Pekka Väikkä

LANGATTOMAN TYÖASEMAN KIRJAUTUMINEN VERKKOPALVELUIHIN

Tietotekniikan koulutusohjelma

2009

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

LANGATTOMAN TYÖASEMAN KIRJAUTUMINEN VERKKOPALVELUIHIN

Väikkä, Pekka
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Joulukuu 2009
Ohjaaja: Olli Vainio
Sivumäärä: 25

Asiasanat: Lähiverkot, Palvelimet, Windows, WLAN

Tämä opinnäytetyö tehtiin Satakunnan ammattikorkeakoulun tekniikan ja merenkulun toimialalle ja sen tavoitteena oli mahdollistaa yksinkertainen kirjautuminen langattoman verkon käyttäjille.

Työssä käytettiin Microsoft Active Directoryn sisältämää Network Policy Server-järjestelmää sen yksinkertaisuuden takia. Myös liittyminen jo käytössä olevaan Active Directory-palveluun vaikutti valintaan. NPS toimii myös täysin Ciscon verkkolaitteiden kanssa.

Langattoman verkon tukiasemien hallinta keskitettiin käyttämällä WLAN-Controlleria.

Työ tehtiin ensin valmiiksi palvelimien osalta VMWare Workstation virtualisoinnilla, jonka jälkeen työ tehtiin loppuun erikseen asennetuilla palvelimilla. Silloin myös liitettiin langattoman lähiverkon hallinta ja kytkimet työhön.

LOGON TO NETWORK SERVICES WITH WIRELESS WORKSTATION

Väikkä, Pekka
Technology and Maritime Management Rauma, Satakunta University of Applied Sciences
Degree Programme in Information Technology
December 2009
Tutor: Olli Vainio MSc(Eng), Laboratory Engineer
Number of pages: 25

Keywords: LAN, Server, Windows, WLAN

This Bachelor's thesis was commissioned by Satakunta University of Applied Sciences faculty of Technology and Maritime Management Rauma. The purpose was to achieve simple login for the users of wireless network.

Network Policy Server of Microsoft Active Directory was used in this thesis because of its simplicity. Also because it was included in already existing Active Directory server, it was seen as an advantage. NPS is also compatible with Cisco networking devices.

The work regarding servers was first completed with VMWare Workstation virtualization software. After that it was complemented on physical servers and actual network devices were added.

SISÄLLYS

LYHENTEET

DNS	Domain Name Service
GP	Group Policy, ominaisuus tai toiminto, joka asetetaan käyttäjälle, käyttäjäryhmälle tai tietokoneelle
GPM	Group Policy Manager, hallintatyökalu käyttäjille, käyttäjäryhmille ja tietkoneille asetettaville ominaisuuksille
HRA	Health Registration Authority, käytetään NAP-palvelun kanssa, tarkistaa verkkoon liittyvien tietokoneiden tietoturvan tason
IEEE	Institute of Electrical and Electronics Engineer, järjestö, joka määrittelee kyseisten alojen standardeja ja kehittää koulutusta
IP	Internet Protocol
LAN	Local Area Network, lähiverkko
LWAPP	Lightweight Access Point Protocol
NAP	Network Access Policy, työkalu, jolla hallitaan verkkoon liittyvien koneiden tietoturvavaatimuksia
NPS	Network Policy Server, Microsoftin kehittämä RADIUS-järjestelmä
RADIUS	Remote Authentication Dial In User Service, palvelu jolla voidaan hallinnoida etä- ja WLAN-käyttäjiä
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
WLAN	Wireless Local Area Network, langaton lähiverkko

1 JOHDANTO

Satakunnan ammattikorkeakoulun tekniikan Rauman toimipisteen langaton lähiverkko toimii nykyisin ilman keskitettyä hallintaa erillisillä tukiasemilla. Työssä hahmotellaan siirtyminen keskitettyyn hallintaan ja käyttäjien tunnistamiseen Windows Active Directory (AD) -tunnuksin.

RADIUS-palvelu mahdollistaa langattomaan verkkoon liityttäessä yksinkertaisen käyttäjän tunnistuksen eli autentikoinnin. Ensimmäiseksi tuli päättää, minkä tyyppistä RADIUS-palvelua käytetään ja päätöksenä oli Microsoft Windows Server 2008 ja sen mukana toimitettava Network Policy Server. Päätökseen vaikuttavia tekijöitä oli se, että koululla oli jo ennestään Microsoft-tuotteita ja lisenssejä, joten hinta ei ollut ratkaisevassa asemassa. Päätökseen vaikuttivat myös Linux-käyttöjärjestelmien käytön hankaluus ja tietty yhteensopimattomuus Microsoft-tuotteiden ja palveluiden kanssa.

NPS-toiminnon avulla voidaan ohjata käyttäjät eri virtuaalisiin verkkoihin, rekisteröidyt käyttäjät sisäiseen verkkoon ja vieraat vain ulkoiseen verkkoon. Tämä mahdollistaa sen, että AD-käyttäjät pääsevät samoihin palveluihin käsiksi, kuin heillä olisi myös kiinteässä verkossa. Samalla vierastunnuksilla pääsee käsiksi Internet-materiaaliin, mutta ei sisäisen verkon resursseihin.

NPS-palvelun avulla voidaan silti rajoittaa myös rekisteröityjä käyttäjiä Health Policyjen avulla. On mahdollista määrittää esimerkiksi, että rajoitetaan käyttäjän pääsyä sisäiseen verkkoon, jos käyttäjällä ei ole virustorjuntaohjelmistoa asennettuna tai sen päivitykset ovat vanhoja.

Verkkolaitteina työssä oli Cisco 2600-kytkin ja Cisco 2000 Series WLAN Controller. Työn alkuvaiheessa kytkimessä käytettiin RADIUS-konfigurointia testauksen takia, mutta loppuvaiheilla kun langaton verkko liitettiin verkkoon, poistettiin kytkimestä kaikki asetukset.

2 MICROSOFT ACTIVE DIRECTORY

2.1 Active Directory yleisesti

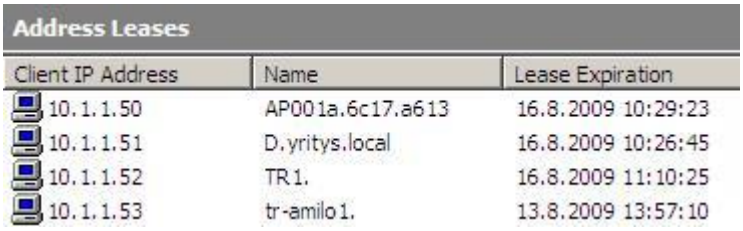
Active Directory (AD) on Microsoftin kehittämä teknologia, joka mahdollistaa erilaisten palveluiden ja palvelimien keräämisen samaan ympäristöön ja parantaa niiden yhteentoimivuutta. AD:n avulla on mahdollista hallita käyttäjiä ja käyttäjien resursseja. Käyttäjiä voidaan luoda yhdessä paikassa, jonka jälkeen käyttäjä voi kirjautua verkkoon kaikilta verkon työasemilta. Toinen pienissäkin AD-ympäristöissä käytettävä ominaisuus on tulostimien sijoittaminen palvelimille, joista niitä voidaan jakaa esimerkiksi tilojen mukaan käyttäjille. Miksi asentaa jokaiselle käyttäjälle oma tulostin, tai toisaalta, miksi asentaa kaikki verkon tulostimet jokaiselle käyttäjälle.

Active Directoryn avulla on myös mahdollista hallita verkkoa ja sen käyttöoikeuksia. Jokaiselle käyttäjälle voidaan asettaa verkkolevyltä oma alue, johon käyttäjä voi tallentaa tietoa ja päästä siihen käsiksi kaikilta verkon tietokoneilta, mutta vain omilla tunnuksillaan. Samaa voidaan myös soveltaa verkon käyttöoikeuksiin NPS-palvelun avulla. Kiinteässä verkossa voidaan asettaa kytkimiin tai reitittimiin politiikat, jotka tarkistavat AD-palvelimelta, onko käyttäjällä vaadittavat oikeudet verkon käyttöön.
AD tarjoaa käyttäjälle hierarkkisen rakenteen laitteille ja objekteille, joita domainissa on. Objekteja voivat olla käyttäjät, tietokoneet ja käyttäjäryhmät. /1, s. 656./

2.2 DHCP

Dynamic Host Configuration Protocol (DHCP) on protokolla, jota käytetään verkko-osoitteiden jakamiseen. Kaikille verkon laitteille ei ole tarvetta jakaa kiinteää osoitetta. Vain palvelimet ja verkkolaitteet vaativat kiinteän osoitteen. DHCP mahdollistaa osoitteiden jakamisen tietokoneille, mutta siihen voidaan myös määrittää, mitkä laitteet vaativat kiinteän IP-osoitteen.

TCP/IP-verkossa on mahdollista hakea esimerkiksi IP-osoite, aliverkon peite ja DNS serverin osoite. Kaikki nämä tiedot voidaan hakea DHCP-palvelimelta. DHCP-palvelimen käyttö vähentää huomattavasti ylläpitoa ja helpottaa käyttäjien liittymistä verkkoon ja siellä liikkumista. Jos käyttäjät saisivat itse asettaa osoitteensa, tulisi varmasti päällekkäisyyksiä osoitteissa, jolloin verkkoon pääsy estyisi. /1, s. 379./



Address Leases

Client IP Address	Name	Lease Expiration
10.1.1.50	AP001a.6c17.a613	16.8.2009 10:29:23
10.1.1.51	D.yritys.local	16.8.2009 10:26:45
10.1.1.52	TR1.	16.8.2009 11:10:25
10.1.1.53	tr-amilo1.	13.8.2009 13:57:10

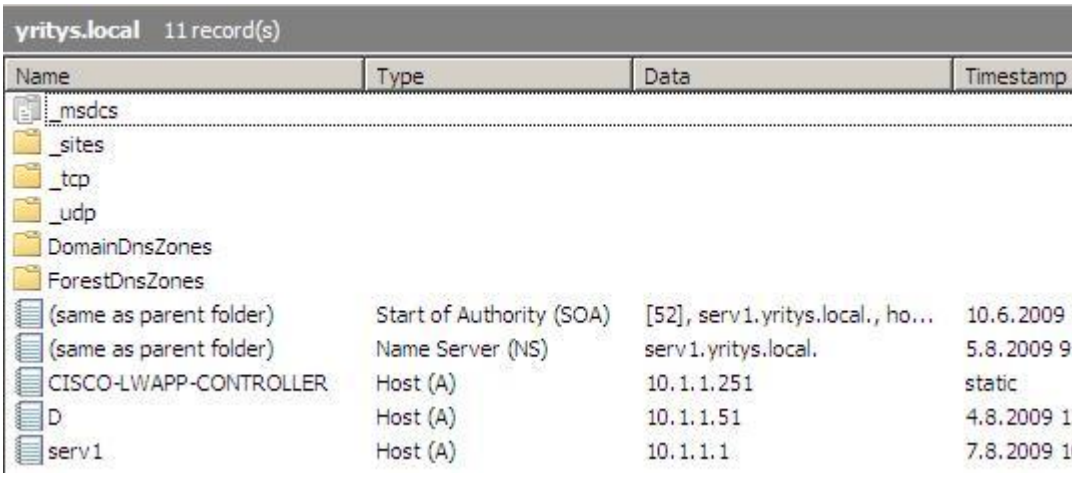
Kuva 1. DHCP-osoitelaina.

Kuvasta 1 voidaan nähdä Microsoft Server 2008 DHCP-palvelun jakamia IP-osoitteita. Kaikki laitteet ovat saaneet dynaamisen osoitteen. Dynaaminen osoite tarkoittaa, että laitteen sammuessa osoitteen lainausaika menee umpeen ja tämä osoite voidaan antaa toiselle laitteelle. Client IP Address -sarakkeesta nähdään tietokoneen lainaama osoite. Tässä työssä osoiteavaruudeksi valittiin koko 10.1.1.0-aliverkko , 255.255.255.0 maskilla, mutta ensimmäiset ja viimeiset 49 osoitetta varattiin kiinteitä osoitteita varten. Name-sarakkeessa näkyvät laitteiden nimet. Laitteiden nimistä voidaan päätellä, että AP001a.6c17.a613 on WLAN-tukiasema, D.yritys.local on kiinteässä verkossa sijaitseva työasema ja TR1. ja tr-amilo1. ovat langattomaan verkkoon vierastunnuksilla kirjautuneita. Viimeisenä sarakkeena oleva Lease Expiration tarkoittaa lainan loppumisaikaa. Esimerkkinä osoitteen 10.1.1.51 lainausaika päättyy 16.8.2009 kello 10:26:45. Jos tämä tietokone ei ole päällä ja kytkettynä verkkoon tuohon aikaan, vapautetaan osoite muitten laitteiden käyttöön. Kuitenkin, jos tietokone on päällä ja edelleen kytkettynä verkkoon, varataan tämä sama osoite uudelleen samalle tietokoneelle.

2.3 DNS

DNS on kehitetty jo 80-luvulla ratkaisemaan ongelma, miten muistaa tietokoneitten osoitteet. Järjestelmän ideana on, että muutetaan helposti muistettavat laite- ja domainnimet nelioktettisiksi IP-osoitteiksi. /1, s. 394./

Kun tietokone ottaa yhteyttä serv1.yritys.local-osoitteeseen, DNS-palvelu ohjeistaa tietokonetta ottamaan yhteyttä IP-osoitteeseen 10.1.1.1. Palvelu on tehty sitä varten, että ihmisen on vaikeampi muistaa numerosarjoja kuin nimiä.



yritys.local 11 record(s)

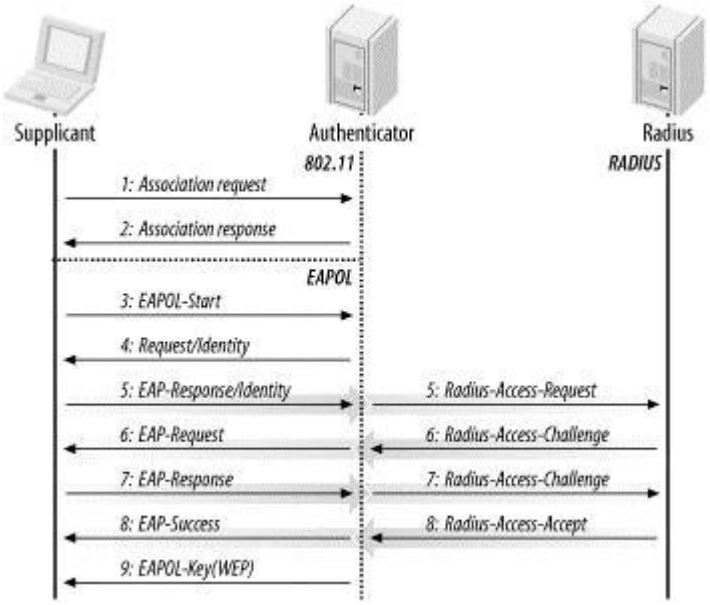
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[52], serv1.yritys.local., ho...	10.6.2009
(same as parent folder)	Name Server (NS)	serv1.yritys.local.	5.8.2009 9
CISCO-LWAPP-CONTROLLER	Host (A)	10.1.1.251	static
D	Host (A)	10.1.1.51	4.8.2009 1
serv1	Host (A)	10.1.1.1	7.8.2009 1

Kuva 2. DNS-merkinnät.

Kuvassa 2 nähdään serv1-palvelimella toimivan DNS-palvelun merkinnät. Name-sarakkeessa nähdään laitteen nimi ja Data-sarakkeessa laitteen IP-osoite. Jos laite D haluaa ottaa yhteyttä palvelimeen serv1, lähettää se pyynnön DNS-pavelulle, joka lähettää kyseisen laitteen IP-osoitteen takaisin laitteelle D. DNS-palveluun voidaan myös määrittää, mitkä osoitteet ovat kiinteitä, eli ne on asetettu käsin. Timestamp-sarakkeessa nähdään laitteen CISCO-LWAPP-CONTROLLER kohdalla static, joka merkitsee kiinteää osoitetta. AD:n DHCP- ja DNS-palvelut tukevat dynaamista DNS:ää, jolloin automaattisesti DHCP-tiedot siirtyvät DNS:ään. DNS-palveluun ei ole kuitenkaan pakko mainita kiinteää osoitetta, jos kiinteä osoite on muutenkin jo merkitty DHCP-palvelussa, mutta tämä saattaa kuitenkin tuottaa hieman lisää rasitusta DNS-palvelimelle.

2.4 NPS

Network Policy Server on palvelu, jota käytetään käyttäjien autentikointiin ja työasemien turvallisuuden tarkkailuun. Palvelulla voidaan esimerkiksi tarkastaa tietokoneen virusturvan tila, onko mitään virustorjuntaohjelmistoa asennettu ja onko se ajan tasalla. Mahdollisia toimenpiteitä on eri virtuaalisiin verkkoihin liittäminen tai verkon käytön esto.

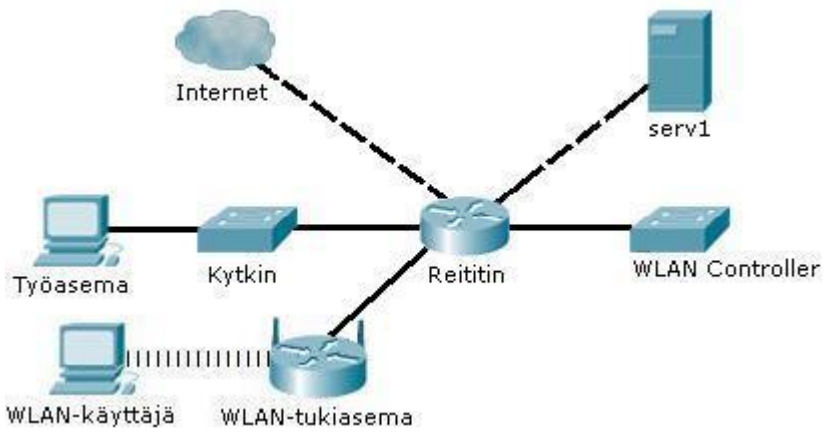


Kuva 3. RADIUS-kirjautuminen ja WEP-salaus /2, s. 91/.

Kun laite halutaan liittää langattomaan verkkoon, laitteesta lähtee pyyntö tukiasemalle. Langattomat tukiasemat ottavat pyynnön vastaan ja suodattavat kaiken ylimääräisen liikenteen tältä koneelta. Kun tukiasema on vastannut tietokoneen pyyntöön, lähettää tietokone EAPOL-käynnistyskäskyn, jonka jälkeen tukiasema pyytää tunnusta. Tietokone lähettää tunnuksen tukiasemalle, joka taas ohjaa tiedon eteenpäin autentikointipalvelimelle. Palvelin ja tietokone vaihtavat tämän jälkeen tietoa, jossa käyttäjätunnus ja salasana tarkistetaan. Tässä käytetään Radius-protokollaa. Kun yhteys on muodostettu, lähetetään tietokoneelle vielä EAPOL-avain, joka mahdollistaa salauksen käytön.

3 VERKKO

Tässä työssä käytettiin hyvin yksinkertaista verkkoa. Halutut palvelut vaativat verkolta vain yhteyttä eri verkon osiin, Internetiin ja virtuaalisiin verkkoihin.



Kuva 4. Verkon rakenne.

Kun käyttäjä liittyy langattomaan verkkoon ja haluaa päästä jollekin sivustolle Internetissä, lähettää käyttäjä tukiasemalla pyynnön yhteyden luomisesta. Tukiasema taas lähettää pyynnön WLAN Controllerille, missä kysytään käyttäjän oikeutta kirjautua verkkoon. WLAN Controller lähettää tämän jälkeen tiedustelun palvelimelle, joka kuittaa takaisin, onko käyttäjällä oikeutta kirjautua vai katkaistaanko yhteys. Jos käyttäjällä on erikseen annettu käyttäjätunnus, voidaan hänelle antaa myös tiettyjä oikeuksia sisäiseen verkkoon, kuten tulostinpalvelimelle tai luku- ja kirjoitusoikeudet verkossa sijaitsevalle levylle.

3.1 Kiinteä verkko

Verkon niin sanottuun kiinteään osaan kuuluu sen runko, jossa sijaitsevat reitittimet, kytkimet sekä hallintalaitteet. Tässä työssä käytettiin yhtä reititintä, johon oli sijoitettu koko verkon yhteystiedot. Koska käytössä oli pieni määrä laitteita ja alueet vähäisiä, päätettiin reititys suorittaa RIPv2-reitityksellä. Myös staattinen reititys olisi ollut mahdollinen, mutta RIPv2 on tarpeen verkon kasvaessa.

3.1.1 Verkon rakenne

Kiinteään verkkoon kuului Ciscon kytkin ja reititin. Suoraan reitittimeen kytkettiin yhteys ulkoverkkoon ja palvelimeen, jota työssä käytettiin. Koska verkossa oli myös kiinteään verkkoon yhdistettyjä tietokoneita, vaadittiin niitä varten kytkin. Myös langattoman verkon hallintalaite ja tukiasema olivat kytkettynä reitittimeen.

3.1.2 Kiinteän verkon konfigurointi

Kiinteän verkon konfigurointi oli hyvin suoraviivaista ja yksinkertaista. Työssä vaadittiin vain yksinkertaista ja kevyttä reititystä ja täksi valittiin RIP versio 2. Reititystaulussa oli Active Directoryn Domain Controller-palvelin, jossa olivat kaikki verkon palvelut kuten DHCP ja DNS. Ulkoinen verkko oli lisätty reititykseen staattisella reitillä. Jos haettu IP-osoite kuuluu osoitealueeseen, joka on eri kuin sisäisen verkon osoitealue, lähettää reititin paketin ulkoverkkoon. Langattoman verkon laitteista vain hallintalaitteella oli kiinteä osoite. Työssä päätettiin, ettei tukiasemien osoitteiden välttämättä ole pakko olla staattisia, koska niitä pidetään aina päällä ja laitteet hakevat tiedot hallintalaitteelta nimen perusteella.

Päällimmäinen vaatimus reitittimelle tässä työssä on tapa, miten NPS toimii. Käyttäjätunnuksen asetuksista johtuen kirjautunut käyttäjä ohjataan johonkin virtuaaliseen verkkoon. Omilla AD-tunnuksilla kirjautuneet käyttäjät voidaan ohjata esimerkiksi VLAN-verkkoon 100, missä sijaitsevat myös kaikki kiinteään verkkoon yhdistetyt tietokoneet ja palvelimet. Vierastunnuksilla kirjautuvat käyttäjät voidaan ohjata VLAN-verkkoon 200, missä ei ole muita laitteita, mutta siitä pääsee ulkoiseen verkkoon käsiksi. Käytettäessä virtuaalisia verkkoja on verkosta löydyttävä vähintään yksi reititin, joka yhdistää virtuaaliset verkot ja osaa reitittää yhteydet oikein.

3.2 Langaton verkko

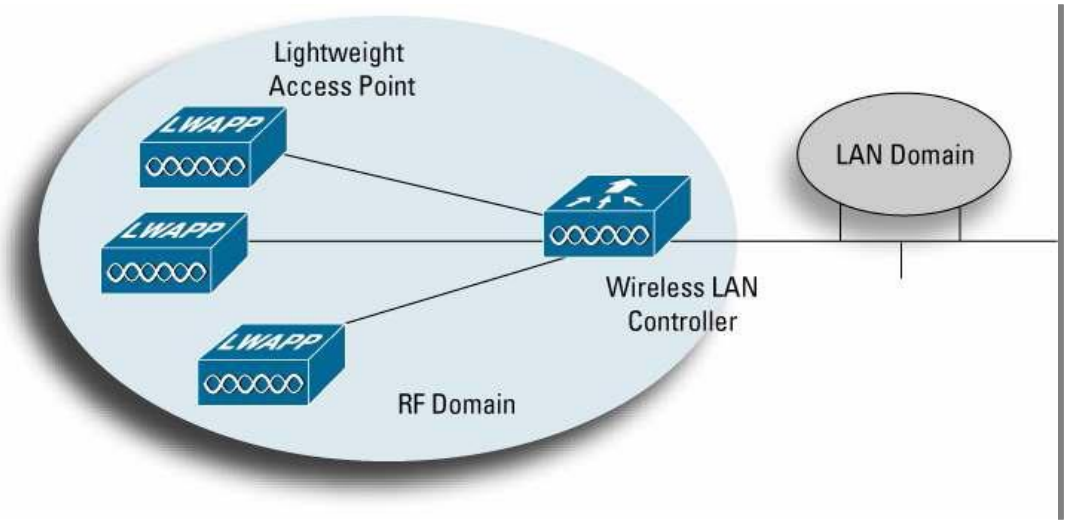
Työssä käytettiin Ciscon 2100-sarjan WLAN-hallintalaitetta ja Ciscon tukiasemaa. Varsinainen konfigurointi tehtiin hallintalaitteella, joka taas jakoi tiedot tukiasemille.

Pienessä verkossa hallintalaitteesta ei ollut suurta hyötyä, mutta suuremmassa kokonaisuudessa hallintalaitteesta on paljon apua, kun ei tarvitse tehdä samaa asiaa jokaiselle tukiasemalle erikseen. Langattomat tukiasemat hakevat kiinteän verkon kautta hallintalaitetta, joka taas lähettää tukiasemille niiden konfiguraation. Koska tukiasemat hakevat hallintalaitetta nimen perusteella, pitää laitteelle antaa DHCP-palvelimella kiinteä IP-osoite ja merkitä tämä osoite myös DNS-palvelimen rekisteriin.

3.2.1 Light Weight Access Point Protocol

Langattomissa verkoissa on uusi trendi, joka suuntaa keskitettyyn tietoon ja hallintaan. Uudessa järjestelmässä käytetään WLAN-hallintalaitetta, jolla luodaan ja valvotaan sääntöjä jokaisella tukiasemalla. Keskittämällä turvallisuus, liikkuvuus ja palvelun laatu sekä monet muut toiminnot jotka ovat tärkeitä langattomassa verkossa, voidaan tehokkaasti hallita koko yrityksen langatonta verkkoa. Kun vielä jaetaan toiminnot tukiasemille ja hallintalaitteelle voidaan helpottaa ylläpitoa, parantaa tehoa ja tietoturvan tasoa suurissakin verkoissa. /3, s. 1./

Kun useammat laitevalmistajat siirtyvät hierarkkiseen järjestelmään ja suuret verkot on rakennettu lightweight-tukiasemilla, tulee tarve standardisoidulle protokollalle, jolla säädellään, miten tukiasemat kommunikoivat langattomien laitteiden kanssa. Tämän vuoksi IETF on määrittänyt LWAPP-protokollan. LWAPP-protokollan avulla voidaan saavuttaa parempi joustavuus ja mahdollistaa kaikki toiminnot langattomassa verkossa /3, s. 1/.

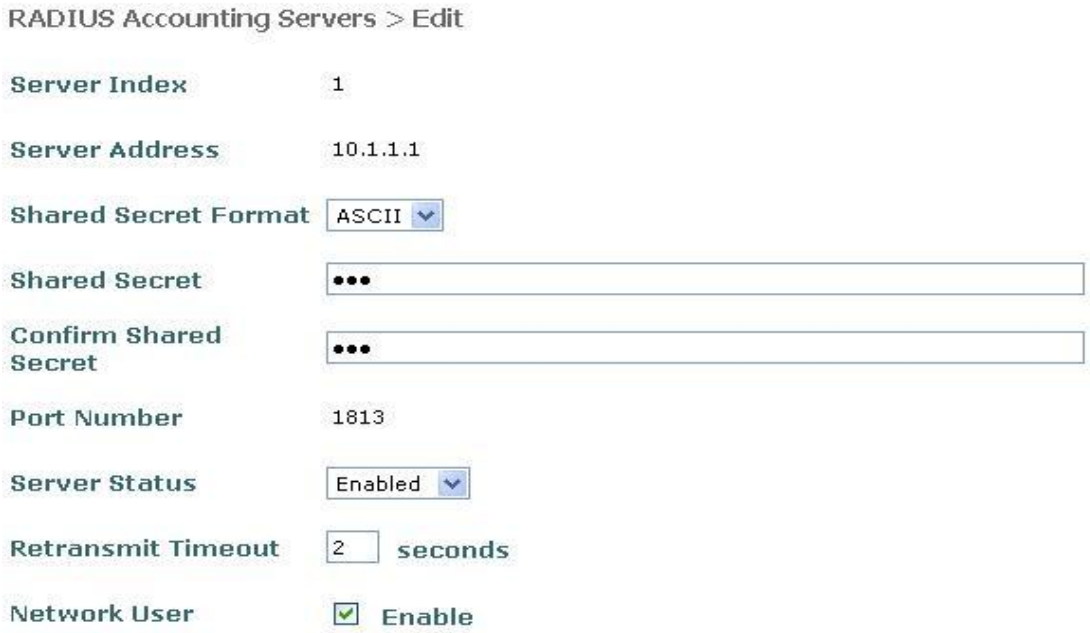


Kuva 5. Langaton verkko, jossa käytetään LWAPP-protokollaa /3, s. 1/.

Kuvassa 5 näkyvässä rakenteessa WLAN-hallintalaite on sijoitettu tukiasemien ja kiinteän verkon väliin. Tässä työssä kuitenkin käytettiin erilaista rakennetta, jossa hallintalaite sijoitettiin osaksi kiinteää verkkoa ja tukiasemat liitettiin samaiseen verkkoon. Tämä rakenne mahdollistaa useampien laitteiden kytkemisen hallintalaitteeseen. Hallintalaitteessa on useimmiten 1-8 porttia, joihin voidaan kytkeä tukiasema ja yksi tai useampi portti, joista saadaan yhteys kiinteään verkkoon. Kun tukiasemat sijoitetaan kiinteään verkkoon eikä suoraan hallintalaitteeseen, voidaan verkkoon liittää paljon suurempi määrä tukiasemia.

3.2.2 Langattoman verkon konfigurointi

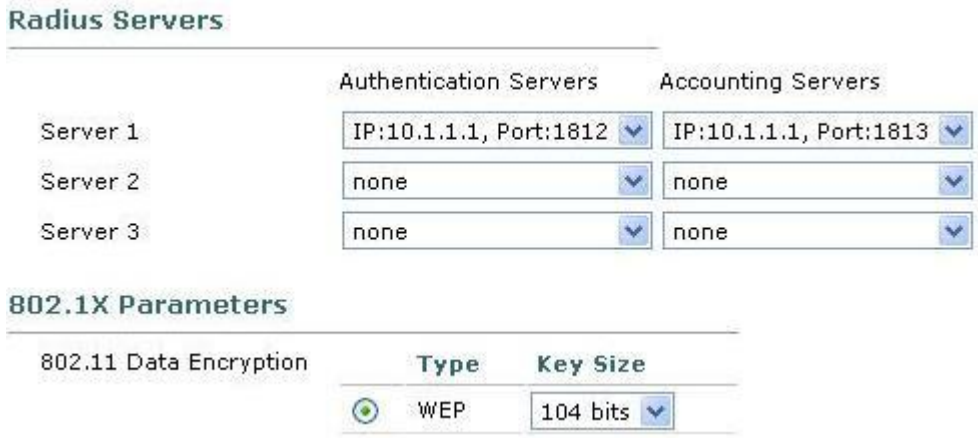
Työssä kaikki konfigurointi tehtiin hallintalaitteelle, joka lähetti konfiguraation tukiasemille. Tämä säästää runsaasti aikaa konfiguroinnissa ja samalla varmistaa, että jokaisella tukiasemalla on varmasti samat asetukset. Koska kiinteässä verkossa käytettiin useita virtuaaliverkkoja, tulee asettaa kaikki tukiasemat, hallintalaite ja palvelimet samaan virtuaaliverkkoon. Tämä siksi, että laitteet löytävät toisensa verkosta ja saavat haettua autentikointitiedot palvelimelta.



Kuva 6. WLAN Controller, Radius Authentication server-asetukset.

Kun langattomassa verkossa halutaan käyttää RADIUS-autentikointia, pitää se asettaa hallintalaitteelta. Tämä onnistuu, kun laitteelle lisätään palvelimen IP-osoite,

porttinumero ja jaettu salasana. Salasana asetetaan ensin RADIUS-palvelimeen, jonka jälkeen se annetaan kaikille laitteille, jotka lähettävät ja vastaanottavat tietopalvelimelta. Salasana jaetaan tästä eteenpäin langattoman verkon tukiasemille, jotta ne pystyvät kysymään palvelimelta käyttäjien tunnuksia.



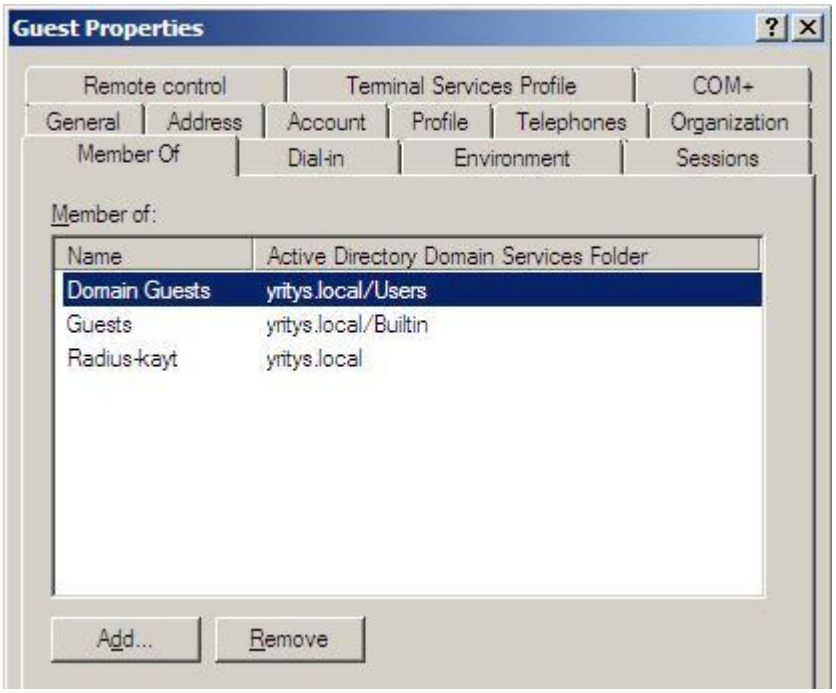
Kuva 7. RADIUS-serveri ja salausmenetelmä.

Kuvassa 7 nähdään että NPS-palvelin on liitetty langattoman verkon RADIUS-autentikointipalvelimeksi ja käyttäjätilien hallintapalvelimeksi. Langattomassa verkossa haluttiin myös käyttää jotain salausta ja tähän valittiin WEP. Kyseinen salaus ei ole paras mahdollinen, mutta tässä työssä se riitti salaukseksi. Haluttaessa voitaisiin myös käyttää muita salausmenetelmiä. Valitettavasti autentikointia käytettäessä ei voida käyttää sisäänkirjautumista intrasivuilla.

4 NPS KÄYTTÖÖNOTTO

Työtä aloitettaessa harkittiin mahdollista Linux-palvelinta ja sen käyttämistä RADIUS-palvelimena, mutta tämä suunnitelma jäi tekemättä. Pääsyy tähän oli monimutkaisuus. Miksi asentaa erillistä palvelinta, kun voitiin käyttää Active Directoryssä NPS-palvelua. Tässä työssä NPS oli sijoitettu Domain Controlleriin, mutta suuremmassa verkossa palvelu voidaan sijoittaa esimerkiksi member serverille, jonka työnä on tulostinpalvelu tai jokin muu vastaava kevyt työ. Asiaan myös vaikutti Linux-käyttöjärjestelmä, joka eroaa suuresti Mircosoftin tuotteista. Ohjelmistot ovat erilaisia, eikä yhteyden muodostaminen ole aina niin suoraviivaista.

4.1 WLAN-käyttäjien luonti



Kuva 8. Guest-tili kuuluu Radius-käyttäjiin

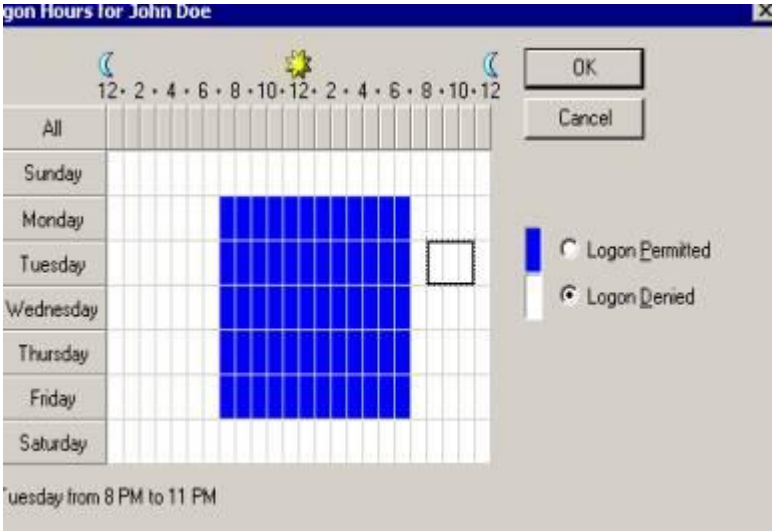
Langattoman verkon käyttäjiä varten luotiin AD-palvelimelle oma ryhmä, Radius-kayt. Siihen lisättiin kaikki käyttäjät, jotka tarvitsivat sitä. Verkossa myös aktivoitiin Guest-tili, joka ei vaadi mitään salasanaa, mutta samalla sillä on hyvin vähän käyttöoikeuksia, ja esimerkiksi verkkoasemaa tällä käyttäjätilillä ei ole lainkaan. Tämä johtuu siitä, että Guest-tiliä voi käyttää samaan aikaan useampi henkilö ja tietoturvan tarjoaminen tällaiselle tilille on melko hankalaa. Työtä tehtäessä mietittiin

myös mahdollisuutta, jossa vierastilit tehtäisiin aina tilauksesta. Tämä jätettiin kuitenkin tekemättä sen takia, että verkkoon ei tulisi samaan aikaan kirjautumaan kuin enintään 8 käyttäjää vierastunnuksella. Tämä käyttäjämäärän rajoitus johtuu työssä käytetyistä WLAN-tukiasemista ja hallintalaitteesta, jotka tukevat vain 8 käyttäjän samaan aikaan kirjautumista samoilla tunnuksilla. Erillisten tunnusten luonti määräaikaisesti tuottaisi myös ylimääräistä työtä ja vaatisi aina käyttäjätilin luovalta henkilöltä vaadittavia oikeuksia, joita jaetaan hyvin harvoille.

4.2 Group Policy

Group Policy on työkalu, jolla voidaan hallita käyttäjiä ja tietokoneita keskitetysti. Käyttäjille ja käyttäjäryhmille voidaan antaa tiettyjä oikeuksia tai rajoituksia. Käyttäjää voidaan esimerkiksi estää kirjautumasta työasemalle tiettyyn aikaan päivästä tai estää kirjautuminen kokonaan. GP mahdollistaa myös verkkokansioiden liittämisen käyttäjän profiiliin, jolloin käyttäjä pääsee aina käsiksi omaan verkkokansioonsa, kun hän kirjautuu omilla tunnuksillaan verkkoon. /1, s. 738./

Työssä käytettiin Group Policyn mahdollistamaa tilin käyttöajan rajoitusta. Viikonloput ja työajan ulkopuolinen verkon käyttö poistettiin vierastililtä



Kuva 9. Rajoitettu kirjautumisaika.

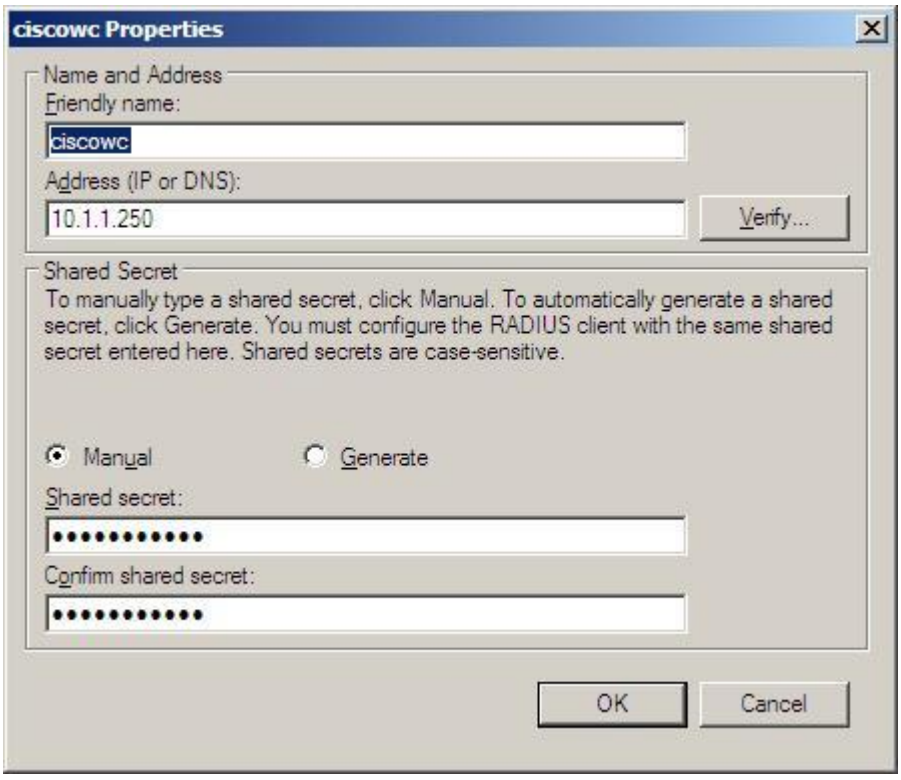
Aika, milloin tunnuksella voidaan kirjautua verkkoon, määritellään tunnin tarkkuudella kuvan 9 mukaan. Kuvassa 9 sininen alue tarkoittaa mahdollista kirjautumisaikaa, tässä se on arkipäivinä kello 7-19.

4.3 NPS konfigurointi Domain Controllerissa

Kuva 10. Autentikoinnissa käytetään PEAP-MS-CHAPv2 salasanaa.

NPS-palveluun asetettiin sertifikaatti ja määriteltiin salasanan tyyppi. Sertifikaatin käyttö ei ollut välttämätöntä, koska toinen EAP-autentikointimenetelmä oli salasanan käyttö. Sertifikaattien käyttö päätettiin jättää pois, koska tällöin sertifikaatti pitäisi erikseen siirtää tietokoneelle, joka halutaan päästää verkkoon. Tämä on kätevää, kun kyseessä on tietokone, jota toistuvasti käytetään verkossa.

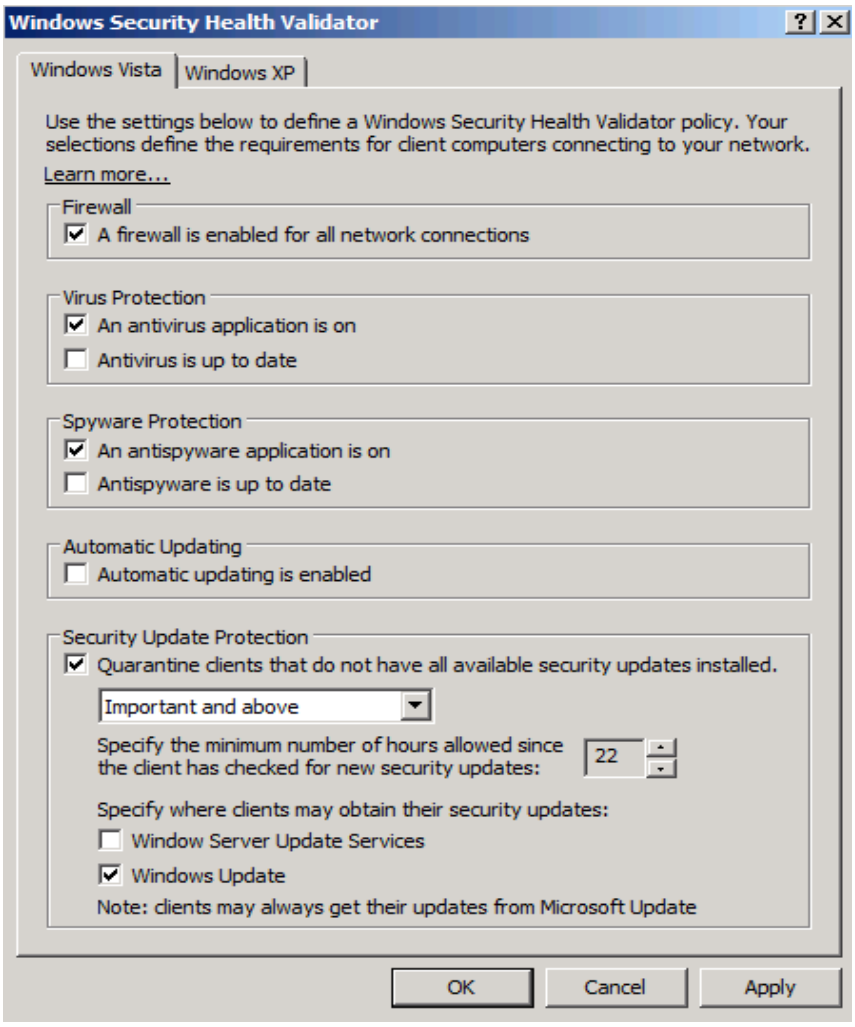
Kun autentikointimenetelmä oli asetettu, piti määrittää verkon laitteet, jotka ovat yhteydessä palvelimeen. Tähän riitti tässä työssä vain WLAN-hallintalaite, joka taas toimitti tiedot eteenpäin tukiasemille.



Kuva 11. Cisco WLAN Controller.

Hallintalaitetta lisättäessä pitää sen IP-osoite ilmoittaa. Samaan aikaan pitää myös muistaa antaa jaettu salasana laitteelle. Tämän salasanan pitää olla sama kuin hallintalaitteelle annettu. Salasana voi olla hyvin vaikeaa muotoa, koska sitä ei tarvitse kirjoittaa mihinkään muualle kuin serverille ja laitteille, jotka siihen ovat suorassa yhteydessä. Salasana on silti hyvä kirjata jonnekin, jos sitä joskus tarvitaan.

Työssä myös käytettiin Health Policy-toimintoa, joka mahdollistaa heikon tietoturvan tietokoneiden ohjaamisen rajoitettuun verkkoon. /4, s. 18./



Kuva 12. NAP Health Policy Windows Vistalle.

Health Policyllä voidaan määrittää, että tietokoneessa, joka kytketään verkkoon pitää olla palomuuri ja käynnissä oleva virustorjunta. Myös Windows-päivityksiä voidaan tarkkailla ja määrittää, kuinka uudet päivitykset tietokoneessa pitää olla.

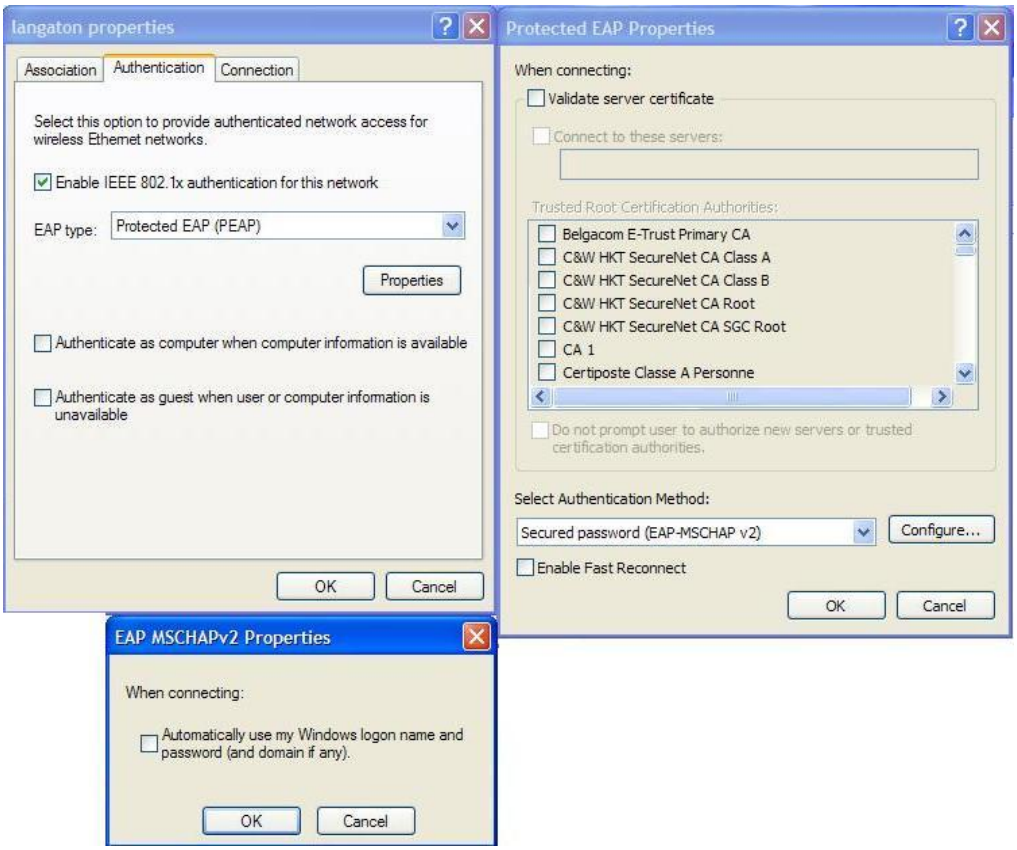
5 WLAN-KÄYTTÄJÄT

Langattoman verkon käyttäjiä voivat olla koulun henkilökuntaa tai opiskelijoita, jotka tuovat oman kannettavan tietokoneen mukanaan, tai vierailija, joka vaatii pääsyä Internetiin. Kirjautumiskäytäntö on kaikille samanlainen. Haluttaessa helpottaa kirjautumista voidaan tietokoneelle lisätä käyttäjätunnus, mikä vastaa AD-verkossa olevia tunnuksia. Näin kannettavan tietokoneen konfigurointi voidaan jättää minimiin. Pitää kuitenkin muistaa, että tämä heikentää tietoturvan tasoa, koska käyttäjän tunnukset ovat nyt koulun ulkopuolisella tietokoneella tallennettuna.

5.1 Laite- ja ohjelmistovaatimukset

Kirjautuminen ja autentikointi langattomaan verkkoon ei vaadi mitään erikoislaitteita tai ohjelmistoja tietokoneessa. Tavallinen langaton verkkokortti ja Windows-käyttöjärjestelmä riittävät. Myös Linux-käyttöjärjestelmällä autentikointi on mahdollista, mutta sitä ei tätä työtä tehdessä kuitenkaan testattu.

5.2 Konfigurointi



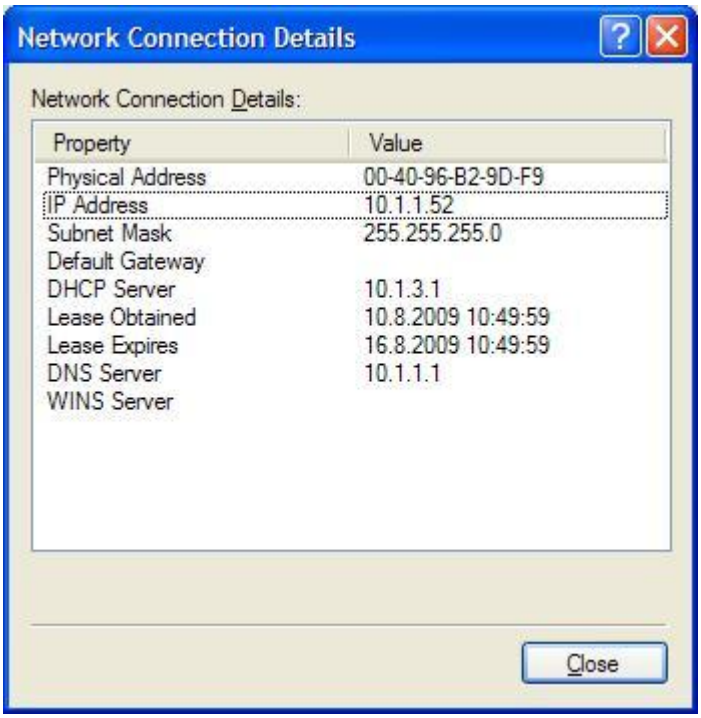
Kuva 13. Päätekoneen asetukset.

Kun langaton verkko on löydetty, muutetaan sen asetuksia Windowsin verkkoasetuksista seuraavasti. Mahdollistetaan IEEE 802.1x autentikointi ja valitaan EAP-tyypiksi Protected EAP (PEAP). Tämän jälkeen poistetaan sertifikaattivalinta ja muutetaan autentikointimenetelmä Secured password (EAP-MSCHAP v2) -tyyliseksi. Jos tietokoneella käytetään samaa tunnusta kuin käyttäjän AD-tunnus, voidaan EAP MSCHAPv2 -asetuksista jättää Windows logon nimi ja salasana autentikointitarkoitukseen. Henkilökunnan kannettavat tietokoneet olisi parasta liittää suoraan AD-verkkoon, niin että ne kirjautuvat samalla AD-tunnuksella sisään kannettavalla tietokoneella ja autentikoivat automaattisesti palvelimelle, niin käyttäjät pääsevät myös käsiksi omiin profiileihinsa ja verkkoresursseihin. Verkkoresursseihin pääsee myös ilman tätä, mutta silloin kaikki verkkoresusrssit on liitettävä erikseen tietokoneelle tai ne on selattava verkkoympäristöstä. Mikäli käyttäjällä on oma tunnus tietokoneeseen ja toinen AD-verkkoon, on merkintä poistettava.

On kuitenkin huomioitavaa, että käyttäjänimi, mikä rekisteröidään NPS-palvelimelle, on tietokoneelle kirjaudutun tilin tunnus.

Kuva 14. Autentikointi.

Kun asetukset on annettu, käynnistyy ilmoitus, joka pyytää antamaan käyttäjätunnuksen, jotta voidaan kirjautua verkkoon. Tätä ilmoitusta painamalla päästään varsinaiseen kirjautumisikkunaan, johon kirjoitetaan käyttäjänimi ja salasana. Logon domain-kenttä voidaan jättää tässä tyhjäksi, koska verkossa on vain yksi domain.



Kuva 15. WLAN-käyttäjän osoitetiedot.

6 TYÖN TULOKSET

Työ tehtiin monessa eri vaiheessa. Ensimmäisessä vaiheessa työstä tehtiin palvelinosuus mahdollisimman pitkälle ilman verkkolaitteiden liittämistä työhön. Tässä vaiheessa palvelimelta käynnistettiin kaikki työssä vaaditut palvelut, määriteltiin group policyt ja lisättiin käyttäjät Active Directoryyn. Ensimmäinen osuus suoritettiin yhdellä tietokoneella, ja sen toimivuutta testattiin VMWare workstation virtuaalikäyttöjärjestelmillä. Tämä mahdollisti monen laitteen samanaikaisen käytön yhdeltä tietokoneelta, mikä suuresti nopeutti työtä ja vähensi vaadittavien laitteiden määrää.
Työn toisessa vaiheessa asennettiin ensin palvelin sen mukaan, mitä ensimmäisessä vaiheessa oli tehty ja liitettiin kiinteän verkon laiteet työhön. Tässä vaiheessa ei tehty mitään uutta, vaan testattiin ainoastaan, että asetukset toimivat myös fyysisillä laitteilla.

Työn kolmannessa osuudessa lisättiin myös langattoman verkon laitteet ja määriteltiin niiden asetukset. Langattoman verkon asetuksia sai vasta tässä vaiheessa määriteltyä, koska laitteet vaativat palvelimen toimiakseen täydellisesti ja aiemmassa vaiheessa ei ollut mahdollista näitä laitteita liittää palvelimeen. Osuudet kaksi ja kolme haluttiin myös erottaa, jotta mahdollisessa vikatilanteessa ei vian etsintään kuluisi pitkään. Jos langaton verkko ei toimi, on helpompaa alkaa etsiä vikaa, kun tiedetään, että kiinteä verkko ja palvelin toimivat.

Työn viimeisessä osuudessa lisättiin langattomaan verkkoon päätelaitteet. Käytettiin muutamaa erityyppistä laitetta varmistamaan verkon ja kirjautumisen toimivuus. Toinen laitteista oli kannettava tietokone ja toinen normaali pöytäkone, johon on lisätty langaton verkkokortti. Molemmissa tietokoneissa oli käyttöjärjestelmänä Windows XP Professional, ja niihin oli asennettu kaikki päivitykset. Lyhyen asetusten määrittelyn jälkeen molemmat tietokoneet saatiin kytkeytymään langattomaan verkkoon. Autentikoinnin toiminta varmistettiin myös NPS-palvelimen lokitiedostoista, joista nähtiin myös onnistumista edeltäneet epäonnistuneet autentikointi- ja yhdistämisyritykset.

LÄHTEET

1. Ivens, Kathy. Windows Server 2003: The Complete Reference, Brandon A. Nordin

2. S. Gast, Matthew. 802.11 Wireless Network: The Definite Guide, O'Reilly

3. Cisco Systems, Understanding the Lightweight Access Point Protocol [Verkkodokumentti, viitattu 4.11.2009] Saatavissa: http://www.conticomp.com/PDF/LWAPP_td.pdf

4. Tittel, Ed & Korelc, Justin. Windows Server 2008 For Dummies, Wiley Publishing