VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Mikko Luukkonen

Langaton lähiverkko pienyritykselle

Liiketalous ja matkailu

2011

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Mikko Luukkonen
Opinnäytetyön nimi	Langaton lähiverkko pienyritykselle
Vuosi	2011
Kieli	suomi
Sivumäärä	48
Ohjaaja	Antti Mäkitalo

Opinnäytetyön tarkoituksena on luoda mahdollisimman selkeä ja informatiivinen opas langattoman verkon pystyttämiseen. Työn tarkoitus on antaa käytännön ohjeiden lisäksi myös mahdollisimman paljon hyödyllistä tietoa langattomista verkoista ja niiden käytöstä.

Työn tekemiseen on käytetty apuna internetistä saatavaa tietoa, alan kirjallisuutta sekä koulutusohjelmassa opittua asiaa. Käytännön kokemusta aiheesta on saatu koulussa ja työharjoittelussa.

Työn tuloksena kokonaiskuva langattomista verkoista on selkeytynyt ja varsinkin tietoturvaan liittyvät harhaluulot ovat korjautuneet. Myös oppaan tekemisestä on kertynyt kokemusta työtä tehdessä. Tarkoituksena luoda informatiivinen ja selkeä opas, jonka avulla it-alan harrastaja voi pystyttää langattoman lähiverkon pieneen tai keskisuureen yritykseen.

Avainsanat WLAN, Langaton verkko, Opas

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Mikko Luukkonen
Title	Wireless local area network for Small Enterprises
Year	2011
Language	Finnish
Pages	48
Name of Supervisor	Antti Mäkitalo

The aim of the bachelor's thesis was to create an informative guide for the setting up of the wireless network as clearly as possible. In addition to practical instructions the goal of the work was to give as much useful information as possible about wireless networks and their use.

Information available on the internet, the literature of the field and the matters that have been learned in the education programme have been used as the sources to this work. Experience on the practical subject has been obtained at school and in practical training.

The general understanding of wireless networks become more detailed as a result of the work and particularly the wrong ideas which are related to the information security were clarified. Experience has accumulated also from the doing of the guide. The result of the work is an informative and clear guide with which help an enthusiast of the field can set up a wireless local area network for a small or medium-sized enterprise.

Keywords WLAN, wireless network, guide

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

KÄSITTEET

802.11	IEEE:n julkaisema standardi langattomille lähiverkoille.
ADSL	Asymmetric Digital Subscriber Line on verkkokytkintekniikka, jolla on mahdollista siirtää dataa tavallista puhelinlinjaa käyttäen.
IAPP	Inter Access-Point Protocol on protokolla, joka parantaa laitteen liikuteltavuutta tukiasemalta toisella.
IEEE	Institute of Electrical and Electronics Engineers on kansainvälinen standardisointijärjestö, joka edistää sähköteknisiä tieteitä julkaisemalla standardeja.
OFDM	Orthogonal Frequency Division Multiplexing on taajuuskanavointitekniikka, siirrettävän datan jaetaan eri taajuuksien alikanaviin joita käytetään rinnakkain.
OSI-malli	Open Systems Interconnection Reference Model on tiedonsiirtoprotokollien yhdistelmä seitsemässä kerroksessa.
PEAP	Protected Extensible Authentication Protocol on tunnistus-protokolla, joka salaa verkossa lähetettäviä kriittisiä tietoja, kuten salasanoja ja muita tunnistetietoja.
SSID	Service Set Identifier on langattoman lähiverkon verkkotunnus eli langattoman verkon “nimi”.
USB	Universal Serial Bus on sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen.

WAN	Wide Area Network eli laajan alueen kattava tiedonsiirtoverkko, joka peittää isoja maantieteellisiä alueita. Suurin tämänkaltainen verkko on internet.
Wi-Fi	On Wi-fi alliencen julkaisema multimediastandardi langattomille lähiverkoille. Käytetään tietynlaisena laatustandardina tukiasemille.
WLAN	Lyhenne sanoista Wireless Local Area Network, tarkoittaa langatonta paikallista lähiverkkoa.

1 JOHDANTO

Langattomat verkot ovat nykyään arkipäivää lähes kaikkialla ja niiden halpuus ja helppous on johtanut siihen, että niitä on käytössä jopa tavallisissa kotitalouksissa. Myös pienyritykset käyttävät langattomia verkkoja, mutta ammattilaisen apu on kallista eikä asennusta kannata tehdä pelkällä ”mutu” -tuntumalla. Verkon pystytys kuitenkin onnistuu atk-alan harrastajalta, varsinkin jos apuna on selkeä opas.

Tämä opinnäytetyö on opas langattoman verkon pystytystä varten. Työssä on oppaan lisäksi myös muuta tarpeellista tietoa langattomista verkoista. Tämän luettuaan lukijalla on käsitys siitä, miten langaton verkko pystytetään ja mikä ratkaisu on hänen käyttöönsä paras. Työ sopii myös henkilölle, joka haluaa yleistietoa langattomista verkoista ja niiden toiminnasta.

2 TUTKIMUSONGELMAT

Mitkä ovat langattoman verkon hyödyt verrattuna langalliseen verkkoon? Työn tarkoituksena on selvittää, miksi langaton verkko on hyvä vaihtoehto kaapelin korvikkeeksi.

Kannattaako langatonta verkkoa lähteä pysyttämään omin voimin? Työssä käydään läpi, mitä tarvitsee tietää ja hankkia pystyttääkseen langattoman verkon.

Onko langaton verkko yhtä turvallinen käyttää kuin langallinen? Työssä käsitellään langattoman verkon tietoturvaa ja sen luotettavuutta.

3 WLAN

WLAN (lyhenne sanoista Wireless Local Area Network) on langaton lähiverkkotekniikka, jossa data liikkuu sähkömagneettisina aaltoina työasemien ja tukiasemien välillä. Tästä johtuen kaapeleita ei tarvita työasemien ja tukiasemien välille. WLAN eroaa normaalista LAN-verkosta ainoastaan langattomuudessa ja tietysti nopeuksissa, mutta muuten kaikki verkon yli tapahtuva toiminta voidaan hoitaa samalla tavalla kuin LAN-verkossa.

WLAN-verkon pystyttäminen ei vaadi isoja panostuksia tai sijoituksia, vaan se on jopa halvempaa kuin langallisen verkon rakentaminen. Langattomaan verkkoon pääsemiseksi tarvitaan ainoastaan langaton reititin ja työasemiin vastaanottimet.

WLAN:in suurimpia etuja on ehdottomasti vapaa liikkuvuus tukiaseman kantavuusalueella ilman katkoksia. Myöskään ympäristöä ei tarvitse muokata ja kuuluvuus riittää hankaliinkin paikkoihin. Yrityksen muuttaessa toimitiloista toiseen on purkaminen ja pystyttäminen nopeaa ja vaivatonta.

WLAN:ia käytettäessä tietoturvan tulee olla kunnossa ja se on oikeastaan ainut asia, joka vaatii enemmän panostusta kuin perinteisessä LAN-verkossa. Onneksi suojaukset ovat nykyään hyviä ja helposti kytkettäviä, eli tietoturvakaan ei ole enää syy syrjiä langattomia verkkoja. (Gunvald Hedemalm)

3.1 Historia

Ensimmäisen WLAN-tuotteen (Altairin) julkaisi Motorola 1980-luvun puolivälissä. WLAN-verkkojen alkuaikoina ongelma oli yhteensopimattomuus: 80- ja 90-luvun tuotteet olivat valmistajakohtaisia, joten käyttäjä joutui ostaessaan tuotteen sitoutumaan yhteen valmistajaan ja epävarmoihin lupauksiin tulevasta. IEEE:n (Institute of Electrical and Electronics Engineers) LAN/MAN-standardointiryhmä (LMSG, LAN/MAN Standardization Group) aloitti

langattoman verkon standardikehityksen vuonna 1990, ja työn tuloksena julkaistiin ensimmäinen 802.11-standardi vuonna 1997. Tekniikka oli samankaltaista kuin Ethernetissä (802.3) ja tämän vuoksi langatonta verkkoa kutsuttiin alkuaikoina langattomaksi Ethernetiksi, nykyään yleisempi nimitys on Wi-Fi. (Matti Puska); (Kaj Granlund)

IEEE (Institute of Electrical and Electronics Engineers) on kansainvälinen tekniikan alan organisaatio, joka edistää muun muassa lähiverkkojen yhteensopivuutta julkaisemalla ja valmistamalla standardeja. Organisaatioon kuuluu yli 370 000 jäsentä yli 160 maassa. IEEE:llä ei ole virallista oikeutta julkaista standardeja, vaan julkaisut hoitaa erillinen standardointiorganisaatio, kuten ISO (International Standardization Organisation), jotka ottavat käyttöön IEEE:n menetelmät ja julkaisevat ne omilla standardinumeroillaan. Yksi aktiivisimmista standardeja julkaisevasta osastoista on LMSG (LAN/MAN Standardization Group), joka on toiminut lähes 30 vuotta lähiverkkojen 802-standardien parissa. (Matti Puska)

3.2 Wi-Fi

WLAN tunnetaan nykyisin Wi-Fi-nimityksellä, mutta todellisuudessa se on Wi-Fi Alliancen ”leima”, joka takaa, että laite täyttää tietyt laatuvaatimukset. Wi-Fi Alliance on ollut aktiivisesti mukana standardointi- ja yhteensopivuustyössä, ja vuonna 2004 se julkaisi oman Wi-Fi Multimedia -standardin (WMM) ja yhteensopivuustestausmenettelyn. WMM-standardi on tarkoitettu ratkaisemaan osittain ääni- ja multimediasovellusten tarvitseman liikenteen priorisoinnin. Wi-Fi Alliance pyrkii määrittelyllään edistämään laitteiden yhteensopivuutta. (Matti Puska)

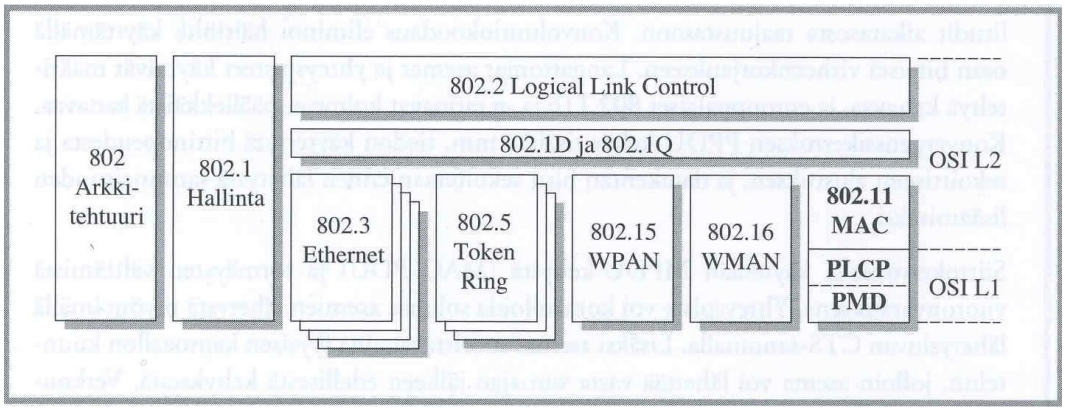
4 IEEE 802.11X STANDARDIT

4.1 802.11

802.11 oli IEEE:n ensimmäinen langattomille verkoille tarkoitettu yleisstandardi, jonka valmistus aloitettiin 1990 ja se valmistui 1997. Nopeus oli 1 tai 2 megabittiä sekunnissa ja se toimi vapaalla 2,4 gigahertsin taajuudella.

802-standardit (kuva 2) kattavat vain OSI-mallin (Open System Interconnection) (kuva 1) kaksi alinta kerrosta: fyysinen kerroksen ja siirtokerroksen. Siirtokerroksen toiminnot jaetaan siirtotien ohjaukseen (LLC, Logical Link Control) ja vuoronvaraukseen (MAC, Medium Access Control). Myös 802.11 WLAN-standardit noudattavat tätä yleistä konseptia, mutta toisin kuin perinteisissä lähiverkoissa langattomissa 802.11-verkoissa käytetään LLC-protokollaa ja -kehystä. (Matti Puska)

Kuva 1. OSI-malli

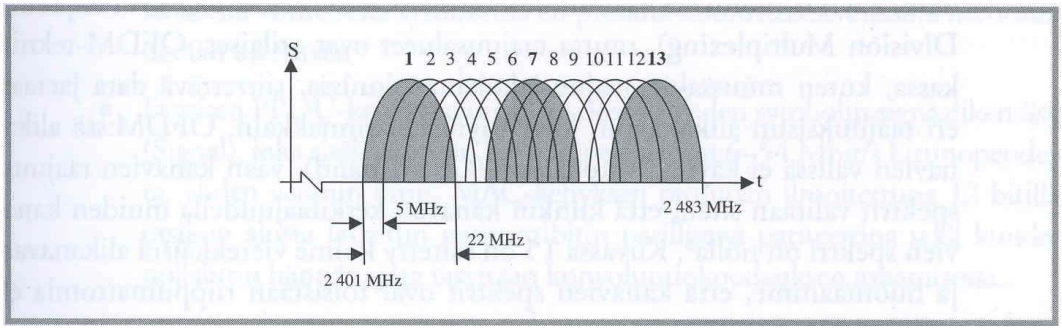


Kuva2. 802.x standardit. (Matti Puska)

4.2 802.11b

Myös 802.11b käyttää 2,4 gigahertsin taajuutta ja tarjoaa 1, 2 ja 5,5 sekä 11Mbit/s bittinopeudet suorasekvenssihajaspektritekniikkaa käyttäen. 802.11b:n mukaiset laitteet ovat yleisesti käytettyjä, vaikka kaikki uudemmat laitteet käyttävät nopeampaa 54 Mbit/s:n tekniikkaa.

Eurooppalainen 11 Mbit/s 802.11b käyttää 2,400–2,485 GHz:n ETSI:n (European Telecommunications Standards Institute) vapaasti käytettäväksi määrittelemää taajuusaluetta, joka on jaettu 13:een kanavaan 5 MHz:n välein (kuva 3). Kun kanavat ovat 22 MHz leveitä, menevät vierekkäiset kanavat päällekkäin häiriten toisiaan. Vierekkäisissä soluissa tulisi käyttää ei-päällekkäisiä kanavia (non-overlapping channels), joita Euroopassa ovat 1, 7 ja 13. (Matti Puska)



Kuva 3. 802.11b-radiokanavat Euroopassa. (Matti Puska)

4.3 802.11a

802.11a toimii 5 GHz:n U-NII-taajuusalueella (Unilicensed National Information Infrastructure), taajuusrajat eri maissa erilaiset, toimii nopeudella 6–54 Mbit/s. Kun kanavat ovat 20 MHz:n välein, menevät ne osittain päällekkäin, mutta 802.11a tarjoaa 12 toisiinsa vaikuttamatonta kanavaa OFDM-tekniikan avulla.

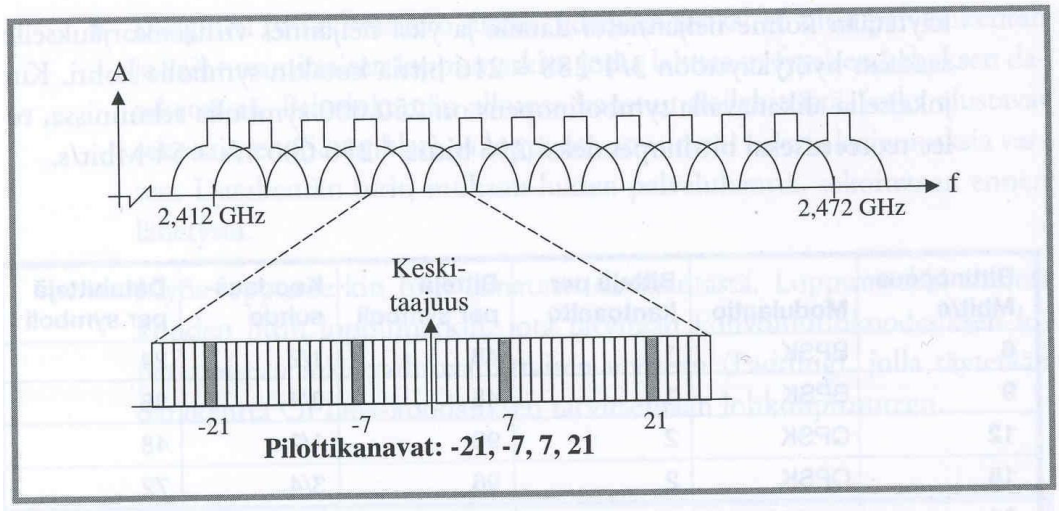
Koska 802.11a käyttää korkeampia taajuuksia, radioaaltojen vaimennus on suurempaa, mistä aiheutuu pienempi kantomatka ja suuremman lähetystehon ja tehonkulutuksen tarve. Saman alueen kattamiseen tarvitaan 1.5-kertainen määrä asemia 802.11a-tekniikalla kuin 802.11g:ssa. Taajuusaluetta lukuun ottamatta 802.11a:n ominaisuudet ja toiminta ovat samanlaiset kuin eurooppalaisen 802.11g:n. (Matti Puska)

4.4 802.11g

802.11g toimii 54 Mbps:n nopeudella 802.11-a-version tapaan, mutta 2,4 GHz:n taajuudella (kuva 4), lisäksi 802.11g pystyy toiminaan 11 Mbps:n nopeudella, joten se on yhteensopiva vanhemman 802.11b-standardin kanssa. 802.11g-standardi valmistui vuonna 2003 ja on risteytys 802.11a- ja 802.11b-standardeja.

802.11g- ja 802.11a-standardi käyttää monikantoaaltomodulointia (OFDM, Orthogonal Frequency Division Multiplexing), mutta taajuusalueet ovat erilaiset.

OFDM-tekniikassa, kuten muussakin taajuusjakokanavoinnissa, siirrettävä data jaetaan eri taajuuksien alikanaviin, joita käytetään rinnakkain. OFDM:ssä alikanavien välissä ei käytetä varokaistaa (Guard Band), vaan kanavien taajuus-spektri valitaan siten, että kunkin kanavan keskitaajuudella muiden kanavien spektri on nolla. (Matti Puska)



Kuva 4. 802.11g-kanavat ja -alikanavat. (Matti Puska)

4.5 802.11e

802.11e (2005) sisältää palvelulaatuun ja verkon suorituskyvyn parantamiseen liittyviä päivityksiä. Tukiasemat lähettävät viestejä vuorotellen ja, jos päällekkäisyyttä tapahtuu, odottavat tukiasemat hetken uudelleen lähetystä. 802.11e-standardissa tukiasemia voidaan priorisoida, mikä vähentää odotusaikaa ja nopeuttaa verkkoliikennettä. 802.11e-standardi on suunniteltu lähinnä multimedialiikennettä (kuten VoIP) varten, jossa viiveen tulisi olla mahdollisimman pieni. (Matti Puska)

4.6 802.11f

802.11f (2006) määrittelee liityntäpisteiden välistä liikennöintiä. 802.11f-standardi käyttää IAPP-protokollaa (Inter Access-Point Protocol), joka parantaa laitteen liikuteltavuutta tukiasemalta toiselle. 802.11f-protokolla siis parantaa laitteen liikuteltavuutta verkossa, jossa on monen eri valmistajan tukiasemia ja langatonta laitetta liikutellaan alueella. 802.11f-standardia ollaan korvaamassa k- ja r-laajennuksilla. (Matti Puska)

4.7 802.11d

802.11d (2001) lisäosa sisältää menetelmän, joka osaa laitteen sijainnista riippuen itse valita oikean taajuuskaistan. Tarkoitus on helpottaa paljon matkustavan henkilön langattoman verkon käyttöä, kun laite itse osaa valita kussakin maanosassa luvalliset taajuudet.

4.8 802.11h

802.11h (2004) sisältää lisämääritykset 5 GH:n taajuusalueen käytölle Euroopassa (kuva 5). 5 GH:n taajuus oli aikaisemmin varattu muulle liikenteelle, esimerkiksi satelliiteille. Lisäksi 802.11h-päivitys tukee taajuusalueen vaihtoa, jos käytetty kanava on häiriöllinen sekä virransäästöominaisuutta. (Matti Puska)

Alue	Kanavat	Taajuusalue
Eurooppa poikkeuksin	1 - 13	2,400 - 2.485 GHz
Ranska	10 - 13	2,445 - 2,485 GHz
Espanja	10 - 11	2,445 - 2,475 GHz
USA ja Kanada	1 - 11	2,400 - 2,475 GHz
Japani	14	2,473 - 2,495 GHz

Kuva 5. Sallitut DSSS-kanavat. (Matti Puska)

4.9 802.11i

802.11i (2004) on tieturvapäivitys ”MAC Enhancements for Enhanced Security”, jonka tarkoituksena on nostaa langattomien verkkojen tietoturvaa. Päivitys sisältää istuntokohtaisen TKIP-avainnuksen, WEP-parannukset, esitunnistuksen (Pre-authentication) ja kaksisuuntaisen PEAP-tunnistuksen. 802.11i soveltuu sekä staattisille että dynaamisille salausavaimille, ja yleensä sitä käytetään 802.1x-järjestelmissä. (Matti Puska)

4.10 802.11s

802.11s-lisäosa sisältää tuen WMesh (Wireless mesh)-verkolle. Tämä mahdollistaa tukiasemien vaihdon ilman yhteyden katkeamista. WMesh muistuttaa vähän GSM-verkkoa, jossa viesti kulkee useamman tukiaseman kautta, vaikka keskustelijoita onkin vain kaksi.

4.11 802.11n

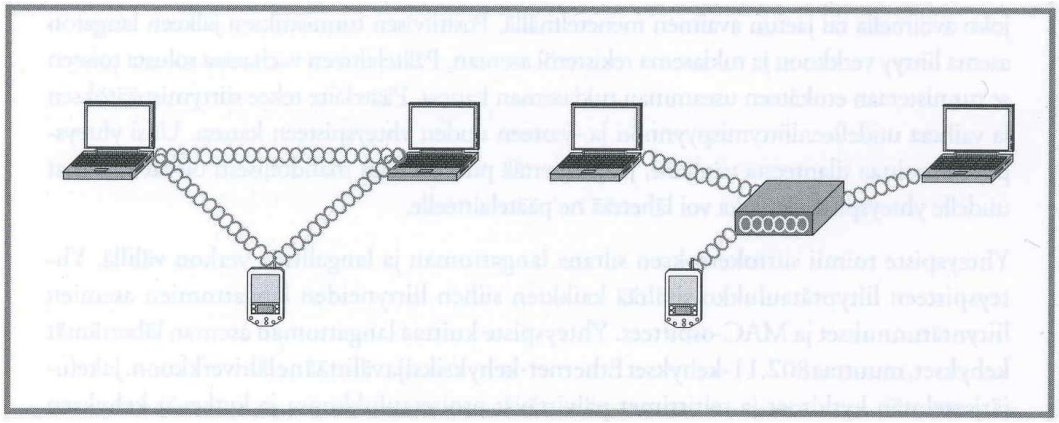
802.11n (2009) laajennus tuo lähinnä lisänopeutta vanhoihin 802.11b- ja 802.11g-standardeihin. 802.11n tukee MIMO (Multiple-Input, Multiple-Output)-tekniikkaa, mikä tarkoittaa sitä, että laite tukee useamman antennin ja taajuuden yhteiskäyttöä, joka nostaa teoreettisen nopeuden jopa 600 megabittiä sekunnissa. 802.11n on yhteensopiva vanhempien 802.11b- ja 802.11g-laitteiden kanssa, mutta siirtonopeus luonnollisesti määräytyy hitaamman laitteen mukaan.

4.12 Topologiat

WLAN voidaan rakentaa kolmella eri topologialla tavalla.

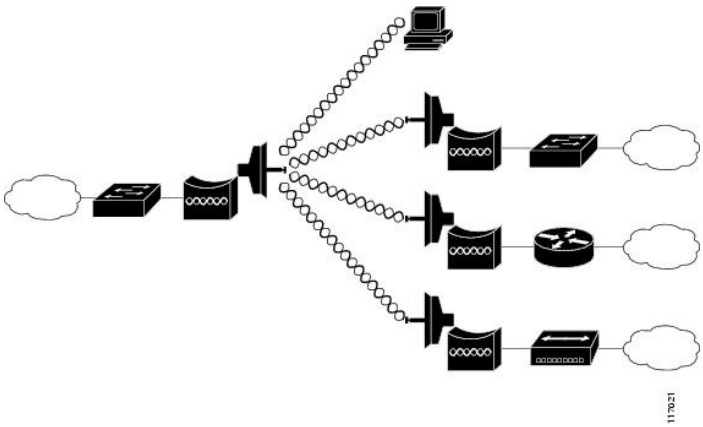
- P2P (peer-to-peer) eli vertaisverkko (ad hoc) topologia. Tässä tilassa koneet keskustelevat keskenään ilman minkäänlaisia tukiasemia (kuva 6).

- AP-pohjainen (Access points) infrastruktuuri verkko. Eli tukiasemallinen langaton verkko johon tässä työssä keskitytään (kuva 6).
- Point-to-Multipoint bridge- topologia yhdistää useita paikkoja yhdeksi ja antaa niiden jakaa saman verkon resursseja (kuva 7). (David Clark)



Kuva 6. Ad-hoc- ja infrastruktuuritopologiat.

Ad-hoc-verkko (vasemmalla) ja infrastruktuuriverkko (oikealla). (Matti Puska)



Kuva 7. Point-to-Multipoint bridge-topologia. (Cisco)

5 TIETOTURVASTANDARDEJA

WLAN-verkon tietoturva oli varsinkin alkuaikoina melko heppoista ja tästä syystä jotkut yritykset pelkäävät vieläkin langatonta vaihtoehtoa. Pelko langattomien verkkojen turvattomuudesta on saanut jotkut yritykset kieltämään sen täysin. Myös internetistä löytyy ohjeita ja jopa ohjelmia, joilla saa joitakin salauksia

murrettua. Suurin syy turvattomuuteen on kuitenkin itse käyttäjä. Iso osa verkoista jätetään turvattomille tehdasasetuksille, jolloin niihin on helppo päästä käsiksi ilman sen suurempaa asiantuntemusta tai ohjelmia.

Tosiasia on kuitenkin se, että langattoman verkon suojaamiseen on olemassa useita yksinkertaisia ja tehokkaita tapoja. Menetelmät koostuvat verkkoon pääsyn ja autentikoinnin ratkaisuista sekä moninkertaisesta tiedon salaamisesta. Kun nämä asiat ovat kunnossa, ei verkkoon pääse sinne kuulumattomat ”vieraat”.

5.1 WEP

Wired Equivalent Privacy (WEP) on 802.11-standardeissa määritelty siirtokerroksen salausmenetelmä, jonka käyttö on vapaaehtoista. WEP-salaus on symmetrinen, ja kaikille langattomille asemille pitää määritellä sama avain kuin yhteyspisteelle. Salausavaimia on kaksi: 40-bittistä, joihin molempiin lisätään 24 bitin alustusvektori (Initialization Vector). WEP-salauksen tietoturvasalausmenetelmä on huono, mutta kun ottaa huomioon sen rajoitteet, se tarjoaa kohtuullisen ja yksinkertaisen vaihtoehdon päätelaitteen tunnistusmenetelmänä. (Matti Puska)

5.2 802.1x

IEEE:n 802.1x perustuu porttikohtaiseen todentamiseen, joka estää luvattoman pääsyn langattomaan verkkoon sen liityntäpisteiden kautta. Liityntäpisteitä ovat esimerkiksi kytkimen tai tukiaseman portit. 802.1x käyttää dynaamista 128-bittistä salausavainta, joka tarkoittaa, että avaimen elinikä voidaan määrittää ja se on yksilökohtainen jokaiselle käyttäjälle ja sessiolle.

IEEE:n 802.1x tarjoaa laajennetun konseptin käyttäjän tunnistukseen. Se perustuu IETF:n EAP:hen (Extensible Authentication Protocol), joka tarjoaa optimoidun kuljetusalustan tunnistustoteutuksille, mutta ei ole mikään tunnistusmenetelmä.

802.1x tarjoaa yksinkertaisen kuljetustavan EAP-sanomille kaikissa 802.x-lähiverkoissa. (Matti Puska)

5.3 WPA

Kun WEP-salauksen tietoturva, aukot huomattiin, oli kehitettävä uudenlainen turvallisempi salausmenetelmä. Wi-Fi Alliance rupesi kehittämään uutta salausmenetelmää ja tuloksena oli WPA (Wi-Fi Protected Access), joka valmistui 2002. WPA on yhteensopiva vanhempien ja uudempien laitteiden kanssa.

WPA-salaus perustuu molemminpuoliseen tunnistukseen. WPA käyttää EAP-protokollaa (Extensible Authentication Protocol) tiedonsiirron salaamiseen ja tiedon eheyden turvaamiseen. WPA on tarkoitettu käytettäväksi 802.1X-autentikoinnin kanssa, joka jakaa salausavaimet kaikille käyttäjille. Sitä voi käyttää myös vähemmän turvallisessa "Pre-Shared Key (PSK)"-tilassa. PSK on tarkoitettu koti- ja pientoimistokäyttöön, jossa kaikki käyttävät samaa salasanaa. WPA-PSK tunnetaan myös nimellä WPA-Personal. WPA-PSK:avulla kone pystyy ottamaan yhteyttä yhteyspisteeseen (Access Point) TKIP- tai AES-salausta käyttäen. (brother.com)

5.4 WPA2

WPA2 on uusin tietoturvastandardi, joka tarjoaa samat ominaisuudet kuin WPA, mutta tuo mukanaan täysin uuden AES-salausalgoritmin. AES poikkeaa paljon aikaisemmista salausalgoritmeista ja vaatii myös enemmän tehoa sitä pyörittävältä laitteelta, valittavana on 128-, 192-, tai 256-bittinen avain. (brother.com)

5.5 RADIUS

RADIUS (Remote Authentication Dial In User Service)-palvelin salaa lähettämänsä haasteen paikallisesti käyttäjän salasanalla ja vertaa tulosta saamaansa sanomaan. Jos salatut haasteet täsmäävät, oli salakirjoitusavain oikein ja tunnistettu käyttäjä voidaan liittää verkkoon. Tunnistuspalvelin lähettää tällöin positiivisen RADIUS-Access-Accept-sanoman, jonka tunnistaja muuttaa EAP-Success-sanomaksi. Samassa sanomassa RADIUS-palvelin lähettää myös istunnon WEP-avaimen, jonka yhteyspiste tallentaa itselleen ja lähettää edelleen päätelaitteelle. Avain on joka kerralla erilainen. WEP-avain voidaan vaihtaa määräajoin, jolloin samalla avaimella salattua liikennettä ei kerry niin paljon analysoitavaksi. (Matti Puska)

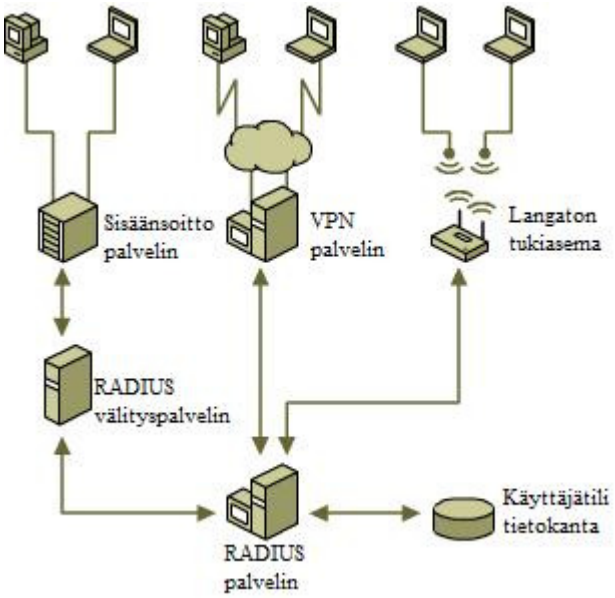
RADIUS-palveluun kuuluu asiakaskoneet, joilla on pääsy verkkoon esim. VPN-palvelimen tai langattoman tukiaseman kautta.

Pääsypalvelimet ovat laitteita tai palvelimia, jotka mahdollistavat pääsyn RADIUS-palvelimelle. Pääsypalvelin, joka käyttää RADIUS infrastruktuuria, on myös RADIUS-asiakas.

RADIUS-välityspalvelin on laite, joka välittää RADIUS-pyyntöjä ja viestejä RADIUS-asiakkaan ja RADIUS-palvelimen välillä.

RADIUS-palvelin vastaanottaa ja käsittelee yhteyspyyntöjä ja tiliviestejä joita RADIUS-asiakkaat tai RADIUS-välityspalvelin lähettävät. RADIUS-palvelin päättää, sallitaanko yhteys palvelimelle vai hylätäänkö yhteyspyyntö.

Käyttäjätilitietokanta on lista käyttäjätileistä ja niiden ominaisuuksista, joita RADIUS-palvelin voi tarkastella varmistaakseen tunnistuksen ja käyttäjätilin ominaisuudet (katso kuva 8). (Microsoft)



Kuva 8. RADIUS-palvelun toiminta. (microsoft.com)

6 VERKON RAKENTAMINEN

6.1 Alkusanat

Pienyrityksen langattoman verkon pystytykseen ei välttämättä tarvita vaikeita erikoistekniikoita, hienoja mittareita ja verkkoinsinöörejä. Jos vaatimustaso on maltillinen eivätkä olosuhteet ole erityisen hankalat, myös isompi verkko voidaan saada toimimaan omin voimin.

Muutaman tukiaseman langattoman verkon saa rakennettua jo erittäin halvalla. hyvän tukiaseman saa jo alle 30:en euron kappalehintaan, loppusummaan tietysti vaikuttaa koneiden ja tukiasemine määrä. Langattoman verkon etuna on koneiden liikuteltavuus ja vapaa sijoittelu. Kaapeleitakaan ei joudu vetämään eikä reikiä poreilemaan seiniin.

Nykyään langattoman verkon rakentaminen saattaa olla jopa helvemaa kuin langallisen verkon toteuttaminen. Nopeuskaan ei ole enää syy syrjiä langattomia verkkoja, sillä tiedonsiirtonopeudet ovat jopa 300 Mbps.

Myös verkon pystyttäminen on vaivatonta ja alan harrastaja pystyttää langattoman verkon pienyritykselle siinä missä minkä tahansa muunkin toimiston atk-laitteen. On kuitenkin hyvä olla tukena opas, jos kaikista asioista ei ole ihan varma, ja on kätevää, kun kaikki tarvittava tieto on yhdessä oppaassa.

6.2 Aloitus

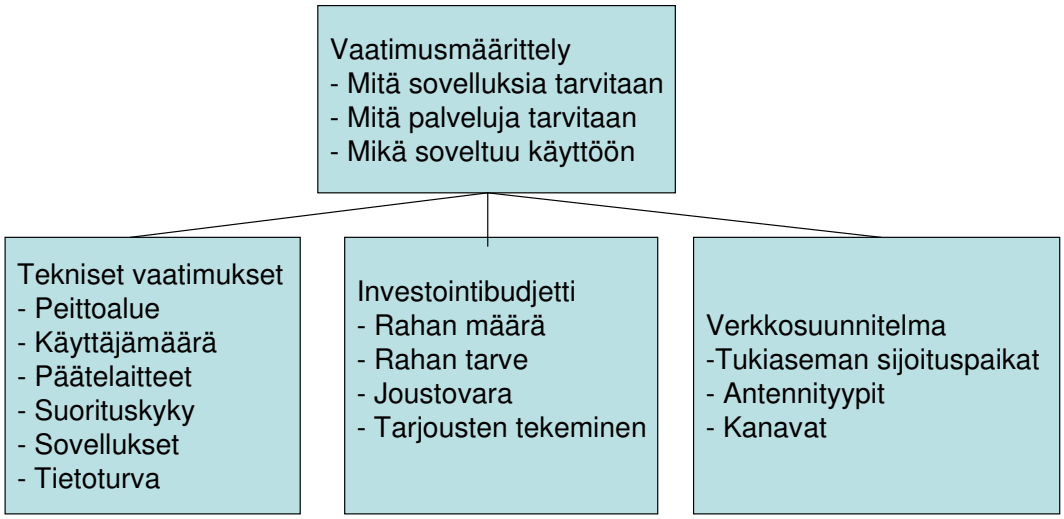
Langattoman verkon asentaminen tulee aloittaa suunnittelulla. Suunnitteluvaihe jätetään turhan usein väliin. Suunnitteluun kuuluu vaatimusmäärittely, asemien ja laitteiden määrän kartoitus sekä sijoittelu. Yleinen virhe asemien sijoittelussa on sijoittaa tukiasemat tiiviiseen välikattoon. Sitten ihmetellään, kun nopeus ei olekaan sitä, mitä pitäisi. Hyvällä suunnittelulla säästetään aikaa ja rahaa.

WLAN-projektin vaiheet

Tietotekniikkaprojektit, kuten monet muutkin, tulee aloittaa vaatimusmäärittelyllä (kuva 9). Vaatimukset tulevat yrityksen liiketoiminnasta ja käyttäjien tarpeista, näihin tarpeisiin etsitään sovellukset ja palvelut. Näiden palveluiden ja sovellusten toiminta määrittää pitkälti verkolle tekniset vaatimukset, verkon tulee kyetä tukemaan kaikkia tarvittuja sovelluksia ja ohjelmia.

Teknisiin vaatimuksiin sisältyy ohjelmien ja sovellusten lisäksi myös tiedot peittoalueista, käyttäjämääristä, päätelaitteista, verkon suorituskyvystä ja tietoturvasta. Kustannusarvion ja aikataulun laatiminen ovat osa vaatimuksia. Teknisten vaatimusten, investointibudjetin ja tuotetarjonnan perusteella saadaan selkeä kuva siitä, miltä tuleva verkko tulee näyttämään.

Verkkosuunnitelmassa kartoitetaan tukiasemien alustavat sijoituspaikat, antennityypit ja kanavat. Radiosignaalin etenemistä ja häiriötekijöitä on vaikea tietää, ennen kuin verkko on pystyssä. Alueelle kannattaa tehdä katselmus ennen lopullisen verkon pystyttämistä, näin vältytään ikäviltä yllätyksiltä. Katselmuksen voi tehdä itse esimerkiksi yhdellä tukiasemalla ja kannettavalla tietokoneella. Katselmuksessa varmistetaan, että signaali on hyvä halutuissa paikoissa ja tukiasemat on madollista sijoittaa suunniteltuihin paikkoihin. (Matti Puska)



Kuva 9. WLAN-projektin vaiheet.

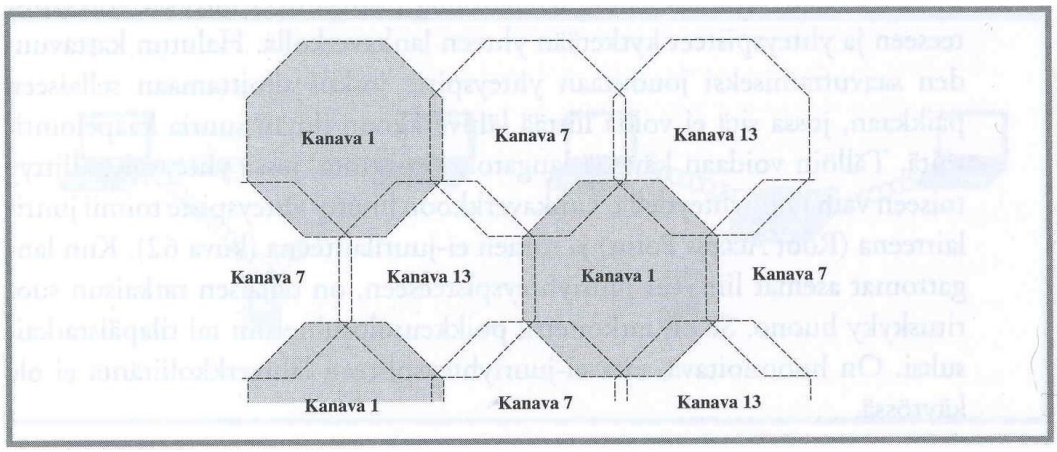
6.3 Tukiasemien sijoittelu

Tukiasema kannattaa sijoittaa sitä tarvitsevien koneiden ”keskelle” siten, että mahdollisimman monesta koneesta olisi siihen lyhyt matka. Jos kantama ei riitä kaikille koneille tai välissä on paksu seinä tai muu häiriötekijä, on turvauduttava useampaan tukiasemaan. Jos tukiaseman ja työasemien välissä on näköyhteys, on pystyttäminen yleensä helppoa ja nopeus paras mahdollinen. Pienet kepeät väliseinätkään eivät rajoita nopeutta paljoa, eikä tukiasemia välttämättä tällaisessa ympäristössä tarvita useita.

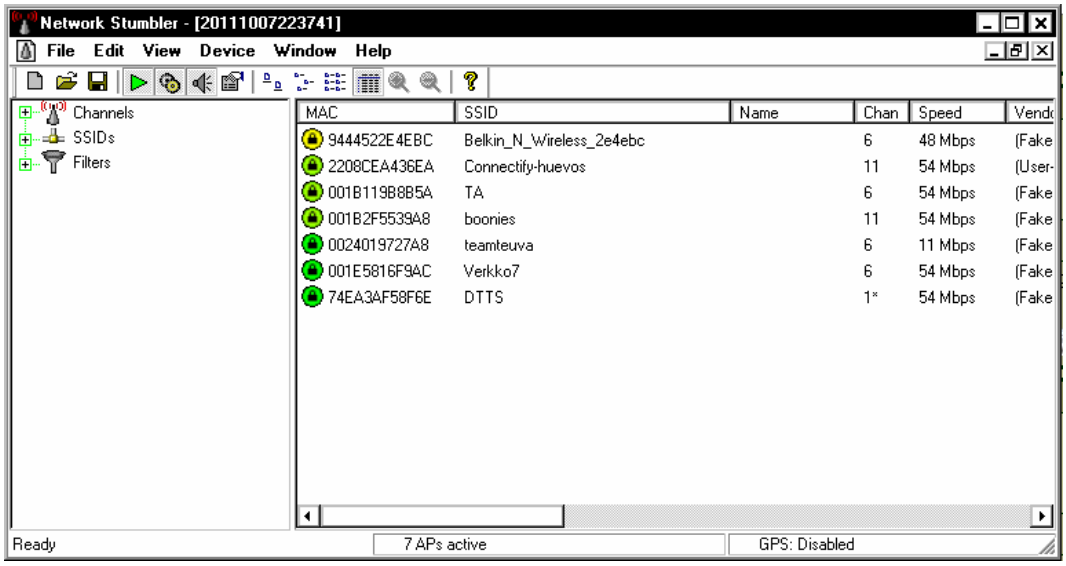
Tukiasema ei saa myöskään olla liian lähellä vastaanotinta, sillä signaali ei ole välttämättä ehtinyt levitä tarpeeksi ja menee osittain vastaanottimen ohi, jolloin tiedonsiirtonopeus laskee. Suositeltava minimietäisyys on noin muutama metri. Tukiasemiakaan ei saa sijoittaa liian lähekkäin, sillä ne voivat häiritä toisiaan. Jos tukiasema on lähellä kohteita ja kantamaa jää ”yli”, kannattaa antennin tehoa laskea, jos se on mahdollista. Tiedonsiirtonopeus saattaa jopa kasvaa, kun tehoa lasketaan tai etäisyyttä kasvatetaan tukiaseman ollessa lähellä vastaanotinta. Antennitehon ollessa maksimissaan saattaa myös signaalin virheiden määrä kasvaa, joka aiheuttaa tiedonsiirtonopeuden laskua.

Jos tukiasemia tarvitaan useita tai lähistöllä on useita WLAN-verkkoja, voi yhteys pätkiä, jos yhteyttä ei rakenneta oikein. Tukiasemien ollessa omia kannattaa vierekkäiset asemat laittaa käyttämään mahdollisimman kaukana toisistaan olevia kanavia (kuva 10). Jos tukiasemat ovat muiden käytössä, on vaikeampi tietää, mitä kanavaa käyttää ettei päällekkäisyyksiä ei tulisi. Tähän on kuitenkin olemassa ohjelmia, esimerkiksi Netstumbler jolla voi tarkkailla tietoja lähialueen langattomista verkoista (kuva 11).

Harkinnan arvoinen asia on myös USB-porttiin kytkettävä WLAN-sovitin, tällä saadaan antenni kauemmas katvetta aiheuttavasta tietokoneen peltikotelosta, joka on vieläpä yleensä sijoitettu pöydän alle tai nurkkaan. Jos USB WLAN-,sovitinta käytetään kannattaa huomioida, että tietokoneessa täytyy olla vähintään USB 2.0-portit, sillä 802.11a ja sitä uudemmat standardit kykenevät suurempaan siirtonopeuteen kuin vanhempi USB 1.1 -liitäntä. (mikropc) (mvnet.fi)



Kuva 10. Wlan-kanavien uudelleenkäyttö. (Matti Puska)



Kuva 11. Netstumbler-käyttöliittymä.

Netstumblerilla näkee kätevästi tietoa lähialueen langattomista verkoista, esimerkiksi mitä kanavaa muut verkot käyttävät.

6.4 Verkon valinta

Verkkoa valitessa pitää tietää, mitä ominaisuuksia tarvitaan (vaatimusmäärittely), tosin suurin ero yleisimmissä standardeissa pienyrityskäytössä on nopeus. Suurin ero on 802.11a-verkolla muihin standardeihin. Sillä se tarjoaa 12 toisiaan häiritsemätöntä kanavaa, muiden tarjotessa vai kolme, mutta sen kantama on huonoin, koska se toimii korkeammilla taajuuksilla ja hyödyn kanavista saa vasta isommissa verkoissa.

Yleisiä standardeja ovat 802.11b, 802.11a ja 802.11g eli b-, a- ja g-verkko, kuitenkin uusin standardi tällä hetkellä on 802.11n. Verkkojen nopeudet ovat suoraavat: B-tyyppi 4.5-11Mb/s, A-tyyppi 6-54Mb/s, G-tyyppi 19-54Mb/s tai N-tyyppi 74-300Mb/s. Henkilökohtaisesti suosittelisin aina uusimman vaihtoehdon valintaa, sillä uudessa standardissa on yleensä aina jotain parannuksia tietoturvan ja siirtonopeuden saralla. Uudemmat standardit ovat myös sopivia alaspäin, mutta nopeus on aina luonnollisesti hitaimman ehdoilla.

6.5 Tukiaseman valinta

Pienissä lähinnä yhden tukiaseman verkoissa voi harkita hankkivansa tukiaseman, jossa on samassa liitäntä tulostinta varten, ethernet-verkkokytkin ja palomuuri. Nämä ominaisuudet eivät nosta tukiaseman hintaa kuin muutamalla kymmenellä eurolla. Verkkokytkin on hyvä olla olemassa myös langattomien verkkojen ympäristössä sillä yrityksessä voi olla koneita, jotka halutaan pitää langallisessa yhteydessä esimerkiksi suuren tiedonsiirron johdosta ja myös kannettavien tietokoneiden varmuuskopiot sujuvat nopeammin langallisella verkolla.

Suurin osa tukiasemista on varustettu Wi-Fi-merkinnällä, joka tarkoittaa sitä, että ne ovat läpäisseet Wi-Fi-testin, joka takaa sen, että laite on yhteensopiva yleisten WLAN-laitteiden kanssa. Tukiasema voi kuitenkin olla ihan hyvä, vaikka siinä ei Wi-fi-merkintää olisikaan, ja todennäköisesti laite läpäisisikin testin, mutta valmistaja ei vain ole halunnut maksaa Wi-Fi-tarrasta. Vakavat yhteensopivuusongelmat ovat kuitenkin harvinaisia nykyään.

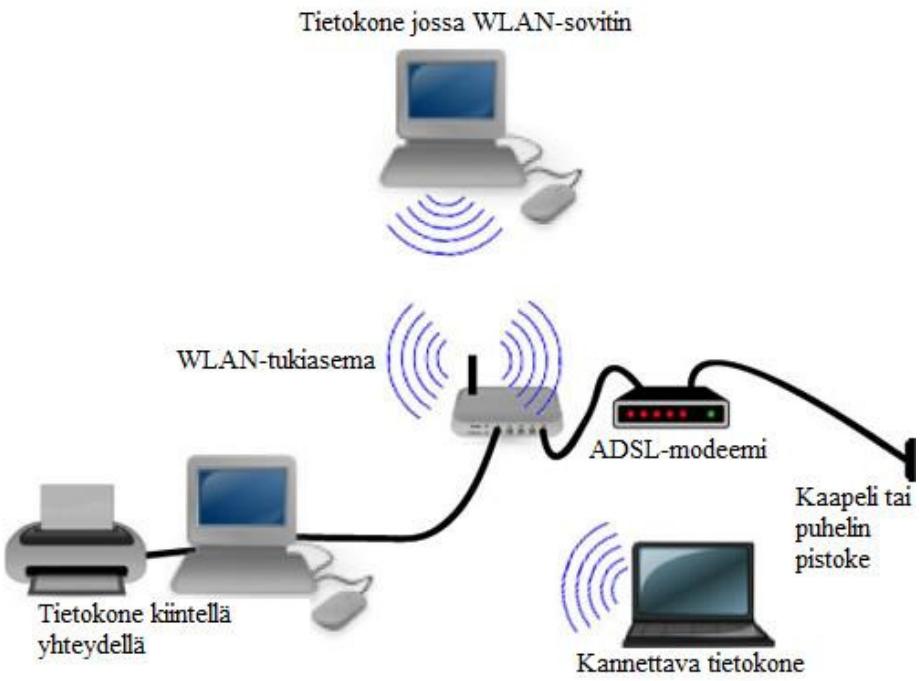
Suositeltavaa on myös käyttää saman valmistajan tuotteita. Sillä varmistetaan, että yhteensopivuus on paras madollinen ja eri komponenttien käyttöliittymät ovat samankaltaiset, joka helpottaa asetuksia laitettaessa. Yleensä kun ostaa kaikki tavarat yhdellä kertaa ja samalta valmistajalta, saa laitteet halvemmalla. (mikropc)

6.6 Kiinteään verkkoon liittäminen

Lähiverkon kautta voidaan jakaa kaikenlaisia resursseja, tiedostoja ja ohjelmia, mutta yleisin on varmasti internetyhteys. Jos langattomassa verkossa on ainoastaan yksi lähetin, voidaan hankkia tukiasema, jossa on sisäänrakennettu ADSL-modeemi, mutta jos modeemi on jo ennestään tai tukiasemia tarvitaan useita, on parempi hankkia pelkkä tukiasema (kuva 12).

Tukiasemassa, jossa on ADSL-modeemi, ei tarvita erillisiä laitteita internetiin pääsyyn, vaan yksi laite hoitaa internetin ja langattoman verkon jakamisen.

Suurimmassa osasta markkinoilla olevista langattomista reitittimistä ei kuitenkaan ole ADSL-modeemia, vaan laajakaistamodeemi, joka liitetään langattoman tukiaseman WAN-porttiin, jolloin internet saadaan jaettua kaikille langattomanverkon käyttäjille.



Kuva 12. Verkon rakenne. (wlanbook.com)

7 TIETOTURVA

7.1 Tietoturvan perusmäärittely

Fyysiseen tietoturvaan kuuluu WLAN-laitteiden sijoittelu siten, että tukiasemat ja antennit ovat poissa ulkopuolisten näkyvistä. Tämä auttaa tietoturvaa siten, että kukaan ei voi kytkeä tietokonetta tukiaseman konsoliporttiin ja muutella

asetuksia. Fyysiseen tietoturvaan kuuluu myös kulunseuranta, asiattomilla ei ole tarvetta päästä tukiasemien tai palvelimien läheisyyteen.

Käyttäjien tunnistus tulisi hoitaa henkilökohtaisilla käyttäjätunnuksilla ja keskittyä käyttäjätietokantaan ja lokikirjauksiin jos mahdollista. Kaikki hallintasalasanat ja tunnukset tulee olla vaikeasti arvattavia eikä niitä saa kirjoittaa muistilapulle, joka liimataan näytön kulmaan.

WLAN-tukiasemista tulee poistaa kaikki oletusasetukset kuten SSID, käyttäjät, salasanat ja SNMP-yhteisötunnukset (community string). Sulje myös kaikki käyttämättömät liitännät.

Etähallinta tulee myös suojata hyvin, käytä ainoastaan salattua yhteyttä ja poista kaikki palvelut, jotka lähettävät salasanat suojaamattomana kuten Telnet ja HTTP-palvelu. Rajoita hallintayhteydet ainoastaan ennalta määriteltyihin IP-osoitteisiin. Jos WEB-hallintaa halutaan kuitenkin käyttää, kannattaa etähallinta rajata lankaverkkoon tai suojata yhteys turvallisemmalla HTTPS-palvelulla.

Poista WLAN-laitteesta kaikki ylimääräiset palvelut ja jätä vain välttämättömimmät. Erityisesti kannattaa kiinnittää huomiota Telnet, TFTP, ja SNMP-versiot 1 ja 2c, mutta myös kaikki muut tarpeettomat palvelut kannattaa poistaa.

WLAN-laitteiden toimintaa ja läsnäoloa tulee seurata tarkasti. Tukiasema kannattaa tunnistaa myös MAC-osoitteella, jolloin sen korvaaminen väärennetyllä asemalla on vaikeampaa. On syytä myös tarkkailla verkossa olevia käyttäjiä ja laitteita: verkosta ei saa löytyä tunnustamattomia laitteita tai käyttäjiä.

Laitteet tulee myös pitää ajan tasalla. On hyvä seurata säännöllisesti valmistajan sivuilta päivityksiä ja uutisia ja päivittää laitteet tarvittaessa.

On syytä pysyä tietoturvasuunnitelmassa ja käyttää valittuja laitteita ja salausmenetelmiä.

7.2 Salauksien valinta

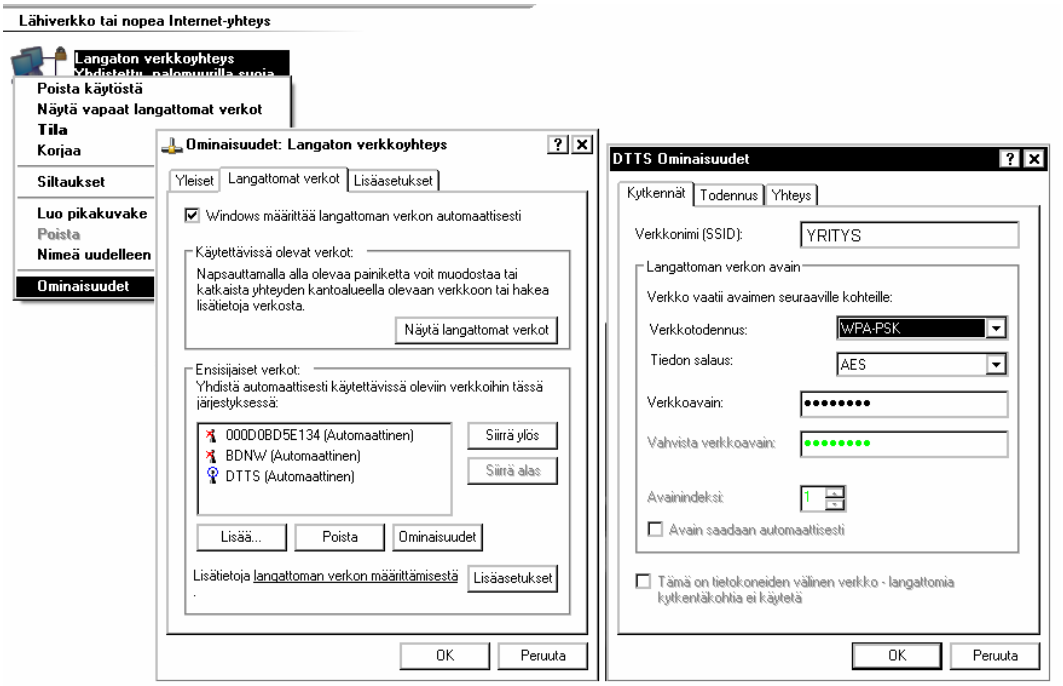
Ensimmäiseksi on hyvä kartoittaa, minkälaisia salauksia langattomaan verkkoon tulevat tietokoneiden käyttöjärjestelmät ja verkkokortin ajurit tukevat. Eri verkkokorttien tukemat salaukset voidaan tarkistaa verkkokorttien ajureiden asetuksista. Kannattaa ottaa ylös, mitä salauksia mikäkin kone tukee. Kun kaikki koneet on tarkistettu ja tiedetään, mitä salauksia voidaan käyttää niin, että kaikki pääsevät verkkoon, valitaan salausprotokollista vahvin. Mikäli tästä huolimatta jotkin koneet eivät pääse verkkoon, voidaan keventää salausta ja, jos tämäkään ei auta, kokeilla kokonaan ilman salaista. Jos yhteys ei toimi ilman salausta, on vika todennäköisesti verkkokortin ajureiden asetuksissa. Jos edellä mainittuja ongelmia ilmenee, en kuitenkaan suosittele salausten laskemista kuin testimielessä -parempi päivittää konetta kuin laskea tietoturvaa. Pienyritysverkon suojaksi hyviä perussalauksia ovat WPA2 – AES tai WPA – AES. Älä missään nimessä luota pelkkään WEP-salaukseen, sillä se on helposti kierrettävissä ilman suurempaa hakkerointia.

7.3 Salauksen asettaminen

Windows XP SP2-, Vista- ja 7-käyttöjärjestelmissä voidaan tarkistaa seuraavasti, mitä salauksia kone tukee ja käyttää. Mene Käynnistä-valikkon kautta Ohjauspaneeliin, napauta Verkko ja internet-yhteydet, napauta Verkkoyhteydet, napauta hiiren oikeanpuoleisella näppäimellä langattoman verkkoyhteyden kuvaketta ja valitse Ominaisuudet. Mene välilehdelle Langattomat verkot ja ensisijaiset verkot Ominaisuudet ja Wlan-salausasetukset-ikkuna aukeaa (Kuva 13). Mikäli käytössä on langattoman kortin valmistajan hallinnointiohjelma, täytyy muutokset tehdä kyseisen ohjelman kautta. (pukema)

Osissa tukiasemista on salausten asettamiselle oma painike, jota painamalla asetukset menevät automaattisesti päälle. Tämä nopeuttaa salausten asettamista huomattavasti, mutta tässä on omat riskit, sillä salausohjelmia on useita ja osa niistä ei ole yhteensopivia tällaisia ovat esimerkiksi AOSS ja SES. Parhaiten

ominaisuus toimii, kun tukiasemat ja verkkokortit ovat samalta valmistajalta. Tähän ominaisuuteen kannattaa suhtautua pienellä varauksella ja asetukset kannattaa tarkistaa, vaikka pika-asetus näyttäisi toimivan hyvin. (pukema)



Kuva 13. Salauksien valinta.

7.4 Termistöä

Tukiaseman käyttöliittymä on täynnä valikoita ja englanninkielisiä termejä, joita on hyvä tietää ennen muutosten tekemistä. Seuraavassa luetteloa yleisimmistä ja tarpeellisista asetuksista. (pukema)

7.4.1 Network type - verkon tyyppi

Yleisimmät verkkotyypit ovat Infrastructure ja AD-hoc. Infrastructure on tukiasemiin pohjautuva verkko eli yleisin tapa ja AD-hoc verkossa laitteet keskustelevat keskenään ilman tukiasemaa. Joissakin käyttöliittymissä kysytään

myös verkon nopeutta, mutta sen määrää tukiasema eli verkko ei toimi nopeammin kuin tukiasema antaa myöten. Kannattaa siis olla tietoinen, onko verkko B-, G- tai N-tyyppinen. (pukema)

7.4.2 Channel - radiokanava

Radiokanavan valintaan vaikuttaa, onko alueella muita langattomia verkkoja. Jos verkossa on useita tukiasemia, kannattaa vierekkäiset tukiasemat laittaa käyttämään mahdollisimman kaukaisia kanavia. Asiaa voi hankaloittaa, jos läheiset tukiasemat eivät ole omia koska on vaikeaa tietää, mitä kanavaa ne käyttävät. Tähän on tosin olemassa ohjelmia, esimerkiksi Netstumbler. Useissa tukiasemissa on myös auto-toiminto, joka tarkoittaa, että tukiasema valitsee itse hyvän kanavan. Kanavia on 13, mutta osa niistä häiritsee toisiaan, siksi läheisiä tukiasemia ei saa laittaa käyttämään vierekkäisiä kanavia. (pukema)

7.4.3 SSID – verkkonimi

Jokaisella verkolla on oma nimi, jotta verkot on helppo erottaa toisistaan. SSID ei siis ole verkon salasana niin kuin monesti luullaan. Osassa tukiasemista on mahdollisuus piilottaa SSID, mutta se ei tuo lisäturvaa, sillä verkko näkyy, kun siinä on liikennöintiä ja se hidastaa joidenkin koneiden liittymistä verkkoon. Jätä siis SSID näkyviin ja valitse nimi siten, että tunnistat verkon ja muutkin tietävät, että yhteys on sinun ja se ei ole julkinen. (pukema)

7.4.4 Security mode -tietoturvatila

Yleisiä vaihtoehtoja ovat WEP, WPA ja WPA2. Tietoturva kannattaa asettaa mahdollisimman kovaksi, pelkkä WEP-salaus ei riitä suojaamaan verkkoa tarpeeksi, mutta on parempi kuin ei salausta ollenkaan. WPA ja WPA2 ovat uudempia ja vahvempia salauksia, joihin saa liitettyä lisäominaisuuksia

paremmin. WPA2 on paras valinta, sillä se on uusin ja siihen saa liitettyä tarvittaessa RADIUS-palvelun. (pukema)

7.4.5 WPA algorithm – WPA-salausalgoritmi

WPA-salausta valittaessa on yleensä valittavana TKIP- tai AES-salaus. Näistä kannattaa valita uudempi ja turvallisempi AES-salaus. (pukema)

7.4.6 Shared key – jaettu salausavain

Salausavain on langattoman verkon salasana, jota se kysyy siihen liityttäessä. Salasanan valinnassa kannattaa olla tarkkana niin kuin aina salasanaa valittaessa, sillä huono avain voidaan arvata tai päätellä. Salausavain kannattaa tehdä mahdollisimman pitkäksi ja vaikeaksi, sillä kone muistaa salasanan eli sitä ei tarvitse itse muistaa. Kannattaa tietenkin laittaa salasana ylös sen varalta että verkkoon pitää liittää uusi kone. (pukema)

7.4.7 MAC filter – MAC-suodatin

Jokaisella verkkokortilla on oma yksilöllinen MAC-osoite. Langattoman tukiaseman voi määrittää siten, että se ottaa vastaan ainoastaan tietyt MAC-osoitteet, mutta tämäkään ei tuo merkittävää, lisäturvaa sillä on olemassa ohjelmia, joilla osoitteen voi muuttaa tai väärentää. (pukema)

7.5 Tietomurron havaitseminen

Monet WLAN-kortit saa asetettua kuuntelutilaan, jolloin ne eivät lähetä tietoa, vaan vastaanottavat verkossa liikkuvaa tietoa. Tämänkaltaista verkkokuuntelua on mahdotonta havaita. Tätä ominaisuutta voi kuitenkin käyttää tietomurron

havaitsemiseen ja sillä on kätevä tarkistaa vieraat tai väärennetyt MAC-osoitteet, jotka yrittävät tunkeutua verkkoon. Väärennetyn MAC-osoitteen tunnistaa helposti silloin jos tietokone jolle osoite kuulu on suljettuna mutta verkossa tapahtuu liikennettä kyseisellä osoitteella. Myös tukiaseman loki on hyvä tarkistaa säännöllisesti, sillä myös sieltä näkee, onko tukiasemaa kohtaan yritetty hyökätä. Näiden tietojen perusteella voidaan tarkistaa, onko verkon tietoturva halutulla tasolla vai tulisiko sitä nostaa.

7.6 Tarkistuslista

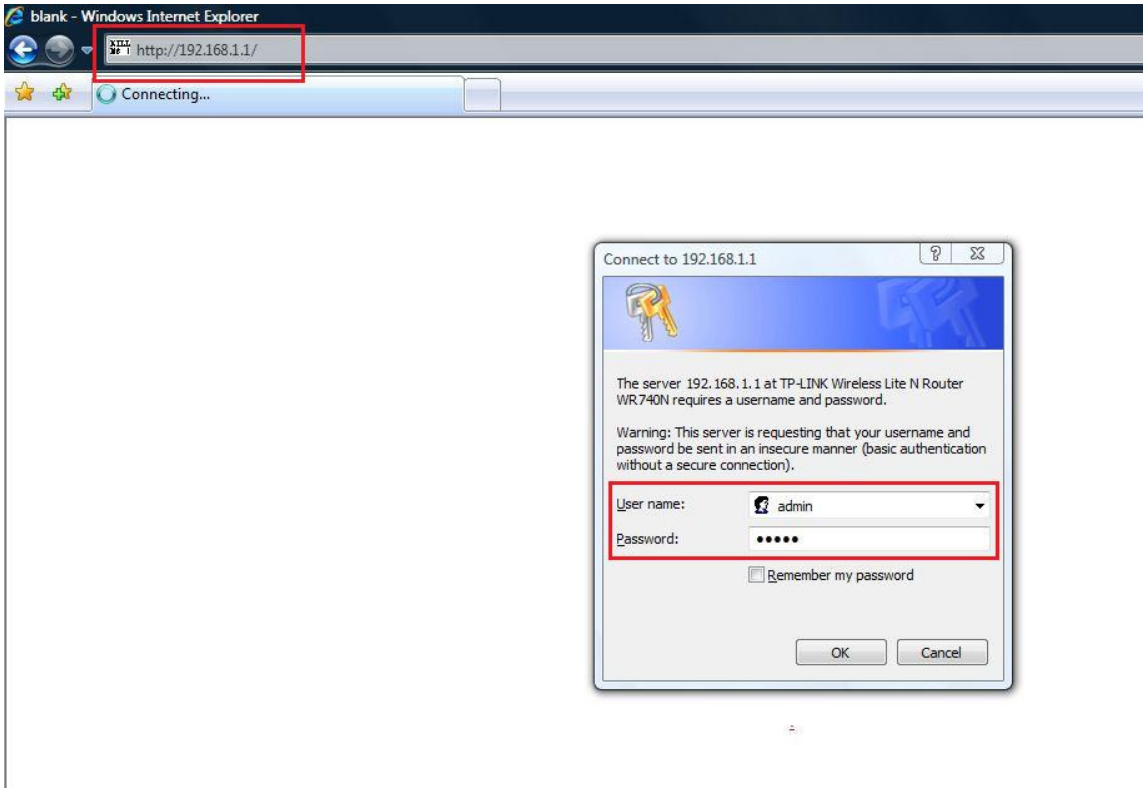
- Muuta WLAN-tukiaseman käyttäjätunnus ja salasana. Muuten kuka tahansa voi mennä tukiasemaan ja muuttaa sen asetuksia.
- Liikenteen salaus tulee olla vähintään WPA- ja WPA2-salaus. Käytä ainoastaan hätätapauksessa ja tilapäisesti WEP-salausta, sillä se on heikko ja helppo murtaa.
- SSID kannattaa muuttaa sellaiseksi, että tunnistat oman verkon.
- Säädä tukiaseman lähetysvoimakkuus siten, että verkko ei kanna halutun alueen ulkopuolelle.
- Poista ja estä kaikki turhat yhteydet, joita et käytä.
- Sulje kaikki laitteet ja tukiasemat, jos ne ovat käyttämättä pidemmän aikaa. Suljettuun tukiasemaan on mahdotonta tunkeutua.
- Internetyhteys tulee aina suojata palomuurilla. Tukiasemissa saattaa olla myös palomuuri ja tietokoneiden ohjelmallisia palomuureja kannattaa käyttää.
- Tarkista, että sinulla on käytössä viimeisimmät tietoturvapäivitykset.

8 LANGATTOMAN TUKIASEMAN ASETUKSET

Seuraavassa näytän, kuinka tukiasema asennetaan ja sen tietoturva-asetukset laitetaan päälle. Asetukset ovat kaikissa tukiasemissa samankaltaisia ja käyttöjärjestelmällä ei ole merkitystä niitä päälle laitettaessa.

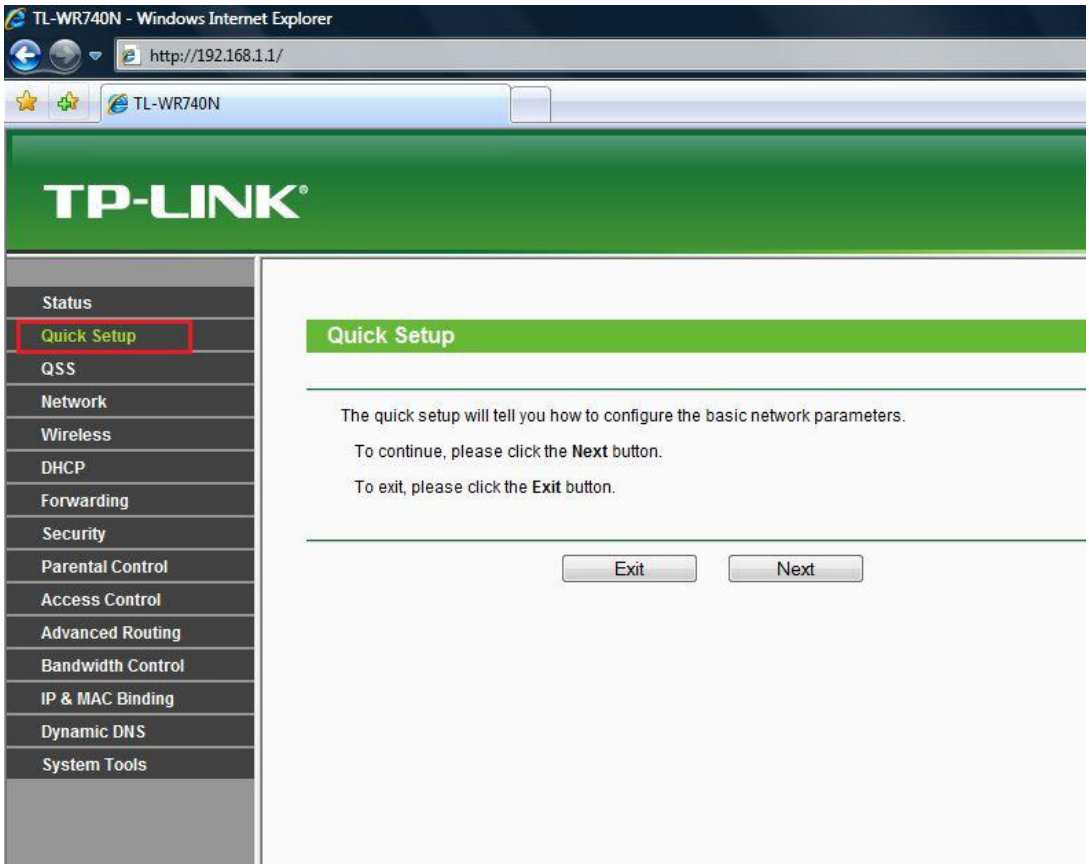
Tukiasema: TP-LINK TL-WR740N

Tukiaseman mukana tuli asennus-CD. jonka avulla saa aseman nopeasti toimimaan, mutta tätä en kuitenkaan missään nimessä suosittele. sillä asennuksessa ei missään vaiheessa kosketa moneen tärkeään tietoturva-asetukseen esimerkiksi tukiaseman salasana ja osoite jätetään tehdasasetuksille, joten kuka tahansa voi käydä muuttamassa aseman asetuksia.



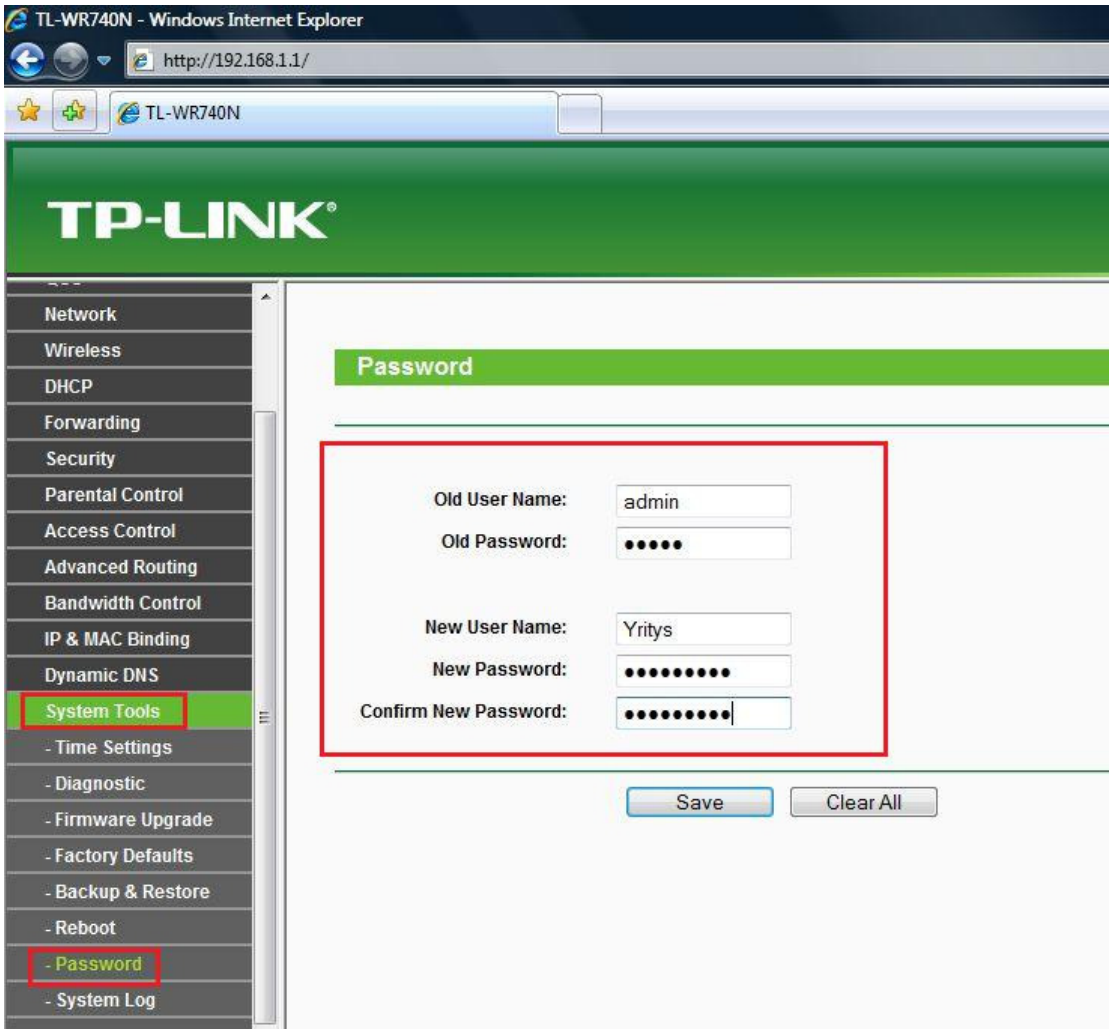
Kuva 14. Tukiasemaan kirjautuminen.

Kun tukiaseman on pistetty päälle saa siihen yhteyden selaimella laittamalla osoitekenttään tukiaseman IP-osoitteen. Tässä tapauksessa se on http://192.168.1.1. Kun selain kysyy salasanaa, tarkista ohjeista tehdasasetusten salasana. Tässä laitteessa salasana ja käyttäjänimi olivat *admin*.



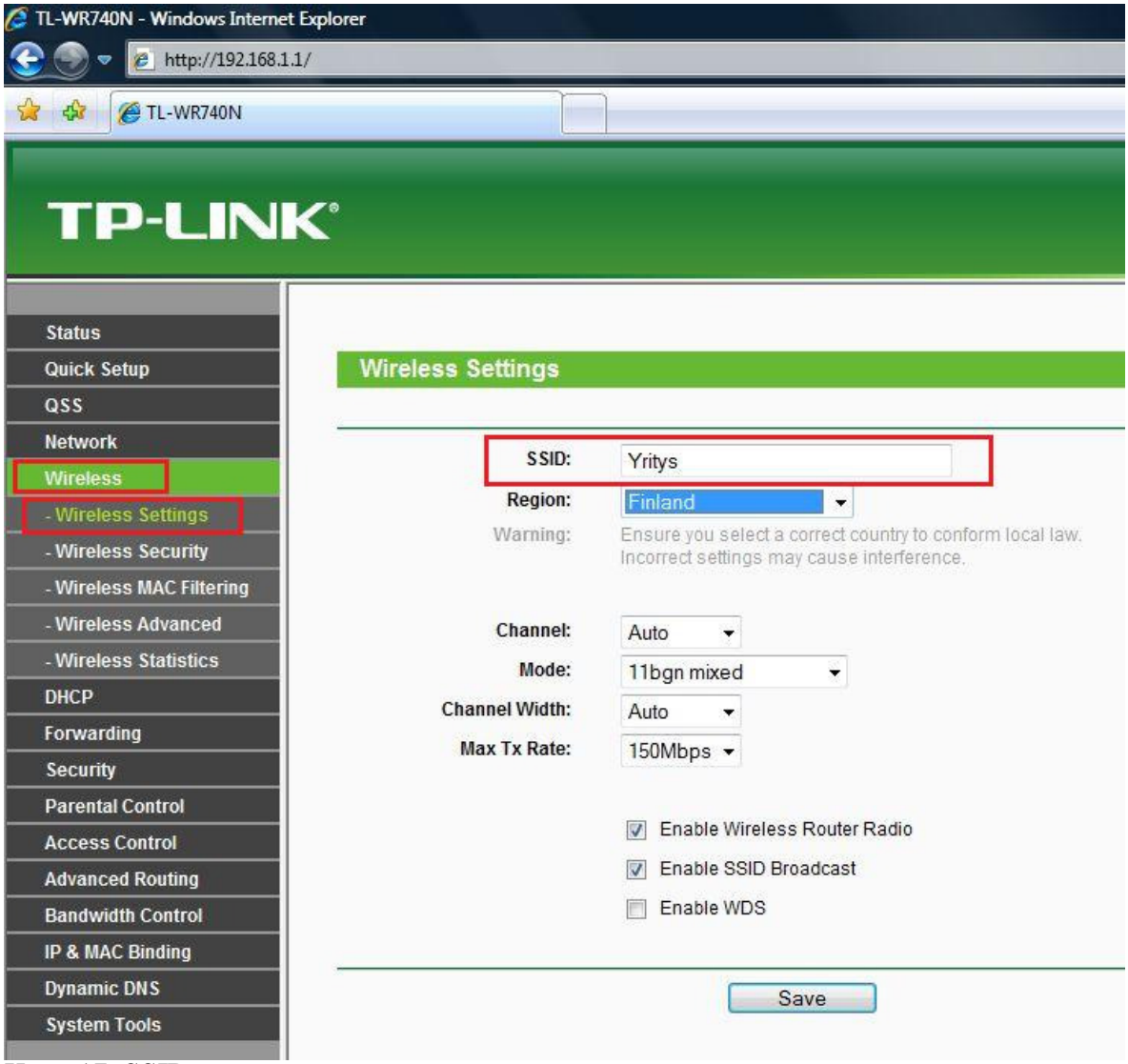
Kuva 15. Quick Setup.

Myös tästä käyttöliittymästä löytyy quick Setup-toiminto, jolla saa langattoman verkon nopeasti toimimaan, mutta en tätä kuitenkaan suosittele pelkästään käytettäväksi. Quick Setupilla saa kätevästi internetin toimimaan nopeasti, varsinkin jos ei ole varma kaikista internetyhteyden tiedoista. Asetus kuitenkin jättää tietoturvan täysin auki, joten asetukset on laitettava manuaalisesti päälle.



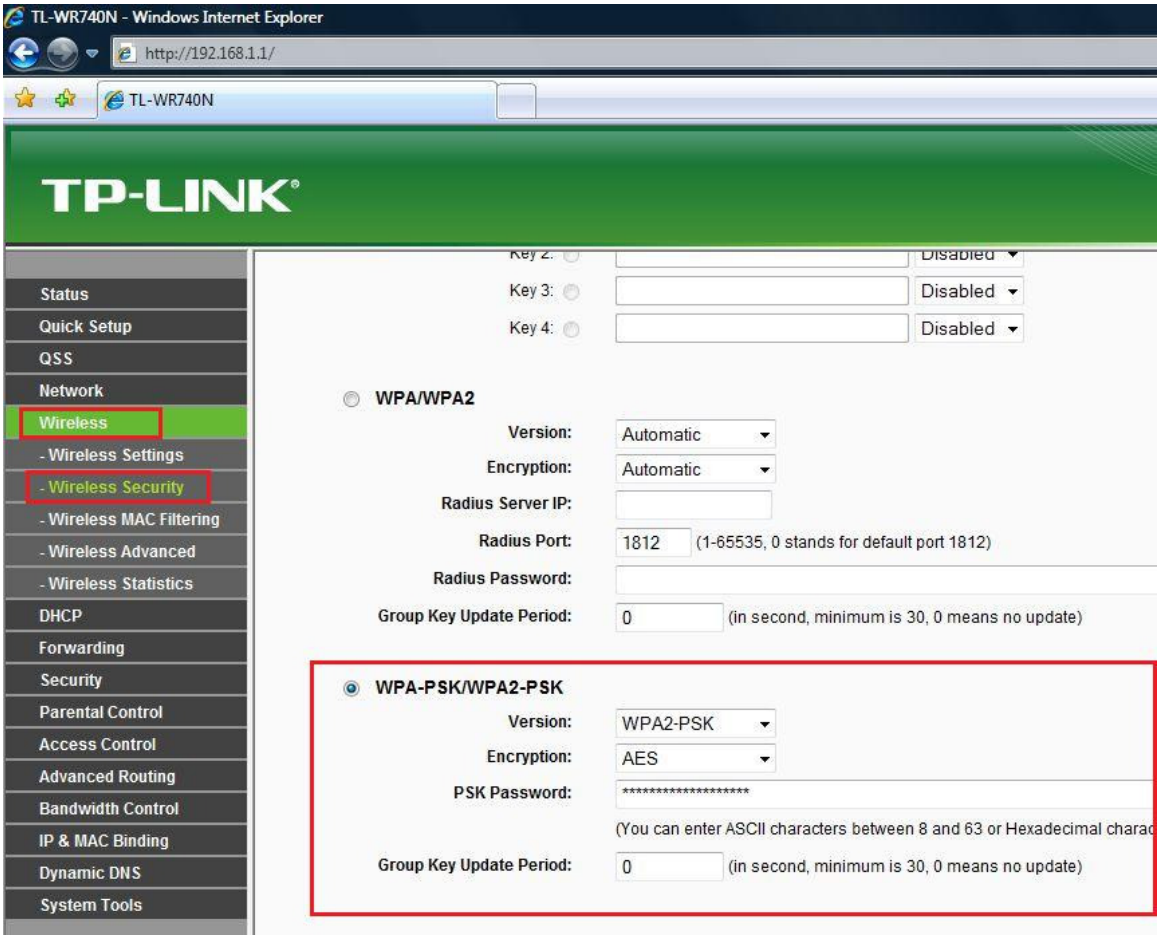
Kuva 16. Salasanan vaihtaminen.

Aivan ensimmäiseksi kannattaa vaihtaa tukiaseman salasana ja käyttäjätunnus, sillä nämä ovat kaikissa vastaavissa laitteissa samat ja ne saa helposti tietoon kuka tahansa. Jos nämä jättää tehdasasetuksille, voi kuka tahansa ottaa yhteyden tukiasemaasi, mennä vakiosalasanoilla sisään ja päästä verkkoosi käsiksi tai jopa kaapata tukiaseman omaan käyttöönsä. Tämän sattuessa kannattaa resetoida tukiasema siinä olevasta napista, jolloin kaikki asetukset nollautuvat. Tämä on myös kätevä keino, jos unohdat oman tukiaseman salasanan.



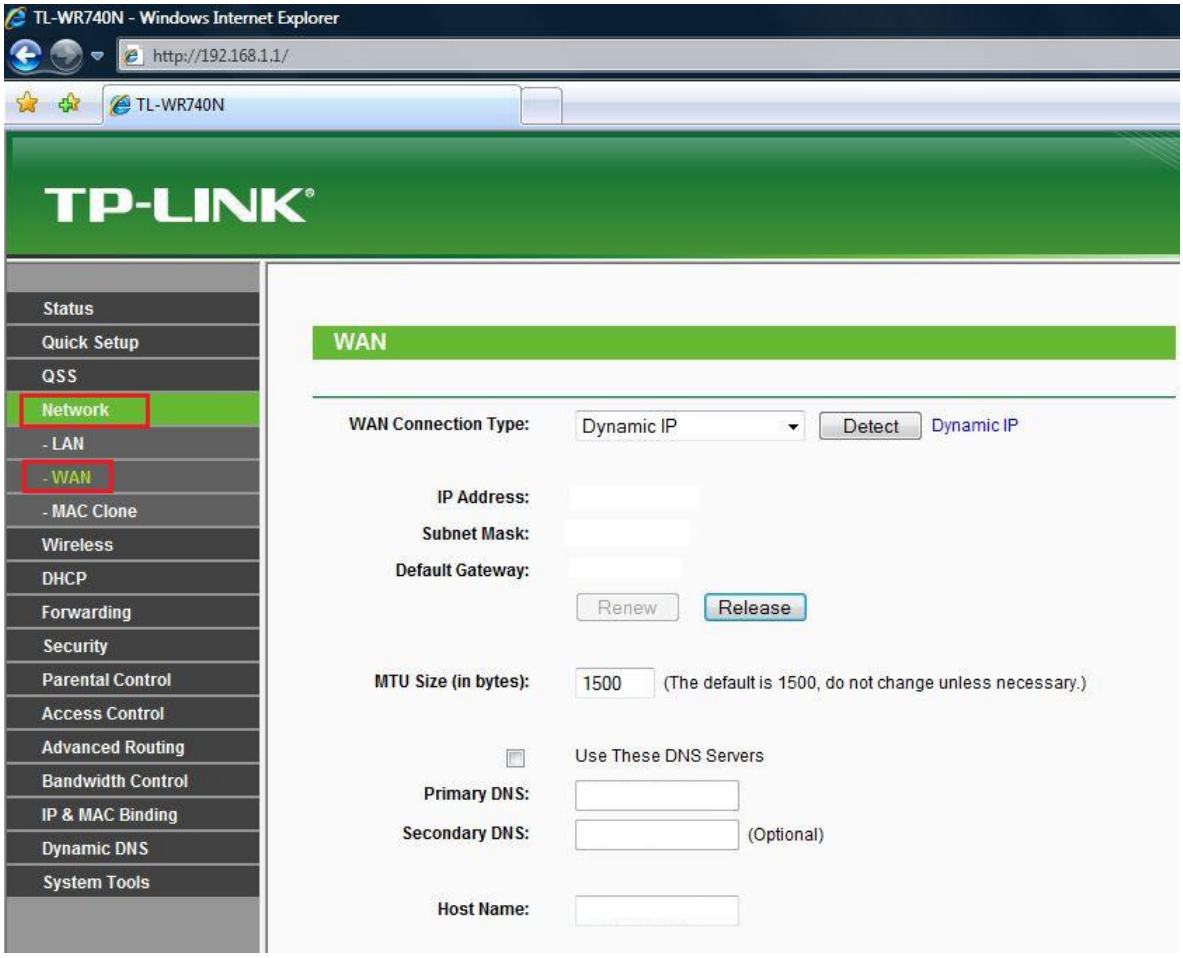
Kuva 17. SSID.

Langattoman verkon asetuksista kannattaa vaihtaa SSID sellaiseksi, että tunnistat verkon, johon yrität liittyä. Varsinkin kaupunkialueella saattaa langattomia verkkoja olla useita, jolloin kanavan valintaan ja muihin lähetystietoihin kannattaa kiinnittää huomiota.



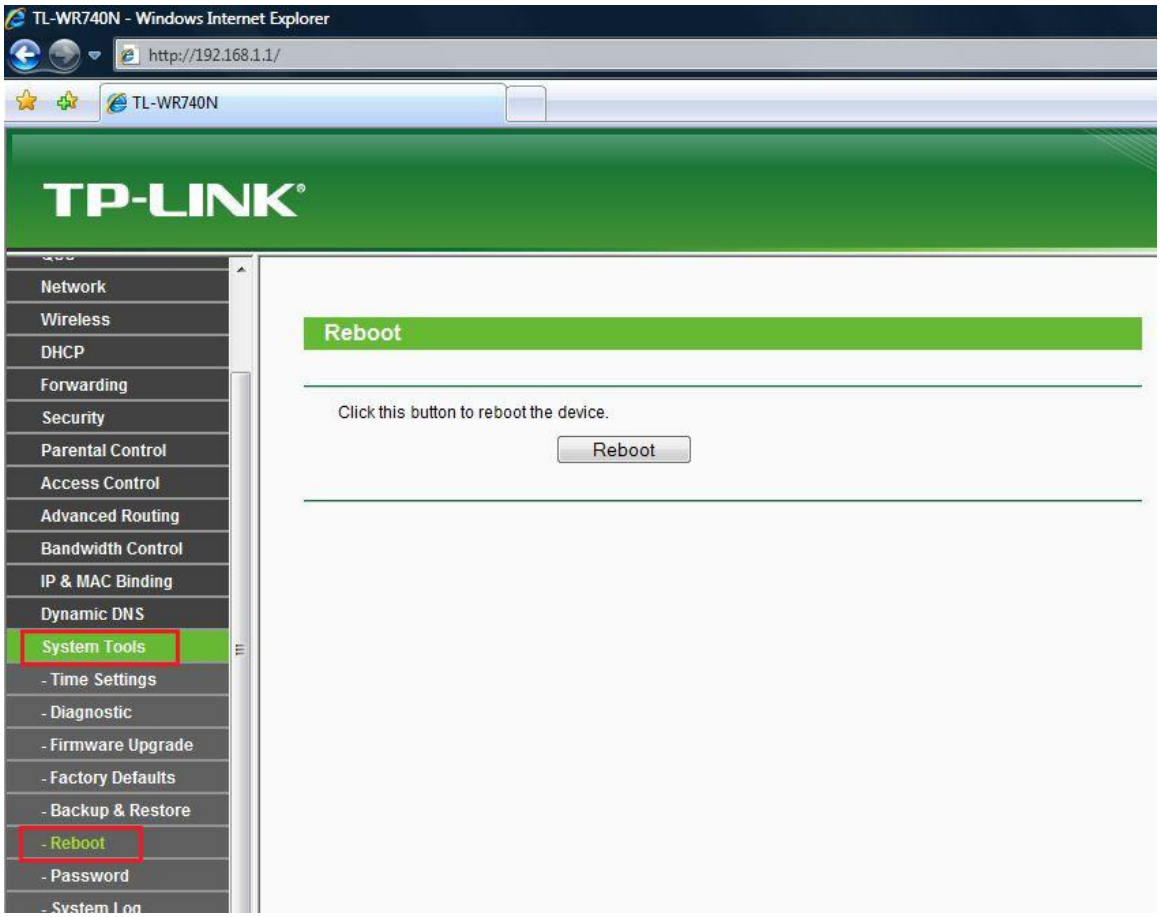
Kuva 18. Tietoturva-asetukset.

Tietoturva-asetukset kannattaa aina laittaa mahdollisimman koviksi. Jotkut vanhat koneet eivät välttämättä tue uusimpia tietoturva-asetuksia, mutta silloin kannattaa päivittää konetta eikä laskea tietoturvaa. Tämä tukiasema tukee myös RADIUS-palvelun käyttöä, joka on suositeltavaa varsinkin isommissa verkoissa.



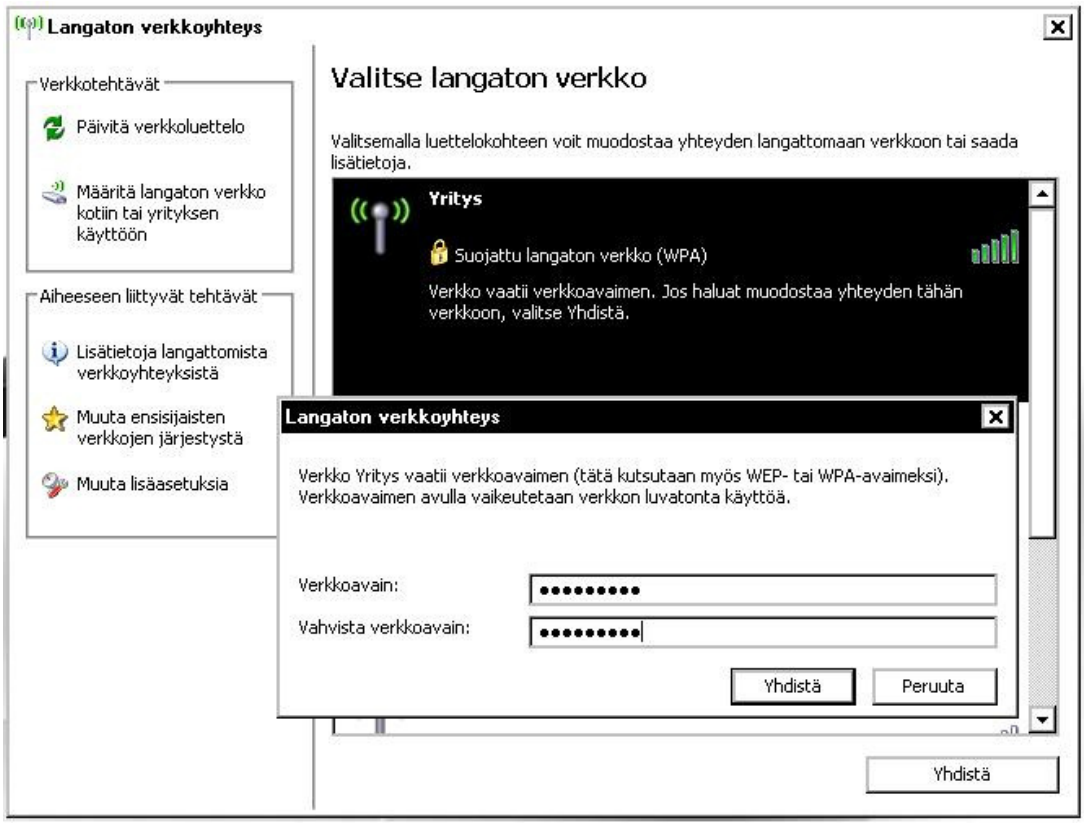
Kuva 19. Internet asetukset.

Jos et aikaisemmin käyttänyt quick Setup-toimintoa, pitää internetasetukset määrittää manuaalisesti.



Kuva 20. Uudelleen käynnistys.

Jotta asetukset tulisivat voimaan, täytyy asema välillä käynnistää uudelleen.



Kuva 21. Tukiasemaan yhdistäminen.

Kun asetukset ovat valmiit, näkyy langaton verkkosi tietokoneiden langattomissa verkkoyhteyksissä.

9 YHTEENVETO

Langattomuus on nykyään enemmän sääntö kuin poikkeus. Laitteen sitominen yhteen paikkaan hidastaa toimintaa ja hankaloittaa tiedon liikuteltavuutta. Langattomassa ympäristössä liikkuminen on vapaata, helppoa ja luotettavaa. Myös verkon pystyttäminen on kätevää eikä vaadi ympäristön muokkausta. Langaton verkko yltää syrjäisimpiinkin kolkkiin, jonne langallinen verkko olisi vaikeaa tai jopa mahdotonta saada.. Langattoman verkon pystyttäminen on usein jopa halvempaa kuin langallisen. Myös nopeuserot verrattuna langalliseen verkkoon ovat pienet eivätkä ne näy normaalikäytössä.

Pienessä tai keskisuuressakin yrityksessä verkon pystyttäminen omin voimin on ehdottomasti harkinnan arvoinen vaihtoehto, etenkin jos yrityksestä löytyy henkilö, jolla on vähän pohjatietoa aiheesta. Muutamia tukiasemia sisältävän verkon pystyttäminen ja sen hallinta onnistuu alan harrastajalta siinä missä minkä tahansa muun toimistolaitteen asentaminen varsinkin, kun apuna on opas. Pystyttämällä verkon itse säästää rahaa ja aikaa, kun ei tarvitse odotella ammattilaisen kallista apua.

Pelkkä verkon pystyyn saaminen ei vaadi isoa ponnistelua kiitos helppokäyttöisten pika-asennusohjelmien, mutta että verkko olisi oikeasti turvallinen ja fiksusti koottu, kannattaa apuna käyttää opasta. Opas on pystytysvaiheessa korvaamaton apu, sillä verkon pystytyksessä on monta kohtaa, mitkä helposti unohtuvat tai niitä ei osaa ottaa huomioon. Myös tietoturvasyistä on hyvä käyttää apuna opasta, sillä pienikin unohdus tai rastin poistaminen asetuksista saattaa luoda tietoturvariskin.

Tietoturva arveluttaa vielä joitakin yrityksiä johtuen Wlan-verkkojen turvattomuudesta sen alkuaikoina. Nämä pelot johtuvat kuitenkin vain tietämättömyydestä ja asiaan perehtyneet tietävät, että verkot ovat olleet turvallisia jo vuosia ihan harrastelijakäytössäkin. Tiedon salaamiseen ja yhteyksien suojaamiseen on olemassa useita hyviä keinoja, jotka ovat tehty helppokäyttöisiksi ja nopeiksi asentaa. Langaton verkko on oikein rakennettuna ja suojattuna pienyrityskäytössä yhtä turvallinen kuin langallinenkin verkko. Langattomassa verkossa tietoturvassa keskitytään tiedon salaukseen, mutta kuten langallisessakin verkossa myös fyysinen tietoturva on tärkeää. Tukiasemien sijoittelussa on otettava huomioon niin kuuluvuus kuin tietoturva.

Suunnittelu on tässäkin asiassa erittäin tärkeää: hyvin suunniteltu verkko on turvallinen eikä verkon tietoturvaa kannata oppia epäonnistumisten kautta. Verkon on oltava turvallinen alusta asti eikä niin, että tietoturvaa parannellaan sitä mukaa kun murtoja ja aukkoja havaitaan.

LÄHTEET

Kaj Granlund - Langaton Tiedonsiirto 2001 Docendo Finland Oy

Matti Puska - Langattomat Lähiverkot 2005 Talentum Media Oy ja Matti Puska

Gunvald Hedemalm - Tietoverkon perusteet 2000 3.uudistettu painos Tummavuoren kirjapaino Oy, Vantaa

David Clark - Wireless Networking Complete 2009 By Pei Zheng, Professor, Arcadia University, Glenside, PA, USA; Consultant in mobile wireless sevices Larry Peterson, Robert E. Kahn Professor of Computer Science, Princeton University Vice President and Chief Scientist, Verivue, IncBruce Davie, Cisco Systems, Boxborough, MA, USAAdrian Farrel, Founder of Old Dog Consulting, North Wales, UK

Internetistä:

Vesa Ylä-Jääski, Janne Antson - mikropc [viitattu 10.4.2011] Saatavilla Internetissä: <http://mikropc.net/nettilehti/pdf/2503200440.pdf>

Sami Pukema - pukema [viitattu 12.5.2010] Saatavilla Internetissä: <http://www.pukema.net/wlan.html>

cisco [viitattu 16.8.2011] Saatavilla Internetissä: <http://www.cisco.com/en/US/docs/wireless/access_point/1300/12.2_15_JA/configuration/guide/o13ovrv.html>

brother.com [viitattu 18.9.2011] Saatavilla Internetissä: <http://welcome.solutions.brother.com/BSC/public/eu/fi/fi/faq/faq/000000/002100/000097/faq002197_001.html?reg=eu&c=fi&lang=fi&prod=mfc5895cw_>

microsoft.com [viitattu 2.10.2011] Saatavilla Internetissä: <http://technet.microsoft.com/en-us/library/cc757652%28WS.10%29.aspx>

Zaib Kaleem - wlanbook.com [viitattu 2.10.2011] Saatavilla Internetissä: <http://wlanbook.com/which-is-faster-wireless-router-or-wired-internet>