OULUN AMMATTIKORKEAKOULU

Teemu Paldanius

RASPBERRY PI VIRTUAALINEN ERILLISVERKKO

RASPBERRY PI VIRTUAALINEN ERILLISVERKKO

Teemu Paldanius
Opinnäytetyö
Kevät 2020
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma, Järjestelmäasiantuntemus

---

Tekijä(t): Teemu Paldanius
Opinnäytetyön nimi: Raspberry Pi virtuaalinen erillisverkko
Työn ohjaaja: Ani Ruusila
Työn valmistumislukukausi ja -vuosi: Kevät 2020 Sivumäärä: 47 + 1

Opinnäytetyöni tavoitteena oli luoda toimiva Raspberry Pi VPN-reititin. Opinnäytetyössäni loin Raspberry Pi VPN-reitittimen, joka käytti kahta Ethernet-porttia (USB-Ethernet adapteria ja Raspberry Pi:n omaa Ethernet-porttia) ja langatonta verkkoa. Tavoitteena oli kehittää helppokäyttöinen ja halpa ratkaisu yksityiskäyttöön. Kaiken verkkoliikenteen oli tarkoitus kulkea Raspberry Pi:n kautta. VPN:n avulla saatiin lisää suojaa ja yksityisyyttä koko verkolle, eikä vain yhdelle laitteelle.

Käyttöjärjestelmänä toimi OpenWrt, VPN-protokollana OpenVPN ja VPN-palveluntarjoajana NordVPN. Testaustuloksen perusteella Raspberry Pi 3 B+ malli hidasti Internet-yhteyden nopeutta ilman VPN-yhteyttä ja sen kanssa enemmän kuin ASUS RT-N18U reititin. Testit osoittivat, että UDP-protokolla on huomattavasti nopeampi kuin TCP-protokolla. Tästä syystä OpenVPN-protokollaa käytettäessä VPN-palveluntarjoajat suosittelevat yleensä käyttämään UDP-protokollaa.

Internet-yhteyksien nopeudet testattiin kolmeen kertaan, jonka jälkeen laskettiin Internet-nopeuksien keskiarvo. Tutkimuksen luotettavuuden kannalta oli hyvä testata Internet-yhteyksien nopeudet useampaan kertaan. Tutkimuksen luotettavuutta olisi lisännyt Internet-yhteyksien nopeuksien testaaminen useina eri päivinä. Tulokset eivät välttämättä olisi muuttuneet olennaisesti, mutta VPN-palvelimien kuormitus voi vaikuttaa yhteyksien nopeuksiin satunnaisesti.

Jatkotutkimuksessa kannattaa verrata uusia Raspberry Pi 4 B-malleja opinnäytetyössä käytettyyn Raspberry Pi 3 B+ malliin. Uusissa Raspberry Pi 4 B-malleissa on nopeammat prosessorit ja enemmän RAM-muistia mallista riippuen. Eri Raspberry Pi 4 B-mallien välinen vertailu VPN-käytössä olisi kiinnostava ja uutta tietoa tuottava projekti.

Asiasanat: VPN, Raspberry Pi, reititin, NordVPN, OpenVPN, Openwrt

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Business Information Systems, System expertise

---

Author(s): Teemu Paldanius
Title of thesis: Raspberry Pi Virtual Private Network
Supervisor(s): Ani Ruusila
Term and year when the thesis was submitted: Spring 2020 Number of pages: 47 + 1

The goal of my thesis was to create a working Raspberry Pi VPN router. In my thesis I created Raspberry Pi VPN router that used two Ethernet ports (USB-Ethernet adapter and Raspberry Pi's own Ethernet port) and wireless network. The goal was to develop an easy-to-use and inexpensive solution for private use. All network traffic passed through the Raspberry Pi. VPN provided more protection and privacy for the entire network, and not just for one device.

The used operating system was OpenWrt, as the VPN protocol was OpenVPN and the VPN service provider was NordVPN. Based on the test results, the Raspberry Pi model 3B+ slowed down the speed of the Internet connection without a VPN connection and with it more than the ASUS RT-N18U router. Tests showed that the UDP protocol is significantly faster than the TCP protocol. For this reason, when using the OpenVPN protocol, VPN service providers generally recommend using the UDP protocol.

Internet connection speeds were tested three times, after which the average Internet speeds were calculated. From the point of view of the reliability of the study, it was good to test the speeds of Internet connections several times. The reliability of the study would have been increased by testing the speeds of Internet connections on several different days. The results might not have changed significantly, but the load on the VPN servers can affect connection speeds occasionally.

In further research, it is worth comparing the new Raspberry Pi 4 model B's with the Raspberry Pi model 3B+ used in this thesis. The new Raspberry Pi model 4 B's have faster processors and more RAM depending on the model. A comparison between different Raspberry Pi 4 model B's in VPN use would be an interesting and informative project.

Keywords: VPN, Raspberry Pi, router, NordVPN, OpenVPN, Openwrt

SISÄLLYS

1 JOHDANTO

Opinnäytetyön aiheena oli Raspberry Pi VPN-reitittimen toteuttaminen käyttäen kahta Ethernet-verkkokorttia sekä langatonta verkkoa. Opinnäytetyössä käytettiin Raspberry Pi 3 B+ mallia, koska malli 4:n versioita ei ollut opinnäytetyön aloitushetkellä Suomessa helposti saatavilla. Sain idean Raspberry Pi VPN-ratkaisun tekemiseen entisen työpaikkani esimieheltä. Opinnäytetyön teoria-osassa käsitellään esimerkiksi, mitä VPN tarkoittaa käytännössä sekä millaisia VPN-protokollia ja -ratkaisuja on olemassa. Opinnäytetyössä käsitellään Raspberry Pi:n historiaa ja erilaisia malleja sekä Linux-jakelu vaihtoehtoja.

Opinnäytetyön kehitystehtävässä luotiin toimiva VPN-reititin käyttäen Raspberry Pi:tä, jossa käyttöjärjestelmänä toimi OpenWrt, VPN-protokollana toimi OpenVPN ja VPN-palveluntarjoajana käytettiin maksullista NordVPN-palvelua. Kehitystehtävässä käytettiin kahta Ethernet-verkkokorttia. Toisena Ethernet-verkkokorttina toimi Raspberry Pi:ssä oleva Ethernet-portti, jonka lisäksi Raspberry Pi:hin kiinnitettiin USB-Ethernet adapteri. Raspberry Pi toimi kehitystehtävässä reitittimenä, jonka kautta kulkeva liikenne kulki VPN:n läpi. Raspberry Pi:n Ethernet-porttiin yhdistettiin tietokone, USB-Ethernet adapteriin yhdistettiin ulkoverkko ja Rasperry Pi:n langattomaan verkkoon voitiin yhdistää esimerkiksi kannettava tai puhelin. Tämä ratkaisu mahdollisti Raspberry Pi:hin, yhteydessä olevalle käyttäjälle sen, että hänen ei tarvitse erikseen yhdistää VPN-sovellukseen. Raspberry Pi VPN-reititin on pieni, halpa ja helposti mukaan otettava laite, jonka avulla on mahdollista suojata oman verkon käyttöä matkoilla tai kotona.

2 KÄSITTEET

AES	Advanced Encryption Standard on symmetrinen lohkosalausmenetelmä, jota käytetään tietojen salaamiseen (DeMuro 2018, viitattu 23.5.2020).
DHCP	Dynamic Host Configuration Protocol on verkkoprotokolla, joka tarjoaa nopean ja automaattisen tavan IP-osoitteiden jakeluun verkon sisällä. DHCP:tä käytetään lisäksi laitteen aliverkon peitteen, oletusyhdyskäytävän ja DNS-palvelimen tietojen määrittämiseen. (Fisher 2019, viitattu 23.5.2020.)
DNS	Domain Name System antaa käyttäjälle mahdollisuuden muodostaa yhteyden verkkosivustoihin käyttämällä Internet-verkkotunnuksia ja haettavissa olevia URL-osoitteita numeeristen IP-osoitteiden sijasta (IBM Cloud Education 2020, viitattu 23.5.2020).
DNS-vuoto	VPN-yhteyttä käytettäessä DNS-pyyntöjen tulisi kulkea salatun tunnelin kautta suoraan VPN-palveluntarjoajan DNS-palvelimiin. DNS-vuoto on tietoturva-aukko, joka mahdollistaa DNS-pyyntöjen kulkemisen Internet-palveluntarjoajan DNS-oletuspalvelimiin. (NordVPN 2020a, viitattu 23.5.2020.)
Geoblokkaus	Geoblokkauksella tarkoitetaan sitä, kun käyttäjältä estetään pääsy sisältöön hänen maantieteellisen sijaintinsa perusteella (FlashRouters 2018, viitattu 23.5.2020).
GeoIP	GeoIP tarkoittaa menetelmää, jolla etsitään tietokonepäätteen maantieteellinen sijainti selvittämällä päätteen IP-osoite (Nexcess 2019, viitattu 23.5.2020).
GNU GPL	GNU General Public License on ilmainen, vapaan levitysoikeuden lisenssi ohjelmistoille ja muunlaisille teoksille (GNU.org 2007, viitattu 23.5.2020).
Käyttöjärjestelmä	Käyttöjärjestelmä on tärkein tietokoneella toimiva ohjelmisto. Se hallitsee tietokoneen muistia ja prosesseja samoin kuin kaikkia sen ohjelmistoja ja laitteistoja. (GCFGlobal 2020, viitattu 23.5.2020.)
Laajaverkko	Yksinkertaisimmassa muodossaan laajaverkko eli Wide area network (WAN) on kokoelma lähiverkkoja tai muita verkkoja, jotka ovat yhteydessä toisiinsa (Cisco 2020c, viitattu 23.5.2020).
Langaton lähiverkko	Langattomat verkot ovat tietokoneverkkoja, joita ei ole liitetty minkäänlaisilla kaapeleilla. Langattomat verkot yhdistävät laitteita Internettiin radioaaltoja käyttämällä. (Techopedia 2016, viitattu 23.5.2020.)
Linux-jakelu	Linux-käyttöjärjestelmää levitetään useana eri jakeluna. Linux-jakelu koostuu Linux-ytimestä, joukosta apuohjelmia ja konfigurointitiedostoja. (Bresnahan & Blum 2015, 13.)

Lähiverkko	Lähiverkko eli local area network (LAN) on kokoelma laitteita, jotka on kytketty yhteen fyysiseen sijaintiin, kuten esimerkiksi rakennukseen, toimistoon tai kotiin (Cisco 2020a, viitattu 23.5.2020).
NordVPN	NordVPN:n on opinnäytetyössä käytettävä VPN-palveluntarjoaja.
OpenVPN	OpenVPN on SSL-pohjainen salaus- ja todennusprotokolla (Aoki 2019, viitattu 14.5.2020).
Openwrt	OpenWrt on GNU/Linux-jakelu sulautetuille laitteille (OpenWrt 2020, viitattu 23.5.2020).
Raspberry Pi	Raspberry Pi on luottokortin kokoinen tietokone, jota käytetään esimerkiksi koodauksen opettelemiseen ja elektroniikkaprojektien rakentamiseen (Raspberrypi.org 2020a, viitattu 18.4.2020).
Reititin	Reititin yhdistää verkossa olevia laitteita välittämällä datapaketteja niiden välillä. Datapaketteja voidaan lähettää laitteiden välillä tai laitteista Internetiin. (Ellis 2019, viitattu 23.5.2020.)
Sulautettu laite	Sulautettu laite on erittäin erikoistunut laite, joka on tarkoitettu yhteen tai muutamaan erityistarkoitukseen. Sulautettu laite on yleensä sulautettu tai sisällytetty toiseen esineeseen tai osaksi suurempaa järjestelmää. (Techopedia 2020a, viitattu 24.5.2020.)
TCP	Transmission Control Protocol on tiedonsiirtoprotokolla, joka varmistaa datapakettien onnistuneen vaihdon laitteiden välillä verkon yli. TCP-yhteyden muodostaminen vaatii sekä asiakkaan, että palvelimen osallistuvan niin kutsuttuun kolmivaiheiseen kättelyyn. (Imperva 2020, viitattu 24.5.2020.)
UDP	User Datagram Protocol on tiedonsiirtoprotokolla, jota käytetään esimerkiksi videoiden toistamiseen ja DNS-hakuihin. UDP nopeuttaa viestintää, koska se ei vaadi niin kutsuttua kolmivaiheista kättelyä. Tämä mahdollistaa tiedon siirron ennen kuin vastaanottava osapuoli on suostunut viestintään. (Cloudflare 2020b, viitattu 24.5.2020.)
Verkkokortti	Verkkokortti eli verkkosovitin on komponentti, joka tarjoaa verkkoyhteyden tietokoneelle. Se voi mahdollistaa langallisen yhteyden (Ethernet) tai langattoman yhteyden (Wi-Fi) lähiverkkoon. (Mitchell 2020, viitattu 24.5.2020.)
VPN	Virtuaalinen erillisverkko eli Virtual Private Network on turvallinen, yksityinen yhteys laitteen ja päätepisteen tai määränpään välillä (Greenberg 2020, viitattu 25.4.2020).
Kiinteä yhteys	Kiinteä yhteys (leased line) on pysyvä tietoliikennekanava, joka yhdistää kahta tai useampaa sijaintia. Tämä on palvelusopimus asiakkaan ja palveluntarjoajan välillä. Se toimii erillisenä tunnelina pisteestä toiseen, jonka kautta tiedot voivat jatkuvasti kulkea kiinteää kuukausimaksua tai vuokraa vastaan. (Techopedia 2020b, viitattu 24.5.2020.)

3 VIRTUAALINEN ERILLISVERKKO

Virtuaalinen erillisverkko eli Virtual Private Network (VPN) luo turvallisen, salatun yhteyden vähemmän suojatussa verkossa, kuten julkisessa Internetissä. VPN käyttää tunnelointiprotokollia tietojen salaamiseen lähetyspäässä ja salauksen purkamiseen päätepisteessä. Lisäsuojauksen tarjoamiseksi myös alkuperäiset ja vastaanottavat verkko-osoitteet ovat salattuja. (Rouse 2020, viitattu 11.4.2020.) VPN on pohjimmiltaan turvallinen kanava (tunneli) kahden laitteen tai päätepisteen välillä. VPN-päätepisteet salaavat koko alkuperäisen IP-paketin. Salauksen takia alkuperäisen paketin sisältöä ei saada selville, vaikka joku näkisikin paketin kopion, kun se kulkee verkon läpi. (Free CCNA Study Guide 2020, viitattu 12.1.2020.)

VPN-yhteyksiä voidaan käyttää esimerkiksi seuraavissa tarkoituksissa:

- Pankkiautomaateissa: Pankkiautomaatit voivat luoda turvallisemman yhteyden pankkijärjestelmiin VPN-yhteyden avulla.
- Julkisissa langattomissa verkoissa: Käyttäjä voi suojata oman verkkoliikenteensä muilta.
- Yritysverkoissa: Yritykset ja muut organisaatiot voivat käyttää VPN-yhteyttä useiden toimipisteiden tai kokonaisten palvelinkeskusten yhdistämiseen.
- Sijaintipohjaisissa palveluissa: Jotkin verkkosivustot tarjoavat sisältöä maantieteellisen sijainnin perusteella käyttämällä GeoIP-tietokantoja ja muita tietueita. Internet-videopalvelut, kuten Hulu, YouTube ja Netflix ovat yleisiä esimerkkejä sijaintipohjaisista palveluista.
- Sensuurin ohittamisessa: Joissakin maissa, kuten esimerkiksi Kiinassa Internetin käyttöä on rajoitettu erilaisten sääntöjen ja seurannan avulla. VPN-yhteys voi auttaa pääsemään rajoittavien sääntöjen ulkopuolelle käyttämään Internettiä vapaasti. (Crist & Keijser 2015, 19-20.)

VPN:ät voidaan jakaa yrityskäytössä ja yksityiskäytössä oleviin. Yrityskäytössä olevia VPN:iä ovat esimerkiksi etäyhteys VPN ja site-to-site VPN. Yksityiskäytössä käytetään yleensä erilaisia maksullisia tai ilmaisia VPN-palveluntarjoajien palveluita.

3.1 Erilaiset VPN-ratkaisut

3.1.1 VPN-ratkaisut yrityskäyttöön

Organisaatiot ottavat käyttöön VPN:iä tietojen eheyden, todennuksen ja tietojen salauksen aikaansaamiseksi suojaamattoman verkon tai Internetin kautta lähetettyjen pakettien luottamuksellisuuden varmistamiseksi. VPN suunniteltiin alun perin tarpeettomien kiinteiden yhteyksien (leased line) kustannuksien välttämiseksi. Nykyään VPN:illä on kuitenkin kriittinen rooli turvallisuudessa ja joissain tapauksissa yksityisyydessä. (Santos 2020, 467.)

VPN:ät ovat olemassa, jotta tietoja olisi mahdollista siirtää kahden verkon välillä tehokkaasti, salaisesti ja yksityisesti verkkojen välisestä yhteisestä, jaetusta ja erikseen ylläpidetystä infrastruktuurista. Tämän tehtävän suorittamiseksi on neljä tavoitetta, jotka luotettavan VPN-toteutuksen tulee täyttää:

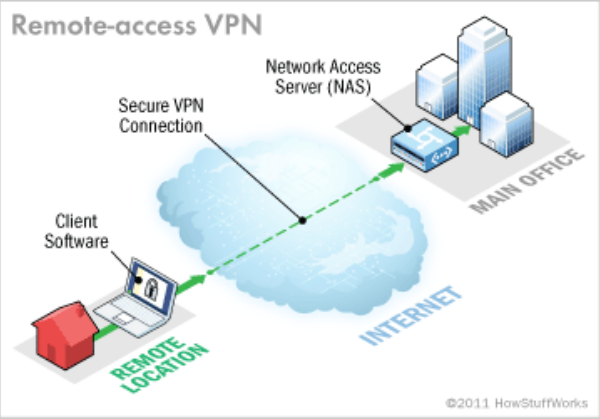
- Tietojen luottamuksellisuus: Suojaa viestin sisällön todentamattomien tai luvattomien lähteiden tulkinnalta.
- Tietojen eheys: Takaa sen, että viestin sisältöä ei ole peukaloitu tai muutettu tiedon kulun aikana lähteestä määränpäähän.
- Lähettäjän kiistämättömyys: Keino estää lähettäjää kieltämästä lähettäneensä viestin vastaanottajalle.
- Viestin todennus: Varmistaa, että viesti on lähetetty aidosta lähteestä ja, että viestit lähetetään aitoihin kohteisiin. (Carmouche 2006, 6.)

VPN:n avulla voi laajentaa yritysverkkoa Internetin välityksellä muodostettujen salattujen yhteyksien avulla. Koska liikenne on salattu laitteen ja verkon välillä, voi työntekijä työskennellä toimiston ulkopuolella ja olla silti turvallisesti yhteydessä yritysverkkoon. (Cisco 2020b, viitattu 25.4.2020.)

3.1.1.1.1 Etäyhteys VPN

Etäyhteys (remote access) VPN:n avulla yksittäinen käyttäjä voi luoda turvallisen yhteyden yrityksen verkkoon. Käyttäjä voi yhteyden luomisen jälkeen käyttää yrityksen resursseja samalla tavalla kuin hän olisi suoraan yhteydessä yrityksen verkkoon. (Tyson, Pollette, & Crawford 2019a, viitattu 27.10.2019.)

Etäyhteys VPN:n sopii hyvin etätyötä tekeville, matkapuhelimen käyttäjille tai ekstranetin käyttäjille. Yhteys käyttäjän ja yritysverkon välillä tapahtuu Internetin kautta. Etäyhteys VPN:n käyttö voi vaatia erillisen VPN-asiakasohjelmiston asentamista, tai käyttäjä voi joutua käyttämään verkkopohjaista asiakasohjelmistoa. VPN-asiakasohjelmisto muodostaa suojatun tunnelin VPN-palvelimen kanssa ja kapseloi sekä salaa tiedot ennen niiden lähettämistä Internetin välityksellä VPN-palvelimelle. (Chauhan 2018, 261.)

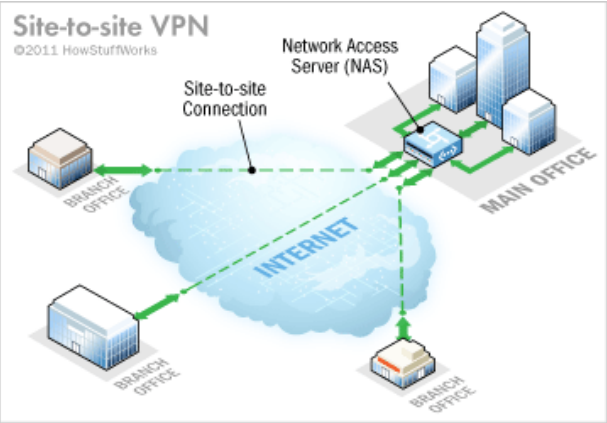


KUVIO 1. Miten etäyhteys VPN toimii (Tyson, Pollette, & Crawford 2019a, viitattu 27.10.2019.)

3.1.1.1.2 Site-to-site VPN

Site-to-site VPN:n avulla yritys, jolla on toimipisteitä useissa paikoissa, voi luoda turvallisia yhteyksiä näiden toimistojen eri lähiverkkojen välille Internetin välityksellä. Site-to-site VPN voi esimerkiksi yhdistää sivutoimipisteen lähiverkon yrityksen pääkonttorin pääverkkoon. (vpnMentor 2020, viitattu 18.4.2020.)

Site-to-site VPN:iä on olemassa Intranet- ja Extranet-pohjaisia. Intranet-pohjaisia site-to-site VPN-ratkaisuja käytetään yhdistämään yrityksen useiden toimipisteiden lähiverkot yhteen laajaverkkoon. (Tyson, Pollette, & Crawford 2019b, viitattu 10.5.2020.) Ekstranet-pohjainen site-to-site VPN-ratkaisu antaa yritykselle mahdollisuuden käyttää julkista Internettiä lähiverkon yhdistämiseen muiden yritysten, asiakkaiden tai yhteisöjen lähiverkkoihin. Tämän avulla yritys voi jakaa tarpeellisia tietoja kumppaneidensa kanssa, ja samalla suojata lähiverkkonsa (intranet) niiltä. (Skoler 2020, viitattu 10.5.2020.)



KUVIO 2. Miten site-to-site VPN toimii (Tyson, Pollette, & Crawford 2019b, viitattu 27.10.2019)

3.1.2 VPN-palvelu yksityiskäyttöön

Yksityiskäyttöön tarkoitetut VPN-palvelut tarjoavat verkkoliikenteen turvallista välittämistä oman verkkonsa kautta. Tämän etuna on, että kaikki lähettämäsi ja vastaanottamasi tiedot ovat piilossa paikallisissa verkoissa. Tämän takia tietosi ovat paremmin turvassa lähellä olevilta rikollisilta, epäluotettavilta paikallisilta Internet-palveluntarjoajilta tai muilta, jotka mahdollisesti vakoilevat paikallisessa verkossa. (SURVEILLANCE SELF-DEFENSE 2019, viitattu 27.10.2019.)

VPN-palveluiden hyviin puoliin kuuluu esimerkiksi julkisten langattomien verkkoyhteyksien turvallinen käyttö, mahdollisen geoblokkauksen ohittaminen, sensuurin torjuminen ja oman sijainnin salaaminen. VPN-palvelun avulla on mahdollista rajoittaa Internet-palveluntarjoajan saamaa tietoa verkkoliikenteestäsi. Internet-palveluntarjoaja näkee VPN-yhteyttä käytettäessä vain, että käyttäjä on yhdistänyt Internettiin VPN-yhteyttä käyttäen. (Hoffman 2019, viitattu 1.3.2020.)

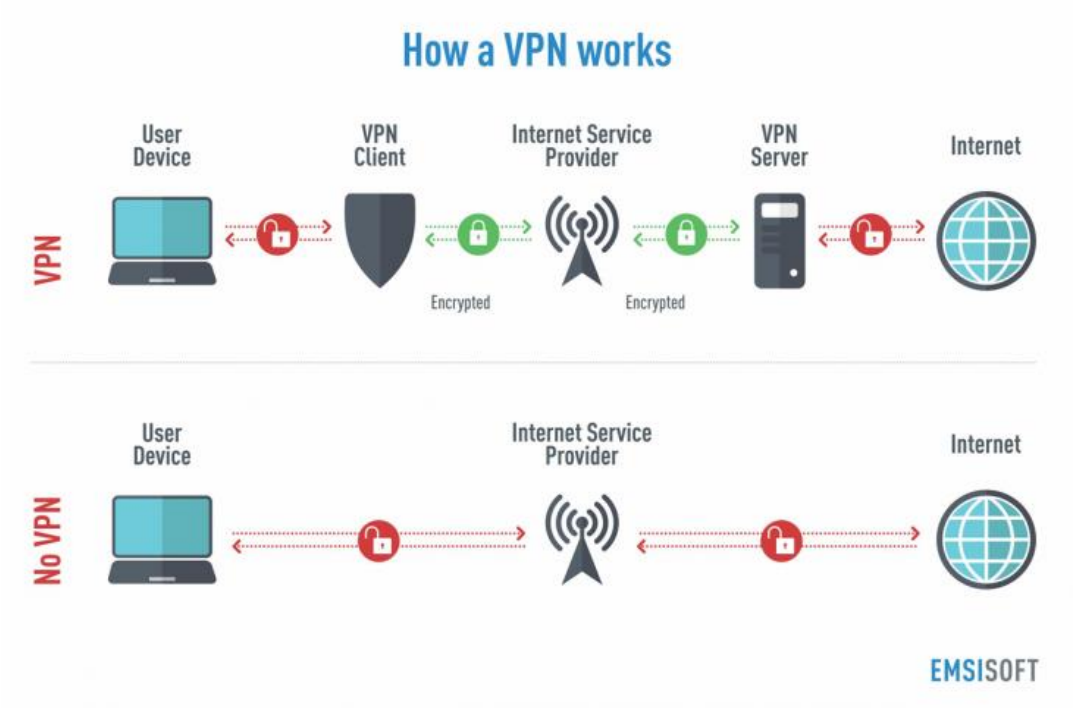
VPN-palveluissa on kuitenkin joitakin huonojakin puolia, joihin kuuluu esimerkiksi verkkoyhteyden hidastuminen ja mahdollisuus, että osa verkkosivuista ei päästä yhdistämään sivulle VPN-yhteyden ollessa käytössä. Osassa maissa kuten esimerkiksi Venäjällä ja Kiinassa on laillista käyttää vain hallituksen hyväksymiä VPN-palveluita. Vaikka Internet-palveluntarjoaja ei näe, että mitä teet verkossa VPN-yhteyttä käytettäessä, voi VPN-palveluntarjoajasi mahdollisesti pitää lokeja verkon käytöstä. VPN-palveluntarjoajan lupaus lokien pitämättömyydestä jää käyttäjän oman luottamuksen varaan, joten VPN-palveluntarjoajaksi kannattaa valita hyvän maineen omaava VPN-palveluntarjoaja. (Marks 2020, viitattu 15.5.2020.)

VPN-palvelua valittaessa kannattaa kiinnittää huomiota siihen, että missä maassa VPN-palveluntarjoaja sijaitsee. VPN-palveluntarjoajille parhaita sijainteja ovat maat, joissa hallitus ei vaadi lokien säilyttämistä. Lisäksi on paljon turvallisempaa, jos VPN-palveluntarjoaja sijaitsee maassa, jossa on tiukat tietosuojalait. (Walsh 2018, viitattu 15.5.2020.)

VPN-palveluista on olemassa ilmaisversioita. Yleensä ilmaisversioita ei kannata kuitenkaan käyttää sen takia, että ”maksuna” saattaa toimia käyttäjän henkilökohtaiset tiedot, joita ilmaisversiota tarjoava saattaa myydä eteenpäin eniten maksavalle taholle. Ilmaiset VPN-palvelut voivat esimerkiksi pitää lokeja ja seurata kaikkea käyttämääsi sisältöä, IP-osoitteitasi, käyttämiäsi verkkosivustoja jne. Toisin sanoen ilmaiset VPN-palvelut voivat toimia vastoin sitä, miltä VPN-palveluiden olisi tarkoitus suojata käyttäjiään. Ilmaisversioiden huonoja puolia ovat tietojen seurannan lisäksi esimerkiksi mahdolliset mainokset, hidas ja epävakaa yhteys, mahdolliset tiedonkäyttörajoitukset sekä vanhentuneet salaukset. (Levavi-Eilat 2020, viitattu 1.3.2020.)

Jos kuitenkin aikoo käyttää VPN-palvelun ilmaisversioita kannattaa yleensä valita vaihtoehdoksi sellainen VPN-palveluntarjoaja, joka omaa luotettavan maineen sekä tarjoaa maksullista VPN vaihtoehtoa. On todennäköisempää, että luotettavan maineen omaava VPN-palveluntarjoajan ei halua esimerkiksi myydä käyttäjiensä tietoja eteenpäin, vaan toivoo, että ilmaisversioon tyytyväinen käyttäjä haluaa siirtyä maksulliseen versioon testattuaan VPN-palvelun toimivaksi.

Tässä opinnäytetyössä tehtävässä kehitystehtävässä käytetään NordVPN nimisen VPN-palveluntarjoajan VPN-palvelua. NordVPN valittiin kehitystehtävään, koska se on yksi parhaita arvosteluita saaneita VPN-palveluita, eikä NordVPN säilytä heidän mukaansa käyttölokeja.



KUVIO 3. Yksityiskäyttöön tarkoitettu VPN-yhteys vastaan ei VPN-yhteyttä (Haylee 2017, viitattu 27.10.2019)

3.2 Erilaisia VPN protokollia

3.2.1 Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) protokollan ovat kehittäneet Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics ja U.S. Robotics. PPTP perustuu puhelinverkkoyhteyksissä käytettyyn Point-to-Point Protocol (PPP) standardiin, joka antaa kaikille PPP-asiakasta käytäville mahdollisuuden käyttää Internet-palveluntarjoajaa Internet yhteyden muodostamiseen. PPTP kehittää PPP:n toiminnallisuutta antamalla käyttäjille mahdollisuuden muodostaa turvallisia yhteyksiä VPN:n kautta esimerkiksi heidän työnantajansa tai liikekumppaninsa suojattuihin verkkoihin. (Thomas & Stoddard 2011, 177.)

PPTP on edelleen suosittu verkkoprotokolla etenkin Windows-tietokoneissa, ja se on yksi vanhimmista protokollista, joita edelleen käytetään. PPTP on sisällytetty Windowsiin vuodesta 1995 lähtien, ja se on edelleen mukana useimmissa käyttöjärjestelmissä. Nykyään PPTP:tä pidetään pohjimmiltaan turvattomana, koska yhteyden turvallisuuden vahvuus liittyy suoraan valitun todennusmekanismin (esimerkiksi salasanan) vahvuuteen. Täten turvaton salasana johtaa turvattomaan

VPN-yhteyteen. (Crist & Keijser 2015, 6.) PPTP käyttää taustalla olevia todennusprotokollia, kuten MS-CHAP (Challenge Handshake Authentication Protocol (CHAP)) v1/v2, joihin kohdistuu vakavia tietoturva-aukkoja. PPTP VPN salaa tiedot käyttämällä 128-bittistä salausta, mikä tekee siitä nopeimman, mutta turvallisuuden kannalta heikoimman VPN-protokollan. (Chauhan 2018, 263.)

3.2.2 Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec)

Layer 2 Tunneling Protocol (L2TP) julkaistiin vuonna 1999. Se on suunniteltu eräänlaiseksi PPTP:n seuraajaksi, ja sen ovat kehittäneet Microsoft ja Cisco. Protokolla ottaa erilaisia ominaisuuksia Microsoftin PPTP:stä ja Ciscon L2F (Layer 2 Forwarding) protokollasta ja parantaa niitä. (Mocan 2016, viitattu 12.5.2020.) L2TP ei yksin tarjoa luottamuksellisuutta tai salausominaisuuksia, joten yhteyden turvaamiseksi käytetään toista Internet Protocol Security (IPSec) nimistä protokollaa (Chauhan 2018, 263.)

L2TP on sisäänrakennettu melkein kaikkiin nykyaikaisiin käyttöjärjestelmiin ja VPN-yhteensopiviin laitteisiin, joten sen käyttöönotto on yhtä helppoa kuin PPTP:n. L2TP/IPsec kapseloi tiedot kahdesti, mikä hidastaa asioita. Tätä kompensoi se, että salaus/salauksen purku tapahtuu ytimessä (kernel) ja L2TP/IPsec sallii monisäikeistämisen, jota esimerkiksi OpenVPN ei salli. Tuloksena on, että L2TP/IPsec on teoriassa nopeampi kuin OpenVPN. AES salausta käyttävällä L2TP/IPsec:llä ei ole merkittäviä tunnettuja haavoittuvuuksia ja, jos se on asianmukaisesti toteutettu, se voi olla silti turvallinen vaihtoehto. Edward Snowdenin paljastukset ovat kuitenkin viitanneet voimakkaasti siihen, että National Security Agency (NSA) on murtanut salauksen. (Crawford 2019, viitattu 13.5.2020.)

3.2.3 Internet Key Exchange Version 2 (IKEv2)

Internet Key Exchange version 2 (IKEv2) on Microsoftin ja Ciscon yhdessä kehittämä. Sitä tukevat natiivisti Windows 7 sekä sitä uudemmat Windows versiot, Blackberry ja iOS. Tästä syystä monet iOS VPN-palvelut käyttävät IKEv2:ta OpenVPN:n sijaan. (Crawford 2019, viitattu 13.5.2020.) IKEv2 on etenkin hyödyllinen 3G tai 4G LTE-laitteille, koska se on hyvä yhdistämään aina uudelleen, kun yhteys katkeaa. Näin voi tapahtua esimerkiksi, kun käyttäjä ajaa tunnelin läpi ja menettää väliaikaisesti palvelun tai, kun siirrytään mobiiliyhteydestä langattomaan verkko yhteyteen. (Bischoff 2019, viitattu 13.5.2020.)

IKEv2 ei ole yhtä yleinen kuin L2TP/IPSec, koska sitä tuetaan harvemmilla alustoilla. Sitä pidetään kuitenkin vähintään yhtä hyvänä, ellei jopa parempana kuin L2TP/IPsec turvallisuuden, suorituskyvyn (nopeuden), vakauden ja yhteyden muodostamisen sekä palauttamisen suhteen. (Crawford 2019, viitattu 13.5.2020.)

3.2.4 OpenVPN

OpenVPN-projektin perusti James Yonan, joka on OpenVPN Technologies yrityksen perustaja ja teknologiajohtaja. Alun perin vuonna 2001 julkaistu OpenVPN on SSL-pohjainen salaus- ja todennusprotokolla, joka julkaistiin GNU GPL-lisenssin alaisena. (Aoki 2019, viitattu 14.5.2020.) Yksi syy OpenVPN:n suosioon on se, että siitä löytyy tuki kaikkiin merkittävimpiin käyttöjärjestelmiin, kuten esimerkiksi Windows-, MacOS- ja Linux-työpöytäalustoihin sekä Android- ja iOS-mobiiliympäristöihin. OpenVPN ei kuitenkaan ole osana mitään käyttöjärjestelmää, kuten esimerkiksi PPTP tai L2TP ovat, vaan sen käyttämiseen tarvitsee kolmannen osapuolen ohjelmiston. (Bozovic 2019, viitattu 14.5.2020.)

OpenVPN käyttää avoimen lähdekoodin tekniikoita, kuten OpenSSL-salauskirjastoa. OpenVPN voidaan määrittää toimimaan missä tahansa portissa, joten palvelimen voi määrittää toimimaan TCP-portin 443 yli. OpenSSL VPN-liikenne olisi tällöin käytännössä katsoen mahdoton erottaa tavallisesta HTTPS-liikenteestä, joka esiintyy, kun muodostaa yhteyden suojattuun verkkosivustoon. Tästä syystä OpenVPN:ää on vaikea estää kokonaan. OpenVPN on hyvin konfiguroitavissa, ja se on turvallisin vaihtoehto, jos se on asetettu käyttämään AES-salausta heikomman Blowfish-salauksen sijaan. Tällä hetkellä ei ole todisteita siitä, että OpenVPN olisi murrettu NSA:n tai kenenkään muun toimesta. (Hoffman 2018, viitattu 14.5.2020.)

Tässä opinnäytetyössä käytetään OpenVPN-protokollaa, koska se on hyvin mukautuva avoimen lähdekoodin ratkaisu, joka on yksi turvallisimmista VPN-protokollista, eikä sen murtamisesta ole todisteita tällä hetkellä.

4 RASPBERRY PI

4.1 Yleistietoa

Raspberry Pi on pieni, tehokas ja edullinen yhden piirilevyn tietokone, jonka Raspberry Pi-säätiö on kehittänyt. Raspberry Pi suunniteltiin koulutuslaitteeksi, ja sen innoituksena toimi BBC Micro yrityksen menestys tietokoneohjelmoinnin opettamisessa kokonaiselle sukupolvelle. Raspberry Pi-säätiö ryhtyi tekemään samoin nykymaailmassa, missä ei tarvitse osata kirjoittaa ohjelmistoja tietokoneen käyttämistä varten. (Harrington 2015, 6.)

4.2 Historiaa

Raspberry Pi:n tarina alkoi Cambridgen yliopiston tietokonelaboratoriossa vuonna 2006. Eben Upton, Rob Mullins, Jack Lang ja Alan Mycroft, olivat huolestuneita siitä, että tulevat tietotekniikan perustutkintoa suorittaneet opiskelijat olivat eriytyneet tietojenkäsittelyn teknisistä näkökohdista. Tämä johtui pitkälti kouluopetuksesta, jossa painotettiin tietokoneiden käyttöä sen ymmärtämisen sijaan. (Dennis 2016, 2.)

Tämän alkuperäisen huolenaiheen takia vuoden 2009 alussa Eben Upton, Pete Lomas, Alan Mycroft, David Braben, Jack Lang ja Rob Mullins perustivat Raspberry Pi-säätiön. Hyväntekeväisyysjärjestön, joka keskittyy antamaan ihmisille maailmanlaajuisesti tietoa ja työkaluja tietokoneohjelmistojen sekä laitteistojen luomiseen. (Heath 2018, viitattu 5.10.2019.)

Seuraavien vuosien aikana Raspberry Pi-säätiö kehitti halpaa ja helppokäyttöistä laitetta, joka auttaisi kouluja opettamaan käsitteitä, kuten ohjelmointia, tuoden oppilaat lähemmäksi tietotekniikan toiminnan ymmärtämistä. Raspberry Pi:n alkuperäinen kaupallinen julkaisu tapahtui helmikuussa vuonna 2012. (Dennis 2016, 2.)

4.3 Erilaiset mallit

Raspberry Pi-malleja on olemassa monia erilaisia. Mallit jaetaan A-, B-, Compute- ja Zero-malleihin. Mallien erot näkyvät Raspberryn koossa, painossa, muistin määrässä, prosessorin nopeudessa ja verkko-ominaisuuksissa. (Maker.io 2018, viitattu 9.2.2020.) Opinnäytetyön liitteissä oleva taulukko 1 sisältää tarkempia tietoja eri malleista. Alla olevassa kuviossa 4 on kuvattuna suurin osa eri Raspberry Pi-malleista, mutta siitä puuttuu uusin Raspberry Pi 4 B-malli.

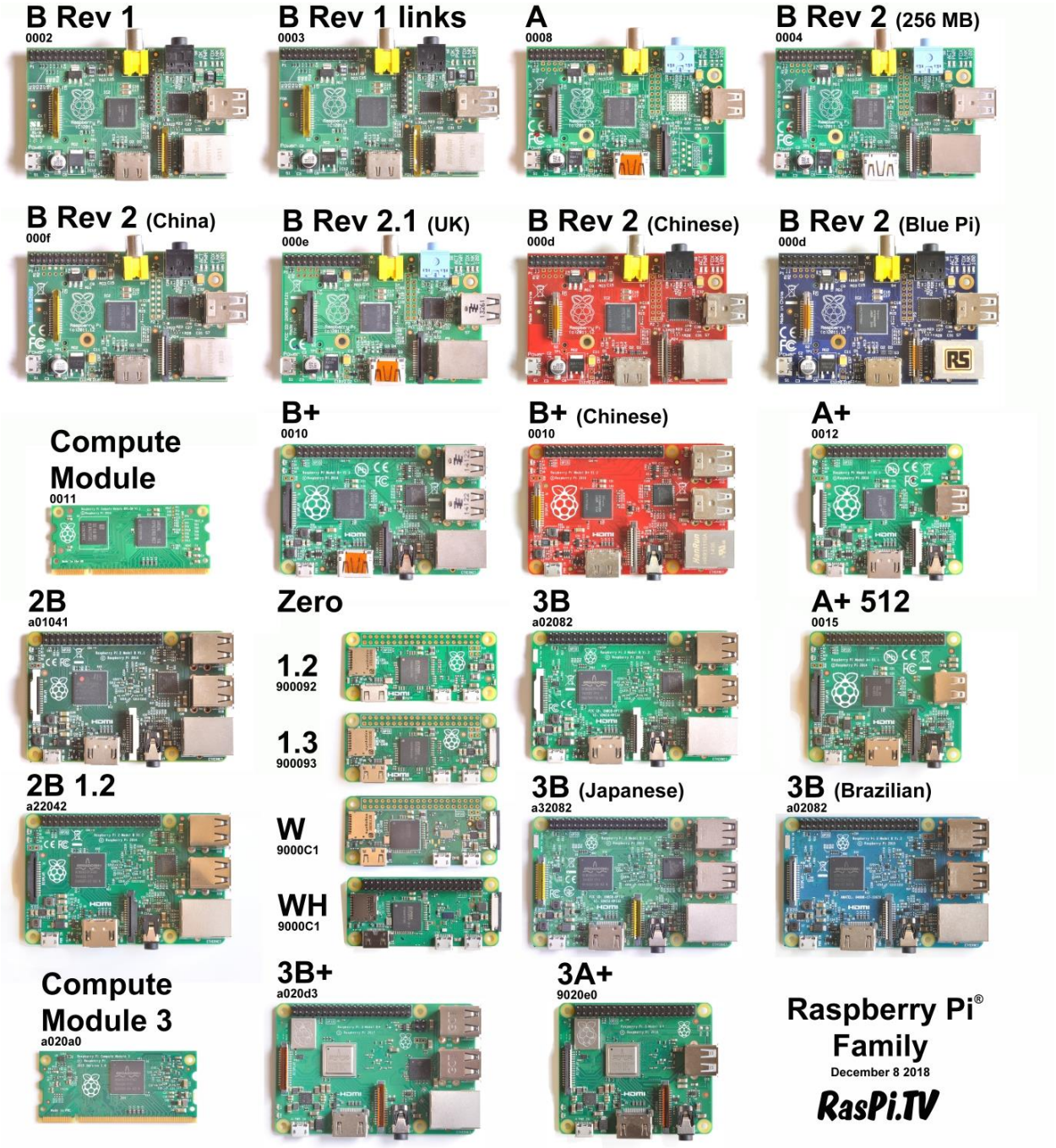
A-malli ostetaan yleensä sulautettuihin projekteihin. A-mallissa on vähemmän USB-portteja kuin B-mallissa, eikä siinä ole Ethernet-porttia. A-malli on kevyempi ja kuluttaa vähemmän virtaa kuin B-malli. A-malleja käytetään paljon robotiikassa ja projekteissa, joissa paino ja pieni virrankulutus ovat ensiarvoisen tärkeitä. (Raspberrypi.org 2020b, viitattu 14.5.2020.)

B-mallia voidaan käyttää projektiin, jossa hinta tai koko ei ole esteenä. B-malli on tehokkain ja iso kokoisin (noin luottokortin kokoinen) Raspberry Pi-malleista. B-malli sisältää eniten USB-portteja, RAM-muista ja tehokkaimman prosessorin, joten se soveltuu hyvin kaikenlaisiin projekteihin. (Maker.io 2018, viitattu 14.5.2020.)

Compute-malli, jota ei löydy liitteenä olevasta taulukosta on laskentamoduuli, joka on tarkoitettu teolliseen käyttöön. Se on pieni laite, joka kytkeytyy esimerkiksi teollisuustuotteen sisällä olevaan piirilevyyn, ja antaa valmistajille helpon tavan käyttää Raspberry Pi-ekosysteemiä omissa laitteissaan. (Raspberrypi.org 2020a, viitattu 9.2.2020.)

Zero-malli on erittäin edullinen ja karsittu versio B-mallista. Zero-malli on suunniteltu esimerkiksi sulautettuihin sovelluksiin ja prototyyppien suunnitteluun. Zero-malli on hitaampi ja tehottomampi kuin muut nykyiset Raspberry Pi-mallit, mutta se tarvitsee vähiten virta. Zero-mallissa ei ole Ethernet-porttia. (The Pi Hut 2017, viitattu 14.5.2020.) Zero-malli on noin puolet pienempi kuin A-malli.

Tässä opinnäytetyössä käytetään Raspberry Pi 3 B+ mallia. Opinnäytetyössä käytetään uusimman 4 B-mallin sijaan 3 B+ mallia, koska opinnäytetyön aloituksen aikaan 4 B-mallin saatavuus oli huono Suomessa.



KUVIO 4. Suurin osa erilaisista Rasperry Pi-malleista (Raspberry Pi 4 B-malli puuttuu) (RasPi.TV 2018, viitattu 9.2.2020)

4.4 Raspberry VPN

Raspberry Pi VPN on hyvä vaihtoehto, jos haluaa suojata kaikki omassa verkossa olevat laitteet VPN-yhteyden avulla ilman, että jokainen laite tarvitsee yhdistää erikseen VPN-sovelluksen kautta.

Osaa laitteista ei ole edes mahdollista yhdistää VPN-sovelluksen kautta VPN-yhteyteen esimerkiksi älytelevisioita ja pelikonsoleita. Toinen ratkaisu on ostaa reititin, jolla on mahdollista muodostaa yhteys suoraan VPN-palveluun. Voi olla kuitenkin halvempaa ja mahdollisesti yksinkertaisempaa vain reitittää kaikki liikenne Raspberry Pi:n kautta, joka on aina yhteydessä VPN:ään. (Oxford 2019, viitattu 14.5.2020.)

VPN-palveluntarjoajat mahdollistavat yleensä useamman kuin yhden laitteen käyttämisen samanaikaisesti yhdellä VPN-tilauksella. Jos VPN-yhteyden luo koko verkolle esimerkiksi Raspberry Pi:n tai reitittimen avulla, niin se lasketaan vain yhdeksi laitteeksi, vaikka sen läpi kulkisikin esimerkiksi viiden muun laitteen verkkoliikenne.

5 MAHDOLLISET LINUX-JAKELU VAIHTOEHDOT

Linus Torvalds aloitti Linuxin kehittämisen opiskellessaan Helsingin yliopistossa vuonna 1991. Hän halusi luoda UNIX-tyyppisen käyttöjärjestelmäytimen, jotta hän voisi käyttää kotitietokoneessaan samanlaista käyttöjärjestelmää, jota hän käytti koulussa. Tuolloin Linus käytti Minix-käyttöjärjestelmää, mutta hän halusi ylittää sen, mitä Minix-standardit sallivat. Linux-ydin oli viimeinen ja tärkein koodi, jota tarvittiin UNIX-tyyppisen käyttöjärjestelmän kokoamiseen GPL:n alaisuuteen. Kun jakeluita alettiin koota, niin Linux nimi tarttui eikä GNU. Jotkut jakelut, kuten Debian, viittaavat kuitenkin itseensä GNU/Linux-jakeluna. (Negus 2015, 13-14.)

Linuxista puhutaan monesti kuin se olisi vain pelkästään yksi saatavilla oleva käyttöjärjestelmä, kuten esimerkiksi Windows tai macOS ovat. Tämä ei kuitenkaan pidä paikkaansa, koska Linux-jakeluita on saatavilla satoja erilaisia. Jokainen Linux-jakelu koostuu Linux-ytimestä, joukosta apuohjelmia ja konfigurointitiedostoja. Näiden yhdistämisen tuloksena syntyy kokonainen Linux-käyttöjärjestelmä. Kaksi Linux-jakelua voivat erota toisistaan yhtä paljon kuin esimerkiksi Windows- ja macOS-käyttöjärjestelmät eroavat toisistaan. (Bresnahan & Blum 2015, 13.)

5.1 Raspbian

Raspbian on avoimen lähdekoodin Debianiin pohjautuva jakelu, jota kehittävät pääasiassa Mike Thompson ja Peter Green. Raspbian-projektilla ei ole yhteyttä Raspberry Pi -säätiöön, mutta se on Raspberry Pi:n virallinen käyttöjärjestelmä. (Connor 2019, viitattu 15.5.2020.) Raspbian on rakennettu erityisesti Raspberry Pi:tä varten. Tämä on yksi syistä, miksi Raspbian on yksi eniten käytetyistä Raspberry Pi-jakeluista. (Klosowski 2016, viitattu 15.5.2020.)

5.2 Openwrt

OpenWrt on GNU/Linux-jakelu sulautetuille laitteille (yleensä langattomille reitittimille). OpenWrt on rakennettu alusta alkaen täysin varustelluksi, helposti muokattavaksi käyttöjärjestelmäksi sulautetuille laitteille. Käytännössä tämä tarkoittaa, että käyttäjällä voi olla kaikki tarvitsemansa ominaisuudet ilman mitään ylimääräistä. (OpenWrt 2020, viitattu 23.5.2020.)

OpenWrt tarjoaa täysin kirjoitettavan tiedostojärjestelmän valinnaisella paketinhallinnalla. Tämä vapauttaa käyttäjän valmistajan tarjoamien sovelluksien valinnan ja määrityksien rajoituksista sekä antaa mahdollisuuden mukauttaa sulautettua laitetta pakettien avulla mihin tahansa käyttöön. Kehittäjille OpenWrt tarjoaa kehyksen sovelluksen rakentamiseen ilman, että kehittäjän tarvitsee rakentaa täydellistä laiteohjelmistoa sen ympärille. Käyttäjille tämä tarkoittaa täyden mukauttamisen vapautta, joka mahdollistaa sulautetun laitteen käytön tavoilla, joita valmistaja ei koskaan osannut kuvitellakaan. (OpenWrt 2020, viitattu 23.5.2020.)

OpenWrt valittiin käyttöjärjestelmäksi tässä opinnäytetyössä, koska se on hyvin mukautuva erilaisiin käyttötarkoituksiin, kevyt ja se mahdollistaa hallinnan web-käyttöliittymän kautta.

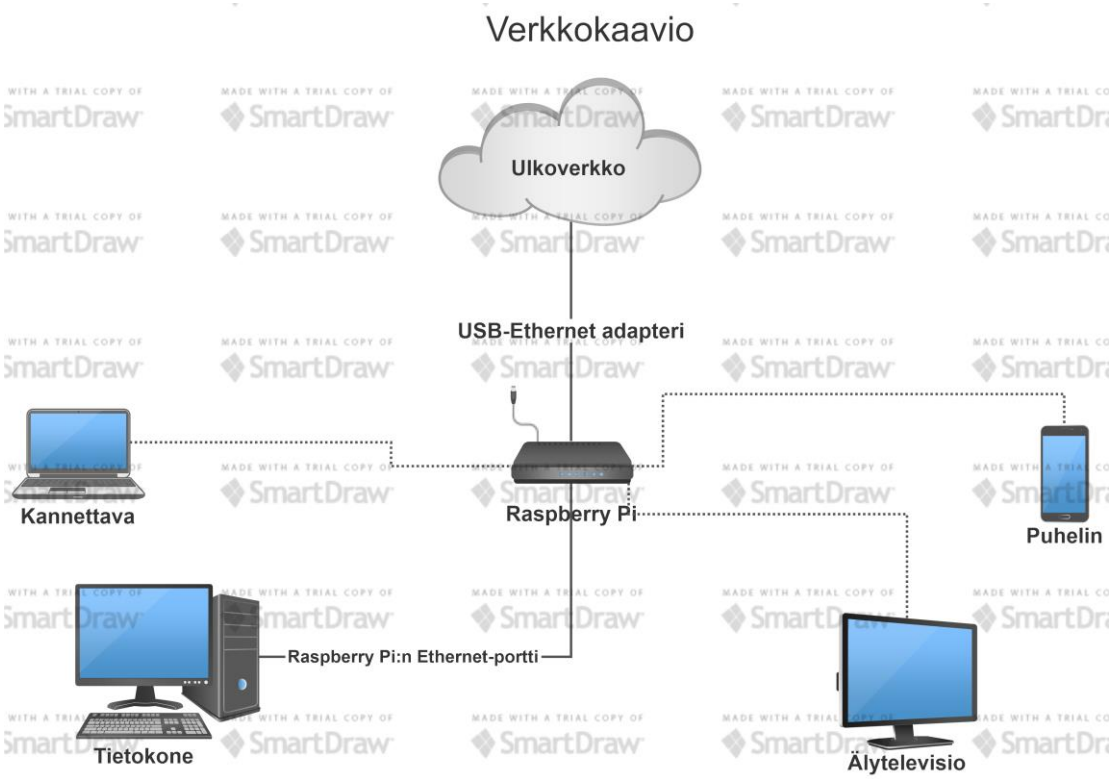
6 RASPBERRY PI VPN REITITTIMEN TOTEUTUS

Kehitystehtävässä luotiin kahta Ethernet-verkkokorttia (USB-Ethernet adapteria ja Raspberry Pi:n omaa Ethernet-porttia) sekä langatonta verkkoa käyttävä VPN-reititin Raspberry Pi:n avulla. Tavoitteena oli luoda mahdollisimman helppokäyttöinen ja halpa ratkaisu, jota voitaisiin hyödyntää yksityiskäytössä. Kaiken verkkoliikenteen oli tarkoitus kulkea Raspberry Pi:n kautta. Tarkoituksena oli saada VPN:n avulla lisää suojaa ja yksityisyyttä koko verkolle, eikä vain yhdelle laitteelle. Opinnäytetyössä käytettiin OpenWrt-käyttöjärjestelmää ja OpenVPN-protokollaa.

Opinnäytetyössä käytetyt laitteet, tarvikkeet ja ohjelmat:

- Raspberry Pi 3 B+ malli.
    - Raspberry Pi virtalähde.
    - Muistikortti ja muistikortinlukija.
- StarTech.com USB 3.0 to Gigabit Ethernet Adapter (malli USB31000S).
- Kaksi Verkkokaapelia (tietokoneeseen ja ulkoverkkoon).
- Käytin reititintä (ASUS RT-N18U) toteutuksessa, mutta ratkaisun voi tehdä ilman sitäkin yhdistämällä Raspberry Pi:n näppäimistöön, näyttöön ja suoraan ulkoverkkoon.
- Käytetyt ohjelmat: Etcher, PuTTY ja WinSCP.

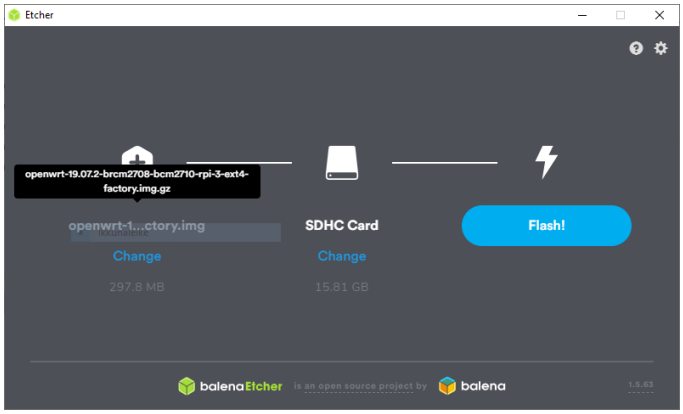
KUVIO 5. Kuva opinnäytetyössä käytetyistä laitteista ja tarvikkeista



KUVIO 6. Verkkokaavio yhdistetyistä laitteista

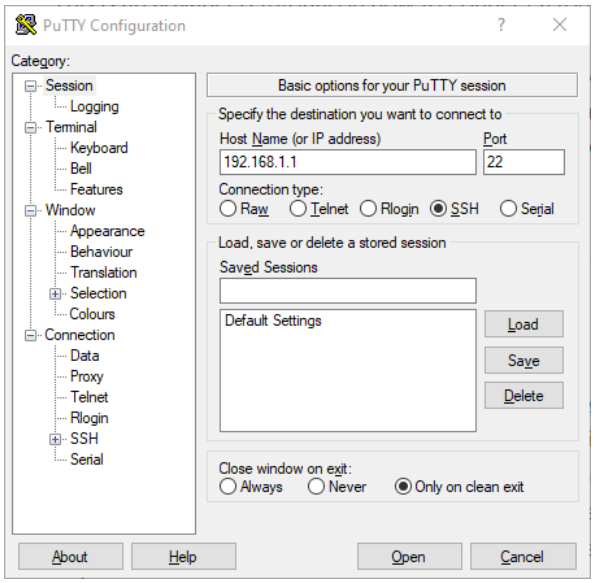
6.1 Raspberry Pi reitittimen luominen

Ladataan OpenWrt verkkosivulta uusin OpenWrt-versio openwrt-19.07.2-brcm2708-bcm2710-rpi-3-ext4-factory.img.gz tiedosto. Puretaan .img tiedosto ja kirjoitetaan OpenWrt Etcher-ohjelman avulla muistikortille.



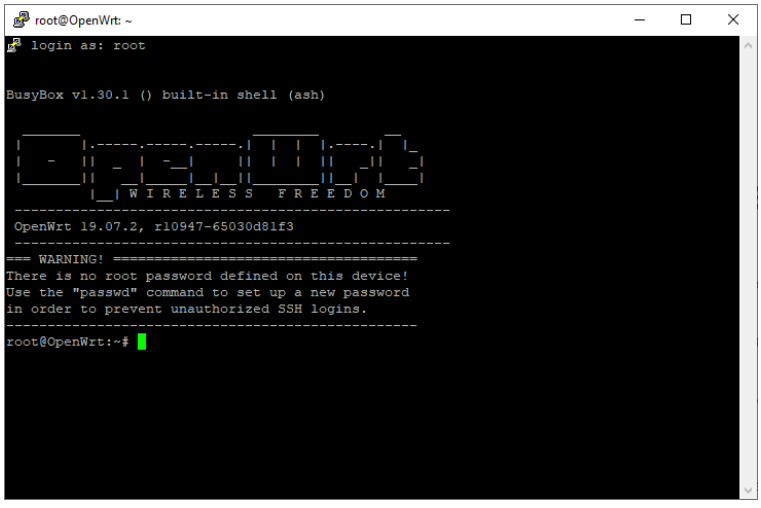
KUVIO 7. OpenWrt:n kirjoittaminen muistikortille Etcher-ohjelman avulla

Yhdistetään Raspberry Pi tietokoneeseen Raspberry Pi:ssä olevan Ethernet-portin kautta. OpenWrt:n alkuasetuksena IP-osoite on 192.168.1.1, joten sitä ei voi yhdistää suoraan omaan reitittimeeni, koska sen IP-osoite on sama 192.168.1.1.



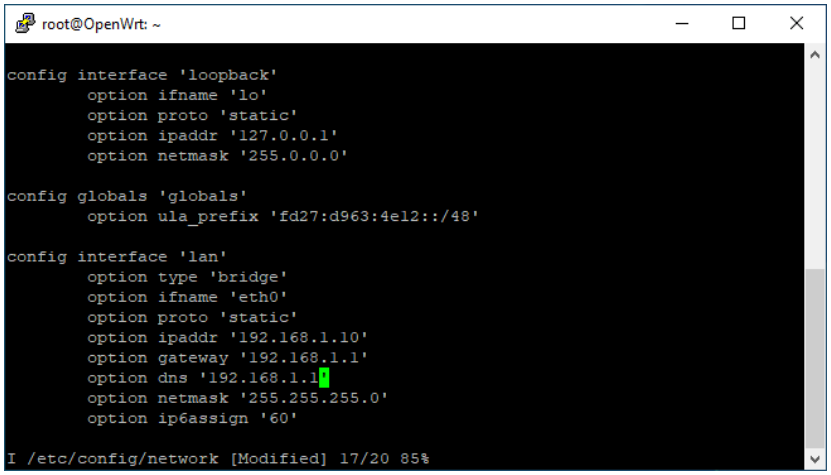
KUVIO 8. Yhdistetään PuTTY:llä Raspberry Pi:hin

Yhdistämisen jälkeen kirjaudutaan sisään root-käyttäjätunnuksella. Ensimmäisen yhdistämisen yhteydessä tulee ilmoitus, että root-käyttäjätunnuksella ei ole salasanaa. Annetaan salasana passwd komennolla.



KUVIO 9. OpenWrt aloitusnäkymä

Muokataan /etc/config/network asetuksia. Vaihdetaan Raspberryn IP-osoitteeksi 192.168.1.10, laitetaan yhdyskäytäväksi ja DNS-palvelimeksi reitittimen IP-osoite 192.168.1.1. Tämän jälkeen käynnistetään Raspberry Pi uudelleen komennolla reboot. Tämän vaiheen joutuu tekemään, koska USB-Ethernet adapteri ei vielä toimi ajuri puutteen vuoksi. Tämä vaihe on erilainen, jos yhdistää Raspberry Pi:n näppäimistöön, näyttöön ja suoraan ulkoverkkoon.

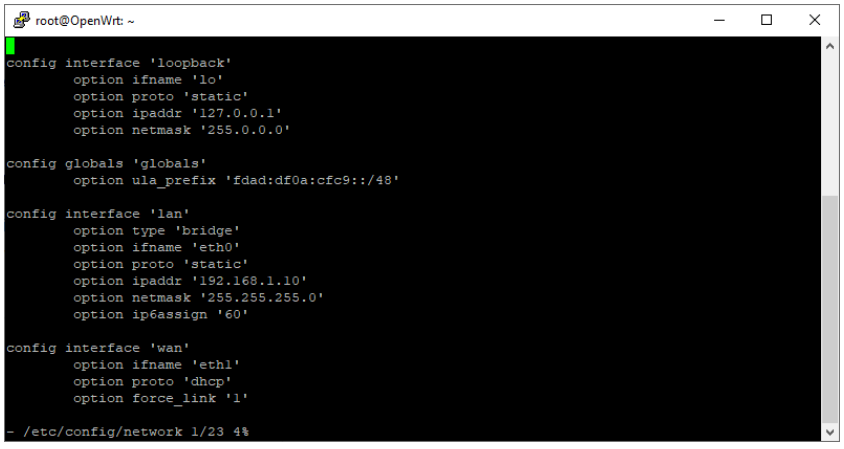


KUVIO 10. /etc/config/network asetukset reitittimeen yhdistämistä varten

Tämän jälkeen yhdistetään Raspberry Pi reitittimeen ja otetaan yhteys PuTTYn avulla.

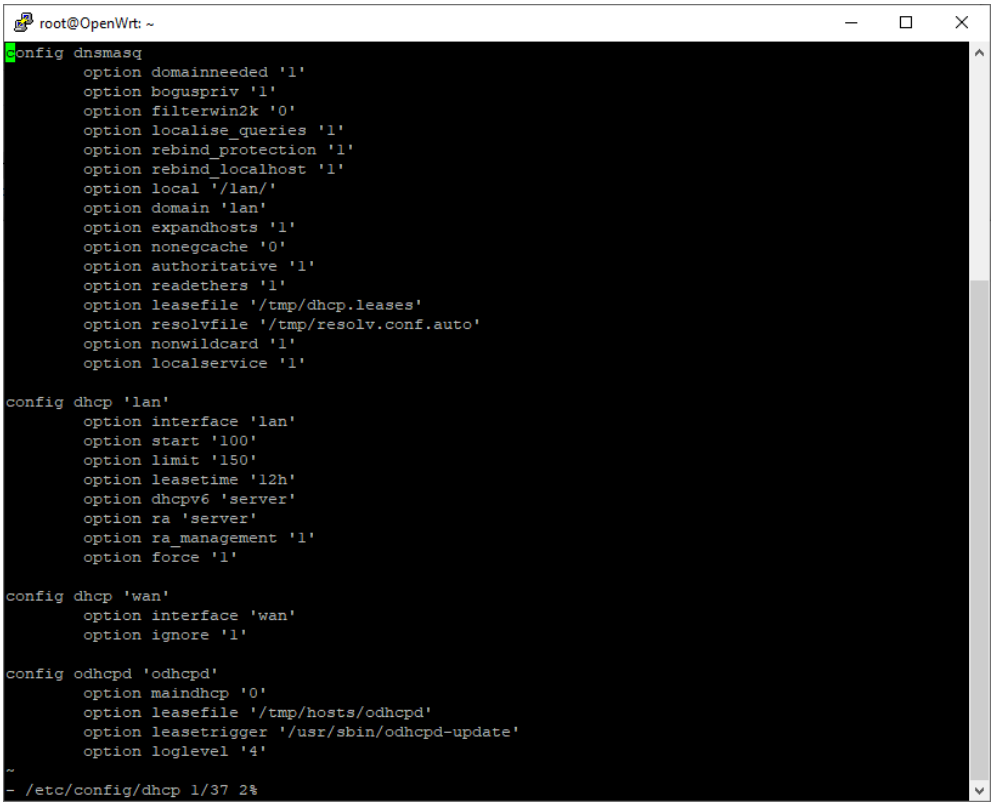
Ajetaan seuraavat komennot:
opkg update (päivittää luettelon käytettävissä olevista paketeista).
opkg install kmod-usb-net-asix-ax88179 (USB-Ethernet ajuri).

Muokataan /etc/config/network asetukset samanlaisiksi kuin alla olevassa kuvassa.



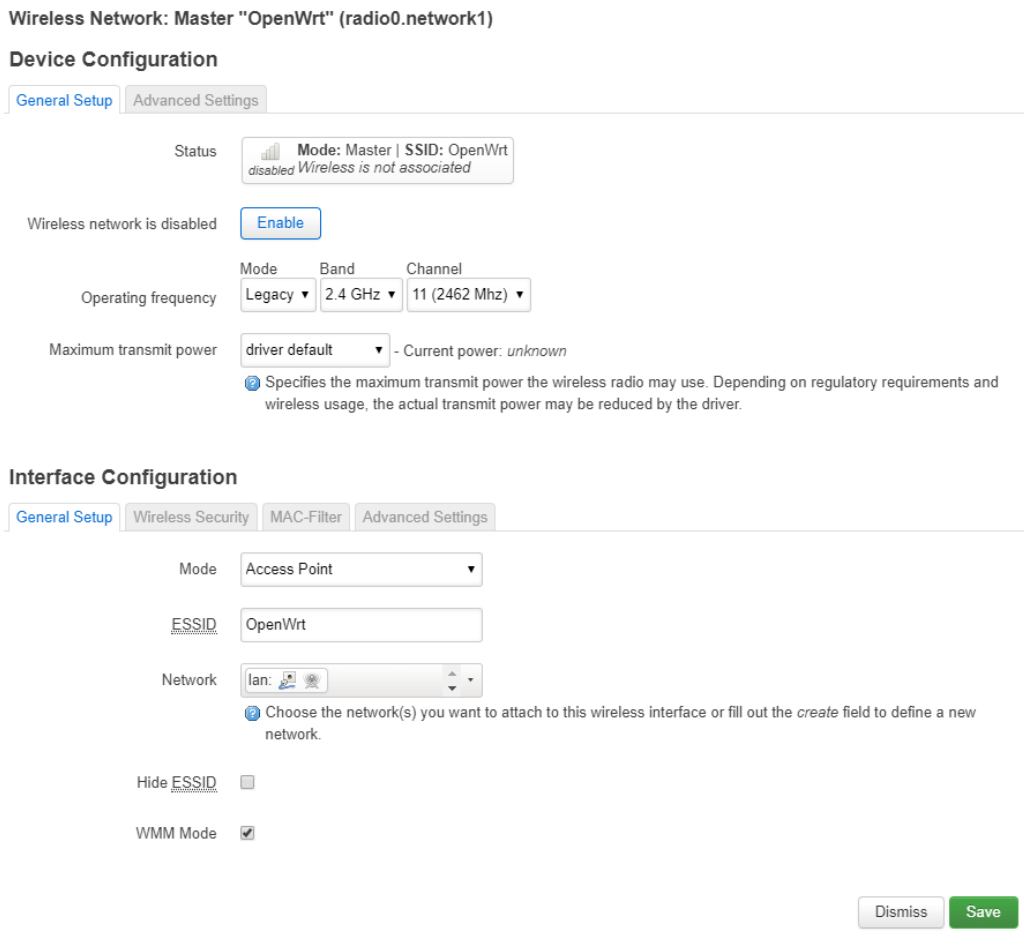
KUVIO 11. Muokatut /etc/config/network *asetukset*

Muokataan /etc/config/dhcp asetukset alla olevan kuvan mukaisesti. Raspberry Pi:hin yhdistävät laitteet saavat DHCP:n kautta IP-osoitteen.

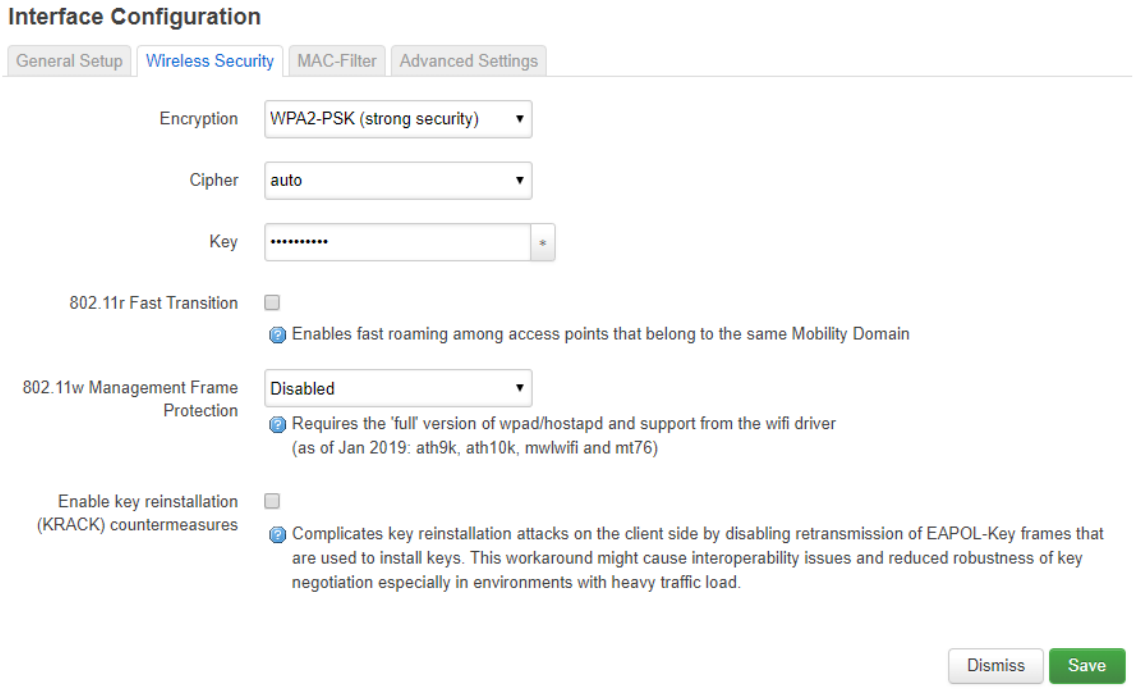


KUVIO 12. Muokatut /etc/config/dhcp *asetukset*

Tämän jälkeen käynnistetään Raspberry Pi uudelleen ja muokataan Luci-verkonhallintasivulta langattoman verkon asetukset.



KUVIO 13. Luci-verkonhallintasivun langattoman verkon asetukset ”General Setup”



KUVIO 14. Luci-verkonhallintasivun langattoman verkon asetukset ”Wireless Security”

Laitetaan ”Wireless network” ”Enabled” tilaan. Tämän jälkeen käynnistetään Raspberry Pi uudelleen, jonka jälkeen sen voi yhdistää suoraan tietokoneeseen ja ulkoverkkoon.

6.2 VPN-yhteyden käyttöönotto

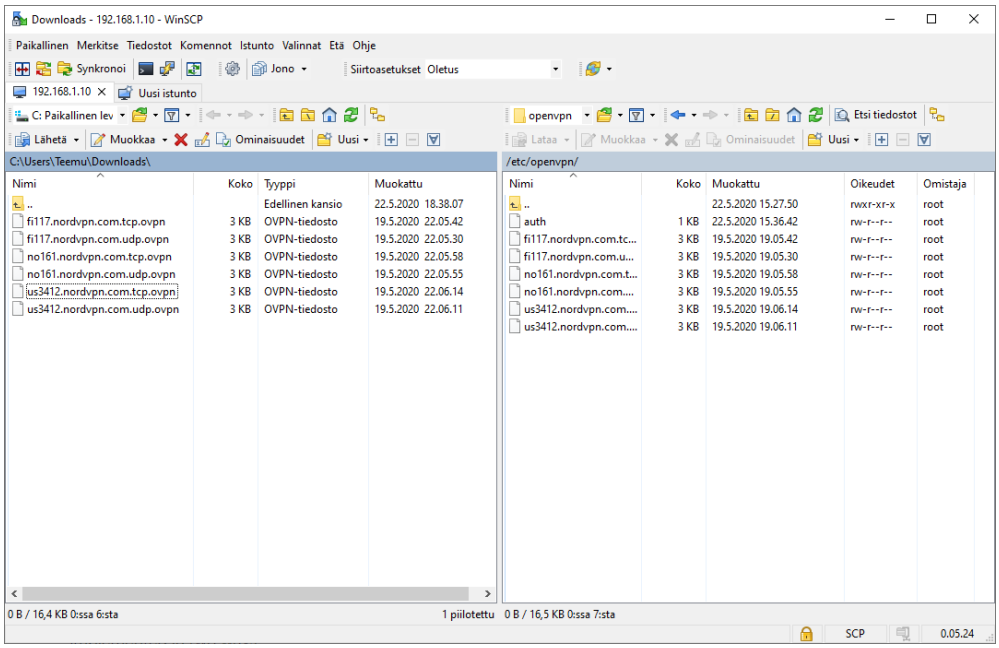
Käytän NordVPN:n käyttöönotossa ohjeena NordVPN verkkosivulla olevaa OpenWRT CI setup with NordVPN ohjetta (NordVPN 2020b, viitattu 26.5.2020).

Ajetaan seuraavat komennot:
opkg update (päivittää luettelon käytettävissä olevista paketeista).
opkg install openvpn-openssl (asentaa OpenVPN:n).
opkg install ip-full (reitityksen ohjausapuohjelma).
opkg install luci-app-openvpn (asentaa Luci-verkonhallintasivulle OpenVPN kohdan). Sain tämän aikaisemmin asentumaan, mutta nyt asennuksen aikana tuli virheilmoitus. Tämä saattaa johtua siitä, että OpenWrt-versio oli aikaisemmalla testauskerralla vanhempi.

/etc/init.d/openvpn enable (käynnistää OpenVPN käynnistyksen yhteydessä).

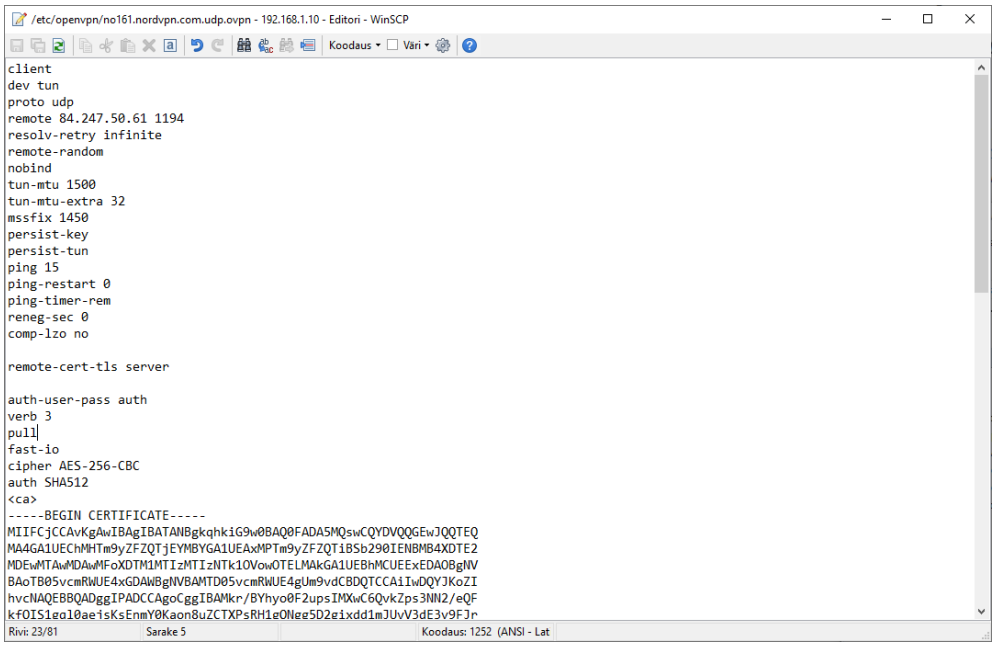
Ladataan NordVPN verkkosivuston (https://nordvpn.com/fi/servers/tools/) suosittelemat VPN-palvelimien konfiguraatiotiedostot. Testausta varten valittiin yksi VPN-palvelin Yhdysvalloista, Norjasta ja Suomesta. Kaikista kolmesta maasta valittiin samasta palvelimesta UDP- ja TCP-protokolla versiot.

Käytetään WinSCP-ohjelmaa VPN-palvelimien konfiguraatiotiedostojen siirtämiseen tietokoneesta Raspberry Pi:hin /etc/openvpn kansioon. Tehdään /etc/openvpn kansioon käyttäjätunnusta varten ”auth” niminen tiedosto, johon laitetaan NordVPN-käyttäjätunnus (rivi 1) ja salasana (rivi 2) allekkain. OpenVPN vaatii käyttäjänimen ja salasanan syöttämisen jokaisen käynnistyksen yhteydessä.



KUVIO 15. Siirretään WinSCP-ohjelman avulla VPN-palvelimien konfiguraatiotiedostot

Valitsin testattavaksi no161.nordvpn.com.udp.ovpn. VPN-palvelimen. Lisätään auth-user-pass kohdan perään käyttäjätunnus tiedoston nimi (auth).



KUVIO 16. Muokataan VPN-palvelimen konfiguraatiotiedostoon käyttäjätunnus tiedoston nimi

Muokataan no161.nordvpn.com.udp.ovpn tiedoston nimeksi no161.nordvpn.com.udp.conf. Tämän jälkeen OpenVPN osaa löytää tiedoston automaattisesti.

Luodaan uusi network interface tiedostoon /etc/config/network:

uci set network.nordvpntun=interface

uci set network.nordvpntun.proto='none'

uci set network.nordvpntun.ifname='tun0'

uci commit network

```
config interface 'nordvpntun'
        option proto 'none'
        option ifname 'tun0'
```

KUVIO 17. /etc/config/network tiedoston sisältö

Luodaan tiedostoon /etc/config/firewall palomuurivyöhyke ja lisätään välityssääntö lähiverkosta VPN:ään:

uci add firewall zone

uci set firewall.@zone[-1].name='vpnfirewall'

uci set firewall.@zone[-1].input='REJECT'

uci set firewall.@zone[-1].output='ACCEPT'

uci set firewall.@zone[-1].forward='REJECT'

uci set firewall.@zone[-1].masq='1'

uci set firewall.@zone[-1].mtu_fix='1'

uci add_list firewall.@zone[-1].network='nordvpntun'

uci add firewall forwarding

uci set firewall.@forwarding[-1].src='lan'

uci set firewall.@forwarding[-1].dest='vpnfirewall'

uci commit firewall

```
config zone
        option name 'vpnfirewall'
        option input 'REJECT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option masq '1'
        option mtu_fix '1'
        list network 'nordvpntun'

config forwarding
        option src 'lan'
        option dest 'vpnfirewall'
```

KUVIO 18. /etc/config/firewall tiedoston sisältö

Lisätään tiedoston /etc/config/network WAN-asetuksiin NordVPN DNS-palvelimet:

uci set network.wan.peerdns='0'

uci del network.wan.dns

uci add_list network.wan.dns='103.86.96.100'

uci add_list network.wan.dns='103.86.99.100'

uci commit

```
config interface 'wan'
        option ifname 'eth1'
        option proto 'dhcp'
        option force_link '1'
        option peerdns '0'
        list dns '103.86.96.100'
        list dns '103.86.99.100'
```

KUVIO 19. /etc/config/network WAN-asetukset

Tehdään liikennevuodon esto VPN-tunnelin mennessä alas. Muokataan /etc/firewall.user tiedostoon:

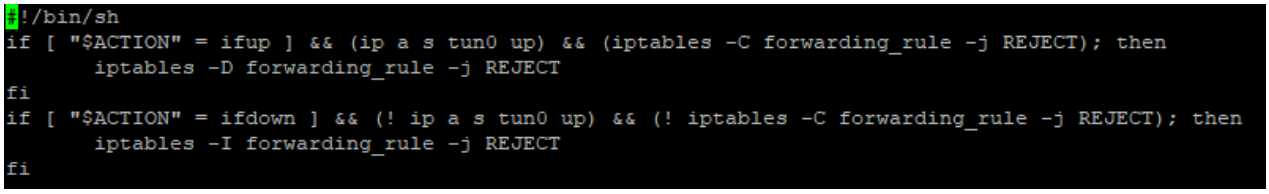
```
if (! ip a s tun0 up) && (! iptables -C forwarding_rule -j REJECT); then
      iptables -I forwarding_rule -j REJECT
fi
```

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.

if (! ip a s tun0 up) && (! iptables -C forwarding_rule -j REJECT); then
      iptables -I forwarding_rule -j REJECT
fi
~
~
~
~
~
~
- /etc/firewall.user 1/11 9%
```

KUVIO 20. /etc/firewall.user tiedoston sisältö

Tehdään kansioon /etc/hotplug.d/iface/prevent-leak niminen tiedosto:

```
#!/bin/sh
if [ "$ACTION" = ifup ] && (ip a s tun0 up) && (iptables -C forwarding_rule -j REJECT); then
	iptables -D forwarding_rule -j REJECT
fi
if [ "$ACTION" = ifdown ] && (! ip a s tun0 up) && (! iptables -C forwarding_rule -j REJECT); then
	iptables -I forwarding_rule -j REJECT
fi
```

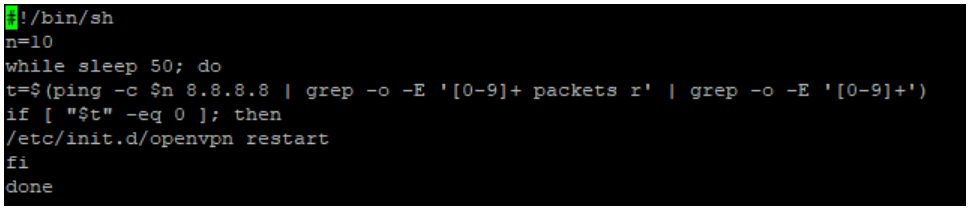


KUVIO 21. /etc/hotplug.d/iface/prevent-leak tiedoston sisältö

Joissain tapauksissa OpenVPN jää lokisanomaan (couldn't resolve host…). Tässä tapauksessa tunneli on käytössä, mutta yhteys ei ole. Sen voi yhdistää manuaalisesti /etc/openvpn/reconnect.sh tiedoston avulla.

Reconnect.sh tiedoston sisältö:

```
#!/bin/sh
n=10
while sleep 50; do
t=$(ping -c $n 8.8.8.8 | grep -o -E '[0-9]+ packets r' | grep -o -E '[0-9]+')
if [ "$t" -eq 0 ]; then
/etc/init.d/openvpn restart
fi
done
```



KUVIO 22. /etc/openvpn/reconnect.sh tiedoston sisältö

Lisätään “/etc/openvpn/reconnect.sh &” tiedostoon /etc/rc.local.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

/etc/openvpn/reconnect.sh &

exit 0
```

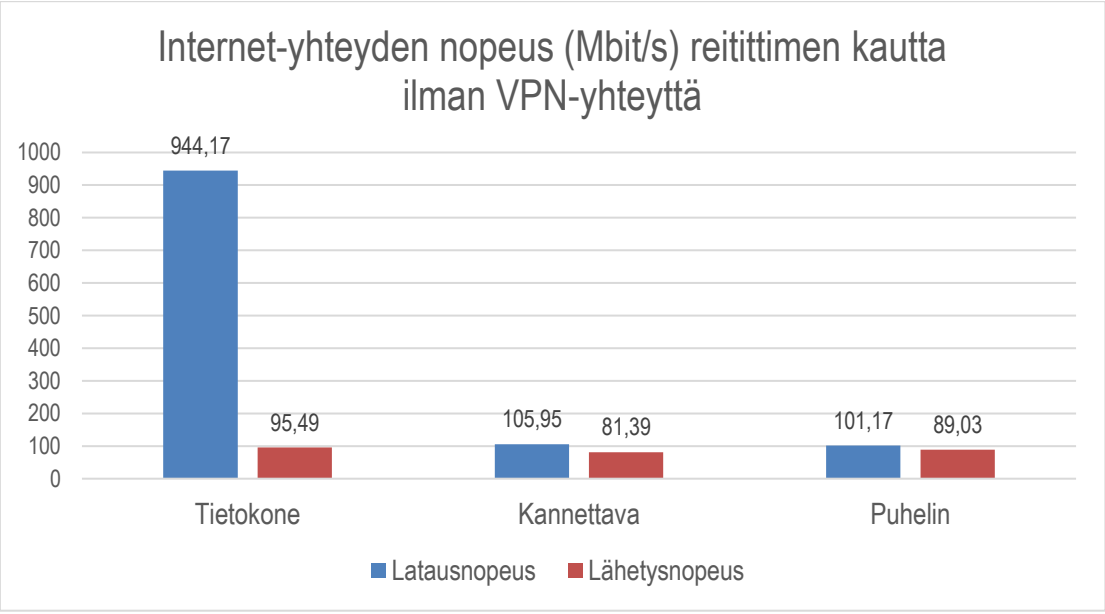
KUVIO 23. /etc/rc.local tiedoston sisältö

Käynnistetään Raspberry Pi uudelleen. Raspberry Pi VPN-reititin on uudelleenkäynnistämisen jälkeen valmis.

6.3 Tulokset

6.3.1 Yhteys ilman VPN-yhteyttä reitittimen kautta

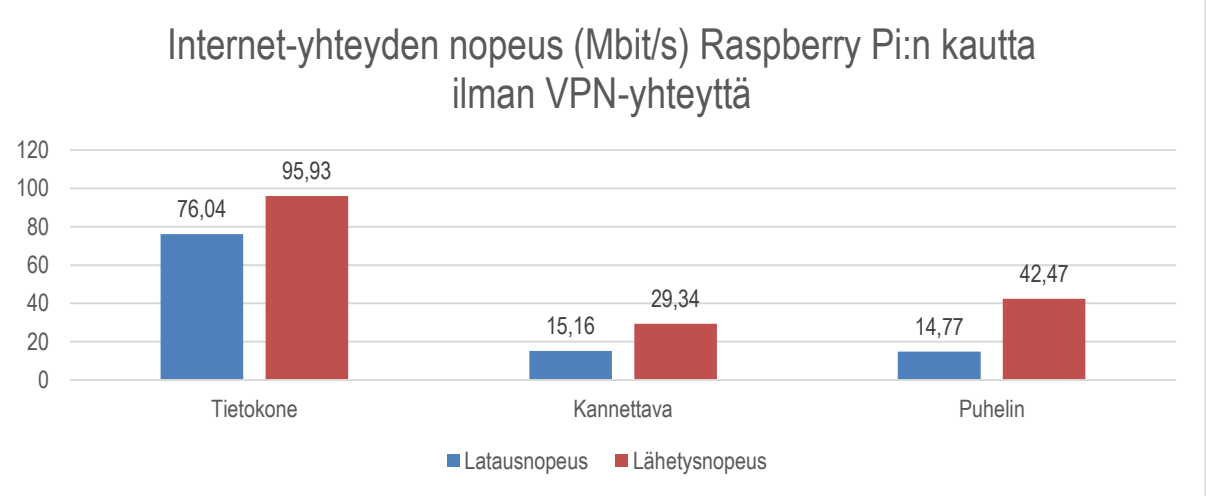
Testasin ensin Internet-yhteyden nopeuden (latausnopeus ja lähetysnopeus) ilman VPN-yhteyttä ASUS RT-N18U reitittimen kautta. Yhteyden testaamiseen käytettiin Speedtest.net (https://www.speedtest.net/) verkkosivua. Testasin Internet-yhteyden nopeuden kolme kertaa, jonka jälkeen laskin testitulosten keskiarvon. Tietokone käytti langallista yhteyttä reitittimeen. Kannettava ja puhelin käyttivät langatonta verkkoa. Puhelimen yhteys testattiin Speedtest-mobiilisovelluksen kautta. Käytin testissä palvelimena Oulussa olevaa Netplaza Oy:tä. (KUVIO 24.)



KUVIO 24. Yhteyden nopeus (Mbit/s) reitittimen kautta ilman VPN-yhteyttä

6.3.2 Yhteys ilman VPN-yhteyttä Raspberry Pi:n toimiessa reitittimenä

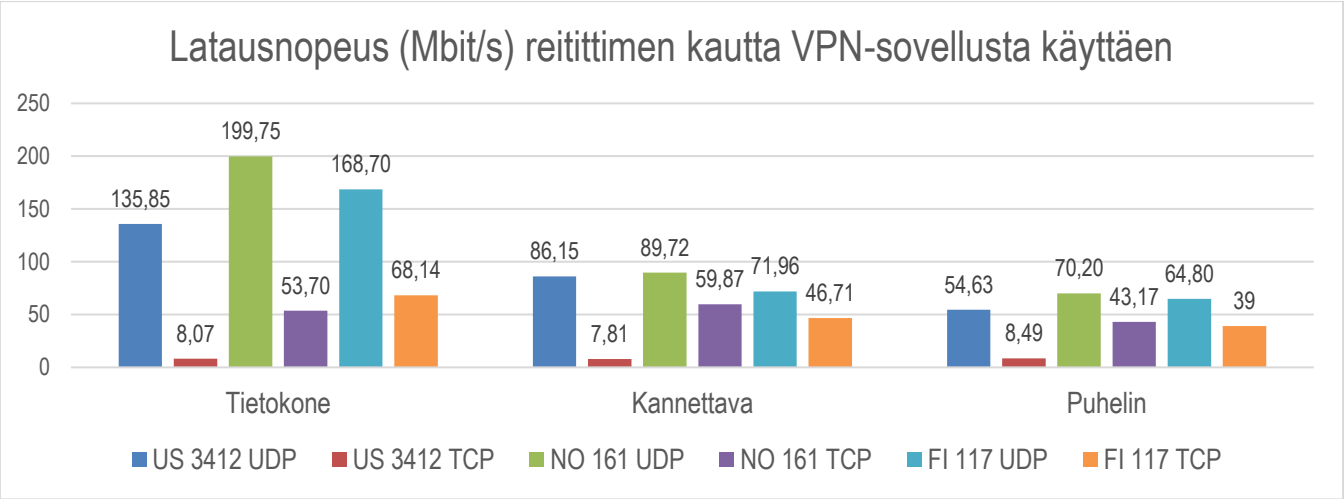
Seuraavaksi testasin Internet-yhteyden nopeuden Raspberry Pi:n toimiessa reitittimenä. Testin tulokset osoittivat sen, että Raspberry Pi 3 B+ malli ei ole tarpeeksi tehokas toimimaan reitittimenä omassa käytössäni, mutta se voi sopia käyttöön, jos Internet-yhteyden nopeus on noin 100 Mbit/s. Internet-yhteyden nopeus hidastui Raspberry Pi:n kautta kaikilla testaamillani laitteilla noin 10-kertaisesti. Tulokset olisivat todennäköisesti paremmat uudella Raspberry Pi 4 B-mallilla. (KUVIO 25.)



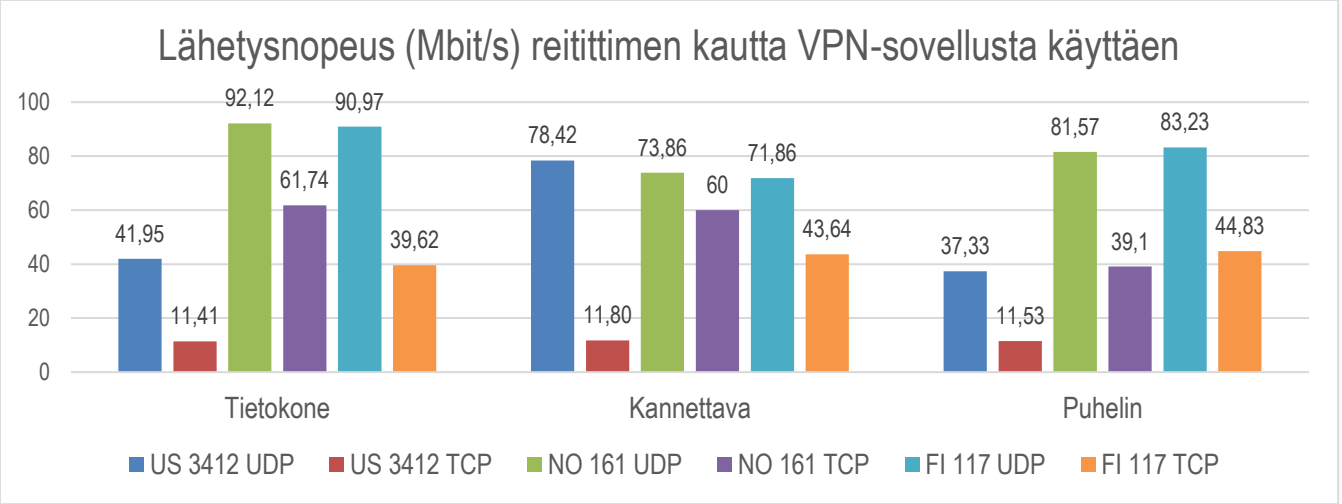
KUVIO 25. Internet-yhteyden nopeus (Mbit/s) Raspberry Pi:n kautta ilman VPN-yhteyttä

6.3.3 Yhteys reitittimen kautta VPN-sovellusta käyttäen

Testasin Internet-yhteyden nopeuden VPN-sovellusta käyttäen, kun olin yhdistänyt reitittimeen. Testasin Internet-yhteyden nopeuden kolme kertaa, jonka jälkeen laskin niiden keskiarvon. Annoin Speedtest verkkosivun valita automaattisesti testipalvelimen. Testasin kolmen maan VPN-palvelimet (Yhdysvallat, Norja, Suomi) sekä testasin myös UDP- ja TCP-protokollaa käyttävät palvelimet. Testin aikana selvisi, että TCP-protokollan käyttäminen hidasti Internet-yhteyden nopeutta huomattavasti esimerkiksi US 3412 TCP-palvelinta käytettäessä. (KUVIO 26 & 27.)



KUVIO 26. Latausnopeus (Mbit/s) reitittimen kautta VPN-sovellusta käyttäen. VPN-palvelimien selitteet US (Yhdysvallat), NO (Norja) ja FI (Suomi)

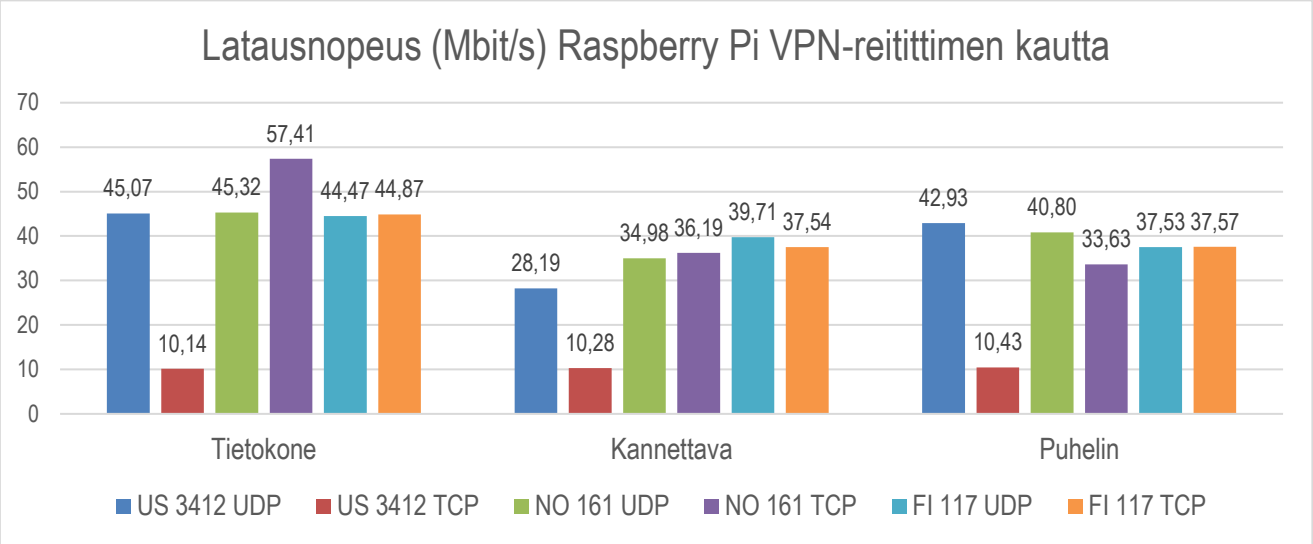


KUVIO 27. Lähetysnopeus (Mbit/s) reitittimen kautta VPN-sovellusta käyttäen. VPN-palvelimien selitteet US (Yhdysvallat), NO (Norja) ja FI (Suomi)

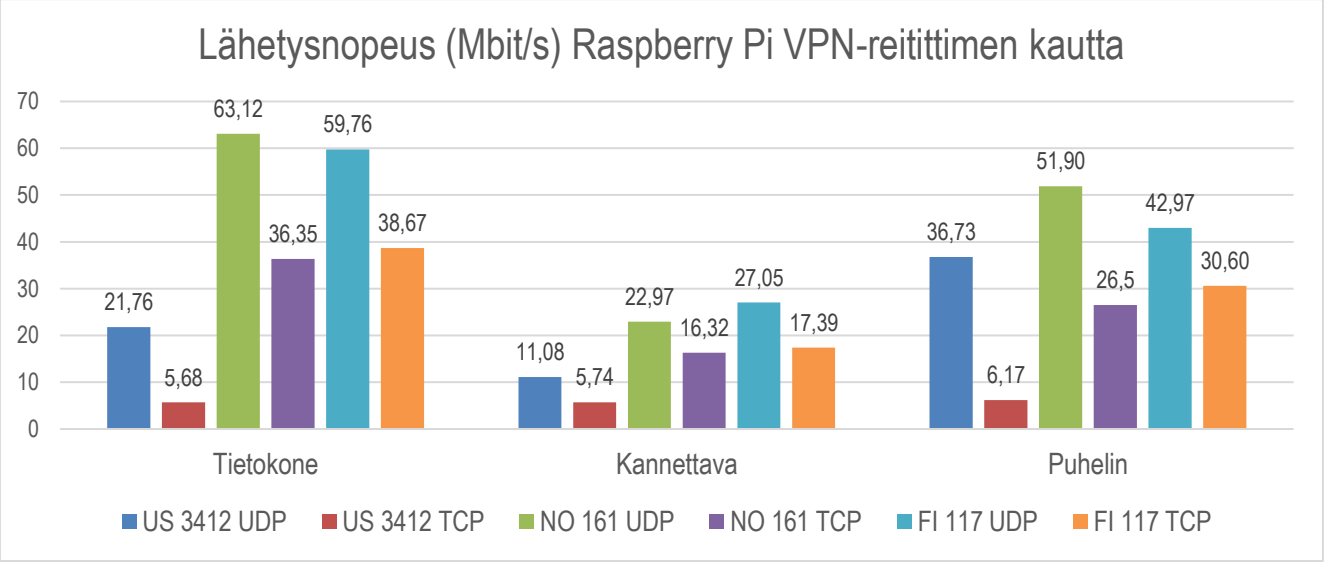
6.3.4 Yhteys Raspberry Pi VPN reitittimen kautta

Testasin Internet-yhteyden nopeuden samalla tavalla kuin reitittimen kautta VPN-sovellusta käyttäen. Suurimmassa osassa latausnopeus tippui huomattavasti verrattuna VPN-sovellukseen. Kuitenkin US 3412 TCP-palvelimen kautta Internet-yhteyden nopeus kasvoi noin 2 Mbit/s. (KUVIO 28.) Lähetysnopeus lähes puolittui tietokoneella, mutta FI 117 TCP-palvelimen lähetysnopeus oli oikeastaan sama kuin VPN-sovellusta käyttämällä. Lähetysnopeus oli puhelimessa nopeampi kuin kannettavassa, kun käytettiin Raspberry Pi VPN-yhteyttä. (KUVIO 29.) Yllättäen Raspberry Pi VPN-

ratkaisua käytettäessä lataus- ja lähetysnopeus kasvoi puhelimessa sekä kannettavassa verrattuna Raspberry Pi:n ollessa pelkkänä reitittimenä.



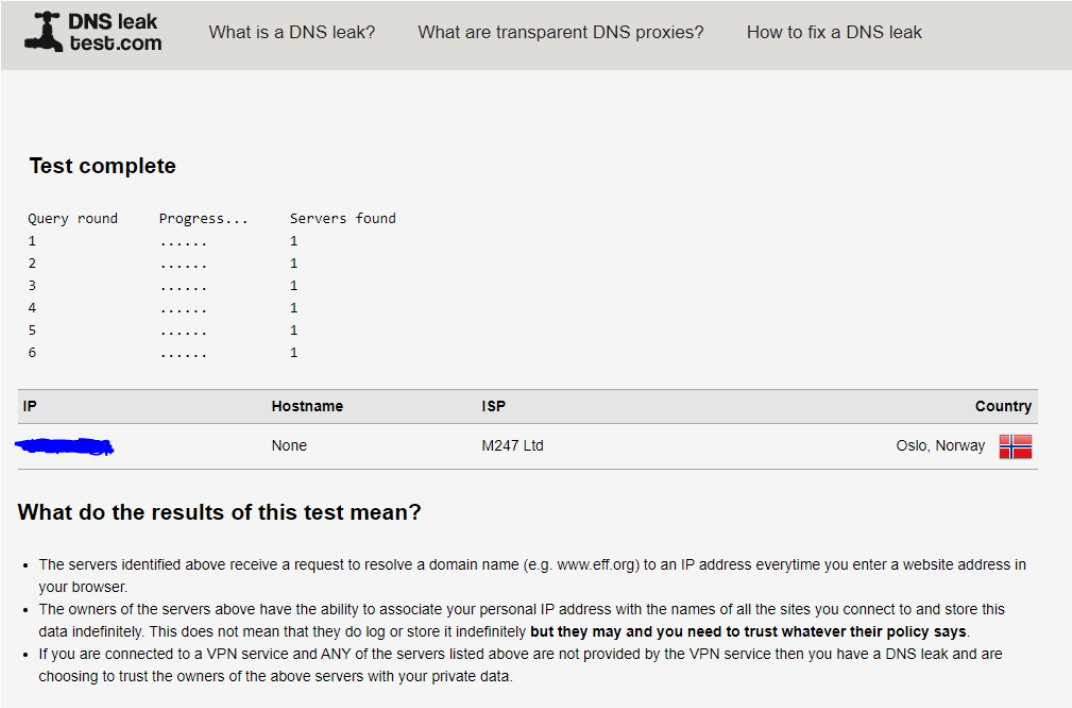
KUVIO 28. Latausnopeus (Mbit/s) Raspberry Pi VPN-reitittimen kautta. VPN-palvelimien selitteet US (Yhdysvallat), NO (Norja) ja FI (Suomi)



KUVIO 29. Lähetysnopeus (Mbit/s) Raspberry Pi VPN-reitittimen kautta. VPN-palvelimien selitteet US (Yhdysvallat), NO (Norja) ja FI (Suomi)

6.3.5 DNS-vuototesti

Tein pidennetyn (kuusi testikierrosta) DNS-vuototestin DNS leak test (https://www.dnsleak-test.com/) verkkosivun kautta. DNS-vuototesti osoittaa, että VPN-yhteys ei vuoda DNS-osoitteita, ja VPN-yhteyttä on turvallista käyttää. (KUVIO 30.)



KUVIO 30. DNS-vuototestin tulos

7 POHDINTA

Opinnäytetyöni tavoitteena oli luoda toimiva Raspberry Pi VPN-reititin. Käyttöjärjestelmänä toimi OpenWrt, VPN-protokollana OpenVPN ja VPN-palveluntarjoajana NordVPN. Testaustuloksen perusteella Raspberry Pi 3 B+ malli hidastaa Internet-yhteyden nopeutta ilman VPN-yhteyttä ja sen kanssa enemmän kuin ASUS RT-N18U reititin. Testeissä selvisi, että UDP-protokolla on huomattavasti nopeampi kuin TCP-protokolla. Ilmeisesti tästä syystä OpenVPN-protokollaa käytettäessä VPN-palveluntarjoajat suosittelevat yleensä käyttämään UDP-protokollaa.

Testasin Internet-nopeuden kolmeen kertaan, jonka jälkeen laskin niiden keskiarvon. Tutkimuksen luotettavuuden kannalta halusin testata Internet-yhteyden nopeudet useampaan kertaan. Tutkimuksen luottamusta olisi lisännyt, jos olisin testannut Internet-yhteyden nopeudet useana eri päivänä. On kuitenkin mahdollista, että tulokset eivät olisi muuttuneet olennaisesti, mutta VPN-palvelimien kuormitus voi vaikuttaa tuloksiin satunnaisesti (Cloudflare 2020a, viitattu 26.5.2020).

Valitsin käyttöön OpenVPN-protokollan, koska se on hyvin mukautuva avoimen lähdekoodin ratkaisu, jonka murtamisesta ei ole todisteita tällä hetkellä. Valitsin OpenWrt:n käyttöjärjestelmäksi, koska se on kevyt, hyvin mukautuva ja sitä on mahdollista hallita web-käyttöliittymän kautta. Kehittämistehtävässäni tein toimivan Raspberry Pi VPN-reitittimen, joka käytti NordVPN-palveluntarjoajan VPN-palvelua. Valitsin VPN-palveluntarjoajaksi NordVPN:n, koska olen itse käyttänyt heidän VPN-palveluaan noin viiden vuoden ajan. Omat kokemukseni NordVPN-palvelusta ovat hyvät, eivätkä he pidä käyttölokeja.

Jouduin selvittämään opinnäytetyön aikana ongelmia, jotka liittyivät esimerkiksi Raspberry Pi reitittimen toimivuuteen ja VPN-yhteyden toimintaan. Sain kuitenkin lopulta VPN-yhteyden toimimaan Raspberry Pi:ssä. Ongelmana oli, että OpenVPN ei tunnistanut VPN-palvelinta, jonka sain korjattua kokeilemalla OpenWRT CI setup with NordVPN ohjeessa olevaa kahta vaihtoehtoa. Kokeilin saada toimimaan VPN-ratkaisua noin viisi kertaa. Sain yleensä VPN-yhteyden Raspberry Pi:hin, mutta en saanut sitä jaettua muille laitteille. Sain ratkaisun toimimaan, kun päädyin tekemään Raspberry Pi:stä ensin reitittimen, minkä jälkeen asensin siihen VPN:n.

Raspberry Pi VPN-ratkaisun saa toimivammaksi, jos ratkaisussa käyttää uudempia Raspberry Pi 4 B-malleja. Uudemmissa Raspberry Pi-malleissa on nopeammat prosessorit ja enemmän RAM-

muistia mallista riippuen. Raspberry Pi:hin voi myös halutessaan lisätä paremman langattoman verkon vastaanottimen, jotta langattoman verkon yhteyksien nopeudet eivät kärsi niin paljon.

LÄHTEET

Aoki, K. 2019. What Is OpenVPN? Is It Safe?. Viitattu 14.5.2020, https://www.lifewire.com/openvpn-for-networking-818194.

Bischoff, P. 2019. VPN protocols explained and compared. Viitattu 13.5.2020, https://www.comparitech.com/vpn/protocols/.

Bozovic, N. 2019. What is OpenVPN? – A Beginners-Friendly Guide to OpenVPN, The Most Popular VPN Protocol!. Viitattu 14.5.2020, https://www.technadu.com/openvpn/8640/.

Bresnahan, C. & Blum, R. 2015. Linux Essentials, 2nd Edition. Indianapolis: John Wiley and Sons.

Carmouche, J. 2006. IPsec Virtual Private Network Fundamentals. Indianapolis: Cisco Press.

Chauhan, A. 2018. Practical Network Scanning. Birmingham: Packt Publishing.

Cisco 2020a. What Is a LAN?. Viitattu 23.5.2020, https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html.

Cisco 2020b. What Is a VPN? - Virtual Private Network. Viitattu 25.4.2020, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html.

Cisco 2020c. What Is a WAN? Wide-Area Network. Viitattu 23.5.2020, https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html.

Cloudflare 2020a. How VPNs affect Internet speed. Viitattu 26.5.2020, https://www.cloudflare.com/learning/access-management/vpn-speed/.

Cloudflare 2020b. What is UDP?. Viitattu 24.5.2020, https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/.

Connor, J. 2019. A complete guide to Raspbian. Viitattu 15.5.2020, https://www.itpro.co.uk/operating-systems/33629/a-complete-guide-to-raspbian.

Crawford, D. 2019. OpenVPN vs IKEv2 vs PPTP vs L2TP/IPSec vs SSTP - Ultimate Guide to VPN Encryption. Viitattu 13.5.2020, https://proprivacy.com/vpn/guides/vpn-encryption-the-complete-guide#comments.

Crist, E & Keijser, J. 2015. Mastering OpenVPN. Birmingham: Packt Publishing.

DeMuro, J. 2018. What is AES?. Viitattu 23.5.2020, https://www.techradar.com/news/what-is-aes.

Dennis, A. 2016. Raspberry Pi Computer Architecture Essentials. Birmingham: Packt Publishing.

Ellis, M. 2019. How Does a Router Work? A Simple Explanation. Viitattu 23.5.2020, https://www.makeuseof.com/tag/technology-explained-how-does-a-router-work/.

Fisher, T. 2019. What Is DHCP? (Dynamic Host Configuration Protocol). Viitattu 23.5.2020, https://www.lifewire.com/what-is-dhcp-2625848.

FlashRouters 2018. What is Geo-Blocking And How Do I Get Around It?. Viitattu 23.5.2020, https://blog.flashrouters.com/2018/06/17/what-is-geo-blocking-and-how-do-i-get-around-it/.

Free CCNA Study Guide 2020. 12-1 VPN Concepts. Viitattu 12.1.2020, https://www.freeccnastudyguide.com/study-guides/ccna/ch12/12-1-vpn-concepts/.

GCFGlobal 2020. What is an operating system?. Viitattu 23.5.2020, https://edu.gcfglobal.org/en/computerbasics/understanding-operating-systems/1/.

Greenberg, R. 2020. Different Types of VPNs and When to Use Them (Updated 2020). Viitattu 25.4.2020, https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/.

GNU.org 2007. GNU General Public License. Viitattu 23.5.2020,

https://www.gnu.org/licenses/gpl-3.0.html.

Haylee. 2017. VPNs: Your personal tunnel to privacy. Viitattu 27.10.2019, https://blog.emsisoft.com/en/27485/vpn-privacy-2/.

Harrington, W. 2015. Learning Raspbian. Birmingham: Packt Publishing.

Heath, N. 2018. Inside the Raspberry Pi: The story of the $35 computer that changed the world. Viitattu 5.10.2019, https://www.techrepublic.com/article/inside-the-raspberry-pi-the-story-of-the-35-computer-that-changed-the-world/.

Hoffman, C. 2018. Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP. Viitattu 14.5.2020, https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpip-sec-vs.-sstp/.

Hoffman, C. 2019. What Is a VPN, and Why Would I Need One?. Viitattu 1.3.2020, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/.

IBM Cloud Education 2020. DNS. Viitattu 23.5.2020, https://www.ibm.com/cloud/learn/dns#toc-what-is-dn-6HhNK5D5.

Imperva 2020. Transmission control protocol (TCP). Viitattu 24.5.2020, https://www.imperva.com/learn/application-security/tcp-transmission-control-protocol/.

Klosowski, T. 2016. The Best Operating Systems for Your Raspberry Pi Projects. Viitattu 15.5.2020, https://lifehacker.com/the-best-operating-systems-for-your-raspberry-pi-projec-1774669829.

Levavi-Eilat, S. 2020. 7 Hidden Dangers to Using Free VPNs in 2020. Viitattu 1.3.2020, https://www.vpnmentor.com/blog/free-vpns-are-not-safe-to-use/.

Maker.io 2018. Raspberry Pi Comparison: Which Pi is Right for My Application?. Viitattu 14.5.2020,

https://www.digikey.com/en/maker/blogs/2018/how-to-pick-the-right-raspberry-pi.

Marks, T. 2020. Disadvantages of a VPN. Viitattu 15.5.2020,
https://vpnoverview.com/vpn-information/disadvantages-vpn/.

Mitchell, B. 2020. Guide to Computer Network Adapters. Viitattu 24.5.2020,
https://www.lifewire.com/definition-of-adapter-817585.

Mocan, T. 2016. What Is L2TP (Layer 2 Tunneling Protocol)?. Viitattu 12.5.2020,
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-l2tp/#how-l2tp-works.

Negus, C. 2015. Linux Bible, Ninth Edition. Indianapolis: John Wiley and Sons.

Nexcess 2019. What is GeoIP?. Viitattu 23.5.2020,
https://help.nexcess.net/77285-other/what-is-geoip.

NordVPN 2020a. DNS leak test. Viitattu 23.5.2020,
https://nordvpn.com/features/dns-leak-test/.

NordVPN 2020b. OpenWRT CI setup with NordVPN. Viitattu 26.5.2020,
https://support.nordvpn.com/Connectivity/Router/1047411192/OpenWRT-CI-setup-with-NordVPN.htm.

OpenWrt 2020. About the OpenWrt/LEDE project. Viitattu 23.5.2020,
https://openwrt.org/about.

Oxford, A. 2019. How to Use Raspberry Pi as a VPN Gateway. Viitattu 14.5.2020,
https://www.tomshardware.com/reviews/raspberry-pi-vpn-gateway,6103.html.

Raspberrypi.org 2020a. FAQs. Viitattu 18.4.2020,
https://www.raspberrypi.org/documentation/faqs/#introduction.

Raspberrypi.org 2020b. Raspberry Pi 1 Model A. Viitattu 18.4.2020,
https://www.raspberrypi.org/model-a/.

RasPi.TV 2018. New Raspberry Pi Family Photo including Pi3A+ plus Zero WH. Viitattu 9.2.2020, https://raspi.tv/2018/new-raspberry-pi-family-photo-including-pi3a-plus-zero-wh.

Rouse, M. 2020. VPN (virtual private network). Viitattu 11.4.2020, https://searchnetworking.techtarget.com/definition/virtual-private-network.

Santos, O. 2020. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. Hoboken: Cisco Press.

Skoler, B. 2020. Remote-Access VPN vs Site-to-Site VPN – Full Guide 2020. Viitattu 10.5.2020, https://www.vpnmentor.com/blog/remote-access-vpn-vs-site-to-site-vpn-full-guide/.

SURVEILLANCE SELF-DEFENSE 2019. Commercial VPN. Viitattu 27.10.2019, https://ssd.eff.org/en/glossary/commercial-vpn.

Techopedia 2016. Wireless Network. Viitattu 23.5.2020, https://www.techopedia.com/definition/26186/wireless-network.

Techopedia 2020a. Embedded Device. Viitattu 24.5.2020, https://www.techopedia.com/definition/10179/embedded-device.

Techopedia 2020b. Leased Line. Viitattu 24.5.2020, https://www.techopedia.com/definition/5595/leased-line.

The Pi Hut 2017. Raspberry Pi Models. Viitattu 14.5.2020, https://thepihut.com/blogs/raspberry-pi-roundup/raspberry-pi-comparison-table.

Thomas, T. & Stoddard, D. 2011. Network Security First-Step, Second Edition. Indianapolis: Cisco Press.

Tyson, J., Pollette, C. & Crawford, S. 2019a. How VPNs Work. Viitattu 27.10.2019, https://computer.howstuffworks.com/vpn3.htm.

Tyson, J., Pollette, C. & Crawford, S. 2019b. How VPNs Work. Viitattu 10.5.2020, https://computer.howstuffworks.com/vpn4.htm.

vpnMentor 2020. What Is a Site-to-Site VPN and Does Your Business Need One for 2020?. Viitattu 18.4.2020, https://www.vpnmentor.com/blog/what-is-a-site-to-site-vpn-and-does-your-business-need-one/.

Walsh, R. 2018. VPN Jurisdiction: Where's best place for a VPN to be based?. Viitattu 15.5.2020, https://proprivacy.com/vpn/guides/best-jurisdiction-vpn.

LIITTEET

TAULUKKO 1. Erilaiset Raspberry Pi-mallit (Raspberrypi.org 2020a, Viitattu 18.4.2020)

Malli	**Piirisarja**	**Prosessorin nopeus**	**Muisti**	**USB-portit**	**Verkko-sovitin**	**Langatto-mat yhtey-det**	**Bluetooth**
Malli A+	BCM2835	700MHz	512 MT	1	Ei	Ei	Ei
Malli B+	BCM2835	700MHz	512 MT	4	100Base-T	Ei	Ei
Malli 2 B	BCM2836/7	900MHz	1 GT	4	100Base-T	Ei	Ei
Malli 3 B	BCM2837A0/ B0	1200MHz	1 GT	4	100Base-T	802.11n	4.1
Malli 3 A+	BCM2837B0	1400MHz	512 MT	1	Ei	802.11ac/n	4.2
Malli 3 B+	BCM2837B0	1400MHz	1 GT	4	1000Base-T	802.11ac/n	4.2
Malli 4 B	BCM2711	1500MHz	1 GT	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Malli 4 B	BCM2711	1500MHz	2 GT	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Malli 4 B	BCM2711	1500MHz	4 GT	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Zero	BCM2835	1000MHz	512 MT	1	Ei	Ei	Ei
Zero W / WH	BCM2835	1000MHz	512 MT	1	Ei	802.11n	4.1