LANGATTOMAT LÄHIVERKOT

Case: WPK

Eliisa Romunen

Katja Tikkanen

Opinnäytetyö
Marraskuu 2010
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut
Tampereen ammattikorkeakoulu

TAMPEREEN AMMATTIKORKEAKOULU

Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

ELIISA ROMUNEN & KATJA TIKKANEN: Langattomat lähiverkot, CASE: WPK

Opinnäytetyö 44 s., liitteet 46 s.
Marraskuu 2010

Opinnäytetyön aiheena oli rakentaa kontrolleripohjainen langaton jatke Tampereen ammattikorkeakoulun WPK-nimiseen verkkoon. Työn kirjallinen osuus laajennettiin koskemaan langattomia verkkoja yleisesti ja siksi tehtiin laajaa tutkimustyötä niin langattoman verkon tietoturvasta, eri salaustavoista kuin langattomuuden historiastakin. Työn niin sanotun A-osan on tarkoitus olla kattava paketti oleellista tietoa langattomista verkoista ja niin sanottu B-osa keskittyy langattoman verkon implementointiin WPK-verkkoon.

Työn tuloksena syntynyttä langatonta verkkoa on helppo kehittää eteenpäin, lisätä siihen uusia ominaisuuksia tai laajentaa sitä tarvittaessa. WPK-verkko on pääsääntöisesti opiskelijoiden ylläpitämä, joten rakennettu verkko antaa mukavan lisän muun muassa WPK-verkossa harjoittelijana työskenteleville opiskelijoille, ja mahdollisesti antaa aiheita myös tulevaisuudessa harjoitus- ja opinnäytetöihin.

Asiasanat: Langattomat lähiverkot, tietoturva, salausmetodit, standardit

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Networking Services

ELIISA ROMUNEN & KATJA TIKKANEN: Wireless Local Area Networks, CASE: WPK

Bachelor's thesis 46 pages, appendices 46 pages.
November 2010

The purpose of this thesis was to build a controller-based wireless local area network into the WPK-network which is a separate part of Tampere University of Applied Sciences network. The theory section of this thesis was extended to cover wireless local area networks in general and major research was carried out about the information security in wireless networks, about different methods on how to encrypt data as well as about the history of wireless networks. Part A of our thesis offers a wide area of knowledge about wireless networks and part B focuses on how the wireless solution was implemented into the WPK-network.

As a result was created a wireless network, which is easy to develop even further, add new features into it or expand it if necessary. WPK-network is mainly managed by students so the wireless solution makes a nice addition to the students who work as the administrative persons of the WPK-network. It is also hoped that the wireless network will give opportunities for more practical exercises or work and even for new fields of theses.

Key words: wireless local area network, information security, encryption methods, standards

LYHENTEET

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
CLI	Command-Line Interface
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service, palvelunestohyökkäys
DSL	Digital Subscriber Line
DSSS	Direct-Sequnce Spread Spectrum, suorasekvenssihajaspektri
EDGE	Enhanced Data rates for Global Evolution
FHSS	Frequency-Hopping Spread Spectrum, taajuushyppelyhajaspektri
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile
HiperLAN	High Performance Radio Local Area Networks
IEEE	Institute of Electrical and Electronics Engineering
IETF	Internet Engineering Task Force
IP	Internet Protocol
IrDA	Infrared Data Association
LWAPP	Light-Weight Access-Point
MAC	Media Access Control
NAP	Network Access Protocol
NAT	Network Address Translation, osoitteenmuunnos
OFDM	Orthogonal Frequency Division Multiplexing, monitaajuusmodulointi
OSI	Open Systems Interconnection
PAT	Port Address Translation
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency, radiotaajuus
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network, virtuaallinen lähiverkko
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network, langaton lähiverkko
WMAN	Wireless Metropolitan Area Network, langaton kaupunkiverkko
WPA	Wi-Fi Protected Access

WPAN	Wireless Personal Area Network, langaton henkilökohtainen lähiverkko
WWAN	Wireless Wide Area Network, langaton laajaverkko

1 JOHDANTO

Langattomuus on nykyaikaa. Ihmiset miltei kaikkialla maailmassa käyttävät päivittäin useita laitteita edes ajattelematta sen helppoutta ja vaivattomuutta – ja langattomuutta. Kelläpä meillä ei olisi kännykkää taskussa, mutta langattomuutta kotona edustavat myös muun muassa television kaukosäädin, navigaattori ja kannettava tietokone. Myös uusimpien autojen avaimet lukitsevat ja avaavat auton ovet ”langattomasti” - ilman että avainta tarvitsee kääntää lukossa.

Tämä opinnäytetyö käsittelee yhtä langatonta saavutusta, langattomia lähiverkkoja, joissa kodin tai yrityksen Internet-yhteys toteutetaan langattomasti. Käsittelemme tämän kirjallisen osuuden ns. A-osassa langattomia verkkoja yleisesti: kerromme niiden historiasta, tietoturvasta ja eri tavoista miten langattoman verkon voi muodostaa. Työn niin sanotussa B-osuudessa käymme läpi langatonta verkkoratkaisua jonka rakensimme Tampereen Ammattikorkeakoululle WPK-verkon jatkeeksi.

Toimeksiantonamme oli rakentaa kolme erillistä langatonta verkkoa: opiskelijaverkko, adminverkko sekä vierailijaverkko, joista kahteen ensimmäiseen kirjautuminen tulisi hoitaa RADIUS-palvelun (Remote Authentication Dial In User Service) avulla. Vierailijaverkkoon tulisi toteuttaa web-autentikointi. Tavoitteena oli saada työhömme liitettyä myös koulumme toisen opiskelijan opinnäytetyö, joka käsitteli turvallista verkkoon pääsyä eli NAPia (Network Access Protection).

Työmme kirjallinen osuus koskee pääsääntöisesti 802.11-standardien mukaisia langattomia lähiverkkoja, mutta kerromme myös muista tekniikoista joilla langattomuutta voidaan lähteä rakentamaan. Näitä tekniikoita ovat esimerkiksi Bluetooth, infrapuna ja HiperLan (High Performance Radio Local Area Networks).

Opinnäytetyömme toimeksiantaja on Tampereen ammattikorkeakoulu / tietojenkäsittelyn koulutusohjelma ja tilaajana toimii Ville Haapakangas.

2 LANGATTOMIEN LÄHIVERKKOJEN HISTORIA

Ihmisillä on ollut kautta aikain tarve ja keinot kommunikoida toistensa kanssa pitkien matkojenkin päästä. Keinot ovat ajan kuluessa huomattavasti parantuneet, mutta langattomuuden juuret ulottuvat aina esihistorialliselle aikakaudelle, jolloin viestintään käytettiin esimerkiksi peilejä, tulta ja savumerkkejä. (Wikipedia: langattoman tiedonsiirron historia) Aistihavaintoihin perustuvaa kommunikointia on myös esimerkiksi kaikkien tunteman valkoisen lipun heiluttaminen antautumisen merkiksi, tai erilaisilla rummuilla tai torvilla armeijan ohjaaminen hyökkäykseen.

Nykyaikainen langattomuus pohjautuu pitkälti monen 1800-luvulla eläneen tiedemiehen elämäntyöhön. Alulle kaiken pisti skotlantilainen fyysikko James Maxwell, joka esitteli teoriansa sähkömagneettisista aaltoliikkeistä vuonna 1873. (Wikipedia: radio) Maxwellin työtä jatkoi hänen saksalainen kollegansa Heinrich Hertz, joka todisti sähkömagneettisen säteilyn olemassaolon rakentamalla laitteen, joka tuotti radioaaltoja. (Wikipedia: Heinrich Hertz) Vuonna 1893 Nikola Tesla keksi menetelmän radioaaltojen hyödyntämiseksi kommunikoinnissa ja järjesti ensimmäisen julkisen radiolähetyskokeilun St. Louisissa Missourissa. (Wikipedia: radio) Italialainen fyysikko Guglielmo Marconi tutki myös tahollaan radioaaltoja ja vuonna 1895 hän muodosti radioyhteyden muutaman kilometrin päähän ja seuraavana vuonna hänelle myönnettiin sähköistä lennätintä koskeva patentti. Vuonna 1899 Marconi pystyi muodostamaan radioyhteyden jo Englannin ja Ranskan välille, kaksi vuotta myöhemmin lennätinyhteys oli olemassa jo Atlantinkin yli. (Wikipedia: langattoman tiedonsiirron historia) Radioaaltojen havaitseminen olikin langattomuuden läpimurto, joka myöhemmin johti myös muihin keksintöihin kuten morsetukseen, radiopuhelimiin, kännyköihin, satelliitteihin, erilaisiin tiedonsiirtotekniikoihin – ja myös langattomiin lähiverkkoihin.

Langattomien lähiverkkojen lähtölaukaus alkaa Motorolan ensimmäisen WLAN-tuotteen (Wireless Local Area Network), Altairin, myötä 1980-luvun puolivälissä. Näihin aikoihin kaikki tuotteet ja uudet tekniikat olivat valmistajakohtaisia kunnes IEEE (Institute of Electrical and Electronics Engineering) aloitti langattoman lähiverkon standardikehityksen vuonna 1990. Ensimmäinen 802.11-standardi julkaistiin vuonna 1997. (Puska 2005, 15) 802.11 määrittelemät nimelliset nopeudet olivat 1 tai 2 megabittiä sekunnissa ja välitystekniikoina käytettiin infrapunaa ja radiotietä. Radiotaajuustekniikoista käytettiin sekä suorasekvenssihajaspektriä (Direct-Sequence Spread Spectrum,

DSSS) että taajuushyppelyhajaspektriä (Frequency-hopping spread spectrum, FHSS). (Wikipedia: IEEE 802.11)

802.11 -standardi kävi kuitenkin nopeasti liian hitaaksi jatkuvasti kehittyvien verkkosovellusten sekä langattomien verkkojen laajentuneen käytön vuoksi. (Wikipedia: IEEE 802.11) Vuonna 1999 IEEE vastasi muuttuneen maailman haasteisiin julkaisemalla 802.11b -standardin, joka nosti nimellisen nopeuden 11 megabittiin sekunnissa. Infrapunayhteys poistettiin, ainoaksi siirtotieksi määriteltiin 2,4 GHz:n radiotaajuudet ja radiolähetyksiin määriteltiin vain DSSS-tekniikka. Uuden standardin edut huomattiin markkinoilla ja se olikin huomattavasti edeltäjäänsä suositumpi. (Puska 2005, 15)

Samana vuonna valmistui 802.11a-standardi, joka siirtyi käyttämään 5 GHz:n taajuuksia verkkoyhteyden nopeuden kasvattamiseksi. 802.11a tarjoaakin jopa 54 Mbit/s teoreettisen nopeuden mutta korkeampi taajuus aiheutti myös kantaman pienentymisen, sillä 5GHz:n taajuusalue on monissa maissa varattu muuhun käyttöön. Standardin merkittävimmäksi alueeksi jäikin vain Yhdysvallat sekä Kanada. Euroopalle 802.11a:n merkitys oli siinä, että standardi esitteli OFDM-monitaajuusmodulointia (Orthogonal Frequency Division Multiplexing, OFDM), jota myöhemmin käytettiin 802.11g-standardissa. (Puska 2005, 16) OFDM-tekniikka perustuu signaalin jakamiseen pienempiin alasignaaleihin, jotka siirtävät tietoa lukuisilla taajuuskanavilla yhtä aikaa. Tätä samaa tiedonsiirtotapaa käytetään mm. ADSL:ssä (Asymmetric Digital Subscriber Line) sekä digitelevisiossa. (Wikipedia: OFDM)

Uusin IEEE:n kehittämä standardi on 802.11g, joka ratifioitiin vuonna 2003. Se tarjoaa edeltäjänsä lailla bittinopeudet 54 Mbit/s saakka, mutta käyttää hyväkseen Euroopassakin vapaassa käytössä olevaa 2,4 Ghz:n taajuutta. (Puska 2005, 16)

802.11-standardien lisäksi IEEE kehittelee jatkuvasti langattomiin lähiverkkoihin tietoturvaan ja palvelunlaatuun liittyviä laajennuksia. (Puska 2005, 16) Näissä laajennuksissa pyritään mm. priorisoimaan tärkeää liikennettä ja sitä kautta vähentämään verkkoviivettä (802.11e), parantamaan tietoturvaa salausmenetelmien avulla (802.11i) sekä nopeuttamaan verkon bittinopeuksia edelleen (802.11n). (IEEE 802.11)

Langattomat lähiverkot -kuten muukin langattomuus- kehittyvät jatkuvasti. Voimme vain arvailla, millaisessa langattomassa maailmassa elämme viidenkymmenen, sadan tai vaikkapa kahden sadan vuoden päästä. Tekniikat ovat kehittyneet huippuvauhtia ja samoin laitteet. Markkinoilla on myös ns. hybridilaitteita, jotka yhdistävät useita langattomuuden eri etuja sen sijaan että tarvitsisi ostaa jokainen laite erikseen. Meillä on esimerkiksi kännyköitä, jotka päivittävät säätilaa, joissa on sisäänrakennettu karttapalvelu, joilla voi ladata musiikkia ja surffailla netissä, päivittää Twitteriä, blogia tai Facebookia. Kaikki helposti, vaivattomasti -ja langattomasti.

3 LANGATTOMIEN VERKKOJEN RAKENNE

Langattomat verkot voidaan luokitella karkeasti neljään eri perustyyppiin: kiinteän infrastruktuurin langattomiin verkkoihin, satelliittien välityksellä kommunikoiviin langattomiin verkkoihin, mobiili-infrastruktuurisiin langattomiin verkkoihin sekä langattomiin verkkoihin, joissa ei ole infrastruktuuria ollenkaan. (Vesanen 2003)

Useimmat nykyverkot kuuluvat kategoriaan yksi, eli niissä langattomat laitteet kommunikoivat kiinteään verkkoon liitettyjen tukiasemien välityksellä. Myös meidän opinnäytetyöhömme kuulunut langattoman verkon rakentaminen kuuluu tähän kategoriaan. Satelliittien välityksellä toimiviin verkkoihin lukeutuvat muun muassa matkapuhelinverkot. Kolmannen tyypin verkossa päätelaitteet kommunikoivat toistimien ja liikkuvien tukiasemien välityksellä ja neljännen kategorian verkot muodostuvat yksinomaan langattomista päätelaitteista. Muun muassa Bluetooth-verkot kuuluvat infrastruktuurittomiin verkkotyyppeihin. (Vesanen 2003)

Useimmissa langattomissa verkoissa tietoa siirretään näkymättömästi ilmatiessä radiotaajuus, eli RF-signaalina. RF-signaali on sähkömagneettinen aalto, joka mahdollistaa tiedonsiirron ilmateitse paikasta toiseen. Tiedonsiirtomenetelmänä voidaan käyttää myös valosignaaleja, joita käytetään yleensä rakennusten välisissä linkeissä ja lyhyen kantaman henkilökohtaisissa lähiverkoissa. Suurin osa valosignaaleja hyödyntävistä langattomista verkoista käyttää infrapunavaloa joka jää taajuutensa vuoksi ihmisen näköalueen ulkopuolelle. (Geier 2005, 76).

Viestinvälityksen tekniikan osalta verkot voidaan jakaa piiri- ja pakettikytkentäisiin. Ensimmäisessä muodostetaan kommunikoinnin ajaksi yhteys, joka pysyy koko ajan varattuna riippumatta siitä kulkeeko yhteydessä dataa vai ei. Toisessa välitettävä data pilkotaan paketeiksi, jotka kulkevat verkossa toisistaan välittämättä ja vastaanottaja kokoaa paketit yhteen. Yhteyttä pidetään yllä silloin kun verkossa on liikennettä. Piirikytkentäiset verkot ovat luotettavampia, sillä yhteys on koko ajan auki, mutta pakettikytkentäinen verkko on taloudellisempi. Internet on kokonaisuudessaan täysin pakettikytkentäinen. (Vesanen 2003)

4 LANGATTOMAN MAAILMAN KÄSITTEITÄ

Langattomat verkot on mahdollista jakaa useaan erilaiseen ryhmään sen perusteella, kuinka laajan fyysisen alueen ne pystyvät peittämään. Verkkojen tyypit vaihtelevat henkilön lähiympäristöstä jopa maailmanlaajuiseen verkkoon.

4.1 Wireless Personal Area Network (WPAN)

Henkilökohtainen lähiverkko (Wireless Personal Area Network, WPAN), voidaan toteuttaa niin langallisesti kuin langattomastikin. Langallisessa henkilökohtaisessa lähiverkossa käytetään tietokoneen väyläportteja ja USB-ratkaisuja rakentamiseen. (Geier 2005, 5)

Langattoman henkilökohtaisen lähiverkon kantama ei ole kovinkaan pitkä, joten verkkoa kutsutaan myös likiverkoksi. Verkko on parhaimmillaan pienessä tilassa, sillä WPANin kantama ei ole enempää kuin 15 metriä. Verkko soveltuu hyvin elektronilaitteiden väliseen kommunikointiin, jossa esimerkiksi kammentietokoneen, kannettavan tai pöytäkoneen tiedot voidaan synkronoida keskenään (kuva 1). WPANIN tarkoituksena on korvata liitäntäkaapelit ja yksinkertaistaa tiedonsiirto kahden käyttäjän välillä. Langattomien henkilökohtaisten verkkojen tiedonsiirtonopeus on alhainen, sillä se voi olla enintään 2 Mbps. (Geier 2005, 5)

Langattomat henkilökohtaiset lähiverkot ovat ihanteellisia pieniin käyttäjälaitteisiin, kuten kannettaviin tietokoneisiin, kuulokkeisiin ja GPS-laitteisiin (Global Positioning System), sillä ne eivät tarvitse toimiakseen paljon akkuvirtaa. WPANin avulla voidaan esimerkiksi kuunnella matkapuhelimella olevaa musiikkia langattomilla kuulokkeilla, joka lisää viihdelaitteen helppokäyttöisyyttä ja vaivattomuutta. (Geier 2005, 5)

Bluetooth, Zigbee ja IrDA (Infrared Data Associationin) ovat yleisempiä langattoman henkilökohtaisen lähiverkon tekniikoita, joista kerrotaan tarkemmin langattomuuden eri toteutustavat osiossa.

Kuva 1: Kodin laitteiden synkronointi tietokoneen kanssa onnistuu langattomien henkilökohtaisten lähiverkkojen ansiosta (webtechnoworld.com, 2010)

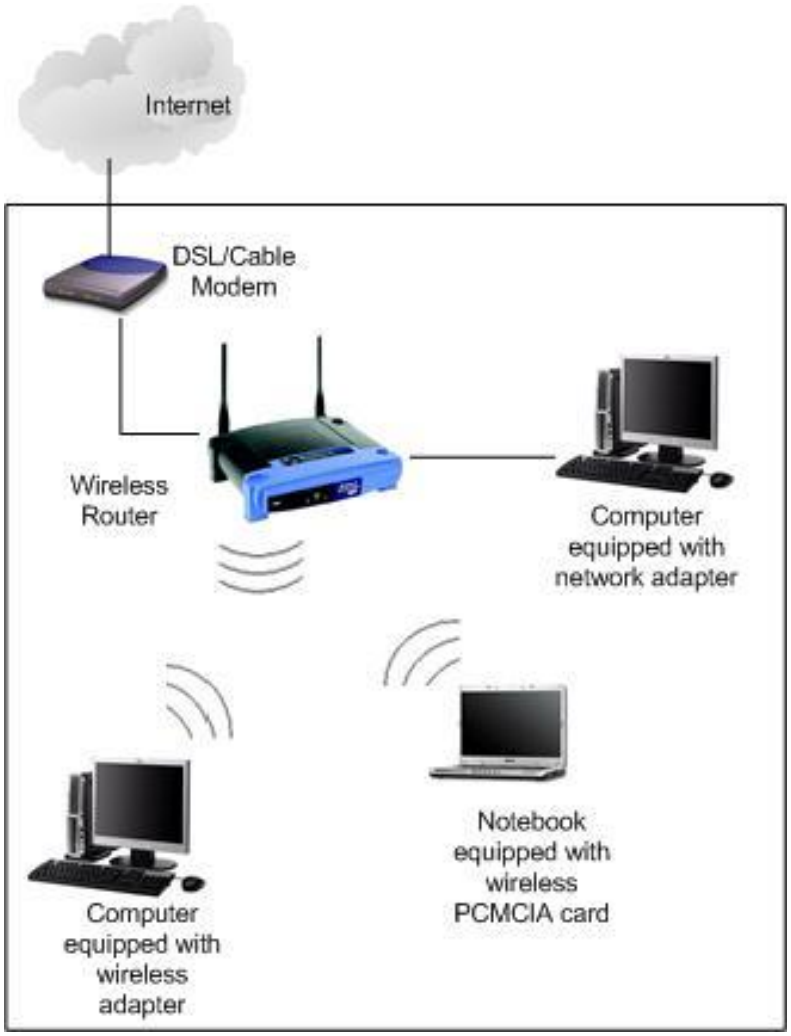
4.2 Wireless Local Area Network (WLAN)

WLANit, eli tuttavallisemmin langattomat lähiverkot, mahdollistavat tietokonelaitteiden yhdistämisen rakennuksen rajoissa. Wlan-verkkojen korkea suorituskyky on niin kotitalouksien kuin yritystenkin saatavilla. Kotitalouksissa langatonta lähiverkkoa käytetään langallisen lähiverkon korvikkeena, jottei asuntoihin tarvitse kaapeloida erillistä sisäverkkoa. Yritykset yleensä tarjoavat työntekijöilleen langattoman lähiverkon kannettavasta tietokoneesta yrityksen sovelluksiin, jotta työntekijä voi työskennellä tehokkaasti myös muualla kuin työpöytänsä äärellä ja hyödyntää verkon palveluita mm. kokoustiloissa (kuva 2). (Granlund 2001, 230) (Geier 2005, 8)

Langattomat lähiverkon tiedonsiirtonopeus voi olla 54 Mbps, joka riittää hyvin toimisto- ja kotiverkkosovellusten tarpeisiin. Suorituskyvyn, rakenneosien ja toimintansa suhteen WLAN muistuttaa perinteisiä langallisia Ethernet-lähiverkkoja. Langattomissa verkoissa käytetään useimmiten laitteiden toisiinsa yhdistämiseen tukiasemaa, mutta myös sovittamilla on mahdollista muodostaa samalla alueella verkko keskenään. Tukiasema antaa helpomman hallittavuuden ja paremman kantomatkan, joten sen käyttö on aina suositeltavaa. (Geier 2005, 9)

Datan kuljettaminen WLAN-verkossa tapahtuu radioaalloilla. Tällä hetkellä yleisimmin käytettävä standardi IEE 802.11 toimii 2.4 GHz avoimella taajuusalueella ja se on ensimmäinen langattoman verkon tekniikka. (Granlund 2001, 230) (Geier 2005, 8)

Kannettavien tietokokeiden, älypuhelinten, taulutietokoneiden ja muiden langattomia verkkoja hyödyntävien laitteiden määrä on huikeasti yleistynyt, joten useat yritykset tarjoavat asiakkailleen langattomia Internet-laajakaista yhteyksiä. Lentokentät, hotellit ja baarit ovat ottaneet langattomien verkkojen tarjoamisen rohkeimmin käyttöön joko maksua vastaan tai ilmaiseksi.



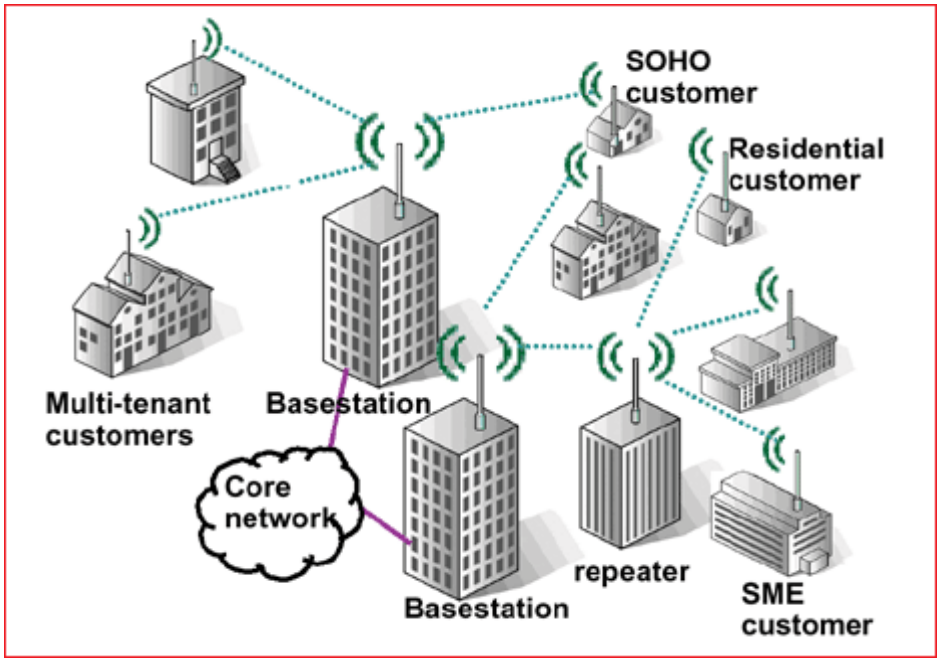
Kuva 2: Langaton lähiverkko (home-network-help.com, 2010)

4.3 Wireless Metropolitan Area Network (WMAN)

WMAN (Wireless Metropolitan Area Network) tarkoittaa langatonta kaupunkiverkkoa, ja ne ovat laajuudeltaan yhden tai useamman kaupungin laajuisia, ja niitä käytetään suurimmaksi osaksi kiinteiden yhteyksien dataverkkoina. Kaupunkiverkkoa hyödyntävät isommat organisaatiot kuten yliopistot, sairaalat ja suuret yhtiöt. Esimerkiksi yritykset voivat käyttää langatonta kaupunkiverkkoa pääpisteen ja sivutoimipaikan väliseen tietoliikenneyhteyteen (kuva 3). (Geier 2005, 9)

Langattomat kaupunkiverkot ovat suuressa hyödyssä silloin kun perinteisiä lankayhteyksiä, kuten DSL (Digital Subscriber Line) ja kaapeli, ei ole mahdollista asentaa edullisesti. Langattomat kaupunkiverkot kaupungissa ja myös niiden ulkopuolella omistavat langattomien Internet-palvelujen tarjoajat. Osa valmistajista hyödyntää langattomien kaupunkiverkkojen perustana IEEE 802.11 -standardia. (Geier 2005, 10)

Langattomien kaupunkiverkkojen todellinen suorituskyky vaihtelee suuresti. Verkon todellinen suorituskyky riippuu siitä millaista teknologiaa ja komponentteja rakentaessa on käytetty. Yhteydet voivat olla parhaimmissa tapauksissa nopeudeltaan yli 150 Gbps, mutta on myös mahdollista että kolmenkymmenen kilometrin mittaiset radiolinkit saattavat toimia vain 100 kbps nopeudella. (Wikipedia: Metropolitan area network)



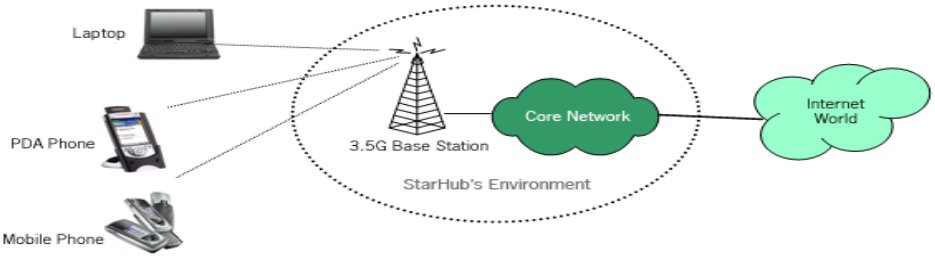
Kuva 3: langattomat kaupunkiverkot (iapplianceweb.com, 2004)

4.4 Wireless Wide Area Network (WWAN)

WWAN (Wireless Wide Area Network) tarkoittaa langattomia laajaverkkoja. Nämä verkkoratkaisut mahdollistavat tiedon siirron laajoilla, kokonaisen maan tai maanosan suuruisilla alueilla. Langattomia laajaverkoja ei tarkoitettu alun perin käytettäväksi sisätiloissa, koska niiden käytössä oleva tekniikka oli suunniteltu lähinnä avoimeen maastoon. Verkko toimii radiosignaaleilla jonka vuoksi työtiloissa, lentokentillä tai muissa rakennuksissa radiosignaali voi olla heikko. Teleoperaattorit asentavat rakennuksiin toistimia parantaakseen verkkojen kattavuutta sisätiloissa, mutta verkon suorituskyky voi siltikin jäädä alhaiseksi. (Geier 2005, 11)

Langattomat laajaverkot voivat parhaimmassa tapauksessa kattaa lähes koko maapallon. Etuina siis onkin laaja peitto ja suuruuden ekonomia, josta seuraa alemmat käyttökustannukset. WWAN verkko saadaan aikaan matkapuhelinsignaaleja käyttämällä. Matkapuhelinpalvelujen tarjoajat ylläpitävät tavallisesti WWAN-verkkopalveluja. WWAN -verkon avulla käyttäjä voi pitää yllä yhteyttä, vaikka olisikin etäällä muunlaisista verkkoyhteyksistä. Langattomaan laajaverkkoon liittyminen on mahdollista kaikkialla, minne on rakennettu matkapuhelinpalveluja tarjoava verkko (kuva 4). (Geier 2005, 11–12)

Suorituskyvyltään langattomat laajaverkot ovat alhaisia, sillä tiedonsiirtonopeudet voivat olla enintään 170 kbps, mutta yleensä nopeus jää modeemin tasolle joka on noin 56 kbps. Alhaisesta tiedonsiirtonopeudesta ei kuitenkaan ole yleensä suurta haittaa, sillä verkkoja käyttävät laitteet ovat lähinnä matkapuhelimia ja näihin videon tai tiedoston siirto voi tapahtua alhaisemmallakin nopeudella. On kuitenkin olemassa erikoistuneita web-portaaleja, joka mahdollistaa tietosisällön siirron pieniin laitteisiin, ja tällöin saadaan WWAN-verkkojen kaistanleveydestä suurin hyöty irti. (Geier 2005, 11–12)



Kuva 4: langattomat laajaverkot (kramfs.com, 2009)

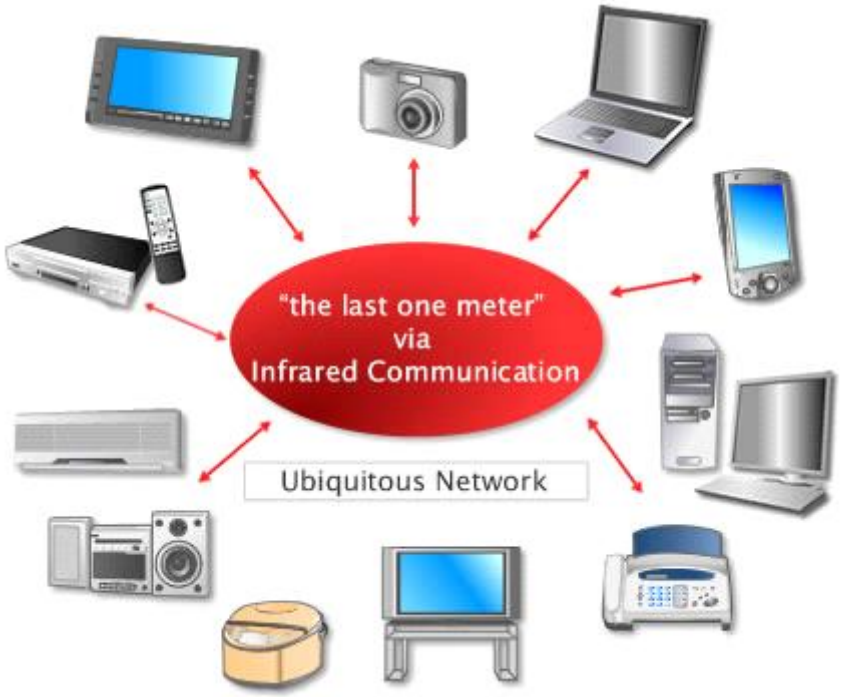
5 LANGATTOMUUDEN ERI TOTEUTUSTAVAT

Langattomuutta voidaan toteuttaa nykyisin monin eri tekniikoin. Langattomat henkilökohtaiset verkot, lähiverkot, kaupunkiverkot ja laajaverkot sopivat erilaisiin käyttötarpeisiin ja täydentävät hyvin toisiaan. Langattomien verkkojen teknologiat ja standardit eroavat toisistaan selvästi. Langattomat henkilökohtaiset lähiverkot rakentuvat valtaosin IEEE 802.15:een tai Bluetoothiin kuin taas langattomat lähiverkot käyttävät IEEE 802.11 tekniikkaa. Langattoman verkon käyttöönotossa on hyvä ottaa huomioon laitteiden resurssit ja valita verkkotyyppi, joka mahdollistaa asetetut vaatimukset parhaiten. (Geier 2005, 13) Standardista 802.11 kerroimme langattomuuden historiaa käsittelevässä kappaleessa, joten pureudumme tässä osiossa nyt muihin langattomuuden eri tekniikoihin.

5.1 Infrared Data Association

Vuonna 1993 osa elektroniikka-alan yrityksiä perusti Infrared Data Association-nimisen (IrDA) yhteisön, jonka päämääränä oli kehittää infrapunasäteilyllä toimiva lyhyen kantaman tietoliikennestandardi. Monissa kannettavissa ja matkapuhelimissa IrDa-liitäntä on ollut jo vuosia sen toimivuuden, turvallisuuden ja edullisuuden vuoksi. IrDa perustuu infrapunavaloon, jonka kantama on enintään yksi metri. IrDa 1.0 siirtonopeus vaihtelee 2400 - 115200 bps välillä, mutta IrDa 1.1 tukee nopeimmillaan jopa 4Mbps saakka. Infrapunavalo ei läpäise seiniä eikä muita esteitä, joten se rajoittaa IrDa-laitteiden kantaman vain näköetäisyyden puitteisiin. Yleisin IrDA:n käyttötarkoitus on kannettavan tietokoneen ja pöytäkoneen helppo yhdistäminen toisiinsa ilman kaapeleita (kuva 5). (Geier 2005, 101)

IrDan etuina kilpailevaan Bluetoothiin on sen kustannustehokkuus, lisensoinnin huolettomuus ja siirtonopeus, joka tulee olemaan suurempi kuin vastaavan radiolaitteen nopeus. (Geier 2005, 101, Granlund 2001, 287)



Kuva 5: IrDa (linkevolution.e-globaledge.com, 2007)

5.2 Bluetooth

Bluetooth SIGin (Special Interest Group) perustivat vuonna 1998 yhteistuumin Nokia, Toshiba, Intel, IBM ja Ericsson. Ryhmän tarkoituksena oli korvata kaapelit luomalla avoin tekniikka lyhyen kantaman radiotekniikalle. Bluetooth ei ole standardi vaan se on tekniikka, jonka päätehtävä on yksinkertaisuus, edullisuus, luotettavuus ja alhainen virrankulutus. Bluetoothilla voidaan yhdistää pienellä alueella lähellä toisiaan olevat tietokonelaitteet kuten matkapuhelimet, mp3-soittimet, kannettavat tietokoneet sekä muut oheislaitteet (kuva 6). Bluethooth ei tarvitse infrapunan tavoin suoraa yhteyttä laitteiden välillä vaan yhdistäminen on mahdollista seinien ja muiden esteiden lävitse. (Granlund 2001, 289) (Geier 2005, 96)

Kiinnostus Bluetooth tekniikkaa kohtaan on vuosien varrella ollut kasvavaa. Ensimmäinen Bluetooth spesifikaatio 1.0 julkaistiin kesäkuussa vuonna 1999 jonka jälkeen sitä on kehitetty versioon 2.0. Tekniset ominaisuudet ovat keskeisiltä osin pysyneet kehityttämisestä huolimatta ennallaan, mutta tiedon siirronnopeutta on pystytty 2.0-version myötä hieman nostamaan. Bluetooth lähetinvastaanottimet toimivat versiosta riippuen 64 kpbs - 1 Mbps nopeudella. (Granlund 2001, 289)

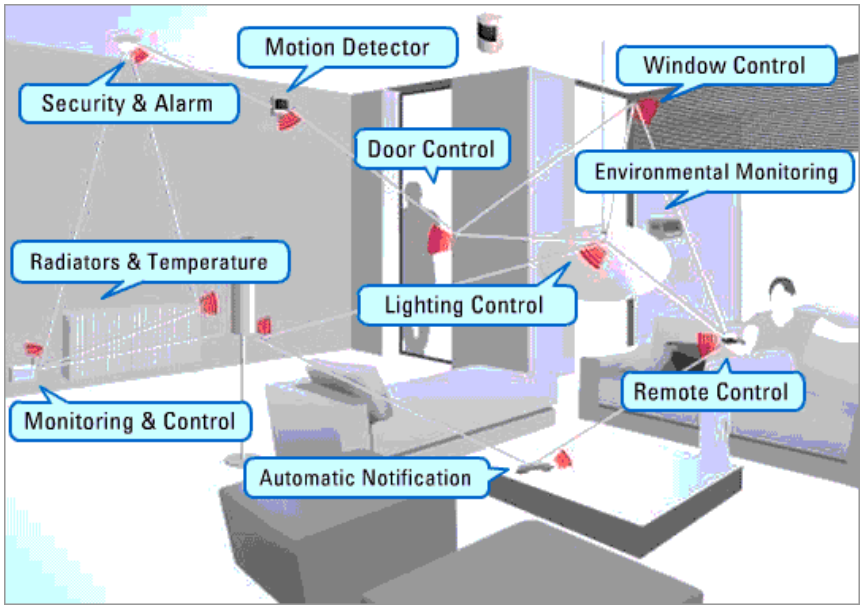
Alhaisen tehon Bluetooth-laitteiden tiedonsiirtoetäisyydet ovat vain muutamia metrejä, mutta suuren tehon Bluetooth-laitteilla kantama voi ulottua kymmenien metrien päähän. Bluetooth mahdollistaa kahdeksan eri laitteet liittämisen samaan verkkoon. Bluetooth-laitteet voidaan määritellä ottamaan yhteys toisiinsa automaattisesti, mutta käyttäjä voi kuitenkin halutessaan manuaalisesti sallia tai estää yhteyden. Yhteyden ollessa puhelimessa päällä ja näkyvissä kaikille, voi laite altistua viruksille, jos käyttäjä hyväksyy saastuneen viestin. (Geier 2005, 97)

Kuva 6: Bluetooth (amitbhawani.com, 2010)

5.3 Zigbee

Zigbee verkkoja alettiin suunnitella vuonna 1998, kun arviointiin että Bluetooth ja IrDa eivät ole sopivia kaikkiin langattomiin käyttötarkoituksiin. Zigbee on IrDan ja Bluetoothin tavoin tarkoitettu pienten ja yksinkertaisten laitteiden verkottamiseen langattomasti. Zigbeellä tarkoitetaan IEEE 802.14-4-standardin mukaista lyhyen kantaman tietoliikenneverkkoa. Zigbee tekniikalla toteutettujen laitteiden pisin mahdollinen kantomatka voi olla noin 100 metriä. (Zigbee.org)

Zigbee-tekniikan ideana on laitteiden äärimmäisen vähäinen virrankulutus, josta voisi olla hyötyä ajatellen muun muassa valaistus-, vartiointi-, lämmitys- ja ilmastointikustannuksia (kuva 7). Zigbee laitteiden menestys on kumminkin ollut pientä, vaikkakin se on standardoitu ja yhteensopiva eri valmistajien laitteiden kanssa. (Zigbee.org)



Kuva 7: Zigbeen mahdollisia käyttökohteita (focus.ti.com, 2010)

5.4 High Performance Radio Local Area Networks

High Performance Radio Local Area Networks eli lyhyemmin HiperLAN on IEEE:n 802.11 tavoin langaton lähiverkko, jonka siirtonopeus on 20–54 Mbps. HiperLAN:in kehittämisen aloitti vuonna 1991 ETSI (European Telecommunications Standards Institute). Vuonna 1999 julkaistiin ensimmäinen HiperLAN-standardi, jota kutsutaan nimellä HiperLAN/1. HiperLAN/1 käyttämä taajuus on 5 GHz ja verkkoyhteyksien enimmäissiirtonopeus 23,5 Mbps. (Geier 2005, 132)

Vuonna 2000 ETSI julkaisi Hiperlan/2-standardin, joka korvasi aikaisemmin kehitetyn Hiperlan/1:sen. Hiperlan/2 – standardin etuna edeltäjäänsä verrattuna on verkon parempi tietoturva ja nopeammat verkkoyhteydet. Hiperlan/2 käyttää Hiperlan/1:sen tavoin 5 GHz taajuutta, mutta verkkoyhteyden nopeus on määritetty 54 Mbps. Hiperlan/2 poikkeaa muista standardeista sillä että se käyttää käyttäjien välisen tiedonsiirron perustana yhteydellistä protokollaa ja aikajakokanavointia. Multimediasovellukset, kuten ääni ja video, käyttävät kyseistä tiedonsiirtomenetelmää tehokkaasti. (Geier 2005, 132)

HiperLan/2-teknologian ainutlaatuinen ominaisuus on sen yhdistettävyys muihin nopeisiin langattomiin verkkoihin kuten 3G, ATM ja muut Internet- protokolla pohjaiset verkot. Suurin hyöty saadaan integroitaessa langattomia lähiverkkoja matkapuhelinjärjestelmiin ja laajaverkkoihin.

2000-luvun alkupuoliskolla esitettiin rohkeita ennusteita HiperLAN/2-tuotteiden yleistymisestä ja käyttöönotosta, mutta HiperLAN/2-tuotteita ei juuri ole kuluttaja-asiakkaille saatavilla. HiperLAN:in suurimpien tukijoiden vetäytyessä pois HiperLAN:ista ei ollut enää kilpailijaksi IEEE:n standardoimalle 802.11 langattomalle lähiverkkostandartille. (Wikipedia: HiperLAN)

5.5 Global System for Mobile

Global System for Mobile, eli GSM, -verkkoa alettiin kehitellä vuonna 1982, jotta saataisiin yhteinen eurooppalainen suositus 900 MHz alueella toimivasta puhelinjärjestelmästä. Vuonna 1990 valmistuivat ensimmäiset GSM-verkkoa koskevat suositukset. GSM -järjestelmä toimii 890–916 MHz ja 935–960 MHz taajuusalueilla sekä 1710–1785 MHz ja 1805 – 1880 MHz taajuus alueilla. (Granlund 2001, 114)

GSM on täysin digitalisoitu ja sen järjestelmän laitteet toimivat kaikissa komitean jäsenmaissa. GSM-verkkoa kutsutaan ns. toisen sukupolven (2G) matkapuhelinverkoksi ja tavallisten puheluiden lisäksi verkossa voi tehdä datapuheluita, lähettää teksti- ja muita lyhytviestejä ja käyttää pakettidatapalveluja. (Granlund 2001, 114)

Suomessa lisättiin vuonna 2001 matkapuhelinverkkoihin tietoliikennettä varten GPRS-pakettiradiopalvelu (General Packet Radio Service). GPRS mahdollistaa internet-yhteyden muodostamisen matkapuhelimella tai GPRS-sovittimen avulla. Teoriassa GPRS:llä on mahdollista saavuttaa 114 kb/s tiedonsiirtonopeus verkosta laitteelle, mutta käytännössä se jää alle 50 kb/s. GPRS:an avulla haluttiin parantaa matkapuhelinten WAP- (Wireless Application Protocol) ja Internet-palveluiden toimivuutta ja mahdollistaa tiedon siirto sekä vastaanotto tarvittaessa. (Wikipedia: GSM)

Vuonna 2003 otettiin GSM-verkossa käyttöön toinen pakettikytkentäiseen tiedonsiirtoon suunniteltu tekniikka EDGE (Enhanced Data rates for Global Evolution). EDGE:n avulla voidaan kasvattaa radiotiellä siirrettävän tiedon määrää muuttamatta GSM-verkon rakenteita. EDGE-standardi mahdollistaa GPRS-standardia nopeamman tiedonsiirtonopeuden joka on loppukäyttäjillä keskimäärin 160–296 kb/s luokkaa vastaanottosuunnassa ja lähetyssuunnassa vastaavasti saavutetaan keskimäärin 80–236,8 kb/s nopeus. GPRS -standardiin verrattaessa nopeus on keskimäärin kolmin- tai nelinkertainen. (Granlund 2001, 198)

5.6 Universal Mobile Telecommunications System

UMTS (Universal Mobile Telecommunications System) on GSM -verkon seuraajaksi rakennettu kolmannen sukupolven matkapuhelinteknologia. Tästä syystä verkkoa kutsutaan yleisemmin nimellä 3G. UMTS on alusta asti suunniteltu nopeamman datan siirtoon ja se tarjoaakin 384 kb/s latausnopeuden signaalin laadusta, verkon ruuhkasta ja muista tekijöistä riippuen. Käytännössä käyttäjätasolla nopeudet jäävät noin 100–250 kb/s. (Granlund 2001, 203)

Euroopassa ja Japanissa on käytössä UMTS-taajuusalueista 2100 MHz alue, joka on tuetuin nykyisissä päälaitteissa. Osassa Euroopan maista, kuten Suomessa, on käytössä myös 900 MHz alue joka mahdollistaa laajentamisen kustannustehokkaasti hyödyntäen GSM-verkkoja varten rakennetut mastopaikat. (Wikipedia: UMTS)

6 LANGATTOMIEN LÄHIVERKKOJEN TIETOTURVA

Tietoturva on elintärkeä asia, olipa kyse sitten mistä tahansa tiedonsiirrosta. Langattomien lähiverkkojen tietoturvariskit ovat pääasiassa samanlaisia mitä perinteisissä lähiverkoissa, mutta langattomuus tuo asiaan uusia haasteita ja painotuksia. (Puska 2005, 69) Langattomuuden etuna olevat ilmassa liikkuvat signaalit ovat myös niiden haittapuoli; signaalit ovat avoimesti tavoitettavissa, koska niiden ympärillä ei ole mitään niitä suojaamassa. (Geier 2005, 171)

6.1 Tietoturvan tavoitteet

IETF (Internet Engineering Task Force) on määritellyt kuusi tavoitetta, joita tietoturvalla lähdetään hakemaan. Nämä niin sanotut turvapalvelut soveltuvat hyvin myös langattomien lähiverkkojen turvavaatimuksiksi. (Puska 2005, 70)

Tiedon luottamuksellisuus (Confidentiality)

Tiedon luottamuksellisuudella tarkoitetaan sitä, että verkossa liikkuva data pysyisi poissa sellaisten ihmisten ulottuvilta, joille se ei kuulu. Käytännössä tämä tavoite voidaan toteuttaa muun muassa erilaisilla kryptauskeinoilla. (Prasad & Prasad 2005, 97) Se, että verkossa liikkuvaa tietoa voi lukea ja välittää vain siihen oikeutetut henkilöt, on ehdottomasti yksi tietoturvallisen viestinnän peruskivistä. (Puska 2005, 70)

Tiedon eheys (Integrity)

Tiedon eheyteen voidaan luottaa silloin, kun estetään datan muokkaaminen kaikilta muilta henkilöiltä, paitsi niiltä joilla pitäisi olla kyseiset oikeudet. Vaatimus koskee datan muokkaamista, poistamista, käsittelyä, luomista sekä sen siirtämistä eteenpäin. (Prasad & Prasad 2005, 97)

Todennus (Authentication)

Todennuksen merkitys on, että kaikki tehdyt toimenpiteet ja kommunikaatio joko ihmisten tai laitteiden kesken voidaan todentaa myös jälkeenpäin (Puska 2005, 70), ja että esimerkiksi keskustelun osapuolet ovat niitä henkilöitä joita väittävät olevansa, eikä heidän väliinsä mahdu kolmatta osapuolta. (Prasad & Prasad 2005, 97)

Kiistämättömyys (Non-repudiation)

Kiistämättömyys ja todennus ovat tietoturvan tavoitteina hyvin lähellä toisiaan. Kiistämättömyydellä tarkoitetaan esimerkiksi sellaista tilannetta, missä viestin lähettäjä voi todistaa että viesti on lähtenyt häneltä ja viestin vastaanottaja voi todistaa, että viesti on saapunut perille sille henkilölle jolle sen pitikin saapua. (Prasad & Prasad 2005, 97-98)

Pääsynhallinta (Access Control)

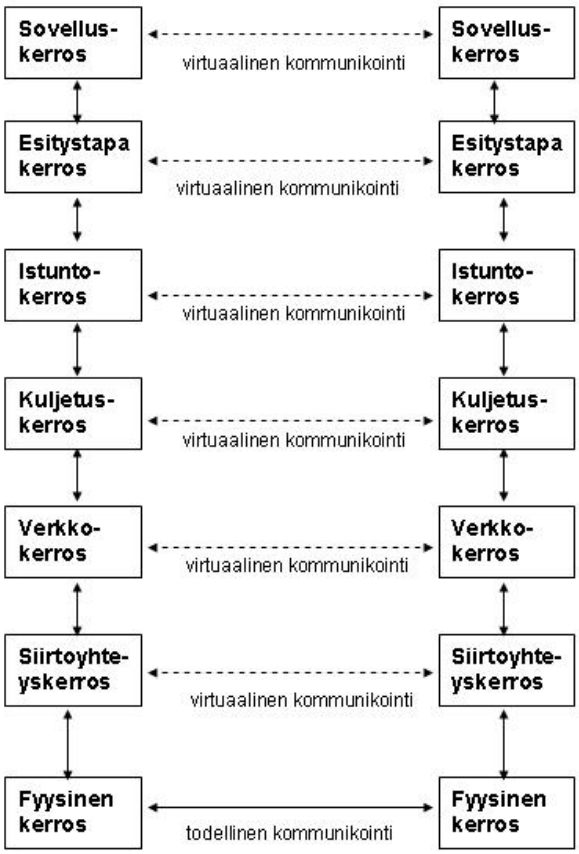
Pääsynhallinnalla rajoitetaan tai estetään asiattomien henkilöiden pääsy verkkoon ja sen resursseihin, kuten erilaisiin sovelluksiin. Käyttäjän todentaminen käy käsi kädessä pääsynhallinnan kanssa, sillä käyttäjän on ensin kirjautumisellaan todistettava ”henkilöllisyytensä” ennen kuin hänelle annetaan (tai evätään) pääsy verkkoon. (Prasad & Prasad 2005, 97)

Käytettävyys (Availability)

Käytettävyydellä tarkoitetaan sitä, että kaikki käyttäjien ulottuvilla oleva tieto (johon heillä on oikeudet) on saatavilla ja käytettävissä sovittuina aikoina kaikissa olosuhteissa. (Puska 2005, 70)

6.2 Tietoturvauhat

Langattoman verkon vaatimia tietoturvapiirteitä voidaan tarkastella paremmin sen mukaan, millä protokollatasolla hyökkäys tapahtuu. Tietoverkon toimintaa kuvaava OSI (Open Systems Interconnection)-malli auttaa hahmottamaan tiedon kulkemista, vaikkakin on muistettava että malli on abstraktio ja kerrosten rajat voivat olla häilyvät (Vesanen 2003).



Kuva 8: OSI-malli (Vesanen / Oulun yliopisto 2003)

Tiivistettynä kerrokset vastaavat seuraavista tehtävistä:

- Sovelluskerros: käyttäjälle näkyvien sovellusten viestintä.
- Esitystapakerros: yhtenäinen esitystapa datalle, esimerkiksi merkistöjen koodaukset ja tietojen pakkaaminen.
- Istuntokerros: yhteyksien muodostaminen ja purkaminen
- Kuljetuskerros: datan kuljetuspalvelu, eli huolehtii siitä, että paketit tulevat perille
- Verkkokerros: pakettien reititys, niin sanottu päästä-päähän yhteys eri verkkolaitteiden välillä.

- Siirtoyhteyskerros: organisoi bittejä niin sanottuihin kehyksiin.
- Fyysinen kerros: määrittelee tiedonsiirron fyysisen median ja siirtää käsittelemätöntä bittivirtaa.

Tietoturvahyökkäykset kohdistuvat yleensä kolmeen kerrokseen: fyysiseen-, kuljetus- ja sovelluskerrokseen. Fyysisen kerroksen hyökkäyksiin lukeutuvat muun muassa signaalin ja/tai laitteiden sieppaaminen, vakoilu ja salakuuntelulaitteet. Suurimmat osat hyökkäyksistä alkavat fyysiseltä kerrokselta, kun verkko paljastuu hyökkääjille. Kuljetuskerroksella tapahtuvia hyökkäyksiä voivat olla esimerkiksi palvelunestohyökkäykset ja sovelluskerroksella ongelmia voivat aiheuttaa haittaohjelmat, kuten virukset, madot, troijalaiset ja etähallintaohjelmat. Toisaalta, OSI-mallin kerrosten rajat eivät ole kirveellä veistettyjä joten esimerkiksi madot voidaan laskea kuuluvaksi myös verkkokerroksen hyökkäyksiin. (Vesanen 2003)

Langattomien (ja langallistenkin) verkkojen vakavin hyökkäystyyppi on hyökkäys, joka murtaa viestien tai käyttäjätietojen salauksen. Tätä hyökkäystä kutsutaan nimellä kryptografinen hyökkäys ja onnistuessaan hyökkääjä voi pahimmillaan saada täydet oikeudet toimia koko verkossa. Kryptografisen hyökkäyksen mahdollistavat usein virheet sovellus- tai kuljetuskerroksella, jolloin hyökkääjä voi saada haltuunsa esimerkiksi osan käytetystä salausvaimesta. Nämä hyökkäykset edellyttävät hyökkääjältä suurta asiantuntemusta, sillä useimmat käytössä olevat salausjärjestelmät ovat erittäin hankalia murtaa, vaikka hyökkääjä saisikin osan salaisista tiedoista haltuunsa. (Vesanen 2003)

Langattomiin lähiverkkoihin kohdistuvat uhat voidaan karkeasti jakaa kahteen eri ryhmään: passiivisiin- ja aktiivisiin uhkiin. Passiivisina uhkina pidetään tilanteita, joissa hyökkääjä ei häiritse tai kuormita verkkoa, vaan koittaa kerätä verkossa liikkuvia henkilökohtaisia tietoja. Näitä tietoja voivat olla esimerkiksi käyttäjätunnukset ja salasanat, joita hyökkääjä voi käyttää myöhemmin omaksi edukseen. Aktiivisiin uhkiin lukeutuvat ne hyökkäykset, joissa verkkoon tunkeutuja koittaa häiritä verkon normaalia toimintaa, muokata verkossa kulkevaa dataa tai lamauttaa koko verkon. (Prasad & Prasad 2005, 95) Passiiviset, eli epäsuorat, hyökkäykset verkkoon voivat olla hyvinkin vaikeasti havaittavia, koska ne voivat olla täysin passiivista datan tarkkailua. Tämänkaltainen hyökkäys voi kuitenkin johtaa aktiiviseen, eli suoraan, hyökkäykseen mikäli tunkeutujat saavat selville esimerkiksi tärkeitä salasanoja. Hyökkäysten vaikutukset voivat tekotavasta ja tarkoitusperästä riippuen ulottua pienestä kiusasta katastrofiin. (Vesanen 2003)

Tietojen peukalointiin liittyvät hyökkäykset voidaan jakaa sisältöhyökkäyksiin ja temporaalisiin hyökkäyksiin. Sisältöhyökkäyksissä muutetaan tietojen sisältöä, kun taas temporaalisissa hyökkäyksissä pyritään vaikuttamaan tietojen ajanmukaisuuteen. Voidaan esimerkiksi aiheuttaa vanhentuneiden tietojen hyväksymistä asianmukaisina tietoina viivyttämällä viestien perille menoa. (Vesanen 2003)

Seuraavaksi vielä kerrottuna muutamista verkkoon kohdistuvista passiivisista- ja aktiivisista uhista.

Passiiviset uhat

Salakuuntelu

Salakuuntelu kaikissa muodoissaan on ollut yksi ihmiskunnan salaisuuksien varjelun suurimpia ongelmia jo vuosisatojen ajan. Tämä hyökkäys on nimensä mukaisesti sitä, että hyökkääjä ”kuuntelee” verkosta sellaista liikennettä, joka ei hyökkääjälle kuulu. (Prasad & Prasad 2005, 96) Tarkoituksena on kerätä tietoja, jotka voivat myöhemmin auttaa verkkoon tunkeutumisessa. (Puska 2005, 69) Jopa aivan satunnainen, utelias ohikulkija voi helposti tarkkailla suojaamattomissa langattomissa verkoissa liikkuvia datapaketteja erilaisilla hakkerointisovelluksilla ja -työkaluilla. Verkon liikenteestä kiinnostunut nuuskija voi seurata verkon tapahtumia etäältäkin ja saada tietoonsa käyttäjätunnuksia, salasanoja ja muita henkilökohtaisia tietoja joita verkossa liikkuu. Salakuuntelua on mahdoton havaita, mutta sitä voidaan estää tai ainakin vähentää käyttämällä asiakaslaitteen ja tukiaseman välillä salausta, joka muuttaa datavirran bitit tunnistamattomaksi. (Geier 2005, 172)

Liikenteen analysointi

Tämä on hienovarainen hyökkäys verkkoon, jossa hyökkääjä voi haluta saada tietoonsa ainoastaan esimerkiksi sen, kuka lähettää viestejä kenelle ja kuinka usein, viestin sisältöön koskematta. (Prasad & Prasad 2005, 96) Verkon liikenteen analysointi voi paljastaa verkosta myös luottamuksellista tietoa, kuten suojausasetukset tai salausavaimet. (Puska 2005, 69)

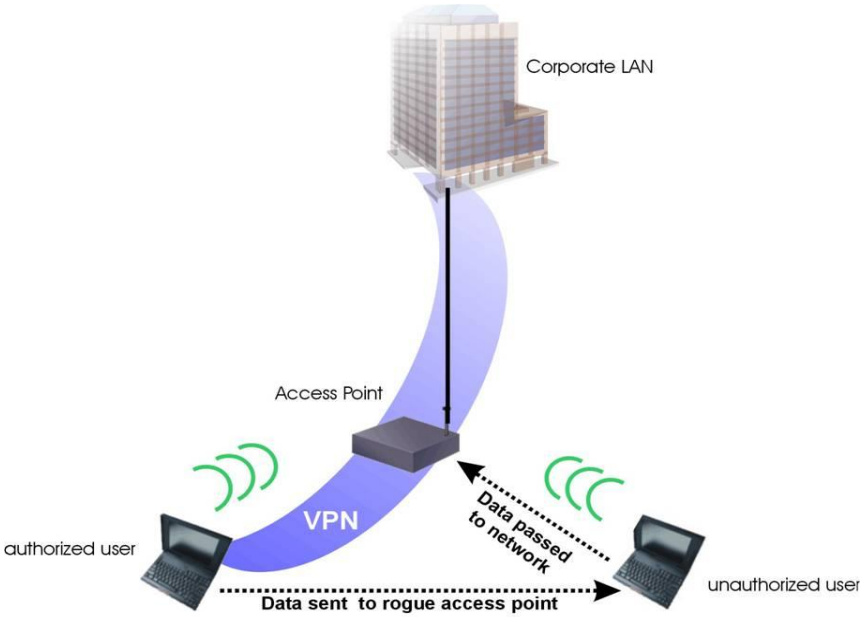
Aktiiviset uhat

Tekeytyminen toiseksi käyttäjäksi

Hyökkääjä teeskentelee olevansa luvallisesti verkossa oleva käyttäjä. Tämänkaltainen hyökkäys on mahdollinen, mikäli hyökkääjä on esimerkiksi saanut haltuunsa hyökkäyksen kohteena olevan käyttäjän käyttäjätunnuksen ja salasanan (Prasad & Prasad 2005, 96)

Välistävetohyökkäys

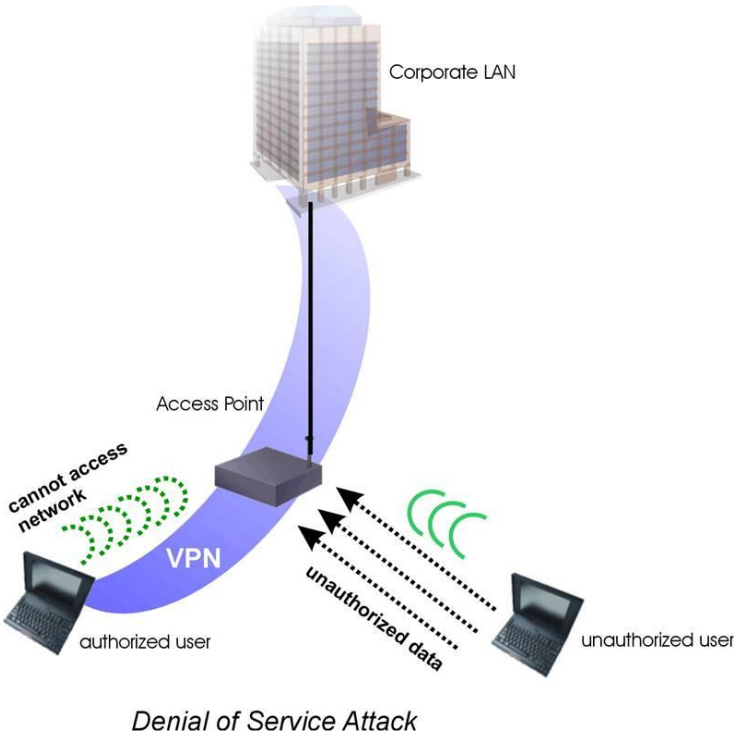
Välistävetohyökkäys eli man-in-the-middle-attack on nimensä mukaisesti tietoturvahyökkäys, jossa hyökkääjä asettaa valelaitteen kahden osapuolen verkon väliin (kuva 9). (Geier 2005, 174) Yleensä tarkoituksena on verkossa liikkuvan datan muokkaaminen. Välistävetohyökkäykset voidaan torjua salaamalla liikenne siten, että yhteyden alussa laitteet vaihtavat yhteisen ”salaisuuden” (salausavaimen) jolloin sekä lähettäjä että vastaanottaja voivat varmistua siitä, että toinen osapuoli ei ole huijari. Tunkeutumisyritykset huomataan kun pakettien tarkistussumma ei täsmää ja hyökkääjän muokkaamat paketit tiputetaan verkosta pois. (Puska 2005, 69)



Kuva 9: Välistävetohyökkäys (interlinknetworks.com)

Palvelunestohyökkäys

Palvelunestohyökkäys eli DoS (Denial of Service) on siirtomedian häirintää joka voidaan toteuttaa esimerkiksi ylikuormittamalla WLAN-yhteyspisteitä tai muita verkon laitteita tai palvelimia turhilla liityntä- tai palvelupyynnöillä (kuva 10). (Puska 2005, 69) Palvelunestohyökkäys voi rampauttaa tai kaataa koko verkon, josta kotikäyttäjälle ei yleensä aiheudu muuta kuin päänvaivaa ja pahaa mieltä, mutta yritystasolla se voi aiheuttaa suuriakin taloudellisia tappioita. (Geier 2005, 176) Yksinkertaisimmillaan palvelunestohyökkäys voi olla tuhansien sähköpostien lähettäminen yrityksen sähköpostipalvelimelle ja tämänkaltainen hyökkäys on helposti toteutettavissa. Muista hyökkäystyypeistä poiketen DoS-hyökkäyksen tavoite ei ole verkkoon tunkeutuminen tai tietojen urkkiminen, vaan verkon toiminnan häiritseminen. (Wikipedia: palveluestohyökkäys) Verkon häirinnältä ja palvelinestohyökkäyksiltä voi parhaiten välttyä eristämällä verkko ulkopuolisilta häiriöiltä ja rajoittamalla palvelupyyntöjen määrää. (Puska 2005, 69)



Kuva 10: Palvelunestohyökkäys (interlinknetworks.com)

7 LANGATTOMAN LÄHIVERKON SALAUSMETODIT

Salauksen avulla muutetaan datapaketin bittejä, jotta tiedonsiirto ja kirjautuminen olisivat turvallista langattomassa lähiverkossa. Salaus muuttaa selväkielisen tekstin salatuksi, jolloin sitä ei voida purkaa muuta kuin oikealla salausavaimella. Verkon salaustapoja on useita, joista osa on huomattavasti helpompi murtaa kuin toiset. (Geier 2005, 181)

7.1 Wired Equivalent Privacy

WEP (Wired Equivalent Privacy) oli ensimmäinen 802.11-standardin mukana tullut salausprotokolla, joka on nykypäivänä jo vanhentunut ja osoittautunut alttiiksi verkkohyökkäyksille. WEP ei tarjoa riittävää tietoturvaa, sillä se perustuu RC4-nimiseen salausalgoritmiin, joka lähettää joidenkin pakettien kehyksissä salaamattomia bittejä, niin sanottuja alustusvektoreita, joiden avulla voidaan helposti purkaa käytetty salausavain. (Gaier 2005, 182)

WEP-salauksen ongelmat eivät ainoastaan liity RC4-salausalgoritmiin, vaan WEP:in heikkous salausmenetelmänä WLAN-verkoille perustuu sen salaamattomaan 24-bittiseen alustusvektoriin. Alustusvektori voi suuresti liikennöidyssä verkossa toistua lyhyessäkin ajassa, joka nopeuttaa salausavaimen selvittämistä. Mikäli tunkeutuja onnistuu keräämään riittävän määrän kehyksiä, jotka perustuvat samaan alustusvektoriin, on hänen mahdollista päätellä salauksessa käytetty avain. WEP-salausta ei suositella käytettäväksi verkkoihin joissa on paljon liikennettä, mutta koti- ja pienyritys käytössä se kuitenkin pitää useimmat tunkeilijat hyvin loitolla. (Geier 2005, 182)

7.2 Temporal Key Integrity Protocol

TKIP (Temporal Key Integrity Protocol) on langattomien lähiverkkojen tietoturvaprotokolla, joka korjaa WEP:in sisältämän avaimen uusiokäytöstä syntyvän ongelman. Monissa langattomien lähiverkkojen tuotteissa TKIP on pääsääntöisesti jo oletuksena. TKIP käyttää 128-bittistä avainta, jonka se luo ensin väliaikaiseksi. TKIP yhdistää väliaikaisen avaimen käyttäjän MAC-osoitteen (Media Access Control) kanssa ja lisää 16 oktetin alustusvektorin tuottaakseen avaimen, jolla lopulta data salataan. Tällä menetelmällä

voidaan varmistaa, että jokainen asema käyttää datan salaamisessa eri avainmerkkijonoa. (Gaier 2005, 183)

Keskeisin ero WEPin ja TKIPin välillä on väliaikaisten avainten vaihtaminen aina 10 000 paketin välein. Tällä menetelmällä voidaan parantaa merkittävästi verkon turvallisuutta. (Gaier 2005,182)

7.3 Advanced Encryption Standard

AES (Advanced Encryption Standard) on 802.11-standardin salausprokotolla, joka mahdollistaa TKIP:iä paljon vahvemman salauksen. AES ei käytä RC4- salausalgoritmia vaan korvaa tämän erittäin vahvalla Rine Dale –salausalgoritmilla. AES vaatii TKIP:ia enemmän prosessoritehoja, joten vanhimmat käytössä olevat tukiasemat eivät välttämättä tue AES-salausprotokollaa. (Gaier 2005, 184)

AES-salausta pidetään murtumattomana, joten mm. Yhdysvaltojen hallinnon organisaatiot käyttävät AES:aa suojatakseen arkaluontoisen, mutta salaamattomaksi luokitellun informaation. Yhdysvaltain kauppa- ja teollisuusministeriö on hyväksynyt AES:n viralliseksi hallinnon standardiksi vuonna 2002. (Gaier 2005,184)

7.4 Wi-Fi Protected Access

WPA (Wi-Fi Protected Access) on Wi-Fi Alliancen luoma standardi, joka kehitettiin WEP-salauksen ongelmien paljastuttua. WPA on kehitetty mahdollistamaan eri valmistajien laitteiden yhteensopivuus samassa ympäristössä. Julkisella langattomalla palvelualueella voidaan hyödyntää parhaiten WPA-pohjaisia salausmuotoja, sillä tällaisessa ympäristössä on käytössä monia erityyppisiä 802.11-radioverkkokortteja. (Gaier 2005, 184)

WPA on WEP:in päivitys, joka mahdollistaa dynaamisen avaimen salauksen ja kaksisuuntaisen todennuksen. WPA:sa on käytössä TKIP- ja 802.1x- mekanismit. Ensin langattoman verkon käyttäjä todentaa itsensä tukiasemalle, jonka jälkeen WPA suorittaa käyttäjätason todennuksen 802.1x:llä, jolloin WPA ottaa yhteyden yrityksen niin sanottuun todennuspalvelimeen, eli RADIUS-palvelimeen. WPA pystyy toimimaan myös ilman todennuspalvelinta esimerkiksi kotitalouksissa ja pientoimistoissa, jolloin käyte-

tään niin sanottua etukäteen jaettua avainta. (Geier 2005, 184)

7.5 Wi-Fi Protected Access 2

Vuonna 2004 julkaistiin uusi Wi-Fi Protected Access 2 eli WPA2-salausmenetelmä, jota kutsutaan myös nimellä IEEE 802.11i. WPA2 tarjoaa samat ratkaisut kuin aiempi WPA-standardi, mutta eroaa edeltäjästänsä sillä että se käyttää uudenlaista salausmekanismia AES:ää. (Wikipedia: IEEE 802.11i)

7.6 Media Access Control – suodattimet

Useimmat langattoman verkon tukiasemat tarjoavat mahdollisuuden Media Access Control (eli MAC)-suodatukseen, jolloin tukiasema tutkii asiakaslaitteiden MAC-osoitteet ja estää niiden laitteiden yhteydet, joiden MAC-osoitetta ei löydy järjestelmänvalvojan luomasta listasta. (Geier 2005, 187)

MAC-suodatusta ei voida pitää kovin turvallisena suojauksena, sillä WEP -salaus ei salaa kehyksen MAC-osoitekenttää ja tästä syystä se voi joutua helposti vääriin käsiin. Internetissä on vapaasti saatavilla ohjelmia, joilla hakkerit voivat muuttaa radioverkkokorttien MAC-osoitteet vastaamaan oikeita. Oikean MAC-osoitteen saatuaan hakkereiden on helppo naamioitua verkon käyttäjäksi silloin kun oikea käyttäjä ei ole verkossa. (Geier 2005, 187)

MAC-osoitesuodatus voi olla ihan riittävä suojaus koti- ja pientoimisto käyttöön, mutta paljon manuaalista työtä vaativan luonteensa vuoksi se ei sovellu laajoihin langattomiin yritysverkkoihin. (Gaier 2005, 187)

7.7 IEE 802.1X

802.1x:n porttikohtainen todentaminen on IEEE:n 802.1X:n standardi, joka mahdollistaa tehokkaan suojauksen Ethernet- ja WLAN-verkoissa. 802.1X tarjoaa automaattisen todennuksen ja valvonnan lisäksi myös dynaamisen salausavainten muuttamisen. 802.1X:sen tarkoituksena on estää verkon luvaton käyttö liityntäpisteen, esimerkiksi kytkimen tai tukiaseman kautta. (Geier 2005, 188)

802.1x toiminta alkaa kun tuntematon langaton laite yrittää muodostaa yhteyden langattomaan tukiasemaan. Tukiasema avaa portin, mutta sallii vain EAP (Extensible Authentication Protocol)-paketit käyttäjältä todennuspalvelimelle, joka sijaitsee tukiaseman sisäverkon puolella. Tukiasema estää HTTP (Hypertext Transfer Protocol), DHCP *(*Dynamic Host Configuration Protocol) ja POP3-paketit (Post Office Protocol version 3) kunnes tukiasema varmentaa asiakkaan identiteetin todennuspalvelimen, esimerkiksi RADIUS-palvelimen, kautta. (Geier 2005, 189)

8 REMOTE AUTHENTICATION DIAL IN USER SERVICE (RADIUS)

RADIUS-protokolla kehitettiin, koska oli tarve saada keino autentikointiin, valtuutukseen ja tilastointiin, joita käytetään erilaisissa tietokoneresursseissa. (networksorcery.com)

RADIUS-autetintikointi prosessiin sisältyy kolme osapuolta: Asiakaskone, NAS-laite (esimerkiksi kytkin, joka on konfiguroitu RADIUS-asiakkaaksi) sekä RADIUS-palvelin. Autentikointiprosessi alkaa kun asiakaskone yrittää päästä verkkoon NAS-laitteen kautta. Tällöin laite lähettää RADIUS Access-Request -pyynnön palvelimelle. Jos asiakaskone ei saa vastausta lähettämäänsä pyyntöön RADIUS-palvelimelta tietyn ajan sisällä, lähetetään kyseinen pyyntö uudelleen. Isoissa verkoissa voi olla useita RADIUS-palvelimia, jolloin ensisijainen palvelin vastaanottaa lähetetyt pyynnöt. Jos ensisijainen palvelin ei jostain syystä vastaa, pyyntö siirtyy seuraavaksi suurimman pistemäärän omaavalle palvelimelle. Kun palvelin vastaanottaa pyynnön, se joko autentikoi käyttäjän (pääsy verkkoon) tai jättää asiakkaan verkon ulkopuolelle. (networksorcery.com)

9 NETWORK ACCESS PROTOCOL (NAP)

Network Access Protocol eli NAP on Microsoftin kehittämä sääntöpohjainen käyttöoikeuksia valvovan tekniikka, jolla voidaan suojata verkko saastuneilta ja vaarallisilta tietokoneilta. NAP-suojaus mahdollistaa Windows-verkoissa tietoturvallisuusehtojen asettamisen NAP-yhteensopiville työasemille ja näin rajoittamaan saastuneiden koneiden pääsyä lähiverkkoon. Jos työasema ei ole turvallinen, NAP mahdollistaa automaattisen päivityksen vaadittavalle tietoturvatasolle. Päivityksen jälkeen käyttäjä voi halutessaan liittyä verkkoon uudelleen ja käyttää sitä normaalisti. (Davies & Northrup 2008, 572)

Windows Vista- ja Windows 7 – käyttöjärjestelmissä NAP-clientit ovat valmiiksi asennettuna. Windows XP Service Pack 3-käyttöjärjestelmä mahdollistaa myös NAP-clientin käytön erillisenä päivityksenä. NAP tulee vakiona Windows 2008 – käyttöjärjestelmässä, mutta muiden valmistajien tuotteisiin tarvitaan päivityksiä, jotta ne tulevat toimimaan NAP-suojauksen kanssa. (Davies & Northrup 2008, 568)

NAP:lla on kolme tärkeää ominaisuutta verkon suojaamiseen:

- Terveydentilan tarkistaminen. Verkon ylläpitäjä määrittää verkkoon ehdot, jotka työasemien pitää täyttää. Jos työasema ei saavuta tarvittavia ehtoja, ylläpitäjä päättää mitä työasemalle tehdään.
- Terveydentilan korjaaminen. Saastuneet työasemat päivitetään automaattisesti erillisten ohjelmistohallintaohjelmien avulla.
- Verkkoon pääsyn rajoittaminen. Rajoitetaan käyttäjän pääsy tuotantoverkkoon niiltä työasemilta jotka ovat saastuneet. Työaseman turvallisuustarkistuksen perusteella, NAP voi myöntää sille pääsyn verkkoon täysin oikeuksin, ohjata työaseman erilliseen verkkoon tai estää pääsemästä verkkoon kokonaan. Työasemat jotka eivät tue NAP-teknologiaa, voidaan sallia tai estää verkkoon pääsy kokonaan. (Davies & Northrup 2008 , 572)

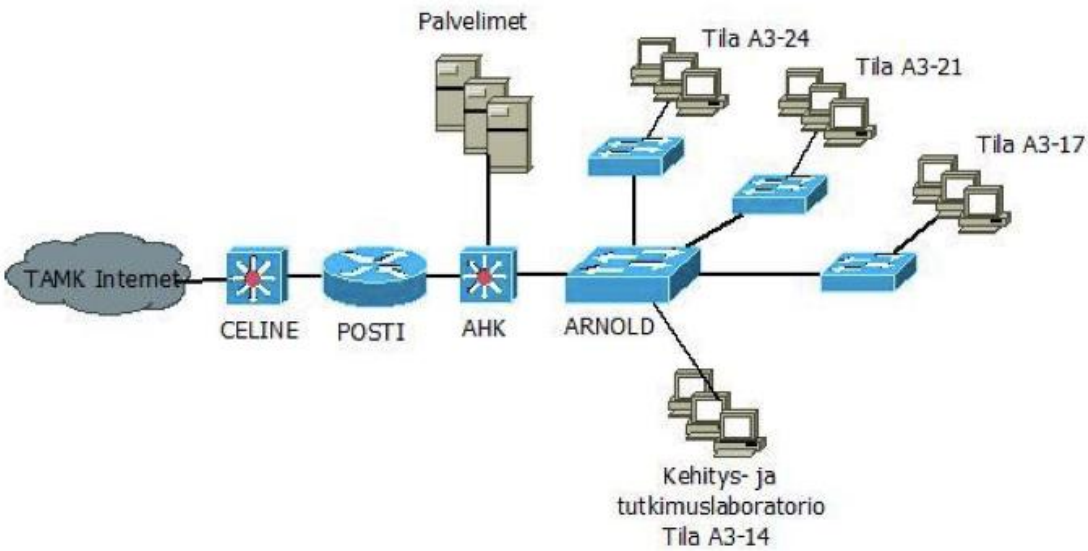
10 WPK-VERKKO

Pirkanmaan ammattikorkeakoulun ja Tampereen ammattikorkeakoulun yhdistymisen myötä uudessa Tampereen ammattikorkeakoulussa, eli TAMKissa, on noin 10 000 opiskelijaa. Näitä opiskelijoita koulussamme palvelee kaksi erillistä lähiverkkoa: TAMKin oma, sekä tietoverkkopalveluopiskelijoiden käytössä toimiva, niin sanottu WPK-verkko. Langattomia verkkoja koulussamme on useita, mutta WPK-verkon puolelta langaton jatke vielä uupui.

WPK-verkossa on n. 90 työasemaa ja 6 Windows Server 2008 palvelinta. Reitittimiä verkossa on yhteensä n. 100 ja kytkimiä n. 60 kun lasketaan luokkien opetuskäytössä olevat laitteet myös mukaan. WPK-verkon yhdistymisen TAMKin verkkoon ja sitä kautta pääsyn Internetiin hoitaa Posti-niminen reititin. WPK-verkkoa hyödynnetään koulussamme pääosin CCNA-, CCNP- sekä Microsoftin serverikursseilla.

WPK-verkko ja sen rakenne oli meille molemmille entuudestaan tuttu, sillä olemme molemmat olleet WPK-verkon ylläpitäjinä työharjoittelussa.

Kuvassa 11 yksinkertaistettuna WPK-verkon rakennetta.



Kuva 11: WPK-verkon rakenne

10.1 Langaton WPK

Opinnäyteyömme tarkoituksena oli laajentaa tietoverkkopalveluopiskelijoiden käytössä olevaa WPK-verkkoa turvalliseksi langattomaksi verkoksi johon opiskelijat pääsisivät käsiksi vaikka omilla kannettavilla tietokoneillaan.

Langattomuuden rakentamiseen on useita eri tapoja kiinteän infrastruktuurin verkoissa. Esimerkiksi yksi tapa olisi liittää itsenäisiä langattoman verkon liityntäpisteitä (myöhemmin nimellä Access-Point) kiinni langalliseen verkkoon. Tässä tapauksessa kuitenkin jokaista itsenäistä Access-Point –laitetta tulisi hallinnoida erikseen ja yhdelle tehdyt asetusmuutokset eivät periydy muille, vaikka asetus olisikin sellainen joka koskisi kaikkia laitteita. WPK-verkossa päädyttiin keskittämään verkkojen hallinta yhdelle laitteelle, ja rakentamamme toteutus olikin keskitetyn hallinnan kontrolleripohjainen langaton verkko. Yksinkertaisesti sanottuna kontrolleripohjaisuus tarkoittaa sitä, että verkossa on yksi laite joka ”kontrolloi” eli hallitsee muita verkon laitteita. Nämä verkon muut laitteet ovat ei-itsenäisiä, niin sanottuja LWAPP -laitteita, (Light-Weight Access Point) joihin käyttäjien koneet ottavat yhteyttä verkkoon kirjautuessaan.

Kontrolleripohjainen ratkaisu helpottaa verkon ylläpitäjän työtä verkon hallinnoimisessa, sillä lähes kaikki muutokset ja asetukset, joita verkkoon tehdään, tehdään kontrollerille. Kontrollerille syötetään muun muassa tiedot langattomista verkoista (meidän tapauksessamme WPK-vieraat ja WPK-langaton) ja niiden tarkemmista asetuksista, kuten suojausvaatimuksista sekä siitä, kuuluuko verkkoa mainostaa yleisesti vai ei. Kaikki nämä asetukset välittyvät kontrollerin kautta kaikille siinä kiinni oleville LWAPP-laitteille, jotka toimivat verkossa ainoastaan vastaanottavassa roolissa, kun käyttäjän kone ottaa yhteyttä langattomaan verkkoon.

Alkuperäisenä ideana oli saada kolme erillistä langatonta verkkoa: opiskelijoille, vierailijoille ja admineille omansa. Lopullisessa työssä verkkojen määrä kutistui lopulta kahteen (vierailijaverkko ja yleinen, WPK-langaton verkko), jonka syitä käsittelemme vielä myöhemmin. Myöhemmin tekstissä kutsumme verkkoja nimellä vierailija- ja opiskelijaverkko, vaikkakin WPK-langaton on käytössä myös tietoverkkopalvelun opettajille. Kuitenkin näiden kahden verkon eritteleminen näillä kahdella nimellä on selkeämpää.

Verkko rakennettiin ensisijaisesti toimimaan Tampereen ammattikorkeakoulun A-siivessä, mutta siihen jätettiin sen verran joustavuutta että tulevaisuudessa verkko on mahdollista laajentaa myös C-rakennukseen.
Käytimme työssämme Ciscon valmistamia verkkolaitteita, yhtä kontrolleria ja neljää LWAPP -laitetta. Kaikki verkon laitteet nimettiin huumorimielessä Islannin tulivuorten mukaan. Asetusmuutoksia jouduimme tekemään myös muutamalle Windows Server –palvelimelle sekä WPK-verkon rajareitittimelle ja reitittävälle kytkimelle AHK:lle, joka on WPK-verkon keskeisin laite.

Opinnäytetyömme vaatimuksiin kuului myös ohjeiden tekeminen WPK-verkon dokumentteihin, jotka löytyvät tämän opinnäytetyön liitteistä. Tietoturvasyistä ohjeet on tätä julkaisua varten muutettu niin, ettei esimerkiksi IP-osoitteita tai muita tunnistetietoja ole nähtävillä.

10.2 Verkon rakentaminen

Aloitimme työn tekemällä karkean suunnitelman siitä, mihin laitteita sijoitetaan ja tekemällä IP-osoitesuunnitelman. Otimme myös selvää langattomista verkoista ylipäätään sekä niissä käytetyissä salaustavoista. Melko pian työn aloittamisen jälkeen aloimme pitää blogia työn edistymisestä (http://langatonverkko.blogspot.com), joka oli myös toimeksiantajan toive.

Alkusuunnitelmien jälkeen aloitimme varsinaisen konfigutointiurakan tekemällä ip-osoitepuulit WPK-verkon DHCP-palvelimille. Näistä ”altaista” verkkoon kirjautuvat asiakkaat saavat IP-osoitteensa. Hallintaverkkona kontrollerille (sekä alkuvaiheessa myös ip-puulina adminverkolle) toimi WPK-verkon yleinen hallintaverkko 172.16.x.x (erillistä puulia ei tarvinnut luoda). Opiskelijoita varten teimme osoitteiston 172.18.x.x ja vierailijoita varten varattiin osoitteet verkosta 172.19.x.x.

Jotta opiskelija- ja vierailijaverkon liikenne saataisiin kulkemaan erillään, loimme kaksi erillistä virtuaalista lähiverkkoa (VLANia) kontrollerimme oletusyhdyskäytävälle eli reittivälle kytkimelle AHK:lle. Virtuaaliset lähiverkot mahdollistavat sen, että fyysinen tietotoliikenneverkko voidaan jakaa useampiin loogisiin osiin. Käytännössä tämä tarkoittaa esimerkiksi yritysten verkoissa sitä, että vaikka osastoja olisi jaoteltu eri kerroksiin tai eri rakennuksiin, voidaan samat osastot yhdistää niin, että ne kuuluvat samaan

verkkoon (esimerkiksi jos hallintaosastot ovat jaettu useamman rakennuksen kesken, tai vaikkapa kirjanpito-osasto on monessa kerroksessa). Virtuaalilähiverkoissa liikkuvaan dataan liitetään tunnuksia, joista vastaanottava laite tietää mihin verkkoon tieto kuuluu ja osaa lähettää sen oikeaan paikkaan. Ennen pääsyä vastaanottajalle tunnus poistetaan, joten käyttäjillä ei ole tietoa siitä, kuuluvatko he johonkin virtuaaliseen lähiverkkoon vai eivät.

Tämän lisäksi tehtiin vielä muutama muutos WPK-verkon rajareitittimelle, eli Postille, joka tarjoaa reitin sisäverkosta Internetiin. Postille tarvitsi luoda pääsylistat, NAT (Network Address Translation)-puulit sekä NAT overload.

Pääsylistoilla määritellään mistä verkoista on pääsy (tai evätty pääsy) ulkoverkkoon. Pääsylistoilla voidaan ottaa kantaa myös siihen, minkä protokollan on sallittu pääsevän verkosta ulos tai sinne sisään (esimerkiksi voidaan sallia ainoastaan www-selailu tai vaikka erikseen kieltää telnet-yhteyksien ottaminen laitteille tai niille suunnatut yhteyskokeilut (ping)). Pääsylistat kiinnitetään aina reitittimen joko ulos- tai sisäänmenevään porttiin ja suunnaksi määritellään joko in tai out, eli pääsylista tarkkailee joko portista sisään tulevaa liikennettä, tai portista ulospäin lähtevää dataa.

NAT-osoitteenmuunnosta tarvitaan sisäverkon osoitteiden piilottamiseen, sillä ns. harmaan sarjan osoitteita ei reititetä ikinä ulkoverkkoihin. Näitä osoitteita ovat kaikki väliltä 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 173.31.255.255 ja 192.168.0.0 – 192.168.255.255, ja niitä voidaan siis käyttää täysin vapaasti sisäverkon puolella. Ulkoverkkoihin tarvitaan julkiset ip-osoitteet ja NAT kääntää sisäverkon osoitteita julkisiksi. Tähän liittyen käyttöön kannattaa ottaa niin sanottu NAT overload eli PAT (Port Address Translation), jolla säästetään julkisia ip-osoitteita. Yksinkertaisesti sanottuna PAT merkitsee sitä, että samaa julkista osoitetta voi käyttää yhtäaikaisesti useampi ”ulkomaailman” kanssa kommunikoiva laite, sillä liikennettä ohjataan porttinumeroin.

Verkon muille laitteille tehtävien asetusten jälkeen siirryimme konfiguroimaan itse kontrolleria. Kontrollerin alkukonfigurointi tehtiin konsoliyhteydellä HyperTerminal – ohjelman avulla (niin sanottu CLI konfigurointi, eli Command-Line Interface). Uuteen, tyhjään laitteeseen ei saa yhteyttä esimerkiksi selaimen kautta ennen kuin alkuasetukset on käyty laitteelle asettamassa. Kun laite ensimmäistä kertaa kiinnitettiin konsoliyhteydellä tietokoneeseen, käynnistyi automaattisesti niin sanottu StartUp Wizard joka kyseli

tarvittavat tiedot että laite saatiin toimintakuntoon.

Aloituswizardin jälkeen kontrollerille piti vielä kirjautua admin-tunnuksilla ja tehdä käsin kaksi konfiguraatiomuutosta telnet- ja webbinäkymän sallimiseksi. Telnet-yhteys on tarpeellinen silloin kun kone on verkossa eikä esimerkiksi webbinäkymään jostain syystä pääse, tai kun halutaan manuaalisesti komentorivin kautta käydä muuttamassa asetuksia. Kontrolleria ei tällöin tarvitse yhdistää koneeseen konsoliportin kautta. Web-näkymä kannattaa sallia koska silloin käyttöön saadaan graafinen käyttöliittymä, jonne pääsee kirjoittamalla selaimen osoiteriville kontrollerin hallintaportin IP-osoite ja syöttämällä avautuvalle sivulle admin-tunnukset. Komentorivi ja sen tilat ovat kontrollerissa erilaiset mitä tavallisissa Ciscon reitittimissä ja kytkimissä, esimerkiksi erillisiä niin sanottuja katselu- ja edistyneen käyttäjän tiloja ei ole ollenkaan.

Web-näkymän sallimisen jälkeen liitimme kontrollerin verkkoon sen lopulliselle sijoituspaikalle ja jatkoimme asetusten syöttämistä graafisen käyttöliittymän puolelta, jolloin esim. Wlan-verkkojen määrittäminen oli huomattavasti komentorivikonfigurointia helpompaa.

Viimeisenä työnä oli RADIUS-palvelimen konfigurointi, jonka avulla määriteltiin se, kuka verkkoon sai liittyä. Ehdoiksi verkkoon pääsemiselle asetimme muun muassa sen, että verkkoihin pyrkivä asiakas tulee verkkoon langattomasti ja kuuluu tiettyyn käyttäjäryhmään.

10.3 Verkon salaus

Verkon salausta mietittäessä tarkistimme ensiksi, minkä tyyppisiä salaustapoja kontrollerimme tukee. Näitä metodeja olivat:

-WPA+WPA2
-802.1x
-StaticWEP
-StaticWEP+802.1x
-CKIP

Testasimme eri salaustapojen toimimista, mutta päädyimme tietoturvallisimpaan ratkaisuun, eli WPA+WPA2 + 802.1x –ratkaisuun. 802.1x –lisä on erittäin hyvä ratkaisu yritysverkoissa, sillä silloin käyttöön tulee (jo valmiiksi konfiguroimamme) RADIUS-palvelin, joka jakaa vaihtuvaa salausavainta verkkoon kytketyille laitteille. RADIUS-kirjautuminen otettiin käyttöön sekä admin- että opiskelijaverkoissa.

Vierailijaverkkoa varten käytimme web-autentikointia, joka ei sinänsä ole mikään salausmetodi. Web-autentikoinnissa kontrollerille asetetaan ns. Local Net User, jolle tehdään paikallinen kirjautumistunnus sekä salasana. Vierailijaverkkoon pyrkivä käyttäjä pakotetaan verkkoon yhdistymisen jälkeen kontrollerin luomalle web-sivulle, jonne käyttäjän on syötettävä käyttäjätunnus ja salasana. Ilman oikeita tunnuksia verkkoon pääsy ei onnistu, mutta oikeilla tunnuksilla kirjautuessa asetimme kontrollerin ohjaamaan käyttäjä ensin Tampereen Ammattikorkeakoulun sivuille, joilta käyttäjä pääsee selaamaan Internetiä normaalisti.

10.4 Ongelmakohtia

Verkon rakentamisessa kohtasimme monia turhauttavia, meistä riippumattomia ongelmia, jotka kuitenkin olivat loppuviimein erittäin opettavaisia. Huomattavasti eniten päänvaivaa aiheutui RADIUS-tunnistautumisesta, sillä jostain syystä palvelimella olevat eri verkkopolitiikat sotkivat toisiaan ja mikäli jokin vaatimus ei täyttynyt ensimmäisestä politiikasta, serveri siirtyi automaattisesti tarkastelemaan seuraavaa politiikkaa. Tämä aivan normaali käytäntötapa aiheutti meille erittäin paljon vaikeuksia ja lopulta myös verkon admin-puoli piti pudottaa tämän asian vuoksi pois.

Meillä oli kaksi erillistä verkkopolitiikkaa (toisessa sallittiin pääsy admintunnuksilla ja toisessa opiskelijatunnuksilla) ja kun koneelta yritettiin kirjautua admin-verkkoon opiskelijatunnuksilla, serveri tarkisti voimassa olevan politiikan numero 1, joka oli ”pääsy admintunnuksilla”. Opiskelijatunnus ei kuulu tähän ryhmään, joten politiikka hylättiin ja siirryttiin seuraavaan. Seuraava politiikka oli ”pääsy opiskelijatunnuksilla”, jolloin serveri hyväksyi pyynnön, vaikka kirjautuminen tapahtui verkon admin-puolelle. Mitään sellaista eriyttävää asetusta emme löytäneet, joka olisi voinut tämän estää. Kokeilimme testauksen vuoksi myös kahden kontrollerin verkkoa, joista toinen hallitsi pelkkää adminverkkoa, ja toinen hallitsi opiskelija- ja vierailijaverkkoa. Laitoimme palvelimelle politiikkaan 1 ”pyyntö täytyy tulla kontrollerilta X ja käyttäjän on kuuluttava adminryhmään” ja politiikkaan 2 ”pyyntö täytyy tulla kontrollerilta Y ja käyttäjän on kuuluttava opiskelijaryhmään”. Edes tällainen ratkaisu ei auttanut, vaan kun adminverkkoon koitettiin kirjautua opiskelijatunnuksilla, serveri tarkasti, että politiikka 1 ei päde aivan täysin ja siirtyi politiikkaan 2, otti sieltä kohdan ”opiskelijatunnus” ja yhdisti sen politiikan 1 kanssa ”pyyntö kontrollerilta X” ja näin ollen antoi pääsyn adminverkkoon. Edes kieltävän asetuksen lisääminen politiikkojen väliin ei muuttanut asiaa suuntaan tai toiseen.

Seuraava suuri ongelma oli saada Windows-koneet verkkoon. Ongelman tutkimista hankaloitti myös se, että Macintoshilla verkkoon pääsi helposti ja automaattisesti kirjautumaan, joten tiesimme, että RADIUS-palvelimen konfiguroinnissa ei ole vikaa vaan asetukset pitää löytää ja tutkia Windowsin puolelta. Meille tuntemattomasta syystä Windows ei osaa automaattisesti määrittää tai ei saa asetuksia verkosta valmiiksi, jolloin joudutaan kirjautumisasetukset syöttämään manuaalisesti. Tämä mielestämme syö langattoman verkon ”tarkoitusta” olla helppo ja vaivaton tapa yhdistyä WPK-verkkoon.

Alun perin työhömme oli tarkoitus myös liittää koulumme toisen opiskelijan opinnäytetyö, jonka hän teki turvallisesta verkkoon pääsystä eli NAPista, josta hieman kerroimmekin omassa kirjallisessa osuudessamme. Valmistunut NAP-toteutus oli suunniteltu langalliseen verkkoon, joten emme saaneet sitä suoraan liitettyä omaan työhömme ja työn valmistuminen viivästyi niin paljon, että meillä ei ollut enää aikaa edes alkaa soveltamaan sen tuloksia langattomaan verkkoomme. Mahdollisesti tämä kuitenkin poikii uuden opinnäytetyöaiheen jollekin koulumme opiskelijalle jatkossa.

11 YHTEENVETO

Tämän opinnäytetyön tarkoitus oli tutkia langattomia verkkoja ja niiden eri toteutustapoja, sekä myös langattomien verkkojen tietoturva-asioita. Tampereen Ammattikorkeakoulun WPK-verkkoon tarkoituksenamme oli toteuttaa kontrolleripohjainen langaton verkkoratkaisu.

Tärkeimpinä lähteinä kirjallisessa osiossa meillä oli Jim Geierin ”Langattoman verkon perusteet”, Matti Puskan ”Langattomat verkot”, Kaj Granlundin ”Langaton tiedonsiirto” ja Anand R. Prasadin & Neeli R. Prasadin ”802.11 WLANs and IP Networking” –kirjat. Varsinaisessa käytännön osuudessa meille oli paljon hyötyä Cisco Systemsin sivuilta löytyvistä konfigurointioppaista sekä Microsoftin TechNet-sivujen ohjeista.

Opinnäytetyöprosessimme aloitimme keväällä 2010 tiedon hankkimisen merkeissä. Käytännön toteutusta aloimme rakentaa loppukeväästä, ja se saatiin kesän aikana hyvälle mallille. RADIUS-ongelmia jouduttiin ratkomaan vielä syksyn puolella, lähinnä siis Windows-koneiden verkkoonpääsyn vuoksi.

Toteutus jäi osin puutteelliseksi admin-verkon ja NAP-suojauksen puuttumisen myötä, mutta verkko ja sen perustoiminnot ovat muuten kunnossa ja verkko toimii kuten sen pitääkin. Admin-verkon liittäminen olisi saattanut onnistua, mikäli meillä olisi ollut lopussa vielä enemmän aikaa ongelman miettimiseen. NAPin liittäminen verkkoon sen sijaan jäi puuttumaan täysin meistä riippumattomista syistä, sillä työn valmistuminen viivästyi niin paljon, että kun työn tulokset tulivat julki, oli meillä enää kuukausi jättää oma työmme esitarkastukseen.

Opinnäytetyössämme pääsimme soveltamaan hyvin CCNA- ja CCNP kursseilla oppimaamme. Työ kehitti ongelmanratkaisutaitojamme ja saimme varmuutta verkon ylläpitämiseen. Opinnäytetyömme antaa WPK-verkossa toimivalle harjoittelijalle monipuolisemman työnkuvan ja tilaisuuden jatkokehittää langatonta verkkoa tulevaisuudessa.

LÄHTEET

Davies Joseph, Northrup Tony 2008. Windows Server 2008 Networking and Network Access Protection (NAP) Washington: Microsoft press

Geier, Jim 2005. Langattomat verkot perusteet. Helsinki: Edita Prima Oy

Grandlund, Kaj 2001. Langaton tiedonsiirto. Porvoo: WSOY

Prasad Anand R. & Prasad, Neeli R. 2005. 802.11 WLANs and IP Networking: security, QoS, and mobility. Yhdysvallat: Artech House

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

Verkkolähteet

Networksorcery - RADIUS, Remote Authentication Dial-In User Service 2010 [online] [viitattu 20.10.2010] http://www.networksorcery.com/enp/protocol/radius.htm

Vesanen, Ari 2003. Oulun yliopiston luennot [online]
[viitattu 25.8.2010]
http://www.tol.oulu.fi/users/ari.vesanen/Langaton_TT/luennot/johdanto/Uhkat.html

Wikipedia - GSM 2010 [online]
[viitattu 27.09.2010] http://fi.wikipedia.org/wiki/GSM

Wikipedia - Hiperlan 2009 [online]
[viitattu 27.09.2010] http://fi.wikipedia.org/wiki/HIPERLAN

Wikipedia – Heinrich Hertz 2010 [online]
[viitattu 18.8.2010] http://fi.wikipedia.org/wiki/Heinrich_Hertz

Wikipedia – IEEE 802.11 2010 [online]
[viitattu 18.8.2010] http://fi.wikipedia.org/wiki/IEEE_802.11

Wikipedia - IEEE 802.11i 2010 [online]
[viitattu 03.10.2010] http://fi.wikipedia.org/wiki/IEEE_802.11i

Wikipedia – Metropolitan area network 2010 [online]
[viitattu 1.10.2010] http://en.wikipedia.org/wiki/Metropolitan_area_network

Wikipedia – OFDM 2010 [online]
[viitattu 30.9.2010] http://fi.wikipedia.org/wiki/Ofdm

Wikipedia – Palvelunestohyökkäys 2010 [online]
[viitattu 28.8.2010] http://fi.wikipedia.org/wiki/Palvelunestohy%C3%B6kk%C3%A4ys

Wikipedia – Radio 2010 [online]
[viitattu 29.9.2010] http://fi.wikipedia.org/wiki/Radio

Wikipedia – UMTS 2010 [online]
[viitattu 28.09.2010] http://fi.wikipedia.org/wiki/UMTS

Zigbee - Zigbee Alliance 2010 [online]
[viitattu 20.10.2010] http://zigbee.org/About/FAQ.aspx

Kuvat

Web Technology World - Basic Networking Guide. 2010 [online]
[viitattu 22.10.2010.] http://webtechnoworld.com/Networking.php

Home Network Help -What is Wireless Network 2010 [online]
[Viitattu 22.10.2010] http://www.home-network-help.com/wireless-network.html

Iapplianceweb- IEEE 802.16, 2004 [online]
[viitattu 23.10.2010] http://www.iapplianceweb.com/story/oeg20020808s0002.htm

Kramfs Tech Chronicles - What is HSPA? 2009 [online]
[viitattu 23.10.2010]
http://kramfs.com/starhub-commences-upgrade-of-mobile-broadband-network-to-hspa-plus/

Link Evolution – What is infrared communication? 2010 [online]
[viitattu 23.10.2010] http://linkevolution.e-globaledge.com/english/infrared/rcandir.html

Amit Bhawani – How does bluetooth work? 2010 [online]
[viitattu 23.10.2010] http://www.amitbhawani.com/blog/how-bluetooth-works-guide/

Texas Instrument- ZigBee & RF4CE, 2010 [online]
[viitattu 23.10.2010]
http://focus.ti.com/analog/docs/gencontent.tsp?familyId=367&genContentId=24190

Interlink Networks - RADIUS Server vs. VPN - Link Layer and Network Layer Security for Wireless Networks , 2006-2007 [online]

[viitattu 15.10.2010]
http://www.interlinknetworks.com/images/Man-in-the-middle_attack.jpg

Interlink Networks - RADIUS Server vs. VPN - Link Layer and Network Layer Security for Wireless Networks , 2006-2007 [online]

[viitattu 15.10.2010]
http://www.interlinknetworks.com/images/DOS_attack.jpg

LIITTEET

Ohjeet ja dokumentit verkon ylläpitoa varten.

IP-osoitesuunnitelma

Taulukko 1: Kontrollerin porttien IP-osoitteet

Kontrollerin portti	IP
Management interface	172.16.X.X
Access-point management interface	172.16.X.X

Taulukko 2: WPK-langaton –verkon IP-osoitteita

WPK-langaton	IP	DHCP puuli
DHCP Palo1	172.16.X.X	172.18.X.X/X
DHCP Palo2	172.16.X.X	
Default Gateway AHK vlan18	172.18.X.X	

Taulukko 3: WPK-vieraat –verkon IP-osoitteita

WPK-vieraat	IP	DHCP puuli
DHCP Palo1	172.16.X.X	172.19.X.X/X
DHCP Palo2	172.16.X.X	
Default Gateway AHK vlan19	172.19.X.X	

Kontrollerin alkuasetukset, StartUp Wizard

Taulukko 4: Kontrollerin alkuasetukset

Asetus	Tarkoitus	Vastaus
System name	Järjestelmän, eli kontrollerin nimi. Maksimissaan 32 ASCII-merkkiä	Eyjafjallajokull
Administrative user name	Järjestelmän ylläpitäjän kirjautumistunnus	WPK
Administravite user password	Järjestelmän ylläpitäjän salasana	Salasana
Management interface IP address	Kontrollerin hallintaportin IP-osoite	172.16.X.X
Management interface netmask	Kontrollerin hallintaportin verkkomaski	X.X.X.X
Management interface default router	Kontrollerin oletusyhdyskäytävä	172.16.X.X
Management interface vlan identifier	Kontrollerin hallintaportin VLAN numero, täytyy vastata kytkimelle konfiguroitua vlania. Jos vlania ei ole määritelty, kirjoitetaan 0	50
Management interface port number	Kontrollerin hallintaportin porttinumero	1
Management interface DHCP address	Kontrollerin hallintaportin DHCP-serverin IP osoite	172.16.X.X
AP manager interface IP address	Kontrollerin Access-Pointien hallinta IP. Tämä IP hallitsee kaikkia kontrollerille liittyneitä Access-Pointteja	172.16.X.X
Virtual Gateway IP address	Kontrollerin virtuaalisen yhdyskäytävän IP-osoite, joku fiktiivinen käyttämätön osoite	Esim. 1.1.1.1 (voidaan muuttaa myöhemmin)

Mobility/ RF Group name	Mobiili/radiotaajuusryhmän nimi, ei pakollinen	WPK
Network name (SSID)	Tähän syötetään se yksilöivä nimi (service set identifier) verkolle, johon Access-Pointit liittyvät. **HUOM.! EI OLE SE MIKÄ NÄKYY KÄYTTÄJILLE**	WPK
Allow static IP addresses [YES] [no]	Vastataan YES / NO sen mukaan, sallitaanko kiinteät IP:t (YES) vai saavatko koneet IP-osoittensa DHCP-palvelimelta (NO). Oletuksena on Yes.	NO
Configure a RADIUS server now? [YES] [no]	Mikäli RADIUS-palvelimen haluaa jo tässä vaiheessa konfiguroida, vastataan YES (tai painetaan Enteriä, sillä Yes on oletuksena) ja vastataan sen jälkeen vielä seuraaviin kysymyksiin: RADIUS server IP address RADIUS server port (1812) RADIUS server secret. Jos vastaa NO, saa varoituksen, mutta siitä ei tarvitse tässä vaiheessa välittää.	NO (tämä on helppo hoitaa myöhemmin)
Enter country code	Syötetään maatunnus, kirjoittamalla Help saa listan tunnuksista	FI
Enable 802.11b network	Otetaan 802.11b käyttöön	Oletuksena Yes/ voi myös vastata No
Enable 802.11a network	Otetaan 802.11a käyttöön	Oletuksena Yes / voi myös vastata No
Enable 802.11g network	Otetaan 802.11g käyttöön	Oletuksena Yes / voi myös vastata No

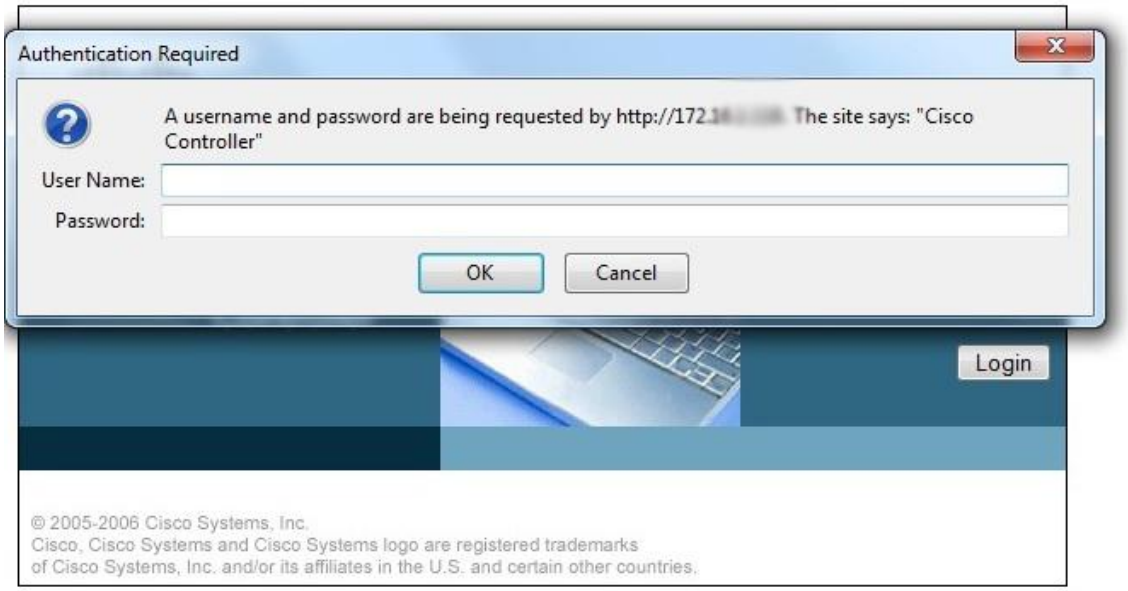
Enable auto-RF	Otetaan käyttöön automaattinen radiotaajuuksienhallinta	Oletuksena Yes/ voi myös vastata No

Käsin tehtävät muutokset alkuasetusten jälkeen

(Eyjafjallajokull) > config network telnet enable
(Eyjafjallajokull) > config network webmode enable

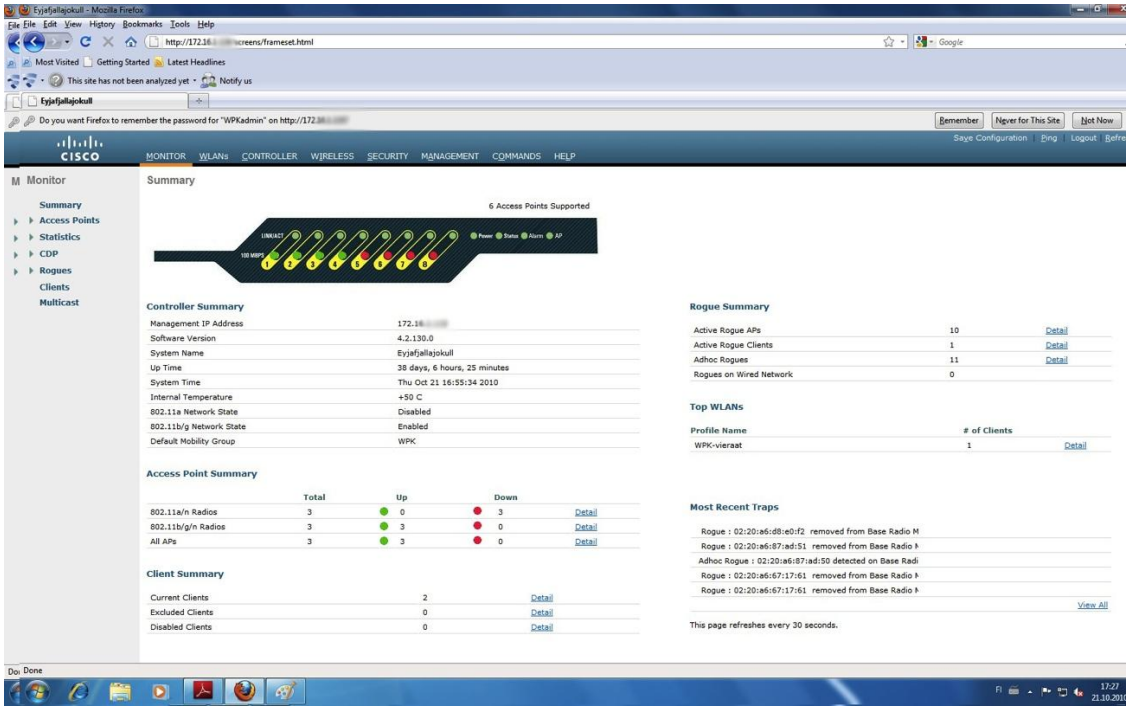
Kontrollerin konfigurointi web-näkymässä

Webbinäkymään pääsee käsiksi kirjoittamalla selaimen otsikkoriville kontrollerin IP-osoitteen, eli hallintaportin IP-osoitteen, ja syöttämällä alkukonfiguraatiossa annetut admin-tunnukset niille varattuihin paikkoihin (kuva 13).



Kuva 13: Web-näkymään kirjautuminen

Kirjautumisen jälkeen avautuu kontrollerin graafisen käyttöliittymän aloitussivu (kuva 14)



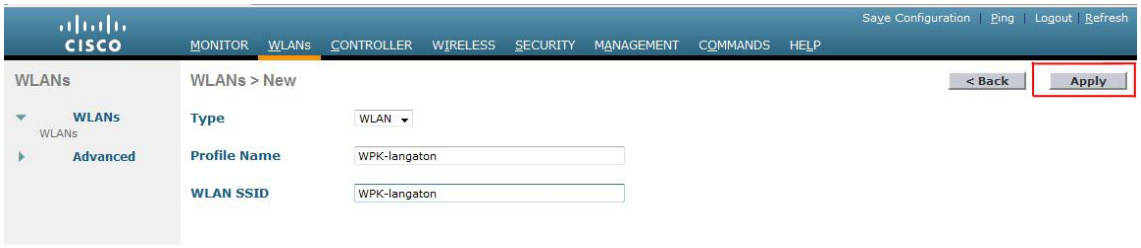
Kuva 14: Kontrollerin graafinen käyttöliittymä

WLAN-verkkojen luominen

WLAN-verkkojen luominen aloitetaan valitsemalla yläriviltä kohta WLANs. Uutta verkkoa pääsee luomaan painamalla New... –nappulaa (kuva 15).

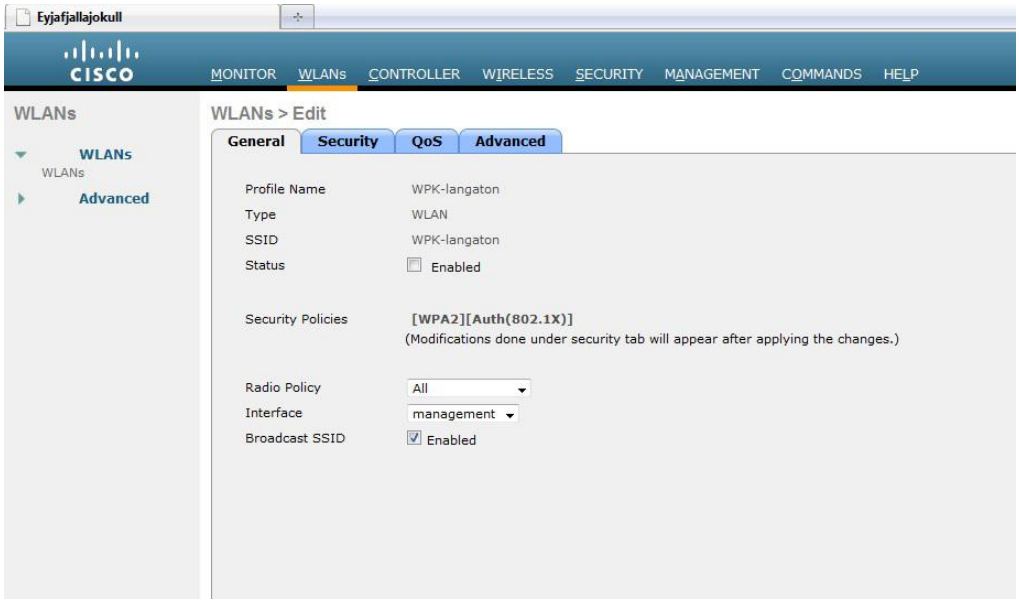
Kuva 15: WLANin luomisen aloitus

WLANs > New sivulla annetaan uuden langattoman verkon tiedot. SSID- kohdassa lukeva teksti on verkon mainostettava nimi, eli se verkkonimi johon käyttäjät liittyvät. Asetusten antamisen jälkeen painetaan Apply-nappia (kuva 16). On huomattavaa, että WLAN-verkon nimeä ei pysty tämän jälkeen vaihtamaan, vaan mikäli nimeä tarvitsee vaihtaa, on luotava kokonaan uusi verkko ja poistettava sitten entinen.



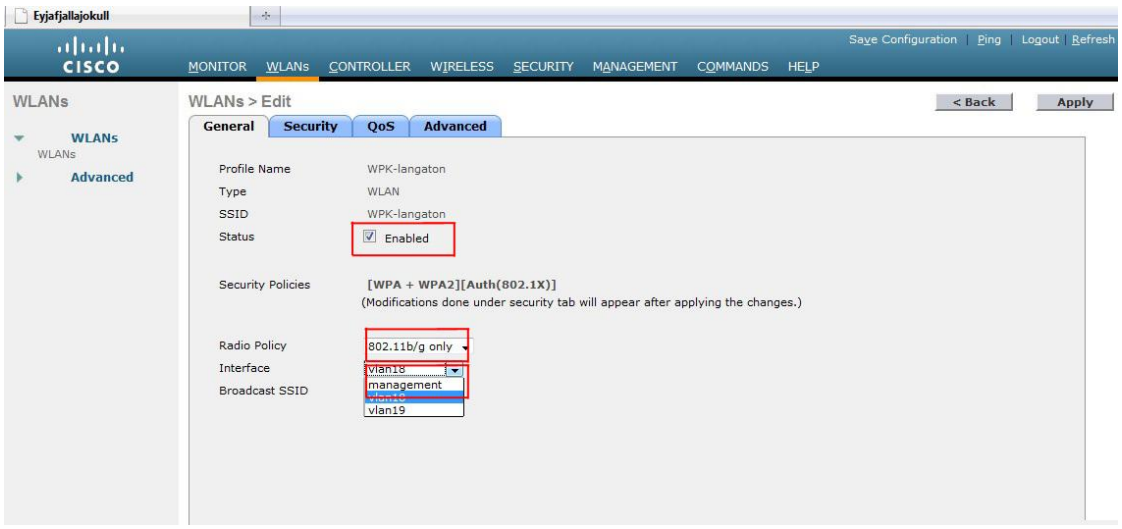
Kuva 16: WLAN-tietojen syöttäminen

Napin painalluksen jälkeen päästään takaisin WLANs aloitussivulle, jolloin listaan on ilmestynyt juuri luotu WLAN. Sitä klikkaamalla pääsee muuttamaan kyseisen WLANin asetuksia, kuten salausmetodia (kuva 17).



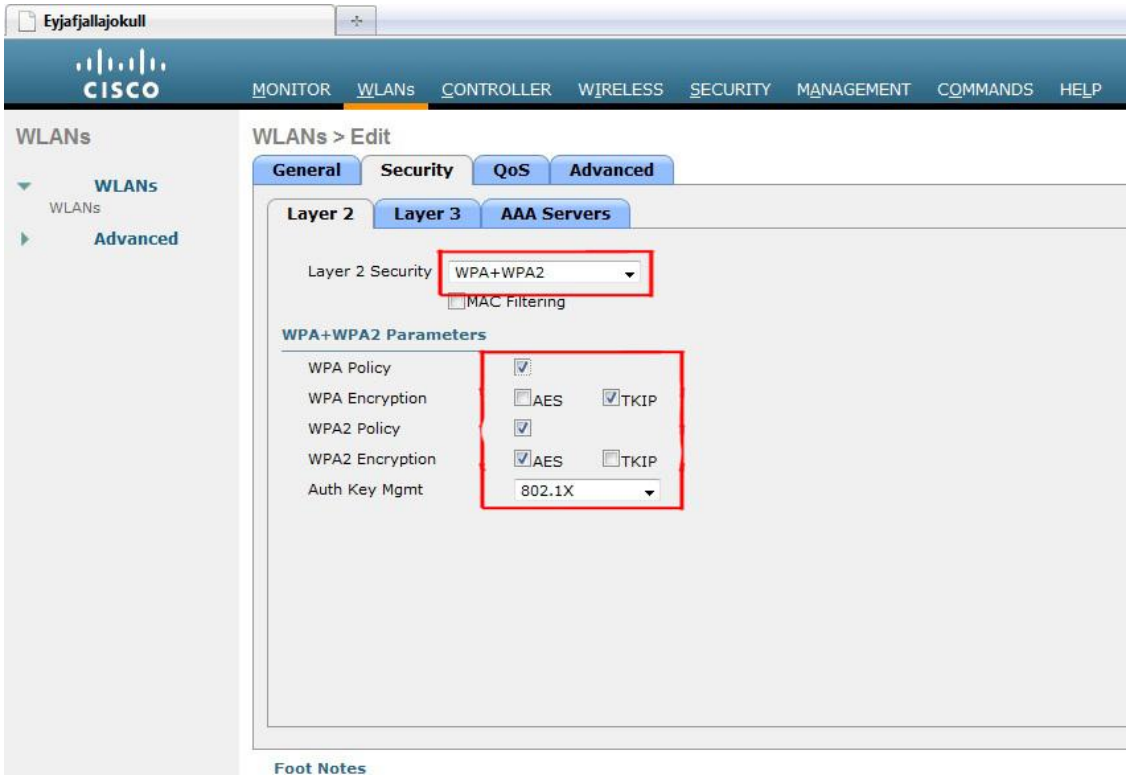
Kuva 17: WLANin asetukset oletusarvoisina

Ruksitetaan kohta Enabled, jolloin WLAN tulee käyttöön. Radiopolitiikaksi valitsimme ainoastaan 802.11b/g, sillä 802.11a-standardin käyttöalueena toimii vain Kanada ja Yhdysvallat. Sinänsä asetuksesta ”All” ei ole mitään haittaa, mutta kannattaa karsia kaikki ”turha” pois. Interface –kohdasta pääsee kytkemään WLANIN johonkin tiettyyn VLANiin. Kohta ”management” laittaa WLANin kuulumaan hallintaverkkoon. Otetaan rati pois kohdasta Broadcast SSID, tässä kuvassa (kuva 18) se onkin jäänyt pudotusvalikon taakse piiloon.



Kuva 18: WLAN asetusten muuttaminen

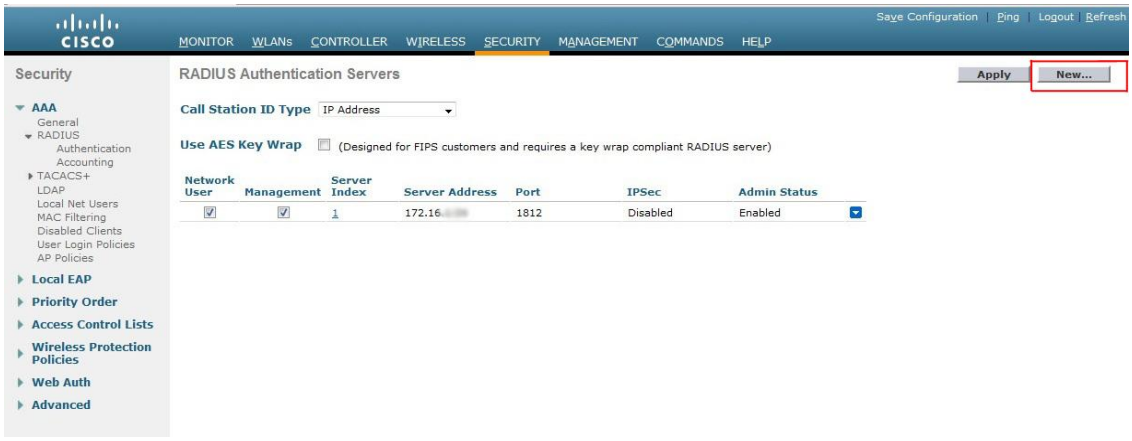
Security-välilehdeltä käydään tekemässä muutokset salaus- ja tunnistautumistapoihin. RADIUS-kirjautumisessa Layer 2 security -kohtaan valitaan ensin pudostusvalikosta WPA+WPA2 ja sen valittua aukeaa alas vielä muutama korjattava asetus. WPA Policy -kohtaan laitetaan ruksi ja WPA Encryptionista valitaan TKIP. WPA2 Policy ja Encyption (AES) voivat jäädä oletusasetuksilleen. Auth Key Mgmt pudotusvalikosta valitaan 802.1x (kuva 19).



Kuva 19: Salaustapojen muutos

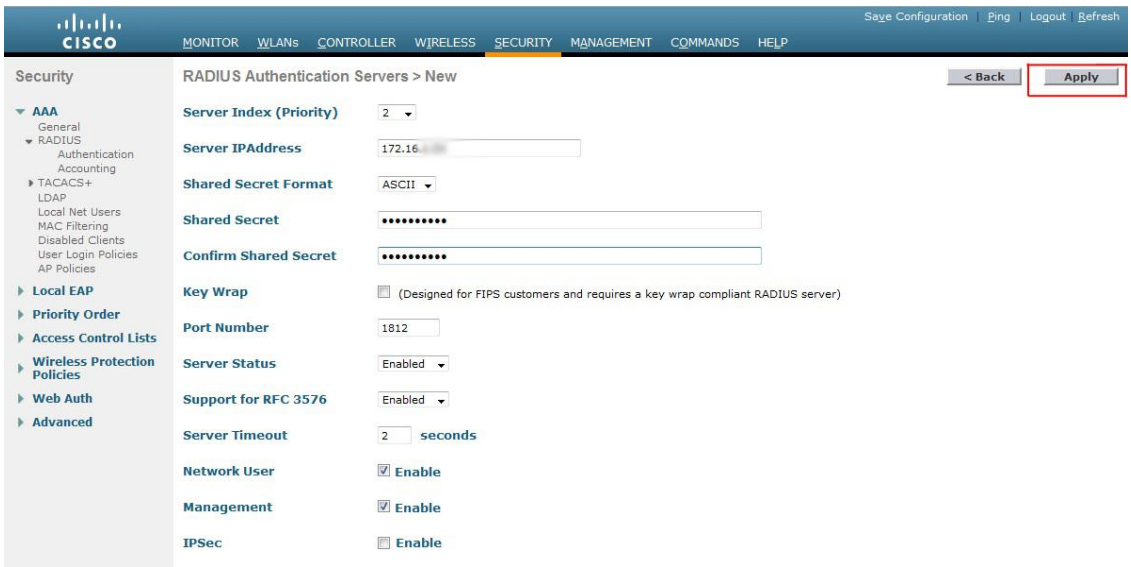
RADIUS-palvelimen asettaminen

Mikäli RADIUS-palvelinta ei konfiguroinut StartUp Wizardissa, voi sen käydä helposti lisäämässä käsin Security-kohdan AAA > RADIUS -valikosta. Uuden palvelimen pääsee lisäämään painamalla New... (kuva 20)



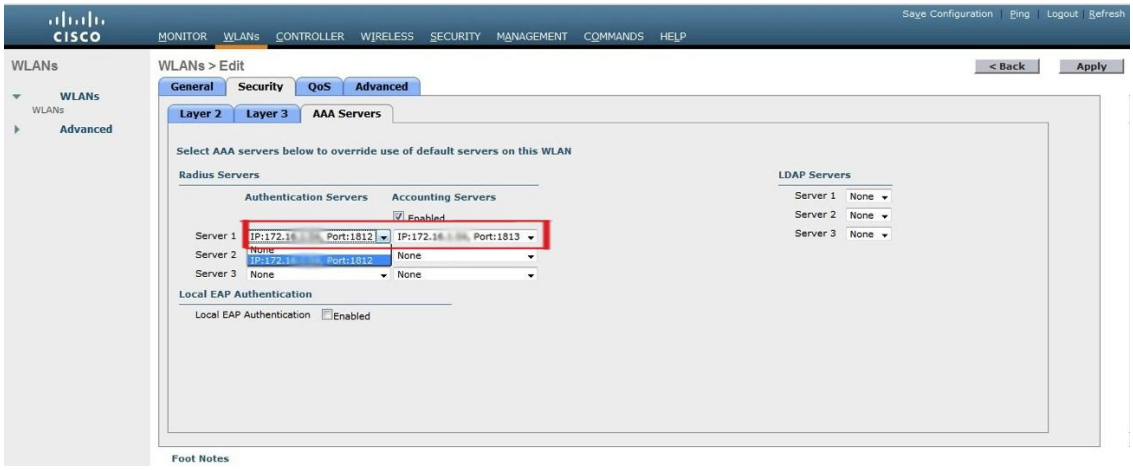
Kuva 20: Uuden RADIUS-palvelimen asettamisen aloitus

Sivulla annetaan kaikki tarvittavat tiedot yhteyden muodostamista varten. IP-osoite ja Shared Secret -kohdat ovat tärkeitä. Shared Secret pitää olla sama sekä kontrollerilla, että RADIUS-palvelimella (RADIUS-konfigurointi opastetaan myöhemmin). Kun asetukset ovat valmiit, painetaan Apply (kuva 21).

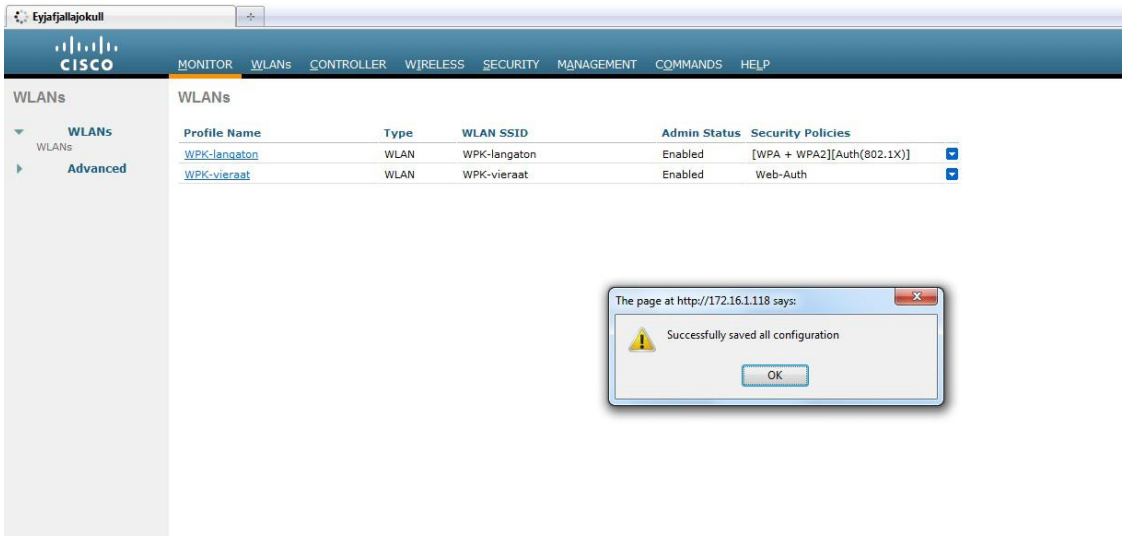


Kuva 21: RADIUS-asetuksia

AAA-Servers välilehdellä valitaan pudotusvalikosta juuri asetetun RADIUS-palvelimen IP-osoite, jolloin kyseinen palvelin saadaan käyttöön painamalla Apply (kuva 22). Konfiguraatiot kannattaa aina välillä tallentaa painamalla Save Configuration, jonka jälkeen tulee ilmoitus asetusten tallettumisesta (kuva 23).



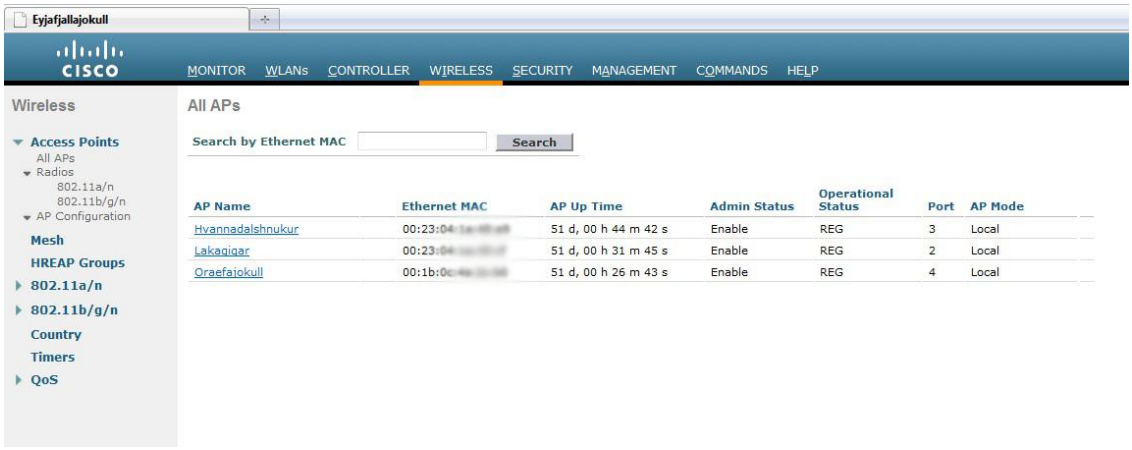
Kuva 22: RADIUS-palvelimen ottaminen käyttöön



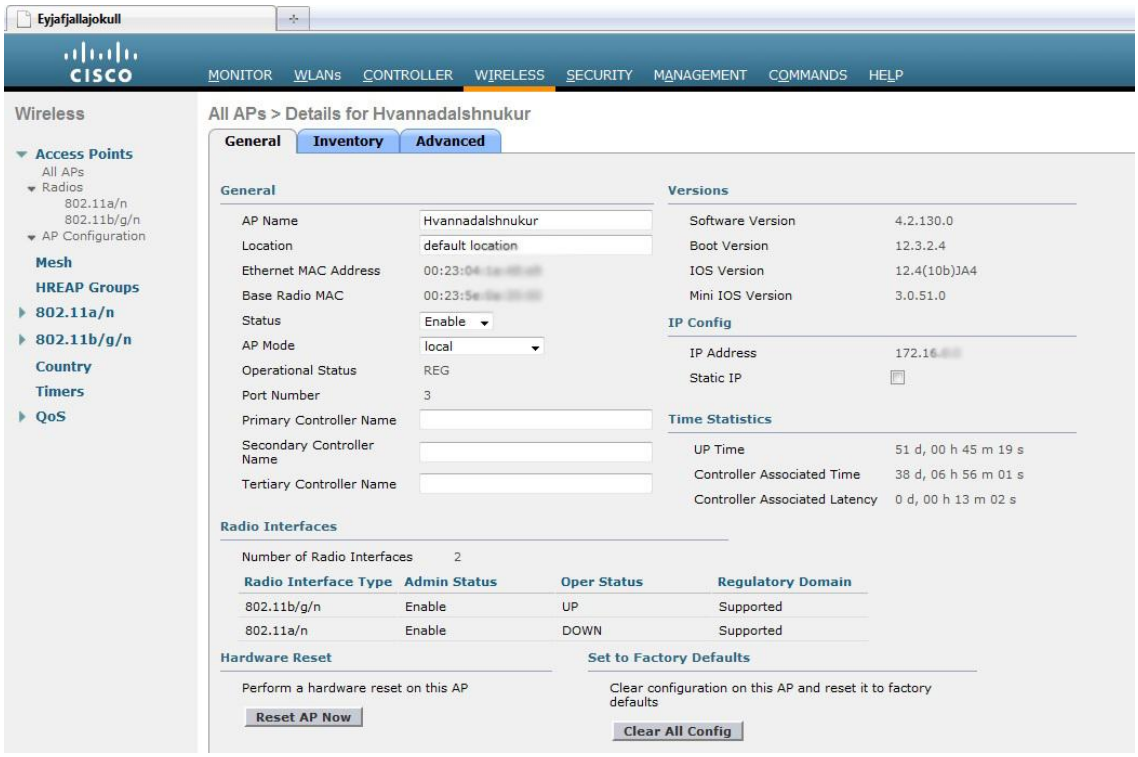
Kuva 23: Konfiguraatio tallennettu

Access-Pointien tarkastelu

Kun verkkoon on liitetty Access-Pointteja, niitä pääsee tarkastelemaan kohdasta Wireless (kuva 24). Klikkaamalla Access-Pointin nimeä pääsee näkemään tietoa ko laitteesta, muuttamaan sen nimeä ja tekemään muita pieniä muutoksia (kuva 25).



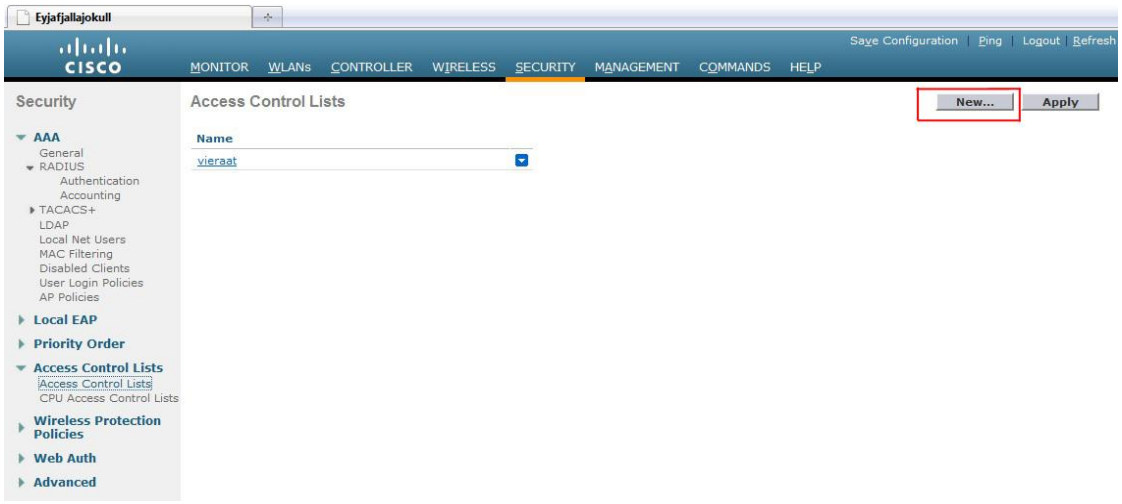
Kuva 24: Access-Point -lista



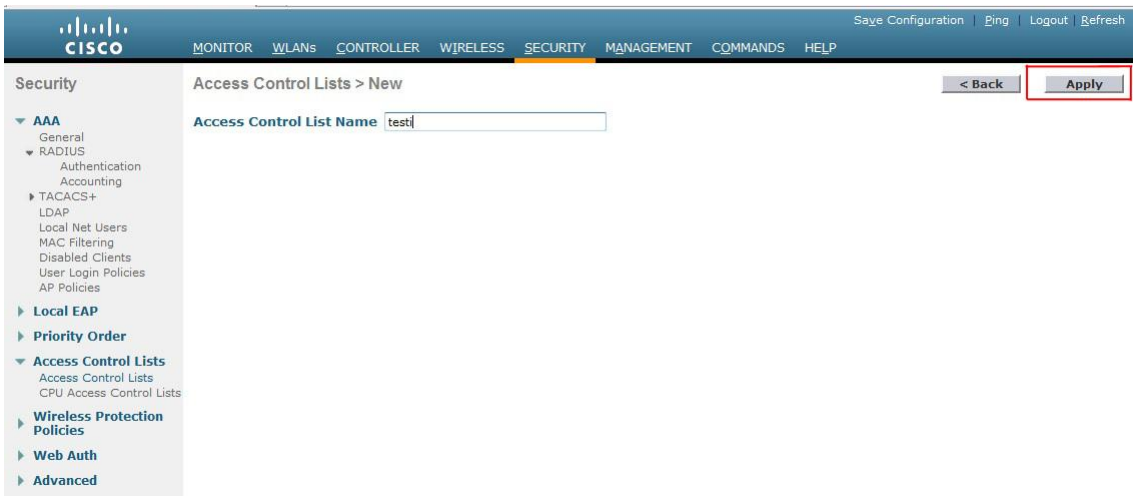
Kuva 25: Hvannadalshnúkurin asetuksia

Pääsylistojen tekeminen

Joissain tilanteissa voi olla tarpeen luoda kontrollerille pääsylistoja. Näitä pääsylistoja pääsee tosin käyttämään ainoastaan web-autentikointia hyödyntävissä verkoissa, kuten meidän työssämme vierailijaverkossa. Uutta pääsylistaa pääsee tekemään Security-kohdan Access Control Lists > Access Control Lists -valikosta. Painetaan New... uuden listan luomista varten (kuva 26). Pääsylistalle annetaan nimi ja painetaan Apply (kuva 27). Ehtojen asettaminen aloitetaan painamalla Add New Rule (kuva 28).



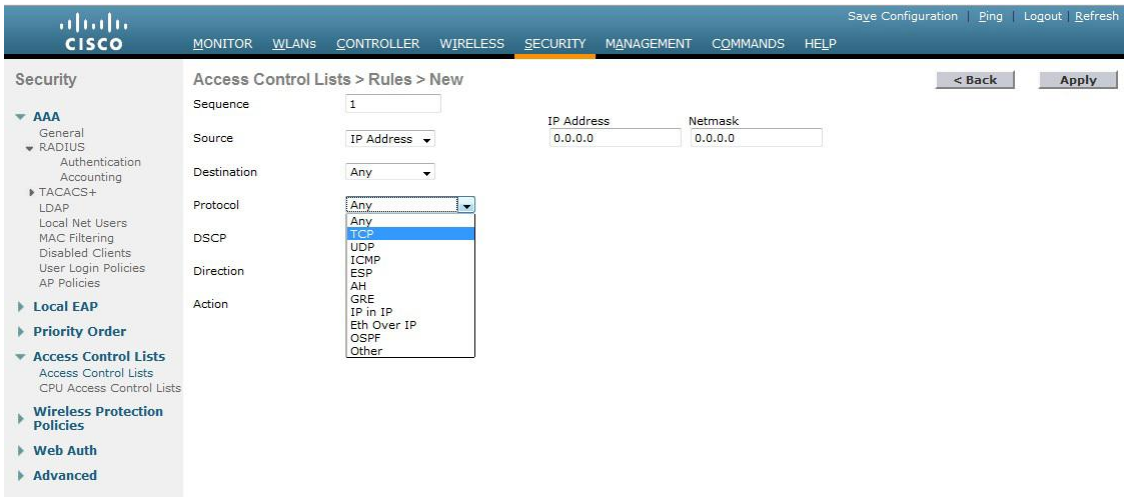
Kuva 26: Pääsylistan luomisen aloitus



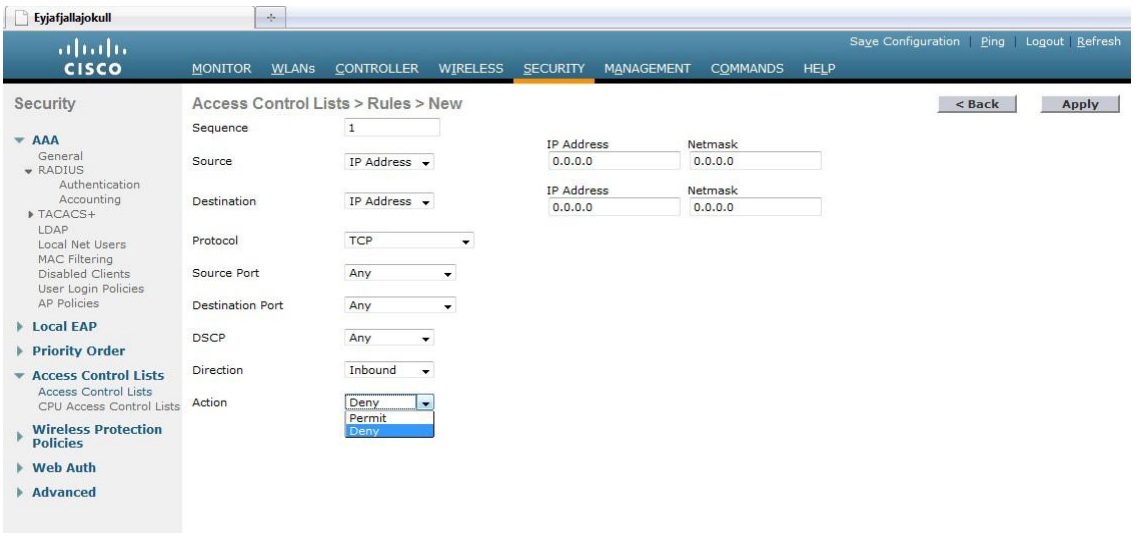
Kuva 27: Pääsylistan nimen syöttäminen

Kuva 28: Pääsylistan ehtojen asettamisen aloitus

Add New Rule -näkymästä pääsee syöttämään haluamansa tiedot pääsylistan luomista varten. Source- ja destination pudotusvalikoista voi valita itselleen sopivammat vaihtoehdot, muita tärkeitä valintoja ovat Protocol, joka määrittelee käytettävän protokollan (kuva 29), Direction, joka määrittelee tiedon liikkumisen suunnan (kontrollerille sisään tai kontrollerilta ulos) sekä Action (kuva 30), joka määrittelee kielletäänkö kyseinen liikenne vai sallitaanko se. Kun asetukset ovat valmiit, painetaan Apply.

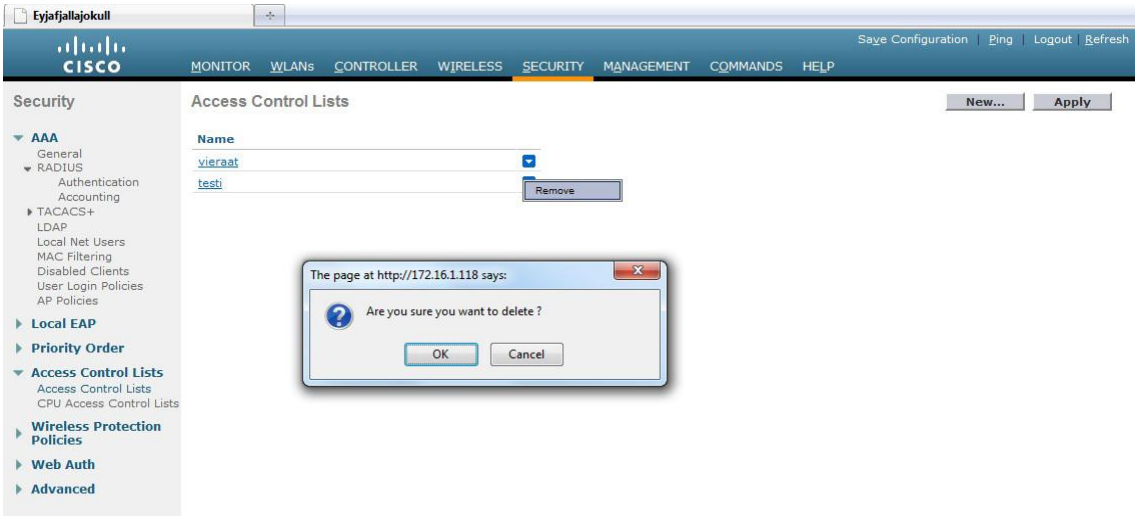


Kuva 29: Pääsylistalle asetettavia asetuksia 1



Kuva 30: Pääsylistalle asetettavia asetuksia 3

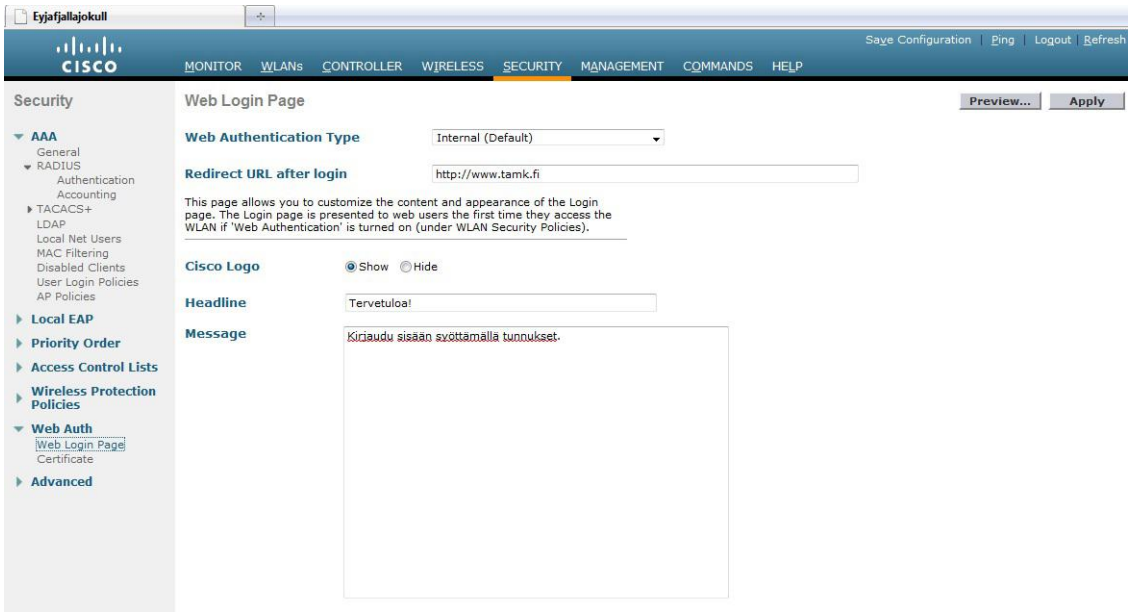
Mikäli pääsylistan haluaa poistaa, tarvitsee vain klikata listan perässä olevaa sinistä nuolta ja valita Remove (kuva 31).



Kuva 31: Pääsylistan poistaminen käytöstä

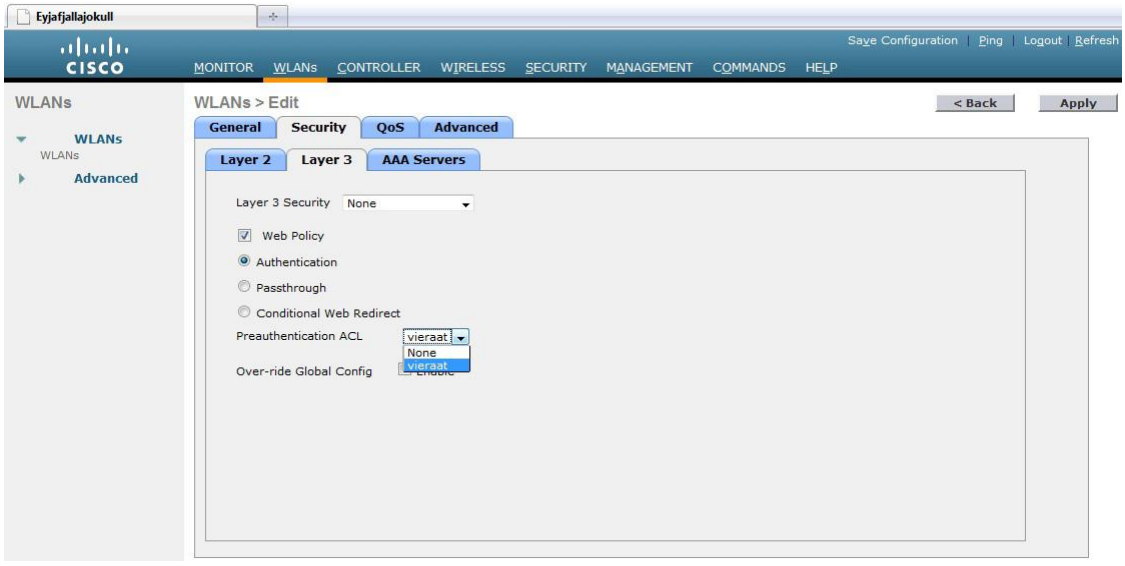
Web-autentikointi

Web-autentikoinnin tekemisen voi aloittaa Security-kohdan Web Auth > Web Login Page -valikosta. Tässä voidaan valita etusivu, jonne käyttäjä pakotetusti ohjautuu kirjautumisen jälkeen, sekä kirjoittaa tekstit mitkä näkyvät käyttäjille kirjautumissivulla (kuva 32).



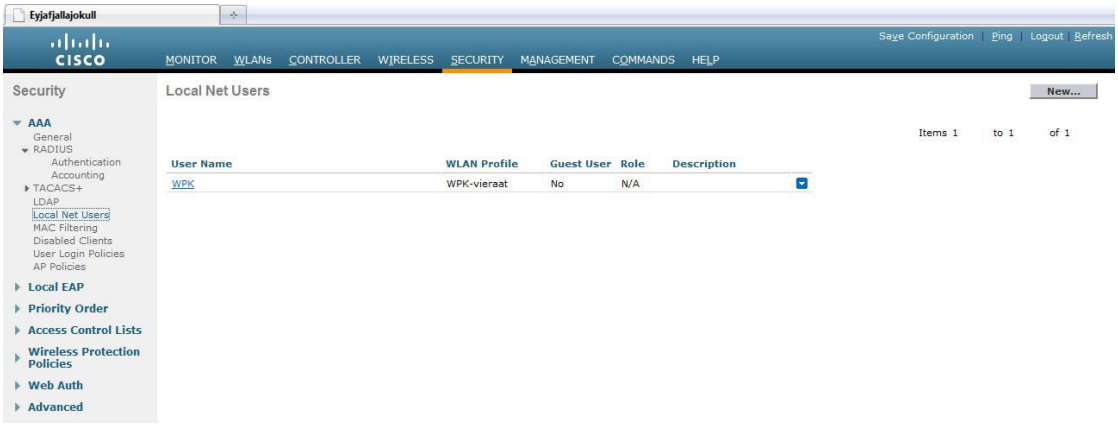
Kuva 32: Web-autentikoinnin ohjaussivu

Web-autentikointi saadaan päälle WLANs-kohdasta. Valitaan vierailijaverkko ja mennään sen asetuksissa kohtaan Security > Layer 3 ja rastitetaan kohta Web-Policy. Pre-authenticatuin ACL-pudotusvalikosta voi valita verkkoa koskevan pääsylistan mikäli sellaisen on tehnyt (kuva 33).



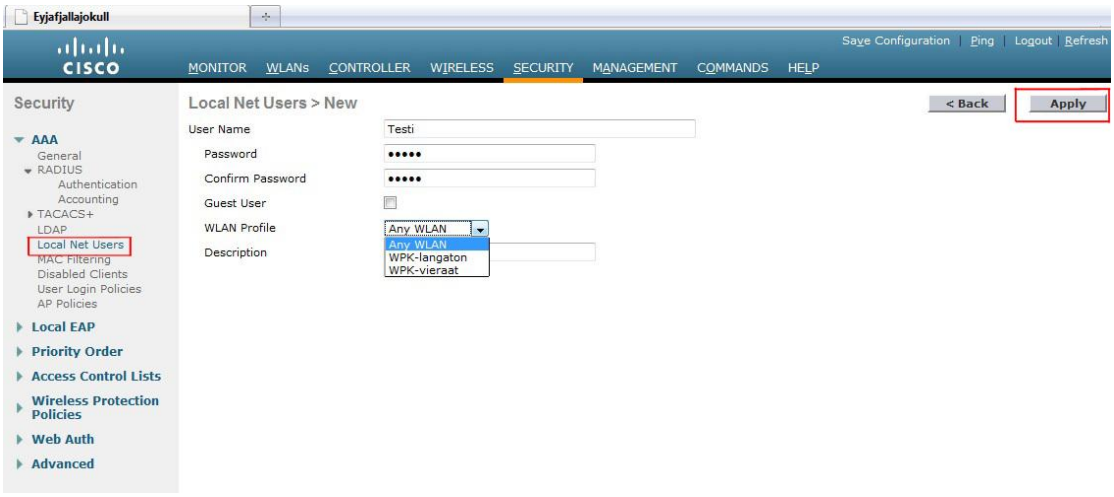
Kuva 33: Web-autentikoinnin ottaminen käyttöön.

Web-autentikointia varten tarvitsee vielä käydä Security-kohdan AAA > Local Net Users -valikosta lisäämässä ”käyttäjä” eli käyttäjätunnus- ja salasanapari jolla Web-autentikointi onnistuu. Painetaan New... (kuva 34)



Kuva 34: Local Net Usersin lisäämisen aloitus

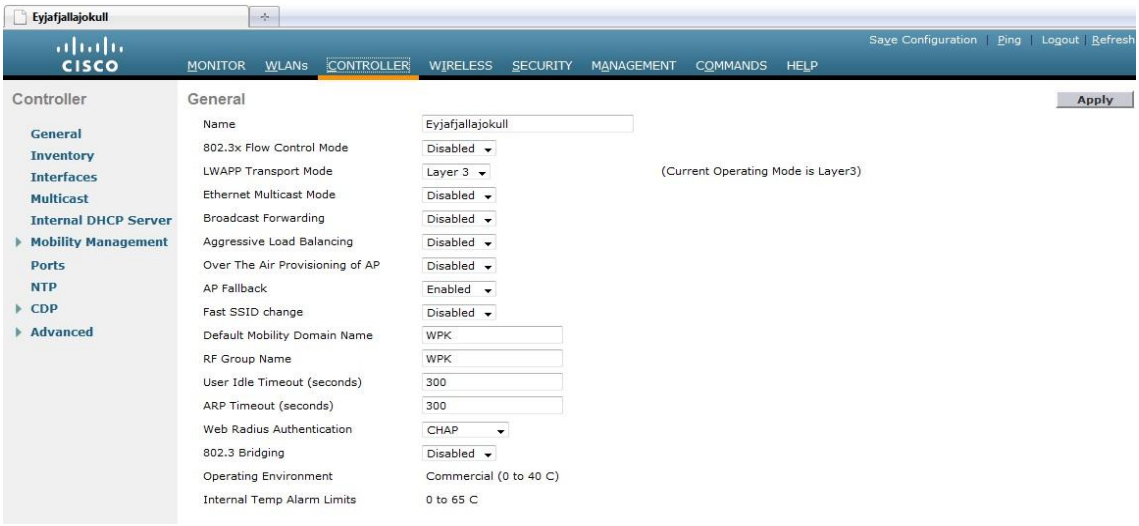
Syötetään halutut tiedot. User Name -kohtaan annetaan se kirjautumistunnus jolla käyttäjien halutaan pääsevän kiinni verkkoon. Salasana syötetään kaksi kertaa. WLAN Profilesta valitaan, mihin langattomaan verkkoon kirjautumisen haluaa ottaa käyttöön. Asetusten asettamisen jälkeen painetaan Apply (kuva 35).



Kuva 35: Local Net Users asetuksia

Kontrollerin tarkastelu

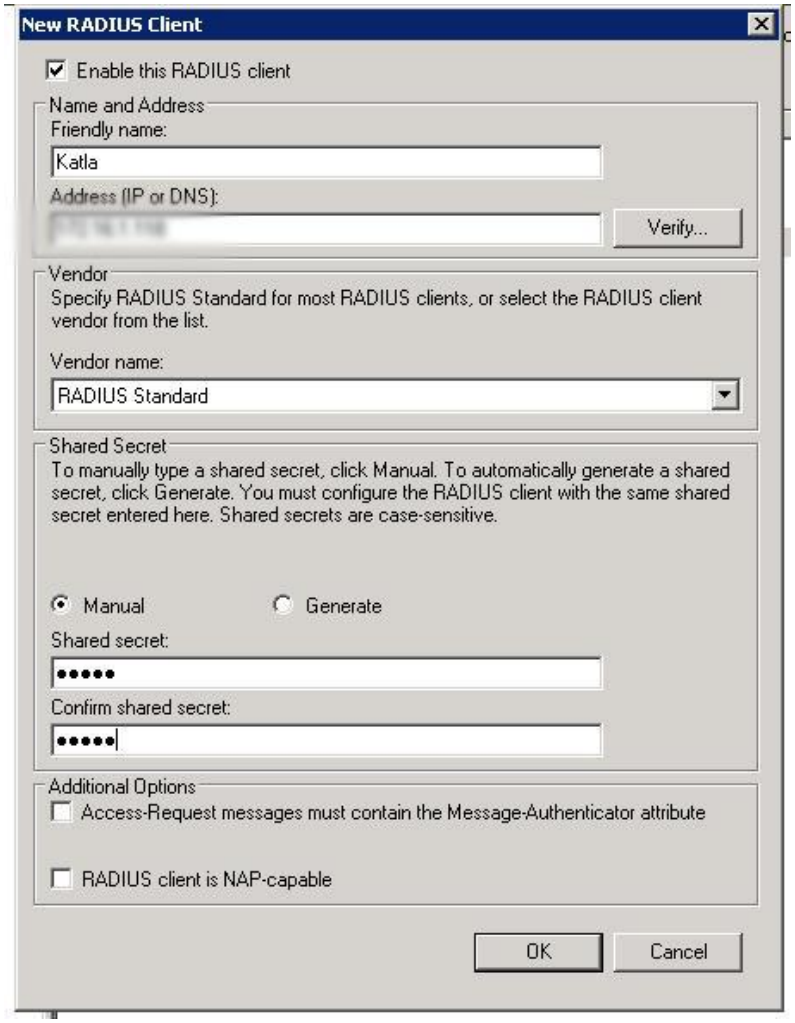
Kontrolleria itseään pääsee tarkastelemaan Controller-kohdasta (kuva 36).



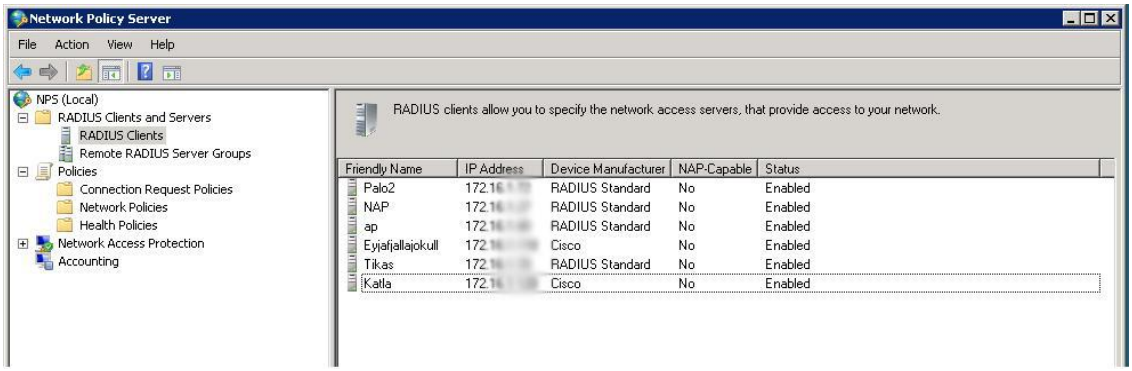
Kuva 36: Kontrollerin asetuksia

RADIUS-konfigurointi

RADIUS-asetukset löytyvät Luukun Administrative Toolsien Network Policy Server (NPS) -kohdasta. Ensimmäisenä luodaan uusi RADIUS Client (yhteys kontrollerin ja serverin välillä). Uutta ”asiakasta” pääsee asettamaan klikkaamassa hiiren oikealla painikkeella kohdasta RADIUS Client ja valitsemalla New (kuva 37). Avautuu ikkuna, jossa pääsee syöttämään laitteen tiedot. Tärkeitä kohtia nimen ja IP-osoitteen lisäksi ovat Enable this RADIUS client -kohta, joka täytyy olla valittuna tai muuten yhteyttä ei luoda, ja Shared Secret-kohta, jonka salasana täytyy olla täsmälleen sama mitä on asetettu kontrollerille. Kun asetukset ovat oikein, klikataan OK ja näkymä palaa takaisin RADIUS Clients-näkymään. Uusi client on ilmestynyt listaan (kuva 38).

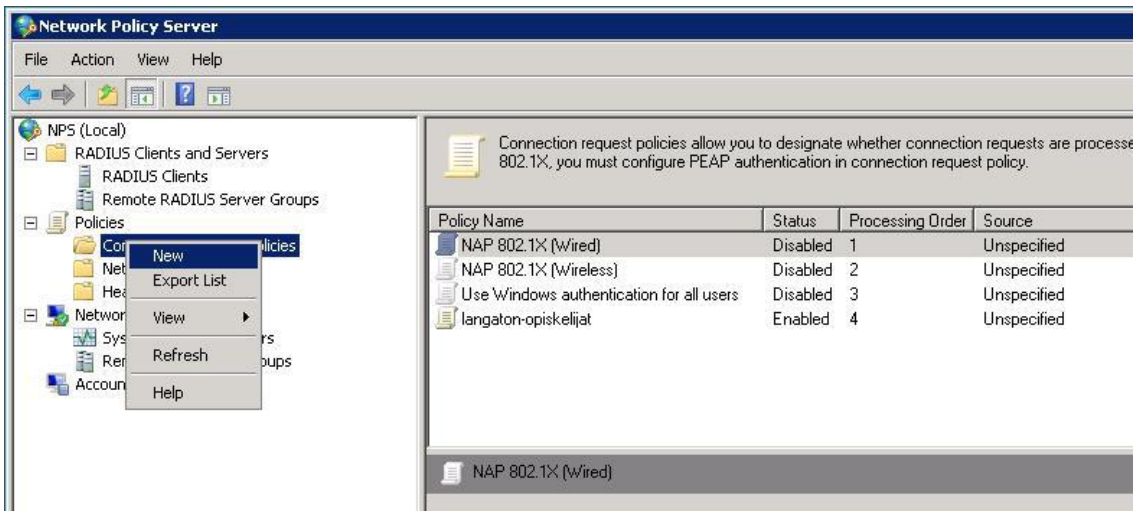


Kuva 37: RADIUS-asiakkaan luominen



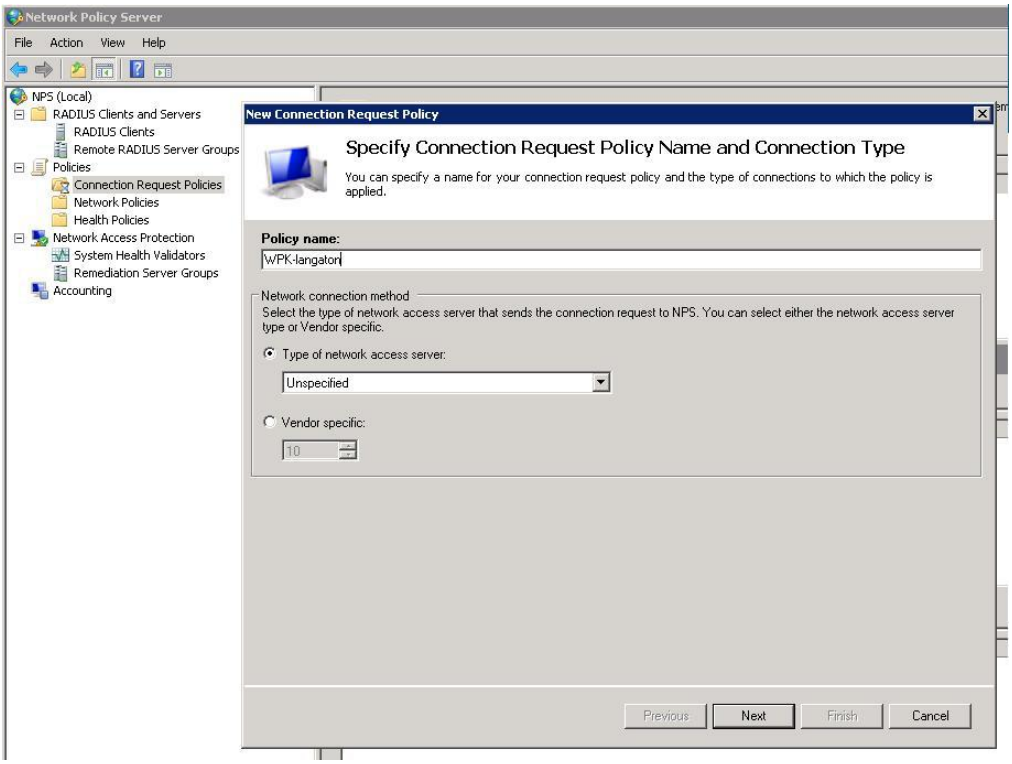
Kuva 38: RADIUS-asiakkaiden lista

Verkkopolitiikkojen luonti aloitetaan kohdasta Connection request policy, joka määrittelee yhteyspyynnön verkkoon pääsemiseksi. Klikataan hiiren oikealla ja valitaan New (kuva 39).



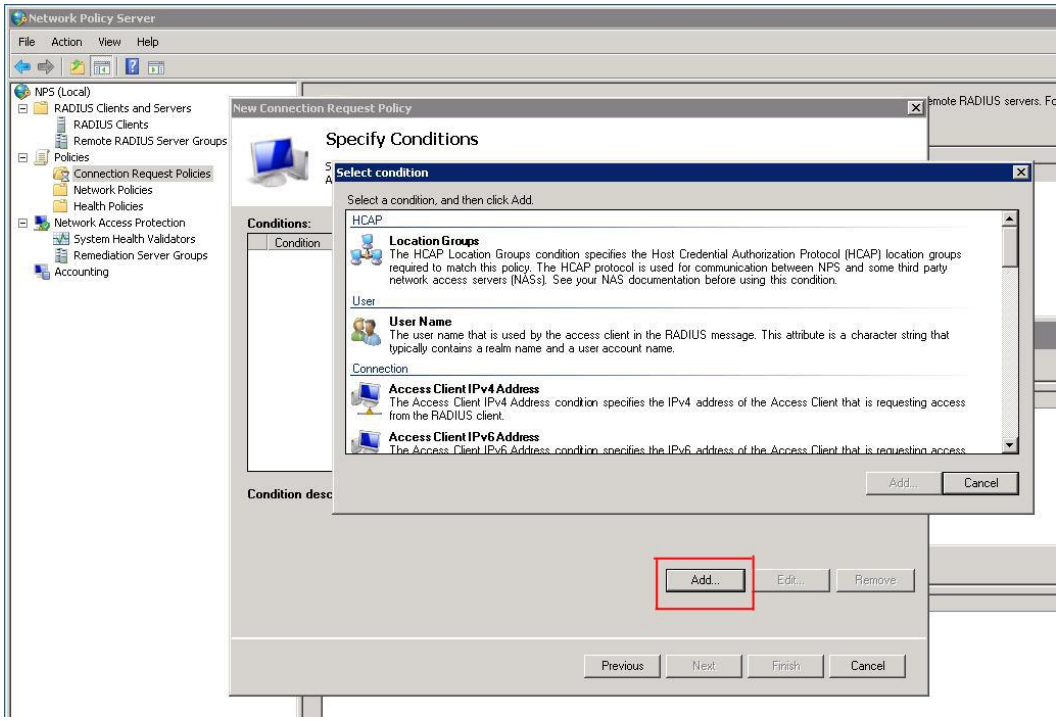
Kuva 39: Yhteyspyyntöpolitiikan luomisen aloitus

Seuraavaksi nimetään politiikka. Nimeämisessä on hyvä olla looginen ja johdonmukainen, ja nimetä politiikka vaikka samalla nimellä mitä langaton verkkokin on. Nimen antamisen jälkeen painetaan Next (kuva 40).



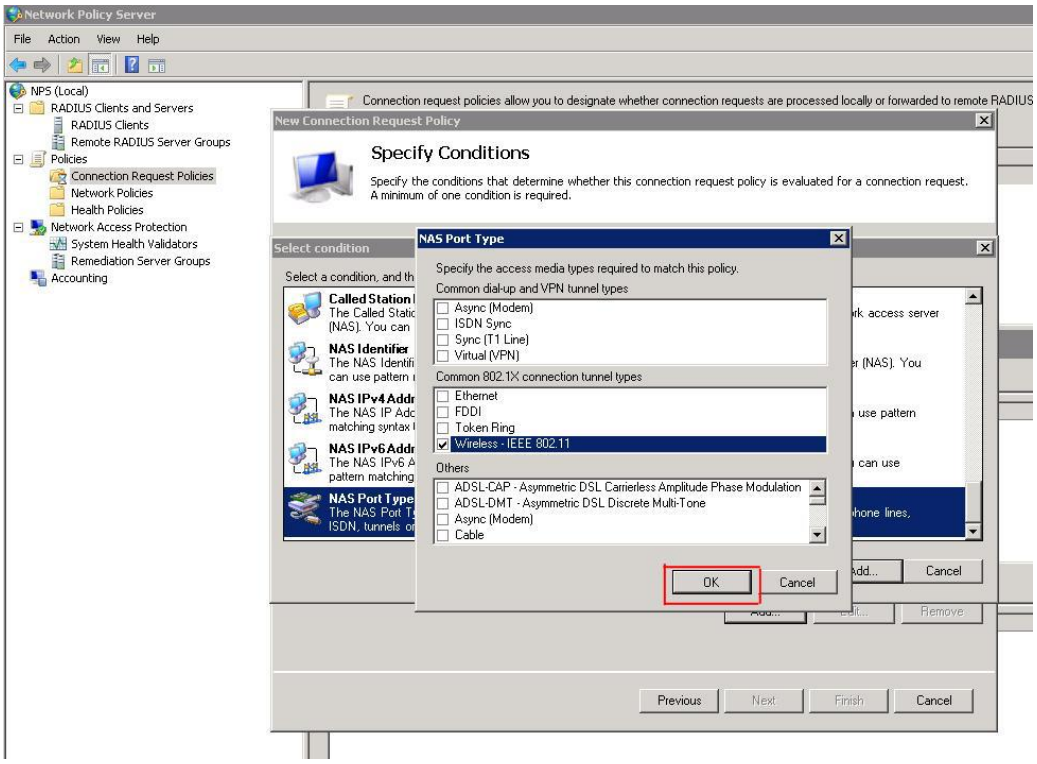
Kuva 40: Politiikan nimeäminen

Seuraavaksi määritellään ehdot sille, miten verkkoon pääsyä haetaan. Painetaan kohdasta Add..., jolloin aukeaa uusi ikkuna, josta pääsee valitsemaan ehtoja (kuva 41).



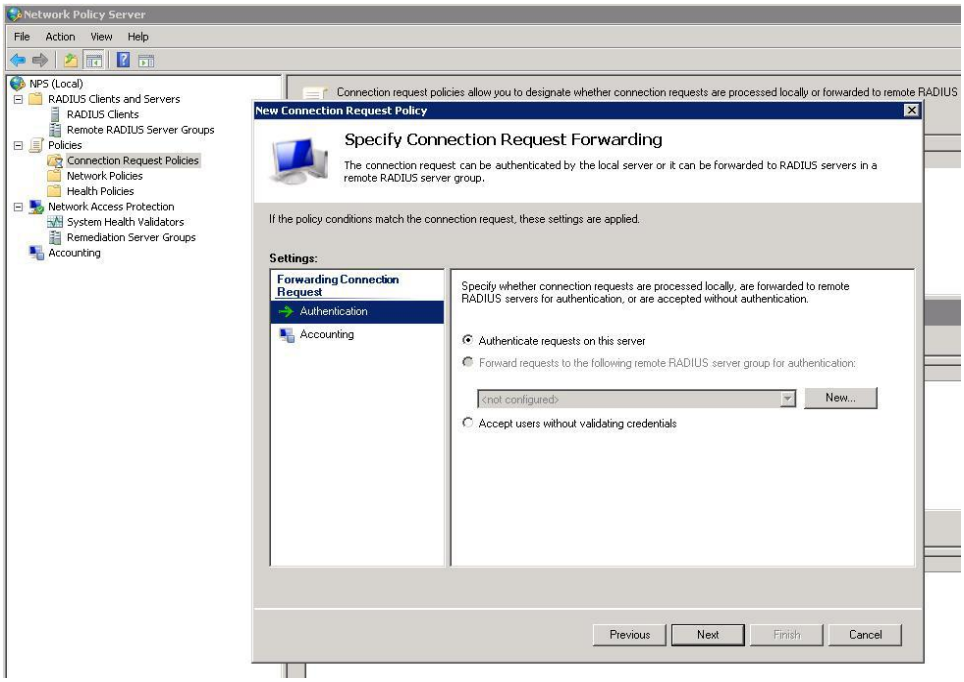
Kuva 41: Ehtojen lisääminen 1

Koska kyseessä on langaton verkko, valitaan kohta NAS Port Type ja sieltä Wireless – IEEE 802.11. Painetaan OK. Ja sen jälkeen Next (kuva 42).



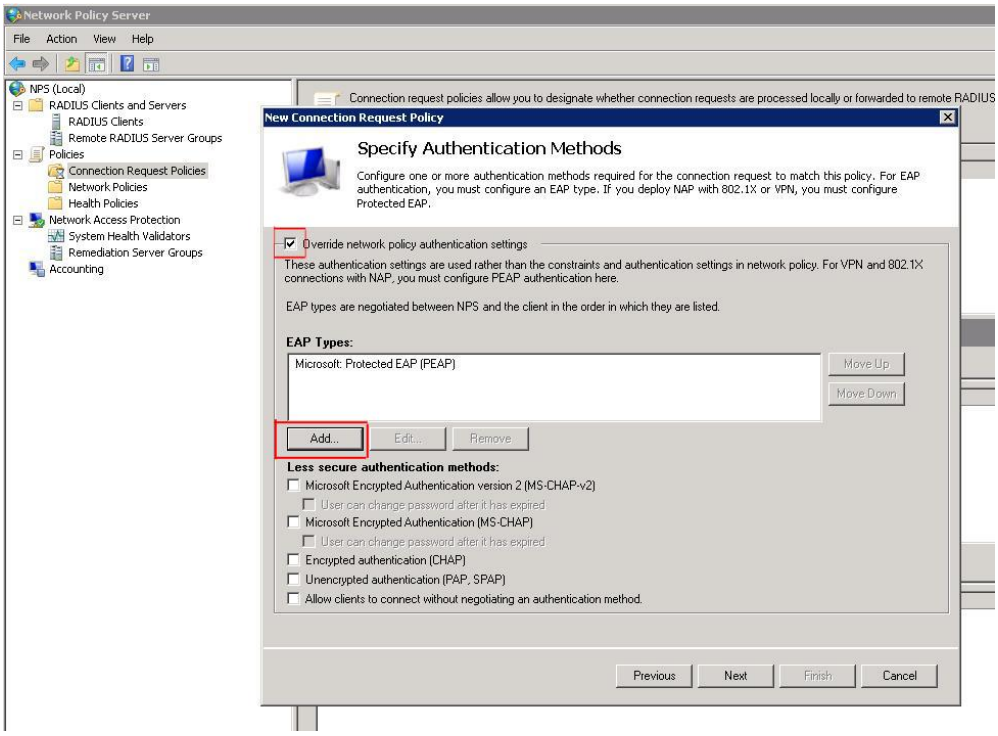
Kuva 42: Ehtojen lisääminen 2

Seuraavassa kohdassa annetaan olla oletusasetuksena Authenticate requests on this server. Halutessaan pääsypyynnöt voisi ohjata myös toiselle RADIUS-palvelimelle mikäli verkossa on niitä useampi, tai hyväksyä yhteyspyynnöt ilman autentikointia. Painetaan Next (kuva 44)

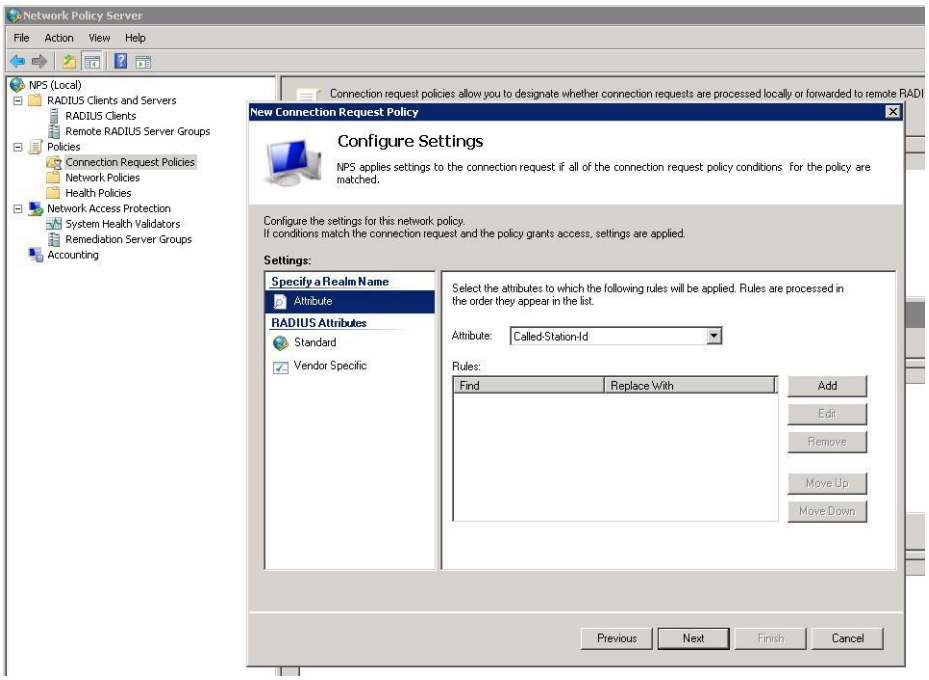


Kuva 44: Autentikoinnin asettaminen

Autentikointitapa-kohdassa laitetaan rasti kohtaan Override network policy authentication settings jotta päästään lisäämään verkkoon Microsoft: Protectes EAP (PEAP). Painetaan Next (kuva 44). Ja sen jälkeen vielä Next (kuva 45).

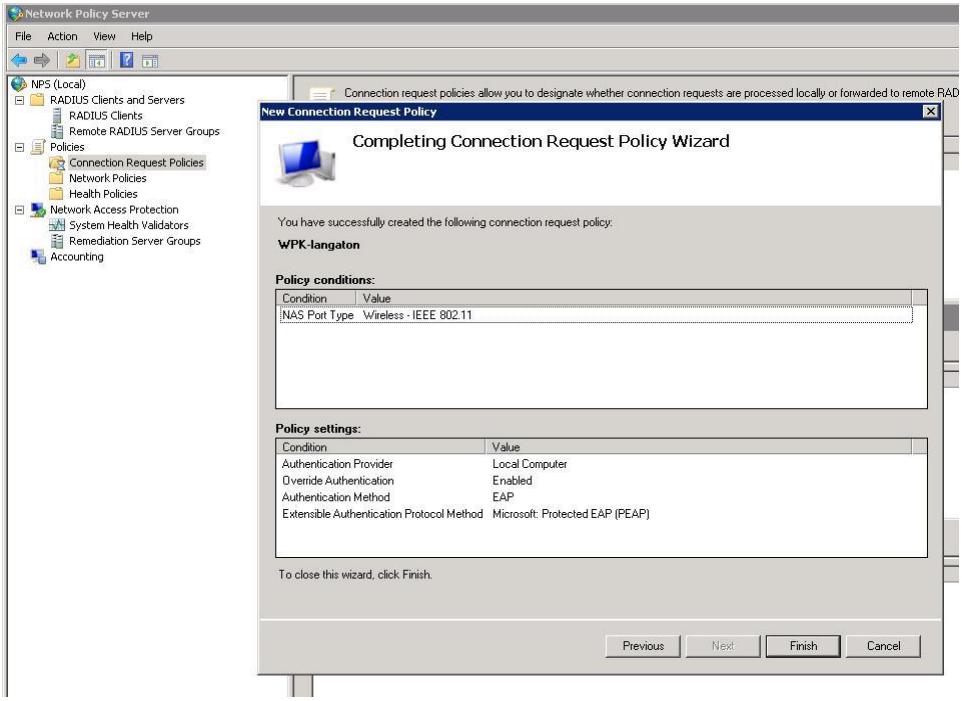


Kuva 44: Microsoft Protected EAP (PEAP) asettaminen

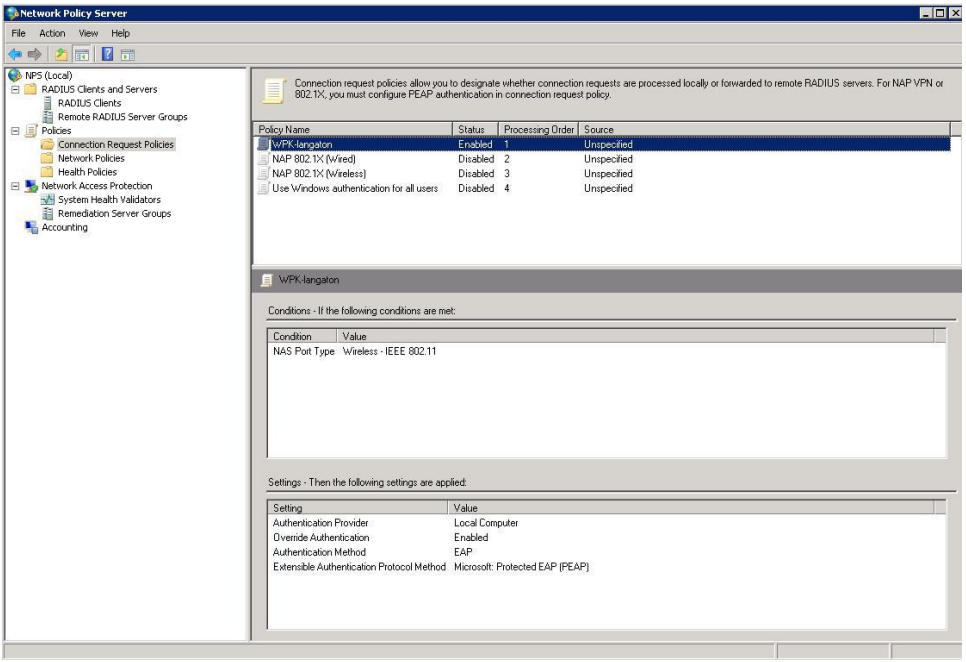


Kuva 45: Yhteyspolitiikan luomista

Seuraava sivu tekee yhteenvedon laitetuista asetuksista, joita pääsee vielä muuttamaan halutessaan palaamalla taaksepäin (Previous) (kuva 46). Mikäli kaikki asetukset ovat kunnossa, voidaan painaa Finish, jolloin uusi yhteyspyyntöpolitiikka näkyy listassa (kuva 47).

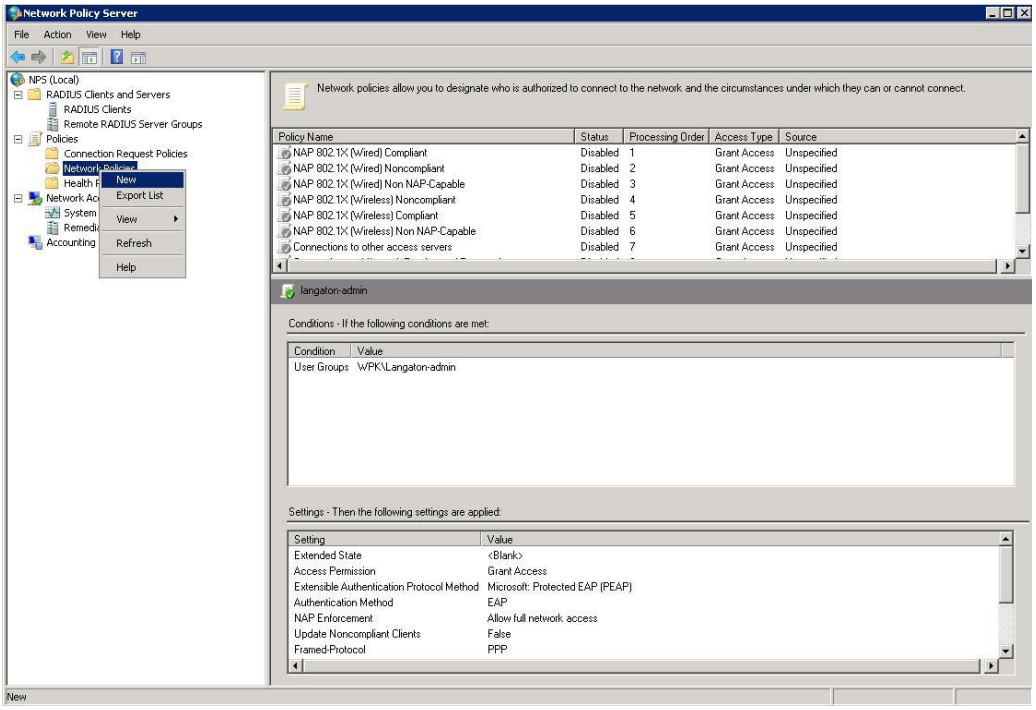


Kuva 46: Yhteenveto



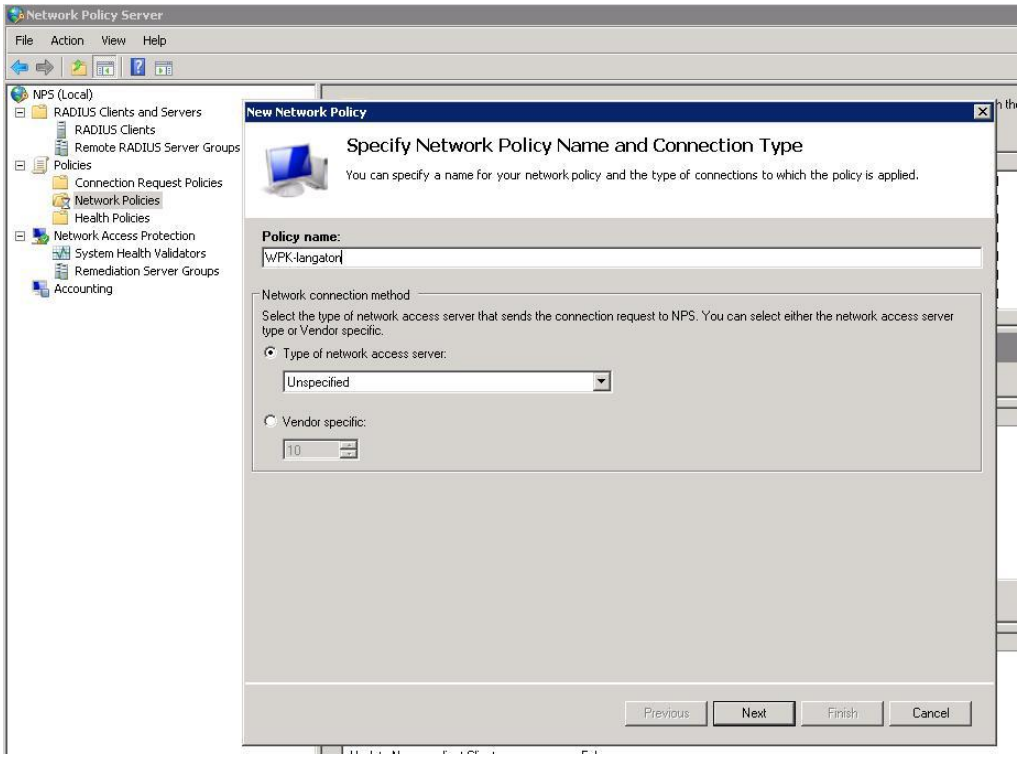
Kuva 47: Yhteyspolitiikkalista

Seuraavaksi luodaan uusi verkkopolitiikka, eli säädetään tarkemmin esimerkiksi sitä, ketkä verkkoon saavat kirjautua. Klikataan hiiren oikealla kohtaa Network Policies ja valitaan New (kuva 48).



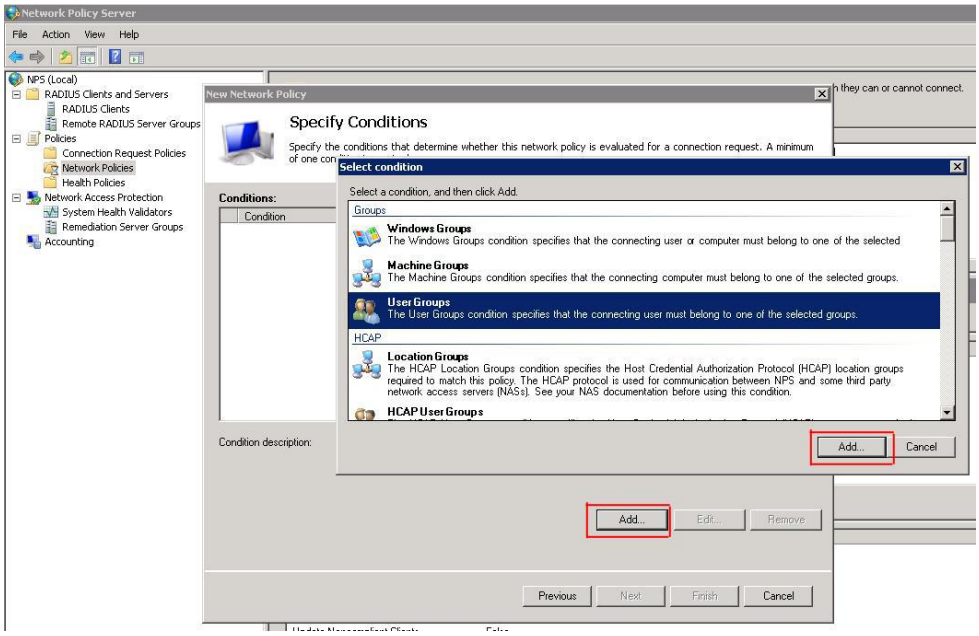
Kuva 48: uuden verkkopolitiikan luomisen aloitus

Seuraavassa annetaan jälleen nimi uudelle politiikalle. Tässäkin on hyvä olla johdonmukainen ja nimetä politiikka vaikka samalla nimellä mitä langatonkin verkko on. Painetaan Next (kuva 49).

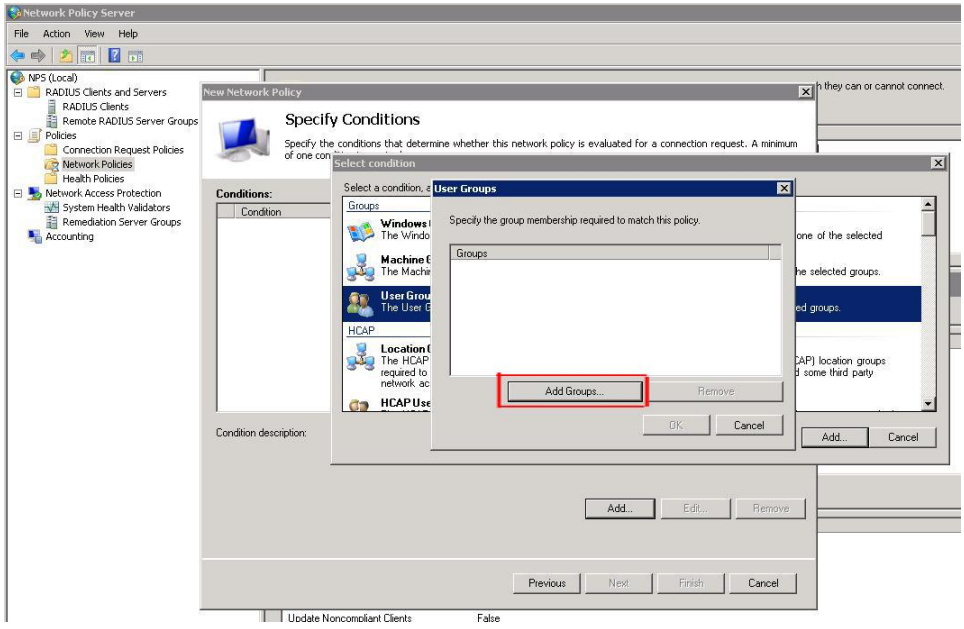


Kuva 49: verkkopolitiikan nimeäminen

Seuraavaksi valitaan ehdot. Painetaan Add... Haluamme määritellä mistä käyttäjäryhmistä käyttäjien pitää olla verkkoon päästäkseen, joten valitsemme User Groups ja painamme Add... (kuva 50). Painetaan Add Group… (kuva 51).

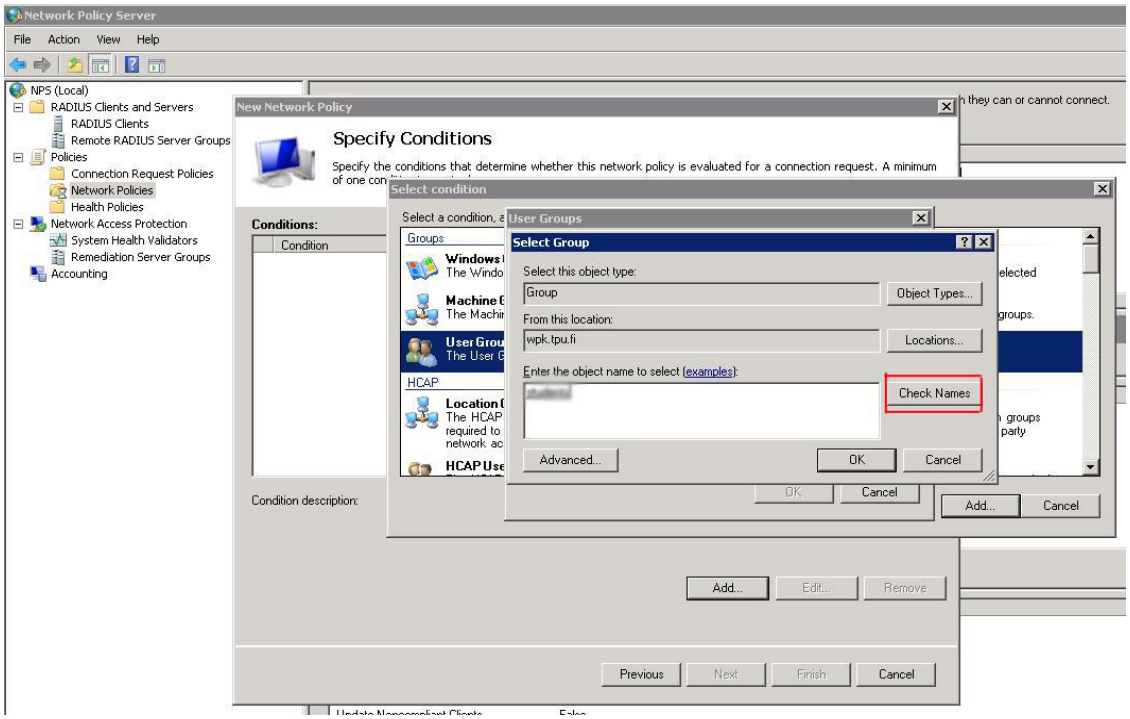


Kuva 50: Ehtojen asettaminen

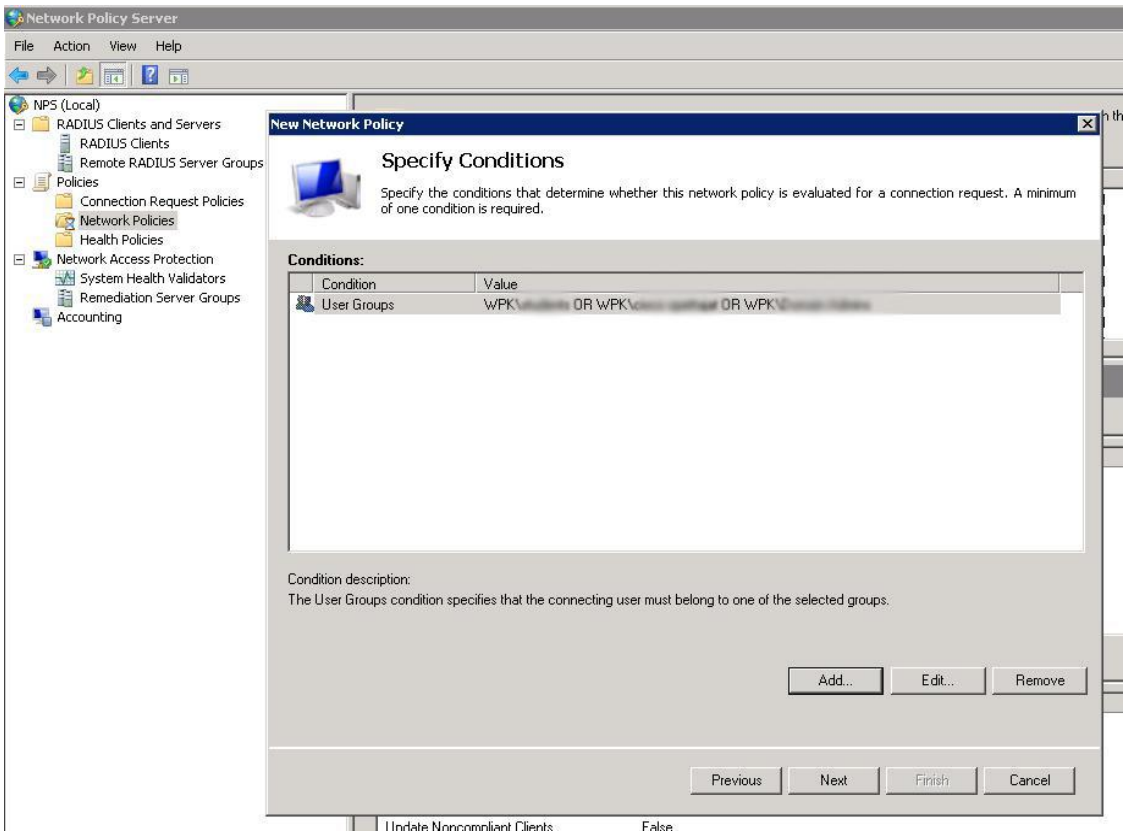


Kuva 51: Ryhmän lisäämisen aloitus

Enter the object name to select -laatikkoon kirjoitetaan halutun ryhmän nimi ja painetaan Check Names. Mikäli ryhmä löytyy, ryhmän nimi alleviivataan (kuva 52). Toistetaan nämä vaiheet niin monta kertaa kuin on tarve. Kun halutut ryhmät on lisätty, painetaan OK. Ryhmät ilmestyvät näkyviin ehtolistaan (kuva 53). Painetaan Next.

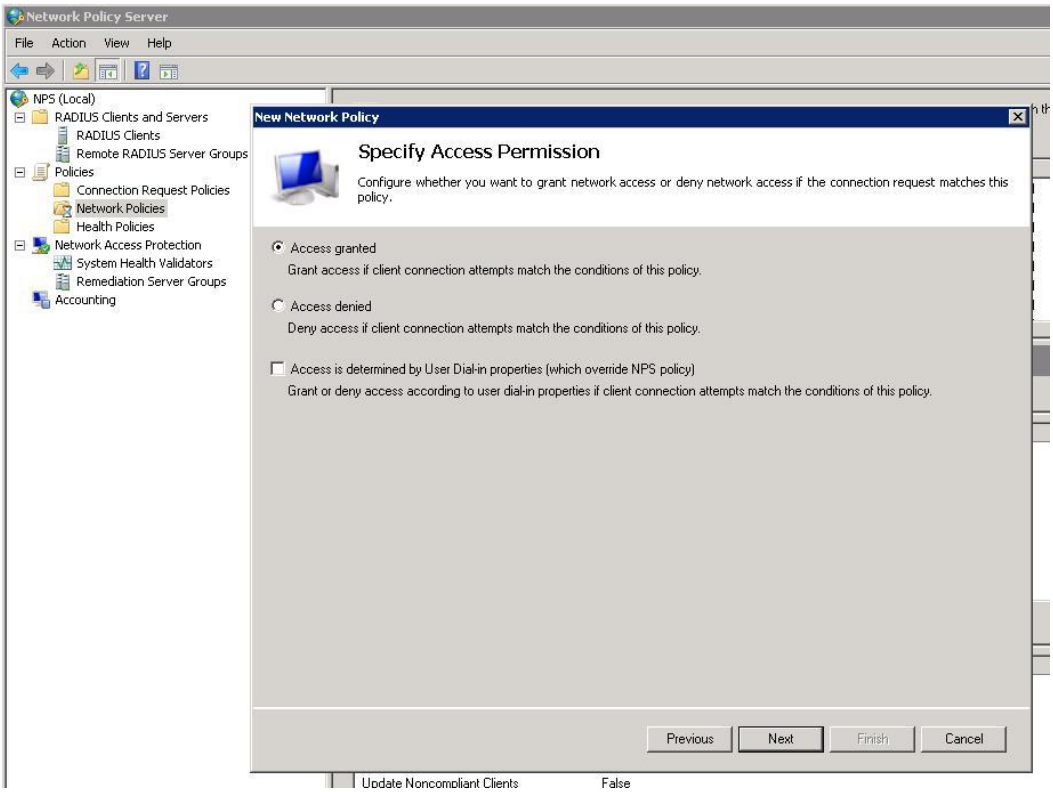


Kuva 52: Ryhmän lisääminen



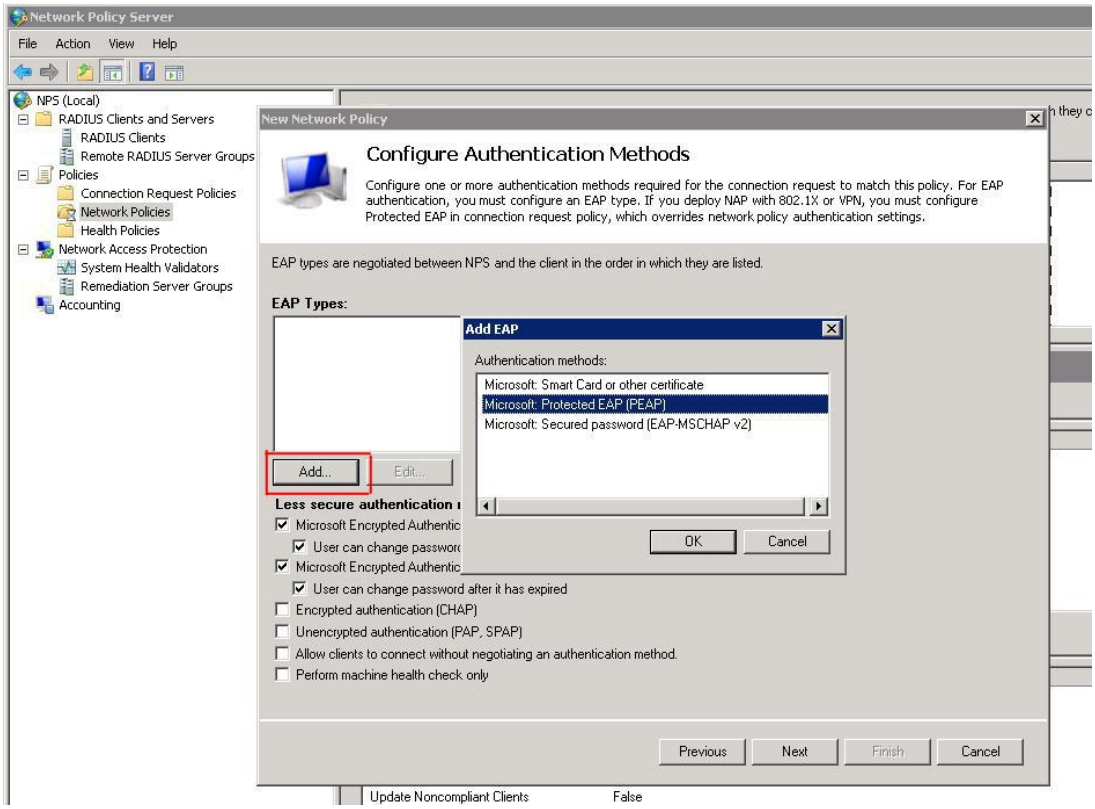
Kuva 53: Ehtolista

Seuraavaksi valitaan, annetaanko kyseiselle ryhmälle oikeudet verkkoon liittymiseen, vai kielletäänkö ne (kuva 54). Valinnan jälkeen painetaan Next.



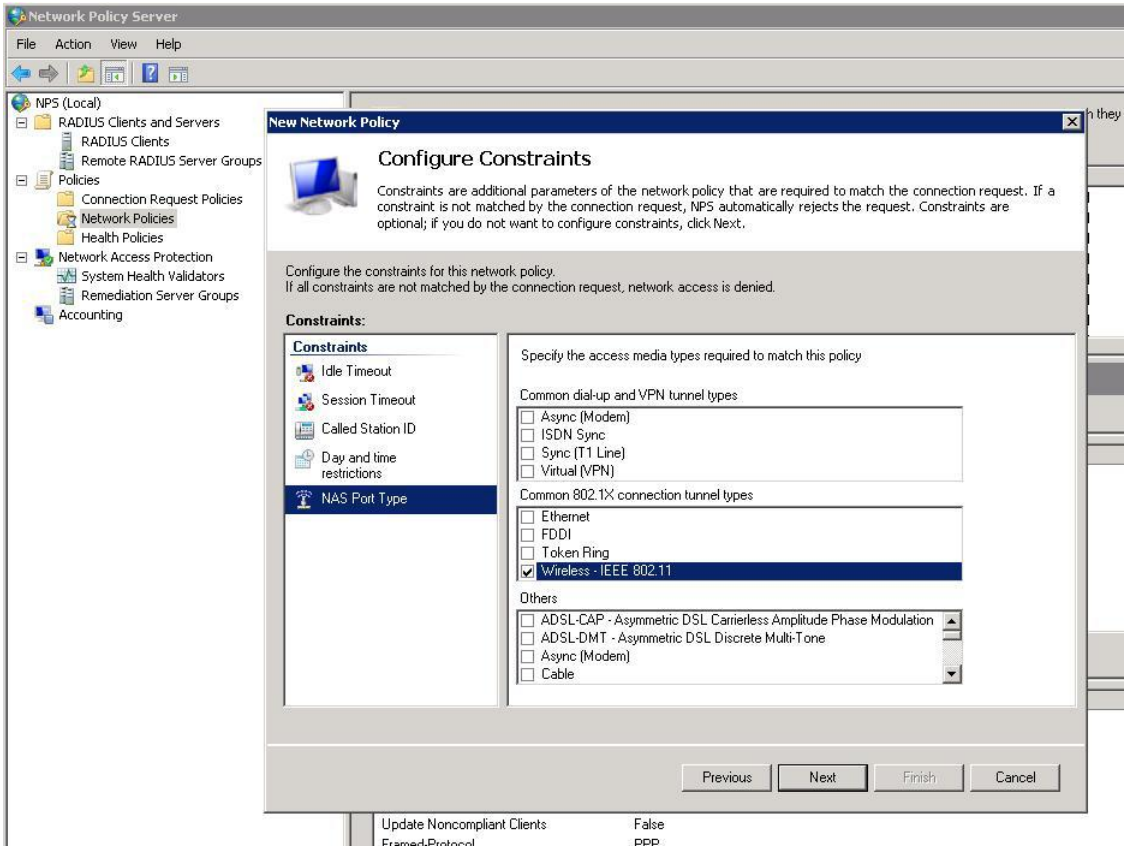
Kuva 54: Pääsyn myöntäminen tai kieltäminen

Autentikointitavaksi valitaan jälleen Microsoft: Protected EAP (PEAP) ja painetaan Next (kuva 55).

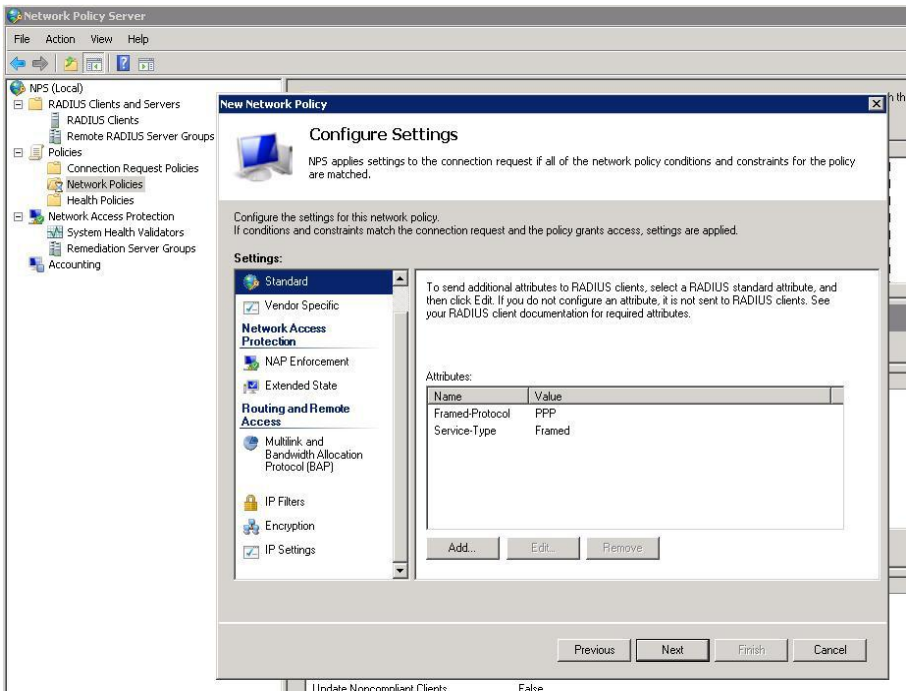


Kuva 55: PEAP-asetuksen valinta

Valitaan, että käyttäjä pääsee verkkoon langattomasti. NAS Port type Wireless – IEEE 802.11. Painetaan Next (kuva 56). Seuraavasta painetaan Next (kuva 57).

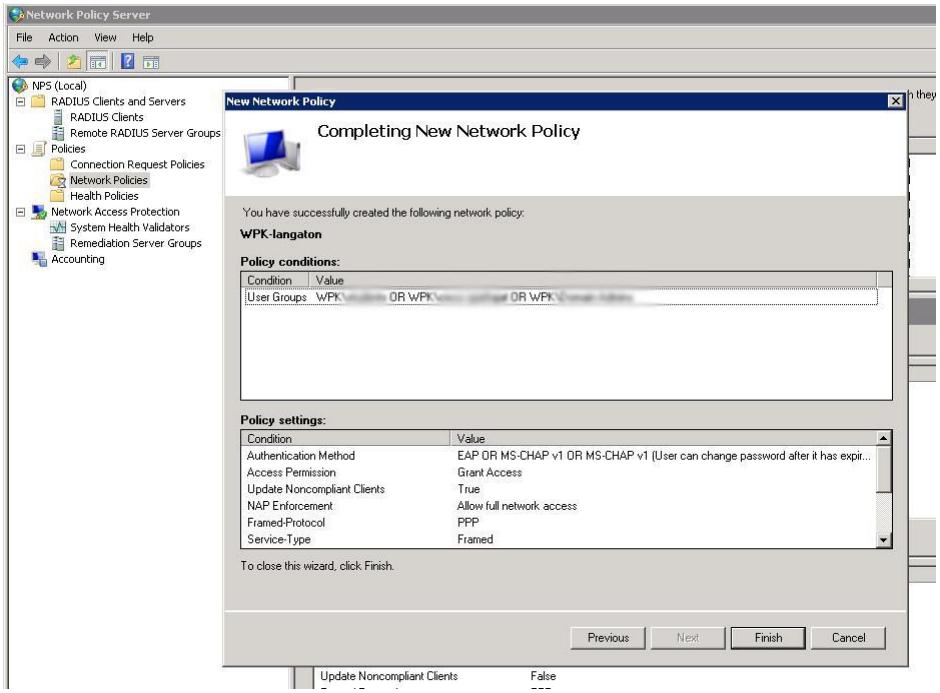


Kuva 56: NAS port type –valinta

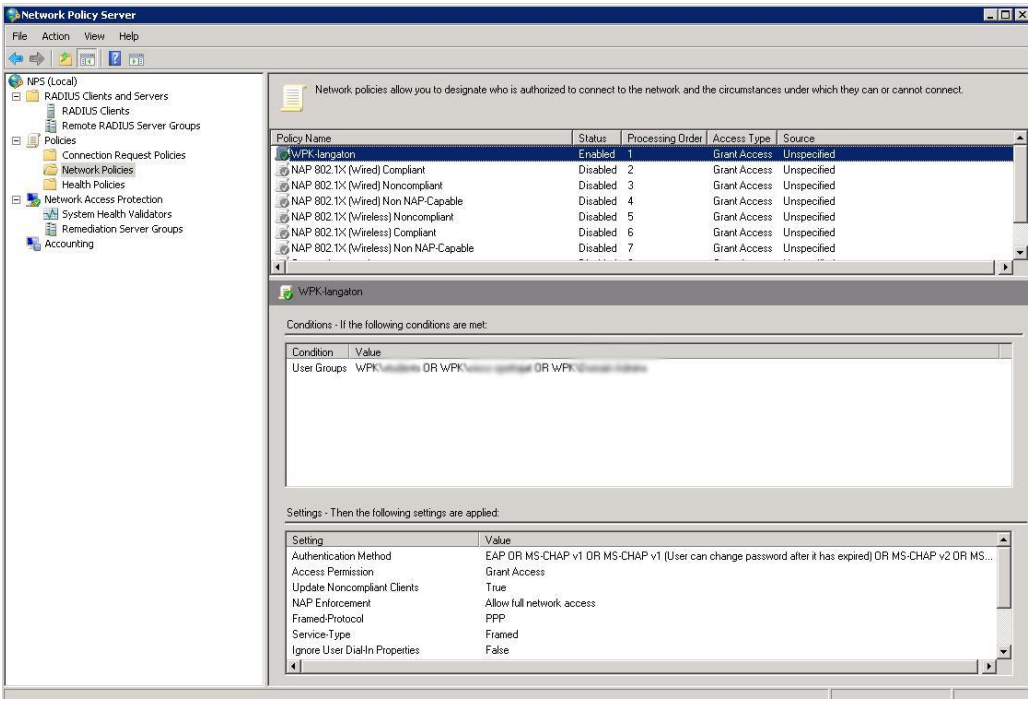


Kuva 57: Asetuksissa eteenpäin

Tulee jälleen koontisivu (kuva 58). Jos asetukset ovat kunnossa, painetaan Finish ja uusi politiikka ilmestyy listaan (kuva 59).



Kuva 58: Yhteenveto määritellyistä asetuksista



Kuva 59: RADIUS-asetukset valmiit

AHK&POSTI

Taulukko 5: AHK:n VLAN-konfiguroinnit

Konfiguraatio	Tarkoitus
interface GigabitEthernet0/13 description Eyjafjallajokull switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,18,19 switchport mode trunk	Avataan kontrollerille menevä portti ja sallitaan siinä VLAN-liikenne virtuaalisista lähiverkoista 1, 18 ja 19 (1 = hallintaverkko, 18 = opiskelijaverkko ja 19 = vierasverkko).
interface Vlan18 ip address 172.18.X.X X.X.X.X ip helper-address 172.16.X.X ip helper-address 172.16.X.X	Luodaan virtuaalisen lähiverkon liitäntä ja ohjataan se kysymään DHCP-tietoja kahdelta verkossa olevalta DCHP-palvelimelta.
interface Vlan19 ip address 172.19.X.X X.X.X.X ip helper-address 172.16.X.X ip helper-address 172.16.X.X	Luodaan virtuaalisen lähiverkon liitäntä ja ohjataan se kysymään DHCP-tietoja kahdelta verkossa olevalta DCHP-palvelimelta.

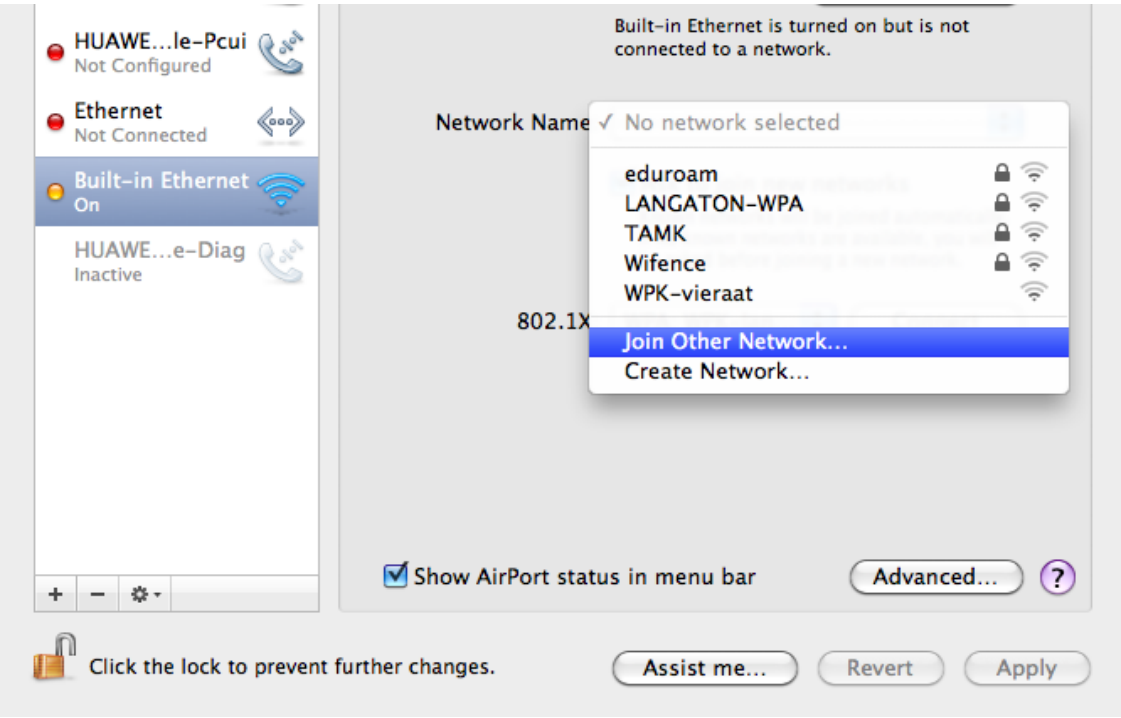
Taulukko 6: Postille tehdyt konfiguraatiomuutokset

Konfiguraatio	Tarkoitus
access-list 18 permit 172.18.0.0 0.0.255.255 access-list 19 permit 172.19.0.0 0.0.255.255	Pääsylistojen luominen, sallitaan liikenne opiskelija- ja vierailijaverkoista.
ip nat pool 18-pool 195.148.X.X 195.148.X.X netmask 255.255.255.X ip nat pool 19-pool 195.148.X.X 195.148.56.191 netmask 255.255.255.X	Luodaan NAT-puulit, varataan käyttöön muutama julkisen sarjan IP-osoite.
ip nat inside source list 18 pool 18-pool overload ip nat inside source list 19 pool 19-pool overload	Otetaan käyttöön NAT overload eli PAT.

Verkkoihin kirjautuminen

Apple MAC OS X

Avataan Network Preferences, ja sieltä Network Name -pudotusvalikosta valitaan Join other Network... (kuva 60)



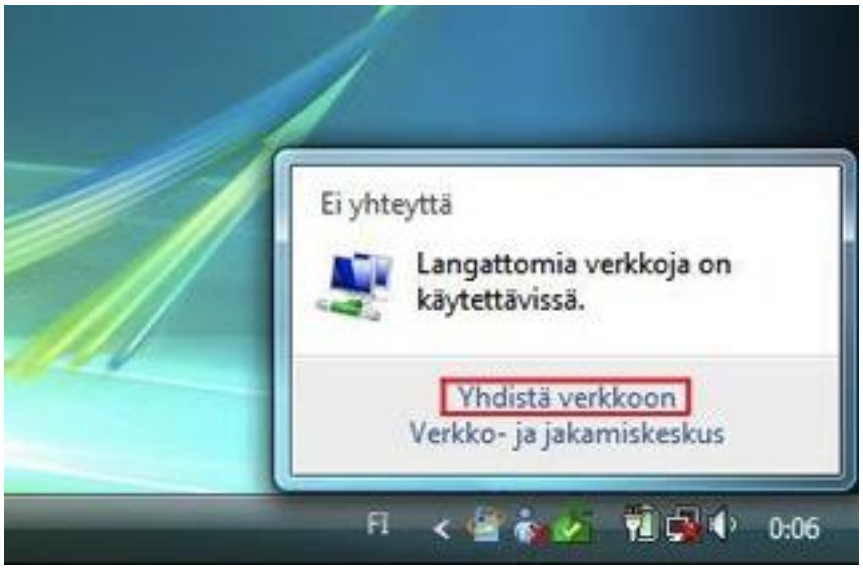
Kuva 60: Yhteyden muodostaminen, Macintosh 1

Network Name -kohtaan kirjoitetaan WPK-langaton. Securityksi valitaan WPA2 Enterprise, sitten syötetään oman koulun WPK-verkon tunnukset ja painetaan Join (Remember this network -rasti on hyvä olla, jolloin Mac muistaa asetukset seuraavaa kertaa varten). Kone liittyy verkkoon (kuva 61).

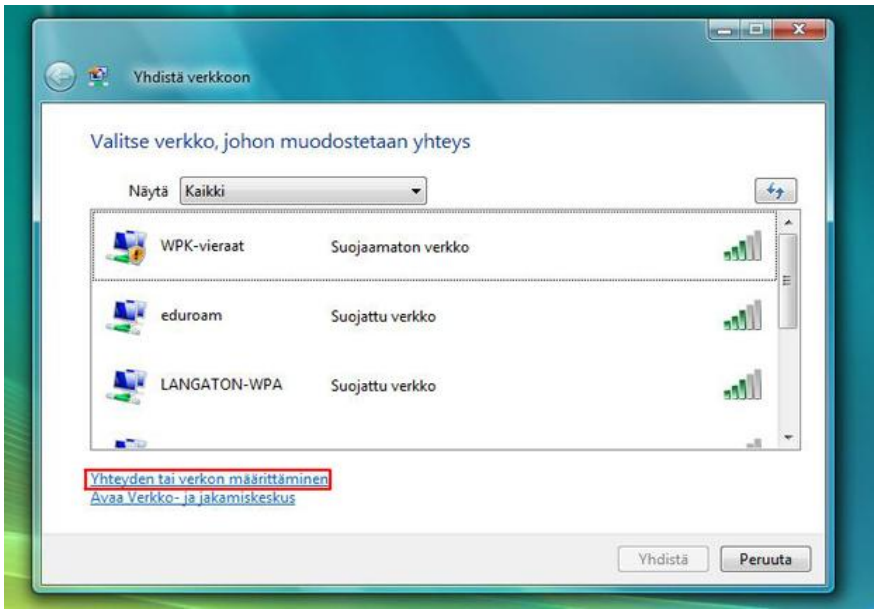
Kuva 61: Yhteyden muodostaminen, Macintosh 2

Windows Vista

Vistassa täytyy olla vähintään Service Pack 1 asennettuna, muuten verkkoon ei pääse. Ensimmäisenä vaiheena Vista antaa ilmoituksen, että langattomia verkkoja on käytettävissä. Klikataan Yhdistä verkkoon (kuva 62). Klikataan Yhteyden tai verkon määrittäminen (kuva 63).

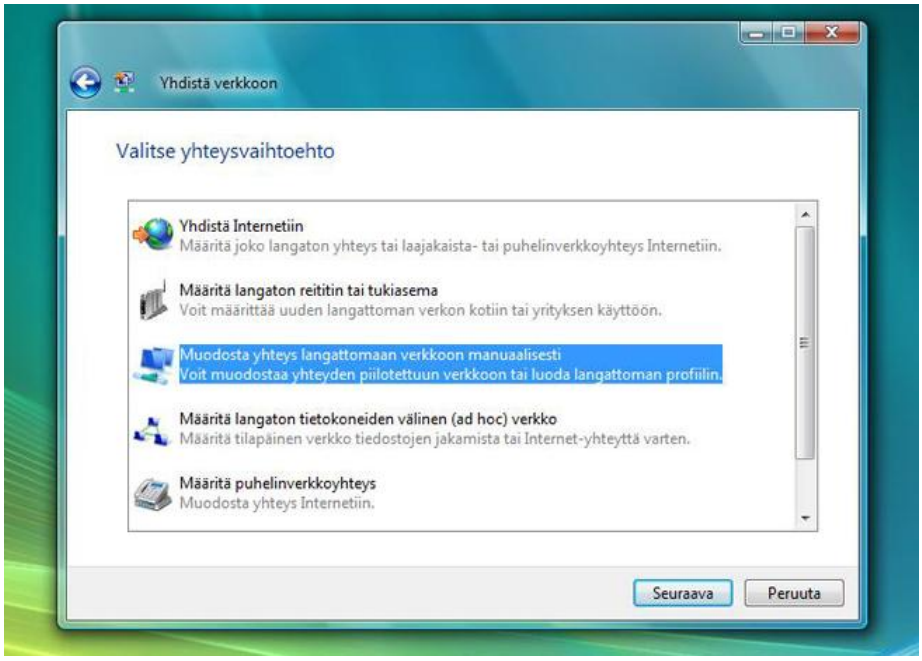


Kuva 62: Yhteyden muodostaminen, Vista 1



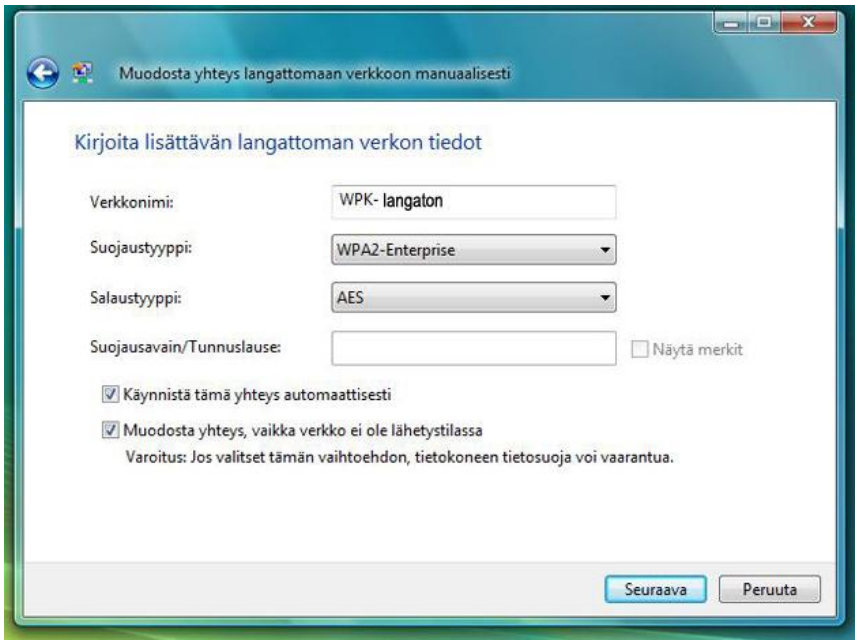
Kuva 63: Thteyden muodostaminen, Vista 2

Valitaan Muodosta yhteys langattomaan verkkoon manuaalisesti ja painetaan Seuraava (kuva 64).



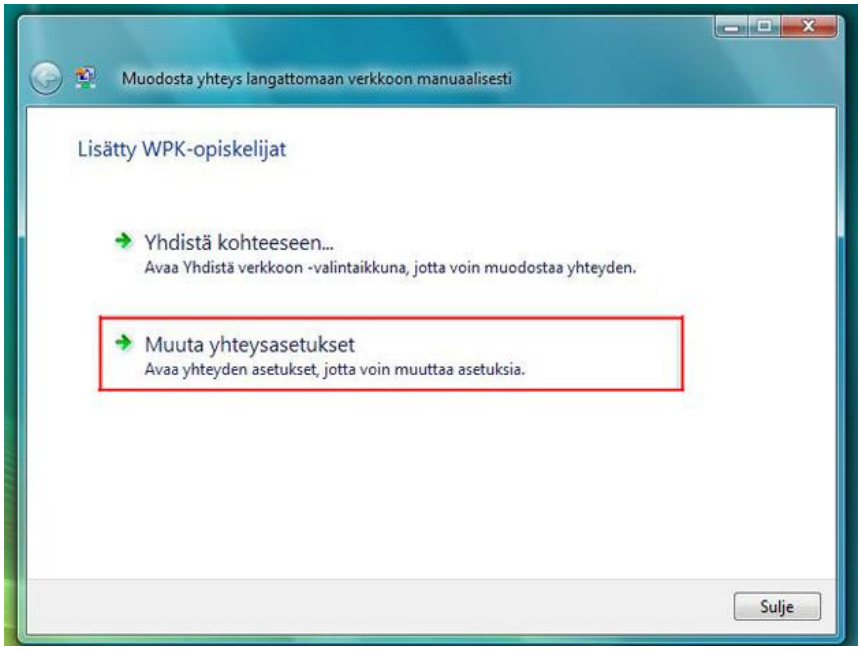
Kuva 64: Yhteyden muodostaminen, Vista 3

Seuraavaksi annetaan tietoja langattomasta verkosta. Verkkonimeksi WPK-langaton, suojaustyypiksi WPA2-Enterprise ja salaustyypiksi AES. Tarkista myös että rastit ovat kohdissa ”Käynnistä tämä yhteys automaattisesti” ja ”Muodosta yhteys, vaikka verkko ei ole lähetystilassa” (kuva 65). Painetaan seuraava.



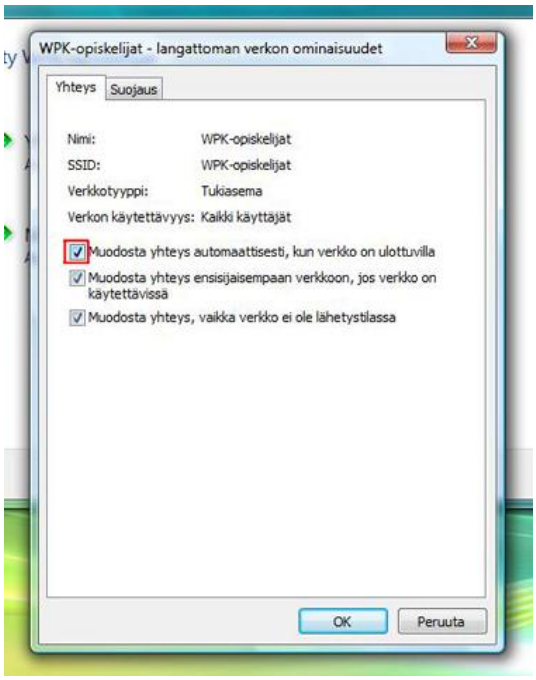
Kuva 65: Yhteyden muodostaminen, Vista 4

Seuraavalta sivulta ei voida vielä mennä yhteyden muodostamiseen, vaan täytyy käydä muuttamassa yhteysasetuksia (kuva 66).



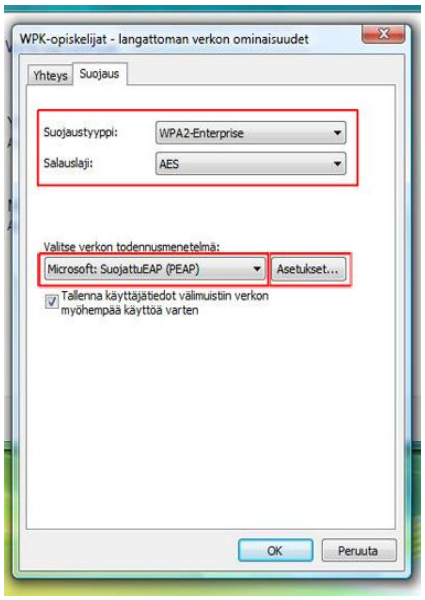
Kuva 66: Yhteyden muodostaminen, Vista 5

Yhteys-välilehdeltä voi laittaa rastin kohtaan ”Muodosta yhteys automaattisesti, kun verkko on ulottuvilla” (mikäli haluaa koneen yhdistyvän verkkoon automaattisesti kun kone on verkon ulottuvilla) (kuva 67).



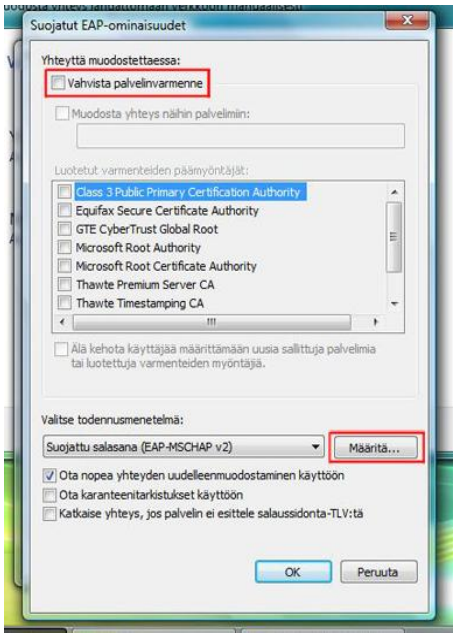
Kuva 67: Yhteyden muodostaminen, Vista 6

Suojaus-välilehdeltä suojaustyypiksi valitaan WPA2-Enterprise ja salauslajiksi AES. Verkon todennusmenetelmäksi valitaan Microsoft: SuojattuEAP (PEAP). Tärkeää on myös muistaa laittaa rasti kohtaan ”Tallenna käyttäjätiedot välimuistiin verkon myöhempää käyttöä varten”. Klikataan Asetukset... (kuva 68).



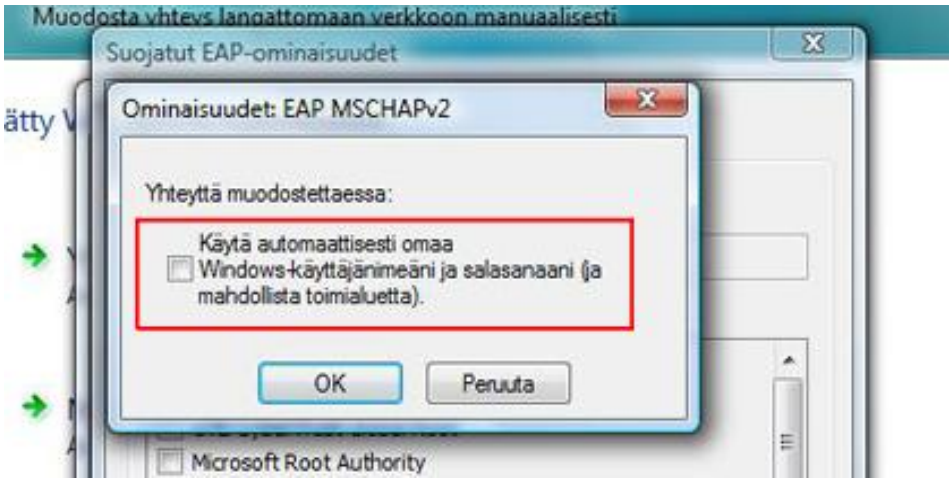
Kuva 68: Yhteyden muodostaminen, Vista 7

Otetaan rasti pois kohdasta ”Vahvista palvelinvarmenne” ja määritetään todennusmenetelmän ominaisuudet painamalla Määritä... (kuva 69).

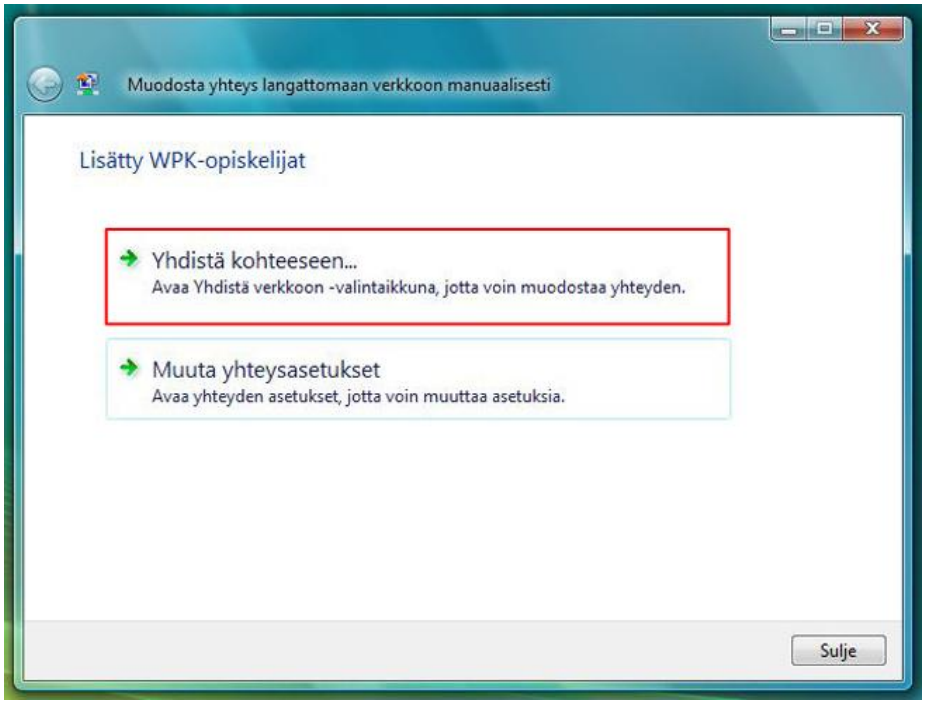


Kuva 69: Yhteyden muodostaminen, Vista 8

Otetaan rasti pois kohdasta ”Käytä automaattisesti omaa Windows-käyttäjänimeäni ja salasanaani (ja mahdollista toimialuetta)” (kuva 70). Näiden asetusten asettamisen jälkeen painetaan OK:ta muutaman kerran että päästään takaisin yhteyden muodostamiseen. Valitaan Yhdistä kohteeseen... (kuva 71)

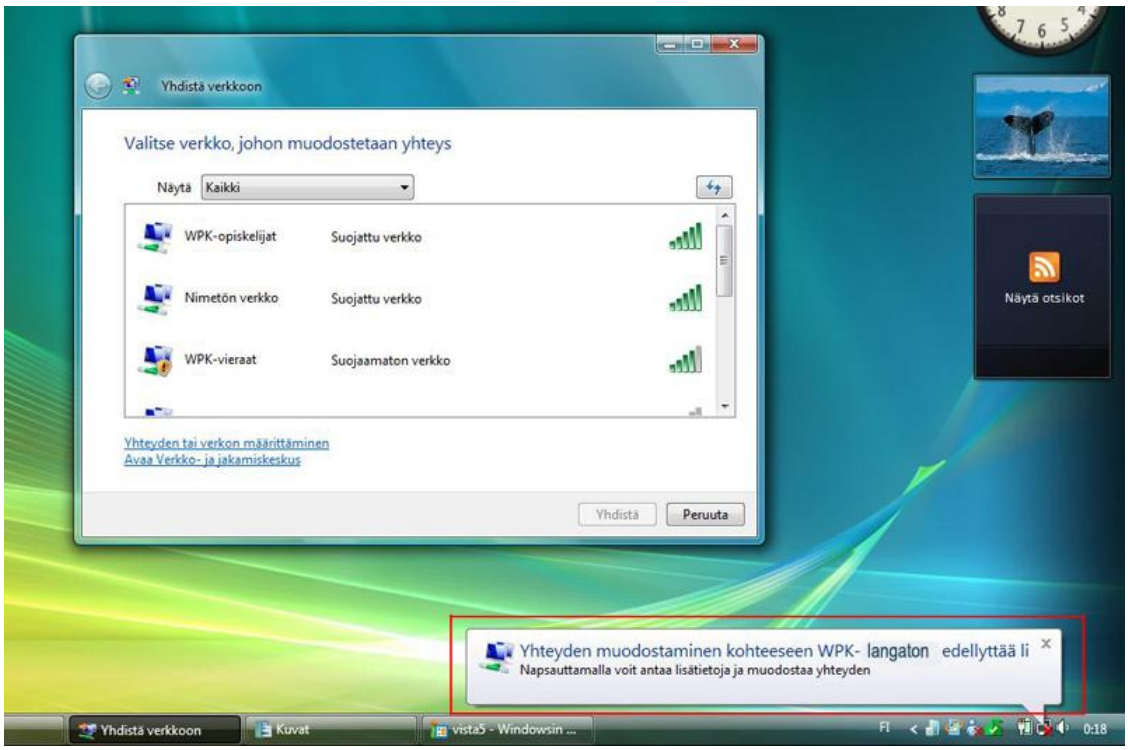


Kuva70: Yhteyden muodostaminen, Vista 9



Kuva 71: Yhteyden muodostaminen, Vista 10

Verkkoa ei voi valita suoraan listasta, vaan odotetaan, että Vista ilmoittaa oikeassa alanurkassa kuplaviestinä yhteyden muodostamisesta. Napsautetaan kuplaa (kuva 72).



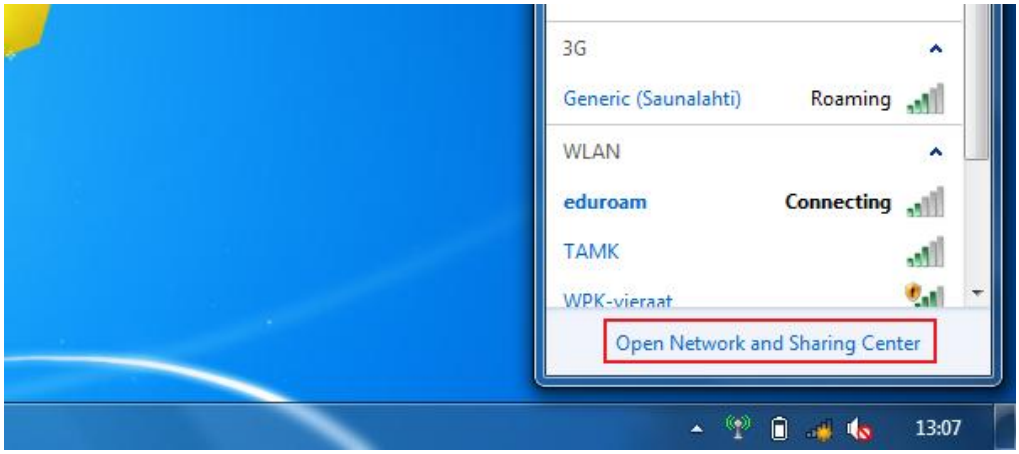
Kuva 72: Yhteyden muodostaminen, Vista 11

Näiden vaiheiden jälkeen pääsee syöttämään omat WPK-verkon tunnuksensa ja verkkoon kirjautuminen onnistuu (kuva 73).

Kuva 73: Yhteyden muodostaminen, Vista 12

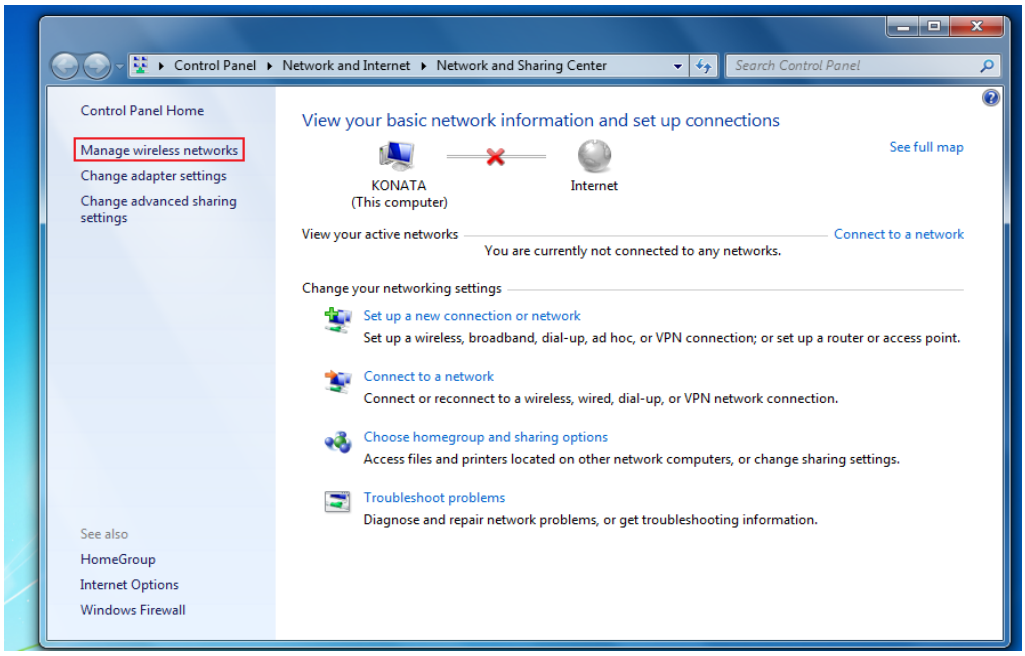
Windows 7

Ensimmäisenä avataan Network and Sharing Center (kuva 74)

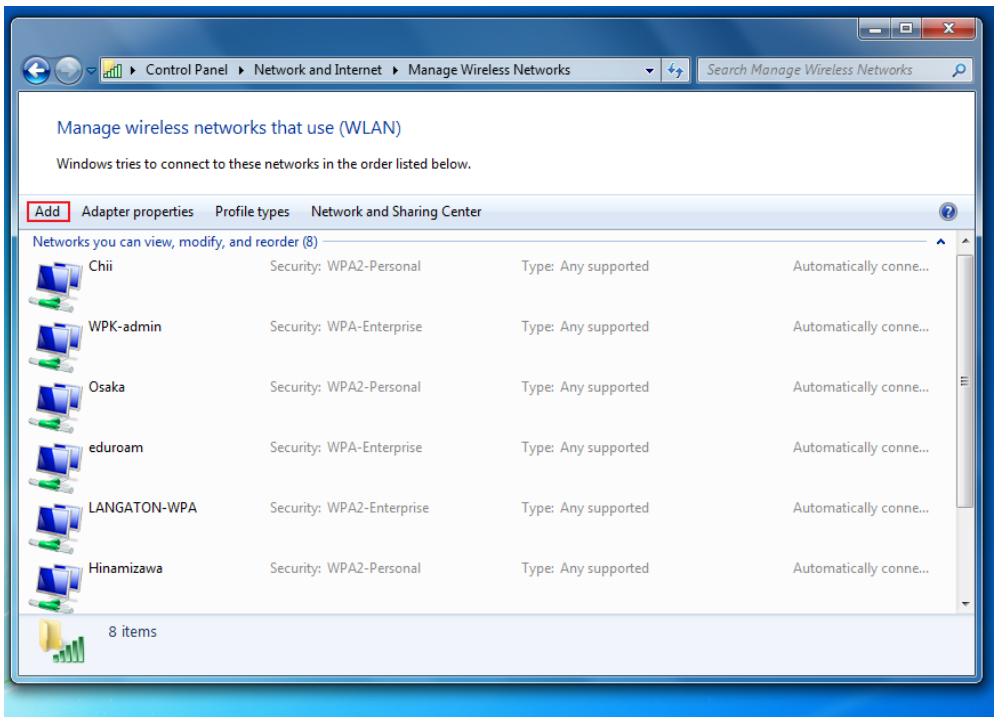


Kuva 74: Yhteyden muodostaminen Windows 7, 1

Verkko pitää määritellä manuaalisesti, joten valitaan Manage wireless networks (kuva 75). Painetaan Add (kuva 76).

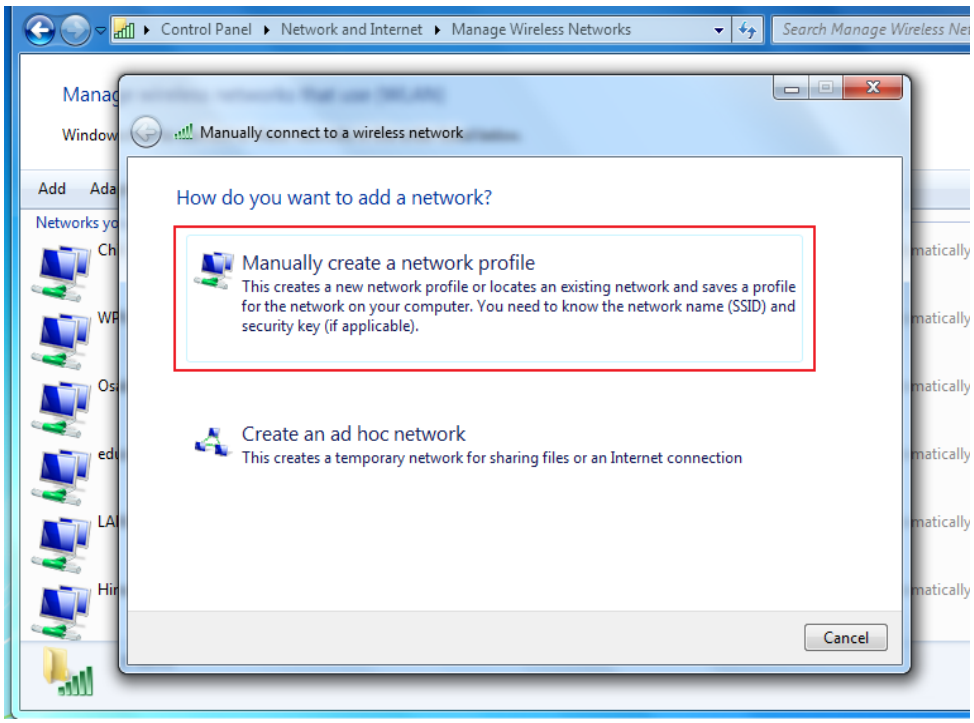


Kuva 75: Yhteyden muodostaminen Windows 7, 2



Kuva 76: Yhteyden muodostaminen Windows 7, 3

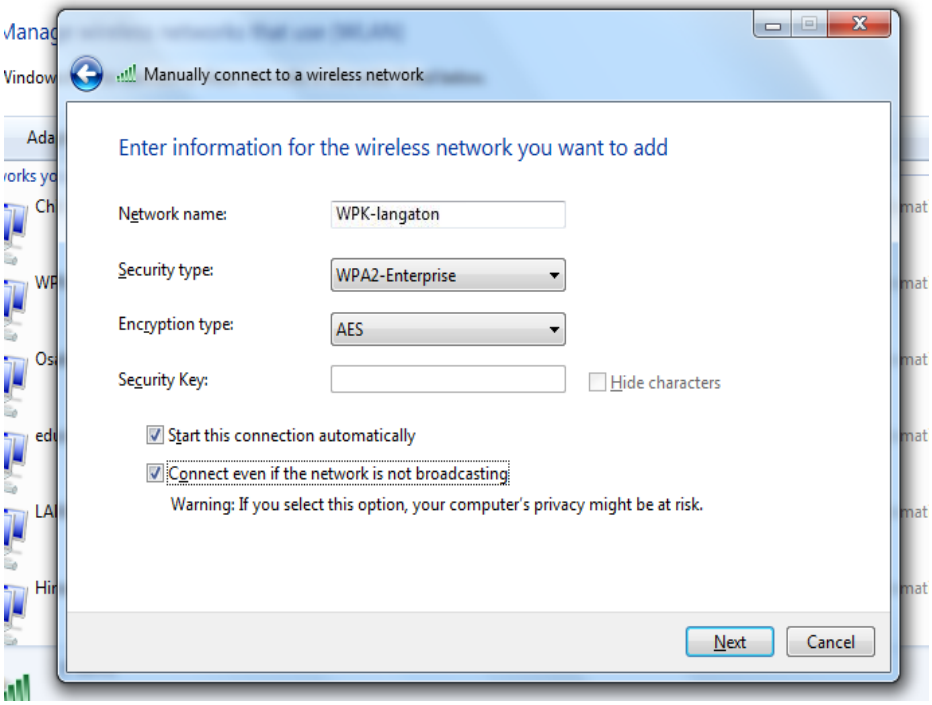
Jotta päästään manuaalisesti syöttämään verkon vaatimat asetukset, valitaan Manually create a network profile (kuva 77).



Kuva 77: Yhteyden muodostaminen Windows 7, 4

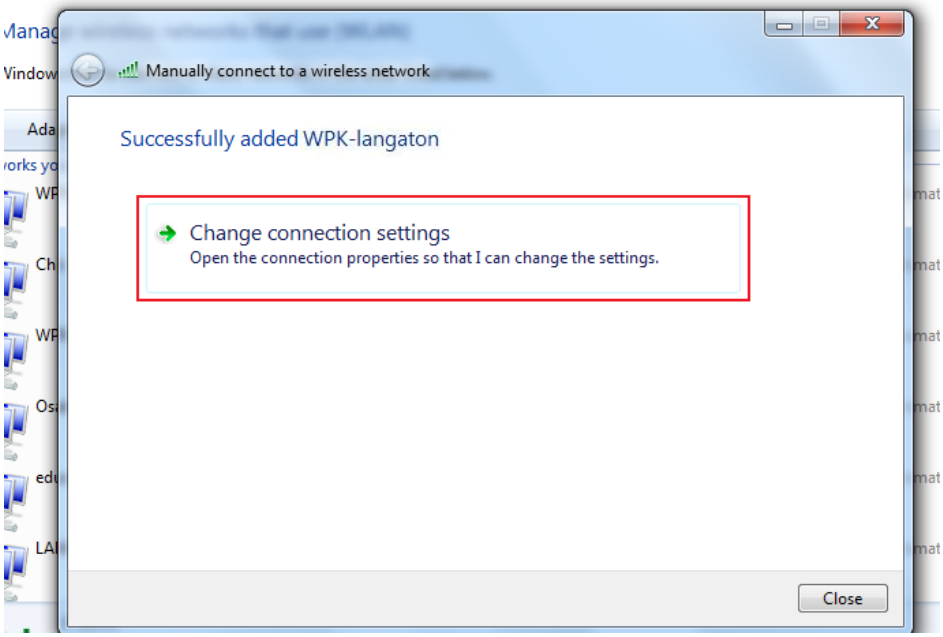
Langattoman verkon nimeksi syötetään WPK-langaton, Security typeksi valitaan WPA2 Enterprise ja Encryption typeksi AES. Tärkeää on myös muistaa laittaa rastit kohtiin

”Start this connection automatically” ja ”Connect even if the network is not broadcasting” (kuva 78).



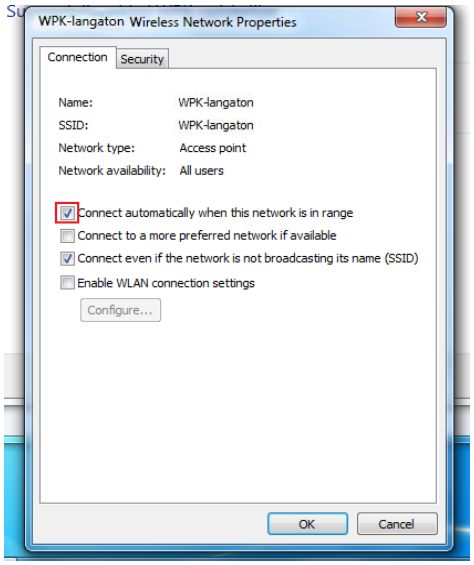
Kuva 78: Yhteyden muodostaminen, Windows 7, 5

Kun WPK-langaton on lisätty, käydään muuttamassa sen asetuksia painamalla Change connection settings (kuva 79).



Kuva 79: Yhteyden muodostaminen, Windows 7, 6

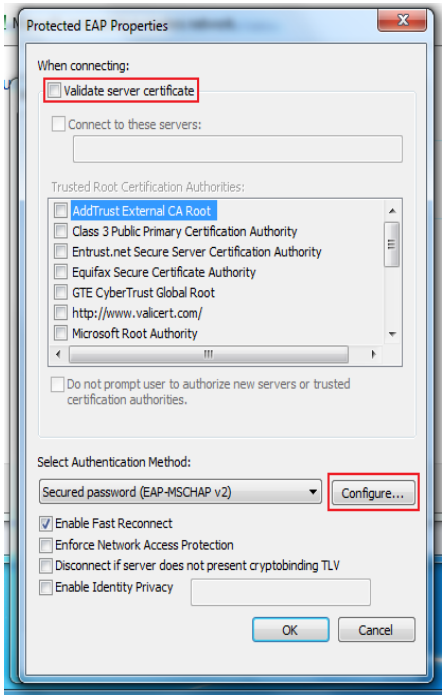
Connection-välilehdeltä ruksitetaan kohdat ”Connect automatically when this network is in range” (mikäli haluaa koneen yhdistyvän verkkoon automaattisesti kun kone on verkon ulottuvilla) ja ”Connect even if the network is not broadcasting” (kuva 80).



Kuva 80: Yhteyden muodostaminen, Windows 7, 8

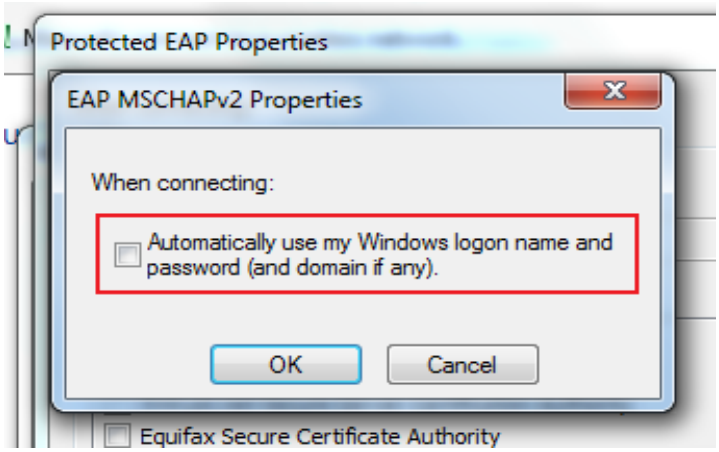
Security-välilehdeltä suojaustyypiksi valitaan WPA2-Enterprise ja salauslajiksi AES. Verkon todennusmenetelmäksi valitaan Microsoft: SuojattuEAP (PEAP). Tärkeää on

myös muistaa laittaa rasti kohtaan ”Tallenna käyttäjätiedot välimuistiin verkon myöhempää käyttöä varten”. Klikataan Asetukset... Poistetaan rasti kohdasta Validate server certificate ja painetaan Configure… (kuva 81).



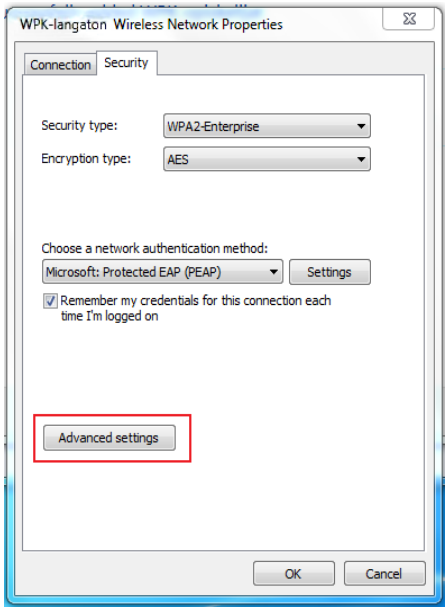
Kuva 81: Yhteyden muodostaminen, Windows 7, 9

Poistetaan rasti kohdasta ”Automatically use my Windows logon name and password”. Painetaan OK (kuva 82).



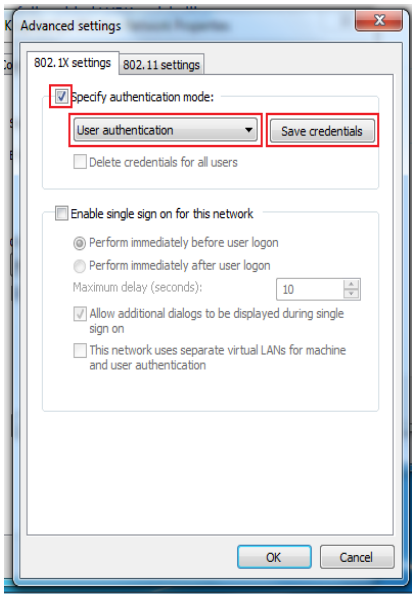
Kuva 82: Yhteyden muodostaminen, Windows 7, 10

Security-välilehdeltä painetaan Advanced settings (kuva 83).

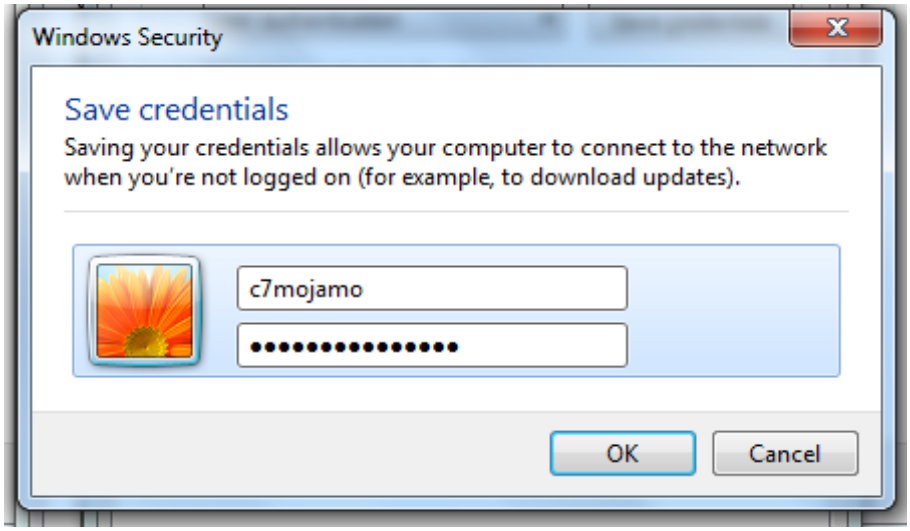


Kuva 83: Yhteyden muodostaminen Windows 7, 11

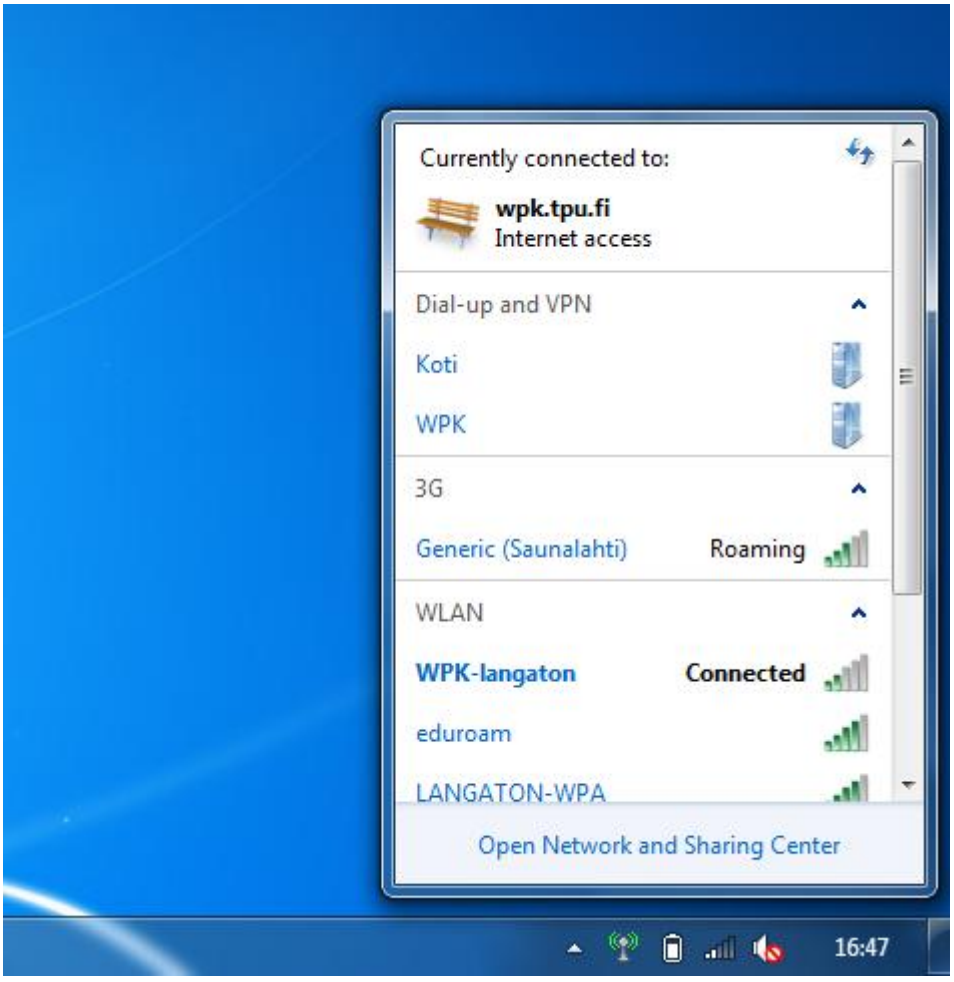
802.1X välilehdeltä laitetaan rasti kohtaan Specify authentication mode, pudotusvalikosta valitaan User authentication (kuva 84) ja omat käyttäjätunnukset syötetään painamalla save credentials (kuva 85). Jos tietokonetta ei oltu yhdistetty aluksi toiseen verkkoon, niin näiden askelten jälkeen kirjautuminen WPK-langaton –verkkoon on automaattista ja Windows muistaa käyttäjän kirjautumistunnukset sekä verkon asetukset (kuva 86). Jos tietokoneesi käytti aluksi toista verkkoa, käy painamassa langattomattomien verkkojen listasta WPK-langattoman connect painiketta.



Kuva 84: Yhteyden muodostaminen, Windows 7, 12



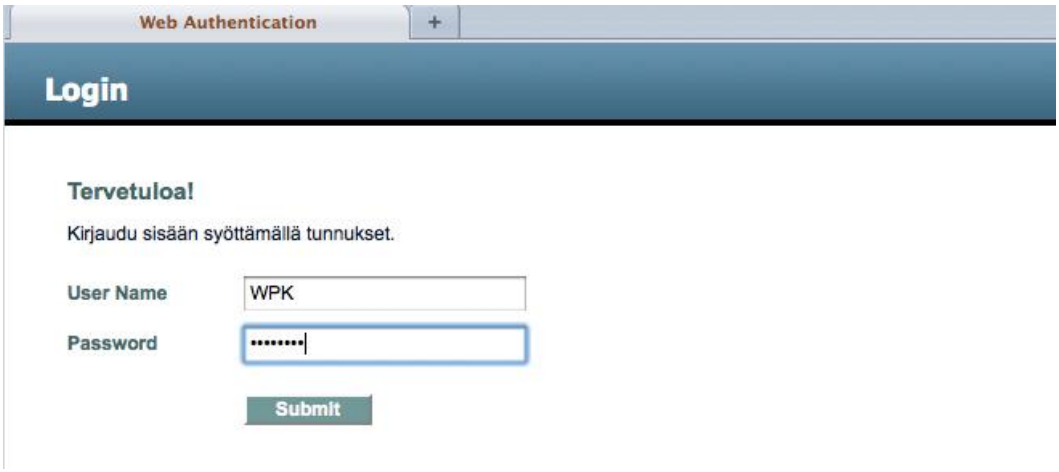
Kuva 85: Yhteyden muodostaminen, Windows 7, 13



Kuva 86: Yhteys muodostunut, Windows 7, 14

Vierailijaverkko

Vierailijaverkkoon pääsee kirjautumaan kaikista käyttäjärjestelmistä samalla tavalla, eli vain valitsemalla verkon WPK-vieraat langattoman verkon listalta. Verkkoon pääsee yhdistymään ilman minkään tunnuksen syöttämistä, mutta kun avaa selaimen, kontrolleri pakottaa asiakaskoneen kirjautumissivulle. Tähän syötetään käyttäjätunnus ja salasana, jotka verkon testaamishetkellä olivat WPK ja salasana (kuva 86). Käyttäjätunnusta ja salasanaa voi vaihtaa kontrollerilta luomalla uusia Local Net Userseja.



Kuva 86: Web-autentikoinnin etusivu

Kirjautumisen jälkeen kontrolleri ohjaa käyttäjän määritellylle aloitussivulle, joka meillä on Tampereen Ammattikorkeakoulun verkkosivu. Käyttäjä voi nyt normaalisti käyttää Internet-yhteyttään (kuva 87).

Kuva 87: Web-autentikoinnin jälkeen käyttäjä ohjataan pakotetusti TAMKin etusivulle