Joose Lahtinen

Langattoman lähiverkon keskitetty hallinta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

11.5.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Joose Lahtinen Langattoman lähiverkon keskitetty hallintaan 20 sivua 11.5.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Sulautetut järjestelmät.
Ohjaaja(t)	Yliopettaja Matti Puska

Tämän insinöörityön tavoitteena oli rakentaa prototyyppi yrityksen langattoman lähiverkon keskitetystä hallinnasta. Työhön kuului langattomaan lähiverkkoon kirjautuvien ohjaaminen RADIUS-palvelimen tekemään tunnistukseen ja tällä tavoin käyttäjäkohtaisiin verkkoresurssien käyttölupien myöntämiseen.

Työ tehtiin Metropolian tiloissa ja Metropolialta lainatuilla laitteilla Metropolian tietoverkkotekniikan laboratoriossa. Työssä käytettiin verkkoinfrastruktuurina tietoverkko kurssi CCN 3:ssa tekemääni harjoitusta jonka päälle lisättiin langaton lähiverkko ohjaimen ja tukiaseman avulla. Työssä käytettiin yhtä ohjainta, yhtä tukiasemaa, yhtä reititintä, kahta kytkintä ja kahta pöytäkonetta. Langattoman verkon testilaitteina toimi matkapuhelin ja kannettava tietokone.

Työ saatiin tehtyä laitteiden iästä johtuvista ongelmista huolimatta ja työtä tehdessä tuli opittua paljon langattoman verkon ohjaimen käytöstä ja hallinnoinnista. Työn jälkeen tavoitteena on siirtää oppimani tuotantoon ja nähdä työn konkreettisesti yritysympäristössä.

Avainsanat	Wlan, ohjain, tukiasema, radius

Author(s) Title Number of Pages Date	Joose Lahtinen Centralized management of wireless local area network 20 pages 11 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Embedded Systems
Instructor(s)	Matti Puska, Principal Lecturer

The purpose of this final year project was to build a prototype of centralized control for a wireless local area network with a company's network infrastructure in mind. The work included a wireless local area network for users to authenticate with the RADIUS server to get access to network resources allocated to them.

The work was done on the premises of Metropolia University of Applied Sciences and using equipment borrowed from Metropolia in a Metropolia networking technology laboratory. The network infrastructure of this project was copied from an exercise done for a CCNA 3 network course. A wireless local area network controller and access point was added to the network infrastructure to make it operational. A controller, an access point, a router, two switches and two tabletop computers were used to create this network. The equipment that was used to test the wireless network included a mobile phone and a laptop computer.

The project could be carried out in spite of the difficulties caused by the age of the equipment. This project taught a lot about using and controlling a wireless network controller. Now that the project is finished it would be interesting to compare this process to an actual company situation and to actually see how everything works in practice.

Keywords	Wlan, controller, access point, radius

Sisällys

Lyhenteet

1 Johdanto 1

2 Langattomat lähiverkot 2

2.1 Standardit 2
2.2 Langattomien verkkojen tietoturva 4

3 Keskitetty hallinta 7

4 Työn suunnittelu ja toteutus 9

5 Työn kuvaus 14

6 Yhteenveto 20

Lähteet 21

Lyhenteet

AES	Advanced Encryption Standard. Salausmenetelmä.
AP	Access Point. Langattoman verkon tukiasema.
CAPWAP	Control And Provisioning of Wireless Access Points. Langattoman verkon kontrollerin ja tukiaseman yhteysprotokollan standardi.
CLI	Command-Line Interference. Tekstipohjainen käyttöliittymä.
FTP	File Transfer Protocol. Tiedostonsiirtomenetelmä kahden tietokoneen välillä.
GHz	Gigahertz
GUI	Graphical User Interface. Graafinen käyttöliittymä.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen standardointijärjestö.
IETF	Internet Engineering Task Force. Suuri kansainvälinen avoin yhteisö verkkostruktuurin parissa työskenteleville.
IP	Internet Protocol. Yhteysprotokolla tietokoneiden välillä.
IT	Information Technology. Tietotekniikka
LAP	Lightweight Access Point. Kevyt langattoman verkon tukiasema
LWAPP	Lightweight Access Point Protocol. Langattoman verkon tukiaseman ja ohjaimen yhteysprotokolla.
MAC	Media Access Control. Verkkosovittimen yksilöivä osoite.
Mbit/s	Megabittiä sekunnissa.

MIMO	Multiple-Input, Multiple-Output. Useamman antennin samanaikaisen käytön tekniikka.
OFDM	Orthogonal Frequency Division Multiplexing. Signaalin jakamistekniikka.
POE	Power Over Ethernet. Tekniikka jolla voidaan syöttää virtaa verkkojohtoa pitkin.
PSK	Pre-Shared Key. Langattoman verkon salausmenetelmä.
RADIUS	Remote Authentication Dial In User Service. Verkon kirjautumispalvelu.
SSID	Service Set Identifier. Langattoman verkon verkkotunnus.
USB	Universal Serial Bus. Yleinen liitin monille eri laitteille.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
WLAN	Wireless Local Area Network. Langaton lähiverkko.
WLC	Wireless Lan Controller. Langattoman verkon ohjaini.
WPA	Wi-Fi Protected Access. Salausmenetelmä langattomaan verkkoon.
QoS	Quality of Service. Tietoliikenteen priorisointimenetelmä.

1 Johdanto

Yrityksen langattomien verkkojen määrä alkoi kasvaa ja verkkojen hallintaan haluttiin parannusta. Useiden toimipisteiden ja vielä useamman langattoman verkon sijalle haluttiin parempaa langattoman verkon hallintaa ja selkeämpää verkkoon kirjautumista. Keskitetty langattoman verkon hallinta nousi ideana toimivimmaksi yrityksen tarpeisiin vastaavana teknologiana.

Tavoitteena on suunnitella ja toteuttaa prototyyppi yrityksen keskitetystä langattomasta verkosta mukailemalla tulevaa toteutusta. Nykyisestä lähiverkosta on tarkoitus siirtyä kontrolloituun langattomaan lähiverkkoon, jossa tunnistamismenetelmänä on RADIUS- (Remote Authentication Dial In User Service) palvelin. Tätä mallia on tarkoitus käyttää tulevaisuudessa yrityksen useassa eri toimipisteessä.

Verkon yleistä käyttömukavuutta pyritään parantamaan käyttämällä RADIUS-palvelinta, joka nopeuttaa ja helpottaa verkon käyttöä ja poistaa mahdollisuuden langattoman verkon salasanan hukkaamiselle tai vääriin käsiin joutumiselle.

2 Langattomat lähiverkot

Osa nykyaikaisen liikkuvan ja avoimen toimiston arkipäivää ovat langattoman lähiverkot, jotka nopeuttavat ja helpottavat tiedon hakemista verkosta. Yhteydenpito helpottuu eikä kommunikointi ole kiinni työntekijän sen hetkisestä sijainnista. Myyjä voi olla yhteydessä asiakkaaseen langattoman verkon ansiosta mistä tahansa verkon kantaman sisällä. Helppous ja liikkuvuus ovat yksi langattomien lähiverkkojen tärkeimpiä piirteitä. [1;2.]

2.1 Standardit

Käytetyimpiä standardeja langattomissa verkoissa ovat IEEE:n (Institute of Electrical and Electronics Engineers) 802.11-standardit. IEEE 802.11 -standardiperhe käsittelee langattomia verkkoja. IEEE on kansainvälinen tekniikan alan järjestö. IEEE on jakanut 802.11-standardin kehityksen työryhmille, joista jokainen keskittyy eri ominaisuuksiin standardissa. Tästä johtuen IEEE 802.11 -standardit eivät seuraa lineaarista liitekirjaimen järjestystä, esimerkiksi IEEE 802.11b tulee ennen IEEE 802.11a:ta. [3;4;5;6.]

IEEE 802.11 oli ensimmäinen WLAN-(Wireless Local Area Network) -tekniikka. IEEE esitteli jo vuonna 1990 ensimmäisen version standardista, josta kehittyi vuonna 1997 julkaistu IEEE 802.11 -standardi kuuden eri version jälkeen. Tällä standardilla verkkoyhteyden nimelliseksi nopeudeksi saatiin 1 ja 2 Mbit/s, ja verkon taajuus on 2,4 GHz. [4;5;6.]

IEEE 802.11b oli päivitys IEEE 802.11 -standardiin, joka nosti nimellisen nopeuden aina 2 Mbit/s taajuudella 2,4 GHz. Tälle oli tarvetta, koska langattomien verkkojen ja verkkosovellusten määrä kasvoi jatkuvasti, joten myös kaistaa kului enemmän. IEEE 802.11b tunnetaan myös IEEE 802.11hr nimellä. IEEE 802.11b julkaistiin vuonna 1999. [4;5;6.]

IEEE 802.11a julkaistiin vuonna 1999 ja se nosti nimellisen nopeuden 54 Mbit/s:iin taajuuksilla 5,150–5,350 ja 5,475–5,725 GHz, mutta ei ollut yhteensopiva IEEE 802.11b:n kanssa. Nopeutta saatiin nostettua nostamalla taajuutta ja käyttämällä OFDM-(Orthogonal Frequency Division Multiplexing) tekniikkaa, joka hajottaa signaalin pienempiin osiin jonka jälkeen se lähetetään eri taajuuksilla ja vastaanottaja kasaa signaalin taas

alkuperäisen kokoiseksi signaaliksi. IEEE 802.11a ei saanut suurta suosiota Euroopassa, koska tämä tekniikka olisi vaatinut kalliita yhteyslaitteita. Nopeuden hintana oli lyhempi kantomatka langattomalle verkolle, korkeampien taajuuksien vuoksi. [4;5;6.]

IEEE 802.11g -standardi julkaistiin vuonna 2003 ja se on käytännössä syrjäyttänyt IEEE 802.11b -standardin. IEEE 802.11g kykenee 54 Mbit/s:n nopeuteen taajuudella 2,4 GHz IEEE 802.11b:n tavoin ja on myös yhteensopiva IEEE 802.11b:n kanssa, toisin kuin IEEE 802.11a. IEEE 802.11g käyttää OFDM-tekniikkaa nostamaan nopeutta. Vaikka IEEE 802.11g on yhteensopiva IEEE 802.11b:n ja IEEE 802.11a:n kanssa, se ei vaikuta vanhempaa standardia käyttävän laitteen nopeuteen. Vanhempaa standardia käyttävä laite, joka toimii IEEE 802.11g:n kanssa, toimii vanhan standardin maksiminopeudella. [4;5;6.]

IEEE 802.11e laajennus tuli vuonna 2005 joka parantaa QoS (Quality of Service) -palvelua IEEE 802.11-standardiperheessä. Verkossa tapahtuu yhteentörmäyksiä jatkuvasti kun laitteet koittavat kommunikoida ja yrittävät lähettävää viestejä samaan aikaan. QoS-palvelu priorisoi viestejä sovelluksen QoS numeron perusteella ja nopeuttaa korkeamman prioriteetin omaavan sovelluksen viestin kulkemista vähentämällä kyseisen sovelluksen uudelleenlähetys aikaväliä. [4;5;6.]

IEEE 802.11F -laajennus paransi IEEE 802.11 -standardin toimivuutta eri valmistajien tukiasemien välisessä kommunikaatiossa. IEEE 802.11F -laajennus julkaistiin vuonna 2003, mutta poistettiin käytöstä 2006. [4;5;6.]

IEEE 802.11d -laajennus lisäsi levitysviesteihin tiedon missä laite kulloinkin sijaitsi, jotta langaton laite osaa itse valita taajuusalueen millä toimia. Eri maissa käytetään eri taajuusalueita, joten tämä on erittäin käytännöllinen lisä paljon matkustaville.

IEEE 802.11h -laajennus muokkasi 5 GHz taajuusaluetta. Euroopassa 5 GHz taajuus oli varattu muun muassa satelliittiliikenteelle. Lisäksi IEEE 802.11h -laajennus toi tuen älykkäälle taajuusalueen vaihtamiselle ja langattomien laitteiden virrankulutuksen vähentämiselle. [4;6;7;8.]

IEEE 802.11i -laajennus parantaa tietoturvaa IEEE 802.11:n lisäämällä siihen WPA2 (Wi-Fi Protected Access) -salausmenetelmän ja määrittelee sen osaksi standardia. IEEE

802.11i lisäsi vielä täysin uudenlaisen salausmekanismin AES (Advanced Encryption Standard), joka mahdollistaa eripituisten salasana -avaimien käytön. [4;5;6.]

IEEE 802.11n -laajennus mahdollistaa suurimmaksi nimelliseksi nopeudeksi aina 600 Mbit/s. IEEE 802.11n käyttää MIMO (Multiple-Input, Multiple-Output) -tekniikkaa, joka mahdollistaa useamman antennin ja taajuuden käytön samaan aikaan. MIMO mahdollistaa huomattavan nopeuden nousun aikaisempiin standardeihin nähden. IEEE 802.11n -laajennus on yhteensopiva aiempiin standardeihin, kuten IEEE 802.11a:n ja IEEE 802.11g:n kanssa, kyeten käyttämään molempien taajuuksia. IEEE 802.11n kykenee nopeaan yhteysnopeuksiin, mutta keskustellessaan vanhemman standardin kanssa n laajennus toimii hitaamman standardin nopeudella.[4,5,6.]

IEEE 802.1X on tietoturvastandardi koko IEEE 802 -standardi perheelle. IEEE 802.1X on porttikohtainen tunnistaminen, eli esimerkiksi kytkimen porttiin kiinnitettyjen käyttäjien todentaminen. Langattomassa verkossa ei luonnillisestikaan ole kiinteitä portteja joten ne luodaan virtuaalisesti laitteen MAC-(Media Access Control) osoitteen perusteella. Tämän jälkeen IEEE 802.1X todentaa käyttäjän RADIUS-(Remote Authentication Dial In User Service) palvelimen kanssa. IEEE 802.1X:n tarkoituksena on estää luvattomia asiakaslaitteita kommunikoimasta lähiverkossa. [9.]

2.2 Langattomien verkkojen tietoturva

Langattomien verkkojen helppous on myös yksi langattomien verkkojen heikkous tietoturvan näkökulmasta. Mitä helpompi käyttää, sitä helpompi väärinkäyttää. Yritysten tietoturva ja helppokäyttöisyys ovat jatkuvassa kädenväännössä. Langattomissa lähiverkoissa jokaiseen verkkoon on yleensä yksi yhteinen salasanaan perustuva tunnistautuminen, joka antaa pääsyn haluttuun verkkoon. Langattoman verkon SSID:n (Service Set Identifier) nimen mukaan käyttäjälle on annettu pääsy kohteisiin, jotka ovat samat kaikille kyseisen lähiverkon käyttäjille. RADIUS-palvelin toimii yhden SSID -nimen alla, jonka jälkeen käyttäjät ohjataan oman käyttäjäryhmän tai käyttäjän henkilökohtaisten asetusten perusteella omiin lähiverkkoihin, joissa heillä on heidän ryhmänsä tai henkilökohtaisten asetustensa mukaan annetut oikeudet. [10;11.]

Salaus

Langattomassa verkossa tapahtuvassa liikenteessä on useampia mahdollisia salausmenetelmiä. Kotikäytössä yleisimpiä ovat nykyään WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key) ja yrityskäytössä WPA2 (Wi-Fi Protected Access). Yrityksen näkökulmasta salasanoihin perustuva yhdistäminen langattomaan verkkoon on isompi riski kuin kotikäytössä tai pienessä yrityksessä. Jokainen käyttäjä tarvitsee salasanan langattomaan lähiverkkoon. Ensimmäinen ongelma on, jos yrityksessä on monta verkkoa. Esimerkiksi, uuden työntekijän pitää tietää mihin verkkoon yrittää liittyä. Toinen ongelma on se että jokaisen työntekijän pitää tietää salasana kyseiseen verkkoon. Se mihin verkkoon liittyy, on pieni haitta uuden työntekijän arjessa.

Se, että jokainen työntekijä tietää salasanan vähintään yhteen langattomaan verkkoon, tuo ison riskin yrityksen verkon tietoturvalle. Yleensä langattoman verkon salasana tarvitsee asettaa kerran, jonka jälkeen käytettävä kone muistaa salasanan. Tämä on samalla sekä hyvä että huono asia. Jos kaikki menee hyvin, käyttäjän tarvitsee kerran kirjoittaa salasana, ja tämä toimii langattoman laitteen elinkaaren loppuun asti. Jos asiat eivät mene hyvin, joutuu käyttäjä kirjautumaan useamman kerran samaan verkkoon, joten verkon salasana pitää muistaa. Jokaisen työntekijän pitää siis muistaa salasana omaan verkkoonsa. Tämä luo tilanteen, jossa salasanat joko kirjoitetaan muistiin tai ne ovat niin helppoja, että ne muistetaan. Kumpikin ratkaisu on erittäin huono tietoturvallisesta näkökulmasta. [10;11;12.]

RADIUS-palvelin

RADIUS-palvelin on omiaan yrityksen langattoman verkon salasanan julkisen leviämisen estoon. RADIUS-palvelin jakaa käyttäjälle oikeuden verkkoon perustuen käyttäjän laitteen kirjautumistietoihin, jolloin käyttäjä ei tarvitse salasanaa verkkoon kirjautumiseen. RADIUS-palvelin tunnistaa käyttäjän rekisteriin kirjoitettujen käyttäjätunnusten perusteella ja osaa jakaa tunnistetulle käyttäjälle oikeat resurssit verkkoon joko käyttäjäkohtaisesti tai ryhmäkäytännön (Group policy) mukaan. Silloin useampi käyttäjä voi saada samat oikeudet verkkoon, joka on isoissa yrityksissä huomattavasti tehokkaampi tapa hallita yrityksen työntekijöiden verkkoresurssien käyttöä. RADIUS ei poista mahdollisuutta verkon väärinkäyttöön ja tietomurtoihin, koska käyttäjien pitää edelleen kirjautua omaan langattomaan laitteeseen, jolloin salasanan muistiin kirjoittaminen tulee jälleen

esille. Koska ihmiset yleensä käyttävät omissa laitteissaan salasanoja, jotka he muistavat, tämä ei ole niin suuri riski kuin se, että laitetaan yrityksen seinälle lappu, missä on salasana langattomaan verkkoon. [13;14;15.]

3 Keskitetty hallinta

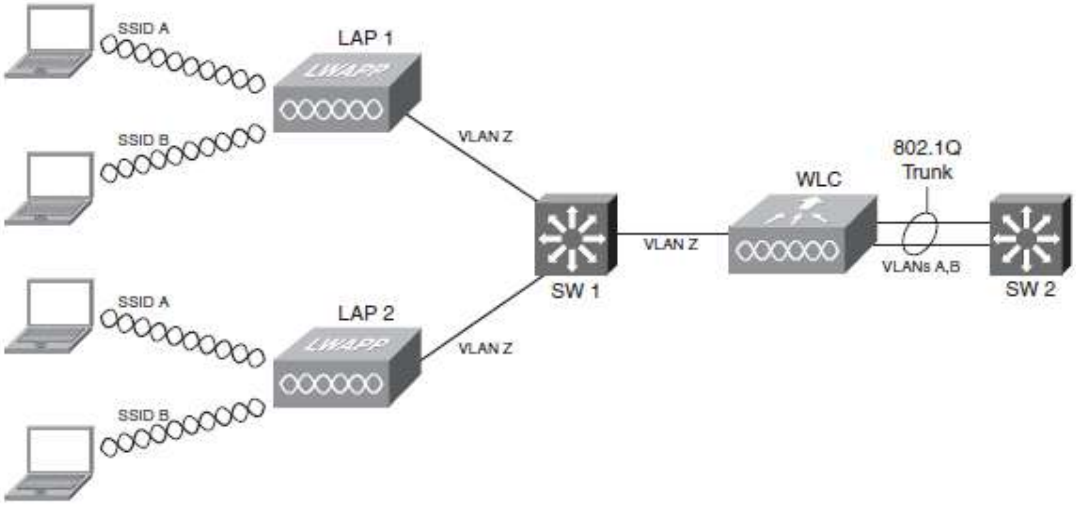
Tämän luvun tarkoitus on avata keskitetyn hallinnan tarkoitusta ja kertoa oleellisista protokollista.

Hallinnan idea

Pienen yrityksen langattoman verkon hallintaan saattaa riittää yksi langattoman verkon tukiasema, jonka kattavuus riittää pienen yrityksen tiloihin. Yhden tukiaseman asetusten määritteleminen ja ylläpito eivät vaadi yritykseltä suuria resursseja. Muutaman tukiaseman verkossa yhtenäisten asetusten määritteleminen on vielä mahdollista ja järkevää hoitaa tukiasemakohtaisesti.

Kun yritys kasvaa useampaan kuin yhteen toimitilaan, tai toimitila on isompi kuin mitä muutaman tukiaseman verkko kattaa, alkaa olla edullisempaa siirtyä käyttämään keskitettyä hallintaa langattoman verkon ylläpitämiseksi. Keskitetyssä hallinnassa kaikki tukiasemat menettävät itsemääräämisoikeutensa ja niiden kaikki päätökset tehdään yleensä yhden ohjaimen kautta, kuten kuvassa 1 on esitetty. Tämä helpottaa koko langattoman verkon asetusten määrittelemistä ja hallintaa. Tämä mahdollistaa myös tukiasemaverkon laajentamisen huomattavasti tehokkaammin, kuin yksittäisten tukiasemien lisäämisen. Lisäksi ne vielä säädettäisiin erikseen kohteen tarpeiden mukaan.

Keskitetyn hallinnan suurimpia ongelmia on ohjaimen valinta ja hinta. Pienemmälle yritykselle hinta saattaa olla este. Langattoman verkon haluttu ja tarvittu koko sanelevat, kuinka montaa tukiasemaa ohjaimen on kyettävä hallinnoimaan, mikä vaikuttaa siihen, minkälaisen ohjaimen yritys hankkii. Ohjaimia voi myös ketjuttaa, jolloin toinen ohjaini muuttuu orja-asemaksi ja jakaa ainoastaan pääohjaimen antamia käskyjä oman alueensa langattomille tukiasemille. Tämä voi olla kätevää yrityksen laajentaessa toimintaa. Näin säästyy myös vaiva uuden ohjaimen asentamisesta. Ohjaimessa on myös raportointi- ja analyysityökalut verkon eheyden seuraamista varten, joten yksittäisen AP:n (Access Point) tilan voi tarkistaa pääohjaimen tiedoista.



Kuva 1. Langattoman verkon ja kontrollerin kuvaus.[16.]

LWAPP-protokolla

LWAPP - (Lightweight Access Point Protocol) on protokolla, jolla ohjain hallitsee langattomia tukiasemia. Siihen rakennetun hallintaympäristön lisäksi langattoman verkon kunnon tarkkailemiseen on tehty analyysityökalu. LWAPP on Airespace -yrityksen lanseeraama protokolla langattomien verkkojen hallintaan. LWAPP on jäänyt Airespace ja Cis-con pääsääntöiseen käyttöön.[17.]

CAPWAP-protokolla standardi

CAPWAP - (Control And Provisioning of Wireless Access Points) -protokolla on IETF:n (Internet Engineering Task Force) standardoima. CAPWAP on LWAPP:n pohjalta kehitetty protokollastandardi, joka antaa mahdollisuuden kontrolloida langattomia verkkoja useamman valmistajan verkkolaitekokoonpanolla. Tämä helpottaa siirtymistä langattomaan ja kontrolloituun lähiverkkojen hallintaan. Silloin ei tarvitse ostaa koko pakettia kerralla, vaan kaikki valmiiksi hankitut laitteet toimivat uudessa kontrolloidussa lähiverkossa. CAPWAP on sidottu IEEE 802.11 -standardiin joten se toimii kaikissa laitteissa, jotka käyttävät IEEE 802.11 -standardiperhettä.[18.]

4 Työn suunnittelu ja toteutus

Työn tavoitteena oli tehdä prototyyppi yrityksen langattoman verkon vaihtamisesta kontrolloituun langattomaan verkkoon. Yrityksessä on useita eri SSID tunnuksia ja useita toimipisteitä. Keskitetyllä kontrolloinnilla haluttiin tehostaa langattoman verkon ylläpitoa ja työntekijöiden toimipisteiden välisen liikkuvuuden helpottamista. Kontrollointi selkeyttää langattomaan verkkoon liittymistä ja käyttäjien verkko oikeuksien kontrollointia.

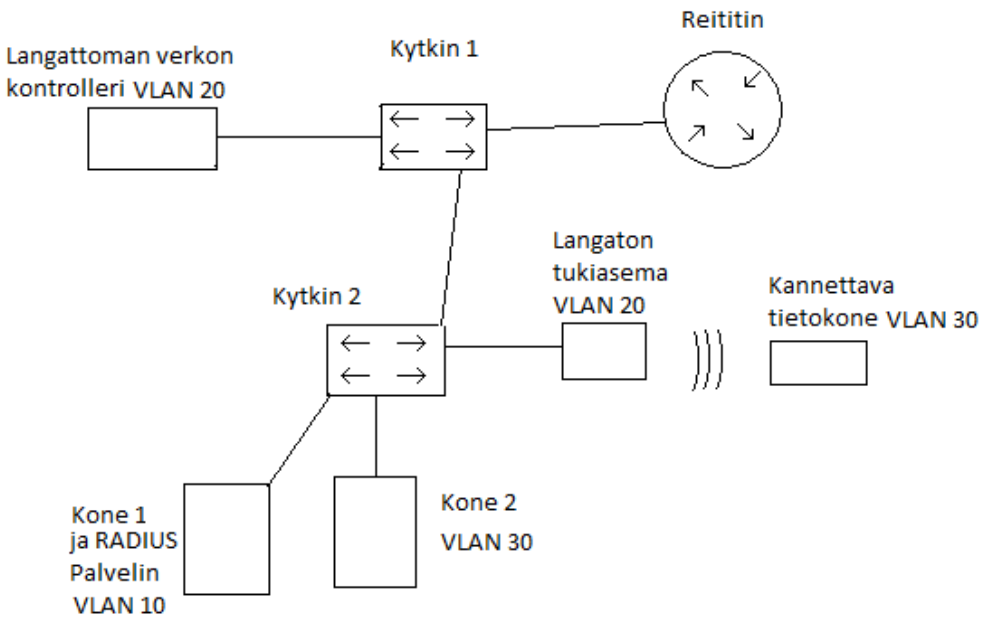
Verkkotopologia

Käytin prototyyppiverkon suunnittelussa hyödyksi virtuaalisia lähiverkkoja käsitellyllä CCNA (Cisco Certified Network Associate) 3 -kurssilla harjoituksena tekemääni valmista verkkoa. Harjoituksessa tekemäni verkko sisälsi muutaman virtuaalisen lähiverkon ja oli toiminnaltaan sopiva prototyypin rakentamiseen. Koska työn pääpiirteet olivat ohjaimen lisääminen lähiverkkoon ja langattoman tukiaseman yhdistäminen ohjaimeen virtuaalisessa lähiverkossa, tämän valmiin harjoituksen käyttäminen nopeutti itse työtä ja antoi valmiin verkkotopologian käytettäväksi. Topologiaa on esitetty kuvassa 2.

Valmiin harjoituksen valitseminen työn perusverkoksi myös selvensi ja helpotti työn toteuttamista. Virtuaaliset lähiverkot ovat oleellinen osa verkon jakamista osiin ja näin käyttäjien ohjaamista verkossa. Virtuaalinen lähiverkko voidaan määritellä sallimaan vain tietyt koneet näkemään toisensa välittämättä siitä, että ne kaikki ovat kytkettynä samaan verkkoon fyysisesti. Tämä ei estä koneita keskustelemasta keskenään. Käyttämässäni harjoituksessa on neljä virtuaalista lähiverkkoa: VLAN 10 (Virtual Local Area Network), VLAN 20, VLAN 30 ja VLAN 99. VLAN 10 oli vain yhdessä koneessa. VLAN 20 oli ohjaimen ja tukiasemien oma VLAN. VLAN 30 oli tarkoitettu langattomien laitteiden verkoksi. VLAN 99 on tässä työssä hallintaverkko joka on tarkoitettu verkon ylläpitäjille.

Virtuaalisen verkon numerolla ei ole väliä. Reitittimen tarkoitus verkossa on jakaa virtuaaliset lähiverkot, ja se toimii näiden verkkojen yhteyspisteenä, jolloin koneet voivat keskustella keskenään. Virtuaalisien lähiverkkojen toteuttaminen näin pieneen projektiin ei vaatinut kovin isoa miettimistä, mutta yritysverkossa, jossa käyttäjiä ja tarpeita on huomattavasti enemmän, virtuaalisten verkkojen numerointi ja jakaminen pitää miettiä huomattavasti tarkemmin. Verkot kannattaa nimetä ja niiden numerot miettiä loogisesti, jotta

uusien ihmisten lisääminen tiettyyn virtuaaliseen verkkoon ei vaadi koko verkon läpikäymistä.



Kuva 2. Työn verkkotopologia.

Laitteisto

Työ tehtiin Cisco 2106 -ohjaimen ja langattoman verkon tukiasemalla Cisco 3502. Sain kyseiset laitteet lainaksi Metropolialta. Ohjain on vanhempaa sarjaa, ja se piti päivittää uudempaan ohjelmistoversioon, jotta se toimisi Cisco 3502 -sarjan tukiaseman kanssa. Lisäksi kytkiminä toimivat Cisco Catalyst 2960 -sarjan kytkimet. Reitittimenä toimi Cisco 2911 -sarjan reititin. Kaksi pöytäkonetta toimi päätelaitteina runkoverkolle, ja toinen laitteista toimi myös RADIUS palvelimena. Kaikki laitteet olivat koululta lainassa tai luokassa valmiiksi. Työssä en olisi tarvinnut kuin yhden pöytäkoneen, mutta käytin toista konetta verkkoinfrastruktuurin toimimisen testaamistyökaluna.

Cisco 2106 -ohjain

Cisco 2106 -ohjain kykenee hallinnoimaan kuutta langatonta tukiasemaa samaan aikaan. Cisco 2106 -ohjaimessa on kahdeksan verkkoliitäntää, joista kaksi on POE (Power Over Ethernet) -liitäntöjä (kuva 3). Laitteessa on myös yksi konsoliporttiliitäntä, jonka avulla voi käyttää laitetta CLI:n (Command-Line Interference) kautta. Laitteessa on myös kolme USB (Universal Serial Bus) –liitäntää, joissa ei ole mitään toiminnollisuutta.

Laitetta voi hallinnoida CLI:n avulla tai web-selaimella graafisesti, kunhan on ensin tehnyt esiasetukset tekstipohjaisella käyttöliittymällä CLI:n kautta. Työn kannalta oleellisia liitäntöjä olivat verkkoliitäntä portissa 1 ja konsoliporttiliitäntä. Laite tukee seuraavia langattomia IEEE standardeja: 802.11a, 802.11b, 802.11g, 802.11d, 802.11h ja 802.11n.

Yrityksen kannalta ohjaimen valintaan vaikuttaa hinta. Tietenkin hintaan vaikuttaa se, kuinka monta tukiasemaa ohjaimen pitää kyetä hallinnoimaan ja kuinka monta ohjainta tulee samaan verkkoon. Samoin pitää huomioida yrityksessä jo olevat tukiasemat ja niiden yhteensopivuus valittavan ohjaimen kanssa. Erityisesti vanhemmat laitteet joudutaan ehkä uusimaan, jos valittu tukiasema ei ole yhteensopiva niiden kanssa. [19.]

Kuva 3. Kontrolleri takaa kuvattuna ja kontrollerin liittimet.

langattoman verkon tukiasema Cisco 3502

Cisco 3502 Aero LAP (Lightweight Access Point) on langattoman verkon tukiasema jonka sain lainaksi Metropolialta. Laite on uudempi kuin ohjain, jonka vuoksi ohjaimen ohjelmisto piti päivittää. Laite tukee Ciscon käyttämää LWAPP (Lightweight Access Point Protocol) -protokollaa ja uudempaa CAPWAP:a (Control And Provisioning of Wireless Access Points). LWAPP on työn kannalta tärkeämpi ohjaimen iästä ja ohjelmistosta johtuen. Laitteessa on vain muutama liitäntä, yksi verkkoliitäntä ja yksi konsoliportti, kuten kuvassa 4. Laite tukee POE kytkentää, joten se vaatii vain verkkoliitännän ja POE -liitännän kontrollerilta.

Työssä käytin verkkovirtaa langattomassa tukiasemassa. Langattoman tukiaseman ja kontrollerin ikäeron vuoksi langattomalle tukiasemalle piti kertoa ohjaimen AP -ohjausportin IP (Internet Protocol) -osoitteella. Tämän jälkeen langaton tukiasema sai yhteyden ohjaimeen ja sai toimintaohjeet ohjaimelta. Laite tukee seuraavia langattomia IEEE standardeja: 802.11b, 802.11a, 802.11g, 802.11n, 802.11h and 802.11d. [20.]

Kuva 4. Tukiaseman liittimet.

Cisco Catalyst 2960 -kytkimet

Ciscon Catalyst 2960 -sarjan tason kaksi kytkimet olivat keskeisiä työn runkoverkon kannalta. Kytkimet tukevat virtuaalisia lähiverkkoja, mitkä on oleellinen osa langattoman verkon toimintaa. Kytkimiä ohjattiin CLI -yhteydellä ja niihin määritettiin runkoverkon toiminnallisuus virtuaalisten lähiverkkojen kanssa. Käytössäni oli 24 -porttiset kytkimet. En olisi tarvinnut näin montaa paikkaa prototyypin pienen koon vuoksi, mutta ne olivat valmiiksi paikallaan ja toimivia. Yrityksessä kytkimet ovat yleensä valmiina ja riippuen niiden iästä saatetaan joutua uusimaan, jos ne eivät tue virtuaalisia lähiverkkoja.

Cisco 2911 -reititin

Cisco 2911 -reititti virtuaaliset lähiverkot ja yhdisti verkon topologian toimivaksi kokonaisuudeksi. Reititin on myös keskeinen osa runkoverkon toimivuutta. Reitittimen vaatimukset prototyypissä oli toimia virtuaalisten lähiverkkojen yhteyspisteenä ja reitittää verkon sisäinen liikenne.

RADIUS-palvelin

RADIUS-palvelimena toimi WinRadius -niminen ohjelma. Ohjelma on aika yksinkertainen ja helppokäyttöinen, koulun versio oli 1.04. Nykyinen jaossa oleva versio on 3.00. Käytin kyseistä RADIUS-palvelinta prototyypissä sen vuoksi, että se oli valmiiksi koulun koneissa asennettuna. Ohjelma toimi ja tämän vuoksi en nähnyt syytä asentaa uutta versiota. RADIUS-palvelimia on internetissä useampia erilaisia, osa ilmaisia ja osa maksullisia. Yrityksen kannalta valintaan vaikuttaa ohjelman tai palvelimen tuki, hinta ja sopivuus yrityksen tarpeisiin.

5 Työn kuvaus

Yrityksen uuden toimistokokoonpanon myötä tuli tarvetta uudelleen organisoida lähiverkot. Langattomat lähiverkot haluttiin keskittää yhden ohjaimen alle, jotta usean eri toimipisteen langattomia verkkoja olisi helpompi hallita. Ensimmäisenä täytyi laatia määrittelyt ja suunnitelmat, jotka yritys hyväksyi.

Alkuasetelmat

Prototyyppi tehtiin Metropolian tiloissa tietoverkkotekniikan laboratoriossa Leppävaarassa. Työ oli alun perin tarkoitus tehdä yrityksen tiloissa, jolloin kaikki laitteet ja palvelimet olisivat olleet saman tien verkossa ja toimintakunnossa. Koulussa tehdessä ongelmana oli valmiin infrastruktuurin puute. Tämän takia kaikki verkon toimintaan liittyvät ratkaisut täytyi tuottaa joko virtuaalisesti tai jollain muulla tapaa, mikä ei vastaa oikeata yrityksen infrastruktuuria. Tämä ei ole huono asia oppimisen kannalta, mutta ei todennäköisesti vastaa oikeata yritysverkkoa, jolloin työn tekeminen oikean yrityselämän tuotantokuvioiden oppimiseksi ei toteutunut.

Työn eteneminen

Alkuun suunnitelma eteni hyvin, alustava määritelmä ja rajaus tehtiin. Tämän jälkeen mitään ei tapahtunut yrityksen puolelta. Tilanne jatkui muutamia viikkoja, joten työ päätettiin tehdä koulun puolella ja koulun laitteilla. Tällä menetelmällä opin langattoman ohjaimen käytön ja sen miten se liitetään tukiasemiin ja verkkoon. Koululta sai lainaksi ohjaimen ja tukiaseman. Työn tekeminen alkoi määrittelemällä lähiverkko, jonka tarkoituksena oli olla prototyyppinen pieni lähiverkko, jossa langaton kontrolleri ja tukiasema toimisivat osana muuta verkkoa. Valitsin verkkotopologiaksi harjoituksena tekemäni verkkotopologian. Kyseisessä harjoituksessa oli kaikki tarvittava toiminnallisuus prototyypin tekemisen kannalta ja jo tehtynä sen päälle rakentaminen oli tehokkaampaa kuin uuden suunnittelu.

Lähiverkon suunnittelu

Koulun tiloissa oli mahdollista tehdä verkkoympäristö, johon kuuluu yksi reititin, kaksi kytkintä, yksi ohjain ja yksi tukiasema. Nämä laitteet riittivät hyvin prototyyppisen verkkoratkaisun rakentamiseen. Lähiverkkoon täytyi lisätä vielä kaksi tietokonetta verkon testausta varten, joista toinen toimi myös RADIUS-palvelimena.

Ohjaimen liittäminen lähiverkkoon

Ohjaimen verkkoon lisääminen sujui vaivatta ja graafisen käyttöliittymän kautta asetusten muuttaminen ja hallinnointi oli selkeämpää kuin etäyhteyden tekstipohjaisella käyttöjärjestelmällä.

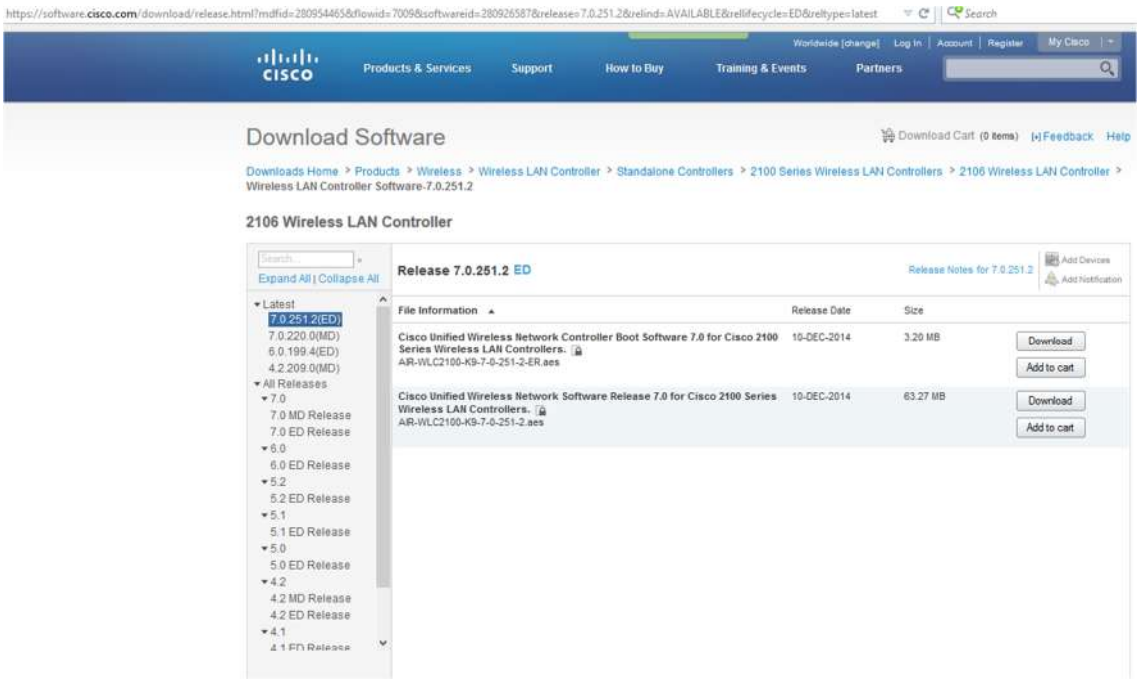
Ohjaimen liittäminen verkkoon tapahtui vasta, kun muu verkkoinfrastruktuuri oli toimintakunnossa. Ohjain täytyi liittää myös konsoliportilla tietokoneeseen, ja alkukonfiguraatio tapahtui CLI -yhteydellä. Laite tarvitsee alustaa useammalla alkuasetuksella, jotta se toimisi oikein. Yksi tärkeimmistä on Management Interface IP Address (hallinta ympäristön IP osoite), joka mahdollistaa GUI:n käytön.

Alkukonfiguraatiossa annetaan ohjaimelle myös ohjaimen management IP:n käyttämä virtuaalinen lähiverkko. Tämä mahdollistaa Management IP -osoitteen sijoittamisen niin, että siihen pääsevät käsiksi vain IT(Information Technology) -tukihenkilöt. Tämä toiminnallisuus lisää langattoman lähiverkon ohjaimen tietoturvaa ja vähentää mahdollisuutta, että muut kuin hallintaverkkoon oikeutetut ihmiset voisivat muutta langattoman lähiverkon asetuksia.

Toinen tärkeä asetus joka alkuasetuksia tehdessä kysytään, on AP Management interface IP A address. Osoite on tarkoitettu IP -osoitteeksi johon langattomat tukiasemat ottavat yhteyttä kommunikoidakseen ohjaimen kanssa. Alkuasetuksissa voi myös antaa RADIUS-palvelimen IP -osoitteen, mutta tämän voi kyllä myöhemminkin lisätä tai vaihtaa graafisesta käyttöliittymästä. Alkukonfiguraatiossa pystyi myös määrittelemään virtuaalisen yhdyskäytävän ja ryhmänimen usean ohjaimen sisäisen keskusteluverkon määrittelemiseksi. Määrittelemällä yhdyskäytävän ja ryhmän nimen voidaan määritellä, mitkä oh-

jaimet toimivat keskenään, joten useampi ohjainryhmä voi toimia samassa verkkoinfrassa. Tämä ominaisuus ja sen tuoman mahdollisuudet tulevat olemaan tärkeä osa yrityksen langattoman verkon hallintaa.

Ohjaimessa oli aluksi ongelmia ohjelmistoversion kanssa. Laitteessa ollut ohjelmistoversio ei ollut yhteensopiva Cisco 3500 sarjan AP:n kanssa. Tämä selvisi vasta useamman yrityksen jälkeen. Laitteen ohjelmiston päivitys tapahtui lataamalla uusi ohjelmistoversio Ciscon sivuilta. Kuvan 5 näkymästä sai ladattua tarvittavan ohjelmapäivityksen.



Kuva 5. Ciscon ohjelmistopäivityksen lataussivu.

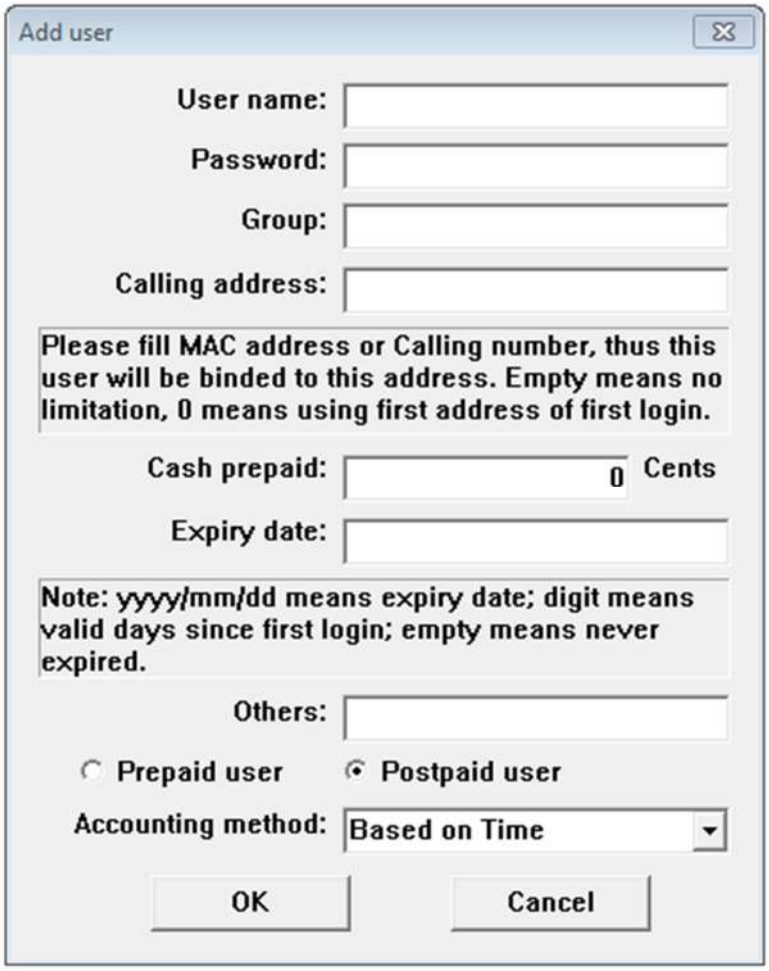
Päivitys vaatii Ciscon käyttäjätunnuksen ja voimassa olevan palvelusopimuksen. Tämä järjestyi koulun puolelta. Tiedoston lataamisen jälkeen se laitetaan koneelle, joka on samassa verkossa kontrollerin kanssa ja koneeseen asennetaan FTP(File Transfer Protocol) -palvelin, FTP -palvelimena toimi koulun koneessa jo olevaa Filezilla -niminen ilmaisohjelma.

Langattoman tukiaseman liittäminen lähiverkkoon ja ohjaimeen

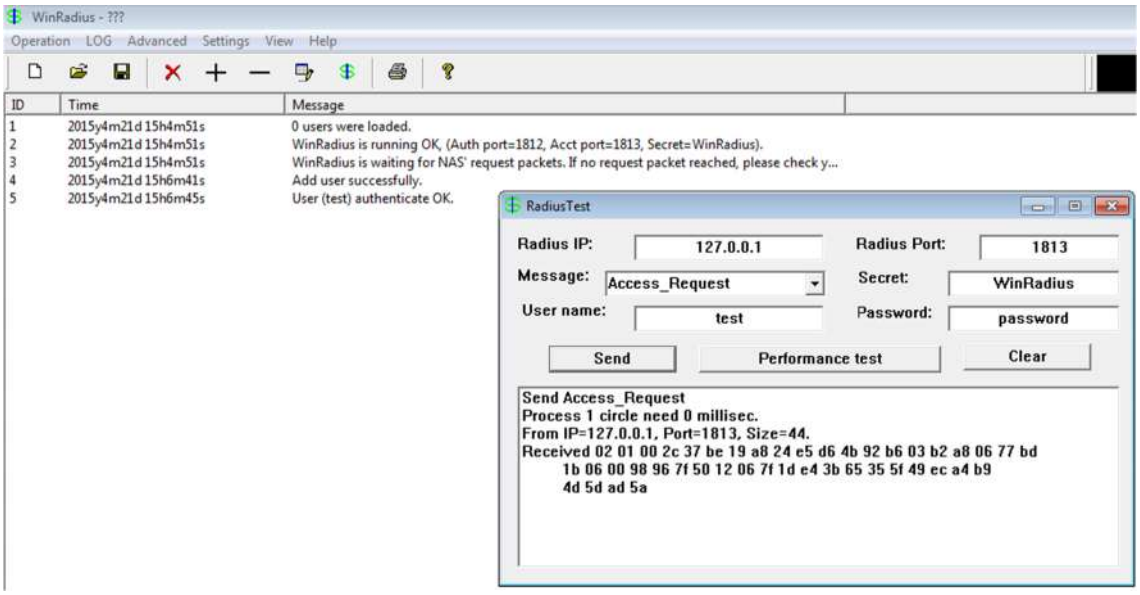
Langaton tukiasema liitettiin lähiverkkoon ja sille annettiin CLI:in kautta ohjaimen AP management interfacen IP (AP:n hallinnointi IP) -osoite, jotta se osasi löytää ohjaimen verkosta. Tämän jälkeen laite pyysi ohjaimelta uudet ohjeistukset toimintaansa, jonka jälkeen laite toimi ohjaimen ohjeiden mukaisesti. Muuta asennusta ei tarvitse tehdä.

RADIUS-palvelimen asettaminen

RADIUS-palvelimena toimi WinRadius -niminen ilmaisohjelma, joka oli valmiina Metropolian Ciscon laboratorion koneisiin asennettuna. Ohjelma oli helppokäyttöinen ja toimi hyvin. Ensin täytyi lisätä testikäyttäjä; kuvan 6 näkymässä on käyttäjän lisäämisikkuna. Testaus tapahtui WinRadius -ohjelman mukana tulevalla Radius test -ohjelmalla. Kuvassa 7 näkyy testiohjelman ajaminen testitunnuksen avulla. Tämän toiminnan jälkeen pystyi kokeilemaan kirjautumista langattomaan verkkoon kannettavalla tietokoneella ja matkapuhelimella.



Kuva 6. Käyttäjän lisääminen WinRadius ohjelmaan.



Kuva 7. WinRadius testiohjelma.

Kannettavan tietokoneen ja matkapuhelimen liittäminen langattomaan lähiverkkoon onnistui mainiosti RADIUS-palvelimen kanssa ja ilman. Lisäsin RADIUS-palvelimeen kannettavan tietokoneen ja matkapuhelimen käyttäjätunnukset ja liityin langattomaan verkkoon. Tämän jälkeen pystyin toimimaan verkossa kummallakin laitteella.

6 Yhteenveto

Työn tavoitteena oli tehdä prototyyppinen verkko, johon liitetään ohjain ja tukiasema jota ohjain hallitsee. Lisäksi verkkoon tuli liittää RADIUS -palvelin ja saada palvelimen kautta tunnistettua käyttäjä ja antaa käyttäjälle oikeudet verkon käyttöön.

Työn piti olla opettavainen kokemus ja apua piti saada tarvittaessa. Työ osoittautui haastavaksi tehdä itsekseen vähäisen verkkopuolen osaamisen vuoksi. Monia ongelmia joutui tutkimaan ja yksinkertaisiakin vastauksia hakemaan ja selvittelemään turhan kauan. Työssä riitti haasteita aina tekopaikasta laitteisiin asti. Lopulta haasteet voitettiin ja työ saatiin tehtyä. Verkkopuolen hallinta vaatii paljon rutiininomaista tekemistä ja asioiden tutkimista ja selvittelyä. Virhetilanteiden tapahtuessa vian löytäminen on yleensä vaikein haaste. Työn tekeminen olisi ollut mieluisampaa yrityksen tiloissa ja yrityksen laitteilla. Siellä olisi infrastruktuuri ollut valmiina eikä työtä olisi tarvinnut joka kerta aloittaa alusta koulun laitteiden tyhjentäessä asetukset virran sammuttamisen yhteydessä.

Työssä tekemäni verkko toimi hyvin, ja sain liitettyä siihen ohjaimen, jonka jälkeen myös langattoman verkon tukiasema ja langattomat laitteet löysi ja pääsi verkkoon. Työssä käytin yhden valmistajan laitteita; olisi ollut mielenkiintoista nähdä ja kokeilla eri laitevalmistajien laitteiden toimivuutta keskenään. Samoin useamman RADIUS-palvelimen käyttö olisi ollut hyödyllistä tulevaisuutta ajatellen.

Työn loppuun vieminen oli positiivinen kokemus. Oikean yrityksen siirtämistä langattoman verkon hallintaan on huomattavasti helpompi lähteä toteuttamaan tämän prototyypin tekemisen jälkeen. Opinnäytetyön jälkeen toivon, että pääsen toteuttamaan yrityksen langattomien verkkojen siirtämistä keskitettyyn langattomien verkkojen hallintaan, jotta näkisin työni konkreettisia tuloksia yritysympäristössä.

Lähteet

[1] Wlan 2015. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/WLAN. Luettu 25.2.2015

[2] Langattomat verkot Suomessa.Wikipedia. 2015. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/Langattomat_verkot_Suomessa Luettu 25.2.2015

[3] IEEE kotisivu.2015. Verkkodokumentti. IEEE. http://www.ieee.org/index.html?WT.mc_id=hpf_logo Luettu 25.2.2015

[4] IEEE_802.11. 2015. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/IEEE_802.11 Luettu 25.2.2015

[5] IEEE 802.11 standards tutorial. 2015. Verkkodokumentti. Ian Poole. http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php Luettu 25.2.2015

[6] IEEE 802.11. 2015. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/IEEE_802.11 Luettu 25.2.2015

[7] IEEE 802.11d. 2015. Verkkodokumentti. Cory Janssen. http://www.techopedia.com/definition/16646/ieee-80211d Luettu 25.2.2015

[8] IEEE 802.11h. 2015. Verkkodokumentti. Cory Janssen. http://www.techopedia.com/definition/15786/ieee-80211h Luettu25.2.2015

[9] IEEE 802.1X. 2015. Verkkodokumentti. Cory Janssen. http://www.techopedia.com/definition/509/ieee-8021x Luettu 25.2.2015

[10] Langaton lähiverkko – enemmän kuin silmä näkee. 2015. Verkkodokumentti. Viestintävirasto. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409021705.html Luettu 5.3.2015

[11] Määritä langattoman verkon suojausavain. 2015. Verkkodokumentti. Microsoft. http://windows.microsoft.com/fi-fi/windows/set-security-key-wireless-network#1TC=windows-7 Luettu 3.3.2015

[12] Security. 2015. Verkkodokumentti. Wi-fi.org. http://www.wi-fi.org/discover-wi-fi/security Luettu 3.3.2015

[13] RADIUS Server. 2015. Verkkodokumentti. Microsoft. https://msdn.microsoft.com/en-us/library/cc755248.aspx Luettu 4.3.2015

[14] How Does RADIUS Work? 2015. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html Luettu 4.3.2015

[15] Remote Authentication Dial In User Service (RADIUS). 2015. Verkkodokumentti. IETF. https://tools.ietf.org/html/rfc2865 Luettu 4.3.2015

[16] LAP-WLC connection. 2015. Verkkodokumentti. Julián. https://learningnetwork.cisco.com/thread/50678 Luettu 4.3.2015

[17] Lightwight Access Point Protocol. 2015. Verkkodokumentti. IETF Tools. http://tools.ietf.org/html/rfc5412 Luettu 3.3.2015

[18] Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification. 2015. Verkkodokumentti. IETF Tools. http://tools.ietf.org/html/rfc5415 Luettu 3.3.2015

[19] Cisco 2100 controller quick start guide. 2015. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/td/docs/wireless/controller/2100/quick/guide/ctrl206q.html Luettu 19.3.2015

[20] Cisco 2502P Access Points. 2015. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/td/docs/wireless/access_point/3500/quick/guide/ap3502getstart.html Luettu 19.3.2015