

Henri Saarela

## **Langaton lähiverkko osaksi Labranet-järjestelmää**

Opinnäytetyö

Kevät 2015

SeAMK Tekniikka

Tietotekniikan tutkinto-ohjelma

SEINÄJOEN AMMATTIKORKEAKOULU

## Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikan koulutusohjelma

Suuntautumisvaihtoehto: Verkkotekniikka

Tekijä: Henri Saarela

Työn nimi: Langaton lähiverkko osaksi Labranet-järjestelmää

Ohjaaja: Alpo Anttonen

Vuosi: 2015

Sivumäärä: 40

Liitteiden lukumäärä: 1

---

Tämän opinnäytetyön tarkoituksena on liittää toimiva langaton lähiverkko osaksi Seinäjoen ammattikorkeakoulun Labranet-järjestelmää. Langatonta lähiverkkoa käytetään tietoliikennetekniikan kursseilla tehtävissä harjoituksissa ja opetustilanteissa.

Tavoitteena on saada toimiva ja turvallinen langaton verkko osaksi Labranetiä.

Ensin tutustutaan langattoman verkon historiaan, standardeihin, tekniikoihin ja tietoturvasuuteen alan kirjallisuuden avulla. Tämän jälkeen tutustutaan hieman Labranet-järjestelmään ja sen taustoihin.

Seuraavaksi tutustutaan työssä käytettävään testauslaitteistoon ja Cison Aironet 1131AG langattomiin laitteisiin ja niiden konfigurointiin.

Lopulta suoritetaan lopulliset kytkennät ja laitteiden asennukset. Lopputuloksena saatiin toimiva langaton verkko osaksi Labranet-järjestelmää.

Avainsanat: langaton tiedonsiirto, langaton lähiverkko, tietoturva, tietoliikenne

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

## **Thesis abstract**

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Networking Technology

Author: Henri Saarela

Title of thesis: Adding Wireless local area network to a Labranet system

Supervisor: Alpo Anttonen

Year: 2015

Number of pages: 40

Number of appendices: 1

---

The objective of this thesis was to add a fully operational and secure wireless network to a Labranet system. The wireless network would be used for educational purposes.

The history, standards, technology and security of wireless networks were studied by reading literature on the field. Then the backgrounds and functionality of the Labranet system were studied. After that the functionality of the Cisco Aironet1131AG Access Points was explored and it was studied how to configure the device. Finally the connections and instalments were made. The outcome was an operational wireless network as a part of the Labranet system.

Keywords: Wireless local area network, WLAN, information security, data communications

## SISÄLTÖ

Opinnäytetyön tiivistelmä.....	2
Thesis abstract.....	3
SISÄLTÖ.....	4
Kuvio- ja taulukkoluetelo.....	6
Käytetyt termit ja lyhenteet .....	8
1 JOHDANTO .....	11
1.1 Työn tausta .....	11
1.2 Työn tavoite .....	11
1.3 Työn rakenne.....	11
2 LANGATON LÄHIVERKKO (WLAN).....	12
2.1 Yleistä.....	12
2.2 WLAN-standardoinnin historiaa .....	12
2.3 IEEE 802.11n.....	13
2.4 802.11-standardien yhteenveto.....	13
3 WLAN-TEKNIIKAT JA TIETOTURVA .....	15
3.1 OFDM-tekniikka .....	15
3.2 MIMO-tekniikka.....	15
3.3 Hajaspektritekniikat.....	15
3.3.1 FHSS-tekniikka .....	15
3.3.2 DSSS-tekniikka.....	16
3.4 Tietoturva.....	17
3.4.1 WEP.....	17
3.4.2 WPA.....	18
3.4.3 WPA2.....	18
4 LABRANET .....	19
4.1 Tausta.....	19
4.2 Esittely .....	19
4.3 Laitteisto .....	21
5 KÄYTETTÄVÄ LAITTEISTO .....	22
5.1 Cisco Aironet 1131AG .....	22

5.2	Langattoman verkon testauksessa käytettävä laitteisto .....	22
5.3	Langattoman verkon testauksessa käytettävä ohjelmisto .....	23
6	LANGATTOMAN VERKON RAKENTAMINEN .....	25
6.1	Konfigurointi .....	25
6.2	Käyttöönotto ja kytkentä .....	32
7	YHTEENVETO .....	36
8	POHDINTA .....	37
	LÄHTEET .....	38
	LIITTEET .....	40

## Kuvio- ja taulukkoluetelo

Kuvio 1. FHSS:n periaate. ....	16
Kuvio 2. DSSS:n periaate (Data Communications 2008). ....	16
Kuvio 3. SeAMK Labranet (Saari ym. 2013, 5). ....	20
Kuvio 4. Cisco AIR-AP1131AG-E-K9 (Cisco 2013a).....	22
Kuvio 5. Google Nexus 4 (Gadgets). ....	23
Kuvio 6. HP Pavilion 15-E058SO (HP 2013).....	23
Kuvio 7. D-Link DWA-160 WLAN -adapteri.....	23
Kuvio 8. inSSIDer 4 (Metageek 2015).....	24
Kuvio 9. WiFi Analyzer (Google Play 2015). ....	24
Kuvio 10. Cisco DB9-RJ45 console cable (Instructables 2011). ....	25
Kuvio 11. AIR-AP1131AG-E-K9:n osat (Cisco 2013b).....	25
Kuvio 12. PuTTY Session -valikko. ....	26
Kuvio 13. Terminaali-ikkuna.....	27
Kuvio 14. Hallintasivuston etusivu.....	28
Kuvio 15. EXPRESS SET-UP.....	29
Kuvio 16. Figure 19-3 Workgroup Bridge (Cisco 2010).....	29
Kuvio 17. Express Security. ....	30
Kuvio 18. SSID Manager 1(3). ....	30
Kuvio 19. SSID Manager 2(3). ....	31
Kuvio 20. SSID Manager 3(3). ....	31

Kuvio 21. Langattomien lähettimien asetukset.....	32
Kuvio 22. inSSIDer 2,4 GHz:n taajuus. ....	32
Kuvio 23. inSSIDer 5 GHz:n taajuus. ....	33
Kuvio 24. HP:n kytkin.....	34
Kuvio 25. Aironet-tukiasema rakkikaapin päällä.....	34
Kuvio 26. Aironet-tukiasema johtohyllyn päällä.....	35
Taulukko 1. Yhteenveto 802.11 -standardeista (Puska 2005, 46).....	14
Taulukko 2. AIR-AP1131AG-E-K9:n osaluettelo (Cisco 2013b).....	26

## Käytetyt termit ja lyhenteet

<b>AD</b>	Active Directory, Windows serverin käyttäjätietokanta.
<b>AES</b>	Advanced Encryption Standard
<b>DB9</b>	Katso "RS-232".
<b>DHCP</b>	Dynamic Host Configuration Protocol, DHC-palvelu. Huolehtii IP-osoitteiden ja muiden TCP/IP-asetusten antamisesta verkon koneille (Hakala & Vainio, 2002,154).
<b>DNS-palvelin</b>	Domain Name Server. Nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia eli domaineja IP-osoitteiksi.
<b>Dual-band</b>	Teknologia, joka mahdollistaa 2,4 GHz:n ja 5 GHz:n taajuuksien yhtäaikaisen käytön langattomassa reitittimessä.
<b>Freeware</b>	Ilmaishjelma. Tavallisesti vain korvaukseton kopioiminen on sallittua.
<b>IEEE</b>	Institute of Electrical and Electronics. Maailman laajin teknisten ammattilaisten muodostama yhteisö. Perustettu v. 1884. Muutaman sähköinsinöörin perustamaan yhteisöön kuuluu tänä päivänä yli 300 000 ammattilaista lähes kaikista maista. (Granlund, 2007, 4.)
<b>IP</b>	Internet Protocol, internetkerroksen protokolla. Huolehtii IP-tietoliikennepakettien perille toimittamisesta.
<b>IP-osoite</b>	Numerosarja, jota käytetään verkkolaitteiden yksilöimiseen verkossa.
<b>ISM</b>	Industrial, Scientific, Medical. Vapaasti käytettävä taajuusalue.

<b>KVM</b>	Keyboard, Video, Mouse-kytkin. Mahdollistaa usean tietokoneen hallinnan yhden näppäimistön, näytön ja hiiren avulla.
<b>LAN</b>	Local Area Network, lähiverkko.
<b>LMSG</b>	LAN/MAN Standardization Group.
<b>MAC-osoite</b>	Media Access Control -osoite. Yksilöity osoite, jonka avulla laite tunnistetaan verkossa.
<b>Nonssi</b>	Nonse, eli nonssi on mitäänsanomaton luku- tai kirjainyhdistelmä (Granlund 2007, 318).
<b>Ping</b>	Komento, jolla voidaan kokeilla jonkin laitteen saavutettavuutta.
<b>PuTTY</b>	Terminaalimulaattori. Maksuton ohjelma, jolla voi ottaa pääteyhteyksiä Windows-koneesta muihin tietokoneisiin, jos käytössä on jonkinlainen Internet-yhteys (Korpela, 2002).
<b>RC4</b>	Ron Rivestin mukaan nimetty jonosalaaja, Rivest Cipher 4 (Granlund 2007, 318).
<b>RJ45</b>	Ethernet-kaapeli, puhekielessä verkkokaapeli.
<b>RS-232</b>	Kahden laitteen väliseen kommunikointiin tarkoitettu tietoliikenneportti. Tunnetaan nimellä sarjaportti.
<b>SSID</b>	Service Set Identifier, Langattoman verkon tunnus.
<b>TCP/IP</b>	Transmission Protocol/Internet Protocol. Määrittelee miten verkossa olevien laitteiden pitäisi yhdistyä toisiinsa internetin välityksellä ja miten datan pitäisi kulkea niiden välillä.
<b>TKIP</b>	Temporal Key Interchange Protocol

<b>Toimialue</b>	Joukko verkkoon liitettyjä tietokoneita, joita hallitaan yhteisenä yksikkönä. Käytetään etenkin yrityksissä ja kouluilla.
<b>U-NII</b>	Unlicensed National Information Infrastructure, 5 GHz:n yläpuoliset vapaasti käytettävät taajuusalueet (Puska, 2005, 284).
<b>UPS</b>	Uninterruptible Power Supply. Varavirtalähde lyhytaikaisten sähkökatkosten varalle.
<b>VLAN</b>	Virtual LAN, virtuaalilähiverkko. Tekniikka, jolla fyysinen lähiverkko voidaan jakaa loogisiin osiin.
<b>VMware</b>	Virtuaalikoneiden luontiin ja suorittamiseen tarkoitettu ohjelmisto.
<b>WGB</b>	Workgroup Bridge. Käytetään yhteyden luomiseen työasemien välillä, jotka eivät ole samassa langallisessa verkossa.
<b>Wi-Fi Alliance</b>	Organisaatio joka testaa, että laitteet ovat 802.11-standardin mukaisia. Näille testatuille laitteille se myöntää Wi-Fi CERTIFIED -sertifikaatin, joka merkitsee että se toimii kaikkien muidenkin sertifikaatin saaneiden laitteiden kanssa.
<b>Wi-Fi</b>	Yleisesti käytettävä nimitys langattomasti lähiverkosta. Wi-Fi Alliancen tavaramerkki ja WLAN:in kaupallinen nimi.
<b>WLAN</b>	Wireless LAN, langaton lähiverkko.

# 1 JOHDANTO

## 1.1 Työn tausta

Opinnäytetyön aihe ja toimeksianto saatiin Seinäjoen Ammattikorkeakoulun tietoliikennetekniikan lehtorilta Alpo Anttoselta. Tietoliikennetekniikan laboratoriossa sijaitsevaan Labranet-järjestelmään tarvittiin WLAN-verkko osaksi järjestelmää. Langatonta lähiverkkoa voitaisiin käyttää opetuskäytössä ja tietoliikennekurssien laboratorioharjoituksia tehdessä.

## 1.2 Työn tavoite

Tämän opinnäytetyön ensisijaisena tavoitteena on rakentaa Seinäjoen Ammattikorkeakoulun tietoliikennetekniikan laboratorioon toimiva ja tietoturvallinen langaton verkko, jota voidaan käyttää opetustarkoituksessa ja oppilaskäytössä.

Toissijaisena tavoitteena, työn tekijän kannalta, on tutustua langattoman tiedonsiirron historiaan, standardeihin, eri tekniikoihin sekä tutustua työssä käytettävään WLAN-laitteistoon.

## 1.3 Työn rakenne

Opinnäytetyön ensimmäisessä luvussa kerrotaan työn taustasta ja tavoitteista. Luvussa 2 käsitellään yleistä tietoa langattomista lähiverkoista sekä niiden historiaa ja standardeja. Kolmannessa luvussa tutustutaan langattomiin tiedonsiirtotekniikoihin ja tietoturvaan. Luvussa 4 tutustutaan Labranet-järjestelmään. Luvussa 5 esitellään työssä käytettävää laitteistoa, eli WLAN-reitittäjiä ja yhteyden testaamiseen käytettäviä laitteita. Luku 6 keskittyy varsinaiseen työn toteutukseen eli langattoman lähiverkon rakentamiseen/konfigurointiin. Luvussa 7 tehdään yhteenveto työstä ja luvussa 8 pohditaan työn onnistumista.

## 2 LANGATON LÄHIVERKKO (WLAN)

### 2.1 Yleistä

Wi-Fi, WLAN, langaton lähiverkko – kaikki tarkoittavat samaa asiaa. Langattomuus on nykykehityksessä tärkeä asia, ja langatonta teknologiaa hyödynnetään yhä enemmän uusissa laitteissa. Televisiot, matkapuhelimet, pelikonsolit ja tietokoneet hyödyntävät langatonta tiedonsiirtoa. Langattomia verkkoja on nykyisin tarjolla monissa julkisissa tiloissa, kuten huoltoasemilla, lentokentillä, junissa ja jopa linja-autoissa. Langaton tiedonsiirto on nykyisin niin suosittua, että sitä joudutaan jatkuvasti kehittämään nopeammaksi kasvavan datamäärän vuoksi.

### 2.2 WLAN-standardoinnin historiaa

1980-luvun puolivälissä Motorola esitteli Altairin, ensimmäisen WLAN-tuotteensa. Altairin langaton teknologia, kuten myös muiden valmistajien tuotteet 80- ja 90-luvun alkupuolella, oli valmistajien omaa käsialaa. Tästä johtuen kuluttajat joutuivat sitoutumaan yhteen toimittajaan, ja tuotteen tulevaisuus oli epävarma. Tämän vuoksi IEEE:n LAN/MAN-standardointiryhmä (LMSG) alkoi kehittää standardia langattomille lähiverkoille. (Puska 2005, 15.)

LMSG alkoi kehittää ensimmäistä standardia vuonna 1990 ja ensimmäinen 802.11-standardi julkaistiin vuonna 1997. Ensimmäisen 802.11-standardin hitaan, 1 ja 2 Mbit/s siirtonopeuden lisäksi sitä vaivasi puutteet yhteensopivuudessa sekä käyttöluo-ongelmat käytettyyn taajuuskaistaan liittyen. Näistä huolimatta 802.11 tarjosi hyvän pohjan tuleville standardeille. (Puska 2005, 15.)

Vuonna 1999 julkaistiin 802.11b-standardi, joka nosti bittinopeuden 11 Mbit/s. Inf-  
rapunavalo jätettiin pois suurempaa nopeutta tavoiteltaessa, ainoaksi siirtotieksi valittiin 2,4 GHz:n radiotaajuudet, ja siirtotekniikaksi valittiin DSSS aikaisemman FHSS:n sijaan. Uusi standardi nousi edeltäjänsä huomattavasti suosittumaksi. Tekniikkaa laajennettiin 802.11b+ -standardilla, joka kaksinkertaisti siirtonopeuden, mutta sen suosio jäi marginaaliseksi. (Puska 2005, 15.)

Myöhemmin samana vuonna, 1999, kehitettiin 802.11a-standardi. Sen teoreettiseksi bittinopeudeksi luvattiin 54 Mbit/s 5 GHz:n U-NII-taajuusalueella ja siinä esiteltiin uutta OFDM-siirtotekniikkaa. Koska taajuudet olivat varattuja monissa maissa, 802.11a oli käytössä lähinnä USA:ssa ja Kanadassa. Ongelmaksi muodostui huono kantomatka ja laitteiden korkeahko hinta. (Puska 2005, 16.)

Vuonna 2003 ratifioitu 802.11g tarjosi myös siirtonopeuden 54 Mbit/s, mutta se käytti Euroopassakin vapaassa käytössä olevaa 2,4 GHz:n ISM-taajuusaluetta. (Puska 2005, 16.)

### **2.3 IEEE 802.11n**

IEEE 802.11n -standardi valmistui vuonna 2009 ja se kasvoi nopeasti 802.11g-standardia suosittumaksi. Se tarjoaa edellisiin standardeihin nähden huomattavasti suuremman tiedonsiirtonopeuden (600 Mb/s, todellinen 100–200 Mb/s vrt. 802.11a:n ja 802.11g:n 54 Mb/s, todellinen 25 Mb/s). 802.11n tukee taajuuksia 2,4 GHz ja 5 GHz ja käyttää sekä OFDM että MIMO-tekniikoita. (Granlund 2007, 305.)

### **2.4 802.11-standardien yhteenveto**

Taulukossa 1 esitetään yhteenveto esiteltyjen standardien tärkeimmistä ominaisuuksista, kuten käytettävästä taajuusalueesta, tekniikasta ja teoreettisesta data-siirtonopeudesta.

Taulukko 1. Yhteenveto 802.11 -standardeista (Puska 2005, 46)

<b>Standardi</b>	<b>Ratifioitu</b>	<b>Taajuusalue</b>	<b>Tekniikka</b>	<b>Teoreettinen nopeus</b>
<b>802.11</b>	<b>1997</b>	<b>2,4 GHz</b>	<b>FHSS, DSSS</b>	<b>1 ja 2 Mbit/s</b>
<b>802.11b</b>	<b>1999</b>	<b>2,4 GHz</b>	<b>DSSS</b>	<b>1, 2, 5,5 ja 11 Mbit/s</b>
<b>802.11a</b>	<b>1999</b>	<b>5 GHz</b>	<b>OFDM</b>	<b>6-54 Mbit/s</b>
<b>802.11g</b>	<b>2003</b>	<b>2,4 GHz</b>	<b>OFDM</b>	<b>1-54 Mbit/s</b>
<b>802.11n</b>	<b>2009</b>	<b>2,4 GHz, 5 GHz</b>	<b>MIMO, OFDM</b>	<b>600 Mbit/s</b>

## **3 WLAN-TEKNIIKAT JA TIETOTURVA**

### **3.1 OFDM-tekniikka**

OFDM eli Orthogonal Frequency Division Multiplexing on monikantaaltomodulointi-tekniikka, jossa taajuusalue, jolla dataa siirretään, jaetaan alikanaviin ja niitä käytetään rinnakkain (Granlund 2007, 112; Puska 2005, 40).

### **3.2 MIMO-tekniikka**

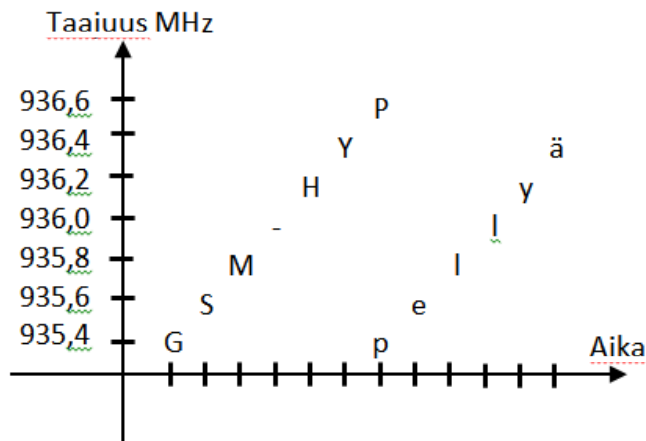
MIMO-nimitys muodostuu sanoista Multiple Input Multiple Output. MIMO eli moni-lähetintekniikan toiminta perustuu usean vastaanotto- ja lähetysantennin käyttöön. Jokainen antennipari käsittelee omaa itsenäistä lähetettä. (Granlund 2007, 305.)

### **3.3 Hajaspektritekniikat**

Hajaspektritekniikka perustuu kapean digitaalisignaalin hajauttamiseen leveälle taajuuskaistalle. Sen hyötyjä on hyvä häiriönsietokyky ja sitä on vaikea salakuunnella, sillä sen signaali muistuttaa kohinaa. Hajaspektritekniikka sai alkunsa toisen maailmansodan sotateollisuudesta. (Rackley 2007, 76-77.)

#### **3.3.1 FHSS-tekniikka**

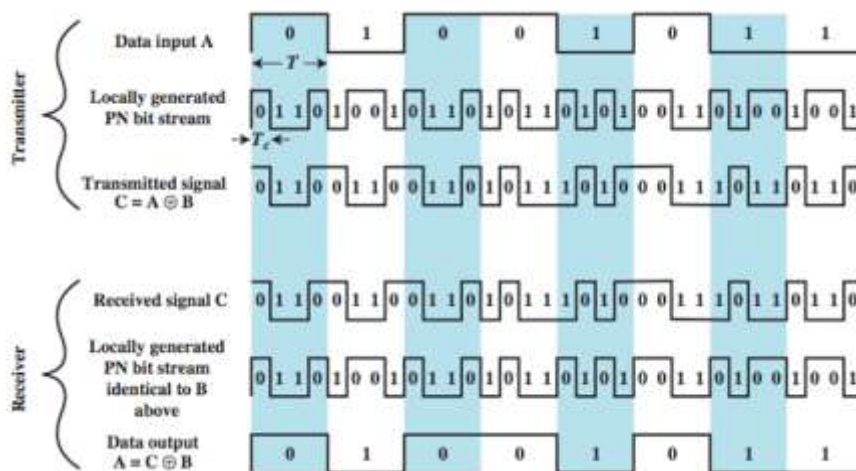
Frequency Hopping Spread Spectrum eli taajuushyppelytekniikka on yksi hajaspektritekniikoista. Viesti hajautetaan koko käytettävälle taajuusalueelle, taajuusalue on jaettu tasakokoisiin alikanaviin ja kiinteään mittaisiin aikaväleihin. Näennäissatunnainen hyppyjärjestys sovitaan ennakkoon, vastaanottaja ja lähettäjä molemmat noudattavat sitä. Kun siirto alkaa, data paloitellaan ja jokainen pala siirretään sovitun hyppyjärjestyksen mukaisesti. (Granlund 2001, 234; Granlund 2007, 117.)



Kuvio 1. FHSS:n periaate.

### 3.3.2 DSSS-tekniikka

Direct Sequence Spread Spectrum eli suorasekvenssihajaspektri menetelmä toimii siten, että kapea signaali hajautetaan eli levitetään laajemmalle taajuuskaistalle. Hajautuksessa käytetään 11-bittistä koodia/hajautusavainta, jota kutsutaan Chikipiksi (suom. lastu) ja koodi hajautetaan alikanaville. Viesti kerrotaan koodilla lähettäessä, jolloin kertolaskun lopputuloksena saadaan hajautusavaimen ”taajuuden” sisältämä lähete. Vastaavasti vastaanotettaessa lähete kerrotaan hajautusavaimella ja tulokseksi saadaan alkuperäinen signaali. (Granlund 2007, 118.)



Kuvio 2. DSSS:n periaate (Data Communications 2008).

### 3.4 Tietoturva

Tietoturva on oleellinen osa langatonta lähiverkkoa. Hyvän tietoturvan saavuttamiseksi on syytä tutustua olemassa oleviin salaustapoihin. Huolella valitut langattoman verkon suojausasetukset estävät langattoman verkon luvattoman käytön sekä estävät tietojen pääsyn ulkopuolisen käsiin.

#### 3.4.1 WEP

WEP eli Wired Equivalent Privacy on IEEE 802.11 -standardin mukainen tietoliikenteen salaustapa. Autentikointiin eli todentamiseen on kaksi menetelmää, Open system ja SHA. (Granlund 2007, 318.)

Open system on sananmukaisesti avoin ja kaikilla on vapaa pääsy verkkoon (Granlund 2007, 318). Tällaisia käytäntöjä näkee usein julkisissa tiloissa.

SHA eli Shared Key Authentication perustuu yhteiseen salaiseen avaimen. Autentikointi tapahtuu haaste-vastaus-menetelmällä. Tukiasema lähettää yhteyttä yrittävälle laitteelle nonssin. Nonssi on mitäänsanomaton luku- tai kirjainyhdistelmä. Laitteen pitää salata nonssi verkon omalla WEP-avaimella ja lähettää se sitten takaisin tukiasemalle. Tukiasema tekee tarkistuksen nonssin oikeinkirjoituksesta. Tiedon luottamuksellisuus varmistetaan WEP-menetelmällä, joka perustuu RC4-jonosalaukseen. (Granlund 2007, 318.)

WEP-salaus sisältää paljon heikkouksia, joita ei osattu ottaa ensimmäisessä 802.11-standardissa huomioon. Autentikointi koskee ainoastaan laitetta eikä käyttäjää ja näin ollen se mahdollistaa verkon luvattoman käytön. Myös yksi heikkous liittyy salausavaimen, sillä se on kiinteästi asetettu. Näin salausavaimen pystyy selvittämään salakuuntelemalla liikennettä. Tavallisesti avain on 128 bittinen ja se sisältää 24 bitin alustusvektorin ja 104 bittisen avaimen. (Granlund 2007, 318.)

WEP-salausta ei suositella käytettäväksi paikoissa, joissa verkossa voi liikkua arkaluontoisia tai salaisia dokumentteja.

### 3.4.2 WPA

WPA tulee sanoista Wi-Fi Protected Access. Se kehitettiin WEP-salauksen puutteiden vuoksi. WPA täytyi WEP:in puutteiden vuoksi saada nopeasti myös markkinoilla oleviin laitteisiin, joten se suunniteltiin käyttöönotettavaksi ohjelmistopäivityksellä. WPA-salauksessa käytetään TKIP-protokollaa, joka muuttaa salausavaimia niin että avain esiintyy samana vain äärimmäisen harvoin. IEEE 802.1x -protokollaa voidaan käyttää käyttäjien autentikoimiseen, esim. AD:ta apuna käyttäen. (Granlund 2007, 320.)

### 3.4.3 WPA2

WPA-salauksessa käytettävät uudet menetelmät korjasivat WEP-suojauksen puutteet ja loivat pohjan IEEE 802.11i -standardille eli WPA2-suojaukselle (Granlund 2007, 321).

WPA2-suojausta ei voitu enää toteuttaa ohjelmistopäivityksellä, vaan laitteistoihin piti tehdä muutoksia. Nykyisin WPA2-suojaus on pakollinen kaikissa Wi-Fi CERTIFIED -laitteissa. (Granlund 2007, 321.)

RC4 eli Rivest Cipher 4 on saanut nimensä Ron Rivestin mukaan. RC4-jonosalaaja korvattiin AES-salauksella. AES käyttää erittäin tehokas Rijndael-algoritmia ja 128-, 192- sekä 256-bittisiä salausavaimia ja se vaatii laitteilta erillisen salauspiirin. (Granlund 2007, 321.)

## 4 LABRANET

### 4.1 Tausta

Labranet on Seinäjoen Ammattikorkeakoulun tietoliikennetekniikan laboratoriosta löytyvä opetusympäristö. Labranet rakennettiin projektityönä keväällä 2013. Sen rakensivat Seinäjoen Ammattikorkeakoulun Tietotekniikan 2010 -vuosikurssin opiskelijat Jori Saari, Arttu Antila, Tuomas Kivimäki, Ville Uusitalo sekä Jaakko Ketelimäki.

Seinäjoen Ammattikorkeakoulun tietotekniikan koulutusohjelma tarjoaa suuntautumisvaihtoehdoksi tietoverkkotekniikan, joten sitä varten täytyy myös olla hyvä opetusympäristö. Labranetin rakentamisen ideana oli saada ammattikorkeakoululle samankaltainen opetusympäristö kuin Jyväskylän tai Kymenlaakson ammattikorkeakoulussa. (Saari ym. 2013, 3.)

Jyväskylän ammattikorkeakoulun tuotantoverkkoa kutsutaan LabraNet-ympäristöksi ja osana tätä toimii SpiderNet-ympäristö. Nämä ympäristöt mahdollistavat erilaisten ja hyvinkin monimutkaisten verkkojen toteutuksen. Järjestelmään on kytketty noin 20 luokkaa, se ylläpitää ja palvelee 900 käyttäjää ja 300 työasemaa. (Saari ym. 2013, 3.)

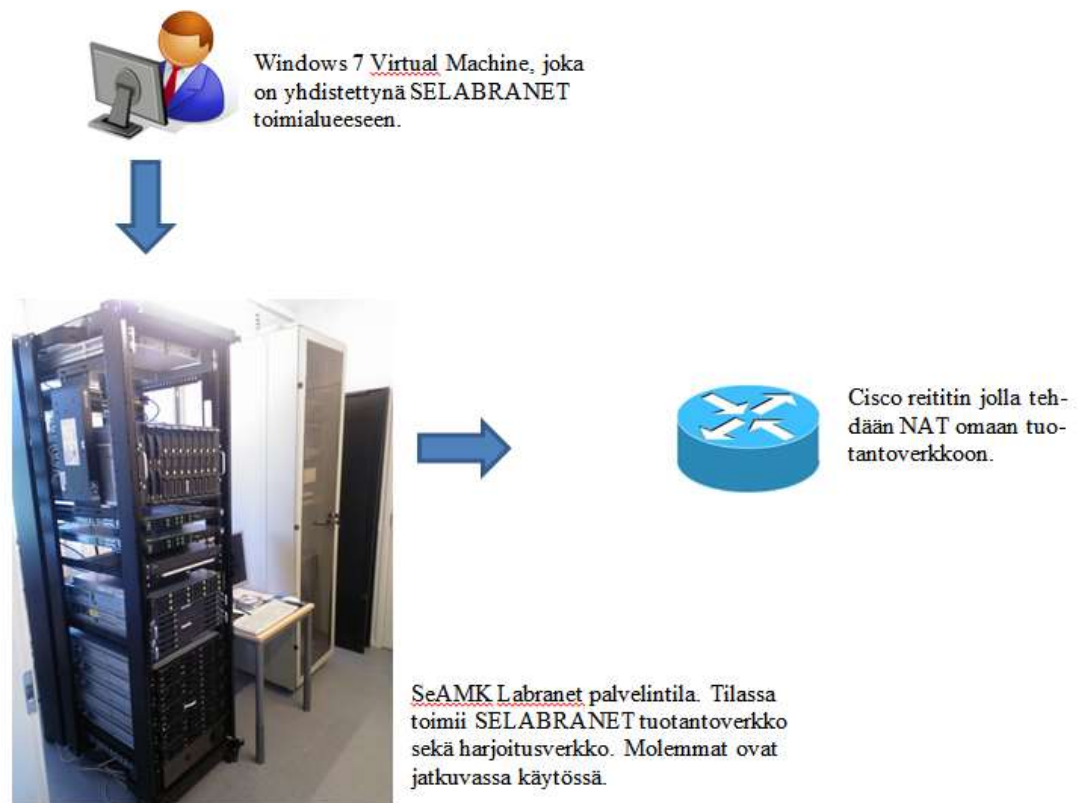
Operaattoritasoisen verkkoympäristön rakentaminen Seinäjoen Ammattikorkeakoululle oli mahdotonta, mutta muiden ammattikorkeakoulujen toteutusta soveltamalla koululle saatiin rakennettua toimiva kokonaisuus (Saari ym. 2013, 3).

### 4.2 Esittely

Labranet on täysin EPEDU-tuotantoverkosta eristetty tuotantoverkko opetuskäyttöön ja laboratorioharjoituskäyttöön. Pääasiassa verkkoa käyttävät tietoverkkotekniikan opiskelijat. Labranet-projekti toteutettiin Tietoliikennetekniikan laboratorion takaosassa sijaitsevaan varastotilaan. SeAMK Labranet koostuu sekä uudesta että vanhasta palvelinkalustosta. (Saari ym. 2013, 3-4.)

Tietoliikennetekniikan laboratoriossa oleville työasemille asennetaan VMware Workstation ja ohjelmalla luodaan koneelle virtuaalinen työasema. Työasemissa on kaksi verkkokorttia, joista toinen on varattu ainoastaan VMWaren käyttöön. Tämä virtuaalinen työasema yhdistetään Labranetin SELABRANET-toimialueeseen. Toimialue on palvelintilassa ja jatkuvassa tuotantokäytössä. (Saari ym. 2013, 4.)

Palvelimet toteutetaan VMware ESXi -ympäristöön ja näille palvelimille on tarkoitus jatkossa asentaa kaikki kurseilla tarvittavat palvelimet. Tämä ympäristö eristetään EPEDU-tuotantoverkosta. Kuviossa 3 on Labranetin toiminta selkiytettynä. (Saari ym. 2013, 4.)



Kuvio 3. SeAMK Labranet (Saari ym. 2013, 5).

Liitteestä 1 löytyy PacketTracer-ohjelmalla tehty piirros Labranet-järjestelmästä.

### **4.3 Laitteisto**

Labranetin laitteistoon kuuluu kaksi Fujitsu RX200 S7 -palvelinta, kaksi Fujitsu RX300 S2 -palvelinta, yksi Fujitsu Primergy BX600 S2 10-paikkainen korttipalvelin ja yksi Fujitsu FiberCat SX 80 iSCSI -levyjärjestelmä. Näiden lisäksi laitekannasta löytyy KVM-kytkin, kaksi Brocade valokuitukytkintä ja UPS. (Saari ym. 2013, 5.)

## 5 KÄYTETTÄVÄ LAITTEISTO

### 5.1 Cisco Aironet 1131AG

Työssä käytetään kahta Ciscon valmistamaa Aironet 1131AG Access Point -laitetta. Aironet 1131AG:n ensimmäinen versio julkaistiin 10. marraskuuta 2004. Sitä valmistettiin lähes yhdeksän vuoden ajan, kunnes 26. heinäkuuta 2013 sen valmistus lakkautettiin. Laitetuki jatkuu 31. heinäkuuta 2018 asti. (Cisco 2013a.)

Opinnäytetyössä käytettävän laitteen ominaisuuksiin lukeutuu muun muassa 802.11g- ja 802.11a-standardi tuki, eli se tukee 2,4 GHz:n ja 5 GHz:n taajuuksia ja Dual-bandia.



Kuvio 4. Cisco AIR-AP1131AG-E-K9  
(Cisco 2013a).

### 5.2 Langattoman verkon testauksessa käytettävä laitteisto

Yhteyden testaamiseen käytetään Google Nexus 4 -älypuhelinta ja HP Pavilion 15-E058SO -kannettavaa tietokonetta. Testaamiseen käytetään lisäksi D-Link DWA160 -adapteria sillä käytettävissä olevan HP:n kannettavan verkkokortista ei löydy tukea 5 GHz:n taajuuksille.



Kuvio 5. Google Nexus 4 (Gadgets).



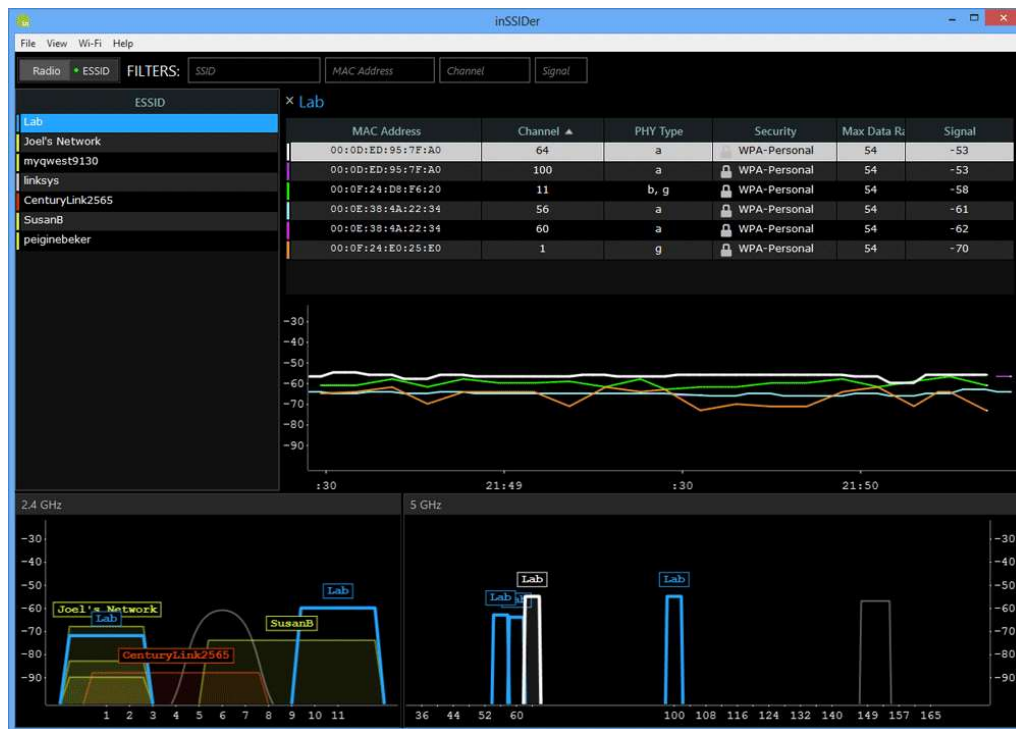
Kuvio 6. HP Pavilion 15-E058SO (HP 2013).



Kuvio 7. D-Link DWA-160 WLAN -adapteri.

### 5.3 Langattoman verkon testauksessa käytettävä ohjelmisto

Kannettavalla tietokoneella verkon skannaamisen käytetään inSSIDer 2.1 -ohjelmaa. Nimensä mukaisesti ohjelma skannaa lähistöltä löytyvät langattoman tukiasemat, niiden käyttämän taajuuden, kanavat, MAC-osoitteet ja paljon muuta. Kuviossa 8 on sovelluksen päivitetty versio. Sovelluksesta on saatavilla freeware-versio (Techspot 2015).



Kuvio 8. inSSIDer 4 (Metageek 2015).

Google Nexus 4 -älypuhelimella käytettiin WiFi Analyzer -nimistä sovellusta. Työssä käytettiin testaamiseen myös älypuhelimta sen vuoksi että verkot voitiin skannaata kätevämmiin kuin inSSIDer-ohjelmalla. inSSIDeria käytettiin, kun haluttiin yksityiskohtaisempaa tietoa. Sovellus on saatavissa ilmaiseksi Google Playsta.



Kuvio 9. WiFi Analyzer (Google Play 2015).

## 6 LANGATTOMAN VERKON RAKENTAMINEN

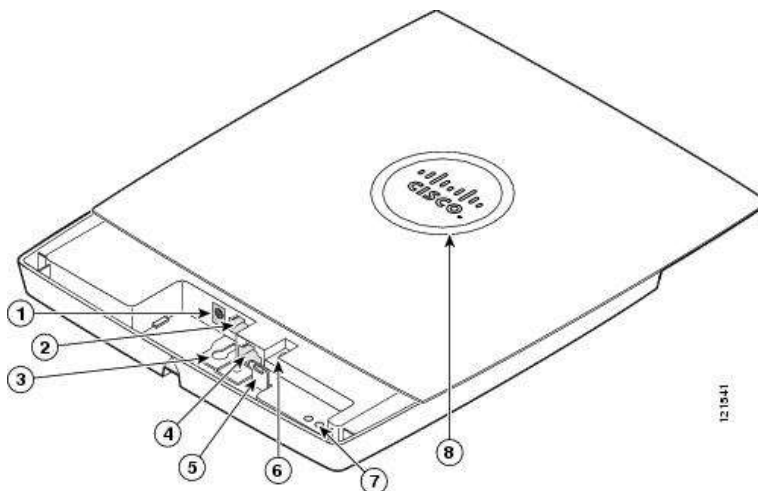
### 6.1 Konfigurointi

Cisco Aironet 1131AG AP -laitteen konfiguroimiseksi täytyy se ensiksi kytkeä osaksi toimivaa lähiverkkoa. Kun laite kytketty lähiverkkoon, voidaan sen IP-osoite tarkistaa mukana tullutta DB9-RJ45 console -kaapelia käyttäen.



Kuvio 10. Cisco DB9-RJ45 console cable (Instructables 2011).

Konfigurointiin käytettävästä tietokoneesta riippuen voidaan myös tarvita RS232-USB-adapteri, mikäli tietokoneesta ei löydy sarjaporttiliitäntämahdollisuutta. DB9-RJ45-kaapelista kytketään toinen pää Aironetin Console-porttiin (katso kuvio 11 sekä taulukko 2) ja toinen pää tietokoneeseen.

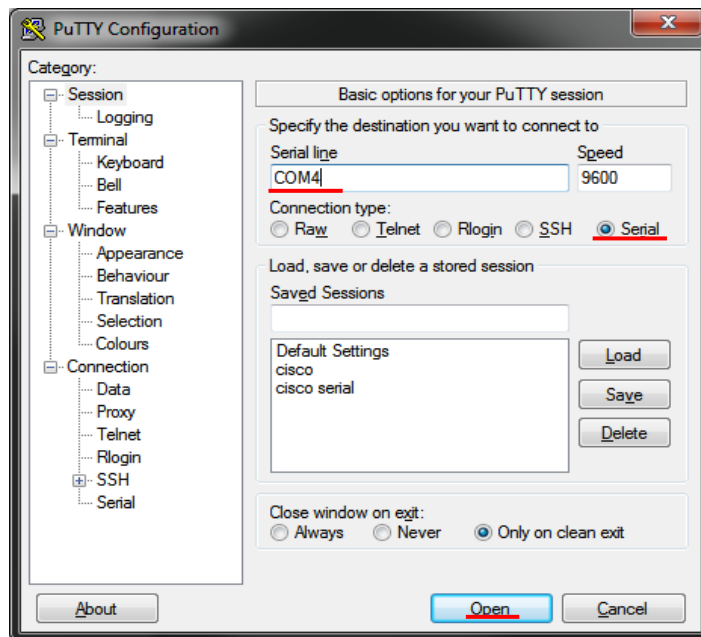


Kuvio 11. AIR-AP1131AG-E-K9:n osat (Cisco 2013b).

Taulukko 2. AIR-AP1131AG-E-K9:n osaluettelo (Cisco 2013b).

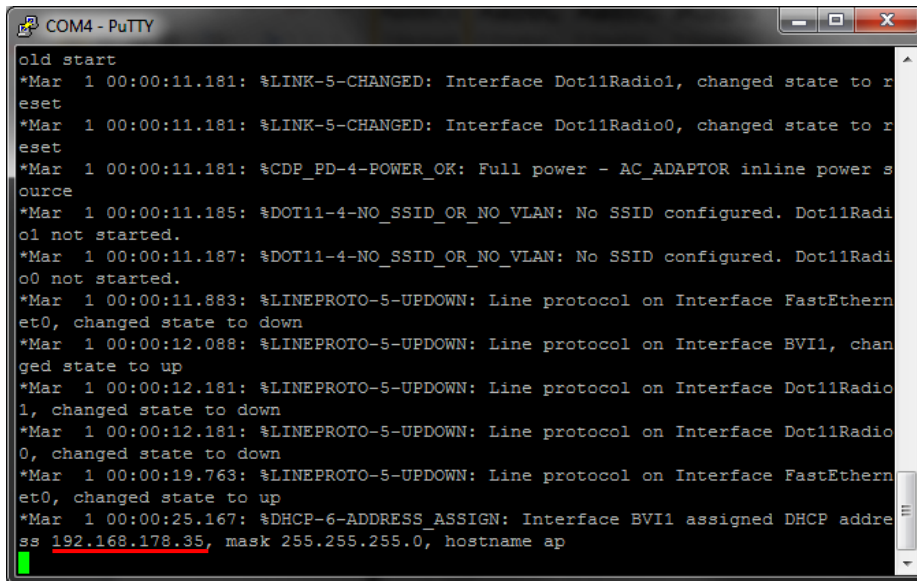
1	<b>Power connector</b>	5	<b>Padlock post</b>
2	<b>Ethernet port</b>	6	<b>Mode button</b>
3	<b>Keyhole slot</b>	7	<b>Ethernet (E) and Radio (R) LEDs</b>
4	<b><u>Console port</u></b>	8	<b>Status LED</b>

Seuraavaksi täytyy selvittää laitteen IP-osoite. Tähän tarvitaan terminaaliemulaattoria, kuten PuTTYa. Ohjelman Session-valikosta (kuvio 12) valitaan yhteystavaksi serial ja serial line -kohtaan pitää määrittää oikea portti, tässä tapauksessa COM4. Lopuksi klikataan Open.



Kuvio 12. PuTTY Session -valikko.

Seuraavaksi aukeaa terminaali-ikkuna (kuvio 13), josta selviää minkä IP-osoitteen laite on saanut. Kuvion 13 alimmalta riviltä nähdään saatu IP-osoite, 192.168.178.35. Tällä osoitteella laitteen asetuksia pääsee hallitsemaan. Mikäli ikkuna jää mustaksi, kannattaa laitteen virtajohto irrottaa hetkeksi ja kokeilla sitten uudelleen.



```

COM4 - PuTTY
old start
*Mar 1 00:00:11.181: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to r
eset
*Mar 1 00:00:11.181: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to r
eset
*Mar 1 00:00:11.181: %CDP_PD-4-POWER_OK: Full power - AC_ADAPTOR inline power s
ource
*Mar 1 00:00:11.185: %DOT11-4-NO_SSID_OR_NO_VLAN: No SSID configured. Dot11Radi
o1 not started.
*Mar 1 00:00:11.187: %DOT11-4-NO_SSID_OR_NO_VLAN: No SSID configured. Dot11Radi
o0 not started.
*Mar 1 00:00:11.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0, changed state to down
*Mar 1 00:00:12.088: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, chan
ged state to up
*Mar 1 00:00:12.181: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio
1, changed state to down
*Mar 1 00:00:12.181: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio
0, changed state to down
*Mar 1 00:00:19.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0, changed state to up
*Mar 1 00:00:25.167: %DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP addre
ss 192.168.178.35, mask 255.255.255.0, hostname ap

```

Kuvio 13. Terminaali-ikkuna.

Kun IP-osoite on selvitetty, voidaan siirtyä varsinaiseen konfigurointiin. Tämä on yksinkertaisinta suorittaa selaimen kautta. Saatu IP-osoite syötetään selaimen osoiteriville. Selain kysyy tunnusta ja salasanaa. Huomaa että konfiguroinnissa tulee käyttää Internet Exploreria ja yhteensopivuusnäkyä, muutoin asetukset eivät määräydy oikein. Seuraavassa kuviossa 14 nähdään, millainen on hallintisivuston etusivun näkymä. Tässä kappaleessa ei käydä läpi jokaista valikkoa ja asetusta, vaan ainoastaan tärkeimmät ja opinnäytetyön kannalta oleelliset kohdat.

The screenshot displays the configuration page for a Cisco Aironet 1130AG Series Access Point. The page title is 'Cisco Aironet 1130AG Series Access Point'. The hostname is 'TietoliikenneLabra2503a' and it has been up for 2 hours and 15 minutes. The page is divided into several sections:

- Home: Summary Status**
  - Association:** Clients: 0, Republishes: 0
  - Network Identity:** IP Address: 192.168.178.35, MAC Address: 0026.cba9.5324
  - Network Interfaces:**

Interface	MAC Address	Transmission Rate
FastEthernet0	0026.cba9.5324	100Mbps
Radio0-802.11G	0026.9906.b290	54.0Mbps
Radio1-802.11A	0026.9906.e800	54.0Mbps
  - Event Log:**

Time	Severity	Description
Mar 1 02:15:12.870	Warning	No SSID configured. Dot11Radio0 not started.
Mar 1 02:15:12.869	Warning	No SSID configured. Dot11Radio1 not started.
Mar 1 02:15:12.665	Notification	Configured from http by cisco on 192.168.178.21
Mar 1 00:03:29.719	Warning	No SSID configured. Dot11Radio0 not started.
Mar 1 00:03:29.520	Notification	Configured from http by cisco on 192.168.178.21
Mar 1 00:00:19.764	Notification	Line protocol on Interface FastEthernet0, changed state to up
Mar 1 00:00:12.183	Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:12.183	Notification	Line protocol on Interface Dot11Radio1, changed state to down
Mar 1 00:00:12.088	Notification	Line protocol on Interface BVI1, changed state to up
Mar 1 00:00:11.883	Notification	Line protocol on Interface FastEthernet0, changed state to down

Kuvio 14. Hallintasivuston etusivu.

Express Set-Up -osiossa (kuvio 15) voidaan määrittellä tukiasemalle Hostname, jolla se erotetaan helposti verkon muista laitteista. Hostname-kohdan alta löytyy MAC-osoite, jota käytetään samaan tarkoitukseen. Seuraavassa kohdassa voidaan määrittää tukiasema hakemaan IP-asetukset DHCP-palvelimelta, asettaa staattinen IP-osoite ja määrittää käytettävä oletusyhdyskäytävä. Kaksi seuraavaa kohtaa säätää Radio0- ja Radio1-perusasetuksia, kuten roolia. Rooli määrää miten laite toimii verkossa esim. yhteyspisteenä, toistimena tai WGB:nä (katso kuvio 16). Lisäksi voidaan valita, optimoidaanko radiot mahdollisimman suurelle lähetyksenopeudelle vai -kantamalle.

**Express Set-Up**

Host Name:   
 MAC Address: 0026.cba9.5324

Configuration Server Protocol:  DHCP  Static IP  
 IP Address:   
 IP Subnet Mask:   
 Default Gateway:

SNMP Community:   
 Read-Only  Read-Write

---

**Radio0-802.11G**

Role in Radio Network:  Access Point  Repeater  
 Workgroup Bridge  Universal Workgroup Bridge Client MAC:   
 Scanner

Optimize Radio Network for:  Throughput  Range  Default  Custom

Aironet Extensions:  Enable  Disable

---

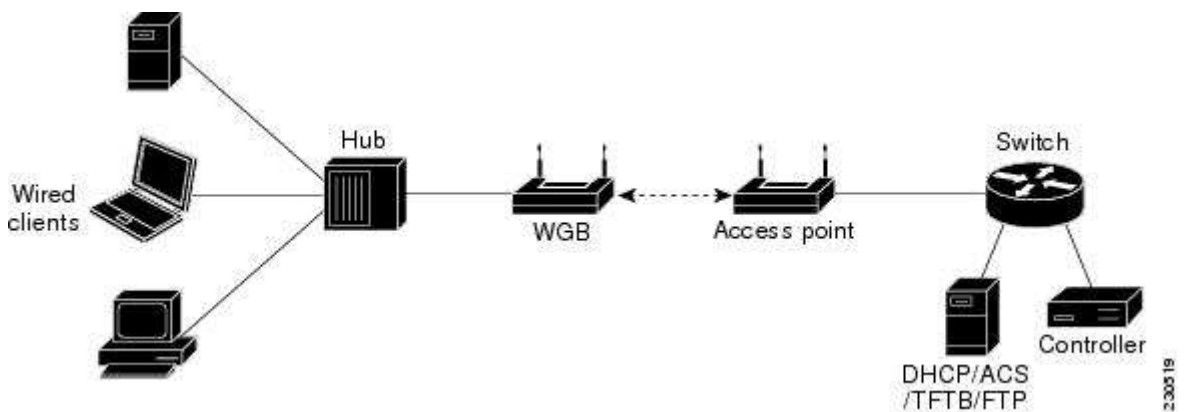
**Radio1-802.11A**

Role in Radio Network:  Access Point  Repeater  
 Workgroup Bridge  Universal Workgroup Bridge Client MAC:   
 Scanner

Optimize Radio Network for:  Throughput  Range  Default  Custom

Aironet Extensions:  Enable  Disable

Kuvio 15. EXPRESS SET-UP.



Kuvio 16. Figure 19-3 Workgroup Bridge (Cisco 2010).

Perusasetukset langattoman verkon konfiguroimiseen löytyvät Express Security -valikon (kuvio 17) alta. Sieltä voidaan määrittellä langattomalle verkolle SSID, VLAN ja kaikkein tärkein asetus, käytettävä turva-asetus. Jos molemmilla taajuuksilla (2,4 GHz:llä ja 5 GHz:llä) aikoo käyttää samaa SSID-tunnusta, voidaan se lisätä tätä kautta laitteelle, muutoin kannattaa käyttää SSID Manageria. Tämän

valikon turvallisuus asetukset ovat myös hyvin yksinkertaiset, eikä säätövaraa juurikaan löydy.

The screenshot shows the 'Express Security Set-Up' window with the 'SSID Configuration' tab selected. It is divided into three sections:

- 1. SSID:** The SSID name is 'Tietokone/Labra3503'. There is a checked checkbox for 'Broadcast SSID in Beacon'.
- 2. VLAN:** The 'No VLAN' option is selected. Other options include 'Enable VLAN ID' (with a field for ID 1-4094) and 'Native VLAN'.
- 3. Security:**
  - 'No Security' is selected.
  - 'Static WEP Key' is unselected, with a 'Key 1' dropdown and a '128 bit' dropdown.
  - 'EAP Authentication' is unselected, with fields for 'RADIUS Server' (Hostname or IP Address) and 'RADIUS Server Secret'.
  - 'WPA' is unselected, with fields for 'RADIUS Server' (Hostname or IP Address) and 'RADIUS Server Secret'.

'Apply' and 'Cancel' buttons are located at the bottom right.

Kuvio 17. Express Security.

Järkevintä on kuitenkin käyttää eri nimiä eri taajuuksilla, näin voidaan välttää esimerkiksi ongelmat joissa tietokone ei ymmärrä vaihtaa 2,4 GHz:n verkkoon, kun tietokone joutuu 5 GHz:n kantaman ulkopuolelle. Security -osion SSID Manager -valikosta (kuvio 18) voidaan lisätä useita SSID-tunnuksia ja niille voidaan määrittää omat VLAN-tunnukset ja käytettävät taajuudet. Samasta valikosta löytyy myös laajemmat turvallisuusasetukset (kuvio 19).

The screenshot shows the 'SSID Manager' configuration page. On the left is a navigation menu with categories like 'HOME', 'EXPRESS SETUP', 'NETWORK MAP', 'ASSOCIATION', 'NETWORK REFERENCES', 'SECURITY', 'SERVICES', 'WIRELESS SERVICES', 'SYSTEM SOFTWARE', and 'EVENT LOG'. The main content area is titled 'Security: Global SSID Manager' and 'SSID Properties'. It includes:

- 'Current SSID List' showing 'Labra3503' and 'Labra3503\_5GHz'.
- 'SSID' field with a dropdown menu.
- 'VLAN' field with a dropdown menu set to '< NONE >' and a link for 'Default VLAN'.
- 'Backup' fields for Backup 1, Backup 2, and Backup 3.
- 'Interface' field with checkboxes for 'Radio0-802.11G' and 'Radio1-802.11A'.
- 'Network ID' field with a dropdown menu set to '(1-4094)'.

A 'Delete' button is located at the bottom left of the main content area.

Kuvio 18. SSID Manager 1(3).

**Client Authentication Settings**

**Methods Accepted:**

Open Authentication: < NO ADDITION > ▾

Shared Authentication: < NO ADDITION > ▾

Network EAP: < NO ADDITION > ▾

**Server Priorities:**

**EAP Authentication Servers**

Use Defaults [Default Defaults](#)

Customize

Priority 1: < NONE > ▾

Priority 2: < NONE > ▾

Priority 3: < NONE > ▾

**MAC Authentication Servers**

Use Defaults [Default Defaults](#)

Customize

Priority 1: < NONE > ▾

Priority 2: < NONE > ▾

Priority 3: < NONE > ▾

---

**Client Authenticated Key Management**

**Key Management:** < Mandatory > ▾  CKM  Enable WPA < WPA0 > ▾

**WPA Pre-shared Key:**   ASCII  Hexadecimal

Kuvio 19. SSID Manager 2(3).

**Guest Mode/Infrastructure SSID Settings**

**Radio0-802.11G:**

Set Beacon Mode:  Single BSSID Set Single Guest Mode SSID: < LabraNetA\_2.4Ghz > ▾

Multiple BSSID

Set Infrastructure SSID: < NONE > ▾  Force Infrastructure Devices to associate only to this SSID

**Radio1-802.11A:**

Set Beacon Mode:  Single BSSID Set Single Guest Mode SSID: < LabraNetA\_5Ghz > ▾

Multiple BSSID

Set Infrastructure SSID: < NONE > ▾  Force Infrastructure Devices to associate only to this SSID

Kuvio 20. SSID Manager 3(3).

Network Interface -valikon (kuvio 21) alta löytyvät Radio0- ja Radio1-valikot, joiden alta päästään säätämään langattomien lähettimien asetuksia erittäin yksityiskoh-  
 taisesti. Eri asetuksia on kymmeniä, niiden säädöt riippuvat käyttökohteesta ja tar-  
 koituksesta, joten asetuksia ei tässä eritellä.



Kuvio 21. Langattomien lähettimien asetukset.

## 6.2 Käyttöönotto ja kytkentä

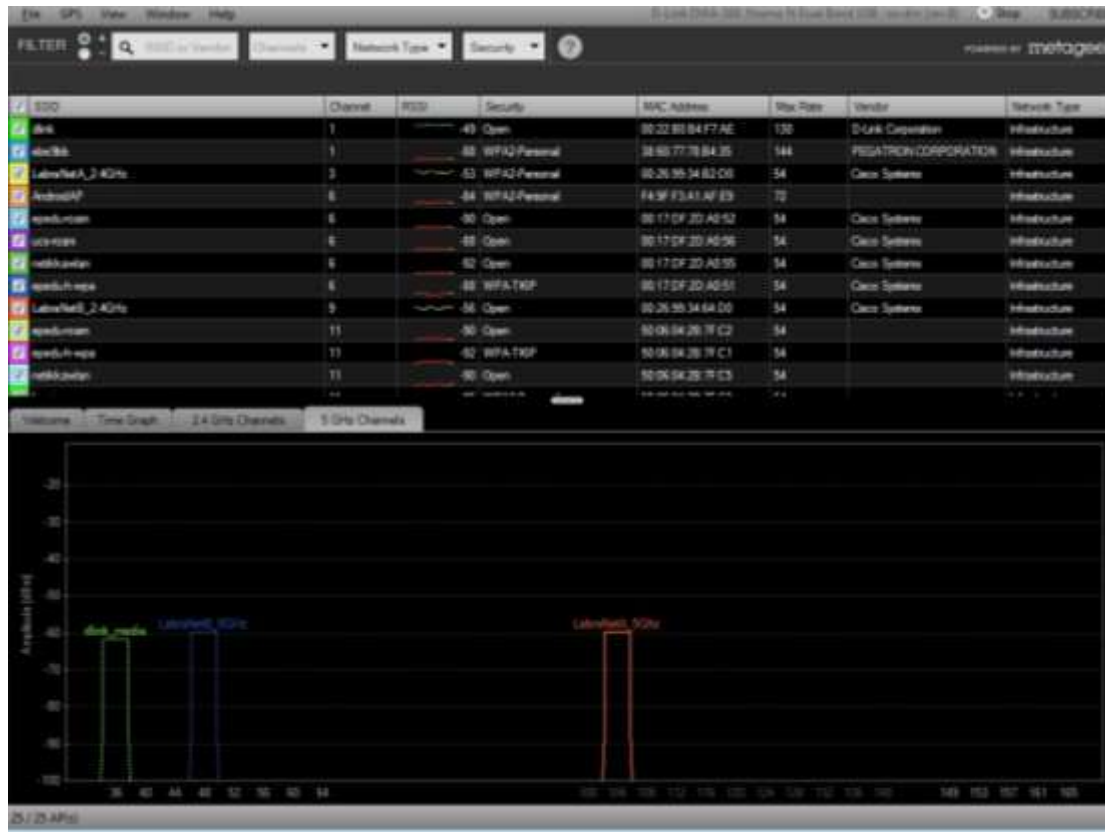
Käyttöönoton kannalta on tärkeää skannata lähistöltä löytyvät verkot. Kuvio 22 nähdään että 2,4 GHz:n taajuusalue on hyvin ruuhkainen, joten käytettävä kanava kannattaa valita huolella. 2,4 GHz:n taajuudelle valittiin kanavat 3 ja 9, sillä ne osuivat suhteellisen vapaaseen kanava-alueeseen.



Kuvio 22. inSSIDer 2,4 GHz:n taajuus.

Vastaavasti 5 GHz:n taajuusalue on hyvin ruuhkaton. Ruuhkattomuus johtuu osittain 5 GHz:n heikommasta kantamasta ja osittain matalemmasta suosiosta 2,4

GHz:n taajuuteen nähden. Käytettävässä laitteessa 5 GHz:n taajuudella ei kana-  
vaa voinut itse valita, vaan laite skannasi automaattisesti ympäristössä olevat ver-  
kot ja teki kanavavalinnan sen mukaan. Laite valitsi kanavat 48 ja 104. Kuviosta  
23 nähdään, että 5 GHz:n taajuudelta ei löytynyt kuin Tietoliikennetekniikan labo-  
ratoriossa olevat laitteet.

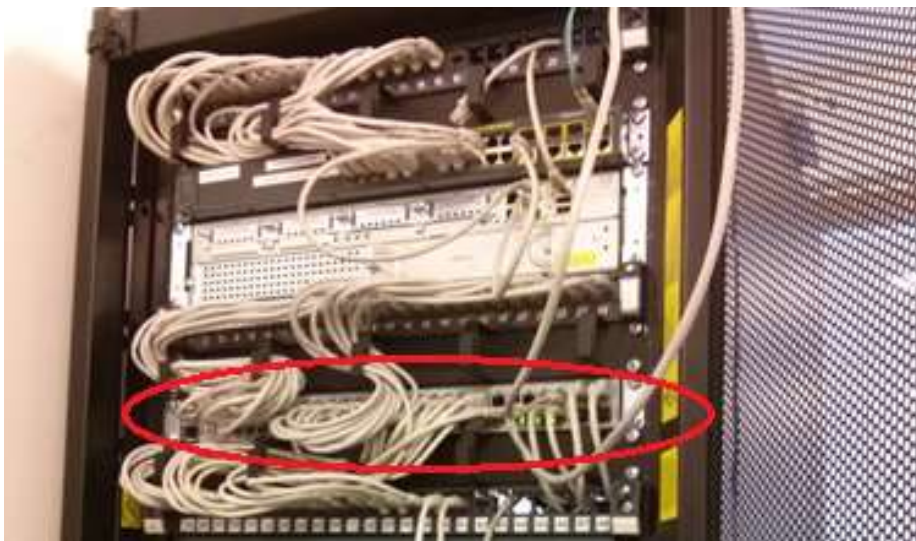


Kuvio 23. inSSIDer 5 GHz:n taajuus.

Tietoturva-asetuksista valittiin salaustavaksi TKIP ja autentikointitavaksi valittiin WPA2 ja WPA Pre-shared Key. Pre-shared Keyksi, eli langattoman verkon sa-  
lasanaksi sovittiin sellainen salasana, joka on helposti muistettava, muttei liian yk-  
sinkertainen.

Itse kytkennän suorittaminen on erittäin suoraviivaista sen jälkeen, kun konfigu-  
rointi on suoritettu. Labranet-järjestelmä on käyttövalmis ja HP:n kytkin (johon Ai-  
ronet-laitteet kytketään) ja sen portit olivat valmiiksi konfiguroituja. Ensiksi Ai-  
ronetin Ethernet-porttiin kytketään RJ45-kaapeli, sitten valitaan HP:n kytkimestä  
vapaa portti ja kytketään RJ45-kaapelin toinen pää siihen. Tämän jälkeen laitteet  
ovat käyttövalmiina. HP:n kytkin on ympyröitynä kuviossa 24. Aironet 1131AG

-laitteet päätettiin sijoittaa siten, että toinen jäi varastotilaan rakkikaapin päälle (kuvio 25), ja toinen siirrettiin laboratorion puolelle johtohyllyn päälle (kuvio 26).



Kuvio 24. HP:n kytkin.



Kuvio 25. Aironet-tukiasema rakkikaapin päällä.



Kuvio 26. Aironet-tukiasema johtohyllyn päällä.

## 7 YHTEENVETO

Tässä opinnäytetyössä rakennettiin langaton lähiverkko osaksi Seinäjoen Ammattikorkeakoulun Labranet-järjestelmää. Labranet on ammattikorkeakoulun opiskelijoiden rakentama järjestelmä, joka on tarkoitettu tietoliikennetekniikan opiskelijoiden käyttöön harjoitustöitä ja kytkeviä tehdessä.

Työssä käytettiin kahta Cisco Aironet 1131AG Access Point -laitetta. Laitteista löytyy tuki 2,4 GHz:n ja 5 GHz:n taajuuksille, ja se tukee molempien taajuuksien yhtäaikaista käyttöä.

Laitteisto konfiguroitiin luokkaympäristöön sopivaksi ja kanaviksi valittiin sellaiset kanavat, jotka olivat mahdollisimmat ruuhkattomat, tässä tapauksessa kanavat 3 ja 9 2,4 GHz:n verkossa ja 5 GHz:n verkossa laite itse valitsi sopivat kanavat 48 ja 104.

Laitteille valittiin konfiguroimisen jälkeen sopivat loppusijoituspaikat. Toinen Cisco Aironet 1131AG jäi rakkikaapin päälle tietoliikennetekniikan laboratorion perällä olevaan varastotilaan. Toinen laite sijoitettiin laboratorion puolelle johtohyllyn päälle.

## 8 POHDINTA

Opinnäytetyö oli mielenkiintoinen. Työ oli hyvää harjoitusta, sillä työtä tehdessä oppi konfiguroimaan muitakin Ciscon laitteita kuin peruskytkimiä. Tavoitteena oli saada toimiva langaton tiedonsiirtojärjestelmä osaksi Labranet-järjestelmää ja tässä onnistuttiin osittain.

Koululta lainattuun Aironet-tukiasemaan tutustuttiin ensin kotona. Tämä helpotti kytkentöjen ja konfiguroinnin tekemistä koululla, kun laitteet olivat jo osittain tuttuja.

Opinnäytetyössä onnistuttiin osittain, sillä laitteiden kytkentöjä tehtäessä Labranet-järjestelmän asetuksissa oli jotain vikaa, eikä Aironet-laitteiden kautta päästy verkkoon. Vikaa etsittäessä selvisi, ettei DNS-palvelin vastannut lainkaan ja se esti langattomien laitteiden pääsyn verkkoon. Kun toinen laitteista siirrettiin uuteen kytkentärasiaan, ja kytkimen portti vaihtui, verkkoyhteys alkoi toimia normaalisti. Tästä voidaan tehdä johtopäätös, että joku oli konfiguroinut kytkimen loppupään portit (ne portit joita käytettiin laitteiden konfiguroimiseen ja mihin toinen laite jätettiin kinni) erilailla kuin alkupään portit johon toinen laitteista siirrettiin.

DNS-palvelimen vastaamattomuus tuotti kytkentävaiheessa aika paljon päänvaihua ja ylimääräistä työtä, sillä ensin luultiin, että laitteet oltiin konfiguroitu väärin kun yhteys ei toiminut aluksi. Asiaa selvitettiin ja huomattiin, että ensisijainen DNS-palvelin ei vastannut lainkaan pingaukseen (ping). Yritimme Alpo Anttosen kanssa selvittää mistä vika johtui, mutta emme saaneet asiaan selvyyttä. Hän sanoi tutkivansa, että onko Labranetin asetuksia muutettu.

Kokonaisuudessaan työ oli hyvää harjoitusta, kun tuli ongelmiaakin vastaan, niin sai kehittää omia vianselvitystaitojaan.

## LÄHTEET

- Cisco 2010. Cisco IOS Software Configuration Guide for Cisco Aironet Access Points. [Verkkosivu]. Cisco Systems. [Viitattu 24.4.2015]. Saatavissa: [http://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/12-4\\_10b\\_JA/configuration/guide/scg12410b/scg12410b-chap19-wgb-standby.html](http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4_10b_JA/configuration/guide/scg12410b/scg12410b-chap19-wgb-standby.html)
- Cisco 2013a. Cisco Aironet 1130 AG Access Point. [Verkkosivu]. Cisco Systems. [Viitattu 24.4.2015]. Saatavissa: <http://www.cisco.com/c/en/us/support/wireless/aironet-1130-ag-access-point/model.html>
- Cisco 2013b. Quick Start Guide Cisco Aironet 1130 AG Access Point. [Verkkosivu]. Cisco Systems. [Viitattu 24.4.2015]. Saatavissa: [http://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/1130/quick/guide/ap1130qs.html](http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1130/quick/guide/ap1130qs.html)
- Data Communications. 2008. DSSS-Periaate. [Viitattu 22.5.2015]. La Trobe University. Saatavissa: <http://ironbark.xtelco.com.au/subjects/DC/lectures/22/>
- Gadgets. Ei päivystä. Google Nexus 4. [Verkkosivu]. NDTV. [Viitattu 27.4.2015]. Saatavissa: <http://gadgets.ndtv.com/lg-nexus-4-781>
- Google Play. 2015. Wifi Analyzer. [Verkkosivu]. Google Inc. [Viitattu 12.5.2015]. Saatavissa: <https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=fi>
- Granlund, K. 2001. Langaton tiedonsiirto. Jyväskylä: Docendo.
- Granlund, K. 2007. Tietoliikenne. Jyväskylä: Docendo.
- Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Jyväskylä: Docendo.
- HP. 2013. HP Pavilion 15-E058SO -kannettava. [Verkkosivu]. Hewlett-Packard Development Company, L.P. [Viitattu 27.4.2015]. Saatavissa: <http://support.hp.com/fi-fi/product/HP-Pavilion-15-Notebook-PC-series/5355006/model/5389991>
- Instructables. 2011. Cisco RJ45 DB-9 console cable. [Verkkosivu]. Autodesk, Inc. [Viitattu 24.4.2015]. Saatavissa: <http://www.instructables.com/id/Simple-RJ45-DB9-Cisco-console-cable/>

- Korpela, J. 2002. PuTTY-ohjelman asetukset – vinkkejä. [Verkkosivu]. Datatekniikka ja viestintä. [Viitattu 25.4.2015]. Saatavissa: <https://www.cs.tut.fi/~jkorpela/putty.html>
- Metageek. 2015. inSSIDer. [Verkkosivu]. MetaGeek, LLC. [Viitattu 12.5.2015]. Saatavissa: <http://www.metageek.com/products/inssider/>
- Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Talentum media Oy.
- Rackely, S. 2007. Wireless Networking Technology: From Principles to Successful Implementation. [Verkkokirja]. Newnes. Saatavissa: <http://home.ustc.edu.cn/~wfsun/lab/course/wireless/Steve%20Rackley%20-%20Wireless%20Networking%20Technology.pdf>
- Saari, J., Antila, A., Kivimäki, T., Uusitalo, V. & Ketelimäki, J. 2013. SeAMK Labranet. Seinäjoen ammattikorkeakoulu. Projektityö. Julkaisematon.
- Techspot. 2015. inSSIDer. [Verkkosivu]. Techspot, Inc. [Viitattu 12.5.2015]. Saatavissa: <http://www.techspot.com/downloads/5936-inssider.html>

## LIITTEET

Liite 1. SeAMK LabraNetin PacketTracer piirros

## LIITE 1 SeAMK LabraNetin PacketTracer piirros

