802.1X AUTENTIKOINTI KYTKINVERKOSSA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2007
Harri Heinonen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HEINONEN HARRI: 802.1x autentikonti kytkinverkossa

Tietoliikennetekniikan opinnäytetyö, 71 sivua, 15 liitesivua

Syksy 2007

TIIVISTELMÄ

Suurien käyttäjämäärien hallinta erilaisia käyttäjäryhmiä sisältävissä lähiverkoissa on muodostumassa yhä haasteellisemmaksi. Verkon käyttäjien tunnistamiseen käytetyt metodit vaativat ylläpitäjiltä suurta työpanosta ja jatkuvaa verkon valvontaa. Lähiverkkojen turvallisuutta voidaan kasvattaa järjestämällä erilaiset käyttäjäryhmät omiin aliverkkoihinsa. Keskitettyjen käyttäjätietokantojen käyttö yhdistettynä vahvaan autentikointiprotokollaan sekä dynaamisiin VLAN-verkkoihin vähentää ja yksinkertaistaa verkkojen ylläpitotehtäviä huomattavasti.

Tässä opinnäytetyössä keskitytään RADIUS-protokollien käyttöön dynaamisten VLAN-verkkojen muodostamisessa 802.1x autentikoinnin ja AAA-protokollaa tukevien lähiverkkokytkimien avulla.

Opinnäytetyö tehtiin Päijät-Hämeen koulutuskonsernille, jossa on siirrytty käyttämään Microsoftin Active Directory-hakemistopalvelua sekä henkilökunnan että opiskelijoiden palvelemiseksi. Konsernin lähiverkkoympäristöä on kehitetty viime vuosina ja tarkoituksena on, että se täyttäisi suurimmalta osaltaan myös RADIUS-palvelun vaatimukset.

Opinnäytetyön teoriaosassa perehdytään tietoturvan peruskäsitteisiin ja tiedon salauksessa käytettäviin metodeihin. Erityisen painotuksen saa sertifikaattien merkitys ja käyttö autentikoinnin yhteydessä. Autentikoinnin keskeisenä välineenä toimivat AAA- ja 802.1x-protokollat käydään läpi yleisiltä ominaisuuksiltaan.

Käytännön osuudessa testataan vahvaa autentikointia ja dynaamisten VLAN-verkkojen muodostamista kahdessa tätä tarkoitusta varten rakennetussa RADIUS-palvelinverkossa. Vertailtavat palvelimet ovat kaupallinen Microsoft IAS-palvelin ja GNU-lisenssiin perustuva ilmainen FreeRADIUS-palvelin.

Molempien RADIUS-palvelinten käyttö vahvaan autentikointiin ja dynaamisten VLAN-verkkojen muodostamiseksi onnistui. Tuloksista voidaan kuitenkin päätellä, että Microsoft IAS-palvelin on integroidulta ympäristöltään valmiimpi ja täyttää paremmin opinnäytetyölle asetetut vaatimukset.

Avainsanat: RADIUS, 802.1X, autentikointi, VLAN

Lahti University of Applied Sciences
Degree Programme in Information Technology

HARRI HEINONEN: 802.1x authentication in a switched LAN network

Bachelor's thesis in Telecommunications Technology, 71 pages, 15 appendices

Autumn 2007

ABSTRACT

Management of local area networks with different kinds of user groups is more challenging than ever. A method to authenticate users in a local area network requires its administrator's of workload and continuing surveillance. The security of local area networks can be assured by organizing its user groups into dedicated subnets. Centralized user databases combined with a strong authentication protocol and dynamic VLAN-networks can reduce and simplify the task of maintaining local area networks.

The objective of this thesis was to concentrate on use of RADIUS-protocols when constituting dynamic VLAN's with an 802.1x authentication and AAA-protocol supporting switches in a local area network.

This thesis was made for the Lahti Region Educational Consortium, which has started to use Microsoft Active Directory services both for it's personnel and students. The consortium's local area network has been developed in the recent years, in order to fulfill the requirements of RADIUS services.

The theory part of this thesis introduces the basics of network security and methods of data encryption. The use of certificates for authentication was given special attention. The overall properties of AAA- and 802.1x-protocols as the essential appliances of authentication are presented.

The empirical part describes how strong authentication and the forming of dynamic VLAN networks were tested in two RADIUS-server networks that were built for this purpose. The comparison was made between the commercial Microsotf IAS-server and the free GNU-license based FreeRADIUS-server.

Strong authentication and the forming of dynamic VLAN networks was successful with both RADIUS-servers. However, the results indicate that the integrated environment of Microsoft IAS server is more advanced and it better meets with the requirements for a final thesis better.

Keywords: RADIUS, 802.1X, Authentication, VLAN

SISÄLLYS

AAA	Authentication, Authorization and Accounting. Autentikointi, valtuutus ja tilastointi.
AD	Active Directory. Microsoftin toteutus LDAP-hakemistopalvelusta.
CA	Certficate Authority. Sertifikaatin myöntäjänä ja varmentajana toimiva taho.
CHAP	Challenge-Handshake Authentication Protocol. Haaste/Vastaus protokolla, käytetty yleisesti soittosarjoissa asiakkaan todentamiseksi.
CSMA/CD	Carrier Sense Multiple Access With Collision Detection. Tietoliikenteen siirtotien varausmenetelmä.
DHCP	Dynamic Host Configuration Protocol. Protokolla, jonka avulla jaetaan dynaamisesti IP-osoitteita lähiverkon laitteille.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa nimiä IP-osoitteiksi.
EAP	Extensible Authentication Protocol. PPP-protokollan yhteydessä kehitetty käyttäjien todentamisprotokolla.
EAPOL	EAP Over LAN. Paketointitekniikka jolla 801.1x-protokollan EAP-viestit kuljetetaan
ECP	Encryption Control Protocol. PPP-yhteyden salauksen valvontaa kontrolloiva protokolla.

IEEE	Institute of Electrical and Electronics Engineers. Tekniikan alan kansainvälinen järjestö joka julkaisee ja määrittelee standardeja.
IETF	Internet Engineering Task Force. Internet-protokollien standardisoinnista vastaava kansainvälinen järjestö.
LAN	Local Area Network. Lähiverkko.
LCP	Link Control Protocol. Integroitu PPP-protokollaan, huolehtii verkkoliitännöiden automaattisesta konfiguroinnista molemmissa päätepisteissä.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttöön tarkoitettu yhteysprotokolla.
LLC	Logical Link Control. OSI-mallin siirtoyhteyskerroksen ylempi protokolla. Huolehtii vuonohjauksesta ja multi/demultipleksauksesta.
MAC	Media Access Control. OSI-mallin siirtoyhteyskerroksen alempi protokolla. Tarjoaa fyysiset osoitteet ja pääsyn verkkomedialle.
MD5	Message Digest 5. Haaste/Vastaus-menetelmä, käyttää MD5-algoritmiä vasteiden laskemiseen.
MMC	Microsoft Management Console. Microsoft Windows työasemien ja palvelimien hallintatyökalusovellus.

MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol. Microsoftin versio CHAP-protokollasta, joka mahdollistaa kaksisuuntaisen todentamisen.
MS-MPPE	Microsoft Point-to-Point Encryption. Microsoftin kehittämä PPP-protokollan salausmenetelmä.
NAS	Network Access Service. Laite, joka välittää yhteydenotto pyynnöt RADIUS-palvelimelle.
NCP	Network Control Protocol. Paketoioi eri verkkoprotokollat PPP-kehykseen.
OSI	Open Systems Interconnection Basic Reference Model. Kuvaa tiedonsiirtoprotokollat seitsemällä tasolla.
PAP	Password Authentication Protocol. Autentikointiprotokolla, jota käytetään käyttäjien todentamiseen NAS:lle.
PKCS	Public Key Cryptography Standards. Salausmenetelmä, joka käyttää RSA-algoritmia.
PPP	Point-to-Point Protocol. Protokolla, jonka avulla voidaan muodostaa suora verkkoyhteys kahden laitteen välillä.
RADIUS	Remote Authentication Dial In User Service. Alkujaan soittosarjapalveluihin kirjautuvien käyttäjien autentikointiin kehitetty protokolla.
RAM	Random Access Memory. Tietokoneen työnaikainen muisti, joka tyhjenee virrankatkaisun yhteydessä.

RSA	Rivest, Shamir, Adleman algorithm. Kehittäjien sukunimien alkukirjainten mukaan ristitty salausalgoritmi.
SHA	Security Hash Algorithm. Tiiviste funktio, jota käytetetään digitaalisessa allekirjoituksessa.
TCP	Transmision Control Protocol. Yhteydellinen tietoliikenneprotokolla, joka on yksi IP-protokollaperheen ydinprotokollista.
UDP	User Datagram Protocol. Yhteydetön tietoliikenneprotokolla.
VLAN	Virtual LAN. Virtuaalinen lähiverkko

1 JOHDANTO

1.1 Työn tausta

Lähiverkkoon liitettyjen tietokoneiden tunnistaminen ja hallinta vaatii verkon ylläpitäjiltä nykyisin yhä enemmän valvontaa ja työtä, koska helposti verkkoon kytkettävät laitteet yleistyvät. Kannettavien tietokoneiden hintojen laskeminen tasolle, jossa niiden hankintaa ensisijaisena työvälineenä ei rajoita hinta vaan käyttäjän henkilökohtaiset tarpeet, on lisännyt tietoturvavaatimuksia. Riippumatta toimintaympäristöstä yleisenä käytäntönä on, että käyttäjät autentikoidaan lähiverkkoon jonkin verkkopalvelun kautta, ennen kuin tarjolla olevat resurssit saadaan käyttöön. Suurissa julkisissa laitoksissa, joissa vierailijoilta ei vaadita erillisiä kulkulupia, on mahdotonta kontrolloida jokaista kävijää, joka voi liittää koneita verkkoon.

Julkisissa laitoksissa, erityisesti kouluympäristöissä, lähiverkkoon luvattomasti liitettyjen tietokoneiden havaitseminen, paikallistaminen ja käytön estäminen vaikuttaa lähes mahdottomalta tehtävältä. Tietoverkon suojaaminen luvattomalta käytöltä vaatii erityisiä palvelurakenteita, jotta se täyttäisi tietoverkon turvallisuudelle asetetut perusvaatimukset, joiden avulla saavutettaisiin tarkoituksenmukainen lisäarvo. Nykyisten hallittavien lähiverkon kytkimien porttien perinteiset turvatoimet ovat rajalliset, ja niiden käyttöönotto saattaa aiheuttaa käyttäjille jopa tarpeetonta haittaa.

1.2 Työn tavoitteet

Tässä työssä tutkitaan lähiverkon tietoturvaa käyttämällä autentikointipalvelinta verkkoon liitettyjen tietokoneiden sekä niiden käyttäjien tunnistamiseen. Tavoitteena on rakentaa testiympäristö, joka toteuttaa autentikointiprotokollasta riippuen, käyttäjän tai työaseman autentikoinnin lähiverkkoon RADIUS-palvelimen avulla. Samassa yhteydessä on tarkoitus liittää käyttäjä tai työasema ennalta mää-

rättyyn VLAN:iin ryhmäjäsenyyden perusteella. Toteutuksessa keskitytään kahteen yleisemmin käytettyyn RADIUS-protokollaan, joiden avulla testiympäristön autentikointipalvelut ja VLAN:iin liittäminen testataan. Tarkoituksena on saada aikaiseksi mahdollisimman yksinkertaisesti ylläpidettävä järjestelmä, joka vähentää työasemien hallinnointiin kuluvaa aikaa sekä kustannuksia.

2 TIETOTURVA

2.1 Tietoturvan peruskäsitteitä

Tietoturva on jatkuvasti käynnissä oleva prosessi, jolla pyritään suojaamaan tärkeä kohde ulkopuoliselta uhkalta. Kohde voi olla henkilö, organisaatio tai omaisuus, kuten tietojärjestelmä tai yksittäinen tiedosto. Tietojärjestelmiin kohdistuvat uhat voivat kohdistua fyysisiin laitteisiin tai niiden sisältämään informaatioon. Näissä kaikissa tapauksissa tietoturvan tarkoituksena on estää luvaton pääsy näihin resursseihin, luvaton käyttö, muuttaminen tai niiden vahingoittaminen. Tietoturva voidaan jakaa seuraaviin pääosiin. (Kizza 2005, 49.)

1. Luottamuksellisuus

   Tiedot ovat vain niihin oikeutettujen käytettävissä ja tietojen paljastuminen kolmannelle osapuolelle estetään.

2. Eheys

   Tietojen luvaton muuttaminen estetään, samoin kuin niiden tuhoutuminen laitteisto- tai ohjelmistovikojen tai inhimillisen virheen seurauksena.

3. Saatavuus

   Tiedot, järjestelmät ja palvelut ovat esteettä niihin oikeutettujen käytettävissä, kun niiden käyttöön ilmenee tarvetta.

4. Osapuolten todentaminen

   Autentikointimenetelmä, jolla varmistetaan osapuolten olevan varmuudella niitä, joita ne väittävät olevansa.

5. Kiistämättömyys

Jälkikäteen voidaan todistaa jonkin tapahtuman tapahtuneen ja tapahtumaan osallistuneiden kiistaton osuus tapahtumien kulkuun. (Kizza 2005, 49-59.)

2.2 Tietoturvakäytännöt ja autentikointi

Tietoturvaratkaisuihin on olemassa monia erilaisia vaihtoehtoja ja niissä käytetään erilaisia teknologioita ja turvallisuusstandardeja. Päätarkoituksena on tuoda käytettävyyttä ja yhdenmukaisuutta erilaisten järjestelmäresurssien sisällä ja niiden välillä. Organisaatioiden sisällä tehdään päätökset toimialaan ja tarkoitukseen parhaiten sopivan standardin käyttöönottamiseksi. Oikean standardin valinnassa otetaan huomioon yrityksen koko, palvelun tyyppi ja toimiala.

Autentikointi on palvelu, jolla tunnistetaan verkon palveluja käyttävä asiakas. Tietojärjestelmien käytössä palvelua käyttävän asiakkaan tunnistaminen voi olla vaikea tehtävä, koska tunnetuksi asiakkaaksi voi tekeytyä joku toinen, joka haluaa mahdollisesti aiheuttaa vahinkoa järjestelmälle. Autentikointi on myös tietojärjestelmäprosessi, jossa palvelu kerää tietoa asiakkaasta tai asiakkaista, millä varmistetaan heidän henkilöllisyytensä. Tietoliikenteessä tyypillinen tapa autentikoida asiakas on käyttää salasana/haaste-menettelyä. Toinen tapa on käyttää autentikointiprotokollia, jotka perustuvat henkilökohtaisen avaimen tai julkisen avaimen käytäntöön, joilla käyttäjä tai laite tunnistetaan. Autentikointiprotokollakäytäntöjä käytetään myös lähetettävien viestien ja tiedostojen suojaamiseen sekä niiden aitouden varmistamiseen. (Kizza 2005, 55-56.)

2.3 Julkisen avaimen menetelmä

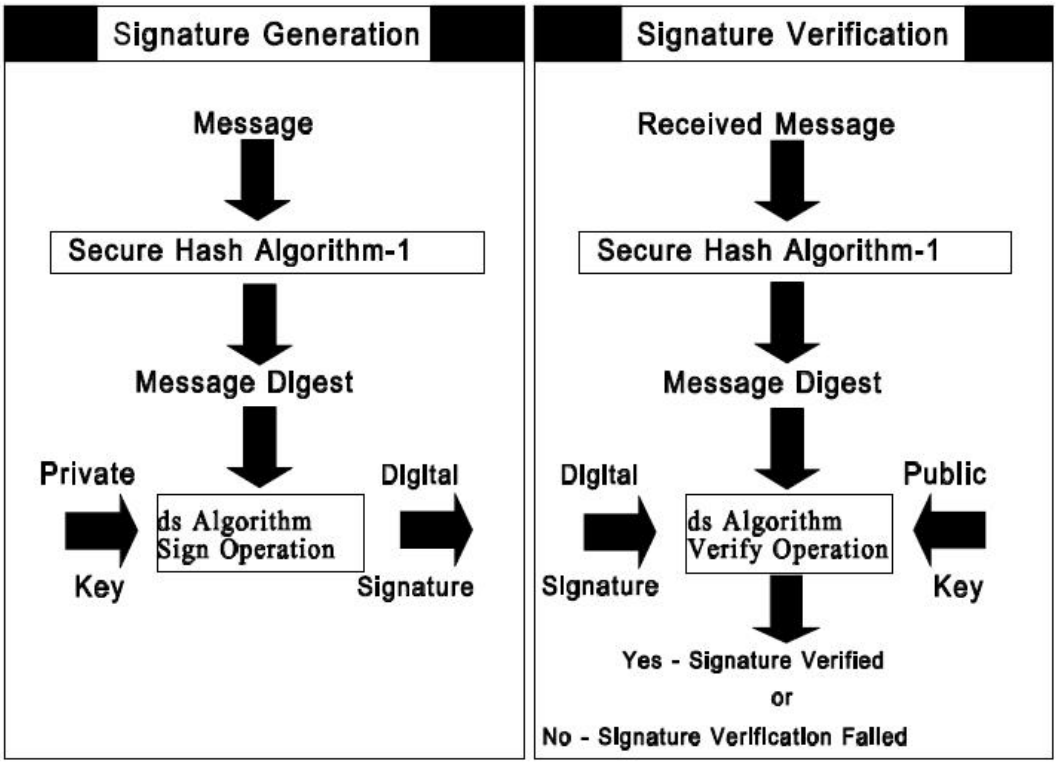
Julkisen avaimen järjestelmä on teknologinen ja poliittinen järjestelmä, jolla todennetaan käyttäjien, koneiden ja muiden tahojen henkilöllisyys kolmannen osapuolen avulla. Julkisen avaimen avulla voidaan selvittää, kenen hallussa julkista

avainta vastaava yksityinen avain on. Tämä on pohjana sille, että voidaan varmistaa lähettäjän aitous ja lähetetyn tiedon muuttumattomuus. Julkisen avaimen järjestelmä koostuu asiakasohjelmasta, palvelinohjelmasta ja sertifikaatin varmentajasta. (NIST 2001, 5.)

2.4 Digitaalinen allekirjoitus ja hash-funktio

Digitaalinen allekirjoitus esitetään tietokoneissa binäärimerkkijonona. Digitaalinen allekirjoitus muodostetaan sarjasta erilaisia sääntöjä ja muuttujia, niin että allekirjoittajan henkilöllisyys ja siirrettävän tiedon eheys voidaan todentaa. Allekirjoituksien luontiin ja varmentamiseen käytetään erityisiä algoritmejä. Digitaalisen allekirjoituksen luontiin käytetään henkilökohtaista avainta ja allekirjoituksen varmentamiseen käytetään julkista avainta. Salaukseen ja purkamiseen käytettävät avaimet ovat matemaattisesti toisistaan riippuvia siten, että toisella avaimella salattu viesti voidaan purkaa vain toista avainta käyttäen. Avaimet valitaan kuitenkin siten, että toista avainta on käytännössä mahdotonta saada laskettua toista hyväksi käyttäen. Jokainen käyttäjä hallitsee omaa henkilökohtaista- ja julkista avainpariaan. Julkisen avaimen oletetaan yleisellä tasolla olevan julkisesti tiedossa ja henkilökohtaista avainta ei koskaan lähetetä viestin tai tiedoston mukana sen salassa pitämiseksi. Käyttäjät, joilla on hallussaan jonkin toisen käyttäjän julkinen avain, voivat vahvistaa tältä tulleen tiedon kyseisellä avaimella. Digitaalisen allekirjoituksen voi luoda vain se henkilö, jolla on hallussaan henkilökohtainen avain. Digitaalisen allekirjoituksen menetelmä on esitetty kuviossa 1. (Kizza 2005, 279-282.)

SHA-, MD5- ja RSA-algoritmejä käytetään yleisesti hash-funktioina digitaalisten allekirjoitusten yhteydessä. Salattavaksi halutusta tiedosta lasketaan hash-funktion avulla tarkastussumma, jota kutsutaan tiivisteeksi (Message Digest). Tiiviste salataan digitaalisella allekirjoitusalgoritmilla ja lähetetään allekirjoitetun tiedon mukana. Vastaanottaja vahvistaa ja purkaa vastaanotetun tiedon lähettäjän julkisella avaimella ja laskee oman tiivisteen vastaanotetusta tiedosta, ja jos tiivisteet vastaavat toisiaan, oletetaan vastaanotetun tiedon olevan aito ja muuttumaton. (NIST 2000, 1.)



KUVIO 1 Digitaalisen allekirjoituksen toiminta. (NIST 2000, 2.)

2.5 Varmenne (certificate)

Varmenne on luotettavan kolmannen osapuolen myöntämä digitaalinen todistus, jonka avulla tietoa vaihtavat osapuolet tunnistavat toisensa. Tarkoituksena on estää ulkopuolisen tahon pääsy luottamukselliseen tietoon. Varmenteesta käy ilmi sen haltija, voimassaoloaika ja sen yksilöllinen sarjanumero. (Viestintävirasto 2007.)

Varmenteita on olemassa neljää eri tyyppiä.

Henkilövarmenne

Yksityisen henkilön käyttöön luovutettu varmenne. Henkilö tunnistetaan julkisen avaimen perusteella. Tyypillisesti varmenteessa on esitetty varmenteen haltijan sähköpostiosoite jolla varmenteen haltija voidaan tavoittaa. (Viestintävirasto 2007.)

Organisaatiovarmenne

Organisaatiovarmenne on tyypiltään muuten samanlainen kuin henkilövarmenne, mutta rooli on laajempi kuin yksityisellä henkilöllä. Usein varmenteessa on esitetty varmenteen haltijan sähköpostisoite, joka organisaation tapauksessa on yleisosoite, eikä kenenkään henkilökohtainen. (Viestintävirasto 2007.)

Palvelinvarmenne

Palvelinvarmenteella todennetaan palvelin sen kanssa tiedonvaihtoon pyrkiville käyttäjille tai tietokoneille. Usein varmenteessa on esitetty varmenteen haltijan sähköpostiosoite, joka palvelinvarmenteen tapauksessa on yleisosoite, eikä kenenkään henkilökohtainen. (Viestintävirasto 2007.)

Laatuvarmenne

Täyttää sähköisestä allekirjoitetusta säädetyn lain ja on laillisen varmentajan myöntämä. (Viestintävirasto 2007.)

2.6 Varmentaja (CA), Rekisteröijä (RA) ja Varmenteen luotettavuus

Varmentaja on luotettava julkisen avaimen järjestelmän taho, joka tuottaa ja allekirjoittaa varmenteet. Varmentaja tallettaa varmenteet julkiseen hakemistoon ja voi tarvittaessa peruuttaa varmenteen. Kesken voimassaoloajan peruutetut varmenteet julkaistaan erityisellä sulkulistalla. (Viestintävirasto 2007.)

Rekisteröijä on varmenteen hakijan todentava taho, joka varmistaa hakijan henkilöllisyyden varmentajan toimeksiannosta. Voi olla sama kuin varmentaja. (Viestintävirasto 2007.)

Varmenteen luotettavuudelle asetetaan seuraavat vaatimukset.

a) Varmenne on myönnetty hyväksyttynä varmenteena.

b) Varmenteen myöntäjä on virallisesti hyväksytty taho.

c) Varmenteen allekirjoittaja, organisaatio tai laite on tunnistettavissa

d) Allekirjoittajaan liitettävä erityismääre riippuen varmenteen käyttötarkoituksesta.

e) Allekirjoittajan valvonnassa olevat todentamiseen käytettävät tiedot on esitetty.

f) Varmenteen voimassaoloaika on selvästi esitetty.

g) Jokaisella varmenteella on oma yksilöllinen sarjanumero.

h) Varmenteesta on nähtävissä sen myöntäjän digitaalinen allekirjoitus.

i) Varmenteiden käytölle asetetut varmenteen lisälaajennukset sekä niihin liittyvät rajoitukset on esitetty.

j) Varmenteen käyttöä rajoittavat arvomääritykset toiminnoista, joissa sitä voidaan käyttää, on määritetty. (Directive 1999/93/EC, 7.)

Euroopan Unionin direktiivissä 1999/93 on määritelty suositukset unionin jäsenmaille koskien sähköisiä allekirjoituksia. Euroopan Unionin komission oli määrä seurata direktiivin toteutumista ja antaa siitä selvitys Euroopan parlamentille ja neuvostolle viimeistään 19. heinäkuuta vuonna 2003. Asiakirjaa, josta kävisi ilmi komission antamat suositukset sähköisen allekirjoituksen suuntaviivoiksi, ei kuitenkaan ollut saatavilla annetusta linkistä.

2.7 Varmenteiden sulkulista (certification revocation list)

Digitaalinen sertifikaattistandardi X.509, määrittelee myös metodin, josta käytetään nimeä sertifikaattien sulkulista. Tässä metodissa velvoitetaan jokainen varmentaja säännöllisin aikavälein julkaisemaan virallinen sertifikaattien sulkulista. Sertifikaattien sulkulista on aikaleimalla varmistettu ja varmentajan allekirjoittama lista, joka sisältää suljettujen sertifikaattien sarjanumerot ja on julkisesti saatavilla. Sulkulistan tarkoituksena on estää esimerkiksi sellaisten sertifikaattien käyttö, joiden salainen avain on joutunut vääriin käsiin tai varmenteen haltijan nimi on vaihtunut ennen varmenteen voimassaoloajan päättymistä. Varmenteen voimassaolo pitää aina varmistaa tarkastamalla sulkulista, ennen kuin se voidaan hyväksyä. (Network Working Group 2002, 11-12.)

3 ETHERNET JA VLAN

3.1 Ethernet

Ethernetin kehitys alkoi 1970-luvun alussa Xerox-yhtymän koeympäristössä, jossa koaksiaalikaapelilla toteutetussa Ethernet-verkossa saavutettiin 3 Mbit/s nopeus. Tämä onnistunut koe herätti yleistä kiinnostusta ja johti myöhemmin sen ajan kolmen suuren tietotekniikan kärkinimen Intelin, Digitalin ja Xeroxin yhteenliittymään. Nämä kehittivät yhdessä 10 Mbit/s Ethernet-versio 2.0:n 1980-luvun alussa. (Cisco Systems 2000, 81.)

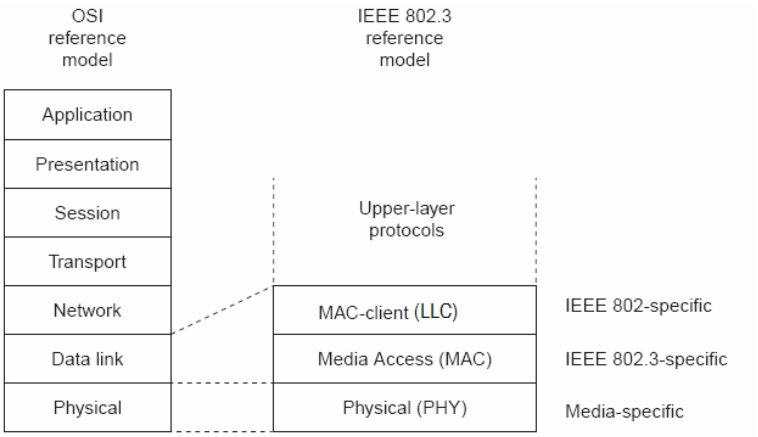
Nykyinen 802.3-standardi perustuu pitkälti versioon 2.0, joka otettiin ensimmäisen kerran käyttöön vuonna 1983 ja hyväksyttiin viralliseksi standardiksi 1985. Ajan kuluessa on standardia kehitetty tietoliikennetekniikoiden kehittyessä, liikennöintinopeuksien lisääntyessä sekä lisätty joustavuutta ottaen huomioon muita kehittyviä lähiverkon tekniikoita. (Cisco Systems 2000, 81.)

Kaikki uudemmat Ethernet-standardit ovat olennaisilta osiltaan yhteensopivia alkuperäisen standardin kanssa. Alkuperäistä standardia on korjattu siirtomedioiden ja siirtonopeuksien kehittyessä. Alaspäin yhteensopivuus takaa sen, että Ethernet-kehys voi siirtyä vanhemman version verkkomediasta uudempaan kehyksen muuttumatta. Tämä ominaisuus ja Ethernet-verkon hyvä laajennettavuus on sen nykyisen suosion perustana. (Cisco Systems 2000, 84.)

Ethernet on CSMA/CD-protokollaan perustuva jaetun verkkomedian kanavanvaraustekniikka. CSMA/CD-protokolla suunniteltiin alun perin ei-kytkentäiseen verkkoon, missä protokolla ei vaadi keskitettyä kehyksen välitystä, medialle pääsyn vuorottelua tai aikaan sidottua verkkomedian käytön jaksotusta. Ethernet-kanavanvarauksessa datalähetystä käyttävä verkkolaite kuuntelee ensin, onko verkko varattu, ja jos verkko on varattu, se odottaa satunnaisen ajan ennen kuin tekee uuden kuunteluyrityksen. Mikäli verkko on tällä kertaa vapaa, se aloittaa

datalähetyksen ja lähetyksen jälkeen siirtyy jälleen kuuntelemaan verkkoa. Jos joku toinen verkkolaite on lähettänyt samaan aikaan verkkoon dataa ja on tapahtunut lähetyksien yhteentörmäys, verkkolaitteet jatkavat lähettämistä niin kauan, että verkon kaikki laitteet huomaavat törmäyksen tapahtuneen. Törmäyksessä siirtomedian signaalin amplitudi nousee, mikä kertoo jaetun siirtomedian laitteille törmäyksestä. Törmäyksen sattuessa törmäyksen havainnut verkkoasema lähettää verkkoon jam-signaalin, jonka seurauksena lähettäminen keskeytetään ja erityinen backoff-algoritmi asettaa jokaiselle laitteelle lähetyskiellon satunnaiseksi ajaksi. Kaikki laitteet odottavat kunnes vaihtelevanmittainen lähetyskieltoaika on loppunut ja sen päätyttyä voi jokainen laite aloittaa uudelleen verkon kuuntelun. (Cisco Systems 2002, 253-254.)

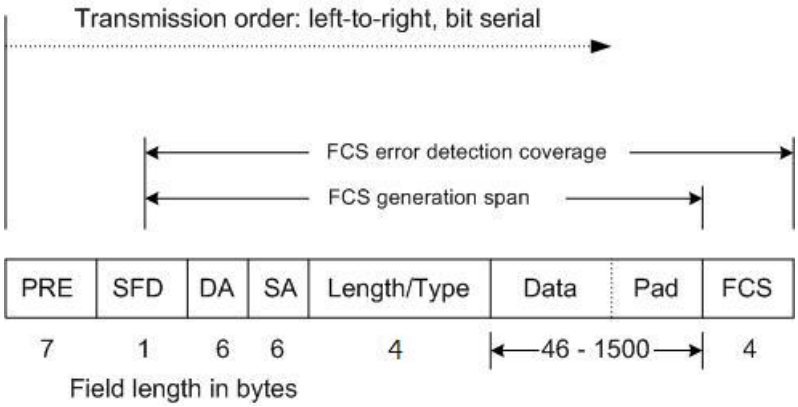
Ethernet toimii OSI-mallin kahdella alimmalla kerroksella, Fyysisellä (Physical Layer), joka on fyysinen siirtotie, ja siirtoyhteyskerroksella (Data Link Layer) joka huolehtii varsinaisesta lähiverkon laitteiden välisestä ja siirtomedian välisestä yhteydestä. Siirtoyhteyskerros jakaantuu kahteen osaan, MAC (Media Access Control) ja LLC (Logical Link Control). MAC-alikerros kontrolloi verkossa olevien verkkolaiteiden pääsyä ylemmälle OSI-tasolle ja datan lähetystä. LLC-alikerros huolehtii kehysten synkronoinnista, vuonohjauksesta ja virheentarkastuksesta. Ethernet- ja OSI-mallien kerrosrakenteet on esitetty kuviossa 2. (Cisco Systems 2000, 83.)



KUVIO 2. Ethernet- ja OSI-viitemalli (Cisco Systems 2000, 83.)

Datasiirron onnistumisen edellytyksenä Ethernetissä on osoitejärjestelmä, jolla lähettäjä ja vastaanottaja tunnistavat toisensa. Tämä osoitejärjestelmä perustuu verkkokorttien yksilöllisiin MAC-osoitteisiin. MAC-osoite on 48-bittiä pitkä ja esitetään 12-merkkisenä heksadesimaalilukuna. IEEE hallinnoi MAC-osoitteen kuutta ensimmäistä heksadesimaalilukua, jolla tunnistetaan verkkokortin valmistaja. Loput kuusi heksadesimaalilukua ovat valmistajakohtaisia laitteen sarjanumeroita. MAC-osoite on sisällytetty verkkokortin ROM-muistiin ja kopioidaan RAM-muistiin kun verkkokortti alustetaan. (Cisco Systems 2002, 217-221.)

IEEE 802.3 standardi määrittelee reunaehdot Ethernet-kehykselle sekä siinä käytetyt kentät jotka ovat pakollisia MAC-toteutuksille. Ethernet kehyksen rakenne on esitetty kuviossa 3. (Cisco Systems 2000, 85.)



KUVIO 3. IEEE 802.3 MAC-kehyksen rakenne (Cisco Systems 2000, 86.)

Seuraavassa on käyty läpi kuvion 3 kehyksen kenttien selitteet:

- PRE = Preamble, 7 tavua pitkä kenttä, joka sisältää vaihtuvalla sekvenssillä ykkösiä ja nollia, kenttää käytetään vastaanottajan tahdistukseen datasiirron alussa.

- SFD = Start-Of-Frame delimiter, 1 tavun mittainen kenttä, joka sisältää vaihtuvalla sekvenssillä ykkösiä ja nollia, loppuen kahteen peräkkäiseen 1 bittiin.

- DA = Destination Address, 6 tavua pitkä kenttä. Sisältää kehyksen vastaanottajan 48-bittisen MAC-osoitteen.

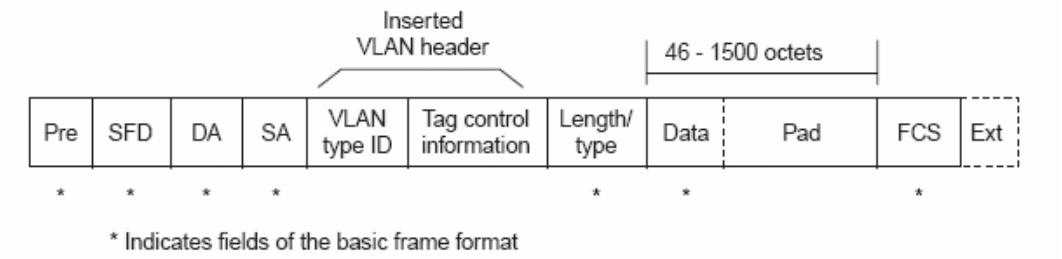
- SA = Source Address, 6 tavua pitkä kenttä. Sisältää kehyksen lähettäjän 48-bittisen MAC-osoitteen.

- Length/Type , 2 tavusta koostuva kenttä. Sisällön merkitys riippuu kentän arvon suuruudesta. Jos arvo ≤ 1500, niin kyseessä on pituusinformaatio, ja jos arvo < 1536, niin se kertoo kuljetettavan lisäoptiokehyksen lisäyksestä ja kentän arvo ilmoittaa uuden kehyksen lähetyksestä tai vastaanotosta.

- Data , 46-1500 tavua pitkä kenttä. Mikäli kentän pituus on alle 64 tavua lisätään siihen täytettä (Pad).

- FCS , Frame check sequence, 4 tavua pitkä kenttä. Sisältää siirretyn datan tarkastussumman (CRC) cyclic redundance check arvon. Sen luo lähettäjä ja vastaanottaja tarkastaa, onko kehys ehyt. (Cisco Systems 2000, 85.)

IEEE 802.3-standardi sisältää myös määrittelyt Ethernet-kehyksen lisäkentille, joita käytetään lisäämään protokollan ominaisuuksia. Yksi näistä lisäoptioista on VLAN-otsake. VLAN-otsake on esitetty kuviossa 4. (Cisco Systems 2000, 90.)



KUVIO 4. VLAN-laajennus Ethernet-kehykseen. Cisco Systems 2000, 91.)

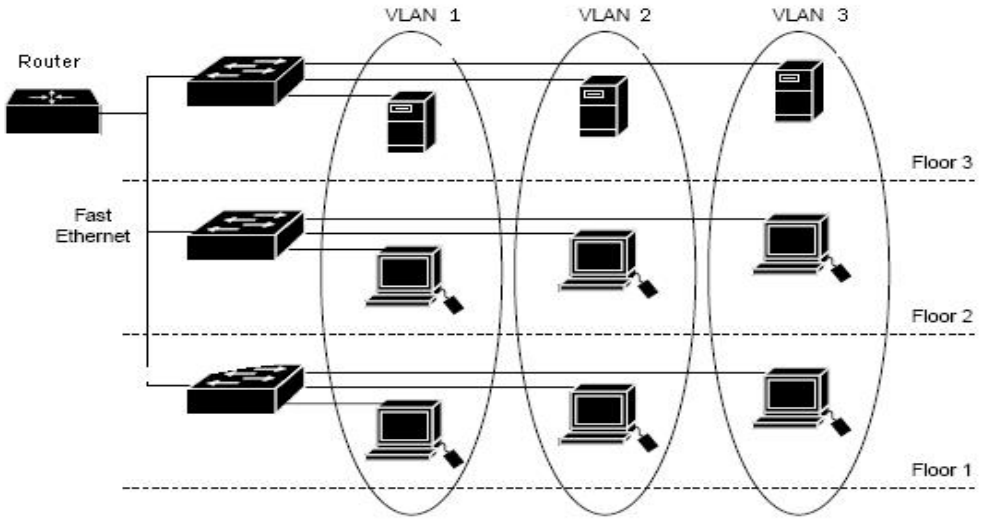
VLAN-otsake lisätään Source Address ja Length/Type-kenttien väliin. Otsake sisältää kaksi 2 tavun mittaista kenttää. Ensimmäinen 2 tavun VLAN-tag-kenttä sisältää 802.1Q-tag tyypin, ja sen arvo on oletuksena heksadesimaaliluku 0x8100. Tämä arvo on varattu Ethernet-kehyksen VLAN-laajennukselle ja ilmoittaa VLAN-tag lisäyksestä kehykseen ja kertoo Length/Type-kentän siirrosta 4 tavua eteenpäin kehyksessä. Toinen 2 tavun VLAN-tag sisältää kehyksen siirtoprioritee-

tin (0-7), jossa 7 on korkein prioriteetti ja VLAN ID:n, joka ilmoittaa mihin tiettyyn VLAN:iin kehys siirretään. (Cisco Systems 2000, 90-91.)

3.2 VLAN-protokollien kehitys

1990-luvun alussa alettiin lähiverkon keskittimiä ja 2-porttisia siltoja korvata moniporttisilla kytkimillä, mikä vähensi reitittimien käytön tarvetta jaettaessa verkkoja pienempiin segmentteihin. Segmentoinnin tarkoituksena on jakaa lähiverkko pienempiin osiin, koska etenkin Ethernet-tekniikkaa käyttävissä verkoissa voidaan yhtäaikaisista lähetyksistä aiheutuvia törmäyksiä vähentää kytkimillä. Reitittimien jakaessa lähiverkkoja segmentteihin OSI-mallin 3-kerroksella, päästiin kytkimillä rajoittamaan segmentit pienempiin osiin jo OSI-mallin 2-kerroksella. Tämä vapautti reitittimille kapasiteettiä hoitamaan päätehtäväänsä reititystä ja rajoittamaan lähiverkkojen yleislähetysviestejä. Kytkentäisellä verkolla saadaan myös kaistanleveys paremmin hyödynnettyä, kun tiettyyn kohteeseen kohdistettu lähetys ohjataan vain kytkimen portista toiseen, eikä kaikkiin portteihin, kuten keskittimissä. Kytkimien jatkuvasti lisääntyneestä käytöstä huolimatta lähiverkkojen jakaminen pienempiin osiin ei ratkaissut yleislähetysviestien osuuden vähentämisen tarvetta. VLAN:n-tekniikan esiintulo tarjosi vaihtoehtoisen tavan reitittimien ohella rajoittaa yleislähetysviestisegmenttien kokoa lähiverkoissa. (Decisys 1996, 2.)

VLAN, alkuperäiseltä nimeltään Virtual LAN, on kytkentäinen tietoliikenneverkko, joka on jaettu loogisiin segmentteihin ennalta määritetyn toiminnallisuuden mukaan. Samaan LAN:iin kuuluvien laitteiden ei tarvitse näin ollen sijaita fyysisesti samassa segmentissä, tilassa, kerroksessa tai rakennuksessa. Samaan yleislähetysviestialueeseen kuuluvien VLAN:ien välinen liikenne välitetään ohjelmallisesti kytkimissä, ja eri VLAN:ien välinen liikenne ohjataan reitittämällä. Kytkinten välittämällä liikenteellä saadaan yhteyksien muodostamisessa aikaan pienempi viive verrattuna reitittimellä yhdistettäviin verkkoihin, koska reitittimien vaatima reititysprosessi vaatii enemmän laskentaa ja aikaa. VLAN-reitityksen periaate on esitetty kuviossa 5. (Decisys 1996, 10.)



KUVIO 5. VLAN reititys. (Cisco Systems 2006, 254.)

Kuviossa 5 samassa fyysisessä kerroksessa sijaitsevat työasemat ovat kytkettyinä kytkimeen, joka jakaa kerroksen kolmeen eri VLAN:iin, Kytkimet ovat yhdistettyinä trunk-porttien kautta reitittimen sisäverkon liitäntärajapintaan, johon on konfiguroitu jokaista VLAN-verkkoa vastaavat aliverkot reitityksen mahdollistamiseksi.

VLAN-tekniikan käytöstä on seuraavia etuja:

1) Verkkokapasiteetin tehokas hyödyntäminen

Tarpeettomien yleislähetysviestien ja monilähetysviestien suodattaminen pois vähentää verkon kapasiteetin tuhlausta ja näin jää hyötydatalle enemmän kaistanleveyttä käytettäväksi. Kytkimien OSI:n 2-tasolla välittämä liikenne vähentää reitityksen tarvetta ja nopeuttaa pakettien välitystä.

2) Virtuaalisten käyttäjäryhmien muodostaminen

VLAN:n käyttö mahdollistaa käyttäjien helpomman ryhmittelemisen ja hallinnan, kun verkon fyysinen topologia ei ole enää sitä rajoittava tekijä.

3) Verkon ylläpito

Verkon ylläpitoon kuluvaa aikaa voidaan vähentää jos käytetään joko dynaamista käyttäjien tunnistusta tai MAC-osoitteisiin perustuvaa VLAN-määritystä.

4) Verkon turvallisuuden lisääntyminen

Lähiverkon tietoturvaa voidaan parantaa hallittavilla kytkimillä, koska käyttäjät tai laitteet voidaan tunnistaa porttikohtaisesti IEEE 802.1x-standardin mukaisilla autentikointi menetelmillä. (Schneider 2001, 17-19.)

3.3 VLAN-verkkojen toiminta

Data-paketin saapuessa verkon laitteelta kytkimeen siihen liitetään VLAN-tag osoittamaan siihen VLAN:iin, mistä paketti saapui. On myös mahdollista päätellä paketin VLAN-ID sen välittäneen portin perusteella siitä, mihin VLAN-ryhmään portti kuuluu. VLAN-tag:n lisääminen pakettiin voi perustua sen välittäneeseen porttiin, lähettäjän MAC-osoite kenttään tai protokollaan perustuvaan lähettäjän osoitteeseen. VLAN:it luokitellaan käytettävän menetelmän mukaan. Riippumatta käytettävästä menetelmästä on kytkimen ylläpidettävä tietokantaa olemassa olevista VLAN:eista ja päivitettävä sitä säännöllisesti, jotta on tiedossa, mitä tag-luokittelua kulloinkin käytetään. Kytkimet liitetään toisiinsa ja myös reitittimeen käyttäen sitä tarkoitusta varten luotua trunk-porttia. Trunk-portti on yksi kytkimen portti, johon on yhdistetty kaikkien kytkimessä olevien VLAN:ien verkkoliikenne ohjelmallisesti. VLAN-verkkojen välinen liikenne erotetaan toisistaan käyttämällä VLAN-tageja, jotka on esitetty kehyksen VLAN-otsakkeessa. Eri VLAN-tyyppejä on esitetty seuraavassa. (Schneider 2001, 19.)

Porttikeskeinen VLAN:

Porttikeskeisessä VLAN:ssa kaikki kytkimen portit määritellään erikseen tiettyyn VLAN:iin kuuluvaksi ja samaan VLAN:iin kuuluviin portteihin liitetyt verkon laitteet saavat saman VLAN-ID:n. (Schneider 2001, 20.)

MAC-Osoite VLAN:

Työasemat liitetään VLAN:iin verkkokortin MAC-osoiteen perusteella ennalta määritettyyn VLAN:iin. Siirrettäessä työasema fyysisesti toiseen kytkimeen tämä ei aiheuta kytkimen uudelleen konfigurointia, vaan työaseman VLAN-ID jäsenyys säilyy, kunnes MAC-osoitteen mukaista VLAN-ID jäsenyyttä muutetaan. (Schneider 2001, 20-21.)

Dynaaminen VLAN:

Työasemien liittäminen tiettyyn VLAN:iin voi perustua MAC-osoitteisiin, loogisiin osoitteisiin tai käytettävään protokollaan. Kytkimeen konfiguroidaan tarvittavat VLAN:it ja määritellään kytkin käyttämään 802.1x-protokollan mukaista autentikointia. Autentikointiin käytetään erillistä siihen tarkoitettua palvelinta, jonka tietokannassa on tieto työaseman kuulumisesta tiettyyn VLAN:iin. Oletuksena kaikki kytkimen portit kuuluvat samaan VLAN:iin, kunnes työasema kytketään kytkimen vapaana olevaan porttiin, mikäli autentikointipalvelin vahvistaa työaseman lähettämät tiedot, liitetään työasema autentikonti palvelimessa määriteltyyn VLAN:iin. (Cisco Systems 2006, 187-189.)

4 RADIUS

4.1 AAA-autentikointipalvelu ja -protokollat

AAA-protokolla on tarkoitettu autentikoimaan käyttäjiä sekä antamaan heille valtuuksia palveluihin dynaamisesti, käyttäjän tai palvelun perusteella. Valtuudet määritellään käyttäjille luomalla erilaisia sääntöjä ja lisäämällä nämä tarjolla oleviin palveluihin. AAA-arkkitehtuuri perustuu kolmeen turvallisuustoimintoon, jotka tarjoavat joustavan mahdollisuuden vahvaan käyttäjän sekä palvelun autentikointiin ja niiden avulla luottamukselliseen palveluiden tarjontaan ja käyttöön. AAA-arkkitehtuurin kolme turvallisuustoimintoa on seuraavat. (Cisco Systems 2001, 2.)

Autentikointi (Authentication)

Metodi, jolla käyttäjä tunnistetaan, voi sisältää erilaisia menetelmiä mukaan lukien sisäänkirjautumisen yhteydessä käytävän käyttäjä/salasana-dialogin, vastaus/haastemenettelyn ja riippuen käytettävästä protokollasta myös mahdollisen salausmenetelmän. .(Cisco Systems 2006, 1-2.)

Valtuutus (Authorization)

Metodi, jolla käyttäjän valtuudet käyttää verkon resursseja on määritetty. Käyttäjän kirjautuessa työasemalta verkkoon, käyttäjän oikeudet verkon resursseihin tarkastetaan keskitetystä käyttäjätietokannasta ja lisätään välittämällä ne AAA-palvelimelle. .(Cisco Systems 2006, 1-2.)

Tilastointi (Accounting)

Metodi, jolla kerätään tietoa laskutuksen ja raportoinnin pohjaksi käyttäjien resurssien käytöstä, niiden käyttöajankohdasta ja siirretyn datan määristä. (Cisco Systems 2006, 1-2.)

AAA-protokolla on alun perin suunniteltu NAS (Network Access Server) käyttöön. Tarkoituksena oli tarjota NAS:ien ohjaama ja välittämä PPP (Point-To-Point) -yhteys Internet-resursseihin. Käyttäjämäärien kasvaessa kävi epäkäytännölliseksi jokaisessa NAS-palvelimessa sijaitsevien omien käyttäjälistojen ja käyttäjäoikeuksien ylläpitäminen. Ongelman ratkaisemiseksi kehitettiin uusia protokollia, jotka tukivat keskitettyä AAA-palvelinkäytäntöä. Näiden uusien protokollien avulla tuli mahdolliseksi ottaa käyttöön keskitetty AAA-palvelin, joka mahdollisti käyttäjien autentikoinnin, valtuuksien tarkastamisen palveluiden käytössä sekä niiden käytön tilastoinnin. (Network Working Group 2006, 17.)

PPP-protokolla jakaantui alkuperäisessä muodossaan kolmeen pääosaan.

1. Enkapsulointi

Metodi, jolla paketoidaan multiplexeriin eri verkkotason protokollia samalle fyysiselle siirtotielle. PPP-protokollan enkapsulointiominaisuudet on huolellisesti suunniteltu sisällyttämään yhteensopivuus useimpien verkkolaitevalmistajien tuotteiden kanssa. (Network Working Group 1994, 1.)

2. LCP-protokolla

Varmistaakseen riittävän monipuolisen tuen erilaisiin verkkoympäristöihin PPP-protokollaan sisällytettiin Link Contol-protokolla. LCP:n tehtävänä on hyväksyä automaattisesti enkapsulointimuotoiluoptiot, huolehtia pakettien kokoon liittyvistä vaihtelevista rajoituksista ja mahdollisista konfigurointivirheistä sekä linkkiyhteyden päättämisestä. LCP:n muita lisäpalveluoptioita ovat päätelaitteen autentikointi ja linkkiyhteyden tilan valvominen. (Network Working Group 1994, 1.)

3. NCP-protokollat

PPP-protokollalla oli taipumuksena aiheuttaa monia ongelmia käytössä olevien verkkoprotokollien kanssa, ja erityisesti IP-osoitteiden liittäminen verkon laitteisiin ja osoitteiden hallinta oli erityisen vaikeata piirikytkentäisissä verkkoyhteyksissä. Näitä ongelmia pyrittiin ratkaisemaan NCP-protokollien avulla, joista jokainen tarjosi erityisiä palveluja ylemmän tason verkkoprotokollille. (Network Working Group 1994, 1.)

PPP-protokollaan oli alkujaan määritelty tuki vain PAP-ja CHAP-autentikoinnille, ja niiden käytön laajentuesssa tuli esille niiden autentikointimekanismien rajallisuus. PAP ja CHAP ovat yksisuuntaiseen autentikointiin perustuvia, jossa käyttäjä todennetaan NAS-palvelimelle. PAP:n puutteena on vielä salasanan lähettäminen selväkielisenä ja todennusprosessi on siten alttiina verkossa tapahtuvalle käyttäjän ja NAS-palvelimen välisen liikenteen kaappaukselle. CHAP on MD5-algoritmiin perustuva haaste/vastaus-protokolla ja tarjoaa PAP-protokollaa paremman suojan autentikointiin, mutta on haavoittuvainen viestin murtoyrityksille, jotka perustuvat sanakirjatekniikkaan. (Network Working Group 2006, 17.)

Tietoturvavaatimuksien ja vahvemman salauksen tarpeen kasvaessa määriteltiin PPP-protokollaan lisäosana ECP-protokolla, jossa OSI-2:n linkkitason salakirjoitusavainten tasoa parannettiin huomattavasti. PPP-yhteyden tietoturvan lisäämiseksi sekä kaksisuuntaisen autentikoinnin ja dynaamisen avaimen luonnin mahdollistamiseksi kehitettiin vielä valmistajakohtaiset MS-CHAP ja MS-CHAPv2 laajennukset PPP-protokollaan. Myöhemmin, kuten PAP-ja CHAP-protokollien kohdalla, löytyi näidenkin mekanismeista omat heikkoutensa. Huolimatta siitä, että PPP toteutti yhteyden muodostamisen ja autentikoinnin perusvaatimukset, autentikontimekanismeista löytyneet heikkoudet vaativat korjauksia yhteyden muodostaviin prookolliin. (Network Working Group 2006, 17-18.)

Uutta autentikointimenetelmää tarvittiin niin yhteyden muodostamista tarvitsevan käyttäjän kuin AAA-palvelimen taholta. Tehokkaampaan autentikointiin sekä korjauksena aikaisempiin menetelmiin kehitettiin uusi autentikointiprotokolla

EAP, johon oli otettu mukaan tuki myös keskitetylle autentikointipalvelulle, joka sai nimen RADIUS (Remote Authentication Dial In User Service). EAP-protokolla toi mukaan myös uuden käytännön, jossa NAS, yleensä verkon kytkin tai langaton tukiasema, toimii autentikointipyynnön välittäjänä työaseman ja keskitetyn autentikointipalvelimen välillä. (Network Working Group 2006, 18.)

4.2 RADIUS-protokollan historia

Vuonna 1991 Michiganin osavaltion yliopistojen MichNet-verkkoa ylläpitävä Merit Network Inc. käynnisti prosessin valitakseen uuden sovelluksen hoitamaan soittosarjapalveluiden käyttäjien hallintaa. Merit-yhtymä laati RFI-pohjan (Request For Information) siitä, mitä palvelun tuli pitää sisällään ollakseen riittävän tehokas ja tarjotakseen verkkoyhteyksiä suurelle määrälle käyttäjiä. Tarjouspyynnöt osoitettiin kahdeksalle ohjelmistovalmistajalle, mutta suurimmalle osalle valituista ohjelmistovalmistajista vaatimukset olivat ylivoimaisia toteutettavaksi ja vain yhden toimittajan kanssa oli vakavampia neuvotteluja. Tämänkin ohjelmistovalmistajan autentikointiprotokolla oli osittain puutteellinen ja neuvottelut loppuivat tuloksettomina. Muutamia kuukausia myöhemmin yhtymästä nimeltään Livingston otettiin yhteyttä Merit Network:iin joka tarjosi omaa tuotettaan ehdolle. Livigston-yhtymällä oli lähes RFI:n vaatimukset täyttävä ”postmaster” soittosarjapalvelintuote, johon he olivat kehittäneet myös asiakassovelluksen. Tutkittuaan tuotteen soveltuvuutta MichNetin käyttöön, Merit-yhtymä teki sopimuksen Livigstonin kanssa tuotteen ostamisesta. Merit kehitti ostamaansa ”postmaster” tuotetta lisäämällä siihen lisäominaisuuksia, ja vuoden kehitystyön tuloksena oli Merit-RADIUS Server, jota on käytetty suojaamaan niin modeemi-yhteyksien kuin myös langattomien verkkojen käyttäjien autentikointia. (Interlink Networks 2006, 1-2.)

Vuonna 1992 muodostettiin IETF:n työryhmä kehittämään NAS-vaatimuksia, ja vuonna 1994 RADIUS-protokollan kehittäjät tarjosivat esitystä standardisoitavaksi. Esitys pohjautui Livingstonin kehittämään protokollaan ja lähdekoodi tarjottiin avoimesti käytettäväksi. Suuri osa tällä hetkellä käytössä olevista RADIUS-palvelimista perustuu kyseiseen lähdekoodiin.(Interlink Networks 2006, 1-2.)

4.3 RADIUS-autentikoinnin osapuolet

RADIUS-autentikointi tapahtuu yleensä kolmen osapuolen kesken, jos asiakkaina langattomassa verkossa ovat kannettavat tietokoneet tai kiinteässä lankaverkossa kiinteästi verkkoon kytketyt työasemat. Autentikoijana toimii NAS eli kytkin tai AP (Access Point) eli langaton tukiasema. Autentikointipalvelimena toimii RADIUS-palvelin, joka voi ylläpitää omaa käyttäjätietokantaa tai olla yhteydessä keskitettyyn käyttäjätietokantaan. Autentikoija ja autentikointipalvelin käyttävät toistensa tunnistamisen vahvistamiseksi salasanaa, joka määritellään NAS:iin ja autentikointipalvelimeen, jota ei koskaan lähetetä verkon yli. Autentikoija välittää verkkoon kirjautumista yrittävän asiakkaan kirjautumisyrityksen autentikointipalvelimelle ja toimii Radius-viestien välittäjänä asiakkaan ja autentikointipalvelimen välillä yhteyden muodostamisen aikana. Verkkoon autentikoitumiseen välitettävää informaatiota voi olla RADIUS-palvelimesta riippuen henkilökohtainen käyttäjätili, tiettyyn käyttäjäryhmään kuuluminen tai tietokoneen ainutkertainen tunnus. (Network Working Group 2000, 10.)

RADIUS käyttää UDP-protokollaa autentikointiviestien välittämiseen. Aikaisempien versioiden käyttämä porttinumero oli 1645, mutta se oli myös datametrics-palvelun käyttämä, joten RADIUS-palvelulle määritettiin käyttöön uusi porttinumero 1812. UDP-protokollaan päädyttiin käytännöllisistä syistä, joita on esitetty seuraavana.

1. Alkuperäinen Access Request -viesti säilytetään OSI-mallissa määritetyn transport-kerroksen yläpuolella vaihtoehtoista RADIUS-palvelinta varten, jos primääripalvelinta ei tavoiteta.

2. UDP:n ajoitusmääritykset poikkeavat merkittävästi TCP-protokollasta. Käyttäjän ei tarvitse odottaa TCP-protokollan kaltaista uudelleenlähetystä, vaan Access Request -viesti voidaan ohjata uudelleen toiselle RADIUS-palvelimelle, mikäli primääripalvelinta ei tavoiteta.

3. UDP on yhteydetön protokolla ja siitä johtuen yhteyden muodostaminen ja sulkeminen voidaan suorittaa ilman monimutkaisia kättelyjä.

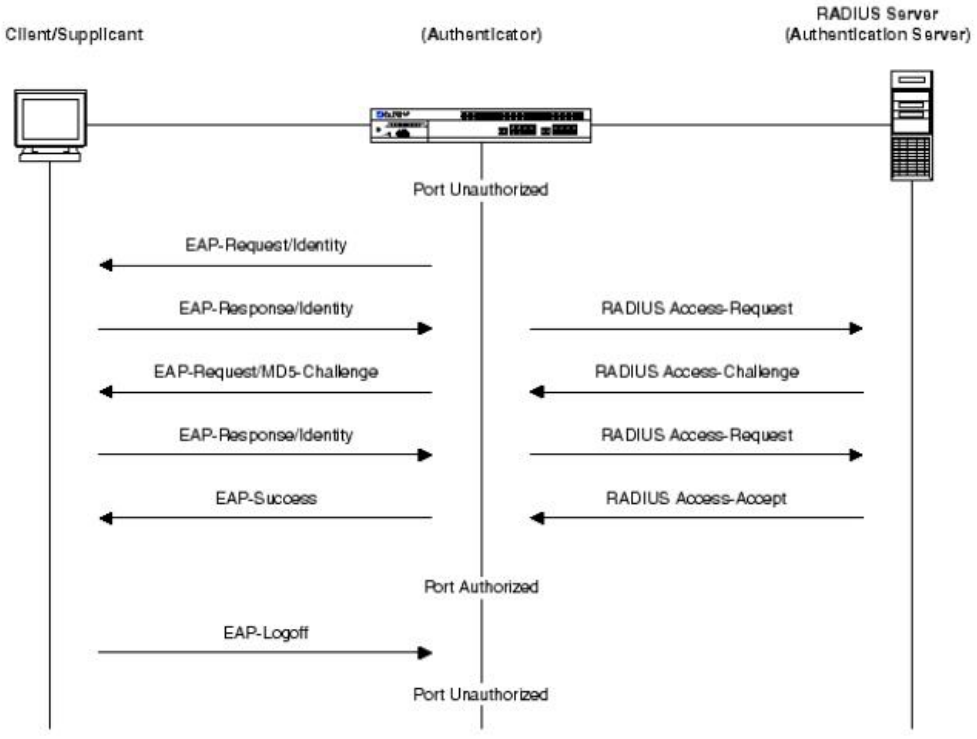
4. Ensimmäisissä RADIUS-versioissa palvelin pystyi käsittelemään vain yhden Request/Response -prosessin kerrallaan, jättäen asiakkaat jonoon odottamaan. Request/Response -prosessin uudelleenkäynnistymistä säätävää aikaa muutettiin, jotta vältettäisiin turhat samojen asiakkaiden autentikointipyynnöt. Seurauksena olivat pidentyneet odotusajat ja asiakkaiden turhautuminen. Asia ratkaistiin muuttamalla palvelimen rakenne monisäikeiseksi. Kaiken pohjana oli UDP-protokollan käyttö pakettien välittämisessä, joka vähensi viiveitä ja palvelin kykeni vastaamaa nopeasti lähetettyyn pyyntöön. Kaikesta tästä huolimatta UDP-protokollan käyttö vaatii RADIUS palvelimelta yhtä ominaisuutta käytettäväksi, joka sisältyy TCP-protokollaan, uudelleenlähetyksen ajoittamiset on suoritettava keinotekoisesti verrattuna TCP:en. (Network Working Group 2000, 11-12.)

4.4 RADIUS-protokollan toiminta kytkinverkossa

RADIUS:ta käytettäessä täytyy asiakastyöasema määritellä käyttämään valittua tunnistusmetodia; tämä riippuu siitä, mitä yhteydenmuodostamisprotokollaa on tarkoitus käyttää. Vastaavasti kytkin (NAS), joka toimii RADIUS-viestien välittäjänä, määritellään käyttämään automaattista porttien tilanmuutoksien valvontaa ja toimimaan yhteydessä RADIUS-palvelimen kanssa.

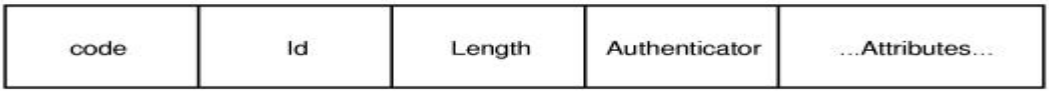
Kun työasema on määritetty käyttämään RADIUS-autentikointia ja se kytketään verkkoon, niin varsinainen RADIUS-istunnon muodostaminen voi alkaa. Mikäli kytkin(NAS) havaitsee kyseisen portin tilanmuutoksen, se lähettää EAP-Request/Identity -viestin työasemalle. Mikäli työasema ei saa kyseistä RADIUS-viestiä, se voi käynnistää istunnon lähettämällä EAPOL-Start-viestin kytkimelle. Työasema vastaa kyselyyn lähettämällä EAP-Response/Identity-viestin kytkimelle, tämä voi sisältää käyttäjätunnuksen ja salasanan sekä työaseman ID:n ja porttinumeron, johon työasema haluaa kytkeytyä. Mikäli viesti sisältää salasanan, niin viesti salataan käyttämällä RSA:n Message Digest algoritmia MD5:ttä. Kytkin välittää viestin RADIUS Access-Request muodossa RADIUS-palvelimelle. Mikäli viestiin ei saada vastausta kehykseen asetetun aikarajan puitteissa, viesti lähete-

tään uudelleen. RADIUS-palvelimen saadessa viestin se tarkistaa lähettäjän aitouden, jos lähettäjä todetaan aidoksi, palvelin tarkastaa tietokannasta tunnistettavan oikeudet, täyttävätkö ne verkkoon pääsyn vaatimukset, mikä riippuu siitä täyttyvätkö pääsyvaatimukset, jos vaatimukset eivät täyty, lähettää palvelin Access-Reject –viestin, jolla verkkoon pääsy evätään. Pääsyvaatimuksien täyttyessä RADIUS-palvelin lähettää Access-Challenge -viestin kytkimelle, joka vastaa siihen lähettämällä alkuperäisen RADIUS Access-Request -viestin muuttamalla sen ID-tunnisteen ja lisäämällä käyttäjä/salasana-atribuutin salattuna vastaukseen sekä tila-atribuutin Access-Challenge -viestistä. Vain tila-atribuutin arvot 0 tai 1 ovat sallittuja. Jos kaikki yhteyden muodostamiseen vaadittavat kriteerit täyttyvät, RADIUS-palvelin lähettää Access-Accept -viestin kytkimelle, joka avaa kyseisen portin käyttöön ja välittää työasemalle EAP-Success viestin sekä konfiguraatioparametrit yhteyden käyttämiseksi. Työaseman päättäessä istunnon se lähettää EAPOL-Logoff -viestin kytkimelle, joka vaihtaa portin tilan suljetuksi. EAP-vietien vaihto on esitetty kuviossa 6. (Cisco Systems 2006, 187-193.)



KUVIO 6 EAP viestien vaihto RADIUS Autentikoinnissa (Cisco Systems 2006, 192.)

RADIUS Access-Request- ja muut datapaketit sisältävät kehyksen ja muuttuvan määrän attribuutti-arvopareja, joita käytetään RADIUS-viestien vaihdossa. RCF 2865:ssa on määritelty eri laitevalmistajille tarkat suositukset, joiden rajoissa ne voivat käyttää kyseistä protokollaa. RFC 2865:ssa on määritelty myös enkapsulointi, minkä puitteissa protokollan laajennuksia voidaan ottaa käyttöön. Mikäli näitä määrityksiä ei noudateta, seurauksena voi olla odottamattomia dataliikenteeseen vaikuttavia ristiriitoja. Ristiriitojen seurauksena voi olla, että näissä RADIUS-viestien vaihtoprosesseissa voidaan ottaa vahingossa käyttöön vääriä sisäisiä ID-tunnisteita. RADIUS-kehys on esitetty kuviossa 7. (Hewlett Packard 2003.)



KUVIO 7 RADIUS- Request/Reply viesti kehys (Hewlett Packard 2003.)

Seuraavassa esitetään kuvion 7, RADIUS-viestin kenttien selitteet.

Code = 8-bittinen Request/Reply tyyppi, jonka arvo kertoo sen tarkoituksen.

1 = Access-Request, asiakkaan lähettämä todentamispyyntö.

2 = Access-Accept, palvelimen lähettämä todentamisen hyväksyminen

3 = Access-Reject, palvelimen lähettämä todentamisen epäonnistuminen/hylkääminen.

4 = Accounting-Request, asiakkaan lähettämä tilastoinnin aloituspyyntö.

5 = Accounting-Response, palvelimen vastaus tilastoinnin aloittamisesta.

11 = Access-Challenge, palvelimen asiakkaalle lähettämä autentikointi haaste.

Id = 8-bittinen järjestysnumero, jossa Reply arvo = Request arvo

Length = 16-bittinen, viestin pituus sisältäen otsakkeen alkaen Code-kentästä.

Authenticator = 16 oktetin pituinen binääri-vektori-muotoinen kenttä, joka Request-tyyppisenä generoidaan sattumanvarais-menetelmällä. Reply on MD5-digest-tiivistellä salattua Request-vektori arvosta laskettua dataa. (Hewlett Packard 2003.)

Attributes = Sattumanvarainen määrä informaatiopareja joiden arvoja on esitetty kuvion 8 selitteessä.

Attribuutti-arvopari esittää muuttujan tyypin ja sen arvon. Tyypillisesti nämä parit ovat muotoa: käyttäjätunnus/salasana tai NAS-IP-osoite/NAS-porttinumero. Attribuutti-arvoparien mukanaolo riippuu normaalisti konfiguraatiotiedostojen määrityksistä, eli siitä mitä atribuutteja autentikoinnissa käytetään. Atribuuttien määrästä huolimatta vain osa näistä lähetetään salattuina verkon yli, tyypillisesti käyttäjätunnus ja salasana. Näiden atribuuttien salaaminen perustuu NAS:in ja autentikointipalvelimen väliseen yhteiseen salaisuuteen, joka takaa sen, että yhteyspyyntö tulee luotettavasta lähteestä. Kehyksen atribuuttien pariarvot on esitetty kuviossa 8. (Hewlett Packard 2003.)

KUVIO 8 Atribuutti-pariarvon muoto (Hewlett Packard 2003.)

Seuraavana on esitetty attribuutti arvoparien arvojen muodostuminen.

Atribuutti = 8-bittinen arvopari numero.

Length = 8-bittinen kokonaisluku väliltä 2-255.

Value = 0-253 oktettia pitkä informatiivinen tietotyyppi. Tietotyypin arvo määritetään attribuuttikentässä olevan tiedon perusteella. (Hewlett Packard 2003.)

4.5 EAP-protokolla

Yleisesti käytettyjä EAP-protokollia on olemassa EAP-MD5, EAP-OTP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-FAST ja EAP-PEAP(MS_CHAPv2). Näistä osa on valmistajakohtaisia ja osa verkkomediaan sidottuja protokollia. Koska osa näistä protokollista on osoittautunut tietoturvaominaisuuksiltaan heikoksi, on vahvaa autentikointia vaadittaessa keskityttävä vain vahvaksi tunnustettuihin EAP-TLS- ja EAP-PEAP-protokolliin. Käytettäessä sertifikaattipohjaista tunnistusmenetelmää tai älykorttia on protokollana EAP-TLS, joka on myös vahvin EAP-suojausmenetelmä. Käytettäessä henkilökohtaista käyttäjätunnusta ja salasanaa on protokollana EAP-PEAP (MS-CHAPv2). Autentikointiprosessi on edellisissä hyvin samanlainen, erona on vain se että EAP-PEAP-prosessi on kaksivaiheinen. Yhteisenä osana on EAP-TLS:ssa ja EAP-PEAP:ssa on TLS-yhteyden luominen autentikoinnin suojaamiseksi. (Cisco Systems 2004, 14-17, 20.)

4.6 EAP-TLS

Extensible Authentication Protocol - Transport Layer Security-metodia käytetään sertifikaattipohjaisessa autentikoinnissa, joka on kaksisuuntainen tunnistusmenetelmä, jossa molemmat autentikoinnin osapuolet varmistavat toistensa aitouden. Tunnistaminen perustuu osapuolien neuvottelemaan yhteiseen salausmenetelmään ja salausavaimeen, joka on vain asiakastyöaseman ja tunnistamisen suorittavan RADIUS-palvelimen käytössä. EAP-TLS-käyttö vähentää autentikoinnin viivettä, koska autentikoinnin alkaessa TLS tallentaa välimuistiin vaihdetun sertifikaatin tiedot molempien osapuolien käyttöön. Tarkoituksena on vähentää sertifikaatin uudelleenvälittämistä asiakkaan ja autentikointipalvelimen kesken. EAP-TLS on protokolla, jonka avulla voidaan käyttää myös työasemakohtaista tunnistusta, jossa työasemalle on jaettu oma sertifikaatti tätä tarkoitusta silmälläpitäen. Tämä menetelmä mahdollistaa myös työaseman liittämisen verkkoon ennalta määriteltyyn VLAN:iin ilman käyttäjän identifiointia. Tämänkaltainen tietokonetilien käyttö edellyttää työasemakohtaisen sertifikaatin jakelua ennen autentikointipro-

sessia, joka on EAP-TLS-menetelmän heikoin kohta. On myös olemassa käyttöjärjestelmäympäristöjä, joissa on mahdollista myös automatisoida työasemakohtainen sertifikaatin jakelu. Kyseisen menetelmän käyttö on riippuvainen jakeluun liittyvien asetusten asettamisesta etukäteen sekä autentikointipalvelimeen että asiakaskoneeseen. (Microsoft 2003.)

EAP-TLS autentikoinnin vaiheet on esitetty seuraavassa ja havainnollisemmin kuviossa 9 sivulla 30.

1. Kytkin havaitsee uuden työaseman verkossa ja lähettää sille EAP-Request/Identity-viestin. Vaihtoehtoisesti työasema voi halutessaan liittyä verkkoon lähettämällä kytkimelle EAP-Start-viestin, jolloin kytkin vastaa lähettämällä EAP-Request/Identity-viestin työasemalle.

2. Työasema lähettää kytkimelle EAP-Response/Identity-viestin joka sisältää käyttäjätunnuksen tai työaseman nimen. Kytkin välittää viestin eteenpäin RADIUS-palvelimelle muodostaen siitä RADIUS Access-Request-viestin.

3. RADIUS-palvelin lähettää RADIUS Access-Challenge-viestin, joka sisältää Start-EAP-TLS-pyynnön. Kytkin välittää EAP-viestin työasemalle.

4. Työasema lähettää EAP-Response-viestin, jossa se ilmoittaa EAP-tyypin asetetuksi EAP-TLS-muotoon, joka ilmenee TLS-Client-Hello-viestinä. Kytkin välittää viestin eteenpäin RADIUS-palvelimelle.

5. RADIUS-palvelin lähettää RADIUS Access-Challenge-viestin, jonka EAP-tyyppi on EAP-TLS sisältäen RADIUS-palvelimen sertifikaatin. Kytkin välittää EAP-viestin työasemalle.

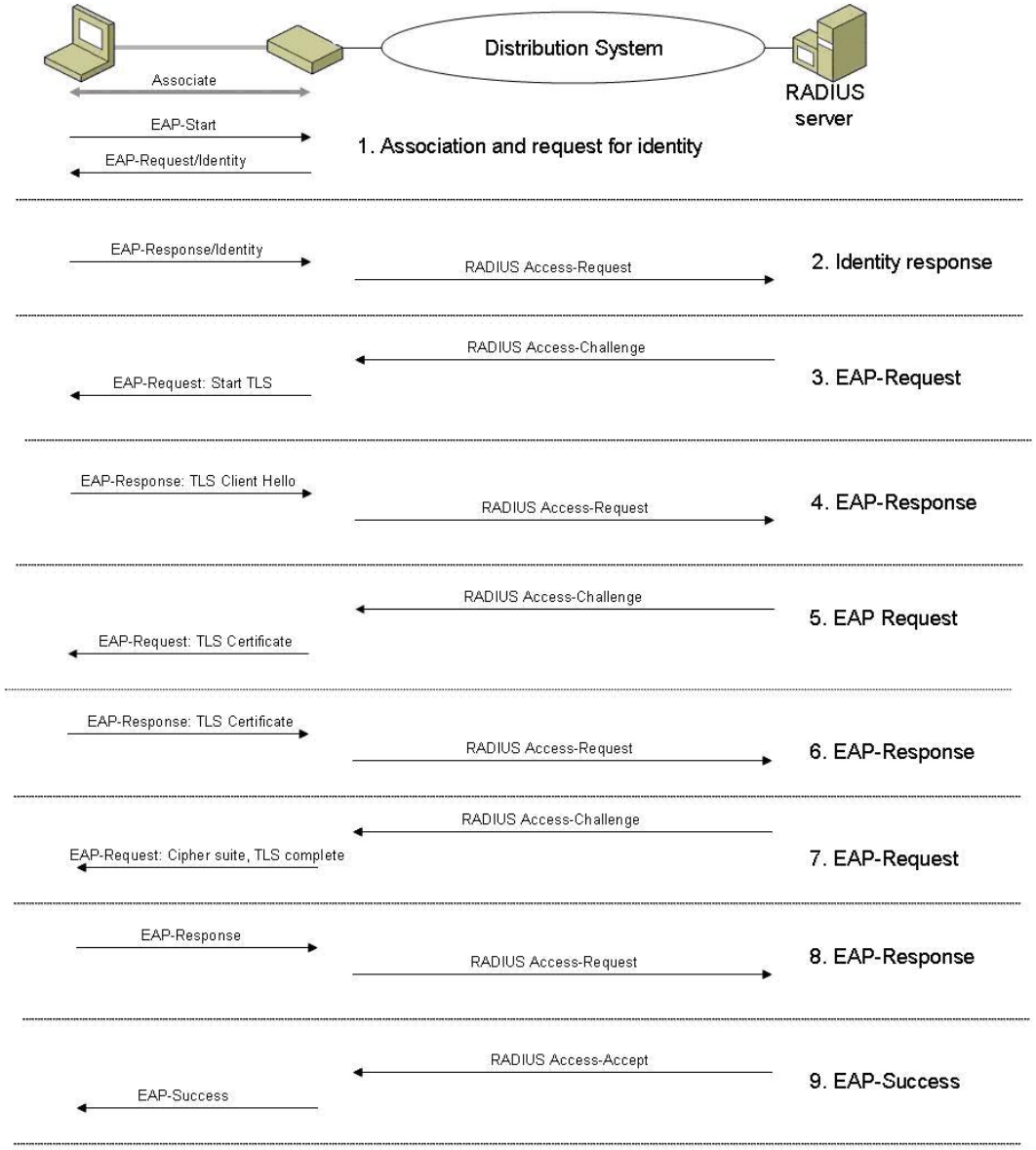
6. Työasema lähettää EAP-Response-viestin, jonka EAP-tyyppi on EAP-TLS sisältäen työaseman asiakassertifikaatin. Kytkin välittää EAP-viestin RADIUS-palvelimelle.

7. RADIUS-palvelin lähettää EAP-Request-viestin, jonka EAP-tyyppi on EAP-TLS sisältäen käytettävän salauksen tyypin ja tiedon siitä, että TLS-autentikointi on päättynyt. Kytkin välittää EAP-viestin työasemalle.

8. Työasema vastaa EAP-Response-viestillä, jonka EAP-tyyppi on EAP-TLS. Kytkin välittää EAP-viestin RADIUS-palvelimelle.

9. RADIUS-palvelin laskee asiakaskohtaiset istunto- ja vastaanottoavaimet, jotka on laskettu EAP-TLS-autentikoinnin perusteella. RADIUS-palvelin lähettää kytkimelle RADIUS Access-Accept-viestin sisältäen EAP-Success-viestin ja MPPE-avainattribuutit. Kytkin käyttää salattua MS-MPPE-Send-Key-attribuuttia salattaessa datasiirtoa kytkimeltä työasemalle, ja toiseen suuntaan kytkin käyttää salattua MS-MPPE-Recv-Key-atribuuttia allekirjoitusavaimena työasemalta saapuville paketeille.

Työasema laskee samat asiakaskohtaiset MPPE-avainattribuutit EAP-TLS-autentikointiprosessin perusteella, jolloin kytkimellä ja työasemalla on käytössään samat asiakaskohtaiset avaimet allekirjoitukseen ja salaukseen. Kytkin välittää EAP-Success-viestin työasemalle. EAP-TLS-autentikoinnin kulku on esitetty kuviosssa 9. (Microsoft 2007, 12-13.)



KUVIO 9. EAP-TLS-autentikointi prosessi. (Microsoft 2007, 14.)

4.7 EAP-TTLS

EAP-TTLS on laajennus EAP-TLS-protokollaan ja se laajentaa autentikointia ottamalla käyttöön TLS-kättelyn lisäinformaation lähettämiseksi asiakkaan ja autentikointipalvelimen välillä. TLS-kättelyn muodostaminen voi olla yksisuuntaista, missä vain palvelimen aitous varmistetaan asiakkaalle, tai kaksisuuntaista jossa molemmat osapuolet varmistavat toisensa, ja asiakkaan todentaminen voidaan varmistaa RADIUS-palvelimen avulla. Asiakkaan todentaminen voidaan välittää PPP-, CHAP-, MS-CHAP- tai MS-CHAPv2-protokollaa käyttäen. Vaikka todentamiseen käytetään näitä suojaustasoltaan heikkotasoisia protokollia, EAP-TTLS sallii käyttäjän tunnistamiseen turvallisemmin, koska se suojaa protokollien heikkoudet verkon salakuuntelua ja lähetettyjen pakettien kaappausyrityksiä vastaan. Yhteyden turvaaminen on kaksivaiheinen, joka perustuu TLS-tunnelin luomiseen ja sen jälkeen tekstimuotoisten attribuutti-arvoparien vaihtamiseen asiakkaan ja palvelimen kesken. Tämä mahdollistaa salausavainten vaihdon ja autentikoinnin, joka perustuu EAP-protokollaan ja on yhteensopiva AAA-käytäntöjen kanssa. (PPPEXT Working Group 2002, 1-3.)

EAP-TTLS-yhteyden muodostaminen alkaa asiakkaan aloitteesta, jossa TTLS-palvelin autentikoidaan TLS-kättelyssä asiakaskoneelle, kun asiakas lähettää EAP-response/Identity-paketin palvelimelle. Lähetetty paketti ei saa sisältää autentikoitavan käyttäjän nimeä, vaan se voi sisältää luotetun palvelimen domain tunnisteen, jonne EAP-TTLS-paketit on tarkoitettu lähetettäväksi. TTLS-palvelin vastaa asiakkaan lähettämään pakettiin EAP-TTLS/Start-paketilla, joka on EAP-request ja muotoa EAP-TTLS ja sisältää start-bitin mutta ei varsinaista dataa. Tämän paketin tarkoituksena on pyytää asiakasta aloittamaan TLS-kättely lähettämällä ClientHello-viesti. TTLS-palvelin vastaa viestiin lähettämällä EAP-Request/AccessChallenge-viestin, joka sisältää myös palvelimen sertifikaatin. Tätä sertifikaattia käytetään yhdessä yksityisen avaimen kanssa vahvistamaan kättelyn osapuolet toisilleen. TLS-kättelyn päätyttyä siirrytään tunnistamisen toiseen vaiheeseen jossa TLS-Record Layer-protokollaa käytetään suojaamaan viestien vaihtoa asiakkaan ja TTLS-palvelimen välillä. Asiakas aloittaa informaation

vaihdon enkapsuloimalla viestit attribuuttipari-jaksoihin ja siirtämällä ne TLS-Record Layerille salattavaksi, minkä jälkeen ne lähetetään TTLS-palvelimelle. TTLS purkaa salatun informaaation selväkieliseksi ja mikäli se sisältää autentikointi- informaatiota, se siirretään AAA-palvelimelle. Usein TTLS- ja AAA-palvelin ovat yksi ja sama palvelin, mikä yksinkertaistaa prosessia. Viestien vaihto jatkuu kunnes TTLS-palvelimella on riittävästi tietoa hyväksyä tai hylätä asiakkaan todentamispyyntö. TTLS-palvelin lähettää siirtoyhteyden vaatimat avainten vaihtotiedot ja muun autentikointi-informaation välittäjänä toimineelle verkon kytkimelle samassa AAA-viestissä, mikä sisältää EAP-Success-tiedon asiakkaalle. (PPPEXT Working Group 2002, 12-13.)

4.8 EAP-PEAP

EAP-PEAP on suunniteltu osittain korvaamaan EAP-TLS-menetelmää. PEAP käyttää alkuvaiheessa TLS-kättelyä ja tunnelointia, joka on EAP-TTLS:n kanssa identtinen. Toisessa vaiheessa suojatun EAP-TLS-tunnelin muodostamisen jälkeen, kun RADIUS-palvelin on autentikoinut itsensä asiakkaalle, ja molemmat ovat vahvistaneet allekirjoitusavaimet, siirrytään käyttämään MSCHAPv2-protokollaa. Tässä vaiheessa on saavutettu TLS-RecordLayer-suoja yhteyden välille, joten yhteys ei ole alttiina tavanomaisille käyttäjän tietojen murtoyrityksille. (Microsoft 2003.)

Seuraavassa on esitetty PEAP yhteyden muodostaminen. ja havainnollisemmin kuviossa 10 sivulla 34.

1. Kytkin havaitsee uuden työaseman verkossa ja lähettää sille EAP-Request/Identity-viestin. Vaihtoehtoisesti työasema voi halutessaan liittyä verkkoon lähettämällä kytkimelle EAP-Start-viestin, jolloin kytkin vastaa lähettämällä EAP-Request/Identity-viestin työasemalle.

2. Työasema lähettää kytkimelle EAP-Response/Identity-viestin joka sisältää käyttäjätunnuksen tai työaseman nimen. Kytkin välittää EAP-Response/Identity-viestin eteenpäin RADIUS-palvelimelle muodostaen siitä RADIUS Access-Request-viestin.

3. RADIUS-palvelin lähettää RADIUS Access-Challenge-viestin, joka sisältää Start-PEAP-pyynnön. Kytkin välittää EAP-viestin työasemalle.

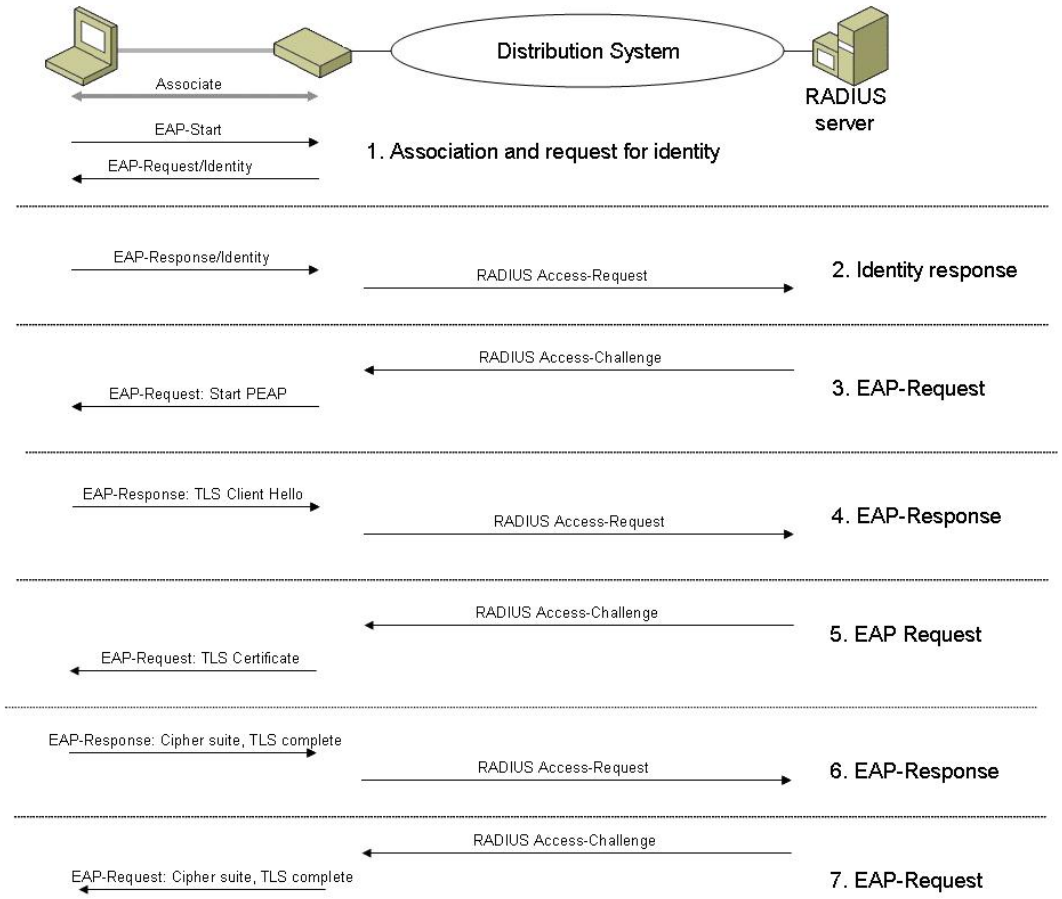
4. Työasema vastaa EAP-Response/TLS-Client-Hello-viestillä, jonka kytkin välittää RADIUS-palvelimelle.

5. RADIUS-palvelin lähettää RADIUS Access-Challenge-viestin jonka tyyppi on EAP-Request/PEAP ja joka sisältää palvelinsertifikaatin. Kytkin välittää EAP-viestin työasemalle.

6. Työasema vastaa EAP-Response/PEAP-viestillä, jossa kerrotaan käytettävän salauksen tyyppi sekä tieto TLS-salatun kanavan käyttöönotosta. Kytkin välittää viestin RADIUS-palvelimelle.

7. RADIUS-palvelin vastaa EAP-Request/PEAP-viestillä, jossa kerrotaan käytettävän salauksen tyyppi sekä tieto TLS-salatun kanavan käyttöönotosta. Kytkin välittää EAP-viestin työasemalle

EAP-TLS-salattu kanava on nyt käytössä ja voidaan jatkaa MS-CHAPv2-autentikoinnilla, jossa työasema autentikoidaan verkkoon. PEAP-autentikonnin kulku on esitetty kuviossa 10. (Microsoft 2007, 15-16.)



KUVIO 10. PEAP autentikointi prosessi (Microsoft 2007, 17.)

4.9 MS-CHAPv2

MS-CHAPv2 on salasanan vaihtoon perustuva haaste/vastaus-protokolla, joka mahdollistaa kaksisuuntaisen todentamisen. Se perustuu yleisesti käytettyyn standardiin, jossa viestit salataan Message Digest 4 (MD4) ja Data Encryption Standard (DES) salaus-algoritmeihin perustuvilla metodeilla. Kyseisessä metodissa autentikointipalvelin haastaa asiakkaan vastaamaan palvelimen lähettämiin haasteviesteihin. Mikäli haasteeseen ei saada todentamisen kannalta oikeata vastausta, niin palvelin hylkää asiakkaan autentikoinnin. MS-CHAP-protokolla tarjoaa aikaisempiin PPP-protokollaan perustuviin Challenge/Response-menettelyä käyttäviin protokolliin verrattuna paremman suojan mutta on silti alttiina sanakirjahyökkäyksiin perustuville murtoyrityksille. Tämä yleisesti tiedossa oleva heikkous on vältettävissä käytettäessä yhdistettyä PEAP/MS-CHAPv2-metodia, jossa

viestiliikenne on salattua perustuen salaukseltaan vahvaksi tunnettuun TLS-tunneliin. (Microsoft 2007, 15.)

Seuraavassa on esitetty MS-CHAPv2 yhteyden muodostaminen ja havainnollisemmin kuviossa 11 sivulla 36.

1. RADIUS-palvelin lähettää EAP-Request/Identity-viestin kytkimelle. Kytkin välittää EAP-viestin työasemalle.

2. Työasema vastaa EAP-Response/Identity-viestillä, joka sisältää käyttäjän tai työaseman nimen. Kytkin välittää viestin RADIUS-palvelimelle RADIUS Access-Request-viestin muodossa.

3. RADIUS-palvelin lähettää EAP-Request/EAP-MS-CHAPv2-viestin työasemalle, joka sisältää Challenge-viestin. Kytkin välittää EAP-viestin työasemalle.

4. Työasema lähettää vastauksen palvelimen Challenge-viestiin ja lähettää oman MS-CHAPv2-Challenge-viestin RADIUS-palvelimelle. Kytkin välittää viestin RADIUS-palvelimelle.

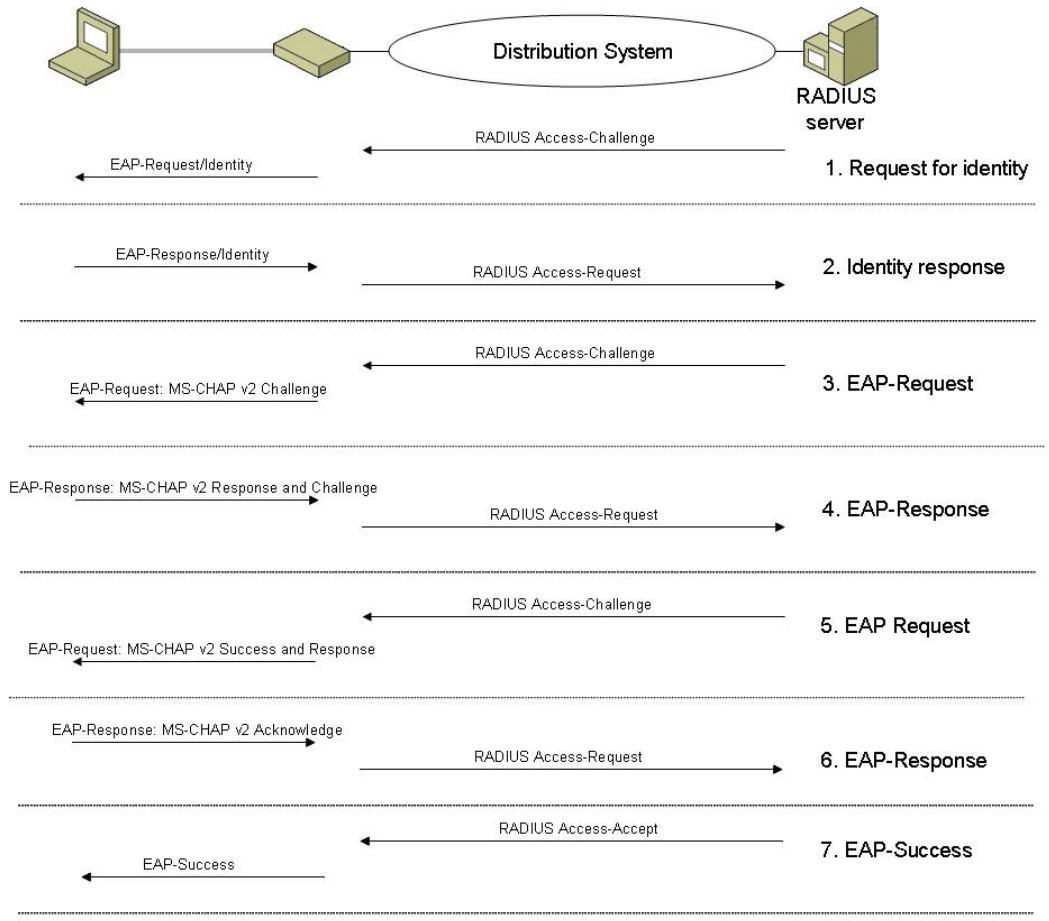
5. RADIUS-palvelin lähettää EAP-Request/MS-CHAPv2-Success-viestin, joka on vastaus työaseman lähettämään haasteeseen sekä ilmoituksen hyväksytystä vastauksesta RADIUS-palvelimen työasemalle lähettämään Challenge-viestiin.

6. Työasema lähettää EAP-Response/MS-CHAPv2-Acknowledge-viestin jossa ilmoitetaan työaseman hyväksyneen palvelimen vastauksen. Kytkin välittää viestin RADIUS-palvelimelle.

7. RADIUS-palvelin laskee asiakaskohtaiset istunto- ja vastaanottoavaimet, jotka on laskettu PEAP-autentikoinnin perusteella. RADIUS-palvelin lähettää EAP-Success-viestin sekä MS-MPPE-Send-Key- ja MS-MPPE-Recv-Key-attribuutit kytkimelle. Kytkin käyttää MS-MPPE-Send-Key-attribuutin salausavaimia asiakaskohtaisissa istun-

noissa datasiirrossa palvelimelle. Kytkin käyttää salattua MS-MPPE-Recv-Key-attribuuttia allekirjoitusavaimena datasiirrossa työasemalle.

Työasema laskee samat asiakaskohtaiset istunto avaimet (MS-MPPE-Send-Key ja MS-MPPE-Recv-Key) PEAP-autentikonti prosessin perusteella, jolloin kytkimellä ja työasemalla on käytössään samat asiakaskohtaiset avaimet allekirjoitukseen ja salaukseen. Kytkin välittää EAP-Success-viestin työasemalle, jossa kerrotaan avaimien käyttöönotosta. MS-CHAPv2 autentikoinnin kulku on esitetty kuviossa 11. (Microsoft 2007, 17-18.)



KUVIO 11. MS-CHAPv2-autentikointi prosessi (Microsoft 2007, 20.)

Tähän kappaleeseen päättyvässä opinnäytetyön teoriaosuudessa on käyty läpi 802.1x-autentikointiin liittyviä ja siihen tietoturvan näkökulmasta oleellisesti liittyviä seikkoja. Tarkoituksena on ollut painottaa laajassa käytössä olevan Ethernet-

tekniikan ominaisuuksia ja siihen liittyviä laajennuksia, jotka ovat saavuttaneet myös standardisoinnin asteen. Vahvaan autentikointiin perustuvia tekniikkaa ja protokollia on kehitetty jo pidemmän aikaa vaihtelevin tuloksin, mutta aina yhtä optimistisesti. Laitetekniikan kehitys ja sen suora vaikutus verkkolaitteiden kustannuksiin on osaltaan auttanut suotuisasti turvallisempien lähiverkkojen rakentamiseen. RADIUS-palvelimien käyttö on lisääntymässä, koska lähiverkkojen turvallisuus saa niiden ylläpitäjät hakemaan yhä parempaa suojaa lähiverkon väärinkäytöksiltä.

5 KÄYTÄNNÖN TOTEUTUS

5.1 Testiympäristön kuvaus

Testauksen tarkoituksena oli simuloida lähiverkkoon kytkettyjen tietokoneiden suojattu autentikointi lähiverkon palveluihin 802.1x-ja RADIUS-protokollia käyttäen. Testaukseen valittiin yleisemmin käytetyt ja tietoturvatasoltaan vahvimmat RADIUS-protokollat EAP-PEAP ja EAP-TLS. Testiympäristö koostui Linux ja Windows-palvelimiin asennetuista RADIUS-palvelimista sekä lähiverkon kytkimestä (NAS) ja Windows-työasemista. Ensimmäiseksi asennettiin palvelimet toimintakuntoon ja testattiin EAP-PEAP-autentikontia. Toisessa vaiheessa testattiin EAP-TLS-autentikointia, joka ei vaadi suuria muutoksia EAP-PEAP-protokollan vaatimiin asetuksiin. Testiympäristön kokoonpanossa käytettiin vain yhden valmistajan kytkintuotetta, ja työasemissa käytettiin vain Windows-käyttöjärjestelmiä. Vastaavilla ominaisuuksilla varustettuja kytkimiä on myös muilta laitevalmistajilla ja käyttöjärjestelmäpuolelta löytyvät vahvimmat ehdokkaat Linux-jakeluista, joille on olemassa kaupallisia 802.1X-asiakasohjelmistoja. Maksuttomasta Open 802.1X-clientistä on Linuxille toistaiseksi olemassa vain komentorivi pohjainen versio. AEGIS Linux Client on siirtynyt Cisco System:in omistukseen ja tuote on vaihtanut nimeä, eikä sitä ole tällä hetkellä saatavana kuin Windows-järjestelmille. Juniperilla on olemassa Odysseys Linux-Client-ohjelmisto, mutta sen sopivuudesta yleisellä tasolla eri Linux-jakeluille ei ole tarkempaa tietoa

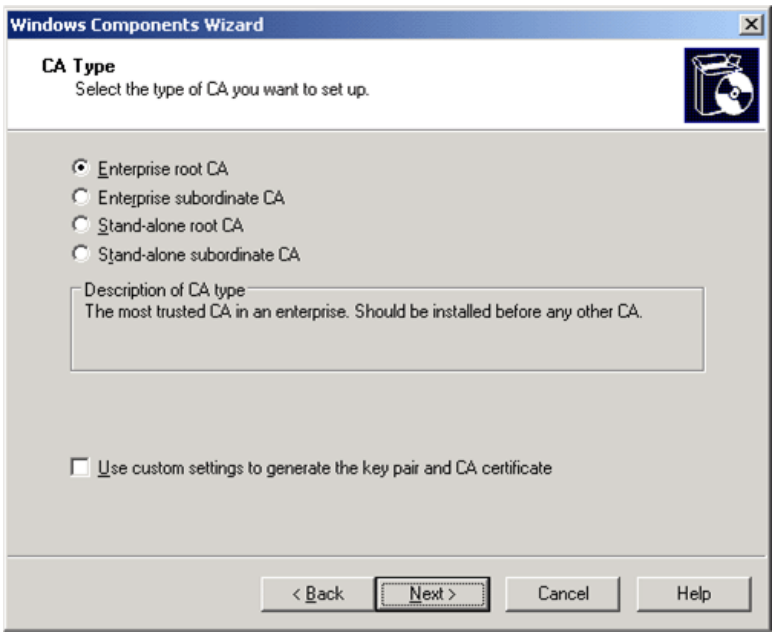
5.2 Internet Authentication Service (IAS)

Microsoft IAS on Windows-palvelinympäristöön suunniteltu RADIUS-palvelin, ja se voi myös toimia välityspalvelimena välittämällä käyttäjien autentikoinnin muille RADIUS-palvelimille. IAS on joustava, erilaisiin verkkomedioihin sopiva AAA-palvelin, joka mahdollistaa käyttäjien keskitetyn hallinnan. IAS-palvelimen

toteutus tehtiin yhteen serveriin, joten Windows Server perheestä oli vaihtoehtoina joko Enterprise Edition- tai Media Server-versio. Vaatimukset perustuvat sertifikaattipalvelimen (CA-Authority) toimintaan. Työssä käytettiin Windows 2003 Enterprise Edition -palvelinversiota. IAS-asennuksen vaatimat tarkemmat yksityiskohdat on esitetty liitteessä 4, joten tässä luvussa asiat käydään läpi vain tärkeimmiltä pääkohdiltaan.

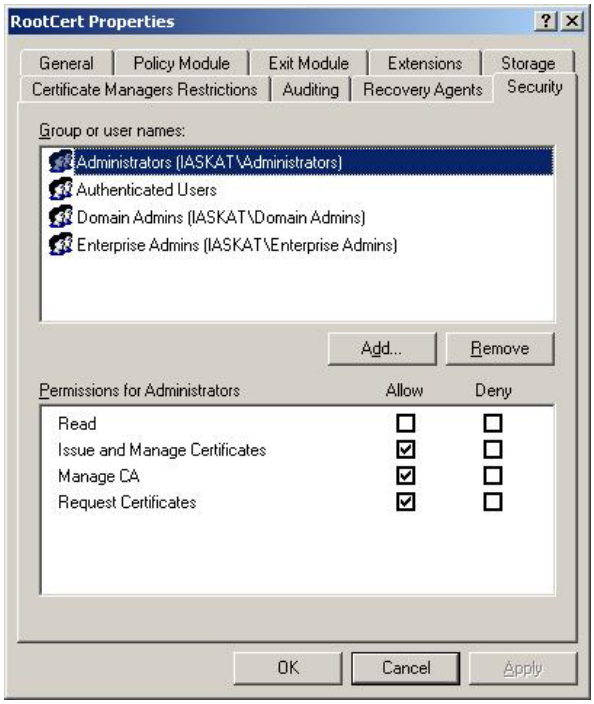
Palvelimeen asennetaan DNS-palvelin ja AD-hakemistopalvelut, jotka ovat riippuvaisia DNS:n olemassaolosta. Lisäksi asennetaan IIS ja Certificate Services, joka puolestaan on riippuvanen IIS:n ASP-koodien suorittamisesta, joita tarvitaan sertifikaattien luomisprosessissa. Palvelimen verkkokortille määritellään kiinteä IP-osoite, koska DNS-palvelin vaatii asentuakseen IP-osoiteen. Lopuksi asennetaan IAS-palvelin ja määritellään tarvittavat konfiguraatiot. Asennukseen löytyy useampikin ohjeistus, mutta niitä täytyy käyttää hieman soveltaen, koska niissä käytetään usein useampaa palvelinta, joille eri palvelut jaetaan.

Palvelimen asennus aloitetaan asentamalla peruskomponentit. Asennusta jatketaan käynnistämällä Active Directory-asennus dcpromo-komennolla ja valitaan lisäksi myös asennusvelhon tarjoama DNS-palvelimen asennus. Seuraavaksi on muutettava AD:n toiminnallisuus vastaamaan palvelinversiota, eli korotettiin palvelin Active Directory 2003 tasolle, tämän jälkeen AD on (natiivi-modessa) joka mahdollistaa laajemmat ryhmäkäytännöt. Myös DHCP-palvelin asennettiin, mutta sitä ei käytetty koska käytössä ei ollut reititintä. Tämä siksi koska VLAN-verkoissa eri VLAN:ien välillä vaaditaan reititys eri IP-aliverkkojen valille. Seuraavaksi asennetaan palvelimeen IIS-palvelin sekä Certificate Services eli sertifikaattipalvelut, jotka vaaditaan IAS-todennuksen tarvitsemien sertifikaattien luomiseen. Sertifikaattipalvelimen asennuksessa on valittava asennettava CA-tyyppi, joka tässä tapauksessa oli Enterprise root CA. Lisäksi valittiin sertifikaatin voimassaoloaika, joka hyväksyttiin oletusasetuksin 5 vuodeksi. Hyväksyttiin juurisertifikaatin oletusnimi ja säilytyskansio. CA-tyypin valinta on esitetty kuviossa 12.



KUVIO 12. CA-tyypin valinta.

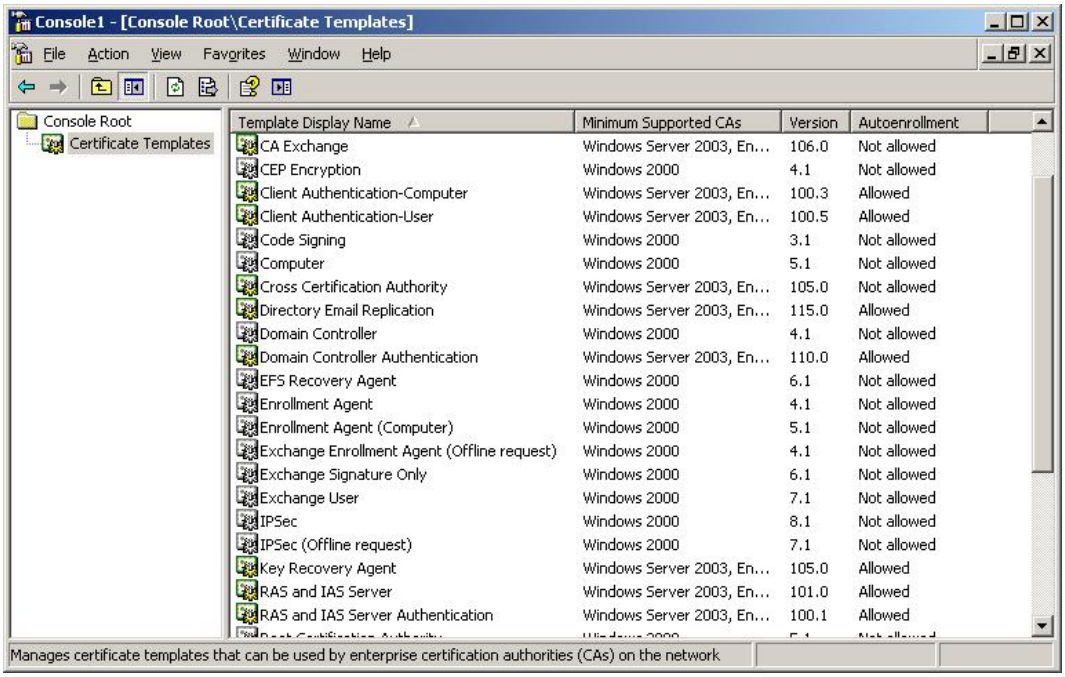
Varmistetaan, että Administrator-ryhmällä on oikeus hyväksyä ja hallita sertifikaatteja, hallita CA:ta ja oikeus anoa sertifikaatteja. Juurisertifikaatin käyttöoikeudet on esitetty kuviossa 13.



KUVIO 13. Juurisertifikaatin oikeudet.

Seuraavaksi asennetaan IAS-palvelin ja rekisteröidään se Active Directoryyn. Koko palvelinasennuksen viimeistelemiseksi on suositeltavaa asentaa Windows Server Service Pack:sta uusin versio sekä uusimmat tietoturvapäivitykset. Palvelimen uudelleen käynnistyksen jälkeen on syytä tarkistaa AD:n ja DNS-palvelimien toiminta tapahtumalokeista. Mikäli lokeista löytyy virheitä on syytä tarkistaa asennuksen eri vaiheet uudelleen ja varmistaa jo tehdyt konfiguroinnit.

EAP-TLS ja EAP-PEAP-todentamiseen vaadittavat sertifikaatit luodaan avaamalla MMC-työkalu, joka on avattava päävalikosta Add/Remove-snap-in sertifikaattipohjien lisäämiseksi ja muokkaamiseksi käyttöön sopivaksi. Lisätään Certificate Templates-kansio ja suljetaan ikkuna. MMC-työkalun sertifikaatipohjat on esitetty kuviossa 14.

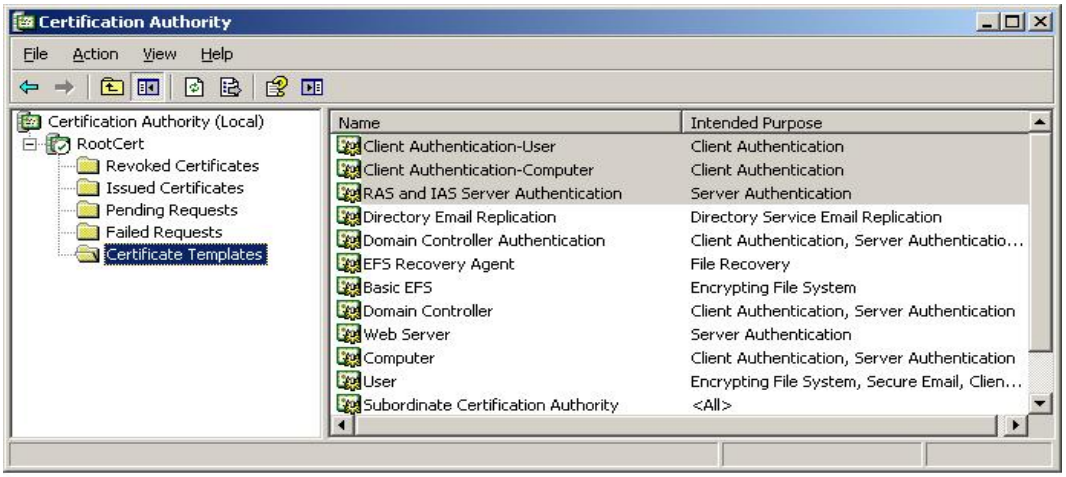


KUVIO 14. Sertifikaattipohjat

Luodaan ensimmäiseksi sertifikaattipohja palvelimen autentikointiin. Konsolin oikeanpuoleisessa Template Display Name -ikkunassa valitaan RAS and IAS Server -pohja ja luodaan siitä kopio Duplicate Template-valinnalla ja annetaan nimeksi RAS and IAS Server Authentication. Seuraavaksi luodaan sertifikaattipohja käyttäjien autentikointiin. Luodaan kopio Authenticated Session -pohjasta ja annetaan nimeksi Client Authentication-User. Viimeiseksi luodaan sertifikaattipohja

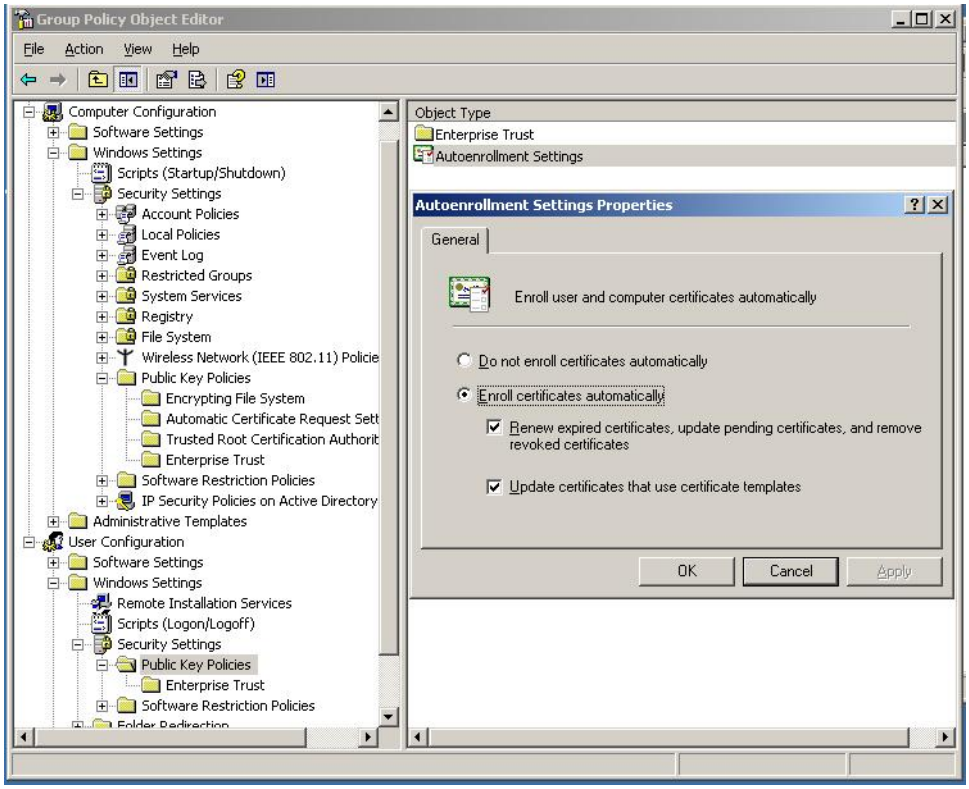
tietokoneiden autentikointiin. Luodaan kopio Workstation Authentication -pohjasta ja annetaan nimeksi Client Authentication-Computer. Sertifikaattien voimassaoloaikaa voidaan säädellä muuttamalla sertifikaattipohjassa olevaa oletusaikaa tarpeen mukaan. Sertifikaattikopioiden nimi oli vapaasti valittavissa, ja nimeämisessä käytettiin kuvaavaa nimeä, jotta ne ovat helposti tunnistettavissa.

Sertifikaattien allekirjoittaminen ja tuominen AD:n käyttöön tapahtuvat Certification Authority-työkalulla. Laajennetaan CA:n kansiot auki ja laajennetaan Certificate Templates ja valitaan juuri luodut sertifikaattipohjat. Hyväksytään ne CA:n allekirjoitettavaksi, ja minkä jälkeen uudet sertifikaatit ovat käytettävissä. CA ja allekirjoitettavat sertifikaatit on esitetty kuviossa 15.



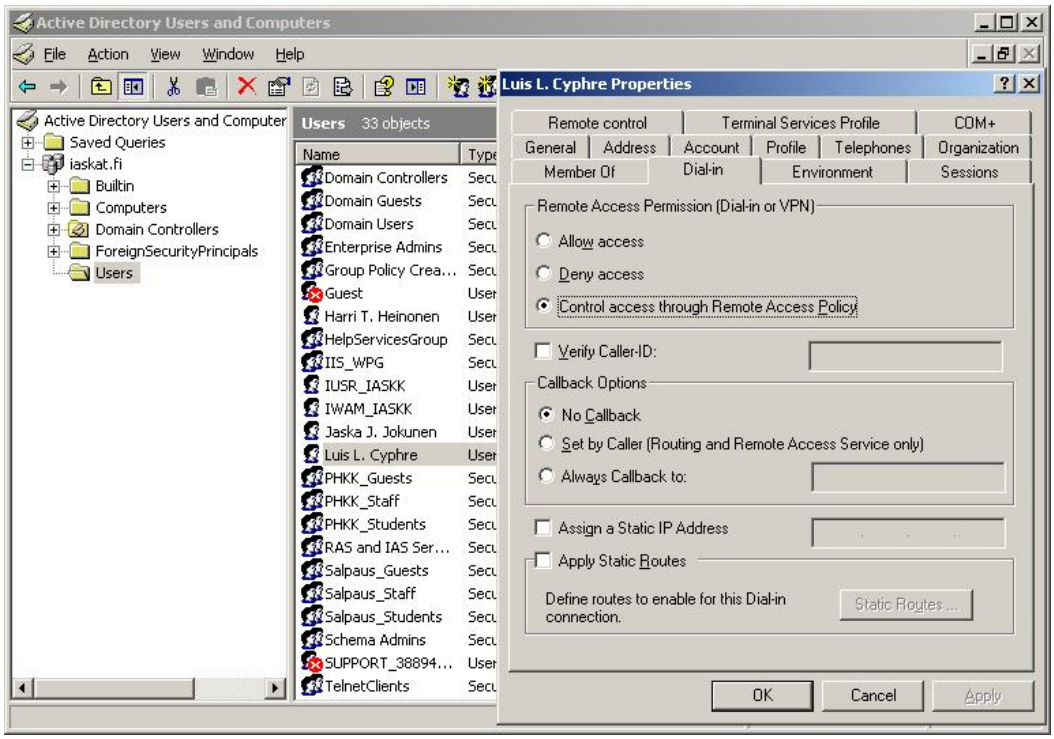
KUVIO 15. Certification Authority ja allekirjoitettavat sertifikaatit.

EAP-TLS on menetelmä, jossa käytetään sertifikaattia asiakkaiden todentamiseen, ja se vaatii myös lisämäärityksiä AD:lle automaattisen sertifikaattien jakelun osalta. Automaattinen jakelu perustuu Group Policy-määrityksiin, ja IAS-sertifikaattien jakelu voidaan määritellä Active Directory Users and Computers-työkalun kautta. Automaattinen jakelu täytyy lisätä samassa GP-editorissa myös käyttäjien Group Policy-asetuksiin. Automaatisen sertifikaattijakelun määritykset on esitetty kuviosssa 16.



KUVIO 16. GroupPolicy Object Editor ja automaattinen sertifikaatin jakelu.

Saadakseen käyttöön IAS:n tarjoamia verkkopalveluita, täytyy käyttäjillä ja tietokoneilla olla ryhmäjäsenyys sellaisesta ryhmästä, joilla on oikeus käyttää Remote Access-palveluita. Aluksi on luotava ryhmät, jotka vastaisivat todellista työskentely-ympäristöä. Olisi myös mahdollista luoda omia organisaatioyksikköjä lisäämällä ne suoraan domain-juureen, mutta tässä tapauksessa luotiin ryhmät olemassa olevaan organisaatiokansioon. Avataan Active Directory User and Computers-työkalu ja laajennetaan auki domain-kansion alla olevat kansiot. Luodaan uusi ryhmä users-kansioon ja annetaan ryhmälle sitä kuvaava nimi ja hyväksytään OK-painikkeella. Tarkoituksena oli testata RADIUS-palvelimen toimintaa eri EAP-protokollien kanssa, joten tätä varten luotiin useita ryhmiä eri tarkoituksiin. EAP-PEAP-protokolla, joka perustuu käyttäjä/salasana-todentamiseen, vaati myös muutaman koekäyttäjätunnuksen testausta varten. Lisäksi luotiin yksi ryhmä asiakas-koneiden liittämiseksi AD-toimialueelle ja sille luotettu käyttäjä. Lopuksi varmistettiin, että käyttäjillä on oikeudet päästä verkkoon Dial-in-palveluiden avulla. Dial-in-määritykset on esitetty kuviossa 17.

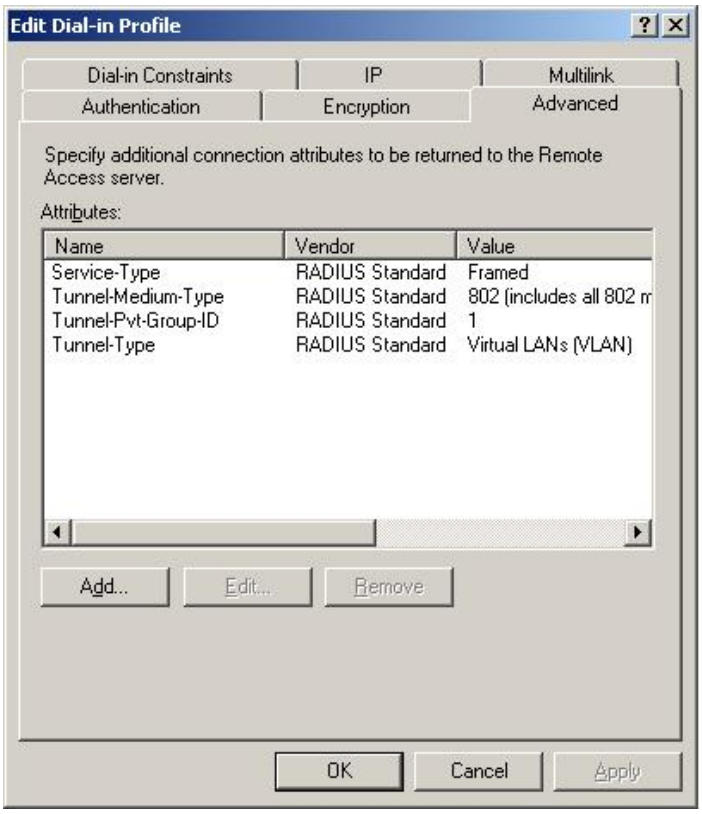


KUVIO 17. Käyttäjän Remote Access-oikeudet.

IAS:n konfigurointi aloitetaan lisäämällä välityspalvelijana toimiva kytkin (NAS), joka tässä tapauksessa on mallia Hewlett Packard 2524. Avataan Internet Authentication Services-työkalu ja lisätään uusi RADIUS Client. Annetaan laitetta kuvaava nimi ja IP-osoite, ja mikäli alasvetovalikosta löytyy laitteen valmistajan nimi, valitaan se. Mikäli ei laitevalmistajan nimeä löydy listalta, valitaan RADIUS Standard ja toivotaan, että laite on yhteensopiva RADIUS-standardin kanssa. Alempiin lomakekenttiin kirjoitetaan IAS-palvelimen ja NAS:n käyttämä yhteinen salasana ja vahvistetaan se.

Luodaan IAS:n Remote Access Policies-kansioon aikaisemmin luotuja käyttäjäryhmiä vastaavat verkon käyttöön oikeuttavat määritykset. Lisätään haluttu käyttäjäryhmä ja protokolla todentamiskäytännön mukaan. Mikäli halutaan todentaa asiakas käyttäjätunnus/salasana-menetelmällä, valitaan Protected EAP (PEAP), ja jos käytetään sertifikaattia, niin valitaan Smart Card or other certificate.

Luotu IAS Remote Access Policy tarvitsee vielä lisämäärityksiä, ennen kuin se on tarkoituksen mukaisesti toimiva. Valitaan luotu Remote Access Policy ja avataan se, lisätään aikarajoitukset ja varmistetaan myös, että Grant remote access permission on valittuna. Lisätään yhteyden kannalta tärkeät Service-Type, Tunnel-Medium-Type, Tunnel-Pvt-Group-ID ja Tunnel-Type-attribuutit. RADIUS-attribuutit on esitetty kuviossa 18.



KUVIO 18. IAS:n Remote Access Policy RADIUS-Attribuutit.

Kuviossa esitetty VLAN-ID eli Tunnel-PvtGroup-ID on tarkoitettu työasemien AD:alueelle liittämistä varten.

Luodaan Policyt jokaiselle ryhmälle, jolle on tarkoitus antaa pääsy verkkoon dynaamisten VLAN:ien kautta. Kaikkien luotujen Remote Access Policyjen salausavainmääritykset on tarkastettava, jotta ne käyttävät vahvinta mahdollista salausta. Kuviossa 18 esitetty Remote Access policy on tarkoitettu työasemien liittämiseen AD-toimialueelle. Tunnel-Pvt-Group-ID:n arvo on 1, mikä on useissa kytkimissä oletus eli Default-VLAN. Työssä käytetty IAS-palvelin oli kytketty oletus VLAN:iin.

5.3 AAA-kytkimen konfigurointi

Kytkimen konfigurointi vaati ensin yhteyden muodostamisen RS-232-kaapelin avulla, jotta kytkimeen saadaan määriteltyä IP-osoite. Tämän jälkeen kytkimeen saadaan yhteys verkon kautta ja RADIUS-asetusten määrittäminen on mahdollista myös IAS-palvelimelta. HP2524-kytkimessä on menu-pohjaiset ja www-selaimella hallittavat toiminnot, mutta ne ovat sen verran puutteelliset, että kummastakaan ei voi määritellä AAA-palvelun käyttöönottoa. Ainoa tapa määritellä koeympäristön vaatimat konfiguraatiot ovat komentoriviltä suoritettavat komennot. HP2500-sarjan kytkimien käyttö-oppaasta ei löytynyt tarvittavia komentoja, joten oli käytettävä seuraavan 2600-sarjan Access Security Guide for the ProCurve Switch 2600-opasta. Annettavien komentojen määrä ei ole suuri, jotta saadaan kytkimeen tarvittavat toiminnot. Kytkimen konfiguraatio on esitetty liitteessä 1.

Määritellään RADIUS-palvelimen IP-osoite ja käytettävä salasana-avain

radius-server host <IP-Osioite> key <käytettävä salasana>

Otetaan käyttöön AAA-autentikointi ja EAP-metodi.

aaa authentication port-access eap-radius

Aktivoidaan AAA-palvelu.

aaa port-access authenticator active

Lisätään AAA-palvelun valvottavat portit.

aaa port-access authenticator <ensimmäinen portti – viimeinen portti>

Lisätään vielä varotoimi tunkeilijoita ja murtautumisyrityksiä vastaan. Yhteyttä yrittävä asiakas liitetään autentikoinnin ajaksi VLAN:iin, joka eristää asiakkaan verkosta kunnes autentikointi on onnistunut tai epäonnistunut.

aaa port-access authenticator <valvottavat portit> unauth-vid <unauth VLAN>

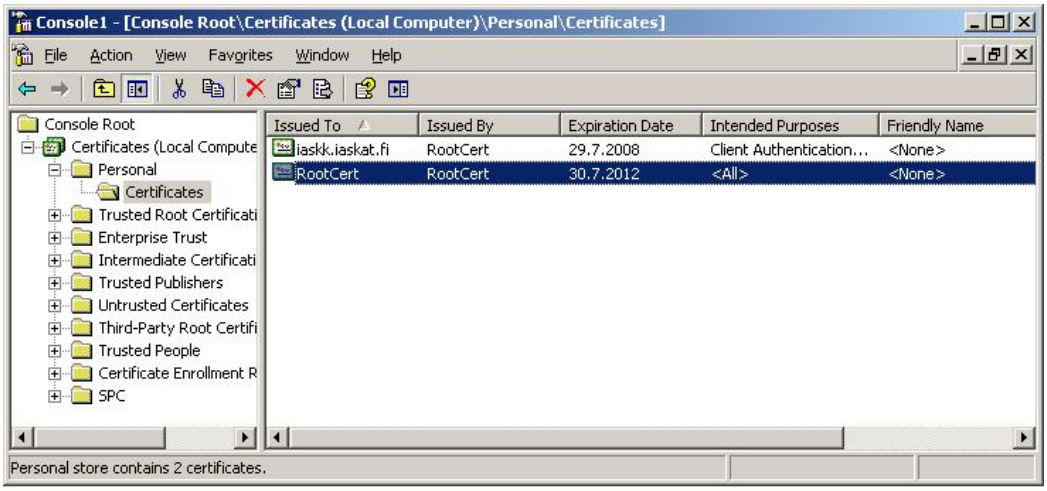
Kytkimeen on vielä määritettävä samat VLAN:it jotka määritettiin IAS-palvelimeen Remote Access Policies kohdassa. VLAN:it saadaan helposti määri-

teltyä kytkimeen menu-toimintoja käyttäen. VLAN-nimillä kytkimessä ei ole autentikointi prosessiin kannalta merkitystä, ainoastaan on 802.1Q VLAN-ID numerolla.

5.4 IAS-sertifikaattien jakelu työasemille

Sertifikaattien jakeluprosessi on tarkoituksenmukaista käydä läpi EAP-PEAP-todentamisen vaatimalla palvelinsertifikaatilla, koska työasemien liittäminen AD-toimialueelle tapahtuu PEAP-yhteyden avulla. Työaseman ollessa liitettynä AD-toimialueelle, Group Policy-määritykset hoitavat sertifikaattien jakelun automaattisesti niille työasemille, jotka kuuluvat sallittuun Remote Access ryhmään.

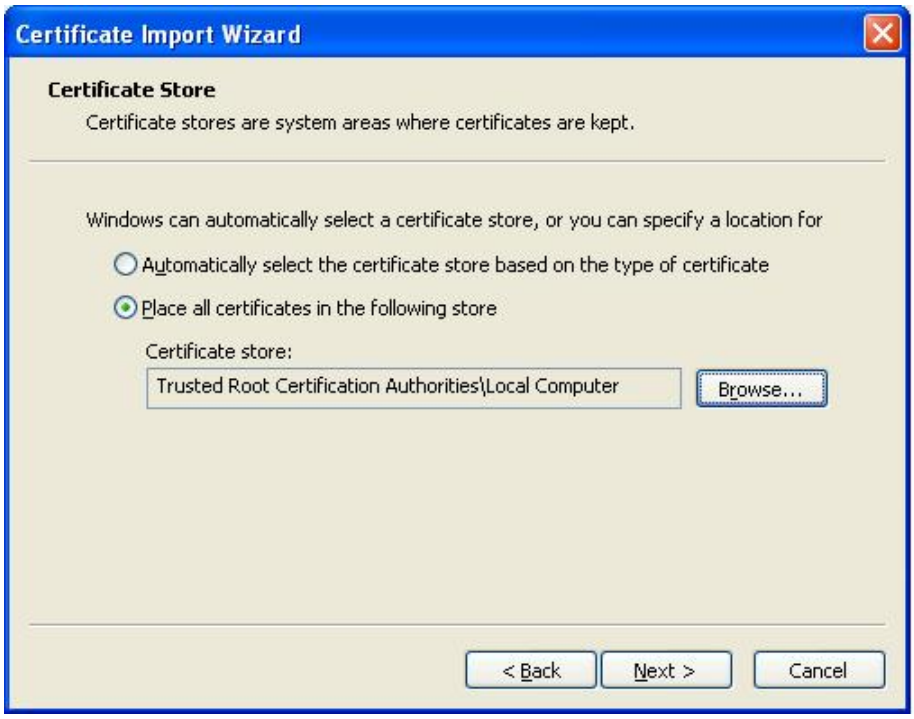
Sertifikaatin vienti on selitetty seuraavassa (Kuvio 19). Avataan MMC-työkalu ja ladataan Add/Remove Snap-in-ikkunan Local computer sertifikaatit. Konsolin vasemmasta ikkunasta valitaan Certificates-kohta ja valitaan sertifikaatti (Intended Purposes = All), joka tarkoittaa kaikkiin tarkoituksiin.



KUVIO 19. Sertifikaatin vienti MMC-konsolista.

Avataan sertifikaatti, valitaan export-toiminto, hyväksytään export the private key ja tallennusmuodoksi, valitaan PKCS #12(.PFX), kirjoitetaan salasana ja tallennetaan sertifikaatti sitä kuvaavalla nimellä. Siirretään sertifikaatti työasemalle jonkin tallennusmedian avulla.

Sertifikaatti tuodaan työasemalle avaamalla sertifikaatti kaksoisklikkaamalla siirtoon käytetyltä medialta ja valitaan tallennuskansioksi Trusted Root Certification Authorities\Local Computer. Sertifikaattisäilön valinta on esitetty kuviossa 20.

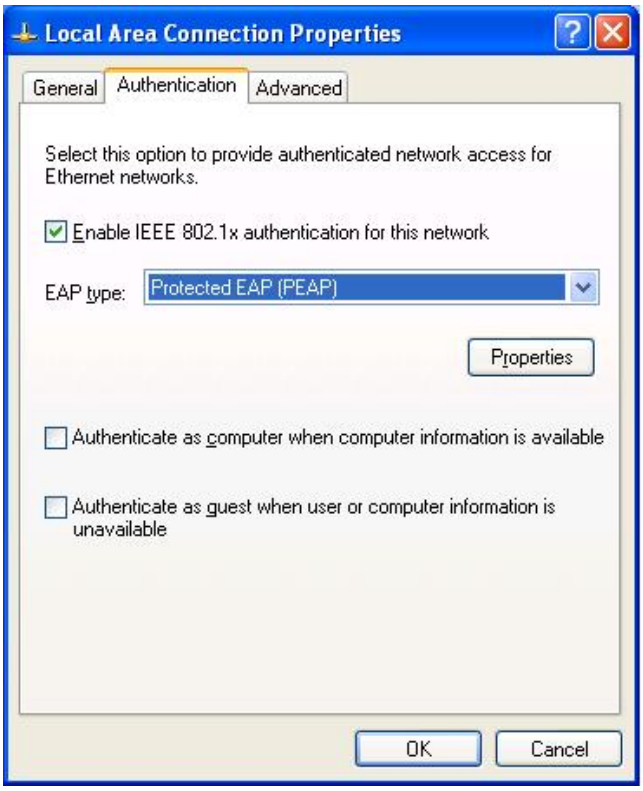


KUVIO 20. Sertifikaatin tallennus sertifikaattisäiliöön.

5.5 IAS PEAP-yhteyden muodostaminen

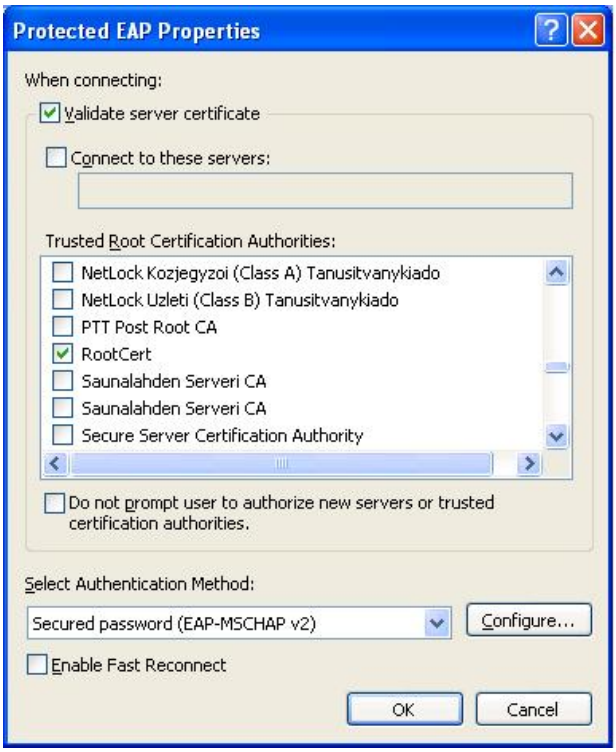
Yleisesti käytetyin asiakaskäyttöjärjestelmä RADIUS-yhteyden muodostamiseen on Windows 2000 tai Windows XP-työasema. Valmiudet 802.1X-yhteyden muodostamiseen vaativat Windows 2000-tasolla vähintään Service Pack 3:n ja Windows XP:ssa 802.1X-tuki on valmiina.

EAP-PEAP-yhteyden vaatimat asetukset tehdään Windows:n verkkoympäristössä käytössä olevan verkkoyhteyden Authentication-välilehdellä. Varmistetaan, että IEEE 802.1x todennus on otettu käyttöön, ja EAP tyyppi on Protected EAP. EAP-protokollan valinta on esitetty kuviossa 21.



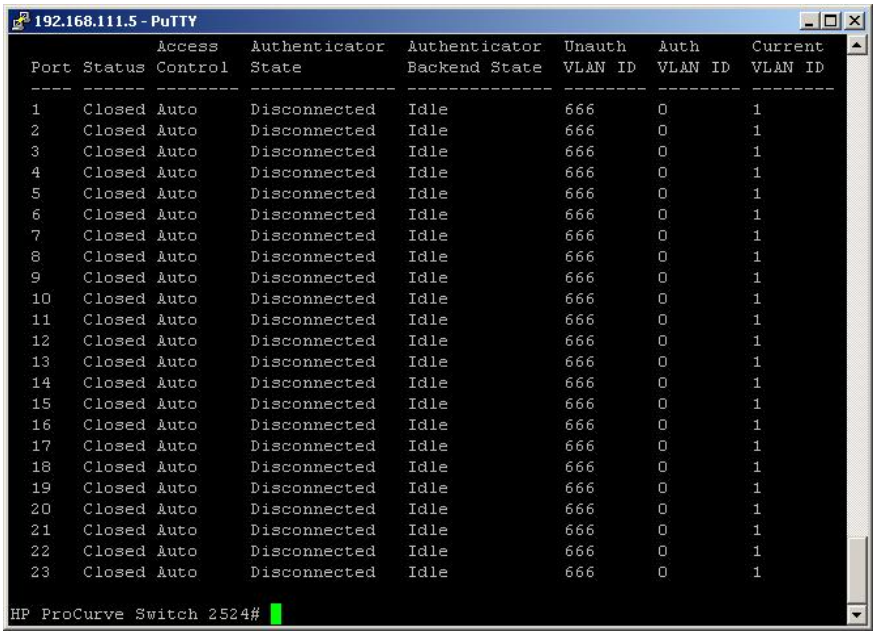
KUVIO 21. Lähiverkkoyhteyden Authentication-välilehti

Valitaan Properties-painike ja siirrytään PEAP:n lisäasetuksiin. Otetaan käyttöön Validate server certificate-vaihtoehto ja valitaan listasta työasemalle tuotu palvelinsertifikaatti. Tarkastetaan vielä, että käytössä on EAP-MSCHAPv2-metodi ja Configure-painikkella siirrytään EAP-MSCHAPv2-ominaisuuksiin, ja estetään työasemalle kirjautuneen käyttäjätunnuksen käyttö oletuksena PEAP-todennuksessa. PEAP-todennuksen lisäasetukset on esitetty kuviossa 22.



KUVIO 22. PEAP-lisäasetukset.

Yhteyden muodostamiseen tarvittavat asetukset on nyt määritetty. Asetetaan nykyinen verkkoyhteys Disable-tilaan ja kytketään verkkokaapeli kytkimeen. Otetaan IAS-palvelimelta telnet-yhteys kytkimeen (NAS) ja tarkastetaan porttien nykyinen tila. Kytkimen porttien tila on esitetty kuviossa 23.



KUVIO 23. Kytkimen porttien tila ennen autentikoinnin aloittamista.

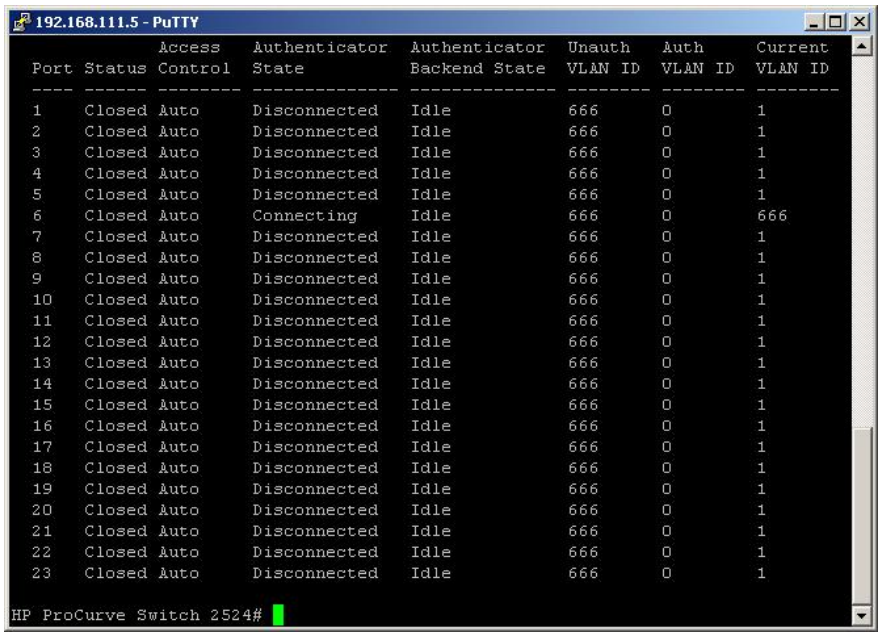
Vaihdetaan tietokoneen verkkoyhteys Enable-tilaan. Kytkimeen määritetystä säännöstä johtuen tietokone siirretään todentamisen ajaksi VLAN1:stä VLAN666:een, joka on kytkimeen määritelty unauthorized-vlan. Tietokoneen näytön oikeaan alanurkkaan ilmestyy huomautusikkuna, jota klikataan, jolloin avautuu dialogi-ikkuna, jossa pyydetään asiakkaan käyttäjätunnusta ja salasanaa, syötetään pyydetyt tiedot ja kuitataan OK-napilla. Dialogi-ikkuna on esitetty kuviossa 24.

KUVIO 24. Dialogi-ikkuna

Koska PEAP-verkkoyhteden määrityksissä valittiin Validatate server certificate-ruutu, esiin tulee ikkuna jossa pyydetään vahvistamaan RADIUS-palvelimen sertifikaatin hyväksyminen. Sertifikaatin hyväksyntä on esitetty kuviossa 25.

KUVIO 25. IAS RADIUS-palvelimen sertifikaatin hyväksyntä.

Tarkastetaan kytkimestä sen portin VLAN-tila, johon tietokone on kytketty. Portin pitäisi vaihtaa VLAN1:stä VLAN666:een autentikoinnin ajaksi. Kytkimen portin tila on esitetty kuviossa 26.



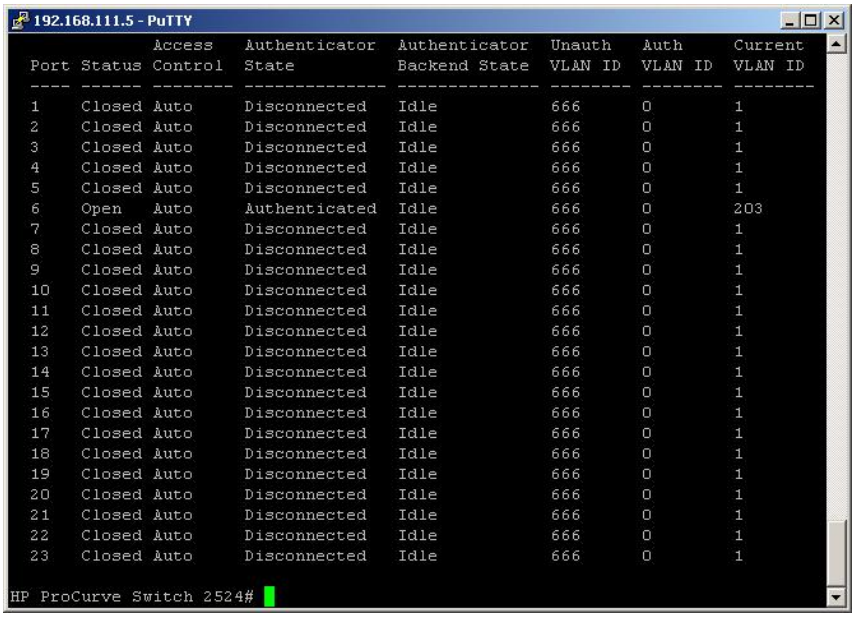
KUVIO 26. Kytkimen portin tila autentikointiprosessin aikana.

Asiakkaan PEAP-yhteyden muodostumisen tai hylkäämisen voi tarkastaa IAS-palvelimen järjestelmälokeista. Onnistunut todentaminen on esitetty kuviossa 27.

```
User luis was granted access.
Fully-Qualified-User-Name = iaskat.fi/Users/Luis L. Cyphre
NAS-IP-Address = 192.168.111.5
NAS-Identifier = HP ProCurve Switch 2524
Client-Friendly-Name = HP_ProCurve2524
Client-IP-Address = 192.168.111.5
Calling-Station-Identifier = 00-c0-9f-4c-a1-06
NAS-Port-Type = Ethernet
NAS-Port = 12
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = PHKK_Guests
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)
```

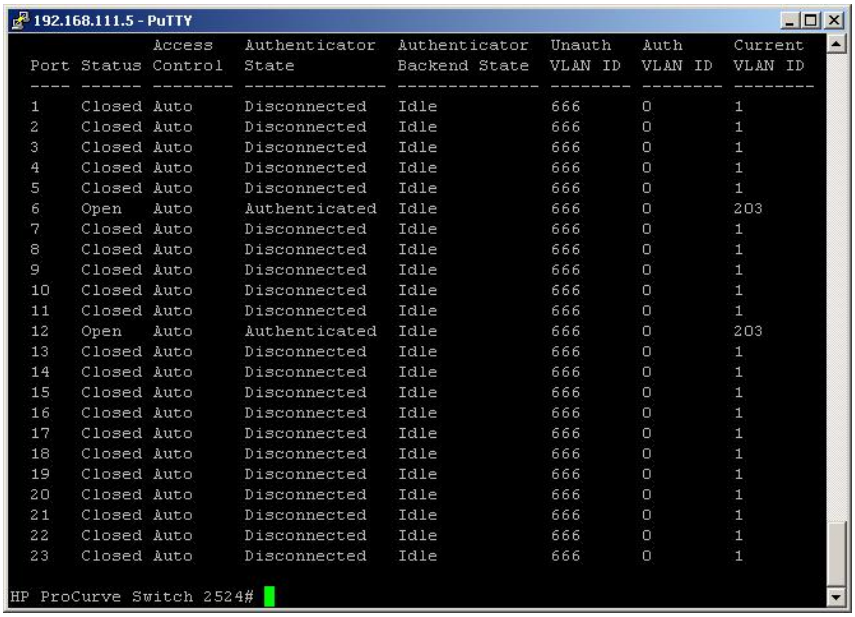
KUVIO 27. Tekstituloste järjestelmälokista.

Vahvistetaan kytkimen toiminta IAS-palvelimen kanssa. Kytkimen portin tila on esitetty kuviossa 28.



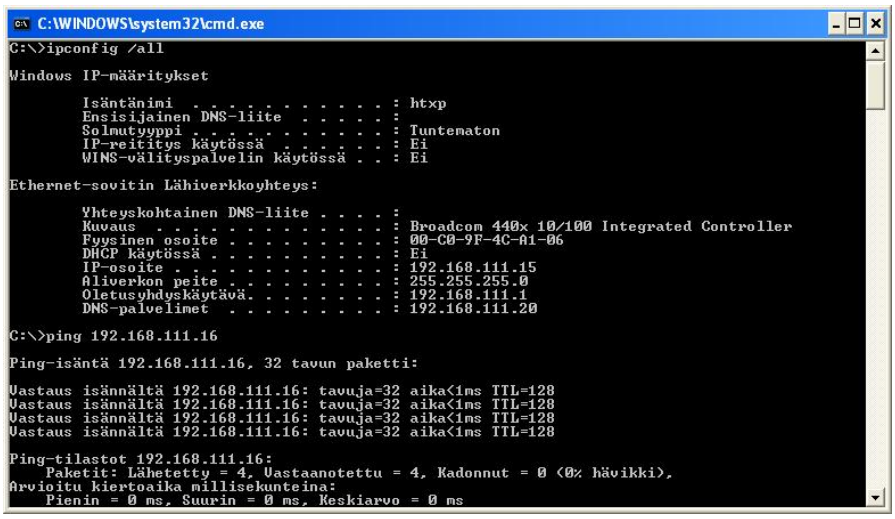
KUVIO 28. Kytkimen portti no:6 avattu käyttöön.

Kytkimen portti on siirretty IAS-palvelimen Remote Policy sääntöjen mukaisesti VLAN203:een. Verkkotoimintojen testaamiseksi tarvitaan toinen kone liitettäväksi samaan VLAN:iin. Käytetään toista konetta ja käyttäjätunnusta. Tulos on esitetty kuviossa 29.



KUVIO 29. Kaksi työasemaa liitettynä samaan VLAN:iin PEAP-autentikoinnilla.

Testataan yhteyden toiminta koneiden välillä. Tulos esitetty kuviossa 30.



KUVIO 30. Ping-testi PEAP-testikoneiden välillä.

PEAP(MS-CHAPv2)-todennuksen voidaan todeta toimivan oikein ja ennalta määritettyjen parametrien mukaisesti. Dynaamisen VLAN-yhteyden liittäminen toimii ennakoidulla tavalla ja samassa VLAN:ssa olevat koneet voivat kommunikoida toistensa kanssa.

5.6 IAS EAP-TLS-yhteyden muodostaminen

EAP-TLS-autentikointi vaatii PEAP:ssa käytetyn juurisertifikaatin lisäksi myös asiakassertifikaatin työasemalle. IAS:n yhteydessä asiakassertifikaatin jakelu on toteutettu AD:n Group Policy-määrityksillä, missä AD-toimialueelle liitetty työasema saa oman sertifikaatin automaattisesti. Työasema on liitettävä AD-toimialueelle ennen kuin EAP-TLS yhteyden vaatima sertifikaatin jakelu voi toimia. Kytkimen määrityksien vuoksi on liittämisessä nyt käytettävä PEAP-yhteyttä, jotta tarvittava yhteys AD-toimialueen ohjauskoneeseen saavutetaan. AD:n ohjauskoneen ollessa liitettynä omaan VLAN:iin, on luotava IAS-Remote Policy-määrityksien yhteydessä myös yksi erityinen Policy, jossa liitettävä työasema liitetään samaan VLAN:iin AD-ohjauskoneen kanssa. Liittämisessä käyte-

tyn Policyn pitää sisältää käyttäjä/käyttäjäryhmä, jolla on työasemien Domain-alueelle liittämiseen vaadittavat oikeudet.

Työaseman Domain-alueelle liittäminen tapahtuu työpöydällä olevan My Computer kuvakkeen kautta. Kirjoitetaan Domain-alueen nimi ja painetaan OK-painiketta. Nyt avautuu Dialogi-ikkuna, missä pyydetään liittämiseen tarvittava käyttäjätunnus ja salasana. Täytetään lomakekentät ja painetaan OK-painiketta, ja pienen viiveen jälkeen tulee esiin tiedotusikkuna missä toivotetaan työasema tervetulleeksi Domain-alueelle. Työasema on nyt käynnistettävä uudelleen. Onnistunut työaseman liittäminen Domain-alueelle on esitetty kuviossa 30.

KUVIO 30. Tervetuloa Domain-alueelle.

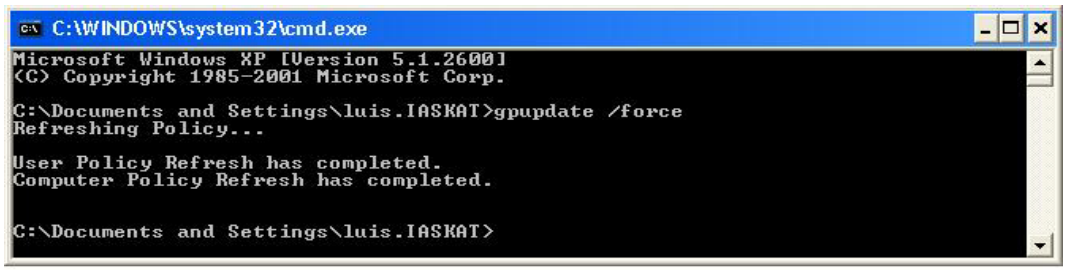
Uudelleenkäynnistyksen jälkeen on kirjauduttava työasemaan uudelleen ja on muutettava verkkoyhteyden asetuksia. Muutetaan nyt EAP type-astukseen Smart-Card or other Certificate ja Authenticate as computer. Tarkastetaan, että kohdassa When connecting-määritykset Use a certificate on this computer ja Use simple certification selection-kohdat ovat valittuina. Tavoitteena on nyt käyttää AD-kirjautumisessa vain tietokonetiliä ja siksi järjestelmärekisteriin on lisättävä uusi DWORD-arvo seuraavasti.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global]
"AuthMode"=dword:00000002

Tämä rekisterin DWORD-arvo estää käyttäjätunnuksen käyttämisen IAS-autentikoinnissa. Koska nyt käytetään työasema-autentikointia, on työasema liitet-

tävä ryhmään, joka vastaa haluttuun VLAN:iin liittämistä ja on vastaavasti määritetty IAS:n Remote-Access-Policy:ssä.

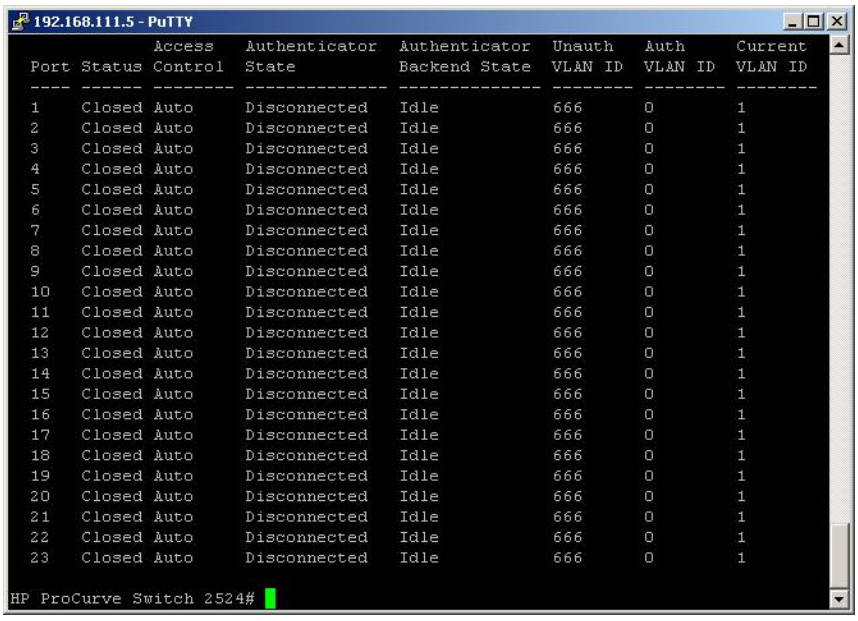
Lopuksi on päivitettävä Group Policy paikallisella työasemalla. Päivittäminen tapahtuu käyttämällä DOS-komentoriviä ja gpupdate-komentoa. Gpupdate-komento on esitetty kuviossa 31.



KUVIO 31. Gpupdate DOS-ikkuna.

Kaikki EAP-TLS-autentikoinnin vaatimat konfiguraatiot on nyt tehty ja seuraavaksi testataan yhteyden toimintaa. Työasema on käynnistettävä uudelleen, jotta tehdyt muutokset järjestelmärekisterissä astuvat voimaan.

EAP-TLS-yhteyden testaamisen aluksi tarkastetaan kytkimen porttien tila. Kytkimen porttien tila on esitetty kuviossa 32.



KUVIO 32. Kytkimen porttien tila ennen EAP-TLS autentikointia.

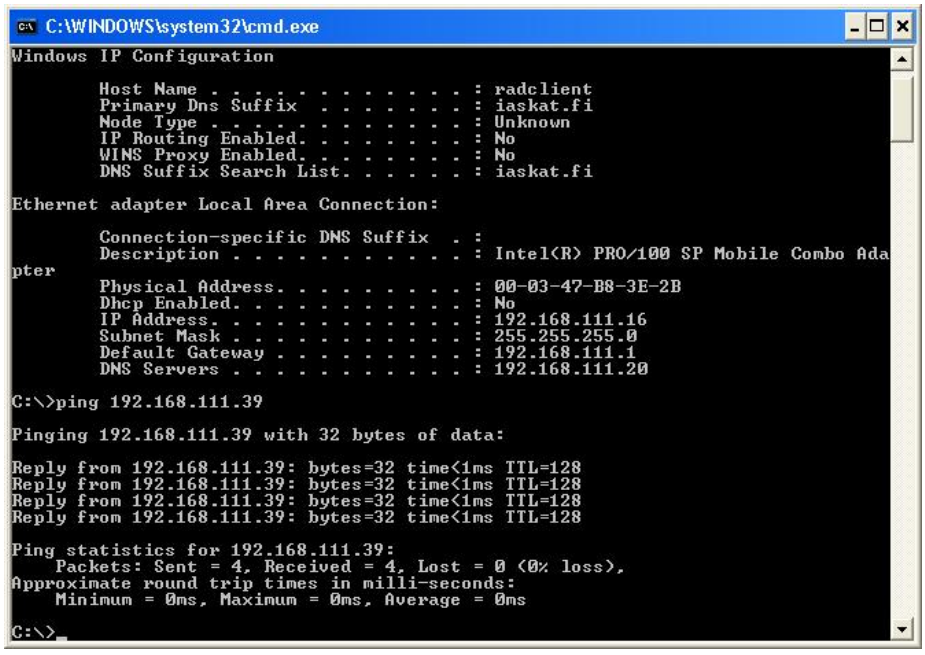
EAP-TLS-yhteyksissä oli tarkoitus testata IAS:n soveltuvuutta työasemien liittämisessä eri VLAN:iin ilman käyttäjien vaikutusta. Tarkoituksena oli helpottaa kytkimien konfigurointia ja mahdollistaa turvallinen verkkoympäristö vahvalla autentikoinnilla.

EAP-TLS ero PEAP:iin oli havaittavissa kytkimestä jo ennen sisään kirjautumista työasemalle. Työasema oli liitetty IAS:n Group Policy:ssä määritettyyn VLAN:iin ilman mitään käyttäjän toimenpiteitä. Asiakkaan EAP-TLS-yhteyden muodostumisen tai hylkäämisen voi tarkastaa IAS-palvelimen järjestelmälokeista. Onnistunut todentaminen on esitetty kuviossa 33.

```
User host/radclient.iaskat.fi was granted access.
Fully-Qualified-User-Name = iaskat.fi/Computers/RADCLIENT
NAS-IP-Address = 192.168.111.5
NAS-Identifier = HP ProCurve Switch 2524
Client-Friendly-Name = HP_ProCurve2524
Client-IP-Address = 192.168.111.5
Calling-Station-Identifier = 00-03-47-b8-3e-2b
NAS-Port-Type = Ethernet
NAS-Port = 4
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = PHKK_Edu
Authentication-Type = EAP
EAP-Type = Smart Card or other certificate
```

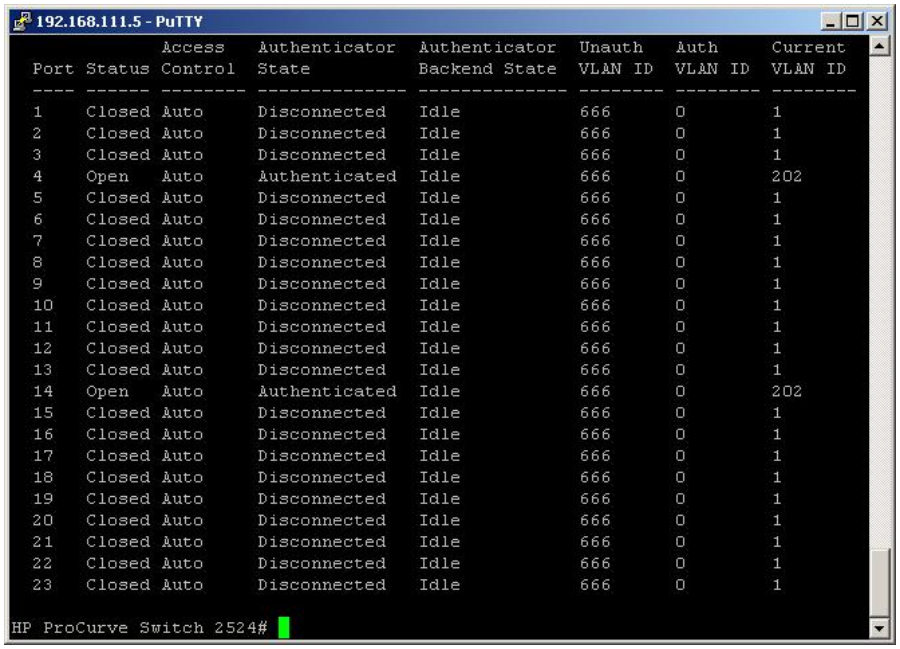
KUVIO 33. Järjestelmälokituloste

Testauksessa liitettiin kaksi konetta samaan VLAN:iin ja varmistettiin verkkoon pääsy yksinkertaisella ping-testillä. Testi on esitetty kuviosssa 34.



KUVIO 34. Ping-testi EAP-TLS-testikoneiden välillä.

Onnistuneet EAP-TLS-liittymiset voitiin todeta myös kytkimestä antamalla komento ”show port-access authenticator”, josta oli havaittavissa, että molemmat työasemat oli liitetty onnistuneesti VLAN:iin. Liitokset on esitetty kuviossa 35.



KUVIO 35. show port-access authenticator-komento.

EAP-TLS-autentikointi toimi odotetulla tavalla, ja tavoitteet saavutettiin. Varmuuden vuoksi testattiin vielä työasemaan sisäänkirjautuneen käyttäjän pääsy oletettuun palvelimella sijaitsevaan kotihakemistoon.

5.7 FREERADIUS

FreeRADIUS-palvelin on radius-protokollaa käyttävä UNIX-johdannaisiin käyttöjärjestelmiin soveltuva vapaaseen lähdekoodiin perustuva ohjelmisto. FreeRADIUS on tarkoitettu asiakkaiden autentikointiin ja radius-yhteyksien tilastointiin. Se on monipuolinen, ominaisuuksiltaan joustavasti muokattavissa ja sisältää palvelimen, asiakasohjelmiston sekä lukuisia hyödyllisiä työkaluohjelmia. FreeRADIUS tukee yleisiä EAP-MD5, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-PEAP ja EAP-LEAP-tyyppisiä EAP-protokollia. FreeRADIUS vaatii IAS:n tapaan sertifikaatit palvelimelle sekä työasemalle, ja näiden luontiin tarvitaan jokin ulkopuolinen työkaluohjelmisto kuten OpenSSL.

FreeRADIUS-testauksessa käytetty käyttöjärjestelmä oli Novell Suse Linux Enterprise Server, joka on kaupallinen versio alkujaan ilmaisesta Suse Linux-jakelusta. Kaikki Linux-jakelut sisältävät nykyisin OpenSSL paketin oletuksena, joka helpottaa sertifikaattien luomista. Linux-ympäristössä ei ole Windows-käyttöjärjestelmään tottuneille tyypillisiä graafisia työkaluja sertifikaattien luomiseen ja sertifikaattien luomiseen tarvittavat käskyt on suorittettava komentoriviltä. Aluksi on editoitava OpenSSL:n konfiguraatiotiedostoa, joka monissa Linux jakeluissa tämä sijaitsee /etc/ssl hakemistossa, mutta poikkeuksiakin on. Tiedosto openssl.cnf avataan jollakin käytössä olevalla editorilla ja muokataan sertifikaattien kohdehakemiston nimi tarkoituksen mukaiseksi, tässä tapauksessa kansion nimeksi annetaan ./TH_CA. Samaan tiedostoon kannattaa täyttää muutamat sertifikaattien luonnissa toistuvat tiedot, jotta vältytään turhalta kirjoittamiselta, ja mahdollisten kirjoitusvirheiden määrä pienenee. Seuraavaksi on siirryttävä hakemistoon /usr/share/ssl/misc/, mistä löytyy CA.sh ja CA.pl ja scriptit, joita oli myös editoitava, muuttamalla CATOP = ./TH_CA, jotta hakemistot täsmäisivät. Alkuvalmistelujen lopuksi on luotava xpextensions-tiedosto, jota käytetään palvelin- ja

asiakassertifikaatteja luotaessa. Tämä on pakollinen tiedosto, koska Windows-työasemat odottavat tiettyjä attribuutteja käytettävän niiden autentikointiin.

Seuraavassa on esitetty xpextensions tiedoston sisältö.

[xpclient_ext]
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
[xpserver_ext]

extendedKeyUsage = 1.3.6.1.5.5.7.3.1

Sertifikaattien luomiseksi oli siirryttävä takaisin /etc/ssl/-kansioon, jotta sertifikaattien generointi voidaan aloittaa.

Palvelimen juurisertifikaatti palvelun eli CA:n (Certficate Authority) luomiseen tarvittava työ aloitetaan luomalla itseallekirjoitettu sertifikaatti newreq.pem, joka sisältää yksityisen avaimen ja sertifikaatin.

openssl req -new -x509 -days 730 -keyout newreq.pem -out newreq.pem

Luodaan varsinainen CA käyttämällä edellä generoitua sertifikaattia ja yksityistä avainta. Ei tulosteta mitään ruudulle.

echo ”newreq.pem” | /usr/share/ssl/misc/CA.pl -newca > /dev/null

Luodaan sarjanumeroa ylläpitävä serial-tiedosto TH_CA-kansioon

echo '01' >> TH_CA/serial

Luodaan PCKS#12-versio juuri edellä luoduista sertifikaatista ja yksityisestä avaimesta. Tämä on salasanaan perustuva symmetrinen salausavainmenetelmä.

openssl pkcs12 -export -in TH_CA/cacert.pem -inkey newreq.pem -out root.p12 –cacerts

Muokataan edellisessä luotu root.p12- sertifikaatti PEM-muotoiseksi. Tätä muotoa voidaan käyttää Linux-Client-koneissa poistamalla siitä kaikki tieto riveiltä ennen ”BEGIN CERTIFICATE” riviä.

openssl pkcs12 -in root.p12 -out root.pem

EAP-TLS:n käyttäminen autentikoinnissa vaatii asiakaskoneelle juurisertifikaatin ja Windows-työasemat vaativat käytettäväksi DER-muotoista sertifikaattia, joten on vielä muokattava root.pem-sertifikaatti kopiomalla se root.der-muotoiseksi.

openssl x509 -inform PEM -outform DER -days 730 -in root.pem -out root.der

Lopuksi poistetaan alussa luotu sertifikaatti/avain-pari newreq.pem komennolla rm -rf newreq.pem

Seuraavaksi tehdään FreeRADIUS-palvelinta varten allekirjoituspyyntö sertifikaatille sekä yksityinen avain.

openssl req -new -nodes -keyout server_key.pem -out server_req.pem -days 730 -config ./openssl.cnf

Allekirjoitetaan palvelinsertifikaatti pyyntö juurisertifikaatilla ja käytetetään xpextensions-tiedoston xpserver-atribuuttia.

openssl ca -config ./openssl.cnf \
-policy policy_anything -out server_cert.pem \
-extensions xpserver_ext -extfile ./xpextensions \
-infiles ./server_req.pem

Poistetaan server_cert.pem-certifikaatista kaikki tieto ”BEGIN CERTIFICATE” yläpuolelta ja yhdistetään se avaimen server_key.pem:n kanssa yhdeksi sertifikaatiksi, joka sisältää näin myös julkisen avaimen.

cat server_key.pem server_cert.pem > server_keycert.pem

Seuraavaksi luodaan asiakassertifikaatin allekirjoituspyyntö ja yksityinen avain. Parametri ”-nodes” jätetään pois, koska nyt kysytään salasana, jolla sertifikaatin yksityinen avain voidaan salata.

openssl req -new -keyout client_key.pem \

-out client_req.pem -days 730 -config /etc/ssl/openssl.cnf

Allekirjoitetaan asiakassertifikaatti ja käytetään xpextensions-tiedoston xpclient-attribuuttia.

```
openssl ca -config ./openssl.cnf \
-policy policy_anything -out client_cert.pem \
-extensions xpclient_ext -extfile ./xpextensions \
-infiles ./client_req.pem
```

Viimeiseksi on muutettava client_cert.pem-sertifikaatti Windows:in käyttämään PCKS12-muotoon.

```
openssl pkcs12 -export -in client_cert.pem \
-inkey client_key.pem -out client_cert.p12 -clcerts
```

Kaikki EAP-TLS-ja PEAP-autentikonnissa tarvittavat sertifikaatit on nyt luotu, kopioidaan kaikki sertifikaattitiedostot TH_CA/certs kansioon. Luodaan vielä kaksi RADIUS-avainten luonnissa tarvittavaa tiedostoa.

Ensimmäiseksi luodaan Diffie-Hellman parametritiedosto:

```
openssl dhparam –check –text -5 512 –out dh
```

Luodaan sattumanvarainen bittivirtatiedosto TLS-salaukseen:

```
dd if=/dev/urandom of=random count=2
```

Kopioidaan dh-ja random-tiedostot TH_CA kansioon ja siirretään koko kansio /etc/raddb-hakemistoon.

5.8 FreeRADIUS PEAP-yhteyden muodostaminen

FreeRADIUS on konfiguroitavien tiedostojen osalta jaettu moneen osaan, ja eri ominaisuuksia voidaan ottaa mukaan tarpeen mukaan. Tässä työssä karsittiin kaikki turhat moduulit pois konfiguraatiosta. Tärkeimmät ja yleisemmin käytetyt konfiguroitavat tiedostot ovat radius.conf, eap.conf, clients.conf ja users. Ensimmäiseksi testattiin PEAP-yhteyden luomista ja toimintaa FreeRADIUS-

ympäristössä. Konfigurointi aloitettiin varmistamalla eap.conf tiedostossa käytettävä autentikointimenetelmä sekä käytettävät sertifikaatit ja niiden sijainti.

```
eap {
        default_eap_type = peap

        tls {
        private_key_password = Salainen
        private_key_file = ${raddbdir}/TH_CA/certs/server_keycert.pem
        certificate_file = ${raddbdir}/TH_CA/certs/server_keycert.pem
        CA_file = ${raddbdir}/TH_CA/cacert.pem
        dh_file = ${raddbdir}/TH_CA/dh
        random_file = ${raddbdir}/TH_CA/random
        fragment_size = 1024
        include_length = yes
        }
}
peap {
        default_eap_type = mschapv2
        use_tunneled_reply = no
                proxy_tunneled_request_as_eap = yes
    }
```

Pääkonfigurointitiedosto radius.conf on laaja, ja siitä on otettu seuraavaan listaukseen vain olennaiset osat.

```
mschap {
        authtype = MS-CHAP
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
        }

files {
        usersfile = ${confdir}/users
        compat = no
```

```
        }
authorize {
                mschap
                eap
                files
        }
authenticate {
                Auth-Type MS-CHAP {
                mschap
                }
                eap
        }
```

clients.conf-tiedostoon määritellään välityspalvelimena toimivan NAS:n IP-osoite ja radius-palvelimen kanssa jaettu yhteinen salasana.

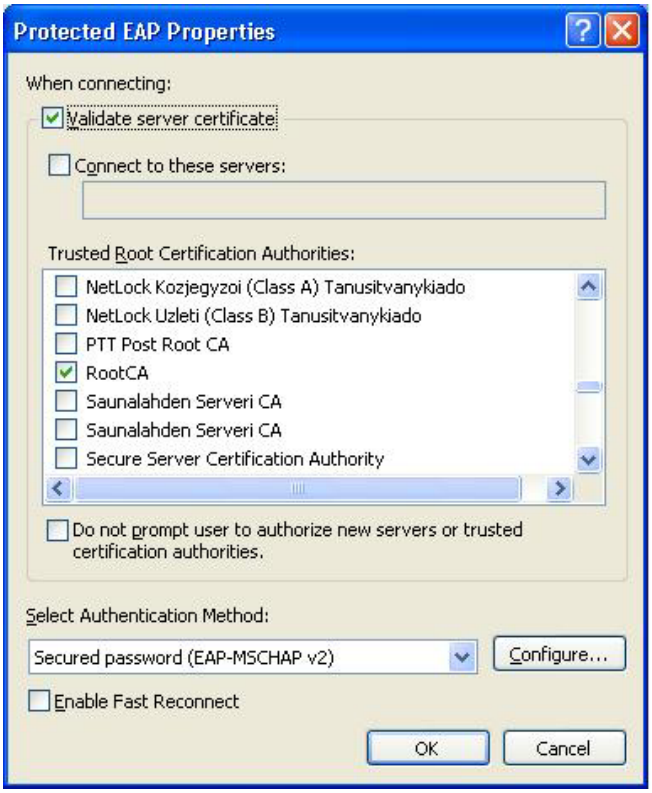
```
client 192.168.111.5/24 {
                secret= Salainen
                shortname= HP2524
}
```

users-tiedosto sisältää käyttäjätiedot ja niiden lisäattribuutit.

```
"luis"          User-Password=="Salasana"
                Tunnel-Type:= VLAN,
                Tunnel-Medium-Type:=IEEE-802,
                Tunnel-Private-Group-ID:= 201

"Charlie"       User-Password=="Brown"
                Tunnel-Type:=VLAN,
                Tunnel-Medium-Type:=IEEE-802,
                Tunnel-Private-Group-ID:=201
```

Työaseman konfigurointi on vastaavanlainen kuin IAS:n PEAP-yhteyden, ja RADIUS-palvelimen root.der-sertfikaatti on lisättävä työaseman Trusted Root Certification Authorities\Local Computer säilöön. Verkkoyhteyden konfiguroinnissa valitaan palvelinsertifikaatin vahvistaminen yhteyden avaamisessa. Sertifikaatin valinta on esitetty kuviossa 36.



KUVIO 36. Protected EAP Properties-ikkuna

Kytkimeen muutetaan FreeRADIUS-palvelimen osoite, jotta NAS osaa ohjata autentikointipyynnöt oikeaan osoitteeseen.

radius-server host 192.168.111.22 key Salainen.

Yhteyden testaaminen aloitetaan asettamalla työaseman verkkoyhteys disable-tilaan ja käynnistämällä FreeRADIUS -ohjelmisto antamalla komentoriviltä käsky radiusd –X –A. Tämä käynnistää radius daemonin debug-modeen, jossa voidaan seurata radius-viestien vaihtoa ja tallentaa autentikoinnit lokitiedostoon. Mikäli radius daemon käynnistyy ilman virheitä, se jää tilaan, jossa se odottaa autenti-

kointipyyntöjä ”Ready to process requests”-ilmoituksella. PEAP-prosessin kulku on esitetty liitteessä 2.

Työasemassa muutetaan verkkoyhteys enable-tilaan ja oikeaan alakulmaan ilmaantuvan huomautusikkunan klikkaaminen avaa dialogi-ikkunan. Annetaan users-tiedostoon määritelty käyttäjätunnus ja salasana. Radiusd alkaa käsitellä autentikointipyyntoä ja mikäli autentikointi onnistuu, se ilmenee ruudulla Access-Accept-ilmoituksena. Kytkimestä voidaan havaita portin avautuneen users-tiedostossa määritettyyn VLAN:iin. Onnistunut autentikonti on esitetty kuviossa 37.

```
                Access    Authenticator  Authenticator  Unauth    Auth      Current
Port  Status    Control   State          Backend State  VLAN ID   VLAN ID   VLAN ID
----  ------    --------  -------------  -------------  --------  --------  ----------
1     Closed    Auto      Disconnected   Idle           666       0         1
2     Open      Auto      Authenticated  Idle           666       0         201
3     Closed    Auto      Disconnected   Idle           666       0         1
4     Closed    Auto      Disconnected   Idle           666       0         1
5     Closed    Auto      Disconnected   Idle           666       0         1
6     Closed    Auto      Disconnected   Idle           666       0         1
7     Closed    Auto      Disconnected   Idle           666       0         1
8     Closed    Auto      Disconnected   Idle           666       0         1
9     Closed    Auto      Disconnected   Idle           666       0         1
10    Closed    Auto      Disconnected   Idle           666       0         1
11    Closed    Auto      Disconnected   Idle           666       0         1
12    Closed    Auto      Disconnected   Idle           666       0         1
13    Closed    Auto      Disconnected   Idle           666       0         1
14    Closed    Auto      Disconnected   Idle           666       0         1
15    Closed    Auto      Disconnected   Idle           666       0         1
16    Closed    Auto      Disconnected   Idle           666       0         1
17    Closed    Auto      Disconnected   Idle           666       0         1
18    Closed    Auto      Disconnected   Idle           666       0         1
19    Closed    Auto      Disconnected   Idle           666       0         1
20    Closed    Auto      Disconnected   Idle           666       0         1
21    Closed    Auto      Disconnected   Idle           666       0         1
22    Closed    Auto      Disconnected   Idle           666       0         1
23    Closed    Auto      Disconnected   Idle           666       0         1

HP ProCurve Switch 2524#
```

KUVIO 37. FreeRADIUS PEAP VLAN-näkymä kytkimestä.

FreeRADIUS tallentaa määritysten mukaan autentikointipyynnöt ja vastaukset erillisiin lokitiedostoihin, joista voidaan hakea hyväksytyt yhteydet. Ote lokitiedostosta on esietty kuviossa 38.

```
Packet-Type = Access-Accept
Sun Sep 16 13:44:39 2007
        Tunnel-Type:0 := VLAN
        Tunnel-Medium-Type:0 := IEEE-802
        Tunnel-Private-Group-Id:0 := "201"
        MS-MPPE-Recv-Key = 0x41afc4167e97748ba59c2efa6f1cd6c551f1474e7f54a9e75ce92b0e593e8472
        MS-MPPE-Send-Key = 0x308cafd1ea31328ca95361bbb077913c8611d7f9e302926b6a686457eacc8bd7
        EAP-Message = 0x03090004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "luis"
```

KUVIO 38. FreeRADIUS reply-loki.

FreeRADIUS PEAP-autentikointi onnistuu tarkoitetulla tavalla, ja konfiguroinnin vaatima työ pienimuotoisessa testissä on vähäistä. Dynaaminen VLAN-yhteys toteutuu määritettyjen sääntöjen mukaisesti, ja työssä on saavutettu ennalta asetetut tavoitteet.

5.9 FreeRADIUS EAP-TLS-yhteyden muodostaminen

FreeRADIUS EAP-TLS:n käyttöön otto ei vaadi suuria muutoksia PEAP-konfiguraatioon. Vain tiedostoja eap.conf ja users on editoitava. Avataan ne editorilla ja muokataan ensin eap.conf tiedostoa.

```
eap {

        default_eap_type = tls
```

users-tiedostoon lisätään rivi

```
DEFAULT                 Auth-Type:= EAP
```

Users-tiedostosta on joko poistettava rivit, joissa on käyttäjätunnus ja salasana tai lisättävä #-merkki niiden rivien alkuun estämään niiden käsittelyn. EAP-TLS ei käytä autentikoinnissa käyttäjätunnuksia ja salasanoja, vaan käyttää niiden sijaan asiakassertifikaattia. Yhteyden muodostamisessa ei käytetä myöskään dialogi-ikkunoita eikä asiakkaan toimia tarvita. Työasemaan on asennettava asiakassertifikaatti client_cert.p12, joka sijoitetaan asennus ohjelman tarjoamaan oletus säiliöön, joka on käyttäjäkohtainen säiliö (Certificates/CurrentUser/Personal). Verkkoyhteyden EAP-type muutetaan valintaan Smart Card or other Certificate ja palvelin sertifikaatti on sama kuin PEAP -yhteydessä. Asiakassertifikaatin asentumisen oikeaan paikkaan voi tarvittaessa tarkastaa MMC-konsolin avulla.

Asetetaan työaseman verkkoyhteys disable-tilaan ja käynnistetään RADIUS-palvelin komentoriviltä komennolla radiusd -X -A. Muutetaan työaseman verkkoyhteys enable-tilaan. Yhteyttä testattiin kahdella työasemalla. Yhteyden onnistumisen saattoi tarkastaa palvelimen reply-lokista. Loki on esitetty kuviossa 39 ja prosessin kulku on esitetty liitteessä 3.

```
Packet-Type = Access-Accept
Sun Sep 16 14:09:05 2007
        Tunnel-Type:0 := VLAN
        Tunnel-Medium-Type:0 := IEEE-802
        Tunnel-Private-Group-Id:0 := "101"
        MS-MPPE-Recv-Key = 0x0abb09bd1acdaa6d17e72614b713d391a77902e42b702b549695cca0a2524978
        MS-MPPE-Send-Key = 0x2212ab6eb37b8f0e450d739fe5792153fd44bca8938ee1805aec8dedb91e6d92
        EAP-Message = 0x03050004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "ClientRAD"

Packet-Type = Access-Accept
Sun Sep 16 14:09:12 2007
        Tunnel-Type:0 := VLAN
        Tunnel-Medium-Type:0 := IEEE-802
        Tunnel-Private-Group-Id:0 := "101"
        MS-MPPE-Recv-Key = 0x2faa67b29b0cebd291136729ba428f8581cb494ad91c66982bb480cfbc7571b2
        MS-MPPE-Send-Key = 0x92222619528b04b5291f03ff152fec4ec55719574423a4c885aabcd004db4922
        EAP-Message = 0x03050004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "ClientRAD"
```

KUVIO 39. Näkymä FreeRADIUS-palvelimen EAP-TLS-reply-lokista.

VLAN-kytkennän voi tarkastaa kytkimen konsolilta show port-access authenticator-komennolla. Kytkimen porttien tila on esitetty kuviossa 40.

```
                Access   Authenticator  Authenticator  Unauth    Auth      Current
  Port Status   Control  State          Backend State  VLAN ID   VLAN ID   VLAN ID
  ---- -------- -------- -------------- -------------- --------- --------- ----------
  1    Closed   Auto     Disconnected   Idle           666       0         1
  2    Open     Auto     Authenticated  Idle           666       0         101
  3    Closed   Auto     Disconnected   Idle           666       0         1
  4    Closed   Auto     Disconnected   Idle           666       0         1
  5    Closed   Auto     Disconnected   Idle           666       0         1
  6    Closed   Auto     Disconnected   Idle           666       0         1
  7    Closed   Auto     Disconnected   Idle           666       0         1
  8    Closed   Auto     Disconnected   Idle           666       0         1
  9    Closed   Auto     Disconnected   Idle           666       0         1
  10   Open     Auto     Authenticated  Idle           666       0         101
  11   Closed   Auto     Disconnected   Idle           666       0         1
  12   Closed   Auto     Disconnected   Idle           666       0         1
  13   Closed   Auto     Disconnected   Idle           666       0         1
  14   Closed   Auto     Disconnected   Idle           666       0         1
  15   Closed   Auto     Disconnected   Idle           666       0         1
  16   Closed   Auto     Disconnected   Idle           666       0         1
  17   Closed   Auto     Disconnected   Idle           666       0         1
  18   Closed   Auto     Disconnected   Idle           666       0         1
  19   Closed   Auto     Disconnected   Idle           666       0         1
  20   Closed   Auto     Disconnected   Idle           666       0         1
  21   Closed   Auto     Disconnected   Idle           666       0         1
  22   Closed   Auto     Disconnected   Idle           666       0         1
  23   Closed   Auto     Disconnected   Idle           666       0         1

 HP ProCurve Switch 2524#
```

KUVIO 40. EAP-TLS-yhteyden VLAN:it kytkimessä.

EAP-TLS yhteyden muodostaminen FreeRADIUS palvelimella onnistui tavoitteiden mukaisesti. Yhteyden muodostaminen työasematiliä käyttäen ei kuulu Free-

RADIUS-palvelimen perus toimintoihin, joten työasemien liittäminen eri VLAN aliverkkoihin EAP-TLS-autentikointia käyttäen ei onnistu. Tämä johtuu siitä syystä, että kaikissa työasemissa käytetään samaa asiakassertifikaattia, jota käytetään asiakkaantunnisteena. Muita keinoja varmaankin löytyy lisämoduulien avulla, mutta niiden testaaminen ei kuulunut työn tavoitteisiin.

6 YHTEENVETO

Autentikoinnin rooli lisääntyy koko ajan lisääntyvien verkkopalveluiden mukana. Yhä useammin vaaditaan asiakkaalta autentikointia ennen pääsyä lähiverkon palveluihin. Useissa kohteissa on havaittu tarpeelliseksi asiakkaan todentaminen jo ennen lähiverkkoon pääsyä. Tästä on seurauksena jonkin asteisten varmenteiden tarve, joilla osapuolet voivat todentaa toisensa. Tämä asettaa haasteita verkkoyhteyden muodostamisessa suojaukselle, joiden turvin osapuolet voivat tarkistaa toistensa aitouden ennen yhteyden avaamista. Suurten käyttäjämäärien ollessa kyseessä, saattaa palveluiden autentikointi ilman keskitettyä käyttäjätietokantaa johtaa hallitsemattomaan tilanteeseen. Käyttämällä tarkoitukseen sopivia autentikointimenetelmiä ja -protokollia eri käyttäjäryhmille, on mahdollista tarjota turvallinen yhteys verkonpalveluihin.

Työn tarkoituksena oli testata työasemien liittämistä ennalta määriteltyihin VLAN-aliverkkoihin RADIUS-palvelimen ja AAA-autentikointia tukevan lähiverkkokytkimen kanssa. Lähtökohtana oli vertailla jo olemassa olevaan hakemistopalvelurakenteeseen integroitavaa Microsoft IAS-palvelinta sekä täysin muista käyttöjärjestelmäpalveluista riippumatonta ja omaa käyttäjätiedostoa käyttävää FreeRADIUS-palvelinta.

Microsoft IAS-palvelimen asennus ja käyttöönotto on hyvin dokumentoitua, joten yllätyksiä ja vaikeuksia ei niiltä osin tullut. Suurin ongelma oli löytää dokumentointi IAS-palvelimen käyttökuntoon saattamiseksi vain yhden Windows-palvelimen avulla. Microsoft IAS on kohtalaisen helposti muokattavissa tämän työn vaatimiin tavoitteisiin, ja suurin työ oli saada asennettua DNS, AD ja CA palvelut, jotka toimivat perustana IAS-palvelimen toiminnalle. IAS:n toiminta dynaamisten VLAN verkkojen liittämisessä käyttäjille ja työasemille oli hyvin toimivaa ja parametrien valikoima on riittävää vaativampiinkin toimintoihin. IAS-palvelimen policy-ryhmien verkkoonkirjautumisen aikarajan säätämisten mahdollisuus antaa myös verkolle tarvittavaa lisäturvaa.

FreeRADIUS-palvelimen toimintakuntoon saattamisessa suurin työ on sertifikaattien luomisessa. Palvelimen konfigurointi on hieman haasteellisempaa kuin Microsoftin tuotteessa, johtuen graafisten työkalujen puutteesta. Tekstieditorin avulla tarvittavat muutokset konfigurointitiedostoihin saadaan kuitenkin tehtyä kohtuullisen vaivan jälkeen. Palvelimen toiminta työssä käytettyjen EAP-protokollien kanssa oli hyvin toimivaa ja VLAN-liittämiset saatiin toimimaan tavoitteiden mukaisesti. Ainoiksi puutteiksi voidaan katsoa työasemakohtaisen tilimahdollisuuden puuttuminen ja palvelimen hallinnan parametrien lisääminen editorilla käsityönä. FreeRADIUS palvelimen käyttäjätietokannan voi myös hakea ulkoisesta hakemistopalvelusta, mutta sen tarkoituksenmukaisuutta ja muita RADIUS palvelin vaihtoehtoja kannattaa harkita tarkoin ennen käytäntöön ryhtymistä.

RADIUS-palvelinten toiminta työssä oli niiden tarjoamien mahdollisuuksien rajoissa moitteetonta. Voidaan siis todeta, että opinnäytetyöhön asetetut tavoitteet saavutettiin suunnitelman mukaisesti. Työasemien liittäminen tarkoitettuun VLAN-verkkoon ryhmäjäsenyyden perusteella toteutui suunnitelmien mukaisesti sekä EAP-TLS-, että PEAP(MSCHAPv2)-protokollilla. Microsoft IAS-palvelin on toistaiseksi laajempien toimintojensa ja integroidun hakemistopalvelun puolesta valmiimpi vaihtoehto RADIUS-palvelimeksi. Microsoft IAS on hyvä vaihtoehto suuriin käyttäjä ympäristöihin, ja se on helppo ottaa käyttöön. FreeRADIUS on taloudellinen vaihtoehto ja soveltuu paremmin pienempiin ympäristöihin, tosin myös se on mahdollista liittää jo olemassa olevaan hakemistopalveluun lisäprotokollaa käyttäen.

Tulevaisuudessa voitaisiin tehdä jatkotutkimusta eri päätelaitteiden liittämiseksi 802.1x-autentikoinnilla verkkoon. Työasemissa käytettävät käyttöjärjestelmät vaihtelevat käyttötarkoituksien mukaan Windows-, Linux- ja MAC-järjestelmien välillä. Tässä työssä ei tutkittu 802.1x autentikointia, muiden kuin Windows käyttöjärjestelmien osalta, joten tulevaisuudessa olisi hyvä suorittaa laajempaa kartoitusta RADIUS-järjestelmään liitettävien muiden käyttöjärjestelmien vaatimista asetuksista. Linux-käyttöjärjestelmien yleistyminen käytössä ja niihin kohdistuva laaja kehitystyö tekee niistä varteenotettavan vaihtoehdon työaseman käyttöjärjestelmänä. MacOS on säilyttänyt suosionsa, ja siihen on myös saatavana 802.1x-

protokollan tuki. Tämän lisäksi olisi vielä tutkittava kämmentietokoneiden ja verkkotulostimien liittämisen mahdollisuutta, koska osa laitteista sisältää 802.1x-tuen. Myöhemmässä vaiheessa, kun RADIUS-protokollan todennäköisesti korvaava DIAMETER-protokolla saa standardin statuksen ja sen myötä tuki mobiililaitteille muuttuu, olisi palveluntarjonnan tilan uudelleentarkastelun aika.

LÄHTEET

Cisco Systems 2000. Internetworking Technologies Handbook,Third Edition. Cisco Press, Indianapolis

Cisco Systems 2001. Authentication, Authorization and Accounting [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/aaans_ov.pdf

Cisco Systems 2002. Cisco Networking Academy Program: Second-Year Companion Guide, Cisco Press, Indianapolis

Cisco Systems 2005. Cisco Wireless LAN Security/EAP Authentication Protocols for WLANs [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.ciscopress.com/content/images/1587051540/samplechapter/1587051540content.pdf

Cisco Systems 2006. Catalyst 2960 Switch Software Configuration Guide [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://cco-rtp-1.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/2960SCG.pdf

Cisco Systems 2006. Cisco IOS Security Configuration Guide/AAA Overview, [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfaaa.pdf

Decisys Inc 1996. The Virtual LAN Technology Report [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf

European Parliament and of the Council. Directive 1999/93/EC 13 December 1999 [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

Hewlett-Packard. RADIUS-Overview 2003 [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.docs.hp.com/en/T1428-90025/ch01s01.html

Interlink Networks 2006. The Beginnings and History of RADIUS [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf

Kizza M Joseph. 2005. Computer Network Security. Springer, New York .

Microsoft Corporation. PEAP with MS-CHAP Version 2 for Secure Password-National Institute of Standards and Technology 2000, Digital Signature Standard [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

Microsoft Corporation. How IAS Technology Works 2003 [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://technet2.microsoft.com/windowsserver/en/library/e9a30a60-7f8b-435f-b210-d47c3b7ecb961033.mspx?mfr=true

Microsoft Corporation. IEEE 802.11 Wireless LAN Security with Microsoft Windows 2007[verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.microsoft.com/downloads/details.aspx?familyid=67fdeb48-74ec-4ee8-a650-334bb8ec38a9&displaylang=en#AffinityDownloads

National Institute of Standards and Technology 2001. Introduction to Public Key Technology and the Federal PKI Infastructure[verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

Network Working Group 2000. Remote Authentication Dial In User Service (RADIUS) [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://rfc.net/rfc2865.html

Network Working Group 2002. EAP Tunneled TLS Authentication Protocol [verkkodokumentti], [viitattu 21.11.2007]] Saatavissa: http://tools.ietf.org/html/draft-ietf-pppext-eap-ttls-02

Network Working Group 2002. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://ietfreport.isoc.org/rfc/PDF/rfc3280.pdf

Network Working Group 2006. Guidance for AAA Key Management [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://tools.ietf.org/html/draft-housley-aaa-key-mgmt-04

Edward Schneider 2001. LAN Switching Technologies and Virtual LAN [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://ise.gmu.edu/~eschneid/infs612/projects/LAN.pdf

Viestintävirasto 2007. Varmenne [verkkodokumentti], [viitattu 21.11.2007] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/varmenne.html

LIITTEET

LIITE 1

HP 2524 Kytkimen konfiguraatio IAS-Palvelimen kanssa.

```
hostname "HP ProCurve Switch 2524"
snmp-server location "FARM"
cdp run
interface 1
   no lacp
exit
interface 2
   no lacp
exit
interface 3
   no lacp
exit
interface 4
   no lacp
exit
interface 5
   no lacp
exit
interface 6
   no lacp
exit
interface 7
   no lacp
exit
interface 8
   no lacp
exit
interface 9
   no lacp
exit
interface 10
   no lacp
exit
interface 11
   no lacp
exit
interface 12
   no lacp
exit
```

LIITE 1 (JATKUU)

```
interface 13
  no lacp
exit
interface 14
  no lacp
exit
interface 15
  no lacp
exit
interface 16
  no lacp
exit
interface 17
  no lacp
exit
interface 18
  no lacp
exit
interface 19
  no lacp
exit
interface 20
  no lacp
exit
interface 21
  no lacp
exit
interface 22
  no lacp
exit
interface 23
  no lacp
exit
ip default-gateway 192.168.111.1
snmp-server community "public" Unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-26
  ip address 192.168.111.5 255.255.255.0
  exit
vlan 101
  name "HK_PHKK"
  tagged 24
  exit
vlan 102
  name "OPP_PHKK"
  tagged 24
```

LIITE 1 (JATKUU)

```
   exit
vlan 103
   name "GUEST_PHKK"
   tagged 24
   exit
vlan 201
   name "HK_SALPAUS"
   tagged 24
   exit
vlan 202
   name "OPP_SALPAUS"
   tagged 24
   exit
vlan 203
   name "GUEST_SALPA"
   tagged 24
   exit
vlan 666
   name "NotUsed"
   exit
aaa authentication port-access eap-radius
radius-server host 192.168.111.20
aaa port-access authenticator active
aaa port-access authenticator 1-23
aaa port-access authenticator 1-23 unauth-vid 666
password manager
password operator
```

LIITE 2

FreeRADIUS palvelimen PEAP Autentikonti prosessi

```
Starting - reading configuration files ...
reread_config:  reading radiusd.conf
Config:   including file: /etc/raddb/clients.conf
Config:   including file: /etc/raddb/eap.conf
 main: prefix = "/usr"
 main: localstatedir = "/var"
 main: logdir = "/var/log/radius"
 main: libdir = "/usr/lib/freeradius"
 main: radacctdir = "/var/log/radius/radacct"
 main: hostname_lookups = no
 main: max_request_time = 30
 main: cleanup_delay = 5
 main: max_requests = 1024
 main: delete_blocked_requests = 0
 main: port = 0
 main: allow_core_dumps = no
 main: log_stripped_names = no
 main: log_file = "/var/log/radius/radius.log"
 main: log_auth = yes
 main: log_auth_badpass = yes
 main: log_auth_goodpass = yes
 main: pidfile = "/var/run/radiusd/radiusd.pid"
 main: bind_address = 192.168.111.22 IP address [192.168.111.22]
 main: user = "radiusd"
 main: group = "radiusd"
 main: usercollide = no
 main: lower_user = "no"
 main: lower_pass = "no"
 main: nospace_user = "no"
 main: nospace_pass = "no"
 main: checkrad = "/usr/sbin/checkrad"
 main: proxy_requests = no
 security: max_attributes = 200
 security: reject_delay = 1
 security: status_server = no
 main: debug_level = 0
read_config_files:  reading dictionary
read_config_files:  reading naslist
read_config_files:  reading clients
read_config_files:  reading realms
radiusd:  entering modules setup
Module: Library search path is /usr/lib/freeradius
Module: Loaded MS-CHAP
 mschap: use_mppe = no
 mschap: require_encryption = no
```

LIITE 2 (JATKUU)

```
 mschap: require_strong = yes
 mschap: with_ntdomain_hack = no
 mschap: passwd = "(null)"
 mschap: authtype = "MS-CHAP"
 mschap: ntlm_auth = "(null)"
Module: Instantiated mschap (mschap)
Module: Loaded eap
 eap: default_eap_type = "peap"
 eap: timer_expire = 60
 eap: ignore_unknown_eap_types = no
 eap: cisco_accounting_username_bug = no
 tls: rsa_key_exchange = no
 tls: dh_key_exchange = yes
 tls: rsa_key_length = 512
 tls: dh_key_length = 512
 tls: verify_depth = 0
 tls: CA_path = "(null)"
 tls: pem_file_type = yes
 tls: private_key_file = "/etc/raddb/TH_CA/certs/server_keycert.pem"
 tls: certificate_file = "/etc/raddb/TH_CA/certs/server_keycert.pem"
 tls: CA_file = "/etc/raddb/TH_CA/cacert.pem"
 tls: private_key_password = "Salainen"
 tls: dh_file = "/etc/raddb/TH_CA/dh"
 tls: random_file = "/etc/raddb/TH_CA/random"
 tls: fragment_size = 1024
 tls: include_length = yes
 tls: check_crl = no
 tls: check_cert_cn = "(null)"
rlm_eap_tls: Loading the certificate file as a chain
rlm_eap: Loaded and initialized type tls
 peap: default_eap_type = "mschapv2"
 peap: copy_request_to_tunnel = no
 peap: use_tunneled_reply = no
 peap: proxy_tunneled_request_as_eap = yes
rlm_eap: Loaded and initialized type peap
 mschapv2: with_ntdomain_hack = no
rlm_eap: Loaded and initialized type mschapv2
Module: Instantiated eap (eap)
Module: Loaded preprocess
 preprocess: huntgroups = "/etc/raddb/huntgroups"
 preprocess: hints = "/etc/raddb/hints"
 preprocess: with_ascend_hack = no
 preprocess: ascend_channels_per_line = 23
 preprocess: with_ntdomain_hack = no
 preprocess: with_specialix_jetstream_hack = no
 preprocess: with_cisco_vsa_hack = no
Module: Instantiated preprocess (preprocess)
Module: Loaded detail
```

LIITE 2 (JATKUU)

```
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/auth-detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (auth_log)
Module: Loaded files
 files: usersfile = "/etc/raddb/users"
 files: acctusersfile = "/etc/raddb/acct_users"
 files: preproxy_usersfile = "/etc/raddb/preproxy_users"
 files: compat = "no"
Module: Instantiated files (files)
Module: Loaded Acct-Unique-Session-Id
 acct_unique: key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IP-
Address, NAS-Port"
Module: Instantiated acct_unique (acct_unique)
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (detail)
Module: Loaded radutmp
 radutmp: filename = "/var/log/radius/radutmp"
 radutmp: username = "%{User-Name}"
 radutmp: case_sensitive = yes
 radutmp: check_with_nas = yes
 radutmp: perm = 384
 radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/reply-detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (reply_log)
Listening on authentication 192.168.111.22:1812
Listening on accounting 192.168.111.22:1813
Ready to process requests.
```

LIITE 3

FreeRADIUS palvelimen EAP-TLS Autentikonti prosessi

```
Starting - reading configuration files ...
reread_config:  reading radiusd.conf
Config:   including file: /etc/raddb/clients.conf
Config:   including file: /etc/raddb/eap.conf
 main: prefix = "/usr"
 main: localstatedir = "/var"
 main: logdir = "/var/log/radius"
 main: libdir = "/usr/lib/freeradius"
 main: radacctdir = "/var/log/radius/radacct"
 main: hostname_lookups = no
 main: max_request_time = 30
 main: cleanup_delay = 5
 main: max_requests = 1024
 main: delete_blocked_requests = 0
 main: port = 0
 main: allow_core_dumps = no
 main: log_stripped_names = no
 main: log_file = "/var/log/radius/radius.log"
 main: log_auth = yes
 main: log_auth_badpass = yes
 main: log_auth_goodpass = yes
 main: pidfile = "/var/run/radiusd/radiusd.pid"
 main: bind_address = 192.168.111.22 IP address [192.168.111.22]
 main: user = "radiusd"
 main: group = "radiusd"
 main: usercollide = no
 main: lower_user = "no"
 main: lower_pass = "no"
 main: nospace_user = "no"
 main: nospace_pass = "no"
 main: checkrad = "/usr/sbin/checkrad"
 main: proxy_requests = no
 security: max_attributes = 200
 security: reject_delay = 1
 security: status_server = no
 main: debug_level = 0
read_config_files:  reading dictionary
read_config_files:  reading naslist
read_config_files:  reading clients
read_config_files:  reading realms
radiusd:  entering modules setup
Module: Library search path is /usr/lib/freeradius
Module: Loaded eap
 eap: default_eap_type = "tls"
 eap: timer_expire = 60
 eap: ignore_unknown_eap_types = no
```

LIITE 3 (JATKUU)

```
 eap: cisco_accounting_username_bug = no
 tls: rsa_key_exchange = no
 tls: dh_key_exchange = yes
 tls: rsa_key_length = 512
 tls: dh_key_length = 512
 tls: verify_depth = 0
 tls: CA_path = "(null)"
 tls: pem_file_type = yes
 tls: private_key_file = "/etc/raddb/TH_CA/certs/server_keycert.pem"
 tls: certificate_file = "/etc/raddb/TH_CA/certs/server_keycert.pem"
 tls: CA_file = "/etc/raddb/TH_CA/cacert.pem"
 tls: private_key_password = "Salainen"
 tls: dh_file = "/etc/raddb/TH_CA/dh"
 tls: random_file = "/etc/raddb/TH_CA/random"
 tls: fragment_size = 1024
 tls: include_length = yes
 tls: check_crl = no
 tls: check_cert_cn = "(null)"
rlm_eap_tls: Loading the certificate file as a chain
rlm_eap: Loaded and initialized type tls
Module: Instantiated eap (eap)
Module: Loaded preprocess
 preprocess: huntgroups = "/etc/raddb/huntgroups"
 preprocess: hints = "/etc/raddb/hints"
 preprocess: with_ascend_hack = no
 preprocess: ascend_channels_per_line = 23
 preprocess: with_ntdomain_hack = no
 preprocess: with_specialix_jetstream_hack = no
 preprocess: with_cisco_vsa_hack = no
Module: Instantiated preprocess (preprocess)
Module: Loaded detail
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/auth-detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (auth_log)
Module: Loaded files
 files: usersfile = "/etc/raddb/users"
 files: acctusersfile = "/etc/raddb/acct_users"
 files: preproxy_usersfile = "/etc/raddb/preproxy_users"
 files: compat = "no"
Module: Instantiated files (files)
Module: Loaded Acct-Unique-Session-Id
 acct_unique: key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IP-
Address, NAS-Port"
Module: Instantiated acct_unique (acct_unique)
```

LIITE 3 (JATKUU)

```
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (detail)
Module: Loaded radutmp
 radutmp: filename = "/var/log/radius/radutmp"
 radutmp: username = "%{User-Name}"
 radutmp: case_sensitive = yes
 radutmp: check_with_nas = yes
 radutmp: perm = 384
 radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
 detail: detailfile = "/var/log/radius/radacct/%{Client-IP-Address}/reply-detail-
%Y%m%d"
 detail: detailperm = 384
 detail: dirperm = 493
 detail: locking = no
Module: Instantiated detail (reply_log)
Listening on authentication 192.168.111.22:1812
Listening on accounting 192.168.111.22:1813
Ready to process requests.
```

LIITE 4

IAS ASENNUS

Palvelimen asennus käynnistetään CD:ltä ja asennetaan normaalit oletuskomponentit, koska asennusta täydennetään myöhemmin. Määritellään verkkokortille kiinteä IP-osoite, tämä vaatimus johtuu Windows Active Directoryn vaatimasta DNS-palvelimesta.

Asennetaan Active Directory asennus ”dcpromo” komennolla. Asennusvelho tarjoaa alussa valittavaksi myös DNS-palvelimen asennuksen, joka asennetaan velhon avustuksella. DNS-palvelin vaatii hieman tarkempaa hienosäätöä toimiakseen tarkoituksen mukaisella tavalla, mikä tässä tarkoittaa luomalla Pointer (PTR-record) merkinnän Reverse Lookup Zone kansioon. DNS-palvelin on Active Directory ympäristössä pakollinen, johtuen hakemistopalvelu rakenteesta.

Muutetaan AD:n toiminnallisuus vastaamaan palvelin versiota, eli korotetaan palvelin Active Directory 2003 tasolle. Dynaamisen IP-osoitteiden jakamiseksi palvelimelta on asennetteva DHCP-palvelin, jolla jaetaan IP-osoitteet Domain-alueen työasemille. Mikäli tarkoituksena on jakaa lähiverkonosoitteet useisiin eri IP-aliverkkoihin, esimerkiksi VLAN-verkkoihin, on DHCP-palvelimeen määriteltävä nämä aliverkkoalueet. Useisiin aliverkkoihin jaetut IP-osoitteet vaativat niiden käytettävyyden mahdollistamiseksi myös reitittimen, mihin on konfiguroitava vaadittavat aliverkkoalueet. Seuraavaksi asennetaan palvelimeen IIS-palvelin sekä Certificate Services eli sertifikaatti palvelut. Sertifikaatti palvelimen asennuksessa on valittava CA-tyyppi, mikä tässä tapauksessa oli Enterprise root CA ja sertifikaatin voimassaoloaika, mikä hyväksyttiin oletusasetuksin 5 vuodeksi. Asennusvelho kysyy vielä seuraavalla sivulla juurisertifikaatin nimen ja säilytys kansion.

LIITE 4 (JATKUU)

Asennus jatkuu asentamalla varsinainen Windows RADIUS-palvelin IAS, joka asennuksen päätteeksi on rekisteröitävä Active Directoryyn. Koko palvelin asen

nuksen viimeistelemiseksi on suositeltavaa asentaa Windows Server Service-Pack:sta uusin versio sekä uusimmat tietoturva päivitykset. Palvelimen uudelleen käynnistämisen jälkeen on syytä tarkistaa AD:n ja DNS-palvelimien toiminta tapahtumalokeista. Mikäli lokeista löytyy virheitä on syytä tarkistaa asennuksen eri vaiheet uudelleen ja varmistaa jo tehdyt konfiguroinnit.

Sertifikaattien luonti

Käynnistetään start→Run→mmc →MMC-työkalu, missä on avattava päävalikosta Add/Remove-snap-in sertifikaatti pohjien lisäämiseksi ja muokkaamiseksi käyttöön sopivaksi.Lisätään Certificate Templates-kansio ja suljetaan ikkuna.

Luodaan ensimmäiseksi sertifikaattipohja palvelimen autentikointiin. Konsolin oikean puoleisessa Template Display Name-ikkunasta valitaan RAS and IAS Server-pohja ja luodaan siitä kopio Duplicate Template valinnalla. Sertifikaatin voimassaoloaika on määriteltävissä General välilehdellä, ja tässä työssä valittiin 4 vuoden aikajakso. Extensions välilehdeltä tarkistetaan, että vain Server Authentication (OID-1.3.6.1.5.5.7.3.1) on valittu ja Issuance Policies on Medium Assurance. Subject välilehdeltä muutetaan Subject name format → Common name ja että vain DNS name on valittu. Security välilehdeltä tarkistetaan että RAS and IAS Servers ryhmällä on Read, Enroll ja Autoenroll oikeudet.

Seuraavaksi luodaan sertifikaattipohja käyttäjien autentikointiin. Luodaan kopio Authenticated Session-pohjasta ja määritetään sen ominaisuudet ohjeen mukaisesti. Request Handling välilehdeltä → CSP ja poistetaan valinnat kaikista Microsoft Base DSS Cryptografig Provider kohdista. Subject välilehdeltä valitaan Common name ja User Principal Name. Extensions välilehdeltä tarkistetaan, että vain

LIITE 4 (JATKUU)

Client Authentication (OID-1.3.6.1.5.5.7.3.2) on valittu ja Issuance Policies on Low Assurance. Security välilehdeltä tarkistetaan että Domain Users ryhmällä on Read, Enroll ja Autoenroll oikeudet.

Viimeiseksi luodaan sertifikaattipohja tietokoneiden autentikointiin. Luodaan kopio Workstation Authentication-pohjasta ja määritetään sen ominaisuudet ohjeen mukaisesti. Subject välilehdeltä valitaan Common name ja DNS name. Extensions välilehdeltä tarkistetaan, että vain Client Authentication (OID-1.3.6.1.5.5.7.3.2) on valittu ja Issuance Policies on Low Assurance. Security välilehdeltä tarkistetaan että Domain Computers ryhmällä on Read, Enroll ja Autoenroll oikeudet.

Sertifikaattien allekirjoittaminen ja tuominen AD:n käyttöön tapahtuu Certification Authority-työkalulla. Laajennetaan CA:n kansiot auki ja valitaan Certificate Templates → painetaan hiiren oikeanäppäin alas → New → Certificate template to Issue ja valitaan juuri luodut sertifikaattipohjat → OK ja uudet sertifikaatit ovat käytettävissä.

AD:n Automaattisen sertifikaattien jakelu

Automaattinen jakelu perustuu Group Policy määrityksiin ja IAS sertifikaattien jakelu voidaan määritellä Active Directory Users and Computers työkalun kautta. Avataan se ja valitaan domain→ hiiren oikea näppäin → properties → Group Policy välilehti. Avautuneesta ikkunasta valitaan Default Domain Policy → Edit nappi ja Group Policy Object Editor avautuu. Valitaan Computer Configuration → Windows Settings →Security Settings → Public Key Policies → Automatic Certificate Request Settings. Painetaan hiiren oikea näppäin ja valitaan → New → Automatic Certificate Request …→ next ja avautuneesta ikkunasta valitaan Computer → next → finish.

Automaattinen jakelu täytyy lisätä samassa GP-editorissa myös käyttäjien Group Policy asetuksiin. Valitaan User Configuration → Windows Settings →Security

LIITE 4 (JATKUU)

Settings → Public Key Policies → Autoenrollment Settings→ valitaan Enroll certificates automatically → OK.

Käyttäjien ja Ryhmien luonti AD hakemistopalveluun

Avataan Active Directory User and Computers työkalu ja laajennetaan auki domain-kansion alla olevat kansiot. Valitaan users kansio ja hiiren oikealla näppäimellä → New → Group → varmistetaan, että Group Scope → Global ja Group type → Security valinta painikkeet ovat valittuina. Annetaan ryhmälle sitä kuvaava nimi ja hyväksytään OK-painikkeella. Tarkoituksena oli testata RADIUS-palvelimen toimintaa eri EAP-protokollien kanssa, joten luotiin useita ryhmiä eri tarkoituksiin. EAP-PEAP-protokolla joka perustuu käyttäjä/salasana todentamiseen, vaati myös muutaman koekäyttäjä tunnuksen testausta varten.

NAS Kytkimen lisääminen IAS:aan

Avataan Internet Authentication Services työkalu ja kansion RADIUS Clients päällä hiiren oikea näppäin → New RADIUS Client. Annetaan laitetta kuvaava nimi ja sen IP-osoite → next → jos Client-Vendor alasveto valikosta löytyy laitteen valmistajan nimi, niin valitaan se. Mikäli ei laitevalmistaja nimeä löydy listalta valitaan RADIUS Standard ja toivotaan, että se on yhteensopiva tämä standardin kanssa. Alempiin lomake kenttiin kirjoitetaan IAS-palvelimen ja NAS:n käyttämä yhteinen salasana ja vahvistetaan vielä se alempaan lomakekenttään → finish.

LIITE 4 (JATKUU)

IAS Remote Access Policy

Luodaan Remote Access Policies kansioon aikaisemmin luotuja käyttäjäryhmiä vastaavat verkon käyttöön oikeuttavat määritykset. Valitaan Remote Access Policies → hiiren oikea näppäin → New → Remote Access Policy. Asennusvelho ilmoittaa avustavansa luonnissa → Next → jatketaan velhon kanssa ja annetaan Policy Name → Ethernet → Lisätään haluttu käyttäjäryhmä → seuraavaksi on valittava protokolla todentamiskäytännön mukaan. Mikäli halutaan todentaa asiakas käyttäjätunnus/salasana menetelmällä, valitaan Protected EAP (PEAP), jos käytetään sertifikaattia, niin valitaan Smart Card or other certificate → finish.

Valitaan luotu Remote Access Policy ja avataan se tuplaklikkaamalla sitä. Lisätään aikarajoitukset painamalla add-painiketta ja lisätään listasta Day-And-Time Restrictions ja määritellään Policyn sallitut käyttöaikarajoitukset. Varmistetaan että Grant remote accesss permission on valittuna. Lisätään avaamalla Edit Profile-painikkeella yhteyden kannalta tärkeät RADIUS-atribuutit. Valitaan Advanced-välilehti jossa näkyy jo valmiina Service-Type = RADIUS Standard ja sen arvo Framed. Lisätään Add-painikkella Tunnel-Medium-Type = RADIUS Standard ja sen arvo 802. Lisätään Add-painikkella Tunnel-Pvt-Group-ID = RADIUS Standard ja sen arvo on se VLAN-tunnus mihin ryhmä halutaan liittää. Lisätään vielä Tunnel-Type-atribuutti, mikä on tässä tyypiltään RADIUS Standard ja sen arvo Virtual LANs (VLAN). IAS Sertifikaattien jakelu työasemille

Avataan MMC työkalu ja ladataan Add/Remove Snap-in. Painetaan Add painiketta ja valitaan Certificates avautuneesta listasta → valitaan Computer account → Next → Local computer …→ finish → suljetaan ikkuna ja kuitataan OK. Konsolin vasemmasta ikkunasta laajennetaan Certificates (Local …) → Personal → Certificates ja valitaan sertifikaatti (Intended Purposes = All).

LIITE 4 (JATKUU)

Avataan se tuplaklikkaamalla, valitaan Details välilehti ja alareunasta Copy to File → next → Yes, export the private key→ next → Personal Informatian Exhange – PKCS #12(.PFX) ja Enable strong protection…→ next → kirjoitetaan salasana ja vahvistetaan se uudelleen → File name ruutuun kirjoitetaan sertifikaattia kuvaava nimi ja tallennuskansio → next → tarkistetaan vienti tiedot ja painetaan finish. Saadaan. Siirretään sertifikaatti työasemalle jonkin tallennusmedian avulla.

Sertifikaatin tuonti työasemalle

Avataan sertifikaatti siirtoon käytetyltä medialta kaksoisklikkaamalla sitä. Asennusvelhon Welcome to the Certificate Import Wizard sivulta jatketaan next painikkella, hyväksytään ikkunassa näkyvä sertifikaattitiedosto → annetaan exportvaiheessa annettu salasana → Next → valitaan Place all certificate in the following store → Browse → valitaan Show physical stores → valitaan yllä näkyvästä luettelosta Trusted Root Certification Authorities → Local Computer → OK → finish. The import was successfull, teksti ilmoittaa tuonnin onnistuneen.