Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2011

Pekka Sookari

TIETOTURVALLISEN LANGATTOMAN LÄHIVERKON TOTEUTUS VAL-TRADINGILLE

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Marraskuu 2011 | 59 sivua

Esko Vainikka

Pekka Sookari

TIETOTURVALLISEN LANGATTOMAN LÄHIVERKON TOTEUTUS VAL-TRADINGILLE

Tämän opinnäytetyön tarkoituksena on suunnitella ja toteuttaa tietoturvallinen langaton lähiverkko Val-Tradingille. Työn lähtökohtana on taata korkean tason tietoturva yrityksen verkolle käyttämällä IEEE 802.1X-todennusta.

Työn teoriaosuudessa käsitellään langattoman verkon yleisiä ominaisuuksia, standardit sekä yleisimmät modulointitekniikat. Tietoturvaa, joka on langattomien verkkojen haastavampia sekä keskeisempiä ominaisuuksia, käsitellään esittelemällä salaustekniikoita sekä autentikointimenetelmiä. Lisäksi tutkitaan Windows-palvelimen ominaisuuksia sekä Active Directory-hakemistopalvelun pääpiirteitä.

Käytännön osuudessa toteutetaan langaton lähiverkko langallisen verkon yhteyteen, asennetaan Microsoft Windows Server 2008-palvelinympäristö sekä Active Directory-hakemistopalvelu. Langattoman verkon autentikointi toteutetaan käyttämällä Windows-palvelimelle asennettavaa NPS-palvelinta, joka on Microsoftin toteutus RADIUS-protokollasta. NPS-palvelin hoitaa keskitetysti käyttäjien autentikoinnin yhdessä Active Directoryn kanssa.

Työn teoriaosuudessa käsiteltävät menetelmät ja käytännöt määritetään palvelimeen, tukiasemaan ja langattomille työasemille. Työn lopputuloksena on pienelle yritykselle tietoturvallinen langaton lähiverkko.

ASIASANAT:

802.1X, Active Directory, Network Policy Server, RADIUS, Windows Server 2008, WLAN

BACHELOR´S THESIS | ABSTRACT

UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

November 2011 | 59 pages

Esko Vainikka

Pekka Sookari

IMPLEMENTING A SECURE WIRELESS LOCAL AREA NETWORK FOR VAL-TRADING

The purpose of this thesis was to plan and implement a secure wireless local area network (WLAN) for Val-Trading. The starting point for the study was to ensure a high level of corporate network security by using IEEE 802.1X-authentication.

The theoretical part of the thesis is concerned with general WLAN features, standards and the most common modulation techniques. Information security, which is the most challenging and most essential feature in WLAN's, is dealt with by introducing encryption techniques and authentication methods. In addition, features of Windows-server and main features of Active Directory-directory service are researched.

In the practical part of the thesis WLAN is implemented to communicate with existing wired network also Windows Server 2008-server environment and Active Directory-directory service are installed. The authentication of WLAN is implemented by using NPS-server installed on Windows server. The NPS-server is Microsoft's implementation of RADIUS-protocol and it centrally manages user authentication with Active Directory.

Methods and practices dealt with in the theoretical part are configured to servers, access points and wireless work stations. The result of this thesis is a secure WLAN for a small company.

KEYWORDS:

802.1X, Active Directory, Network Policy Server, RADIUS, Windows Server 2008, WLAN

SISÄLTÖ

KUVAT

TAULUKOT

1 JOHDANTO

Opinnäytetyön aiheena on toteuttaa tietoturvallinen langaton lähiverkko (WLAN) Val-Tradingille. Langattoman lähiverkon toteuttaminen tuli ajankohtaiseksi, kun yritys hankki kaksi kannettavaa tietokonetta, jotka haluttiin verkkoon langattomasti. Toteutettava verkkoratkaisu mahdollistaa tehokkaan työskentelyn kannettavilla tietokoneilla ilman paikkasidonnaisuutta.

Yrityksessä on käytössä myös älypuhelimia, jotka voivat tarvittaessa käyttää langatonta verkkoa. Langaton lähiverkko toteutetaan IEEE 802.11g -standardin mukaisesti ja se liitetään Microsoft Windows Server 2008 -palvelinympäristöön.

Tutkimuksen teoriaosuus selvittää langattoman lähiverkon perusteita, IEEE 802.11 -standardia, siirtotekniikoita sekä tietoturvaa. Lisäksi esitellään erilaisia autentikointimenetelmiä sekä Windowsin Active Directoryn pääpiirteitä.

Käytännön toteutuksena rakennetaan langaton lähiverkko, asennetaan Microsoft Windows Server 2008 -palvelinympäristö sekä Active Directory -hakemistopalvelu. Langattoman verkon autentikointi toteutetaan käyttämällä asennettavaa RADIUS-palvelinta.

Opinnäytetyön tavoitteena on toteuttaa toimeksiantajalle tietoturvallinen langaton lähiverkko. Omana tavoitteenani on pyrkiä saavuttamaan kiitettävä tietotaito langattomista lähiverkoista sekä Windows-palvelinympäristöstä.

Opinnäytetyössä käytetään konstruktiivista tutkimusotetta. Lähteinä käytetään alan kirjallisuutta, suomalaisia ja englantilaisia sekä sähköisiä lähteitä.

2 LANGATON LÄHIVERKKO

2.1 Yleistä

Langattomalla lähiverkolla erona perinteiseen lähiverkkoon on se, että WLAN-verkko käyttää siirtotienä langatonta radiotietä. Langattomat lähiverkot (Wireless Local Area Network, WLAN) tarjoavat kustannuksiltaan edullisen mahdollisuuden kannettavien laitteiden liittämiseen yrityksen sisäiseen tietojärjestelmään ja tarvittaessa sen kautta Internetin tarjoamiin palveluihin. (Hakala & Vainio 2005, 152.)

Langattomat lähiverkot ovat yleistyneet nopealla tahdilla, kun kannettavien tietokoneiden, kämmentietokoneiden sekä älypuhelinten käyttö on lisääntynyt ihmisten päivittäisessä elämässä. Ilmaisia langattomia verkkoja on käytössä nykypäivänä siellä, missä ihmisetkin liikkuvat: lentokentät, hotellit, junat, koulut ja monet muut julkiset tilat tarjoavat mahdollisuuden langattomaan verkkoon liittymiseen.

WLAN-tekniikan hyötyinä voidaan pitää sen käyttäjälleen mahdollistamaa liikkuvuutta, nopeaa asennusta ja käyttöönottoa. Lisäksi tekniikka sopii vaikeasti verkotettaviin paikkoihin, jossa ei voida käyttää tai ei sallita kaapelointia.

WLAN tuo mukanaan myös tietoturvariskit, joita verkon käyttäjä ei tule aina ajatelleeksi. Suojaamaton langaton verkko on suorastaan kutsuhuuto rikolliselle, joten tietoturvaan kannattaa panostaa.

2.2 Langattoman lähiverkon standardit

Yleisin suomalaisten yritysten ja julkisyhteisöjen käyttämä langaton lähiverkko on IEEE (Institute of Electrical and Electronics Engineers) 802.11 -standardeihin perustuva ratkaisu. IEEE 802.11 -standardista on olemassa useita eri versioita, jotka edustavat eri teknologiasukupolvia. (Hakala & Vainio 2005, 152.)

Tällä hetkellä tavallisin käytössä oleva versio on IEEE 802.11g, jonka radiorajapinnan teoreettinen maksimisiirtonopeus on 54 Mbps (WLAN 2010).

802.11

IEEE 802.11 -suosituksen ensimmäinen versio hyväksyttiin 1997. 802.11 määrittää pääasiassa OSI-mallin fyysisen kerroksen ja siirtokerroksen alemman osan, joka tunnetaan nimellä MAC- (Media Access Control) kerros. (IEEE 802.11 2010.)

WLAN-tekniikan nimellisnopeus oli 1 tai 2 megabittiä sekunnissa. Se toimi 2,4 gigahertsin taajuudella. Vaikkakin se julkaistiin vuonna 1997, markkinoilla ei ollut montaa tuotetta ennen kuin vuonna 1999, jolloin 802.11b julkaistiin. (Conlan 2009, 673.)

802.11b

802.11b on ensimmäinen varsinainen WLAN-standardi, joka otettiin laajalti käyttöön sekä valmistajien että kuluttajien toimesta vuonna 1999. Sen nopeus 11 megabittiä sekunnissa toimi melko hyvin useimmilla sovelluksilla verrattuna IEEE 802.11 -standardiin. Toimintataajuus on 2,4 gigahertsiä.

Yhteys toteuttaa tiedonsiirrossa CCK-tekniikkaa (Complementary Code Keying). Tämä tarkoittaa, että tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. 802.11b on yhteensopiva aiemman 802.11 -standardin kanssa. (Conlan 2009, 675.)

802.11a

802.11a oli toinen vuonna 1999 julkaistu standardi. Se toimii 5 gigahertsin taajuudella ja sen maksiminopeus on 54 megabittiä sekunnissa. Taajuutta nostettiin, koska tarvittiin lisää kaistaa verkkoyhteyksien nopeuksien kasvattamiseksi. Lisäksi korkeampi taajuus oli immuuni laitteille, jotka toimivat 2,4 gigahertsin taajuudella, kuten mikroaaltouunit, langattomat puhelimet sekä Bluetooth-laitteet.

Standardi määrittelee tiedonsiirtotekniikaksi OFDM-tekniikan (Orthogonal Frequency Division Multiplexing), joka perustuu signaalin jakamiseen pienempiin alasignaaleihin. Jaetut signaalit siirretään yhtäjaksoisesti eri

taajuuksilla. A-standardi ei ole yhteensopiva b-standardin kanssa. (Conlan 2009, 677.)

802.11g

802.11g -standardi julkaistiin vuonna 2003 ja se on yhteensopiva 802.11b:n kanssa. 802.11g toimii samalla 2,4 gigahertsin taajuudella kuin 802.11b ja sen nopeus on 54 megabittiä sekunnissa. Tiedonsiirtoon käytetään CCK-OFDM-tekniikkaa. (Conlan 2009, 676.)

Yhteensopivuus 802.11b:n kanssa toimi avainperiaatteena 802.11g:tä suunniteltaessa ja näin standardi mahdollistaa kolmen eri tilan käytön laitteille: vain g-tila, vain b-tila sekä yhdistetty b ja g-tila.

802.11n

IEEE 802.11n standardoitiin syyskuussa 2009. 802.11n perustuu aikaisempiin 802.11 -standardeihin lisäämällä niihin MIMO (Multiple-Input-Multiple-Output) -tekniikan, joka käyttää useita lähetin- ja vastaanottoantenneja kasvattamaan tiedonsiirron nopeutta.

802.11n:n teoreettinen maksiminopeus on 600 megabittiä sekunnissa, jonka mahdollistaa jopa kahdeksan antennin käyttö. Antenneja kutsutaan älykkäiksi antenneiksi, koska useampi antenni voi lähettää ja vastaanottaa dataa samanaikaisesti. Standardi käyttää OFDM-tekniikkaa. (Conlan 2009, 678.)

Suuret parannukset IEEE 802.11n -standardin suorituskyvyssä tekevät siitä houkuttelevan vaihtoehdon kun käytetään esimerkiksi suoratoistoa (streaming), IP-puhetta (Voice over IP, VoIP) tai videokonferenssisovelluksia. (Soyinka 2010, 34).

Taulukossa 1 on esitelty IEEE 802.11 -standardien ominaisuuksia.

Taulukko 1. IEEE 802.11 -standardit (Soyinka 2010, 32).

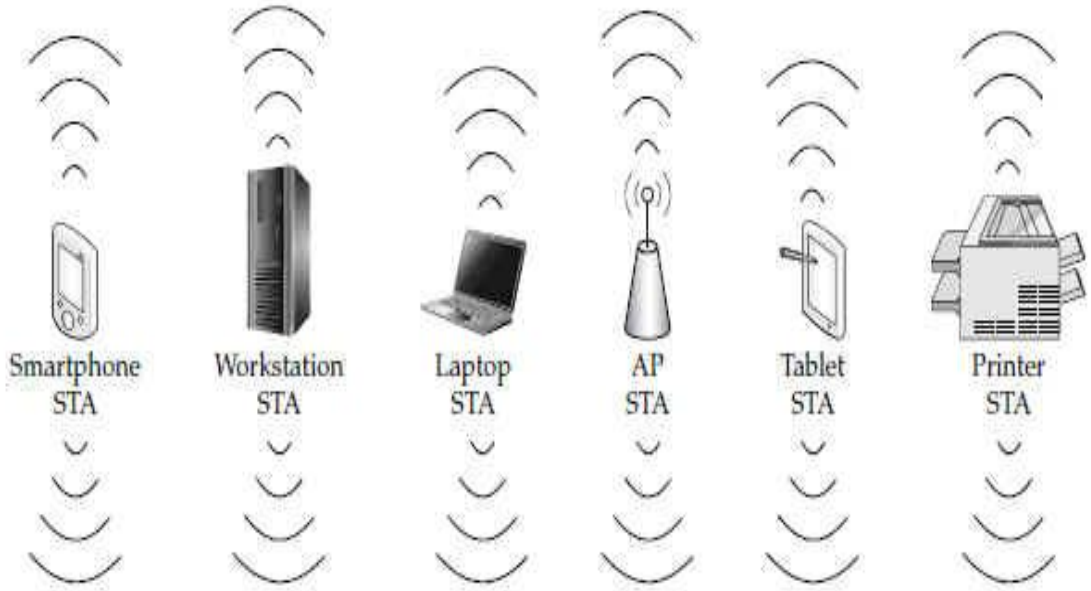
Standard	Center Frequency	Bandwidth (MHz)	Data Rates (Mbps)	Modulation
802.11a	5 GHz	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM
802.11b	2.4 GHz	20	1, 2, 5.5, 11	DSSS
802.11g	2.4 GHz	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	OFDM and DSSS
802.11n	2.4 GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	OFDM
802.11n	5 GHz	40	15, 30, 45, 60, 90, 120, 135, 150	OFDM

2.3 Laitteet ja topologiat

IEEE 802.11 -standardi määrittelee verkon peruskomponenteiksi kaksi laitetta: päätelaitteen (STA, station), joka on langaton laite, esimerkiksi kannettava tietokone, kännykkä tai Personal Digital Assistant (PDA) -laite.

Toiseksi laitteeksi se määrittelee tukiaseman (AP, Access Point), joka loogisesti yhdistää päätelaitteen esimerkiksi yrityksen langalliseen verkkoon. Tukiasema voi myös yhdistää langattomat päätelaitteet keskenään. (Frankel ym. 2007, 2-4.)

Kuvassa 1 on esitetty eri päätelaitteita.



Kuva 1. Esimerkkejä päätelaitteista (STA) (Soyinka 2010, 75).

Langaton lähiverkkostandardi IEEE 802.11 sallii kaksi eri tapaa kytkeä verkon laitteita toisiinsa. Langattoman verkon voi muodostaa kahden tai useamman laitteen välille (Ad Hoc) tai langattoman verkon asiakkaat voivat olla tukiaseman kautta yhteydessä toisiin asiakkaisiin tai kiinteään lankaverkkoon (infrastruktuuriverkko).

Ad-Hoc -verkko

Jos laitteiden muodostama verkko ei kytkeydy kiinteään verkkoon, verkosta käytetään nimitystä IBSS (Independent Basic Service Set). Verkosta käytetään myös nimitystä Ad Hoc -verkko (kuva 2). Ad Hoc -verkko ei vaadi lainkaan tukiasemaa, esimerkkinä kahden kannettavan tietokoneen muodostama verkko. Tällöin tietokoneiden langattomat verkkokortit toimivat lähettiminä sekä vastaanottimina. Ad Hoc -verkko onkin tyypillisesti lyhytikäinen ratkaisu, esim. kokoustilanne. (Granlund 2003, 297.)

Kuva 2. Ad Hoc -verkko (Frankel ym. 2007, 2-5).

Infrastruktuuriverkko

Infrastruktuuriverkko muodostuu yhdestä tai useammasta Basic Service Setistä (BSS). BSS-verkko muodostuu kiinteästä tukiasemasta sekä siihen liitetyistä työasemista. Tukiasema (AP, Access Point) hallitsee ja välittää liikennettä verkossa olevien laitteiden välillä.

Päätelaite tunnistaa tukiaseman sen yleisviestinä kantoalueellaan lähettämän Service Set Identifierin (SSID) perusteella. SSID toimii verkon sekä siihen yhdistyneiden langattomien tukiasemien tunnistetietona eli nimenä. SSID voi olla 0-32 bitin mittainen.

Tukiasemat yhdistävät päätelaitteet Distribution System -järjestelmään (DS), joka on tyypillisesti yrityksen lankaverkko ja jonka kautta päätelaitteet voivat olla yhteydessä myös ulkopuolisiin verkkoihin. Extended Service Set (ESS) muodostuu useammasta Basic Service Setistä ja se on yleisin tapa muodostaa langattomia lähiverkkoja (kuva 3). ESS mahdollistaa laajempien verkkojen luonnin sekä sallii myös sen, että päätelaitteet liikkuvat verkon alueella ilman, että verkkoyhteys katkeaa (roaming-ominaisuus) vaikka tukiasema vaihtuu. (Granlund 2003, 297.)

Kuva 3. Infrastruktuuriverkko (Frankel ym. 2007, 2-5).

2.4 Langattomat modulointitekniikat

Modulaatio on prosessi, jossa kantoaallon signaalia tai taajuutta vaihdellaan. Datan lisäystä tähän kantoaaltoon kutsutaan koodaukseksi. (Brandon 2008, 12.)

DSSS

Suorasekvenssihajaspektritekniikkaa (Direct-Sequence Spread Spectrum, DSSS) käytetään sekä IEEE 802.11b- että 802.11g -verkon alle 20 Mb/s lähetyksessä.

Siinä käytetään koodausbittejä (Chipping code, Pseudo Noise Code) varsinaisen lähetettävän datan lisäksi. Koodausbittien avulla signaalia lähetetään useammalla vaihtuvalla taajuudella. Vastaanottaja rakentaa informaation uudelleen yhdistämällä eri taajuuksilta luetut signaalit käyttäen samaa koodausbittikuviota kuin lähettäjä. Koodausbitit mahdollistavat tiedon aikana turmeltuneiden databittien uudelleenkokoamisen.

Moduloinnin lisäksi käytössä on Complementary Code Keying (CCK) -koodaus, joka mahdollistaa suuremman tietomäärän lähettämisen yhtenä signaalina. (Hakala & Vainio 2005, 155–156.)

FHSS

Vaikka taajuushyppelyhajaspektritekniikka (Frequency-Hopping Spread Spectrum, FHSS) on alkuperäinen IEEE 802.11 -standardin mukainen modulaatiotekniikka, sitä ei enää käytetä nykyisissä langattomissa lähiverkoissa. Tekniikkaa käytettäessä signaalia siirretään useilla ajan mukaan vaihtuvilla taajuuksilla. (Conlan 2009, 679–680.)

OFDM

Monikantoaaltomodulointi (Orthogonal Frequency Division Multiplexing, OFDM) on menetelmä, jossa siirrettävä informaatio lähetetään samanaikaisesti käyttämällä useampia eritaajuuksisia kantoaaltoja. IEEE 802.11g käyttää OFDM:ssa 52 kantoaallon järjestelmää (Conlan 2009, 680.)

3 WLANIN TIETOTURVA

Langattomat lähiverkot käyttävät tiedonsiirtoon radioaaltoja, jolloin liikennettä on helpompi vakoilla kuin kiinteässä lankaverkossa. Myös luvaton verkkoon kytkeytyminen on helpompaa, koska fyysistä yhteyttä ei tarvita. Langattomiin verkkoihin on suunniteltu useita erilaisia suojauskäytäntöjä sekä liikenteen salakuuntelun että verkon luvattoman käytön estämiseksi. (Hakala & Vainio 2005, 167.)

Tietoturvan perustana voidaan pitää seuraavia peruselementtejä: luottamuksellisuus, eheys, todennus, kiistämättömyys, pääsynvalvonta sekä käytettävyys (Kaarlo 2002, 292).

Luottamuksellisuudella (Confidentiality) tarkoitetaan sitä, että tietoa ei ole kenelläkään ulkopuolisella vaan ainoastaan niillä, joille se kuuluu.

Eheys (Integrity) tarkoittaa sitä, että tieto ei ole muuttunut tahattomasti taikka tahallisesti tiedonsiirron aikana.

Todennus (Authentication) tarkoittaa menetelmää, jolla varmistetaan osapuolten olevan juuri niitä, joita väittävät olevansa. Salasanan käyttö on tyypillinen todennusmenetelmä.

Kiistämättömyys (Non-repudiation) varmistaa osapuolen olleen mukana tapahtumassa ja se onkin itse asiassa todennuksen erittäin vahva muoto. Digitaalinen allekirjoitus perustuu kiistämättömyyteen.

Pääsynvalvonta (Access Control) rajoittaa laitteen tai ihmisen oikeutta päästä verkkoon tai verkon resursseihin.

Käytettävyys (Availability) varmistaa sen, että laite tai ihminen pääsee käsiksi verkkoon tai sen tietoihin milloin tahansa. (Kaarlo 2002, 293–294.)

Todellisessa elämässä yksi ratkaisu voi tarjota vaikka todennuksen, mutta on kykenemätön tarjoamaan luottamuksellisuuden. Toisin sanoen, mikään turvallisuusratkaisu ei ole täydellinen. (Soyinka 2010, 154.)

3.1 WLAN-salaustekniikat

WEP-protokolla

Wired Equivalent Privacy -protokolla (WEP) on IEEE:n 802.11 -standardin työaseman ja tukiaseman välistä langatonta tiedonsiirtoa suojaamaan kehitetty salausmenetelmä, jossa käytetään RC4-salausalgoritmia. WEP-salauksella suojataan langatonta verkkoa salakuuntelulta sekä pyritään estämään laitteiden luvaton verkkoon pääsy. Salaus perustuu tukiasemiin ja päätelaitteisiin määriteltyihin salausavaimiin. Avaimia voidaan käyttää neljää erilaista, jotka ovat yhteisiä kaikille päätelaitteille ja tukiasemille, mutta protokollassa ei ole varsinaista mekanismia avainten automaattiseen vaihtamiseen. Käytännössä tämä tarkoittaa sitä, että verkkoliikenteessä käytetään jatkuvasti samaa avainta. (Hakala & Vainio 2005, 168.)

Avaimen pituudet ovat 64 tai 128 bittiä. Salausavain sisältää 24-bittisen alustusvektorin, IV:n (Initialisation Vector), joka lähetetään salaamattomana jokaisen kehyksen ensimmäisissä biteissä. Loppuosat, 40 tai 104 bittiä muodostavat varsinaisen salausavaimen. Useimmat hyökkäykset WEP-salausta vastaan perustuvat alustusvektoreiden haavoittuvuuksiin. Koska alustusvektori-osa lähetetään selväkielisenä, voidaan tietoliikennettä seuraamalla ja analysoimalla laskea salattu avain eli murtaa verkon salaus. Verkon liikenteen määrä vaikuttaa siihen, kuinka nopeasti salaus pystytään murtamaan. (Frankel ym. 2007, 3-5.)

WEP-tunnistus käyttää jaetun avaimen menetelmää (Preshared Key Authentication), joka ei todenna käyttäjää vaan yksinkertaisesti vahvistaa, että käyttäjällä on avain. Tällöin ei tiedetä kuka käyttäjä on, mutta tiedetään että hän tuntee avaimen. (Brandon 2008, 334.)

Kuvassa 4 on esitelty jaetun avaimen menettelyn tunnistusprosessi.

Kuva 4. Jaetun avaimen menettelyn tunnistusprosessi (Frankel ym. 2007, 3-3).

WEP-tunnistuksen sanomaliikenne on seuraavanlainen (kuva 4):

1. Päätelaite lähettää tukiasemalle Authentication Request-pyynnön, jossa se ilmoittaa tukevansa jaetun avaimen tunnistusta.
2. Tukiasema lähettää satunnaisen, salaamattoman haastetekstin päätelaitteelle.
3. Käyttäen omaa WEP-avaintaan päätelaite salaa haastetekstin ja lähettää sen takaisin tukiasemalle.
4. Tukiasema purkaa vasteen omalla avaimellaan ja vertaa tulosta lähettämäänsä haastetekstiin. Jos tulos on sama, tunnistus hyväksytään kuittaussanomalla.

WPA-protokolla

Wireless Fidelity Protected Access -protokolla kehitettiin korjaamaan WEP-protokollan puutteita. Salausavainta vaihdetaan 10 000 paketin välein. Käytössä ovat myös pakettikohtaiset salausavaimet. WPA-protokolla hyödyntää myös TKIP (Temporal Key Integrity Protocol) -protokollaa, joka huolehtii pakettien salauksesta käyttäen RC4-salausalgoritmia. TKIP pitää sisällään myös MIC-toiminnon (Message Integrity Check), jossa jokainen datapaketti tarkistetaan muutosten varalta. EAP (Extensible Authentication Protocol) -protokolla puolestaan mahdollistaa käyttäjien luotettavan tunnistuksen. (Hakala & Vainio 2005, 169.)

WPA Personal -tilaa käytettäessä WPA käyttää etukäteen jaettuja aloitussalausavaimia (PreShared Key, PSK). Menetelmää käytettäessä tukiasemiin ja päätelaitteisiin määritetään aloitusavain, jota käyttämällä laitteet muodostavat yhteyden toisiinsa. Salausavainta vaihdetaan aina 10 000 kehyksen välein. Personal-tila on yleinen kotikäytössä. (Brandon 2008, 346.)

WPA Enterprise -tila vaatii autentikointiserverin (RADIUS), joka hoitaa tunnistuksen sekä avainten jaon. TKIP:n lisäksi voidaan käyttää myös AES-salausta (Advanced Encryption Standard). (Brandon 2008, 346.)

WPA:n heikkouksiksi voidaan sanoa sen käyttämän RC4-salausalgoritmin haavoittuvuus sekä protokollan reagoiminen palvelunestohyökkäyksiin (Denial of Service Attack, DoS Attack). Verkon joutuessa hyökkäyksen uhriksi, tukiasema sulkee verkon hetkeksi, jolloin kaikki liikenne estyy. (Hakala & Vainio 2005, 169.)

WPA2-protokolla

IEEE 802.11i -standardiin perustuva WPA2-salausmenetelmä julkaistiin vuonna 2004. Se ei ollut pelkkä parannusosa WPA-protokollalle vaan se vaatii myös laitteistoilta laitepohjaisen tuen, koska se käyttää AES/CCMP-salausta (Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol). (Brandon 2008, 348.)

Salaus pystyy käyttämään eripituisia avaimia, joiden pituus voi olla 128, 192 tai 256-bittiä. (IEEE 802.11i 2010).

3.2 WLAN-autentikointi

IEEE 802.1X -todennus

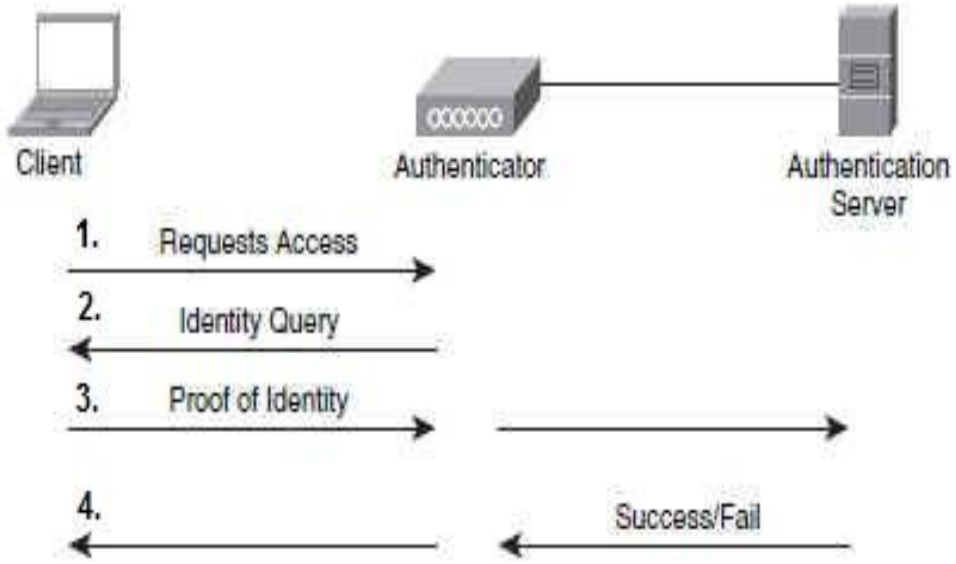
Standardi määrittelee ns.porttiperusteisen verkkoonpääsymenettelyn (Port Based Network Access Control), jossa asiakaslaitteen verkon käyttöä rajoitetaan langattoman verkon loogisten porttien ja todennuspalvelimen avulla.

Menetelmään kuuluvat asiakaskoneen verkkokortti (Suplicant), tukiasema (Authenticator) sekä käyttäjän todentava palvelin (Authentication Server). Langattomat laitteet toimivat loogisina verkkoportteina (Port Access Entity), jotka muodostavat keskenään päästä päähän -yhteyden (Point to Point). (Hakala & Vainio 2005, 169–170.)

IEEE 802.1X -todennusta käytetään yleensä jonkun AAA-palvelimen (Authentication, Authorization, Accounting) kanssa, useasti RADIUS-palvelimen. Tällöin saadaan käyttöön käyttäjien tunnistus, käyttäjien oikeuksien määrittely verkon resursseihin sekä tietokantojen ylläpito verkonhallinnassa. (Hakala & Vainio 2005, 170.)

EAP-protokolla

EAP-protokolla (Extensible Authentication Protocol) kehitettiin alun perin PPP-protokollan tunnistusmenetelmäksi, mutta se otettiin käyttöön myös IEEE 802.1X -standardissa. EAP-protokolla ei itsessään ole tunnistusmenetelmä, vaan se tukee useita erilaisia tunnistustapoja, kuten käyttäjänimiä, kertakäyttösalasanoja, digitaalisia sertifikaatteja sekä älykortteja. Kuvassa 5 on esitetty miten tunnistus tapahtuu EAP-protokollan ollessa käytössä. (Brandon 2008, 338; Soyinka 2010, 168).



Kuva 5. EAP-prosessi (Brandon 2008, 340).

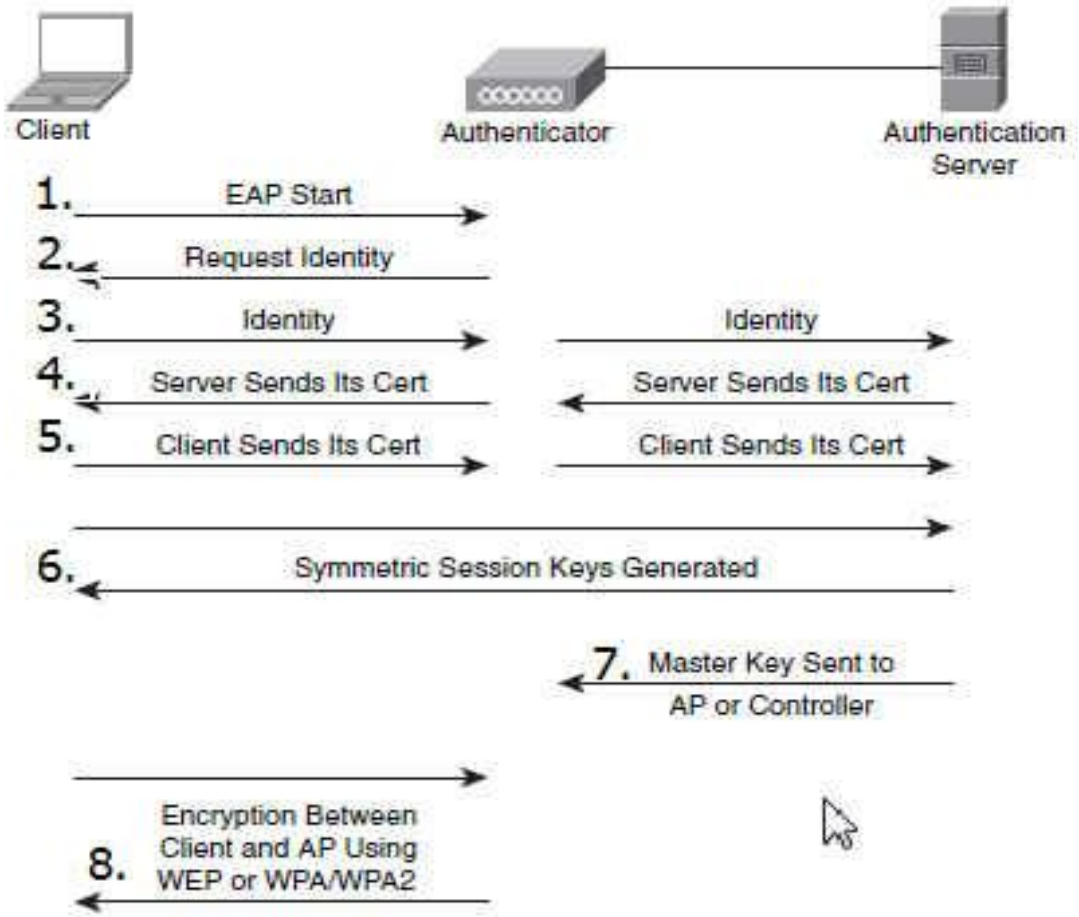
EAP-prosessi on aina samanlainen, riippumatta mikä tunnistustapa on käytössä. Prosessi pitää sisällään seuraavat vaiheet (kuva 5).

1. Päätelaite pyytää lupaa liittyä verkkoon.
2. Tukiasema pyytää päätelaitteelta tunnistusta.
3. Päätelaite toimittaa tunnistustiedon.
4. Päätelaite saa vastauksen palvelimelta. Palvelin joko hyväksyy tai hylkää päätelaitteen.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) on yleinen langattomissa verkoissa käytössä oleva tunnistustapa, jossa sekä päätelaite että verkko autentikoivat toisensa. Tässä metodissa sertifikaatti pitää asentaa sekä todentavalle palvelimelle että päätelaitteelle. Tästä syystä EAP-TLS-protokollaa pidetään yhtenä turvallisimmista metodeista, joita on saatavilla. Prosessissa päätelaitteen ja palvelimen avainparit muodostetaan ensiksi, jonka jälkeen todennuspalvelin varmistaa ne. TLS-protokolla on esimerkiksi pankkiyhteyksissä käytettävän SSL-protokollan (Secure Sockets Layer) seuraaja. EAP-TLS-protokolla muodostaa salatun TLS-tunnelin, jossa käyttäjän sertifikaatti lähetetään. (Brandon 2008, 342.)

Kuvassa 6 on esitetty EAP-TLS-tunnistusprosessin kulku.



Kuva 6. EAP-TLS-prosessi (Brandon 2008, 342).

1. Prosessi alkaa EAP Start-viestillä, jonka päätelaite lähettää tukiasemalle.
2. Tukiasema pyytää päätelaitteen tunnistetta.
3. Päätelaite lähettää käyttäjätunnisteensa tukiasemalle, joka välittää sen eteenpäin todennuspalvelimelle (RADIUS).
4. RADIUS-palvelin lähettää oman sertifikaattinsa. Tukiasema välittää viestin päätelaitteelle.
5. Päätelaite vastaa lähettämällä oman sertifikaattinsa, jonka tukiasema välittää RADIUS-palvelimelle.
6. Symmetriset istuntoavaimet lasketaan.
7. RADIUS-palvelin lähettää pääavaimen (Master Key) tukiasemalle.
8. Salauksen käyttö alkaa päätelaitteen ja tukiaseman välillä. Käytössä joko WEP- tai WPA/WPA2-salaus.

Yksi EAP-TLS-protokollan heikkouksista on se, että autentikoimisprosessi sisältää enemmän vaiheita kuin muut metodit, jolloin sen todennusprosessi kestää kauemmin. Tämä voi aiheuttaa ongelmia ympäristössä, jossa käyttäjät liikkuvat paljon ja voivat joutua useasti uudelleen tunnistamaan itsensä. (Frankel ym. 2007, 6-7.)

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) on laajennus EAP-TLS-protokollaan. Protokolla vaatii varmenteen käyttöä ainoastaan todentavalta palvelimelta, ei päätelaitteelta. Todentava palvelin autentikoidaan käyttämällä sen digitaalista sertifikaattia.

Tämän jälkeen salattu tunneli muodostetaan päätelaitteen ja todentavan palvelimen välille. Päätelaitteen autentikoituminen palvelimelle tapahtuu käyttämällä käyttäjätunnusta tai digitaalista sertifikaattia.

EAP-TTLS voi käyttää muitakin autentikointimenetelmiä, kuten Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP) ja Microsoft CHAP (MS-CHAPv2).

Koska vain palvelin huolehtii sertifikaateista, EAP-TTLS-protokolla on paljon helpompi hallita kuin esimerkiksi EAP-TLS. EAP-TTLS-protokollassa langattoman verkon ylläpitäjän ei tarvitse tehdä eikä hallita digitaalisia sertifikaatteja jokaiselle verkon päätelaitteelle. (Soyinka 2010, 171.)

EAP-PSK

EAP-Pre-Shared Key (EAP-PSK) on EAP-protokolla, joka käyttää hyväkseen PSK:ta (Pre-Shared Key). EAP-PSK on yksinkertaisempi toteutukseltaan sekä toiminnaltaan verrattuna EAP-TLS:ään tai EAP-TTLS:ään. Protokolla käyttää AES-salausmenetelmää (Advanced Encryption Standard), joka sopii useimmille laitteille ja on kevyt käyttää. (Soyinka 2010, 171.)

EAP-SIM

Tämä EAP-autentikointi tyyppi käyttää SIM-korttia (Subscriber Identity Module) käyttäjätietojen laillisuustarkastuksessa (Soyinka 2010, 172).

PEAP

PEAP (Protected EAP) on Microsoftin, RSA:n sekä Ciscon kehittämä autentikointimenetelmä. Se toimii samantapaisesti kuin EAP-TTLS eli siinä käytetään sertifikaattia, joka sijaitsee vain palvelimella. Tätä sertifikaattia käytetään muodostamaan salattu tunneli asiakkaan ja autentikointipalvelimen välille, jossa varsinainen tunnistus tapahtuu. Microsoftin Active Directory käyttää tunnistuksessa PEAP(MS-CHAPv2)-menetelmää. (Brandon 2008, 344.)

4 WINDOWS-PALVELIN

Val-Tradingissa on käytössä vain yksi pöytäkone, johon asennetaan Windows Server 2008 Enterprise -käyttöjärjestelmä.

Palvelimeen asennetaan:

- AD DS (Active Directory Domain Services)
- DNS (Domain Name System)

- DHCP (Dynamic Host Configuration Protocol)
- NPS (Network Policy Server)
- CA (Certificate Authority).

On suositeltavaa, että muut kuin Active Directory Domain Services (AD DS) ja Domain Name System (DNS) asennetaan eri palvelimille, jolloin vikatilanteessa verkko ei lamaannu täysin. Tässä opinnäytetyössä asennetaan kaikki palvelut vain yhdelle koneelle. Tulevaisuudessa tarkoituksena on hankkia myös toinen pöytäkone, jolla parannetaan verkon suorituskykyä.

4.1 Active Directory

Active Directory (AD) on käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. (Kivimäki 2005, 1.)

Active Directory pitää sisällään tietokonetilit, käyttäjätunnukset ja salasanat, joita vaaditaan 802.1X- ja PEAP-tunnistukseen langattomassa verkossa.

AD DS:ssä voidaan luoda ryhmiä, joiden avulla järjestelmänhallinta helpottuu. Ryhmälle voidaan sallia tai kieltää siltä pääsy tiettyihin verkon resursseihin. Esimerkiksi tässä opinnäytetyössä luodaan AD DS:ään langattoman verkon käyttäjille oma ryhmä.

Group Policy Objectin (GPO) eli tilikäytännön avulla voidaan muuttaa oikeuksia sekä asetuksia koskien yksittäistä käyttäjää, konetta tai ryhmää.

Tilikäytäntöjä voidaan muuttaa Group Policy Managementissa (GPM), joka on administrative tools -valikossa. Microsoft Management Console (MMC) on ohjelma, jonka avulla määritellään Group Policy -asetukset tietylle ryhmälle tai tietokonetilille.

4.2 DNS

Ennen Active Directoryn asennusta pitää palvelimelle asettaa DNS-palvelimen määritykset.

Active Directory käyttää DNS-järjestelmää (Domain Name System). DNS on standardi Internetin palvelu, joka organisoi tietokonejoukot toimialueiksi. DNS-toimialueen hierarkia määritellään Internetin laajuisesti ja eri hierarkiatasoilla tunnistetaan tietokoneet, organisatoriset toimialueet sekä ylätason toimialueet. DNS:ää käytetään isäntäkoneiden nimien muuntamiseen. Esimerkiksi google.com muunnetaan numeeriseksi TCP/IP-osoitteeksi (Transmission Control Protocol/Internet Protocol) 209.85.149.105. (Stanek 2003, 133.)

Kun Active Directory -toimialueessa viitataan tiettyyn tietokoneresurssiin, on käytettävä täyttä tietokoneen nimeä, esimerkiksi Kone.Yritys.com. Tässä Kone tarkoittaa yksittäisen tietokoneen nimeä, Yritys tarkoittaa organisatorista toimialuetta ja com on ylätason toimialue. Ylätason toimialueet ovat DNS-hierarkian juuressa ja niitä kutsutaan tämän vuoksi juuritoimialueiksi.

Nämä toimialueet on organisoitu maantieteellisesti kaksikirjaimisten maakoodien mukaan (esimerkiksi Suomen maakoodin fi), organisaation tyypin mukaan (esimerkiksi com kaupallisten organisaatioiden) sekä toiminnon mukaan (esimerkiksi mil USA:n armeijan käytössä). (Stanek 2003, 133–134.)

Tässä opinnäytetyössä palvelimeen asennetaan oma DNS-palvelin, jolloin sisäistä DNS-palvelua käytetään verkon asiakaskoneiden nimien selvitykseen ja ulkoista DNS-palvelua ulospäin Internetiin näkyvän palvelimen nimen selvitykseen.

4.3 DHCP

DHCP (lyhenne sanoista Dynamic Host Configuration Protocol) on verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita uusille lähiverkkoon kytkeytyville laitteille. Ylläpitäjä antaa tietyn IP-osoiteavaruuden,

jolloin jokainen laite pyytää käynnistyksen yhteydessä DHCP-palvelimelta oman IP-osoitteen.

Annettu osoite on voimassa ennalta määrätyn ajan. Kun ennalta määrätty aika on kulunut, kysyy IP-laite osoitteelle lisäaikaa. Menettely yksinkertaistaa asiakaskoneiden asetuksien hallintaa huomattavasti, koska koneille ei tarvitse määrittää osoitteita käsin. (DHCP 2011.)

Kun DHCP-palvelu on asennettu palvelimelle, DHCP-palvelin ylläpitää TCP/IP-verkon toiminnassa tarvittavia tietoja, joita ovat IP-osoite, aliverkon peite, oletusyhdyskäytävän osoite, ensisijaisen ja toissijaisen DNS-palvelimen osoite, ensisijaisen ja toissijaisen WINS-palvelimen osoite ja DNS-toimialueen nimi.

DHCP-palvelimelle määritellään jaettavat osoitealueet (scope), joista asiakaskoneille myönnetään IP-osoitelainoja ja -varauksia. Osoitealueiden avulla määritetään IP-osoitteet, jotka ovat DHCP-asiakkaiden käytössä. Tässä työssä osoitteet jaetaan C-luokan verkosta. (Stanek 2003, 443.)

4.4 NPS

NPS (Network Policy Server) on Microsoftin kehittämä täytäntöönpano, joka sisältää:

- RADIUS-palvelun (Remote Authentication Dial-In User Service)
- RADIUS-proxyn (Remote Authentication Dial-In User Service Proxy)
- NAP-palvelun (Network Access Protection).

Näiden palveluiden avulla NPS suorittaa keskitetyn yhteyksien autentikoinnin, auktorisoinnin sekä erilaisten verkonhallinnassa käytettävien tietokantojen ylläpidon. NPS korvaa aiemman IAS-palvelun, jota käytettiin Windows Server 2003 -käyttöjärjestelmässä. (Microsoft, Network Policy Server 2011.)

4.5 Varmenteet

Varmenne on luotettavan kolmannen osapuolen digitaalisesti allekirjoittama todistus siitä, että tietty julkinen avain kuuluu tietylle avaimen käyttäjälle.

Julkisen avaimen lisäksi varmenne sisältää myös muita tietoja, kuten esim. 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. (Viestintävirasto, varmenne 2011.)

Tässä opinnäytetyössä käytetään varmenneviranomaisena omaa Windows-palvelinta. Varmenneviranomainen lisätään palvelimeen ottamalla käyttöön Active Directory Certificate Services (AD CS). Oman varmenteen käyttö on edullinen vaihtoehto näin pienessä yrityksessä, mutta sen joutuu asentamaan manuaalisesti.

Käytettävissä olevia autentikoimistapoja varmenteen kanssa ovat EAP sekä PEAP. EAP:ssa voidaan määritellä tyypiksi TLS ja PEAP:ssa TLS sekä MS-CHAP v2.

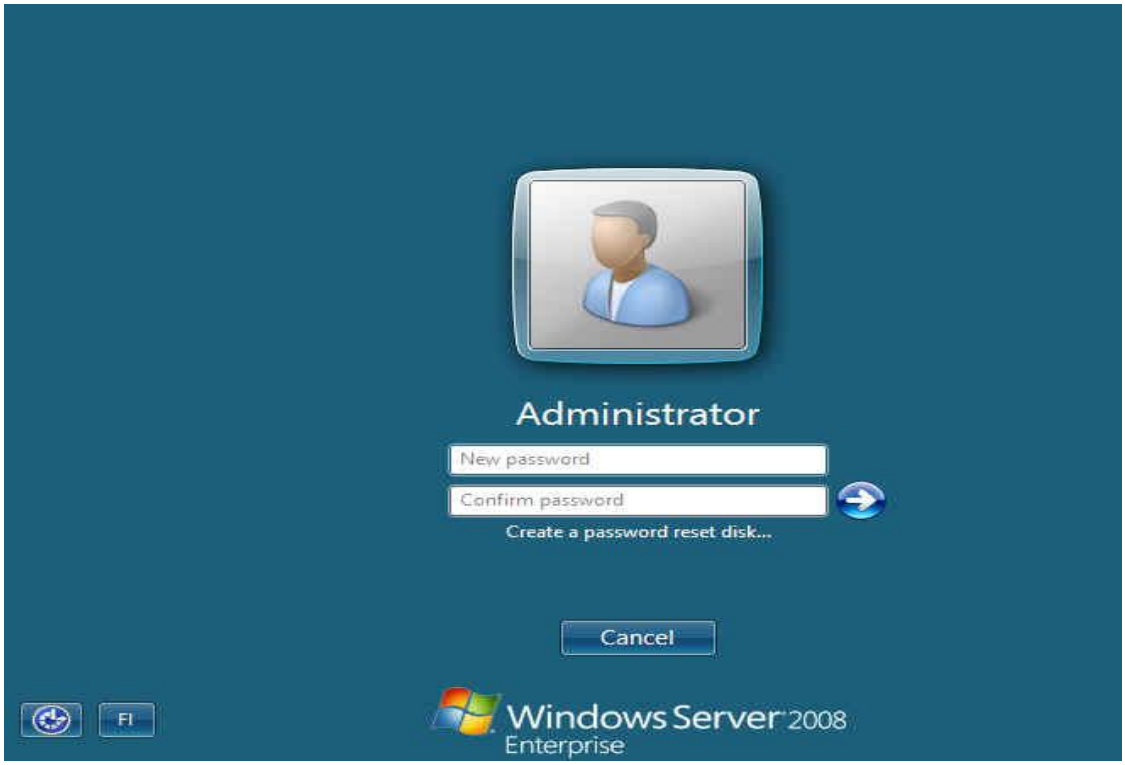
5 Asennus

Asennusvaihe aloitetaan asentamalla Val-Tradingin pöytäkoneeseen Windows Server 2008 Enterprise. Langaton tukiasema liitetään langalliseen verkkoon, josta se on yhteydessä palvelimeen. Kaikki langattomat laitteet, joita yrityksessä käytetään tai tullaan käyttämään, liittyvät langattomaan tukiasemaan.

5.1 Aloitustoimenpiteet

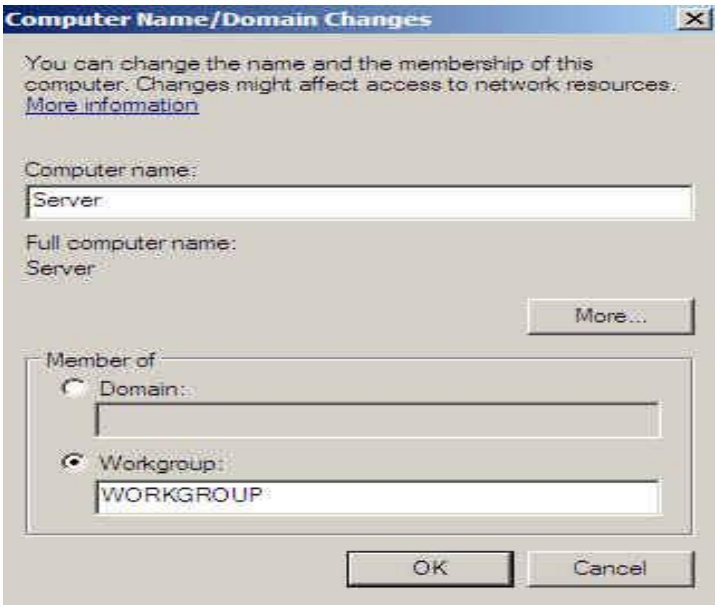
Windows Server 2008:n asennuksen jälkeen palvelimelle määritetään järjestelmänvalvojan salasana, tietokoneen nimi ja IP-osoite (kuva 7).

Järjestelmänvalvojan salasanan pitää täyttää Windowsin vaatimukset sisältämällä isoja ja pieniä kirjaimia, sekä numeroita ja erikoismerkkejä.



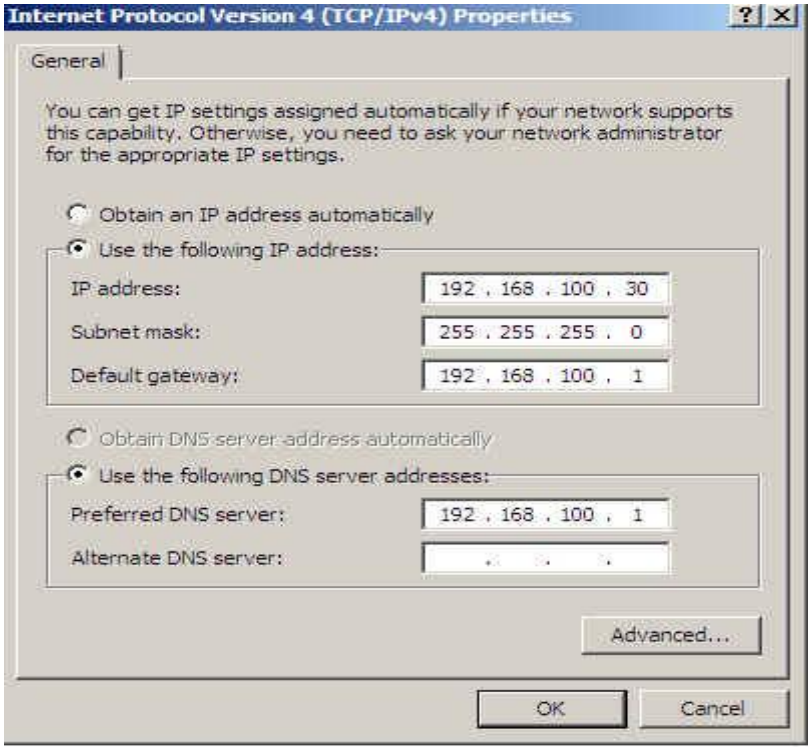
Kuva 7. Järjestelmänvalvojan salasanan muuttaminen.

Windows Serverin asetuksista vaihdetaan tietokoneen nimi, jotta se on paremmin tunnistettavissa verkossa (kuva 8). Tietokoneen nimeä ei voi vaihtaa enää toiminimen (Domain Name) asennuksen jälkeen.



Kuva 8. Tietokoneen nimen vaihto.

IP-osoitteen määritykset suoritetaan palvelimen verkkoasetuksista, joista valitaan verkkokortin asetukset. Vaihdetaan palvelimen IP-osoite staattiseksi, jolloin se pysyy samana DHCP:n ollessa päällä (kuva 9).

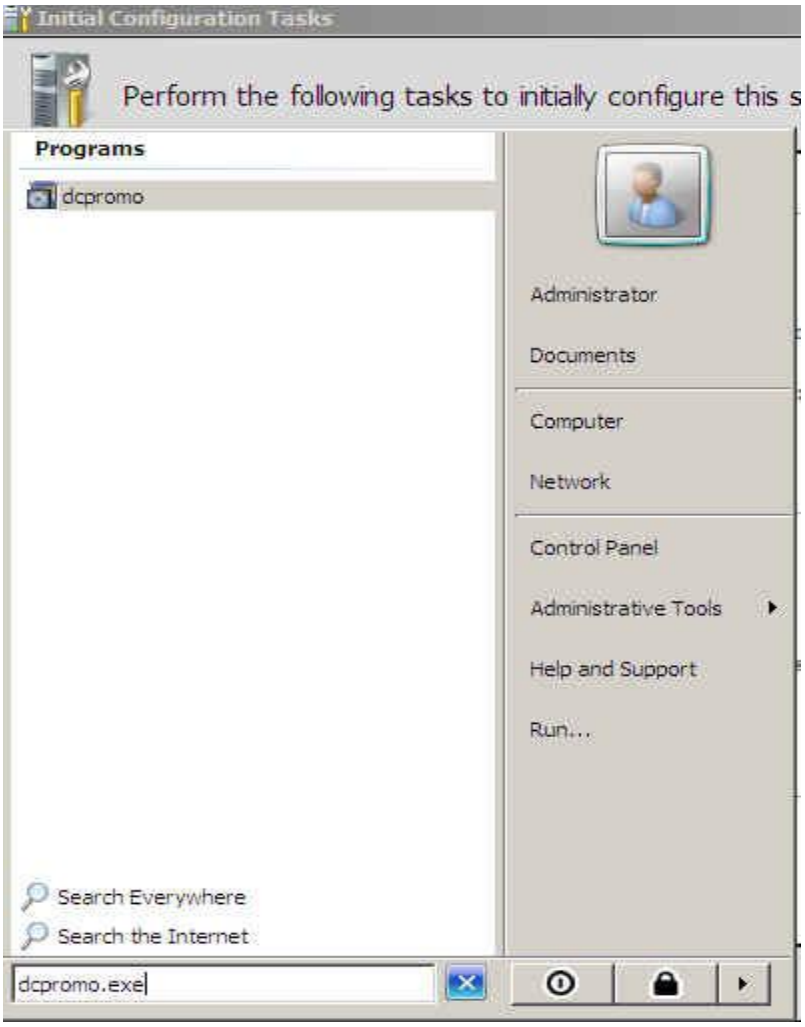


Kuva 9. IP-osoitteen vaihto.

5.2 Active Directory, AD CS ja DNS

Palvelimeen asennetaan Active Directory (AD), Active Directory Certificate Services (AD CS) sekä Domain Name System (DNS). Val-Tradingissa on käytössä Windows Server 2008 Enterprise -versio, joka tukee automaattista sertifikaattien latausta PEAP-TLS-autentikoinnissa.

Active Directory Domain Services (AD DS) käyttöönotto aloitetaan kirjoittamalla komentokehotteeseen ”dcpromo.exe” (kuva 10).

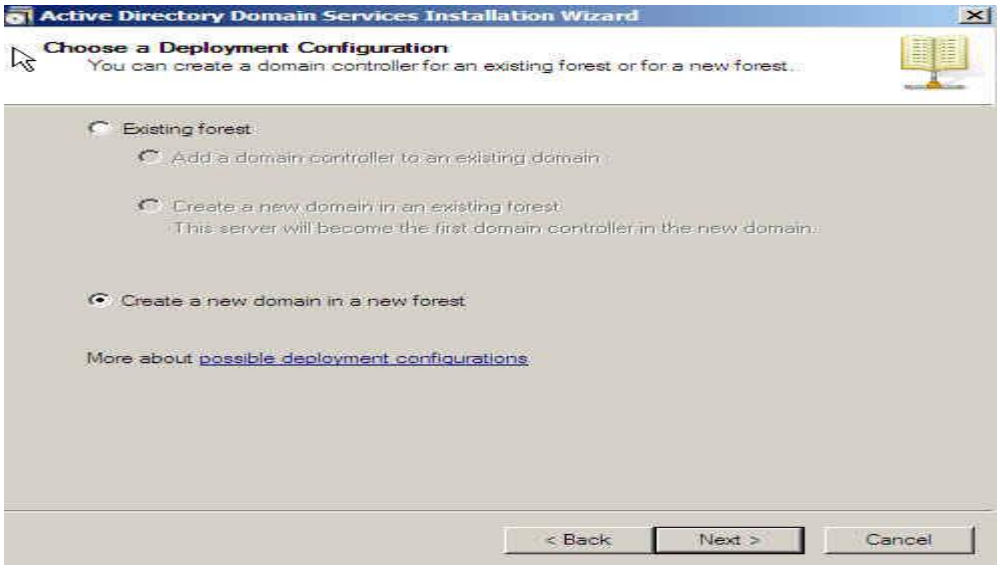


Kuva 10. AD DS:n asennuksen aloitus.

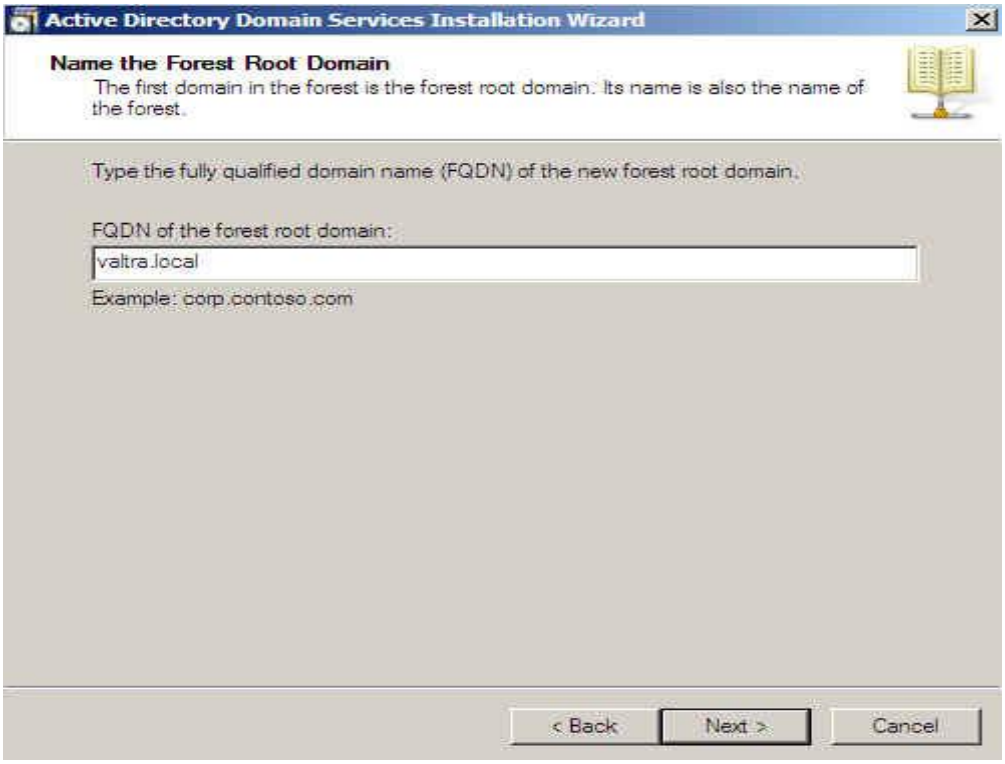
Seuraavaksi käynnistyy asennusvelho, jossa asennus tehdään ilman advanced-vaihtoehtoa (kuva 11).

Kuva 11. Asennusvelho AD DS.

Luodaan uusi toimialue uuteen metsään (New Forest) ja annetaan toimialueelle nimi, mihin langattomat päätelaitteet tulevat liittymään (kuva 12 ja kuva 13).

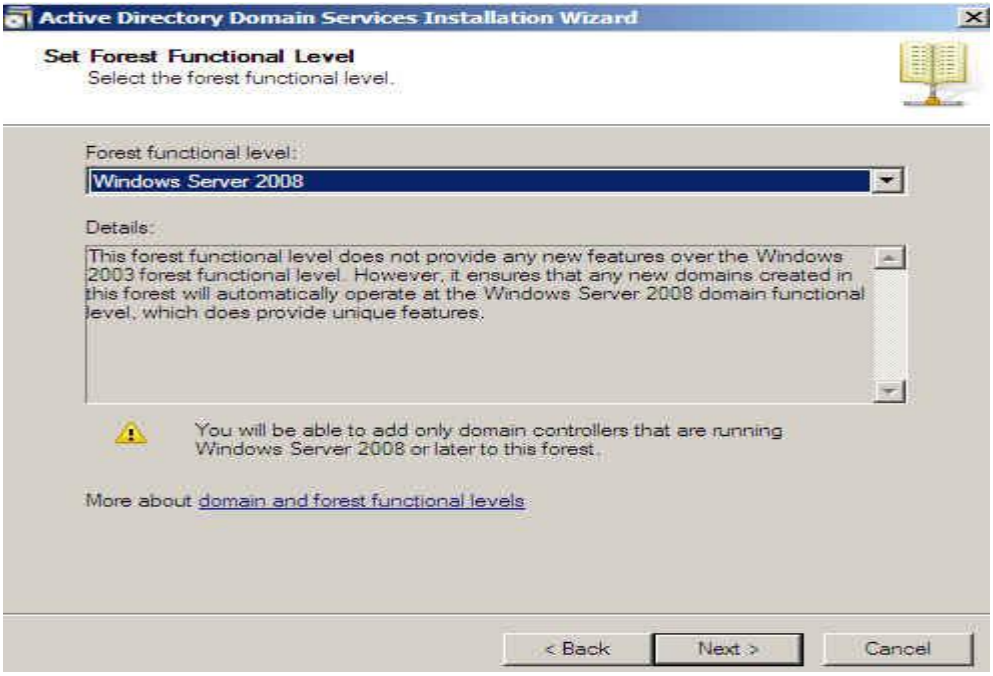


Kuva 12. Uuden toimialueen luonti.



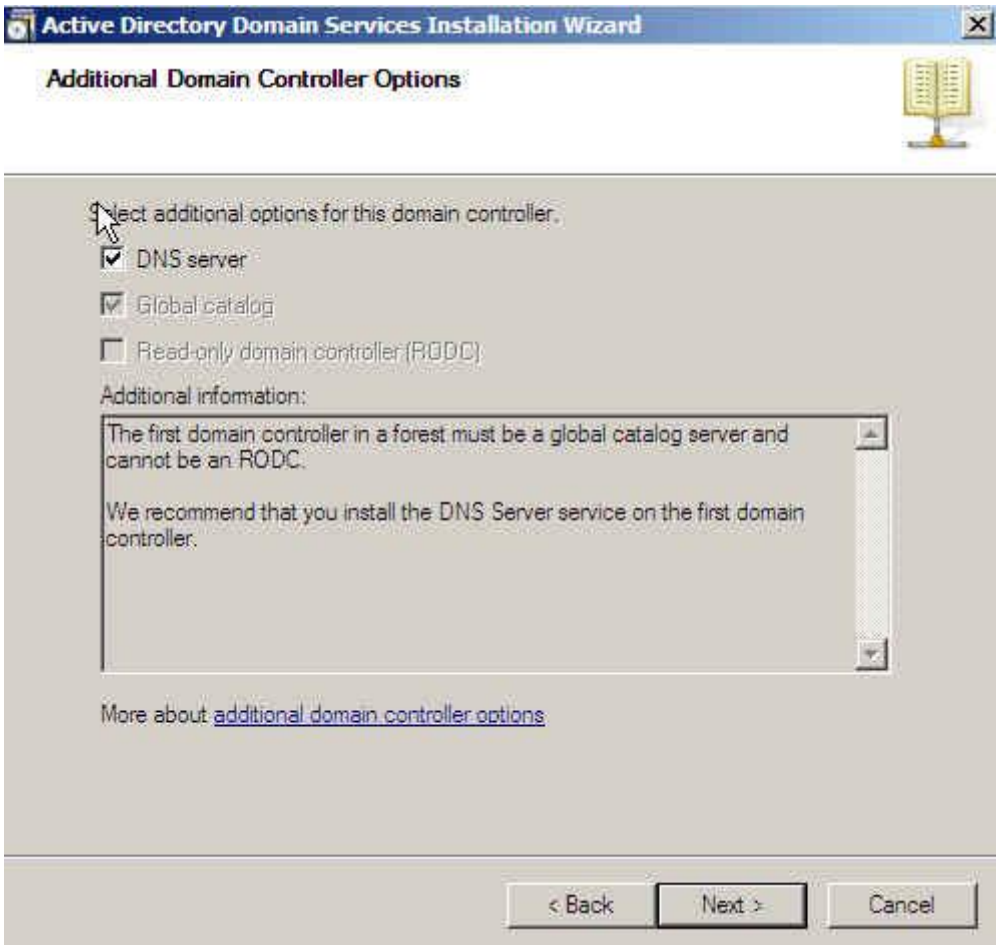
Kuva 13. Toimialueen nimeäminen.

Koska Val-Tradingissa ei ole käytössä kuin Windows Server 2008 -versio, valitaan Forest Functional Leveliksi pelkästään Server 2008 (kuva 14).



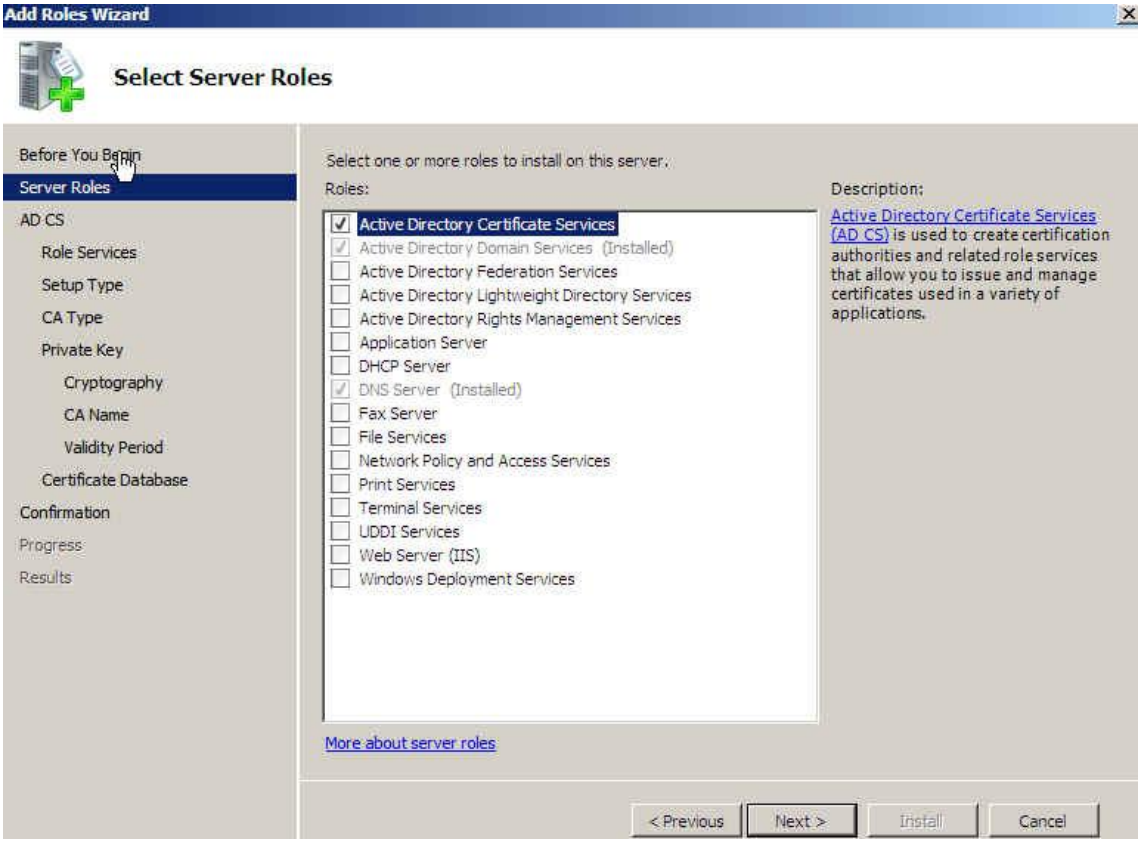
Kuva 14. Forest Functional Level.

Windows suosittelee DNS-palvelun asentamista palvelimelle asennuksen tässä vaiheessa, muutoin se pitää asentaa manuaalisesti myöhemmin (kuva 15).



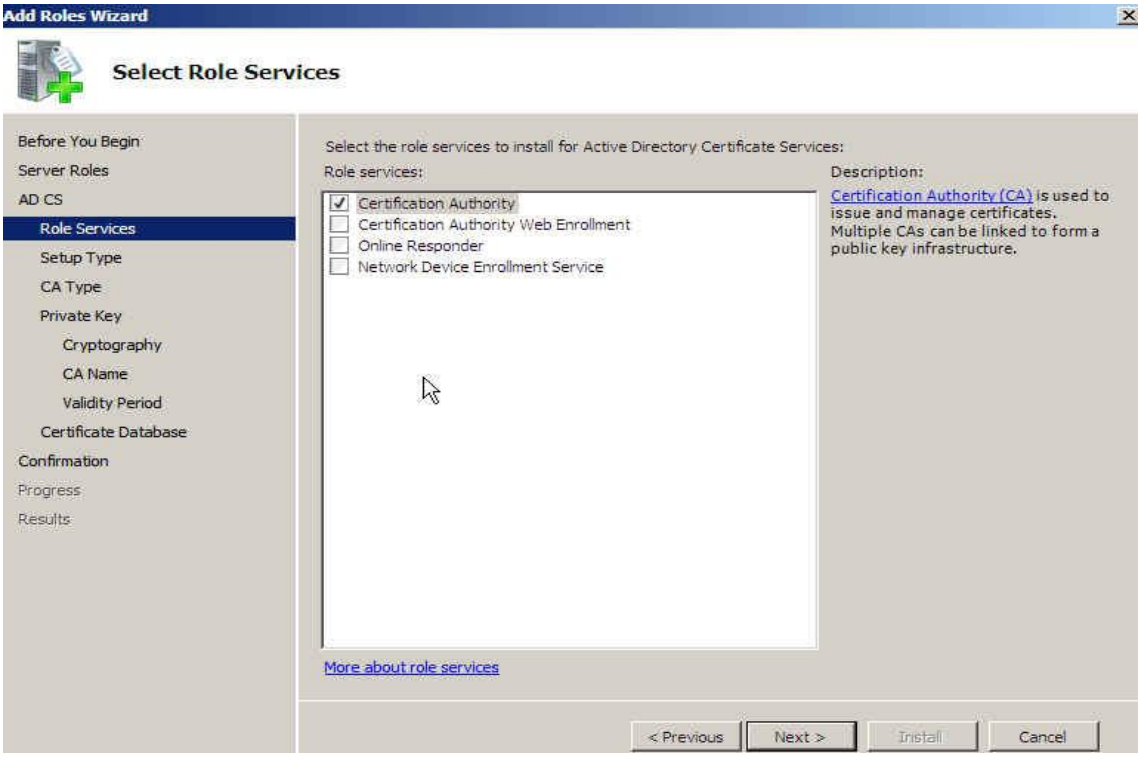
Kuva 15. DNS-palvelun asennus.

Active Directory Certificate Services (AD CS)-palvelu asennetaan Server Managerin avulla käyttämällä ”Add Roles Wizard”-toimintoa (kuva 16).

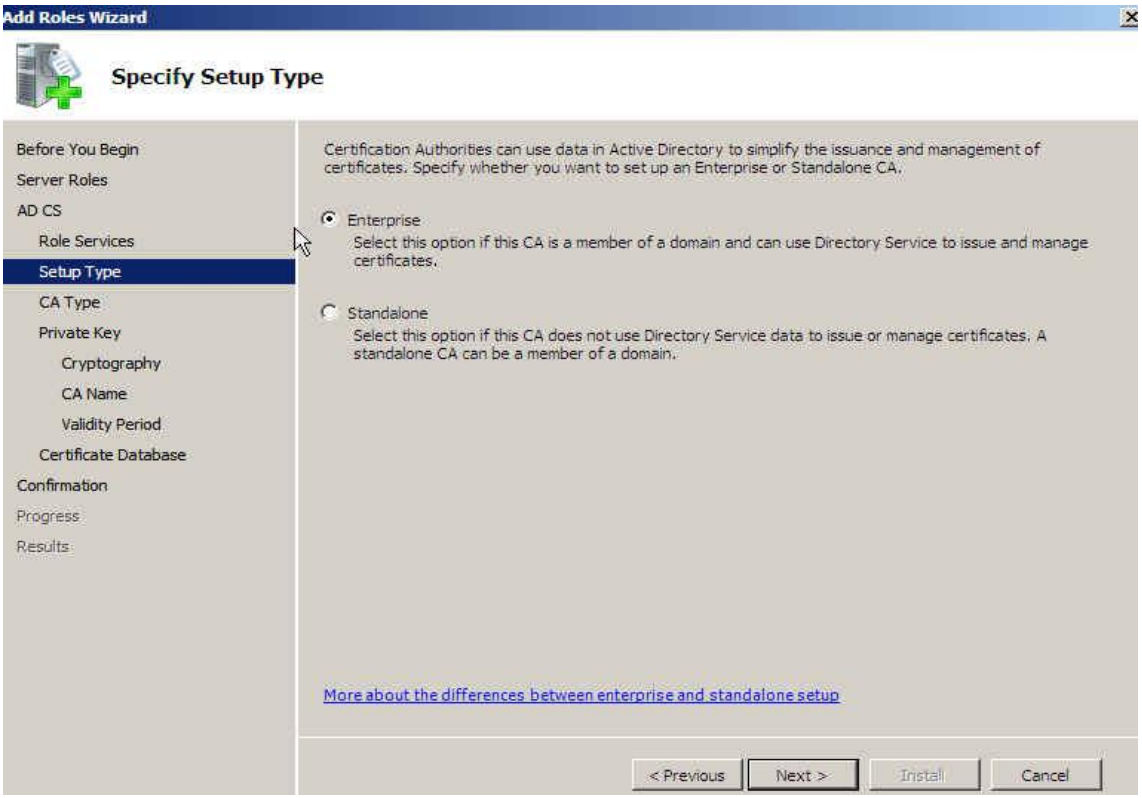


Kuva 16. AD CS-palvelun asennus.

Varmenneviranomainen (CA) valitaan asennettavaksi (kuva 17) ja varmennetyypiksi valitaan Enterprise (kuva 18). Tällöin käytetään Active Directorya varmenteiden hallintaan.

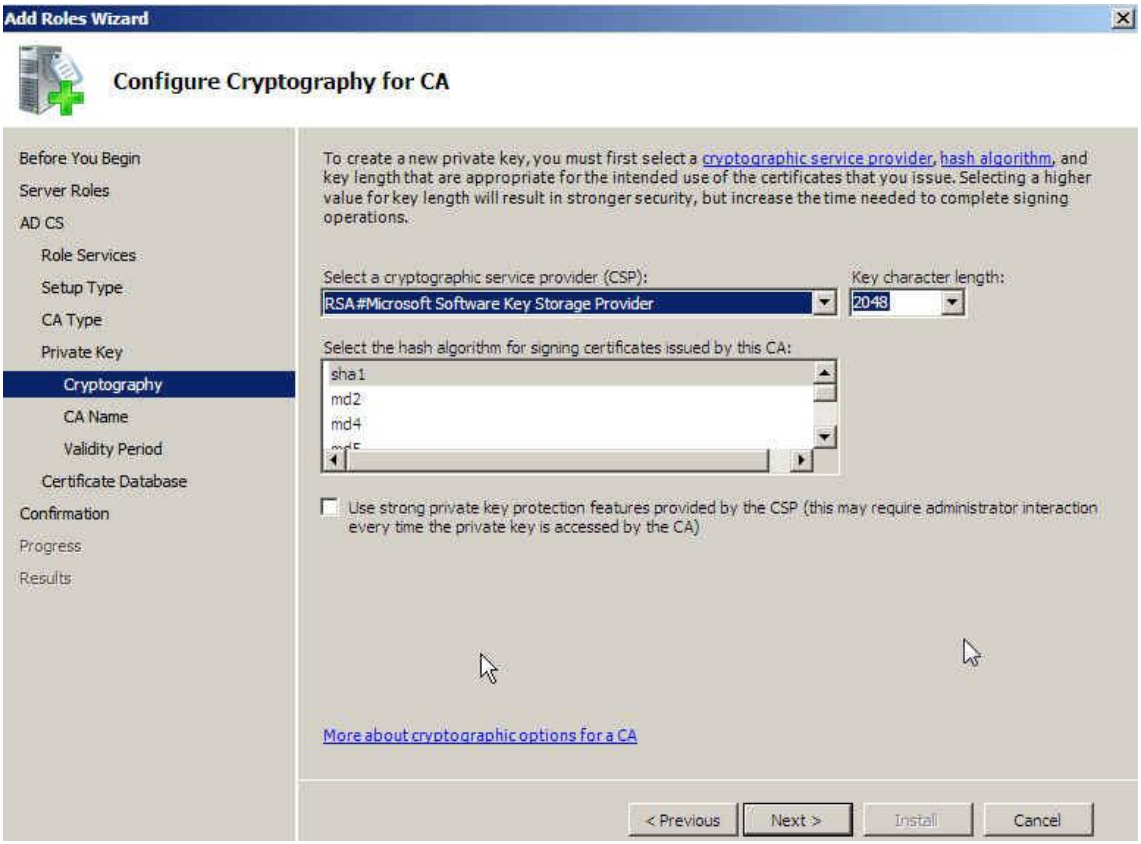


Kuva 17. Varmenneviranomaisen (CA) asennus.



Kuva 18. Varmennetyypin (Enterprise) valinta.

Asennetaan juurivarmenne (Root CA) ja valitaan sille oletuksena olevat suojausarvot. Salausmenetelminä käytetään Microsoftin Software Key Storage Provideria (RSA), joka käyttää 2048 bittistä salausavainta sekä Secure Hash Algorithm 1 (SHA1) -algoritmia (kuva 19).

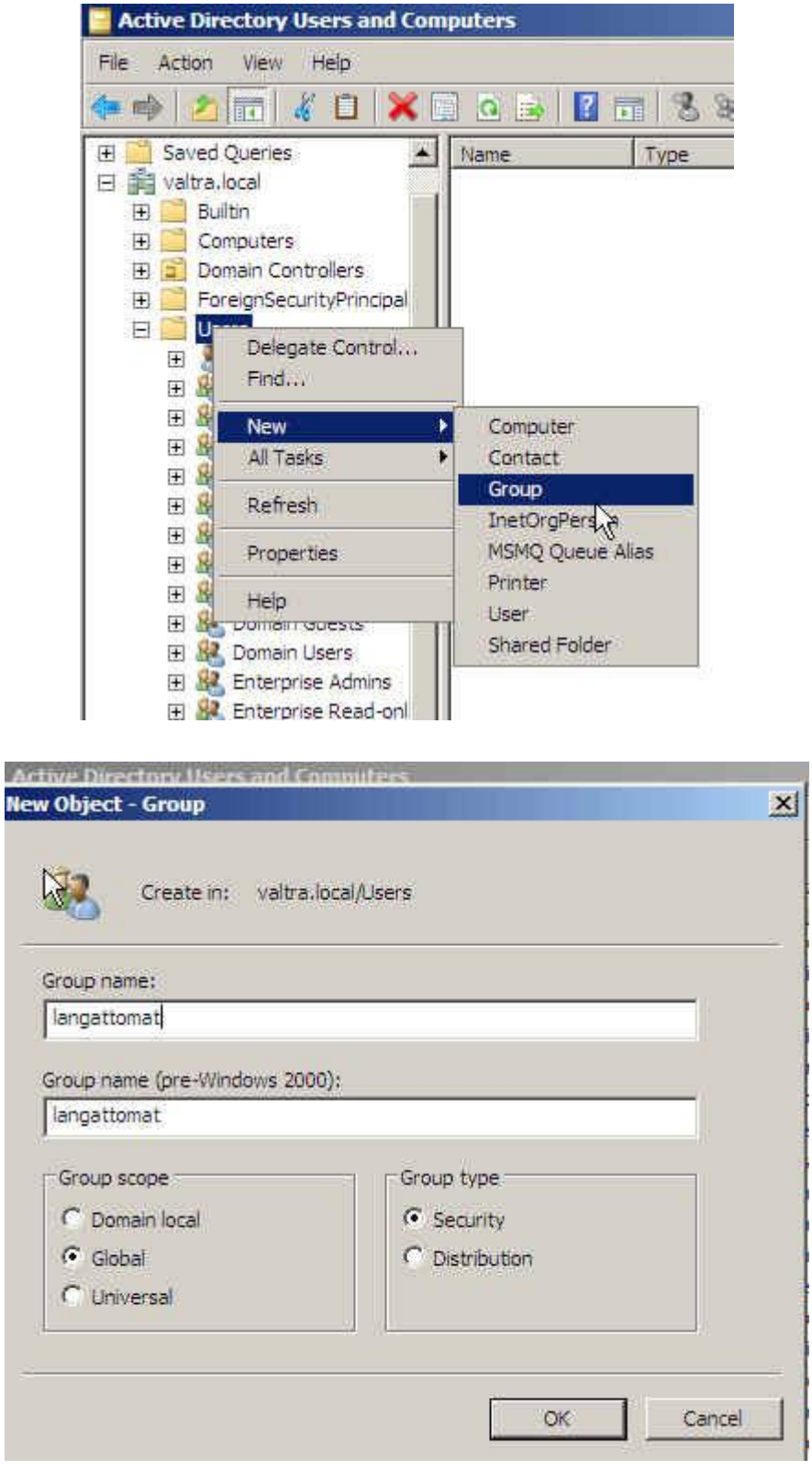


Kuva 19. Suojausarvojen valinta.

Ryhmien ja käyttäjien luonti Active Directoryyn

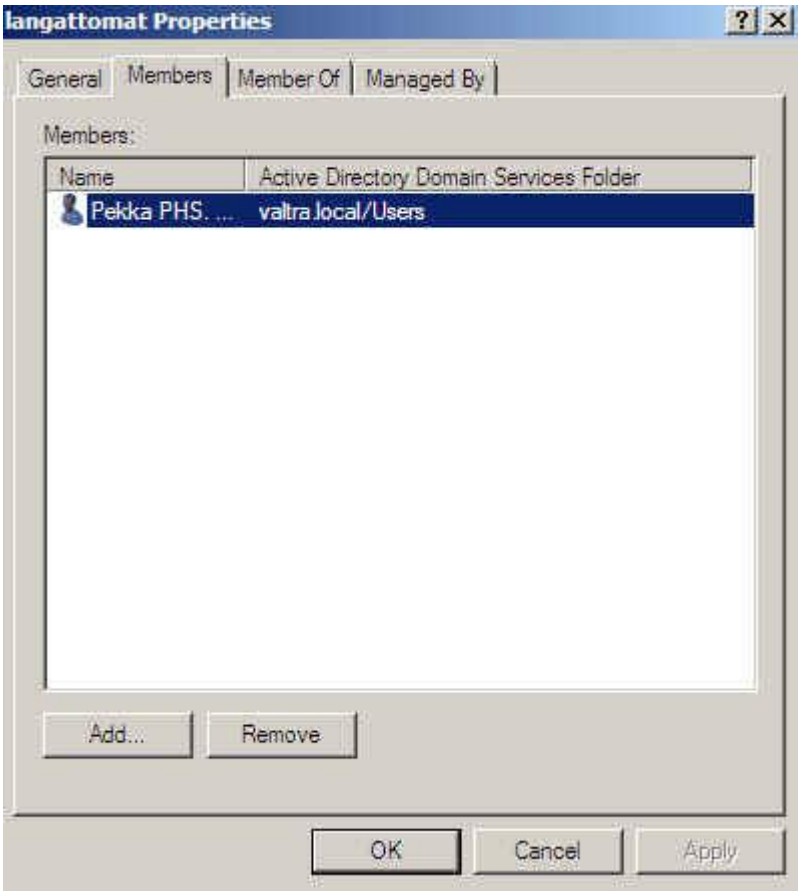
Active Directoryyn lisätään ryhmä ”langattomat”, johon lisätään Val-Tradingin kannettavat tietokoneet sekä niiden käyttäjät. Tässä vaiheessa ei vielä lisätä vieras-tiliä, joka mahdollistaa langattoman verkon käytön myös yrityksessä vieraileville.

Uusi ryhmä luodaan Active Directory Users and Computers-valikon kautta (kuva 20).



Kuva 20. Ryhmän luonti langattomille käyttäjille.

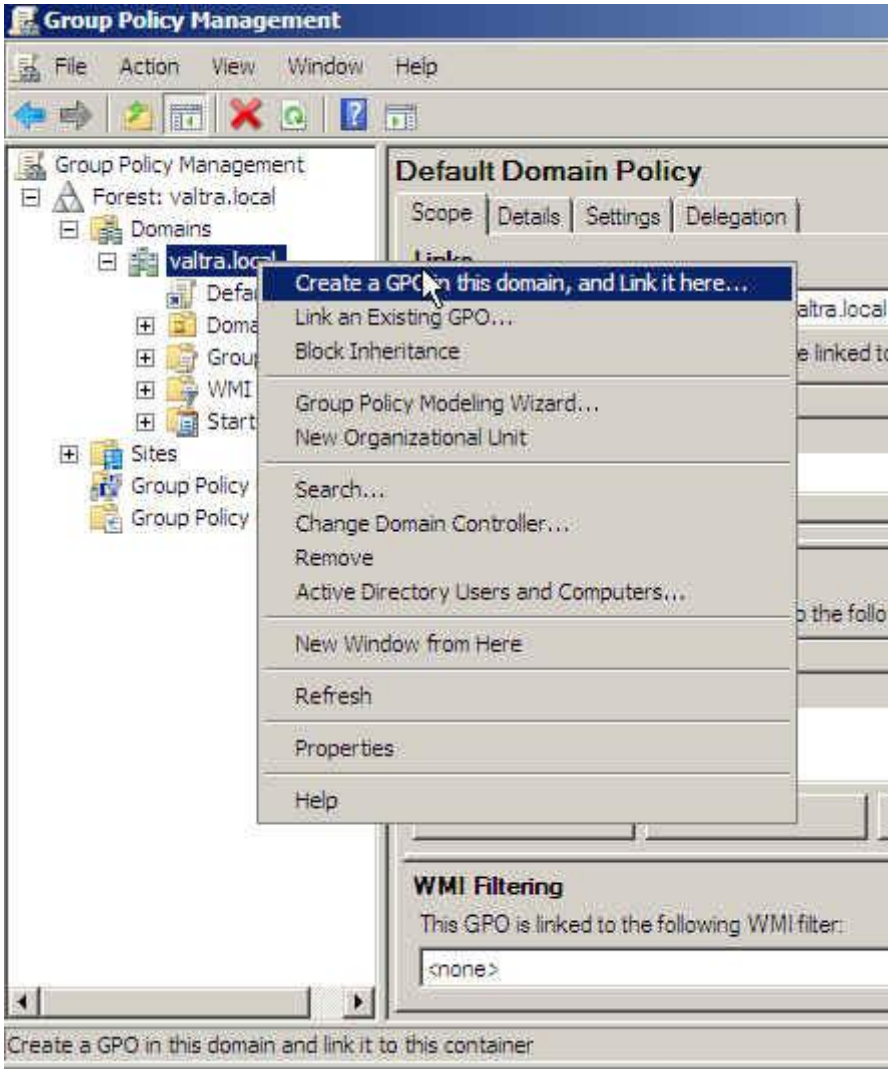
Käyttäjän lisääminen Active Directoryyn tapahtuu samalla tavalla, valitsemalla ”New” ja ”User”. Tämän jälkeen luotu käyttäjä siirretään ”langattomat”-ryhmään. Tietokoneiden lisääminen ”langattomat”-ryhmään tapahtuu sen jälkeen, kun se on lisätty valtra.local-toimialueeseen (kuva 21).



Kuva 21. Käyttäjän lisäys ”langattomat”-ryhmään.

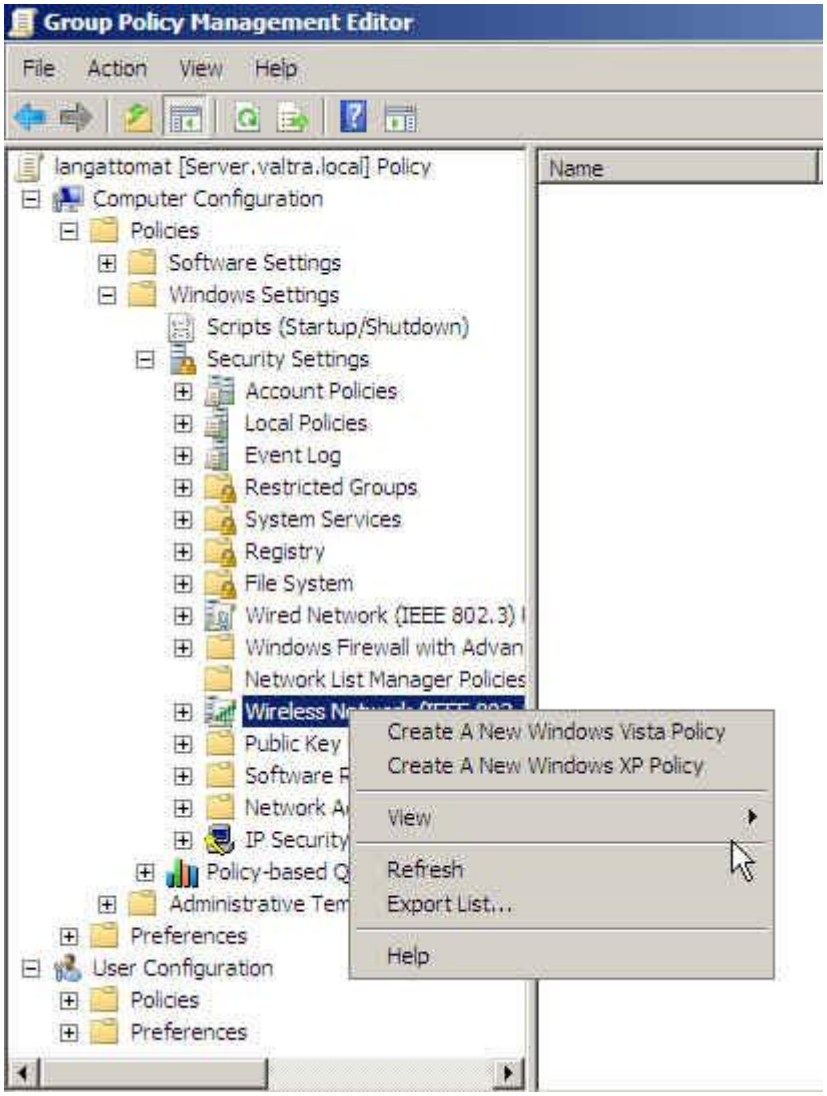
Ryhmäkäytännöt

Valtra.local-toimialueelle luodaan ryhmäkäytäntö, jonka avulla langattomien laitteiden käyttäjät voivat kirjautua langattomaan verkkoon. Määritykset tehdään luomalla uusi Group Policy Object (GPO) valtra.local-toimialueeseen käyttämällä Group Policy Management -työkalua (GPM) (kuva 22). GPM:n avulla luodaan uusi käytäntö, jossa varmenne latautuu automaattisesti valtra.local-toimialueeseen liittyvälle langattomalle laitteelle. Kun määritys on tehty, kaikki toimialueen koneet saavat tietokonevarmenteen, kun GPO on päivitetty palvelimelta.



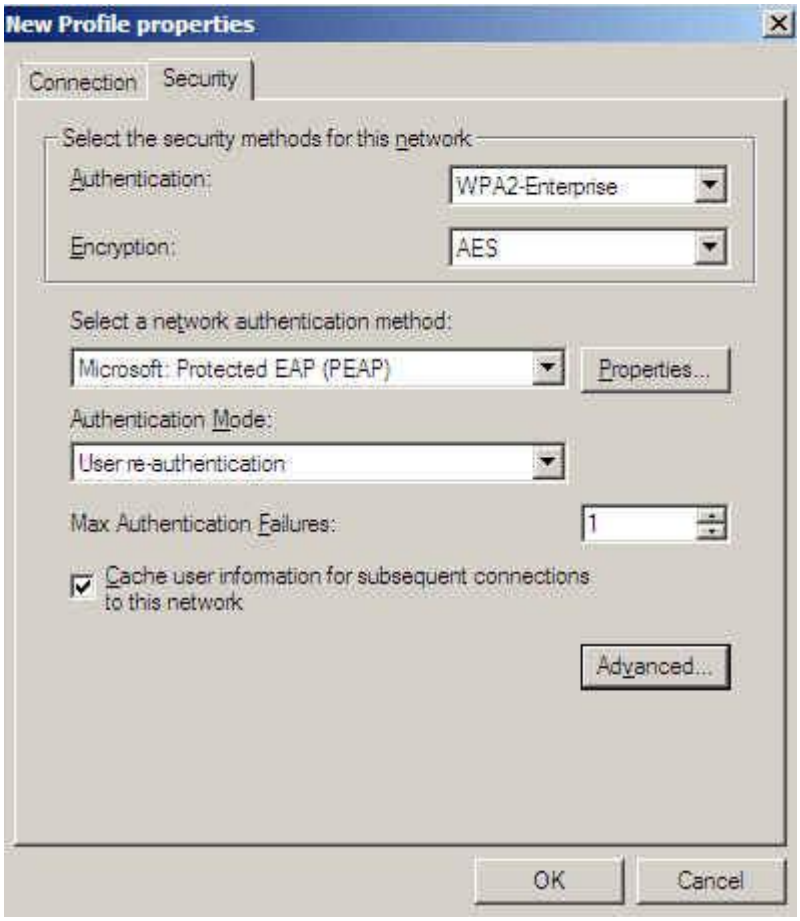
Kuva 22. Uuden GPO:n luonti.

Group Policy Management Editor (GPME) -työkalun avulla määritetään uusi ”langattomat”-käytäntö (kuva 23). Kun langaton laite kirjautuu Windowsiin valtra.local-toimialueessa, latautuu samalla uusi käytäntö. Koska käytössä on uudet, vastikään hankitut langattomat tietokoneet, joissa on Windows 7-käyttöjärjestelmät, valitaan käytäntö Windows Vistalle. Käytäntö on tarkoitettu Windows Vistalle sekä sitä uudemmille käyttöjärjestelmille, kuten Windows 7.



Kuva 23. “langattomat”-käytännön luominen GPME:n avulla.

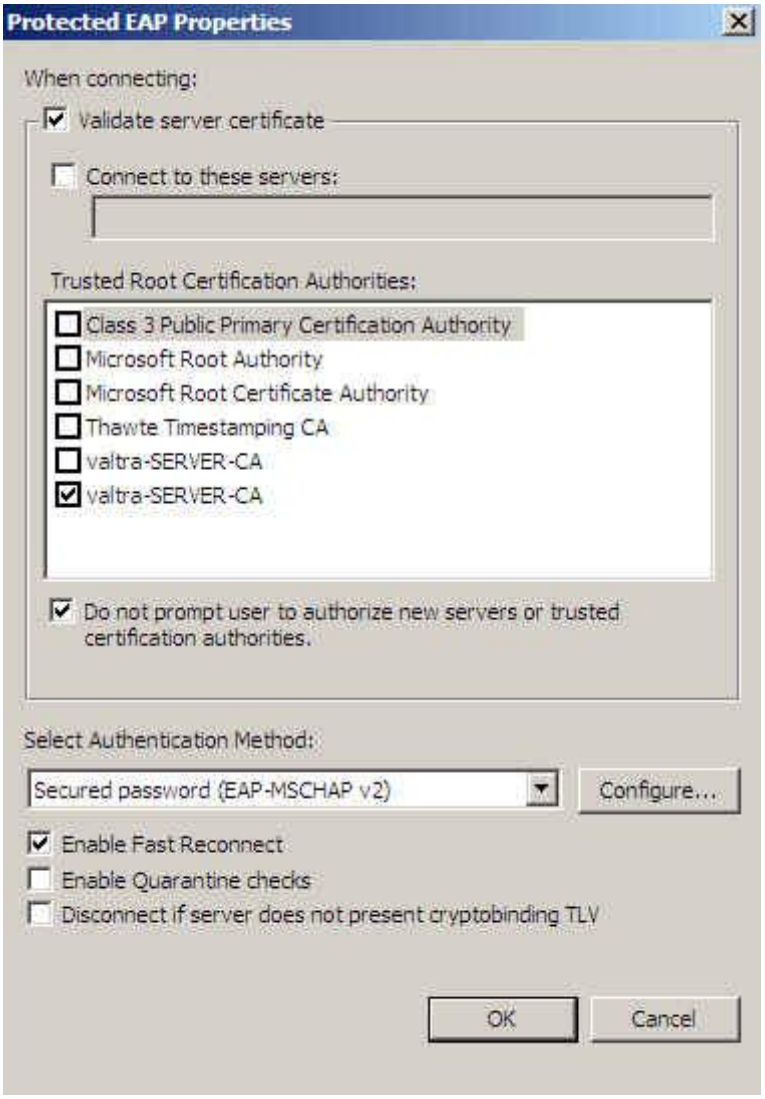
Uuteen ”langattomat”-käytännön profiiliin luodaan langattoman tukiaseman määritykset. Valitaan turvallisuusasetuksiksi WPA2-Enterprise, AES-salaus sekä langattoman verkon autentikointimenetelmäksi Protected EAP (PEAP) (kuva 24).



Kuva 24. ”Langattomat”-käytännön turvallisuusasetukset.

Protected EAP-ominaisuuksista määritellään varmenteeksi valtra-varmenneviranomainen (CA), joka asennettiin palvelimelle aikaisemmin. Valitaan myös vaihtoehto, jossa toimialueeseen kirjautuva langaton laite käyttää ainoastaan valtra-varmenneviranomaista eikä palvelin yritä ehdottaa laitteelle jonkun muun varmenteen käyttöä (kuva 25).

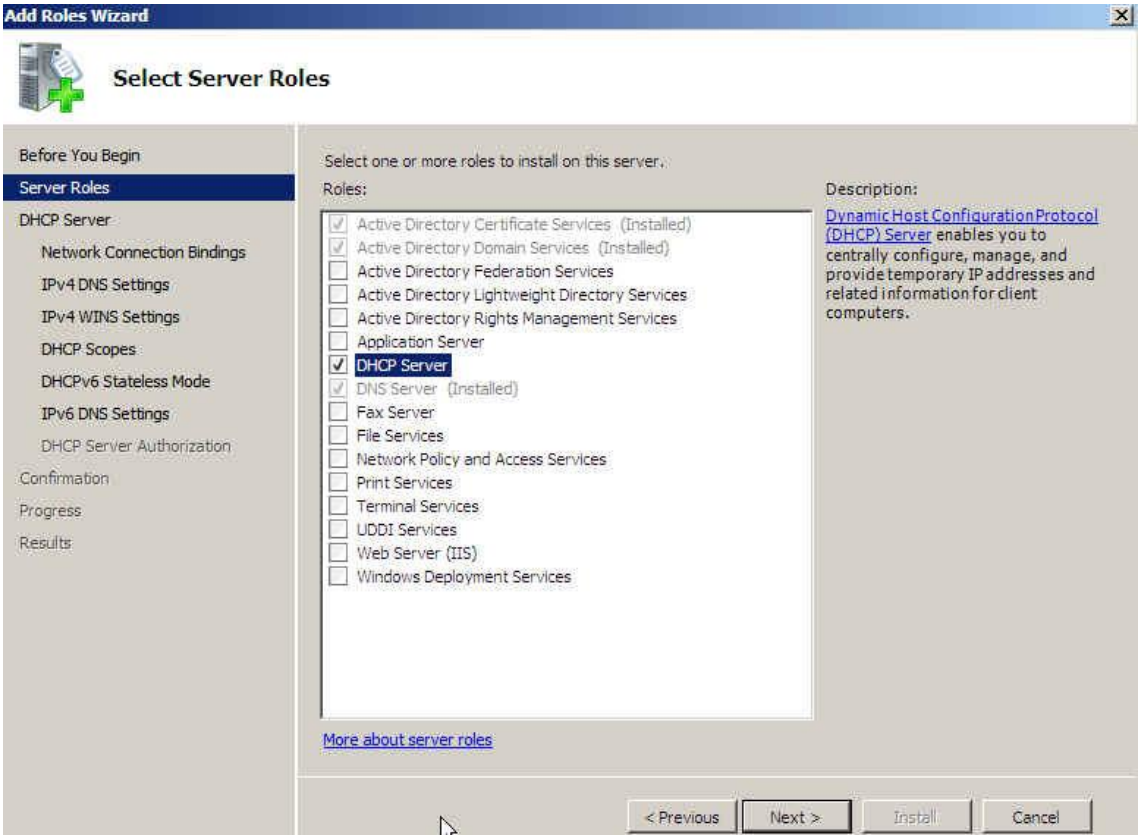
Tällä vaihtoehdolla parannetaan yhteyden tietoturvallisuutta, koska käytetään vain luotettua varmennetta. PEAP-protokollan avulla käyttäjät voivat käyttää verkkoon autentikoituessaan Windows-verkon kirjautumisnimeä ja salasanaa. Kirjautumisnimi ja salasana tarkistetaan Windowsin Active Directorystä.



Kuva 25. Valtra-varmenteen valinta ”langattomat” käytäntöön.

5.3 DHCP

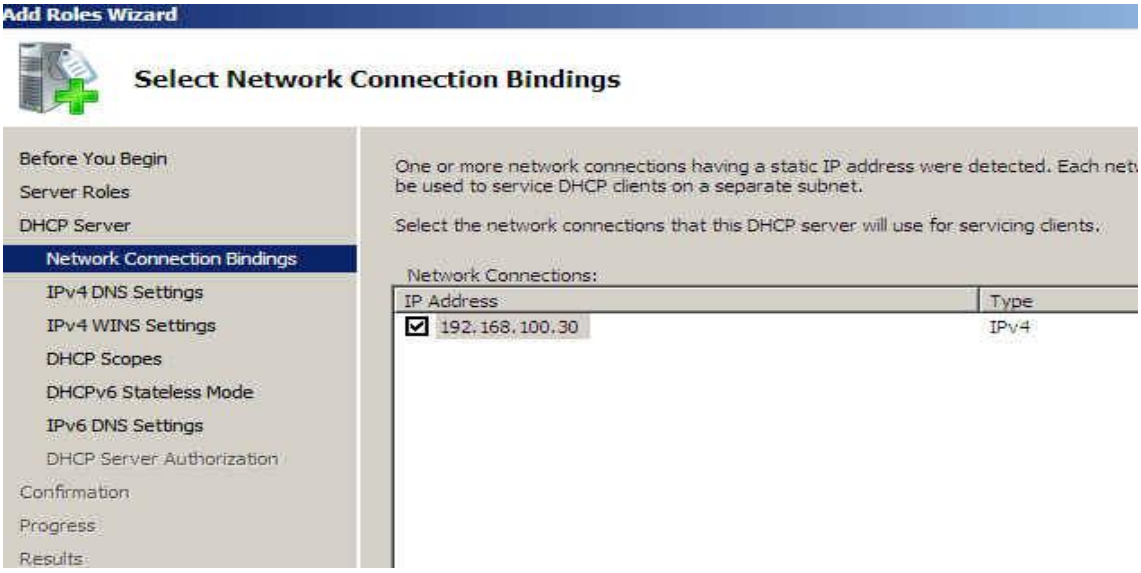
Asennetaan DHCP-palvelu Server Managerin kautta ja valitaan Add Roles Wizard-toiminto (kuva 26).



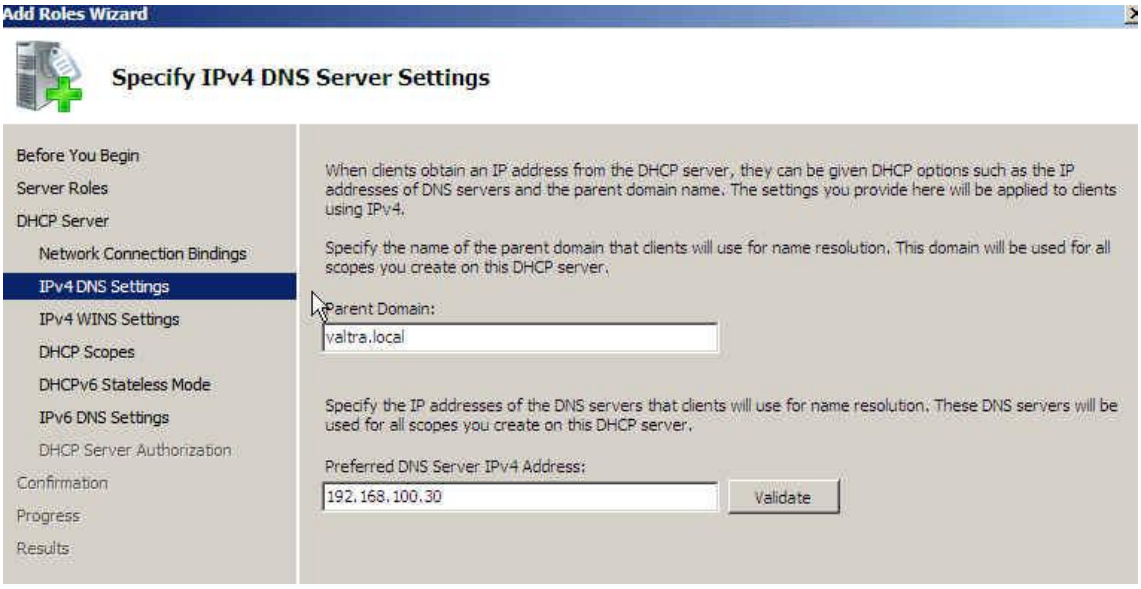
Kuva 26. DHCP-palvelun asennus Add Roles Wizardilla.

Asennuksen käynnistyttyä DHCP-asetuksiin määritellään:

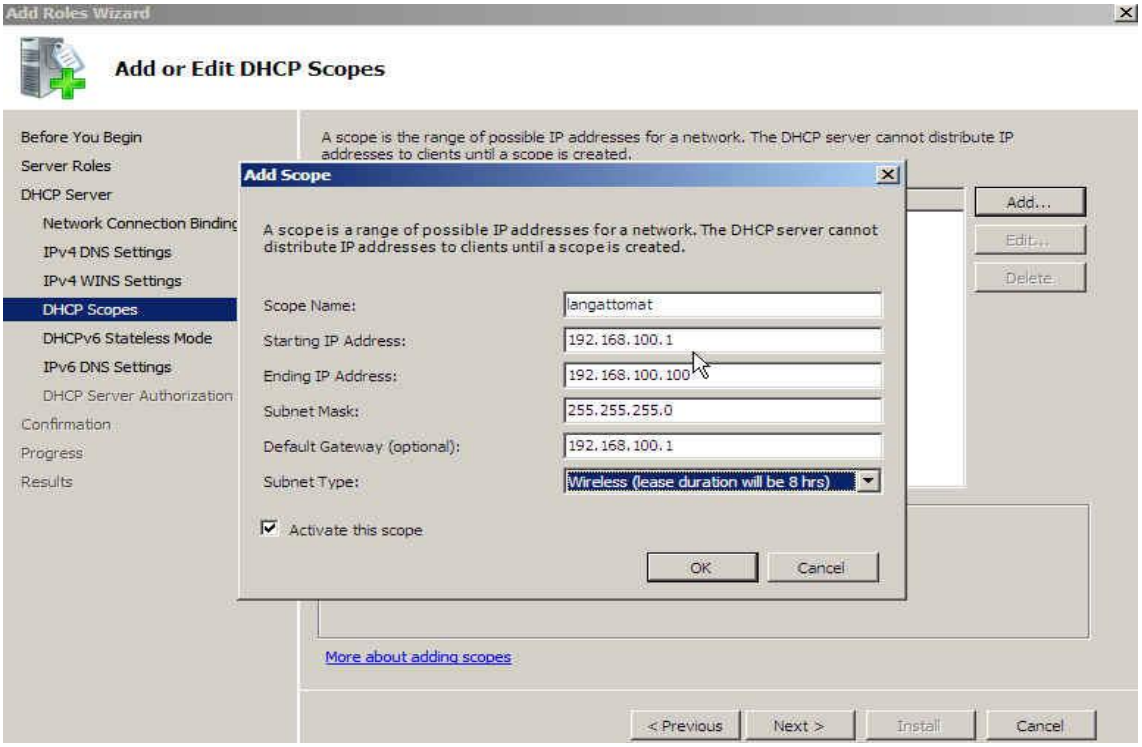
- palvelimen IP-osoite (kuva 27)
- toimialueen nimi ja IP-osoite (kuva 28)
- WINS-asetukset (ei oteta käyttöön)
- IP-osoiteavaruus langattomille yhteyksille (kuva 29)
- DHCPv6 protokollan määritykset
- järjestelmänvalvojan oikeudet.



Kuva 27. Palvelimen IP-osoite.



Kuva 28. Toimialueen nimi ja IP-osoite.

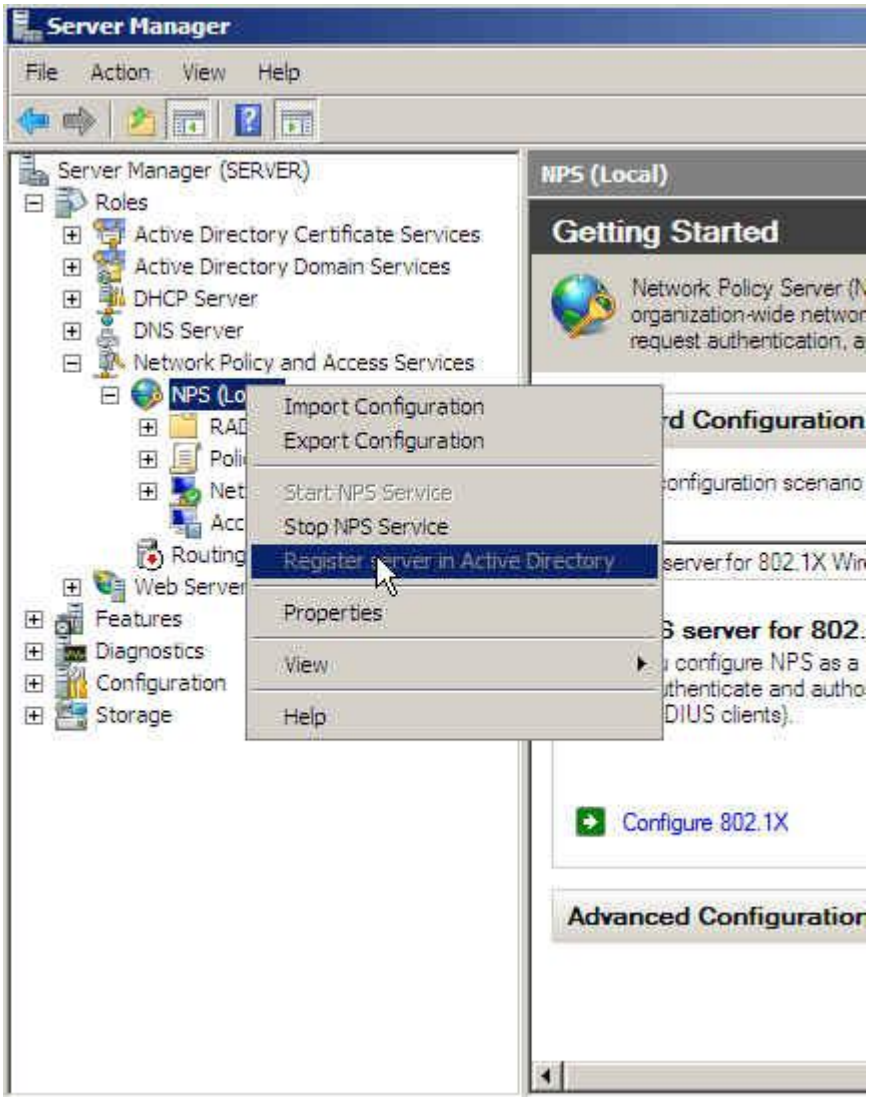


Kuva 29. IP-osoiteavaruuden määritys langattomille yhteyksille.

DHCP-palvelin pitää varmentaa Active Directory Domain Services -palvelussa (AD DS) ennen kuin se voi palvella asiakkaitaan.

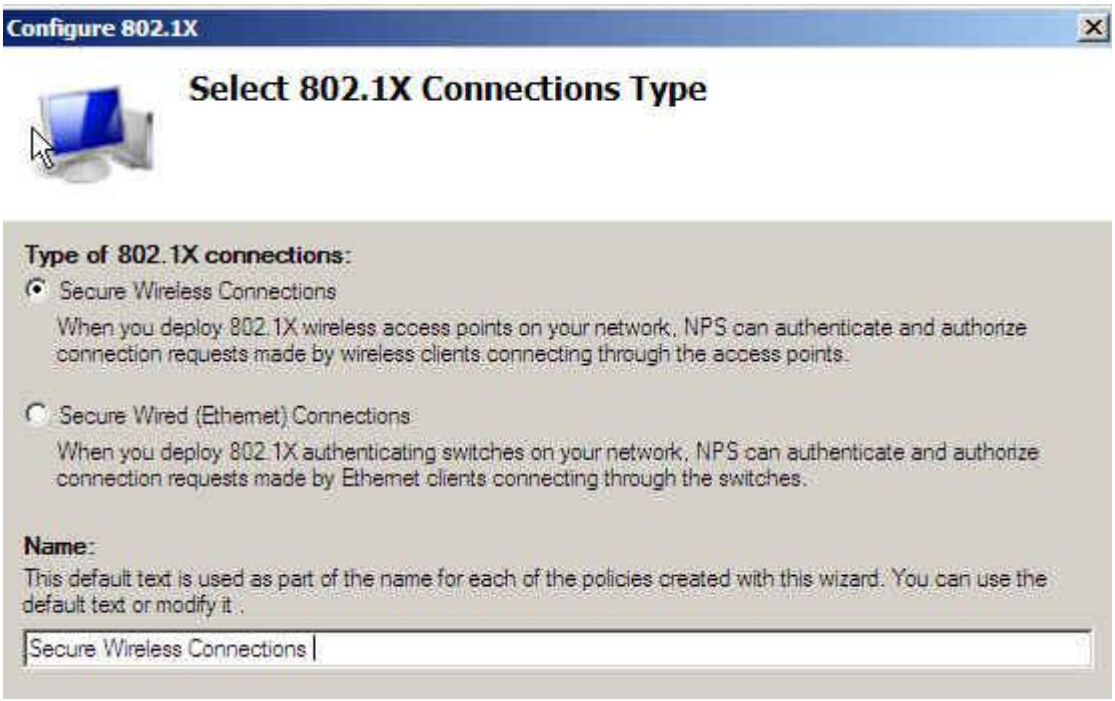
5.4 Network Policy Server (NPS)

Network Policy Server asennetaan Server Managerin avulla. NPS-palvelu liitetään Active Directoryyn NPS:n asetuksista (kuva 30). Palvelu käyttää Active Directoryä autentikoimiseen sekä oikeuksien jakamiseen.



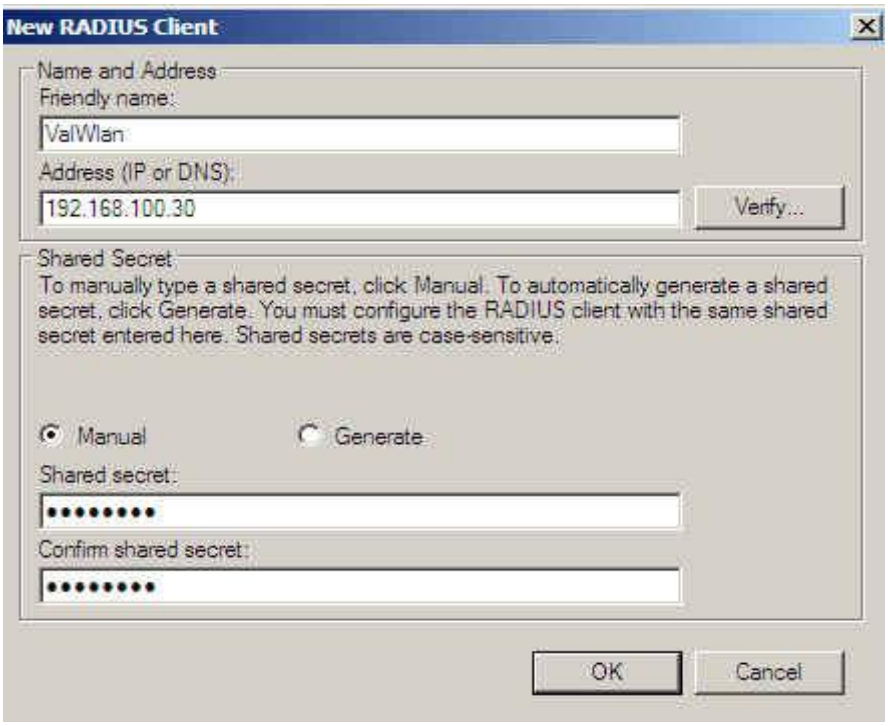
Kuva 30. NPS-rekisteröinti Active Directoryyn.

NPS-palveluun määritetään käytettävä 802.1X-yhteyden tyyppi (kuva 31).



Kuva 31. 802.1X -yhteyden tyyppi.

Seuraavaksi määritetään RADIUS-asiakkaan tiedot. Määritettäviä tietoja ovat tukiaseman SSID-tunnus, IP-osoite sekä Shared Secret -salasana. Sama salasana määritellään myöhemmin tukiasemaan. Valitsin käytettäväksi oman, manuaalisen salasanan (kuva 32). Vaihtoehtoisesti voi käyttää Windowsin generoimaa salasanaa.

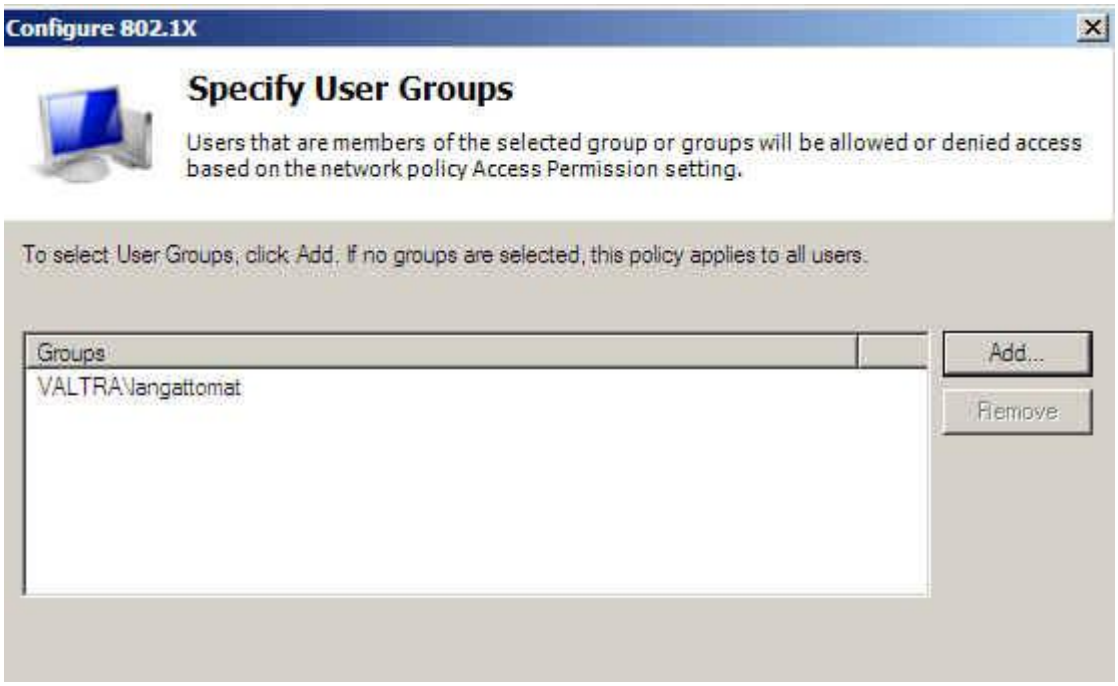


Kuva 32. Uuden RADIUS-asiakkaan määrittely.

Valitaan autentikointitavaksi PEAP ja valitaan sille oikea varmenne, joka tässä tapauksessa on server.valtra.local (kuva 33).

Kuva 33. PEAP-ominaisuuksien ja varmenteen valinta.

Lisätään ”langattomat”-ryhmälle oikeudet käyttää langatonta verkkoa (kuva 34).



Kuva 34. Oikeuksien lisäys ”langattomat”-ryhmälle.

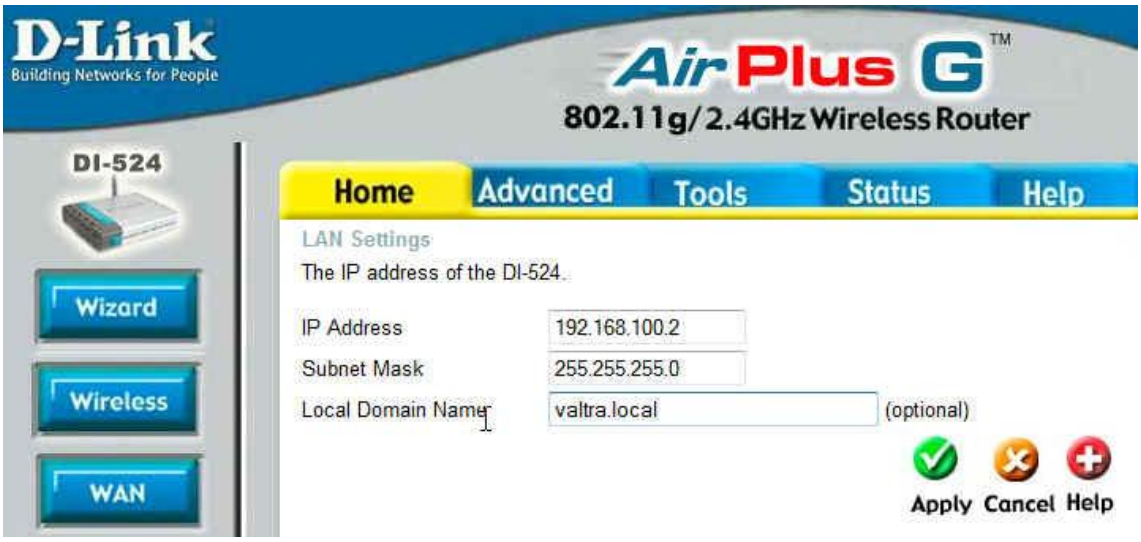
5.5 Tukiasema

Yrityksessä on käytössä D-Linkin AirPlus DI-524 WLAN-tukiasema (kuva 35). Se tukee WPA2-Enterprise sekä RADIUS-standardeja, joita tässä opinnäytteessä käytetään. Laitteeseen tehdään asetukset kirjautumalla laitteen graafiseen hallintapaneeliin.

Kuva 35. D-Link DI-524.

Liitin kannettavan tietokoneeni tukiasemaan, jotta pääsin muuttamaan tarvittavat asetukset ennen kuin tukiasema kytketään yrityksen verkkoon.

Tukiasemaan määritellään tukiaseman IP-osoite, aliverkon peite sekä toimialueen nimi (kuva 36).

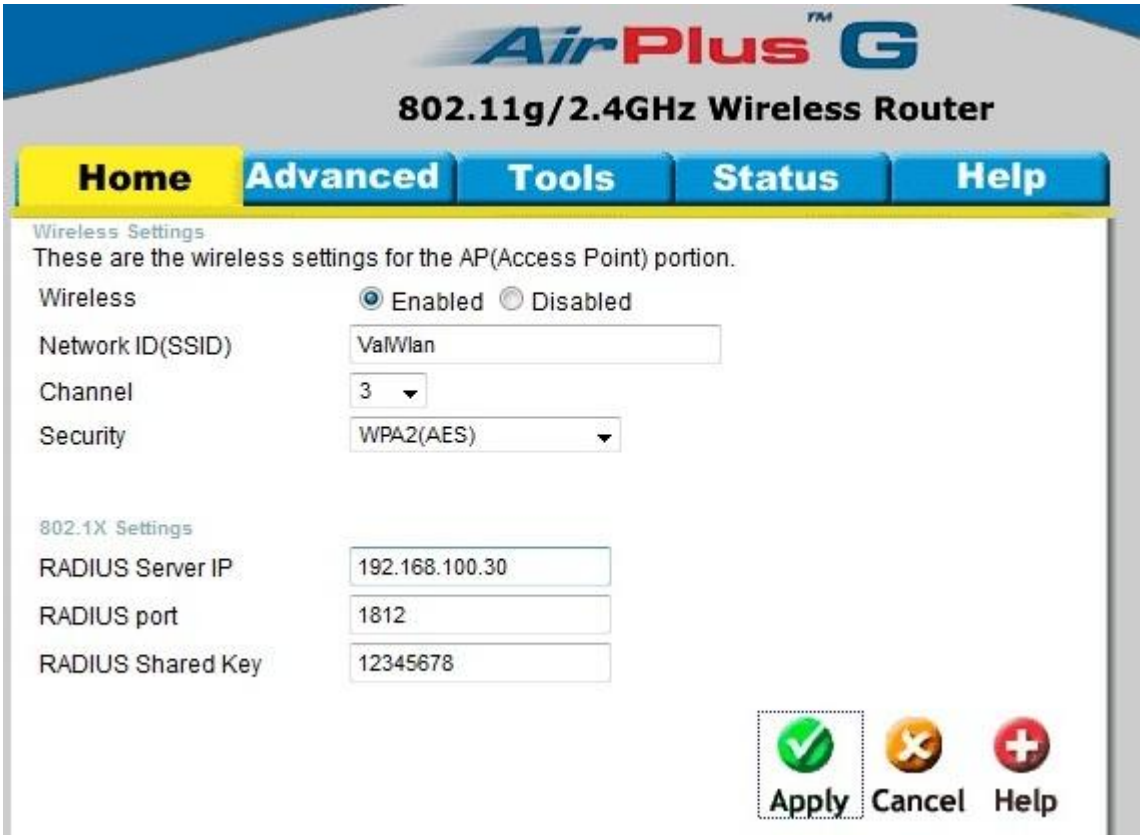


Kuva 36. D-Linkin IP-asetukset.

Langattoman verkon asetuksiin määritellään verkon nimi (SSID) sekä lisäasetuksena, mainostaako tukiasema verkon nimeä (Enabled). Verkon nimi voidaan myös piilottaa (Disabled), mutta se ei varsinaisesti ole mikään tietoturvaa parantava tekijä. Seuraavaksi valitaan kanava millä tukiasema toimii. Tässä kohdassa käytin hyväkseni puhelimeeni asennettua Wifi Manager-ohjelmaa, millä pystyin määrittämään vapaan kanavan ValWlan-verkolle.

Turvallisuusasetuksiin valitaan käytettäväksi WPA2-Enterprise-tila AES-salauksella.

802.1X-asetuksiin lisätään RADIUS-palvelimen IP-osoite ja porttinumero, joka on oletuksena 1812. Jos oletusporttia muutetaan, pitää palvelimen palomuurista avata kyseinen portti. Salainen avain (Shared Secret)-asetukseen määritetään sama merkkijono, joka määriteltiin NPS-palveluun palvelimelle (kuva 37).



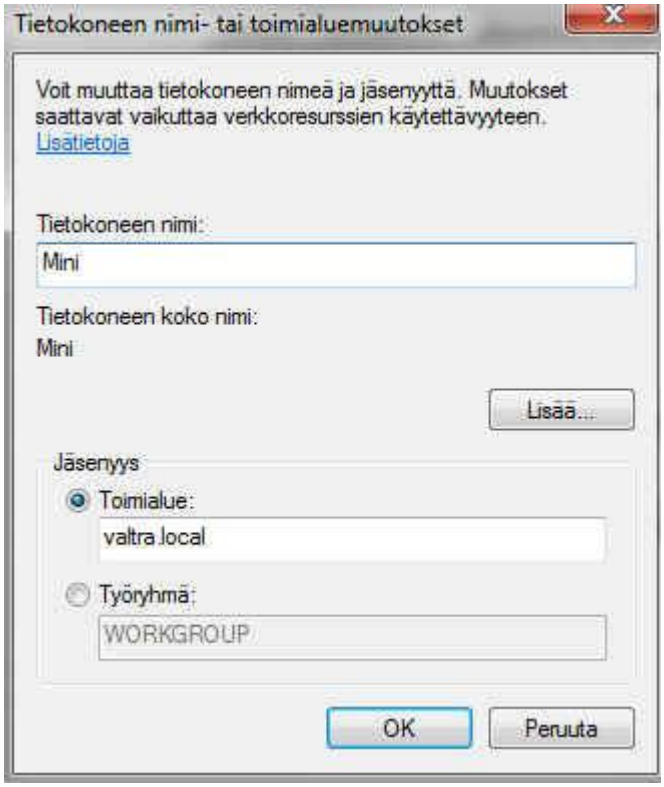
Kuva 37. Langattoman verkon asetukset.

Edellä määritellyt asetukset tukiasemaan riittävät muodostamaan yhteyden Val-Tradingin yritysverkkoon tietoturvallisesti käyttäen WPA2-Enterprise suojausta. Muihin asetuksiin ei tässä opinnäytetyössä koskettu.

5.6 Langattomat työasemat

Yrityksen käytössä olevissa kannettavissa tietokoneissa on molemmissa Windows 7-käyttöjärjestelmä, joka tukee 802.1X -standardia. Langattomien verkkojen määritykset tehdään Windowsin omalla ohjelmistolla parhaan yhteensopivuuden turvaamiseksi. Val-Tradingin langattomaan verkkoon pääsy vaatii, että päätelaite tukee 802.1X-tunnistautumista sekä kuuluu valtra.local-toimialueeseen. Lisäksi käyttäjätunnuksen pitää kuulua Active Directoryn ”langattomat”-ryhmään, jolla on verkonkäyttö-oikeudet.

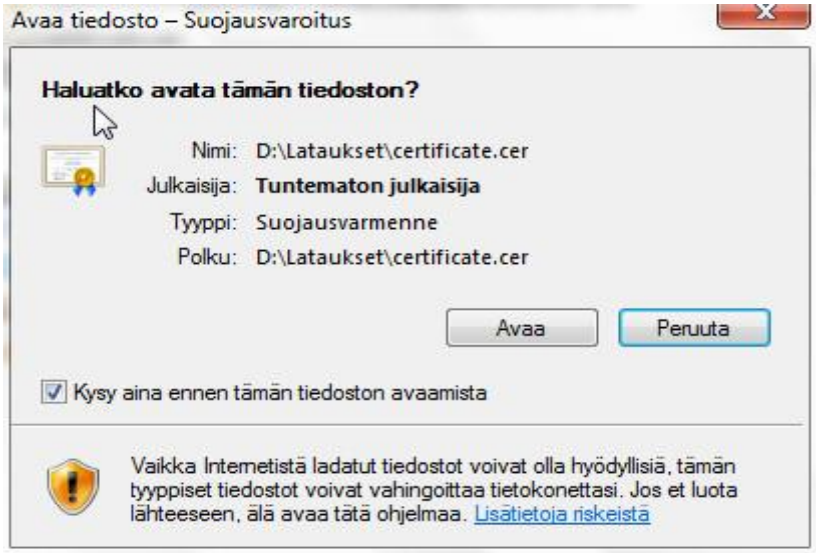
Lisätään langaton tietokone valtra.local-toimialueeseen, minkä jälkeen kone käynnistetään uudelleen muutosten voimaanastumiseksi (kuva 38).



Kuva 38. Tietokoneen lisäys valtra.local-toimialueeseen.

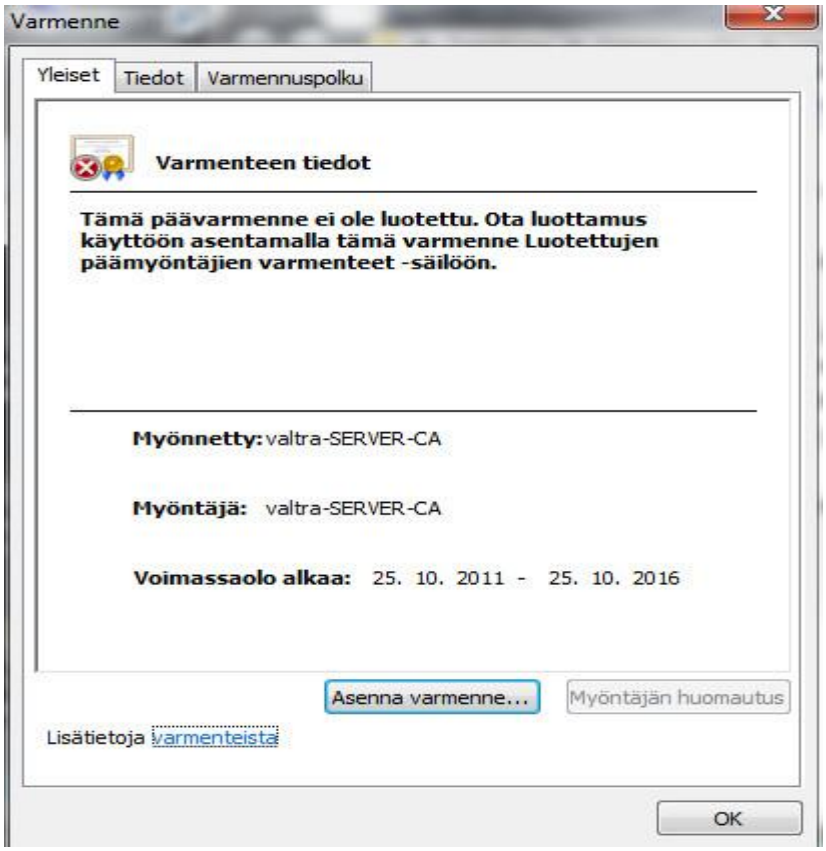
Kun tietokone on liittynyt valtra.local-toimialueeseen, latautuu ”langattomat”-yhteyskäytäntö palvelimelta automaattisesti muodostaen yhteyden yrityksen langattomaan verkkoon.

Päätelaite, joka ei kuulu valtra.local-toimialueeseen, vaatii varmenteen asennuksen manuaalisesti. Varmenne asennetaan esim. muistitikulta, jonne se on tallennettu palvelimelta. Windows antaa suojausvaroituksen avattaessa varmennetta (kuva 39).



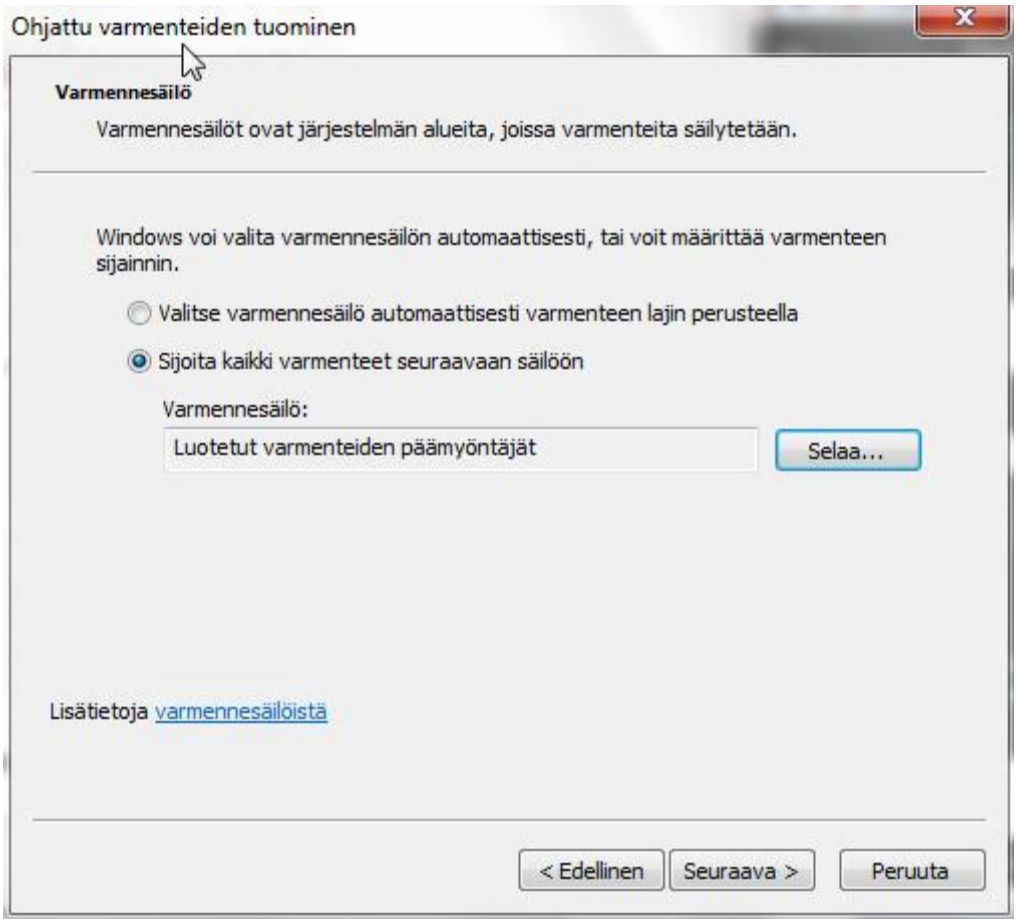
Kuva 39. Varmenteen avaus Windows 7:ssa.

Päätelaite, joka ei kuulu valtra.local-toimialueeseen ei pysty varmistamaan varmenteen luotettavuutta palvelimelta. Varmenne ilmoittaa tällöin, että päävarmenne ei ole luotettu (kuva 40).



Kuva 40. Varmenteen hyväksyminen Windows 7:ssa.

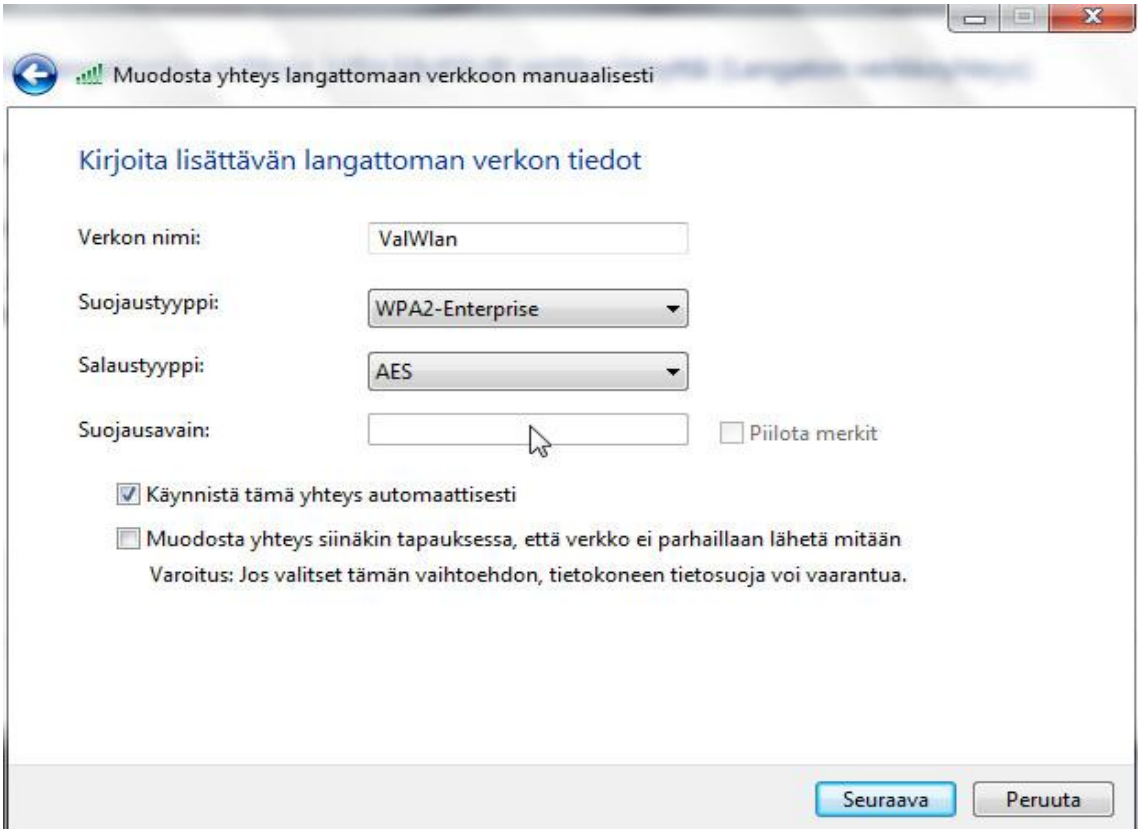
Varmenne hyväksytään luotettavaksi, kun se asennetaan päätelaitteen ”Luotetut varmenteiden päämyöntäjät”-säilöön (kuva 41).



Kuva 41. Varmenteen sijoitus luotettuihin varmenteisiin.

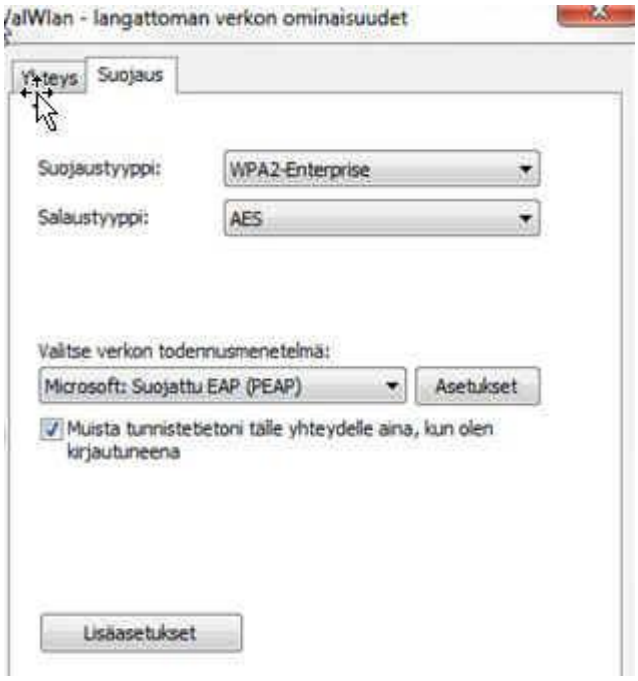
Varmenne on nyt tallennettu luotettuihin varmenteisiin. Seuraavaksi luodaan Val-Tradingin langattomaan verkkoon haluavalle päätelaitteelle uusi langaton verkkoprofiili. Profiilissa käytetään samoja asetuksia, jotka on aiemmin määritelty palvelimelle sekä tukiasemalle.

Langattoman verkon asetuksiin määritetään verkon nimi, suojaustyypiksi WPA2-Enterprise-tila sekä salaustyypiksi AES (kuva 42).



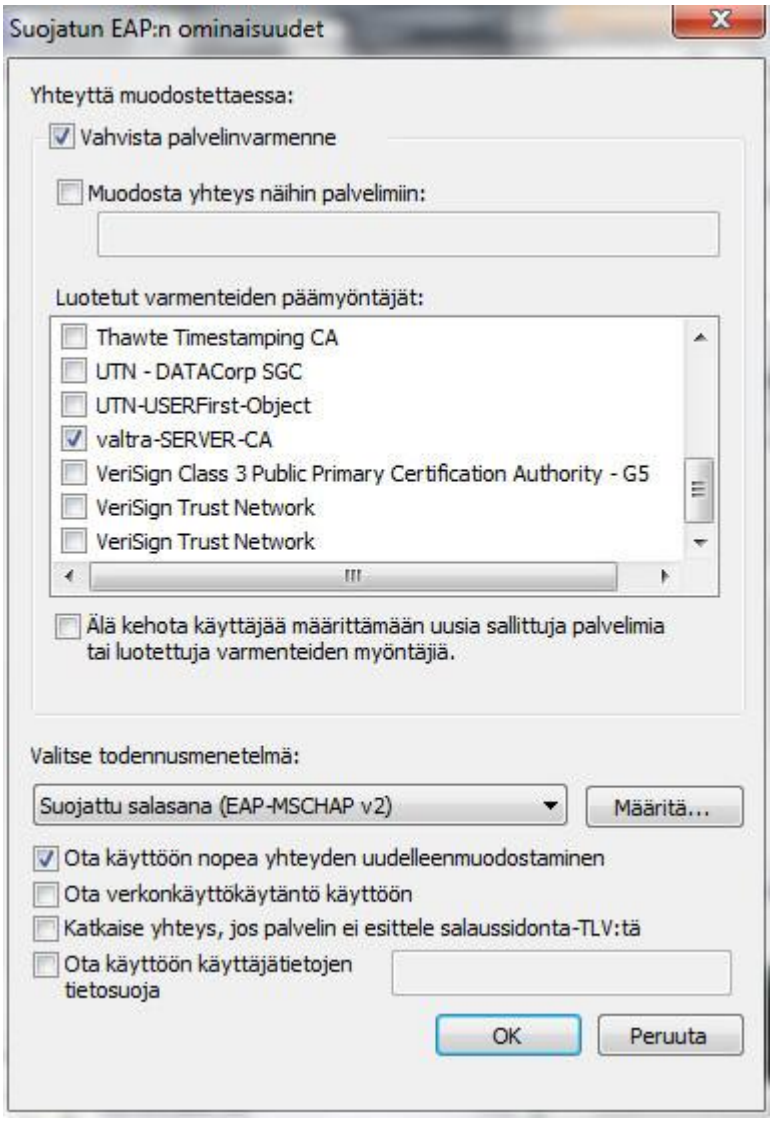
Kuva 42. Langattoman verkon nimi ja asetukset.

Valitaan verkon todennusmenetelmäksi Protected EAP (PEAP) (kuva 43).



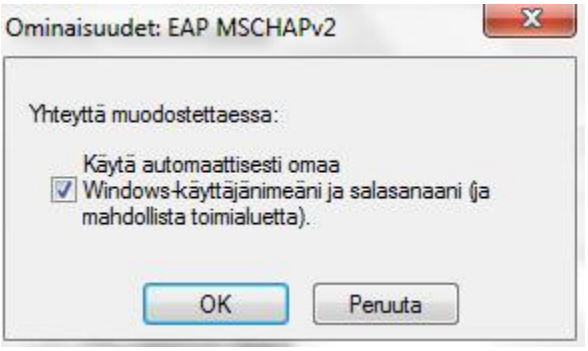
Kuva 43. PEAP-todennusmenetelmä.

PEAP-asetuksista valitaan käytettäväksi aiemmin asennettu varmenne (kuva 44).



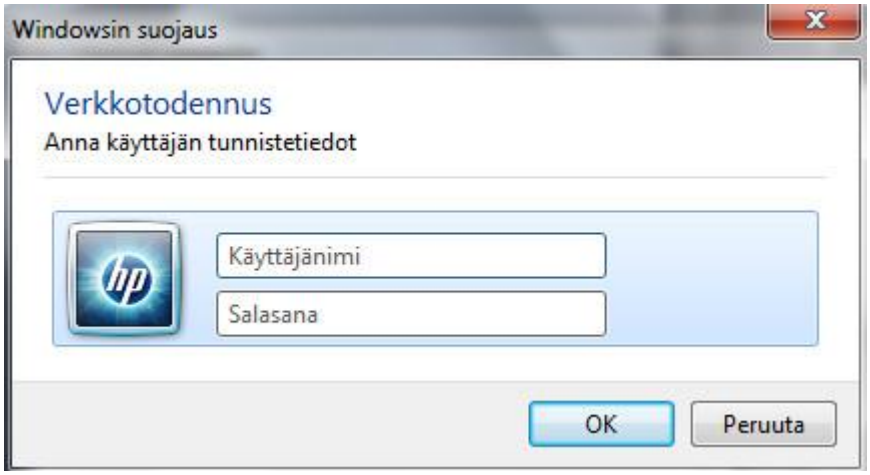
Kuva 44. Valtra-varmenteen valinta uuteen langattomaan profiiliin.

Lopuksi määritetään EAP-MSCHAP v2-asetuksista se, millä tunnuksilla yrityksen verkkoon kirjaudutaan. Poistamalla rasti automaattisesta kirjautumisesta koneen omalla, paikallisella Windows-tunnuksella langaton verkkoyhteys vaatii käyttäjätunnuksen ja salasanan, joka on määritelty AD DS:ään (kuva 45).



Kuva 45. EAP-MSCHAP v2-asetukset.

Tämän jälkeen Windows kysyy käyttäjätunnusta ja salasanaa. ValWlan-verkkoon kirjaudutaan syöttämällä palvelimelle aikaisemmin määritetyt ”langattomat”-ryhmään kuuluvat tunnukset (kuva 46).



Kuva 46. Kirjautuminen ValWlan-verkkoon Windows 7:ssa.

6 Yhteenveto

Opinnäytetyöni tavoitteena oli suunnitella Val-Tradingille tietoturvallinen langaton lähiverkko, joka liitetään osaksi yrityksen lankaverkkoa. Yritykselle oli heti alusta asti tärkeää tietoturvan osuus verkon toteutuksessa, joten päädyin käyttämään tällä hetkellä turvallisinta langatonta suojausta, IEEE 802.1X-standardiin perustuvaa RADIUS-protokollaa yhdessä WPA2-Enterprisen ja AES:n kanssa.

Työn teoriaosuudessa käsittelin langattoman verkon yleisiä ominaisuuksia, IEEE 802.11 -standardeja, laitteita ja topologioita. Lisäksi esittelin lyhyesti yleisimmät modulointitekniikat. Tietoturvasta tutkin eri salausmenetelmiä sekä autentikointimenetelmiä. Windows-palvelimesta kävin läpi tässä työssä tärkeät osa-alueet, kuten Active Directoryn sekä DHCP-, DNS- ja NPS-palvelimen ominaisuudet ja määritelmät.

Työn käytännön osuudessa toteutettiin langaton verkko käyttämällä hyväksi teoriaosuudessa käsiteltyjä asiakokonaisuuksia. Windows Server 2008-palvelimen asennus ja määrittely, tukiaseman asetukset, päätelaitteiden konfigurointi ja sertifikaatin luominen kuuluivat uuden langattoman verkon luomiseen.

Uuden, vahvaa käyttäjien ja laitteiden tunnistusta käyttävän langattoman verkon toteuttaminen oli ensikertalaiselle ajoittain hyvinkin haastavaa ja työlästä. Lopputuloksena kuitenkin oli toimiva, tietoturvallisesti vahvan suojauksen omaava langaton verkko. Työn tavoitteet täyttyivät sekä yritykselle että itselleni, koska opin valtavasti langattomista lähiverkoista sekä Windows-palvelinympäristöstä.

Tulevaisuudessa Val-Tradingin verkkoa joudutaan varmasti päivittämään lisäämällä siihen toinen palvelin, jo pelkästään vikasietoisuuden parantamiseksi. Tällöin voidaan myös jakaa palvelimen rooleja, koska nyt kaikki vaadittavat palvelut toimivat yhdessä palvelinkoneessa.

LÄHTEET

Brandon, J.C. 2008. CCNA Wireless Official Exam Certification Guide. Indianapolis: Cisco Press.

Conlan, P.J. 2009. Cisco® Network Professional's Advanced Internetworking Guide. Indiana: Wiley Publishing, Inc.

DHCP 2010. Wikipedia. Viitattu 1.6.2011 http://fi.wikipedia.org/wiki/DHCP.

Frankel, S.; Eydt, B.; Owens, L. & Scarfone, K. 2007. National Institute of Standards and Technology (NIST). SP 800–97. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

Viitattu 21.10.2010 http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

Granlund, K. 2003. Tietoliikenne. Jyväskylä: Docendo Finland Oy.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy.

IEEE 802.11 2010. Wikipedia. Viitattu 14.10.2010 http://fi.wikipedia.org/wiki/IEEE_802.11.

IEEE 802.11i 2010. Wikipedia. Viitattu 3.11.2010 http://fi.wikipedia.org/wiki/IEEE_802.11i.

Kaarlo, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo Finland Oy.

Kivimäki, J. 2005. Windows Server 2003 Active Directory. Readme.fi Oy.

Network Policy Server 2011. Microsoft. Viitattu 12.10.2011

http://technet.microsoft.com/fi-fi/network/bb629414.

Soyinka, W. 2010. Wireless Network Administration A Beginner's Guide. McGraw-Hill.

Stanek, W.R. 2003. Microsoft Windows Server 2003 – Asiantuntijan käsikirja. Helsinki: Edita Prima Oy.

Varmenne 2011. Viestintävirasto. Viitattu 12.10.2011

http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/varmenne.html.

WLAN 2010. Wikipedia. Viitattu 12.10.2010 http://fi.wikipedia.org/wiki/WLAN.