TURVALLINEN KIRJAUTUMINEN YRITYKSEN WLAN-VERKKOON RADIUS-TUNNISTUKSEN AVULLA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Kari Seppälä

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

SEPPÄLÄ, KARI: Turvallinen kirjautuminen yrityksen WLAN-verkkoon
RADIUS-tunnistuksen avulla

Tietoliikennetekniikan opinnäytetyö, 54 sivua, 7 liitesivua

Kevät 2006

TIIVISTELMÄ

Lähtötilanteena tässä opinnäytetyössä oli Päijät-Hämeen Koulutuskonsernin tarve saada tiloihinsa jo muualla paljon yleistynyt WLAN-verkko. Tätä langatonta yhteyttä tultaisiin käyttämään ainakin tekniikan laitoksella, sekä tietohallinnon tiloissa, jossa tämä työ varsinaisesti tehtiin. Ongelmana oli saada aikaiseksi kaksi erillistä langatonta verkkoa, joista vain toiseen olisi pääsy vierailijoilla. Suurin ongelma olikin saada aikaiseksi turvallinen kirjautumisvaihtoehto, joka toimisi molemmissa verkoissa.

Teoriaosassa käydään läpi RADIUS-protokollan toimintaa, sen periaatteita ja salausta. Lisäksi käydään läpi RADIUS-protokollan salausalgoritmeja. Samalla selvitetään myös langattomien verkkojen tekniikkaa sekä niiden yleisimpiä standardeja.

Käytännön osassa asennetaan RADIUS-protokollaa käyttävä IAS-palvelin (Internet Authentication Service), sekä Hewlett-Packard W420 WLAN-tukiasema. Samalla kerrotaan tehdyistä testauksista ja saaduista tuloksista.

Työssä onnistuttiin hyvin ja tehty verkko sekä kirjautuminen toimi melkein kaikilta osin niin kuin sen pitikin. Työn tuloksena voidaan sanoa, että RADIUS-protokollaa käyttäen tietoverkkoon kirjautuminen on sekä helppoa, että suhteellisen turvallista.

Asiasanat: RADIUS, IAS, WLAN, autentikointi

Lahti University of Applied Sciences
Faculty of Technology

SEPPÄLÄ, KARI: Safe logging into the WLAN deploying the RADIUS authentcation

Bachelor's Thesis in Telecommunications Technology, 54 pages, 7 appendices

Spring 2006

ABSTRACT

The aim was to examine possible ways to authenticate into a WLAN safely. This thesis was commissioned by the Lahti Region Educational Consortium (PHKK) because it needed of a wireless network in its different facilities.

There were several requirements to be met. There should be two different WLANs, which should not interfere with each other. Logging into the network should be simple and effortless and, furthermore, it should be safe.

The two WLANs to be created were to serve different purposes. The first one was to be used by the visitors only. It was important that people who use this WLAN could not use or see the other WLAN. The other WLAN was built for the people who work at the office. The WLAN was built so that these people could use their WLAN like the visitors. The only difference was that instead of getting only the Internet access, they get access to their work folders in the intranet, as well.

The work was a success. All the requirements were met. Safe logging into the WLAN was done by using the RADIUS protocol. That protocol turned out to be both reliable and easy to use.

Keywords: RADIUS, WLAN, authentication

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, Authorization, Accounting. AAA-palvelut, jotka käsittävät kaikki ne menetelmät ja tiedot, joita tarvitaan yksittäisen asiakkaan tunnistamiseen, valtuuttamiseen ja laskuttamiseen.
AD	Active Directory. Tietokanta, johon on tallennettu tiedot verkon käyttäjistä ja laitteista, kuten käyttäjätunnukset ja salasanat.
AP	Access Point. Langattoman yhteyden liityntäpiste, yleensä tukiasema.
ASP	Active Server Pages. Dynaamisesti generoituvat Web-sivut. Lisäpalvelu IIS:iin.
ASP.NET	Active Server Pages. Microsoftin kehittämä dynaamisten www-sivujen luomiseen tarkoitettu palvelinpuolen ohjelmointimenetelmä.
CA	Certification Authority. Sertifikaatteja myöntävä palvelu, joka allekirjoittaa sertifikaatit sekä sulkulistat yksityisellä avaimellaan.
CCK	Complement Code Keying. Koodaus, jossa data lähetetään 64 8-bittisenä koodisanan sarjoina.
CHAP	Challenge-Handshake Authentication Protocol. Haaste-vaste autentikaatioprotokolla.
DSSS	Direct Sequence Spread Spectrum. suorasekvenssihajaspektrihyppely-tekniikka, jossa sanoma lähetetään jaettuna pieniin osiin ja lähetetään koko taajuusalueella yhtenä signaalina.
EAP	Extensible Authentication Protocol. 801.1X:n kanssa toimiva tunnistusprotokolla.
FHSS	Frequency Hopping Spread Spectrum. Taajuushyppelyhajaspektritekniikka. Taajuushyppelyssä lähettäjä vaihtaa satunnaisesti lähetystaajuutta tietyn algoritmin mukaisesti.

FTP	File Transfer Protocol. TCP-protokollaa käyttävä tiedostonsiirto-menetelmä kahden tietokoneen välille.
FUNET	Finnish University and Research Network. Suomen korkeakoulujen ja tutkimuksen tietoverkko.
HTML	Hypertext Markup Language. Avoin standardoitu kuvauskieli, jolla voidaan kuvata Web-pohjaisia sivuja ja niiden rakennetta.
HTTP	Hypertext Transfer Protocol. Protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
HTTPS	HTTP-protokollan salattu versio.
IAS	Internet Authentication Service. Microsofin kehittämä ohjelma, joka takaa käyttäjälle keskitetysti AAA-palvelut.
ID	Identity. Yksilöllinen tunnus tai nimi.
IEEE	Institute of Electrical and Electronics Engineers. Yhdysvaltalainen sähkö-ja elektroniikka-alan järjestö, jonka dokumentteja on yleisesti alettu pitää standardeina.
IETF	The Internet Engineering Task Force. Internet-protokollien standar-doinnista vastaava organisaatio.
IIS	Internet Information Services. Microsoftin kehittämä WWW/FTP-palvelinohjelmisto, joka on tarkoitettu käytettäväksi Windows-pohjaisissa palvelimissa.
IP	Internet Protocol. Pakettien siirrosta vastaava protokolla.
IP-luokka	International Protection. Koodi, joka ilmaisee, millaisia ulkoisia vai-kutuksia laitteisto on suunniteltu kestämään.
MAC	Medium Access Control. OSI-mallin siirtoyhteyskerroksen alempi kerros.

MAC-osoite	Media Access Control. Verkkokortin fyysinen osoite (12-hexa-desimaali- numeroinen), joka koostuu verkon valmistajan omasta osoitteesta (6 ensimmäistä) sekä juoksevasta sarjanumerosta (6 viimeistä).
MD-5	Message Digest (Version 5). Viestintiivistealgoritmi.
MS-CHAP	Microsoft Challenge. Handshake Authentication Protocol, Micro-softin versio haaste-vaste autentikaatioprotokollasta.
NAS	Network Access Server. Palvelin, jonka kautta langaton kone pääsee verkkoon. Esimerkiksi tukiasema.
OFDM	Orthogonal Frequency-Division Multiplexing. Monikantoaalto-modulaatio, tiedon siirtoa lukuisilla toisiaan häiritsemättömillä taajuuskanavilla yhtä aikaa.
OSI	Open Systems Interconnection, malli. Joka kuvaa tiedonsiirto-protokollien yhdistelmän seitsemässä kerroksessa.
OTP	One Time Password. Kertakäyttösalasana.
PAP	Password Authentication Protocol. Autentikaatioprotokolla.
PHKK	Päijät-Hämeen Koulutuskonserni.
PHP	Hypertext Preprocessor. Ohjelmointikieli, jota käytetään etenkin Web-palvelinympäristössä luotaessa dynaamisia sivuja.
PPP	Point-to-Point Protocol. Koneiden välille muodostetaan suora yhteys verkon yli.
RADIUS	Remote Authentication Dial In User Service. Etäautentikointi-protokolla.
RAS	Remote Access Server. Etäutentikointipalvelin. Yleensä esimerkiksi WLAN-tukiasema.

SNMP	Simple Network Management Protocol. TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla.
SSID	Service Set ID. Tukiasemalle asetettava ainutlaatuinen nimi, jolla verkot voidaan erottaa toisistaan ja jolla oikeaa verkkoa on helpompi hakea.
TLS	Transport Level Security. Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
UDP	User Datagram Protocol. Yhteydetön TCP/IP-yhteyskäytäntö, jolla sovellus voi lähettää viestejä toiselle tietokoneelle.
VLAN	Virtual Local Area Network. Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin verkkoihin. Koneet voidaan jakaa omiin loogisiin verkkoihin riippumatta fyysisestä kaapeloinnista.
VPN	Virtual Private Network. Etätyöskentelyssä käytettävä yhteys. VPN:llä saadaan aikaan suojattu yhteys kotikoneen ja työpaikan verkon välille, jolloin työskentely ja datan siirto on turvallista.
WEP	Wired Equivalent Privacy. 802.11-suosituksen ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.
WLAN	Wireless Local Area Network. Langaton lähiverkko, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.
WPS	Wireless Provisioning Services. Microsoftin käyttämä autentikointipalvelu. WPS Toolilla pystytään myös luomaan käyttäjä/salasanapareja.

1 JOHDANTO

Langattomat tietoverkot lisääntyvät nopeasti. Yhä useammin niitä on myös yrityksissä. Joskus on tärkeää sallia myös yrityksessä vierailleville asiakkaille mahdollisuus päästä Internetiin, kuten vaikkapa datan hakemiseen omalta palvelimelta. Se millainen verkkokortti asiakkaan koneessa on, vaikuttaa luonnollisesti Internet-yhteyden muodostamiseen. Asiakkaan halutessa liittää koneensa suoraan yrityksen ns. langalliseen verkkoon nousee aina kysymyksiä, kuten virus- ja tietoturvakysymykset. Nämä on mahdollista jättää vierailijan omiksi ongelmiksi käytettäessä langatonta verkkoa. Suurimmiksi ongelmiksi muodostunee vain kirjautuminen ja autentikointi.

Työn tilaaja, PHKK (Päijät-Hämeen Koulutuskonserni), haluaa ottaa käyttöön tiloissaan langattoman WLAN-yhteyden, jonka kautta vierailijalla olisi mahdollisuus saada langaton yhteys Internetiin. Aluksi tätä testataan tietohallinnon tiloissa, mutta tarkoitus on kattaa kaikki PHKK:n toimitilat samanlaisella tekniikalla. Verkon käytöstä haluttiin tehdä helppoa. Avoin, suojaamaton verkko ei tullut kyseeseen, sillä asiattomia käyttäjiä ei verkkoon haluttu. Ongelmaksi oli muodostunut turvallinen kirjautuminen, jolla vierailijalle saataisiin ko. yhteys luotua. Toisaalta myös työntekijöille haluttiin antaa mahdollisuus käyttää samaa tekniikkaa omilla kannettavilla tietokoneillaan. Työtekijöille haluttiin taata mahdollisuus päästä halutessaan myös käsiksi omiin tiedostoihinsa, mutta kuitenkin haluttiin luoda yhtenäinen kirjautumisvaihtoehto. Vaihtoehtoina langattomaan verkkoon kirjautumisessa oli Smart Cardin käyttö, Shared Secret tai RADIUS-protokolla (Remote Authentication Dial In User Service). Smart Card jätettiin heti aluksi vaihtoehdoista pois kustannussyistä. Tarkemmin asiaa tarkasteltuna turvallinen kirjautuminen saatiinkin luoduksi käyttäen RADIUS-autentikointia.

2 WLAN-STANDARDIT

2.1 Langattomat lähiverkot

Jokainen yritys tarvitsee tietoverkon siirtääkseen dataa koneelta toiselle tai siirtääkseen vaikka Back-Up tiedostot palvelimelle. Nykyään tietoverkot voidaan toteuttaa myös langattomina. Langattomilla verkoilla säästetään jo pelkästään kaapeloinnissa, ja langaton verkko on vaivatonta jakaa omiin loogisiin verkkoihin. Tämä onnistuu toki perinteisellä langallisella verkollakin. Langattomien verkkojen tukiasemat voidaan säätää siten, että haluttu verkko saadaan kuulumaan vain tietyssä osassa yritystä. WLAN (Wireless Local Area Network), eli langaton paikallisverkko, on juuri tällainen verkko. Siinä dataa siirretään ilmateitse joko langattomasta laitteesta suoraan toiseen langattomaan laitteeseen (ad-hoc-verkko) tai käytetään tukiasemaa ohjaamaan datan kulkua verkon yli. Rakenne on siis melko yksinkertainen; tarvitaan laite, jossa on langaton verkkokortti sekä tukiasema, joka on kiinni reitittimessä, josta taas on pääsy ulkoverkkoon. Langattoman laitteen käyttösäde riippuu monista tekijöistä, kuten käytettävästä tiedonsiirtostandardista, verkkokortista tai vaikkapa vain maastosta. WLAN voi ulottua jopa kattamaan koko kaupungin, jolloin käytetään nimeä MAN (Metropolitan Area Network). Vaikka alue saattaa olla laaja, on se silti vielä käytännössä WLAN. Tiedon salaus tulee tällaisilla alueilla tärkeäksi osaksi turvallista tietoverkkoa. Luvussa 2 käsitelläänkin yleisimmät IEEE (Institute of Electrical and Electronics Engineers) 802-standardit joita käytetään langattomissa verkoissa (IEEE 2006).

2.2 IEEE 802.11

Vuonna 1997 IEEE julkaisi ensimmäisen WLAN-standardinsa, joka nimettiin 802.11:ksi. Standardi oli alun perin esitelty, muttei julkaistu standardina, jo vuonna 1990, eli varsinainen WLAN:iin liittyvä tekniikka esiteltiin siis vasta 1997. Uusi versio määritteli pääasiassa OSI-mallin (Open Systems Interconnection) fyysisen kerroksen sekä siirtokerroksen alemman, eli MAC-osan (Medium Access Control). Se käsittelee siis LAN:ia joissa laitteet ovat lähellä toisiaan sekä yhteydessä keskenään ilmassa kulkevan signaalin kautta. Tämä oli ensimmäinen

WLAN-tekniikka, jossa ainakin nimellinen nopeus oli joko 1 tai 2 megabittiä sekunnissa ja taajuutena oli ns. vapaa taajuus, 2.4 Gigahertsiä. Välitystekniikoiksi ilmoitettiin radiotaajuus sekä infrapuna. Radiotaajuustekniikoista käytetään suorasekvenssihajaspektri- (DSSS, Direct Sequence Spread Spectrum) sekä taajuushyppelyhajaspektritekniikoita (FHSS, Frequency Hopping Spread Spectrum). Infrapuna määriteltiin siis myös jo alkuperäisessä standardissa, mutta sillä ei ole ollut oikein käytännön merkitystä. Verkkotopologiaksi standardissa määritettiin Ad-Hoc-verkko, jossa mobiiliasemat (ms) ovat yhteydessä suoraan toisiinsa. Lisäksi määriteltiin infrastruktuuri, jossa mobiiliasemat liikennöivät tukiaseman kautta. (Intelligraphics Inc 2005.)

2.3 802.11b

Koska 801.11:n taajuudet olivat aika pieniä, alkuperäiseen standardiin tehtiin lisäys vuonna 1999 ja tämä nimettiin 802.11b:ksi (juuri ennen 802.11a:ta). Se käyttää joko 1, 2, 5.5 tai 11 Mbps siirtonopeutta, lähetystaajuuden pysyessä samana, 2.4 GHz. Koodaukseen tuli pieni muutos ja uutena tekniikkana oli CCK-tekniikka (Complement Code Keying), jossa siis data lähetetään 64 8-bittisen koodisanan sarjoina. Sarjamuodossa jokaisella koodisanalla on oma matemaattinen merkityksensä. Vaihtoehtoisena siirtotekniikkana 802.11b tarjoaa PBCC-tekniikan (Packet Binary Convutional Coding) jonka tyypillinen kantama on noin 30 metriä nopeuden ollessa noin 11Mbit/s ja 90 metriä nopeudella 1Mbit/s. 802.11b-verkkokortit toimivat 11Mbit/s nopeudella, mutta ne voivat toimia myös 5.5, 2 ja 1 Mbit/s nopeuksilla. Normaalisti tukiasema hakee automaattisesti nopeimman mahdollisen nopeuden, joka tunnetaan nimellä adaptiivinen nopeus (Adaptive Rate Selection). Nopeutta hidastamalla saadaan signaalin laatua parannettua. 802.11b ja 802.11g jakavat kaistan 14 kanavaan, jotka ovat osittain päällekkäin. Kanavat ovat jaoteltu niin, että niiden keskukset ovat 5 MHz:n päässä toisistaan. 802.11b ja 802.11g eivät määrittele erikseen kanavan leveyttä, vaan paremminkin määrittelevät juuri kanavan keskustaajuuden ja spektrin peittoalueen jokaiselle kanavalle. (Puska, 2005, 15; 25-55.)

802.11b-protokollaan on tehty joitain lisäyksiä, joita ovat mm. purskeiset lähetykset. Lisäyksillä on pyritty nostamaan nopeutta 22, 33 ja jopa 44Mbit/s, mutta näitä

lisäyksiä ei IEEE ole ainakaan vielä vahvistanut. Näitä lisäyksiä jotkut valmistajat kutsuvat nimellä 802.11b+. 802.11g:ssä on otettu huomioon osa näistä parannusehdotuksista. 802.11a:ssa nähtyjä ongelmia valmistuksen ja jakelun suhteen ei nähty, koska 802.11b on suora jatkos 802.11:sta kuvatulle DSSS-tekniikalle. Käytännössä 802.11b käyttää CCK-tekniikkaa, joka taas on variaatio CDMA-tekniikasta. Tästä johtuen tuotteiden valmistussarjat olivat helposti muunneltavissa, eikä suuria investointeja tuotteiden muuntamiseen tarvittu. Hintojen aleneminen, nopeampi yhteys (802.11 verrattuna) ja pidempi kantama lisäsivät langattomien verkkojen suosiota melkoisesti. (Puska, 2005, 15; 25-55.)

2.4 802.11a

Vuonna 1999 tehtiin 802.11:sta toinenkin lisäys, joka nimettiin 802.11a:ksi. Tämä julkaistiin siis 802.11b:n jälkeen. 802.11a-standardi käytti samoja protokollia kuin alkuperäinen 802.11-standardi. Taajuudeksi ilmoitetaan 5 GHz, se käyttää 52 alikanavaa, ja nopeus on kasvanut 54 Mbps:ään. Myös siirtotekniikkaan tuli muutos. Uusi tekniikka on nimeltään OFDM (Orthogonal Frequency-Division Multiplexing). OFDM-tekniikassa siirretään lähetettävät bitit yhtäjaksoisesti eri taajuuksilla.

Siirtonopeutta voidaan tarvittaessa vähentää nopeuteen 48, 36, 24, 18, 12, 9 tai 6 Mbit/s. 802.11a:ssa on 12 eri kanavaa. Nämä kanavat eivät mene toistensa päälle. 8 kanavaa on tarkoitettu erityisesti sisäkäyttöön ja 4 ulkokäyttöön. 802.11a- ja 802.11g-standardit eivät ole keskenään yhteensopivia, koska nämä standardit käyttävät eri taajuuksia. Käytettäessä 5 GHz taajuutta 2.4 GHz:n sijaan saavutetaan etuna ainakin se, että mahdollisuudet häiriöihin vähenevät. 2.4 GHz:n alue on vapaa alue ja tiuhaan liikennöity. Tosin 5 GHz käyttö vähentää aallon kantavuutta ja lyhentää matkan lähes näköyhteydeksi.

802.11a otettiin huonosti vastaan, koska samaan aikaan julkaistu 802.11b oli siihen aikaan ylivertainen teknisten ominaisuuksiensa vuoksi. Syynä saattoi olla myös se, ettei 802.11a-tuotteita ollut aluksi oikein saatavilla. Nykyisin 802.11a-tuotteita on parannettu melkoisesti. Kantama on noussut melkein 802.11b:n

tasoiseksi ja monet laitteet tukevat kahta tai jopa kolmea standardia (802.11a, b ja g).
(Puska, 2005, 13 - 105).

2.5 802.11g

Vuonna 2003 tehtiin kolmas muutos 802.11-standardiin, nimeltään 802.11g. Se toimii 2.4 GHz:n taajuudella, kuten 802.11b, mutta sen nopeudeksi on saatu 54Mbit/s. 802.11g on ns. alaspäin (taaksepäin) yhteensopiva, eli se toimii myös 802.11b standardeja käyttävien laitteiden kanssa. Tämä taas tarkoittaa sitä, että käytettäessä 802.11b- standardin laitteita (esim. verkkokortti), koko verkko hidastuu. Näin käy myös silloin, vaikka käytössä olisikin toinen laite samaan aikaan, joka käyttää 802.11g-standardia. Yleisesti voidaankin asettaa esim. tukiasema käyttämään sekä b- että g-standardeja, mutta vanhemmissa verkoissa jo pelkkä b:n mukana olo saattaa hidastaa 802.11g-verkkoa huomattavasti. Tukiasema voidaankin asettaa halutessa käyttämään pelkästään 802.11g-standardia, jos ollaan varmoja siitä, ettei 802.11b-standardia vaativia laitteita ole käytössä. Tästä on käytetty myös nimeä PureG-verkko, joka siis nimensä mukaisesti käyttää vain ja ainoastaan 802.11g-standardia. 802.11g käyttää OFDM-modulaatiotekniikkaa nopeuksilla 6, 9, 12, 18, 24, 36, 48 ja 54 Mbit/s. Nopeuksilla 5.5 ja 11Mbit/s käytetään CCK-modulaatiota. Toisin sanoen silloin liikutaan 802.11b:n nopeuksilla. Jos nopeutta lasketaan yhteen tai kahteen Mbit/s, käytetään silloin DBPSK/DQPSK+DSSS -modulaatiota. Vaikka 802.11g toimii samalla taajuudella kuin 802.11b, sillä saavutetaan suurempi datasiirtonopeus. (IEEE 2003; Puska, 2005, 13 – 105.)

Suuresta suosiostaan huolimatta 802.11g kärsii samoista ongelmista kuin pikkuveljensä 802.11b. Kuten jo aiemmin on mainittu, 2.4GHz taajuus on rankasti käytössä. Samalla taajuudella langattomien WLAN-verkkojen kanssa toimivat myös mm. mikroaaltouunit, Bluetooth-laitteet sekä langattomat puhelimet. (Puska, 2005, 13 – 105; IEEE 2006.)

IEEE:n LAN/WAN-sivusto löytyy osoitteesta: http://www.ieee802.org/. Kaikki standardit ovat täältä vapaasti ladattavissa. Liitteessä 1 on lueteltu IEEE:n 802.11 standardit.

3 RADIUS

3.1 RADIUS-protokolla

Radiuksen kehitti Yhdysvaltalainen yritys nimeltä Livingston Enterprises, Inc. Alun perin RADIUS oli suunniteltu käytettäväksi ns. sisäänsoittosarjoissa (Dial-In). Nykyään se on käytössä laajemmin, mm. langattomissa yhteyksissä, VPN-yhteyksissä (Virtual Private Network) sekä myös Apple-talk-yhteyksissä. RADIUS-spesifikaatio löytyy numerolla RFC (Request for Comments) 2865. RADIUS-autentikointistandardi löytyy numerolla RFC 2866. (Interop iLabs 2006.) RADIUS-palvelin tarkastaa kaikki yhteydenottopyynnöt ja tekee tarvittavat toimenpiteet yhteyden muodostamiseksi. RADIUS on toisin sanoen palvelin, johon keskitetään kaikki yhteydenottopyynnöt. Pyynnöt joko hyväksytään tai hylätään. (Microsoft Tech Net 2002.)

RADIUS-client, esimerkiksi tukiasema (Access Point, AP), lähettää käyttäjä- sekä yhteysparametrit RADIUS-palvelimelle RADIUS-viestinä. RADIUS-palvelin autentikoi ja antaa hyväksynnän clientin pyyntöön ja lähettää takaisin RADIUS-viestin vastauksen. Myös tukiasemassa kiinni olevat laitteet lähettävät RADIUS-kirjautumisviestejä itse RADIUS-palvelimelle. Tämän lisäksi RADIUS-standardi tukee Radiuksen käyttöä välityspalvelimena (Proxy). Tällöin proxya voidaan käyttää koneena, joka välittää viestejä ja pyyntöjä RADIUS-clienttien sekä RADIUS-palvelimen (tai toisten RADIUS-palvelimien) välillä. Proxya käytettäessä itse RADIUS-viestiä ei koskaan lähetetä suoraan clientin ja palvelimen välillä vaan aina Proxy-palvelimen kautta. (Microsoft Tech Net 2002.)

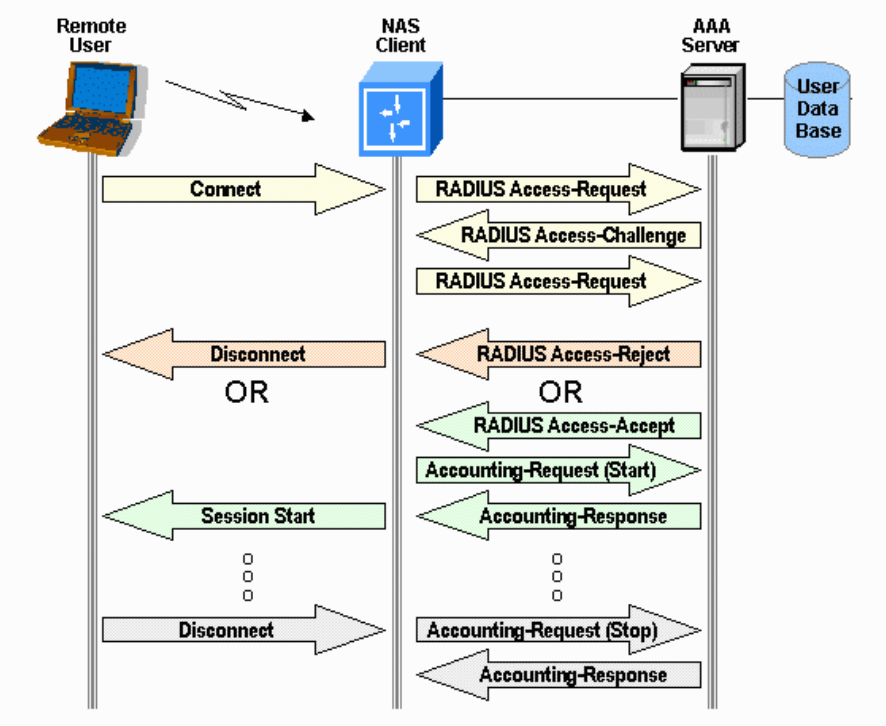
RADIUS-viestit lähetetään UDP (User Datagram Protocol) viesteinä. Radius käyttää UDP-porttia 1812 RADIUS-autentikaatioon (Authentication) ja UDP-porttia 1813 Radiuksen tilastointiin (Accounting) (Microsoft Tech Net 2002.)

Jotkut vanhemmat palvelimet voivat käyttää UDP-portteja 1645 ja 1646 samoihin tehtäviin. Näitä portteja käytettiin aiemmin vanhemmissa Windows-palvelinversioissa, mutta ne aiheuttivat ongelmia muiden järjestelmien kanssa. Aiemmin mainittu RFC 2865 määritteleekin virallisiksi porteiksi 1812 ja

1813. Mainittakoon, että yhteen UDP-pakettiin sisällytetään vain yksi viesti, eli clientin ja palvelimen välillä kulkee lukuisia paketteja, jotta autentikointi saadaan tehtyä. (Kivimäki, 1999, 831; Microsoft Tech Net 2002.)

3.2 RADIUS-viestityypit

RFC 2865 sekä 2866 määrittelevät tässä luvussa esiteltävät RADIUS-viestityypit. Vertaa niitä kuvioon 1. Kuviossa 1 Remote User kuvaa kannettavaa tietokonetta. NAS (Network Access Server) Client on tukiasema ja AAA (Authentication, Authorization, Accounting) Server RADIUS-palvelin. User Database taas on esimerkiksi AD-tietokanta (Active Directory).



KUVIO 1. RADIUS-viestityypit (Wi-Fi Planet 2003)

- Access-Request. Sisäänkirjautumispyyntö. Työasema ottaa yhteyden tukiasemaan. Tukiasemasta lähtee sisäänkirjautumispyyntö RADIUS-palvelimelle.

- Access-Challenge. Pääsyhaaste. Pääsyhaasteviestin lähettää RADIUS-palvelin vastineena sisäänkirjautumispyynnölle. Se on haaste RADIUS-clientille (tukiasemalle) ja vaatii vastauksen.

- Access-Request. Sisäänkirjautumispyyntö. Toiseen kertaan lähetetty sisäänkirjautumispyyntö on nyt vastaus pääsyhaasteeseen. Tämä on siis käytännössä eri viesti kuin ensimmäinen sisäänkirjautumisviesti..

- Access-Accept. Hyväksymisviesti. Hyväksymisviestin lähettää RADIUS-palvelin vastineena sisäänkirjautumispyynnölle. Tämä viesti kertoo clientille, että yhteydenottoyritys on autentikoitu sekä authorisoitu.

- Access-Reject. Hylkäämisviesti. Hylkäämismisviestin lähettää RADIUS-palvelin vastineena sisäänkirjautumispyynnölle. Tämä viesti kertoo clientille, että yhteydenottoyritys on hylätty. RADIUS-palvelin lähettää viestin silloin, kun yhteydenottovalmiudet tai itse yhteydenottoyritys ei ole authorisoituja.

- Accounting-Request. Tilastointipyyntö. Tilastointipyynnön lähettää client, jolla se määrittelee tilastointi-informaation juuri hyväksyttyä yhteyttä varten. Tilastoinnin avulla voidaan etäkonetta laskuttaa yhteydestä. Tilastoinnilla saatetaan kerätä myös muuta tietoa, kuten IP-osoitteita, vierailtujen sivujen osoitteita tai muuta operaattorille oleellista tietoa.

- Accounting-Response. Tilastointivastine. RADIUS-palvelin lähettää tilastointivastineen vastineeksi tilastointipyynnölle. Viesti ilmoittaa clientin saaneen onnistuneen tilastoinnin. (Microsoft Tech Net 2002.)

Huomaa, että myös yhteyttä lopetettaessa lähetetään Accounting-Request-pyyntö, kuten kuviossa 1. Accounting-Request (Stop) tarkoittaa tässä tapauksessa, että mahdollinen laskutus yhteydestä voidaan katkaista. Mainittakoon, että jos yhteys katkeaa jostain muusta tuntemattomasta syystä, katkeaa laskutus (yleensä) automaattisesti.

3.3 RADIUS-viestien salaus

Miten RADIUS-viestit sitten saadaan pidettyä salattuna? Viestien vaihto clienttien ja RADIUS-palvelimen välillä on autentikoitu ns. shared key:n avulla. Tätä avainta ei koskaan lähetetä verkon yli, vaan se täytyy olla molempien päiden tiedossa etukäteen. Ilman tätä avainta ei autentikointi onnistu. Lisäksi käyttäjän salasanat lähetetään salattuna (encrypted). Tällä estetään se mahdollisuus, että mahdollinen verkkoon tunkeutuja tai sitä kuunteleva saisi selville salasanat. (Ilabs Interop. 2002)

Kun RADIUS-palvelin saa kirjautumispyynnön NAS-Clientilta, käy palvelin läpi tietokannan ja etsii tarvittavan käyttäjänimen. Pyynnössä saattaa olla myös informaatiota siitä, millaista ”kättelyä” käyttäjä haluaa käyttää yhteydenottoon. Radiuksessa autentikaatio ja autorisointi ovat kytketty aina samaan viestiin. Jos käyttäjänimi löytyy tietokannasta ja jos salasana on oikein, palauttaa RADIUS-palvelin pääsy hyväksytty (Access-Accept) vastauksen. Tähän kuuluu myös attribuutit siitä, millaisia parametreja käytetään juuri tässä yhteydessä. Tyypillisesti parametreihin kuuluu mm. palvelun tyyppi, protokolla, VLAN (Virtual Local Area Network), käytettävä Access-lista tai vaikkapa käytettävä WEP-avain (Wired Equivalent Privacy). (Ilabs Interop. 2002)

Jos käyttäjänimeä ei esiinny tietokannassa, RADIUS-palvelin lähettää automaattisesti hylkäämisviestin (Access-Reject Message). Sama tehdään myös, jos salasana kirjoitetaan väärin tai halutaankin kirjautua johonkin tuntemattomaan palvelimeen. Tähän viestiin voidaan liittää myös syy siihen, miksi yhteyttä ei voitu muodostaa. (Ilabs Interop. 2002.)

3.4 Point-to-Point Protocol (PPP)

Point-to-Point Protocol –authentikaatioprotokollia ovat esimerkiksi Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) sekä tästä uudempi versio, MS-CHAP version 2 (MS-CHAP v2). Käytettävä autentikaatio tukiaseman sekä clientin välillä lähetetään edelleen RADIUS-palvelimelle tarkistusta varten. Taatakseen varmasti turvallisen RADIUS-viestin client sekä RADIUS-palvelin jakavat jo edellä mainitun shared-keyn. Tällä varmistetaan RADIUS-liikenteen luottamuksellisuus. Shared key on yleensä tekstitiedostona (text string) sekä RADIUS-palvelimella että clientillä. PAP-protokolla käyttää kolmea erilaista viestityyppiä, joita ovat Authentication-Request, Authentication-Ack ja Authentication-Nack. Authentication-Request-viestiä käytetään, kun halutaan tunnistautua eli päästä verkkoon. Parametreinä käytetään käyttäjätunnus/salasana-paria. Jos vastapään käyttäjätunnus/salasana-pari vastaa ilmoitettua, on tunnistautuminen onnistunut. Silloin vastauksena lähetetään Authentication-Ack-viesti, joka ilmoittaa siis onnistuneesta autentikoinnista. Jos

autentikointi ei onnistu yllämainitulla tavalla, lähetetään Authentication-Nack-viesti. Tässä viestissä voi mukana olla parametrinä syy epäonnistuneeseen tunnis tautumiseen. PAP-protokollassa salasana lähetetään selväkielisenä, eli PAP-protokolla ei salaa salasanaa.

CHAP-protokollassa käytetään neljää eri viestityyppiä. Nämä ovat Challenge, Response, Success ja Failure. Erona PAP-protokollaan CHAP:issa tunnistamista vaativa osapuoli lähettää ensimmäiseksi Challenge-viestin, jossa se pyytää käyttäjältä käyttäjätunnusta sekä antaa haasteen. Tähän vasteena käyttäjä lähettää Response-viestin, joka sisältää käyttäjätunnus/salasana-parista lasketun tarkistussumman. Jos lähetetty tarkistussumma täsmää, on tunnistautuminen onnistunut ja tällöin tunnistautumista pyytänyt laite lähettää Success-viestin. Muussa tapauksessa lähetetään Failure-viesti, joka sisältää syyn epäonnistumiseen. CHAP-protokollaa pidetään yleisesti parempana ja turvallisempana protokollana kuin PAP-protokollaa.

3.5 MS-CHAP

MS-CHAP on Microsoftin versio Challenge-Handshake Authentication protokollasta (CHAP). Protokollasta om kaksi versiota; MS-CHAPv1 (määritelty RFC 2433) ja MS-CHAPv2 (määritelty RFC 2759). MS-CHAPv2 on päivitetty versio MS-CHAP v1:sta. MS-CHAPv2 julkaistiin varsinaisesti Windows 2000:sen yhteydessä. MS-CHAP v2 on salasanaan perustuva haaste-vaste-protokolla. Kun vastauksia lähetetään verkon yli, käytetään salausalgoritmina MD5:sta sekä DES:siä. Käytännössä palvelin, johon halutaan autentikoitua, haastaa siihen yhteyttä yrittävän laitteen. Haaste tehdään myös toiseen suuntaan, eli molemmat haastavat toisensa. Jos kummankaan vaste on väärä, yhteys evätään. Microsoft kehitti MS-CHAP v2:sen alun perin PPP-protokollaksi saadakseen paremman turvan dial-up- ja VPN-palveluihin.

3.6 IEEE 802.1X

PPP:n lisäksi EAP (Extensible Authentication Protocol) on tuettu IEEE 802-siirtoyhteyskerroksessa. IEEE 802.1X on IEEE:n standardi verkon porttiautentikoinnin toteuttamiseksi, joka määrittelee miten EAP:tä käytetään IEEE 802:sta käyttävien välineiden kanssa. Tähän kuuluu IEEE 802.11b, 802.11g sekä ethernet-kytkimet. 802.1X:n ero PPP:hen on siinä, että ainoastaan EAP-autentikaatiometodit ovat tuettuja. Tästä johtuen muiden kuin EAP-protokollien käyttö 802.1X:n kanssa on siis mahdotonta. (Microsoft Tech Net 2002.)

3.7 EAP-autentikointityypit

3.7.1 Extensible Authentication Protocol (EAP)

EAP kuten myös myöhempänä esiteltävä EAP over RADIUS kuuluvat 801.1X-salauksen piiriin. EAP oli alun perin suunniteltu PPP:n jatkeeksi satunnaisten verkkoon liittymisien mekanismiksi. Sillä yksinkertaistetaan PPP:llä tapahtuvaa tunnistusta ja helpotetaan täten vaikkapa VPN-etäyhteyksien luontia. Valittaessa jokin edellä mainituista protokollista ko. protokollan autentikaatiomekanismi otetaan käyttöön yhteyden muodostumisvaiheessa. Tämä protokolla todentaa yhteyden aitouden. Protokolla itsessään on sarja ennaltamäärättyjä viestejä lähetettynä tietyssä järjestyksessä. EAP:tä käytettäessä tarkkaa autentikaatiomekanismia ei valita yhteyden muodostusvaiheessa. Jokainen PPP-yhteys neuvottelee EAP-autentikaation vasta siinä vaiheessa, kun tulee varsinaisen autentikaation vuoro. Kun autentikaatiovaihe on saavutettu, jokainen yhteys neuvottelee erityisen EAP-yhteyden. Kun EAP-tyyppi on valittu, EAP avaa avoimen viestien vaihdon

tukiaseman ja RADIUS-palvelimen välillä. Näiden välinen neuvottelu koostuu autentikaatiopyynnöistä sekä -vastauksista. Niiden pituus ja yksityiskohdat riippuvat siitä, mitä EAP-tyyppiä käytetään. EAP tukee myös mm. OTP:tä (One Time Password), MD-5-haastetta (Message Digest Version 5 Challenge) sekä TLS (Transport Level Security) smart cardia sertifikaatin käyttöä varten. Se on suunniteltu myös tukemaan tulevia autentikaatioteknologioita. Voidaankin sanoa, että EAP on kriittinen osa turvallista yhteyttä.

3.7.2 EAP TLS ja PEAP

EAP TLS:ssä on käytössä kaksisuuntainen tunnistuminen: EAP-liikenteen salaus ja sisällön suojaus. Toimintaperiaatteeltaan EAP TLS on samanlainen kuin EAP-autentikointi, mutta erona on se, että autentikointi tapahtuu sertifikaatin pohjalta, joka vaihdetaan autentikoinnin neuvotteluvaiheessa. EAP-asiakkaan kannalta sertifikaatin varmennus voi olla hankalaa, koska sillä ei ole yleensä autentikointivaiheessa Internet-yhteyttä. Tästä johtuen palvelimen sertifikaatin oikeellisuus voi jäädä tarkistamatta. Tästä syystä käytössä on kaksi IETF:n tekemää ns. draft-määritelmää: PEAP ja EAP-TTLS (EAP Tunneled TLS). Näissä muodostetaan TLS:n avulla salattu ja suojattu yhteys, jonka sisällä autentikointi suoritetaan. Tähän käytetään jotain EAP:n autentikaatiomenetelmää, vaikkapa MD5-haastetta. PEAP:n (Protected EAP) tarkoituksena on tarjota kaksivaiheinen autentikointimenettely. Ensiksi täytyy luoda turvallinen TLS-kanava autentikoitavalta koneelta palvelimelle. Tässä vaiheessa palvelin autentikoituu työsemalle omalla palvelinvarmenteellaan, ja myös työasema pystyy tässä vaiheessa autentikoitumaan palvelimelle omalla asiakasvarmenteellaan. Jos työasema autentikoituu jo tämän ensimmäisen vaiheen aikana, on seuraava vaihe tarpeeton, jolloin sitä siis ei tehdä. Toisessa vaiheessa, kun turvallinen kanava on muodostettu, suoritetaan varsinainen autentikoituminen. Tähän käytetään jotakin EAP-menetelmää. (Microsoft Tech Net 2002.)

3.7.3 EAP OVER RADIUS

EAP over RADIUS ei ole varsinaisesti oma EAP-tyyppi, vaan siinä lähetetään EAP-viestin RAS:silta (remote access server) RADIUS-palvelimelle autentikointia varten. Clientiltä (access client. Tässä tapauksessa kannettava tietokone) RAS:sille lähetettävä viesti muutetaan EAP-viesti RADIUS-attribuutiksi ja lähetetään RAS:silta (access server) RADIUS-palvelimelle. Tukiasemasta tulee tässä tapauksessa viestien kauttakulkuohjain, jonka kautta EAP-viestit kulkevat työaseman ja RADIUS-palvelimen välillä. EAP-viestit käsitellään vain työasemassa sekä RADIUS-palvelimella. Tukiasema ei osallistu viestien käsittelyyn lainkaan. EAP over RADIUSta käytetään sellaisissa paikoissa, joissa on siis käytössä RADIUS-autentikointi. EAP over RADIUS:ksen etuna on se, ettei EAP-tyyppejä tarvitse asentaa jokaiselle tukiasemalle, vaan asennus pelkästään RADIUS-palvelimelle riittää. Kuitenkin tukiasemassa täytyy olla tuki sekä EAP:lle, että viestien välitystä varten RADIUS-palvelimelle. Tyypillisessä tapauksessa EAP over RADIUS on konfiguroitu käyttämään EAP:tä sekä käyttämään RADIUS-palvelinta autentikoinnissa. Yhteydenottotilanteessa kannettava laite neuvottelee tukiaseman kanssa EAP:n käytöstä. Kannettavan laitteen lähettäessä EAP-viestin tukiasemalle AP enkapsuloi viestin RADIUS-viestiksi ja lähettää sen eteenpäin RADIUS-palvelimelle. RADIUS-palvelin käsittelee EAP-viestin ja lähettää sen RADIUS-viestinä takaisin tukiasemalle. Tämän jälkeen tukiasema välittää EAP-viestin kannettavalle. (Microsoft Tech Net 2002.)

3.8 TACACS+

TACACS+ on Cisco Systemsin kehittämä autentikaatiomenetelmä, joka on vaihtoehtoinen RADIUS-protokollalle. TACACS+ on protokolla, joka luo yhteydet reitittimille, Network Access Servereille ja muille tietovälineille joko yhden tai useamman keskitetyn palvelimen kautta. TACACS+ tarjoaa siis erillisiä AAA-palveluja. Vaikka TACACS+ perustuu löyhästi sen edeltäjään TACACSiin, on + versio täysin uusi eikä se toimi minkään vanhemman TACACS-version kanssa. Sanotaankin, että TACACS+ ja RADIUS ovat kokonaan korvanneet vanhat

versiot, vaikkakin joitain TACACS- sekä XTACAXS-versioita on yhä käytössä. XTACACS on TACACSin parannettu versio.

Siinä missä RADIUS vertailee authentication ja authorization -parametreja käyttäjäprofiilissa, TACACS+ erottelee nämä kaksi toisistaan erillisiksi operaatioiksi. Toisena varsinaisena erona RADIUS-protokollaan voidaan pitää sitä, että RADIUS käyttää UDP-protokollaa, kun TACACS+ taas puolestaan käyttää TCP-protokollaa. Joidenkin tietohallintovastaavien mielestä TACACS+ olisi RADIUS-ta parempi vaihtoehto juuri UDP:n haavoittuvuuden takia. TCP:tä pidetään yleensä turvallisempana ja luotettavampana protokollana. Kolmas suora ero on porteissa, joita käytetään: RADIUS käyttää portteja 1812 ja 1813 ja TACACS+ käyttää TCP porttia 49. Vielä selvänä erona on tietenkin siinä, että TACACS+ tarvitsee toimiakseen Cisco Systemsin laitteita. (Cisco Systems 2005.)

Ehkä suurin ero näissä kahdessa eri protokollassa on se, että RADIUS salaa pelkästään käyttäjätunnus-salana attribuutin, ja TACACS+ puolestaan salaa kaiken datan pois lukien otsikkokentän.

RADIUS-protokollastakin on tehty uusia versioita. Uudempi RADIUS-versio on nimeltään (hupaisasti 2 x radius = diameter) DIAMETER. Suurimpina muutoksina voitaisiin mainita TCP-protokollan käyttöä TACACS+ tapaan. Kyseisestä protokollasta on tietoa ainakin tällä hetkellä hankala saada, joten se on voinut jäädä kokeilun asteelle. Ainakaan Microsoftin sivuilta ei löytynyt mitään tietoa DIAMETER-protokollasta. (DIAMETER 2005.)

4 RADIUS-PALVELIMET

4.1 Microsoft Windows 2003 IAS

4.1.1 IAS ja RAS

Windows-ympäristössä RADIUS tarvitsee toimiakseen IAS-palvelun (Internet Authentication Service). Tämä saadaan asennettua Windowsin lisää/poista ohjelmia -valikosta. IAS on lisä Microsoftin RADIUS-palvelimen sekä proxynä käytettävän palvelimen protokollaan. RADIUS-palvelinta käytettäessä IAS tarjoaa AAA-palvelut kaikille niille käyttäjille, jotka haluavat ottaa etäyhteyden verkkoon. Näitä muotoja voi olla vaikkapa VPN (Virtual Private Network) yksityisverkon käyttö tai kuten tässä tapauksessa, langattoman tukiaseman kautta, käyttäen 802.1X-protokollaa. Jos RADIUS toimii proxynä, lähettää IAS autentikaatio- ja accounting-viestit eteenpäin toiselle RADIUS-palvelimelle. Jos IAS ei ole käytettävissä, ei langattoman verkon asiakkailla ole pääsyä Internetiin, sillä IAS on pakollinen palvelu tälle toiminnalle. Toinen pakollinen palvelu, joka täytyy asentaa, on RAS. RAS on etäkäytön yhteyksienhallintapalvelu. Ilman tätä palvelua eivät yhteydet toimi, sillä RAS sekä luo, ylläpitää että katkaisee käytössä olevat etäyhteydet. Sellaisia voivat olla vaikka VPN tai dial-up (RADIUS) palvelut. Tämä saadaan asennettua myös lisää/poista ohjelmia -valikosta ja se kannattaa tehdä samaan aikaan IAS:sin asennuksen kanssa. (Kivimäki, 2005, 719.)

4.1.2 IIS ja ASP.NET

IIS ja ASP.NET kuuluvat Windowsin Application server, eli sovelluspalvelinryhmään. Näitä ei ole asennettu valmiiksi peruspalvelinasennuksessa, vaan myös ne täytyy asentaa erikseen. Application server on sovelluspalvelin, joka tarjoaa XML Web-palvelut, Web-sovellukset sekä sovellusten jakelun. IIS (Internet Information Service) on palvelu, joka avulla on mahdollista ottaa käyttöön halutessa FTP (File Transfer Protocol), SMTP, NNTP ja HTTP/HTTPS (Hypertext Transfer

Protocol/Hypertext Transfer Protocol Secure) palvelimet. ASP.NET (Active Server Pages) on ohjelmisto, jolla voidaan tuottaa ja muokata HTML-tyylisiä (Hypertext Markup Language) Web-sivuja, kuten vaikka PHP-kielellä (Hypertext Preprocessor). (Kivimäki, 2005, 1038 – 1040.)

4.1.3 Sertifikaatit

CA (Certification Authority) allekirjoittaa kaikki julkaisemansa sertifikaatit omalla yksityisellä (Private key) avaimellaan. Tätä vastaava julkinen (Public key) avain on sisällytetty sertifikaattiin, nimeltään CA-sertifikaatti (CA Certificate). Käyttäjän selaimessa täytyy olla asetettuna sertifikaatin antajan julkinen avain ns. ”luotettuna lähteenä”, jotta CA:n myöntämiin sertifikaatteihin voidaan luottaa. Julkisen avaimen periaate perustuu siihen, että henkilöllä on kaksi avainta, julkinen ja salainen. Julkinen avain voidaan julkaista vaikkapa Internetissä tai lähettää sähköpostilla salaamattomana vaikka kaikille osoitelistalla olijoille. Salainen avain on vain käyttäjän hallussa. Sertifikaatin tarkistaminen julkisen avaimen avulla toimii seuraavasti: palvelimelta lähetettävä sertifikaatti on salattu vastaanottajan julkisella avaimella. Selväkielisenä tekstinä se näyttää pelkältä kirjain/numero-sekasotkulta. Vastaanottaja avaa sertifikaatin omalla salaisella avaimella ja toteaa sen joko oikeaksi tai vääräksi. Vastaavasti voidaan sertifikaatti todeta välittömästi vanhentuneeksi tai muuten kelvottomaksi, jos se on ns. CRL-eli sulkulistalla (Certificate Revocation List). Tänne on kirjattu kaikki ne sertifikaatit, joiden ei haluta olevan enää voimassa, vaikkapa salaisen avaimen paljastumisen vuoksi. Sulkulistalla näkyy varmenteen sarjanumero, jota verrataan avattavaan varmenteeseen. Sertifikaatti onkin siis tae sille, että tilaaja saa sitä mitä tilaa ja AAA on pysynyt koskemattomana. (Netscape 2001.)

Sertifikaattipalvelimen asennuksessa kannattaa käyttää Wizardia, sillä se helpottaa työtä kummasti. Vaihtoehtoja on neljä. Ensimmäinen vaihtoehto on Enterprise root CA joka toimii ”juurena” puumaisessa rakenteessa. Kaikki sertifikaatit ovat alun perin tästä juuresta lähtöisin. Toinen vaihtoehto on Enterprise subordinate CA, jonka sertifikaatin allekirjoituksen on sertifioinut joku toinen (root) CA ja joka valvoo tämän subordinate CA:n tekemisiä. Kolmas ja neljäs vaihtoehto ovat Stand-alone CA-tyyppisiä, jotka ovat muuten samanlaisia kuin edellä, mutta voi-

vat jakaa omia allekirjoittamiaan sertifikaatteja ja ovat kuitenkin Root CA:n valvonnassa. Sertifikaattipalvelimen asennus käydään tarkemmin läpi työn käytännön osuudessa luvussa 5.

4.2 FreeRADIUS

FreeRADIUS on ilmainen ohjelma, joka on jokaisen ladattavissa vaikkapa osoitteesta http://freeradius.org. Toisin kuin Windowsin RADIUS-palvelin, joka toimii Windows-ympäristössä, on FreeRADIUS suunniteltu Linux-pohjaisille työympäristöille. FreeRADIUS-palvelimen asennuskin on erilainen kuin Windowsin vastaava. Kun Windowsin asennus toimii pelkästään graafisen ohjelman pohjalta, on Linuxin vastaava pelkästään tekstipohjaisen ympäristön varassa. Tämä asettaakin näiden ohjelmien asentajat sekä käyttäjät hieman eri asemaan, sillä ilman Linuxin tuntemusta sekä tekstipohjaisten komentojen hallitsemista, jää FreeRADIUS helposti asentamatta. Toinen ilmeinen asia on tietenkin se, että toimiakseen FreeRADIUS tarvitsee siis Linux-pohjaisen palvelimen. Molemmat RADIUS-palvelimet käyttävät UDP-protokollaviestejä toimissaan, ja molemmat käyttävät samoja portteja viestien lähettämiseen ja vastaanottamiseen. Erillistä käyttäjätietokantaa ei FreeRADIUS välttämättä tarvitse, vaan käyttäjiä voi itse lisätä halutessaan käsin. Joten periaatteeltaan sekä toiminnoltaan ovat nämä kaksi eri työympäristössä toimivaa ohjelmaa melkein samanlaisia. Mainittakoon, että clientit, eli tässä tapauksessa kannettavat tietokoneet, voivat käyttää mitä käyttöjärjestelmää hyvänsä kummassakin tapauksessa. Kannettava tietokone, jossa on Linux-käyttöjärjestelmä voi mainiosti olla yhteydessä Windows-pohjaiseen RADIUS-palvelimeen, samoin kuin Windows-käyttöjärjestelmää käyttävä kone voi ottaa yhteyden Linuxia käyttävään palvelimeen.

5 KÄYTÄNNÖN TOTEUTUS

5.1 Päijät-Hämeen koulutuskonserni

Koulutuskonserniin kuuluu kunnallisina liikelaitoksina Koulutuskeskus Salpaus, Lahden ammattikorkeakoulu ja Tuoterengas. Sisäisinä palveluyksikköinä toimivat yhteiset palvelut, joita ovat hallintopalvelut, kirjasto- ja tietopalvelut, kiinteistöpalvelut, ravintolapalvelut ja tietohallintopalvelut. Konsernin toimitusjohtajana toimii TkT Arvo Ilmavirta. Talousarvion 2004 luvuilla budjetti oli yhteensä 99 milj. euroa. Henkilöstöä kaikissa laitoksissa on yhteensä 1606 henkeä. (PHKK 2006.)

Vaikka ydinopetus onkin Lahdessa, ovat mainitut laitokset jakaantuneet yhteensä 16 eri kunnan alueelle. Eri opetuspisteitä on yhteensä 17. Myös tietohallinto sijaitsee Lahdessa, Svinhufvudinkadulla. Tämän ryppään kaikki toimipisteet ovat liitetty PHKK:n runkoverkkoon, joka on nopeudeltaan 1Gbit/s. PHKK:n runkoverkosta on suora 1Gbit/s yhteys Suomen korkeakoulujen ja tutkimuksen tietoverkkoon FUNETiin (Finnish University and Research Network). Tätä yhteyttä käytetään myös Tekniikan laitoksen työasemilla. (PHKK 2006.)

Vuonna 2005 otti PHKK käyttöön runkoverkon osalta uudet eri toimipisteitä yhdistävät yhteydet ja niiden ylläpidossa palvelut PHP:ltä (Päijät-Hämeen puhelin). Lähiverkko hoidetaan suurimmalta osalta hallittavilla kytkimillä, ja verkon hallinta sekä valvonta on jätetty PHKK:n tietohallinnon vastuulle. Tämä hoidetaan keskitetysti samasta toimipisteestä, ja tietohallinto vastaa mm. verkon toimivuudesta, kehityksestä, muutoksista, valvonnasta, liikenteen seurannasta ja ylläpidosta. (PHKK 2006.)

Tämän työn tavoitteena oli saada aikaiseksi langaton yhteys tekniikan laitoksen C-siipeen. Myöhemmin langaton verkko tulisi olemaan osa koko koulun kattavaa langatonta kampusverkkoa. Langattomia verkkoja on suunniteltu myös muihin toimipisteisiin, ja ne tultaneen toteuttamaan sellaisella aikataululla, jonka talous

antaa periksi. Tämän verkon rakennus ja testaus suoritettiin PHKK:n tietohallinto-osastolla, Svinhufvudinkadulla. Työ oli helpompi tehdä keskitetysti yhdessä paikassa ja koska tietohallinnossa löytyi sekä reitittimiä, että paikka jossa tehdä, päätettiin projekti tehdä siellä.

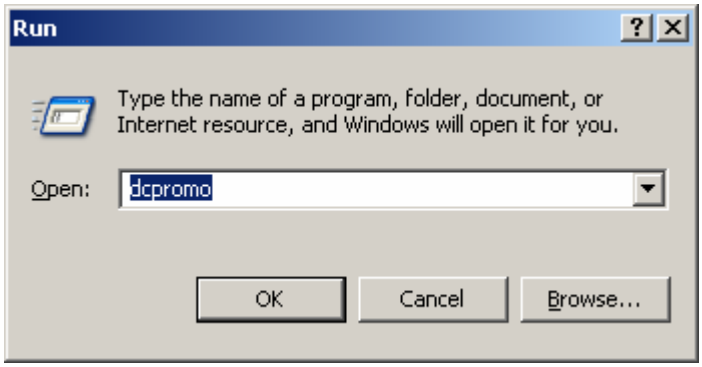
5.2 RADIUS-asennuksen taustaa

Microsoft Windows 2003 palvelimeen asennettiin RADIUS-palvelin. Kun kyseessä on Windows-ympäristö, tapahtuu sen asennus graafisessa ympäristössä. Koska RADIUS ei varsinaisesti ole oma ohjelmansa, täytyy sen toimintaan saattamiseksi tehdä joitain asetuksia ja asennuksia. Ensimmäiseksi asennettiin AD, jonka nimi kannattaa miettiä valmiiksi omaa käyttötarkoitusta silmällä pitäen. Kun tämä on tehty, voidaan edetä monella tapaa. Voidaan tehdä uusia käyttäjäryhmiä tai asentaa IAS, IIS tai CA. Tässä tapauksessa seuraavaksi asennettiin IAS ja samalla IIS. Tämä olikin viisasta, sillä jos CA:n asentaa ennen IIS:siä, se saattaa aiheuttaa joidenkin sertifikaattien toimimattomuutta. Tämä todettiin Microsoftin sivuilla, ja tyydyimme kiltisti seuraamaan ohjeita. Sekä IAS, että IIS lisätään Windowsin lisää/poista ohjelmia -valikosta. IIS:siä asennettaessa kannattaa muistaa rastittaa samalla ASP.NET, joten se asennetaan samalla. Seuraavana oli vuorossa CA:n asennus. Varsinaisessa asennuksessa kannatti käyttää työtä helpottamaan Wizardia. Tällä työkalulla saadaan aikaiseksi perusasetukset, joiden pohjalta on helppoa saada aikaiseksi tarvittava hienosäätö. CA:n palvelintyypiksi valittiin Enterprise Root Server. Tämä sopi tarkoituksiimme parhaiten, sillä tässä vaiheessa ei haluttukaan asentaa muita palvelimia tähän työympäristöön. Lisäksi asetukset tultaisiin siirtämään myöhemmin tästä testiympäristöstä varsinaiseen tuotantoympäristöön, jossa PHKK:n AD myös sijaitsee. Wizardissa kysellään kaikkea tarpeellista, kuten tehtävän palvelimen nimeä ja sertifikaatin umpeutumisaikaa. Umpeutumisajaksi jätettiin Wizardin ehdottama 5 vuotta, jolla siis ei meidän kannalta ollut merkitystä. Sertifikaatit asetetaan luotavaksi automaattisesti, joka sopi meidän tarkoituksiin mainiosti, sillä emme halunneet puuttua sertifikaattien luotiin.

5.3 IAS-asennus

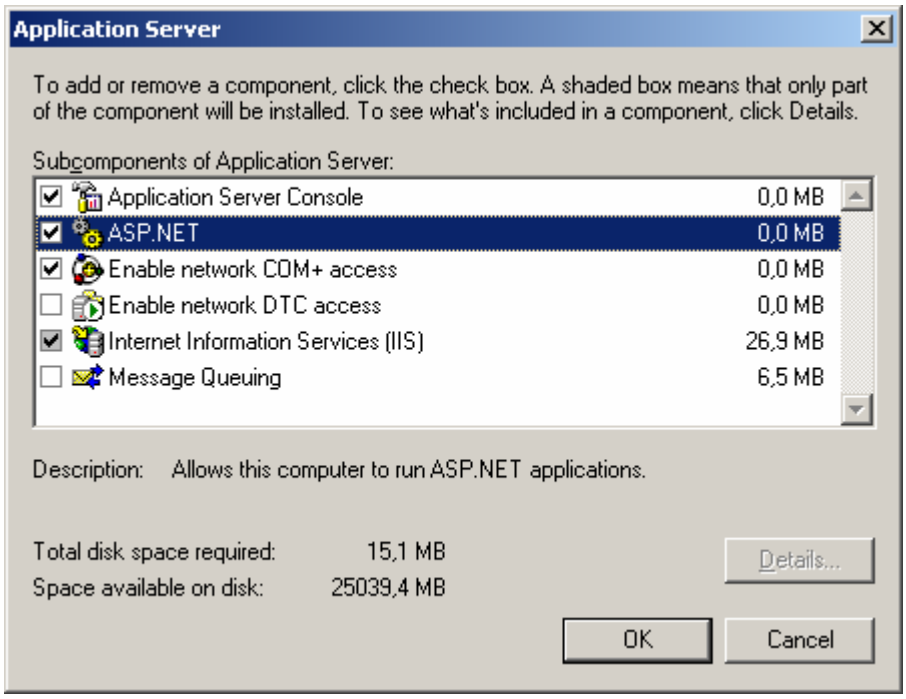
Kuten aiemmin kerrottiin, RADIUS ei ole automaattisesti valmis käyttöön Windows-palvelimen asennuksen jälkeen. Se täytyi erikseen asettaa toimimaan, ja siihen vaadittiin muutamia toimintoja. Tässä luvussa kerrotaan hieman yksityiskohtaisemmin, miten tässä työssä meneteltiin, jotta RADIUS-autentikointi saatiin toimimaan. Ensiksi asennettiin koneelle paikallinen Active Directory.

Jotta voidaan demonstroida oikean AD:n toimintaa, on palvelimella oltava joku AD, johon kirjautuminen voidaan suorittaa. AD:n teko voidaan tehdä myös lisää/poista Windowsin osia -ohjelmalla, mutta se sujuu helpoimmin komentokehotteesta aloittamalla Start -> Run. Aukeavaan kehotteeseen kirjoitettiin dcpromo, kuten voi todeta kuviosta 2.



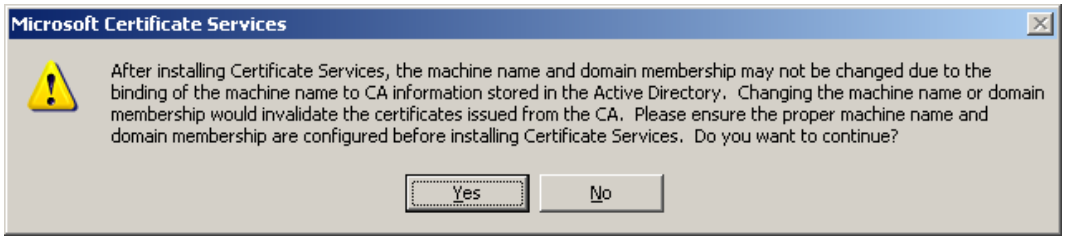
KUVIO 2. Komentokehotteen käsky

Asennus on melko yksinkertainen. Asennuksessa käytettiin oletusasetuksia, ja ne näyttivät toimivan hyvin. Tämän jälkeen asennetaan muita puuttuvia osia, joita ei ole valmiiksi asennettu perusasennuksessa, kuten IAS-palvelu. Ne löytyvät lisää/poista Windowsin osia -ohjelmasta. Täältä valitaan kuviossa 3 näkyvät vaihtoehdot.



KUVIO 3. Application Server valinnat

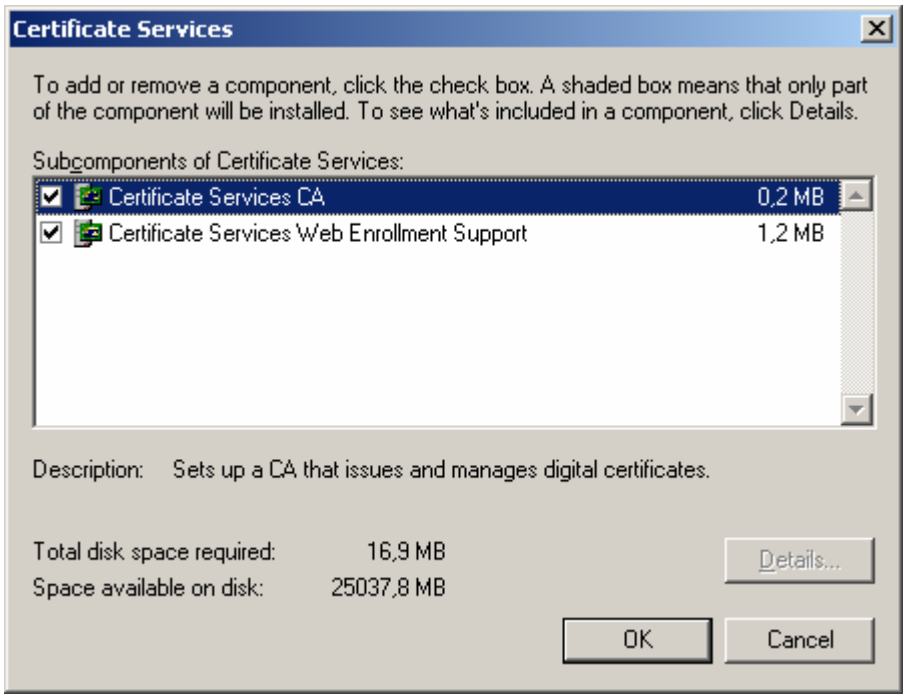
Application Server valinnan alta täytyy olla valittuna seuraavat kohdat: Application Server Console, APS.NET Enable Network COM+ access sekä Internet Information Services (IIS). Klikataan ok -> Next.



KUVIO 4. CA-nimen varoitus

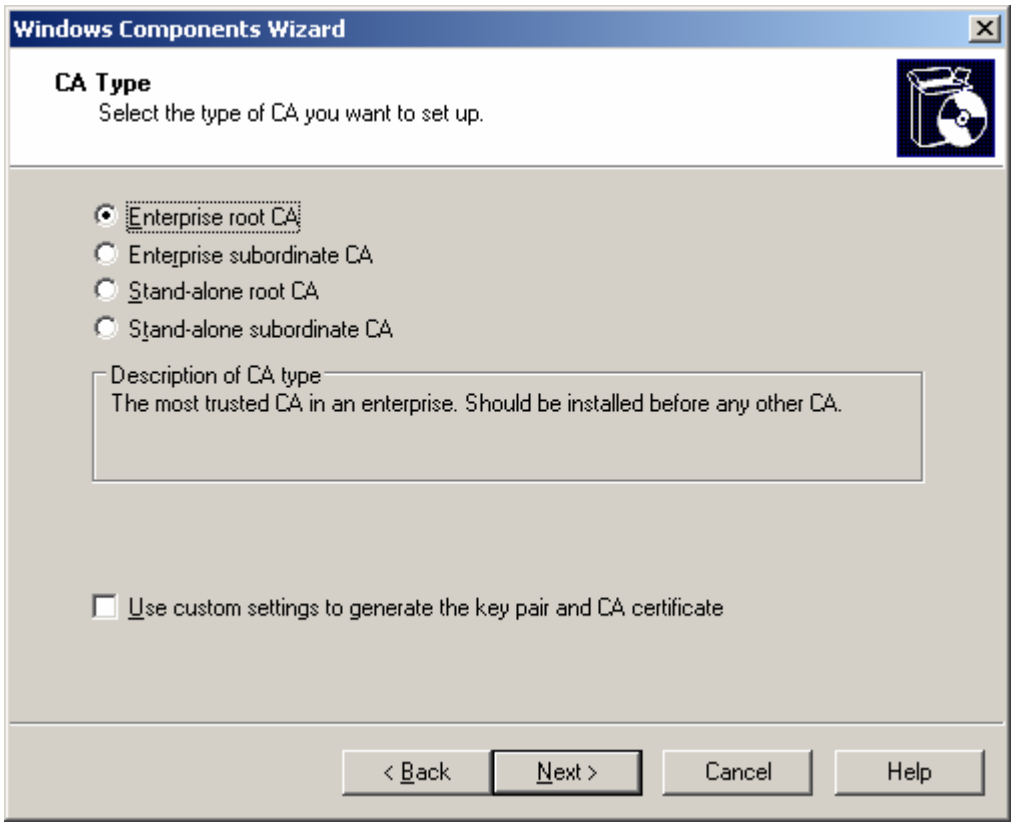
Kun Certificate services valitaan, tulee näkyviin kuvion 4 mukainen varoitusikkuna. Se ilmoittaa, ettei domainin nimeä enää tämän jälkeen voi muuttaa. Jos domainin nimeä kuitenkin muutetaan tämän jälkeen, eivät domainin sertifikaatit enää toimi. Tämän vuoksi täytyykin domainin nimi olla jo valmiiksi mietittynä.

Tämä kuitenkaan ei ole ongelma sellaisissa palvelimissa, joissa on AD jo valmiina. Seuraavaksi lisätään CA-palvelin ja valitaan molemmat kuviossa 5 olevat vaihtoehdot.



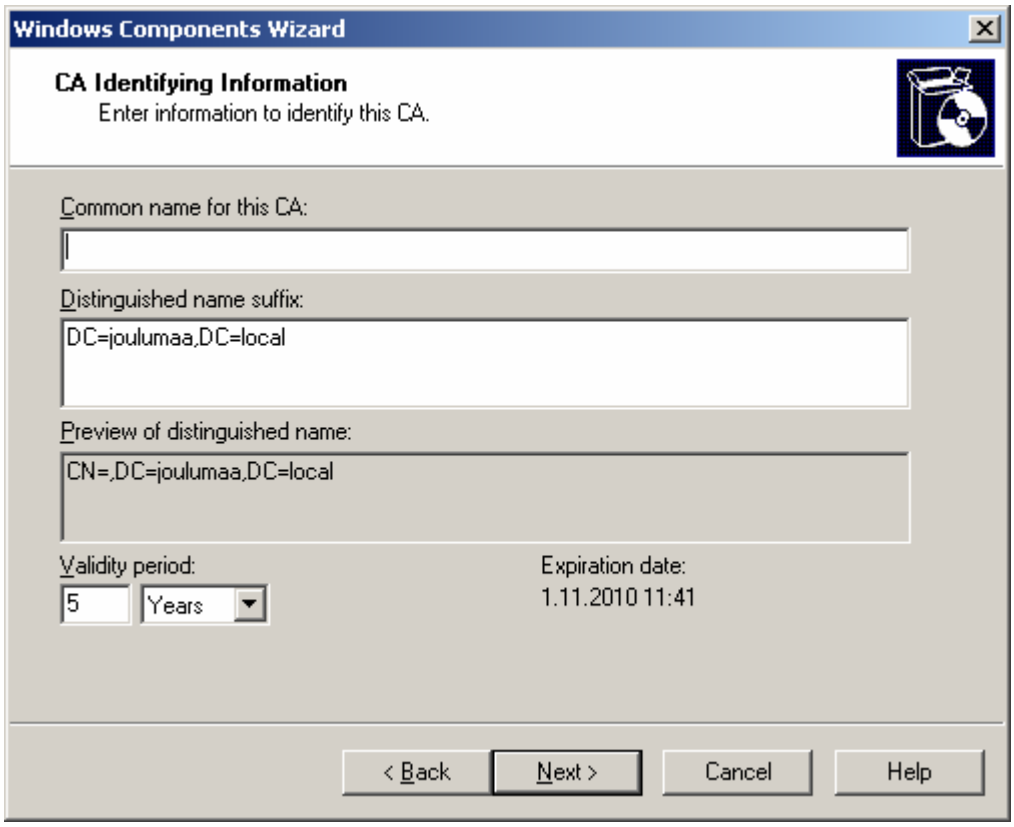
KUVIO 5. CA-palvelimen asennus

Valitaan OK ja saadaan kuvion 6 mukainen valikko, jossa kysytään CA-palvelimen tyyppiä. Valitaan Enterprise root CA, eli Enterprise (WIN 2003 Enterprise) juuri sertifikaatti –tyyppinen palvelin.



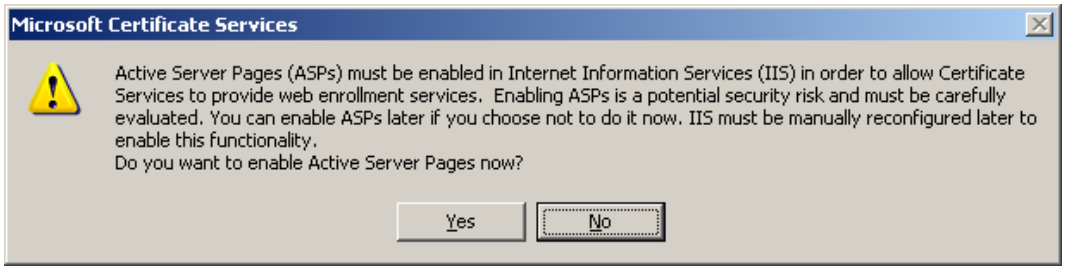
KUVIO 6. CA-tyyppi

Seuraavaksi lisätään common name, tässä tapauksessa JOULUMAA. Joulumaa tulee siis olemaan palvelimen ”virallinen” nimi, joka näkyy kaikissa hakemistoissa sekä rakennepuissa. Palvelimessa jossa siis on jo valmiiksi asennettu AD, täytyy tähän kohtaan kirjoittaa jo käytössä oleva palvelimen nimi. Validity periodiksi, eli CA-palvelimen sertifikaattien voimassaolon kestoisuuden pituudeksi voidaan valita haluttu aika. Tässä tapauksessa ajaksi jätettiin aika kuvion 7 mukainen 5 vuotta, koska sitä ei nähty tarpeelliseksi muuttaa.



KUVIO 7. CA Id info

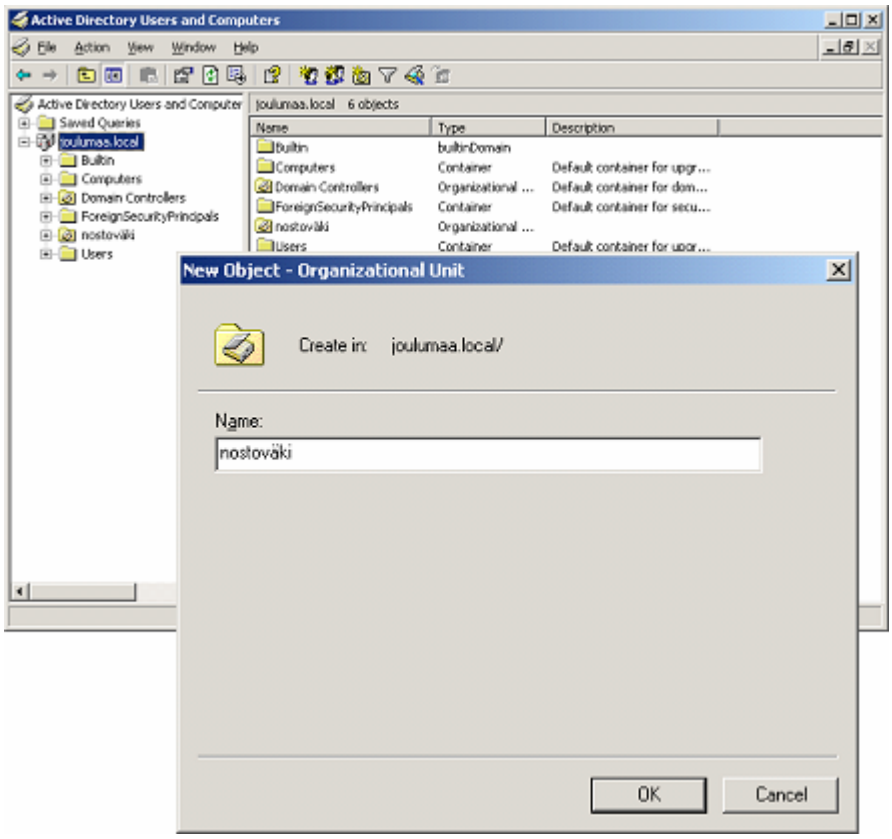
Kuviossa 8 näkyy seuraavanlainen varoitusikkuna, joka aukeaa Next-nappulan painamisen jälkeen.



KUVIO 8. IIS-varoitus

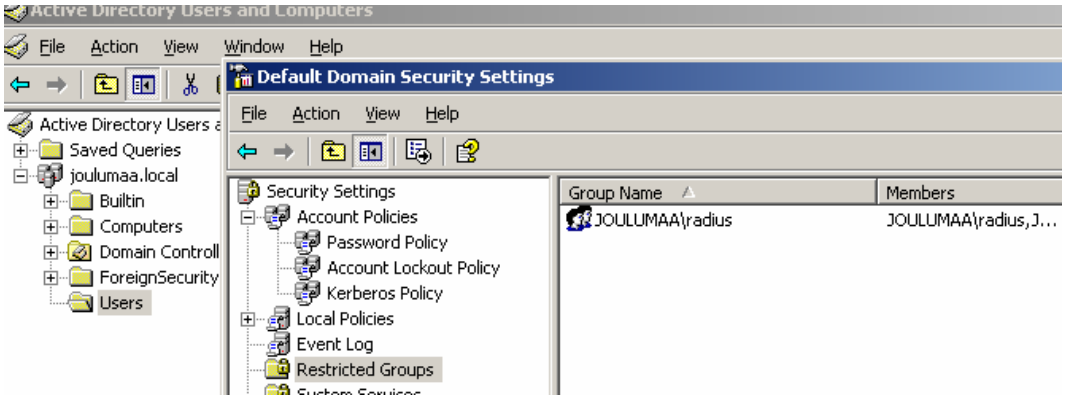
Siinä ilmoitetaan että, jo aiemmin valitsemamme ASP täytyy olla valittuna IIS:issä, jos autentikaatioita halutaan tehdä web-pohjaisina. Seuraavaksi tehdään

kuvion 9 mukainen uusi käyttäjäryhmä, nimeltään Nostoväki. Tämä ryhmä oli ensimmäinen luomamme ryhmä.



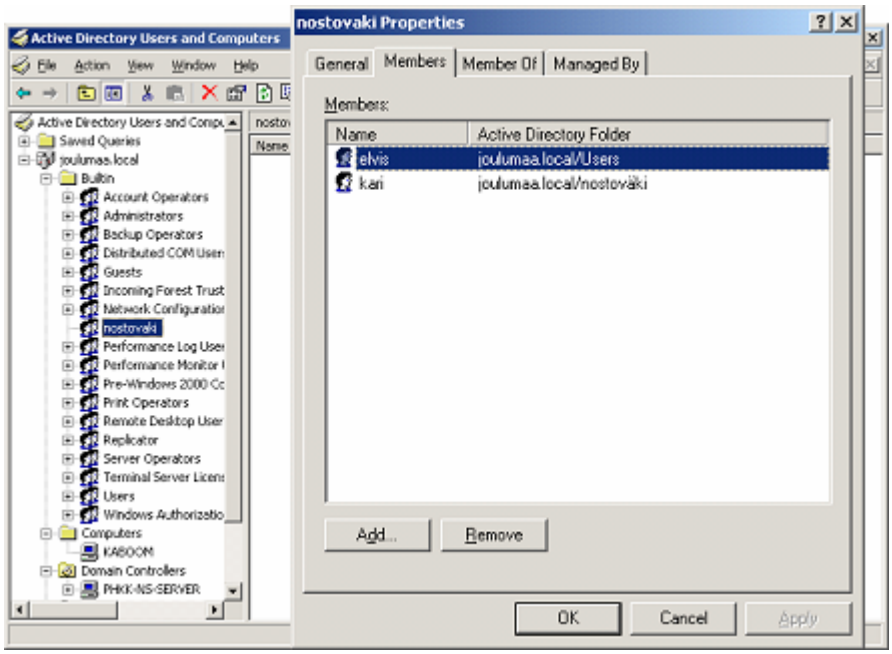
KUVIO 9. Nostoväki

Seuraavaksi lisäämme, tai paremminkin liitämme luomamme AD:n, eli joulumaan, restricted-ryhmään. Mikä tahansa muu ryhmä käy yhtä hyvin, ja myös uuden ryhmän luonti on jo tässä vaiheessa mahdollista. Näin ei vielä tässä vaiheessa kuitenkaan tehty, vaan toimimme kuvion 10 mukaisesti.



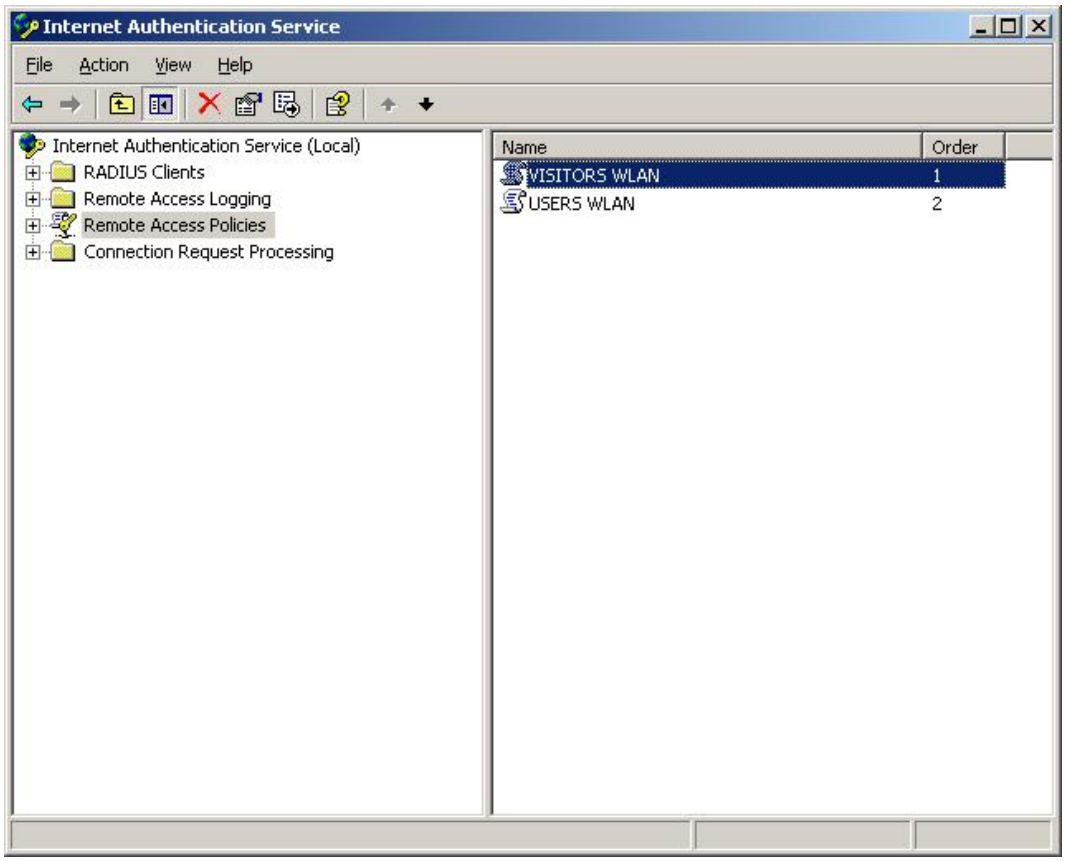
KUVIO 10. Restricted ryhmään lisääminen

Nyt AD Users and Computers otsakkeen alle luodaan tehdyn nostoväki-ryhmän alle käyttäjät. Lisätään käyttäjät kari sekä elvis. Kuvion 11 mukaisessa ikkunassa näemme tehdyt käyttäjät. Nämä käyttäjät olivat varsinaiset testihenkilöt tässä työssä.



KUVIO 11. Käyttäjien lisääminen.

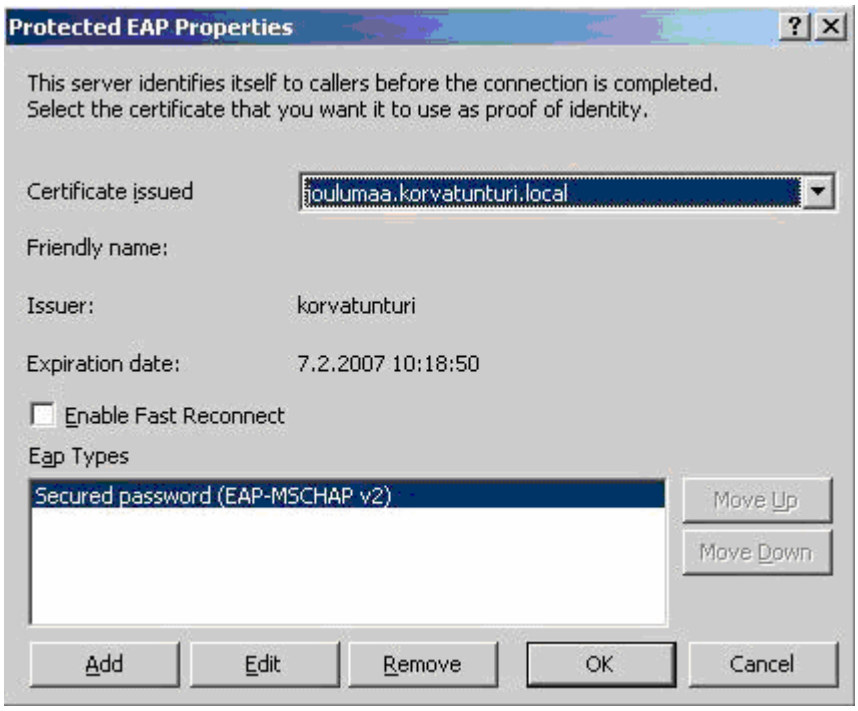
Kun avataan IAS-service, sen oikealla puolella tulee näkyviin kuvion 12 mukaiset tilit. Nämä oli siis asennettu jo tässä vaiheessa



KUVIO 12. Remote Access Policies

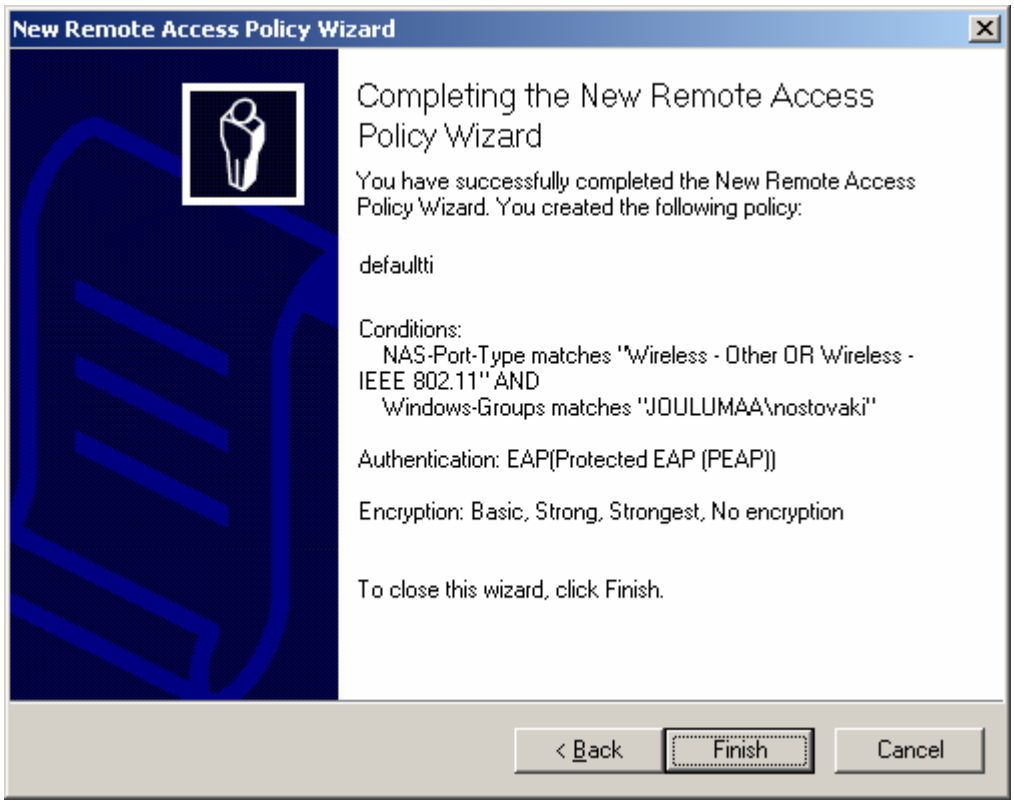
Jokaiselle ryhmälle kannattaa luoda omanlaisensa profiili. Tällöin saadaan jokaiselle ryhmälle asetettua juuri tarvittavat ryhmäkohtaiset asetukset. Tässäkin tapauksessa vierailija- ja henkilökuntatileille asetettiin erilaiset kirjautumis- ja turva-asetukset. Kaikki valmiina olevat tilit voidaan poistaa. Oletuksena oleva ”Connections to Microsoft…” -tili on meille tarpeeton. Lisätään tilit nimeltä Visitors WLAN sekä Users WLAN. Se tapahtuu seuraavasti New -> RAS-policy -> next ja alle annetaan uusi tilin nimi -> valitaan wireless Next -> klikataan Group ja sen jälkeen Add. Tästä valitaan Advanced ja Find now. Täältä valitaan tarkoitukseen sopiva profiili ja tilejä tehdään niin monta kuin on tarpeellista. Tässä työssä tilejä jäi lopullisesti yllämainitut Visitors WLAN, joka on tarkoitettu vierailijoille sekä Users WLAN joka taas on henkilökunnalle. Klikataan next, kunnes kysytään

EAP-tyyppiä, valitaan PEAP ja Configuresta kuvion 13 asetukset. OK:lla tili on valmis



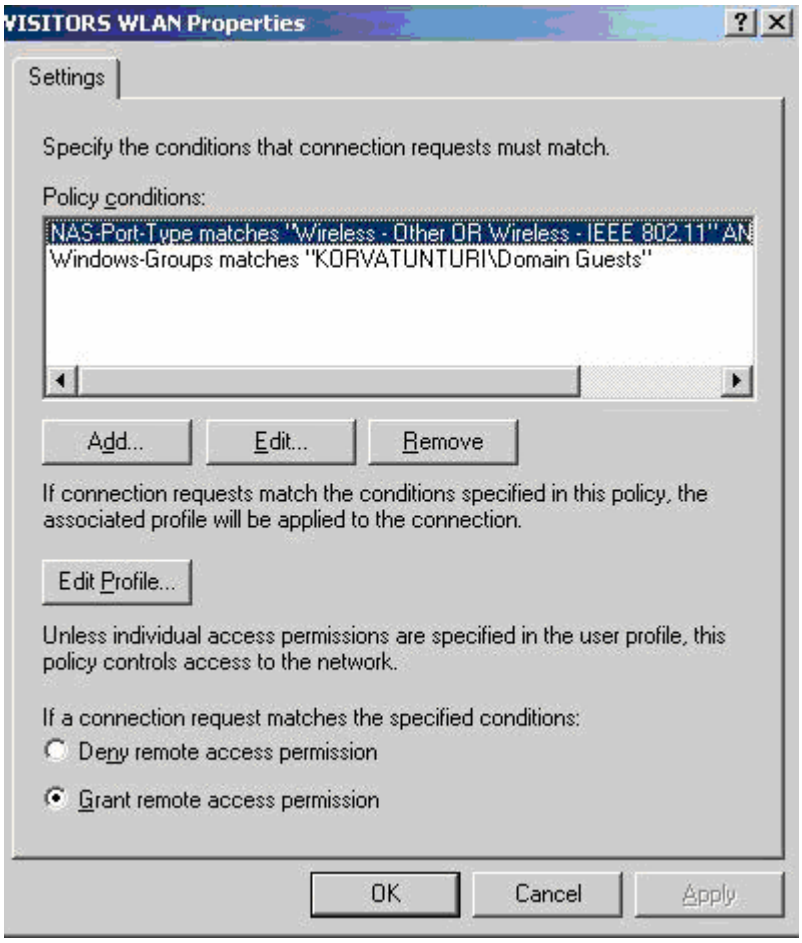
KUVIO 13. PEAP-asetukset

Lopuksi saadaan kuviossa 14 oleva näkymä. Ikkunassa kerrotaan kaikki tarpeellinen informaatio, jota juuri on tehty. Tässä vaiheessa voidaan vielä palata taaksepäin ja tehdä tarpeelliset muutokset, myöhemmin muutokset voi tehdä muuttamalla käytännön (policy) ominaisuuksia.



KUVIO 14. Yhteenvetoikkuna

Huomaa, että kuviossa 14 luodun tilin nimi on defaultti. Jokaiselle luodulle tilille aukeaa vastaava ikkuna. Defaultti-tiliä ei otettu käyttöön. Klikataan Visitors WLAN-tiliä IAS-ikkunassa, ja hiiren oikealla näppäimellä aukeaa kuviossa 15 näkyvä ikkuna.

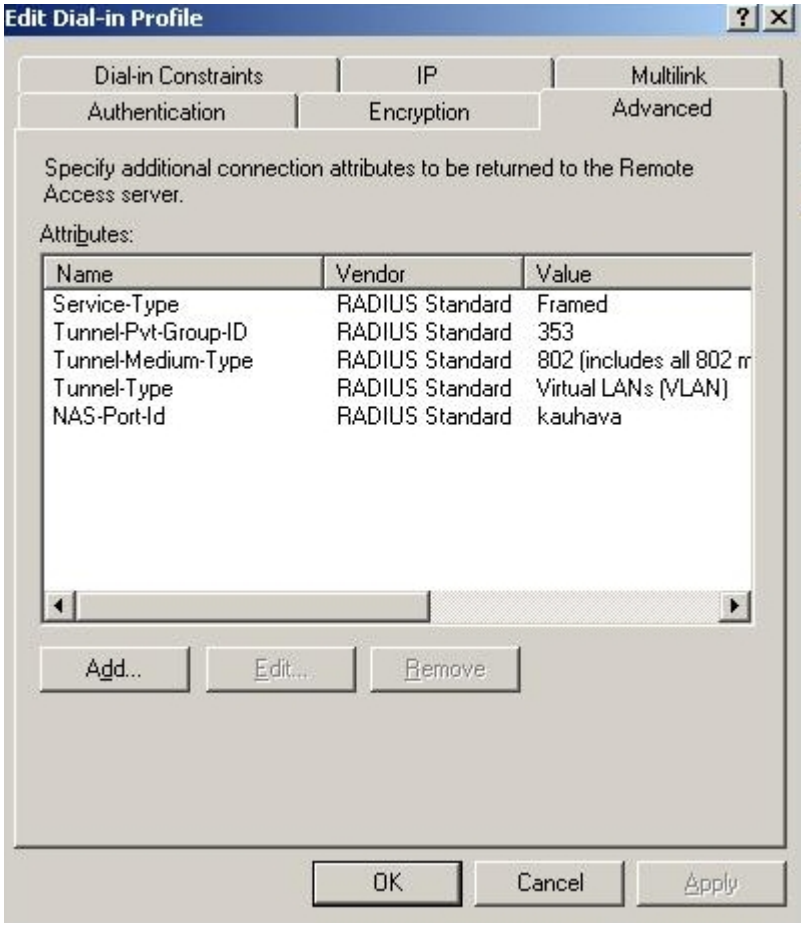


KUVIO 15. Visitors WLAN-ominaisuudet

Jos kuviossa olevia asetuksia ei ole valmiina, ne lisätään klikkaamalla Next -> ja siellä valmiina olevia policyja. Pitää muistaa myös sallia yhteys kuvion 15 mukaisesti Grant remote access permission-kohdan avulla. Editillä päästään lisäämään NAS-Port Typejä. Valittuna täytyy olla Wireless-IEEE 802.11 ja Wireless-other.

Edit profile-kohdan alta löytyy mm kohta Authentication, jonka alta valitaan kaikki vaihtoehdot (kuten PAP, Chap jne.). Tämä siksi, että näin saadaan varmistettua paras mahdollinen autentikaatio. Encryptionin-kohdan alta valitaan kaikki salausvahvuudet (40bit, 56bit jne). Vierailijan ainoa toiminto on päästä Internetiin omalta kannettavalta koneeltaan tai vastaavalta laitteelta. Henkilökunnan täytyy päästä Internetin lisäksi myös halutessaan omaan kansioonsa. Luonnollisesti vierailija ei saa päästä samaan verkkoon edes vahingossa, joten henkilökunnan SSID asetettiin salaiseksi. Toisin sanoen vain vierailijaverkkoa mainostetaan tukiasemalla.

Tukiaseman asetuksissa voidaankin valita yksi ensisijainen SSID, jota mainostetaan automaattisesti. Tästä johtuen edellä suoritettuja toimenpiteitä EAP:lle ei suoritetakaan vierailija (Visitors WLAN) verkolle. Sen sijaan kaikki salausvahvuudet valitaan. Advanced-kohtaan valitaan kuvion 16 mukaiset attribuutit.

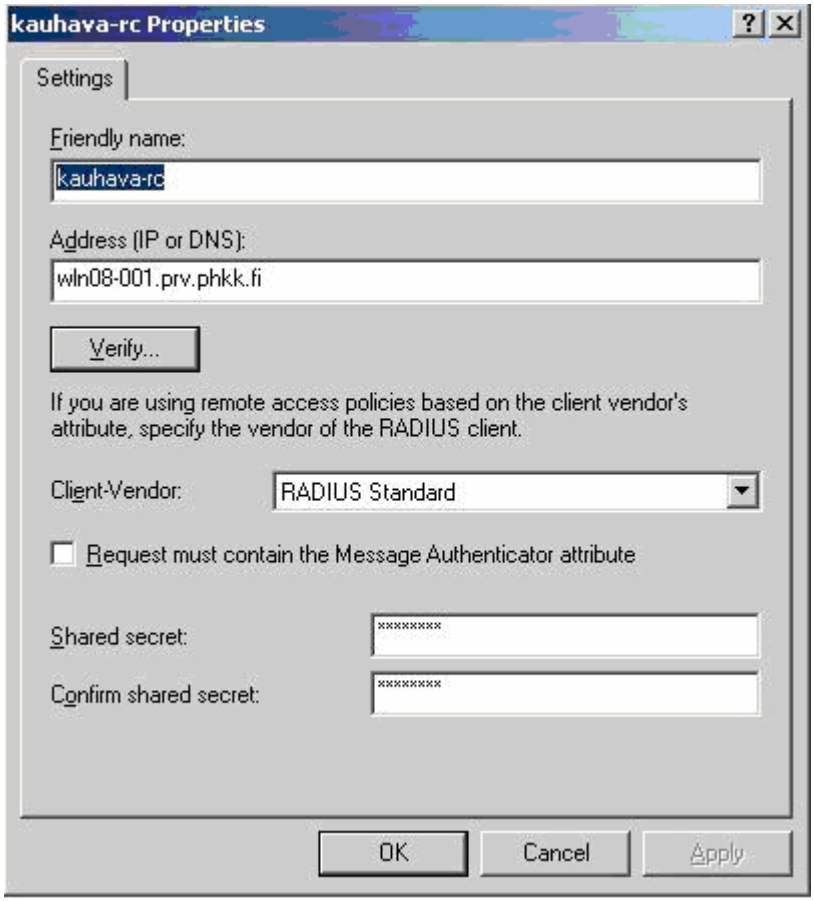


KUVIO 16. Tarvittavat attribuutit

Ne eivät ole todennäköisesti valmiina, mutta ne löytyvät Add-nappulan alta. Ohje näiden löytämiseksi löytyi Microsoftin sivuilta. Tunnel-Pvt-Group-ID 353 on vierailijaverkon SSID numero ja Nas-Port-Id kauhava on puolestaan tukiaseman nimi. Vierailijoiden verkkoliikenteen ei tarvitse olla salattua PHKK:n näkökannan mukaan. Vierailija voi itse tehdä tarvittaessa halutut salaustoimenpiteensä

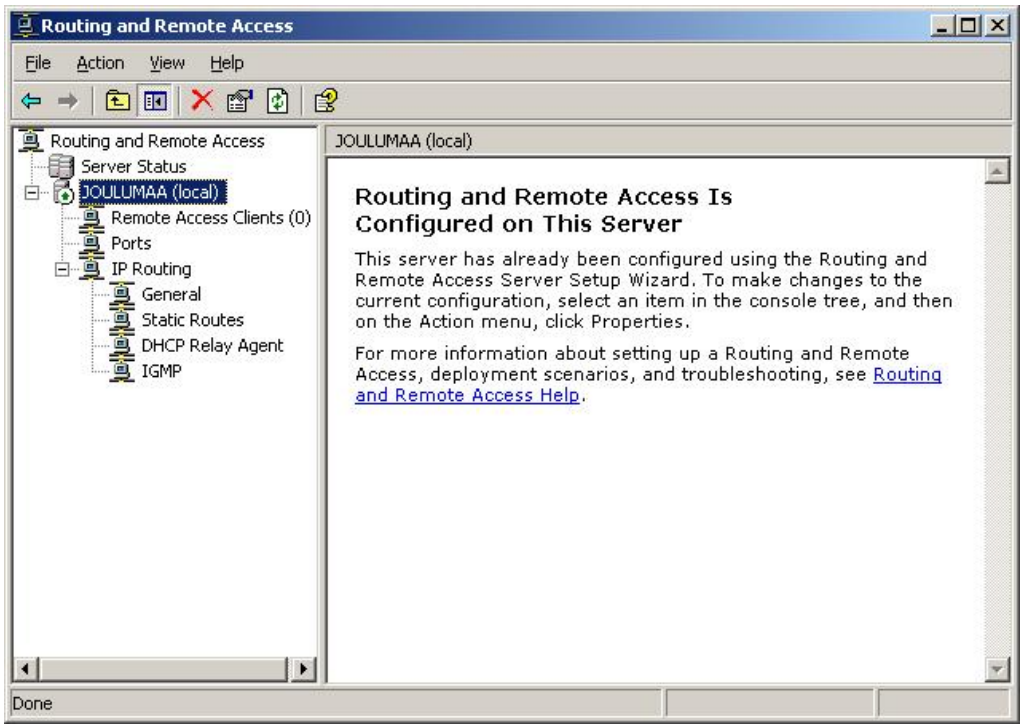
esimerkiksi siirtäessään dataa vaikkapa oman toimipisteensä ftp-palvelimelta. Sen sijaan users (työntekijöille) kaikki salaukset päälle

Kuvion 17 RADIUS-clients-kohdan alle lisätään tukiasema, jota halutaan käyttää. Tunnistusnimeksi on tässä tapauksessa laitettu kauhava-rc, tosin hieman sekoittavasti kauhava SSID:n kanssa. Sen voisi nimetä paremminkin. Shared Key täytyy olla sama, joka on laitettu myös tukiasemaan.



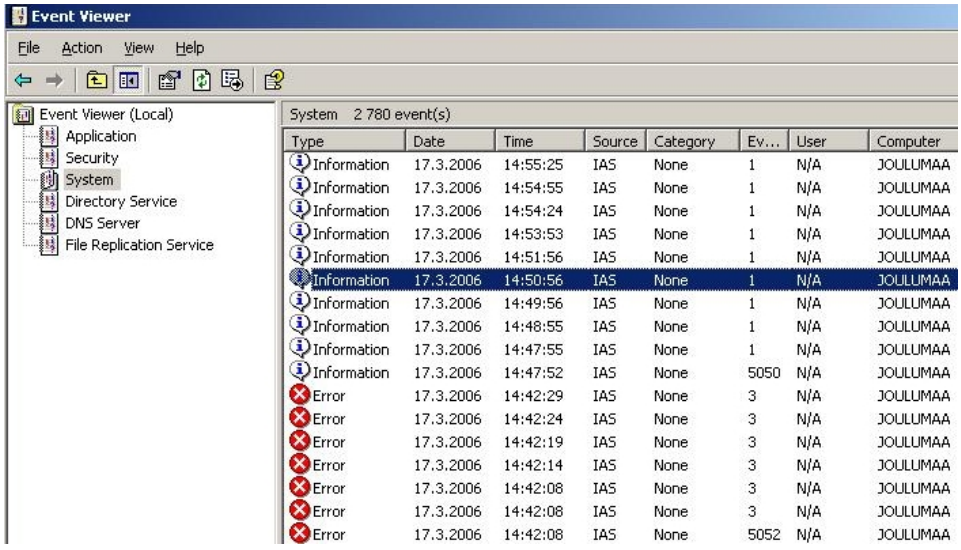
KUVIO 17. Kauhava-rc Properties

Routing and remote access-kohdan alta löytyy joulumaa-palvelin. Siinä täytyy näkyä kuviossakin 18 näkyvä vihreä täplä. Tällöin palvelu on päällä. Ominaisuuksista General-välilehden alta valitaan Remote Access Server ja Security-lehden alta RADIUS-Authentication ja RADIUS-Accounting.



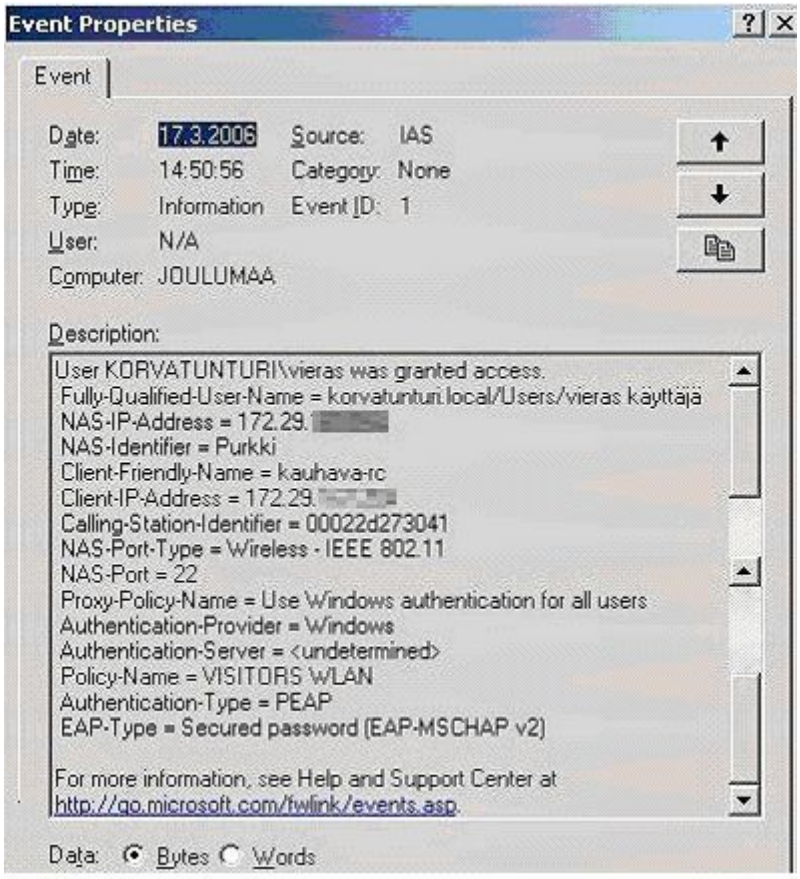
KUVIO 18. Jouluman RAS asetuksia voi muuttaa

Kuviossa 19 on näkymä palvelimen Event Vieweristä. Kun kirjautuminen on onnistunut, saadaan ilmoitus Event Vieweriin.



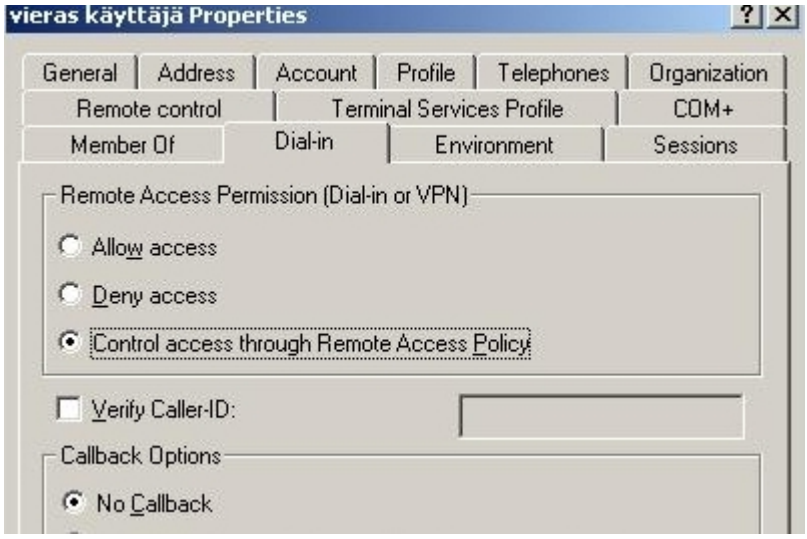
KUVIO 19. Windows 2003-palvelimen Event Viewer-kuvaa

Maalatua riviä klikattaessa saadaan näkyviin kaikki tarvittava tieto sisään kirjautuneesta koneesta. Tarkasteltaessa kuviota 20 nähdään, että aiemmin luotu käyttäjä ”vieras käyttäjä” on saanut IP-osoitteen tukiaseman 172.29. xxx.xxx kautta. Hän on tullut palvelimelle tukiasemalta nimeltä ”Purkki”, ja hän on ottanut yhteyden ”Kauhava-rc” SSID:n kautta.



KUVIO 20. Henkilö nimeltä ”vieras” on kirjautunut palvelimelle

Ikkunassa näkyy myös mm. policyn nimi sekä EAP-tyyppi. Jos yhteys ei meinaa onnistua, kannattaa tarkistaa kuvion 21 asetus, ”Control access through Remote Access Policy, eli RADIUS”. Asetuksissa on oletusarvoisesti asetettu arvo ”Deny access”, eli ”kiellä yhteys”. Toisin sanoen, tällä asetuksella yhteyttä ei voi muodostaa.



KUVIO 21. Muista sallia yhteys

Tämän jälkeen yhteys pitäisi onnistua. Yllä olevat asetukset tehdään molempiin tileihin. Erona on siis vain se, että vierailijaverkkoon asetetaan salausalgoritmien kanssa paljon heppoisemmat asetukset kuin henkilökunnan verkkoon.

5.4 WLAN-verkon käyttäjätunnukset ja laitevaatimukset

Vierailijoiden käyttäjätunnus salasana-parit voisi tietenkin ainakin teoriassa tehdä käsin. Se on kuitenkin aikaa vievää. Salasanojen generointiin käytetään Microsoftin kehittelemää ohjelmaa nimeltä WPS (Wireless Provisioning Services) authoring tool. WPS on käytössä jo melko laajalti ja sitä käytetään mitä erilaisimmissa paikoissa kuten hotelleissa, lentokentillä ja vaikkapa messuilla. Käyttäjä ottaa yhteyden verkkoon normaaliin tapaan. Tässä vaiheessa häneltä kysytään nimeä, organisaatiota tms. ja varsinkin pankkikortin tietoja. Tämä siksi, että verkon käyttö ei yleensä ole ilmaista. Käyttäjätunnus-salasana-pari on kertakäyttöinen ja vain käytetystä ajasta veloitetaan. WPS:ssä on valikoima mitä tietoja kirjautuessa kysytään, eli se voi olla hyvinkin muunneltavissa. PHKK:ssa tämä toiminto kuitenkaan ei kysele pankkikorttia, vaan verkko tulee olemaan vierailijoille ilmainen. Henkilökunnan käyttäjätunnukset ovat puolestaan valmiiksi jo luotuna PHKK:n AD-tietokantaan.

Laitevaatimukset varsinkin vierailijoiden osalta ovat PHKK:n vaatimuksesta seuraavat: 1. Laitteen ollessa kannettava tietokone, täytyy koneessa olla Windows XP-käyttöjärjestelmä, jossa on asennettuna vähintään SP2. 2. Verkkokortin täytyy tukea 802.11b tai 802.11g-protokollaa. Kumpi vain käy, sillä tukiasema tukee molempia.

5.5 Tukiaseman käyttöönotto

5.5.1 HP Procurve W420 -tukiasema

KUVIO 22. Tässä työssä käytetty tukiasema HP Procurve W420 (W=Wireless). (Hewlett-Packard Development Company 2005 a)

Lopputyössä käytetty langaton Access Point oli Hewlett-Packardin valmistama Procurve W420. Kuviossa 22. nähdään kyseinen laite. Työn tilaaja oli valinnut kyseisen tukiaseman jo ennalta, eli mitään valintoja tai vertailuja kyseisistä laitteista ei käytännössä tehty. Laitetta on kuitenkin hieman vertailtu taulukossa 1 keskeisimpien ominaisuuksien pohjalta. Huomaa varsinkin ylivoimaisesti parhaat salausvaihtoehdot HP:n laitteessa. 3Comin laitteessa mainittu monimuoto tarkoittaa a, b ja g-standardien tukea, joita se voidaan päivittää tukemaan samaan aikaa.

TAULUKKO 1. Muutaman tukiaseman keskinäinen vertailu (vertaa.fi 2006; Cisco 2006)

Tuotteen nimi	Tukee	Kantama	Salaus	Hinta
LINKSYS 54 MBPS WIRELESS ACCESS POINT	802.11b, g	300m	256-bittinen WPA-salaus ja MAC-osoitteiden filtteröinti.	71€
LINKSYS 802.11A+G WIRELESS ACCESS POINT	802.11a, b, g	300m	152-bittinen WEP-salaus ja MAC-osoitteiden suodatus.	117€
WIRELESS SOHO ACCESS POINT WITH 4 10/100	802.11b	540m	64- tai 128 bittinen WEP-salaus, DHCP-serveri, MAC-osoitteiden suodatus	133€
HP PROCURVE WIRELESS ACCESS POINT 420	802,11b, g	305m	EAP, MD-5, TLS, TTLS, PEAP, RADIUS-based MAC suodatus, WPA2 tai WPA	375€
CISCO AIRONET 1230AG ACCESS POINT	802.11a, g	Max 500m	WEP, WPA, TKIP, AES, LEAP, TLS, TTLS, PEAP, 64-, 128 bit kryptaus	648€ Hinta saksassa

(jatkuu)

TAULUKKO 1 (jatkuu)

3COM WIRELESS LAN ACCESS POINT 8500	Päivitettävissä 802.11b-802.11a monimuotoon.	100m	64-, 128- sekä 154-bit WEP kryptaus	733€

Ilmoitettu kantama vaihteli sadasta metristä (3Com) yli viiteensataan metriin (Soho). Hinta ei näytä olevan suoraan verrannollinen tukiaseman salausvaihtoehtoihin. 3Comin tukiaseman salausvaihtoehdot ovatkin aikalailla samanlaisia kuten Linksysin vastaavat. Silti hinnalla on eroa reilut 600€. Samoin näillä näyttää käyvän kantaman kanssa, 3Comin 100m vastaan Linksysin 300m. Käytännössä nämä kaksi laitetta näyttävät olevan periaatteiltaan aivan samoja, joten en keksi syytä, miksi juuri näistä pitäisi valita 3Com. Tosin tähän vertailuun oli otettu vain muutama vertailukohta, ja juuri ratkaiseva tekijä johonkin toiseen verkkoon saattaa olla nyt piilossa. Hintaa vertailtaessa tulee pakosti mieleen, että näissäkin laitteissa joudutaan maksamaan jo pelkästään tuotteen nimestä. HP:n tukiaseman toiminta ei eroa käytännössä muista samanlaisista tukiasemista. Sen käyttöönotossa tarvitsee käydä läpi käyttöohje, sillä tukiaseman toiminnot ovat todella monipuoliset. Laite on tarkoitettu ainoastaan sisäkäyttöön, koska sillä ei ole roiskeluokitusta (IP-luokka) ja sen käyttölämpötila on 0 – (+)40 °C. Seuraavaksi on listattu muutamia ominaisuuksia joita tukiasemasta löytyy. Tukiasema ominaisuuksiin kuuluu:

- jopa kahdeksan eri SSID:tä (Service Set ID)
- omat erilliset turva-asetukset jokaiselle SSID:lle
- 64/128/152-bit WEP-salaus
- Wi-Fi Protected Access (WPA and WPA2)
- IEEE 802.1X
- etäautentikaatio RADIUS-serverin avulla
- MAC-osoitteiden (Media Access Control) suodattaminen
- naapuritukiasemien etsintä (Rogue Access Points)
- automaattinen vapaan kanavan etsintä
- sekä konsoli- että WEB-pohjainen konfigurointimahdollisuus

- SNMP-tuki (Simple Network Management Protocol) versioille 1-3
- jopa 64 VLANia
- seinäkiinnitysmahdollisuus
- lähetystehon säätö
- roaming-tuki (Hewlett-Packard Development Company 2005 b).

Useampi SSID oli meille tarpeen, sillä jo alun perin oli vaatimuksena, että ainakin kolme (vierailija, henkilökunta ja hallinta) SSID:tä olisi oltava käytössä. Myöhemmin käyttöön saattaa tulla vielä muitakin SSID:itä. Tärkeää oli myös mahdollisuudet asettaa jokaiselle SSID:lle omat turva-asetukset, niiden erilaisen käytön takia. IEEE 802.1X ja RADIUS-protokollan tuki oli myös vaatimuksena verkkoa tehtäessä. Roaming-tuki tulee olemaan käyttökelpoinen, kun verkko laajenee vaikkapa tekniikan laitoksen kokonaan kattavaksi. Tällöin saadaan käyttöön myös useampi VLAN. Kaikkia mahdollisia 64:ää VLAN:ia tuskin silti otetaan käyttöön.

Langattoman verkkokortin omaava henkilö saattaa yllättäen säästää kuukausimaksuissa käyttämällä, luvattomasti tosin, jonkun toisen verkkoa. Mainittakoon, että se ei ole sallittua myöskään lain puitteissa. Käytännössä tämä tapahtuu seuraavasti: kytketään verkkokortti koneeseen ja ohjelmallisesti haetaan vapaita verkkoja. Ohjelma joko kytkeytyy automaattisesti ensimmäiseen vapaaseen verkkoon tai kysyy käyttäjältä mitä tehdään. Yleensä kaikki alueella olevat verkot tulevat näkyviin SSID-listassa. Listauksessa jopa kerrotaan, onko verkko salattu vai salaamaton. Klikattaessa haluttua verkkoa verkkokortti ottaa yhteyden haluttuun verkkoon ja avaa (jos kyseessä ei ole salattu yhteys) yhteyden Internetiin. Verkon ollessa salattu joutuu verkkoon yrittävä henkilö yleensä kirjautumaan ennalta annetuilla tunnuksilla päästäkseen sisään. Tämä onkin suositeltavaa. Verkkoon saattaa päästä kirjautumaan myös pelkän MAC-osoitteen avulla. Tarkemmin sanottuna MAC-osoite saattaa olla joskus ainoa varmenne pääsylle verkkoon, mutta MAC-osoitekin voidaan väärentää. Siksi olisikin suotavaa, että MAC-tunnistusta käytettäisiin vain jonkin toisen autentikoinnin kanssa. Käyttäjä saattaa kirjautua myös joltain toiselta koneelta, joten myös se luo oman ongelmansa ko. kirjautumiseen.

5.5.2 SSID

SSID, eli Service Set ID (Identity) on se tunnus, jolla langaton verkko tunnistetaan toisista verkoista. SSID voi olla nimeltään vaikkapa KAUHAVA, kuten tässä työssä on käytetty. SSID voidaan ilmoittaa julkisesti, jolloin tukiasema mainostaa haluttua verkkoa. Tällöin verkko tulee näkyviin kaikille, jotka hakevat vapaita verkkoja lähialueelta. Se voidaan myös pitää salaisena, jolloin kyseiseen verkkoon haluavan täytyy ensin tietää, minkä nimistä verkkoa hän hakee. Kunnolla salattu verkon nimi voi olla muotoa AuIj%d5S(Sf8hfw8flU/6, jolloin sen arvaaminen alkaa olla lottovoiton luokkaa, jollei jopa vaikeampi. Verkko saattaa olla myös täysin avoin kuten Lahdessa toimiva Mastonet, joka on avoin kaikille käyttäjille. Vaikka se on ensisijaisesti tarkoitettu vain kaupungin omille asukkaille, on se avoinna mm. Salpausselän kisojen aikana kaikille halukkaille. Verkko on tarkoitettu lähinnä kevyeen surffailuun, kuten sähköpostin lukuun tai linja-autojen aikataulujen hakemiseen. Samanlaisia verkkoja löytynee varmasti jo muistakin kaupungeista. Yleistä näissä on, että verkko toimii periaatteella ”toimii kun toimii”. Mitään siis ei taata varmaksi ja verkko on salaamaton. Niitä käyttävän kannattaa olla varovainen mitä ja miten dataa niissä siirtää juuri tämän vuoksi.

5.5.3 Tukiaseman asetukset

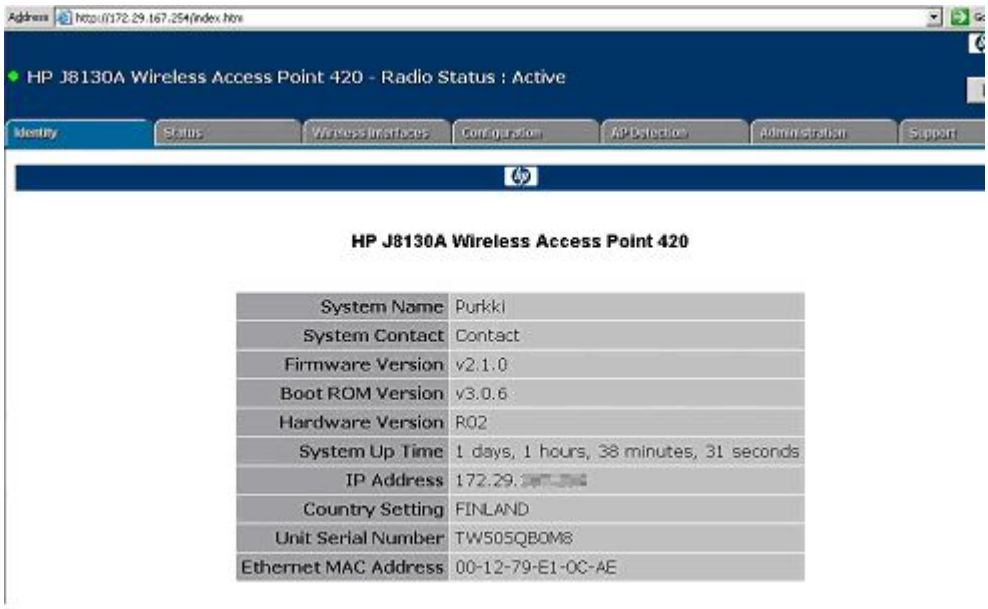
Varsinaisesti tukiasema oli ensiksi saatava käyttökuntoon. Tukiaseman asennusta varten tehtiin tarkempi ns. pikaohje. Tämä on varsinaisesti tarkoitettu tukihenkilölle, joka joutuu laitteen asentamaan. Ohje löytyy liitteestä 2.

Tukiasemalle sekä RADIUS-palvelimelle annettiin kiinteät IP-osoitteet (Internet Protocol). Jos osoitteet vaihtuisivat kesken kaiken, ei yhteys enää toimisi. Tämä tietenkin siksi, että asetetusta osoitteesta ei enää löydykään oletettua laitetta/palvelua. Ensiksi tukiasemalle asetettiin kiinteä IP-osoite. Laite asetettiin käyttämään tekemäämme AD:tä, eli JOULUMAAta. Joulumaalle oli annettu kiinteä IP-osoite, sillä se ei saa muuttua kesken kaiken. Puutumatta oikeastaan sen enempää aseman asetuksiin voidaan mainita, että kaikki vastaavuudet täytyy löytyä myös RADIUS-palvelimelta. Näitä ovat mm. Shared Secret-avain, EAP-turvataso ja SSID-asetukset. Vaikka tukiasema on mahdollista konfiguroida

komentokehotteella käyttäen Telnet-yhteyttä, on asiaan perehtymättömän huomattavasti helpompi tehdä muutoksia asetuksiin Web-selaimen avulla.

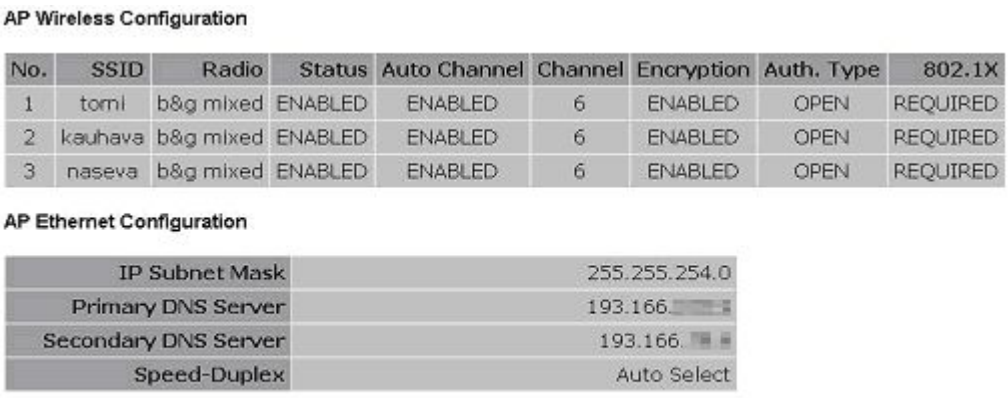
5.5.4 Tukiaseman asennus

Tukiasema-asennus tai paremminkin tukiaseman asetukset tehtiin palvelimen asennuksen jälkeen. Tarvittavat ohjeet löytyivät HP:n sivuilta, jotka olivat pdf-tiedostoina. Näistä ohjeista saikin paljon tarpeellista informaatiota sekä itse tukiasemasta että sen asetuksista. Jotta tukiasemaan päästiin kiinni, oli se ensin saatava konfiguroitua toivomallamme tavalla. Tukiaseman ylösajosta löytyy enemmän liitteessä 2. Alla esitetyt toimenpiteet tehtiin selaimen kautta, graafisella liittymällä. Käydään läpi tukiaseman asetukset, joita teimme. Kuviossa 23 näkyy aloitussivu.



KUVIO 23. Aloitussivu, jossa näkyy yleisimmät tiedot

Kuvassa 23 on valittuna Identity-välilehti. Status-välilehden alla on kolme välilehteä: AP status, Station Status ja Event log. AP Statuksen alta saadaan näkyviin sivu, jossa näkyy etusivuun verrattuna tietoja hieman tarkempia tietoja. Sieltä näkyy myös kuviossa 24 näkyvä AP Wireless Configuration.



AP Wireless Configuration

No.	SSID	Radio	Status	Auto Channel	Channel	Encryption	Auth. Type	802.1X
1	torni	b&g mixed	ENABLED	ENABLED	6	ENABLED	OPEN	REQUIRED
2	kauhava	b&g mixed	ENABLED	ENABLED	6	ENABLED	OPEN	REQUIRED
3	naseva	b&g mixed	ENABLED	ENABLED	6	ENABLED	OPEN	REQUIRED

AP Ethernet Configuration

IP Subnet Mask	255.255.254.0
Primary DNS Server	193.166.
Secondary DNS Server	193.166.
Speed-Duplex	Auto Select

KUVIO 24. AP Wireless Configuration

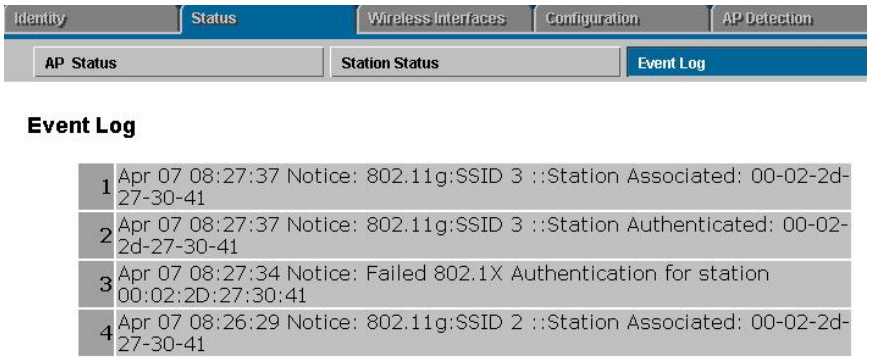
AP Ethernet Configuration kertoo tukiaseman Ethernet-asetukset. Station Status puolestaan kertoo kaikki kannettavat, jotka ovat kiinni tukiasemassa, ja Event Log on nimensä mukaisesti tapahtumalogi, josta näkyy kaikki koneiden yhteydenotto-yritykset.

Station Status

Station Address	Authenticated	Associated	Forwarding Allowed	Key Type	VLAN ID
kauhava					
00:02:2D:27:30:41	TRUE	TRUE	TRUE	DYNAMIC WEP	353

KUVIO 25. Station Status

Yllä olevasta kuviosta 25, voidaan todeta, että MAC-osoitteella 00:02:2D:27:30:41 oleva kone on autentikoitunut, se on kiinni tukiasemassa ja RADIUS on antanut luvan käyttää verkkoa. Alla oleva kuvio 26 puolestaan kertoo Event Login tapahtumia.

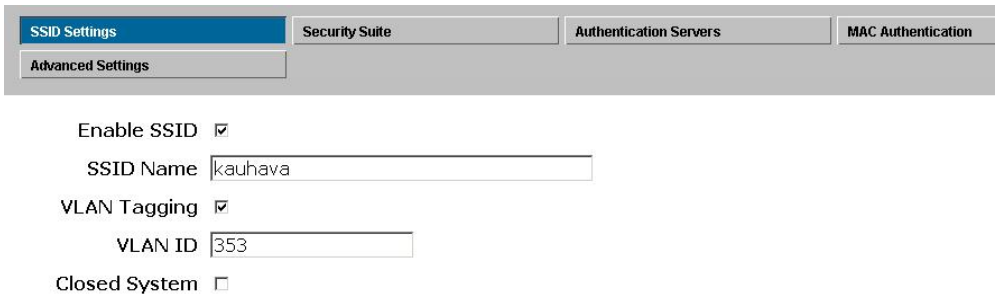


KUVIO 26. Tapahtumalogi

Rivillä yksi voi todeta päivämäärän ja kellonajan. Seuraavaksi Noticen jälkeen tulee informaatiota siitä, että tukiasemassa on kiinni kone, jonka MAC-osoite on ilmoitettu. Rivillä 3 todetaan, että samainen kone on epäonnistunut 802.1X-autentikoinnissa. Wireless interfaces-välilehti kuviossa 27 kertoo SSID optionsit.

KUVIO 27. SSID Options

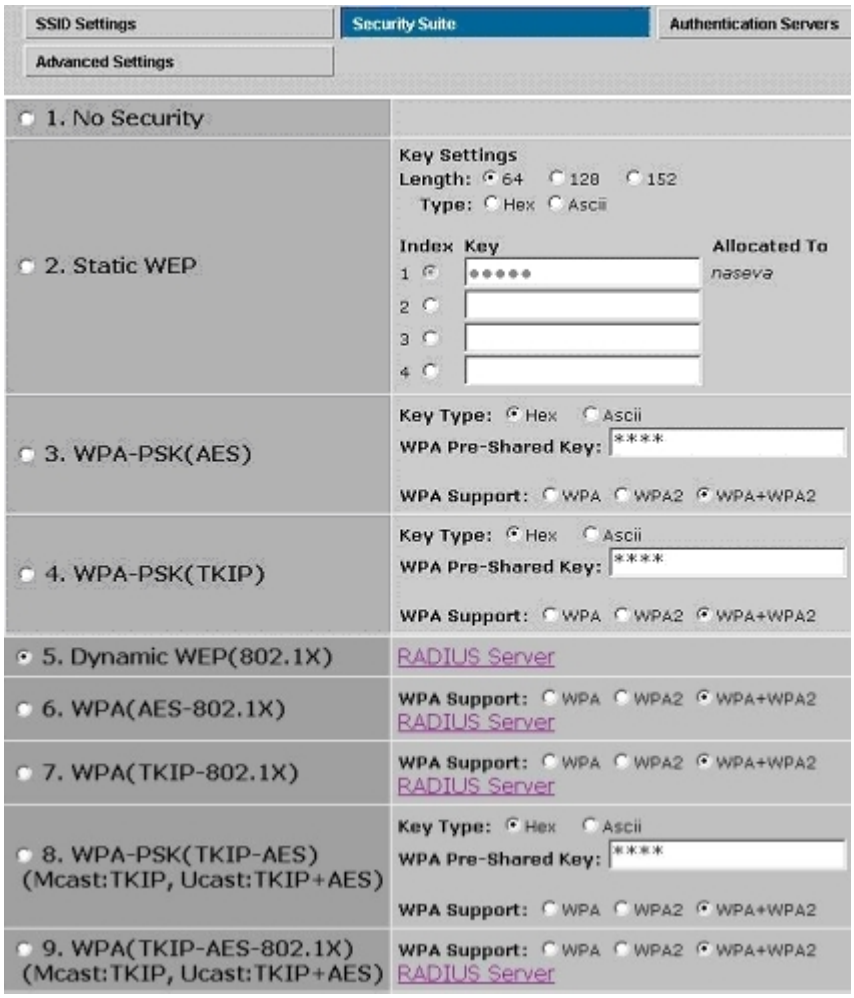
Siitä näkyy mm. SSID-nimet, tyypit sekä turva-asetukset. Kuviossa näkyvä Security Suite 5 on valitun tietoturvatason järjestysnumero (katso kuvio 29). Tagged merkitsee, että kaikki lankaverkkoon lähetettävät paketit varustetaan VLAN ID -tunnuksella. Klikattaessa halutun SSID:n modify-painiketta, päästään seuraavaan ikkunaa, joka näkyy kuviossa 28.



KUVIO 28. Modify-painikkeen alta paljastuu tällainen näkymä

Closed System tarkoittaa, että clientit, joilla ei ole valmiiksi asetettu SSID:tä, eivät pääse käsiksi tähän WLANiin konfiguroimatta ensin käsin WLANin SSID-tunnusta. Huomaa, että tässä tapauksessa rasti on jätetty pois, eli vieraat voivat löytää verkon tällä tavalla helpommin.

Security Suite-välilehden alta löytyy näkymä, joka on kuviossa 29.



KUVIO 29. Turva-asetukset

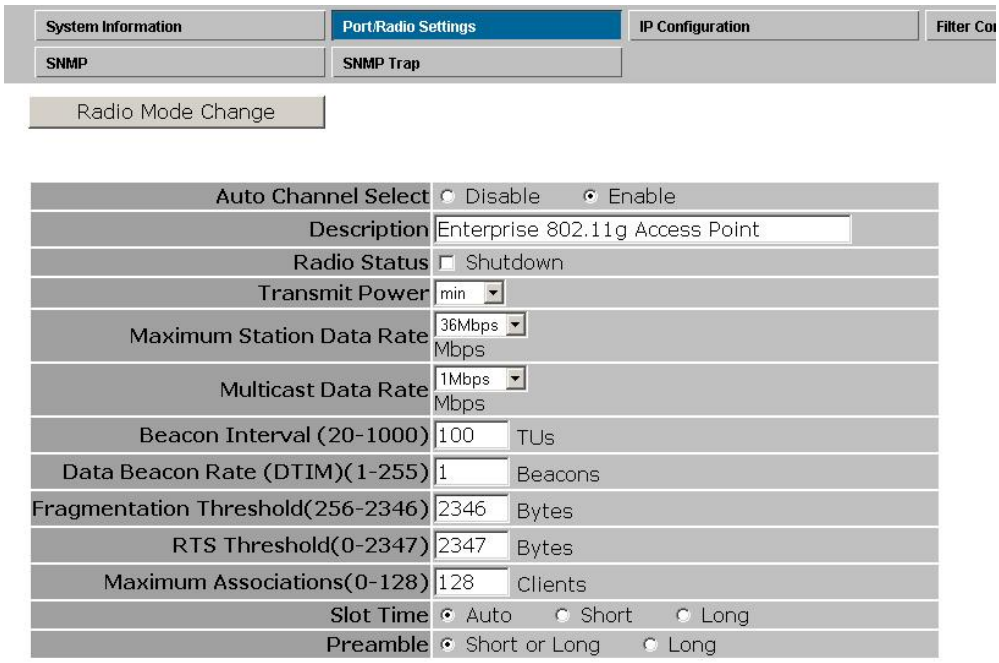
Tässä vaiheessa Security Suitessa valitaan haluttu suoja taso. Minimi on ykkösvaihtoehto No Security ja maksimivaihtoehto yhdeksän, oma asetettava, jossa saa päälle kaikki mahdolliset salaukset. Täältä valittiin kohta 5, sillä se sopi parhaiten tarkoituksiimme. Vaatimuksenahan oli saada käyttöön RADIUS-autentikointi ja käytössä piti olla 802.1X. Muut vaihtoehdot eivät täten oikein sopineet tähän tarkoitukseen.

Authentication Servers-kohdasta asetetaan RADIUS-asetukset, kuten käytettävän RADIUK-palvelimen IP, portti ja secret key. Varalle voi asettaa myös toisen RADIUS-palvelimen. Tässä työssä toista Back-up palvelinta ei ole, joten asetetaan Secondary Serverin IP:ksi 0.0.0.0. Tämä tarkoittaa, että se ole käytössä.

Mac-authentication kohdasta voidaan asettaa päälle MAC-autentikaatio. Jos se on asetettu päälle, joudutaan listalle lisäämään kaikki MAC-osoitteet, jotka pääsevät kiinni verkkoon tai vastaavasti sieltä voidaan kieltää jonkun MAC-osoitteen pääsy. Tässä työssä tämä oli pois käytöstä alun kokeilun jälkeen.

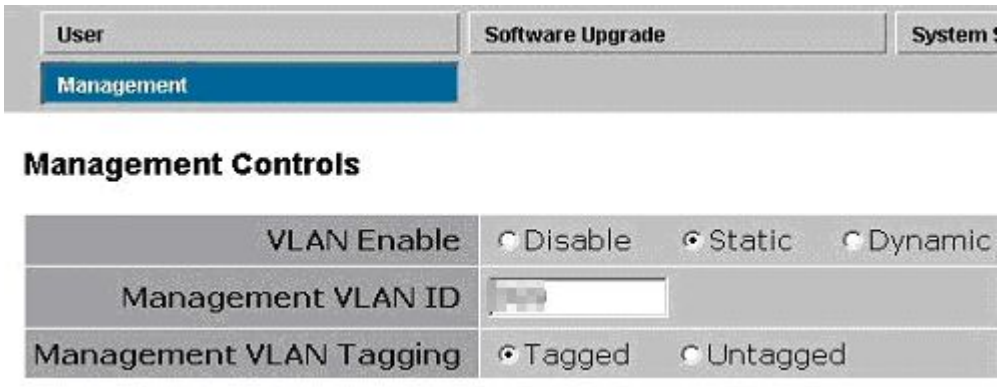
Advance settings -kohdan kautta voidaan asettaa Broadcast Key Refresh Rate, session key ja 802.1x refresh. Broadcast Key Refresh Rate tarkoittaa sitä, miten usein Broadcast key uusitaan, Session key on käytettävä salausavain ja 802.1X refresh tekee tarvittaessa päivitykset asetuksiin. Configuration-lehden alta löytyvät System Information (tukiaseman asetukset), Port/Radio settings (portti ja Radio asetukset), IP Configuration Filter Control (IP-asetukset), SNMP ja SNMP Trap (SNMP-asetukset ja trapit).

System Name-kohtaan voidaan asettaa systeemin nimi, tässä tapauksessa siis PURKKI. Port/Radio Settings-kohdassa valitaan Ethernet Settings. Vaihtoehdoista valitaan AUTO. Niitä on 100BaseTXfull ja Half Duplex, 10BaseTfull ja Half Duplex. Näitä voi terkastella hieman tarkemmin kuviosta 30.



KUVIO 30. Port/Radio asetukset

IP Configuration kohdassa asetetaan kiinteä IP. Filtteröinnissä tyydyttiin default asetuksiin, samoin kuin SNMP-trapeissa. Oletusasetuksissa kaikki trapit olivat pois päältä, ja tämä sopi parhaiten tähän työhön. SNMP-kohdassa oli tehty asetukset jo aiemmin, eli asetettu SNMP-palvelimen IP-osoite. AP Detection-välilehden alta voidaan asettaa tukiasema hakemaan toisia tukiasemia. Tämä on hyödyllinen toiminto, jolla voi hakea lähettyvillä olevia tukiasemia. Jos jostain syystä alueelta löytyy toinen tukiasema, joka käyttää samoja SSID:itä, voi tästä päätellä, että kyseinen tukiasema on laitettu pystyyn vain huijaustarkoituksessa. Koska tälle ei ollut meillä käyttöä, se jätettiin Disable-tilaan. Administration-kohdan alta löytyvät kohdat User, Software Upgrade, System Servers, Acconting Servers ja Management. Userin alta voi tehdä uuden käyttäjän ja Software Upgrade on puolestaan softan-päivitys valikko. System Servers-kohdassa voidaan antaa SNMP-palvelimen IP-osoite ja enabloida se. Samassa kohdassa voidaan tehdä myös aikavyöhykesäätöjä. Accounting Servers-kohdassa voidaan määritellä RADIUS accounting-palvelimen asetukset. IP:t ja portit voidaan asettaa sekä Primarylle että Secondarylle serverille. Management-kohdassa asetetaan tukiasemanhallinta säädöt, kuten onko reset nappula käytössä tai voiko Serial-porttia käyttää. Valittavana on myös voiko Telnet-yhteyden ottaa tukiasemaan, sekä voidaan asettaa käytettävät http- ja https-portit sekä ssh-portti.



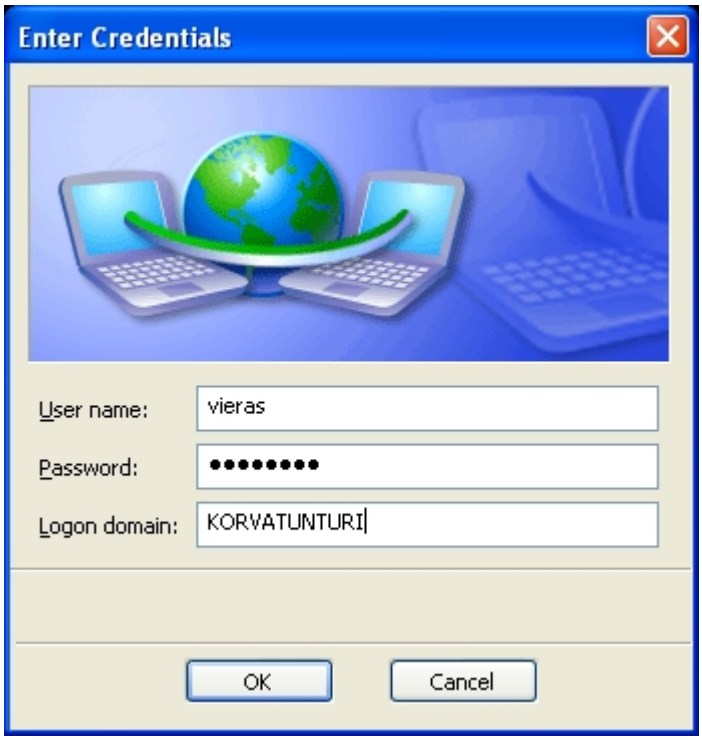
KUVIO 31. Osa Management-sivusta

Kuviossa 31 näkyy osa Management-sivusta. Management VLAN ID -kohtaan annettiin hallinta-vlanin tunnus, joka on sama koko PHKK:n alueella. Vlanille on annettu staattinen osoite ja liikenne on tagattua.

Näillä asetuksilla tulisi tukiaseman toimia. Ongelmatapauksissa kannattaa yleensä tutkiskella manuaaleja, jotka, kuten jo sanottu, olivat hyviä ja informatiivisia.

5.6 Kirjautuminen vierailijaverkkoon

Miten sitten vierailija pääsee käytännössä kiinni verkkoon? Riippuen siitä millaista ohjelmaa vierailija käyttää, hän ottaa normaalisti yhteyden tehtyyn vierailija SSID:hen. Jos verkkokortti saa yhteyden mainostettuun verkkoon, hän klikkaa ”yhdistä verkkoon” tms. nappulaa. Muussa tapauksessa hän hakee verkon manuaalisesti. Kummassakin tapauksessa aukeaa hänelle kuviossa 32 näkyvä ikkuna.



KUVIO 32. Kannettavassa näkyvä autentikaatioikkuna

Vierailija syöttää hänelle annetun käyttäjätunnus-salasana -parin ja yhteys on valmis. Mainittakoon vielä, että vierailijalle on annettu oikeudet ainoastaan päästä Internetiin, eikä hän näe henkilökunnan verkkoa ja/tai kansioita.

5.7 Toteutetun verkon testaus

Testaus suoritettiin PHKK:n tietohallinnan tiloissa. Käytössä oli yksi kannettava tietokone, jolla otettiin yhteyttä tukiasemaan. Välillä kävimme pyytämässä apua naapurihuoneessa työskenteleviltä, josko yhteys onnistuisi heidän koneilla selvittääksemme, olivatko kaikki asetukset kohdallaan ja ettemme päässeet verkkoon vain sen vuoksi, että RADIUS tunnisti väärin koneemme, jota käytimme. Käytimme aina kirjautumisyrityksissä luomiamme tilejä, Elvis ja Kari, joille olimme siis määritelleet tilit RADIUS-palvelimelle. Kirjautumista seurasimme sekä tukiasemalta että palvelimelta. Varsinkin palvelimen Evet Viewer oli tässä työssä lyömätön väline. Siitä pystyi seuraamaan, oliko kirjautumispyyntö tullut perille ja jos oli, niin miksi kirjautuminen onnistui tai ei onnistunut. Aluksi testeissä ei ollut päällä juuri mitään salauksia. Varsinkin ensimmäisissä yhteyskokeiluissa kaikki tieto oli salaamatonta, ja pidimme jopa WLAN-verkkoa avoimena. Toisin sanoen kaikilla halukkailla oli pääsy tukiaseman kautta Internetiin. Tukiaseman logista näimmekin, että sitä myös yritettiin käyttää. Tarpeettoman liikenteen lopettamiseksi asetimmekin tukiasemaan päälle MAC-osoitesuodatuksen. Tukiaseman logista näkyi, että tämä auttoi, vaikka moni (meille) vieras kone vielä olikin pitkään kiinni tukiasemassa.

Kun kannettavalla otettiin yhteyttä tukiasemaan, täytyi valita mihin SSID:hen haluttiin yhteys. Tässä vaiheessa oli myös verkkoliitännän asetuksiin tehtävä muutoksia. Kun haluttiin käyttää henkilökunnan verkkoa, asetettiin päälle lisäkohta, jossa kannettava tietokone voitaisiin autentikoida koneena. Oletettiin, että henkilökunnan koneita ei tulisi niin paljon yhden tukiaseman alle, ettei niitä voitaisi lisätä käsin tietokantaan. Tosin sanoen; vaikka kirjautuminen täytyisi vielä kuitenkin tehdä, tunnistettiin kone, josta henkilö yrittää kirjautua. Luonnollisesti vierailijoille tämä kohta täytyi siis poistaa asetuksista, muuten kirjautuminen ei onnistuisi.

Kun kirjautuminen alkoi pikkuhiljaa onnistua, tuli eteen pulma. Logista pystyi lukemaan, että kone oli yrittänyt ottaa yhteyttä tukiaseman kautta palvelimelle, mutta 802.1X-autentikointi oli epäonnistunut. Tämän selvittelyyn menikin aikaa paljon. Lopulta tämä selvisi kuitenkin verkkokortin asetuksista. Jostain syystä oli PEAP-asetus vaihtunut aina Smart Cardin käytöksi. Miksi näin oli käynyt, ei saatu

selville. Käytössä oli tehokkaaksi havaittu ”kokeilemalla”-metodi, joka selvitti monia ongelmia tai asetuksia.

5.8 Saadut tulokset ja tulevaisuus

Tulokset olivat positiivisia. Verkkojen tekeminen onnistui toivotulla tavalla. Aikaiseksi saatiin siis kaksi erillistä verkkoa, joihin kumpaankin päästiin kirjautumaan RADIUS-protokollalla. Vierailijat eivät pääse käsiksi henkilökunnan verkkoon edes vahingossa, mikä oli yksi tärkeimmistä kriteereistä. Molemmat verkot saivat IP-osoitteet omista IP-avaruuksista, jotka PHKK oli asettanut. Todettakoon myös se, että HP 420W-tukiasema oli melko käyttökelpoinen tukiasema tähän tarkoitukseen, ja paikalle suunniteltua toista tukiasemaa tuskin tullaan tarvitsemaan. Vaikka tukiaseman lähetysteho oli säädetty minimiin, oli verkon kuuluvuus hyvä koko toimiston alueella. Tällöin tosin roaming-palvelu jäi tyystin testaamatta. Tukiaseman säädettävyys ja varsinkin sen graafinen hallintaohjelma olivat todella hyviä ja käyttöohjetta seuraten oli koko tukiaseman käyttö helppoa. Kun WPS-autentikointi saadaan todella toimimaan, tulee langattoman verkon käytöstä sekä vaivatonta, että turvallista.

Tulevaisuus tulee olemaan langaton. WLAN-verkot lisääntyvät ja sitä mukaa siihen liittyvät palvelut. Kämmenmikrot korvaavat ehkä kokonaan niin kannettavat tietokoneet kuten puhelimetkin. Siirrettävien tiedostojen koko kasvaa koko ajan, ja ne on saatava reaaliajassa. 802.11b ja 802.11g käyttävät taajuutta joka tulee olemaan aina vaan tukkoisempi, ja häiriöt tulevat kasvamaan. Tarvitaan siis lisää kaistaa.

Verkkojen väärinkäyttöä ei saada koskaan tyystin loppumaan, siksi on tärkeää saada verkon valvonta täysin automaattiseksi. Jokaiselle verkolle on saatava edes minimaalinen salaus, ja varsinkin autentikointi on järjestettävä niin, ettei nykyisen kaltaista villiä länttä ole salaamattomien verkkojen osalta. Turva-asetukset on saatava automaattisesti kaikkiin langattomiin verkkoihin. Verkon seurantaa täytyy tehostaa, ja varsinkin tunkeutumisyrityksistä täytyy tulla joku ilmoitus verkon valvojalle/omistajalle. Vaikka tunkeutuja käyttäisikin verkkoa harmittomaan surffailuun, voi siitäkin koitua harmia. Pahimmassa tapauksessa tunkeutuja saattaa

käyttää verkosta saatavaa IP-osoitetta laittomiin toimiin. Tällaisissa tapauksissa on verkon haltijalla aina vaikeuksia todistaa syyttömyytensä.

Tulevaisuuden langattomana verkkona voidaan pitää WIMAX-verkkoa. Se toki on jo kokeiluluontoisesti käytössä eri puolilla suomea. Virallinen nimi WIMAXille on 802.16a ja se sisältää tuen luvallisille ja lupavapaille toiminnoille alle 11GHz:n taajuuksilla. Siinä on lisäksi tehokas kaistan käyttö sekä virheenkorjaus, jolloin saavutetaan luotettavampi lähetys. Eri koodaustapojen käyttö, joita voidaan muunnella olosuhteiden muuttuessa, sisältyy tähän standardiin. 802.16a sisältää tuen edistyneimmille antennitekniikoille, joilla voidaan parantaa kuuluvuusaluetta sekä kapasiteettiä. ja tekniikalle, joka mahdollistaa kaistan pienentämisen jotta päästäisiin pidempiin lähetysmatkoihin (jopa ~50 KM). 802.16a:ssa on myös tuki sellaisille ohjelmille joissa ei saa olla paljoa viivettä. Tällaisia ovat mm. Voip-palvelut, videokuvan lähetys sekä datalähetyksen priorisointi.

Lyhyesti voidaan todeta, että tulevaisuuden langattomat verkot tulevat olemaan nopeampia kantaman ollessa suurempi. Verkonvalvontaan tullaan myös kiinnittämään enemmän huomiota, sillä langattomien verkkojen väärinkäyttö on jo nyt lisääntynyt valtavasti.

6 YHTEENVETO

Tässä työssä tutustuttiin langattoman verkon erilaisiin kirjautumistapoihin ja tutkittiin siihen liittyviä protokollia. Teoriaosassa tutkittavana olivat myös TACACS+ ja FreeRadius. Lisäksi syvennyttiin IEEE-standardeihin.

Opinnäytetyössä oli testattavana Windows-työympäristössä toimiva RADIUS-autentikointi . Lisäksi tutustuttiin lyhyesti Linux-ynpäristössä toimivaan FreeRadius-palvelimeen sekä TACACS+-protokollaan. Windowsin RADIUS-protokolla selvisi voittajana näistä kolmesta vaihtoehdosta. Windows 2003 palvelimen käytössä oleva protokolla toimi testissä halutulla tavalla, ja kaikki asetetut tavoitteet saavutettiin, poislukien WPS:n käyttö. Vaatimuksena oli saada aikaan turvallinen kirjautumistapa, joka samalla olisi myös helppokäyttöinen. Lisää hankintoja ei enää haluttu tehdä, joten tehtävä oli suoritettava annetuille komponenteilla. Tämä sulki pois siis vaikkapa Smart Card-käyttösysteemin. WPS-käyttäjätunnusluontiohjelmaa ei saatu tämän työn puitteissa vielä toimimaan, mikä tullaan hoitamaan kuntoon kevään 2006 kuluessa.

Työssä tehtiin kolme erillistä SSID:tä, joissa jokaisella oli eri funktio. Vierailijaverkolla on omat ominaisuutensa ja samoin henkilökunnan verkolla. Kolmas verkko tehtiin pelkästään hallintaohjelmaa varten, ja se ei tule näkymään ulospäin, kuten myös oli toivottu.

Tukiasema saatiin konfiguroitua toimimaan niin, että se mainostaa haluttua verkkoa, joka voi olla vierailijoiden käytössä. Samaan aikaan henkilökunnan verkko täytyi olla näkymättömissä. Työssä onnistuttiin myös siinä suhteessa, että vierailijoilla ei ole pääsyä henkilökunnan verkkoon.

LÄHTEET

PAINETUT LÄHTEET

Kivimäki, J. 1999. Windows tietoturva. IT-Press. Gummerus Kirjapaino Oy, Jyväskylä.

Kivimäki, J. 2005. Windows server 2003. Readme.fi. Gummerus Kirjapaino Oy, Jyväskylä.

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

ELEKTRONISET LÄHTEET

Cisco Systems. Terminal Access Controller Access Control System (TACACS+) [verkkodokumentti]. 2005 [viitattu 11.1 2006]. Saatavissa: http://www.cisco.com/pcgi-bin/search/search.pl?siteToSearch=cisco.com%23TSD&country=US&language=en&as_q=tacacs%2B&as_epq=&as_oq=&as_eq=&as_occt=any&submit=Search

Cisco Systems. Cisco Aironet 1230 AG Access Point Introduction [verkkodokumentti]. 2006 [viitattu 15.4 2006]. Saatavissa: http://www.cisco.com/en/US/products/ps6132/index.html

DIAMETER. Comparison of DIAMETER Against AAA Network Access Requirements [verkkodokumentti]. 2005 [viitattu 1.4. 2006]. Saatavissa: http://www.diameter.org/

Hewlett-Packard Development Company [verkkodokumentti]. 2005 a [viitattu 10.12 2005]. Saatavissa: http://www.hp.com/rnd /products/wireless/420_series/large_420.htm

Hewlett-Packard Development Company. ProCurve Wireless Access Point 420 (J8131A) – tekniset tiedot ja takuu [verkkodokumentti]. 2005 b [viitattu 10.12.2005]. Saatavissa: http://h10010.www1.hp.com/wwpc/fi/fi/sm/WF06b/23663-345857-345857-345857-1789149-1789151-7963977.html

IEEE Standards Assosioation, IEEE Standards Interpretations [verkkodokumentti]. Tammikuu, 2006 [viitattu 10.2 2006]. Saatavissa: http://standards.ieee.org/reading/ieee/interp/

IEEE. IEEE P802.11g (TM), 54Mbps Extension to 802.11b Wireless Local Area Networks, Gains Working Group Approval Final Approval Expected in June 2003 [verkkodokumentti]. 2003 [viitattu 1.4 2006]. Saatavissa: http://standards.ieee.org/announcements/80211gapp2.html

IEEE. IEEE 802 LAN/MAN Standards Committee [verkkodokumentti]. 6.4 2006 [viitattu 20.4 2006]. Saatavissa: http://www.ieee802.org/

Intelligraphics Inc. Introduction to IEEE 802.11 [verkkodokumentti]. 2005 [viitattu 24.12 2005]. Saatavissa: http://www.intelligraphics.com/articles/80211_article.html

Interop iLabs. What is RADIUS [verkkodokumentti]. 2006 [viitattu 11.1 2006]. Saatavissa: http://www.ilabs.interop.net/LANSec/papers/02_What_is_RADIUS-LV04.pdf

Microsoft TechNet. RADIUS Protocol Security and Best Practices [verkkodokumentti]. 17.1 2002 [viitattu 28.11 2005]. Saatavissa: http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/security/RADIUSsec.mspx#EFAA

Netscape. What is a Certificate Authority (CA) certificate? [verkkodokumentti]. 22.6 2001 [viitattu 30.3 2006]. Saatavissa: http://help.netscape.com/kb/consumer/19990622-2.html

PHKK. Päijät-Hämeen koulutuskonsernin tietoverkko [verkkodokumentti]. 2006 [viitattu 9.4 2006]. Saatavissa: http://www.phkk.fi/esittely/

Vertaa.fi [verkkodokumentti]. 2006 [viitattu 04.04 2006]. Saatavissa: http://vertaa.fi/cgi-bin/s.cgi?cat=fi_hardware&theme=vertaa&searchwords=access%20point&subcat=muut

Wi-FiPlanet. Using RADIUS For WLAN Authentication, Part II [verkkodokumentti]. 2003 [viitattu 4.4 2006]. Saatavissa: http://www.wi-fiplanet.com/img/tutorial-radius-fig1.gif

IEEE 802.11 standardit aakkosjärjestyksessä. Huomaa julkaisuvuodet. Ne ovat suluissa jokaisen standardin lopussa. http://standards.ieee.org/reading/ieee/interp/

The following IEEE Standards and task groups exist within the IEEE 802.11 working group:

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003) Withdrawn 2005
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1Q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames
- IEEE 802.11x - reserved
- IEEE 802.11y - Contention Based Protocol

W420 CLI-PIKA-ASENNUS

Tällä pikaoppaalla pääsee alkuun ja se on tarkoitettu lähinnä niille henkilöille, jotka pitävät järjestelmää yllä. Lista on pelkistetty. Käytössä on myös nettipohjainen (GUI) hallintaohjelma, johon pääsee kiinni selaimella. Kaikki ”hienosäätö” on parasta tehdä sitä kautta.

Yhteys otetaan teratermillä käyttäen com1 :stä.
Username: admin//annetaan itse
Password: //jätetään tyhjäksi

HP ProCurve Access Point 420**#conf**//*päästään configuration tilaan*
Enter configuration commands, one per line.
HP ProCurve Access Point 420(config)#**management**
Enter management commands, one per line.

Annetaan haluttu salasana ja heti perään salasana, kuten tässä A1passi
HP ProCurve Access Point 420(config-mgmt)#**password-admin A1passi**
HP ProCurve Access Point 420(config-mgmt)**#exit**

Asetataan maakoodi. Jos maakoodia ei ole asetattu, ei radioasetuksia pääse muuttamaan.
HP ProCurve Access Point 420#**country FI**
Reboot system now to make the country code change effective? <y/n>: **y**
Reboot system...//*Eli buutataan*

Buutin jälkeen kirjaudutaan takaisin sisään. Käytössä on nyt siis asetettu salasana.
Username: **admin**
Password:**A1passi**
HP ProCurve Access Point 420#

HP ProCurve Access Point 420#**sh sys**

Alla näkyy asetustiedot.

System Information
Serial Number : TW505QB0M8
System Up time : 0 days, 0 hours, 1 minutes, 2 seconds
System Name : Enterprise AP
System Location ://*haulutessa voidaan asettaa*
System Contact : Contact
System Country Code : FI - FINLAND //*Huomioi siis maakoodi!*
MAC Address : 00-12-79-E1-0C-AE
IP Address : 192.168.xxx.xxx //*dhcp:ltä automaattisesti, jos radio on enabled*
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.xxx.xxx
VLAN State : DISABLED
Management VLAN ID(AP): 1 (U) //*U = Untagged, T=Tagged*
IAPP State : ENABLED
DHCP Client : ENABLED
HTTP Server : ENABLED
HTTP Server Port : 80
HTTPS Server : DISABLED
HTTPS Server Port : 443
Slot Status : 802.11g
Radio Status : Disabled //*asetetaan päälle alla*
Software Version : v2.1.0
SSH Server : DISABLED
SSH Server Port : 22
Telnet Server : ENABLED
Max Telnet Session : 4
Serial Port : ENABLED
Reset Button : ENABLED
SSID Number Supported : 8

Nostetaan tukiasema Up-tilaan

HP ProCurve Access Point 420#configure

Enter configuration commands, one per line.

HP ProCurve Access Point 420(config)**#interface wireless g**

Enter Wireless configuration commands, one per line.

HP ProCurve Access Point 420(if-wireless-g)#**no shutdown**

Active scanning 2.4GHz 54Mbps channels for 6 seconds...

Auto Channel Scan selected 2412 MHz, channel 1//*kanava voidaan halutessa määrätä*

HP ProCurve Access Point 420(if-wireless-g)**#exit**

HP ProCurve Access Point 420#**sh sys**

System Information

==========

Serial Number : TW505QB0M8

....

....

Slot Status : 802.11g

Radio Status : Enabled //*nyt käytössä*

Software Version : v2.1.0

....

Seuraavaksi muutetaan System Name. Annetaan uusi nimi Purkki.

HP ProCurve Access Point 420**#configure**

HP ProCurve Access Point 420(config)#**system name Purkki**

HP ProCurve Access Point 420(config)#**exit**

HP ProCurve Access Point 420**#show system**

Sh sys-komennolla nähdään muutos. Alla on poimittu vain tämä kohta koko listasta.

System Information

...

System Name : Purkki //*Uusi nimi*

Muutetaan SSID-nimi

HP ProCurve Access Point 420**#configure**

Enter configuration commands, one per line.

HP ProCurve Access Point 420(config)#**interface wireless g**

HP ProCurve Access Point 420(if-wireless-g)#**ssid index 1** //*järj. numero, jonka SSID halutaaan muuttaa*

HP ProCurve Access Point 420(if-wireless-g-ssid-1)#**ssid-name kauhava**

HP ProCurve Access Point 420(if-wireless-g-ssid-1)# //*nimi muutettu*

Asetetaan lähetysteho pienemmäksi. Tällä kertaa 10% teho riitti. Vaihtoehtoja näkyy alla.

HP ProCurve Access Point 420(if-wireless-g)#**transmit-power 10%**
full Set transmit power to full (100%)
90% Set transmit power to 90%
...
...
10% Set transmit power to 10%
min Set transmit power to min

Vaihdetaan komento kehote. Tämähän tosin yleensä tehdään aluksi, mutta sen voi toki jättää halutessa vaikka oletusmuotoon.

HP ProCurve Access Point 420(config)#**prompt**
HP ProCurve Access Point 420(config)#**prompt wln08-001**
wln08-001(config)**#**//*Vaihdettu*

Seuraavaksi määritetään vlan XXX, joka on varattu hallinnalle.

wln08-001(config)#**management-vlanid ?**
 <1-4094> Set Management VLAN ID for AP <1-4094>
wln08-001(config)**#management-vlanid XXX ?**//*?-merkki antaa vaihtoehdot*
 tagged Set Management VLAN tagged
 untagged Set Management VLAN untagged
wln08-001(config)#**management-vlanid 999 tagged**

Asetetaan vlan XXX (hallinta) ja muut aktiivisiksi

wln08-001(config)#**vlan enable ?** //*Vaihtoehdot dynamic ja static*
dynamic Enable dynamic Vlan //*Jos radius on konffattu SSID:T tulevat sieltä, jos ei ole konffattu ->ohjataan default SSID:hen*
static Enable static Vlan //*ohjataan default SSID:hen. Radiukselta tulevia ohjauksia ei sallita*
wln08-001(config)#**vlan enable dynamic**
Reboot system now? <y/n>: **y**

Asetataan SNTP

wln08-001(config)#**sntp-server ?**

date-time Set SNTP Date and Time //*ajan asetus*

daylight-saving Set SNTP daylight saving //*kesäaika*

enable Set SNTP enable //*pälle*

ip Set SNTP IP //*annetaan SNTP serverin osoite, josta aika päivitetään*

timezone Set SNTP time zone(-12, -11..., -1, 0, +1..., +11, +12) //*annetaan aikavyöhyke ->+2*

wln08-001(config)#**sntp-server** //*asetetaan kesäajan automaattinen vaihtuminen*.

wln08-001(config)**#sntp-server enable** //*asetetaan aktiiviseksi*

wln08-001(config)#**sntp-server daylight-saving** //*kesäajan asetus. Oikeat päivämäärät tosin voisi tarkistaa, nämä on ravistettu hihasta.*

Enter Daylight saving from which month<1-12>: 4

and which day<1-31>: 30

Enter Daylight saving end to which month<1-12>: 10

and which day<1-31>: 30

wln08-001(config)#

<134>Sep 16 08:27:13 192.168.xxx.xxx global: Information: Enable DayLight Saving

: 04/30 ~ 10/30

<134>Sep 16 09:27:12 xxx.xxx. xxx.xxx sntp: Information: Get time from SNTP Server Successfully

Tallennetaan konffis tftp-palvelimelle

wln08-001**#copy config tft**

wln08-001#**copy config tftp text**

TFTP Destnation file name:**2005-09-16-wln08-001** //*annetaan tiedoston nimi muodossa vuosi-kk-päivä-vehkeen nimi*

TFTP Server IP:192.168. xxx.xxx //*ja palvelimen ip-osoite*

TFTP transfer succeeded! //*jippii*

Asetetaan muut vlan ID:t. Ensiksi SSID 1, joka on henkilökunnan verkko, 347.

wln08-001# **interface wireless g**

wln08-001(if-wireless-g)#**ssid index ?**

<1-8> Select the SSID <1-8>

wln08-001(if-wireless-g)#**ssid index 1**
wln08-001(if-wireless-g-ssid-1)#**vlan-ID 347 tagged** //*vlan347 toimimaan reitittimen ethernet portista. Hallintaohjelmalla ei pääse käsiksi kuin (reitittimen) merkatusta portista*

Sitten SSID 2, vierailijaverkko 353 ja asetetaan samalla RADIUS-palvelimen IP.
wln08-001# **interface wireless g**
wln08-001(if-wireless-g)#**ssid index 2**
wln08-001(if-wireless-g-ssid-2)#**vlan-ID 353 tagged**
wln08-001(if-wireless-g-ssid-2**)#radius-authentication-server address 192.168.xxx.xxx** //*annetaan palvelimen osoite*
wln08-001(if-wireless-g-ssid-2)#**radius-authentication-server key fatima** //*autentikaatio avain fatima*
wln08-001(if-wireless-g-ssid-2)#**radius-authentication-server port 1812** //*mitä porttia käytytetään*
wln08-001(if-wireless-g-ssid-2)#**radius-authentication-server vlan-format ?** //*missä muodossa ID lähetetään*
HEX set the VLAN ID format to HEX
ASCII set the VLAN ID format to ASCII
wln08-001(if-wireless-g-ssid-2**)#radius-authentication-server vlan-format HEX**

Jos halutaan käyttää mm. MAC-suodatusta, on ositteiden lyönti koneeseen helpompaa selaimen kautta. Samoin kaikki turva-asetukset kannattaa tehdä sitä kautta, vaikka kaikki asetukset on mahdollista tehdä komentokohotteellakin.

Tiedostonimi: printtiversio
Hakemisto: Z:\LOPPUTYÖ
Malli: Normal.dot
Otsikko: Turvallinen kirjautuminen käyttäen Radiusta
Aihe:
Tekijä: Kari Seppälä
Avainsanat:
Kommentit:
Luontipäivä: 2.5.2006 11:42:00
Version numero: 8
Viimeksi tallennettu: 2.5.2006 12:02:00
Viimeksi tallentanut: seppaka1
Kokonaismuokkausaika: 23 minuuttia
Viimeksi tulostettu: 2.5.2006 12:11:00
Viimeisestä täydestä tulostuksesta
Sivuja: 71
Sanoja: 10 367 (noin)
Merkkejä: 83 973 (noin)