HAAGA-HELIA
ammattikorkeakoulu

Langattoman vierailijaverkon suunnittelu ja toteutus

Joni Junni

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

21.11.2014

Tietojenkäsittelyn koulutusohjelma

Tekijä tai tekijät Joni Junni	**Ryhmätunnus tai aloitusvuosi** 2011
Raportin nimi Langattoman vierailijaverkon suunnittelu ja toteutus	**Sivu- ja liitesivumäärä** 31+1
Opettajat tai ohjaajat Juhani Merilinna	

Langattomat verkot ovat yleistyneet jatkuvasti aina 2000-luvun alusta lähtien. Erityisesti yritysmaailmassa on kiinnostuttu niiden tuomasta vapaudesta työskentelymenetelmissä ja työtiloissa. Usein myös yritysten ulkopuolisille asiantuntijoille halutaan tarjota verkkoyhteys etätyöskentelyä varten, mutta tietoturvasyistä ulkopuolisia ei sovi päästää kytkeytymään toimistoverkkoon.

Toimeksiantajan organisaatiossa syntyi tarve korvata vanha langaton vierailijaverkko rakentamalla vierailijaverkkotoiminnallisuus uuden langattoman verkon järjestelmään. Uusi järjestelmä oli toteutettu vain sisäistä toimistoverkkoa varten, joten tavoitteena oli saada samaan järjestelmään liitettyä erillinen vierailijaverkko talossa vierailevien asiantuntijoiden käyttöön.

Tässä opinnäytetyössä käydään läpi langattoman vierailijaverkon suunnittelu ja toteutus. Projektin ensisijainen tavoite oli korvata vanha olemassa oleva langaton vierailijaverkko, jonka ongelmia on turvaton konfiguraatio, huono suorituskyky ja rajattu kuuluvuus. Projektia edeltävä osuus kattaa langattoman verkon fyysisen toteuttamisen ja langattoman toimistoverkon toteutuksen, eikä niitä käydä läpi tässä työssä tarkemmin.

Opinnäytetyö toteutettiin 12 viikossa, jonka aikana langaton vierailijaverkko suunniteltiin ja toteutettiin. Aikataulu oli melko tiukka omien työtehtävien ohessa projektin toteutuksessa, mutta projekti onnistui tavoitteissaan luoda tietoturvallinen, suorituskykyinen ja koko kiinteistön kattava langaton vierailijaverkko. Vierailijaverkossa käytetään melko harvinaista tekstiviestien avulla tehtävää käyttäjärekisteröintitapaa, joka mahdollistaa tällä hetkellä turvallisimman WPA2-Enterprise-salausmenetelmän käyttämisen.

Asiasanat
Langattomat lähiverkot, langaton tiedonsiirto, salaus, tietoturva

HAAGA-HELIA
University of Applied Sciences

Abstract

Date of presentation

Degree programme

Authors Joni Junni	**Group or year of entry** 2011
The title of thesis **DESIGNING AND IMPLEMENTING A WIRELESS GUEST NETWORK**	**Number of report pages and attachment pages** 31+1
Advisor(s) Juhani Merilinna	

Wireless networks have become an essential network infrastructure on the 21st century world. The business world in particular is interested in wireless networks that gives them more freedom in terms of workplace and working methods. Often companies want to offer an internet connection for their visitors to use, but for security reasons it is not acceptable to allow unauthorized devices to access the office network.

The employer organization wanted to replace an old wireless guest network by building a guest network functionality to a new wireless network system. The new wireless system was implemented only for the internal office network, so goal for this project was to implement a wireless guest WLAN to the new wireless system.

This thesis goes through the process for designing and implementing a wireless guest network for the employer organization. Primary objective for this project was to replace the old existing wireless guest WLAN which is insecure by design, has poor performance and very limited coverage. The previous project before this thesis covers the physical installation of the wireless network system and the office WLAN network implementation and are not included in this thesis.

The project was accomplished in 12 weeks, during which the wireless guest WLAN was planned and implemented successfully. The schedule was pretty tight for the tasks of this project, but the project succeeded in its goals to create a secure and efficient wireless guest network which covers the whole organization premises. The design of the wireless guest WLAN is quite unique. The network authentication is username and password based, which are generated by the system when user sends a text message to the system. Username and password based authentication allows the use of WPA2-Enterprise encryption method, which is the most secure encryption for wireless networks at the moment.

Key words
Wireless LAN, WLAN, encryption, information security

Sisällys

1 Johdanto

Langattomat verkot ovat yleistyneet huomattavasti 2000-luvun alusta lähtien. Erityisesti yritysmaailmassa on kiinnostuttu niiden tuomasta vapaammasta työskentelytavasta. Vastaavasti myös yrityksissä vieraileville asiantuntijoille halutaan usein saada langattomat verkkoyhteydet, mutta ulkopuolisia ei haluta tietoturvasyistä kytkeä toimistoverkkoon. Tästä syystä on hyvä ottaa mukaan vierailijaverkko langattoman toimistoverkon suunnittelussa.

Tämä opinnäytetyö on toteutettu projektityönä eräälle suomalaiselle organisaatiolle. Organisaatiossa työskentelee noin tuhat henkilöä ja sen pääkonttori sijaitsee Helsingissä. Organisaatiossa syntyi tarve saada koko kiinteistön kattava langaton vierailijaverkko, jolla korvataan vanha olemassa oleva vierailijaverkko konfiguroimalla vierasverkkotoiminnallisuus uuteen langattoman verkon järjestelmään. Uusi järjestelmä on toteutettu toistaiseksi vain organisaation sisäistä toimistoverkkoa varten. Tämän projektin tarkoitus on laajentaa järjestelmää tarjoamaan suojattua vierailijaverkkoa organisaation ulkopuolisille vierailijoille sekä korvata vanha vierailijaverkko.

Tässä opinnäytetyössä käydään läpi langattoman vierailijaverkon suunnittelu- ja toteutusprosessi. Tätä projektia edeltävä osuus kattaa langattoman verkon fyysisen toteuttamisen sekä langattoman toimistoverkon suunnittelun ja toteutuksen, eikä niitä käydä tässä läpi. Langattoman vierailijaverkon rakentamiseen määritettiin 12 viikkoa aikaa, jonka aikana tavoitteena oli suunnitella ja toteuttaa vierailijaverkko sekä tuottaa dokumentaatio ja tämä opinnäytetyön raportti.

Projektin hyödyiksi voidaan laskea tietoturvallisemman vierailijaverkon syntyminen aikaisemman tietoturvattoman avoimen vierailijaverkon korvaajana. Työn ensisijaisena tavoitteena on korvata vanha vierailijaverkko, jonka ongelmina on havaittu heikko suorituskyky, avoin konfiguraatio sekä hyvin rajoittunut kuuluvuus kiinteistössä. Tavoitteena on luoda uuteen langattomaan järjestelmään rakennettava vierailijaverkko, jonka kuuluvuus kattaa suurimman osan organisaation kiinteistöstä, sen käyttö on turvallista salatun yhteyden ansiosta.

1.1 Käsitteet

AES

AES tai Advanced Encryption Standard on vuonna 2001 standardoitu salausalgoritmi ja yksi maailman laajimmin käytössä olevista symmetrisistä salausalgoritmeista. Sitä käytetään laajasti erilaisissa sovelluksissa, kuten IPsec VPN-tuotteissa, TLS-salatuissa yhteyksissä, WPA2-salauksessa, SSH-tunneleissa ja jopa Skypessä. Vielä tänä päivänäkään siihen ei ole käytännöllisiä hyökkäystapoja olemassa. (Paar, C. & Pelzl, J. 2011, s. 87-89.)

Captive Portal

Captive Portal on eräänlainen tervetuloportaali, jota käytetään yleisimmin langattomissa vierailijaverkoissa kahviloissa, lentokentillä, ym. julkisissa tiloissa.

CCMP

CCMP tai Counter Mode with Cipher Block Chaining Message Authentication Code Protocol on AES CCM-salausalgoritmiin perustuva salausmenetelmä langattomille verkoille. (IEEE Standards Association 2007.)

DD-WRT

DD-WRT on Linux-pohjainen avoimen lähdekoodin laiteohjelmisto langattomiin reitittimiin ja tukiasemiin. (DD-WRT 2014.)

Denial of Service Attack

Denial of Service (DoS) Attack tai palvelunestohyökkäys on tapahtuma, jossa estetään jollakin tavalla tiettyyn palveluun pääsy käyttäjiltä. Palvelunestohyökkäyksen tuntomerkkeihin kuuluu yleisimmin tietoliikenneverkon ruuhkauttaminen tavalla, jolla normaali liikenne palveluun häiriintyy tai estyy. (CERT Division 2014.)

Firmware

Firmware, eli laiteohjelmisto on ohjelmakoodia joka kirjoitetaan piirilevyllä sijaitsevan mikropiirin muistiin. Ohjelmakoodin avulla laitetta ja sen resursseja voidaan hallita ja konfiguroida.

Gammu-SMSD

Gammu-SMSD on tekstiviestipalvelu Linuxille. Palvelu käyttää tietokoneeseen kytkettyä GSM-modeemia tekstiviestien lähetykseen ja vastaanottoon.

IEEE 802.1X

802.1X on IEEE Standards Associationin luoma standardi, joka määrittelee porttikohtaisen autentikointimenetelmän lähiverkossa. Sen avulla voidaan autentikoida lähiverkkoon kytketyt laitteet autentikointipalvelimella ennen kuin laitteet hyväksytään verkkoon liikennöimään. Alkuperäinen standardi on määritelty vuonna 2001 ja uusin versio siitä on päivitetty vuonna 2010. (IEEE Standards Association 2010.)

LAN

LAN (Local Area Network) eli lähiverkko on fyysinen verkkoinfrastruktuuri joka yhdistää työasemat, verkkotulostimet ja palvelimet yhtenäiseen verkkoon. Lähiverkolla tarkoitetaan organisaation sisäistä fyysistä verkkoinfrastruktuuria.

Man-in-the-Middle Attack (välimieshyökkäys)

Välimieshyökkäys tai ”Man-in-the-Middle attack” on yksi salakuuntelun muoto, jossa kahden toimijan välistä kommunikaatiota seurataan ja yritetään muokata jonkin kolmannen osapuolen toimesta. Yleensä kommunikaation osapuolet voivat kommunikoida normaalisti eivätkä havaitse liikenteen kulkevan hyökkäävän osapuolen kautta. (Technopedia 2014.)

MySQL-palvelin

MySQL on maailman yleisin avoimen lähdekoodin relaatiotietokantaohjelmisto. Sitä käytetään yleisimmin erilaisissa web-pohjaisissa sovelluksissa ja se on yksi tärkeä komponentti LAMP-ohjelmistopinossa (Linux, Apache, MySQL ja PHP5). (Oracle Corporation 2014.)

OpenID

OpenID on OpenID Foundationin ylläpitämä autentikointipalvelu, jonka kautta voidaan autentikoida käyttäjiä erilaisiin järjestelmiin.

OpenWRT

OpenWRT on avoimen lähdekoodin projekti, joka kehittää avointa firmware-laiteohjelmistoalustaa.

Radius

Radius (Remote Authentication Dial In User Service) on verkon autentikointipalvelin, jonka avulla voidaan autentikoida käyttäjiä ennen verkkoon pääsyä.

TKIP

TKIP tai Temporal Key Integrity Protocol on paranneltu versio WEP-salauksesta joka luotiin paikkaamaan WEP-salauksen heikkouksia. (Tech-FAQ 2014.)

VLAN

VLAN (Virtual LAN) on lähiverkon tekniikka, jolla voidaan jakaa fyysinen lähiverkko virtuaalisiin lähiverkkoihin. VLAN:ien avulla voidaan käytännössä rakentaa samaan fyysiseen verkkoinfrastruktuuriin useampi looginen verkko jotka ovat täysin eristetty toisistaan.

VoIP

Voice over Internet Protocol (VoIP) on teknologia joka sallii perinteisten äänipuheluiden soittamisen laajakaistayhteyden yli. VoIP-palvelusta riippuen puhelimella on mahdollista soittaa joko vain saman palvelun käyttäjille verkon yli tai jopa normaaliin puhelinverkon puhelimeen.

WAN

WAN (Wide Area Network) käsittää Internet-operaattoreiden verkkoinfrastruktuurin, joka yhdistää lähiverkkoja toisiinsa ympäri maailmaa.

WRT

WRT on lyhenne sanoista Wireless Receiver/Transmitter ja sillä tarkoitetaan langatonta reititintä/tukiasemaa.

2 WLAN-järjestelmä

Langattomat verkot ovat yleistyneet yritysmaailmassa huomattavasti aina 2000-luvun alusta lähtien. Yleisimpänä syynä langattomien verkkojen lisääntymiseen työpaikoilla on kannettavien tietokoneiden yleistyminen työvälineenä. Langattomat verkot mahdollistavat mobiilin ja avoimen työskentelytavan, koska langattomien verkkojen myötä ei ole tarvetta aina etsiä verkkopistoketta huoneista palavereissa, kokouksissa ja ryhmätyöskentelytilanteissa. Suuria langattomia verkkoja varten on olemassa erilaisia ratkaisuja, jolla saadaan toimitettua suurella alueella toimiva verkko. Tyypillisesti yrityskäytössä käytetään kontrolleripohjaisia ratkaisuja, jossa kaikki tukiasemat kytketään yhteen keskitettyyn kontrolleriin. Kontrollerilaite hoitaa yleensä kaikkien tukiasemien liikenteenohjauksen, kaistanhallinnan, käyttäjien autentikoinnin sekä kuormantasauksen. Kontrolleripohjaiset ratkaisut yleisesti ovat kustannuksiltaan suuremmat johtuen sen yritystasoisesta laitteistosta ja järeästä kontrollerista.

Yritysverkoissa tietoturva on yksi tärkeimpiä näkökohtia, koska heikko tietoturva voi helposti jopa tuhota yrityksen liiketoiminnan. Langattomien verkkojen tietoturvaan liittyy vahvat salausmenetelmät, keskitetty käyttäjänhallinta sekä vahvat salasanat. Jotta langattoman verkon käyttäjiä saadaan autentikoitua, tarvitaan langattoman verkon taustapalveluihin jonkinlainen autentikointipalvelin. Esimerkiksi FreeRADIUS on avoimen lähdekoodin autentikointipalvelin. Se on hyvin laajasti käytössä ja mainostaa olevansa maailman yleisin Radius-palvelinohjelmisto. (The FreeRADIUS Server Project 2014.)

3 Käyttäjien autentikointimenetelmät

Vaihtoehtoja vierailijaverkon käyttäjien autentikontimenetelmiin pohdittiin projektin aikana useasti. Autentikointimenetelmän vaatimuksena teoriassa on saada yksilöllisesti salattu yhteys käyttäjän ja tukiaseman välille, jotta esimerkiksi välimieshyökkäysten riski verkon sisällä putoaisi minimiin. Yhteyden yksilöllistä salausta varten vaaditaan yksilöllinen autentikointimenetelmä. Vaihtoehtoina on pohdittu erilaisia todentamismenetelmiä, kuten perinteistä käyttäjätunnuksilla kirjautumista, kertakäyttösalasanoja sekä autentikoitumista jotakin julkista palvelua vasten (OpenID, Facebook, Google+, ym.).

3.1 Autentikointi käyttäjätunnuksella ja salasanalla

Perinteinen käyttäjätunnuksella ja salasanalla autentikointi perustuu käyttäjälle annettuun käyttäjätunnus-salasanapariin tai käyttäjän itsensä rekisteröimiin käyttäjätunnuksiin. Kun käyttäjä syöttää käyttäjätunnuksen ja salasanan kirjautumiskenttiin, lähtee pyyntö verkossa sijaitsevalle Radius-palvelimelle. Jos tunnukset ovat oikein, palvelin hyväksyy pyynnön ja käyttäjä sallitaan käyttämään langatonta verkkoa. Jos tunnukset eivät kelpaa, palvelin hylkää autentikointipyynnön eikä käyttäjä pääse käyttämään verkkoa. Käyttäjätunnusten hyvä puoli on käyttäjien yksilöllinen tunnistautuminen langattomaan verkkoon ja helpompi konfigurointi eri laitteisiin, koska tunnukset voidaan tallentaa laitteiden asetuksiin. Yksilölliset käyttäjätunnukset mahdollistavat jokaiselle käyttäjälle oman salatun yhteyden langattomaan tukiasemaan, joka parantaa tietoturvaa huomattavasti. Huonona puolena käyttäjätunnuksissa on henkilöstölle sen tuoma kuormitus käyttäjätunnusten ylläpidossa. Perinteisesti yritysverkossa käyttäjätunnukset linkitetään johonkin olemassa olevaan käyttäjätietokantaan, kuten esimerkiksi Active Directoryyn. Tämänlaista toimintatapaa ei suoraan voida kuitenkaan käyttää vierailijaverkkoon, vaan verkon käyttäjien tulisi itse hoitaa käyttäjätunnusten rekisteröiminen.

3.2 Kertakäyttösalasanat

Kertakäyttöisillä käyttäjätunnuksilla autentikoituminen tapahtuu ohjaamalla käyttäjä langattoman verkon Captive Portaliin, jossa käyttäjä voi rekisteröidä käyttäjätunnuksensa. Rekisteröinnin jälkeen käyttäjä voi kirjautua rekisteröimillään käyttäjätunnuksilla ja salasanalla verkkoon. Rekisteröintivaiheessa käyttäjätunnus määritellään vanhene-

maan esimerkiksi parissa vuorokaudessa, jonka jälkeen käyttäjän on rekisteröidyttävä uudelleen. Kertakäyttötunnukset on hyvä menetelmä ylläpidon näkökulmasta, koska käyttäjätunnusten luominen on ulkoistettu käyttäjälle eikä käyttäjätunnuksia tarvitse hallinnoida erikseen. Kertakäyttötunnusten huono puoli on yleensä tällaisissa ratkaisuissa Captive Portalin käyttö. Perinteisesti Captive Portalilla toteutettu langaton verkko on suojaamaton, jolloin kuka tahansa voi liittyä siihen. Verkossa ei kuitenkaan voi liikennöidä, ennen kuin on suorittanut tarvittavat toimenpiteet verkon Captive Portalissa. Usein portaalissa täytyy hyväksyä jonkinlaiset käyttöehdot tai suorittaa tunnusten rekisteröiminen, ennen kuin istunto aukeaa ja verkkoon pääsee liikennöimään. Tämä aiheuttaa ongelmia useimmiten mobiililaitteissa, jotka eivät osaa välttämättä esittää Captive Portaalin sivua verkkoon liityttäessä. Tämä hankaloittaa verkon käyttämistä käyttäjän näkökulmasta. Käyttäjää voi myös häiritä jatkuva verkkoon rekisteröityminen ja kirjautuminen, kun käyttäjätunnukset tai kirjautumisistunto vanhenee.

3.3 Julkisen palvelun kautta autentikointi

Julkisen palvelun tunnistautuminen perustuu käyttäjän autentikoimiseen esimerkiksi OpenID:n, Facebookin, Googlen tai muun kolmannen osapuolen kirjautumispalvelussa. Julkisessa palvelussa autentikoituminen yksinkertaistaisi ylläpitoa käyttäjätunnuksien osalta, koska organisaation ei tarvitse hallinnoida käyttäjätunnuksia. Heikkoutena julkisen palvelun autentikoinnissa on riippuvuus kolmanteen osapuoleen järjestelmään kirjautumisessa, ulkoisen palvelun kautta mahdolliset tietoturvaongelmat sekä vaatimus käyttäjille omistaa käyttäjätunnukset kyseiseen kolmannen osapuolen palveluun.

4 Langattoman verkon ominaisuuksia

Tässä kappaleessa on kuvattu erilaisia osa-alueita langattomien verkkojen ja erityisesti langattomien vierasverkkojen toteutukseen. Tässä kappaleessa esitellään erilaisia langattoman verkon salausmenetelmiä, langattomien verkkojen reititys- ja eristämistapoja, kaistanhallinnan menetelmiä sekä verkkoliikenteen suodatusmenetelmiä. Lisäksi selvitetään VLAN:in toimintaa, tukiasemien kuuluvuutta ja sijoittelua, taajuusalueita sekä roaming-toimintaa.

4.1 Salausmenetelmät

WEP-salaus tai ”Wired Equivalent Privacy” on langattomien verkkojen vanhin salausstandardi. Se kehitettiin vuonna 1999 suojaamaan siihen asti täysin avoimina olleita langattomia verkkoja. WEP todettiin vain muutama vuosi myöhemmin hyvin turvattomaksi salausmenetelmäksi. WEP-salauksen suurin heikkous on sen lyhyet salausavaimet, jotka loppuvat nopeasti kesken ja tukiasema alkaa kierrättää niitä. Salausavaimien kierrättämisen johdosta on mahdollista selvittää verkon salausavain jolla liikenne salataan. (Justin Pot 2013.)

WPA-salaus eli “Wi-Fi Protected Access” on WEP-salausta uudempi langattomien verkkojen salausstandardi. Standardista on kaksi versiota, vanhempi WPA sekä uudempi WPA2-salausstandardi. Alkuperäinen WPA luotiin korjaamaan WEPin sisältämiä tietoturvaongelmia ja se toimi pitkälti väliaikaisratkaisuna ennen WPA2-salauksen julkaisemista. WPA-salausta käytetään yleensä yhdessä TKIP-salausprotokollan kanssa, jonka kautta WPA-salaus on murrettavissa muutamalla eri menetelmällä, kuten esimerkiksi palvelunestohyökkäyksellä (Denial-of-Service) ja IP-pakettien pilkkomisella. Ongelma ei kuitenkaan ole yhtä vakava kuin WEP-salauksessa, koska WPA-salauksen purkaminen vaatii huomattavasti enemmän työtä ja aikaa. (Chris Hoffman, Mathy Vanhoef, Frank Piessens 2013.)

WPA2-salaus on uusin versio WPA:sta ja tällä hetkellä turvallisin salausmenetelmä langattomissa verkoissa. WPA2-salausta voidaan käyttää kahdessa moodissa: WPA2-PSK tai WPA2-Enterprise. WPA2-PSK-salaus eli ”Pre-Shared Key” on yleisin salausmene-

telmä langattomien tukiasemien kotikäytössä sekä pienissä toimistoissa. WPA2-salauksessa voidaan käyttää sekä TKIP-salausprotokollaa että uudempaa AES-salausalgoritmiin perustuvaa CCMP-salausprotokollaa. Salaukseen käytetään salausavainta, joka lasketaan verkolle määritetystä salasanasta. Suurin tietoturvaongelma WPA2-PSK-salauksessa on liian lyhyet ja yksinkertaiset salasanat. Yleisesti WPA2-salauksessa ei ole teknisestä näkökulmasta yhtä isoja tietoturvaongelmia kuin vaikkapa WEP-salauksessa, mutta liian heikko ja yksinkertainen salasana asettaa suuremman riskin verkkoon murtautumiselle. WPA2-PSK-salatussa verkossa on myös teoriassa mahdollista salakuunnella samassa verkossa olevien liikennettä, koska kaikkien käyttäjien liikenne salataan samalla salausavaimella. Salakuuntelu vaatii kuitenkin pääsyn samaan langattomaan verkkoon sekä erityiset työkalut verkon liikenteen kuuntelemiseen. (Chris Hoffman 2013.)

WPA2-Enterprise on yrityskäyttöön tarkoitettu salaustandardi. WPA2-Enterprisessä käytetään 802.1X-standardiin perustuvaa autentikointia, jonka vuoksi sitä kutsutaan myös WPA2-802.1X-salaukseksi. Siinä käytetään yhteisen salasanan sijasta käyttäjäkohtaisia uniikkeja tunnuksia verkon käyttäjien autentikoimiseen. Käyttäjien autentikointikointia varten verkkoon tarvitaan Radius-palvelin, joka usein samalla sisältää tietokannan käyttäjien tunnuksista ja salasanoista. WPA2-Enterprise on tällä hetkellä turvallisin langattoman verkon salausmenetelmä, johtuen WPA2-standardin pakottamasta AES-salausalgoritmista, käyttäjäkohtaisesta autentikoinnista sekä yksilöllisestä yhteyden salauksesta. WPA2-Enterprise-salauksessa käyttäjät autentikoidaan käyttäjätunnuskohtaisesti Radius-palvelimella ja jokaisen käyttäjän istunto salataan yksilöllisellä salausavaimella. (The Cisco Learning Network 2011.)

4.2 Radius-autentikointi

Radius (Remote Authentication Dial-In User Service) on autentikointipalvelin, jonka avulla käyttäjiä voidaan autentikoida keskitetysti. Radius on määritelty RFC 2865 ja RFC 2866-määrittelydokumenteissa, joissa kuvataan Radiuksen toimintaperiaate ja sen käyttämä Radius-protokollan toiminta. Radius-protokolla on UDP-pohjainen autentikointiprotokolla, jota Radius-palvelin ja asiakas käyttää kommunikointiin keskenään. Tyypillisesti Radius-asiakkaana toimii NAS (Network Access Server) ja Radius-palvelin

ajetaan prosessina Windows, UNIX tai Linux-palvelimella. Langattoman verkon tapauksessa langattomat tukiasemat toimivat Radius-asiakkaina, jotka tekevät autentikointipyyntöjä verkossa sijaitsevalle Radius-palvelimelle. Radius-asiakkaan ja palvelimen välillä käytetään ns. jaettua salaisuutta, jonka avulla niiden välinen liikenne salataan.

Kuva 1: Radius-protokollan perusrakenne tukiasemaratkaisussa.

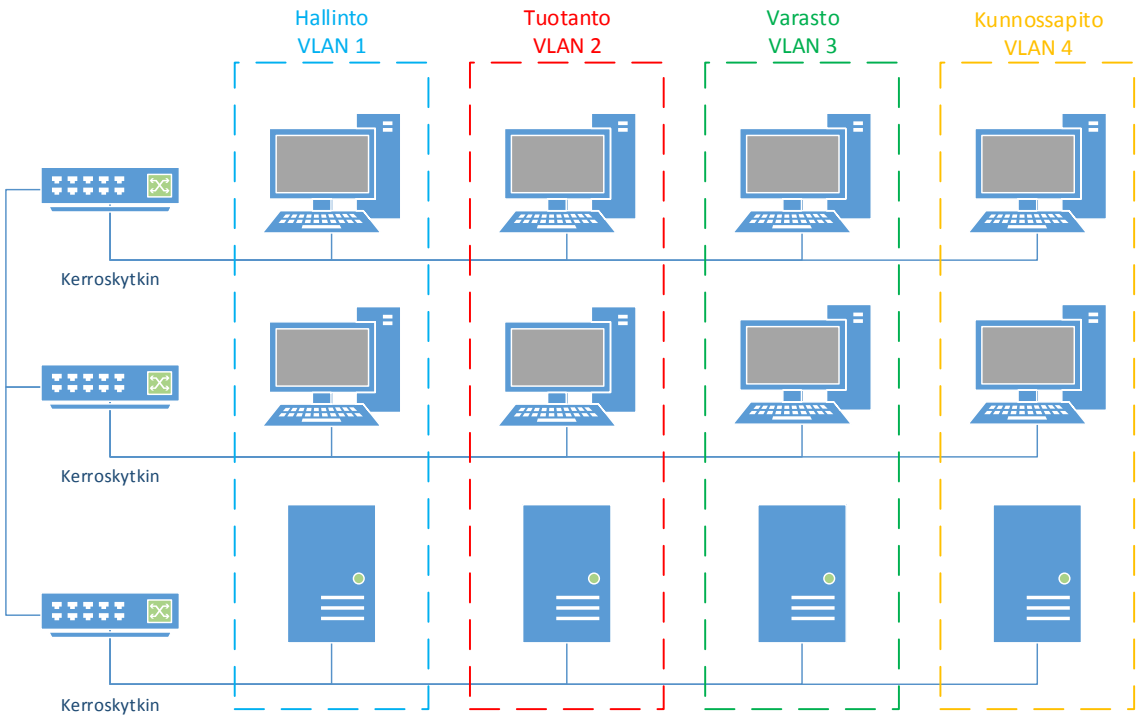
Kuvassa 1 on kuvattu Radius-protokollan eri vaiheet, jotka käydään läpi tyypillisessä langattoman verkon autentikoinnissa. Aluksi käyttäjä liittyy langattoman tukiaseman tarjoamaan verkkoon, jolloin Radius-asiakkaana toimiva tukiasema pyytää käyttäjältä käyttäjätunnusta ja salasanaa. Käyttäjän syöttäessä käyttäjätunnuksen ja salasanan, tukiasema lähettää ne eteenpäin Access-Request-tyyppisessä datapaketissa Radius-palvelimelle. Radius-palvelin tarkistaa sille määritetystä käyttäjätietolähteestä löytyykö vastaanotetulle käyttäjätunnus-salasanaparille vastinetta. Jos vastaavuus löytyy, palvelin vastaa tukiasemalle Access-Accept-tyyppisellä paketilla, joka sisältää parametreja attribuutti-arvo-pareina kuvaamaan käyttäjän istuntoa. Tyypillisiä parametreja ovat esimerkiksi palvelutyyppi, protokollatyyppi, asiakkaalle määritettävä IP-osoite ja istuntoon käytettävä pääsylista. Jos annettuja käyttäjätunnuksia ja salasanaa vastaavaa tietoa ei löydy käyttäjätietolähteestä, Radius-palvelin vastaa Access-Reject-tyyppisellä paketilla joka yleensä sisältää virheilmoituksen jonka palvelin on kohdannut autentikoinnissa.

Radius-palvelin tukee myös Access-Challenge-pakettityyppiä, jonka avulla toimitetaan asiakkaalle haaste, johon asiakkaan pitää vastata oikein. Lopuksi tukiasema joko sallii käyttäjän kirjautumisen langattomaan verkkoon, pyytää vastausta palvelimen kysymään haasteeseen tai estää yhteyden riippuen Radius-palvelimen vastauksesta. (Cisco Systems 2006.)

4.3 VLAN

VLAN:it tai virtuaalilähiverkot ovat teknologia, jonka avulla fyysinen lähiverkko voidaan jakaa loogisiin verkkosegmentteihin organisaation osastojen, toimintojen, työryhmien, sovelluspalveluiden tai muun toiminnallisen syyn perusteella. Niiden avulla voidaan liittää esimerkiksi kaikki saman projektityöryhmän käyttämät työasemat ja palvelimet samaan VLAN:iin riippumatta projektiryhmän henkilöiden fyysisestä sijainnista lähiverkossa. VLAN:ia käytetään yleisimmin segmentoimaan fyysistä lähiverkkoa pienempiin osiin, jossa perinteisesti jakaminen tehdään reitittimien toimesta. VLAN:ien avulla lähiverkosta saadaan skaalautuvampi, tietoturvallisempi sekä helpommin hallittava. VLAN:ien skaalautuvuus perustuu lähiverkon konfigurointiin reitittimien ja kytkimien ohjelmistoissa, eikä siihen että verkon laitteita fyysisesti siirrellään ja kytketään eri kytkimiin. Tietoturvallisuus paranee, koska VLAN:it eivät keskustele keskenään missään kohtaa vaan toimivat täysin omina lähiverkkoinaan. Lähiverkon hallittavuus paranee, koska se saadaan pilkottua pienempiin, paremmin hallittaviin segmentteihin. Reitittimien tehtävä VLAN-topologioissa on tarjota kaistanhallintaa, suodattamista ja sitä kautta tietoturvaa. VLAN:ien välillä on myös mahdollista liikennöidä, jos lähiverkon reititin konfiguroidaan reitittämään liikenne niiden välillä. (Cisco Systems Inc. 2014.)

VLAN:in toiminta määritellään IEEE:n 802.1Q-standardissa. VLAN:in toiminta perustuu normaalien IP-datapakettien enkapsulointiin, jossa lähiverkon kytkimet ”taggaavat” verkkoliikenteen datapaketit uniikilla VLAN ID:llä niiden saapuessa kytkimen portille. Kytkin tunnistaa mihin VLAN:iin datapaketti kuuluu ja merkitsee siihen VLAN ID-tunnisteen ennen paketin toimittamista eteenpäin verkossa. Tämän tunnisteen avulla muut kytkimet tunnistavat mihin VLAN:iin paketti kuuluu ja ohjaavat paketin sen otsikkotietojen perusteella oikeaan osoitteeseen. (Cisco Systems Inc. 2014.)



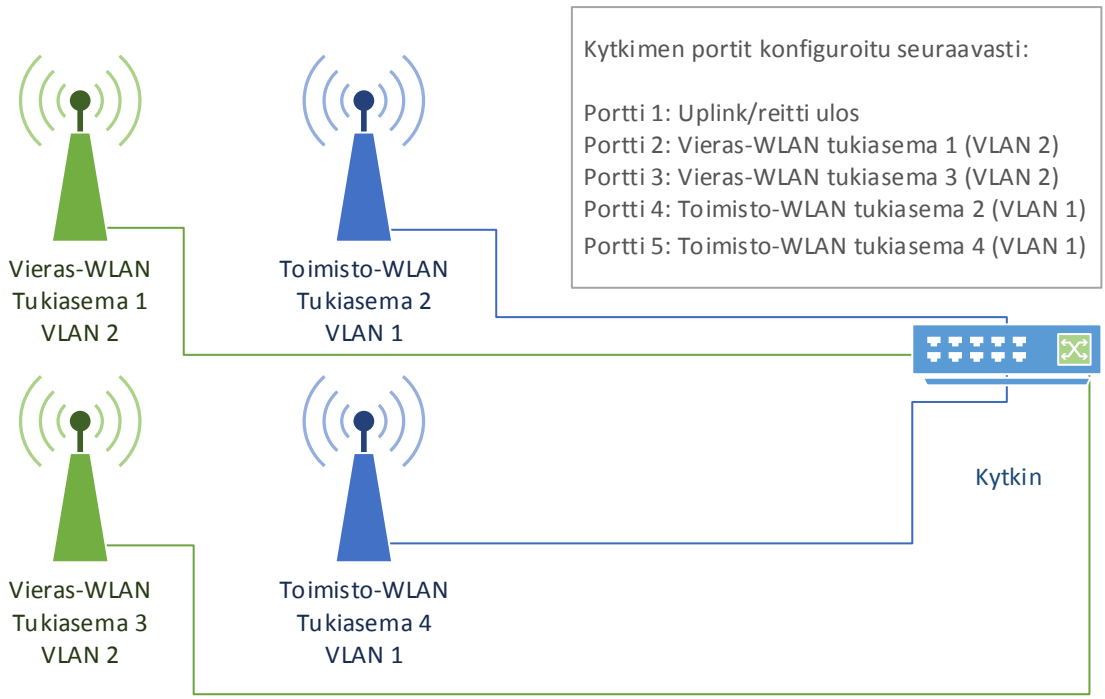
Kuva 2: Esimerkki organisaation VLAN-segmentoinnista.

Kuvassa 2 on esiteltynä esimerkkitapaus organisaation lähiverkosta ja sen jakamisesta eri verkkosegmentteihin osaston perusteella. Esimerkissä työasemat ja palvelimet sijaitsevat rakennuksen kolmessa eri kerroksessa, joka käy ilmi laitteiden kytkemisestä eri kerroskytkimiin. Organisaation hallinnon työasemat ja sen käyttämät verkkopalvelut on konfiguroitu toimimaan VLAN 1:ssä. Tuotanto-osaston kaikki työasemat ja palvelut ovat konfiguroitu VLAN 2:een sekä varaston laitteet VLAN 3:een. Kunnossapito-osaston koneet ovat VLAN 4:ssa. Kuten kuvassa havainnollistetaan, kaikki laitteet kerroksessa on kytkettynä yhteen kytkimeen. Kytkimen portit ovat kuitenkin niin sanotusti ”tagattu” tiettyyn VLAN:iin, eli konfiguroitu palvelemaan tiettyä VLAN:ia, eikä siinä portissa oleva laite voi nähdä kuin samassa VLAN:ssa olevat muut laitteet ja työasemat.

4.4 Reititys ja eristäminen

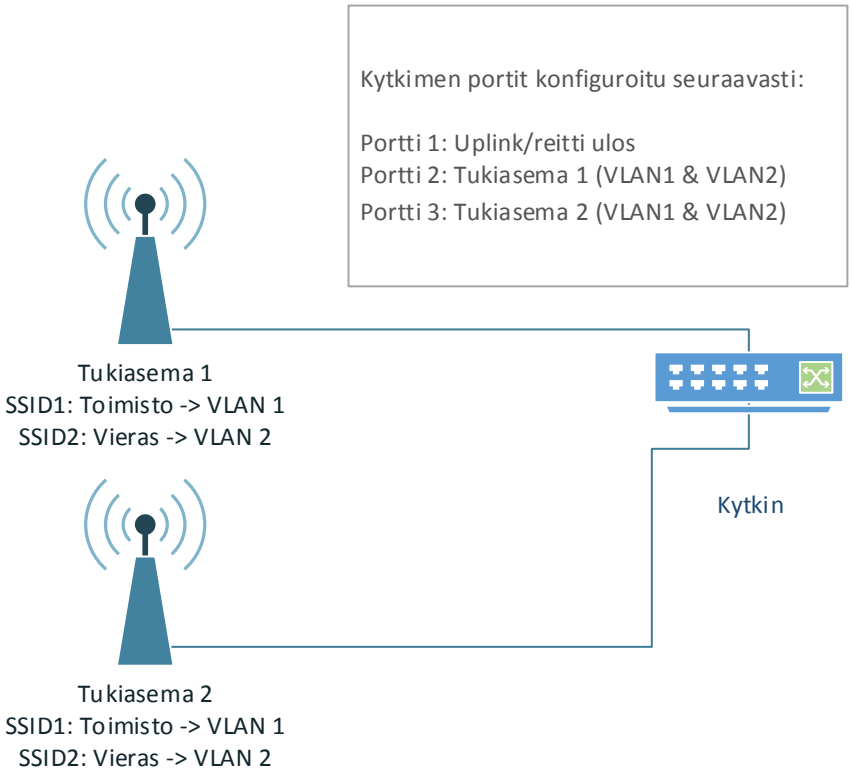
Langattomien verkkojen liikenteen reititykseen ja eristämiseen on monia erilaisia tapoja. Esimerkkinä voidaan mainita esimerkiksi VLAN-pohjainen verkotustapa, jonka avulla voidaan toimistoverkko ja vierailijaverkko jakaa loogisiin verkkosegmentteihin tukiasemapohjaisesti tai SSID-pohjaisesti. Molemmissa tavoissa lopullinen verkkoliikenteen reititys eri verkkoihin tehdään reitittimellä tai palomuurilla. Tukiasemapohjainen jaka-

minen perustuu eri fyysisten tukiasemien määrittämiseen eri verkon käyttöön, jolloin toimistoverkolla on omat tukiasemansa ja vierailijaverkolla on omat tukiasemansa. Kuvassa 3 on esitetty tukiasemapohjainen verkon erottelu. Tällöin tukiasemat kytketään omiin määritettyihin portteihin kytkimessä ja portti konfiguroidaan liitetyksi joko vierailijaverkon VLAN:iin tai toimistoverkon VLAN:iin.



Kuva 3: Langattoman verkon eristys tukiasemapohjaisesti VLAN:lla

SSID-pohjainen jakaminen perustuu tukiaseman päässä tehtyyn konfiguraation, jossa määrättyyn tukiaseman langattomaan verkkoon liittynyt päätelaite saa käyttöönsä vain sen verkon palvelut. Kuvassa 4 on kuvattu SSID-pohjainen verkkojen erottelu VLAN:in avulla. Tässä tapauksessa kaikki langattomat tukiasemat konfiguroidaan niin sanottuun multi-SSID-tilaan, jossa ne tarjoavat useampaa langatonta verkkoa (SSID) samasta fyysisestä laitteesta. Jokainen SSID konfiguroidaan viittaamaan omaan VLAN:iinsa, jolloin esimerkiksi toimistoverkko on VLAN 1:ssä ja vierailijaverkko on VLAN 2:ssa. Langallisen lähiverkon puolelta kytkimestä määritetään jokaisen tukiaseman käyttämään porttiin molemmat VLAN:it. (TechTarget 2014.)



Kuva 4: Langattomien verkkojen eristäminen SSID-pohjaisesti VLAN:lla.

4.5 Kaistanhallinta

Lähiverkon kaistanhallintaan on monia eri menetelmiä riippuen käytettävästä siirtotiestä. Yleisin menetelmä langallisen lähiverkon liikenteen priorisointiin on 802.1Q ja 802.1D -standardeihin perustuva toteutus nimeltä Quality of Service tai QoS. Se perustuu lähiverkon liikenteen ryhmittelyyn tärkeyden mukaan eriarvoisiin prioriteettijonoihin. Normaalisti lähiverkossa jossa minkäänlaista liikenteenhallintaa ei tehdä, kaikki verkon liikenne liikkuu tasa-arvoisena samalla todennäköisyydellä päästä perille kohdeosoitteeseensa. Tätä tätä ilmiötä kutsutaan termillä ”Best Effort”, eli kaikki verkossa liikkuvat datapaketit yritetään toimittaa perille parhaimmalla mahdollisella tavalla, reitillä ja nopeudella. Tästä johtuen lähiverkko saattaa ruuhkautua suurella kuormalla ja käyttäjämäärällä, koska kaikki lähiverkossa liikkuvat datapaketit ovat tasa-arvoisia toisiinsa nähden. Jos lähiverkon reititin tai kytkin ruuhkautuu, se joutuu pudottamaan datapaketteja pois puskurimuistin loppumisen vuoksi. Tästä voi aiheutua jopa lisää ruuhkaa, kun asiakaspää saattaa lähettää paketin uudelleen protokollasta riippuen. (IEEE Standards Association 2011.)

Yhtenä ratkaisuna ongelmaan on Quality of Service, jonka avulla liikennettä voidaan priorisoida liikenteen kriittisyyden mukaan. Monesti käytännön toteutukset laite- ja ohjelmistovalmistajien ratkaisuissa eroavat hieman toisistaan, mutta noudattavat kuitenkin pitkälti kyseisiä standardeja. Uudemmassa vuoden 2011 802.1Q-standardin liitteessä I määritellään seitsemän erilaista tietoliikennetyyppiä lähiverkon tietoliikenteen luokitteluun, joiden perusteella liikenne ryhmitellään tärkeysjärjestykseen. Taulukossa 1 kuvataan standardin määrittelemät liikennetyypit ja niiden suositeltu prioriteettijärjestys pienimmästä tärkeydestä suurimpaan: (IEEE Standards Association 2011; IEEE Standards Association 2004.)

Taulukko 1: QoS-liikennetyypit prioriteettijärjestyksessä. (IEEE Standards Association 2011.)

Prioriteetti	**Liikennetyyppi**
1	Background
2	Best Effort
3	Excellent Effort
4	Critical Applications
5	Video
6	Voice
7	Network Control

Pienimmällä prioriteetilla 1 on kaikki taustaliikenteeksi kategorisoitava verkkoliikenne, joka on sallittu lähiverkossa, mutta sen ei haluta vaikuttavan muihin verkon käyttäjiin tai sovelluksiin. Prioriteetilla 2 on kaikki normaali verkkoliikenne, johon ei ole kohdistettu priorisointisääntöjä. Tällä prioriteetilla koko lähiverkon liikenne normaalisti toimii jos verkkoon ei ole konfiguroitu kaistanhallintaa. Prioriteetille 3 on tarkoitettu ns. VIP-henkilöt ja palvelut, joiden halutaan saavan verkossa parempaa palvelua kuin normaalisti. Prioriteetille 4 on tarkoitettu kaikki liiketoimintakriittiset sovellukset ja palvelut. Prioriteetti 5 on tarkoitettu liikkuvalle kuvalle, kuten videostreamaussovellukset, videokonferenssisovellukset, ynnä muut sovellukset sekä palvelut jotka vaativat suurta kaistanleveyttä ja lyhyttä viivettä. Prioriteetti 6 on tarkoitettu äänipalveluille, kuten VoIP-puhelimet, etäkokoussovellukset, ja muut sovellukset joille pitää taata vakaa viiveetön

liikennevirta. Korkeimmalla prioriteetilla 7 toimii kaikki verkon ylläpitoon ja hallintaan liittyvät työkalut ja palvelut. (IEEE Standards Association 2011; IEEE Standards Association 2004.)

4.6 Suodatus

Verkkoliikenteen suodattamista varten on olemassa useita eri ratkaisuja, joista yleisimpiä on Stateful Packet Inspection (SPI) ja Deep Packet Inspection (DPI) palomuurit. SPI-palomuuri löytyy yleensä kaikista koti- ja pientoimistokäyttöön tarkoitetuista reitittimistä sekä DSL- ja kaapelimodeemeista. Sen toiminta perustuu IP-pakettien otsikkotietojen tarkastukseen, jonka perusteella tarkastetaan sopiiko paketti palomuurisääntöissä sallittuihin tai kuuluuko se jo aktiiviseen yhteyteen tilataulukon avulla. Tilataulukko sisältää tiedot verkon kaikista aktiivisista yhteyksistä, jonka perusteella palomuuri voi päätellä datapakettien liittymisen tiettyyn yhteyteen. SPI-palomuuri ei ota kantaa itse paketin sisältöön, josta aiheutuu ongelmia erilaisten haittaohjelmien kanssa, jotka käyttävät normaaleja ”turvallisia” portteja verkkoon tunkeutumiseen. (Informit 2005.)

Tähän ongelmaan avuksi on Deep Packet Inspection, joka perustuu datapakettien sisällön tarkastukseen haitallisen sisällön varalta. DPI-palomuuri tarkastaa datapaketit siltä kantilta, että niissä on sellaista sisältöä kuin protokollan määrittämässä paketissa kuuluisi olla. Jotkin DPI-palomuurit saattavat jopa sisältää jonkinlaisen tietokannan tunnetuista haittaohjelmista, jolloin ne voivat vielä tehokkaammin tunnistaa haittaohjelmia jo ennen kuin niitä päästetään lähiverkkoon. (Informit 2005.)

4.7 Taajuusalueet ja kanavat

IEEE:n 802.11-työryhmä määrittelee langattomien verkkojen käyttöön pääsääntöisesti kaksi eri taajuusaluetta, 2,4 gigahertsin taajuusalueen sekä 5 gigahertsin taajuusalueen. Myös muita taajuusalueita on, mutta ne ovat harvinaisempia käytössä. 2,4 gigahertsin taajuusalue ulottuu 2400 megahertsistä 2500 megahertsiin ja sitä käytetään 802.11b, 802.11g sekä 802.11n-standardien mukaisissa langattomissa verkoissa. Se on jaettu 14 kanavaan, joista vain 3 kanavaa ei ole päällekkäin keskenään. Standardista johtuen kaistanleveydeksi on määritelty 20/22 megahertsin kaistanleveys, joka aiheuttaa päällekkäisyyksiä vierekkäisillä kanavilla. Euroopassa 14 kanavasta sallittuja ovat vain kanavat

väliltä 1-13. Taulukossa 2 on kuvattu kaikki 2,4 gigahertsin alueella saatavilla olevat kanavat ja niiden taajuushaarukka. Taulukosta voimme havaita, kuinka vierekkäiset kanavat ovat limittäin toisiinsa nähden, josta johtuu kanavien sekoittuminen keskenään. (Adrio Communications Ltd. 2014.)

Taulukko 2: 2,4 gigahertsin taajuusalueen kanavavälit (Adrio Communications Ltd. 2014.)

Kanava	Taajuusalueen alaraja	Taajuusalueen yläraja
1	2401	2423
2	2404	2428
3	2411	2433
4	2416	2438
5	2421	2443
6	2326	2448
7	2431	2453
8	2436	2458
9	2441	2463
10	2456	2468
11	2451	2473
12	2456	2478
13	2461	2483
14	2473	2495

5 gigahertsin taajuusalue on otettu käyttöön 802.11n-standardin langattomien verkkojen myötä. Tällä taajuusalueella on käytettävissä 24 kanavaa, joista 23 kanavaa ei ole päällekkäin muiden kanssa. 5 gigahertsin taajuusalueen käytössä on asetettu rajoituksia euroopan alueella taulukossa 3 kuvatulla tavalla. (Adrio Communications Ltd. 2014.)

Taulukko 3: 5 gigahertsin kanavarajoitukset (Adrio Communications Ltd. 2014.)

Kanava	**Taajuus**	**Säännöstö Euroopan alueella**
36	5180	Sisätiloissa

40	5200	Sisätiloissa
44	5220	Sisätiloissa
48	5240	Sisätiloissa
52	5260	Sisätiloissa / DFS / TPC
56	5280	Sisätiloissa / DFS / TPC
60	5300	Sisätiloissa / DFS / TPC
64	5320	Sisätiloissa / DFS / TPC
100	5500	DFS / TPC
104	5520	DFS / TPC
108	5540	DFS / TPC
112	5560	DFS / TPC
116	5580	DFS / TPC
120	5600	DFS / TPC
124	5620	DFS / TPC
128	5640	DFS / TPC
132	5660	DFS / TPC
136	5680	DFS / TPC
140	5700	DFS / TPC
149	5745	SRD
153	5765	SRD
157	5785	SRD
161	5805	SRD
165	5825	SRD

DFS (Dynamic Frequency Selection) tarkoittaa teknologiaa, jolla tukiasema itse määrittää käyttämänsä kanavan valitsemalla kanavan jossa on vähiten häiriöitä havaittavissa. TPC (Transmit Power Control) on tekniikka, jolla pyritään vähentämään langattomien verkkojen välistä häiriötä pudottamalla tukiaseman lähetystehoa. SRD-kanavat (Short Range Devices) on tarkoitettu vain lyhyen matkan laitteiden käyttöön, joissa käytetään korkeintaan 25 milliwatin tehoja. (Adrio Communications Ltd. 2014.)

4.8 Sijoittelu ja kuuluvuus

Langattomien tukiasemien optimaalinen sijoittelu on suhteellisen tärkeää, jotta verkon signaali on paras mahdollinen eikä katvealueita syntyisi. Tukiasemien sijoittelussa tulee välttää suuria metallisia esteitä, jotka estävät ja heijastavat langattoman verkon signaalia. Myös paksut kivi- ja betoniseinät estävät signaalin kulkua. On syytä välttää sijoittamasta tukiasemaa lähelle samalla taajuusalueella toimiva laitteita, kuten esimerkiksi mikroaaltouuneja. Paras sijainti tukiasemalle on usein keskellä aluetta, jossa langattomia laitteita tullaan käyttämään. Jos langattoman verkon alueelle jää katvealueita, joita ei tukiasemaa

siirtelemällä tai antenneja suuntaamalla saada katettua, markkinoilla on ostettavissa langattoman verkon toistimia, joilla verkkoa voidaan laajentaa.

4.9 Roaming-toiminnallisuus

Roaming tai verkkovierailu on tärkeä ominaisuus kaikissa suurissa langattomissa verkoissa, joiden pitää kattaa suurempi alue kuin yhdellä tukiasemalla on mahdollista. Verkkovierailulla tarkoitetaan tässä tapauksessa päätelaitteen liikkumista useamman langattoman tukiaseman välillä. Yksinkertaisimmillaan verkkovierailu saadaan aikaiseksi kytkemällä tukiasemat johdolla samaan lähiverkkoon ja konfiguroimalla ne siltaavaan tilaan normaalin reitittävän tilan sijasta. Tukiasemat tulisivat konfiguroida käyttämään samaa SSID-nimeä ja salaustapaa, mutta eri kanaville jotta ne eivät häiritse toisiaan. Tukiasemien täytyy olla myös riittävän lähellä toisiaan, jotta asiakaspäätteet liikkuessaan voivat havaita molemmat tukiasemat samanaikaisesti katkotonta tukiasemanvaihdosta varten.

5 Langattoman vierailijaverkon toteutus

Organisaatiossa koettiin tarpeelliseksi toteuttaa langaton verkko koko kiinteistön laajuisesti, pääasiasiassa johtuen kannettavien tietokoneiden yleistymisen johdosta. Tähän asti talossa on toimistoverkko toteutettu vain langallisesti käyttäjien työpisteisiin ja neuvotteluhuoneisiin. Tästä syystä organisaatiossa lähdettiin tutkimaan langattoman lähiverkon hankintaa. Kun langattoman verkon hankintaa alettiin selvittää, organisaatiossa koettiin eri toimittajien ”avaimet käteen”-pakettiratkaisuiden olevan liian kalliita hankittavaksi. Tästä syntyi ehdotus rakentaa langaton verkko itse organisaation omilla resursseilla käyttäen avoimen lähdekoodin ratkaisuja. Langattoman verkon hankintaa pohdittaessa vertailtiin kustannuksia ja sen tuoman lisäarvon suhdetta valmiiden pakettiratkaisuiden sekä organisaation sisällä itse toteutetun ratkaisun välillä. Organisaation johdossa todettiin että kolmannen osapuolen toteuttama ratkaisu ei tuo enempää lisäarvoa langattoman verkon toteutukselle, koska koettiin että organisaatiolla on riittävästi osaamista sekä resursseja ennestään langattoman verkon toteuttamiselle. Tällä perusteella päädyttiin toteuttamaan langatonta verkkoa organisaation omilla resursseilla.

Langattoman verkon rakentaminen vaiheistettiin niin, että langaton toimistoverkko rakennettiin ensimmäisenä koska se oli tärkeämmällä prioriteetilla. Tämän jälkeen lähdettiin toteuttamaan langatonta vierailijaverkkoa, jotta vieraille saadaan toimivat yhteydet. Järjestelmän toteutus perustuu avoimen lähdekoodin ohjelmistoratkaisuihin, jolloin itse ohjelmistoista ei tule hankinta- tai lisenssikustannuksia. Kustannuksena järjestelmän toteutuksessa on asiantuntijoiden työpanos organisaatiossa sekä itse laitteiston hankinta, joka koostuu lähinnä langattomista tukiasemista, kaapeloinnista sekä asennuksesta organisaation tiloihin.

5.1 Laitteisto- ja laiteohjelmistovalinnat

Langattomia tukiasemia hankittaessa ensisijaisena vaatimuksena oli saada laitteeseen asennettua avoimen lähdekoodin kustomoitava OpenWRT tai DD-WRT firmware-laiteohjelmisto. Kustomoitu laiteohjelmisto mahdollistaa sen, että laitteita voidaan ylläpitää ja konfiguroida keskitetysti. Ne saadaan myös integroitumaan paremmin organisaation infrastruktuuriin omalla laiteohjelmistolla.

Laiteohjelmistoa valittaessa aluksi tutkittiin DD-WRT-laiteohjelmistoa vaihtoehtona, mutta nopeasti huomattiin tuetun laitteiston heikko valikoima. Yrityskäyttöön olevia laitteita ei ollut montaa ja niistäkin monet poistuneet jo markkinoilta. Tämän johdosta siirryttiin tutkimaan OpenWRT-laiteohjelmistoa vaihtoehtona sopivaksi alustaksi. Pienehkön selvitystyön jälkeen OpenWRT todettiin hyväksi laiteohjelmistovalinnaksi johtuen laajasta tuettujen laitteiden laitekannasta, laiteohjelmiston loogisesta ja modulaarisesta rakenteesta sekä tekstitiedostopohjaisista konfiguraatiotiedostoista.

Laitevalinnoissa haettiin laitteita, jotka olisivat helppo konfiguroida käyttämään kustomoitua laiteohjelmistoa, ne olisi riittävän tehokkaita palvelemaan montaa käyttäjää ja ne olisivat riittävän edullisia hankittavaksi koko kiinteistön kattavasti. Tekniset vaatimukset langattomille tukiasemille oli kustomoitava laiteohjelmisto kuten DD-WRT tai OpenWRT, dual band-tuki, Gigabit Ethernet-tuki, VLAN-tuki ja monen SSID:n tuki. Hankinnoissa päädyttiin TP-Link WDR-4300-tukiasemaan joka täyttää yllä määritetyt vaatimukset.

Laitteen tekniset ominaisuudet (OpenWRT Project 2014.):

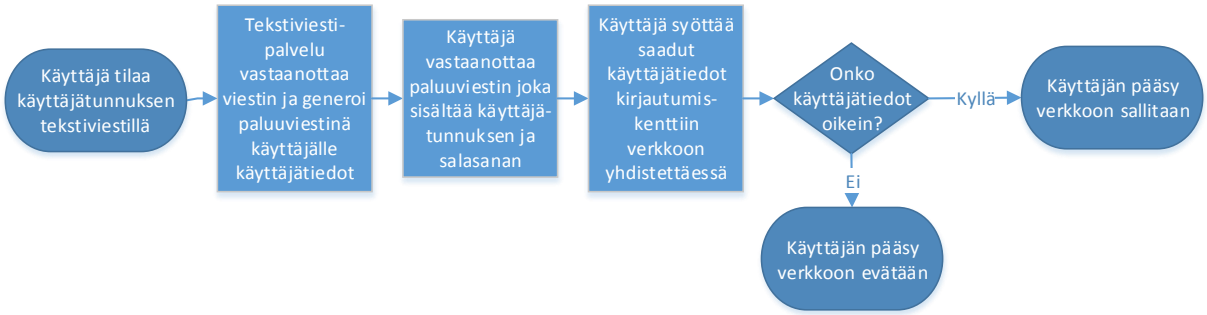
- Prosessori: Atheros AR 9344 (MIPS-pohjainen)
- Flash-muistia: 8 megatavua
- RAM-muistia: 128 megatavua
- 4 Gigabit Ethernet-porttia
- 1 Gigabit Ethernet-portti WAN-liitäntään
- 2 USB 2.0 porttia
- VLAN-tuki: 128 virtuaalilähiverkolle

5.2 Käyttäjätunnusten rekisteröiminen

Projektissa päädyttiin autentikoimaan käyttäjiä käyttäjätunnus-salasanaparilla. Tämä koettiin helpoimmaksi tavaksi toteuttaa ja sillä päästään tavoitteeseen luoda suojattu langaton vierailijaverkko. Käyttäjätunnusten toimitus käyttäjälle on toteutettu Gammu-SMSD-tekstiviestijärjestelmällä. Gammu-SMSD-sovellukseen päädyttiin, koska se projektin asiantuntijoilla oli ennestään kokemusta kyseisen sovelluksen konfiguroinnista ja

käytöstä. Gammu-SMSD on GSM-modeemin kautta toimiva tekstiviestien toimituspalvelu Linuxille. Palvelu kuuntelee palvelimeen liitetyn GSM-modeemin avulla siihen saapuvia tekstiviestejä. Kun modeemiin asetettuun puhelinnumeroon lähetetään määrätyn muotoinen tekstiviesti, tekstiviestipalvelu reagoi siihen generoimalla satunnaisen käyttäjätunnuksen ja salasanan. Salasanasta lasketaan tiiviste, joka tallennetaan käyttäjätunnuksen kanssa MySQL-tietokantaan. Käyttäjätunnusten luomisen jälkeen käyttäjätunnus ja salasana lähetetään tekstiviestinä takaisin käyttäjän matkapuhelimeen, josta tilausviesti lähetettiin.

Kuvassa 5 on kuvattu langattoman vierailijaverkon käyttäjätunnusten tilausprosessi. Käyttäjä voi tilata itse tunnukset tekstiviestillä, jolloin järjestelmä luo satunnaisen käyttäjätunnuksen sekä salasanan ja lähettää ne paluuviestinä käyttäjälle. Käyttäjätunnukset ja salasanat tallennetaan MySQL-tietokantaan, jota vasten langattoman verkon Radius-palvelin autentikoi langattomaan verkkoon kirjautuvia käyttäjiä.



Kuva 5: Vuokaavio käyttäjätunnusten tilausprosessista

5.3 Käyttäjien autentikoiminen

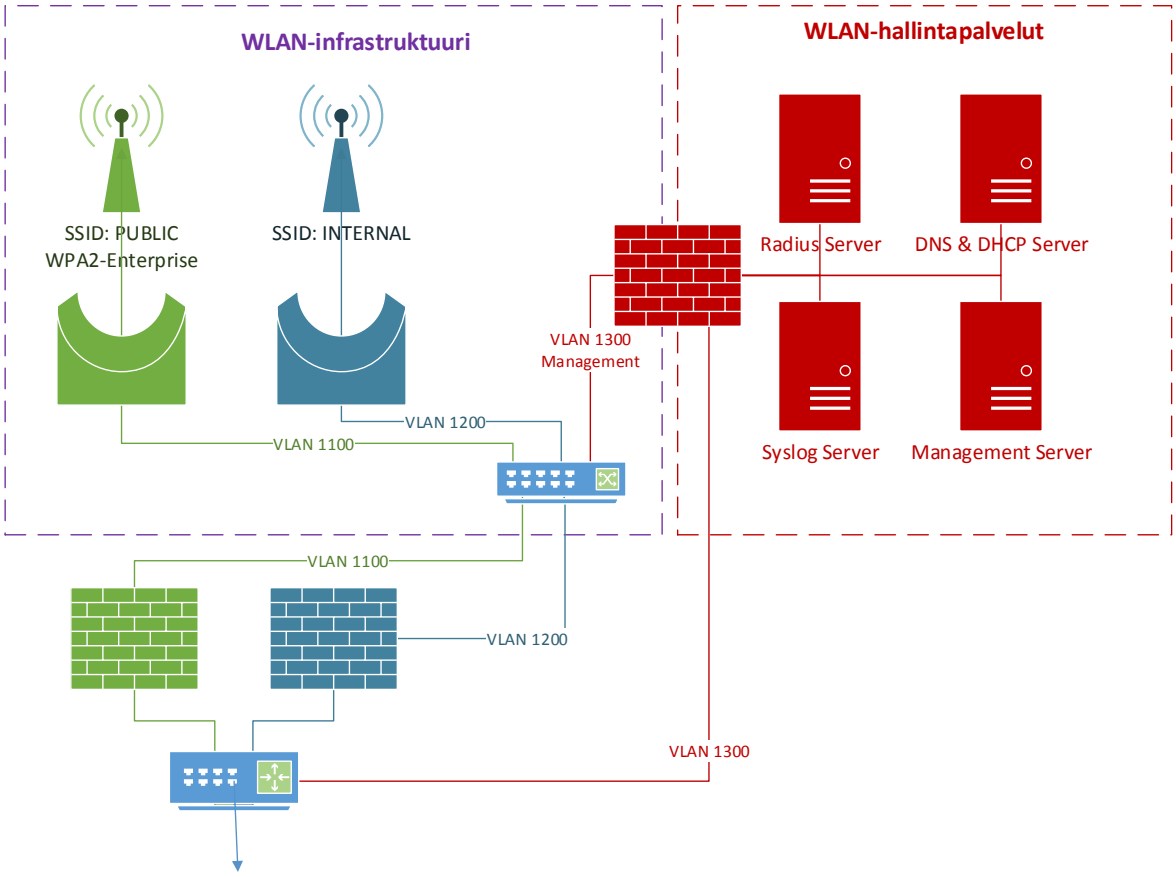
Käyttäjien autentikoiminen langattomassa vierailijaverkossa tapahtuu Radius-palvelimen avulla. Langattoman toimistoverkon puolella käyttäjien autentikointi oli ratkaistu FreeRADIUS-palvelimen avulla, jolloin oli luonnostaan helppoa ottaa samanlainen ratkaisu käyttöön myös vierailijaverkon puolella. Vierailijaverkon tukiasemat on määritetty käyttämään WPA2-Enterprise-salausta, jossa käyttäjät autentikoidaan 802.1X-standardin mukaisen toimintalogiikan mukaisesti. Kun käyttäjä liittyy verkkoon päätelaitteella, kysytään häneltä käyttäjätunnusta ja salasanaa jotka hän on itse tilannut tekstiviestitse. Käyttäjä syöttää käyttäjätunnuksen ja salasanan kenttiin, tukiasema lähet-

tää Radius-autentikointipyynnön Radius-palvelimelle. Palvelin tarkastaa MySQL-tietokannasta löytyykö kyseistä käyttäjätunnus-salasanaparia ja jos vastaavuus löytyy, Radius-palvelin vastaa myöntävästi tukiaseman autentikointipyyntöön.

5.4 Vierailijaverkon salaus

Langatonta vierailijaverkkoa määriteltäessä yksi kriteereistä oli saada yksilöllinen salaus käyttäjän päätelaitteen ja langattoman verkon tukiaseman välille. Tämä vaatimus estää langattoman verkon salausvaihtoehdoista täysin avoimen verkon rakenteen, WEP-salauksen sekä WPA/WPA2-PSK-salauksen. Tästä johtuen langattoman vierailijaverkon salausmenetelmäksi valittiin WPA2-Enterprise, joka mahdollistaa käyttäjäkohtaisen autentikoinnin sekä yksilöllisen suojatun yhteyden tukiaseman ja asiakkaan välillä. Valittu salausmenetelmä on tällä hetkellä turvallisin langattomien verkkojen salauksessa teoriaosuudessa mainituista syistä.

5.5 Verkkoliikenteen reititys



Kuva 6: Langattoman verkon verkkokaavio

Langaton vierailijaverkko on haluttu pitää irrallaan organisaation sisäisestä lähiverkosta. Kuvassa 6 on esitetty verkkokaavio langattoman verkon fyysisestä reitityksestä. Langaton vierasverkko on määritetty käyttämään virtuaaliverkkoa (VLAN) 1100, joka yhdistyy palomuurin kautta vierasverkkoon ja on sitä kautta täysin irrallaan organisaation omasta verkosta. Vierailijaverkon SSID:ksi on määritetty ”PUBLIC” ja sillä nimellä se näkyy myös päätelaitteille.

Langattomat tukiasemat on asetettu siltaaviksi, jolloin tukiasemat eivät itsessään tee mitään reitityksiä vaan toimivat siltana eri verkkoihin, riippuen mihin tukiaseman tarjoamaan verkkoon käyttäjä on liittynyt. PUBLIC-verkosta on päätelaitteilla pääsy vain vierailijaverkon VLAN:iin, eikä sitä kautta pääse toimistoverkkoon tai hallintaverkkoon. INTERNAL-verkosta on pääsy vain toimistoverkon VLAN:iin, eikä sitä kautta ole pääsyä vierailijaverkkoon tai hallintaverkkoon. Hallintaverkon VLAN:iin ei ole pääsyä langattomasti lainkaan, vaan hallinta tapahtuu langallisen toimistoverkon kautta. Tuki-

asemat tekevät ainoastaan autentikointipyyntöjä verkkoon kirjautuvista käyttäjistä hallintaverkon läpi Radius-palvelimelle ja sallivat liikenteen palvelimen hyväksymiltä käyttäjiltä.

Toimistoverkko käyttää virtuaaliverkkoa VLAN 1200, joka yhdistyy palomuurin läpi talon sisäiseen verkkoon. Toimistoverkon langattoman verkon SSID:ksi on määritelty ”INTERNAL”. Hallintaverkko (VLAN 1300) sisältää tarpeelliset taustapalvelut langattoman verkon toiminnalle. Palveluihin sisältyy Radius-palvelin käyttäjien autentikointia varten, DNS- ja DHCP-palvelin nimipalveluita sekä osoitejakelua varten, Syslog-palvelin lokeja varten ja http-pohjainen hallintapalvelin tukiasemien hallintaa varten. Langattomia tukiasemia voidaan hallita etänä web-selaimella tai SSH:n yli hallintaverkon kautta.

5.6 Verkkoliikenteen kaistanhallinta ja suodatus

Langattoman vierailijaverkon kaistanhallintaa sekä suodatusta ei tulla toteuttamaan tämän opinnäytetyön aikataulun puitteissa. Ne kuitenkin tullaan toteuttamaan myöhemmässä vaiheessa langattoman verkon projektissa.

5.7 Käyttäjätunnustietokanta

Vierailijaverkkoa varten rekisteröidyt käyttäjätunnukset ja salasanat tallennetaan MySQL-tietokannan tauluun nimeltä ”user_db”, josta Radius-palvelin käy tarkistamassa käyttäjän kirjautuessa syöttämät arvot. Tauluun tallennetaan käyttäjätunnuksen ja salasanan lisäksi yksilöllinen guid-tunnus, luontiaika sekä vanhentumisen päivämäärä ja kellonaika. Käyttäjätunnustaulun rakenne on kuvattu seuraavassa taulukossa:

Taulukko 4: user_db-tietokantataulun rakenne

Attribuutti	**Tyyppi**
guid	int(10)
username	varchar(20)
password	varchar(20)
creation_time	timestamp
expiration_time	datetime

5.8 Taajuusalueet

Langaton verkko on toteutettu tarjoamaan toimistoverkkoa ja vierailijaverkkoa kahdella eri taajuusalueella, sekä 2,4 Ghz alueella että 5 Ghz:n alueella. Perinteisellä 2,4 Ghz:n taajuusalueella verkkojen kanaviksi on määritelty kanavat 1, 7 ja 13. Uudella 5 Ghz:n taajuusalueella kanavaksi on asetettu kanavat 36, 40 ja 44. Tukiasemat ovat konfiguroitu mittauksien perusteella sopiville kanaville riippuen tukiaseman sijainnista rakennuksessa. Tukiasemiin on määritelty molempien taajuusalueiden kanavat pareina pienimmästä suurimpaan seuraavasti: 1 + 36, 7 + 40 ja 13 + 44. Tämä tarkoittaa sitä, että tukiasema joka on konfiguroitu toimimaan kanavalla 1 2,4 gigahertsin alueella, tarjoaa samaan aikaan verkkoa kanavalla 36 5 gigahertsin verkossa.

7 Yhteenveto

Projektin tekeminen oli melko haasteellista johtuen hyvin tiiviistä aikataulusta. Projektityöhön paneutuminen ei ollut aina mahdollista johtuen muista ajankäytöllisistä tekijöistä. Aikataulu ei antanut myöskään kovin paljon mahdollisuuksia projektin vaiheiden viivästymiselle. Projektissa ei kuitenkaan tapahtunut pahoja viivästyksiä tiukasta aikataulusta huolimatta, vaan aikataulussa pysyttiin kohtalaisen hyvin lukuun ottamatta muutamaa aikataulun ulkopuolelle jätettyä vaihetta. Projektissa jouduttiin jättämään kaistanhallinnan ja verkkoliikenteen suodatuksen toteutus projektiaikataulun ulkopuolelle aikataulusyistä. Projektille varattiin 12 viikkoa aikaa, johon sisältyi vierailijaverkon määrittely, verkkoreitityksen suunnittelu ja toteutus, käyttäjien autentikoinnin suunnittelu ja toteutus, käyttäjätunnusten rekisteröinnin suunnittelu ja toteutus, kaistanhallinta, liikenteen suodatus sekä dokumentaation ja tämän raportin työstäminen. Eniten aikaa projektissa kului käyttäjien autentikointimenetelmän valintaan ja sitä kautta käyttäjätunnusten rekisteröimisen suunnitteluun ja toteutukseen.

Projektin tavoitteet saavutettiin onnistuneesti, joista tärkeimpänä itse vierailijaverkko saatiin rakennettua toimintakuntoon. Käyttäjätunnusten rekisteröiminen verkkoon on suhteellisen uniikki tapa toimittaa käyttäjätunnuksia vierailijaverkkoa varten, tyypillisesti vierailijaverkkoon jaetaan käyttäjätunnukset aulan vastaanottovirkailijan tai muun henkilön kautta.

Ehkä suurin oppimistapahtuma oli huomata projektin aikatauluttamisen haasteellisuus. Projekti toteutui aika pitkälti eri järjestyksessä kuin aikataulussa määriteltiin, vaikkakin tehtävät ja vaiheet pysyivät aika pitkälti samoina. Moniin tehtäviin meni enemmän aikaa kuin oli aikataulutettu. Vastaavasti kuitenkin osa tehtävistä oli nopeampia toteuttaa kuin aikataulussa oli varattu aikaa. Opin myös raporttia kirjoittaessa paljon lähteiden käyttämisestä sekä järjestelmällisestä kirjoittamisesta. Projekti oli mielenkiintoinen usean minulle uuden teknologian puolesta, joista monet ovat hyvin yksinkertaisia ajatustasolla mutta hämmästyttävän monisyisiä kun niiden toimintalogiikkaa lähtee tutkimaan syvemmältä konepellin alta.

Vierailijaverkon toteuttamista kannattaa suunnitella ja pohtia etukäteen, jotta verkosta saadaan kunnollinen, turvallinen ja varmatoiminen samalla kertaa. Tässä projektissa olisi voitu mennä aina helpoimman mukaan, mutta määrittelyt ja vaatimukset pitivät huolen että laatustandardi pysyy kunnollisella tasolla. Aikaisempi langaton vierailija-verkko oli toteutettu hieman helpommalla tavalla, joka johti tämän projektin syntyyn. Tämän kaltainen projekti on erinomainen tilaisuus oppia eri osa-alueiden teknologioita laajalla skaalalla aina perustason tietoliikenteestä langattomien verkkojen toimintaan, liikenteen salaukseen, pääsynvalvontaan ja moneen muuhun.

Lähteet

CERT Division 2014. Denial of Service Attacks. Luettavissa: http://www.cert.org/historical/tech_tips/denial_of_service.cfm. Luettu 2.11.2014.

Chris Hoffman 2013. WPA2, WEP, And Friends: What's The Best Way To Encrypt Your Wi-Fi. Luettavissa: http://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi-fi/. Luettu 13.10.2014.

Cisco Systems 2006. How Does RADIUS Work?. Luettavissa: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html. Luettu 5.11.2014.

Cisco Systems 2014. Routing Between VLANs Overview. Luettavissa: http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfvl.html#wp1003415. Luettu 4.11.2014.

DD-WRT 2014. About DD-WRT. Luettavissa: http://www.dd-wrt.com/site/content/about. Luettu 15.10.2014.

Federal Communications Commission 2009. Voice Over Internet Protocol. Luettavissa: http://www.fcc.gov/encyclopedia/voice-over-internet-protocol-voip. Luettu 3.11.2014.

IEEE Standards Association 2004. IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges. Luettavissa: http://standards.ieee.org/getieee802/download/802.1D-2004.pdf. Luettu 25.10.2014.

IEEE Standards Association 2007. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Luettavissa: http://standards.ieee.org/getieee802/download/802.11-2007.pdf. Luettu 29.10.2014.

IEEE Standards Association 2010. IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control. Luettavissa: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf. Luettu 28.10.2014.

IEEE Standards Association 2011. IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks. Luettavissa: http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf. Luettu 28.10.2014.

Informit 2005. Stateful Firewalls. Luettavissa: http://www.informit.com/articles/article.aspx?p=373120. Luettu 30.10.2014.

Justin Pot 2013. What Is WEP Wi-Fi Encryption & Why Is It Really Insecure. Luettavissa: http://www.makeuseof.com/tag/what-is-wep-wi-fi-encryption-and-why-is-it-really-insecure-makeuseof-explains/. Luettu 13.10.2014.

Mathy Vanhoef, Frank Piessens 2013. Practical Verification of WPA-TKIP Vulnerabilities. Luettavissa: http://people.cs.kuleuven.be/~mathy.vanhoef/papers/wpatkip.pdf. Luettu 21.10.2014.

OpenWRT Wiki 2014. TP-Link TL-WDR4300 Hardware specs. Luettavissa: http://wiki.openwrt.org/toh/tp-link/tl-wdr4300. Luettu 1.10.2014.

Oracle Corporation 2014. About MySQL. Luettavissa: http://www.mysql.com/about/. Luettu 28.10.2014.

Paar, C. & Pelzl, J. 2011. Understanding Cryptography. Springer. s. 87-89.

Adrio Communications Ltd 2014. Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths. Luettavissa: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php. Luettu 4.11.2014.

Tallinn University of Technology 2007. VLAN-Perusteet. Luettavissa: http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html. Luettu 1.10.2014.

Tech-FAQ 2014. Temporal Key Integrity Protocol. Luettavissa: http://www.tech-faq.com/tkip-temporal-key-integrity-protocol.html. Luettu 29.10.2014.

Technopedia 2014. Man-in-the-Middle Attack (MITM). Luettavissa: http://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm. Luettu 28.10.2014.

TechTarget 2014. Using VLANs to compartmentalize WLAN traffic. Luettavissa: http://searchnetworking.techtarget.com/feature/Using-VLANs-to-compartmentalize-WLAN-traffic. Luettu 22.10.2014.

The Cisco Learning Network 2011. WEP, WPA, WPA2, TKIP, AES, CCMP, EAP. Luettavissa: https://learningnetwork.cisco.com/thread/11207. Luettu 15.11.2014.

The FreeRADIUS Server Project 2014. The FreeRADIUS Project Home. Luettavissa: http://freeradius.org/. Luettu 16.11.2014.

Liitteet

Liite 1. Langattoman verkon tietokannan rakenne

```
CREATE TABLE `txtmsg_in` (
  `sms_sender_phonenumber` varchar(20) NOT NULL,
  `sms_message` varchar(32) NOT NULL,
  `message_serial` int AUTO_INCREMENT NOT NULL,
  `sms_received_from_network` timestamp NOT NULL DEFAULT CUR-
RENT_TIMESTAMP,
  `work_status` int(4) NOT NULL DEFAULT '1' COMMENT 'received=1, under
work=2, ready=3',
  /* Keys */
  PRIMARY KEY (`message_serial`)
) ENGINE = MyISAM;

CREATE TABLE `txtmsg_out` (
  `message_serial` int AUTO_INCREMENT NOT NULL,
  `sms_message` varchar(20) NOT NULL,
  `sms_receiver_number` varchar(20) NOT NULL,
  `sms_recived_from_worker` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `work_status` int(4) NOT NULL DEFAULT '1' COMMENT 'received=1, under
work=2, ready=3',
  /* Keys */
  PRIMARY KEY (`message_serial`)
) ENGINE = MyISAM;

CREATE TABLE `user_db` (
  `guid` int(10) UNSIGNED AUTO_INCREMENT NOT NULL,
  `username` varchar(20) NOT NULL,
  `password` varchar(20) NOT NULL,
  `creation_time` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `expiration_time` datetime NOT NULL,
  /* Keys */
  PRIMARY KEY (`guid`)
) ENGINE = MyISAM;
```