Tomi Salo

Porttikohtainen 802.1x-todennus yritysverkossa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

20.4.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Tomi Salo Porttikohtainen 802.1x-todennus yritysverkossa 34 sivua + 1 liitettä 20.4.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Yliopettaja Matti Puska ICT-asiantuntija Antti Laaksonen

Insinöörityössä toteutettiin, Paikkatietokeskuksen tietohallinnon toimeksiannosta, IEEE 802.1x -standardin mukainen porttikohtainen todennus tutkimuslaitoksen tietoverkkoon. Tavoitteena työssä on luoda verkko, jossa käyttäjä joutuu tunnistautumaan toimialueen jäseneksi. Työssä tutustutaan RADIUS-palvelimen toimintaan: kytkimien, Windows-järjestelmän ja loppukäyttäjän näkökulmasta. Painopisteenä työssä ovat käytännön toteutus ja yliheitto.

Teoriaosuudessa tutustutaan verkkoteknologiaan, porttikohtaisen todennuksen standardiin ja protokolliin sekä Windows-palvelinympäristön toimintaan. Käytännön osuudessa luotiin aluksi testiympäristö, jonka avulla varmistetaan toimeksiannossa vaadittujen kriteerien toimivuus. Testausvaiheessa käytiin läpi verkon kytkimien ja RADIUS-palvelimen toimintaa.

Vaaditun toiminnallisuuden varmistamisen jälkeen siirryttiin valmistelemaan käytännön ympäristöä yliheittoon. Tutkimuslaitoksen sisäverkon kytkimet käytiin läpi fyysisellä tasolla ja dokumentoitiin. Tarvittavat konfiguraatiot lisättiin laitteisiin ja työntekijöitä informoitiin verkkoon kohdistuvista muutoksista. Yliheitto toteutettiin vaiheittain, mahdollisten ongelmatapauksien rajaamiseksi.

Työssä onnistuttiin konfiguroimaan vaatimusten mukainen verkko. Muutamia ongelmakohteita ilmeni yliheiton jälkeen, jotka vaativat ylläpidollisia toimenpiteitä ja soveltamista porttikohtaisen todentamisen suhteen. Lopputuloksena tutkimuslaitoksen verkko oli tietoturvan kannalta tehokkaampi ja hallittavampi.

Avainsanat	IEEE 802.1x, RADIUS, NPS, AD, EAP, Ethernet

Author	Tomi Salo
Title	Port-based 802.1x authentication in enterprise network
Number of Pages	34 pages + 1 appendix
Date	20th April 2015
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructors	Matti Puska, Principal Lecturer Antti Laaksonen, ICT Specialist

The goal of this bachelor's thesis was to study implementing changes in a institute network. Network security within the institute was in need of improvement and the decision was to implement IEEE 802.1x port-based authentication. The goal was to have the users of the network to be recognized as members of the domain, before gaining access to the network. The focus was on the practical implementation, rather than on the theoretical side.

The thesis sheds light on the port-based authentication standard, network environment, switch configuration and on the Radius authentication server. It starts out giving an idea about the theoretical side of the implementation, before moving onto the practical side. The requirements set by the IT department of FGI were first tested with the network equipment.

After the requirements were fulfilled in the test environment, it was time to move onto preparing the devices for the turnover. The employers were informed beforehand about the changes that were about to be implemented and the turnover was done gradually.

The goals of the thesis were successfully fulfilled. Few issues were raised after the turnover was complete and required some attention. The network in the research institute is now more secure and controlled.

Keywords	IEEE 802.1x, RADIUS, NPS, AD, EAP, Ethernet

Sisällys

Lyhenteet

AAA	Authentication, Authorization, Accounting. Todentaminen, valtuutus ja kirjaaminen.
AD	Active Directory. Aktiivihakemisto. Windows-järjestelmän käyttäjätietokanta.
CA	Certificate Authority. Taho, joka myöntää sertifikaatteja palveluiden käyttöön.
EAP	Extensible Authentication Protocol. Todentamisprotokolla.
EAPOL	Extensible Authentication Protocol Over LAN. Paketointitekniikka, jolla verkkolaitteet keskustelevat ilman IP-osoitetta.
Ethernet	Pakettipohjainen lähiverkkotekniikka.
GP	Group Policy. Työkalu käyttäjien ja työasemien hallintaan.
IEEE 802.1x	Porttikohtaisen todennuksen standardi.
IEEE	The Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
IP	Internet Protocol. Protokolla, joka toimittaa IP-paketteja pakettikytkentäisessä verkossa.
Kytkin	Laite, joka yhdistää pakettikytkentäisen verkon laitteita.
LAN	Local Area Network. Maantieteellisesti rajoitetulla alueella toimiva tietoliikenneverkko.
MAC	Media Access Control. Laitteen ethernet-verkossa yksilöity osoite. Liitetään yleensä valmistusvaiheessa laitteeseen.
NPS	Network Policy Server. Windows-järjestelmän RADIUS-palvelin.

OU	Organizational Unit. AD-ryhmä, jossa käyttäjillä on omat ryhmäkäytännöt.
Palvelin	Palvelimen tehtävänä on tarjota erilaisia palveluita muille verkon laitteille.
RADIUS	Remote Authentication Dial In User Service. Yleinen todennusprotokolla.
RFC	IETF-organisaation Internet-standardeihin liittyvät dokumentit.

1 Johdanto

Insinöörityön tarkoituksena oli toteuttaa tilaajan toimeksiannosta The Institute of Electrical and Electronics Engineers (IEEE) 802.1x-standardin mukainen porttikohtainen todennus yrityksen verkkoympäristöön. Työssä tutustutaan myös yrityksen tietoverkkoon kohdistuvien muutoksien läpivientiin ja niiden sujuvaan läpivientiin.

Geodeettinen laitos oli vuoden 2015 vaihteessa yhdistymässä Maanmittauslaitokseen. Yhdistyminen toi mukanaan uusia tietoturvaan liittyviä haasteita, ja yksi näistä oli tietoverkon käyttäjien hallinnointi. Tutkimuslaitoksessa käy huomattava määrä vierailijoita ympäri vuoden ja näiden vierailijoiden verkkoon pääsyyn on tehtävä rajoitteita.

Työn tavoitteena on kehittää olemassa olevaa lähiverkkoympäristöä, niin että sen käyttäjät joutuvat tunnistautumaan toimialueen jäseniksi.

Aloite Geodeettisen laitoksen perustamisesta toimitettiin eduskunnalle tammikuussa 1918. Asetus heinäkuun 5. päivänä 1918 perustettavasta laitoksesta tuli Suomen Senaatin Maatalous-toimituskunnan alainen (nyk. maa- ja metsätalousministeriö). Geodeettisen laitoksen päätehtäviin kuului ensimmäisen luokan kolmiomittaukset sekä geodeettis-tähtitieteellisen perustan täydentäminen. [1.]

Geodeettisen laitoksen rakenne on muuttunut vuosien varrella merkittävästi. Vuonna 1973 Maa- ja metsätalousministeriö asetti työryhmän selvittämään Geodeettisen laitoksen organisaation kehittämistarvetta. Mietinnössä todettiin, että vuoden 1933 toimintojen laajentumisen jälkeen, on geodesian alalla tapahtunut huomattavaa kehitystä. Uusi teknologia mahdollisti uusien tutkimustehtävien suorittamisen. [1.]

Geodeettinen laitos yhdistettiin 1.1.2015 Maanmittauslaitokseen, jossa sen toiminta jatkuu nimellä Paikkatietokeskus. Paikkatietokeskuksen organisaatiorakenne koostuu viidestä osastosta:

- geodesia ja geodynamiikka
- geoinformatiikka ja kartografia
- navigointi ja paikannus

- kaukokartoitus ja fotogrammetria
- paikkatietoinfrastruktuurin palvelut.

Paikkatietokeskuksessa sijaitsee Masalassa ja siellä työskentelee n. 120 henkilöä 12:sta eri tutkimusryhmässä. Työntekijöillä on käytössään 1—2 henkilökohtaista työasemaa sekä muutama yhteinen käytävätyöasema. Tutkimuslaitoksessa on myös useita verkkotulostimia ja muita verkkoon kytkettyjä laitteita. Kolmikerroksisessa tutkimuslaitoksessa on kymmeniä verkon aktiivilaitteita, joihin kuuluu esimerkiksi palvelimet, kytkimet, palomuurit ja varmuuskopiolaitteet. [1; 2.]

2 Verkkoteknologia

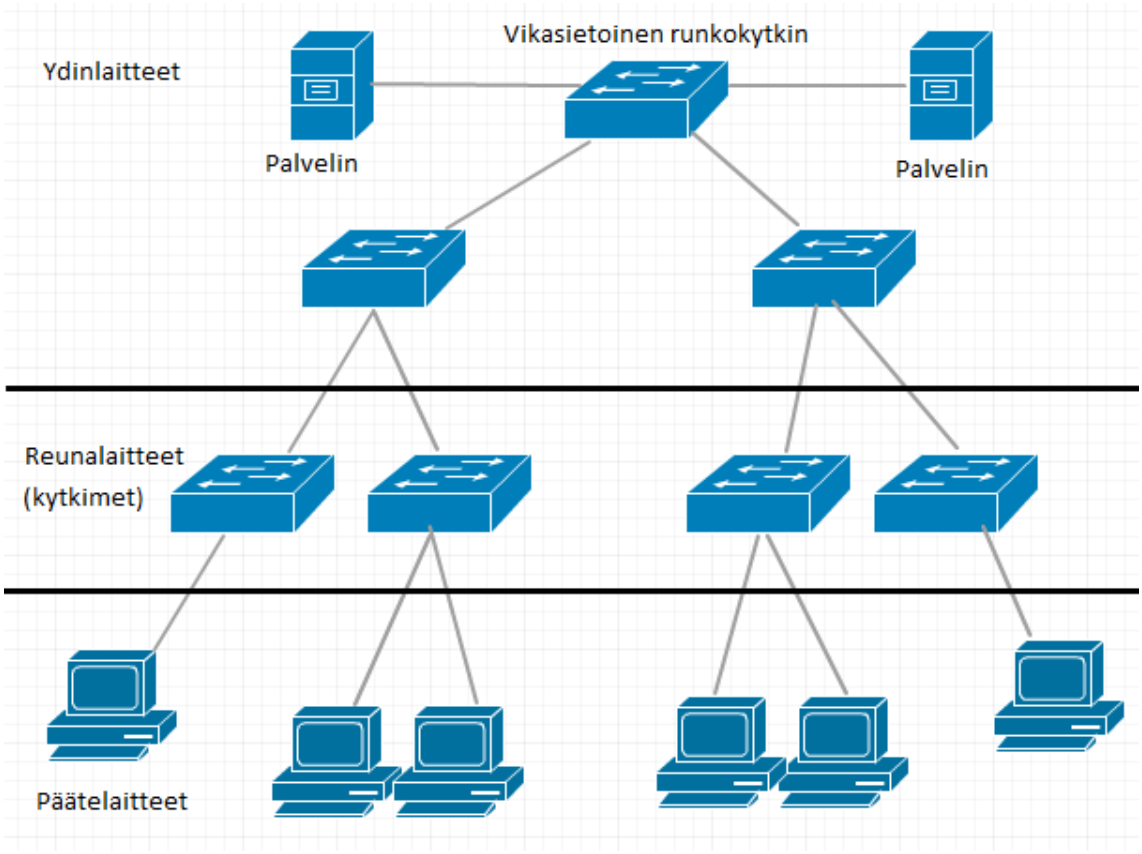
Ethernet on IEEE 802.3-standardin mukainen toteutus lähiverkossa [13, s. 139]. Ethernet on yksi suosituimmista verkon toteutustavoista nykyisin. Ethernetistä teki aikoinaan suositun sen hyvä hinta-laatusuhde, helppokäyttöisyys ja tietokonevalmistajien tuki [17]. Ethernet oli myös ensimmäinen verkon toteutustapa, joka kehitettiin teollisuustandardiksi eikä valmistajakohtaiseksi toteutukseksi [18, s.13]. Ethernetiä voidaan pitää lähes ainoana toteutustapana verkossa, jossa käytetään kytkimiä [18, s. 24].

Lähiverkolla (Local Area Network) tarkoitetaan tietoverkkoa, joka sijoittuu maantieteellisesti pieneen alueeseen, kuten vaikka yrityksen sisäinen verkko. Lähiverkon etuna on, että käyttäjät voivat olla yhteydessä jaettuihin resursseihin yrityksen sisällä. Lähiverkkoon kuuluu yleensä päätelaitteita, tulostimia, palvelimia ja muita verkkolaitteita. [13, s.65.]

Lähiverkon rakentamiseen kuuluu erilaisia laitteiden välisiä kytkentätapoja ja yhteyden muodostamiseen liittyviä standardoituja metodeja. Insinöörityössä käydään läpi työn kannalta oleellisemmat ratkaisut.

Laajaverkosta (Wide Area Network) puhuttaessa tarkoitetaan verkkoa, joka sijoittuu maantieteellisesti suurelle alueelle. Laajaverkkoja hallitsevat teleoperaattorit, ja niille on ominaista, että ne yhdistävät lähiverkkoja toisiinsa. [18, s. 5.]

Lähiverkoissa esiintyy yleisesti *hierarkkinen verkkomalli*. Sillä tarkoitetaan mallia, jossa verkkolaitteet jaetaan kahteen osaan: ydinlaitteisiin (core equipments) sekä runko- ja reunalaitteisiin (edge equipments) niiden vikasietoisuuden mukaan. Ydinlaitteisiin kuuluvat tehokkaammat ja vikasietoisemmat kytkimet, joihin verkon palvelut ovat kytkettyinä. Reunalaitteisiin kytketään taas verkon päätelaitteet. Kuvassa 1 on hahmoteltu hierarkkinen verkkomalli. [18, s. 280.]



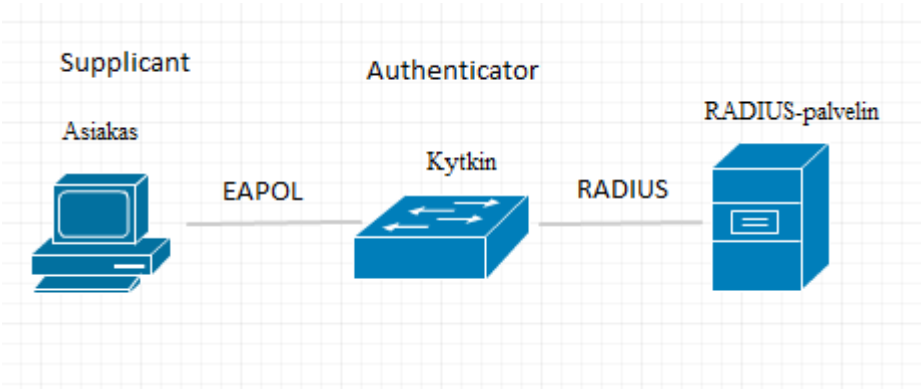
Kuva 1. Hierarkkinen verkkomalli.

Hierarkkisen verkkomallin käytettävyyttä voidaan tehostaa vielä luomalla varayhteyksiä kytkinten välille, jolloin pääsy lähiverkon tärkeisiin palveluihin ei ole esimerkiksi vain yhden runkokytkimen varassa [18, s. 175]. Insinöörityön tietoverkkoa voidaan verrata kuvassa 1 esitettyyn hierarkkiseen verkkomalliin.

Virtuaalinen lähiverkko (Virtual Local Area Network) on kytkintekniikka, jossa kytkimiin kytketyt laitteet voidaan jakaa omiin ryhmiinsä kytkinverkossa. Virtuaalisella lähiverkkotekniikalla, eli lyhyemmin VLAN-tekniikalla, voidaan esimerkiksi kasvattaa lähiverkon tietoturvaa jakamalla päätelaitteita omiin VLAN-alueisiin, jolloin lähiverkkoliikennettä voidaan rajoittaa vain niille työasemille, jotka kuuluvat kyseisen liikenteen piiriin. VLAN-tekniikka on Ethernet-toteutuksessa olennainen osa verkon toimintaa, vaikka se insinöörityön toteutuksessa jääkin vähemmälle huomiolle — johtuen tutkimuslaitoksen VLAN-määrityksistä.

3 IEEE 802.1x

802.1x-porttikohtainen todennus on IEEE:n määrittelemä standardi, jossa määritellään asiakkaan ja palvelimen välinen hallinta, joka estää luvattomien käyttäjien pääsyn lähiverkkoon. Todennuspalvelin todentaa jokaisen käyttäjän, joka on yhdistettynä kytkinportiin ja asettaa portille VLAN-arvon ennen kuin antaa käyttäjälle luvan verkon palveluihin. Ennen käyttäjän todentamista portissa on sallittuna vain Extensible Authentication Protocol Over LAN (EAPOL) -liikenne. Todennuksen jälkeen verkkoliikenne liikkuu normaalisti. [14.]



Kuva 2. 802.1x porttikohtainen todennus

Kuvassa 2 esitetään porttikohtaisen todennuksen asiakas-palvelin suhdetta. Asiakas, eli tässä tapauksessä päätelaite, pyytää saada yhteyden verkkoon todentavalta kytkimeltä. Kytkin pyytää asiakkasta tunnistautumaan ja vertaa asiakkaan tietoja, tässä tapauksessa, RADIUS-palvelimen kanssa. Jos kaikki vaaditut ehdot ovat tosia, muodostuu verkkoyhteys, mutta muussa tapauksessa yhteydenottopyyntö hylätään. [14.]

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) on todennuksessa käytetty konsepti, joka tukee esimerkiksi langatonta ja langallista todennusta. EAP:ssa voidaan hyödyntää salasana- tai sertifikaattipohjaista todennustapaa. EAP:lla päätelaite ja asiakaskytkin keskustelevat keskenään ilman Internet Procotol (IP) -osoitetta. [11; 19.]

Työssä käydään läpi toteutuksen kannalta oleellisia EAP-tyyppejä, ilman että jokainen protokolla eriteltäisiin. Toteutuksessa päädyttiin tiettyyn protokollaan, koska sille oli verkon aktiivilaitteiden tuki ja tarkoituksena oli saada käyttäjäkohtainen todennusympäristö.

Protected Extensible Authentication Protocol (PEAP) on yksi EAP-kehyksessä käytettävistä protokollista. PEAP käyttää Transport Layer Security (TLS) -istuntoa luodessaan salatun yhteyden käyttäjän ja todennuspalvelimen välille. PEAP on yleinen Windows-järjestelmissä ja se tukee 802.1x-todennettuja langattomia tukiasemia sekä 802.1x todentavia kytkimiä. [12.]

PEAP ei määrää todennusmenetelmää, vaan se voi tarjota lisäturvaa muille EAP-protokollille. PEAP:ia käytetään EAP-TLS- tai EAP-Microsoft Challenge-Handshake Authenticator Protocol version 2 -protokollien kanssa. [12.]

Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAPv2) -protokollaa käytetään käyttäjäkohtaisessa todennuksessa. MS-CHAP v2 -protokolla on yksi PEAP:n kanssa käytetyistä protokollista. [9.]

MS-CHAP v2 -protokolla on myös ainoa protokolla, joka tukee vanhenevan toimialuesalasanan vaihtamista, mutta siihen tarvitaan verkon asiakaskytkimien tuki. Insinöörityössä käytetään PEAP-MS-CHAPv2-protokollaa [12].

4 AAA-malli

Authentication, Authorization and Accounting (AAA) on arkkitehtuurinen kehysmalli, jossa kolme tietoturvamenetelmää (todentaminen, valtuutus ja kirjaaminen) sidotaan yhdeksi kokonaisuudeksi [15, s. 57]. AAA-mallin vahvuuksiin kuuluvat:

- joustavuus ja määrittelyn hallinta
- skaalautuvuus
- standardoidut todennusmenetelmät, kuten Remote Authentication Dial-In User Service (RADIUS) ja Terminal Access Controller Access-Control System Plus (TACACS+)
- useat eri varmuuskopiojärjestelmät. [15, s.60.]

Todentamisprosessissa (Authentication) käyttäjä tunnistetaan ennen verkkoyhteyden luontia. Käyttäjän tunnistamiseen voidaan käyttää eri metodeita, jotka liitetään todennettaviin rajapintoihin. [15, s. 57.]

Valtuutusprosessissa (Authorization) todennetulle käyttäjälle annetaan ominaisuuksia, joiden mukaan käyttäjä saa luvan toimia verkossa. RADIUS-todennuksessa valtuutuksen hoitaa yleensä RADIUS-palvelin, johon käyttäjää koskevat valtuutukset ovat määritelty. [15, s. 58].

Kirjaamisessa (Accounting) kerätään tietoa verkon käyttäjistä. Verkon tapahtumat kirjautuvat esimerkiksi RADIUS-palvelimelle. Kirjattaviin tapahtumiin kuuluvat muun muassa: verkon käyttäjien tiedot, valtuutukset ja toiminnat. Kirjaaminen voidaan tutkia myös verkon palveluiden käyttöä ja sen kuormittumista. Työssä kirjaamisen hoitaa toimialueohjaimen Event Viewer -näkymä. [15, s. 58.]

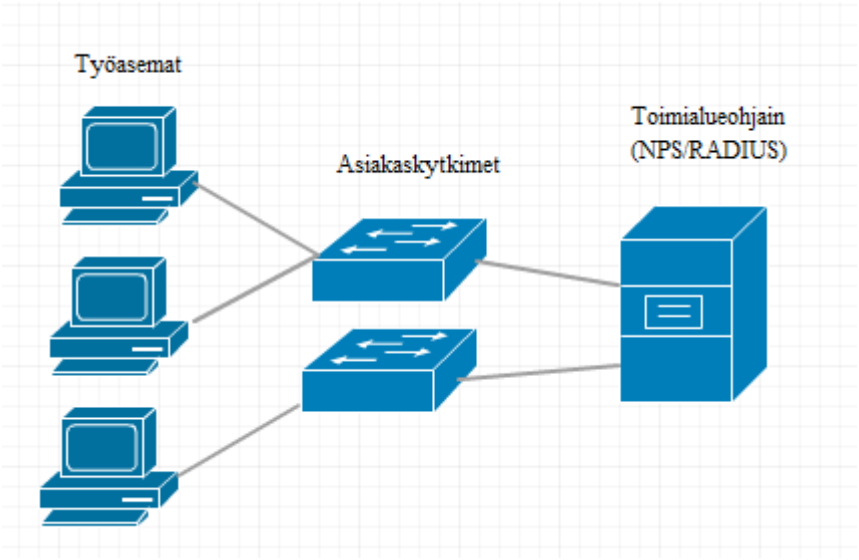
Remote Authentication Dial-In User Service (RADIUS) on yleinen asiakas-palvelin järjestelmä, joka suojaa tietoverkkoa luvattomalta käytöltä. RADIUS on standardin mukainen järjestelmä, joka voidaan muokata mihin tahansa turvaympäristöön [15, s. 151]. RADIUS-järjestelmiä käytetään monissa erilaisissa verkkoympäristöissä, jotka vaativat korkean tason tietoturvaa. [15, s. 152.]

Käytännössä RADIUS-järjestelmä toteuttaa AAA-mallin mukaista menettelyä. RADIUS-palvelin järjestelmä hyödyntää siihen liitettyjä asiakaskytkimiä, erillistä käyttäjätietokantaa, kirjaamista ja säännöksiä, toteuttaessaan tietoverkon hallintaa. [16; 20.]

5 Toimialueympäristö

Käyttöjärjestelmät

Tutkimuslaitoksen työasemissa on oletuksena Windows 7 -käyttöjärjestelmä, ja toimialueen palvelimet käyvät Windows Server 2008 -käyttöjärjestelmällä. Ympäristössä on myös esimerkiksi Linux-virtuaalipalvelimia, mutta tässä työssä keskitytään lähinnä tutkimuslaitoksen Windows-maailman toimintaan. On tärkeää saada kuva työympäristön toiminnasta RADIUS-todennuksen kannalta. Kuvassa 3 on hahmoteltu esimerkki RADIUS-todennusta käyttävä verkkoympäristö Microsoft-järjestelmillä.



Kuva 3. RADIUS-ympäristö Microsoft-palvelinympäristössä.

Active Directory Domain Services

Active Directory Domain Services (AD DS) on Windows Server 2008:aan lisättävä palvelinrooli, joka toimii toimialueen runkopalveluna. Aktiivihakemistoa voidaan pitää myös RADIUS-palvelimen runkona, koska verkkoon pääseminen vaatii käyttäjältä osallisuutta toimialueeseen. [3.]

Aktiivihakemistoon liitetään toimialueen käyttäjät ja ylläpitäjät. Yksittäisellä käyttäjällä on käyttäjätunnus ja salasana. Käyttäjät voidaan sitoa ryhmiin ja näille ryhmille voidaan asettaa omia sääntöjä. Perustasolla voidaan rajoittaa käyttäjän oikeuksia vaikka toimialueen tiedostoihin. [3.]

Network Policy and Access Services

Network Policy and Access Services (NPAS) on palvelinrooli, joka sisältää seuraavat tietoturvaan liittyvät työkalut:

- Network Policy Server (NPS)
- Routing and Remote Access Service (RRAS)
- Health Registration Authority (HRA)
- Host Credential Authorization Protocol (HCAP). [4.]

Windowsin RADIUS-palvelimena toimii tässä tapauksessa NPS. Windows Server 2008 Standard -version NPS-roolissa ei ole suuria toiminallisia eroja. Standard-versiossa voidaan määritellä enintään 50 kytkintä RADIUS-palvelimeen ja kaksi etäpalvelinryhmää. Standardia uudemmissa versioissa ei ole rajoituksia näiden määrien suhteen. [5.]

RADIUS-palvelimena toimiessaan NPS tarjoaa keskitettyä verkkoon pääsyn hallintaa. NPS:stä voidaan asettaa verkon käyttäjille ehtoja, joiden täyttyessä, käyttäjä saa pääsyn verkkoon. [6.]

Group Policy

Toimialueessa ryhmäkäytäntö mahdollistaa aktiivihakemistoon liitettyjen päätelaitteiden ja käyttäjien asetuksien hallinnan. Ryhmäkäytännöstä voidaan esimerkiksi asettaa määrityksiä käyttäjille ja päätelaitteille, rekisteripohjaisia käytäntöjä, turva-asetuksia, ohjelmistojen käyttöönottoja sekä muita toimialueeseen liittyviä asetuksia.

Käytännössä ryhmäkäytännössä luodaan ryhmäkäytäntöobjekti (Group Policy Object) ja objekti liitetään omaan organisaatioyksikköön (Organizational Unit). Insinöörityössä on käytössä vain Default Domain Policy, joten työasemia ei ole eroteltu organisaatioyksiköihin. [7.]

Certificate Authority

Insinöörityössä käytetään palvelinvarmennetta, koska valittu EAP-protokolla vaatii sen toimiakseen. Itse käyttäjiä ei työssä tunnisteta varmenteen avulla, vaan käyttäjien täytyy luoda luottosuhde toimialueeseen, jotta yhteys muodostuisi. [10.]

Toimialueen varmenne oli luotu ennen työn aloittamista, ja sen rooli on melko vähäinen, joten sen toiminnallisuus ei ole työn kannalta oleellista. Varmennetta sivutaan muutamassa työhön liittyvässä vaiheessa.

6 Käytännön toteutus

6.1 Yleinen suunnitelma

Ensimmäisenä työvaiheena käytännön toteutuksessa oli tutustuminen yrityksen verkkoon ja sen aktiivilaitteisiin. Käytännössä osa Geodeettisen laitoksen infrastruktuurista oli siirtymässä Maanmittauslaitoksen vastuulle, joten oli tärkeää saada kattava kokonaiskuva yrityksen infrastruktuuriin kohdistuvista muutoksista, ja kuinka nämä muutokset tulevat vaikuttamaan yritykseen jäävään verkkoon.

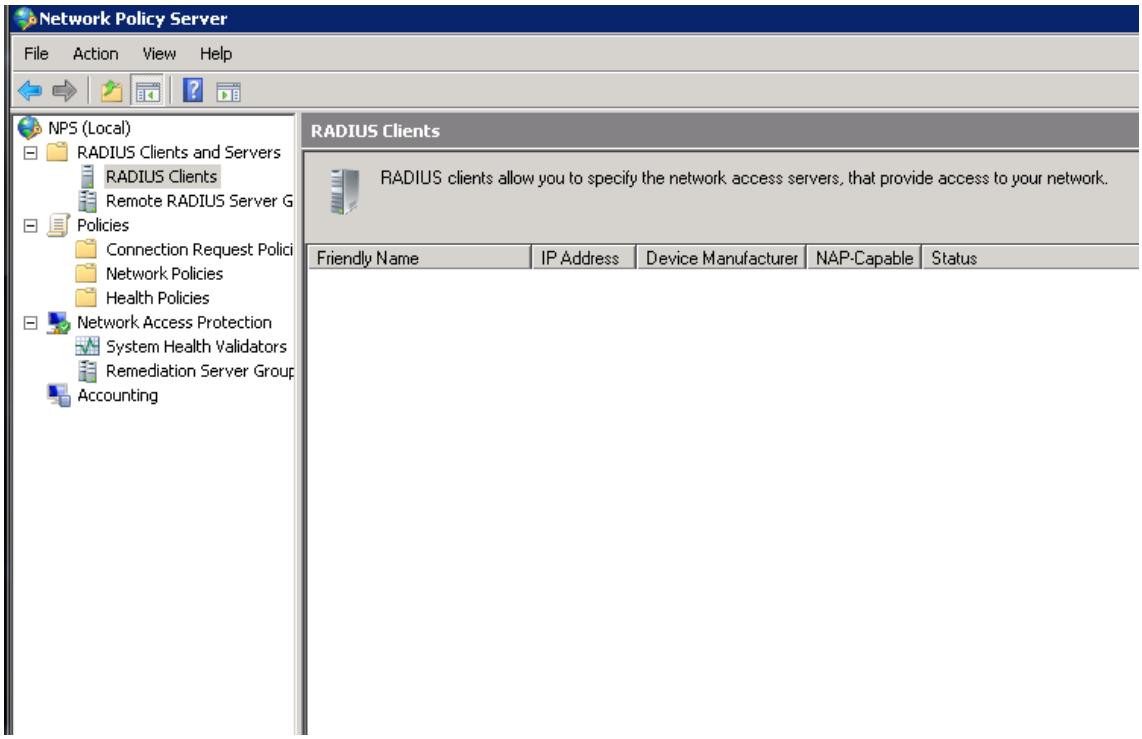
Lopulta ratkaisu oli jättää Geodeettisen laitoksen sisäinen verkko ennalleen, jolloin porttikohtaisen todennuksen tuominen yrityksen nykyiseen järjestelmään oli käytännössä tehokkain ratkaisu. RADIUS-palvelimena toimisi ympäristössä jo käytössä oleva toimialueohjain ja verkkotopologia pysyisi ennallaan. Kytkimet dokumentoitaisiin ja valmisteltaisiin ennen RADIUS-todennuksen käyttöönottoa.

Suunnitteluvaiheessa tuli myös esille tarve antaa vain toimialueen käyttäjille mahdollisuus verkkoyhteyteen. Tutkimuslaitoksella on toiminnassa langaton vierasverkko, jolla tarjotaan vieraille mahdollisuus Internet-yhteyteen.

6.2 RADIUS-palvelin

RADIUS-palvelimena insinöörityössä toimii esiasennettu palvelinrooli toimialueenohjaimessa (Domain Controller), Network Policy Server. Network Policy Server sopii hyvin työssä käytettäväksi RADIUS-palvelimeksi, koska sillä on luonnollinen tuki Windows-ympäristöön, ja se ei vaadi myöskään yritykseltä hankintoja tai palvelinmuutoksia.

RADIUS-palvelimella on käyttöjärjestelmänä Windows Server 2008 Standard ja sen runkona ovat aktiivihakemisto ja ryhmäkäytäntö. Toimialueeseen on myös luotu oma varmenne, joka on ollut aikaisemmin langattoman verkon käytössä. Kuvassa 4 on NPS:n käyttöliittymä.



Kuva 4. Network Policy Server -käyttöliittymä.

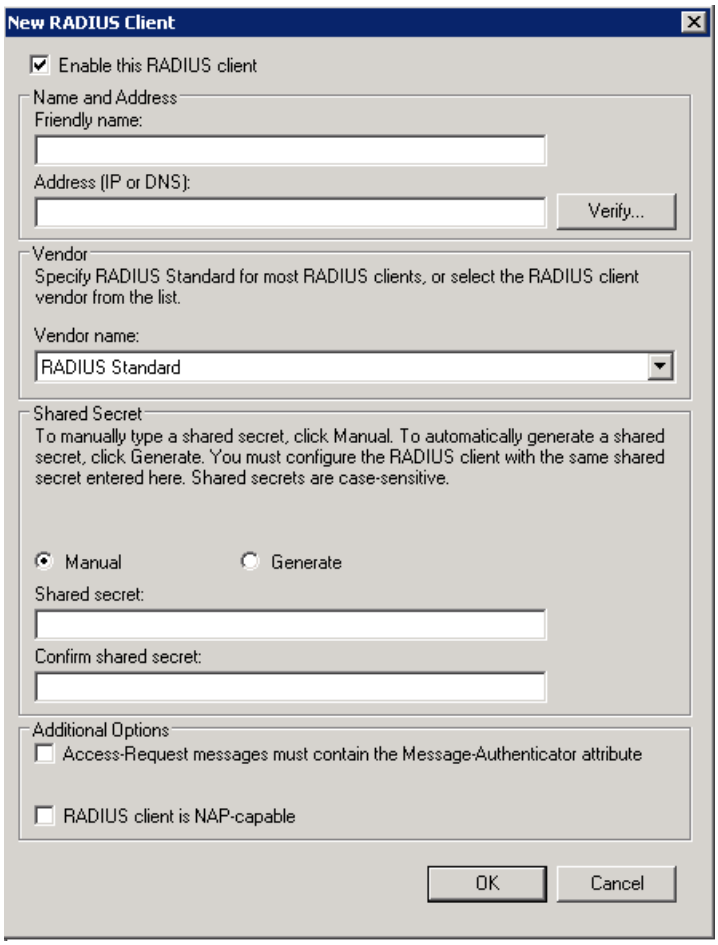
6.3 Kytkimien liittäminen palvelimeen

Insinöörityössä tutkittiin aluksi kytkimien toimintaa, määrittelyä ja lisäämistä asiakkaiksi RADIUS-palvelimeen. Toimialueessa oli noin kymmenen kytkintä, jotka kaikki kuuluivat HP:n 2000-sarjaan. Kytkinmallien välillä ei todettu merkityksellisiä toiminnallisia eroja, vaan käytännössä kytkimen määrittäminen oli lähes kaikissa tapauksissa sama.

Kytkimien konfiguraatioihin tutustuttiin valmistajan julkaisemien dokumentaatioiden avulla. Testauksessa käytettiin jo käytöstä poistettua HP:n 2000-sarjan kytkintä. Kytkimeen lisättiin komentoriviltä RADIUS-palvelimen osoite ja avain, jonka avulla kytkin ja palvelin tunnistavat toisensa:

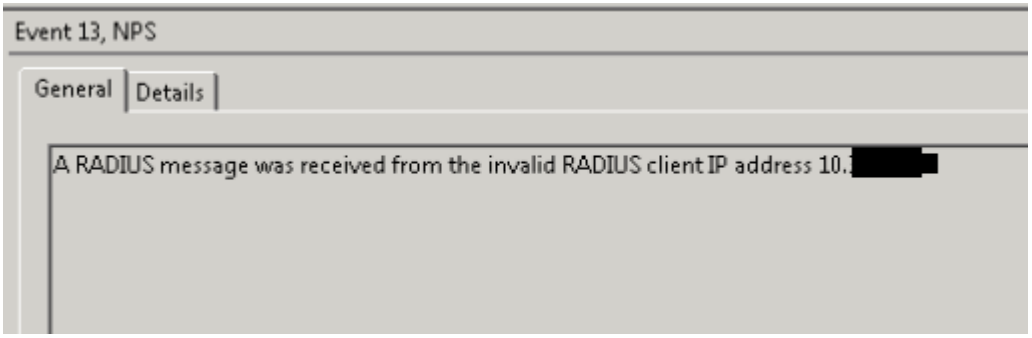
```
#radius host <IP-osoite> key <avain>
```

Komennon antamisen jälkeen kytkin pitää lisätä myös RADIUS-palvelimelle. Vain kytkimet, jotka NPS tunnistaa asiakaskytkimikseen voivat toimia todennuksessa. Kuvassa 5 RADIUS-asiakaskytkimelle annetaan nimi, lisätään määritettävän kytkimen IP-osoite ja sama avain, joka on määritelty kytkimen konfiguraatiossa.



Kuva 5. Uuden RADIUS-kytkimen lisääminen.

Kytkin on tämän jälkeen lisätty RADIUS-palvelimeen. Varsinaista asiakaskytkimen ja palvelimen välistä toimivuutta ei voi NPS:ssä testata muuten kuin New RADIUS Client -välilehden Verify-komennolla. Verify-komento ei kerro lopullista toimivuutta vaan lähinnä ovatko Internet Control Message Protocol (ICMP) -kyselyt sallittuja. Windows Server -palvelimissa on käytössä Event Viewer -näkymä, jossa voidaan tutkia erilaisia toimialueeseen ja verkkoon liittyviä lokitietoja. Event Viewer ei anna mainintaa yhteyden toimivuudesta, ainoastaan virhetilanteen syntymisestä. Esimerkkinä kuvassa 6 on väärän jaetun salasanan kokeilu:



Kuva 6. Virheellinen kytkimen konfiguraatio.

Voidaan todeta, että jos Event Viewer -näkymään ei synny virheilmoitusta ja kytkin löytyy NPS:n Verify-komennolla, on yhteys toiminnassa. Kytkimeltä on mahdollista tarkastella palvelinasetuksia komennolla `show radius`. Kuvassa 7 esitetään kytkimen tuloste komennosta.

```
gsw-l3# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- --------------------------------
  10. [redacted]      1812  1813  [redacted]


gsw-l3#
```

Kuva 7. Show radius -komento.

Kytkimen ja palvelimen välisissä virhetilanteissa `show radius` -komento auttaa tarkastelemaan kytkimelle syötettyjä RADIUS-palvelimen tietoja. Kuvassa 7 nähdään esimerkiksi palvelimen IP-osoite ja annettu salausavain tekstimuodossa.

6.4 Porttikohtaisen todennuksen testaaminen

Seuraavaksi kytkimeen määriteltiin porttikohtaiseen todennukseen liittyvät komennot:

```
#aaa port-access authenticator <numero>

#aaa port-access eap-radius
```

Ensimmäisellä komennolla valittiin yksittäinen portti kytkimestä, josta testaaminen suoritetaan. Porttiin kytketään fyysisesti testaukseen käytettävä kone. Toisella komennolla valitaan EAP-RADIUS todennustavaksi. Porttikohtainen todennus täytyy vielä näiden jälkeen aktivoida komennolla:

```
#aaa port-access authenticator active
```

Ensimmäisellä testauskerralla todettiin, että jos on kytkettynä porttiin, joka aktivoidaan porttikohtaiseen todennukseen, katoaa myös etähallintayhteys kytkimeltä.

Kytkimeltä voidaan tarkastella todennettuja portteja komennolla `show port-access authenticator`.

```
gsw-l3(config)# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes

       Auths/  Unauth   Untagged Tagged          Cntrl
  Port Guests  Clients  VLAN     VLANs  Port COS  Dir
  ---- ------- -------- -------- ------ --------- -----
  2    0/0     0        0        No     No        both
  3    1/0     0        1        No     No        both
  4    1/0     0        1        No     No        both
  5    0/0     0        0        No     No        both
  6    1/0     0        1        No     No        both
  8    0/0     0        0        No     No        both
  9    0/0     0        0        No     No        both
  11   1/0     0        1        No     No        both
  12   0/0     0        0        No     No        both
  13   1/0     0        1        No     No        both
  15   1/0     0        1        No     No        both
  17   0/0     0        0        No     No        both
  18   0/0     0        0        No     No        both
```

Kuva 8. Todennetut käyttäjät kytkimellä.

Kuvassa 8 on testaamisen jälkeen kaapattu tuloste valmiista kytkimestä. Tulosteesta voidaan kuitenkin tarkastella porttikohtaisesti todennettuja käyttäjiä. Auths/Guests-sa-

rakkeessa näkyy todennettujen käyttäjien määrä porttia kohden. Yksinkertaistettuna tuloste siis kertoo, onko kyseisestä kytkimestä yhdistynyt lähiverkkoon käyttäjä, joka on läpäissyt porttikohtaisen todennuksen vaatimukset.

Kytkimen konfiguraation jälkeen lisätään NPS:ään Connection Request Policy -sääntö. Säännöksi lisättiin, että käyttäjä on yhteydessä Ethernet-portin kautta. Työssä hallinnoidaan Ethernet-porttien kautta lähiverkkoon liittyviä käyttäjiä, jonka takia kyseinen sääntö määriteltiin.

Jos kaikki RADIUS-palvelimella asetetut ehdot ovat tosia, kun päätelaite kytketään todennettuun porttiin, pitäisi verkkoyhteyden muodostua. Yhdistettyjä laitteita voidaan vielä tarkastella kytkimeltä komennolla:

```
#show port-access authenticator <portit> statistics.
```

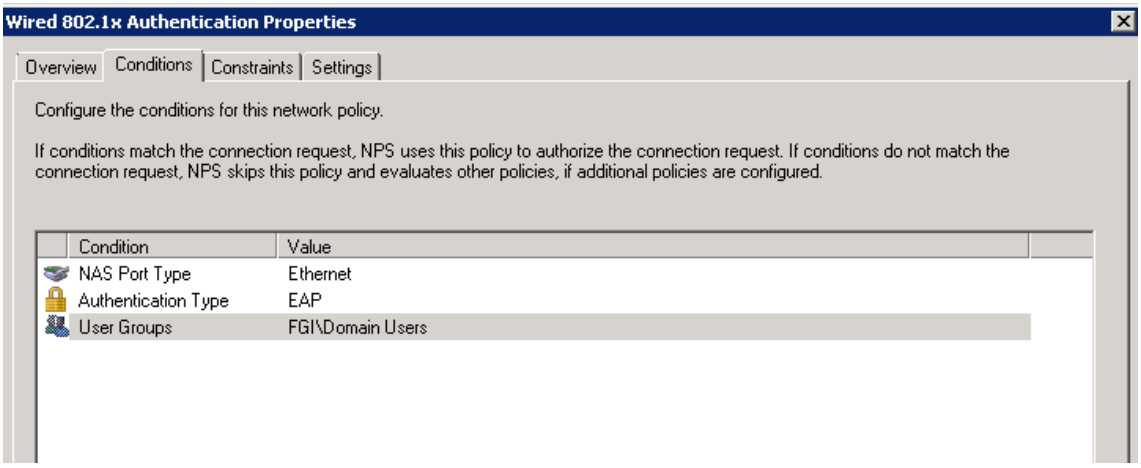
Komennolla voidaan tunnistaa todennettuja laitteita esimerkiksi niiden MAC-osoitteen avulla.

```
gsw-l3(config)# show port-access authenticator 2-6 statistics

 Port Access Authenticator Statistics

  Port-access authenticator activated [No] : Yes

       Source        TX      TX      RX      RX      RX      RX      RX
  Port MAC address   ReqId   Req     Start   Logoff  RespId  Resp    Errors
  ---- ------------- ------ ------ ------- ------- ------- ------- -------
  2                  0      0      0       0       0       0       0
  3    5c9[redacted] 690    585    379     0       259     570     0
  4    e01[redacted] 165393 1274   2240    0       835     1176    0
  5    001[redacted] 402    286    123     0       105     274     0
  6    901[redacted] 66610  319    53      0       80      319     0
```

Kuva 9. Kytkimeen yhdistettyjen laitteiden tietoja.

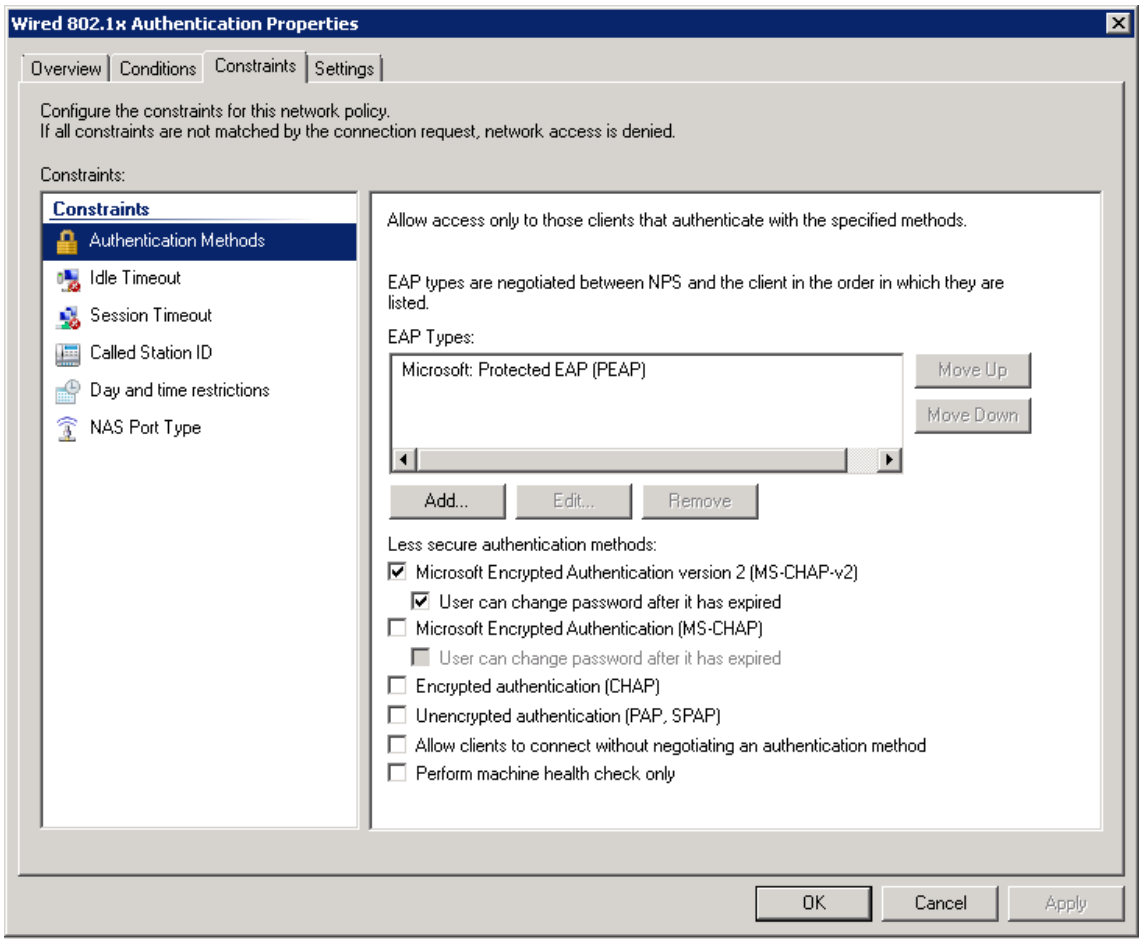
6.5 Yhteensopivuus aktiivihakemiston kanssa

Lopuksi testattiin aktiivihakemiston yhteensopivuutta RADIUS-palvelimen kanssa. Kuvassa 10 NPS:n Network Policies -välilehteen lisättiin ehto, että päätelaitteella täytyy kirjautua toimialueeseen kuuluvalla käyttäjätunnuksella.



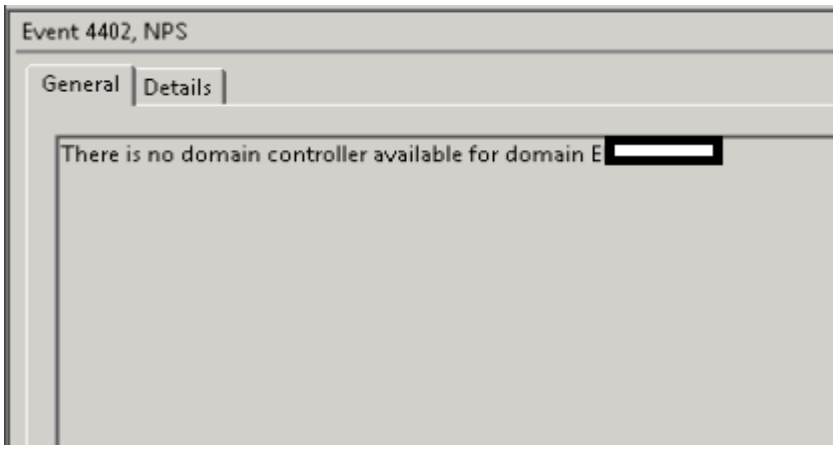
Kuva 10. Toimialue-ehdon lisääminen.

Network Policies -välilehdessä myös asetettiin ehtojen toteutumisen jälkeen käyttäjälle määriteltävät asetukset. Näissä asetuksissa määritellään käytännössä työssä käytetyt protokollat ja todennustavat. Kuvassa 11 nähdään, että EAP-tyypiksi on valittu PEAP-MS-CHAP v2 -protokolla. Todennustyypin valintaan päädyttiin, koska sille oli tuki lähiverkon laitteilla.



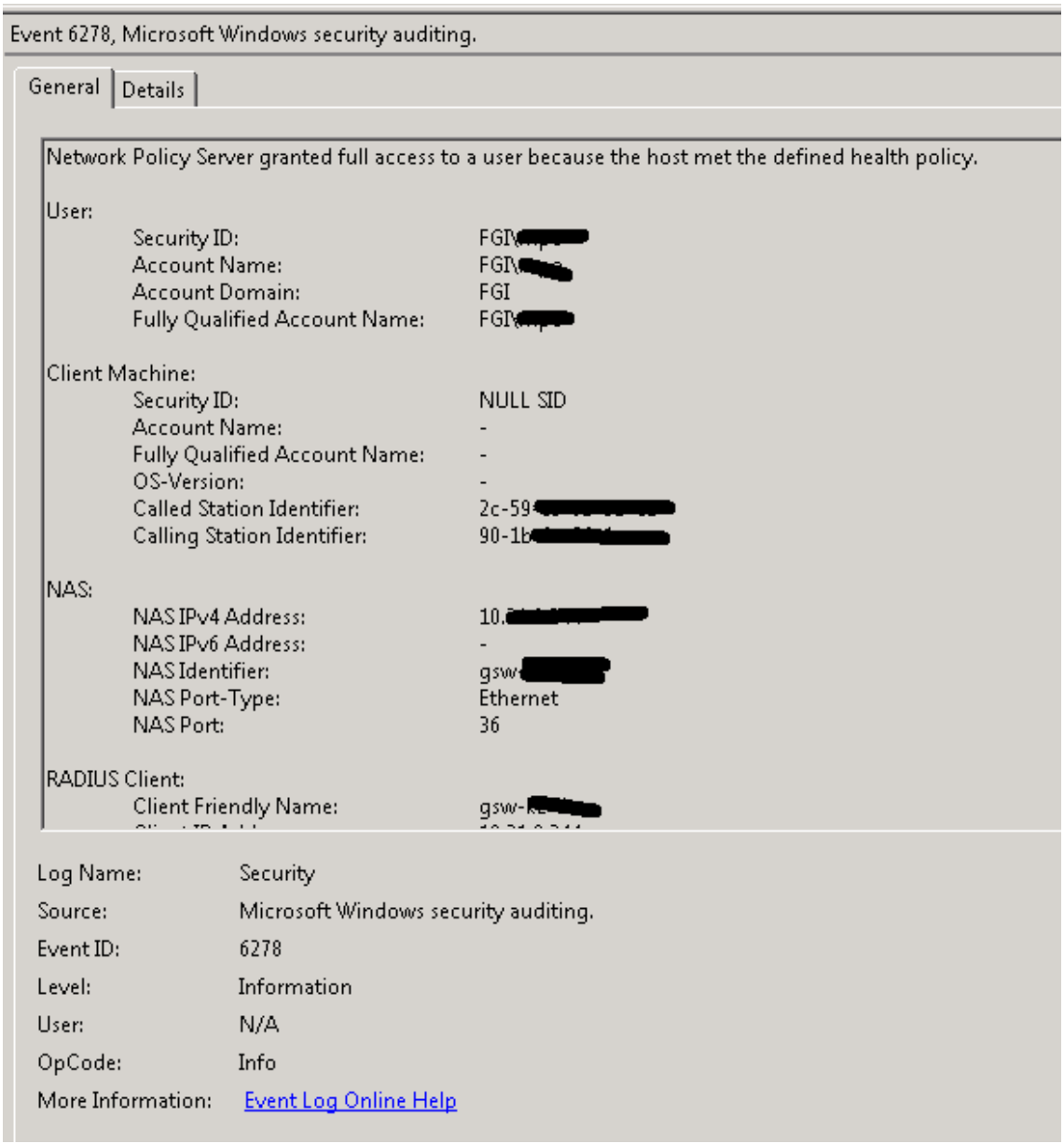
Kuva 11. Käyttäjien asetuksien määrittely.

Käyttäjäkohtaista todennusta testattiin päätelaitteen paikallisella käyttäjätunnuksella, jolloin todettiin, että yhteys ei muodostu, kuten kuvassa 12. Syynä käyttäjän hylkäämiseen on se, ettei kyseistä tunnusta löydy toimialueen aktiivihakemistosta.



Kuva 12. Event Viewer -näkymän virhe yhdistettäessä paikallisesti.

Toimialueeseen kuuluva käyttäjä saa ehtojen täyttyessä verkkoyhteyden, kuten kuvassa 13.



Kuva 13. Event Viewer: porttitodennuksen läpäissyt käyttäjä.

User-kohdassa nähdään käyttäjää koskevat tiedot ja NAS-kohdassa asiakaskytkin, josta käyttäjä on yhdistänyt. Käyttäjän täytettyä vaaditut ehdot RADIUS-palvelin asettaa kohteelle NPS:n Network Policies -määrityksissä asetetut ehdot.

Todennusta suunnitellessa tuli esille, että on tärkeää saada pelkästään toimialueeseen kuuluvat käyttäjät läpäisemään porttikohtainen todennus. Työssä olisi ollut mahdollista

käyttää konekohtaista todennusta, mutta koska muutamilla tutkijoilla on paikalliset ylläpitötunnukset, haluttiin mahdollistaa ainoastaan toimialueeseen kuuluvilla tunnuksilla verkkoyhteys. Paikalliset ylläpitotunnukset ovat käytössä, koska tutkijoilla on käytössään muutamia ohjelmia, jotka vaativat ylläpito-oikeuksia.

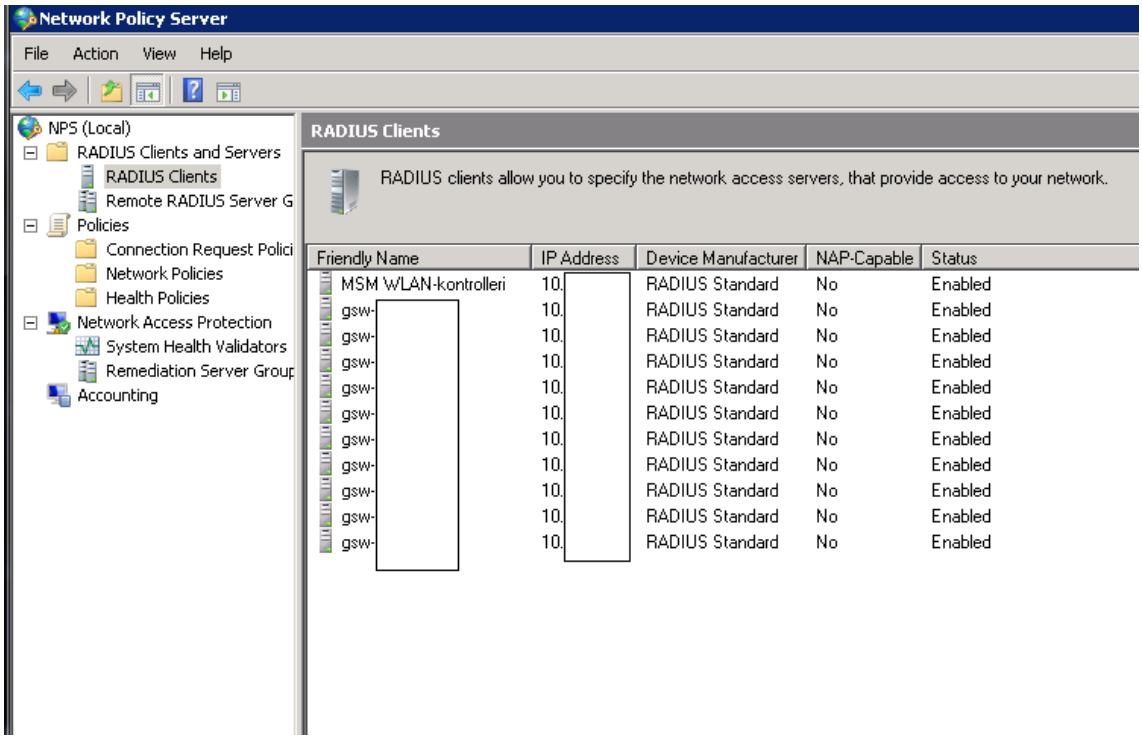
Testausvaiheen jälkeen voitiin todeta, että Paikkatietokeskuksen vähimmäisvaatimukset todennuksen suhteen pystyttiin täyttämään ja seuraavaksi siirryttäisiin suunnittelemaan varsinaista yliheittovaihetta. Porttikohtaisen todennuksen ympäristöä voidaan muokata tehokkaammaksi, kun perustoiminnallisuus saadaan tutkimuslaitoksen verkossa kuntoon tai kun se on ajankäytöllisesti mahdollista.

6.6 Yliheitto

Vaikka porttikohtaisen todennuksen konfigurointi oli suhteellisen helppoa, ei kuitenkaan sen tuominen Paikkatietokeskuksen kokoiseen yritykseen ollut niin helppoa. Aluksi oli tärkeää kartoittaa, mitä on kytkettynä tutkimuslaitoksen kytkimiin. Laitoksella oli kytkimiin liittyvät dokumentaatiot, mutta niiden ajankohtaisuudesta ei ollut varmuutta. Paikkatietokeskuksessa on monia geodesiaan ja muihin tutkimusaloihin liittyviä tärkeitä tietoteknisiä laitteita, joiden toimivuuden takaaminen oli erityisen tärkeää. Tärkeää oli myös kartoittaa, että esimerkiksi tulostimet ja langattoman verkon tukiasemat (Access Point) olivat todennuksen ulkopuolella.

Käytännössä päädyttiin kartoittamaan, mihin portteihin on kytketty loppukäyttäjä ja mihin muita tietoverkkoon kuuluvia laitteita sekä dokumentoimaan nämä tulokset. Kolmikerroksisen tutkimuslaitoksen tietoverkon kaapeloinnin dokumentoimisessa meni muutamia päiviä. Kytkimistä myös siivottiin turhat kaapelit ja kytkentöjen logiikkaa selvennettiin.

Porttikohtaiseen todennukseen siirtymisestä tiedotettiin laitoksen sisällä, kuten liitteessä 1 mainitaan. Kaikki konfiguroitavat kytkimet liitettiin RADIUS-palvelimeen ja kytkimiin lisättiin todennettavat portit ja protokollat.



Kuva 14. NPS-palvelimen kytkimet.

Yliheitto suunniteltiin alkavaksi 16.12.2014, kuten liitteessä 1 todetaan. Yliheitto on parasta toteuttaa vaiheittain, jotta mahdolliset ongelmat on helppo paikallistaa. Tutkimuslaitoksen noin kymmenen porttikohtaiseen todennukseen osallistuvaa kytkintä aktivoitiin yksi kerrallaan komennolla `aaa port-access authenticator activate`.

Aktivoinnit tehtiin toimistotyöajalla, koska oli tärkeää saada mahdolliset verkkoyhteysongelmat ratkaistua samalla kun niitä ilmenee. Yksittäisen aktivoimisen jälkeen tarkkailtiin RADIUS-palvelimen log-tietoja Event Vieweristä ja tämän jälkeen paikan päällä. Yliheiton suorittamisen jälkeen todennuksia valvottiin vielä muutamia viikkoja, koska kaikki työntekijät eivät olleet laitoksessa yliheiton aikaan.

7 Yhteenveto

Lähdin etsimään insinöörityötä, jossa saisin tehdä käytännön toteutusta yritykselle. Minusta oli tärkeää saada tehdä tietotekniikan alaan liittyvää kehitys- tai käyttöönottotyötä oikeassa ympäristössä, mittakaavassa ja oikeilla laitteilla. Insinöörityön aiheeksi etsin tietoverkkoihin liittyvää työtä.

Sain toimeksiannon toteuttaa RADIUS-todennuksen Geodeettisen laitoksen verkkoon. Olin IT-harjoittelijana Geodeettisella laitoksella aikaisemmin, joten oli luonnollista kysyä mahdollisuuksista insinöörityön toteuttamiseen. Luultavasti sain sitä kautta myös enemmän vastuuta ja mahdollisuuden itsenäiseen työhön.

7.1 Suunnittelu ja aiheeseen tutustuminen

RADIUS-todentaminen oli aikaisemmin vain pintapuolisesti käyty läpi opinnoissani, joten en ollut siihen aikaisemmin perehtynyt. Tutkimuslaitoksen verkkoon toteutettava todennus antoi loistavan mahdollisuuden perehtyä siihen, kuinka käytännössä yrityksen verkkoon tehdään muutoksia. Paikkatietokeskus antoi toimeksiannossa tietyt rajaukset, kuinka verkon tulisi toimia. Loput toiminnallisuudesta ja optimoimisesta olisivat minun sovellettavissa.

Tutkimuslaitoksen verkkoon ja sen laitteisiin tutustumiseen ei työssä tarvinnut käyttää aikaa, koska se oli jo tuttu harjoitteluajalta. Tulee kuitenkin muistaa, että laitoksen verkko on jo suhteellisen isokokoinen, ja sen ymmärtämiseen meni harjoitteluaikana aikaa.

Todennukseen tutustumiseen käytettiin valmistajien dokumentaatioita ja eri lähteitä Internetistä. Soveltamiseen jäi lopulta vähän varaa, koska tutkimuslaitoksen verkkolaitteet eivät antaneet siihen mahdollisuutta.

7.2 Porttikohtaisen todennuksen testaaminen

Testaaminen alkoi tutustumalla tutkimuslaitoksen kytkimiin. Kytkimien konfiguroiminen oli lopulta hyvin yksinkertainen toimenpide, minimissään vain muutama rivi määrittelyjä.

HP:n kytkimet eivät antaneet varaa soveltamiseen, jolloin protokollat ja toiminnallisuudet tehtiin yleensä sillä ainoalla vaihtoehdolla, jolla oli valmistajan tuki.

RADIUS-palvelimeen tutustuminen oli huomattavasti pidempi prosessi. Palvelimen toimintaa testattiin useaan otteeseen, eri lähtökohdista ja sen monitorointiominaisuuksia tutkittiin. Todennuspalvelimella pelkkä NPS:ään tutustuminen ei riittänyt, koska NPS on niin sidoksissa aktiivihakemistoon ja ryhmäkäytäntöön. Suurin osa testausvaiheessa löydetyistä ongelmista liittyi yleensä ryhmäkäytäntöön eikä itse NPS:n toimintaan. Lopulta testausvaiheessa saatiin haluttu toiminnallisuus käytännön ympäristössä ja oltiin valmiita siirtymään yliheittoon.

7.3 Käytännön toteutuksen vaiheet

Suunnittelu- ja testausvaihe sujuivat lopulta suhteellisen nopeasti. Vaaditun toiminnallisuuden saamiseen ei mennyt kauan; suurin osa testaamiseen käytetystä ajasta oli yritys luoda mahdollisimman hallittava ja käyttäjäystävällinen ympäristö. Tälläisen ympäristön luominen jäi kuitenkin toteuttamatta, lähinnä ajankäytöllisistä syistä, joita käydään läpi myöhemmin.

Aktiivilaitteiden ja palvelimien valmistelemisen jälkeen siirryttiin yliheittovaiheeseen. Seuraavaksi piti kartoittaa, mitä on kytkettyinä laitoksen kytkimiin. Tämä oli tärkeää, koska osaa laitteista ei voitu laittaa porttikohtaiseen todennukseen niiden toiminnallisuuden takia. Paikkatietokeskuksella oli dokumentaatiota liittyen kytkimiin ja niihin liitettyihin laitteisiin, mutta asiasta ei voitu olla varmoja, joten se päädyttiin tarkastamaan fyysisellä tasolla.

Kytkimien tutkiminen fyysisellä tasolla osoittautui suuremmaksi projektiksi kuin osattiin odottaa, joten siihen olisi ollut hyvä varata aikaa enemmän. Paremmalla ajankäytöllä olisi voitu ryhmitellä kytkennät vikasietoisemmin ja porttikohtaisen todennuksen kannalta loogisemmin, esimerkiksi, kytkeä tutkimuslaitoksen tutkimusryhmät ryhmittäin kytkimiin ja näiden ryhmien todennuksen ulkopuolelle jäävät verkkolaitteet kytkimen loppuosaan. Täten porttikohtaiseen todennukseen osallistuvat kytkinportit olisivat olleet kytkimen alkupäässä, jolloin se olisi ollut ylläpidollisesti hallittavampi kuin tapauskohtainen menettely.

Yliheitto oli mielenkiintoinen prosessi, jonka suunnittelu toteutettiin laitoksen tietohallinnon kanssa. Jaksotettu yliheitto toimi suhteellisen hyvin, ja ongelmatilanteissa pystyttiin nopeasti auttamaan. Yliheiton ajankohta ei ollut paras mahdollinen, koska se osui vuoden loppuun ja osa työntekijöistä oli lähtenyt jo aikaisemmin lomille. Näiden työntekijöiden mahdollinen vianselvitys jäi myöhemmäksi.

7.4 Ongelmakohdat ja vianselvitys

Yliheiton jälkeen ilmeni muutamia loogisia ongelmia porttikohtaisen todennuksen kanssa.Tutkimuslaitoksella on logistisista syistä sijoitettu työntekijöitä paikkoihin, jotka eivät ole tietoverkon kannalta suunniteltu tukemaan niin montaa työntekijää. Tämän seurauksena, osa työntekijöistä on jaettu yhteen porttiin niin sanotulla tyhmällä kytkimellä. Nämä yksinkertaiset kytkimet eivät ole yhteensopivia porttikohtaisen todennuksen kanssa. Suunnitteluvaiheessa tämä ongelma jäi huomiotta ja jatkossa se olisi hyvä ottaa yrityksen loppukäyttäjän fyysiset kytkennät paremmin huomioon. Lopulta näissä tapauksissa porttikohtainen todennus jätettiin toteuttamatta, aikatauluun liittyvistä syistä.

Loppukäyttäjät kokivat myös ongelmia toimialueen salasanan kanssa. Vanhat HP:n kytkimet eivät tue uudempia protokollia ja vanhenevan salasanan vaihtaminen Windowsin kirjautumisvaiheessa estyi. Tämä aiheutti sitä, että loppukäyttäjien käyttäjätunnukset menivät lukkoon ja niitä jouduttiin avaamaan manuaalisesti.

Salasanaongelmaa lähdettiin ratkaisemaan PowerShell-skriptillä, joka lähettää käyttäjälle muistutuksen, kun salasana on vanhenemassa. Suurin osa ongelmista toteutukseen liittyen johtui lähinnä vanhojen ja uusien järjestelmien aiheuttamista ristiriidoista. On kuitenkin ymmärrettävää, että toteutukseen liittyvät hankinnat halutaan pitää minimissään ja ongelmakohdat halutaan mahdollisuuksien mukaan soveltaa.

Helpoin ratkaisu tutkimuslaitoksen verkon ongelmiin olisikin investoida uusin kytkimiin ja palvelinlisensseihin, mutta käytännössä se ei ollut työn tekohetkellä vielä ajankohtaista — liittyen Paikkatietokeskuksen ja Maanmittauslaitoksen liittymisprosessiin.

Yliheitto sujui kuitenkin lopulta kiitettävästi ja vain muutamalla käyttäjällä havaittiin ongelmia, jotka vaativat lisäselvitystä. Paremmalla ajankäytöllä, suunnittelulla ja perusteellisemmalla tutkimuslaitoksen verkkokytkentöjen tuntemuksella olisi yliheitto voitu suorittaa vieläkin vikasietoisemmin.

Lähteet

1 Geodeettisen laitoksen historia. 2015. (Verkkodokumentti.) Juhani Kakkuri. <http://www.fgi.fi/fgi/fi/me/geodeettisen-laitoksen-historia>. Luettu 20.3.2015.

2 Organisaatio. 2015. (Verkkodokumetti.) FGI. <http://www.fgi.fi/fgi/fi/me/organisaatio>. Luettu 20.3.2015.

3 Active Directory Domain Services Overview. 2007. (Verkkodokumentti.) TechNet. <https://technet.microsoft.com/en-us/library/9a5cba91-7153-4265-adda-c70df2321982>. Luettu 22.3.2015.

4 Network Policy and Access Services. 2009. (Verkkodokumentti.) TechNet. <https://technet.microsoft.com/en-us/library/cc754521%28v=ws.10%29.aspx>. Luettu 22.3.2015.

5 NPS Fast Facts. 2008. (Verkkodokumentti.) TechNet. <https://technet.microsoft.com/en-us/library/16e2a32a-91db-4e6c-b515-368a2b3721f7>. Luettu 22.3.2015.

6 Network Policy Server. 2012. (Verkkodokumentti.) TechNet. <https://technet.microsoft.com/en-us/library/d80d8fd1-388f-49e1-8b32-855cf8fda137>. Luettu 23.3.2015.

7 Group Policy Planning and Deployment Guide. 2009. TechNet. <https://technet.microsoft.com/en-us/library/cc754948%28v=ws.10%29.aspx>. Luettu 23.3.2015.

8 Release Notes: Version F.05.22 Operating System for the HP ProCurve Series 2300 and 2500 Switches. 2004. Hewlett-Packard Company, LP. <ftp://ftp.hp.com/pub/networking/software/59903102-e3.pdf>. Luettu 27.3.2015.

9 EAP-MS-CHAP-V2 Authentication Protocol. 2010. Juniper Networks, Inc. < http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc72/sw-sbrc-admin/html/EAP-0210.html>. 4.4.2015.

10 Certificate Requirements for PEAP and EAP. 2008. TechNet. <https://technet.microsoft.com/en-us/library/cc731363%28v=ws.10%29.aspx>. Luettu 30.3.2015.

11 Extensible Authentication Protocol (EAP). 2004. (Verkkodokumentti.) Aboba, Blunk, Vollbrecht, Carlson, Levkowetz. RFC-dokumentti. < https://tools.ietf.org/html/rfc3748>. Luettu 31.3.2015.

12 PEAP Overview. 2012. (Verkkodokumentti.) TechNet. <https://technet.microsoft.com/library/cc754179.aspx>. Luettu 30.3.2015.

13 Internetworking Technologies Handbook, Fourth Edition. 2003. Cisco Systems, Inc. Luettu 20.3.2015.

14 IEEE 802.1X Port-Based Authentication. 2012. (Verkkodokumentti.) Cisco Systems, Inc. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#wp1132455>. Luettu 31.3.2015.

15 Cisco IOS Security Configuration Guide. 2006. PDF-dokumentti. Cisco Systems, Inc. <http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c.pdf>. Luettu 1.4.2015.

16 RADIUS Protocol and Components. 200X. (Verkkodokumentti.) TechNet. < https://technet.microsoft.com/en-us/library/cc726017%28v=ws.10%29.aspx>. Luettu 4.4.2015.

17 Ethernet Tutorial - Part I: Networking Basics. 20XX. (Verkkodokumentti.) Lantronix. <http://www.lantronix.com/resources/net-tutor-etntba.html>. Luettu 5.4.2015.

18 Lähiverkot - Ethernet. 2005. Jaakohuhta, Hannu. IT Press. Luettu 9.4.2015.

19 Extensible Authentication Protocol (EAP). 2004. RFC-dokumentti. Aboba, Blunk, Vollbrecht, Carlson, Levkowetz. <https://tools.ietf.org/html/rfc3748>. Luettu 12.4.2015.

20 Remote Authentication Dial In User Service (RADIUS). 2000. RFC-dokumentti. Rigney, Willens, Livingston, Rubens, Merit, Simpson. <https://tools.ietf.org/html/rfc2865>. Luettu 13.4.2015.

Tiedotus 15.12.2014

Tiistaista 16.12. alkaen tehdään muutoksia laitoksen kytkinverkkoon. Muutokset voivat aiheuttaa mahdollisia (max. 5min) käyttökatkoksia Internet-yhteyteen. Jos omassa tai muiden laitteiden yhteyksissä edelleen ilmenee ongelmia, tee ilmoitus IT-osastoon. Ongelma voi myös todennäköisesti kadota käynnistämällä kone uudelleen. Muutokset saadaan valmiiksi viikon 51 kuluessa.

Tietoturvan korostamisen johdosta kytkinverkossa otetaan käyttöön RADIUS-autentikointi, jonka pääasiallisena tehtävänä on estää tuntemattomien laitteiden pääsy laitoksen verkkoon. Käyttöönoton jälkeen kytkinverkosta Internet-yhteyden saa vain laitoksen toimialueeseen kuuluva tietokone.

Käytännössä tämä tarkoittaa, että saadakseen Internet-yhteyden tulee käyttäjän olla kirjautuneena Windows Domain User -tilassa. Mac- ja Linux-käyttäjien tilanne selvitetään tapauskohtaisesti. Järjestelmät, jotka käyttävät sekä Windows- että Linux-käyttöjärjestelmää, tulevat jatkossa käyttämää langatonta vierasverkkoa Linux:n kanssa.