UNIVERSITY OF OULU
TIETO- JA SÄHKÖTEKNIIKAN TIEDEKUNTA

Mikko Rytilahti

Lähiverkon toimivuuden valvontajärjestelmä Raspberry Pi -alustoille

Kandidaatintyö
Tietotekniikan tutkinto-ohjelma
Huhtikuu 2022

Rytilahti M. (2022) Lähiverkon toimivuuden valvontajärjestelmä Raspberry Pi -alustoille. Oulun yliopisto, tietotekniikan tutkinto-ohjelma. Kandidaatintyö, 34 s.

TIIVISTELMÄ

Kannettavat, mobiililaitteet ja erilaiset IoT-laitteet ovat yleistyneet kovaa tahtia viime vuosien aikana. Erilaisten laitteiden määrän ja tiedonsiirron tarpeiden kasvaessa toimiva lähiverkko sekä WLAN-verkko ovat laitteiden käyttämisen kannalta ehdottoman tarpeellisia. Vaikka WLAN-verkko helpottaa laitteiden käyttöä, kun verkkokaapeleita ei tarvitse tuoda päätelaitteille asti, langattoman verkon kanssa voi tulla yllättäviä ongelmia esimerkiksi kuuluvuuden ja häiriöiden kanssa. Lähiverkkojen toimivuuden valvontaan tarvitaan uusia ratkaisuja, joiden avulla voidaan selvittää lähiverkon ongelmia ja toimivuutta myös etänä.

Tässä työssä toteutettiin WLAN- ja lähiverkkojen toimivuuden valvontaan työkalu. Idea työhön syntyi IT-palveluja tarjoavan yrityksen käytännön tarpeesta valvoa yrityksen asiakkaiden lähiverkkojen toimivuutta etänä, ilman että tiloissa on IT-henkilöstöä paikalla. Työssä kehitetyn järjestelmän vaatimuksia ja hyödynnettäviä ominaisuuksia suunniteltiin yhteistyössä oululaisen IT-palveluja tarjoavan yrityksen kanssa. Työssä tunnistettiin mahdollisia ongelmakohtia, joita voi esiintyä tyypillisen lähiverkon komponenttien toiminnassa. Merkittävimpiä käyttäjäkokemukseen vaikuttavia ongelmia ovat esimerkiksi langattoman lähiverkon kuuluvuus, DNS-ongelmat, DHCP-ongelmat, ja internetyhteyteen liittyvät ongelmat. Tunnistettujen ongelmakohtien pohjalta suunniteltiin ja toteutettiin erilaisia testejä sisältävä ohjelmisto, jota käyttämällä voidaan analysoida lähiverkon toimivuutta. Lisäksi toteutettiin automaatio ohjelmiston asentamiseen Raspberry Pi -alustoille Ansiblea hyödyntäen.

Työssä tutkittiin ja vertailtiin myös mahdollisia kaupallisia vaihtoehtoja työssä tehdylle järjestelmälle, kuten esimerkiksi Netbeeziä ja Unifi Controlleriin integroitua Wifi Experienceä. Lisäksi työssä esitellään mahdollisia jatkokehitysideoita ja toiminnallisuuksia työssä tehdyn ohjelmiston laajentamiseksi, kuten esimerkiksi mobiiliverkkoa hyödyntävä varayhteys. Työn tekninen toteutus rajattiin kuitenkin keskittymään pääosin edellä mainittujen merkittävimpien verkon komponenttien ongelmien tunnistamiseen.

Avainsanat: WLAN, lähiverkko, Raspberry Pi, Ansible

Rytilahti M. (2022) Local area network troubleshooting and monitoring system for Raspberry Pi platforms. University of Oulu, Degree Programme in Computer Science and Engineering. Bachelor's Thesis, 34 p.

ABSTRACT

Laptop computers, mobile devices, and IoT devices have become more common in recent years. As the number of devices and data transfer requirements increase, seamless and functional local area network and WLAN connectivity have become increasingly important. Although WLAN facilitates easier connectivity compared to traditional cabled networks, wireless networks have their own drawbacks. Interference and signal strength remain considerable issues. New solutions for WLAN and LAN monitoring are needed to troubleshoot and diagnose network connectivity remotely.

In this thesis, a tool was designed for monitoring local area network functionality. This tool was developed in cooperation with a local commercial IT services provider. The idea for this thesis arose from the need of a Finnish IT company, who needed a practical tool to troubleshoot and monitor their clients' office networks, without the need for on-premises IT staff presence. Common problems and failure points for local area networks were identified. The most significant problems affecting user experience are for example WLAN coverage, DNS issues, DHCP issues, and internet connection related issues. Based on these common problems a software with a set of tests was designed, which can be used to analyze the performance and functionality of the local network. In addition, an automation was implemented to install the software on Raspberry Pi platforms, using Ansible.

Possible commercial alternatives, such as NetBeez and Wifi Experience integrated into Unifi Controller software, were also explored and compared. In addition, key points for further development and expansion of the software developed in this thesis were identified, such as adding a backup internet connection using mobile networks. However, the technical scope of the work was limited mainly to the testing and identification of common network problems for troubleshooting usage.

Key words: WLAN, Local area network, Raspberry Pi, Ansible

SISÄLLYSLUETTELO

ALKULAUSE

Haluan kiittää työn ohjaajaa Teemu Tokolaa neuvoista ja palautteesta. Lisäksi haluan kiittää Antti Jaakkolaa Remod Oy:stä neuvoista ja avusta aiheen rajaamisen kanssa, sekä mahdollisuudesta kehittää työtä yrityksen tarpeisiin.

Oulu, Huhtikuu 4. 2022

Mikko Rytilahti

LYHENTEIDEN JA MERKKIEN SELITYKSET

ARP	Protokolla, jonka avulla selvitetään IP-osoitetta vastaava MAC-osoite, Address Resolution Protocol
dBm	Signaalinvoimakkuuden yksikkö, desibelimilliwatti
DDoS	Hajautettu palvelunestohyökkäys, Distributed Denial of Service
DHCP	Verkkoasetuksien jakeluun käytettävä protokolla, Dynamic Host Configuration Protocol
DNS	Nimipalvelujärjestelmä, Domain Name System
HTTP	Selainten ja palvelimien väliseen tiedonsiirtoon käytettävä protokolla, HyperText Transfer Protocol
ICMP	Protokolla jonka avulla voidaan välittää viestejä verkon tilasta, Internet Control Message Protocol
IDS	Tunkeutumisen havaitsemisjärjestelmä, Intrusion Detection System
IPS	Tunkeutumisen estämisjärjestelmä, Intrusion Prevention System
IoT	Esineiden internet, Internet of Things
IP	Internetyhteyskäytäntö, Internet Protocol
IPv4	Internetyhteyskäytäntö versio 4, Internet Protocol version 4
IPv6	Internetyhteyskäytäntö versio 6, Internet Protocol version 6
LAN	Lähiverkko, Local Area Network
MAC	Verkon siirtoyhteyskerroksen alijärjestelmä, Media Access Control
SSH	Salatun tietoliikenteen protokolla, Secure Shell
VLAN	Virtuaalilähiverkko, Virtual Local Area Network
WEP	Langattoman verkkoliikenteen salausprotokolla vuodelta 1997, Wired Equivalent Privacy
WPA	Langattoman verkkoliikenteen salausprotokolla vuodelta 2003, Wi-Fi Protected Access
WLAN	Langaton lähiverkko, Wireless Local Area Network
YAML	Helposti ihmisten luettavissa oleva merkintäkieli, YAML Ain't Markup Language

1. JOHDANTO

Langattomien verkkojen käyttö sekä niitä hyödyntävien laitteiden määrä on viime vuosina kasvanut. Perinteisen langalliseen verkkoon liitetyn tietokoneen rinnalle on tullut lisää kannettavia tietokoneita, tablet-tietokoneita, älypuhelimia, älykelloja, sekä erilaisia IoT-laitteita ja -sensoreita, jotka useimmiten voivat hyödyntää langattomia 2.4GHz- sekä 5GHz-taajudella toteutettuja WLAN-lähiverkkoja. WLAN-verkot ovat erityisen tärkeitä mobiililaitteille myös ympäristöissä, joissa matkapuhelinverkossa ei välttämättä ole riittävää kuuluvuutta esimerkiksi talon rakenteiden tai eristävien ikkunalasien aiheuttaman signaalin vaimenemisen takia. Myös työympäristöissä WLAN on tärkeässä roolissa liikuteltavien laitteiden yleistyttyä myös työpaikoilla.

Tässä työssä perehdyttiin langattomien verkkojen ja lähiverkkojen mahdollisten ongelmien tunnistamiseen, testaukseen ja toimintaan. Lähiverkkoon liittyneelle loppukäyttäjälle näkyviä ongelmia voi esiintyä käyttäjän laitteesta johtuvista syistä, paikallisen verkon vikatilasta, tai laajemmasta paikallisen verkon ulkopuolisesta internet-ongelmasta johtuen. Idea tähän työhön tuli tilanteesta, jossa ICT-palveluita tarjoavan yrityksen asiakas kertoo ongelmista WLAN-verkon kanssa asiakkaan toimipisteillä, joissa ei ole yhtään IT-asiantuntijaa paikalla. Tällöin olisi hyvä saada paras mahdollinen kuva verkon tilanteesta ja tapahtumista ongelmahetkellä, vaikka viasta kertovalla asiakkaalla ei välttämättä olisi taitoja kertoa ongelman ratkaisemisessa tarvittavia ja olennaisia lisätietoja verkosta. Olennaisia tietoja voivat olla esimerkiksi verkon kuuluvuus, saako asiakkaan tietokone IP-osoitetta, tai onko esimerkiksi ulkoverkon yhteys katkennut, vaikka sisäverkko toimii.

Työssä toteutettiin Raspberry Pi -alustalle tietoliikenneverkon valvontajärjestelmä, jolla voidaan valvoa ja testata etänä asiakkaan tiloihin asennettua verkkoa, ja kerätä siitä mahdollisen vian selvittämisessä auttavaa tietoa etänä toimiville IT-asiantuntijoille. Työssä käytettävä laitteisto ja ohjelmisto asennetaan valvottavaan verkkoon, ja mahdollisissa vikatilanteissa sen keräämän tiedon avulla voidaan pyrkiä päättelemään, johtuuko vikatilanne erinäisistä mahdollisista verkko-ongelmista, vai yksittäisen käyttäjän laitteen ongelmasta. Vianetsinnässä käytettävät testit on suunniteltu vastaamaan verkon loppukäyttäjän tietokoneen toimia, joita tavalliseen verkon käyttöön liittyy käyttäjän tai käytettävän laitteen näkökulmasta. Tässä työssä selvitetään, miten tästä ideasta rakennettiin ratkaisu, jonka avulla asiakasympäristöjen lähiverkkoja voidaan helposti valvoa ongelmien varalta jatkuvasti etänä.

2. TAUSTAA

Lähiverkolla tarkoitetaan verkkolaitteista ja sitä hyödyntävistä asiakaslaitteista koostuvaa kokonaisuutta. Tyypillisesti lähiverkossa on ainakin reititin, kytkin, ja usein myös WLAN-tukiasemia. On myös mahdollista käyttää näitä ominaisuuksia yhdisteleviä laitteita. WLAN-verkolla tarkoitetaan IEEE:n 802.11-standardin mukaan määriteltyjä langattomia lähiverkkoja. WLAN-verkko on edullinen ja mahdollistaa paikasta riippumattoman verkon käytön, mutta on myös kaapeloitua verkkoa alttiimpi häiriöille.

Domain Name System eli nimipalvelujärjestelmä yhdistää verkkotunnuksia IP-osoitteisiin. Järjestelmä on tarpeellinen käyttäjäystävällisyyden kannalta, koska IP-osoitteet ovat hankalia muistaa eivätkä kuvaa osoitteessa tarjottuja palveluja. DHCP-palvelu mahdollistaa automaattisen verkkoasetusten konfiguroinnin lähiverkoissa, ja ARP on tarpeellinen protokolla laitteen MAC-osoitteen selvittämiseksi IP-osoitteen perusteella.

Lähiverkkoihin voi myös kohdistua tietoturvauhkia sekä verkossa käytettyjen teknologioiden osalta, että myös verkkoon liitettyjen haavoittuvaisten ja murrettujen asiakaslaitteiden osalta.

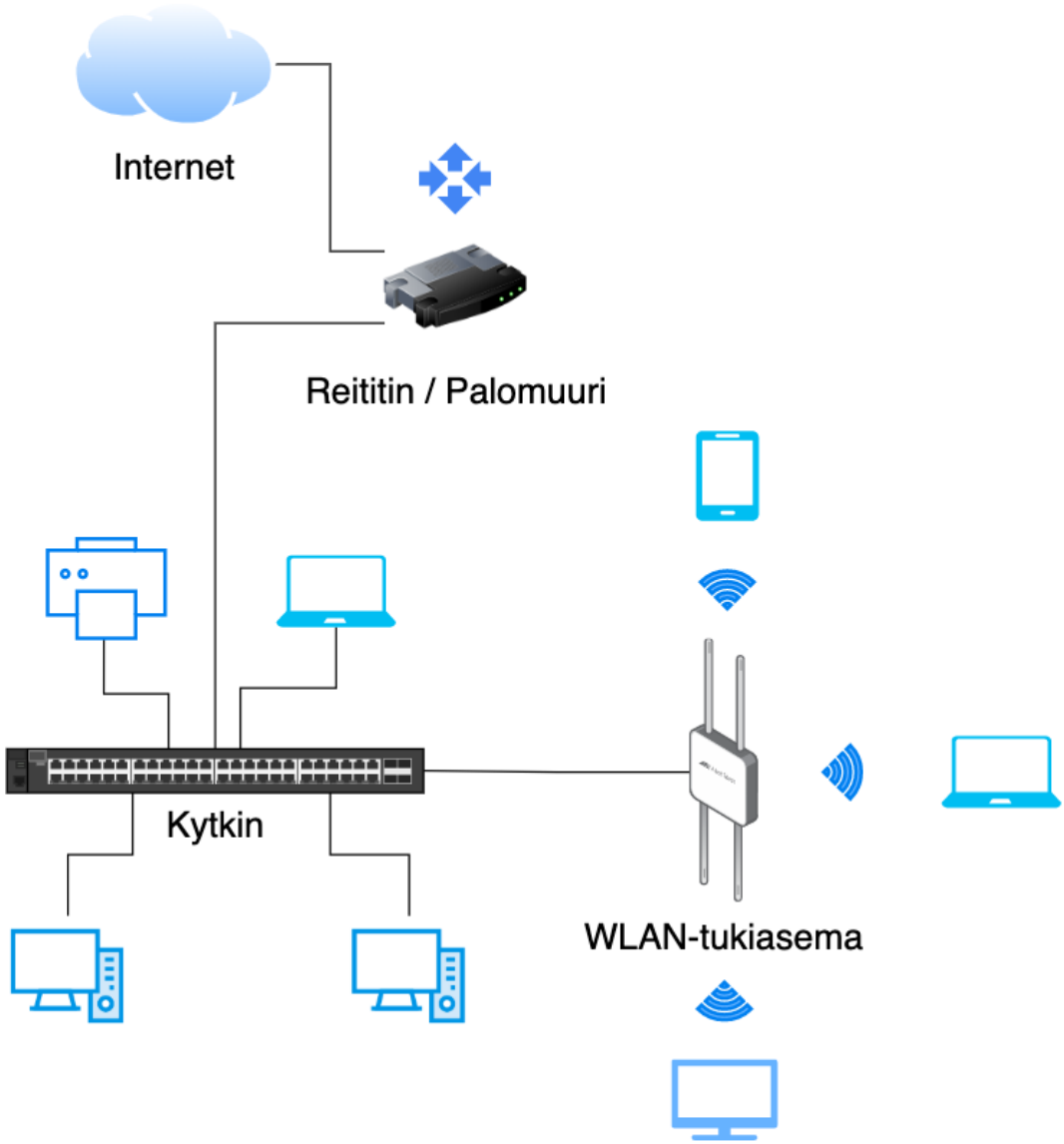
2.1. Lähiverkko

Lähiverkolla tarkoitetaan laiteympäristöä, jotka on liitetty yhtenäiseen verkkoon tyypillisesti yhdessä sijainnissa, esimerkiksi kotona, toimistorakennuksessa yksittäisen yrityksen tiloissa, tai yliopiston tiloissa [1]. Tyypilliseen lähiverkkoon kuuluu loppukäyttäjien tietokoneiden ja mobiililaitteiden lisäksi myös reitittimiä, kytkimiä, ja WLAN-tukiasemia [2], kuten kuvassa 1. Lähiverkon laitteet voivat käyttää yhtä internet-yhteyttä ulkoverkkoon liikennöimiseen, ja lähiverkossa voidaan jakaa esimerkiksi verkkotulostimen tai palvelimen resursseja useille käyttäjille helposti. Lähiverkko mahdollistaa verkossa olevien laitteiden välille suuren tiedonsiirtokapasiteetin verkon fyysisen rakenteen ja käytetyn teknologian niin salliessa, koska yksittäisessä sijainnissa verkossa rajoittavia tekijöitä on vähän, ja liikenne ei kierrä internetin kautta [1].

Lähiverkossa käytettäviä tyypillisiä verkon toimintaa mahdollistavia laitteita ovat reititin, kytkin, ja WLAN-tukiasemat. Yritysverkoissa nämä ovat yleensä erillisiä laitteita, mutta kuluttajille markkinoidut laitteet ja operaattorien kuluttajille suunnattujen internetliittymien mukana tarjottavat laitteet ovat usein yksittäinen laite, joka osaa edellä mainitut toiminnot yhdessä paketissa. Näistä toiminnoista reitittimen tehtävä on välittää tietoliikennettä internetin ja lähiverkon välillä, sekä tarvittaessa liittää useita lähiverkkoja toisiinsa. Kytkimen tehtävä lähiverkossa on yhdistää useita laitteita verkkoon, ja mahdollistaa kommunikointi laitteiden välillä. WLAN-tukiasemat ovat toiminnallisuudeltaan lähellä kytkimiä, eli niiden avulla myös langattoman yhteyden kautta yhdistävät laitteet voivat liittyä verkkoon ja kommunikoida muiden lähiverkon laitteiden kanssa.

Lähiverkko voidaan jakaa edelleen virtuaalisiin lähiverkkoihin eli VLAN-verkkoihin, mikäli halutaan edelleen eriyttää samoihin verkkolaitteisiin yhdistettyjä laitteita toisistaan. Näin esimerkiksi yritysverkoissa lähekkäisten osastojen verkot

voivat olla erillisiä toisistaan eristettyjä verkkoja, mutta käyttää silti samoja fyysisiä lähiverkon verkkolaitteita.



Kuva 1. Verkkokuva yksinkertaisesta lähiverkosta. Kuvan lähiverkko koostuu reitittimestä, kytkimestä, WLAN-tukiasemasta, sekä loppukäyttäjien laitteista.

2.2. WLAN

Wireless Local Area Network eli WLAN on langattomiin verkkoihin käytetty tekniikka, jossa WLAN-tukiaseman kautta voidaan yhdistää laitteita tietoverkkoon langattomasti. WLAN-verkkoja määrittelee IEEE:n standardi 802.11 [3]. Uusia verkkoteknologioita kehitetään jatkuvasti lisää, ja jokaiselle on omat standarditunnuksensa. Tällä hetkellä yksi moderni ja laajasti tuettu verkkostandardi on IEEE 802.11ac, jossa verkko toimii 5GHz:n taajuudella. Myös IEEE 802.11ax

joka tunnetaan myös nimellä ”WiFi 6” kasvattaa suosiotaan, ja tuki tälle verkolle löytyy vasta aivan uusimmista laitteista.

WLAN-verkon etuja on langattomuuden tuoman edullisuuden lisäksi myös käyttäjien laitteiden helppo liikuteltavuus verkon kantama-alueella. Verkkokaapelointi luo kuluja asennusvaiheessa, ja kaapelointi rajoittaa yksittäisen käyttäjän tiettyyn pisteeseen johon kaapelointi on tuotu. Yksinkertaisissa WLAN-verkoissa liikkuminen on mahdollista tietyn tukiaseman kantaman alueella, mutta usean tukiaseman asennuksissa liikkuminen useampien tukiasemien alueella on myös mahdollista ilman negatiivisia vaikutuksia verkon käyttökokemukselle.

Langattomaan verkkoon yhdistettävien laitteiden suosio on kasvussa. Yleisimpiä laitteita WLAN-verkoissa ovat puhelimet, kannettavat tietokoneet, tabletit, ja älykellot. Lisäksi usein IoT-laitteita voidaan yhdistää myös WLAN-verkkoihin.

WLAN-verkkojen yleistymisen myötä mm. yrityksen asiakkaille tarjottavat lähiverkot ovat myös yleistyneet lähes kaikkialla. Nykyään WLAN-verkkoja löytyy hyvin monipuolisista ympäristöistä; toimistojen ja kotien lisäksi esimerkiksi ravintoloissa, kahviloissa, kaupoissa, ja jopa lentokoneissa on usein WLAN-verkko käytettävissä asiakkaiden laitteita varten [2].

WLAN-verkkojen nimistä käytetään termiä SSID (Service Set Identifier), kun taas yksittäiset tukiasemat tunnistaa BSSID-tunnisteesta (Basic Service Set Identifier). Yksi WLAN-tukiasema voi palvella useaa eri nimistä WLAN-verkkoa. Huomionarvoisia ominaisuuksia tässä työssä WLAN-verkon toimivuuden ja valvonnan kannalta ovat myös langattoman verkon kuuluvuus sekä signaalinvoimakkuus, mutta myös erilaiset verkkojen käyttämät taajuudet.

2.3. Domain Name System

Domain Name System eli DNS, suomeksi nimipalvelujärjestelmä, on yksi tärkeä osa verkkoja, sekä paikallisessa verkossa että Internetissä laajempana kokonaisuutena. DNS:n tarkoitus on yhdistää verkkotunnuksia IP-osoitteisiin. Tämä on tarpeellista koska verkkotunnusten nimet ovat yleensä palvelun käyttötarkoitusta tai sisältöä kuvaavia ja helposti muistettavia, toisin kuin numeeriset IPv4-osoitteet tai alfanumeeriset IPv6-osoitteet. Esimerkiksi Oulun Yliopiston verkkosivuille pyrkiessä osoite oulu.fi on huomattavasti helpompi muistaa, kuin IPv4-osoite 130.231.240.1, johon DNS-kysely osoitteelle oulu.fi ohjaa. IPv6-osoitteet ovat vielä huomattavasti IPv4-osoitteita monimutkaisempia pidemmän muodon sekä alfanumeerisen merkistön takia, joten nimipalvelun merkitys korostuu entisestään IPv6:n yleistyessä.

DNS-palvelimia on useita toiminnallisuudeltaan eroavia tyyppejä: rekursiivinen (recursive), juurinimipalvelin (root), ylätason nimipalvelin (TLD) ja auktoritatiivinen nimipalvelin (authoritative) [4]. Rekursiivinen DNS-palvelin on tämän työn kannalta oleellisin, sillä se on käytännössä aina DNS-palvelimen tyyppi, joka käyttäjän laitteelta tulevat kyselyt ottaa ensimmäisenä vastaan. Rekursiivinen DNS-palvelin säilyttää aiemmin haettuja ja usein käytettyjä osoitteita välimuistissaan (DNS-cache), jotta pyyntöjen käsittely olisi nopeampaa [5]. Näin jokaista DNS-pyyntöä ei tarvitse lähettää uudelleen muille nimipalvelimille, vaan vastaus saadaan rekursiivisen DNS-palvelimen muistista nopeasti. Konfiguraatiosta riippuen, yleensä rekursiivinen DNS-palvelin suorittaa edelleen kyselyitä eteenpäin muille nimipalvelimille vain, mikäli ajantasaista tietoa kysytystä osoitteesta ei löydy kyseisen palvelimen DNS-tietojen välimuistista [6]. DNS-välimuistin tiedot vanhenevat tietyn konfiguroitavissa

olevan ajan välein, jotta mahdollisesti muuttuneet tiedot tulevat aina lopulta päivitetyksi [7].

Juurinimipalvelin vastaanottaa ketjussa aiemmille nimipalvelimille tuntemattomien osoitteiden kyselyitä, ja ohjaa ne edelleen TLD-nimipalvelimille. TLD-nimipalvelimet vastaavat esimerkiksi maakohtaisista ja yleiskäyttöisistä osoitteista, kuten esimerkiksi .fi ja .com -verkkotunnuksien osoitteista. TLD-nimipalvelimet ohjaavat kyselyitä edelleen auktoritatiivisille nimipalvelimille [4].

Auktoritatiivinen DNS-palvelin pitää yllä DNS-tietueita, joista selviää lopullinen ja ajantasainen tieto siitä, mikä nimi ohjataan mihinkin IP-osoitteeseen. Tämän tyyppinen DNS-palvelin osaa vastata sille kuuluvien osoitteiden DNS-kyselyihin suoraan ilman tarvetta välittää kyselyä toisille palvelimille, ja auktoritatiivisen DNS-palvelimen vastausta pitäisi aina käyttää välimuistiin tallennetun tiedon sijaan, mikäli ne eroavat toisistaan. [6] Mikäli auktoritatiivinen DNS-palvelin saa kyselyn verkkotunnuksesta, jolle se ei ole auktoritatiivinen, kysely voidaan välittää edelleen toiselle ylemmän tason verkkopalvelimelle.

Yleensä olemassa oleva verkkotunnus löytyy viimeistään juuritason nimipalvelimien avustuksella, sillä kyselyt välittyvät aina alemman tason nimipalvelimilta ylöspäin, mikäli vastausta ei löydy. Mikäli verkkotunnusta ei löydy nimipalvelusta ollenkaan, voidaan kyselyyn vastauksena palauttaa myös siitä kertova virheilmoitus [8].

Jokaisella Internetiin liitetyllä laitteella on IP-osoite tai mahdollisesti useampi, joten käytettävyyden helpottamiseksi nimipalvelujärjestelmä on tarpeellinen. DNS:n toiminta on siis hyvin olennaista verkon sujuvan toiminnan ja käytettävyyden kannalta loppukäyttäjän näkökulmasta, ja DNS-palvelinten toimivuutta sekä saavutettavuutta on siksi hyödyllistä valvoa ja tutkia mahdollisissa ongelmatilanteissa.

2.4. Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol eli DHCP on protokolla, jonka avulla verkkoon voidaan liittää laitteita dynaamisesti ilman etukäteistietoa tarvittavista verkkoasetuksista [9]. Jokainen verkkoon liitettävä laite tarvitsee oman IP-osoitteensa, eikä samaa IP-osoitetta tule käyttää samassa verkossa usealla eri laitteella yhtä aikaa. Jotta IP-osoitteista ja niiden käytöstä ei tarvitsisi pitää kirjaa manuaalisesti itse, IP-osoitteiden sekä muiden tarvittavien verkkoasetusten jakaminen voidaan automatisoida DHCP-palvelimella [10].

DHCP-palvelin ylläpitää listaa verkossa käytettävistä ja saatavilla olevista IP-osoitteista [9]. DHCP-palvelin jakaa pyynnön tehneille laitteille yleensä laitekohtaisten IP-osoitteiden lisäksi muitakin verkon tietoja, kuten esimerkiksi oletusyhdyskäytävän (default gateway), aliverkon peitteen (subnet mask), sekä DNS-palvelimien osoitteet. Kotikäytössä DHCP-palvelin on yleensä käytössä Internet-palveluntarjoajan toimittamalla reitittimellä, mutta DHCP-palvelin voi olla myös reitittimestä erillisenä ratkaisuna esimerkiksi yritysverkoissa. DHCP-palvelimia voidaan käyttää sekä IPv4- että IPv6-verkoissa [10], joskin IPv6:ssa on olemassa osittain DHCP:n toimintaa vastaava ominaisuus ”Stateless Autoconfiguration”.

DHCP toimii ilman autentikaatiota [10]. Tällöin DHCP-kyselyn tekevä laite voi esittää olevansa jokin muu laite, mutta myöskin DHCP-palvelin voi olla jokin toinen laite kuin verkon ylläpitäjä on tarkoittanut. DHCP-asiakaslaite lähettää viestinsä

yleislähetyksenä koko verkkoon broadcast-osoitteella, mutta vain DHCP-palvelimien on tarkoitus vastata siihen [9]. Mikään ei estä lisäämästä esimerkiksi virheellisesti konfiguroitua tai ylimääräistä DHCP-palvelinta verkkoon, jolloin joidenkin laitteiden kyselyt ja vastaukset voivat ohjautua mahdollisesti väärin konfiguroitujen DHCP-palvelimien kautta.

DHCP-palvelimien jakamilla IP-osoitteilla on yleensä määritelty tietty vanhenemisaika (DHCP lease time) [9], jonka jälkeen laitteen on pyydettävä IP:n uusimista. Useimmiten DHCP-palvelin myöntää laitteelle saman IP:n joka sillä oli käytössä aiemmin, mutta on myös mahdollista että laitteen IP-osoite vaihtuu [11]. Samaa IP-osoitetta ei voi käyttää kuin yksi laite kerrallaan, mutta esimerkiksi saman päivän aikana tietty aiemmin käytetty IP-osoite voidaan jakaa uudelle laitteelle eri aikaan, mikäli aiemmin osoitetta käyttänyt laite ei ole enää verkossa.

IP-osoitteiden uudelleen käyttämisen tarve riippuu DHCP:lle käytettävissä olevan IP-osoiteavaruuden koosta. Mikäli verkossa käy paljon laitteita, mutta jaettava IP-osoiteavaruus on pieni, tarvitaan lyhyt DHCP:n vanhenemisaika, jotta osoitteita vapautuisi nopeasti uudelleen käytettäväksi, ja niitä riittäisi aina tarvittavalle määrälle laitteita. Vastaavasti jos jaettava IP-osoiteavaruus on lähes sama tai suurempi kuin verkossa vierailevien laitteiden määrä, DHCP:n vanhenemisaika voidaan tarvittaessa määritellä myös hyvin pitkäksi.

Useimmiten laitteille annettavan IP-osoitevarauksen vanhenemisajaksi halutaan määritellä kohtuullisen pitkä aika, jolla kuitenkin saadaan ylläpidettyä kohtuullinen IP-osoiteavaruuden täyttöaste. Näin ruuhkapiikkien aikaan osoitteita silti riittää jaettavaksi kaikille laitteille [11]. Mikäli DHCP:n jakama IP-osoiteavaruus on täynnä aktiivisia laitteita, DHCP-palvelin ei voi jakaa asiakkailleen vapaana olevia IP-osoitteita, ja siten verkkoon ei pääse yhdistämään enää lisää laitteita ilman ongelmia. Loppukäyttäjien laitteilla IP-osoitteen puuttuminen näkyy verkon toimimattomuutena, vaikka verkkoon näennäisesti pystyy yhdistämään.

2.5. Address Resolution Protocol

Address Resolution Protocol eli ARP on protokolla, jonka tarkoitus on auttaa selvittämään tietyn IP-osoitteellisen laitteen MAC-osoite [12]. Tämä on tarpeen esimerkiksi Ethernet-verkoissa, sillä kommunikoidakseen toisen laitteen kanssa, täytyy tietää vastaanottajan fyysinen osoite, eli MAC-osoite.

Vastaanottajalaitteen tuntemattoman MAC-osoitteen selvittämiseksi lähettäjäpään laite lähettää verkon broadcast-osoitteeseen ARP-pyynnön, jossa mainitaan haluttu vastaanottajan IP-osoite [12]. Kyseistä IP-osoitetta käyttävä laite vastaa ARP-pyyntöön omalla MAC-osoitteellaan. Broadcast-osoitteen takia kaikki verkon laitteet näkevät pyynnön, mutta protokollan mukaan vain yksittäisen ARP-pyynnössä mainitun laitteen on tarkoitus vastata siihen.

Verkossa toimivien laitteiden on tarkoitus säilyttää saatuja osoitetietoja ARP-taulussa, joka sisältää muiden verkossa olevien laitteiden IP-osoitteen, sitä vastaavan MAC-osoitteen, sekä tietojen vanhenemisajan (TTL, time-to-live).

Historiallisesti ARP suuniteltiin alun perin käytettäväksi tietyn tyyppisten 10Mbit/s Ethernet -verkkojen kanssa, mutta se sitä käytetään myös yleisemmin IPv4-verkoissa. IPv6-verkoissa samankaltaista toiminnallisuutta toteuttaa Neighbor Discovery Protocol [13].

2.6. Lähiverkon kyberturvallisuus ja uhat

Lähiverkossa oleviin laitteisiin kohdistuu myös tietoturvauhkia, vaikka ne eivät olisi suoraan avoimena internetissä. Langattomissa verkoissa ei välttämättä ole salausta ollenkaan, tai salaus voi olla vanhentunutta tyyppiä ja siten helposti murrettavissa. Langattomat verkot ovat helppo tapa päästä sisään lähiverkkoihin ilman fyysistä murtautumista, mutta toisaalta myös yleistyneet IoT-laitteet ja päivittämättömät ohjelmistot mahdollistavat paljon hyökkäyspinta-alaa lähiverkoissa. Murrettuja tai saastuneita verkkoon liitettyjä laitteita voidaan edelleen verkkoyhteyttä hyödyntäen käyttää hyväksi erilaisissa palvelunestohyökkäyksissä ja bottiverkoissa, tai muihin laitteisiin murtautumisessa. Langattomia verkkoja voidaan myös hyödyntää tietojenkalastelussa, esittämällä käyttäjälle luotettua verkkoa.

2.6.1. WLAN-verkkojen tietoturva

WLAN-verkko aiheuttaa lähiverkolle langallisesta verkosta poikkeavia uhkakuvia langattomuuden takia. Langattoman verkon kuuluvuus ei lopu esimerkiksi yrityksen toimitilojen seiniin, vaan verkko kuuluu usein myös viereisiin tiloihin tai jopa rakennusten ulkopuolelle. WLAN-verkot ovat siten houkutteleva kohde murtautumiselle, koska fyysistä pääsyä verkkoon tai verkkolaitteisiin ei välttämättä tarvita [14]. Langattomaan verkkoon kytkettyjä laitteita voidaan käyttää hyväksi esimerkiksi roskapostin lähettämiseen, teollisuusvakoiluun, ja muihin verkkoon liitettyihin laitteisiin hyökkäämiseen [14].

Langattomat lähiverkot on useimmiten suojattu erilaisia salausprotokollia hyväksikäyttäen, mutta myös avoimet ja salaamattomat verkot ovat yleisiä. Tutkitusti esimerkiksi Yhdysvalloissa noin 45 % langattomista verkoista eivät ole salattuja [15]. Salatuissa verkoissa käyttäjältä voidaan vaatia verkkoon liittymiseksi esimerkiksi salasanaa, käyttäjätunnus- ja salasanaparia, tai sertifikaattia. Yleisesti käytettyjä salausprotokollia ovat muun muassa WEP, WPA, WPA2, ja WPA3 [16][17]. Myös ”MAC filtering” eli suodatus laitteiden MAC-osoitteiden perusteella on mahdollista. Tällöin pääsy verkkoon voidaan sallia tai estää laitteiden MAC-osoitteiden mukaan [18]. MAC-osoitteet ovat teoriassa uniikkeja laitteen verkkokorttiin liitettyjä tunnisteita, mutta verkkokorttiin liitetty MAC-osoite on myös mahdollista väärentää. MAC-osoitteiden perusteella ei kuitenkaan voida tunnistaa käyttäjiä, sillä tiettyä laitetta käyttävä käyttäjä ei eroa mitenkään toisesta käyttäjästä, joka voi käyttää samaa laitetta toisen käyttäjän kanssa.

WEP on vanha, vuonna 1999 suunniteltu salausprotokolla, joka on jo pitkään tiedetty helposti murrettavaksi salausprotokollaksi. Sen käyttö WLAN-verkkojen salauksena nykypäivänä on tietoturvariski vanhentuneen algoritmin ja avainten uudelleenkäytön vuoksi [16]. Hyökkääjän on mahdollista selvittää WEP-protokollan salausavain, ja salausavainta käyttäen on mahdollista kuunnella kaikkea verkon liikennettä [19].

WPA ja siitä edelleen paranneltu WPA2 ovat olleet pitkään hyvin yleisesti käytössä langattomissa verkoissa. WPA-protokollaa pidetään väliaikaisena ratkaisuna WEP-protokollan ongelmiin, kunnes WPA2 valmistui [16]. WPA2 julkaistiin vuonna 2004 ja se on edelleen laajasti käytössä. WPA2 on kuitenkin haavoittuvainen esimerkiksi sanastohyökkäyksille, joissa kokeillaan erilaisia sanoja ja merkkijonoja niin kauan, kunnes oikea salasana löytyy. Erilaisilla ”Brute Force”-

tyyppisillä työkaluilla on mahdollista kokeilla jopa 300 miljoonaa erilaista salasanaa noin 20 minuutissa [19]. Uusimmassa WPA3-protokollassa on pyritty muun muassa estämään sanastohyökkäyksien käyttöä [17]. Uudempien salausprotokollien käytön vaikutus lähiverkon suorituskykyyn on hyvin pieni [16] ja lähes kaikki nykyaikana käytettävät langatonta verkkoa hyödyntävät laitteet tukevat usein vähintään WPA2-protokollaa. Suositeltu vähimmäistaso langattomien lähiverkkojen salaukselle on WPA2, monimutkaista ja pitkää salasanaa käyttäen [3].

WLAN-verkkoja voidaan myös käyttää tietojenkalasteluun. Esimerkiksi niin kutsutuissa ”Evil twin”-tyyppisissä hyökkäyksissä huijataan käyttäjiä yhdistämään verkkoon, joka esittää luotettavaa verkkoa. Tyypillisesti hyökkäyksissä luodaan luotettua SSID:tä käyttävä verkko, ja yritetään saada käyttäjiä yhdistämään verkkoon luotettavan nimen ja paremman verkon kuuluvuuden perusteella. Kun käyttäjä liittyy hyökkääjän verkkoon, hyökkääjä voi tarkastella käyttäjien verkkoliikennettä sen kulkiessa hyökkääjän hallitseman verkkolaitteen kautta. Verkkoliikennettä voidaan myös mahdollisesti ohjata tietojenkalastelua varten tehdyille sivustoille oikeiden sivustojen sijaan. Näin hyökkääjä voi ohjata käyttäjän esimerkiksi verkkopankkia esittävälle sivustolle, ja siten kerätä käyttäjän mahdollisesti syöttämät kirjautumistiedot.

2.6.2. Haitallinen verkkoliikenne

Verkkoon liitettävien laitteiden yleistyessä myös lähiverkoissa tapahtuva haitallinen verkkoliikenne on kasvanut. Erityisesti virheellisesti konfiguroidut tai vanhoja ohjelmistoversioita käyttävät IoT-laitteet ovat usein osallisena haitalliseen verkkoliikenteeseen niin yritysten kuin kotitalouksien verkoissa.

Haitallinen liikenne on tärkeää tunnistaa, jotta ongelmia voidaan korjata liikenteeseen osallistuvalta laitteelta, sekä ennaltaehkäistä vastaavia tietoturvaongelmia jatkossa. Haitallista liikennettä voidaan lähiverkossa seurata ja tunnistaa liikennettä analysoimalla. Esimerkiksi lähdelaitteen portin sekä kohdelaitteen IP-osoitteen ja portin yhdistelmän avulla voidaan yrittää erotella bottiverkkoihin osallistuvaa liikennettä normaalin verkkoliikenteen joukosta [20]. Myös poikkeuksellisen paljon verkkoliikennettä aiheuttavia laitteita kannattaa tarkastella. Manuaalisesti liikenteen analysointi on työlästä, mutta haitallisen liikenteen analysointi on erityisesti yritysverkoissa toteutettu usein palomuureilla, IDS-järjestelmillä, tai IPS-järjestelmillä. IDS- ja IPS-järjestelmien ero palomuureihin on verkkoliikenteen syvällisempi tarkastaminen, pelkkien protokollien sekä lähde- ja kohdeosoitteiden sijaan [21].

Haavoittuvuuksien kautta hyväksikäytettävillä laitteilla voidaan muun muassa suorittaa DDoS-hyökkäyksiä ja osallistua bottiverkkoihin [22]. Haitallista liikennettä verkossa tuottava laite voi tietoturvallisuuden uhkien lisäksi myös vakavasti haitata lähiverkon käytettävyyttä ja suorituskykyä. Edellä mainittu palvelunestohyökkäys perustuu tehtyjen pyyntöjen suureen määrään, ja siten myös kuormittaa verkkoa huomattavan paljon. Tällöin muut verkossa liikennöivät laitteet eivät saa käytettäväksi tavanomaista verkkokapasiteettia. Lähiverkossa esimerkiksi WLAN-tukiasemat sekä internetyhteys voivat olla rajoittavia tekijöitä, joiden kapasiteetti loppuu helposti kesken liian suuren liikennöintimäärän takia.

Verkkoliikenteen kapasiteettiongelman lisäksi myös esimerkiksi yrityksen tai operaattorin IP-osoitteen maineelle voi aiheutua ongelmia haitallisesta verkkoliikenteestä. Hyväksikäytettävä IoT-laite voi osallistua esimerkiksi

roskapostien lähettämiseen. Tällöin verkon omistajan oikea sähköpostiliikenne saattaa myös kärsiä, mikäli omistajataho ylläpitää itse sähköpostipalvelimia. Useimmiten roskapostia lähettävät osoitteet päätyvät nopeasti estolistoille, joista lähtevät sähköpostit merkataan roskapostiksi, tai niitä ei toimiteta vastaanottajalle perille ollenkaan.

3. VERKKOJEN ANALYSOINTI

Loppukäyttäjälle ilmeneviä verkko-ongelmia etsiessä täytyy käytännössä tarkastella useita erilaisia verkon komponentteja, joista sekä paikallinen lähiverkko että internet koostuvat. Esitellyille verkon komponenteille on työssä tunnistettu käyttäjän näkökulmasta olennaisimpia valvottavia ominaisuuksia, ja kehitetty niille testejä valvontaa varten.

Langattomien verkkojen kanssa ongelmaksi usein muodostuu verkon kuuluvuus ja häiriöt. Muut langattomat verkot samalla taajuudella voivat haitata suorituskykyä, ja myös asuintalojen ja toimistojen rakennusmateriaalit vaikuttavat langattoman verkon kuuluvuuteen. Myös WLAN-tukiaseman vikaantuminen tai jumittuminen on jokseenkin yleistä. Kaapeloidussa verkossa voidaan myös käyttää monia samoja testejä verkon toimivuudelle, kuin langattoman lähiverkon kanssa.

DHCP:n toiminnan valvomisessa on olennaista DHCP-palvelimen saavutettavuus, sekä palvelimen tarjoamien verkkoasetusten oikeellisuus. Palvelusta ei ole hyötyä, mikäli se tarjoaa virheellisiä verkkoasetuksia käyttäjille. Myös nimipalvelun valvonta ja testaaminen lähtevät nimipalvelinten saatavuudesta. Usein mahdolliset virhetilanteet johtuvat väärin konfiguroidusta nimipalvelimesta, tai nimipalveluliikennettä estävistä palomuurisäännöistä.

3.1. WLAN-verkkoon liittyminen ja kuuluvuus

Langattomaan verkkoon liityttäessä laitteet skannaavat lähiympäristössä kuuluvat WLAN-verkot, ja yleensä liittyvät verkkoon automaattisesti. Automaattinen verkkoon liittyminen vaatii, että verkko on entuudestaan tallennettu laitteelle. Laite täytyy myös olla konfiguroitu liittymään tunnettuihin verkkoihin automaattisesti, mutta useimmissa käyttöjärjestelmissä tämä on oletusasetus. Ensimmäinen mahdollinen vikatilanne voi olla verkon löytyminen ja kuuluminen. Mikäli verkkoa ei löydy ollenkaan tai signaali on liian heikko, verkkoon liittyminen ja sen käyttäminen ei onnistu. Tällöin on hyödyllistä tarkastella ympäristöstä löytyviä WLAN-verkkoja. WLAN-verkkojen kuuluvuus voi esimerkiksi olla heikkoa, tai jokin tietty 2.4GHz tai 5GHz:n kanava voi toimia heikosti WLAN-verkon ulkopuolisten laitteiden aiheuttamien häiriöiden takia. Myös jonkin toisen WLAN-verkon taajuus voi olla päällekkäinen käytetyn WLAN-verkon taajuuden kanssa.

Yhdessä WLAN-verkossa voi olla myös useita tukiasemia. Tällöin on hyödyllistä mahdollisten ongelmatilanteiden vianselvityksen kannalta tarkastella myös tukiasemien toimintaa samassa verkossa erikseen. Näin esimerkiksi yksittäisestä vikaantuneesta WLAN-tukiasemasta johtuvien ongelmien jäljille on mahdollista päästä helposti.

3.2. Lähiverkon toimivuus

WLAN-verkon kuuluvuuden ja verkkoon liittymisen jälkeen mahdolliset ongelmakohdat ovat samat, vaikka verkkoa käyttäisi myös langallisen verkon kautta. Moni tässä työssä luoduista työkaluista toimii siten yhtä lailla myös tapauksissa, joissa halutaan valvoa WLAN-verkon lisäksi myös kaapeloidun lähiverkon

toimintaa. Lähiverkon ongelmia tutkiessa esimerkiksi kaapeloidun verkon yhdistyminen verkkolaitteeseen sekä oletusyhdyskäytävän saatavuus ovat mahdollisia testattavia kohteita ja ongelmakohtia lähiverkon toimivuudessa. Mikäli yhteyttä verkon oletusyhdyskäytävään ei ole saatavilla, yhdistäminen laitteelle kytketyn aliverkon ulkopuolelle ei onnistu ilman erillistä konfiguraatiota, koska liikenteen pitäisi kulkea oletusyhdyskäytävän kautta.

3.2.1. DHCP:n toiminnan valvominen

Yleensä loppukäyttäjille tarkoitetuissa verkoissa on käytössä DHCP, eli Dynamic Host Configuration Protocol. Tällöin laite kysyy verkkoon liittyessään DHCP-palvelimelta, minkälaisia asetuksia kyseisessä verkossa tulisi käyttää. DHCP-palvelimelta laite saa tarvittavat verkkoasetukset, kuten esimerkiksi IP-osoitteen, verkkomaskin, ja DNS-palvelimien osoitteet.

DHCP:n toiminnassa hyvä lähtökohta on, että DHCP-palvelimeen on mahdollista saada yhteys loppukäyttäjän laitteelta, ja että laite saa kysyttäessä palvelimelta vastauksena sopivat verkkoasetukset kyseiseen lähiverkkoon. Ongelmia voi tulla esimerkiksi, jos DHCP:n antamat verkkoasetukset ovat virheellisiä, tai mikäli vastausta DHCP-kyselyyn ei saada ollenkaan perille päätelaitteelle, esimerkiksi hyvin rajoitetun palomuurikonfiguraation takia. On myös mahdollista, että verkossa on useampia DHCP-palvelimia, jotka antavat toistensa kanssa ristiriidassa olevia vastauksia. Tällöin käyttäjän laite saattaa esimerkiksi toimia vain tietyltä DHCP-palvelimelta saaduilla verkkoasetuksilla, eli käyttäjän näkökulmasta verkon toimivuus saattaa vaihdella satunnaisesti yhdistämiskertojen välillä.

Tässä tapauksessa loppukäyttäjän laitteen toiminnallisuutta mukaillen DHCP:n valvontaa kannattaa suorittaa tekemällä DHCP-kysely palvelimelle valvontalaitteelta. Tällöin halutaan tarkistaa, että vastaus saadaan, ja että vastauksena saadut verkkoasetukset ovat sopivat kyseiseen lähiverkkoon. On kuitenkin myös hyödyllistä suorittaa valvontaa säännöllisin väliajoin, jotta varmistutaan että vastauksena tulee konsistentisti vain yhdenlaisia asetuksia, sillä ylimääräiset ja virheellisesti konfiguroidut DHCP-palvelimet voivat aiheuttaa turhia ongelmia käyttäjille.

Tässä työssä valvonta on toteutettu skriptinä, joka suorittaa DHCP-kyselyn ja vertaa saatuja vastauksia odotettuihin oikeisiin arvoihin, jotka täytyy itse määrittää ohjelmistoon omaa verkkoa vastaaviksi asetuksiksi. Lisäksi voidaan selvittää verkossa olevien DHCP-palvelimien lukumäärä, jolloin voidaan valvoa, ettei verkkoon ilmesty ylimääräisiä DHCP-palvelimia.

On myös mahdollista, että verkossa ei ole DHCP-palvelinta. Tämä ei ole kuitenkaan kovin yleistä, koska tällöin verkkoon liitettyihin laitteisiin täytyy jokaiseen erikseen konfiguroida verkkoasetukset manuaalisesti.

3.2.2. DNS:n toiminnan valvominen

DNS:n toimivuus on loppukäyttäjän kannalta hyvin olennaista, eikä käytännössä tavanomainen internetin käyttäminen ole mahdollista ilman toimivaa DNS-palvelua. Valvominen tässä tapauksessa hyvin helppoa myös loppukäyttäjän toiminnallisuutta replikoiden, ja se kannattaa suorittaa tekemällä DNS-kyselyitä DHCP-palvelimelta

saatuihin DNS-palvelimen osoitteisiin. Tämä vastaa täysin myös käyttäjien laitteiden toimintaa verkossa, jossa loppukäyttäjän laite suorittaisi myös DNS-kyselyitä laitteelle DHCP:lla asetettuihin nimipalvelimiin, kun laitteella käytetään verkkotunnuksen kautta käytettäviä palveluita. Yksi ongelmatilanteissa vianetsintää helpottava testi on tehdä verkon ulkopuoliselle nimipalvelimelle DNS-kysely, jolloin saadaan selville, onko esimerkiksi verkon palomuurilla estetty loppukäyttäjien verkosta kaikki verkon ulkopuoliset DNS-kyselyt. Näin voidaan toimia tyypillisesti tilanteissa, joissa halutaan pakottaa käyttöön esimerkiksi lähiverkon oma nimipalvelin. Tällöin muun muassa manuaalisesti käyttäjän laitteelle asetetut DNS-asetukset voivat aiheuttaa ongelmia, koska käyttäjän näkökulmasta mikään nimipalvelu ei tällöin vastaa itse asetetuilla DNS-asetuksilla.

3.3. Verkon toiminta lähiverkon ulkopuolella

Lähiverkon ulkopuolisen verkon testaamista varten voidaan tarkastella esimerkiksi internetissä sijaitsevien palvelimien saatavuutta, ja niille kommunikaatioon käytettävän yhteyden luotettavuutta. Näitä voidaan testata esimerkiksi HTTP- ja HTTPS-sivustojen latausta testaamalla. Mikäli jokin ennalta määritetty sivusto saadaan ladattua onnistuneesti valvontalaitteella, sen pitäisi olla mahdollista myös muille samassa verkossa oleville käyttäjien laitteille. Työkalua käytettäessä täytyy ottaa huomioon mahdolliset verkon välityspalvelimet, joita toisinaan käytetään erityisesti yritysten verkoissa. Välityspalvelinta käytettäessä valvontalaitteelle täytyy määritellä tarvittavat välityspalvelimen asetukset, jotta testistä saadaan hyödyllisiä tuloksia. Sivulatausten lisäksi ping-työkalulla voidaan myös testata viivettä ja katoavien pakettien määrää haluttuun kohdeosoitteeseen.

4. KAUPALLISET VAIHTOEHDOT

Työssä käytetylle ohjelmistolle on myös kaupallisia vaihtoehtoja, jotka toteuttavat samaa toiminnallisuutta osittain tai kokonaan, tuotteesta riippuen. Jotkin kaupalliset toteutukset toimivat itsenäisinä sensoreina, mutta myös verkkolaitteisiin liitetyllä ohjainohjelmistolla sekä käyttäjien tietokoneisiin asennettavilla ohjelmistoilla on mahdollista tutkia verkon suorituskykyä ja mahdollisia ongelmia.

4.1. NetBeez

Vastaavanlaisia verkonvalvontatoteutuksia kuin tässä kandidaatintyössä käsitellään, on myös saatavilla kaupallisina ratkaisuina. Eniten tätä työtä ominaisuuksiltaan vastaava kaupallinen tuote, joka on valmis ratkaisu, on tällä hetkellä NetBeezin kehittämä valvontajärjestelmä. NetBeez tarjoaa kehittämäänsä ratkaisua juuri loppukäyttäjän näkökulmasta tapahtuvaan verkon seurantaan. NetBeezin valikoimassa on sekä langallisen että langattoman verkon valvonnan mahdollistavia sensoreita. Osassa Netbeezin tuotteita on myös käytetty Raspberry Pi:tä alustana. NetBeezin edullisin sensori käyttää Raspberry Pi -alustaa, mutta erillisellä WLAN-adapterilla Raspberry Pi:n oman WLAN-adapterin sijaan [23]. Sen lisäksi vaihtoehdoissa on myös tehokkaampi Intel Atom -pohjainen sensorialusta, sekä virtuaaliympäristöissä käytettäviä valmiita Linux-pohjaisia Virtual Appliance -levykuvia esimerkiksi VMware-ympäristöön.

NetBeezin langatonta verkkoa valvovat laitteet seuraavat WLAN-verkosta kuuluvuutta ja signaalin laatua, eri tukiasemien kuuluvuutta, ja yhdistävät laitteensa internetiin langattoman verkon kautta. Sensorilaitteet suorittavat erilaisia testejä, kuten, verkon nopeustestejä, pingaavat internetissä tiettyjä osoitteita, ja lataavat verkkosivuja [23].

Kokonaisuuteen kuuluu keskitetty hallintapaneeli, johon tietoa eri sijainneista keräävät sensorin raportoivat havaintonsa. Hallintapaneeli visualisoi tietoa esimerkiksi verkon ylläpitäjien käyttöön. NetBeezin tuotteessa on myös valmiita integraatioita, muun muassa datankeräyssovellus Splunkiin [23].

4.2. Aruba

Toinen samankaltainen kaupallinen tuote on Cape Networksin tuote Cape, jonka Aruba sittemmin osti ja uudelleennimesi Aruba Service Assurance Sensoriksi. Myös tässä tapauksessa käytetään sensorilaitteita, jotka sijoitetaan erikseen jokaiseen sijaintiin, jonka verkkoa halutaan valvoa. Aruban sensorit raportoivat havaintonsa heidän palvelukokonaisuuteensa kuuluvaan pilvipalveluun, jossa eri sensoreiden tuottaman datan prosessointi tapahtuu [24]. Vaikka Aruba valmistaa myös verkkolaitteita ja sensorit integroituvat Aruban verkkolaitejärjestelmiin, heidän valvontaratkaisunsa on ainakin osittain yhteensopiva myös muiden valmistajien laitteiden kanssa. Aiemmista esitellyistä ratkaisuista poiketen Aruban sensoreissa on 4G-modeemi ja SIM-kortti [24] datan raportointia varten varayhteydeksi, mikäli sekä langaton että langallinen verkko eivät mahdollista yhteyttä Aruban pilvipalveluun.

Tämä lisää sensoreiden valmistuskustannuksia merkittävästi, mutta toisaalta antaa selkeämmän kuvan tilanteessa, jossa sensorilaite ei ole saavutettavissa valvottavia verkkoja pitkin. Tällöin voidaan varmistua siitä, että esimerkiksi itse sensorilaitteella ei ole ongelmaa useamman verkkoliitännän kanssa, vaan valvottavissa verkoissa on todellakin laajempi ongelma.

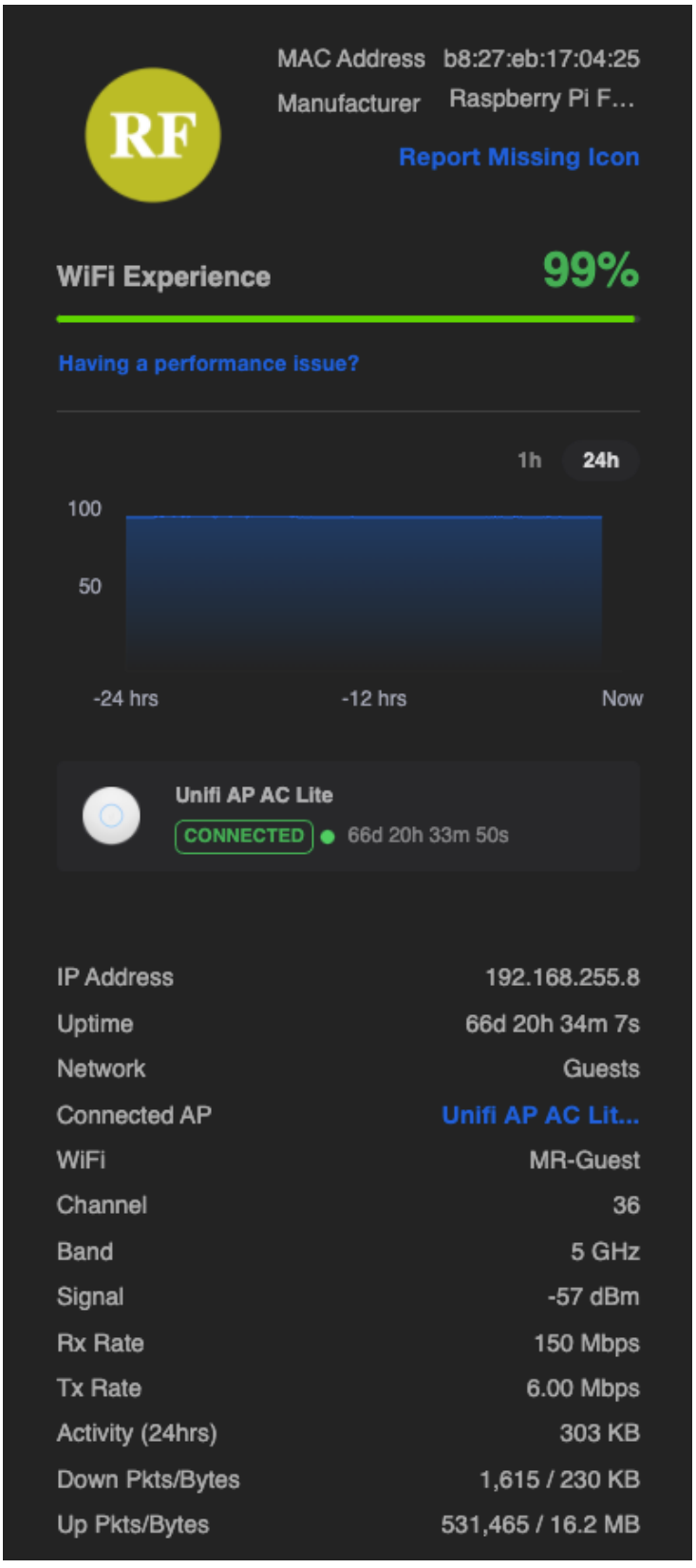
4.3. Fing

Fing on myös yksi osittain samankaltaista toiminnallisuutta mainostava tuote. Fing Desktop on käyttäjän laitteella ajettava ohjelmisto, joka näyttää tietoja nykyisestä verkkoyhteydestä, sekä suorittaa erinäisiä tarkistuksia ja ilmoittaa käyttäjälle mahdollisista verkon ongelmista. Fing Desktop käyttää vianselvitykseen muun muassa ping- ja traceroute-työkaluja, sekä porttiskannauksia. Lisäksi sovelluksella voidaan porttiskannausta hyödyntäen selvittää tietoja muista samassa lähiverkossa olevista laitteista.

Fing Desktop täytyy olla asennettuna loppukäyttäjän omalle koneelle, ja vaatii asennusvaiheessa järjestelmäylläpitäjätason tunnuksia. Tässä työssä tehty vianselvitystyökalu asennetaan verkkoon erillisenä laitteena, joten toiminnallisuus ei vaadi mitään muutoksia yksittäisten käyttäjien laitteisiin. Sovelluksen käyttäminen vaatii myös tunnuksen luomisen Fingin pilvipalveluun, joten käyttäjistä kerätään myös tietoja Fingin sovellukseen liitetyn tietosuojaselosteen mukaisiin käyttötarkoituksiin. Fing Desktop myös rajoittaa ilmaisversiossa verkon testien tekemistä kuuteen kertaan päivässä ilmaiseksi.

4.4. Ubiquiti Unifi Controller

Yksi vaihtoehto verkon analysointiin myös kuluttajakäyttöön ja pienten yritysten lähiverkkoihin suunnatuissa tuotteissa on Ubiquitin verkkotuotteita ohjaavaan Unifi Controlleriin sisäänrakennettu WiFi Experience. Wifi Experiencestä voidaan tarkkailla esimerkiksi WLAN-verkkojen kanavia ja muiden alueella kuuluvien verkkojen taajuuksia. Sen avulla voidaan myös tarkastella yksittäisten WLAN-verkkoon yhdistettyjen laitteiden signaalinvoimakkuustietoja. Wifi Experience luottaa kuitenkin WLAN-tukiasemalle saatavilla oleviin tietoihin, joten esimerkiksi käyttäjän laitteella olevat tai DHCP:lta saatavat virheelliset verkkoasetukset eivät näy sen analyysissä minkäänlaisena ongelmana. Ubiquitin Unifi Controllerin uusimmille versioille ei kuitenkaan tarjota dokumentaatiota, joten Wifi Experiencen käyttö rajoittuu lähinnä yksittäisen sijainnin verkon seuraamiseen suoraan Controllerin kautta, eikä todennäköisesti ole helposti integroitavissa muihin järjestelmiin. Ominaisuuksia voi hyödyntää vain Ubiquitin valmistamien WLAN-tukiasemien kanssa, ja Unifi Controller on sovellus jota täytyy ajaa verkkolaitteista erillisellä laitteella.



Kuva 2. Unifi Controllerin Wifi Experience -paneelin tarjoamia tietoja tässä työssä käytetyn Raspberry Pi 3B+ -laitteen yhteydelle.

5. TYÖSSÄ KÄYTETYT LAITTEET JA OHJELMISTOT

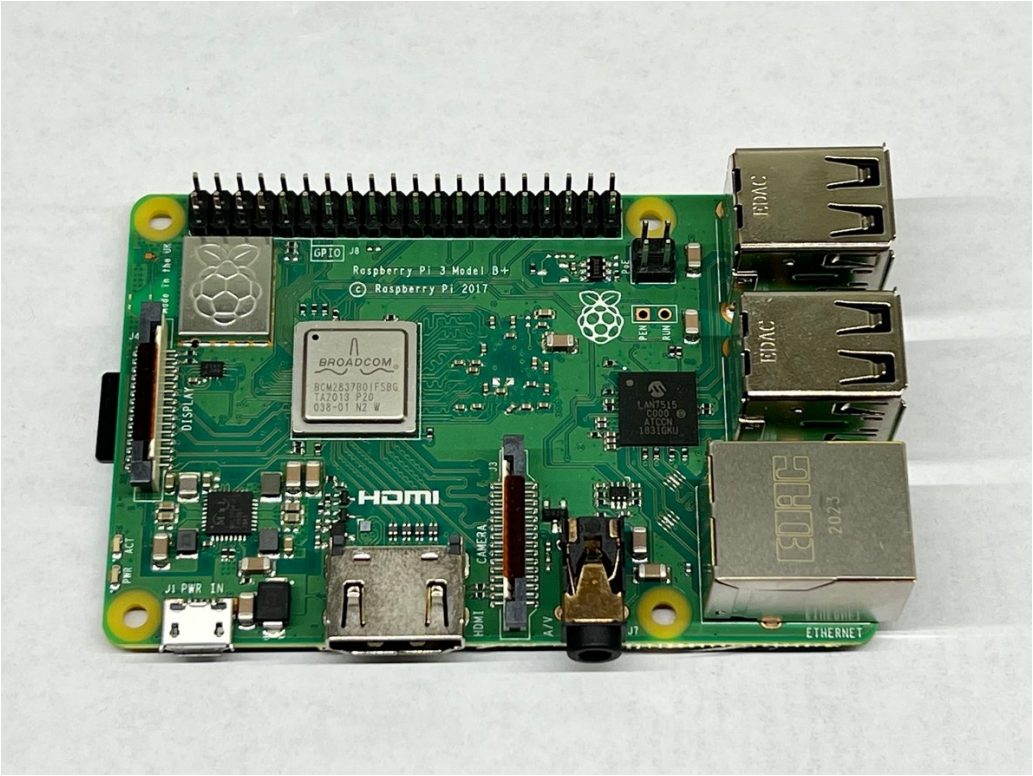
Työssä toteutettiin ohjelmisto, joka sisältää testejä lähiverkon ja WLAN-verkon vianetsintää ja toiminnan tarkastelua varten. Ohjelmisto käyttää ja testaa verkkoa WLAN-verkkoon liittymällä, loppukäyttäjien laitteiden toimintaa mukaillen. Langalliseen verkkoon kytketyllä verkkoliitännällä hallitaan valvontalaitetta ja voidaan tarkastella ohjelmiston suorittamista. Lisäksi toteutettiin ohjelmiston asentamiselle automaatio Ansiblen avulla. Ohjelmisto ja käyttöjärjestelmän tietoturvakovennukset voidaan helposti asentaa uudelle ARM-pohjaiselle Raspberry Pi -alustalle, jos käytössä on Debian-pohjainen käyttöjärjestelmä.

5.1. Raspberry Pi 3 Model B+

Työssä käytettiin ohjelmiston ajamiseen ja eri verkkojen testaamiseen Raspberry Pi 3 Model B+ -tietokonetta. Raspberry Pi 3 Model B+:ssä on tämän työn kannalta oleellisesti kaksi erilaista verkkoliitäntää: Gigabit ethernet sekä WLAN, joka pystyy sekä 2.4GHz:n että 5GHz:n taajuusalueisiin [25]. Muita laitteen ominaisuuksia ovat:

- 1.4 GHz ARMv8 neliytiminen suoritin
- 1GB LPDDR2 keskusmuistia
- Bluetooth 4.2 ja BLE
- HDMI-portti
- 3.5mm audioplugi
- 4 USB-porttia
- CSI-liitin kameralle
- DSI-liitin kosketusnäytölle
- Micro SD -korttipaikka käyttöjärjestelmälevylle
- Micro USB -liitin virransyötölle

Testien aikana laitteessa oli käyttöjärjestelmänä Raspberry Pi -alustoille suunnattu Raspberry Pi OS, joka pohjautuu Debian-käyttöjärjestelmän 11. versioon.



Kuva 3. Työn kehittämisessä ja testaamisessa käytetty Raspberry Pi 3B+ -tietokone.

5.1.1. Valvontalaitteen turvallisuus ja kovennukset

Tässä työssä esitetty WLAN-verkkojen valvontalaite on tarkoitus kytkeä vähintään kahteen verkkoon; verkkoon, jota halutaan valvoa, sekä toiseen verkkoon, jota kautta dataa valvonnasta lähetetään käyttöä varten. Koska nämä kytketyt verkot voivat olla myös esimerkiksi erillisiä VLAN-verkkoja yritysympäristöissä, laitteella on tavallista laitetta laajempi näkymä verkkoihin. Tästä johtuen valvontalaitteeseen voi kohdistua myös uhkia useammasta verkosta, ja siten myös valvontalaitteen turvallisuus täytyy kiinnittää huomiota. Valvontalaitteena käytettävä Raspberry Pi Debian-pohjaisella käyttöjärjestelmällä tarjoaa laajalti konfigurointimahdollisuuksia yleisten Linux-käyttöjärjestelmien tapaan. Valvontalaitteella tehdään ohjelmiston asennuksen mukana yleisten hyvien käytäntöjen mukaisia kovennuksia: Yleensä samanlaisissa laitteissa Raspberry Pi OS:lla varustettuna on oletuksena käyttäjätunnus ”pi” ja salasana ”raspberry”. Tämä tunnus-salasanapari on yksi yleisimpiä, joita SSH-palveluita etsivät hyökkääjät kokeilevat [26], joten pi-tunnus on poistettu käytöstä kokonaan. Laitteelle voi kirjautua ja sitä voi käyttää helposti SSH-yhteydellä etänä. Sen takia SSH-yhteydellä kirjautumisesta on myös poistettu käytöstä root-pääkäyttäjätunnuksella kirjautuminen, ja sallittu vain SSH-avaimia käyttävät kirjautumiset muille tunnuksille. Tällöin pelkän tunnuksen ja salasanan tietäminen ei riitä vielä kirjautumiseen millään tunnuksilla, vaan tarvitaan myös tunnukselle asetettua julkista avainta vastaava yksityinen avain.

5.2. Projektia varten tehdyt ohjelmistot

Tässä työssä tehdyissä ohjelmistoissa käytettiin pääasiassa Bashia. Ohjelmaa suoritetaan Raspberry Pi -minitietokoneella joko manuaalisesti, tai käyttäjän määrittelemin aikavälein. Työssä tehty kokonaisuus koostuu Bash-komentokielellä toteutetusta pääohjelmasta ja apuohjelmista, Jinja2- ja YAML-muotoisista konfiguraatioista, sekä erinäisistä selkokielisistä konfiguraatiotiedostoista esimerkiksi WLAN-verkkoihin liittymistä varten. Ohjelman tarkoituksena on kerätä tietoja verkon toiminnallisuudesta ja mahdollisista ongelmista, jotta verkko-ongelmia olisi mahdollista selvittää etänä helposti. Ohjelmisto suorittaa verkkoon kohdistuvia testejä, jotka tehtiin vastaamaan tilannetta, jossa loppukäyttäjä käyttäisi verkkoa tyypillisessä koti- tai toimistoympäristössä.

Ennen kuin verkon testejä voidaan suorittaa, täytyy luoda testattavaa verkkoa varten erillinen namespace eli nimiavaruus ”ip netns” komentojen avulla. Verkon nimiavaruus on kuin looginen kopio verkkoasetuksista ja laitteista, jolla on erikseen määritellyt reitit, palomuurisäännöt, sekä verkkolaitteet [27]. Erillinen verkon nimiavaruus tarvitaan, jotta testit voidaan kohdistaa vain tietyn verkkolaitteen kautta käytettäviin verkkoihin, tässä tapauksessa haluamme käyttää vain Raspberry Pi:n WLAN-verkkoadapteria valvottaville verkoille. Kaapelin kautta kytketty ethernet-verkko on käytössä laitteen hallintaan ja ohjelmiston keräämien tietojen välitykseen, sillä osa testeistä saattaa katkaista verkon valvontaan käytettävän verkkoliitännän liikenteen hetkeksi. Tätä työtä varten tehdyllä wifi-netns.sh -skriptillä sekä wlan-namespace@.service -konfiguraatiotiedoston avulla voidaan luoda käyttöjärjestelmään systemd-palvelu, joka luo tarvittavan verkon nimiavaruuden automaattisesti.

Ohjelmistolle toiminnalle tarpeellisia riippuvaisuuksia ovat Raspberry Pi OS -käyttöjärjestelmän pakettihallinnan kautta saatavat arping, dnsutils, bind9-dnsutils, libnet1, libpcap0.8, ja whois-paketit.

Kaikista testeistä voidaan halutusta käyttötarkoituksesta riippuen luoda ihmisen luettavissa oleva lokitiedosto, tai palauttaa testien yksittäisiä arvoja jatkokäyttöä ajatellen esimerkiksi Zabbixiin tai muihin valvontasovelluksiin lähettämistä varten.

5.2.1. WLAN-verkkojen valvonnan toteutus

Ohjelmiston WLAN-verkkojen osion tarkoituksena on valvoa WLAN-verkkojen kuuluvuutta ja verkkoon liittymistä, jotta verkkoihin liittyviä ongelmia olisi helpompaa selvittää. Halutun ratkaisun täytyy siten toimia kuten loppukäyttäjien päätelaitteiden, eli testata liittymistä WLAN-verkkoon käytännössä. Toteutettu ohjelmisto liittyy WLAN-verkkoon WLAN-adapterille tehdyssä nimiavaruudessa. Verkkoon yhdistäessä ohjelmisto tekee DHCP-pyynnön, ja listaa verkon kuuluvuustiedot. Tehdyssä ohjelmistossa on myös toiminnallisuus, joka listaa kaikki laitteelle näkyvät 2.4GHz:n ja 5GHz:n taajuudella toimivat langattomat lähiverkot. Mikäli haluttu valvottava verkko löytyy, listataan myös kyseisen verkon kuuluvuuden voimakkuus, jonka yksikkö on dBm eli desibelimilliwatti. Listaukseen tallennetaan myös käytetyn verkon kanavan taajuus. Tehty ohjelma listaa myös fyysisen tukiaseman tunnistamista helpottavan BSSID:n, josta voidaan selvittää mihin yksittäiseen tukiasemaan yhdistettiin laitetasolla.

5.2.2. Lähiverkkojen valvonnan toteutus

Lähiverkoissa ohjelmiston tarkoituksena on valvoa muita paikalliseen verkkoon liittyviä verkon komponentteja WLAN-tekniikan ulkopuolella. Ratkaisun on tarkoitus käyttäytyä ja testata verkkoa loppukäyttäjän näkökulmasta. Lähiverkossa toteutettu ohjelmisto testaa verkon oletusyhdyskäytävän saatavuutta arping-työkalun, sekä tavallisen ICMP-protokollaa käyttävän pingin avulla. DHCP:n toimintaa testataan ohjelmiston suorittamalla ICMP-pingillä, sekä kysymällä nykyisen osoitteen uusintaa DHCP-palvelimelta dhclient-komennolla. Lisäksi ohjelmalla voidaan selvittää nykyisen DHCP-osoitteen antaneen palvelimen osoite, jotta esimerkiksi useamman DHCP-palvelimen ympäristöissä voidaan rajata vianselvitystilannetta palvelinkohtaisesti. On myös mahdollista, että verkossa on sinne kuulumattomia DHCP-palvelimia, joita voidaan havaita ajamalla ohjelmistoa säännöllisesti ja tarkastelemalla testituloksia.

DHCP-palvelimien antamia tietoja ohjelmisto kerää mm. /var/lib/dhcp/dhclient.leases -tiedostosta nyt käytetyllä Raspberry Pi OS -käyttöjärjestelmäversiolla. DNS:n toimivuutta valvotaan työssä tehdyillä skripteillä ja nslookup-työkalun avulla, joilla tehdään kyselyjä DHCP-palvelimelta saatujen DNS-palvelimien osoitteisiin sekä internetin julkisille nimipalvelimille. DNS-palvelimia testataan jokaista erikseen, ja mahdollisia ongelmia etsitään myös vertaamalla DNS-kyselyjen tuloksia keskenään ohjelman suorituskerran sisällä. Esimerkiksi vain osalla verkon käyttäjistä voi esiintyä ongelmia, mikäli yksi useamman DNS-palvelimen joukossa palauttaa virheellistä tai vanhentunutta tietoa.

5.2.3. Internetyhteyden valvonnan toteutus

Internetyhteyden testaamisella halutaan selvittää mahdollisia verkon vikatilanteita, jotka johtuvat valvottavan lähiverkon rajalla olevista tai ulkopuolisista tekijöistä, kuten esimerkiksi väärin konfiguroidusta palomuurista, proxy-asetuksista, tai internet-palveluntarjoajan viasta. Ratkaisun pitää siten pystyä kertomaan, saadaanko tavallisen loppukäyttäjän laitteen kaltaisesti käyttäytymällä yhteys esimerkiksi määritellyille http- ja https-sivustoille paikallisen verkon ulkopuolelle internetiin.

Toteutettu ohjelmisto valvoo cURL- ja ping-työkaluilla tehtävien pyyntöjen avulla internetyhteyden toimivuutta. cURL-työkalun avulla tehdyillä testeillä voidaan valvoa http- ja https-sivustojen lataamista. Jos sivustoja voidaan ladata ongelmitta sen avulla, myös samassa verkossa olevilla käyttäjillä pitäisi onnistua kyseisten sivustojen käyttäminen verkkoon vaikuttavien tekijöiden osalta. Käyttäjien laitteilla voi silti olla ohjelmistoja, kuten esimerkiksi virustentorjuntasovelluksia tai mainostenesto-ohjelmia, jotka rajoittavat erinäisille sivustoille pääsyä, mutta niitä ei ole mahdollista huomioida erillisellä valvontaan käytettävällä verkkolaitteella kuten tässä työssä. Työkalun avulla tehdyillä testeillä voidaan testata, että haluttuun kohteeseen päätyy ICMP-paketteja, ja että vastaus kohteelta tulee myös takaisin. Samalla saadaan myös valvottua mahdollisesti matkalla katoavien pakettien määrää, sekä mitattua verkon latenssia valvovan laitteen ja kohteen välillä. Verkon ulkopuolisen palvelimen ping-testi siten kertoo, montako pakettia esimerkiksi ulkopuoliseen kohteeseen yhdistettäessä ei koskaan päädy perille asti, tai mikäli yhteyden latenssi on huomattavan suuri, ja siten aiheuttaa haittaa loppukäyttäjälle.

5.3. Ansible

Ansible on pääosin Pythonilla toteutettu avoimen lähdekoodin ohjelmisto, jolla voidaan helposti automatisoida ja hallinnoida tehtäviä kuten ohjelmistojen asennuksia, pilvipalveluiden resurssien käyttöönottoa, ja konfiguraatioiden hallintaa. Ansiblen käyttäminen ei vaadi kohdekoneelle erikseen asennettavaa ohjelmistoa, vaan toimii moduulien avulla esimerkiksi SSH-yhteyden ylitse [28]. Ansiblen avulla voidaan ajaa niin kutsuttuja playbookeja, eräänlaisia YAML-muodossa tehtyjä konfiguraatiotiedostoja, joiden mukaan Ansible suorittaa halutulle kohteelle konfiguraatiotiedostossa määritellyt toimenpiteet [29]. Playbookissa voidaan esimerkiksi määritellä, että määritellylle laitteelle halutaan asentaa yksittäinen sovellus, mikäli sovelluksen asentamisesta on tehty Ansiblella rooli. Roolit puolestaan ovat myös pohjimmiltaan YAML-tiedostoja, mutta voivat sisältää myös esimerkiksi ohjelmiston asennuspaketin tai muita asentamiseen tarvittavia tiedostoja, konfiguraatioita, ja muuttujia. Playbookit usein sisältävät useita rooleja, joita tarvitaan esimerkiksi yhden sovelluskokonaisuuden asentamiseen riippuvaisuuksineen. Ansiblelle voidaan määritellä kohteita asennusta varten Inventory-hakemiston kautta, ja myös eri asennuskohteille voidaan määritellä erilaisia muuttujia asennuskohteesta riippuen [29]. Ansiblen playbookeja voidaan myös ajaa useille laitteille yhtä aikaa, mikä nopeuttaa asennusprosessia huomattavasti, jos tarvitaan useita laitteita verkon valvontaan kerrallaan.

5.3.1. Asennuksen automatisointi ja koventaminen Ansiblella

Tässä työssä luodun ohjelmiston asennus automatisoitiin Ansiblella, jotta järjestelmän asennus ja käyttöönotto olisi helpompaa. Ansible-konfiguraatioissa käytettiin pelkästään Ansiblen sisäänrakennettuja funktioita ja moduuleita. Ansiblen avulla kaikki ohjelmiston tarvitsemat skriptit ja konfiguraatiotiedostot kopioidaan automaattisesti halutulle laitteelle SSH-yhteyttä käyttäen, ja asennetaan paikoilleen. Ansiblella voidaan myös tehdä tarvittavat muutokset käyttöjärjestelmän omiin konfiguraatiotiedostoihin.

Ansiblen käyttö asennuksessa tuli myös työn idean antaneen IT-alan yrityksen tarpeesta, jonka toiminnassa Ansible on laajasti käytössä yrityksen asiakasympäristöissä. Ohjelman asentamista varten tehdyssä ”Verkonvalvoja”-nimisessä Ansible-roolissa pääkonfiguraatiotiedosto main.yaml on jaettu kahteen osaan: ensimmäinen osa install.yaml asentaa verkon vianselvityksessä tarvittavia skriptejä ja konfiguraatiotiedostoja, ja toinen osa ssh-configure.yaml tekee muutoksia laitteen SSH-konfiguraatioon ja käyttäjätileihin, jotta laite olisi tietoturvallisempi. Näin asennettu laite ei esimerkiksi asentajan huolimattomuuden vuoksi jää Raspberry Pi -laitteille tyypillisille oletusasetuksille, joita yritetään käyttää hyväksi jatkuvasti ja automaattisesti [30].

Verkonvalvoja-roolin install.yaml tiedostossa määritellään, että Ansiblen avulla luodaan Systemd-palvelu tarvittavaa WLAN-nimiavaruutta varten, sekä asetetaan se käynnistymään laitteen käynnistymisen yhteydessä automaattisesti. Asennusvaiheessa on tarpeen muuttaa verkkoon liittyvät asetukset Ansible-roolin konfiguraatiotiedostoon kohdeympäristön verkkoon sopiviksi. Tällaisia ovat esimerkiksi valvottavan WLAN-verkon nimi ja kirjautumistiedot, sillä myös ne asennetaan paikoilleen automaattisesti konekohtaisilla muuttujilla täydennettynä. Seuraavassa vaiheessa asennettavalle laitteelle kopioidaan verkon vianetsinnässä

tarvittavat skriptit ja konfiguraatiotiedostot, joihin myös asetetaan verkkokohtaisia muuttujia Ansiblen avulla. Lisäksi asennetaan tarvittavat ohjelmistopakettien riippuvaisuudet käyttöjärjestelmän pakettienhallintajärjestelmän kautta.

Roolin ssh-configure.yaml tiedostossa määritellään kovennuksia laitteen etäkäytölle, jotka asennetaan myös paikoilleen Ansiblen avulla. Laitteelle lisätään verkonvalvoja -niminen käyttäjä, jolle voidaan antaa muuttujissa määritelty SSH-avain, sekä salasana sudo-komennon käyttöä varten. Järjestelmän pääkäyttäjän eli root-käyttäjän SSH-kirjautuminen estetään, kuten myös SSH-kirjautuminen kaikilta käyttäjiltä salasanaa käyttäen. Ainoastaan SSH-avaimilla kirjautuminen sallitaan kovennuksien jälkeen. Raspberry Pi OS:n oletuskäyttäjä pi poistetaan käytöstä. Lopuksi SSH-palvelu uudelleenkäynnistetään muutosten käyttöönottamiseksi.

Verkon valvonnassa käytetty laite on myös hyvä pitää ajan tasalla käyttöjärjestelmän päivitysten suhteen. Työn idean antaneen yrityksen käytössä on Ansible-rooli, joka asentaa tarvittavat konfiguraatiot päivitysten automaattiselle asentamiselle päivittäin, mutta vastaava toiminnallisuus on mahdollista tehdä myös itse käyttöjärjestelmän pakettienhallinnan kautta saatavan unattended-ugprades-paketin avulla.

6. JATKOKEHITYSIDEAT

Osana työtä tunnistettiin myös ominaisuuksia, joita työssä toteutettuun järjestelmään olisi mahdollista liittää. Esitetyt jatkokehitysideat rajattiin kuitenkin toteutuksen ulkopuolelle, jotta kandidaatintyön laajuus pysyy sopivissa rajoissa. Varayhteys internetiin olisi erityisen hyödyllinen erityisesti tilanteessa, joissa yhteys internetiin on katkennut, mutta se lisäisi valvontalaitteen kustannuksia merkittävästi. Varayhteyden lisäksi myös Zabbix-integraatio tunnistettiin myös yrityskäytön kontekstissa hyödylliseksi jatkokehityskohteeksi. Työssä käytetty Raspberry Pi 3B -alusta on sopiva demoalusta ohjelmistolle kahden verkkoliitännän ansiosta, mutta suorituskyvyltään tehokkaampi alusta voi olla tarpeen erilaisia kyberturvallisuusominaisuuksia, esimerkiksi IDS- tai IPS-toimintoja, sisältävän toteutuksen kanssa.

6.1. Varayhteys internetiin

Yksi haasteista, joihin tässä työssä ei otettu kantaa, on tiedon saaminen valvottavasta verkosta ulkoverkkoon ongelmatilanteissa. Mikäli valvottavan kohteen internet-yhteydessä on ongelmia, tiedon saaminen internetin välityksellä kohteen ulkopuolelle ei välttämättä ole ongelmatonta. Vaikka valvonta olisikin pääasiassa WLAN-verkon kautta, samat verkon ongelmat voivat mahdollisesti vaikuttaa myös langalliseen verkkoon, jonka kautta valvontalaitetta hallitaan. Tällöin tieto ongelmista ei välttämättä välity valvottavan sijainnin ulkopuolelle, mikäli ongelmista viestimiseen käytetään samaa yhteyttä missä ongelmia esiintyy.

Ratkaisuna tähän ongelmaan on esimerkiksi 4G-varayhteyden käyttäminen. Joissain yritysverkoissa tämänkaltaisia ratkaisuja löytyy jo loppukäyttäjienkin internetin varayhteydeksi, ja samaa yhteyttä voisi hyödyntää myös Raspberry Pi:n toisena verkkoyhteytenä. Vaihtoehtoisesti olisi mahdollista rakentaa varayhteys suoraan valvontalaitteena käytettävään Raspberry Pi:hin mukaan, joko USB-liitäntään liitettävällä modeemilla, tai laitteen GPIO-pinneihin kiinnitettävällä lisäkortilla. Esimerkiksi Wavesharen valmistama SIM7600E-H 4G HAT voisi toimia Raspberry Pi:n mobiiliverkkomodeemina, jolloin yhteys internetiin olisi saatavilla suoraan laitteelta, riippumatta valvottavan kohteen omista verkoista. Tietoja verkko-ongelmista saataisiin tällöin perille, vaikka valvottavan kohteen verkko olisi epäkunnossa. Huono puoli oikeastaan kaikissa mobiiliverkkoa hyödyntävissä ratkaisuissa on hinta; USB-modeemi maksaa noin 60 euroa, ja GPIO-lisäkortti maksaa noin 100 euroa, eli saman verran kuin kaikki muut tarvittavat osat sisältävä Raspberry Pi -paketti. Varayhteyden lisääminen siis kasvattaa yhden valvontasensorin hintaa merkittävästi. Lisäksi tarvitaan myös erillinen mobiili-internetliittymä, josta syntyy jatkuvia kuluja. Yrityskontekstissa kokemusten perusteella varayhteydestä koettiin olevan hyötyä osassa valvottavista verkoista, riippuen siitä kuinka kriittistä verkon toimivuuden valvonta on tietyssä sijainnissa.

6.2. Zabbix-integraatio

Zabbix on avoimen lähdekoodin ohjelmisto, jonka tarkoitus on toimia alustana hajautetulle IT-ympäristön valvonnalle. Ohjelmistoa kehittää ja tukee latvialainen yritys Zabbix SIA, mutta GPLv2 lisensoinnin ansiosta lähdekoodi on vapaasti saatavilla ja sitä voi käyttää myös kaupallisissa käyttötarkoituksissa ilmaiseksi [31].

Zabbix-ohjelmistolla voidaan valvoa määriteltyjä kohteita, esimerkiksi palvelininfrastruktuuria yksinkertaisilla tarkistuksilla. Tarkistukset eivät vaadi asennettua ohjelmistoa kohdekoneelle, mutta tarkempaa valvontaa voidaan suorittaa myös asennettavilla Zabbix Agenteilla. Tässä työssä valvontaa suorittavalle Raspberry Pi:lle olisi mahdollista asentaa Zabbix Agent joka välittää kerätyt tiedot eteenpäin Zabbix-palvelimelle. Palvelimella kerätty data säilötään tietokantaan, ja siten myös aiempien ajanhetkien data esimerkiksi verkon latenssista on saatavilla vertailua varten Zabbix-palvelimen käyttöliittymän kautta. Valvottavista kohteista voidaan edelleen määriteltyjen raja-arvojen ylittyessä lähettää hälytyksiä esimerkiksi yrityksen IT-asiantuntijoille, jotta mahdolliset ongelmat voidaan korjata. Tehty ohjelmisto olisi pienillä muutoksilla mahdollista yhdistää Zabbix-valvontaohjelmistoon käyttämällä testejä yksittäisinä osina ilman pääohjelmaa. Zabbix-integraatiota varten testeille täytyisi luoda UserParameter-konfiguraatiotiedosto, joka mahdollistaa Zabbix-ohjelmiston suorittaa valvovalla laitteella käyttäjän itse luomia testejä, joita ei tule valmiina Zabbix-asennuksen mukana. Zabbix-integraatio tunnistettiin hyödylliseksi jatkokehityskohteeksi Zabbix-ohjelmiston avoimen lähdekoodin tuoman vapaan muokattavuuden, sekä työn yrityskäytössä selvinneiden kokemusten perusteella.

6.3. Hälytykset suoraan ohjelmistosta

Työssä kehitetty järjestelmä rajattiin vikojen etsintään ja tunnistamiseen verkosta, ja hälytyksien tuottaminen näistä löydetyistä ongelmista ei ole työssä toteutettujen ohjelmistojen pääasiallinen tarkoitus. Esimerkiksi edellä mainittu Zabbix on tarkoitettu valvonnasta johdettujen hälytysten tekemiseen. Muiden yleisimpien valvontajärjestelmien lisäksi kuitenkin myös suora viestintäkanavaintegraatio voisi olla käyttökelpoinen toteutus pienimuotoisempiin käyttötarkoituksiin, mikäli käytössä ei ole yrityksen tarpeisiin tuotettua hälytys- tai valvontajärjestelmää. Esimerkiksi Telegram- tai Discord-viestintäsovelluksiin voisi olla hyödyllistä saada tämän työn ohjelmiston keräämiä tietoja nähtäville viestien muodossa, jos verkon ylläpitäjällä ei ole käytössä erillistä valvonta- tai hälytystyökalua. Erilaisiin nykyaikaisiin viestintäsovelluksiin on usein mahdollista tuottaa hälytyksiä esimerkiksi webhook-integrointien tai ohjelmointirajapintojen avulla.

6.4. Useiden eri tukiasemien valvominen

Saman verkon eri tukiasemiin yhdistäminen ja testaaminen voisi tietyissä tapauksissa olla myös hyödyllistä tietoa, esimerkiksi jos verkossa on useampi WLAN-tukiasema

mutta vain yksi niistä on viallinen. Halutun yhdistettävän tukiaseman voi määritellä verkosta yksittäisellä BSSID-tunnisteella. Ongelmaksi tässä kuitenkin muodostuu tukiasemien kuuluvuus; mikäli ympäristössä on tarvetta useille tukiasemille, tarve todennäköisesti syntyy esimerkiksi laajan toimistopinta-alan kattamisesta. Yksittäinen Raspberry Pi -laite ei kuitenkaan välttämättä saa riittävää kuuluvuutta tukiasemiin, jotka sijaitsevat fyysisesti kauempana laitteesta. Tällöin hyöty ominaisuudesta, joka mahdollistaisi useamman tukiaseman valvomisen on vähäinen, koska yhdellä laitteella voi kuuluvuuden rajoitteiden takia valvoa käytännössä vain yhdessä sijainnissa kuuluvien laitteiden verkkoja.

6.5. Kyberturvallisuusominaisuudet

Valvontalaite olisi mahdollista myös toteuttaa niin, että kaikki verkkoliikenne kulkee sen kautta. Tämä vaatii verkkolaitteiston konfigurointia, sekä mahdollisesti enemmän laajennusmahdollisuuksia valvontalaitteistolta ja paremman suorituskyvyn valvontalaitteen kuin Raspberry Pi, erityisesti jos lähiverkossa on paljon liikennettä kuten esimerkiksi yrityskäytössä. Verkkoliikennettä olisi mahdollista valvoa myös kytkimeltä peilatuilla verkkoporteilla, jos verkkolaitteet tukevat liikenteen peilausominaisuuksia. Verkkoliikenteen toimivuuden testaamisen lisäksi myös liikenteen sisältöä ja kohteita olisi tällöin mahdollista tarkastella haitallisen verkkoliikenteen varalta.

Avoimen lähdekoodin sovellukset Snort tai Suricata olisivat mahdollisia IDS- ja IPS-sovelluksia, joita voisi hyödyntää lähiverkon toimintaa valvovalla laitteella. Ne ovat yhteensopivia myös työssä käytetyn Raspberry Pi -alustan ja Raspberry Pi OS -käyttöjärjestelmän kanssa. Esimerkiksi Snort voidaan IDS-toimintatilassa konfiguroida analysoimaan ja hälyttämään erikseen määriteltyjen sääntöjen mukaan epäilyttävästä verkkoliikenteestä. Intrusion Prevention System -tyyppisesti käytettävä järjestelmä mahdollistaisi myös havaitun haitallisen liikenteen estämisen, mikäli liikenne kulkee valvontalaitteen kautta [21].

Verkkoliikenteen turvallisuuden kannalta myös Evil twin -tyyppisten hyökkäyksien havaitseminen voisi olla hyödyllistä. Hyökkäyksessä esitetään luotettavaa langatonta verkkoa käyttäjille, joten hyökkäyksiä olisi mahdollista tunnistaa laitteelle kuuluvia langattomia verkkoja analysoimalla. Esimerkiksi listaamalla luotetut langattoman verkon tukiasemat olisi mahdollista hälyttää ylimääräisistä alueelle kuulumattomista tukiasemista, jotka käyttävät samaa SSID:tä kuin valvottava langaton verkko.

7. YHTEENVETO

Tässä työssä toteutettiin verkon toimivuuden valvontaa varten järjestelmä, joka koostuu Raspberry Pi 3B -alustasta, ohjelmistosta, joka hyödyntää myös unix-järjestelmien verkkotyökaluja, sekä Ansiblella toteutetusta automaattisesta asennustyökalusta. Alustana käytetty Raspberry Pi:n kolmas B-versio on edullinen, pienikokoinen, sisältää kaksi erillistä verkkosovitinta, ja laitteisto on kattavasti tuettu Linux-käyttöjärjestelmissä. Järjestelmän asennuksen automatisointiin Raspberry Pi OS:lle käytettiin Ansiblea, jolle toteutettiin työssä tarvittavat roolit ja konfiguraatiot. Ansible on avoimen lähdekoodin ohjelmisto, eikä se myöskään vaadi asennettavalta kohdelaitteelta mitään erityistä ohjelmistoa. Ansible valikoitui käyttöön yrityskäytössä kerätyn kokemuksen perusteella.

Verkko-ongelmien tunnistaminen etänä on relevantti ongelma, ja ratkaisun tarve vain kasvaa erilaisten verkkoon kytkettävien mobiili- ja IoT-laitteiden sekä etätyön yleistyessä. Tuotetun järjestelmän tarkoitus on testata ja havaita verkko-ongelmia asennussijainnin verkossa muun muassa WLAN-verkon, DHCP:n, DNS:n, ja internetyhteyden toimivuutta valvomalla. Edellä mainituista testeistä koostettua tietoa voidaan käyttää verkon ylläpitäjien tukena helposti myös etänä, vaikka valvottavissa sijanneissa ei aktiivisesti olisi IT-henkilöstöä paikalla.

Osoittautui että verkonvalvontajärjestelmä on mahdollista toteuttaa verkkolaitevalmistajasta riippumattomasti ja automatisoida prosessin asennus yksinkertaiselle ja edulliselle alustalle. Järjestelmä toimii hyvinkin yksinkertaisilla tietokoneilla, kunhan verkkosovittimia on vähintään kaksi kappaletta. Työssä myös kartoitettiin valmiita kaupallisia vaihtoehtoja työssä tehdylle järjestelmälle, joskin ne ovat usein liitännäisiä tiettyyn verkkolaitemerkkiin ja verkkolaitteiden ohjelmistoihin. Työssä tunnistettiin myös mahdollisia jatkokehitysideoita järjestelmälle työn rajauksen ulkopuolelta. Työssä tehty ohjelmisto on osoittautunut kokemusten perusteella hyödylliseksi lähiverkoissa esiintyvien ongelmien tunnistamisessa ja selvittämisessä IT-alan yrityksen käytössä.

8. LÄHTEET

[1] Jaakohuhta, H. (2005). Lähiverkot: Ethernet (4. uud. p.). [Helsinki]: IT Press : 4-5

[2] Cisco - What Is a LAN? Lainattu 18.8.2020, URL: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

[3] Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Langattomasti, mutta turvallisesti: Langattomien lähiverkkojen tietoturvallisuudesta. Lainattu 3.4.2022, URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

[4] Pang J., Hendricks J., Akella A., De Prisco R., Maggs B., & Seshan S. (2004) Availability, usage, and deployment characteristics of the domain name system. URL: https://dl.acm.org/citation.cfm?id=1028790 doi 10.1145/1028788.1028790

[5] RFC1035 – Domain names – Implementation and specification (1987). Lainattu 6.3.2019, URL: https://tools.ietf.org/html/rfc1035 : 46

[6] RFC1034 - Domain names – Concepts and facilities (1987). Lainattu 5.3.2019, URL: https://tools.ietf.org/html/rfc1034 : 21-22, 32

[7] RFC1912 - Common DNS Operational and Configuration Errors (1996). Lainattu 6.3.2019, URL: https://tools.ietf.org/html/rfc1912 : 3-4

[8] RFC8020 - NXDOMAIN: There Really Is Nothing Underneath (2016) Lainattu 6.3.2019, URL: https://tools.ietf.org/html/rfc8020 : 1-5

[9] RFC2131 - Dynamic Host Configuration Protocol (1997) Lainattu 10.3.2019, URL: https://tools.ietf.org/html/rfc2131 : 1-3, 7, 12-13

[10] Rouse M., Burke J., Gerwig K. DHCP (Dynamic Host Configuration Protocol) (2017). Lainattu 10.3.2019, URL: https://searchnetworking.techtarget.com/definition/DHCP

[11] Khadilkar M., Feamster N., Sanders M., Clark R. (2007). Usage-Based DHCP Lease Time Optimization, Lainattu 10.3.2019, saatavilla https://dl.acm.org/citation.cfm?id=1298315 doi 10.1145/1298306.1298315 : 74-75

[12] RFC826 - An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware (1982) Lainattu 11.4.2019, URL: https://tools.ietf.org/html/rfc826

[13] RFC4861 - Neighbor Discovery for IP version 6 (IPv6) (2007). Lainattu 11.4.2019, URL: https://tools.ietf.org/html/rfc4861 : 13-15

[14] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.

[15] A. Zafft and E. Agu, "Malicious WiFi networks: A first look," 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 1038-1043, doi: 10.1109/LCNW.2012.6424041.

[16] G. Z. Gurkas, A. H. Zaim and M. A. Aydin, "Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks," 2006 International Symposium on Computer Networks, 2006, pp. 1-5, doi: 10.1109/ISCN.2006.1662520.

[17] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 517-533, doi: 10.1109/SP40000.2020.00031.

[18] H. Peng, "WIFI network information security analysis research," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 2243-2245, doi: 10.1109/CECNet.2012.6201786.

[19] C. Kolias, G. Kambourakis, A. Stavrou and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 184-208, Firstquarter 2016, doi: 10.1109/COMST.2015.2402161.

[20] S. Saad et al., "Detecting P2P botnets through network behavior analysis and machine learning," 2011 Ninth Annual International Conference on Privacy, Security and Trust, 2011, pp. 174-180, doi: 10.1109/PST.2011.5971980.

[21] F. Hock and P. Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks," 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2015, pp. 1-4, doi: 10.1109/ICETA.2015.7558466.

[22] V. R. Kebande, N. M. Karie, A. Michael, S. M. G. Malapane and H. S. Venter, "How an IoT-enabled “smart refrigerator” can play a clandestine role in perpetuating cyber-crime," 2017 IST-Africa Week Conference (IST-Africa), 2017, pp. 1-10, doi: 10.23919/ISTAFRICA.2017.8102362.

[23] NetBeez Product information (2019). Lainattu 4.3.2019, URL: https://netbeez.net/product/

[24] Data Sheet, Aruba Service Assurance (2018). Lainattu 5.3.2019, URL: https://www.arubanetworks.com/assets/ds/DS_UserCentricServiceAssurance.pdf

[25] Raspberry Pi 3 Model B+ Specifications (2018). Lainattu 27.2.2019, URL: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

[26] SecLists – Top 20 Common SSH Passwords. URL: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt

[27] ip-netns(8) — Linux manual page. Lainattu 26.08.2020, URL: https://man7.org/linux/man-pages/man8/ip-netns.8.html

[28] C. Ebert, G. Gallardo, J. Hernantes and N. Serrano (2016) "DevOps". IEEE Software, vol. 33, no. 3 : 94-100, doi: 10.1109/MS.2016.68.

[29] Red Hat Inc., How Ansible works. Lainattu 12.11.2021, URL: https://www.ansible.com/overview/how-ansible-works

[30] E. D. Martin, J. Kargaard and I. Sutherland (2019) "Raspberry Pi Malware: An Analysis of Cyberattacks Towards IoT Devices," *2019 10th International Conference on Dependable Systems, Services and Technologies* : 161-166, doi: 10.1109/DESSERT.2019.8770027.

[31] Zabbix Documentation – What is Zabbix. Lainattu 13.8.2020, URL: https://www.zabbix.com/documentation/current/manual/introduction/about