LAUREA

# Langattoman verkon suunnittelu ja toteutus yrityskäyttöön

Haka-Taivalmäki, Juha

2011 Leppävaara

**Laurea-ammattikorkeakoulu**
**Laurea Leppävaara**

# Langattoman verkon suunnittelu ja asennus yrityskäyttöön

Haka-Taivalmäki, Juha
Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Maaliskuu, 2011

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Haka-Taivalmäki, Juha

**Langattoman verkon suunnittelu ja asennus yrityskäyttöön**

Vuosi 2011 Sivumäärä 49

Tämän työn tavoitteena on esitellä langattomiin verkkoihin liittyvää teoriaa ja yhdenlainen langattoman verkon ratkaisu. Ratkaisussa käytetään Trapezen järjestelmää ja siinä on huomioitu sisäverkko ja vierailijaverkko. Teorian avulla lukija saadaan ymmärtämään, mitä asioita on huomioitava langattoman verkon asennuksessa. Asennusprosessi ja vaiheet on dokumentoitu ohjeistuksena, vastaavan asennuksen varalle.

Työ rajattiin käsittelemään ainoastaan langattoman verkon järjestelmän asetuksia ja määrityksiä. Työtä varten tuli kuitenkin tehdä myös langallisen verkon puolelle muutoksia. Nämä muutokset tekee lähiverkoista vastaava henkilö.

Alkutilanteessa kohdeyritys käytti langallista verkkoa kaikissa työpisteissä ja kokoustiloissa. Kokoustilojen rajallisten verkkopaikkojen takia, kaikki kokoukseen osallistujat eivät pystyneet kytkeytymään yhtä aikaa verkkoon. Langattoman verkon avulla kokoustiloista pystyy jokainen osallistuja liittymään verkkoon helposti ja työpisteistä saadaan joustavampia.

Teoriavaiheessa määritettiin peruskäsitteet langattomista verkoista, yleisstandardeista ja tietoturvasta. Haastattelun perusteella saatiin selville, missä ja ketkä langatonta verkkoa tarvitsisi. Näiden tietojen perusteella suunniteltiin langaton verkko ja siihen tarvittavat ominaisuudet. Suunnittelussa selvitettiin ensin, mitä vaihtoehtoja on saatavilla ja millä tavalla päästäisiin haluttuun lopputulokseen. Suunnitelma ja ohjeistus on tehty Trapezen järjestelmään.

Lopputuloksena saatiin tehtyä langaton verkko käytännössä ja ohjeistus sen asennusta varten. Työntekijöitä ja vierailijoita varten tehtiin omat langattomat verkot, ja peittoalue saatiin kattamaan toimitilat ja kokoustilat.

Asiasanat Langaton verkko, langattoman verkon tietoturva, tukiasema, signaali, WLAN, Trapeze, Ringmaster, Smartpass

**Laurea University of Applied Sciences** **Abstract**
Laurea Leppävaara
Bachelor's Programme in Business Information Technology

Haka-Taivalmäki, Juha

**Wireless network planning and installation for enterprise use**

Year 2011 Pages 49

The objective of this thesis is to present theory and one type of solution for a wireless local area network (WLAN). I produced the solution with Trapeze system. With the theory section of the thesis the reader gains knowledge of what needs to be considered in the installation process of the WLAN. Based on this theory, the installation was carried out and the process as well as the stages were documented as instructions for later installation needs.

This project is limited to include only the required configurations for the WLAN. The project also requires changes to be made to local area network. These changes have to be made by the person in charge of the local area network.

At the start of this project the target company had only a local area network for workstations and meeting rooms. The meeting rooms had only a few plug-ins for the network so everyone could not connect to the network at same time. With the WLAN everyone can access to network at same time and workstations become more flexible.

The basic concepts of the WLAN, common standards and network security are determined in the theory section. Users and their locations were determined by interviewing. Based on this information plans were made for the WLAN and the features it would need. At the start of the planning it was examined what options there were and with which options the goals would be reached. The plan and instructions were produced with one single example solution.

The outputs of this project are WLAN installation and instructions for the installation. Separate networks for company employees and for guests were created. The networks also covered all working stations and meeting rooms.

Key words Wireless network, wireless network security, access point, signal, WLAN, Trapeze, Ringmaster, Smartpass

Sisällys

# 1 Johdanto

Työn tarkoituksena on luoda langaton verkko (WLAN). Lopputyö sisältää toiminnallisesti laitteiden asennuksen, asetusten määrittelyn, testaamisen, ohjeistamisen ja järjestelmän esittelemisen muulle tietohallinnolle. Dokumenttien osalta opinnäytetyö sisältää teoriaa ja ohjeistuksen minkä avulla vastaavan ratkaisun voi toteuttaa toisessa toimipisteessä tai yrityksessä. Esimerkkiratkaisun ohjeistuksessa kerrotaan kaikki oleelliset asiat, jotka tulee ottaa huomioon langatonta verkkoa rakentaessa. Lisäksi kohdeyritykselle annetaan tarkennettu dokumentti kaikista projektiin liittyvistä tarkemmista tiedoista ja määrityksistä. Kohdeyrityksessä pidetään myös esitys langattoman verkon ominaisuuksista ja hallinnointimenetelmistä. Esityksen avulla yrityksen on mahdollista ylläpitää ja käyttää järjestelmää.

## 1.1 Työn taustat ja tarkoitus

WLAN-verkon asennus tehdään Lemminkäinen Talotekniikka Oyj:n pääkonttorin tiloihin ja se kattaa rakennuksen kaikki neljä kerrosta. Rakennuksessa ei ole entuudestaan WLAN-verkkoa ja sen tarpeellisuus todettiin vuonna 2007. Tarpeellisuus määritettiin ja havaittiin runsaiden asiakkailta tulleiden kyselyjen perusteella (Mäkelä 2010). WLAN-verkko tulee kaikkien Lemminkäisen kannettavien tietokoneiden käyttöön ja vierailijoiden kannettavien tietokoneiden käyttöön. Verkon tärkein kattavuusalue on neuvotteluhuoneet, joita on viisi. Ensimmäiseen kerrokseen on alustavasti suunniteltu laitettavan kolme tukiasemaa ja muihin kerroksiin kaksi. Yhteensä tukiasemia on yhdeksän.

WLAN-verkko tulee helpottamaan kokouksissa käytettävien kannettavien tietokoneiden käyttöä. Tällöin kokouksiin osallistuvat henkilöt pääsevät helposti Internetiin. WLAN-verkko mahdollistaa myös usean tietokoneen yhtäaikaisen yhdistämisen verkkoon samasta kokoustilasta. Langallisella verkolla yhtäaikainen yhteys vaatisi jokaiselle koneelle oman johdon ja kytkimen jakamaan sen hetkistä yhtä verkkojohtoa. Suojatun WLAN-yhteyden kautta Lemminkäisen työntekijät pääsevät myös sisäiseen verkkoon.

WLAN-verkko rakennetaan Trapezen laitteilla ja ohjelmistoilla. Päätös Trapeze-järjestelmän hankkimisesta tehtiin 2007 ja laitteet hankittiin heti päätöksenteon jälkeen. Silloin vahvimpina vaihtoehtoina oli Trapeze ja Cisco. Trapezen järjestelmän todettiin sopivan paremmin yrityksen tarkoituksiin. (Mäkelä 2010.)

## 1.2 Käsitteet

Tässä luvussa selvitetään yleisellä tasolla opinnäytetyöhön liittyviä käsitteitä. Käsitteiden tarkoitus on antaa hyvä yleiskuva projektista ja siihen olennaisesti liittyvistä asioista. Joitakin käsitteitä on kuitenkin tarkennettu ja selitetty syvällisemmin opinnäytetyön muissa luvussa.

WLAN

Langaton lähiverkko eli WLAN (Wireles Local Area Network) on langaton kommunikointijärjestelmä, joka mahdollistaa kahden tietokoneen kommunikointitiedostojen siirron radioaaltoja käyttäen. WLAN-verkko pystytään liittämään osaksi langallista verkkoa ja se tarjoaa nopeaa tiedonsiirtoa ilman langallisen verkon fyysisiä rajoitteita. Erityisiä WLAN-verkon muotoja ovat 802.11-teollisuusstandardi ja sen monet eri versiot. (Lawrence 2005, 367.) Eri standardit on tarkemmin esiteltynä myöhemmin luvussa 2.1.

Wi-Fi

802.11 WLAN- Wi-Fi (wireless fidelity) -verkoilla tarkoitetaan yleensä samaa asiaa. Wi-Fi on kuitenkin Wi-Fi Alliance:n rekisteröimä merkki. Kaikkiin Wi-Fi Alliancen merkin saaneet tuotteet on testattu ja todettu toimivan muiden merkin saaneiden tuotteiden kanssa. (Lawrence 2005, 367.)

Trapeze

Trapeze perustettiin vuonna 2002 ja yrityksen osti Belden Inc. vuonna 2008. Vuonna 2007 Trapeze WLAN-ratkaisut tulivat Suomen markkinoille (Lahti 2007). Trapezen tavoite on valmistaa luotettavia WLAN-ratkaisuja (Trapeze Networks 2010.)

Trapeze valmistaa koko langattoman verkon kattavia ratkaisuja. Ratkaisuissa Trapeze käyttää Smart mobile -arkkitehtuuria. Smart mobile-arkkitehtuuri yhdistää sekä hajautettua (fat ap) että keskitettyä (thin ap) arkkitehtuuria. Hajautetussa (fat ap) arkkitehtuurissa tukiaseman asetukset ajetaan erikseen jokaiselle tukiasemalle, ja jokainen tukiasema toimii itsenäisesti. Keskitetyssä (thin ap) arkkitehtuurissa tukiasemalle ajetaan asetukset yhdestä keskitetystä WLAN-hallitsijasta ja kaikki käyttäjien tiedonsiirto tapahtuu tämän kautta. (Trapeze Networks 2010a, 4-6.)

Isoissa yrityksissä hajautettu arkkitehtuuri on liian vaikea hallinnoida, mutta keskitetty arkkitehtuuri on liian hidas ratkaisu. Trapezen Smart mobile -arkkitehtuuri yhdistelee näitä molempia tekniikoita.

Ringmaster

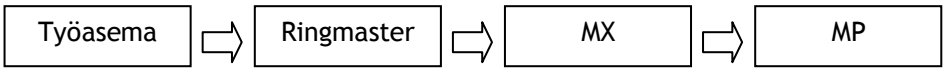
Ringmaster on Trapezen ohjelmisto. Ohjelmistolla pystytään suunnittelemaan, hallinnoimaan asetuksia ja valvomaan Trapezen langattomia verkkoja. Ohjelmisto asennetaan palvelimelle ja ohjelmistoa voi käyttää Javan ohjelmiston sisältävältä koneelta verkon yli. Ohjelmisto pystyy hallinnoimaan verkon kautta kaikkia Trapezen laitteita ja huomioimaan suunnittelussa muiden valmistajien laitteet.

Trapeze MX-kytkin

Trapeze tarjoaa kytkimiä useaan eri tarkoitukseen: palvelinhuone-, kytkentäkaappi- ja toimipisteversioita. Kaikissa laitteissa on Trapezen MSS (Mobile System Software) ja useampaa eri MX-kytkintä voidaan hallinnoida yhtenä verkkona tai toimialueena. Laitteesta riippumatta kaikkia MX-kytkimiä voidaan hallita Ringmaster-ohjelmistolla. (Trapeze Networks 2010c.)

Trapeze MP-tukiasema (MobilPoint)

MP tukiasema hakee asetuksensa MX-kytkimeltä aina kun tukiasema kytketään verkkoon ja hävittää asetukset aina kun tukiasemasta kytketään virta pois. Kaikkia Trapezen tukiasemia voidaan hallinnoida samalla tavalla MX-kytkintä käyttäen. Alla on kuva siitä, mitä kautta asetukset tulevat tukiasemille. Asetukset pystytään kuitenkin määrittämään suoraan Ringmaster-palvelimella MX-kytkimelle tai suoraan MX-kytkimelle, joka lähettää asetukset tukiasemalle.




Kuva 1: Asetusten määrittely

AirDefense

AirDefense järjestelmä on palvelimelle asennettava järjestelmä, joka on tarkoitettu yrityksille. Se suojaa langatonta verkkoa uhilta ja murtautumisyrityksiltä. AirDefense voidaan liittää osaksi Trapezen mobility-järjestelmää. Sen tarkoitus on tarkkailla, kerätä ja analysoida langattomassa verkossa liikkuvaa tietoa. RingMaster-palvelimen kanssa toimiessaan AirDefense-palvelin voi lähettää RingMaster-palvelimelle tiedon hyökkäyksestä ja RingMaster-palvelin voi sen perusteella tehdä hälytyksen. Trapezen tukiasemat voidaan myös asettaa toimimaan AirDefence-palvelimen sensoreina, jotka lähettävät tiedot mahdollisesta uhasta tai murtautumisesta AirDefense-palvelimelle. (Trapeze Networks 2007, 53.)

VLAN

VLAN (virtuaaliverkko) voidaan totateuttaa neljällä menetelmällä: porttiperusteella, MAC-osoitteen perusteella, verkkokerroksen palveluiden perusteella tai policy-määritysten avulla. Porttiperusteisessa VLAN-menetelmässä kytkimen portteihin määritetään, mihin VLAN:iin mikäkin portti kuuluu. MAC-osoitteen perusteella VLAN määritetään jokaiselle tietokoneen

MAC-osoitteellee ja tällöin yksi tietokone voi kuulua vain yhteen VLAN:iin. Verkkokerrokseen perustuvassa menetelmässä voidaan koneet jakaa aliverkkojen tai IPX-verkkonumeroiden perusteella. Policy-perustainen menetelmä mahdollistaa useamman eri menetelmän käytön ja protokollien otsakkeista voidaan käyttää tietoja VLAN-määrityksissä. (Hakala, Vainio, & Vuorinen, 2006, 232-234.)

SSID

SSID (Service set identifier) on tukiaseman lähettämä majakkaviesti. Oletusarvoisesti tukiasema lähettää majakkaviestin muutaman sekunnin välein. SSID-yleislähetyksen voi kuitenkin laittaa pois päältä. (Thomas 2005, 303-304.) Tällöin käyttäjän tulee tietää SSID ennen kuin hän voi yrittää liittyä verkkoon.

BSSID

BSSID (Basic Service Set Identifier) on tukiaseman yksilöllinen tunniste ja sitä käytetään tunnistamaan tukiasema langattomassa verkosta (Wi-Fi alliance 2011). Muodoltaan BSSID muistuttaa MAC-osoitetta.

# 2 Langattoman verkon suunnittelu

## 2.1 Standardit 802.11a, 802.11b, 802.11g ja 802.11n

802.11-standardeilla on erilaisia ominaisuuksia, jotka vaikuttavat sen toimivuuteen ja soveltuvuuteen. Siirtonopeus on kuitenkin aina uuden version myötä nopeutunut.

802.11a-standardi käyttää muista standardeista poiketen korkeampaa 5GHz:n taajuutta. 802.11n-standardi pystyy kuitenkin toimimaan 2,4- ja 5 GHz:n taajuuksilla, ja se on myös yhteensopiva 802.11a ja 802.11b-standardien kanssa. Yhteensopivuustila hidastaa kuitenkin siirtonopeuden samalle tasolle vanhojen standardien kanssa. (Puska 2005, 124-127; Kassner 2008; United Business Media 2010, 17-27.)

Korkeammalla taajuudella saadaan signaalista enemmän tilaa ja parempi suorituskyky. Korkeamman taajuuden heikkoutena on kuitenkin sen kantama, joka on lyhyempi kuin alemmalla taajuudella toimivat standardit. Alemman 2,4 GHz:n taajuuden käyttö kuitenkin altistaa verkon herkemmin häiriöille. Häiriötä voivat aiheuttaa mikroaaltouuni, puhelimet ja muut 2,4 GHz-kanavaa käyttävät laitteet. 802.11n-standardissa on kuitenkin pyritty vähentämään häiriöherkkyyttä MIMO –tekniikalla, mikä perustuu useamman antennin käyttöön. MIMO -tekniikassa useampi antenni lähettää samat paketit yhtä aikaa tai antennit lähettävät eri paketteja yhtä aikaa. Kun antennit lähettävät samoja paketteja yhtä aikaa, saadaan järjestelmästä luotettavampi. Kun taas eri paketteja lähetetään yhtä aikaa useammalla antennilla,

saadaan kasvatettua tiedonsiirto nopeutta. (Geier 2005, 124-127; Kassner 2008; United Business Media. 2010, 17-27.)

802.11n-standardin kehittäminen aloitettiin 2002 ja ensimmäinen luonnosversio julkaistiin 2003. Luonnosversiota kehitettiin kuusi vuotta ja standardi hyväksyttiin 2009. Luonnosversiot pystytään kuitenkin tuomaan hyväksytylle standardisointitasolle ohjelmistopäivityksellä. (Ngo 2009.)

Alla oleva taulukko on laadittu useita eri lähteitä käyttäen. Ylärajana on standardin määrittämä nopeus ja alarajana todellisuutta kuvaava nopeus mahdollisessa normaalissa käyttötilanteessa. Poikkeuksena taulukossa on 802.11n-standardi minkä maksiminopeus on standardoitu 600 Mbps, mutta käytännössä tämä 600 Mbps-nopeus vaatii erityisen hyviä puitteita. (Geier 2005, 124-127; Kayne, 2010; Ngo 2009.)

Taulukko 1: Standardit ja niiden ominaisuudet (Geier 2005, 124-127; Kayne, 2010; Ngo 2009)

| **Standardi** | **Siirtonopeus** | **Taajuus** | **Saatavilla** |
|---|---|---|---|
| 802.11n | 100-200+ Mbps | 2,4 GHz / 5 GHz | 2009 |
| 802.11g | 25-54 Mbps | 2,4 GHz | 2003 |
| 802.11a | 25-54 Mbps | 5 GHz | 2000 |
| 802.11b | 5-11 Mbps | 2,4 GHz | 1999 |
| 802.11 | 2 Mbps | 2,4 GHz | 1997 |

## 2.2 Tietoturva

Opinnäytetyössä on kartoitettu tietoturva Trapezen järjestelmän puolelle näkyvältä osalta. Kohdeyrityksen tietoturvavastaava on tehnyt suurimmat päätökset tietoturvan kannalta tärkeissä asioissa verkon puolella.

### Hyökkääjät

Trapezen Wired and Wireless Security Best Practices komiteamietintö (white paper) kehottaa varautumaan kolmen tyyppisiin hyökkääjiin.

Wardrive on hyökkäystapa, missä hyökkääjät kiertelevät etsien avoimia tai huonosti suojattuja verkkoja. Heidän ainoa motivaationsa on saada yhteys verkkoon, eivätkä he tee useimmiten minkäänlaista vahinkoa. Tämän tyyppisiä hyökkääjiä varten riittää yksinkertainenkin suojaus. (Trapeze Networks 2008d, 1.)

Kaistan varastajat ja roskapostittajat ovat suurempi uhka, sillä he tekevät hyökkäyksiä tavoitteenaan saada rahaa. Tällöin hyökkääjä on valmis näkemään suuremman vaivan verkon murtamiseen. Tämän tyyppiset hyökkääjät käyttävät kuitenkin saatavilla olvista verkoista mieluiten huonoimmin suojattua verkkoa. (Trapeze Networks 2008d, 1.)

Kaikista vaarallisimman tyyppiset hyökkääjät ovat tietoiset hyökkääjät. Tämän tyyppiset hyökkääjät ovat harvinaisia, mutta he ovat erityisesti kiinnostuneet hyökkäämään kohteeksi valitsemaansa verkkoon. Tarkoituksenaan heillä on saada pääsy verkossa liikkuvaan tietoon tai aiheuttaa vahinkoa. Suurella todennäköisyydellä tämän tyyppisessä hyökkäyksessä hyökkääjä on entinen työntekijä, tai hyökkääjä saa apua entiseltä työntekijältä. Hänellä on yleensä hyvä tietämys tai olettamus kohde yrityksen tietoturvamenetelmistä. Käytössä on yleensä uusimmat työkalut, joilla hän yrittää saada pääsyä verkkoon ja aiheuttaa vahinkoa. Mitä suurempaa vahinkoa hänellä on mahdillista aiheuttaa, sitä kiinnostuneempi hyökkääjä on verkkoon hyökkäämisestä. (Trapeze Networks 2008d, 2.)

Salausmenetelmät

PSK (Pre-shared Key) menetelmässä voidaan käyttää WEP, WPA ja WPA2 protokollia. PSK menetelmän yleisenä heikkoutena on avain. Avaimena on salasana, joka on määritetty etukäteen järjestelmään. PSK menetelmässä kaikki käyttäjät käyttävät samaa salasanaa. Mitä enemmän verkolla on käyttäjiä, sitä suurempi mahdollisuus on että salasanaa käytetään väärin ja sitä vaikeampi salasanaa on vaihtaa. (Trapeze Networks 2008d, 3.)

WEP (Wired Equivalent Privacy) salauksella päästään langattomassa verkossa samalle tietoturvatasolle kuin langallinen verkko ilman salausta. WEP salauksessa voidaan käyttää 64 tai 128-bittistä salausta. Kummatkin käyttävät kuitenkin 24-bittistä alustusvektoria, minkä ansiosta hakkerit voivat murtaa salauksen liikennettä kuunnellen. (Thomas 2005, 305-306.) WEP salauksen murtamiseen löytyy Internetistä paljon ohjeita ja ohjelmia, joten salauksen murtaminen onnistuu helposti keneltä tahansa. Perusideana ohjeissa on etsiä WEP salauksella toimiva langaton verkko ja kuunnella sen liikennettä useiden kymmenien tuhansien pakettien ajan. Tämän jälkeen ohjelma voi päätellä kerättyjen pakettien perusteella, mikä verkon salasana on.

TKIP-protokolla (Temporary Key Integrity Protocol) on tarkoitettu parantamaan WEP-protokollan heikkoutta, avainten uudelleen käytössä. TKIP käyttää 128-bittistä väliaikaista avainta ja yhdistää sen asiakkaan MAC-osoitteen kanssa, sekä lisää 16 oktetin alustusvektorin tuottaakseen avaimen. Tällä avaimella tiedostot salataan ja varmistutaan että jokainen asema käyttää eri avainmerkkijonoa. Salaamisessa TKIP käyttää WEP-protokollan tavoin RC4 algoritmia salaukseen. TKIP:n merkittävin parannus WEP:iin nähden on väliaikaisten avainten

käyttö, sillä TKIP vaihtaa avaintaan aina kymmenentuhannen paketin välein. (Geier 2005, 183.)

MAC (Media Access Control) osoite on 12-numeroinen heksadesimaaliluku, joka on yksilöllinen jokaiselle verkkokortille. MAC-osoitesuodatuksessa määritetään sallitut MAC-osoitteet ja estetään tuntemattomien osoitteiden pääsy verkkoon. Tämä suojaus yksinään ei kuitenkaan ole turvallinen, sillä verkkoliikennettä nuuskimalla voidaan selvittää verkossa liikennöivän laitteen MAC-osoite. Tämän jälkeen hyökkääjä voi vaihtaa MAC-osoitteensa sallituksi osoitteeksi ja onnistua täten liittymään verkkoon. (Thomas 2005, 307.)

WPA-protokolla (Wireless Fidelity Protected Access) on WEP-protokollaa parempi. WPA protokolla pystyy käyttämään WEP-protokollan tavoin TKIP:iä. TKIP:in on kuitenkin todettu vuonna 2008 sisältävän heikkouden. Heikkouden avulla verkkoon voidaan tehdä ARP (Address Resolution Protocol) myrkytys tai DNS (Domain Name Service) huijaus tai myrkytys. (Fleishman 2008.) Trapezen tietoturvallisuutta käsittelevä dokumentti Wired and Wireless Security Best Practices on määrittänyt vuonna 2008 WPA2 AES/CCMP standardin olevan salaukseltaan vahva ja paremmaksi kuin WPA. (Trapeze Networks 2008d, 7.)

VPN-yhteys (Virtual Private Network) on salattu yhteys turvattoman verkon yli. Se tarjoaa turvallisen etäyhteyden julkisen Internetin yli. (Thomas 2005, 115.) WLAN-verkossa VPN-yhteyttä voidaan käyttää vierailijaverkossa. Tällöin vierailijaverkolle ei tarvitse tehdä minkäänlaista salausta ja salaus jätetään vierailijan VPN-yhteyden vastuulle.

VPN-toteutukset voidaan toteuttaa siirtoyhteyskerroksella PPTP, L2F tai L2TP protokollilla, verkkokerroksella IPSec protokollalla, kuljetuskerroksella SSL (Secure Socket Layer) protokollalla tai sovelluskerroksella SSH (Secure Shell) protokollalla. (Langattomat lähiverkot 2005 85-86.) Alla oleva taulukko on laadittu kahden kirjan perusteelta, selkeyttämään OSI-mallin kerroksia ja sitä millä kerroksella mikäkin salaus toimii.

Taulukko 2: OSI malli ja VPN salausprotokollat (Wendell 2004, 58; Puska 2005, 85-86).

| **OSI-malli** | **TCP/IP** | **Salausprotokolla** |
|---|---|---|
| Sovellus | Sovellu | SSH |
| Esitystapa | | |
| Istunto | | |
| Kuljetus | Kuljetus | SSL |
| Verkko | Internetwork | IPSec |
| Siirtoyhteys | Verkkoliitäntä | PPTP, L2F tai L2TP |
| Fyysinen | | |

AAA

AAA (Authentication Authorization Accounting) lyhenne tulee sanoista todennus, valtuutus ja tilastointi. Nämä asiat tarvitaan, jotta verkkoa voidaan suojata väärinkäytöiltä. Todennuksessa varmistetaan, että käyttäjä on kuka väittää olevansa. Todennuksessa voidaan käyttää esimerkiksi käyttäjätunnusta ja salasanaa. Valtuutuksella määritetään käyttäjien oikeudet. Oikeuksilla tarkoitetaan käyttäjän oikeuksia käyttää tiettyjä ominaisuuksia tai tiedostoja. Tilastoinnissa käyttäjien tekemät asiat tilastoidaan. Tilastojen avulla voidaan todeta, kuka käyttäjä on tehnyt mitä ja milloin. (Thomas 2005, 115.)

RADIUS (Remote Authentication Dial-In User Service) on asiakaspalvelinpohjainen järjestelmä. Sitä voidaan käyttää todennukseen, valtuutukseen ja tilastointiin. (Verkkojen tietoturva perusteet 2005 118-119.) Ensin asiakassovelluksen ja RADIUS–palvelimen välille pitää luoda suojattu yhteys. Suojatun yhteyden voi luoda salaisen avaimen perusteella. Tällöin salainen avain syötetään asiakassovelluksen IP-osoite RADIUS-palvelimelle ja määritetään salainen avain. Kun sama on tehty asiakassovellukselle, voi asiakassovellus salatusti lähettää valtuutuspyyntöjä RADIUS-palvelimelle.

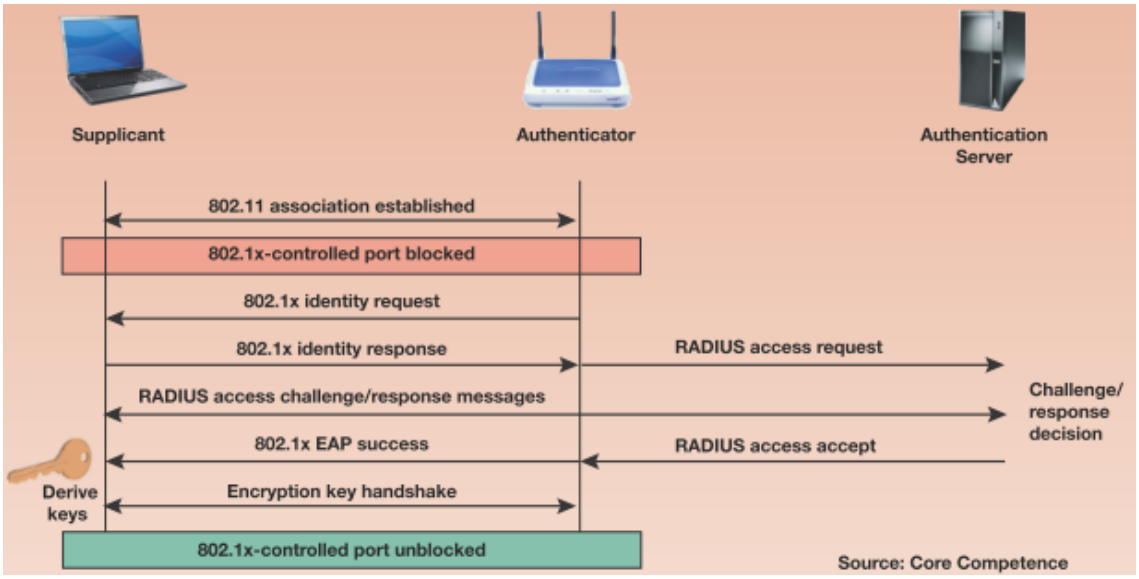
Trapezen Wired and Wireless Security Best Practices komiteamietintö (white paper) on määrittänyt MAC-suodatuksen ja PSK-menetelmät heikoiksi todennusmenetelmiksi. Vahvempina pidettävät salausmenetelmät ovat yleisesti IEEE 802.1X johdannaisia. (Trapeze Networks 2008d, 3.) 802.11X protokollassa on kolme tärkeää ominaisuutta, jotka tekevät siitä paremman kuin PSK (Trapeze Networks 2008d, 8):

- yksittäinen käyttäjäntodennus, eli mahdollisuus todentaa käyttäjän identiteetti
- istuntokohtainen salaus, eli EAP toiminnon mahdollistama uniikin salausavaimen käyttö jokaisessa istunnossa
- helppo liitettävyys jo olemassa olevaan järjestelmään, eli voi käyttää jo olemassa olevaa RASIUS-palvelinta

802.1x protokolla on kehys käyttäjäliikenteen automaattiseen todennukseen ja valvontaan. Se yhdistää EAP-protokollan sekä lanka- että langattomaan verkkosiirtotiehen. 802.1x tukee useita todennusmenetelmiä, kuten token card–tunnistus, Kerberos, kertakäyttöiset salasanat, varmenteet ja julkisen avaimen todennusmenetelmää. (Geier 2005, 188.)

802.1x todennus toimii niin kuin näytetään kuvassa ”802.1x käyttäjän todennus”, joka on otettu Wired & Wireless security best practices pdf dokumentista. Ennen asiakkaan todennusta, tukiasema estää kaiken muun kuin EAP-pakettiliikenteen asiakkaalta todennuspalvelimelle. Todennusprosessin aloittaakseen käyttäjä lähettää EAP-aloitusviestin tukiasemalle ja tu-

kiasema lähettää vastauksena EAP-identiteettipyyntöviestin. Asiakas vastaa pyyntöön EAP-vastauspaketilla, mikä sisältää asiakkaan identiteetin ja tukiasema toimittaa sen todennuspalvelimelle. Todennuspalvelin käyttää todennusalgoritmia ja vahvistaa tällä tavalla käyttäjän identiteetin. Todennuspalvelin voi käyttää tähän sähköisiä varmenteita, tai jotain muuta EAP:n todennusmenetelmää. Tämän jälkeen todennuspalvelin lähettää tukiasemalla hyväksyvän tai hylkäävän viestin. Mikäli viesti on hyväksyvä, tukiasema lähettää hyväksyvän EAP-viestin käyttäjälle ja muuttaa käyttäjän portin valtuutettuun tilaan. Valtuutetussa tilassa käyttäjän portin kautta sallitaan muukin kuin EAP liikenne. (Geier 2005, 189-190.)




Kuva 2: 802.1X käyttäjän todennus (Trapeze Networks 2008d).

EAP (Extensible Authentication Protocol) protokollaa käytetään tukiaseman ja päätelaitteen välisessä liikenteessä todennusvaiheessa. EAP-protokollasta on tehty useita erilaisia menetelmiä ja ne toimivat samalla perusperiaatteella. EAP menetelmiä ovat esimerkiksi EAP-MD5, LEAP (Cisco Lightweight EAP), EAP-TLS (EAP Transport Layer Security), EAP-TTLS (EAP Tunneled Transport Layer Security) ja PEAP (Protected EAP). (Puska 2005, 75 -77; Thomas 2005 308; Geier 2005, 190; Trapeze Networks 2008d, 4.)

AES (Advanced Encryption Standard) on vuonna 2001 standardisoitu salausmenetelmä. Salausmenetelmä käyttää kehittynyttä matemaattista kaavaa salauksessa. EAS on yleisimmin käytössä oleva salausstandardi, eikä siitä ole vielä löydetty heikkouksia. (Kempf 2008, 46)

Valtuutuksia määrittämällä voidaan vaikuttaa käyttäjien oikeuksiin käyttää järjestelmää, tai vaatia käyttäjältä tiettyjä ominaisuuksia ennen kuin käyttäjälle annetaan tiettyjä oikeuksia. Käyttäjiä voidaan rajoittaa alla listatuilla tavoilla ja niiden yhdistelmillä:

- salausmenetelmän mukaan
- ryhmän mukaan
- järjestelmän päivitysten
- rajoittamalla käyttö ainoastaan Internetiin
- rajoittamalla käyttäjänoikeuksia tiettyihin ryhmiin tiettyinä aikoina
- rajoittamalla käyttäjän oikeuksia käyttäjän sijainnin mukaan
- yhtäaikaisten kirjautumisten määrä voidaan rajoittaa
- kaistan leveys voidaan rajoittaa tai jakaa
- rajoittamalla käyttäjän oikeuksia käyttäjän käyttämien ohjelmien mukaan (Kempf 2008 5-6.)

Tilastointi kerää ja lähettää tietoja laskutusta, tarkastelua ja raportointia varten. Mikäli tilastointia ei ole toteutettu oikein tai ollenkaan, ei pystytä virhetilanteen sattuessa vastaamaan kysymykseen mitä tapahtui. Hyvän tilastoinnin avulla pystytään määrittämään missä, milloin ja mitä tapahtui. (Kempf 2008, 7.)

## 2.3 Toteutuksen suunnittelu

Tässä luvussa käydään läpi asioita, jotka tulee huomioida ennen toteutukseen siirtymistä. luvussa on erityisesti Trapezen järjestelmää koskevia asioita.

### Laitevaatimukset

Laitevaatimukset on tarkoitettu tilanteeseen, missä Ringmaster ja SmartPass ovat käytössä eri palvelimilla. Ohjelmistot voidaan kuitenkin asentaa samallekin palvelimelle, tällöin ohjelmistojen käyttämien porttien tulee kuitenkin olla eri. SmartPass-palvelimen portiksi kannattaa määrittää 443, mikä on vakio salattu https-portti ja Ringmaster-palvelimelle kannattaa määrittää jokin muu. Tällöin on SmartPass-palvelimella helpompi ottaa yhteys selaimelle, kun käyttäjän ei tarvitse tietää erityistä porttia. Ringmaster-palvelinta käyttää ainoastaan asiantuntijat, ja he osaavat ja tietävät paremmin, mikä portti on käytössä.

Seuraavissa taulukoissa selvitetään Ringmaster-palvelimen laitevaatimukset. Niissä on otettu huomioon verkossa olevien laitteiden määrä ja ensimmäisessä taulukossa on Linux ja Windows-palvelimille laitevaatimukset. Toisessa taulukossa on MAC-palvelimelle laitevaatimukset.

Taulukko 3: Ringmaster Windows ja Linux-palvelimen laitevaatimukset

| | AP:ita | MX:iä | Prosessori | Kellotaajuus | RAM | Kovalevytila |
|---|---|---|---|---|---|---|
| Pieni | 50 | 10 | Intel/AMD x86-compatible Dual Core processor | 2.0 GHz | 2 GB | 50 GB |
| Keskikokoinen | 200 | 50 | Intel Dual Core Xeon | 3.0 GHz | 4 GB | 100 GB |
| Iso | 1000 | 100 | Intel Quad Core Xeon | 2.66Ghz | 4 GB | 150 GB |

Taulukko 4: Ringmaster MAC-palvelimen laitevaatimukset

| | AP:ita | MX:iä | Prosessori | Kellotaajuus | RAM | Kovalevytila |
|---|---|---|---|---|---|---|
| Pieni | 50 | 10 | Mac Pro | 2x 3.0 GHz | 2 GB | 50 GB |
| Keskikokoinen | 200 | 50 | Mac Pro | 2x 2.66 GHz | 4 GB | 100 GB |
| Iso | 1000 | 100 | Mac Pro/Xserve | 2x 3.0 GHz | 4 GB | 150 GB |

Seuraavassa taulukosta näkyy Smartpass-palvelimen laitevaatimukset. Kaikissa kokoluokissa minimivaatimuksena on 1024x768 pikselin kuva, 24-bit värit ja CD-asema.

Taulukko 5: Smartpass palvelimen laitevaatimukset

| | Prosessori | Kellotaajuus | RAM | Kovalevytila |
|---|---|---|---|---|
| Pieni | Intel/AMD x86-compatible Dual Core processor | 2 GHz | 2GB | 75 GB |
| Keskikokoinen | Intel Dual Core Xeon | 2.66 GHz | 4 GB | 100 GB |
| Iso | Intel Dual Core Xeon | 3 GHz | 4 GB | 150 GB |

Lisenssit

Lisensointi mahdollistaa verkon laajentamisen ilman laitteiston uusimista, koska kaikki ominaisuudet ovat jo laitteissa ja ohjelmistoissa valmiiksi. Lisenssit vain mahdollistavat ominaisuuksien käytön. Seuraavassa taulukossa selvitetään, minkälaisia lisenssejä on tarjolla ja mitä ominaisuuksia ne avaavat. Alla oleva taulukko on laadittu RingMaster 7-ohjekirjan perusteella (Trapeze Networks 2008b, 8-9).

Taulukko 6: Ringmaster 7.0 lisenssit

| | |
|---|---|
| EVAL | Järjestelmän kokeilua varten oleva lisenssi. Voi käyttää 90 päivää, mahdollistaa 50 tukiasemaa ja rajattoman määrän kytkimiä. |
| RMTS | Perustason lisenssi, joka tulee hankkia aina aluksi. Mahdollistaa 5 tukiasemaa ja yhden kytkimen |
| RMTS-50 | Mahdollistaa 50 lisätukiaseman liittämisen |
| RMTS-100 | Mahdollistaa 100 lisätukiaseman liittämisen |
| RMTS-500 | Mahdollistaa 500 lisätukiaseman liittämisen |
| RMTS-PLAN | Mahdollistaa suunnitteluominaisuuden käytön |

Taulukko 7: SmartPass 7.0 lisenssit

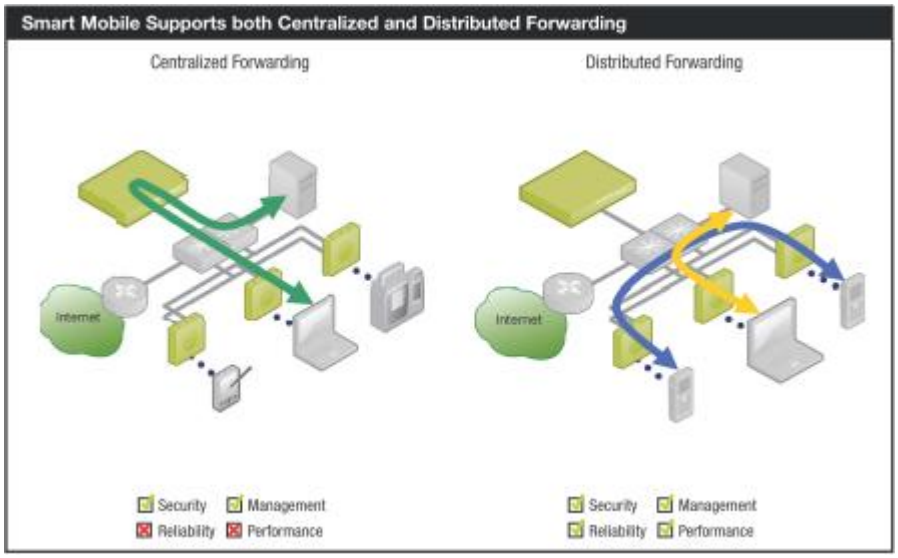
| | |
|---|---|
| SP | Perustason lisenssi mahdollistaa 50 käyttäjän luomisen |
| SP-ENT | Yritys lisenssi mahdollistaa 10000 käyttäjätunnusta, RADIUS tilastointipalvelun, käyttäjätunnuksen ja salasanan automaattisesti määrittelevän käyttäjän luomisen ja selainkäyttöliittymän SmartPass-ohjelmiston asetusten määrittämistä varten |
| SP-ACC | Sisältää SP ja SP-ENT lisenssien ominaisuudet, sekä todentamis-, tilastointi-, aikapalvelu ja paikka pääsynvalvonnan. |

Palvelut

Suunnittelun alkuvaiheessa pitää miettiä kuka ja miksi langatonta verkkoa tarvitaan. Kun asiakkaat ja tarpeet on määritetty, voidaan alkaa miettimään mitä palveluita tarvitaan. Palvelut voivat olla seuraavanlaisia: työntekijäverkko, vierailijaverkko ja VoWIP (Voice Over Wireless IP). Todentamismenetelmiä on 802.11x, Web sivu ja MAC-osoite. Salausmenetelmäksi voi valita 802.11i, WPA, WEP tai salaamaton. Työntekijäverkolle määritetään yleensä salattu yhteys ja vierailija verkolla valitaan yleensä suojaamaton yhteys (Trapeze Networks 2008c, 28).

Niin kuin johdannossa, haastattelun avulla selvitettiin asiakkaiksi työntekijät ja vierailijat. Tulee täten luoda työntekijäverkko ja vierasverkko. VoWIP verkolle ei kuitenkaan todettu vielä tarvetta. Täten tehdään työntekijöille suojattu virtuaaliverkko, minkä käyttäjät todennetaan RADIUS–palvelimella ja vieraille luodaan suojaamaton virtuaaliverkko, minkä käyttäjät todennetaan Smartpass-palvelimella. Työntekijäverkosta tehdään pääsy yrityksen sisäverkkoon ja vierasverkko ohjataan suoraan ulkoverkkoon, eli Internetiin.

Palveluiden lisäksi tulee etukäteen miettiä myös verkon yleiskuvaa ja sitä kuinka laitteet kytketään. Mikäli tukiasemia ei kytketä suoraan MX-kytkimeen vaan osaksi suurempaa verkkoa, löytävät tukiasemat MX-kytkimen verkosta ja lataavat asetukset sieltä liittyessään verkkoon. Niin kuin kuvassa ”Hajautettu ja keskitetty tiedonsiirto” havainnollistetaan, Trapezen järjestelmä saadaan toimimaan keskitetysti todentaessaan käyttäjän ja hajautetusti todennuksen jälkeen (Trapeze Networks 2009a, 2).




Kuva 3: Hajautettu ja keskitetty tiedonsiirto

VLAN-verkon määritykset tulee tehdä Trapezen laitteiden lisäksi verkon muille laitteille. Nämä määritykset tehdään verkoista vastaavan henkilön toimesta.

Palvelinsovellukset

Kytkintä pystytään hallinnoimaan CLI:n (Comand-line interface), Ringmaster-ohjelmiston ja asetustiedostojen avulla. Ringmaster-palvelinta voidaan hallinnoida osittain selaimella, mutta pääosin sitä hallinnoidaan siihen tarkoitetulla Java-pohjaisella sovelluksella. Smartpas-palvelinta hallinnoidaan ja käytetään ainoastaan selaimella. Alla olevassa taulukossa on merkitty mitä yhteysprotokollaa eri hallinnointimenetelmät käyttävät.

Taulukko 8: Hallinnointimenetelmät ja protokollat

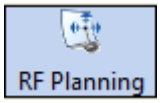
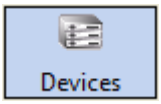
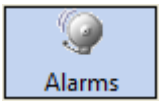
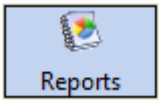
| **Hallinnointimenetelmä** | **Protokolla** |
|---|---|
| CLI (Comand-line interface) | SSH |
| Ringmaster | SSL |
| selain | HTTPS |

Ringmaster on Trapeze Networks:in verkon hallinnointityökalu. Työkalu käyttää hallinnoinnissa java- pohjaista hallinnointi ohjelmaa, joten sen pystyy asentamaan kaikille Java:a tukeville alustoille. Ohjelmiston saa asennettua Ringmaster palvelimelta. Palvelimeen otetaan yhteys selaimella, käyttäen Ringmaster –palvelimen IP osoitetta ja porttia, esimerkiksi https://99.99.9.999:999. Etusivulla (Home) on linkki Java JRE:n asennusta varten, mitä tarvitaan Rigmaster –ohjelmiston käyttöön. Kun Java-ohjelmisto on asennettu, voidaan Ringmaster asiakasohjelmisto avata painamalla ”Launch Client” painiketta. Tämän jälkeen Ringmaster –ohjelmisto käynnistyy ja kysyy IP-osoitetta, porttia, käyttäjätunnusta ja salasanaa Ringmaster palvelimelle.

Käyttöliittymä sisältää seitsemän eri paneelia: valikko, navigointi, organisointi (organizer), sisältö, tehtävät (tasks), hälytys ja palvelinikoni. Valikkopalkki sisältää alasvetovalikoita, jotka sisältävät linkkejä hallinnollisiin työkaluihin. Navigointipalkki sisältää painonappeja, joilla voidaan vaihtaa näkymiä välilehtien tavoin. organisointipalkissa näkyy laitteet ja niiden ominaisuudet puumaisena rakenteena, havainnollistava kuva on System valikko organizer paneelissa. Sisältöpalkissa näkyy tarkempia tietoja ja sen sisällä voidaan tehdä muutoksia asetuksiin. Tehtäväpalkissa on näkymästä riippuen linkkejä yleisiin asetusmäärityksiin. Tehtäväpalkin linkit aukeavat ponnahdusikkunana ja ovat joko valikoita tai ohjattuja toimintoja. Hälytyspalkissa näkyy aina kaikki hälytykset, varoitukset ja virheilmoitukset. Palvelinikonista voi nähdä palvelimen tilan ja käyttäjätunnuksen millä palvelimeen ollaan yhteydessä.

Navigointipalkista valittaessa vaihtuu organisointi, sisältö ja tehtäväpalkin sisältö. Seuraavassa taulukossa selvitetään mihin mistäkin napista pääsee.

Taulukko 9: Ringmaster ominaisuuksia

| | |
|---|---|
| Policies   | välilehdellä pystytään luomaan uusia sääntöjä verkkoon ja sen käyttäjiin |
| RF Planning   | välilehdellä päästään näkymään missä pystytään suunnittelemaan langaton verkko graafisesti. Suunnitelmiin voidaan ladata pohjapiirroksia ja määritellä laitteiden sijainnit. Määritysten perusteella ohjelmisto voi laskea laitteiden määrän tarvetta, tukiasemien sijainnin ja määrittää asetuksia. |
| Configuration   | välilehdeltä voidaan järjestelmään lisätä hallittavia laitteita. Laitteen lisäyksen jälkeen laitteiden asetuksia voidaan muuttaa. |
| Verification   | nähdään kaikki hälytykset mitä järjestelmä automaattisesti ilmoittaa. |
| Devices   | nähdään kaikki laitteet, ja tältä välilehdeltä voidaan lähettää kaikki laitteelle tehdyt muutokset yhdellä kerralla. |
| Monitor   | kytkinten, tukiasemien ja antennien tilaa ja tietoja. |
| Security   | nähdään luvattomat verkot, murtoyritys- ja palvelunestohyökkäyshälytykset. |
| Alarms   | nähdään kaikki hälytykset, kuten myös graafinen näkymä hälytyksistä. |
| Reports   | voidaan tehdä ajoitetusti raportteja järjestelmän ominaisuuksista, kuten käytöstä ja hälytyksistä. |

SmartPass-palvelimen avulla pystytään luomaan käyttäjiä joilla on oikeus käyttää langatonta verkkoa. Käyttäjät voivat olla myyjiä, urakoitsijoita, väliaikaisia työntekijöitä, tilintarkastajia tai vierailijoita. Näille käyttäjille voidaan antaa rajoitettuja oikeuksia verkkoon määräajaksi.

Yleisimmin vierailijan todennus suoritetaan selaintodennusmekanismilla. (Trapeze Networks. 2009b.) Tällöin Smartpass toimii RADIUS palvelimena vierailijaverkolle.

Suunnitteluvaiheessa järjestelmänvalvojan tulee suunnitella alla listatut asiat.

- kuka on vastuussa tunnusten luonnista, ylläpidosta, perusohjeistuksesta, salasanojen vaihdosta ja käyttäjätunnuskuponkien tulostuksesta
- tarvitseeko käyttäjiä seurata
- onko vierailijatunnukset käytettävissä langallisessa ja langattomassa verkossa
- minkälaisia käyttäjäprofiileja tarvitsee luoda (rajoitukset ajan tai sijainnin suhteen)
- tarvitseeko verkon kaistanleveyksiä määritellä
- miltä verkon topologia näyttää kun muutokset on tehty
- mitkä ovat turvallisuuden kannalta huolehdittavat asiat vierailijaverkkoa käytettäessä
- kuinka GuestPass skaalautuu
- mitä verkolle tapahtuu, mikäli tukiasema rikkoutuu
  (Trapeze Networks. 2009b.)

SmartPass–palvelimelle voidaan määrittää asetuksia selaimella. Selaimeen osoitteeksi kirjoitetaan https://<ip-osoite>:<portin-numero>. Mikäli palvelimelle on määritetty sisäänkirjautuminen pakolliseksi, palvelin kysyy käyttäjätunnusta ja salasanaa. Mikäli salasanaa ei ole vielä määritetty tulee ensimmäiseksi palvelimelle määrittää käyttäjätunnukset ja salasanat.

Tunnuksia pystytään määrittämään setup välilehden Access Control valikosta. Ensin tulee lisätä vähintään järjestelmänvalvojan salasana. Vähintään yhden järjestelmänvalvojan tunnuksen määrittämisen jälkeen voidaan painaa enable login-required nappia. Tämä toiminto pakottaa sisäänkirjautumisen palvelimelle.

Järjestelmänvalvojantunnusten lisäksi Smartpass palvelimelle voidaan luoda tunnukset ainoastaan ylläpitoa varten ja ainoastaan vierailijaverkontunnusten luontia varten. Ylläpitotunnuksilla voidaan suorittaa ylläpitoa koskevia toimintoja ja luoda vierailijaverkon tunnuksia. Pienimmillä oikeuksilla varustetulla tunnuksella voidaan luoda ainoastaan vierailijaverkon käyttäjätunnuksia.

Smartpass-palvelimelle voidaan luoda omat tunnukset kaikille järjestelmää käyttäville henkilöille. Tällöin voidaan rajoittaa mitä muutoksia kukakin käyttäjä voi tehdä tai minkälaisia tunnuksia kukakin voi luoda. Tunnusten luonti tulee suunnitella hyvin, mikäli palvelimella on paljon eri käyttäjiä ja ylläpitäjiä.

Palvelimen käyttäjien lisäksi tulee suunnitella minkä tyyppisiä käyttäjätunnustyyppejä tarvitaan. Käyttäjätunnustyypit ovat tyyppejä, mihin Smartpass-palvelimella luotavat vierasverkonkäyttäjätunnukset määritetään. Käyttäjätunnustyyppeihin voidaan määrittää salasanan väärinkirjoittamisen jälkeen odotettava aika, kuinka monta kertaa salasanan voi kirjoittaa väärin ennen kuin tunnus lukitaan ja lukitaanko tunnus kun käyttäjä poistuu verkosta. Tämän lisäksi käyttäjätunnustyyppiin voidaan määrittää rajoituksia tunnuksen käytölle. Tunnuksen käytölle voidaan määrittää käyttöaika tunneissa ja minuuteissa, käyttöajan jälkeen tunnus poistuu käytöstä. Tunnuksen käyttöä voidaan rajoittaa myös vuorokauden aikojen mukaan. esimerkiksi tunnusten käytettävyyden voi rajoittaa ainoastaan työaikoihin, jotka voidaan määrittää jokaiselle profiilille erikseen ja halutuille päiville tai tunneille. Mikäli käyttöä ei haluta rajoittaa voidaan kaikki tai osa rajoituksista jättää pois. Halutut rajoitukset tulee kuitenkin suunnitella hyvin, jottei langattoman verkon käytettävyys kärsi.

# 3 Toteutus

Tässä luvussa ohjeistetaan kaikille verkoille tarvittavien perusasetusten määrittäminen. Aluksi ohjeistetaan miten Trapezen järjestelmää voidaan hallinnoida ja kuinka muodostetaan yhteydet Ringmaster- ja Smartpass-palvelinten välille. Tämän jälkeen luvusssa ohjeistetaan kuinka Ringmaster-ohjelmistolla määritetään porttien asetukset ja lisätään tukiasemat.

Lisenssit voidaan määrittää palvelimen setup välilehden licensing valikosta. Valikossa new serial number kohtaan kirjoitetaan Smartpass-palvelimen sarjanumero. Sarjanumero löytyy Smartpass paketin kyljestä. New license key kohtaan kirjoitetaan lisenssin avain. Tämän jälkeen painetaan save nappia ja lisenssi tallentuu palvelimelle ja palvelin avaa lisenssin oikeuttamat ominaisuudet.

SmartPass-palvelimen ja Ringmaster-palvelimen välille luodaan suojattu yhteys määrittämällä IP-osoite ja salasana palvelimille. SmartPass-palvelimelle voidaan määrittää yhteys selaimelle setup välilehden RADIUS client settings sivulta. Listaan lisätään kaikki osoitteet millä on oikeus palvelimelle ja mitä salasanaa yhteyden todentamiseen käytetään. Ringmaster palvelimelle yhteys muodostetaan lisäämällä SmartPass-palvelimen IP-osoite, yhteyden salasana ja portin osoite. Mikäli SmartPass- ja Ringmaster-palvelimet ovat samalla palvelimella, tulee niiden käyttää eri porttia. SmartPass-palvelimen lisäyksen voi tehdä configuration välilehden tasks paneelista valitsemalla SmartPass Server. Tämä valikko on näkyvissä kun organizer paneelissa on valittuna default.

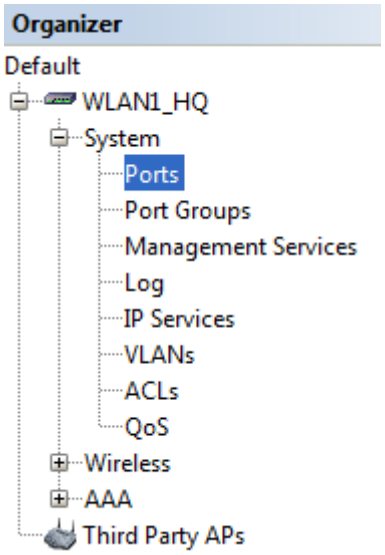
Yhteyden toimivuutta voidaan kokeilla Ringmaster ohjelmistolla. Ensin tulee kuitenkin määrittää yksi käyttäjätunnus mitä testataan. Käyttäjätunnus luodaan Smartpass-palvelimelle selaimen avulla. Selaimen osoitekenttään kirjoitetaan palvelimen IP-osoite ja portin osoite,

mikäli porttina käytetään eri porttia kuin oletus portti 443. Tämän jälkeen järjestelmään voidaan kirjautua sisään ja sisäänkirjautumisen jälkeen käytetyistä tunnuksista riippuen avautuu laajempi tai suppeampi käyttöliittymä. Testausta varten riittää hyvin suppeilla oikeuksilla varustettu tunnus.

Liitteenä on ohjeistus tunnusten luontia varten. Ohjeistus on tarkoitettu henkilöille joilla on rajoitetut Smartpass käyttöoikeudet ainoastaan vierailijaverkon tunnusten luontiin. Ohjeistus on tehty sillä olettamuksella ettei rajoitetuilla oikeuksilla oleva henkilö tiedä paljon tietotekniikasta.

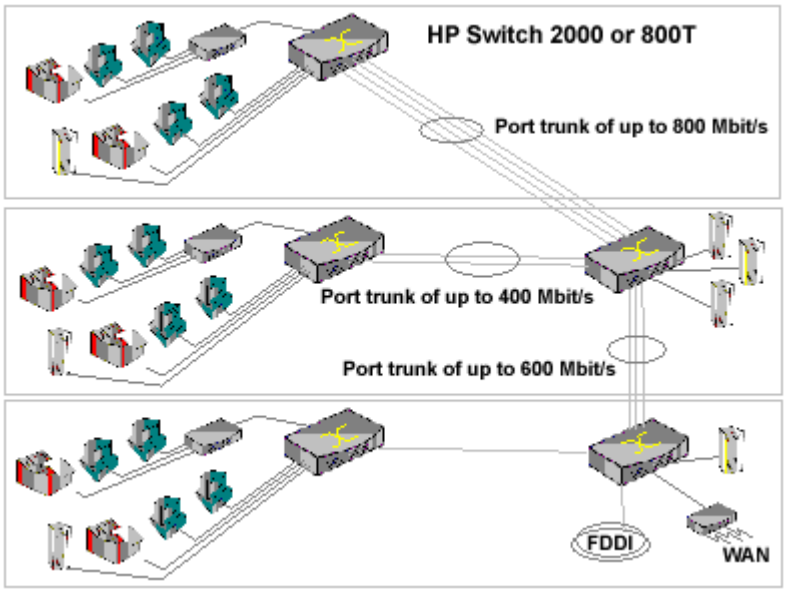
Kun tunnus on luotu, voidaan avata Ringmaster ohjelmisto ja mennä configuration välilehden organizer paneelin AAA valikon alta löytyvään RADIUS valikkoon. Tällöin saadaan task paneeliin näkyville RADIUS ping näppäin, mitä painamalla saadaan näkyviin ponnahdusikkunavalikko. Valikosta voidaan valita RADIUS-palvelin tai RADIUS-palvelinryhmä mitä halutaan testata. Edellytyksenä RADIUS ping toiminnon onnistumiselle on kuitenkin että RADIUS-palvelin on asetettu todentamaan MS-CHAP versio 2:lla. (Trapeze Networks 2008a, 169).

MX-kytkin lisätään Ringmaster ohjelmiston configuration välilehdellä, task -paneelista. Paneelille ilmestyy painike Create mobile exchange, kun organizer paneelilla on valittuna default. Kytkimen lisäämiseen tulee tietää laitteen sarjanumero ja salasana (enable password). Kytkintä lisätessä ei välttämättä tarvitse määrittää mitään muita asetuksia, mutta jo tässä vaiheessa kannattaa kuitenkin määrittää kytkimelle VLAN-osoite.



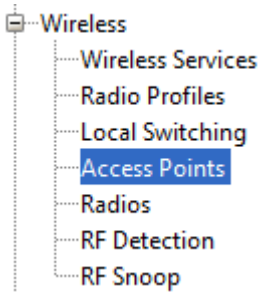

Kuva 4: System valikko organizer paneelissa

Kytkimen lisäyksen jälkeen configuration välilehden organizer paneeliin ilmestyy lisäämäsi kytkin. Kytkimen nimeä painettaessa avautuu lisävalikoita (kuva 4 System valikko organizer paneelissa). Ensimmäisenä on System ja sen alla Ports valikko. Tässä valikossa näkyy kaikki kytkimen portit ja niistä kannattaa tietoturvallisuus syistä sulkea käyttämättömät portit. Portit voidaan sulkea ottamalla ruksi pois portin enable kohdasta. Vähintään yksi ulkoverkkoon vievä portti tulee olla auki hallinnointia varten. Muut portit voidaan sulkea, mikäli tukiasemat eivät ole kytkettyinä suoraan MX-kytkimeen.



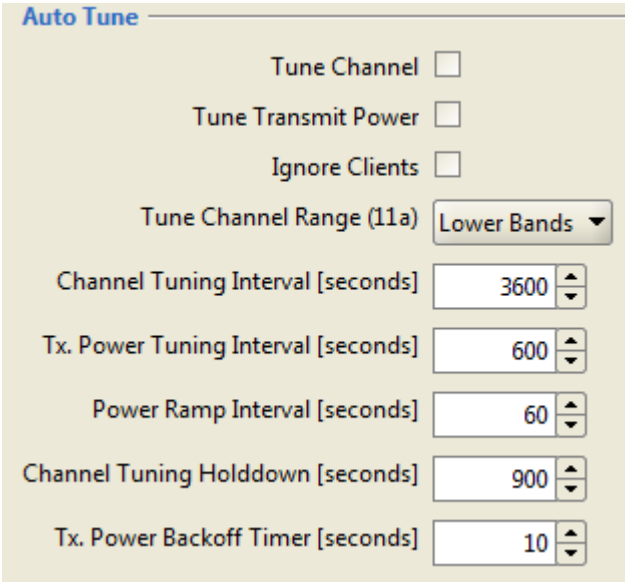

Kuva 5: Porttiryhmät (Hewlett-Packard Development Company 2010)

Toisena valikossa on Port Groups. Mikäli kytkimessä on useampi ulkoverkon portti, voidaan toisesta portista tehdä porttiryhmä sisäverkon kytkimen ja MX-kytkimen välille. Porttiryhmällä saadaan järjestelmään varmuutta ja nopeutta. Porttiryhmän varmuus ilmenee kun yksi porttiryhmän linja katkeaa. Tällöin muut linjat pystyvät toimimaan ilman sitä ja ainoastaan nopeus hidastuu. Porttiryhmän nopeuden huomaa aina kun lisää enemmän portteja samaan ryhmään. Mikäli yhden linjan sijasta muodostetaan kahden linjan porttiryhmä, nopeuskin kaksinkertaistuu. Porttiryhmät kuva havainnollistaa hyvin käytettyjen linjojen määrän vaikutuksen nopeuksiin. Kytkettäessä porttiryhmää tulee huomioida, että ryhmä on määritetty kummallekin kytkimelle ennen useamman linjan fyysistä kytkemistä.




Kuva 6: Wireless valikko organizer

Tukiaseman lisäämisessä tarvitsee tietää tukiaseman sarjanumero ja niin sanottu sormenjälkitunniste (fingerprint). Sormenjälkitunnistetta tarvitaan kytkimen ja tukiaseman välille luotavaa suojattua yhteyttä varten. Sarjanumero ja sormenjälkitunniste on merkitty tukiaseman pohjaan. Ennen tukiaseman lisäämistä kannattaa suunnitella mihin tukiasema suurin piirtein sijoitetaan. Sijainnin voi kirjoittaa tukiaseman nimi tai -kuvaus kenttään. Tämä helpottaa hallinnointia ja rikkinäisen tukiaseman paikantamista. Näiden kenttien lisäksi ei tarvitse määrittää kuin tukiaseman malli. Radioasetuksia ei tarvitse välttämättä muuttaa oletuksesta, sillä Ringmaster osaa säätää taajuudet ja kanavat automaattisesti (autotuning) ominaisuudella.




Kuva 7: Auto Tune-valikko

Autotuning asetuksen saa laitettua päälle Radio Profiles valikosta. Valitse default radioprofiili ja paina properties. Ponnahdusikkunasta pitää mennä Auto Tune-välilehdelle, mistä voidaan laittaa ruksi kohtiin mitä halutaan käyttää. Vaihtoehtoina on Tune Channel mikä säätää automaattisesti kanavia ja Tune Transmit Power säätää automaattisesti signaalin lähetystehoa. Lisäksi voidaan laittaa ruksi Ignore Clients kohtaan, jolloin automaattinen säätö ei huomioi

toiminnassaan käyttäjiä. Käyttäjien huomiointi säätää tukiasemien kantaman käyttäjän signaalin voimakkuuden mukaan. Tune Channel Range (11a) kohdasta voidaan valita All Bands tai Lower Bands. Tällä valinnalla voidaan määrittää säätääkö järjestelmä automaattisesti 802.11a protokollan verkoissa kaikkia kaistan taajuuksia vai ainoastaan alempia taajuuksia. Lopuista valikoista voidaan määrittää eri asetusten vaihtovälejä. (Trapeze Networks 2008a, 189 - 190).

Joissain tilanteissa on kuitenkin suositeltavaa laittaa Auto tune  pois päältä ja säätää antennit itse. Tällöin voi katsoa ensin Auto Tune-toiminnolla suosituksen kanavista ja tehoista, minkä perusteella voi määrittää asetukset käsin. Tällöin automaatio ei säädä verkkoa täysin sekaisin väliaikaisten häiriöiden vuoksi.

Tukiasemien paikkoja määrittäessä voidaan antenneja säätää organizer paneelin Wireless kohdan alla olevasta valikosta radios. Valikossa näkyy kaikki järjestelmään lisättyjen tukiasemien antennit. Valikoista voidaan laittaa antenni pois päältä, vaihtaa kanavaa tai signaalin voimakuutta. Näillä määrityksillä ei ole väliä mikäli Auto tune-toiminto on päällä.

## 3.1 Yleisasetukset

Ringmaster-palvelimella pystytään luomaan palveluprofiileja Trapezen langattomiin verkkoihin. Palveluprofiileja luodaan ohjatun toiminnon avulla. Ohjattu toiminto valitaan sen perusteella miten käyttäjä halutaan todentaa tai minkä tyyppinen palvelu halutaan luoda. Palvelumahdollisuuksina on 802.1x todennus, puhelu palvelu, Web poratali todennus, avoin pääsy ilman todennusta, verkkopalvelu ja mukautettu palvelu. Mukautetulla palvelulla voidaan luoda useamman todennusmenetelmän yhdistelmiä. Tällöin samaan verkkoon voidaan liittyä useammalla eri todennusmenetelmällä.

Verkkopalvelulla (mesh service profile) tarkoitetaan palvelua missä tukiasema ei ole langallisesti kytketty verkkoon. Mikäli kuuluvuusaluetta halutaan laajentaa, mutta lankaverkko ei yllä halutulle alueelle voidaan tehdä verkkopalvelu. Verkkopalveluun lisätään haluttujen tukiasemien MAC-osoitteet ja/tai salausavain. Tämän jälkeen tukiasemat voidaan sijoittaa kuuluvuusalueen rajamaille ja liittää ne verkkoon salausavaimen avulla.

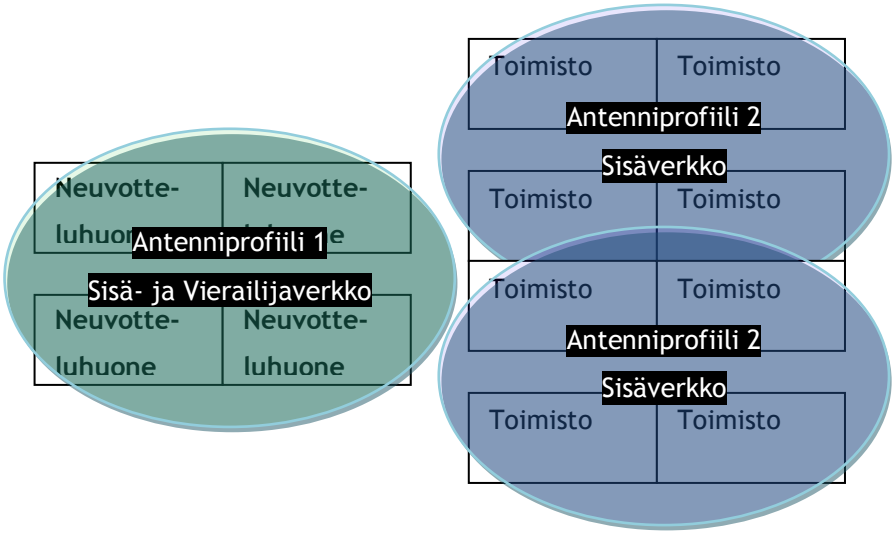
IP services-valikosta voidaan määrittää staattisien reittien osoitteita, alias-osoitteita, DNS-palvelimien osoitteita, NTP-palvelimien osoitteita ja ARP-taulun osoitteita. Nämä asetukset tulee määrittää vastaamaan verkossa olevia asetuksia. Staattisiksi reiteiksi voidaan määrittää kytkinten välisiä yhteyksiä. Alias-osoitteilla voidaan nimetä tunnettuja palvelinten tai palveluiden IP-osoitteita. DNS-palvelimien osoitteisiin voidaan lisätä verkossa olevien DNS-palvelimien osoitteet. NTP (network time protocol)-palvelimen lisäyksellä saadaan päivämää-

rä ja aika synkronoitua tietyin väliajoin Ringmaster-palvelimelle. ARP tauluun voidaan lisätä haluttaessa osoitteita, mutta kytkin kuitenkin ylläpitää aina automaattisesti ARP-taulua.

VLAN:eja kannattaa luoda haluttujen palveluiden mukaan. VLAN:lla pystytään eristämään verkkoja toisistaan. Ringmaster-palvelimella on aina pakko olla yksi Default niminen VLAN. Default VLAN kannattaa jättää ylläpitoverkoksi. Ylläpitoverkko määritetään kytkimen asetuksista. Luomalla oma VLAN-verkko jokaiselle palvelulle voidaan eristää liikennettä toisistaan. Merkitsemällä (TAG) palveluiden VLAN liikenteen, voidaan sisäverkossa ohjata liikenne haluttuun osoitteeseen tai rajata pääsy tiettyihin osoitteisiin. Osoitemääritykset tulee tehdä myös sisäverkon muihin laitteisiin ja rajoitukset määritetään ainoastaan verkon laitteissa.

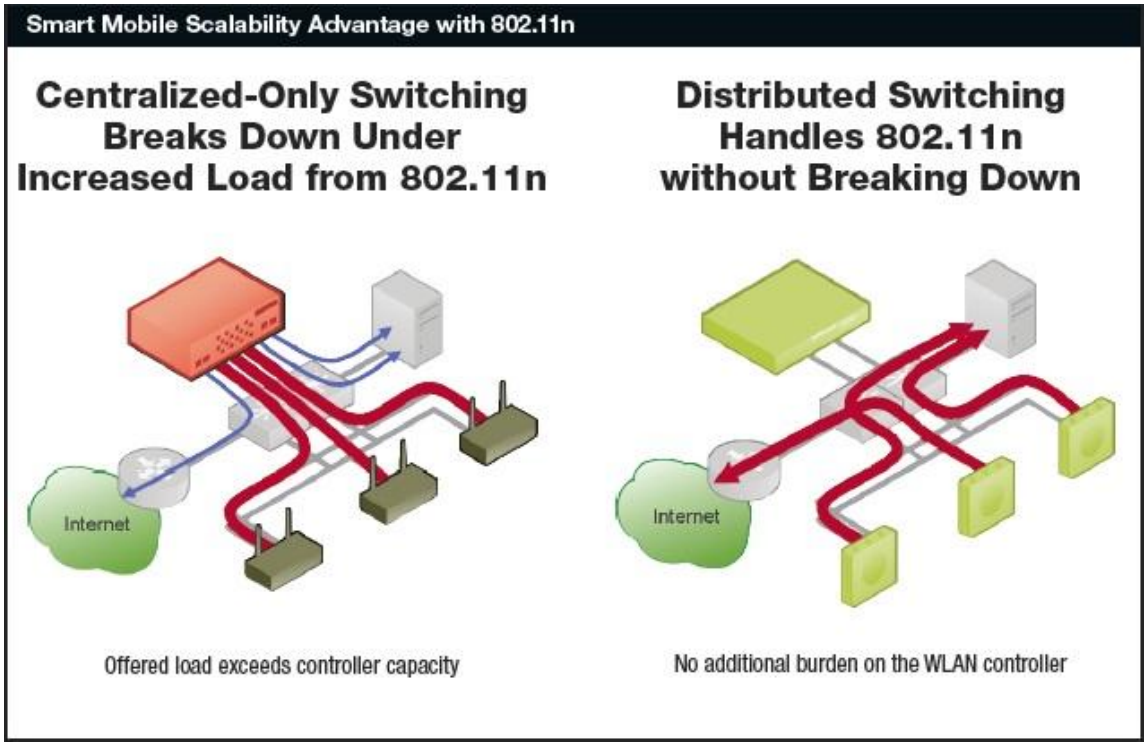
Kun VLAN-verkot on muodostettu muualle sisäverkkoon, voidaan ne muodostaa MX-kytkimelle Ringmaster –ohjelmalla. Configuration -välilehden organizer –paneelista valitaan haluttu kytkin, painetaan system ja VLANs. Tässä näkymässä valitaan tasks –paneelista create VLAN. Esiin tulee ohjattu toiminto mistä määritetään VLAN. Ohjatussa toiminnossa määritetään VLAN:in ID, IP-osoite ja aliverkonpeitteen bittien määrä. Näiden tietojen lisäksi voidaan määrittää nimi VLAN:ille ja mitä porttia tai porttiryhmiä VLAN käyttää.

Antenneja voidaan jakaa antenniprofiileihin. Antenniprofiileja tulee olla aina vähintään yksi. Oletusantenniprofiilina on Default, mihin kuuluvat kaikki antennit. Uusia antenniprofiileja voidaan luoda organizer-paneelin Wireless valikon alla olevasta Radio Profiles-valikosta, mistä voidaan määrittää myös mihin palveluun mikäkin antenniprofiili kuuluu. Jakamalla antenneja eri profiileihin ja määrittämällä eri palveluille eri antenniprofiileja, voidaan rajoittaa eri verkkojen kuuluvuusalueita. Antenniprofiilit-esimerkkikuvassa nähdään esimerkki siitä miten profiileilla voidaan rajoittaa alueita. Kuvassa neuvotteluhuoneisiin on määritetty toimimaan sisä- ja vierailijaverkkopalvelu ja toimistoihin ainoastaan sisäverkkopalvelu.




Kuva 8: Antenniprofiilit-esimerkki

Local switching Valikosta voidaan luoda niin kutsuttuja VLAN-profiileja. Profiileihin voidaan määrittää kuulumaan VLAN:eja ja tukiasemia. Näiden määritysten perusteella, samaan VLAN-profiiliin kuuluvat tukiasemat voivat kommunikoida suoraan oman porttinsa kautta määritetyssä VLAN-verkoissa. Tällä ominaisuudella voidaan nopeuttaa verkon toimintaa ja se on erittäin olennainen asetus etenkin WoWLAN-puheluiden kanssa, koska puhelussa on erittäin tärkeää sujuva tiedonsiirto. Sujuvampi tiedonsiirto saadaan, kun kaikki tieto ei mene MX-kytkimen kautta. Havainnollistava esimerkki on kuvassa tietoliikenteen ohjaus. (Trapeze Networks 2008a, 193.) Tässä projektissa ei kuitenkaan perehdytä WoWLAN puheluihin, mutta sujuvampi tiedonsiirto on aina tavoiteltava asia.




Kuva 9: tietoliikenteen ohjaus (Trapeze Networks 2009a, 6)

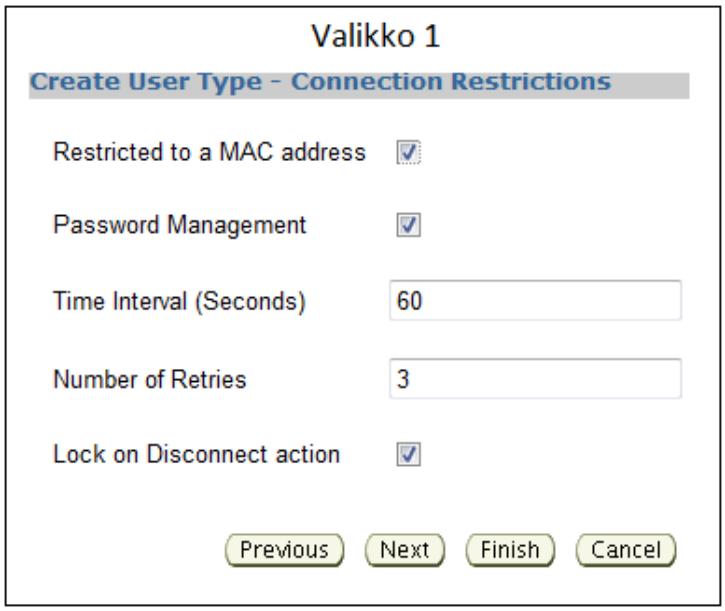
## 3.2 Vierailijaverkko

Vierailijaverkkopalvelua varten tarvitsee määrittää SmartPass-palvelimelle järjestelmän käyttäjät, lisenssit ja verkon käyttäjäprofiilit. Ringmaster- palvelimelle tarvittavat asetusten muutokset käydään läpi luvussa Ringmaster-palvelimelle tehtävät muutokset. Esimerkissä on kuitenkin selitetty ainoastaan kuinka todennus suoritetaan selaintodennuksella. Todennuksen voi toteuttaa kuitenkin myös open access-palveluprofiililla. Tämä ei kuitenkaan ole suositeltavaa yritys verkossa, sillä Open access-menetelmässä yhteys on avoinna kaikille.

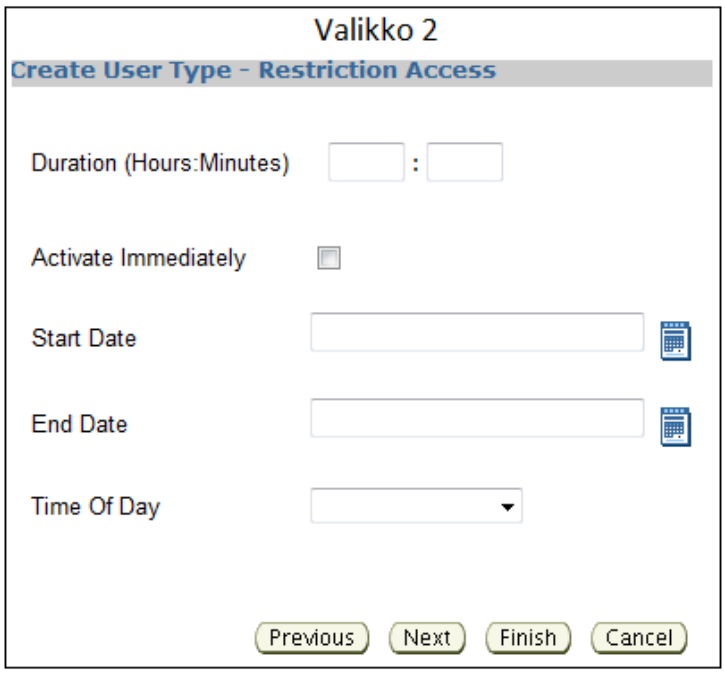
### Smartpass-palvelimelle tehtävät muutokset

Smartpass-sovelluksen selainkäyttöliittymässä verkon käyttäjäprofiilit nähdään ja niitä voidaan muokata User type -välilehden user type management -valikosta. Valikossa valitaan oikeassa reunassa olevasta valikosta haluttu toiminto siltä riviltä, jota halutaan muuttaa. Uusia käyttäjätyyppejä pystytään luomaan create user type -valikosta. Valikossa määritetään ensin käyttäjätyypille nimi, VLAN, johon käyttäjätyypillä luodut tunnukset kuuluvat sekä se, sallitaanko tunnuskohtainen päättymispäivän määrittäminen ja kuvaus käyttäjätyypistä. Kuvaukseen kannattaa kirjoittaa kyseistä käyttäjätyyppiä varten suunnitellut rajoitukset, sillä rajoitukset eivät tule ilmi tunnusta luodessa kuin käyttäjänimestä ja kuvauksessa. Mikäli käyttäjätyypille ei haluta rajoituksia, voidaan valita "finish", muuten painetaan next-painiketta, josta

päästään seuraavaan valikkoon (kuva 10 Smarpass rajoitukset 1), missä voidaan määrittää rajoitteita kyseisellä tunnustyypillä luoduille tunnuksille. Lisää rajoitteita voidaan määrittää painettaessa next-painiketta uudestaan (kuva 11 Smartpass rajoitukset 2). Halutut rajoitukset määritettyä voidaan painaa finish-painiketta, minkä jälkeen palvelin luo määritetyn tunnus-tyypin.




Kuva 10: Smartpass-rajoitukset 1




Kuva 11: Smartpass-rajoitukset 2

Valinnaisina ominaisuuksina voidaan muokata käyttäjälle näkyvää sisäänkirjautumisikkunaa tai käyttäjälle tulostettavaa verkkoonliittymisohjetta. Verkkoonliittymisohjeesta käytetään nimitystä kuponki. Kuponkia voidaan muokata Smartpass-palvelimen selai käyttöliittymällä. Valikoissa tulee mennä setup-valikon coupon management-valikkoon. Valikossa näkyy kaikki luodut kupongit ja lisää kuponkeja voidaan luoda painamalla add coupon-nappia. Kuponkeja tehdään html koodia muokkaamalla. Esimerkkinä on kuitenkin oletuskuponki, joten kupongin muokkaus ei vaadi erityistä ohjelmointitaitoa. Ennen kupongin muokkausta tulee kuitenkin nimetä kupongille SSID-nimi, mikä määrittää missä SSID:ssä kuponkia käytetään.

Web-portaalin sisäänkirjautumisikkunaa voidaan muokata MX-kytkimen selainkäyttöliittymällä. Valikosta tulee mennä maintain välilehdelle ja sieltä Manage web portal access page. Tästä valikosta päästään ohjattuun toimintoon, minkä avulla pääsee muokkaamaan sisäänkirjautumissivua. Sisäänkirjautumissivua voidaan muokata ainoastaan otsikon, tervetulotekstin, varoitustekstin ja otsikkokuvan osalta. Tekstien muokkaamisten tekemiseen ei tarvitse osata mitään ohjelmointikieltä. Otsikkokuva ladataan palvelimelle selaamalla se tietokoneen hakemistoista. Kaikkia sisäänkirjautumisikkunan tekstejä ei voi muokata, eikä tekstien sijoituspaikkoja voi muuttaa. Tekstejä kirjoittaessa tulee huomioida myös, ettei kytkin osaa tulkita kuin englannin kielessä käytettyjä kirjaimia.

Ringmaster-palvelimelle tehtävät muutokset

Vierailijaverkkoa varten Ringmaster- palvelimen asetuksiin tulee lisätä VLAN, langaton palveluprofiili, web-kirjautumisen säännöt ja haluttaessa radioprofiili. Kaikki asetusten lisäykset voidaan tehdä Ringmaster-sovelluksen configuration-välilehdeltä.

VLAN:eja voidaan luoda system-valikon VLANs-valikosta. Task-paneelista valitaan create vlan ja päästään ohjattuun VLAN:in luontiin. VLAN:ina määrittäessä tulee tietää VLAN:in nimi, ID-tunniste, portti tai porttiryhmä, IP-osoite ja tieto siitä halutaanko kyseisessä VLAN:issa käyttää Trapezen DHCP-palvelinta vai verkossa olevaa DHCP-palvelinta. Kummatkin DHCP-palvelimet eivät voi olla yhtä aikaa päällä. VLAN:in tietoja määrittäessä tulee huomioida että samat asetukset tulee olla määritettynä muuallekin verkkoon.

Langaton palveluprofiili voidaan luoda wireless-valikon alta löytyvästä wireless services-valikosta. Vierailijaverkkoa varten web-kirjautumista käyttävän palveluprofiilin voi luoda valitsemalla task-paneelista web-portal service profile ja seuraamalla ohjatun toiminnon ohjeita. Ohjatussa toiminnossa määritetään palveluprofiilin nimi, SSID, salaustyyppi (salattu tai salaamaton), mihin VLAN:iin palveluprofiili kuuluu, mitä ACL määrityksiä halutaan käyttää, mitä todennuspalvelinta tai todennuspalvelin ryhmää halutaan käyttää, mitä radio profiilia

halutaan käyttää ja mitä langattoman verkon standardeja sallitaan käytettävän. Vierailijaverkkoa varten voidaan käyttää Smartpass-palvelinta todennuspalvelimena. Halutessa voidaan käyttää myös paikallista todennusta, jolloin käyttäjätunnukset luodaan Ringmaster-palvelimella.

Web-kirjautumisen säännöt voidaan luoda AAA valikon alta löytyvästä valikosta web access rules. Tasks-paneelista valittaessa web network access avautuu ohjattu toiminto web-kirjautumissääntöjen luomiseksi. Ohjatussa toiminnossa määritetään mitä käyttäjiä säännöt koskevat, mikä SSID sääntöjä käyttää ja mitä todennuspalvelinta tai todennuspalvelin ryhmää käytetään käyttäjäntodennukseen tai käyttäjäntodennukseen ja tilastointiin. Käyttäjiksi voidaan merkitä ** jolloin sääntö koskee kaikkia käyttäjiä. Tilastointipalvelimen määrittäminen ei ole pakollista ja sen voi jättää pois päältä. Tilastointipalvelinta voidaan kuitenkin käyttää, mikäli halutaan seurata käyttäjiä laskutuksen tai jonkin muun syyn takia.

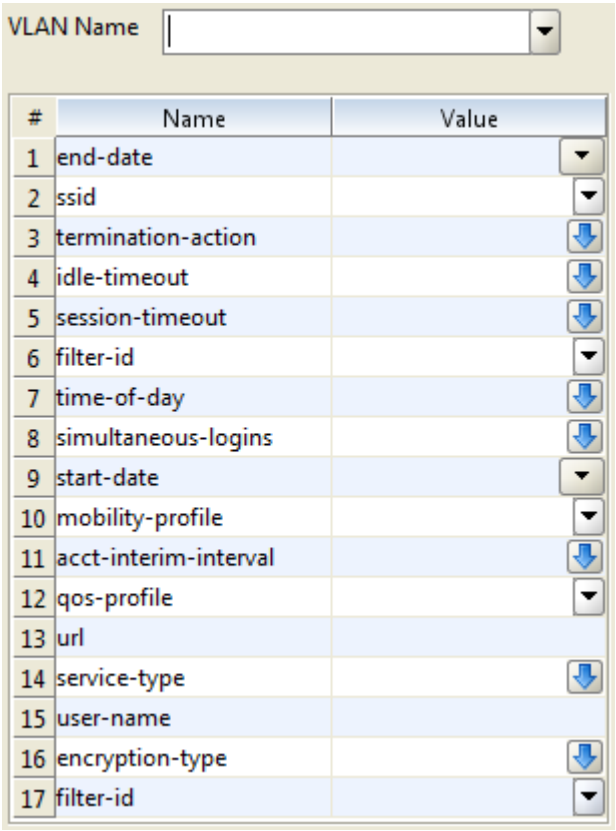
Radioprofiileja voidaan luoda wireless-valikon radio profiles-valikosta valitsemalla tasks-paneelista create radio profile. Avautuvassa ohjatussa toiminnossa määritetään radioprofiilin nimi, mitä antenneja profiiliin kuuluu ja mikä tai mitkä langattomat palvelut profiilia käyttää. Radioprofiilien avulla pystytään rajaamaan SSID:n kuuluvuusaluetta tukiasemien peittoalueiden mukaan.

## 3.3 Työntekijäverkko

Työntekijäverkolla tarkoitetaan verkkoa, mistä on pääsy yrityksen sisäverkkoon. Tämän takia tulee tarkkaan miettiä mitä todennusmenetelmää käytetään ja mihin kyseisenverkon kautta sallitaan pääsy. Tietoturvakartoitukseni perusteella luotettavimmaksi vaihtoehdoksi osoittautui 802.1x todennusmenetelmä ja AES salausmenetelmä. Ringmaster-ohjelmistolla pystytään kuitenkin luomaan myös useamman eri todennusmenetelmän ja salausmenetelmän yhdistelmiä. Työntekijäverkon todennuspalvelimena voidaan käyttää sisäverkon todennuspalvelinta tai paikallista käyttäjätunnusten todennusta.

Työntekijäverkko voidaan luoda Ringmaster-ohjelmistolla. Työntekijäverkon VLAN- ja radioprofiili tehdään samalla tavalla kuin vierailijaverkossa. VLAN:ien rajoitukset, ja paikallista todennusta varten, voidaan luoda käyttäjätunnuksia ja tunnusryhmiä, AAA valikon alta löytyvästä local user database valikosta. Tässä valikossa voidaan lisätä myös paikallisista MAC-osoite suodatusta varten sallitut MAC-osoitteet. Käyttäjiä ja MAC-osoitteita varten tulee tehdä kuitenkin ryhmä. Ryhmät luodaan ohjatulla toiminnolla task-paneelin create user group- ja create MAC user group-painikkeista. Ryhmiä luodessa voidaan määrittää tarkat rajoitukset käyttäjien tunnusten voimassaoloajoista ja muista vaatimuksista tunnuksia koskien (kuva 12 ryhmän käyttäjien rajoitusmahdollisuuksia). Password management-painikkeesta avautuu

ponnahdusikkuna mistä voidaan säätää salasanan yrityskertojen määrää ja salasanan vähimmäispituutta. Käyttäjätunnuksia tai sallittuja MAC-osoitteita voidaan lisätä painamalla create user- tai create mac address user-painikkeesta. Käyttäjiä lisätessä voidaan käyttäjälle määrittää käyttäjätunnus, salasana ja ryhmän kaltaisesti rajoitteita (kuva 12 ryhmän käyttäjien rajoitusmahdollisuuksia). Sallittua MAC-osoitetta lisätessä voidaan määrittää MAC- osoite tai MAC-osoite avaruus mitä sallitaan. MAC-osoitteille voidaan myös määrittää erillisiä tarkennettuja rajoitteita (kuva 12 ryhmän käyttäjien rajoitusmahdollisuuksia).




Kuva 12: ryhmän käyttäjien rajoitusmahdollisuuksia

Sisäisen verkon RADIUS-palvelin voidaan lisätä AAA valikon RADIUS-valikosta. RADIUS-palvelimen lisäksi pitää tehdä RADIUS-palvelinryhmä. RADIUS-palvelinryhmän voi luoda create RADIUS server group-painikkeesta. RADIUS-palvelimien lisäyksen voi tehdä tasks paneelin create RADIUS server-painikkeesta. RADIUS-palvelimen lisäksi voidaan lisätä RADIUS DAC (Dynamic Authorization Client)-palvelin painamalla create RADIUS DAC-painikkeesta tasks-paneelista.

802.1x access rules-valikosta voidaan luoda 802.1x kirjautumisen säännöt. Sääntöihin määritetään mitä verkkosääntö koskee ja mitä todennusmenetelmää kyseessä olevassa verkossa saa käyttää. Vaihtoehtoina ovat EAP-MD5 offload, PEAP offload, local EAP-TLS ja external authen-

tication server. Kun todennusmenetelmän on valittu, voidaan valita mitä todennuspalvelinryhmää sääntö koskee. Tarvittaessa voidaan sallia myös tilastointipalvelimen käyttöä varten ryhmä.

Palveluprofiileja voidaan luoda wireless services-valikosta. Tasks-valikosta voidaan valita haluttu palveluprofiili. Työntekijäverkkoa varten voidaan valita 802.1x service profile tai custom service profile. 802.1x service profile valikossa määritetään profiilille nimi, SSID, todennus- ja salausmenetelmä, todennuspalvelinryhmä, VLAN, antenniprofiili ja sallitut yhteysprotokollat.

## 3.4 Laitteiden sijoittelu ja kuuluvuuksien testaus

Laitteiden sijoittelu-luvussa käydään läpi kaikki asiat mitä tulee ottaa huomioon laitteiden sijoittelussa. Kytkinten ja palvelinten sijoittelu on jätetty pienemmälle huomiolle, sillä tukiasemien oikea sijoittelu on erittäin olennainen osa langattoman verkon rakentamista. Huonolla sijoittelulla tukiasemien kuuluvuus ei peitä haluttua aluetta, tukiasemat kuuluvat alueella mihin niiden ei tulisi kuulua tai tukiasemat häiritsevät toistensa signaaleja.

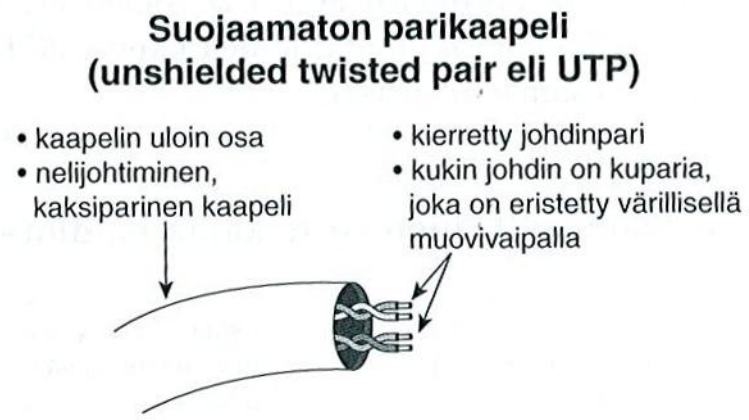
Kytkimet ja palvelimet tulee sijoittaa kuivaan ja hyvin ilmastoituun paikkaan. Erillisessä lukitussa palvelinhuoneessa tai kytkinkaapissa laitteet pysyvät viileinä ja kuka tahansa ei pääse niihin fyysisesti käsiksi.

Kaapelointia suoritettaessa tulee huomioida minkä tyyppisiä verkkojohtoja käytetään. Verkkojohdoissa on määritetty eri kategorioita. Kategorioista käytetään yleisesti lyhennettä CAT ja kategorian numero tai numeroa ja kirjainta. Alla olevassa taulukossa on listattu PCmag uutissivuston julkaisema lista eri kategorioiden johtojen nopeuksista.

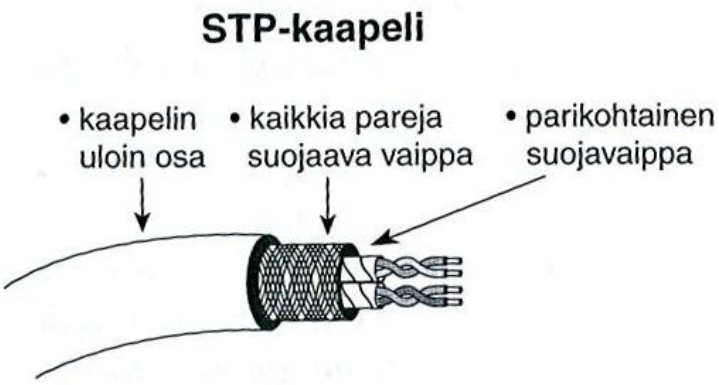
Taulukko 10: Kaapelien kategoriat (PC Magazine)

| kategoria | kaapeli tyyppi | taajuus | tiedonsiirto |
|---|---|---|---|
| CAT 1 | UTP | Analog voice | |
| CAT 2 | UTP | | 1 Mbps |
| CAT 3 | UTP/STP | 16 MHz | 4 Mbps |
| CAT 4 | UTP/STP | 20 MHz | 16 Mbps |
| CAT 5 | UTP/STP | 100 MHz | 100 Mbps |
| CAT 5e | UTP/STP | 100 MHz | 1 Gbps |
| CAT 6 | UTP/STP | 200 MHz | 10 Gbps (<10 m) |
| CAT 6a | UTP/STP | 500 MHz | 10 Gbps (>10 m) |
| CAT 7 | STP | 600 MHz | 10 Gbps |
| CAT 7a | STP | 1000 MHz | 40 Gbps (<15 m) |

Kaapelin kategorian lisäksi tulee huomioida käytetäänkö suojaamatonta parikaapelia (UTP), vai suojattua parikaapelia (STP). Suojaamatonta parikaapelia voidaan käyttää useimmissa paikoissa. Suojattua parikaapelia käytetään yleisesti paikoissa missä on paljon sähkömagneettisia häiriöitä. Suojattu parikaapeli on jäykempää kuin suojaamaton parikaapeli. Suojattu parikaapeli vähentää kuitenkin huomattavasti sähkömagneettisen häiriön vaikutusta. Mikäli kaapeliin kohdistuu sähkömagneettista häiriötä, voi kaapelissa liikkuva data vääristyä. Mikäli data muuttuu matkalla, vastaanottava tietokone voi tulkita ykkösen nollaksi tai tietokone ei saa lähetyksestä ollenkaan selvää. Sähkömagneettista säteilyä voi tulla muista johtimista tai kaapelin lähellä olevista sähköisistä laitteista. Alapuolella on kuvat suojaamattomasta ja suojatusta parikaapelista. (Wendell 2004, 72-74.)




Kuva 13: Suojaamaton parikaapeli (Wendell 2004, 72)




Kuva 14: Suojattu parikaapeli (Wendell 2004, 74)

Tukiasemien sijoittelun voi suunnitella Ringmaster-ohjelmiston RF Planning-ominaisuuksilla. Palvelimelle voi ladata rakennuksen pohjapiirrokset kuvana tai cad-tiedostona. Tämän jälkeen määritellään seinämateriaalit ja tarvittavat peittoalueet. Näiden tietojen perusteella Ringmaster pystyy laskemaan tarvittavien tukiasemien määrän ja suositella sijoituspaikkoja. Laskennan jälkeen suunnitelmaa pystyy kuitenkin muuttelemaan ja laskemaan uudestaan. Pitää kuitenkin muistaa, että suunnitteluun tarvitaan RMTS-PLAN lisenssi.

RF Planning ei ole kuitenkaan kuin apuväline ja suunnittelu voidaan tehdä yksinkertaisessa tilassa helposti kokeilemalla kuuluvuutta. Kokeilua varten tulee yhden verkon olla asetettuna majakka (beacon)-toiminto päällä ja suurinpiirtein oikeassa paikassa. Tällöin voidaan mennä halutun alueen reunamille ja kokeilla mitä tietokone antaa kuuluvuudeksi. Kuuluvuutta voidaan testata esimerkiksi Network Stumbler -ohjelmalla. Ohjelmistoon tutustutaan tarkemmin testauksen Network Stumbler luvussa.

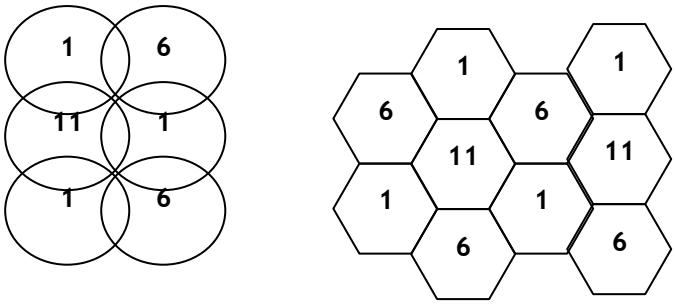
Taajuudet ja kanavat

Mikäli käytössä on useita tukiasemia lähekkäin, tulee huomioida tukiasemien signaalien taajuudet Taajuuksia voidaan muuttaa vaihtamalla tukiaseman käyttämää kanavaa. 2,4 GHz verkossa jokainen kanava käyttää 22 MHz. Tällöin jää kolme kanavaa, jotka eivät käytä päällekkäisiä taajuuksia. Käytettävissä olevat kanavat ja taajuudet on merkitty alla olevaan taulukkoon. Käyttämällä punaisella tekstillä merkittyjä kanavia 1,6 ja 11, päästään parhaimpiin tuloksiin (Hakala ym. 2006, 294). Tämä johtuu siitä, etteivät kyseisten kanavien taajuudet mene päällekkäin ja saadaan silti käyttöön kolme eri kanavaa. Eri taajuuksilla olevia kanavia haluttaan käyttöön sen takia, etteivät samalla kuuluvuusalueella olevat tukiasemat häiritsisi toisiaan. Alla oleva taulukko ”2,4 GHz-kanavat ja -taajuudet” on tehty ficoran määräys 15 ja Puskan kirjan perusteella (Viestintävirasto 2009, 14; Puska 2005, 43-45). Taulukoita katsoessa tulee kuitenkin huomioida minkä maan määräysten mukaiseksi laite on tehty. Sinisellä merkityt 12 ja 13 kanavat eivät ole sallittuja kanavia kaikkialla, Euroopassa ne kuitenkin ovat.

Taulukko 11: 2,4 GHz-kanavat ja -taajuudet

| Kanava | Alin taajuus | Keskitaajuus | Ylin taajuus |
|---|---|---|---|
| 1 | 2,401 | 2,412 | 2,423 |
| 2 | 2,404 | 2,417 | 2,428 |
| 3 | 2,411 | 2,422 | 2,433 |
| 4 | 2,416 | 2,427 | 2,438 |
| 5 | 2,421 | 2,432 | 2,443 |
| 6 | 2,426 | 2,437 | 2,448 |
| 7 | 2,431 | 2,442 | 2,453 |
| 8 | 2,436 | 2,447 | 2,458 |
| 9 | 2,441 | 2,452 | 2,463 |
| 10 | 2,446 | 2,457 | 2,468 |
| 11 | 2,451 | 2,462 | 2,473 |
| 12 | 2,456 | 2,467 | 2,478 |
| 13 | 2,461 | 2,472 | 2,483 |

Kuvassa 15 Tukiasemien kanavien sijoittelu ja määrittely on kaksi esimerkkiä tukiasemien sijoittelua varten. Esimerkit on tehty Puskan kirjan perusteella (Puska 2005, 134).



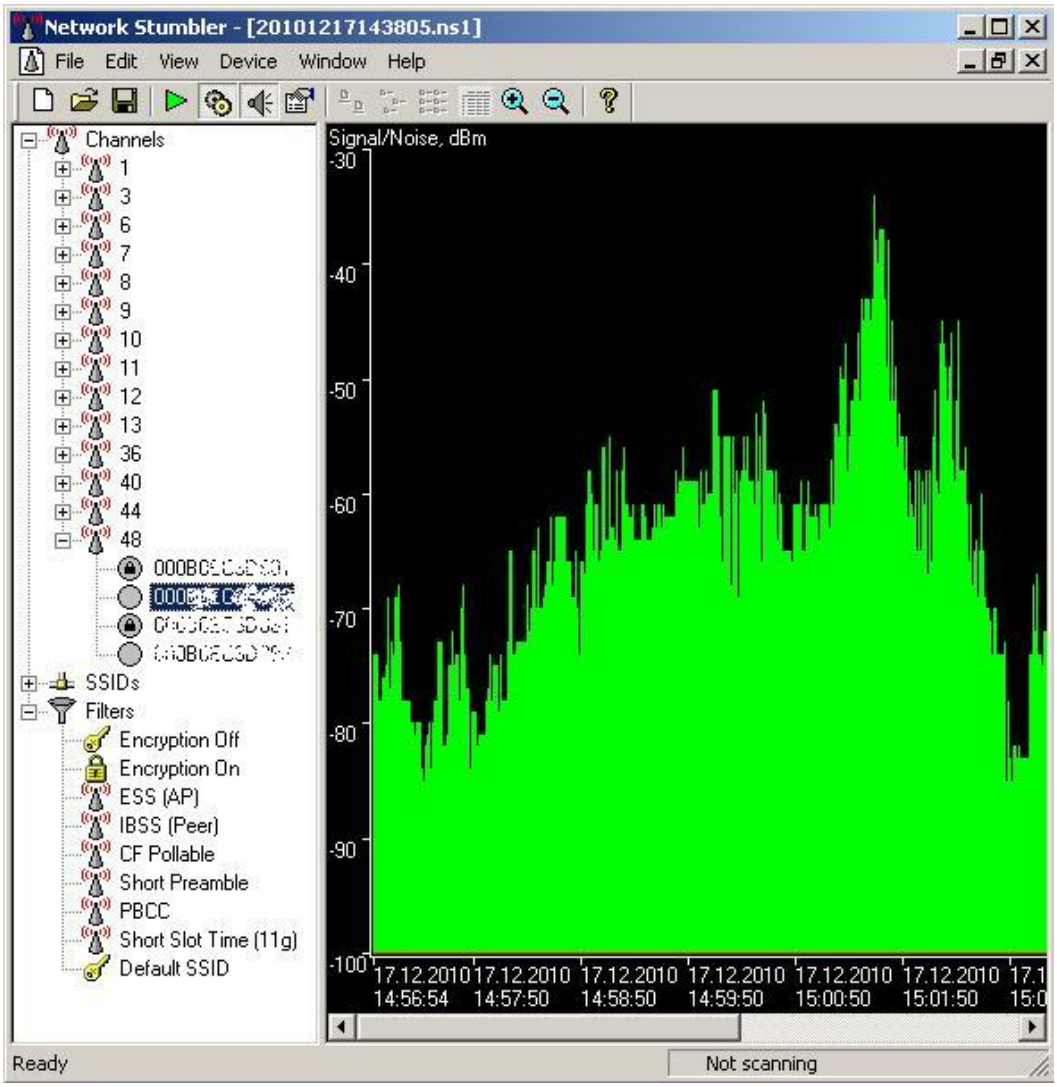

Kuva 15: Tukiasemien kanavien sijoittelu ja määrittely

5 GHz taajuudella toimivat 802.11a ja 802.11n standardit. 5 GHz taajuus on jaettu kolmeen taajuuskaistaan. Suomessa viestintävirasto on määrittänyt sallituiksi kaistoiksi 5,15GHz - 5,25GHz, 5,25GHz – 5,35GHz ja 5,470GHz - 5,725GHz (Viestintävirasto 2009, 14).

## 3.5 Verkon ja kuuluvuuksien testaus

Testaus-luvussa ohjeistetaan kuinka voidaan testata tukiasemien kuuluvuutta ja selvitetään mitä asioita tulee testata valmiista järjestelmästä. Testaamalla voidaan todeta järjestelmän toimivuus ja ennaltaehkäistä ongelmatilanteita.

Network Stumbler on ilmaisohjelmisto, jolla voidaan mitata verkon kuuluvuutta BSSID:n perusteella. Ohjelmassa BSSID:itä voi katsoa SSID:n tai kanavan mukaan. Ohjelmisto on hyvä verkkojen testauksessa ja sen avulla pystytään helposti toteamaan onko langattomassa verkossa päällekkäisiä peittoalueita samalla kanavalla. Alapuolella on kuvankaappaus Network Stumbler ohjelmankäyttöliittymästä.




Kuva 16: Network Stumbler-käyttöliittymä

Käyttöliittymän vasemmassa palkissa voidaan valita mitä BSSID:tä kuunnellaan ja nähdään mitkä BSSID:t kuuluvat milläkin kanavalla tai mitkä BSSID:t mainostavat mitäkin SSID:tä. Mikäli tukiaseman asetuksista on määritetty yleislähetyksiin vastaus pois päältä, tukiasema ei näy listassa. Oikean puolen paneelista voidaan nähdä signaalin kuuluvuus ja aika. Helpoiten verkon testauksen saa suoritettua laittamalla ohjelmiston nauhoittamaan ja valitsemalla lähimpänä olevan tukiaseman BSSID:n kanavavalikosta. Tämän jälkeen voidaan kävellä tietokoneen kanssa halutun kuuluvuusalueen ympäri ja tarkistaa ettei samalla alueella kuulu kahta tu-

kiasemaa, jotka käyttävät samaa kanavaa. Mikäli on tilanne missä mikään tukiasema ei kuulu tai samassa paikassa kuuluu kaksi tukiasemaa, jotka käyttävät samaa kanavaa. Pitää tukiasemien kanavaa, sijaintia tai kuuluvuudentehoa vaihtaa.

Verkon toimivuustestaus

Järjestelmää testattaessa on hyvä kokeilla ensin itse millä laitteilla järjestelmä toimii. Tällöin voidaan ongelmatilanteessa todeta järjestelmän toimineen kyseisellä laitteella tai ohjelmistolla. Mikäli laite tai ohjelmisto on toiminut testeissä, voidaan olettaa vian olevan käyttäjän laitteessa. Täten voidaan alkaa selvittämään onko vika asetuksissa vai onko laite rikki. Mikäli laitetta ei ole aikaisemmin kokeiltu, joudutaan miettimään voiko järjestelmän jossain asetuksessa olla vikaa vai eikö järjestelmä vain tue kyseistä laitetta.

Käytännön testauksessa katsotaan osaako oletetut käyttäjät käyttää järjestelmää. Periaatteessa testauksessa testataan siis annettuja ohjeistuksia. Testauksen perusteella voidaan todeta onko käyttöohjeet tarpeeksi selkeät vai tuleeko niitä kehittää. Lisäksi käyttäjien testauksessa voi järjestelmästä ilmetä ennalta arvaamattomia tositilanteen tapahtumia.

Kokeiluissa tulee järjestelmänvalvojan olla mukana huomatakseen mahdolliset puutteet tai parannusmahdollisuudet heti käyttäjän eleistä, ilmeistä tai kommenteista. Lisäksi järjestelmänvalvojan on oltava tavoitettavissa ongelmatilanteissa, jolloin voidaan ohjelmistoa ja järjestelmää tarkkailla tarkemmin mahdollisen vian selvittämiseksi. Tällöin saadaan selville järjestelmän heikkouksia tai voidaan korjata mahdollisia virheitä.

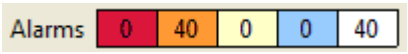
Ensimmäisessä käyttötestauksessa ilmeni Web-portal todennuksessa odottamaton heikkous. Heikkous ilmeni kun vierailijan tietokone ei saanut sisäänkirjautumisikkunaa auki. Syynä tähän oli selaimen asetukset, mihin oli määritetty vierailijan oman verkon proxy-palvelimen osoite. Verkkoon kirjautuessa tulisi kuitenkin selaimen olla säädettynä hakemaan lähiverkon asetukset automaattisesti. Vierailijan yrityksen tietohallinto oli kuitenkin estänyt asetuksen muuttamisen. Jotta kyseinen käyttäjä olisi voinut käyttää verkkoa, olisi verkossa pitänyt olla eri todennusmenetelmä käytössä.

Verkon ylläpito

Ylläpitoa voi tehdä seuraamalla lokitietoja, uhka- ja varoitusilmoituksia, päivityksillä, vikatilanteita ja laitevikoja selvittämällä ja korjaamalla.

Yleistä tarkastelua järjestelmän toimivuudesta voi suorittaa Ringmaster –ohjelmiston Monitor-välilehdellä. Monitor-välilehdeltä nähdään graafisesti laitteiden tila, hälytykset, käyttäjät ja liikenteen määrä. Laitteiden ja antennien tilana voi olla yhteydessä (UP), ei yhteyttä (DOWN), ei tiedossa (Unknown) tai pois käytöstä (Disabled). Hälytykset, käyttäjät ja liikennetietoja voidaan tarkkailla taulukossa ja graafisessa kaaviossa. Lisäksi tila, käyttäjät ja liikennetiedoista voidaan painaa ”Details” nappia mistä nähdään tarkemmat tiedot. Hälytykset ruudun ”Details” nappia painamalla päästään ”alarms” välilehdelle, missä nähdään hälytykset tarkemmin.

Uhka- ja varoitusilmoituksia pystytään seuraamaan Ringmaster –ohjelmistolla. Ohjelmiston Security-välilehdellä nähdään kaikki hälytykset yleisesti. Hälytystyyppiä painamalla ohjelmisto siirtyy Alarms-välilehdelle. Alarms-välilehdellä voi hälytyksiä tarkastella tarkemmin ja nähdä kaikki saatavilla olevat tiedot hälytyksen aiheuttaneesta laitteesta tai verkosta. Alarms-välilehdeltä hälytyksiä voidaan myös käsitellä, merkitsemällä ne huomioiduksi tai poistamalla ne. Alarms-välilehdeltä voidaan myös päättää mistä kaikista asioista järjestelmä tekee hälytyksen ja minkä tasoisen hälytyksen mistäkin asiasta tehdään. Nämä asetukset löytyvät Task –paneelin setup-kohdasta avautuvassa ponnahdusikkunassa. Hälytykset on jaettu neljään osaan ”Critical”, ”major”, ”minor” ja ”info”, eli kriittisiin, suuriin, pieniin ja tiedotuksiin. Eri hälytysten määrät nähdään suoraan ohjelmiston oikeasta alakulmasta, mistä painama pääsee suoraan kyseisen hälytystason Alarms-välilehdelle. Hälytykset paneelikuvassa näkyy eri väreillä hälytystasot ja oikeanpuolimaisena hälytykset yhteensä.




Kuva 17:hälytykset-paneeli

Lokitietoja seuraamalla voidaan selvittää missä vaiheessa tai mistä johtuen jokin ongelma johtuu. Eri lokeja pääsee lukemaan SmartPass –palvelimelta, MX-kytkimeltä ja Ringmaster –palvelimelta. SmartPass –palvelimelta lokitiedot löytyvät Maintanance-välilehdeltä. MX-kytkimellä lokitiedot löytyvät Monitor-välilehden Log-valikosta. Ringmaster –palvelimella lokitiedostot löytyvät Maintanance-välilehden Current Log-valikosta. Kaikissa näissä järjestelmissä lokitietoja voidaan suodattaa lokimerkinnän tyypin mukaan, tarvittavan tiedon löytämisen helpottamiseksi. Lisäksi jokaisesta lokin tapahtumasta on tarkka tapahtuma-aika. Mikäli tiedossa on ongelman ilmenemisajankohta, on helppo lokista tarkistaa mitä silloin on tapahtunut.

Palvelinten päivitys tapahtuu ajamalla uusin päivityspaketti palvelimella. MX-kytkimen päivittäminen voidaan suorittaa Ringmaster-ohjelmistolla. Ohjelmiston Devices -välilehdeltä valitaan Task –paneelista ”Image Install”, tämän jälkeen esiin tulee ponnahdusikkuna mistä vali-

taan mikä päivitys halutaan asentaa millekin MX-kytkimelle. Päivitykset saadaan laitteiston toimittajalta tai Trapezen tukisivustolta.

# 4 Kehitysehdotukset ja loppupäätelmä

Tietoturva on yksi tärkeimmistä kehitysmahdollisuuksista. Tietoturvan kannalta voitaisiin määrittää tarkasti kaikki langattomiin verkkoihin liittyvät riskit. Riskien perusteella pystyttäisiin hahmottamaan tarvittava tietoturvataso. Tasoissa voitaisiin määrittää verkossa kulkevien tietojen kriittisyys. Erittäin kriittisiin tietoihin pääsy voitaisiin kieltää kokonaan. Vähemmän kriittisiin tietoihin pääsylle voitaisiin määrittää erilaisia tietoturvan kannalta tarvittavia vaatimuksia. Näihin määrityksiin Trapeze antaa hyvät mahdollisuudet, sillä rajoituksia voidaan tehdä muun muassa ajan, sijainnin, ohjelmiston, käyttäjätunnuksen ja asennettujen ohjelmistojen perusteella.

Kehityksenä voidaan pitää myös langattoman verkon laajentamista. Laajentamisen suunnitteluun tulee ottaa huomioon tarvittavat laitteet, lisenssit ja laitteiden sijoittelu. Kaikkien toimipisteiden kannalta tulisi kuitenkin kartoittaa ensin langattoman verkon tarpeellisuus.

Laajennettaessa verkkoa useiden toimipisteiden kattavaksi verkoksi olisi kannattavaa miettiä mahdollista VoWLAN (Voise over WLAN)-puheluiden mahdollisuutta. VoWLAN-verkko voisi tuoda säästöjä toimipisteiden välisten tai yrityksen sisäisten puheluiden osalta. Aiheesta tulisi kuitenkin ensin kartoittaa VoWLAN:in tarpeellisuus ja sen tuomat hyödyt. Tämän jälkeen voitaisiin alkaa selvittää, minkälaisilla laitteilla puheluita voitaisiin suorittaa tai mahdolliset muut kustannukset. Tällä tavoin voitaisiin selvittää, olisiko VoWLAN-verkon rakentaminen kannattavaa.

WLAN-verkkoa tehdessä kannattaa projekti suunnitella hyvin. Suunnittelu aloitetaan määrittämällä ongelma, joka halutaan ratkaista. Kun ongelma tiedetään, voidaan tutustua eri WLAN-järjestelmien mahdollisuuksiin ja ominaisuuksiin. Kun sopiva järjestelmä on valittu, voidaan miettiä millä ominaisuuksilla ongelma voidaan ratkaista tietoturvallisesti ja toimivimmin. Hyvän suunnittelun jälkeen järjestelmän toteutus on helpompaa.

Toteutuksessa määritettiin ensin asetukset perustasolle ja tämän jälkeen sijoiteltiin laitteet suunnitelluille paikoille. Asetuksia piti kuitenkin muutella ja määritellä lisää sijoittelun jälkeen. Tukiasemien sijainnin valinnassa kokeiltiin kuuluvuuksia useampaan otteeseen. Sopivien tukiasemien paikkojen löydyttyä voitiin järjestelmää alkaa testata käytännössä. Käytännöntestauksen aikana voitiin myös kokeilla ylläpidollisia toimintoja, kuten tarkkailla lokitietoja, hälytyksiä ja muuten langattoman verkon toimivuutta.

Yllämainittua tehtävientekojärjestystä noudattaessani WLAN-verkon asennus sujui hyvin, eikä toteutuksessa tullut suurempia ongelmia. Projekti oli mielenkiintoinen ja opin erittäin paljon uusia asioita langattomista verkoista, niiden tietoturvasta ja laitteiden sijoittelusta. Työn alussa asetetut tavoitteet saavutettiin ja lopputulokseen oltiin tyytyväisiä, niin asiakkaan puolesta kuin omastanikin.

Langattoman verkon peittoalue saatiin kattamaan kaikki kokoustilat ja rajattua hyvin rakennuksen sisätiloihin. Käyttötestauksen aikana ei ilmennyt suuria ongelmia ja langattoman verkon käyttö oli helppoa käyttäjille. Ohjeistus voidaan täten todeta olleen riittävän kattava. Opinnäytetyön julkisesta dokumentista poisjääneet tietoturva asiat tarkasti Lemminkäisen tietoturva päällikkö ja totesi tietoturvatason olevan riittävä. Yritykselle Opinnäytetyöstä jäi tuotoksina langaton verkko, opinnäytetyö, tarkemmat tiedot sisältävä dokumentti, liitteenä olevat ohjeistukset ja käyttäjille tulleet tarkemmat ohjeistukset.

Lähteet

Kirjallisuus

Geier, J. 2005. Langattomat verkot. Suomentaja Holttinen, J. Helsinki: Edita Prima Oy.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WSOY.

Kempf, J. 2008. Wireless Internet secerity. Cambridge University Press.

Lawrence, H. 2005. Wireless systems. La Verge: Althos Publishing.

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

Thomas, T. 2005. Verkkojen tietoturva perusteet. Suomentaja Holttinen, J. Helsinki: Edita Prima Oy.

Trapeze Networks 2007. Trapeze RingMaster Reference Manual. 6. versio.

Trapeze Networks 2008a. RingMaster Configuration Guide. 7. versio.

Trapeze Networks 2008b. RingMaster quick start guide. 7. versio.

Trapeze Networks 2008c. RingMaster 7.0 Planning Guide.

Trapeze Networks 2008d. Wired and Wireless Security Best Practices.

Trapeze Networks 2009a. Smart Mobile®: A Better Architecture for NonStop Wireless Networking.

Trapeze Networks 2010a. Trapeze White Paper overview.

Wendell, O.2004. Tietoverkot perusteet. Suomentaja Holttinen, J. Helsinki: Edita Prima Oy.

Sähköiset lähteet

Fleishman, G. 2008. Battered, but not broken: understanding the WPA crack. Viitattu 19.2.2011. http://arstechnica.com/security/news/2008/11/wpa-cracked.ars

Hewlett-Packard Development Company 2010. What is port trunking, and how do I configure it?. http://www.hp.com/rnd/support/faqs/sw_800t.htm?jumpid=reg_R1002_USEN#question21

Kassner, M. 2008.802.11n: MIMO really needs smart antennas. Viitattu 19.2.2011. http://blogs.techrepublic.com.com/networking/?p=505

Kayne, R. 2010. What Is 802.11n?. Muokattu Foster, N. 3.12.2010. Viitattu 13.12.2010. http://www.wisegeek.com/what-is-80211n.htm

Lahti, J. 2007. Trapeze levittää WLAN-verkkonsa Suomeen. Viitattu 19.2.2011. http://www.digitoday.fi/bisnes/2007/09/21/trapeze-levittaa-wlan-verkkonsa-suomeen/200723333/66

Ngo, D. 2009. 802.11n Wi-Fi standard finally approved. Viitattu 19.2.2011. http://news.cnet.com/8301-1035_3-10351215-94.html

PC Magazine. Definition of: Cable categories. Viitattu 19.2.2011. http://www.pcmag.com/encyclopedia_term/0,2542,t=cable+categories&i=39162,00.asp

Trapeze Networks. 2009b. Guest Access Deployment Guide. Viitattu 19.2.2011. www.trapezenetworks.com/file.cfm?content=1430&pageId=23

Trapeze Networks 2010b. Viitattu: 5.10.2010. www.trapezenetworks.com/about_trapeze/company_overview

Trapeze Networks 2010c. Wireless LAN Controllers. Viitattu: 5.10.2010. http://www.trapezenetworks.com/products/wlan_controllers/v

United Business Media. 2010. InformationWeek. Viitattu 19.2.2011. http://www.wi-fi.org/files/informationweek_2010_01_25.pdf

Viestintävirasto. 2009. 15Z/2009 M http://www.ficora.fi/attachments/suomiry/5l1x1FIlk/Viestintavirasto15Z2009M.pdf

Wi-Fi alliance 2011. Glossary. Viitattu 19.2.2011. http://www.wi-fi.org/knowledge_center_overview.php?type=3

Haastattelut

J. Mäkelä, Lemminkäinen Oyj haastattelu 27.10.2010.

Kuvat ja kuviot



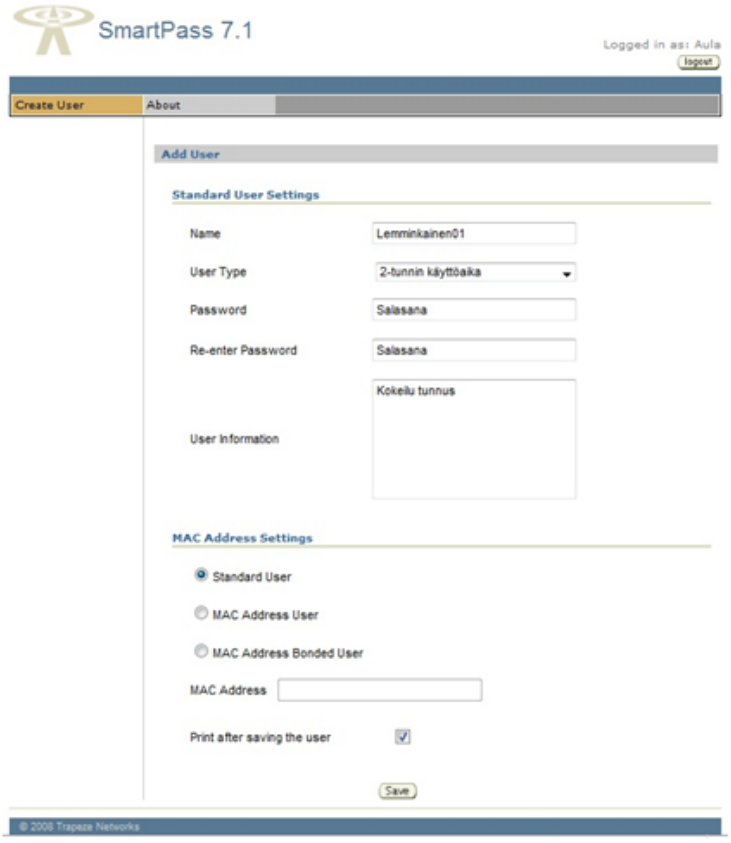
Taulukot

Liitteet

Liite 1: Aulahenkilökunnan ohjeistus

## WLAN vierailijatunnusten luonti ohjeistus


1. **Mene selaimella osoitteeseen: https://smartpass**
2. **Kirjoita käyttäjätunnus ja salasana.**
3. **Kirjoita vierailijan käyttäjätunnus, Name kohtaan**
   käyttäjätunnuksena käy vierailijan yrityksennimi. järjestelmä ei hyväksy ääkkösiä nimessä.
4. **Valitse User Type kohdasta kuinka kauan tunnus on voimassa.**
   Vaihtoehtoina on 2 tuntia, 8 tuntia tai 5 päivää.
5. **Kirjoita vierailijan salasana Password ja uudestaan Re-enter password kohtiin**
6. **Kirjoita User Information kohtaan lisätietoja**
   User Information kentän pystyy jättämään myös tyhjäksi.
7. **MAC Address Settings kohdasta valitaan Standard User**
8. **Print after saving the user kohdan voi valita mikäli haluaa tulostaa ohjeistuksen ja tunnuksen tiedot vierailijalle**



9. **Valitessasi tulostuksen, tulee esiin ponnahdusikkuna. ponnahdusikkunasta näet tulostettavan kupongin ja voit tulostaa sen painamalla Print nappia.**


**Lisätietoja:**

**Huomioi että kaikissa tunnuksissa ja salasanoissa on isoilla ja pienillä kirjaimilla väliä.**

**Yhtä käyttäjätunnusta pystyy käyttämään enintään kolme tietokonetta yhtä aikaa.**

**Vierailija verkko ei toimi mikäli järjestelmänvalvoja on estänyt selaimen asetusten muuttamisen ja selaimen yhteysasetuksista ei ole määritetty automaattista asetustenhakua päälle**