Ville Naumanen

802.1X-porttikohtaisen todennuksen suunnittelu ICTLAB-ympäristöön

Opinnäytetyö
Tieto- ja viestintätekniikka

2018

Kaakkois-Suomen
ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Ville Naumanen	Insinööri (AMK)	Toukokuu 2018

Opinnäytetyön nimi

802.1X-porttikohtaisen todennuksen suunnittelu ICTLAB-ympäristöön

51 sivua
9 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu, XAMK ICTLAB

Ohjaaja

Vesa Kankare

Tiivistelmä

Tämän opinnäytetyön tavoitteena on tutustua IEEE 802.1X -standardin mukaiseen porttipohjaiseen todennukseen ja sen toimitaan sekä suunnitella todennuksen käyttöönotto ICTLAB-ympäristöön. Käyttöönoton suunnittelu toteutettiin tekemällä ICTLAB-kesätyöharjoittelijoille kattava ohjeistus, jonka avulla he voivat suorittaa suunnitellun porttitodennuksen käyttöönoton kesällä 2018.

IEEE 802.1X -porttitodennuksen tarkoituksena on parantaa kohdeverkon tietoturvaa todentamalla käyttäjät tai työasemat niiden liittyessä verkkoon. Oikein konfiguroituna vain käyttäjät, joilla on tarvittavat oikeudet saavat pääsyn verkkoon. Luvattomilta käyttäjiltä pääsy verkkoon evätään suoraan. 802.1X-todennus oli jo käytössä ICTLAB:n langattomassa verkossa, joten tavoitteena oli parantaa myös langallisen verkon tietoturvaa ottamalla porttipohjainen todennus käyttöön. Työn yhtenä tavoitteena oli myös segmentoida verkon käyttäjiä omiin lähiverkkoihin aktiivihakemiston käyttäjäryhmän mukaisesti.

Työ aloitettiin tutkimalla porttikohtaisen todennuksen teoriaa ja sen käyttämiä protokollia, kuten EAP, RADIUS ja EAPOL. Teoriaosuudessa tutustuttiin myös lähiverkkojen ja tietoturvan teoriaan. Työn käytännön osuus koostui kahdesta osiosta. Ensimmäisessä osiossa porttitodennuksen käyttöönottoa harjoiteltiin suljetussa virtuaaliympäristössä. Toisessa osassa porttitodennusta testattiin ICTLAB-ympäristössä kahdella testikoneella. ICTLAB-testivaiheessa kokeiltiin myös käyttäjäsegmentointia, jossa eri käyttäjäryhmään kuuluvat käyttäjät ohjataan omiin lähiverkkoihinsa. Testauksen onnistuttua siirryttiin työn viimeiseen vaiheeseen eli käyttöönotto-ohjeistuksen tekemiseen kesäharjoittelijoita varten.

Työn lopputuloksena oli onnistunut pilottitesti ICTLAB-ympäristön kahdella työasemalla, sekä yksityiskohtainen ohjeistus porttitodennuksen käyttöönottamiseksi kesällä 2018.

Asiasanat

autentikointi, porttitodennus, dot1x, 802.1x-protokolla, radius

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Ville Naumanen	Bachelor of Information Technology	May 2018

Thesis title

Designing the implementation of 802.1X-port based authentication for ICTLAB-environment

51 pages
9 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences, XAMK ICTLAB

Supervisor

Vesa Kankare

Abstract

The goal of this thesis was to design the implementation of IEEE 802.1X-port based authentication for ICTLAB-environment. The design for the implementation was carried out by producing a comprehensive guide for ICTLAB summer trainees, enabling them to implement the designed authentication for the ICTLAB-environment during the summer of 2018.

The function of the 802.1X-port based authentication is to improve the information security of the target network by authenticating users or workstations when joining the network. When configured right, only authorized users will have access to the network. Unauthorized users will be denied instantly. The 802.1X-authentication method was already implemented in ICTLAB Wireless network, so the goal was to improve also the wired network security by implementing the port-based authentication protocol. One of the thesis goals was also segmenting users to different VLANs based on their Active Directory user group.

The thesis was started by studying the theory of port-based authentication and its protocols, such as EAP, RADIUS and EAPOL. The theory of local area networks and information security was also covered. The practical part of the thesis consisted of two sections. In the first section, the implementation of port-based authentication was studied and practiced in a closed virtual environment. The second part consisted of testing the 802.1X-authentication in real life environment using two workstations in the ICTLAB-environment. During the test phase user segmentation was also tested. After successful testing, it was time to move on to the final part of the thesis – producing a comprehensive guide for the summer trainees.

The result of the thesis was a successful pilot test using two workstations in the ICTLAB-environment, as well as the detailed guide for implementing the port-based authentication during the summer of 2018.

Keywords

authentication, port-based authentication, dot1x, 802.1X, radius,

SISÄLLYS

KÄSITTEET JA LYHENTEET

AAA-MALLI AAA-malli on käyttäjän tunnistamiseen käytetty kehysmalli. Nimi tulee sanoista *authentication (todennus), authorization (valtuutus)* ja *accounting (tilastointi).*

AD Active Directory eli aktiivihakemisto on Windows-palvelinympäristön rooli, jonka avulla voidaan hallita toimialueen käyttäjiä, ryhmiä ja laitteita.

AUTENTIKAATTORI Autentikaattori on 802.1X-todennuksessa käytetty aktiivilaite (esim. kytkin), joka toimii asiakkaan ja autentikointipalvelimen välissä tiedonvälittäjänä.

ASIAKAS 802.1X-standardissa asiakkaalla tarkoitetaan päätelaitetta tai käyttäjää, joka on verkon ulkoreunalla.

EAP *Extensible Authentication Protocol* on 802.1X-todennuksessa tiedonsiirtoon käytetty viitekehys, jonka avulla kuljetetaan todennustietoja.

EAPOL *EAP over LAN*. 802.1X-standardin käyttämä tiedonsiirtoprotokolla.

IEEE 802.1X IEEE 802.1X-standardinumero jolla tarkoitetaan porttikohtaista todennusta. Tunnetaan myös nimellä *dot1x.*

LAN *Local Area Network*, Lähiverkko.

OSI-MALLI Viitemalli, jolla kuvataan tiedonsiirtoprotokollien arkkitehtuuria seitsemässä kerroksessa.

NPS	*Network Policy Server*. Windows-palvelimen rooli, joka toimii RADIUS-palvelimena.
RADIUS	*Remote Authentication Dial-In User Service.* Todennusprotokolla, jonka avulla siirretään kirjautumistietoja palvelimen ja RADIUS-asiakkaan välillä.
PORTTI	Portti tarkoittaa verkon aktiivilaitteen liityntäpistettä, johon työasema kytketään kiinni verkkojohdon avulla.

1 JOHDANTO

Tietoturvaan liittyvät asiat ovat nykypäivänä suuri huolenaihe yrityksille ja organisaatioille. Suurin osa tiedosta kulkee Internetin ja tietoliikenneväylien välityksellä, joten tietoturvaan liittyvät riskit ovat huomattavat. Tämän työn tavoitteena on pyrkiä parantamaan Kaakkois-Suomen ammattikorkeakoulun Kotkan kampuksella toimivan ICTLAB-ympäristön tietoturvaa suunnittelemalla porttikohtaisen käyttäjätodennuksen käyttöönotto langalliseen verkkoon. Porttikohtaisella todennuksella voidaan valvoa ja rajata käyttäjien pääsyä verkkoon portti- tai käyttäjäkohtaisesti.

Opinnäytetyö koostuu kahdesta osiosta. Työn teoriaosiossa käsitellään IEEE 802.1x -protokollaa ja mm. eri yhteys- ja autentikointiprotokollia sekä tietoturvallisuuden ja lähiverkkojen teoriaa. Käytännön osio koostuu kahdesta osiosta: porttitodennuksen toteutus ja suunnittelu Jaakko Nurmen virtuaalilaboratoriossa sekä käytännön testiosuudesta, jossa porttitodennusta testataan ICTLAB-ympäristön valituilla, vähemmän käytössä olevilla työasemilla. Opinnäytetyön liitteeksi toteutetaan kattava ohjeistus, jonka avulla porttipohjainen todennus otetaan käyttöön ICTLAB-kesäharjoittelijoiden toimesta kesän 2018 aikana.

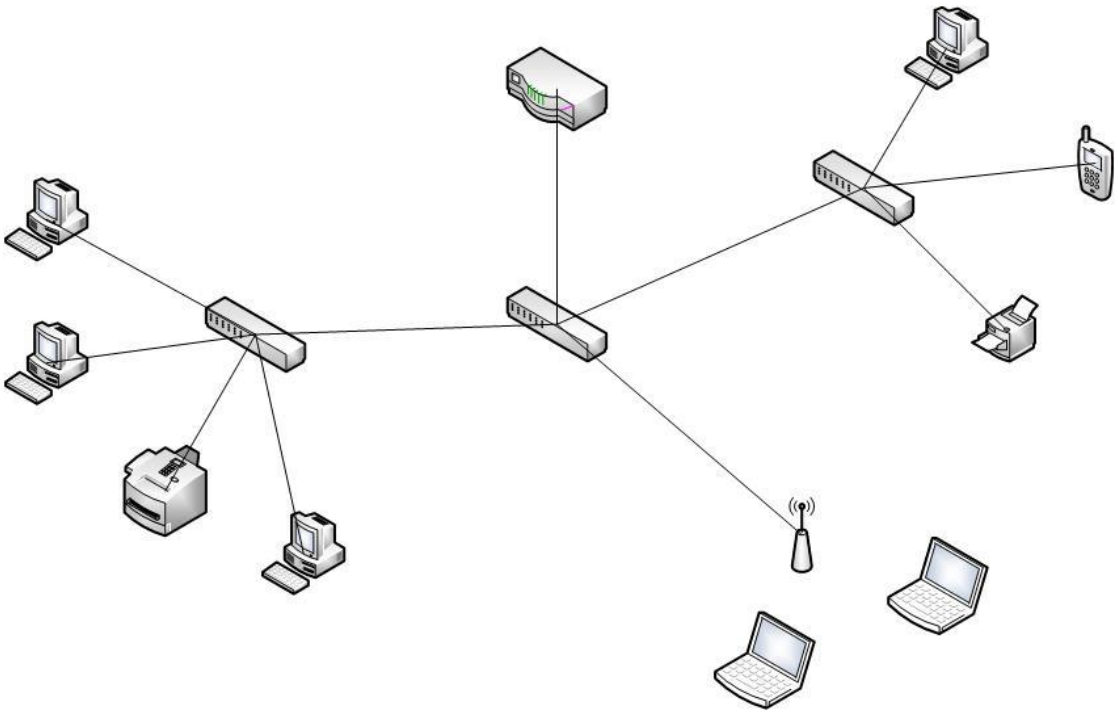
Opinnäytetyön toimeksiantaja on Kaakkois-Suomen Ammattikorkeakoulu XAMK. Työ suoritetaan Kotkan kampuksen ICTLAB-laboratorioympäristössä. Työ toteutetaan kokonaisuudessaan kevään 2018 aikana. Vastaavanlaista toteutusta on selvitetty Laurea-Leppävaaran ammattikorkeakoulussa vuona 2010 Laura Gummeruksen ja Petteri Iivosen opinnäytetyössä ”IEEE 802.1X:n todennus & käyttöönotto Fenniassa” (Gummerus & Iivonen 2010).

Opinnäytetyön tutkimusmenetelmänä on projektinomainen kehittämistyö. Kyseessä on teoriaan pohjautuva toiminnallinen työ, jonka tavoitteena on luoda konkreettinen ja hyödyllinen lopputulos organisaation jo olemassa olevaan järjestelmään.

2 LÄHIVERKKO

Lähiverkko (*Local Area Network, LAN*) on tietokoneita ja muita oheislaitteita yhdistävä tietoliikenneverkko, joka toimii maantieteellisesti suhteellisen pienellä alueella. Lähiverkko kattaa normaalisti yhden tai useampia rakennuksia, kuten esimerkiksi työ- tai kouluympäristön. Lähiverkon toiminta rajoittuu maksimissaan muutamaan kilometriin, ja lähiverkot voidaan yhdistää toisiinsa kaupunkiverkoilla (*MAN, Metropolitan Area Network)*. Lähiverkko on normaalisti yhden organisaation hallinnoima. (Puska 2000, 12.)

Lähiverkon etuna on tehokas resurssien jako verkon käyttäjien kesken. Samassa lähiverkossa toimivat laitteet voivat jakaa yhteisiä resursseja, kuten tietokanta- tai tulostinpalveluita, tai yhteisessä käytössä olevia verkkolevyjä. Lähiverkkojen avulla jaettuja resursseja voidaan yksilöidä esimerkiksi osastojen mukaan: myynnin henkilöstö pääsee käsiksi vain heille tarkoitettuihin resursseihin ja palveluihin ja hallinnon käyttäjät omiinsa. Lähiverkkojen rakennuksessa voidaan käyttää päätelaitteita, verkon aktiivilaitteita (kuten kytkimet ja reitittimet), oheislaitteita (tulostimet, kamera, VoIP-puhelimet) sekä verkkokaapelia (parikaapeli, optinen kaapeli). Lähiverkon topologiaa on kuvattu kuvassa 1. (Puska 2000, 46–47.)



Kuva 1. Lähiverkko

2.1 Virtuaalinen lähiverkko

VLAN (*Virtual Local Area Network*) eli virtuaalinen lähiverkko tarkoittaa loogista ryhmää joka koostuu tietokoneista, palvelimista ja verkkolaitteista. VLAN:iin kuuluvat laitteet toimivat samassa lähiverkossa huolimatta niiden fyysisestä tai maantieteellisestä sijainnista, joten esimerkiksi organisaatioissa osastot voidaan jaotella virtuaalisten lähiverkkojen avulla riippumatta osastojen fyysisestä jaottelusta. Samaan kytkimeen voidaan konfiguroida useita virtuaalilähiverkkoja, jonka avulla voidaan parantaa verkon skaalautuvuutta ilman fyysisiä laitehankintoja. (Puska 2000, 104–105.)

VLAN-verkko voidaan toteuttaa kahdella eri menetelmällä:

- **Porttipohjainen VLAN**. Työaseman VLAN-jäsenyys määritellään suoraan kytkimen liitäntäporttiin. Tällöin porttiin kytketty työasema liittyy aina ennalta määrättyyn VLAN:iin. Jos käyttäjä siirtyy toiseen työpisteeseen, on tarvittavat määrittelyt oltava myös toisessa kytkimessä. Tällaista VLAN:ia kutsutaan myös staattiseksi VLAN:ksi.
- **MAC-osoitteeseen perustuva VLAN**. VLAN-jäsenyys määritellään liitettävän työaseman verkkokortin MAC-osoitteen mukaan. Tällöin käyttäjän siirtyessä toiseen paikkaan, ei kytkinten konfiguraatioita tarvitse muuttaa. Muuttuvissa työympäristöissä MAC-osoitteeseen perustuva dynaaminen VLAN on ylläpidon kannalta järkevämpi toteutustapa. (Hakala, Vainio & Vuorinen 2006, 232–243.)

2.2 OSI-malli

OSI-malli (*Open Systems Interconnection Reference Model)* on ISO-järjestön (*International Organization for Standardization)* vuonna 1983 kehittämä viitemalli, joka kuvaa tiedonsiirtoprotokollien arkkitehtuuria seitsemässä kerroksessa (kuva 2). OSI-malli ei ole protokolla, vaan viitekehys tietoliikenteen ja protokollien suunnittelulle jonka tavoitteena on yhtenäistää tietoliikennejärjestelmien suunnittelua. OSI-malli on kuvattu pyramidimaisesti seitsemään kerrokseen, jossa jokainen kerros kommunikoi ainoastaan yhtä alemman ja yhtä ylemmän kerroksen kanssa. (Tampere University of Technology 2002.)

OSI-Mallin kerrokset (alhaalta ylöspäin kuvattuna) ovat:

1. **Fyysinen kerros (physical layer)**
   OSI-Mallin alin kerros, Fyysinen kerros määrittelee tiedonsiirron fyysiset ominaisuudet, kuten kaapeloinnit ja liittimet. Fyysisellä tasolla dataa voidaan siirtää kahdella tapaa, *Sarjamuotoisesti* jossa bitit liikkuvat yksi kerrallaan peräkkäin sekä *Rinnakkaismuotoisesti* jolloin kaikki yhden merkin bitit siirtyvät yhdenaikaisesti kukin omaa johdintaan pitkin.
2. **Siirtoyhteyskerros (link layer)**
   Siirtoyhteyskerros on vastuussa päätepisteiden välisen yhteyden luomisesta, yhteyden purkamisesta sekä fyysisellä kerroksella tapahtuneiden virheiden korjaamisesta. Tämän lisäksi siirtoyhteyskerros pitää huolta, ettei dataa lähetetä nopeammin kuin vastaanottaja pystyy sitä käsittelemään.
3. **Verkkokerros (network layer)**
   Verkkokerros tarjoaa ylemmille kerroksille yhteyden, joka ei ole riippuvainen verkon rakenteesta. Toisin sanoen verkkokerroksen tehtävänä on ”piilottaa” verkon fyysiseen toteutukseen liittyvät piirteet. Verkkokerros on myös vastuussa pakettien reitityksestä.
4. **Kuljetuskerros (transport layer)**
   Kuljetuskerroksen tehtävänä on tarjota luotettava päästä-päähän- eli point-to-point yhteys, jota pitkin OSI-mallin ylemmät kerrokset voivat siirtää dataa. Alemman kerroksen (*verkkokerros)* tehtävänä on pitää huolta kahden päätelaitteen kommunikaatiosta verkon eri osissa, kun taas kuljetuskerros muodostaa koneiden välille varsinaisen yhteyden. Kuljetuskerroksen tehtävänä on myös huolehtia siitä, että esim. vikatilanteen sattuessa yhteys alkaa käyttää vaihtoehtoista reittiä.
5. **Istuntokerros (session layer)**
   Istuntokerros (tai yhteysjaksokerros) muodostaa yhteyden koneiden välille verkon yli. Istuntokerroksen tehtäviin kuuluu myös erilaisten datavirtojen synkronointi, sekä tarvittaessa tiedon salaaminen. Istuntokerros pitää myös huolta siitä, että tiedonsiirto ei sekoa esimerkiksi fyysisen yhteyden katketessa (*Ylläpito*).
6. **Esitystapakerros (presentation layer)**
   Esitystapakerroksen tehtävänä on huolehtia, että lähetetty data on sellaisessa muodossa, jota myös datan vastaanottaja ymmärtää. Esitystapakerroksella sovitaan missä muodossa esim. kuva ja ääni esitetään. Esitystapakerroksella voidaan myös hoitaa tiedon salaaminen ja salauksen purkaminen.
7. **Sovelluskerros (application layer)**
   Sovelluskerroksen tehtävänä on tarjota rajapinnat sovelluksille, joita ne käyttävät viestintään. Toisin sanoen sovelluskerros toimii linkkinä tiedonsiirtoa tarvitsevalle ohjelmalle, esimerkiksi sähköpostille. (Kouvolan Seudun Ammattiopisto 2010.)

Kuva 2. OSI-Mallin kerrosrakenne (OSI-Malli 2010.)

2.3 Tietoturva

Tietoturvallisuus on tärkeä osa organisaatioiden toiminnan laatua. Yksinkertaisesti sanottuna tietoturvalla pyritään siihen, että tietojärjestelmät sekä tiedot ovat saatavilla vain niiden käyttöön oikeutetuille henkilöille. Perinteisesti tietoturvallisuus voidaan määritellä tiedon arvoon perustuen kolmeen eri osa-alueeseen: käytettävyys (availability), luottamuksellisuus (confidentiality) sekä eheys (integrity). (Hakala ym. 2006, 4.)

Tiedon käytettävyydellä pyritään siihen, että tieto- sekä tietojärjestelmät ovat saatavilla oikeassa muodossa silloin kuin niitä tarvitaan. Käytettävyyttä voidaan ylläpitää huolehtimalla tietojärjestelmien riittävästä kapasiteetista sekä ohjelmien sopivuudesta tarvittavien tietojen käsittelyyn. (Hakala ym. 2006, 4.)

Luottamuksellisuuden tarkoituksena on taata, että tiedot ovat saatavilla vain niille oikeutetuille henkilöille tai organisaatioille. Tiedon luottamuksellisuutta voidaan parantaa esimerkiksi suojaamalla järjestelmien laitteet ja tietokannat salasanoilla. Arkaluontoisen materiaalin salauksessa voidaan hyödyntää myös erilaisia salakirjoitusmenetelmiä. (Hakala ym. 2006, 5.)

Tiedon eheys tarkoittaa yksinkertaisesti selitettynä sitä, että informaatio pysyy muokkaamattomana ja sitä ei pääse muokkaamaan ilman riittäviä valtuuksia. Eheyden tavoitteena on myös estää tahattomien virheiden synty tietoihin tai

tietojärjestelmiin. Eheyttä voidaan ylläpitää ohjelmistoteknisesti käyttämällä esimerkiksi syöttörajoituksia ja käyttäjän syötteen tarkistuksia. Fyysisellä puolella eheyttä voidaan ylläpitää käyttämällä erilaisia virheenkorjaavia komponentteja. (Hakala ym. 2006, 4–5.)

Kyseistä kolmeen osatekijään perustuvaa tietoturvan määritelmää pidetään nykyään riittämättömänä, sillä se ei huomioi tiedon käsittelijän identiteettiä tai käytettyjen tietojärjestelmien arvoa riittävästi. Klassisen tiedon arvoon perustuvan määritelmän lisäksi puhutaan *laajennetusta tietoturvallisuuden määritelmästä*, joka käsittää aiempien kolmen osatekijän lisäksi kiistämättömyyden (non-repudiation) sekä pääsynvalvonnan (access control). (Hakala ym. 2006, 5.)

Kiistämättömyyden tarkoituksena on tunnistaa järjestelmää käyttävä henkilö luotettavasti, sekä tallentaa käyttäjän tiedot järjestelmään. Tiedon kiistämättömyyttä voidaan parantaa käyttämällä salaukseen perustuvia tunnistemekanismeja, kuten älykortteja tai RFID-tunnisteita. (Hakala ym. 2006, 4–5.)

Pääsynvalvonnalla pyritään turvaamaan tietojenkäsittelyinfrastruktuurin käyttöä. Organisaatioiden pääsynvalvonnan tehtävänä on varmistaa, ettei luvattomat käyttäjät pääse käyttämään organisaation tietojärjestelmiä tai yhteyksiä omiin käyttötarkoituksiinsa. Pääsynvalvonnan tärkeys on lisääntynyt viimeisten vuosien varrella, kun langattomat verkot ovat yleistyneet huomattavasti. (Hakala ym. 2006, 6–8.)

2.4 AAA-malli

AAA-malli on verkon käyttäjän tunnistamiseen käytettävä kehysmalli. Mallin nimi koostuu sanoista Authentication (autentikointi), Authorization (valtuutus) ja Accounting (tilastointi/kirjaaminen). AAA-mallin tarkoituksena on varmistaa käyttäjän identiteetti, sallia tai estää pääsy kohdeverkkoon sekä pitää kirjaa käyttäjän toimista verkossa. (Carroll 2004, 5.)

Autentikointipalvelun tehtävänä on tunnistaa kohdeverkkoon pyrkivä käyttäjä. Tunnistus voi tapahtua yksinkertaisella käyttäjänimi/salasana-yhdistelmällä,

digitaalisella sertifikaatilla, kertakäyttöisellä avaimella tai jopa puhelinnumerolla. Tämä riippuu kohdeverkon määrittelyistä ja siitä, millaista autentikointitapaa käytetään. (Carroll 2004, 6.)

Valtuutusprosessin aikana todennetulle käyttäjälle voidaan antaa tai evätä pääsy tiettyihin palveluihin tai verkon osiin. Toisin sanoen valtuutuksen avulla käyttäjiä ja heidän pääsyä tiettyihin palveluihin voidaan profiloida. Profilointi voi perustua esimerkiksi fyysiseen sijaintiin, käyttäjätasoon tai kellonaikaan. Esimerkiksi yritysverkossa kirjanpidossa työskentelevä kirjanpitäjä saa pääsyn kirjanpidolle tarkoitettuun verkkoon, mutta ei myynnin puolelle. (Carroll 2004, 8.)

Tilastoinnin avulla voidaan kerätä tietoja verkon käyttäjistä. Tilastoon kerättäviä tietoja voivat olla mm. käyttäjätunnus, IP-osoite, yhteysaika sekä käytetyt palvelut. Tilastointia voidaan käyttää myös apuna tutkittaessa esimerkiksi verkon kuormitusta. (Carroll 2004, 10–11.)

3 IEEE 802 -STANDARDI

IEEE 802 on standardointijärjestö IEEE:n (*Institute of Electrial and Electronics Engineers)* työryhmä joka kehittää ja ylläpitää lähi(*LAN)*- ja kaupunkiverkkojen (*MAN)* standardeja. 802-työryhmän standardien tarkoituksena on määritellä vaihtoehtoisia lähiverkkototeutuksia sekä yhtenäisen rajapinnan erilaisille lähiverkoille. (Puska 2000, 21.)

IEEE 802 -työryhmän standardiperheeseen kuuluu useita eri standardeja, jotka merkitään 802.x-tyylisesti. Jokaiselle osa-alueelle on oma työryhmänsä, joka keskittyy sen standardin kehitykseen. Tunnetuimpia 802.x-standardeja ovat mm. Ethernet ja WLAN. (IEEE Standards 2017.)

Aktiivisia 802.x-työryhmiä ovat mm.

IEEE 802.1	yleiset LAN-standardit (802.1D STP, 802.1Q VLAN sekä tässä opinnäytetyössä tarkemmin tutkittu 802.1X)
IEEE 802.3	Ethernet

IEEE 802.11	Langattomat lähiverkot (*WLAN,* sisältää monia alastandardeja kuten 802.11a, 802.11b, 802.11ac, 802.11ad, jotka määrittelevät erilaisia WLAN-tekniikoita.)
IEEE 802.16	Langaton laajakaista (WiMAX)
IEEE 802. 22	Langattomat alueelliset verkot (*Wireless Regional Area Networks)* (IEEE Standards 2017.)

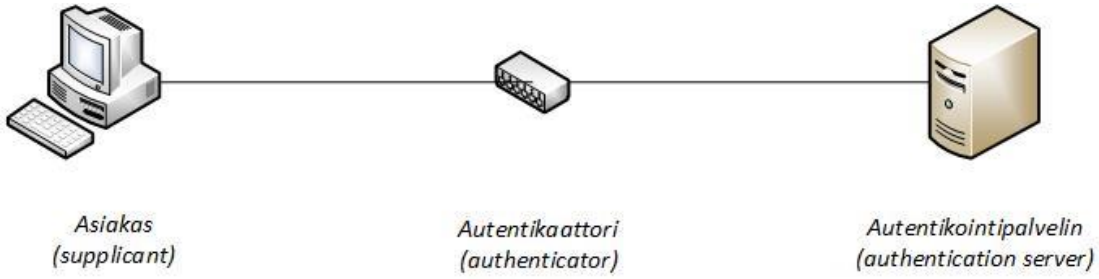
3.1 802.1X

IEEE:n 802.1X on lähiverkossa toimiva standardi, joka määrittelee asiakkaan ja palvelimen välisen porttikohtaisen todennuksen. 802.1X-standardin tarkoituksena on parantaa käyttöympäristön tietoturvaa estämällä luvattomien käyttäjien ja laitteiden pääsy kohdeverkkoon. 802.1X-porttikohtaista todennusta voidaan hyödyntää niin langattomissa (*WLAN)* kuin langallisissakin (*ethernet)* verkoissa. (Geier 2008, 33.)

Porttikohtaisen todennuksen avulla voidaan parantaa verkon tietoturvaa huomattavasti, sillä käyttäjien ja päätelaitteiden pääsyä verkkoon voidaan hallita ja tarkkailla monipuolisesti. Ilman porttipohjaista todennusta potentiaalinen hakkeri voisi käytännössä kytkeä oman koneensa yrityksen ethernet-porttiin ja saada pääsyn yrityksen sisäverkkoon ja sen tiedostoihin. Porttikohtaisen todennuksen avulla ainoastaan autentikoidut käyttäjät/päätelaitteet saavat pääsyn verkkoon, jolloin pelkkä verkkojohdon liittäminen tietokoneeseen ei enää riitä.

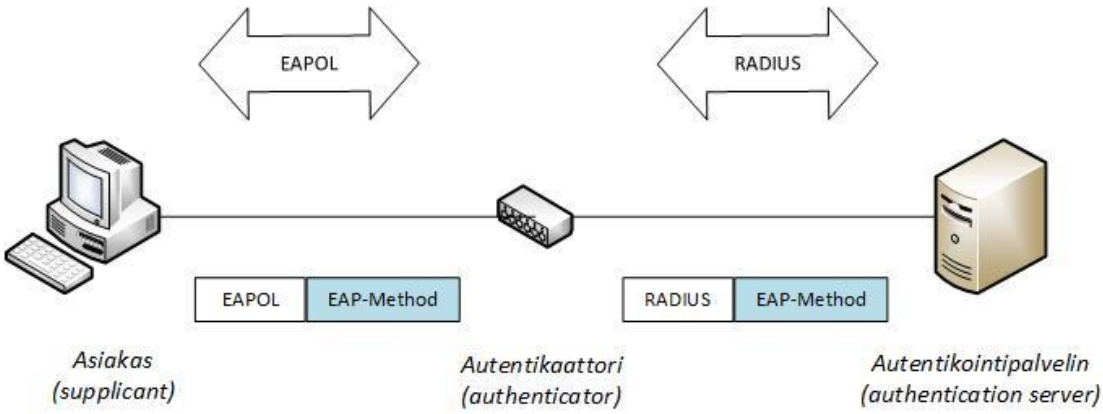
802.1X:n toiminta perustuu kolmeen komponenttiin (kuva 3): asiakas (*supplicant)*, autentikaattori (*authenticator)* ja autentikointipalvelin (*authentication server).* Asiakas on todennusta pyytävä päätelaite tai käyttäjä, joka haluaa pääsyn verkkoon. Autentikaattori on asiakkaan ja autentikointipalvelimen välissä oleva aktiivilaite kuten kytkin tai langaton tukiasema, joka toimii OSI-mallin toisella kerroksella. Autentikaattorin tehtävänä on toimia välikätenä asiakkaan ja autentikointipalvelimen välisessä kommunikoinnissa. Suurimmassa osassa toteutuksista autentikointipalvelimena toimii RADIUS-palvelin, joka suorittaa itse

autentikoinnin. Palvelin pitää sisällään käyttäjien ja päätelaitteiden tunnistetiedot ja asiakkaasta riippuen antaa tai evää pääsyn verkkoon. (Geier 2008. 38.)



Kuva 3. IEEE 802.1x standardin komponentit

Komponentit keskustelevat keskenään käyttäen EAP-Method-viestejä, jotka kuljetetaan komponenttien välillä käyttäen EAPOL- ja RADIUS-protokollia. Asiakkaan ja autentikaattorin välinen viestintä tapahtuu EAPOL-protokollan avulla, kun taas autentikaattorin ja autentikointipalvelimen välinen kommunikointi tapahtuu RADIUS-protokollan avulla (kuva 4). Molemmissa tapauksissa EAP-Method-viesti sisällytetään EAPOL/RADIUS-kehykseen kuljetusta varten.



Kuva 4. Komponenttien välinen viestintä.

EAP ei itsessään ole autentikointiprotokolla, vaan tarjoaa kuljetuspohjan valitulle autentikointimenetelmälle, kuten esimerkiksi EAP-TLS tai EAP-MD5, joita käydään läpi tarkemmin luvussa 5. (Geier 2008. 44.)

3.2 Todennusprosessi

Todennusprosessin ensimmäisessä vaiheessa asiakas (supplicant) kytketään 802.1X-porttitodennusta käyttävän kohdeverkon porttiin. Ennen autentikoinnin alkamista portti on luvaton-tilassa, jossa kaikki muu paitsi 802.1X-liikenne on estetty. Kun autentikaattorina toimiva kytkin (authenticator) huomaa liikennettä portissa, se lähettää EAPOL-pakettiin kapseloidun EAP-Request Identity -kyselyn asiakaslaitteelle.

Toisessa vaiheessa asiakaslaite vastaa kytkimen viestiin EAP-Response Identity -viestillä, joka sisältää asiakkaan tunnistetiedot. Mikäli kytkin ei saa vastausta kyselyynsä, se odottaa määritellyn ajan ennen kuin yrittää uudelleen. Jos vastausta ei useasta yrityksestä huolimatta tule, kytkin sulkee portin liikenteeltä ja estää näin pääsyn verkkoon.

Kolmannessa vaiheessa, kytkimen vastaanotettua asiakkaan EAP-Response Identity -viestin, se etsii IP-osoitteen perustella sille määritellyn autentikointipalvelimen (useimmissa tapauksessa RADIUS-palvelimen). EAP-Response Identity -viesti paketoidaan RADIUS-Access Request -viestiin ja uudelleen lähetetään autentikointipalvelimelle tietojen tarkistusta varten.

Todennuksen neljännessä vaiheessa autentikointipalvelin vertaa vastaanottamaansa tunnistetietoja sisältävää viestiä palvelimella sijaitseviin tietokantoihin ja päättää sen perusteella hylätäänkö pääsy verkkoon vai jatketaanko tunnistautumisprosessia. Mikäli tunnistetiedot eivät vastaa palvelimella oleviin tietoihin, se vastaa kytkimelle viestillä RADIUS-Access Reject, jonka jälkeen kytkin välittää asiakkaalle EAP-Failure-viestin ja pääsy verkkoon estetään.

Prosessin viidennessä vaiheessa autentikointipalvelin lähettää kytkimelle RADIUS-Access Challenge -viestin, joka sisältää todennuksessa käytettäviä määrityksiä, kuten käytetyn EAP-tunnistemenetelmän. Kytkin paketoi viestin EAPOL-kehykseen ja lähettää asiakkaalle EAP-Request Identity -viestin. Asiakas vastaa EAP-Response Identity -viestillä, joka taas paketoidaan RADIUS-

kehykseen ja toimitetaan autentikointipalvelimelle. Määrityksistä ja todennustavasta riippuen tätä kytkimen välityksellä tapahtumaa viestintää jatketaan, kunnes palvelin on saanut riittävän tarkan kuvan asiakkaasta.

Prosessin kuudennessa vaiheessa, kun autentikointipalvelin on varmistunut asiakkaan pääsyoikeudesta verkkoon, se lähettää kytkimelle RADIUS-Access Accept -viestin, jonka kytkin toimittaa asiakkaalle EAP-Success-viestillä ja asiakkaalle myönnetään pääsy kohdeverkkoon. (Geier 2008, 45–49.)

3.3 802.1X:n vaatimukset

Toimiakseen 802.1X-todennus vaatii minimissään edellä mainitut kolme komponenttia (asiakas, autentikaattori sekä autentikointipalvelin), joille on myös tiettyjä vaatimuksia.

Microsoftin käyttöjärjestelmissä on sisäänrakennettu tuki 802.1X:lle Windows XP -versiosta lähtien. OS X -käyttöjärjestelmissä tuki löytyy versiosta 10.3.-lähtien. Linux-käyttöjärjestelmät vaativat erillisen ohjelmiston kuten XSupplicant tai wpa_supplicant. Myös Windows-käyttöjärjestelmissä on mahdollista käyttää erillistä ohjelmistoa kuten Cisco Secure Services Client. (Cisco 2011.)

Autentikaattorina toimii yleisimmin kytkin. Kytkimen on oltava 802.1X-yhteensopiva ja sen on kyettävä keskustelemaan RADIUS-palvelimen kanssa. (Cisco 2011.)

Autentikointipalvelimena käytetään yleisesti RADIUS-palvelinta. Microsoft-ympäristössä RADIUS-palvelimena toimii yleensä Windows Serverin NPS-palvelu, kun taas Linuxille on saatavissa esimerkiksi vapaan lähdekoodin FreeRadius. (SANS Institute. 2012.) Tämän työn toteutus sijoittuu Windows-ympäristöön, joten työssä käsitellään pääasiassa Windows Serverin NPS-palvelua.

Koska tämä työ rakentuu tiivisti Active Directory -toimialueen ja sen käyttäjien yhteyteen, on Active Directory -toimialuepalvelun toiminta oleellista työn

onnistumiselle. 802.1X-autentikointi voidaan suorittaa joko käyttäjä/salasana-yhdistelmällä tai varmenteella. Varmenteiden hallintaan vaaditaan Windows Serverin *Active Directory Certificate Services* -palvelu. Näiden lisäksi palvelimella tulee olla asennettuna *Network Policy Server* (NPS) joka toimii RADIUS-palvelimena ja vertaa käyttäjien todennustietoja aktiivihakemistosta löytyviin käyttäjätietoihin. (SANS Institute 2012.)

3.4 802.1X-todennuksen hyödyt ja rajoitukset

Oikein konfiguroituna todennus tarjoaa kohdeverkolle useita hyötyjä. 802.1X -todennus tarjoaa paremman näkyvyyden verkolle ja sen käyttäjille, sillä verkon käyttäjä linkittyy IP-osoitteeseen, MAC-osoitteeseen, käytettyyn kytkimeen sekä sen porttiin. Tätä voidaan hyödyntää esimerkiksi verkon käytön valvonnassa, tilastoinnissa sekä vianetsinnässä. (Cisco 2011.)

Turvallisuuden puolesta 802.1X on vahvin todennustapa verkon käyttäjille. Porttikohtainen todennus toimii OSI-mallin toisella kerroksella, joten pääsyä verkkoon voidaan hallita suoraan liityntäpisteestä. Koska käyttäjän tunnistus tehdään suoraan kytkimen liityntäportissa, käyttäjä jolla ei ole oikeutta kohdeverkkoon voidaan uudelleenohjata esimerkiksi rajoitettuun vieras-VLAN:iin. VLAN:ien lisäksi käyttäjien pääsyä verkon eri osiin voidaan rajoittaa pääsylistojen avulla. (Cisco 2011.)

802.1X -todennuksen avulla voidaan myös jakaa kustomoituja palveluja verkon eri käyttäjille. Käyttäjä voidaan esimerkiksi valtuuttaa tiettyyn VLAN:iin jossa käyttäjälle tarjotaan tiettyjä palveluita. (Cisco 2011.)

Yksi todennuksen tarjoama hyöty on myös näkymättömyys käyttäjälle. Oikein konfiguroituna päätelaitteen käyttäjä ei edes huomaa 802.1X-todennuksen olemassaoloa. (Cisco 2011.)

Todennuksen käyttöön liittyy myös rajoituksia. Vanhemmat tai yhteensopimattomat laitteet joissa ei ole tukea 802.1X-protokollalle, eivät saa yhteyttä verkkoon. Tällaisia laitteita ovat mm. Vanhat käyttöjärjestelmät (Windows XP tai sitä vanhemmat käyttöjärjestelmät), Linux-käyttöjärjestelmät ilman erillistä

802.1X-yhteysohjelmaa sekä oheislaitteet, kuten tulostimet. Tällaisia laitteita varten on suositeltavaa konfiguroida esimerkiksi *MAC Authentication Bypass* -todennus, joka 802.1X-todennuksen epäonnistuessa suorittaa todennuksen asiakkaan MAC-osoitteen perusteella. Päätelaitteiden lisäksi myös autentikaattoreina toimivien kytkimien on oltava 802.1X- ja RADIUS-yhteensopivia. (Bradford Networks 2013.)

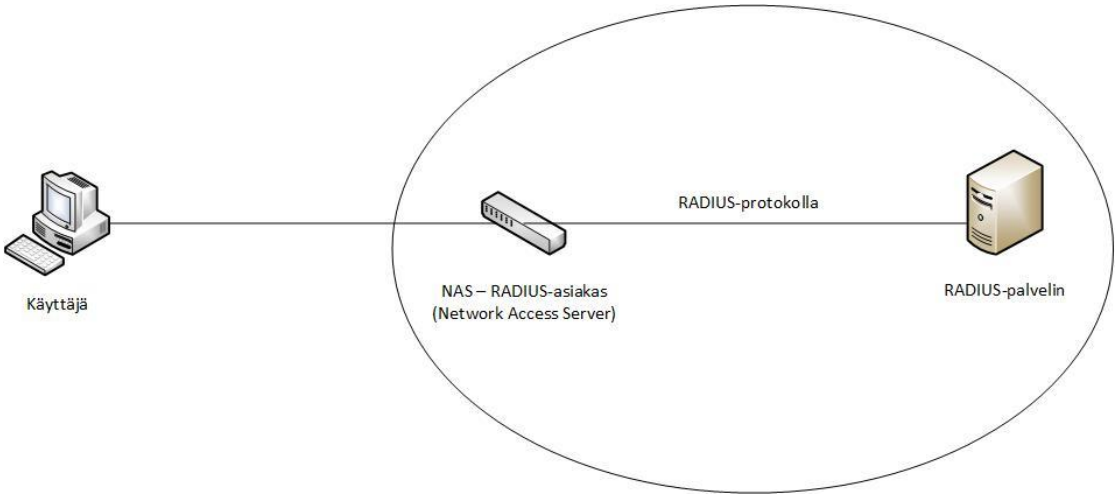
4 MUUT TYÖHÖN LIITTYVÄT PROTOKOLLAT

802.1X-porttipohjainen todennus hyödyntää useita varmennus- ja tiedonsiirtoprotokollia, kuten RADIUS, EAPOL ja EAP.

4.1 RADIUS

RADIUS (*Remote Authentication Dial-In User Service*) on Livingston Enterprisesin alun perin vuonna 1991 suunnittelema käyttäjien sekä laitteiden todennukseen tarkoitettu tiedonsiirtoprotokolla. RADIUS-protokollan avulla voidaan toteuttaa AAA-mallin mukainen käyttäjän autentikointi, valtuutus sekä tilastointi. (Microsoft 2018.)

RADIUS-protokollan toiminta perustuu asiakas-palvelin-yhteyteen. NAS (*Network Access Server*) tarkoittaa verkon laitetta, joka on määritelty RADIUS-asiakkaaksi (*RADIUS-Client*). NAS voi olla esimerkiksi lähiverkon 802.1X-yhteensopiva kytkin tai WLAN-tukiasema. Palvelimia jotka tukevat RADIUS-protokollaa kutsutaan yleensä RADIUS-palvelimiksi. RADIUS-palvelimena voi toimia esimeriksi Linux-palvelimilla ajettava *FreeRadius*-ohjelmisto tai Windows Serverin NPS-palvelu. RADIUS-protokolla toimii vain asiakkaan ja palvelimen välillä (kuva 5), eikä esimerkiksi verkon ulkoreunalla olevia päätelaitteita huomioida. (Cisco 2006.)



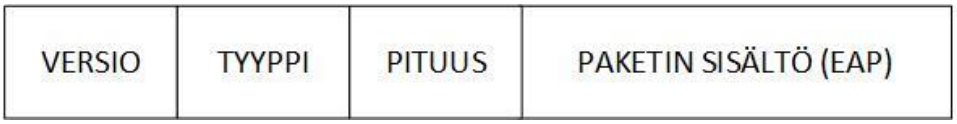
Kuva 5. RADIUS-protokolla.

4.2 EAPOL

EAPOL (*Extensible Authentication Protocol over LAN*) on 802.1X-standardissa käytetty paketointitekniikka jonka avulla kuljetetaan EAP-protokollan datapaketteja. EAPOL toimii pääasiallisena yhteysväylänä asiakkaan ja autentikaattorin välillä, kun taas autentikaattorin ja autentikointipalvelimen välinen kommunikointi tapahtuu RADIUS-protokollan avulla. EAPOL toimii OSI-mallin toisella kerroksella ja tukee tiedonsiirtoa ethernet- ja WLAN-verkoissa. Ennen asiakkaan tunnistautumista ainoastaan EAPOL-liikenne on sallittu asiakkaan ja autentikaattorin välillä. (Geier 2008, 55.)

802.1X-todennuksen komponenttien välisen liikenteen tärkeimpänä tehtävänä on kuljettaa EAP-Method Data -paketteja jotka sisältävät valitun todennusmekanismin tietoja. Method Data -termi viittaa käytettyyn todennustapaan, esimeriksi EAP-MD5 tai EAP-TLS, joten EAP-Method Data on yleisnimitys EAP-protokollan paketeille. EAP-Method Data -paketit kapseloidaan EAP-paketteihin, jotka taas kapseloidaan EAPOL-paketteihin tiedonsiirtoa varten. (Geier 2008, 56–57.)

Kapseloidessa EAP-pakettia EAPOL lisää pakettiin kolme ylimääräistä kenttää joita tarvitaan EAP-pakettien kuljettamiseen. EAPOL-paketin rakenne on suhteellisen yksinkertainen ja sitä on kuvattu kuvassa 6.



Kuva 6. EAPOL-paketin rakenne

Versio-kenttä määrittelee EAPOL-protokollan version, jota paketin lähettäjä tukee. 802.1X-toteutuksissa versio-kentän arvo on aina ”0000 0002”. (Geier 2008, 57.)

Pituus-kenttä määrittelee paketin sisältö (EAP)-kentän pituuden joka esitetään binäärilukuna. Pituus-kentän koko on kahden oktetin pituinen. Esimerkkinä pituus-kentän arvo ”0000 0000 0001 1011” kertoo EAP-paketin sisältävän 27 oktettia dataa. Pituus-kentän arvona voi olla myös 0, joka tarkoittaa, että EAPOL-paketti ei sisällä ollenkaan EAP-pakettikenttää. Tällaisia paketteja ovat EAPOL-Start ja EAPOL-Logoff-paketit. (Geier 2008, 58.)

Tyyppi-kenttä määrittelee EAPOL-paketin käyttötarkoituksen. Erilaisia EAPOL-paketteja on viisi kappaletta:

Paketin tyyppi	Tyyppi-kentän arvo	Binääriarvo
EAPOL-EAP Packet	0	0000 0000
EAPOL-Start	1	0000 0001
EAPOL-Logoff	2	0000 0010
EAPOL-Key	3	0000 0011
EAPOL-Encapsulated-ASF-Alert	4	0000 0100

Taulukko 1. EAPOL-pakettityypit.

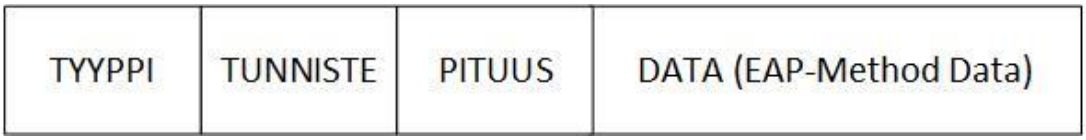
EAP-Packet (tyypin ”0” paketti) sisältää nimensä mukaisesti EAP-paketin. EAP-paketissa kuljetetaan todennukseen tarvittua EAP-Method Data -tietoa. Suurin osa EAPOL-protokollan avulla kulkevista paketeista ovat tyypin 0 EAP-paketteja. Tyypin 1 *EAPOL-Start*-pakettia käytetään tilanteessa jossa autentikaattorina toimiva kytkin ei jostain syystä ole huomannut asiakkaan liittymistä verkkoon. Asiakaskone lähettää kytkimelle *EAPOL-Start*-pyynnön, jolloin kytkin aloittaa todennusprosessin. *EAPOL-Logoff*-paketin tarkoituksena on ilmoittaa autentikaattorille käyttäjän poistuvan verkosta, jolloin käytetty liityntäportti

voidaan muuttaa ei-todennettuun (*unauthorized*) tilaan. *EAPOL-Key*-pakettia käytetään salausavainten vaihtoon asiakkaan ja autentikaattorin välillä, mikäli käytetty 802.1X-konfiguraatio niitä vaatii. *EAPOL-Encapsulated-ASF-Alert*-pakettia käytetään *Alert Standard Forum* -sanomien (ASF) lähettämiseen portin läpi joka on ei-todennetussa tilassa. (Geier 2008, 58–64.)

4.3 EAP

EAP (*Extensible Authentication Protocol*) on todennuksessa käytettävä viitekehys, jonka avulla kuljetetaan todennukseen käytettäviä EAP-Method Data -viestejä. EAP ei itsessään siis ole todennusmekanismi, vaan se tarjoaa rungon käytetyn todennustavan (EAP-tyyppi) tiedonsiirtoon. Nimensä mukaisesti se on joustava protokolla, joka tukee monia erilaisia todennusmenetelmiä, kuten EAP-TLS, PEAP, LEAP, EAP-MD5 ja EAP-MS-CHAPv2. (Hucaby 2014. 292–294.)

EAP-paketin rakenne on EAPOL-paketin tavoin hyvin yksinkertainen ja se sisältää neljä kenttää. EAP-paketin rakennetta on kuvattu kuvassa 7.



Kuva 7. EAP-Paketin rakenne.

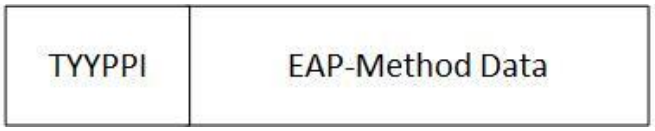
Tyyppi-kenttä kertoo, minkälaisesta EAP-paketista on kyse. EAP-paketteja on olemassa neljä erilaista ja tyyppi-kentän arvo on esitettynä binäärilukuna taulukon 2 mukaisesti. Kaikki EAP-paketit eivät sisällä Data-kenttää, sillä ainoastaan EAP-Request ja EAP-Request sisältävät Data-kentän joka, pitää sisällään EAP-Method Data-tunnistetietoja. Autentikaattori ja asiakas vaihtavat tunnistetietoja keskenään näiden viestien avulla. EAP-Success ja EAP-Failure-paketteja käytetään onnistuneen tai epäonnistuneen todennuksen jälkeen, kun autentikaattorina toimiva kytkin toimittaa tiedon todennuksesta asiakkaalle. (Geier 2008, 64–67.)

Paketin tyyppi	Tyyppi-kentän arvo	Binääriarvo
EAP-Request	1	0000 0001
EAP-Response	2	0000 0010
EAP-Success	3	0000 0011
EAP-Failure	4	0000 0100

Taulukko 2. EAP-pakettityypit

EAP-paketin tunniste-kentän arvon avulla voidaan verrata EAP-Response-pakettia EAP-Request-pakettiin ja varmistaa että asiakas vastaa oikeaan EAP-Request-pyyntöön. Esimerkiksi, jos autentikointipalvelimelta tuleva EAP-Request-paketti sisältää tunnistearvon ”0000 0101”, vastaa asiakas EAP-Response-paketilla jonka tunnistearvo on sama ”0000 0101” (Geier 2008, 64.). Pituus-kentän arvo kertoo DATA-kentässä olevan EAP-paketin koon. Samoin kun EAPOL-paketeissa, voi pituus-kentän arvo olla 0 joka tarkoittaa, ettei paketti sisällä ollenkaan EAP Method -dataa. DATA-kenttä sisältää todennuksessa käytetyn EAP-Method Data -tiedon. (Geier 2008, 66)

EAP-paketin sisältämä DATA-kenttä jakautuu kahteen kenttään (kuva 8), joista muodostuu kyseinen EAP-Method Data-paketti.



Kuva 8. EAP-Method Data-paketti.

Tyyppi-kenttä määrittelee, mikä EAP-todennustyyppi on käytössä ja EAP-Method Data pitää nimensä mukaisesti sisällään todennukseen käytettävää tietoa. Tieto vaihtelee todennustavasta riippuen, mutta se voi pitää sisällänsä esimerkiksi digitaalisen varmenteen tai käyttäjän kirjautumistiedot. (Geier 2008, 96.)

4.3.1 EAP-MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2 eli MS-CHAPv2 on todentamiseen käytetty protokolla, joka tukee molempien osapuolien (asiakkaan ja palvelimen) todentamista eli niin sanottua kaksisuuntaista autentikointia. Nimessä oleva EAP tarkoittaa EAP-protokollaa, jonka avulla todennustiedot kulkevat asiakkaan ja autentikointipalvelimen välillä. MS-

CHAPv2-protokolla käyttää eri salausavaimia viestien vastaanottoon ja lähetykseen, mikä lisää protokollan tietoturvaa. MS-CHAPv2 tarjoaa myös käyttäjälle mahdollisuuden vaihtaa salasanansa. (Microsoft 2008.)

4.3.2 EAP-TLS

EAP-TLS (*EAP with Transport Layer Security*) on todennuksessa käytetty EAP-metodi, joka MS-CHAPv2:n tapaan tarjoaa molempien osapuolien todennuksen. EAP-TLS hyödyntää salauksessa julkisten avainten salaustekniikkaa, joka käytännössä tarkoittaa digitaalisten sertifikaattien käyttöä todennuksessa. EAP-TLS-protokollalle on laaja tuki eri valmistajien laitteilla, ja esimerkiksi Cisco, Microsoft ja FreeRadius tukevat EAP-TLS-protokollaa RADIUS-palvelimilla. Kommunikaatio laitteiden välillä tapahtuu salatun TLS-tunnelin avulla, joka parantaa kommunikaation tietoturvaa. (Geier 2008, 109–110.)

4.4 PEAP

Protected Extensible Authentication Protocol (PEAP) ei itsessään toimi todennusprotokollana, vaan se tarjoaa lisäturvaa muille EAP-todennusprotokollille. Esimerkiksi MS-CHAPv2-todennustapaa voidaan käyttää yhdessä PEAP:in kanssa. EAP-TLS:n tavoin PEAP käyttää asiakkaan ja palvelimen väliseen tiedonsiirtoon salattua TLS-tunnelia. Salatun tunnelin käyttö parantaa tietoturvaa estämällä verkkohyökkäyksiä. (Microsoft 2009.)

5 KÄYTTÖÖNOTTO

802.1X-porttitodennuksen käyttöönotto ICTLAB-ympäristössä tapahtuu progressiivisesti kolmessa vaiheessa:

1. pilottitoteutus virtuaaliympäristössä
2. käytännön toteutus pienimuotoisesti muutamalla työasemalla
3. käyttöönoton suunnittelu kesäharjoittelijoita varten.

Ensimmäisen vaiheen tarkoituksena on harjoitella ja testata 802.1X-porttitodennuksen käyttöönottoa ja toteutusta turvallisessa virtuaaliympäristössä, jolloin vikatilanteen sattuessa verkon käyttö ei katkea, eikä muille verkon käyttäjille aiheudu häiriötilanteita.

Kun testaukset virtuaaliympäristössä on saatu onnistuneesti loppuun, siirrytään seuraavaan vaiheeseen. Tarkoituksena on valita ICTLAB:n luokkatiloista muutama, harvemmin käytetty työasema testausta varten. Näihin työasemiin otetaan käyttöön 802.1X-todennus, ja niiden toimintaa verkossa seurataan tietyn ajan.

Työn kolmannessa vaiheessa suunnitellaan yksityiskohtainen ohjeistus, jonka avulla ICTLAB kesätyöharjoittelijat voivat suorittaa 802.1X-todennuksen käyttöönoton verkkoympäristössä kesällä, kun verkon käyttöaste on huomattavasti vähäisempi.

6 TOTEUTUS VIRTUAALIYMPÄRISTÖSSÄ

6.1 Tarkoitus

Ennen käyttöönottoa todellisessa ympäristössä porttikohtaista todennusta oli tarkoitus mallintaa virtuaalisessa ympäristössä. ICTLAB-laboratorio on päivittäisessä oppilaskäytössä, joten käyttöönoton on sujuttava nopeasti ja huomaamattomasti ilman häiriöitä. Käyttöönoton harjoittelu ja tekeminen virtuaalilaboratoriossa mahdollistaa ICTLAB-ympäristön mallintamisen ja porttitodenuksen käyttöönoton harjoittelemisen siten, että mahdollisissa häiriötilanteissa muiden käyttäjien työskentely ei katkea.

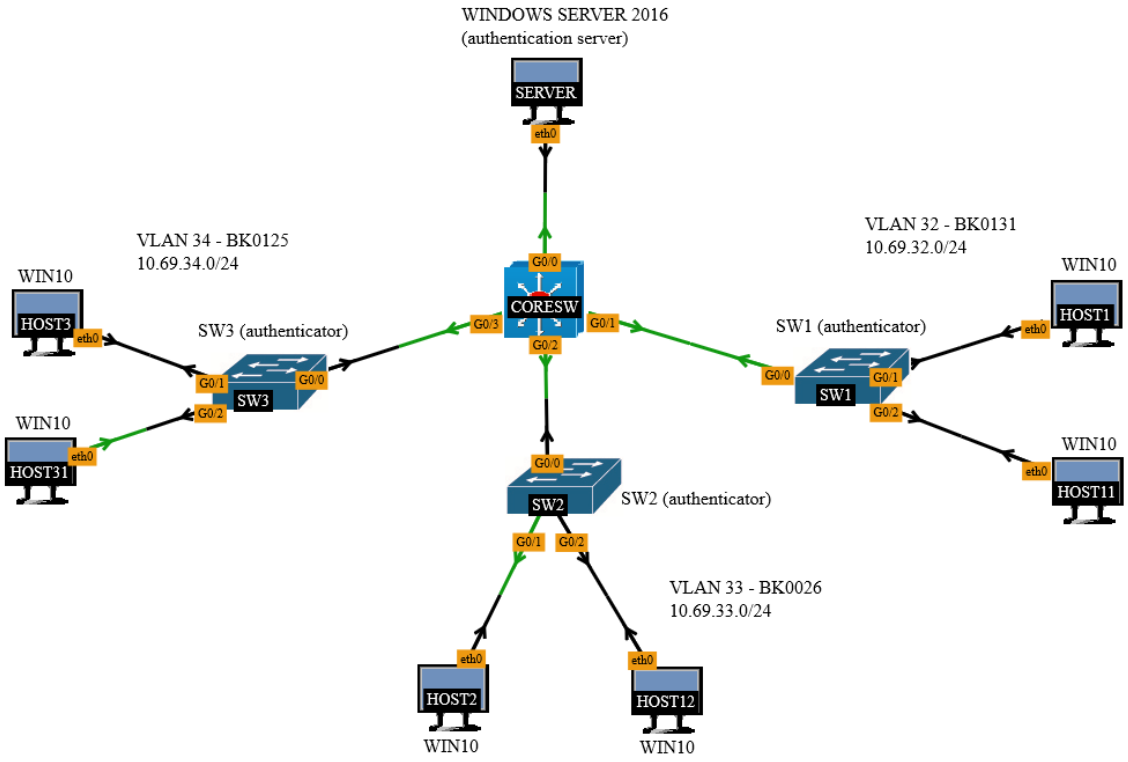
Käytännön toteutus tehdään jo valmiiseen palvelinympäristöön, jossa suurin osa vaadituista palveluista on asennettuna. Virtuaalitoteutuksen tarkoituksena oli myös tutustua 802.1X-todennuksen komponenttien määrittelyihin (asiakas, autentikaattori sekä autentikointipalvelin) sekä opiskella todennuksen käyttöönottoa täysin alusta alkaen, sillä kyseessä oli niin sanottu puhdas asennus, jossa mitään palveluita tai konfiguraatioita ei ollut valmiiksi tehtynä.

6.2 Virtuaalilaboratorio

Virtual Lab -ympäristö on Jaakko Nurmen vuonna 2016 insinöörityönä toteuttama virtualisoitu laboratorioympäristö. Virtuaalilaboratoriota hyödynnetään nykyään kattavasti tietoverkko- ja kyberturvallisuusopinnoissa. Virtuaalilaboratorion avulla oppilaat voivat harjoitella suurempienkin verkkojen konfiguroimista ilman fyysisten resurssien tuomia rajoituksia. Virtual Lab -ympäristöä hyödynnetään tietoverkko-opinnoissa mm. Advanced Switching, Network Security Equipment ja Service Provider Networks -opintojaksoilla. Kyberturvallisuuden puolella Virtual Lab -ympäristö on käytössä mm. penetraatiotestauksessa, jossa oppilaat voivat harjoitella penetraatiotestausta erilaisten valmiiden skenaarioiden avulla. (Nurmi 2016.)

6.3 Topologia

Virtuaalilaboratorioon luodun verkon topologiaa on kuvattu kuvassa 9.



Kuva 9. Virtual Lab-topologia

6.4 Valmistelut

Virtual Lab -toteutuksen tarkoituksena oli mallintaa ICTLAB-ympäristöä pienessä mittakaavassa. Laboratorion teko aloitettiin luomalla tarvitut laitteet Virtual Lab -ympäristön tyhjään laboratoriopohjaan. Harjoituksessa käytetyt laitteet olivat:

- **Windows Server 2016 -palvelin**, joka sisältää Active Directory -käyttäjät päätelaitteita varten sekä toimii RADIUS-palvelimena autentikointia varten
- **Cisco-kytkin,** joka toimii yhteyspisteenä muille kytkimille ja päätelaitteille
- **3kpl Cisco-kytkimiä,** jotka toimivat autentikaattoreina ja yhteyspisteinä päätelaitteille
- **6kpl Windows 10 -työasemia**, jotka toimivat asiakkaina.

Koska tarkoituksena oli mallintaa lähiverkon toimintaa, ei tarvetta ulkoiselle internetyhteydelle ollut.

Autentikointikytkimet ja päätelaitteet jaettiin ICTLAB-luokkatilojen mukaisesti omiin virtuaalilähiverkkoihin seuraavien osoiteavaruuksien mukaan:

- VLAN 32 - BK0131 10.69.32.0/24
- VLAN 33 - BK0026 10.69.33.0/24
- VLAN 34 - BK0125 10.69.34.0/24

Windows-palvelimelle annettiin staattinen IP-osoite 10.69.10.5, joka toimii myös verkon DNS-nimipalvelimena.

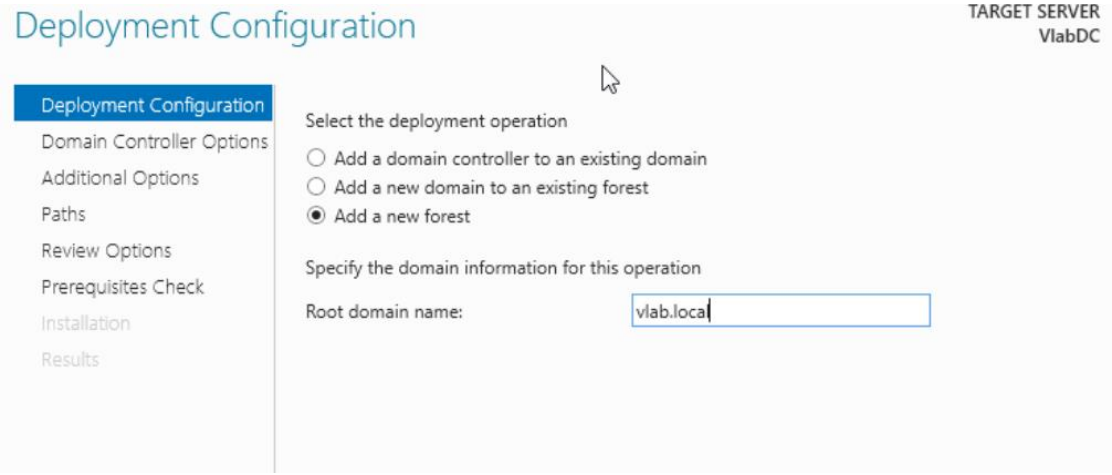
6.5 Windows-palvelin

Koska kyseessä oli Windows-palvelimen puhdas asennus, oli palvelimelle asennettava tarvittavia palveluita verkon ja porttitodennuksen toimivuuden takaamiseksi. Palvelimelle asennettiin seuraavat palvelut: *Active Directory Domain Services, Active Directory Certificate Services, DNS Server, Network Policy and Access Services (NPS),* sekä *Web Server (IIS)***.** Käytännön toteutuksessa porttikohtainen todennus otetaan käyttöön valmiiseen ja käytössä olevaan palvelinympäristöön, jossa suurin osa palveluista (kuten domain, DNS-palvelut sekä Active Directory käyttäjätiedot) on jo konfiguroitu ja toiminnassa.

Active Directory Domain Services on Windows-palvelimelle asennettava palvelinrooli, ja se toimii verkon toimialueen runkopalveluna. Aktiivihakemiston kautta voidaan lisätä toimialueelle käyttäjiä, ylläpitäjiä sekä päätelaitteita. Käyttäjiä voidaan myös jakaa omiin ryhmiinsä. Aktiivihakemiston avulla esimerkiksi käyttäjien palveluita ja pääsyä tiedostoihin voidaan rajoittaa. (Active Directory Domain Services 2018.)

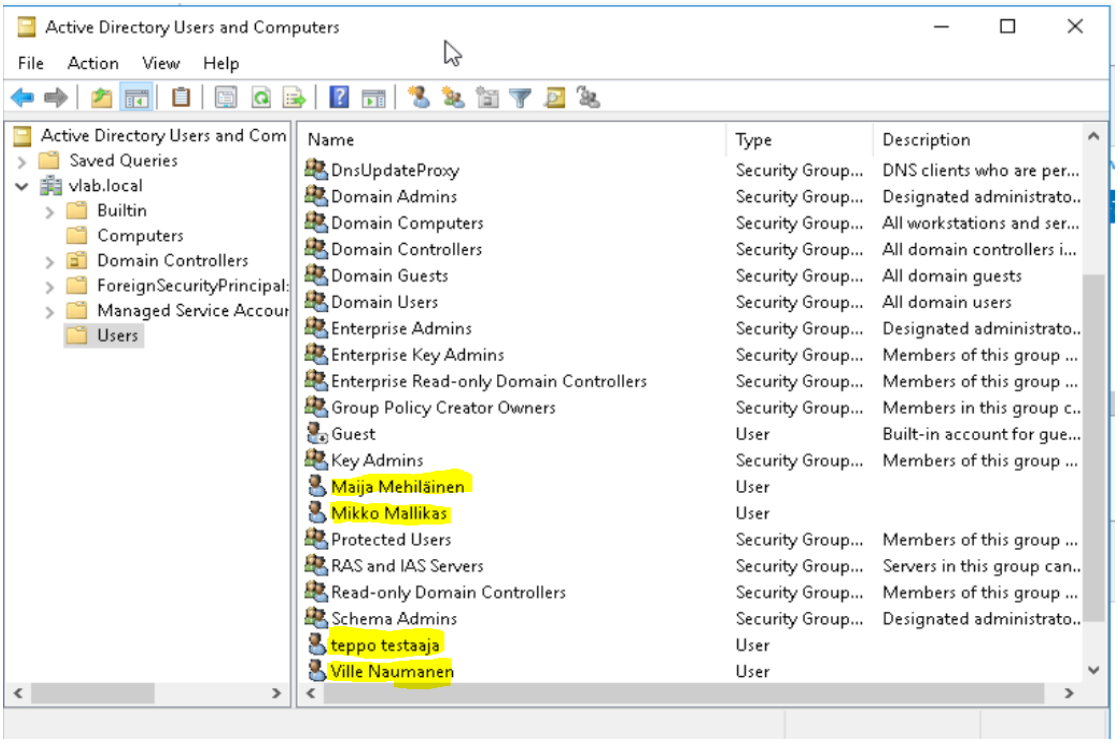
Koska 802.1X-porttitodennus vaatii käyttäjiltä pääsyä toimialueeseen, on Active Directory Domain Services -palvelu oleellinen osa RADIUS-palvelinta.

Aktiivihakemiston asennuksen jälkeen ensimmäisenä palvelimelle luotiin uusi toimialue *vlab.local* (kuva 10), johon päätelaitteet pääsevät liittymään.



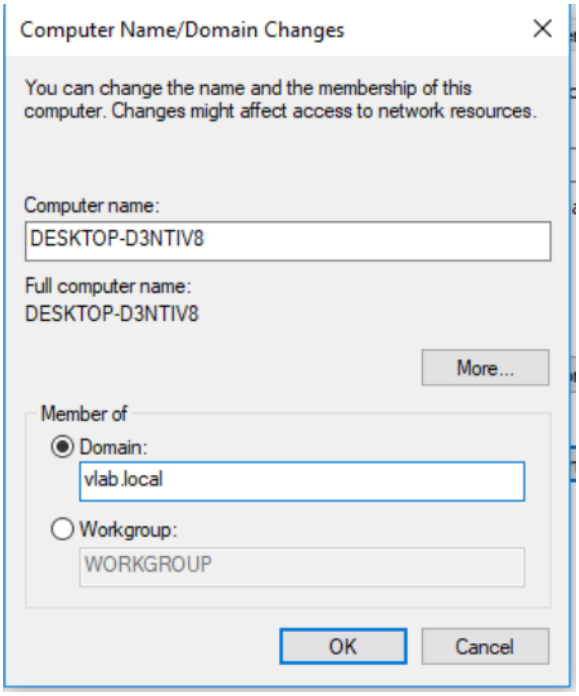
Kuva 10. Uuden toimialueen luominen Windows-palvelimelle.

Tämän jälkeen Active Directory -palveluun lisättiin muutama testikäyttäjä (kuva 11), joilla voidaan mallintaa oikeaa käyttöympäristöä ja käyttäjien todennusta.



Kuva 11. Käyttäjien luominen Active Directory-hakemistoon.

Kun käyttäjät oli luotu, lisättiin päätelaitteet vlab.local-toimialueeseen (kuva 12) jonka jälkeen kirjautuminen juuri luoduilla käyttäjillä oli mahdollista.



Kuva 12. Tietokoneen liittäminen toimialueeseen.

6.5.1 RADIUS-palvelin

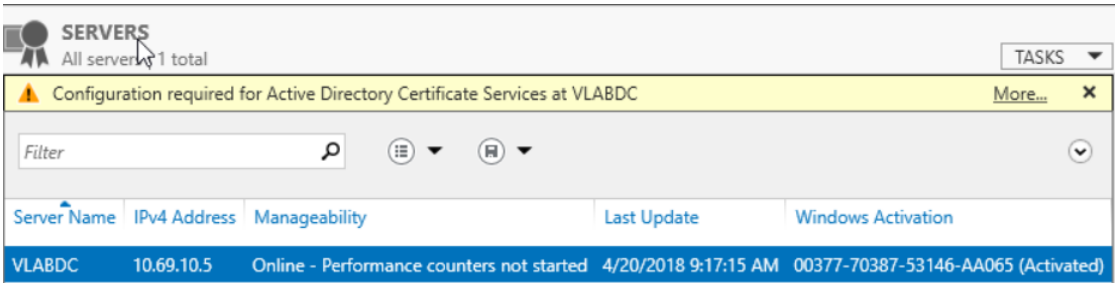
Windows Server -ympäristössä RADIUS-palvelimena toimii Windowsin NPS- eli *Network Policies Services* -palvelu. Harjoituksessa on käytetty vain yhtä RADIUS-palvelinta, mutta tuotantoympäristön toteutuksissa on suositeltavaa käyttää vähintään kahta palvelinta vikasietoisuuden takia, sillä RADIUS-palvelimien toiminta on välttämätöntä käyttäjien verkon toiminnan kannalta.

NPS-palvelu asennetaan Windows-palvelimen *Add Server Roles* -kohdasta, josta valitaan *Network Policy and Access Services.* NPS-palvelu voidaan asentaa oletusarvoilla. Palvelun tarkempiin määrityksiin palataan luvussa 6.5.3, kun konfiguroidaan 802.1X-porttitodennusta.

6.5.2 Varmenteen luominen

801.1X-todennuksen käyttämä EAP-protokolla vaatii toimiakseen varmenteen. Varmenteen tehtävänä on varmistaa, että laitteella tai käyttäjällä on oikeus päästä kohdeverkkoon. Virtuaaliympäristössä tehtävässä toteutuksessa käytetään *Active Directory Certificate Authority* -roolin avulla luotua omaa varmennetta, kun taas ICTLAB-ympäristön toteutuksessa käytetään koulun puolesta saatua varmennetta. *Active Directory Certificate Authority* -rooli on Windows Serverin palvelu, jonka avulla voidaan luoda ja ylläpitää varmenteita.

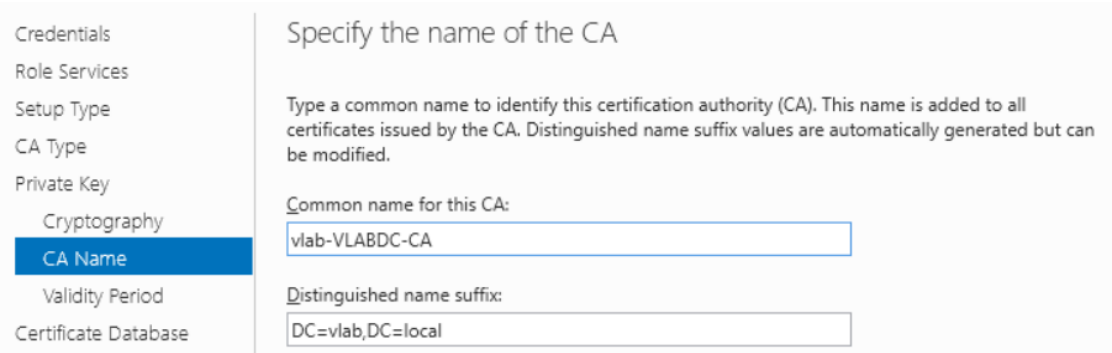
Kun *Active Directory Certificate Authority* -roolin asennus on valmis, palvelin pyytää määrittelemään muutamia asetuksia ennen kuin varmennuspalvelua voidaan käyttää (kuva 13).



Kuva 13. Active Directory Certificate Authority-roolin lisämääritykset.

Server Role Services -kohdasta valitaan *Certification Authority*-, sekä *Cerfitication Authority Web Enrollment* -kohdat. Asennustyypiksi valitaan *Enterprise*, jotta aktiivihakemistoa voidaan käyttää varmenteiden jakamiseen. CA-tyypiksi

valitaan *Root CA*, koska kyseessä on toimialueen hierarkian ylin palvelin. *Private Key* -valinnan kohdalla valitaan *Create New Private Key*. Salausvalinnassa ohjelma ehdottaa oletuksena RSA SHA256 -salausta 2048-merkkisen avaimen kanssa, joka on riittävä tässä harjoituksessa ja se voidaan valita. Seuraavana asennus kysyy nimeä juuri luodulle CA:lle (*Cerfitication Authority)*, ja oletuksena se luo nimen palvelimen toimialueen mukaan (kuva 14).



Kuva 14. CA:n nimivalinta.

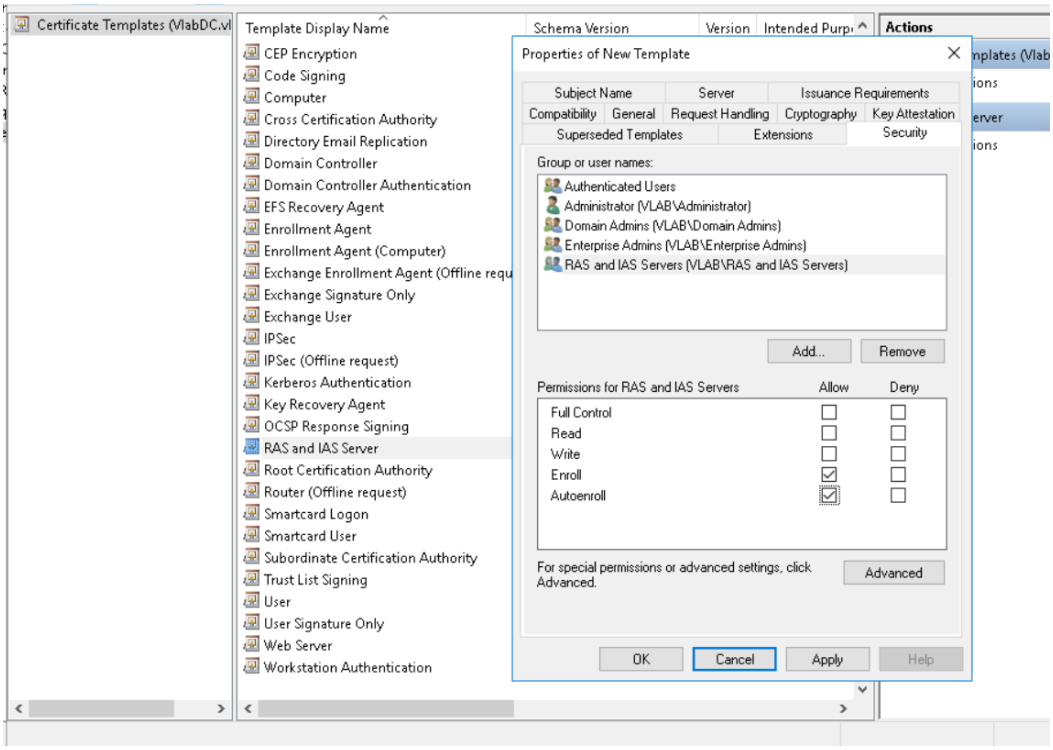
CA:n voimassaoloajaksi valitaan oletuksena oleva 5 vuotta, sillä se ei ole niin oleellista virtuaalilaboratoriossa tehtävän harjoituksen kannalta. Varmenteiden tietokannoiksi hyväksytään ohjelman tarjoamat oletusarvot.

Kun *Cerftification Authority* -palvelu on asennettu ja konfiguroitu, voidaan siirtyä itse varmenteen tekemiseen. Tuotantoympäristön toteutuksissa käytetty varmenne voidaan ostaa ulkopuoliselta palveluntarjoalta, mutta koska kyseessä on suljettu virtuaalilaboratorion testiympäristö, voidaan varmenteena käyttää Windowsin omia varmenteita, joista kopioidaan yksi ja määritellään se omien tarpeiden mukaisesti.

Varmenteida päästään tarkastelemaan valitsemalla palvelimen Server Manager -kohdasta *Tools* ja *Certification Authority*. Tämän jälkeen valitaan *Certificate Templates* -kansio, josta löytyy *RAS and IAS Server* -niminen varmenne. Valitaan se, painetaan hiiren oikealla ja valitaan *Duplicate Template. RAS and IAS Server* -varmennetta käytetään, koska se sisältää palvelimen ja asiakkaan todentamisen, joka on edellytyksenä käytettäessä PEAP-todennusta.

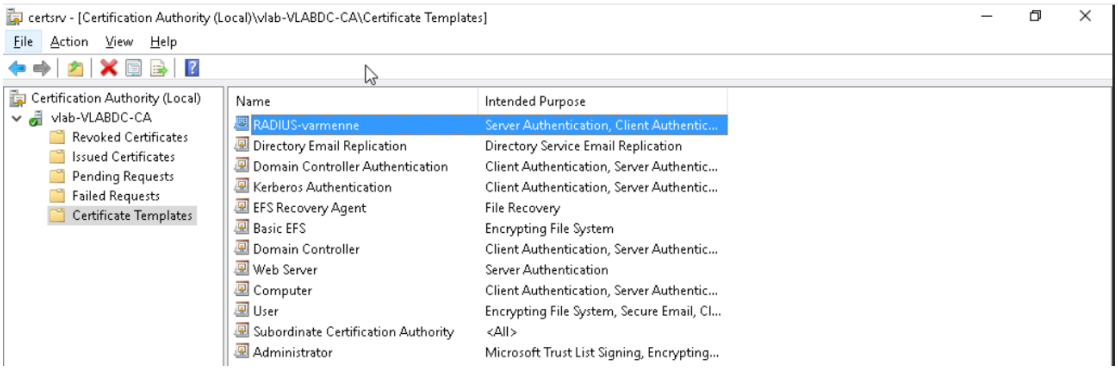
Annetaan varmenteelle nimi sekä valitaan kohta *Publish certificate in Active Directory*. Nimen lisäksi voidaan myös muokata varmenteen voimassaolo- ja

uusiutumisaikaa. Varmistetaan myös, että *Security*-välilehdellä *RAS and IAS Servers* -ryhmällä on *Enroll*- sekä *Autoenroll*-oikeudet (kuva 15).



Kuva 15. Varmenteen luominen.

Kun varmenne on luotu, lisätään se käytössä olevien varmennepohjien joukkoon. *Certificate Templates* -kansion sisällä painetaan hiiren oikealla ja valitaan *New -> Certificate Template to Issue* ja valitaan äsken luotu varmenne (kuva 16).

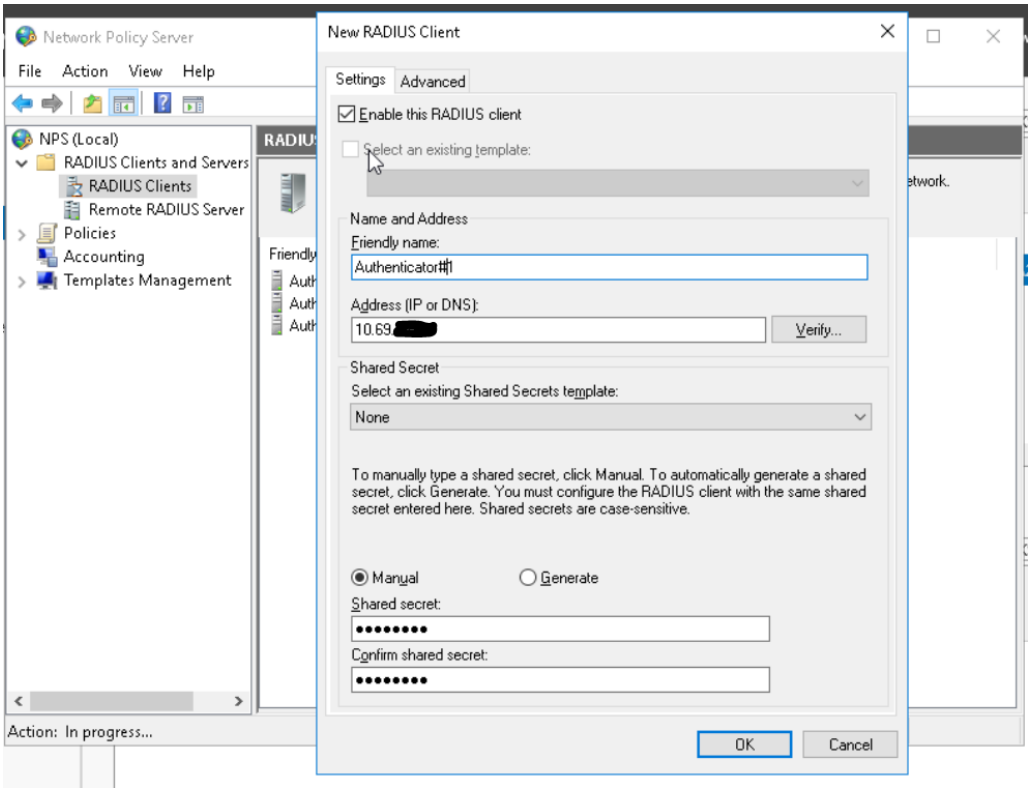


Kuva 16. Luotu varmenne varmennehakemistossa.

6.5.3 802.1X-todennuksen käyttöönotto palvelimella

Kun tarvittava varmenne on luotu, voidaan siirtyä itse 802.1X-todennuksen käyttöönottoon. Ensimmäisenä konfiguroidaan NPS-palvelu siten, että se hyväksyy RADIUS-liikenteen RADIUS-asiakkaina toimivilta kytkimiltä. *Network*

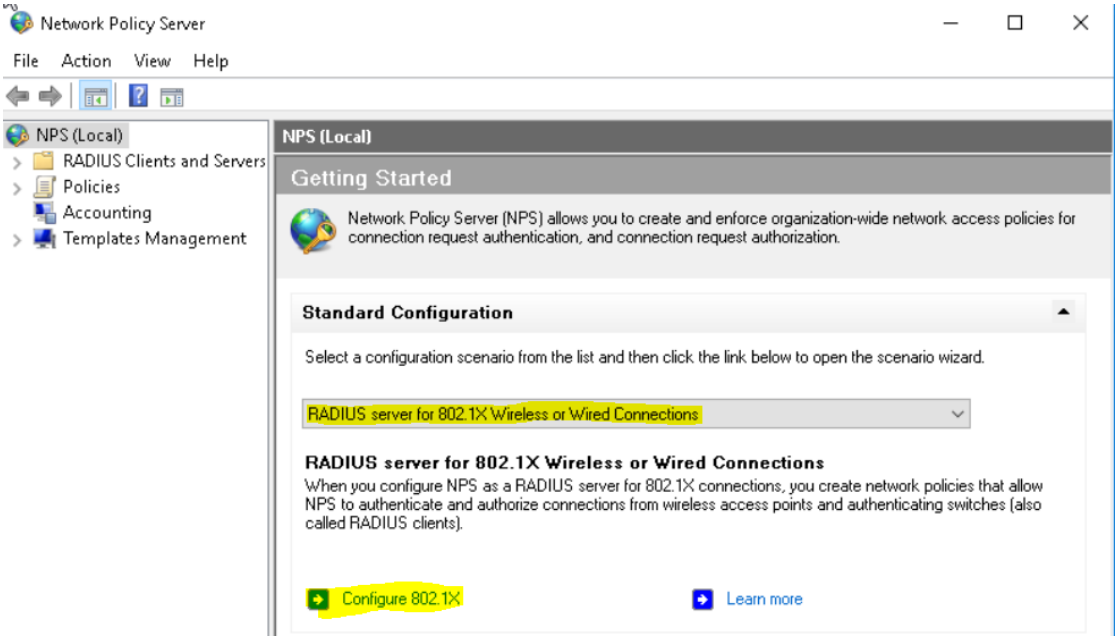
Policy Server -asetusten alta valitaan *RADIUS Clients* ja valitaan *New.* Annetaan laitteelle kuvaava nimi sekä IP-osoite osoitesuunnitelman mukaisesti (kuva 17). Tämän lisäksi kaikille RADIUS-asiakkaille on annettava yhteinen salausavain.



Kuva 17. RADIUS-asiakkaan luominen.

Tämä tehdään kaikille topologian kytkimille jotka toimivat RADIUS-asiakkaina.

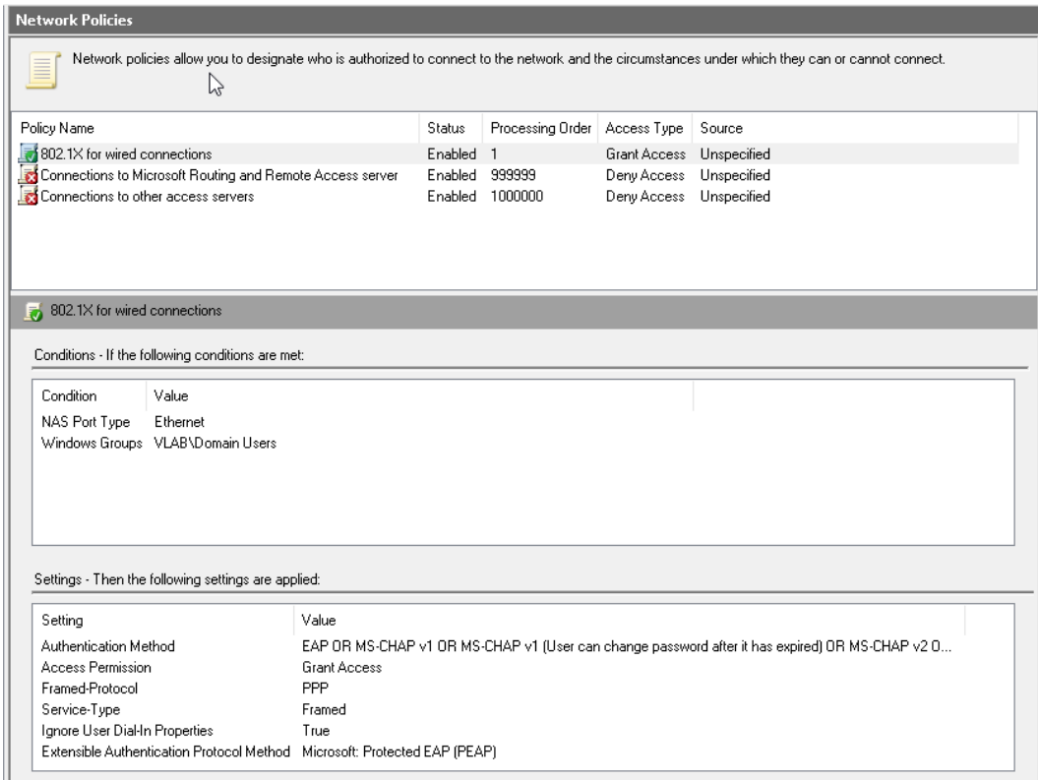
Seuraavaksi konfiguroidaan 802.1X-verkkoliikenteelle oma sääntö *Network Policies* -kohdasta (kuva 18).



Kuva 18. 802.1X-säännön luominen.

Koska kyseessä on sääntö ethernet-yhteyksille, valitaan avautuvasta valikosta *Secure Wired (ethernet) Connections* ja annetaan sille kuvaava nimi. Seuraavaksi määritellään kytkimet jotka toimivat RADIUS-asiakkaina. Lisätään listaan kaikki kolme aiemmin määriteltyä RADIUS-asiakasta. Varmennustavaksi valitaan *Microsoft: Protected EAP (PEAP),* sillä se on tietoturvallisesti vahvin varmennus, ja painetaan *Next.* Käyttäjäryhmät-kohdassa valitaan käyttäjiksi aktiivihakemiston käyttäjät *Domain Users*. Tarvittavat määritykset ovat tehty, joten painetaan *Finish*.

Luotua sääntöä voidaan tarkastella *Network Policies*-kohdan alta (kuva 19):



Kuva 19. 802.1X-sääntö.

Mikäli sääntöjä luodaan useita, on tärkeää huomioida sääntöjen prosessointijärjestys, sillä säännöt käydään läpi numerojärjestyksessä.

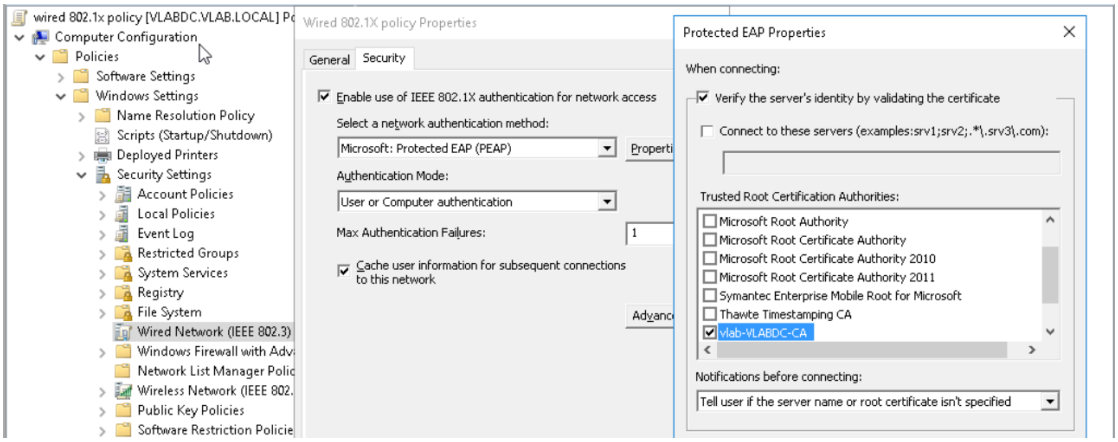
6.5.4 Ryhmäkäytännön luominen työasemia varten

Viimeisenä tehdään palvelimelle uusi ryhmäkäytäntö, jonka avulla työasemille lähetetään tarvittava varmenne heti käyttäjän kirjautuessa työasemalle. Tarvittavat asetukset on myös mahdollista tehdä paikallisesti työasemille, mutta suuremmissa käyttäjäympäristöissä on huomattavasti helpompaa jakaa varmenteet työasemille ryhmäkäytännön avulla. Ryhmäkäytäntöjä voidaan tarkastella ja muokata palvelimen *Group Policy Management* -palvelun avulla.

Avataan *Group Policy Management* ja valitaan *Domains*-kohdan alta käytössä oleva toimialue. Klikataan hiiren oikealla, valitaan *Create a GPO on this domain, and Link it here,* ja annetaan säännölle kuvaava nimi, kuten *Wired 802.1X Policy*. Tämän jälkeen muokataan luotua ryhmäkäytäntösääntöä 802.1X-todennuksen vaatimusten mukaisesti:

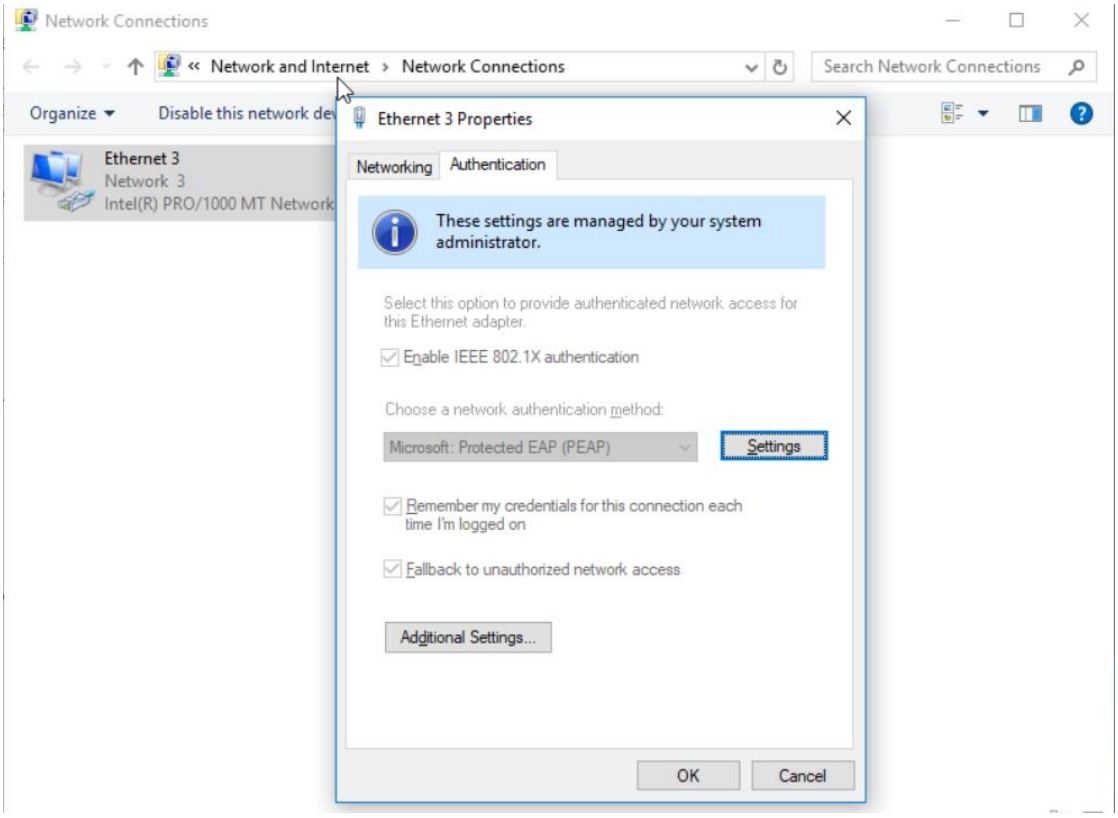
- Otetaan käyttöön varmenteiden automaattinen lähetys työasemille kohdasta *Cerftificate Services Client – Auto Enrollment*

- Otetaan käyttöön 802.1X-autentikointi ja konfiguroidaan palvelu käynnistymään automaattisesti kohdasta *Wired AutoConfig*
- Valitaan autentikointimenetelmäksi PEAP kohdasta *Wired Network (IEEE 802.3) Policies*.
- Valitaan käytössä olevaksi varmenteeksi aiemmin luotu *vlab-VLABDC-CA*-varmenne kohdasta *Wired AutoConfig Security – Properties,* kuvan 20 mukaisesti.



Kuva 20. Varmenteen valitseminen.

Kun tarvittavat asetukset on määritelty, on ryhmäkäytännön luominen valmis ja sen toimivuus voidaan tarkistaa työasemalta. Kirjaudutaan työasemalle toimialueeseen kuuluvalla käyttäjällä ja varmistetaan uuden ryhmäkäytännön käyttöönotto avaamalla komentokehote ja kirjoittamalla komento *gpupdate /force.* Ryhmäkäytännön toimivuus voidaan tarkistaa avaamalla verkkoasetukset ja menemällä verkkosovittimen lisäasetuksiin. Jos kaikki toimii, pitäisi siellä näkyä kuvan 21 mukainen *Authentication*-välilehti, jossa palvelimelta saadut varmenneasetukset näkyvät (kuva 21).



Kuva 21. 802.1X-asetukset työasemalla.

6.6 Kytkimien konfigurointi

Palvelimen määritysten jälkeen tulee konfiguroida tarvittavat määritykset myös RADIUS-asiakkaina toimiviin kytkimiin.

Ensimmäisenä määritellään valitut kytkimet toimimaan RADIUS-asiakkaina:

```
#aaa-new model
    #radius server SRV1
    #address ipv4 10.69.x.x
    #key XXXXXXX
```

AAA-New model-komennolla otetaan käyttöön AAA-protokolla kytkimessä. *Radius-server*-komennolla annetaan nimi RADIUS-palvelimena toimivalle laitteelle, ja *address ipv4* -komennolla kerrotaan, mistä osoitteesta kyseinen palvelin löytyy. Lopuksi syötetään aiemmin palvelimelle määritelty RADIUS-protokollan yhteinen salausavain (*Shared Secret*). (Cisco 2018.)

Otetaan käyttöön 802.1X-todennus kytkimissä:

```
#dot1x system-auth-control
#aaa authentication dot1x default group radius

#interface range GigabitEthernet0/x-x
    #switchport mode access
    #authentication port-control auto
    #dot1x pae authenticator
```

Dot1x system-auth-control -komento käynnistää 802.1X-protokollan kytkimessä. Useimmissa kytkimissä protokolla ei ole oletuksena käytössä, joten se on käynnistettävä manuaalisesti. (Geier 2008, 149).

Aaa authentication dot1x default group radius -komento määrittelee 802.1X-todennuksen todennustavaksi Radiuksen. (Cisco 2014.)

Interface range GigabitEthernet0/x-x -komennon avulla valitaan halutut kytkinportit, joita käytetään todennukseen.

Authentication port-control auto -komento aktivoi kytkinportin käyttämään 802.1X-todennusta jossa *auto*-määritys vaatii asiakkaalta jonkinlaista todennusta. (Geier 2008, 154.)

Dot1x pae authenticator -komennolla määritellään kytkimen portti toimimaan 802.1X-autentikaattorina. (Cisco 2018.)

Todennetut käyttäjät voidaan tarkistaa kytkimen seuraavilla komennoilla:

```
#show authentication sessions
#show authentication sessions session-id <session-id> details
```

Kytkimen komentosyötteestä nähdään kuvan 22 mukaisesti porttikohtaisen todennuksen tila, liityntäportti, MAC- ja IP-osoite sekä kirjautunut käyttäjä.

```
SW1(config)#do show authentication sessions

Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/2        0033.4bf5.9a10 dot1x   DATA    Auth      0A450A0A00000014294D4130
Gi0/1        00cf.cb0d.aa10 dot1x   DATA    Auth      0A450A0A0000001128F69847

Session count = 2

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
SW1(config)#$n sessions session-id 0A450A0A0000001128F69847 details
Session id=0A450A0A0000001128F69847
           Interface:  GigabitEthernet0/1
         MAC Address:  00cf.cb0d.aa10
        IPv6 Address:  Unknown
        IPv4 Address:  10.69.32.100
           User-Name:  VLAB\ville.naumanen
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
    Common Session ID:  0A450A0A0000001128F69847
     Acct Session ID:  Unknown
              Handle:  0xF7000002
      Current Policy:  POLICY_Gi0/1

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:


Method status list:
      Method           State
      dot1x            Authc Success
```

Kuva 22. Todennustiedot kytkimessä

7 TOTEUTUS KÄYTÄNNÖSSÄ

Virtuaalilaboratoriossa tehdyn harjoitustyön jälkeen oli aika siirtyä käytännön toteutuksen testaamiseen ICTLAB-ympäristössä. Käytännön toteutuksen tavoitteena oli, että 802.1X-porttitodennus saadaan toimimaan sekä porttitodennuksessa käytetään käyttäjäryhmään perustuvaa segmentointia.

Tavoitteena oli toteuttaa porttitodennus siten, että STAFF-ryhmään kuuluvat käyttäjät ohjataan omaan VLAN-verkkoon ja he saavat IP-osoitteen VLAN-määritysten mukaisesti. Muut käyttäjät (testausvaiheessa käytimme aktiivihakemiston käyttäjäryhmää ”Other users”) ohjataan heille tarkoitettuun VLAN:iin ja heille jaetaan eri IP-osoite.

ICTLAB-verkon suuren käytettävyyden takia sovittiin laboratorioinsinööri Jaakko Nurmen kanssa, että porttitodennusta ei oteta käyttöön opiskeluaikana mahdollisten vikatilanteiden takia. Opinnäytetyön liitteeksi luodaan kattava ohjeistus, jonka avulla ICTLAB:n kesätyöharjoittelijat voivat toteuttaa porttitodennuksen käyttöönoton kesällä jolloin verkon käyttö on huomattavasti vähäisempää.

7.1 Käytännön toteutuksen haasteet

Käytännön toteutusta suunniteltaessa tuli ottaa huomioon verkon muut käyttäjät. Koska ICTLAB-ympäristö on jatkuvassa käytössä, oli tärkeää valita testikäyttöön muutama sellainen työasema, jotka eivät ole niin aktiivisessa käytössä.

ICTLAB-ympäristö on myös suhteellisen laaja verkkoympäristö verrattuna virtuaalilaboratoriossa toteuttamaani verkkoon. Koska käytössä oleva ICTLAB-verkko oli jo valmiiksi konfiguroitu päivittäiseen käyttöön, oli tärkeää olla huolellinen määrityksiä tehtäessä. Tästä syystä laboratorioinsinööri Jaakko Nurmi oli läsnä testausta tehdessä.

Erona virtuaalitoteutukseen oli myös vaatimus segmentoida käyttäjiä käyttäjäryhmän perusteella omiin virtuaalilähiverkkoihin.

7.2 Toteutus

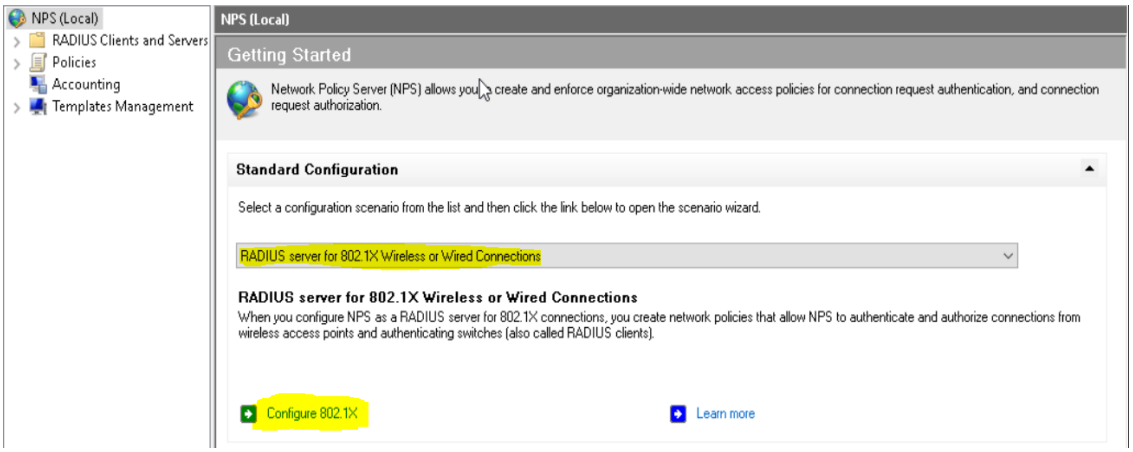
Käytännön toteutusta varten valitsimme Jaakko Nurmen kanssa BK0026-luokkatilasta kaksi työasemaa, jotka ovat vähemmällä käytöllä. Käyttöönotto aloitettiin varmistamalla laitekaaviosta, että kyseessä on oikea kytkin, sekä tarkistamalla kytkimen konfiguraatiosta että kyseessä on oikeat liityntäportit ja työasemat.

Palvelimelle oli konfiguroitu jo NPS-palvelu sekä RADIUS-asiakkaina toimivat kytkimet. Myös aktiivihakemisto ja sen muut palvelut oli konfiguroitu valmiiksi. Autentikointitietojen jakamiseksi työasemille palvelimelle oli luotava uusi Group Policy -sääntö, joka tuli asettaa asentumaan automaattisesti verkon työasemille. Group Policy -säännön lisäksi palvelimelle tuli määritellä NPS-sääntöjä 802.1X-todennusta varten.

Group Policy -sääntö tehtiin samojen määritysten mukaisesti kuin insinöörityön osassa 6.5, jossa työasemille konfiguroitiin *Certificate Services Client – Auto Enrollment,* jonka avulla todennussertifikaatit jaetaan käyttäjille aktiivihakemiston avulla sekä *Wired AutoConfig,* jonka avulla työasemat ottavat käyttöön 802.1X todennuksen ethernet-liitynnöissä. Kolmantena konfiguroitiin 802.1X-todennuksen turvallisuustiedot kuten käytetty sertifikaatti *Wired Network Policies*-asetusvalikon alta.

Group Policy -sääntöä varten teimme uuden TESTI-käyttäjäryhmän aktiivihakemistoon, johon lisättiin kaksi testikäyttöön valittua työasemaa. Tämä esti Group Policy -säännön jakamisen muihin verkon työasemiin.

NPS-sääntöjen luominen aloitettiin luomalla sääntö verkon työasemille (kuva 23).



Kuva 23. NPS-säännön luominen.

Säännön nimeksi annettiin *Wired Computer Accounts,* ja RADIUS-asiakkaaksi valittiin työaseman käyttämä kytkin. Todennusmenetelmäksi valittiin suojattu EAP eli PEAP. Koska ensimmäinen sääntö koskee vain työryhmän työasemia, valittiin käyttäjäryhmäksi *Domain Computers*. Kyseiselle säännölle ei tehty muita asetuksia.

Seuraavaksi teimme säännön STAFF-luokkaan kuuluville käyttäjille. Prosessi oli muuten sama, mutta käyttäjäryhmäksi valittiin *STAFF*-ryhmä. STAFF-ryhmän erona oli se, että ryhmän käyttäjät tuli ohjata kirjautumisvaiheessa tiettyyn VLAN-verkkoon, joten asennusvaiheessa muokattiin *Traffic Controls* -asetuksia. *Tunnel-Type*-arvoksi tuli *Commonly used for 802.1x – VLANs*, *Tunnel-Medium-Type*-arvoksi *802* ja *Tunnel-Pvt-Group-ID*-arvoksi asetettiin haluttu VLAN-verkko, joka tässä tapauksessa oli 16.

Kolmas sääntö luotiin verkon muille käyttäjille, joten ryhmäksi valittiin säännön luomisvaiheessa *Other users* -ryhmä. Kyseinen käyttäjäryhmä tuli niin ikään ohjata omaan VLAN-verkkoonsa, joten asetuksista vaihdettiin *Tunnel-Pvt-Group-ID*-arvo vastaamaan haluttua VLAN-verkkoa, joka tässä tapauksessa oli 32.

Kun säännöt oli luotu, oli tärkeää tarkistaa NPS-hallinnan *Network Policies* -listauksesta, että luodut säännöt olivat oikeassa prosessointijärjestyksessä. Koulun sääntölistauksessa oli esimerkiksi liikenteen kieltävä *Deny Access* -

sääntö, joten oli huomioitava, että kyseinen sääntö ei ole listauksessa korkeammalla kuin luodut 802.1X-säännöt, sillä muuten liikenne estettäisiin suoraan.

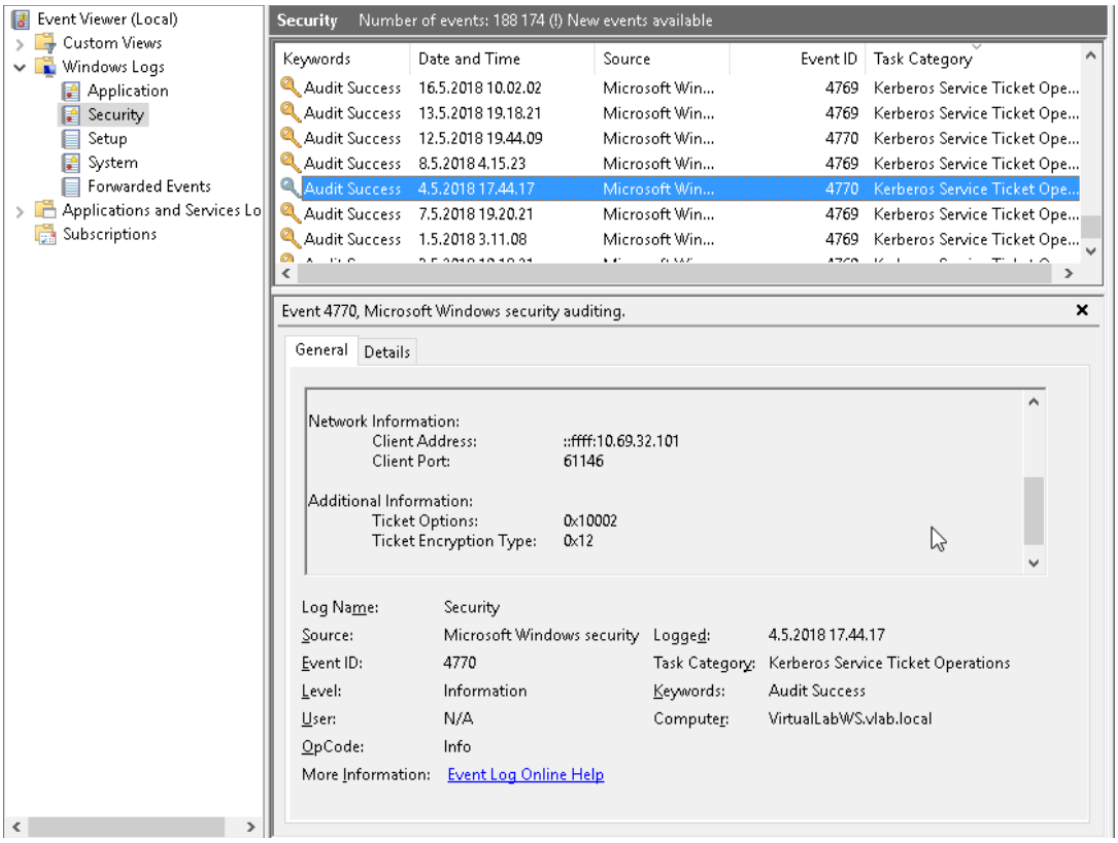
Palvelinmääritysten jälkeen tuli kytkimelle tehdä vielä muutama tarvittava määritys 802.1X-todennuksen käyttöönottamiseksi. Kytkimeen päästiin kiinni telnet-yhteyden avulla ja kytkimen *show int desc* -komennon avulla näkyi, mikä työasema on liitettynä mihinkin liityntäporttiin. RADIUS-palvelin oli jo lisätty kytkimen konfiguraatioon, joten globaalisti tehtäviä muutoksia konfiguraatioon oli vain kaksi. Ensimmäinen oli *#dot1x system-auth-control,* joka käynnistää 802.1X-palvelun kytkimessä. Toinen tarvittava lisäys oli *#aaa authorization network default group radius* -komento, jonka avulla kytkin ohjaa käyttäjien valtuutuksen RADIUS-palvelimen hallintaan. Tämä mahdollistaa käyttäjien ohjaamisen VLAN-verkkoihin, vaikka kytkimen liityntäportteihin olisikin lisätty pääsysääntöjä.

Seuraavaksi tuli määritellä halutut kytkimen liityntäportit toimimaan 802.1X-todennuksen autentikaattorina. Valitut kaksi porttia valittiin *int range* -komennolla ja konfiguraatioon lisättiin komennot *#dot1x port-control auto* (802.1X-todennuksen käyttöönotto portissa) sekä *#dot1x pae authenticator* (portti määritellään toimimaan autentikaattorina).

Työasemilta tarkistimme, että halutut todennustiedot oli saatu palvelimelta avaamalla verkkoadapterin asetukset, josta löytyi *Authentication*-välilehti. Toiselle työasemalle välilehti ilmestyi heti kirjautumisen jälkeen, mutta toinen työasema vaati GPO-sääntöjen päivityksen komennolla *gpupdate /force*.

Määritysten jälkeen kokeilimme todennuksen toimintaa kirjautumalla ensin yhdelle työasemalle Jaakon tunnuksilla (Staff-käyttäjäryhmän tunnus) ja tarkistamalla *ipconfig*-komennolla saatu IP-osoite, joka oli oikean VLAN-verkon mukainen. Tämän jälkeen kirjauduin samalle työasemalle omilla tunnuksillani (Other users -ryhmän tunnus), ja tarkistimme taas saadun IP-osoitteen. IP-osoite oli vaihtunut eri VLAN:in IP-osoitteeksi, joten 802.1X-segmentointi toimi.

Autentikoinnin onnistumista seurasimme kirjautumisvaiheessa palvelimen *Event Viewer* -lokista. Koska loki kirjaa kaikkia palvelinverkon tapahtumia, oli sen lukeminen hieman haastavaa, mutta löysimme kuitenkin oikean lokitiedoston, josta näkyi onnistunut todennusprosessi (kuva 24).



Kuva 24. Event Viewer-lokitiedosto

7.3 Lopputulos

Testausvaiheen jälkeen lopputuloksena oli onnistunut 802.1X-todennus kahdella eri työasemalla. Myös käyttäjäryhmän mukainen VLAN-segmentointi onnistui. Käyttöönotto onnistui hyvin ja melko nopeasti, sillä tarvittavien määritysten konfiguroimista oli harjoiteltu virtuaaliympäristössä. Ainut ongelma johon törmäsimme testausvaiheessa, oli RADIUS-asiakaskytkinten valinta NPS-sääntöä luodessa. Oletusarvoisesti ohjelma tarjoaa listaukseen kaikki RADIUS-verkkoon kuuluvat asiakaskytkimet, ja mikäli listauksesta yrittää valita vain yhden kytkimen poistamalla muut kytkimet listalta, poistaa ohjelma niiden RADIUS-asiakkuuden kokonaan. Tämä aiheutti Jaakolle hieman lisätyötä, mutta ongelma saatiin korjattua.

8 YHTEENVETO

Opinnäytetyön tavoitteena oli tutustua 802.1X-standardin mukaiseen porttikohtaiseen todennukseen, ja suunnitella todennuksen käyttöönotto Kaakkois-Suomen ammattikorkeakoulun Kotkan kampuksen ICTLAB-laboratorioon. ICTLAB-verkossa 802.1X-todennus oli jo käytössä langattomissa verkoissa, mutta tavoitteena oli saada todennus käyttöön myös langallisessa verkossa ja näin ollen parantaen verkon tietoturvaa.

Opinnäytetyön teoriaosiossa perehdyttiin tietoturvaan, lähiverkon toimintaan, 802.1X-todennuksen toimintaan sekä todennuksen käyttämiin protokolliin. Työn käytännön osuus koostui kahdesta osiosta. Ensimmäisen osan tavoitteena oli tutustua porttikohtaisen todennuksen toimintaan kattavasti ja harjoitella sen käyttöönottoa suljetussa virtuaalilaboratoriossa. Toisessa osassa porttitodennusta testattiin kohdennetusti kahdella vähemmällä käytöllä olevalla ICTLAB-laboratorion työasemalla.

Alkuperäisen suunnitelman mukaan porttitodennus oli tarkoitus ottaa laajamittaiseen käyttöön kevään 2018 aikana. Aikataulujen ja henkilökunnan toiveiden vuoksi käyttöönottoa siirrettiin kesään 2018, jolloin käyttöaste verkossa on huomattavasti pienempi. Opinnäytetyön liitteeksi toteutettiin kesäharjoittelijoille suunnattu ohjeistus, jonka avulla he suorittavat todennuksen käyttöönoton.

Saavutin opinnäytetyön aikana itselleni asettamani oppimistavoitteet. Opin kattavasti porttitodennuksen teoriasta ja sen toiminnasta. Käytännön toteutuksen aikana opin monipuolisesti Windows-palvelinympäristön käyttöä ja sen ominaisuuksia. Itse työn tekeminen oli mielekästä, sillä aihe oli mielenkiintoinen ja antoi mahdollisuuden oppia lisää jo koulussa opiskelluista asioista. Opinnäytetyö onnistui mielestäni kohtuullisen hyvin, vaikka alkuperäiseen suunnitelmaan tulikin muutoksia työn aikana, ja laajamittainen käyttöönotto siirtyi myöhempään ajankohtaan. Myös osa alun perin suunnitelluista osista jäi toteuttamatta, kuten esimeriksi 802.1X-todennuksen integraatio Jiri Rantalan opinnäytetyön aiheena olevaan OSSIM SIEM -järjestelmään.

Opinnäytetyö tarjoaa pohjan erilaisille jatkokehityshankkeille. Jatkon kannalta tärkein vaihe on saada itse porttitodennus käyttöön koko ICTLAB-verkkoon onnistuneesti. Tämän jälkeen verkon tietoturva on jo kiitettävällä tasolla, sillä langattomassa verkossa on jo ollut 802.1X-todennus käytössä, ja verkon oheislaitteet (tulostimet yms.) on suojattu MAC-osoitteen avulla.

Jatkokehityskohteena voisi pohtia 802.1X-todennuksen käyttöä siten, että verkkoon luotaisiin Guest-VLAN, johon käyttäjät joilla ei ole tarvittavia oikeuksia ohjattaisiin automaattisesti. Guest-VLAN tarjoaisi käyttäjille vain rajoitetun oikeuden esimerkiksi internet-palveluihin, mutta ei pääsyä itse koulun verkkoon ja jaettuihin materiaaleihin. Toinen vaihtoehto olisi luoda esimerkiksi Sandbox-niminen VLAN, johon luvattomat käyttäjät ohjattaisiin ja pääsy verkkoon estettäisiin täysin. Sandbox VLAN voisi tarjota verkon ylläpitäjälle mahdollisuuden tutkia luvattomia käyttäjiä ja heidän tietojaan mahdollisten verkkohyökkäysten varalta. Kyseiset muutokset vaatisivat koulun lähiverkon konfiguroimista uudelleen kyseisten VLAN-verkkojen osalta ja pieniä muutoksia 802.1X-konfiguraatioon.

Toinen kehityskohde voisi olla 802.1X-todennuksen integraatio Jiri Rantalan opinnäytetyössä tutkittuun OSSIM SIEM -valvontajärjestelmään. Tämä oli yksi tutkimuskohde opinnäytetyötä tehtäessä, mutta aikataulujen tullessa vastaan siitä jouduttiin luopumaan. Tarkoituksena oli saada integroitua 802.1X-todennus osaksi OSSIM SIEM -valvontajärjestelmää, jolloin käyttäjän kirjautuessa työasemalle OSSIM SIEM loisi siitä merkinnän lokitiedostoon, josta kirjautumisia voitaisiin valvoa.

Kolmas pohdittava kehityskohde olisi Cisco ISE -järjestelmän käyttöönotto. Cisco ISE (*Identity Services Engine*) on Ciscon luoma pääsynhallintajärjestelmä, jonka avulla voidaan hallita verkon käyttäjiä ja pääsyä verkkoon keskitetysti yhdellä järjestelmällä. Sen avulla voidaan hallita kaikkia verkon laitteita, mukaan lukien langattomat ja langalliset laitteet, tietokoneet, tulostimet, valvontakamerat sekä esimerkiksi älypuhelimet ja tabletit. ISE ei ole tarkoitettu pelkästään 802.1X-todennuksen hallintaan, mutta 802.1X-todennus voidaan

toteuttaa myös Cisco ISE:n avulla. ISE:n avulla koko ICTLAB-verkon käyttäjänhallinta voisi toteutua tehokkaammin ja helpommin. Järjestelmän käyttöönotto vaatisi kuitenkin investointeja, sillä kyseessä on maksullinen ohjelma.

LÄHTEET

Carroll, B. 2004. Cisco Access Control Security: AAA Administration Services. Indianapolis: Cisco Press.

Bradford Networks. 2013. 802.1X And NAC: Best Practices for Effective Network Access Control. WWW-Dokumentti. Saatavissa: http://cipherwire.net/wp-content/uploads/2013/06/802.1X_and_NAC___Best_Practices_for_Effective_Network_Access_Control.pdf [Viitattu: 16.04.2018].

Cisco. 2006. How Does RADIUS Work? WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html [Viitattu: 03.04.2018].

Cisco. 2011. Wirex 802.1X Deployment Guide. WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386743 [Viitattu 12.04.2018].

Cisco. 2013. Configuring 802.1X. WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x_chapter_01011.pdf [Viitattu: 18.04.2018].

Cisco. 2014. Demystifying RADIUS Server Configurations. WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/whitepaper_C11-731907.html [Viitattu: 26.04.2018].

Cisco. 2018. Configuring Basic AAA on an Access Server. WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html [Viitattu: 20.04.2018].

Geier, J. 2008. Implementing 802.1X Security Solutions for Wired And Wireless Network. Indianapolis: Wiley Publishing, Inc.

Gummerus, L. & Iivonen, P. 2010. IEEE 802.1x todennus & käyttöönotto Fenniassa. Laurea Ammattikorkeakoulu. Leppävaara. Opinnäytetyö. Saatavissa: http://www.theseus.fi/handle/10024/15731 [Viitattu 18.05.2018].

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Hakala, M. Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Hucaby, D. 2014. CCNA Wireless 640-722 Official Cert Guide. Indianapolis: Cisco Press.

Kouvolan Seudun Ammattiopisto. 2010. OSI-Malli. WWW-Dokumentti. Saatavissa: http://www.koudata.fi/node/598 [Viitattu 21.02.2018].

Microsoft. 2008. MS-CHAPv2. WWW-Dokumentti. Saatavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc957983(v=technet.10) [Viitattu 3.5.2018].

Microsoft. 2009. PEAP. WWW-Dokumentti. Saatavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757996(v=ws.10) [Viitattu 02.05.2018].

Microsoft. 2018. RADIUS Authentication, Authorization and Accounting.WWW-Dokumentti. Saatavissa: https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb892012%28v=vs.85%29.aspx [Viitattu: 18.04.2018].

Microsoft Developer Network. 2018. Active Directory Domain Services. WWW-Dokumentti. Saatavissa: https://msdn.microsoft.com/en-us/library/aa362244(v=vs.85).aspx [Viitattu 12.04.2018].

Nurmi, J. 2016. Implementation of Nested Virtual Laboratory System. Opinnäytetyö. Saatavissa: http://www.theseus.fi/handle/10024/107061 [Viitattu: 18.05.2018].

Puska. M. 2000. Lähiverkkojen Tekniikka. Jyväskylä: Gummerus.

Tampere University of Technology. 2002. OSI-Malli. WWW-Dokumentti. Saatavissa: http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html [Viitattu 21.02.2018].

Liite 1/1

802.1X-TODENNUKSEN KÄYTTÖÖNOTTO ICTLAB-YMPÄRISTÖSSÄ

Todennuksen käyttöönottamiseksi määrityksiä on tehtävä lähinnä palvelimille ja kytkimille. Palvelimen group policy-määritysten avulla tarvittavat määritykset jaetaan AD-päivitysten mukana työasemille, mutta työasemilta on hyvä tarkistaa, että AD-päivitykset ovat onnistuneet. Kytkimille tehtävät konfiguraatiomuutokset tulee tehdä jokaiselle kytkimelle, johon porttitodennukseen osallistuvat työasemat ovat kytkettynä.

Suuri osa palvelimille tehtävistä määrityksistä tehtiin keväällä todennuksen testausvaiheessa, mutta määritykset on silti syytä käydä läpi ja varmistaa että ne löytyvät vielä palvelimelta, ja ovat todenmukaiset. Suurin työ todennuksen käyttöönotossa on autentikaattorikytkinten manuaalinen konfigurointi.

1. Palvelimen määrittelyt

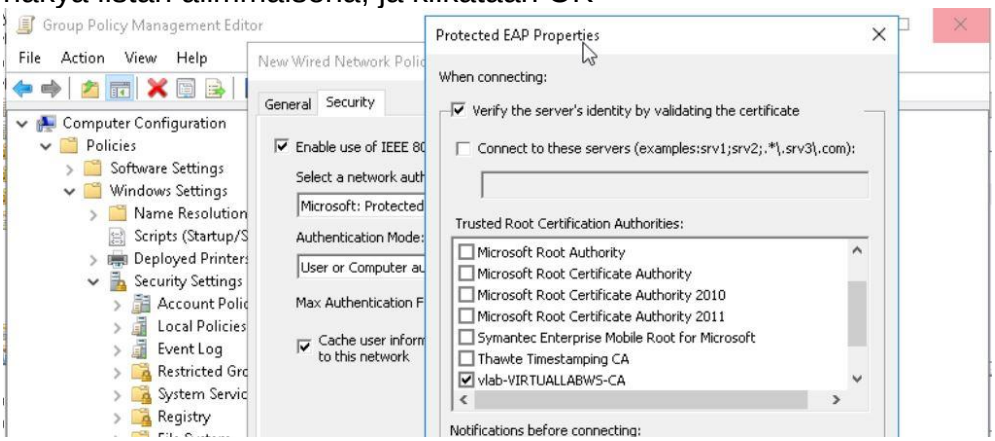
Group Policy-sääntöjen luominen työasemille

Group Policy-sääntöjen avulla työasemat valmistellaan käyttämään dot1x-todennusta. Todennuksen käyttöönotto vaatii muutaman asetuksen konfiguroimista Windows-palvelimella. Group Policy-sääntöjen avulla voidaan myös kontrolloida sitä, mille työasemille/käyttäjille säännöt jaetaan. Palvelimelle luodut säännöt voi tarkistaa Group Policy Management-hallinnan *Group Policy Objects*-kansion alta. Testausvaiheessa teimme tarvittavat GP-säännöt palvelimelle, mutta niiden toiminta on hyvä tarkistaa.

Mikäli tarvittavat GPO-säännöt löytyvät palvelimelta, voidaan siirtyä suoraan kohtaan ”NPS-Policyn luominen 802.1X-todennukselle”.

Group Policy-sääntöjä päästään tarkastelemaan avaamalla Server Managerista *Tools* ja *Group Policy Management*.

1. Valitaan vasemalla olevasta listauksesta ICTLAB:in toimialue, klikataan hiiren oikealla ja valitaan *Create a GPO in this domain, and Link it here.*
2. Annetaan luotavalle säännölle nimi, esimerkiksi Wired dot1x policy.
3. Luotu sääntö löytyy vasemmalla olevasta listauksesta *Group Policy Objects*-kansiosta. Etsitään luotu sääntö ja klikataan hiiren oikealla ja valitaan *Edit*.
4. Ensimmäisenä konfiguroidaan todennussertifikaatin automaattinen jako työasemille (auto-enrollment):
   - Avautuvasta ikkunasta laajennetaan valinta *Computer Management → Policies → Windows Settings → Security settings* ja valitaan kansio *Public Key Policies*
   - Kansion juuresta löytyy tiedosto *Certificate Services Client – Auto Enrollment*. Valitaan se, klikataan hiiren oikealla ja valitaan *Properties*.
   - Pudotusvalikosta valitaan *Enabled*, ja ruksitetaan alla olevat *Renew-* ja *Update*-laatikot, jonka jälkeen suljetaan valikko painamalla Ok.
5. Seuraavan konfiguroidaan ethernet-porttien 802.1X-todennus:
   - *Computer Management → Policies → Windows Settings → Security settings*, ja valitaan kansio *System Services*.
   - Selataan listaa alas, kunnes sääntöasetus *Wired AutoConfig*-löytyy, ja avaan sen ominaisuudet hiiren oikealla
   - Valitaan *Define this policy setting*, sekä käynnistysasetukseksi *Automatic*
   - Suljetaan valikko painamalla Ok.
6. Kolmantena konfiguroidaan käytetty todennusmetodi:
   - *Computer Management → Policies → Windows Settings → Security settings*, jonka juuresta löytyy tiedosto *Wired Network (IEEE 802.3) Policies*
   - Klikataan hiiren oikealla ja valitaan *Create a New Wired Network Policy for Windows Vista and Later Releases*
   - Annetaan säännölle kuvaava nimi, esimeriksi EAP Policy for wired 802.1x
   - Avataan *Security*-välilehti ja valitaan *Enable use of IEEE 802.1X authentication for network access*, sekä valitaan alla olevasta pudotusvalikosta *Microsoft: Protected EAP (PEAP)*
   - Klikataan *Security*-välilehden *Properties*-valintaa. Avautuvasta valikosta voidaan valita todennuksen käyttämä turvallisuussertifikaatti. Valitaan listalta ictlab:in käyttämä sertifikaatti (kuva 1), joka pitäisi näkyä listan alimmaisena, ja klikataan OK



Kuva 1. Sertifikaatin valinta
- Valitaan vielä *Advanced*-valikko, ja ruksitetaan *Single Sign On*-kohdasta *Enable – Perform immediatly after user logon* ja *This network uses different VLAN*-valinnat

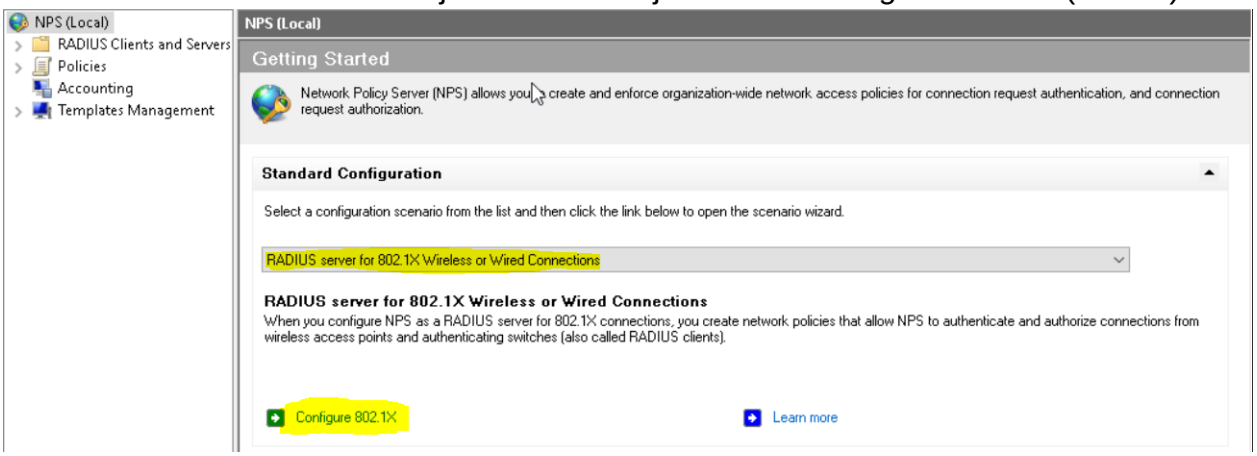
7. Tarvittavat GP-määritykset on tehty, lopuksi on vielä varmistettava, että luotu sääntö on linkitetty ictlab-toimialueeseen
8. Palataan takaisin *Group Policy Management*-hallintaan, valitaan ictlab-toimialue hiiren oikealla, *Link an Existing GPO* ja valitaan listalta juuri luotu sääntö
9. Tämän jälkeen GPO-sääntö on linkitetty ictlabin toimialueeseen, ja se jaetaan automaattisesti työasemille niille kirjauduttaessa

NPS-Policyn luominen 802.1X-todennukselle

Tämä tehtiin keväällä 802.1X-todennuksen testausvaiheessa ja teoriassa palvelimelta pitäisi löytyä jo säännöt “Wired 802.1X users” ja “Wired 802.1X Staff”, mutta mikäli ei löydy, niin tehdään ne uudestaan. Mikäli tarvetta on ohjata sääntöjen avulla useampia AD-käyttäjäryhmiä, tulee kyseisille ryhmille tehdä omat sääntönsä seuraavien ohjeiden mukaisesti.

NPS-sääntöjen avulla voidaan segmentoida verkon käyttäjiä VLAN-verkkojen mukaisesti. Testivaiheessa teimme kaksi sääntöä: STAFF-luokan käyttäjät ja muut verkon käyttäjät (AD-ryhmä ”Other users”). Varmistakaa Jaakolta, että kyseiseen suunnitelmaan ei ole tullut muutoksia, tai käytetyt VLAN-verkot eivät ole muuttuneet.

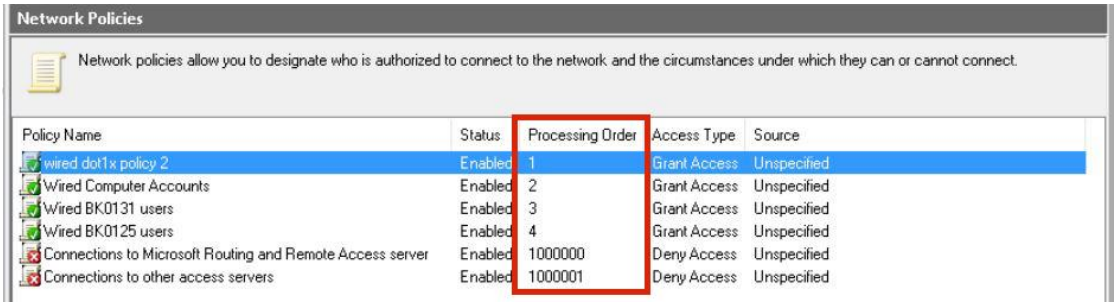
1. Avataan palvelimelta *Tools -> Network Policy Server*
2. Varmistetaan että ollaan NPS-palvelun juuressa (*NPS (Local)*)
3. Valitaan aloitusruudun pudotusvalikosta *RADIUS Server for 802.1X Wireless or Wired* ja *connections* ja valitaan *Configure 802.1X* (kuva 2).



Kuva 2. NPS-säännön luominen

4. Valitaan *Secure Wired (ethernet) Connections*, ja annetaan sille nimi, esim. “Wired dot1x users”
5. Valitaan seuraavaksi RADIUS-asiakkaat. Asennusvalikon pitäisi ehdottaa kaikkia RADIUS-palvelimella toimivia asiakaskytkimiä joten painetaan *Next*. **HUOM!!!** Tässä kohtaa ei kannata poistaa RADIUS-asiakkaita listalta, sillä se poistaa ne myös RADIUS-asiakkuudesta ja ne pitää konfiguroida uudelleen.
6. EAP-tyypiksi valitaan *Microsoft: Protected EAP (PEAP)*
7. Seuraavaksi valitaan käyttäjät, ketä NPS-Policy koskee. Keväällä testausvaiheessa tehtiin kaksi erillistä policyä, toinen normaaleita käyttäjiä varten ja toinen STAFF-ryhmän käyttäjiä varten. Valitaan tässä kohtaa käyttäjäryhmäksi STAFF (Jaakko Nurmi neuvoo oikeiden ryhmien löytämisessä).
8. Seuraavana konfiguroidaan STAFF-käyttäjäryhmän VLAN, johon käyttäjät liitetään onnistuneen autentikoinnin jälkeen. *Configure Traffic Tools*-ikkunasta valitaan *Configure*, ja avautuvasta ikkunasta muutetaan kolme arvoa:
   ***Tunnel-Type**:* Valitaan *Edit → Add → Commonly used for 802.1x → Virtual LAN (VLAN)*
   ***Tunnel-Medium-Type**:* Valitaan *Edit → Add → Commonly used for 802.1x → 802*
   ***Tunnel-Pvt-Group-ID**:* Valitaan *Edit → Add → String,* ja arvoksi syötetään haluttu VLAN-verkko numerona tai nimenä (esim. 16). Varmistakaa oikeat VLAN-verkot Jaakolta!
9. Tämän jälkeen NPS-policy on luotu. Tehtyjä asetuksia pääsee tarkastelemaan ja muokkaamaan NPS-konsolin *Policies - Network Policies*-kohdasta jossa näkyy lista käytössä olevista NPS-säännöistä.
10. Kun sääntö STAFF-ryhmän käyttäjille on tehty, tehdään seuraavaksi uusi sääntö muille käyttäjille (sääntöjä voidaan tehdä useita ja mikäli jatkossa on tarvetta jaotella useita käyttäjäryhmiä VLAN:ien perusteella, se tehdään juurikin näiden sääntöjen perusteella)
11. Palataan NPS-konsolin juureen (NPS (local)) ja aloitetaan uuden säännön teko kohdan 3. Mukaisesti.
12. Säännön luominen on muuten sama prosessi, mutta kohdassa 7. Valitaan eri käyttäjäryhmä, sekä 8-kohdan *Tunnel-Pvt-Group-ID*-arvoksi tulee eri arvo (koska kyseessä on eri VLAN-verkko)

HUOM! Network Policies-listalla näkyvät säännöt suoritetaan prosessointijärjestyksessä (Processing Order), joten on tärkeää, että dot1x-säännöt ovat listan alussa (kuva 3). Jos listalla on esimerkiksi jokin Deny Access-sääntö ennen dot1x-sääntöjä, liikenne estetään ennen kuin autentikointi ehtii edes tapahtua.



Kuva 3. NPS-sääntöjen prosessointijärjestys

2. Kytkimiin tehtävät määrittelyt

Jokainen todennuksessa toimiva RADIUS-kytkin tulee konfiguroida toimimaan 802.1X-autentikaattorina, sekä jokainen työaseman liityntäportti tulee myös määritellä erikseen toimimaan 802.1X-todennuksen mukaisesti. Koska kytkimet ovat jo osana toimivaa verkkoympäristöä, on 802.1X-todennuksen käyttöönotto melko yksinkertaista, sillä se vaatii vain muutaman komennon.

Kytkinten hallintaan päästään telnet-yhteydellä. Lisätietoja hallintayhteydestä (ip-osoitteet, käyttäjätunnukset) tulee kysyä *Jaakko Nurmelta*.

Globaalisti tehtävät määritykset

Seuraavat komennot tulee suorittaa kytkimen *configure terminal*-tilassa.

#aaa new-model (tämä todennäkösesti on jo käytössä kytkimissä, sillä RADIUS on toiminnassa palvelimilla)
#aaa authentication dot1x default group radius
- määrittelee 802.1X-yhteysprotokollaksi Radiuksen
#aaa authorization network default group radius
- Ohjaa käyttäjien valtuutuksen RADIUS-palvelimen käyttöön, eli antaa RADIUS-palvelimelle oikeuden ohjata käyttäjiä VLAN-verkkoihin, vaikka kytkimessä olisi aseteltukin access-säännöt VLAN-verkoille.
#dot1x system-auth-control
- Käynnistää 802.1X-palvelun kytkimessä

Liityntäporteissa tehtävät määritykset

Seuraavat komennot tulee syöttää kytkimen interface-tilassa. Valitaan tarvittu interface (tai usempi interface käyttäen int range-komentoa). Työaseman käyttämä liityntäportti löytyy vertaamalla koneen numeroa kytkimen interface-tauluun (*show ip interface description*), jossa liityntäporttin kytketty tietokone löytyy description-kohdasta.

#switchport mode access

- Todennäköisesti jokainen käytössä oleva kytkin on jo konfiguroitu, joten kyseistä komentoa ei tarvitse syöttää.

#dot1x port-control auto

- Määrittelee kytkinportin käyttämään 802.1X-todennusta

#dot1x pae authenticator

- Määrittelee kytkinportin toimimaan autentikaattorina

Kytkimeen tehtävät määritykset ovat nyt tehty.

Konfiguroinnin tarkistus

802.1X-todennuksen tilaa voidaan tarkastella muutamilla kytkinkomennoilla.

#show dot1x interface <interface>

- näyttää 802.1X-protokollan tilan valitussa liityntäportissa (kuva 4):

```
SW1#show dot1x int g0/1
Dot1x Info for GigabitEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Kuva 4. Dot1X-tila liityntäportissa-

#show authentication sessions

- Näyttää kytkimellä tapahtuvat (kuva 5) todennukset (liityntäportti, MAC-osoite, todennuksen tila, session id)

```
SW1#show authentication sessions

Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/2        0033.4bf5.9a10 dot1x   DATA    Auth      0A450A0A00000014294D4130
Gi0/1        00cf.cb0d.aa10 dot1x   DATA    Auth      0A450A0A0000001128F69847

Session count = 2

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
SW1#
```

Kuva 5. Kytkimellä tapahtuvat todennukset.

#show authentication sessions session-id <session-id>

tai

#show authentication sessions session-id <session-id> details

riippuen IOS-versiosta.

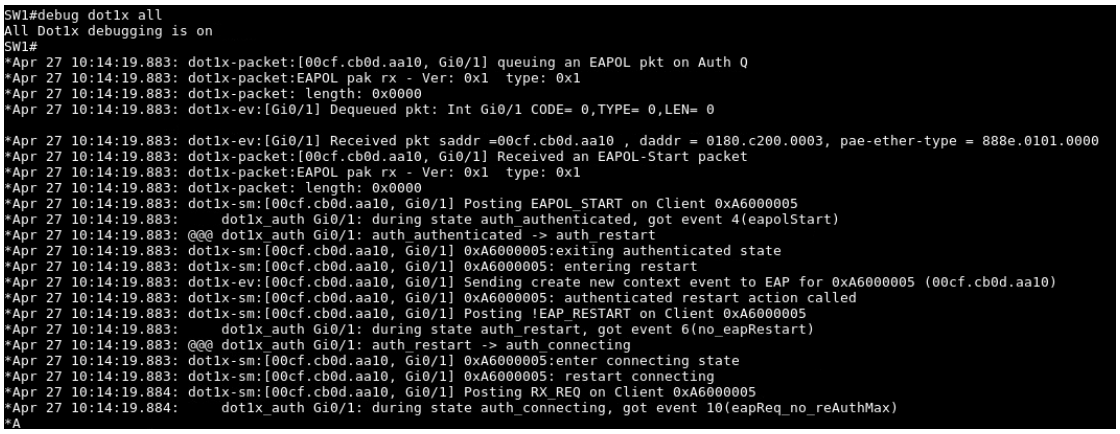
- näyttää valitun autentikointiprosessin tilan (kuva 6) ja lisätietoja (kuten käyttäjänimi, IP-osoite, todennuksen tila, toimialue)

```
SW1#show authentication sessions session-id 0A450A0A0000001128F69847 details
Session id=0A450A0A0000001128F69847
           Interface:  GigabitEthernet0/1
         MAC Address:  00cf.cb0d.aa10
        IPv6 Address:  Unknown
        IPv4 Address:  10.69.32.100
           User-Name:  VLAB\ville.naumanen
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A450A0A0000001128F69847
     Acct Session ID:  Unknown
              Handle:  0xF7000002
      Current Policy:  POLICY_Gi0/1

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:


Method status list:
      Method           State
      dot1x            Authc Success
```

Kuva 6. Todennuksen tarkemmat tiedot.

#debug dot1x all

- debug-komentoa voidaan käyttää vianetsinnässä, sillä debug dot1x all näyttää kytkimen komentorivillä kaiken kytkimessä tapahtuvan dot1x-liikenteen (kuva 7).



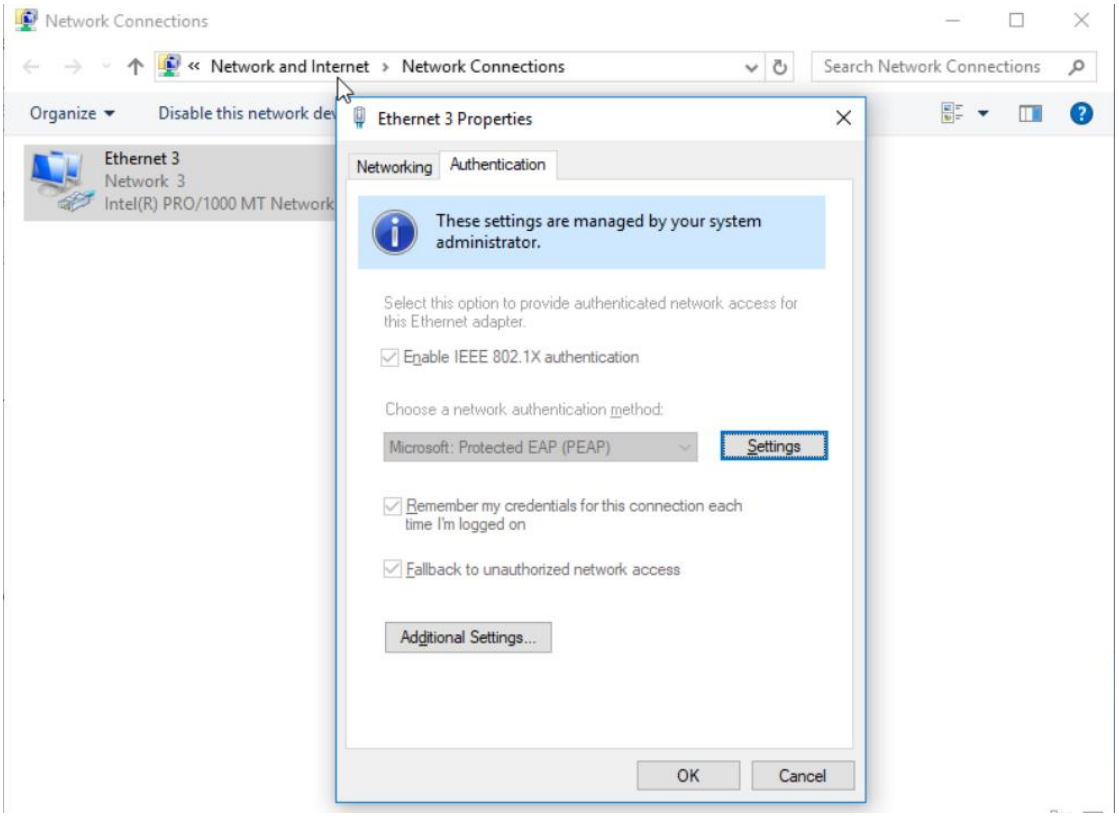
Kuva 7. debug dot1x all-komennon syöte

Debug saadaan pois päältä syöttämällä *#no debug dot1x all*-komento.

3. Työasemat

Työasemien tulisi saada vaadittavat autentikointitiedot palvelimen GP-päivitysten kautta. GP-päivitys voidaan tehdä myös manuaalisesti avaamalla tietokoneen komentokehote ja kirjoittamalla komento *gpupdate /force*, jolloin työasema hakee uusimman GP:n palvelimelta.

Saadut autentikointitiedot voidaan tarkistaa menemällä verkkoadapterin asetuksiin, jossa pitäisi näkyä *Authentication*-välilehti (kuva 8):



Kuva 8. Autentikonti-välilehti työasemalla