jamk.fi

SDN-pohjainen langattoman verkon toteutus

Roozbeh Negahban

Opinnäytetyö
Toukokuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), Tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Negahban, Roozbeh	Opinnäytetyö, AMK	Toukokuu 2017
	Sivumäärä 54	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

SDN-pohjainen langattoman verkon toteutus

Tutkinto-ohjelma

Tietotekniikan koulutusohjelma

Työn ohjaaja(t)

Mika Rantonen, Antti Häkkinen

Toimeksiantaja(t)

Cyber Trust -projekti, Jyväskylän ammattikorkeakoulu, Tuure Valo

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulun Cyber Trust -projekti, joka tutkii uusia verkkotekniikoita ja kehittää tietoturvaratkaisuja niihin. Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa SDN-pohjainen langaton verkko.

Opinnäytetyön toteutuksessa käytettiin sekä fyysisiä että virtuaalisia laitteita. Verkon fyysiset laitteet ovat Zodiac OpenFlow-kytkin ja WLAN-tukiasemat, jotka rakennettiin Raspberry Pi -tietokoneista. Virtuaalisesti toteutetut komponentit ovat SDN-kontrolleri, RADIUS-palvelin ja Pfsense. SDN-kontrollerilla hoidettiin tukiasemien hallinta OpenFlow-protokollan avulla. Käyttäjien autentikointi toteutettiin pfsenselle asennetulla RADIUS-palvelimella.

Opinnäytetyön tuloksena saatiin SDN-pohjainen langaton verkko, jossa on toimeksiantajan vaatimia ja tarvitsemia ominaisuuksia. Rakennetussa SDN-verkossa käytettiin myös roaming-ominaisuutta. Roamingilla varmistettiin, että SDN-verkon käyttäjien siirtyminen yhdestä tukiasemasta toiseen sujuu saumattomasti.

Avainsanat (asiasanat)

SDN, WLAN, OpenFlow, Ryu

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Negahban, Roozbeh	Bachelor's thesis	May 2017
		Language of publication: Finnish
	Number of pages 54	Permission for web publication: x

Title of publication

Implementation of SDN-based wireless network

Degree programme

Information Technology

Supervisor(s)

Rantonen Mika, Häkkinen Antti

Assigned by

Cyber Trust-project, JAMK University of Applied Sciences, Tuure Valo

Abstract

The bachelor's thesis was assigned by JAMK University of Applied Sciences, the Cyber Trust project which researches new network technologies and develops security solutions for them. The purpose of the thesis was to design and implement an SDN-based wireless network.

The thesis was implemented with both physical and virtual equipment. The physical devices of the network are Zodiac OpenFlow switch and WLAN access points built using Raspberry Pi computers. The virtually implemented components are SDN controller, RADIUS server and Pfsense. The access point management was handled by SDN-controller with OpenFlow protocol. The authentication of the network users was implemented by RADIUS server installed on Pfsense.

As a result of the thesis, an SDN-based wireless network was built with the features required by the client. Roaming feature is also implemented to the designed SDN-network. The roaming feature allows the users to switch between access points as seamlessly as possible.

Keywords/tags (subjects)

SDN, WLAN, OpenFlow, Ryu

Miscellaneous

Sisältö

Kuviot

Taulukot

Lyhenteet

API	Application Programming Interface
BSS	Basic Service Set
CLI	Comand-line Interface
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
IBSS	Independent Basic Service Set
MIMO	Multiple-Input and Multiple-Output
OFDM	Orthogonal Frequency Division Multiplexing
ONF	Open Networking Foundation
OVSDB	Open Virtual Switch Database
PMK	Pairwise Master Key
SDN	Software Defined Networking
SSID	Service Set Identifier
WLAN	Wireless Local Area Network

1 Työn lähtökohdat

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Cyber Trust -projekti. Tekesin rahoittama DIMECC:n Cyber Trust -projekti on suunniteltu nelivuotiseksi ohjelmaksi, johon Jyväskylän ammattikorkeakoulun IT-instituutti on osallistunut alusta lähtien. Cyber Trust -projektissa on mukana yhteensä 30 yritystä ja tutkimuslaitosta kuten Elisa, Nokia, F-Secure, Bittium ja Oulun yliopisto.

Cyber Trust -projektin tavoitteena on vastata Suomen tutkimuksen ja teollisuuden tietoturvatarpeisiin luomalla pohja siihen. Projekti pyrkii parantamaan digitaalisen infrastruktuurin yksityisyyden ja luottamuksen, seuraamalla ja analysoimalla liikennettä ja tapahtumia uusissa tekniikoissa. Tämä tavoite saavutetaan kehittämällä ja ylläpitämällä kyberturvallisuuspalveluita yhdessä huippuasiantuntijoiden sekä yrityksien kanssa. (DIMECC Cyber Trust Program n.d.)

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa SDN-pohjainen langaton verkko JAMK:n IT-instituutille. Työn teoriaosuudessa käsitellään SDN-verkkotekniikan perusteet, arkkitehtuuria ja protokollat. Teoriaosuudessa käydään läpi myös langattoman lähiverkon perusteet, standardit ja suunnittelussa huomioon otettavat seikat.

Opinnäytetyön käytännön osuudessa suunniteltiin SDN-pohjainen langaton verkko ja toteutettiin se. Langattomassa verkossa käytettiin sekä fyysisiä että virtuaalisia laitteita. Verkon WLAN-tukiasemat rakennettiin Raspberry Pi -piirilevytietokoneista ja niiden konfigurointi hoidettiin avoimen lähdekoodin käyttöjärjestelmällä. SDN-kontrollerina käytettiin sekä Ryu että Puikkari ja SDN-verkon käyttäjien autentikointi hoidettiin RADIUS-palvelimella. SDN-verkossa käytettiin myös roaming-ominaisuutta, jolla varmistettiin käyttäjien saumattoman siirtymisen yhdestä tukiasemasta toiseen.

2 Software Defined Networking

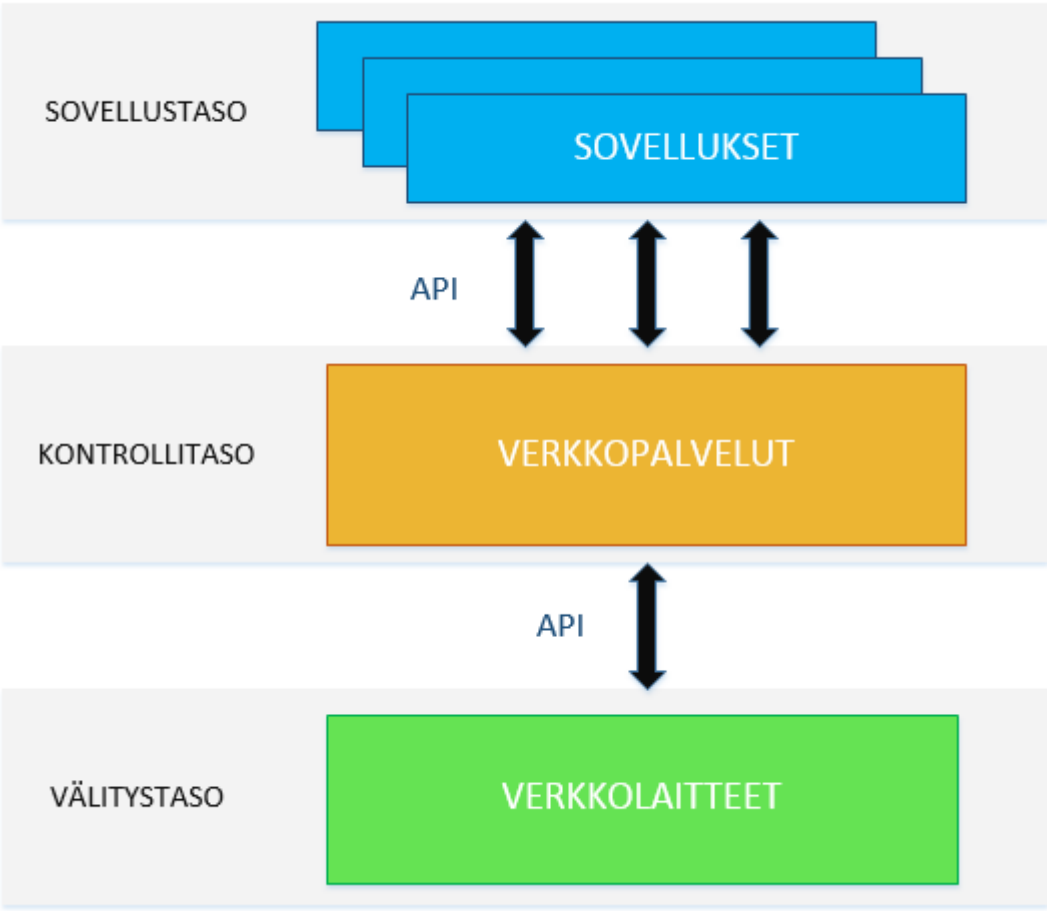
2.1 Yleistä

SDN eli Software Defined Networking on tekniikka, jonka tarkoituksena on yksinkertaistaa verkon rakennetta. SDN-verkossa kontrollitaso ja välitystaso on erotettu toisistaan ja verkkolaitteiden ohjaus hoidetaan keskitetysti ohjelmiston avulla. SDN-tekniikan ansiosta verkon joustavuus ja skaalattavuus paranee huomattavasti. SDN-verkossa verkkolaitteiden hallinta on valmistajasta riippumaton ja tapahtuu keskitetysti, joten ei tarvitse konfiguroida jokaista verkkolaitetta erikseen. (What is Software Defined Networking? n.d.)

SDN-tekniikan kehityksestä vastaa ONF eli Open Networking Foundation, joka on täysin voittoa tavoittelematon käyttäjälähtöinen organisaatio. ONF koostuu yli 100 jäsenyrityksestä, kuten Microsoft, Google, Intel, IBM ja Cisco. ONF:n tunnetuin ja eniten käytetty protokolla on OpenFlow, joka mahdollistaa verkkolaitteiden ja SDN-kontrollerin välisen kommunikoinnin. (ONF Overview n.d.)

2.2 Arkkitehtuuri

SDN-arkkitehtuuri koostuu kolmesta tasosta, jotka ovat sovellustaso, kontrollitaso ja välitystaso. APIs eli Application programming interfaces ovat SDN-verkon ohjelmointirajapintoja, joiden avulla eri tasot keskustelevat keskenään. Sovellustason sovellusten ja palveluiden avulla määritellään verkon käyttäytymistä. Kontrollitasolla päätetään, kuinka käsitellään vastaanotetut paketit, niiden sisällön perusteella. Välitystasolla hoidetaan pakettien välitys kontrollitasolla kerättyjen tietojen avulla. SDN-verkon arkkitehtuuri on esitetty kuviossa 1. (Understanding the SDN Architecture n.d.)

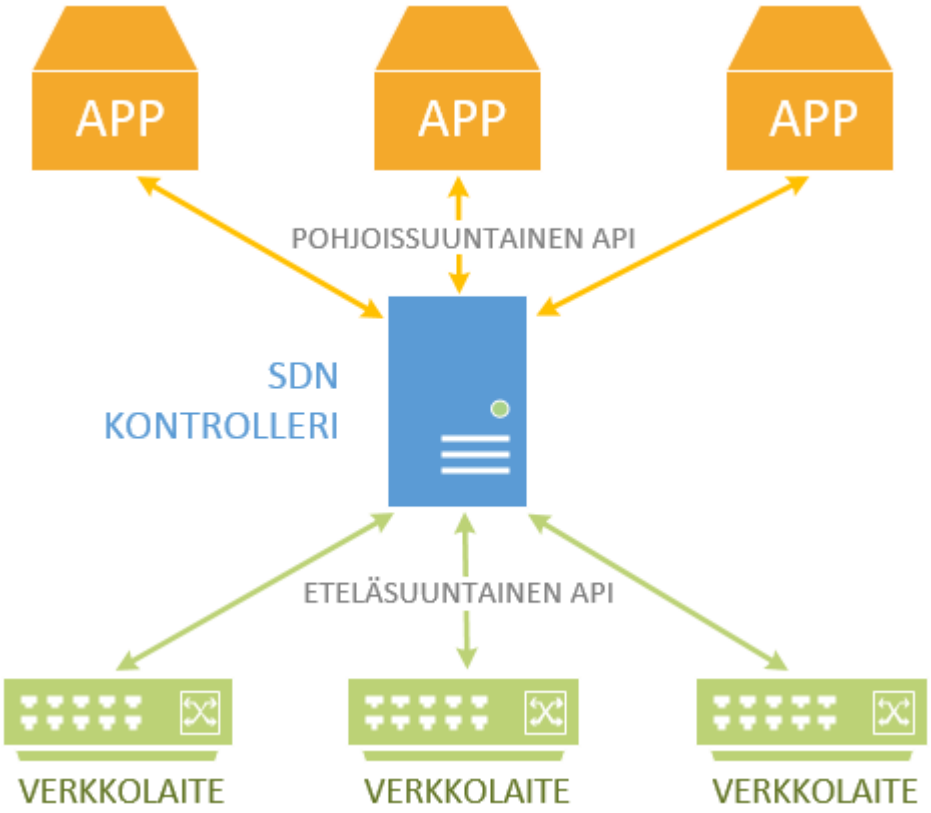


Kuvio 1. SDN-verkon arkkitehtuuri

Perinteisessä verkossa jokaisella verkkolaitteella on sekä kontrollitaso että välitystaso. Tästä johtuen useiden eri protokollien liikenne läpäisee yhdestä rajapinnasta, joka hidastaa liikennettä ja aiheuttaa sen monimutkaisuuden. SDN-verkossa kontrollitaso on eritelty välitystasosta ja sen ansiosta verkkolaitteiden hallinta hoidetaan keskitetysti yhdestä paikasta ohjelmiston avulla. Ohjelmallisesti hallittu SDN-verkossa muutosten teko on nopea, koska jokaisen laitteen asetuksiin ei tarvitse tehdä erikseen muutoksia. (Ihanainen 2016, 8-9.)

2.3 SDN-kontrolleri

SDN-kontrolleri on strateginen ohjauspiste SDN-verkossa. Sen avulla hoidetaan tiedon välitys verkkolaitteiden ja sovellusten välillä. SDN-kontrolleri kommunikoi sovellustason sovelluksilla ja palveluilla Northbound API eli pohjoissuuntaisen ohjelmointirajapinnan kautta. Välitystasolla olevien verkkolaitteiden hallinta tapahtuu Southbound API eli eteläsuuntaisen ohjelmointirajapinnan kautta. SDN-kontrollerin yhteys muihin tasoihin ohjelmointirajapintojen kautta on esitetty kuviossa 2. (What are SDN Controllers? n.d.)



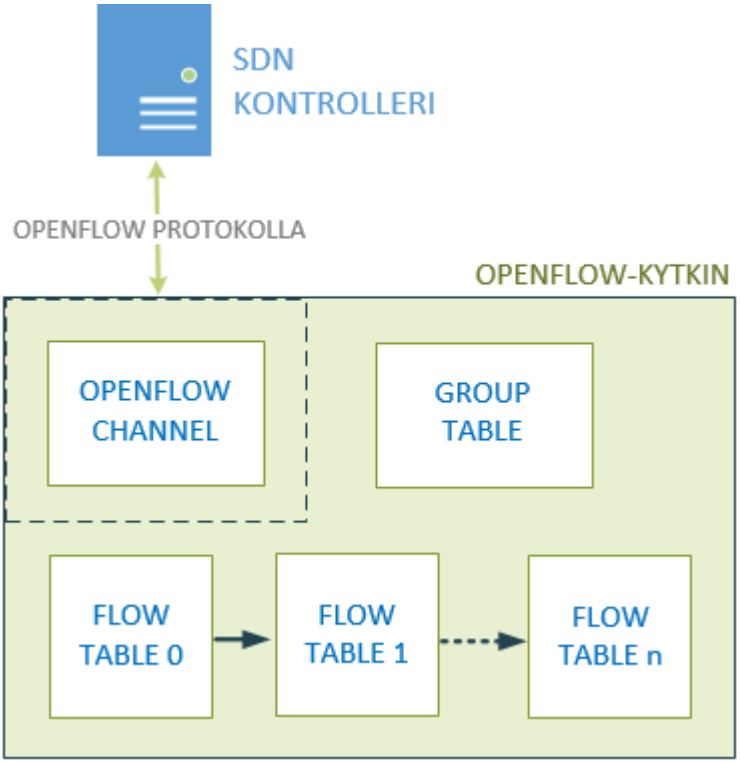
Kuvio 2. SDN-kontrollerin ja ohjelmointirajapintojen välinen yhteys

SDN-kontrolleri sisältää moduuleita, joiden avulla suorittaa verkon erilaiset tehtävät. Moduulien perustehtäviin kuuluvat verkon laitteiden kartoitus ja statistiikan keräys. Verkon toiminnallisuutta voidaan parantaa milloin vain lisäämällä uusia moduuleita SDN-kontrollerille. OpenFlow ja OVSDB ovat kaksi tunnetuinta protokollaa, joiden avulla SDN-kontrolleri kommunikoi verkkolaitteiden kanssa. (What are SDN Controllers? n.d.)

2.4 OpenFlow

OpenFlow on yleisin SDN-verkossa käytetty protokolla, joka mahdollistaa kontrollerin ja välitystasolla olevien verkkolaitteiden kommunikoinnin eteläsuuntaisella ohjelmointirajapinnalla. OpenFlow'n ansiosta verkkolaitteiden hallinta ja konfigurointi onnistuu kontrollerilla. OpenFlow-protokollaa on mahdollista käyttää täysin SDN-verkkoa varten suunniteltujen OF-kytkinten lisäksi OpenFlow-tuella varustetuilla kytkimillä, jotka toimivat myös perinteisissä tietoverkoissa. (What is OpenFlow? n.d.)

OpenFlow-kytkin koostuu vuotauluista, ryhmätaulusta ja salatusta kanavasta, jonka avulla kommunikoi turvallisesti kontrollerin kanssa. Kanavien määrä vaihtelee käytössä olevien kontrollerien mukaan. Vuotaulussa olevien tietojen perusteella hoidetaan pakettien välitys välitystasolla. Vuotaulu voi ohjata vuon ryhmätaululle, joka käsittelee vuot toimintalistojen perusteella. Kuviossa 3 on esitetty OpenFlow-kytkimen rakenne. (OpenFlow Switch Specification 2014, 11.)



Kuvio 3. OpenFlow-kytkimen rakenne

Flow eli vuo muodostuu paketin kulkemasta reitistä yhdestä verkkolaitteesta toiselle. Vuotaulussa löytyvät polkutiedot ja pakettien välitykseen liittyvät säännöt siihen tallennettujen vuomerkintöjen ansiosta. OpenFlow'n avulla SDN-kontrolleri pystyy hallitsemaan vuot manipuloimalla vuotaulussa olevat vuomerkinnät. Taulukossa 1 on esitetty seitsemästä kentästä koostuva vuomerkinnän rakenne.

Taulukko 1. Vuomerkinnän rakenne

MATCH FIELDS	PRIORITY	COUNTERS	INSTRUCTIONS	TIMEOUTS	COOKIE	FLAGS

Pakettien käsittelyn kannalta Match Fields ja Instructions ovat tärkeimmät kentät vuotaulussa. Sisään tulevien pakettien vertailu hoidetaan Match Fields-kentän määrittämien parametrien avulla. Parametrit ovat otsikkotietoja, kuten IP-osoite, MAC-osoite ja sisääntuloportti. Mikäli pakettia vastaava parametri löytyy vuotaulusta, suoritetaan Instructions-kentän mukaiset toiminnot. Instructions-kentällä löytyy tietoa, mitä vastaanotetulla paketilla tehdään, kuten uudelleen ohjaus ja muokkaus. Jos pakettia vastaavaa vuomerkintää ei löydy, kytkimen konfiguraation perusteella pakettia ohjataan toiselle vuotaululle käsiteltäväksi, pudotetaan tai lähetetään kontrollerille takaisin. (OpenFlow Switch Specification 2014, 22.)

3 Langaton lähiverkko

3.1 Yleistä

WLAN eli Wireless Local Area Network on langaton verkkotekniikka, jonka avulla voidaan yhdistää langattomasti verkkolaitteita toisiinsa. Langattoman verkon laitteet ovat langattomat tukiasemat ja päätelaitteet. Tukiasemien ja päätelaitteiden välinen kommunikointi tapahtuu radioaallolla. Radioaaltojen käyttämät taajuusalueet ovat 2,4 GHz tai 5 GHz. (Moisio 2015, 9.)

Euroopassa 2,4 GHz:n taajuusalueella käytössä olevien kanavien määrä on 13 ja 5 GHz:n taajuusalueella on 19 kanavaa. Langattomassa verkossa lähetyksen laatuun vaikuttavat seikat ovat laitteiden välinen matka, käytetty standardi ja ympäristöllä olevat esteet. Ympäristöllä olevat rakenteet saattavat heikentää tai vahvistaa signaalin voimakkuuden. (Moisio 2015, 9-10.)

3.2 Modulointitekniikat

Modulointitekniikat mahdollistavat datan lisäämisen lähetyksiin muokkaamalla alkuperäisen taajuuden aaltomuotoa. Muokkaus hoidetaan vaihtamalla aaltomuodon taajuuden, huippuarvon tai signaalin vaiheen. Yleisimmin käytetyt modulointitekniikat IEEE 802.11 -sarjan standardien kanssa ovat FHSS, DSSS ja OFDM.

FHSS eli Frequency Hopping Spread Spectrum on taajuushyppelytekniikka, jossa hyödynnetään kaikki käytössä olevat vapaat kanavat datan lähettämiseen ja vastaanottamiseen. Tekniikassa lähettäjä vaihtaa nopeasti kanavia näennäissatunnaisesti tiedonsiirtoon osallistuville jaetun avaimen perusteella. Taajuushyppely toteutetaan joko hitaalla hyppelyllä, jossa yhdellä aikavälillä lähetetään useita bittejä tai nopealla hyppelyllä, jossa lähetetään yksi bitti usealla aikavälillä. (What is FHSS? n.d.)

DSSS eli Direct Sequence Spread Spectrum on suorasekventointitekniikka, jossa pieniin osiin jaettu data lähetetään koko kanavan taajuusalueella yhtenä signaalina. Jokaisen datasignaalin rinnalla lähetetään myös suuremmalla nopeudella kohinaa, jonka ansiosta samalla kanavalla lähetetyt eri lähetykset eivät häiritsee toisiaan. DSSS

on vastustuskykyisempi häiriöitä vastaan verrattuna FHSS-tekniikkaan. (DSSS - Direct Sequence Spread Spectrum n.d.)

OFDM eli Orthogonal Frequency Division Multiplexing on monikaistatekniikka, jossa data jaetaan ensin useiksi signaaleiksi, minkä jälkeen lähetetään yhtäaikaisesti eri taajuuskanavilla rinnakkain. OFDM:n kanssa käytetään yleensä MIMO-tekniikka tiedonsiirron luotettavuuden parantamiseksi. MIMO eli Multiple-Input and Multiple-Output -tekniikka mahdollistaa tiedon lähetyksen ja vastaanoton samanaikaisesti useammalla antennilla. (Introduction to OFDM 2011.)

3.3 Standardit

Langattomassa lähiverkossa käytetään IEEE 802.11 -sarjan standardeja, jotka määrittävät verkon ominaisuudet. IEEE 802.11 -sarjan keskeisimmät standardit ja niiden ominaisuudet on esitetty taulukossa 2. Ensimmäinen WLAN-standardi on IEEE 802.11, joka toimii 2,4 GHz:n taajuusalueella ja sen tiedonsiirtonopeus on 1 - 2 Mbit/s. Tämän standardin mukaan käytetyt tiedonsiirtomenetelmät ovat DSSS ja FHSS. (Salonen 2016, 7.)

Taulukko 2. IEEE 802.11 -sarjan keskeisimmät standardit

STANDARDI	JULKAISU	TAAJUUSALUE	MODULAATIO	MAX SIIRTONOPEUS
802.11	1997	2,4 GHz	DSSS, FHSS	1 - 2 Mbit/s
802.11a	1999	5,0 GHz	OFDM	54 Mbit/s
802.11b	1999	2,4 GHz	DSSS	11 Mbit/s
802.11g	2003	2,4 GHz	OFDM	54 Mbit/s
802.11n	2009	2,4 ja 5,0 GHz	MIMO-OFDM	600 Mbit/s
802.11ac	2013	5,0 GHz	MIMO-OFDM	866 Mbit/s

Vuonna 1999 IEEE julkaisi uuden 802.11b -standardin, jonka maksimisiirtonopeus on 11 Mbit/s. IEEE 802.11b -standardi toimii 2,4 GHz:n taajuusalueella ja tiedonsiirrossa

hyödyntää DSSS-tekniikkaa. IEEE julkaisi samana vuonna myös 802.11a - standardin, joka toimii 5 GHz:n taajuusalueella ja tarjoaa jopa 54 Mbit/s tiedonsiirtonopeutta. 802.11a-standardi käyttää OFDM-tekniikkaa tiedonsiirrossa. (The 802.11 family explained n.d.)

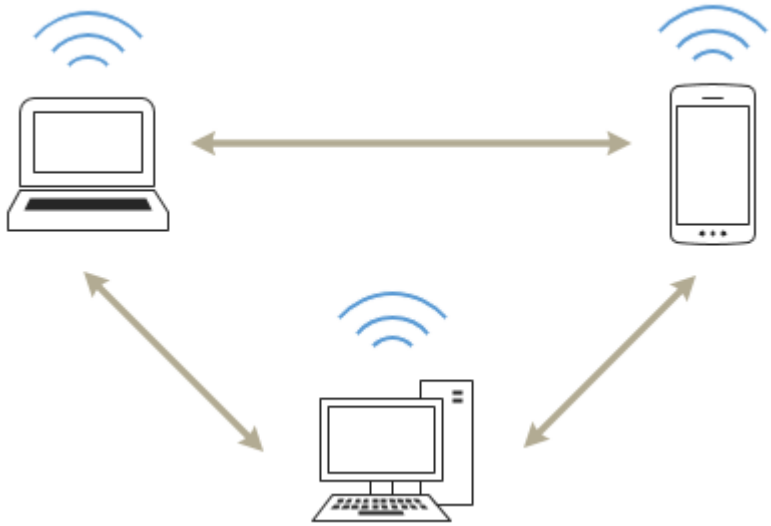
Vuonna 2003 julkaistiin 802.11g-standardi, joka oli kehitetty nostamaan suosittu 802.11b-standardilla toteutetut verkkojen tiedonsiirtonopeudet. IEEE 802.11g-standardi mahdollistaa 54 Mbit/s tiedonsiirtonopeuden, toimii 2,4 GHz:n taajuusalueella ja hyödyntää OFDM-tekniikkaa tiedonsiirtoa varten. (The 802.11 family explained n.d.)

IEEE julkaisi 802.11n-standardin vuonna 2009. Se toimii sekä 2,4 GHz:n että 5 GHz:n taajuusalueella ja tukee MIMO-tekniikkaa. 802.11n-standardi tarjoaa teoreettisesti 600 Mbit/s tiedonsiirtonopeutta MIMO-tekniikan ansiosta, mikä mahdollistaa useamman antennin käytön signaalin lähetyksessä ja vastaanotossa. 802.11n on myös yhteensopiva a-, b- ja g-standardien kanssa. (The 802.11 family explained n.d.)

Vuonna 2013 julkaistu 802.11ac-standardi toimii ainoastaan 5 GHz:n taajuusalueella. 802.11ac-standardi tukee 20 MHz:n ja 40 MHz:n kaistanleveyksien lisäksi 80 ja 160 MHz:n kaistanleveyksiä. 802.11ac-standardi tarjoaa jopa 866 Mbit/s tiedonsiirtonopeutta 160 MHz:n kaistanleveydellä. 802.11ac tukee Multi-User MIMO-tekniikkaa, mikä mahdollistaa käyttämään enemmän antenneja verrattuna 802.11n-standardilla käytössä olevaan MIMO-tekniikkaan. (Salonen 2016, 10.)

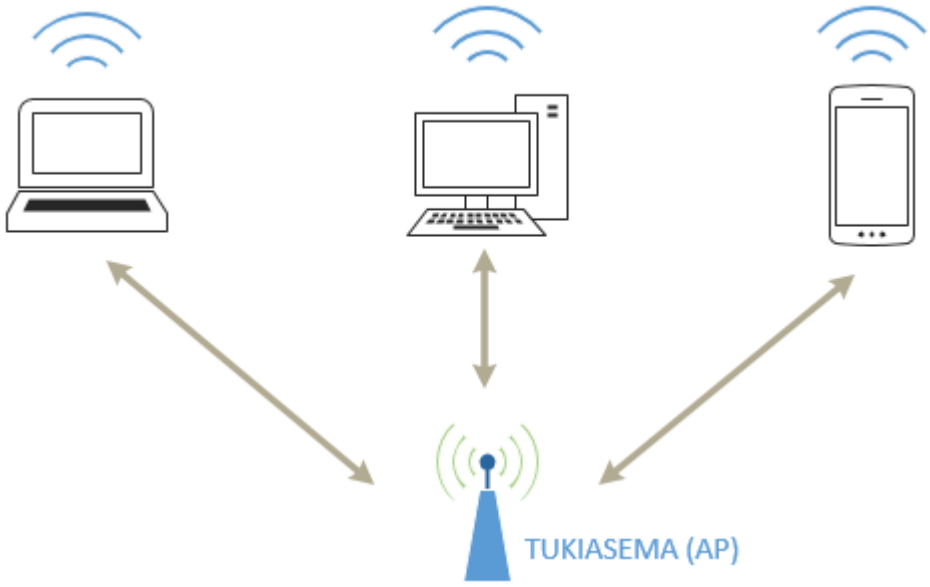
3.4 Topologiat

Langattoman verkon topologian toteutuksessa on käytössä eri toteutustapoja, joiden perusteella verkon laitteet kytkeytyvät toisiinsa. Ensimmäinen toteutustapa on IBSS eli Independent Basic Service Set, jossa eri laitteet kommunikoivat suoraan toistensa kanssa ja muodostavat yhteyden ilman tukiasemaa. IBSS on yksinkertainen tilapäisverkko, joka kutsutaan yleensä Ad-hoc-verkoksi. Kuviossa 4 on esitetty IBSS-topologia. (WLAN topologies 2014.)



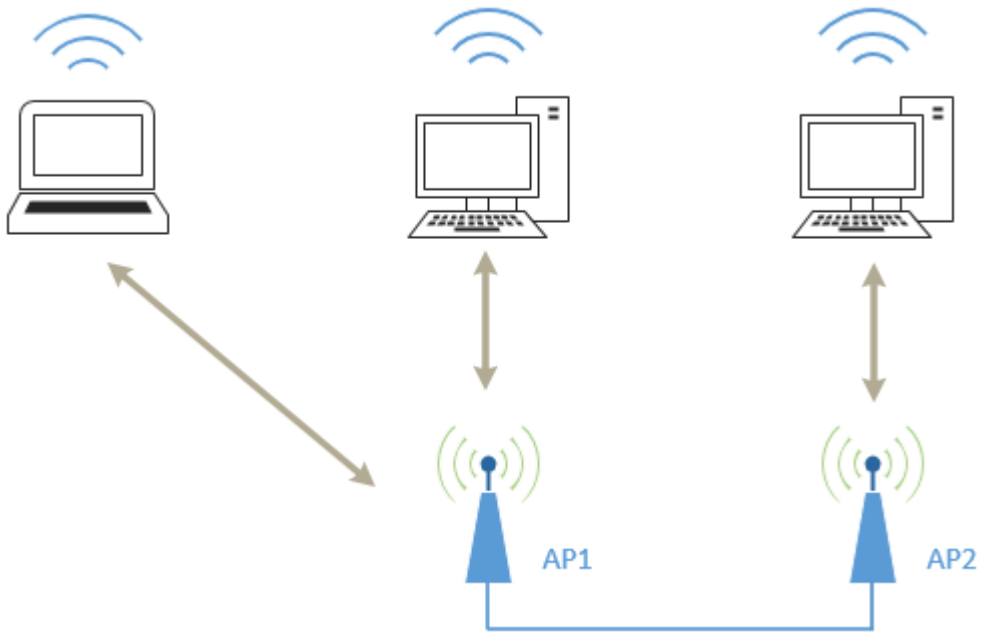
Kuvio 4. IBSS-topologia

BSS eli Basic Service Set on perusarkkitehtuuri, jossa verkon laitteet keskustelevat keskenään tukiaseman kautta. Tukiasema mahdollistaa myös laitteiden liittymisen Ethernet-verkkoon. BSS-topologia on yleisin toteutustapa pienyritys- ja kotiverkoissa. Kuviossa 5 on esitetty BSS-verkon rakenne. (WLAN topologies 2014.)



Kuvio 5. BSS-topologia

Kolmas toteutustapa on ESS eli Extended Service Set, joka on BSS-verkon laajennettu versio. ESS-verkko koostuu useammasta tukiasemasta, jotka on kytketty samaan runkoverkkoon. ESS on hyvin suosittu menetelmä isoissa rakennuksissa, minkä ansiosta käyttäjät nauttivat langattomasta verkosta koko rakennuksessa huomaamatta tukiaseman vaihdosta. ESS-topologia on esitetty kuviossa 6. (WLAN topologies 2014.)



Kuvio 6. ESS-topologia

4 Langattoman verkon suunnittelu

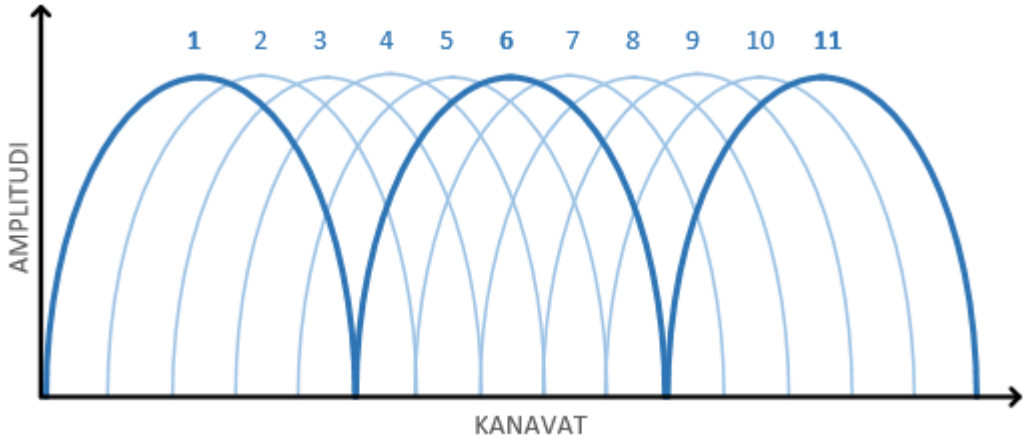
4.1 Signaalin eteneminen ja häiriöt

Langattoman verkon suunnittelussa kannattaa ottaa huomioon signaalin etenemisen vaikeuttavat seikat kuten heijastuminen ja vaimeneminen. Amplitudin heikkeneminen eli vaimennus tapahtuu signaalin etenemisen aikana väliaineessa. Signaalin amplitudin heikkenemiseen vaikuttavat lähetyksen taajuus, etäisyys ja teho. Huonekalut ja fyysiset esteet kuten seinät, ovet ja ikkunat ovat myös ongelman aiheuttajia langattoman verkon kuuluvuuden kannalta. (Kaksonen 2014, 27.)

Samalla taajuusalueella toimivat laitteet voivat aiheuttaa erilaisia häiriöitä langattoman verkon toiminnalle. Bluetooth-laitteet, mikroaaltouunit ja älypuhelimet aiheuttavat häiriöitä 2,4 GHz:n taajuusalueella. Kyseiset häiriöt vaikuttavat negatiivisesti tiedonsiirtonopeuteen aiheuttamalla bittivirheitä, jotka joudutaan korjamaan uudelleenlähetyksillä. (Kaksonen 2014, 30.)

4.2 Kanavasuunnittelu

Keskeisimmät laitteet langattomassa lähiverkossa ovat tukiasemat. Tukiasemien kanavasuunnittelu kannattaa tehdä erittäin tarkasti, jotta saadaan hyvin toimiva langaton verkko. Huolellisesti tehdyllä kanavasuunnittelulla vältetään kanavien päällekkäisyysriskit samalla taajuusalueella toimivien tukiasemien kannalta. Kanavien päällekkäisyys heikentää langattoman verkon suorituskykyä aiheuttamalla häiriösignaaleja. 2,4 GHz:n taajuusalueella toimivien tukiasemien käytössä on ainoastaan kolme ei-päällekkäistä kanavaa. 2,4 GHz taajuusalueen ei-päällekkäiset kanavat ovat 1, 6 ja 11, jotka on esitetty kuviossa 7. Kanavien määrä 5 GHz:n taajuusalueella on huomattavasti enemmän, joten kanavasuunnittelu on suhteellisesti helpompaa käytössä olevien ei-päällekkäisten kanavien runsauden ansiosta. (Channel Planning Best Practices n.d.)

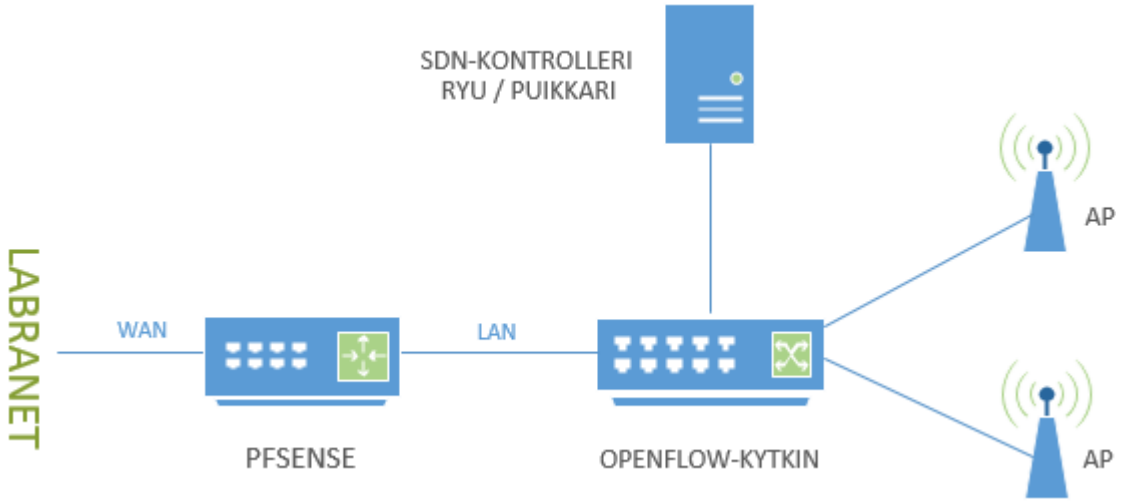


Kuvio 7. 2,4 GHz:n taajuusalueen ei-päällekkäiset kanavat

5 Käytännön toteutus

5.1 Suunnitelma

Langattoman SDN-verkon suunnittelussa käytetään sekä fyysisiä että virtuaalisia laitteita. Verkon fyysiset laitteet ovat Zodiac OpenFlow-kytkin ja WLAN-tukiasemat, jotka rakennetaan Raspberry Pi -piirilevytietokoneista. Virtuaalisesti toteutetut komponentit ovat SDN-kontrolleri, RADIUS-palvelin ja Pfsense. Verkon looginen topologia on esitetty kuviossa 8.

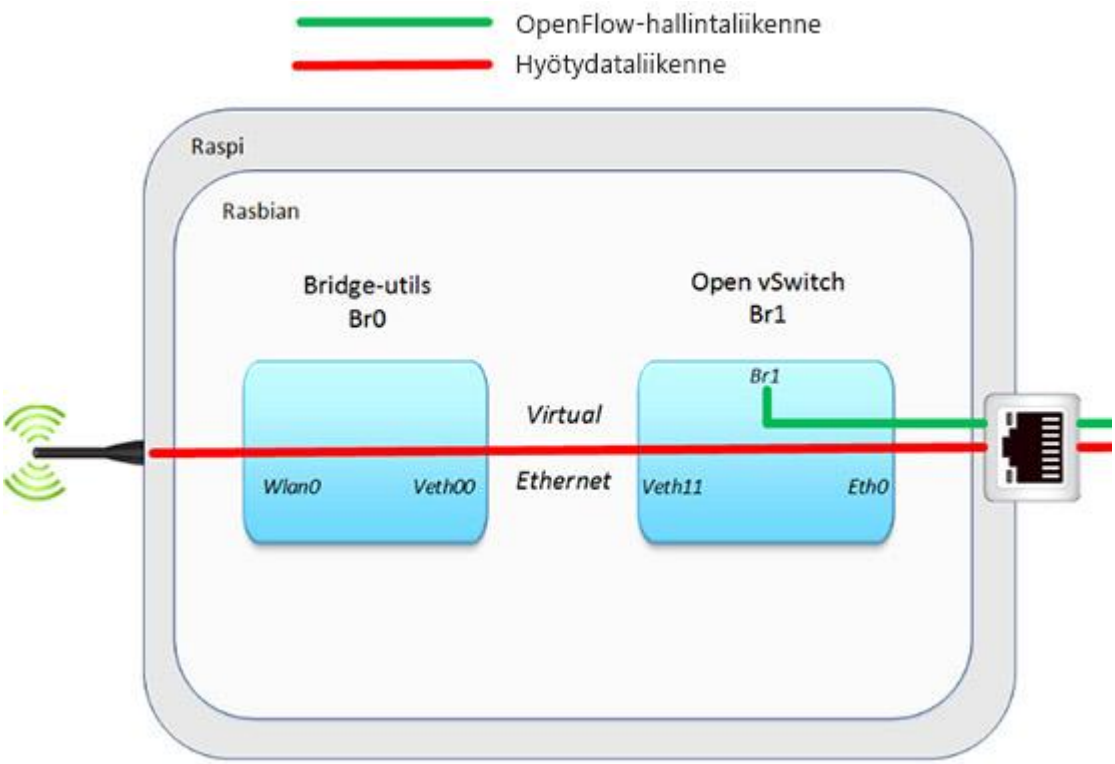


Kuvio 8. SDN-verkon looginen topologia

Pfsense on palomuuriohjelmisto, joka hoitaa myös verkon reititykset. Pfsensen LAN-puolen rajapinta on kaapeloitu OF-kytkimeen ja WAN-rajapinta on kytketty LabraNet-tiin, jonka kautta yhteyden muodostaminen ulkoverkkoon onnistuu. Pfsensellä on myös sisäänrakennettu Captive portal -ratkaisu, jonka ansiosta voidaan ohjata käyttäjät ensin halutulle laskeutumissivulle. Laskeutumissivulla kerrotaan langattoman SDN-verkon käyttöehdot, ja hyväksymällä ehdot käyttäjät voivat kirjautua sisään palveluun. Käyttäjien autentikointi hoidetaan pfsenselle asennetulla RADIUS-palvelimella.

Raspberry Pi -tietokoneille asennetaan ensin Raspbian käyttöjärjestelmä ja sen jälkeen virtuaalikytkimet Open vSwitch ja Bridge-utils -ohjelmilla. Open vSwitchillä

tehdään virtuaalikytkin nimellä Br1 ja siihen liitetään rajapinta eth0, jonka avulla voidaan tuoda OpenFlow-protokolla Raspberry Pi:lle. Bridge-utilsin avulla tehdään toinen virtuaalikytkin nimellä Br0 ja siihen liitetään rajapinta wlan0 siltaavassa tilassa. Eth0 ja wlan0 ovat Raspin fyysiset rajapinnat. Virtuaalikytkinten välinen yhteys muodostetaan virtuaalisilla rajapinnoilla veth00 ja veth11. Virtuaalikytkinten looginen topologia on esitetty kuviossa 9. Lopuksi Raspille asennetaan Hostapd-ohjelma, jonka avulla voidaan toteuttaa tukiasemat.



Kuvio 9. Virtuaalikytkinten looginen topologia (Ihanainen 2016, 34)

Työssä käytetty Zodiac FX on Northbound Networksin kehittämä neliporttinen OpenFlow-kytkin, joista kolme ensimmäistä porttia ovat OpenFlow-portteja ja neljäs on kontrollerille tarkoitettu portti. OF-kytkimen nelosportille kytketyllä SDN-kontrollerilla hoidetaan tukiasemien hallinta OpenFlow-protokollan avulla. Työssä käytetään SDN-kontrollerina ensin virtuaalisesti toteutettu RYU-kontrolleri, ja kun kaikki on saatu toimimaan sen kanssa, asennetaan sen tilalle Puikkari. Puikkari on Cyber Trust -projektin kehittämä käyttöliittymä SDN-verkon visualisointiin ja hallintaan.

5.2 Tukiasemien asennus

Tukiaseman asennus aloitettiin kirjoittamalla Internetistä ladatun NOOBS-käyttöjärjestelmäasentajan Raspin MicroSD-kortille. NOOBS tarjoaa laajan valikoiman eri käyttöjärjestelmistä, joiden joukosta voidaan valita sopiva. Käyttöjärjestelmien joukosta valittiin Raspbian-käyttöjärjestelmä asennettavaksi Raspille, joka on hyvin suosittu ja eniten käytetty käyttöjärjestelmä Raspberry Pi:llä. Käyttöjärjestelmän asennuksen jälkeen aloitettiin asentamaan Raspille ohjelmat suunnitelman mukaisesti. Ensimmäisenä asennettiin Open vSwitch-ohjelma käyttämällä seuraavia komentoja:

```
root@SDN-AP1:/home/pi# apt-get update

root@SDN-AP1:/home/pi# apt-get install -y autoconf libtool openssl
pkg-config make gcc libssl-dev

root@SDN-AP1:/home/pi# git clone
git://git.kernel.org/pub/scm/devel/sparse/sparse.git

root@SDN-AP1:/home/pi# cd sparse

root@SDN-AP1:/home/pi/sparse# make

root@SDN-AP1:/home/pi/sparse# make install

root@SDN-AP1:/home/pi/sparse# cd ..

root@SDN-AP1:/home/pi# git clone
https://github.com/openvswitch/ovs.git

root@SDN-AP1:/home/pi# cd ovs

root@SDN-AP1:/home/pi/ovs# apt-get install dh-autoreconf

root@SDN-AP1:/home/pi/ovs# ./boot.sh

root@SDN-AP1:/home/pi/ovs# ./configure --prefix=/usr --
localstatedir=/var --sysconfdir=/etc
```

```
root@SDN-AP1:/home/pi/ovs# make -j3

root@SDN-AP1:/home/pi/ovs# make install

root@SDN-AP1:/home/pi/ovs# cp debian/openvswitch-switch.init
/etc/init.d/openvswitch-switch
```

Asennuksen jälkeen Open vSwitch voidaan käynnistää seuraavalla komennolla:

```
root@SDN-AP1:~# /etc/init.d/openvswitch-switch start
```

Open vSwitchin käynnistyksen jälkeen ohjelma luo automaattisesti tyhjän tietokannan, johon tallennetaan Open vSwitchin konfiguraatiot. Kuviosta 10 voidaan todeta, että Open vSwitch on käynnistynyt onnistuneesti ja luonut uuden tietokannan.

```
root@SDN-AP1:~# /etc/init.d/openvswitch-switch start
 * Inserting openvswitch module
 * /etc/openvswitch/conf.db does not exist
 * Creating empty database /etc/openvswitch/conf.db
 * Starting ovsdb-server
 * Configuring Open vSwitch system IDs
 * Starting ovs-vswitchd
 * Enabling remote OVSDB managers
root@SDN-AP1:~# /etc/init.d/openvswitch-switch status
ovsdb-server is running with pid 1402
ovs-vswitchd is running with pid 1413
```

Kuvio 10. Open vSwitchin käynnistys

Open vSwitchin asennuksen jälkeen voidaan aloittaa konfiguroimaan ensimmäinen virtuaalikytkin. Konfigurointi aloitettiin luomalla virtuaaliset rajapinnat ja niiden välinen linkki. Seuraavaksi tehtiin uusi virtuaalikytkin nimellä br1, johon voidaan lisätä rajapinnat eth0 ja veth11. Kyseiset toimenpiteet toteutetaan seuraavilla komennoilla:

```
root@SDN-AP1:/home/pi# ip link add veth00 type veth peer name veth11
root@SDN-AP1:/home/pi# ovs-vsctl add-br br1
root@SDN-AP1:/home/pi# ovs-vsctl add-port br1 eth0
root@SDN-AP1:/home/pi# ovs-vsctl add-port br1 veth11
```

Seuraavalla komennolla tukiasema liitetään SDN-kontrolleriin br1:n avulla:

```
root@SDN-AP1:/home/pi# ovs-vsctl set-controller br1 tcp:192.168.1.100:6633
```

Kuviosta 11 voidaan todeta, että virtuaalikytkin nimellä br1 on liitetty SDN-kontrolleriin ja rajapinnat eth0 ja veth11 on lisätty siihen.

```
root@SDN-AP1:~# ovs-vsctl show
090ae09e-3589-4de5-96a6-18c8146a8a6e
    Bridge "br1"
        Controller "tcp:192.168.1.100:6633"
            is_connected: true
        Port "br1"
            Interface "br1"
                type: internal
        Port "veth11"
            Interface "veth11"
        Port "eth0"
            Interface "eth0"
    ovs_version: "2.7.90"
```

Kuvio 11. Virtuaalikytkin br1:n tiedot

Seuraavaksi asennetaan Bridge-utils-ohjelma, jonka avulla luodaan toinen virtuaalikytkin nimellä br0. Toisen virtuaalikytkimen luonnin jälkeen siihen liitetään rajapinnat wlan0 ja veth00.

```
root@SDN-AP1:/home/pi# apt-get install bridge-utils

root@SDN-AP1:/home/pi# brctl addbr br0

root@SDN-AP1:/home/pi# brctl addif br0 wlan0

root@SDN-AP1:/home/pi# brctl addif br0 veth00
```

Kuviossa 12 on esitetty Bridge-utils-ohjelmalla tehty toisen virtuaalikytkimen tiedot ja siihen liitetyt rajapinnat.

```
root@SDN-AP1:~# brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.2e1fbf9cbbd4       no              veth00
                                                        wlan0
```

Kuvio 12. Toisen virtuaalikytkimen tiedot

Virtuaalikytkinten asennuksen jälkeen Raspille asennetaan Hostapd-ohjelma seuraavalla komennolla:

```
root@SDN-AP1:~# apt-get install Hostapd
```

Hostapd-ohjelman asennuksen jälkeen luodaan hostapd.conf tiedoston, johon lisätään tukiaseman konfiguroinnit. Tiedoston sisältö on esitetty kuviossa 13.

```
  GNU nano 2.2.6                    File: /etc/hostapd/hostapd.conf

interface=wlan0
bridge=br0
driver=nl80211
ssid=SDN-test
hw_mode=g
channel=6
macaddr_acl=0
```

Kuvio 13. Hostapdin konfigurointi tiedosto

Tämän jälkeen hostapd.conf tiedoston sijainti lisätään Hostapdille. Tämän ansiosta ohjelma pystyy lukemaan tukiaseman konfiguraatiot käynnistyessään. Kyseinen toimenpide on esitetty kuviossa 14.

```
GNU nano 2.2.6                          File: /etc/default/hostapd

 Defaults for hostapd initscript

 See /usr/share/doc/hostapd/README.Debian for information about alternative
 methods of managing hostapd.

 Uncomment and set DAEMON_CONF to the absolute path of a hostapd configuration
 file and hostapd will be started during system boot. An example configuration
 file can be found at /usr/share/doc/hostapd/examples/hostapd.conf.gz

DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Kuvio 14. Hostapd.conf-tiedoston sijainnin määritys

Seuraavaksi lisättiin interfaces-tiedostolle sillatut portit ja määritettiin mistä jokainen rajapinta saa IP-osoitteensa. Kuviossa 15 on esitetty interfaces-tiedoston sisältö.

```
GNU nano 2.2.6                          File: /etc/network/interfaces
# Please note that this file is written to be used with dhcpcd
# For static IP, consult /etc/dhcpcd.conf and 'man dhcpcd.conf'
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto lo
iface lo inet loopback

iface eth0 inet manual

allow-hotplug wlan0
iface wlan0 inet manual
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

allow-hotplug wlan1
iface wlan1 inet manual
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

auto br0
iface br0 inet manual
bridge_ports wlan0

auto br1
iface br1 inet dhcp
```

Kuvio 15. Interfaces-tiedoston sisältö

Tässä vaiheessa voidaan käynnistää Hostapd-ohjelma ja sen jälkeen tarkistaa tukiaseman tiedot seuraavilla komennoilla:

```
root@SDN-AP1:~# /etc/init.d/hostapd start

root@SDN-AP1:~# iw wlan0 info
```

Kuviosta 16 voidaan todeta, että nyt rajapinta wlan0:n tyyppi on AP eli Access Point ja aloittanut mainostamaan määritetty SSID:n.

```
root@SDN-AP1:~# iw wlan0 info
Interface wlan0
        ifindex 3
        wdev 0x1
        addr b8:27:eb:c9:fa:50
        ssid SDN-test
        type AP
        wiphy 0
```

Kuvio 16. Wlan0-rajapinnan tiedot

Näiden asennusten ja konfigurointien jälkeen meillä on toimiva tukiasema, johon käyttäjät voivat yhdistyä. Ainoa ongelma on se, että osa ohjelmista ja palveluista eivät käynnistyy automaattisesti laitteen uudelleenkäynnistyksen jälkeen. Seuraavaksi automatisoidaan ohjelmien ja palvelujen käynnistys käyttäen crontab-työkalua. Crontabin avulla voidaan suorittaa automaattisesti komennot ja palvelut käynnistyksen yhteydessä.

Kuviosta 17 voidaan todeta, että Open vSwitch ja Hostapd käynnistetään heti laitteen uudelleenkäynnistyksen jälkeen. 30 sekunnin viiveellä lähetetään DHCP-pyyntö br1:lle. Lopuksi alustetaan hostapd.conf-tiedoston, jonka jälkeen laite siirtyy AP-tilaan. Viiveillä varmistetaan, että alustus tapahtuu viimeisenä.

```
@reboot sudo /etc/init.d/openvswitch-switch start
@reboot sudo /etc/init.d/hostapd start
@reboot sudo sleep 30 && sudo dhclient br1
@reboot sudo sleep 40 && sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf &
@reboot sudo sleep 45 && sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf &
```

Kuvio 17. Crontabilla määritetyt asetukset

Seuraavaksi lisättiin komennot, jotka halutaan suorittaa käynnistysprosessin loppuvaiheessa rc.local-tiedostolle. Rc.local ajetaan vasta crontabin ja kaikki muiden init-prosessien jälkeen. Kuviossa 18 on esitetty rc.local-tiedostolle lisätyt komennot.

```
  GNU nano 2.2.6                          File: /etc/rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# By default this script does nothing.

sudo ip link add veth00 type veth peer name veth11
sudo brctl addif br0 veth00

exit 0
```

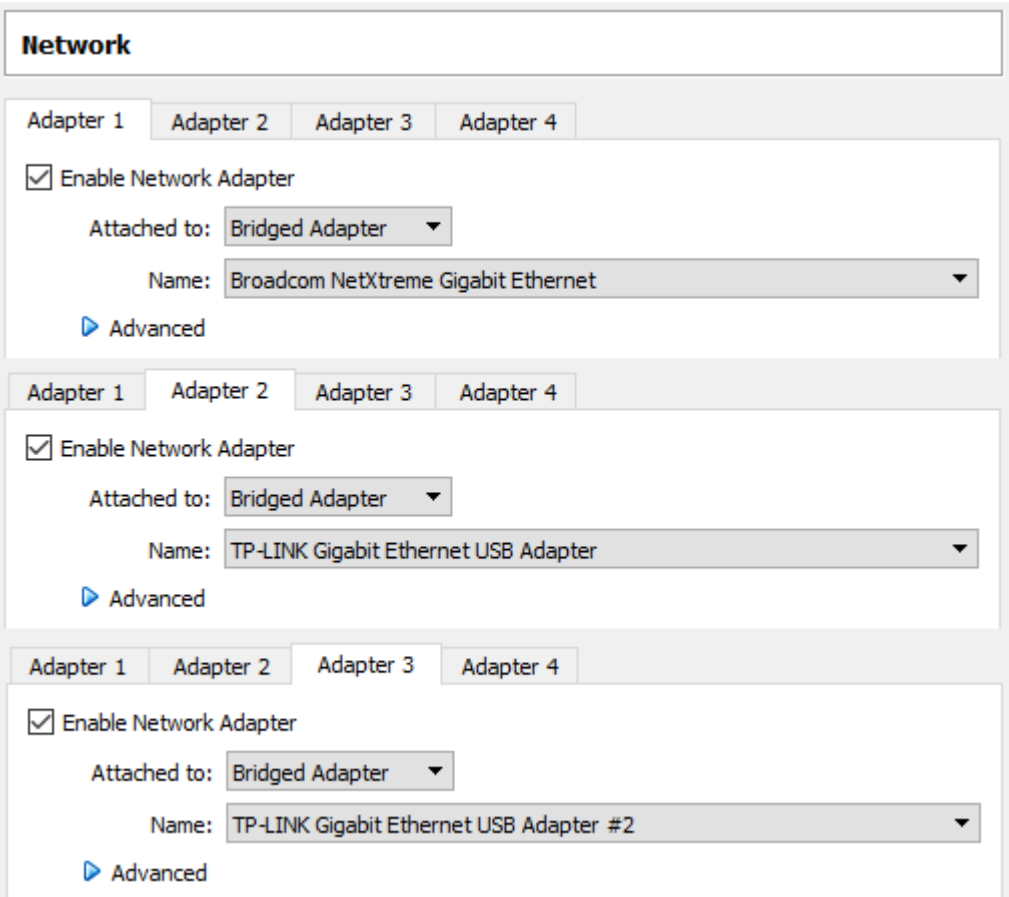
Kuvio 18. Rc.local-tiedostolle lisätyt komennot

Crontab ja rc.local-tiedostolla määritetyillä asetuksilla varmistettiin, että kaikki palvelut toimivat ja rajapinnat nousevat oikeassa järjestyksessä mahdollisen uudelleenkäynnistyksen jälkeen.

5.3 Pfsense

5.3.1 Asennus ja konfigurointi

Aloitettiin Pfsensen asennuksen luomalla uuden virtuaalikoneen VirtualBox-ohjelmalla. Virtuaalikoneelle asennettiin Pfsensen viimeisin vakaa 64-bittinen versio. Seuraavaksi määritettiin rajapinnat ennen virtuaalikoneen käynnistämistä kuvio 19 mukaisesti.



Kuvio 19. Pfsensen verkkoadapterit

Kuviosta voidaan todeta, että koneen WAN-puolen rajapinta eli Adapter 1 on sillattu paikallisen koneen rajapintaan, joka on kytketty LabraNettiin. LAN-puolen rajapinnat eli Adapter 2 ja 3 ovat sillattu USB-porttiin liitetyt verkkoadaptereihin. Seuraavaksi laitettiin virtuaalikone päälle. Kuviossa 20 on esitetty Pfsensen CLI-näkymä, josta käy ilmi määritetyt rajapinnat ja niiden IP-osoitteet.

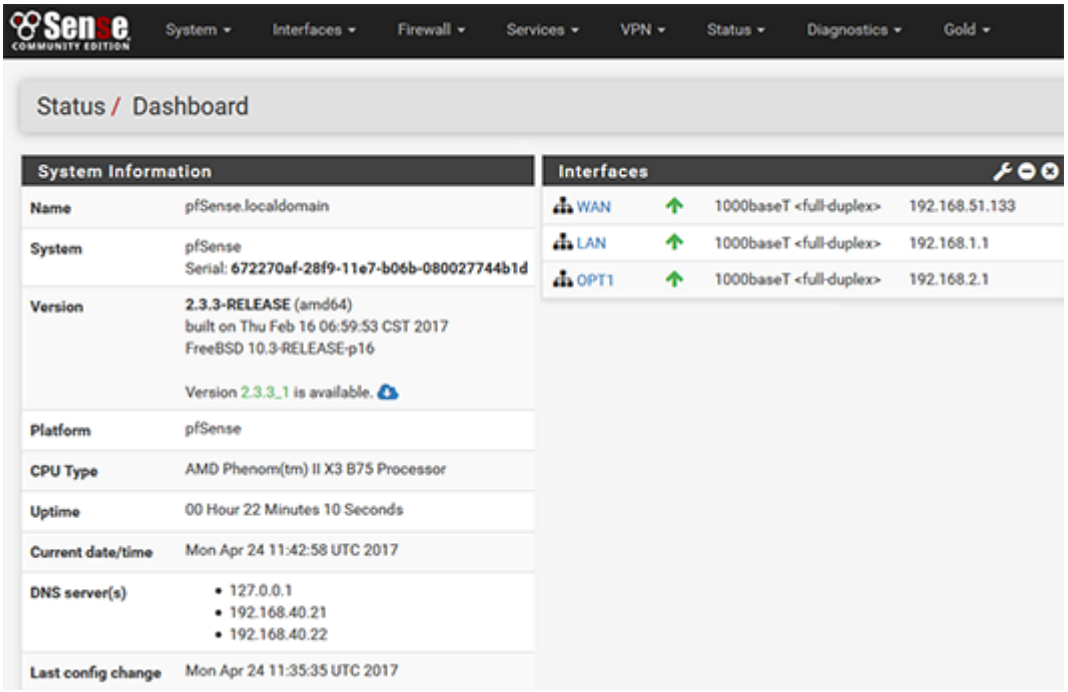
```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.3-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.51.133/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.2.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 
```

Kuvio 20. Pfsensen komentorivi

Kuvion LAN-rajapinnoista LAN on management-rajapinta, joka on tarkoitettu kontrollerille ja OPT1 on asiakaslaitteiden rajapinta. Pfsense on mahdollistaa konfiguroida myös graafisen käyttöliittymän avulla, mutta siihen kirjautuminen WAN-puolelta on estetty palomuurilla. Tästä johtuen otettiin palomuuri pois käytöstä väliaikaisesti seuraavalla komennolla:

```
[2.3.3-release][root@pfSense.localdomain]/root: pfctl -d
```

Tämän jälkeen voidaan käyttää Pfsensen graafisen käyttöliittymän selaimella myös WAN-puolelta. Kuviossa 21 on esitetty Pfsensen graafisen käyttöliittymän etusivu sisäänkirjautumisen jälkeen.

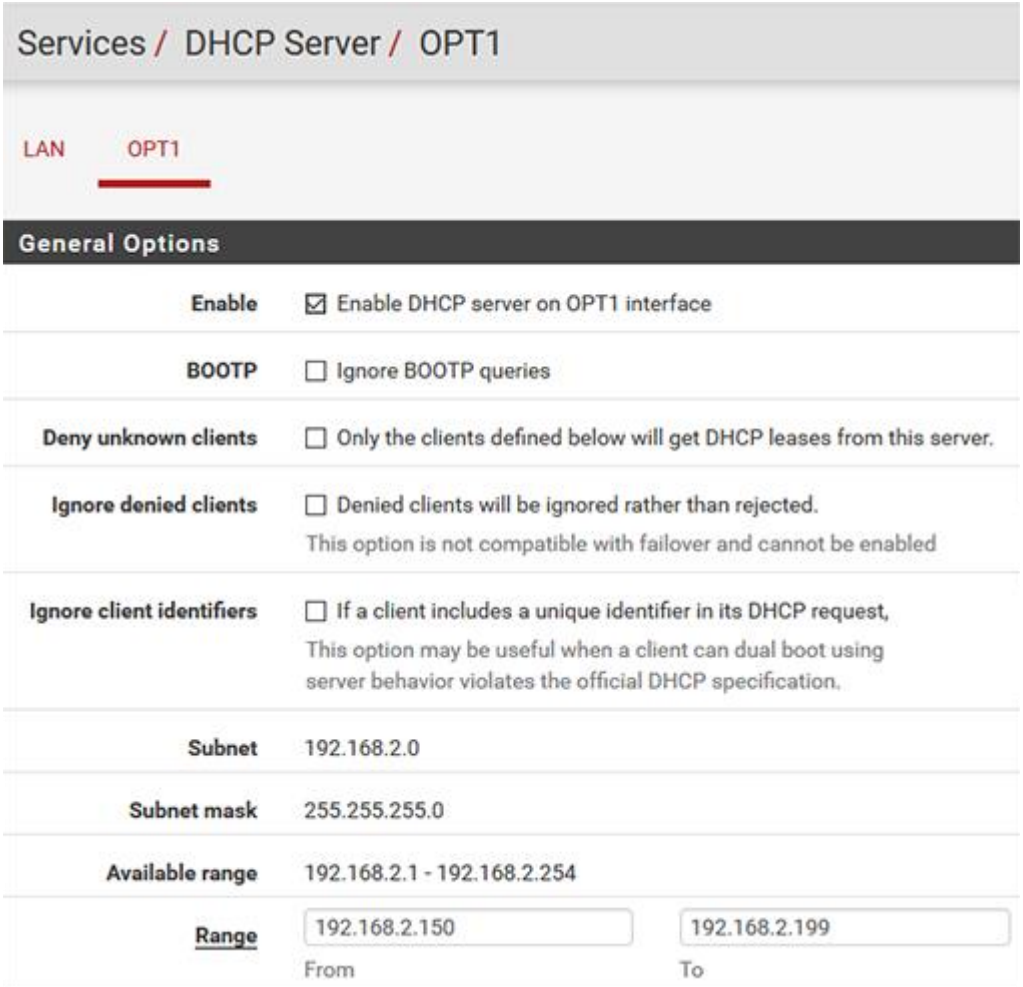


Kuvio 21. Pfsensen graafisen käyttöliittymän etusivu

Graafisella käyttöliittymällä lisättiin ensimmäisenä uuden palomuurisäännön, jonka avulla sallitaan HTTPS-yhteyden muodostaminen WAN-puolelta. Tämän jälkeen otettiin palomuuri käyttöön komentorivillä seuraavalla komennolla:

```
[2.3.3-release][root@pfSense.localdomain]/root: pfctl -e
```

Seuraavaksi konfiguroidaan DHCP-palvelimen asetukset ja määritetään osoitealue, josta verkkoon liittyneet asiakaslaitteet saavat IP-osoitteensa. DHCP-palvelimen asetukset on esitetty kuviossa 22.



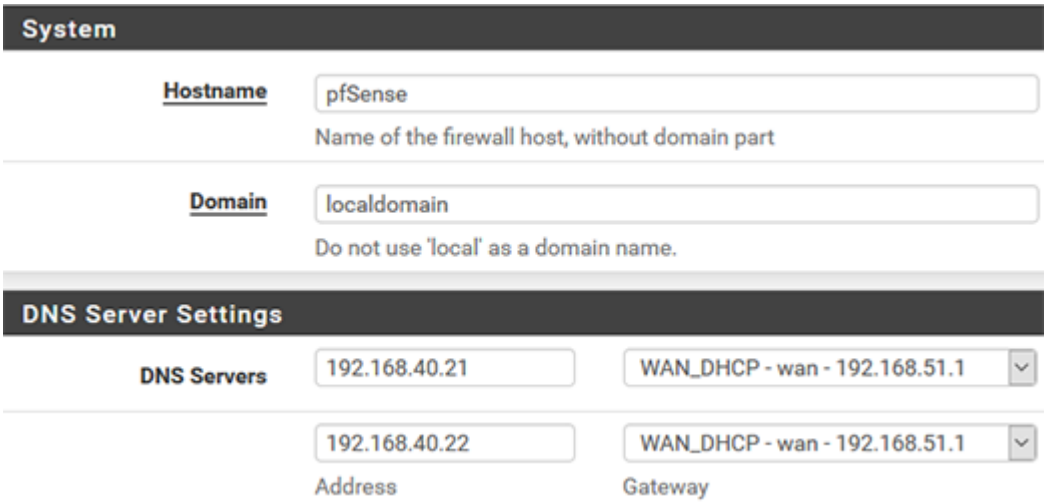
Kuvio 22. Asiakaslaitteiden DHCP-osoitealue

Verkkolaitteiden IP-osoitteet määritettiin staattisesti. Verkkolaitteiden IP-osoitteet on esitetty tauloukossa 3.

Taulukko 3. Verkkolaitteiden IP-osoitteet

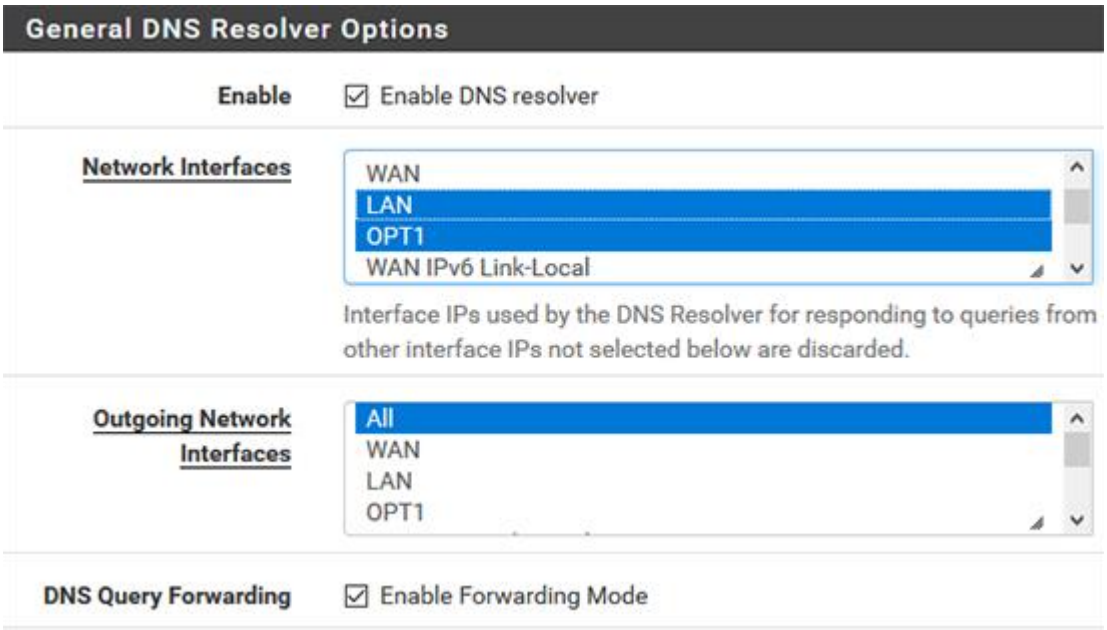
LAITTEEN NIMI	IP-OSOITE
Tukiasema 1	192.168.2.11
Tukiasema 2	192.168.2.12
OF-kytkin	192.168.1.11
SDN-Kontrolleri	192.168.1.100

Seuraavaksi määritettiin DNS-palvelut, jotta LAN-verkosta olisi mahdollisuus päästää Internettiin. DNS-palvelimena käytettiin LabraNetin DNS-palvelimet. Kuviossa 23 on esitetty Pfsensen DNS-asetukset.



Kuvio 23. Pfsensen DNS-asetukset

Tämän jälkeen otettiin käyttöön DNS-resolverin, jonka tehtävä on vastata asiakaslaitteiden nimipalvelukyselyihin. Kuviossa 24 on esitetty DNS-resolverin asetukset.



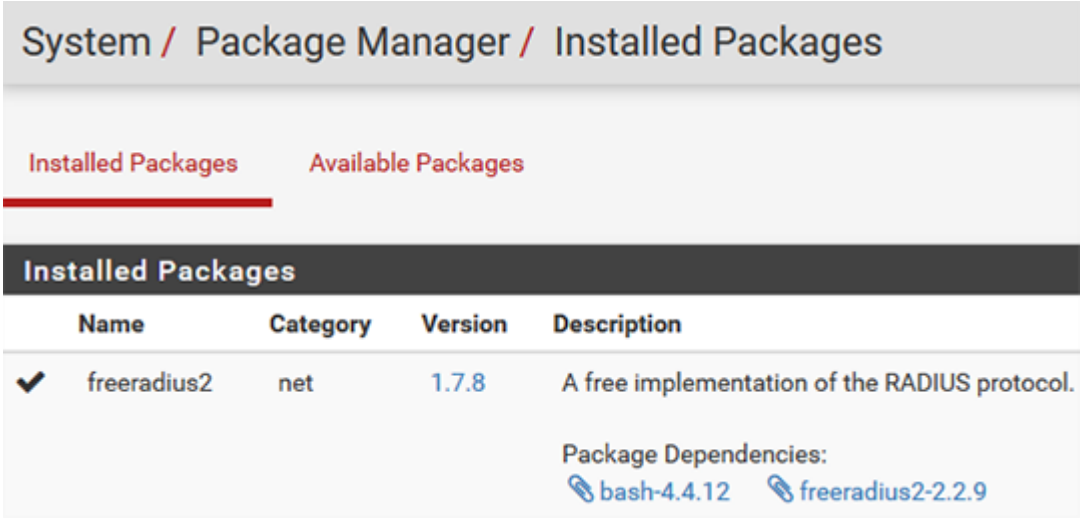
Kuvio 24. DNS-resolverin asetukset

Lopuksi määritettiin asiakaslaitteiden rajapinta IP-osoitteella 192.168.2.1 nimipalvelukyselyiden rajapinnaksi. Määritys on esitetty kuviossa 25.

Kuvio 25. DNS-kyselyiden rajapinnan määritys

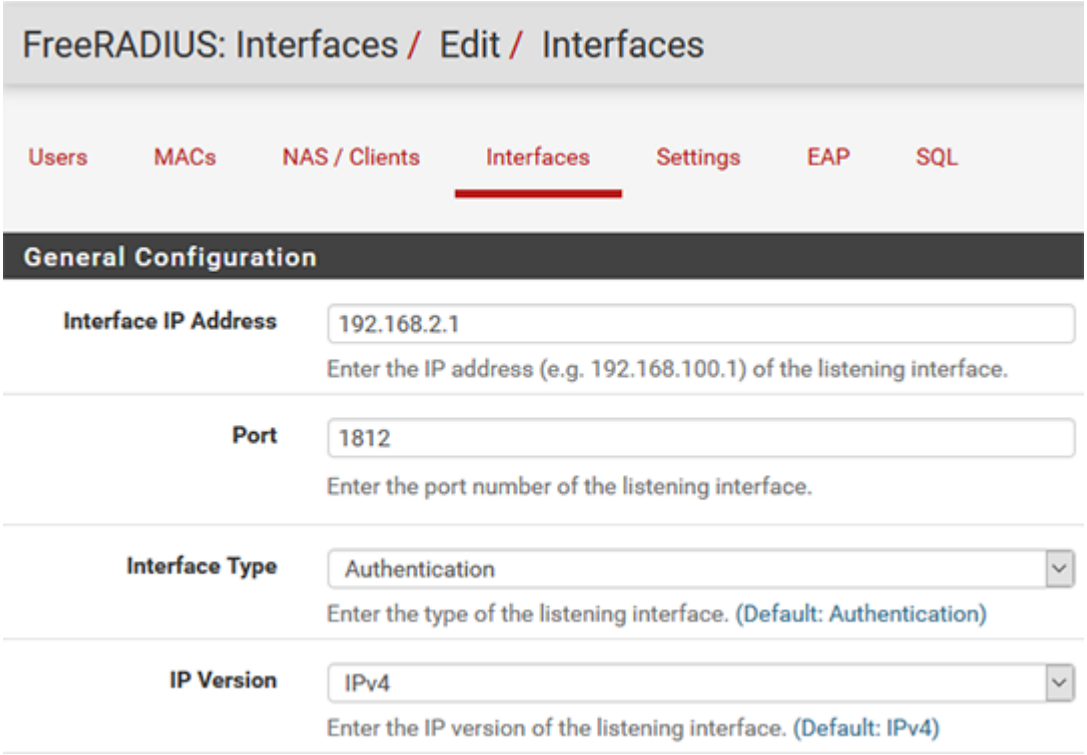
5.3.2 RADIUS-palvelin

RADIUS-palvelimen asennuksen aloitettiin asentamalla FreeRadius2-paketin, Pfsensen graafisella käyttöliittymällä. FreeRadius2-paketti löytyy välilehdeltä System > Package Manager > Available Packages. Kuviossa 26 on esitetty, että FreeRadius2 ja sen riippuvuudet on asennettu onnistuneesti.



Kuvio 26. FreeRadius2-paketin asennus

RADIUS-palvelimen asennuksen jälkeen aloitettiin konfiguroimaan sen Pfsensen välilehdeltä Services > FreeRADIUS. Ensimmäiseksi määritettiin rajapinta, joka palvelin kuuntelee autentikointia varten. Kuviossa 27 on esitetty Interfaces-välilehdellä määritetyt asetukset.



Kuvio 27. RADIUS-palvelimen Interfaces-välilehdellä määritetyt asetukset

Seuraavaksi Clients-välilehdellä lisättiin palvelimelle tukiasemien tiedot. Palvelimelle lisättiin tukiasemien IP-osoitteet, nimet ja jaettu salasana, jonka avulla tukiasemat pääsevät kommunikoimaan RADIUS-palvelimen kanssa. Clients-välilehdellä lisätyt tiedot on esitetty kuviossa 28.

Package / FreeRADIUS: Clients / NAS / Clients

Users MACs NAS / Clients Interfaces Settings

Client IP Address	Client IP Version	Client Shortname	Client Protocol
192.168.2.11	ipaddr	SDN-AP1	udp
192.168.2.12	ipaddr	SDN-AP2	udp

Kuvio 28. RADIUS-palvelimen asiakkaat

Lopuksi RADIUS-palvelimelle lisättiin uusi käyttäjä, joka tullaan käyttämään palveluun sisäänkirjautumisvaiheessa. Users-välilehdellä lisätyt tiedot on esitetty kuviossa 29.

FreeRADIUS: Users / Edit / Users

Users MACs NAS / Clients Interfaces Settings

General Configuration

Username vieras

Enter the username.
Note: May only contain a-z, A-Z, 0-9

Password •••••• <- vieras

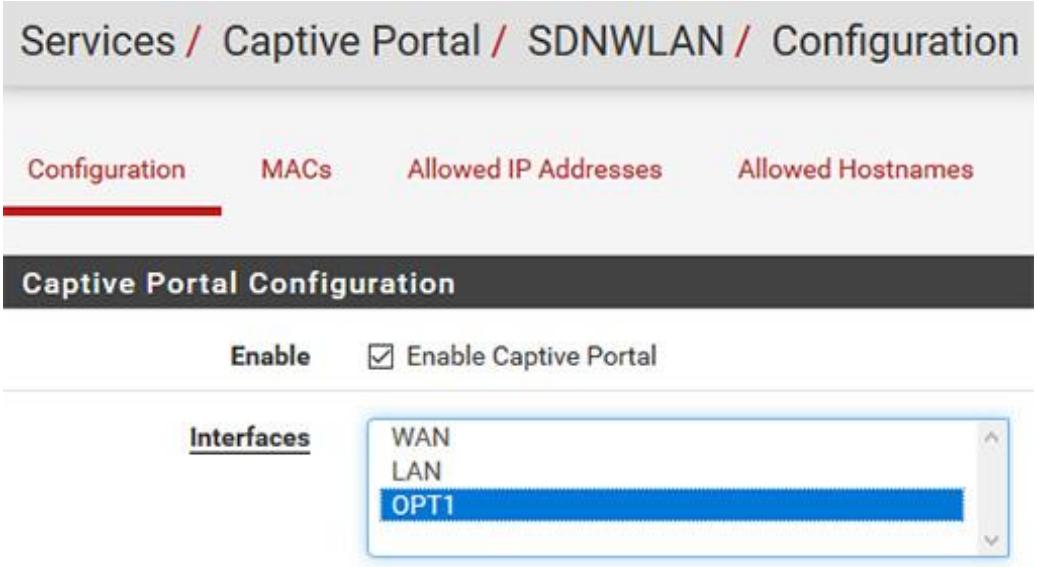
Enter the password for this username.

Kuvio 29. Uuden käyttäjän lisääminen RADIUS-palvelimelle

Tässä vaiheessa RADIUS-palvelimen konfigurointi on valmis ja pystyy vastaanottamaan tulevat todennuspyynnöt.

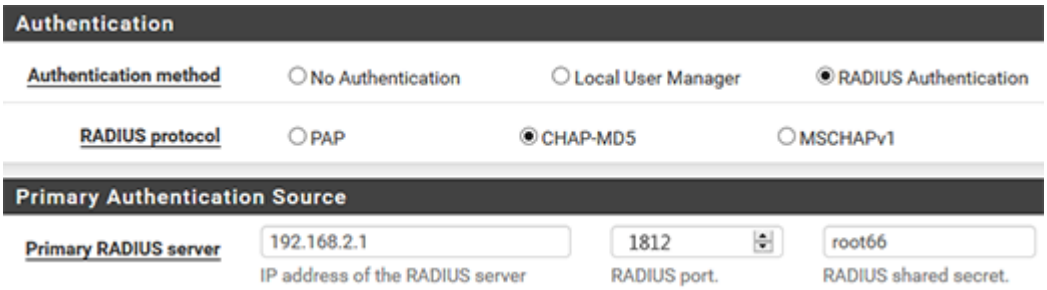
5.3.3 Captive Portal

Captive Portalin asennuksen aloitettiin luomalla uusi Zone nimellä SDNWLAN. Tämän jälkeen otettiin käyttöön Captive Portal-palvelu kyseiselle Zone:lle ja määritettiin asiakaslaitteiden rajapinta eli OPT1 palvelun rajapinnaksi. Kuviossa 30 on esitetty Captive Portal-palvelun käyttöönotto.



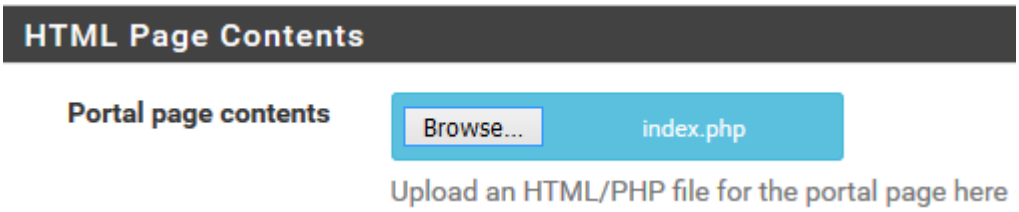
Kuvio 30. Captive Portal-palvelun käyttöönotto

Seuraavaksi määritettiin Captive Portalin asetukset konfiguraatiosivulla. Palvelun todennusmenetelmäksi valittiin RADIUS-autentikointi ja palvelulle lisättiin RADIUS-palvelimen tiedot. Todennusmenetelmän asetukset on esitetty kuviossa 31.



Kuvio 31. Captive Portalin todennusmenetelmän asetukset

Lopuksi konfiguraatiosivulla lisättiin myös palvelun laskeutumissivu php-tiedostona, joka on esitetty kuviossa 32. Verkkoon liittyneet käyttäjät ohjataan ensin laskeutumissivulle, jossa kerrotaan langattoman SDN-verkon käyttöehdot, ja hyväksymällä ehdot käyttäjät voivat kirjautua sisään palveluun. Liitteessä 1 on esitetty Brackets-tekstieditorilla suunniteltu laskeutumissivun lähdekoodi.



Kuvio 32. Captive Portalin laskeutumissivun lisääminen

5.4 OpenFlow-kytkimen konfigurointi

Zodiac FX OpenFlow-kytkimen konfigurointi hoidettiin Puttyn avulla. Laitteen IP-osoite, Netmask, Gateway, OpenFlow-portti ja SDN-kontrolleri määritettiin suunnitelman mukaisesti seuraavilla komennoilla:

```
Zodiac_FX# config
Zodiac_FX(config)# set ip-address 192.168.1.11
Zodiac_FX(config)# set netmask 255.255.255.0
Zodiac_FX(config)# set gateway 192.168.1.1
Zodiac_FX(config)# set of-controller 192.168.1.100
Zodiac_FX(config)# set of-port 6633
Zodiac_FX(config)# save
```

Konfiguroinnin jälkeen laite käynnistettiin uudelleen, että uudet asetukset tulisivat voimaan. Kuviossa 33 on esitetty OpenFlow-kytkimelle määritetyt asetukset.

```
Zodiac_FX# config
Zodiac_FX(config)# show config

-----------------------------------------
Configuration
 Name: Zodiac_FX
 MAC Address: 70:B3:D5:6C:D6:99
 IP Address: 192.168.1.11
 Netmask: 255.255.255.0
 Gateway: 192.168.1.1
 OpenFlow Controller: 192.168.1.100
 OpenFlow Port: 6633
 Openflow Status: Enabled
 Failstate: Secure
 Force OpenFlow version: Disabled
 Stacking Select: MASTER
 Stacking Select: Disabled
 EtherType Filtering: Disabled
```

Kuvio 33. OpenFlow-kytkimen asetukset

5.5 SDN-kontrolleri

5.5.1 Ryu

Ryu-kontrollerin asennuksen aloitettiin luomalla uuden virtuaalikoneen VirtualBoxilla. Virtuaalikoneen käyttöjärjestelmä on 64-bittinen Ubuntu 16.04.2 LTS. Käyttöjärjestelmän asennuksen jälkeen asennettiin Ryu ja sen tarvitsemat paketit ja lisäosat. Ryun ohjelmointikieli on Python, joten asennettiin ensin Python-paketit ja -kirjastot seuraavilla komennoilla:

```
root@ryu:~# apt-get update

root@ryu:~# apt-get install python-setuptools python-pip

root@ryu:~# pip install lxml paramiko eventlet msgpack-python
netaddr oslo.config routes six webob
```

Python-pakettien asennuksen jälkeen, asennettiin Ryu seuraavilla komennoilla:

```
root@ryu:~# apt-get install git-all

root@ryu:~# git clone git://github.com/osrg/ryu.git

root@ryu:~# cd ryu

root@ryu:~/ryu# python ./setup.py install
```

Kuviosta 34 voidaan todeta, että Ryu on asennettu ja sen versio on 4.12.

```
root@ryu:~# ryu-manager --version
Registered VCS backend: git
Registered VCS backend: hg
Registered VCS backend: svn
Registered VCS backend: bzr
ryu-manager 4.12
```

Kuvio 34. Ryu-kontrollerin asennus

Seuraavaksi asennettiin Faucet, joka on Ryulle tarkoitettu layer 2/3 -kytkinkontrolleri ja parantaa työssä käytetyn Zodiac FX OpenFlow-kytkimen toiminnallisuuden. Faucet tukee virtuaaliset lähiverkot, pääsylistat, portin peilaus ja L3-tason reitityksen. Ryu-faucet asennettiin seuraavalla komennolla:

```
root@ryu:~# pip install ryu-faucet
```

Kuviosta 35 voidaan todeta, että Ryu-faucet on asennettu onnistuneesti ja sen versio on 1.4.

```
root@ryu:~# pip show ryu-faucet
Name: ryu-faucet
Version: 1.4.0
Summary: FAUCET is a Ryu application to enable drop-in replacement
 for a legacy L2/L3 switch with extra SDN based functionality
```

Kuvio 35. Ryu-faucet-ohjelman asennus

Ryu-faucetin asennuksen jälkeen aloitettiin konfiguroimaan sen, faucet.yaml-tiedoston avulla. Faucet.yaml on Ryu-faucetin konfigurointi tiedosto, johon voidaan lisätä OF-kytkimen asetukset. Faucet.yaml-tiedoston sisältö on esitetty kuviossa 36.

```
version: 2
vlans:
    100:
        name: "openflow"

dps:
    zodiac-fx-1:
        dp_id: 0x70B3D56CD699
        interfaces:
            1:
                native_vlan: 100
                name: "zfx-port1"
            2:
                native_vlan: 100
                name: "zfx-port2"
            3:
                native_vlan: 100
                name: "zfx-port3"
```

Kuvio 36. Faucet.yaml-tiedoston sisältö

Kuten kuviosta käy ilmi, tiedostolle on lisätty OF-kytkimen OpenFlow-portit ja kytkimen ID. Kytkimen ID muodostettiin sen MAC-osoitteesta, jonka alkuun on lisätty 0x ja kaksoispisteet on poistettu. Tämän jälkeen lisättiin Ryu-faucet järjestelmään systemd-palveluksi, jotta ohjelma käynnistyy automaattisesti uudelleenkäynnistyksen jälkeen. Tätä varten ensimmäisenä luotiin uusi tiedosto nimellä start-faucet.sh, johon lisättiin kuviossa 37 esitetty skripti.

```
  GNU nano 2.5.3          File:  /etc/ryu/faucet/start-faucet.sh

#!/bin/bash

export FAUCET_CONFIG=/etc/ryu/faucet/faucet.yaml

export FAUCET_LOG=/etc/ryu/faucet/faucet.log

export FAUCET_EXCEPTION_LOG=/etc/ryu/faucet/faucet_exception.log

ryu-manager --ofp-listen-host=192.168.1.100 --ofp-tcp-listen-port=6633

--verbose /etc/ryu/faucet/faucet.py
```

Kuvio 37. Start-faucet.sh-tiedosto

Kuviosta voidaan todeta, että skriptillä asetetaan ympäristömuuttajat konfigurointi ja lokitiedostoille. Seuraavaksi tehtiin toinen tiedosto nimellä faucet.service, johon lisättiin kuviossa 38 esitetty tiedot.

```
  GNU nano 2.5.3            File: /etc/systemd/system/faucet.service

[Unit]
Description=FAUCET

[Service]
User=root
TimeoutStartSec=0
ExecStart=/etc/ryu/faucet/start-faucet.sh

[Install]
WantedBy=multi-user.target
```

Kuvio 38. Faucet.service-tiedosto

Lopuksi otettiin palvelu käyttöön ja käynnistettiin sen seuraavilla komennoilla:

```
root@ryu:~# systemctl enable /etc/systemd/system/faucet.service

root@ryu:~# systemctl start faucet.service
```

Näiden asennusten ja konfigurointien jälkeen meillä on toimiva Ryu-faucet-kontrolleri. Kuviosta 39 voidaan todeta, että Ryu-faucet on käynnistynyt onnistuneesti ja on valmis hallitsemaan verkon laitteet.

```
root@ryu:~# systemctl start faucet.service
root@ryu:~# systemctl status faucet.service
● faucet.service - FAUCET
   Loaded: loaded (/etc/systemd/system/faucet.service; enabled;
   Active: active (running) since Fri 2017-04-28 10:43:50 EEST; 8s ago
 Main PID: 1644 (start-faucet.sh)
    Tasks: 2
   Memory: 81.3M
      CPU: 1.179s
   CGroup: /system.slice/faucet.service
           ├─1644 /etc/ryu/faucet/start-faucet.sh
           └─1647 /usr/bin/python /usr/local/bin/ryu-manager --verbose

Apr 28 10:43:52 ryu start-faucet.sh[1644]: switch features ev version=0x4
Apr 28 10:43:52 ryu start-faucet.sh[1644]: move onto main mode
Apr 28 10:43:52 ryu start-faucet.sh[1644]: EVENT ofp_event->dpset
Apr 28 10:43:52 ryu start-faucet.sh[1644]: DPSET: register datapath
Apr 28 10:43:52 ryu start-faucet.sh[1644]: EVENT dpset->Faucet EventDP
Apr 28 10:43:52 ryu start-faucet.sh[1644]: EVENT ofp_event->Faucet EventOFPPacketIn
```

Kuvio 39. Ryu-faucetin käynnistys

5.5.2 Puikkari

Puikkari asennettiin importoimalla LabraNetin verkkolevyltä ladattu puikkari-vm.ova templaatin VirtualBoxiin. Asennuksen jälkeen oli tärkeä lisätä heti ensimmäisenä laitteen IP-osoite env.sh-tiedostolle. Puikkarin tärkeimmät asetukset löytyvät env.sh-tiedostossa. Seuraavalla komennolla lisättiin laitteen IP-osoite env.sh-tiedostolle:

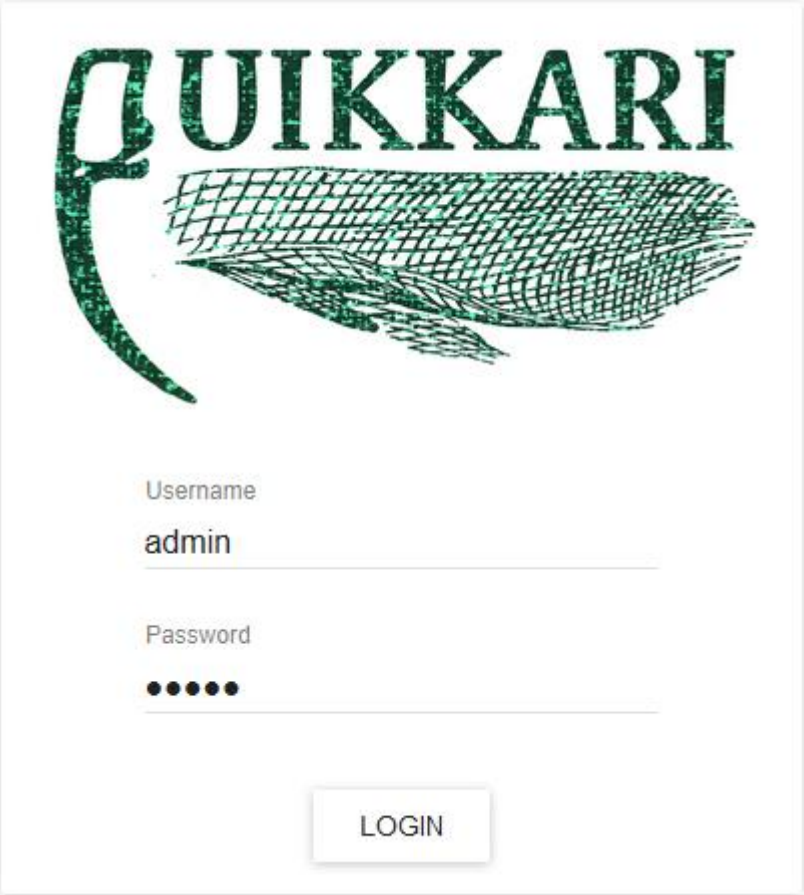
```
/opt/puikkari-vm/update_myip.sh
```

Tämän jälkeen käynnistettiin Puikkari ja sen toiminnan kannalta tärkeät palvelut seuraavilla komennoilla:

```
/opt/puikkari-vm/start_puikkari.sh
```

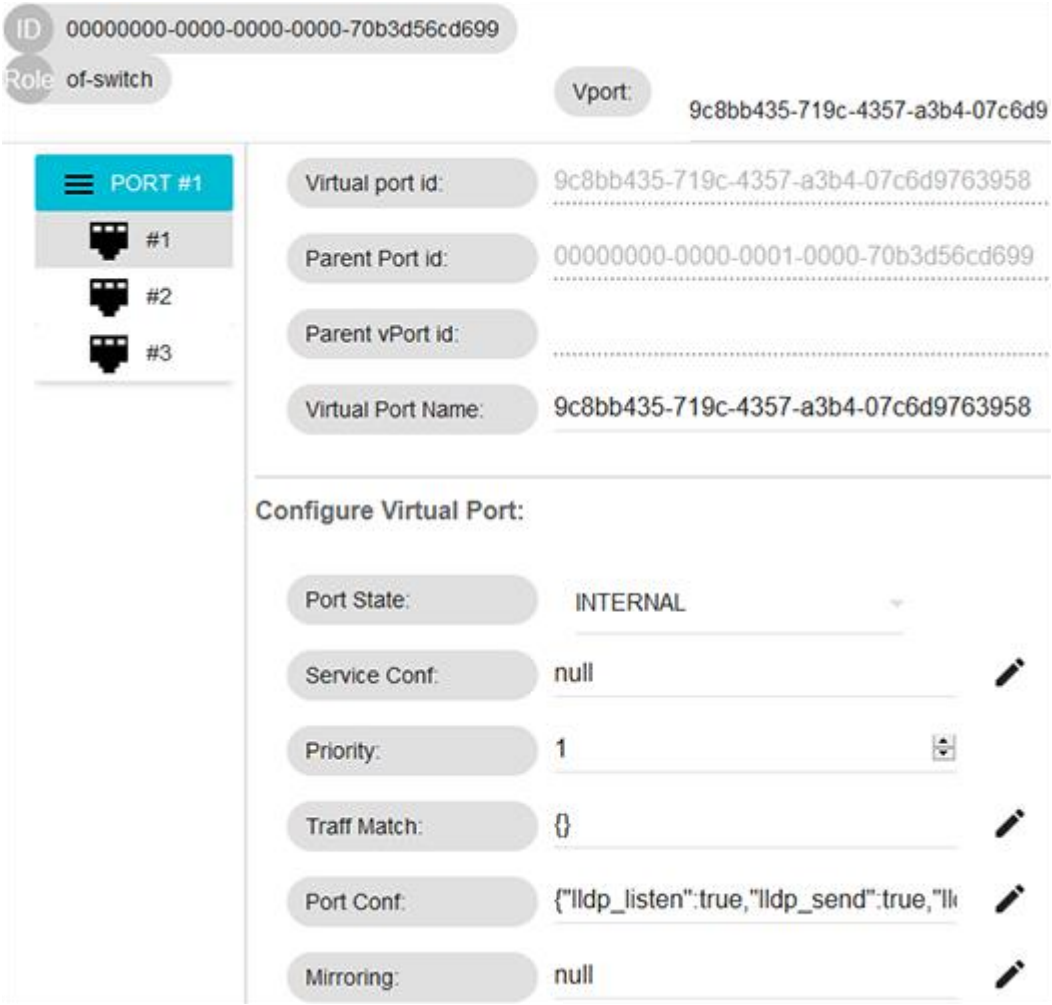
```
/opt/puikkari-vm/start_redis.sh

/opt/puikkari-vm/start_socket.sh

/opt/puikkari-vm/start_topo.sh

/opt/puikkari-vm/start_ryu.sh
```

Palveluiden käynnistyksen jälkeen voidaan kirjautua Puikkarin graafisen käyttöliittymään selaimen kautta. Puikkarin käyttöliittymän kirjautumisikkuna on esitetty kuviossa 40.



Kuvio 40. Puikkarin käyttöliittymän kirjautumisikkuna

Lopuksi graafisella käyttöliittymällä lisättiin OpenFlow-kytkimen portit Puikkariin kuvio 41 mukaisesti.



Kuvio 41. OpenFlow-kytkimen porttien lisääminen Puikkariin

5.6 Roaming-toiminto

Roaming-toiminnolla varmistettiin, että käyttäjän liikkuessa tai tukiaseman signaalin heikentyessä siirtyminen yhdestä tukiasemasta toiseen sujuu saumattomasti. Tätä varten käytettiin 802.11i-esitodennus menetelmä, joka nopeuttaa roaming-prosessin. 802.11i-esitodennus mahdollistaa autentikoinnin, kun asiakaslaite on edelleen kytkettynä vanhaan tukiasemaan. Tämän ansiosta käyttäjän ei tarvitse tunnistautua uudelleen siirtyessään uuteen tukiasemaan.

802.11i-esitodennus otettiin käyttöön lisäämällä kuviossa 42 esitetty asetukset hostapd.conf-tiedostolle. Hostapd.conf on tukiasemille aiemmin asennettu Hostapd-ohjelman konfigurointitiedosto.

```
  GNU nano 2.2.6                    File: /etc/hostapd/hostapd.conf

auth_server_addr=192.168.2.1
auth_server_port=1812
auth_server_shared_secret=root66
wpa_key_mgmt=WPA-EAP
disable_pmksa_caching=1
okc=0
eapol_key_index_workaround=1
ieee8021x=1
wpa_key_mgmt=WPA-EAP
wpa_group_rekey=2000
auth_algs=1
wpa=2
wpa_pairwise=CCMP
wpa_group_rekey=2000
interface=wlan0
bridge=br0
driver=nl80211
ssid=SDN-test
hw_mode=g
channel=6
macaddr_acl=0
rsn_preauth=1
rsn_preauth_interfaces=br0
```

Kuvio 42. 802.11i-esitodennuksen asetukset

Asetuksilla tukiasemille määritettiin RADIUS-palvelimen tiedot, identtiset SSID-tunnukset ja salaustekniikat. Tukiasemille asetettiin myös toisiaan häiritsemättömät kanavat. Seuraavaksi varmistettiin esitodennuksen toimivuus kuviossa 43 esitetty komennolla verkkoon liittynyt asiakaslaitteella.

```
valotu@workstation:~$ sudo wpa_cli -i wlp1s0 pmksa
Index / AA / PMKID / expiration (in seconds) / opportunistic
1 b8:27:eb:c9:fa:50 62274618d8da81a71ba37dfc9595a6c1 43130 0
2 b8:27:eb:4a:34:bb 3bdcfca11762e45db7b9bacc4b5d3f01 43191 0
```

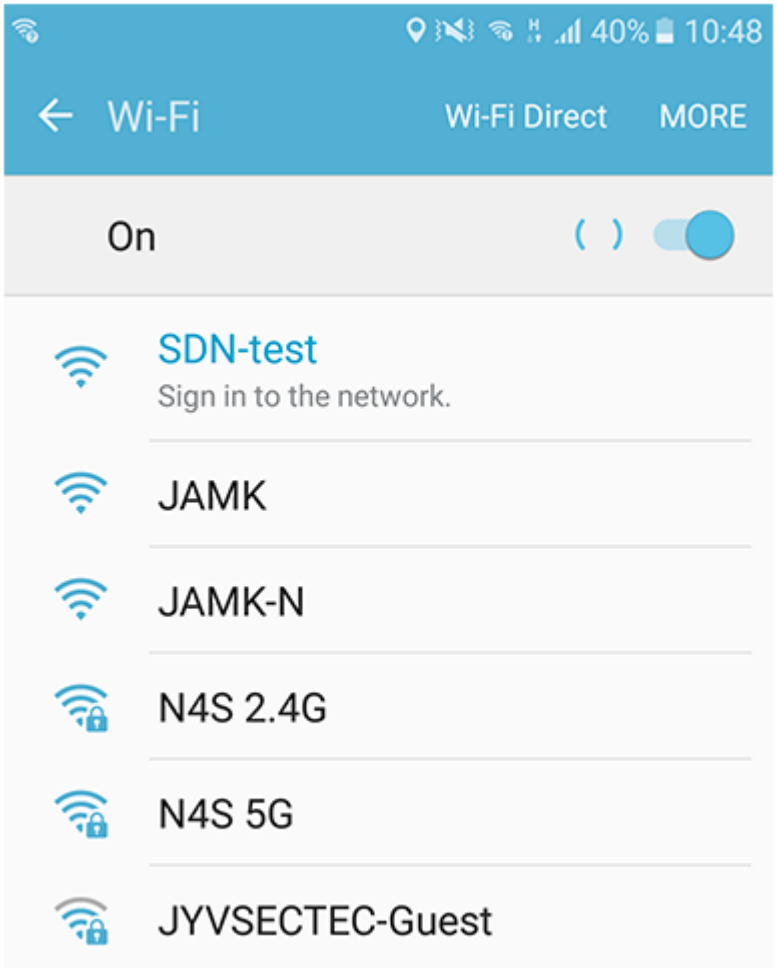
Kuvio 43. 802.11i-esitodennuksen varmitus

Kuviosta voidaan todeta, että verkkoon liittynyt asiakaslaitteella löytyy käytössä olevien tukiasemien MAC-osoitteet ja PMK-avaimet. PMK eli Pairwise Master Key on onnistuneen autentikoinnin tulos asiakaslaitteen ja tukiaseman välillä. Kun asiakas-laite siirtyy yhdestä tukiasemasta toiseen, kohdetukiasema tarkistaa asiakaslaitteen

PMK-avaimen. Jos asiakaslaitteella löytyy kohdetukiaseman PMK-avain, tukiasemien vaihto tapahtuu asiakkaan huomaamatta.

6 Toiminnan todennus ja analysointi

Langattoman SDN-verkon toiminnan testaus aloitettiin käynnistämällä verkon komponentit. Ensin käynnistettiin OpenFlow-kytkin ja Pfsense, seuraavaksi Puikkari ja lopuksi tukiasemat. Testauksessa käytettiin myös Android-matkapuhelin asiakaslaitteena. Tukiasemien käynnistyksen jälkeen asiakaslaitteella tuli niiden mainostama SSID nimellä SDN-test näkyviin, joka on esitetty kuviossa 44.



Kuvio 44. Tukiasemien mainostama SSID asiakaslaitteella

Seuraavaksi valittiin SDN-test -verkko asiakaslaitteella. Verkon valinnan jälkeen käyttäjä ohjattiin Captive Portal -asetuksissa määritelty laskeutumissivulle. Kuviossa 45 on esitetty SDN-verkon laskeutumissivu.

Kuvio 45. SDN-verkon laskeutumissivu

Tämän jälkeen muodostettiin yhteys verkkoon laskeutumissivulla esitetyt tunnusten avulla. Kuviosta 46 voidaan todeta, että käyttäjä on onnistuneesti sisäänkirjautunut Captive Portalin kautta ja yhdistynyt verkkoon.

Status / Captive Portal / SDNWLAN

Users Logged In (1)

IP address	MAC address	Username	Session start
192.168.2.155	84:9b:65:cd:d6:e7	vieras	May 2 10:49:14

Kuvio 46. SDN-verkon käyttäjät

Seuraavaksi testattiin SDN-verkon roaming-toiminto. Testauksessa haluttiin saada selville kuinka hyvin roaming toimii käyttäjän liikkuessa tai tukiaseman signaalin heikentyessä. Testissä verkkoon liittynyt käyttäjä käveli toisen tukiaseman suuntaan, joka oli muutaman metrin päästä. Käyttäjän nykyisen tukiaseman nimi on SDN-AP1 ja kanavanumero 1. Toisen tukiaseman nimi on SDN-AP2 ja kanavanumero 6. SDN-AP1:n signaalin heikentyessä asiakaslaite siirtyi automaattisesti toiseen tukiasemaan, jonka signaali oli voimakkaampi. Tukiaseman vaihto on esitetty kuviossa 47.

Kuvio 47. Tukiaseman vaihto signaalin heikentyessä

7 Yhteenveto ja pohdinta

Työn tavoitteena oli SDN-pohjainen langaton verkon suunnittelu ja toteutus. SDN-verkon suunnittelussa käytettiin sekä fyysisiä että virtuaalisia laitteita. Verkon toteutus aloitettiin rakentamalla tukiasemat Raspberry Pi -tietokoneista. SDN-kontrollerina käytettiin Puikkari ja tukiasemien hallinta mahdollistettiin sen avulla. Tukiasemille määritelty roaming-toiminnolla varmistettiin, että käyttäjän siirtyminen yhdestä tukiasemasta toiseen sujuu saumattomasti. SDN-verkon käyttäjien autentikointi hoidettiin RADIUS-palvelimella.

Opinnäytetyön tavoitteiden toteuttamiseen onnistuttiin hyvin ja projekti valmistui sovitun aikataulun mukaisesti. Oman oppimisen kannalta projekti tarjosi paljon uutta opittua asiaa sekä SDN-tekniikoista että langattoman verkon suunnittelusta. Linux-käyttöjärjestelmä oli itselleni entuudestaan tuttu, mutta opinnäytetyön ansiosta käyttötaitoani parani huomattavasti. Työn toteutusvaiheessa ongelmia tuli vastaan jonkin verran, mutta niistä selviydyin työn ohjaajilta saamani ohjeiden ansiosta.

Jatkokehitysideana olisi LDAP-autentikoinnin käyttöönotto, Kun myöhemmin kyseinen SDN-verkko tullaan toteuttamaan JAMK:ssa. Tämän ansiosta JAMKin opiskelijat pääsevät kirjautumaan verkkoon omilla käyttäjätunnuksilla. Työssä käytetty RADIUS-palvelimella on mahdollistaa toteuttaa myös LDAP-autentikointia.

Lähteet

Channel Planning Best Practices. N.d. Artikkeli Meraki-verkkosivulla. Viitattu 12.3.2017. https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Channel_Planning_Best_Practices

DIMECC Cyber Trust Program. N.d. Cyber Trust -projektin esittely. Viitattu 6.2.2017. http://cybertrust.fi

DSSS - Direct Sequence Spread Spectrum. N.d. Artikkeli Telecomabc-verkkosivulla. Viitattu 1.3.2017. http://www.telecomabc.com/d/dsss.html

Ihanainen, T. 2016. Langattoman verkkoratkaisun toteutus SDN-verkkoon. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tietoverkkotekniikan koulutusohjelma. Viitattu 15.2.2017. https://www.theseus.fi/bitstream/handle/10024/120990/Ihanainen_Timo.pdf

Introduction to OFDM. 2011. Artikkeli Gaussianwaves-verkkosivulla. Viitattu 3.3.2017. http://www.gaussianwaves.com/2011/05/introduction-to-ofdm-orthogonal-frequency-division-multiplexing-2/

Kaksonen, J. 2014. IT-Dynamon langattoman verkon mittaus ja optimointi. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tietoverkkotekniikan koulutusohjelma. Viitattu 10.3.2017. https://www.theseus.fi/bitstream/handle/10024/72538/Kaksonen_Joonas.pdf

Moisio, M. 2015. WLAN-verkon kapasiteettipohjainen mitoitus. Opinnäytetyö. Tampereen ammattikorkeakoulu, tietoliikennetekniikan koulutusohjelma. Viitattu 27.2.2017. https://www.theseus.fi/bitstream/handle/10024/94090/Moisio_Matti.pdf

ONF Overview. N.d. ONF organisaation esittely. Viitattu 14.2.2017. https://www.opennetworking.org/about/onf-overview

OpenFlow Switch Specification. 2014. PDF-tiedosto opennetworking.org-verkkosivustolla. Viitattu 24.2.2017. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.noipr.pdf

Salonen, T. 2016. WLAN-mittaukset. Opinnäytetyö. Tampereen ammattikorkeakoulu, tietoliikennetekniikan koulutusohjelma. Viitattu 4.3.2017. https://www.theseus.fi/bitstream/handle/10024/120894/Salonen_Tomi.pdf

The 802.11 family explained. N.d. Artikkeli Lifewire-verkkosivulla. Viitattu 7.3.2017. https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

Understanding the SDN Architecture. N.d. SDX Centralin verkkojulkaisu SDN-verkon arkkitehtuurista. Viitattu 18.2.2017. https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture/

What are SDN Controllers? N.d. Artikkeli SDN-kontrollerista. Viitattu 21.2.2017. https://www.sdxcentral.com/sdn/definitions/sdn-controllers/

What is FHSS? N.d. Artikkeli Techtarget-verkkosivulla. Viitattu 1.3.2017. http://searchnetworking.techtarget.com/definition/frequency-hopping-spread-spectrum

What is OpenFlow? N.d. Artikkeli SDX Central-verkkosivulla. Viitattu 24.2.2017. https://www.sdxcentral.com/sdn/definitions/what-is-openflow/

What is Software Defined Networking? N.d. Artikkeli SDX Central-verkkosivulla. Viitattu 12.2.2017. https://www.sdxcentral.com/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/

WLAN topologies. 2014. Artikkeli Controleng-verkkosivulla. Viitattu 9.3.2017. http://www.controleng.com/single-article/wlan-topologies/499aeba08a9b2d0741e5f992974db2ce.html

Liitteet

Liite 1. Laskeutumissivun lädekoodi

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>JAMK SDN WLAN</title>
<style type="text/css">
body,td,th {
                font-family: "Trebuchet MS", Arial, Helvetica, sans-serif;
}
</style>
</head>

<body>
<table width="680" height="624" border="0" align="center">
  <tr>
    <td width="667" height="24"> </td>
  </tr>
  <tr bgcolor="#00CCFF">
    <td height="26">    <font color="white"><strong>JAMK SDN
WLAN</strong></font></td>
  </tr>
  <tr>
    <td height="197"><div align="center"><img src="captiveportal-cybertrust-
logo.jpg" width="484" height="190" alt="CYBER TRUST" /></div></td>
  </tr>

  <tr>
    <td height="6"></td>
  </tr>
  <tr bgcolor="#333333">
    <td height="24"><div align="center"><font color="white"><strong>KIRJAUDU
SISÄÄN | LOGIN</strong></font></div></td>
  </tr>
  <tr>
    <td height="165"><div align="center">  <form method="post"
action="http://192.168.2.1:8002/index.php?zone=sdnwlan">
                <input name="redirurl" type="hidden" value="https://www.jamk.fi">
                <input name="zone" type="hidden" value="sdnwlan">

                        <table>

                                <tr><td> </td></tr>
```

```
                                        <tr><td class="text-
right">Username:</td><td><input name="auth_user" type="text" style="border: 1px
dashed;"></td></tr>

                                        <tr><td class="text-
right">Password:</td><td><input name="auth_pass" type="password"
style="border: 1px dashed;"></td></tr>

                                        <tr><td> </td></tr>

                                        <tr>

                                                <td
colspan="2"><center><input name="accept" type="submit"
value="Continue"></center></td>

                                        </tr>

                            </table>
</form></div></td>
  </tr>
  <tr bgcolor="#FF9900">
    <td height="24">  <font color="white"><strong>LIITTYÄKSESI TÄHÄN WLAN-
VERKKOON HYVÄKSYT SIIHEN LIITTYVÄT KÄYTTÖEHDOT:</strong></font></td>
  </tr>
  <tr>
    <td height="140"><table width="640" border="0" align="center">
      <tr>
        <td height="125"><p>Tämä langaton verkko on osa SDN-testiverkkoa (Software
Defined Networking).<br />
         Yhteyttäsi monitoroidaan ja tutkitaan JAMKin CyberTrust projektiryhmän
toimesta.<br />
         Hyväksymällä nämä ehdot, voit kirjautua verkkoon seuraavilla
tunnuksilla:</p><table width="460" border="0" align="center">
      <tr>
        <td bgcolor="#E4F3F8"><div align="center">USERNAME:</div></td>
        <td><div align="center">vieras</div></td>
        <td bgcolor="#E4F3F8"><div align="center">PASSWORD:</div></td>
        <td><div align="center">vieras</div></td>
      </tr>
    </table></p></td>
      </tr>
    </table></td>
  </tr>

</table>
</body>
</html>
```