LAUREA

IEEE 802.1X -tunnistautuminen langattomissa verkoissa

Jarnola, Miikka
Katainen, Juhana

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

IEEE 802.1X -tunnistautuminen langattomissa verkoissa

Jarnola, Miikka
Katainen, Juhana
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2009

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yrityksen tietoverkot

Jarnola, Miikka
Katainen, Juhana

IEEE 802.1X -tunnistautuminen langattomissa verkoissa

Vuosi 2009 Sivumäärä 77

Tämän opinnäytetyön tarkoituksena on tutkia, miten IEEE 802.1X -tunnistautumisprotokolla toimii ja kuinka sitä voidaan hyödyntää langattomissa verkoissa, joissa vaaditaan hyvää tietoturvaa. Ensin selvitetään, mitä IEEE 802.1 –standardeja langattomat laitteet käyttävät ja millaisia suojaukseen liittyviä ominaisuuksia ne tukevat.

Käytännön osuudessa tutkitaan Windows Server 2008 –palvelinympäristöön toteutettavaa langatonta verkkoa sekä tutustutaan sen asennusvaiheisiin. Teoriaosuudessa mainitut menetelmät ja käytännöt määritellään palvelimiin, tukiasemiin ja asiakaskoneille, jotta langaton verkko toimisi nopeasti ja turvallisesti vaativassa käytössä.

Opinnäytetyön kehitysehdotuksen tilaaja on Laurea-ammattikorkeakoulun Leppävaaran toimipisteen tietoliikennelaboratorio, jonne on suunnitteilla suojattu langaton verkko opiskelijoiden ja opettajien käyttöön. Samalla tutustutaan Laurean opettajille tarkoitetun langattoman verkon toteutukseen. Tutkitun tiedon avulla tehdään kehitysehdotus tilaajalle.

Yhteenvedossa tarkastellaan hyväksi todettuja käytäntöjä toteuttaa langaton verkko opitun tiedon pohjalta. Tulevaisuuden näkymiä langattoman verkon turvallisuuteen liittyen verrataan vanhentuneisiin ja opinnäytetyön aikana vallitseviin käytäntöihin. Lopuksi tarkastellaan langattomia verkkoja käyttäjän näkökulmasta.

Asiasanat 802.1X, Active Directory, AES, Cisco, Network Policy Server, PEAP, RADIUS, TTLS, Windows Server 2008, WLAN, WPA2

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Degree Programme in Business Information Technology
Business Information Networks

Jarnola, Miikka
Katainen, Juhana

IEEE 802.1X -authentication in wireless networks

Year 2009 Pages 77

The purpose of this thesis is to research how the IEEE 802.1X authentication protocol operates and how it can be used in wireless networks which demand strong information security. Firstly, the IEEE 802.1 standards that wireless devices use and what protection features those protocols support will be determined.

The practical section contains research of a wireless network which is implemented in the Windows Server 2008 server environment. In the theory section, the above mentioned methods and policies will be configured to servers, access points and client computers so that the wireless network could work faster and securely in demanding use.

The customer of the development proposal is Laurea University of Applied Sciences Leppävaara's data communication lab where a protected wireless network for students and teachers is proposed. The development proposal also researches the current wireless network for teachers in Laurea. The development proposal is prepared using the information gathered.

The synopsis scrutinizes the best ways to implement a wireless network with the acquired knowledge. The prospects of future wireless network security are compared to previous and current practices. In conclusion, wireless networks are examined from the user's perspective.

Key words 802.1X, Active Directory, AES, Cisco, Network Policy Server, PEAP, RADIUS, TTLS, Windows Server 2008, WLAN, WPA2

Sisällys

1 Johdanto

Langattomista verkoista on tullut suosittu lähiverkon palvelu yksityisessä ja julkisessa käytössä. Yksityisasiakkaille suunnatut langattomat tuotteet ovat nykyään tietoturvallisia ja helppokäyttöisiä. Yrityksille tarkoitetut ratkaisut langattoman verkon toteutukseen ja ylläpitoon vaativat laitteiston ja ohjelmiston puolesta monipuolisempaa määrittelyä.

Yrityksissä WLAN-verkko (Wireless Local Area Networks) jaetaan usein kahteen osaan. Vierailijoille ja työntekijöille tarkoitettu langaton verkko voidaan jakaa fyysisesti ja ohjelmallisesti olemassa olevassa lähiverkossa. Yleisesti ottaen vierailijoiden pääsy on rajattu fyysisesti ja työntekijöiden pääsy on sidottu ohjelmallisesti esimerkiksi käyttäjätunnukseen.

Fyysisesti suojattu langaton verkko sisältää määritykset verkkolaitteisiin, kuten kytkimiin ja reitittimiin. Ohjelmallisesti langaton verkon suojaus määritellään esimerkiksi Windows Server –palvelimen palveluihin. Fyysistä ja ohjelmallista suojausta käytetään usein samanaikaisesti langattoman verkon turvaamiseen ulkopuolisilta hyökkäyksiltä.

Laite- ja ohjelmavalmistajat kehittelevät jatkuvasti uusia langattomia tuotteita nykyisten standardien mukaisesti sekä parantavat niitä tulevaisuuden tarpeisiin. Tämän opinnäytetyön käytännön osuudessa tutustutaan tarkemmin Microsoftin valmistaman Windows Server–palvelinympäristön mahdollisuuksiin toteuttaa turvallinen langaton verkko.

1.1 Tutkimusongelma

Laurea-ammattikorkeakoulun Leppävaaran toimipisteen tietoliikennelaboratoriossa on lähiverkko, jonka käyttäjiä ovat pääasiallisesti tietojenkäsittelyn opiskelijat ja opettajat. Tietoliikennelaboratoriossa on myös langaton verkko. Sen laajempi käyttöönotto vaatii tietoturvaselvityksen, jota hyödyntämällä verkko voidaan suojata ulkopuolisilta käyttäjiltä.

Tämän työn tarkoituksena on selvittää, mikä salaus- ja tunnistautumismenetelmä on helppokäyttöinen ja luotettava vaihtoehto Windows-verkkoympäristöön, joka kuuluu toiminimeen. Työssä selvitetään yleisimmät salaus- ja tunnistautumiskeinot, joita tukee lähes kaikki ohjelmisto- ja laitevalmistajat. Suojaamaton langaton verkko antaa luvattomalle käyttäjälle mahdollisuuden päästä käsiksi tärkeisiin verkon sisällä oleviin palveluihin.

Tässä opinnäytetyössä tutkitaan Laurean nykyisten langattomien verkkojen toteutusta sekä selvitetään mikä olisi varteenotettava malli toteuttaa langaton verkko tietoliikennelaboratorioon. Tutkimuksessa paneudutaan opettajille tarkoitettuun langattomaan verkkoon sekä sen

tekniseen toteutukseen. Tutkimuksen perusteella tehdään kehitysehdotus tietoliikennelaboratorion sekä opettajien käyttöön tarkoitetulle langattomalle verkolle.

1.2 Nykytila

Leppävaaran toimipisteessä on käytössä opiskelijoille ja opettajille langaton verkko. Laurean opettajien langaton verkko on toteutettu tietoturvallisesti kehittyneemmällä tekniikalla kuin opiskelijoille suunnattu langaton verkko. Opettajien langaton verkon ero on piilotettu SSID (Service Set Identifier) ja LEAP-tunnistautumisprotokolla (Lightweight Extensible Authentication Protocol), joka käyttää AD:n (Active Directory) tietokantaa. Opiskelijoiden langaton verkko pohjautuu esimääriteltyihin salausavaimiin. Opiskelijoiden julkinen langaton verkko käyttää esimääriteltyjä avaimia (PSK, PreShared Key).

Taulukko 1: Laurean langattomien verkkojen vertailu

	SSID	Suojaus	Salaus	Tunnistautuminen
Opettaja-WLAN	Piilotettu	WPA	TKIP	LEAP
Opiskelija-WLAN	Näkyvä	WPA	TKIP	PSK

Laurean nykyinen verkkoinfrastruktuuri tukee mahdollisuutta ottaa käyttöön uusimmat salaustekniikat ja autentikointitavat esimerkiksi käyttäen WPA2 (Wireless Fidelity Protected Access) ja PEAP-protokollia (Protected Extensible Authentication Protocol). Lähiverkko on toteutettu pääasiassa Ciscon laitteilla, mikä on ollut yksi syy ottaa LEAP käyttöön, kun nykyinen langaton toteutus otettiin käyttöön henkilökunnalle.

Ciscon standardisoimaton LEAP-tunnistautumistapa käyttää AD:n tietokantaa käyttäjien tunnistukseen. Vuonna 1999 julkistetun WPA:n ja vuonna 2002 WPA:han lisätyn TKIP:n (Temporal Key Integrity Protocol) on korvannut WPA2 ja AES (Advanced Encryption Standard).

WPA2 ja AES ovat Ciscon ja Microsoftin hyväksymiä käytäntöjä langattomissa verkoissa. Verrattuna opiskelijoiden julkiseen langattomaan verkkoon, opettajien langaton verkko on vahvemmin suojattu, mutta vanhentunut suojauksen osalta.

PSK:n käyttö WPA-suojauksen yhteydessä on heikko salausvaihtoehto, ellei salausavainta vaihdeta riittävän usein. PEAP-tunnistautuminen antaa varmemman suojan tunnistaa käyttäjät, sillä kaikilla käyttäjillä on oma käyttäjätunnus sekä määritellyt oikeudet verkon palveluihin. Lisäksi käyttäjien hallinta ja seuraaminen helpottuu, jos tunnistautumispalvelimissa käytetään tilastointipalveluita, jotka tallentavat lokitiedostoja käyttäjän toimista.

1.3 Rajaus

Opinnäytetyössä ei käsitellä langattoman verkon toteutukseen tarvittavia kaikkia fyysisiä verkkolaitteita, kuten reitittimiä ja kytkimiä. Langattoman verkon fyysisen tason standardeista käydään läpi yleisimmät markkinoilla olevat vaihtoehdot. Langattoman tiedonsiirron teknisiin vaiheisiin ei myöskään perehdytä tarkemmin.

Langattoman verkon käyttöönottoon liittyvä asennusdokumentaatio on suuntaa antava ohje, joka sisältää tärkeimmät kohdat, joilla langaton verkko voidaan kyseisellä kokoonpanolla toteuttaa. Asennusdokumentaation verkkotopologia on kuvattu langattoman verkon näkökulmasta. Siinä ei oteta kantaa, kuinka langaton verkkotopologia liitetään lähiverkkoon.

2 IEEE 802.11 -standardit

2.1 IEEE

IEEE (Institute of electrical and electronics engineers) on johtava kansainvälinen tekniikan edistämisen hyväksi toimiva järjestö. IEEE:n päätehtäviin kuluu erilaisten standardien valmisteleminen ja julkaiseminen. IEEE toimii avaruuden, tietoliikenteen, kulutuselektroniikan ja biolääketieteen aloilla. Tämän organisaation jäsenet hyödyntävät IEEE:tä teknillisen ja ammatillisen informaation lähteenä.

IEEE-organisaatioon kuuluu yli 375 000 jäsentä yli 160 maasta. IEEE on jakautunut kymmenelle maantieteelliselle alueelle, joissa toimii yhteensä 324 jaostoa. Tällä organisaatiolla on kehitteillä yli 1300 projektia ja standardia. Voimassa olevia IEEE standardeja löytyy yli 900 kappaletta. (IEEE. About IEEE. 2009).

2.2 802.11

802.11 on IEEE:n standardi langattomille lähiverkoille. 802.11 määrittää OSI-mallin fyysisen kerroksen sekä siirtokerroksen alemman osan, joka tunnetaan nimellä MAC (Media Access Control).

Standardin verkkotopologiat ovat Ad hoc -verkko, jossa mobiiliasemat (MS) ovat suoraan yhteydessä toisiinsa ja infrastruktuuri-verkko, jossa mobiiliasemat liikennöivät tukiasemien (AP) kautta.

802.11-standardin ensimmäinen hyväksytty versio julkistettiin vuonna 1997. Langattomien lähiverkkojen standardit käyttävät Ethernet-lähiverkkoprotokollaa ja CSMA/CA tekniikkaa

(Carrier Sense Multiple Access With Collision Avoidance). 802.11-standardeista tärkeimmät ja yleisimmin käytetyt ovat 802.11a, 802.11b, 802.11g ja 802.11n.

2.3 802.11a

Tämä standardi toimii 5 GHz:n (Gigahertz) taajuusalueella tarjoten teoriassa 54 Mbps (Mega bit per second) nopeuden. Todellisuudessa tiedonsiirtonopeus puolittuu. Tämä johtuu käytetystä taajuudesta ja signaalin kantamasta.

2.4 802.11b

802.11b-standardi tarjoaa teoriassa 11 Mbps tiedonsiirtonopeuden. B-standardi toimii 2,4 GHz:n taajuudella. Tässäkin tapauksessa ero teoreettisen ja todellisen nopeuden välillä selittyy kantamalla ja rakenteellisilla esteillä.

2.5 802.11g

802.11g toimii 2,4 gigahertsin taajuudella, tarjoten 54 Mbps tiedonsiirtonopeuden. Standardi käyttää OFDM-lähetystekniikkaa (Orthogonal Frequency-Division Multiplexing). G-standardissa on yhdistetty a- ja b-standardien parhaat ominaisuudet. 802.11g-standardi on taaksepäin yhteensopiva b-standardin laitteiden kanssa.

802.11g-standardi on risteytys 802.11a- ja 802.11b-standardeista, koska se käyttää tiedonsiirtoon CCK-OFDM-tekniikkaa (Complimentary Code Keying/Orthogonal FDM) ja tarjoaa vaihtoehtoisesti siirtotavaksi PBCC-tekniikan (Packet Binary Convolutional Code).

Standardi määrittää radiotaajuustekniikoista DSSS (Direct Sequence Spread Spectrum)-, HR/DSSS (High Rate / Direct Sequence Spread Spectrum)- ja OFDM-tekniikat. Se kykenee liikennöimään nopeuksilla 54 ja 11 Mbps käyttäen 2,4 GHz:n taajuutta ollen siksi täysin yhteensopiva vanhemman 802.11b-standardin kanssa.

2.6 802.11n

802.11n – standardi on tuotu markkinoille vuonna 2008. Sen tarkoitus on korvata a-, b- ja g-standardit. IEEE:n arvion mukaan n- standardi on standardisoitu joulukuuhun 2009 mennessä.

802.11n – standardi tukee MIMO-tekniikkaa (Multiple Input, Multiple Output). Tämä tarkoittaa kahden tai useamman antennin ja kanavan yhtäaikaista käyttöä. Käytettävät taajuudet ovat 2,4 ja 5 GHz.

N-standardi mahdollistaa todellisuudessa 100–200 megabitin tiedonsiirtonopeuden. 802.11n-standardi on taaksepäin yhteensopiva 802.11a, 802.11b ja 802.11 g-standardien kanssa.

2.7 802.11e

E-standardiin on lisätty QoS-ominaisuuksia (Quality of Service), sekä multimedian tuki. 802.11e- standardiin on lisätty verkon suorituskykyä parantavia ominaisuuksia. Tämän takia on saatu mahdolliseksi VoIP- palvelu (Voice over Internet Protocol) sekä reaaliaikainen video-kuvan toisto langattomiin yhteyksiin.

2.8 802.11f

Tällä standardilla mahdollistetaan langattomien liityntäpisteiden välinen liikenne. F-standardi käyttää IAPP-protokollaa (Internet Access-Point Protocol). 802.11f-standardin avulla eri valmistajien ja Internet-palveluiden tarjoajien laitteet ja palvelut ovat yhteensopivia.

2.9 802.11i

I-standardi sisältää tietoturvaparannuksia. Tähän standardiin on lisätty AES-salausalgoritmi. Toisena parannuksena 802.11i-standardista löytyy TKIP-salaus.
(http://www.ieee.org/portal/site).

Taulukko 2: IEEE 802.11 -protokollien vertailu

Protokolla	Julkaisuvuosi	Taajuusalue	Teoreettinen tiedonsiirtonopeus	Todellinen tiedonsiirtonopeus
802.11	1997	2,4 GHz	1 Mbit/s	1 Mbit/s
802.11a	1999	5,0 GHz	54 Mbit/s	23 Mbit/s
802.11b	1999	2,4 GHz	11 Mbit/s	4,3 Mbit/s
802.11g	2003	2,4 GHz	54 Mbit/s	19 Mbit/s
802.11n	2008	2,4 ja 5,0 GHz	600 Mbit/s	130 Mbit/s

2.10 802.1X

Porttiperusteisessa verkkoon pääsy -menetelmässä (Port Based Network Access Control) rajoitetaan käyttäjän pääsyä langattomaan verkkoon loogisten porttien ja todennuspalvelimien avulla. 802.1X:n tarkoituksena on estää luvattoman työaseman kommunikointi langattomien verkkojen liityntäpisteiden kautta. Menetelmään kuuluvat työasema (Suplicant), tukiasema (Authenticator) ja todennuspalvelin (Authentication Server).

Langattomat laitteet toimivat loogisina verkkoportteina (Port Access Entity), jotka muodostavat päästä-päähän-yhteyden (Point to Point). Protokolla tukee 128-bittisiä salausavaimia, jotka ovat yksilöllisiä käyttäjille ja verkkosessiolle. Avaintenhallinta tukee automaattista avaintenvaihtoa ja avaintenvaihdon aikavälin määritystä.

802.1X on suunniteltu käytettäväksi kaikissa IEEE 802 –verkoissa, jolla rajoitetaan verkkoon pääsyä. Se myös mahdollistaa paremman ja laajemman suojauksen kuin verkossa yleisesti käytetyt käyttäjienhallintatekniikat, jotka rajoittavat käytännössä lähinnä palvelimiin ja työasemiin pääsyä. (Hakala-Vainio-Vuorinen 2006, 298.)

3 Suojausprotokollat

3.1 SSID

SSID (Service Set Identifier) on langattomissa verkoissa käytetty verkkotunnus. SSID-tunnuksen avulla voidaan yksilöidä samalla alueella toimivat WLAN-verkot. Tunnus mahdollistaa myös kytkeytymisen haluttuun verkkoon. SSID-tunnus on myös kaikissa verkossa liikkuvissa paketeissa. Paketeissa oleva tunnus yksilöi nämä paketit maksimissaan 32-merkkisellä merkkijonolla. SSID:n avulla yksilöidään myös kaikki verkossa olevat tietoliikennelaitteet.

3.1.1 Ad hoc -verkot

Ad hoc –verkossa lankaverkkoon liitetyt laitteet kommunikoivat keskenään langattomasti. Näitä laitteita on tavallisesti yhdestä kolmeen. Esimerkiksi kahden kannettavan tietokoneen välille luotu yhteys. Ad hoc:n tunniste on IBSS ID (Independent Basic Service Set Identifier). (Odom 2008, 305–306.)

3.1.2 Tukiasemalliset verkot

Tukiasemallisissa verkoissa BSS (Basic Service Set) käyttää yhtä liityntäpistettä langattoman verkon luomiseen. ESS Extended Service Set) käyttää verkon luomiseen useita liityntäpisteitä. ESS sallii myös verkkovierailut ja mahdollistaa käyttäjän siirtymisen verkosta toiseen ilman yhteyden katkeamista. (Odom 2008, 305–306.)

3.1.3 Tietoturva

SSID näkyy usein oletuksena langattomissa laitteissa. Se on mahdollista piilottaa, jotta kaikki eivät näe langatonta verkkoa. SSID:n piilottaminen estää vain satunnaiset hyökkäysyritykset.

SSID kulkee avoimena tekstinä verkossa, kun käyttäjät kirjautuvat verkkoon. Langattomia verkkoja salakuuntelemalla SSID voidaan löytää kohtuullisessa ajassa.

3.2 MAC

MAC (Media Access Control) on tapa, jolla tietoliikenteessä valvotaan tietokoneiden tiedonsiirtoa. MAC:n tarkoituksena on huolehtia, että vain yksi kone kerrallaan lähettää tietoja verkossa, jotta ei tule törmäyksiä. Liikennettä voidaan hallita kontrolloidulla pääsyllä (Controlled Access) ja kilpailukäytännöllä (Contention).

3.2.1 Kontrolloitu pääsy

Kontrolloitu pääsy toimii kiertokysely-periaatteella. Keskuskone hallinnoi piiriä ja päättää kuka pääsee milloinkin käsiksi mediaan. Kiertokyselyssä signaali lähetetään asiakkaalle, joka antaa luvan lähettää tai vastaanottaa tietoa. Keskuskone tai palvelin lähettää tietyin aikavälein kiertokyselyn asiakkaille. Jos tietokoneella tai terminaalilla on lähetettävää dataa, se lähetetään. Keskuskoneen saadessa kielteisen vastauksen datan lähetystarpeesta tehdään kysely seuraavalle koneelle.

Kiertokyselyitä on useita erilaisia. Käytetyimmät ovat roll-call polling ja hub polling. Roll-call-kyselyssä palvelin käy läpi listalla olevat asiakkaat, esimerkiksi asiakas 1, asiakas 2 ja asiakas 3. Asiakkaiden tärkeyttä voidaan priorisoida niin, että palvelin käy läpi tietyt asiakkaat useampaan kertaan, esimerkiksi asiakas1, asiakas 2, asiakas 1, asiakas 3, asiakas 4, asiakas 1, asiakas 5 ja asiakas 6. Roll-call-kiertokyselyssä pieni viive on tyypillistä, koska kysely on tehtävä, vaikkei olisi mitään lähetettävää. Näin ollen palvelin joutuu tekemään kyselyn ja odottamaan aina vastausta.

Hub polling tunnetaan myös nimellä token passing. Hub polling-kyselyssä yksi tietokone aloittaa kiertokyselyn ja lähettää sen eteenpäin seuraavalle koneelle. Kyselyn saanut kone lähettää tarvittaessa datansa ja siirtää kyselyn seuraavalle koneelle. Kiertokyselyä lähetetään eteenpäin kunnes se saavuttaa ensimmäisen koneen. Tämän jälkeen kierros aloitetaan alusta. (FitzGerald 2007, 119–120).

3.2.2 Kilpailukäytäntö

Kilpailukäytäntö on vastakohtainen toimintatapa hallitulle pääsylle. Kilpailukäytäntöä käyttävässä ympäristössä koneet odottavat, kunnes verkko on vapaa ja lähettävät dataa tarvittaessa. (FitzGerald 2007, 119–120).

3.2.3 Langattomat verkot

MAC käyttää langattomissa verkoissa CSMA/CD-tekniikkaa, joka on eräänlainen kilpailukäytäntö. Tässä käytänteessä verkon laitteet lähettävät vapaasti paketteja siirtotielle. Yhteentörmäyksen sattuessa paketille määrätään satunnaisesti uusi lähetysaika. Verkossa olevat laitteet kuuntelevat verkkoa ja verkon ollessa vapaa, ne lähettävät viestinsä. Törmäysten havaitseminen langattomissa verkoissa on vaikeampaa kuin langallisissa verkoissa. Tämän takia törmäyksiä yritetään välttää mahdollisimman paljon. (FitzGerald 2007, 247 - 248).

3.2.4 MAC-osoitteiden suodatus

Langattomista ja langallisista verkkokorteista löytyvät yksilölliset MAC-osoitteet. Näillä osoitteilla verkossa olevat laitteet voidaan tunnistaa. Tämä tapahtuu laittamalla tukiasemiin vain sallittujen laitteiden MAC-osoitteet. Toimenpide on erittäin yksinkertainen tapa suojata langaton verkko.

MAC-osoitteiden suodatus on heikko tapa suojata langaton verkko, sillä verkkokorttien MAC-osoitteet on helppo vaihtaa mukana tulevilla ajureilla tai Internetistä saatavilla ilmaisohjelmilla. MAC-osoitteet kulkevat selväkielisinä verkossa, josta luvattomat käyttäjät voivat poimia tukiaseman hyväksymän MAC-osoitteen ja laittaa sen oman verkkokorttinsa osoitteeksi. MAC-osoitelistan ylläpitäminen isossa ympäristössä on haastavaa. (Barken 2004, 6-7).

3.3 WEP

WEP (Wired Equivalent Privacy) on ensimmäinen 802.11- standardien langattomille verkoille määritelty salausmenetelmä. WEP perustuu jaetun avaimen menetelmään, jossa työasemiin ja tukiasemiin määritellään samat avaimet. Avaimen pituus voi olla 64- tai 128-bittiä. Molemmat avaimen pituudet sisältävät 24 bitin alustusvektorin (Initialization Vector).

Työasemiin ja tukiasemiin voidaan määritellä enintään neljä avainta, mutta järjestelmässä ei ole automaattista avainten vaihtoa. WEP toimii myös salausmenetelmänä perustuen RC4-salausalgoritmiin (Rivest Cipher 4).

Työaseman ja tukiaseman sanomaliikenne tunnistustilanteessa tapahtuu seuraavasti:

- Tunnistustilanteessa työasema lähettää Authentication Request – pyynnön, jossa se ilmoittaa tukevansa jaetun avaimen tunnistusta. Tässä tunnistustyyppisessä hallintakehyksessä on sekvenssinumerona 1.

- Tukiasema lähettää työasemalle satunnaisen haastetekstin hallintakehyksessä, jonka tunnistusalgoritmiksi ilmoitetaan jaetun avaimen tunnistus, tilakoodiksi onnistunut, haastetekstiksi generoidaan satunnainen merkkijono ja sekvenssinumeroksi 2.
- Työasema lähettää vasteena saman tunnistusalgoritmin, haastetekstin ja sekvenssinumeron 3 ja salaa informaatioelementit omalla WEP-avaimella.
- Tukiasema purkaa vasteen informaation omalla avaimella ja vertaa tulosta haasteeseen. Jos tulokset ja salausavaimet ovat samat, tunnistus hyväksytään kuittaussanomalla. Negatiivisessa tapauksessa lähetetään epäonnistunut syykoodi. Vastauksen sekvenssinumero on 4.

(Puska 2005, 74.)

WEP-salauksen puutteita ovat:

- WEP-avaimet on määriteltävä manuaalisesti.
- WEP-avaimet tallentuvat työaseman asetuksiin.
- ”IV-alustusvektori lähetetään kehyksen alussa salaamattomana ja sama vektori toistuu noin 17. miljoonan kerran välein.” (Puska 2005, 81)
- 64- ja 128-bitin salausavainten voidaan murtaa käyttämällä voimahyökkäystä (Brute Force Attack), jolla tarkoitetaan eri avainyhdistelmien kokeilemista.
- Samaa avainta useasti käytettäessä, vuosalausmenetelmät ovat haavoittuvia ja mahdollistavat tiedon analysoinnin.

(Puska 2005, 74.)

3.4 WPA

WPA (Wireless Fidelity Protected Access) kehitettiin WEP-salauksen ongelmien paljastuttua. WEP-salauksen heikot aloitusvektorit on korjattu ja lisäksi salausavainta vaihdetaan automaattisesti 10000 paketin välein. WPA tukee kahta protokollaa, joista TKIP (Temporal Key Integrity Protocol) hoitaa pakettien salauksen ja EAP (Extensible Authentication Protocol) käyttäjätunnistuksen.

TKIP kehitettiin korjaamaan WEP:n puutteita. TKIP–algoritmijoukko on käytössä WEP-salauksessa ja WPA-salauksessa. WPA ja TKIP julkistettiin etukäteen, koska ei ollut mahdollista odottaa, että 802.11i-tietoturvastandardi tulisi valmiiksi. TKIP yhdessä 802.1X:n kanssa korjaa suurimman osan WEP:n puutteista.

TKIP:n tarkoitus on korjata seuraavat WEP-salauksen heikkoudet:

- Väliintulohyökkäys (Replay attack)
- Huijaus/väärennös-hyökkäykset (Forgery attacks)
- “Avaintörmäys” -hyökkäys (Key collision attacks)
- ”Heikon avaimen” -hyökkäys (Weak key attacks).

TKIP sisältää parannellun MIC-funktion (Message Integrity Code), uudistetun alustusvektorin sisältäen vektorien vaihtosäännöt ja salausavaimien pakettikohtaisen käytön. TKIP käyttää samaa RC4-salausalgoritmia kuin WEP, jossa avaimen pituus on 128 bittiä.

Protokollassa voidaan käyttää autentikointipalvelimiin ja älykortteihin perustuvaa salausta ja etukäteen jaettuja aloitusavaimia (PreShared Key, PSK). PSK:ssa työasemiin ja tukiasemiin määritellään aloitusavain, jota käyttämällä laitteet muodostavat yhteyden.

TKIP:n salaus tapahtuu seuraavalla tavalla:

- Salaus aloitetaan kahdella avaimella, joista toinen on 128-bittinen salausavain: Temporal Key (TK) ja toinen 64-bittinen eheysavain, Message Integrity Code (MIC).
- Seuraavaksi lähettäjän MAC-osoitteen avulla TK luo 1. vaiheen avaimen. Tämä avain yhdistetään järjestysnumeroon, jotta saadaan 2. vaiheen avain, niin kutsuttu pakettikohtainen avain.
- Pakettikohtainen avain lähetetään eteenpäin tavallisena 128-bittisenä avaimena. Loppuosa prosessista hoituu normaalilla WEP-siirtotavalla. Tällä tavoin kukaan asiakas ei käytä samaa WEP-avainta.

(Barken 2004, 62-65.)

WPA:n heikkoudet ovat TKIP:n käyttämässä RC4-salauksessa ja palvelunestohyökkäyksien (Denial of Service Attack, DoS Attack) torjunnassa. Verkon jouduttua hyökkäyksen uhriksi, tukiasema sulkee verkon minuutiksi, jolloin kaikki liikenne estyy. (Hakala 2006, 297.)

3.5 WPA2

WPA2 (Wireless Fidelity Protected Access 2) tarkoittaa samaa kuin 802.11i-tietoturvastandardi. Siinä määritellään 802.1X:n todennus- ja avaintenhallintakäytännöt sekä parannetut menetelmät tiedon salaukseen. 802.11i tarjoaa samat ratkaisut kuin WPA, mutta lisäksi valittavana on AES-salaus.

WPA2:n avaintenhallinta perustuu avainpareihin. Työasema ja tukiasema salaavat liikenteen parittaisilla lähetysavaimilla, jotka vaihdetaan määräajoin. Työasemaan ja tunnistuspalvelimeen määritellään yleisavain (Master Key), jonka perusteella muodostetaan muut tarvittavat avaimet. Yleisavain on uniikki kyseiselle avaimelle.

WPA2 sisältää esitunnistuksen (Pre-authentication) ja siirtymisen tukiasemasta toiseen ilman uudelleentunnistusta. Järjestelmä perustuu siihen, että tunnistuspalvelin lähettää käyttäjätiedot tukiasemille. Työaseman siirtyessä tukiasemasta toiseenp tarvitaan vain liittyminen tukiasemaan.

AES (Advanced Encryption Standard) kehitettiin WPA2-salaukseen korvaamaan RC4-standardi. AES käyttää RC4:ää vahvempaa Rijndael-algoritmia ja 128, 192 ja 256 bitin salausavainta. WPA2 sisältää CCMP-salauksen (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), joka toteutetaan AES-salauksella.

WPA2: ssa käytetään CBC-MAC-lohkosalausta (Counter Mode with Chiper Block Chaining Messsage Authentication Code). AES toimii ”counter mode” -periaatteella. Käytännössä tämä tarkoittaa, että ”counter mode” huolehtii salauksesta sekä samaan aikaan CBC-MAC-protokolla toimittaa tarvittavat autentikoinnit ja huolehtii datan eheydestä.

RC4:n tavoin AES on suunniteltu symmetrisen avaimen algoritmin periaatteilla. Salattu teksti salataan ja puretaan käyttäen samaa symmetristä salausavainta. AES tuottaa edeltäviin tekniikoihin nähden erittäin vahvan salauksen. WPA2 soveltuu staattisille ja dynaamisille salausavaimille ja sitä käytetään myös 802.1X-järjestelmissä.

AES-salauksen vaiheet ovat:

- Asiakaskone ja tunnistuspalvelin luovat yhteisestä yleisavaimesta parittaisen yleisavaimen (PMK, Pairwise Master Key), jonka tunnistuspalvelin lähettää tukiasemalle.
- Tukiasema lähettää yksittäisen bittijonon (Anonce) asiakaskoneelle, joka luo tästä jo omasta yksittäisestä bittijonosta Snonce parittaisen tilapäisavaimen (PTK, Pairwise Transient Key), joka lähetetään tukiasemalle PMK:lla salattuna.
- Nelinkertainen kättely (Four-Way Handshake) kuittaa viestinvaihdon ja MIC-otsikko varmistaa sanomien eheyden.
- PTK-avaimesta lasketaan avaintenvaihdon vahvistusavain (TK, Temporar Key).
- Ryhmä- ja yhteislähetyksiä varten tukiasema generoi satunnaisen ryhmälähetysavaimen (GTK, Group Transmit Key), salaa sen avaintenvaihdon salausavaimella ja lähettää työasemalle ryhmäavainkättelyä (Group Key Handshake) käyttäen.

(Barken 2004, 66-68).

Taulukko 3: Langattomien verkkojen suojaustapojen vertailu (CCENT/CCNA ICND 1 Official Exam Certification Guide, 326)

Standardi	Julkaisuvuosi	Avaintenhallinta	Laitehallinta	Käyttäjienhallinta	Salaus
WEP	1999	Staattinen	Kyllä (heikko)	Ei	Kyllä (heikko)
WPA	2003	Staattinen ja dynaaminen	Kyllä	Kyllä (802.1X)	Kyllä (TKIP)
WPA2	2006	Staattinen ja dynaaminen	Kyllä	Kyllä (802.1X)	Kyllä (AES)

4 Tunnistusprotokollat

4.1 EAP

EAP:n (Extensible Authentication Protocol) alkuperäinen tarkoitus oli toimia laajennuksena PPP:lle (Point-to-Point Protocol), jonka tarkoitus on muodostaa suora yhteys verkkolaitteiden välille. PPP:tä on käytetty puhelin- ja modeemiyhteyksissä. EAP mahdollistaa yleisen rungon useille tunnistusmenetelmille. Käyttäjän voi tunnistaa millä tahansa käytössä olevalla menetelmällä, joita ovat esimerkiksi varmenteet ja biometriset tunnisteet.

EAP-järjestelmän toiminta vaatii asiakaskoneen (Supplicant), tukiaseman (Authenticator) ja tunnistuspalvelimen (Authentication Server). Langattomassa verkossa asiakaskone ja tukiasema keskustelevat EAPOW-protokollalla. Tukiaseman ja tunnistuspalvelimen kommunikoinnissa käytetään esimerkiksi RADIUS-tunnistusprotokollaa (Remote Authentication Dial-In User Service).

EAP toimii seuraavalla tavalla:

- Asiakaskone liittyy tukiasemaan MAC-osoitteella. Tukiasema välittää tässä vaiheessa vain EAP-liikennettä kyseisestä osoitteesta. Todennus tapahtuu 802.11:n avoimella autentikoinnilla.
- Asiakaskone lähettää EAPOL-Start-sanoman, johon tukiasema vastaa kysymällä käyttäjätietoja.
- Asiakaskone ilmoittaa käyttäjätiedot tiivisteellä (Hash), joka ei sisällä salasanaa.
- Tukiasema tarkistaa käyttäjätiedot ja muuttaa ne RADIUS-pyynnöksi ja lähettää EAP-sanoman RADIUS-attribuuttina.

- Tunnistuspalvelin vastaa haastepaketilla, joka sisältää satunnaisen merkkijonon (Challenge) ja salaisella avaimella salatun haasteen.
- Asiakaskone lukee käyttäjän salasanan ja salakirjoittaa sille haastejonon.
- Tunnistuspalvelin salaa lähetetyn haasteen paikallisesti käyttäjän salasanalla ja vertaa tulosta saamaansa sanomaan. Jos salatut haasteet täsmäävät, käyttäjä voi liittyä verkkoon.
- Tunnistuspalvelin lähettää positiivisen RADIUS-Access-Accept-sanoman, jonka tukiasema muuttaa EAP-Success-sanomaksi. Samassa sanomassa tunnistuspalvelin lähettää myös istunnon avaimen, joka voi olla esimerkiksi WEP- tai WPA-avain.
- Tukiasema lähettää asiakaskoneelle toisen avaimen, jota käytetään ryhmä- ja yleislähetyskehyksillä, joka salataan istuntoavaimilla. Tällöin vain oikea asiakaskone voi selvittää yhteislähetysavaimen sisällön.
- Asiakaskoneen katkaistessa yhteyden, se lähettää EAP-Logoff-sanoman tukiasemalle, jolloin kyseisen asiakaskoneen assosiaatio poistuu tukiaseman tiedoista.

EAP-protokollat ovat 802.1X-standardin autentikointimenetelmiä. EAP-metodeja on kymmeniä, joista käytetyimpiä ovat: MD5, TLS, TTLS, PEAP ja LEAP.

4.2 MD5

MD5:ssä (Message-Digest 5) salasanat ovat varastoitu selväkielisinä palvelimelle. MD5 tarjoaa vain yksisuuntaisen autentikoinnin. MD5 ei myöskään tue dynaamista WEP- tai TKIP-avaimen luontia. MD5 on altis useille hyökkäyksille kuten esimerkiksi sanakirjahyökkäyksille. MD5:tä on parempi käyttää näiden ongelmien takia vain testiympäristöissä.

4.3 TLS

TLS (Transport Layer Security) on tässä luvussa mainituista salausmenetelmistä vahvin ja vaikein toteuttaa. TLS tarjoaa kaksisuuntaisen tunnistuksen ja dynaamisten avaimenluonnin. Protokolla käyttää salattua tunneliyhteyttä käyttäjätunnisteiden siirtämisessä. Tästä johtuen työaseman ja palvelimen on käytettävä digitaalisia varmenteita.

4.4 TTLS

Autentikointitietojen välittämisessä voidaan käyttää myös EAP-TTLS:ää (EAP Tunneled TLS Authentication Protocol), jossa varmenteet sijaitsevat RADIUS-palvelimella. Se tunnistaa käyttäjän käyttäjätunnus- ja salasana -menetelmällä, jossa käyttäjätunnus salataan palvelimella olevalla varmenteella. Keskitetyn hallinnoinnin etuna ovat pienemmät hallinnointikustannukset käyttäjää kohden.

Palvelimen hyväksyessä saadut autentikointitiedot, se luo dynaamisen yhteysavaimen, jonka palvelin lähettää takaisin asiakkaalle langattoman liityntäpisteen kautta yhteyden hyväksyntäviestinä. Onnistuneen autentikoinnin jälkeen muodostetaan dynaaminen WEP-tunneli, jonka avulla voidaan aloittaa varsinainen dataliikenne.

4.5 PEAP

PEAP on avoin standardi, joka tukee laajasti 802.1X-tunnistautumista työasema- ja palvelinpuolella. TLS-kanavan ansiosta se tarjoaa päästä-päähän-suojauksen, jossa on mukana langaton yhteys tukiasemalle. TLS-kanava voidaan myös piilottaa PEAP:ssa ja data pystytään varmistamaan palvelimesta työasemalle molemminpuolisesti. PEAP tukee kaikenlaisia EAP-ratkaisuja, joissa autentikointi tapahtuu salasanapohjaisesti tai varmenteen avulla RADIUS-palvelimessa. PEAP ei tarvitse langattomille yhteyksille varmennetta, sillä vain tunnistautumispalvelimelle asennettu varmenne riittää.

PEAP:n (Protected Extensible Authentication Protocol) ensimmäisessä vaiheessa RADIUS-palvelin lähettää digitaalisen varmenteen asiakaskoneelle. Palvelimen osoittaessa luottamus pyynnön lähettävään asiakaskoneeseen, syntyy luottamussuhde laitteiden välille.

Toisessa vaiheessa asiakaskone lähettää oman autentikointitiedon RADIUS-palvelimelle. Autentikointitiedot voidaan välittää EAP–TLS:ssä, jossa käyttäjällä on oltava oma varmenne. EAP-TLS lisää hallinnointikuluja, sillä käyttäjien varmenteita hallinnoidaan, jaetaan ja peruutetaan käyttäjäkohtaisesti.

Microsoft suosittelee käyttämään turvallisuuden varmentamiseen EAP-TLS:ää, joka on tarkoitettu varmennepohjaisiin ympäristöihin sekä PEAP:a, joka on erittäin turvallinen ja joustava standardi tällä hetkellä. (Securing Wireless LANs with PEAP and Passwords 2007.) Microsoftin käyttöjärjestelmät tukevat 802.1X-kirjautumista ja uudet standardit toimivat viimeistään, kun on päivittänyt käyttöjärjestelmään uusimman Service Packin, joka sisältää monta pienempää päivitystä samassa paketissa.

4.6 LEAP

LEAP (Lightweight Extensible Authentication Protocol) on Ciscon kehittämä protokolla, joka kehitettiin samoihin aikoihin kun WPA. LEAP:n tarkoitus oli korjata WEP:n tietoturvaongelmia. LEAP käyttää kaksisuuntaista autentikointia ja dynaamisia WEP-avaimia. LEAP on vahva salausratkaisu. Tämä protokolla on standardisoimaton ja patentoitu Ciscolle.

LEAP ei tue TLS-suojausta, jolloin salasanat ovat helpommin luettavissa langattomaan verkkoon kirjautuessa. Se ei myöskään tue Single Logon – toimintoa, joka tarkoittaa kirjautumista monelle palvelulle automaattisesti kirjautumisen jälkeen. Windows Serveriin luotuja ryhmäkäytäntöjä sekä tietokoneen autentikointia palvelimelle ei voida käyttää PEAP:ssa. (Barken 2004, 69-76).

5 Palvelimet

Langattoman verkon rakentamiseen Windows-palvelinympäristössä tarvitaan kolme palvelinta, joihin on asennettu Windows Server 2008 Standard- tai Enterprise -versiot.

Palvelimiin asennetaan:

- AD DS (Active Directory Domain Services)
- CA (Certificate Authority)
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- NPS (Network Policy Server).

AD DS- ja DNS-palvelut voidaan asentaa samalle palvelimelle. Muut palvelut on suositeltavaa asentaa eri palvelimille, jotta vikatilanteissa moni verkon palvelu ei olisi pois käytöstä yhtä aikaa.

5.1 Active Directory

AD DS tarjoaa keskitetyn tietokannan hallinnoida tietoa verkon tarpeisiin. AD DS sisältää käyttäjätunnukset, tietokonetilit ja tiliin liittyvät ominaisuudet, jotka vaaditaan 802.1X- ja PEAP-tunnistukseen langattomissa verkoissa.

AD DS:ään pystytään määrittelemään ryhmiä, joihin voi lisätä käyttäjätunnuksia ja tietokonetilejä. Ryhmien avulla järjestelmänvalvonta helpottuu ja pääsy tiettyihin verkon resursseihin voidaan sallia tai kieltää tietyltä ryhmältä.

Group Policy Management (GPM) on ominaisuus, jolla pystytään määrittelemään ja vaihtamaan käyttäjä- ja tietokoneasetuksia. GPM:n avulla määritellään käyttäjille ja tietokoneille asetuksia, jotka voivat liittyä tietoturvallisuuteen, ohjelmisto-asennuksiin ja scripteihin.

Group Policy Object (GPO) sisältää Group Policyn määritteet, jotka voidaan siirtää käyttäjille ja tietokoneille AD DS:n avulla. Microsoft Management Console (MMC) on ohjelma, jonka avulla määritellään Group Policy – asetukset tietylle ryhmälle käyttäjiä tai tietokonetilejä.

5.2 DNS

DNS (Domain Name System) on nimipalvelu, joka muuttaa verkkotunnukset (domain) IP-osoitteiksi. Tietokoneet kommunikoivat keskenään numeeristen osoitteiden avulla ja nimipalvelun ansiosta voidaan käyttää helpommin muistettavia nimiä. Pienissä lähiverkoissa DNS-nimipalvelusta vastaa usein Internet-palveluntarjoaja, joka ylläpitää palvelimien nimipalvelutietoja ja niitä vastaavia IP-osoitteita.

Verkkotunnuksen osat erotetaan toisistaan pisteellä esimerkiksi yritys.fi. Ensimmäisen tason domain on juuri, joka on pelkkä piste. Juuresta seuraavan tason tunnus on ylätason verkkotunnus (Top-Level Domain). Verkkotunnuksen omistaja voi tehdä verkkotunnukselle aliverkkotunnuksia (subdomain), esimerkiksi dhcp.yritys.fi, jonka alla olevat verkkotunnukset ovat samassa verkossa olevien asiakaskoneiden tunnuksia.

Ylätason verkkotunnuksia ovat maa- ja yleisluontoiset tunnukset. Suomessa ylätason verkkotunnuksen ylläpitäjä on Viestintävirasto, joka hallinnoi maatunnusta .fi ja aliverkkotunnusta esimerkiksi yritys. Yleisluontoisia tunnuksia ovat esimerkiksi .com, .org ja .net, joita voi rekisteröidä eri palveluntarjoajien kautta ympäri maailman.

Windows Server 2008 Active Directory-hakemistopalveluun perustuvaan tietojärjestelmään siirryttäessä tulee tarpeelliseksi ottaa käyttöön oma DNS-palvelin. Sisäistä DNS-palvelua käytetään usein verkon asiakaskoneiden nimien selvitykseen ja ulkoista DNS-palvelua Internetiin näkyvien palvelimien nimien selvitykseen.

Tiedot on hyvä tallentaa usealle palvelimelle, joista ensisijainen nimipalvelin (primary name server) on tarkoitettu tietueiden syöttämistä ja muokkaamista varten. Ensisijaisen nimipalvelimen tiedot tallennetaan nimijakelussa toissijaisten nimipalvelimien (secondary name server) tietokantaan kopioina, joita ei voi muokata.

5.3 Varmenteet

Varmenne on luotettavan tahon digitaalisesti allekirjoittama asiakirja siitä, että tietty julkinen avain kuuluu tietylle avaimen käyttäjälle. Varmenteita käytetään henkilön tai laitteen identiteetin varmistamiseen, palvelun todentamiseen ja tiedoston salaamiseen.

Varmennekäytännön avulla henkilöt ja julkiset avaimet sidotaan toisiinsa. Varmenneviranomainen (Certificate Authority, CA) toimii julkisena notaarina, joka tarkistaa henkilön identiteetin ja myöntää nimetyn henkilön julkisen avaimen todentavan varmenteen. Varmenneviranomainen allekirjoittaa varmenteen omalla yksityisellä avaimellaan. Näin ollen sanoman vastaanottaja voi varmistaa lähettäjän henkilöllisyyden tulkitsemalla tiedot henkilön julkisella avaimella. (Holttinen, 2005.)

Julkisen avaimen lisäksi varmenne sisältää myös muita tietoja, kuten henkilön tai organisaation nimen, varmenteen myöntämispäivän, viimeisen voimassaolopäivän tai yksilöllisen sarjanumeron. Yksi yleisimmin käytetyistä varmennerakenteista on kuvattu ITU-T:n (International Telecommunication Union - Telecommunication Standardization Sector) suosituksessa X.509v3.
(http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/varmenne.html)

Varmenne lähetetään sitten keskeiseen tietovarastoon, joka sisältää voimassa olevia ja peruutettuja varmenteita koskevat luettelot (Certificates and Certificate Revocation List, CRL) Kuvan 4.21 kaaviossa on esitetty toiminnot, jotka on suoritettava, kun varmennetta käyttävä osapuoli lähettää sanoman vastaanottajalle. (Tietoturvasertifikaatti, s. 164)

Kuvio 1: Varmenteiden käyttöön liittyvät tapahtumat (Tietoturvasertifikaatti, s. 164)

Varmenneviranomainen voi olla oma palvelin tai sen voi tilata palveluna kolmannelta osapuolelta. Varmenneviranomainen otetaan käyttöön Windows Serverissä lisäämällä Active Directory Certificate Services (AD CS) –ominaisuus. Suomessa varmenteita tarjoaa esimerkiksi Sonera ja kansainvälisesti tunnettuja varmentajia ovat esimerkiksi Thawte, Verisign ja Entrust.

Omalle palvelimelle asennettu varmenne on edullisempi vaihtoehto, mutta kolmannen osapuolen kautta hankittuna varmenteen käyttöönotto ja ylläpito on vaivattomampaa isommassa

verkossa. Esimerkiksi Windows-käyttöjärjestelmät tukevat tunnettujen kolmannen osapuolien varmenteita, jolloin säästytään varmenteen manuaaliselta asennukselta.

Varmenteen avulla autentikointiin on vaihtoehtoina EAP ja PEAP. EAP:ssa voi määritellä autentikointityypiksi TLS (EAP-TLS) ja PEAP:ssa TLS (PEAP-TLS) ja MS-CHAP v2 (PEAP-MS-CHAP v2) Nämä vaihtoehdot käyttävät varmennetta palvelimen autentikointiin. Näiden tapojen varmennetta voidaan käyttää myös käyttäjän ja tietokoneen autentikointiin.

5.4 DHCP

DHCP:n (Dynamic Host Configuration Protocol) tehtävänä on jakaa IP-osoitteita verkon asiakaskoneille. DHCP:n avulla voidaan jakaa myös muita asetuksia, kuten oletusyhdyskäytävän (router) ja nimipalvelimen (name server) IP-osoitteet. DHCP-palvelimelle määritellään IP-osoiteavaruus, josta asiakaskone saa oman IP-osoitteen käyttöön ja annettu IP-osoite on voimassa ennalta määrätyn ajan riippuen käyttötarkoituksesta.

DHCP-palvelimelle määritellään jaettavat osoitealueet (Scope) kullekin reitittimen erottamalle aliverkolle. Osoitealuemäärityksen liitetään muut TCP/IP:n vaatimat asetukset (Options), joita halutaan jakaa asiakaskoneille. Jaettava osoitealue on määriteltävä yhtenäisenä ja sen pitää vastata reitittimeen kytketyn aliverkon maskia. Jos reitittimeen on esimerkiksi kytketty C-luokan osoitesarja, osoitealue on määriteltävä vastaamaan tätä sarjaa.

Jaettavat osoitteet määritellään osoitepoolina (Address Pool). Siihen kuuluvat osoitealueen vapaat IP-osoitteet, joita DHCP-palvelin voi jakaa asiakaskoneille. Kiinteät IP-osoitteet, jotka on varattu esimerkiksi palvelimille, määritellään pooliin kuulumattomaksi (Excluded Addresses). Osoitealueelle määritellään nimi, jolla se tallentuu DHCP-palvelun tietokantaan sekä määritellään osoitevuokrauksen kestoaika (Lease Duration).

Seuraavaksi määritellään mitä TCP/IP-asetuksia osoitealueen asiakaskoneille jaetaan. Määritys voidaan tehdä joko kaikkia osoitealueita koskevana määrityksenä tai asiakaskonekohtaisesti. Asiakaskone-kohtainen määritys vaatii IP-osoitteen liittämisen MAC-osoitteeseen. Globaalina määrityksenä voidaan määritellä DNS-järjestelmän tiedot, jotka ovat kaikkien aliverkkojen asiakaskoneille yhteisiä. Osoitealuekohtaisia määrityksiä ovat esimerkiksi oletusyhdyskäytävät (router) ja konekohtaisia asetuksia ovat esimerkiksi konenimet (host).

DHCP asennetaan Windows Server 2008- alustalle fyysisesti yhdelle palvelimelle. Tällä varmistetaan, että muiden verkon toimintojen ollessa pois päältä, ainakin DHCP-palvelin voi jakaa IP-osoitteita keskitetysti verkon asiakaskoneille. Windows Server 2008 tukee IPv6: ta (Internet Protocol version 6), sekä NAP: ia (Network Access Protection). IPv6:ssa käytetään 128-bittisiä

IP-osoitteita ja NAP vaatii asiakaskoneelta todistamaan järjestelmän kuntoisuuden ennen kuin se lähettää IP-osoitteen käytettäväksi.

5.5 NPS

NPS (Network Policy Server) sisältää kolme palvelua, joita voidaan käyttää langattoman verkon määrityksessä ja hallinnoinnissa:

- RADIUS (Remote Authentication Dial-In User Service)
- RADIUS proxy (Remote Authentication Dial-In User Service proxy)
- NAP (Network Access Protection)

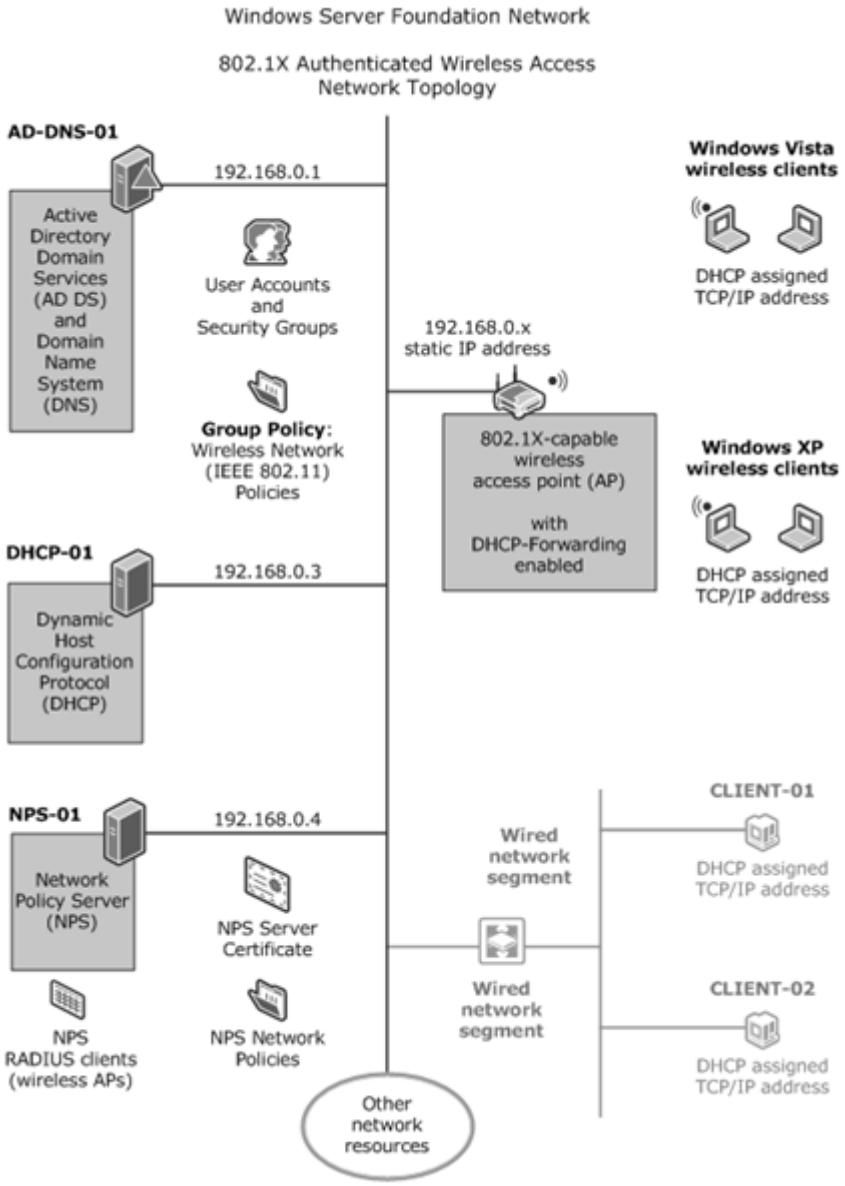
RADIUS (Remote Authentication Dial-in User Service) on yleinen tapa tunnistaa käyttäjät (Authentication) langattomassa verkossa. RADIUS-palvelimesta käytetään nimeä AAA (Authentication, Authorization ja Accounting) ja sen käyttäjähallinta hoidetaan keskitetysti. AAA:n avulla määritellään käyttäjien oikeudet verkon resursseihin (Authorization) ja sillä ylläpidetään verkonhallinnassa käytettyjä tietokantoja (Accounting).

NPS:n käyttö RADIUS proxynä siirtää autentikointi- ja tilastointiviestit muille RADIUS-palvelimille. NAP pitää huolen siitä, että verkkoon pyrkivässä asiakaskoneessa on esimerkiksi vaadittavat viruksentorjunta- ja palomuuriohjelmistot kunnossa sekä tarkistaa onko asiakaskoneen verkkoasetukset säännönmukaiset verkkoon pyrittäessä.

Langattoman tukiaseman SSID-nimi, IP-osoite ja salausavaimet määritellään NPS-palvelimen RADIUS-palveluun. Langaton tukiasema ja NPS-palvelin luo yhteyden toisiinsa ja suorittaa tarvittavat toimenpiteet autentikoinnissa riippuen millaista tunnistusta langattomassa verkossa käytetään asiakaskoneen ja NPS-palvelimen välillä. Langattomien tukiasemien tietojen keskittäminen yhteen palveluun helpottaa tukiasemien hallintaa.

6 Asennus

Asennusvaiheessa toteutettavan langattoman verkon topologia on infrastruktuurinen, jossa kaikki langattomat asiakaslaitteet liittyvät tukiasemiin. Tukiasemat liitetään lankaverkkoon, josta ne ovat yhteydessä palvelimiin. Palvelimiin asennetaan Windows Server 2008, jonka avulla on mahdollista luoda tietoturvallinen langaton verkko.



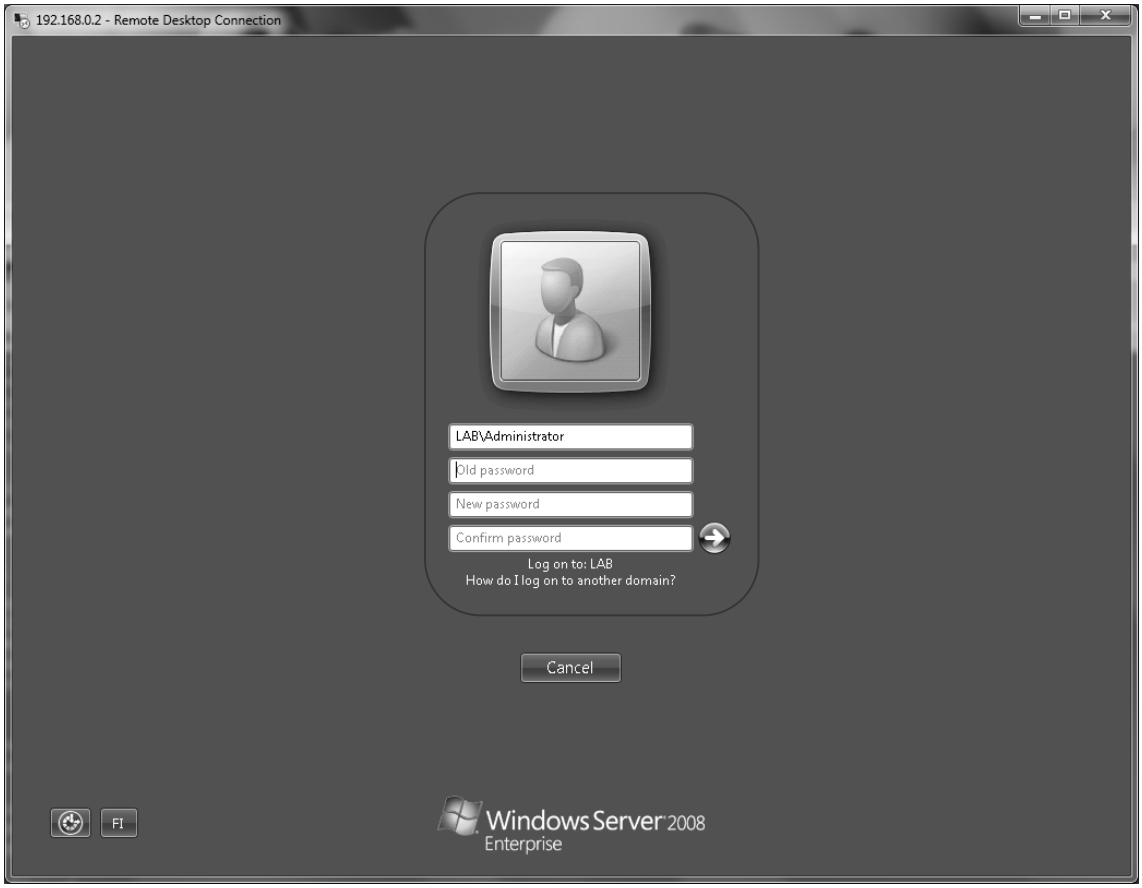
Kuvio 2: Langattoman verkon topologia (Foundation Network Companion Guide: Deploying 802.1X Authenticated Wireless Access with PEAP-MS-CHAP v2. Microsoft.)

6.1 Alkutoimenpiteet

Windows Server 2008 -asennuksen jälkeen kaikkiin palvelimiin määritetään:

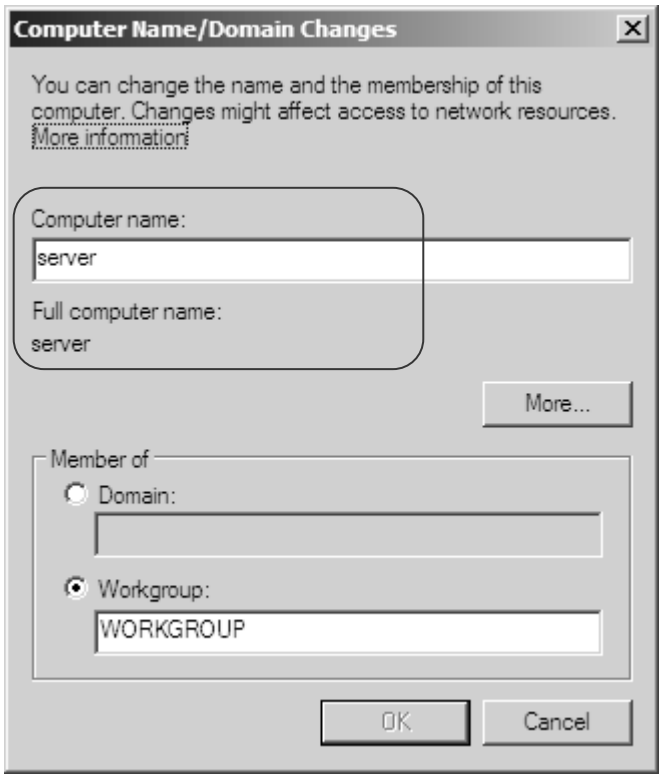
- järjestelmänvalvojan salasana
- tietokoneen nimi
- staattinen IP-osoite.

Järjestelmänvalvojan salasanan on oltava vähintään kuusi merkkiä pitkä ja sen pitää sisältää isoja (A-Z) ja pieniä (a-z) kirjaimia, sekä numeroita (0-9) ja erikoismerkkejä (!$#,%). Kirjautuneen käyttäjän salasana vaihdetaan painamalla Ctrl + Alt + Del tai Windows Etäyhteys-ohjelmalla Ctrl + Alt + End ja valitsemalla valikosta kohta Change a password.



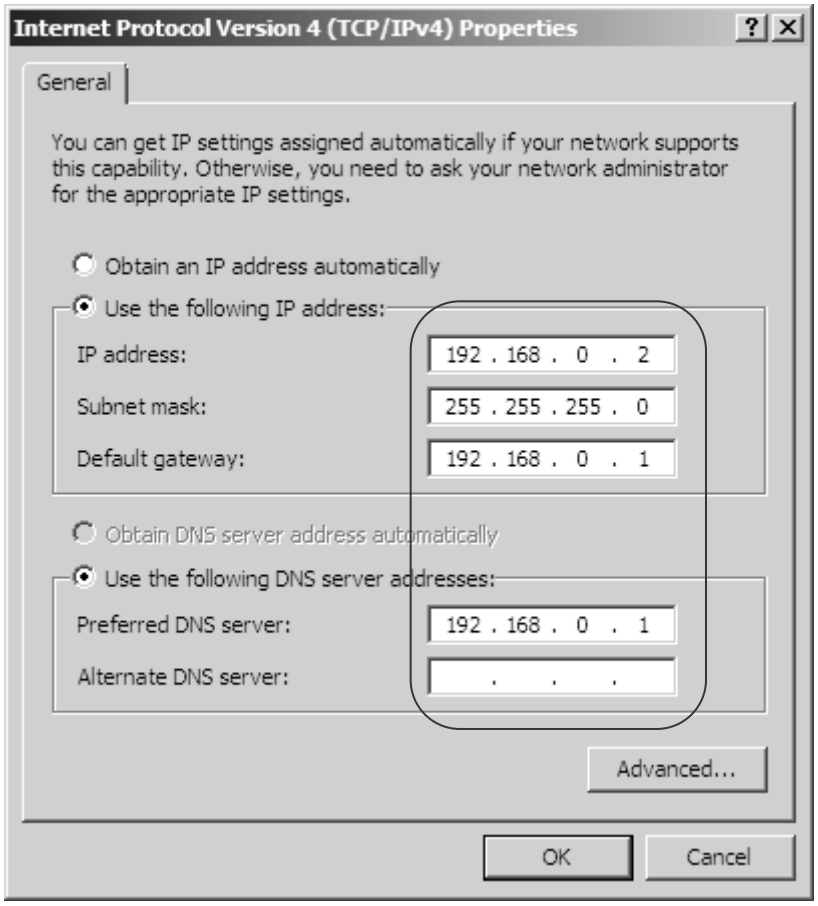
Kuvio 3: Järjestelmänvalvojan salasanan vaihto

Käyttöjärjestelmän asetuksista muutetaan tietokoneen nimi, jotta se on paremmin tunnistettavissa verkossa. Tietokoneen nimeä ei voi vaihtaa toiminimen asennuksen jälkeen.



Kuvio 4: Tietokoneen uudelleennimeäminen

IP-osoite muutetaan staattiseksi verkkokortin asetuksista. IP-osoite ja aliverkon peite ovat pakollisia muutettavia tietoja. Staattinen IP-osoite sopii hyvin palvelimelle, sillä se ei vaihdu jos DHCP on päällä.

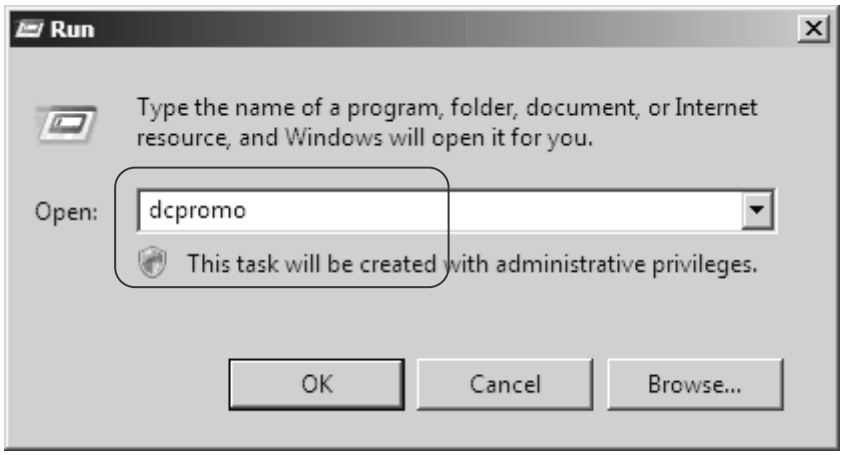


Kuvio 5: IP-osoitteen muuttaminen

6.2 Active Directory ja DNS

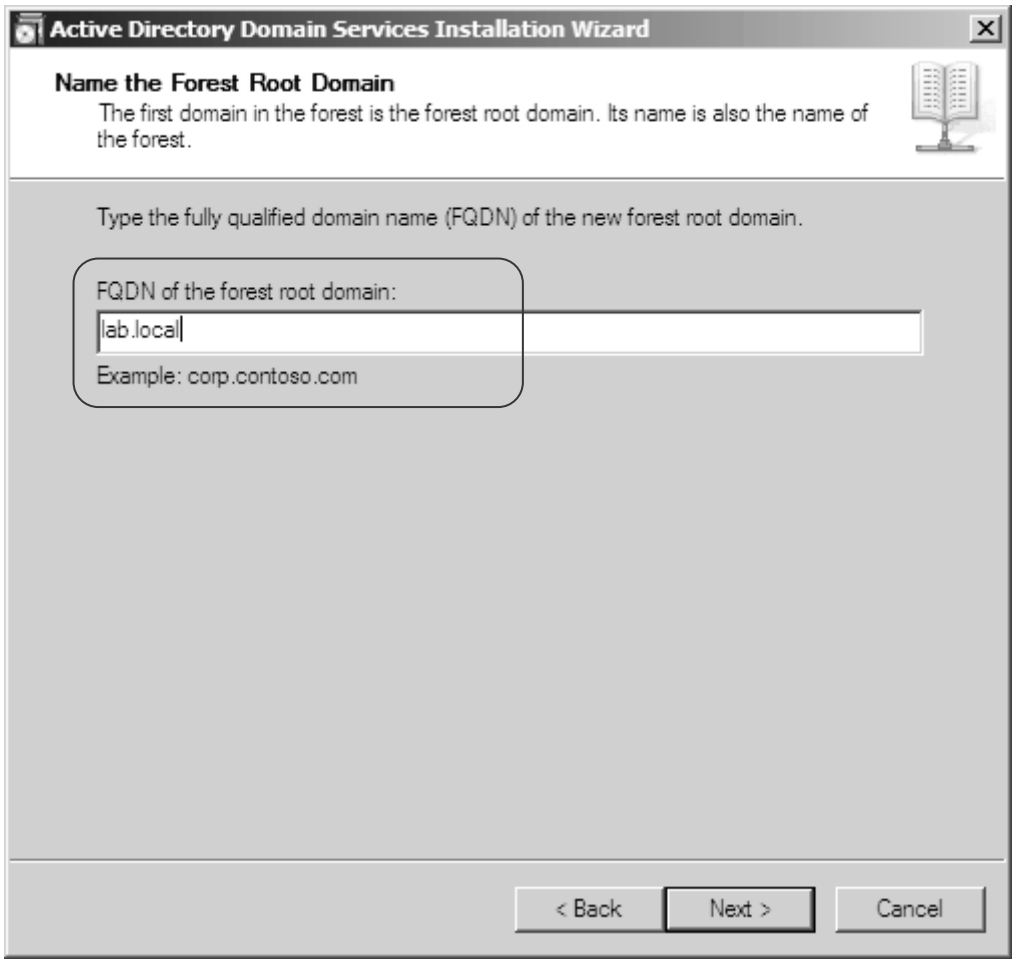
AD-DNS-01-palvelimelle asennetaan AD-, CA-, ja DNS-palvelu. Palvelimeen tarvitaan Windows Server 2008 Enterprise-versio, sillä se tukee automaattista varmenteiden latausta PEAP-TLS-autentikoinnissa käyttäjä- ja tietokonekohtaisesti. Automaattinen varmenteiden lataus helpottaa ottamaan varmenteita käyttöön. Se myös parantaa turvallisuutta automaattisesti uusiutuvien ja vanhentuneiden varmenteiden hallinnassa.

AD DS:n asennus aloitetaan antamalla palvelimelle komento ”dcpromo”. Komento käynnistää asennuksen, joka lataa tarvittavat tiedostot palvelimelle ja avaa graafisen asennusohjelman.



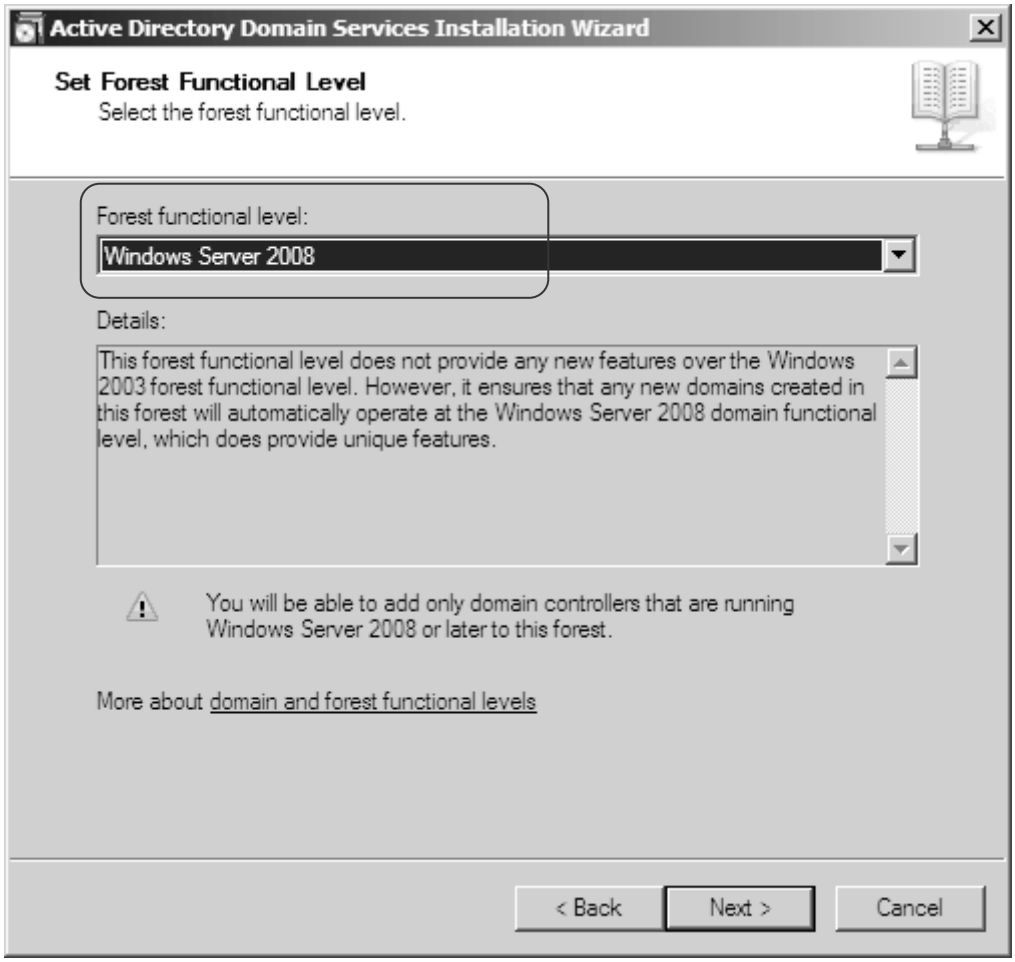
Kuvio 6: AD DS:n asennuksen aloitus

Asennuksen alkuvaiheessa määritellään verkkotunnus, johon langattoman verkon tietokoneet liittyvät myöhemmissä asennuksen vaiheissa.



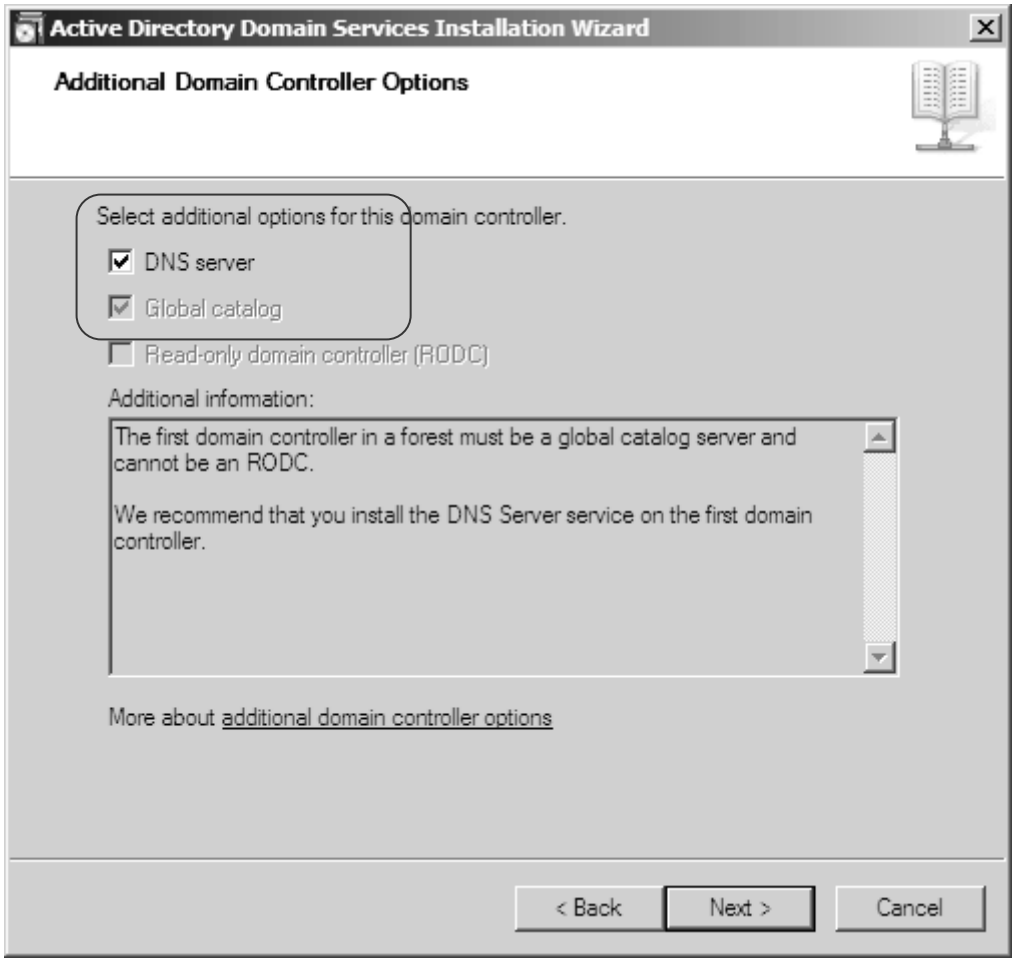
Kuvio 7: Toiminimen määrittäminen

Forest functional level määrittää mitä versioita Windows Server -palvelimesta voidaan lisätä samaan verkkotunnukseen. Jos käytössä ei ole muita versioita kuin Windows Server 2008, valitaan se tähän kohtaan.



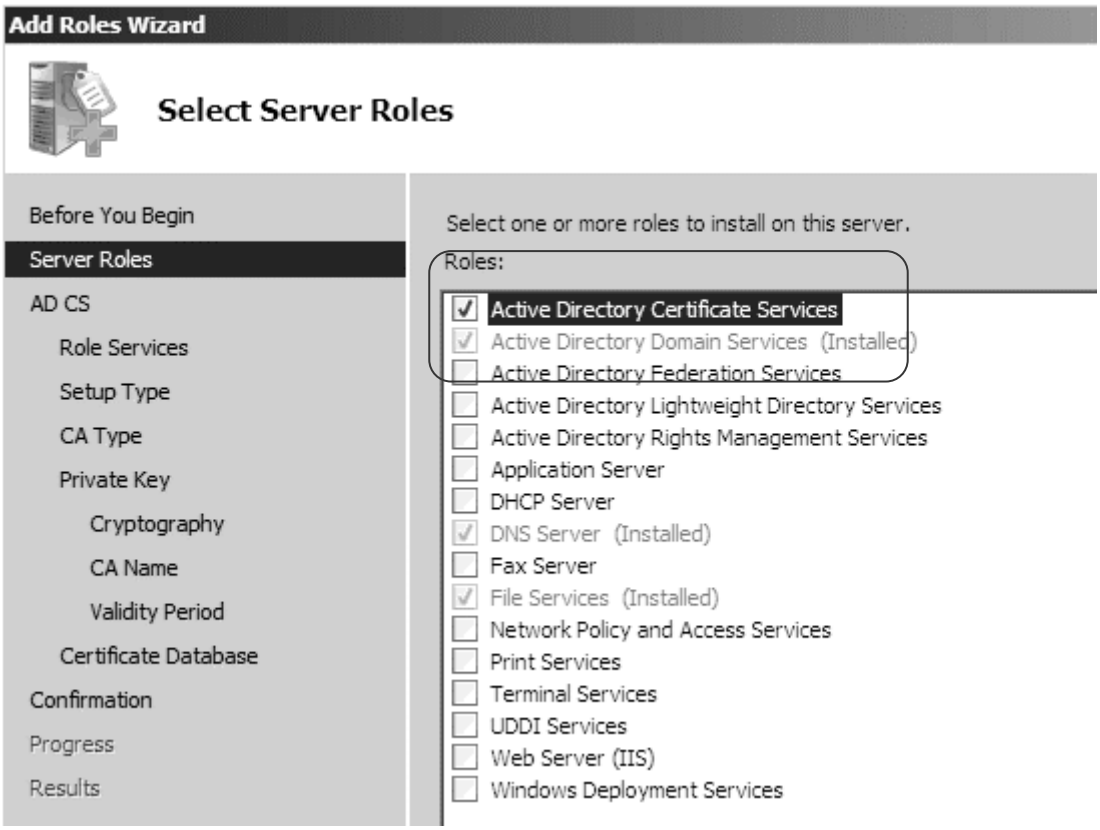
Kuvio 8: Forest functional level

Valinnaisista ominaisuuksista on valittavissa DNS, joka tässä vaiheessa voidaan asentaa samanaikaisesti AD:n kanssa. Suositus on, että DNS asennetaan tässä vaiheessa palvelimelle. Muuten se pitää asentaa myöhemmin manuaalisesti palvelimelle.



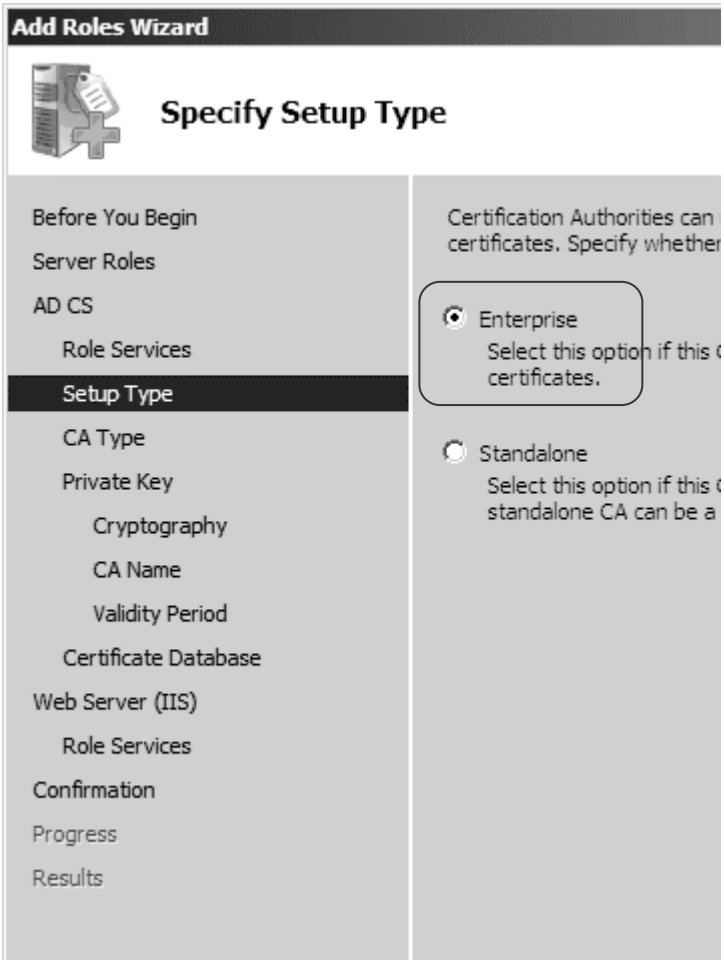
Kuvio 9: DNS-palvelun asennus

Varmennepalvelu asennetaan ”Add Roles Wizard” –toiminnon avulla, jonne pääsee Server Manager –ohjelman kautta Windows Server 2008 –versiossa.



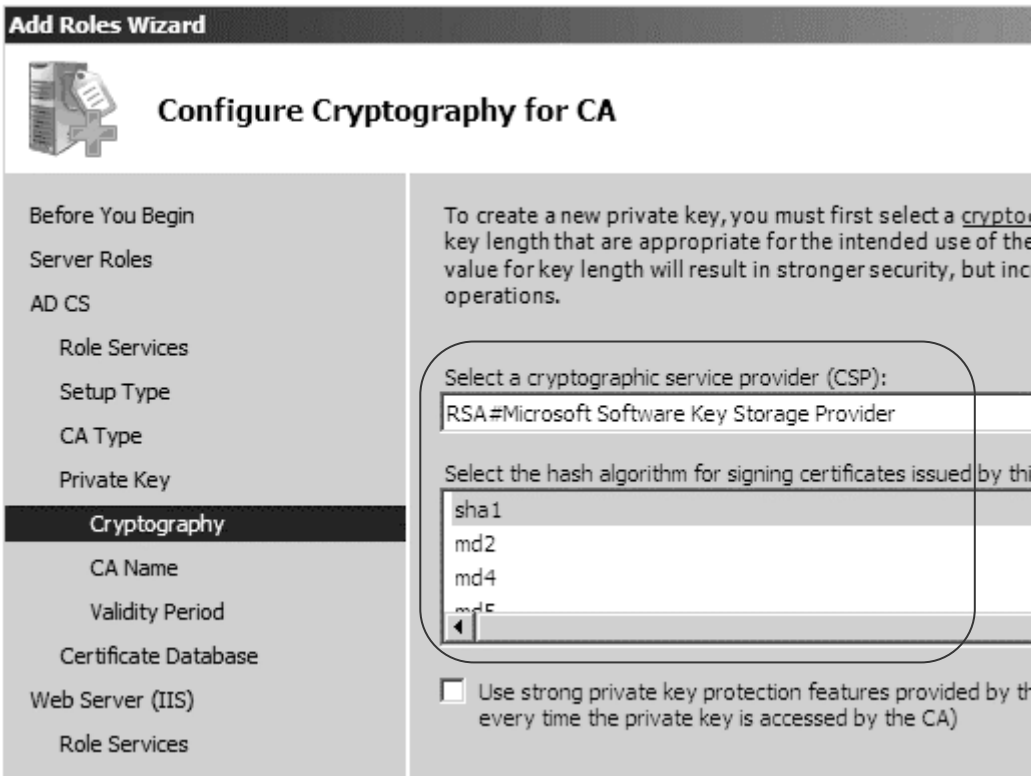
Kuvio 10: Varmennepalvelun lisäys

Varmennetyyppi, jonka nimi on ”Enterprise”, voidaan valita vain samassa versiossa. Se sisältää kattavat ominaisuudet hallita useita varmenteita eri palvelimilla.



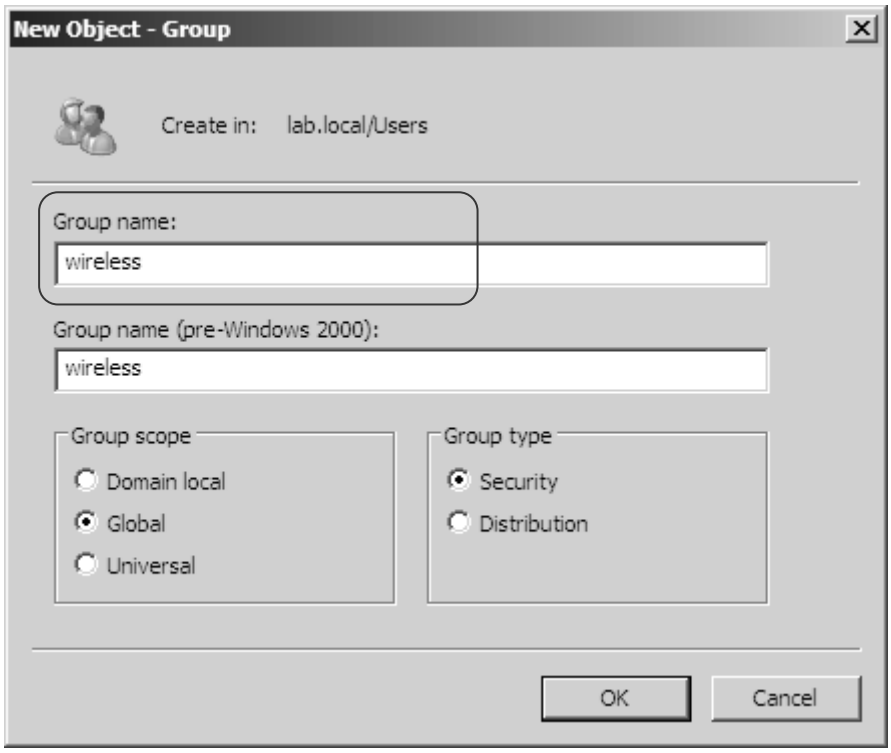
Kuvio 11: Varmennetyypin valinta

Microsoft Software Key Storage Provider (RSA), jonka avaimen pituus on 2048 bittiä ja SHA1 (Secure Hash Algorithm 1) algoritminä riittävät suojaamaan Root CA:n.



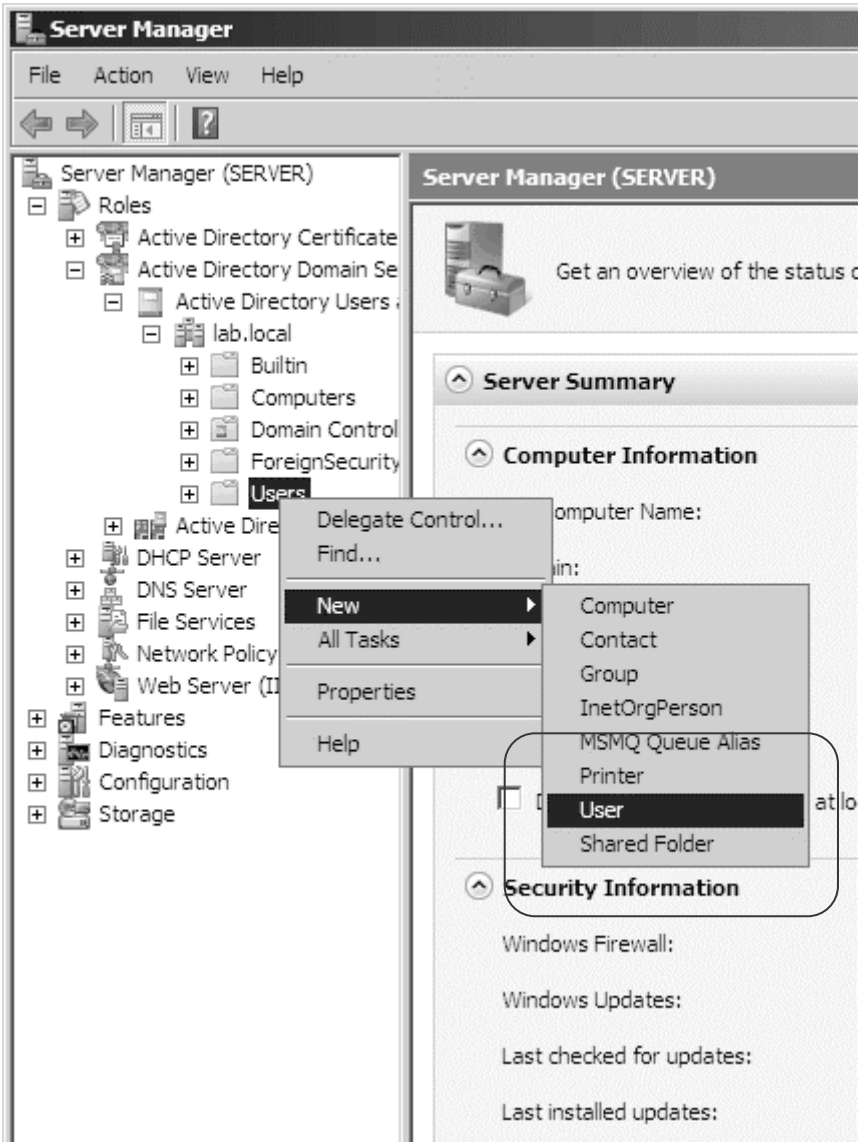
Kuvio 12: Varmenteen algoritmin valinta

AD:hen luodaan ryhmä, joka sisältää langattoman verkon käyttäjät ja tietokoneet. ”Group scope” on ”Global” ja ”Group type” on ”Security”.



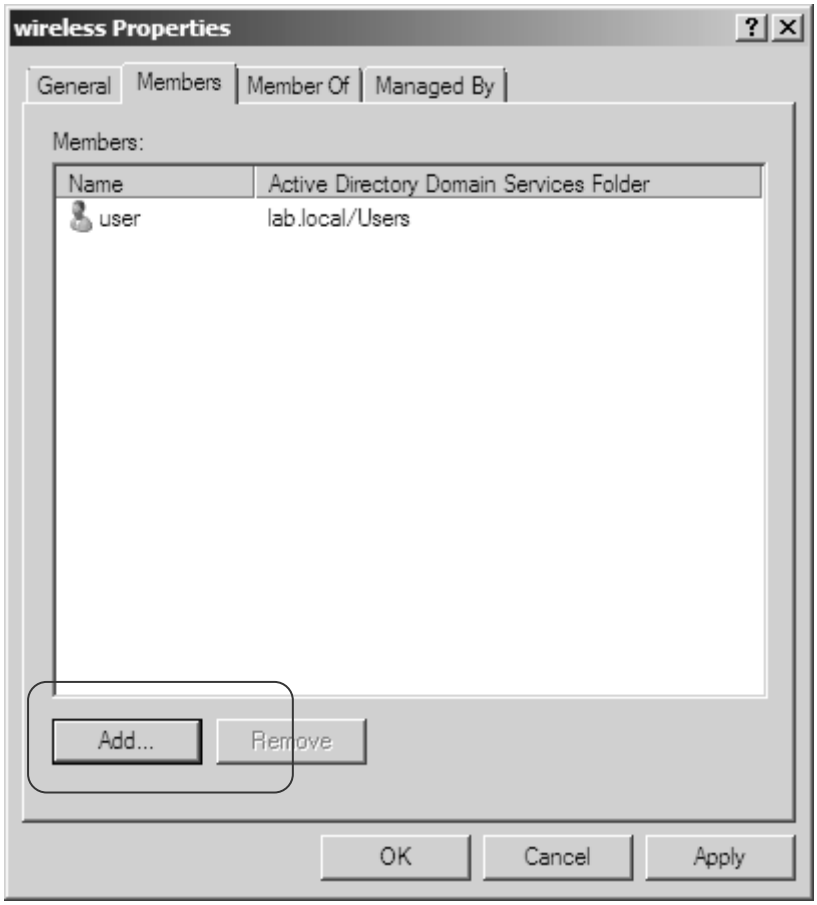
Kuvio 13: Ryhmän luonti langattomille käyttäjille

Käyttäjä lisätään AD:hen hallintapaneelin kautta. Myöhemmin samalle käyttäjälle annetaan oikeuksia palveluihin ja tarvittaessa muita lisämääritteitä.



Kuvio 14: Käyttäjän lisäys AD:hen

Luotuun ryhmään lisätään käyttäjät ja tietokoneet, joille halutaan antaa oikeus käyttää tämän ryhmän palveluita langattomassa verkossa. Tietokoneita voi lisätä ryhmään vasta kun ne on lisätty toiminimeen.

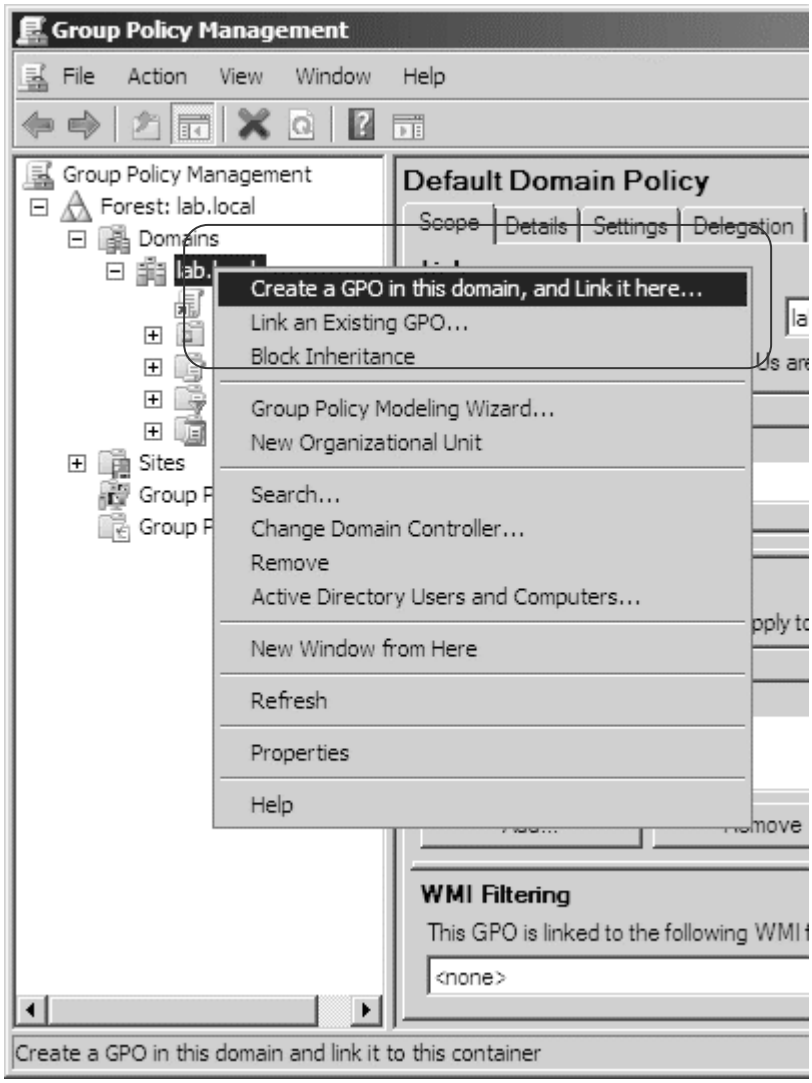


Kuvio 15: Käyttäjän lisäys langattomaan ryhmään

Kaikille toiminimessä oleville tietokoneille luodaan ryhmäkäytäntö, jonka avulla käyttäjä voi yhdistyä langattomaan verkkoon. Asetukset voidaan määritellä olemassa olevaan ryhmäkäytäntöön tai niille pystytään luomaan uusi ryhmäkäytäntö Group Policy Management –työkalulla (GPM).

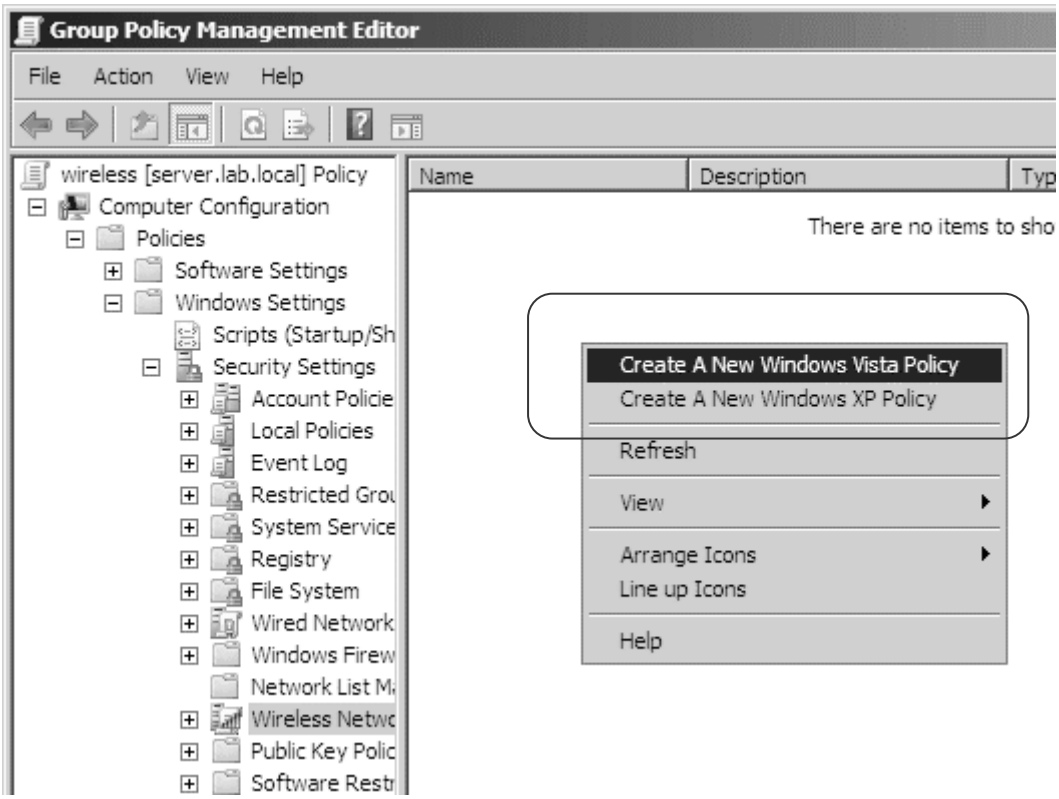
GPM:ssa voidaan määritellä varmenne latautumaan automaattisesti toiminimeen liitetylle asiakaskoneelle. Automaattisen varmenteen määrityksen jälkeen kaikki toiminimen tietokoneet saavat tietokonevarmenteen, kun Group Policy Object (GPO) on päivitetty palvelimelta. GPO:lle voidaan rajata käyttäjät ja asiakaskoneet, jotka saavat varmenteen.

Group Policy Management Editor –työkalulla (GPME) luodaan uusi käytäntö langattoman verkon tarpeisiin. Käytäntö tulee tietokoneen määrityksiin, joka latautuu automaattisesti käyttäjän kirjautuessa Windowsiin.



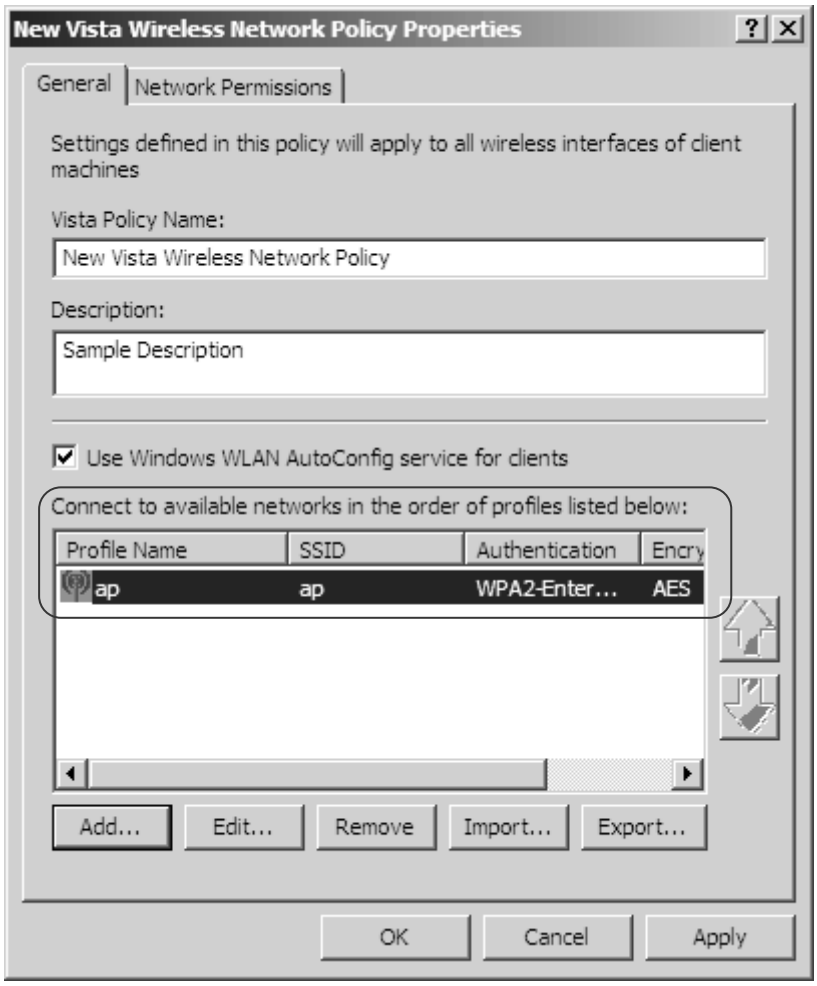
Kuvio 16: Uuden GPO:n lisäys GPM:n avulla

Valittavissa on käytäntö Windows XP:lle tai Vistalle. Windows XP:lle tarkoitettu käytäntö toimii myös tietokoneissa, joissa on Windows Vista, mutta rajoitetuin asetuksin. Windows Vistalle tarkoitettu käytäntö on tarkoitettu Windows Vistalle tai sitä uudemmille käyttöjärjestelmille.



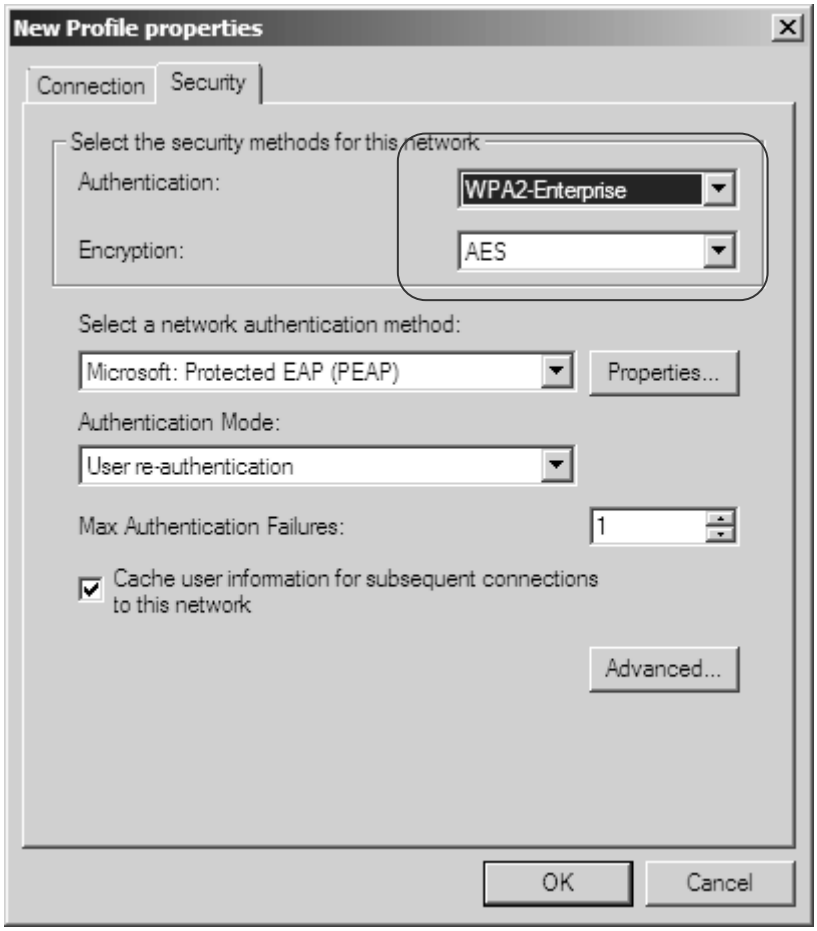
Kuvio 17: Uuden langattoman käytännön luominen GPME:n avulla

Uuden Windows Vista- käytännön profiiliin tallennetaan langattoman tukiaseman määritykset.



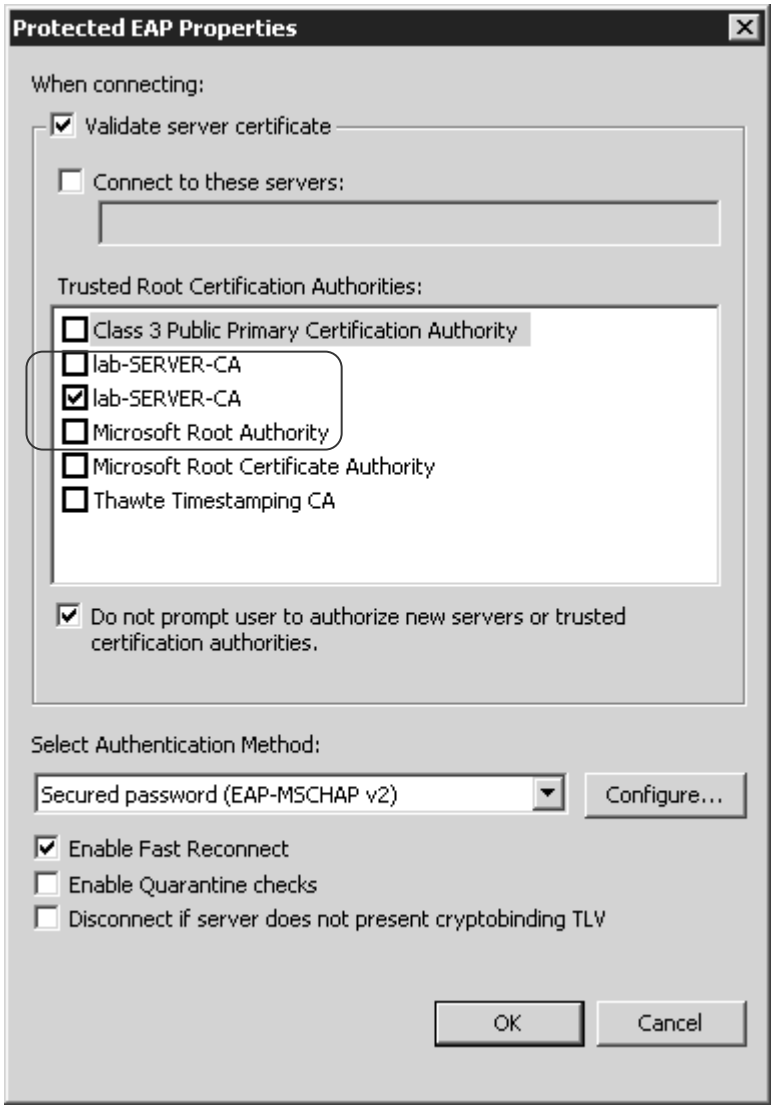
Kuvio 18: Uuden langattoman käytännön tukiaseman asetukset Vista-käyttöjärjestelmälle

Turvallisuus-välilehdeltä määritellään autentikoinniksi WPA2-Enterprise, salaukseksi AES ja langattoman verkon autentikointitavasta vastaa PEAP.



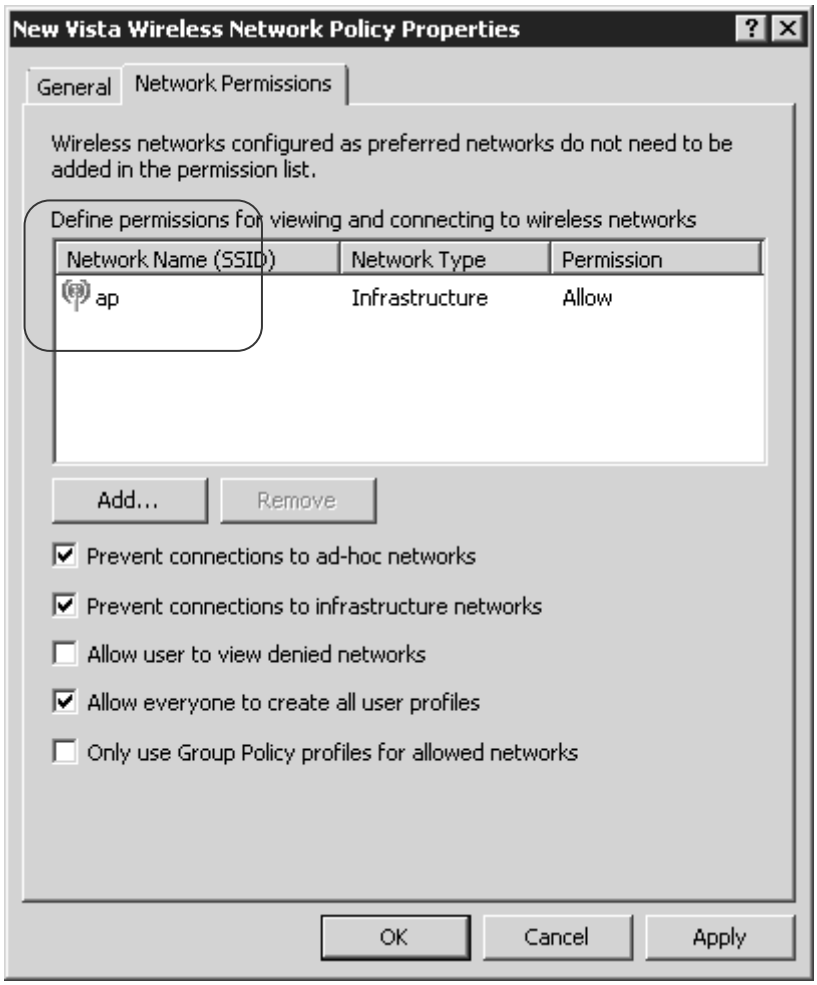
Kuvio 19: Uuden langattoman käytännön autentikoinnin ja suojauksen valinta

PEAP-asetuksista valitaan palvelimen varmenne varmentamaan langaton verkkoyhteys tietokoneelle. Tietoturvaa voidaan parantaa valitsemalla kohta ”Do not prompt user to authorize new servers or trusted certification authorities”, jossa määritellään käytettäväksi vain valittu varmenne, jota asiakaskone voi käyttää langattomaan yhteyteen.



Kuvio 20: Varmenteen valinta uuteen langattomaan käytäntöön

Langattoman verkon oikeuksia muihin tukiasemiin voidaan rajata Windows Vista -profiilissa lisäämällä SSID-tunnuksia ja antaa niille lupa tai kielto yhdistyä käyttäjän tietokoneessa.



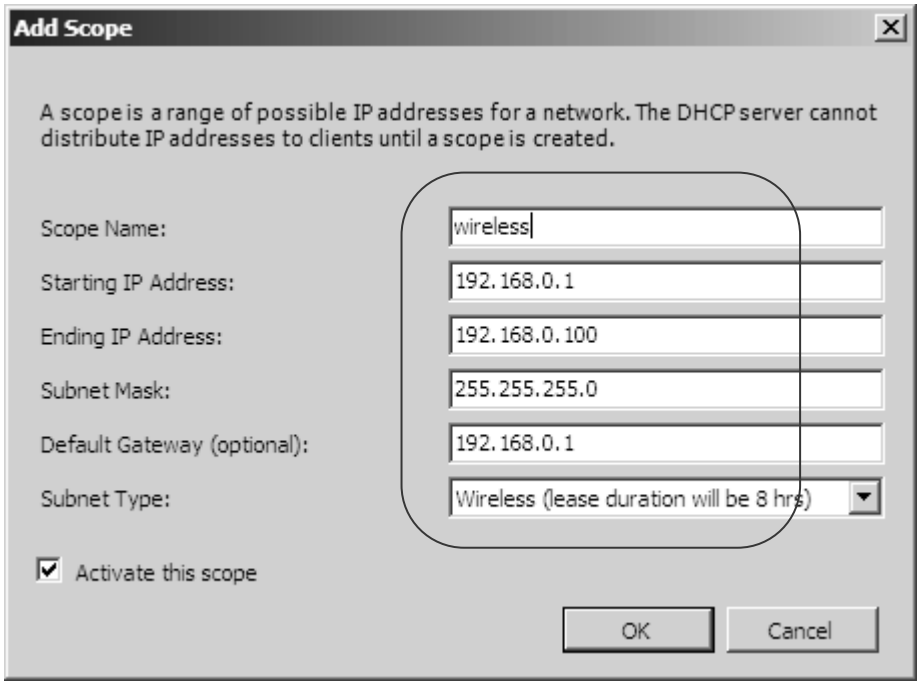
Kuvio 21: Tukiaseman oikeuksien määrittäminen uuteen langattomaan käytäntöön

6.3 DHCP

DHCP-palvelu asennetaan myös Add Roles Wizard- toiminnon avulla.

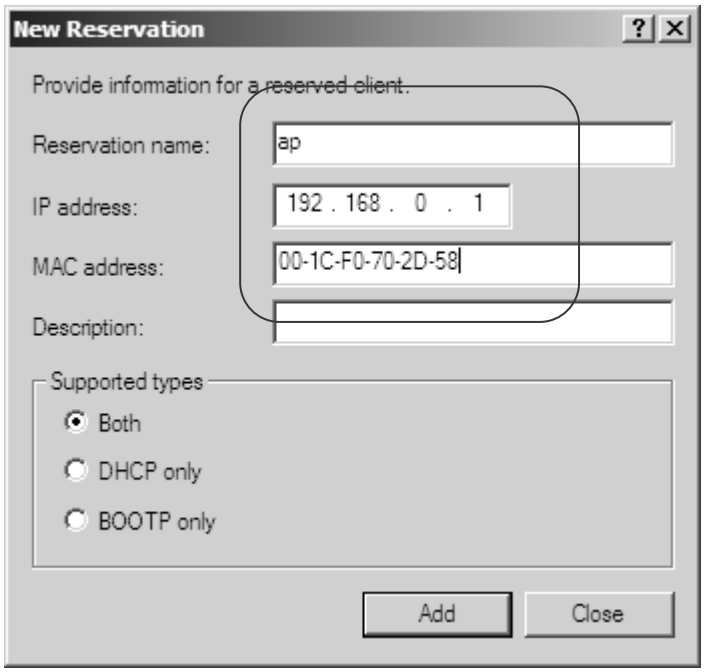
DHCP-asetuksiin määritellään:

- palvelimen IP-osoite
- toiminimi ja sen IP-osoite
- valinnaisen WINS-palvelun IP-osoitteet
- IP-osoiteavaruus langattomille yhteyksille
- valinnainen DHCPv6, joka tukee IPv6-osoitteita
- järjestelmänvalvojan oikeudet.



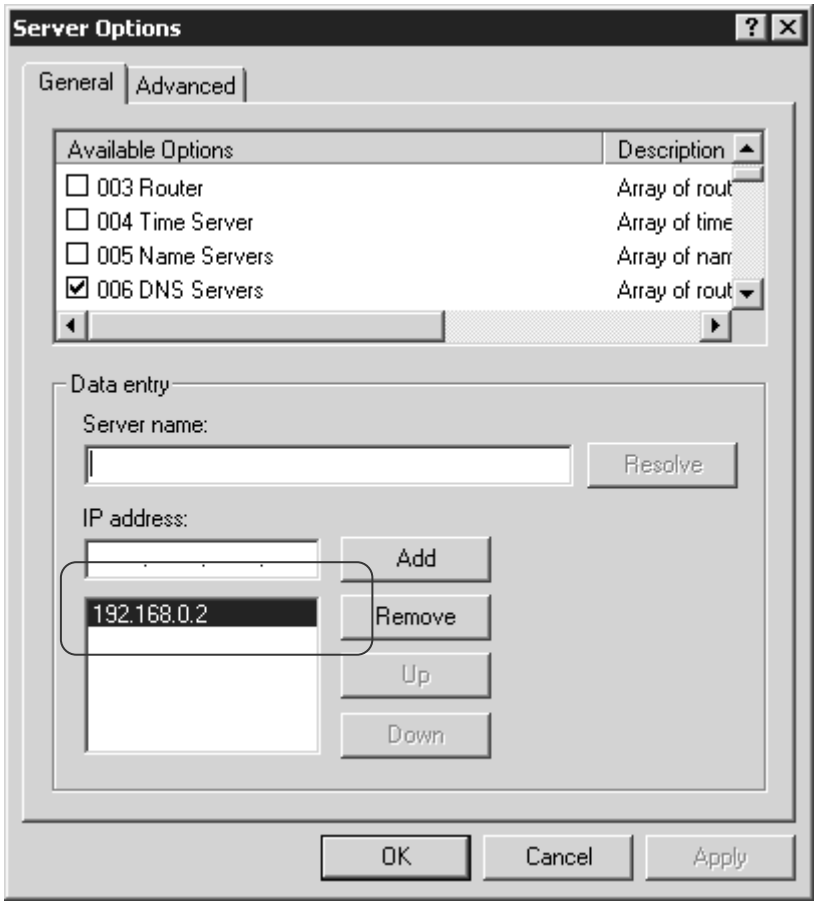
Kuvio 22: IP-osoite-avaruuden määrittäminen langattomille yhteyksille

DHCP-asetuksista voidaan määritellä varauksia tietokoneille, joille halutaan kiinteä IP-osoite. Tällaisia tietokoneita voi olla palvelimet, joiden IP-osoite ei saa muuttua.



Kuvio 23: Varauksen tekeminen DHCP:hen

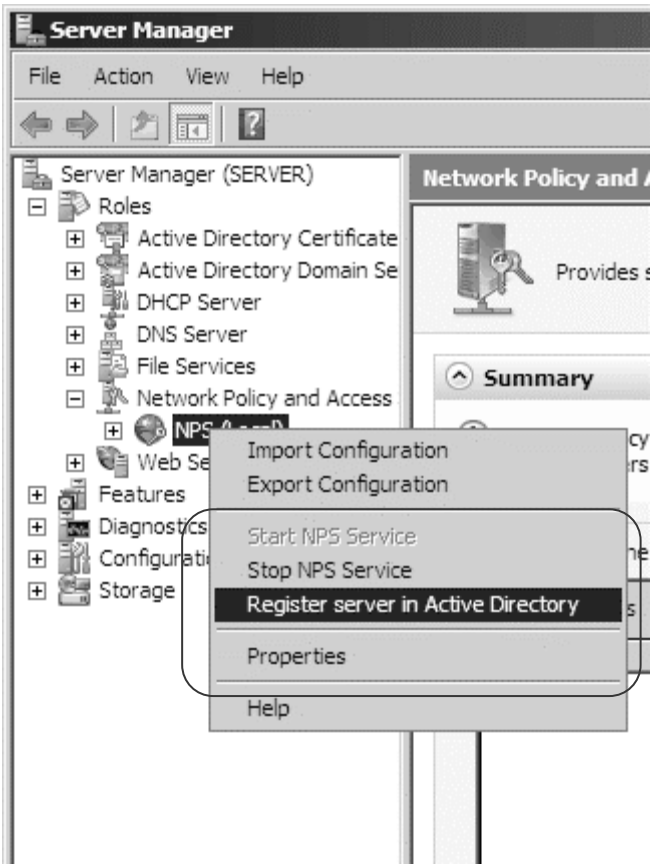
Kaikki määritykset, jotka asennuksen yhteydessä on tehty DHCP-palveluun, voidaan muuttaa myöhemmin. DHCP-palvelu voi välittää verkon tietokoneille reititin-, nimipalvelu- ja DNS-tiedot automaattisesti.



Kuvio 24: Valinnaisten asetuksien jakaminen DHCP:n avulla

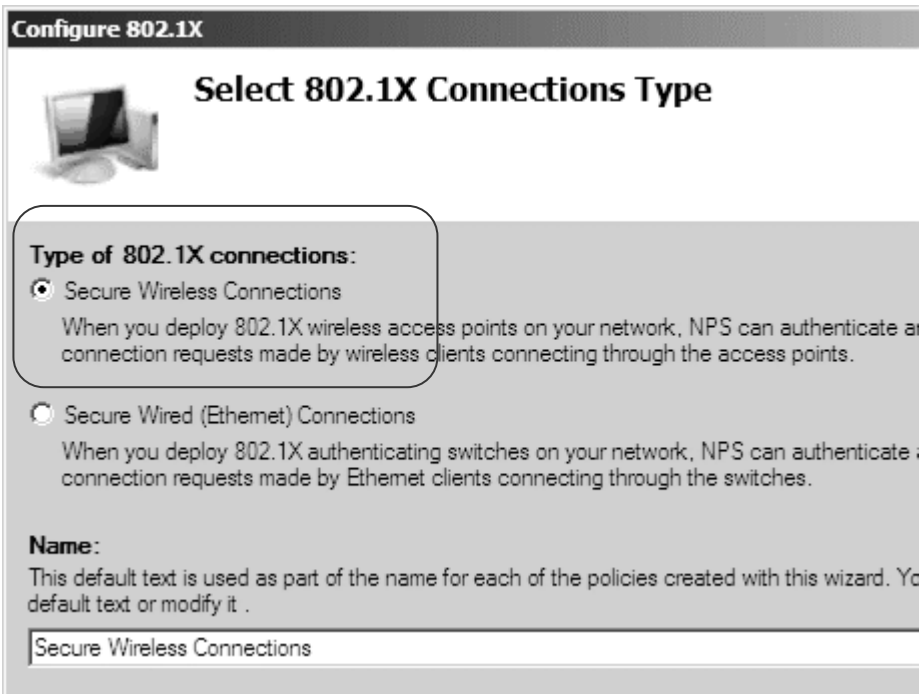
6.4 NPS

NPS käyttää AD:hen tallennettuja tietoja, kun käyttäjä tunnistautuu langattomaan verkkoon. Tämän takia NPS on liitettävä AD:hen NPS:n asetuksista.



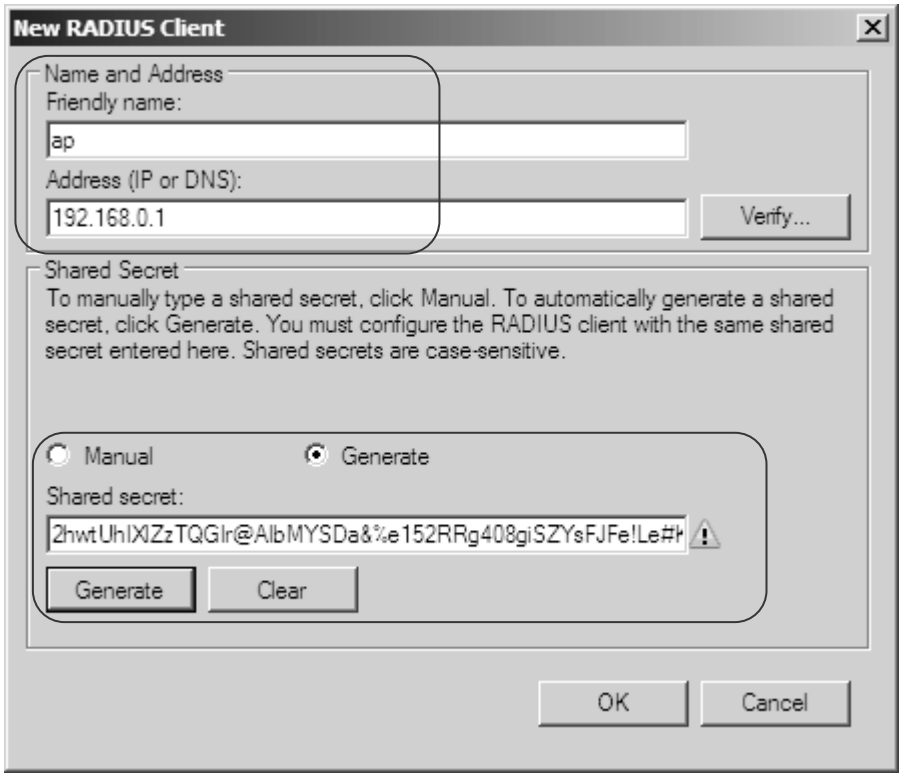
Kuvio 25: NPS-palvelun rekisteröinti AD:hen

NPS-palveluun määritetään menettelytapa, joka vaaditaan, kun 802.1X-tukiasemat yhdistyvät RADIUS-palvelimeen, joka tässä tapauksessa on NPS-palvelu.



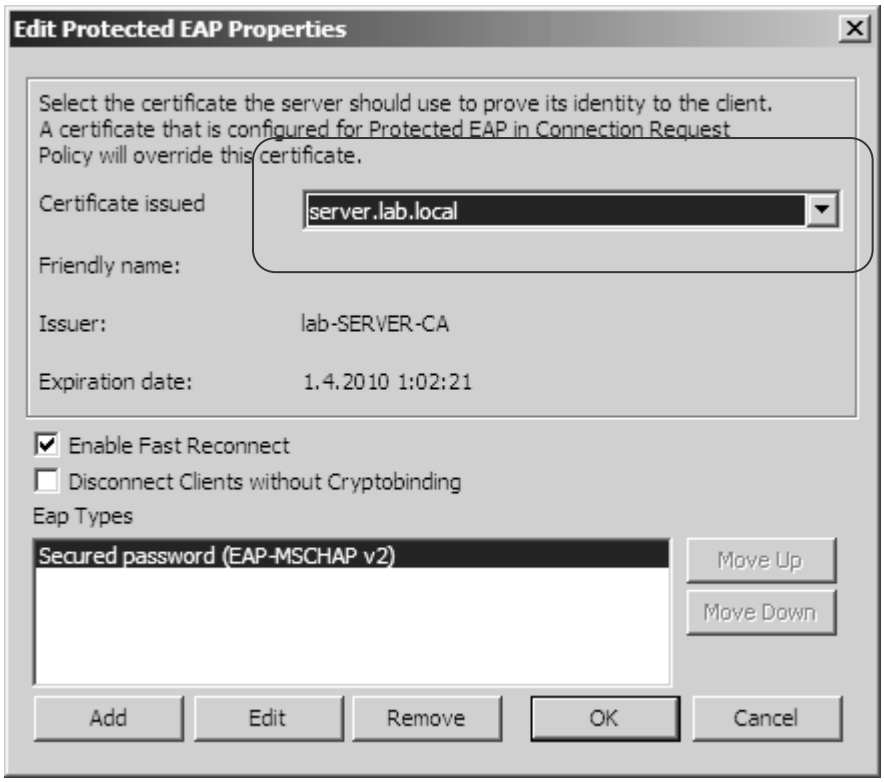
Kuvio 26: Langattoman yhteyden oikeuksien luominen

”New RADIUS Client” -kohdassa määritetään tukiaseman tiedot, joita ovat nimi, IP-osoite ja salasana. Nimi voi olla sama kuin tukiaseman SSID-tunnus ja ”Shared Secret” tarkoittaa salasanaa, joka määritellään samaksi tukiaseman määrityksiin. Se voidaan valita manuaalisesti tai generoimalla.



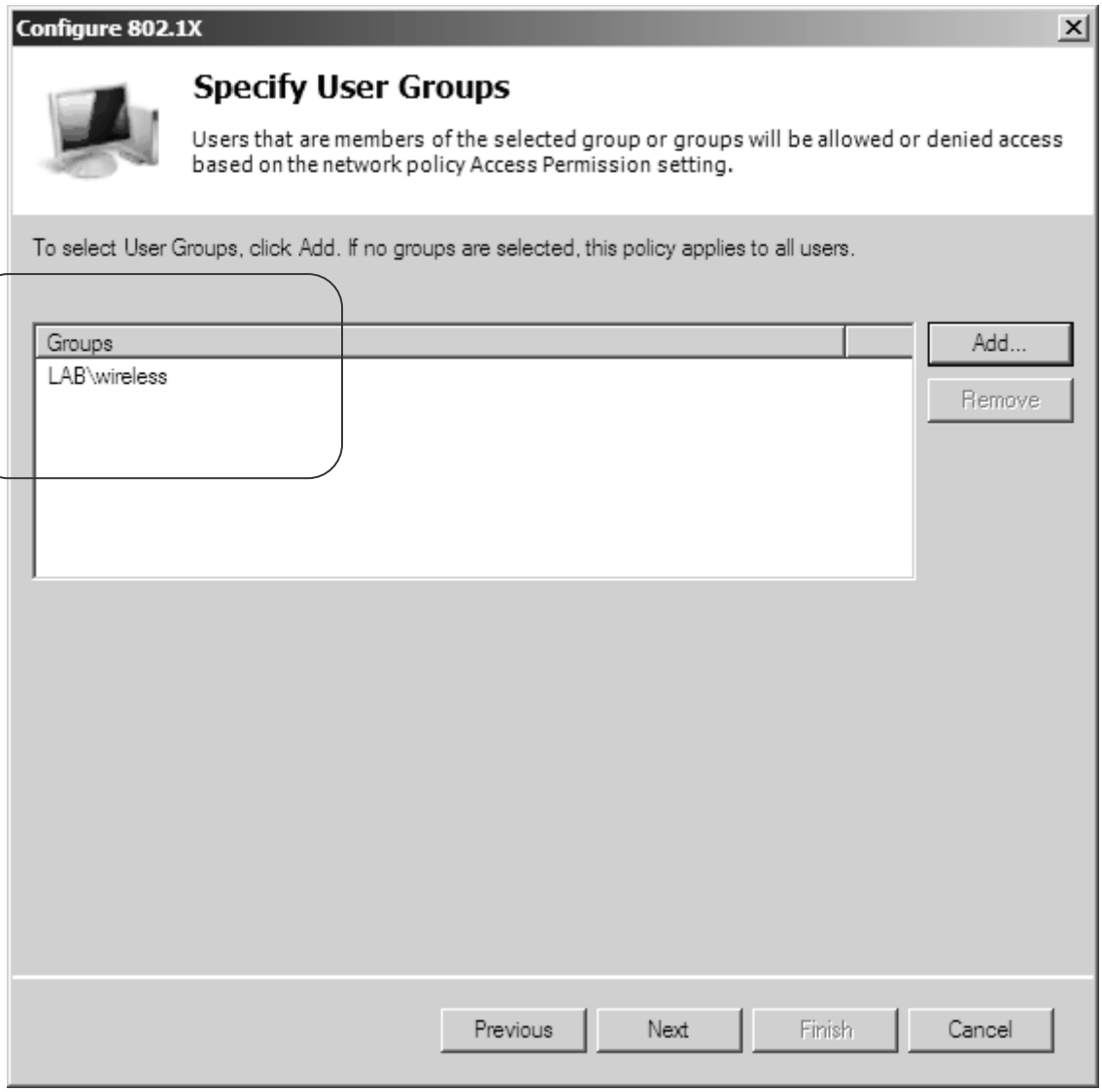
Kuvio 27: Tukiaseman tallentaminen NPS:ään

Autentikointitavan PEAP-määrityksissä varmistetaan, että käytetään oikeaa palvelimen varmennetta langattomalle yhteydelle.



Kuvio 28: Varmenteen varmistaminen NPS:ssä

Asetuksiin lisätään vielä ryhmä, joka luotiin langattomille käyttäjille. Ainoastaan tämän ryhmän käyttäjille on oikeus kirjautua verkkoon langattomasti.



Kuvio 29: Oikeuksien antaminen ryhmälle NPS:ssä

6.5 Tukiasemat

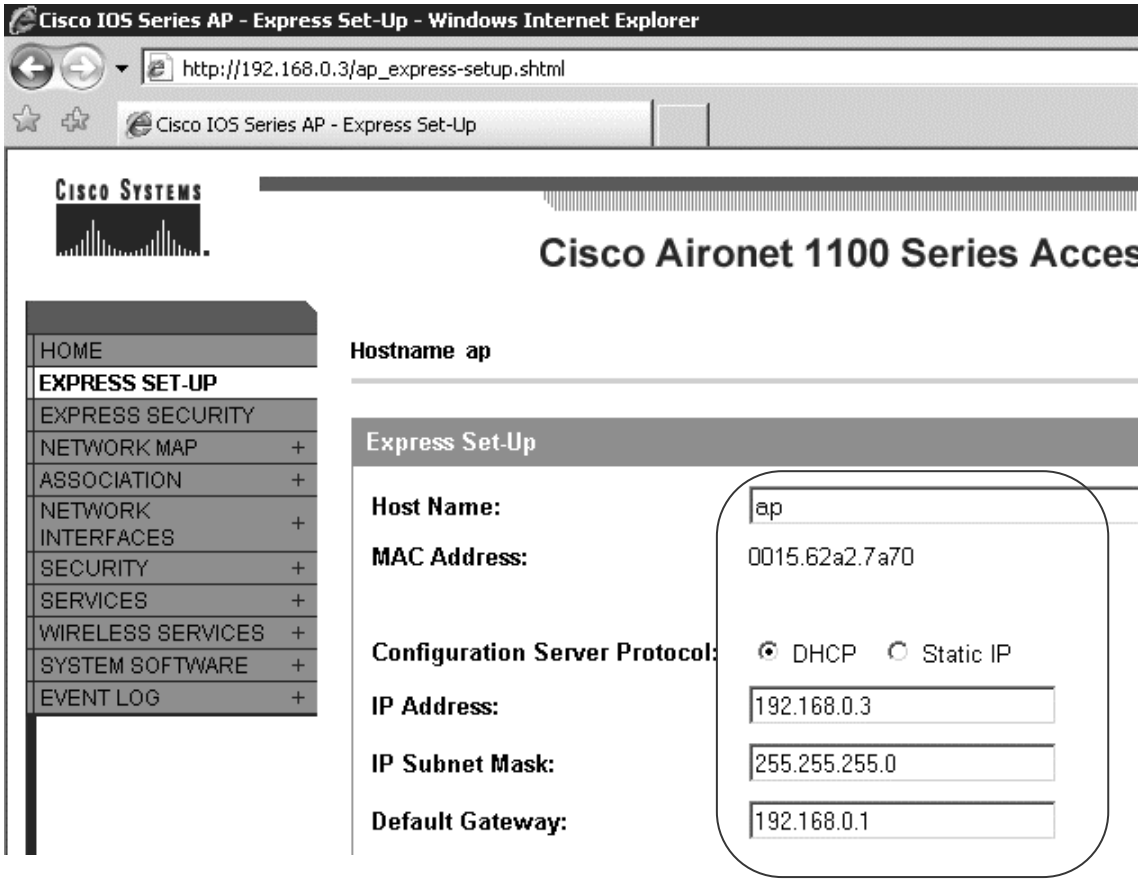
WLAN-tukiaseman määritykset tehdään Cisco Aironet 1100 –sarjan laitteeseen, joka tukee WPA2, AES ja RADIUS-standardeja. Asetukset tehdään käyttäen graafista käyttöliittymää. Ciscon laitteisiin on mahdollista tehdä asetukset myös komentorivin avulla (Cisco IOS).

Kuvio: Cisco Aironet 1100 –sarjan WLAN-tukiasema (Cisco Aironet 1100 Series Access Point Data Sheet. Cisco)

Tukiasemaan määritellään:

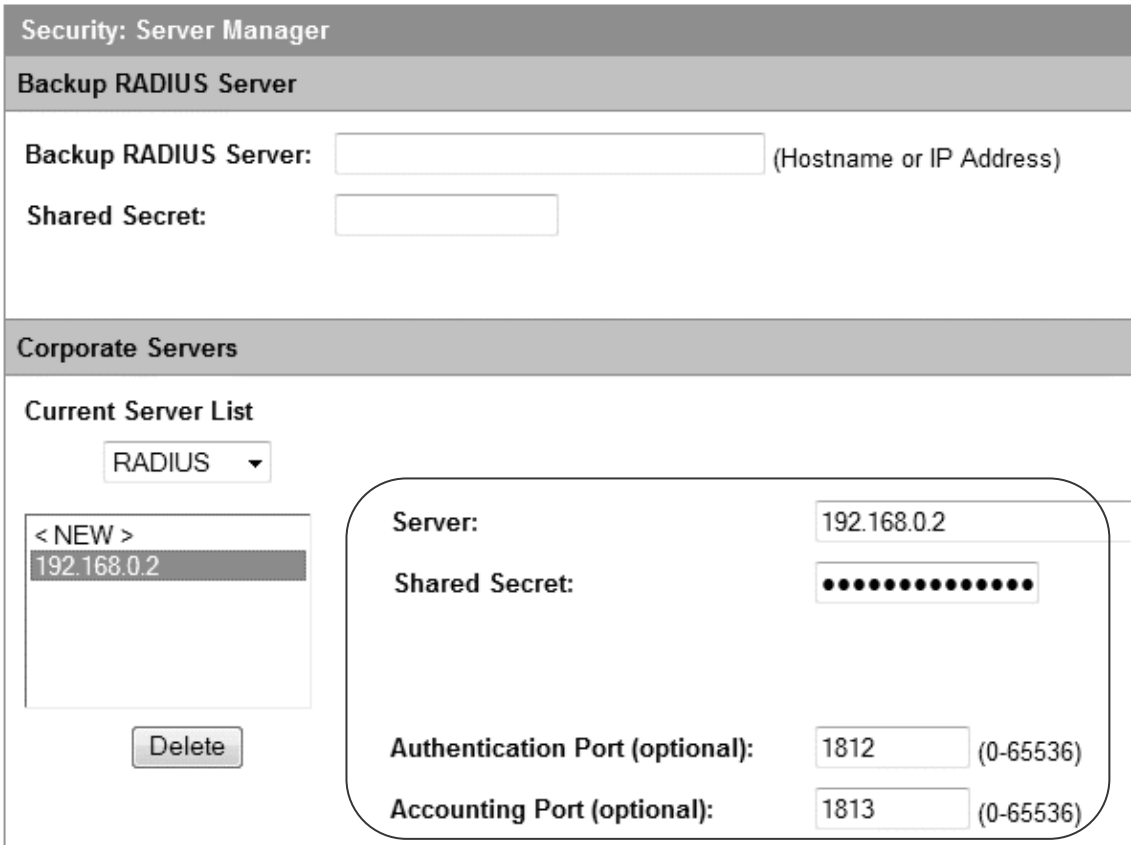
- SSID-tunnus, joka on 1-32-merkkinen
- tunnistusmenetelmä ja avaimet
- käytetty kanava taajuutena tai kanavanumerona
- 802.1X-tunnistusprotokolla ja EAP-määritteet
- SSID-tunnuksen käyttö majakkasanomassa
- tunnuksettomien liittymispyyntöjen hyväksyminen
- mahdollinen VLAN-tunniste SSID-tunnukselle.

”Express set-up” -valikosta määritellään seuraavat asetukset: tukiaseman nimi, IP-osoite, aliverkon peite ja oletusyhdyskäytävä. IP-osoite voi olla DHCP-palvelun kautta saatu tai manuaalisesti määritetty staattinen IP-osoite. Aliverkon peite määräytyy verkon mukaan ja oletusyhteyskäytävä on tässä tapauksessa reitittimen IP-osoite.



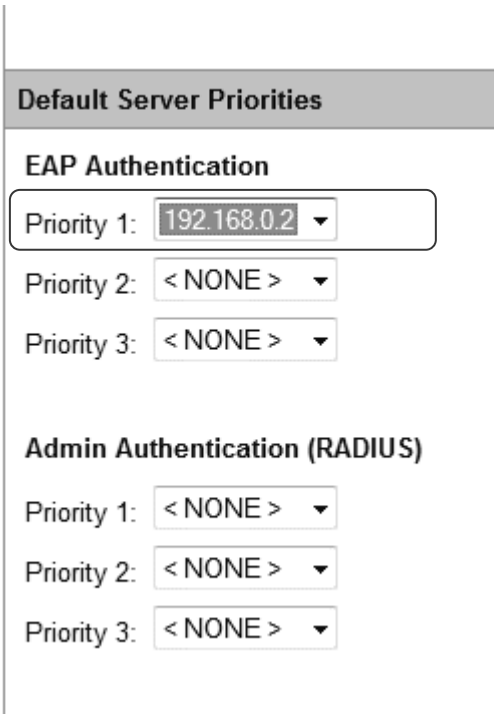
Kuvio 30: Tukiaseman IP-osoitteen määrittäminen

Seuraavaksi määritetään RADIUS-palvelimen IP-osoite, jaettu avain sekä tunnistautumis- ja tilastointiportti. Jaettu avain on luotu RADIUS-palvelimessa automaattisesti tai manuaalisesti. Porttiasetukset ovat oletuksena Windows Serverissä 1812 ja 1813. Portit voidaan muuttaa palvelimelta, mutta silloin on avattava palomuurista kyseiset portit, jotta RADIUS toimisi.



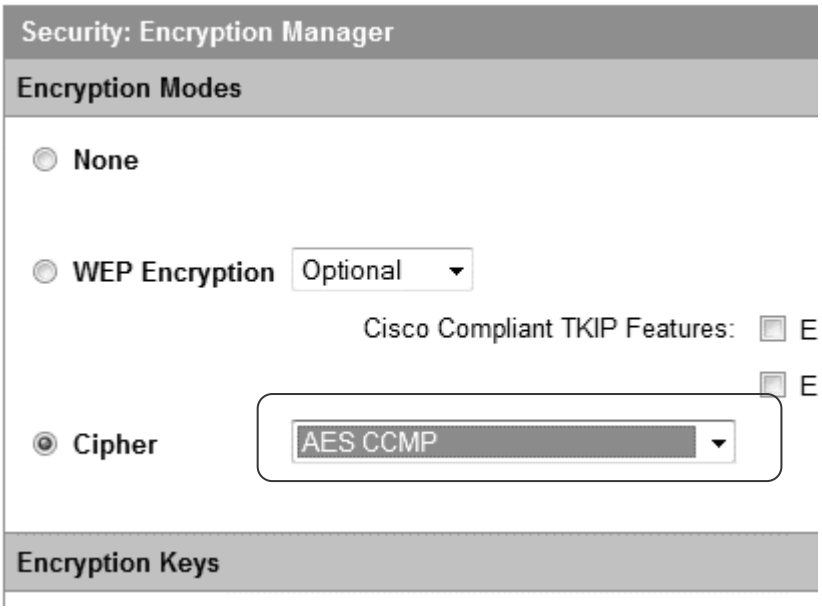
Kuvio 31: RADIUS-palvelimen määrittäminen

Tunnistautuminen tapahtuu EAP:n avulla. Tämä toiminto on määriteltävä myös WLAN-tukiaseman tietoihin. Tietoihin lisätään IP-osoite, jonne RADIUS-palvelin on asennettu.



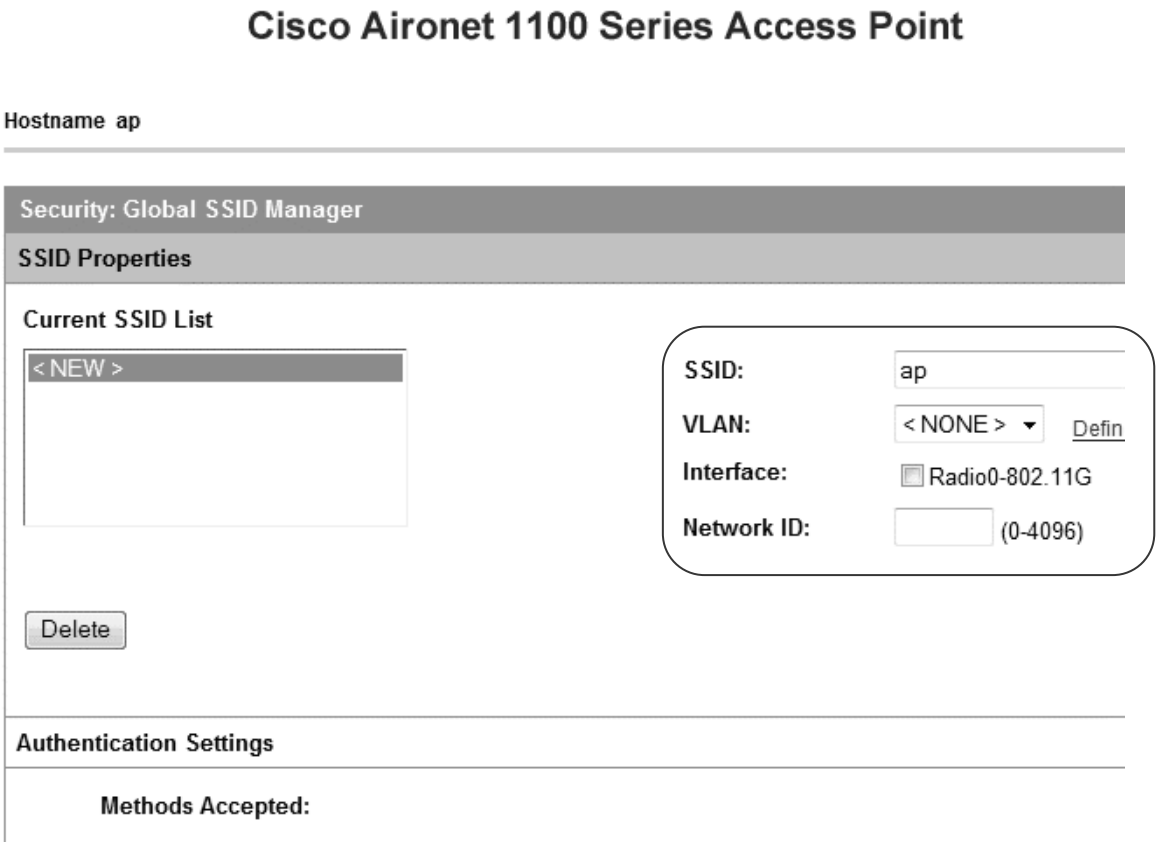
Kuvio 32: NPS-palvelimen valinta EAP-autentikointiin

Salaukseksi vahvistetaan ”AES CCMP”, joka tarkoittaa WPA2:n AES-salausta. Vaihtoehto tarjoaa erittäin vahvan suojauksen langattomiin verkkoihin.



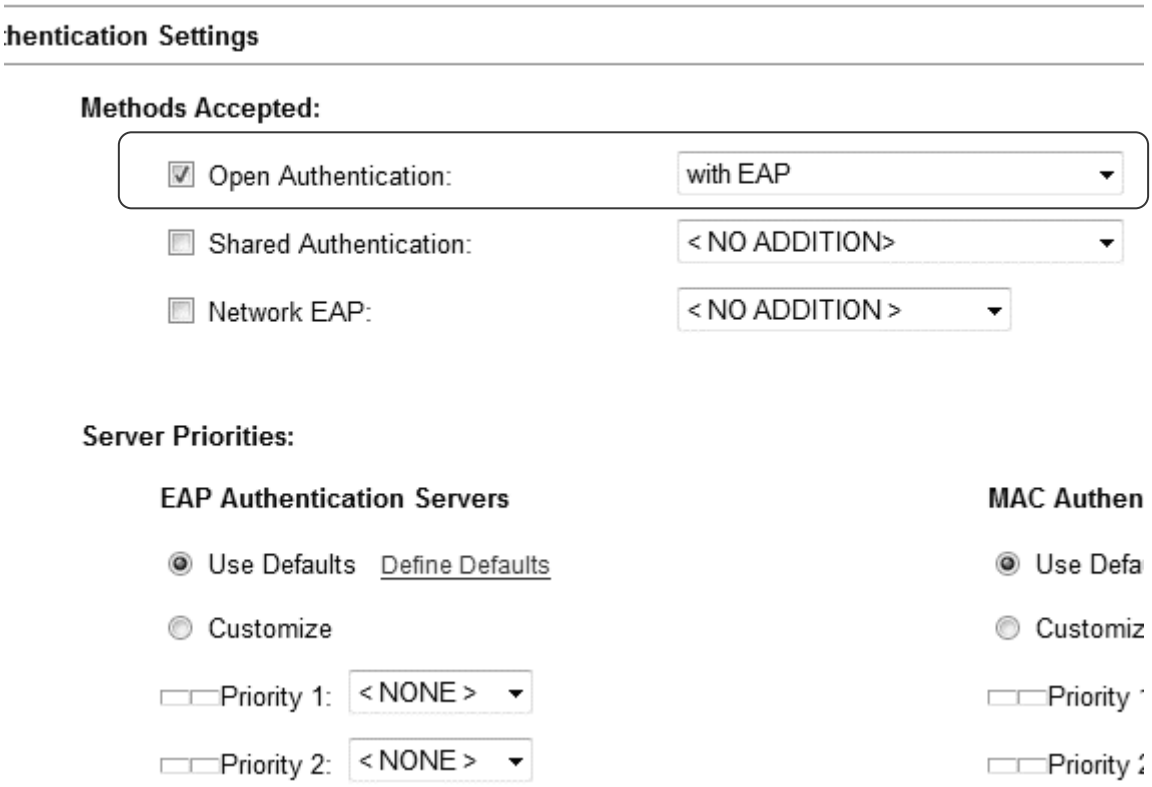
Kuvio 33: AES-salauksen määrittäminen

WLAN-tukiaseman SSID-tunnus näkyy kaikille, jotka ovat langattoman verkon peittoalueella. SSID:lle tunnistetaan langaton verkko, jota halutaan käyttää. SSID voidaan myös piilottaa, mutta se ei ole varsinainen suojauskeino.



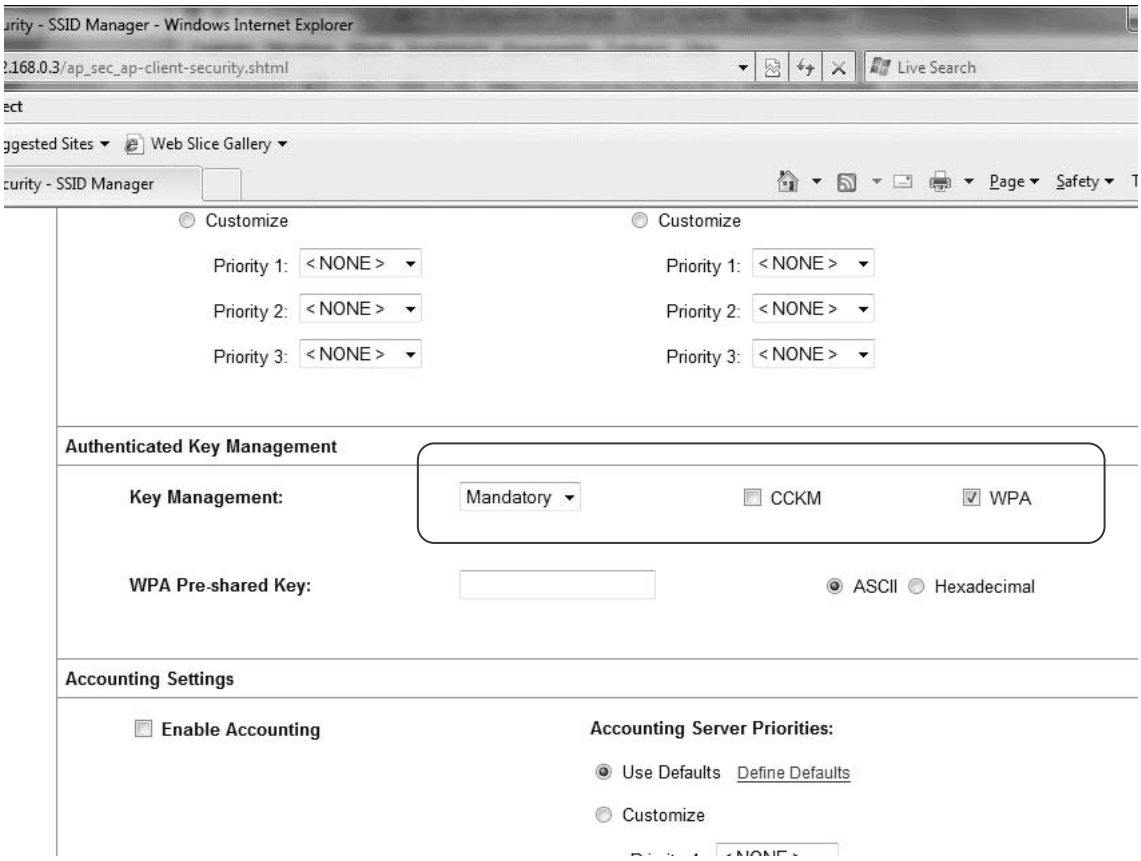
Kuvio 34: Tukiaseman SSID:n lisääminen

Tunnistautumistavaksi valitaan EAP, joka on avoin tunnistautumistapa. Se sopii tunnistukseen, josta on vastuussa Windows Serverille asennettu palvelu. Cisco Aironet 1100 –sarjan laite tukee Ciscon kehittämää tunnistautumistapaa, joka voidaan tähän kohtaan määritellä.



Kuvio 35: EAP-tunnistautumismenetelmän valinta

Avaintenhallinta tapahtuu WPA:n avulla. Aiemmin määritetty asetus vahvisti WPA2:n käytön, joka sisältää AES-salauksen.



Kuvio 36: WPA-suojauksen määrittäminen

6.6 Työasemat

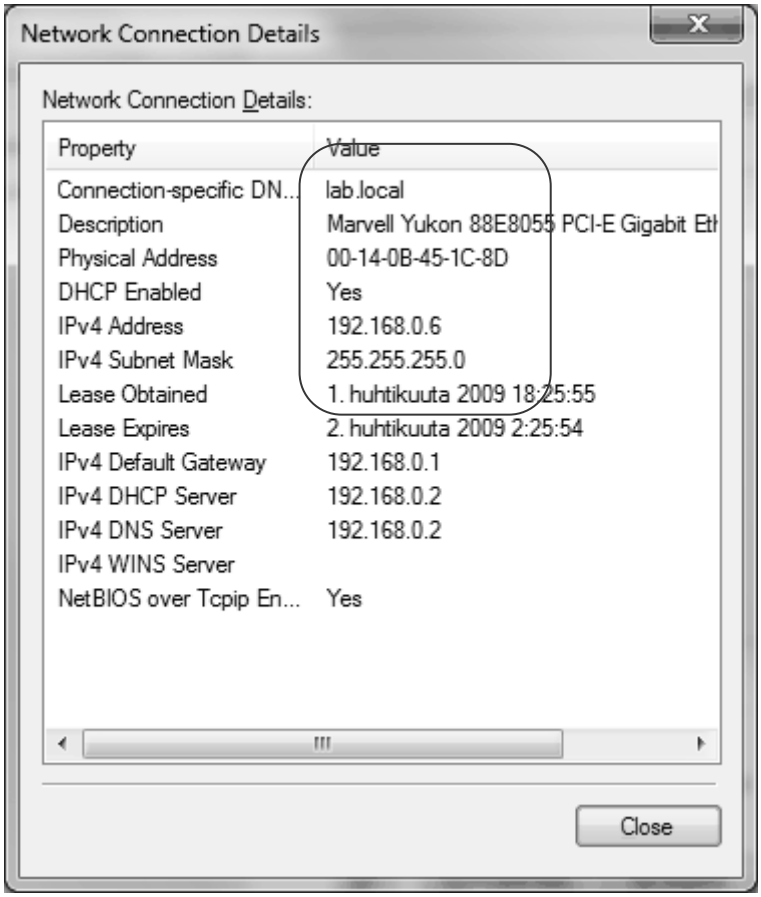
Windows-, Mac OS X- ja Linux-käyttöjärjestelmät tukevat WLAN-yhteyksiä, jotka on toteutettu 802.1X-standardin mukaisesti tietyin ehdoin. Windows XP:ssä ja Vistassa on sisäänrakennettuna tuki 802.1X-standardille ja Mac OS X tukee ominaisuutta versiosta 10.3 lähtien. Linux ei suoraan tue, mutta asentamalla esimerkiksi wpa_supplicant-ohjelman, saadaan 802.1X-standardi toimimaan langattomassa verkossa.

Langattomaan verkkoon kirjautumisen ehdot ovat, että asiakaskone tukee 802.1X-kirjautumista ja kuuluu toiminimeen tai siihen on asennettuna varmenne. Käyttäjätunnuksen on myös kuuluttava ryhmään, jolla on oikeus langattomaan verkkoon.

Tietokoneen on kuuluttava toiminimeen, jotta langaton verkkoyhteys toimisi. Tietokoneen voi liittää toiminimeen järjestelmänvalvojan oikeuksilla ja käyttöjärjestelmän uudelleenkäynnistys on tarpeen tämän toimenpiteen jälkeen.

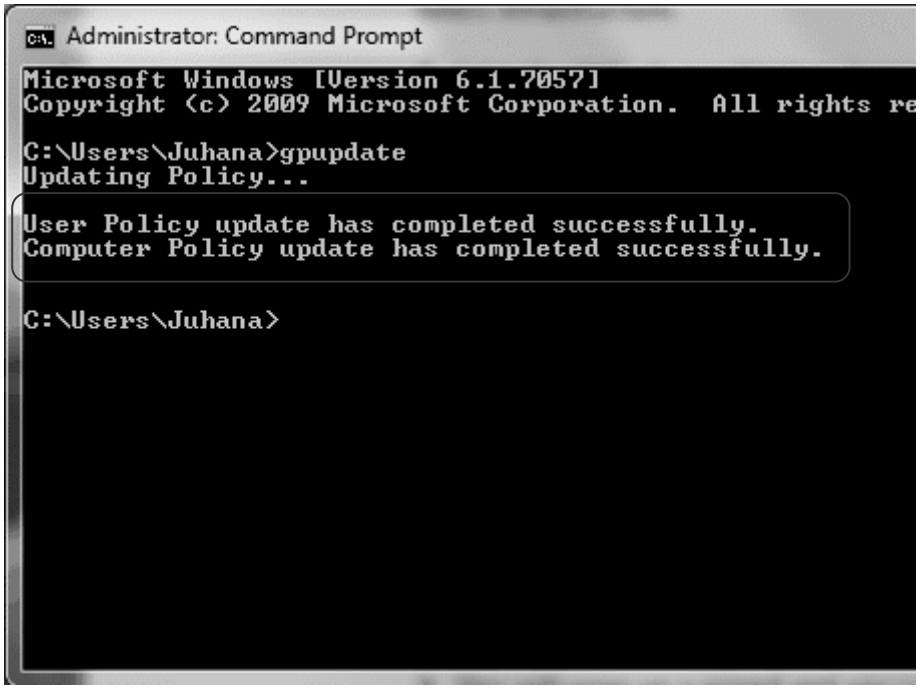
Kuvio 37: Tietokoneen liittäminen toiminimeen

Kirjautumisen jälkeen Group Management Policy latautuu palvelimelta asiakaskoneelle yhdistäen langattoman verkkoyhteyden automaattisesti. Verkkokortin asetuksista voi tarkistaa, että DHCP-palvelin on antanut oikeat tiedot tietokoneelle.



Kuvio 38: Langattoman yhteyden tarkistaminen Windows Vistassa

Ryhmäkäytäntöhallinnassa tehdyt muutokset tulevat voimaan, kun käyttäjä käynnistää tietokoneen tai kirjautuu siihen uudestaan. ”Group Policy” voidaan myös päivittää komentokehotteessa komennolla ”gpupdate”, jolloin ei tarvitse uudelleenkirjautua tietokoneelle.



Kuvio 39: Gpupdate-komennon käyttö komentorivissä

Varmenne on asennettava toiminimen ulkopuolella olevaan asiakaskoneeseen manuaalisesti. Varmenteen asentaminen asiakaskoneeseen tapahtuu järjestelmänvalvojan toimesta lataamalla varmenne tiedostona tai pyytämällä käyttäjävarmennetta palvelimelta suojatun verkkosivun kautta (CA Web enrollment tool).

Kuvio 40: Varmenteen avaaminen Windows Vistassa

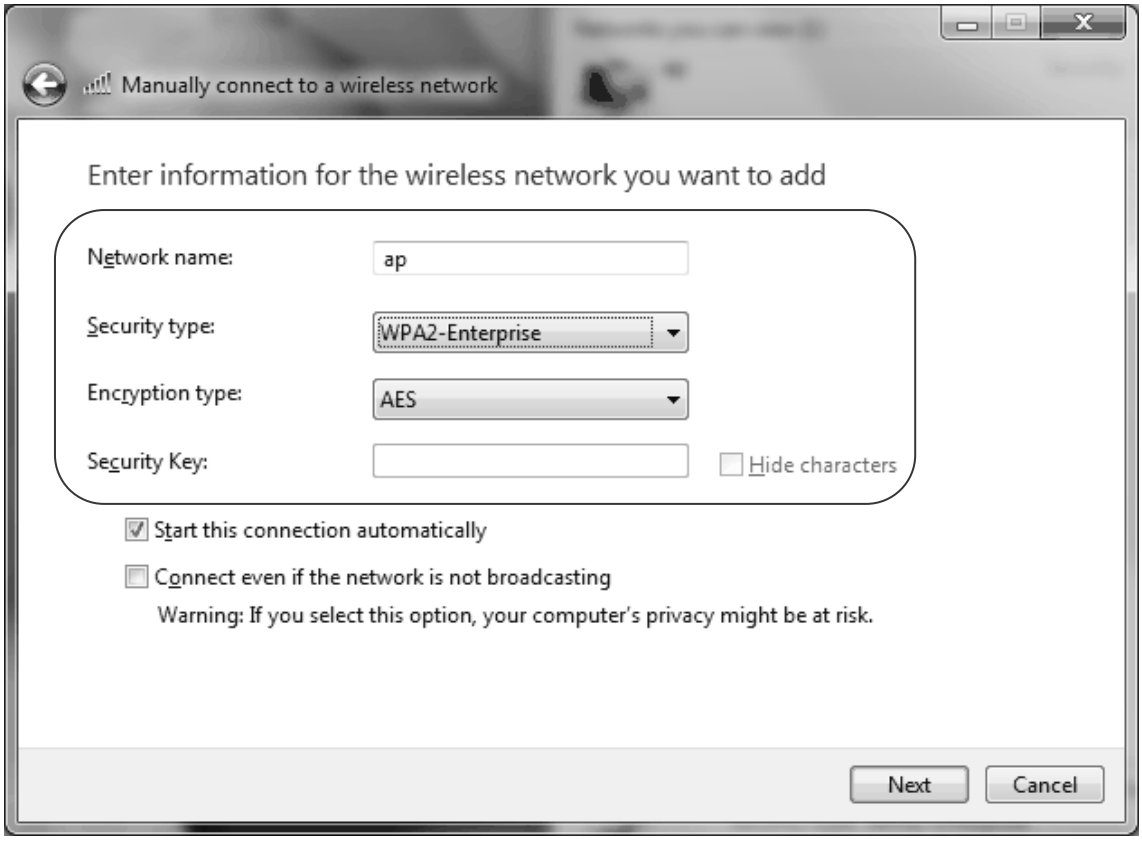
Asiakaskone ei voi varmistaa varmennetta jos se ei kuulu toiminimeen. Varmenne ilmoittaa, että asiakaskone ei voi luottaa varmenteeseen. Ennen varmenteen asennusta on tarkistettava tietojen oikeellisuus esimerkiksi järjestelmänvalvojalta.

Kuvio 41: Varmenteen tarkistaminen Windows Vistassa

Varmenteen tallennuspaikaksi on valittava ”Trusted Root Certification Authorities”, jotta asiakaskone hyväksyy varmenteen luotettavaksi.

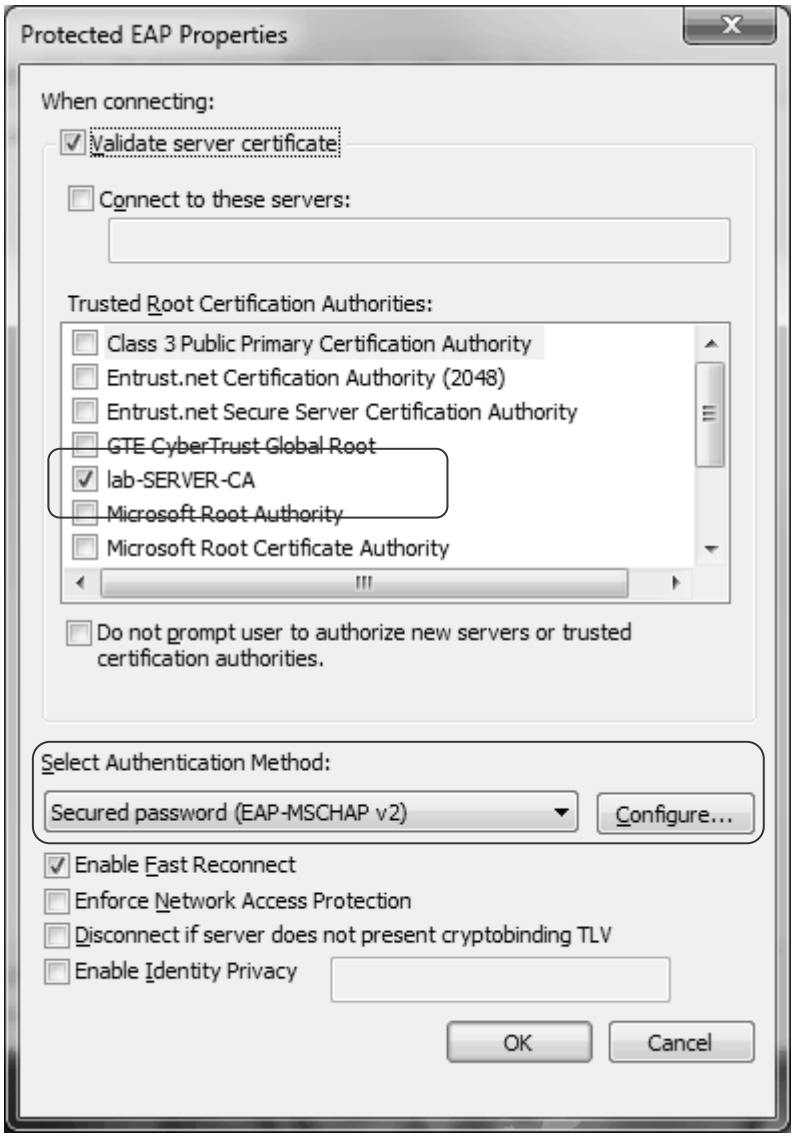
Kuvio 42: Varmenteen lisääminen luotettuun ryhmään

Asiakaskoneeseen luodaan langaton profiili, johon määritellään NPS-palvelimeen ja tukiasemaan merkityt tiedot yhteydestä.



Kuvio 43: Langattoman verkon määrittäminen manuaalisesti Windows Vistassa

PEAP-asetuksissa valitaan palvelimen varmenteeksi aiemmin asennettu varmenne.



Kuvio 44: Varmenteen valinta langattoman yhteyden profiiliin

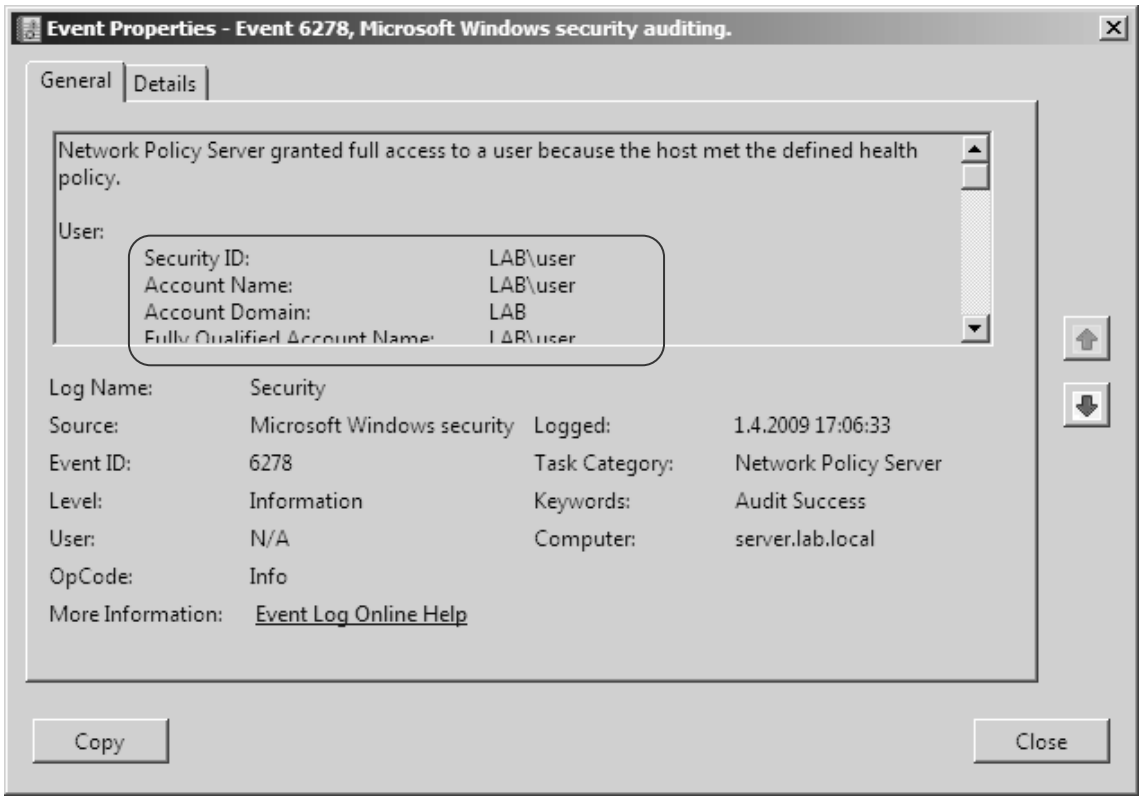
EAP MSCHAPv2-asetuksista otetaan pois käytöstä paikallisen Windows-käyttäjätunnuksen käyttö, sillä langaton yhteys vaatii käyttäjätunnuksen, joka on määritelty AD DS:ään.

Kuvio 45: EAP-MSCHAPv3-kirjautumisasetukset

7 Testaus

7.1 Lokitiedostot

NPS-palvelimen lokeista voidaan tarkistaa, onko asiakaskone saanut yhteyden langattomasti verkon palveluihin. Lokit auttavat vikatilanteissa paikallistamaan ongelman. Esimerkin kuvassa NPS on antanut täydet oikeudet käyttää verkkoa, sillä käyttäjä on todettu luotettavaksi. Ilmoitus ” Network Policy Server granted full access to a user because the host met the defined health policy.” tarkoittaa, että asiakaskone on läpäissyt kaikki tietoturvakäytännöt, jotka NPS on asettanut langattomille yhteyksille.



Kuvio 46: NPS:n tapahtumienvalvonnan loki

7.2 Onnistunut liittyminen

NPS tallentaa lokiin seuraavan ilmoituksen, jossa asiakaskone on hyväksytty verkkoon kaikin oikeuksin, sillä asiakaskone kuuluu oikeaan toiminimeen ja täyttää muut verkon edellytykset:

Log Name:	Security
Source:	Microsoft-Windows-Security-Auditing
Date:	1.4.2009 17:06:33
Event ID:	6278
Task Category:	Network Policy Server
Level:	Information
Keywords:	Audit Success
User:	N/A
Computer:	server.lab.local
Description:	Network Policy Server granted full access to a user because the host met the defined health policy.

7.3 Epäonnistunut liittyminen

NPS tallentaa lokiin seuraavan ilmoituksen jos asiakaskone ei ole toiminimessä eikä siihen ole asennettu luotettavaa varmennetta, jonka palvelin on hyväksynyt:

Log Name:	System
Source:	NPS
Date:	11.4.2009 13:30:16
Event ID:	4402
Task Category:	None
Level:	Error
Keywords:	Classic
User:	N/A
Computer:	server.lab.local
Description:	There is no domain controller available for domain LAPTOP.

8 Kehitysehdotus

IEEE 802.1X-käyttäjätunnistukseen pohjautuva langaton verkko on mahdollista toteuttaa teknisesti ja taloudellisesti pienin kustannuksin Laurea-ammattikorkeakoulun Leppävaaran tietoliikennelaboratoriossa sekä talon sisäverkossa. Tämänhetkinen fyysinen tietoliikennelaitteisto tukee WPA2- AES-standardeja langattoman verkon suojauksessa sekä Laurean lähiverkossa toimiva Active Directory –hakemistopalvelu voidaan yhdistää RADIUS-tekniikalla tunnnistamaan käyttäjät.

Asennusdokumentaation mukaan määritelty langaton verkko sopii hyvin Laurean käyttöön. Toiminimen alla olevat työasemat tunnistautuvat PEAP-TTLS:n avulla ja muut työasemat EAP-TLS:n avulla. PEAP lataa varmenteet ja käytännöt automaattisesti työasemaan ja EAP vaihtoehtona on parempi pelkästään varmennepohjaiseen tunnistautumiseen. Esimerkiksi vieraskone voisi ladata ja asentaa WLAN-varmenteen kotisivulta ja kirjautua vieras-tunnuksella tai omalla Active Directory –tunnuksella verkkoon.

Käyttäjien tunnistus, hallinta ja valvonta ovat tärkeimpiä hyötyjä miksi asennusdokumentaation mukainen langaton määrittely lähiverkkoon on tarpeellista. Käyttäjille suunnatut palvelut, kuten verkkolevyt, oppimisympäristöt, pikaviestimet ja reaaliaikainen tunteihin osallistuminen ovat esimerkkejä kuinka yhtenäisestä käyttäjätunnistuksesta olisi hyötyä opiskeluympäristössä. 802.1X mahdollistaa turvallisen, nopean, helppokäyttöisen ja edullisen langattoman verkon rakentamisen Laureaan tai muihin isompiin yrityksiin tai organisaatioihin.

9 Yhteenveto

Tässä opinnäytetyössä tutustuttiin keinoihin, joilla langaton verkko voidaan toteuttaa turvallisesti sekä selvitettiin, millaisia suojauskeinoja langattomiin verkkoihin on saatavilla. Tukiasemien kehittyminen suojaamiseen liittyvissä asioissa on kasvattanut langattomien verkkojen suosiota yritys- ja yksityiskäytössä. Langattoman verkon lisääminen lähiverkon jatkeeksi antaa käyttäjille uusia mahdollisuuksia käyttää verkkoa hyväksi.

Langattomien laitteiden tekniikat suorituskyvyn ja suojauksen osalta ovat kehittyneet muutaman vuoden aikana huomattavasti. Esimerkiksi langaton 802.11n-standardi kykenee siirtämään dataa teoriassa 600 Mbps sekä WPA2-salaus mahdollistaa murtamattoman suojauksen teoriassa. Vanhoja standardeja päivitetään ja uusia kehitetään laite- ja ohjelmistovalmistajien toimesta jatkuvasti, sillä nopeat langattomat yhteydet vaativat myös suurempaa tietoturvaa käyttäjämäärien kasvaessa langattomissa verkoissa.

802.1X-protokolla tarjoaa monipuolisen suojauksen yhdessä WPA2:n ja AES:n kanssa. Nämä kolme elementtiä muodostavat kolmen tason suojausmekanismin, jota tarvitaan yritysverkkojen suojauksessa. 802.1X tunnistautuu RADIUS-palvelimen kanssa saaden käyttäjätiedot ja oikeudet AD:sta, WPA2 pitää asiakaskoneen, tukiaseman ja tunnistautumispalvelimen yhteyden salassa muilta ja AES luo liikenteelle vahvasti salatun tunnelin.

Windows Server 2008:n NPS-palvelussa yhdistyy tärkeät langattoman verkon tunnistautumiskeinot. NPS:n sisällä oleva RADIUS-toiminto kommunikoi AD:n ja muiden palvelimien kanssa, kun liikenne asiakaskoneen ja tukiaseman välillä on hyväksytty. Monipuolisten käytäntöjen avulla voidaan luoda sääntöjä, joita asiakaskoneet joutuvat noudattamaan, jotta langaton yhteys voisi muodostua ja verkon palveluihin pääsy olisi mahdollista.

Langattomat palvelut voidaan myös ottaa pois käytöstä tarvittaessa, kun palvelut ovat yhdistetty yhteen palvelimeen. Vikatilanteissa NPS:n lokitiedostot antavat kattavan kuvan ongelmasta. Palvelimien ja työasemien lokeista voi todentaa ongelman lähes reaaliaikaisesti. Ongelmanratkaisu vikatilanteissa siis nopeutuu, kun voidaan tarkastella, onko vika palvelimissa, tukiasemissa vai asiakaskoneissa.

Käyttäjän toimenpiteitä langattoman verkon määrityksessä työasemaan ei tarvita, ellei työaseman käyttöjärjestelmä ole jokin muu kuin Windows ja se kuuluu yrityksen lähiverkon toiminimeen. Muissa käyttöjärjestelmissä langaton verkko saadaan toimimaan, mutta se vaatii käyttäjältä enemmän tietotaitoja ja opastusta ennen käyttöä. Toiminimen ulkopuolella oleva työasema vaatii esimerkiksi varmenteen lataamisen ja sen hyväksymisen ennen langattomaan verkkoon pääsyä.

Windows Server –alustalle ja Ciscon laitteilla toteutettu 802.1X-pohjainen tunnistautumismenetelmä sopii hyvin vaativaan yritys- ja oppilaitoskäyttöön turvaamaan langaton tietoliikenne. Asennusdokumentaation mukainen langattoman verkon käyttöönotto valmiiseen lähiverkkoon on kustannustehokas ja tietoturvallinen isommankin organisaation käyttöön. Toteutustapa on myös hyvin hallittavissa ja päivitettävissä myöhemmin ja tulevaisuuden tarpeisiin.

Lyhenteet

AAA	Authentication Authorization Accounting
AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CA	Certificate Authority
CA	Collision Avoidance
CCK	Complementary Code Keying
CCK-OFDM	Complimentary Code Keying/Orthogonal FDM
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CHAP	Challenge-Handshake Authentication Protocol
CRL	Certificate Revocation List
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
GHz	Gigahertz
GPM	Group Policy Management
GPME	Group Policy Management Editor
GPO	Group Policy Object
GTK	Group Transmit Key
HR	High Rate
HR/DSSS	High Rate / Direct Sequence Spread Spectrum
IAPP	Inter-Access Point Protocol
IBSS ID	Independent Basic Service Set Identifier
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU	International Telecommunication Union
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MD	Message-Digest algorithm
MIC	Message Integrity Code
MIMO	multiple-input and multiple-output
MS	Mobile Station

NAP	Network Access Protection
NPS	Network Policy Server
OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open Systems Interconnection Reference Model
PBCC	Packet Binary Convolutional Code
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPP	Point-to-Point Protocol
PSK	PreShared Key
PTK	Pairwise Transient Key
QFDM	Quadrature Frequency Division multiplexing
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RSA	Microsoft Software Key Storage Provider
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TK	Temporar Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
WEP	Wired Equivalent Privacy
VoIP	Voice over Internet Protocol
WPA	Wireless Fidelity Protected Access

Lähteet

Kirjallisuus

Barken, L. 2004. How secure is your wireless network?: safeguarding your Wi-Fi LAN. New Jersey: Pearson Education Inc.

Dennis, A. & FitzGerald J. 2007. Business Data Communications and Networking. 9. painos. USA: John Wiley & Sons Inc.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. 2. painos. Jyväskylä: Docento.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Kempf, J. 2008. Wireless Internet Security. Cambridge: Cambridge University Press.

Langattomat verkot: perusteet. 2005. Suomentaja Holttinen, J. Helsinki: IT-Press.

Miller, S. 2003. Wi-Fi security. New York: McGraw-Hill

Odom, W. 2008. CCENT/CCNA ICND1, Official Exam Certification Guide. 2. painos. Indianapolis: Cisco Press.

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Gummerus Kirjapaino Oy.

Swaminatha, T. & Elden, C. 2003. Wireless Security and Privacy: Best Practices and Design Techniques. Boston: Addison-Wesley.

Tietoturvasertifikaatti - CISSP. 2003. Suomentaja Suominen, E. Helsinki: Edita Prima Oy.

Vines, R. 2002. Wireless security essentials: defending mobile systems from data piracy. Indianapolis: Wiley.

Elektroniset lähteet

Active Directory Certificate Services Step-by-Step Guide. Microsoft. Viitattu 24.2.2009. http://technet.microsoft.com/en-us/library/cc772393.aspx

Anderson, D. 2008. Secure Your Wireless Network With WPA2-EAP. Viitattu 19.3.2009. http://www.msserveradmin.com/secure-your-wireless-network-with-wpa2-eap

Cisco Aironet 1100 Series Access Point Data Sheet. Cisco. Viitattu 10.4.2009. http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps4570/ps4612/product_data_sheet09186a00800f9ea7_ps4570_Products_Data_Sheet.html

EAP Authentication with RADIUS Server. Cisco. Viitattu 11.4.2009. http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801bd035.shtml

Foundation Network Companion Guide: Deploying 802.1X Authenticated Wireless Access with PEAP-MS-CHAP v2. Microsoft. Viitattu 19.3.2009. http://www.microsoft.com/downloads/details.aspx?FamilyID=A1746605-4248-4E61-970B-509AA5ED0FE8&displaylang=en

How to Build a Secure Wireless Network using PEAP and MS-CHAPv2. Bits & Bytes Consulting, Inc. Viitattu 5.2.2009.

http://www.bitsbytes.com/MCSE/SecureWirelessViaPEAPMSCHAPv2.htm

IEEE 802.11 Official Timelines. 2009. Institute of Electrical and Electronics Engineers, Inc. Viitattu 12.4.2009.
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Mirabito, M. 2008. Securing Wireless Networks with Windows Server 2008 and NPS. Viitattu 1.3.2009.
http://techblog.mirabito.net.au/?p=87

Recommendations for Small Office or Home Office Wireless Networks. 2006. Microsoft. Viitattu 20.3.2009.
http://technet.microsoft.com/en-us/library/bb727047.aspx

Securing Wireless LANs with Certificate Services. 2004. Microsoft. Viitattu 20.3.2009.
http://www.microsoft.com/downloads/details.aspx?familyid=cdb639b3-010b-47e7-b234-a27cda291dad&displaylang=en

Securing Wireless LANs with PEAP and Passwords. 2007. Microsoft. Viitattu 1.3.2009.
http://www.microsoft.com/downloads/details.aspx?familyid=60c5d0a1-9820-480e-aa38-63485eca8b9b&displaylang=en

Step-by-Step Guide for Secure Wireless Deployment for Small Office/Home Office or Small Organization Networks. 2005. Microsoft. Viitattu 11.1.2009.
http://www.microsoft.com/downloads/details.aspx?FamilyID=269902e8-fc41-4eb1-9374-44612e64f0fb&displaylang=en

Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab. 2005. Microsoft. Viitattu 15.2.2009.
http://www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&DisplayLang=en

The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network Access. 2004. Microsoft. Viitattu 1.4.2009.
http://download.microsoft.com/download/4/4/7/447404a7-c373-4bf4-9c77-daee54b1f6fc/PEAP.doc

Varmenne. Viestintävirasto. Viitattu 10.4.2009.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/varmenne.html