TIETOTURVALLISEN LANGATTOMAN LÄHIVERKON TOTEUTUS HAKEMISTOPALVELUUN INTEGROITUNA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Opinnäytetyö
Kevät 2006
Juha Korhonen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KORHONEN, JUHA:
Tietoturvallisen langattoman lähiverkon toteutus hakemistopalveluun integroituna

Tietoliikennetekniikan opinnäytetyö, 60 sivua

Kevät 2006

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli suunnitella päivitys tietoturvaltaan jo vanhentuneelle langattomalle lähiverkolle. Tarkoituksena oli selvittää teorian ja käytännön toteutuksen avulla, kuinka langattoman verkon tietoturva saataisiin nykyaikaiselle tasolle ja kuinka turvallinen langaton verkko tulee toteuttaa. Vanha verkko pohjautui 802.11b standardin mukaisiin laitteisiin, ja salauksessa käytettiin ainoastaan WEP-salausta. Työn tärkeimpänä lähtökohtana olikin mahdollisimman hyvän tietoturvan takaaminen uuteen verkkoon.

Työn teoriaosuudessa käsitellään langattomien verkkojen yleisiä ominaisuuksia sekä tutustutaan erilaisiin langattomien lähiverkkojen standardeihin. Teoriaosuuden tietoturvaosiossa on otettu esille menetelmiä, joilla langattomasta verkosta saataisiin mahdollisimman tietoturvallinen. Lisäksi on esitelty erilaisia autentikointimenetelmiä, langattoman lähiverkon suunnittelua sekä Windowsin Active Directoryn pääpiirteitä. Teoriaosuuden pääpaino on kuitenkin langattoman verkon tietoturvaongelmissa ja ulkoisten uhkien torjumisen erilaisissa vaihtoehdoissa.

Käytännön osuudessa suunniteltiin ja rakennettiin jo olemassa olevalle langattomalle verkolle korvaava ratkaisu. Uuden mallin mukainen ratkaisu käyttää vahvaa käyttäjän ja laitteiden tunnistamista. Peruselementtinä uudessa verkossa on Microsoftin IAS-palvelin, joka on Microsoftin toteutus RADIUS-protokollasta. Microsoft IAS tarjoaa keskitetyn käyttäjän autentikoinnin, joka perustuu tietokantoihin. Tietokannat pitävät sisällään tiedot käyttäjätunnuksista ja salasanoista. Käyttäjätietokantana IAS käyttää Windows Server 2003 Active Directorya. Työssä asennettiin ja konfiguroitiin kaikki verkon komponentit: palvelin, tukiasemat sekä työasemat. Tukiasemiksi valittiin Cisco Aironet 1230AG, johon oli mahdollista määritellä kaikki halutut ominaisuudet.

Opinnäytetyön tuloksena syntyi 802.1x standardiin perustuva ratkaisu yrityksen käyttöön. Rakennetun langattoman verkon suorituskyky ja tietoturva täyttää tämänhetkiset vaatimukset hyvin.

Asiasanat: langaton lähiverkko, 802.1x, Microsoft IAS, RADIUS

Lahti University of Applied Sciences
Faculty of Technology

KORHONEN, JUHA:
Implementing a secure wireless local area network integrated in Active Directory

Bachelor's thesis in Telecommunications, 60 pages

Spring 2006

ABSTRACT

The purpose of the study was to plan an upgrade to a wireless local area network which had outdated security. The intention was to find out how to build a wireless local area network where the security settings meet the present demands. This was done with the help of source material and practical testing. The old network was based on the 802.11b standard. The network equipment was also based only on that standard and the only security method used was WEP encryption. When planning a new network the most important task was to build as strong security methods as possible.

The theoretical part deals with general features of wireless networks. Also different wireless network standards are presented. The part on security presents different methods of making a wireless network as secure as possible. In addition, it presents different kinds of authentication methods, designing of the wireless network and main features of the Windows Active Directory. The main focus of the theoretical part, however, was to study security flaws of the wireless networks and how to protect them against the threats from outside.

In the practical part of the study a new network to replace the old one was designed and implemented. The new network uses strong user and device authentication. The basic element is a Microsoft IAS server, which is Microsoft's implementation of the RADIUS protocol. Microsoft IAS provides centralized user authentication, which is based on databases. These databases include information about usernames and passwords. As a database IAS uses Windows Server 2003 Active Directory. In the practical part, all the components of the network, i.e. server, access points and workstations, were installed and configured. The access points used were Cisco Aironet 1230 AG models which have all the necessary features.

The result of this thesis was a security solution for the company's use. The solution is based on the 802.1x standard. The wireless network which was built has enough capacity and security for today's needs.

Key words: Wireless Local Area Network, 802.1x, Microsoft IAS, RADIUS

SISÄLLYS

1 JOHDANTO 1

2 LANGATTOMAT LÄHIVERKOT 2

2.1 Yleistä langattomista lähiverkoista 2
2.2 Langattomien lähiverkkojen historiaa 2
2.3 WLAN, edut ja haitat 3
2.4 IEEE 802.11-standardit 5
2.4.1 802.11 5
2.4.2 802.11b 5
2.4.3 802.11a 6
2.4.4 802.11g 7
2.4.5 802.1x 7
2.4.6 802.11i 9
2.4.7 802.11n 10

3 WLAN-VERKON TIETOTURVA 11

3.1 Yleistä tietoturvasta 11
3.2 WLAN-verkon tietoturvauhat 12
3.3 WLAN-salaustekniikat 13
3.3.1 SSID 13
3.3.2 MAC-osoitetunnistus 14
3.3.3 WEP-salaus 14
3.3.4 WPA (Wi-Fi Protected Access) 16
3.3.5 TKIP ja muut WPA:n ominaisuudet 16
3.4 Sertifikaatit 18
3.5 PKI-järjestelmä 19
3.6 RADIUS 20
3.7 Microsoft IAS 21

4 AUTENTIKOINTIPROTOKOLLAT 23

4.1 AAA-protokolla 23
4.2 PPP-protokolla 23
4.3 LCP- ja NCP-protokolla 24
4.4 PAP- ja CHAP-autentikointiprotokollat 24

4.5 EAP-protokollat 25
4.5.1 EAP-TLS 26
4.5.2 PEAP (MSCHAPv2) 28
5 ACTIVE DIRECTORY 33
5.1 Yleistä 33
5.2 Active Directory ja DNS 33
5.3 Active Directoryn käsitteet ja ominaisuudet 34
6 LANGATTOMAN LÄHIVERKON SUUNNITTELU 36
6.1 Yleistä 36
6.2 Katselmus 36
6.3 Asennus ja käyttöönotto 38
7 KÄYTÄNNÖN TOTEUTUS 39
7.1 Lähtökohdat 39
7.2 Laiteympäristö 39
7.3 Tukiasemien konfigurointi 41
7.4 Päätelaitteiden määritykset 46
7.5 Microsoft IAS ja RADIUS 48
7.6 Sertifikaatit 53
7.7 Vanhan ja uuden järjestelmän vertailu 55
8 YHTEENVETO 57
LÄHTEET 58

LYHENNELUETTELO

AAA	Authentication, Authorization and Accounting, AAA protokolla on menetelmä, jolla voidaan identifioida toinen osapuoli tietoverkossa
AES	Advanced Encryption Standard, kehittynyt salausstandardi
CA	Certification Authority, luotettu taho, joka varmistaa sertifikaatin aitouden
CHAP	Challenge Handshake Authentication Protocol, PPP-protokollan päällä toimiva autentikointiprotokolla
CKK	Complementary Code Keying, 802.11b-koodaustekniikka
CMMP	Counter-Mode Cipher Block Chaining Message Authentication Code Protocol, 802.11i-lohkosalaus
DNS	Domain Name System, nimipalvelu, jonka tehtävänä on muuntaa nimet osoitteiksi ja osoitteet nimiksi
DSSS	Direct Sequence Spread Spectrum, suorasekvenssihajaspektritekniikka
EAP	Extensible Authentication Protocol, PPP-protokollan laajennukseksi määritelty protokolla
EAP-MD5	Extensible Authentication Protocol-Message Digest 5, EAP-autentikointiprotokolla, joka perustuu MD5 hasheihin
EAPOL	Extensible Authentication Protocol over LAN, määrittelee, miten EAP-viestit kapseloidaan ja kuljetetaan 802.11-verkossa
EAP-SIM	Extensible Authentication Protocol - Subscriber Identity Module, SIM-kortteihin perustuva EAP-autentiprotokolla
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security, julkisiin avaimiin perustuva EAP-autentikointiprotokolla
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security, EAP-autentikointiprotokolla, joka käyttää kaksivaiheista autentikointimenettelyä
IAS	Internet Authentication Service, Microsoftin toteutus RADIUS-protokollasta
IEEE	Institute of Electrical and Electronics Engineering, standardisointiorganisaatio
IV	Initialization Vector, alustusvektori

LCP	Link Control Protocol, PPP-yhteyksien käyttämä protokolla
LEAP	Lightweight Extensible Authentication Protocol, Ciscon EAP-autentikointiprotokolla
MAC	Media Access Control, verkkosovittimen ethernet-verkossa yksilöivä osoite
MD5	Message Digest 5, tiivistealgoritmi
MIC	Message Integrity Check, tarkistussumma
MIMO	Multiple Input, Multiple Output, moniantennitekniikka
MPPE	Microsoft Point-to-Point Encryption, salausavain
MSCHAPv2	Microsoft Challenge-handshake authentication protocol, ks. PEAP
NCP	Network Control Protocol, PPP-yhteyksien käyttämä protokolla
OFDM	Orthogonal Frequency-Division Multiplexing, moniaaltomodulointi
PAP	Password Authentication Protocol, PPP-protokollan päällä toimiva autentikointiprotokolla
PDA	Personal Digital Assistant, kämmentietokone
PEAP	Protected Extensible Authentication Protocol, EAP-protokolla, joka käyttää kaksivaiheista autentikointimenettelyä
PKI	Public Key Infrastructure, julkisten avainten jakelujärjestelmä
POE	Power Over Ethernet, virran toimittaminen tukiasemalle ethernet-kaapelia pitkin
PPP	Point-to-Point Protocol, suora yhteys verkkolaitteiden välillä
RADIUS	Remote Access Dial-In User Service, autentikointipalvelimessa toimiva autentikointiprotokolla
RC4	Rivest Cipher 4, salausalgoritmi
SSID	Service Set Identifier, langattoman verkon nimi
TKIP	Temporal Key Integrity Protocol, muuttuva-avaiminen salausmenetelmä
TSC	TKIP Sequence Counter, sekvenssilaskuri
TTAK	TKIP mixed Transmit Address and Key
WEP	Wired Equipvalent Privacy, salausmenetelmä
VLAN	Virtual LAN, virtuaalilähiverkko
WPA	Wireless Fidelity Protected Access, tietoturvatekniikka
WPA-PSK	WPA Pre Shared Key

1 JOHDANTO

Opinnäytetyössäni on tarkoituksena suunnitella päivitys tietoturvaltaan jo vanhentuneelle WLAN-verkolle. Työn tarkoituksena on selvittää, kuinka langattoman verkon tietoturva saataisiin nykyaikaiselle tasolla ja kuinka turvallinen langaton verkko tulee toteuttaa. Vanha verkko pohjautui 802.11b-standardin mukaisiin laitteisiin ja salauksessa käytettiin ainoastaan WEP-salausta (Wired Equipvalent Privacy). Työn tärkeimpänä lähtökohtana olikin mahdollisimman hyvän tietoturvan takaaminen uuteen verkkoon.

Työn teoriaosuudessa tutustutaan langattomien verkkojen erilaisiin ominaisuuksiin. Luvussa kaksi on kerrottu yleistä tietoa langattomista verkoista sekä esitelty yleisimpiä käytössä olevia WLAN-standardeja. Kolmannessa luvussa esitellään erilaisia autentikointiprotokollia ja niiden ominaisuuksia. Neljännessä luvussa perehdytään langattomien verkkojen tietoturvaan. Siinä esitellään erilaisia salaustekniikoita, sertifikaatteja sekä RADIUS-palvelimen (Remote Access Dial-In User Service) toimintaperiaatetta. Viidennessä luvussa on esitelty lyhyesti langattoman verkon suunnittelua. Luvussa kuusi on esitelty varsinainen käytännön toteutus. Siitä ilmenee, mitkä menetelmät otettiin käyttöön uuden verkon osalta. Luvussa on kerrottu yksityiskohtaisesti verkon eri komponenttien konfiguroinnista.

Työn tavoitteena on rakentaa langaton verkko, jonka suorituskyvyn tuli olla riittävä normaaliin työasemakäyttöön. Myös tietoturvan tulisi nousta sellaiselle tasolle, että ulkopuolisten tunkeutuminen yrityksen verkkoon WLAN:ia hyväksi käyttäen voidaan riittävän varmasti estää. Jo alusta alkaen oli selvillä se, että tietoturvan pohjana tulee toimimaan Microsoft IAS-palvelimeen (Internet Authentication Service) perustuva RADIUS-autentikointi.

2 LANGATTOMAT LÄHIVERKOT

2.1 Yleistä langattomista lähiverkoista

Langattomien lähiverkkojen (WLAN, Wireless Local Area Network) idea ja tarve ovat syntyneet, kun kannettavien työasemien määrä on kasvanut yhä suuremmaksi. WLAN mahdollistaa verkkojen muodostamisen erilaisten tietojärjestelmien välille langattomasti. Kiinteissä verkoissa käyttäjä on sidottu työskentelemään verkkopistokkeiden läheisyydessä kun taas langattoman verkon käyttäjä voi kulkea vapaasti tukiasemaverkon kuuluvuusalueella.

Tavallisesti WLAN-verkko koostuu WLAN-kortilla varustetusta kannettavasta työasemasta tai PDA-laitteesta (Personal Digital Assistant). Ne voivat olla yhteydessä sekä toisiinsa että muuhun tietojärjestelmään tukiasemien kautta.

Langattomat verkot ovat yleistyneet vauhdilla mitä erilaisimmissa käyttötarkoituksissa (koulut, hotellit, lentokentät) johtuen verkon käytön ja rakentamisen helppoudesta. WLAN-verkkojen yleistyessä myös tietoturvaongelmat lisääntyvät. Etenkin yksityisten käyttäjien WLAN-verkoissa ei yleensä ole paneuduttu riittävästi tietoturvaan. Puutteellisesti hoidettu tietoturva johtaa siihen, että verkossa liikkuva data on kaikkien ulottuvilla.

2.2 Langattomien lähiverkkojen historiaa

Langattomien lähiverkkojen historia alkaa 1980-luvun puolestavälistä, jolloin Motorola esitteli ensimmäisen WLAN-tuotteensa, Altairin. Tämä, kuten muutkin 1980- ja 1990-luvun alun ratkaisut olivat valmistajakohtaisia. Tuon ajan tekniikan käyttäjät joutuivat siis sitoutumaan yhteen laitteistotoimittajaan. Siirtonopeudet langattomissa olivat silloin verrattavissa senaikaisten jaetun median koaksiaalikaapeli- ja keskitinverkkoihin. (Puska 2005, 13–14.)

Standardisointityö langattomissa lähiverkoissa aloitettiin vuonna 1990, jolloin IEEE:n LAN/MAN-standardointiryhmä (Institute of Electrical and Electronics

Engineering) aloitti toimintansa. Työn tuloksena julkaistiin ensimmäinen 802.11-standardi vuonna 1990. Siirtonopeudet ensimmäisissä 802.11 verkoissa olivat ainoastaan 1 ja 2 Mbits. Pari vuotta tämän jälkeen julkaistiin 802.11b standardi, joka oli nopeudeltaan jo 11 Mbits. Tämä standardi sai hyvän vastaanoton kuluttajamarkkinoilla. Sitä voidaankin pitää ensimmäisenä standardina, joka oli (ja on edelleen) erittäin yleisessä käytössä ja avasi varsinaisesti "pään" langattomille lähiverkoille. (Puska 2005, 13–16.)

2.3 WLAN, edut ja haitat

Langattomat lähiverkot ovat tuoneet perinteiseen lankaverkkoon verrattuna mukanaan monia etuja. Seuraavassa on mainittu muutamia niistä.

- Langattoman lähiverkon suurin hyöty on päätelaitteen mahdollisuus käyttää verkon palveluja ilman, että se on kytkettynä kiinteään kaapelointiin. Tämä mahdollistaa toimistokäytössä monenlaisia etuja. Esimerkiksi omasta työpisteestään voi lähteä palaveriin ilman, että yhteys verkkoon missään vaiheessa katkeaa, tai nykyisin hyvin yleisissä avokonttoreissa mahdollistaa langattomuus ihmisten työskentelyn toimiston jokaisessa pisteessä. (Puska 2005, 18.)

- Langattomuus on mahdollistanut uudenlaisten päätelaitteiden ja sovellusten käytön. Esimerkiksi yritysten tavaravarastojen seuraaminen ja ylläpito voidaan hoitaa langattomien lähiverkkojen avulla. Työntekijöillä voi olla käytössään viivakoodinlukijat ja kämmentietokoneet, joilla he voivat syöttää, tavaraa varastosta noudettaessa tai sitä sinne tuotaessa, muuttuneen tilanteen, joka sitten päivittyy suoraan tietokantaan. Varaston tilanne pysyy silloin erittäin hyvin reaaliaikaisena. (Puska 2005, 19.)

- Langaton verkko on myös perinteistä yleiskaapelointiin perustuvaa lähiverkkoa helpompi, halvempi ja nopeampi asentaa. Yrityskäytössä se mahdollistaa sellaistenkin rakennusten kohtuullisen vaivattoman verkottamisen, joissa ei ole aikaisemmin verkkoa ollut. Koti-

käytössä voidaan WLAN:in avulla jakaa internet yhteys useamman työaseman kesken. (Puska 2005, 19.)

- Tilapäisten verkotusten tekeminen on huomattavasti helpompaa toteuttaa langattomasti. Tällaisia ratkaisuja näkeekin usein esim. messuilla, kongresseissa, urheilutapahtumissa ym. vastaavissa tilaisuuksissa, jotka ovat yleensä kestävät muutamia päiviä. (Puska 2005, 20.)

Langattomien lähiverkkojen tekniikka on vielä iältään kohtuullisen nuori. Se on tuonut tullessaan useita teknisiä ja taloudellisia haasteita. Seuraavassa on mainittu joitain suurimpia ongelmakohtia.

- Radiotiestä johtuva huono tietoturva. Radioaaltoja ei voi pysäyttää tietyn maantieteellisen alueen sisälle vaan ne kuuluvat yleensä halutun alueen ulkopuolelle. Tämä mahdollistaa verkon kuuntelemisen ja häiritsemisen ulkopuolelta käsin. Tätä ongelmaa on kuitenkin nykyisin pyritty korjaamaan kehittelemällä uusia tietoturvaratkaisuja. (Puska 2005, 23.)

- Suorituskyky langattomissa lähiverkoissa ei yllä Ethernet-lähiverkkojen tasolle. Yhden yhteyspisteen WLAN-solu tarjoaa jaettua kaistaa, josta päätelaitteet kilpailevat. Käytännössä asemakohtainen siirtokapasiteetti voi jäädä huonoimmassa tapauksessa jopa 0,5 Mbits:iin. Siirtokapasiteetti vaihtelee päätelaitteiden määrän, kentänvoimakkuuden ja päätelaitteiden sijainnin mukaan. (Puska 2005, 23.)

- Rakennusten verkottaminen on vaikea toteuttaa niin, että verkon kuuluvuus olisi joka paikassa hyvä. Kentän voimakkuuteen ja samalla langattoman verkon suorituskykyyn vaikuttavat tekijät kuten, kalusteet, seinät, ulkoiset häiriölähteet yms. ovat vaikeita ennakoida ja mallintaa verkkoa suunniteltaessa. Tämän vuoksi langattoman ver-

kon suunnittelu on ja asennus on vaativampaa kuin lankaverkkojen tapauksessa. (Puska 2005, 24.)

2.4 IEEE 802.11-standardit

802.11 on IEEE:n yleinen standardi langattomille lähiverkoille. IEEE 802.11-suosituksen tehtävänä on määritellä toiminta sellaisessa langattomassa lähiverkossa, jossa kanavavaraukseton päätöksenteko on yksittäisillä työasemilla tai keskitetysti tukiasemalla. Seuraavissa luvuissa on esitelty tärkeimmät WLAN standardit 802.11, 802.11b, 802.11g ja 802.11a. Lisäksi on esitelty tietoturvastandardit 802.1x ja 802.11i.

2.4.1 802.11

IEEE 802.11-suosituksen ensimmäinen versio hyväksyttiin vuonna 1997. Alkuperäinen siirtonopeus oli yksi ja kaksi megabittiä sekunnissa. Standardi sisälsi verkoille monia vaihtoehtoisia toteutuksia eikä taannut keskinäistä yhteensopivuutta, mikä vähensi niin laitevalmistajien kuin kuluttajienkin suosiota. Paranneltu versio julkaistiin vuonna 1999, ja se toi mukanaan kaksi laajennusta: IEEE 802.11a, joka toimii 5 GHz:n ISM-alueella, ja IEEE 802.11b, joka toimii 2,4 GHz:n ISM-alueella. (Granlund 2001, 230.)

2.4.2 802.11b

Jatkuvasti kehittyvien verkkosovellusten ja langattomien verkkojen laajentuneen käytön takia 802.11-standardin määrittämät nopeudet kävivät auttamatta liian hitaiksi ja tarvittiin uusi standardi, joka vastaisi paremmin käyttäjien ja sovellusten vaatimuksiin. IEEE julkaisi syyskuussa 1999 802.11b-standardin. Siinä määriteltiin tiedonsiirtonopeudet 5,5 ja 11 Mbps sekä parempi yhteyden laatu. Suurempaa tiedonsiirtonopeutta varten valittiin suorasekvenssi. 802.11b-järjestelmät toimivat 1 ja 2 Mbps 802.11 DSSS-järjestelmien (Direct Sequence Spread Spectrum) kanssa. Koodaustekniikka CKK (Complementary Code Keying) kehitettiin 802.11-standardin nopeuden lisäämiseksi. (Geier 2002a.)

802.11b-laitteet ovat edelleen yleisesti käytettyjä. Niiden liikennöinti tapahtuu 2,4 ja 2,4835 GHz:n välisellä vapaalla ISM-taajuusalueella, joka on jaettu 13 kanavaan 5 MHz:n välein. Samaa taajuutta käyttävät muun muassa bluetooth-laitteet. Vapaan taajuusalueen ansiosta jokainen voi pystyttää verkon mihin tahansa ilman radiolupaa, kunhan ei ylitä suurinta sallittua, 100 mW:n, lähetystehoa. Samalla taajuusalueella toimivat laitteet sekä erilaiset esteet tekevät mahdottomaksi kuitenkin tällaisiin nopeuksiin yltämisen. Todellinen nopeus jää maksimissaankin välille 5-7 Mbps. (Geier 2002a.)

802.11b-standardissa käytetään WEP-salausta. Salaus pohjautuu RC4-algoritmiin (Rivest Cipher 4). RC4 on symmetrinen salausmenetelmä, jossa salaus puretaan samalla avaimella, millä se on kirjoitettu. Käytännössä verkon kaikille laitteille on määritelty sama salausavain. Mahdollinen salausavaimen pituus voi olla 40, 64 tai 128 bittiä. WEP toimii vähäisimpänä langattoman verkon turvana kohtuullisen hyvin, ja sen luoma tietoturva on ainakin kotikäytössä riittävä. (Geier 2002a.)

2.4.3 802.11a

Standardi julkistettiin samaan aikaan kuin 802.11b. A-version nopeus yltää teoriassa 54 Mbps:n nopeuteen. 802.11a toimii Pohjois-Amerikassa vapaasti käytettävällä 5 GHz:n U-NII (Unilicensed National Information Infrastructure), joka sisältää kolme taajuuskaistaa. (Puska 2005, 40.)

- Neljä kanavaa taajuusalueella 5,15–5,25 GHz, jolloin maksimilähetysteho saa olla 40 mW. Tämän taajuusalueen käyttö on sallittua vain sisätiloissa. (Puska 2005, 41.)

- Neljä kanavaa taajuusalueella 5,25–5,35 GHz maksimilähetystehon ollessa maksimissaan 200 mW. Tämänkin taajuusalueen käyttö on sallittua vain sisätiloissa. (Puska 2005, 41.)

- Neljä kanavaa taajuusalueella 5,725–5,825 GHz maksimiteholla 800 mW. Tämän taajuusalueen käyttö on sallittua sekä sisä- että ulkotiloissa. (Puska 2005, 41.)

Kaikkien edellä mainittujen taajuusalueiden käyttö ei ole Euroopassa vapaasti käytettävissä. Esimerkiksi Suomessa 802.11a-verkossa saa käyttää vapaasti taajuusalueita 5,15–5,25 GHz sekä 5,25–5,35 GHz. Molemmissa saadaan käyttää maksimitehoa 200 mW ja käyttö on sallittu ainoastaan sisätiloissa. (Puska 2005, 44.)

802.11g-standardi käyttää moniaaltomodulointia (OFDM, Orthogonal Frequency Division Multiplexing). OFDM-tekniikassa siirrettävä data jaetaan eri taajuuksisiin alikanaviin, joita sitten käytetään rinnakkain. (Puska 2005, 46.)

Eurooppalaista 802.11g-standardia korkeamman taajuuden vuoksi radioaaltojen vaimennus on suurempaa, mistä aiheutuu pienempi kantomatka ja suuremman lähetystehon ja tehonkulutuksen tarve (Puska 2005, 46).

2.4.4 802.11g

802.11g-standardi on laajennus 802.11b-standardiin. Tämä standardi on täysin alaspäin yhteensopiva 802.11b-standardin kanssa. Suurin ero on siirtonopeus, joka 802.11g-verkossa on maksimissaan 54 Mbps. Muita nopeusluokkia ovat 48, 36, 24, 12 ja 6 Mbps. 802.11b- ja g-verkkojen käyttäminen rinnakkain samalla alueella heikentää g-verkon suorituskykyä huomattavasti. Tällöin g-standardin mukaiset laitteet eivät pääse niiden teoreettiseen maksiminopeuteen. Laitteet liikennöivät 802.11b:n tapaan 2,4 ja 2,4835 GHz:n välisellä vapaalla ISM-taajuusalueella, joka on jaettu 13 kanavaan 5 MHz:n välein. Suurin sallittu lähetysteho g-standardissa on 100 mW, ja sen käyttö on sallittua sekä sisä-, että ulkotiloissa. 802.11g-standardi käyttää 802.11a:n tapaan moniaaltomodulointia. Tämän modulointitekniikan käyttö mahdollistaa b-standardia nopeamman tiedonsiirron. (Geier 2002a.)

2.4.5 802.1x

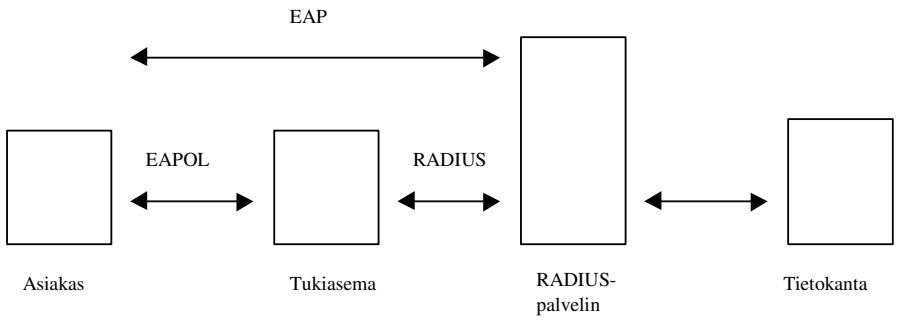
IEEE 802.11-standardin tukemat tietoturvamekanismit eivät tarjoa riittävää tietoturvan tasoa yritysten langattomille verkoille. WEP-protokolla on osoittautunut tietoturvaltaan heikoksi ja avainten jakaminen ongelmalliseksi. IEEE on määritellyt 802.1x-standardin 802-lähiverkoille. 802.1x-standardi mahdollistaa dynaami-

sen istunto- ja käyttäjäkohtaisen avaimen sekä käyttäjän autentikoinnin. Standardi tukee useita autentikointimenetelmiä, kuten sertifikaatteja ja julkiseen avaimeen perustuvaa tunnistusta. 802.1x käyttää EAP-protokollaa (Extensible Authentication Protocol), joka tukee RADIUS:sta. Kyseistä standardia voidaan käyttää myös langallisessa lähiverkossa, jolloin niidenkin autentikointi voidaan suorittaa samalla protokollalla. (Jokisuu 2002; Geier 2002b.)

802.1x-määrittely mahdollistaa lähiverkkotekniikoissa paremman tietoturvan tason 802.11-tietoturvamekanimeihin verrattuna, sillä käyttäjä autentikoidaan porttikohtaisesti. Langattomissa lähiverkoissa tukiasema muodostaa jokaista autentikoituvaa käyttäjää kohden oman virtuaaliportin, jonka avulla liikennöinti voidaan estää tai sallia. Ensin asiakas liikennöi auktorisoimattoman portin kautta. Tällöin tukiasema ohjaa liikenteen autentikointipalvelimelle, joka tekee päätöksen verkkoon pääsyn sallimisesta tai kieltämisestä. Portin ollessa auktorisoimattomassa tilassa sallitaan ainoastaan EAP-viestien lähetys. Jos käyttäjän autentikointi onnistuu, asiakkaan virtuaaliportti siirretään auktorisoituun tilaan ja asiakas voi liikennöidä normaalisti verkossa. (Jokisuu 2002; Geier 2002b.)

802.1x-standardi ottaa kantaa vain asiakkaan ja autentikoijan väliseen liikenteeseen eikä tarjoa varsinaista autentikointimekanismia. Asiakkaan ja autentikoijan välinen liikenne toteutetaan EAPOL-protokollalla (Extensible Authentication Protocol over LAN). Kyseinen protokolla määrittelee, miten EAP-viestit kapseloidaan ja kuljetetaan 802.11-verkossa. (Heikkinen 2003.)

Kuviossa 1 on esimerkki 802.1x-autentikaatiosta. Siinä autentikointitieto siirtyy asiakkaan ja RADIUS-palvelimen välillä EAP-protokollalla. Tämä puolestaan on sovitettu EAPOL:n päälle asiakkaan ja tukiaseman välillä sekä RADIUS-protokollan päälle tukiaseman ja RADIUS-palvelimen välillä. RADIUS-palvelin puolestaan hakee varsinaisen käyttäjätiedon tietokannasta käyttäen tietokantakohtaista protokollaa. (Heikkinen 2003.)



KUVIO 1. 802.1x:n autentikointi

2.4.6 802.11i

802.11i on langattomien 802.11-verkkojen viimeisin tietoturvastandardi. Sen olisi tarkoitus lopullisesti ratkaista kaikki 802.11-verkkojen ongelmat. Standardissa määritellään 802.1x:n mukainen todentamis- ja avaintenhallintakäytäntö sekä parannetut menetelmät tiedon salaukseen. Sen tärkeimmät parannukset ovat seuraavanlaisia:

- Istuntokohtaiset TKIP-avaimet (Temporal Key Integrity Protocol) sekä avainten hallinnan, joka perustuu avainpareihin. WLAN-asema ja yhteyspiste salaavat liikenteen parittaisella lähetysavaimella, joka vaihdetaan määräajoin turvallisesti. Työasemiin ja autentikointipalvelimeen on määritelty yleisavain, jonka perusteella muut tarvittavat avaimet muodostetaan. (Griffith 2004.)

- CMMP-lohkosalauksen (Counter-Mode Cipher Block Chaining Message Authentication Code Protocol), joka on toteutettu vahvalla AES-salauksella (Advanced Encryption Standard). AES käyttää RC4:ää vahvempaa salausalgoritmia ja 128, 192 ja 256 bitin salausavaimia. (Griffith 2004.)

- Esitunnistuksen ja siirtymisen tukiasemasta toiseen ilman päätelaitteen tai käyttäjän uudelleen tunnistusta. Autentikointipalvelin lähettää tunnistetiedot myös verkon muille tukiasemille. Tämä ominai-

suus nopeuttaa myös roaming-toimintoa, kun siirrytään yhden tukiaseman alueelta toiseen. (Griffith 2004.)

2.4.7 802.11n

Vielä julkaisemattoman IEEE 802.11n-standardin avulla pyritään nostamaan 802.11a- ja 802.11g-standardien määrittelemää tiedonsiirtonopeutta moninkertaiseksi sekä saavuttamaan nykyisiä verkkoja pidempi toimintaetäisyys. Tavoitteena on jopa 540 Mbps teoreettinen tiedonsiirtonopeus, johon pyritään uudenlaisen modulaation, moniantennitekniikan (MIMO, Multiple In, Multiple Out), uuden koodaustekniikan ja uusien kaistanleveyksien avulla. Käytännössä tiedonsiirtonopeus tullee olemaan nykyisten laajakaistaverkkojen tasoa eli noin 100 Mbps. 802.11n-standardin laitteet ovat yhteensopivia 802.11a- ja 802.11g-standardien laitteiden kanssa. (Wilson 2004.)

3 WLAN-VERKON TIETOTURVA

3.1 Yleistä tietoturvasta

Tietoturva on tietoriskien hallintaa poistamalla riskit tai optimoimalla niistä koituvia haittoja. Tietoturva on tietojen suojausta, varmistusta sekä luottamuksellisuuden turvaamista. (Kerttula 1998, 492.)

Tietoturvalle voidaan asettaa kuusi perusedellytystä: luottamuksellisuus, autenttisuus, eheys, kiistämättömyys, pääsynvalvonta ja käytettävyys (Kerttula 1998, 93).

- Luottamuksellisuudella tarkoitetaan sitä, että tietojärjestelmässä oleva tai siirretty tieto on saatavilla vain siihen oikeutetuille henkilöille, eikä tietoja myöskään paljasteta tai anneta sivullisten käyttöön (Kerttula 1998, 93).

- Autentikointi eli todentaminen on menetelmä, jolla alkuperäinen henkilö tai tieto voidaan erottaa muista. Esimerkiksi verkon käyttäjän tulee kirjoittaa oikea salasana päästäkseen käyttämään omaa verkkotiliään. (Kerttula 1998, 93.)

- Eheydellä pyritään tietojen sekä järjestelmien rakenteiden ja sisältöjen muuttumattomuuteen. Eheys edellyttää myös, että tiedot eivät muutu tai tuhoudu laitteisto- tai järjestelmävian, inhimillisen erehdyksen tai ulkoisen hyökkäyksen vuoksi. (Kerttula 1998, 94.)

- Kiistämättömyydellä tarkoitetaan sitä, että lähettäjä ja vastaanottaja eivät pysty kiistämään lähettämäänsä tietoa. Esimerkiksi digitaalisen allekirjoituksen avulla vastaanottaja voi todentaa, että sanoman oli lähettänyt väitetty lähettäjä. Kun sanoma on vastaanotettu, lähettäjä voi todentaa, että sanoman on todella vastaanottanut haluttu vastaanottaja. (Kerttula 1998, 94.)

- Pääsynvalvonta tarkoittaa sitä, että vain todennetut henkilöt pääsevät käyttämään palvelua. Identiteettiin perustuva pääsynvalvonta edellyttää aina jonkinlaista autentikointimenetelmää. (Kerttula 1998, 95.)

- Käytettävyydellä tarkoitetaan, että järjestelmien tiedot ja muut resurssit ovat tarvittaessa niihin oikeutettujen käytettävissä (Kerttula 1998, 95).

3.2 WLAN-verkon tietoturvauhat

Langaton lähiverkko on haavoittuvampi kuin langallinen verkko, koska siinä käytetään datan siirtoon radio-aaltoja. Radioaallot läpäisevät fyysisiä esteitä ja leviävät joka puolelle lähettimen ympäristöön. Tämän seurauksena ulkopuolisilla on mahdollisuus kuunnella luottamuksellista dataa vaikka toimiston seinien ulkopuolella. WLAN-verkkojen tietoturvauhat jaetaan passiivisiin ja aktiivisiin uhkiin. Vakavimmat passiiviset uhat ovat seuraavat: (Puska 2005, 89.)

- Liikenteen salakuuntelu, joka on yleensä mahdollista myös rakennuksen ulkopuolella. Tarkoituksena on yleensä kerätä tietoa, joka mahdollistaisi verkkoon tunkeutumisen. Tätä uhkaa on vaikea estää ja mahdotonta havaita. (Puska 2005, 89.)

- Liikenteen analysointi, jolloin ulkopuolinen voi saada selville luottamuksellista tietoa. Analysointiin on saatavilla monia valmiita ohjelmia, joilla on mahdollista selvittää jopa langattoman verkon salausavaimet. (Puska 2005, 89.)

Aktiivisissa tapauksissa tunkeutujan tarkoituksena on lähettää kohdeverkkoon dataa tai häiritsevää signaalia. Aktiivisia uhkia ovat mm. seuraavat:

- Siirtomedian häirintä, joka voidaan toteuttaa WLAN:n kanssa samalla taajuudella toimivilla radiolähettimillä tai ylikuormittamalla WLAN-yhteyspisteitä turhilla palvelupyynnöillä. Tällaisen häirinnän

tarkoituksena voi olla esimerkiksi palveluksenestohyökkäys yritystä vastaan. (Puska 2005, 89.)

- Langattoman verkon mahdollinen uhka on myös datan muokkaus. Kyseessä on tapahtuma, jossa verkossa siirtyvä tieto muokkaantuu, sitä poistuu, siihen lisätään tai se tuhoutuu. Ulkopuolinen taho voi aiheuttaa tämän tahallisesti, mutta myös laitevian seurauksena data saattaa muuttua. Tarkistussummien avulla voidaan päätellä, onko tieto alkuperäisessä muodossa. (Puska 2005, 89.)

- Usein päämääränä on tietojärjestelmään tunkeutuminen ja muita keinoja käytetään tämän päämäärän saavuttamiseksi. Koska langaton verkko on yleensä osa yrityksen muuta tietoverkkoa, voi ulkopuolinen taho päästä WLAN:n kautta käsiksi yrityksen sisäisiin palvelimiin tai työasemiin. (Puska 2005, 89.)

3.3 WLAN-salaustekniikat

Langattomien lähiverkkojen fyysisen tietoturvan puutteen takia, pitää siellä liikkuva tieto pyrkiä salaamaan jollain tavalla. Tämän ongelman takia on langattomien verkkojen suojaksi kehitetty useita erilaisia salaustekniikoita, joita esitellään seuraavissa luvuissa.

3.3.1 SSID

SSID (Service Set Identifier) on langattoman verkon nimi, joka verkkoon haluavan on tiedettävä. SSID tarjoaa alkeellisen pääsynvalvonnan. 802.11-verkoissa tukiasema tunnistaa päätelaitteen tämän tunnuksen perusteella ja hyväksyy palvelupyynnön vain tunnistetulta päätelaitteelta. SSID-tunnus voidaan käsittää yksinkertaiseksi salasanaksi, jolla päätelaitteet tunnistetaan. Luotettava tunnistusmenetelmä se ei kuitenkaan ole. Useissa laitteissa on oletusasetuksena SSID:n nimenä ANY, jolloin verkkoon pääsy mahdollistetaan kaikille. Tämän vuoksi verkko tulee nimetä heti verkon rakentamisen yhteydessä. (Puska 2005, 72–73.)

Oletuksena on, että langattoman verkon tukiasemat lähettävät SSID-tunnuksensa beacon-sanomien mukana. Turvallisuutta voidaan lisätä estämällä tukiasemaa mainostamasta verkon nimeä. Tällöin käyttäjän on tiedettävä verkon nimi saadakseen yhteyden muodostettua. Tämä toimenpide ei kuitenkaan lisää merkittävästi tietoturvaa. On olemassa ohjelmia, joiden avulla verkkoa kuuntelemalla pystytään selvittämään verkon SSID nimi. (Järvinen 2002, 309–311.)

3.3.2 MAC-osoitetunnistus

MAC-osoitetunnistus (Media Access Control) on tietoturvaominaisuus, jonka avulla pystytään rajaamaan verkkoon pääseviä laitteita niiden MAC-osoitteiden perusteella. Osoitetunnistus ei suojaa verkon liikennettä kuuntelulta, mutta estää muiden kuin sallittujen laitteiden pääsyn verkkoon. Jokaisella verkkoon liitettävällä laitteella on oma uniikki tunnisteensa, jota kutsutaan MAC-osoitteeksi. MAC-osoite asetetaan verkkolaitteeseen jo valmistusvaiheessa, eikä samaa osoitetta voi olla kahdella eri laitteella.

Tukiasemaan määritellään hyväksytyt MAC-osoitteet ja listaan kuulumattomien laitteiden kommunikointi estetään. Heikkouksia tässä menetelmässä on se, että MAC-osoitteen vaihto onnistuu ohjelmallisesti ja tukiaseman liikennettä kuuntelemalla on mahdollista saada selville siinä liikennöivien laitteiden osoitteet.

3.3.3 WEP-salaus

WEP on salausmenetelmä, jolla pyritään suojaamaan tukiaseman ja päätelaitteen välinen tiedonsiirto RC4-jonosalauksella. WEP-suojauksen avulla voidaan ehkäistä luvattomien laitteiden kytkeytyminen verkkoon. WEP tukee kahta avainpituutta: 64-bittistä ja 128-bittistä. Nämä salausavaimet sisältävät 24-bittisen alustusvektorin, IV (Initialisation Vector), joka lähetetään salaamattomana radiorajapinnan yli. Loput 40 tai 104 bittiä muodostavat varsinaisen salaisen avaimen. WEP-tunnistus perustuu jaetun avaimen menetelmään. Tämä tarkoittaa sitä, että jokaiselle verkon päätelaitteelle tulee olla määriteltynä sama salausavain kuin tukiasemille. Kuviossa 2 on esitelty jaetun avaimen menettelyn autentikointiprosessi. (Cisco 2006a.)

KUVIO 2. Jaetun avaimen menettelyn autentikointiprosessi (Cisco 2006a)

Sanomaliikenne autentikointiprosessissa on seuraavanlainen (Cisco 2006a):

1. Päätelaite lähettää tukiasemalle Authentication Request-pyynnön, jossa se ilmoittaa tukevansa jaetun avaimen tunnistusta.

2. Tukiasema vastaa Authentication Response-viestillä, joka sisältää satunnaisen haastetekstin (Challenge).

3. Päätelaite salaa haastetekstin omalla WEP-avaimellaan ja lähettää sen takaisin tukiasemalle.

4. Tukiasema purkaa päätelaitteen lähettämän vasteen omalla WEP-avaimellaan ja vertaa tulosta lähettämäänsä haastetekstiin. Jos tulokset ovat samat, myös salausavaimet ovat samat ja tunnistus hyväksytään. Tällöin siitä lähetetään päätelaitteelle kuittaussanoma.

WEP-salaus on helppo murtaa nykypäivän työasemilla ja vapaasti saatavilla olevilla ohjelmilla. Sen takia sen tarjoama tietoturvan taso ei ole yrityskäytössä riittävä. WEP-salauksen ongelmakohtana ovat aikaisemmin mainitut lyhyet alustusvektorit (IV), jotka siis lähetetään salaamattomina jokaisen kehyksen parissa ensimmäisessä bitissä. Tietoliikennettä kuuntelemalla sekä siirrettävää dataa ja samankaltaisia alustusvektoreita seuraamalla voidaan laskea salattu avain eli murtaa verkon salaus. Siirrettävät datamäärät langattomassa verkossa vaikuttavat siihen, kuinka helposti ja nopeasti avain on murrettavissa. (Ahvenainen 2003.)

3.3.4 WPA (Wi-Fi Protected Access)

WPA (Wireless Fidelity Protected Access) on tietoturvaratkaisu, jonka tarkoituksena oli korjata WEP-salauksessa ilmenneet puutteet. WPA suunniteltiin toimivaksi kaikissa 802.11-standardin mukaisissa laitteissa. Se pitää sisällään komponentteja 802.11i-tietoturvastandardista, joka oli vasta kehitteillä, kun WPA julkaistiin. WPA toi mukanaan kokonaan uuden salausalgoritmin sekä käyttäjän tunnistuksen, jota ei WEP-salauksessa ollut lainkaan. (Wi-Fi Alliance 2003.)

WPA-tekniikka koostuu neljästä uudesta algoritmista. Salausta parantamaan on määritelty TKIP sekä laajennettu alustusvektoriavaruus. TKIP pitää myös sisällään MIC-tarkistussumman (Message Integrity Check), joka tarjoaa suojan datapakettien väärennystä vastaan. Autentikointiin ja avainten hallintaan WPA käyttää IEEE 802.1X-standardia ja erilaisia EAP-protokollia. (Wi-Fi Alliance 2003.)

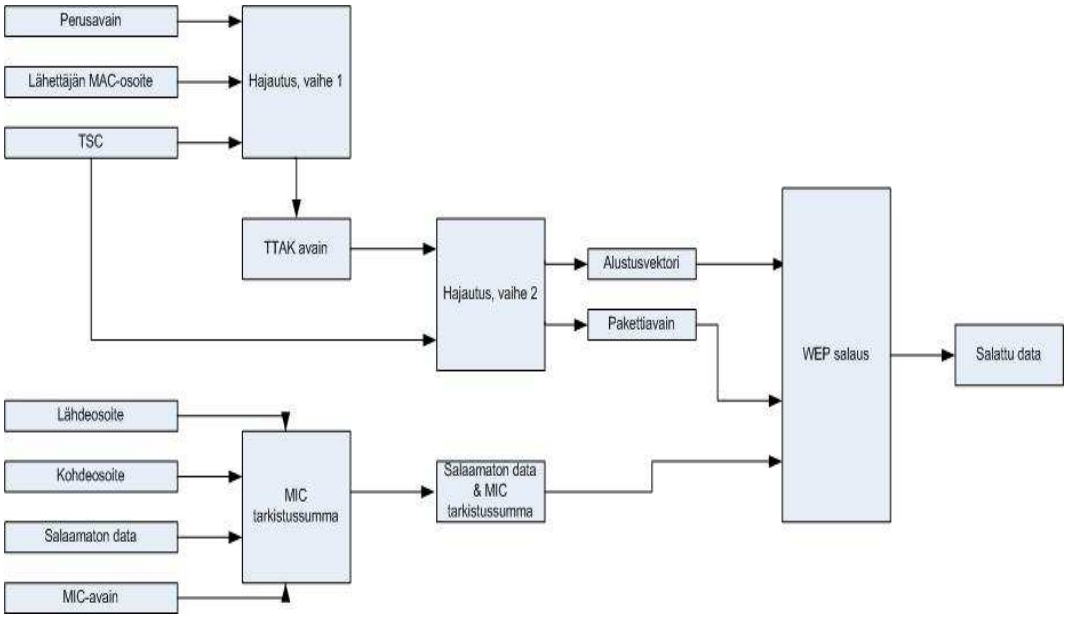
3.3.5 TKIP ja muut WPA:n ominaisuudet

WEP:iin verrattuna TKIP:n käyttö parantaa WLAN verkon turvallisuutta huomattavasti, koska siinä käytetään pakettikohtaisia salausavaimia yhden kiinteän avaimen sijaan. Erilaisia dynaamisesti luotuja salausavain mahdollisuuksia on yli 500 biljoonaa. Salauksessa käytetään edelleen RC4-salausalgoritmia, mutta salausavaimen pituus on 128 bittiä. TKIP-perusavaimen luomisesta ja hallinnoinnista huolehtii autentikointipalvelin (esim. RADIUS) erilaisten EAP-protokollien avulla. Perusavaimesta muodostetaan salauksessa käytettävät pakettiavaimet kaksivaiheisessa prosessissa. Perusavainta sellaisenaan ei käytetä itse salaukseen. (Ahvenainen 2003.)

TSC (TKIP Sequence Counter) on sekvenssilaskuri, jonka tarkoituksena on torjua WLAN-verkkoon kohdistettuja toistohyökkäyksiä. Jokaisella päätelaitteella on oma laskuri, jonka arvoa kasvatetaan aina kun uusi kehys salataan ja lähetetään. Tämä arvo toimitetaan vastaanottajalle WEP-alustusvektorina, joka sitten tarkastaa sekvenssilaskurin arvon. Jos arvo ei ole odotetusti muuttunut, on seurauksena kyseisen paketin hylkääminen. TSC:n pituus on 48 bittiä, eli alustusvektoriavaruus on kasvanut selvästi WEP:ssä käytetystä 24 bitistä. (Ahvenainen 2003.)

Datapakettien väärennystä vastaan käytettävä MIC-tarkistussumma lasketaan lähde- ja kohdeosoitteista sekä salaamattomasta datasta MIC-algoritmia hyväksi käyttäen. Vastaanottaja laskee samaisen MIC-tarkistussumman ja hylkää datapaketin, jos summa ei täsmää. Tämä tarkistussumman hajautusmenetelmä tarvitsee laskentaan MIC-avaimen, jonka luonti tapahtuu pakettiavaimen luonnin yhteydessä. Jos MIC-arvot eivät vastaa toisiaan, on seurauksena vastatoimenpiteet, joilla pyritään torjumaan mahdollinen käynnissä oleva hyökkäys. Näillä toimilla pyritään estämään tiedonsaanti käytetyistä salausavaimista. MIC on tehokas keino estää datan muuttamiseen ja osoitteiden manipulointiin perustuvat tietoturvahyökkäykset. (Ahvenainen 2003.)

Salauksessa käytettävät pakettiavaimet muodostetaan kahdessa vaiheessa. Avaimen muodostamisen vaiheet on esitetty kuviossa 3.



KUVIO 3. TKIP-salauksen toimintaperiaate

Hajautuksen ensimmäisessä vaiheessa muodostetaan hajautusalgoritmia käyttäen TTAK-avain (TKIP mixed Transmit Address and Key). Se koostuu perusavaimesta, lähettäjän MAC-osoitteesta ja TSC:stä. Tässä vaiheessa käytetään perusavaimesta sen 80 ensimmäistä bittiä ja TSC:stä 32 merkitsevintä bittiä. Muodostunut TTAK-avain on pituudeltaan 80 bittiä. Se ei ole jokaiselle paketille yksilöl-

linen, joten samaa avainta voidaan käyttää peräkkäin lähteville paketeille. (Ahvenainen 2003.)

Hajautuksen toisessa vaiheessa muodostetaan edelleen hajautusalgoritmia käyttäen pakettiavain. Sen luomiseen käytetään edellisessä vaiheessa luotua TTAK:ta ja TSC:tä. Pakettiavain pitää sisällään myös alustusvektorin. Perusavaimesta käytetään tässä vaiheessa 24 viimeistä bittiä ja TSC:stä kaikki sen 48 bittiä. Pakettiavain lasketaan jokaiselle lähetettävälle paketille erikseen, joten se on kaikille paketeille yksilöllinen. Vastaanottopäässä suoritetaan sama prosessi uudestaan, jotta salaus saadaan puretuksi ja MIC-arvo tarkastetuksi. (Ahvenainen 2003.)

WPA:n tuomat tietoturvaparannukset on myös mahdollista toteuttaa ilman erillistä autentikointipalvelinta. Tämän menetelmän nimi on WPA-PSK (Pre Shared Key). Sen käyttäminen voisi tulla kysymykseen esim. kotikäytössä. PSK tarjoaa täysin samat tietoturvaominaisuudet kuin täysi TKIP, mutta salauksessa käytetty perusavain pitää asettaa käsin kaikkiin verkon laitteisiin. (Wi-Fi Alliance 2003.)

3.4 Sertifikaatit

Sertifikaatti on sähköinen todistus, joka sisältää joukon tietoja. Sertifikaatin myöntäjä on tarkistanut ja todennut kyseiset tiedot oikeiksi. Sen jälkeen myöntäjä on laskenut tiedoista tiivisteen ja allekirjoittanut sen digitaalisesti. Kohde, jolle sertifikaatti esitetään, tarvitsee julkisen avaimen saadakseen tiivisteen puretuksi ja voidakseen verrata sitä itse laskemaansa. Jos tulokset ovat samanlaisia, voidaan sertifikaatin sisältämää tietoa pitää uskottavana. (Järvinen 2003, 159.)

Sertifikaatin sisältämiä tietoja voidaan pitää luotettavina, jos kaikki seuraavat edellytykset täyttyvät (Järvinen 2003, 160):

1. Sertifikaatin myöntäjään luotetaan ja voidaan olla varmoja, että myöntäjä on tarkistanut tietojen aitouden ennen todistuksen myöntämistä.

2. Sertifikaatin myöntäjän yksityisen avaimen tulee pysyä salassa. Yksityisen avaimen paljastuminen mahdollistaa sertifikaattien väärentämisen.

3. Sertifikaatin myöntäjän julkinen avain on saatu turvallista kanavaa pitkin, joten sitä voidaan pitää aitona.

4. Sertifikaatissa käytössä oleva salaustekniikka on riittävän vahva

Sertifikaatteja voidaan käyttää monessa yhteydessä. Niitä tarvitaan joka paikassa, missä halutaan olla varmoja toisen osapuolen identiteetistä tai tiedon oikeellisuudesta. (Järvinen 2003, 160.)

3.5 PKI-järjestelmä

PKI-järjestelmä (Public Key Infrastructure) on julkisen avaimen salaukseen, digitaaliseen allekirjoitukseen ja avainten hallintaan tarvittava järjestelmä. Digitaaliset allekirjoitukset mahdollistavat mm. luotettavan tunnistuksen ja tiedon eheyden. Julkisen avaimen sertifikaateilla taataan, että julkisen avaimen luovuttaja ei ole joku ulkopuolinen taho. Sillä pyritään estämään tilanteet, joissa osapuoli 1 yrittää saada osapuolen 2 julkista avainta haltuunsa, mutta saakin haltuunsa salakuuntelijan julkisen avaimen. (Kerttula 1998, 357.)

Sertifiointiin liittyy aina joku kolmas osapuoli. Tämä osapuoli on luotettu taho (CA, Certification Authority), joka voi olla joku julkinen viranomainen tai esimerkiksi yrityksen sisäinen varmennuselin. CA varmistaa sen, että kaksi toisilleen tuntematonta osapuolta voivat luottaa toisiinsa, koska ne molemmat luottavat yhteiseen kolmanteen osapuoleen. Julkisen avaimen sertifikaatissa tulee olla vähintään tunnistetiedot kohteesta, julkisen avaimen arvo, CA:n nimi ja CA:n digitaalinen allekirjoitus. (Kerttula 1998, 358.)

3.6 RADIUS

RADIUS-protokolla on alun perin suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen, jossa se on yhä edelleen laajassa käytössä. Nykyisin RADIUS:ta käytetään kaikkeen erilaiseen tietoverkkoihin liittyvään tunnistukseen. RADIUS on todennus- ja pääsynvalvontaprotokolla, ja sen toimintamalli perustuu keskitettyyn palvelu- ja käyttäjätietojen ylläpitoon. Jos lähiverkoissa halutaan käyttää AAA-palveluita (Authentication, Authorization and Accounting), on lähiverkolla oltava oma RADIUS-palvelin, johon esim. WLAN-tukiasemat ottavat RADIUS-protokollalla yhteyden. RADIUS-palvelin pitää sisällään tietokannan, jossa säilytetään käyttäjänimiä ja salasanoja. RADIUS-palvelin osaa myös käyttää olemassa olevia tietokantoja käyttäjätunnistukseen, muun muassa Windowsin Active Directorya. (Rigney, Willens, Rubens & Simpson 2000.)

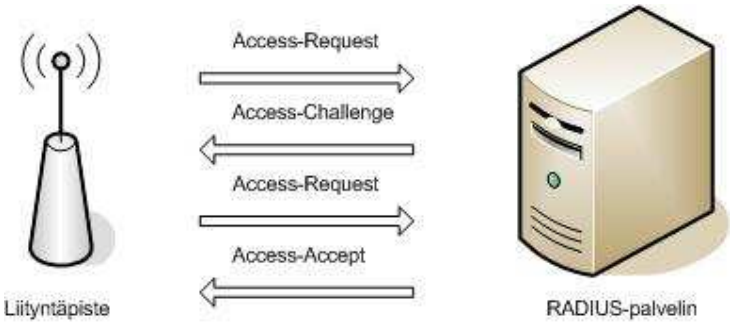
Kun käyttäjä yrittää kirjaantua RADIUS-autenkikointia vaativaan järjestelmään, liityntäpiste (esim. WLAN-tukiasema) lähettää RADIUS-palvelimelle Access Request -viestin, johon on määriteltynä käyttäjätunnus, salasana salattuna, päätelaitteen nimi sekä portti, johon käyttäjä on pyrkimässä. RADIUS-palvelimen saatua viestin se ensin varmistaa, että liityntäpisteen IP-osoite ja salasana on määriteltynä palvelimelle. Jos näin on, niin palvelin hyväksyy viestin ja alkaa käsitellä sitä. Ensimmäisenä RADIUS-palvelin kysyy tietokannasta käyttäjätunnusta vastaavat tiedot. Tietokanta käsittää ne vaatimukset, jotka käyttäjän pitää täyttää päästäkseen verkkoon. Vaatimuksina ovat aina salasana sekä mahdollisesti muita optionaalisia parametreja, kuten sallitut porttinumerot. (Rigney ym. 2000.)

Jos RADIUS-palvelimen vaatimat parametrit eivät täyty, se lähettää Access-Reject -viestin ja hylkää käyttäjän kirjaantumisyrityksen. Onnistuneessa tapauksessa se lähettää joko Access-Challenge-viestin, jolla palvelin pyytää haaste/vastaustyyppistä tunnistamista, tai hyväksyy yhteyden muodostamisen lähettämällä Access-Accept-viestin. (Rigney ym. 2000.)

Access-Challenge tapauksessa haaste on satunnaisluku, jolla käyttäjän pitää salata oma salasanansa ja lähettää se vastauksena RADIUS-palvelimelle. Tavallisesti tämä toimii niin, että kun käyttäjä kirjaantuessaan syöttää käyttäjätunnuksensa ja

salasanansa, niin ensimmäisessä Access-Request-viestissä lähetetään vain käyttäjätunnus. Haasteen saamisen jälkeen käyttäjän päätelaite laskee salasanasta saamallaan haasteella tiivisteen, jonka se liittää vastausviestiin. Liityntäpiste välittää viestin RADIUS-palvelimelle, joka laskee samalla haasteella tietokannassaan olevasta salasanasta tiivisteen ja vertaa niitä keskenään. Jos tiivisteet ovat samanlaisia, on käyttäjän autentikointi onnistunut ja RADIUS-palvelin lähettää Access-Accept-viestin. (Rigney ym. 2000; Keski-Kasari 2002.)

Kuviossa 4 on esitetty onnistuneen RADIUS-autentikoinnin kulku.



KUVIO 4. RADIUS-autentikointi

RADIUS-protokollaan oli alun perin määriteltynä ainoastaan käyttäjän autentikointiin liittyvät tunnistus ja valtuutus käytännöt. Myöhemmin siihen on lisätty myös tilastointipalvelu. Sen avulla voidaan seurata verkossa tapahtuvaa liikennöintiä, muun muassa siirretyn datan määrää. (Keski-Kasari 2002.)

3.7 Microsoft IAS

IAS on Microsoftin toteutus RADIUS-protokollasta. Se on yksi Windows Server 2003 tai 2000 käyttöjärjestelmien komponenteista. Microsoft IAS tarjoaa keskitetyn käyttäjän autentikoinnin, joka perustuu tietokantoihin. Tietokannat pitävät sisällään tiedot käyttäjätunnuksista ja salasanoista. Käyttäjätietokantana IAS voi käyttää esimerkiksi Windows Active Directorya. (Microsoft 2006a.)

IAS tukee useita autentikointiprotokollia, joista mainittakoon jo aikaisemmin esitellyt PPP- (Point-to-Point Protocol) ja EAP-protokollat. PPP-protokollista voi-

daan käyttää muun muassa PAP- (Password Authentication Protocol), CHAP- (Challenge Handshake Authentication Protocol) ja MSCHAPv2-protokollia (Microsoft Challenge-handshake authentication protocol). EAP-protokollia käytettäessä tuettuja menetelmiä ovat muuan muassa Smart Cardin käyttöön perustuva autentikointi sekä sertifikaatit. (Microsoft 2006a.)

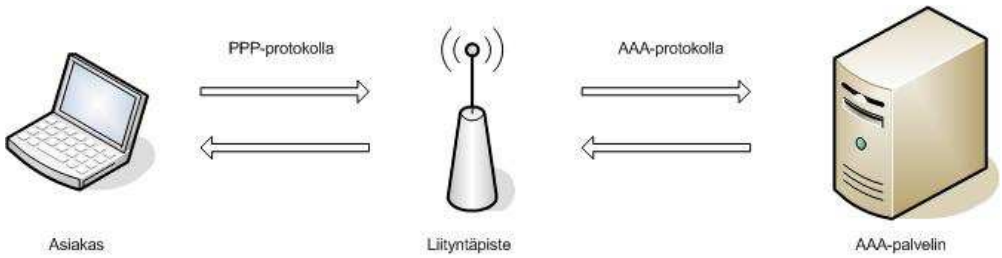
IAS voi toimia langattomissa verkoissa RADIUS-palvelimena, ja sitä voidaan käyttää sekä käyttäjien autentikoimiseen että langattomien tukiasemien todentamiseen (Microsoft 2006a).

4 AUTENTIKOINTIPROTOKOLLAT

4.1 AAA-protokolla

AAA on lyhenne sanoista Authentication, Authorization ja Accounting (autentikointi, valtuutus ja tilastointi). Näistä autentikointipalvelu mahdollistaa käyttäjien tunnistuksen, valtuutuspalvelun avulla käyttäjien saamia palveluja pystytään profiloimaan ja tilastointipalvelun avulla pystytään keräämään käyttäjistä tilastotietoja, kuten esimerkiksi yhteysaikoja. (Keski-Kasari 2002.)

AAA-protokollassa palvelu koostuu yleensä kolmesta eri komponentista: asiakkaasta, liityntäpisteestä ja AAA-palvelimesta. Asiakkaan ja liityntäpisteen välisessä yhteydessä käytetään yleensä alemman tason protokollaa, jolla on mahdollista toteuttaa autentikointipalvelu. Esimerkkinä tällaisesta on PPP-protokolla, joka pitää sisällään myös PAP-, CHAP- sekä myös siihen jälkeenpäin määritellyn EAP-protokollan. Liityntäpisteen ja AAA-palvelimen välisessä yhteydessä on käytössä jokin AAA-protokolla, joka huolehtii varsinaisesta käyttäjän tunnistuksesta. Esimerkkinä tällaisesta protokollasta on RADIUS. Kuviossa 5 on esitetty AAA-palvelun rakenne. (Keski-Kasari 2002.)



KUVIO 5. AAA-palvelun rakenne

4.2 PPP-protokolla

PPP-protokollaa käytetään verkon siirtoyhteyskerroksessa tietojen välittämiseen sarjaliikenteenä kahden pisteen välillä. Protokolla koostuu seuraavista pääkomponenteista: PPP-kapseloinnista, jonka avulla verkko-ohjelmistolla on mahdollisuus käyttää sarjaliikennettä useiden erilaisten protokollien kanssa, LCP-

protokollasta (Link Control Protocol), jota käytetään luomaan, katkaisemaan, muokkaamaan ja testaamaan yhteyttä sekä, NCP-protokollista (Network Control Protocol), joiden avulla PPP-yhteydet käyttävät erilaisia verkkokerroksen protokollia. (Simpson 2000.)

4.3 LCP- ja NCP-protokolla

Kun kahden pisteen välille on muodostunut fyysinen yhteys, aloittaa LPC-protokolla PPP-yhteyden muodostamisen. Yhteysparametrit neuvotellaan aina molempiin suuntiin erikseen ja toisistaan riippumatta. Tämän takia yhteys ei aina ole välttämättä symmetrinen kaikkien parametrien osalta. Yhteysparametreja ovat esimerkiksi suurin siirtokehyksen koko, yhteyden hallintatapa sekä käyttäjän tunnistusprotokolla. Vaihtoehtoina käyttäjän tunnistamiseen ovat PAP-, CHAP- ja EAP-protokollat. Autentikointiprotokollan käyttö ei ole pakollinen toimenpide yhteyden muodostamisessa. Yhteydenluontivaihe on suoritettu, kun molemmat osapuolet ovat lähettäneet ja vastaanottaneet kokoonpano hyväksytty paketin (Configure-Ack). Tämän jälkeen siirrytään joko optionaaliseen autentikointivaiheeseen tai verkkokerros vaiheeseen (NCP). Kun linkkitason yhteysparametrit on saatu määriteltyä ja optionaalinen autentikointi suoritettu loppuun, on verkkotason hallintoprotokollan tehtävänä muodostaa yhteys loppuun. NCP-protokollien tehtävänä on sopia verkkokerroksella käytettävistä protokollista (esimerkiksi IP-protokolla). Kun yhteys halutaan lopettaa, käytetään siihen jälleen LCP-protokollaa. (Vesanen 2006.)

4.4 PAP- ja CHAP-autentikointiprotokollat

Alkuperäisen PPP-määrittelyn mukaisia autentikointiprotokollia on kaksi: PAP ja CHAP. PAP-protokolla on vanhin autentikoinnissa käytettävä protokolla. Tämän protokollan mukaan tehty autentikointi ei ole kovinkaan tietoturvallinen, sillä tunnistautumistiedot lähetetään selkokielisenä siirtotielle. PAP-protokollassa on kolme viestityyppiä. Nämä ovat Authentication-Request, Authentication-Ack ja Authentication-Nak. Authentication-Request viestissä asiakas lähettää sekä käyttäjätunnuksen että salasanan. Jos ne ovat samoja kuin vastapäähän on määritelty, on autentikointi onnistunut ja vastaanottaja lähettää Authentication-Ack-viestin asi-

akkaalle. Muussa tapauksessa lähetetään Authentication-Nak-viesti. Käyttäjätunnusta ja salasanaa lähetetään niin kauan, kunnes saadaan hyväksyminen tai yhteys katkaistaan. (Vesanen 2006.)

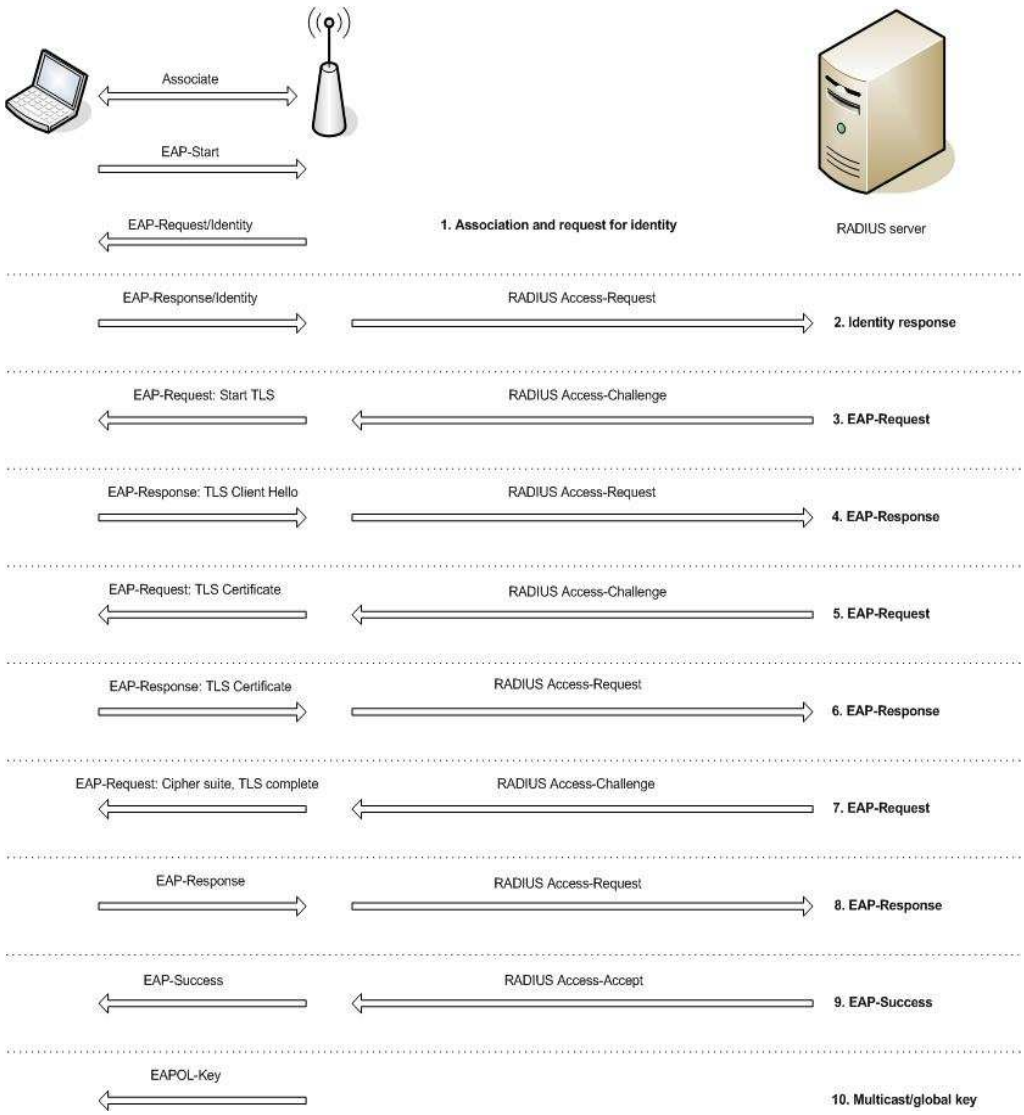
CHAP-protokollassa on erilaisia viestityyppejä neljä. Ne ovat Challenge, Response, Success ja Failure. Autentikoinnissa tunnistusta vaativa osapuoli lähettää ensimmäisenä Challenge-viestin, jossa pyydetään asiakkaalta käyttäjätunnusta ja salasanaa, sekä antaa lisäksi haasteen. Asiakas salaa salasanan saadulla haasteella. Tähän käytetään yleensä MD5-algoritmia (Message Digest 5). Tämän jälkeen asiakas lähettää Response-viestin, joka pitää sisällään sekä käyttäjätunnuksen että salasanasta lasketun tarkistussumman. Jos tarkistussumma täsmää tunnistusta pyytäneellä laitteella, on autentikointi onnistunut ja se lähettää asiakkaalle Success-viestin. Muussa tapauksessa lähetetään Failure-viesti, joka pitää sisällään myös syyn autentikoinnin epäonnistumisesta. (Keski-Kasari 2002.)

4.5 EAP-protokollat

EAP-protokolla on määritelty alun perin laajennukseksi PPP-protokollaan. Koska se oli niin hyvä, sovitti IEEE sen toimimaan myös 802.1x-protokollan kanssa. EAP-protokollaa käytetään yleensä jonkun AAA-protokollan (esim. RADIUS) kanssa, jolloin saadaan todentamis-, valtuutus- ja tilastointipalvelut käyttöön. Mahdollisia EAP-autentikointimenetelmiä ovat mm. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), PEAP (MSCHAPv2), EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security), EAP-MD5 (Extensible Authentication Protocol-Message Digest 5), EAP-SIM (Extensible Authentication Protocol - Subscriber Identity Module) ja LEAP (Lightweight Extensible Authentication Protocol). Niistä esitellään tämän työn kannalta tärkeimmät EAP-TLS ja PEAP. (Keski-Kasari 2002.)

4.5.1 EAP-TLS

EAP-TLS-autentikointiprotokolla mahdollistaa kaksisuuntaisen tunnistuksen, jossa sekä päätelaite että verkko autentikoivat toisensa. Autentikointi tapahtuu sertikaattien avulla, jotka vaihdetaan päätelaitteen ja autentikointipalvelimen kesken neuvotteluvaiheessa. Kuviossa 6 on esitetty EAP-TLS-autentikoinnin kulku.



KUVIO 6. EAP-TLS autentikoinnin kulku (Microsoft 2006b)

Autentikointitapahtuman kulku on seuraava (Microsoft 2006b):

1. Jos langaton tukiasema havaitsee langattoman laitteen, joka pyrkii verkkoon, se lähettää sille EAP-Request/Identity-viestin. Jos taas

päätelaite aloittaa autentikointiprosessin, se lähettää EAP-Start-viestin, johon tukiasema vastaa EAP-Request/Identity-viestillä.

2. Jos verkkoon pyrkivään päätelaitteeseen ei ole kukaan kirjaantunut, lähetettävä EAP-Response/Identity-viesti pitää sisällään tiedon päätelaitteen nimestä. Jos taas käyttäjä on kirjaantuneena, pitää EAP-Request/Identity-viesti sisällään käyttäjätunnuksen. Tämän jälkeen tukiasema välittää saamansa EAP-Response/Identity-viestin edelleen RADIUS-palvelimelle.

3. RADIUS-palvelin lähettää tukiaseman kautta päätelaitteelle EAP-Request: Start TLS-viestin, jolla se pyytää päätelaitetta aloittamaan TLS-autentikointiprosessin.

4. Päätelaite lähettää EAP-Response: TLS client hello-viestin, jonka tukiasema edelleen välittää RADIUS-palvelimelle.

5. RADIUS-palvelin lähettää EAP-Request-viestin, joka pitää sisällään palvelimen sertifikaatin. Tukiasema välittää viestin päätelaitteelle.

6. Päätelaite vastaa saamaansa EAP-Request-viestiin lähettämällä oman sertifikaattinsa EAP-Response-viestillä. Tukiasema välittää viestin RADIUS-palvelimelle.

7. RADIUS-palvelin lähettää EAP-Request-viestin, jossa on tieto käytettävästä salauksesta, sekä ilmoittaa, että TLS-autentikointi on saatu päätökseen. Tukiasema välittää viestin päätelaitteelle.

8. Päätelaite vastaa EAP-Response-viestillä ja kuittaa autentikoinnin päättyneeksi. Tukiasema välittää viestin edelleen RADIUS-palvelimelle.

9. RADIUS-palvelin laskee istuntokohtaiset lähetys- ja vastaanottoavaimet TLS-autentikoinnissa käytettyjen MPPE-avaimien (Micro-

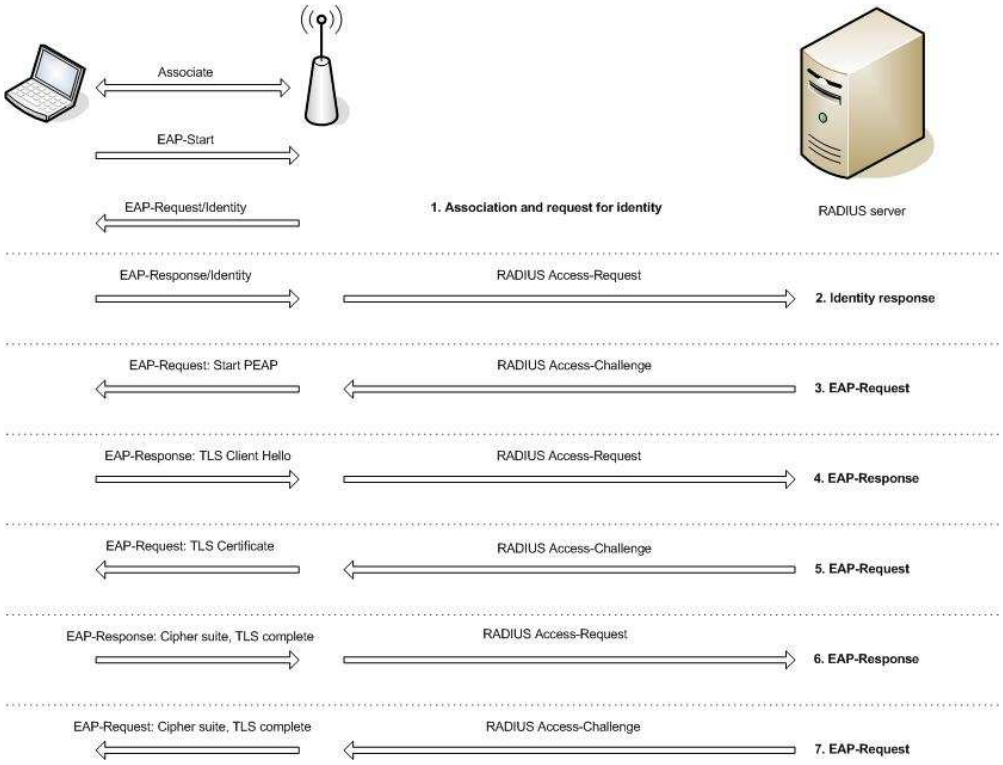
soft Point-to-Point Encryption) perusteella ja lähettää ne edelleen tukiasemalle. Tukiasema muokkaa saatuja avaimia niin, että ne mahtuvat käytettyyn WEP-avainpituuteen. Näitä avaimia tukiasema käyttää keskustellessaan päätelaitteen kanssa. Päätelaite laskee edelleen istuntokohtaiset lähetys- ja vastaanottoavaimet TLS-autentikoinnin perusteella ja ottaa ne käyttöön. Tämän jälkeen sekä päätelaitteella että tukiasemalla on salausavaimet hallussaan ja liikenne on tästä eteenpäin salattua. Tässä vaiheessa tukiasema myös välittää päätelaitteelle RADIUS-palvelimelta saamansa EAP-Success-viestin, jolla se ilmoittaa avaimien käyttöönotosta.

10. Viimeisessä vaiheessa tukiasema laskee multicast-avaimen (multicast (ryhmälähetys) on menetelmä, jolla sama sisältö voidaan jakaa useille vastaanottajille (päätelaitteille) IP-verkossa), jonka se lähettää päätelaitteelle äsken saaduilla avaimilla salattuna.

EAP-TLS on tietoturvaltaan vahva autentikointimenetelmä. Sen ongelmana on kuitenkin se, että tiedot asiakkaasta lähetetään RADIUS-palvelimelle salaamattomana. Liikenteestä tulee salattua vasta sertifikaattien vaihtamisen ja lähetys- ja vastaanottoavaimien luomisen jälkeen.

4.5.2 PEAP (MSCHAPv2)

PEAP (Protected Extensible Authentication Protocol) on Microsoftin, RSA Securityn ja Ciscon kehittelemä, salasanoihin perustuva, haaste-vastaus autentikointimenettely. Autentikointi tapahtuu kahdessa vaiheessa, joista ensimmäisessä luodaan salattu PEAP-TLS-kanava päätelaitteen ja palvelimen välille. Ensimmäisen vaiheen aikana palvelin todentaa itsensä päätelaitteelle. Toisessa vaiheessa suoritetaan varsinainen päätelaitteen autentikointi. Kuviossa 7 on esitelty ensimmäisen vaiheen mukainen PEAP-TLS-kanavan luonti. (Microsoft 2006b.)



KUVIO 7. PEAP-TLS-kanavan luonti (Microsoft 2006b)

Salatun kanavan luonnin kulku on seuraava (Microsoft 2006b):

1. Jos langaton tukiasema havaitsee langattoman laitteen, joka pyrkii verkkoon, se lähettää sille EAP-Request/Identity-viestin. Jos taas päätelaite aloittaa autentikointiprosessin, se lähettää EAP-Start-viestin, johon tukiasema vastaa EAP-Request/Identity-viestillä.

2. Päätelaite vastaa lähettämällä EAP-Response/Identity-viestin, joka pitää sisällään päätelaitteen nimen tai käyttäjätunnuksen. Tämän jälkeen tukiasema välittää saamansa EAP-Response/Identity-viestin edelleen RADIUS-palvelimelle.

3. RADIUS-palvelin lähettää tukiaseman kautta päätelaitteelle EAP-Request: Start PEAP -viestin, jolla se pyytää päätelaitetta aloittamaan PEAP-autentikointiprosessin.

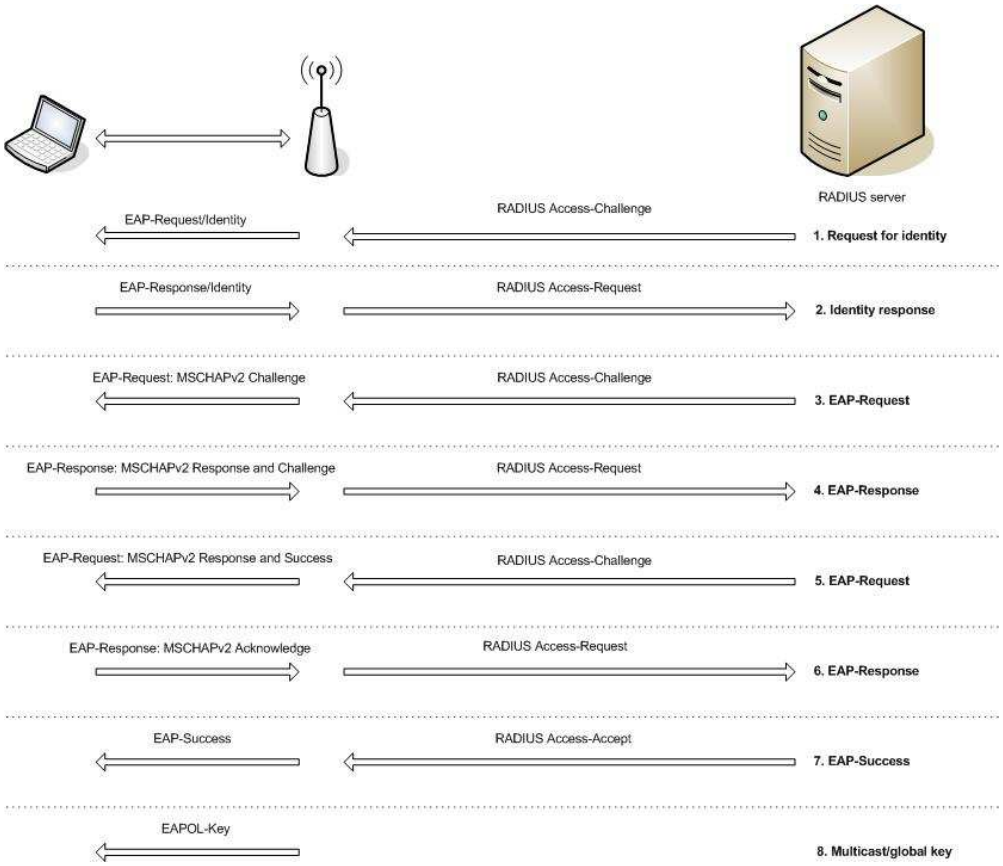
4. Päätelaite lähettää EAP-Response: TLS client hello -viestin, jonka tukiasema edelleen välittää RADIUS-palvelimelle.

5. RADIUS-palvelin lähettää EAP-Request-viestin, joka pitää sisällään palvelimen sertifikaatin. Tukiasema välittää viestin päätelaitteelle.

6. Päätelaite vastaa saamaansa EAP-Request-viestiin, jossa on tieto käytettävästä salauksesta, sekä ilmoittaa, että TLS-autentikointi on saatu päätökseen. Tukiasema välittää viestin RADIUS-palvelimelle.

7. RADIUS-palvelin kuittaa edellisen viestin ilmoittamalla myös tiedon käytettävästä salauksesta ja TLS-autentikoinnin päättymisestä. Tukiasema välittää viestin päätelaitteelle.

Tämän vaiheen tuloksena on saatu luotua salattu kanava päätelaitteen ja RADIUS-palvelimen välille. Samalla RADIUS-palvelin on todentanut itsensä päätelaitteelle lähettämälle sille oman sertifikaattinsa. Seuraavaksi tapahtuu varsinainen autentikointiprosessi MSCHAPv2-protokollan mukaisesti. Siinä päätelaite autentikoidaan verkkoon. Autentikointiprosessin kulku on esitelty kuviossa 8.



KUVIO 8. MSCHAPv2-autentikointiprosessi (Microsoft 2006b)

MSCHAPv2-autentikointiprosessin kulku on seuraava (Microsoft 2006b):

1. RADIUS-palvelin lähettää EAP-request/Identity-viestin päätelaitteelle, jonka tukiasema välittää perille.

2. Päätelaite vastaa lähettämällä EAP-Response/Identity-viestin, joka pitää sisällään päätelaitteen nimen tai käyttäjätunnuksen. Tukiasema välittää viestin edelleen RADIUS-palvelimelle.

3. RADIUS-palvelin lähettää MSCHAPv2-haasteen päätelaitteelle. Tukiasema välittää haasteen.

4. Päätelaite vastaa saamaansa haasteeseen lähettämällä oman MSCHAPv2-haasteensa RADIUS-palvelimelle. Tukiasema välittää viestin.

5. RADIUS-palvelin vastaa haasteeseen ja lähettää viestin, jossa se ilmoittaa päätelaitteelle onnistuneesta autentikoinnista. Tukiasema välittää viestin.

6. Päätelaite vastaa RADIUS-palvelimelle ja kuittaa tiedon onnistuneesta autentikoinnista. Tukiasema välittää viestin perille.

7. RADIUS-palvelin laskee istuntokohtaiset lähetys- ja vastaanottoavaimet PEAP-autentikoinnissa käytettyjen avaimien perusteella ja lähettää ne edelleen tukiasemalle. Tukiasema muokkaa saatuja avaimia niin, että ne mahtuvat käytettyyn WEP-avainpituuteen. Näitä avaimia tukiasema käyttää keskustellessaan päätelaitteen kanssa. Päätelaite laskee edelleen istuntokohtaiset lähetys- ja vastaanottoavaimet PEAP-autentikoinnin perusteella ja ottaa ne käyttöön. Tämän jälkeen sekä päätelaitteella, että tukiasemalla on salausavaimet hallussaan. Tässä vaiheessa tukiasema myös välittää päätelaitteelle RADIUS-palvelimelta saamansa EAP-Success-viestin, jolla se ilmoittaa avaimien käyttöönotosta.

8. Viimeisessä vaiheessa tukiasema laskee multicast-avaimen, jonka se lähettää päätelaitteelle äsken saaduilla avaimilla salattuna.

Nyt päätelaite on suorittanut onnistuneen kaksisuuntaisen autentikoinnin RADIUS-palvelimen kanssa ja sen oikeudet käyttää verkkoa on todennettu.

5 ACTIVE DIRECTORY

5.1 Yleistä

Windows Server 2003:n ja vanhemman Windows Server 2000:n hakemistopalvelut pohjautuvat Active Directoryyn. Active Directory on Microsoftin toteutus hakemistopalveluista. Määrityksen mukaan hakemistopalvelu eroaa hakemistosta siten, että sisältämällä hakemiston tiedot eli tietokannan se myös tarjoaa palvelut, joilla tietokantaan päästään käsiksi. Active Directoryn tehtävänä on vähentää ylläpidettävien hakemistojen määrää, sillä esimerkiksi käyttäjätilien, tietokonetilien ja jaettujen resurssien hallinta voidaan tehdä yhtenäisillä rajapinnoilla ja työkaluilla. Hakemistopalvelu tarjoaa keskitetyn paikan, jossa on tiedot verkon laitteista, verkon palveluista sekä käyttäjistä. Active Directory ei yleensä näy käyttäjälle asti mitenkään. Se mahdollistaa kuitenkin loppukäyttäjille erilaisia resurssien etsimistä ja käyttöä helpottavia toimintoja. (Kivimäki 2005, 1.)

5.2 Active Directory ja DNS

Active Directory käyttää DNS-järjestelmää (Domain Name System). DNS on standardi Internetin palvelu, joka järjestelee tietyn joukon tietokoneita toimialueiksi. DNS on erittäin oleellinen osa Windows Active Directory -tekniikkaa. Ennen kuin Active Directory voidaan asentaa, pitää verkkoon olla tehtynä DNS-määritykset. Active Directoryn käyttämä DNS-rakenne on hierarkkinen. Eri hierarkiatasoilla tunnistetaan tietokoneet, toimialueet ja ylätason toimialueet. DNS:n kautta Active Directoryn toimialuehierarkia voidaan määritellä Internetin laajuiseksi tai erilliseksi ja yksityiseksi. DNS:ää voidaan käyttää myös isäntäkoneiden nimien muuttamiseen. Esimerkiksi firma.com voidaan muuntaa IP-osoitteeksi 10.10.10.10. (Stanek 2003, 133.)

Kun Active Directory -tyyppisessä toimialueessa viitataan johonkin tiettyyn tietokoneresurssiin, on käytettävä täyttä tietokoneen nimeä, esim. Computer.Firma.com. Tässä Computer on yksittäisen tietokoneen nimi, Firma tarkoittaa organisatorista toimialuetta ja com on ylätason toimialue. Ylätason toimialueet ovat DNS-hierarkian juuressa, ja siksi niitä kutsutaan juuritoimialueiksi. Nämä

toimialueet on luokiteltu maantieteellisesti kaksikirjaimisten maakoodien mukaan (esim. Suomen maakoodi on fi), organisaatiotyypin mukaan (esim. com on tarkoitettu kaupallisia organisaatioita varten) tai toiminnon mukaan (esim. gov on tarkoitettu Yhdysvaltojen valtiovallan käyttöön). (Stanek 2003, 133–134.)

5.3 Active Directoryn käsitteet ja ominaisuudet

Seuraavaksi on esitelty tärkeimmät ja keskeisimmät Active Directoryyn liittyvät käsitteet ja ominaisuudet.

- Toimialueeseen (domain) pitää olla määriteltynä käyttäjä- ja tietokonetilit ja käyttäjät kirjaantuvat toimialueelle. Toimialueella on oma nimi, ja Active Directoryn tapauksessa nimi noudattaa DNS:n standardia nimeämismenetelmää (esim. firma.com). (Kivimäki 2005, 6.)

- Luottosuhteet (trust relationship) yhdistävät toimialueita. Puurakenne (domain tree) tarkoittaa hierarkkista toimialuerakennetta, jossa ylemmän tason toimialueen (parent) ja alemman tason toimialueen (child) välillä on luottosuhde. Koska Active Directory noudattaa DNS:n nimeämismallia, ylemmän tason toimialueen nimen ollessa firma.com alemman tason toimialue voisi tällöin olla nimeltään lahti.firma.com. Active Directory -toimialueilla luottosuhteet muodostetaan automaattisesti toimialuepuun sisällä ja välille. (Kivimäki 2005, 6.)

- Useamman toimialuepuun muodostama ryhmä on nimeltään toimialuepuuryhmä eli metsä (forest). Kaikilla samaan toimialuepuuryhmään kuuluvilla toimialueilla on yhteinen Active Directoryn rakenne. (Kivimäki 2005, 6.)

- Ohjauspalvelimet (domain controllers) ylläpitävät Active Directoryn hakemistoa eli tietokantaa. Ohjauspalvelimia on yleensä useita sa-

massa toimialueessa. Mikä tahansa niistä voi käsitellä esimerkiksi käyttäjätilin poistamisen toimialueelta. Tällöin tehty muutos replikoidaan toisille ohjauspalvelimille. (Kivimäki 2005, 6.)

- Monet Active Directoryn asiat määritellään objekteina. Ne ovat toimialueella sijaitsevia kohteita, esimerkiksi käyttäjätilejä, jaettuja kansioita. organisaatioyksiköitä jne. Objekteilla on erilaisia attribuutteja, jotka määrittelevät niille erilaisia ominaisuuksia. Esimerkiksi objektin käyttöoikeusluettelolla voidaan määritellä pääsyoikeudet johonkin tiettyyn kansioon. Käyttöoikeudet voivat myös periytyä emo-objektista. Esimerkiksi jollekin käyttäjäryhmälle oikeuksia annettaessa ne periytyvät kaikille ryhmään kuuluville objekteille. (Kivimäki 2005, 6–7.)

- Organisaatioyksiköt ovat toimialueella sijaitsevia säilöjä konetilien, käyttäjätilien ja -ryhmien tallennukseen. Organisaatioyksikköön voidaan määritellä ryhmäkäytäntö (group policy), jonka avulla voidaan hallita esimerkiksi työasemien käyttöliittymiä, asentaa ohjelmistoja ja hallita esim. sisään- ja uloskirjaantuessa ajettavia scriptejä. (Kivimäki 2005, 7.)

- Jakeluryhmät ja suojausryhmät (distribution groups, security groups) ovat käyttäjäryhmien tyyppejä. Kumpikin voi toimia jakeluluettelona, mutta ainoastaan suojausryhmille on mahdollista määritellä käyttöoikeuksia esimerkiksi jaettuun kansioon. (Kivimäki 2005, 7.)

- Toimipaikat (sites) ovat IP-aliverkkojen muodostamia kokonaisuuksia. Määritelmän mukaan toimipaikan tietokoneet ovat lähiverkkotason nopeudella yhteydessä toisiinsa. Tämän avulla voidaan määritellä käyttäjiä läheltä löytyvät palvelut sekä replikointi eri toimipaikkojen välillä. Myös toimipaikkoihin voidaan kohdistaa ryhmäkäytäntöjä. (Kivimäki 2005, 7.)

6 LANGATTOMAN LÄHIVERKON SUUNNITTELU

6.1 Yleistä

WLAN-verkon suunnittelu alkaa vaatimusten määrittelyllä, jonka tarkoituksena on saada aikaan alustava verkkosuunnitelma. Sovelluksien, päätelaitteiden, palveluiden, käyttäjien ja käyttötapojen perusteella voidaan muotoilla langattoman verkon tekniset vaatimukset. Verkkosuunnitelman teknisistä tiedoista tulee ilmetä vaatimukset peittoalueesta, käyttäjämääristä, päätelaitteista, verkon suorituskyvystä, sovelluksista ja niiden palveluvaatimuksista, liikenteen kohteista sekä tietoturvapolitiikasta. Suunnitelmasta tulisi ilmetä myös mahdollisesti jo olemassa olevan verkon kuvaus, langattoman verkon fyysinen ja looginen kuvaus, mukaan luettuna tukiasemien määrä, niiden alustavat sijoituspaikat, antennityypit ja käytettävät kanavat. Hankkeelle tulee myös laatia kustannusarvio sekä aikataulu, jonka mukaan prosessi etenee. Edellisten seikkojen tarkoituksena on saada aikaan suunnitelma, jonka pohjalta voidaan tehdä käyttökelpoinen, joustava ja kustannustehokas verkkoratkaisu. (Puska 2005, 219.)

6.2 Katselmus

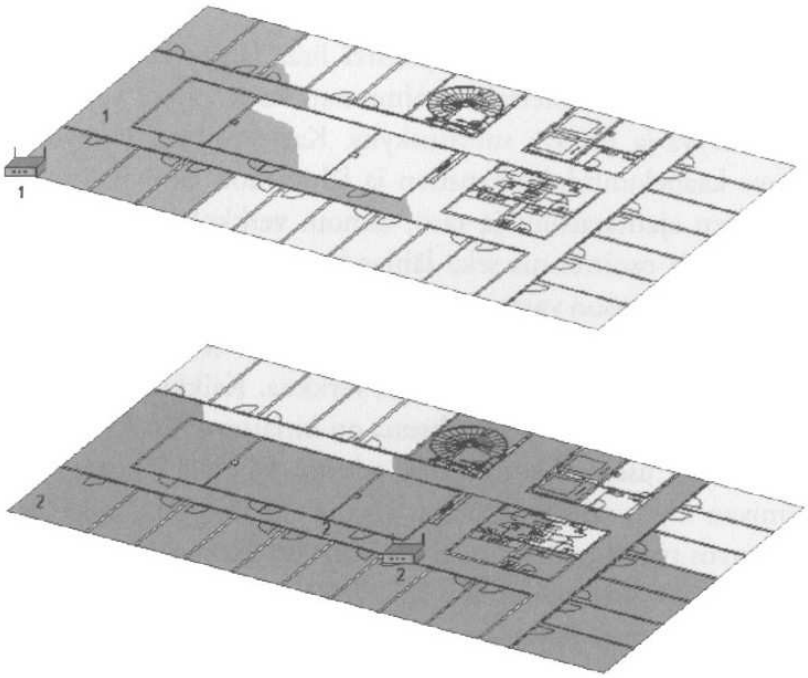
Radioaaltojen etenemisen vaikean mallintamisen vuoksi on ennen asennusta tehtävä katselmus. Katselmuksen tarkoituksena on varmistaa langattoman verkon toiminta haluttujen vaatimusten mukaisesti ja se kattaa seuraavat aiheet: (Puska 2005, 220.)

- langattoman verkon peittoalueen varmistaminen halutulla bittinopeudella
- antennityyppien, sijoituspaikkojen, suuntauksen ja kiinnityksen määrittäminen
- mahdollisten häiriölähteiden kartoittaminen ja korjaavien toimenpiteiden selvittäminen

- langattomien laitteiden asennusten yksityiskohtien määrittely

- mahdollisesti jo olemassa olevan lähiverkon WLAN-valmiuden ja tukiasemien sähkönsyötön varmistaminen

WLAN-verkkosovittimet sisältävät yleensä katselmusohjelman, jolla voidaan mitata kentänvoimakkuus, häiriötasot ja monitie-eteneminen. Peittoalueen mittaus aloitetaan niin, että sijoitetaan tukiasema väliaikaisesti esim. kerroksen kulmahuoneeseen ja liikutaan WLAN-päätelaitteen kanssa, kunnes löydetään peittoalueen reuna. Tällöin bittinopeus on pudonnut alle halutun minimin. Seuraavassa vaiheessa tukiasema viedään äsken löydettyyn peittoalueen reunaan ja kartoitetaan kyseisen yhteyspisteen peittoalue. Peittoalueen pitäisi nyt kattaa myös alkuperäinen sijoituspaikka eli kulmahuoneen nurkka. Koe toistetaan kerroksen toisesta nurkasta vastaavalla tavalla. Lopuksi mitataan mahdolliset väliin jäävät alueet, porraskäytävät, aulat ja muut erityiskohteet samalla huomioiden noin 15 %:n solujen päällekkäisyys. Yksityiskohdat tulisi dokumentoida ja samalla merkitä ylös mahdolliset puutteet. Kuviossa 9 on esitetty tukiasemien sijoituspaikkojen määrittelyn periaate. (Puska 2005, 220–221.)



KUVIO 9. Tukiasemien sijoituspaikkojen määrittely (Puska 2005, 223)

Tukiasemien sijoituspaikkojen ja lukumäärän selvityksen pitää suunnitella niiden kiinnitys ja sähkönsyöttö. Yleensä tukiasemat sijoitetaan niin, että niihin eivät normaalit käyttäjät pääse käsiksi. Tällä haetaan laitteille suojaa mm. ilkivaltaa vastaan. Sähkönsyöttö voidaan hoitaa normaalisti pistorasiasta, mutta sen jakelu on myös mahdollista hoitaa verkkokaapeloinnin kautta Power-over-Ethernet ratkaisulla. (Puska 2005, 220–221.)

6.3 Asennus ja käyttöönotto

WLAN-laitteiden asennus tehdään suunnittelu- ja katselmusdokumenttien pohjalta. Antennien sijoitukseen, kiinnitykseen ja suuntaukseen kannattaa kiinnittää erityistä huomiota, koska niillä on suuri merkitys verkon toimivuuden ja kattavuuden kannalta. Kun kaikki verkon laitteet on saatu kiinnitetyksi, tulee vielä ennen käyttöönottoa testata, että koko verkko toimii suunnitellulla tavalla. (Puska 2005, 226.)

7 KÄYTÄNNÖN TOTEUTUS

7.1 Lähtökohdat

Työn tavoitteena oli päivittää jo olemassa oleva langaton lähiverkko, joka pohjautui 802.11b-standardin mukaisiin laitteisiin, nykyaikaiselle tasolle. Vanhaa langatonta verkkoa pidettiin tietoturvaltaan riittämättömänä ja sen parantaminen olikin pääsyy päivitykselle. Aikaisemmin käytössä ollut WEP-salaus korvattiin 802.1x-määritelmän mukaiseksi, tietoturvaltaan riittävän vahvaksi järjestelmäksi. Uuden verkon tuli olla myös suorituskyvyltään edeltäjäänsä parempi. Uusien tukiasemien myötä verkon nopeus kasvoi 11 Mbps:sta 54 Mbps:iin. Käytännössä tuohon teoreettiseen maksiminopeuteen ei kuitenkaan päästy. Verkon käytännön nopeutta hidastaa entisestään se, että verkossa on samaan aikaan käytössä sekä 802.11b- ja 802.11g-standardin mukaisia laitteita.

7.2 Laiteympäristö

Jotta 802.11x-määritelmän mukainen ympäristö on mahdollista toteuttaa, tulee verkon kaikkien laitteiden tukea kyseistä standardia. Tämä pätee sekä tukiasemiin että päätelaitteiden langattomiin verkkokortteihin.

Valitun tukiaseman tuli täyttää seuraavat vaatimukset:

- hyvä lämmönkesto mm. tehdasympäristöä silmälläpitäen
- virransyöttöominaisuudet – mahdollisuus käyttää sekä normaalia verkkovirtaa, että POE-ratkaisua (Power Over Ethernet)
- mahdollisuus käyttää ulkoisia antenneja
- tuki VLAN:lle (Virtual LAN)

Tukiaseman päivitettävyyttä pidettiin myös tärkeänä seikkana. Tulevaisuudessa ilmestyvillä päivityksillä on mahdollista parantaa tukiasemien tietoturva- ja muita ominaisuuksia. Tämän vuoksi ajateltiin, että ns. suuret valmistajat ovat ainoita vaihtoehtoja.

Tukiaseman valinnassa päädyttiin Cisco Aironet 1230AG -malliin. Se täyttää kaikki edellä luetellut vaatimukset sekä monia muita mahdollisesti tulevaisuudessa tarpeellisia ominaisuuksia. Kyseinen tukiasema on suunniteltu vaativiin ympäristöihin, kuten esimerkiksi tehdasalueille. Sen kuoret ovat kokonaan metallia, ja sen lämmönkestävyys on erittäin hyvä. Laitekannan yhtenäisyyden vuoksi samaa tukiasemaa käytetään myös konttoritiloissa. Kuviossa 10 on Cisco Aironet 1230AG tukiasema.

KUVIO 10. Cisco Aironet 1230AG -tukiasema (Cisco Aironet 1230 AG Series. 2006)

Päätelaitteiden verkkokortteina voidaan käyttää useampia eri vaihtoehtoja. Yrityksen käytössä olevissa IBM:n valmistamissa kannettavissa tietokoneissa on likimain kaikissa integroituna langaton verkkokortti. Käyttöjärjestelmänä koneissa on Windows XP.

Kannettavan mallista riippuen on verkkokorttivaihtoehtoja kolme. Yksi on IBM:n valmistama IBM Mini-PCI WLAN -kortti ja toinen on Intelin valmistama Intel 2100 PRO Wireless -kortti. Kolmantena vaihtoehtona on Cisco 350 Mini-PCI -kortti. Näistä vaihtoehdoista sekä Intelin että Ciscon valmistamat kortit tukevat

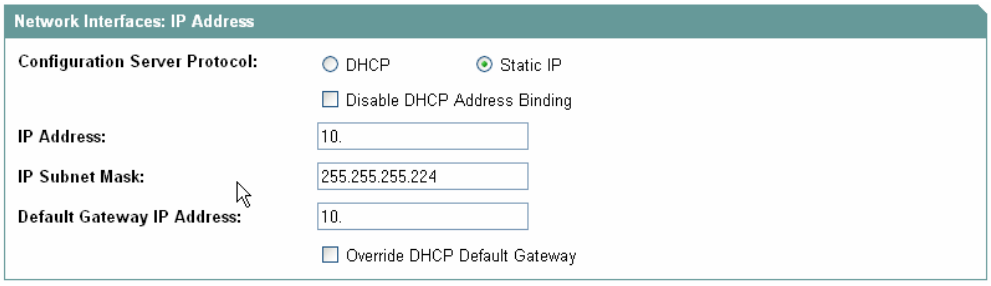
ainoastaan 802.11b-standardia. IBM:n kortit sen sijaan tukevat sekä 802.11b- ja 802.11g-standardeja. Niissä päätelaitteissa, joissa integroitua langatonta korttia ei ole, on mahdollisuus käyttää PCMCIA-väylään liitettävää ulkoista korttia. Tähän tarkoitukseen valittiin Ciscon CB21AG -kortti. Se tukee myös 802.11g-standardia.

Suurin osa verkon päätelaitteista on sellaisia, joissa on tuki vain 802.11b-standardille. Lisäksi kaikki vanhempien kannettavien (ennen vuotta 2004 käyttöönotetut) verkkokortit olivat sellaisia, että ne eivät suoraan tukeneet 802.1x-standardia. Kannettavat, jotka eivät suoraan tukeneet 802.1x-standardia, piti päivittää. Tämä piti sisällään kannettavan tietokoneen BIOS:n päivityksen, langattoman kortin Firmwaren päivityksen ja käyttöjärjestelmän langattoman verkkokortin ajurin päivityksen. Tämä operaatio piti suorittaa manuaalisesti jokaiselle päätelaitteelle erikseen. Jokaiselle kannettavan mallille ja eri verkkokorttityypeille edellä mainitut päivitysohjelmistot olivat erilaisia. Päivityksen jälkeen saatiin vanhemmillekin laitteille tuki 802.1x, standardille. Uusimmille kannettaville ja niille päätelaitteille, joissa oli PCMCIA-väyläinen verkkokortti, ei päivitystä tarvinnut tehdä.

7.3 Tukiasemien konfigurointi

Tukiasemien konfiguroinnissa piti ottaa huomioon se, että verkossa on laitteita, jotka eivät tue uusia autentikoitumismenetelmiä lainkaan. Tästä syystä tukiasemiin piti konfiguroida kaksi langatonta verkkoa, joista toinen oli samanlainen kuin aikaisemmin käytössä ollut. Päätelaitteistokantaa uusitaan koko ajan, ja ajan mittaan tarve vanhan mallin mukaiseen langattomaan verkkoon katoaa. Toinen huomioitava seikka oli se, että verkossa on laitteita, jotka tukevat vain 802.11b-standardia. Tästä syystä piti tukiasemiin jättää tuki myös niille laitteille.

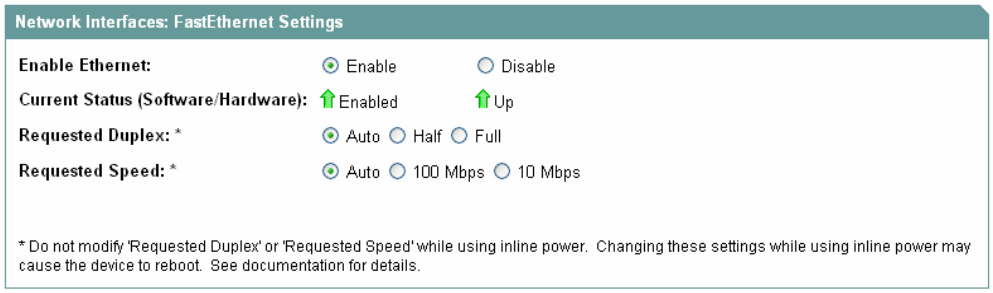
Ensin määriteltiin tukiasemien liitäntöjen asetukset. Kaikille tukiasemille määriteltiin ensin IP-osoitteet. Kuviossa 11 on esitetty tukiasemien IP-osoitteiden asetukset.



KUVIO 11. Tukiasemien IP-osoitteiden määritys

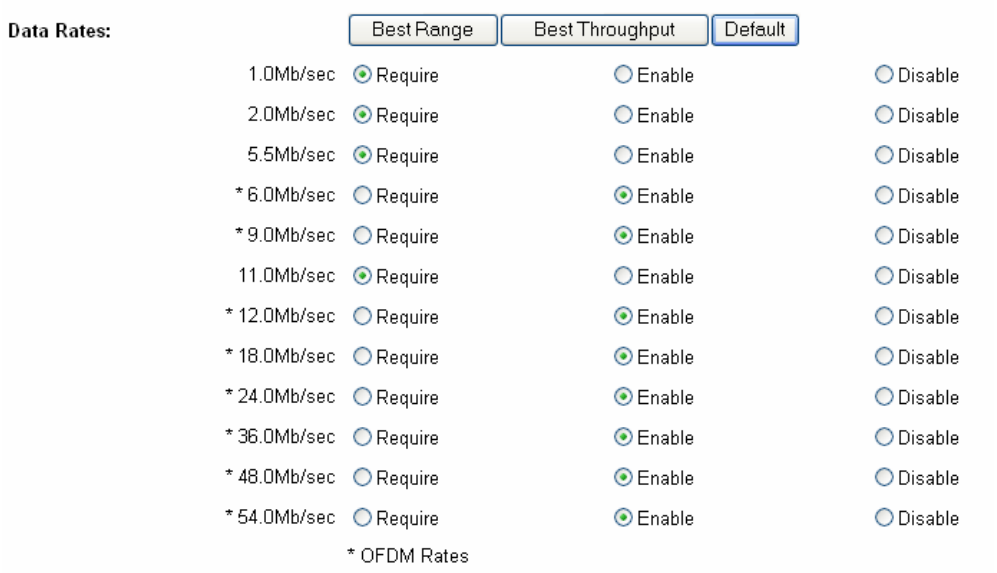
Kuten kuviosta 11 ilmenee, määriteltiin kaikille tukiasemille kiinteät IP-osoitteet. Langattomat tukiasemat ovat kokonaan omassa VLAN:ssa, jossa ei ole muita laitteita.

Kuviossa 12 on tukiasemien ethernet-liitännän asetukset. Ne jätettiin oletusasetuksille.



KUVIO 12. Ethernet-liitännän asetukset

Kuviossa 13 on esitetty radioliitännän tuettujen nopeuksien asetukset. Nekin jätettiin Ciscon oletusasetuksille.



KUVIO 13. Tuetut nopeudet

Nopeusasetusten lisäksi radioliitännälle määriteltiin sallitut kanavat, lähetystehot, antennien asetukset yms. Ne kaikki jätettiin Ciscon tarjoamille oletusasetuksille, joten en niitä tässä tarkemmin esittele.

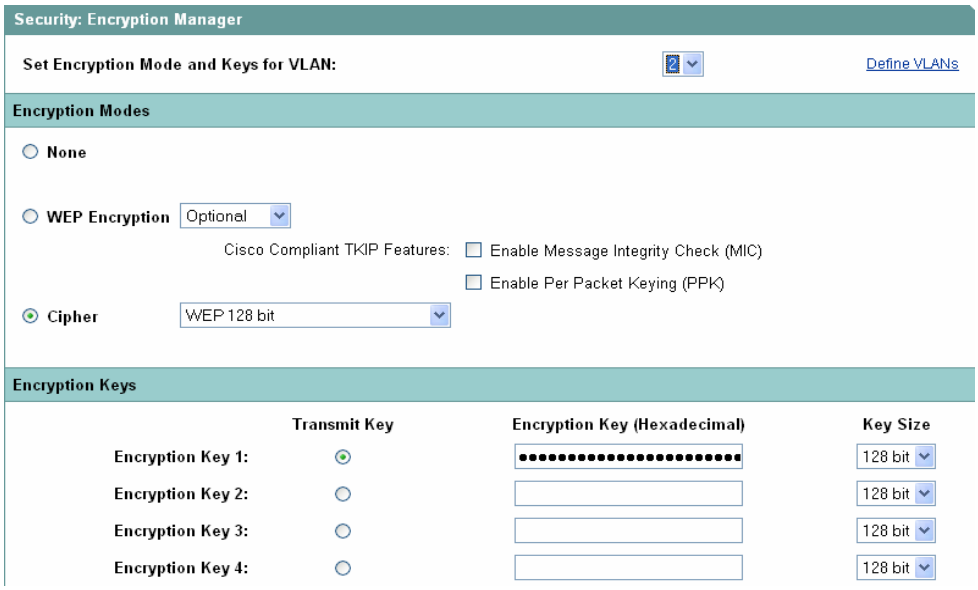
Perusverkkoasetusten laittamisen jälkeen oli vuorossa tietoturva-asetusten konfigurointi. Tässä vaiheessa huomioitavia asetuksia olivat SSID:t, käytettävät salausmenetelmät ja avainpituudet, autentikointimenetelmät sekä RADIUS-palvelimen osoitteiden konfigurointi. Kuten aikaisemmin jo tuli ilmi, tukiasemiin määriteltiin kaksi WLAN-verkkoa. Toinen oli vanhan mallin mukainen ja toinen 802.1x-määrittelyt täyttävä uuden mallin mukainen verkko. Langattomat verkot piti määritellä omiksi VLAN:ksi. Vanhan mallin mukainen verkko on VLAN 2 ja uusi VLAN 3. Molemmat verkot määriteltiin niin, että ne eivät mainosta omaa SSID-tunnustaan. Kuviossa 14 on esitetty käyttöön otetut SSID:t

Service Set Identifiers (SSIDs)

SSID	VLAN	Radio	BSSID/Guest Mode	Open	Shared	Network EAP
OLDWLAN	2	Radio0-802.11G	0014.	no addition		
NEWWLAN	3	Radio0-802.11G	0014.	with EAP		no addition

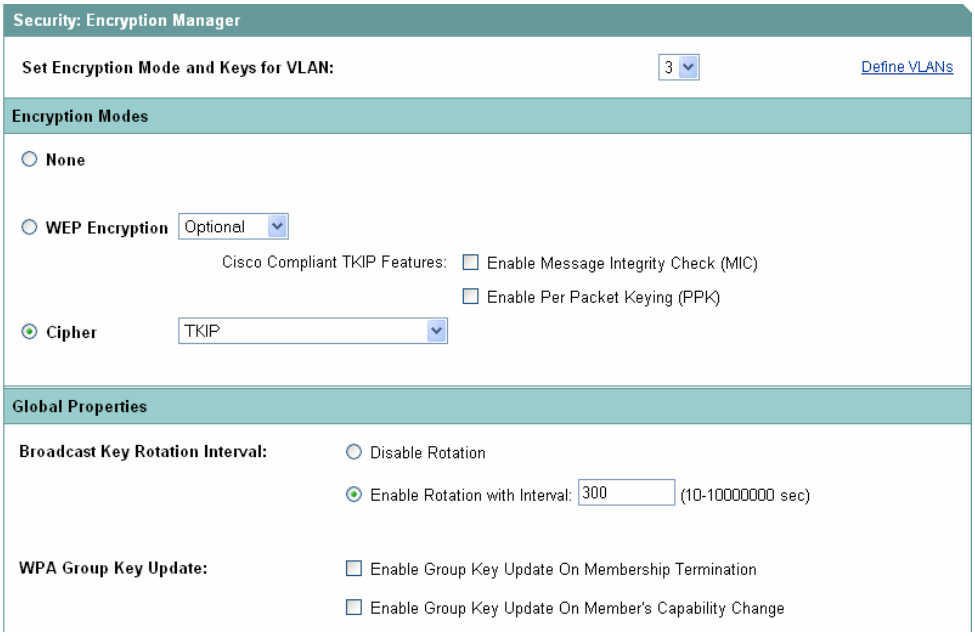
KUVIO 14. Käytetyt SSID:t

Vanhan mallin mukaiseen verkkoon määriteltiin salausmenetelmäksi 128-bittinen WEP-salaus. Käytetty salausavain syötettiin tukiasemaan. Sama avain tulee olla määriteltynä myös päätelaitteisiin, jotka käyttävät tätä verkkoa. Kuviossa 15 on esitetty VLAN 2 -salausmenetelmien konfigurointi-asetukset. Kuten kuviosta käy ilmi, olisi WEP-avaimia mahdollisuus syöttää neljä kappaletta. Sen ei kuitenkaan katsottu olevan tässä vaiheessa tarpeellista, koska tämän verkon elinikä ei tule olemaan enää pitkä. Laitteistokannan uusiuduttua uuden mallin vaatimalle tasolle ei tälle verkolle ole lainkaan tarvetta. WEP-avaimia käytettäessä tulee sekä tukiasemaan, että päätelaitteeseen määritellä mitä avainta salaukseen käytetään. Tässä tapauksessa vaihtoehtoja ei ole kuin yksi – Encryption Key 1.



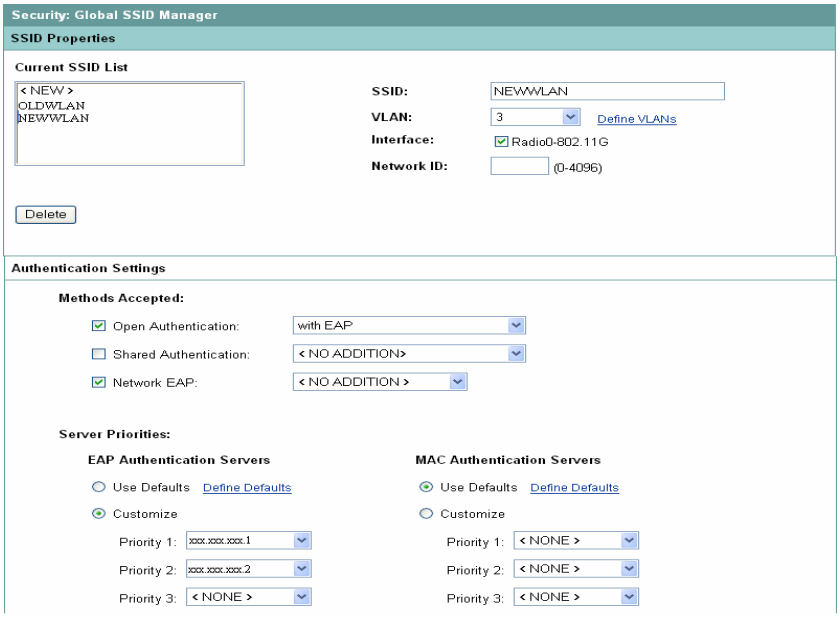
KUVIO 15. VLAN 2 -salausasetukset

VLAN 3 on uuden mallin mukainen verkko. Sen salausasetukset on esitetty kuviossa 16. Kuten kuviosta käy ilmi, on salausmenetelmänä käytetty TKIP:aa. TKIP-avaimen rotaatioajaksi määriteltiin 5 minuuttia.



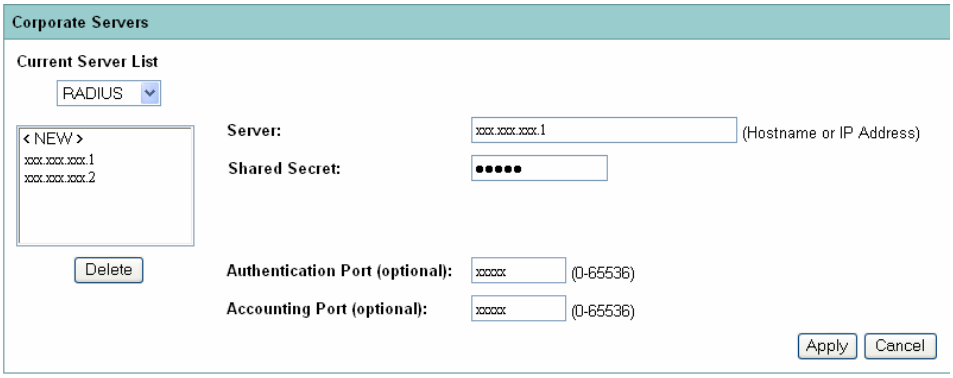
KUVIO 16. VLAN 3 -salausasetukset

Autentikointimenetelmänä VLAN 3:ssa on EAP – RADIUS-autentikointi. Sen määritykset on esitetty kuviossa 17. Tukiasemaan piti määritellä käytettävä autentikointimenettely ja autentikointipalvelimien osoitteet. Autentikointipalvelimista jälkimmäinen toimii varmistuksena sille, jos ensisijainen palvelin sattuu esim. laiterikon seurauksena olemaan pois käytöstä.



KUVIO 17. VLAN 3 -autentikointiasetukset

Tukiasemiin määriteltiin autentikointipalvelimien osalta IP-osoitteiden lisäksi Shared Secret -salasana sekä porttinumerot, joita käytetään RADIUS-palvelimien ja tukiasemien väliseen liikennöintiin. Edellä mainitut asetukset on esitetty kuviossa 18.

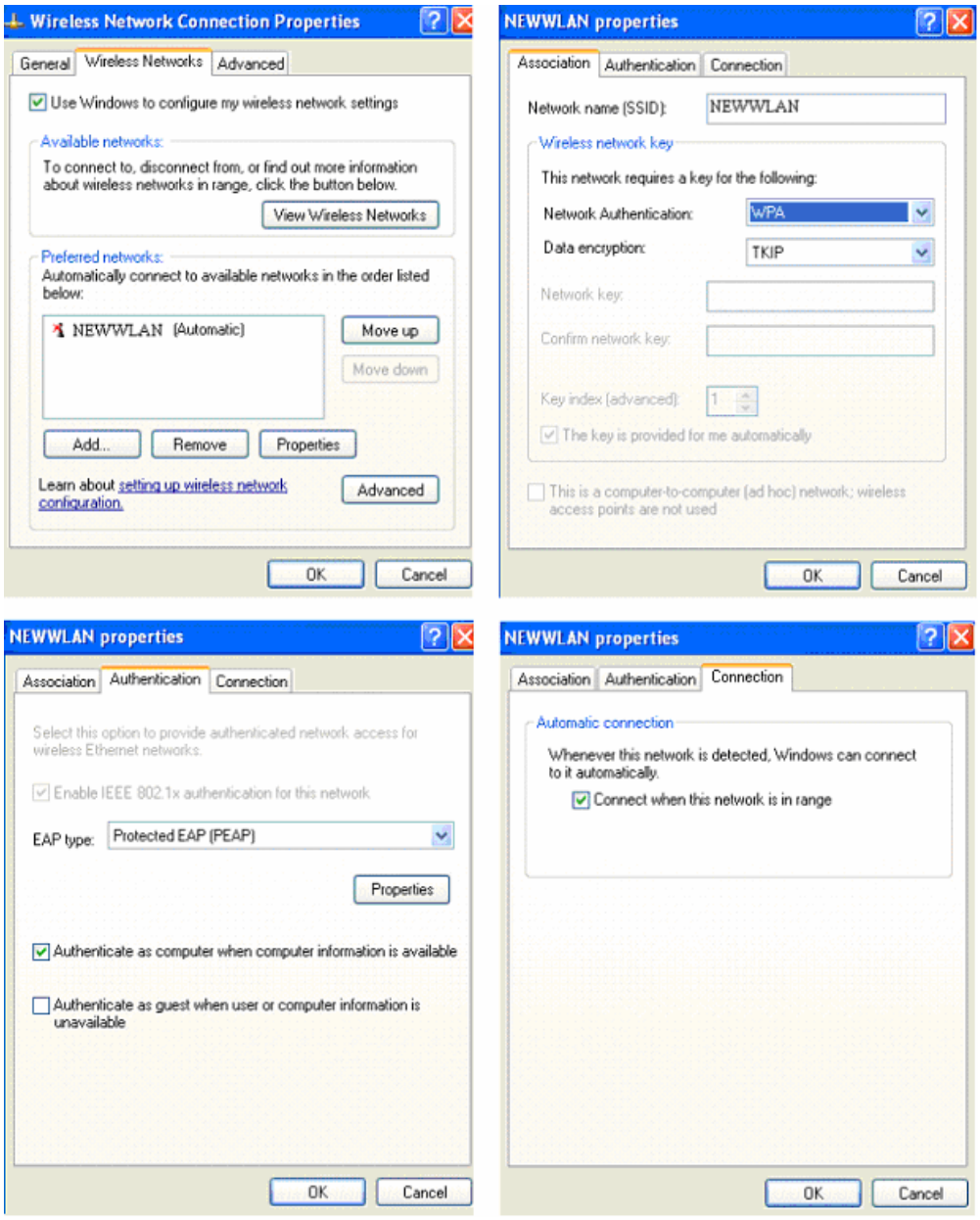


KUVIO 18. RADIUS-palvelimen asetukset tukiasemissa

7.4 Päätelaitteiden määritykset

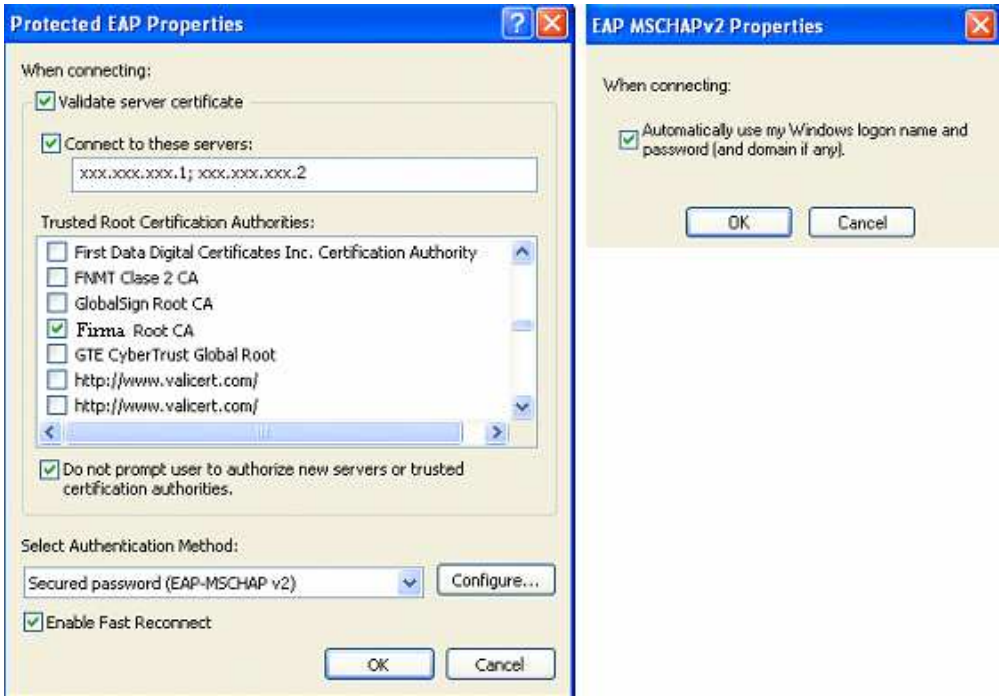
Windows XP -käyttöjärjestelmä tukee natiivisti 802.1x-määritystä. Tämän takia sitä käyttäviin kannettaviin tietokoneisiin ei tarvitse asentaa mitään erillistä ohjelmistoa. Kannettavien langattoman verkon konfigurointiin käytettiin Windowsin omaa työkalua. Sillä määriteltiin langattoman verkon yhteyden käyttävän 802.1x:ää, WPA-TKIP avaimia ja PEAP-autentikointiprosessia. Työasemien määritykset tehtiin Windowsin Control Panelista löytyvään Network Connections kohtaan. Sieltä valittiin Wireless Network Connections ja edelleen Wireless Networks Connection. Määritellyt asetukset on esitetty kuviossa 19. Kuten kuviosta käy ilmi tuli työasemiin määritellä langattoman verkon nimi SSID (NEWWLAN). Tämän lisäksi määrityksiin piti laittaa Network Authentication tyypiksi WPA ja salausasetukseksi TKIP. EAP autentikoinniksi tuli määritellä PEAP. Authentication välilehdellä piti myös valita kohta Authenticate as computer when computer information is available. Tällä määrityksellä työasema voi käyttää autentikoitumiseen koneen nimeä. Tällainen tapaus tulee kyseeseen silloin kun käyttäjä ei ole kirjaantunut koneeseen. Lisäksi määrityksiin asetettiin automaattinen yhteyden luonti, kun NEWWLAN verkko on saatavilla. Tämä tarkoittaa sitä, että työasema ottaa tähän langattomaan verkkoon automaattisesti yhteyden, kun se havaitsee

sen. Käyttäjältä ei siis vaadita mitään erityisiä toimenpiteitä. Samalla kun hän kirjaantuu normaalisti koneeseen sisään, tulee hän myös autentikoituneeksi langattomaan verkkoon.



KUVIO 19. Työasemien asetukset

Edellä esiteltyjen työasemien asetusten lisäksi, piti määritellä erikseen PEAP-autentikointiprotokolla asetukset. Määritellyt PEAP-asetukset on esitetty kuviossa 20.



KUVIO 20. Työasemien PEAP-asetukset

Validate server certificate -kohdan ollessa valittuna työasema tarkistaa, että sen palvelimelta saama sertifikaatti on edelleen voimassa. Connect to these servers -kohtaan on määritelty ne palvelimet, joihin työasema automaattisesti ottaa yhteyttä tarkistaakseen sertifikaatin. Määritellyt palvelimet ovat luotettuja. Tässä tapauksessa luotettuna tahona toimii yrityksen oma palvelin.

Select authentication method -kohtaan määritellään käytettävä autentikointityyppi. Sen määrityksenä tulee olla EAP-MSCHAPv2. Sen konfigurointiasetuksiin tulee edelleen määritellä se, että autentikoitumiseen käytetään Windowsin sisäänkirjaantumisen yhteydessä syötettyjä käyttäjätunnus – salasana – toimialue -yhdistelmää.

7.5 Microsoft IAS ja RADIUS

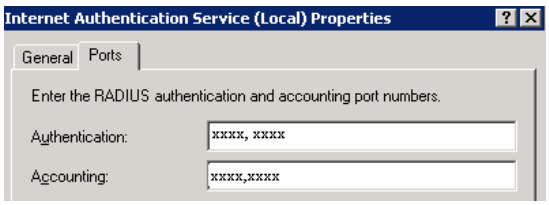
Microsoft IAS -palvelu asennettiin Microsoft Server 2003 Enterprise Edition -käyttöjärjestelmään. Kyseisen käyttöjärjestelmän Standard -versioon ei olisi voitu konfiguroida enempää kuin 50 RADIUS-asiakasta. RADIUS-asiakkaat ovat tässä tapauksessa langattoman verkon tukiasemat. Tällä hetkellä tuo määrä ei vielä ylit-

tynyt, mutta tulevaisuuden tarpeita ajatellen haluttiin käyttää Enterprise Editionia. Siinä RADIUS-asiakkaiden määrää ei ole rajoitettu.

IAS-palvelin liitettiin osaksi Active Directory -toimialuetta. Kun IAS-palvelin toimii samassa toimialueessa, se käyttää Active Directoryn tietokantaa käyttäjien autentikointiin. Tämä toiminto mahdollistaa Single Sign-on -tyyppisen kirjaantumisen. Samalla käyttäjätunnus – salasana yhdistelmällä autentikoidutaan sekä langattomaan verkkoon että kyseiseen toimialueeseen.

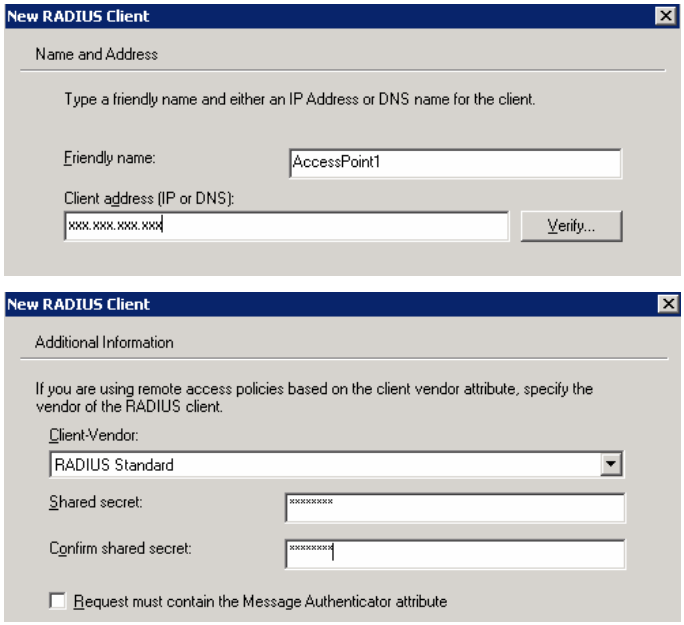
IAS-palvelimen konfigurointi aloitettiin asentamalla Windows-palvelimeen Internet Authentication Service. Se on yksi Windowsin komponenteista, joka ei ole oletuksena asennettu. Tämä tapahtui Control Panelin Add Remove Windows Components -valikosta.

Seuraavaksi asetettiin IAS-palvelimen porttinumerot. Näillä määritetään autentikointiin ja tilastointiin käytettävät portit. Samat porttinumerot konfiguroitiin jo aikaisemmin tukiasemiin. Asetukset on esitetty kuviossa 21.



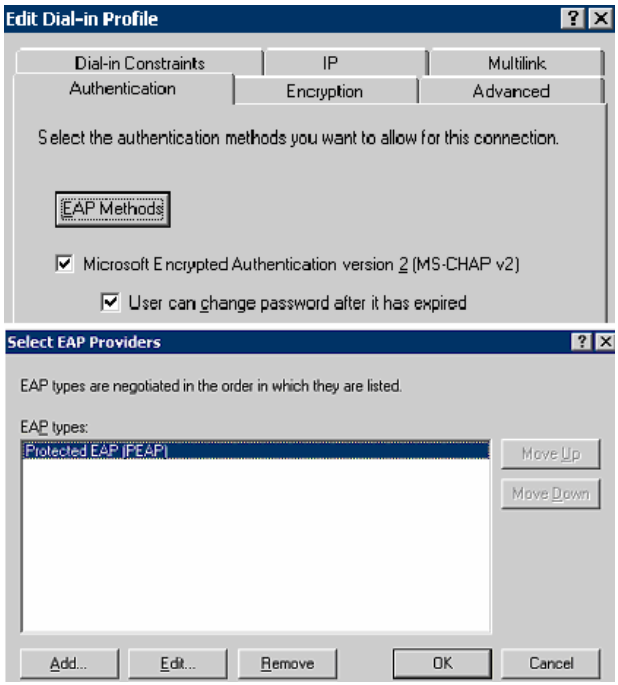
KUVIO 21. IAS Porttiasetukset

Seuraavaksi IAS-palvelimeen määritettiin RADIUS-asiakkaiden tiedot. Jokaisesta verkossa olevasta tukiasemasta piti määritellä ensin sen nimi ja IP-osoite. Seuraavassa vaiheessa määriteltiin Shared Secret -salasana. Sama salasana syötettiin jo aiemmin kaikkiin tukiasemiin. Niiden tulee siis olla identtiset. Verify-toiminnolla voi tarkistaa, että syötetty tukiaseman nimi ja IP-osoite myös löytyvät verkosta. Kuviossa 22 on esitetty RADIUS-asiakkaiden määrittelyn asetukset.



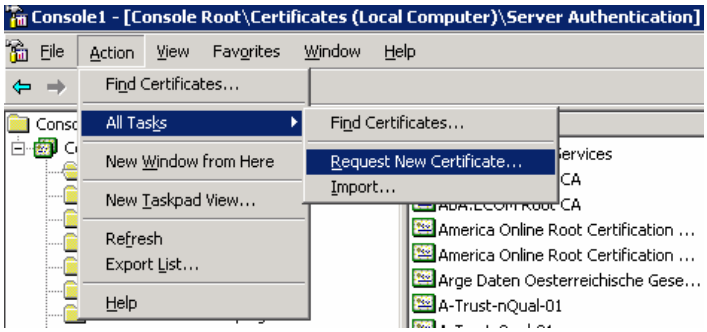
KUVIO 22. RADIUS-asiakkaiden määrittely

IAS-palvelimeen määriteltiin käyttäjäryhmä, jolle annettiin oikeudet käyttää langatonta verkkoa. Käytännössä tämä ryhmä kattaa lähes kaikki käyttäjät. Autentikoitumistavaksi tuli määritellä kuvion 23 osoittamalla tavalla PEAP - MSCHAPv2.



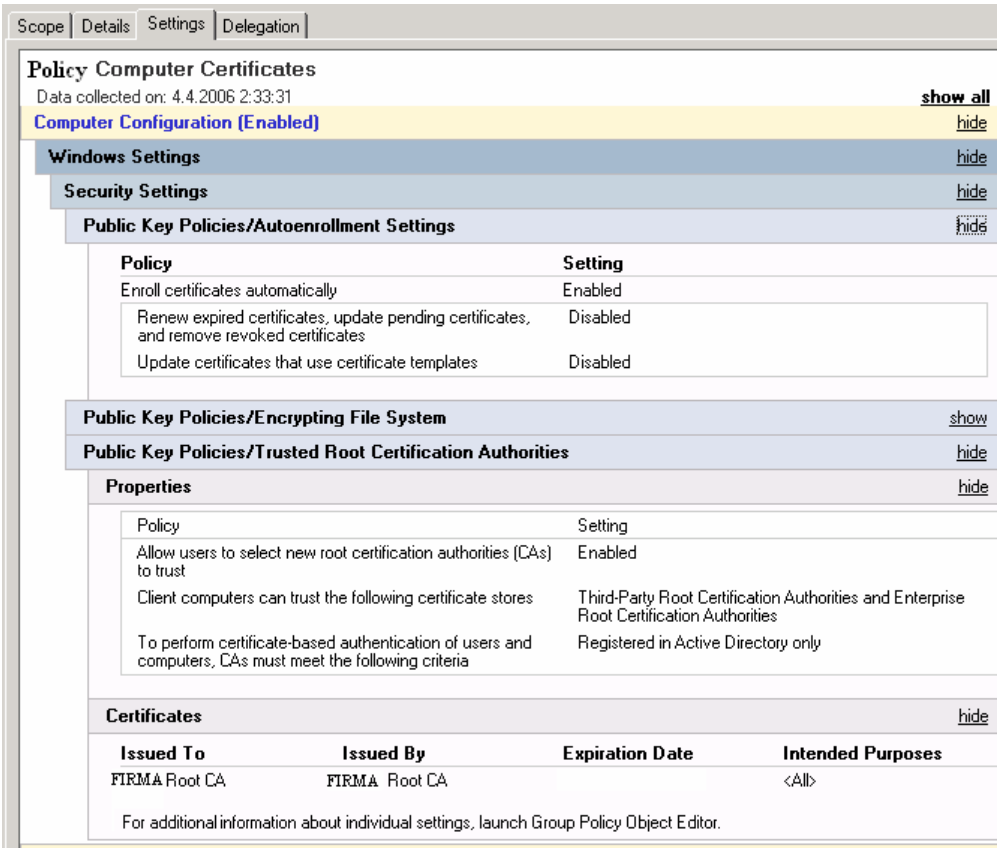
KUVIO 23. IAS-autentikointimääritykset

PEAP-määrityksiin tuli lisäksi määritellä sertifikaatti, jota IAS-palvelin käyttää todentaakseen itsensä langattoman verkon asiakkaille. Palvelimelle sertifikaatti haettiin CA-palvelimelta kuvion 24 osoittamalla tavalla.



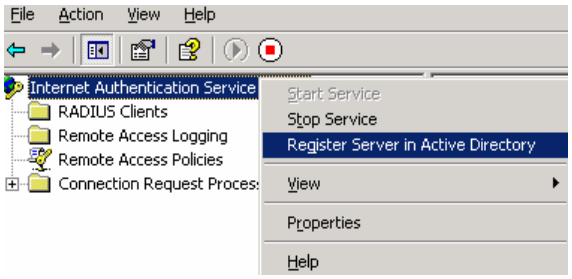
KUVIO 24. Palvelinsertifikaatin asentaminen

Kun PEAP-MSCHAPv2-autentikointimenettely on käytössä, tulee kaikissa langattoman verkon asiakaslaitteissa olla CA:n Root-sertifikaatti. Tämän voi tehdä manuaalisesti samaan tapaan kuin IAS-palvelimen tapauksessa, mutta suurissa Active Directory -ympäristöissä sen jakaminen onnistuu helpommin Group Policya hyväksi käyttäen. Käytännössä tämä tehtiin luomalla ensin ryhmä, johon kuuluivat kaikki langatonta verkkoa käyttävät laitteet. Sen jälkeen kyseiselle ryhmälle määriteltiin Group Policy, jonka asetuksiin määriteltiin luotettu CA sekä automaattinen sertifikaattien jakaminen. Group Policyn asetukset ovat kuvion 25 mukaiset.



KUVIO 25. Group policy -asetukset

IAS-palvelimen asennuksen viimeisessä vaiheessa se tuli rekisteröidä osaksi toimialueen Active Directorya. Tämä tapahtui Windowsin Internet Authentication Service -komponentista kuvion 26 osoittamalla tavalla.



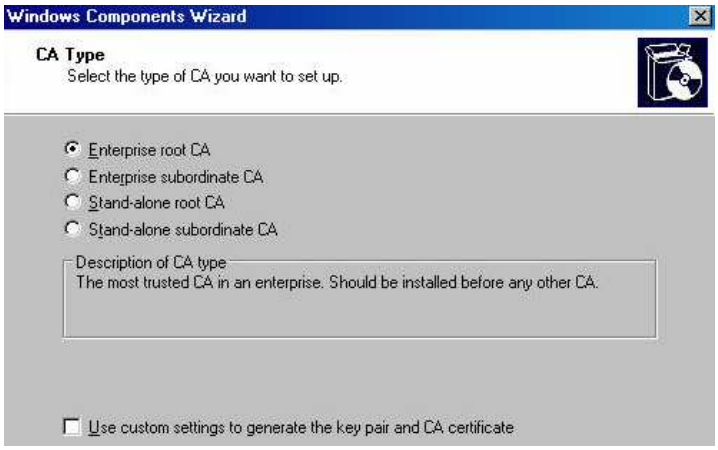
KUVIO 26. IAS-palvelimen rekisteröinti Active Directoryyn

7.6 Sertifikaatit

Käytetty sertifikaatti, jolla IAS-palvelin todentaa itsensä asiakaslaitteille, oli jo valmiiksi olemassa. Sitä ei siis tarvinnut erikseen luoda tätä tarkoitusta varten. Seuraavassa on kuitenkin pääpiirteittäin esitetty, kuinka kyseinen sertifikaatti olisi mahdollista luoda.

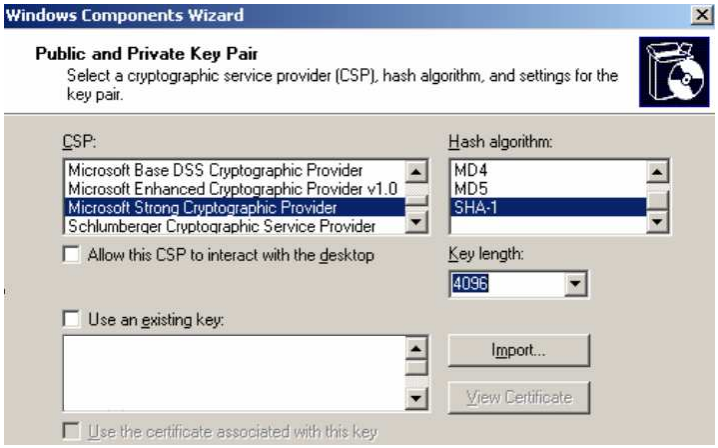
Palvelimeen, joka toimii luotettuna tahona CA, tulee olla asennettuna Windowsin Certification Authority -komponentti. CA varmistaa digitaalisella allekirjoituksellaan, että sertifikaatin tiedot ovat oikein ja että sertifikaatti on aito. Käytännössä se siis varmentaa sen, että asiakas on se, joka väittää olevansa. CA:n asentamisen yhteydessä luodaan myös palvelinsertifikaatti, jonka avulla langattoman verkon asiakaslaite pystyy todentamaan palvelimen.

Ensimmäisenä valitaan CA:n tyyppi. Tässä tapauksessa valitaan Enterprise Root CA. Kuviossa 27 on esitetty ko. valinta.



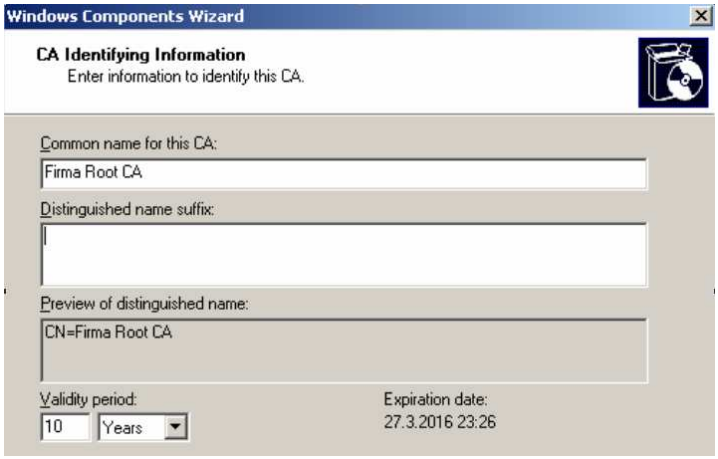
KUVIO 27. CA-tyypin valinta

Edellisessä vaiheessa on myös mahdollista tehdä muutoksia luotavaan sertifikaattiin. Kun valitaan custom settings -vaihtoehto, voidaan muun muassa luotavan avainparin pituutta ja käytettävää hajautusalgoritmia muuttaa. Se ei kuitenkaan ole välttämätöntä, sillä Windowsin tarjoamat oletusasetukset ovat tähän tarkoitukseen riittävät. Kuviossa 28 on esitetty edellä mainitut optionaaliset asetukset.



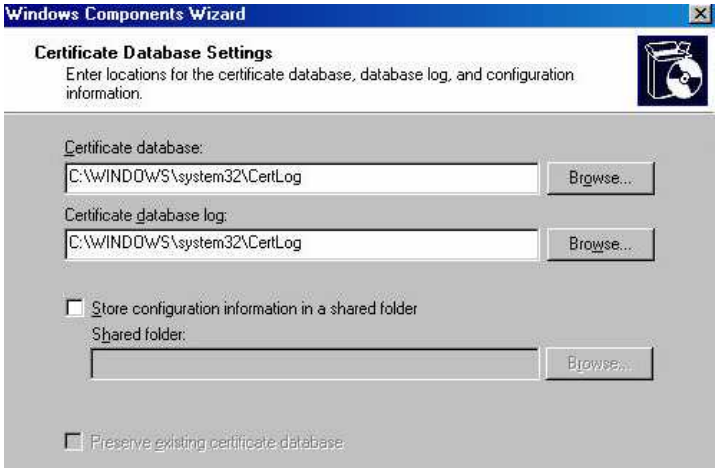
KUVIO 28. Sertifikaatin optionaaliset asetukset

Seuraavaksi valitaan CA:lle nimi. Se on yleensä sama kuin palvelimen nimi. Samassa yhteydessä määritetään CA:n voimassaoloaika. Kuviossa 29 on edellä mainitut asiat.



KUVIO 29. CA:n nimi ja voimassaoloaika

CA:n perustamisen viimeisessä vaiheessa valitaan tallennuspaikat sertifikaateille. Konfigurointitiedoille ei tarvitse määritellä omaa jaettua hakemistoa, koska ne tallennetaan Active Directoryyn.



KUVIO 30. Sertifikaattien tallennuspaikat

7.7 Vanhan ja uuden järjestelmän vertailu

Vertailtaessa vanhaa järjestelmää uuteen oli yllättävää se, että verkkoon kirjaantuminen ei hidastunut lainkaan. Tätä olisi voinut hyvinkin odottaa, sillä onhan uudessa verkossa huomattavasti monimutkaisempi autentikoitumismenettely. Työasemiin kirjaantuminen sujui suurin piirtein yhtä nopeasti kuin ennenkin.

Normaalissa työasemakäytössä ei nopeuden kasvua juurikaan huomannut. Suurin syy tähän on se, että verkossa toimii samaan aikaan sekä 802.11b- ja 802.11g -standardien mukaisia asiakaslaitteita. Tällöinhän 802.11g-verkon suorituskyky laskee huomattavasti. Laitekannan pikkuhiljaa uusiutuessa 802.11g-tasolle voidaan odottaa, että verkon suorituskyky nousee jonkun verran. Verkkoa käyttäviä käyttäjiä haastatellessa he eivät huomanneet verkon nopeudessa mitään muutosta edelliseen. Voidaan kuitenkin todeta, että uusi järjestelmä on suorituskyvyltään jo nykyisellääänkin riittävä normaaliin työasemakäyttöön.

Parantunutta tietoturvaa ei päästy käytännössä testaamaan. Tämän testaaminen olisi vaatinut erilaisten hyökkäysohjelmistojen käyttämistä. Näiden avulla olisi voitu testata, onko verkon tietoturvan murtaminen mahdollista. Lupaa tällaisten hyökkäysten suorittamiseen ei yrityksen taholta kuitenkaan saatu. Teoriaosassa tutustuin kuitenkin erilaisiin salausmenetelmiin. Niiden perusteella voidaan helposti todeta, että pelkkää WEP-salausta käytettäessä ei langattoman verkon tieto-

turva ole riittävä. WEP-salaus on helppo murtaa nykypäivän työasemilla ja vapaasti saatavilla olevilla hyökkäysohjelmilla. Uutta ratkaisua pitäisin nykypäivän vaatimuksiin hyvinkin tietoturvallisena. RADIUS-protokollan, sertifikaattien ym. uudessa ratkaisussa käytettyjen menetelmien käyttö lisää langattoman verkon tietoturvaa tuntuvasti. Parantunut tietoturva olikin tärkein seikka tässä langattoman verkon päivittämisessä.

8 YHTEENVETO

Opinnäytetyössäni oli tarkoituksena suunnitella jo olemassa olevan langattoman verkon päivitys nykyaikaisempaan ratkaisuun. Vanha verkko pohjautui 802.11b -standardin mukaisiin laitteisiin, ja salauksessa käytettiin ainoastaan WEP-salausta. Työn tärkeimpänä lähtökohtana olikin mahdollisimman hyvän tietoturvan takaaminen uuteen verkkoon.

Työn teoriaosuudessa tutustuin langattoman verkon ominaisuuksiin, erilaisiin 802.11-standardeihin, erilaisiin autentikointimenettelyihin, langattoman verkon tietoturvaan ja erilaisiin salausmenettelyihin. Lisäksi esittelin lyhyesti langattoman verkon suunnittelun pääpiirteet. Työn käytännön osuudessa suunniteltiin ja toteutettiin uuden ratkaisun mukainen verkko. Siihen kuului tukiasemien valinta ja niiden konfigurointi, verkon asiakaslaitteiden määritysten asettaminen ja sertifikaattien luominen. Lisäksi asennettiin ja konfiguroitiin RADIUS-palvelin, joka oli tyypiltään Microsoftin IAS -palvelin. IAS-palvelin asennettiin Windows 2003 Server -käyttöjärjestelmään.

Vaikka tässä työssä tehdyn mallin mukainen langaton verkko on kohtuullisen työläs toteuttaa ja sen suunnittelussa tulee ottaa huomioon monia seikkoja, niin sen tarjoama tietoturvan taso on erittäin hyvä. Mielestäni työn tavoitteet täyttyivät hyvin. Kun kaikki asetukset oli saatu eri osapuolille konfiguroiduksi, toimi verkko täysin moitteettomasti.

Rakennetun langattoman verkon suorituskyky ja tietoturva täyttää tämänhetkiset vaatimukset hyvin. Tulevaisuuden uudet langattomat ratkaisut mahdollistavat entisestäänkin nopeampia ja turvallisempia ratkaisuja. Datamäärien kasvun ja käytettävien sovellusten luonteen muuttuessa on jossain vaiheessa varmastikin tarvetta päivittää nykyistä verkkoa. Arvioisin kuitenkin, että tämän kyseisen yrityksen tarpeisiin on nykyinenkin ratkaisu täysin riittävä vielä vuosiksi eteenpäin.

LÄHTEET

Granlund, K. 2001. Langaton tiedonsiirto. Docendo, Jyväskylä.

Järvinen, P. 2002. Tietoturva & yksityisyys. Docendo, Jyväskylä.

Järvinen, P. 2003. Salausmenetelmät. Docendo, Jyväskylä.

Kerttula, E. 1998. Tietoverkkojen tietoturva. Edita, Helsinki.

Kivimäki, J. 2005. Active Directory – Tehokas hallinta. Gummerus, Jyväskylä.

Puska, M. 2005. Langattomat lähiverkot. Gummerus, Jyväskylä.

Stanek, W. 2003. Microsoft Windows Server 2003 – Asiantuntijan käsikirja. 3. painos. Edita Prima Oy, Helsinki.

Elektroniset lähteet:

Ahvenainen, M. Langattomien Lähiverkkojen Turvallisuus [verkkodokumentti]. Espoo: Helsingin teknillinen korkeakoulu, 2003 [viitattu 10.3.2006]. Saatavissa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf

Cisco. Cisco – Wireless LAN Security White Paper [verkkodokumentti]. 2006a [viitattu 12.3.2006]. Saatavissa: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm

Cisco. Cisco Aironet 1230 AG Series [verkkodokumentti]. 2006b [viitattu 2.4.2006]. Saatavissa: http://www.cisco.com/en/US/products/ps6108/products_data_sheet0900aecd801b9068.html

Geier, J. 802.11 Alphabet Soup [verkkodokumentti]. 2002a [viitattu 4.3.2006]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/1439551

Geier, J. 802.1X Offers Authentication and Key Management [verkkodokumentti]. 2002b [viitattu 4.3.2006]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/1041171

Griffith, E. 802.11i Security Specification Finalized [verkkodokumentti]. 2004 [viitattu 4.3.2006]. Saatavissa: http://www.wi-fiplanet.com/news/article.php/3373441

Griffith, E. 802.11n Draft Approved [verkkodokumentti]. 2006 [viitattu 4.3.2006]. Saatavissa: http://www.wi-fiplanet.com/news/article.php/3578886

Heikkinen, S. Autentikointi WLAN-verkossa [verkkodokumentti]. Tampere: Tampereen Teknillinen Yliopisto, 2003 [viitattu 4.3.2006]. Saatavissa: http://www.cs.tut.fi/~sheikki/kurssit/Wlan-essee.doc

Jokisuu, M. Verkkotutkimuskeskuksen organisointihanke [verkkodokumentti]. Seinäjoki: Tampereen yliopisto, Täydennyskoulutuskeskuksen Seinäjoen toimipaikka, 2002 [viitattu 4.3.2006]. Saatavissa: http://www.wirlab.net/raportit/loppuraportti_WirlabII.pdf

Keski-Kasari, S. Verkkopalveluiden autentikointi yhteisen käyttäjätietokannan avulla [verkkodokumentti]. Tampere: Tampereen Teknillinen Korkeakoulu, 2002 [viitattu 18.3.2006]. Saatavissa: http://www.wirlab.net/pdf/di_tyo_samikk.pdf

Microsoft. Microsoft TechNet: Introducing IAS [verkkodokumentti]. 2006a [viitattu 25.3.2006]. Saatavissa: http://technet2.microsoft.com/WindowsServer/f/?en/Library/e679603e-40eb-4c14-bffb-ccb8efd67ff81033.mspx

Microsoft. Windows XP Wireless Deployment Technology and Component Overview [verkkodokumentti]. 2006b [viitattu 19.3.2006]. Saatavissa: http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx

Rigney, C., Willens, S., Rubens, A. & Simpson, W. Remote Authentication Dial In User Service (RADIUS) [verkkodokumentti]. 2000 [viitattu 24.3.2006]. Saatavissa: http://www.ietf.org/rfc/rfc2865.txt

Simpson, W. RFC 1661 - The Point-to-Point Protocol (PPP) [verkkodokumentti]. 2000 [viitattu 18.3.2006]. Saatavissa: http://www.faqs.org/rfcs/rfc1661.html

Vesanen, A. Siirtoyhteysprotokollien tietoturvaa [verkkodokumentti]. Oulu: Oulun yliopistojen tietojenkäsittelyn laitos, 2006 [viitattu 19.3.2006]. Saatavissa: http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/wlan/Siirtoyhteys.html

Wi-Fi Alliance. Wi-Fi Protected Access [verkkodokumentti]. 2003 [viitattu 12.3.2006]. Saatavissa: http://www.wi-fi.org/files/uploaded_files/wp_8_WPA%20Security_4-29-03.pdf

Wilson, J. Quadrupling Wi-Fi speeds with 802.11n [verkkodokumentti]. 2004 [viitattu 4.3.2006]. Saatavissa: http://www.deviceforge.com/articles/AT5096801417.html