jamk

Autentikointi ja VLAN -ratkaisut prosessinohjausjärjestelmän WLAN-verkossa

Jaakko Irva

Opinnäytetyö, AMK
Joulukuu 2021
Tekniikan ala
Insinööri(AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Irva, Jaakko

Autentikointi ja VLAN -ratkaisut prosessinohjausjärjestelmän WLAN-verkossa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Joulukuu 2021, 47 sivua.

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

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Saatiin Valmet Automation Oy:ltä toimeksianto, jonka tavoitteena oli rakentaa Ruckuksen laitteilla langattomien verkkojen ympäristö, jota voidaan käyttää Valmet Automation prosessinohjausjärjestelmissä. Ympäristön vaatimuksena oli vähintään kolme eriytettyä langatonta verkkoa, joiden käyttäjät tai laitteet todennetaan laitteiden asettamien vaatimuksien tai käytön mukaisesti. Sivutuotteena oli luotava ympäristön asennusohjeet, joiden mukaan ympäristö voidaan asentaa eri toimipisteille.

Valmet Automation toimitti Ruckuksen tukiasemat ja Cisco kytkimen, joilla ympäristöä rakennettiin ja testattiin aluksi kotona. Ympäristö rakennettiin yhdistämällä reitittimen perään kytkin, johon tukiasemat yhdistettiin. Päädyttiin toteuttamaan Ruckus Unleashed -ympäristö, jossa yksi tukiasema toimii Master-AP:na eli kontrollerina, jonka kautta voidaan hallita kaikkia ympäristössä olevia tukiasemia, päätelaitteita ja käyttäjiä. Todentamisessa päätettiin käyttää tukiasemien näkökulmasta ulkoista RADIUS-palvelinta, joka toteutettiin sisäverkkoon asennetulla virtuaalikoneella sekä Windows Active Directory -ympäristöllä. Kun vaatimusmäärittelyn mukainen ympäristö oli saatu luotua, siirryttiin Valmet Automation laboratoriotiloihin Tampereelle ja rakennettiin uusi useamman tukiaseman ympäristö asennusohjeiden mukaisesti sekä testattiin toiminta.

Todettiin, että käytössä olevilla laitteilla voidaan rakentaa langattomien verkkojen ympäristö, jossa kaikki prosessinohjausjärjestelmässä olevat laitteet ja käyttäjät saavat tarvittavat toiminnallisuudet. Tukiasemien toimintaa testatessa todettiin, että useamman tukiaseman ympäristössä liikkuessa päätelaitteet vaihtavat tukiasemaa saumattomasti ilman pakettihukkaa ja myös virransyötön tai verkkoyhteyden vikatilanteissa palvelun palautuminen kesti maksimissaan muutaman minuutin. Huomattiin, että käyttöliittymän tarjoama näkymä päätelaitteiden toimintaan antoi hyödyllistä dataa langattomien verkkojen kuormasta ja käyttäjämäärästä. RADIUS-palvelimen käyttö mahdollisti sen, että tulevaisuudessa pystytään käyttämään toimipisteiden olemassa olevia Active Directory ympäristöjä, mikä helpottaa käyttöönottoa ja käyttäjien hallintaa. Testatuilla laitteilla on mahdollista kasvattaa langattomien verkkojen määrää tarpeen mukaan vain pienillä muutoksilla toimipisteen verkkolaitteilla.

Avainsanat (asiasanat)

Todentaminen, VLAN, WLAN, Active Directory, RADIUS

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Irva, Jaakko

Authentication and VLAN solutions in process control system's WLAN network

Jyväskylä: JAMK University of Applied Sciences, December 2021, 47 pages.

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

Permission for web publication: Yes

Language of publication: Finnish

Abstract

An assignment was received from Valmet Automation Oy with the aim of building an environment for wireless networks with Ruckus equipment that can be used in Valmet Automation's process control systems. The environment required at least three differentiated wireless networks whose users or devices were authenticated according to their requirements or usage. The installation instructions for the environment also had to be created so that the environment could be installed on different sites.

Valmet Automation supplied Ruckus access points and a Cisco switch to initially build and test the environment at home. The environment was built by connecting the switch behind the router and the Access Points to the switch. The decision was to implement a Ruckus Unleashed environment, where one Access Point acts as a Master Access Point – as a controller, which manages all Access Points, devices and users in the environment. It was decided to use an external RADIUS server for the authentication, which was implemented on a virtual machine installed on the intranet using the Windows Active Directory environment. Once the required environment had been created, it was moved to Valmet Automation's laboratory facilities in Tampere in a larger scale and the operations were tested.

It was found that the devices in use can be used to build a wireless network environment where all devices and users in the process control system receive the necessary functionalities. When testing the operation, it was noticed that when moving in the environment of multiple Access Points the transfer from one Access Point to another took place without packet loss, and in the event of power supply or network connection failure the service was restored automatically within few minutes. It was noticed that the view provided by the user interface of Master-AP provided useful data on the load and a number of users of the wireless networks. The use of RADIUS server made it possible to use the existing Active Directory environments in the future, thus making it easier to deploy and manage users. With the devices tested, it is possible to increase the number of wireless networks as needed with only minor configuration changes to the site's network equipment.

Keywords/tags (subjects)

Authentication, VLAN, WLAN, Active Directory, RADIUS

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Työn lähtökohdat

1.1 Tehtävän kuvaus

Opinnäytetyön toimeksianto saatiin Tampereen Valmet Automation Oy:ltä ja sen tavoittena oli suunnitella sekä kehittää yhdenmukainen ja helposti hallinnoitava langaton verkkototeutus prosessinohjausjärjestelmiin. Prosessinohjausjärjestelmien langattomat verkkototeutukset oli tehty aiemmin asiakkaan tilauksesta, asiakkaan tarpeiden mukaisesti ja nyt langattomien verkkojen yleistyessä huomattiin, että erilaisten toteutusten hallinta sekä päivittäminen on hankalaa ja erittäin työlästä. Valmet Automation Oy määritti tehtävän langattoman verkon vaatimukset, ratkaisussa oli oltava vähintään kolme langatonta verkkoa/VLAN:ia erilaisille käyttäjäryhmille tai laitteille, osa käyttäjäryhmistä pitää pystyä autentikoimaan ennen verkkoon liittymistä ja ympäristö pitää olla helposti hallinnoitava sekä monitoroitava. Opinnäytetyön sivutuotteena Valmet Automation Oy:lle tehtiin englannin kieliset asennusohjeet, jonka avulla langaton verkkototeutus voidaan ottaa käyttöön missä tahansa. Tutkimuksessa selvitettiin jokaisen käyttäjäryhmän tarpeet, aiempien ratkaisuiden ongelmakohdat ja pyrittiin löytämään yhdenmukainen ratkaisu, joka voidaan toteuttaa prosessinohjausjärjestelmässä. Valmet Automation Oy määritti työn tehtäväksi Ruckus-laitevalmistajan tukiasemilla.

1.2 Tavoite

Opinnäytetyön tavoitteena oli rakentaa toimeksiantajan valitsemilla laitteilla useamman langattoman verkon ympäristö, joka olisi tietoturvallinen ja helposti hallinnoitavissa. Työn keskeinen tutkimuskysymys oli, onko mahdollista toteuttaa määrittelyn mukainen tietoturvallinen langaton ympäristö Ruckuksen laitteilla. Jatkokysymyksillä kartoitettiin luotavan ympäristön käytettävyyttä, joten jatkokysymyksinä oli, onko luotava ympäristö helposti hallinnoitavissa ja voidaanko ympäristö toteuttaa missä tahansa.

1.3 Tutkimusmenetelmä

Työssä käytettiin kvalitatiivista tutkimusmenetelmää ja konstruktiivista tutkimusotetta. Kvalitatiivisella eli laadullisella tutkimusmenetelmällä tutkitaan tosielämän tilanteita ja pyritään selvittämään tutkittavan aiheen laatua, ominaisuuksia ja merkitystä. Kvalitatiiviselle tutkimusmenetelmälle on

ominaista, että tutkimustulokset saattavat mukautua sitä mukaan, kun ymmärrys aiheesta laajenee. Kvalitatiivisen tutkimuksen tarkoituksena on olla laaja sekä tarkka ja sen tiedot pohjautuvat ammattilaisten kokemukseen tai luotettaviin lähteisiin (Auvinen, A. & Tarkiainen, E., 2018.). Konstruktiivisessa tutkimusotteessa pyritään ratkaisemaan tosielämän ongelmia, jotka tarvitsevat ratkaisua ja sen tavoitteena on luoda alalle jotain uutta tuotteen, palvelun, mallin tai informaation muodossa. Konstruktiivinen tutkimusote on sidottu olemassa olevaan teoriaan ja se sisältää kehitetyn suunnitelman toteuttamisen käytännössä, jolla testataan suunnitelman toimintaa ja soveltuvuutta. Konstruktiivisen tutkimusotteen tavoitteena on tarkastella ja ratkaista tosielämän ongelma yhdistämällä teoria sekä käytäntö ja analysoimalla mikä toimii ja mikä ei toimi (Lukka, 2001.).

1.4 Toimeksiantaja

1.4.1 Valmet

Valmet on kansainvälinen yritys, joka on johtava kehittäjä sekä toimittaja sellu-, paperi ja energiateollisuuden teknologian, automaation ja palveluiden parissa. Valmetin teknologioihin kuuluu sellutehtaat, kartongin ja paperin tuotantolinjat sekä voimalaitokset bioenergian tuotannossa. Lisäksi Valmet tarjoaa palveluita tehdas- ja laiteparannuksiin, varaosiin, kunnossapitoon sekä automaatioratkaisuja. Valmetin liikevaihto vuonna 2020 oli noin 3,7 miljardia euroa ja se työllistää noin 14 000 työntekijää ympäri maailman. (Valmet in brief, 2021.)

1.4.2 Valmet Automation

Valmet Automation kehittää ja toimittaa automaatio- ja tiedonhallintajärjestelmiä, sovelluksia ja palveluita sellu-, energia-, paperi-, prosessi-, meri- ja kaasuteollisuuden yrityksille. Kansainvälisesti Valmet Automation työllistää lähes 2000 työntekijää yli 30 maassa. Valmet Automationin päätuotteita ovat hajautetut ohjausjärjestelmät, laadunvalvontajärjestelmät, analysaattorit ja mittauslaitteet. (Automation business line, 2021.)

2 Tietoverkko

2.1 Langaton verkko

Wireless Local Area Network eli WLAN on langaton kommunikointijärjestelmä, joka mahdollistaa tietokoneiden ja päätelaitteiden lähettää liikennettä ja kommunikoida radioaalloilla. IEEE 802.11 on standardi, joka määrittelee ominaisuudet ja protokollat WLAN käyttöön. Langattomia verkkoja voidaan käyttää sekä sisä- että ulkotiloissa ja ne voidaan kytkeä langallisen LAN-verkon yhteyteen. WLAN tarjoaa kaikki samat toiminnallisuudet kuin langallinen LAN-verkko, mutta antaa lisämahdollisuuksia, kun päästään eroon fyysisen kaapelin tuomista rajoituksista. 802.11 WLAN-järjestelmät voivat toimia 2.4 GHz ja 5 GHz taajuudella. (Harte, 2004.)

2.1.1 2.4 GHz

2.4 GHz kaista on yleisimmin käytössä oleva WLAN-verkkojen kaista, jonka taajuuden alaraja on 2400 MHz ja yläraja 2500MHz. Wi-Fi standardeista 802.11b/g/n käyttävät 2.4 GHz kaistaa. 2.4 GHz kaistalla on 14 kanavaa, joista kanavat 1-11 on hyväksytty käytettäväksi ympäri maailman ja lisäksi kanavat 12-13 on hyväksytty käyttöön Euroopassa. Kanavat on jaettu 5 MHz välein, mutta kanavien kaistanleveys on 22 MHz, minkä myötä kanavat ovat osittain päällekkäin. Taulukossa 1 on esitetty 2.4 GHz kaistan kanavat, kanavien keskitaajuus, jotka on jaettu 5 MHz välein sekä kanavien ala- ja ylätaajuudet. Taulukosta voidaan huomata, että esimerkiksi kanavan 5 alataajuus 2421 MHz on päällekkäin kanavan 1 ylätaajuuden 2423 MHz kanssa. Kanavien päällekkäisyyksien takia langattoman verkon ympäristön suunnittelu kannattaa tehdä niin, että ympäristössä on käytössä ainoastaan kanavat, jotka eivät ole päällekkäin. Taulukosta nähdään, että kanavia 1, 6, 11 tai 2, 7, 12 tai 3, 8, 13 tai 4, 9, 14 tai 5, 10, 14 voidaan käyttää yhdessä ilman päällekkäisyyksiä. (Wi-Fi Channels, Frequencies, Bands & Bandwidths, 2021.)

Taulukko 1 2.4 GHz kanavat ja taajuudet

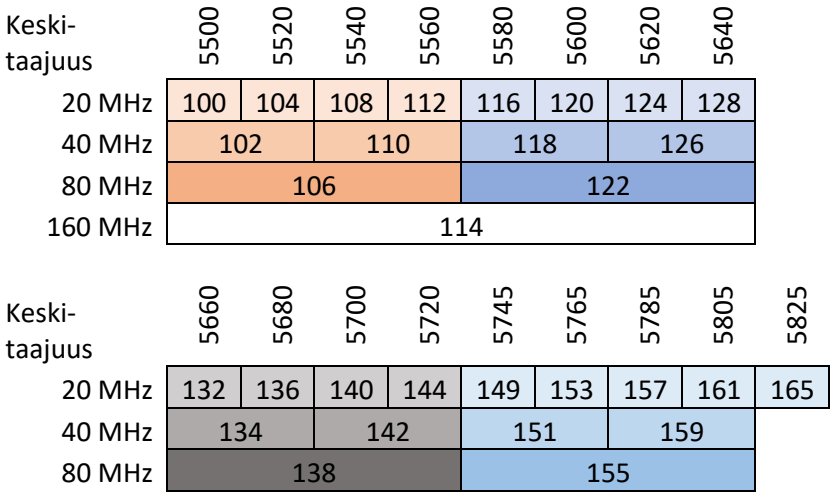
Kanava	Taajuus ala MHz	Taajuus keski MHz	Taajuus ylä MHz
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

2.1.2 5 GHz

5 GHz kaista on käytössä Wi-Fi standardeista 802.11a/n/ac -tyypeissä ja se tarjoaa käyttöön laajemman asteikon, jonka avulla jokaisella kanavalla on oma 20 MHz osuus, joka ei ole päällekkäin minkään muun kanavan kanssa. 802.11ac Wi-Fi standardi mahdollistaa kanavien yhdistämisen ja leveämmän kaistankäytön. Taulukossa 2 esitetty 5 GHz kaistan kanavajako. Taulukossa nähdään jokaisen 20 MHz kaistanleveydellä olevan kanavan keskitaajuus ja esitetään miten pienemmällä kaistanleveydellä olevat vierekkäiset kanavat voidaan yhdistää omaksi leveämmäksi kanavaksi. Esimerkiksi 20 MHz kanavat 60 ja 64 muodostavat yhdessä 40 MHz leveyden kanavan 62.

Taulukko 2 5 GHz kanavat ja keskitaajuudet

Keski-taajuus	5180	5200	5220	5240	5260	5280	5300	5320
20 MHz	36	40	44	48	52	56	60	64
40 MHz	38		46		54		62	
80 MHz	42				58			
160 MHz	50							



Isompi kanavan leveys mahdollistaa sen, että isompi määrä dataa voidaan ajaa langattoman verkon läpi, mutta joka kerta kun kanavanleveys kaksinkertaistetaan, aiheuttaa se ylimääräistä kohinaa kanavaan. (O'Brien, 2020.)

2.2 DHCP

DHCP tarjoaa kuljetusmekanismin, jolla annetaan DHCP-palvelimella olevat konfiguraatiotiedot TCP/IP-verkossa oleville päätelaitteille, minkä jälkeen päätelaite pystyy kommunikoimaan kaikkien päätelaitteiden sekä palvelimien kanssa internetissä. DHCP perustuu Bootstrap-protokollaan ja DHCP-viestit ovat samassa muodossa kuin BOOTP-viestit. Verrattuna BOOTP-protokollaan DHCP tuo lisäksi ominaisuuden, joka tukee IP-osoitteiden vuokraamista eli tietoja pyytävät päätelaitteet saavat osoitteen DHCP-palvelimelta, mutta palauttavat sen käytön jälkeen. DHCP koostuu kahdesta osasta, protokollasta, jolla välitetään palvelimelle määritettyjä parametreja ja ominaisuudesta jakaa IP-osoitteita. DHCP perustuu asiakas/palvelin -malliin, jossa päätelaite pyytää tietoja palvelimelta. (Naugle, 1999.)

2.2.1 IP-osoitteiden jakaminen

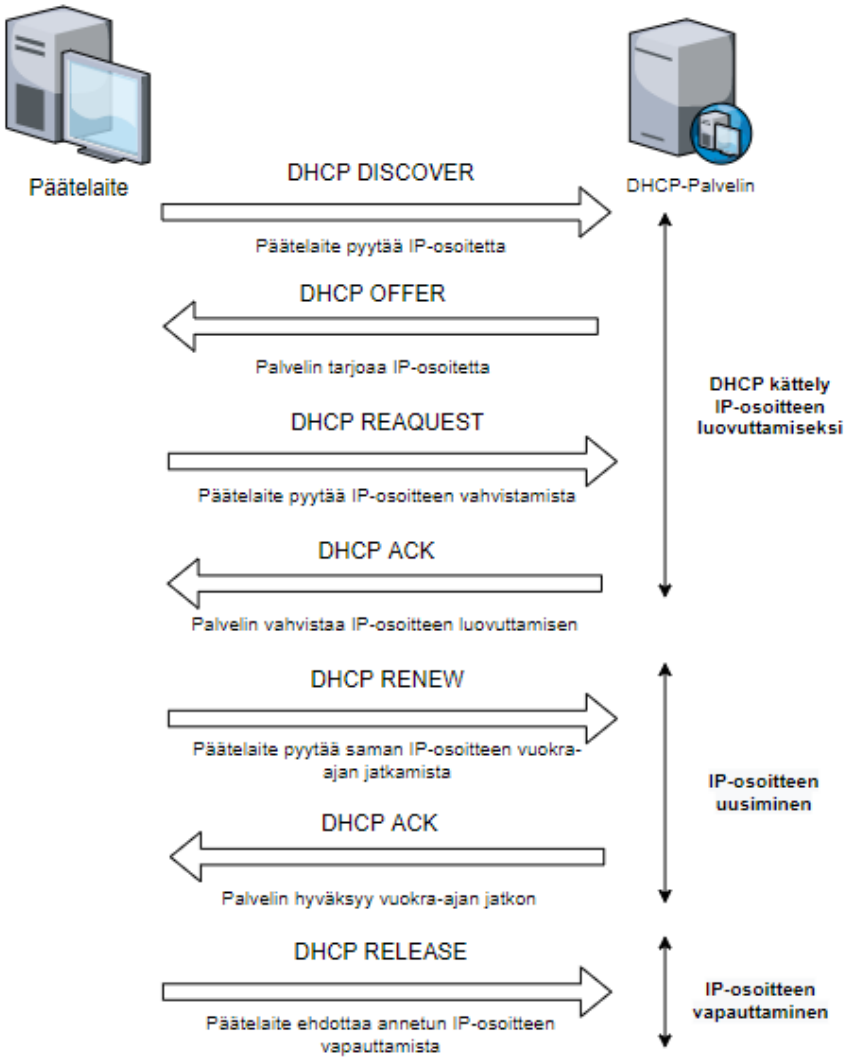
DHCP jakaa IP-osoitteita kolmella eri tavalla, jotka ovat automaattinen jakaminen, dynaaminen jakaminen sekä manuaalinen jakaminen. Automaattisessa jakamisessa DHCP-palvelin antaa IP-osoitetta pyytävälle päätelaitteelle pysyvästi IP-osoitteen. Dynaamisessa jakamisessa DHCP-palvelin vuokraa IP-osoitetta pyytävälle päätelaitteelle IP-osoitteen tietyksi ajaksi. Manuaalisessa

jakamisessa DHCP-palvelin on konfiguroitu antamaan sama IP-osoite tietylle päätelaitteelle, kun päätelaite pyytää IP-osoitetta. (Naugle, 1999.)

2.2.2 DHCP-viestit ja toiminta

DHCP käyttää seuraavia viestejä päätelaitteen ja palvelimen välillä keskustellessa. DHCPDISCOVER on päätelaitteen lähettämä broadcast-viesti, jota käytetään paikallistamaan käytettävissä olevia palvelimia. DHCPOFFER on palvelimelta päätelaitteelle DHCPDISCOVER-viestiin lähetettävä vastaus, jolla tarjotaan palvelimelle määritettyjä konfiguraatioparametrejä. DHCPREQUEST on päätelaitteelta palvelimelle lähetettävä viesti, jolla joko hyväksytään annetut parametrit ja hylätään parametrit muilta palvelimilta, vahvistetaan aiemmin saatujen parametrien oikeellisuus esimerkiksi päätelaitteen uudelleenkäynnistämisen yhteydessä tai jatketaan jo käytössä olevan IP-osoitteen vuokra-aikaa. DHCPACK on palvelimelta päätelaitteelle lähetettävä viesti, joka sisältää konfiguraatioparametrit, kuten päätelaitteelle annettu IP-osoite. DHCPNAK on palvelimelta päätelaitteelle lähetettävä viesti, joka hylkää päätelaitteen ehdottaman IP-osoitteen esimerkiksi väärän aliverkon takia tai päätelaitteen vuokra-aika on jo päättynyt. DHCPDECLINE on päätelaitteelta palvelimelle lähetettävä viesti, joka kertoo, että IP-osoite on jo käytössä. DHCPRELEASE on päätelaitteelta palvelimelle lähetettävä viesti, jolla päätelaite luopuu IP-osoitteesta ja peruuttaa jäljellä olevan vuokra-ajan. DHCPINFORM on viesti, jolla päätelaite kysyy palvelimelta vain paikallisia konfiguraatioparametrejä tilanteessa, jossa päätelaitteella on jo IP-osoite. (Naugle, 1999.)

Kuviossa 1 nähdään päätelaitteen ja DHCP-palvelimen välinen kommunikointi, kun päätelaite yhdistyy verkkoon ja pyytää IP-osoitetta, pyytää annetun IP-osoitteen vuokra-ajan uusimista sekä luopuu annetusta IP-osoitteesta.



Kuvio 1 DHCP kättely

2.3 VLAN

VLAN eli virtual local area network on aliverkko, jolla voidaan ryhmitellä loogisesti verkon käyttäjiä ja resursseja, jotka ovat kytkettynä layer 2-tason kytkimeen määriteltyihin portteihin. VLAN:a käytetään estämään broadcast-liikenteen leviäminen koko verkkoon ja aina kun uusi VLAN luodaan, luodaan samalla uusi broadcast-toimialue. Kaikki laitteet samassa VLAN:ssa kuuluvat samaan broadcast-toimialueeseen ja vastaanottavat kaiken broadcast-liikenteen, mutta kytkimen kaikissa muissa porteissa, jotka eivät kuulu samaan VLAN:iin, broadcast-liikenne suodatetaan. Oletuksena solmut ja päätelaitteet samassa VLAN:ssa pystyvät sijainnista riippumatta kommunikoimaan keskenään, mutta eivät pysty kommunikoimaan toisessa VLAN:ssa olevien laitteiden kanssa. Jotta

päätelaitteet pystyisivät kommunikoimaan toisessa VLAN:ssa olevien laitteiden kanssa, on liikenteen mentävä layer 3-tason reitittävän laitteen, reitittimen tai kytkimen kautta. (Lammle, 2003.)

Kytkimet käyttävät kehyksen merkkaamista tunnistamaan mihin VLAN:iin paketit kuuluvat, että liikennettä voidaan ohjata eteenpäin oikeisiin portteihin. Verkkolaitteiden väliset linkit voivat olla joko access-linkkejä tai trunk-linkkejä. Access-linkit kuuluvat vain yhteen VLAN:iin ja niiden takana olevat laitteet eivät ole tietoisia mihin VLAN:iin kuuluvat, koska kytkimet poistavat kaiken VLAN-informaation kehyksestä ennen laitteelle lähettämistä. Trunk-linkkejä käytetään kuljettamaan VLAN:a verkkolaitteiden välillä ja ne voivat kuljettaa useita VLAN:a. Trunk-linkkien välillä VLAN:ien tunnistamisessa käytetään yleisesti IEEE 802.1Q standardia, jossa kehykseen lisätään kenttä, jolla VLAN tunnistetaan. Kenttä lisätään jokaiseen kehykseen sen saapuessa ensimmäiselle kytkimelle, jolloin jokainen kytkin tunnistaa mihin VLAN:iin kehys kuuluu ja lähettää paketin edelleen määrättyihin portteihin suodatus taulukon mukaisesti. Kehyksen saapuessa kytkimelle, jolla on toinen trunk-linkki, lähetetään kehys toiseen trunk-linkkiin ja kehyksen saapuessa acces-linkkiin, poistetaan VLAN-tunniste ja lähetetään alkuperäinen kehys päätelaitteelle. (Lammle, 2003.)

2.4 Power over Ethernet

Power over Ethernet eli PoE on IEEE 802.3 standardiin tehty lisäys, jonka avulla voidaan lähettää tasavirtajännitettä ja dataa samaa Ethernet-kaapelia pitkin, jolloin ei tarvita erillistä virtalähdettä laitteen läheisyydessä. Ethernet-kaapelissa on kahdeksan kuparijohtoa tai neljä kuparijohtoparia ja riippuen käytössä olevasta tekniikasta joko kahta tai neljää paria käytetään kuljettamaan dataa. PoE lisäys mahdollistaa sähkövirran syöttämisen kahdella tavalla, käyttämällä samoja pareja, joilla kuljetetaan dataa tai käyttämällä pareja, jotka eivät kuljeta dataa. Standardi määrittää mitkä johtoparit voivat kuljettaa tasavirtajännitettä sen mukaisesti onko verkko 10BASE-T, 100BASE-T eli Fast Ethernet toteutus vai 1000BASE-T eli Gigabit Ethernet toteutus. Fast Ethernet toteutuksissa vain kahta johtoparia käytetään kuljettamaan dataa ja Gigabit Ethernet toteutuksissa kaikkia neljää johtoparia voidaan käyttää datan kuljettamiseen. Sähköä tuottavat laitteet jaetaan päätelaitteisiin eli kytkimiin ja kontrollereihin, jotka tuottavat sähköä suoraan Ethernet-portista tai välissä oleviin laitteisiin eli PoE-injektoreihin, jotka lisäävät sähkönsyötön Ethernet-kaapeliin. (Bartz, 2012.)

3 Tietoturva ja autentikointi

3.1 Wi-Fi Protected Access

Wi-Fi Alliance kehitti Wi-Fi Protected Access:n eli WPA:n langattomassa verkossa ja WEP-salauksessa olevien haavoittuvuuksien takia. WPA käyttää temporal key integrity protokollaa (TKIP) avainten hallintaan ja sitä on mahdollisuus käyttää joko Enterprise-tilassa tai Personal-tilassa. Vuonna 2004 julkaistu WPA2 toi mukanaan vahvennetun salauksen ottamalla käyttöön AES-standardin. Enterprise-tila hyödyntää 802.1x autentikointikehystä sekä Extensible Authentication Protocol (EAP) -protokollaa ja Personal-tilassa käytetään pre-shared key (PSK) todennusta sekä joko TKIP tai AES salausta. Yleisesti Personal-tilaa käytetään kotiverkoissa sekä pienissä toimistoissa, joissa ei ole autentikointipalvelinta käytössä ja Enterprise-tilaa isommissa ympäristöissä. (Rackley, 2007.)

3.1.1 Temporal Key Integrity Protocol

WPA toi uutena ominaisuutena Temporal Key Integrity Protokollan (TKIP), jota käytetään avaimien luomiseen ja hallintaan. Kun päätelaite on todennettu, luodaan sessiolle 128-bittinen avain autentikointipalvelimella tai derivoidaan käsin annetusta salasanasta. TKIP-protokollan avulla jokainen päätelaite käyttää erillistä avainta salaamaan liikenteen ja protokolla hallinnoi kaikkien verkossa olevien päätelaitteiden salausavaimia sekä päivittää avaimet vähintään 10 000 paketin välein. TKIP muodostaa avaimen liikenteen salaamiseen yhdistämällä salasanaan päätelaitteen MAC-osoitteen ja TKIP-järjestysnumeron sekä 48-bittisen alustusvektorin, minkä myötä vaihtoehtoja on 280 biljoonaa. (Rackley, 2007.)

3.1.2 Message Integrity Check Function

Message Integrity Check Function eli MIC on myös WPA:n tuoma uusi ominaisuus, joka tarkistaa onko datapaketteja kaapattu, muokattu ja lähetetty uudestaan laskemalla matemaattisella funktiolla jokaisen paketin lähettäjän ja vastaanottajan välillä. MIC on hash-funktio, joka lasketaan käyttämällä lähettäjän ja vastaanottajan MAC-osoitteita, lähetettyä dataa, MIC avainta ja TKIP-järjestysnumeroa. Mikäli laskettu MIC-arvo vastaanottajan päässä ei vastaa lähettäjän puretun paketin MIC-arvoa, paketti hylätään ja MIC asettaa uudet avaimet sekä määrittää avaimien päivittämisen tiheyden nopeammaksi automaattisesti. (Rackley, 2007.)

3.1.3 Advanced Encryption Standard

Vuonna 1997 National Insitute of Standards and Technology (NIST) aloitti Advanced Encryption Standardin eli AES:n kehittämisen ja kahden vuoden tutkimisen jälkeen Rinjndael:n algoritmi valittiin uudeksi AES:ksi lokakuussa 2000. Rijndael:n algoritmi on määritetty käyttämään 128-, 192- sekä 256-bitin lohkoja, mutta AES-standardi on rajoitettu käyttämään ainoastaan 128 bitin lohkoja, niin että avaimen koko voi olla kuitenkin 128, 192 tai 256 bittiä. Jokaisella algoritmin kierroksella tehdään neljä tasoa, jotka ovat bitin vaihto (ByteSub - BSB), rivin vaihto (ShiftRow - SR), sarakkeen sekoitus (MixColumn - MS) ja kierrosavaimen lisääminen (AddRoundKey - ARK). Yhden lohkon salaaminen alkaa kierrosavaimen lisäämisellä, jossa käytetään 0-avainta. Tämän jälkeen tehdään yhdeksän kierrosta kaikkia tasoja ja tehdään yksi kierros ilman sarakkeen sekoitusta. Salauksen purku voidaan suorittaa tekemällä kaikki kierrokset ja tasot käänteisessä järjestyksessä. (McAndrew, 2012.)

3.2 Autentikointiprotokollat

3.2.1 Password Authentication Protocol

Password authentication protocol eli PAP, joka on määritelty RFC 1334:ssä, on salasanaan perustuva autentikointitapa, joka käyttää Point to Point -protokollaa käyttäjien vahvistamiseen. PAP perustuu kaksisuuntaiseen kättelyyn, jossa päätelaite ottaa yhteyttä palvelimeen lähettämällä käyttäjätunnus/salasana parin ja palvelin tarkistaa aiemmin määritetyistä tiedoista täsmääkö salasana kyseiselle käyttäjätunnukselle. Jos käyttäjätunnus/salasana pari varmistetaan, palvelin lähettää takaisin hyväksynnän ja yhteys muodostetaan, muussa tilanteessa palvelin katkaisee yhteyden tai lähettää virheviestin ja antaa uuden mahdollisuuden autentikointiin. Isoin haaste PAP autentikoinnissa on se, että salasanat lähetetään selkotekstinä, jolloin kolmas osapuoli voi mahdollisesti saada käyttäjätunnus/salasana parin tietoon yhteydenmuodostamista monitoroimalla ja käyttää myöhemmin paria saadakseen yhteyden palvelimelle. (Held, 2004.)

3.2.2 Challenge-Handshake Authentication Protocol

CHAP eli Challenge-Handshake Authentication Protocol on PAP:a turvallisempi autentikointitapa, jossa tapahtuu kolmisuuntainen kättelyprosessi. Ensimmäisessä vaiheessa päätelaite muodostaa

yhteyden palvelimelle ja palvelin vastaa päätelaitteelle lähettämällä haaste-viestin. Toisessa vaiheessa päätelaite lisää haaste-viestiin laskemansa yksisuuntaisen hash-funktion ja lähettää takaisin palvelimelle. Kolmannessa vaiheessa palvelin käyttää samaa yksisuuntaista hash-funktiota ja luo laskennallisen paikallisen arvon, johon vastaanotettua viestiä verrataan. Jos arvot täsmäävät, autentikointiprosessi hyväksytään ja mikäli ei täsmää, yhteys katkaistaan tai prosessi aloitetaan alusta. Haaste-viesti sisältää yleensä istunto-ID:n ja mielivaltaisen haaste-merkkijonon, joista hash-algoritmi palauttaa käyttäjätunnuksen selkokielisenä, mutta istunto-ID:n ja salasanan salattuna, mikä tekee protokollasta turvallisemman verrattuna PAP-protokollaan. Microsoft on kehittänyt protokollasta oman versionsa Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), jossa myös käyttäjän salasana on tallennettu palvelimelle hash-muodossa, mikä lisää turvallisuutta. Uudemmassa MS-CHAPv2 -versiossa autentikointi on kaksisuuntainen, joka tukee palvelinautentikointia, jossa palvelin pystyy vahvistamaan autentikointidatan omassa tietokannassaan tai keskitetyssä autentikointitietokannassa, mikä mahdollistaa Remote Authentication Dial-In User Service eli RADIUS-palvelimen käytön. (Held, 2004.)

3.2.3 Extensible Authentication Protocol

Extensible Authentication Protocol eli EAP on autentikointiin käytettävä viitekehys, joka on suunniteltu käytettäväksi OSI-mallin Layer 2 -tason protokollien, kuten PPP ja Ethernet, yli. EAP on autentikoinnin suhteen joustava, koska se ei itsessään suorita autentikointia, vaan tarjoaa infrastruktuurin ja tukee pääteasemia keskustelemaan ja autentikoimaan itsensä. EAP autentikointi tapahtuu joko kahden tai kolmen osapuolen todennuksena. Kahden osapuolen todennuksessa todentaja eli reunalaitteena toimiva langattoman verkon tukiasema tai NAS-palvelin todentaa verkkoon liittymistä yrittävän päätelaitteen itse ja kolmen osapuolen todennuksessa todentaja kysyy kolmatta osapuolta, autentikointipalvelinta, tekemään todennuksen. (Prasad & Sö, 2011.)

3.2.4 IEEE 802.1x ja RADIUS

802.1x on Institute of Electrical and Eletronics Engineers (IEEE) julkaisema standardi, joka määrittää porttiin perustuvan autentikoinnin LAN-verkossa. 802.1x on asiakas-palvelin mallin hallinta- ja autentikointiprotokolla, jolla estetään julkisesti saatavilla olevien porttien luvaton käyttö eri päätelaitteilla. 802.1x käyttää EAP-protokollan Extensible Authentication Protocol over LAN (EAPOL) -versiota autentikoinnin saavuttamiseksi.

802.1x standardiin osallistuvat laitteet on jaettu kolmeen ryhmään. Asiakkaat eli päätelaitteet, jotka yhdistyvät kytkimeen joko suoraan porttiin kytketyllä Ethernet-kaapelilla tai langattomasti tukiaseman kautta. Asiakas eli päätelaite pyytää pääsyä LAN-verkkoon ja vastaa kytkimen pyyntöihin. LAN-verkon kytkin toimii autentikoijana, jonka tehtävä on välittää viestejä asiakkaan ja autentikointipalvelimen välillä. Autentikoija hallinnoi päätelaitteen pääsyä verkkoon sen mukaan onko asiakas todennettu vai ei. Autentikoija pyytää asiakkaalta identiteettitietoja, varmistaa tiedon autentikointipalvelimelta ja välittää vastauksen asiakkaalle. Kun asiakas yhdistyy kytkimen porttiin tai langattomaan verkkoon, ainoastaan EAPOL-liikenne on sallittu, niin kauan kun asiakasta ei ole todennettu. Vasta asiakkaan todentamisen jälkeen portista sallitaan kaikki muu liikenne. (Understanding and Configuring 802.1X Port-Based Authentication, Nd.)

4 Tietoverkon suunnittelu ja valmistelu

4.1 Käytettävät laitteet

4.1.1 Ruckus R310

Testi- ja laboratorioympäristössä käytettiin Ruckus R310 -tukiasemia (Kuvio 2). Ruckus R310 on tarkoitettu pieni- ja keskikokoisille yrityksille helposti käyttöön otettavaksi ja hallinnoitavaksi tukiasemaksi. Tukiasema tukee IEEE 802.11a/b/g/n/ac Wi-Fi-standardeja ja mahdollistaa käytettäväksi useita eri WPA-salaustekniikoita. Tukiasema tukee 2.4 GHz kanavia 1-13 ja 5 GHz kanavia 36-64, 100-144 sekä 149-165. R310-tukiasema on tarkoitettu käytettäväksi sisätiloissa ja se toimii lämpötilassa välillä 0 ºC – +40 ºC. Tukiasema tarjoaa laajan kapasiteetin tarjoamalla mahdollisuuden käyttää 16 eri SSID:tä, 100 yhtäaikaista päätelaitetta ja maksimiminopeus 2.4 GHz -verkossa on 300 Mbit/s sekä 867 Mbit/s 5 GHz -verkossa. Tukiasemaa voidaan käyttää sekä verkkovirrassa että Power over Ethernet – ominaisuutta hyödyntäen. (Ruckus R310, Nd.)

Kuvio 2 Ruckus R310

4.1.2 Ruckus T310

Tuotantoon menevässä tuotteessa tullaan käyttämään Ruckus T310 -tukiasemaa (Kuvio 3), joka on tarkoitettu myös ulkokäyttöön. Tukiasemalla on vastaavat ominaisuudet R310-malliin, mutta lisänä sitä voidaan käyttää isomman skaalan lämpötiloissa välillä -40 ºC – +65 ºC, tukiasema tukee 512 yhtäaikaista päätelaitetta sekä 31 SSID:tä. T310-mallissa on lisänä oletuksena myös Ruckuksen oma SmarthMesh-ominaisuus, jolla voidaan käyttää langatonta Mesh-teknologiaa. (Ruckus T310, Nd.)

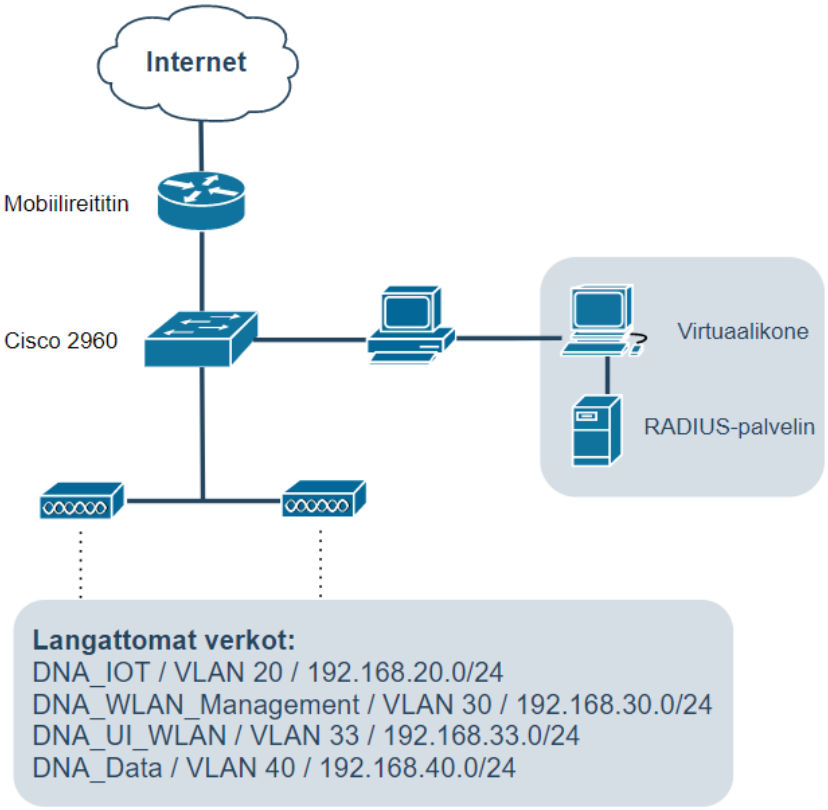
Kuvio 3 Ruckus T310

4.2 Topologia

4.2.1 Testiympäristö

Testiympäristö rakennettiin kotona olevalla laitteistolla sekä Valmet Automation:lta saaduilla Cisco 2960 -kytkimellä ja kahdella Ruckus R310 -tukiasemalla. Käytössä oli Huawei B525s-23a -mobiilireititin, jonka perään Cisco 2960 -kytkin kytkettiin. Kytkimen Vlan1-rajapintaan asetettiin IP-osoite yhteyksien testaamista varten ja rajapintaan määritettiin IP helper-osoite, että päätelaitteet eli tietokone sekä tukiasemat saavat osoitteen automaattisesti mobiilireitittimen DHCP-palvelimelta. Tietokone kytkettiin kytkimen GigabitEthernet0/10 porttiin ja tietokoneelle käynnistettiin virtuaalikone, jolle määritettiin staattinen IP-osoite 192.168.8.105 sekä asennettiin RADIUS-palvelin autentikointia varten. Tukiasemat kytkettiin kytkimen GigabitEthernet0/1 ja 0/2 portteihin ja tukiasemat saivat IP-osoitteen mobiilireitittimen DHCP-palvelimelta, kun ne kytkettiin virtoihin.

Tukiasemille määritettiin staattiset IP-osoitteet 192.168.8.110 ja 192.168.8.111 Unleashed-ohjelmiston asennuksen yhteydessä. Molemmat tukiasemat jakoivat kaikkia neljää langatonta verkkoa (Kts. Kuvio 4).

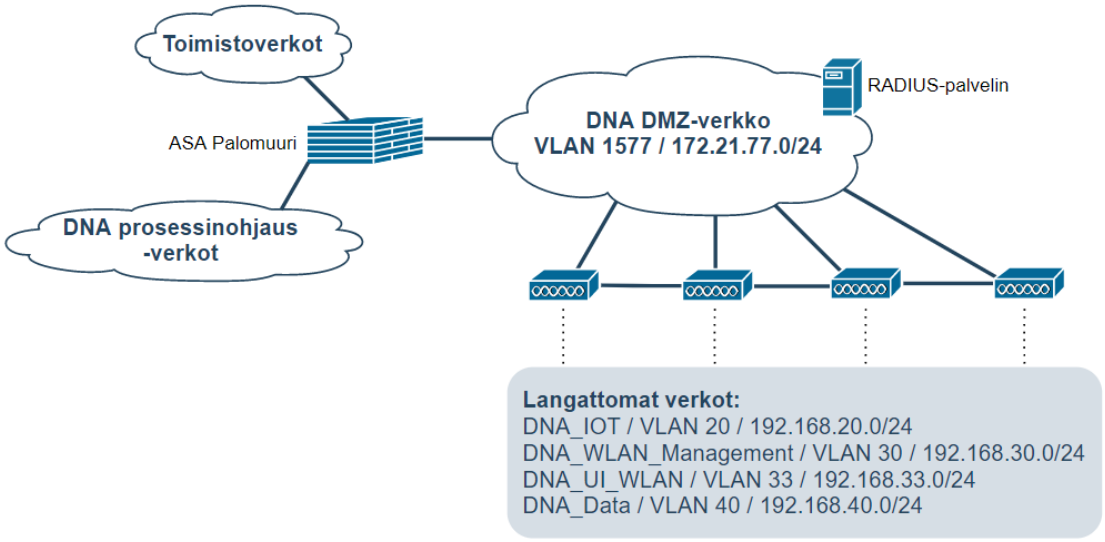


Kuvio 4 Testiympäristön topologia

4.2.2 Valmetin laboratorioympäristö

Valmet Automation Oy:n tiloissa Tampereella oli valmiiksi rakennettu laboratorioympäristö, jossa Cisco ASA palomuuriin oli kytkettynä toimistoverkot, jossa kaikki toimiston työntekijät ovat kiinni, Valmet DNA prosessinohjausverkot, jossa on prosessinohjausjärjestelmään liittyvät laitteet ja monitorointi sekä DNA DMZ-verkko, jossa tehdään laitteiden ja järjestelmien laboratoriotestausta. DNA DMZ-verkon verkkolaitteelle luotiin DHCP-palvelin ja osoitealueet tukiasemia sekä langattomia verkkoja varten. DNA DMZ-verkossa oli valmiina virtuaalikone, jolla ajettiin Windows Server -palvelinta testaamista varten. Virtuaalikoneen Windows Server -palvelimelle asennettiin RADIUS-palvelin, jolle määritettiin staattinen IP-osoite. Neljä tukiasemaa asennettiin ympäri laboratorioti-

laa ja kytkettiin DMZ-verkon verkkolaitteelle ja verkkovirtaan käyttämällä PoE-injektoreita. Tukiasemat saivat IP-osoitteen automaattisesti DHCP-palvelimelta, mutta niille määritettiin staattinen IP-osoite Unleashed-ympäristön asentamisen ja tukiasemien ympäristöön mukaan ottamisen yhteydessä. Kaikki neljä tukiasemaa jakoivat kaikkia käytössä olevia langattomia verkkoja (Kts. Kuvio 5).



Kuvio 5 Valmetin laboratorioympäristön topologia

4.3 DHCP konfigurointi

Testiympäristön valmistelu aloitettiin konfiguroimalla Ciscon kytkimelle DHCP-asetukset langattomille verkoille Taulukon 3 mukaisesti. Testiympäristössä sekä Valmetin laboratorioympäristössä käytettiin 192.168. -alkuisia yksityisiä osoitteita ja jokaisella langattomalla verkolla oli käytössä /24-verkkoblokki eli 254 osoitetta.

Taulukko 3 Testiympäristön DHCP määritykset

Nimi	Verkko	Maski	Oletusreititin
DNA_IOT	192.168.20.0	255.255.255.0	192.168.20.1
DNA_WLAN_Maint	192.168.30.0	255.255.255.0	192.168.30.1
DNA_UI_WLAN	192.168.33.0	255.255.255.0	192.168.33.1
DNA_Data	192.168.40.0	255.255.255.0	192.168.40.1

Kuviossa 6 nähdään kuinka DNA_IOT-langattoman verkon DHCP-asetukset konfiguroitiin Cisco 2960-kytkimelle. Ensimmäisellä rivillä määritettiin DHCP-poolille nimi, toisella rivillä määritettiin poolin käyttämä verkko sekä verkkomaski, kolmannella rivillä määritettiin oletusreititin, joka määritetään myöhemmin VLAN-rajapinnan IP-osoitteeksi ja lopuksi estetään oletusreitittimen osoitteen jakaminen DHCP:n kautta asiakkaille. Nämä komennot toistettiin jokaiselle langattomalle verkolle Taulukon 3 mukaisilla osoitteilla.

```
jkl-sw-01(config)#ip dhcp pool DNA_IOT
jkl-sw-01(dhcp-config)#network 192.168.20.0 255.255.255.0
jkl-sw-01(dhcp-config)#default-router 192.168.20.1
jkl-sw-01(dhcp-config)#exit
jkl-sw-01(config)#ip dhcp excluded-address 192.168.20.1
jkl-sw-01(config)#
```

Kuvio 6 DHCP-asetuksien konfigurointi kytkimellä

4.4 VLAN konfigurointi

VLAN asetukset määritettiin jokaisella langattomalle verkolle testiympäristössä Taulukon 4 mukaisesti. VLAN konfigurointi aloitettiin määrittämällä Vlan1 tukiasemia varten. Vlan1-rajapintaan asetettiin IP-osoite 192.168.8.200 yhteyksien testaamista varten ja määritettiin ip helper address osoitteeksi 192.168.8.1, että kytkimeen yhdistettävät tukiasemat saavat IP-osoitteen mobiilireitittimen omalta DHCP-palvelimelta.

Taulukko 4 Testiympäristön VLAN määritykset

VLAN ID	Nimi	Verkko	Oletusyhdys-käytävä
1	Tukiasemat	192.168.8.0 /24	192.168.8.1
20	DNA_IOT	192.168.20.0 /24	192.168.20.1
30	DNA_WLAN_Maint	192.168.30.0 /24	192.168.30.1
33	DNA_UI_WLAN	192.168.33.0 /24	192.168.33.1
40	DNA_Data	192.168.40.0 /24	192.168.40.1

Kuviossa 7 nähdään komennot DNA_IOT-langattoman verkon VLAN:n luontiin. Ensimmäiseksi luotiin uusi vlan ID:llä 20, annettiin VLAN:lle nimi ja siirryttiin vlan20-rajapintaan, jolle määritettiin IP-osoite ja aliverkon peite sekä kuvaus. Samat komennot toistettiin Taulukon 4 mukaisesti myös DNA_WLAN_Maintenance, DNA_UI_WLAN ja DNA_Data langattomille verkoille.

```
jkl-sw-01(config)#vlan 20
jkl-sw-01(config-vlan)#name DNA_IOT
jkl-sw-01(config-vlan)#exit
jkl-sw-01(config)#int vlan 20
jkl-sw-01(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

jkl-sw-01(config-if)#ip address 192.168.20.1 255.255.255.0
jkl-sw-01(config-if)#description DNA_IOT
jkl-sw-01(config-if)#
```

Kuvio 7 VLAN konfigurointi kytkimellä

4.5 Verkkolaitteen rajapinnat tukiasemille

Kun tukiasemat oli yhdistetty verkkolaitteeseen, määritettiin verkkolaitteen rajapintoihin, joihin tukiasemat olivat kytkettynä, Kuviossa 8 näkyvät komennot. Testiympäristössä määritettiin komennot rajapintoihin GigabitEthernet 0/1 ja 0/2 antamalla range-komento. Määritettiin rajapintojen switchport mode trunkiksi, sekä native vlan ID:llä 1 ja lopuksi määritettiin sallituiksi VLAN:ksi käytössä olevat 1, 20, 30, 33 ja 40.

```
jkl-sw-01(config)#int range gigabitEthernet 0/1 - 2
jkl-sw-01(config-if-range)#switchport mode trunk
jkl-sw-01(config-if-range)#switchport trunk native vlan 1
jkl-sw-01(config-if-range)#switchport trunk allowed vlan 1,20,30,33,40
```

Kuvio 8 Tukiasemien rajapintojen konfigurointi

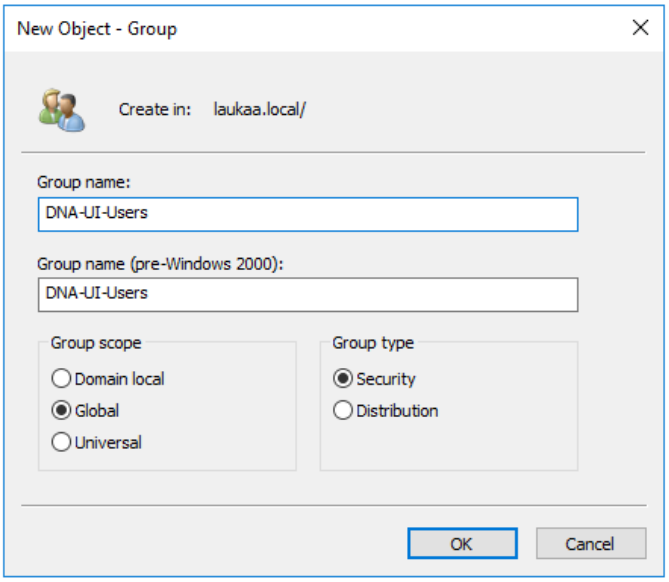
4.6 RADIUS-palvelimen konfigurointi

Lopullisessa ympäristössä yhden langattoman verkon käyttäjät on tarkoitus autentikoida Valmetin omalla RADIUS-palvelimella, joten testiympäristössä ja Valmetin laboratorioympäristössä luotiin RADIUS-palvelin ja käyttäjät, joilla mallinnettiin lopullista toimintaa. Virtuaalikoneelle asennettiin Windows Server 2016 käyttöjärjestelmä, jolle asennetaan RADIUS-palvelimen vaatimat ADCS – Certification Authority ja Network Policy and Access Services (NPAS). Testiympäristössä asennettiin virtuaalikoneelle AD DS-rooli, määritettiin tietokoneen nimeksi DC1, domainiksi kuvitteellinen laukaa.local ja määritettiin staattinen IP-osoite, jotta tukiasemilta voidaan ottaa yhteyttä RADIUS-palvelimelle.

4.6.1 Käyttäjien ja ryhmän luonti

Luotiin testiympäristöön muutamia käyttäjiä testaamista varten valitsemalla Server Managerin Tools ja avaamalla Active Directory Users and Computers. Avattiin alavalikot painamalla domainia laukaa.local, painettiin hiiren oikealla Users-kansiota ja valittiin New – User. Määritettiin käyttäjille etunimi, sukunimi ja User logon name, joka oli muotoa etunimen kolme ensimmäistä merkkiä sekä sukunimen neljä ensimmäistä merkkiä ja painettiin Next. Määritettiin käyttäjille salasana, asetettiin ettei salasana vanhene koskaan ja painettiin Next. Tarkistettiin, että tiedot ovat oikein ja painettiin Finish.

Luotiin Security Group, johon lisätään käyttäjät, joille annetaan oikeus kirjautua langattomaan verkkoon. Painettiin domainia laukaa.local hiiren oikealla painikkeella ja valittiin New – Group. Määritettiin Security Group:n nimeksi DNA-UI-Users, Group scope Global ja Group type Security kuvion 9 mukaisesti.



Kuvio 9 Security Group luominen

Seuraavaksi lisättiin halutut käyttäjät luotuun ryhmään maalaamalla käyttäjät domainin Users-välilehdellä, painamalla hiiren oikealla yhtä valituista käyttäjistä ja painamalla Add to a group. Kirjoitettiin Enter the object names to select -laatikkoon DNA, painettiin Check Names ja OK, minkä jälkeen avautui ilmoitusikkuna, että ryhmään lisääminen on onnistunut.

4.6.2 Active Directory Certification Authority

Asennettiin DC1-palvelimelle ADCS – Certification Authority painamalla Server Managerin oikeasta yläkulmasta Manage ja Add Roles and Features. Valittin Role-based or feature-based installation ja painettiin Next, valittiin oikea palvelin ja painettiin Next. Valittiin listalta Active Directory Certificate Services, painettiin Add Features ja painettiin Next, kunnes voitiin aloittaa asennus painamalla Install.

Kun asennus oli valmistunut, Server Managerin oikeaan yläkylmään tuli keltainen kolmio Notifications-painikkeen alle. Konfiguroitiin ADCS avaamalla Notifications ja painamalla Configure Active Directory Certificate Services on the destination server. Painettiin Next, valittiin Certification Authority ja painettiin Next, valittiin Enterprise CA ja painettiin Next. Valittiin Root CA, painettiin Next, valittiin Create a new private key ja painettiin Next. Valittiin salauksen tarjoajaksi alasvetovalikosta

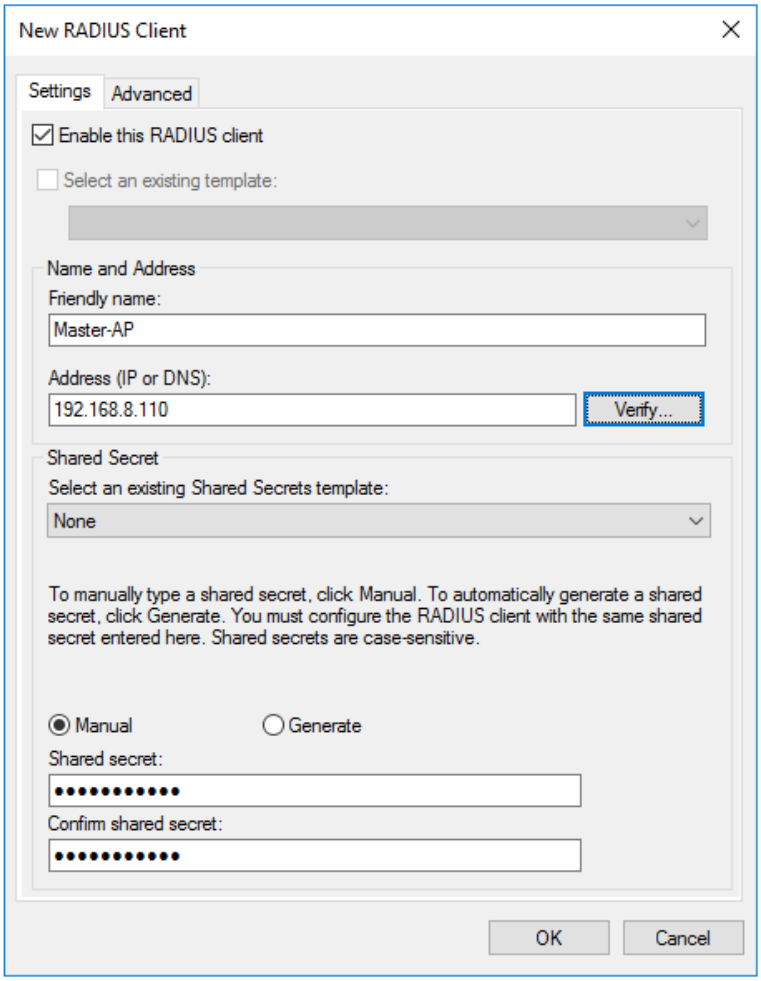
RSA#Microsoft Software Key Storage Provider ja määritettiin alasvetovalikosta 2048 avaimen pituudeksi. Valittiin hash-algoritmiksi SHA256 ja painettiin Next.

Seuraavalla sivulla annettiin CA:lle nimi, tarkistettiin, että Distinguished name suffix on oikeassa muodossa ja painettiin Next. Valittiin sertifikaatin voimassaoloajaksi viisi vuotta ja painettiin Next. Tarkistettiin, että sertifikaatin tiedot ovat oikein asennusta varten ja painettiin Configure. Konfiguroinnin valmistumisen jälkeen tuli ilmoitus onnistumisesta, painettiin Close ja ADCS oli valmiina RADIUS-palvelinta varten.

4.6.3 Network Policy and Access Services

Asennettiin NPAS painamalla Server Managerin Manage ja valitsemalla Add Roles and Features. Valittiin Role-based or feature-based installation ja painettiin Next. Valittiin Network Policy and Access Services, painettiin Add Features avautuneesta ikkunasta ja painettiin Next, kunnes voitiin aloittaa asennus painamalla Install. Asennuksen valmistumisen jälkeen painettiin Close.

Tämän jälkeen määritettiin tukiasemat RADIUS asiakasohjelmiksi valitsemalla Server Managerista Tools ja Network Policy Server. Laajennettiin RADIUS Clients and Servers -otsikkoa, painettiin hiiren oikealla RADIUS Clients ja valittiin New. Määritettiin kuvion 10 mukaisesti tukiasemalle tunnistettava nimi, IP-osoite, joka varmennettiin sekä määritettiin manuaalisesti Shared secret, jota tarvitaan myöhemmin Master-tukiasemalla AAA-palvelinta määritettäessä.



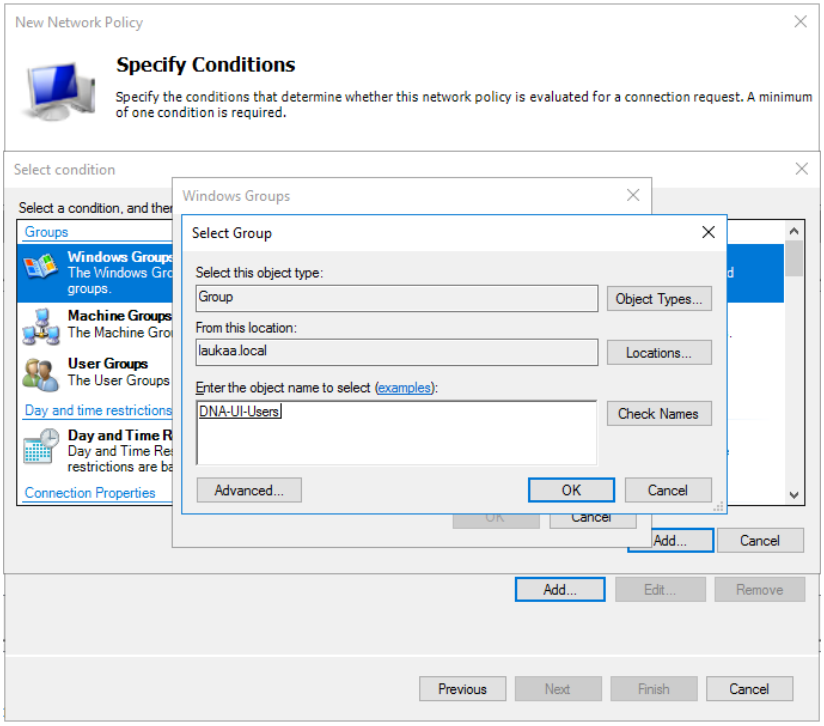
Kuvio 10 RADIUS asiakasohjelman määrittäminen

Kaikki varmennuspyynnöt RADIUS-palvelimelle tulevat Master-tukiasemalta riippumatta siitä, mihin tukiasemaan käyttäjä on yhteydessä, joten autentikoinnin toimimiseksi riittäisi vain Master-tukiaseman lisääminen asiakasohjelmaksi. Vikatilanteissa, joissa Master-tukiasema menettää yhteyden verkkoon tai virransyötön, siirtyy Master-tukiaseman ominaisuudet toiselle ympäristössä olevalle tukiasemalla ja tämän vuoksi kaikki ympäristössä olevat tukiasemat lisättiin RADIUS-asiakasohjelmaksi toiminnan takaamiseksi.

Seuraavaksi määritettiin yhteydenottopyyntöjen menettelytapa laajentamalla Network Policy Serverin Policies, painamalla hiiren oikealla Connection Request Policies ja valitsemalla New. Asetettiin Policy name ja painettiin Next. Painettiin Add, valittiin listalta NAS Port Type, painettiin Add,

valittiin Wireless – IEEE 802.11, painettiin OK ja Next, kunnes voitiin painaa Finish. RADIUS noudattaa ylhäältä alaspäin arvojärjestystä, joten painetaan luotua menettelytapaa hiiren oikealla ja painetaan Move Up, kunnes se on listalla ensimmäisenä.

Määritettiin vielä menettelytapa, jolla annetaan oikeus liittyä langattomaan verkkoon vain halutuille käyttäjille painamalla hiiren oikealla Network Policies ja valitsemalla New. Annettiin nimeksi DNA-UI-WLAN ja painettiin Next. Painettiin Add, valittiin listalta Windows Groups, painettiin Add sekä Add Groups, kirjoitettiin DNA, painettiin Check Names, jolloin aiemmin luotu DNA-UI-Users tulee valituksi, painettiin OK, OK ja Next. Valittiin Access granted ja painettiin Next (Kts. Kuvio 11).



Kuvio 11 Ryhmän määrittäminen RADIUS-palvelimelle

Seuraavalla sivulla painettiin Add, valittiin PEAP ja painettiin OK. Maalattiin PEAP, painettiin Edit ja tarkistettiin, että käytössä on oikea aikaisemmin luotu sertifikaatti. Painettiin Add, valittiin EAP-MSCHAP v2 ja painettiin OK. Master-tukiasemalta voidaan testata yhteyttä RADIUS-palvelimelle käyttäen joko CHAP- tai PAP-autentikointiprotokollaa, joten valittiin listalta Encrypted authentication (CHAP) sekä Unencrypted authentication (PAP, SPAP) ja painettiin Next, kunnes voitiin painaa Finish. Painettiin vielä luotua DNA-UI-WLAN hiiren oikealla ja painettiin Move Up, kunnes se oli listalla ensimmäisenä.

5 Ympäristön käyttöönotto

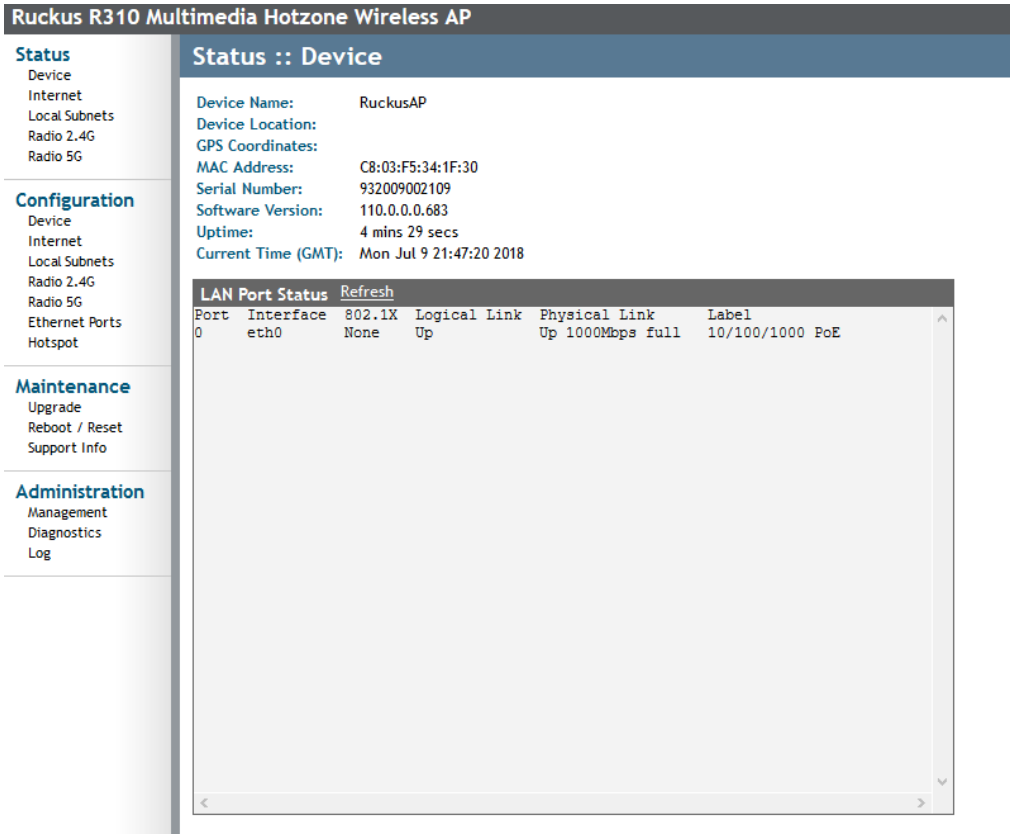
5.1 Päivittäminen Unleashed ohjelmistoon

Tehdasasetuksilla olevissa Ruckus R310 laitteissa on oletuksena Solo Access Point ohjelmisto, joka tunnistetaan 110.x.x.x.x ohjelmistoversiosta. Unleashed ympäristössä olevissa tukiasemissa on oltava Unleashed-ohjelmisto, joka tunnistetaan 200.x.x.x.x ohjelmistoversiosta. Tehtiin tunnukset Ruckuksen tukisivustolle ja kirjauduttiin sisään osoitteessa support.ruckuswireless.com. Unleashed-ohjelmisto on ilmainen, joten sen lataamiseksi ei vaadita erillisen lisenssin hankkimista. Ladattiin sivustolta R310-laitteen uusimman Unleashed ohjelmiston bl7-tiedosto, jota käytetään myöhemmin tukiaseman päivittämiseksi.

Otettiin tukiaseman pohjasta laitteen MAC-osoite ylös myöhempää käyttöä varten ja yhdistettiin tukiaseman POE IN-portti tietokoneen verkkoporttiin verkkokaapelilla sekä kytkettiin tukiasema verkkovirtaan verkkoadapterilla. Vaihtoehtoisesti voidaan käyttää PoE-injektoria, jolloin kytketään tietokone PoE-injektorin DATA-porttiin ja PoE-portti tukiaseman POE IN-porttiin.

Määritettiin tietokoneelle staattinen IP-osoite samasta verkosta tukiaseman oletusyhdyskäytävän kanssa. Windows 10 tietokoneella staattinen IP-osoite määritettiin menemällä polkua Start – Control Panel – Network and Sharing Center – Change Adapter Settings. Painettiin hiiren oikealla Local Area Connection, valittiin Properties. Avautuvasta ikkunasta valittiin Internet Protocol Version 4 (TCP/IPv4) ja painettiin Properties. Valittiin Use the following IP address ja määritettiin IP-osoitteeksi mikä tahansa osoite väliltä 192.168.0.2 - 192.168.0.254, määritettiin aliverkon peitteeksi 255.255.255.0 ja jätettiin oletusyhdyskäytävä sekä DNS palvelin kentät tyhjiksi.

Avattiin verkkoselain ja siirryttiin osoitteeseen https://192.168.0.1. Tässä vaiheessa selain saattaa antaa turvallisuusvaroituksen, koska ei tunnista SSL-sertifikaattia. Esimerkiksi Chrome-selaimella päästiin eteenpäin valitsemalla Advanced ja Proceed to https://192.168.0.1. Tämän jälkeen Ruckus Wireless Admin -kirjautumissivusto avautui ja kirjauduttiin sisään käyttämällä käyttäjätunnusta super ja salasanaa sp-admin. Kirjautumisen jälkeen avautui Kuviossa 12 näkyvä tukiaseman oletusnäkymä, josta nähtiin tukiaseman MAC-osoite sekä käytössä ollut ohjelmistoversio.



Kuvio 12 Tukiaseman oletusnäkymä

Valittiin Maintenance-otsikon alta Upgrade, jolloin uusi sivu avautui. Sivulta voidaan päivittää laitteen ohjelmistoversio tai laitteen sertifikaatti lokaalisti, verkosta tai tiedonsiirtoprotokollia käyttämällä. Valittiin Upgrade Method Local ja Target Selection Firmware ja painettiin Browse, minkä jälkeen valittiin aikaisemmin Ruckuksen tukisivustolta ladattu bl7-tiedosto. Painettiin Perform Upgrade ja tukiasema aloitti päivittämisen. Tukiaseman päivittäminen Unleashed-versioon on tehtävä kaikille Unleashed-ympäristössä käytettäville tukiasemille erikseen.

5.2 Master-tukiaseman konfigurointi

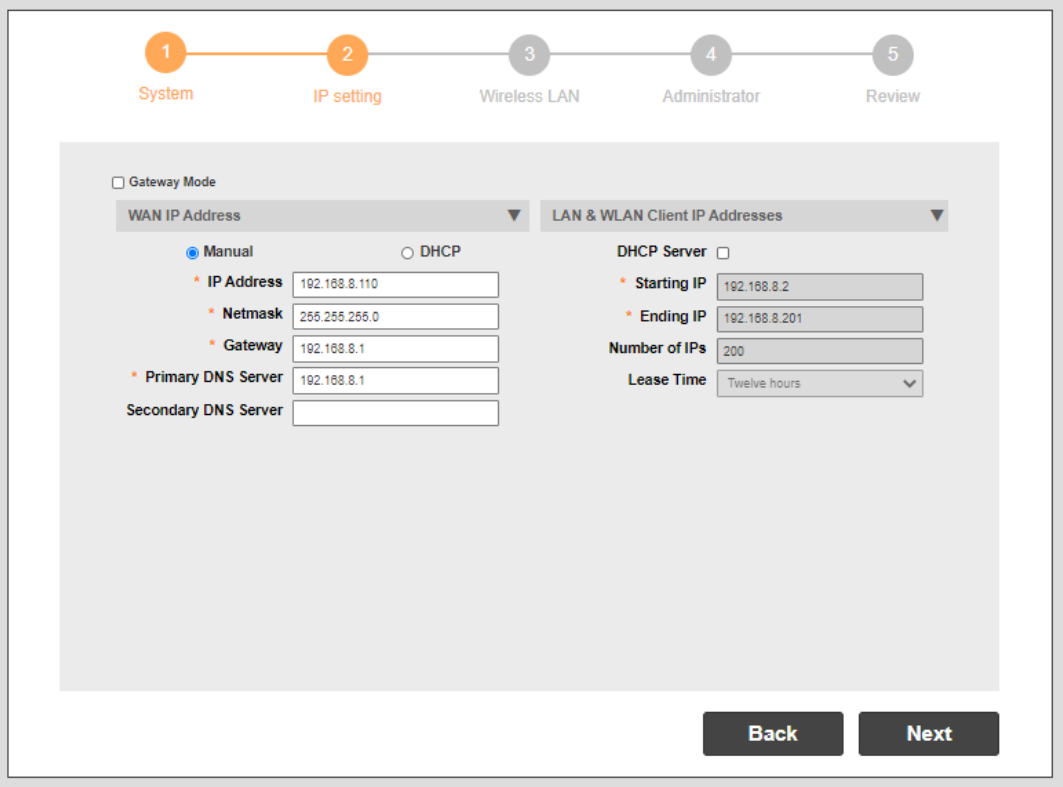
Master-tukiaseman kautta hallinnoidaan kaikkia ympäristöön liitettyjä tukiasemia ja sen kautta tehdään konfiguraatiot ympäristön langattomien verkkojen osalta. Valittiin tukiasema, joka asennetaan ympäristön Master-tukiasemaksi ja otettiin tukiaseman MAC-osoite ylös laitteen pohjasta myöhempää käyttöä varten. Kytkettiin tukiasema sisäverkkoon verkkokaapelilla ja verkkovirtaan verkkoadapterilla. Vaihtoehtoisesti voidaan käyttää PoE-injektoria, jolloin kytketään PoE-injektorin DATA-portti sisäverkkoon ja PoE-portti tukiaseman POE IN-porttiin.

5.2.1 Esiasennus

Käynnistymisen jälkeen tukiasema mainostaa 2.4 GHz taajuudella suojaamatonta langatonta verkkoa, jonka nimi on Configure.Me-xxxxxx, jossa x-kirjaimet vastaavat tukiaseman MAC-osoitteen viimeisiä merkkejä. Yhdistettiin langattomaan verkkoon, avattiin verkkoselain, kirjoitettiin URL-kenttään unleashed.ruckuswireless.com ja painettiin enter. Selain antoi jälleen turvallisuusvaroituksen, Chrome-selaimella päästiin eteenpäin painamalla Advanced ja Proceed to unleashed.ruckuswireless.com.

Unleashed asennussivusto avautui ja valittiin käytettäväksi kieleksi englanti, valittiin Typical Install ja painettiin Next. Asennuksen ensimmäisessä vaiheessa annettiin tehtävälle Unleashed-ympäristölle nimi, valittiin Country Code eli missä maassa ympäristö on käytössä ja otetaan tarvittaessa Mesh-ominaisuus käyttöön. Testiympäristössä käytössä olleilla R310-laitteilla Mesh-ominaisuus ei ole tuettuna.

Asennuksen toisessa vaiheessa määritettiin tukiaseman IP-asetukset. Sisäverkkoon kytkettynä laite sai automaattisesti osoitteen DHCP:n kautta, mutta ympäristön toiminnan takaamiseksi määritettiin tukiasemalla staattinen IP-osoite verkkosuunnitelman mukaisesti. WAN IP Address kohtaan valittiin Manual, määritettiin IP-osoite, aliverkon peite, oletusyhdyskäytävä ja DNS-palvelin (Kts. Kuvio 13).



Kuvio 13 Esiasennuksen IP-asetuksien määrittäminen

Kolmannessa vaiheessa määritettiin ensimmäinen WLAN-verkko. Määritettiin langattomalle verkolle nimi, valittiin Password Protect (WPA2) kohtaan Yes ja määritettiin langattoman verkon salasana. Lopullisessa ympäristössä tätä luotavaa langatonta verkkoa ei tulla käyttämään, vaan sitä käytetään ainoastaan ympäristön konfigurointiin tarvittaessa.

Neljännessä vaiheessa määritettiin ympäristön ylläpitäjälle käyttäjätunnus ja salasana, joiden avulla kirjaudutaan Master-tukiasemalle ympäristön konfigurointia varten. Tässä vaiheessa voidaan ottaa käyttöön myös Password Recovery, johon määritetään sähköpostiosoite, turvakysymys ja turvavastaus, joiden avulla voidaan salasana palauttaa.

Asennuksen viimeisessä vaiheessa näkyi määritetyt asetukset ja kaiken ollessa kunnossa, painettiin Finish. Tukiasema aloitti konfiguroimaan määritettyjä asetuksia ja käynnisti itsensä uudestaan. Asennuksen valmistumisen jälkeen tuli ilmoitus, joka kertoi, että Unleashed Master on konfiguroitu ja ohjeisti, kuinka Master-tukiasemaa pääsee hallinnoimaan.

5.2.2 Konfigurointi webkäyttöliittymässä

Master-tukiasemaa ja ympäristöä voidaan hallinnoida liittymällä esiasennuksessa luotuun langattomaan verkkoon ja kirjautumalla ylläpitäjän tunnuksilla osoitteessa unleashed.ruckuswireless.com tai sisäverkon kautta kirjoittamalla selaimen osoitekenttään tukiaseman IP-osoite ja kirjautumalla ylläpitäjän tunnuksilla.

Kirjautumisen jälkeen avautui Master-tukiaseman webkäyttöliittymän oletusnäkymä, jossa on otsikot Internet, WiFi Networks, Clients, Access Points ja Admin & Services. Internet otsikon alta nähdään tukiaseman IP-tiedot ja onko tukiasema yhteydessä ulkoverkkoon. WiFi Networks otsikon alta luodaan uusia langattomia verkkoja sekä muokataan ja monitoroidaan jo luotuja langattomia verkkoja. Clients otsikon alta voidaan monitoroida kaikkia langattomien verkkojen käyttäjiä. Access Points otsikon alla nähdään kaikki järjestelmään liitetyt tukiasemat ja voidaan muokata tukiasemien tietoja sekä asetuksia. Admin & Services otsikon alta löytyy Master-tukiaseman ja ympäristön palvelut sekä yleiset asetukset.

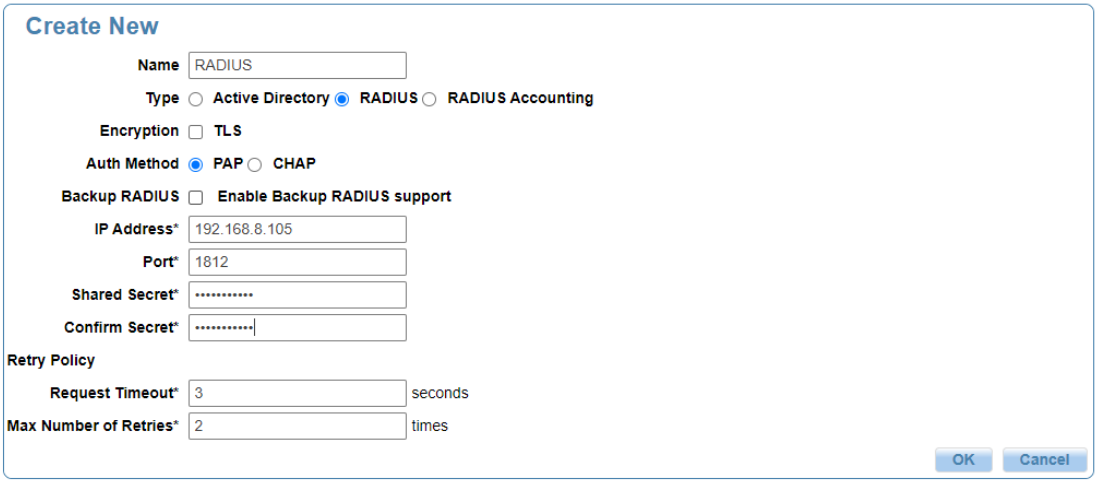
Kun ympäristöön tulee monta tukiasemaa, on hyvä eritellä jokaiselle tukiasemalle tunnistettavat tiedot. Se tehtiin avaamalla Access Points otsikko, valittiin tukiasema MAC-osoitteen perusteella ja painettiin Edit, jolloin tukiaseman muokkaus -ikkuna avautui. General välilehdelle määritettiin laitteelle tunnistettava nimi, kuvaus ja sijainti, tarvittaessa voidaan määrittää myös GPS koordinaatit.

Prosessinohjausjärjestelmän ympäristössä pyritään siihen, ettei langattomissa verkoissa tule päällekkäisyyksiä ja varmistetaan paras mahdollinen toimivuus, joten määritettiin tukiasemille käyttöön ainoastaan yleisimmät käytössä olevat 2.4 GHz ja 5 GHz kanavat. Valittiin tukiaseman muokkaus -ikkunasta Radio B/G/N(2.4G) ja valittiin Radio-listalta käytettäväksi ainoastaan kanavia 1, 5, 9, 13 sekä Channnelization-valikkoon määritettiin kaistanleveydeksi 20 MHz, jolloin kanavat eivät ole päällekkäin. Radio A/N/AC(5G) välilehdellä valittiin Radio-listalta käytettäväksi kanavat 36, 40, 44 ja 48 sekä Channelization-valikkoon määritettiin kaistanleveydeksi 40 MHz.

5.2.3 AAA-palvelimen lisääminen Master-tukiasemalle

Lisättiin aiemmin Windows AD:lla luotu RADIUS-palvelin Master-tukiasemalle langattomien verkkojen käyttäjien autentikointia varten painamalla Master-tukiaseman käyttöliittymässä Admin &

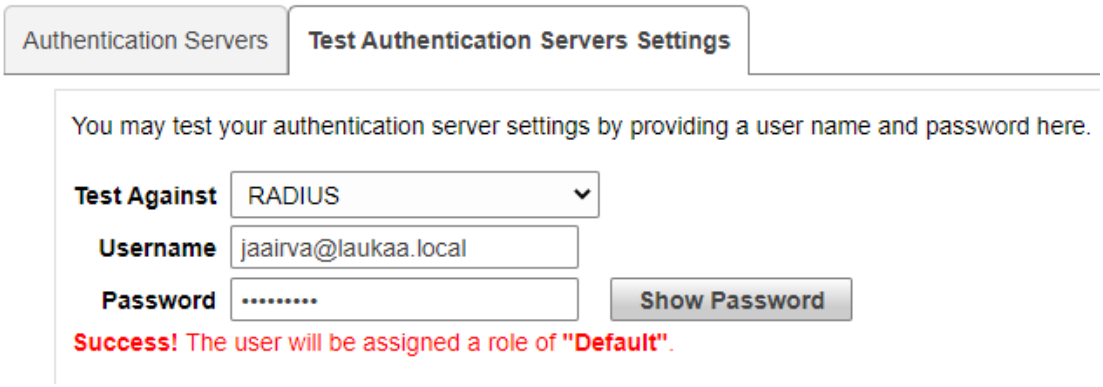
Services – Services – AAA Servers ja painamalla avautuneesta Authentication Servers listalta Create New. Määritettiin palvelimen tiedot Kuvion 14 mukaisesti.



Kuvio 14 RADIUS-palvelimen määrittäminen Master-tukiasemalle

Annettiin palvelimelle tunnistettava nimi, valittiin tyypiksi RADIUS, määritettiin RADIUS-palvelimen IP-osoite ja annettiin RADIUS-palvelimelle kohdassa 4.7.3 määritetty Shared Secret. Valittiin autentikointitavaksi PAP, joka on käytössä ainoastaan yhteyttä testatessa Master-tukiasemalta RADIUS-palvelimelle. Oletuksena yhteydenottopyynnön aikakatkaisu on 3 sekuntia ja uudelleen yrityksiä on kaksi kappaletta, mutta nämä voidaan tarvittaessa määrittää halutun laisiksi.

Testattiin yhteyttä RADIUS-palvelimelle valitsemalla Test Authentication Servers Settings -välilehti, valittiin alasvetovalikosta luodun palvelimen nimi, kirjoitettiin käyttäjätunnus muodossa <käyttäjätunnus@domain>, annettiin salasana ja painettiin Test. Testin onnistuessa nähtiin Kuviossa 15 näkyvä ilmoitus.



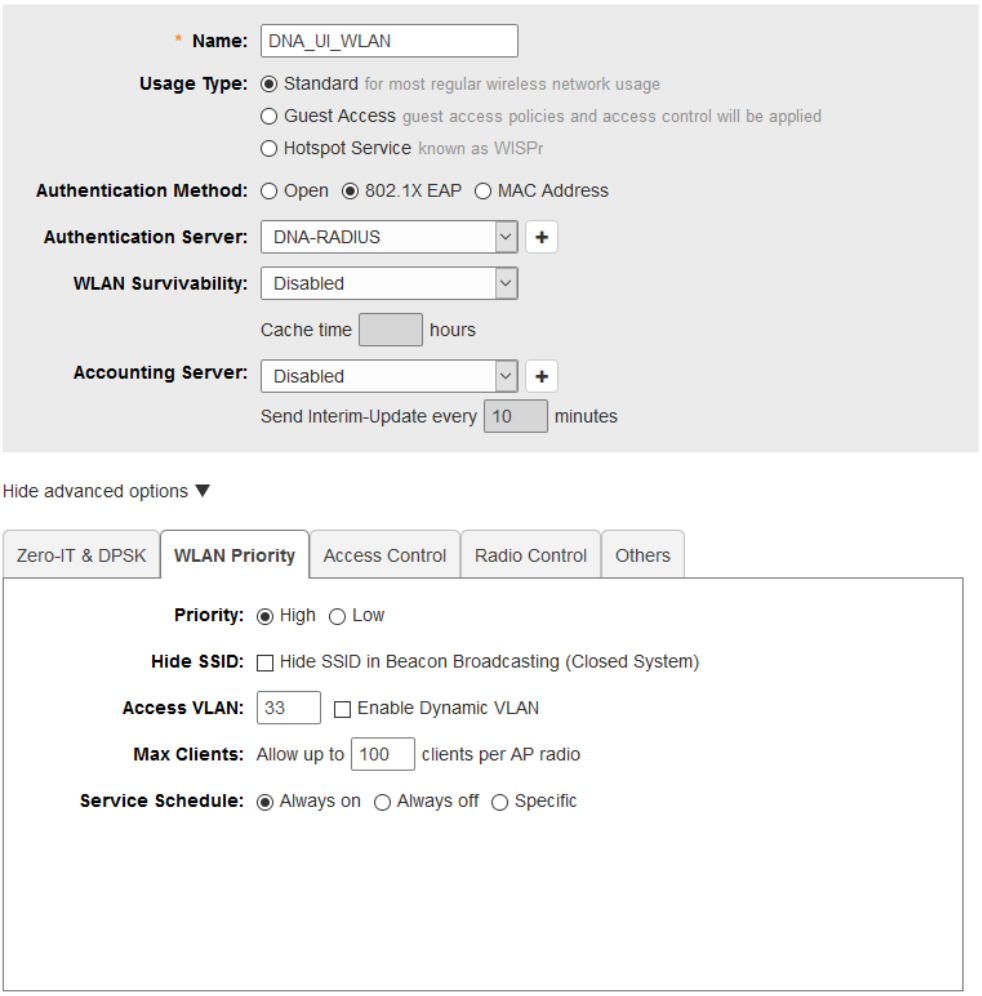
Kuvio 15 RADIUS-palvelimen yhteystesti Master-tukiasemalta

5.3 Langattomien verkkojen luonti

5.3.1 DNA_UI_WLAN

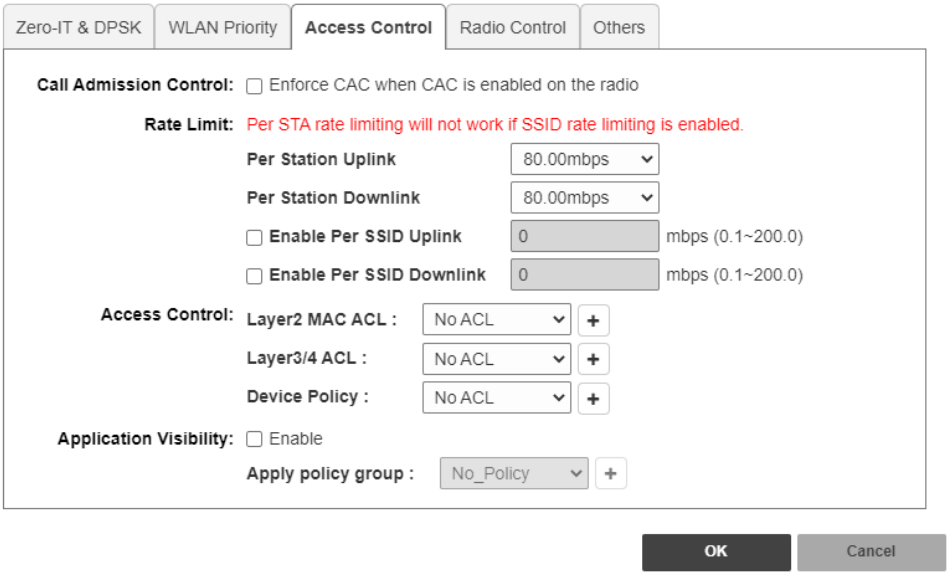
DNA_UI_WLAN on tarkoitettu Valmetin omille työntekijöille, jotka ovat päivittäin ympäristössä ja käyttävät omia laitteitaan työntekoon sekä laitteiden ylläpitoon ja huoltoon. Kaikki verkon käyttäjät autentikoidaan Valmetin DNA-RADIUS -palvelimella.

Langattoman verkon luomiseksi valittiin Master-tukiaseman käyttöliittymän etusivulta WiFi Networks ja painettiin Create, uudesta ikkunasta avattiin Advanced options ja sen WLAN Priority -välilehti, jolloin näkymä oli Kuvion 16 mukainen.



Kuvio 16 DNA_UI_WLAN luonti

Määritettiin langattoman verkon nimeksi DNA_UI_WLAN, käyttötyypiksi Standard, autentikointitavaksi 802.1X EAP, valittiin alasvetovalikosta autentikointipalvelimeksi kohdassa 5.3.2 määritetty palvelin. Lisävaihtoehtojen WLAN Priority -välilehdellä asetettiin Priority High, määritettiin Access VLAN 33 ja palveluaikatauluksi langaton verkko olemaan aina päällä. Avattiin Access Control -välilehti ja valittiin Per Station Uplink ja Per Station Downlink alasvetovalikoista arvoksi 80 mbps (Kuvio 17). Tällä varmistettiin ettei yksi tukiasema pysty ruuhkautuessaan käyttämään kokonaan sisäverkossa olevien 100 mbit/s linkkien kaistaa.

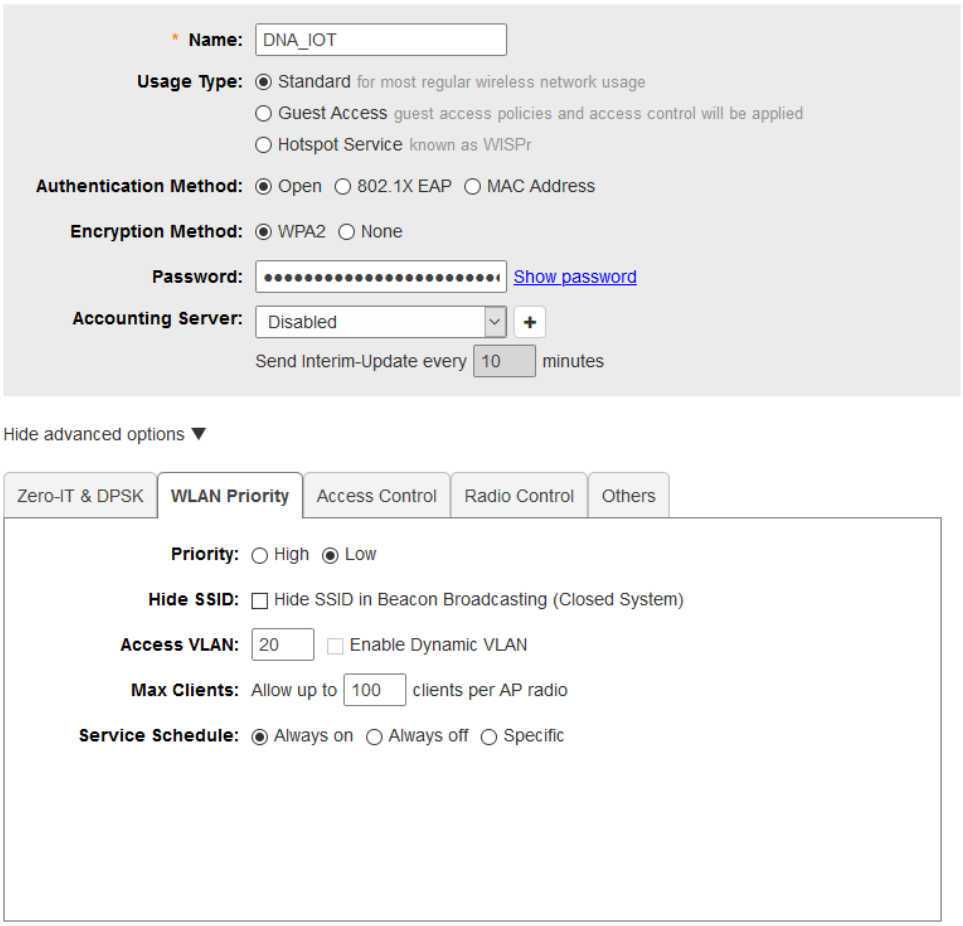


Kuvio 17 Access Control määrittäminen

5.3.2 DNA_IOT

DNA_IOT langaton verkko on ympäristössä oleville IOT- ja sensorilaitteille, jotka lähettävät jatkuvasti dataa palvelimille, joilta voidaan monitoroida laitteiden toimintaa. IOT- ja sensorilaitteilla ei ole ihmisiä käyttäjinä ja autentikoinnin pitää tapahtua ilman toimenpiteitä, joten langattomassa verkossa on WPA2-salaus.

Luotiin uusi langaton verkko valitsemalla Master-tukiaseman käyttöliittymän etusivulta WiFi Networks ja painettiin Create, uudesta ikkunasta avattiin Advanced options ja sen WLAN Priority -välilehti. Määritettiin langattoman verkon nimeksi DNA_IOT, käyttötyypiksi Standard, autentikointitavaksi Open, salausmetodiksi WPA2 ja annettiin salasana. Lisävaihtoehtojen WLAN Priority -välilehdellä asetettiin Priority High, määritettiin Access VLAN 20 ja palveluaikatauluksi langaton verkko olemaan aina päällä (Kuvio 18). Avattiin Access Control -välilehti ja valittiin Per Station Uplink ja Per Station Downlink alasvetovalikoista 40 mbps.

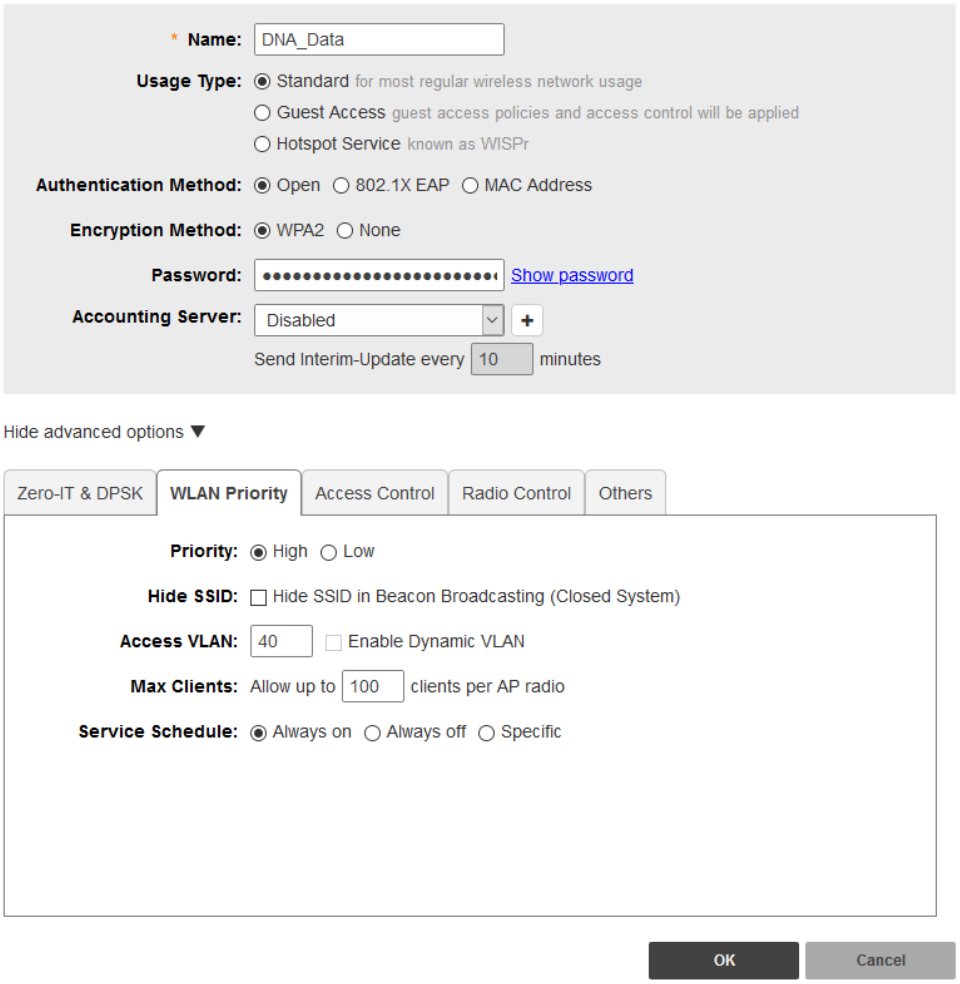


Kuvio 18 DNA_IOT luonti

5.3.3 DNA_Data

DNA_Data langaton verkko on ympäristön datalaitteille, joilla ei ole ihmisiä käyttäjinä ja autentikoinnin pitää tapahtua ilman toimenpiteitä, joten langattomassa verkossa on WPA2-salaus.

Uuden langattoman verkon luomiseksi valittiin Master-tukiaseman käyttöliittymän etusivulta WiFi Networks ja painettiin Create, uudesta ikkunasta avattiin Advanced options ja sen WLAN Priority -välilehti. Määritettiin langattoman verkon nimeksi DNA_Data, käyttötyypiksi Standard, autentikointitavaksi Open, salausmetodiksi WPA2 ja annettiin langattomalle verkolle salasana. Lisävaihtoehtojen WLAN Priority -välilehdellä asetettiin Priority High, määritettiin Access VLAN 40 ja palveluaikatauluksi langaton verkko olemaan aina päällä (Kuvio 19). Avattiin Access Control -välilehti ja valittiin Per Station Uplink ja Per Station Downlink alasvetovalikoista 80 mbps.

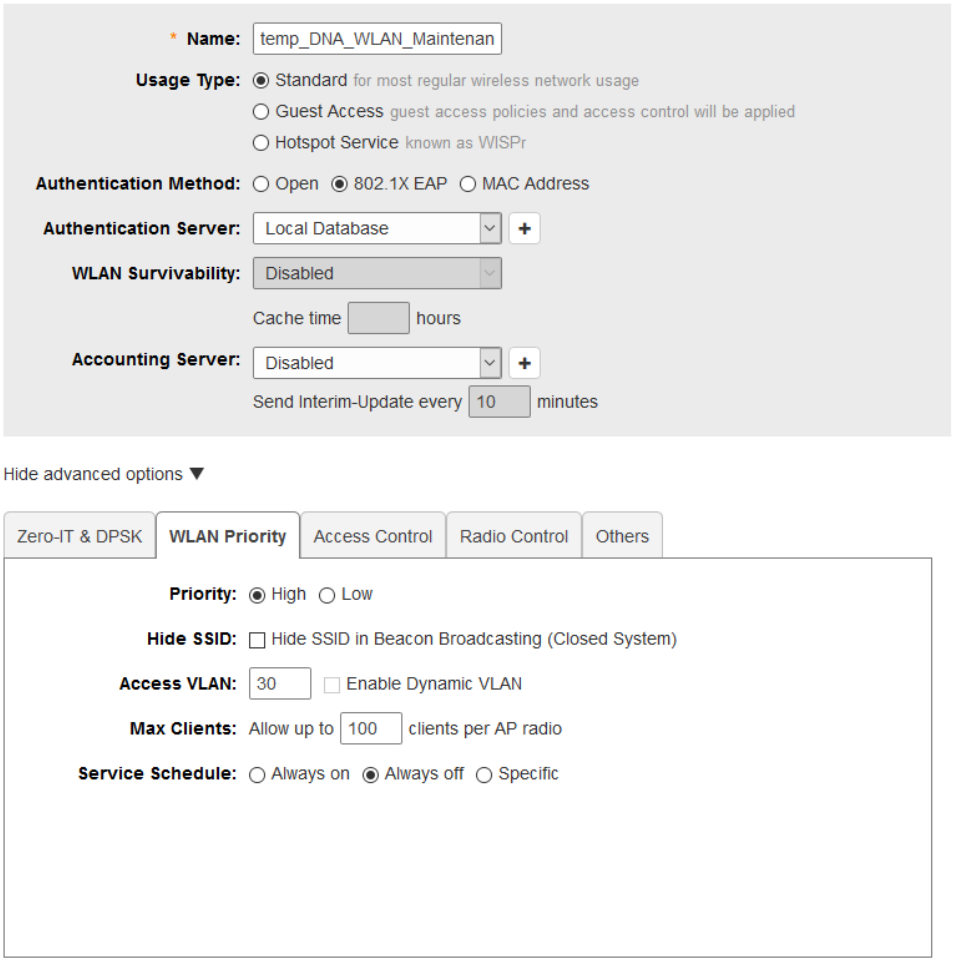


Kuvio 19 DNA_Data luonti

5.3.4 DNA_WLAN_Maintenance

DNA_WLAN_Maintenance langaton verkko on tarkoitettu ympäristössä vikatilanteissa vieraileville huoltomiehille ja halutaan, että huoltomiehet joutuvat kirjautumaan päästäkseen verkkoon. Huoltomiehet halutaan pitää erillään Valmetin omista DNA-käyttäjistä, joten käytetään Master-tukiasemalla olevaa paikallista RADIUS-palvelinta, jota on helppo hallinnoida. Master-tukiaseman paikalliseen tietokantaan luodaan käyttäjäryhmä, jolle annetaan oikeus kirjautua ainoastaan DNA_WLAN_Maintenance langattomaan verkkoon, minkä jälkeen luodaan tarvittavat käyttäjät, jotka sidotaan käyttäjäryhmään. Näin voidaan tarvittaessa luoda ja poistaa huoltomiehien henkilökohtaiset tunnukset tapauskohtaisesti tai tehdä yleiset tunnukset, jotka annetaan vain ympäristössä vieraileville huoltomiehille. DNA_WLAN_Maintenance langaton verkko luodaan valmiiksi, mutta on tarkoitus, että se aktivoidaan käyttöön ainoastaan huoltotilanteissa.

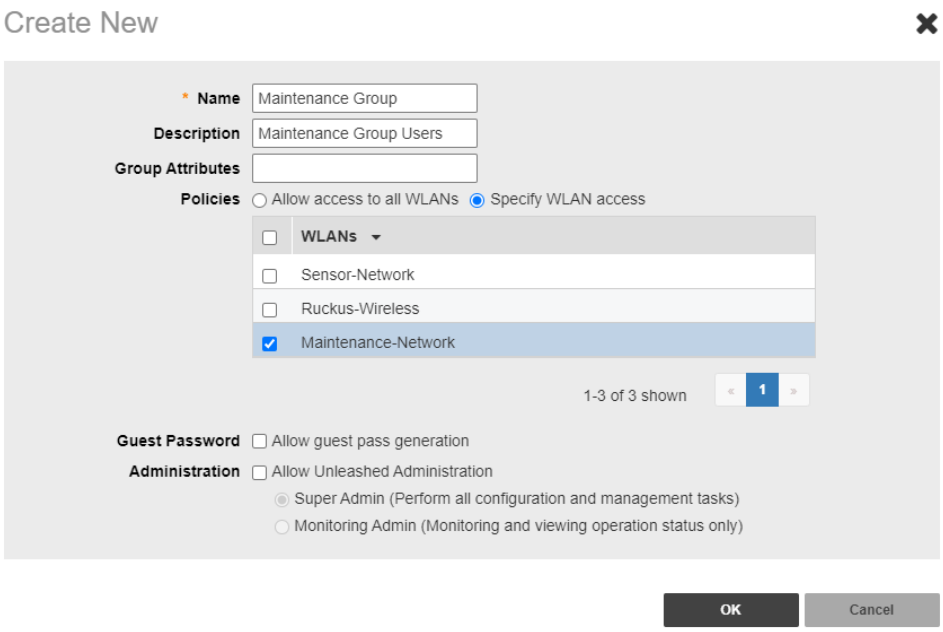
DNA_WLAN_Maintenance-verkon luomiseksi valittiin Master-tukiaseman käyttöliittymän etusivulta WiFi Networks ja painettiin Create, uudesta ikkunasta avattiin Advanced options sekä sen WLAN Priority -välilehti ja määritettiin tiedot Kuvion 20 mukaisesti.



Kuvio 20 DNA_WLAN_Maintenance luonti

Määritettiin langattoman verkon nimeksi DNA_WLAN_Maintenance, käyttötyypiksi Standard, autentikointitavaksi 802.1X EAP ja autentikointipalvelimeksi alasvetovalikosta Local Database. Lisävaihtoehtojen WLAN Priority -välilehdellä asetettiin Priority High, määritettiin Access VLAN 30 ja palveluaikatauluksi langaton verkko olemaan aina pois päältä. Avattiin Access Control -välilehti ja valittiin Per Station Uplink ja Per Station Downlink alasvetovalikoista 80 mbps. Kun langaton verkko halutaan kytkeä päälle huoltomiestä varten, avataan Master-tukiaseman käyttöliittymän WiFi Networks, valitaan DNA_WLAN_Maintenance langaton verkko ja painetaan Enable. Langaton verkko poistetaan käytöstä valitsemalla DNA_WLAN_Maintenance ja painamalla Disable.

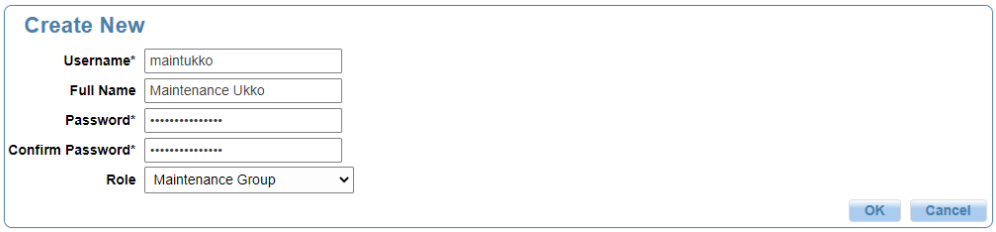
Kun langaton verkko oli valmiina, luotiin rooli valitsemalla käyttöliittymästä Admin & Services – System – Roles ja painamalla Create New, jolloin Kuvion 21 mukainen näkymä avautui.



Kuvio 21 Ryhmän luonti paikalliseen tietokantaan

Annettiin roolille nimeksi Maintenance Group sekä lisättiin kuvaus, jonka jälkeen valittiin roolin käyttämä politiikka. Vaihtoehtoina oli pääsyoikeus kaikkiin langattomiin verkkoihin tai tarkennettu käyttöoikeus. Haluttiin, että roolin käyttäjillä on pääsy ainoastaan DNA_WLAN_Maintenance langattomaan verkkoon, joten valittiin Specify WLAN access ja valittiin listalta vain kyseinen verkko. Roolia luodessa olisi voinut antaa myös Unleashed-järjestelmän ylläpito-oikeudet, mutta tässä tapauksessa, kun käyttäjät ovat ulkopuolisia huoltotyöntekijöitä, jätettiin ylläpito-oikeudet valitsematta.

Seuraavaksi luotiin Maintenance Group:lle käyttäjiä valitsemalla Admin & Services – System – Users ja painamalla Internal User Database -otsikon alta Create New. Määritettiin Kuvion x mukaisesti käyttäjätunnus, kokonimi sekä pitkä salasana useilla eri erikoismerkeillä ja valittiin alasvetovalikosta luotu Maintenance Group -ryhmä (Kts. Kuvio 22).



Kuvio 22 Käyttäjän luonti paikalliseen tietokantaan

Nyt vain Maintenance Group -ryhmään liitetyillä käyttäjillä on pääsyoikeus DNA_WLAN_Maintenance verkkoon ja Internal User Database -otsikon alta voidaan hallinnoida eli luoda, poistaa ja muokata kyseisiä käyttäjiä.

5.4 Uuden tukiaseman lisääminen

Kun uusi tukiasema lisätään ympäristöön, saa tukiasema automaattisesti IP-osoitteen DHCP:n kautta ja tunnistaa, että samassa verkkoblokissa on Master-tukiasema. Uusi tukiasema saa tarvittavat tiedot Master-tukiasemalta ja alkaa jakamaan luotuja langattomia verkkoja automaattisesti käynnistymisen jälkeen.

Master-tukiaseman konfiguroinnin ja langattomien verkkojen luonnin jälkeen lisättiin kolme Unleashed-versioon päivitettyä tukiasemaa ympäristöön yksitellen. Kytkettiin tukiasema verkkoon sekä verkkovirtaan PoE-injektorin avulla ja tukiaseman käynnistymisen jälkeen huomattiin Master-tukiaseman käyttöliittymän Access Points -otsikon alta, että uusi tukiasema ilmestyi listalle.

Ympäristöön tullessaan uudella tukiasemalla ei ole muita tunnistettavia tietoja MAC-osoitteen lisäksi, joten määritettiin tukiasemille tunnistettavat tiedot kohdan 5.2.2 mukaisesti. Määritettiin uusille tukiasemille Edit Access Point:n General-välilehdellä kuvaava nimi, kuvaus ja sijainti. Tämän jälkeen valittiin Radio B/G/N(2.4G) -välilehti ja määritettiin Radio-listalta käytettäväksi kanavia 1, 5, 9, 13 sekä Channnelization-valikkoon asetettiin kaistanleveydeksi 20 MHz ja Radio A/N/AC(5G) -välilehdellä määritettiin käyttöön kanavat 36, 40, 44 ja 48 sekä Channelization-valikkoon asetettiin 40 MHz kohdan 5.2.2 ohjeiden mukaisesti.

6 Toiminnan testaaminen

Toimintaa testattiin alustavassa testiympäristössä sekä Valmetin laboratorioympäristössä. Testiympäristössä toimintaa testattiin 3-5 yhtäaikaisella päätelaitteella käyttäen kaikkia eri langattomia verkkoja. Testiympäristössä tukiasemat oli sijoitettuna omakotitaloon, jolloin tukiasemien etäisyys jäi suhteellisen pieneksi ja päätelaitteen yhdistyessä verkkoon, laite yhdistyi yleensä lähempään laitteeseen seinistä huolimatta. Asunnossa liikkumalla päätelaitteen yhteys pysyi aina tukiasemassa, johon oli alun perin yhdistynyt, siitäkin huolimatta, että siirtyi toisen tukiaseman viereen ja signaalinvoimakkuus oli toiselta tukiasemalta vahvempi. Mikäli päätelaitteet olivat kiinni tukiasemassa, joka ei ollut Master-roolissa ja tukiasemasta kytkettiin virrat pois, siirtyivät päätelaitteet Master-tukiasemalle käytännössä välittömästi. Useissa testeissä siirtymä tapahtui ilman pakettihukkaa ja aiheuttaen vain satunnaisesti yhden tai kahden paketin häviämisen. Mikäli Master-tukiasemasta kytkettiin virrat pois, siirtyi koko ympäristön hallinta automaattisesti toiselle tukiasemalle. Langattomat verkot tulivat näkyville suhteellisen nopeasti, mutta päätelaitteilla, jotka tarvitsivat RADIUS-palvelimen autentikoinnin, katkos venyi n. 2,5 minuutin mittaiseksi, mutta siirtymä tapahtui automaattisesti ilman manuaalisia toimenpiteitä. Salasanalla oleviin langattomiin verkkoihin DNA_Data ja DNA_IOT yhdistyneet päätelaitteet siirtyivät uudelle tukiasemalle huomattavasti nopeammin ja katkos jäi lyhyemmäksi.

Valmetin laboratorioympäristössä asetettiin neljä tukiasemaa ison laboratorion eri osastoille, jolloin tukiasemien väliin jäi 20-50 metriä sekä mahdollisesti yksi tai useampi betoniseinä. Alustavissa testeissä ihmeteltiin miksei saada katkosta aikaan kytkemällä virrat pois tukiasemasta, johon päätelaitteet olivat alun perin yhdistyneet, vaan päätelaitteet yhdistyivät uuteen tukiasemaan niin nopeasti, ettei katkosta havaittu. Testit toteutettiin yhdistämällä jokaiseen langattomaan verkkoon yksi päätelaite esimerkiksi Tukiasema1 vieressä ja siirtämällä päätelaitteet Tukiasema4 viereen ja kytkemällä virrat pois Tukiasema1:stä. Master-tukiaseman kontrollerilta havaittiin, että päätelaitteet siirtyivät uudelle tukiasemalle automaattisesti jo siinä vaiheessa, kun päätelaitteita siirrettiin fyysisesti paikasta toiseen. Näin voitiin todeta, että tiloissa liikkumalla pystytään siirtymään tukiasemalta toiselle ilman katkoksia liikenteessä. Master-tukiaseman alasajoa testattiin useaan otteeseen ja todettiin, että kaikki langattomat verkot sekä päätelaitteet siirtyivät uudelle Master-tukiasemalle ja olivat toimintakuntoisia maksimissaan 3,5 minuutin katkoksen jälkeen.

7 Pohdinta

7.1 Tuloksen arvionti

Tutkimuksen tavoitteena oli luoda Ruckuksen tukiasemilla langattomien verkkojen toteutus, jolla voidaan suorittaa kaikki prosessinohjausjärjestelmän toiminnallisuudet. Tutkimuksen aikana haastateltiin prosessinohjausjärjestelmien suunnittelijoita sekä ylläpitäjiä, että saatiin tietoon aiempien ympäristöjen haasteet ja ongelmat. Ympäristön suunnittelun ja testaamisen yhteydessä keskusteltiin avoimesti ylläpitäjien kanssa ja jokaisen käyttäjäryhmän tarpeet pyrittiin toteuttamaan mahdollisimman hyvin. Työn keskeinen tutkimuskysymys oli, onko mahdollista toteuttaa määrittelyn mukainen tietoturvallinen langaton ympäristö Ruckuksen laitteilla. Voitiin todeta, että tutkimuksen tuloksena saatiin rakennettua ympäristö, jonka toiminnallisuus täytti yrityksen vaatimusmäärittelyn tietoturvan ja langattomien verkkojen osalta. Kaikille käyttäjäryhmille saatiin luotua eriytetty langaton verkko ja jokaisen ryhmän käyttäjät sekä päätelaitteet autentikoitiin toivotulla tavalla. Lisäkysymyksinä oli, onko langaton verkkoympäristö helposti hallinnoitavissa ja voidaanko se ottaa käyttöön missä tahansa. Pystyttiin toteamaan, että Active Directory -ympäristön ja RADIUS-palvelimen käyttö teki käyttäjien hallinnoimisesta helppoa ja tarvittaessa voidaan hyödyntää toimipisteiden olemassa olevaa AD-ympäristöä. Tämän lisäksi tehtiin toimeksiantajan hyödynnettäväksi asennusohjeet, joiden avulla ympäristö voidaan ottaa käyttöön jokaisessa prosessinohjausjärjestelmässä. Jatkotutkimuksen aiheena voisi olla, mitä uusia ominaisuuksia langattomaan verkkoympäristöön lopullisessa tuotannossa käytettävä Ruckus T310-tukiasema ja sen SmarthMesh-ominaisuus voisivat tuoda.

7.2 Johtopäätökset

Todettiin, että Ruckus Master-AP:n käyttöliittymä on erittäin helppokäyttöinen ja langattomien verkkojen sekä käyttäjien hallinta vaivatonta. Käyttöliittymän tarjoama näkymä päätelaitteiden toimintaan antoi myös paljon hyödyllistä dataa langattomien verkkojen kuormasta ja käyttäjämääristä. Asennusohje testattiin käytännössä Valmetin laboratorioympäristöä pystyttäessä ja voitiin todeta, että ohjeen avulla pystytään rakentamaan ympäristö alusta loppuun saakka ilman syvempää osaamista laitteista. Laboratorioympäristössä tehdyissä testeissä huomattiin, että päätelaitteet siirtyivät tukiasemien välillä automaattisesti tiloissa liikkuessa, minkä piti olla mahdollista ainoastaan Ruckuksen laitteilla, joissa on SmartMesh-tuki. Testien tuloksien perusteella todettiin,

että Master-tukiaseman yhteyden menettämisen myötä aiheutuva 3,5 minuutin katkos on ominaisuus, joka on tiedostettava ja lopullisessa ympäristössä Master-tukiaseman sähkönsyöttö ja verkkoyhteys on turvattava mahdollisimman hyvin katkoksien minimoimiseksi.

7.3 Hyödynnettävyys

Todettiin, että lopullinen verkkototeutus on mahdollista ottaa käyttöön toimipisteillä sellaisenaan asennusohjeiden avulla. Testiympäristöissä käytettiin DNA_UI-käyttäjien autentikointiin testejä varten luotua AD-ympäristöä sekä käyttäjäryhmää, mutta tuotannossa voidaan käyttää jokaisella toimipisteellä jo olemassa olevaa AD-ympäristöä sekä käyttäjiä, mikä helpottaa käyttöönottoa ja hallittavuutta. Mikäli tarpeet tulevaisuudessa muuttuvat, pystytään langattomien verkkojen määrää lisäämään helposti. Tutkimuksessa käytetyillä kirjautumismahdollisuuksilla Master-tukiaseman käyttöliittymästä voidaan lisätä langattomia verkkoja nopeasti ja muutoksia täytyy tehdä ainoastaan toimipisteen verkon VLAN-, DHCP- sekä verkkolaitteen rajapinnan asetuksiin.

Lähteet

Automation business line. Nd. Esittely Valmet.com verkkosivulla. Viitattu 10.11.2021. https://www.valmet.com/about-us/valmet-in-brief/our-businesses/automation/

Auvinen, A. & Tarkiainen, E. 2018. Soluessee: Kvalitatiivinen tutkimus. Artikkeli proakatemia.fi verkkosivulla. Viitattu 7.12.2021. https://esseepankki.proakatemia.fi/soluessee-kvalitatiivinen-tutkimus-2/

Bartz, R. J. 2012. CWTS: Certified wireless technology specialist official study guide (2nd ed.). Wiley Pub. E-kirja. Viitattu 12.3.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition

Harte, L. 2004. Introduction to 802. 11 Wireless LAN (WLAN), Technology, Market, Operation, and Services. Althos. E-kirja. Viitattu 10.11.2021. https://janet.finna.fi, Skillsoft Books ITPro

Held, G. 2004. Virtual private networking: A construction, operation and utilization guide. John Wiley. E-kirja. Viitattu 19.2.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition

Lammle, T. & Quinn, E. 2003. CCNP: Switching study guide (2nd ed.). Sybex. E-kirja. Viitattu 15.2.2021. https://janet.finna.fi, Skillsoft Books ITPro

Lukka, K. 2001. Konstruktiivinen tutkimusote. Menetelmäartikkeli metodix.fi verkkosivulla. Viitattu 7.12.2021. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

McAndrew, A. 2012. Introduction to cryptography with open-source software (1st edition.). CRC Press, an imprint of Taylor and Francis. E-kirja. Viitattu 10.11.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition

Naugle, M. G. 1999. Illustrated TCP/IP. Wiley. E-kirja. Viitattu 12.2.2021. https://janet.finna.fi, Skillsoft Books ITPro

O'Brien, T. 2020. Channel Planning Best Practices for Better Wi-Fi. Artikkeli ekahau.com verkkosivulla 20.6.2020. Viitattu 10.11.2021. https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/

Prasad, A. R. & Sŏ, S. 2011. Security in next generation mobile networks: SAE/LTE and WiMAX. River Publishers. E-kirja. Viitattu 6.10.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition

Rackley, S. 2007. Wireless networking technology: From principles to successful implementation (1st edition.). Newnes/Elsevier. E-kirja. Viitattu 10.11.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition

Ruckus R310, Nd. Data sheet ruckuswireless.com verkkosivulla. Viitattu 10.11.2021. https://webresources.ruckuswireless.com/datasheets/r310/ds-commscope-r310.html

Ruckus T310, Nd. Data sheet ruckuswireless.com verkkosivulla. Viitattu 10.11.2021. https://webresources.ruckuswireless.com/datasheets/t310/ds-commscope-t310.html

Understanding and Configuring 802.1X Port-Based Authentication, Nd. Software Configuration Guide cisco.com verkkosivulla. Viitattu 6.10. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dot1x.pdf

Valmet in brief. Nd. Esittely Valmet.com verkkosivulla. Viitattu 10.11.2021. https://www.valmet.com/about-us/valmet-in-brief/

Wi-Fi Channels, Frequencies, Bands & Bandwidths. Nd. Artikkeli electronics-notes.com verkkosivulla. Viitattu 10.11.2021. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php