jamk

Langattoman verkkoympäristön toteutus RADIUS-protokollaa hyödyntäen

Kristoffer Rannasmaa

Opinnäytetyö, AMK
Toukokuu 2021
Tekniikan ala
Insinööri (AMK), Tieto- ja Viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Rannasmaa, Kristoffer

Langattoman verkkoympäristön toteutus RADIUS-protokollaa hyödyntäen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 50 sivua

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Langattomat verkot ovat nykyään hyvin tärkeitä, elleivät välttämättömiä toimivan yrityksien verkkoinfrastruktuurille. Langattomat verkot mahdollistavat yrityksille huomattavasti joustavammat työolosuhteet, sekä parantavat työntekijöiden työergonomiaa. Tämän vuoksi Combitech Oy:lle tarvittaisiin myös langaton lähiverkko, mutta tällaista ei ollut vielä pystytty toteuttamaan heränneiden tietoturvaseikkojen vuoksi.

Combitech Oy:lle haluttiin tämän vuoksi sellainen langaton verkkoympäristö, joka olisi toteutettu tavalla, että lähiverkon tietoturvallisuudesta voidaan olla varmoja. Toinen tärkeä tavoite verkkoympäristölle oli, että se pystytään ottamaan helposti käyttöön myös muissa Combitech Oy:n toimipisteissä. Tavoitteet olivat siis tietoturvassa ja helppokäyttöisyydessä. Verkkoympäristön toteutustavaksi valikoitui RADIUS-protokolla, jolla pystyttiin toteuttaman Combitech Oy:n asettamat tietoturvan ja helppokäyttöisyyden tavoitteet verkkoympäristölle.

Langatonta verkkoympäristöä lähdettiin toteuttamaan soveltavalla tutkimuksella, jossa käytetiin apuna kvantitatiivista tutkimusmenetelmää. Näihin tutkimusmenetelmiin päädyttiin sen vuoksi, että toteutettava aihe oli hyvin konkreettinen. Toteutuksessa oli hyvin vahvasti mukana laitevalmistajien tekemät ohjeet, joita seurattiin jokaisen eri palvelun asentamisen yhteydessä tarkasti. Toteutuksessa oli myös vahvasti osallisena erilaiset lokijärjestelmät, joista tutkittiin palveluiden antamia virheilmoituksia, ja niiden avulla selvitettiin, kuinka langaton verkkoympäristö saataisiin toteutettua onnistuneesti. Hankalissa tilanteissa jouduttiin myös turvautumaan erilliseen verkon liikenteen kaappaamiseen erikoistuneeseen sovellukseen, jota ilman ongelmanratkaisu olisi ollut hyvin haastavaa.

Lopullinen tulos verkkoympäristön toteutuksesta oli onnistunut RADIUS-ympäristö, jossa käyttäjät pystyttiin tunnistamaan tietoturvallisesti langattomassa verkossa. Lopulliseen RADIUS-ympäristöön asetettiin useita kovennuksia, jotta sen tietoturva pysyi korkealla tasolla. Kovennuksien avulla pystyttiin pääsemään Combitech Oy:n asettamiin tiukkoihin tietoturvavaatimuksiin. Ympäristöstä tuli halutun kaltainen, ja se pystyttiin pienellä vaivalla ottamaan käyttöön myös toisessa Combitech Oy:n toimipisteessä. Lopulta RADIUS-ympäristö, joka Combitech Oy:lle toteutettiin, todettiin hyväksi ja sille asetetut ehdot täyttäväksi.

Avainsanat (asiasanat)

AAA, EWC, NPS, PEAP, RADIUS, WLAN, 802.1x

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Rannasmaa, Kristoffer

Implementing wireless network environment using the RADIUS protocol

Jyväskylä: JAMK University of Applied Sciences, May 2021, 50pages

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Wireless networks have grown to be essential for a functioning business network infrastructure. Wireless networks enable companies to have much more flexible working conditions, as well as improve employee's ergonomy. For this reason, Combitech Oy also wants a functioning wireless network, but this has not been possible due to the arisen security issues about wireless networks.

Therefore Combitech Oy wanted a wireless network environment that would have been implemented in such a way that the security of the network environment could be assured. Another important goal for the network environment was ease of use. The network environment should be easy to implement in other Combitech Oy offices. Therefore, the goals for the network environment were in security and ease of use. The RADIUS protocol was chosen as the implementation method for the network environment, because it could provide the ease of use and security goals set by Combitech Oy.

The wireless network environments implementation was started with applied research, which was assisted by quantitative research methods. These research methods were picked because the topic was very specific. The equipment manufacturer's instruction manuals were strongly involved in the implementation, and they were followed very thoroughly. The implementation also strongly involved various logging systems, which were a lot of help when there were challenging problems. In the most difficult situations, it was also necessary to use a separate application specializing in capturing network traffic to find the solution for the most challenging problems.

The result of the implementation of the wireless network environment was a successful RADIUS environment, where users could be authenticated securely in the wireless network. Several security hardenings were also applied to the final RADIUS environment to maintain high security level. Hardening the wireless network environment were necessary to meet the high security requirements set by Combitech Oy. The final wireless network environment met the requirements set for it, and it could be put into use at another Combitech Oy office with little effort. The final RADIUS environment met its requirements fully.

Keywords/tags (subjects)

AAA, EWC, NPS, PEAP, RADIUS, WLAN, 802.1x

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

Tietoturvallisuus on nykyään IT-toimialan yrityksille tärkeimpiä huomiolle pantavia asioita. Tämän lisäksi kuitenkin helppokäyttöisyys on myös hyvin olennainen osa IT-infrastruktuuria, koska se vaikuttaa suoraan yrityksen tuottamisen tehokkuuteen. Nämä kaksi asiaa ovat olleet opinnäytetyöni toimeksiantajalla, Combitech Oy:llä, hyvin keskeisessä roolissa, kun yrityksen verkkoympäristöä on toteutettu.

Combitech Oy:llä on tällä hetkellä mahdollista käyttää verkkoyhteyttä toimipisteellä vain langallisesti Ethernet-pistokkeiden kautta, mikä ei ole kaikissa tilanteissa helpointa ja tehokkainta. Pistokkeita ei ole välillä välttämättä paikoissa missä niitä tarvittaisiin tai pistokkeita ei ole riittävästi, jolloin koneita joudutaan käyttämään verkossa vuorotellen tai pistokkeisiin joudutaan kytkemään erillisiä kytkimiä, jotta verkkopistokepaikkoja saadaan lisää työasemille. Näiden haittatekijöiden vuoksi yrityksessä on tutkittu, että olisiko tähän sisäverkkoon mahdollista ottaa käyttöön myös langatonta verkkoa, sillä sen avulla edellä mainitut haittatekijät saataisiin ratkaistua tehokkaasti.

Asian tutkimisen jälkeen todettiin, että langaton verkko olisi hyvin hyödyllinen, kunhan sen tietoturvallisuudesta pystytään varmistumaan. Tämä kuitenkin aiheutti seuraavan kysymyksen, mikä tekniikka on sopivin Combitech Oy:n langattoman verkon tarpeisiin? Asiaa lähdettiin tutkimaan, ja lopulta päädyttiin siihen, että RADIUS-protokolla vaikuttaa sopivimmalle ratkaisulle. RADIUS on yksi yleisesti käytössä olevista AAA-protokollista, ja siksi sen todettiin olevan hyvä valinta, sillä protokollan toiminta on hyvin tunnettua, joten sen voidaan todeta olevan varmasti tehokas ja toimiva.

Tavoitteena on siis tuottaa toimiva langaton verkkoympäristö RADIUS-protokollan avulla. Samalla vertaillaan RADIUS-protokollaa muihin yleisesti käytettyihin AAA-protokolliin, kuten esimerkiksi TACACS+ -protokollaan. Vertailussa luodaan protokollista listat niiden hyvistä sekä huonoista puolista, ja sen perusteella tutkitaan, että olisiko tulevaisuudessa syytä siirtyä toiseen vaihtoehtoon RADIUS:sta.

Vertailun jälkeen opinnäytetyössä on jäljellä vielä itse palveluiden konfiguraatio ja asennusvaihe. Käyttöönottoprosessi sisältää sekä langattomien tukiasemien, että RADIUS-palvelimen konfiguroimisen. Tämän lisäksi yrityksen valmiiseen sisäverkkoon joudutaan mitä ilmeisemmin tekemään

muutoksia kytkinten konfigurointeihin, sekä palomuuriasetuksiin. Koska yrityksen sisäverkko on ennestään jo hyvin tietoturvallinen, voi siinä olevat rajoitukset aiheuttaa asennusprosessissa erinäisiä haasteita.

Käyttöönoton aikana tehdään työstä myös erilliset muistiinpanot yrityksen omaan käyttöön. Nämä muistiinpanot tulevat olemaan huomattavasti teknisemmät ohjeet, joiden perusteella pystytään pystyttämään toinen vastaavanlainen langaton verkkoympäristö käyttäen samoja protokollia. Tämä ohje tullaan jakamaan Combitech Oy:n toiselle toimipisteelle Tampereelle, jossa otetaan myöskin käyttöön langaton verkkoympäristö, kunhan ensiksi se saadaan rakennettua toimivaksi Jyväskylään. Tämä antaa opinnäytetyön aiheelle entistä enemmän arvoa yritykselle, koska se tulee käyttöön laajasti yrityksen sisällä.

2 Langaton lähiverkko ja sen standardit

Langattomasta lähiverkosta on ajan saatossa tullut yksi hyvin tärkeä osa tiedonsiirtoa. Tähän on useita syitä, mutta yksi suurimmista on sen helppokäyttöisyys langalliseen verkkoon verrattuna. Se että käyttäjien ei tarvitse liittää tietokoneitaan tai muita laitteitaan mihinkään erilliseen telakkaan tai pistokkeeseen, tekee langattomasta lähiverkosta monelle helpoimman ratkaisun. Kuitenkaan langaton verkko ei aina ole ollut niin nopea kuin nykypäivänä. Tämän vuoksi langattomaan verkkoon on kehitetty ajan mittaan useita eri standardeja, jotka ovat aina kehittyneempiä kuin aikaisemmat. Alla olevassa taulukossa 1, on esiteltynä yleisimmin käytettyjen langattomien standardien eroja.

Taulukko 1 Langattomien standardien erot (Phillips 2021.)

IEEE Standardi	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Julkaisuvuosi	1999	1999	2003	2009	2014	2019
Taajuus	5GHz	2.4GHz	2.4GHz	2.4GHz & 5GHz	2.4GHz & 5GHz	2.4GHz & 5GHz
Korkein siirtonopeus	54Mbps	11Mbps	54Mbps	600Mbps	6.93Gbps	10-12Gbps

Taulukosta 1 voidaankin huomata, että tiedonsiirtonopeudet ovat olleet langattomassa verkossa hyvin pitkään huomattavasti hitaampia, kuin langallisessa. Vasta vuonna 2014 kehitetty standardi 802.11ac pystyy siirtämään dataa yli 1Gbps nopeudella, kun taas langallisessa verkossa gigabitin nopeuteen on päästy jo vuodesta 1999 alkaen. (Gigabit Ethernet, & 1000BASE-T n.d.)

Langaton lähiverkko on tuonut myös mukanaan paljon muita huomiolle pantavia asioita. Näitä ovat muun muassa tietoturva, langattoman verkon käyttämä taajuus sekä langattoman verkon kantavuus. Useat näistä asioista vaihtelevat eri standardeissa, koska niiden välillä on yleensä tapahtunut huomattavaa kehitystä aikaisempaan standardiin verrattuna.

2.1 802.11

Aivan ensimmäinen, alkuperäinen langattoman lähiverkon standardi 802.11 keksittiin jo vuonna 1997. Tämä standardi ei kuitenkaan koskaan yleistynyt kuluttajien ja yrityksien keskuudessa samalla tavalla kuin myöhemmät langattoman lähiverkon standardit. Alkuperäisen 802.11 standardin siirtonopeus oli 1-2Mbps, joka oli hyvin pieni verrattuna langalliseen verkkoon. Tämä mahdollisesti oli yksi syy, miksi standardi ei yleistynyt heti. Toimintaansa alkuperäinen 802.11 käytti 2.4GHz taajuutta, joka toimii perustana useille myöhemmin keksityille standardeille. (Riihikallio 2017.)

2.2 802.11a

Ensimmäinen IEEE:n määrittämä langaton standardi yleiseen käyttöön oli 802.11a. Tämä standardi julkaistiin vuonna 1999 802.11b standardin kanssa samaan aikaan. Ne olivat ensimmäisiä yleiseen käyttöön tarkoitettuja langattomia standardeja. Kuitenkaan 802.11a:sta ei tullut julkaisun aikana läheskään niin yleisesti käytettyä, kuin samoihin aikoihin julkaistusta 802.11b:stä. Tähän johti standardin korkeammat valmistuskulut, ja sen hankalammat käyttöönottovaatimukset. (Romano 2014.)

802.11a standardilla pystytään pääsemään parhaimmillaan 54Mbps siirtonopeuksiin, joka on huomattavasti korkeampi kuin samaan aikaan julkaistulla 802.11b:llä. 802.11a standardi toimii 5Ghz taajuudella, ja käyttää 20Mhz kaistanleveyttä. Standardilla arvioitu kantama on n. 30 metriä, mutta tähän pääseminen on haastavaa oikeassa käyttöympäristössä. Modulaationa standardissa

toimi OFDM. Taulukossa 2 on vielä näkyvillä 802.11a standardin ominaisuudet selkeämmin. (IEEE 802.11a n.d.)

Taulukko 2 802.11a ominaisuudet (IEEE 802.11a n.d.)

Siirtonopeus (Max	54Mbps
Kantama	n. 30 metriä
Modulaatio	OFDM
Taajuus	5GHz
Kaistanleveys	20Mhz

2.3 802.11b

IEEE:n toisena määrittelemä langaton standardi oli nimeltään 802.11b. Tästä standardista tuli julkaisun yhteydessä huomattavasti suositumpi, kuin sen kanssa samaan aikaan julkaistusta 802.11a standardista. Tämä johtui pääosin siitä, että 802.11b standardi käytti toimintaansa matalampaa 2.4Ghz taajuutta, johon osien rakentaminen oli halvempaa. (Romano 2014.)

Matalamman taajuuden käyttämisellä oli kuitenkin omat ongelmansa. 802.11b standardilla ei nimittäin pystytty saamaan kuin 11Mbps nopeuksia parhaimmillaan, mikä on huomattavasti heikompi kuin samaan aikaan julkaistulla 802.11a standardilla. Toisena ongelmana olivat muut laitteet, jotka käyttivät samaa taajuutta. Esimerkiksi mikroaaltouunit voivat häiritä hyvinkin voimakkaasti 2.4Ghz verkkoa. Etuina matalamman taajuuden käyttämisellä oli se, että langaton signaali 2.4Ghz taajuudessa läpäisi paremmin seiniä kuin korkeampi 5Ghz taajuus. (Romano 2014.)

Kantama 802.11b standardissa on arviolta kuitenkin sama kuin 802.11a:ssa, eli n. 30 metriä. Standardi käyttää myös samaa 20Mhz kaistanleveyttä. Modulaationa 802.11b:ssä on käytössä CCK. Alla olevassa taulukossa 3 on tiivistettynä 802.11b standardin tärkeimmät ominaisuudet. (IEEE 802.11a n.d.)

Taulukko 3 802.11b ominaisuudet (IEEE 802.11b n.d.)

Siirtonopeus (Max)	11Mbps
Kantama	n. 30 metriä
Modulaatio	CCK
Taajuus	2.4GHz
Kaistanleveys	20Mhz

2.4 802.11g

Vuonna 2003 julkaistiin uusi langaton standardi, joka tuli korvaamaan aikaisempaa 802.11b standardia. Uusi 802.11g standardi oli myös 2.4Ghz taajuudella toimiva, mutta se pystyi samoihin tiedonsiirtonopeuksiin kuin 802.11a standardi, eli 54Mbps. 802.11g standardissa olivat siis 2.4Ghz taajuuden edut, kuten parempi kuuluvuus seinien läpi ja halvemmat valmistuskustannukset, ja se pystyi samoihin nopeuksiin kuin 5Ghz taajuudella toiminut aikaisempi standardi. Tämän vuoksi 802.11g standardista tuli sen ajan yleisinten käytetty standardi. (Romano 2014.)

802.11g:n etuina oli myös taaksepäin yhteensopivuus 802.11b standardin kanssa. Koska standardi pystyi samoihin nopeuksiin kuin 802.11a, tuli sen myös käyttää samaa modulaatiota. Tämän vuoksi 802.11g standardissa olivat käytössä CCK, DSSS ja OFDM modulaatiot. Taulukkoon 4 on kerätty 802.11g:n tärkeimmät ominaisuudet. (IEEE 802.11g Wi-Fi n.d.)

Taulukko 4 802.11g ominaisuudet (IEEE 802.11g Wi-Fi n.d.)

Siirtonopeus (Max)	54Mbps
Kantama	n. 30 metriä
Modulaatio	CCK, DSSS tai OFDM
Taajuus	2.4GHz
Kaistanleveys	20Mhz

2.5 802.11n

IEEE julkaisi vuonna 2009 seuraavan langattoman standardinsa, jota yleisemmin alettiin kutsua nimellä Wi-Fi 4. Tämä standardi oli 802.11n, neljännen sukupolven langaton lähiverkko. Suurin muutos 802.11n standardissa oli se, että se tuki MIMO (Multiple-Input and Multiple-Output) tekniikkaa. Tämä tekniikka mahdollisti huomattavasti suuremmat tiedonsiirtonopeudet langattomassa verkossa, kuin mitä aikaisemmilla tekniikoilla pystyttiin saamaan. (Jongerius 2021.)

MIMO-tekniikka hyödyntää useampia antenneja, joiden avulla voidaan siirtää useampaa datastreamia samanaikaisesti. Tämä mahdollisti huomattavasti suuremmat siirtonopeudet langattomassa lähiverkossa. Korkein nopeus mitä Wi-Fi 4:llä pystytään siirtämään, on 600Mbps. Tämä on huomattava kasvu aikaisempaan nähden. 802.11n käyttää myös dual-band tekniikkaa, jolla se pystyy hyödyntämään yhtäaikaisesti kahta eri taajuutta datan siirtämiseen. Tämän vuoksi 802.11n standardi toimiikin sekä 2.4GHz ja 5GHz taajuuksilla. (Shaw 2020)

Modulaatioina Wi-Fi 4 käyttää samoja kuin aikaisempi 802.11g. Aiempaan standardiin nähden kaistanleveydessä on tullut myös päivitystä, Wi-Fi 4 tukee joko 20Mhz tai 40Mhz kaistanleveyttä. Suurempaa kaistanleveyttä tarvitaan korkeampien tiedonsiirtonopeuksien saavuttamiseksi. Taulukossa 5 on listattuna Wi-Fi 4:n ominaisuudet tiivistetysti.

Taulukko 5 802.11n ominaisuudet (IEEE 802.11n WLAN Standard n.d.)

Siirtonopeus (Max)	600Mbps
Modulaatio	CCK, DSSS tai OFDM
Taajuus	2.4GHz tai 5Ghz
MIMO	1–4 datastreamia
Kaistanleveys	20Mhz tai 40Mhz

2.6 802.11ac

Nykyään yksi yleisimmin käytetty langattoman lähiverkon standardeista on 802.11ac, jota myös kutsutaan nimellä Wi-Fi 5. 802.11ac standardi julkaistiin 2014, ja on huomattava kehitys 802.11n

standardiin nähden. Siitä löytyy myös täysi taaksepäin yhteensopivuus aikaisempien standardien kanssa. Wi-Fi 5 tuo mukanaan parhaimmillaan 160Mhz kaistanleveyden ja 8 yhtäaikaista datastreamia MIMO-tekniikan avulla. Näiden avulla huippunopeudeksi standardilla saadaan jopa 6.93Gbps, joka on todella suuri hyppy aikaisempaan huippunopeuteen nähden. (IEEE 802.11ac Gigabit Wi-Fi n.d.)

802.11ac kehittää myös MIMO-tekniikkaa eteenpäin, koska standardista löytyy uudempi MU-MIMO (Multi-User MIMO) -tekniikka. Modulaatio on kehittynyt myös huomattavasti eteenpäin Wi-Fi 5 standardissa, ja se on siirtynyt käyttämään aikaisempien standardien lisäksi QAM-modulaatiota. Standardissa on käytössä pääosin 5Ghz taajuus, mutta siinä on mahdollista myös käyttää 2.4Ghz taajuutta 5Ghz taajuuden lisänä. Näiden lisäksi 802.11ac sisältää uuden Beamforming tekniikan, jonka avulla se pystyy antamaan tarkasti vain tarvittavan määrän signaalia käyttäjille, ja täten olemaan entistä tehokkaampi tiedonsiirrossa. Alle on kerätty Wi-Fi 5:n olennaisimmat ominaisuudet taulukkoon 6. (Hardesty 2019.)

Taulukko 6 802.11ac ominaisuudet (IEEE 802.11ac Gigabit Wi-Fi n.d.)

Siirtonopeus (Max)	6.93Gbps
Modulaatio	BPSK, QPSK, 16-QAM, 64-QAM ja 256-QAM
Taajuus	5GHz (2.4GHz lisätehona)
MIMO	MU-MIMO-tuki maksimissaan 8 datastreamille
Kaistanleveys	20Mhz, 40MHz, 80MHz & 160MHz
Muuta	Beamforming -ominaisuus

2.7 802.11ax

Myös Wi-Fi 6 nimellä kutsuttu, uusin langattoman lähiverkon standardi on 802.11ax. Tämä standardi julkaistiin jo vuonna 2019, mutta sitä ei ole vielä otettu yleisesti käyttöön. Wi-Fi 6 on myös täysin taaksepäin yhteensopiva kuten aikaisemmatkin standardit. Uusina lisäyksinä Wi-Fi 6 tuo

OFDMA modulaation, joka on multi-user versio aikaisemmasta OFDM modulaatiosta. Tämä mahdollistaa useamman 802.11ax yhteyden samanaikaisesti langattoman reitittimen ja asiakaskoneiden välillä. (What is 802.11ax (Wi-Fi 6)? n.d.)

Wi-Fi 6 sisältää myös uudemman QAM modulaation, 1024-QAM. Tämän avulla laitteet, joilla on todella hyvä yhteys langattomaan tukiasemaan, pystyvät saamaan vieläkin nopeammat siirtonopeudet. Modulaatio kuitenkin vaati sen monimutkaisuuden takia, että yhteys langattoman lähettimen ja päätelaitteen välillä on todella hyvä. (What is 802.11ax (Wi-Fi 6)? n.d.)

Uusi huippunopeus 802.11ax standardissa ei ole paljoa aikaisempaa standardia korkeampi, se on vain noin 10Gbps. Korkeampi siirtonopeus ei kuitenkaan ollut Wi-Fi 6:n pääasiallinen kehityskohde, vaan yleisesti parempi käyttökokemus asiakaslaitteilla. Näihin lukeutuu sisään muun muassa parempi toimivuus alueilla, joissa on paljon langatonta verkkoa käyttäviä laitteita, tiedonsiirto yhtäaikaisesti useammalle asiakaslaitteille sekä pienempi virrankulutus. (IEEE 802.11ax Wi-Fi 6 n.d.)

Wi-Fi 6 tuo esimerkiksi uuden BSS colouring tekniikan, jonka avulla se muodostaa useita yhteyspisteitä asiakaslaitteille samalle kanavalle. Tämä ei näy asiakkaille mitenkään erilaisena, vaan he pystyvät normaalisti yhdistämään laitteensa langattomaan verkkoon. Langattoman lähettimen päässä kuitenkin nämä yhteyspisteet näkyvät niin sanotusti eri värisinä, jolloin lähetin voi siirtää usealle laitteelle dataa yhtä aikaa samalla kanavalla, kunhan se on vain yhdistettynä eri värisessä verkossa. Toinen tärkeä ominaisuus minkä Wi-Fi 6 tuo, on Target Wake Time. Tämä tekniikka on pääosin suunniteltu mobiililaitteiden akkujen säästämiseksi. Tekniikan ideana on se, että langaton lähetin huomaa milloinka asiakaslaite ei enää lähetä dataa, ja tällöin laittaa yhteyden lepotilaan. Näin yhteys ei koko ajan ole aktiivisena, ja asiakaslaitteen virtaa säästyy. Taulukkoon 7 on kerätty 802.11ax standardin tärkeimmät uudistukset. (IEEE 802.11ax Wi-Fi 6 n.d.)

Taulukko 7 802.11ax ominaisuudet (IEEE 802.11ax Wi-Fi 6 n.d.)

Siirtonopeus (Max)	9.6Gbps, tulevaisuudessa enemmän
Modulaatio	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM & 1024-QAM
Taajuus	5GHz & 2.4GHz

MIMO	OFDMA + MU-MIMO tuki maksimissaan 8 datastreamille
Kaistanleveys	20Mhz, 40MHz, 80MHz & 160MHz
Muuta	BSS colouring & Target Wake Time

2.8 Tietoturva langattomassa verkossa

Langattomat lähiverkot ovat tuoneet mukanaan kuitenkin ongelman, mikä ei ole läheskään niin näkyvä langallisessa verkossa, nimittäin tietoturva. WLAN (Wireless Local Area Network) -tukiasemat lähettävät koko ajan signaalia ympärillensä, mainostaen omaa langatonta verkkoaan. Tämän vuoksi kellä tahansa tukiaseman lähellä olevalla henkilöllä on mahdollisuus yrittää päästä sisälle verkkoon. Vastaavaa ongelmaa ei ole langallisessa lähiverkossa, koska hyökkääjä tarvitsee fyysisen pistokkeen, minkä kautta hän pääsee käsiksi verkkoon. Tämän ongelman vuoksi, langattomaan lähiverkkoon on kehitetty useita erilaisia tietoturvastandardeja, joista toiset on suunniteltu suurempiin langattomiin lähiverkkoihin, ja toiset pienempiin yksittäisten kuluttajien lähiverkkoihin. Näitä standardeja tulee päivittää myös jatkuvasti, jotta voidaan pysyä varmana, että langattomat verkot pysyvät tietoturvallisina. Useimmat vanhemmat langattoman verkon salausstandardit ovat nimittäin jo murrettuja, kuten WEP ja WPA (Bangeman 2007; Bayern 2018).

Nykyään yleisimmin käytetyt langattoman verkon suojausstandardit ovat WPA2-PSK CCMP-salauksella, ja WPA2-Enterprise. WPA2-PSK on suunnattu enemmän yksittäisille käyttäjille, kun taas WPA2-Enterprise on tarkoitettu suurempiin yrityksien verkkoihin. WPA2-PSK suojauksessa käytetään salasanaa langattomaan lähiverkkoon pääsemiseksi. Salasanasta luodaan CCMP-salauksen avulla yksilöllisiä avaimia jokaiselle laitteelle, joka pyrkii liittymään langattomaan verkkoon. Nämä avaimet vaihtuvat tasaisin väliajoin uusiin, jonka vuoksi salausta on hankala rikkoa. (Raphaely n.d.)

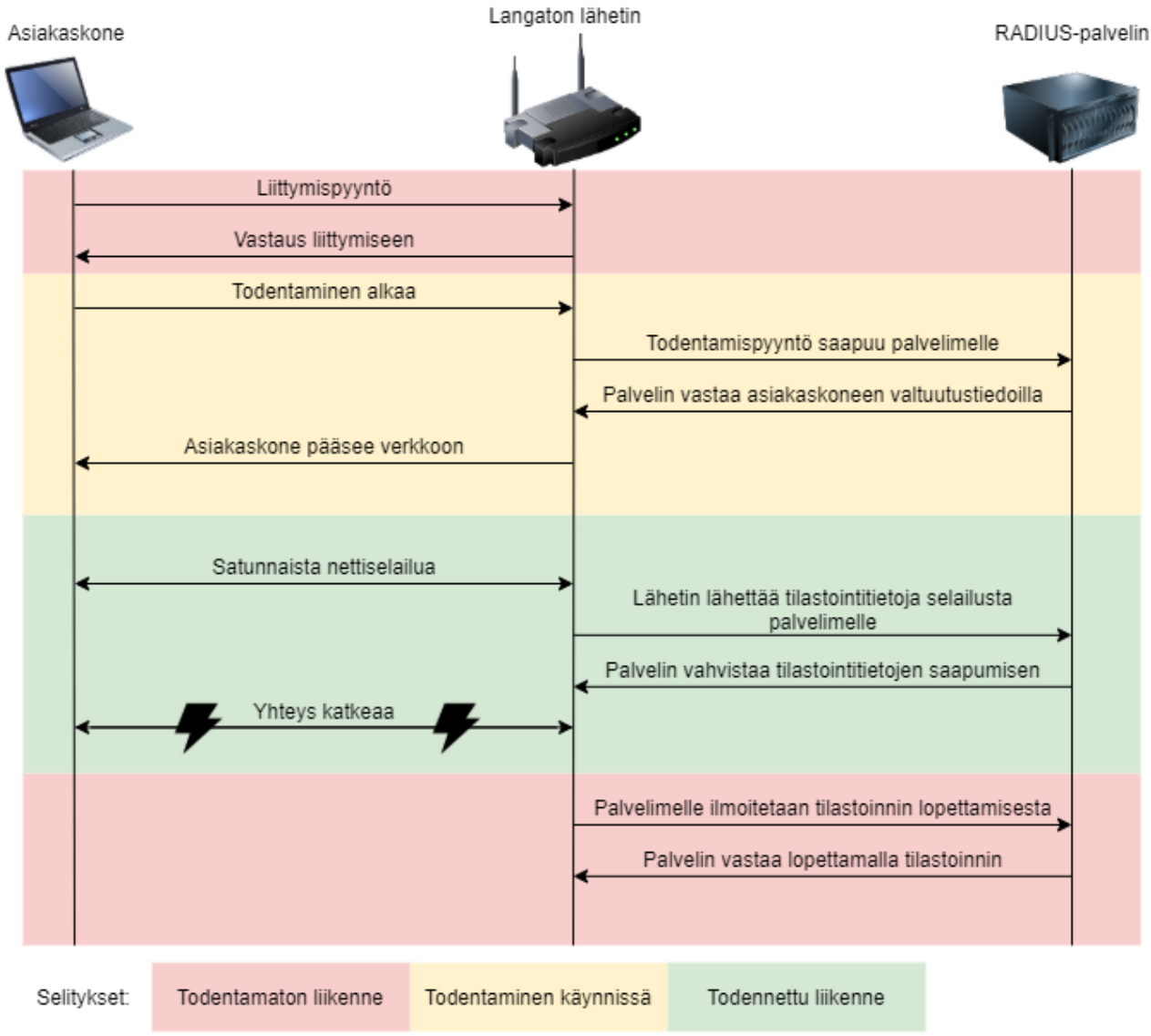
WPA2-Enterprise perustuu siihen, että verkossa on erillinen AAA-palvelin, esimerkiksi RADIUS-palvelin, jonka avulla huolehditaan verkkoon pääsevien käyttäjien tunnistautumisesta. Tunnistamisessa käytetään EAP-protokollaa, josta löytyy monia versioita. Yleisimmin käytetyt versiot ovat PEAP-MSCHAPv2 ja EAP-TLS. EAP-TLS on sertifikaatteihin perustuva menetelmä, jossa jokaisella käyttäjällä on oma sertifikaatti, jonka RADIUS-palvelin tunnistaa. PEAP-MSCHAPv2 on sen sijaan käyttäjätunnuksiin perustuva menetelmä, jossa jokainen käyttäjä tunnistetaan jollain tunnuksella,

joka voi olla käyttäjätunnus ja salasana, tietokone tai niiden yhdistelmä. Kumpaankin EAP-protokollaan pystytään tekemään myös asiakaskoneiden puolelta kovennuksia, kuten sertifikaattien validoimista. (Simplifying WPA2-Enterprise and 802.1x n.d.)

3 AAA-malli

Yksi tärkeimpiä asioita tietoverkkojen ylläpidossa on niiden tietoturvasta huolehtiminen. Mikään ei ole yrityksille vakavampaa, kuin datan vuotaminen ei haluttujen tahojen käsiin. Turvallisuudesta huolehtimiseen pystytään käyttämään AAA-mallia (Authentication, Authorization and Accounting). Tämä malli koostuu kolmesta osuudesta, joiden avulla pystytään todentamaan käyttäjä, valtuuttamaan käyttäjä ennalta määritettyjen oikeuksien mukaan ja tilastoimaan käyttäjän tekemät asiat muistiin. (de Laat, Gross, Gommans, Vollbrech & Spence 2000, 2.)

Alla olevassa kuviossa 1 on esitelty hyvin yksinkertaistetusti missä vaiheissa eri AAA-protokollan vaiheet tapahtuvat. Kuviosta selkenee hyvin, kuinka käyttäjä ensiksi todennetaan, jonka jälkeen käyttäjä saa määritetyt valtuudet sekä kuinka käyttäjän tekemät asiat tilastoidaan muistiin palvelimelle koko sen ajan, kun käyttäjä on verkossa.



Kuvio 1 RADIUS-todentamisen vaiheet

3.1 Authentication

Ensimmäinen osa AAA-protokollaa on käyttäjän todentaminen. Todentamisen avulla varmistetaan, ettei ylimääräisiä käyttäjiä pääse kirjautumaan verkkoon. Kaikista yleisin ja tutuin käytössä oleva menetelmä todentamiseen on käyttäjätunnus ja salasana. Käyttäjätunnukset ja salasanat ovat käteviä, mutta ne ovat yleisesti hyvin tunnettu riskitekijä yrityksille. Suurin riski niissä ovat niiden käyttäjät, joiden vastuulla käyttäjätunnuksen ja salasanan muistaminen sekä suojeleminen on. Tämän vuoksi esimerkiksi korkeamman turvallisuusluokan verkoissa pelkkä salasanalla ja käyttäjätunnuksella tunnistautuminen ei riitä. (Metzler n.d.)

AAA-protokollan todentaminen onneksi mahdollistaa käyttäjän tunnistamisen myös varmemmilla vaihtoehdoilla. Näitä vaihtoehtoja on kolme erilaista, joista käyttäjätunnus ja salasana ovat yksi. Nämä tavat ovat todentaa käyttäjä jollain mitä käyttäjällä on, jollain mitä vain käyttäjä tietää tai tunnistaa itse käyttäjä. Käytännön toteutuksen osiossa nämä todentamistavat tarkoittavat sertifikaatin todentamista, käyttäjätunnuksen ja salasanan kysymistä tai itse tietokoneen todentamista. Näitä aiemmin mainittuja todentamistapoja on myös mahdollista yhdistää, jolloin palvelun käyttämiseksi käyttäjän tulee todentaa itsensä useammalla tavalla, kuten sertifikaatilla sekä käyttäjätunnuksella ja salasanalla. (Santuka, Banga & Caroll 2011.)

3.2 Authorization

Seuraava osa AAA-protokollaa on käyttäjän valtuuttaminen, joka tapahtuu aina käyttäjän todentamisen jälkeen. Valtuuttamista ei pystytä tekemään, ellei käyttäjää ole ensiksi todennettu, jonka vuoksi nämä kaksi osuutta AAA-protokollasta ovat hyvin toisistaan riippuvaisia koko protokollan toiminnalle. Kun käyttäjä on onnistuneesti todennettu, käyttäjälle lisätään ennalta määritettyjen asetusten mukaiset oikeudet. Valtuutuksen avulla pystytään myös rajaamaan käyttäjältä oikeuksia, jos valtuutuksen säännöt ovat määritelty siten. Jos valtuutuksessa käyttäjä saa kielteisen päätöksen, valtuutusprosessi loppuu eikä RADIUS-asiakas yritä valtuuttaa käyttäjää uudelleen. (Authentication Authorization and Accounting Configuration Guide 2019.)

Käyttäjien oikeuksia pystytään määrittämään ryhmätasolla, tai yksittäisille käyttäjille voidaan antaa erityisiä oikeuksia. Valtuuttamisen onnistumiseksi AAA-järjestelmää ylläpitävällä palvelimella täytyy olla pääsy tietokantaan, josta se voi hakea käyttäjien oikeudet. Joissain tapauksessa käyttäjätietoja pystytään säilyttämään myös paikallisesti RADIUS-asiakkaalla. Käytännön toteutuksessa tietokantana toimi Domain Controller, jolla ylläpidettiin Active Directory Users and Computers roolia. Koko Active Directoryn käyttäjien- ja ryhmänhallinta tapahtuu tämän roolin kautta, joten RADIUS-palvelin pystyi hakemaan kaiken tarvitsemansa tiedon sen kautta. (Santuka, Banga & Caroll 2011.)

3.3 Accounting

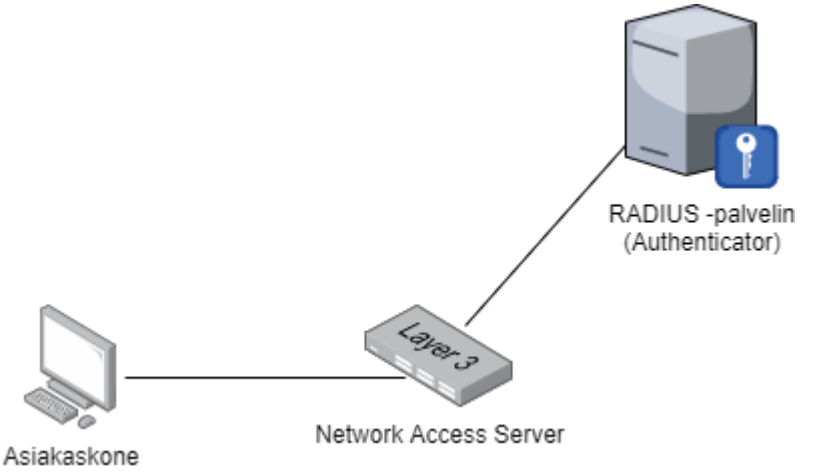
Viimeisenä osana AAA-protokollassa on tilastointi. Tilastoinnin avulla pystytään seuraamaan tarkasti mitä käyttäjät tekevät verkossa ollessaan. Näitä asioita mitä tilastoinnilla pystytään seuraavaan ovat muun muassa:

> käyttäjän session aloitusaika
> kuinka pitkään käyttäjän sessio on kestänyt
> milloin käyttäjä on lopettanut session
> kuinka paljon dataa käyttäjä on lähettänyt ja vastaanottanut (Securing the Corporate Network 2001.)

Tilastoinnin kaikki tiedot siirtyvät verkkolaitteiden kautta oletuksena AAA-palvelimelle, mutta palvelimelle on myös mahdollista määritellä, että tilastointi tapahtuu jollekin toiselle erilliselle palvelimelle. Yrityksen käytössä tällainen palvelin voisi olla keskitetty lokipalvelin, jolle kerätään kaikkien muiden palvelimien lokit. Palvelimelle kerätään myös tiedot kaikista epäonnistuneista kirjautumisista, joka on tärkeää tietoturvan kannalta, jotta voidaan olla tietoisia, jos jostain ulkoisesta lähteestä yritetään tunkeutua verkkoon sisään. (Santuka, Banga & Caroll 2011.)

3.4 RADIUS

Jotta AAA-protokollasta olisi jotain hyötyä, tarvitaan jokin järjestelmä millä sitä pystytään hyödyntämään. Yksi tällainen vaihtoehto on RADIUS-protokolla. RADIUS on client-server periaatteella toimiva, eli RADIUS-ympäristössä tulee olla aina vähintään yksi RADIUS-palvelin ja yksi -asiakas. Usein RADIUS-asiakkaita kutsutaan myös nimellä NAS, eli Network Access Server. Kumpikin nimitys on pätevä, ja tarkoittaa RADIUS-ympäristössä samaa laitetta. Kuviossa 2 on kuvattu pienin mahdollinen RADIUS ympäristö. Kuviossa RADIUS-asiakaslaite voisi olla joko langaton tukiasema tai kytkin, ja RADIUS-palvelimelta voisi olla yhteys yrityksen eri tietokantoihin ja muuhun verkkoon. Tässä esimerkkikuviossa RADIUS-palvelimella itsessään sijaitsee tietokanta, jota vasten asiakaskoneen tietoja verrataan, jonka vuoksi sillä ei ole yhteyttä muihin palvelimiin. (Newton 2017.)



Kuvio 2 Esimerkki RADIUS topologiasta

RADIUS käyttää toimintaansa yhteydetöntä UDP-protokollaa. Aikoinaan protokollaksi valittiin UDP, koska se yksinkertaistaa RADIUS-palvelimen rakennetta. Kun RADIUS:ta kehitettiin, olivat palvelimet vielä huomattavasti yksinkertaisempia kuin nykyään. Palvelimet eivät pystyneet käsittelemään tuolloin kuin yhden pyynnön kerrallaan, jonka vuoksi TCP-protokollaa ei voitu käyttää sen pidemmän tarkistusprosessin takia. Tämän vuoksi UDP:sta tuli RADIUS:n käyttämä standardi. RADIUS Authentication ja Authorization tapahtuvat UDP porteissa 1645 ja 1812, ja Accounting porteissa 1646 ja 1813. Nykyään 1645 ja 1646 porteista on pyritty siirtymään pois, koska ne on virallisesti rekisteröity toisille palveluille. Nämä portit eivät koskaan ole olleet RADIUS-palvelun virallisia portteja, vaan niitä on käytetty ennen kuin 1812 ja 1813 varattiin käyttöön. Tänä päivänä 1645 ja 1646 portit ovat vain jäänteitä RADIUS-palvelun historiasta. (Rigney, Willens, Rubens & Simpson 2000, 10; Rigney 2000, 1.)

Tarkat määritykset koko RADIUS-protokollasta löytyy IETF:n RFC-dokumenteista. RFC-dokumentissa 2865 on kerrottuna Authenticationista ja Authorizationista, ja dokumentissa 2866 on kerrottu Accountingista. (Rigney, Willens, Rubens & Simpson 2000; Rigney 2000.)

3.5 TACACS+ ja vertailu

Toinen yleisesti käytetty AAA-protokollavaihtoehto on TACACS+. TACACS+ on Ciscon kehittämä protokolla käyttäjien tunnistamiseen, joka eroaa ominaisuuksiltaan RADIUS-protokollasta.

Ciscon laitteet tukevat myös RADIUS-protokollaa, joten ne eivät rajaa käyttäjää käyttämään pelkkää TACACS+ -protokollaa. Suurin ero RADIUS- ja TACACS+ -protokollan välillä on se, että TACACS+ käyttää UDP:n sijasta TCP-protokollaa. TCP mahdollistaa sen, että kaikki yhteydet varmistetaan loppuun asti, kun taas UDP:ssa siirretään mahdollisimman paljon paketteja ilman niiden perille pääsemisen varmistamista. TCP:n käyttäminen myös parantaa informaation liikkumista palvelimien ja NAS-laitteiden välillä, sillä TCP paketit ilmoittavat, jos jokin laite on tavoittamattomissa tai toimii hitaasti. Vastaavaa toiminnallisuutta ei ole UDP:ssa, koska paketteja ei siinä varmisteta loppuun asti, vaan ne vain tiputetaan verkosta, jos ne eivät pääse perille. (TACACS+ and RADIUS Comparison 2008; Woland 2014.)

Pakettien salauksessa on eroja protokollien välillä. RADIUS-protokollassa ainoastaan access-request paketin salasana salataan, ja kaikki muu osa paketista menee selkokielisenä. TACACS+ -protokollassa sen sijaan salataan koko paketti TACACS+ -headeria lukuun ottamatta. Tämän vuoksi TACACS+ lähettämät paketit ovat huomattavasti tietoturvallisempia, ja tilanteessa, jossa joku kaappaa paketin, ei kaappaaja pysty saamaan siitä selville mitään käyttäjään liittyvää tietoa. (TACACS+ and RADIUS Comparison 2008.)

Authentication ja authorization pakettien käsittelyssä on myös eroja protokollissa. RADIUS-protokollassa nämä paketit käsitellään yhdessä, jonka vuoksi käyttäjäkoneelle saapuvat myös sen valtuutustiedot, joka ei ole välttämätöntä toiminnalle. TACACS+ -protokollassa paketit ovat erillisiä, jonka vuoksi käyttäjien todentamiseen voidaan käyttää useampaa eri tunnistustapaa. Myöskin tilanteissa, joissa käyttäjiltä tarvitaan uudelleentodennus, TACACS+ pystyy tämän tekemään yhdellä kysymyksellä, sen sijaan että koko todentamis- ja valtuutuskäsittelyä tarvittaisiin tehdä alusta asti uudelleen. (TACACS+ and RADIUS Comparison 2008.)

Näiden ominaisuuksien lisäksi protokollien välillä on myös muita pienempiä eroja. Nämä erot on lueteltu taulukossa 8, josta pystyy vertailemaan protokollia keskenään.

Taulukko 8 RADIUS ja TACACS+ erot (Woland 2014; TACACS+ Advantages 2011, 3)

	RADIUS	TACACS+
Protokolla	UDP	TCP

Portti	1812, 1813, 1645 ja 1646	49
Pakettien salaus	Salaa vain salasanat	Salaa koko paketin
NAS-hallinta	Kaikille laitteille tulee konfiguroida todentaminen	Keskitetty palvelin todentaa kaikki asiakkaat
Authentication ja Authorization	Yhdistää todentamisen ja valtuutuksen	Todentaminen ja valtuutus tapahtuu erilleen
Käyttötarkoitus	Käyttäjien salliminen verkkoon	NAS-laitteiden hallinta

4 Käytännön toteutus ja testaus

Koska Combitech Oy:n lähiverkossa ei ollut aikaisempaa langatonta verkkoa käytössä, käytännön osuus tuli aloittaa kartoittamalla tarvittavat laitteet ja palvelut toiminnan mahdollistamiseksi. Aluksi lähdettiin siis selvittämään mitä kaikkea tarvittaisiin toimivan RADIUS-protokollaa käyttävän langattoman ympäristön toteuttamiseen. Selvitykseen käytettiin hyvin aikaa, jotta mahdollisilta yhteensopivuusongelmilta pystyttiin välttymään. Tärkeässä osuudessa palveluiden toteuttamisessa oli myös se, että ne toteutettiin samankaltaisilla käyttöjärjestelmillä kuin muut palvelut. Täten voitaisiin välttyä yksittäisiltä, hyvin paljon muista eroavilta palveluilta, jotka vaatisivat erityistä ylläpitotietoa ja -kokemusta. Näin pystyttiin varmistumaan myös siitä, että järjestelmän käyttö on helppo opetella ja dokumentoida mahdollisten häiriötilanteiden varalle.

4.1 Laitteisto ja alustat

4.1.1 Langattomat tukiasemat

Combitech Oy:n langattoman verkkoympäristön tarpeita lähdettiin kartoittamaan ensimmäisenä langattomista tukiasemista. Yrityksen verkossa ei ollut ollenkaan sillä hetkellä langattomia tukiasemia, joten ensimmäisenä vaiheena oli selvittää, millaiset tukiasemat sopisivat yrityksen käyttöön. Laitteiden merkissä päädyttiin Ciscoon, koska Combitech Oy:n sisäverkossa oli jo valmiiksi käytetty Ciscon kytkimiä. Henkilöstöllä oli myös valmiiksi kokemusta Ciscon laitteista, joten se oli ehdottomasti paras valinta. Helppokäyttöisyyden vuoksi päädyttiin myös siihen, että langattomilla tukiasemilla tulisi olla Power Over Ethernet tuki. Tällöin langattomat tukiasemat eivät tarvitsisi ollenkaan erillisiä virtajohtoja, vaan ne saisivat tarvitsemansa virtansa PoE-yhteensopivalta kytkimeltä Ethernet portin kautta. Näin loppuvaiheessa langattomien tukiasemien sijoittaminen ja asentaminen

tiloihin olisi huomattavasti helpompaa ja vapaampaa, kun ylimääräisistä johdoista ei tarvitse huolehtia.

Huomattavan tärkeäksi ominaisuudeksi lukeutui myös langattomien tukiasemien keskitetty hallinta. Jyväskylän toimipisteen kytkimet eivät olleet yhteensopivia tukemaan langattomien tukiasemien keskitettyä hallintaa, jonka vuoksi itse tukiasemista tulisi löytyä tämä toiminto. Harkinnan jälkeen lopulliseksi vaihtoehdoksi valikoitui Ciscon 9115-sarjan langattomat Wi-Fi 6 tukiasemat. Kyseisestä langattomasta lähettimestä kuitenkin löytyi useampaa versiota. Alla olevassa taulukossa 9 on listattuna eri versioiden ominaisuudet.

Taulukko 9 Catalyst 9115 mallien eroavaisuudet (Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet 2021.)

Malli	Antennit	Käyttötarkoitus
Catalyst 9115AXI	Sisäiset	Helppoihin sisätiloihin
Catalyst 9115AXE	Ulkoiset	Haastaviin sisätiloihin
Catalyst 9115AXI-e	Sisäiset	Helppoihin sisätiloihin, Controller
Catalyst 9115AXE-e	Ulkoiset	Haastaviin sisätiloihin, Controller

Taulukon 9 perusteella voidaan huomata, että Catalyst 9115 mallista on neljä versiota, joista toisissa on sisässä jo valmiiksi keskitettyyn hallintaan tarkoitettu ohjelmisto, ja toisissa langattomana tukiasemana toimimiseen tarkoitettu ohjelmisto. Näiden lisäksi on vielä erikseen mallit, joissa on ulkoiset antennit haastaviin tiloihin, ja mallit missä on sisäiset antennit. Näistä vaihtoehdoista päätettiin ottaa sisäisten antennien mallit, koska Jyväskylän toimiston tilat eivät ole niin haastavat langattoman verkon suunnittelun suhteen, että ulkoisten antennien katsottaisiin olevan tarpeellisia. Lopullisiksi valinnoiksi päätyivät neljä kappaletta 9115AXI-malleja ja yksi 9115AXI-e -malli.

Viiden langattoman tukiaseman tilaamiseen päädyttiin myös harkitsemisen jälkeen. Neljällä tukiasemalla Jyväskylän toimipisteeseen olisi voinut jäädä katvealueita, jotka olisivat olleet häiritseviä verkon käyttökokemuksen kannalta. Kuudella tukiasemalla kattavuus olisi voinut olla parempi, mutta siitä saatu hyöty olisi ollut niin pieni, että sen hinta- ja hyötysuhde olisi ollut huono. Tämän

vuoksi todettiin, että viisi tukiasemaa on sopivin määrä. Neljä langatonta tukiasemaa olisi myös voinut toimia, koska keskitetyn hallinnan vuoksi tarvittaessa tukiasemien lisääminen verkkoon on hyvin vaivatonta. Tähän ei kuitenkaan päädytty, koska tällöin olisi kuitenkin jouduttu asentamaan tukiasemat uudelleen toimitilojen kattoon, ja tästä olisi koitunut lisää ylimääräistä työtä. Todettiin myös, että jos viisi tukiasemaa onkin liikaa Jyväskylän toimipisteellä, voi valmiiksi asennetun tukiaseman lähettää postitse toiseen toimipisteeseen.

Catalyst 9115 langattomien tukiasemien tietojen tarkemman tutkimisen myötä, huomattiin myös niistä yksi todella hyödyllinen uusi ominaisuus. Kyseisissä tukiasemissa on mahdollista muuttaa sen ohjelmistoversio normaalista CAPWAP-ohjelmistosta, joka tukee vain langattomien asiakkaiden palvelemista, EWC-ohjelmistoon, joka on keskitettyyn hallintaan suunniteltu käyttöjärjestelmä. Näin mistä tahansa tukiasemasta pystytään tekemään halutessaan hallintatukiasema. (Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE Gibraltar 16.12.x 2021.)

Näin ollen laitteita tilatessa olisi voitu ottaa vain yksinkertaisempia malleja, mutta tähän ei päädytty ohjelmiston muuntamisen suositusmenetelmien vuoksi. Muuntamisessa suositeltuna on ladata EWC-hallintakäyttöjärjestelmä Ciscon omilta sivuilta, ja laittaa se yrityksen itse ylläpitämälle TFTP-palvelimelle. Tämän jälkeen tukiasemalle tulisi antaa komento sen käyttöliittymästä, jolla tukiasema lataa ohjelmiston ja asentaa sen entisen tilalle. Tämä olisi vaatinut ylimääräisen palvelimen toiminnon pystyttämistä tai palomuuriavauksia, jonka vuoksi päädyttiin, että on helpompaa tilata suoraan malli, josta löytyy keskitettyyn hallintaan tarkoitettu käyttöjärjestelmä. (Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE Gibraltar 16.12.x 2021.)

4.1.2 RADIUS-palvelin

Langattomien tukiasemien lisäksi RADIUS tarvitsee vielä toimiakseen myös erillisen palvelimen, jolle tunnistautumispyynnöt saapuvat ja jolla ne todennetaan. Joissain WLAN-tukiasemissa on sisäänrakennettuja ominaisuuksia, jolloin niitä voisi käyttää itsessään RADIUS-palvelimena. Tällaista ratkaisua ei kuitenkaan haluttu, koska todettiin että virtualisoidun RADIUS-palvelimen hallinta on helpompaa, kun se on erillisellä käyttöjärjestelmällä omana palvelimena. Ratkaisua vahvisti erityisesti helppokäyttöisyys ja palvelujen yhtenäisenä pitäminen, sillä RADIUS-palvelin toimisi samalla

virtualisointialustalla kuin muut palvelimet, ja se tilastoisi tietoja helposti saatavilla olevaan sijaintiin.

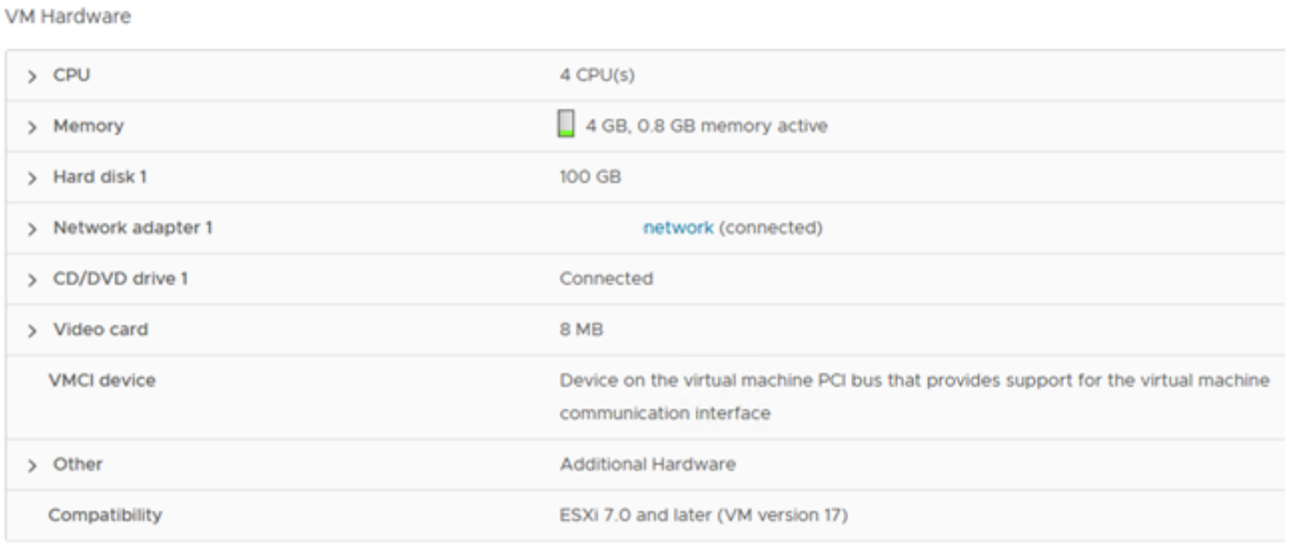
RADIUS-palvelimelle löytyi monenlaisia ratkaisuita. Useimmat vaihtoehdoista olivat palvelimelle asennettavia erillisiä ohjelmia, mutta RADIUS olisi ollut saatavilla myös pilvipalveluna. Pilvipalvelulla toteutettu RADIUS-palvelin ei kuitenkaan ollut vaihtoehto, koska yrityksen sisäisiä käyttäjätietoja ei haluta pääsevän ulkoverkkoon. Tämä olisi itsessään jo tietoturvariski, koska käyttäjätiedot säilyisivät silloin jonkun toisen yrityksen palvelimilla. Vaihtoehdoksi jäi siis paikallinen RADIUS-palvelin.

Paikalliseen RADIUS-palvelimeen löytyi myös useampia ratkaisuja. Asiaa tutkimalla suosituimmiksi palveluiksi osoittautuivat FreeRADIUS, ja Microsoft Serverin sisäänrakennettu NPS-rooli, jossa on täysi RADIUS tuki. FreeRADIUS vaikutti hyvältä vaihtoehdolta, mutta valintaan vaikutti vahvasti se, että FreeRADIUS toimii linux-ympäristössä. Microsoftin Windows Server oli jo valmiiksi enemmän käytetty palvelinympäristössä, ja se oli myös useammille tutumpi vaihtoehto, joten se valikoitui lopulliseksi vaihtoehdoksi. Windows Serverin NPS-roolista myös löytyi hyvin paljon dokumentaatiota, joka vaikutti myös positiivisesti sen valintaan. RADIUS-palvelin päätettiin siis asentaa Windows Server 2019 palvelimelle NPS-roolia hyödyntäen.

4.2 RADIUS-ympäristön toteutus

4.2.1 Palvelimen asennus

Ympäristön toteuttaminen aloitettiin ensiksi miettimällä järkevin kohde, mistä asentaminen kannattaisi aloittaa. Tämän todettiin olevan itse RADIUS-palvelin, jonka vuoksi asentaminen aloitettiin Windows Server 2019:sta. Palvelin asennettiin täysin virtuaaliseen ympäristöön, jonka vuoksi ensimmäisenä tarvittiin luoda uusi virtuaalikone virtuaalialustalle. Palvelimelle arvioitiin sopivaksi määräksi 4GB muistia, ja sille annettiin 100GB levytilaa. Alla olevassa kuviossa 3 on näkyvillä virtuaalikoneelle määritetyt asetukset.



Kuvio 3 RADIUS koneen määritykset

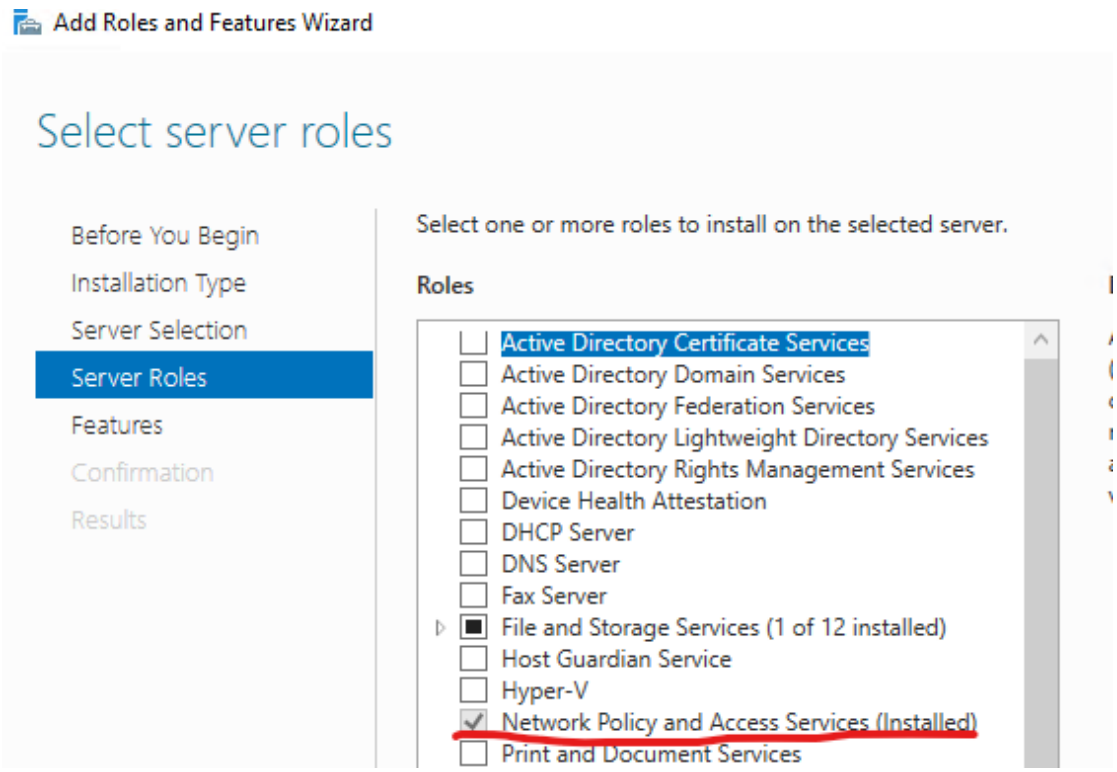
Virtuaalikoneen asetuksien määrityksen jälkeen sille liitettiin Windows Server 2019 levykuva, ja se laitettiin käynnistysasemaksi koneelle. Virtuaalikone käynnistettiin, ja Windows Serveristä asennettiin Standard versio graafisella käyttöliittymällä. Asennuksen tyypiksi valittiin Custom Installation, koska virtualikoneen levyllä ei ollut ennestään mitään dataa. Mitään ylimääräisiä partitioita ei myöskään palvelimelle tehty, vaan se asennettiin koko levytilalle. Windows Server 2019 asennus oli hyvin suoraviivainen ja yksinkertainen prosessi. (Mutai, J 2019.)

Windows Server 2019 asennuksen valmistuttua koneelle päätettiin asentaa saman tien vmware-tools niminen yhteensopivuusohjelma. Vmware-tools auttaa virtuaalipohjalle asennettuja käyttöjärjestelmiä mukautumaan virtuaaliympäristöön paremmin. Tämä esimerkiksi mahdollistaa virtuaalikoneen ruudun resoluution muuttamisen koneen ollessa käynnissä yksinkertaisesti ikkunan kokoa skaalaamalla, äänilaitteiden paremman toiminnan ja ulkoisten liitettävien laitteiden ymmärtämisen virtuaalikoneella. Pääosin vmware-tools asennettiin, jotta virtuaalikoneen näyttö saatiin skaalattua sopivan kokoiseksi.

Jotta juuri asennetulle RADIUS-palvelimelle saataisiin yhteys muista laitteista, tuli tämä palvelin sallia palomuurilla. Palomuurilla asetettiin RADIUS-palvelimelle säännöt, jotka mahdollistivat siihen käsiksi pääsemisen. Sääntöjen asettamisen jälkeen palvelimelle määritettiin staattinen ip-osoite, jotta sille kommunikointi olisi mahdollista helpommin eikä laitteen ip-osoite vaihtuisi tietyn

väliajoin. Kun verkkoasetukset oli määritetty loppuun, voitiin kone liittää Combitech Oy:n domainiin, jonka jälkeen RADIUS-palvelin oli nähtävissä verkossa. RADIUS-palvelin asetettiin sen jälkeen Domain Controllerilla servereille tarkoitettuun ryhmään, jotta se saisi sopivat määritykset Group Policyiden kautta.

Näiden vaiheiden jälkeen itse RADIUS-palvelua voitiin lähteä asentamaan. Windows Serverissä RADIUS toimii osana Network Policy Services (NPS) -roolia. Tämä rooli sisältää tarvittavat ominaisuudet RADIUS-palvelimen ja -asiakkaiden konfiguroimiseen siten, että RADIUS-palvelin pystyy hakemaan käyttäjätiedot suoraan Active Directorystä. NPS-rooli asennettiin Server Managerin Add Roles and Features valikosta kuvion 4 mukaisella valinnalla. (Kardashevsky, C 2021.)



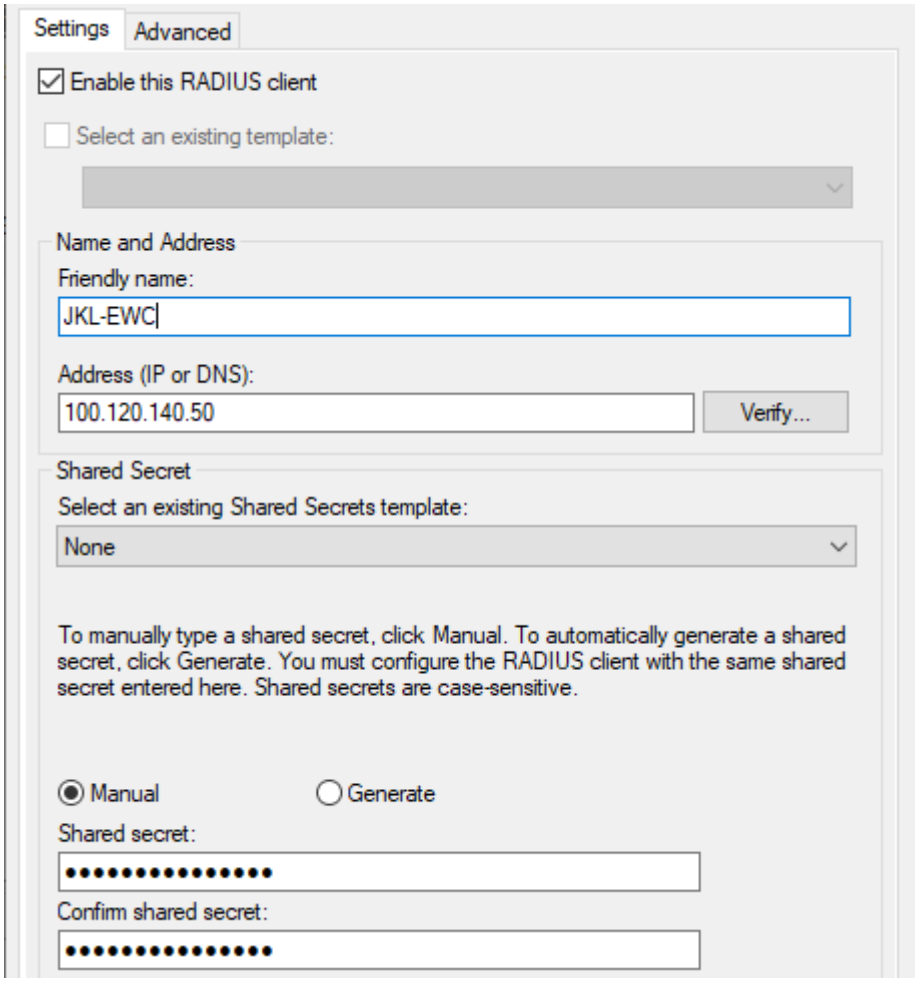
Kuvio 4 NPS-roolin asennus

NPS-roolin asennuksen jälkeen tulee ensimmäisenä asiana rekisteröidä luotu RADIUS-palvelin osaksi Active Directoryä. Tämä tapahtuu avaamalla NPS työkalu Server Managerin kautta, ja sen jälkeen NPS (Local) kohdasta valitsemalla Register server in Active Directory. Ellei tätä vaihetta tehdä, ei palvelin pysty lukemaan tietoja Active Directorystä, jolloin se ei pysty vahvistamaan käyttäjien identiteettiä, kun he yrittävät kirjautua langattomaan verkkoon. Tämän seurauksena kukaan

ei pystyisi käyttämään langatonta verkkoa, jotka on konfiguroitu ottamaan yhteyttä RADIUS-palvelimeen, eli tässä tilanteessa Cisco Catalyst 9115AXI langattomat tukiasemat. Kuviosta 5 näkyy vielä tarkemmin tämä tärkeä vaihe. Rekisteröitymisen jälkeen RADIUS-palvelin lisätään Active Directoryssä automaattisesti RAS and IAS servers -ryhmään, jonka kautta palvelin saa itselleen sertifikaatin. (Kardashevsky, C 2021.)

Kuvio 5 RADIUS-palvelimen rekisteröiminen AD:hen

Palvelimelle aloitetaan lisäämään RADIUS-asiakkaita valitsemalla RADIUS Clients kohdassa New. NPS-rooli itse opastaa hyvin mitä mihinkin kohtaan tarvitsi asettaa. RADIUS-asiakkaille on tärkeintä määrittää oikein sen IP-osoite ja salasana. Jos haluttaisiin, tähän kohtaan voitaisiin määrittää yksi osoiteavaruus, josta RADIUS-asiakkaita etsittäisiin. Tämä ei kuitenkaan ollut tarpeellista, koska ympäristössä oli ainoastaan yksi controller, jonka kautta muut RADIUS-asiakkaat siirtävät todentamistietonsa. Salasanan avulla RADIUS-asiakkaat tunnistautuvat palvelimelle, joten jos se on kummassakaan päässä erilainen, ei tunnistautuminen onnistu. Kuviossa 6 on esimerkkiasetukset RADIUS-asiakkaasta. Kuvioissa esiintyvät IP-osoitteet eivät ole ympäristössä käytettäviä lopullisia IP-osoitteita, vaan osoitteita on muutettu tietoturvan vuoksi.

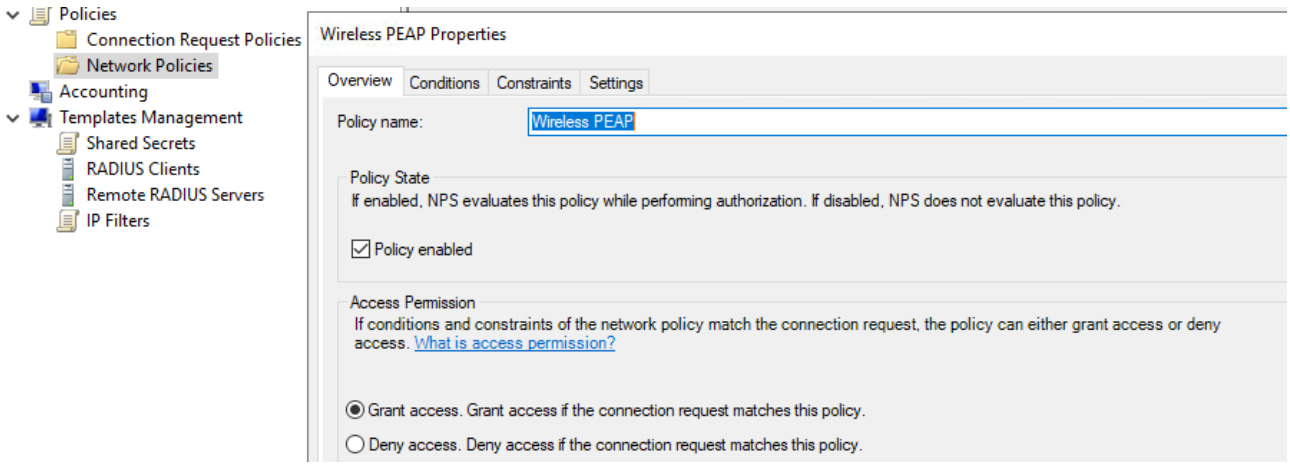


Kuvio 6 RADIUS-asiakkaan asetukset

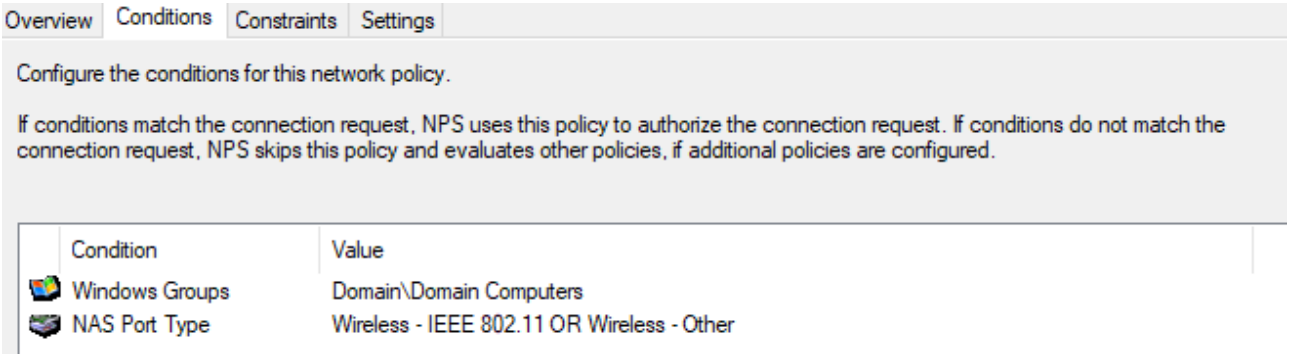
RADIUS-asiakkaan asetusten laittamisen jälkeen on vuorossa Network Policyn määrittely. Policies valikon alta valitaan uusi Network Policy, ja määritellään sille Access Permissioniin vaihtoehto Grant Access. Tämä sen vuoksi, että RADIUS-palvelimen halutaan antavan oikeuksia päästä verkkoon. Jos olisi tarvetta, RADIUS-palvelimelle voitaisiin luoda myös Deny Access Policy, jolla voitaisiin estää tiettyjen käyttäjien pääsy verkkoon. Nyt tarvetta tosin ei ole, joten sitä ei määritelty.

Conditions kohdassa määritellään Policyn ehdot. Policy astuu käyttäjälle vain silloin voimaan, jos kaikki conditionsin ehdot täyttyvät. Tässä tilanteessa ehdoiksi asetettiin, että käyttäjä tulee langattomasta verkosta, sekä käyttäjän tietokone sijaitsee AD:n Domain Computers ryhmässä. Tähän kohtaan pystyttäisiin määrittelemään huomattavasti tarkempia ehtoja, kuten että tietokone tulee tietystä IP-osoitteesta.

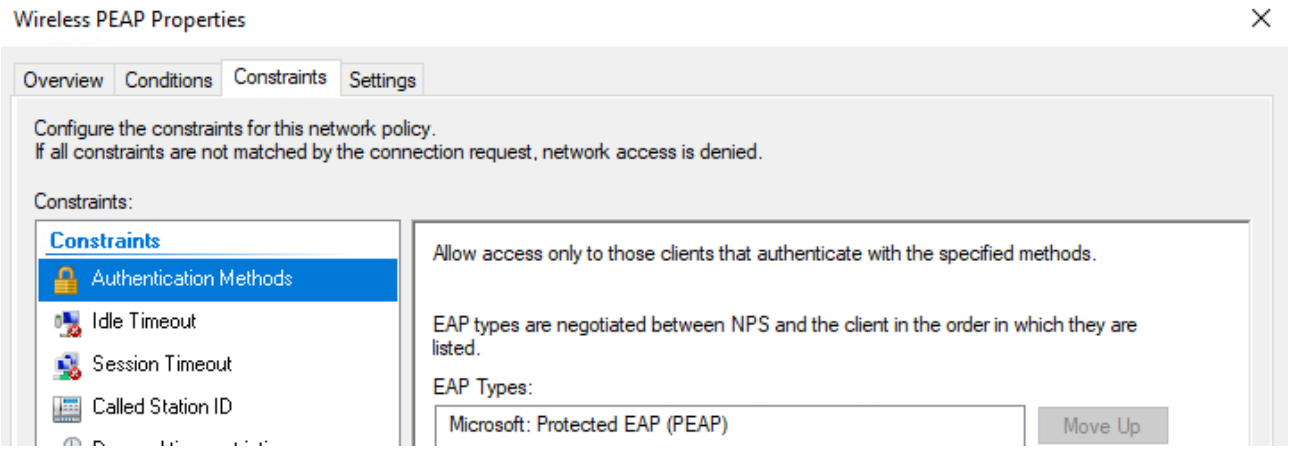
Viimeisenä Constraints kohdassa määritellään autentikaatioprotokolla, mitä policyn tahdotaan käyttävän. Koska käyttäjäkoneiden halutaan tarkistavan, että RADIUS-palvelimella sijaitsee sertifikaatti, joka löytyy myös niiden oman juurisertifikaatin polusta, asetetaan EAP-tyypiksi Microsoft Protected EAP (Liang, Chen, & Xu 2020). Protected EAPin asetuksista asetetaan vielä, että käyttäjän tulee myös sertifikaatin tunnistamisen lisäksi tunnistautua käyttäjätunnuksella ja salasanalla, joka tässä tapauksessa on käyttäjän tietokone, koska se määriteltiin Conditions-valikossa ehdoksi. Mitään heikompia todentamismenetelmiä ei aseteta, jottei verkon tietoturva kärsisi. Näistä kolmesta vaiheesta löytyy esimerkit kuvioista 7, 8 ja 9.



Kuvio 7 Network Policyn Access Permission



Kuvio 8 Network Policyn ehdot



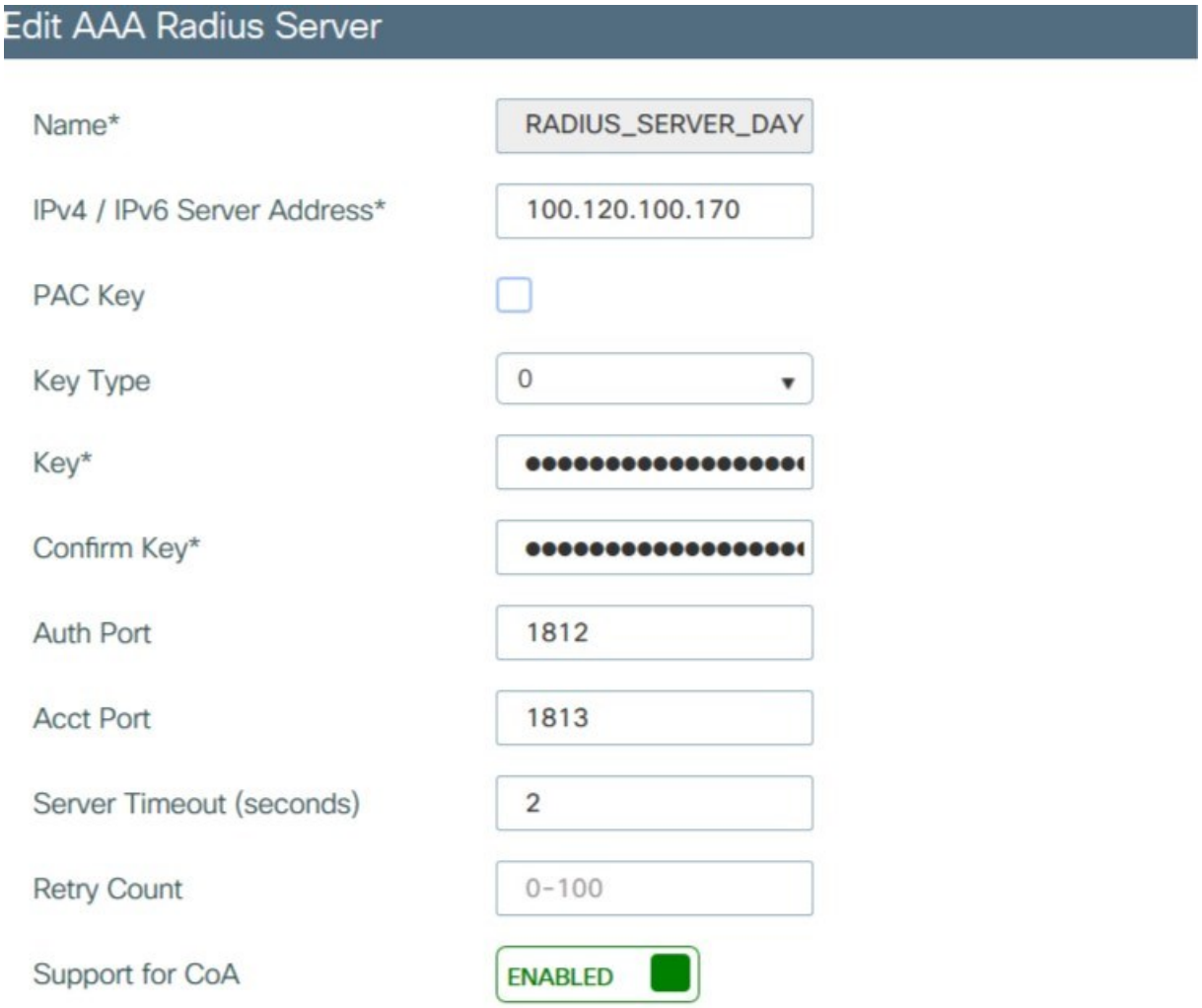
Kuvio 9 Network Policyn todentamisprotokolla

Viimeiseksi RADIUS-palvelimelle tuli luoda Connection Request Policy. Tämän ei tulisi olla pakollista, mutta RADIUS ei suostunut todentamaan käyttäjää ilman sitä. Sen vuoksi luotiin yksinkertainen Request Policy, joka laitettiin tarkistamaan vain, että käyttäjä on langattomasti yhteydessä verkossa. Request Policyn enabloinnin jälkeen RADIUS-palvelimen asetukset olivat valmiina.

4.2.2 Langattomien tukiasemien asennus

Ciscon langattomien tukiasemien konfigurointi oli kaikista helpoin vaihe ympäristön toteuttamisesta. Konfigurointi oli tehty hyvin suoraviivaiseksi ja Ciscon omilta verkkosivuilta löytyi hyvin kattavat ohjeet WLAN-tukiasemien käyttöönottoon. Käyttöönotto suoritettiinkin seuraamalla täysin valmista opastusta. WLAN-tukiasemat käynnistyivät heti kun ne liitettiin PoE yhteensopivaan kytkimeen, ja hetken päästä ne mainostivat asennukseen käytettävää langatonta verkkoa. Tähän langattomaan verkkoon muodostettiin yhteys salasanalla password. Onnistuneen langattoman yhteyden muodostumisen jälkeen avattiin selaimella osoite mywifi.cisco.com, jonne pääsi kirjautumaan käyttäjätunnuksella webui ja salasanalla cisco. Sivusto antoi hyvin yksinkertaiset kentät, joihin sai määritettyä WLAN-tukiaseman IP:n, ja langattomat verkot mitä sen halutaan jakavan. Sivustolla tuli asettaa myös hallintasivulle uusi käyttäjätunnus ja salasana, jotta käyttöönoton jälkeen vakiotunnus ei enää toimisi. (Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) White Paper 2020.)

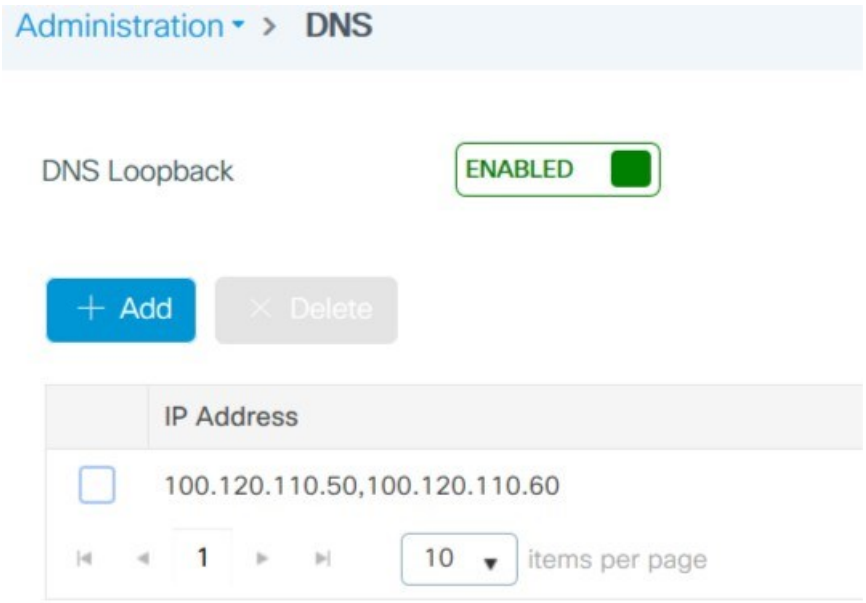
WLAN-tukiasemalle, josta oli tulossa controller verkkoon, asetettiin IP-osoitteeksi 100.120.140.50 ja sen verkkomaskiksi asetettiin /24. Langattomiksi verkoiksi luotiin ensiksi WPA2 salauksella toimiva verkko, siltä varalta, että WPA2-Enterprisellä toimiva verkko ei toimisikaan. WPA2-Enterprise verkon määrittely oli hyvin yksinkertaista laitteen asennuksen yhteydessä. Langattoman verkon profiilille tuli asettaa vain RADIUS-palvelimen IP-osoite, sekä sen salasana. Tämän jälkeen WLAN-tukiasema loi itse kaikki loput tarpeelliset profiilit verkolle. Kuviossa 10 näkyy WPA2-Enterprise -verkolle asetetut määritykset hallintasivulla ensimmäisen käytönoton jälkeen.



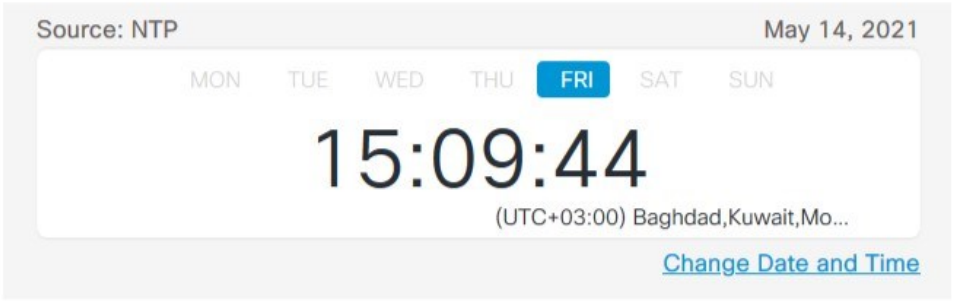
Kuvio 10 RADIUS-asetukset hallintasivulla

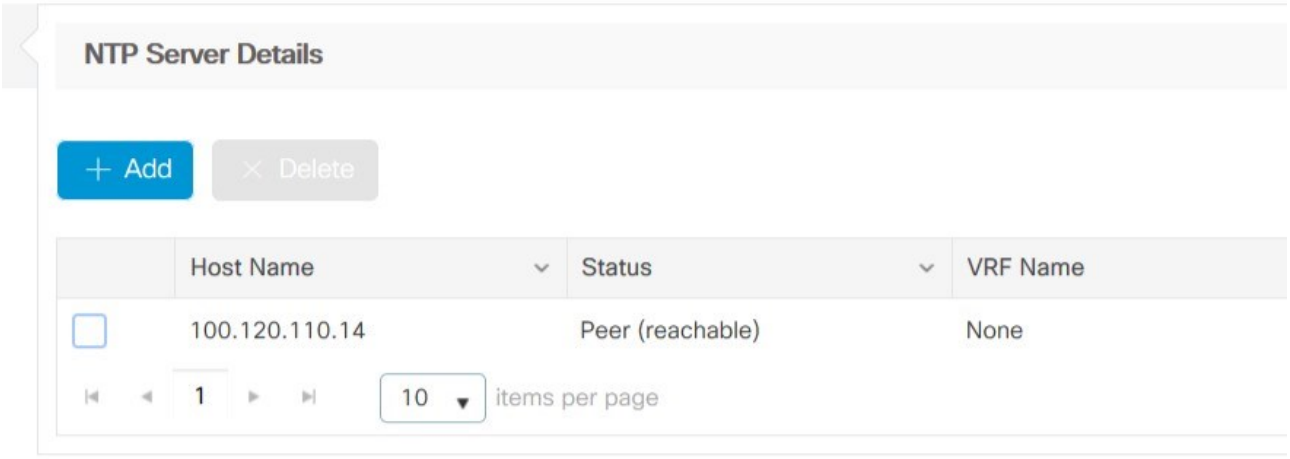
Langattomien verkkojen määritysten jälkeen WLAN-tukiasemat käynnistyivät uudelleen, ja niillä oli käytössä kaikki juuri määritetyt asetukset. Tarpeelliseksi katsottiin kuitenkin vielä määrittää tuki-

asemalle DNS-palvelimien IP-osoitteet, sekä NTP-palvelimen IP-osoite, sillä näitä ei pystynyt määrittelemään alkukonfiguraatiossa. DNS-palvelimet sai määritettyä hallintasivulta Administrationin alta löytyneestä DNS-sivusta, ja NTP löytyi myös Administrationin alta. Näihin asetettiin yrityksen sisäverkon DNS- ja NTP-palvelimien osoitteet, jonka jälkeen konfiguraatio tallennettiin kertaalleen hallintasivun yläkulmasta löytyneestä Save Configuration painikkeesta. Kuvioista 11 ja 12 näkyvät asetetut DNS- ja NTP-asetukset



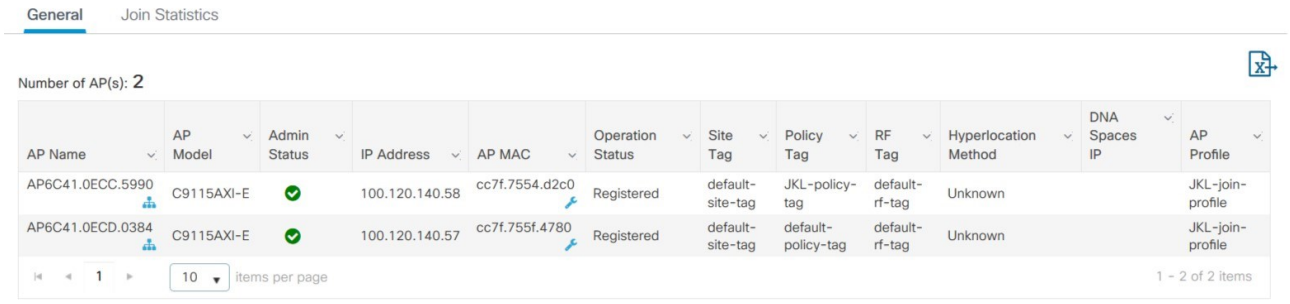
Kuvio 11 DNS-palvelinten määritys





Kuvio 12 NTP-palvelimen ja kellon määritys

Tässä vaiheessa yksittäisen WLAN-tukiaseman määritykset olivat valmiit. Koska verkkoon oli kuitenkin tulossa useampi tukiasema, haluttiin että loput tukiasemista osaisivat asentaa itsensä automaattisesti, käyttäen controllerin asetuksia. Automaattisen asennuksen määritys onnistui määrittelemällä hallintasivulta AP Profile. Tähän profiiliin sai määriteltyä suoraan, että millaisilla asetuksilla uusi WLAN-tukiasema asennetaan, kun se liitetään samaan verkkoon kuin missä controller sijaitsee. Hallintasivuilta luotiin JKL-join-profile, johon asetettiin täysin samat määritykset kuin alkuperäiseen controlleriin, lukuun ottamatta controllerin toimintoja. Muut WLAN-tukiasemat tulisivat olemaan verkossa vain yksinkertaisia, langatonta verkkoa jakavia laitteita ilman muuta toiminnallisuutta. Lisäksi profiiliin määritettiin, että WLAN-tukiasemat tarkistavat asiakaskoneilla olevat yhteydet aina 30 minuutin välein, ja asettavat yhteyden lepoon, jos ne eivät ole enää aktiivisia. AP Profilen asetusten määrittämisen jälkeen testattiin määritysten toimivuutta. Verkkoon liitettiin toinen WLAN-tukiasema, joka sai haettua JKL-join-profile:lla määritetyt asetukset controllerilta, ja asensi itsensä toimintaan niillä. Asia pystyttiin tarkistamaan vielä hallintasivun kautta, joka näkyy kuviossa 13. Kumpikin verkossa olevista WLAN-tukiasemista käyttää JKL-join-profilea, ja on täten toiminnassa halutuilla asetuksilla.

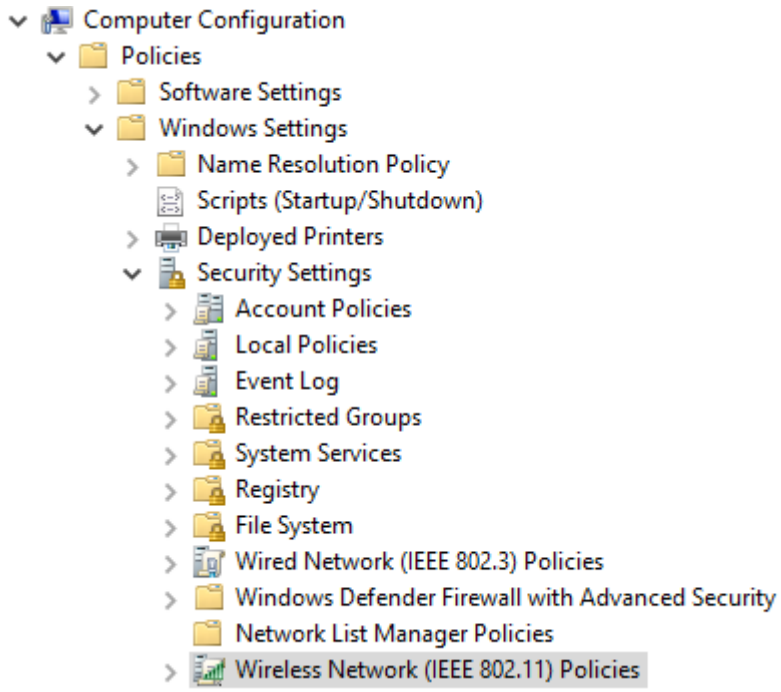


Kuvio 13 WLAN-tukiasemat liittyvät automaattisesti profiililla

4.2.3 Asiakaskoneiden konfigurointi

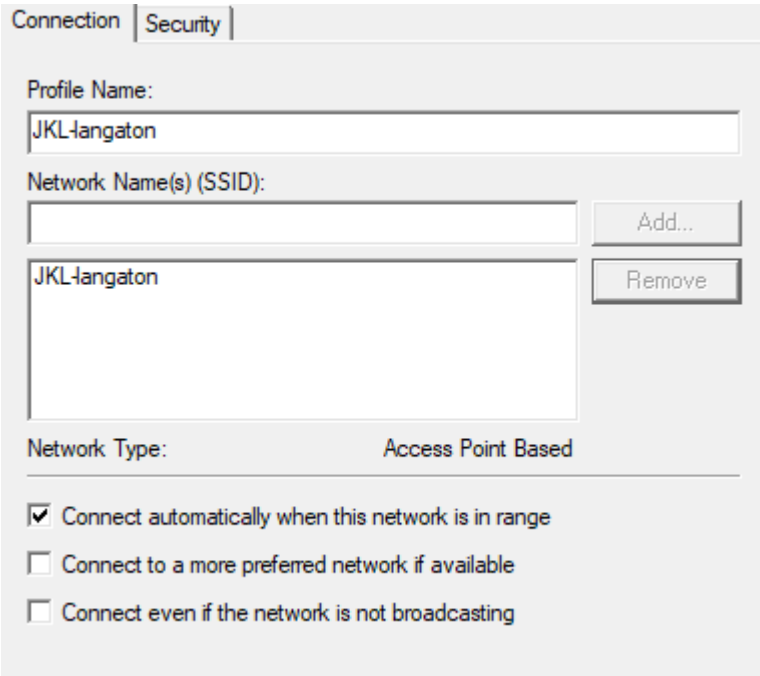
RADIUS-ympäristön tietoturvan varmistamiseksi domain controllerille päätettiin tehdä erillinen GPO-sääntö langatonta verkkoa varten. Tämä tehdään täysin tietoturvan varmistamiseksi, koska muuten yrityksen käyttäjien koneet saattaisivat luovuttaa dataa hyökkääjälle, joka esittää oikeaa langatonta tukiasemaa. Sen takia GPO-asetetaan tekemään erillisiä varmistuksia, jotta mahdollisessa edellä mainitussa hyökkäystilanteessa yrityksen käyttäjien koneet eivät luovuttaisi eteenpäin mitään arkaluontoisia tietoja hyökkääjälle.

GPO:n konfigurointi aloitettiin selvittämällä mistä sijainnista GPO:n rakenteesta voi määritellä asiakaskoneille ennalta langattoman verkon asetukset. Poluksi tälle asetukselle löytyi Computer Configuration, Policies, Windows Setting, Security Settings ja Wireless Network (IEEE 802.11) Policies. Tämä polku näkyy kuviossa 14.



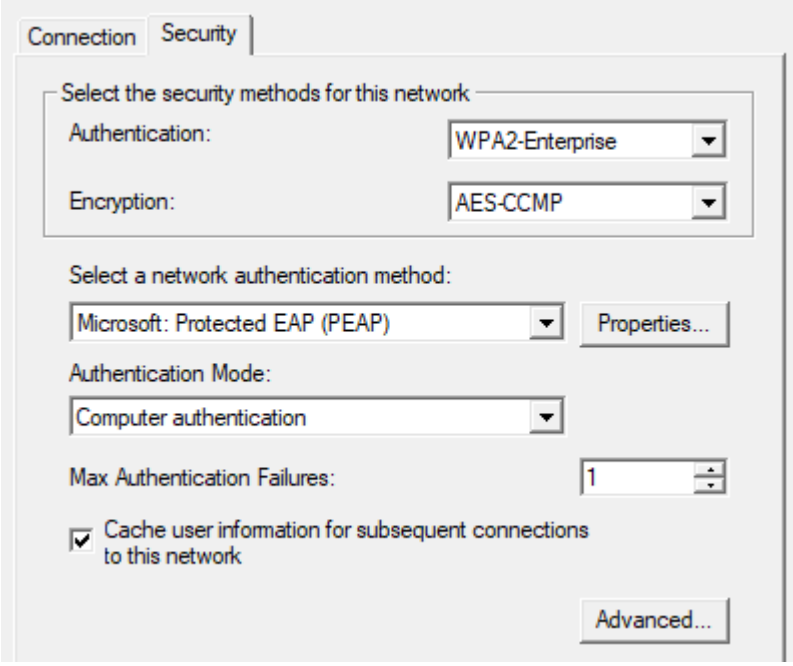
Kuvio 14 GPO:n polku

Sijaintiin määriteltiin uusi sääntö, joka asetettiin vaikuttamaan Windows Vistalle ja sitä uudemmille Windows-käyttöjärjestelmille. Sääntö halusi ensimmäisenä, että sille määriteltiin jokin nimi. Tämä nimi näkyisi vain GPO:ssa, joten sen ei vielä tarvinnut olla sellainen, josta yrityksen käyttäjät ymmärtävät mikä verkko on kyseessä. Nimen asettamisen jälkeen määriteltiin Langattoman verkon profiilin nimi, joka on huomattavasti tärkeämpi kuin aikaisempi säännön nimi. Profiilin nimi tulee näkymään kaikkien yrityksen tietokoneiden langattomien verkkojen listassa, joten sen pitää olla sellainen, että käyttäjät ymmärtävät liittyä siihen. Profiilin alle vasta asetettiin itse langattoman verkon tunnus, joka ei näy loppukäyttäjälle ollenkaan. Loppukäyttäjä näkee ainoastaan profiilin nimen. Kuviosta 15 näkyy, kuinka asetukset määritettiin.



Kuvio 15 Profiilin asetukset

Profiilin nimen ja langattoman verkon tunnuksen lisäämisen jälkeen määriteltiin tärkeimmät säännöt, langattoman verkon tietoturvasäännöt. Tietoturvasäännöistä tuli määrittää todentamisprotokollaksi WPA2-Enterprise ja salaukseksi AES-CCMP, koska nämä määriteltiin myös Ciscon langattomille lähettimille. Todentamisen tarkemmista asetuksista määritettiin, että käytetään Microsoft: Protected EAP sekä Computer authentictionia. Nämä asetukset näkyvät kuviossa 16.

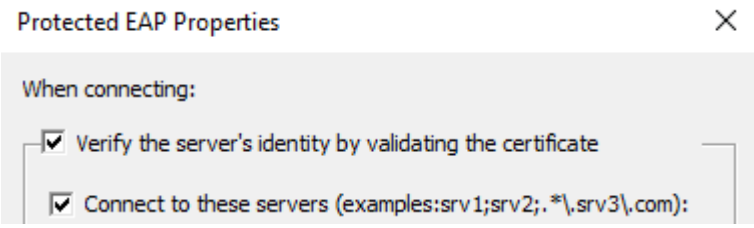


Kuvio 16 Langattoman profiilin tietoturva-asetukset

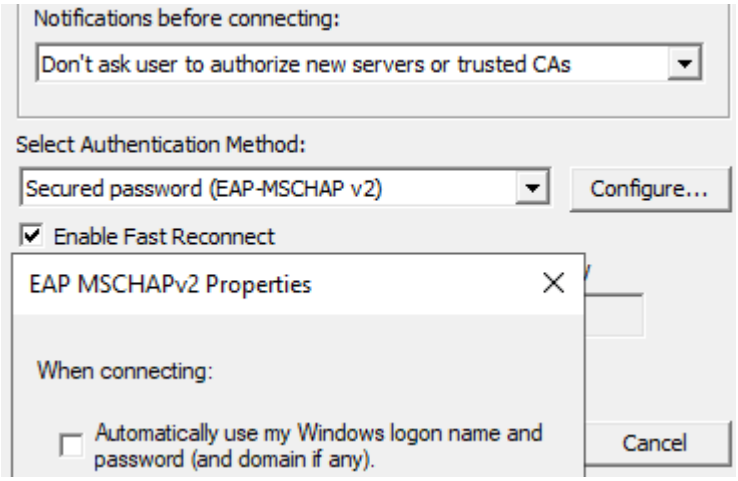
Tietoturvasäännöistä tuli vielä muokata PEAP-lisäasetuksia, jotta verkosta saataisiin varmasti mahdollisimman turvallinen. Lisäasetuksista asetettiin päälle asetus, joka pakottaa asiakaskoneet varmistamaan palvelimen identiteetin sen sertifikaatin perusteella. Jos tätä asetusta ei olisi päällä, asiakaskoneet voisivat yhdistää itsensä hyökkääjän esittämään langattomaan verkkoon. Tämän vuoksi asetus on pakollinen, ja sen alta löytyvästä listasta määritettiin vahvistettavaksi sertifikaatiksi verkkoympäristön juurisertifikaatti. Asetuksista myös asetettiin päälle asetus Connect to these server, jolla voidaan vielä paremmin koventaa ympäristön tietoturvaa. Tämä asetus pakottaa, että asiakaskoneet muodostavat vielä yhteyden tietyn nimiseen palvelimeen ennen käyttäjätietojen lähettämistä. Jos palvelimeen ei saada yhteyttä, langattomaan verkkoon yhdistäminen keskeytyy välittömästi.

Lisäasetuksista asetetiin päälle myös valinta, jolla asiakaskoneita ei pyydetä vahvistamaan uusia palvelimia tai sertifikaatteja. Tällä asetuksella varmistetaan, että tilannetta, jossa hyökkääjän verkko olisi määritetty pyytämään asiakaskoneita lisäämään hänen luomansa palvelimen tiedot, ei pysty muodostumaan. Asiakaskoneet suoraan hylkäisivät tällaisen pyynnön, eivätkä suostuisi yhdistämään hyökkääjän langattomaan verkkoon. Viimeisenä lisäasetuksista määritettiin EAP-MSCHAP v2 lisäasetuksista, että se ei käytä automaattisesti käyttäjien Windows-kirjautumistietoja.

Tällä varmistetaan vielä lisää, että asiakaskoneiden tiedot eivät pysty vuotamaan hyökkääjien verkkoon. Kuvioista 17 ja 18 näkyy lisäasetuksiin tehdyt määritykset.

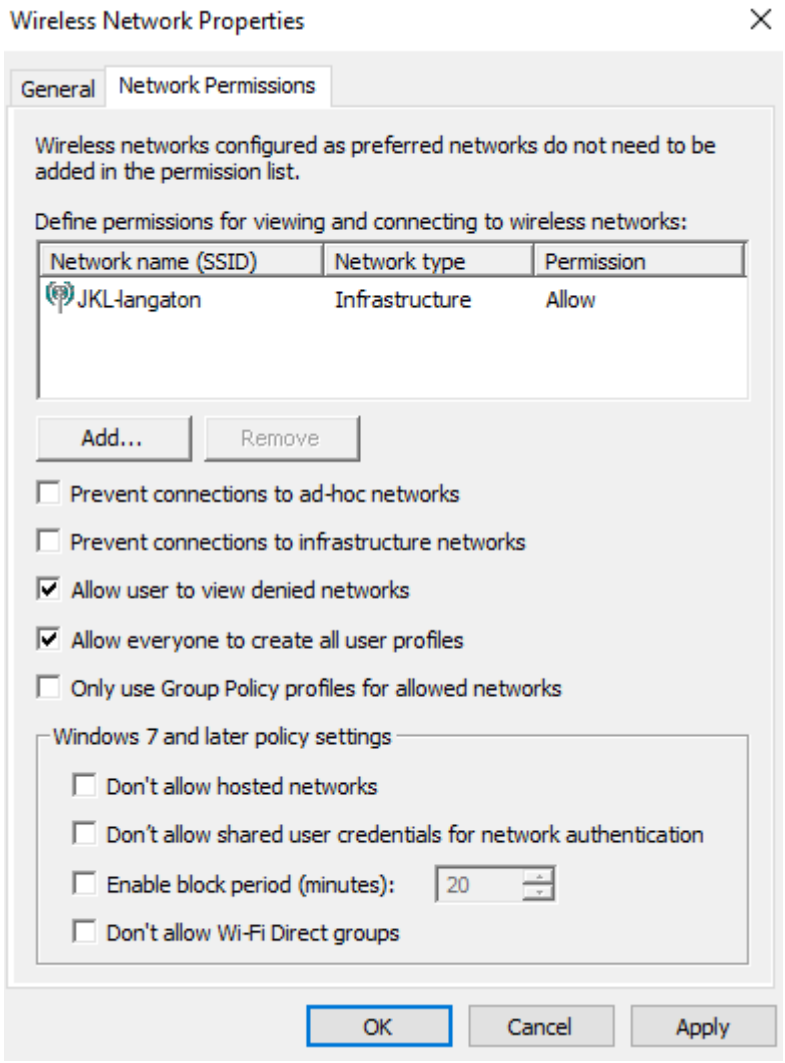


Kuvio 17 PEAP validointiasetukset



Kuvio 18 PEAP todentamisasetukset

Aikaisempien lisäasetuksien lisäksi määritettiin vielä Network Permissions välilehdeltä langattomalle verkolle asioita. Näistä olennaisimmat olivat ottaa säännöstä koneilta pois luvat yhdistää ad-hoc ja yritysverkkoihin. Näin asiakaskoneita ei pystyisi yhdistämään mihinkään muuhun WPA2-Enterprise määritettyyn langattomaan verkkoon, kuin mikä määriteltiin GPO:lle. Ad-hoc verkot on myös hyvä ottaa pois, koska ne eivät olleet yrityksen käytössä. Näin ylimääräisiä tietoturvariskejä saatiin karsittua pois. Tehdyt määritykset näkyvät kuviosta 19.



Kuvio 19 Profiilin network permissions

Langattoman verkon asetukset olivat tämän jälkeen valmiita, joten enää GPO tuli jakaa kaikille asiakaskoneille. Tämä onnistui parhaiten asettamalla GPO:n alle ryhmä, mihin kaikki asiakaskoneet kuuluivat. Sen jälkeen, kun asiakaskoneet käynnistettiin uudelleen, tai ne tarkastivat GPO-asetuksensa ja huomasivat niissä muutoksia, kaikille asiakaskoneille tuli näkyviin langattomiin verkkoihin GPO:ssa luodun profiilin nimi, kuten kuviossa 20 näkyy.

Kuvio 20 Profiili näkyy koneella

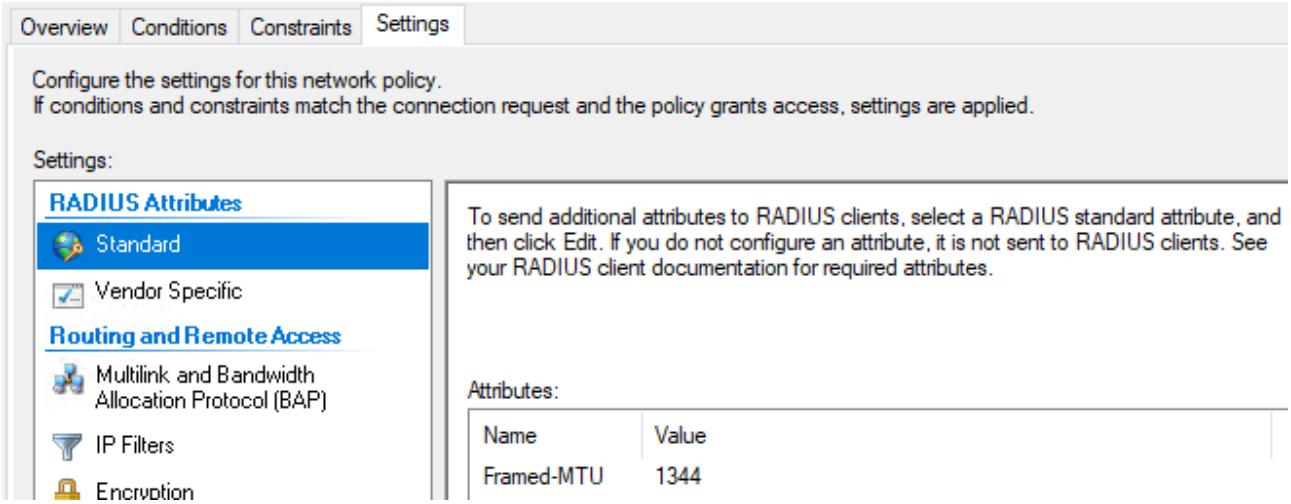
4.3 RADIUS-ympäristön testaus

4.3.1 Toiminta ja tietoturva

Ympäristön onnistuneen asentamisen jälkeen, sen testaus aloitettiin. Ensimmäiset testaukset aiheuttivat ihmetystä, koska testikäyttöön valmisteltu asiakaskone jäi jumiin langattomaan verkkoon yhdistäessä. Yhdistäminen verkkoon kesti hyvin pitkään ja lopulta epäonnistui. Syy tähän löytyi tarkastelemalla RADIUS-palvelimen lokitietoja. WLAN-tukiasemalta saapuvat, portteihin 1812 ja 1813 osoitetut paketit oli tiputettu, koska portteja ei ollut avattu palomuurista. Ongelma ratkesi, kun palvelimelle määriteltiin Windowsin omaan palomuuriin, että näihin portteihin sai vastaanottaa viestejä.

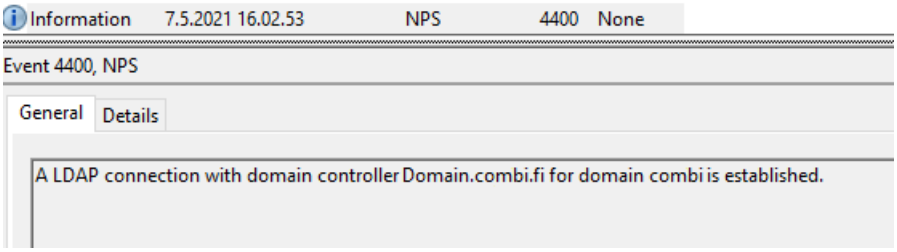
Palomuuriavauksen jälkeen ongelma ei kuitenkaan lopullisesti ratkennut. Vaikka Windowsin palomuuri ei enää estänyt paketteja pääsemästä palvelimelle, ei asiakaskone silti saanut pääsyä langattomaan verkkoon. Tilanne oli haastava, koska yhdistämisyrityksistä ei muodostunut mitään lokitietoja palvelimelle. Asiaa tutkimalla päädyttiin siihen, että UDP-paketit jossain vaiheessa vain tippuvat verkosta pois. Koska UDP-paketeissa ei ole varmistusta, piti asiaa tutkia kaappaamalla liikennettä. Palvelimelta kaapattiin liikennettä, josta huomattiin, että RADIUS-pyyntö saapuu palvelimelle, ja palvelin lähettää sen takaisin RADIUS-asiakkaalle. Tämän jälkeen kuitenkin paketti katoaa verkosta, eikä saavu asiakaskoneelle asti takaisin.

Ongelmaan löytyi ratkaisu RADIUS-paketin koosta. RADIUS-paketti minkä palvelin lähetti vastauksena WLAN-tukiasemalle, oli yli 1500 bitin kokoinen. Tukiasema ei kuitenkaan pystynyt käsittämään paketteja, joiden koko ylitti 1433 bittiä. Tämän vuoksi palvelimelle tuli asettaa asetus Framed-MTU 1433, joka rajoitti paketit 1433 bittiin. Kun asetus oli laitettu ja NPS-palvelu käynnistettiin uudelleen, asiakaskone pystyi saamaan yhteyden langattomaan verkkoon. Kuviosta 21 näkyy paikka, johon Framed-MTU komento tuli asettaa, jotta paketit eivät pudonneet verkossa.

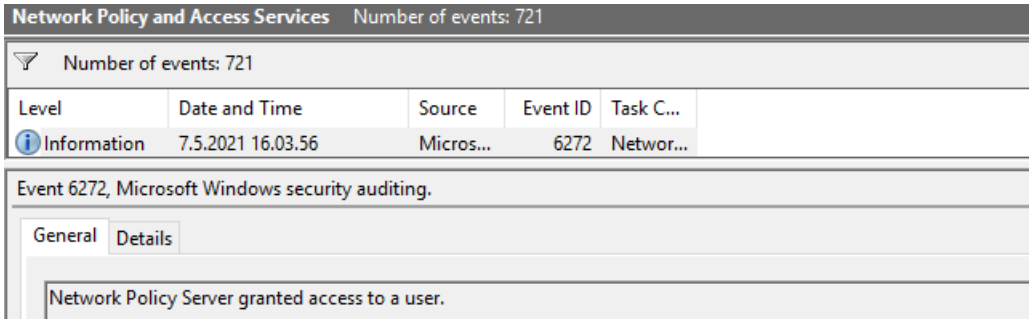


Kuvio 21 Framed-MTU -komento

Nyt asiakaskoneet viimeinkin pystyivät ottamaan yhteyden onnistuneesti langattomaan verkkoon. RADIUS-palvelimen lokitiedoista pystyi näkemään, kuinka RADIUS hyväksyi käyttäjien liittymis-pyynnöt. Ennen liittymispyynnön hyväksyntää, RADIUS-palvelin muodosti vielä erikseen yhteyden domainin LDAP-palvelimeen, ja teki siitä lokeihin tapahtuman. Liittymisen lokeista pystyi näkemään, että mikä käyttäjäkone oli kyseessä, ja millä ehdoilla se oli liittynyt verkkoon. Kuvioista 22 ja 23 näkyvät hyväksytty liittyminen langattomaan verkkoon, sekä LDAP-yhteyden muodostumisesta tullut ilmoitus.

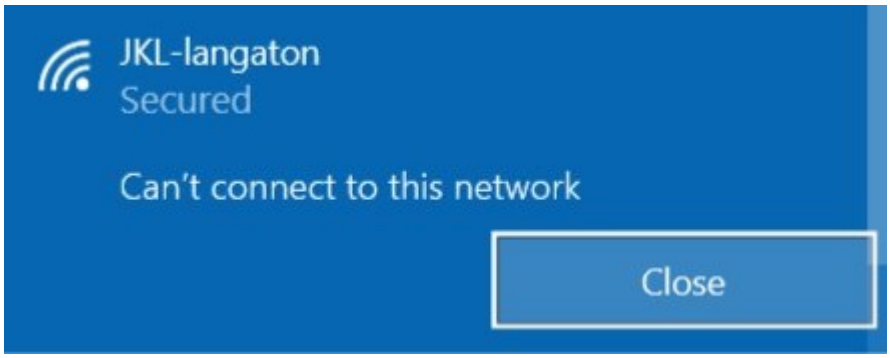


Kuvio 22 LDAP-yhteys valmisteltu

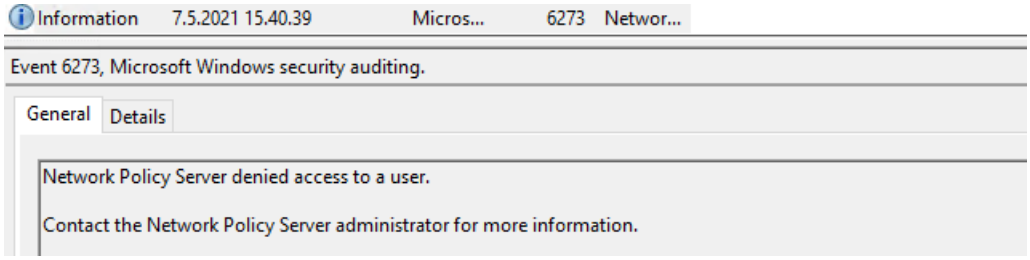


Kuvio 23 Hyväskytty liittyminen langattomaan verkkoon

Koska RADIUS-palvelimelle oli määritelty, että ainoastaan domainiin kuuluvat koneet pystyisivät liittymään langattomaan verkkoon, testattiin miten palvelin reagoisi sellaiseen koneeseen, joka ei ollut domainissa. Tätä varten asennettiin uusi kone, jota ei liitetty yrityksen domainiin. Kun tällä koneella testattiin liittyä langattomaan verkkoon, verkko pyysi käyttäjätunnusta ja salasanaa. Tässä kohdassa ei ollut mitään merkitystä mitä asiakaskoneella kenttiin kirjoitettiin, koska kone ei ollut domainissa, eikä siten pääse verkkoon. Käyttäjätunnuksen ja salasanan syöttämisen jälkeen kone ilmaisi, että ei pystynyt muodostamaan yhteyttä verkkoon. Tästä epäonnistuneesta yrityksestä muodostui RADIUS-palvelimelle lokeihin tieto, jossa näkyi mitä käyttäjätunnusta asiakaskone oli yrittänyt. Kuvioissa 24 ja 25 näkyvät asiakaskoneella tulleet ilmoitukset epäonnistuneista liittymisistä langattomaan verkkoon sekä RADIUS-palvelimelle muodostunut lokitieto.



Kuvio 24 Epäonnistunut kirjautuminen asiakaskoneelta



Kuvio 25 Epäonnistuneen kirjautumisen lokitiedot

Matkapuhelimet reagoivat hieman eri tavalla langattomaan verkkoon, kun niitä testattiin. Puhelimet ilmoittivat yhdistettäessä, että niille tulee määrittää ensiksi sertifikaatti mitä verkko käyttää. Koska puhelimilla ei luonnollisesti ollut mitään sertifikaattia mitä verkko olisi hyväksynyt, ei yhdistäminen ollut mahdollista. Yhdistämistä testattiin useammalla mallilla, joissa sertifikaattipyyntö ilmaistiin hieman eri tavalla. Kaikki mallit kuitenkin tarvitsivat sertifikaatin yhdistämistä varten, jota millään puhelimella ei ollut.

Langattoman verkkoon liittymisen GPO:n asetuksia haluttiin myös testata, jotta voitiin varmistua kovennuksien toiminnasta. Tätä varten tehtiin testikone, joka liitettiin yrityksen domainiin. Tälle koneelle määritettiin erilainen GPO, jossa langattomalle verkolle määritetyt asetukset poikkesivat hieman muilla koneilla olevista. Ensimmäinen testaus oli määrittää asetuksiin väärä palvelin, jolla asiakaskone kävisi vahvistamassa sertifikaatin. Palvelimeksi asetettiin toinen yrityksen verkosta löytyvä olemassa oleva palvelin, kuin RADIUS-palvelin. Tämä määritys esti asiakaskoneen pääsemisen langattomaan verkkoon, ja RADIUS-palvelimelle muodostui lokitietoihin ilmoitus yrityksestä, jota ei pystytty vahvistamaan. Kyseinen kovennus voitiin siis todeta toimivaksi.

GPO:n asetuksiin testattiin muitakin hyvin pieniä muutoksia, kuten vaihtaa sertifikaatti mikä vahvistettaisiin ja laittaa todentamisprotokollaksi jokin väärä protokolla mitä RADIUS-palvelimelle ei ollut konfiguroitu. Nämä kaikki asetukset saivat aikaan epäonnistumisia kirjautumisia langattomaan verkkoon, ja kaikista näistä muodostui RADIUS-palvelimelle merkintä. Kovennukset olivat siis hyvin toimivia, eikä asiakaskoneet pystyneet yhdistämään verkkoon kuin juuri oikein määritetyillä GPO-asetuksilla.

Asiakaskoneella myös testattiin, kuinka se reagoisi samannimiseen langattomaan verkkoon, joka ei kuitenkaan ollut oikea verkko. Testausta ei pystytty suorittamaan täysin samoilla määrityksillä kuin

mitä langattomilla lähettimillä oli, koska paikalta ei löytynyt laitteita, joilla olisi voinut jakaa WPA2-Enterprise määritettyä langatonta verkkoa. Testiä varten luotiin siis langaton verkko samalla nimillä, mutta toisella tunnistamistavalla. Asiakaskone ei pystynyt muodostamaan yhteyttä tähän verkkoon, vaan ilmoitti heti, että siihen ei voida yhdistää.

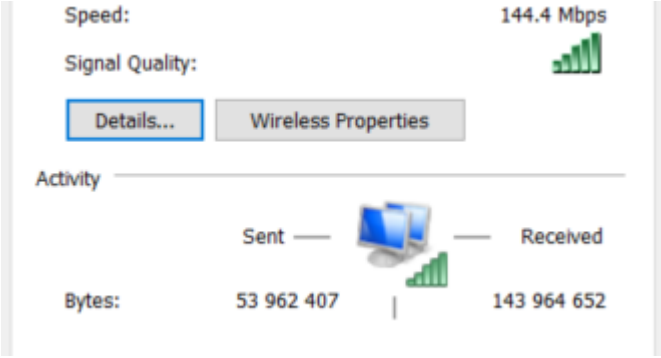
4.3.2 langattoman signaalin testaus

RADIUS-palvelimen onnistuneen toiminnan toteamisen jälkeen lähdettiin testaamaan Cisco 9115AXI -langattomien tukiasemien toiminnallisuutta. Langattomien tukiasemien toiminnassa oltiin kiinnostuneimpia niiden siirtonopeudesta, kantamasta ja asiakaskoneiden kyvystä liikkua tukiasemien välillä. Ensimmäisenä lähdettiin testaamaan asiakaskoneiden kykyä liikkua tukiasemien välillä, koska ominaisuus on yksi tärkeimmistä.

Tämän testaaminen oli helppoa, sillä testausta varten ei tarvinnut, kun asettaa kaksi langatonta tukiasemaa hieman kauemmaksi toisistaan. Asiakaskone laitettiin yhdistämään langattomaan verkkoon, jonka jälkeen varmistettiin lähettimien hallintasivulta, että asiakaskone oli ottanut varmasti yhteyttä haluttuun tukiasemaan. Kun tämä oli varmistettu, liikutettiin asiakaskonetta ensimmäisestä tukiasemasta kauemmaksi toista tukiasemaa kohti. Asiakaskonetta liikutettiin noin kaksikymmentä metriä, jonka jälkeen WLAN-tukiasemien hallintasivulta tarkastettiin mihin tukiasemaan asiakaskone oli yhteydessä. Hallintasivulta voitiin todeta, että asiakaskone oli onnistuneesti siirtynyt aiemman tukiaseman alaisuudesta toiselle.

Yksittäisten WLAN-tukiasemien kantama yllätti huomattavasti. Yksi tukiasema pystyi lähettämään langatonta verkkoaan jopa kolmenkymmenen metrin päähän 5GHz taajuudella, joka oli todella hyvä tulos laitteen käyttöympäristössä. Tätä vahvisti myös vielä se, että WLAN-tukiaseman ja asiakaskoneen välillä oli useampia seiniä, jotka heikentivät signaalia ennestään. Silti asiakaskone pysyi kiinni langattomassa verkossa, ja asiakaskoneella pystytiin pitämään onnistuneesti tunnin pituinen videopuhelu. Testin perusteella todettiin, että viisi WLAN-tukiasemaa olisi mahdollisesti liiankin suuri määrä tukiasemia Jyväskylän toimistolle. Tämä kuitenkin vaati pidempää testausta, jonka vuoksi tukiasemia ei lähdetty vielä ottamaan pois ympäristöstä.

Ciscon WLAN-tukiasemissa on tuki usealle eri langattomalle standardille sekä 2.4GHz että 5GHz taajuudelta. Tämän vuoksi haluttiin testata, kuinka suuria eroja langattomien standardien siirtonopeuksissa on. Ensimmäisenä lähdettiin testaamaan 2.4GHz taajuudella toimivaa 802.11n standardia. Asiakaskone yhdistettiin WLAN-verkkoon, johon oli määritetty, että verkko toimii vain 2.4Ghz taajuudella. Näin ollen paras standardi mitä verkko pystyisi käyttämään on 802.11n. Asiakaskoneen yhdistämisen jälkeen tarkastettiin vielä WLAN-tukiasemien hallintasivuilta, että asiakaskone oli varmasti ottanut yhteyden 802.11n verkkoon. Asiakaskoneen WLAN-asetuksia tutkimalla pystyttiin näkemään, että siirtonopeudeksi asiakaskoneen ja langattoman verkon välille saatiin 144Mbps 802.11n standardilla. Testiympäristössä asiakaskone sijaitsi noin kolmen metrin päässä WLAN-tukiasemasta, ilman että välissä oli mitään häiriötekijöitä. Kuviossa 26 näkyy langattoman verkon testin siirtonopeus.

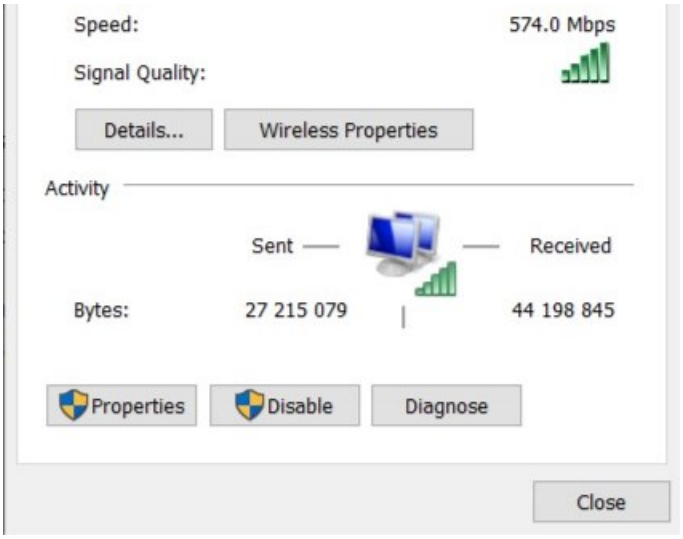


Kuvio 26 802.11n nopeus

5Ghz taajuutta aloitettiin testaamaan 802.11ac standardista. Tämä standardi valittiin testattavaksi, koska se on nopein yleisesti käytössä olevista 5Ghz taajuuden standardeista, sekä kaikki asiakaslaitteet näyttivät pyrkivän ottamaan eniten yhteyttä tällä standardilla. Testaus suoritettiin vastaavassa testiympäristössä kuin 802.11n standardin testaus. Testausta varten valittiin asiakaskone, jossa ei ollut WI-FI 6 tukea. Tämä kone yhdistettiin langattomaan verkkoon, joka oli määritetty WLAN-tukiasemassa toimimaan vain 5Ghz taajuudella. WLAN-tukiasemien hallintasivuilta tarkastettiin jälleen, että asiakaskone oli ottanut yhteyden varmasti halutulla standardilla. Kun nämä oli tehty, tarkistettiin siirtonopeus asiakaskoneelta samasta sijainnista mistä 802.11n nopeus tarkastettiin. Siirtonopeudeksi asiakaskoneen ja langattoman verkon välille muodostui 400Mbps, joka oli todella hyvä. Kuviosta 27 näkyy 802.11ac siirtonopeuden testitulos.

Kuvio 27 802.11ac nopeus

Viimeisenä standardeista testattavaksi otettiin uusi WI-FI 6 standardi, 802.11ax. Kuten teoriaosuudessa tutkittiin, 802.11ax -standardin ei pitäisi tuoda huomattavaa parannusta siirtonopeuteen 802.11ac -standardiin verrattuna. Testiä lähdettiin toteuttamaan jälleen samassa testiympäristössä, kuin aikaisemmat testit suoritettiin. Asiakaskoneeksi valittiin tietokone, josta löytyi WI-FI 6 tuki. Asiakaskone yhdistettiin WLAN-tukiasemien langattomaan verkkoon, jossa oli käytössä kaikki saatavilla olevat langattomat standardit. WLAN-tukiasemien hallintasivulta todettiin, että asiakaskone otti suoraan yhteyden 802.11ax standardilla. Kun langattoman verkon tietoja lähdettiin tutkimaan, huomattiin että siirtonopeus oli 574Mbps. Siirtonopeuden kasvu 802.11ac -standardiin verrattuna oli huomattava, mutta ei silti niin suuri kuin 802.11n -standardista 802.11ac -standardiin. Kuviossa 28 on näkyvillä 802.11ax testin tulokset.



Kuvio 28 802.11ax nopeus

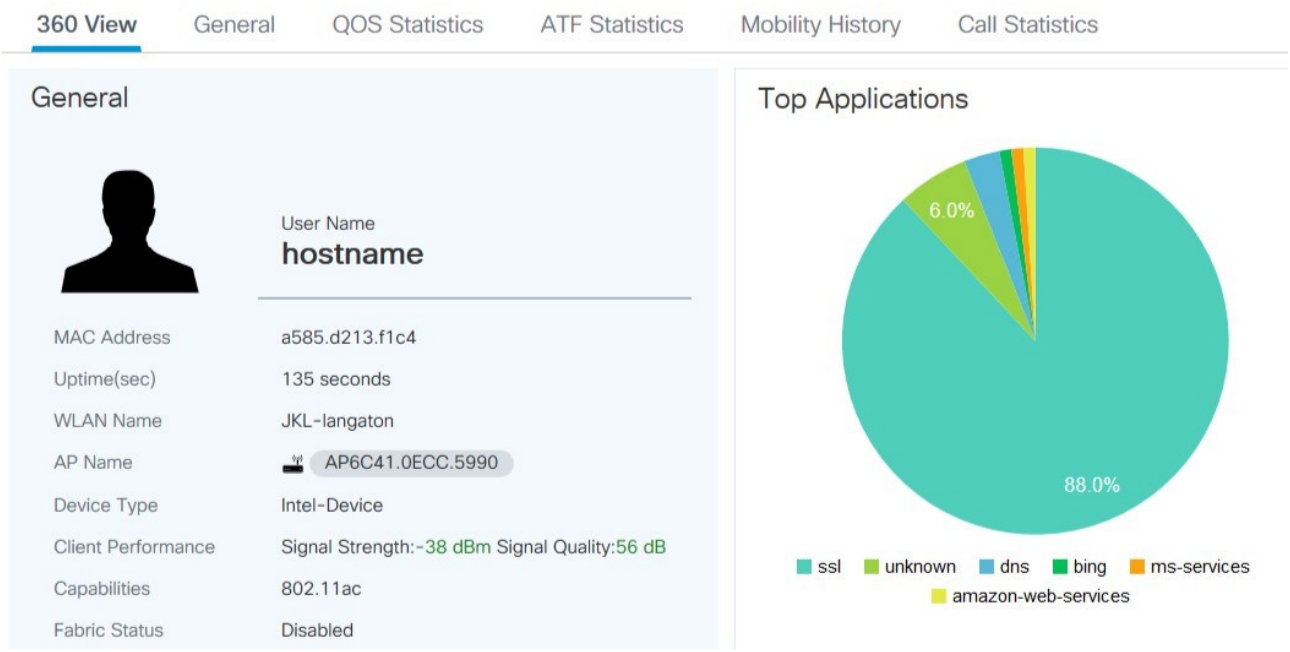
Siirtonopeuksien testauksiin oltiin tyytyväisiä, koska testaukset antoivat odotettuja parempia tuloksia. Jopa 2.4Ghz taajuus antoi sen verran hyviä nopeuksia, että asiakaskoneilla saavutettiin tarpeellinen nopeus sulavan toiminnan ylläpitämiseksi. Yleisesti asiakaskoneet käyttivät 802.11ac taajuutta toimintaansa, jolla langattomat yhteydet toimivat erinomaisesti. Siirtonopeudet olivat siis langattomassa verkossa todella hyvät.

4.3.3 Käyttäjienhallinta

Ciscon WLAN-tukiasemien hallintasivulta haluttiin selvittää, millaista dataa asiakaskoneista pystytään näkemään. Hallintasivuilta löytyi erillinen osio, Monitoring, jossa oli paljon tietoa saatavilla langattomasta verkosta ja sen laitteista. Monitoring -valikon alta löytyi valinta, jolla saatiin esille tietoa langattomissa verkoissa olevista asiakkaista. Valikosta huomattiin, että langattoman verkon asiakkaista nähtiin huomattava määrä dataa, kuten niiden MAC-osoite, IP-osoitteet, Langaton verkko ja -tukiasema jossa asiakkaat ovat yhteydessä ja protokolla millä yhteys verkkoon on muodostettu. Kuviossa 29 on näkyvillä, millaisia tietoja asiakaskoneista pystyi näkemään.

Kuvio 29 Asiakastietokoneiden tiedot WLAN-hallintasivulla

Langattoman verkon asiakkaista pystyttiin näkemään vielä tarkempaakin tietoa. Tämä onnistui valitsemalla Monitoring valikosta yksittäinen asiakas. Asiakkaista pystyttiin näkemään esimerkiksi tarkka aika, minkä kone oli ollut yhteydessä langattomaan verkkoon. Myös tarkat signaalitiedot langattoman yhteyden vahvuudesta oli nähtävissä, sekä hallintasivuilta näkyivät jopa sivustot, joilla asiakas oli käynyt. Sivustoista ei kuitenkaan näkyneet mitkään sivut, joihin oli käytetty ssl-protokollaa, koska yhteys näissä on salattua. Kuviossa 30 on nähtävissä miltä asiakkaiden tarkempi valvonta hallintasivulta näytti.



Kuvio 30 yksittäisen asiakkaan tietoja

5 Johtopäätökset ja jatkosuunnitelmat

Langattoman RADIUS-ympäristön asennus oli periaatteessa yksinkertainen työ, mutta siinä oli useita vaiheita, joissa oli pieniä määrityksiä, jotka estivät sitä toimimasta oikein. Näistä merkittävimpiä olivat RADIUS-serverin lähettämien pakettien koon rajoittaminen, sekä langattoman verkon kovennuksien määrittäminen. Näitä vaiheita lukuun ottamatta työ onnistui ilman ongelmia, ja haluttuun lopputulokseen päädyttiin suhteellisen nopeasti.

Langattoman verkon toimivuus ylitti ennalta asetetut arviot täysin, sillä siirtonopeudet asiakaskoneilla olivat erinomaiset. Asiakaskoneilla verkon käyttämisessä ei esiintynyt mitään eroa langalliseen verkkoon verrattuna. Langattoman verkon kuuluvuus oli myös huomattavasti odotettua suurempi, jonka vuoksi mahdollisesti Jyväskylään lähetetyistä tukiasemista yhtä kappaletta voi hyödyntää toisella toimipisteellä. Näin Combitech Oy pystyy säästämään langattoman verkon käyttöönoton kuluissa.

Koventamisen asetukset toimivat myös hyvin. Näiden testaaminen ja asettaminen olivat hyvin olennaiset, jotta yrityksen tietoturva ei joudu riskiin. Koventamisien testaamiseksi käytettiinkin

runsaasti aikaa, ja ympäristössä kokeiltiin useita erilaisia asetuksia, jotta parhaiten toimivat asetukset saatiin määriteltyä asiakaskoneille, WLAN-tukiasemille ja palvelimille.

Tulevaisuuden kannalta parannuksia, mitä RADIUS-ympäristöön voitaisiin tehdä, ovat toinen EWC ja toinen RADIUS-palvelin. Ympäristössä on käytössä viisi WLAN-tukiasemaa, joista yksi toimii EWC-controllerina. Jos näistä neljästä, yksinkertaisena toimivasta CAPWAP WLAN-tukiasemasta määritettäisiin ainakin yksi lisää EWC-controlleriksi, voitaisiin parantaa langattoman verkon viansietokykyä. Tällöin langattomassa verkossa ei tulisi ongelmia, vaikka controller menisi vikatilaan, koska sillä olisi varalla toinen controller, joka siirtyisi ongelmatilanteen alkaessa aktiiviseksi.

Toinen RADIUS-palvelin olisi myös ympäristöön hyvä samasta syystä, kuin toinen EWC-controller. Tällä hetkellä ympäristö on huomattavasti vähemmän vikasietoinen, koska RADIUS-todentaminen tapahtuu vain yhdellä palvelimella. RADIUS-tukee itsessään useampaa palvelinta, jotka pystytään asettamaan Windows Serverin Network Policy Servicessä omaksi RADIUS-ryhmäksi. RADIUS-ryhmä toimii automaattisesti jakaen pyynnöt kahdelle palvelimelle, vähentäen yhdelle palvelimelle muodostuvaa ruuhkaa. Nämä kaksi asiaa ovat sellaiset, joita ympäristö vielä kaipaisi paremman vikasietoisuuden vuoksi.

Haluttu lopputulos toteutuneesta RADIUS-ympäristöstä ja sen käyttöönotosta oli onnistunut, ja se todettiin hyväksi. Tehty ympäristö tullaan ottamaan Combitech Oy:llä suoraan tuotantokäyttöön muissakin toimipisteistä, joten luodun RADIUS-ympäristön arvo on yritykselle merkittävä. Kun ympäristöt saadaan asennettua muihinkin toimipisteisiin, tulee kaikkien Combitech Oy:n työntekijöiden arki helpottumaan langattoman verkon myötä. Sen jälkeen työntekijöiden verkon käyttäminen ei ole enää rajoitettu yhteen pisteeseen kerrallaan, vaan toimipisteiden tilat muuttuvat vapaammaksi. Tämä mahdollistaa sen, että yrityksessä pystytään olemaan entistä kilpailukykyisempiä ja tehokkaampia.

Lähteet

Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE Gibraltar 16.10.x. 2019. Viitattu 24.4.2021. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec-usr-aaa-xe-16-10-book/sec-cfg-authorizatn.html

Bangeman, E. 2007. New attack cracks WEP in record time. Viitattu 11.5.2021. https://arstechnica.com/gadgets/2007/04/new-attack-cracks-wep-in-record-time/

Bayern, M. 2018. New method makes cracking WPA/WPA2 Wi-Fi network passwords easier and faster. Viitattu 11.5.2021. https://www.techrepublic.com/article/new-method-makes-cracking-wpawpa2-wi-fi-network-passwords-easier-and-faster/

Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet. 2021. Viitattu 20.4.2021. https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html

Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) White Paper. 2020. Viitattu 15.5.2021. https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/white-paper-c11-743398.html

Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE Gibraltar 16.12.x. 2021. Viitattu 21.4.2021. https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/config-guide/ewc_cg_16_12/conversion_and_migration.html

de Laat, C., G, Gross., L, Gommans., J, Vollbrecht. & D, Spence. 2000. Generic AAA Architecture. Request for Comments: 2903. Network Working Group. Viitattu 22.4.2021. https://tools.ietf.org/html/rfc2903

Gigabit Ethernet, & 1000BASE-T. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/gigabit-ethernet-1ge-1000-base-t.php

Hardesty, G. 2019. WiFi Network Standards Compared: 802.11ac, 802.11n, 802.11g, 802.11b and 802.11a. Viitattu 9.5.2021. https://www.data-alliance.net/blog/wifi-network-standards-80211ac-compared-to-80211n-80211g-80211a-and-80211b/

IEEE 802.11a. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11a.php

IEEE 802.11ac Gigabit Wi-Fi. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php

IEEE 802.11ax Wi-Fi 6. N.d. Viitattu 10.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ax.php

IEEE 802.11b. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11b.php

IEEE 802.11g Wi-Fi. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11g.php

IEEE 802.11n WLAN Standard. N.d. Viitattu 9.5.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11n.php

Jongerius, J. 2021. Wi-Fi 4/5/6/6E (802.11 n/ac/ax). Viitattu 9.5.2021. https://www.duckware.com/tech/wifi-in-the-us.html

Kardashevsky, C. 2021. How to Configure RADIUS Server on Windows Server 2016?. Viitattu 23.4.2021. https://theitbros.com/radius-server-configuration-on-windows/

Liang, H., Chen, Lu. & Xu, S. 2020. Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS. Viitattu 24.4.2021. https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificate-requirements-eap-tls-peap

Metzler, S. n.d. Digital Certificates vs Password Authentication. Viitattu 24.4.2021. https://www.securew2.com/blog/digital-certificates-vs-password-authentication

Mutai, J. 2019. How to Install Windows Server 2019 Step by Step. Viitattu 21.4.2021. https://computingforgeeks.com/install-windows-server-2019/

Newton, M. 2017. Network Access Server. Viitattu 24.4.2021. https://wiki.freeradius.org/glossary/NAS

Phillips, G. 2021. The Most Common Wi-Fi Standards and Types, Explained. Viitattu 9.5.2021. https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

Raphaely, E. N.d. A Complete Guide To Wireless (Wi-Fi) Security Viitattu 11.5.2021. https://www.securew2.com/blog/complete-guide-wi-fi-security

Rigney, C. 2000. RADIUS Accounting. Request for Comments: 2866. Network Working Group. Viitattu 24.4.2021. https://tools.ietf.org/html/rfc2866

Rigney, C., Willens, S., Rubens, A. & Simpson, W. 2000. Remote Authentication Dial In User Service (Radius). Request for Comments: 2865. Network Working Group. Viitattu 24.4.2021. https://tools.ietf.org/html/rfc2865

Riihikallio, P. 2017. Joo, 802.11 mutta mikä kirjain? (a,b,g,n,ac). Viitattu 13.5.2021. https://metis.fi/fi/2017/01/standardit/

Romano, P. 2014. Wifi Standards 802.11a/b/g/n vs. 802.11ac: Which is Best? Viitattu 9.5.2021. https://www.semiconductorstore.com/blog/2014/WiFi-standards-802-11a-b-g-n-vs-802-11ac-Which-is-Best/806/

Santuka, V., Banga, P. & Caroll, B. 2011. AAA Identity Management Security. Cisco Press 2011.

Shaw, K. 2020. 802.11x: Wi-Fi standards and speeds explained. Viitattu 9.5.2021. https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html

Securing the Corporate Network. 2001. Cisco Press. Viitattu 24.4.2021. https://www.ciscopress.com/articles/article.asp?p=24605&seqNum=6

Simplifying WPA2-Enterprise and 802.1x. N.d. Viitattu 11.5.2021. https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified#p4

TACACS+ Advantages. 2011. Viitattu 13.5.2021. https://www.tacacs.net/docs/TACACS_Advantages.pdf

TACACS+ and RADIUS Comparison. 2008. Viitattu 13.5.2021. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

What is 802.11ax (Wi-Fi 6)?. N.d. Viitattu 10.5.2021. https://www.extremenetworks.com/wifi6/what-is-80211ax/

Woland, A. 2014. RADIUS versus TACACS+. Viitattu 13.5.2021. https://www.networkworld.com/article/2838882/radius-versus-tacacs.html