LAPIN AMK
Lapland University of Applied Sciences

VIERASVERKKO

Vuori Tuomo

Opinnäytetyö

Tieto- ja viestintätekniikan koulutus
Insinööri (AMK)

2022

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikan koulutus
Insinööri (AMK)

Tekijä	Tuomo Vuori	Vuosi	2022
Ohjaaja	Kenneth Karlsson		
Toimeksiantaja	Lapin AMK		
Työn nimi	Vierasverkko		
Sivumäärä	34		

Opinnäytetyön tavoitteena oli tuottaa lisätietoa ja valmiita toteutusvaihtoehtoja erilaisten vierasverkkojen toteutuksen pohjaksi. Työssä keskitytään ratkaisuihin, jotka parhaiten soveltuvat vierasverkoissa käytettäviksi.

Alustuksena aiheelle esitellään langattomien verkkojen tekniikkaa ja 802.11-standardeja. Lisäksi esitellään työhön oleellisesti liittyvät verkkotekniikat ja verkkopalvelut, kuten OSI-malli, RADIUS ja 802.1x.

Testiympäristöstä esitellään ympäristön laitteistokokoonpano yleisellä tasolla sekä laitteiston ominaisuudet. Käydään läpi testiympäristön konfiguraation sisältöä, kuten langattomat verkot, VLAN:ien ominaisuudet, erotuksen toteutusratkaisut ja käyttäjätunnukset.

Toteutusvaihtoehtojen osuudessa käydään läpi neljä erilaista toteutusvaihtoehtoa. Toteutusvaihtoehdoista esitellään käyttäjän verkkoon liittymisprosessi sekä ominaisuuksien pohjalta kunkin vaihtoehdon vahvuudet ja heikkoudet käyttäjän ja ylläpidon näkökulmasta. Lisäksi käydään läpi käyttötilanteet, joihin kukin vaihtoehto parhaiten soveltuu. Lopuksi vertaillaan tiivistetysti eri toteutusvaihtoehtoja.

Opinnäytetyön toteutus ei ollut liian haastava. Aihe oli mielenkiintoinen, mutta laaja. Työ eteni aikataulussa, eikä vastaan tullut suuria ongelmia. Tuloksena saatiin tavoitteen mukaisesti lisätietoa ja vaihtoehtoja toteutuksen suunnittelun tueksi. Johtopäätöksenä voidaan todeta, että suunnittelua ohjaavat tietoturvallisuus ja verkonhallinta.

Avainsanat IEEE 802.1X -standardi, RADIUS, todentaminen, WLAN

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Degree Programme in Information
and Communication Technology
Bachelor of Engineering

Author	Tuomo Vuori	Year	2022
Supervisor	Kenneth Karlsson		
Commissioned by	Lapland UAS		
Subject of thesis	Guest network		
Number of pages	34		

The aim of this thesis was to produce additional information and ready-made options for the implementation of different kinds of guest networks. The thesis focuses on the solutions that are best suited for use in guest networks.

As an introduction to the topic, wireless networking technologies and 802.11 standards were presented. In addition, network technologies and network services relevant to the work, such as the OSI model, RADIUS, and 802.1x, were introduced. The test environment section included a general overview of the hardware configuration of the environment, as well as hardware features. The configuration of the test environment was discussed, including wireless networks, VLANs, isolation implementations, and user credentials. The implementation options section introduced four different implementation options. The implementation options presented the process of connecting a user to the network and based on the features, strengths, and weaknesses of each option from a user and maintenance perspective. The use cases, for which each option is best suited, were also discussed. Finally, a summary comparison of the different implementation options was presented.

The implementation of the thesis was not too challenging. The topic was interesting but broad. The work progressed on time and no major problems were encountered. As a result, additional information, and options to support the implementation planning were obtained in line with the objective. In conclusion, the design is guided by information security and network management.

Key words authentication, IEEE 802.1X-standard, RADIUS, WLAN

SISÄLLYS

KÄYTETYT LYHENTEET JA TERMIT

ARP	Address Resolution Protocol (IEEE 2019, 92), osoitteen-selvittämisprotokolla, joka selvittää IP-osoitteen perusteella MAC-osoitteen
Broadcast	yleislähetys
BSS	Basic Service Set (Geier 2015, 45)
Captive portal	Vierailijaportaali, verkkosivu, jolla käyttäjän on käytävä saadakseen pääsyn verkkoon
DHCP	Dynamic Host Configuration Protocol (IEEE 2019, 92), verkkoprotokolla, jonka tehtävänä on jakaa IP-osoitteita verkon laitteille
GHz	gigahertsi
ISO	International Organization for Standardization (ISO 1994, 4)
LAN	Local Area Network
MAC	Media Access Control
NAS	Network Access Server
PSK	Pre-Shared Key, esijaettu salasana
PVLAN	Private VLAN
RADIUS	Remote Access Dial On User Service
SSID	Service Set Identifier (Geier 2015, 143)
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
WLAN	Wireless Local Area Network

1 JOHDANTO

Yritykset tarjoavat usein vierailleen Internet-yhteyden, joka on toteutettu langattomalla verkolla. Vaikka monissa päätelaitteissa on mahdollisuus Internet-yhteyteen myös matkapuhelinverkon kautta, tuo vierasverkko monia etuja niin yritykselle kuin vieraillekin. Yritysten näkökulmasta esimerkiksi hotellille vierasverkon tarjoaminen voi olla rahanarvoinen lisäpalvelu, joka samalla mahdollistaa vieraille suunnatun tiedottamisen. Yritys voi vierasverkon avulla tarjota vieraille turvallisen ja hallitun yhteyden Internetiin tilanteessa, jossa yrityksen tiloissa matkapuhelinverkon kuuluvuus on rajoittunutta. Vieraiden näkökulmasta vierasverkolla voidaan tarjota heille vakaampi ja nopeampi yhteys ja he voivat välttää matkapuhelinverkon datansiirtokulut.

Opinnäytetyön aihe sai alkunsa mielenkiinnosta tutustua syvällisemmin verkkotekniikoihin, verkkopalveluihin ja niillä toteutettuihin langattomien verkkojen ratkaisuihin, joita käytetään eri aloilla toimivissa yrityksissä. Aihe syventää aiemmin hankittua osaamistani tietoverkoista ja erityisesti langattomista verkoista. Työn aluksi tarkastellaan nykyisin käytössä olevia ratkaisuja sekä määritellään tavoitteet ja reunaehdot toteutusvaihtoehdoille.

Opinnäytetyön tavoitteena on tuottaa lisätietoa ja valmiita toteutusvaihtoehtoja erilaisten vierasverkkojen toteutuksen pohjaksi. Tavoitteena on löytää käyttäjän näkökulmasta tietoturvallisia ja helppokäyttöisiä vaihtoehtoja. Ylläpidon näkökulmasta tavoitteena on löytää ratkaisu, joka on tietoturvallinen, helppo ottaa käyttöön eri kokoonpanoissa ja joka mahdollistaa verkon helpon keskitetyn hallinnan ja konfiguroinnin. Koska kaikki tavoitteet liittyvät toisiinsa, on oletettavaa, että vastaan tulee keskenään ristiriidassa olevia tavoitteita. Tietoturvallisen, mutta helppokäyttöisen ratkaisun löytäminen on ennakko-odotusten perusteella haastavinta.

Työssä ei käydä läpi yksityiskohtaisia valmistajakohtaisia ratkaisuita, koska kun pitäydytään universaaleissa ratkaisuissa, työ on laajemmin hyödynnettävissä. Samoin laitteiden konfigurointi on rajattu pois työstä. Työssä käsitellään LAN:ia vain siinä laajuudessa, kuin on tarpeellista toteutusvaihtoehtojen toimintaperiaatteiden ymmärtämiseksi.

2 VERKKOTEKNIIKAT JA VERKKOPALVELUT

2.1 Langattomien lähiverkkojen tekniikka

Langaton lähiverkko (WLAN) on langaton verkkoteknologia, joka mahdollistaa laitteiden, kuten tietokoneiden, mobiililaitteiden ja muiden sitä tukevien laitteiden langattoman verkkoyhteyden toisiinsa ja muihin verkkoihin (Cisco 2020b). Wi-Fi-verkot perustuvat IEEE 802.11 -sarjan standardeihin. Ryhmä laitteita voi kommunikoida keskenään langattomasti, kun ne on varustettu 802.11 standardin mukaisilla verkkokorteilla. (Al, Pujolle & Yahiha 2016, 154.)

Wi-Fi Alliance on voittoa tavoittelematon teollisuusjärjestö, joka muun muassa edistää rekisteröidyn Wi-Fi-markkinointinimen käyttöä ja tarjoaa Wi-Fi-tuotteiden sertifiointia (Electronics Notes 2022). Järjestö on 802.11n-standardista alkaen antanut standardeille myös Wi-Fi-alkuiset nimet, jotka helpottavat eri sukupolvien tunnistamista ja järjestystä (Electronics Notes 2022). Termit WLAN ja Wi-Fi mielletään useasti samaa tarkoittaviksi. Näin tarkkaan ottaen ei ole, vaan Wi-Fi on vain yhdentyyppinen WLAN. Wi-Fi kuvaa laitteita, jotka noudattavat IEEE 802.11 -sarjan standardeja (Router-switch Ltd. 2020).

Langattomille lähiverkoille on olemassa kolme eri arkkitehtuuria, jotka ovat ad hoc, infrastruktuuri ja mesh. Ad hoc -verkossa päätelaitteet kytkeytyvät langattomasti suoraan toisiinsa ja eivätkä tarvitse erillistä tukiasemaa (Access Point). Tätä kutsutaan joskus myös vertaisverkoksi. Infrastruktuuri on yleisin käytössä oleva arkkitehtuuri. Siinä langattomat päätelaitteet kommunikoivat tukiaseman kanssa, ja sen kautta tarjotaan yhteys langalliseen verkkoon. Jokainen tukiasema muodostaa radiosolun, jota kutsutaan myös BSS:ksi. (Geier 2015, 43–48.) Jokainen WLAN nimetään yksilöllisellä nimellä, jota kutsutaan myös SSID:ksi (Lowe 2010, 175). Solun kuuluvuusalueella olevat päätelaitteet voivat muodostaa yhteyden tukiasemaan ja sitä kautta toisiin verkon käyttäjiin ja resursseihin (Geier 2015, 45). IEEE 802.11 kattaa kaksi alinta OSI-mallin kerrosta, fyysisen kerroksen ja siirtoyhteyskerroksen (Al ym. 2016, 156).

IEEE loi 1997 ensimmäisen WLAN-standardin nimeltä 801.11, joka käytti 2,4 GHz:n taajuusaluetta ja tuki vain 2 Mbit/s:n nimellistä yhteysnopeutta. Yhteysno-

peus oli useimmille sovelluksille liian hidas ja tämän takia tämän standardin mukaisia laitteita ei enää valmisteta. (Bradley 2021.) Tämän standardin mukaiset verkkolaitteet ovat jo yli vuosikymmenen vanhoja, eivätkä enää toimi nykyisillä laitteilla.

Vuonna 1999 julkaistu 802.11a tukee 54 Mbit/s:n nimellistä yhteysnopeutta ja käyttää 5 GHz:n taajuusaluetta. Samana vuonna julkaistiin myös 802.11b, jonka nimellinen yhteysnopeus on 11 Mbit/s ja käytettävä taajuusalue on 2,4 GHz. (Bradley 2021.)

802.11g julkaistiin vuonna 2003, sen nimellinen yhteysnopeus on 54 Mbit/s ja taajuusalueena 2,4 GHz. Yrityksenä oli yhdistää 802.11a:n ja 802.11b:n parhaat puolet sekä olla taaksepäin yhteensopiva 802.11b:n kanssa. Tässä tapauksessa tosin koko verkko hidastui 802.11b:n mukaiseen nopeuteen. (Bradley 2021.)

Vuonna 2009 julkaistiin 802.11n, joka tukee 600 Mbit/s:n nimellistä yhteysnopeutta ja käyttää 2,4 GHz:n sekä 5 GHz:n taajuusalueita (Bradley 2021). Tämä tunnetaan myös nimellä Wi-Fi 4 (Electronics Notes 2022). Se on taaksepäin yhteensopiva 802.11a/b/g:n kanssa. Ideana oli parantaa yhteysnopeutta. (Bradley 2021.)

802.11ac julkaistiin kahdessa eri vaiheessa. Ensimmäinen Wave 1 julkaistiin vuonna 2013 ja myöhempi Wave 2 julkaistiin vuonna 2016. Nimellinen yhteysnopeus on 6,93 Gbit/s ja käytetty taajuusalue 5 GHz. (Electronics Notes 2020.) Tunnetaan myös nimellä Wi-Fi 5 (Electronics Notes 2022).

802.11ax ensimmäinen julkaisu oli vuonna 2019. Nimellinen yhteysnopeus oli 10 Gbit/s ja käytetyt taajuusalueet 2,4 GHz ja 5 GHz. Toinen julkaisu tapahtui vuonna 2021, jolloin tuotiin uutena taajuusalueena 6 GHz. (Fisher 2022.) Ensimmäinen julkaisu tunnetaan myös nimellä Wi-Fi 6 ja jälkimmäinen nimellä Wi-Fi 6E (Electronics Notes 2022).

2.2 Wi-Fi-tukiasema

Tukiasema on tietoverkon laite, joka yhdistää langallisen tietoverkon langattomaan tietoverkkoon. Tukiasema toimii langattomien radiosignaaleiden keskitettynä lähetinvastaanottimena (Mitchell 2021). Tukiasema tarvitsee yhteyden LAN-verkkoon. Yhteys voi olla esimerkiksi fyysinen Ethernet-kaapeli kytkimeen tai Wi-Fi-yhteys toiseen tukiasemaan, jonka kautta saadaan yhteys kytkimeen. Wi-Fi-tukiasemat toimivat 2,4 GHz:n, 5 GHz:n ja 6 GHz:n taajuuksilla (Electronics Notes 2022).

Tukiasemalla voidaan rakentaa sen kuuluvuusalueelle langaton verkko, johon käyttäjät voivat liittyä päätelaitteillaan langattomasti. Tukiasema voi kaiuttaa yhtä tai useampaa langatonta verkkoa. Nykyaikaiset tukiasemat tukevat peräti 255:tä yhtäaikaista käyttäjää (Mitchell 2021). Tukiasemia käytetään laajasti kodeissa ja yrityksissä. Kodeissa tukiasema on yleensä integroitu reitittimeen, kun taas yrityksissä käytetään erillisiä tukiasemia.

2.3 OSI-malli

OSI-malli on standardoitu viitemalli, joka kuvaa, kuinka eri verkotetut järjestelmät vaihtavat tietoa keskenään. OSI-mallin tarkoituksena on toimia viitemallina tietoliikennejärjestelmien suunnittelussa. (ISO 1994, 1.)

OSI-malli syntyi vuonna 1980 (Puska 1999, 9). ISO standardi 7498–1 määrittelee tämän mallin. OSI-malli esittää, kuinka erotetaan verkkotoiminnot usealle kerrokselle. Jokainen näistä kerroksista käyttää alemman kerroksen palveluita ja tarjoaa palveluita ylemmälle kerrokselle. Tämä malli mahdollistaa kaikkien verkon osien keskinäisen toiminnan, riippumatta siitä, kuka on luonut protokollat ja mikä tietokonevalmistaja tukee niitä. (Simoneau 2006, 2–3.) OSI-mallia voi havainnollistaa vertaamalla sitä kirjeeseen, joka useita kertoja uudelleen paketoidaan uuteen kirjeeseen matkalla vastaanottajalle.

OSI-malli jakaa yhteysprosessit seitsemään kerrokseen. Jokainen kerros suorittaa tiettyjä toimintoja tukeakseen sen yläpuolista kerrosta ja tarjoaa palveluita sen alapuoliselle kerrokselle. Kolme alinta kerrosta keskittyvät välittämään liikennettä

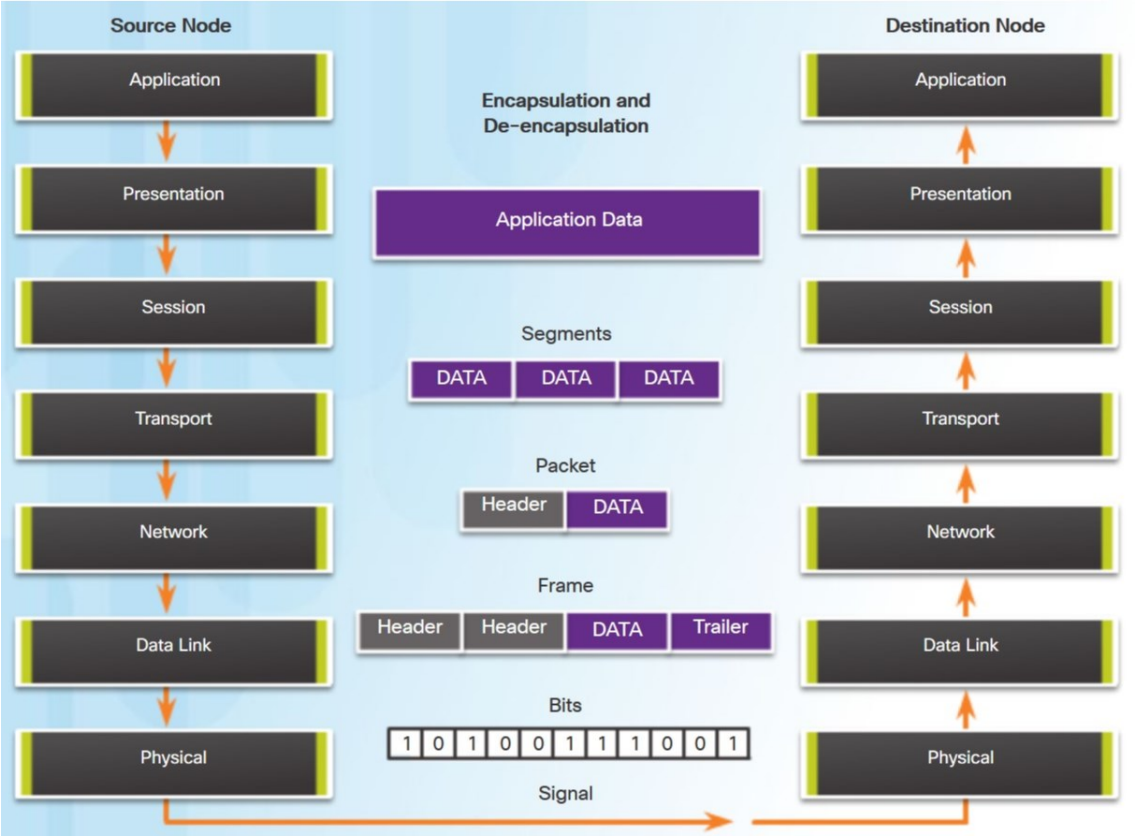
verkon läpi päätelaitteelle. Ylimmät neljä kerrosta toimivat päätelaitteessa täydentämässä prosessia. Tällaista kerroksellista mallia kutsutaan protokollapinoksi tai protokollasarjaksi. Protokolla tai säännöt voivat toimia joko laitteistossa tai ohjelmistossa. Useimmissa protokollapinoissa ne toimivat näiden yhdistelmässä. Pinojen luonne on, että alimmat kerrokset tekevät työnsä laitteistossa tai laiteohjelmistossa, kun taas ylemmät kerrokset toimivat ohjelmistossa. (Simoneau 2006, 2–3.) Kuviossa 1 nähdään mallin eri kerrokset englanniksi ja suomeksi.

Kuvio 1. OSI-malli (mukaillen ISO 1994, 28)

OSI-mallin tärkeimmät hyödyt ovat seuraavat (Simoneau 2006, 3):

- Auttaa käyttäjää ymmärtämään verkotuksen ison kuvan.
- Auttaa käyttäjää ymmärtämään, kuinka laitteisto- ja ohjelmistoelementit toimivat yhdessä.
- Tekee vianetsinnästä helpompaa jakamalla verkot hallittaviin osiin.
- Määrittää termit, joita verkkoasiantuntijat voivat käyttää vertaillessa perustoimintojen suhteita erilaisissa verkoissa.
- Auttaa käyttäjää ymmärtämään uusia teknologioita, kun niitä kehitetään.
- Auttaa tuotteen toimintojen tulkinnassa toimittajan toimintaselosteesta.

Kuviossa 2 on esitetty datan kulku lähdejärjestelmästä kohdejärjestelmään eri kerrosten läpi, datan kapselointi ja dekapselointi. Datan kulku lähdejärjestelmästä kohdejärjestelmään on seuraava. Käyttäjän data segmentoidaan kuljetuskerroksessa, sijoitetaan paketteihin verkkokerroksessa ja kapseloidaan kehyksiksi siirtoyhteyskerroksessa. Fyysinen kerros koodaa uudelleen kehykset ja luo sähköisen, optisen tai radioaaltosignaalin, joka kuvaa kehyksen jokaista bittiä. Nämä signaalit lähetään siirtomediaan yksi kerrallaan. Vastaanottosolmun fyysinen kerros kerää yksittäiset signaalit siirtomediasta, palauttaa ne bittimuotoon ja välittää bitit siirtoyhteyskerrokselle kokonaisina kehyksinä. (Cisco 2020a.)



Kuvio 2. Kerrosten kuvaus (Cisco 2020a)

Fyysisellä kerroksella käsitellään verkon fyysisiin ominaisuuksiin liittyviä asioita, kuten laitteiden liittämiseen käytettäviä kaapeleita, käytettyjen liittimien tyyppejä ja kaapeleiden pituuksia (Lowe 2010, 396). **Siirtoyhteyskerros** mahdollistaa ylemmille kerroksille yhteyden siirtoyhteyteen. Siirtoyhteyskerros vastaanottaa verkkokerroksen paketit ja pakkaa ne kehyksiksi. Se valmistelee datan fyysistä verkkoa varten sekä kontrolloi, kuinka data sijoitetaan ja vastaanotetaan

siirtoyhteydessä. Se myös vaihtaa kehyksiä solmujen yli fyysisessä verkkomediassa, kuten parikaapelissa tai valokuidussa. Siirtoyhteyskerros vastaanottaa ja ohjaa paketit ylemmän kerroksen protokollalle. (Cisco 2020a.) Se huolehtii virheiden havaitsemisesta ja korjaamisesta (Lowe 2010, 397).

Solmuiksi kutsutaan sellaisia siirtoyhteyskerroksen verkkolaitteita, jotka on kytketty yhteiseen siirtoyhteyteen (Cisco 2020a). Solmut rakentavat ja välittävät kehyksiä. Siirtoyhteyskerros on vastuussa Ethernet-kehysten vaihdosta lähde- ja kohdesolmuissa fyysisen verkkomedian yli. (Cisco 2020a.) Siirtoyhteyskerroksella laitteiden osoitteena käytetään niiden MAC-osoitteita. MAC-osoitteet ovat yleensä kovakoodattuina laitteissa ja osoitteet eivät siksi yleensä vaihdu. (Petryschuk 2022.)

MAC-osoite on kuitenkin mahdollista muuttaa, ja tämä mahdollisuus tulee huomioida, mikäli MAC-osoitetta käytetään laitteiden tunnistukseen. Lisäksi monet nykyaikaiset käyttöjärjestelmät tarjoavat mahdollisuuden vaihtuvan satunnaisen MAC-osoitteen käyttöön (Matte, Cunche, Rousseau & Vanhoef 2016). Satunnainen MAC-osoite toimii erityisesti julkisissa verkoissa osana käyttäjän tunnistamisen ja seurannan hankaloittamista. Päätelaitetta ei voida tunnistaa luotettavasti samaksi osoitteen perusteella, koska päätelaitteen osoite voi olla erilainen joka yhteyskerralla. Verkon ylläpidon näkökulmasta olisi hyödyllistä kyetä tunnistamaan päätelaitteet luotettavasti. (Matte ym. 2016.) Satunnainen MAC-osoite aiheuttaa haasteita esimerkiksi tilanteissa, joissa tietyn MAC-osoitteen liikennöinti verkossa on teknisin menetelmin estetty aiemmin tai selvitettäessä käyttäjän ilmoittamaa yhteysongelmaa.

Verkkokerros määrittelee osoitteistuksen ja prosessit, jotka mahdollistavat kuljetuskerroksen datan paketoinnin ja siirron. Se antaa osoitteet päätelaitteille. Tämä kerros kapseloi jälleen kuljetuskerroksen segmentin paketiksi. Verkkokerros tarjoaa palveluita ohjatakseen paketteja kohdejärjestelmään kohdeverkossa. Tällä kerroksella toimivat esimerkiksi reitittimet ja monikerroskytkimet. Verkkokerroksella päätelaitteet käyttävät yleisesti IPv4- ja tai IPv6-osoitteita. (Simoneau 2006, 5–6.)

Kuljetuskerroksen tehtävinä on sovellukselta vastaanotetun datan segmentointi, otsikon lisääminen tunnistusta varten ja segmenttien hallinnointi sekä otsikkotiedon perusteella tapahtuva segmenttien uudelleen kasaaminen sovellusdataksi ja kootun datan välittäminen oikealle sovellukselle. Kuljetuskerroksen protokollia ovat UDP ja TCP. (Simoneau 2006, 6.)

Istuntokerroksen tehtävä on luoda ja ylläpitää dialogeja lähde- ja kohdesovellusten välillä. Istuntokerros hoitaa tiedonvaihdon liittyen dialogin aloitukseen, ylläpitoon ja uudelleen aloitukseen keskeytyneiden tai pitkään käyttämättä olleiden istuntojen osalta. (Simoneau 2006, 7.)

Esitystapakerroksen kolme tärkeintä tehtävää ovat (Simoneau 2006, 8)

- datan muodon määrittäminen tai esittäminen siten, että data on vastaanottajan kanssa yhteensopivassa muodossa
- datan pakkaus niin, että sen on vastaanottopäässä purettavissa
- datan salaus ja salauksen purku.

Sovelluskerros tarjoaa rajapinnan sovellusten ja mallin alempien kerrosten välille (Simoneau 2006, 8). Yleisimpiä sovelluskerroksen protokollia ovat HTTP, FTP, IMAP ja DNS (Cisco 2020a).

2.4 VLAN

VLAN on verkon laitteista koostuva looginen ryhmä. Ryhmän laitteita voivat olla työasemat, palvelimet ja muut verkon laitteet. Kun LAN:issa kytketään laitteita kytkimeen, muodostaa kytkin yhden yleislähetysalueen (*broadcast domain*). Kytkin välittää yleislähetysliikenteen kaikille alueeseen kuuluville. Jokainen VLAN muodostaa oman yleislähetysalueensa. VLAN:ia voisi ajatella aliverkkona. Samoin kuin aliverkot, eivät myöskään VLAN-ryhmät voi kommunikoida keskenään ilman reitittävää laitetta niiden välillä. (Computer Networking Notes and Study Guides 2018.) ARP-viestit ja DHCP-viestit ovat esimerkkejä yleislähetysliikenteestä.

VLAN:eilla on kaksi päätoimintoa LAN-verkossa: fyysisen kytkimen jakaminen useammaksi loogiseksi tai virtuaaliseksi kytkimeksi ja mahdollisuus laajentaa virtuaalikytkin toiminnallisuus useaan fyysiseen kytkimeen. Jakamalla fyysinen kytkin useammaksi loogiseksi tai virtuaaliseksi kytkimeksi voidaan esimerkiksi jakaa 15-porttinen kytkin kolmeksi 5-porttiseksi virtuaalikytkimeksi. Jokainen näistä virtuaalikytkimistä muodostaa oman VLAN:insa. Virtuaalikytkimien liikenne on erotettu toisistaan, kuin kyseessä olisi kolme erillistä fyysistä kytkintä. (Practical Networking 2016.)

Virtuaalikytkin toiminnallisuus on mahdollista laajentaa useaan fyysiseen kytkimeen. Tällöin samaan VLAN:iin kuuluvia portteja voi olla useassa fyysisessä kytkimessä. Kytkimet voivat olla kytkettynä toisiinsa joko suoraan tai esimerkiksi reitittimen välityksellä ja ne voivat sijaita fyysisesti erillään toisistaan. (Practical Networking 2016.)

VLAN-tunnuksen (VLAN ID) numero-osuus on yksinkertaistettuna vain numero, joka on määritelty kullekin portille. Portit kuuluvat oletus-VLAN:iin, jos niitä ei ole erikseen määritelty kuuluvaksi johonkin tiettyyn VLAN:iin. Oletus-VLAN:in numero on yleensä 1. Esimerkiksi kytkimestä voidaan määritellä kolme porttia kuuluvaksi VLAN:iin 20 ja viisi muuta VLAN:iin 30. Mahdolliset loput portit kuuluvat siis oletus-VLAN:iin, koska niitä ei ole erikseen määritelty mihinkään muuhun VLAN:iin. (Practical Networking 2016.)

Kytkimen kukin portti voidaan määritellä joko merkitty portti -tilaan (*tagged port*) tai merkitsemätön portti -tilaan (*untagged port*). Toimitilamäärittely on porttikohtainen. Merkittyjä portteja käytetään verkkolaitteiden, kuten reitittimien ja kytkimien kytkentään. Merkityt portit voivat kuljettaa usean VLAN:in liikennettä. (Practical Networking 2016.)

Merkitsemättömiä portteja käytetään yleensä työasemien, palvelimien ja muiden päätelaitteiden sekä joissain tapauksissa myös kytkimien kytkentään. Kun portti määritellään merkitsemättömäksi portiksi, sille määritellään samalla, mihin VLAN:iin portti kuuluu. Yksittäinen merkitsemätön portti voi kuulua vain yhteen VLAN:iin. Kun kytkin vastaanottaa liikennettä merkitsemättömään porttiin, se hyväksyy liikenteen tähän VLAN:iin. (Practical Networking 2016.)

VLAN voidaan laajentaa useampaan kytkimeen. Laajentaminen voidaan tehdä kahdella tavalla. Ensimmäinen tapa on kytkeä kahden kytkimen samaan VLAN:iin kuuluvat kaksi merkitsemätöntä porttia toisiinsa. Tämä mahdollistaa kaikkien tähän VLAN:iin kuuluvien porttien liikennöinnin keskenään, riippumatta kummassa kytkimessä portit sijaitsevat. Tällä tavalla voidaan laajentaa vain yksittäinen VLAN, joten tapa ei ole skaalaudu helposti. Toinen ja parempi tapa on käyttää merkittyjä portteja, jotka voivat kuljettaa useamman VLAN:in liikennettä yhden portin kautta. (Practical Networking 2016.) Esimerkiksi tapauksessa, jossa 15-porttinen kytkin on jaettu kolmeksi VLAN:iksi, voidaan kaikkien kolmen VLAN:in liikenne välittää toiselle kytkimelle käyttäen vain yhtä merkittyä porttia kytkintä kohden.

VLAN:ien nimeämisessä käytetään usein muotoa, jossa VLAN-tunnus muodostuu tekstistä VLAN ja sen jälkeisestä yhdestä tai useammasta numerosta. Samaa numeroa käytetään usein myös osana IPv4-aliverkon osoitetta, eli VLAN 10 jonka aliverkko olisi muotoa x.x.10.x, kun taas VLAN 20 tapauksessa se olisi x.x.20.x. Tapa ei ole pakollinen, mutta se selkeyttää konfigurointia ja hallintaa.

VLAN:ien etuna on yleislähetysalueiden pieneneminen, koska jokainen VLAN muodostaa oman yleislähetysalueensa. Yleislähetysalueiden määrä kasvaa, mutta yleislähetysliikenteen vastaanottajien määrää pienenee yksittäisellä yleislähetysalueella. Tämä vähentää yleislähetysliikenteen aiheuttamia haittoja muulle liikenteelle. (Computer Networking Notes and Study Guides 2018.) Esimerkkinä on lähetysmyrsky, jossa verkossa lähetetään epänormaalin paljon yleislähetyspaketteja, joiden käsittely kuormittaa verkon laitteita (Patel 2017).

VLAN parantaa myös verkon turvallisuutta. OSI-mallin kerroksen 2 verkoissa kaikki verkon käyttäjät voivat nähdä toisensa. He voivat lähettää ja vastaanottaa yleislähetysliikennettä ja päästä käsiksi kaikkiin verkkoresursseihin. Jakamalla käyttäjät eri VLAN:eihin, voidaan heidät erottaa toisistaan. (Computer Networking Notes and Study Guides 2018.) Esimerkkinä voisi olla Rogue DHCP Server, joka on yksinkertaistettuna verkkoon kuulumaton DHCP-palvelin. Palvelin voi olla esimerkiksi vihamielisen tahon tarkoituksella verkkoon kytkemä tai inhimillisen virheen takia verkkoon kytketty. (Petryschuk 2021.) DHCP-liikenne on salaama-

tonta ja on normaalia, että verkossa voi olla useita DHCP-palvelimia. Näitten syitten takia on yksinkertaista väärentää verkkoon kuulumattoman palvelimen DHCP-liikenne tulevaksi luvalliselta palvelimelta. (Agarwal, Biswas & Nandi 2017, 797, 799.) Rogue DHCP:een vaikutus rajautuu lähtökohtaisesti vain tähän VLAN:iin.

VLAN helpottaa laitehallintaa, koska VLAN:it ovat loogisia ryhmiä. Loogisessa ryhmässä laitteet voivat fyysisesti sijaita missä kohdassa tahansa fyysistä verkkoa ja silti kuulua samaan yleislähetysalueeseen. Käyttäjiä voidaan myös siirtää eri kytkimelle samassa verkossa ja he säilyvät samassa VLAN:issa. (Computer Networking Notes and Study Guides 2018.)

VLAN-jäsenyyksiä on kaksi erilaista, staattinen ja dynaaminen. Staattinen jäsenyys on yleisin ja turvallinen tapa. Staattinen VLAN-jäsenyys määritellään porttikohtaisesti. Määrittely säilyy, kunnes se manuaalisesti muutetaan, ja tapa on siksi turvallinen. Staattinen toimii hyvin verkkoympäristössä, jossa käyttäjän liikkeitä verkossa halutaan kontrolloida. Dynaamisessa VLAN-jäsenyydessä porttiin määritelty VLAN riippuu kytketystä laitteesta, esimerkiksi laitteen MAC-osoitteesta tai IP-osoitteesta. Dynaamisessa jäsenyydessä etuna on laitteiden helppo siirrettävyys, koska laite sijoitetaan aina samaan VLAN:iin riippumatta sen fyysisestä sijainnista tai kytkeytymiseen käytetystä portista, kunhan verkko on oikein konfiguroitu. (Computer Networking Notes and Study Guides 2018.) Dynaamisessa on myös turvallisuuden kannalta etuna se, että tunnistamattomat laitteet voidaan sijoittaa rajattuun VLAN:iin. Lisäksi yhdisteltynä muihin tekniikoihin voidaan portti sulkea, jolloin tunnistamaton laite ei voi liikennöidä verkossa aktiivisesti lähettäen tai passiivisesti verkon liikennettä kuunnellen.

2.5 PVLAN

PVLAN on tekniikka, joka mahdollistaa VLAN:in jakamisen ali-VLAN:eihin. PVLAN-infrastruktuuri koostuu kolmesta erityyppisestä VLAN:ista. PVLAN sisältää aina ensisijaisen VLAN:in (*primary VLAN*), johon määritetyt laitteet voivat liikennöidä kaikkien muiden PVLAN:in laitteiden kanssa. Tätä käytetään yleensä esimerkiksi palvelimille, reitittimelle ja muille OSI-mallin kolmoskerroksen laitteille, joihin on tarpeellista sallia yhteys muistakin VLAN:eista kuin ensisijaisesta

VLAN:ista. Lisäksi PVLAN-infrastruktuuri sisältää yhden tai useamman toissijaisen VLAN:in (*secondary VLAN*), joita on kahta eri tyyppiä eristetty VLAN (*Isolated VLAN*) ja yhteisö VLAN (*Community VLAN*). Eristettyyn VLAN:iin määritetyt laitteet on OSI-mallin kakkoskerroksella erotettu muista laitteista samassa VLAN:issa. Erotus kattaa myös yleislähetysliikenteen, ja eristettyyn VLAN:iin määritetyt laitteet eivät voi liikennöidä muiden kuin ensisijaisessa VLAN:issa olevien laitteiden kanssa. Samassa yhteisö VLAN:issa olevat laitteet voivat liikennöidä keskenään ja ensisijaisessa VLAN:issa olevien laitteiden kanssa, mutta eivät eri yhteisö VLAN:eissa olevien laitteiden kanssa. Kaikki PVLAN:in sisäiset VLAN:it ovat samassa IP-aliverkossa, koska vain ensisijaisella VLAN:illa on OSI-mallin kolmoskerroksen yhteys. (Bazire 2012b.)

2.6 AAA-kehysmalli

AAA-kehysmalli kuvaa ne turvallisuuskontrollit, joilla varmistetaan verkon turvallinen ja oikea käyttö. Malli koostuu tunnistamisesta (*Authentication*), valtuuttamisesta (*Authorization*) ja tilastoinnista (*Accounting*). Käyttäjät saavat pääsyn verkkoihin ja verkkoresursseihin monenlaisten laitteiden kautta, esimerkiksi kytkimien, WLAN-tukiasemien ja VPN-palvelimien kautta. NAS-laitteiksi kutsutaan laitteita, joita hyödynnetään verkon pääsynhallinnassa. NAS-laitteita on WLAN-tukiasema, joka käyttää WPA2 Enterprise -suojausta tai Ethernet-kytkin, jossa on 802.1X-porttikohtainen todennus käytössä. (Walt 2011, 36.)

Tunnistaminen on yleensä ensimmäinen vaihe verkkoon ja sen palveluihin pääsemiseksi. Tunnistamisessa varmistetaan käyttäjän antamat tunnistetiedot. Tunnistetietoina voidaan käyttää käyttäjätunnusta, salasanaa, kertakäyttöistä tunnistetta, varmennetta, PIN-koodia tai biometristä skannausta. Onnistuneen tunnistamisen jälkeen istunto on alustettu, ja se suljetaan, kun yhteys verkkoon suljetaan. (Walt 2011, 37.)

Valtuuttamisessa määritellään käyttäjälle tarjottavat resurssit, kuten IP-osoite, käyttäjäryhmän mukaiset oikeudet, käytettävän laitteen tai kellon ajan perusteella muuttuvat oikeudet. Valtuuttaminen sisältää usein logiikkaa. (Walt 2011, 38.) Otetaan esimerkiksi käyttäjä Kalle Kirjanpitäjä. Kallen kirjautuessa yrityksen työ-

asemalta verkkoon työasemalle annetaan talousosastolle varatusta IP-osoiteavaruudesta osoite ja sallitaan pääsy tarvittaviin verkon resursseihin. Kallella ei ole työtehtävien edellyttämää tarvetta Internetin käyttöön työasemalta, joten Internet-yhteys estetään. Siinä tapauksessa, että Kalle kirjautuu yrityksen älypuhelimella verkkoon, voidaan puhelin ohjata yrityksen puhelimille tarkoitettuun IP-osoiteavaruuteen ja sallia yhteys Internettiin, mutta ei verkon resursseihin. Käytännön sovelluksessa valtuuttaminen perustuu roolitukseen, jossa määritellään kullekin roolille tarjottavat resurssit sen sijaan, että määriteltäisiin jokaiselle käyttäjällä tai laitteelle yksittäin tarjottavat resurssit.

Tilastointi on jatkuvaa käytettyjen resurssien mittausta. Kerätyn datan perusteella esimerkiksi operaattori tai hotelli voi laskuttaa asiakasta. Datan avulla voidaan tehdä kapasiteettisuunnittelua ja tehdä toiminnan seurantaa verkossa. Lisäksi voidaan analysoida trendejä, kuten mihin aikaan päivästä kapasiteettia on eniten käytössä. (Walt 2011, 38.)

2.7 RADIUS

RADIUS-protokolla oli alun perin osa Livingston Enterprisesin vuonna 1991 suunnittelemaa AAA-ratkaisua, jolla voidaan toteuttaa käyttäjien tunnistus, valtuutus ja tilastointi. Sanalla RADIUS voidaan tarkoittaa joko RADIUS-protokollaa tai kokonaista RADIUS-asiakaspalvelinjärjestelmää. (Walt 2011, 40.)

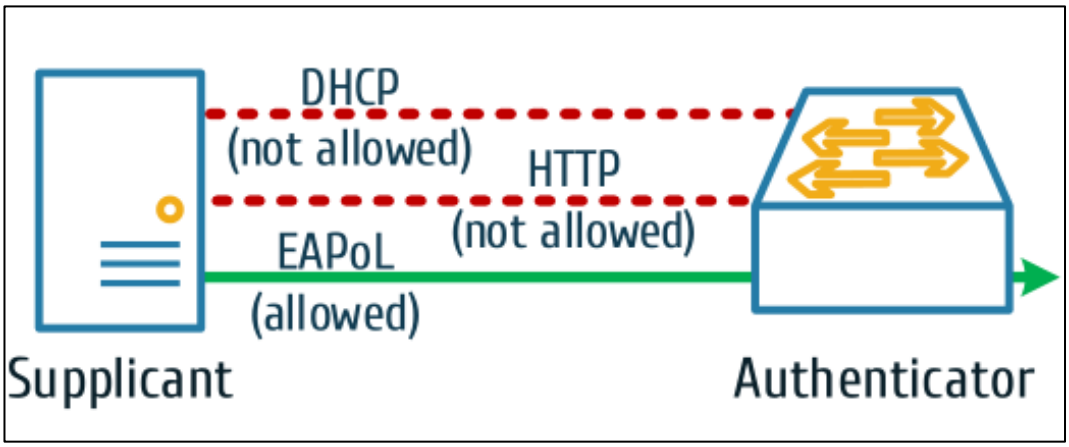
RADIUS-protokolla on asiakas/palvelinprotokolla, joka käyttää UDP-protokollaa. Tyypillinen asiakkaan ja palvelimen välinen liikenne sisältää yksittäisen asiakkaan pyynnön sekä yksittäisen vastauksen palvelimelta. Tämä tekee RADIUS-protokollasta hyvin kevyen ja siten tehokkaan myös hitailla yhteyksillä. (Walt 2011, 41.) RADIUS-asiakkaana toimii NAS, joka voi olla muun muassa WLAN-tukiasema tai Ethernet-kytkin, joka tukee 802.1X-porttikohtaista todennusta (Walt 2011, 36). Asiakas toimii välittäjänä palvelimen ja käyttäjän laitteen välillä. Asiakas ja palvelin käyttävät liikenteen salaamiseen jaettua salaisuutta (*shared secret*) (Walt 2011, 47), jolla palvelin myös todentaa asiakkaat (Walt 2011, 41).

2.8 802.1x

IEEE 802.1x on IEEE-standardi, joka määrittelee porttikohtaisen todennuksen LAN:eissa ja WLAN:eissa (Study-CCNA 2021). 802.1x-porttikohtainen todennus toimii OSI-mallin siirtoyhteys- eli kakkoskerroksella (Kovačić, Đulić & Sehidic 2017). Todennuksen toiminta perustuu kolmeen pääkomponenttiin, jotka ovat asiakas (*supplicant*), todentaja (*authenticator*) ja todennuspalvelin (*authentication server*). Asiakas on laite tai käyttäjä, joka tarvitsee pääsyn verkkoon. Todentaja on verkon laite, kuten tukiasema tai kytkin. Todennuspalvelin on luotettu palvelin, joka toteuttaa verkkoyhteyden todennuksen vastaanottamalla, prosessoimalla ja vastaamalla asiakkaalta tuleviin pyyntöihin. Todennuspalvelin päättää ja ohjeistaa todentajaa joko sallimaan tai kieltämään pääsyn sekä soveltamaan erilaisia asetuksia käyttäjään. (Study-CCNA 2021.)

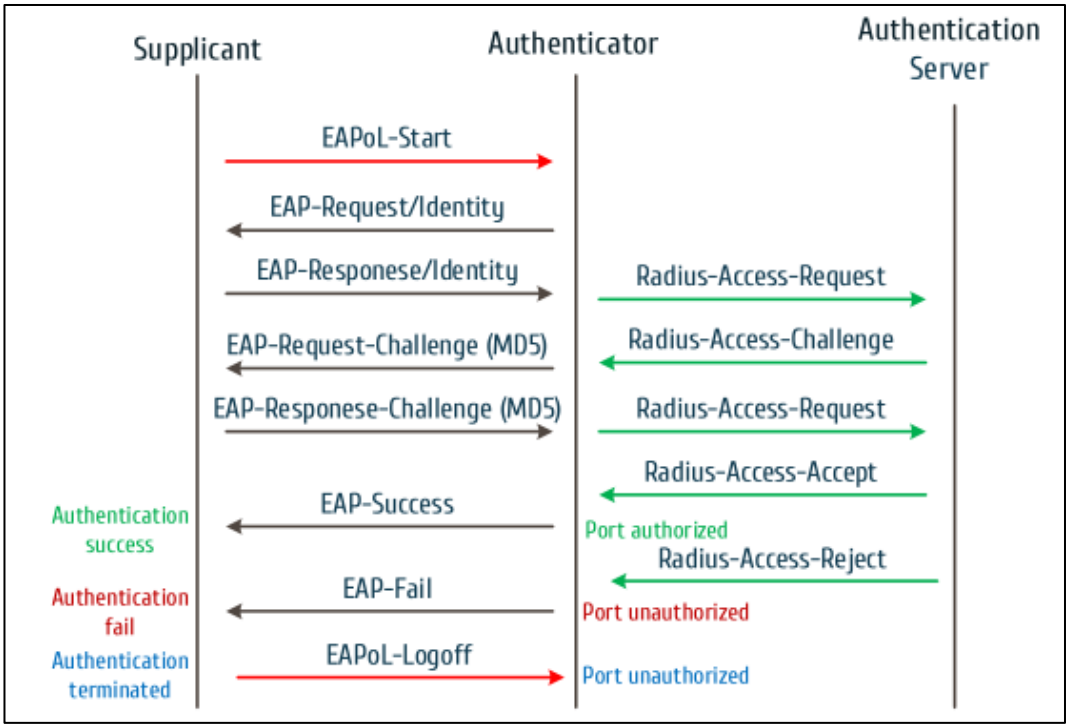
EAP-protokollaa (Extensible Authentication Protocol) käytetään todentamisviestien välitykseen asiakkaan ja todennuspalvelimen välillä. Käytetty EAP-todennusmenetelmä määrittelee ja käsittelee todennuksen. Todentaja toimii välittäjänä asiakkaan ja todennuspalvelimen välissä. (Intel 2021.)

802.1x-todennusprosessi käynnistyy asiakkaan kytkeydyttyä todentajaan. Tässä vaiheessa prosessia portti on tilassa luvaton. Todentaja sallii vain EAP-viestit, jotka todentaja välittää todennuspalvelimelle. Muut verkkopalvelut on tilassa kielletty (Kuvio 3). (Kovačić ym. 2017.)



Kuvio 3. Portti ennen todennusta (Kovačić ym. 2017)

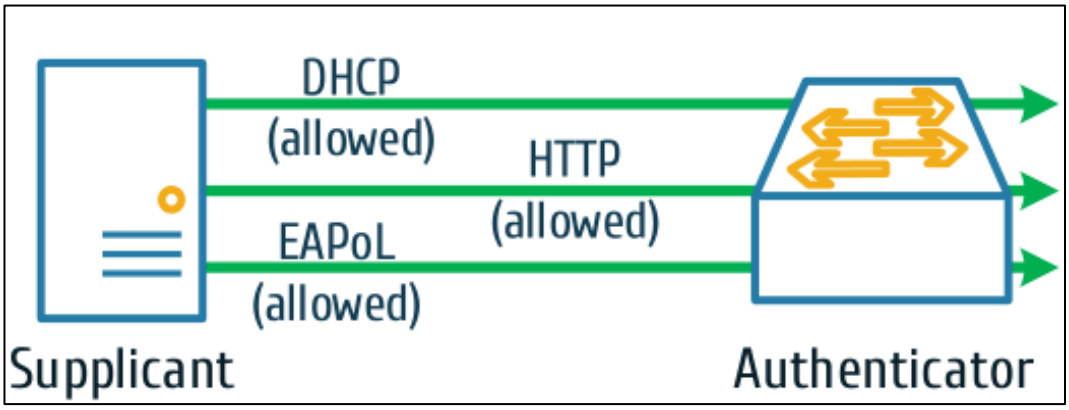
Kuviossa 4 on esitetty 802.1x todennusprosessi. Asiakas lähettää EAPOL-Start -viestin, johon todentaja vastaa lähettämällä EAP-Request/Identity-viestin. Seuraavaksi asiakas lähettää EAP-Response/Identity-vastauksen, jonka todentaja välittää todennuspalvelimelle Radius-Access-Request-viestinä. (Kovačić ym. 2017.) Tässä kohdassa todennusprosessia riippuen käytetystä todennusprotokollasta voidaan käydä läpi kaksipuolinen varmenteiden tarkistus. Sillä voidaan varmistua asiakkaan ja todennuspalvelimen oikeista identiteeteistä ja muodostaa salattu tunneli asiakkaan tunnistetietojen siirtämiseksi palvelimen ja asiakkaan välillä (Raphaely 2019).



Kuvio 4. Todennusprosessi (Kovačić ym. 2017)

Lopputuloksena todennuspalvelin joko hylkää tai hyväksyy asiakkaan. Asiakkaan hylkäys tapahtuu todennuspalvelimen lähettämällä Radius-Access-Reject-viestillä, joka välitetään asiakkaalle EAP-Fail-viestinä ja portti pidetään tilassa luvaton. Asiakkaan hyväksyntä tapahtuu todennuspalvelimen lähettämällä Radius-Access-Accept-viestillä, joka välitetään EAP-Success-viestinä. Todentaja muuttaa portin tilaan luvallinen, jolloin asiakkaan liikenne verkkoon sallitaan (Kuvio 5). Mikäli asiakas ei enää tarvitse verkkoyhteyttä, voidaan yhteys sulkea EAPoL-Logoff-viestillä, jolloin todentaja muuttaa portin takaisin tilaan luvaton (Kuvio 4). Koska todennus tapahtuu OSI-mallin kakkoskerroksella, niin vasta onnistuneen

todennuksen jälkeen DHCP-palvelin voi antaa asiakkaalle IP-osoitteen. (Kovačić ym. 2017.) Tämä hankaloittaa luvatonta käyttöä ja tarjoaa mahdollisuuden ohjata asiakas haluttuun VLAN:iin. VLAN-ohjauksen osalta voidaan ottaa verrattavaksi tilanne, jossa asiakkaalla on IP-osoite ennen todennuksen aloitusta ja asiakas halutaan todennuksen jälkeen ohjata eri VLAN:iin. Silloin asiakas täytyisi ensin hallitusti kytkeä irti nykyisestä yhteydestä ja asiakkaan uudelleen yhdistäessä ohjata haluttuun VLAN:iin.



Kuvio 5. Portti todennuksen jälkeen (Kovačić ym. 2017)

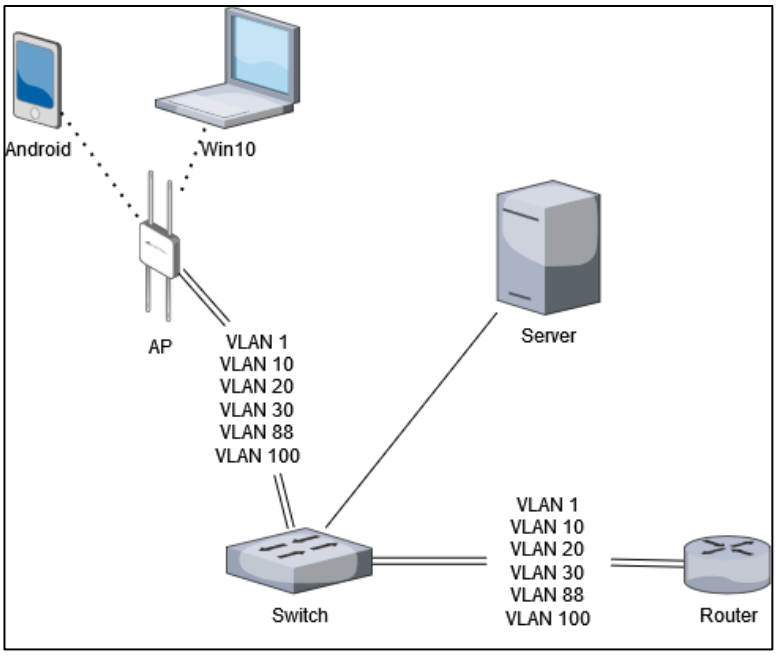
3 TUTKIMUKSEN TOTEUTUS

3.1 Testiympäristö

Käytössä oli testiympäristö eri toteutusvaihtoehtojen testaukseen ja käytännön toiminnan todentamiseen. Testiympäristö olisi mahdollistanut myös valmistajakohtaisten ratkaisuiden käyttämisen, mutta tässä työssä pitäydyttiin ratkaisuissa, jotka on mahdollista toteuttaa eri valmistajien laitteilla. Kuviossa 6 on kuvattuna testiympäristön looginen kaavio.

Testiympäristö sisälsi kiinteästi Windows 10 -kannettavan, Android 12 -älypuhelimen, palvelimen, tukiaseman, kytkimen ja reitittimen. Lisäksi oli tilapäisesti käytössä muutama vanhemmalla Android-versiolla varustettu laite, joilla oli mahdollista testata, että konfiguraatiot toimivat myös vanhemmilla käyttöjärjestelmäversiolla. Testiympäristössä olisi ollut hyödyllistä olla myös joitakin Applen laitteita, mutta sellaisia en onnistunut samaan käyttööni tätä työtä varten.

Palvelin toimi ajoalustana vierasportaalille sekä verkonhallintaohjelmistolle. Verkonhallintaohjelmisto mahdollisti verkkolaitteiden konfiguroinnin sekä verkonvalvonnan. Reititin tuotti DHCP-palvelin, RADIUS-palvelin ja palomuuripalvelut. Kuviossa 6 näkyvät laitteet, tukiasema (AP), kytkin (switch) ja reititin (router) olivat yhteensopivia VLAN:in ja 802.1x:n kanssa.



Kuvio 6. Testiympäristön looginen verkkokaavio

3.2 Tukiaseman konfiguraatio

Tukiasemalle oli konfiguroitu neljä langatonta verkkoa. Nimeämislogiikan tarkoitus oli helpottaa langattoman verkon ominaisuuksien tunnistamista jo nimestä. Ensimmäinen merkki kertoo kyseessä olevan langaton verkko. Toinen merkki kertoo verkon järjestysnumeron. Kolmas ja mahdollinen neljäs merkki kertoo käytetyn salauksen ja tunnistuksen. Taulukossa 1 on esitettynä langattomat verkot ja niiden ominaisuudet.

Taulukko 1. Langattomat verkot

SSID	Salaus	Tunnistus
W0R	WPA2 Enterprise	RADIUS
W1RC	WPA2 Enterprise	RADIUS+ Vierasportaali
W2OC	Avoin	Vierasportaali
W3PC	WPA2 PSK	PSK+ Vierasportaali

VLAN:eja oli konfiguroituna kuusi kappaletta (Taulukko 2), joista VLAN 1 oli oletus-VLAN, jota käytettiin myös hallinta-VLAN:ina. VLAN 10,20 ja 30 olivat eri käyttäjäryhmien käytössä siten, että käyttäjät ohjattiin tiettyyn VLAN:iin IP-osoitteen, SSID:n tai käyttäjätunnuksien perusteella. Käyttäjät ohjattiin ensimmäisenä VLAN:iin 100 niissä vaihtoehdoissa, joissa käyttäjä myöhemmin voitiin siirtää eri VLAN:iin. Käyttäjät jätettiin VLAN:iin 100 siinä tapauksessa, että todennus ei tapahtunut onnistuneesti. Kaikissa paitsi oletus-VLAN:issa käyttäjät on erotettu toisistaan OSI-mallin kerroksella 2 ja OSI-mallin kerroksella 3.

Taulukko 2. VLAN:it ja niiden ominaisuudet

Nimi	Verkko	Tarkoitus
VLAN 1	192.168.69.0/24	Hallinta
VLAN 10	192.168.10.0/24	RADIUS käyttäjät
VLAN 20	192.168.20.0/24	RADIUS käyttäjät
VLAN 30	192.168.30.0/27	RADIUS käyttäjät
VLAN 88	192.168.88.0/25	PSK ja Vierasportaali käyttäjät
VLAN 100	192.168.100.0/24	Eristys

Käyttäjätunnuksia oli konfiguroitu viisi kappaletta (Taulukko 3). Kaikille käyttäjätunnuksille oli asetettu sama salasana testauksen nopeuttamiseksi. Kaikissa todennustavoissa oli käytössä käyttäjänimi ja salasana -yhdistelmä, lukuun ottamatta WPA2 PSK -todennusta, jossa käytettiin esijaettua salasanaa.

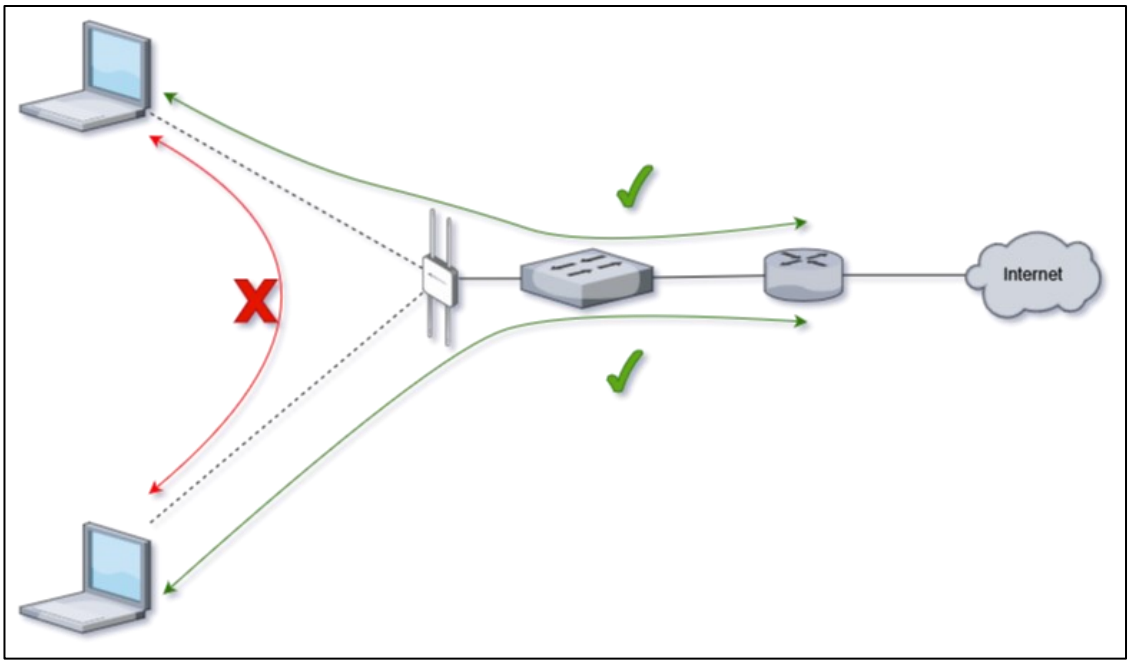
Taulukko 3. Käyttäjätunnukset ja niiden ominaisuudet

Käyttäjänimi	VLAN	Tunnistus
testaaja10	10	RADIUS
testaaja20	20	RADIUS
testaaja30	30	RADIUS
testaaja88	88	Vierasportaali
testaaja100	100	Vierasportaali

3.3 Erotuksen toteutus

Testiympäristössä käytetyn laitteen valmistaja ei kerro julkisesti, millaisella ratkaisulla heidän laitteissaan OSI-mallin kakkoskerroksella toteutettu päätelaitteiden erotus on toteutettu. Erotus OSI-mallin kakkoskerroksella on mahdollista toteuttaa PVLAN-tekniikan avulla sijoittamalla samaa tukiasemaa, SSID:tä ja VLAN:ia käyttävät päätelaitteet eristettyyn VLAN:iin, joka sallii liikennöinnin ainoastaan ensisijaiseen VLAN:iin (Kuvio 7). Jos päätelaitteet olisi erotettu toisistaan ainoastaan laittamalla päätelaitteet eri VLAN:eihin, päätelaitteilla olisi edelleen mahdollista liikennöidä saman VLAN:in sisällä, mikä ei ole toivottavaa vierasverkkojen tapauksessa. (Bazire 2012a.)

Erottelun tarpeesta kertoo esimerkki hotellista, jossa Internet-yhteys on toteutettu hotellivieraille WLAN:in kautta käyttäen yhtä SSID:tä koko vierasverkolle. Kukin hotellin kerros on konfiguroitu omaan VLAN:iinsa ja vieraiden päätelaitteet on sijoitettu eristettyyn VLAN:iin. Tällöin saavutetaan tilanne, jossa päätelaitteet eivät voi kommunikoida keskenään. Samassa tilanteessa ilman erotusta OSI-mallin kakkoskerroksella saman kerroksen vieraiden päätelaitteet voisivat edelleen liikennöidä keskenään, mikä ei ole haluttu tilanne.



Kuvio 7. Laitteiden liikennöinti eristetyssä VLAN:issa

OSI-mallin kolmoskerroksella erotus oli toteutettu palomuurisäännöstöllä, joka esti päätelaitteiden liikennöinnin VLAN:ien välillä. Palomuurisäännöstö salli kuitenkin DHCP:hen, DNS:ään ja todentamiseen liittyvän liikennöinnin hallinta-VLAN:iin sekä Internettiin lukuun ottamatta VLAN:ia 100, josta liikenne Internettiin oli estetty.

4 TOTEUTUSVAIHTOEHDOT

4.1 Toteutus WPA2 PSK -todennuksella

WPA2 PSK:lla toteutetussa todennuksessa käyttäjät todennetaan langattomaan verkkoon liittyessään kaikille langattoman verkon käyttäjille yhteisellä esijaetulla salasanalla, joka on 8–63 ASCII-merkkiä pitkä (Guo, Wang, Zhang & Zhang 2020, 1). Esijaetun salasanan pituus on kompromissi tietoturvallisuuden ja käytettävyyden välillä. Esimerkkinä 63 merkkiä pitkä salasana on pituutensa osalta tietoturvallinen, mutta jos sitä ei saada jaettua käyttäjille turvallisesti sähköisesti, on sen syöttäminen käsin vaativaa ja altista kirjoitusvirheille.

WPA2 PSK on laajasti tuettu erilaisissa päätelaitteissa ja se on yksinkertainen ottaa käyttöön. Sillä on nopeaa luoda langaton verkko isolle käyttäjämäärälle, koska kaikki tietyn langattoman verkon käyttäjät todennetaan samalla esijaetulla salasanalla. Saman esijaetun salasanan käytön takia yksittäistä käyttäjää ei voida helposti tunnistaa, mikä hankaloittaa esimerkiksi ongelmatilanteiden selvitystä. Jos esijaettu salasana täytyy vaihtaa käytön aikana, on tilanne ongelmallinen ylläpidon ja käyttäjien kannalta. Kaikkien käyttäjien täytyy kirjautua verkkoon uudella salasanalla vaihdon jälkeen. Ylläpidolle aiheutuu lisätyötä salasanan vaihdosta ja vaihdosta johtuvien ongelmatilanteiden ratkaisemisesta.

Käyttäjäryhmät voidaan erottaa toisistaan jakamalla käyttäjäryhmät eri langattomiin verkkoihin. Silloin jokaista käyttäjäryhmää varten täytyy luoda oma langaton verkko, jota tukiasema kaiuttaa. Yksittäinen tukiasema voi kaiuttaa vain rajallista määrää langattomia verkkoja. Suunnittelussa tulisi pyrkiä ratkaisuun, jossa saadaan muodostettua mahdollisimman isoja käyttäjäryhmiä, koska näin voidaan minimoida kunkin tukiaseman kaiuttamien langattomien verkkojen määrä. Tilanne voidaan ratkaista myös lisäämällä tukiasemien lukumäärää, mikäli tukiasemat saadaan sijoitettua siten, että ne häiritsevät toisiaan mahdollisimman vähän (Ergin, Ramachandran & Gruteser 2007, 353).

Parhaiten toteutus WPA2 PSK -todennuksella sopii tilanteisiin, joissa isolle käyttäjämäärälle tarvitaan langaton verkko, jossa on laaja päätelaitetuki ja jossa yksittäistä käyttäjää ei ole tarve tunnistaa. Esimerkkinä on tiettyä tapahtumaa varten luotu langaton verkko. Toinen soveltuva tilanne on esimerkiksi tulostimille,

verkkokiintolevyillä tai IoT-laitteille tarkoitettu verkko, koska tällaiset laitteet tukevat vain joitakin todennusvaihtoehtoja. Niitä peruskäyttäjät eivät konfiguroi, ja tästä syystä esijaettu salasana on vain ylläpidon tiedossa.

4.2 Toteutus WPA2 PSK -todennuksella, jossa vierasportaali

Toteutuksessa WPA2 PSK -todennuksella, jossa vierasportaali käyttäjät todennetaan esijaetulla salasanalla langattomaan verkkoon liittyessään ja he saavat vain hyvin rajatun yhteyden. Seuraavaksi heidät ohjataan vierasportaaliin, jossa käyttäjät tunnistautuvat henkilökohtaisilla käyttäjätunnuksilla. Vierasportaalissa suoritetun onnistuneen tunnistuksen jälkeen sallitaan käyttäjille pääsy verkkoon. (Godber & Dasgupta 2002, 42–43.) Verrattuna aiemmin kuvattuun todennukseen pelkällä esijaetulla salasanalla tämä toteutus mahdollistaa yksittäisen käyttäjän tunnistamisen, mikä helpottaa ongelmatilanteiden selvittämistä ja mahdollistaa käyttäjäkohtaisen tilastoinnin. Käyttäjän näkökulmasta tämä toteutus sisältää kaksinkertaisen kirjautumisen. Ylläpidon näkökulmasta käyttäjätunnusten luonti aiheuttaa lisätyötä verrattuna pelkkään WPA2 PSK -todennukseen, mutta toisaalta hyötynä on käyttäjäkohtainen tunnistus. Käyttäjätunnusten käytöstä aiheutuvia haittoja voidaan vähentää pidentämällä aikaa, jonka käyttäjä pidetään kirjautuneena sisään, sekä keventämällä vaatimuksia käyttäjätunnusten pituuden ja merkistön laajuuden osalta.

Parhaiten WPA2 PSK -todennus, jossa vierasportaali toteutus sopii tilanteisiin, joissa halutaan tunnistaa käyttäjät ja vähentää esijaetun salasanan mahdollista vaihtotarvetta. Mikäli esijaettu salasana päätyy halutun käyttäjäryhmän ulkopuolelle, vaaditaan verkkoon pääsyyn myös onnistunut kirjautuminen henkilökohtaisilla käyttäjätunnuksilla. Mikäli henkilökohtaiset tunnukset päätyvät jonkun muun tietoon, voidaan vanhoilla tunnuksilla kirjautuminen estää ja tehdä käyttäjälle uudet tunnukset.

4.3 Toteutus avoimella langattomalla verkolla, jossa vierasportaali

Toteutuksessa avoin langaton verkko, jossa vierasportaali käyttäjät liittyvät avoimeen langattomaan verkkoon, jolloin he saavat vain hyvin rajatun yhteyden. Seu-

raavaksi heidät ohjataan vierasportaaliin, jossa käyttäjät tunnistautuvat henkilökohtaisilla käyttäjätunnuksilla. Vierasportaalissa suoritetun onnistuneen tunnistuksen jälkeen sallitaan käyttäjille pääsy verkkoon tarvittavassa laajuudessa. (Godber & Dasgupta 2002, 42–43.) Esimerkiksi hotellit käyttävät edelleen tällaista toteutusta vieraille tarjottavassa langattomassa verkossa. Toteutuksessa avoin langaton verkko, jossa vierasportaali langattoman verkon liikenne ei ole salattua, joten liikenteen salakuuntelu on mahdollista. Salakuuntelua voi hankaloittaa käyttämällä VPN-sovellusta, joka salaa liikenteen (Sawalmeh, Malayshi, Ahmad & Awad 2021, 236). Tämä toteutus soveltuu parhaiten tilanteisiin, joissa on tarve tunnistaa käyttäjät ja rajoittaa pääsyä langattomaan verkkoon.

4.4 Toteutus WPA2 Enterprise -todennuksella

Toteutuksessa WPA2 Enterprise -todennuksella käyttäjä tunnistetaan 802.1x-todennusprosessilla, jossa käyttäjän verkkoon liittyessään syöttämät henkilökohtaiset käyttäjätunnukset tarkistetaan RADIUS-palvelimelta (Kovačić ym. 2017). Onnistuneen tunnistuksen jälkeen käyttäjän laite valtuutetaan liikennöimään verkossa (Kovačić ym. 2017) ja ohjataan käyttäjätunnusten mukaiseen VLAN:iin. DHCP-palvelin antaa käyttäjän päätelaitteelle IP-osoitteen tämän VLAN:in IP-osoiteavaruudesta.

Käyttäjien tunnistus tekee mahdolliseksi käyttäjäkohtaisen tilastoinnin mahdollisten ongelmatilanteiden varalta. Kyky ohjata käyttäjät haluttuun VLAN:iin mahdollistaa käyttäjäryhmää sekä yksittäistä käyttäjää koskevat muutokset käytön aikana. Tästä esimerkkinä on tilanne, jossa halutaan siirtää käyttäjä eri VLAN:iin tai rajoittaa tietyn käyttäjäryhmän sallittua maksimitiedonsiirtonopeutta.

802.1x-todennusprosessin käyttäjän tunnistusvaiheessa käytetään varmenteita käyttäjätunnusten sisällön salaamiseen käyttäjän laitteen ja tukiaseman välillä. Varmenteiden käytöllä voidaan tunnistaa langattoman verkon laitteita ja verkko, johon ollaan liittymässä. Näin pienennetään riskiä, että käyttäjä liittyy väärään langattomaan verkkoon. Varmenteiden käyttöönottoon liittyy haasteita, kuten itse varmenteiden asennus. Varmenteiden asennus on haastava toteuttaa käyttäjän toimin onnistuneesti ja tehdäänkin yleensä siihen tarkoitetulla ohjelmistolla. Tässä työssä ei ollut resurssien puolesta mahdollista testata ohjelmiston käyttöä

varmenteiden asennukseen. Ohjelmiston asennuksessa on myös haasteena käyttäjien halukkuus asentaa ohjelmistoja omiin laitteisiinsa vierasverkkoon pääsemiseksi. Mikäli kyseessä on yrityksen laite ja se on varustettu hallintasovelluksella tai hallintaratkaisulla, käyttäjän ei välttämättä ole mahdollista asentaa laitteelle mitään asennusoikeuksien puuttuessa.

Toteutus WPA2 Enterprise -todennuksella soveltuu parhaiten tilanteeseen, jossa halutaan tarjota langaton verkko usealle eri käyttäjäryhmälle käyttäen yhtä yhteistä SSID:tä. Tässä ratkaisussa voidaan käyttäjät erotella eri VLAN:eihin käyttäjätunnusten perusteella, ja ratkaisu mahdollistaa muutokset käytön aikana. Tässä ratkaisussa verkon rakentamisvaihe on esitetyistä vaihtoehdoista vaativin laitteiden konfigurointi huomioiden. Joten ratkaisu soveltuu parhaiten tilanteisiin, joissa järjestelmä jää toistaiseksi käyttöön asennuksen jälkeen. Tätä näkemystä tukevat vaihtoehdon laajat mahdollisuudet käytönaikaisiin muutoksiin ja joustavaan käyttäjähallintaan.

4.5 Toteutusvaihtoehtojen vertailu

Jokaiselle toteutusvaihtoehdolle on käyttötapaus, johon se parhaiten soveltuu. Kussakin toteutusvaihtoehdossa on omat vahvuutensa ja heikkoutensa. Toteutusvaihtoehtoja voidaan myös yhdistellä parhaiten tarpeet täyttäväksi kokonaisuudeksi. Voidaan esimerkiksi tarjota WPA2 Enterprise -vaihtoehdon rinnalla toisella SSID:llä WPA2 PSK -vaihtoehtoa tai kuten toteutusvaihtoehdoissa on tehtykin lisäämällä vierasportaali WPA2 PSK -todennusvaihtoehtoon.

WPA2 PSK mahdollistaa vahvan salauksen käytön, mutta esijaetun salasanan hallinta pitkäaikaisessa käytössä voi osoittautua haasteelliseksi. Lisäksi vaihtoehto ei mahdollista käyttäjien ohjausta VLAN:eihin, vaan erottelu täytyy tehdä käyttämällä jokaiselle käyttäjäryhmälle omaa SSID:tä.

Vierasportaali mahdollistaa käyttäjien tunnistamisen, mutta tuo käyttäjille yhden lisävaiheen verkkoon pääsyssä. Vierasportaali ei mahdollista käyttäjien ohjausta VLAN:eihin käyttäjätunnuksien perusteella, joten ainoaksi hyödyksi jää mahdollisuus tilastoinnin toteutukseen. Vierasportaalin käyttö saattaa aiheuttaa ongelmia, mikäli käytössä on VPN-ohjelmisto, joka estää liikennöinnin, kunnes suojattu yhteys on saatu muodostettua (Burkert, McDougall, Federrath & Fischer 2021).

Avoin langaton verkko on turvaton, koska liikenne kulkee salaamattomana langattomassa verkossa. Lisäksi vaihtoehto ei mahdollista käyttäjien ohjausta VLAN:eihin, vaan erottelu täytyy tehdä käyttämällä jokaiselle ryhmälle omaa SSID:tä.

WPA2 Enterprise mahdollistaa vahvan salauksen käytön ja monipuolisimman käyttäjien hallinnan. Lisäksi laiteresurssien käyttö on tehokasta, koska eri käyttäjäryhmät voivat käyttää samaa SSID:tä.

Loppupäätelmänä voidaan todeta, että mikään yksittäisistä toteutusvaihtoehdoista ei ole paras vaihtoehto jokaiseen käyttötapaukseen. Suunnittelua ohjaavat vaadittu tietoturvallisuuden taso ja tarvittava verkonhallinnan taso. Parhaaseen tulokseen päästään valitsemalla kuhunkin käyttötapaukseen parhaiten soveltuva vaihtoehto tai vaihtoehtojen yhdistelmä.

5 POHDINTA

Opinnäytetyön tavoitteena oli tuottaa lisätietoa ja valmiita toteutusvaihtoehtoja erilaisten vierasverkkojen toteutuksen pohjaksi. Verkkotekniikat ja verkkopalvelut -osiota kirjottaessa käytin kirjoja sekä internetistä löytyviä standardeja, e-kirjoja, artikkeleita ja blogikirjoituksia. Haastavaa oli löytää tietoa aiheista, mikä ei ollut kohdennettu vain tietyn valmistajan tuotteisiin. Aiheiden käsittelyn rajaamisessa täytyi keskittyä löytämään aiheen ymmärtämisen kannalta oleelliset asiat, koska aiheet olivat laajoja kokonaisuuksia.

Opinnäytetyötä kirjoittaessa ja eri vaihtoehtoja testiympäristössä testatessa muodostui hyvä käsitys näiden eri vaihtoehtojen ominaisuuksista, niiden käyttöönotosta ja käytöstä, niin käyttäjän kuin ylläpidon näkökulmasta. Lisäksi muodostui selkeä näkemys vaihtoehtojen soveltuvuudesta eri käyttötilanteisiin. Ennakko-odotusten vastaisesti löytyi sekä tietoturvallisia että helppokäyttöisiä ratkaisuja.

Käyttäjän näkökulmasta tavoitteita tarkasteltaessa WPA2 Enterprise -toteutus vaihtoehto on tietoturvallinen ja helppokäyttöinen. Ylläpidon näkökulmasta tarkasteltuna tämä toteutusvaihtoehto täyttää myös kaikki asetetut tavoitteet. Tietoturvallisuuden näkökulmasta katsottuna toteutusvaihtoehto käyttää vahvaa salausta liikenteen salaamiseen ja käytössä on henkilökohtaiset käyttäjätunnukset. Käyttöönoton, keskitetyn hallinnan ja konfiguroinnin näkökulmasta toteutusvaihtoehto on rakennusvaiheen jälkeen helppo ottaa käyttöön eri kokoonpanoissa. Toteutusvaihtoehto sisältää käyttäjäkohtaisen tilastoinnin sekä mahdollistaa laajat käytönaikaiset muutokset ja joustavan käyttäjien hallinnan.

Jatkokehitysideana voitaisiin toteuttaa avoimen lähdekoodin käyttöönottosovellus käyttäjien päätelaitteita varten ja tutkia käytännön vaihtoehtoja tunnusten toimitukseen käyttäjille. Lisäksi voitaisiin lisätä testiympäristöön useampi tukiasema ja tutkia mitä mahdollisuuksia useampi tukiasema toisi toteutusvaihtoehtoihin.

LÄHTEET

Agarwal, M., Biswas, S. & Nandi, S. 2017. Discrete event system framework for fault diagnosis with measurement inconsistency: case study of rogue DHCP attack. Viitattu 19.5.2022 https://ieeexplore-ieee-org.ez.lapinamk.fi/document/7833256.

Al, A. K., Pujolle, G., & Yahiya, T. A. 2016. Mobile and wireless networks. John Wiley & Sons, Incorporated.

Bazire, G. 2012a. What's a private VLAN? Viitattu 12.5.2022 https://www.orange-business.com/en/blogs/connecting-technology/security/whats-a-private-vlan.

Bazire, G. 2012b. Private VLANs: an in-depth look. Viitattu 12.5.2022 https://www.orange-business.com/en/blogs/connecting-technology/security/private-vlans-an-in-depth-look.

Bradley, M. 2021. 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a. Viitattu 4.4.2022 https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

Burkert, C., McDougall, J., Federrath, H. & Fischer, M. 2021. Analysing Leakage during VPN Establishment in Public Wi-Fi Networks. Viitattu 8.6.2022 https://doi-org.ez.lapinamk.fi/10.1109/ICC42927.2021.9500375.

Cisco 2020a. Cisco Networking Academy CCNA1. Viitattu 2.4.2022 https://www.netacad.com.

Cisco 2020b. What is a Wi-Fi or wireless network vs. a wired network? Viitattu 2.4.2022 https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html?ccid=cc001530.

Computer Networking Notes and Study Guides 2018. VLAN Basic Concepts Explained with Examples. Viitattu 20.4.2022 https://www.computernetworking-notes.com/ccna-study-guide/vlan-basic-concepts-explained-with-examples.html.

Electronics Notes 2020. IEEE 802.11ac Gigabit Wi-Fi. Viitattu 5.4.2022 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php.

Electronics Notes 2022. Wi-Fi Generation Numbering. Viitattu 5.4.2022 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/wifi-alliance-generations-designations-numbers.php.

Ergin, M., Ramachandran, K. & Gruteser, M. 2007. Understanding the effect of access point density on wireless LAN performance. Viitattu 4.6.2022 https://doi-org.ez.lapinamk.fi/10.1145/1287853.1287902.

Fisher, T. 2022. What is Wi-Fi 6? Viitattu 5.4.2022 https://www.lifewire.com/wi-fi-6-802-11-ax-4797345.

Geier, J. 2015. Designing and Deploying 802.11 Wireless Networks. 2. painos. Cisco Press.

Godber, A. & Dasgupta, P. 2002. Secure wireless gateway. Viitattu 4.6.2022 https://doi-org.ez.lapinamk.fi/10.1145/570681.570686.

Guo, J., Wang, M., Zhang, H. & Zhang, Y. 2020. A Secure Session Key Negotiation Scheme in WPA2-PSK Networks. Viitattu 22.5.2022 https://ieeexplore-ieee-org.ez.lapinamk.fi/document/9120510.

IEEE 2019. IEEE Recommended Practice for Network Communication in Electric Power Substations. Viitattu 18.5.2022 https://doi-org.ez.lapinamk.fi/10.1109/IEEESTD.2019.8894229.

Intel 2021. 802.1X Overview and EAP Types. Viitattu 9.4.2022 https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html.

ISO 1994. ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. Viitattu 2.4.2022 https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip.

Kovačić, S., Đulić, E. & Sehidic, A. 2017. Improving the Security of Access to Network Resources Using the 802.1x Standard in Wired and Wireless Environments. Viitattu 10.4.2022 https://www.researchgate.net/publication/315011118_Improving_the_Security_of_Access_to_Network_Resources_Using_the_8021x_Standard_in_Wired_and_Wireless_Environments/citations.

Lowe, D. 2010. Networking For Dummies, 9th Edition. Viitattu 2.4.2022 https://doc.lagout.org/network/Networking%20for%20Dummies%2C%209%20Ed.pdf.

Matte, C., Cunche, M., Rousseau, F. & Vanhoef M. 2016. Defeating MAC Address Randomization Through Timing Attacks. Viitattu 19.5.2022 https://doi-org.ez.lapinamk.fi/10.1145/2939918.2939930.

Mitchell, B. 2021. What Is a Wireless Access Point? Viitattu 21.4.2022 https://www.lifewire.com/wireless-access-point-816545.

Patel, R. 2017. How to Troubleshoot High Broadcast Utilization and Broadcast Storms. Viitattu 19.5.2022 https://www.auvik.com/franklyit/blog/broadcast-storms.

Petryschuk, S. 2021. Dealing with Rogue DHCP Servers. Viitattu 19.5.2022 https://www.auvik.com/franklyit/blog/rogue-dhcp-server.

Petryschuk, S. 2022. Layer 2 vs Layer 3 Network Switches: What’s the Difference? Viitattu 20.4.2022 https://www.auvik.com/franklyit/blog/layer-3-switches-layer-2.

Practical Networking 2016. Virtual Local Area Networks (VLANs). Viitattu 20.4.2022 https://www.practicalnetworking.net/stand-alone/vlans.

Puska, M. 1999. Lähiverkkojen tekniikka. Helsinki: Suomen Atk-kustannus.

Raphaely, E. 2019. WPA2-Enterprise Authentication Protocols Comparison. Viitattu 16.4.2022 https://securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison.

Router-switch Ltd. 2020. Compare difference: WLAN vs. Wi-Fi. Viitattu 18.5.2022 https://www.router-switch.com/faq/compare-difference-wlan-vs-wi-fi.html.

Sawalmeh, H., Malayshi, M., Ahmad, S. & Awad, A. 2021. VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements. Viitattu 8.6.2022 https://doi-org.ez.lapinamk.fi/10.1109/3ICT53449.2021.9581512.

Simoneau, P. 2006. The OSI Model: Understanding the Seven Layers of Computer Networks. Viitattu 2.4.2022 http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf.

Study-CCNA 2021. What is 802.1x Authentication and How it Works? Viitattu 7.4.2022 https://study-ccna.com/802-1x-authentication.

Walt, D. 2011. FreeRADIUS beginner's guide. Packt Publishing, Limited.