Useamman SSID:n langaton verkko ja Radius-palvelin

Toteutus Itä-Uudenmaan koulutuskuntayhtymässä

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulututkinnon opinnäytetyö

Tietotekniikan ko.

Riihimäki,

Jesse Koskelainen

OPINNÄYTETYÖ

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma
Riihimäki

Työn nimi	Useamman SSID:n langaton verkko ja Radius-palvelin
Tekijä	Jesse Koskelainen
Ohjaava opettaja	Raimo Hälinen
Hyväksytty	_____._____.20_____

Hyväksyjä

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikan ko.
Tietoliikennetekniikan suuntautumisvaihtoehto

Tekijä Jesse Koskelainen **Vuosi** 2010

Työn nimi Useamman SSID:n langaton verkko ja Radius-palvelin

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli luoda Itä-Uudenmaan koulutuskuntayhtymälle yhdenmukainen WLAN-verkko kaikkiin toimipisteisiin. Tietoliikenneyhteyksien luotettavuuden takaamiseksi, langallinen verkko tulee kumminkin olemaan ensisijainen verkko.

Tavoitteena oli muodostaa useampia langattomia verkkoja, joissa on eri SSID:t. Siten voidaan rajata erilaisia käyttäjäympäristöjä. Tällöin asiattomat eivät pääse kirjautumaan verkkoon ilman käyttäjätunnuksia, mutta niin sanottu vierailijaverkko suodaan kaikille.

Alun perin vierailijaverkon SSID-tunnus piti näkyä kaikille. Mutta kohtaamista ongelmista johtuen myös se jouduttiin piilottamaan. SSID:n piilotusta ei voida kumminkaan pitää periaatteessa minkäänlaisena suojauksena. Tämän takia on tärkeää suojata langaton verkko tarpeeksi vahvalla suojauksella sekä Radius-palvelimella.

Teoriaosioon tutustuttiin lähinnä Ciscon langattoman verkon kurssimateriaalien pohjalta. Langattoman tukiaseman ohjekirjaa ja internetiä hyväksikäyttäen luotiin ensin muusta verkosta eristetty testausympäristö. Onnistuneiden testauksien jälkeen siirryttiin viralliseen verkkoympäristöön.

Monien ongelmavaiheiden ja muutamien kompromissien jälkeen langaton verkko saatiin kuitenkin onnistuneesti toteutettua. Tulevaisuudessa langattomien tukiasemien määrän kasvaessa on suositeltavaa alkaa käyttämään keskitettyä hallintaa.

Avainsanat WLAN, SSID, Radius, HP 420 AP, MSM

Sivut 33 s, + liitteet 10 s

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Riihimäki
Degree Programme in Information Technology
Information Technology

Author Jesse Koskelainen **Year** 2010

Subject of Bachelor's thesis A multiple SSIDs wireless network and Radius server

ABSTRACT

The purpose of this thesis was to create uniform wireless network to all offices in a municipal education federation. To ensure the reliability of data communications, a wired network will be still the primary network.

The aim was to create wireless networks, which have different SSIDs. Thus it is possible to define different user environments, and unauthorized persons cannot log in without a specified account. However, guest network are still nevertheless available to everyone.

Initially a guest network's SSID should have been visible to everyone, but due to some problems it has also had to be hid. Nevertheless hiding the SSID does not basically give any kind of protection. For this reason it is very important to secure the wireless network with protection that is high enough and a Radius server.

The theoretical part was obtained mostly from Cisco's wireless network course materials. The test environment, which was isolated from a real network, was created using the wireless access point manual and the Internet. After successful tests, the test environment was moved to a real network environment.

After many problems and a couple of compromises, the wireless network was finished successfully. In the future if the quantity of wireless access points rises, it is recommended to start using centralized management.

Keywords WLAN, SSID, Radius, HP 420 AP, MSM

Pages 33 p + appendices 10 p

LYHENTEET

802.1X - Port Based Authentication - Porttikohtainen todentaminen, estää luvattomien laitteiden kommunikoinnin

AD - Active Directory - Windows palvelinympäristössä käytetty käyttäjä- ja laitetietokanta

AES - Advanced Encryption Standard - Toistaiseksi murtamaton salausmenetelmä

CLI – Command Line Interface – Komentopohjainen käyttöliittymä

DHCP - Dynamic Host Configuration Protocol - Jakaa IP-osoitteita uusille verkkoon kytkeytyville laitteille

DNS - Domain Name System - Järjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi

DSSS - Direct Sequence Spread Spectrum – Suorasekventointi, modulointimenetelmä

ETHERNET - Yleisin ja ensimmäisenä laajasti hyväksytty lähiverkkotekniikka

IAS - Internet Authentication Service – Microsoftin oma vastine Radius-palvelimelle

IEEE - Institute of Electrical and Electronics Engineers – Suuri kansainvälinen tekniikan alan järjestö

IP - Internet Protocol - Huolehtii IP-pakettien toimittamisesta perille

MAC-address - Media Access Control – Yksilöllinen tunniste verkkokorteille

MIMO - Multiple Input, Multiple Output – Langattomassa tiedonsiirrossa käytetään hyödyksi useampaa antennia

MSM – MultiService Mobility – Hp:n uusin keskitettyä hallintaa tukeva standardi

NPS – Network Policy Server – IAS:n seuraaja Windows Server 2008:ssa

OFDM - Orthogonal Frequency Division Multiplexing – Modulointimenetelmä, jossa tiedonsiirto tapahtuu toisiaan häiritsemättömillä taajuuskanavilla samaan aikaan

OU – Organizational Unit – Organisaatioyksikkö AD:ssa, jolla voidaan rajata esimerkiksi eri alueita

PING - Työkalu, jolla voidaan testata eri laitteiden saavutettavuutta

PoE – Power over Ethernet – Laite saa tarvitsemansa virtansa Ethernet-verkkoa pitkin

PSK – Pre-Shared Key – Ennalta määritetty salasana

QoS - Quality of Service – Tietoliikenteen priorisointia halutulla tavalla

RADIUS - Remote Authentication Dial In User Service – Käyttäjien ja laitteiden tunnistuspalvelu

SSH – Secure Shell – Salattu etäyhteys-protokolla

SSID - Service Set Identifier – Verkkotunnus, joka yksilöi langattomat lähiverkot toisistaan

TKIP - Temporal Key Integrity Protocol – WEP-protokollan seuraaja

VLAN - Virtual LAN – Tämän avulla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin

WEP - Wired Equivalent Privacy – Nykyään jo heikko salausmenetelmä

WLAN - Wireless Local Area Network – Langaton lähiverkko

WPA - Wi-Fi Protected Access – WEP-salauksen seuraaja

WPA2 - Wi-Fi Protected Access – WPA-salauksen päivitetty versio

SISÄLLYS

1 JOHDANTO

Langattoman verkon suosio kasvaa entisestään, varsinkin lähitulevaisuudessa n-standardia tukevien laitteiden myötä. N-standardissa nopeudet kasvavat jo langallisen verkon tasolle. Radiosignaalin kantomatka pitenee myös huomattavasti verrattuna edellisiin standardeihin.

Langaton verkko koostuu neljästä fyysisestä päätekijästä. Näitä ovat langaton tukiasema, hallittava kytkin, palvelin ja käyttäjän tietokone.

Hallittavassa kytkimessä on asetettu langattomalle verkolle omat VLANIT, portit ja niiden ohjaukset eteenpäin palvelimelle ja siitä edelleen ulkomaailmaan. Palvelimella sijaitsevat käyttäjien tiedot ja määritetyt oikeudet. Radius-autentikointipalvelu vertaa tukiaseman lähettämiä tietoja palvelimella sijaitseviin tietoihin. Tietojen täsmätessä kirjautuminen verkkoon onnistuu. Langaton tukiasema toimii yhteyspisteenä (Access Point) langatonta verkkoa käyttäville tietokoneille. Tukiasema on yhdistetty langallisesti verkkopiuhalla kytkinverkkoon.

Tulevaisuus osiossa esittelen tukiasemista kehittyneempiä laitteita, joita hallitaan keskitetysti. Tällöin verkon hallittavuus ja ylläpito helpottuvat huomattavasti. Ei siis ole aivan sama miten langattoman verkon aikoo toteuttaa.

1.1 Toimeksiantaja

Itä-Uudenmaan koulutuskuntayhtymä tarjoaa erilaisia koulutusmahdollisuuksia. Sen alaisuuteen kuuluvat Amiston, Edupolin oppilaitokset ja Itä-Uudenmaan oppisopimuskeskus. Amistolla on neljä toimipistettä, jotka sijaitsevat Askolassa, Loviisassa ja Porvoossa kaksi: Aleksanterinkadulla toimiva Pomo-talo ja päätoimipaikka Perämiehentiellä. Edupolin toimipisteet sijaitsevat Helsingissä Herttoniemessä, Sipoossa, Vantaalla ja päätoimipaikkana toimii Ammattitie Porvoossa. Lisäksi sivutoimipisteenä toimii vielä Perämiehentien toimipiste, josta löytyy myös Itä-Uudenmaan oppisopimuskeskus.

Edellä mainituille oppilaitoksille erilaisia tukipalveluita tarjoavat konsernipalvelut. Konsernipalveluihin kuuluvat seuraavat yksiköt: kiinteistöhuolto, kirjanpito, palkkatoimisto, siivous, taloushallinto ja tietotekniikka. Henkilöstöä kuntayhtymällä on kaiken kaikkiaan noin 400. Opiskelijoita on päiväkohtaisesti noin 2400, johtuen aikuiskoulutuksen varsin vaihtelevan pituisista koulutuksista.

1.2 Lukijalle

Olen yrittänyt pitää työni mahdollisimman selkeänä ja yksinkertaisena, jotta periaatteessa kuka tahansa voi ymmärtää asian sisällön. Vaikeimmissa asioissa olen laittanut kuvia helpottamaan asian ymmärtämistä. Suosittelen ennen mahdollista toteutusta lukemaan koko opinnäytetyön läpi, saadaksesi käsityksen projektin kokonaisuudesta ja vastaan tulleista ongelmista.

2 LANGATON VERKKO (WLAN)

Ennen WLAN-aikakauden alkua kaikki tietoliikenneyhteydet suoritettiin langallisesti. Tämä loi haasteita etenkin yritysmaailmassa, sillä kun haluttiin siirtyä johonkin toiseen paikkaan tai edes huoneeseen oli varmistettava, että sieltäkin löytyy seinästä verkkoyhteys sekä verkkokaapeli, jonka on oltava myös tarpeeksi pitkä. Samaten, jos yritystä haluttiin laajentaa esimerkiksi toiseen maahan. Sopivan kiinteistön löydyttyä saattoi tulla mojovasti lisähintaa, jos verkkoyhteyttä ei ollut valmiina, sillä oli pakko purkaa seinien, lattian ja katon eristeitä, jotta verkkoyhteys saatiin asennettua.

Nykyään varsin kiireiseen elämäntyyliin langattomuudesta on tullut selkeä trendi, sillä se säästää aikaa ja aikahan on vastaavasti rahaa. Langattomuus on siis otettu varsin avokätisesti ja iloisesti vastaan yhtä lailla kuin esimerkiksi kännykkäkin. (Cisco 7.0.1 Chapter Introduction.)

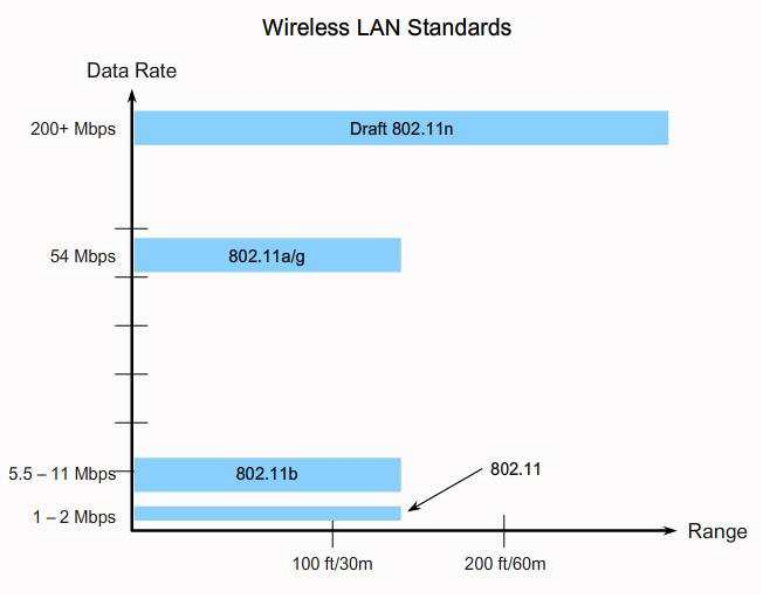
2.1 Wlan-standardit

IEEE:n määrittelemä 802.11 standardikokoelma sisältää kymmeniä eri versioita. Tässä käsitellään niistä yleisimmät, joita ovat: 802.11a, 802.11b, 802.11g ja 802.11n. 802.11 standardia esiteltäessä se kykeni 1-2 Mb/s tiedonsiirtoon 2,4GHz taajuudella, samalla kun langalliset yhteydet saavuttivat jopa 10 Mb/s, joten uusi standardi ei yleisesti herättänyt suurta kiinnostusta. Sittemmin WLAN-standardit ovat kehittyneet huomattavasti. (Cisco 7.1.2 Wireless LAN Standards.)

Tyypillisesti valinta siitä mitä WLAN-standardia käytetään, pohjautuu tiedonsiirtonopeuden tarpeeseen. Esimerkiksi 802.11a ja 802.11g pystyvät jopa 54 Mb/s siirtonopeuteen, kun taas 802.11b maksiminopeus on vain 11 Mb/s. Siirtonopeus vaihtelee standardista riippuen. Nopeuteen vaikuttaa käytettävä modulaatiomenetelmä, joita on käytössä kahta eri tyyppiä. DSSS (Direct Sequence Spread Spectrum) eli suorasekventointi, sekä OFDM (Orthogonal Frequency Division Multiplexing). Näistä kahdesta OFDM kykenee nopeampaan siirtonopeuteen, mutta DSSS on yk-

sinkertaisempi kuin OFDM, joten se on huomattavasti halvempi toteuttaa. (Cisco 7.1.2 Wireless LAN Standards.)

Seuraavasta kuvasta selviää eri WLAN-standardien nopeudet ja signaalien kantomatkat.



Kuva 1 WLAN-standardit

2.1.1 802.11a

802.11a standardissa otettiin käyttöön OFDM-modulaatiomenetelmä ja se toimii 5GHz taajuudella, 802.11a kykenee maksimissaan 54 Mb/s siirtonopeuteen. Verrattuna 2.4GHz taajuudella toimiviin laitteisiin 5GHz taajuudella toimivat häiriintyvät harvemmin, koska korkealla taajuudella toimivia laitteita on huomattavasti vähemmän. Korkea taajuus myös sallii pienemmät antennit. Korkea taajuus aiheuttaa myös huomattavia haittoja. 5GHz radiotaajuudet absorboituvat esteisiin helpommin kuin matalat radiotaajuudet, mikä voi johtaa huonoon signaalin laatuun. Korkeampi taajuus tarkoittaa myös lyhyempää kantamaa. Myös jotkin maat, kuten Venäjä eivät salli 5GHz radiotaajuuden käyttöä. (Cisco 7.1.2 Wireless LAN Standards.)

2.1.2 802.11b

802.11b kykenee maksimissaan 11 Mb/s nopeuksiin 2.4GHz taajuudella käyttäen DSSS-modulointia. 2.4GHz radiotaajuudella on muutamia etuja korkeampiin taajuuksiin nähden. 2.4GHz laitteilla on parempi kantama eikä signaali heikkene niin paljoa esteistä, kuin 5GHz käyttävät laitteet. Kääntöpuolena on, että useimmat langattomat kodinelektroniikkalaitteet käyttävät 2.4GHz taajuutta joka johtaa siihen, että nämä laitteet häiritsevät toisiaan. (Cisco 7.1.2 Wireless LAN Standards.)

2.1.3 802.11g

802.11g toimii kuten 802.11b 2.4GHz radiotaajuudella, mutta käyttää OFDM modulointia ja kykenee täten huomattavasti nopeampiin siirtonopeuksiin, jopa 54 Mb/s. Standardiin määriteltiin myös taaksepäin yhteensopivuus DSSS moduloinnille joten 802.11g laitteet toimivat 802.11b laitteiden kanssa. Kuten 802.11b on 802.11g herkkä muiden laitteiden häirinnälle johtuen käytettävästä 2.4GHz taajuudesta. (Cisco 7.1.2 Wireless LAN Standards.)

2.1.4 802.11n

802.11n on viimeisin standardi, sen uusiin ominaisuuksiin kuuluu MIMO-tekniikka, jonka avulla voidaan saavuttaa jopa yli 200 Mb/s siirtonopeus. 802.11n standardi käyttämä MIMO tekniikka perustuu siihen, että laitteissa käytetään useita antenneja ja vastaanottimia, jotka toimivat samalla taajuudella näin jakaen kuorman useammalle tietovirralle. Kuten kuvasta 1 saatoit huomata, myös radiosignaalin kantomatka on kasvanut huomattavasti edellisiin standardeihin verrattuna. Toisin kuin edelliset standardit, 802.11n laitteet voivat käyttää 5GHz tai 2.4GHz taajuuksia. (Cisco 7.1.2 Wireless LAN Standards.)

2.2 Langattoman verkon käyttö

WLAN-verkko tarjoaa sekä yrityksille, että yksityisille henkilöille useita mahdollisuuksia, mitkä eivät onnistuisi langallisella verkolla, tai ne olisivat varsin epäkäytännöllisiä. Langattomuuden parhaimpiin ominaisuuksiin kuuluu sen joustavuus, käyttäjä ei ole enää rajoitettu pysymään paikallaan. Muita hyötyjä erityisesti yrityksille ovat säästöt ja tuottavuus. Työntekijän siirto uuteen paikkaan ei ole enää rajoitettu rakennettujen

johtojen mukaan. Toinen merkittävä säästö tulee, mikäli yrityksen tulisi siirtyä rakennukseen missä ei ole lainkaan johdotusta verkolle. Yrityksen tarvitsee hankkia vain muutama WLAN-laite, että koko rakennukseen saadaan toimiva verkko, toisin kuin langallisen verkon rakennus, josta koituisi huomattavat kustannukset. (Cisco 7.1.1 Why Use Wireless?)

2.3 Langattoman verkon suunnittelu

Ennen langattoman verkon pystyttämistä on syytä suorittaa varsin perusteellinen suunnitelma ja dokumentoida se. Suunnitelman olennaisena osana toimii karttakuva sunnitellusta verkosta. Kartasta tulisi käydä ilmi, missä tukiasemat sijaitsevat ja niiden kantavuusalue. Kantavuusalue tulisi suunnitella niin, että tukiasemien verkkojen kantavuussäteet eivät lopu toistensa rajoille, vaan menevät jonkin verran myös päällekkäin. Tämä takaa käyttäjien vapaan liikkuvuuden tukiasemien välillä. Lisäksi on hyvä ottaa huomioon käyttäjien määrä suhteessa käytettävissä olevaan tiedonsiirtokaistaan.

Langattoman verkon suunnitteluun on tarjolla myös ohjelmia, johon syötetään rakennusta jäljittelevään karttaan tukiasemien sijainnit ja tämän jälkeen ohjelma simuloi tilanteen ja ehdottaa mahdolliset uudet ja paremmat sijainnit. Lisäksi ohjelma myös kertoo sen kuinka monta tukiasemaa tarvittaisiin lisää, että koko alue peittyisi.

Rakennus tai paikka, mihin WLAN-verkko on suunniteltu pystyttää, tulisi paikan päällä kartoittaa mahdolliset katvealueet ja asettaa tukiasemat niin, että mahdolliset esteet ja häiriötekijät olisi mahdollisimman hyvin minimoitu. Esimerkiksi mikroaaltouunit ja Bluetooth-laitteet käyttävät samaa taajuutta kuin langaton verkko.

Tietoturvallisuuden kannalta tukiasemat tulisi sijoittaa mieluiten niin, ettei kuka tahansa pääse huomaamattomasti langallisesti (fyysisesti) tukiasemaan käsiksi ja näin ollen pääse mahdollisesti vielä helpommin murtautumaan tukiaseman hallintaominaisuuksiin. Parhain paikka olisi siis aina korkealla joko seinällä tai katossa. (Cisco 7.1.5 Planning the Wireless LAN.)

2.4 Langattoman verkon turvallisuus

Langattoman verkon turvallisuuden takaaminen on ensisijaisen tärkeää, koska langattomuudesta johtuen periaatteessa kuka tahansa verkon kantomatkan ulottuvuudella voi yrittää kokeilla päästä käsiksi tukiaseman sisällä sijaitseviin verkon kriittisiin hallintatoimenpiteisiin. Erityisesti yritysverkoissa huoli turvallisuudesta on vieläkin merkittävämpää, sillä yrityksen salaiseksi luokiteltujen tietojen leviäminen vääriin käsiin voi ai-

heuttaa helposti suurta vahinkoa. (Cisco 7.2.1 Treats to Wireless Security.)

Salaustapoja kehitetään jatkuvasti, sillä tietokoneiden laskentakyvyn kasvaessa salauksien purkaminen käy nopeammaksi. WEP-salausta ei suositella enää käytettäväksi, koska sen salausavain ei vaihdu missään vaiheessa ja näin ollen sen pystyy helposti pienellä vaivalla saamaan selville niin sanotusti nuuskimalla (Sniffing) lähetettyjä paketteja. Pelkästään SSID:n piilotus ei myöskään auta, sillä se lähetetään salaamattomana muiden pakettien seassa, jolloin sen saa yhtä lailla nuuskimalla selville. On myös mahdollista käyttää MAC-osoitteiden suodatusta, joka antaa vain tietyille koneille oikeuden päästä verkkoon. Nykyään MAC-suodatus on kumminkin helppo ohittaa ohjelmallisesti väärentämällä oma MAC-osoite. Tilannetta voisi hyvin verrata omakotitaloon, jossa on hälytysjärjestelmä mutta silti pyytäisit poissa olleessasi naapuriasi vahtimaan taloasi. Tästä syystä on edellisten menetelmien lisäksi käytettävä uudempia suojausmenetelmiä, joista lisää seuraavaksi. (Cisco 7.2.2-7.2.3 Wireless Security Protocols, Securing a Wireless LAN.)

2.4.1 WPA (WiFi Protected Access)

WPA-standardi kehitettiin paikkaamaan heikon WEP-salauksen aiheuttamia tietoturva-aukkoja. WPA-suojauksen yhteydessä tuli mahdollisuus käyttää TKIP-salaustapaa. WPA:lle on myös valittavissa AES-salaustapa, mutta toimiakseen se voi vaatia rautatason päivityksiä. WPA:lle on määritelty erikseen koti- ja yrityskäyttöön omat vaihtoehdot. (Say No to WEP, And Yes to WPA)

WPA Personal käyttää PSK (Pre-Shared Key) salauksessa määritellään ennakkoon salasana, jolla kirjaudutaan langattomaan verkkoon. Kyseinen menetelmä sopii lähinnä kotikäyttöön.

WPA Enterprisen myötä tietoturvallisuus paranee entisestään Radius-palvelimen ja käyttäjätunnistuksen avulla. Kyseistä menetelmää käytetään lähinnä yrityksissä. Kyseiset menetelmät ovat valittavissa myös WPA2:ssa. (WPA Personal vs. Enterprise?)

2.4.2 WPA2

Normaali WPA ei täyttänyt täysin IEEE:n määrittelemän 802.11i-standardin ominaisuuksia, jolloin luotiin päivitetty versio. Suurin ero WPA:n ja sen 2. version välillä on niiden käyttämät salausmekanismit. WPA:n käyttäessä TKIP:tä WPA2 käyttää AES:ää. WPA2 on myös taakaisinyhteensopiva WPA:n kanssa. WPA2 + AES yhdistelmä on tällä hetkellä tehokkain ja turvallisin menetelmä. Huomioitavaa on myös, että

kaikista vanhoista laitteista ei valitettavasti löydy uusinta WPA2 + AES salausvaihtoehtoa jolloin suositeltava salaus on vähintään tasoa WPA + TKIP. (A Warm Welcome to WPA2)

2.4.3 Langattomat verkot ja terveys

Luonnollisesti, koska langattomat verkot toimivat radioaalloilla, ne myös lähettävät säteilyä. Tarkemmin ottaen syntyy sähkömagneettisia kenttiä, joita löytyy myös ihan luonnosta kuten esimerkiksi aurinko, salamat ja maapallon oma magneettikenttä. Säteilyn vaikutuksia ihmiseen on tutkittu jo useampi vuosikymmen ja tutkimusten perusteella erilaisille säteilyä lähettäville laitteille on säädetty tietyt raja-arvot, joita ne eivät saa ylittää.

Seuraavassa on suora lainaus STUK:in eli säteilyturvakeskuksen sivuilta, jossa kysyjä on ollut huolissaan langattoman verkon lähettämästä säteilystä.

”**Meille kotiin on asennettu tietokoneita varten langaton verkko tukiasemineen. Minkälaista säteilyä tukiasema lähettää? Voiko kannettavan tietokoneen kanssa työskentely olla vaarallista?”**

”Langattoman verkon (WLAN) tukiasema lähettää mikroaaltoja hyvin pienellä teholla. Metrin etäisyydellä tukiasemasta tehotiheys on noin 1/2000 ja viiden metrin etäisyydellä noin 1/10000 väestön altistumisen enimmäisarvosta.
Yhteys on kaksisuuntainen eli kannettava tietokone lähettää samalla teholla, mutta vain silloin, kun dataa tai puhetta lähetetään. Kannettavan antennihan on käytännössä lähempänä käyttäjän kehoa. Sylimikron aiheuttama altistuminen on arviolta viidesosa väestön altistumisen enimmäisarvosta. Matkapuhelimen aiheuttama altistuminen on tyypillisesti maksimimissaan noin puolet enimmäisarvosta, ja se kohdistuu yleensä päähän, kun sylimikron WLAN-portin säteily kohdistuu lähinnä reisiin.

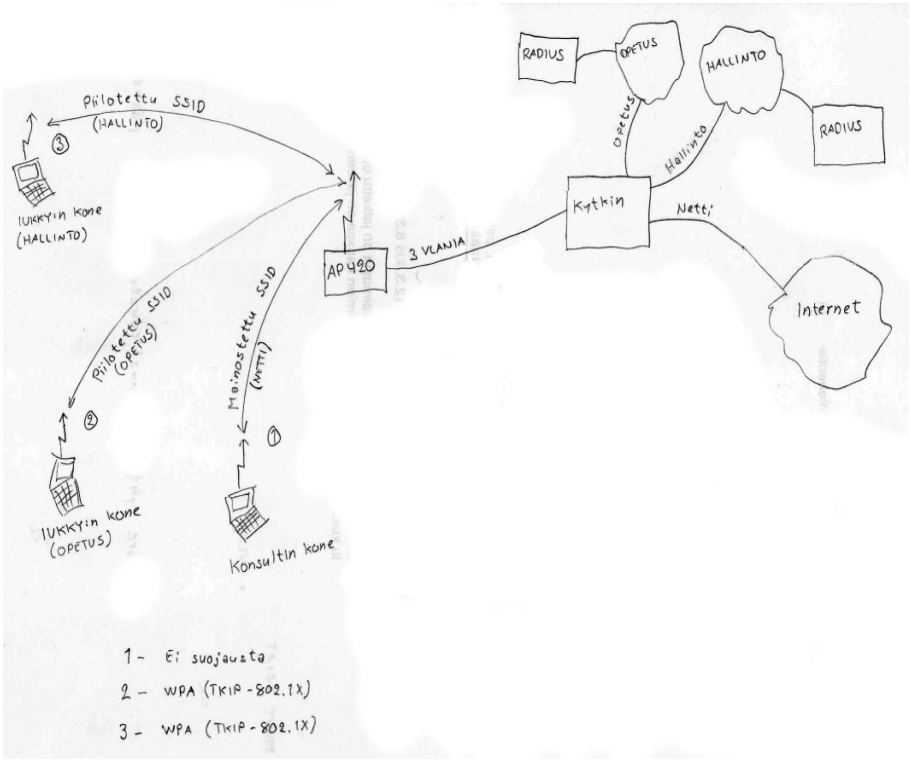
Langattoman lähiverkon ja sylimikron WLAN-portin aiheuttamasta mikroaaltosäteilystä ei ole terveydellistä haittaa.” (STUK – Usein kysytyt kysymykset)

Vastauksesta käy siis ilmi, että on täysin turvallista käyttää langatonta verkkoa. Tästä huolimatta epäilijöitä aina riittää.

3 LANGATON TUKIASEMA JA KYTKIN

Käytännön toteutus koostuu neljästä fyysisestä päätekijästä (Kuva 2). Näitä ovat langaton tukiasema (HP Procurve Wireless Access Point 420),

hallittava kytkin (HP Procurve Switch 5304XL), palvelin (Windows Server 2008) ja käyttäjän tietokone (Windows XP Professional).



Kuva 2 Projektin suunnitelma

3.1 Langattoman tukiaseman ominaisuudet (HP Procurve Wireless AP 420)

HP Procurve Wireless AP 420 (Kuva 3) on langaton tukiasema, joka on suunniteltu suuriin sekä keskisuuriin verkkoympäristöihin. Kyseisessä tukiasemassa on myös elinikäinen takuu. (HP 420, Datasheet, 1-2.)

Tukiasema tukee kahta eri langatonta verkkostandardia eli 802.11b, 802.11g ja lisäksi näiden kahden samanaikaista yhdistelmää. Ulkoiset antennit tuovat lisää kantomatkaa tukiaseman lähettämälle signaalille ja entistä parempaa suorituskykyä lähietäisyydelle. Tukiasemaa on mahdollista käyttää ilman verkkovirtaa, sillä se tukee PoE-tekniikkaa. Tällöin tukiasema saa kaiken tarvitsemansa virran ainoastaan verkkokaapelin kautta. Tukiaseman suojausasetuksista löytyy WEP, WPA ja uusin WPA2-tason suojaus. Kahden viimeisimmän mainitun suojaustavan ohessa salauksena käytetään joko AES- tai TKIP-salausta. Näiden kahden salaustavan ohella on suositeltavaa käyttää myös jotain EAP:n neljästä eri autentikointiprotokollasta kuten: MD-5, TLS, TTLS tai PEAP. (HP 420, Datasheet, 2.)

Kyseinen tukiasema tukee enintään jopa kahdeksaa eri SSID:tä. Tämän takia se soveltuu hyvin suuriin yrityksiin, joissa on useita eri toimialueita. Useamman SSID:n langaton verkko mahdollistaa jokaiselle eri SSID:lle omat suojausasetukset ja ennen kaikkea voidaan määrittää jokaiselle SSID:lle erikseen käyttäjien oikeudet tiettyihin resursseihin palvelimen group policyjen avulla. (HP 420, Datasheet, 2.)

Kuva 3 HP Procurve Wireless AP 420

3.2 Langattoman tukiaseman asetukset (HP Procurve Wireless AP 420)

Nämä asetukset toimivat HP Procurve Wireless Access Point 420 tyyppisessä langattomassa tukiasemassa. Kyseisen tukiaseman valmistus on kylläkin lopetettu marraskuussa 2009. Mallin sivuilta löytyy korvaava vaihtoehto. (HP Procurve 420)

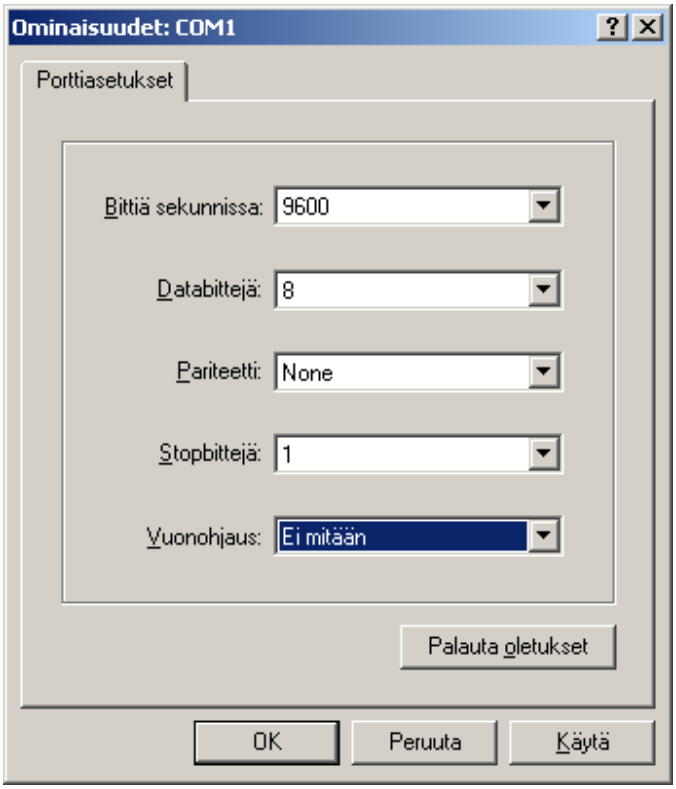
Pienellä vaivalla ja oman langattoman tukiaseman ohjekirjaa apuna käyttäen seuraavat kohdat asetuksista uskoisin löytyvän myös muista vastaavanlaisista langattomista tukiasemista. Komentojen ja valintojen selkeyttämiseksi olen lihavoinut ne.

3.2.1 Command Line Interface (CLI)

Aivan aluksi tukiasemaan on kiinnitettävä konsolikaapeli ja kaapelin toinen pää tietokoneen COM1 porttiin, sillä tukiaseman radiosignaalia ei saa asetettua päälle ennen kuin oman maatunnuksen on käynyt valitsemassa Command Line Interface (CLI) kautta. Maatunnus määrittelee tukiasemalle maakohtaiset maksimi taajuus- ja lähetystehorajat. Myös Ethernet eli verkkokaapeli on hyvä olla kiinni tietokoneen sekä tukiaseman välissä, sillä sitä tarvitaan myöhemmin Web-käyttöliittymässä.

Yhteys tukiasemaan luodaan esimerkiksi **Hyperterminal**-ohjelman tai jonkin muun vastaavan tietoliikenneporttiohjelman avulla. (IP-osoitteen asettamisen jälkeen myös Telnet- ja SSH-yhteys ovat mahdollisia). Valitaan tietokoneen vasemmasta alareunasta *Käynnistä → Ohjelmat → Apuohjelmat → Tietoliikenneyhteydet → Hyperterminal* (Management and Configuration Guide for HP 420, 28-29.)

Luodaan uusi yhteys antamalla sille jokin nimi. Painetaan **OK**. Valitaan **Yhdistä käyttäen**: COM1 Painetaan **OK**. Porttiasetukset laitetaan Kuvan 4 tavalla ja painetaan **OK**.



Kuva 4 Porttiasetukset

Avautuvassa konsoli-ikkunassa painetaan **Enter**, jolloin tukiasema kysyy käyttäjätunnuksen ja salasanan. Kirjautumisen jälkeen kirjoitetaan **configure**, jolloin siirrytään global configuration modeen ja saadaan enemmän oikeuksia ja komentoja käyttöön. Kirjoitetaan **country ?**, tämä komento listaa maat aakkosjärjestyksessä sekä kertoo niiden koodit esim. Suomi = FI. Tämän jälkeen kirjoitetaan uudestaan **country** ja kysymysmerkin tilalle lisätään **FI**. Tämä operaatio vaatii tukiaseman uudelleenkäynnistymistä. Huomioitavaa on, että maatunnuksen vaihtaminen toiseen maatunnukseen ei onnistu ilman tehdasasetuksien palauttamista! CLI-tilassa asetuksia ei tarvitse erikseen tallentaa, sillä tallennus tapahtuu automaattisesti. (Management and Configuration Guide for HP 420, 30-32, 216-218.)

Tukiaseman IP-osoite löytyy yleensä tukiaseman ohjeista mutta sen saa helposti selville global configuration mode:ssa kirjoittamalla **interface ethernet** + **Enter** ja sen jälkeen **show**. Ethernetin IP-osoitetta tarvitaan seuraavassa web-käyttöliittymä kohdassa. Kaikki loput asetukset saa siis asetettua web-käyttöliittymän kautta, jos konsoliympäristö ei innosta. (Kuten allekirjoittanutta ☺). (Management and Configuration Guide for HP 420, 297-298.)

3.2.2 Web-käyttöliittymä

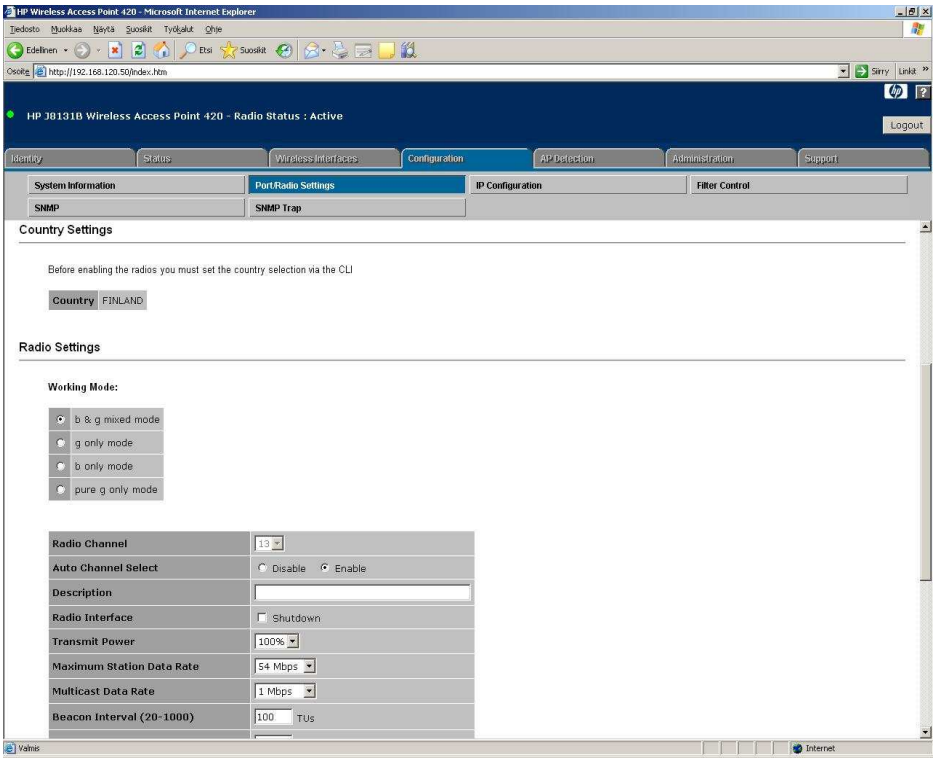
Web-käyttöliittymä on paljon helppokäyttöisempi kuin konsolipohjainen käyttöliittymä, sillä Web-käyttöliittymässä ei tarvitse kirjoittaa niin paljoa, kun voi käyttää apuna hiirtä asetuksien valitsemisessa. Lisäksi näytölle mahtuu enemmän asetuksia kerralla ja myös niiden raja-arvot ovat valmiina pudotusvalikoissa. (Management and Configuration Guide for HP 420, 26.)

Web-käyttöliittymään pääsee käsiksi, minkä tahansa valmistajan selaimen kautta. Osoiteriville kirjoitetaan tukiaseman IP-osoite, painetaan **Enter** ja syötetään tukiaseman käyttäjätunnus ja salasana. (Management and Configuration Guide for HP 420, 48.)

Kaikkien haluttujen muutoksien jälkeen painetaan jokaisen sivun alareunassa olevasta **Apply Changes** painikkeesta. (Huomioi, että en ole aivan jokaista tukiaseman asetusta käynyt lävitse, vain toteutuksen kannalta tärkeimmät. Lisätietoja tarvittaessa kyseisen tukiaseman ohjeesta)

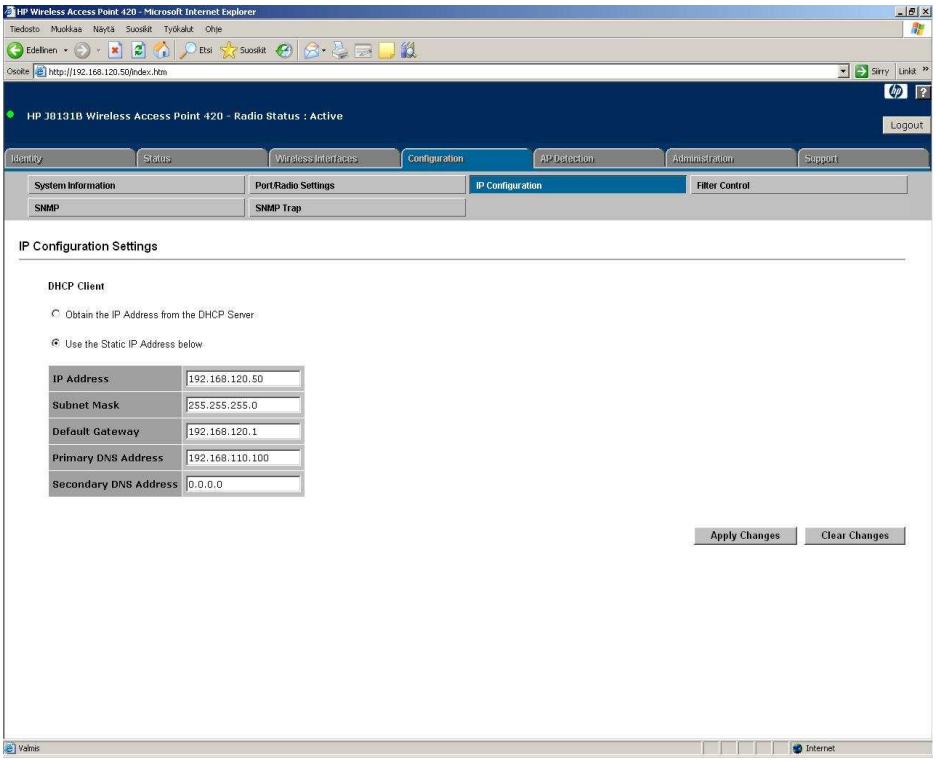
Aivan aluksi on hyvä mennä vaihtamaan tukiaseman kirjautumistiedot. Käyttäjänimen ja salasanan vaihto tapahtuu **Administration** osiosta **User** välilehdeltä. **Edit Existing User** kohdasta pyyhitään oletukset pois. Tämän jälkeen syötetään uudet tunnukset ja painetaan **Update**. Lisäksi **Configuration** osion **System Information** välilehdeltä voi vaihtaa tukiaseman nimen, sillä myöhemmin useampia tukiasemia muokatessa on hyvä tietää onko oikeassa tukiasemassa kiinni. (Management and Configuration Guide for HP 420, 52-53, 86.)

Configuration välilehden kohdasta **Port/Radio Settings** osiosta käydään ottamassa **Radio Interface** kohdasta **Shutdown** ruksi pois. Näin yläreunassa oleva **Radio Status** muuttuu **Active** tilaan ja langaton tukiasema herää eloon (Kuva 5). Tarvittaessa radiokanavan voi muuttaa haluamakseen vaihtamalla **Auto Channel Select** kohdan Disable-tilaan ja tämän jälkeen valitsemalla **Radio Channel** kohdasta haluamansa kanavan. (Management and Configuration Guide for HP 420, 57-58.)



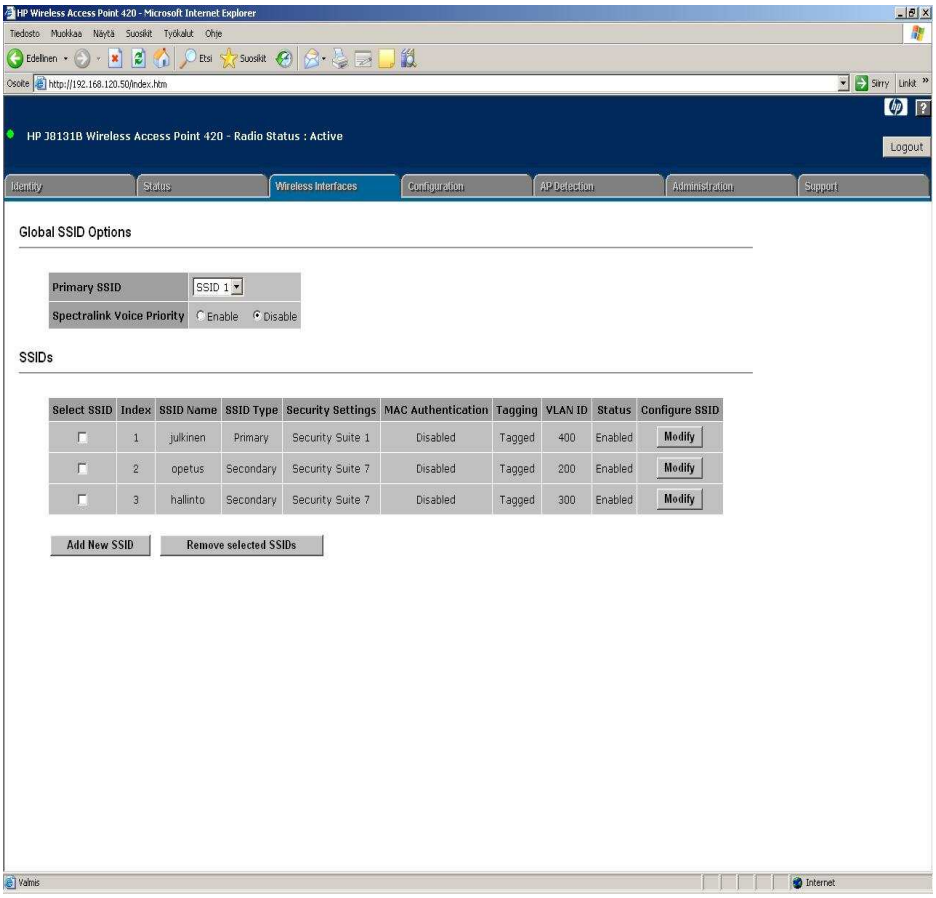
Kuva 5 Portti- ja radioasetukset

Seuraavaksi valitaan viereinen **IP configuration** kohta (Kuva 6). Täällä valitaan vaihtoehto 2: **Use the Static IP address below**, jolloin tukiasema saa määritetyn kiinteän IP-osoitteen. Tämä siksi, että tukiasemaan saadaan aina tarvittaessa yhteys samalla tutulla osoitteella. Huomioi muutoksien hyväksymisen jälkeen, että et enää pääse vanhalla IP-osoitteella tukiasemaan käsiksi. (Management and Configuration Guide for HP 420, 58-59.)



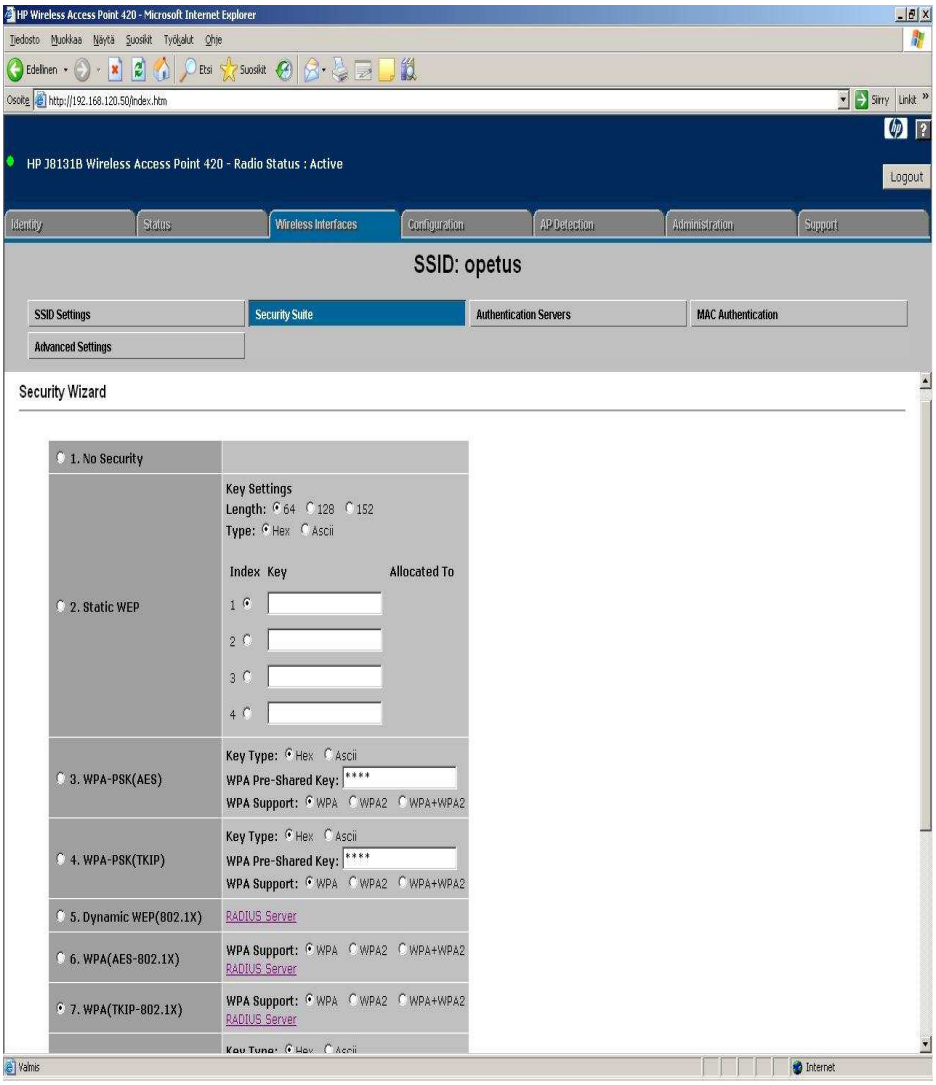
Kuva 6 IP-asetukset

Tämän jälkeen mennään **Wireless Interfaces** välilehdelle. Painetaan **Add New SSID**. Laitetaan ruksit **Enable SSID** ja **VLAN Tagging** kohtiin. **SSID Name** kohtaan lisätään kyseiselle SSID:lle haluttu nimi ja **VLAN ID** kohtaan numero mihin VLAN:iin kyseinen yhteys on tarkoitus yhdistää. Kohdan tyhjäksi jättäminen yhdistää käyttäjän oletus-VLAN:iin (VLAN=1). RADIUS-palvelimelle ja välissä olevalle kytkimelle tulee asettaa myös samat VLAN:it, jotta yhteys löytää perille. Huomioitavaa on, että ainoastaan yhden SSID.n pystyy laittamaan ensisijaiseksi (Primary), joka siis näkyy kaikille ellei ole valinnut kohtaa **Closed System**. Loput toissijaiset (Secondary) SSID:t ovat piilotettuja. Toissijaisia SSID.itä pystyy määrittämään maksimissaan 7 kappaletta. Kuvassa 7 on muodostettu testiverkkoon esimerkiksi 3 eri SSID:tä julkinen, opetus, hallinto ja niille jokaiselle on myös määritetty erinumeroiset VLAN:it. (Management and Configuration Guide for HP 420, 162-164.)



Kuva 7 Useampia SSID:tä

Muokataksesi haluttua SSID:tä painetaan **Modify**. Mennään **Security Suite** kohtaan ja valitaan suojaustapa (Kuva 8). Suositeltua on valita vähintään 6. tai 7. kohta eli **WPA (AES-802.1X)** tai **WPA (TKIP-802.1X)**, jolloin suojauksena voidaan käyttää myös RADIUS-palvelinta. Oikealta valitaan vielä salaustavaksi **WPA, WPA2** tai molempien sallittavuus **WPA+WPA2**. 6. tai 7. kohta kannattaa valita myös siksi, että ei tarvitse erikseen syöttää ennalta määritettyä salausavainta (Pre-Shared Key) vaan se luodaan automaattisesti. Tällöin myöskään langattoman verkon käyttäjien ei tarvitse itse syöttää avainta. (Management and Configuration Guide for HP 420, 179-182.)

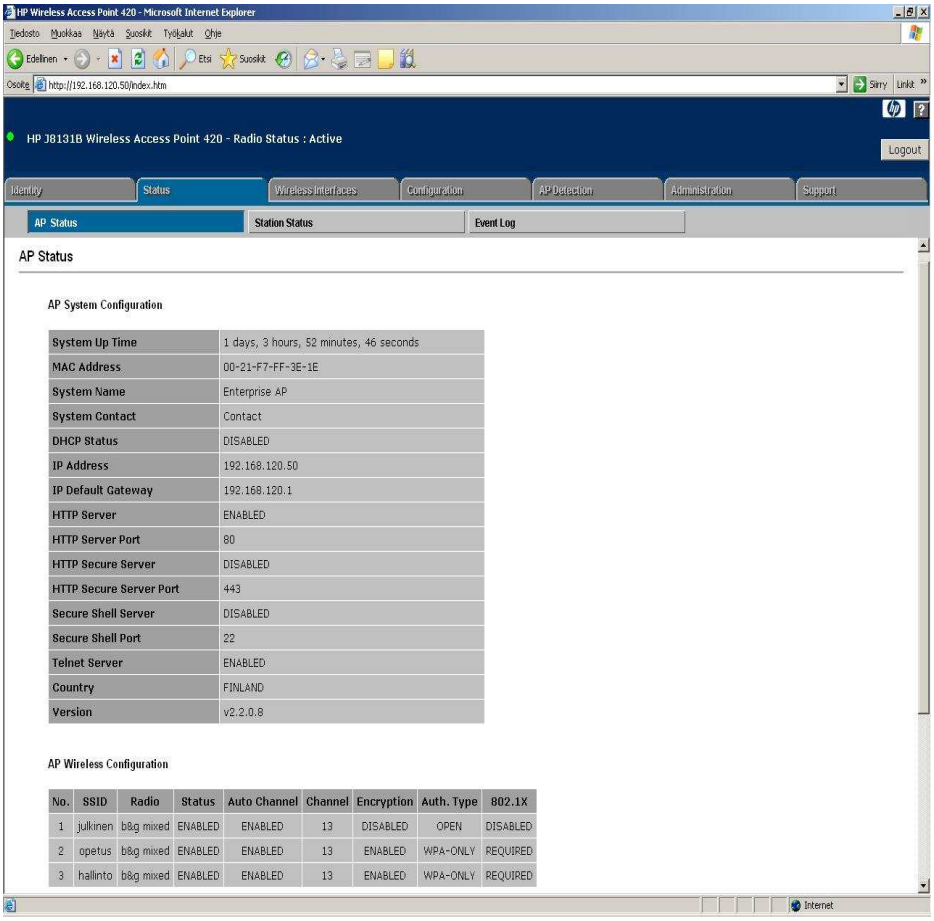


Kuva 8 Suojausasetukset

Seuraavalta välilehdeltä löytyy **Authentication Servers**, jonne lisätään **Primary RADIUS Server Setup** kohtaan samat asetukset mitä löytyy itse radiuspalvelimelta. Eli RADIUS-palvelimen IP-osoite ja Secret-Key kohtaan RADIUS-palvelimelle asetettu salasana. Oletusporttia ei tarvitse vaihtaa. **Secondary RADIUS Server Setup** kohtaan lisätään varmuuskopiopalvelimen asetukset, jos sellainen on käytössä. (Management and Configuration Guide for HP 420, 193-196.)

MAC Authentication kohdasta on mahdollista määrittää koneiden MAC-osoitteiden perusteella oikeudet sallia tai estää yksittäisten koneiden pääsy johonkin SSID-verkkoon. Mutta nykyään Mac-osoite on kovin helppo väärentää, jolloin sen hyöty jää todellista pienemmäksi. (Management and Configuration Guide for HP 420, 199-201.)

Accounting eli autentikoinnin tilastointi löytyy **Administration** osiosta ja **Accounting Servers** kohdasta. **Radius Accounting Servers** kohtaan laitetaan pallukka **Enabled** kohtaan. **Primary Server Setup** kohtiin syötetään samat asetukset kuin RADIUS-palvelimellakin. Tilastoinnin avulla voidaan seurata ja valvoa verkkoa sekä sen käyttöastetta. (Management and Configuration Guide for HP 420, 126-128.)

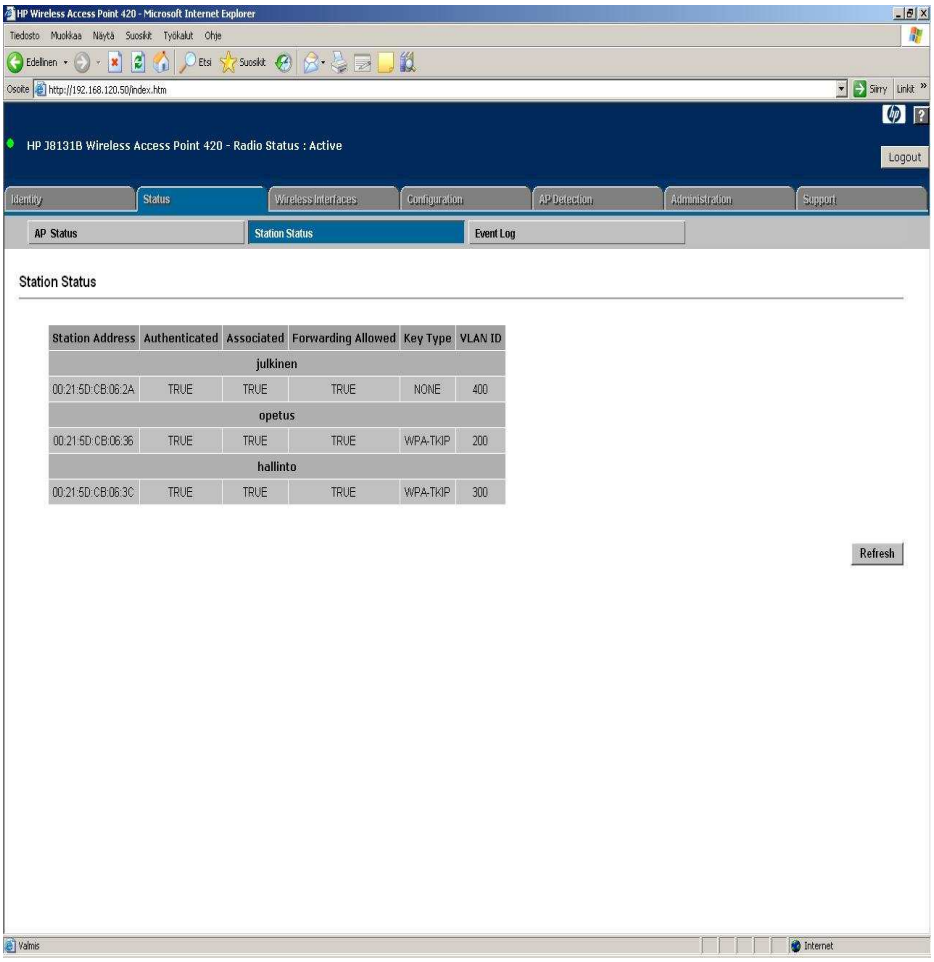


Kuva 9 Tukiaseman tärkeimmät tiedot

Status osiosta näkee tukiaseman tärkeimmät tiedot (Kuva 9), kuten MAC-osoitteen, IP-osoitteen, oletusyhdyskäytävän, protokollien portit ja ovatko ne käytössä. Myös jokaisen SSID:n käyttämä kanava sekä autentikoimis- ja salaustapa löytyvät sivun alareunasta. (Management and Configuration Guide for HP 420, 62-64.)

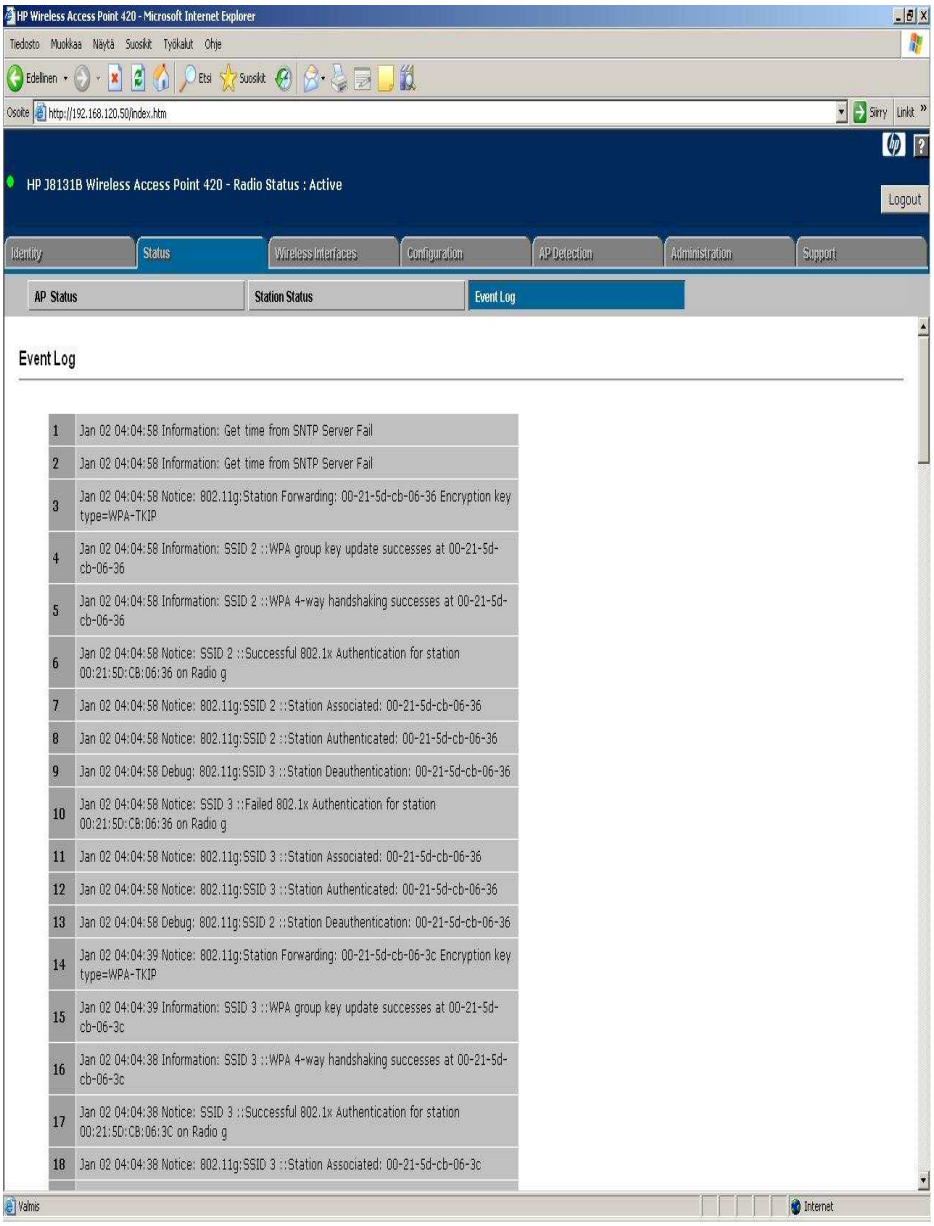
Station status välilehdeltä (Kuva 10) näkee tukiasemaan yhdistyneiden tietokoneiden MAC-osoitteen sekä pystyy tarkastelemaan mistä mahdollisen yhteyden toimimattomuus mahtaisi **authenticated**, **associated** ja **forwading allowed** toimenpiteiden välillä johtua. **True** sanoma kuvaa,

että kaikki on kunnossa. **False** vastaavasti, että jotain on pielessä. (Management and Configuration Guide for HP 420, 65-67.)



Kuva 10 Yhdistyneiden tietokoneiden yhteyden tila

Event log välilehdeltä löytyy vielä tarkemmin tietoa autentikoimisprosessista (Kuva 11). Lokin hyödyn maksimoimiseksi on suositeltavaa asettaa tukiasema hakemaan oikea kellonaika esimerkiksi toimialuepalvelimilta. Valitse **Administration** osio ja sieltä **System Servers** välilehti. **System Log Setup** ja **SNTP Server** kohtiin laitetaan pallukat **Enabled** kohtaan. **Primary Server** ja **Secondary Server** kohtiin syötetään toimialuepalvelimien IP-osoiteet. **Enter Time Zone** kohtaa laitetaan vastaamaan Suomen aikaa eli GMT+02. (Management and Configuration Guide for HP 420, 67, 119-120.)



Kuva 11 Autentikoinnin tapahtumaloki

3.3 KYTKIN (HP Procurve Switch 5304XL)

Kytkimelle ei tarvitse tehdä montaa asiaa. Aluksi pitää luoda VLANIT jokaiselle SSID:lle erikseen. Tämä tapahtuu kohdasta VLAN Names. Lisäksi VLAN:ille asetetaan IP-osoiteet sekä ID:t. Ip helper-address komennolla asetetaan osoite, josta haetaan yhdistyneille koneille IP-osoitteet. VLAN Port Assigment (Kuva 12) kohdasta asetetaan tarvittavat kytkimen portit Untagged tai Tagged tilaan. Tagged portit lähettävät VLAN ID:n eteenpäin toisiin kytkimiin. Untagged portit eivät lähetä ja

niitä voi olla vain yksi per portti. No vaihtoehto tarkoittaa, että portti ei kuulu kyseiseen VLAN:iin. Lisäksi täytyy olla reititin, joka osaa reitittää VLAN-liikennettä.

Kuva 12 Testiverkon VLAN:IEN porttimääritykset

4 PALVELIN JA TYÖASEMAT

Projektien edetessä tapahtuu muutoksia, niin myös tässä. Palvelimen käyttöjärjestelmä vaihtui Windows Server 2003:sta 2008:iin. Rajatakseni hieman opinnäytetyötäni päätin siis jättää vanhentuneen Windows Server 2003 kokonaan käsittelemättä. Lisäksi en käy kaikista yleisimpien palvelimen roolien (Active Directory, DNS ja DHCP) asentamista läpi, sillä työn pääpaino on muissa rooleissa. Kyseisiin rooleihin löytää kyllä varmasti netistä, jopa Youtubesta varsin seikkaperäiset (Step by Step Guide) asennusohjeet. Vaihtoehtoisesti suomeksi painavaa tietoa löytyy Jyrki Kivimäen Windows Server 2008 käsittelevistä tuhatsivuisista tiiliskivistä.

Käyttäjien ja tietokoneiden hallitsemiseksi ja tietoturvallisuuden parantamiseksi asennetaan Windows Server 2008:sen sisältämä Active Directory ja Network Policy and Access Services (NPS). Tällöin pystytään Active Directory:n Group Policyjen avulla luomaan erilaisia sääntöjä ja rajoituksia tietyille organisaatioille sekä käyttäjäryhmille. NPS:n avulla saadaan käyttöön RADIUS-palvelin, joka vertaa kirjautuvien käyttäjien tietoja Active Directory:stä löytyviin ja autentikoi käyttäjän, jos tiedot täsmäävät.

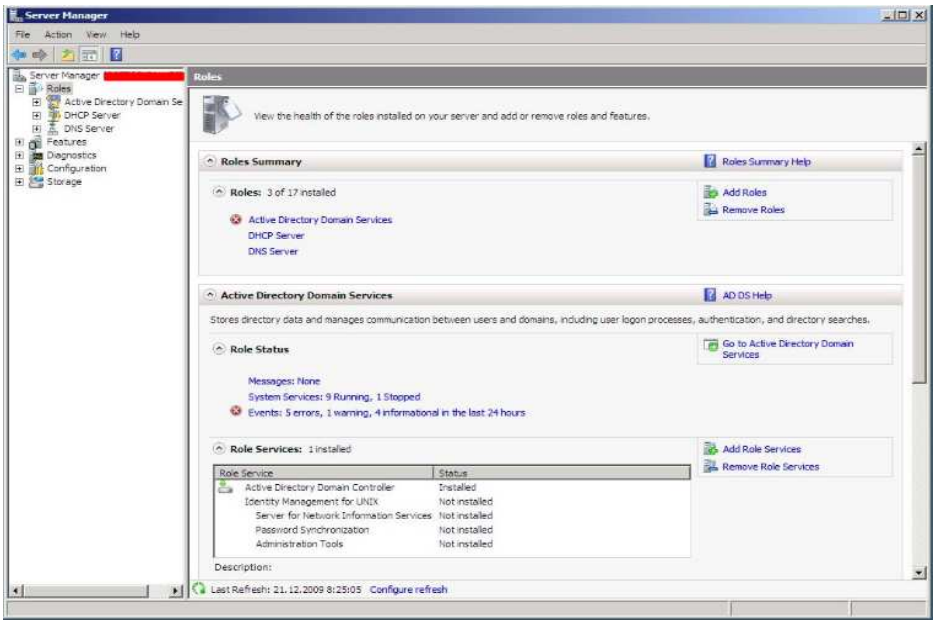
Homma alkaa asentamalla Windows Server 2008 tai muu vastaava palvelimen hallintaohjelma. Kyseisen tuotteen suositellut tietokoneen laitteistovaatimukset ovat luokkaa 2 GHz prosessori, 2 Gt muistia ja vähintään

40 Gt kiintolevytilaa. (Microsoft Windows Server 2008 System Requirements)

Perusroolien asentamisen jälkeen siirrytään RADIUS-palvelimen kannalta olennaisiin rooleihin.

4.1 Network Policy and Access Services

Avataan aloitusnäkymä (Kuva 13), josta hallitaan erilaisia rooleja. Uusien roolien asentaminen aloitetaan Add Roles painikkeesta. Avautuvasta ikkunasta painetaan Next. Server Roles ikkunasta voidaan valita mitä uusia rooleja halutaan asentaa. Tässä tapauksessa valitaan Network Policy and Access Services. Role Services osiosta valitaan komponentit, jotka halutaan sisällyttää Network Policy and Access Services rooliin. Valitaan ainakin Network Policy Server ja Routing and Remote Access Services molemmat alavalinnat. (Simple NPS Configuration as Radius Part 1, 3-7.)

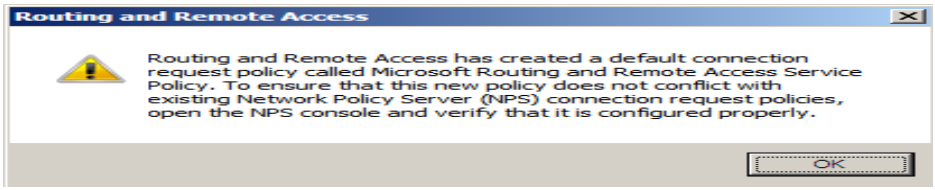


Kuva 13 Server Manager (Aloitusnäkymä)

Confirmation osiosta nähdään valitut komponentit. Valintojen täsmätessä painetaan Install, jolloin uuden roolin asennus käynnistyy. Progress osiosta nähdään asennuksen eteneminen. Results osiosta nähdään onko asennus suoriutunut onnistuneesti. Painetaan Close. Nyt vasemmalla palkissa oleviin rooleihin on ilmestynyt juuri äsken asentamamme Network Policy and Access Services ja sen alle Routing and Remote Access. Pu-

nainen nuoli tarkoittaa, että kyseinen komponentti ei ole vielä täysin konfiguroitu. (Simple NPS Configuration as Radius Part 1, 8-10.)

Routing and Remote Access komponentin konfigurointi tapahtuu klikkaamalla kyseistä kuvaketta vasemmalta. Klikataan hiiren oikealla ja valitaan Configure and Enable Routing and Remote Access. Avautuvassa ikkunassa Painetaan Next. Valitaan Custom configuration. Ruksitaan kohdat VPN access ja Dial-up access. Lopuksi Finish. Ruudulle ponnahtavasta varoituksesta (Kuva 14) ei tarvitse välittää sen enempää, sillä luomme omat sääntömme myöhemmin. Painetaan siis OK. Käynnistetään palvelu valitsemalla Start service. Nyt vasemmalla on näkyvissä kuinka Routing and Remote and Remote Access komponentin kuvake on muuttunut punaisesta vihreäksi.



Kuva 14 Automaattisten sääntöjen luonti varoitus

4.2 DHCP - Scope

Scope kohdassa määritellään IP-osoiteavaruus, josta tukiasemat voivat jakaa IP-osoiteet käyttäjille. DHCP Server kohdan alta IPv4 kohdasta klikataan hiiren oikealla New Scope.... Avautuvasta ikkunasta painetaan Next. Name ja Description kohtiin kuvaava nimi mihin verkonosaan scope vaikuttaa. Start IP address ja End IP address kohtiin määritellään väli, mitä IP-osoitteita scope voi jakaa. Luonnollisesti myös aliverkon peite (Subnet mask) tulee olla kelvollinen määriteltyyn IP-osoiteavaruuteen. Add Exclusions kohtaan lisätään tarvittaessa poikkeukset, joita ei haluta jakaa.

Lease Duration määrittelee, minkä ajan päästä käytettävä IP-osoite vanhenee. Valitaan Yes, I want to configure these options now. Router (Default gateway) kohtaan määritetään oletusyhdyskäytävä, jota tukiasemat käyttävät. Yleensä valitaan ensimmäinen IP-osoite tukiasemille määritellystä osoiteavaruudesta esimerkiksi 192.168.0.1 Painetaan Add. Domain Name and DNS Servers kohtaan määritellään toimialueen nimi ja ip-osoite DNS-palvelua varten. WINS Servers kohtaan voidaan tarvittaessa määritellä WINS-palvelimen nimi ja IP-osoite. Activate Scope kohdassa valitaan Yes, I want to activate this scope now. Lopuksi painetaan Finish.

4.3 Active Directory - Group Policies

Active Directory Domain Services roolin alta löytyy Active Directory Users and Computers. Hallintaikkunassa luodaan uusi Organizational Unit langatonta verkkoa käyttäville käyttäjille. Vierailijaverkon käyttäjiä ei tämän OU:n alle tarvitse lisätä, sillä oikeuksien jakoa tai käyttäjätunnistamista ei tarvita.

Sääntöjen (Policies) asettaminen tapahtuu ryhmäkäytäntöjen (Group Policy Management) alta. Aukeavassa näkymässä selataan oikean OU:n alle ja luodaan uusi sääntö, valitsemalla hiiren oikealla Create a GPO in this domain and Link it here… Tällöin kyseiset sääntöasetukset vaikuttavat vain kyseisessä OU:ssa oleviin tietokoneisiin. Valitaan nimetyn säännön ominaisuudet valitsemalla hiiren oikealla Edit. Avautuu Group Policy Management Editor. Selataan kohtaan Computer Configuration - Policies - Windows Settings - Security Settings ja klikataan hiiren oikealla Wireless Network (IEEE 802.11) Policies kohtaa. Valitaan Create A New Windows Vista tai XP policy sen mukaan millaisia koneita on kyseisessä Ou:ssa. Myöhemmin voidaan valita hiiren oikealla XP Policyn päältä Migrate XP policy to Vista policy, jolloin vastaavat säännöt saadaan automaattisesti luotua myös Windows Vista ja 7 koneille.

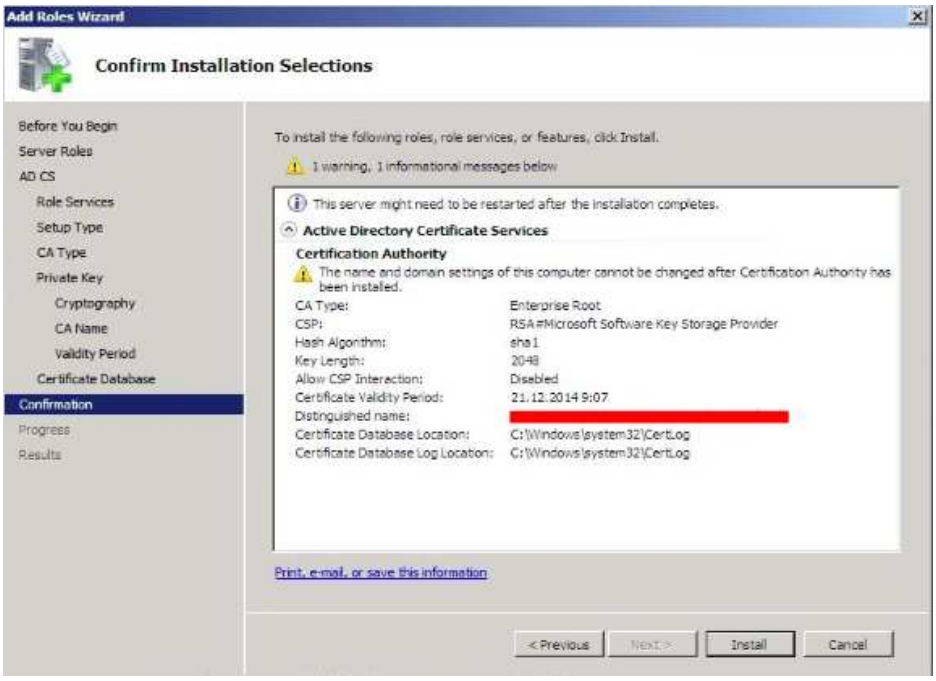
General välilehdeltä asetetaan XP Policy name ja Description kohtiin kuvaavat nimet. Network to access määrittää minkä tyyppiset verkot ovat sallittuja muodostamaan yhteyden. Use Windows WLAN Autoconfig service for clients kohta luo käyttäjille automaattisesti Windowsin ennalta määrittämät asetukset. Automatically connect to non-preferred networks kohta tarkoittaa, että yhdistetään automaattisesti ennalta määrittämättömiin langattomiin verkkoihin.

Preferred Networks välilehdeltä painetaan Add… Infrastructure. Avautuu uusi ikkuna. Network Properties välilehdeltä syötetään Network name (SSID) kohtaan täysin sama SSID, joka on langattomassa tukiasemassa. Tämän jälkeen valitaan Connect even if network is not broadcasting, jolloin yhdistetään vaikka langaton tukiasema ei aktiivisesti lähetä signaalia vaan on piilotettu. Langattoman verkon suojausasetukset asetetaan kohdista Authentication ja Encryption. Huomioi, että suojausasetuksien on oltava täysin yhteneväiset tukiaseman suojauksien kanssa.

IEEE 802.1X välilehdeltä löytyy EAP autentikointiprotokollan eri vaihtoehtoja, joista valitaan PEAP. Authenticate as computer when computer information is available määrittää voidaanko tietokoneen perusteella kirjautua sisään ilman, että käyttäjä kirjautuu sisään. Authenticate as guest when user or computer information is unavailable määrittää autentikoidaanko käyttäjä vierailijaksi, jos tietokoneen tai käyttäjän kirjautumistietoja ei ole saatavilla. Settings kohdasta lisättäisiin vielä sertifikaatti, mutta ensin täytyy luoda sellainen.

4.4 Sertifikaatti

Sertifikaatin tekeminen on nykyään helpompaa kuin Windows Server 2003:ssa, jossa se piti luoda komentoriviltä. Sertifikaatin tekemiseksi pitää asentaa sitä varten uusi palvelinrooli. Valitaan siis Add Roles. Avautuvassa ikkunassa painetaan Next. Valitaan Active Directory Certificate Services. Role Services välilehdeltä valitaan Certification Authority, Certification Authority Web Enrollment ja tarvittavat lisäkomponentit. Kahdesta vaihtoehdosta valitaan Enterprise ja jatketaan eteenpäin. CA-tyypiksi valitaan Root CA. Luodaan uusi salausavain valitsemalla Create a new private key. Seuraavalla sivulla krypttaus- ja algoritmiasetuksiin kelpaavat oletusasetukset. CA Name kohdassa luodaan tarpeeksi hyvin kuvaava nimi. Validity Period kohdassa määritellään sertifikaatin voimassaoloaika. 5 vuotta on palvelinympäristöä ajatelleen hyvä aika, jolloin luultavasti on tullut jo nykyisen palvelimen (Server 2008) uusi käyttöjärjestelmäversio. Toisaalta sertifikaatin pystyy kyllä viemään ja tuomaan (export & import) toiminnolla myös muihin palvelimiin. Certificate Database kohdassa määritellään kansiot, jonne tallennetaan kaikki sertifikaatteja koskevat pyynnöt, muutokset ja lokit. Confirmation kohdassa nähdään yhteenveto valituista asetuksista (Kuva 15). Roolin asennus käynnistetään painamalla Install. Odotetaan hetken aikaa asennuksen valmistumista ja asennuksen valmistuessa painetaan Close. (Securing Wireless Networks with Windows Server 2008 and NPS, 5-9)

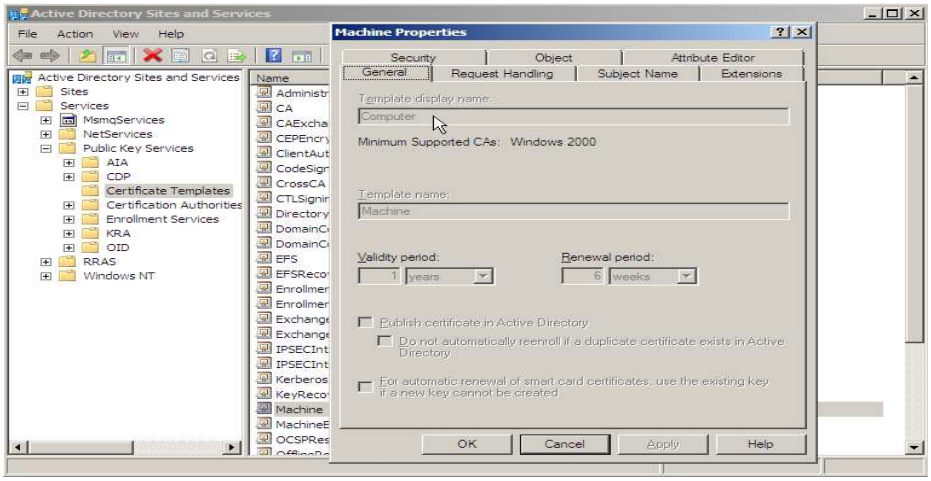


Kuva 15 AD CS-asetukset

4.4.1 Sertifikaatin luonti

Ennen sertifikaatin luontia täytyy asentaa palvelimelle Web Server (IIS) rooli, jotta Computer Certificate saadaan luotua ja jaettua. Roolin asentaminen tapahtuu painamalla Add Roles ja painetaan Next. Server Roles kohdassa valitaan Web Server (IIS), jonka voit asentaa oletusasetuksin loppuun.

Lisäksi täytyy Valitaan käynnistä-valikosta Administrative Tools ja sen vaihtoehdoista Active Directory Sites and Services. Painetaan View kohdasta Show Services Node. Selataan Services haarassa kohtaan Public Key Services - Certificate Templates. Valitaan oikealta Machine, hiiren oikealla Properties (Kuva 16). Mennään Security välilehdelle ja valitaan Authenticated Users. Annetaan Full Control oikeudet.



Kuva 16 Machine Template - Surullisen kuuluisa asetus

Käyttäjien tietokoneita varten sertifikaatti luodaan kirjoittamalla komentokehoitteeseen mmc (löytyy Start - Run - cmd). Avautuvasta ikkunasta valitaan File - Add or Remove Snap-in... Valitaan Available snap-ins kohdasta Certificates ja painetaan Add >. Valitaan kolmesta vaihtoehdosta viimeinen eli Computer Account, painetaan Next ja OK. Selataan Certificates (Local Computer) kohdasta Personal ja tämän alta Certificates.

Hiiren oikealla klikataan Certificates kansion päälle ja valitaan All tasks - Request new Certificate. Painetaan Next. Valitaan Computer kohta ruksaamalla se ja painetaan Enroll (Kuva 17). Huomioi, että tässä kohdassa ei siis ole valittavissa Computer kohtaa mikäli Machine Template mallille ei ole annettu riittäviä oikeuksia tai Web Server (IIS) roolia ei ole palvelimelle asennettu. Voin nimittäin sanoa, että tämän kohdan toimintakuntoon saamiseksi itseltäni meni vianetsintään aikaa useampi päivä. Osittain johtui varmasti siitä, että kyseisen mallin Template display name ja Template name ovat erinimisiä (Kuva 16). (Securing Wireless Networks with Windows Server 2008 and NPS, 1-4)

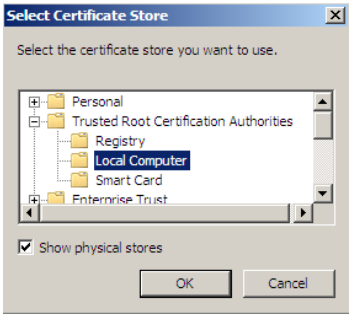
Kuva 17 Computer sertifikaatin luonti

4.4.2 Sertifikaatin tallennus

Sertifikaatti tallennetaan valitsemalla hiiren oikealla haluttua sertifikaattia ja klikkaamalla All Tasks – Export... Painetaan Next. Valitaan No, do not export the private key, sillä emme halua yksityisen avaimen joutuvan kaikkien saataville. Tallennusmuodoksi valitaan DER encoded binary X.509 (.CER), joka on yhteensopiva PEAP-protokollan kanssa. Valitaan kohde minne sertifikaatti halutaan tallentaa. Painetaan Next. Lopuksi saadaan yhteenveto valituista asetuksista. Asetukset saadaan kuitatuksi painamalla Finish.

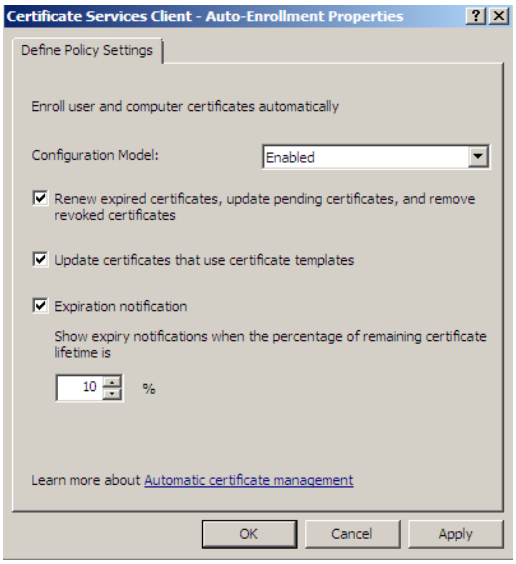
4.4.3 Sertifikaatin lisääminen

Sertifikaatin lisääminen luotettavien sertifikaattien listalle tapahtuu menemällä Certificates (Local Computer) kohdassa Trusted Root Certification Authorities ja sen alla olevaan Certificates kansioon. Valitaan hiiren oikealla Import. Siirrytään eteenpäin. Painetaan Browse... ja selataan kansioon, jonne sertifikaatti on tallennettu. Painetaan Next. Valitaan Place all certificates in the following store Painetaan Browse... Laitetaan ruksi kohtaan Show physical stores ja selataan kohteeseen Trusted Root Certification Authorities\Local Computer (Kuva 18). Lopuksi saadaan jälleen yhteenveto valituista asetuksista. Kuitataan asetukset painamalla Finish.



Kuva 18 Sertifikaattisäilö

Nyt sertifikaatin luomisen jälkeen voidaan lisätä se aikaisemmassa Windows XP policyn EAP-tyyppi kohtaan painamalla Settings... Avautuvassa sertifikaattilistassa selataan AD CS roolissa tehdyn sertifikaatin kohdalle ja ruksataan se käyttöön ja painetaan OK. Suljetaan ikkunat painamalla OK. Päästyämme takaisin Group Policy Management Editor pääikkunaan valitaan Wireless Network (IEEE 802.11) Policies kohdan alta Public Key Policies - Automatic Certificate Request Settings. Valitaan hiiren oikealla New --> Automatic Certificate Request… painetaan Next ja valitaan Computer. Siirrytään käyttäjäkohtaisiin suojausasetuksiin User Configuration - Windows Settings - Security Settings - Public Key Policies. Avataan oikealtapuolelta Certificate Services Client - Auto Enrollment ja asetetaan kuvan 19 mukaiset asetukset. Näiden asetuksien jälkeen sertifikaattiasetukset siirtyvät automaattisesti käyttäjien tietokoneille, kun heidän koneensa lisätään langaton verkon OU:hun ja Group Policyt koneissa päivittyvät.



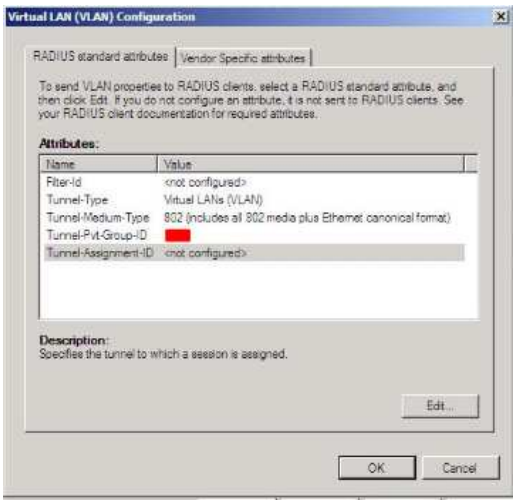
Kuva 19 Sertifikaatin jako-ominaisuudet

4.5 Network Policy Server (NPS)

Valitaan Server Manager pääikkunasta vasemmalta NPS (Local) ja valitaan hiiren oikealta sen päältä Register Server in Active Directory, jolloin RADIUS pystyy hyödyntämään AD:n käyttäjätietoja. Valitse pudotusvalikosta RADIUS server for 802.1X wireless or wired connections, jonka jälkeen alapuolelta painetaan Configure 802.1X. Laitetaan pallukka ylempään kohtaan eli asetukset ovat langattomalle verkolle. Lisäksi alempanan annetaan sopivan kuvaava nimi säännölle. Painetaan Add... luodaksemme uuden RADIUS clientin. (Simple NPS Configuration as Radius Part 2, 1-2.)

Friendly name kohtaan nimi, josta käy ilmi mikä tukiasema on kyseessä. Address (IP or DNS) kohtaan asetetaan osoite, joka on konfiguroitu kiinteänä tukiasemaan. Alempana valitaan Manual ja Shared secret kohtiin syötetään salasanaksi sama kuin tukiaseman Authentication Servers - Primary RADIUS Server Setup - Secret Key kohdassa. Pudotusvalikosta valitaan Microsoft: Protected EAP (PEAP) ja painetaan Configure. Certificate issued kohtaan valitaan aikaisemmin kohdassa 4.4.1 tehty Computer certificate. Add.. nappia painamalla lisätään ryhmät, joihin kyseinen sääntö vaikuttaa. Suosittelen valitsemaan Domain Computers ja Domain Users, jolloin koneita ja käyttäjiä ei tarvitse myöhemmin lisätä ryhmiin käsin vaan ne tulevat automaattisesti kun kone tai käyttäjä lisätään toimialueelle. (Simple NPS Configuration as Radius Part 1, 18-20, 23-26.)

Attributes kohtiin määritellään mitä reittitapaa pitkin tiedot kulkevat RADIUS-palvelimen ja tukiaseman välillä (Kuva 20). Tunnel-type kohtaan Virtual LANs (VLAN). Tunnel-Medium-Type kohtaan 802 (includes all 802 media plus Ethernet canonical format). Tunnel-Pvt-Group-ID kohtaan lisätään VLAN numero, joka on kytkimissä sekä tukiasemassa määritetty kyseiselle yhteydelle. Lopuksi painetaan Finish, jolloin Connection Request Policy sekä Network Policies kohtiin ilmestyy kyseinen sääntö. Uusien sääntöjen tuleminen käyttöön vaatii vielä niiden siirtämisen Processing Order listalla ylimmäisiksi.



Kuva 20 VLAN-asetukset

4.6 Event Viewer (Lokit)

Siinä vaiheessa kun kaiken pitäisi olla kunnossa, mutta yhteys ei toimi on useampia paikkoja, joista voidaan lähteä etsimään vikaa. Oletuksena NPS tallentaa lokia kohteeseen C:\Windows\System32\logfiles. Event Viewer on kumminkin paljon kätevämpi apu RADIUS-palvelimen autentikoinnin toimivuuden tarkistamiseen, sillä se on paljon selkokielisempi. Event Viewer löytyy Server Manager aloitusivun Diagnostics kohdasta. Lokeja voi olla kolmenlaisia Error, Warning ja Information tyyppisiä. Lisäksi palvelinympäristön ulkopuolelta löytyy vianetsintään apua tukiaseman lokista sekä käyttäjän tietokoneen tapahtumienvalvonnasta. (Securing Wireless Networks with Windows Server 2008 and NPS)

Verkkoympäristön muiden osien konfiguroinnin jälkeen siirrytään varsinaisesti testaamaan langattoman verkon toimintaa. Viimeisenä osana on tietokone, yleensä kannettavaa mallia. Myös tietokoneeseen pitää tehdä muutamia muutoksia, jotta langaton verkko saadaan toimimaan.

4.7 Toimialueverkko

Tiedustellaan käyttäjältä miksi tarvitsee langatonta verkkoa ensisijaiseksi tarkoitetun langallisen sijaan. Yhteisymmärrykseen päästessä liitetään tietokone sille tarkoitettuun domainiin, ellei siis ole jo valmiiksi. Tämän jälkeen koneen ilmestyessä AD:n konelistaan siirretään se langatonta verkkoa vastaavan OU:n alle. Päivitetään Group Policyt koneeseen valitsemalla käynnistä-valikosta **suorita...** kirjoitetaan **cmd**, jonka jälkeen kirjoitetaan **gpupdate /force**. Tarkistetaan ovatko policyt päivittyneet

toivotulla tavalla valitsemalla oikeasta alakulmasta **langaton verkkoyhteys** ja aukeavasta ikkunasta **muuta ensisijaisten verkkojen järjestystä**.

Ensisijaisten verkkojen kohdalta langattoman verkon löytyessä valitaan **ominaisuudet** ja avautuvasta ikkunasta todennus-välilehti. **EAP-tyyppi** kohdasta valitaan **ominaisuudet** ja selataan listaa alaspäin nähdäksemme onko tietokone saanut myös oikean sertifikaatin. Tämän jälkeen kirjaudutaan kerran verkkopiuhan kanssa toimialueelle ja katsotaan yhdistääkö tietokone langattomaan verkkoon. Lopuksi käynnistetään tietokone uudelleen ja toistetaan sama testi, mutta ilman verkkopiuhaa.

4.8 Vierailijaverkko

Syötetään käsin oikeat asetukset. Valitaan oikeasta alakulmasta **langaton verkkoyhteys** ja aukeavasta ikkunasta **muuta ensisijaisten verkkojen järjestystä**. Painetaan **Lisää..** Kytkennät välilehdeltä lisätään **verkkonimi (SSID)** kohtaan piilotetun verkon SSID. **verkkotodennus** ja **tiedon salaus** kohtiin asetetaan niitä vastaavat asetukset. Yhteys-välilehdeltä laitetaan ruksi kohtaan Muodosta yhteys tähän verkkoon, kun verkko on kantoalueella. Lopuksi painetaan OK. Vierailijaverkon toimivuutta voidaan testata myös älypuhelimella.

5 TULEVAISUUS

Tämän opinnäytetyön kirjoittamisen edetessä sain tehtäväkseni kirjoittaa tukiasemia uudemmasta tekniikasta nimeltä radioportit. Periaatteessa kuitenkin radioportitkin ovat jo vanhentunutta tekniikkaa, sillä tilalle ovat tulleet niin sanotut MultiService Access Pointit.

Tekniikka kehittyy siis huimaa vauhtia tuoden uusia innovaatioita markkinoille. Tästä syystä langatonta verkkoakin joutuu päivittämään tietyn väliajoin vastaamaan sen hetkisiä trendejä ja vaatimuksia. Kuten olet huomannut langattomaan verkkoon ja sen toimivuuteen vaikuttaa monia erilaisia laitteita. Uutta laitetta vaihdettaessa voit joutua konfiguroimaan sen täysin tyhjältä pohjalta, varsinkin jos se on eri valmistajan tuote. Toisaalta pelkästään jo firmwaren päivitys tukiasemaan tai kytkimeen voi tuoda eteen odottamattomia ongelmia. Lisäksi palvelimen käyttöjärjestelmän päivittyminen tietyin väliajoin vaatii oman osaamisen kartuttamista, jotta uusi ympäristö saadaan entisen kaltaiseksi tai tietenkin mielellään paremmaksi. Isompia muutoksia tehtäessä kannattaa miettiä voidaanko samalla tehdä myös jotain, mikä vaatisi normaalisti useampia käyttökatkoksia tai käyttäjien toimenpiteitä.

Tulevaisuuden myötä laskentatehon kehittyessä myös salaustapoja joudutaan varmasti muuttamaan. Haittaohjelmien määrän lisääntyessä myös suojauksien pitää olla kunnossa. Eritoten tietoturvauhkien ennaltaehkäisy ja varmuuskopioiden ottaminen säännöllisesti ovat vähintä mitä voidaan tehdä.

5.1 Nykyisen langattoman verkon kehittäminen ja parantaminen

Seuraavaksi esittelen toteutustapaa, jossa tukiasemat korvattaisiin radioporteilla. Tällöin muutoksien tekeminen on paljon helpompaa, sillä ne tehdään keskitetysti kytkimen kontrollerilla. Tämä toteutustapa on varsin suositeltavaa siinä vaiheessa, kun tukiasemien määrä kasvaa sellaiseksi, että on liian työlästä päivittää jokainen tukiasema erikseen.

5.1.1 Radioportit

Radioportit ovat paljon alykkäämpiä laitteita, kuin tavalliset tukiasemat. Kytkiessäsi radiportin verkkoon kytkimen kontrolleri löytää ja konfiguroi sen automaattisesti vastaamaan asetuksiltaan jo olemassa olevaa verkkoa. Radioporteissa on sisäänrakennetut antennit ja ne tukevat langattoman standardin b ja g nopeusluokkia. (HP Procurve Radio Port 210, Datasheet, 2.)

Vaikka tukiasemissa on myös mahdollista asettaa jokainen tukiasema samalle radiokanavalle, jolloin Roaming eli siirtyminen tukiasemalta toiselle toimisi parhaimmalla mahdollisella tavalla. Valitettavasti käytännössä se ei kuitenkaan toimi niissä yhtä nopeasti ja varmasti, kuin keskitetyn hallinnan mallisissa verkoissa, joissa tämän hoitaa niin sanottu moduuli (Wireless Edge Services Module). (Businessforumin asiakaslehti 1/2007, 37-38.)

Kontrolleri on kytkimeen kiinnitettävä erillinen moduuli, joka kontrolloi radioportteja keskitetysti. Moduulilta hoituu niin tietoturvan kuin erilaisten sääntöjenkin hallinta Procurve Manager ohjelmaan saatavien erillisen lisäohjelmien avulla. Tilanteissa, joissa on paljon käyttäjiä, joutuu langaton verkko koetukselle. Tällöin avuksi tulee QoS (Quality of Service), joka priorisoi kaistankäytön eri tarpeiden mukaan kuten esimerkiksi puheen, videon tai internetin. Kaikkien edellä mainittujen tärkeysasteiden edelle menee kuitenkin uusien käyttäjien yhdistäminen langattomaan verkkoon. (Businessforumin asiakaslehti 1/2007, 38.)

Keskitetyssä hallinnassa moduuli tarkkailee koko ajan verkon muutoksia ja muuttaa esimerkiksi radiokanavia sen mukaan, kun uusia langattomia laitteita ilmestyy verkkoympäristöön. Radioportit kannattaa asettaa niin, että käytetään esimerkiksi vain puolet maksimi radiotehoista. Tällöin yh-

den radioportin vikaantuessa moduuli pystyy lisäämään muiden radioporttien lähetystehoa kattamaan vikaantuneen aiheuttaman vajeen. Vikasietoisuutta saadaan parannettua entisestään asentamalla kytkimeen toinen moduuli ja virtalähde. Tällöin jommankumman hajotessa verkon toiminta jatkuu ilman katkosta. (HP Procurve Radio Port 210, Datasheet, 2, Tietotekniikan tuoteuutiset 4/2008, 46-47.)

Hintojen puolesta radioportit ovat suurin piirtein samanhintaisia kuin tukiasemat. Mahdollisesti uusien kytkimien hankinta moduulin liittämiseksi maksaa hieman lisää, mutta itse moduuli maksaa useamman tuhannen. Lisäksi radioporteille pitää hankkia vielä lisenssit.

5.1.2 MultiService Access Points

Radioportti mallinen verkko ei sovellu uusille n-standardin laitteille. Nopeuksien kasvaessa moninkertaisiksi kontrolleri alkaa muodostua pullonkaulaksi, koska kaikki liikenne kulkee pelkästään sen läpi. MultiService Mobility mallisessa verkossa liikenne ohjataankin suoraan sinne minne sen on tarkoitettu menevän. (HP Martti Saramies Uuden Sukupolven WLAN, 8-9.)

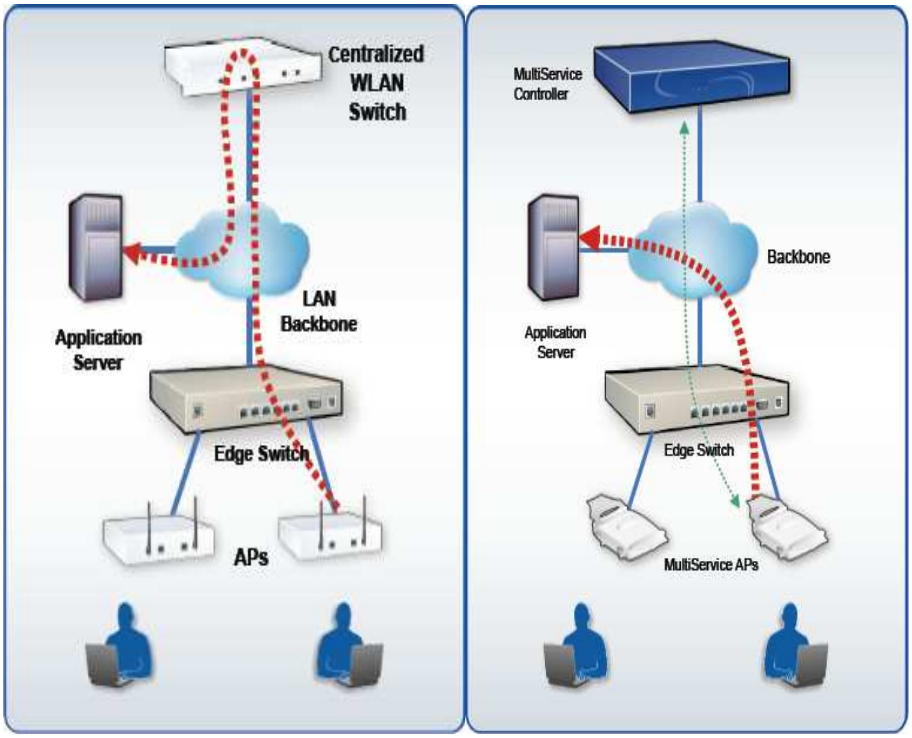
Multiservice Mobility malliset tuotteet jakavat liikenteen kuorman eri laitteiden kesken ja lisäksi hajauttavat vieras- ja toimialueverkkojen liikenteen täysin niille suunnitelluille laitteille (Kuva 21). (HP Martti Saramies Uuden Sukupolven WLAN, 10.)

Tukiasemat (MSM 310, 320, 325, 335, 410 ja 422) on toteutettu joko yhden, kahden tai kolmen radion tekniikalla. Yhden radion malleissa n-standardia ei pysty käyttämään täydellä nopeudella, jos samaan aikaa on käytössä vanhemman standardin malleja. Suositeltavaa on siis valita vähintään kahden radion malli, sillä tällöin pystytään käyttämään uusinta n-standardia sekä vanhoja standardeita yhtä aikaa. Toisaalta, jos käytössä on pelkästään n-standardin laitteita päästään kahden radion avulla tiedonsiirtokapasiteetissa lähemmäksi teoreettisia maksimilukemia. Kahden radion tukiasemasta on hyötyä myös siinä tapauksessa, kun halutaan laajentaa verkkoa langattomasti tukiasemalta toiselle ja samalla vielä tarjota toisella radiolla yhteys käyttäjille. Tukiaseman vikaantuessa luodaan vaihtoehtoinen langaton reitti toiseen tukiasemaan. (HP Martti Saramies Uuden Sukupolven WLAN, 13, 17-19.)

Huomioitavaa on myös, että n-standardiin siirryttäessä on suotavaa päivittää perinteiset 100 Megabitin kytkimet Gigabitin nopeuteen, sillä n-standardin tarjoama yli 200 Mbps nopeus tekee nopeasti 100 Mbps kytkimistä verkon pullonkauloja. (Wireless N - Azlan)

Kontrollerit (MSM 710, 730 ja 750) eroavat toisistaan kuinka montaa tukiasemaa ne maksimissaan pystyvät hallitsemaan ja kuinka paljon verkkovieraita pystyy olemaan yhtäaikaisesti. Lisäksi tietenkin hinta eroaa toisistaan merkittävästi. (Ajankohtaiset hintatiedot)

Guest Management ohjelmistolla vierailijaverkon luominen on entistä vaivattomampaa, sillä ohjelman helppokäyttöisyyden vuoksi sen käyttämiseen ei tarvita välttämättä lainkaan IT-henkilöstöä. Ohjelmalla luodaan vierailijatunnuksia tietyksi määräajaksi, joilla vierailijat pääsevät kirjautumaan laaditun web-sivun kautta verkkoon. (HP Martti Saramies Uuden Sukupolven WLAN, 31)



Kuva 21 Radioportti ja MSM-mallisen verkon erot

6 YHTEENVETO

Projektin edetessä useampien pienten ongelmien lisäksi vastaan tuli kaksi suurempaa ongelmaa, joista selvittiin tekemällä seuraavanlaiset kompromissit.

Ensimmäinen ongelma kohdattiin, kun tukiaseman SSID:istä asetettiin opetus, hallinto piilotetuiksi ja julkinen jäi näkyväksi. Tällöin kannettavat eivät enää löytäneet piilotettuja verkkoja ollenkaan. Ensisijaisilla verkon asetuksilla ei myöskään ollut vaikutusta asiaan. Myöhemmin selvisi, että kyseinen tapahtuma ei olekaan varsinaisesti ongelma vaan Windows XP:n ominaisuus. (Your computer connects to an access point that

broadcasts its SSID instead of an access point that does not broadcast its SSID)

Edellisen kohdan olisi luultavasti pystynyt korjaamalla asentamalla Service Pack 3:sen, sillä Microsoftin support sivulla lukee, että koskee SP1 ja SP2 asennettuja Windows XP koneita. Asia korjattiin tekemällä kompromissi piilottamalla kaikki SSID:t.

Toinen ongelma alkoi yllättäen, sillä yhdessä vaiheessa alkoi ihmetyttää kun osa täysin saman mallin kannettavista toimi ja osa ei. Syyksi paljastui, että osaan koneisiin oli päivittynyt Service Pack 3. Tähänkään päivään mennessä ei ole vielä selvinnyt, mikä lisäosa tulee lisää aiheuttaen langattoman verkon toimimattomuuden. Googlesta löytyy kyllä hakuosumia varsin paljon käyttämällä hakusanoja after sp3 wireless not work. Tässäkin ongelmatapauksessa turvauduttiin kompromissiin. Eli poistettiin kannettavista SP3 päivitys, jolloin jäljelle jääneen SP2:sen jälkeen langaton verkko toimi taas.

Ongelmista huolimatta langaton verkko, saatiin muilta osin kumminkin toteutettua. Loppujen lopuksi tukiasemia asennettiin yhteensä 30 kappaletta.

Tulevaisuudessa Windows 7 ympäristöön siirryttäessä on mahdollista tuoda vierailijaverkon SSID näkyville ja lisäksi tarkoituksena on ottaa vahvempi WPA2-salaus käyttöön.

LÄHTEET

Cisco, Cisco Systems Inc, 2009, CCNA Exploration 4.0. LAN Switching and Wireless. Chapter 7: Basic Wireless Concepts and Configuration, Viitattu 29.07.2009
http://cisco.netacad.net

Internet.com, QuinStreet Inc 2010, Say No to WEP And Yes to WPA, Viitattu 09.05.2010
http://www.wi-fiplanet.com/tutorials/article.php/3672711/Say-No-to-WEP-And-Yes-to-WPA.htm

Internet.com, QuinStreet Inc 2010, A Warm Welcome to WPA2, Viitattu 09.05.2010
http://www.wi-fiplanet.com/news/article.php/3402971.

STUK – Usein kysytyt kysymykset, Viitattu 30.09.2009
http://www.stuk.fi/sateilytietoa/ukk/kentat/fi_FI/kentat18/

Hewlett-Packard Development Company, L.P. 2009, HP 420 Datasheet, Viitattu 06.07.2009
http://www.procurve.com/products/pdfs/datasheets/Wireless_Access_Point_420.pdf

Hewlett-Packard Development Company, L.P. 2009, HP Procurve 420, Viitattu 06.07.2009
http://www.procurve.com/products/wireless/420_series/overview.htm

Hewlett-Packard Development Company, L.P. 2010, Management and Configuration Guide for HP 420, Viitattu 06.07.2009
http://cdn.procurve.com/training/Manuals/420-MgmtCfg-May2005-59906006.pdf

Microsoft Corporation 2010, Microsoft Windows Server 2008 System Requirements, Viitattu 11.01.2010
http://msdn.microsoft.com/en-us/windowsserver/cc196364.aspx

Intel Corporation 2010, Simple NPS Configuration as Radius Part 1, Viitattu 13.01.2010
http://communities.intel.com/servlet/JiveServlet/downloadBody/4321-102-1-7037/SImple%20NPS%20Configuration%20as%20Radius%20Part%201.pdf

Intel Corporation 2010, Simple NPS Configuration as Radius Part 2, Viitattu 13.01.2010
http://communities.intel.com/servlet/JiveServlet/downloadBody/4322-102-1-

7038/SImple%20NPS%20Configuration%20as%20Radius%20Part%202.pdf

Wordpress 2010, Securing Wireless Networks with Windows Server 2008 and NPS, Viitattu 13.01.2010
http://techblog.mirabito.net.au/?p=87

Hewlett-Packard Development Company, L.P. 2010, HP Procurve Radio Port 210 Datasheet, Viitattu 17.01.2010
http://www.procurve.com/products/pdfs/datasheets/ProCurve_Radio_Port_210.pdf

Businessforum Oy 2007, Businessforumin asiakaslehti 1/2007, Viitattu 22.04.2010
www.businessforum.fi/bf_pdf/BFnewz01_2007.pdf

Tietotekniikan tuoteuutiset 4/2008, Viitattu 22.04.2010
http://www.tuoteuutiset.fi/pdf/TIE408s46-47.pdf

HP Martti Saramies Uuden Sukupolven WLAN, Viitattu 22.04.2010
http://palnet.1g.fi/kuvat/Palnet%20Tallinna%2019.5.2009/HP%20Martti%20Saramies%20Uuden%20Sukupolven%20WLAN.pdf/full

Tech Data Group 2010, Wireless N – Azlan, Viitattu 27.04.2010
http://www.azlan.fi/802-11n-ratifioitu.html

Hewlett-Packard Development Company, L.P. 2010, Ajankohtaiset hintatiedot, Viitattu 29.04.2010
http://h10010.www1.hp.com/wwpc/fi/fi/sm/WF02a/12883-12883-3836026.html

Microsoft Corporation 2010, Your computer connects to an access point that broadcasts its SSID instead of an access point that does not broadcast its SSID, Viitattu 23.01.2010
http://support.microsoft.com/kb/811427

Liite 1

HP 420 AP VALMIS KONFIGURAATIO

Tietoturvallisuuden vuoksi olen poistanut tiettyjä tietoja, kuten: tukiaseman IP-osoite, gateway, DNS-palvelinten osoitteet, Radius-serverin IP-osoiteen sekä muuttanut lopulliseen ympäristöön tukiasemien SSID:t sekä niitä vastaavat VLAN ID:t.

```
## This file is generated automatically by hp Access Point 420.

[system]
country=FI
system-name=Enterprise AP
user0-name=empty
user0-password=***
user0-class=empty

[ethernet]
speed-duplex=auto
broadcast-limiting-enable=false
ether-interface-status=Up
ether-admin-status=Up
dhcp=false
address=0.0.0.2
netmask=255.255.255.0
gateway=0.0.0.1
primary-dns-address=0.0.0.3
secondary-dns-address=0.0.0.4

[management]
cli-prompt=HP ProCurve Access Point 420
vlan-enable=true
dynamic-vlan-id=false
management-vlan-id=200
management-vlan-tagging=true
iapp-enable=true
svp-supported=false
reset-button=true
serial-console=true
http-enable=true
http-port=80
https-enable=false
https-port=443
telnet-enable=true
telnet-max-sessions=4
ssh-enable=false
ssh-port=22
```

```
[system-servers]
accounting-server-enable=false
primary-accounting-server=0.0.0.0
primary-accounting-secret=****
primary-accounting-timeout=5
primary-accounting-retries=3
primary-accounting-port=1813
primary-accounting-interimupdate=3600
secondary-accounting-server=0.0.0.0
secondary-accounting-secret=****
secondary-accounting-timeout=5
secondary-accounting-retries=3
secondary-accounting-port=1813
secondary-accounting-interimupdate=3600
logging-enable=false
syslog-server1-enable=false
syslog-server1-address=0.0.0.0
syslog-server1-port=514
syslog-server2-enable=false
syslog-server2-address=0.0.0.0
syslog-server2-port=514
syslog-server3-enable=false
syslog-server3-address=0.0.0.0
syslog-server3-port=514
syslog-server4-enable=false
syslog-server4-address=0.0.0.0
syslog-server4-port=514
logging-console=false
logging-level=Informational
sntp-enable=true
primary-sntp-server=0.0.0.5
secondary-sntp-server=0.0.0.6
sntp-timezone=35   # 35 -> (GMT+02) Helsinki, Riga, Tallinn
                   #  TimeZone code mapping table:
                   # ----------------------------------------------------
                   #  1 -> (GMT-12) Enewetak, Kwajalein
                   #  2 -> (GMT-11) Midway Island, Samoa
                   #  3 -> (GMT-10) Hawaii
                   #  4 -> (GMT-09) Alaska
                   #  5 -> (GMT-08) Pacific Time (US & Canada); Tijuana
                   #  6 -> (GMT-07) Arizona
                   #  7 -> (GMT-07) Mountain Time (US & Canada)
                   #  8 -> (GMT-06) Central Time (US & Canada)
                   #  9 -> (GMT-06) Mexico City, Tegucigalpa
                   # 10 -> (GMT-06) Saskatchewan
                   # 11 -> (GMT-05) Bogota, Lima, Quito
                   # 12 -> (GMT-05) Eastern Time (US & Canada)
```

```
# 13 -> (GMT-05) Indiana (East)
# 14 -> (GMT-04) Atlantic Time (Canada)
# 15 -> (GMT-04) Caracas, La Paz
# 16 -> (GMT-04) Santiago
# 17 -> (GMT-03) Newfoundland
# 18 -> (GMT-03) Brasilia
# 19 -> (GMT-03) Buenos Aires, Georgetown
# 20 -> (GMT-02) Mid-Atlantic
# 21 -> (GMT-01) Azores, Cape Verde Is.
# 22 -> (GMT) Casablanca, Monrovia
# 23 -> (GMT) Greenwich Mean Time: Dublin, Edinburgh
# 24 -> (GMT) Greenwich Mean Time: Lisbon, London
# 25 -> (GMT+01) Amsterdam, Berlin, Bern, Rome
# 26 -> (GMT+01) Stockholm, Vienna, Belgrade
# 27 -> (GMT+01) Bratislava, Budapest, Ljubljana
# 28 -> (GMT+01) Prague,Brussels, Copenhagen, Madrid
# 29 -> (GMT+01) Paris, Vilnius, Sarajevo, Skopje
# 30 -> (GMT+01) Sofija, Warsaw, Zagreb
# 31 -> (GMT+02) Athens, Istanbul, Minsk
# 32 -> (GMT+02) Bucharest
# 33 -> (GMT+02) Cairo
# 34 -> (GMT+02) Harare, Pretoria
# 35 -> (GMT+02) Helsinki, Riga, Tallinn
# 36 -> (GMT+02) Israel
# 37 -> (GMT+03) Baghdad, Kuwait, Nairobi, Riyadh
# 38 -> (GMT+03) Moscow, St. Petersburg
# 39 -> (GMT+03) Tehran
# 40 -> (GMT+04) Abu Dhabi, Muscat, Tbilisi, Kazan
# 41 -> (GMT+04) Volgograd, Kabul
# 42 -> (GMT+05) Islamabad, Karachi, Ekaterinburg
# 43 -> (GMT+05:30) Indian
# 44 -> (GMT+06) Almaty, Dhaka
# 45 -> (GMT+07) Bangkok, Jakarta, Hanoi
# 46 -> (GMT+08) Beijing, Chongqing, Urumqi
# 47 -> (GMT+08) Hong Kong, Perth, Singapore, Taipei
# 48 -> (GMT+09) Toyko, Osaka, Sapporo, Yakutsk
# 49 -> (GMT+09:30) Darwin, Adelaide
# 50 -> (GMT+10) Brisbane
# 51 -> (GMT+10) Canberra, Melbourne, Sydney
# 52 -> (GMT+10) Guam, Port Moresby, Vladivostok
# 53 -> (GMT+10) Hobart
# 54 -> (GMT+11) Magadan, Solamon, New Caledonia
# 55 -> (GMT+12) Fiji, Kamchatka, Marshall Is.
# 56 -> (GMT+12) Wellington, Auckland
daylight-saving-time-enable=true
daylight-saving-period=01/01, 12/31

[filter]
```

local-filter-enable=false
apmgmt-filter-enable=false
ether-type-filter-enable=false
ether-type-filter-Aironet_DDP=false
ether-type-filter-Appletalk_ARP=false
ether-type-filter-ARP=false
ether-type-filter-Banyan=false
ether-type-filter-Berkeley_Trailer_Negotiation=false
ether-type-filter-CDP=false
ether-type-filter-DEC_LAT=false
ether-type-filter-DEC_MOP=false
ether-type-filter-DEC_MOP_Dump_Load=false
ether-type-filter-DEC_XNS=false
ether-type-filter-EAPOL=false
ether-type-filter-Enet_Config_Test=false
ether-type-filter-Ethertalk=false
ether-type-filter-IP=false
ether-type-filter-LAN_Test=false
ether-type-filter-NetBEUI=false
ether-type-filter-Novell_IPX(new)=false
ether-type-filter-Novell_IPX(old)=false
ether-type-filter-RARP=false
ether-type-filter-Telxon_TXP=false
ether-type-filter-X.25_Level3=false

[802.1X-supplicant]
supplicant-enable=false
supplicant-username=
supplicant-password=

[radio-interface1]
description=
radio-mode=11g+11b
antenna-mode=diversity
low-channel-transmit-limit=100%
mid-channel-transmit-limit=100%
high-channel-transmit-limit=100%
radio-shutdown=false
radio-channel=1
auto-channel=true
tx-power=100%
tx-datarate-max=54
tx-mcast-datarate=1
beacon-interval=100
dtim-interval=1
rts-threshold=2347
frag-threshold=2346
max-associations=128

preamble=long
slot-time=auto
wep-key1=****
wep-key2=****
wep-key3=****
wep-key4=****
ap-detection=disable
ap-scan-interval=720
ap-scan-duration=50
ap-scan-first-time-delay=0
pmksa-life-time=720

[radio-interface1/ssid1]
ssid-enable=true
ssid=julkinen
primary-ssid=true
closed-system=true
default-vlan-id=400
vlan-tagging=true
wpa-version=1+2
security-suite=1
auth-mode=open
encryption=no
wpa-mode=disabled
wpa2-mode=disabled
wpa-key-mgmt=psk
wpa-preshared-key=****
wpa-cipher-ucast=aes and tkip
wpa-cipher-mcast=wep
wep-default-key=0
radius-mac-format=no delimeter
radius-vlanid-format=hex
primary-authentication-server=0.0.0.0
primary-authentication-port=1812
primary-authentication-secret=****
primary-authentication-timeout=5
primary-authentication-retries=3
secondary-authentication-server=0.0.0.0
secondary-authentication-port=1812
secondary-authentication-secret=****
secondary-authentication-timeout=5
secondary-authentication-retries=3
802.1X-authenticator-mode=disable
802.1X-reauthentication-interval=0
802.1X-multicast-key-refresh-interval=0
802.1X-unicast-key-refresh-interval=0
mac-authentication-mode=disable
mac-authentication-session-timeout=0

pre-auth=false
local-mac-permission=allow

[radio-interface1/ssid2]
ssid-enable=true
ssid=hallinto
primary-ssid=false
default-vlan-id=300
vlan-tagging=true
wpa-version=1
security-suite=7
auth-mode=open
encryption=yes
wpa-mode=required
wpa2-mode=disabled
wpa-key-mgmt=dynamic
wpa-preshared-key=****
wpa-cipher-ucast=tkip
wpa-cipher-mcast=tkip
wep-default-key=0
radius-mac-format=no delimeter
radius-vlanid-format=hex
primary-authentication-server=0.0.0.7
primary-authentication-port=1812
primary-authentication-secret=****
primary-authentication-timeout=5
primary-authentication-retries=3
secondary-authentication-server=0.0.0.8
secondary-authentication-port=1812
secondary-authentication-secret=****
secondary-authentication-timeout=5
secondary-authentication-retries=3
802.1X-authenticator-mode=require
802.1X-reauthentication-interval=0
802.1X-multicast-key-refresh-interval=0
802.1X-unicast-key-refresh-interval=0
mac-authentication-mode=disable
mac-authentication-session-timeout=0
pre-auth=false
local-mac-permission=allow

[radio-interface1/ssid3]
ssid-enable=true
ssid=opetus
primary-ssid=false
default-vlan-id=200
vlan-tagging=true
wpa-version=1

security-suite=7
auth-mode=open
encryption=yes
wpa-mode=required
wpa2-mode=disabled
wpa-key-mgmt=dynamic
wpa-preshared-key=****
wpa-cipher-ucast=tkip
wpa-cipher-mcast=tkip
wep-default-key=0
radius-mac-format=no delimeter
radius-vlanid-format=hex
primary-authentication-server=0.0.0.9
primary-authentication-port=1812
primary-authentication-secret=****
primary-authentication-timeout=5
primary-authentication-retries=3
secondary-authentication-server=0.0.0.10
secondary-authentication-port=1812
secondary-authentication-secret=****
secondary-authentication-timeout=5
secondary-authentication-retries=3
802.1X-authenticator-mode=require
802.1X-reauthentication-interval=0
802.1X-multicast-key-refresh-interval=0
802.1X-unicast-key-refresh-interval=0
mac-authentication-mode=disable
mac-authentication-session-timeout=0
pre-auth=false
local-mac-permission=allow

[snmp]
snmp-enable=true
snmp-v3-supported=true
snmp-v3-only=false
snmp-v3-engine-id=00:00:00:0b:00:00:00:1f:fe:a2:cc:90
location=
contact=Contact
readonly-community-name=public
readwrite-community-name=private
trap-target1-enable=false
trap-target1-address=0.0.0.0
trap-target1-community-name=public
trap-target2-enable=false
trap-target2-address=0.0.0.0
trap-target2-community-name=public
trap-target3-enable=false
trap-target3-address=0.0.0.0

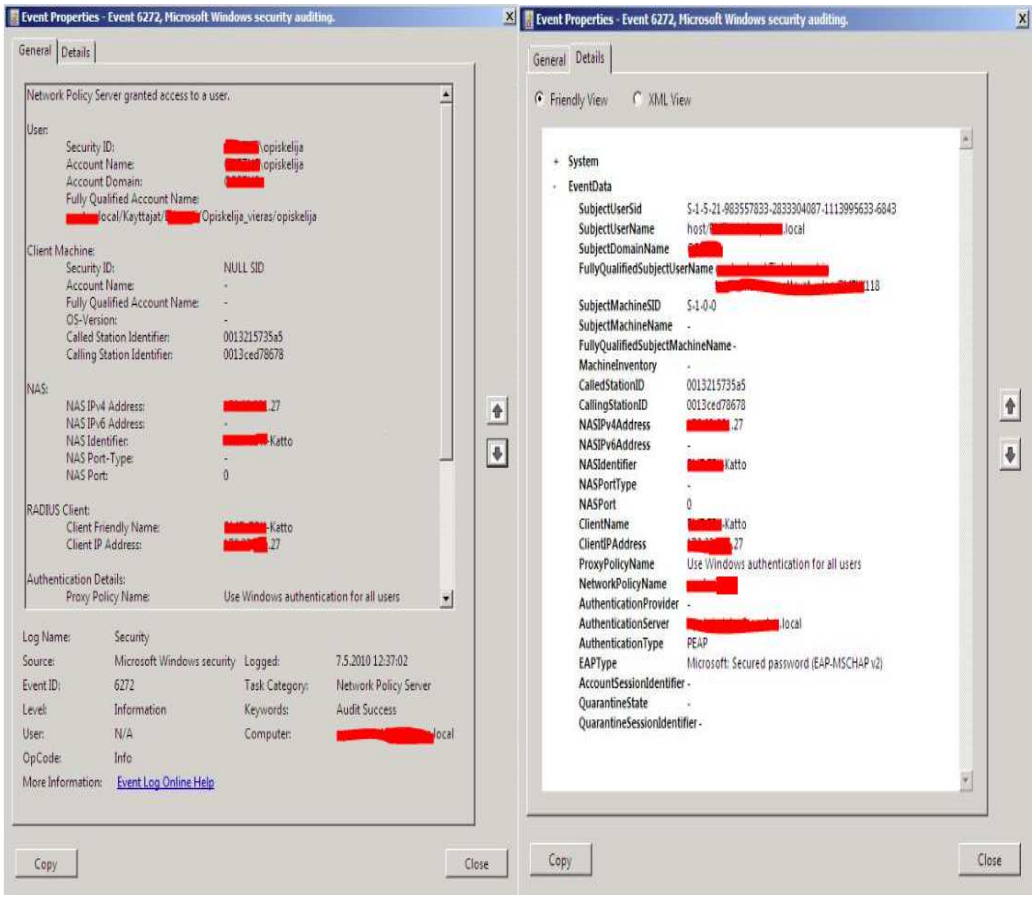
trap-target3-community-name=public
trap-target4-enable=false
trap-target4-address=0.0.0.0
trap-target4-community-name=public
trap-id-hpdot11StationAssociation=enabled
trap-id-hpdot11StationReAssociation=enabled
trap-id-hpdot11StationAuthentication=enabled
trap-id-hpdot11StationRequestFail=enabled
trap-id-hpdot11InterfaceFail=enabled
trap-id-dot1xMacAddrAuthSuccess=enabled
trap-id-dot1xMacAddrAuthFail=enabled
trap-id-dot1xAuthNotInitiated=enabled
trap-id-dot1xAuthSuccess=enabled
trap-id-dot1xAuthFail=enabled
trap-id-localMacAddrAuthSuccess=enabled
trap-id-localMacAddrAuthFail=enabled
trap-id-iappStationRoamedFrom=enabled
trap-id-iappStationRoamedTo=enabled
trap-id-iappContextDataSent=enabled
trap-id-sntpServerFail=enabled
trap-id-sysSystemUp=enabled
trap-id-sysSystemDown=enabled
trap-id-sysRadiusServerChanged=enabled
trap-id-sysConfigFileVersionChanged=enabled
trap-id-dot1xSupplicantAuthenticated=enabled
trap-id-wirelessExternalAntenna=enabled
trap-id-possibleRogueApDetected=enabled
trap-id-httpEnableStatusSet=enabled
trap-id-httpsEnableStatusSet=enabled
trap-id-cliSerialPortEnableStatusSet=enabled
trap-id-cliTelnetPortEnableStatusSet=enabled
trap-id-snmpVersionFilterSet=enabled
trap-id-resetButtonEnableStatusSet=enabled
trap-id-vlanUntaggedSet=enabled
trap-id-mgntVlanIdSet=enabled
trap-id-ssidPrimarySet=enabled
trap-id-apScanDoneAndNewApDetected=enabled
trap-id-apScanEnableStatusSet=enabled
trap-id-apScanNow=enabled
trap-id-adHocDetected=enabled
trap-id-hpdot11BeaconTransmissionOk=enabled
trap-id-hpdot11BeaconTransmissionFail=enabled
trap-id-sshEnableStatusSet=enabled
trap-id-radiusAcctEnableStatusSet=enabled
trap-id-qosSvpEnableStatusSet=enabled

[lldp]
lldp-msg-tx-interval=30

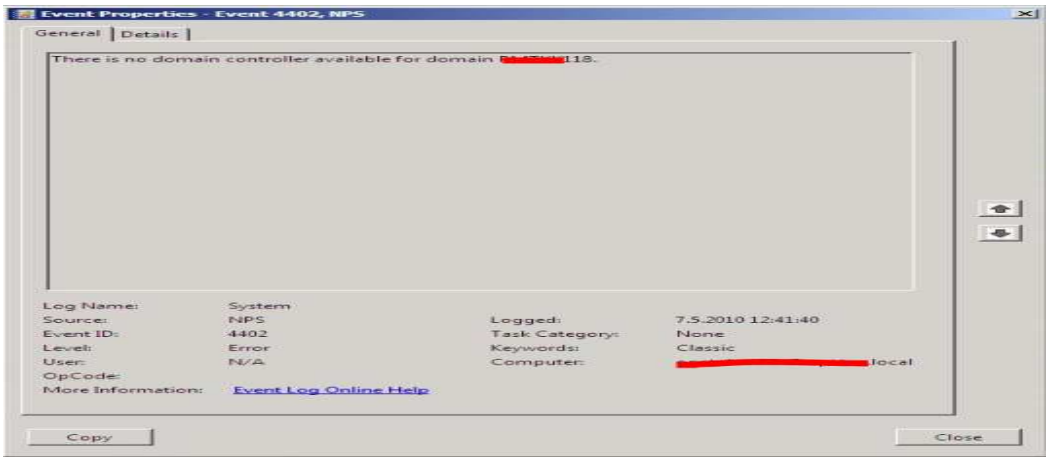
lldp-msg-tx-hold-mul=4
lldp-reinit-delay=2
lldp-tx-delay=2
lldp-enabled=true
lldp-ports-count=1
lldp-lport0-index=2
lldp-lport0-admin-status=enabledTxOnly
lldp-lport0-basic-tlvs-tx-flag=240

Liite 2

ONNISTUNUT JA EPÄONNISTUNUT KIRJAUTUMINEN



Käyttäjän sekä tietokoneen onnistunut kirjautuminen



Epäonnistunut kirjautuminen: syy kone ei ole toimialueella