LANGATTOMAN VERKON KÄYTTÖÖNOTTO

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2009
Vesa Niittylä

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

NIITTYLÄ, VESA: Langattoman verkon käyttöönotto

Tietoliikennetekniikan opinnäytetyö, 37 sivua, 24 liitesivua

Kevät 2009

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee langattoman lähiverkon käyttöönottoa osaksi erään kaupungin lähiverkkoa. Langattoman lähiverkon (WLAN) kattavuutta haluttiin laajentaa kaupungin kahden erillisen rakennuksen tiloissa. Myöhemmin verkkoa on mahdollista laajentaa kaupungin eri alueille ja näin todennäköisesti aiotaan tehdä. Tämän opinnäytetyön tavoitteena on langattoman lähiverkon käyttöönotto kahden erillisen rakennuksen tiloissa.

WLAN:n kehitystyötä tekevät IEEE:n työryhmät kehittävät jatkuvasti standardejaan. Langattoman lähiverkon kehityksen tuloksena verkon toteutuksessa pyritäänkin ottaa käyttöön viimeisimpiä tekniikoita, kuten tässä työssä käyttöön otetut 802.11i ja 802.1X. Myös laitevalmistajien kehitystyön takia uusia tekniikoita otetaan käyttöön.

Langaton verkko päätettiin toteuttaa Hewlett Packardin radioporttijärjestelmällä. Siihen kuuluu tietyn mallisiin kytkimiin liitettävä moduuli ja radioportit, joiden toimintoja edellä mainittu moduuli hallitsee. Radioportteja otettiin käyttöön kuusi kappaletta, kolme kumpaankin rakennukseen. Ohjelmistoista otettiin käyttöön ainoastaan välttämättömät, ja laitehankintoja ja asennuksia tehtiin vain tarvittaessa.

Avainsanat: WLAN, ProCurve Wireless Edge Services -moduuli, 802.11i

Lahti University of Applied Sciences
Faculty of Technology

NIITTYLÄ, VESA: Deployment of a wireless network

Bachelor's Thesis in Telecommunications Technology, 37 pages, 24 appendices

Spring 2009

ABSTRACT

This study deals with the deployment of a wireless network in a town. There was already a wired network and a small-scale wireless network (WLAN) in use. The coverage of the wireless network is to be expanded. The purpose of the study was to deploy a WLAN with a new architecture in two separate buildings.

Continuous WLAN development is done by a work group of the Institute of Electrical and Electronics Engineers and new standards are introduced regularly. Their work is followed with interest and the latest techniques, such as 802.11i and 802.1X, are deployed. Also hardware manufacturers introduce new products, enabling new technologies.

The wireless network was built with a system developed by Hewlett Packard which uses radio ports and a wireless network module that can be used on a certain switch. The module controls the radio ports. Six radio ports were taken in use, three in each building. Only the most necessary programs were taken in use. It was necessary to make some extra equipment acquisitions and installations, such as an extra switch, to one of the buildings.

Keywords: WLAN, ProCurve Wireless Edge Services module, 802.11i

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, Authorization ja Accounting. AAA-palvelut. Tunnistus, valtuutus ja laskutus.
ACL	Access Control List, pääsylistat, on osa tietoturvasuojausta. Reititin suorittaa pakettisuodatusta siirtotiellä listan mukaisesti.
AES	Advanced Encryption Standard. Rijndael-algoritmiin perustuva lohkosalausmenetelmä.
CBC-MAC	Cipher Block Chaining Message Authentication Code. CBC-MAC on osa CCMP-protokollaa.
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. AES-salausta käyttävä salausmenetelmä.
DHCP	Dynamic Host Configuration Protocol. Protokolla IP-osoitteiden jakoon työasemille.
EAP	Extensible Authentication Protocol. Todennusprotokollan runko.
IEEE	The Institute of Electrical and Electronics Engineers. Yhdysvalloissa perustettu sähkö- ja elektroniikka-alan insinöörijärjestö. IEEE-SA (Standard Association) on luonut WLAN-verkkoja määrittelevät IEEE-standardit.
LAN	Local Area Network, lähiverkko.

MIC	Message Integrity Check. Tarkistussummain paketin eheyden todentamiseen. Tunnetaan myös nimellä Michael.
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2. Autentikointiprotokolla, jossa käytetään käyttäjätunnusta ja salasanaa.
NAT	Network Address Translation tarkoittaa yhdessä verkossa (sisäverkko) käytetyn IP-osoitteen muuttamista toisessa verkossa (ulkoverkko) tunnetuksi IP-osoitteeksi.
OSI-malli	Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien viitemalli, jossa on seitsemän kerrosta: Fyysinen kerros, Siirtoyhteyskerros, Verkkokerros, Kuljetuskerros, Istuntokerros, Esitystapakerros ja Sovelluskerros.
PEAP	Protected EAP. EAP-todennusmenetelmä.
QoS	Quality of Service. Tiedonsiirtopalvelun lisäominaisuus, joka mahdollistaa tiedonluokittelun sen aikakriittisyyden perusteella.
RADIUS	Remote Authentication Dial-in User Services. Käytetään keskitettyyn käyttäjäoikeuksien vahvistamiseen, valtuuttamiseen ja tilitietojen hallintaan.
RC4	Rivest Cipher 4. Symmetrinen jonosalaaja, jossa tieto salataan tavu kerrallaan. Tunnetaan myös nimellä Ron's Code 4.
SSID	Service Set Identifie. WLAN-verkon tunnus.

TKIP	Temporal Key Integrity Protocol. WEP-salauksen heikkouksia paikkaava salausmenetelmä.
VLAN	Virtual LAN. Virtuaalilähiverkko on tekniikka, jolla fyysinen tietoliikenneverkko jaetaan loogisiin osiin. Yleisin virtuaalilähiverkkoprotokolla on IEEE 802.1Q.
VPN	Virtual Private Networking. Tietoturvamenetelmä, jossa käytetään salattua tunnelia tiedonsiirrossa. Useimmiten ensin luodaan salattu tunneli salausavainten vaihtoa varten ja sitten uusi salattu tunneli varsinaiseen datan siirtoon.
WEP	Wired Equivalent Privacy. WLAN-verkoissa käytettävä salausmenetelmä. WEP:n salaus on murrettavissa.
WLAN	Wireless Local Area Network, langaton lähiverkko.
WPA	Wi-Fi Protected Access. Langattoman lähiverkon tietoturvaprotokolla.
WPA2	Wi-Fi Alliancen käyttämä merkintä. Taataan keskinäinen yhteensopivuus IEEE 802.11i-standardin mukaisille laitteille.

1 JOHDANTO

Tietokoneiden kehityksen voidaan sanoa tulleen vaiheeseen, jossa kooltaan pienempien tietokoneiden tehokkuus alkaa riittää moneen tarpeeseen. Pöytäkoneita ei enää ole tarvetta hankkia pienempien kustannuksien tai paremman suorituskyvyn takia. Kannettavat koneet ja verkottuminen ovat tehneet langattoman lähiverkon WLAN:n (Wireless Local Area Network) käytöstä yleisen. Lisäksi WLAN:n suorituskyky ja tietoturva ovat vuosien kehitystyön tuloksena parantuneet merkittävästi. Näin ollen langattoman verkon käytön lisääminen on kaupungin tiloissa tullut ajankohtaiseksi.

Ennen tämän työn alkua toisessa rakennuksista oli langallisen verkon lisäksi yksi langattoman verkon tukiasema, joka mahdollisti pääsyn kaupungin sisäverkkoon. Toisessa sen sijaan ei ollut lainkaan käytössä langatonta verkkoa. Tämä yhden tukiaseman verkko otetaan pois käytöstä, kun kattavampi verkko on mahdollista ottaa käyttöön. Verkko on ajateltu toteuttaa tukiasemia vastaavalla radioporttiverkostolla. Keskitetysti hallittavien radioporttien kautta mahdollistetaan pääsy kaupungin sisäiseen verkkoon. Liikenne kulkee tarkoitukseen varatussa virtuaalisessa lähiverkossaan eli VLAN:ssa (Virtual LAN) pääkytkimen langattoman verkon moduulille asti. Tämän jälkeen käyttäjä saa verkkoresursseja käyttöönsä AD-tietokannan (Active Directory) mukaisesti.

Myöhemmin verkkoa on mahdollista laajentaa kaupungin eri alueille ja näin tullaan todennäköisesti myös tekemään. Radioporttien määrän kasvaessa keskitetty hallinta on ensiarvoisen tärkeää. Laitteiden yhteensopivuus parantaa vikasietoisuutta.

Tämän opinnäytetyön tavoitteena on hallittavan langattoman lähiverkon käyttöönotto kaupungin verkon osana. Teoriaosuudessa käydään läpi työn kannalta oleellisia lähiverkon tekniikoita, kuten 802.11i, 802.1X, 802.1q ja PEAP (Protected Extensible Authenticatio Protocol). Lisäksi esitellään langattoman lähiverkon muita tekniikoita sekä laitteita, joilla langattoman lähiverkon käyttöönotto toteutetaan. Valitussa toteutustavassa hyödynnetään keskitettyä hallintaa tukevia laitteilla.

2 WLAN

2.1 Langattoman lähiverkon kehitys

Tässä opinnäytetyössä langattomalla verkolla viitataan IEEE:n (the Institute of Electrical and Electronics Engineers) 802.11 langattoman lähiverkon standardiin. ETSI:n (European Telecommunications Standards Institute) HiperLAN on myös langaton lähiverkko, mutta HiperLAN-standardin mukaisten laitteiden käyttö on vähäistä. (WLAN 2008.)

Ensimmäinen 802.11 perheen standardi esiteltiin vuonna 1997. Nykyään merkittävänä pidettyä liikenteen salausta ei ollut, tosin käyttäjämäärät ja väärinkäytön uhka olivat vielä alkuun vähäiset. Kahden Mbit/s yhteysnopeus olikin suurimpia esteitä käytön yleistymiselle. Vaikka alkuperäisen standardin mukaisia laitteiden käyttöönotto ei ollut yleistä, standardi sisälsi jo monia tekniikoita, joita nykyisetkin tukiasemat käyttävät. Yhteneväisyyksiä 802.11 ja sen laajennuksien välillä on verkkotopologian lisäksi taajuusalueiden ja radiotaajuustekniikoissa käytössä (2,4GHz taajuusalue ja suorasekvenssihajaspektritekniikan, DSSS). (802.11 2008.)

Standardi sai jatkoa ensin 802.11b ja 802.11a -standardeista vuonna 1999. Myöhemmin vuonna 2003 esitettiin 802.11g -standardi. Teoreettiset nopeudet kasvoivat: 802.11b:ssä CCK-tekniikan (Complementary code keying) myötä siirtonopeus kasvoi 11Mbit/s ja 802.11a:ssa sekä 802.11g:ssä OFDM-tekniikan (orthogonal frequency division multiplexing) myötä 54Mbit/s. Lisäksi liikenne ei enää liikkunut täysin suojaamattomana, vaan WEP (wired equivalent privacy) oli mahdollista ottaa käyttöön. (802.11 2008.)

Pari vuotta WEP:n käyttöönoton jälkeen WEP:n todistettiin sisältävän monia tietoturvariskejä, joten seuraavan standardin tärkeimmäksi kehityskohteeksi tulikin ratkaista tietoturvan ongelmia. Kolmen ja puolen vuoden kehitystyön tuloksena toukokuussa 2004 esiteltiin 802.11i. Tosin, jo vuotta aiemmin esiteltiin

WPA (Wireless Fidelity Protected Access), joka sisälsi valmiit ja vakaimmat osat tulevasta 802.11i standardista. 802.11i sisältää vahvemman salauksen, autentikoinnin ja paremman strategian avainten hallintaan. Muutoksia oli tarkoitus tehdä myös Quality of Service:n (QoS) osalta, mutta kehitystyö jakaantui kahtia QoS:iin keskittyneeseen 802.11e:n ja tietoturvaan keskittyneeseen 802.11i:n. (Halasz 2004.)

2.2 WEP

WEP esiteltiin vuonna 1999 osana 802.11a- ja 802.11b -standardeja. Avainten jako oli alku aikoina suurissa verkoissa työteliästä ja sinällään tietoturvariski. Tähän oli kuitenkin ratkaisu. WEP-avainten jakaminen helpottui, kun langattoman verkon käyttäjät tunnistettiin autentikointipalvelimen avulla. Autentikointi-palvelimen hyödyllisyys korostuu verkon laajentuessa. (Kotilainen 2003, 16 – 17.)

WEP tekniikasta löydettiin tietoturva-aukkoja, joista vakavin liittyy alustusvektoreihin. Tämän tietoturva-aukon laitetoimittajat pyrkivätkin paikkaamaan uuden ohjelmistopäivityksen avulla: laitteiden salausalgoritmia muutettiin, jotta heikkojen alustusvektorien syntyminen saataisiin ehkäistyä. Näitä ohjelmistoja saatetaan kutsua WEP-standardin paremmiksi versioiksi, mutta prosessi toteutetaankin tällöin standardista poikkeavalla tavalla. WPA toi sen sijaan standardin mukaisen tavan korjata WEP:n puutteita. Mainitsemisen arvoista on myös, ettei WEP käytä istuntokohtaisia avaimia. Tämän takia avaimen tietävillä on mahdollisuus seurata toisten käyttäjien tietoliikennettä. Siinä mielessä WEP:n käyttö vastaa avointa verkkoa. (Kotilainen 2003, 16.)

WEP:ä käyttävän verkon saa tietoturvalliseksi käyttämällä lisäksi salattua VPN-tunnelia (virtual private network). Työaseman ja VPN-yhdyskanavan välille luodaan salattu yhteys eli tunneli. Tällöin liikenne on siis salattua fyysistä ja siirtoyhteyskerrosta ylemmällä OSI-tasolla (Open Systems Interconnection). (Kotilainen 2003, 16-18.)

2.3 WPA

WPA:sta tuli välivaiheen tietoturvatekniikka, johon sisällytettiin tekeillä olleen tietoturvaan keskittyvän 802.11i:n valmiit ja vakaimmat osa-alueet. Wireless Fidelity Protected Access:ssa on pyritty yhteensopivuuteen niin nykyisten kuin tulevienkin laitteiden kanssa: tarvittavat fyysiset komponentit ovat samat kuin aikoinaan WEP:ä käyttäneissä laitteissa. WPA sertifikoiduissa laitteissa voidaan käyttää kehittyneempää prosessia datan salaukseen.

TKIP (Temporal Key Integrity Protocol) toimii WPA:ssa WEP-salauksen paikkaajana.
TKIP lisää neljä uutta algoritmia WEP:iin. Nämä ovat

- MIC (message integrity code), joka tunnetaan myös sanalla Michael, vastustaa sanomien väärentämistä.
- IV sequencing discipline, poistaa toistohyökkäyksen mahdollisuuden.
- A per-packet key mixing function, hävittää heikot alustusvektorit.
- A rekeying mechanism, ehkäisee avaimen uudelleen käyttöä hyödyntävän hyökkäyksen. (Walker 2003.)

WPA:ssa liikenne salataan RC4-algoritmilla (Rivest Cipher 4), mutta toisin kuin WEP:ssa, salausavaimen pituus on pitempi 128 bittiä. WPA:n heikkoutena pidetään sen alttiutta palvelunestohyökkäyksille. Tämä liittyy Michael algoritmiin liitettyyn vastatoimeen; joka toimii seuraavasti: kun vastaanotetaan kaksi väärennettyä viestiä peräkkäin oletetaan hyökkäyksen olevan käynnissä ja koko verkon suljetaan minuutiksi. Tällöin myös verkon lailliset käyttäjät jäävät katkon aikana ilman palvelua. Ilman vastatoimen olemassaoloa väärennettyjä sanomia voisi lähettää rajoituksetta ja näin ollen jotakin viestiä pidettäisiin oikeana. (Walker 2003.)

Vuoden 2008 Marraskuussa uutisoitiin WAP:n mahdollisesta osittaisesta murrosta TKIP:n osalta. Aiemminkin on tiedetty salauksen olevan murrettavissa pitkän ajan tai suuren laskentakapasiteetin myötä, mutta uutisessa viitattiinkin murtoon tarvittavan ajan dramaattisella putoamisella. Pahimmillaan tämä murto tarkoittaisi sitä, että dataliikennettä reitittimen ja tietokoneen välillä voitaisiin lukea ja reitittimeen kytkettyyn laitteeseen voitaisiin lähettää väärää dataa. Vaikuttaa kuitenkin siltä, ettei kyseessä ole varsinainen murto, varsinkaan samalla tavalla kuin WEP:ssa. Varsinaista dataa ei saada luettua lukuun ottamatta lyhyitä DNS- ja ARP-paketteja. Havaintoa voidaan kuitenkin pitää merkittävä, koska se luo pohjaa lisäselvityksille ja saattaa jouduttaa varsinaisen murron kehittämistä. (Pitkänen 2008; Zoller 2008.)

2.4 802.11i ja WPA2

Vuonna 2004 esitellyn 802.11i-standardin ja WPA:n suurin eroavaisuus on mahdollisuus käyttää CCMP-menetelmää (Counter Mode with CBC-MAC Protocol), joka hyödyntää symmetristä lohkosalausalgoritmia AES:aa (Advanced Encryption Standard). TKIP:ä voidaan kuitenkin edelleen käyttää. (Griffith 2004.)

AES käyttöönoton huonona puolena voidaan pitää sitä, että salaamiseen ja salauksen purkuun keskittyvän piirin lisääminen on tarpeen. Vaikka AES-salaus voitaisiin ottaa käyttöön ilman tälle omistautunutta piiriä, suorituskyky voi heikentyä liian paljon. Toisaalta joidenkin mielestä tietoturvan lisäämiseksi tulisi käyttää vieläkin pitempiä salausavaimia kuin useimmiten käytetään, mutta päätelaitteidenkin piirien suorituskyky ei välttämättä enää riitä. AES:n salauksen käyttöä pidetään 128 bittisenäkin merkittävänä parannuksena aiempaan, joten AES:n käyttöönotto on suositeltavaa. (Kindervag 2006.)

802.11i:sta on Enterprise ja Personal versiot. Kotikäyttäjille ja pienille yrityksille tarkoitettu Personal versio ei vaadi 802.1X- ja EAP-tunnistuksen käyttöä vaan käyttää ennalta jaettua avainta, PSK (pre-shared key). (Griffith 2004.)

WPA2 muistuttaa IEEE 802.11i:tä, mutta poikkeaa siitä hieman mahdollistaen paremman yhteensopivuuden WPA:n kanssa. Jos tukiasema ja sen asiakas käyttävät WPA2:sta ja ainoastaan CCMP:tä, toiminta on standardin 802.11i mukaista. Sen sijaan, tukiaseman hyväksyessä salaukseksi sekä CCMP:n että TKIP:n, kyseessä on sekoitus 802.11i:a ja WPA:ta. (Halasz 2004.)

2.5 MAC-osoite ja tukiaseman tunnus, SSID

Verkkoliikenne käyttää OSI-mallin toisessa tasossa MAC-osoitteita. Laitteet siis erottuvat toisistaan MAC-osoitteen avulla, joten suodatuksella voidaan sallia vain tietyn MAC-osoitteen omaaville laitteille pääsyn verkon osaksi. MAC-osoitteiden suodatuksella on kuitenkin heikkoutensa: MAC-osoite voidaan muuttaa asetuksista halutuksi, joten jos sallittujen listalla olevan laitteen MAC-osoite tunnetaan voidaan toiselle laitteelle antaa sama osoite. Lisäksi laitteiston vaihtuminen ja niiden suuri määrä saattaa tehdä suodatuslistojen kokoamisen työlääksi.

SSID (Service Set Identifier) ja BSSID (Basic SSID) ovat WLAN-verkon tunnuksia. Tunnuksen voi asettaa piilotetuksi, jolloin tukiasema ei aktiivisesti lähetä tunnustaan ja eikä näin ollen näy millekään laitteelle niin pitkään, kuin verkon tunnuksen tietävä laite yrittää ottaa tukiasemaan yhteyttä.

2.6 WLAN arkkitehtuuri

Langattomat lähiverkot voidaan toteuttaa erilaisilla topologialla eli verkkoarkkitehtuureilla; vaihtoehdot ovat ad-hoc ja infrastruktuuriverkko. Ad-hoc verkossa langattoman verkon päätelaitteet kommunikoivat suoraan toistensa kanssa eikä välille tarvita tukiasemaa. Infrastruktuuritopologiassa sen sijaan käytetään yhtä tai useampaa tukiasemaa, joiden kautta työasemien välinen tietoliikenne kulkee.

Tässä työssä WLAN arkkitehtuuriksi määräytyy infrastruktuuriverkko ja sen laajempi versio ESS (Extended Service Set), jossa useat tukiasemat (tai radioportit) ovat yhdistetty toisiinsa. Tämän työn radioportit eivät tosin lähetä toisilleen dataa, vaan kaikki radioportin data kulkee WES-moduulin kautta.

2.7 WLAN kuuluvuusalue

Kuuluvuusmittauksia tehdessä ja verkon kattavuutta suunniteltaessa on radiotaajuuksien käytön rajoituksista hyvä olla perillä. 2,4Ghz taajuusalue on Suomessa vapaasti käytettävissä ja tätä taajuusaluetta käytetään standardeissa 802.11b ja 802.11g. Sen sijaan osassa langattomien lähiverkkojen standardeja käytetään 5GHz taajuutta, jonka käyttö Suomessa on ainakin ollut hyväksytty ainoastaan sisätiloissa. 802.11a radioportti tulisikin mahdollisesti sulkea, tai lähetystehoa voitaisiin vähentää niillä alueilla, joilla verkko kattaa rakennuksien ulkopuolelle jääviä alueita. (Viestintävirasto 2006.)

Verkon kattavuutta ja yhteyksien laatua ei voida useimmiten parantaa lähetystehoa kasvattamalla, koska suurin mahdollinen lähetysteho on yleensä jo käytössä. Lähetystehoa saatetaankin päinvastoin joutua vähentämään, kuten ottaessa käyttöön suuntaavan antennin, koska enimmäislähetystehon ei saa ylittyä missään suunnassa. Suuntaavat antennit kuitenkin parantavat kykyä vastaanottaa dataa, koska muista suunnista tulevien häiriösignaalien vaikutus vähenee. Aina ei tosin ole mahdollistakaan ottaa ulkoista antennia käyttöön. (Hämäläinen 2003, 55.)

3 AUTENTIKOINTI

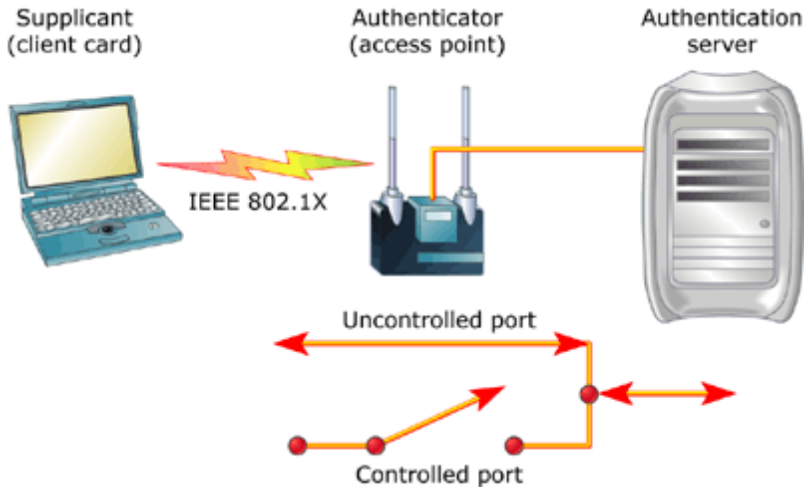
3.1 Autentikointipalvelin

WPA2:n Enterprise versiossa käyttäjä on tunnistettava käyttämällä erillistä autentikointipalvelinta (AAA-palvelin). Autentikointipalvelimen käyttö on ollut toki yleistä suuremmissa verkoissa jo ennen WPA:n käyttöönottoa. Autentikointipalvelimista tunnetuin on RADIUS (Remote Authentication Dial In User Service). RADIUS:n toteutustapoja ovat mm. freeRADIUS ja Microsoftin IAS (Internet Authentication Service).

Aikoinaan käytössä olleessa WEP:ssa, WEP-avainten jako saattoi olla suurissa verkoissa työteliästä ja sinällään tietoturvariski. WEP-avainten jakaminen helpottui, kun langattoman verkon käyttäjät tunnistettiin autentikointipalvelimen avulla. Autentikointipalvelimen hyödyllisyys korostuukin verkon ollessa laaja. (Kotilainen 2003, 16 – 17.)

3.2 Porttikohtainen todentaminen 802.1X

Alunperin 802.1X tekniikka suunniteltiin lankaverkossa käytettäväksi, mutta standardiin tehtiin myöhemmin laajennus, joka mahdollisti sen käytön WLAN-verkoissa. 802.1X:ssa on kyse porttikohtaisesta todentamisesta (Port-Based Network Access Control). Kuvio 1 havainnollistaa 802.1X:n toimintaperiaatetta.



KUVIO 1. 802.1X:n periaate. (Halasz 2004.)

802.1X toimii runkona verkkoon yhteyttä ottavan laitteen, tukiaseman ja autentikointipalvelimen välisessä viestinnässä. Lisäksi tarvitaan käyttäjän tunnistusprotokollaa (esim. PEAP, Protected Extensible Authentication Protocol) ja AAA-protokollaa (esim. RADIUS).

3.3 RADIUS-palvelin

RADIUS on palvelin, johon keskitetään yhteydenottopyynnöt. RADIUS-palvelin tarjoaa kolmea palvelua lyhenteestä AAA: authentication, accounting ja authorizing. Authentication tarkoittaa käyttäjän tunnistautumista (autentikointi), Accounting käyttäjän toiminnan kirjaamista ja Authorization käyttäjän oikeuksien ja käytettävissä olevien palveluiden hallintaa. (Phifer 2003.)

Langaton tukiasema tai kytkin toimii NAS-laitteena (Network Access Server) ja on RADIUS-palvelimen asiakas. RADIUS-viestejä varten käytetään yhteistä salaisuutta (Shared Secret) NAS:n ja palvelimen molemminpuoliseen tunnistamiseen. Yhteinen salaisuus konfiguroidaan täten kummankin asetuksiin.

Autentikointipyynnön tullessa palvelimelle katsotaan onko käyttäjän tietoja tietokannassa, kuten Microsoft Active Directory:ssa (AD). (Phifer 2003.)

3.4 EAP-protokolla

EAP (Extensible Authentication Protocol) on käyttäjäntunnistusprotokolla, joka alunperin kehitettiin PPP-yhteyksiin (Point to Point). Myöhemmin EAP sovitettiin yhteensopivaksi 802.1X-protokollan kanssa. EAP on runko todennusprotokollalle, jolla käytettävä tunnistusmenetelmä voidaan neuvotella.

EAP hoitaa joitakin yleisiä toimintoja ja vuoropuhelua tunnistusmenetelmälle. Tunnistusmenetelmiä on noin 40 erilaista, joista PEAP (Protected EAP) on käytetyimpiä. 802.1X:ä käytettäessä enkapsulointia kutsutaan EAPOL:ksi (EAP over LAN). (EAP 2008.)

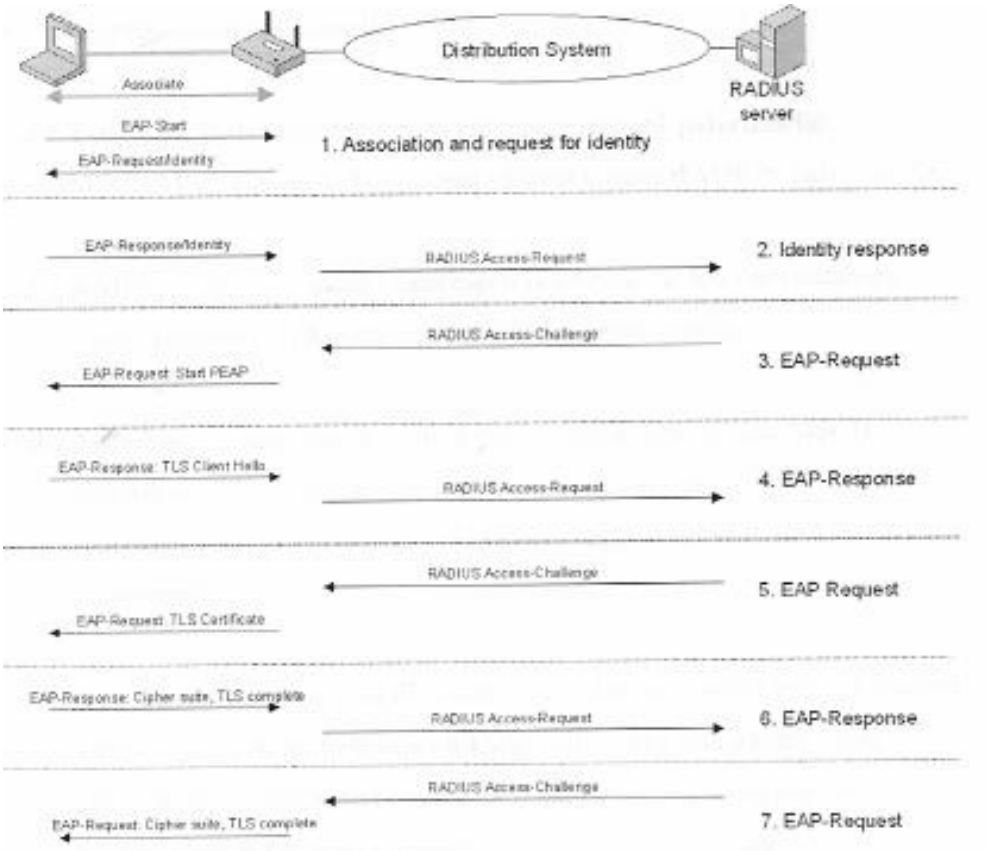
3.5 PEAP

PEAP:n (Protected EAP) autentikointi on kaksivaiheinen: ennen varsinaisten autentikointiviestien lähettämistä luodaan salattu SSL/TLS (Secure Sockets Layer / Transport Layer Security) -tunneli asiakkaan ja autentikointipalvelimen välille.

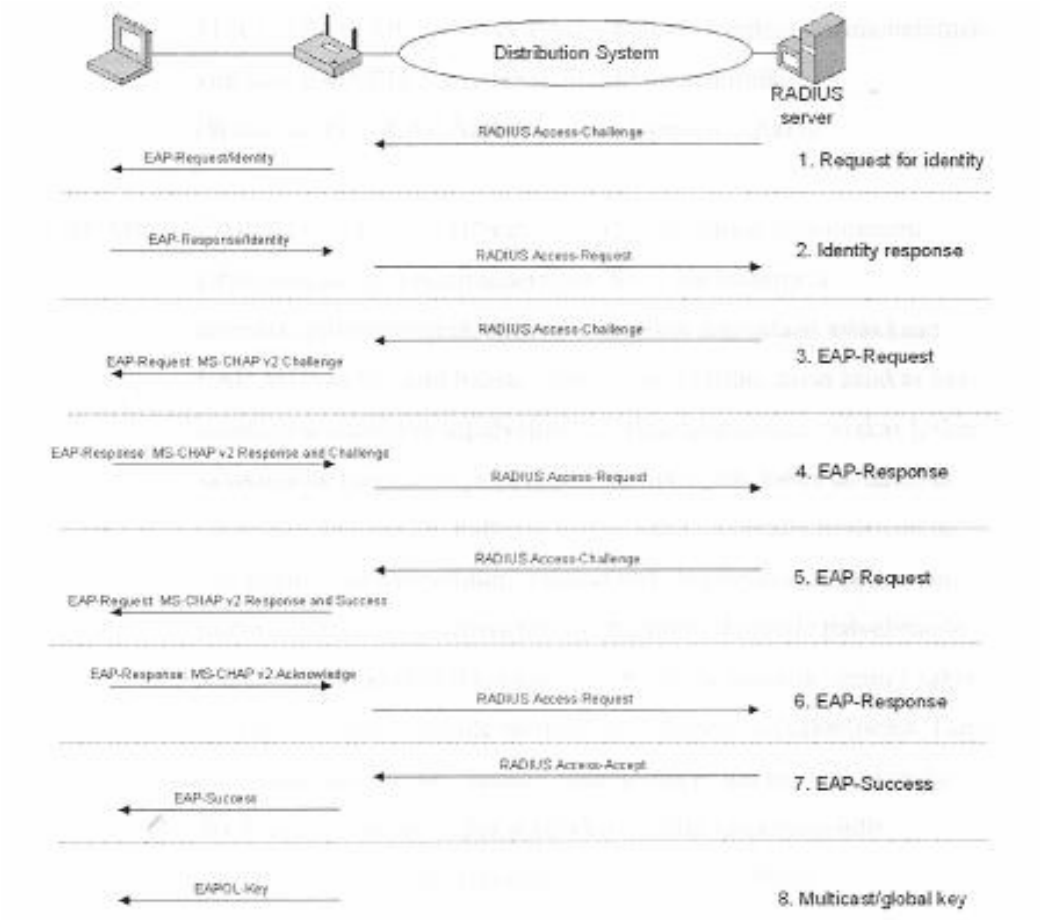
PEAP:sta on olemassa kaksi versiota: PEAPv0/EAP-MSCHAPv2 sekä PEAPv1/EAP-GTC. Kummallakin on lisäksi vaihtoehtoisena sisäisenä EAP-menetelmänä EAP-SIM (Subscriber Identity Module). (PEAP 2008.)

PEAPv0/EAP-MSCHAPv2 on kaikkiaan toiseksi tuetuin EAP-standardi, joka jää jälkeen ainoastaan EAP-TLS:sta (EAP-Transport Layer Security). Kummassakin edellä mainitussa tekniikassa hyödynnetään sertifikaatteja, mutta PEAPv0/EAP-MSCHAPv2:ssa sertifikaatti on vain palvelimessa. Näin ollen PEAP on helpompi ottaa käyttöön. Ohessa kuviot 2 ja 3, joissa PEAP-autentikoinnin vaiheet

esitetään. MSCHAPv2 on haaste-vastaus-autentikointiprotokolla, joka on kehitetty alun perin VPN-yhteyksien autentikointiin. On olemassa myös lähes ainoastaan Microsoftin tukema PEAP-EAP-TLS, jonka toiminta on hyvin samankaltainen kuin EAP-TLS:n. Erot näiden välillä liittyvät asiakkaan sertifikaatin salaukseen. (Alatalo 2005, 21; PEAP 2008.)



KUVIO 2. PEAP-autentikoinnin ensimmäinen vaihe (Alatalo 2005, 22)



KUVIO 3. PEAP-autentikoinnin toinen vaihe: MSCHAPv2-autentikointiprosessi (Alatalo 2005, 24)

4 VLAN

Virtuaalilähiverkko VLAN on tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisesti eri osiin. Verkon aktiivilaitteiden portit liitetään kuulumaan haluttuun loogiseen verkkoon tai useampaan. Näin ollen voidaan käyttää yhteyksien luomiseen yhtä kytkintä ilman, että luodaan kaikkien kytkimeen liitettyjen laitteiden välille yhteyttä. Virtuaalilähiverkkojen käyttöönotto vaatii aktiivilaitteilta tuen. Virtuaalilähiverkkoja tukevat laitteet liittävät lähettämiinsä paketteihin verkon tunnuksen. Lähetettäessä paketteja eteenpäin laitteelle, joka ei tue virtuaalilähiverkkoja, tunnus poistetaan. Virtuaalilähiverkkoprotokollista yleisin on IEEE 802.1q. (VLAN 2008.)

Aktiivilaitteiden porttien määrityksissä käytetään tiloja tagged ja untagged. Tagged-porttiin lähetettävään pakettiin liitetään virtuaalilähiverkkotunnus ja untagged-porttiin (VLAN tuki puuttuu) lähetettävästä paketista poistetaan mahdolliset tunnukset. Laitteen portti voi olla vain yhden virtuaalilähiverkon untagged-jäsen, mutta useamman virtuaalilähiverkon tagged-jäsen. (VLAN 2008.)

5 LAITEVERTAILU

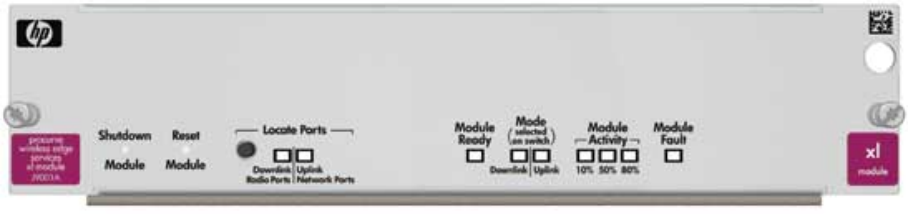
5.1 Keskitetty hallinta

Langattoman lähiverkon päätelaitteiden keskitetylle hallinnalle on tarvetta luoda yhteinen standardi, mutta yhtä tiettyä mallia ei ole kuitenkaan määritelty standardiksi. Protokollamalleilla on yhteistä muodostuminen WLAN-kontrollerista ja keskitettyä hallintaa tukevista tukiasemista. (Hämäläinen 2007, 54.)

Laitevalmistajista ainakin HP ja Cisco ovat kehittäneet keskitettyä hallintaa tukevia laitteita. Laitteet eivät ole keskenään yhteensopivia, eli Cisco Wireless LAN Controller ei ole yhteensopiva HP:n radioporttien kanssa.

5.2 ProCurve Wireless Edge Services (WES) xl -moduuli

Hewlett Packard on luonut keskitettyyn hallintaan perustuvan WES-radioportti-järjestelmällä. Järjestelmässä radioportteja hallitaan WES-moduulilla (KUVIO 4). Käyttäjien ja laitteiden keskitetty hallinta on riippumaton käytetystä yhteystekniikasta. (Hämäläinen 2007, 57.)



KUVIO 4. ProCurve Wireless Edge Services xl -moduuli

WES xl-moduuli on yhteensopiva HP:n 5300xl-sarjan kytkimien kanssa. Kytkimessä on kaikkiaan kahdeksan moduulipaikkaa ja kytkin tukee kahden WES-moduulin käyttöä. Yksittäinen WES-moduuli tukee 12 radioporttia ja lisälisensseillä yhteensä 36 radioporttia. Kytkintä kohden voidaan siten ottaa käyttöön yhteensä 72 radioporttia. (WES-esite 2007.)

5.3 Cisco Wireless LAN Controller

Ciscon langattoman verkon kontrollerit käyttävät LWAPP-protokollaa (Light weight Access Point Protocol). WLAN-kontrolleri hallitsee Lightweight-tukiasemia. Kontrolleri ottaa tehtäväkseen mm. pääsynhallinnan, tietoturvan ja laadun valvonnan (QoS). (Understanding the LWAPP 2008.)

Ciscon kontrollerit poikkeavat toisistaan liitäntöjen lisäksi liitettävien lightweight-tukiasemien määrässä. Määrät ovat: 6, 12, 25, 50 ja 4404:n 100 tukiasemaa. Ciscon WLAN kontrollerit on kuvattu kuviossa 5. (WLAN Controllers 2008.)

KUVIO 5. Cisco Wireless LAN Controllers (4402 ja 4404)

5.4 Toteutustavan valinta

Langattoman verkon toteutustavan suunnittelussa on ymmärrettävää, että tällä hetkellä lähiverkossa käytössä olevaan Hewlett Packard (HP) 5300-sarjan kytkimeen liitettävä moduuli oli vahvoilla. Langattoman lähiverkon käyttöönoton HP on pyrkinyt tehdä vaatimustasoltaan vähäiseksi ja toteutustavaksi HP on valinnut moduulin liittämisen kytkimeen.

Jo käytössä olleen 5300xl-sarjan kytkimeen päätettiin lisätä saman tuoteperheen ProCurve WES-moduuli. Kytkimen konfiguraatiota tarvitsee tällöin muokata melko vähän.

6 PROCURVE WIRELESS EDGE SERVICES (WES) XL -MODUULI

6.1 Hallittavuus

Keskitetty hallinta mahdollistaa WLAN-asetusten tekemisen yhdestä paikasta. Asetuksia voidaan muokata niin SSID:n (service set identifier), salauksen ja tunnistautumisen kuin muidenkin palveluiden osalta.

Kun moduuli otetaan käyttöön, kytkin automaattisesti konfiguroi moduulin löytämään ja ottamaan käyttöön ProCurve radioportit. Samoin tapahtuu radioportteja lisättäessä. (WES-esite 2007.)

6.2 Verkon peittoalue

Skaalautuva radioarkkitehtuuri: ProCurve radioporttimallisto antaa mahdollisuuden valita kuhunkin käyttötarkoitukseen sopivia laitteita. Laitteiden toisistaan poikkeavia ominaisuuksia ovat mm. dual-radion käyttö (samanaikainen 802.11a ja 802.11g käyttö), kustannustehokas pelkän yleisemmän 802.11g käyttö, sisäiset ja ulkoiset antennit sekä käyttökohteeseen suunnitellut ratkaisut. (ProCurve Radio Port 230 2008.)

Auto Channel Select (ACS) helpottavat minimoimaan radioiden vierekkäisten taajuuksien häiriöitä valitsemalla automaattisesti radioportin käyttämään vapaata taajuutta. Lähetystehot ovat säädettävissä, mikä on hyödyllistä etenkin, jos radioportit sijoitetaan lähekkäin. Tätä ominaisuutta voidaan hyödyntää etenkin mahdollisten radioporttien vikaantumisen yhteydessä: Viereiset radioportit pyrkivät paikkaamaan vikaantuneen radioportin jättämän aukon radiopeitossa kasvattamalla lähetystehojaan. Lisäksi, 802.11h laajennuksen mukaisesti tutkan ja satelliittien aiheuttamat häiriöt pyritään minimoidaan. (WES-esite 2007.)

6.3 Vikasietoisuus

Varamoduuli voidaan hankkia ensisijaisen moduulin vikaantumisen varalle. Varalla oleva moduuli ottaa tarvittaessa automaattisesti radioportit kontrolliinsa. Toisaalta, lankaverkonkin varalla olo voidaan pitää riittävänä tekijänä vikasietoisuuden kannalta joissakin verkkosuunnitelmissa. (WES-esite 2007.)

Virransyöttö on olennainen tekijä laitteistojen vikasietoisuudessa. WES-moduulin virransyöttö varmennetaan osana koko kytkimen virransyötön varmennusta, koska WES-moduuli ei sisällä omaa virtalähdettä saadessaan tarvitsemansa virran kytkimeltä.

6.4 Tietoturva

WES-moduuli omaa nykyaikaiset tietoturvaominaisuudet, joita ovat

- Access control list (ACL), liikenteen suodatus niin pelkkien IP-osoitteiden kuin porttien perusteella (Extended ACL)
- NAT (Network address translation), verkko-osoitteen muunnos sisä- ja ulkoverkon välillä
- MAC-osoitteiden mukainen suodatus
- Mahdollisuus laajennettuun tunnistautumiseen: selain pyytää tunnistautumaan (Web-portaali)
- RADIUS pohjainen MAC-todennus
- 802.11i, WPA2 tai WPA, verkon luvattoman käytön esto ja liikenteen salaus siirtotiellä
- Tunkeutumisen havainnointi ja estäminen.

Myös seuraavat tietoturvaominaisuudet ovat käytettävissä:

- Secure management access: CLI, GUI tai MIB ovat kaikki käytettävissä salatulla yhteydellä (SSHv2, SSL tai SNMPv3)

- Management VLAN: Radioportteja pääsee hallitsemaan ainoastaan management VLAN käyttäen
- 4 BSSID tai 16 SSID radioa kohden: Jopa 16 eri SSID voidaan käyttää. SSID voivat poiketa toisistaan niin turvallisuuden, todennuksen kuin yhteyssääntöasetuksien osalta
- Rogue AP:n havaitseminen: Radioportit voidaan asettaa havainnoimaan muiden tukiasemien olemassaoloa ja niiden mahdollista väärinkäyttöä. (WES-esite 2007.)

6.5 Quality of Service (QoS) ja integroidut palvelimet

WES-moduuli sisältää tuen QoS-tekniikoille: Wi-Fi WMM, SpectraLink voice priority (SVP) ja Unscheduled Automatic Power Save Delivery (uASPD). WES-moduuli voi toimia myös DHCP-palvelimena sekä Local RADIUS-palvelimena.

Kaikkia näitä WES-moduulin ominaisuuksia ei tulla ottamaan käyttöön. Osa näistä tehtävistä annetaan sen sijaan esimerkiksi palomuurille WES-moduulin sijaan. Joidenkin ominaisuuksien käyttöönotto saattaa tulla myöhemmin aiheelliseksi, kuten Local RADIUS:n käyttö, jota tarvittaneen halutessa käyttää web-portaalia. (WES-esite 2007.)

6.6 Ohjelmistot

6.6.1 Perushallintaohjelmisto ja lisäohjelmistot

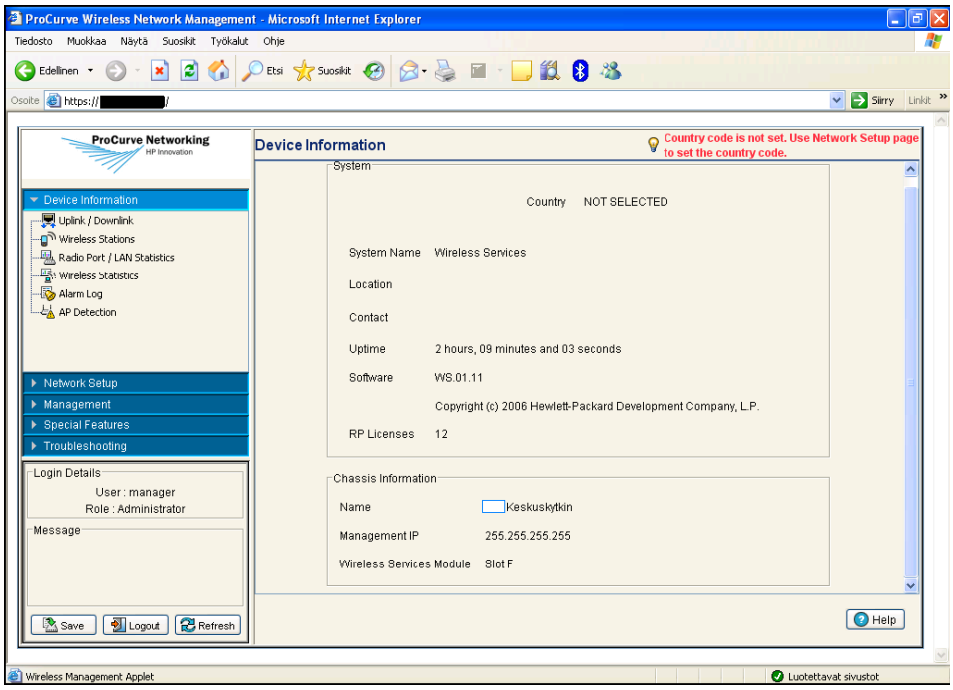
Perushallintaohjelma luo perusedellytykset langattoman verkon keskitettyyn hallintaan. Lisäohjelmiston käyttöönotto mahdollistaa monien hyödyllisten ominaisuuksien hyödyntämisen. ProCurve Manager on muuten samanlainen kuin ProCurve Manager Plus, mutta ominaisuuksia on vähemmän.

ProCurve Manager Plus:aan voidaan hankkia lisäominaisuuksia lisäohjelmistojen avulla. Näitä ohjelmia ovat ProCurve Mobility Manager, ProCurve Identity Driven Manager sekä Network Immunity Manager.

6.6.2 Hallintaohjelmisto

Varsinainen hallintaohjelmisto ProCurve Wireless Network Management (KUVIO 6) sijaitsee WES-moduulissa ja sitä käytetään selaimella. Hallintaohjelmisto hyödyntää java-ohjelmointikieltä. Ohjelmalla voidaan mm. päivittää ohjelmistoa, hallita yksittäisten radioporttien asetuksia sekä luoda VLAN:ja WES-moduuliin.

Hallintaohjelmiston välilehdet jakautuvat kuuteen kategoriaan: hallinta (Management), laitetiedot (Device Information), verkkoasetukset (Network Setup), turvallisuus (Security), erikoistoiminnot (Special Features) ja ongelman ratkaisu (Troubleshooting).



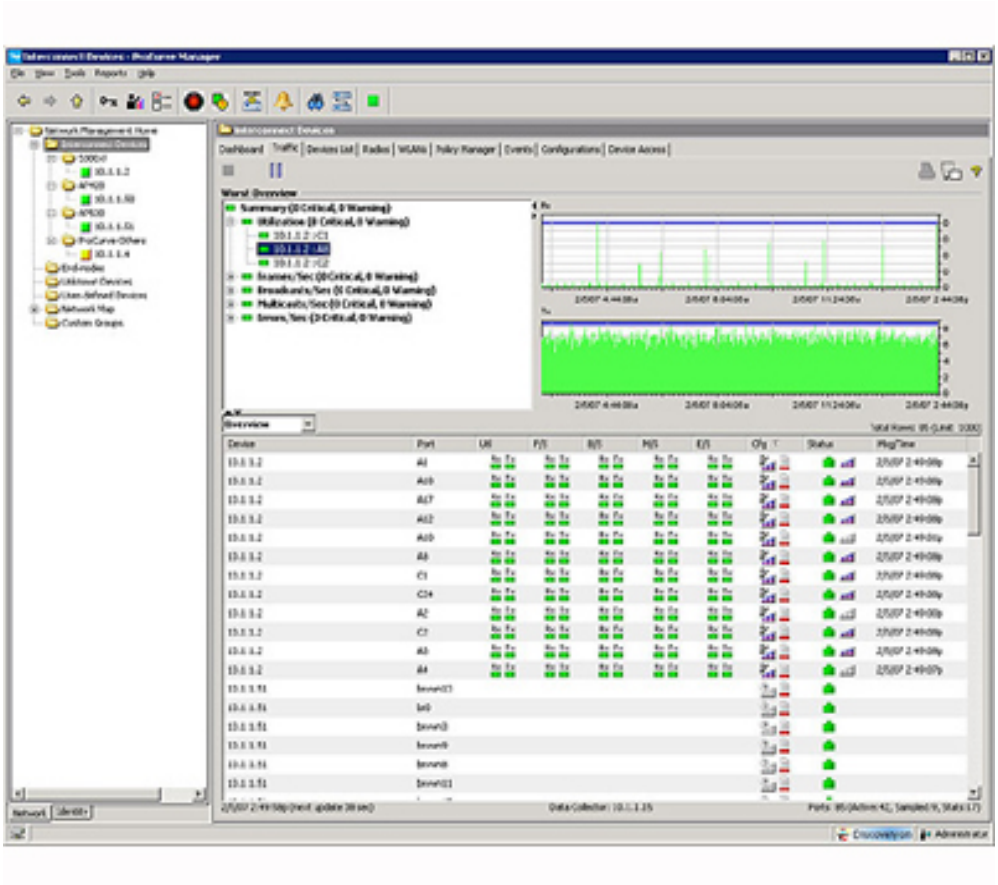
KUVIO 6. Selaimella käytettävä ProCurve Wireless Network Management

6.6.3 ProCurve Manager Plus, PCM+

ProCurve Manager Plus (KUVIO 7) on turvallinen ja kehittynyt Windows-pohjainen verkonhallinnan työkalu. Järjestelmän ylläpitäjä voi ohjelmalla konfiguroida, päivittää, monitoroida sekä ratkoa ongelmia ProCurve laitteista keskitetysti. (PCM+ 2008.)

Ominaisuuksia:

- kehittynyt VLAN:in hallinta. Luodaan koko verkon kattavia VLAN:eja ilman tarvetta ottaa yhteyttä yksittäisiin kytkimiin
- liikenteen analysointi
- Group- ja policy-asetusten hallinta
- helpotusta konfiguraatioiden hallintaan. (PCM+ 2008.)



KUVIO 7. ProCurve Manager Plus

6.6.4 ProCurve Mobility Manager, MM

Mobility Manager (KUVIO 8) on PCM+-ohjelmiston lisäosa ja se luo paremmat edellytykset langattoman verkon keskitettyyn hallintaan. (MM 2008.)

Ominaisuuksia:

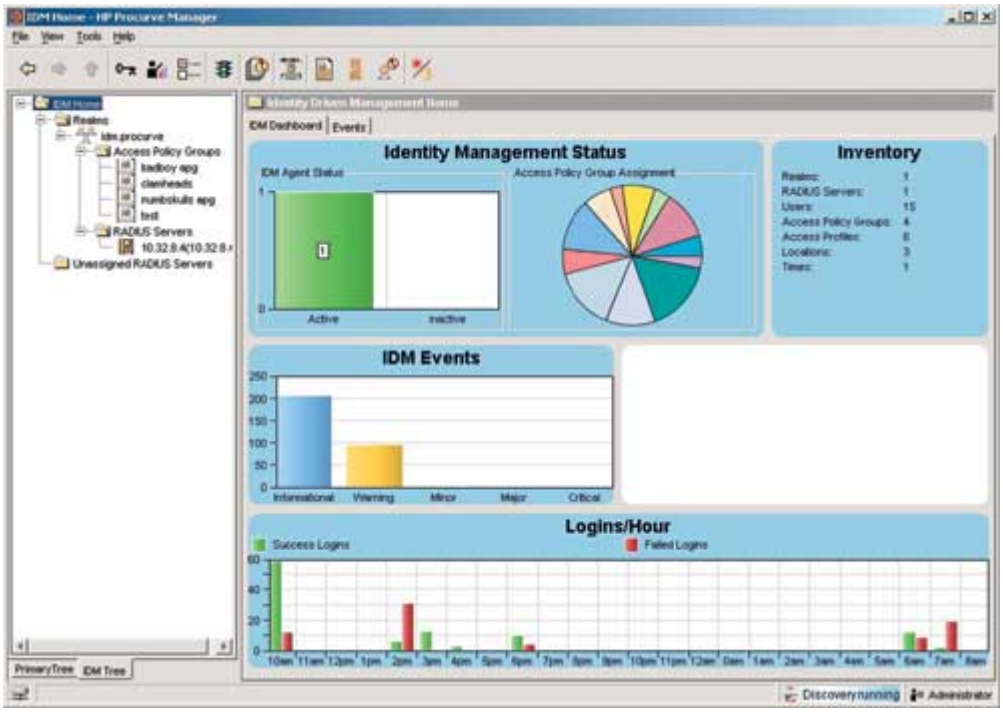
- Yhdistetty tietokanta: Kaikki laitteistotiedot tallennetaan päätietokantaan. Täten langallisen että langattoman verkon elementit voidaan esittää samassa hallintanäkymässä.
- Rogue laitteen havaitseminen: hälyttää, jos havaitaan epäluotettava tukiaseman.
- Turvallisuusasetukset keskitetysti.
- Automaattinen konfiguraation tarkistus: muutokset konfiguraatioihin eivät jää havaitsematta.
- Radioporttien ryhmäperusteinen taajuuslukitus. Tarkoituksena on vähentää radiotaajuushäiriöitä. (MM 2008.)

KUVIO 8. ProCurve Mobility Manager (MM 2008.)

6.6.5 ProCurve Identity Driven Manager, IDM

Identity Driven Manager (KUVIO 9) on PCM+-ohjelmiston lisäosa, ja sen toiminta keskittyy turvallisuuteen, pääsyn hallintaan sekä suorituskykyyn. Sen ominaisuuksiin kuuluvat:

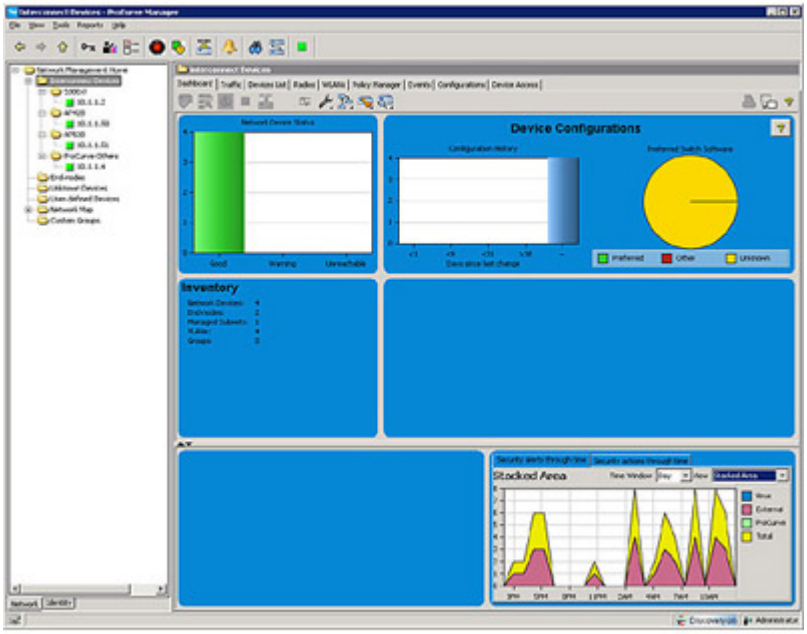
- käyttäjäkohtainen ACL. Verkkoresursseja voidaan muokata käyttäjän ja ajankohdan perusteella
- automaattinen VLAN ohjaus, jossa valintaperusteena toimivat henkilöllisyys, yhteisö ja ajankohta
- liikenteen priorisointi: vaikuttaviksi tekijöiksi voidaan asettaa henkilöllisyys, yhteisö, sijainti sekä ajankohta
- yhteyden nopeuden rajoittaminen perustuen henkilöllisyyteen, yhteisöön ja ajankohtaan. (IDM 2008.)



KUVIO 9. ProCurve Identity Driven Manager (IDM 2008.)

6.6.6 Network Immunity Manager

ProCurve Network Immunity Manager (KUVIO 10) on lisäosa ProCurve Manager Plus:aan, joka havainnoi ja reagoi verkon sisäisiin uhkiin, kuten viruksiin. Ohjelma sisältää monia tietoturvaa parantavia ominaisuuksia. Ohjelma on helppokäyttöinen ja helpottaa järjestelmän ylläpitoa. (NIM 2008.)



KUVIO 10. Network Immunity Manager (NIM 2008.)

6.6.7 Ohjelmistojen valinta

Työn tavoitteena oli luoda langaton lähiverkko kahteen erilliseen rakennukseen. Verkon tuli kattaa aluksi melko pieni alue, joten verkon hallintaohjelmistoista jo ProCurve Wireless Network Management oli ominaisuuksiltaan riittävän

monipuolinen. Tässä vaiheessa ei pidetty tarpeellisena muiden ohjelmistojen hankintaa.

Lisäominaisuuksia tarjoavien ohjelmistojen tarpeellisuus voi kasvaa verkon laajentuessa. Ohjelmistoista ProCurve Manager Plus hankinta on ensimmäisenä hankintalistalla, sillä ProCurve Mobility Manager ja Identity Driven Manager ovat ProCurve Manager Plus:n lisäosia. Ohjelmistojen hankinnan sijaan saatetaan verkon kehittämiseksi ensin harkita muita toiminpiteitä, kuten WES-varamoduulin hankintaa.

7 PROCURVE RADIO PORT -MALLISTO

7.1 ProCurve radioportit

ProCurve radioporttimallisto antaa mahdollisuuden valita kuhunkin käyttötarkoitukseen sopivia laitteita. Nykyinen mallisto käsittää kolme toisistaan melko vähän poikkeavaa päätelaitetta, jotka ovat ProCurve Radio Port 210, 220 ja 230. (ProCurve Radio Port 230 2008.)

Yhteiset ominaisuudet:

- Laitteet on suunniteltu käytettäväksi yhdessä ProCurve WES xl tai zl moduulien kanssa.
- Laitteet saavat virtansa verkkokaapelia pitkin (Power over Ethernet, PoE).
- Radioportit asettuvat automaattisesti kunkin maan radiotaajuusmääräysten mukaisiksi.
- Liikenteen voi salata tekniikoilla 802.11i, WPA2 tai WPA.

Ominaisuudet, joissa 220 eroaa 230:estä:

- Radiot käyttävät ulkoista antennia.
- Ulkonäkö ja fyysinen koko eroavat.
- Ilmoitettu toimintalämpötila on laajempi.
- Kiinnitystapa on erilainen.

Kaikki ominaisuudet, joissa 210 eroaa 230:estä ovat peräisin pelkän 802.11g radion käytöstä. (ProCurve Radio Port 230 2008.)

KUVIO 11. ProCurve Radio Port 210 ja 230 ovat samannäköiset

KUVIO 12. ProCurve Radio Port 220

7.2 Radioporttimallien valinta

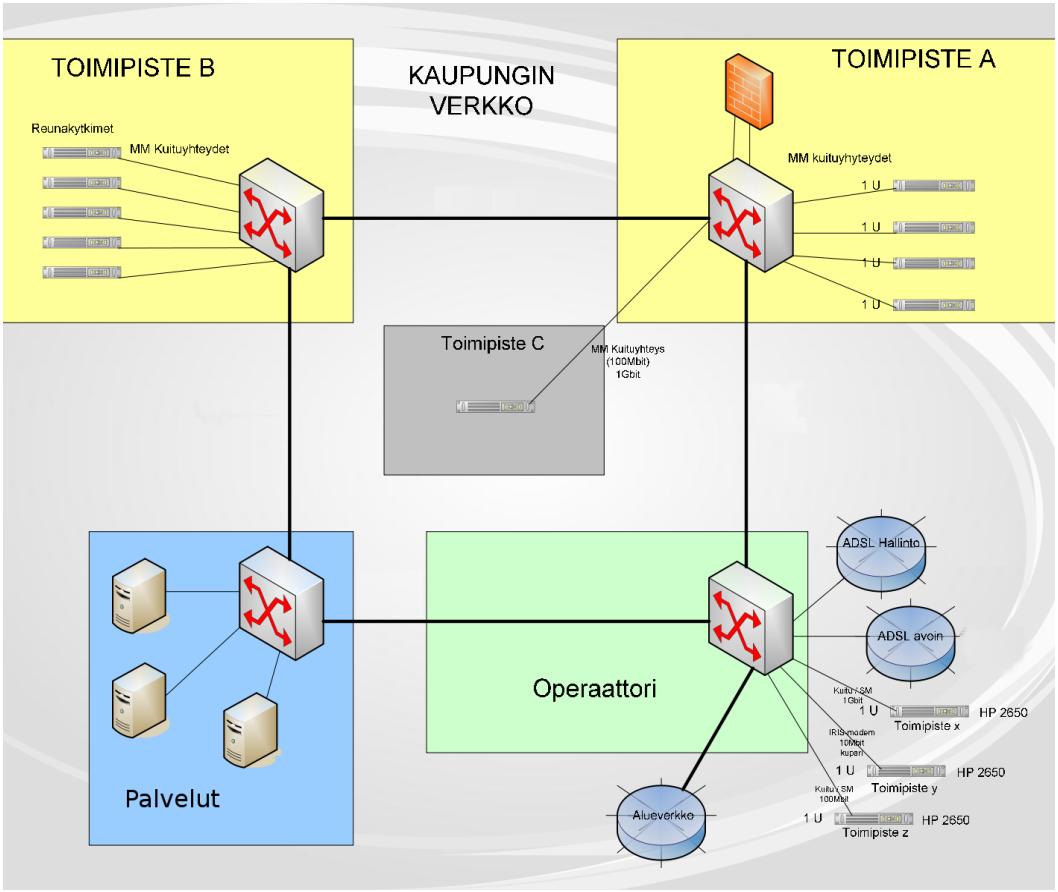
Verkon päätelaitteiksi valittiin ProCurve Radio Port 230. Aluksi verkossa on tarvetta kuudelle päätelaitteelle, jotka tullaan sijoittamaan sisätiloihin. Verkon tulee ensisijaisesti kattaa alueita sisätiloissa, mutta kuuluvuusalue kantautuu myös rakennusten ulkopuolelle.

Lisähankinnoissa muidenkin mallien ominaisuuksia haluttaneen hyödyntää. 802.11a-standardin tukeminen ei välttämättä ole tärkeää, joten tuen tarvetta voitaisiinkin selvittää. Lisäksi viranomaismääräykset saattavat rajoittaa 802.11a käytön sisätiloihin, jolloin ProCurve Radio Port 210 korvaisi täysin Radio Port 230 ulkotilojen osalta. Radio Port 220 käyttö vähentäisi tukiasemien toisilleen aiheuttamaa häiriöitä. Tosin kuuluvuusmittaukset tulisi tehdä tarkemmin, jottei antenneja tule suunnattua virheellisesti.

8 KÄYTÄNNÖN TOTEUTUS

8.1 Kaupungin verkon nykytila

Työn alkaessa kaupungin kahdessa rakennuksessa, joissa langatonta verkkoa oli tarkoitus laajentaa, oli alkuun käytössä jo yksi langaton tukiasema, jonka kuuluvuusalueen ei ollut tarvinnut kattaa suurta aluetta. Tämä tukiasema tullaan korvaamaan yhdellä kuudesta radioporteista. Langalliseen verkkoon ei sen sijaan tämän työn ohessa ollut suunnitteilla muita muutoksia kuin niitä, joita langattoman verkon käyttöönotto vaatii. Verkko koostuu internetyhteyden mahdollistamasta ADSL-modeemista, palomuurista sekä kytkimistä. Kaiken kaikkiaan verkon laajuutta havainnollistaa kuvio 13.



KUVIO 13. Verkkokuva kaupungin lähiverkosta

8.2 Langattoman lähiverkon arkkitehtuuri

Langattoman lähiverkon arkkitehtuureja ovat ad-hoc eli Independent Basic Service Set, Infrastructure Basic Service Set sekä Extended Service Set (ESS). ESS on nimensä mukaisesti laajin arkkitehtuuri sen yhdistäessä tukiasemia toisiinsa.

ESS:ä pidettiin sopivana haluttujen kohteiden peittämiseen langattomalla verkolla. Tukiasemat, tai tässä tapauksessa radioportit, voivat palvella useita asiakas-toimintaperiaatteella toimivia langattomia verkkokortteja.

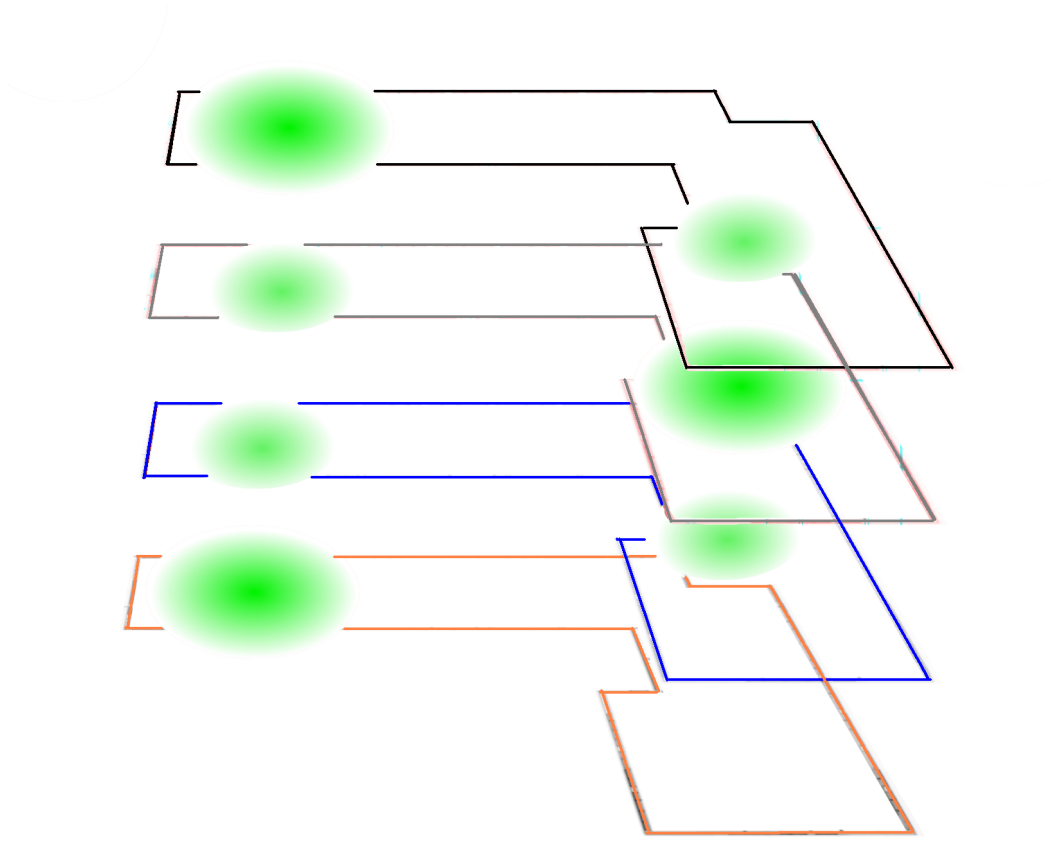
8.3 Langattoman lähiverkon kuuluvuusmittaukset

Kuuluvuusmittaukset oli mahdollista tehdä alustavasti heti alkuvaiheessa, sillä aiemmin käytössä ollut tukiasema oli tähän tarkoitukseen käytettävissä. Laitteen tarvitsi vain palauttaa paikalleen mittausten jälkeen.

Ensimmäisenä mittauksia tehtiin ensimmäisessä rakennuksessa käyttämällä tukiasemaa ja asiakaslaitetta, jossa oli 802.11b-standardin radio. Mittauksista voitiin havaita, että tarkempia kuuluvuusmittauksia kaivattiin kerrosten välisen kuuluvuuden selvittämiseen. Sen sijaan horisontaalisesti toisistaan etäällä olevat paikat päätettiin kattaa kukin omalla radioportilla. Etäisyys oli niinkin suuri, että kun langattoman verkon peittoaluetta halutaan kasvattaa, näiden radioporttien väliin mahtuisi useampi uusi radioportti.

Jälkimmäisellä mittauskerralla mittauksia tehtiin kummassakin rakennuksessa. Tällä kertaa mittaukset tehtiin tukiaseman ja kannettavan tietokoneen avulla. Mittaustuloksien perusteella kummassakin rakennuksessa ennalta katettaviksi määrätyt paikat oli mahdollista kattaa kolmen radioportin verkostolla. Ohessa

(KUVIO 14) on esitetty kuuluvuusalue toisessa rakennuksessa, jossa verkon peittoalue tulee kattamaan tavoitteena olleen alueen.

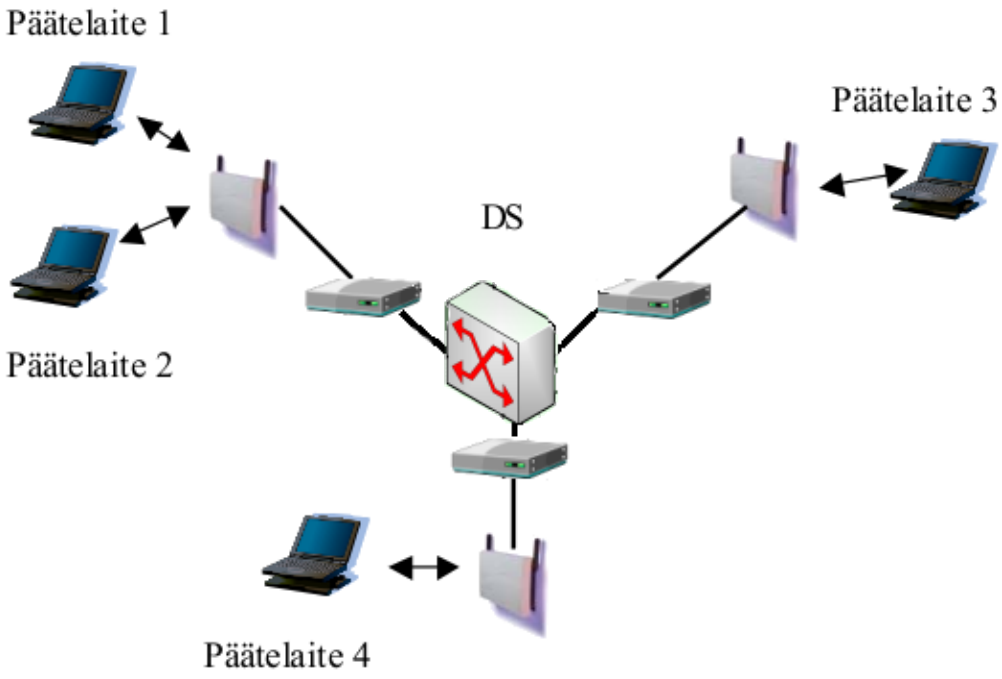


KUVIO 14. Kolmella radioportilla saatu kuuluvuusalue

8.4 Langattoman lähiverkon arkkitehtuurin laitteistot ja ohjelmistot

Radioportteja hallitseva WES-moduuli tulee osaksi 3500-sarjan kytkintä. Kyseiseen keskuskytkimeen muodostuu näin ollen kaksi uutta loogista porttia, jotka ovat moduulin uplink- ja downlink-portit. WES-moduulin ja radioporttien välinen liikenne käyttää 802.1q-standardin mukaista virtuaalista lähiverkkoa (VLAN). VLAN 2100 on tähän tarkoitukseen oletuksena varattu. WES-moduuli ohjaa yhteyden siihen virtuaaliseen verkkoon, joka vastaa käytettyä SSID:tä.

Muut kytkimet ovat ProCurve 2500-sarjalaisia ja radioportit ovat 230-mallisia. Työn yhteydessä kaupungin verkkoon lisättiin radioporttien lisäksi yksi 2500-sarjan kytkin toiseen rakennuksista. Radioporttien malliksi valittiin ProCurve Radio Port 230 -malli, koska 802.11a-standardia haluttiin tukea, eikä suuntaavien antennien käyttöä pidetty tärkeänä. Kuvio 15 havainnollistaa lähiverkon arkkitehtuuria.



KUVIO 15. Verkkokuva langattomasta verkosta

Ohjelmistoista otetaan aluksi käyttöön ainoastaan perushallintaohjelmisto ProCurve Wireless Network Management. Muihin ohjelmistoihin voidaan tutustua paremmin myöhemminkin. Näistä ohjelmistoista ProCurve Manager on ilmainen, muiden ohjelmien ollessa maksullisia. ProCurve Manager Plus:lla voidaan korvata ProCurve Manager. Se sisältää nimensä mukaisesti lisätoimintoja ProCurve Manageriin. Muut ohjelmistot tuovat lisätoimintoja ProCurve Manager Plus:aan.

8.5 Toteutuksen työvaiheet

Langattoman lähiverkon toteutus HP:n 5300-sarjan kytkimellä, WES-moduulilla ja radioporteilla vaatii useita työvaiheita, jotka ovat:

- kytkimien ja radioporttien asennus ja verkkoon kytkeminen
- asetusten teko palvelimeen
- WES-moduulin asennus
- 5300-sarjan kytkimen päivitys ja konfigurointi
- WES-moduulin ohjelmiston päivitys ja konfigurointi
- kytkimien VLAN asetusten teko
- palomuurin asetusten teko (avoimen verkon käyttöönotto).

8.6 Perusteluita asetusvalinnoille

Closed system, verkon piilottaminen: Tukiasemat lähettävät SSID:tä (service set identifier) mainostaakseen itseään ja erottuakseen toisesta tukiasemasta. Kun asiakaslaite havaitsee tukiaseman mainoksen, se saattaa ehdottaa verkkoon liittymistä. Tukiaseman mainostuksen, closed system -asetus, poistaminen ei ole varsinainen tietoturvatekijä. Mutta piilottaminen vähentää tietoutta verkon olemassaolosta, ja vähentää tarpeettomia yhteydenotto yrityksiä. Piilotetun SSID:n saa selville tukiasemalle tai radioportille asiakkaan lähettämästä liikenteestä, joka sisältää SSID:n selkokielisenä.

Salaustavaksi valittiin vain WPA/WPA2-TKIP, koska AES:n ja TKIP:n samanaikaisen käytön toimintavarmuudesta ei oltu täysin vakuuttuneita. WES-moduulin ohjelmiston kehitystyö tulee parantamaan luottamusta toimintavarmuuteen, joten samanaikainen käyttö tullaan ottamaan myöhemmin käyttöön ja koska on ilmaantunut viitteitä mahdollisesta osittaisesta murrosta TKIP:n osalta AES:n käyttöönottoa tulisikin tarkastella uudelleen aiempaa tarkemmin. Tosin edellä mainittu murto ei ensivaikutelmalta vaikuta niin

vakavalta, että TKIP:stä tulisi luopua mahdollisimman nopeasti. Lisäksi autentikointipalvelimen eli tässä tapauksessa RADIUS-palvelimen käyttö saattaa olla tekijä joka vähentää väärinkäytön riskiä entisestään. Mainitsemisen arvoista on kuitenkin se, ettei WPA2-AES:ssä ole havaittu vastaavanlaisia riskitekijöitä.

9. YHTEENVETO

Tämän opinnäytetyön tavoitteena oli langattoman lähiverkon käyttöönotto. Työssä käsiteltiin langattoman lähiverkon kehittymistä aikojen saatossa sekä esiteltiin valitussa toteutustavassa tarvittavat laitteistot.

Tavoitteena ollut langattoman verkon käyttöönotto oli mahdollista toteuttaa keskitetyn hallinnan mahdollistamilla kahdella tavalla, joko Hewlett Packardin WES-radioportti-järjestelmällä tai Cisco:n langattomanverkon kontrollerilla ja lightweight-tukiasemilla. Keskitettyä hallintaa arvostettiin, koska verkkoa laajennettaessa laitteiden käyttöönotto ja hallinta tehostuu. Näiden kahden valmistajan toteutustavoista valittiin Hewlett Packardin WES-radioporttijärjestelmä. Kaupungilla oli jo käytössä HP:n kytkin, johon WES-moduuli oli mahdollista liittää. Näin ollen, HP:n toteutustavan lähtökohdat olivat hyvät.

Laitehankintoihin lukeutuivat radioportit ja niiden hallintalaite, WES-moduuli. Radioportteja otettiin käyttöön kolme kappaletta kumpaankin rakennukseen ja radioporttien malliksi valittiin ProCurve Radio Port 230. Varamoduulia ei hankittu näin alkuun, mutta se on mahdollista hankkia myöhemminkin. Varamoduuli parantaisi vikasietoisuutta ottaessaan tarvittaessa ensisijaisen WES-moduulin tehtävät hoidettavakseen. Ohjelmistoista otettiin käyttöön ainoastaan perushallintaohjelmisto, mutta muihinkin ohjelmistoihin tutustuttiin.

10. MAHDOLLISUUDET TULEVAISUUDESSA

Langattoman lähiverkon käyttöönotto on ollut kasvussa viime vuodet. Langaton verkko on sekä korvannut langallista verkkoa että tullut käyttöön sen rinnalle. Langallinen verkko ei tule häviämään käytöstä, koska sen käytöllä on vielä useita etuja puolellaan, kuten siirtokapasiteetti ja toimintavarmuus. Lisäksi kaupungin verkossakin yhteydet kytkinten välillä sekä kytkimen ja radioporttien välillä on toteutettu langallisesti. Tässä työssä on lankaverkkoa hyödynnetty lisäksi sähkön siirtämiseen päätelaitteeseen.

Kaupungin verkko on jatkuvan kehityksen kohteena. Kaupungin verkon laajentaminen on mahdollista sitä mukaan kun tarvetta laajentamiseen tulee, sillä laitteistohankinnat ja tarvittavat asetukset on tiedossa. WPA2 tai 802.11i käyttöönotto tulee aiheelliseksi viimeistään siinä vaiheessa, kun WPA2 on tuettuna myös päätelaitteissa. Myös WLAN-standardointi on jatkuvan kehityksen kohteena.

LÄHTEET

802.11, 2008. [online]. Wikipedia [viitattu 30.3.2008]. Saatavissa: http://fi.wikipedia.org/wiki/802.11

Alatalo, E. 2005. FreeRADIUS ja 802.1x autentikointi. Lahden ammattikorkeakoulu.

Cisco Systems, Cisco Wireless LAN Controlles. [verkkojulkaisu, viitattu 27.3.2008]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0_ps6366_Products_Data_Sheet.html

Cisco Systems, Understanding the Lightweight Access Point Protocol (LWAPP) [verkkojulkaisu, viitattu 27.3.2008]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6306/prod_white_paper0900aecd802c18ee_ns337_Networking_Solutions_White_Paper.html.

Griffith, E. 2004. A Warm Welcome to WPA2 [verkkojulkaisu].[viitattu 20.3.2008]. Saatavissa: http://www.wi-fiplanet.com/news/article.php/3402971.

Halasz, D. 2004. IEEE 802.11i and wireless security [verkkojulkaisu]. [viitattu 30.3.2008]. Saatavissa: http://www.embedded.com/columns/specialreports/34400002?_requestid=320830.

Hewlett-Packard, ProCurve Identity Driven Manager (IDM), [verkkojulkaisu, viitattu 28.3.2008]. Saatavissa: http://www.hp.com/rnd/products/management/idm/features.htm

Hewlett-Packard, ProCurve Manager Plus (PCM+) [verkkojulkaisu, viitattu 28.3.2008]. Saatavissa: http://h10010.www1.hp.com/wwpc/fi/fi/sm/WF05a/23663-345897-345897-345897-1790351-1790353.html?jumpid=reg_R1002_FIFI

Hewlett-Packard, ProCurve Mobility Manager [verkkojulkaisu, viitattu 28.3.2008]. Saatavissa: http://h10010.www1.hp.com/wwpc/fi/fi/sm/WF05a/23663-345897-345897-345897-1790351-12291574.html?jumpid=reg_R1002_FIFI

Hewlett-Packard, ProCurve Network Immunity Manager [verkkojulkaisu, viitattu 10.12.2008]. Saatavissa: http://www.hp.com/rnd/products/management/ProCurve_Network_Immunity_Manager_1.0/overview.htm

Hewlett-Packard, ProCurve Radio Port 230 [verkkojulkaisu, viitattu 28.3.2008]. Saatavissa: www.hp.com/rnd/products/wireless/ProCurve_Radio_Port_230/overview.htm

Hewlett-Packard, ProCurve Wireless EDGE Services xl module (WES-esite) [verkkojulkaisu, viitattu 28.3.2008]. Saatavissa:http://www.hp.com/rnd/pdfs/datasheets/ProCurve_Wireless_Edge_Services_xl_Module.pdf

Hämäläinen, M. 2007. WLAN ja logistiikka-ala [Verkkojulkaisu]. Helsingin ammattikorkeakoulu. Saatavissa: https://oa.doria.fi/bitstream/handle/10024/28169/stadia-1191323663-0.pdf?sequence=1

Hämäläinen, P. 2003. Ilmojen halki käy verkkojen tie. Tietokone-lehti 5/2003, 55.

Kindervag, J. 2006. The Five Myths of Wireless Security. Information Systems Security 15/2006 4, s7-16. Saatavissa:

http://search.ebscohost.com/login.aspxdirect=true&db=afh&AN=22287936&site=ehost-live.

Kotilainen, S. 2003. Turvaa WLAN-verkkosi. Tietokone-lehti 4B/2003, 14-19.

PEAP. 2008. [online]. Wikipedia [viitattu 30.3.2008]. Saatavissa: http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

Phifer, L. 2003. Using RADIUS For WLAN Authentication. [Verkkojulkaisu, viitattu 25.3.2008] Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/3114511.

Pitkänen, P. 2008. Wlan-salaus-murrettiin [Verkkojulkaisu, viitattu 12.11.2008]. Saatavissa: http://www.itviikko.fi/tietoturva/2008/11/06/wlan-salaus-murrettiin/200828918/7

Viestintäviraston radiotaajuusmääräys 15, 2006. Saatavissa: www.finlex.fi/data/normit/27701-Viestintavirasto15W2006M.pdf

VLAN, 2008. [online]. Wikipedia [viitattu 3.5.2008]. Saatavissa: http://fi.wikipedia.org/wiki/VLAN

Walker, J. 2003. 802.11 Security Series, Part II: The Temporal Key Integrity Protocol (TKIP) [Verkkodokumentti, viitattu 25.3.2008]. Saatavissa: http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf.

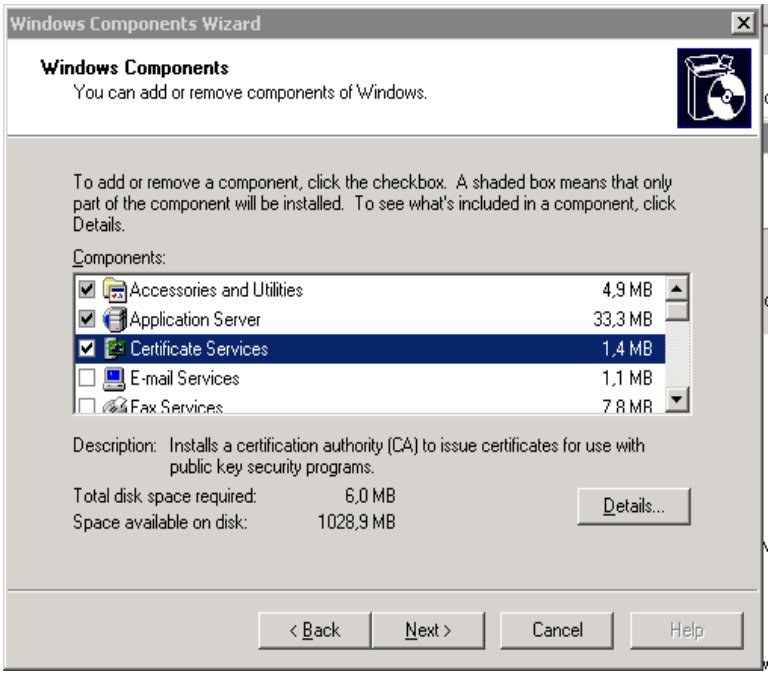
WLAN, 2008. [online]. Wikipedia [viitattu 3.5.2008]. Saatavissa: http://fi.wikipedia.org/wiki/WLAN

Zoller, T. 2008. WPA-cracked-not-really [Verkkojulkaisu, viitattu 12.11.2008]. Saatavissa: http://blog.zoller.lu/2008/11/wpa-cracked-not-really.html

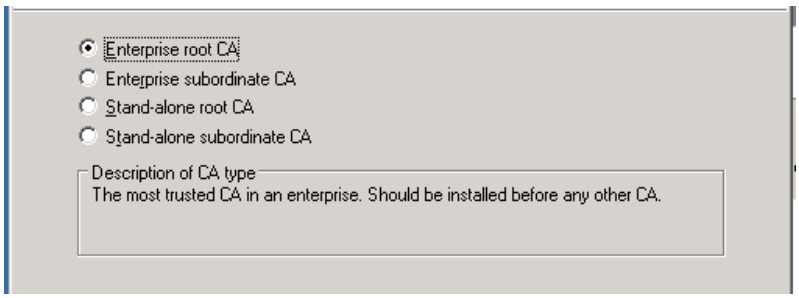
LIITE 1

OHJEISTUS LANGATTOMAN VERKON KÄYTTÖÖNOTTOON

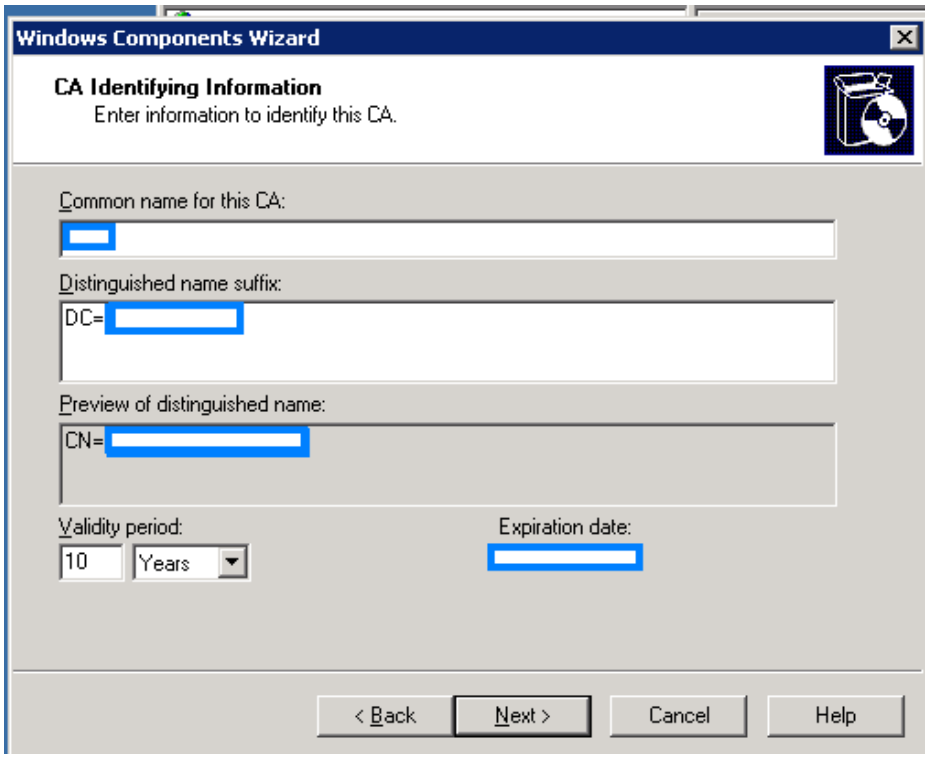
Asennettaan Certificate Services -> listasta valitaan Enterprise root CA -> annetaan CA:lle nimi ja sertifikaatin voimassaoloajaksi 10 vuotta -> Asetetaan sertifikaatin tietokannan ja lokin sijainti.



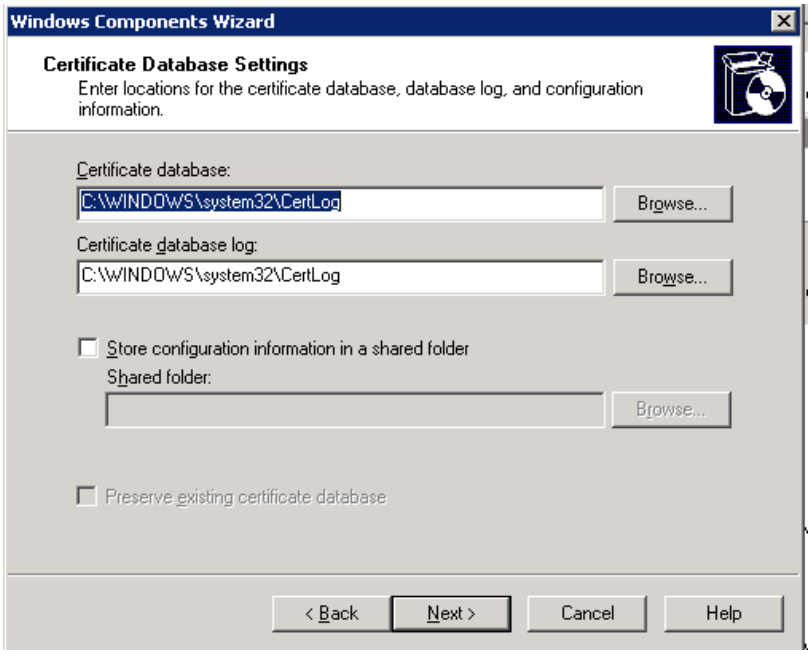
KUVIO 16. Valitaan asennettavaksi Certificate Services



KUVIO 17. CA:n tyypiksi valitaan Enterprise

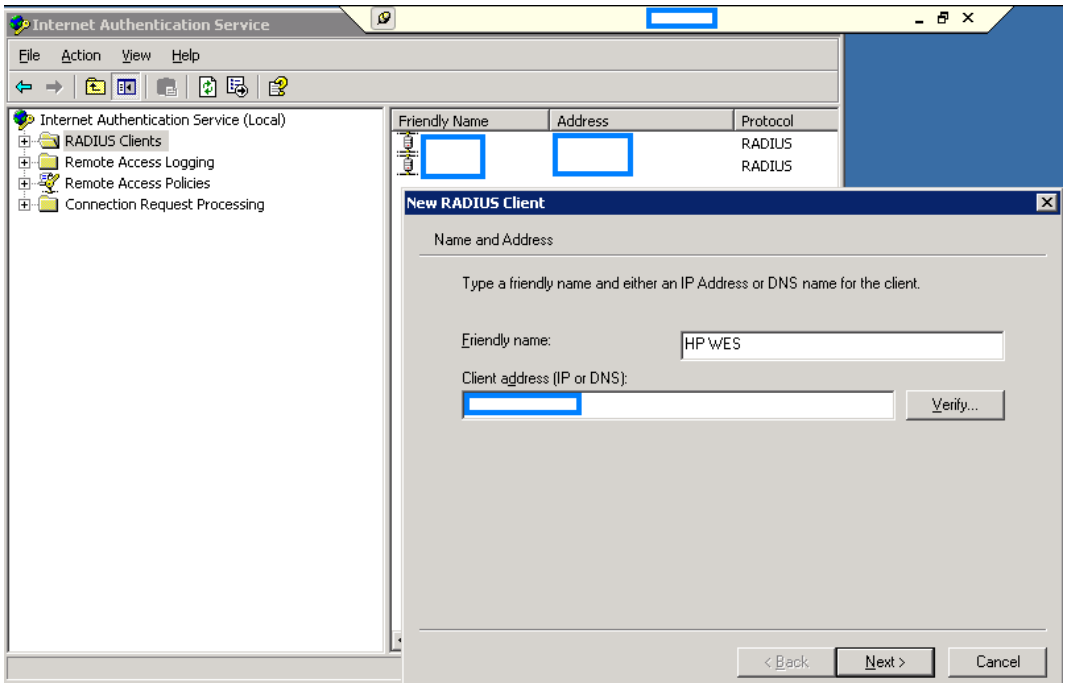


KUVIO 18. CA:n tietojen asettaminen

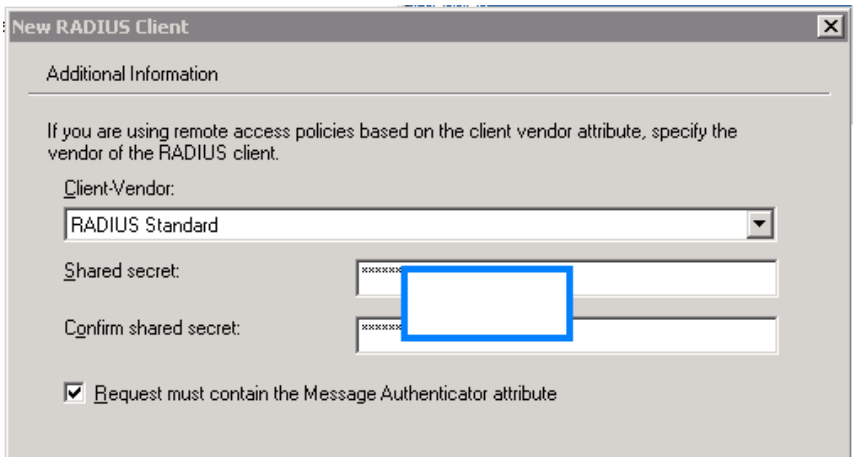


KUVIO 19. Asetetaan sertifikaatin tietokannan ja lokin sijainti

WES-moduulin lisääminen RADIUS-asiakkaaksi: IAS löytyy palvelimelta Järjestelmävalvojan tehtävistä. Käynnistetään ohjelma -> RADIUS clients -> New RADIUS client -> annetaan WES-moduulin nimi ja osoite -> Clien-vendor -valintana RADIUS standard, annetaan avain ja laitetaan ”Request must contain the Message Authenticator attribute” valinta päälle. Avain tullaan määrittämään samaksi WES-moduulin asetukseen.



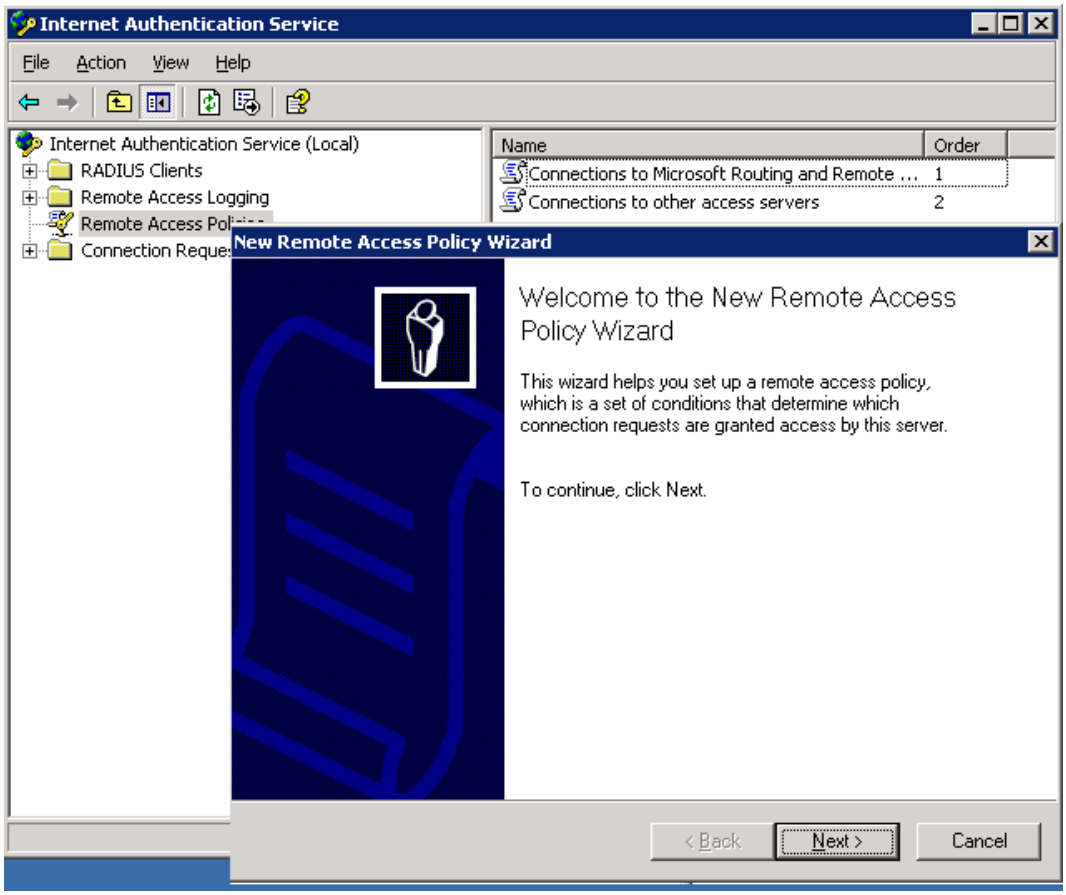
KUVIO 20. RADIUS-asiakkaan määrittäminen



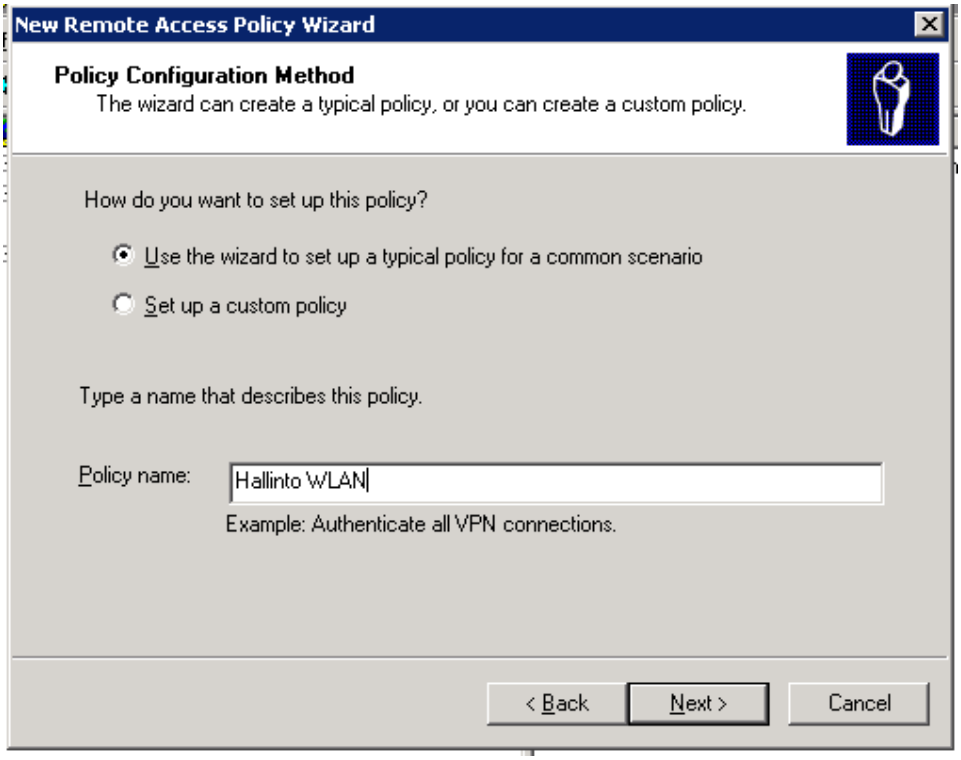
KUVIO 21. Asiakas tyyppi ja avain

KUVIO 22. RADIUS-avain voidaan kirjoittaa esimerkiksi tekstitiedostoon ja kopioida sieltä RADIUS-palvelimelle ja RADIUS-asiakkaslaitteeseen

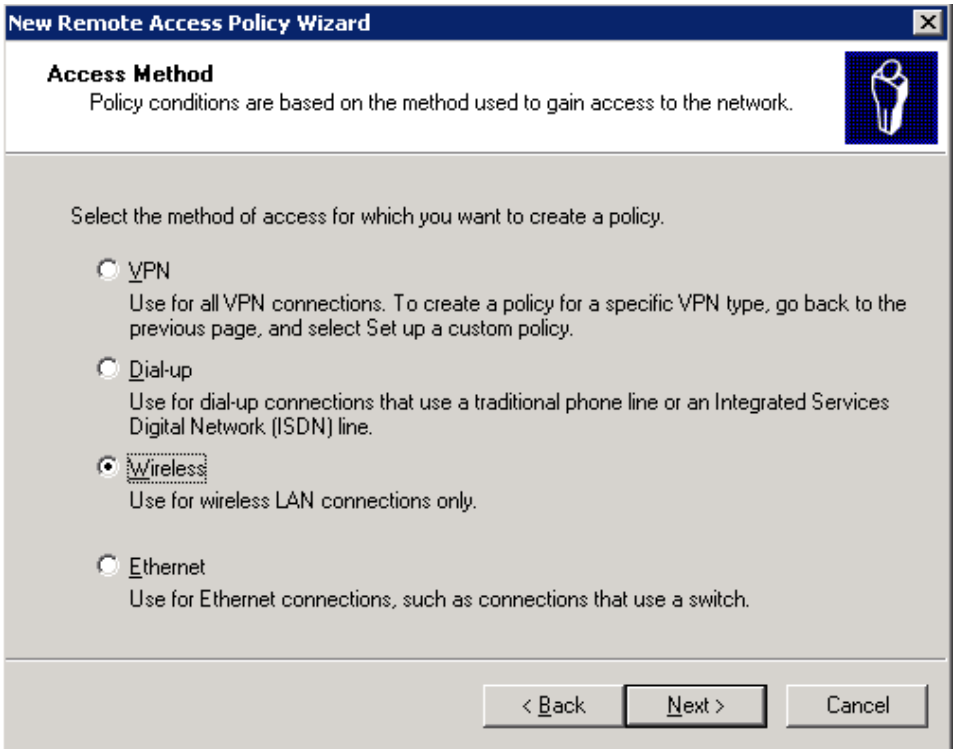
Uuden Remote Access Policyn luonti: Asennusvelhoa käytetään tyypillisen yhteyssäännön tekemiseen ja nimeksi valitaan Hallinto WLAN -> valitaan Wireless -> valitaan Group ja valitaan add -> valitaan ryhmä Hallinto WLAN (edellyttäen, että se on luotu) -> paluu edelliseen valikkoon. Nyt taulukossa on *kansio*\Hallinto WLAN -> EAP tyypin valinta: valitaan PEAP, ja tarkistetaan sen asetukset -> valmis.



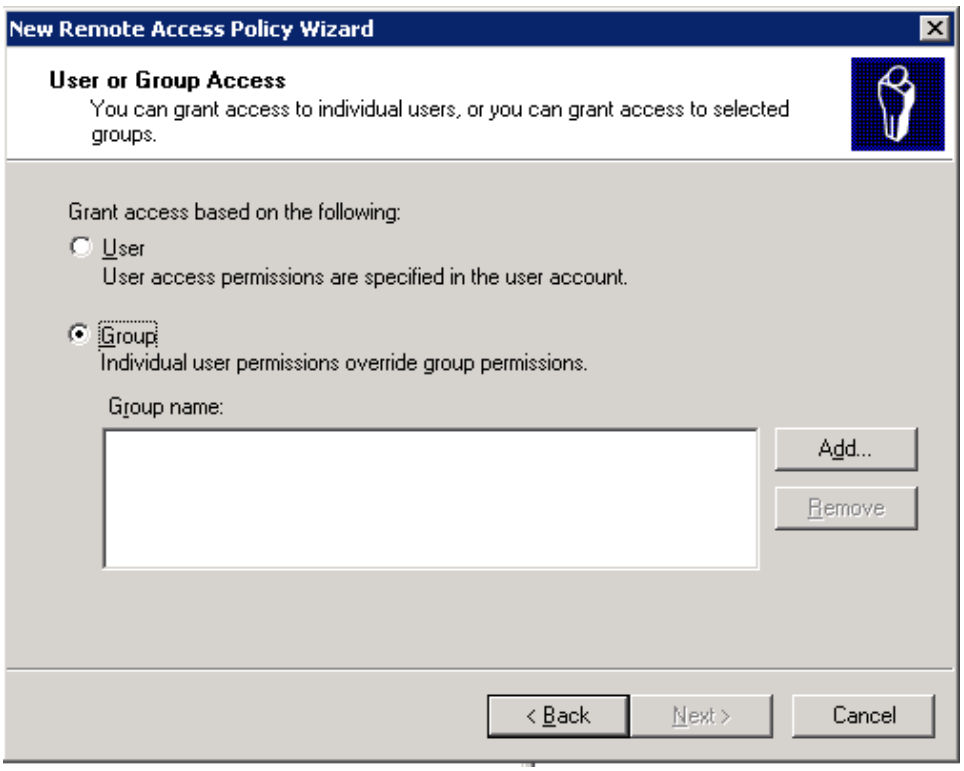
KUVIO 23. Uuden Remote Access Policyn luonti asennusvelholla



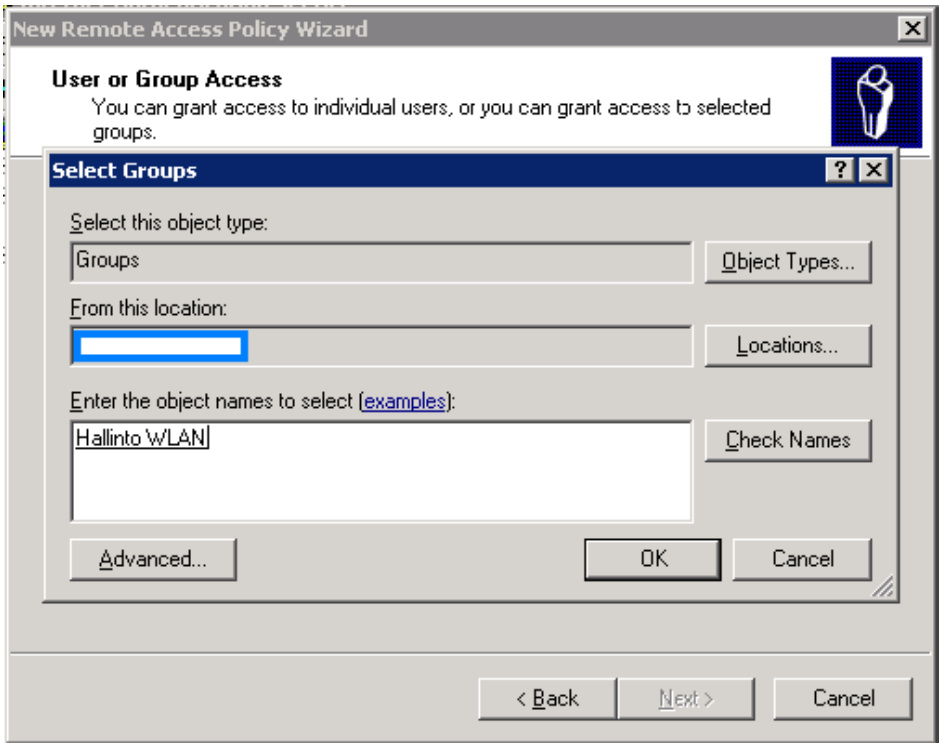
KUVIO 24. Yhteyssäännön asettaminen



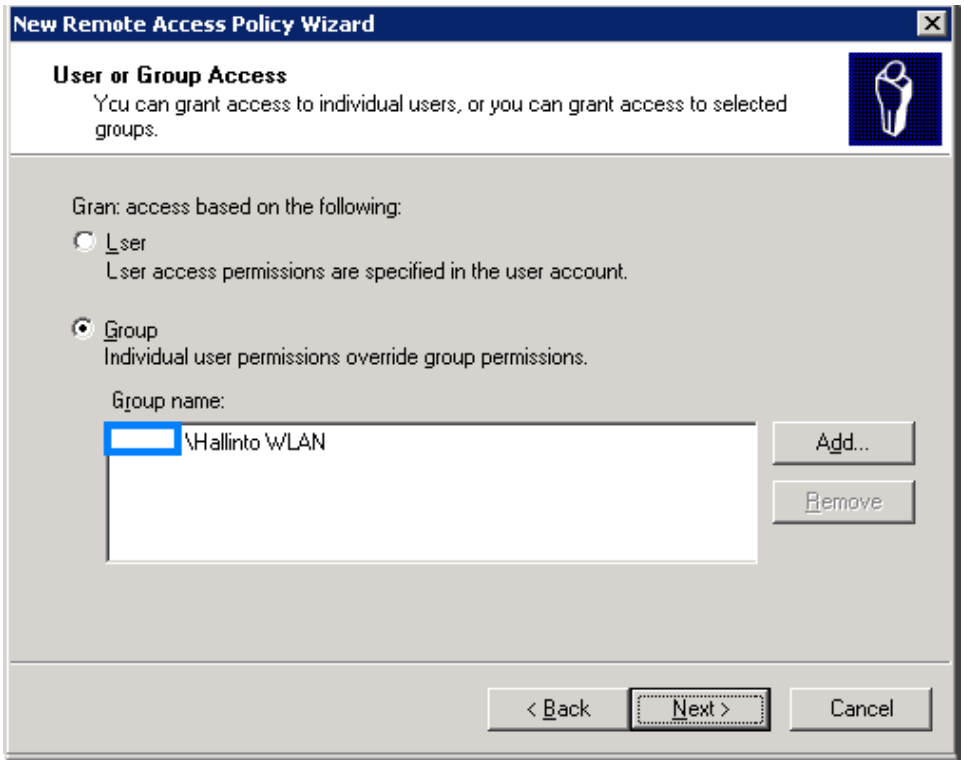
KUVIO 25. Yhteystavan valinta



KUVIO 26. Käyttäjän tai ryhmän pääsyoikeuden määrittäminen

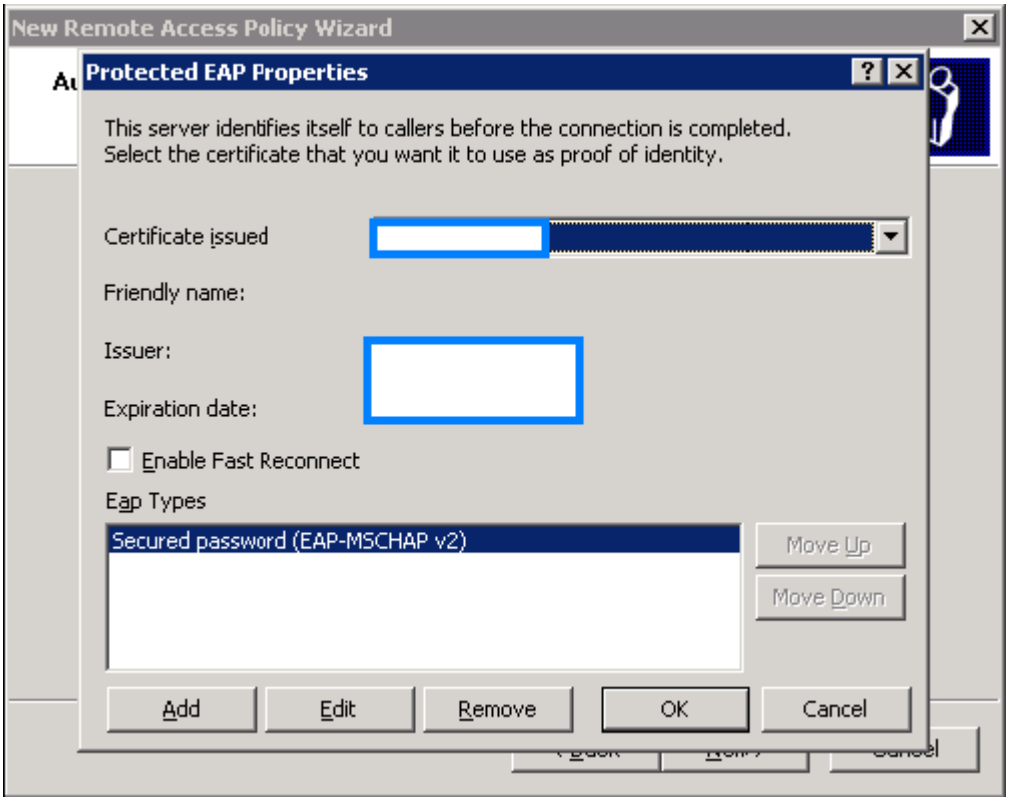


KUVIO 27. Ryhmän haku

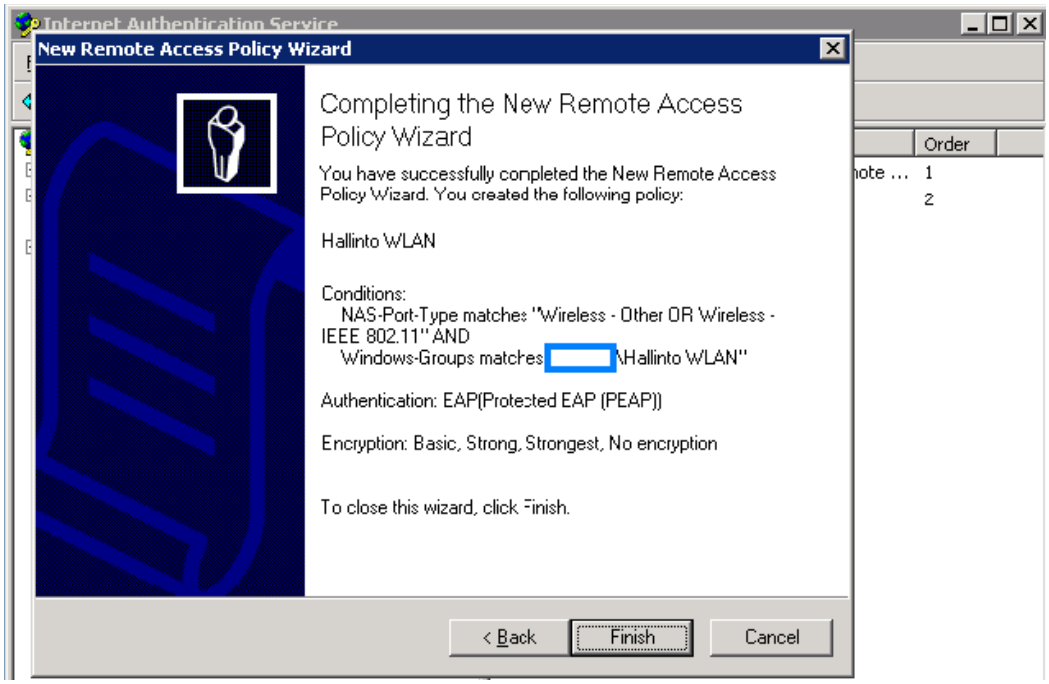


KUVIO 28. Ryhmä valittuna

KUVIO 29. Tunnistusmenetelmän valinta

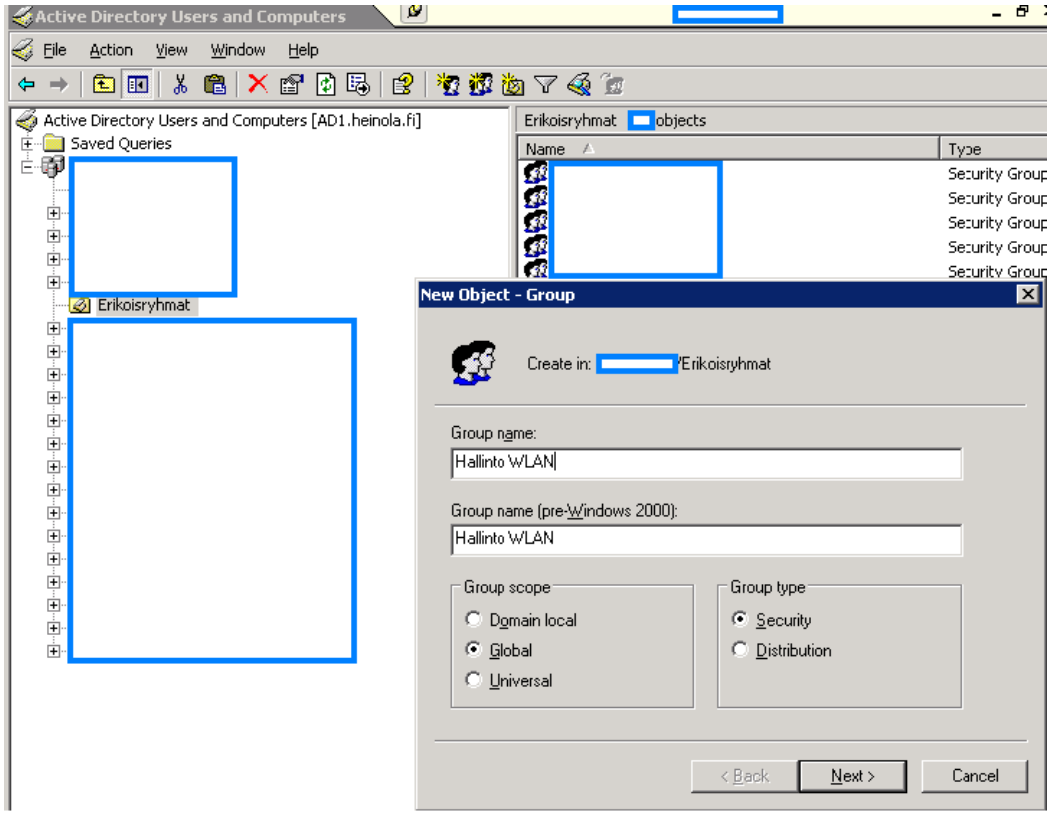


KUVIO 30. PEAP:n ominaisuudet



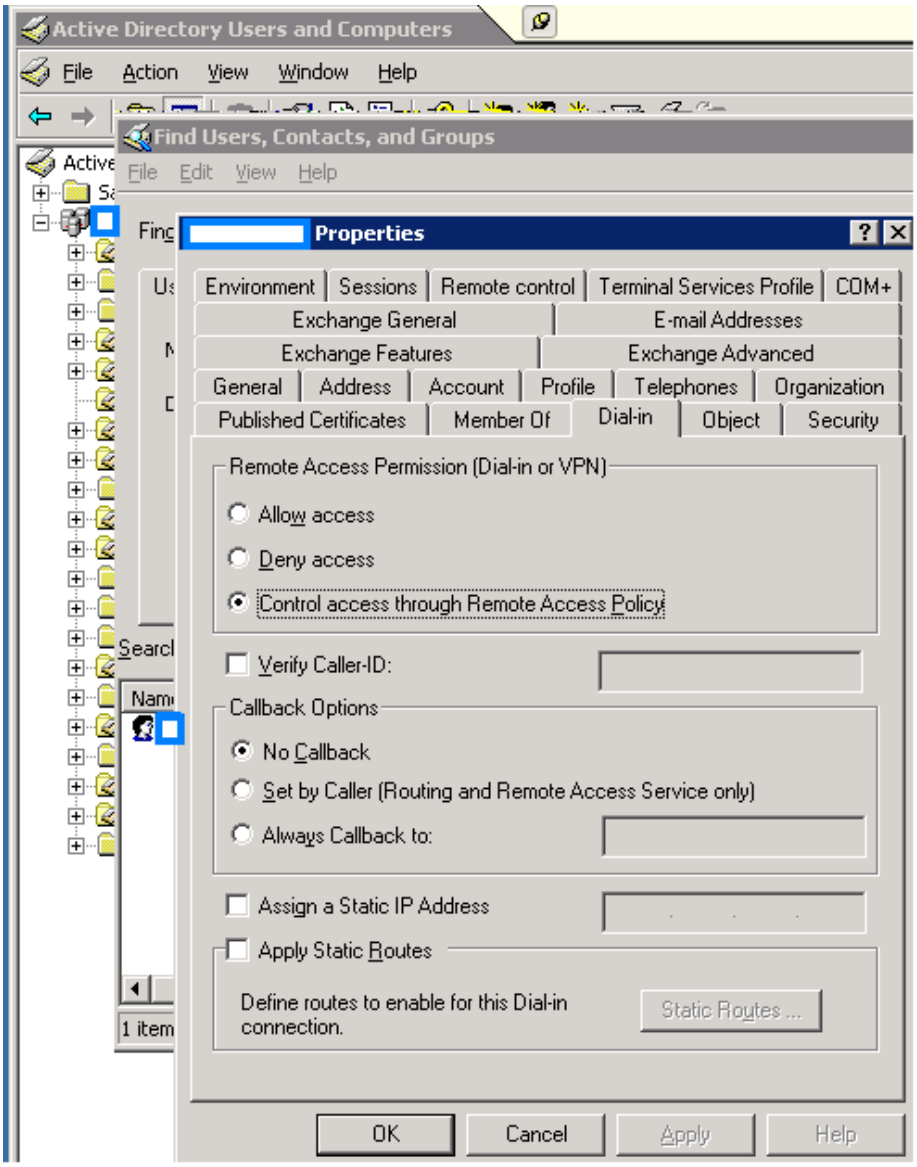
KUVIO 31. Kooste tehdyistä asetuksista

Jotta ”Group: Hallinto WLAN” voidaan valita, Hallinto WLAN on luotava AD:n Käyttäjät ja Tietokoneet -tietokantaan. Erikoisryhmät-välilehden alle (asetukset: Hallinto WLAN, Global ja Security).



KUVIO 32. Ryhmän luominen AD-tietokantaan

Lopuksi on hyvä tarkistaa, että AD:n käyttäjätiedoissa on valittuna ”Control access through Remote Access Policy” eli käyttäjien resurssit määräytyvät AD-tietokannan mukaisesti, kuten on tarkoitus.



KUVIO 33. Pääsynhallinnan määräytyminen

ProCurve WES xl -moduulin asennus ja kytkimen konfigurointi

5300-sarjan kytkimen ohjelmisto tuli päivittää, koska pari vuotta vanha ohjelmistoversio ei ollut yhteensopiva WES-moduulin kanssa. Päivitys tehtiin konehuoneessa, jotta virheet tiedonsiirrossa voidaan minimoida sekä siksi, että moduuli tuli muutenkin asentaa kyseisessä tilassa. WES-moduulin asennus ilman

kytkimen sammuttamista eli hotswap ei tällä kertaa ollut mahdollista, mutta kytkimen uuden ohjelmiston myötä se lienee mahdollista.

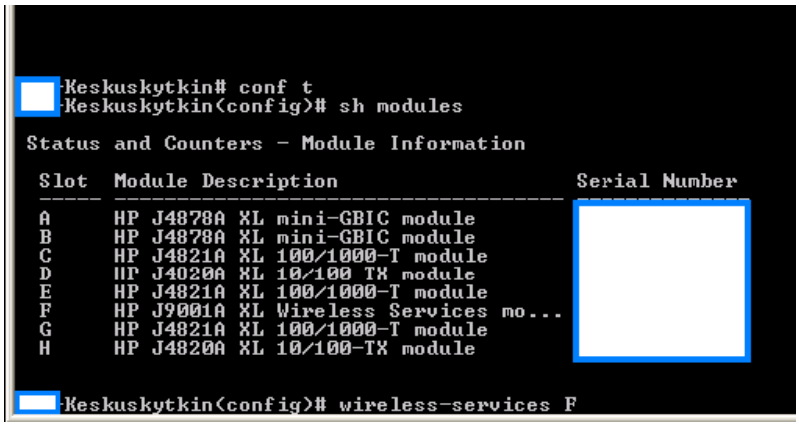
Keskuskytkimen ohjelmiston päivittäminen

Otetaan verkkoyhteys kytkimeen, jonka jälkeen annetaan komennot ”copy tftp flash *ip-osoite versio* secondary” ja ”boot system flash secondary”. (Tftp-palvelimelta ladataan siis toissijaiseen flash-muistipaikkaan ohjelmisto.) Tämän jälkeen otetaan virrat pois, asennetaan moduuli ja käynnistetään uudelleen. Käynnistyessä nähdään mikä versio käynnistyy ja sen kelpoisuus testataan. Tarvittaessa ohjelmisto voidaan kopioida myös primary-paikkaan, jolloin vanha versio ei varmasti käynnisty.

Keskuskytkimen konfiguraation muokkaaminen

Keskuskytkimen konfigurointia varten avattiin telnet-yhteys kytkimeen. WES-moduuli oli asetettu aiemmin paikkaan, joka näkyy moduulitiedoissa ”slot F”:nä. Näin ollen ”wireless-services” komentoon lisätään ”F”.

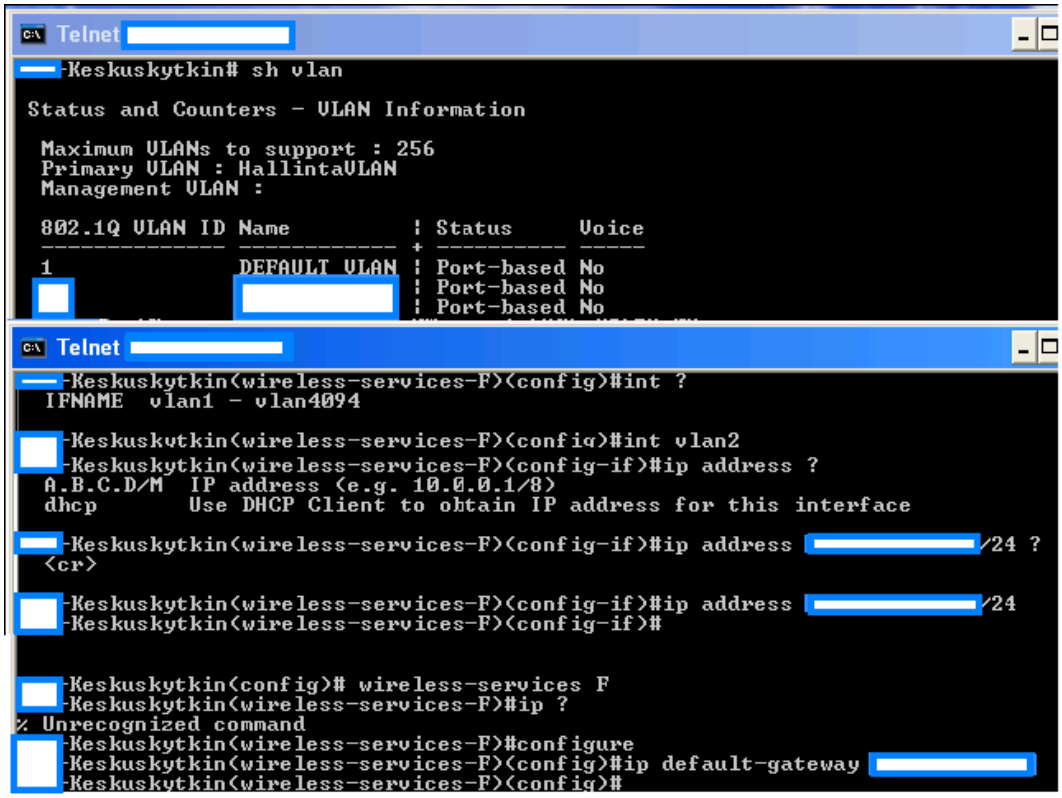
```
Keskuskytkin# conf t
Keskuskytkin(config)# wireless-services F
```



KUVIO 34. Tietoja moduuleista

Wireless-services alla asetetaan oletusreitittimen osoite sekä luodaan VLAN2 ja annetaan sille ip-osoite maskilla. VLAN2:lle tullaan myöhemmin antamaan sen tehtävää kuvaava nimi ”Hallinta VLAN”.

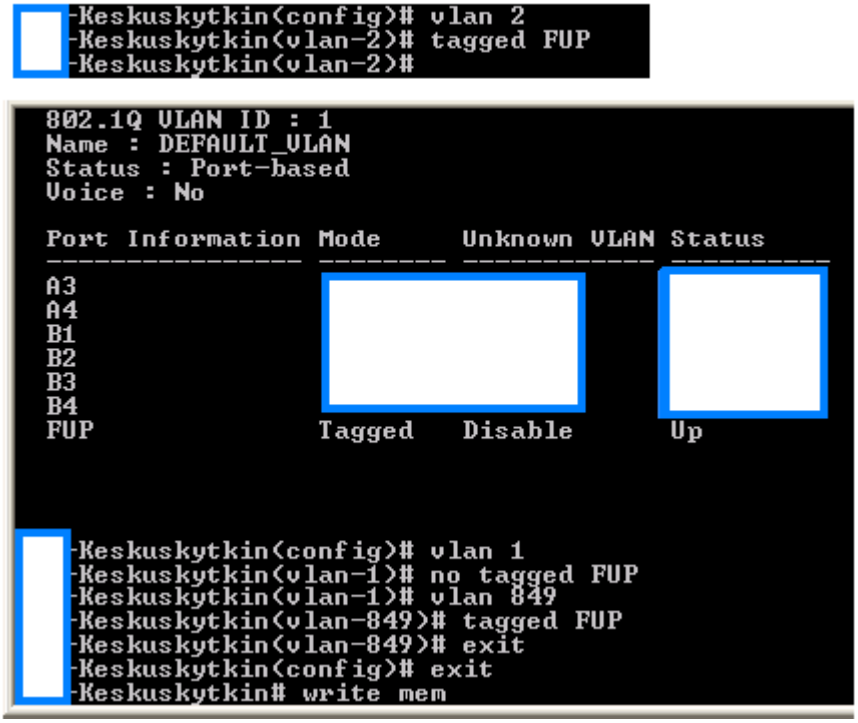
Keskuskytkin(wireless-services F)(config)# ip default-gateway xxx.xxx.xxx.xxx
Keskuskytkin(wireless-services F)(config)# int vlan2
Keskuskytkin(wireless-services F)(config-if)# ip address xxx.xxx.xxx.xxx/24



KUVIO 35. Liitännän ja oletusreitin IP-osoitteiden määrittäminen

Kytkimen VLAN-asetukset: asetetaan vlan 2 ja vlan 849 osalta WES-moduulin looginen portti FUP tagged tilaan ja poistetaan samainen asetus ”Default-Vlan” VLAN 1 osalta.

Keskuskytkin(config)# vlan 2
Keskuskytkin(vlan-2)# tagged FUP
Keskuskytkin(config)# vlan 1
Keskuskytkin(vlan-1)# no tagged FUP
Keskuskytkin(config)# vlan 849
Keskuskytkin(vlan-849)# tagged FUP



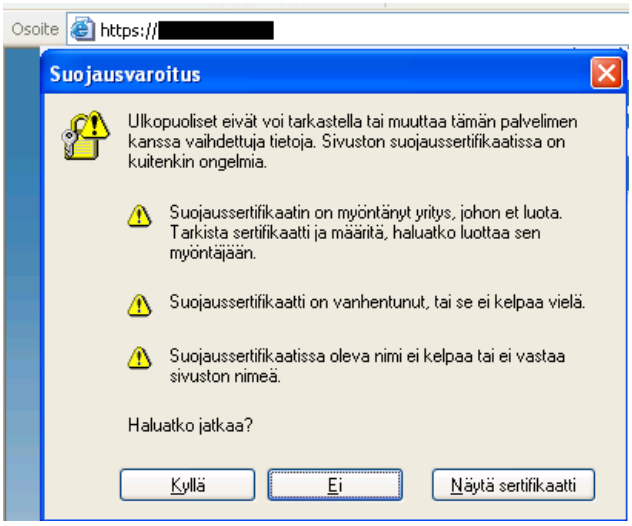
KUVIO 36. VLAN asetukset

Lopuksi tulee muistaa tallentaa asetukset muistiin, jotta ne ovat tallella kytkimen käynnistyessä uudelleen.

Keskuskytkin# write memory

WES-moduulin asetukset

Koska WES-moduulin hallinta on toteutettu web-käyttöliittymällä, asetukset tehdään ottamalla siihen yhteys web-selaimella. Käyttöliittymä käyttää java-ohjelmointikieltä.



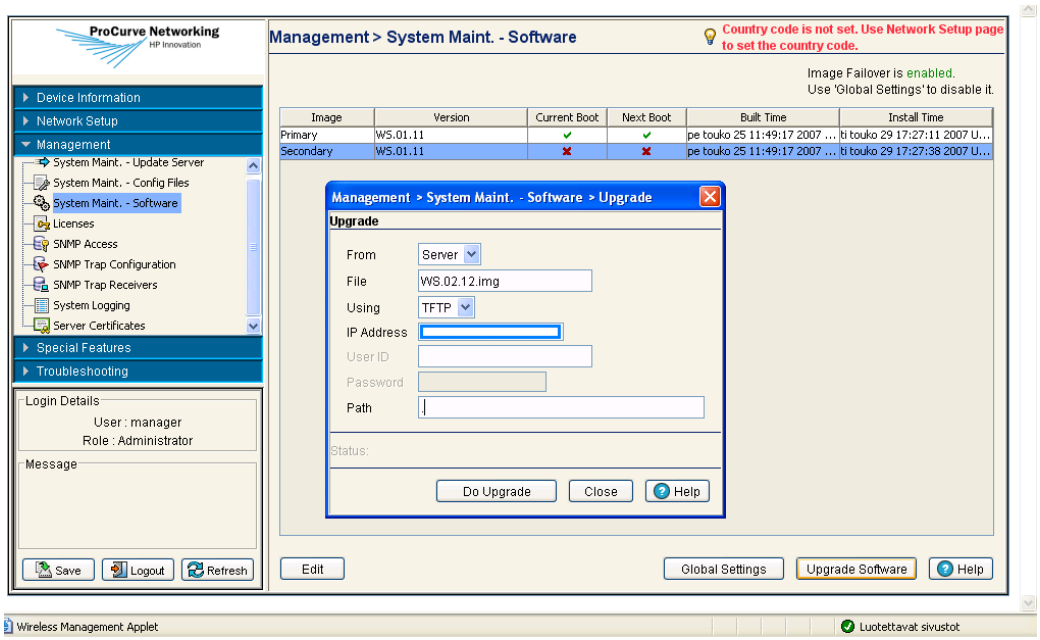
KUVIO 37. WES-moduuliin otetaan suojattu yhteys

Oletus käyttäjänimellä (Manager) ja salasanalla täytyy kirjautua kunnes SuperUser luodaan. Manager-käyttäjätili tullaan poistamaan, ettei oletus käyttäjänimi ja salasana jää käytettäväksi. Ensin kuitenkin päivitetään WES-moduulin ohjelmisto.

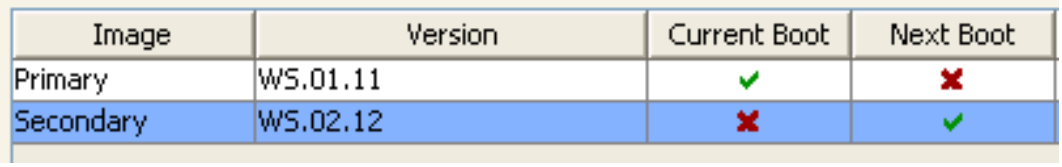
KUVIO 38. Kirjautumisikkuna

WES-moduulin ohjelmiston päivittäminen

Uudemman ohjelmiston voidaan laittaa hakemaan esimerkiksi TFTP:llä palvelimelta. Päivityksen teko löytyy: Management -> System Maint. -Software -> Upgrade. Laite asetetaan ottamaan uusi ohjelmisto käyttöön seuraavan käynnistyksen yhteydessä, ja laite käynnistetäänkin uudelleen.



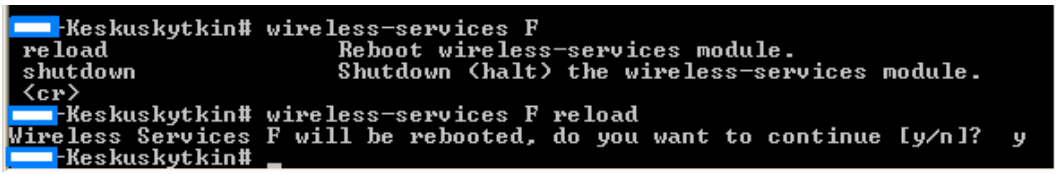
KUVIO 39. Ohjelmiston päivittäminen



KUVIO 40. Seuraavalla käynnistyskerralla otetaan toinen ohjelmistoversio käyttöön

Uudelleenkäynnistys onnistuu parhaiten antamalla kytkimelle käskyn käynnistää WES-moduuli uudelleen komennolla ”wireless-services F reload”, jossa ”F” viittaa moduulipaikkaan. Jos yhteydenotto WES-moduulin web-käyttöliittymään

ei enää onnistu, saattaa olla tarpeen tyhjentää javan välimuisti.



KUVIO 41. WES-moduulin uudelleenkäynnistys

Asetusten muokkaaminen

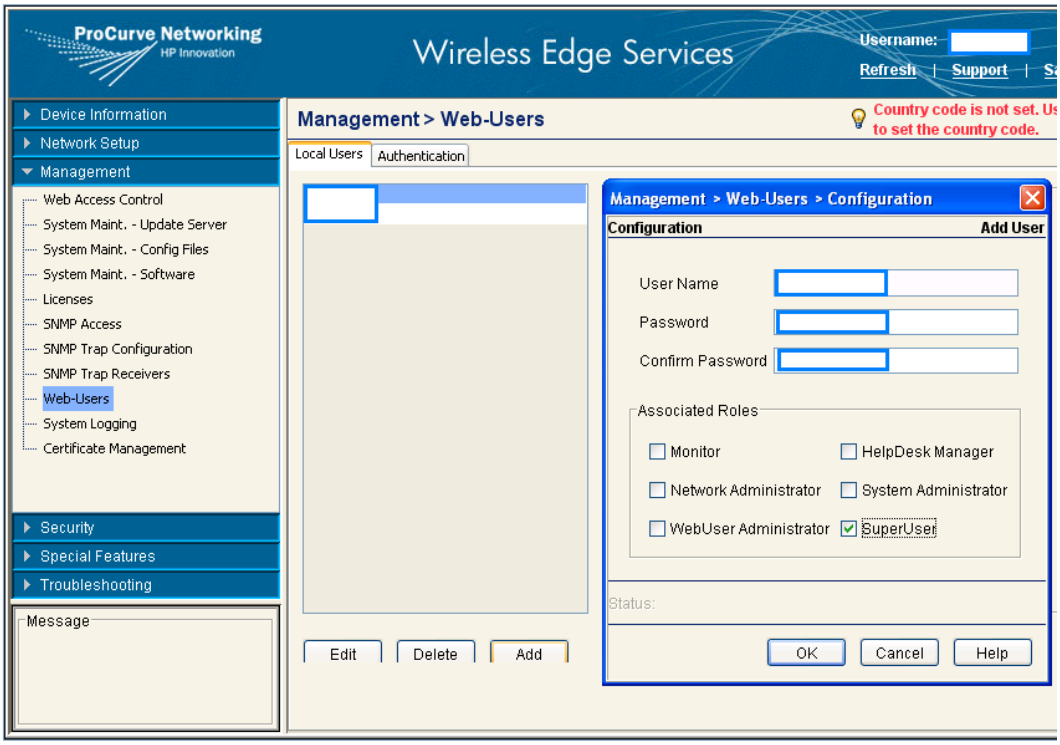
Management-välilehden lisäksi on valittavissa viisi muuta: Device Information, Network Setup, Security, Special Features ja Troubleshooting. Näiden alta löytyy lisäksi monia alasivuja.
Web-users-alasivulta luodaan uusi SuperUser ja poistetaan oletuksena oleva Manager käyttäjä.

Network Setup-välilehdeltä tehdään seuraavat muutokset:

- Annetaan järjestelmästä tietoja
- VLAN 2:lle annetaan kuvaus: ”HallintaVLAN”, ip-osoite ja maski sekä asetetaan Management liitännäksi. Lisäksi lisätään VLAN 849 kuvauksella ”Hallinto” ilman ip-osoitetta ja valintaa ”set as Management Interface”
- Muokataan Hallinto VLAN asetuksia: salaukseksi WPA/WPA2-TKIP ja tunnistus 802.1X EAP. Radius-asetuksista annetaan palvelimen ip-osoite ja avain, joka on sama kuin aiemmin palvelimeen asetettu
- Valinta ”Closed System” päälle.

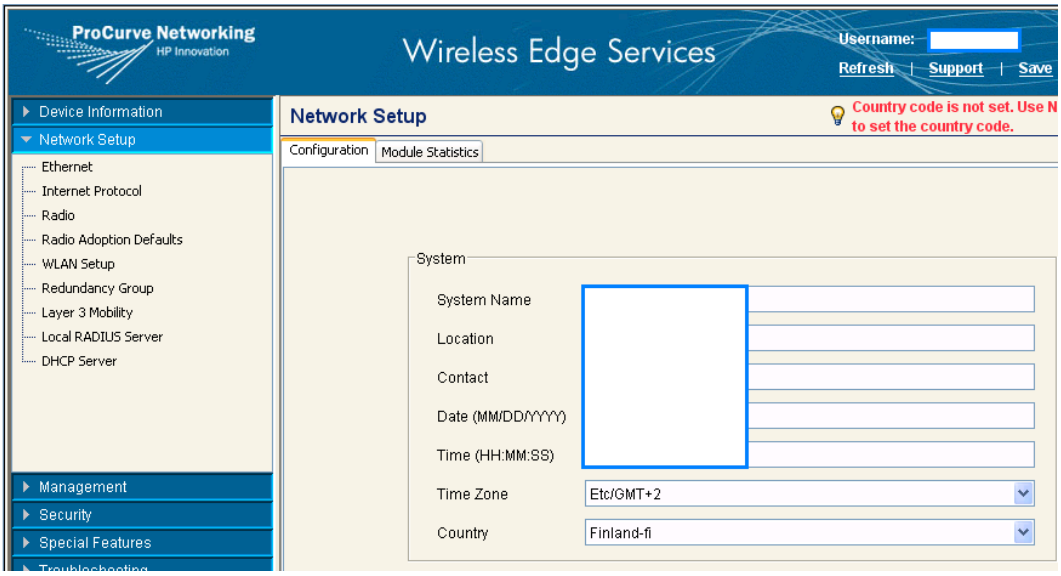
Muita merkittäviä alasivuja ovat ainakin Web Access Control ja SNMP Access.

Lopuksi asetukset on hyvä muistaa tallentaa ylänurkan save-valinnalla.

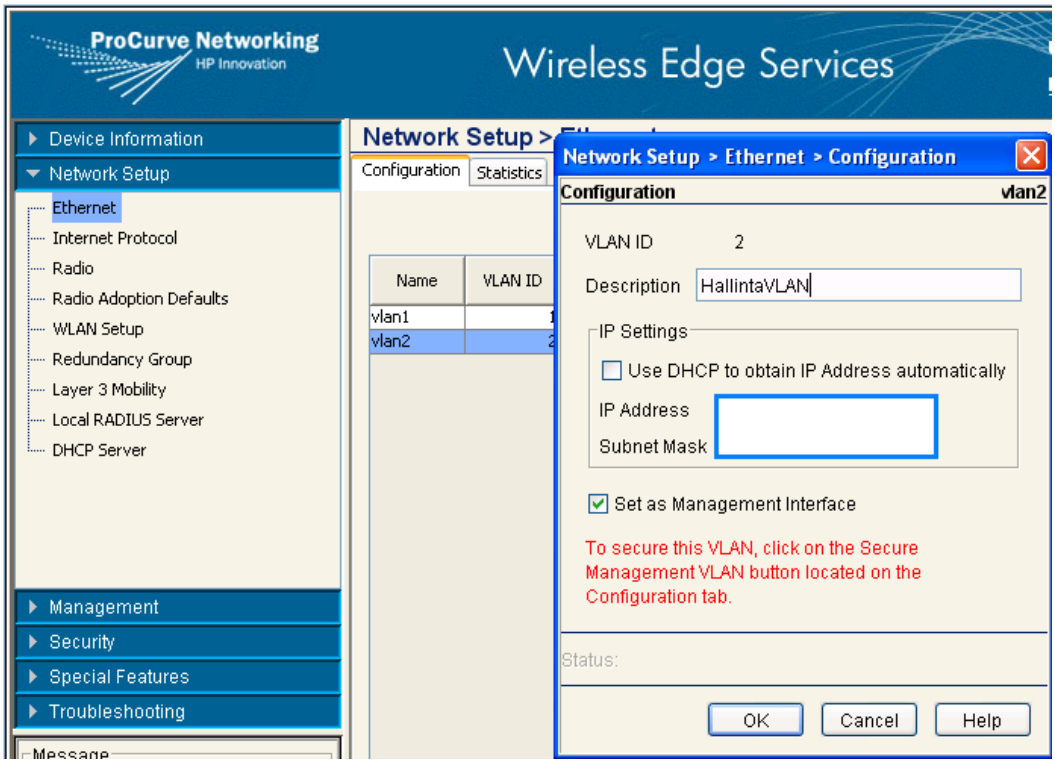


KUVIO 42. Uuden käyttäjän luonti

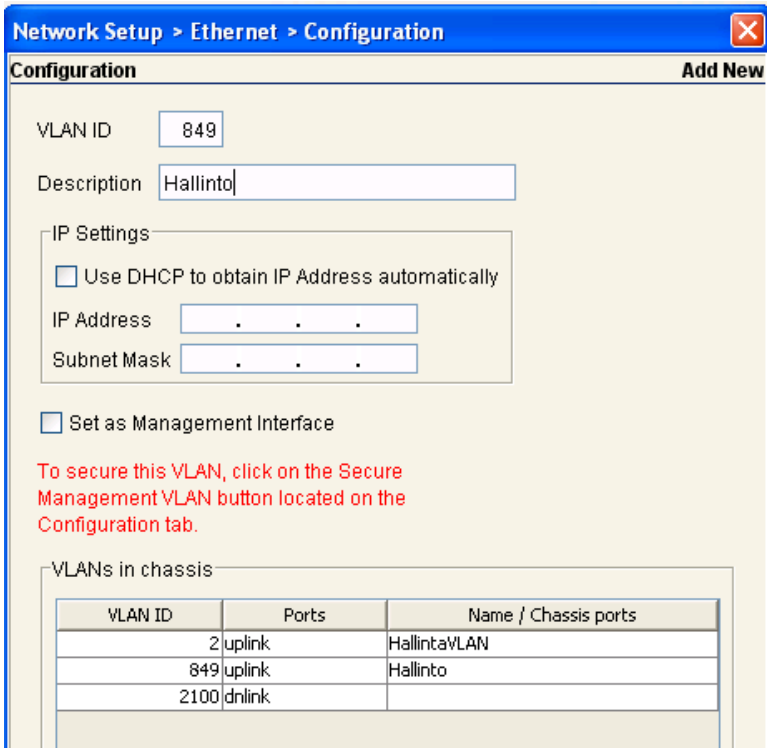
KUVIO 43. Käyttäjätilit



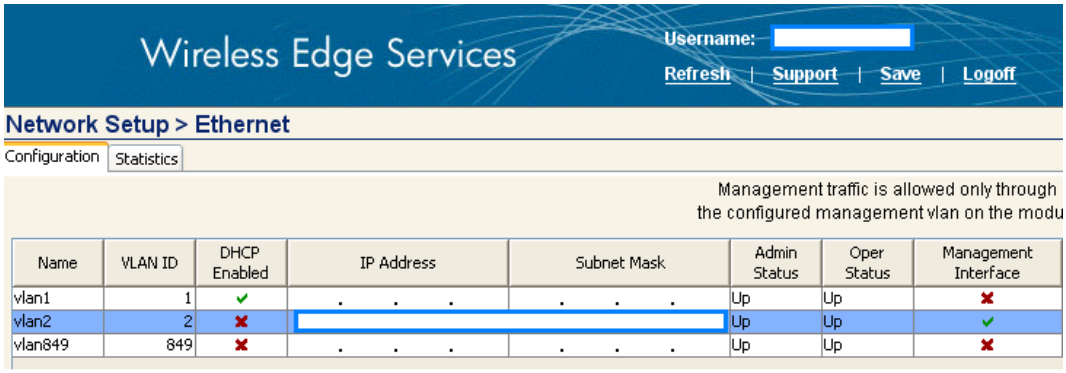
KUVIO 44. Network Setup -välilehti



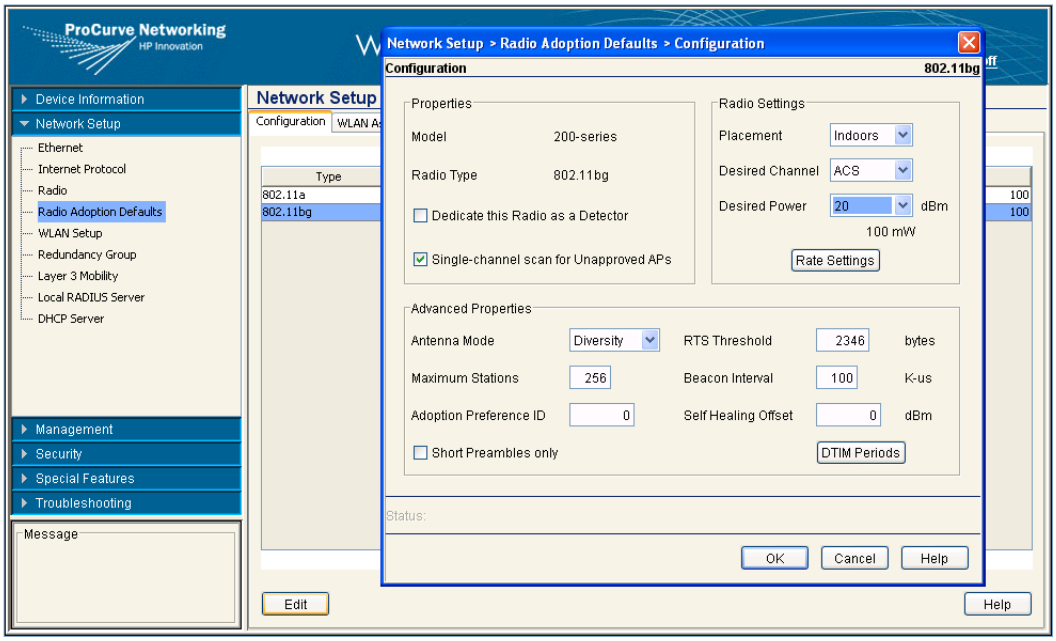
KUVIO 45. Hallinta VLAN:in luominen osoitteineen



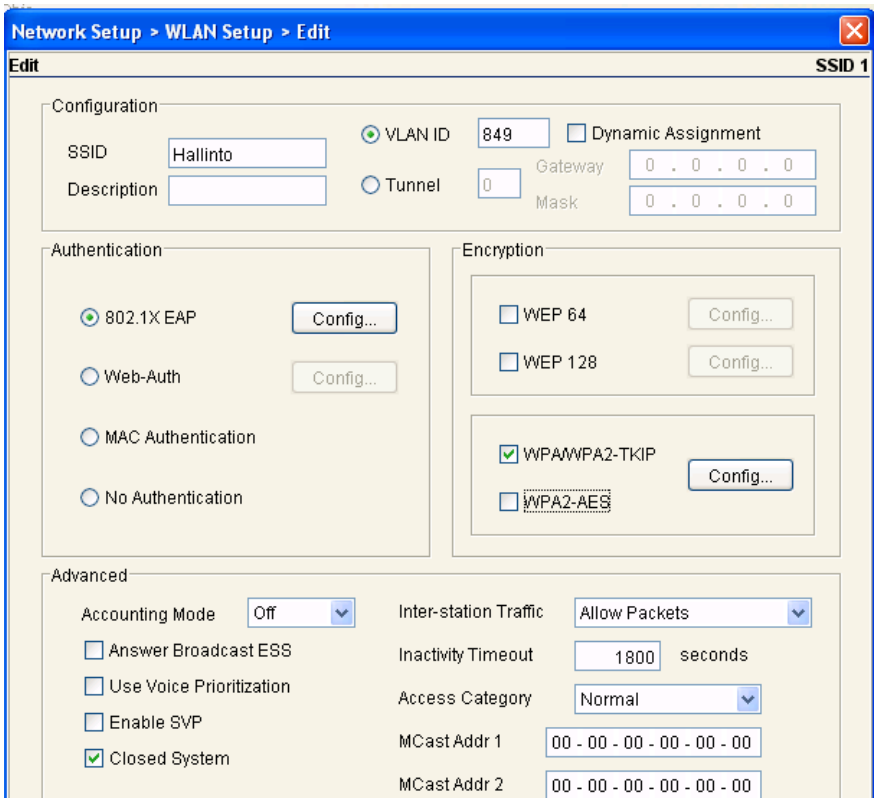
KUVIO 46. Hallinto VLAN:in luonti



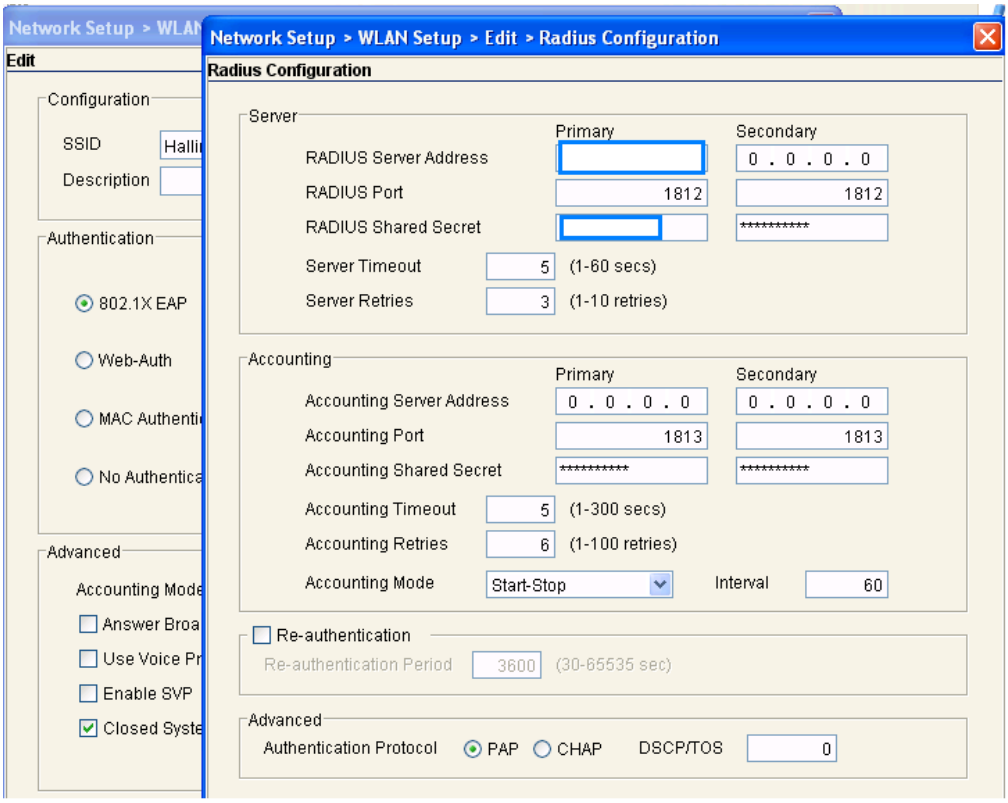
KUVIO 47. Tehdyt asetukset näkyvät taulukossa



KUVIO 48. Radioporttien konfigurointi



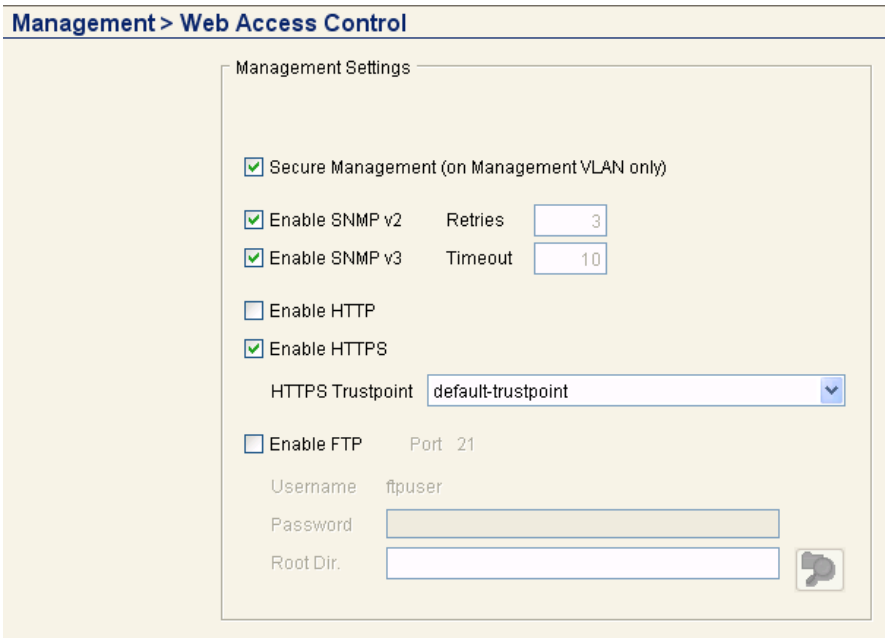
KUVIO 49. Hallinto VLAN:in asetukset



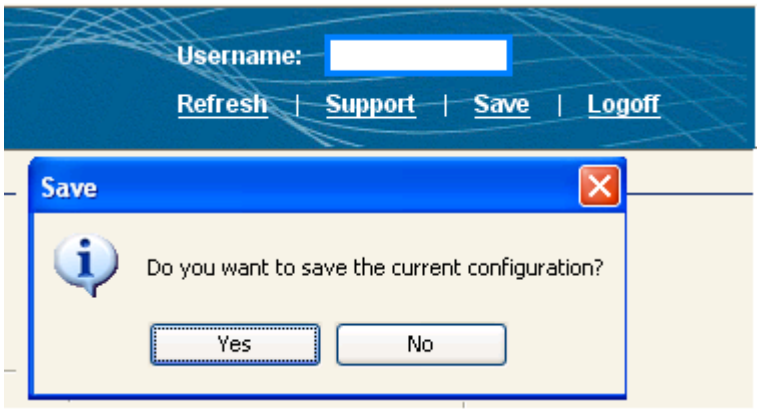
KUVIO 50. RADIUS-asetukset

Index	Enabled	SSID	Description	VLAN / Tunnel	Authentication	Encryption
1	✔	Hallinto		VLAN 849	802.1X EAP	TKIP
2	✖	SSID 2		VLAN 1	None	None

KUVIO 51. VLAN asetukset



KUVIO 52. WES-moduulin hallinnan asetukset

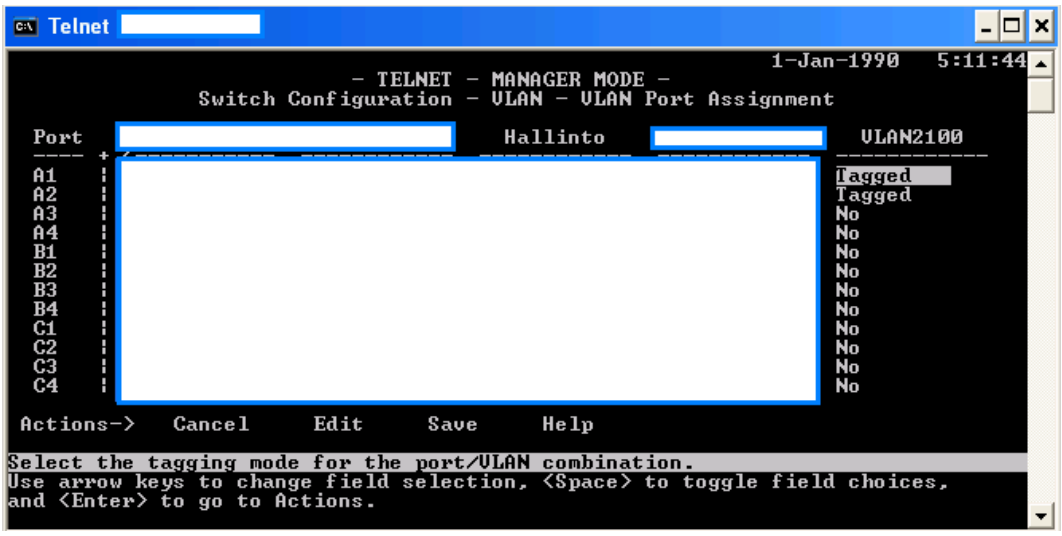


KUVIO 53. Asetusten tallentaminen

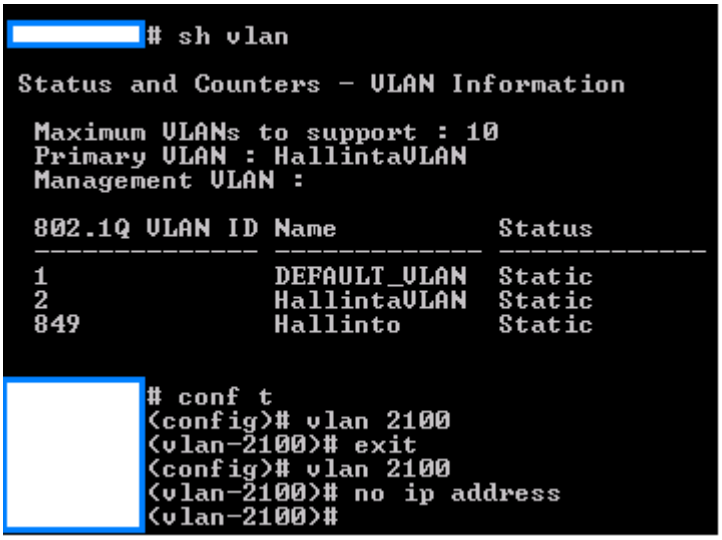
Kytkimien ja radioporttien asennus ja VLAN asetukset

Radioporttien ja WES-moduulin välinen liikenne käyttää oletuksena VLAN 2100:a. Kytkimien portit, joita kautta radioportin liikenne menee WES-moduulille, asetetaan siten ”tagged” tilaan VLAN2100 osalta. Lisäksi varmistetaan, ettei VLAN2100:lla tule olemaan IP-osoitetta.

Keskuskytkimen asetuksiin muokattiin porttien A1:n ja A2:n osalta VLAN2100 tagged-tilaan. Kyseiset portit ovat yhteydessä kytkimiin, joihin taas radioportit ovat yhdistetty. Reunakytkimien keskuskytkimeen yhdistetty portti laitetaan tagged-tilaan ja radioportteihin yhdistetty portti asetetaan Untagged-tilaan.



KUVIO 54. VLAN 2100 asetukset



KUVIO 55. Ip-osoitteen poistaminen VLAN 2100:lta

Avoimen verkon lisääminen

Verkkoasetuksiin lisättiin myös avoin verkko, jota kuka tahansa voi käyttää yhteytenä Internetiin. Avoimen verkon valittiin käyttämään VLAN 848:sta. Kytkimien osalta asetukset tehdään samalla tavoin kuin VLAN 849:lle. Tosin virtuaalisen verkon laajuus on pienempi, koska VLAN 848 luodaan ainoastaan välille keskuskytkin Internet. VLAN 848 asetukset WES-moduulissa eroavat ”WLAN Setup”:n osalta, koska RADIUS-palvelinta eikä liikenteen salausta oteta käyttöön. Lisäksi, vaikka WES-moduulin on mahdollista toimia DHCP-palvelimena, tehtävä annettiin Cisco PIX palomuurille. Cisco PIX Device Managerin asetuksista laitettiin DHCP-palvelu käyttöön: DMZ (Demilitarized zone) otettiin käyttöön ja määriteltiin IP-avaruus (Internet Protocol) sekä DNS -osoitteet (Domain Name System).