipalvelujärjestelmä, jolla nimetään työasemia, palveluita ja muita verkkoon tai internetiin liitettyjä resursseja.
EAP	Extensible Authentication Protocol. Autentikoinnissa käytetty protokolla, joka tukee useita eri autentikointimetodeja.
EAPOL	EAP Over LAN. EAPOL-nimityksellä tarkoitetaan paketointitekniikkaa, jolla 802.1X protokollan EAP-viestit kuljetetaan.

EKU	Extended Key Usage. EKU-nimityksellä tarkoitetaan sertifikaatin omaavia ominaisuuksia Windows-pohjaisissa käyttöjärjestelmissä.
Group policy	Group policy. Tarkoittaa Windows-pohjaisten käyttöjärjestelmien käyttämää ryhmäkäytäntöä, jonka avulla voidaan hallita käyttäjä- ja tietokonetilejä.
IAS	Internet Authentication Service. Tarkoittaa Windows-palvelimella olevaa komponenttia, jonka avulla voidaan keskitetysti hallita käyttäjien autentikointia, toimilupia ja kirjanpitoa.
IEEE 802.11	Kuvaa IEEE-standardia langattomille WLAN-lähiverkoille.
IEEE 802.1X	Kuvaa IEEE-standardia porttikohtaiselle verkonpääsynhallinnalle.
IEEE 802.3	Kuvaa IEEE-standardia, joka käsittää Ethernet-lähiverkkotekniikan.
LAN	Local Area Network. Tarkoittaa lähiverkkoa, jonka suuruus vaihtelee yhdestä huoneesta useaan rakennukseen. Lähiverkon avulla yhdistetään esim. työasemia toisiinsa.
MAC	Media Access Control. Laitteen uniikki fyysinen osoite, jolla laite pystytään tunnistamaan IEEE 802 -verkoissa.
NPS	Network Policy Server. Microsoftin versio RADIUS-palvelimesta ja proxystä. NPS vastaa autentikoinnista, auktorisoinnista ja kirjanpidosta (lokitus).
PEAP	Protected Extensible Authentication Protocol. Toinen versio EAP-protokollasta, joka kapseloi EAP-liikenteen TLS-tunnelin avulla.
PPP	Point-to-Point Protocol. OSI-mallin toisella kerroksella toimiva kommunikointiprotokolla kahden eri reitittimen välillä.

RADIUS Remote Authentication Dial-In User Service. Protokolla, joka käyttää UDP-porttia 1812 ja vastaa keskitetysti AAA:n käytäntöönpanemisesta.

TCP Transmission Control Protocol. TCP-lyhenteellä tarkoitetaan protokollaa, jossa paketit käydään järjestyksessä läpi. TCP:n ominaisuuksiin kuuluu pieni viive isäntien välillä. TCP:n avulla voidaan lähettää paketteja uudelleen, mikäli ne syystä tai toisesta ovat kadonneet bittiavaruuteen lähetyksen aikana.

TLS Transport Layer Security. Kryptografinen protokolla, jolla lisätään kommunikaatioiden välistä turvallisuutta työasemaverkossa.

TRCA Trusted Root Certification Authorities. Windows-pohjaisissa käyttöjärjestelmissä käytetty juurisertifikaattien oikeellisuudesta vastaava entiteetti.

UDP User Datagram Protocol. UDP-protokollassa hyödynnetään prosessista prosessiin välistä yhteyttä, kun taas TCP toimii isännältä isännälle -periaatteella. UDP:n avulla paketteja voidaan vastaanottaa ja hylätä järjestyksestä riippumatta.

VLAN Virtual Local Area Network. Virtuaalilähiverkko, jonka avulla voidaan segmentoida tietoliikenneverkko eri alueisiin ja täten lisätä skaalautuvuutta, tietoturvaa ja helpottaa verkonhallintaa.

Virtualisointialusta Alusta, jonne voidaan asentaa useita eri virtualisoituja työasemia ja palvelimia samanaikaisesti.

VPN Virtual Private Network. VPN-nimityksellä tarkoitetaan yksityistä verkkoa, joka kulkee julkisen verkon lävitse. VPN:n avulla voidaan lähettää ja vastaanottaa dataa sisäverkosta

toiseen ikään kuin ne olisivat samassa yksityisessä verkossa, vaikka niiden liikenne kulkeekin julkisen verkon lävitse.

1 JOHDANTO

Tämä työ käsittelee porttikohtaisen autentikoinnin luomista testiympäristöön käyttäen IEEE 802.1X -standardia. Työ toteutettiin yhteistyössä Seinäjoen ammattikorkeakoulun kanssa, jonne testiympäristö luotiin. Työssä hyödynnettiin Seinäjoen ammattikorkeakoulun tarjoamia teknisiä laitteita, kuten kytkintä, palvelinta ja työasemia. Työssä käydään läpi vaadittavat ohjelmistot, tekniset laitteet ja tarvittava opastus käyttöönottoa varten.

Porttikohtainen todentaminen toteutettiin Ciscon 2960-kytkimellä sekä Fujitsun-palvelimella, jonne oli asennettuna Citrix Server -virtualisointialusta. Virtualisointialustalla sijaitsevaan käyttöjärjestelmään muodostettiin erillinen yhteys kannettavalta työasemalta. Virtualisointialustalle oli asennettuna Windows Server 2016 -käyttöjärjestelmä.

Porttikohtaisen autentikoinnin toimintaideana on verkkoon pääsyn rajaaminen vain varmenteen tai tunnistetietojen omaaville käyttäjille. Tässä työssä käsitellään varmennepohjaista tunnistautumista, jossa työasemille jaettiin henkilökohtainen varmenne. Varmenteen avulla työasemat autentikoivat itsensä sisään verkkoympäristöön. Varmenne jaettiin työasemille hyödyntäen Windows-palvelimella olevaa ryhmäkäytäntöä, joka on liitetty aktiivihakemistoon.

1.1 Työn tavoitteet

Työn tavoitteena oli luoda testiympäristö, jonka pohjalta voidaan rakentaa toimiva porttikohtaisen autentikoinnin omaava verkkoympäristö. 802.1X-standardia hyödyntämällä taataan verkkoympäristön turvallisuus ja vähennetään haitanteon mahdollisuutta.

Tavoitteisiin kuului myös 802.1X-standardista johtuvien haittojen esille tuonti ja niille esitettävät ratkaisut. 802.1X:n avulla voidaan parantaa tietoturvaa, mutta siitä aiheutuu samalla haittoja laitteille, jotka eivät välttämättä osaa käsitellä EAP-viestejä kuten vanhemmat tulostimet tai IP-puhelimet.

1.2 Työn rajaus

Tässä projektissa käsitellään langallisesti toimivaa IEEE 802.3 -standardin mukaista lähiverkkoratkaisua. Projektin ulkopuolelle jätetään langattomasti toimivat IEEE 802.11 -standardin mukaiset ratkaisut ja perehdytään pitkälti siihen, kuinka 802.1X-toteutus voidaan luoda suurille ja keskisuurille organisaatioille mahdollisimman pienellä häiriöajalla.

Työssä luotu testiympäristö toimii pohjana 802.1X:n implementoinnille eikä kaikkia osa-alueita täten sisällytetä siihen. Ulkopuolelle jätetään mobiiliratkaisut, kuten kannettavat tietokoneet, PDA-laitteet ja älypuhelimet. 802.1X -standardia voidaan toteuttaa myös kyseisille laitteille, mutta käytännössä tämä muodostaisi oman kokonaisuutensa.

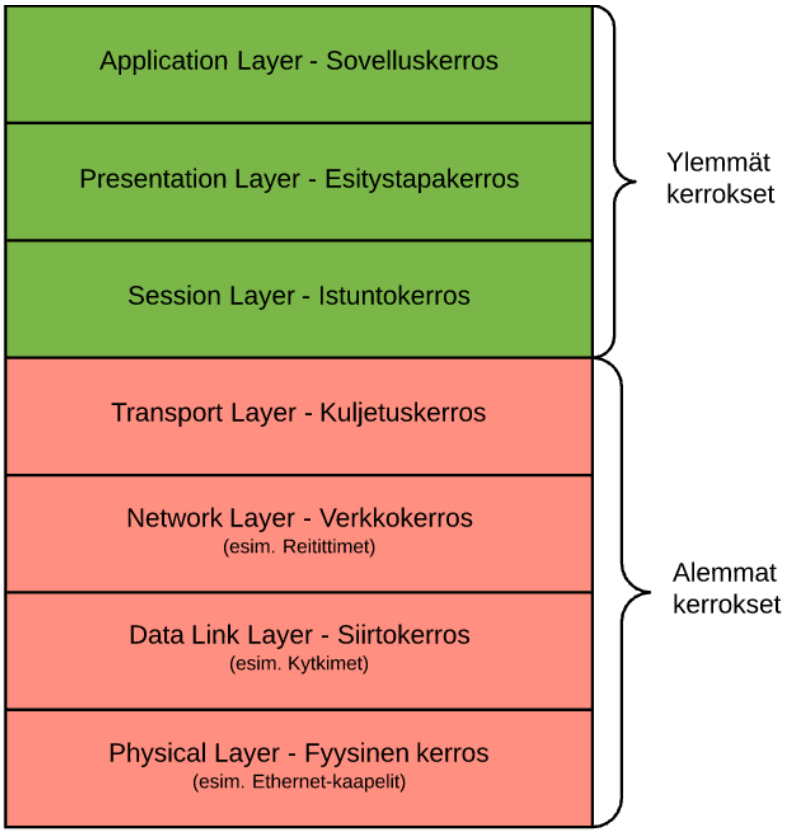
Projektissa esiintyvä testiympäristö kuvaa yhtä ratkaisua 802.1X:n integroimisesta verkkoympäristöön. Tulokset ja päätelmät perustuvat näin projektissa esiintyvien ratkaisujen pohjalle. Testiympäristössä esiintyvät IP-numerot ja laitteiden nimet ovat keksittyjä, eikä niitä suositella käyttämään testiympäristön ulkopuolella samaan tarkoitukseen.

1.3 Työn rakenne

Työn ensimmäinen luku antaa pohjan sille, mitä opinnäytetyössä tullaan käsittelemään, minkälaiset rajaukset sille on asetettu ja minkälaisiin tavoitteisiin pyritään. Toisessa luvussa käydään läpi OSI-malli. Kolmannessa luvussa käydään läpi teoriaa liittyen 802.1X-standardin toimintaan. Neljännessä luvussa käsitellään EAP-, PEAP- ja RADIUS-protokollia. Viidennessä luvussa aloitetaan toteutus. Kuudennessa luvussa käydään läpi projektista saatuja tuloksia ja viimeisessä eli seitsemännessä luvussa käydään läpi opinnäytetyön pohjalta saatu yhteenveto.

2 OSI-MALLI

OSI-mallilla viitataan seitsemänkerroksiseen jaotteluun verkon osalta. Kaikki seitsemän kerrosta omaavat oman roolinsa verkon toiminnan kannalta. IEEE 802.3 eli Ethernet ja IEEE 802.11 eli WLAN, jotka toimivat kerroksella 2, jakavat OSI-mallissa kerroksen 2 omiin alikerroksiin. Kerrokset ovat yhteydessä toisiinsa ainoastaan mentäessä alhaalta ylöspäin. Esimerkiksi kerroksien 2 ja 3 välinen suhde on vain yhdensuuntainen, missä kerros 2 on yhteydessä kerrokseen 3, mutta kerroksessa 3 tapahtuvat toiminnot eivät ole riippuvaisia alemmilla kerroksilla tapahtuvista muutoksista. (Geier 2008, 21.)



Kuvio 1. OSI-malli (Geier 2008, 21).

Kuviossa 1 olevat kerrokset määritellään seuraavasti:

1. **Fyysinen kerros – Physical Layer:** määrittelee nimensä mukaisesti verkossa esiintyvät fyysiset laitteet ja niiden ominaisuudet. Ominaisuutena fyysisellä kerroksella ovat erilaiset kaapelityypit liitäntäpisteissä, kuten Ethernet-kaapelin käyttö verkossa olevien laitteiden välillä. (Geier 2008, 21.)

2. **Siirtokerros – Data Link Layer:** kuvaa laitteiden välille muodostunutta yhteyttä. Tälle kerrokselle ominaisia piirteitä ovat MAC-osoite, jonka avulla voidaan kommunikoida kahden eri laitteen välillä. Siirtokerroksessa olevia laitteita ovat esimerkiksi kytkimet ja langattomat tukiasemat. (Geier 2008, 21.)

3. **Verkkokerros – Network Layer:** kuvaa kerrosta, jossa paketit reititetään verkon läpi kohteesta A kohteeseen B. Reititin on yksi verkkokerroksella toimiva laite, jonka avulla reititys voidaan luoda kohteiden välille. Esimerkkinä verkkokerroksella käytettävistä protokollista on IP eli Internet Protocol. (Geier 2008, 21.)

4. **Kuljetuskerros – Transport Layer:** kuljetuskerroksella luodaan ja ylläpidetään yhteyttä kahden verkossa toimivan laitteen välillä (Geier 2008, 21). Kuljetuskerrokselle tyypillisiä ominaisuuksia ovat siinä esiintyvät uniikit kuljetusosoitteet (transport-address), jotka määrittelevät jokaisen istunnon. (ISO/IEC 7498-1 1994, 37.)

5. **Istuntokerros – Session Layer:** kuvaa datan liikkumista verkossa olevien laitteiden välillä (Geier 2008, 21). Istuntokerroksen on nimensä mukaisesti tarkoitus antaa tarvittavat resurssit kahden istunnossa olevan entiteetin välille, jonka avulla voidaan tukea datan vaihtoa ja katkaista se tarpeen tullen oikeaoppisesti. (ISO/IEC 7498-1 1994, 35).

6. **Esitystapakerros – Presentation Layer:** Esitystapakerroksella viitataan verkossa esiintyvien laitteiden välisen kommunikaation syntaksiin, joka tässä asiayhteydessä viittaa tapaan säilyttää ylemmällä kerroksella eli sovelluskerroksella liikkuvien pakettien sisällön eheys siirrosta johtuvista tekijöistä riippumatta. (ISO/IEC 7498-1 1994, 33.)

7. **Sovelluskerros – Application Layer:** kuvaa korkeinta tasoa OSI-mallissa, mikä sisältää kaikki kommunikaatioon viittaavat tehtävät, joita alemmat tasot eivät ole jo tehneet. Näihin tehtäviin mukaan luetaan ohjelmien sekä ihmisten tekemät toimenpiteet. (ISO/IEC 7498-1 1994, 32.)

3 IEEE 802.1X -STANDARDI

IEEE 802.1X -standardin porttikohtaisella autentikoinnilla tarkoitetaan toimintatapaa, jossa verkkoon pääsy voidaan sallia, rajata tai evätä riippuen laitteelta saaduista tunnistetiedoista. Mikäli laite ei pysty antamaan verkon vaatimia tunnistetietoja, voidaan siltä evätä pääsy kokonaan verkkoon. Vaihtoehtoisesti tunnistetietojen onnistuneesta hyväksynnästä annetaan laitteelle pääsy suojattuun verkkoon. (Geier 2008, 33.)

Porttikohtainen autentikointi vaatii toimiakseen tietyt edellytykset, joita ilman se ei pysty toimimaan. 802.1X-standardin mukaisessa porttikohtaisessa autentikoinnissa olevia pääkomponentteja ovat supplicant (asiakas), authenticator (autentikaattori), authentication server (autentikointipalvelin, joka tässä kontekstissa RADIUS-palvelin). (Geier 2008, 38.)

3.1 Asiakas

Asiakkaalla viitataan tässä kontekstissa laitteeseen, jolla halutaan muodostaa yhteys suojattuun verkkoon käyttäen 802.1X-standardin mukaista tunnistautumista. Asiakasta käsitellään tässä opinnäytetyössä työaseman näkökulmasta eli asiakkaina toimivat työasemat, jotka omaavat verkkokortin, joihin voidaan yhdistää Ethernet-kaapeli. Työasemille on asennettu Windows 10 käyttöjärjestelmä, joka tukee 802.1X-protokollaa. (Microsoft 2016a.)

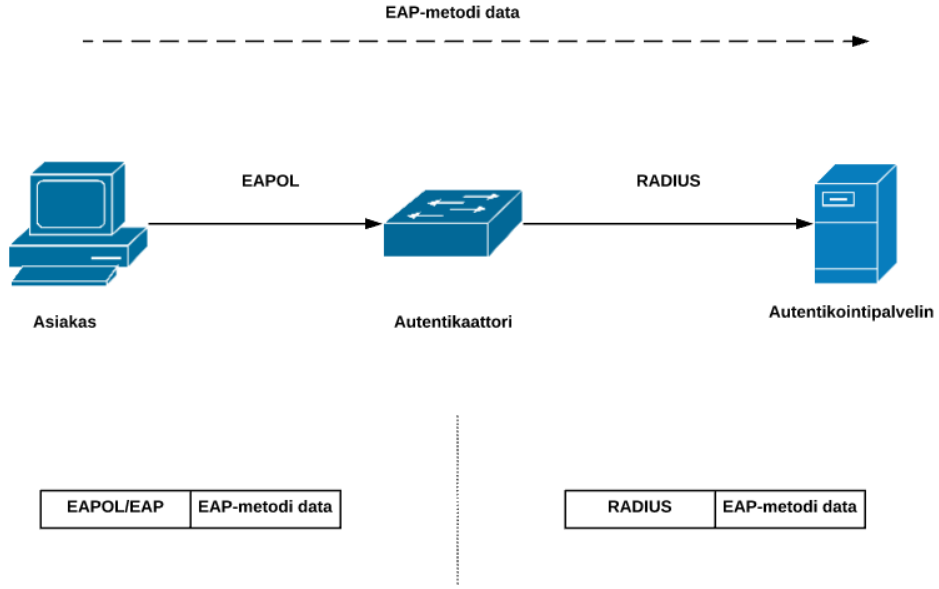
Asiakkaat eli ns. supplicantit ovat lähtökohtaisesti autentikaattoreille tuntemattomia entiteettejä, mikäli asiakkaat haluavat muodostaa yhteyden verkkoon vaaditaan niiltä tunnistetietojen läpikäyntiä. Tämä tunnistetietojen läpikäyntiprosessi aloitetaan lähettämällä autentikointipalvelimelle pyyntö hyödyntämällä EAP-protokollaa. (Geier 2008, 39.)

3.2 Autentikaattori

Autentikaattorilla tarkoitetaan fyysistä laitetta, joka toimii OSI-mallin toisessa eli siirtokerroksessa. Geierin (2008, 284) mukaan autentikaattorit toimivat eräänlaisena turvaporttina asiakkaiden ja suojatun verkon välillä. Jokainen 802.1X-standardin mukaan konfiguroitu portti pysyy kiinni siihen asti, kunnes autentikaattori pystyy vahvistamaan asiakkaalta saatujen tunnistetietojen avulla, minkälainen pääsy asiakkaalle on määritelty.

Autentikaattoreina toimivat Ethernet-kytkimet ja langattomat tukiasemat. Ethernet-kytkimien kohdalla portti pysyy kiinni siihen asti, kunnes järjestelmä on todentanut tunnistetietojen olevan kunnossa, jonka jälkeen pääsy suojattuun verkkoon avataan. (Geier 2008, 39.)

Autentikaattorin toiminta on mahdollistaa asiakkaan ja autentikointipalvelimen välinen dialogi, joka vaaditaan 802.1X-standardissa käytetyn EAP-protokollan toimintaan. Asiakkaan lähettämät tunnistetiedot kapseloidaan EAP-metodissa esiintyvän määrityksen mukaan EAP-kehykseen, joka kapseloidaan uudelleen EAPOL-kehykseen. EAPOL-kehys lähetetään autentikaattorille, joka poistaa EAP-metodissa määritellyn datan. Autentikaattori kapseloi EAP-metodista saadun datan RADIUS-kehykseen, joka lähetetään eteenpäin autentikointipalvelimelle. (Geier 2008, 39.)



Kuvio 2. Laitteiden välinen dialogi

3.3 Autentikointipalvelin

Autentikointipalvelimella tarkoitetaan entiteettiä, joka suorittaa pyynnön asiakkaalle tunnistetietojen tarpeesta. Pyynnön seurauksena asiakas lähettää palvelimelle halutut tunnistetiedot, jotka palvelin joko hyväksyy tai hylkää. Autentikointipalvelin voidaan joissain tapauksissa sisällyttää myös autentikaattoreihin, mikä Geierin (2008, 40) mukaan vähentää verkossa olevaa liikennettä todella paljon, mikä on erityisen tavoiteltua langattomissa verkoissa, joissa liikutaan usein paikasta toiseen.

4 PROTOKOLLAT

Opinnäytetyössä esiintyvät protokollat EAP, RADIUS ja PEAP toimivat OSI-mallin kerroksella 2. Näiden protokollien tarkoituksena on luoda tietoturvallisempi ympäristö aina pienistä yritysverkoista laajoihin organisaatioverkkoihin asti mahdollistamalla porttikohtaisen autentikoinnin integroiminen verkkoympäristöön. Etuna kyseisille protokollille on niiden erinomainen kyky skaalautua tarpeiden mukaan ja säilyttää tietoturvan taso riippumatta mittakaavasta.

4.1 EAP (Extensible Authentication Protocol)

EAP-protokollalla kuvataan autentikoinninrakennetta, joka tukee useata eri autentikointimetodia. EAP toimii tyypillisesti suoraan siirtokerroksella (Data Link Layer), mikä mahdollistaa sen, että se ei tarvitse IP-osoitetta. EAP-protokollaa hyödynnetään IEEE 802- ja PPP-yhteyksissä. (RFC 3748 2004, 2.)

EAP-protokollan hyödyt tulevat esiin sen joustavuudessa hyödyntää useita eri autentikointimenetelmiä. Tyypillisesti autentikointimenetelmä valitaan vasta autentikaattorin pyytäessä lisätietoa asiakkaalta. Autentikointipalvelimen avulla voidaan hyödyntää yhtä tai useampaa autentikointimenetelmää, jossa autentikaattori toimii ainoastaan välikappaleena, joka päästää kaikki autentikointipalvelimella esiintyvät menetelmät lävitseen. (RFC 3748 2004, 2.)

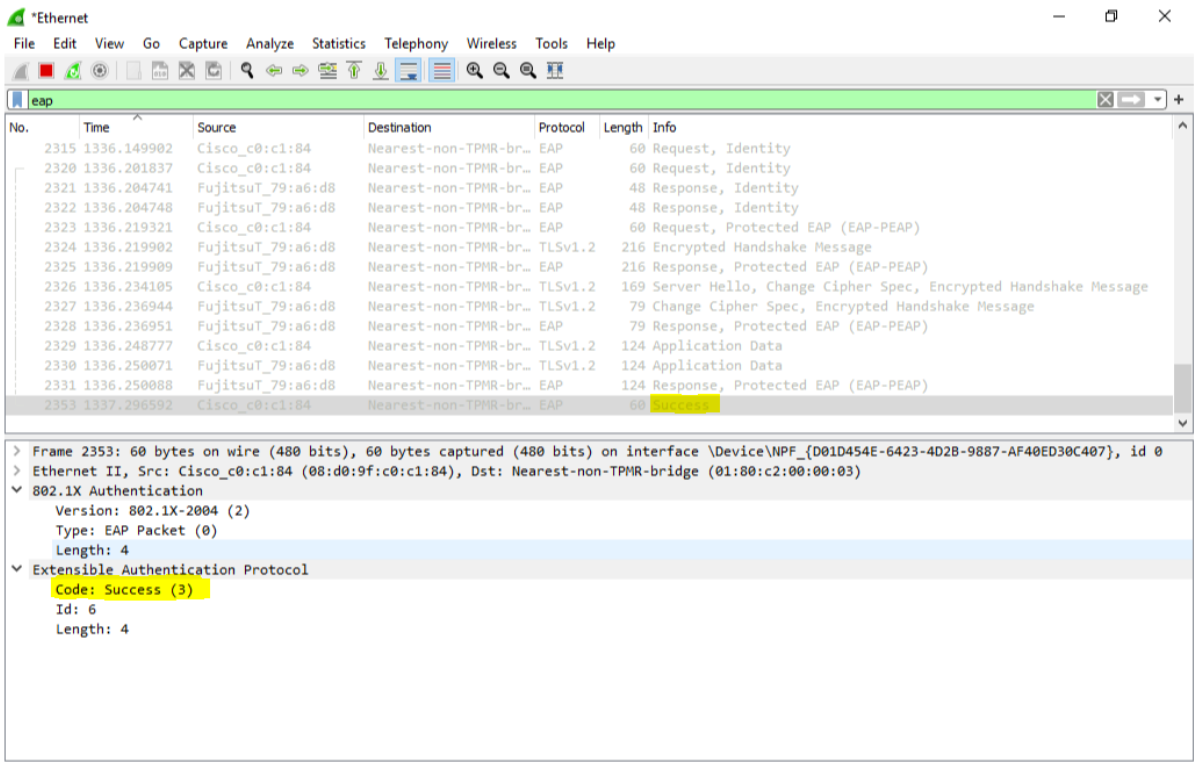
Internet Societyn luomassa standardissa (RFC 3748 2004, 7-8) jaetaan EAP-protokollassa esiintyvä todennus neljään eri vaiheeseen:

1. Ensimmäisessä vaiheessa autentikaattori lähettää pyynnön (Identity-Request) autentikointia tarvitsevalle osapuolelle. Pyyntö sisältää tyyppikentän, jossa kysytään haluttavia tietoja. Autentikaattorin tekemä pyyntö voidaan kuitenkin ohittaa tietyissä tapauksissa, kuten silloin kun toisen osapuolen identiteetti voidaan todentaa toisella tapaa kuten MAC-osoitteella.

2. Todennukseen vastaava osapuoli vastaa niin sanotulla Response-paketilla, joka sisältää saman tyyppikentän, jonka autentikaattori alustavasti on pyytänyt ensimmäisessä vaiheessa.

3. Kolmannessa vaiheessa autentikaattori lähettää uuden pyynnön (Identity/Request) ja asiakas vastaa tähän samaan tapaan kuin toisessa vaiheessa. Tätä jatkuu siihen asti, kun tarve vaatii. RFC 3748 (2004, 8) käyttää ”lock-step”-nimitystä EAP-protokollasta eli se ei laita uutta pyyntöä ennen kuin se on saanut kelvollisen vastauksen edeltävään pyyntöön. Tarvittavan dialogin jälkeen autentikaattorin tulisi lopettaa EAP-kanssakäyminen. Standardissa painotetaan, että autentikaattori ei saa lähettää Success- tai Failure-pakettia, mikäli se ei vastaanota Response-pakettia tai vastaavasti Response <-> Request dialogin ollessa kesken.

4. Mikäli autentikoitavana oleva laite ei pysty vastaamaan tarvittavilla tiedoilla autentikaattorin Request- tai Response-paketteihin päättyy keskustelu EAP-protokollassa esiintyvään koodiin 4 (EAP-Failure). Koodi 4 tarkoittaa EAP-tavassa epäonnistunutta autentikointia. Laitteen pystyessä vastaamaan kelvollisesti autentikaattorin esittämiin pyyntöihin päättyy keskustelu koodiin 3 (EAP-Success), mikä tarkoittaa todennuksen onnistumista.



Kuvio 3. Kuvankaappaus Wireshark-ohjelmasta, jossa näkyy onnistunut todentaminen PEAP-EAP-TLS-metodilla.

4.1.1 EAP-Request

EAP-Request-paketilla tarkoitetaan asiakkaalle autentikaattorilta lähtevää EAP-pakettia. Paketti sisältää EAP-metodidataa autentikointipalvelimelta asiakkaalle. EAP-Request-pakettia voidaan myös käyttää autentikaattorin pyytäessä asiakkaan tunnistetietoja riippuen käytössä olevasta EAP-metodista. (Geier 2008, 290.)

4.1.2 EAP-Response

EAP-Response-paketilla tarkoitetaan pakettia, jonka asiakas lähettää autentikaattorille, silloin kun autentikaattori on pyytänyt esim. EAP-metodidataa tai tunnistetietoja (Geier 2008, 290-291).

4.1.3 EAP-Success

EAP-Success-paketilla tarkoitetaan EAP-metodin pohjalta saatua lopputulosta, jonka autentikaattori lähettää asiakkaalle, mikäli autentikointipalvelin on vahvistanut ja hyväksynyt asiakkaan tunnistetiedot. EAP-Success-paketti indikoi sitä, että pääsy suojattuun verkkoon voidaan sallia asiakkaalle. (Geier 2008, 291.)

4.1.4 EAP-Failure

EAP-Failure-paketilla tarkoitetaan päinvastaista lopputulosta EAP-Success-pakettiin verratessa. EAP-Failure-paketti, jonka autentikaattori toimittaa asiakkaalle kertoo sen, että asiakkaalla ei ole pääsyä suojattuun verkkoon, koska sillä ei ole oikeutta liittyä siihen. (Geier 2008, 287.)

4.2 EAP-TLS (EAP with Transport Layer Security)

EAP-TLS on sertifikaattipohjainen autentikointiprotokolla, joka tarvitsee toimiakseen asiakaspuolen sertifikaatin ja palvelinpuolen sertifikaatin, joiden avulla molemmat osapuolet autentikoivat toisensa. Microsoftin (2012) mukaan EAP-TLS-metodi takaa vahvimman autentikoimismuodon.

Protokolla muodostaa kryptatun TLS-tunnelin asiakkaan ja autentikointipalvelimen välille, jonka avulla yhteyden turvallisuus on taattu. Kyseistä protokollaa voidaan parhaiten hyödyntää yrityksissä, jotka ovat jo ottaneet käytteen digitaaliset sertifikaatit Windows-pohjaisissa työasemissa tai mobiililaitteissa. (Geier 2008, 109.)

Geier (2008, 110) jakaa EAP-TLS-metodin käyttämän autentikointiprosessin kuuteen eri osaan:

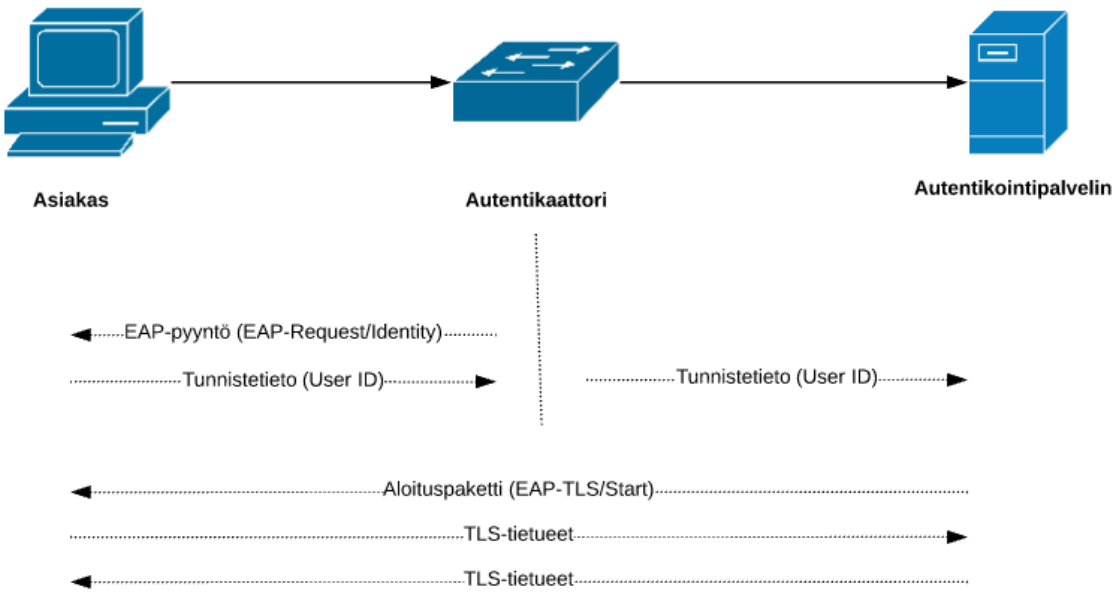
1. Autentikaattori lähettää asiakkaalle EAP-Request/Identity-paketin
2. Asiakas vastaa lähettämällä EAP-Response/Identity-paketin autentikaattorille, paketti sisältää asiakkaalle kuuluvan tunnisteen (User ID).

3. Autentikaattori lähettää asiakkaalta saadun tunnisteen eteenpäin autentikointipalvelimelle.

4. Autentikointipalvelin jatkaa todentamista lähettämällä EAP-TLS/Start-paketin.

5. Asiakas lähettää EAP-Response paketin, jonka tyyppinä on EAP-TLS. Paketin datakentässä on yksi tai useampi TLS-tietue.

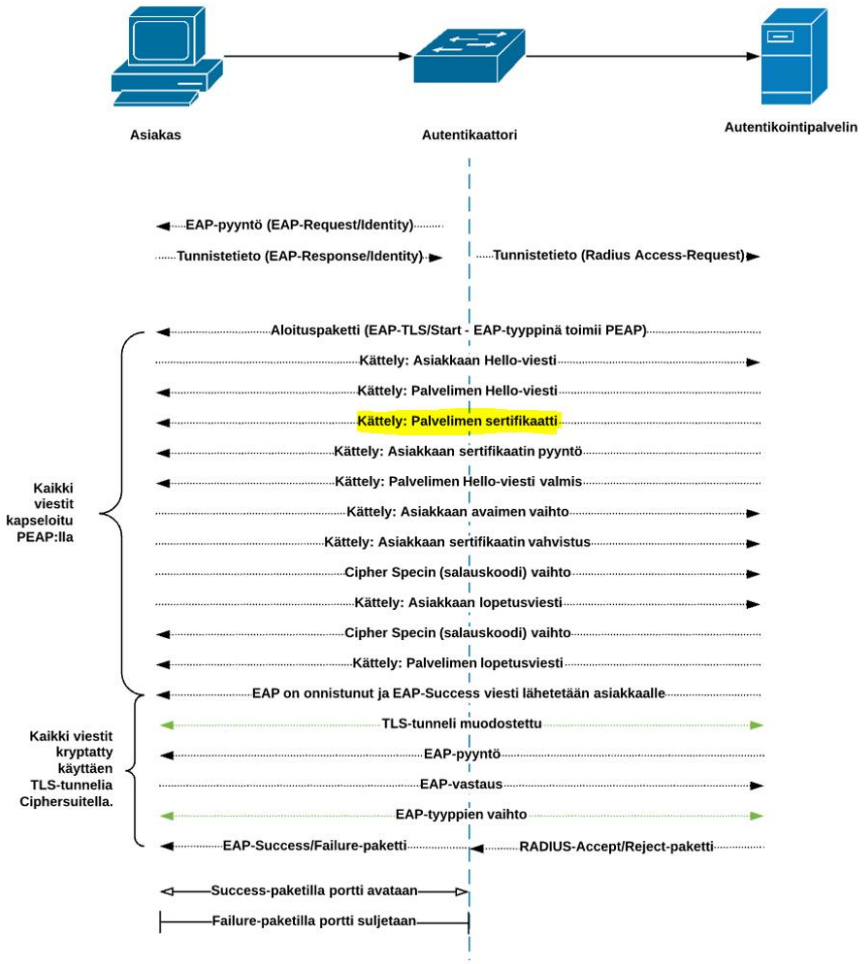
6. Autentikointipalvelin vastaa tähän EAP-Response-pakettiin lähettämällä EAP-Request-paketin, jonka tyyppinä toimii EAP-TLS. Tässä paketissa on samaan tapaan kuin vaiheessa 5 yksi tai useampi TLS-tietue.



Kuvio 4. EAP-TLS-toimintakuva.

4.3 PEAP ja PEAP-EAP-TLS

PEAP eli Protected Extensible Authentication Protocol tarkoittaa protokollaa, joka kapseloi EAP-protokollan sisäänsä ja tunneloi liikenteen käyttämällä TLS-tapaa eli Transport Layer Securityä. PEAP-protokollassa käytetään hyödyksi yhtenäistä autentikoimista, jossa molemmat osapuolet autentikoivat toisensa käyttämällä palvelimelta löytyvää sertifikaattia. Liikenne TLS-tunnelin sisällä on kryptattua, joten pakettikohtaisesti turvallisuus on parempi kuin pelkässä EAP-protokollassa. (Palekar ym. 2003, 2, 5.)



Kuvio 5. EAP-PEAP-tavan toimintakuva

PEAP luotiin paikkaamaan EAP-protokollassa ilmenneitä puutteita, jotka Palekar ym. (2003, 3-4) ovat jakaneet kahdeksaan eri osaan:

1. Tunnisteiden turvallisuus on parantunut, koska PEAP salaa (kryptaa) heti aluksi identiteetin vaihtotapahtuman.

2. Sanakirjahyökkäyksiä vastaan PEAP auttaa TLS-tunnelin avulla, sillä osa EAP-metodeista on alttiita joutumaan sanakirjahyökkäysten kohteeksi erityisesti silloin, kun ollaan ns. offline-tilassa eli irti verkosta. PEAP-protokollaa käytettäessä tämä estetään.

3. Turvallisempi neuvottelu laitteiden välillä, koska PEAP:n avulla EAP-dialogi on autentikoitu molempien osapuolten kohdalta ja se käydään TLS-tunnelin sisällä.

4. Header protection eli otsikkotunnisteiden turvallisuus on parantunut PEAP:n avulla samasta syystä kuin osassa 3. PEAP-protokollassa käytetty TLS-tunneli, jossa EAP-dialogia työstetään, on turvattu eikä tunnisteisiin voida tehdä muutoksia.

5. Suojattu lopetus TLS-tunnelin sisällä (kryptatut success-/failure-paketit) parantaa tietoturvaa palvelunestohyökkäyksiä vastaan, koska haitantekoon pyrkivät entiteetit eivät voi väärentää EAP-paketteja, sillä tarvittavat tiedot esim. EAP-Failure-paketin väärentämiseen eivät ole saatavilla. Kaikki siihen liittyvä materiaali on suojatussa TLS-tunnelissa.

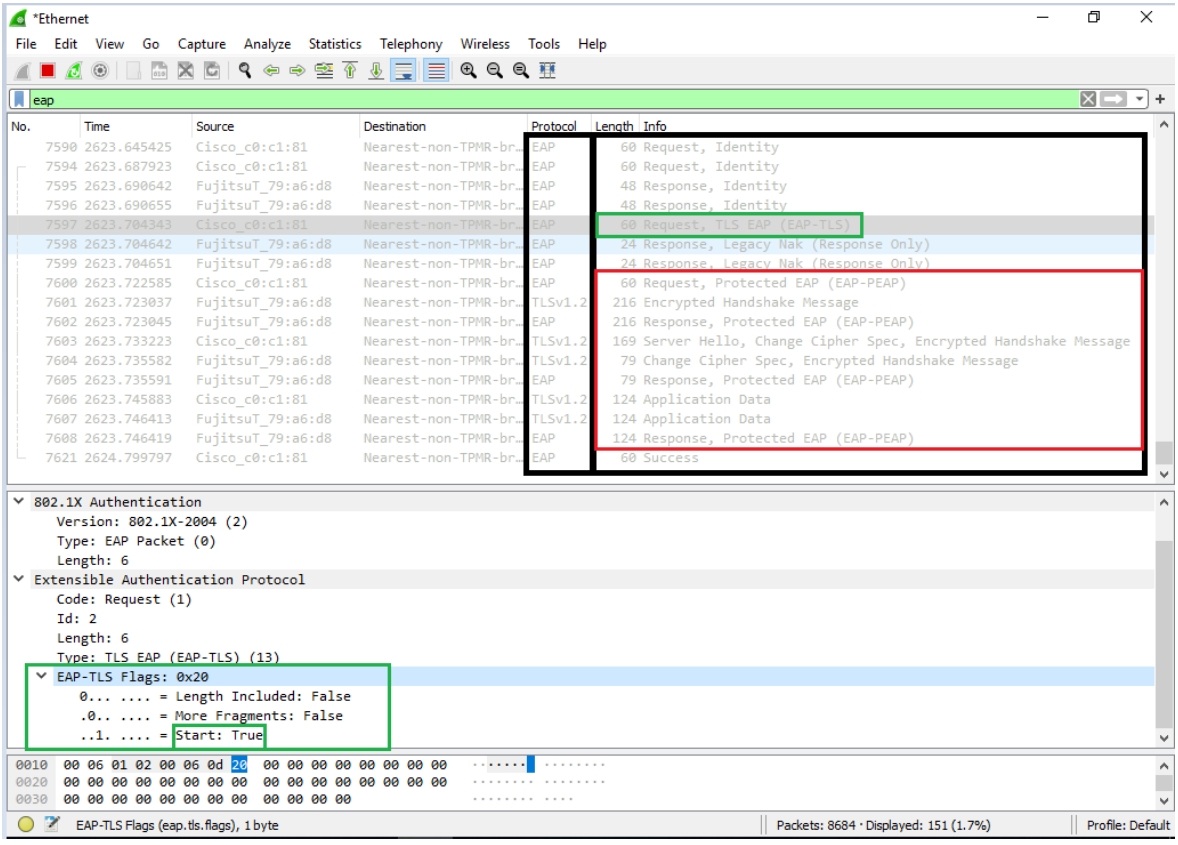
6. Sirpaloituminen ja uudelleenkokoaminen eivät ole EAP-protokollassa tuettuja, mutta PEAP:n avulla molempia tekniikoita voidaan hyödyntää sisällyttämällä ne suoraan PEAP-tapaan.

7. Nopea uudelleen yhdistäminen langattomien verkkojen kohdalla on erityisesti digitalisaation aikana välttämättömyys. Tämän vuoksi viiveestä eli latenssista aiheutuu ongelmia, mikäli uudelleen yhdistämistä ei voida suorittaa nopeasti. PEAP:n avulla tätä voidaan kuitenkin parantaa, koska PEAP tukee TLS-istunnon jatkamista riippumatta käytetystä EAP-metodista PEAP:n sisällä.

8. Todistetusti itsenäinen avaimienhallinta metodista riippumatta. PEAP-protokollassa käytetty TLS huolehtii avaimien derivaatiometodeista, jotka joudut-

taisiin ilman TLS-protokollaa tekemään EAP-metodin mukaan erikseen. Tämän mainitaan olevan todella monimutkaista ja haastavaa, joten TLS:n hyödyntäminen avaimien kanssa auttaa estämään mies välissä -hyökkäyksiä vastaan.

PEAP-EAP-TLS toimii muuten samalla tapaa kuin EAP-TLS, mutta PEAP-EAP-TLS aloittaa kryptauksen ja TLS-tunneloinnin kuviossa 5 esitetystä korostetusta kohdasta.

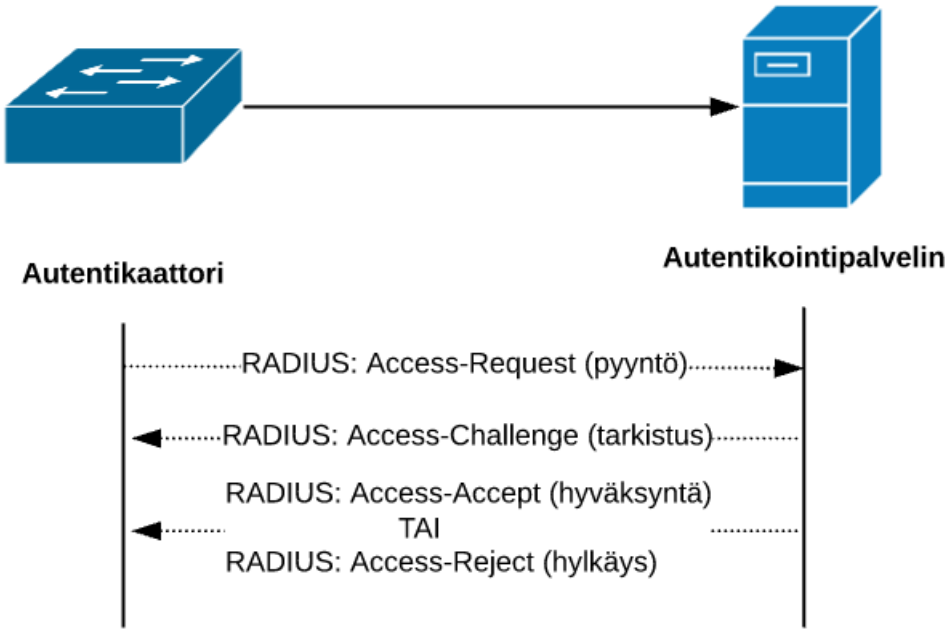


Kuvio 6. PEAP-EAP-TLS-tavan koko keskusteluketju työaseman näkökulmasta.

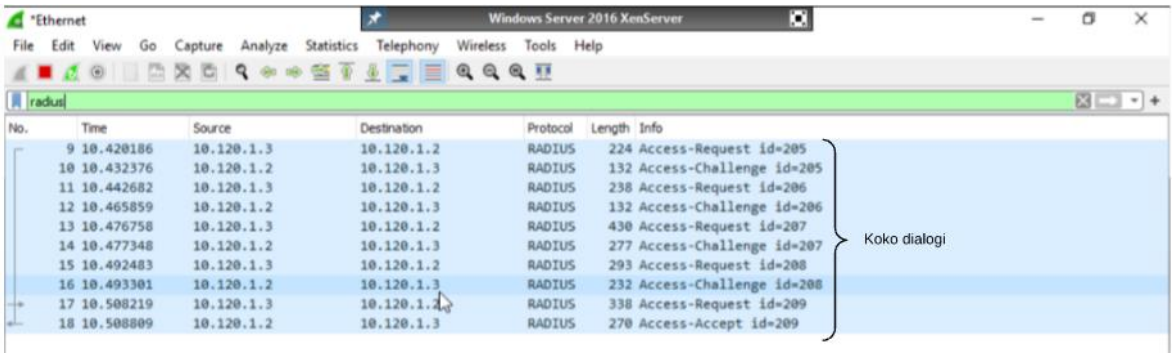
4.4 RADIUS (Remote Authentication Dial-In User Service)

Remote Authentication Dial-In User Service eli RADIUS toimii kommunikointimenetelmänä autentikaattorin ja autentikointipalvelimen välillä, kun puhutaan porttikohtaisesta autentikoimisesta. RADIUS-protokollat kuljettavat EAP-metodidataa sala-

tussa (kryptatussa) muodossa laitteiden välillä. Autentikaattori lähettää EAP-metodidatan autentikointipalvelimelle RADIUS Access-Request -kehyksen avulla ja autentikointipalvelin taasen lähettää EAP-metodidataa autentikaattorille RADIUS Access-Challenge -pakettien avulla. (Geier 2008, 302.)



Kuvio 7. Autentikointipalvelimen ja autentikaattorin välinen dialogi.



Kuvio 8. Autentikointipalvelimen näkökulma koko RADIUS-keskustelusta.

4.4.1 RADIUS Access-Request

RADIUS Access-Request -paketilla tarkoitetaan autentikaattorin lähettämää viestiä autentikointipalvelimelle, mikä voi sisältää esim. asiakkaan tunnistetietoja. Riippumatta käytössä olevasta EAP-metodista tulee kyseinen paketti lähettää autentikointipalvelimelle, jotta asiakas voidaan autentikoida. (Geier 2008, 303.)

4.4.2 RADIUS Access-Challenge

RADIUS Access-Challenge -paketilla tarkoitetaan palvelimelta lähtöisin olevaa vastausta autentikaattorin esittämälle Access-Request-paketille. Access-Challenge-paketissa olevan tunnisteen tulee täsmätä Access-Request-paketissa olevan tunnisteen kanssa. (Geier 2008, 302-303.)

4.4.3 RADIUS Access-Accept

RADIUS Access-Accept -paketti on myös autentikointipalvelimelta lähtöisin oleva paketti, jonka autentikointipalvelin lähettää vastauksena RADIUS Access-Request -paketille. Yleisesti ottaen tämä paketti on koko ketjun viimeinen paketti, sillä se kertoo autentikaattorille, mikäli asiakas voidaan päästää suojattuun verkkoon. Olennaista paketille on myös se, että siinä olevan tunnisteen tulee täsmätä siihen tunnisteeseen, joka vastaa RADIUS Access-Request -pakettia, johon kyseinen RADIUS Access-Accept -paketti vastaa. (Geier 2008, 302-303.)

4.4.4 RADIUS Access-Reject

RADIUS Access-Reject -paketti toimii vastakohtana RADIUS Access-Accept -paketille. Reject-paketti ilmaisee autentikaattorille sen, että jotkin asiakkaan antamista tunnistetiedoista, jotka löytyvät RADIUS Access-Request-paketista, eivät täsmää tai ne eivät ole kelvollisia. Samaan tapaan täytyy tunnistetiedon täsmätä Request-pakettiin. Reject-paketin avulla on mahdollista ilmaista syy miksi asiakasta ei voitu au-

tentikoida välittämällä asiakkaalle tekstimuotoinen viesti hyödyntämällä Reject-paketin Reply-Message-attribuuttikenttiä, joita tyypillisesti löytyy yhdestä pariin kappaleeseen per paketti. Reply-Message-attribuuttikentästä löytyy syy siihen, miksi autentikointi on epäonnistunut, kuten sertifikaatin puuttuminen laitteelta. (Geier 2008, 303.)

5 TOTEUTUS

Testiympäristö luotiin Seinäjoen ammattikorkeakoulun luokan A350.3 yhteydessä olevaan välitilaan, josta löytyi jo valmiiksi asennettu ja koottu räkkikaappi. Räkkikaappiin oli asennettu Fujitsun RX200 S7 fyysinen-palvelin. Palvelimelle oli asennettuna Citrix XenServer, joka on avoimeen lähdekoodiin perustuva palvelinten virtualisointialusta. XenServerin tarkoituksena on mahdollistaa useiden eri virtuaalisten palvelinten asennus, ylläpito ja käyttö. XenServerille oli valmiiksi asennettuna Windows 2016 Server -käyttöjärjestelmä, josta poistettiin kaikki roolit ja ominaisuudet ennen toteutuksen aloittamista. Työasemien tai palvelimen liittämistä toimialueelle ei käsitellä tässä opinnäytetyössä.

Windows 2016 Server -käyttöjärjestelmän lisäksi työssä käytettiin kolmea testityöasemaa, joihin asennettiin Windows 10 -käyttöjärjestelmä. Työasemien lisäksi työssä käytettiin yhtä Ciscon 2960-sarjan kytkintä ja Ciscon 1800-sarjan reititintä.

Kuvio 9. Testiympäristö ylhäältä alas: kytkin, reititin ja palvelin.

5.1 Verkkomääritykset ja topologia

Työssä tähdättiin kolmeen eri aliverkkoon jaettuun ratkaisuun, jonka avulla pystyttiin testaamaan niin NPS-palvelimelta (Network Policy Server) saatuja attribuutteja ja DHCP:n (Dynamic Host Configuration Protocol) toimintaa silloin, kun kaikki roolit ja ominaisuudet on sijoitettu yhdelle palvelimelle.

IP-avaruus jaettiin kolmeen eri virtuaalilähiverkkoon (VLAN), joista VLAN 10 kuului IT-osastolle, VLAN 20 toimistolle ja VLAN 30 tuotannolle. IP-osoitteet jaettiin DHCP-palvelimelta ainoastaan työasemille, ja kiinteät IP-osoitteet määriteltiin palvelimelle ja kytkimelle. Kytkimen IP-osoitteeksi annettiin 10.120.1.3 ja palvelimen IP-osoitteeksi 10.120.1.2. Reitittimelle luotiin reitityssäännöt kaikille kolmelle vlanille ja reititin kytkettiin kytkimen porttiin 24. Palvelin kytkettiin kytkimen porttiin 10 ja työasemat portteihin 1 – 3.

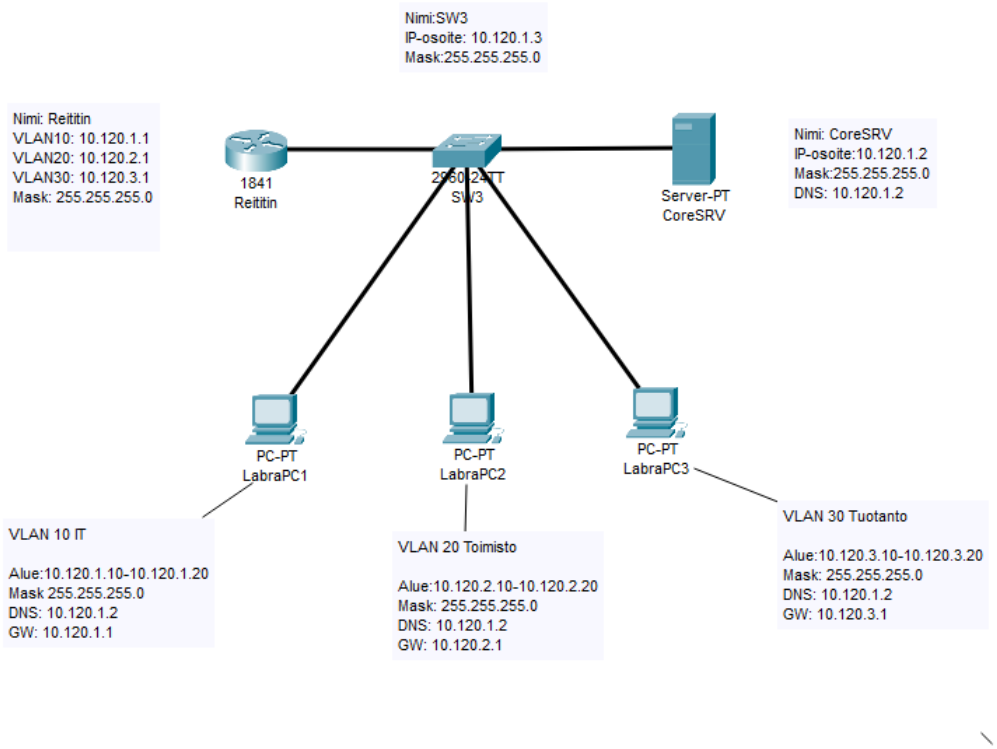
Virtuaalilähiverkon IP-avaruus jaettiin kolmeen eri C-luokkaan:

1. VLAN 10 IT – 10.120.1.0 Maski: 255.255.255.0
2. VLAN 20 Toimisto – 10.120.2.0 Maski: 255.255.255.0
3. VLAN 30 Tuotanto – 10.120.3.0 Maski: 255.255.255.0

```
SW3#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Gi0/1, Gi0/2
10   IT                               active    Fa0/10
20   Toimisto                         active
30   Tuotanto                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Kuvio 10. Kuvankaappaus kytkimen virtuaalilähiverkoista.



Kuvio 11. Testiympäristön verkkotopologia.

5.2 Palvelimen roolien asennukset

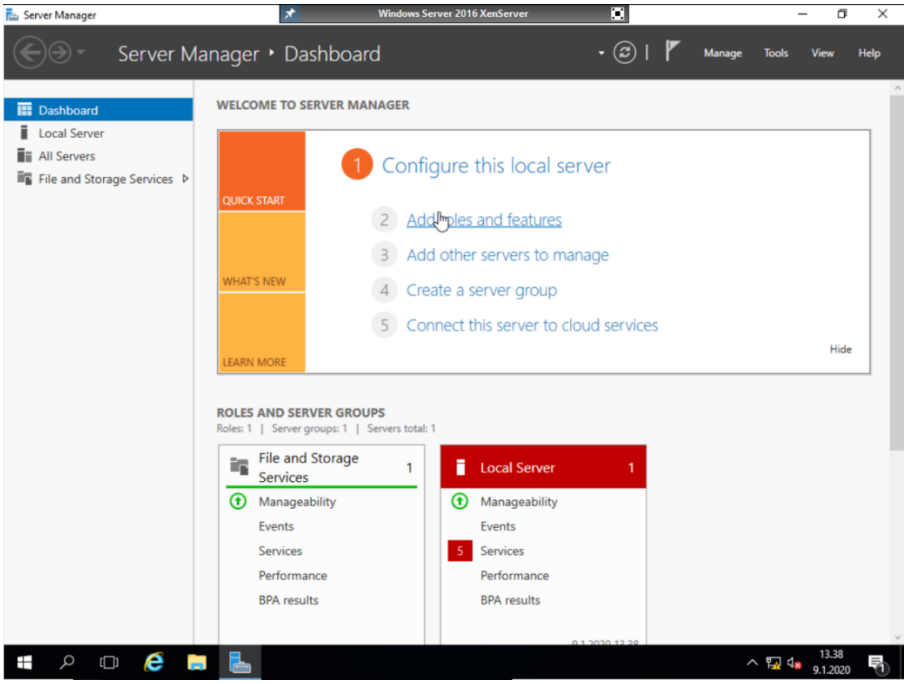
Palvelimelle asennetuista rooleista käydään läpi AD eli Active Directory, CS eli Certificate Services ja NPS eli Network Policy Server. Opinnäytetyössä käytettävä DHCP-rooli on konfiguroitu sillä periaatteella, että jokaisesta aliverkosta on mahdollista jakaa IP-osoitteita 10 kappaletta alkaen osoitteesta 10, esimerkiksi 10.120.1.10 – 10.120.1.20. DNS-roolille ei ole tehty mitään muutoksia, vaan sen asennus on tullut aktiivihakemiston asennuksen mukana.

5.2.1 Active Directory

Aktiivihakemiston eli Active Directoryn ja ryhmäkäytännön eli Group Policyn avulla voidaan hallinnoida toimialueeseen kuuluvia laitteita ja käyttäjiä keskitetysti. Tässä

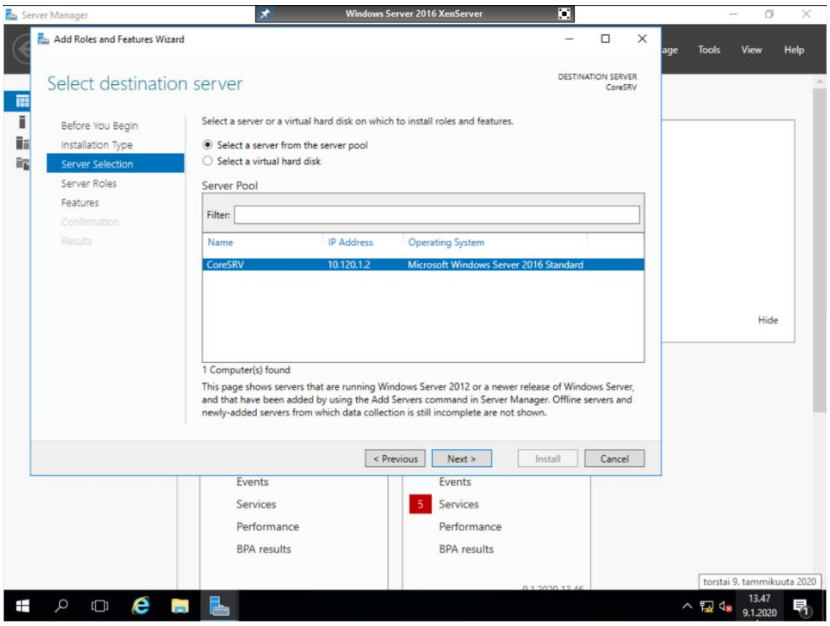
opinnäytetyössä aktiivihakemistoa ja ryhmäkäytäntöä käytetään työasemille ja palvelimille asennettavien sertifikaattien jakamiseen ja työasemien kohdalla verkkoadapterin asetusten muuttamiseen.

Asennus alkaa klikkaamalla palvelimella olevasta Server Manager -sovelluksesta **Add Roles and Features** -valikkoa.



Kuvio 12. Roolin lisäys Windows Server 2016 -järjestelmässä

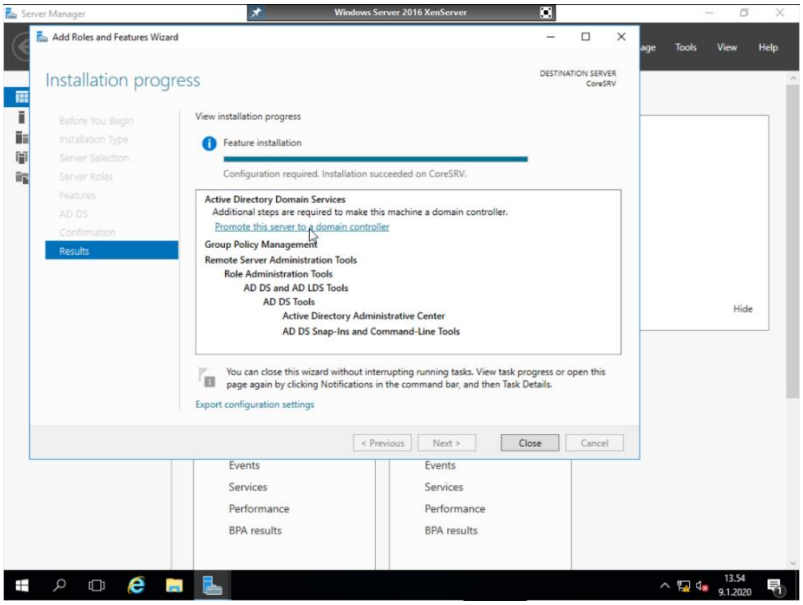
Before You Begin -välilehdeltä voidaan siirtyä suoraan **Next**-näppäintä painamalla seuraavalle välilehdelle. **Installation Type** -välilehdeltä valitaan **Role-based or feature-based installation**, jonka jälkeen klikataan **Next**. **Server Selection** -välilehdeltä tarkistetaan, että palvelin, jolle roolia ollaan asentamassa, on oikea. (Microsoft 2017a.) Tässä opinnäytetyössä se on **CoreSRV**.



Kuvio 13. AD-palvelimen valinta.

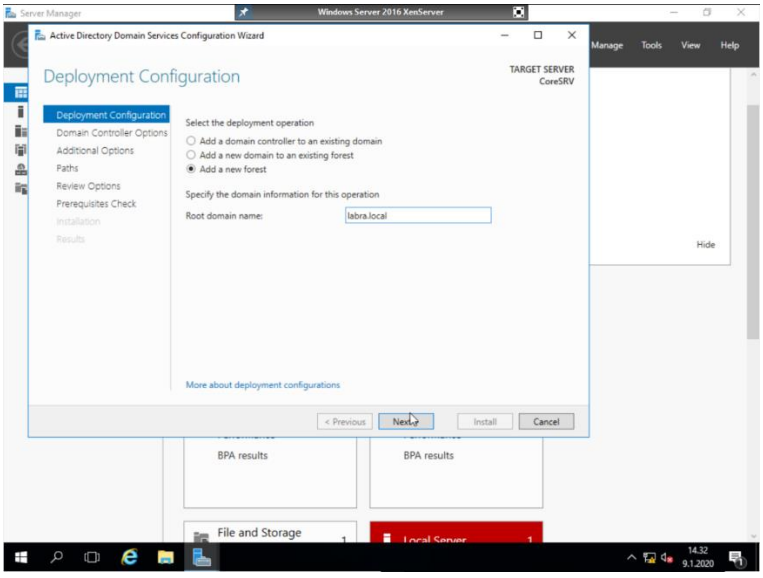
Server Roles -välilehdeltä valitaan **Active Directory Domain Services** -rooli ja klikataan se aktiiviseksi. Klikkaus luo uuden dialoginäkymän, jossa kysytään asennetaanko seuraavat ominaisuudet, ja hyväksytään valinta **Add Features** -painikkeella. Seuraaviin kohtiin ei tarvitse tehdä mitään muutoksia, joten voidaan mennä oletuksilla **Confirmation**-välilehdelle saakka. Klikkaamalla **Install**-painiketta päästään asentamaan aktiivihakemisto. Onnistuneen asennuksen jälkeen aukeaa viimeinen

välilehti **Results**, josta klikataan **Promote this server to a domain controller** -painiketta, jotta saadaan tehtyä palvelimesta toimialueenohjain. (Microsoft 2017a.)



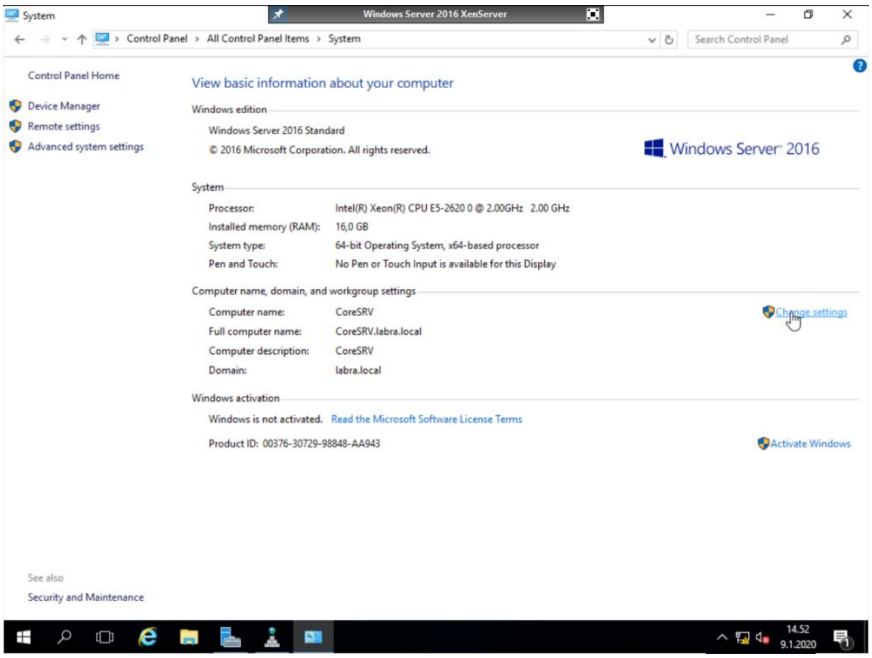
Kuvio 14. AD:n korottaminen toimialueenohjaimeksi.

Ennen kuin palvelimesta on tullut toimialueenohjain aukeaa uusi ikkuna välilehdelle **Deployment Configuration**. Siinä kysytään, minkälainen käyttöönotto on kyseessä. Kyseessä uusi palvelin, joten luodaan uusi toimialue, jolle annetaan nimeksi labra.local ja klikataan **Next.**



Kuvio 15. Uusi toimialue labra.local.

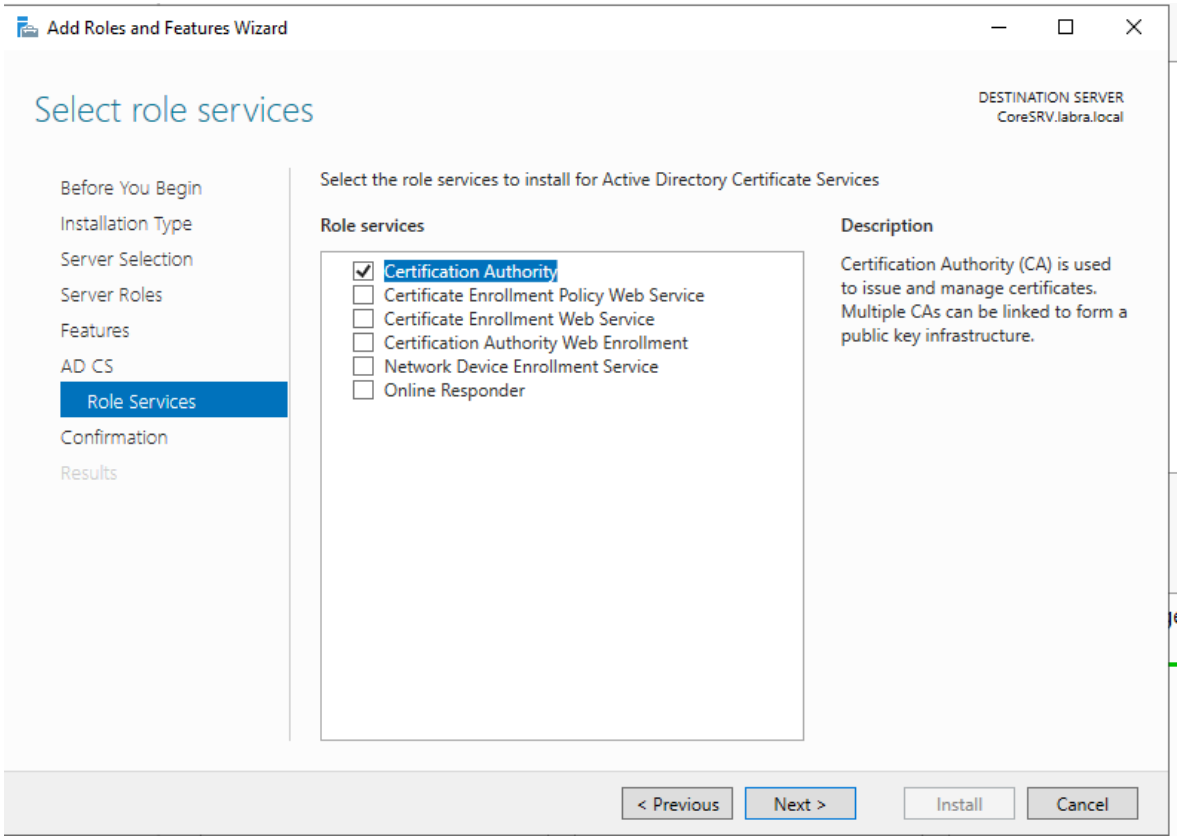
Domain Controller Options -välilehdellä asetetaan salasana hakemistonpalveluiden palautustilaa varten ja klikataan **Next** tähän ja kaikille seuraaville välilehdille. Aktiivihakemiston asennus on valmis ja palvelin voidaan liittää toimialueelle. (Microsoft 2017a.)



Kuvio 16. Palvelin liitettynä toimialueelle.

5.2.2 Certificate Services

Saman kaavan mukaan suoritetaan asennus Certificate Services eli sertifikaattipalveluille. Roolin lisäämisessä tehdään kuitenkin yksi muutos AD CS -välilehdellä sijaitsevassa alivälilehdessä **Role Services**, josta valitaan ainoastaan **Certification Authority** -palvelu**.** Muut kohdat voidaan mennä oletuksilla ja painamalla **Next**-painiketta. (Microsoft 2019e.)



Kuvio 17. Oikean roolipalvelun valinta.

Asennuksen jälkeen huomataan, että **Server Manager** -ikkunassa on tullut kolmio oikeaan yläkulmaan ilmoitusvalikon painikkeen päälle. Avaamalla ilmoitukset ja klikkaamalla **Configure Active Directory Certificate Services on the destination server** päästään tekemään tarvittavat muutokset sertifikaatteja varten. (Microsoft 2019e.)

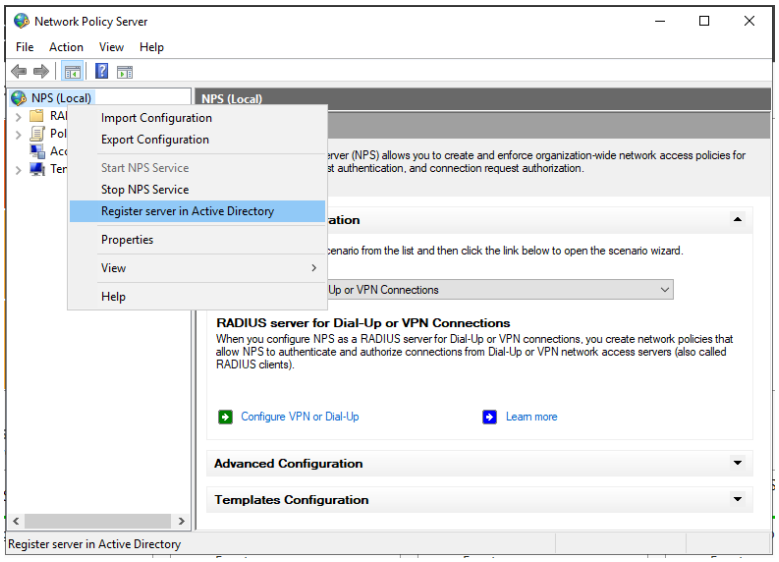
Ensimmäiselle välilehdelle ei tarvitse tehdä muutoksia, joten voidaan jatkaa painamalla **Next,** ja siirtymällä **Role Services**-välilehdelle, josta valitaan taas **Certification Authority** ja klikataan **Next**, koska kyseessä on verkkoratkaisuun kohdistuva sertifikaattien käyttö, valitaan **Enterprise CA** ja siirrytään **Next**-painikkeella eteenpäin. (Microsoft 2019e.)

Seuraavalla välilehdellä pyydetään sertifikaattien tyyppiä, josta valitaan **Root CA**, koska käytössä on yksi palvelin eikä riippuvuuksia muihin palvelimiin ole. Seuraavaan kahteen välilehteen ei tarvitse tehdä muutoksia, mutta tässä opinnäytetyössä **CA Name**-välilehdellä on **Common name for this CA** muutettu muotoon **LABRA Issuing CA** selvyyden parantamiseksi. Seuraavat kohdat voidaan mennä oletuksilla

ja suorittaa asennus loppuun **Confirmation**-välilehdeltä painamalla **Configure**-painiketta, jonka jälkeen sertifikaattiroolin asennus on valmis. (Microsoft 2019e.)

5.2.3 Network Policy Server

NPS:n asennus suoritetaan oletuksilla, eikä muutoksia tarvitse tehdä. Asennuksen jälkeen tulee kuitenkin avata asennettu rooli ja liittää se aktiivihakemistoon. Tämä tehdään siirtymällä **Server Manager** -sovelluksesta **Tools**-valikkoon ja avaamalla **Network Policy Server**. Tämän jälkeen NPS:n liittäminen aktiivihakemistoon voidaan suorittaa painamalla hiiren vasemmalla painikkeella **NPS (local)** -painiketta ja valitsemalla **Register server in Active Directory**. (Microsoft 2018a.)



Kuvio 18. NPS:n liittäminen aktiivihakemistoon.

5.3 Palvelimen roolien asetukset

Palvelimen rooleille tehtäviä määrityksiä tehdään tässä opinnäytetyössä kaikkiin kolmeen asennettuun rooliin. Opinnäytetyön ulkopuolelle jätetään ryhmien luominen aktiivihakemistoon ja työasemien liittäminen toimialueelle. Työasemia varten on luotu kolme eri ryhmää, joista jokaiseen liitetään yksi kone. VLAN10 IT -ryhmään on lisätty työasema LabraPC1, VLAN 20 Toimisto -ryhmään on lisätty LabraPC2 ja

VLAN30 Tuotanto -ryhmään on lisätty LabraPC3. Ryhmäkäytäntöön tehdyt muutokset kohdistetaan kaikkiin toimialueen työasemiin, koska kyseessä on testiympäristö.

5.3.1 Certificate Services

Sertifikaatteja PEAP-EAP-TLS-tavassa tarvitaan kaksi. Toinen sertifikaatti sijoitetaan työasemalle ja toinen palvelimelle. PEAP-EAP-TLS tai PEAP with EAP-TLS autentikoi molemmat osapuolet tietoturvan parantamisen ja eheyden säilyttämisen vuoksi uniikeilla sertifikaateilla. Microsoft (2019d) on jakanut työasemalle sijoitetun sertifikaatin vaatimukset kahdeksaan eri osa-alueeseen:

1. Sertifikaatin myöntäjänä on toiminut yrityksen CA. CA -roolipalvelulla tarkoitetaan entiteettiä, joka vastaa digitaalisten sertifikaattien jakamisesta.

2. Käyttäjä- tai tietokonesertifikaatin ketjutus kulkee luotettuun CA-myöntäjään asti.

3. Sertifikaatti omaa Client Authentication toiminnon eli sertifikaatti on luotu oikeaan tarkoitukseen.

4. Sertifikaatti suoriutuu CryptoAPI:n suorittamista tarkistuksista.

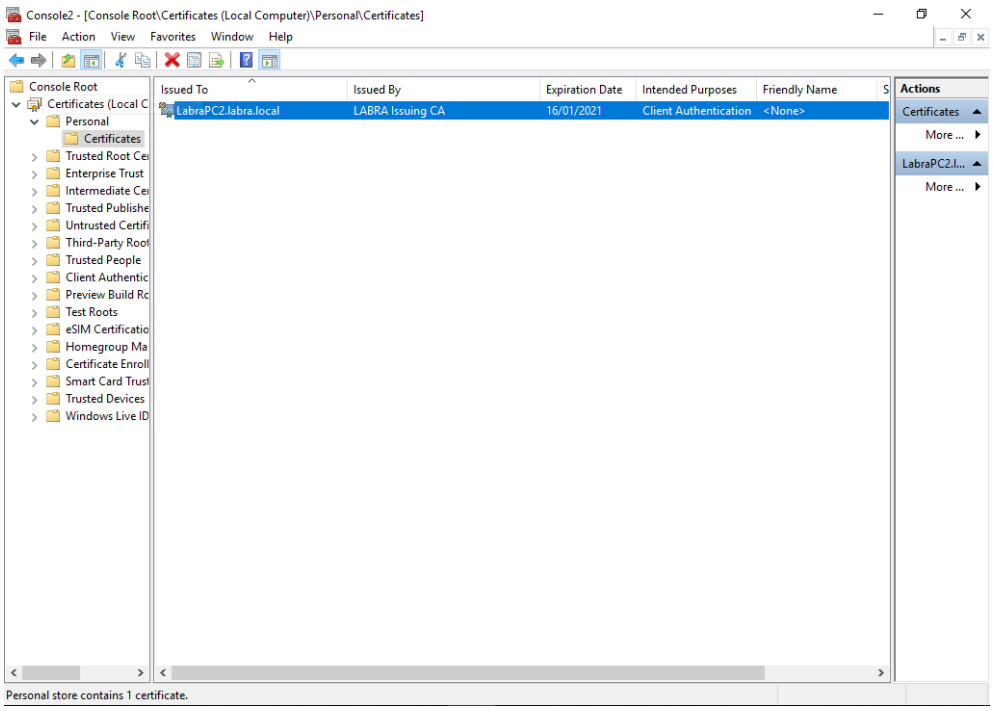
5. Sertifikaatti selviytyy IAS:n suorittamista tarkistuksista koskien sertifikaattiobjektitunnisteita.

6. 802.1X-asiakas ei käytä rekisteripohjaista älykorttia tai rekisteripohjaista salasanalla suojattua sertifikaattia.

7. Subject Alternative Name -laajennus (toissijainen nimi) sertifikaatissa sisältää käyttäjän alkuperäisen nimen.

8. Asiakkaiden käyttäessä EAP-TLS- tai PEAP-EAP-TLS-autentikointia, lista kaikista asennetuista sertifikaateista tulee olla näkyvillä mmc-työkalussa eli Microsoft Management Consolessa lukuun ottamatta langattomien asiakkaiden rekisteripohjaisia sertifikaatteja tai älykorttikirjautumiseen käytettyjä sertifikaatteja, langattomien ja VPN-yhteyttä käyttävien asiakkaiden salasanalla

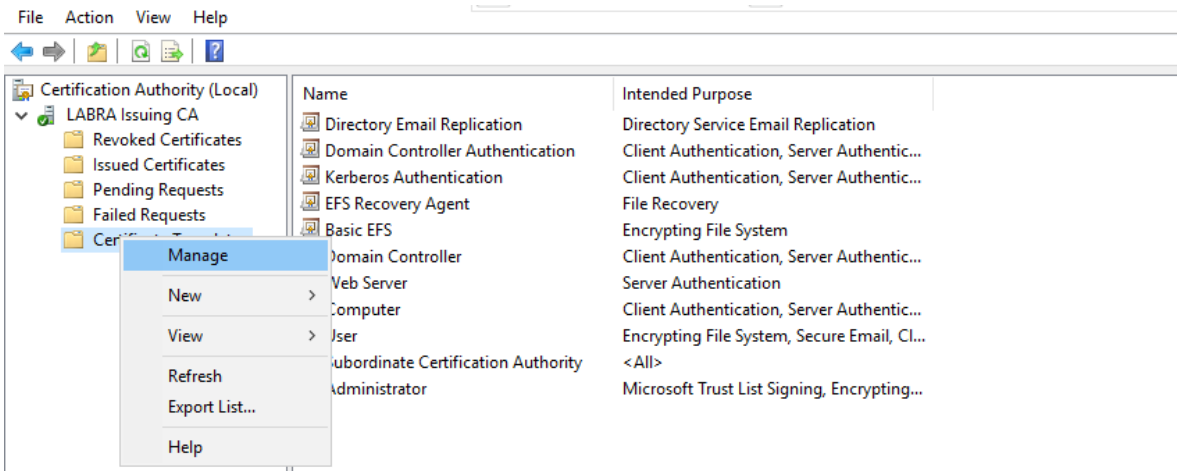
suojattuja sertifikaatteja tai sertifikaatteja, jotka eivät sisällä EKU-laajennuksen omaavaa Client Authentication -sertifikaattia.



Kuvio 19. Työasemalta otettu kuvankaappaus asiakkaan sertifikaatista MMC-työkalusta.

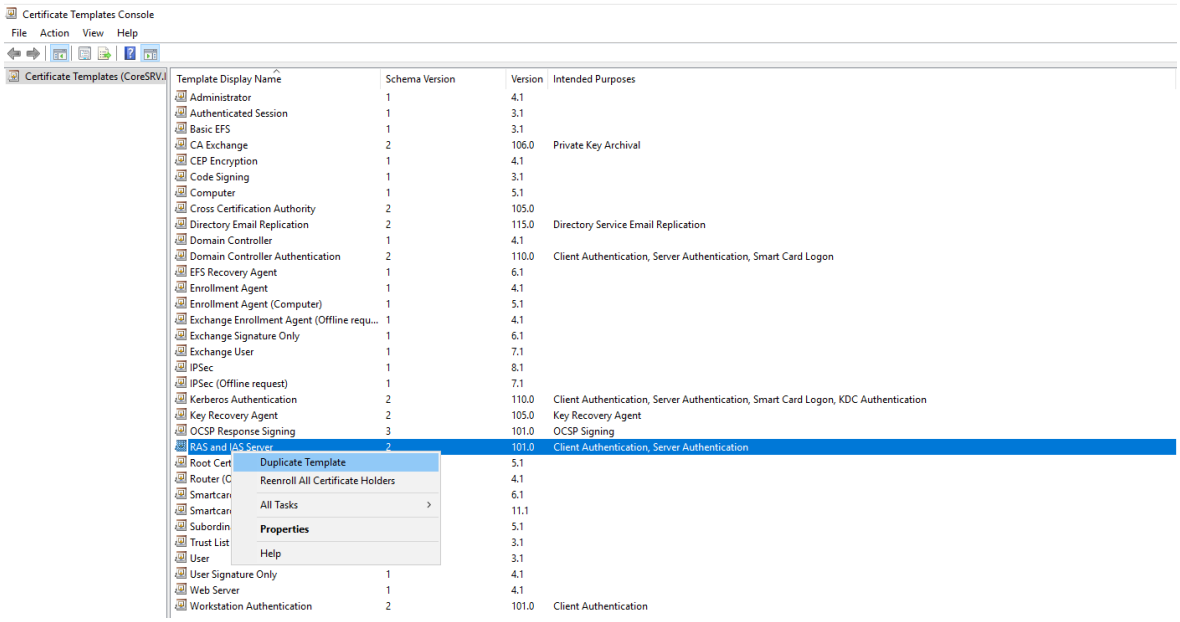
PEAP-EAP-TLS-tavan käyttöönotossa tarvitaan kaksi eri sertifikaattia. Ensimmäinen jaetaan NPS-palvelimelle, jolla se tunnistautuu työasemalle, ja toinen sertifikaatti jaetaan työasemille, joilla työasemat tunnistautuvat NPS-palvelimelle. NPS-palvelimella on käytössä RAS- ja IAS-palvelinten sertifikaatti, jota käytetään yleisesti 802.1X-protokollan porttikohtaisen autentikoinnin toteutuksessa. (Microsoft 2019a.)

Tässä opinnäytetyössä viitataan RAS ja IAS-sertifikaattiin Radius-sertifikaattina. Sertifikaatti luodaan siirtymällä **Certification Authority**-roolille klikkaamalla **Server Manager** -sovelluksesta **Tools**-valikkoa ja valitsemalla **Certification Authority**. Avautuneesta ikkunasta voidaan hallinnoida Microsoftin sertifikaattipohjia klikkaamalla **Certificate Templates** -kansiota hiiren oikealla painikkeella ja valitsemalla **Manage**. (Microsoft 2019f.)



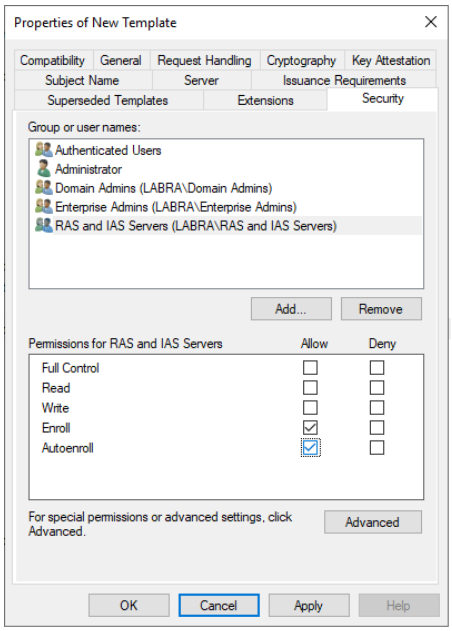
Kuvio 20. Sertifikaattipohjien hallinta.

Certificate Template Console -ikkunasta valitaan **RAS and IAS Server** ja klikataan hiiren oikealla painikkeella ja valitaan **Duplicate Template** (Microsoft 2019f).



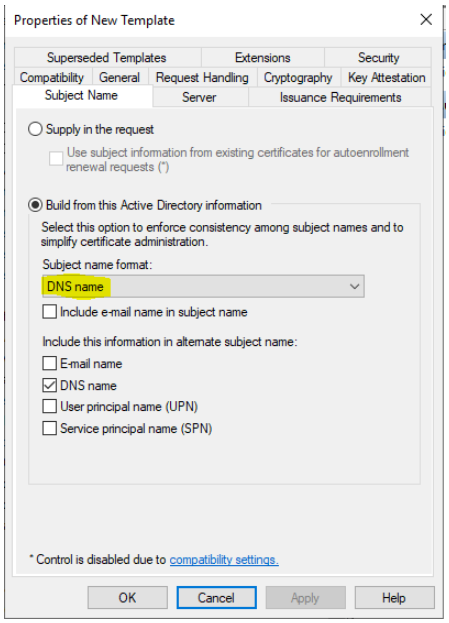
Kuvio 21. Radius-sertifikaatin luonti.

Pohjan ominaisuuksista käydään vaihtamassa pohjan nimi **General**-välilehdeltä muotoon **Radius Server Certificate**, jonka jälkeen käydään **Security**-välilehdellä antamassa oikeudet automaattiseen jakeluun valitsemalla **RAS and IAS Servers** -ryhmä, johon palvelin kuuluu ja laittamalla **Allow** aktiiviseksi **Autoenroll**-oikeuksien kohdalta. Tämän jälkeen muutokset voidaan hyväksyä painamalla **OK**. (Microsoft 2019f.)



Kuvio 22. Oikeudet kuntoon palvelimelle.

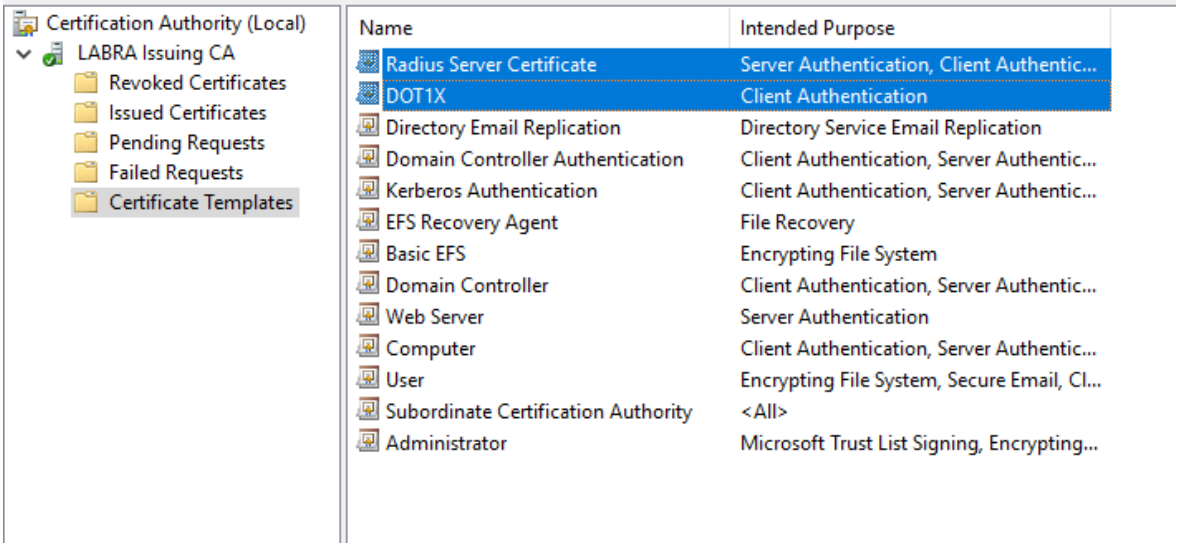
Samalla luodaan asiakkaan käyttöön tuleva sertifikaatti valitsemalla samaan tyyliin hiiren oikealla klikkauksella **Workstation Authentication** -pohjan valikko ja valitaan **Duplicate Template**. Tässä opinnäytetyössä työasemille asennettavan sertifikaatin nimeksi on annettu **DOT1X**. **Subject Name** -välilehdeltä käydään vaihtamassa **Subject name format** muotoon **DNS name**. Tällä saadaan sertifikaatille yksilöivä nimi kuten kuviossa 23. (Microsoft 2019a.)



Kuvio 23. Yksilöivä nimi työasemasertifikaatille.

Työasemille asennettaville sertifikaateille tulee antaa oikeudet automaattisen jakeluun siirtymällä **Security**-välilehdelle, valitsemalla **Domain Computers** ja antamalla oikeudet **Autoenroll**-toiminnolle. Tämän jälkeen sertifikaattipohjat ovat valmiita. (Microsoft 2019a.)

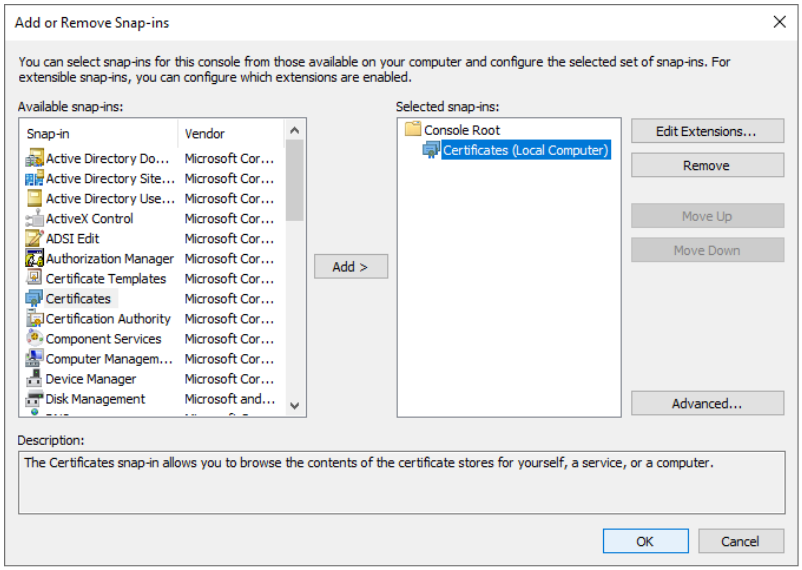
Luodut sertifikaatit pitää kuitenkin vielä lisätä **Certificate Templates** -kansioon siirtymällä takaisin **Certification Authority** -ikkunalle. Valitaan hiiren oikealla klikkauksella avataan **Certificate Templates** -kansion valikko ja valitaan **New** – **Certificate Template to Issue** ja valitaan luodut sertifikaatit. (Microsoft 2019f.)



Kuvio 24. Sertifikaatit asennettuna sertifikaattipohjien kansioon.

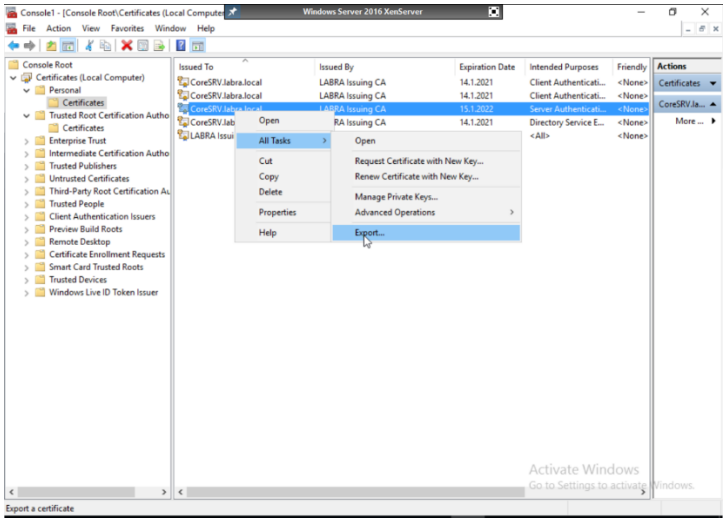
Luvussa 5.3.2 tullaan käsittelemään ryhmäkäytäntöä, jonka vuoksi tarvitaan palvelimelle asennettua Radius-sertifikaattia tiedostona. Palvelimelle myönnetty Radius-sertifikaatti saadaan siirrettyä tiedostomuotoon siirtymällä **Microsoft Management Console** -työkaluun ja avaamalla komentokehote painamalla Windows-näppäintä ja R-kirjainta. Tämän jälkeen syötetään komento **MMC** ja painetaan **OK**-painiketta. MMC:n avauduttua avataan oikeasta yläkulmasta **File – Add/Remove Snap-in**. Avautuneesta ikkunasta valitaan haluttu lisäosa, mikä tässä opinnäytetyössä on **Certificates**. Asettamalla **Certificates**-valinta aktiiviseksi ja painamalla hiiren vasemmalla painikkeella **Add**-painiketta avautuu **Certificates snap-in**-ikkuna, josta valitaan **Computer account**. Seuraavat kohdat voidaan jättää oletuksille ja siirtyä

eteenpäin painamalla **Next** ja **Finish**. Kun tilanne näyttää kuvion 25 mukaiselta voidaan painaa **OK**. (Microsoft 2018b.)



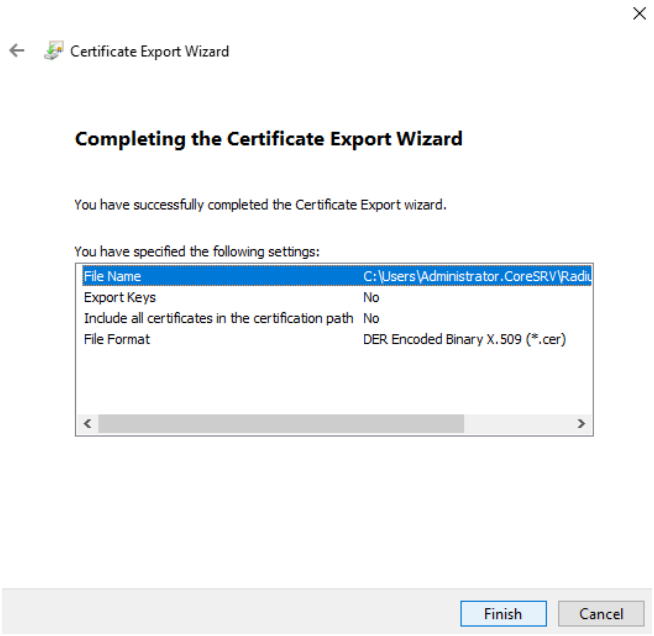
Kuvio 25. Asetukset MMC:n lisäosalle.

Lisäosan aktivoimisen jälkeen siirrytään kansiorakenteessa **Certificates – Personal – Certificates** -kansioon ja klikataan hiiren oikealla painikkeella **Radius Server Certificate** ja valitaan **All Tasks** – **Export** (Microsoft 2018b).



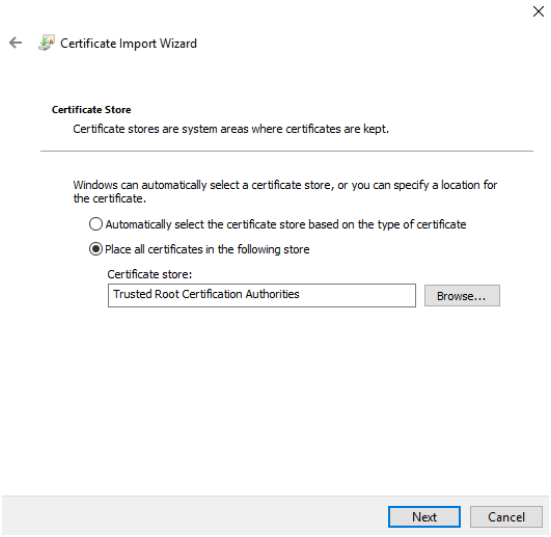
Kuvio 26. Export-toiminnon käyttäminen MMC-työkalussa.

Kaikki ikkunassa esiintyvät kohdat jätetään oletuksille ja edetään **Next**-periaatteella siihen asti, että työkalu pyytää nimen ja sijainnin antamista sertifikaatille. Sertifikaatille annetaan kuvaava nimi ja sijainti, jonka jälkeen vienti on valmis.



Kuvio 27. Certificate Export -työkalun asetukset.

Sertifikaatti lisätään **Trusted Root Certification Authorities** -kansion **Certificates**-alikansioon klikkamalla kansiota hiiren oikealla painikkeella ja valitsemalla **All tasks** ja sen jälkeen **Import**. Valikossa siirrytään eteenpäin oletuksilla. Seuraavalla välilehdellä työkalu pyytää sertifikaattia, joka halutaan tuoda. Viety sertifikaatti etsitään sille kuuluvasta sijainnista ja painetaan **OK**. Seuraavaksi siirrytään eteenpäin **Next**-painikkeella, jonka jälkeen varmistetaan, että sertifikaatti asentuu oikeaan paikkaan eli **Trusted Root Certification Authorities**. Seuraavaksi siirrytään viimeiseen osioon ja painetaan **Finish**-painiketta.



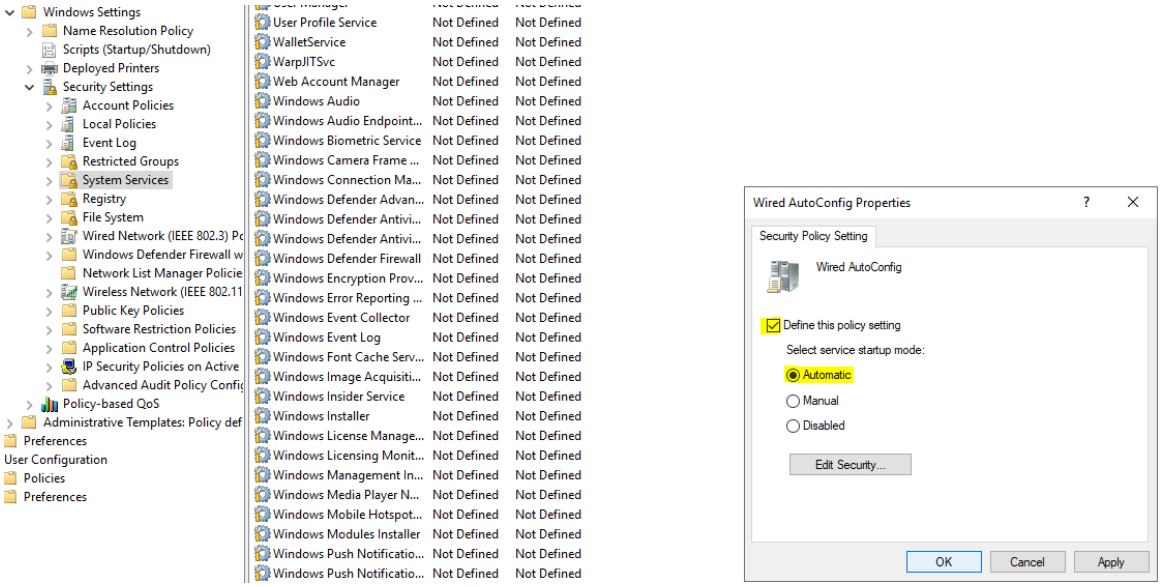
Kuvio 28. Sertifikaatin oikea sijainti.

5.3.2 Group Policy

Ryhmäkäytännön avulla saadaan toimialueen työasemille jaettua tarvittavat asetukset keskitetysti autentikointia varten. Tarvittavia asetuksia ovat luotettavien juurisertifikaatti auktoriteettien lisäys, automaattinen ilmoittautuminen sertifikaattipalveluita koskevalle ohjelmalle (Certificate Services Client), palvelun **Wired AutoConfig** automaattinen käynnistäminen ja langallisen verkkokäytännön asettaminen.

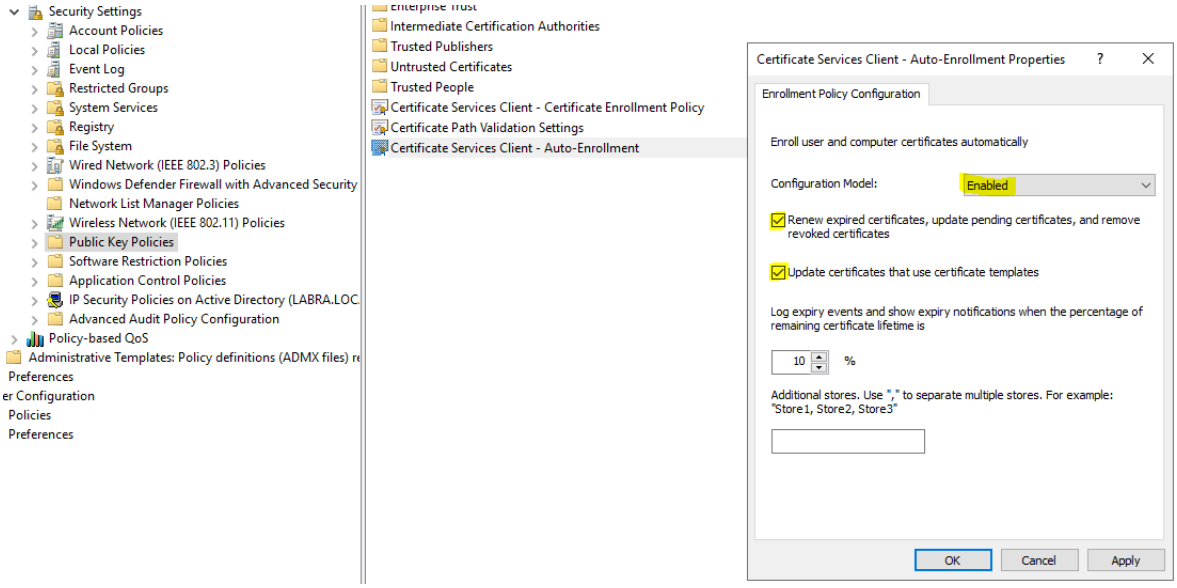
Ensimmäiseksi siirrytään ryhmäkäytännön hallinnointityökaluun **Server Manager**in **Tools**-valikosta valitsemalla **Group Policy Management**. Seuraavaksi navigoidaan omaan toimialueeseen, mikä tässä opinnäytetyössä on **labra.local**. Avaamalla alasvetovalikon toimialueen kohdalta avautuu useita eri vaihtoehtoja, joista pystytään tekemään muutoksia moneen eri toimialueen osa-alueeseen. Tässä opinnäytetyössä käsitellään ainoastaan valikkoa **Default Domain Policy**, koska kyseessä on testiympäristö. Muutoksia ryhmäkäytäntöön tehdään avaamalla **Group Policy Management Editor**. Tämä saadaan auki painamalla hiiren oikealla klikkauksella **Default Domain Policy**n päältä ja valitsemalla **Edit**. Tässä opinnäytetyössä käydään läpi työasemiin kohdistuvaa autentikointia, joten **Computer Configuration** -osio on keskiössä. **Computer Configuration** -valikosta siirrytään kohtaan **Policies – Windows Settings – Security Settings**. Tämän kansion sisältä löytyy kaikki 802.1X
-autentikointiin tarvittavat työasemille tehtävät muutokset lukuun ottamatta työaseman toimialueelle liittämistä, mikä jää tämän opinnäytetyön kokonaisuuden ulkopuolelle. (Microsoft 2016b.)

Ensimmäinen muutos, mikä työasemille tehdään, on palvelun **Wired Autoconfig** automaattinen käynnistäminen. Tämä laitetaan käytäntöön siirtymällä **System Services** -kansioon ja klikkaamalla **Wired Autoconfig** -palvelua hiiren oikealla painikkeella ja valitsemalla **Properties**. Avautuneesta ikkunasta siirrytään **Define this policy setting** -kohdan päälle ja klikataan se aktiiviseksi, jonka jälkeen valitaan **Automatic**. Näiden toimenpiteiden jälkeen painetaan **OK**. (Microsoft 2016b.)



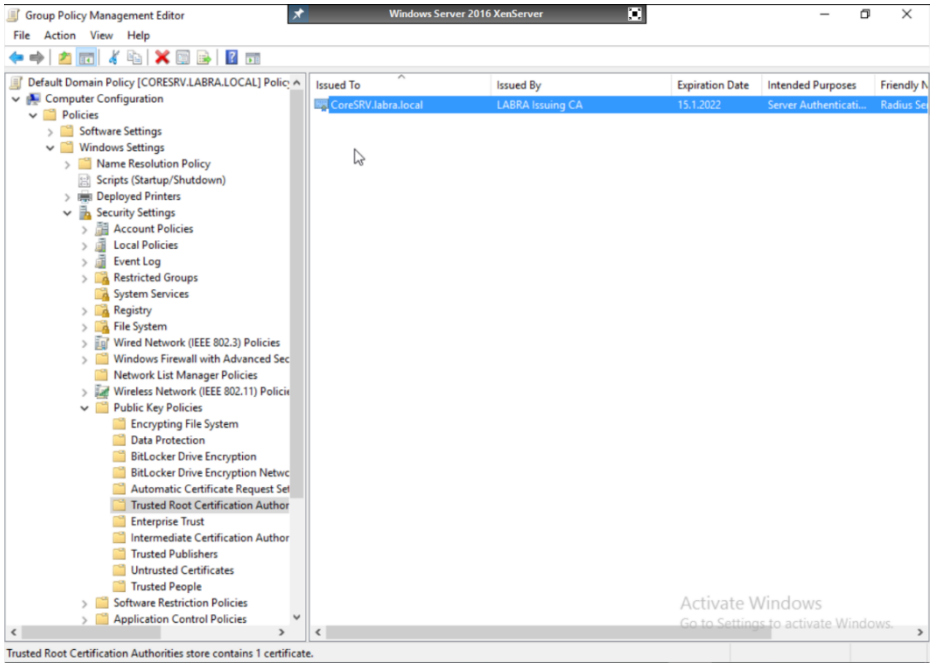
Kuvio 29. Wired AutoConfig -palvelun automaattinen käynnistys.

Seuraavaksi siirrytään muokkaamaan **Public Key Policies**-kansion sisältöä. Ensimmäiseksi asetetaan automaattinen ilmoittautuminen sertifikaateille aktiiviseksi, jotta työasemat saavat tarvittavan sertifikaatin autentikoimista varten. Klikkaamalla kohtaa **Certificate Services Client – Auto-Enrollment** hiiren oikealla painikkeella ja valitsemalla **Properties** päästään muuttamaan asetuksia. Asetuksista muutetaan ensimmäiseksi **Configuration Model** muotoon **Enabled**. Tämän avulla saadaan laitettua automaattinen ilmoittautuminen päälle. Tämän toimenpiteen jälkeen piilotetut asetukset tulevat esiin. Näistä asetettiin aktiiviseksi molemmat. Nämä asetukset takaavat sen, että vanhentuneet sertifikaatit, jakoa odottavat sertifikaatit ja käytöstä poistetut sertifikaatit käydään läpi ja tehdään joko niiden uusinta, jako tai poistaminen. Sertifikaatit, jotka käyttävät sertifikaattipohjia uusitaan myös tämän muutoksen avulla. (Microsoft 2019c.)



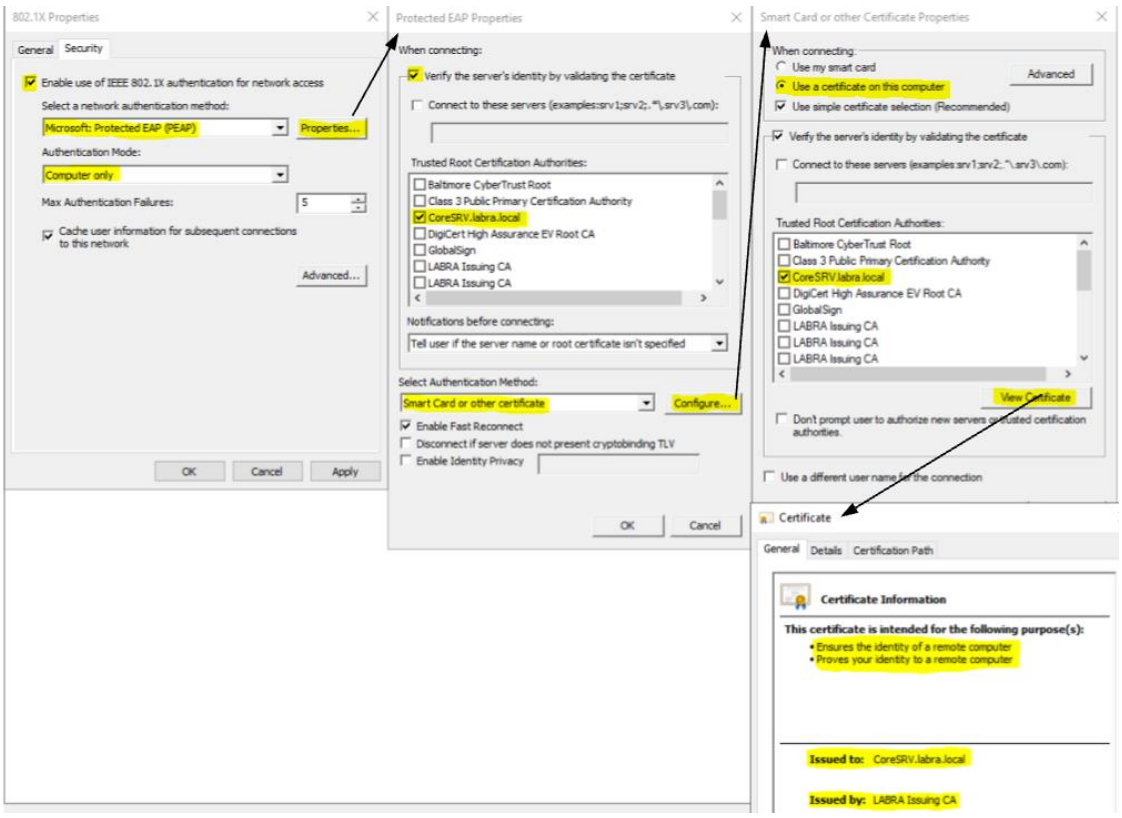
Kuvio 30. Sertifikaattien jako ryhmäkäytännön avulla.

Tämän toimenpiteen jälkeen siirrytään lisäämään luvun 5.3.1 lopussa tuotu sertifikaatti luotettujen juurisertifikaatti auktoriteettien listalle. Klikkaamalla hiiren oikealla painikkeella **Trusted Root Certification Authorities** -kansiota valitaan **Import**. **Certificate Import Wizard**-työkalun avulla lisätään tuotu Radius-sertifikaatti TRCA:n listalle (VMware 2013).



Kuvio 31. Sertifikaatti asennettuna luotettujen juurisertifikaatti auktoriteettien joukkoon.

Viimeisessä vaiheessa asetetaan PEAP-EAP-TLS-tavan käyttämät langallisen verkon asetukset työasemille siirtymällä **Security Settings** -kansiossa **Wired Network (IEEE 802.3) Policies** -kohdan päälle ja klikkaamalla sitä hiiren oikealla painikkeella ja valitsemalla **Create A New Wired Network Policy for Windows Vista and Later Releases**. Tässä opinnäytetyössä nimetään käytäntö muotoon 802.1X ja siirrytään **Security**-välilehdelle. **Security**-välilehdellä asetetaan 802.1X aktiiviseksi ja autentikointimetodiksi **Microsoft: Protected EAP (PEAP)**. Autentikoinnin tilaksi asetetaan **Computer only**, koska opinnäytetyö käsittelee ainoastaan työasemakohtaista autentikointia. Siirtymällä **New Wired Network Policy Properties** -ikkunassa **Properties**-painikkeen taakse päästään muuttamaan autentikointimetodin asetuksia, jotka tässä opinnäytetyössä laitetaan muotoon **Smart Card or other certificate** ja valitaan luvussa 5.3.1 tuotu Radius-sertifikaatti, joka näkyy tässä kontekstissa nimellä **CoreSRV.labra.local**. Tämän valinnan jälkeen siirrytään **Smart Card or other Certificate Properties**-valikkoon klikkaamalla **Configure**-painiketta **Protected EAP Properties** -ikkunassa. Avautuneessa ikkunassa valitaan uudelleen tuotu Radius-sertifikaatti ja tarkistetaan, että sen tiedot ovat oikein **View Certificate** -painikkeella. Asetuksien tulee olla identtiset kuvion 28 kanssa. (Microsoft 2016b.)

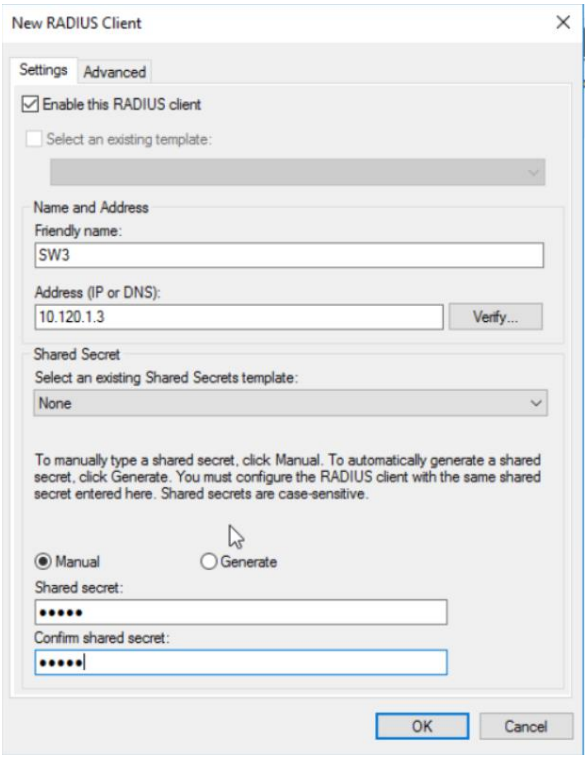


Kuvio 32. Langallisen verkon asetukset työasemille.

5.3.3 Network Policy Server

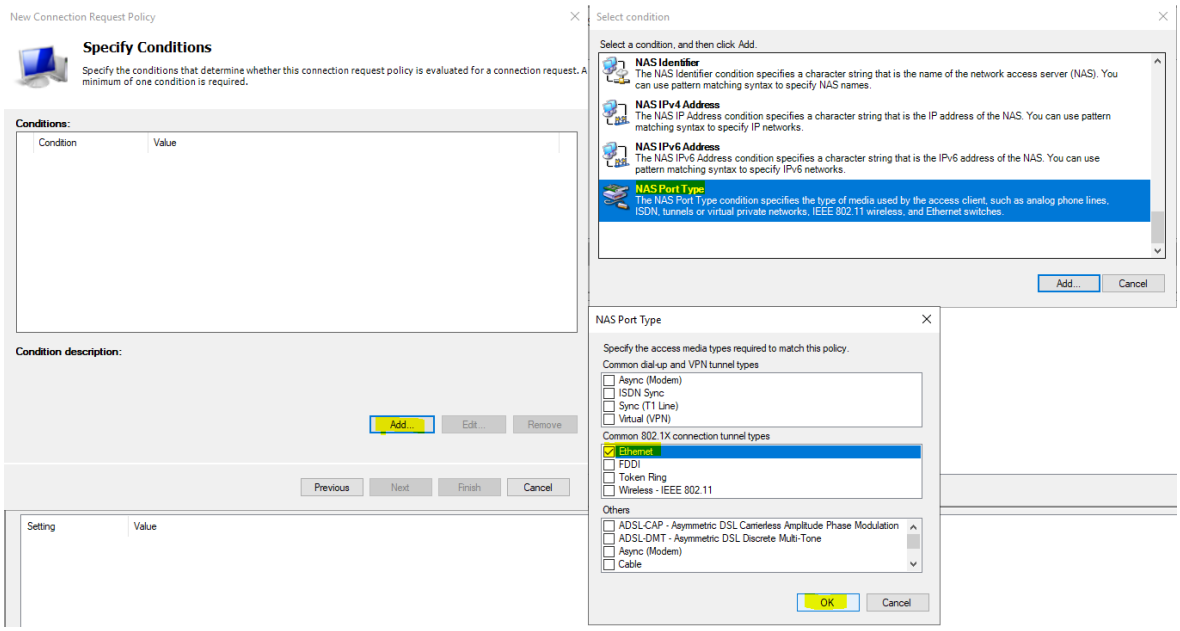
Viimeisessä vaiheessa määritetään käytäntö 802.1X-standardille. Autentikointikäytännön luomista varten siirrytään kohtaan **Server Manager** – **Tools** – **Network Policy Server**. Konfigurointi aloitetaan siirtymällä **RADIUS Clients and Servers** -kansioon ja klikataan hiiren oikealla painikkeella **RADIUS Clients** ja valitaan **New**. (Microsoft 2019g.)

New RADIUS Client -ikkunassa annetaan autentikaattorille nimi, IP-osoite ja jaettu salasana (Microsoft 2019g).



Kuvio 33. Uuden autentikaattorin lisäys.

Seuraavaksi siirrytään **Policies**-kansioon ja klikataan hiiren oikealla painikkeella **Connection Request Policies** -kansiota ja valitaan **New**. **New Connection Request Policy** -ikkunan ensimmäisellä sivulla pyydetään nimeä käytännölle, joka tässä opinnäytetyössä on 802.1X Wired. **Next**-painiketta painamalla siirrytään ehtoihin. Tässä opinnäytetyössä käydään läpi langallista autentikoimista, joten ainoaksi ehdoksi määritellään se, että yhteyden tulee käyttää langallista yhteyttä eli Ethernet:iä. Seuraavat kohdat voidaan ohittaa **Next**-periaatteella, eikä oletusasetuksiin tehdä muutoksia. (Microsoft 2019h.)



Kuvio 34. Network Policy Serverissä määritellyt ehdot yhteyksille.

Viimeisessä vaiheessa määritellään verkkokäytännöt. **Policies**-kansiosta viedään hiiri **Network Policies** -kansion päälle ja klikataan tätä hiiren oikealla painikkeella, jonka jälkeen valitaan **New**. Seuraavaksi avautuu **New Network Policy** -ikkuna, jossa pyydetään antamaan käytännölle nimi. Ensimmäiseksi luodaan IT-osaston käyttöön tuleva käytäntö, joten nimeksi annetaan VLAN10 IT ja painetaan **Next**. Seuraavassa vaiheessa pyydetään ehtoja, joiden mukaan tätä käytäntöä tullaan soveltamaan. Tähän lisätään ehdoksi se, että laite kuuluu ryhmään VLAN10 IT. Ehdon asettamisen jälkeen painetaan **Next** ja siirrytään seuraavalle sivulle. Tällä sivulla määritellään se, annetaanko laitteelle pääsy, hylätäänkö se vai annetaanko käyttäjien **Dial-in**-ominaisuuden määritellä pääsy tai hylkäys. Tähän valitaan **Access granted** ja siirrytään seuraavalle sivulle **Next**-painikkeella. (Microsoft 2019i.)

Seuraavalla sivulla määritellään autentikointimetodit ja EAP-tyypit, joita tullaan käyttämään autentikoinnissa. Tässä opinnäytetyössä käsitellään PEAP-EAP-TLS-metodiin perustuvaa autentikointia, joten valitaan **Add** ja valitaan **Microsoft: Protected EAP (PEAP)**. Tämän jälkeen siirrytään konfiguroimaan kyseistä tyyppiä valitsemalla se aktiiviseksi luettelosta ja painamalla **Edit**. (Microsoft 2019i.)

Edit Protected EAP Properties -ikkunasta tarkistetaan, että **Certificate issued to** -kohdassa on oikea sertifikaatti valittuna, mikä tässä tapauksessa on uusin luette-

losta löytyvä sertifikaatti. Tämän voi tarkistaa vertailemalla **Expiration date** -kohdassa olevia päiväyksiä ja vaihtelemalla sertifikaatteja. Tässä ikkunassa tehdään vielä muutos **Eap types** -valikkoon poistamalla oletuksena käytetty **Secured password (EAP-MSCHAP v2)**, valitsemalla se aktiiviseksi ja painamalla **Remove**-painiketta. Tämän jälkeen lisätään **Smart card or other certificate** -metodi listalle ja painetaan **OK**. Poistetaan vielä oletuksena asetetut valinnat vähemmän turvallisista autentikointimetodeista ottamalla valinnat pois MS-CHAP-v2- ja MS-CHAP-metodeilta **Configure Authentication Methods** -välilehdeltä ja painetaan **Next**. (Microsoft 2019i.)

Seuraavalla sivulla ei tarvitse tehdä muutoksia, koska kyseessä on testiympäristö eikä rajoituksilla ole merkitystä, joten voidaan siirtyä seuraavalle sivulle painamalle **Next**-painiketta.

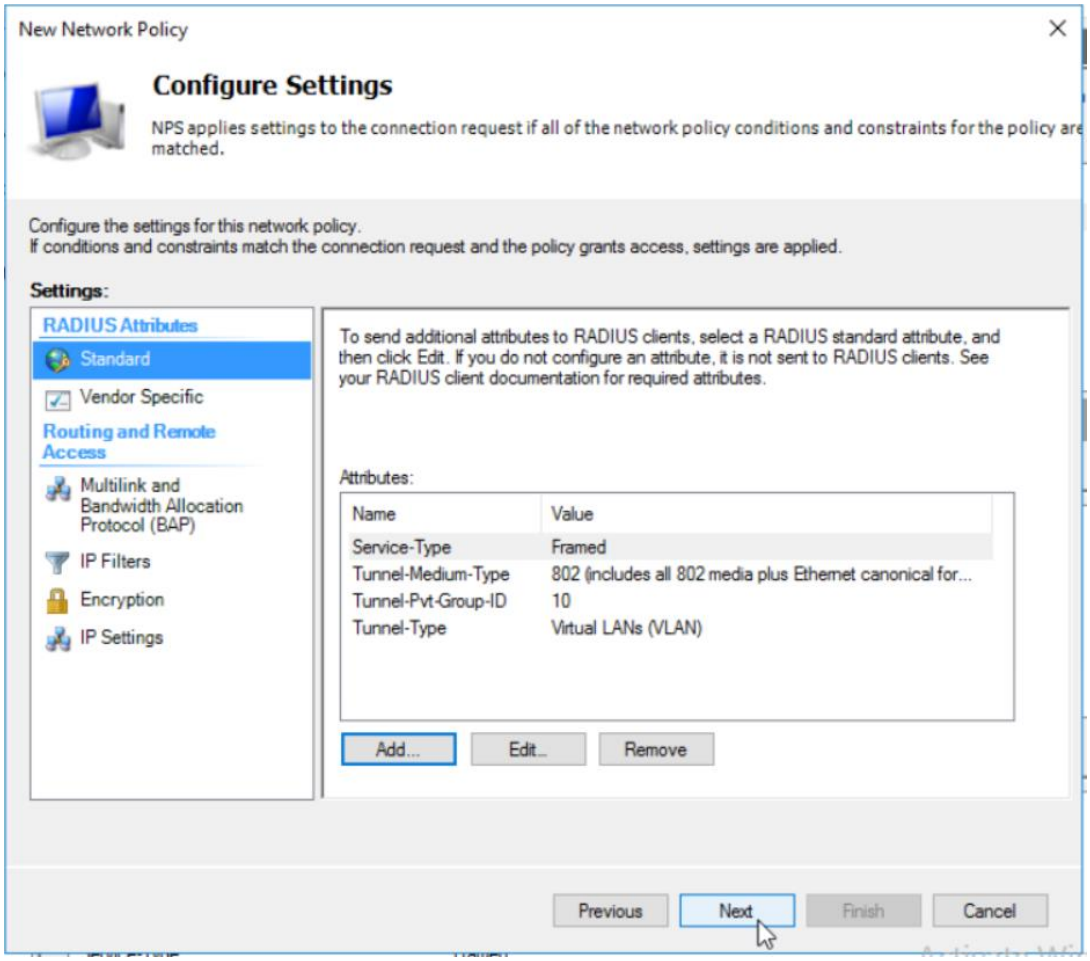
Viimeisessä vaiheessa konfiguroidaan asetukset, jotka NPS asettaa saapuvalle yhteydelle, mikäli kaikki ehdot ja rajoitukset täsmäävät. Tässä opinnäytetyössä käsitellään eri langallisella yhteydellä toimivia työasemia, joten ensimmäiseksi lisätään attribuutti, joka määrittelee yhteyden välittäjäksi langallisen verkon.

Attribuutti lisätään siirtymällä vasemmalla sijaitsevasta **Settings**-valikosta **Standard**-välilehdelle ja klikkaamalla **Add**-painiketta. Ensimmäiseksi poistetaan listalta **Framed-Protocol**, jonka arvona on **PPP**, koska käytössä on useita eri verkossa toimivia laitteita. EAP:n lähettämät viestit eivät käytä PPP-protokollaa, vaan ne lähetetään Ethernet-kehyksillä. Listalta valitaan **Tunnel-Medium-Type** ja klikataan **Add**-painiketta. Aukeaa uusi ikkuna, jossa määritetään attribuutin arvo klikkaamalla **Add**-painiketta, valitaan **Commonly used for 802.1x** ja asetetaan **802 (includes all 802 media plus Ethernet canonical format)**, jonka jälkeen painetaan **OK**-painiketta. Painikkeen painalluksen jälkeen palataan **Attribute Information** -ikkunaan, jossa painetaan **OK**-painiketta. (Microsoft 2019i.)

Tämän jälkeen valitaan listalta **Tunnel-Pvt-Group-ID**, minkä jälkeen klikataan **Add**-painiketta. **Attribute Information** -ikkunassa painetaan uudelleen **Add**-painiketta ja syötetään **String**-muotoinen arvo 10. Tällä asetuksella määritellään se, mihin vir-

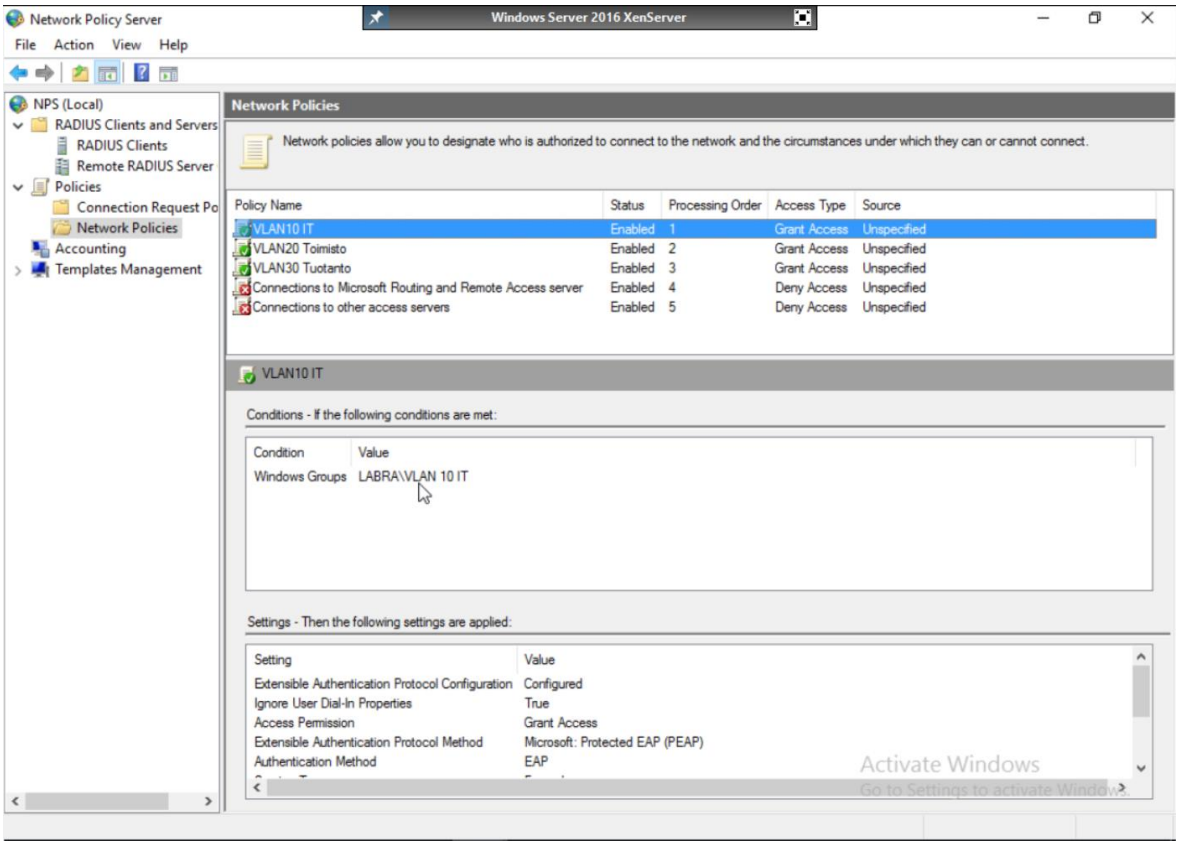
tuaalilähiverkkoon autentikaattori asettaa työaseman, mikäli autentikointi on onnistunut. Klikataan **OK**-painiketta siihen asti, että ollaan takaisin **Add Standard RADIUS Attribute** -ikkunassa. (Microsoft 2019i.)

Viimeiseksi asetetaan **Tunnel-Type**, jolla määritellään mihin ryhmään **Tunnel-Pvt-Group-ID**-kohdassa määritetty arvo kohdistetaan, mikä tässä opinnäytetyössä on **VLAN**. Listalta valitaan **Tunnel-Type** ja painetaan **Add**-painiketta. **Attribute Information**
-ikkunassa klikataan uudelleen **Add**-painiketta. Avautuneesta ikkunasta valitaan aktiiviseksi **Commonly used for 802.1x** ja valitaan **Virtual LANs (VLAN)**, jonka jälkeen klikataan **OK**-painiketta siihen asti, että ollaan takaisin **Configure Settings** -ikkunassa. Painamalla **Next**-painiketta päästään yhteenvetoon, jossa nähdään kaikki kyseiselle käytännölle tehdyt määritykset. Nämä voidaan hyväksyä klikkaamalla **Finish**-painiketta. (Microsoft 2019i.)



Kuvio 35. NPS-käytännön asetukset VLAN10-ryhmälle.

Tämä toimenpide toistettiin VLAN20- ja VLAN30-ryhmille ja ainoat eroavaisuudet VLAN10-ryhmälle luotuun NPS-käytäntöön olivat Tunnel-Pvt-Group-ID:n muutos vastaamaan ryhmän vlania, käytännön nimen asettaminen ryhmää kuvaavaan muotoon ja Windows-ryhmän vaihto.



Kuvio 36. Näkymä kaikkien VLAN-käytäntöjen osalta.

5.4 Kytkimen ja reitittimen asetukset

Kytkimelle ja reitittimelle tehtävissä konfiguroinneissa pääpaino keskittyy kytkimelle, koska se toimii autentikaattorina. Reitittimen konfiguraatioon ei tarvitse tehdä mitään erityisiä muutoksia, vaikka verkkoympäristössä on käytössä 802.1X.

5.4.1 Kytkimen asetukset

Kytkimelle tehtävät konfigurointimuutokset tehtiin käyttämällä Simon Tathamin kehittämää ssh-, telnet- ja pääte-emulaattoria eli PuTTya. Kytkimeen päästiin käsiksi kytkemällä sarjaporttikaapeli työasemasta kytkimelle.

Ensimmäiseksi kytkimelle piti syöttää komento: **enable**, näin saadaan käyttöön korotetut käyttöoikeudet, jonka jälkeen komennolla: **configure terminal** päästään globaaliin konfigurointitilaan. (Cisco 2006a, 3.)

Seuraavaksi kytkimelle luotiin VLAN 10 käyttämällä komentoa **vlan 10**, jonka jälkeen syöttämällä komento **name IT** saatiin asetettua nimi luodulle vlanille. Viimeiseksi syötettiin komento **no shutdown**, jolla määritettiin VLAN aktiiviseksi. Sama toimenpide toistettiin kaikille kolmelle opinnäytetyössä käytetylle VLANille. (Cisco 2006a, 4.)

VLAN 10 kuuluu IT-osastolle, minkä vuoksi kytkimen IP-osoite määritetään kuulumaan tähän IP-avaruuteen. Kytkimen IP-osoite 10.120.1.3 saatiin asetettua komennoilla **interface vlan 10**, jonka jälkeen syötettiin komento **ip address 10.120.1.3 255.255.255.0**. (Cisco 2006a, 112.)

802.1X konfiguraatio luotiin kytkimelle seuraavasti taulukon 1 mukaisesti

Taulukko 1. 802.1X:n käyttöönotto kytkimellä.

Komento	**Toiminta**
aaa new-model	Aktivoi AAA:n kytkimellä.
aaa authentication dot1x default group radius	Määrittelee RADIUS-protokollan metodina 802.1X:ssä käytettävälle autentikoinnille.
aaa authorization network default group radius	Antaa VLAN-hallinnan RADIUS-palvelimelle.

dot1x system-auth-control	Ottaa 802.1X:n käyttöön kokonaisvaltaisesti kytkimellä.
radius-server host 10.120.1.2 auth-port 1812 acct-port 1813 key cisco	Määrittelee RADIUS-palvelimen IP-osoitteen, protokollan käyttämät portit ja jaetun salasanan.

Komennot opinnäytetyössä käytetyille kytkimen porteille löytyvät taulukoista 2 – 4

Taulukko 2. Työasemaporttien 1 – 3 konfiguraatio.

Komento	**Toiminta**
interface range fastEthernet 0/1 - 3	Porttien 1 – 3 konfiguraatioon siirtyminen ja samanaikainen konfigurointi.
switchport mode access	Portin tilan vaihto access-tilaan.
authentication port-control auto	Asettaa portin aloittamaan autentikoinnin, mikäli sen tila vaihtuu DOWN-tilasta UP-tilaan tai pysyy UP-tilassa ja autentikoimattomana.
dot1x pae authenticator	Asettaa portin PAE-tyypin autentikaattoriksi, jolla portti ei vastaa asiakkaalle kuuluviin viesteihin vaan ainoastaan autentikaattorille kuuluviin viesteihin.

Taulukko 3. Palvelimelle tarkoitetun portin konfigurointi.

Komento	**Toiminta**
interface fastEthernet 0/10	Portin 10 konfiguraatioon siirtyminen.
switchport mode access	Portin tilan vaihto access-tilaan.
switchport access vlan 10	Vlanin asettaminen portille.

Taulukko 4. Reitittimelle kuuluvan portin konfiguraatio.

Komento	**Toiminta**
interface fastEthernet 0/24	Portin 24 konfiguraatioon siirtyminen.
switchport mode trunk	Portin tilan vaihto trunk-tilaan, jonka avulla voidaan välittää VLAN-tietoja.
switchport trunk allowed vlan 10,20,30	Useamman vlanin läpi päästäminen kyseisestä portista joko kytkimelle, reitittimelle tai tukiasemalle.

5.4.2 Reitittimen asetukset

Reitittimelle tehdyt konfiguroinnit tehtiin globaalissa konfigurointitilassa, johon päästiin samalla tapaa kuin kytkimellä. Ainoat komennot, joita reitittimeen tarvitsi tehdä, oli kapseloinnin luominen vlaneille 10, 20 ja 30 komennolla **encapsulation dot1Q**. Tämän komennon avulla mahdollistetaan liikenne eri vlanien välillä. Seuraavaksi tehtiin oletusyhdyskäytävän määritys kyseisille vlaneille ja DHCP-palvelimen IP:n asettaminen **ip helper-address** -komennolla. Portin 0/0-tila piti muuttaa aktiiviseksi

no shutdown -komennolla ennen kuin porttiin liitettyjen kytkimeltä tulevien vlanien reititys alkoi toimimaan. (Cisco 2006b.)

```
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 10.120.1.1 255.255.255.0
 ip helper-address 10.120.1.2
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 10.120.2.1 255.255.255.0
 ip helper-address 10.120.1.2
!
interface FastEthernet0/0.3
 encapsulation dot1Q 30
 ip address 10.120.3.1 255.255.255.0
 ip helper-address 10.120.1.2
```

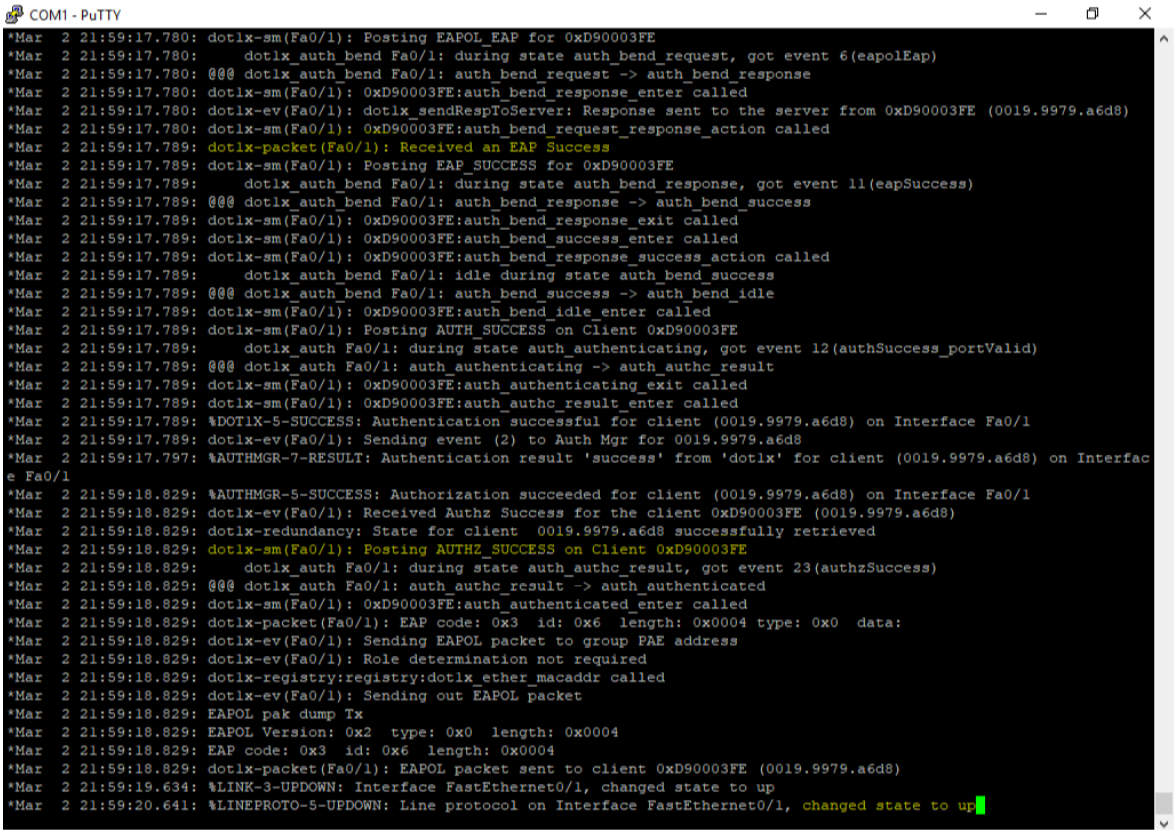
Kuvio 37. Reitittimen asetukset luoduille vlaneille 10, 20 ja 30.

6 TULOKSET JA ONGELMAT

Opinnäytetyössä tehdyn toteutuksen avulla päästiin haluttuun lopputulokseen, mikä tarkoitti sitä, että autentikointi toimi onnistuneesti. Ongelmia ilmeni aluksi työasemilla, sillä palvelimella käytetty Radius-sertifikaatti oli jäänyt lisäämättä ryhmäkäytännön avulla **Trusted Root Certification Authorities** -listalle. Tämän vuoksi työasemat eivät suostuneet aloittamaan autentikointiprosessia ennen kuin niiltä oli käyty hyväksymässä käyttöjärjestelmän luoma dialogi siitä luotetaanko tähän kyseiseen palvelimeen ja sen sertifikaattiin. Tämä piti tehdä työasemalle aina uudelleen käynnistyksen jälkeen. Tämä saatiin kuitenkin korjattua lisäämällä palvelin **Trusted Root Certification Authorities** -listalle ryhmäkäytännön avulla.

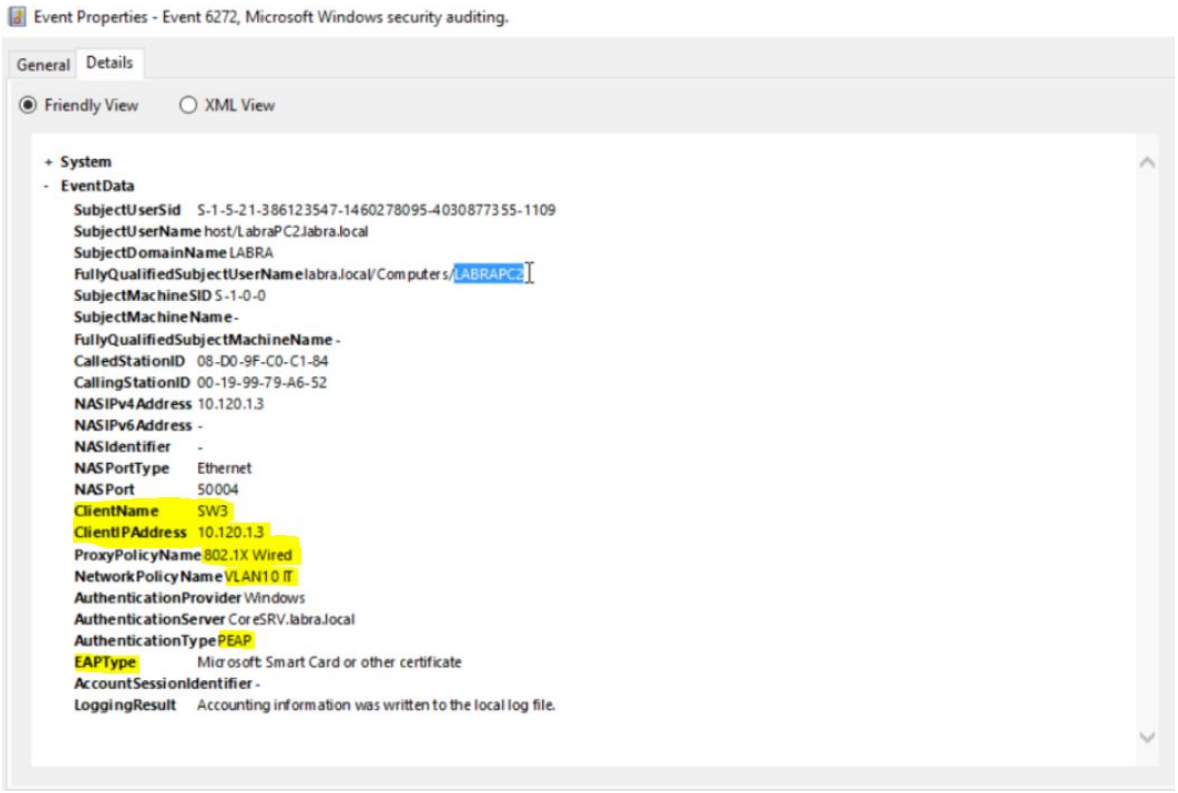
Ryhmäkäytännön saaminen työasemille ja niiden muokkaaminen oli aika ajoin haastavaa, sillä 802.1X-protokollaa käyttävässä portissa oleva työasema ei pystynyt muodostamaan minkäänlaista yhteyttä palvelimelle silloin kun autentikointi oli epäonnistunut. Tästä syystä käytössä oli yksi kytkimen portti, jolle oli asetettu vlan 10 suoraan PuTTyn terminaalista. Tämän portin avulla ajettiin ryhmäkäytännön mukana tulevat asetukset työasemille ennen kuin ne siirrettiin käyttämään 802.1X-protokollaa.

Tuloksia ja ongelmanratkaisua pystyttiin tekemään monella eri tavalla, mutta ehkä tärkeimpänä näistä olivat kytkimeltä tehdyt testaukset käyttäen Ciscon kytkimellä komentoa **debug dot1x all** (Cisco 2018). Tämän avulla pystyttiin monitoroimaan kytkimen puoli päästä asiakkaan ja autentikointipalvelimen välistä kättelyä tarkastelemalla kuviossa 38 esiintyvää lokia, joka sisältää oleellista tietoa autentikoinnin kulusta. Kuviossa 38 ensimmäinen korostettu osio kuvaa autentikaattorin saamaa viestiä palvelimelta, että autentikointi on onnistunut ja laitteelle voidaan antaa pääsy verkkoon. Toisessa korostetussa kohdassa autentikaattori aloittaa Success-viestin lähetyksen asiakkaalle. Kolmannessa korostetussa kohdassa nähdään, että portti on siirtynyt down-tilasta up-tilaan eli aktiiviseksi.



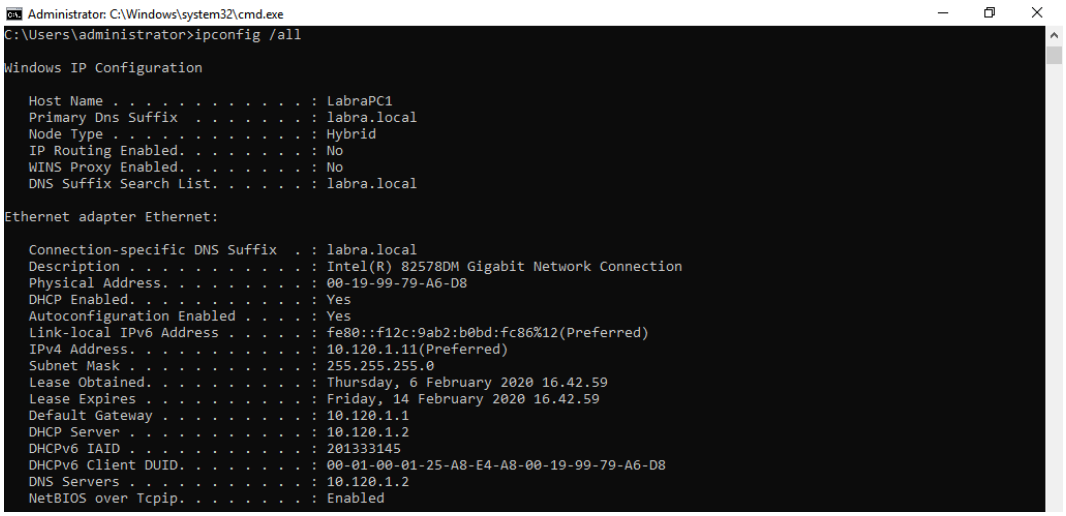
Kuvio 38. Onnistunut autentikointi kytkimen näkökulmasta.

Palvelimella olevan **Event Viewer** -työkalun eli tapahtumienvalvontatyökalun avulla pystyttiin myös näkemään, mikäli autentikointi oli onnistunut tai epäonnistunut. Avaamalla **Event Viewer** palvelimelta ja siirtymällä **Custom Views** -kansion alla olevaan **Server Roles**-kansioon ja valitsemalla **Network Policy and Access Services** voidaan tarkastella NPS:lle tuleviin autentikointipyyntöihin muodostunutta lokia. Sieltä voidaan tarkastella muun muassa miksi pääsy on evätty joltakin laitteelta tai pääsy on myönnetty laitteelle. Kuviossa 39 nähdään, että työasema LabraPC2 on pyytänyt autentikointia, autentikoinnin on välittänyt autentikaattori SW3, jonka IP-osoite on 10.120.1.3. NPS-käytännöt, joita autentikoinnissa on käytetty ovat 802.1X Wired ja VLAN10 IT. Autentikoinnintyyppinä on PEAP ja EAP-tyyppinä älykortti tai sertifikaatti, mikä muodostaa PEAP-EAP-TLS-kokonaisuuden.



Kuvio 39. Onnistunut autentikointi työasemalle palvelimen tapahtumienvalvonta-työkalun näkökulmasta.

Onnistuneen autentikoinnin tuloksena työasemat saatiin jaettua niille kuuluviin ali-verkkoihin. Windows-käyttöjärjestelmissä olevan komentokehotteen avulla voidaan tarkastella saatua lopputulosta syöttämällä komento: **ipconfig /all**, joka näyttää kaikkien verkkoadapterien TCP/IP-konfiguraation. (Microsoft 2017b.)



Kuvio 40. Komentokehotteelta otettu kuvankaappaus ipconfig /all-näkymästä.

7 YHTEENVETO

Opinnäytetyössä saatiin haluttu lopputulos, mikä oli porttikohtaisen autentikoinnin toteutus työasemille käyttäen sertifikaattipohjaista autentikointia. Opinnäytetyössä käytetyt laitteet ja ohjelmistot soveltuivat loistavasti työn tekemiseen, sillä kaikki niistä omasivat kattavan dokumentaation, mikä auttoi toteutuksen tekemisessä ja vikatilanteiden ratkaisemisessa. Opinnäytetyössä läpikäydyt protokollat, verkkoratkaisut, tekniset laitteet ja alustat ovat antaneet kattavan ymmärryksen tietoliikenteestä ja tietojärjestelmistä.

Työasemien IP-osoitteet saatiin CoreSRV:llä toimivalta DHCP-roolilta. Ne määräytyivät sen mukaan, mihin vlaniin kukin työasema oli määritelty NPS-käytännössä. IP-osoitteiden jakamiseen tehdyt määritykset toimivat odotetusti ja IP-osoitteet jakautuivat oikein.

Porttikohtainen autentikointi voi aiheuttaa organisaatioissa ja toteutuksissa ongelmia erityisesti laitteiden kohdalla, jotka eivät syystä tai toisesta pysty käsittelemään EAP-paketteja tai suoriutumaan porttikohtaisesta autentikoinnista. Näitä tapauksia varten eri laitevalmistajat ovat luoneet ratkaisuja kyseiseen ongelmaan. Ciscon luoma ratkaisu tälle ongelmalle on se, että autentikoinnissa epäonnistunut laite on mahdollista siirtää ennalta määriteltyyn vierailija-vlaniin. Tämä vlan voidaan määritellä kaikille 802.1X-protokollaa käyttäville access-tilassa oleville porteille. Trunk-tilassa olevat portit eivät ole tuettuja. (Cisco 2012).

Mitä kannattaa ja ei kannatta tehdä, mistä on hyötyä, ja mihin kannattaa panostaa ovat kysymyksiä, joihin opinnäytetyön tekeminen vastasi. Testiympäristöstä saatuja tuloksia voidaan soveltaa useaan eri käyttötarkoitukseen, mikäli haluttu tulos on tietoturvan lisääminen lähiverkossa.

LÄHTEET

Cisco. 2006a. Catalyst 2960 Switch Command Reference. [www-dokumentti]. Cisco Systems [Viitattu 26.1.2020]. Saatavana: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_25_see/command/reference/cr.pdf

Cisco. 2006b. Configuring the Cisco IOS DHCP Relay Agent. [www-dokumentti]. Cisco Systems. [Viitattu 4.2.2020]. Saatavana: https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html

Cisco. 2012. IEEE 802.1X Auth Fail VLAN. [www-dokumentti]. Cisco Systems. [Viitattu 31.1.2020]. Saatavana: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/sec-ieee-8021x-vlan-assign.html

Cisco. 2018. Chapter: Catalyst 3750-X and 3560-X Switch Debug Commands. [www-dokumentti]. Cisco Systems. [Viitattu 4.2.2020]. Saatavana: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

Geier, J. 2018. Implementing 802.1X Security Solutions for Wired and Wireless Networks. Yhdysvallat: Wiley Publishing, Inc.

ISO/IEC 7498-1. 1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. Sveitsi: ISO/IEC Copyright Office.

Microsoft. 2012. EAP Overview. [www-dokumentti]. Microsoft Corporation. [Viitattu 19.1.2020]. Saatavana: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770622%28v%3dws.10%29

Microsoft. 2016a. 802.1X Authenticated Wired Access Overview. [www-dokumentti]. Microsoft Corporation. [Viitattu 8.1.2020]. Saatavana: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831831(v%3Dws.11)

Microsoft. 2016b. Managing the New Wired Network (IEEE 802.3) Policies Settings. [www-dokumentti]. Microsoft Corporation. [Viitattu 28.1.2020]. Saatavana: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831813(v%3Dws.11)

Microsoft. 2017a. Install Active Directory Domain Services (Level 100). [www-dokumentti]. Microsoft Corporation. [Viitattu 26.1.2020]. Saatavana:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-

Microsoft. 2017b. ipconfig. [www-dokumentti]. Microsoft Corporation. [Viitattu 7.2.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

Microsoft. 2018a. Step 4. Install and configure the Network Policy Server (NPS). [www-dokumentti]. Microsoft Corporation. [Viitattu 2.2.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/vpn-deploy-nps

Microsoft. 2018b. Installing the trusted root certificate. [www-dokumentti]. Microsoft Corporation. [Viitattu 3.2.2020]. Saatavana: https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate

Microsoft. 2018c. Forests. [www-dokumentti]. Microsoft Corporation. [Viitattu 26.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows/win32/ad/forests

Microsoft. 2019a. Configure Certificate Templates for PEAP and EAP Requirements. [www-dokumentti]. Microsoft Corporation. [Viitattu 23.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-cert-requirements

Microsoft. 2019b. Configure the Server Certificate Template. [www-dokumentti]. Microsoft Corporation. [Viitattu 28.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-the-server-certificate-template

Microsoft. 2019c. Configure certificate auto-enrollment. [www-dokumentti]. Microsoft Corporation. [Viitattu 26.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-server-certificate-autoenrollment

Microsoft. 2019d. Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS. [www-dokumentti]. Microsoft Corporation. [Viitattu 27.1.2020]. Saatavana: https://support.microsoft.com/en-za/help/814394/certificate-requirements-when-you-use-eap-tls-or-peap-with-eap-tls

Microsoft. 2019e. Install the Certification Authority. [www-dokumentti]. Microsoft Corporation. [Viitattu 26.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

Microsoft. 2019f. Configure the Server Certificate Template. [www-dokumentti]. Microsoft Corporation. [Viitattu 26.1.2020]. Saatavana: https://docs.microsoft.com/fi-fi/windows-server/networking/core-network-guide/cncg/server-certs/configure-the-server-certificate-template

Microsoft. 2019g. RADIUS Clients. [www-dokumentti]. Microsoft Corporation. [Viitattu 28.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-radius-clients

Microsoft. 2019h. Connection Request Policies. [www-dokumentti]. Microsoft Corporation. [Viitattu 28.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-crp-crpolicies

Microsoft. 2019i. Configure Network Policies. [www-dokumentti]. Microsoft Corporation. [Viitattu 28.1.2020]. Saatavana: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-np-configure

Palekar, A., Simon, D., Microsoft, Zorn, G., Cisco, Josefsson, S. & Extundo. 2003. Protected EAP Protocol (PEAP). [www-dokumentti]. Yhdysvallat: The Internet Society. [Viitattu 23.1.2020]. Saatavana: https://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-06.txt

RFC 3748. 2004. Extensible Authentication Protocol (EAP). Yhdysvallat: The Internet Society.

VMware. 2013. Add the Root Certificate to Trusted Root Certification Authorities. [www-dokumentti]. VMware Inc. [Viitattu 5.2.2020]. Saatavana: https://docs.vmware.com/en/VMware-Horizon-7/7.5/horizon-installation/GUID-7966AE16-D98F-430E-A916-391E8EAAFE18.html