

TAMPEREEN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

Tietokonetekniikan suuntautumisvaihtoehto

Marko Lehtinen

WLAN-HOTSPOT-TOTEUTUS LANGATON TAMPERE -VERKKOYHTEISÖÖN

Työn ohjaaja

Yliopettaja Kai Poutanen

Työn teettäjä

WizIT Oy, valvojana järjestelmäasiantuntija Marko Lähteenmäki

Tampere 2008

TAMPEREEN AMMATTIKORKEAKOULU

Tietotekniikka

Tietokonetekniikka

Lehtinen Marko

WLAN-Hotspot-toteutus Langaton Tampere -verkkoyhteisöön

Insinööriyö

42 sivua + 5 liitesivua

Työn ohjaaja

Yliopettaja Kai Poutanen

Työn teettäjä

WizIT Oy, valvojana järjestelmäasiantuntija Marko Lähteenmäki

Huhtikuu 2008

Hakusanat

Langaton Tampere, WLAN, m0n0wall, tukiasema

TIIVISTELMÄ

Langaton Tampere -verkkoyhteisöltä puuttui pk-yrityksille edullinen ja monipuolinen ratkaisu, joka osaisi myös Langattoman Tampereen WLAN-verkon vierailijoille tarkoitetun käyttötavan. Vierailijoille tarkoitettu käyttötapa vaatii Captive portal -toiminnallisuuden toimiakseen. Captive portal -toiminnallisuus on yleensä vain kalliimmissa yritystason laitteissa, ja ne ovat liian kalliita mikroyrityksille. Työn tavoitteena oli toteuttaa toimiva ja monipuolinen ratkaisu, joka sopii myös hinnaltaan mikroyritykseen.

Toteutus on tehty m0n0wall-palomuuriohjelmistolla ja Soekris net4501 -laitteella. Toteutus toimii lähes minkä tahansa tukiaseman kanssa. Toteutusta tehtäessä testattiin useita tukiasemia, mutta tässä työssä keskitytään niistä vain kolmeen. Perustukiasemia edustamaan valittiin Linksys WAP54G, joka on edullinen ja yksinkertainen tukiasema. Yritystukiasemiksi valittiin Ruckus 2925 ja Zyxel NWA-3500, jotka ovat huomattavasti perustukiasemia monipuolisempia ja kalliimpia.

Työssä käsitellään tietoturvanäkökohtia ja laitteiden ominaisuuksia. Insinööriyössä annetaan yksityiskohtaiset ohjeet, kuinka m0n0wall ja tukiasemat konfiguroidaan Langattomaan Tampereeseen. Lisäksi kerrotaan, kuinka toteutusta voidaan käyttää ilman Langaton Tampere -verkkoyhteisöä.

TAMPEREEN POLYTECHNIC

Computer Systems Engineering

Computer Engineering

Lehtinen Marko

WLAN-Hotspot Implementation to Langaton Tampere

Networking Society

Engineering Thesis

42 pages, 5 appendices

Thesis Supervisor

Senior Lecturer Kai Poutanen

Commissioning Company

WizIT Oy. Supervisor: System Specialist Marko Lähteenmäki

April 2008

Keywords

Langaton Tampere, WLAN, m0n0wall, hotspot, Access Point

ABSTRACT

Langaton Tampere networking society did not have reasonable priced solution for small to medium sized companies, which also knows how to do Langaton Tampere visitors authentication. Visitor's authentication demands Captive portal technique to work properly. Captive portal technique is usually only used in expensive Enterprise-level appliances and those appliances are too expensive for micro corporations. The purpose of this work is to build working and versatile solution, which is cheap enough for micro corporations.

The solution is based on m0n0wall firewall software and Soekris net 4501 hardware. The solution can be used at almost every access point. While developing the solution I tested many access points, but in this thesis I concentrate on only three access points. The Linksys WAP54G is a basic access point which is cheap and simple. Enterprise-level access points Ruckus 2925 and Zyxel NWA-3500 are more expensive and more versatile than basic access points.

This thesis purpose is to examine security aspects and properties of appliances. Thesis gives detailed guides how to configure m0n0wall and access points to Langaton Tampere networking society. Additionally how the solution can be used without Langaton Tampere networking society.

SISÄLLYSLUETTELO

TIIVISTELMÄ	2
ABSTRACT.....	3
SISÄLLYSLUETTELO	4
KÄYTETYT MERKINNÄT JA TERMIT	5
1 JOHDANTO	7
2 TURVALLISEN LANGATTOMAN VERKON TOTEUTUKSESTA.....	8
3 LANGATON TAMPERE -VERKKOYHTEISÖ.....	10
3.1 WirelessTampere-käyttötapa.....	11
3.2 LANGATON-WPA-käyttötapa	12
4 SOEKRI NET4501	12
5 MONOWALL.....	13
6 CAPTIVE PORTAL	14
6.1 HTTP-uudelleenohjaus.....	15
6.2 IP-uudelleenohjaus	15
6.3 DNS-uudelleenohjaus.....	15
6.4 Captive portal -kirjautumissivu.....	16
7. MONOWALLIN KONFIGUROINTI.....	17
7.1 IP-osoitteiden asetukset.....	18
7.2 Palomuurisäännöt	19
7.3 Captive portal -konfigurointi.....	21
8 TUKIASEMIEN KONFIGUROINTI.....	26
8.1 Perustukiasema Linksys WAP54G	26
8.1.1 Linksys WAP54G:n konfigurointi LANGATON-WPA-käyttötapaan.....	27
8.1.2 Linksys WAP54G:n konfigurointi WirelessTampere-käyttötapaan.....	29
8.2 Yritystason tukiasemat	29
8.2.1 Ruckus 2925.....	29
8.2.2 Zyxel NWA-3500	33
9 VIERAILIJAVERKKO ILMAN LANGATON TAMPERE -VERKKOYHTEISÖÄ	38
10 YHTEENVETO	38
LÄHTEET.....	40
LIITTEET	42

KÄYTETYT MERKINNÄT JA TERMIT

802.11g	IEEE:n standardi 54Mbit/s WLAN-yhteydelle
802.1q	IEEE:n standardi virtuaalisille verkoille
802.1x	IEEE:n standardi porttikohtaiselle todentamiselle
Active Directory	Microsoftin tekemä käyttäjätietokanta ja hakemistopalvelu
ADSL	Asymmetric Digital Subscriber Line
Captive portal	Kaappaava WWW-palvelin
CompactFlash	Muistikorttitekniikka
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
Ethernet	Pakettipohjainen lähiverkko, IEEE:n standardi 802.3
Exchange	Microsoftin sähköpostipalvelinohjelmisto
FreeBSD	Free Berkeley Software Distribution
GPL	GNU General Public License
Hotspot	Julkinen yleisessä käytössä oleva WLAN-verkko
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPSEC	IP Security Architecture
LAN	Local Area Network
Layer 3	OSI- mallin mukainen 3. välikerros
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NetBSD	Net Berkeley Software Distribution
OpenBSD	Open Berkeley Software Distribution
P2P	Peer-to-Peer Network
PPTP	Point-to-Point Tunneling Protocol
Radius	Remote Authentication Dial In User Service
SDRAM	Synchronous Dynamic Random Access Memory

SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
WAN	Wide Area Network
WEP-salaus	Wired Equivalent Privacy
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
VLAN ID	Virtual Local Area Identifier
VOIP	Voice Over Internet Protocol
WPA2	Wi-Fi Protected Access 2
WPA2-PSK	Wi-Fi Protected Access 2 - Pre-shared key
WPA-PSK	Wi-Fi Protected Access - Pre-shared key
WPA	Wi-Fi Protected Access
VPN	Virtual Private Network
WWW	World Wide Web

1 JOHDANTO

Langattomat verkot ovat yleistyneet nopeasti myös pk-yrityksissä. Monesti pienillä yrityksillä ei ole resursseja tai osaamista toteuttaa langatonta verkkoa tietoturvallisesti. Useimmiten langattomat tukiasemat jätetään oletusasetuksille, jolloin langaton verkko on täysin suojaamaton ulkopuolisia uhkia vastaan. Tukiaseman oletusasetuksia käytettäessä tukiaseman ja tietokoneen välistä liikennettä ei salata mitenkään, jolloin yrityssalaisuudet ovat helposti kolmannen osapuolen kuunneltavissa ja muokattavissa. Monessa yrityksessä langattomat tukiasemat on liitetty yrityksen omaan lähiverkkoon, jolloin suojaamattomasta tukiasemasta pääsee suoraan yrityksen palvelimiin ja tietoihin käsiksi.

Tämän insinööriyön tarkoituksena oli toteuttaa edullisesti tietoturvallinen langaton vierailijaverkko, jonka voisi myös liittää yrityksen olemassa olevaan Internet - yhteyteen tietoturvallisesti. Toteutus on alun perin suunniteltu käytettäväksi Langaton Tampere -verkkoyhteisön kanssa. Työssä tehty toteutus toimii myös pienin muutoksin täysin itsenäisesti ilman Langaton Tampere -verkkoyhteisöä.

Työn idea tuli siitä, kun ei löytynyt tarpeeksi edullista tukiasemaa, jolla olisi voinut toteuttaa molemmat Langattoman Tampereen käyttötavat eli LANGATON-WPA- ja WirelessTampere-käyttötavat. Ongelmaksi osoittautui Captive portal -toiminnallisuuden puuttuminen, joka tarvitaan WirelessTampere-käyttötavan toimintaan. WirelessTampere-käyttötavalla toteutetaan vierailijoiden kirjautuminen Langattomaan Tampereeseen. Kalliimmissa laitteissa, kuten Trapezessa ja Ciscossa toiminnallisuus on, mutta ne maksavat useita tuhansia euroja.

Ratkaisuksi löytynyt toteutus on tehty GPL-lisenssin (*General Public License*) alaisella m0n0wall-palomuuriohjelmistolla, joka toimii sulautetussa Soekris net4501 -tietokoneessa. m0n0walliin pohjautuvan toteutuksen etuina olivat edullinen hankintahinta ominaisuuksiin nähden, palomuuriominaisuudet, Captive Portal - ominaisuus, VPN-yhteydet (*Virtual Private Network*), VLAN-tuki (*Virtual Local Area Network*), mahdollisuus kytkeä useita tukiasemia ja toimivuus lähes kaikkien

markkinoilla olevien tukiasemien kanssa. Nimenomaan erilaisilla tukiasemilla saavutetaan suurimmat hyödyt. Sen kanssa voidaan käyttää ulkotukiasemaa, tehokkaita pitkänkantaman tukiasemia, edullisia kotitukiasemia tai kaikkia näitä yhtä aikaa. Tukiasemia voidaan liittää useita käyttäen tavallista Ethernet-kytkintä palomuurin ja tukiasemien välissä. Tällöin saadaan langattoman verkon peittoaluetta kasvatettua. Toteutus soveltuu todella monenlaisiin ympäristöihin, ja siinä voidaan käyttää hyväksi myös jo olemassa olevia tukiasemia.

Työssä ei perehdytä varsinaiseen WLAN-tekniikkaan (*Wireless Local Area Network*) eikä siinä käytettäviin salauksiin. Seuraavassa luvussa on kuitenkin muutamia turvallisuusnäkökohtia.

Työssä ei myöskään perehdytä siihen, kuinka tukiasemia ja käyttäjiä lisätään Langattoman Tampereen RADIUS-palvelimeen. Siihen on olemassa hyvät ohjeet, jotka saa halutessaan Technopolis Ventures Professia Oy:lta.

2 TURVALLISEN LANGATTOMAN VERKON TOTEUTUKSESTA

Langattoman verkon toteutuksessa on muutamia yksinkertaisia periaatteita, joilla sen turvallisuutta voidaan parantaa. Tähän voidaan käyttää salausta, käyttäjien autentikointia ja tukiaseman lähetystehon oikeaksi säätöä.

Ilman salausta olevaa langatonta verkkoa voi kuunnella todella helposti ja etsiä dataliikenteestä esimerkiksi käyttäjätunnuksia ja salasanoja. Langattomissa tukiasemissa on useita eri salausvaihtoehtoja. WEP-salauksessa (*Wired Equivalent Privacy*) käytetään ennalta määriteltyjä muuttumattomia salausavaimia, joiden pitää olla samat lähettäjällä ja vastaanottajalla. Vanhempi WEP-salaus voidaan murtaa nykyisellä kannettavalla jopa minuuteissa. WEP-salaus ei salaa myöskään kaikkea liikennettä ainoastaan IP-paketin dataosan. MAC-otsikon (*Media Access Control*) tiedot kulkevat salaamattomana. WEP-salausta ei suositella käytettäväksi enää nykyisin, kun tarjolla on vahvempiakin salaustapoja.

WPA-PSK-salauksessa (*Wi-Fi Protected Access – Pre-Shared Key*) käytetään WEP-salauksen tavoin ennalta määriteltyä salausavainta, mutta siinä on korjailtu WEP-salauksen heikkouksia. WPA-PSK salaa kaikki IP-paketin tiedot, ei siis ainoastaan paketin dataosaa. WPA-PSK-salausta on huomattavasti vaikeampi murtaa kuin WEP-salausta, mutta sekin murtuu netistä saatavilla työkaluilla tunneissa tai vuosissa riippuen täysin salausavaimen pituudesta. Alle 14 merkin salausavaimia ei kannattaisi käyttää. Suositeltava pituus on yli 22 merkkiä. WPA-PSK-salaus soveltuu hyvin kotitukiasemiin ja yrityksiin, joissa on vain muutama käyttäjä. WPA-PSK-salauksesta on olemassa uudempi ja vahvempi WPA2-PSK-salaus (*Wi-Fi Protected Access 2 – Pre-Shared Key*), mutta vanhemmat laitteet eivät sitä tue.

WPA-salaus (*Wi-Fi Protected Access*) eroaa WPA-PSK-salauksesta siinä, että jokainen käyttäjä autentikoidaan kirjautumispalvelimella (*RADIUS*) omalla käyttäjätunnuksellaan ja salasanalla. Jos yritys käyttää Active Directorya tai muuta LDAP-hakemistopalvelua (*Lightweight Directory Access Protocol*), niin käyttäjä kirjautuu samoilla tunnuksilla langattomaan verkkoon kuin omalle työasemalleen. Tällöin käyttö helpottuu, kun ei tarvitse muistaa useita eri tunnuksia. Radius-palvelin generoi satunnaisen salausavaimen kirjautumisen yhteydessä. Salausavain myös vaihtuu joka 10 000 paketin välein, jolloin sen selvittäminen on vaikeampaa. WPA-salauksen murtaminen on todella vaikeaa ja aikaa vievää. WPA-salauksesta on olemassa vahvempi WPA2-salaus (*Wi-Fi Protected Access 2*), mutta kaikki nykyisin käytössä olevat laitteet eivät tue sitä.

Salausta kannattaa aina käyttää. Huonompikin salaus on parempi kuin ei salausta lainkaan. WEP-salauskin saattaa toimia psykologisena hidasteena jo sen takia, että sen murtaminen on rikos. Mitä pidempi salausavain, sitä vaikeampi salausta on murtaa, joten kannattaa pyrkiä käyttämään mahdollisimman pitkiä salausavaimia.

Tukiaseman tehonsäätö on myös tärkeä osa tietoturvaa. Mitä kauemmaksi tukiasema kantaa, sitä helpompaa sen kuunteleminen on kolmansille osapuolille. Langattoman verkon toteutuksessa kannattaa lähteä liikkeelle mahdollisimman pienillä lähetystehoilla ja lisätä lähetystehoa vasta, jos verkko ei kanna tarpeeksi pitkälle.

Yritykset haluavat nykyään tarjota vierailijoilleen mahdollisuutta päästä Internetiin, ja langaton verkko on siihen mainio tapa. Kun yritys tarjoaa Internet-yhteyttä vierailijoille, sitä varten on ehdottomasti hankittava oma yhteys tai erotettava langaton verkko palomuurilla yrityksen sisäverkosta. Langaton tukiasema kannattaa muutenkin aina asentaa yritysverkon ulkopuolelle, mieluiten erilliseen vain langattomalle verkolle tarkoitettuun Internet-yhteyteen. Jos tai kun joku murtaa salauksen ja pääsee sisälle langattomaan verkkoon, mahdolliset tuhot rajoittuvat silloin vain murto-osaan siitä, mitä ne voisivat olla, jos langaton verkko olisi yhteydessä yrityksen sisäverkkoon. Kaikkialla verkkojen erottaminen ei kuitenkaan ole aina mahdollista, jolloin avuksi tulee VLAN-tekniikka (*Virtual Local Area Network*). VLAN-tekniikalla voidaan loogisesti erottaa samassa fyysisessä verkossa olevat verkot toisistaan. Käytännössä siis voidaan useampaa LAN-verkkoa siirtää samassa kaapeloinnissa ja ne ovat silti erillään toisistansa.

/1/ /2/ /3/ /4/ /12/ /13/ /17/

3 LANGATON TAMPERE -VERKKOYHTEISÖ

Langaton Tampere on verkkoyhteisö, jonka jäsenet jakavat oman Internet-yhteytensä muiden yhteisön jäsenten käyttöön. Jakamalla oman langattoman tukiaseman ja Internet-yhteyden yhteisön käytettäväksi saa vierailla muiden Langattoman Tampereen jäsenten tukiasemissa. Yhteisön peittoalue kasvaa jatkuvasti uusien jäsenten myötä. Yksityishenkilöille yhteisö on maksuton. Yrityksiltä peritään vuotuinen jäsenmaksu. Langattoman Tampereen käyttö on pyritty tekemään mahdollisimman helpoksi ja tietoturvalliseksi. Tietoturvaan on yhteisössä kiinnitetty erittäin paljon huomiota, siksi kaikkien yritysratkaisujen toimittajien on noudatettava yhteisön antamia asetuksia ja sääntöjä. Langaton Tampere -käyttäjillä on yksilöllinen käyttäjätunnus, jolloin pystytään valvomaan, kuka käyttää ja missä Langattoman Tampereen tukiasemia. Pystytään siis selvittämään, jos joku käyttää tukiasemia rikollisiin tarkoituksiin. Vierailija-käyttäjätunnuksen voi saada Langattomaan Tampereeseen joko tekstiviestillä tai yrityksestä, jossa käyttäjä on vierailemassa. Sama käyttäjätunnus toimii kaikissa Langaton Tampere -tukiasemissa, jolloin

esimerkiksi yrityksen työntekijä voi käyttää töissä, kaupungilla, kahviloissa ja kotonaan samaa käyttäjätunnusta. Käyttö on helppoa, koska kirjautuminen Langattomaan Tampereeseen tehdään joka paikassa samalla tavalla. Langattomassa Tampereessa on kaksi käyttötapaa: suojaamaton WirelessTampere ja yritystason WPA-salausta käyttävä LANGATON-WPA. Kummassakin käyttötavassa suositellaan käytettäväksi VPN-yhteyksiä yrityskäytössä. /5/ /6/

3.1 WirelessTampere-käyttötapa

WirelessTampere on salaamaton, mutta ei kaikille käyttäjille avoin käyttötapa. WirelessTampereen liikennettä ei salata millään tavalla. Se on tarkoitettu vierailijoiden käyttöön, joilla ei ole varsinaista Langaton Tampere -käyttäjätunnusta. WirelessTampere-käyttötavassa vierailija pääsee kirjautumaan WWW-sivun kautta Langattomaan Tampereeseen. Vierailija pääsee WWW-selaimella ainoastaan kirjautumissivulle ja mahdollisesti sen yrityksen kotisivulle, jonka tukiaseman kantoalueella hän on. Muille Internet-sivuille ennen kirjautumista Langattomaan Tampereeseen vierailijalle ei myönnetä pääsyä. Tämän toiminnallisuuden mahdollistaa Captive portal -niminen ominaisuus, jota kutsutaan myös kaappaavaksi WWW-palvelimeksi.

Langattomaan Tampereeseen kuuluvat yritykset voivat antaa vierailijoilleen ilmaiseksi tunnuksia. Vierailijatunnuksille määritellään tekovaiheessa, millä ajalla ne toimivat ja kuinka pitkään ensimmäisestä kirjautumisesta. Vierailijatunnukset siis vanhenevat automaattisesti, jolloin niitä ei pääse myöhemmin käyttämään väärin. Ensimmäisellä kirjautumisella käyttäjätunnus lukittuu WLAN-sovittimen MAC-osoitteeseen (*Media Access Control Address*), minkä jälkeen sama vierailijatunnus ei toimi kuin kyseisessä tietokoneessa tai älypuhelimessa. /5/ /6/

3.2 LANGATON-WPA-käyttötapa

LANGATON-WPA on tarkoitettu Langattoman Tampereen pääasialliseksi käyttötavaksi. Siinä liikenne salataan WPA-salauksella, jolloin dataliikenteen salakuuntelu on huomattavasti hankalampaa kuin WirelessTampere-käyttötavassa. LANGATON-WPA vaatii tietokoneelle tai älypuhelimelle sertifikaatin ja asetusten määrittämisen, joten sen käyttöönotto ei ole niin yksinkertaista kuin WirelessTampere-käyttötavan. Se siis soveltuu Langatonta Tamperetta päivittäin käytäville paremmin kuin satunnaisille vierailijoille. /5/ /6/

4 SOEKRI NET4501

Soekris net4501 on pienikokoinen sulautettu pc, joka on suunniteltu monipuoliseen kommunikointilaitteikäyttöön, kuten palomuri- ja VPN-reititin käyttöön. Laitteiston piirilevy on suunniteltu vähävirtaiseksi ja pitkäikäiseksi. Piirilevy on fyysisiltä mitoiltaan vain 12,32 cm X 14,48 cm, joten se mahtuu pieneenkin koteloon. Kuvassa 1 on piirilevy, jossa CompactFlash-kortti on paikallaan.



Kuva 1. Soekris net4501 -piirilevy

Soekris net4501 on suunniteltu FreeBSD-, NetBSD-, OpenBSD- ja Linux-käyttöjärjestelmiä varten, mutta se pystyy ajamaan useimpia muitakin reaaliaikaisia käyttöjärjestelmiä. Laite perustuu 133 MHz AMD ElanSC520 -suorittimeen, joka toimii x86-käskykannalla. Laitteessa on 3 kpl 10/100 Mb/s Ethernet-liitäntöjä,

sarjaportti ja 16...64 MB SDRAM-muistia (*Synchronous Dynamic Random Access Memory*) juotettuna piirilevyille. Laitteessa on käyttöjärjestelmää ja ohjelmia varten CompactFlash-muistikorttisovitin, joka pystyy käsittelemään muistikortteja jopa 4GB:n asti. /7/

5 MONOWALL

m0n0wall on täysin WWW-selaimella hallittava GPL-lisenssin alainen Manuel Kasperin kehittämä palomuuriohjelmisto, joka on suunniteltu Soekris net4501:n kaltaisille sulautetuille laitteille. Käyttöjärjestelmänä on FreeBSD. Soekris net4501 -laitteistossa m0n0wall käynnistyy käyttökuntoon 40 sekunnissa ja pystyy 17Mbps läpimenoon WAN-liitännästä (*Wide Area Network*) LAN-liitäntään. m0n0wallin versio 1.233 vie käyttöjärjestelmiseen ainoastaan 6 MB muistia CompactFlash-kortilta. m0n0wall on erittäin monipuolinen ohjelmisto, jonka ominaisuuksia ovat mm. tilallinen pakettisuodatus, VPN-yhteydet IPSEC (*IP Security Architecture*) ja PPTP (*Point-to-Point Tunneling Protocol*), NAT (*Network Address Translation*), 802.1q-yhteensopiva VLAN-tuki ja useimmista kaupallisista ratkaisuista puuttuva Captive portal -ominaisuus. m0n0wallilla pystyy korvaamaan kaupallisen palomuurin pk-yrityskäytössä.

m0n0wallilla on mahdollista toteuttaa kummatkin Langaton Tampere -käyttötavat tukiasemilla, jotka tukevat vain yhtä SSID-tunnusta (*Service Set Identifier*). Käytännössä tarvitaan oma tukiasema kummallekin käyttötavalle eli minimissään kaksi tukiasemaa. Toteutus voidaan myös tehdä yritystason tukiasemalla, joka tukee useampaa SSID:tä ja VLANia, jolloin molemmat käyttötavat voidaan toteuttaa käyttämällä yhtä tukiasemaa. /8/ /9/

6 CAPTIVE PORTAL

Captive portal eli kaappaava WWW-palvelin estää kaikki TCP/IP-paketit riippumatta osoitteesta tai portista, kunnes käyttäjä avaa WWW-selaimen, silloin Captive portal pakottaa käyttäjän WWW-selaimen aina Captive portal -kirjautumissivulle riippumatta siitä, minne URL-osoitteeseen (*Uniform Resource Locator*) käyttäjä haluaisi mennä. Vasta kun käyttäjän autentikointi on suoritettu onnistuneesti, avataan käyttäjälle vapaa pääsy Internetiin.

Captive portal toiminnallisuudelle ei ole väliä, onko käytettävä yhteys langaton vai kaapeloitu. Captive portal -kirjautumissivu voi sijaita missä tahansa Internetissä tai reitittimen sisällä olevassa WWW-palvelimessa. m0n0wallissa kirjautumissivu ja siihen tarvittava WWW-palvelin sijaitsevat laitteessa. Captive portaliin voidaan myös sallia WWW-sivuja, joihin käyttäjä pääsee ilman autentikointia. Yleensä sallitaan sen yrityksen kotisivu, jonka langaton hotspot on kyseessä.

Captive portalin voi toteuttaa monella tavalla, kuten http-uudelleenohjauksella, IP-uudelleenohjauksella tai DNS-uudelleenohjauksella. Kaikki mainitut toteutustavat toimivat samalla periaatteella kirjautumisen jälkeen. Käyttäjän tietokoneen tai älypuhelimien MAC-osoite ja IP-osoite (*Internet Protocol address*) tallennetaan palomuriin, ja sallitaan tälle laitteelle pääsy Internetiin. Tässä toimintatavassa on havaittu haavoittuvuus, silloin kun käytössä ei ole salausta, joka salaisi myös MAC-otsikkotiedot. Yksinkertaisella pakettinuuskijalla on mahdollista saada selville autentikoidun tietokoneen IP-osoite ja MAC-osoite. Molemmat voidaan väärentää autentikoimattomalle tietokoneelle, jolloin palomuri luulee tietokonetta autentikoiduksi. Haavoittuvuutta on erittäin vaikea korjata ja väärinkäyttöä havaita. m0n0wallin Captive portaliin pystyy tekemään autentikointiin aikakatkaisumäärityksen, jolla autentikointi vanhenee määritetyn ajan jälkeen ja käyttäjä kirjataan ulos verkosta. Tämän jälkeen mahdollinen MAC- ja IP-osoitteen väärentäjä ei pääse käyttämään tukiasemaa kyseisen ajan jälkeen ilman käyttäjätunnuksia. Luvussa 7.3 on kerrottu, kuinka kyseinen asetus saadaan kytkettyä päälle. /10/

6.1 HTTP-uudelleenohjaus

HTTP-uudelleenohjaus toimii seuraavasti: Kun autentikoimaton käyttäjä yrittää avata WWW-sivua, niin käyttäjän WWW-selain tekee DNS-pyyntö (Domain Name System) ja IP-osoitteen selvitys tehdään niin kuin normaalisti. Tämän jälkeen selain lähettää HTTP-pyyntö (Hypertext Transfer Protocol) selvitettyyn IP-osoitteeseen. Tämä pyyntö pysähtyy palomuriin. Palomuri vastaa HTTP-vastauksella, joka sisältää HTTP-tilakoodin 302. Se kertoo WWW-selaimelle, että sivu on siirretty väliaikaisesti toiselle palvelimelle eli Captive portalin WWW-palvelimelle. Näin käyttäjän WWW-selain ohjataan Captive portalin kirjautumissivulle joka kerta, kun hän yrittää avata jonkun muun kuin kirjautumissivun. /10/ /11/

6.2 IP-uudelleenohjaus

Käyttäjän liikenne voidaan ohjata Captive portal -kirjautumissivulle myös käyttäen IP-uudelleenohjausta layer 3 -tasolla. Tämä ei ole suositeltu toteutustapa, koska käyttäjälle tarjottu WWW-sivun sisältö ei vastaa URL-osoitetta. /10/ /14/

6.3 DNS-uudelleenohjaus

Kun autentikoimattoman käyttäjän WWW-selain tekee DNS-pyyntö, palomuri vastaa aivan kaikkiin DNS-pyyntöihin antamalla Captive portal -kirjautumissivun IP-osoitteen. Palomuurin pitää varmistaa, että se ohjaa kaikki autentikoimattomien käyttäjien DNS-pyyntöt vain yhdelle DNS-palvelimelle, jonka DHCP-palvelin (Dynamic Host Configuration Protocol) on julkaissut. Yleensä käytetään palomuurin sisäistä DNS-palvelinta. Jossain DNS-uudelleenohjaustoteutuksissa ei ole estetty DNS-pyyntöjä ulospäin käyttäjiltä. Tällöin Captive portal -kirjautumissivu on helppo ohittaa määrittämällä tietokone käyttämään jotain toista DNS-palvelinta. Palomuri täytyy siis määrittää ehdottomasti niin, ettei se salli liikennettä ulkoisiin DNS-palvelimiin, ennen kuin käyttäjä on autentikoitu. /10/

6.4 Captive portal -kirjautumissivu

Kirjautumissivu on HTML-kielellä (*Hypertext Markup Language*) toteutettu WWW-sivu. Kuvassa 2 näkyy esimerkki Langattoman Tampereen WirelessTampere-käyttötavan kirjautumissivusta. Liitteessä 1 on tämän sivun HTML-koodi.

WizIT

LANGATON TAMPERE

Tervetuloa!

Tämä on WizIT Oy:n Langattoman Tampereen tukiasema. Pystyt kirjautumaan siihen käyttämällä Langattoman Tampereen tunnustasi.

Voit vaihtoehtoisesti pyytää tässä tukiasemassa toimivan vierastunnuksen isännältäsi tai tilata tekstiviestillä kaikkialla Langattomassa Tampereessa toimivan vierastunnuksen.

Welcome!

This is The WizIT Oy's Wireless Tampere access point. You can now login by using your Wireless Tampere account.

You can also request a visitor account for this access point from your host or buy a Wireless Tampere visitor account with an SMS.

Tunnus/Username:

Salasana/Password:

WizIT Oy:n sivut uuteen ikkunaan [tästä](#).

Vierastunnuksen tilaaminen tekstiviestillä

Lähetä vierastunnuksen käyttötärpeen mukainen tilauskoodi tekstiviestillä numeroon **16130** (Toimii Elisa, Saunalahti, Sonera, Tele-Finland ja DNA matkapuhelimissa). Saat vastausviestissä vierastunnuksen ja salasanan, jotka toimivat missä tahansa Langattoman Tampereen tukiasemassa

Aikaraja määrittelee tunnuksen voimassaoloajan tunteina ensimmäisestä kirjautumisesta

How to order a guest account with a text message

Send the order code in a text message to **16130** (works with following carriers: Elisa, Saunalahti, Sonera, Tele-Finland and DNA). You'll receive a guest account and password in the return message. The guest account works with any Wireless Tampere access point.

Time Limit specifies the expiration time for your guest account in hours from your first login.

Tämän Langaton Tampere toteutuksen toimitti [WizIT Oy](#)

WizIT

YHTEISTYÖSSÄ MUKANA

GoGo

LIIKUNTAKESKUS PARK • CITY

Luova Tampere

Pirkanmaan Yrittäjät

Tampereen KAUPPAKAMARI

Tampereen kaupunki

Arch-Red

Tupa

Professia

Kuva 2. Langaton Tampereen kirjautumissivu

Kirjautumissivu voi olla lähes minkäläinen tahansa. Esimerkiksi kahvila tai ravintola voi kirjautumissivulla julkaista viikon lounaslistan tai päivän tarjouksia. Ainoat tarvittavat asiat kirjautumissivulla ovat joko käyttäjätunnuksen ja salasanan kysely tai vaihtoehtoisesti esimerkiksi verkon käyttöehdot ja niiden hyväksymispainike.

7. M0N0WALLIN KONFIGUROINTI

Konfiguroidaan liitteen 2 mukainen Langaton Tampere -verkko. Verkko toteutetaan tukiasemilla, jotka tukevat yhtä SSID-tunnusta. Verkkoon tulee siis 3 kpl LANGATON-WPA-tukiasemia ja 3 kpl WirelessTampere-tukiasemia.

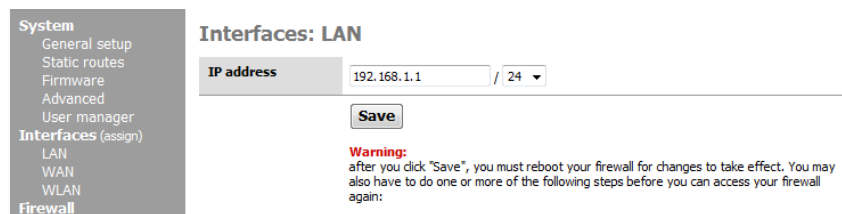


Kuva 3. m0n0wallin hallintasivu

m0n0wallin konfiguroidaan tavallisella PC-tietokoneella, jossa on WWW-selain. Konfigurointi aloitetaan kytkemällä PC-tietokone m0n0wallin eth0- eli LAN-liitännänsä. m0n0wallissa on oletuksena DHCP-palvelin päällä, mikä antaa tietokoneelle IP-osoitteen 192.168.1.1/24-alueelta. WWW-selaimen annetaan osoitteeksi m0n0wallin IP-osoite <http://192.168.1.1> ja kirjaudutaan administrator-tunnuksilla hallintasivulle. Kuvassa 3 on m0n0wallin hallintasivun näkymä. /8/ /9/

7.1 IP-osoitteiden asetukset

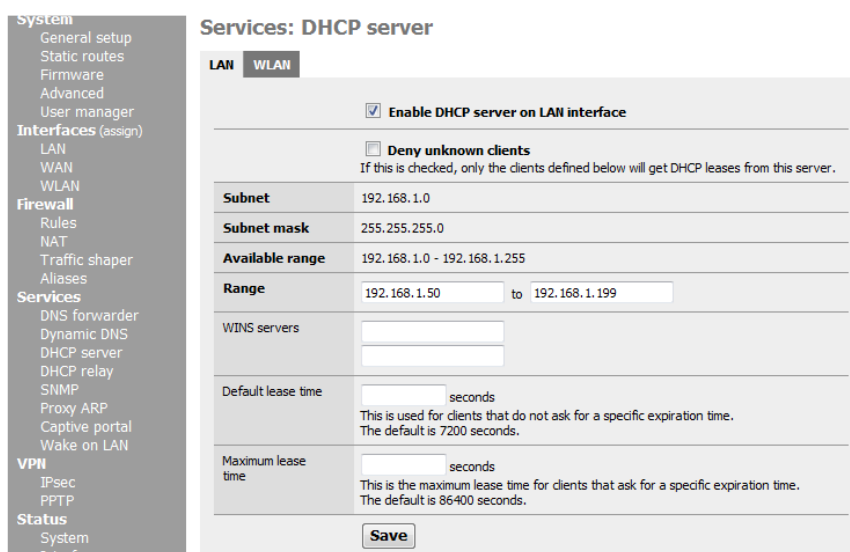
Verkon konfigurointi aloitetaan Ethernet-liitännöiden IP-osoitteista. Niiden asetukset tehdään hallintasivun Interfaces-kohdassa. m0n0wallin eth0-liitäntä määritellään LAN-liitännäksi, jonka IP-osoite on 192.168.1.1/24. Kuvassa 4 näkyvät LAN-liitännän IP-osoitteen asetukset. Eth1-liitäntä määritellään WAN-liitännäksi, joka saa IP-osoitteen operaattorin DHCP-palvelimelta. Eth2-liitäntä määritellään WLAN-portiksi, jonka IP-osoite on 192.168.2.1/24.



The screenshot shows the 'Interfaces: LAN' configuration page in the m0n0wall web interface. On the left is a navigation menu with categories: System, Interfaces (assign), Firewall, and Services. Under 'Interfaces (assign)', 'LAN' is selected. The main content area shows the 'IP address' field set to '192.168.1.1' and a dropdown menu set to '24'. Below the field is a 'Save' button. A red warning message reads: 'Warning: after you click "Save", you must reboot your firewall for changes to take effect. You may also have to do one or more of the following steps before you can access your firewall again:'

Kuva 4. LAN-liitännän IP-asetukset

Seuraavaksi kytketään päälle m0n0wallin DHCP-palvelin ja tehdään sen määriytykset. Ne tehdään Services/DHCP Server -kohdassa. Määritellään DHCP-palvelin päälle LAN- ja WLAN-liitäntöihin. DHCP-alue kannattaa tässä tapauksessa määrittellä mahdollisimman isoksi, koska kiinteille IP-osoitteille ei ole tarvetta. Kuvassa 5 näkyvät LAN-liitännän DHCP-asetukset. /8/ /9/



The screenshot shows the 'Services: DHCP server' configuration page in the m0n0wall web interface. The 'LAN' tab is selected. The 'Enable DHCP server on LAN interface' checkbox is checked. Below it is the 'Deny unknown clients' checkbox, which is unchecked. The 'Subnet' is 192.168.1.0, 'Subnet mask' is 255.255.255.0, and 'Available range' is 192.168.1.0 - 192.168.1.255. The 'Range' is set to 192.168.1.50 to 192.168.1.199. The 'WINS servers' field is empty. The 'Default lease time' is 7200 seconds and the 'Maximum lease time' is 86400 seconds. A 'Save' button is at the bottom.

Kuva 5. LAN-liitännän DHCP-palvelimen asetukset

7.2 Palomuurisäännöt

Palomuurisäännöt ovat tärkeä osa turvallista verkkoinfrastruktuuria. Niiden konfigurointiin kannattaa panostaa ja miettiä etukäteen, mitä halutaan estää ja mitä sallia. Väärillä asetuksilla voi saada lukittua itsensä ulos m0n0wallin hallintasivulta, toisaalta liian löysillä asetuksilla langattoman verkon käyttäjien yksityisyys ja tiedot vaarantuvat.

WLAN-liitännän on tarkoitus kytkeä WirelessTampere-käyttötapaa käyttäviä tukiasemia, joten kannattaa estää WLAN-liitännästä pääsy m0n0wallin hallintasivulle. Sama sääntö toimii myös ilman Langatonta Tamperetta, jos WLAN-liitännän kytketään yrityksen vierailijoille tarkoitettu avoin tukiasema. On mahdollista estää myös hallintasivulle pääsy LAN-liitännästä ja määritellä VPN-yhteys, jolla on oma virtuaalinen IP-verkko, josta on pääsy hallintasivulle. Tässä tapauksessa se ei ole tarpeellista, koska palomuuuri tukiasemineen on ajateltu kytkettäväksi täysin omassa ADSL-yhteydessä.

Nykyisen roskapostiongelman vuoksi on hyvä estää myös SMTP-portin eli TCP/IP-portin 25 käyttö LAN- ja WLAN-liitännöistä. SMTP-portin estämisestä ei ole nykyisin normaalille sähköpostin käytölle haittaa, varsinkaan Langaton Tampere -käytössä, koska Internet-operaattorit estävät nykyisin kaikkien muiden SMTP-palvelimien käytön paitsi heidän omansa. Tavallinen Langaton Tampere -käyttäjä ei tiedä, minkä operaattorin Internet-yhteys on käytössä. SMTP-portin estäminen ei estä sähköpostin lähettämistä, jos käytössä on WWW-pohjainen sähköposti, Exchange, SSL- tai TLS-salaus.

NetBIOS-porttien liikenne kannattaa myös estää, kun ei tiedetä, käyttävätkö mahdolliset rikolliset langatonta verkkoa. Internetistä ilmaiseksi saatavilla ja jopa käyttöjärjestelmän omilla työkaluilla voidaan urkkia muiden samaa tukiasemaa käyttävien NetBIOS-tiedoista esimerkiksi toimialue, työryhmä, tietokoneen nimi ja käyttäjätunnus. Näillä tiedoilla voidaan päästä esimerkiksi huonosti suojatun tietokoneen tietoihin käsiksi. Mahdollisesti urkittuja tietoja voidaan käyttää hyväksi

suuremmissa hyökkäyksessä käyttäjän yritystä vastaan. NetBIOS-liikenne käyttää TCP/IP-portteja 135, 137, 138, 139 ja 445. /9/ /12/

Firewall: Rules

LAN	WAN	PPTP VPN	WLAN			
Proto	Source	Port	Destination	Port	Description	
<input checked="" type="checkbox"/>	TCP	LAN net	*	*	135	NetBIOS block
<input checked="" type="checkbox"/>	TCP	LAN net	*	*	137 - 139	NetBIOS block
<input checked="" type="checkbox"/>	TCP	LAN net	*	*	445	NetBIOS block
<input checked="" type="checkbox"/>	TCP	LAN net	*	*	25 (SMTP)	SMTP block
<input checked="" type="checkbox"/>	*	LAN net	*	! WLAN net	*	LAN -> kaikki muut paitsi WLAN

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Kuva 6. LAN-liitännän palomuurisäännöt

Kuvassa 6 näkyvät LAN-liitännän palomuurisäännöt, joilla on estetty NetBIOS-portit, SMTP-portti ja liikenne LAN-liitännästä WLAN-liitännään. Kuvassa 7 on vastaavat palomuurisäännöt WLAN-liitännälle. /9/

Firewall: Rules

LAN	WAN	PPTP VPN	WLAN			
Proto	Source	Port	Destination	Port	Description	
<input checked="" type="checkbox"/>	TCP	WLAN net	*	*	135	NetBIOS block
<input checked="" type="checkbox"/>	TCP	WLAN net	*	*	137 - 139	NetBIOS block
<input checked="" type="checkbox"/>	TCP	WLAN net	*	*	445	NetBIOS block
<input checked="" type="checkbox"/>	TCP	WLAN net	*	*	25 (SMTP)	SMTP block
<input checked="" type="checkbox"/>	TCP	WLAN net	*	WLAN net	80 (HTTP)	WLAN->web admin block
<input checked="" type="checkbox"/>	*	WLAN net	*	! LAN net	*	WLAN -> kaikki muut paitsi lan

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Kuva 7. WLAN-liitännän palomuurisäännöt

7.3 Captive portal -konfigurointi

Captive portalin asetukset tehdään Services/Captive Portal -kohdassa. Kuvassa 8 on ensimmäiset Captive portal -asetukset Langattomaan Tampereeseen. Ensimmäiseksi valitaan Ethernet-liitäntä, johon Captive portal halutaan käyttöön. Tässä tapauksessa siis WLAN.

Seuraavaksi määritellään maximum concurrent connections -asetus eli määritellään, kuinka monta yhtäaikaista kirjautumista sallitaan Captive portal -palvelimeen. Tämä asetus ei rajoita kirjautuneiden käyttäjien lukumäärää, vaan ainoastaan, kuinka monta voi kirjautua yhtäaikaisesti. Oletusasetukset ovat ihan hyvät eli neljä yhtäaikaista kirjautumista per IP-osoite, ja kirjautumisia sallitaan yhtä aikaa yhteensä 16 kpl.

The screenshot displays the 'Services: Captive portal' configuration page. On the left is a navigation menu with categories like System, Interfaces, Firewall, Services, VPN, and Status. The main area is titled 'Services: Captive portal' and contains several tabs: 'Captive Portal', 'Pass-through MAC', 'Allowed IP addresses', 'Users', and 'File Manager'. The 'Captive Portal' tab is active, showing the following settings:

- Enable captive portal:**
- Interface:** WLAN (dropdown menu). Below it: 'Choose which interface to run the captive portal on.'
- Maximum concurrent connections:** 4 per client IP address (0 = no limit), 16 total. Below it: 'This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.'
- Idle timeout:** 30 minutes. Below it: 'Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.'
- Hard timeout:** 180 minutes. Below it: 'Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).'
- Logout popup window:** **Enable logout popup window**. Below it: 'If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.'
- Redirection URL:** http://www.wizit.fi. Below it: 'If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.'
- Concurrent user logins:** **Disable concurrent logins**. Below it: 'If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.'
- MAC filtering:** **Disable MAC filtering**. Below it: 'If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between m0n0wall and the clients).'
- Per-user bandwidth restriction:** **Enable per-user bandwidth restriction**. Below it: 'Default download 204 Kbit/s, Default upload 102 Kbit/s'. Below that: 'If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit. You will need to enable the traffic shaper for this to be effective.'

Kuva 8. Captive portal -asetukset Langattomaan Tampereeseen

Sitten määritellään aikakatkaisuasetukset: Idle timeout on aika, jolloin ei ole ollut dataliikennettä käyttäjän tietokoneen ja tukiaseman välillä. Tällöin siis voidaan olettaa, että käyttäjä on kadonnut tukiaseman kantoalueelta tai lopettanut yhteyden käytön, joten hänet voidaan kirjata ulos Captive portal -palvelimesta. Tässä tapauksessa käytetään arvoa 30 minuuttia.

Luvussa 6 kerrottiin Captive portalin toteutuksen haavoittuvuudesta, jolla on mahdollista esiintyä toisena käyttäjänä ja tietokoneena. Hard timeout -aikakatkaisulla saadaan pienennettyä haavoittuvuuden hyväksikäyttömahdollisuuksia. Hard timeout on aika, jolloin käyttäjä kirjataan ulos verkosta siitä riippumatta, onko tukiaseman ja käyttäjän tietokoneen välillä dataliikennettä. Käyttäjä pystyy kirjautumaan heti uudestaan Captive portaliin, joten asetuksen ainoa haittapuoli on käyttäjätunnuksen ja salasanan uudelleen kirjoittaminen tietyin välein. Tässä tapauksessa käytetään arvoa 180 minuuttia.

Logout popup window on asetusta, jolla määritellään, avaako Captive portal -sivusto kirjautuneen käyttäjän WWW-selaimeen popup-ikkunan, jossa on kirjautu ulos -nappi. Älypuhelimien WWW-selaimissa popup-ikkunat toimivat huonosti, joten asetusta ei kannata ottaa käyttöön.

Redirection URL -asetuksella voidaan käyttäjä ohjata kirjautumisen jälkeen esimerkiksi yrityksen WWW-sivulle. Tässä tapauksessa käyttäjä ohjataan <http://www.wizit.fi>-sivulle.

Concurrent user logins -asetuksella voidaan estää käyttäjän kirjautuminen samoilla käyttäjätunnuksilla useammalla tietokoneella. Tämä toiminto on jo Langattoman Tampereen Radius-palvelimessa, joten Langaton Tampere -käytössä asetusta ei tarvita.

MAC filtering -asetuksella estetään MAC-osoitteen tarkistus, jolloin Captive portal ei tarkasta, pysyväkö käyttäjän MAC-osoite samana. Asetusta tarvitaan, jos m0n0wallin ja käyttäjän välillä on reitittimiä. Tässä tapauksessa asetusta ei tarvita.

Per-user bandwidth restriction -asetuksella määritellään maksimisiirtokapasiteetti yksittäiselle käyttäjälle. Sillä voidaan estää se, että yksittäinen käyttäjä tukkisi Internet-yhteyden esimerkiksi lataamalla isoja tiedostoja. Se siis kannattaa ottaa käyttöön varsinkin julkisissa paikoissa, joissa on useita käyttäjiä. Asetuksen arvo riippuu käytössä olevasta Internet-yhteydestä. Esimerkiksi Langaton Tampere -käytössä olisi ADSL-yhteys, jonka nopeus on 1024/512 kbit/s. Oletetaan, että kummallakin käyttötavalla on yhtäaikaista käyttäjiä maksimissaan 10 kpl. Koska yksittäinen käyttäjä ei kuitenkaan käytä kaikkea siirtokapasiteettia jatkuvasti vaan yleensä hetkellisesti, niin liikenteen rajoittaminen viidesosaan riittää takaamaan kaikille tarpeeksi siirtokapasiteettia, mutta ei estä esimerkiksi VOIP-puheluiden käyttöä. Eli siksi default download -arvoksi 204 kbit/s ja default upload -arvoksi 102 kbit/s. Tämä asetus koskee siis vain Captive portal -käyttäjiä eli WirelessTampere-käyttäjiä. LANGATON-WPA-käyttötapaan asetuksella ei ole vaikutusta. Per-user bandwidth restriction -asetus vaatii m0n0wallin Traffic shaperin -toiminnallisuuden käyttöä toimiakseen. Traffic shaper -ominaisuudella voidaan rajoittaa myös esimerkiksi P2P -ohjelmien ja LANGATON-WPA-käyttötavan siirtokapasiteettia. Traffic shaper -ominaisuus kytketään päälle Firewall / Traffic Shaper -kohdasta.

Authentication kohdassa valitaan RADIUS authentication. Primary RADIUS -palvelimen IP-osoitteeksi määritellään Langattoman Tampereen RADIUS-palvelimen osoitteen eli 81.90.66.38 ja portiksi 1812. Shared secret eli jaettu salaisuus on salausavain, jota käytetään Captive portalin ja RADIUKSEN väliseen liikenteeseen. Siihen kohtaan kirjoitetaan siis mahdollisimman pitkä ja monimutkainen salausavain, jota halutaan käyttää. Kuvassa 9 on Langattoman Tampereen RADIUS-asetukset.

Langattomassa Tampereessa on hyvä käyttää tilastointia, joten send RADIUS accounting packets -ominaisuus otetaan käyttöön ja sen portti on 1812.

The screenshot shows a configuration page for RADIUS authentication and accounting. The 'Authentication' section has three radio buttons: 'No authentication', 'Local user manager', and 'RADIUS authentication' (which is selected). Below this are sections for 'Primary RADIUS server' and 'Secondary RADIUS server', each with fields for IP address, Port, and Shared secret. The 'Accounting' section has a checked checkbox for 'send RADIUS accounting packets' and an 'Accounting port' field set to 1813. The 'RADIUS options' section has a checked checkbox for 'Use RADIUS Session-Timeout attributes', a 'Type' dropdown set to 'default', and a 'MAC address format' dropdown set to 'unformatted'. The MAC address format section includes a list of options: default (00:11:22:33:44:55), singledash (001122-334455), ietf (00-11-22-33-44-55), cisco (0011.2233.4455), and unformatted (001122334455).

Kuva 9 Langattoman Tampereen RADIUS-asetukset

RADIUS options -kohdassa on asetus Use RADIUS Session-Timeout attributes, joka sallii RADIUS-palvelimelta tulevat aikakatkaisuasetukset. Ilman tätä asetusta Langattoman Tampereen vierastunnusten vanheneminen ei toimi oikein, joten se laitetaan päälle. MAC address format -asetuksella määritellään, missä muodossa RADIUS-palvelin ymmärtää MAC-osoitteet. Langaton Tampere -käytössä sen on oltava unformatted.

Portal page contents -kohdassa Captive portal -palvelimeen ladataan kirjautumissivu HTML-muodossa. Liitteessä 1 on kirjautumissivun HTML-koodista esimerkki.

Authentication error page contents -kohdassa voidaan ladata HTML-sivu, joka näytetään jos kirjautumisen yhteydessä tapahtuu virhe tai käyttäjätunnus ja salasana ovat väärin. Jos kirjautumissivulle halutaan kuvia, niin kuvat voidaan joko laittaa palvelimelle Internetiin tai ladata kuvat m0n0walliin. Kuvien lataus m0n0walliin tapahtuu Services/Captive portal/File manager -kohdasta.

Captive portal ei voi toimia oikein, ennen kuin liikenne sallitaan Langattoman Tampereen RADIUS-palvelimelle ennen kirjautumista. Ilman liikenteen sallimista RADIUS-palvelimelle käyttäjä ei pysty kirjautumaan Langattomaan Tampereeseen ollenkaan. Liikenne kannattaa sallia myös kaikkiin kirjautumissivun linkeihin, kuten yrityksen omaan WWW-sivuun ja Langaton Tampere -sivustolle. Muuten käyttäjä joutuu linkeistä aina takaisin kirjautumissivulle.

Kuvassa 10 näkyy sallitut IP-osoitteet. /6/ /9/

The screenshot shows the m0n0wall webGUI Configuration interface. The main content area is titled "Services: Captive portal: Allowed IP Addresses". There are tabs for "Captive Portal", "Pass-through MAC", "Allowed IP addresses", "Users", and "File Manager". The "Allowed IP addresses" tab is active, displaying a table with the following data:

IP address	Description	
any → 193.111.93.117	Langaton Tampere	⊕ ⊗
any → 193.111.93.118	Langaton Tampere	⊕ ⊗
any → 193.111.93.119	www.langatontampere.fi	⊕ ⊗
any → 62.142.11.2	www.wizit.fi	⊕ ⊗
81.90.66.38 → any	LangatonTampere RADIUS	⊕ ⊗
any → 81.90.66.38	LangatonTampere Radius	⊕ ⊗
any → 81.90.66.39	www.langatonyritys.fi	⊕ ⊗

Below the table, there is a "Note:" section:

Note:
Adding allowed IP addresses will allow IP access to/from these addresses through the captive portal without being taken to the portal page. This can be used for a web server serving images for the portal page or a DNS server on another network, for example. By specifying *from* addresses, it may be used to always allow pass-through access from a client behind the captive portal.

any → x.x.x.x All connections **to** the IP address are allowed
x.x.x.x → any All connections **from** the IP address are allowed

The footer of the page reads: "m0n0wall © is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]"

Kuva 10. Sallitut IP-osoitteet ennen kirjautumista Langattomaan Tampereeseen

8 TUKIASEMIEN KONFIGUROINTI

Tässä luvussa esitetään edullisen perustukiaseman konfigurointi ja kahden erilaisen yritystason tukiaseman konfigurointi Langattomaan Tampereeseen. Toteutusta varten testattiin useita tukiasemia ja jokainen niistä konfiguroidaan hieman erilailla, joten näillä ohjeilla voidaan selvittää todella monen erilaisen tukiaseman konfiguroinnista. Luvussa kerrotaan myös, millä tavalla tukiasemat eroavat toisistaan. Useimmat muutkin tukiasemat konfiguroidaan samantyyppisellä logiikalla. Kaikki asetukset perustuvat luvussa 7 tehtyihin m0n0wallin asetuksiin.

Tukiasemien konfigurointi aloitetaan samalla tavalla kuin m0n0wallin konfigurointi. Ensin kytketään tukiasema PC-tietokoneen Ethernet-porttiin ja kirjoitetaan WWW-selaimen tukiaseman valmistajan antama IP-osoite ja kirjaututaan hallintasivulle sisään. Tukiasemien kohdalla ei hallintasivulle pääsyä käsitellä tämän tarkemmin, koska se kerrotaan tukiasemien mukana tulevissa ohjeissa.

8.1 Perustukiasema Linksys WAP54G

Perustukiasemaksi valittiin Linksys WAP54G:n, joka on kuvassa 11. Tukiaseman hintaluokka on noin 50 € - 100 €. Tukiasema tukee 802.11g standardia, WPA-salausta ja on WWW-selaimella hallittava.

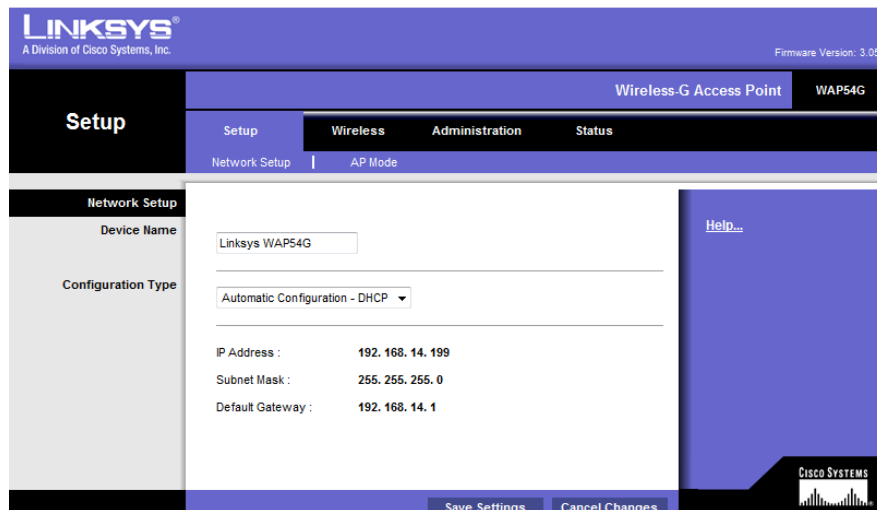


Kuva 11. Linksys WAP54G

Yhdellä tällaisella perustukiasemalla ei voida toteuttaa täydellistä Langaton Tampere -toteutusta, koska se osaa lähettää vain yhtä SSID-nimeä, vaan tarvitaan kaksi tukiasemaa, joista toinen konfiguroidaan LANGATON-WPA- ja toinen WirelessTampere-käyttötapaan. /15/

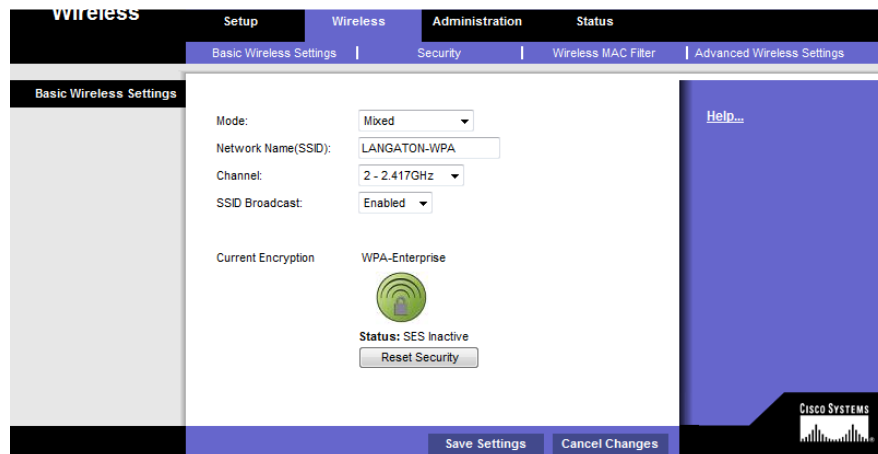
8.1.1 Linksys WAP54G:n konfigurointi LANGATON-WPA-käyttötapaan

Linksys konfiguroidaan Langaton-WPA-käyttötapaan seuraavasti: Ensimmäiseksi määritellään Setup-välilehdeltä tukiasema noutamaan IP-osoitteensa DHCP-palvelimelta. Kuvassa 12 on ruutukaappaus IP-asetuksista.



Kuva 12. Linksys WAP54G:n IP-asetukset

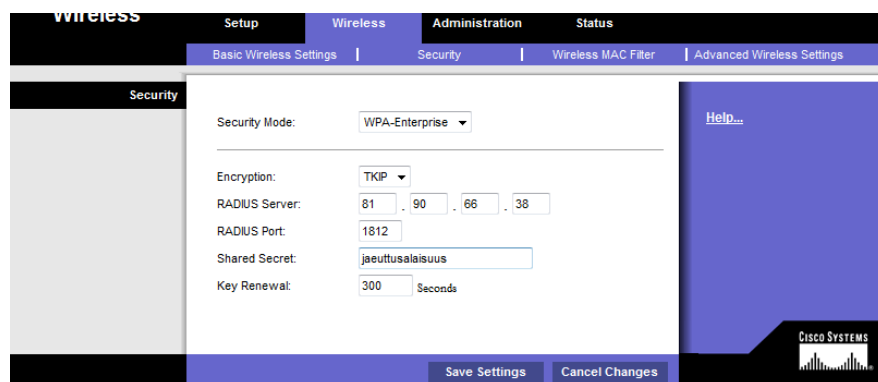
Seuraavaksi määritellään Wireless-välilehdelle SSID-nimi ja kanava. Ennen kanavan valintaa on hyvä tarkistaa vapaana olevat kanavat esimerkiksi kannettavalla tietokoneella tai spektrianalysointorilla. Kuvassa 13 näkyvät Wireless-välilehden asetukset.



Kuva 13. Linksys WAP54G:n Wireless-välilehden asetukset

Seuraavaksi määritellään salausasetukset Wireless/Security-välilehdellä. Security Mode:ksi valitaan WPA-Enterprise. Encryption:ksi TKIP. RADIUS Server -kohtaan kirjoitetaan Langattoman Tampereen RADIUS-palvelimen IP-osoite. RADIUS portiksi määritellään 1812. Shared Secret on oma valintainen salausavain, jonka oltava sama kuin RADIUS-palvelimeen määritelty aivan kuten m0n0wall:ssakin luvussa 7.3. Kuvassa 14 on ruutukaappaus salausasetuksista.

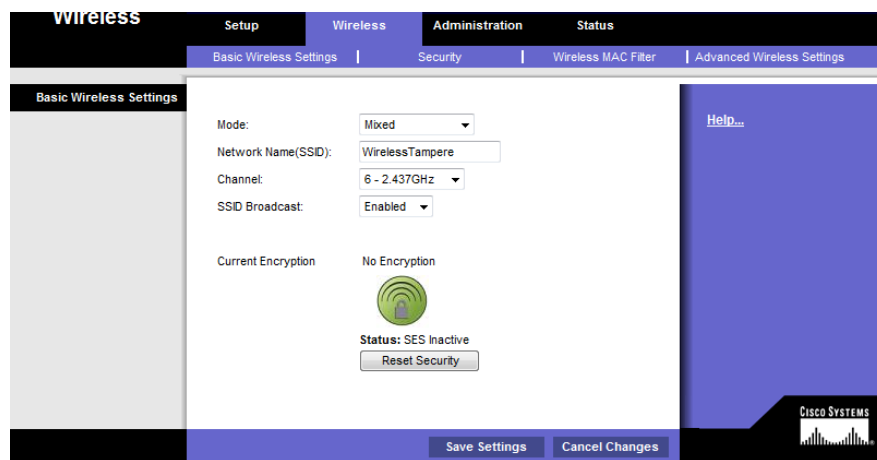
/6/ /15/



Kuva 14. Linksys WAP54G:n salausasetukset

8.1.2 Linksys WAP54G:n konfigurointi WirelessTampere-käyttötapaan

WirelessTampere-käyttötapaan tarvitsee määritellä vain IP-asetuksista DHCP-palvelin päälle, kuten LANGATON-WPA-käyttötavassakin, SSID-nimi ja kanava. Security Mode:ksi valitaan no encryption. Kuvassa 15 WirelessTampereen-asetukset. /6/ /15/



Kuva 15. Linksys WAP54G:n WirelessTampere asetukset

8.2 Yritystason tukiasemat

Yritystason tukiasemiksi valittiin Zyxel NWA-3500 ja Ruckus 2925. Ne eroavat ominaisuuksiltaan huomattavasti perustukiasemista. Molempien hinnat ovat luokkaa 250 € - 300 €. Molemmat tukiasemat tukevat useita SSID-nimiä, VLAN-verkkoja ja niissä on huomattavasti tietoturvaa parantavia ominaisuuksia.

8.2.1 Ruckus 2925

Ruckus 2925 on suunniteltu erityisesti hotspot- ja yrityskäyttöön. Se tukee neljää eri SSID-nimeä ja siinä on neljä Ethernet-liitäntää. Antennijärjestelmä on patentoitu ratkaisu ja siinä on kuusi pientä erillistä antennia, joista muodostuu täysi ympyrä.

Jokaisen antennin tehoa säädellään yksitellen automaattisesti sen mukaan, minkä antennin kantoalueella käyttäjä on. Antenniratkaisulla voidaan tuottaa jopa 64 erilaista suuntakuviota. Ruckusissa on erikoinen ratkaisu turvallisuuden parantamiseksi, ettei WWW-hallintasivulle pääse jos laitteen WAN-liitäntä on kytketty. Oman VLAN-tuen ja usean Ethernet-liitännän takia tukiaseman saa toimimaan m0n0wallin kanssa helposti. Kuvassa 16 on Ruckusin liitännät ja ulkonäkö. Käytännössä Ruckusin kanssa toimivat täysin samat asetukset kuin perustukiasemien kanssa. Liitteessä 3 on konfigurointiesimerkin verkkokaavio.

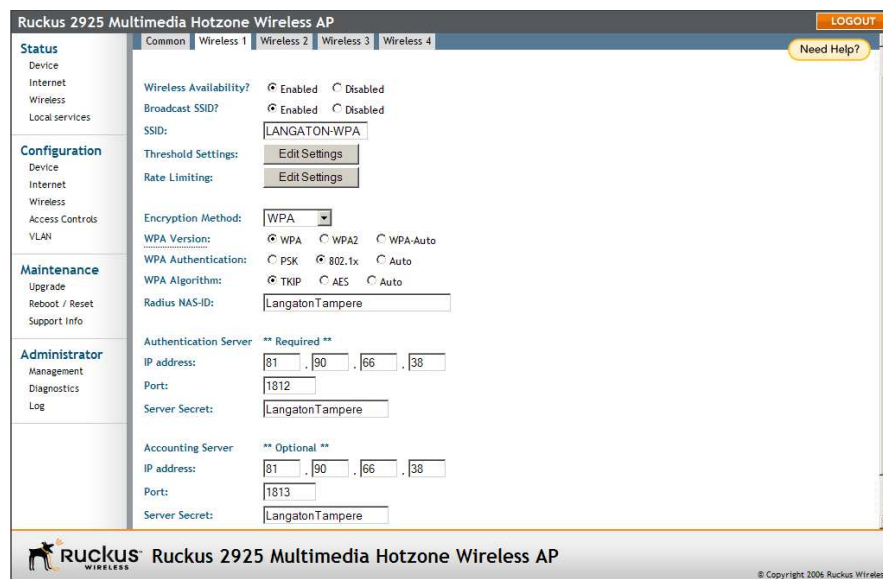


Kuva 16. Ruckus 2925 liitännät ja ulkonäkö

Tukiasema konguroidaan niin, että Ethernet-liitäntään 1 kytketään m0n0wallin WLAN-liitäntä eli WirelessTampere-käyttötapa. Ethernet-liitäntään 5 kytketään m0n0wallin LAN-liitäntä eli LANGATON-WPA-käyttötapa. Ruckusin hallintasivulla mennään Configuration/Wireless/Wireless 1 -välilehdelle, määritellään SSID-nimeksi LANGATON-WPA, salaustavaksi WPA, autentikointitavaksi 802.1x, salausalgoritmiksi TKIP, Langattoman Tampereen RADIUS-palvelimen IP-osoite ja Server secret -kohtaan oma vapaavalintainen jaettu salaisuus-salausavain eli shared secret -salausavain.

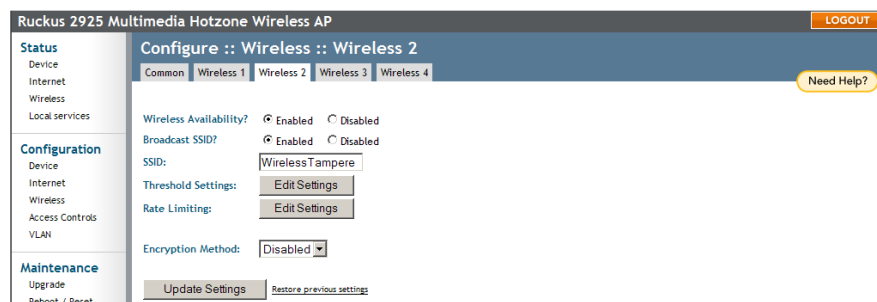
Ongelmaksi Ruckusin konfiguroinnissa muodostui Radius NAS-ID -määrittäminen, jota ilman laite ei suostunut tallentamaan asetuksia. Edes Langattoman Tampereen hallintaorganisaatio Technopolis Ventures Professia Oy ei ollut törmännyt kyseiseen

asetukseen aikaisemmin. Ruckusin käyttöohje eikä Internet auttanut selvittämään, mitä arvoa siinä kysytään. Useiden arvojen, nimien, MAC-osoitteiden ja IP-osoitteiden kokeilun jälkeen tukiasema alkoi toimia Langattomassa Tampereessa. Radius NAS-ID -kohtaan pitää laittaa sama jaettu salaisuus -salaisuus kuin Server secret -kohtaan. Kuvassa 17 on Ruckusin LANGATON-WPA SSID-nimen asetukset.



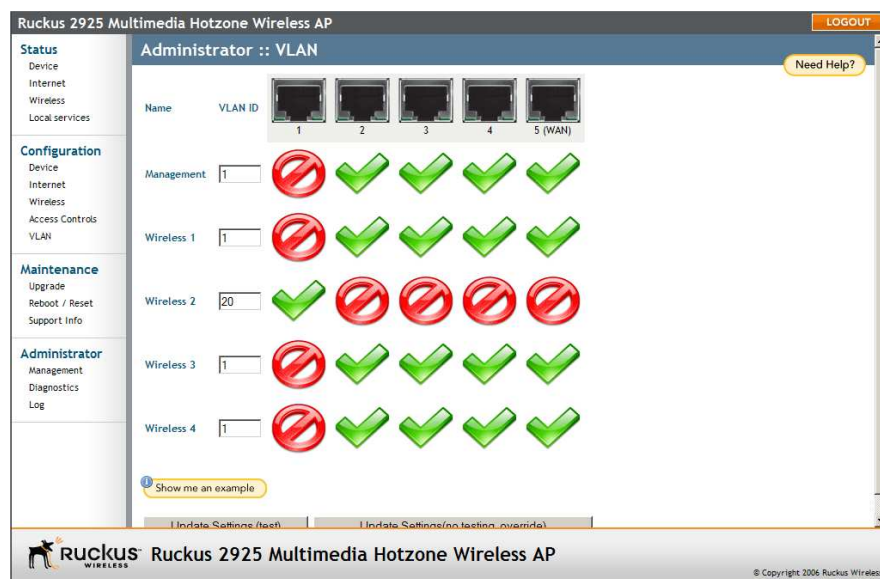
Kuva 17. Ruckus 2925 asetukset LANGATON-WPA SSID-nimelle

Seuraavaksi konfiguroidaan WirelessTampere SSID-nimen asetukset. Ne tehdään Wireless 2 -välilehdellä. Määritellään SSID-nimeksi WirelessTampere ja salaus jätetään Disabled-tilaan. Kuvassa 18 on ruutukaappaus asetuksista. Wireless 3- ja Wireless 4-välilehdillä käydään kytkemässä niiden SSID-nimet pois päältä ja laitetaan rasti Wireless Availability, Disabled kohtaan.



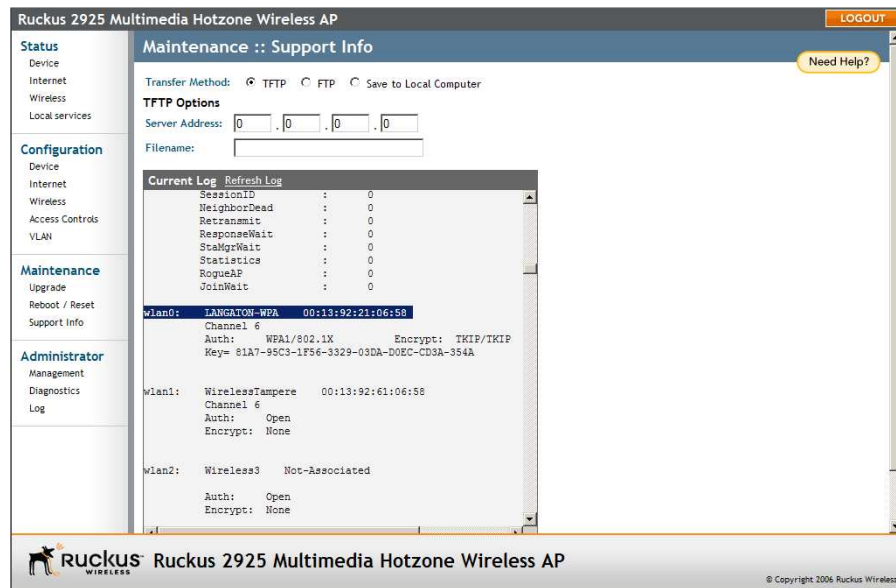
Kuva 18. Ruckus 2925 asetukset WirelessTampere SSID-nimelle

Vielä on määrittämättä Ruckus:n Ethernet-liitännät, joiden asetuksiin pääsee Configuration/VLAN-kohdasta. Wireless 2 SSID-nimelle määritellään VLAN ID, se voi olla mikä tahansa luku 1-4096 väliltä, kunhan se ei ole käytössä jo ennestään samassa verkossa. Esimerkissä VLAN ID:ksi määritetään 20 ja liitetään kyseinen VLAN fyysiseen Ethernet-liitäntään 1. Kuvassa 19 on VLAN-asetukset. Muita määrittämiä ei tarvitse tehdä. Ruckus osaa oletuksena jopa vaihtaa WLAN-kanavan automaattisesti häiriöttömämpään tai vapaana olevaan kanavaan.



Kuva 19. Ruckus 2925 VLAN-asetukset

Seuraavaksi kytketään tukiasema kiinni m0n0wallin ja määritellään Langaton Tampere RADIUS-palvelimeen tukiaseman MAC-osoite. Yleensä tukiasemien MAC-osoite lukee laitteen pohjassa, mutta Ruckusissa kyseinen MAC-osoite on Ethernet-liitäntöjen osoite, eikä langattoman tukiaseman MAC-osoite. Langaton Tampere RADIUS-palvelin saa käyttäjien kirjautumisen yhteydessä langattoman MAC-osoitteen, joten se täytyy vielä selvittää. Se tapahtuu hallintasivun Maintenance / Support info -kohdasta löytyvästä logista. Logista pitää etsiä SSID-nimeä vastaava rivi, jonka vieressä lukee MAC-osoite. Kuvassa 20 on ruutukaappaus logista, jossa SSID-nimi ja MAC-osoite on sinisellä. /6/ /18/



Kuva 20. Ruckusin langattoman MAC-osoitteen selvitys

8.2.2 Zyxel NWA-3500

Zyxel NWA-3500:ssa on kaksi erillistä radiolähetintä, tuki 16 eri SSID-nimelle ja erittäin monipuoliset ominaisuudet. Tukiaseman ulkonäkö näkyy kuvassa 21.

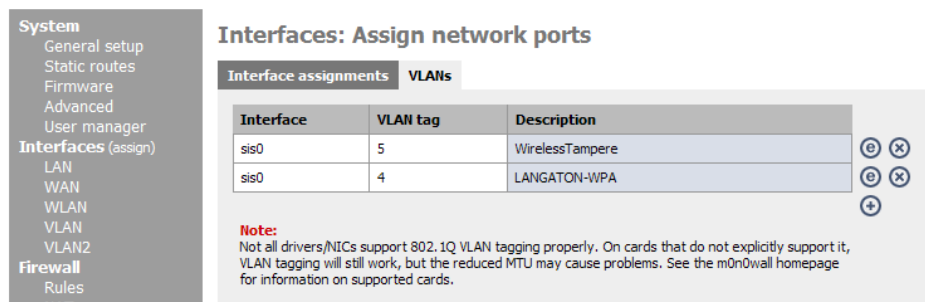


Kuva 21. Zyxel NWA-3500

NWA-3500:sta voi hallita WWW-selaimella ja suoraan sarjaportilla konsolista. Tukiasemassa on vain yksi Ethernet-liitäntä, joten käytetään VLANia erottamaan WirelessTampere- ja LANGATON-WPA-käyttötavat eri verkkoihin. Erottaminen on tehtävä, ettei Captive portal -ominaisuus haittaisi LANGATON-WPA-käyttöä ja

toimisi ainoastaan WirelessTampere-käyttötavassa. Liitteessä 4 on esimerkki konfiguraation verkkokaavio.

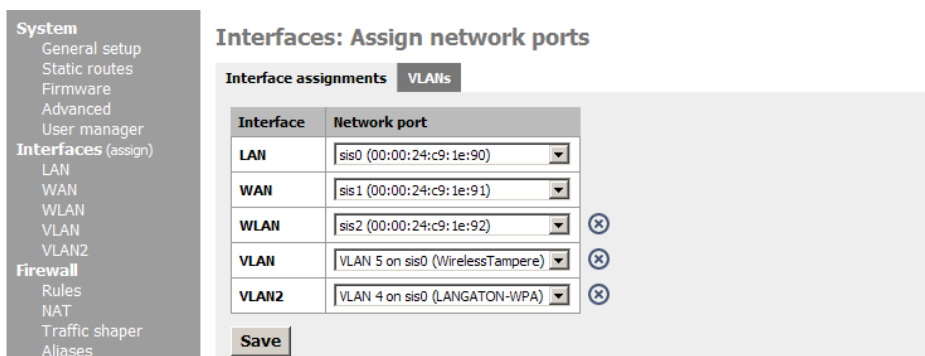
Aikaisemmin tehtyihin m0n0wallin asetuksiin täytyy tehdä lisämäärytyksiä, että pystytään käyttämään VLAN-ominaisuutta. Aloitetaan VLAN-asetuksilla, jotka tehdään Interfaces/assign-valikossa. Lisätään eth0-liitäntään VLAN-tagit 4 ja 5. Kuvassa 22 ovat valmiit asetukset.



Kuva 22. m0n0wall:n VLAN-tag asetukset.

Seuraavaksi määritellään virtuaaliverkkoon kaksi liitäntää VLAN ja VLAN2.

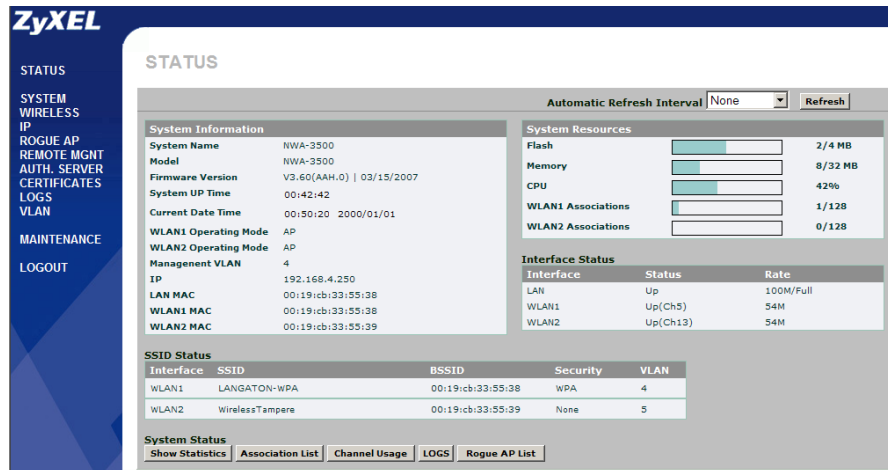
Kuvassa 23 näkyvät valmiit VLAN-liitännät. Sitten VLAN-liitännöille kytketään DHCP-palvelin päälle, tehdään palomuurin asetukset ja kytketään Captive portal päälle VLAN-liitäntään. Näiden määrittelyjen tekeminen käytiin jo luvussa 7.3.



Kuva 23. m0n0wallin VLAN-liitännät

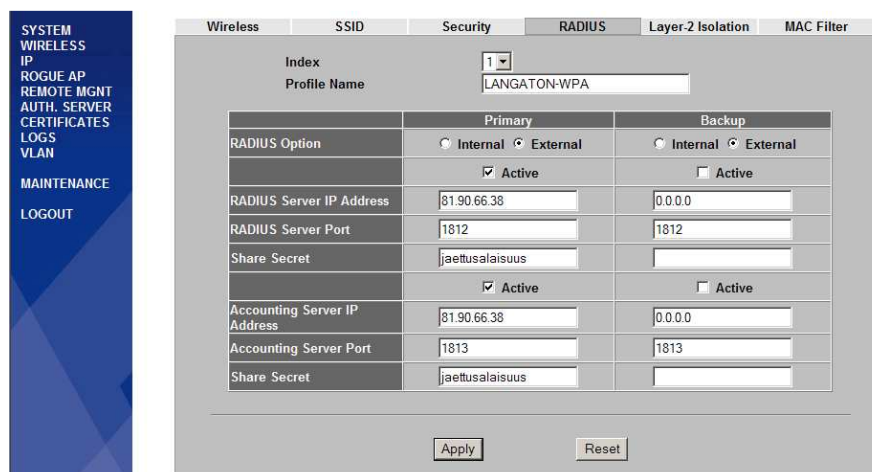
Seuraavaksi konfiguroidaan NWA-3500 tukiasema, jonka hallintasivu näkyy kuvassa 24. Konfigurointi aloitetaan Radius-palvelimen ja salausasetusten määrittämisellä,

koska käytössä on kaksi eri SSID-nimeä, joudumme tekemään asetukset kumpaankin SSID-nimeen erikseen.



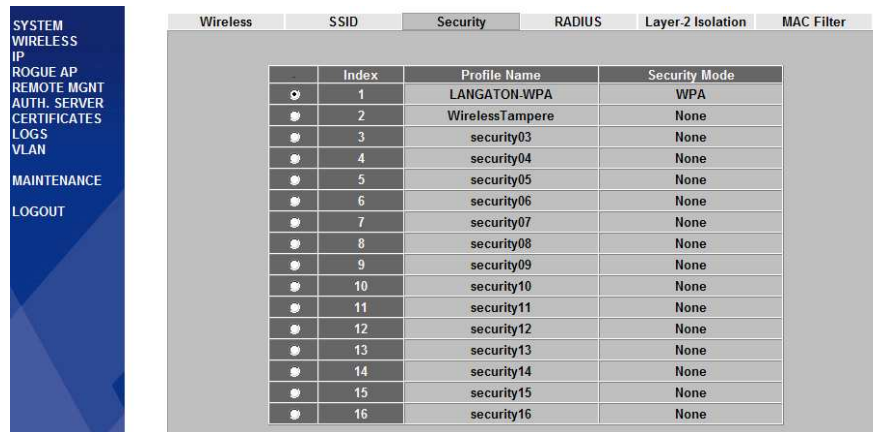
Kuva 24. Zyxel NWA-3500 hallintasisi

Hallintasisivulla mennään WIRELESS-valikon RADIUS-välilehdelle, jossa tehdään Langattoman Tampereen RADIUS-palvelimen määrittelyt, jotka näkyvät kuvassa 25.



Kuva 25. Zyxel NWA-3500 RADIUS-asetukset

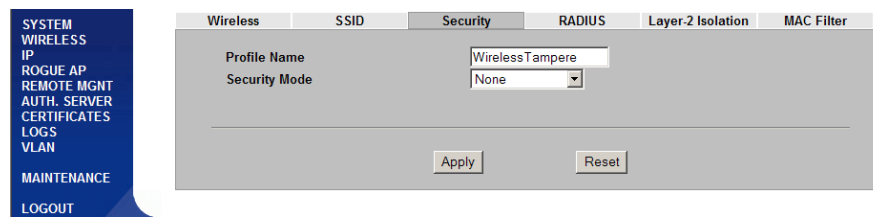
Security-välilehdellä määritellään salausasetukset SSID-nimikohtaisesti, kuten kuvassa 26 näkyy. Sen jälkeen määritellään WirelessTampere-käyttötavan salausasetukset, jotka ovat kuvassa 27. LANGATON-WPA-käyttötavan salausasetukset ovat kuvassa 28.



The screenshot shows the 'Security' tab of a wireless configuration interface. It features a table with 16 rows, each representing a security profile. The columns are 'Index', 'Profile Name', and 'Security Mode'. The first row is selected, showing 'LANGATON-WPA' and 'WPA'. The other rows have 'None' as the security mode.

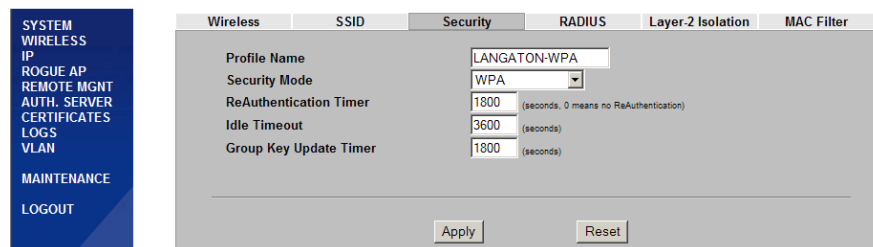
Index	Profile Name	Security Mode
1	LANGATON-WPA	WPA
2	WirelessTampere	None
3	security03	None
4	security04	None
5	security05	None
6	security06	None
7	security07	None
8	security08	None
9	security09	None
10	security10	None
11	security11	None
12	security12	None
13	security13	None
14	security14	None
15	security15	None
16	security16	None

Kuva 26. Salausasetukset SSID-nimikohtaisesti



The screenshot shows the configuration page for the 'WirelessTampere' profile. The 'Profile Name' field is set to 'WirelessTampere' and the 'Security Mode' dropdown is set to 'None'. There are 'Apply' and 'Reset' buttons at the bottom.

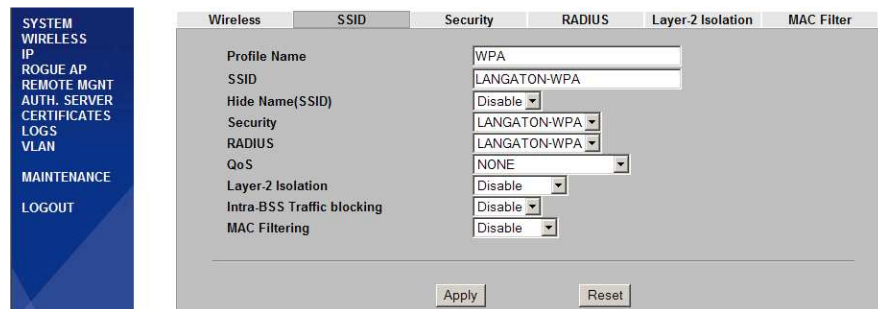
Kuva 27. WirelessTampere-käyttötavan salausasetukset



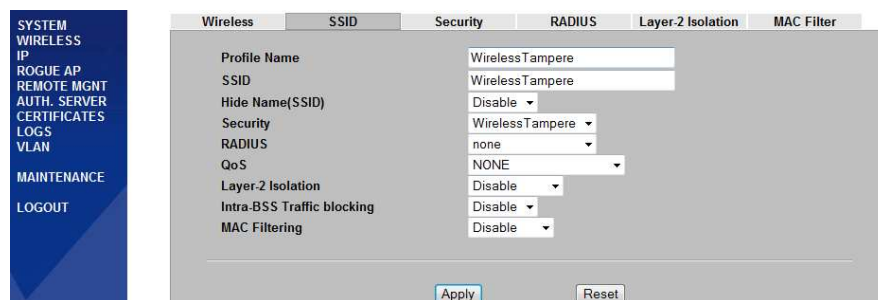
The screenshot shows the configuration page for the 'LANGATON-WPA' profile. The 'Profile Name' field is set to 'LANGATON-WPA' and the 'Security Mode' dropdown is set to 'WPA'. Below the dropdown, there are three fields: 'ReAuthentication Timer' (1800 seconds), 'Idle Timeout' (3600 seconds), and 'Group Key Update Timer' (1800 seconds). There are 'Apply' and 'Reset' buttons at the bottom.

Kuva 28. LANGATON-WPA-käyttötavan salausasetukset

Seuraavaksi SSID-välilehdeltä määritellään SSID-nimi ja asetukset mitkä siinä ovat käytössä. Valitaan aikaisemmin tehdyt Security- ja RADIUS-asetukset. Kuvassa 29 on asetukset LANGATON-WPA-käyttötapaan. Asetukset WirelessTampere-käyttötapaan tehdään samalla logiikalla, kuten kuvassa 30 näkyy.



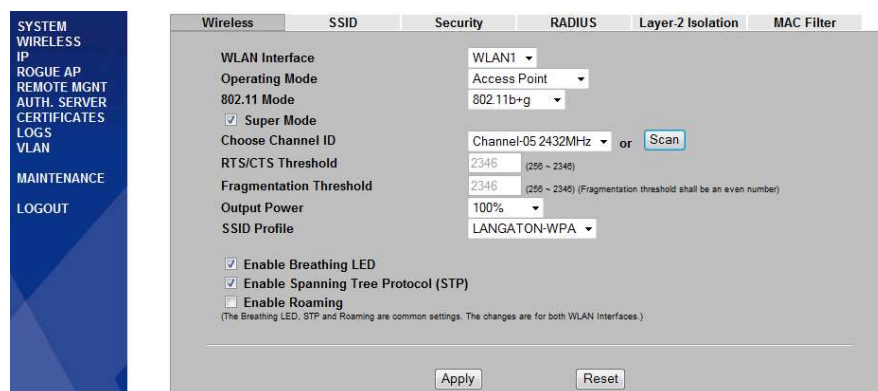
Kuva 29. SSID-asetukset LANGATON-WPA-käyttötapaan



Kuva 30. SSID-asetukset WirelessTampere-käyttötapaan

Zyxelissä on kaksi radiota WLAN1 ja WLAN2. Wireless-välilehdellä valitaan mitä SSID-profiilia kukin radio lähettää, millä kanavalla ja kuinka suurella teholla.

Kuvassa 31 on WLAN1 radio määritelty lähettämään LANGATON-WPA SSID-profiilia. WLAN2 radion ja WirelessTampere SSID-profiilin asetukset tehdään samalla logiikalla.



Kuva 31. WLAN1-radio määriteltyä LANGATON-WPA SSID-profiilille

Viimeisenä kytketään VLAN-ominaisuus päälle, se tehdään VLAN-valikossa. Määritellään LANGATON-WPA:n VLAN ID:ksi 4 ja WirelessTampereen VLAN ID:ksi 5. Management VLAN ID:ksi määritellään 4, sama kuin LANGATON-WPA:ssa, jos Management VLAN ID:n konfiguroi väärin ei pääse enää WWW-hallintasivulle, silloin joudutaan käyttämään konsolia sarjaportilla. /6/ /9/ /16/ /17/

9 VIERAILIJAVERKKO ILMAN LANGATON TAMPERE -VERKKOYHTEISÖÄ

Tässä insinööriyössä esitelty toteutus toimii myös ilman Langaton Tampere -verkkoyhteisöä. Kaikki tässä työssä esitetyt konfiguraatiot ja esimerkit toimivat lähes sellaisenaan, jos yrityksellä on ennestään jokin hakemistopalvelu käytössä kuten Active Directory, jolloin RADIUS-palvelimen asennus sen yhteyteen on melko yksinkertainen operaatio. Ainoastaan RADIUS-palvelimen IP-osoite vaihtuu yrityksen oman RADIUS-palvelimen IP-osoitteeksi. M0n0wall sisältää myös oman käyttäjähakemiston, jota voidaan käyttää Captive portal -ominaisuudessa. Silloin ei määritellä Captive portal -asetuksiin RADIUS-palvelimen tietoja ollenkaan, vaan määritellään käyttäjät Captive portalin Users-välilehdellä. Se on erittäin kätevä ominaisuus jos yrityksen on tarkoitus jakaa sama käyttäjätunnus ja salasana kaikille vierailijoille. Eri käyttäjätunnusten ja salasanojen teko on myös mahdollista, mutta niiden hallinta tulee hankalaksi silloin kun käyttäjätunnuksia on useita.

10 YHTEENVETO

Työssä esitettyjen kolmen tukiaseman lisäksi testattiin ja konfiguroitiin monia muita tukiasemia. Langaton Tampere -verkkoyhteisöön kehitettiin oma yhteisötukiasema sillä aikaa kun tätä työtä tehtiin, joka on huomattavasti edullisempi kuin tässä työssä esitelty ratkaisu, mutta yhteisötukiaseman ominaisuudet ja muokattavuus erilaisiin ympäristöihin eivät ole lähelläkään samaa tasoa.

Työtä tehdessä ongelmia tuli VLAN-verkkojen konfiguroinnissa, lähinnä puutteellisten m0n0wallin ohjeiden vuoksi.

Yritystukiasemien konfigurointi osoittautui hankalammaksi kuin kuviteltiin aluksi. Vaikeudet johtuivat lähinnä erilaisista termeistä ja WWW-hallintasivujen toimintalogiikasta.

Työ onnistui jopa paremmin kuin oli ajateltu, varsinkin VLAN-ominaisuuksien osalta. Työssä esitelty toteutus on ollut kirjoitushetkellä noin puoli vuotta useiden eri yritysten käytössä. Sinä aikana se on osoittautunut erittäin luotettavaksi ja toimivaksi myös erilaisten kannettavien ja älypuhelimien kanssa. Toteutuksessa itsessään ei ole esiintynyt minkäänlaisia ongelmia puolen vuoden aikana.

LÄHTEET

Painetut lähteet

1. Tuominen Toni: WLAN tietoturva. Tutkintotyö. Tampereen ammattikorkeakoulu. Tietotekniikka. Tampere 2005. 42 s. + 1 liites.

Painamattomat lähteet

2. Wireless broadband guide.[WWW-sivu]. [viitattu 4.5.2008] Saatavissa: <http://www.broadband.co.uk/wireless-broadband.jsp>
3. Wi-Fi Protected Access.[WWW-sivu]. [viitattu 4.5.2008] Saatavissa: http://www.wi-fi.org/white_papers/whitepaper-042903-wpa/
4. Intercepting Mobile Communications.[WWW-sivu]. [viitattu 4.5.2008] Saatavissa: <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>
5. Kari, Vääränen, Projektipäällikkö. Tapahtuma 15.5.2007. Technopolis Ventures Professia Oy
6. Kari, Vääränen, Langaton_Tampere_yritystukiaseman_asennusohje[PDF] 26.11.2007
7. net4501.[WWW-sivu]. [viitattu 4.2.2008] Saatavissa: <http://www.soekris.com/net4501.htm>
8. m0n0wall – facts.[WWW-sivu]. [viitattu 4.2.2008] Saatavissa: <http://m0n0.ch/wall/facts.php>
9. m0n0wall Handbook.[WWW-sivu]. [viitattu 4.2.2008] Saatavissa: <http://doc.m0n0.ch/handbook/>
10. Wikipedia.[WWW-sivu]. [viitattu 15.3.2008] Saatavissa: http://en.wikipedia.org/wiki/Captive_portal
11. Status Code Definitions.[WWW-sivu]. [viitattu 15.3.2008] Saatavissa: <http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>
12. Savio, Lau.[WWW-sivu]. [viitattu 15.3.2008] Saatavissa:

http://www.ensc.sfu.ca/~ljilja/cnl/presentations/savio/wlan_sec_savio_edited.pdf

13. Wikipedia.[WWW-sivu]. [viitattu 25.3.2008] Saatavissa:

http://en.wikipedia.org/wiki/Wireless_LAN

14. What is OSI model?.[WWW-sivu]. [viitattu 4.5.2008] Saatavissa:

<http://www.tech-faq.com/osi-model.shtml>

15. Linksys WAP54G User's Guide.[WWW-sivu]. [viitattu 25.3.2008]
Saatavissa:

<ftp://ftp.linksys.com/international/userguides/wap54gv2-eu-ug.pdf>

16. NWA-3500 User's Guide.[WWW-sivu]. [viitattu 25.3.2008] Saatavissa:

http://www.zyxel.com/DownloadLibrary_ShortName/NWA-3500/user_guide/NWA-3500_3.60.pdf

17. VLAN information.[WWW-sivu]. [viitattu 25.3.2008] Saatavissa:

<http://net21.ucdavis.edu/newvlan.htm>

18. Ruckus 2925 User Guide.[WWW-sivu]. [viitattu 4.5.2008] Saatavissa:

<http://support.ruckuswireless.com/documents/44>

LIITTEET

Liite 1.	Kirjautumissivun HTML-koodi	2 sivua
Liite 2.	Toteutuksen verkkokaavio perustukiasemalla	1 sivu
Liite 3.	Toteutuksen verkkokaavio Ruckus 2925 tukiasemalla	1 sivu
Liite 4.	Toteutuksen verkkokaavio Zyxel NWA-3500 tukiasemalla	1 sivu

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>

<title>WizIT Oy - Wireless Tampere Web Login</title>
<style type="text/css">

body {
  font-family: Verdana, Arial, Helvetica, sans-serif;
  font-size: 11px;
  color: #000000;}
td {
  font-family: Verdana, Arial, Helvetica, sans-serif;
  font-size: 11px;
  color: #000000;}
h3 {
  font-family: Verdana, Arial, Helvetica, sans-serif;
  color: #000000;
  font-size: 14px; }
#frame {
  width:800px;
  margin-top:5px;
  text-align:left;}
#top {
  float: left;
  width: 800px;}
#main {
  float: left;
  width: 605px;
  padding: 5px;
  margin:5px;}
#rightcontent {
  float: right;
  width: 150px;
  padding: 5px;
  margin: 2px;
  border: 1px solid #CCCCCC;}
#bottomcontent {
  float: top;
  width: 605px;
  padding: 0px;
  margin: 5px;}
#rightcontent p {
  font-size:10px;}
#leftcontent a {
  font-size:12px;
  line-height:2;}
h1 {
  font-size:large;}
</style></head>

<body>
<div id="frame">
<div id="top">
<a href="http://www.wizit.fi"></a>
<a href="http://www.langatontampere.fi"></a>
</div>

<div id="top">
<hr />
</div>

<div id="main">
<h3>Tervetuloa!</h3>
<p>Tämä on WizIT Oy:n Langattoman Tampereen tukiasema. Pystyt kirjautumaan siihen käyttämällä Langattoman Tampereen tunnustasi.</p>
<p>Voit vaihtoehtoisesti pyytää tässä tukiasemassa toimivan vierastunnuksen isännältäsi tai tilata tekstiviestillä kaikkialla Langattomassa Tampereessa toimivan vierastunnuksen.</p>

<h3>Welcome!</h3>
<p>This is WizIT's Wireless Tampere access point. You can now login by using your Wireless Tampere account.</p>
<p>You can also request a visitor account for this access point from your host or buy a Wireless Tampere visitor account with an SMS.</p>

<form method="post" action="$PORTAL_ACTION$">
<table border="0" cellpadding="3" align="center">
<tr>

```

```
<td align="right">Tunnus/Username:</td>
<td><input type="text" name="auth_user" value="" maxlength="79" size="15" /></td>
</tr>
<tr>
<td align="right">Salasana/Password:</td>
<td><input type="password" name="auth_pass" value="" maxlength="32" size="15" /></td>
</tr>
<tr>
<td colspan="2" align="right">
<input name="accept" type="submit" value=" Kirjaudu/Login " />
</td>
</tr>
</table>
</form>
<p>WizIT Oy:n sivut uuteen ikkunaan <a href="http://www.wizit.fi" target="_blank">tästä</a>.
</div>

<div id="rightcontent">
<!-- ÄLÄ MUUTA TÄTÄ -->
<iframe src="http://www.langatonyritys.fi/weblogin/sivu.html" width="150" height="720" scrolling="no" name="Sivupalkki"
frameborder="0">
</iframe>
<!-- END - ÄLÄ MUUTA TÄTÄ -->
</div>
<div id="bottomcontent">
<!-- ÄLÄ MUUTA TÄTÄ -->
<hr />
<iframe src="http://www.langatonyritys.fi/weblogin/ala.html" width="605" height="300" name="Alapalkki" frameborder="0">
</iframe>
<!-- END - ÄLÄ MUUTA TÄTÄ -->

<br/>
<br/>
Tämän Langaton Tampere toteutuksen toimitti <a href="http://www.wizit.fi" target="_blank">WizIT Oy</a></a>
<a href="http://www.wizit.fi"></a>
</p>
</div>
</div></body></html>
```

