TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Tietoturvallinen WLAN

CASE: ICM Finland Oy

Teemu Wilkman

Tietojenkäsittelyn koulutusohjelma
joulukuu 2006
Työn ohjaaja: Harri Hakonen

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t)	Teemu Wilkman
Koulutusohjelma(t)	Tietojenkäsittely
Opinnäytetyön nimi	Tietoturvallinen WLAN - CASE: Oy Information Chain Management Finland Ltd (ICM Finland)
Työn valmistumis-kuukausi ja -vuosi	Joulukuu 2006
Työn ohjaaja	Harri Hakonen

Sivumäärä: 62

TIIVISTELMÄ

Tämä opinnäytetyö keskittyy langattomien lähiverkkojen tekniikkaan ja tietoturvaan. Langattomuus tuo uusia mahdollisuuksia ja antaa vapauden käyttää verkkopalveluita paikoissa, joissa ei ole kaapeloitua verkkoa.

Langattomat verkot perustuvat IEEE 802.11 -standardiin ja laitteet toimivat lupavapaalla 2,4 GHz:n tai 5 GHz:n taajuusalueella. Tietoa voidaan siirtää langattomasti jopa 54 Mb/s vauhdilla.

Työn alkuosassa perehdytään IEEE 802.11 -standardiin perustuvien langattomien verkkojen tekniikkaan ja tietoturvaan. Tietoturva on langattomien verkkojen keskeisin ja samalla haastavin ominaisuus. Langattomat verkot sisältävät monia erilaisia turvallisuusmekanismeja, jotka antavat hyvin erilaisen suojan verkolle. Tässä työssä käsitellään laajemmin IEEE 802.11i -tietoturvastandardia, johon tulisi nykypäivänä kaikkien langattomien verkkojen tietoturvan perustua. Tällä varmistetaan, että verkon suoja on riittävällä tasolla.

Opinnäytetyön loppuosassa on kuvattu toimeksiantajalle toteutettu langaton lähiverkko. Verkko on toteutettu Windows–ympäristöön ja verkossa käytettävät tietoturvamekanismit perustuvat IEEE 802.11i -tietoturvastandardiin. Verkon autentikointi hyödyntää verkossa olevaa Active Directory -hakemistopalvelua, jossa käyttäjätiedot keskitetysti sijaitsevat.

Langattoman verkon toteuttamisessa tarvitaan erikoisosaamista ja tietoturva-asioiden hallintaa. Opinnäytetyön tarkoitus on omalta osaltaan edistää lukijan osaamista.

Avainsanat WLAN IEEE 802.11 IEEE 802.11i tietoturva autentikointi

TAMPERE
POLYTECHNIC

Author(s)	Teemu Wilkman
Degree Programme(s)	Business Information Systems
Title	Securing wireless network - CASE: Oy Information Chain Management Finland Ltd (ICM Finland)
Month and year	December 2006
Supervisor	Harri Hakonen **Pages:** 62

ABSTRACT

This thesis investigates a mechanics and a security of a wireless local area network. Wireless network brought in new possibilities and gives freedom to use the network services in new places where the cabled network is not available.

A wireless local area network based on the IEEE 802.11 standards. All the hardware that based on this standard operates in 2,4 or 5 GHz frequency band. These frequency bands are licence free bands. With these standards transmission speed is up to 54 Mbps.

Beginning of this thesis investigates a wireless local area network mechanics and data security. Data security is an essential point of a wireless local area network and perhaps a challenging feature. Wireless network includes many different features of data security mechanisms that give the network different level of security. This thesis discuss more widely IEEE 802.11i standard that now days all the data security of a wireless local area network should be based on. That way we can ensure that a security of a wireless local area network is sufficient level.

Final part of this thesis focuses on an employer's case of a wireless local area network. This network is implemented on the Windows environment and the security of this case based on the IEEE 802.11i standard. The network authentication is integrated in the part of the service called Active Directory.

Implementing a wireless local area network needs a special skills and understanding of needs of security elements. This thesis improves the reader's knowledge of a wireless local area network.

Keywords WLAN IEEE 802.11 IEEE 802.11i security authentication

SISÄLLYS

KÄSITTEET

Active Directory	Käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa Windows -verkon käyttäjistä ja laitteista.
Autentikointi	(*Authentication*) on menetelmä, jolla varmistetaan tietojärjestelmien osapuolten alkuperä.
Beacon	(*Majakka-sanoma)* on tukiaseman lähettämä yleislähetys-viesti, jossa tukiaseman mainostaa SSID-tunnusta, käytössä olevia salausmenetelmiä ja verkkonopeutta.
EAP	(*Extensible Authentication Protocol*) on todennusprotokollan runko, jota käytetään todennusmenetelmien kuljetusalustana.
IEEE	(*Institute of Electrical and Electronics Engineers*) on standardisointijärjestö, joka julkaisee tietoliikenneverkoihin standardeja.
IEEE 802.11	IEEE:n julkaisema standardi langattomille lähiverkoille.
IEEE 802.11i	IEEE:n julkaisema tietoturvastandardi langattomille lähiverkoille.
IEEE 802.1X	IEEE:n julkaisema standardi, jolla estetään verkkolaitteen liikennöinti siihen asti, kun se on autentikoitu verkkoon.
IETF	(*Internet Engineering Task Force*) on maailman laajuinen organisaatio, joka antaa suosituksia internet-protokollien parantamiseksi.
RFC	(*Request for Comments*) on IETF:n julkaisemia teknisiä dokumentteja, jotka käsittelevät tietoliikenneverkkojen protokollia.
RSN	*(Robust Security Network*) on IEEE 802.11i –tietoturvastandardia noudattavan langattoman lähiverkon keskeisin käsite.
RSNA	(*Robust Security Network Association*) on turvayhteys, joka luodaan osapuolten välille IEEE 802.11i –tietoturvastandardia noudattavissa langattomissa lähiverkoissa.
Sertifikaatti	(*Certificate*) on keino, jolla voidaan tunnistautua tietoverkossa.
SSID	(*Service Set Identifier*) on langattoman verkkosolun verkkotunnus.
TLS	(*Transport Layer Security*) on salausprotokolla, jolla voidaan salata yhteyspisteiden välinen tietoliikenne.
Varmenneviranomainen	(*Certificate Authority*) on osapuoli, joka varmistaa laitteiden sertifikaattien aitouden.

WEP	(*Wired Equivalent Privacy*) on salausmenetelmä, jolla suojataan liikenne kahden langattoman yhteyspisteen välillä.
WLAN	(*Wireless Local Area Network*) on langaton lähiverkko.
WPA	(*Wi-Fi Protected Access*) on WEP-protokollan seuraaja, joka kehitettiin WEP-protokollasta löytyneiden heikkouksien jälkeen.
WPA2	(*Wi-Fi Protected Access 2*) on IEEE 802.11i -tietoturvastandardin markkinoinnissa käytetty nimi.

1 JOHDANTO

Opinnäytetyön aiheena on tietoturvallisen WLAN-verkon toteuttaminen ICM Finland Oy:lle. Langattoman verkon uudistaminen tuli ajankohtaiseksi viime kesänä, kun yrityksellä ollut langaton verkko ei vastannut tämän päivän vaatimuksia niin turvallisuuden kuin käytettävyydenkään osalta. Verkkoa lähdettiin uudistamaan turvallisuuden ja käytettävyyden parantamiseksi. Toteuttamani langaton verkko noudattaa IEEE 802.11i -tietoturvastandardia ja verkko on toteutettu Microsoft Windows 2003 -palvelinympäristöön. Opinnäytetyö on tehty toimeksiantajan langattoman verkon uudistamiseksi toteutetun projektin pohjalta.

Opinnäytetyö koostuu kahdesta osasta. Työn alussa perehdytään hieman langattomien verkkojen tekniikkaan, käytettäviin standardeihin ja tietoturvaan. Työn loppuosassa esitellään toimeksiantajalle toteutettu langaton verkko. Työn pääpaino on langattoman verkon tietoturva-asioiden käsittelyssä. Työn tietoturva osiossa käsitellään tietoturvaa yleisellä tasolla ja perehdytään langattoman verkon sisältämiin tietoturvauhkiin.

Langaton verkko liittyy läheisesti IEEE 802.11 -standardiin ja standardin pohjalta julkaistuihin parannuksiin. Käsittelen työssäni tarkemmin 802.11 -standardin sisältämiä tieturvamekanismeja ja perehdyn IEEE:n julkaisemaan 802.11i -tietoturvastandardiin. IEEE 802.11i on tietoturvastandardi, joka luo keinot joiden avulla pystytään ratkaisemaan kaikki alkuperäisen 802.11 -standardin tietoturva heikkoudet.

1.1 Toimeksiantajan esittely

Suoritin opintoihini kuuluvan työharjoittelujakson tamperelaisessa ohjelmistoyrityksessä ICM Finland Oy:ssä. Yritys suunnittelee ja toteuttaa sovelluksia projektinhallinta ja kommunikointi käyttöön. Yrityksen tärkeimmät tuotteet ovat ICM Customer, joka on työkalu asiakasinformaation hallintaan ja ICM Project, jolla hallitaan projektitietoja. ICM Project soveltuu myös projektikumppaneiden väliseen kommunikointiin. Yrityksen suunnittelemien sovellusten alla väliohjelmistona käytetään IBM Lotus Dominoa.

1.2 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena oli perehtyä langattomien verkkojen tietoturvallisuus uhkiin ja tutkia minkälaisia mekanismeja langattomiin verkkoihin on kehitetty turvallisen liikennöinnin takaamiseksi. Opinnäytetyö jää toimeksiantajalle teknisenä dokumenttina verkon toteutuksesta. Opinnäytetyötä voi myös hyödyntää langatonta verkkoa suunniteltaessa tai sitä toteuttaessa. Opinnäytetyö kannattaa lukea myös kaikkien niiden, jotka ovat kiinnostuneita langattoman verkon tietoturvallisuustekniikasta.

2 STANDARDIT

IEEE (Institute of Electrical and Electronics Engineers) on määritellyt langattomiin verkkoihin IEEE 802.11 -standardin. Standardista on nykyään useita eri versioita, jotka kaikki pohjautuvat alkuperäiseen 802.11 -standardiin. Alkuperäinen versio saatiin valmiiksi vuonna 1997, jonka jälkeen sen kehittely jaettiin työryhmiin. Jokainen työryhmä keskittyi parantamaan standardia. Alkuperäisestä standardista on julkaistu myöhemmin useita parannettuja versioita. Taulukossa 1 on yleisimmät käytössä olevat standardit.

802.11 on alkuperäinen IEEE:n julkaisema standardi, josta työtyhmät ovat julkaisseet parannettuja versioita. Siirtokapasiteetti on 1 tai 2 megabittiä sekunnissa ja se toimii vapaalla 2,4 GHz:n taajuudella. 802.11a on 5 GHz:n taajuusalueella toimiva verkkotekniikka ja sen siirtokapasiteetti on 54 MB/s. 802.11b on nykyisin yleisin käytössä oleva standardi, jonka siirtokapasiteetti on 11 Mb/s. Tähän standardiin pohjautuvat laitteet toimivat vapaalla 2,4 GHz:n taajuudella. 802.11g -standardi on parannettu versio b-standardista ja se on yhteensopiva b-laitteiden kanssa. g-standardin laitteet keskenään voivat siirtää tietoa 54 Mb/s nopeudella.

Standardi	**Taajuusalue**	**Tiedonsiirtonopeus**
802.11	2,4 GHz	2 Mb/s
802.11a	5 GHz	54 Mb/s
802.11b	2,4 GHz	11 Mb/s
802.11g	2,4 GHz	54 Mb/s

Taulukko 1. standardit

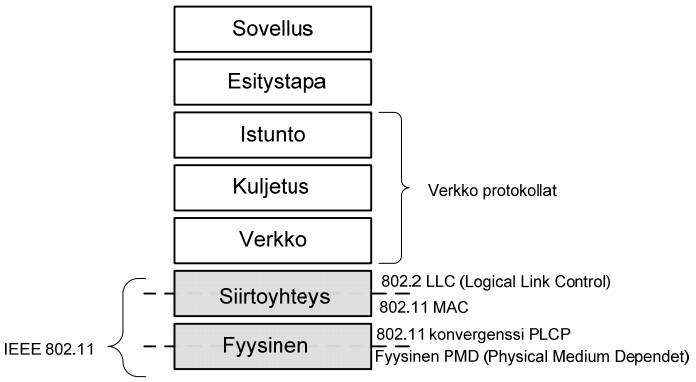
3 TIEDONSIIRTOTEKNIIKKA

IEEE 802.11 -standardi määritellään OSI-mallin kahdella alimmalla kerroksella (kuva 1), jotka ovat siirtoyhteyskerros ja fyysinen kerros. Siirtoyhteyskerroksen toiminnot on jaettu kahtia LLC (logical Link Control) ja vuoronvaraus (MAC, Medium Access Control) toimintoihin. 802.2 LLC-alikerros tarjoaa palveluita verkkokerrokselle. Verkkokerroksen IP-paketti kehystetään LLC-kehyksellä, jonka otsikko sisältää protokollatunnukset ja ohjaustiedot. (Puska 2005: 27)

LLC-alikerroksen alapuolella määritellään vuoronvaraus ja sen hoitaa 802.11 Mac-alikerros. Mac-alikerroksella LLC-kehys pilkotaan pienempiin osiin, jotta siirto virheettömästi olisi helpompaa. LLC-kehys kehystetään tällä kerroksella Mac-tietosähkeeksi (MPDU, MAC Protocol Data Unit). Kehyksen otsikossa on vuoronvarauksen kesto, sekvenssitieto, osoitteet ja tarkastussumma. Tällä kerroksella määritellään myös vuoronvaraus ja kehyksen väliset ajat. (Puska 2005: 27)

Siirtoyhteyskerroksen alapuolella oleva fyysinen kerros jaetaan ylemmänkerroksen tavoin kahtia. Konvergenssi -alikerroksella sovitetaan eri bittinopeudet ja fyysinen siirtotie yhteen, sen sovittamiseen käytetään PLCP-protokollaa (Physical Layer Convergence Procedure). (Puska 2005: 28)

Alimmalla kerroksella, jota kutsutaan PMD-kerrokseksi (Physical Medium Dependent) määritellään kanavointitapa, hajaspektritekniikan toteutus ja modulointi. Tämä kerros on fyysisestä mediasta riippuva, koska 802.11 -standardin eri versiot toimivat eri bittinopeuksilla ja niille on määritelty erilaiset modulointimenetelmät. (Puska 2005: 28)



Kuva 1. OSI-malli

3.1 Taajuusalueet

IEEE 802.11 -standardin verkot käyttävät lupamenettelystä vapautettua taajuusaluetta ja ne toimivat 2,4 GHz tai 5 GHz taajuusalueella. Taajuusalue on pilkottu pienempiin osiin eli kanaviin. Eri kanavilla toimivat WLAN-verkot tai tukiasemat voivat toimia lähekkäin ilman, että ne häiritsevät toisiaan.

2,4 GHz:n taajuusalue

Tällä taajuudella toimivat kanavat kuuluvat ns. ISM-kaistaan (Industrial, Scientific and Medical), joka on maailmanlaajuinen lupavapaa radiotaajuuskaista. Taajuusalueella olevat kanavat menevät osittain päällekkäin, koska radiokaistan leveyttä ei ole määritelty tarkasti. Kanavat on jaettu 5 MHz:n välein. Useiden tukiasemien verkoissa kannattaa lähekkäin oleville tukiasemille valita kaukana toisistaan olevat kanavat. Tämä estää häiriöiden syntymisen. IEEE 802.11b ja -g -standardin verkot käyttävät tätä taajuusaluetta. (Hakala & Vainio 2005: 153–154)

5 GHz:n taajuusalue

5 GHz:n kanavat kuuluvat myös osittain ISM-kaistaan, mutta joitakin kanavia on varattu viranomaisten käyttöön. EU-alueella 5150–5350 MHz:n kanavia voidaan käyttää ainoastaan sisätiloissa. Ulko- ja sisätiloissa voidaan käyttää 5470–5725 MHz alueen kanavia. 5 GHz:n alueella olevien kanavien lupamenettelyssä on maakohtaisia eroja. IEEE 802.11a -standardin laitteet käyttävät tätä taajuusaluetta. (Hakala & Vainio 2005: 155)

3.2 Modulointi

Modulointitekniikka on lähtöisin sotilaskäyttöön suunnitelluista laitteista. Suomessa yleisimmin käytetyt 802.11b ja -g -standardin laitteet perustuvat hajaspektritekniikkaan. Hajaspektritekniikassa digitaalisesta informaatiosta muodostettu radiosignaali siirretään useasti vaihtuvilla taajuuksilla. Kaistan leveys on saatu vaihtuvien taajuuksien ansiosta yli nelinkertaiseksi 5 Ghz:n taajuudella toimiviin kanaviin verrattuna. (Hakala & Vainio 2005: 156)

Modulointi – ja koodaustekniikan muutoksilla on pyritty parantamaan verkon luotettavuutta ja nopeutta. Korkeataajuiset radiosignaalit heijastuvat seinien ja kiinteiden esteiden kautta. Heijastukset summautuvat pienellä viiveellä radiosignaaliin, joka kulkee vastaanottajalle. Heijastuksesta aiheutuvia häiriöitä kutsutaan interfensiksi ja vastaanottaja ei pysty kunnolla lukemaan signaalin sisältämää tietoa ilman virheenkorjaus mekanismia. (Hakala & Vainio 2005: 156)

WLAN-verkon todellinen siirtonopeus jää teoreettisesta nopeudesta erityisesti suuria tietomääriä siirrettäessä. Kannettavan tietokoneen tai PDA-laitteen sisältämän WLAN-piirin todellinen nopeus voi jäädä huomattavasti teoreettisesta nopeudesta. Laitteiden sisältämät WLAN-piirit pudottavat nopeutta signaalin ollessa heikko tai signaali on interfenssin turmelema. Esimerkiksi 802.11b -verkon nopeus putoaa 11 MB/s nopeudesta portaittain ensin 5,5 Mb/s, 2 Mb/s ja 1 Mb/s. Verkon siirtonopeuteen vaikuttaa signaalin vahvuus ja häiriöttömyys.

3.2.1 Monikantoaaltomodulointi

Monikantoaaltotekniikassa informaatio lähetetään samanaikaisesti useaa eritaajuista kantoaaltoa käyttämällä. Tätä tekniikkaa käytetään 802.11a ja 802.11g -verkoissa. 802.11g -verkossa tosin tekniikkaa käytetään vain, kun tietoa siirretään yli 20 Mb/s nopeudella. Pienempää nopeutta käytettäessä 802.11g -standardia tukevat laitteet käyttävät samaa modulointitekniikkaa 802.11b -standardin kanssa, jotta b- ja g-standardin laitteet voivat kommunikoida keskenään. (Puska 2005: 40-44)

3.2.2 Suorasekvenssi hajaspektri

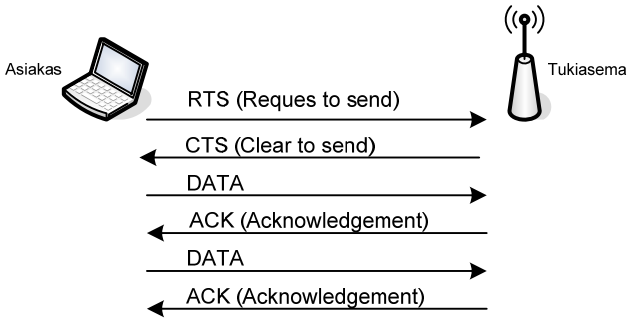
Suorasekvenssi hajaspektri (Direct Sequence Spread Spectrum, DSSS) -tekniikkaa käytetään 802.11b sekä 802.11g -verkossa alle 20 Mb/s nopeudella. Tekniikka toimii koodausbiteillä, joiden avulla signaali lähetetään usealla vaihtuvalla taajuudella. Vastaanottaja rakentaa tiedon uudelleen yhdistämällä eri taajuudella vastaanotetut signaalit koodausbittikaavion avulla. Tiedonsiirron aikana vioittuneet bitit pystytään uudelleen rakentamaan koodausbittien avulla. DSSS -tekniikassa käytetään CCK-koodausta (Complementary Code Keying), jolloin suurempi tietomäärä saadaan lähetettyä yhtenä signaalina. (Puska 2005: 34-36)

3.3 Väylänvaraus- ja siirtoyhteysmäärittely (Puska 2005: 29)

Väylänvaraus- ja siirtoyhteysmäärittelyt tehdään siirtoyhteyskerroksella. Langattomassa verkossa käytetään CSMA/CA (Carrier-Sense Multiple Access / Collision Avoidance) väylänvaraustekniikkaa. Tekniikka muistuttaa Ethernet-verkossa käytettävää CSMA/CD (Carrier Sense Multiple Access With Collision Detection) tekniikkaa. Langattomassa verkossa tekniikka kuitenkin poikkeaa hieman Ethernet-verkon tekniikasta, koska verkossa käytetään ns. half-duplex lähetystapaa eli tietoa voidaan kerrallaan vastaanottaa tai lähettää. Tämän takia törmäyksiä ei voi tunnistaa lähetyksen aikana, kuten Ethernetin CSMA/CD menetelmässä. Törmäysten havaitseminen on korvattukin niiden välttämisellä. Törmäykset vältetään kantoaaltoa kuuntelemalla. Ennen lähetyksen aloittamista laite varmistaa kanavan olevan vapaa kuuntelemalla radiotietä.

Radiotiellä on myös mahdollista, että asiakkaat kuulevat tukiaseman lähetyksen, mutta eivät toistensa lähetystä. 802.11 -verkon vuoronvaraustekniikka mahdollistaa virtuaalisen kantoaallon kuuntelun (Virtual Carrier Sense). Tukiasema tällöin kontrolloi kaikkia solun asiakkaita ja myöntää jokaiselle asiakkaalle lähetysluvan tietyksi ajaksi. Vain lähetysluvan saanut asiakas voi keskustella tukiaseman kanssa. Vuoronvaraus hoidetaan RTS/CTS -kättelyllä (kuva2). Toiminto on langattomassa verkoissa optio, mutta sitä kannattaa käyttää paljon asiakkaita ja liikennettä sisältävissä verkoissa.

Kättely tapahtuu siten, että asiakas lähettää ensin lähetyspyynnön RTS-viestillä (Request to send), johon tukiasema vastaa CTS-viestillä (clear to send) tukiaseman ollessa vapaa vastaanottamaan tietoa. Tämän jälkeen lähetetään varsinainen viesti ja vastaanotto varmistetaan jokaisen kehyksen jälkeen kuittausviestillä (ACK, Acknowledgement).



Kuva 2. *RTS/CTS -kättely* (Puska 2005: 29)

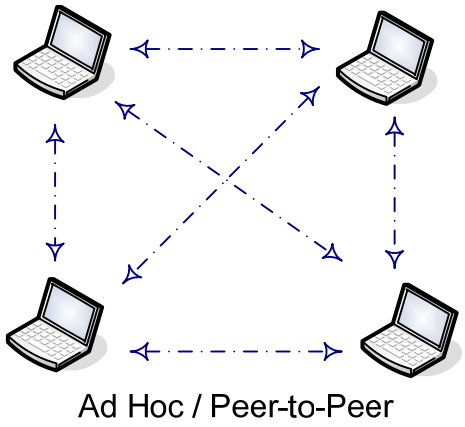
4 LANGATTOMAN VERKON TOPOLOGIAT

Langattomiin verkkoihin on määritelty 802.11 -standardissa kaksi erilaista topologiatoteutusta. Langattoman verkon voi muodostaa kahden tai useamman laitteen välille tai langattoman verkon asiakkaat voivat olla tukiaseman kautta yhteydessä kiinteään lankaverkkoon. Seuraavissa luvuissa perehdytään hieman tarkemmin langattoman verkon topologioihin.

4.1 Ad hoc / Peer-to-Peer (IEEE Computer Society 1999: 25)

Ad hoc -topologia on kaikkein yksinkertaisin verkkototeutus. Ad hoc -verkko koostuu kahdesta tai useammasta laitteesta, joilla on yhteys toisiinsa. Laitteet keskustelevat suoraan toistensa kanssa. Liikenne ei kulje muiden laitteiden, kuten tukiaseman kautta.

Ad hoc on hyödyllinen ratkaisu pienissä tiloissa, koska verkko tietokoneiden välillä saadaan rakennettua nopeasti ja vaivattomasti. Liikenne kulkee suoraan osoitetulle koneelle. Kuvassa 3 on havainnollistettu Ad hoc -topologia.



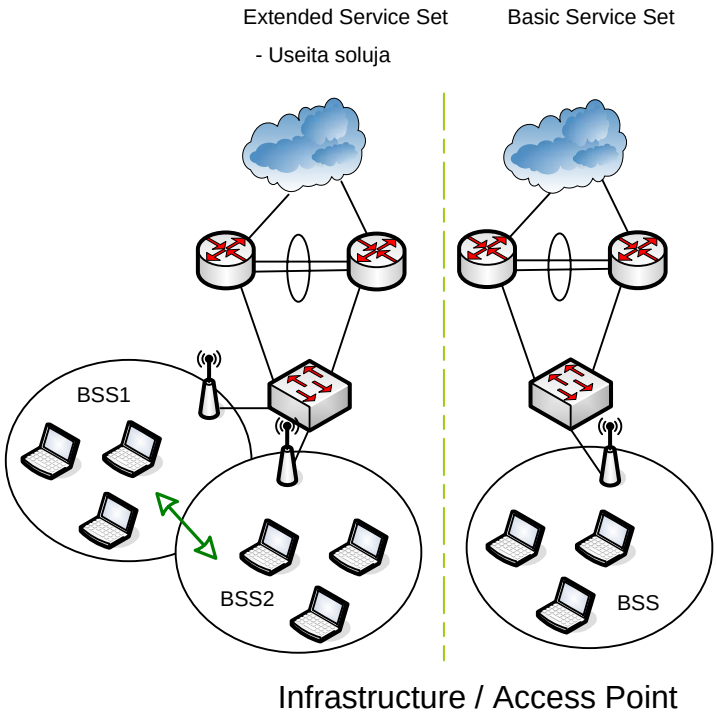
Kuva 3. Ad Hoc -topologia

4.2 Infrastruktuuriverkko (IEEE Computer Society 1999: 25-28)

Infrastruktuuriverkko on kaikkein yleisin langattoman verkon toteutus. Toteutuksessa langaton verkko liitetään osaksi lankaverkkoa tukiaseman avulla. Tukiasema toimii siltana langattoman verkon ja lankaverkon välillä. Tukiasema tarjoaa langattomalle asiakkaalle pääsyn verkon lähi- ja laajaverkkopalveluihin. Asiakkaat käyttävät tukiasemaan määriteltyä kanavaa, bittinopeutta ja SSID-tunnusta (Service Set Identifier).

Infrastruktuuriverkossa pitää olla vähintään yksi tukiasema, jonka kautta PDA-laitteet ovat yhteydessä lankaverkkoon. Yhden tukiaseman verkkoa kutsutaan Basic Service Set (BSS) -verkoksi. Verkko voi koostua myös useammasta tukiasemasta eli solusta. Usean solun verkkoa kutsutaan External Service Set (ESS) -verkoksi. (Kuva 4)

External Service Set (ESS) -verkkoon voidaan implementoida myös roaming-ominaisuus. Roaming-ominaisuus mahdollistaa tukiaseman vaihtamisen yhteyden aikana. Vaihtaminen tukiasemasta toiseen onnistuu, kun topologiaa suunniteltaessa asemat sijoitetaan tarpeeksi lähelle toisiaan. Siirtyminen asemasta toiseen tapahtuu huomaamattomasti, mutta siirtymisen aikana yhteyteen tulee kuitenkin pieni katkos. Roaming-ominaisuudella saadaan verkon toimintasädettä kasvatettua.



Kuva 4. Infrastruktuuri -topologia

4.3 Spanning-tree (virityspuu) -topologia

Verkko voidaan toteuttaa fyysisen topologian osalta siten, että se sisältää useita reittejä samaan aliverkkoon. Useiden reittien käyttö parantaa verkon vikasietoisuutta, mutta samalla verkkoon voi syntyä helposti luuppeja. Tämän takia spanning-tree-protokollan käyttö on välttämätöntä näin toteutetussa verkossa, jotta luupit pystytään havaitsemaan ja luomaan luuppivapaa topologia. Jos verkkosegmentti lakkaa toimimasta spanning-tree-algoritmi laskee topologian uudestaan ja aktivoi seuraavan reitin. (Velte & Velte 2005: 129)

Sillat ja kytkimet lähettävät ja vastaanottavat BPDU-viestejä (Bridge Protocol Data Unit), joiden avulla ne luovat luuppivapaan topologian. Myös langattoman verkon tukiasemat voidaan liittää osaksi spanning-tree-verkkoa, mutta käytettäviltä tukiasemilta vaaditaan spanning-tree-protokollan tuki. Spanning-treetä tukevat laitteet ovat melko kalliita. Ainakin Cisco systems ja Hewlett-Packard valmistaa spanning-tree-tuella varustettuja laitteita.

5 TIETOTURVA

Hakala ja Vainio (2005: 342) esittävät tietoverkon rakentamien kirjassaan, että tietoturvalla pyritään säilyttämään tiedon luottamuksellisuus, eheys ja käytettävyys. Tämä tarkoittaa sitä, että tietojärjestelmiin tallennetut tiedot eivät pääse muuttumaan. Lisäksi tiedon tulee olla saatavilla kohtuullisessa ajassa ja käyttökelpoisessa muodossa. Verkon pääsynvalvonnasta huolehtiminen on tärkeää ja sen avulla varmistetaan tiedon luottamuksellisuuden säilyminen. Pääsynvalvonta kattaa kaikki mekanismit, joiden avulla käyttäjä tunnistetaan ja annetaan oikeudet käyttää sallittuja palveluita.

Tietoturvalla pyritään myös varmistamaan, että tieto säilyy muuttumattomana tietoa siirrettäessä. Salaamista käytetään keinona estää ulkopulista saamasta selville siirrettävän tiedon sisältöä ja näin varmistetaan tiedon pysyminen muuttumattomana. Hakalan ja Vainion (2005: 343) mukaan suojaus tulisi toteuttaa siten, että käyttäjille annetaan oikeudet vain tietoihin, joita käyttäjä tarvitsee. Tietoturvaa suunniteltaessa ja toteuttaessa joudutaan aina tekemään kompromisseja palveluiden käytettävyyden ja uhkatekijöiden välillä.

Langatonta verkkoa koskevat kaikki samat uhat kuin langallista verkkoakin. Langattomassa verkossa tieto liikkuu radioteitä pitkin ja fyysisillä esteillä ei voida täysin rajata verkkoa ulkopuolisilta. Tämä altistaakin verkon uhkiin, jotka eivät lankaverkossa tuota ongelmia. Kuka tahansa voi salakuunnella tai murtautua verkkoon yrityksen tilojen ulkopuolelta käsin ilman, että sitä kukaan edes huomaa. Salakuuntelua onkin erittäin vaikea havaita. Liikenteen salaaminen ja verkkoon pääsyn kontrollointi onkin erittäin tärkeää tietoturvan kannalta.

Langattomanverkon uhat voidaan jakaa karkeasti passiivisiin ja aktiivisiin uhkiin.

Passiiviset uhkat
- salakuuntelu
- liikenteen analysointi

Aktiiviset uhkat
- häirintä
- liikenteen manipulointi
- verkkoon murtautuminen

Langattomaan verkkoon kohdistuvat hyökkäykset

Kuten edellä jo mainittiin, niin langattomat verkot ovat alttiita samoille hyökkäyksille, joita käytetään lankaverkkoon kohdistuvissa hyökkäyksissä. Niiden toteutustapa kuitenkin hieman poikkeaa, koska verkot ovat rakenteeltaan erilaisia. Alla olevia tapoja pidetään yleisimpinä tapoina hyökätä langattomaan verkkoon.

- Man-In-The-Middle (MITM)
- Istunnon kaappaaminen (Session Hijack)
- Paketti manipulointi
- Replay – toistohyökkäys

5.1 Man-In-The-Middle (MITM)

Man-In-The-Middle-hyökkäyksessä hakkeri väärentää verkkoon oman tukiasemansa. Asiakas luulee, että kyseessä on oikea tukiasema ja yhdistää hyökkääjän väärennettyyn tukiasemaan. Hakkeri kaappaa autentikointitiedot asiakkaalta ja kytkeytyy itse aitoon tukiasemaan. Hakkeri osoittaa itsensä asiakkaan ja tukiaseman väliin. Hyökkäyksen onnistuessa hakkeri voi salakuunnella liikennettä tai kaapata istunnon. (Falk 2004: 38)

Tunneloidut EAP-metodit, kuten PEAP ja EAP-TTLS, ovat haavoittuvia Man-In-The-Middle-hyökkäykselle. Hyökkäyksen onnistuminen kuitenkin vaatii, että verkossa käytetään vain yksipuolista tunnistautumista. Toisin sanoen tukiasemaa ei autentikoida asiakkaalle. Kaksipuolisen ja vahvan autentikoinnin käyttäminen estää hyökkäyksen. (Falk 2004: 38)

5.2 Istunnon kaappaaminen (Session Hijack)

Hyökkäystä käytetään käyttäjän istunnon valtaamiseen. Hyökkäystä käytetään usein MITM:n kanssa. Hyökkäyksessä käytetään haaste-vastaus (challenge-response) -protokollaa hyväksi. Hakkeri yhdistää tukiasemaan ja vastaanottaa haasteen. Sitten hyökkääjä tekeytyy tukiasemaksi, jotta saa asiakkaan yhdistämään hyökkääjän koneeseen. Asiakkaan yhdistäessä hyökkääjän koneelle asiakas saa hyökkääjältä saman haasteen, jonka hyökkääjä sai oikealta tukiasemalta. Asiakas salaa haasteen ja lähettää sen hyökkääjälle. Hyökkääjä välittää vastauksen aidolle tukiasemalle ja näin hyökkääjä pääsee verkkoon. Lopuksi hyökkääjä lähettää asiakkaalle log-off-viestin. Kaksipuolinen autentikointi estää myös tämän hyökkäyksen. (Falk 2004: 38)

5.3 Pakettimanipulointi

Pakettimanipulointi tapahtuu siten, että hyökkääjä kappaa lähetetyn paketin ja muuttaa sen sisältöä. Hyökkäys voidaan estää MIC:n (Message Integrity Code) avulla. MIC lasketaan virheiden löytämiseksi paketin datasta ja se estää tietojen muuttumisen tiedonsiirron aikana. (Falk 2004: 38)

5.4 Replay – toistohyökkäys

Hyökkäys tapahtuu kuuntelemalla liikennettä. Hyökkääjä voi kuunnella ja nauhoittaa autentikointi viestien vaihtoa ja myöhemmin toistaa viestit uudestaan. Hyökkääjä yrittää tällä tavoin päästä kirjautumaan verkkoon. (Falk 2004: 39)

Hyökkäys voidaan estää käyttämällä toistolaskinta (replay counter). Laskin on satunnaisesti nouseva ja se lisätään jokaiseen pakettiin. Paketin toistoon hyökkääjän tarvitsee tietää oikea laskimen arvo sekä muuttaa viestin eheyden varmistusarvoa (MIC). (Falk 2004: 39)

6 IEEE 802.11 - TURVALLISUUS

Tiedon turvallinen siirtäminen verkon yli vaatii tietoturvamekanismien käyttöönottoa verkossa. Langattomissa verkoissa tietoturvamekanismien käyttö on välttämätöntä, koska tieto liikkuu vapaasti radiotaajuuksilla. Alun perin langattoman verkon turvataso suunniteltiin lankaverkon tasoa vastaavaksi. Alkuperäinen turvataso on nykyään riittämätön langattoman verkon suojauksessa.

Langattomassa verkossa käytettävä alkuperäinen 802.11 -standardi sisältää yksinkertaisen pääsynhallinta, autentikointi ja liikenteen salausmekanismin. Seuraavassa osiossa perehdytään hieman alkuperäisen standardin turvallisuusominaisuuksiin.

6.1 Pääsynhallinta ja autentikointi

Alkuperäinen 802.11 -standardi määrittelee autentikointiin kaksi eri tekniikkaa avoinjärjestelmä (open system) ja jaettu avain (shared key). Avoinjärjestelmä ei käytännössä sisällä todellista käyttäjä tunnistusta. Asiakas yksinkertaisesti autentikoituu tukiasemalle vain antamalla seuraavat tiedot:

- Tukiaseman SSID (Service Set Identifier).
- Asiakkaan Mac-osoite.

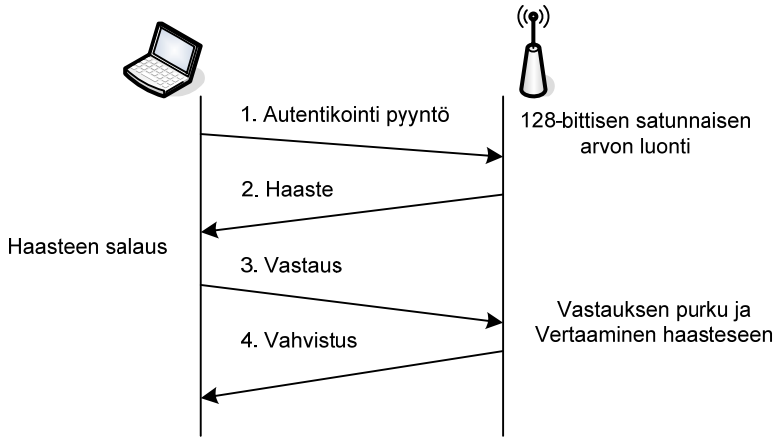
Yleensä SSID-tunnus on helposti arvattavissa, koska SSID-tunnuksena käytetään usein yrityksen nimeä tai muuta helppoa nimeä. Lisäksi tukiasema lähettää oletuksena SSID-tunnuksen majakka (beacon) -viesteissä, ellei sitä ole asetuksista erikseen estetty. Mac-osoite on 48-bittinen heksadesimaaliluku, joka on poltettu WLAN-piirille. Tukiasemaan voidaan määritellä lista sallituista Mac-osoitteista, jolloin vain tietyistä Mac-osoitteista autentikointi sallitaan ja tämä lisäisi näin turvallisuutta. On kuitenkin olemassa ohjelmistoja, joiden avulla voidaan muuttaa laitteen Mac-osoite miksi tahansa.

Avoinjärjestelmä sisältää vain yksisuuntaisen autentikoinnin. Tämä tarkoittaa, että tukiasema ei autentikoidu asiakkaalle lainkaan. Asiakkaan täytyykin luottaa, että todella asioi oikean tukiaseman kanssa.

Jaettuavain autentikointitapa on huomattavasti turvallisempi kuin avointapa. Autentikointi perustuu salaiseen cryptiseen avaimeen. Avaimena käytetään WEP-avainta (Wired Equivalent Privacy). Tämä avain on etukäteen jaettu asiakkaalle ja tukiasemalle. WEP-avainta ei siis koskaan lähetetä verkon yli, vaan avain on aina etukäteen jaettu.

Autentikointimenetelmä käyttää haaste-vastaus -kaavaa. Autentikointi tapahtuu siten, että asiakas lähettää tukiasemalle autentikointi pyynnön. Tukiasema luo satunaisen 128-bittisen arvon ja lähettää sen asiakkaalle haasteena. Asiakas salaa haasteen WEP-avaimen avulla ja lähettää sen takaisin tukiasemalle. Tukiasema purkaa salauksen omalla WEP-avaimellaan ja vertaa sitä lähettämäänsä haasteeseen. Tukiasema sallii pääsyn vain, jos arvot vastaavat toisiaan. Onnistunut autentikointi kuitataan kuittaussanomalla. Autentikoinnin epäonnistuessa tukiasema lähettää syykoodin asiakkaalle. Kuvassa 5 on havainnollistettu autentikoinnin toiminta. (Puska 2005: 74)

Salattu avain autentikointi luokitellaan kuitenkin heikoksi, koska tämäkin autentikointitapa on yksisuuntainen. Edelleen tukiasemaa ei autentikoida asiakkaalle. Lisäksi haaste-vastaus -kaava on jo pitkään luokiteltu heikoksi, jos sen käyttöä ei ole suunniteltu huolellisesti ja käytetyt avaimet eivät ole tarpeeksi pitkiä. (Frankel, Eydt, Owens & Kent 2006: 3-4)



Kuva 5. *Salattuavain autentikointi* (Puska 2005: 75)

6.2 Liikenteen salaus

IEEE 802.11 -standardissa WEP-protokollaa käytetään liikenteen salaamisessa asiakkaan ja tukiaseman välillä. WEP on siirtoyhteyskerroksen salausmenetelmä ja se toimii Mac-alikerroksella. WEP pohjautuu RC4-algoritmiin. Salausavaimena käytettään 40-bittistä WEP-avainta, jonka lisäksi siihen lisätään 24-bittinen alustusvektori (Initialization Vector). (Frankel ym. 2006: 3-4)

Useimmat WEP-protokollaa kohtaan tunnetut hyökkäykset perustuvat alustusvektorissa oleviin heikkouksiin. Matti Puska (2005:75) toteaakin teoksessaan, että WEP-salaus on helposti murrettavissa nykyaikaisilla koneilla ja netistä saavilla olevilla ohjelmistoilla. Kuitenkin se tarjoaa kohtuullisen turvan, kun verkon palveluita rajoitetaan myös muilla tavoin.

6.3 Tiedon eheys (Frankel ym. 2006: 3-5)

802.11 -standardiin sisällytettyä WEP-protokollaa käytetään myös tiedoneheyden varmistamiseen. WEP on suunniteltu hylkäämään kaikki lähetyksen aikana muuttuneet paketit. Tämän varmistamiseksi WEP sisältää yksinkertaisen 32-bittisen tarkistusmekanismin (CRC-32, Cyclic Redundancy Check) – tarkastussumman.

Tarkastussumma lasketaan hyötykuormasta. Hyötykuorma ja tarkastussumma salataan RC4-avaimella ja ne lisätään Mac-kehykseen. Vastaanottaja purkaa vastaanotetun kehyksen ja uudelleen muodostaa tarkastussumman vastaanotetusta hyötykuormasta. Vastaanottaja vertaa sitä vastaanotetun tarkastussumman kanssa. Tarkastussummien täytyy vastata toisiaan tai kehys hylätään.

7 THE WI-FI PROTECTED ACCESS FRAMEWORK (WPA)

Tässä työssä en käsittele WPA-turvatekniikkaa kovin tarkasti, koska se pohjautuu hyvin pitkälti työssä myöhemmin käsiteltävään 802.11i -tietoturvastandardiin, jota käsittelen tarkemmin.

Alkuperäisestä 802.11 -standardin sisältämästä WEP-protokollasta löydettyjen haavoittuvuuksien jälkeen perustettiin 802.11i -työryhmä. Työryhmän tavoite oli kehittää keinot, joilla parannetaan WLANin turvallisuutta. Ennen lopullisen 802.11i -standardin julkaisua siitä julkaistiin esiversio nimeltään WPA (Wi-FI Protected Access). WPA-protokolla perustuu varhaiseen 802.11i:n luonnokseen.

WPA-turvatekniikka tuo uusina ominaisuuksina 802.1x -todennustekniikan ja EAP-protokollan autentikointiprosessiin. Liikenne salataan edelleen WEP-protokollalla mutta siihen on lisätty TKIP (Temporal Key Integrity Protocol), joka kehitettiin erityisesti WPA:ta varten paikkaamaan WEP-protokollassa olleet ongelmat. WPA-protokolla ei ole enää täysin turvallinen, koska siitä on löydetty haavoittuvuuksia. (Falk 2004: 25)

TKIP:n tuomat parannukset WEP-salaukseen: (Puska 2005: 83)

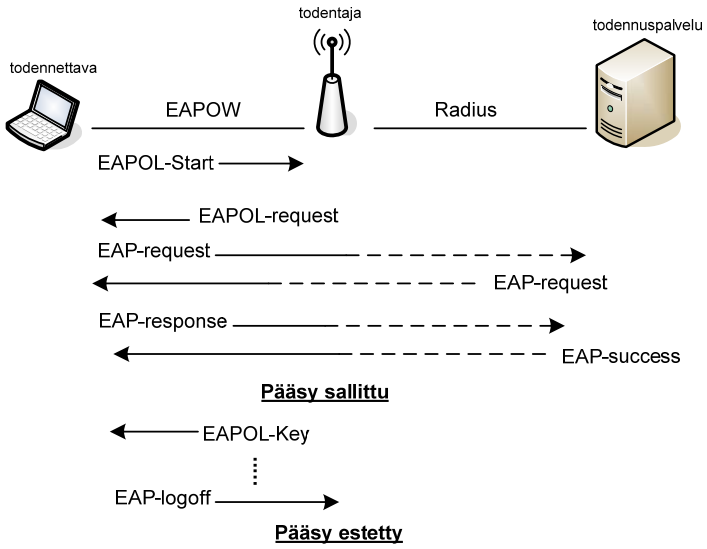
- 128-bitin kehyskohtaiset dynaamiset salausavaimet
- alustusvektori kasvanut 48-bittiseksi
- levitysviestien salausavainta vaihdetaan määräajoin
- viestien eheyden tarkistuksessa käytetään MIC (Message Integrity Check) -toimintoa

8 IEEE 802.1X

IEEE 802.1x -standardi määrittelee laajennettavan todennustekniikan 802 -standardeihin perustuviin verkkoihin. Standardin tarkoituksena on tarjota verkkolaitteen tietoliikenneporttiin kytkeytyvän asiakkaan todentaminen ennen liikenteen sallimista. Standardi perustuu EAP(Extensible Authentication Prtocol) – protokollaan, joka on kuvattu IETF RFC 3748:ssa. EAP-protokollaa käytetään todennettavan ja todentajan välisessä kommunikoinnissa. EAP ei ole tunnistusmenetelmä, vaan sitä käytetään tunnistusmenetelmien alustana. EAP-protokollaa voidaankin käyttää useiden erilaisten autentikointimenetelmien kanssa.

802.1x koostuu todennettavasta, todentajasta ja todennuspalvelusta. Langattomassa lähiverkossa asiakas (todennettava) ja tukiasema (todentaja) käyttävät EAPOW-protokollaa (EAP Over Wireless) kommunikoinnissa. Tukiasema ja autentikointipalvelin (todennuspalvelu) käyttävät kommunikoinnissa jotakin todennusprotokollaa. 802.1x -standardi ei määrittele käytettäväksi mitään tiettyä todennusprotokollaa, mutta Radius-protokolla on yleisimmin käytetty. ([B] IEEE Computer Society 2004: 30-35)

Porttikohtainen pääsynhallinta toteutetaan kuljetuskerroksen Mac-alikerroksella. Pääsynhallinta toimii langattomassa verkossa siten, että tukiasema kontrolloi liikennettä jakamalla yhteyden kahteen virtuaaliseen porttiin kontrolloituun ja kontrolloimattomaan. Kontrolloimatonta porttia käytetään vain autentikointiin ja portista sallitaan vain autentikointi liikenne EAP-viesteillä. Kontrolloitu portti aukeaa vasta onnistuneen autentikoinnin jälkeen ja portista sallitaan normaali liikennöinnöinti. Kuva 6 havainnollistaa 802.1x autentikointi prosessin. ([B] IEEE Computer Society 2004: 12-13)



Kuva 6. 802.1x autentikointi prosessi

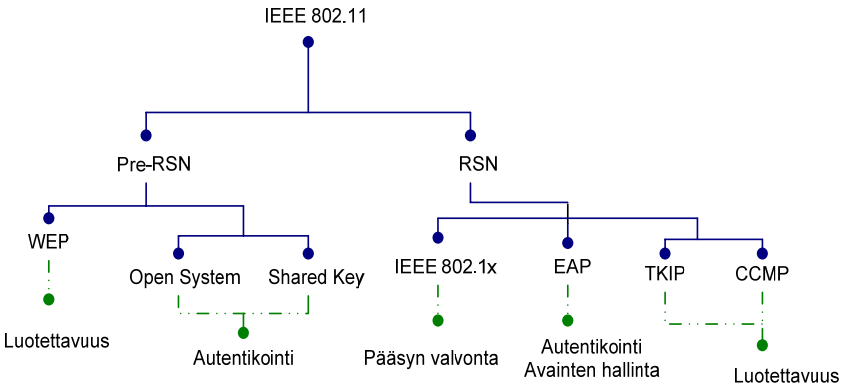
9 IEEE 802.11I

IEEE 802.11i on parannus 802.11 -standardin tietoturvaominaisuuksiin. 802.11i tunnetaan myös nimellä WPA2. Standardi täsmentää tietoturvamekanismeja langattomissa lähiverkko toteutuksissa. 802.11i -prototyyppi ratifioitiin kesäkuussa 2004. Ennen 802.11i:tä julkaistiin tässä raportissa aiemmin mainittu WPA alkuperäisen standardin sisältämien tieturvapuutteiden paikkaamiseksi.

IEEE 802.11i spesifikaatio korvaa alkuperäisen 802.11 -standardin sisältämät turvallisuus ja autentikointi määrittelyt. Spesifikaation keskeisin käsite on RSN (Robust Security Network). Käsite kuvaa joukon tietoturvapolitiikkoja ja avaimia, joita käytetään tiedon turvaamiseksi. RSN on määritelty standardissa langattomaksi turvaverkoksi, joka sallii vain RSNA-yhteyksien (Robust Security Network Assosiations) luomisen.

9.1 Robust Security Network

IEEE 802.11i kuvaa langattomiin verkkoihin kaksi turvallisuusluokkaa Pre-RSN ja RSN. Pre-RSN luokka tarjoaa alkuperäiseen 802.11 -standardiin kehitetyt puutteelliseksi todetut turvallisuusominaisuudet. RSN-luokka tarjoaa langattoman verkon suojaamiseen joukon uusia tekniikoita. Pääsynhallinta toteutetaan 802.1x-tekniikan avulla ja autentikointi tiedot välitetään EAP-protokollan avulla. Tiedon luotettavuuden ja eheyden varmistaa TKIP ja CCMP -protokollat. Kuvaan 7 on koottu 802.11-verkoissa käytetyt tietoturvan parantamista lisäävät protokollat. (Frankel ym. 2006: 4-1)



Kuva 7. *Kaavio turvallisuusprotokollista* (Frankel ym. 2006: 4-1)

802.11 -standardiin kehitetyt turvallisuus määritykset toteutuvat vain siirtoyhteyskerroksella turvaten liikenteen langattomien yhteyspisteiden välillä (Frankel ym. 2006: 4-2). Se ei näin ollen turvaa liikennettä liikenteen siirtyessä lankaverkon puolelle. Niin sanotun End-to-End turvallisuuden takaamiseksi täytyy käyttää muita OSI-mallin ylemmällä kerroksella toteutettuja turvallisuusmekanismeja.

RSNA–turvayhteys

Turvallisuusyhteys määritellään 802.11i -standardissa yhteydeksi, joka koostuu politiikoista ja avaimista, joita käytetään tiedon turvaamisessa. Tukiasema mainostaa politiikkoja ja avaimia majakka- ja vastaussanomien kehyksissä. Kehykset sisältävät RSN informaatioelementin, jossa on määritelty kaikki tukiaseman tukemat politiikat ja suojaus metodit.

RSNA-yhteydellä on 5 eri tilaa infrastruktuuriverkossa. Kuva 8 esittää nämä vaiheet. (Frankel 2006: 5-5)

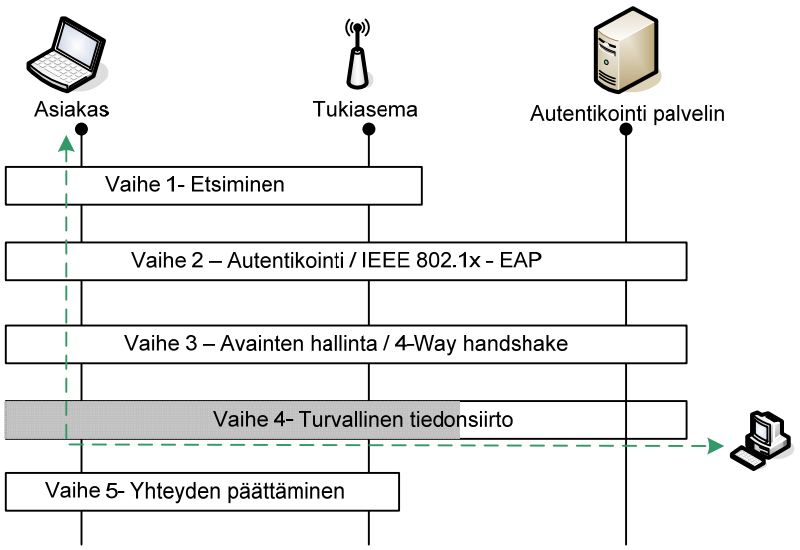
Tila 1: Etsiminen
Tukiasema mainostaa IEE 802.11i -turvallisuuspolitiikkaa majakka (beacon) ja vastaussanomilla (Probe Response). Asiakas tunnistaa oikean tukiaseman sanomien sisältämän SSID-tunnuksen perusteella ja assosioi tukiaseman kanssa. Osapuolet neuvottelevat suojauspaketin (cipher suite) ja autentikointi mekanismin majakka- ja vastaussanomien sisältämien vaihtoehtojen mukaan.

Tila 2: Autentikointi – IEEE 802.1x/EAP
Autentikointi vaiheessa osapuolet tunnistautuvat. Tukiasema tässä tilassa estää normaalin liikenteen asiakkaalta kunnes autentikointi onnistuu.

Tila 3: Avainten luonti ja välitys – 4-Way Handshake
Tukiasema ja asiakas suorittavat useita toimintoja salausavainten luomiseksi ja asentamiseksi.

Tila 4: Turvallinen liikennöinti
Tilassa 4 asiakas liikennöi normaalisti tukiaseman kautta. Liikenne on suojattu tukiaseman ja asiakkaan välillä.

Tila 5: Yhteyden päättäminen
Turvallinen yhteys puretaan osapuolten väliltä ja yhteys palautuu alkutilaan.



Kuva 8. *RSNA-yhteyden vaiheet*
(Frankel ym. 2006: 5-6)

9.2 Avaintenhallinta

802.11i -standardi sisältää kaksi avaintenhallintamekanismia. pariavaintenhallintamekanismi (Pairwese Key Hierarky) on tarkoitettu unicast-liikenteen suojaamiseen. Ryhmäavaintenhallintamekanismilla (Group Key Hierarky) suojataan multicast/broadcast-liikenne (Frankel 2006: 4-4). Avaintenhallinta tapahtuu 802.1x porttikohtaisen autentikoinnin yhteydessä ja avaintenhallinta liikenteessä käytettään EAPOL-Key-kehyksiä.

9.2.1 Pariavainten hierarkia (Frankel ym. 2006: 4-6,7)

Avainhierarkian päällimmäistä avainta kutsutaan PMK-avaimeksi (Pair Master Key). Avainta käytetään luottamuksellisuuden ja eheyden takaamiseen vaadittavien avainten luomiseksi. Yhteyspisteet voivat saada PMK-avaimen kahdella tavalla.

- Pre-Shared Key (PSK)
  - PSK-avain on staattisesti jaettu tukiasemalle ja asiakkaalle ja se täytyy olla molemmilla osapuolilla hallussa ennen yhteyden muodostamista. IEEE 802.11 -standardi ei täsmennä kuinka avaimet jaetaan osapuolille.

- Authentication, Authorization and Accounting Key (AAAK)
  - Avain tunnetaan myös nimellä Master Session Key (MSK). Avain välitetään osapuolille EAP-protokollan mukana RSNA-turvayhteyden muodostuksen yhteydessä. Avain vaihdetaan aina asiakkaan autentikoinnin yhteydessä.

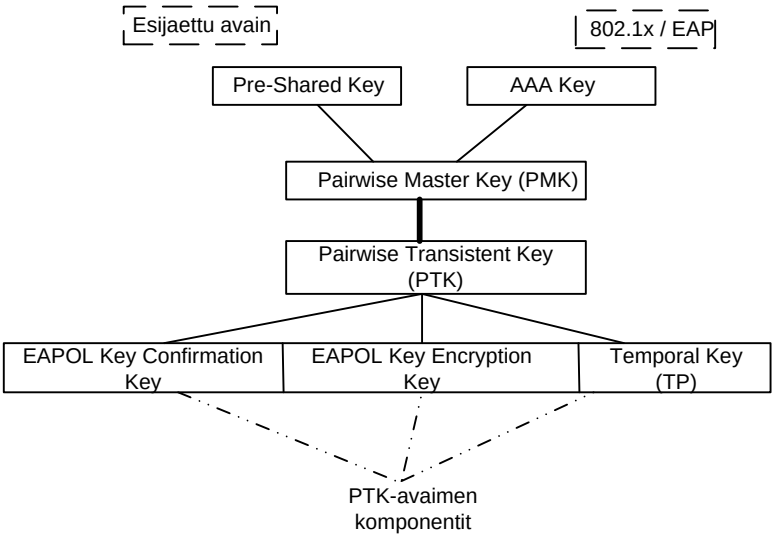
PMK-avain on tukiaseman ja asiakkaan hallussa, mutta avainta ei kuitenkaan käytetä liikenteen suojaamiseen vaan osapuolet muodostavat siitä PTK-avaimen (Pairwise Transistent Key). 4-Way Handshake -kättelyä osapuolet käyttävät PMK-avaimen varmistamiseen ja muodostavat kättelyn yhteydessä PTK-avaimen. Kuva 9 esittää pariavainten hierarkian.

PTK rakentuu seuraavista avaimista.

- EAPOL Key Confirmation Key (EAPOL-KCK)
  Avaimella varmistetaan asiakkaan lähettämien kontrollikehysten eheys ja alkuperä.

- EAPOL Key Encryption Key (EAPOL-KEK)
  Käytetään avainten ja tiedon luottamuksellisuuden turvaamiseen joissakin RSNA-vaiheissa.

- Temporal Key (TK)
  Käytetään asiakkaan liikenteen turvaamiseen.



Kuva 9. *Pariavainten hierarkia* (Frankel ym. 2006: 4-4)

9.2.2 Ryhmäavainten hierarkia

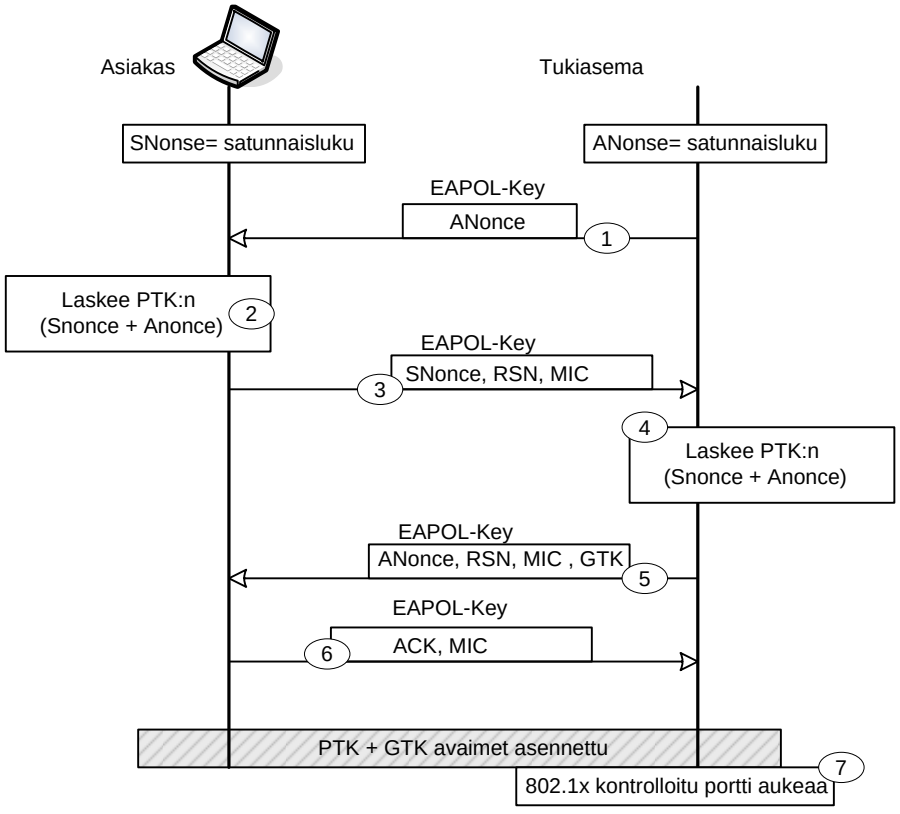
Ryhmäavainhierarkia muodostuu yhdestä Group Temporal Key (GTK) –avaimesta. Tämän avaimen luo tukiasema, joka jakelee avaimen kaikille tukiasemaan yhteydessä oleville asiakkaille. Avain vaihtuu tietyn lyhyen ajan kuluttua sekä aina, kun joku yhteydessä oleva asiakas poistuu verkosta. Ryhmäavain välitetään

asiakkaille 4-Way Handshake –kättelyn yhteydessä ja avaimen uusimiseen käytetään kaksiosaista kättelyä (Group Handshake).

9.2.3 Avainten luonti ja välitys (Frankel ym. 2006: 5-18)

4-Way Handshake -kättelyä käytetään 802.11i -standardissa liikenteen salaamisessa käytettävien avainten luomiseen ja välittämiseen. Kättely on RSNA-turvayhteyden muodostamisen viimeinen vaihe ja sen avulla tukiasema ja asiakas luovat tarvittavat avaimet, joiden avulla turvallinen tiedonsiirto on mahdollista.

Kättelyn aikana tukiasema ja asiakas vahvistavat PMK-avaimen olemassaolon ja luovat liikenteen salaamisessa käytettävät PTK-avaimet. Lisäksi kättelyn yhteydessä tukiasema välittää asiakkaalle ryhmäavaimen (GTK). Onnistuneen kättelyn jälkeen tukiasema ja asiakas ovat autentikoituneet toisilleen onnistuneesti. Tämän jälkeen 802.1x kontrolloituportti aukeaa ja normaali dataliikenne sallitaan. Kuva 10 havainnollistaa 4-Way handshake -kättelyn vaiheet.



Kuva 10. 4-Way handshake -kättelyn vaiheet
(Frankel ym. 2006: 5-19)

1. Tukiasema lähettää EAPOL-key kehyksen, joka sisältää satunnaisen bittiluvun (ANonce).
2. Asiakas muodostaa PTK:n SNonce ja ANonce arvoista.

3. Asiakas lähettää EAPOL-key kehyksessä SNonce arvon, RSN informaatio elementin ja MIC:n.
4. Tukiasema muodostaa PTK:n ANonce ja SNonce arvoista.
5. Tukiasema lähettää EAPOL-key kehyksessä GTK-avaimen ja ilmoituksen tilapäisenavaimen asennuksen onnistumisesta.
6. Asiakas lähettää vahvistuksen avaimen asennuksesta.
7. 802.1x kontrolloitu portti aukeaa.

([A] IEEE Computer Society 2004:90)

9.3 Tiedon luottamuksellisuus ja eheys protokollat

Standardi määrittelee luottamuksellisuuden ja eheyden turvaamiseksi kaksi protokollaa Temporal Key Integrity Protocol (TKIP) ja Counter Mode with Cipher Blok Chaining MAC Protocol (CCMP). TKIP-protokolla on sisällytetty vanhojen Pre-RSN laitteiden yhteensopivuuden säilyttämiseksi ja TKIP-protokolla on suora parannus WEP-protokollaan. TKIP-protokolla saadaan vanhoissa laitteissa ohjelmistopäivityksen avulla käyttöön. Sen käyttäminen on valinnaista eikä protokollan käyttöä suositella sen sisältämien haavoittuvuuksia takia.

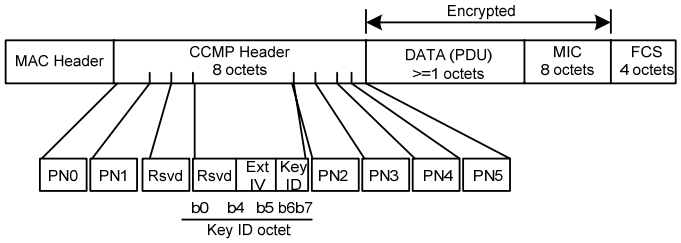
CCMP

CCMP on täysin uusi luottamuksellisuuden ja eheyden takaamiseksi määritelty tekniikka. RSNA-yhteyden suojaamiseksi osapuolet voivat neuvotella tämän uuden suojauspaketin (cipher suite). CCMP suunniteltiin pitkän aikavälin ratkaisuksi, jossa huomioitiin kaikki WEP-protokollan heikkoudet. CCMP:tä ei kuitenkaan suunniteltu käytettäväksi olemassa olevilla laitteilla ja tämän takia vanhat laitteet eivät toimi CCMP:n kanssa. 802.11i -standardi määrittelee RSN-turvallisuus luokassa CCMP:n pakolliseksi salausstandardiksi.

CCMP perustuu AES-salausalgoritmin CCM-tekniikkaan. CCM yhdistää kaksi tunnettua salaustekniikkaa järeän suojauksen toteuttamiseksi. Counter Mode (CTR) luottamuksellisuuden ja Cipher Block Chaining MAC (CBC-MAC) autentikointiin sekä eheyden suojaamiseen. CCMP suojaa koko kehyksen ja paketin eheyden.

CCMP MPDU

Kuten kuvasta 11 voidaan huomata, CCMP-prosessointi laajentaa alkuperäistä MPDU:ta (MAC Protocol Data Unit) 16. oktetilla. 8 oktettia käytetään CCMP-otsikkokenttään ja 8 oktettia MIC-kenttään. CCMP-otsikko muodostuu PN, ExtIV ja KeyID alikentistä. PN eli pakettinumero muodostuu 6 oktetin sarjasta. Sarjan merkittävin oktetti on sarjan suurin. KeyID-oktetin alikenttä (ExtIV) osoittaa, että CCMP-otsikko suurentaa MPDU-otsikkoa kokonaisuudessaan 8 oktetilla. CCMP:ssä ExtIV bitti asetetaan aina numero yhdeksi. *([A]* IEEE Computer Society *2004:57)*



Kuva 11. CCMP MPDU ([A] IEEE Computer Society 2004:58)

CCMP-kapselointi

CCMP-kapselointiprosessi luo MPDU-data ja MAC-otsikko kentistä salatun viestin (cipher text). Kapselointiprosessin päävaiheet ovat seuraavat: (kuva 12) ([A] IEEE Computer Society *2004: 58*)

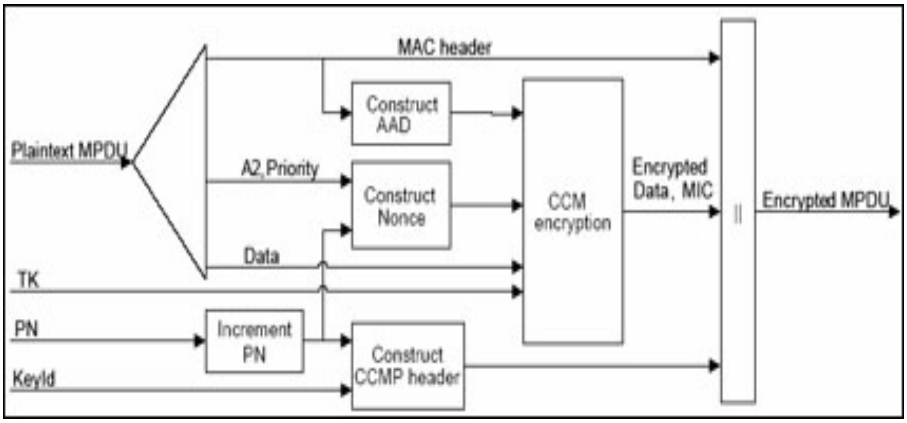
1. Pakettinumeroa (PN) kasvatetaan, jotta saadaan jokaiselle MPDU:lle uusi pakettinumero. Jokaiselle pakettinumerolle käytetään omaa väliaikaista avainta.

2. Kehyksen otsikolle muodostetaan AAD (Additional Authetication Data). CCM tarjoaa aitouden suojauksen AAD kentälle.

3. CCM muodostaa once-lohkon pakettinumerosta (PN), MPDU-osoitteesta (A2) ja prioriteetti kentästä. Prioriteetti kentän arvo on asetettu nollaksi.

4. Avaintunniste (Key ID) ja uusi pakettinumero (PN) asetetaan CCMP-otsikkoon.

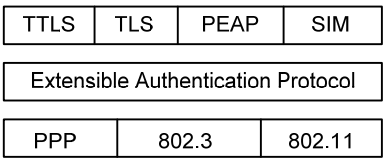
5. Väliaikaisen avaimen, AAD, once-lohkon ja MPDU-datan avulla muodostetaan salattuviesti (cipher text).



Kuva 12. CCM-kapselointi
([A] IEEE Computer Society 2004: 58)

10 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

EAP-protokolla toimii kuljetusalustana eri tunnistus toteutuksille. EAP kehitettiin alun perin PPP-yhteyksille, mutta nykyään sitä käytetään myös 802.3 -ethernet verkoissa ja 802.11 -langattomissa verkoissa. EAP-autentikointi voi perustua salasanoihin, sertifikaatteihin ja älykortteihin tai näiden yhdistelmiin. Erilaisia tunnistus toteutuksia, joita voidaan käyttää EAP-protokollan kanssa, on useita erilaisia. Langattomissa verkoissa käytettäviksi tekniikoiksi on vakiintunut 4 eri tekniikkaa. Tekniikat on esitetty kuvassa 13. (Frankel ym. 2006: 6-1)



Kuva 13. EAP-metodit

Langattomassa verkossa EAP-protokollaa käytetään autentikointivaiheessa, kun tukiaseman ja asiakkaan välille muodostetaan RSNA-turvayhteys. EAP-metodeita käytetään autentikointi tapahtumassa ja avain materiaalin luomisessa. EAP-metodit tukevat useita eri autentikointimenetelmiä. Autentikointi on 802.11i -standardissa määritelty tukiaseman ja asiakkaan välillä kahdensuuntaiseksi, mutta sen ei tarvitse olla symmetristä. Esimerkiksi tukiasema voi autentikoitua asiakkaalle sertifikaatilla ja asiakas autentikoituu käyttäjätunnus/salasana -yhdistelmää käyttäen.

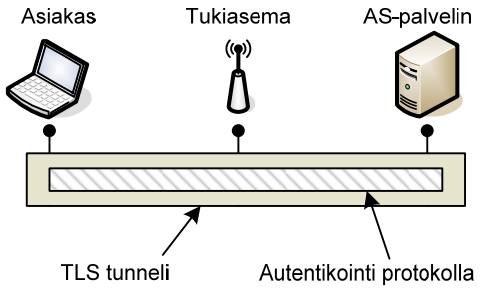
EAP-autentikointia voidaan käyttää monissa eri käyttöympäristöissä ja käytettäviä EAP-metodeita on useita erilaisia. EAP-autentikoinnin käyttö langattomassa verkossa asettaa omat vaatimukset käytettäville tunnistusmenetelmille turvallisen autentikointi tapahtuman takaamiseksi. RFC 4017 asiakirjassa on kuvattu vaatimukset langattomassa verkossa käytettäville tunnistusmenetelmille. Käytettävien EAP-metodien pitää täyttää seuraavat vaatimukset: (IETF 2005: 3)

- Metodien pitää pystyä luomaan symmetrisiä avaimia.
- Luotavien avainten pitää olla vähintään 128-bittisiä.
- Metodien pitää tukea 2-puolista autentikointia.
- Jaetun EAP-metodin tilan tulee olla molemmilla osapuolilla samanlainen, kun se on onnistuneesti jaettu.
- Metodien täytyy suojata MITM ja Dictionary hyökkäyksiä vastaan.

10.1 TLS pohjaiset EAP-metodit

Langattomassa verkossa käytettävät EAP-metodit perustuvat TLS (Transport Layer Security) -laillisuustarkastusmenetelmään. TLS takaa yksityisyydensuojan ja tiedoneheyden asiakkaan sekä autentikointipalvelimen välillä.

Osapuolten välille muodostetaan TLS-kättelyn yhteydessä TLS-tunneli, jonka sisällä jonkin autentikointi protokollan avulla osapuolet autentikoituvat turvallisesti (kuva 14). Tunnistus voidaan suorittaa digitaalisten sertifikaattien tai käyttäjätunnus/salasana -yhdistelmän avulla. Autentikointipalvelin kuitenkin yleensä aina tunnustautuu asiakkaalle sertifikaatin avulla, mutta käyttäjä voi tunnustautua riippuen käytettävästä protokollasta, joko käyttäjätunnus/salasana yhdistelmällä tai digitaalisella sertifikaatilla.



Kuva 14. TLS-tunneli

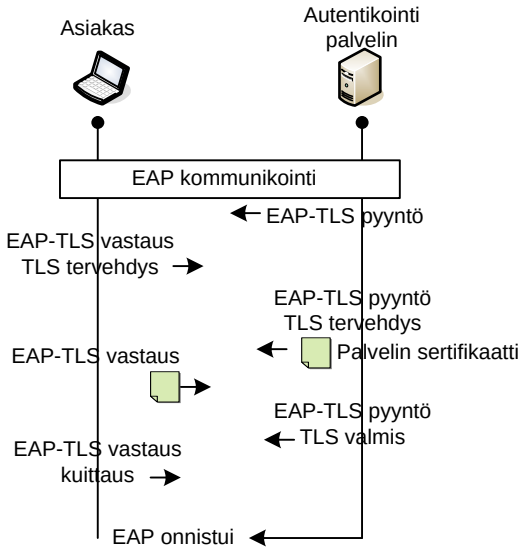
NIST:in raportissa mainitaan yleisimmin käytössä oleviksi TLS pohjaisiksi EAP-metodeiksi alla olevat neljä metodia (Frankel ym. 2006: 6-6).

- EAP-TLS
- EAP tunneled TLS (EAP-TTLS)
- Protected EAP (PEAP)
- EAP Flexible Authentication via Secure Tunneling (EAP-FAST)

10.2 EAP-TLS

EAP-TLS on kaikkein turvallisin EAP-metodi. Tekniikka perustuu vahvaan kahdensuuntaiseen autentikointiin. Asiakas ja autentikointipalvelin käyttävät autentikointiin sertifikaatti varmenteita. Laitteilla on hallussa uniikit X.509 sertifikaatit, jotka verkon varmenneviranomainen (Certification Authotory) on jakanut. Sertifikaattien jakelu ja ylläpito vaatii PKI-järjestelmän (Public Key Infrastructure) perustamista verkkoon.

Asiakkaan ja autentikointipalvelimen välille muodostetaan salattu TLS-yhteys, jonka sisällä osapuolet todentavat toisensa sertifikaatti varmenteiden avulla. TLS-protokollan sisältämää TLS-kättelyä osapuolet käyttävät salatun TLS-yhteyden muodostamiseen ja toisensa todentamiseen (kuva 15). TLS-yhteyttä ei kättelyn päätyttyä käytetä muuhun tietoliikenteeseen.



Kuva 15. EAP-TLS -kättely

NIST:n raportin mukaan EAP-TLS-metodin käyttö voi aiheuttaa ongelmia paljon laitteita sisältävissä verkoissa. EAP-TLS autentikointiprosessi sisältää enemmän vaiheita kuin muut TLS pohjaiset autentikointimetodit, jolloin autentikointi on hitaampaa. (Frankel ym. 2006: 6-7)

10.3 EAP-TTLS

EAP-TTLS on laajennus raportissa aiemmin esiteltyyn EAP-TLS metodiin. EAP-TTLS laajentaa kahdensuuntaisen symmetrisen autentikoinnin käytettäväksi myös autentikointi yhdistelmien kanssa.

EAP-TTLS toimii siten, että autentikointipalvelin tunnistautuu TLS-kättelyn yhteydessä sertifikaatti varmenteella asiakkaalle. Samalla osapuolten välille muodostuu salattu TLS-tunneli. Salatuntunnelin sisällä asiakas tunnistautuu autentikointipalvelimelle jokin autentikointiprotokollan avulla. EAP-TTLS sallii yleisten autentikointi protokollien tunneloinnin, kuten esimerkiksi yleisten salasanaprotokollien (CHAP, PAP, MSCHAP, MSCHAPv2).

10.4 PEAP

PEAP-protokollan on kehittänyt yhteistyössä Microsoft, Cisco Systems ja RSA Security. PEAP toimii hyvin samanlailla kuin EAP-TTLS. Autentikointipalvelin tunnistautuu sertifikaatti varmenteella asiakkaalle ja salatuntunnelin sisällä asiakas autentikoituu PEAP-metodilla. PEAP ei vaadi asiakkaalta sertifikaattia, mutta pakollisena turvallisuusvaatimuksena jokainen asiakas pitää varustaa juurisertifikaatilla (Frankel ym. 2006: 6-9).

10.5 EAP-FAST

EAP-FAST on Cisco Systemsin kehittämä metodi. EAP-FAST toimii PEAP-metodin tavoin kahden vaiheen kautta. Ensimmäisessä vaiheessa osapuolten väliin luodaan salattutunneli ja toisessa vaiheessa asiakas tunnistautuu salatuntunnelin sisällä.

EAP-FAST-metodi ei tarvitse muista TLS pohjaisista metodeista poiketen sertifikaatti varmenteita kummaltakaan osapuolelta. EAP-FAST perustuu PAC (Protected Access Crendentials) esijaettuun avaimeen. Salattutunneli muodostetaan PAC-avaimen avulla. Tunnelin muodostamisen jälkeen asiakas tunnistautuu tunnelin sisällä jollakin sisäisellä EAP-metodilla.

11 CASE ICM FINLAND

ICM Finland Oy:ssä aloitettiin keväällä projekti, jonka tarkoituksena oli parantaa tietoverkon toiminnallisuutta ja tietoturvaa. Projektin päävastuu annettiin hoidettavakseni. Projektin tavoitteena oli nykyisen tietoverkon kehittäminen niin, että se vastaa tämän päivän vaatimuksia.

Tehtävä oli varsin haasteellinen ottaen huomioon lähtötilanteen projektin alussa. Verkossa oli kaksi palvelinta, joissa molemmissa oli Windows 2000 Server käyttöjärjestelmät. Molemmat palvelimet olivat omissa toimialueissa ja palvelimet toimivat niissä ohjauspalvelimina. Henkilökunnan tietokoneista vain osa kuului toimialueeseen. Verkon reunalla reitittimenä ja DHCP-palvelimena toimi ADSL-modeemi.

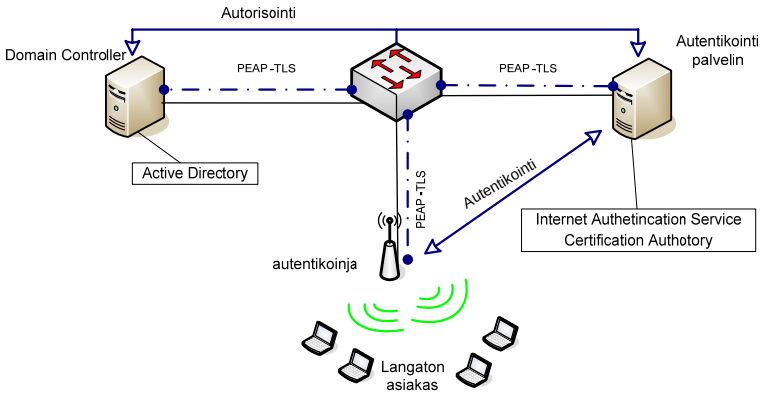
Verkon nykytilan kartoituksen jälkeen alettiin miettiä mitä palveluita ja toimintoja verkolta halutaan. Verkkoon päätettiin laittaa vain yksi ohjauspalvelin ja palvelimeen hankittiin käyttöjärjestelmäksi Windows 2003 R2. Palvelimelle siirrettiin ADSL-modeemin toiminnot ja ADSL-modeemi muutettiin sillaksi. Palvelimelle asennettiin lisäksi nimipalvelu reititys- ja DHCP-palveluiden lisäksi. Verkon toiselta palvelimelta purettiin Active Directory ja se siirrettiin osaksi uutta toimialuetta. Kaikki henkilöstön koneet liitettiin uuteen toimialueeseen. Lisäksi Active Directory -hakemistopalvelu suunniteltiin uudelleen.

Kun verkon perustukset oli saatu asennettua ja toimintakuntoon oli aika miettiä langattoman verkon toimintaa. Alun perin verkossa oli yksi WLAN-tukiasema, jossa oli käytössä WPA-suojaustekniikka. Tukiasemaan autentikoitiin esijaetun avaimen tekniikalla. Kaikki langatonta verkkoa käyttävät käyttivät siis samaa salaista avainta. Esijaetun avaimen käyttö ei sovellu hyvin usean käyttäjän verkkoon ja avaimen vaihtaminen on hankalaa, koska uusi avain täytyy asentaa jokaiselle koneelle uudestaan. Tekniikan käyttö ei ole myöskään tietoturvan kannalta suotavaa. Niinpä verkkoon päätettiin hankkia toinen tukiasema ja tietotuvallisuutta päätettiin lähteä parantamaan.

Verkkoon otettiin käyttöön IEEE 802.11i -tietoturvastandardin mukaiset tietoturvallisuutta parantavat ominaisuudet. IEEE 802.11i edellyttää verkolta tiettyjä ominaisuuksia ja laitteita, jotta se voidaan ottaa käyttöön. Verkolta vaaditaan seuraavat ominaisuudet:

- Tukiasema, jossa tuki 802.1x protokollalle
- Autentikointipalvelin
- Sertifikaattipalvelin

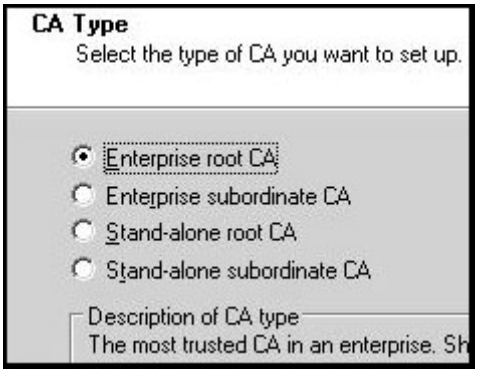
Näiden vaatimusten pohjalta tukiasemaksi hankittiin Linksys WRT54G tukiasema. Autentikointi ja sertifikaatti palvelimena käytetään Windows 2003 R2 palvelinta. Windows 2003 R2:sta löytyy IAS-palvelu, jota voidaan käyttää autentikointiin sekä Certificate Authority –palvelu, jolla saadaan luotua tarvittavat sertifikaatit. Kuva 16 havainnollistaa verkon toiminnan. Verkossa käytetään PEAP-protokollaa asiakkaiden autentikointiin. PEAP-protokollan avulla käyttäjät voivat käyttää verkkoon autentikoituessaan Windows -verkon käyttäjätunnusta ja salasanaa. Autentikointipalvelin tarkistaa käyttäjän antaman salasanan ja käyttäjätunnuksen suoraan Active Directorystä. Autentikointipalvelin tässä ratkaisussa autentikoituu asiakkaalle digitaalisella sertifikaatilla, jonka yhteydessä tukiaseman ja asiakkaan väliin muodostuu salattu TLS-tunneli. Tunnelin sisällä asiakas autentikoituu PEAP-protokollan avulla turvallisesti.



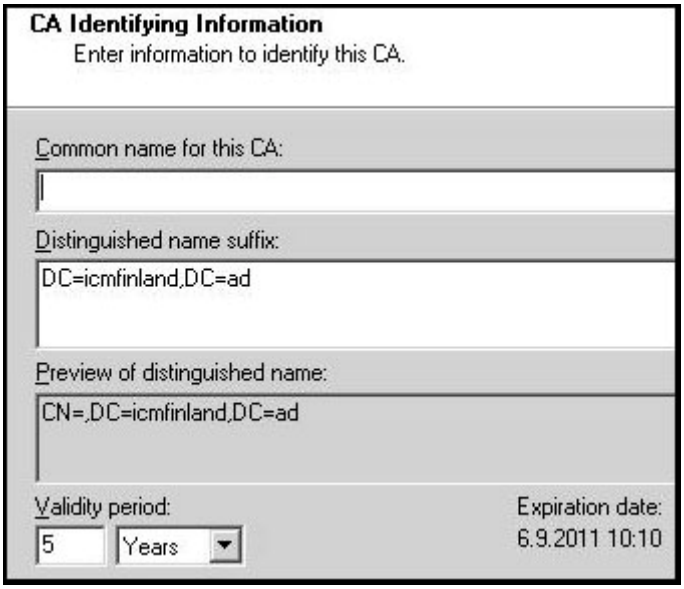
Kuva 16. Verkon rakenne

11.1 Public Key Infrastructure

PEAP-protokollan käyttö vaatii digitaalisen sertifikaatin käyttöä. Näin ollen sertifikaatti täytyy asentaa IAS-palvelimelle autentikoinnin onnistumiseksi. Sertifikaatin käyttö vaatii PKI – infrastruktuurin (Public Key Infrastructure) luomista. Windows-verkossa Certification Authotory –palvelu jakelee sertifikaatit toimialueen laitteille. CA –palvelun asennuksen yhteydessä luodaan sertifikaattiketju ja CA-palvelimen tyypiksi valitaan ”Enterprise root CA”. ”Enterprise root CA” valitaan toimialueen ensimmäisen CA-palvelun tasoksi. Taso on kaikkein luotetuin ja sitä käytetään lähteenä alemman tason CA-palveluille.



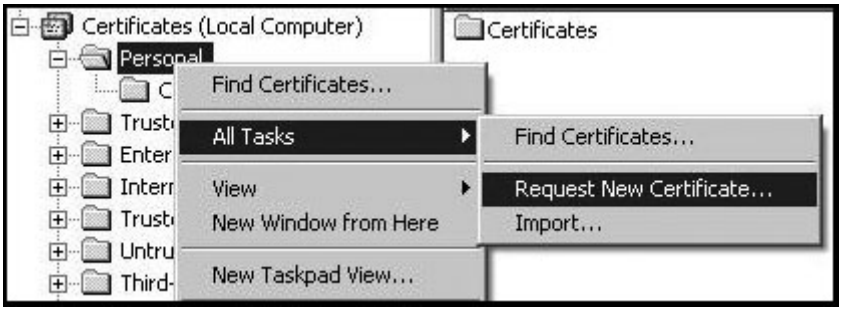
Kuva 17.1 CA-palvelun asennus



Kuva 17.2 CA-palvelun asennus

Certification Authotory –palvelun asennuksen jälkeen täytyy IAS-palvelimelle asentaa tietokone sertifikaatti. Toteuttamassani verkossa CA ja IAS-palvelut on asennettu samalle palvelimelle. Sertifikaatti asennetaan MMC-konsolin avulla. Konsoliin valitaan serti-

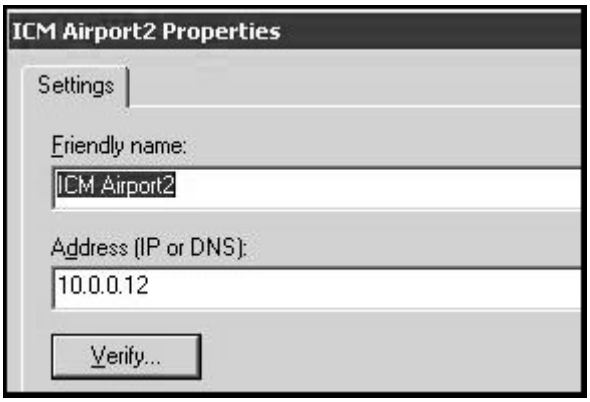
fikaatti laajennus (snap-in) ja laajennuksessa käytettäväksi tiliksi valitaan tietokone (computer). Sertifikaatti pyydetään kohdassa henkilökohtainen (personal) (kuva 18). Tämän jälkeen sertifikaatti asennetaan ohjatun toiminnon avulla. Onnistuneen sertifikaatti asennuksen jälkeen voidaan siirtyä seuraavaan vaiheeseen IAS–palvelun asennukseen.



Kuva 18. Sertifikaatin asennus

11.2 Internet Autentication service

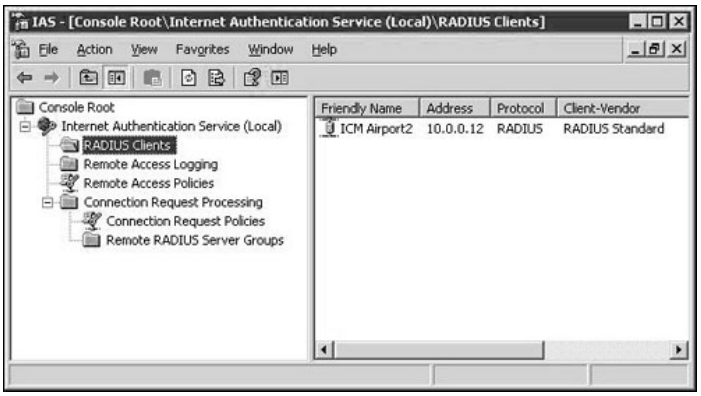
IAS–palvelun asentaminen on helppoa. Palvelu saadaan käyttöön lisäämällä palvelimelle IAS-rooli. Lisäksi IAS–palveluun pitää asentaa langattomassa verkossa käytössä olevat tukiasemat. Tukiaseman lisääminen tapahtuu lisäämällä uusi Radius client. Clientin asennuksessa pitää määritellä tukiaseman IP-osoite, nimi ja valita Radius clientin -tyyppi. Tyypiksi valitaan ”Radius standard”. Tukiasemalle ja IAS – palvelimelle täytyy lisäksi antaa yhteinen salainen avain, jota osapuolet käyttävät toistensa tunnistamiseen.



Kuva 19.1 Radius client asennus

Kuva 19.2 Radius client asennus

Radius clientin asennuksen jälkeen IAS-palvelu täytyy rekisteröidä, jotta AD:ssa olevia käyttäjätunnuksia voi käyttää. Rekisteröinti tapahtuu IAS-konsolissa (kuva 20).



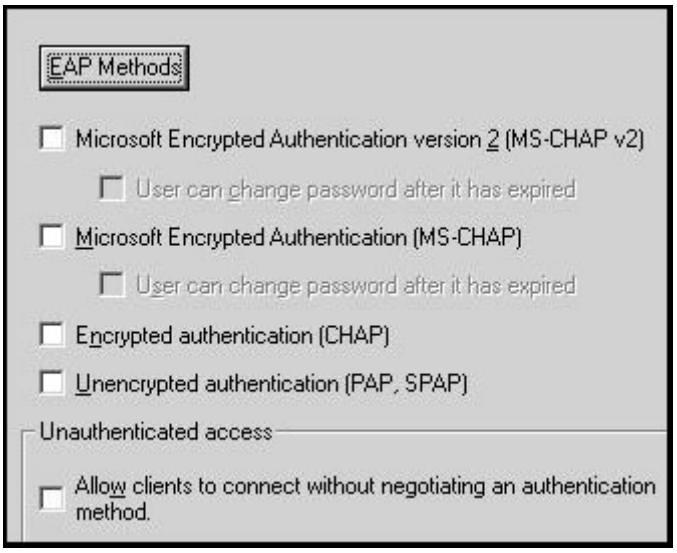
Kuva 20. IAS-konsoli

Remote access Policies

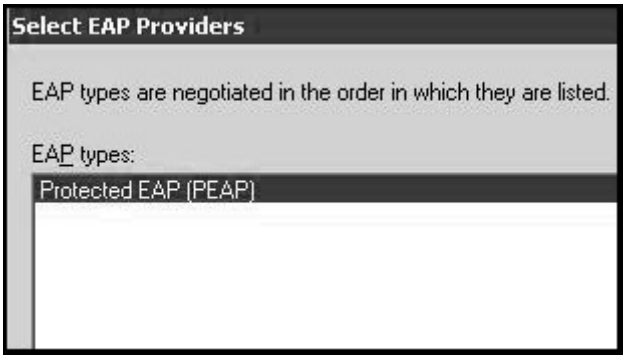
Tukiaseman lisäämisen jälkeen luodaan IAS -palveluun Remote Access politiikka. Politiikka määrittelee käytettävät salaus -ja autentikointimetodit. Sinne määritellään myös Active Directory:ssä olevat käyttäjät, joille myönnetään lupa käyttää verkkoa.

Tein Active directoryyn ryhmän ”WLAN Users”, jolla hallitaan WLAN–verkon käyttäjiä. Ryhmän määritin politiikkaan ryhmäksi, jolle verkkoon pääsy sallitaan. (Huom. toimialueen toiminnallinen tila pitää olla Windows 2003, jotta käyttäjiä voidaan hallita ryhmien avulla.) Politiikan profiiliin tein muutamia muutoksia, jotka selviävät seuraavaksi:

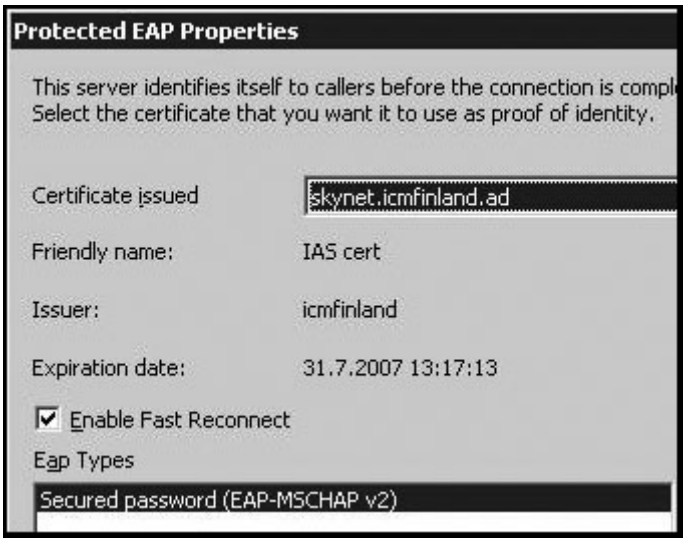
- Autentikointi kohdassa muutin EAP asetuksia ja poistin rastit muista kohdista.
- EAP tyypiksi lisäsin PEAP. (Huom. PEAP-protokollaa ei voi käyttää, jos sertifikaattia ei ole asennettu onnistuneesti.)
- Encryption kohdasta valitsin tiedonsalaukseen vahvimman salauksen.



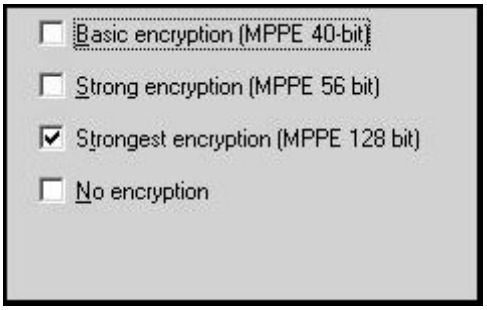
Kuva 21.1 Autentitikointi asetukset



Kuva 21.2 EAP-tyypit



Kuva 21.3. PEAP-ominaisuudet



Kuva 21.4. Tiedonsalaus

Muita muutoksia politiikkaan ei tarvitse tehdä. Politiikkaan voidaan tarvittaessa tehdä paljon erilaisia määrittelyjä. Esimerkiksi voidaan rajoittaa verkkoon pääsy vain tiettyinä kellonaikoina, luoda pakettifilttereitä sekä paljon muita määrityksiä.

11.3 Tukiaseman asennus

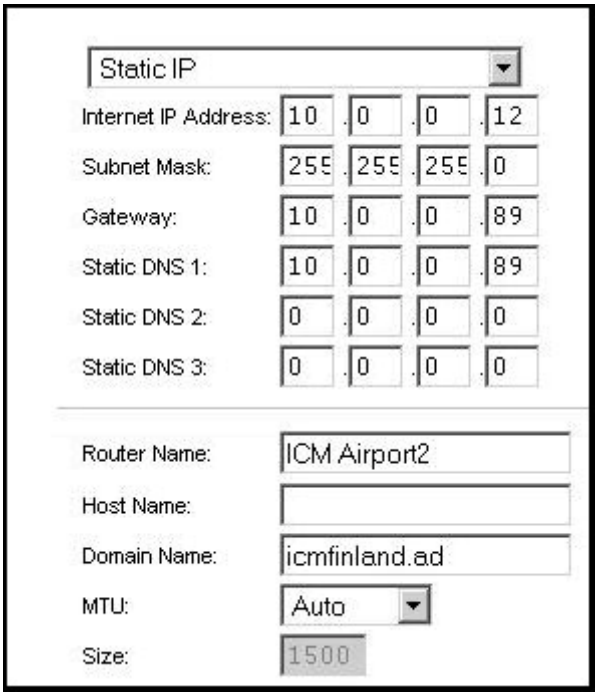
Tukiasemalta vaaditaan IEEE 802.1x-protokollan tuki, jotta sitä voidaan käyttää tässä toteutuksessa. Useimmista tukiasemista löytyy tuki 802.1x:lle. Tässä toteutuksessa käytetään tukiasemana Linksys WRT54G:tä. Siitä löytyy tuki kyseiselle protokollalle. Valitsin vahingossa hieman väärän mallisen tukiaseman. Tukiaseman piti olla sellainen, joka voidaan liittää osaksi olemassa olevaa aliverkkoa. WRT54G on tukiasema, joka toimii reitittimen tavoin. Tämä aiheutti pieniä ongelmia. Ensinnäkin koneille ei voi jakaa IP-osoitteita verkossa olevalta DHCP-palvelimelta, koska tukiaseman reititin estää pyynnöt. Toiseksi tukiasemaa käyttävät koneet ovat omassa aliverkossa, joka aiheutti staattisen reitityksen käyttöönottoa. Oikea tukiasema malli olisi Linksys:in mallistosta ollut Linksys:in WAP54G. Verkko saatiin kuitenkin toimimaan reitittävälläkin mallilla.

Konfiguroin asetukset tukiasemaan ennen sen kytkemistä yrityksen lähiverkkoon. Liitin kannetavan tietokoneen tukiasemassa olevaan LAN-porttiin. LAN-portin kautta pääsin käsiksi tukiaseman graafiseen hallintaohjelmaan. Hallintaohjelmaa käytetään WWW-selaimen kautta.

Basic setup

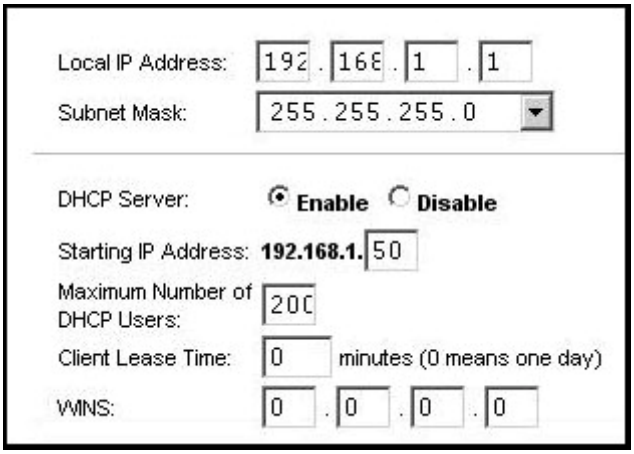
Basic setup kohdassa määritellään tukiaseman WAN-portin IP-asetukset, LAN-portin IP-asetukset ja DHCP-asetukset.

WAN-porttin yhteystyypiksi määritin staattisen IP-osoitteen. Staattinen IP-osoitteen annoin lähiverkon IP-avaruudesta. WAN-porttissa voi käyttää yhteystyyppinä myös DHCP:tä tai tunneloitu- ja yhteyksiä kuten (PPoE, PPTP, L2TP). Näitä käytetään yleensä siinä tapauksessa, että tukiasema on kytketty suoraan ulkoverkkoon.



Kuva 22.1. Linksys Basic setup - WAN

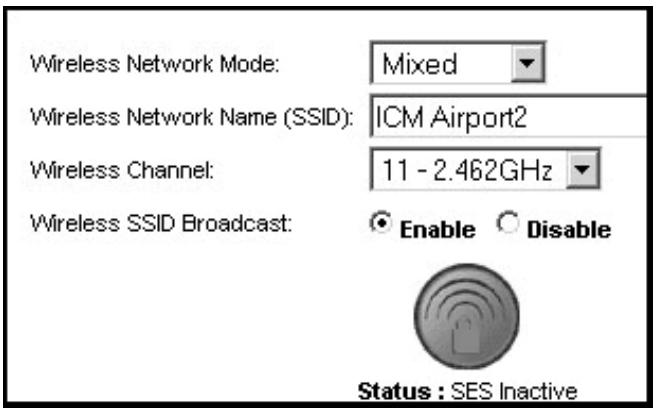
Basic setupissa määritellään myös IP-asetukset langattomille laitteille. Tukiasemaa käyttävien langattomien laitteiden verkossa täytyy käyttää eri IP-aliverkkoa, koska tukiasema toimii reitittimenä. Tässä tuli vastaan ongelma IP-osoitteiden jakelussa. IP-osoitteita ei voinut jakaa verkossa jo olevasta DHCP-palvelimesta, koska palvelin on eri aliverkossa. DHCP-palvelinta voi käyttää, jos reittimenä toimivasta laitteesta löytyy toiminto, joka välittää DHCP-kyselyt eri alivekossa olevalle DHCP-palvelimelle. Toiminnosta laitevalmistajat käyttävät usein nimeä Relay Agent tai IP-helper address. Kyseista toimintoa ei tukiasemasta valitettavasti löytynyt, joten päätin käyttää IP-osoitteiden jakeluun tukiaseman omaa DHCP-palvelua. Palvelu saadaan käyttöön Basic setupista.



Kuva 22.2 Linksys Basic setup - DHCP

Yleiset asetukset

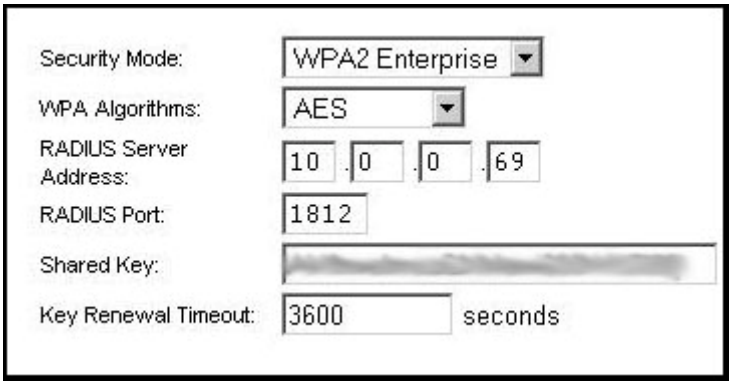
Langattoman verkon asetukset saadaan konfiguroitua kohdasta Wireless. Perusasetuksissa määritellään verkon toimintatila. Verkoissa, joissa käytetään pelkästään IEEE 802.11b tai IEEE 802.11g laitteita määritellään tukiasema toimimaan b- tai g-tilassa. Yrityksellä on laitteita, jotka toimivat sekä b-, että g-tilassa, joten verkon tilaksi määriteltiin mixed. Mixed -tila on yhteensopiva molempien laitteiden kanssa. Perusasetuksissa määritellään lisäksi verkon nimi (SSID) ja mainostetaanko SSID:tä beacon-viesteissä. Tukiasemalle pitää myös määrittää kanava, jolla tukiasema toimii. Useiden tukiasemien verkossa kannattaa tukiasemiin määritellä mahdollisimman kaukana toistaan olevat kanavat häiriöiden välttämiseksi. Yrityksellä on verkossa kaksi tukiasemaa. Tukiasemien kanaviksi määriteltiin 6 ja 11.



Kuva 23. Linksys Basic wireless setup

Turvallisuusasetukset

Turvallisuusasetukset määrittelevät verkon suojaustason. Tukiasema tukee useita eri suojaustiloja. Kotikäyttöön tarkoitetut tilat ovat WEP, WPA- ja WPA2-personal. Näissä tiloissa käytetään esijaettua avainta verkon autentikoinnissa. Kotikäyttöön tarkoitetuissa turvallisuustiloissa ei käytetä erillistä autentikointipalvelinta. Tässä toteutuksessa käytetään turvallisuustilana WPA2-Enterprice. WPA2-Enterprice tilaa käytettäessä täytyy käyttää erillistä autentikointipalvelinta. Autentikointipalvelimen IP-osoite täytyy määritellä tilan asetuksiin. Lisäksi täytyy määritellä mitä porttia palvelin kuuntelee sekä salainen avain. Oletuksena palvelin kuuntelee porttia 1812. Palvelimelle ei vaihdettu porttia, joten voidaan käyttää oletusporttia. Kohtaan salainen avain (Shared Secret) määritellään sama merkkijono, joka on määritelty autentikointipalvelimelle. Merkkijonossa kannattaa käyttää tarpeeksi pitkää ja erikoismerkkejä sisältävää merkkijonoa. Avain vaihdetaan lankaverkossa, joten se ei ole niin haavoittuva. Siitä huolimatta kannattaa käyttää kunnollista avainta. Asetuksiin pitää määritellä myös kuinka usein avain uusitaan yhteydenaikana. Arvona voidaan käyttää oletusarvoa 3600, jos sitä ei ole vaihdettu autentikointipalvelimen päähän.



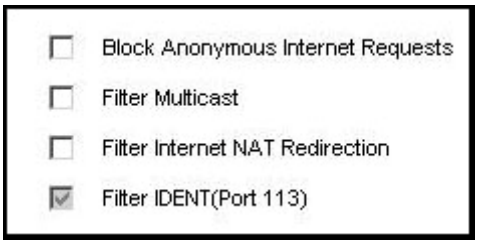
Kuva 24. Linksys Wireless security

Langattoman verkon toiminnan kannalta edellä mainitut määrittelyt olivat keskeiset. Mitään muuta ei välttämättä tarvitse tukiasemaan tehdä, joten langattoman verkon pitäisi näillä asetuksilla toimia. Tukiaseman asetuksiin voidaan lisäksi tehdä tiedonsiirtoon liittyviä muutoksia. Voidaan esimerkiksi säätää beacon –aikaväliä, tiedonsiirtonopeutta ja data-pakettien kokoa. Näihin asetuksiin ei kannata koskea, jos ei todella tiedä mitä on tekemässä. Asetusten muuttamien voi aiheuttaa langattoman verkon toimimattomuuden. Tässä työssä näitä asetuksia ei muutettu.

Muut asetukset

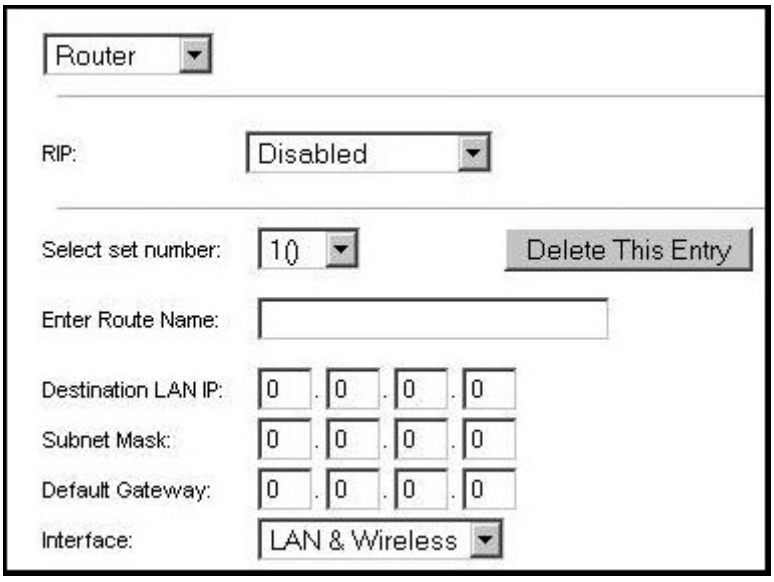
Perusasetusten jälkeen tukiasemalle täytyy vielä tehdä muutamia muutoksia. Tukiasema sisältää palomuuritoiminnon. Tämä toiminto on tukiasemassa oletuksena päällä. Tukiaseman valmistaja on ilmeisesti olettanut, että tukiasema laitettaan yleensä kiinni suoraan ulkoverkkoon. Näin ollen palomuuri on automaattisesti päällä. Sisäverkkototeutuksissa palomuuria ei käytetä.

Palomuurin saa pois päältä security-asetuksista. Asetuksista saa estettyä ICMP- ja multicast-pakettien liikenteen. Pois päältä palomuurin saa ottamalla kaikista kohdista rastit pois.



Kuva 25. Linksys Firewall

Tukiaseman toimintatila pitää määritellä Advanced Routing:in kautta. Toimintatilaksi voidaan valita Gateway tai Router. Gateway valitaan tilaksi silloin, kun tukiasema on suoraan kiinni ulkoverkossa. Router-tila taas silloin, kun verkossa on myös muita reitittimiä. Tässä toteutuksessa käytetään tilana router-tilaa. Advanced Routing-asetuksista saadaan lisäksi asetettua staattisia reittejä tai voidaan ottaa dynaaminen RIP-reititysprotokolla käyttöön.



Kuva 26. Linksys Advanced Rounting

Muita muutoksia tukiaseman asetuksiin ei tarvitse tehdä. Tämän jälkeen tukiasema voidaan kytkeä kiinni yrityksen verkkoon. Tukiasema kytketään WAN-portin kautta yrityksen lähiverkkoon.

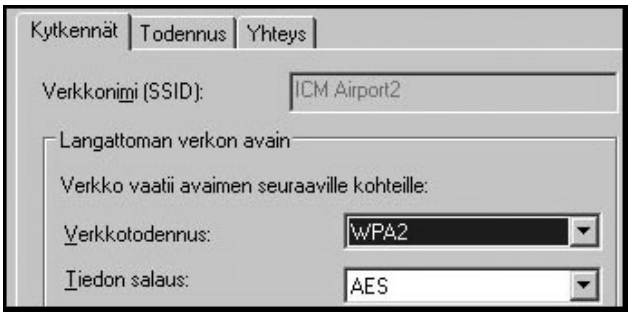
Seuraavaksi täytyy kannettaville tietokoneille laittaa asetukset kuntoon, jotta ne saadaan liitettyä langattomaan verkkoon.

11.4 Langattomien laitteiden asennus

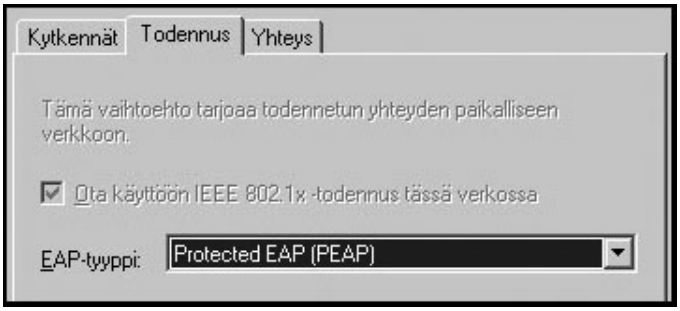
Kannettaville tietokoneille täytyy konfiguroida tiettyjä asetuksia ennen kuin ne saadaan toimimaan langattomassa verkossa. Ensimmäinen ongelma asennuksessa tuli eteen heti alussa. Windows XP –käyttöjärjestelmä ei tue WPA2-protokollaa, mutta Microsoft on kuitenkin julkaissut HotFix-päivityksen XP:lle. Ensimmäiseksi täytyy siis asentaa HotFix –päivitys (KB893357). HotFix –päivitys voidaan asentaa vain XP:lle, jossa on Service Pack 2 päivitys asennettu. Lisäksi täytyy varmistaa wlan-kortin tai piirin ajurien tuki WPA2-protokollalle. Suotavaa on hakea netistä uusimmat ajurit ennen asennuksen jatkamista. Vanhimpien wlan-piirien rauta ei tue WPA2-protokollaa. Näihin kortteihin ei auta ajurien päivittäminen.

Tarvittavien päivitysten jälkeen voidaan jatkaa konfigurointia. Langattomien verkkojen hallintaan kannattaa käyttää Windowsin omaa ohjelmistoa. Verkkoja voidaan hallita myös erillisillä ohjelmilla, mutta yhteensopivuuden kannalta on paras käyttää Windowsin ohjelmistoa. Langattoman verkkoyhteyden asetuksiin täytyy tehdä seuraavat muutokset:

- verkontodennus -protokolla: WPA2
- tiedon salaus -protokolla: AES
- EAP-tyyppi: Protected EAP (PEAP)

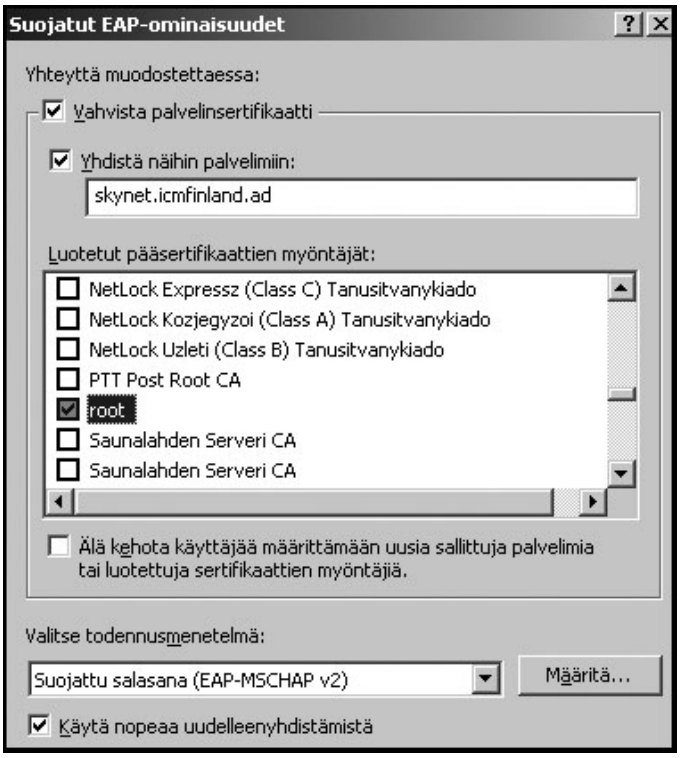


Kuva 27. Langatoman verkon ominaisuudet



Kuva 28. EAP-tyyppi

Lisäksi EAP-tyypin ominaisuuksiin määritellään sertifikaattipalvelin, jota käytetään autentikointipalvelimen varmentamiseen. Autentikointipavelin varmentaminen voidaan määritellä kahdella tavalla. Voidaan määritellä sertifikaattipalvelimen osoite, josta sertifikaatti varmistetaan tai asennetaan kannettavalle tietokoneelle pääsertifikaatti, johon luotetaan. EAP-tyypin ominaisuuksista määritellään myös todennusmenetelmä. Todennusmenetelmänä voidaan käyttää samoja tunnuksia, joilla kirjaudutaan koneelle. Tunnuksia voidaan käyttää koneen kuuluessa toimialueeseen. Koneille, jotka eivät kuulu toimialueeseen verkkoon yhdistäessä tunnuksia kysytään.



Kuva 29. EAP-ominaisuudet

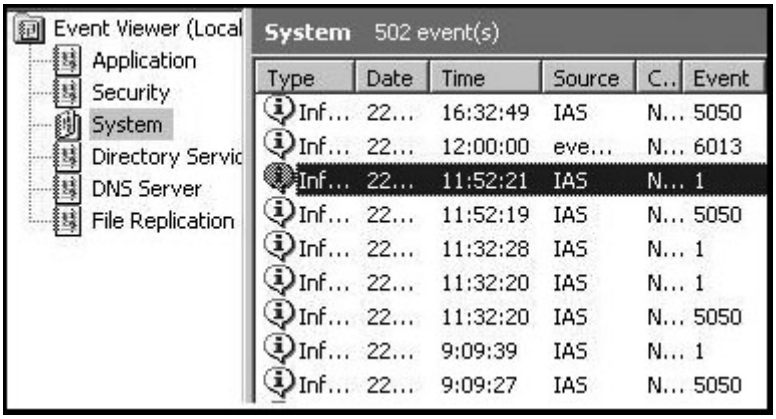
Opinnäytetyön liitteenä 1 on henkilöstölle tehty ohje verkon käyttöönottoon. Ohjeessa on kuvattu yksityiskohtaisemmin kuinka kannettava tietokone saadaan kytkettyä langattomaan verkkoon.

11.5 Verkon testaaminen

Verkko toimi vanhan WLAN-verkon rinnalla noin kaksi viikkoa testien ajan. Verkkoa testattiin kahdella kannettavalla tietokoneella. Kaksi konetta on ihan riittävä testaamiseen, kun verkon kokonaiskäyttäjä määrä on kuitenkin vain noin 15 henkilöä. Näistä käyttäjistä verkkoa yhtä aikaa käyttää korkeintaan 10 henkilöä.

Verkkoa ja sen toimivuutta testattiin kirjautumistestien ja tiedonsiirto kokeilujen avulla. Kirjautumistapahtumia voi seurata autentikointipalvelimen lokitiedoista. Lokitietoja voi tarkastella autentikointipalvelimen Event Viewer –ohjelmalla (kuva 30). Lokitietoihin tallentuu kaikki kirjautumistapahtumat, niin onnistuneet kuin epäonnistuneet. Lokitietoja kannattaa tutkia ongelmatilanteissa, yleensä lokien avulla vian pystyy paikallistamaan.

Autentikointipalvelimen lokitietojen lisäksi tutkin autentikointi liikennettä kaappaamalla Ethereal –ohjelmalla liikennettä yhden kannettavan tietokoneen avulla. Kaappauksen avulla pystyin selvittämään mitä autentikoinnin aikana todella tapahtuu. Sain todettua, että autentikointi toimii oikealla tavalla, eikä autentikoinnin aikana tapahdu virheitä. Kuvassa 31 on Ethereal –ohjelman kaappaama tieto autentikoinin aikana liikuteltavista paketeista.



Kuva 30. Event Viewer

Protocol	Info
EAPOL	Start
EAP	Request, Identity [RFC3748]
EAP	Response, Identity [RFC3748]
EAP	Request, PEAP [Palekar]
TLS	Client Hello
EAP	Request, PEAP [Palekar]
EAP	Response, PEAP [Palekar]
EAP	Request, PEAP [Palekar]
EAP	Response, PEAP [Palekar]
EAP	Request, PEAP [Palekar]
EAP	Response, PEAP [Palekar]
TLS	Server Hello, Certificate, Certificate Request,
TLS	Certificate, Client Key Exchange, Change Cipher
TLS	Change Cipher Spec, Encrypted Handshake Message
EAP	Response, PEAP [Palekar]
TLS	Application Data
TLS	Application Data
TLS	Application Data
TLS	Application Data
TLS	Application Data
TLS	Application Data
TLS	Application Data
TLS	Application Data
EAP	Success
EAPOL	Key
EAPOL	Key
EAPOL	Key
EAPOL	Key
DHCP	DHCP Discover - Transaction ID 0xd8522e0e
DHCP	DHCP Offer - Transaction ID 0xd8522e0e
DHCP	DHCP Request - Transaction ID 0xd8522e0e
DHCP	DHCP ACK - Transaction ID 0xd8522e0e

Kuva 31. kaappaus autentikointiliikenteestä

Testauksessa ilmenneitä ongelmia

Muutamia ongelmia ilmeni testauksen aikana. Ongelmien synty on normaalia uusien palveluiden käyttöönotossa. Ongelmia oli aluksi verkkoon kirjautumisessa. Kirjautuminen juuttui käyttäjätunnuksen varmentamiseen. Lokitiedoista selvisi mistä ongelma johtui. Ongelma liittyi siihen, että autentikointipalvelin ei saanut yhteyttä Active Directory -palveluun. Eikä siis voinut varmentaa käyttäjää. Varsinaista vikaa en löytänyt mikä ongelman aiheutti. Kirjatuminen onnistui jonkin ajan kuluttua ilman, että asetuksiin tehtiin muutoksia. Ilmeisesti ongelma johtui Group policy:stä. Group policy ei ollut ehtinyt päivittyä palveluiden asennusten jälkeen. Asennuksen yhteydessä IAS-palvelu rekisteröitiin Active Directory –palveluun, joten ilmeisesti yhteys Active Directory -palveluun sallittiin vasta Group Policyn päivittymisen jälkeen. Group polycy päivittyy normaalisti 90 minuutin välein. Vian selvittämisessä meni varmasti aikaa sen verran, että group policy ehti päivittyä. Group Policy:n olisi saanut päivitettyä heti cmd-konsolista komennolla ”gpupdate /force”.

Ongelmien selvittyä päästiin verkon liikenteen testaamiseen. Avasin cmd-konsolin ja tarkistin ensin onko laite saanut IP-asetukset. Laitteelle oli DHCP-palvelin määrittänyt IP-osoitteen. Tämän jälkeen testasin ping-ohjelmalla yhteyttä oletusyhdyskäytävään (192.168.1.1). Oletusyhdyskäytävä vastasi ping-kyselyyn, joten yhteys on tukiasemaan kunnossa. Tämän jälkeen laajensin ping-testausta ja testasin yhteyttä verkon reunalla olevaan reittimeen. Verkon reunalla oleva reititin ei vastannut ping-kyselyyn.

Verkon reunareititin ei tietenkään vastannut, koska reitittimelle ei ollut määritelty reittiä tukiaseman LAN-verkkoon (192.168.1.0 /24). Verkonreunalla reitittimenä toimi Windows 2003 palvelin. Lisäsin palvelimen Routing and Remote Access – palveluun staattisenreitin verkkoon 192.168.1.0. Tämän jälkeen testasin uudestaan yhteyttä ping-ohjelmalla ja nyt ping-viestiin tuli myös vastaus. Ping-ohjelmalla sain testattua yhteyden toimivuuden OSI-mallin kolmannelle kerrokselle asti. Seuraavaksi testasin yhteyden toimivuuden sovelluskerrokselle asti. Testaukseen käytin www-selainta. Selaimen avulla saadaan testattua myös nimipalvelu. Selaimen käynnistyttyä aukesi ongelmitta aloitussivu (www.google.fi). Testasin selaimella muutamia www-osoitteita, joiden avulla totesin yhteyden toimivan.

11.6 Verkonkehitys

Langatonta verkkoa ja koko muuta verkkoa on tarkoitus kokoajan kehittää vastaamaan paremmin yrityksen tarpeita. Tietoturvallisuus on myös yksi tärkeä kehityksen osa-alue, jota kehitetään kokoajan eteenpäin. Tarkoitus oli myöhemmin jakaa langattoman verkon asetukset Active Directory – palvelun kautta, mutta kävi ilmi ettei Windows 2003 käyttöjärjestelmän Group policy tue WPA2 autentikointia. Selvitin löytyisikö tähän päivitystä, mutta Microsoft ei ole vielä julkaissut ko. päivitystä. Tällä hetkellä ei ole tietoa milloin päivitys julkaistaan. Microsoftin mukaan tuki löytyy seuraavaksi julkaistavassa Windows palvelinkäyttöjärjestelmässä. Nähtäväksi jää julkaistaanko päivitystä ollenkaan. Asetusten konfigurointi jokaiselle koneelle erikseen ei ole näin pienessä organisaatiossa vielä ongelma, mutta yrityksen kasvaessa asetusten jakelu automaattisesti on erittäin tärkeää ja vähentää ylläpidon työmäärää huomattavasti.

Yrityksessä tulevaisuudessa siirretään VPN-yhteys toimimaan L2TP-protokollan päälle. Nykyisin käytössä on PPTP-protollan päällä toimiva ratkaisu. Sertifikaatti palvelua tarvitaan L2TP-VPN yhteyksissä, joka siis tämän projektin myötä yrityksestä löytyy. Lisäksi sertifikaattipalvelu mahdollistaa 802.1x autentikoinnin laajentamisen myöhemmin myös lankaverkon puolelle. Laajentamista

ei ole ainakaan vielä katsottu tarpeelliseksi, koska yrityksen tiloihin ei pääse ilman avainta. 802.x –protokollan käyttö koko verkon alueella nostaisi tietoturvallisuustasoa merkittävästi ja tekee luvattomien käyttäjien pääsyn verkkoon todella vaikeaksi.

12 YHTEENVETO

Langattoman verkon tekniikka perustuu 802.11 -standardiperheeseen. Standardin kehitys on jaettu työryhmiin, joiden tehtävä on kehittää standardia eteenpäin. Suosituimmat standardit 802.11 -standardiperheestä on 802.11b - ja 802.11g -standardit.

Tietoliikenteeseen liittyy erilaisia tiedon luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviä kysymyksiä. Langattomassa tiedonsiirtotekniikassa nämä kysymykset täytyy ottaa erityisesti huomioon. Radiotaajuuksilla tietoa siirrettäessä tieto on erityisen altis salakuuntelulle, häirinnälle ja hakkerointi yrityksille. Radiotaajuudella toimivaa verkkoa ei voida täysin turvata fyysisillä esteillä tai palomuureilla.

Tietoturvasta huolehtiminen onkin yksi langattoman verkon kivijaloista. Ilman verkon riittävää suojatasoa ei verkkoa saada toimimaan vakaasti ja luotettavasti. IEEE 802.11 -standardi määrittelee verkon suojaamiseksi heikot keinot todennuksen, avaintenhallinnan ja tiedon salauksen toteuttamiseksi, jotka eivät enää tänä päivänä riitä verkon liikenteen suojaamiseksi.

IEEE 802.11 -standarin heikon tietoturvan sijasta langattomien verkkojen tietoturvan tulisi perustua IEEE:n julkaisemaan järeään 802.11i -tietoturvastandardiin. Standardi määrittelee parannetut menetelmät todennuksen, avaintenhallinnan ja tiedon salauksen toteuttamiseksi.

Loppusanat

Työn aiheen valintaan olen tyytyväinen. Ennen opinnäytetyön tekemistä itselläni ei ollut paljon kokemusta langattomista verkoista tai tekniikoista. Työtä tehdessäni huomasin, että langaton verkko koostuu varsin monimutkaisesta tekniikasta. Langattomat verkot pitävät sisällään varsin sekavan standardiviidakon. Langattomaan verkkoon on määritelty useita standardeja ja koko ajan niitä näyttää tulevan lisää.

Työssäni haasteellista oli ymmärtää kaikkien erilaisten standardien käyttötarkoitus ja missä yhteydessä niitä käytetään. Välillä standardiverkostoa tutkiessani olin hieman sekaisin, mutta lähteitä aikani tutkittua hahmottui lopulta kokonaiskuva standardeista.

Langattomien verkkojen tietoturva koostuu mielestäni todella monimutkaisesta kokonaisuudesta. Tietoturva koostuu useista protokollista ja useista erilaisista vaiheista. Haastavinta oli koota tietoturvallisuus tekniikasta työhön tiivis ja selkeä kuva.

Työni perustuu toimeksiantajalle tekemääni verkkoon, jonka toteutusvaiheen aikana idea opinnäytetyön aiheesta syntyi. Aihetta tarkemmin aloin tutkimaan, kun olin saanut työssä esitellyn verkon toteutettua.

Toteutuksen pohjalta ajattelin, että tutkin tarkemmin langattomien verkkojen tietoturvaa ja tiedonsiirtotekniikkaa. Nämä asiat työstäni löytyykin, mutta alun perin minun piti myös perehtyä langattomanverkon suorituskykyyn ja verkon todelliseen tiedonsiirtonopeuteen. Verkkostandardien ilmoitetut nopeudet kun ovat teoreettisia ja todellisuudessa nopeudet ovat alhaisemmat. Tämä osa työstä jäi ajan puutteen vuoksi pois, sillä tietoturvan tutkiminen vei yllättävän paljon aikaa. Ehkäpä langattoman verkon suorituskyvystä saisi vaikka tehtyä kokonaisen opinnäytetyön.

LÄHTEET

Falk, Magnus 2004. Fast and Secure Roaming in WLAN. [online][viitattu 1.12.2006]. http://www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-2695-1__fulltext.pdf

Frankel Sheila, Eydt Bernard, Owens Les, Kent Karen, 2006.
National Institute of Standards and Technology (NIST). SP 800-97 (Draft).
Guide to IEEE 802.11i: Establishing Robust Security Networks. [online][viitattu 1.12.2006]. http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf

Hakala, Mika & Vainio, Mika 2005. Tietoverkon rakentaminen. Jyväskylä:Docendo. ISBN: 951-846-263-1.

IEEE Computer Society 1999. ANSI/IEEE Std 802.11, 1999 Edition (R2003): Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. [online][viitattu 1.12.2006]. http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[A] IEEE Computer Society 2004. ANSI/IEEE Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements. [online][viitattu 1.12.2006]. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[B] IEEE Computer Society 2004. ANSI/IEEE Std 802.1X: Port-Based Network Access Control.[online][viitattu 1.12.2006]. http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

IETF 2005. RFC 4017. [online][viitattu 1.12.2006]. http://www.ietf.org/rfc/rfc4017.txt

Puska, Matti 2005. Langattomat lähiverkot. Helsinki:Talentum. ISBN: 952-14-0934-7.

Velte, Toby J. & Velte, Anthony T. 2005. CISCO 802.11 Wireless Networking Quick Reference. Indianapolis: Cisco Press. ISBN: 1-58705-227-X.

LIITTEET

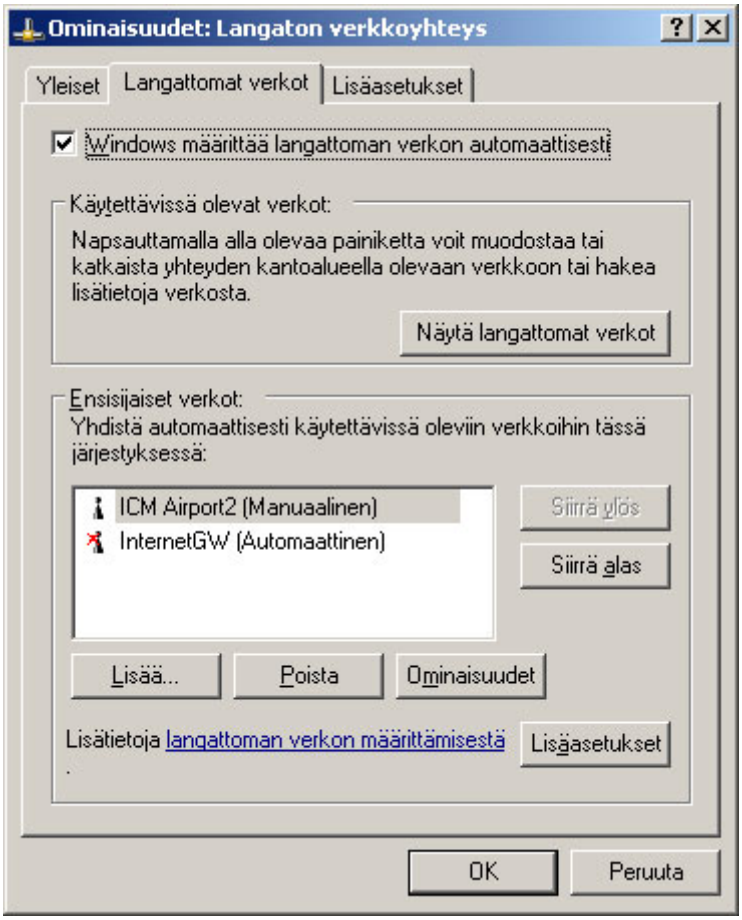
Liite 1 Ohje WLAN-yhteyden muodostamiseksi

1. Avaa verkkoyhteydet -> kaksoisklikkaa langatonta yhteyttä

2. Valitse listasta ”**ICM Airport2**” -> paina vasemmasta kulmasta ” muuta lisäasetuksia

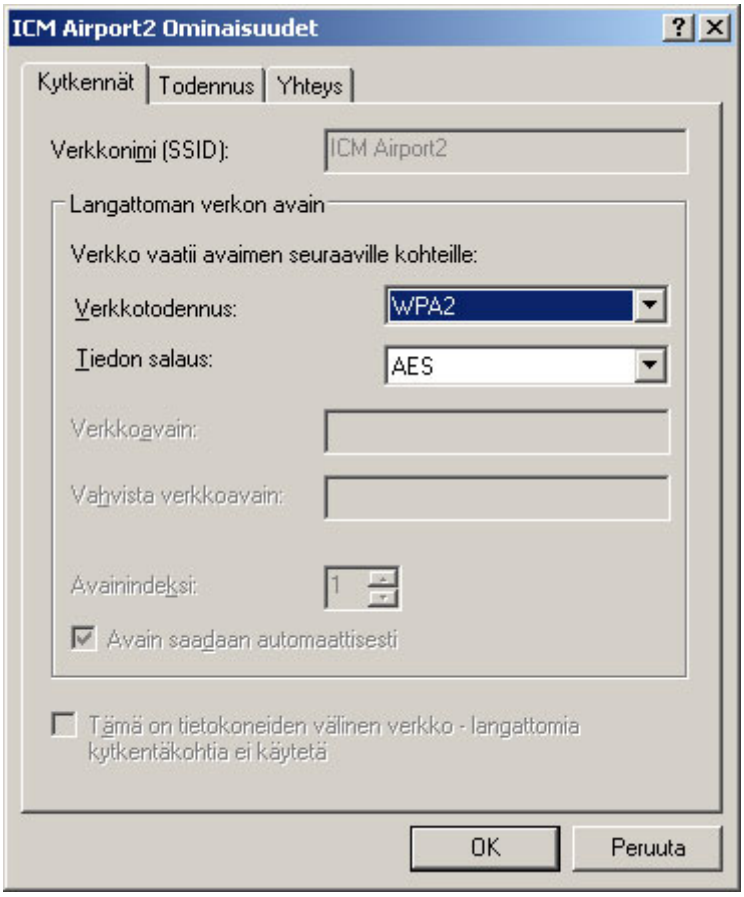
Jatkuu

3. Valitse ”langattomat verkot” – välilehti -> valitse ”ICM Airport2” -> klikkaa ”ominaisuudet”



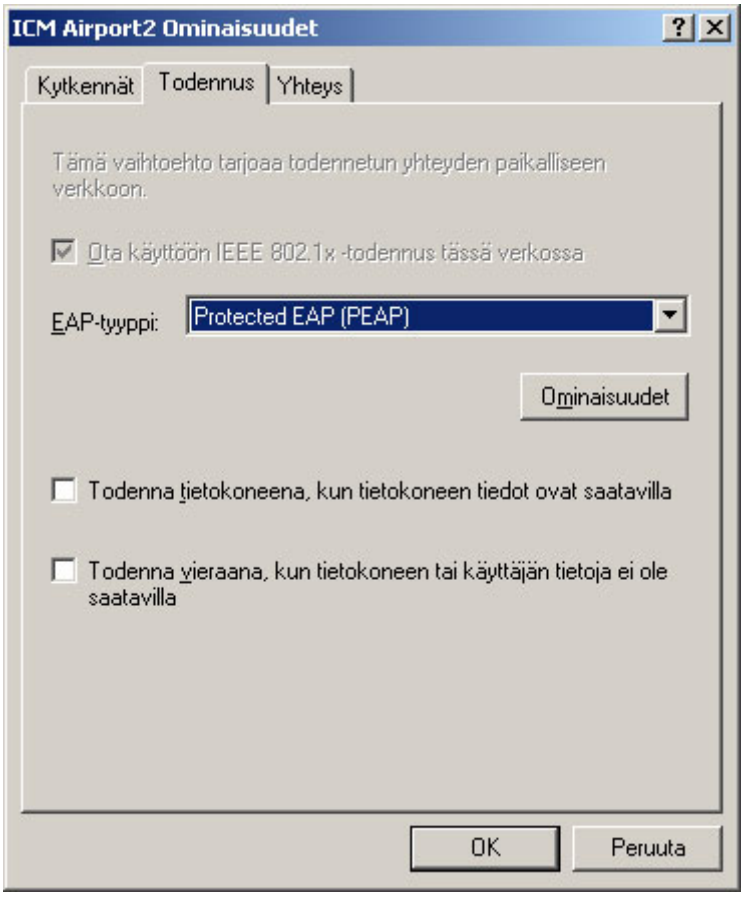
Jatkuu

4. Aseta verkontodennus protokollaksi ”**WPA2**” sekä tiedonsalaus protokollaksi ”**AES**”



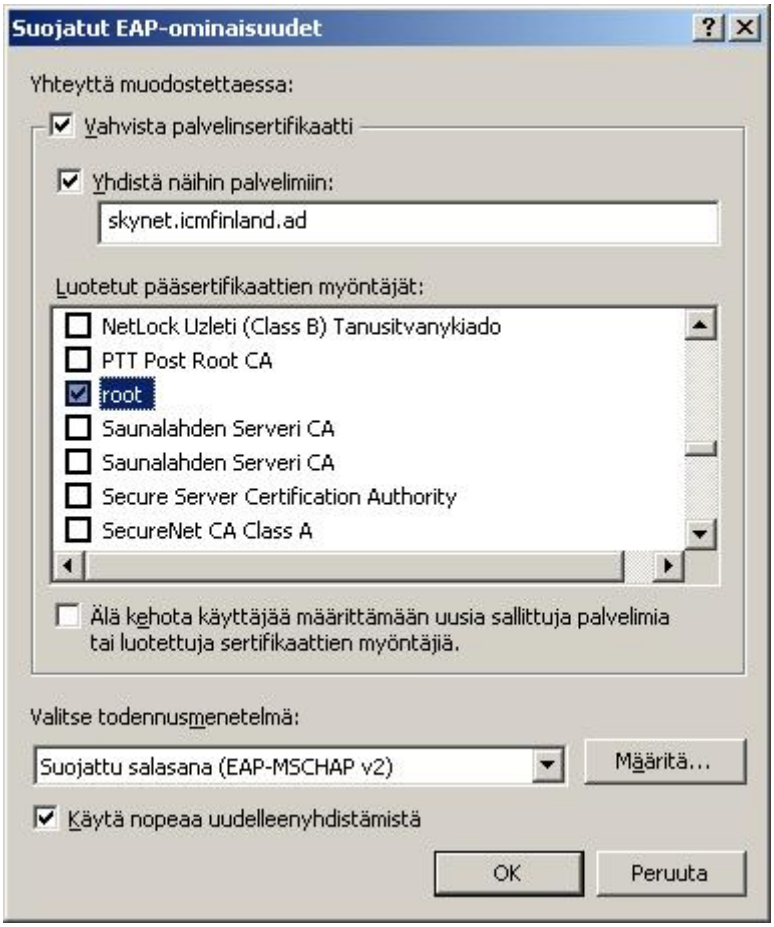
Jatkuu

5. Aseta todennus välilehdeltä EAP-tyypiksi **PEAP** -> poista rastit EAP-tyypin alla olevista kohdista –> klikkaa ”ominaisuudet”



Jatkuu

6. Valitse rastit kohdista ”vahvista palvelinsertifikaatti” / ”käytä nopeaa uudelleenyhdistämistä” / ”yhdistä näihin palvelimiin” -> aseta palvelimen osoitteeksi ”**skynet.icmfinland.ad**” -> valitse ”luotetuksi pääsertifikaatiksi” -> ”**root**” -> klikkaa ”määritä”



Jatkuu

7. Valitse rasti kohdasta ”käytä automaattisesti Windows-käyttäjänimeäni” -> klikkaa ”OK”

8. poistu yhteysasetuksista ja palaa verkkojen valintaan -> yhdistä verkkoon ”ICM Airport2”