LAUREA

Neon-laboratorion DNS- ja AD-palvelimen asentaminen, konfigurointi, dokumentointi sekä luottosuhteen muodostaminen Otaverkko-palvelimen välille

Vorojeikin, Daniel

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Neon-laboratorion DNS- ja AD-palvelimen asentaminen, konfigurointi, dokumentointi sekä luottosuhteen muodostaminen Otaverkko-palvelimen välille

Daniel Vorojeikin
Tietojenkäsittelyn koulutusohjelma
Helmikuu, 2009

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

Daniel Vorojeikin

Neon-laboratorion DNS-ja AD-pavelimen asentaminen, konfigurointi, dokumentointi ja luottosuhteen muodostaminen otaverkko palvelimen välille

Vuosi 2009 Sivumäärä 35

Opinnäytetyö on Laurea-ammattikorkeakoululle Leppävaaran toimipisteessä syksyllä 2008 toteutuneen Neon-laboratoriopalvelimen projektin loppuraportti. Työssä pystytetään Neon-laboratorioluokkaan nimipalvelin ja aktiivihakemisto. Neon-laboratorioluokan päätteet liitetään uuden Labra-toimialueen piiriin. Palvelinprojektin päätavoite oli luoda luottosuhde Neon-laboratoriopalvelimen ja Otaverkossa sijaitsevan Laurea palvelimen välille. Projektin edetessä ilmeni muutama tutkimusongelma, jotka ratkaistiin projektin aikana. Tutkimusongelmat liittyivät verkkojärjestelyihin ja IP-osoitemuunnoksiin ASA-reititinpalomuurissa (NAT). Päätavoitteen saavuttaminen vaatii VPN-yhteyden muodostamisen palvelimien välille. Tämä todettiin tutkimusongelman selvittämisen yhteydessä. Opettajien sekä Laurean henkilökunnan kanssa päätettiin, että VPN-yhteyden muodostaminen on erillisprojekti, joka toteutetaan opinnäytetyön muodossa tulevaisuudessa. NEON-laboratorio on osa Leppävaaran Laurean laboratorioympäristöä.

Loppuraportin alussa määritellään tavoitteet, sidosryhmät, kohdeorganisaatio sekä tutkimusmenetelmä. Projektin lähtötilanteessa Neon-laboratorioluokan koneet eivät kuuluneet mihinkään toimialueeseen. Tämä johtui Tapani Viitasen opinnäytetyön muodossa luomassa erillisestä tietoverkosta. Neon-laboratorioon luotiin oma toimialue pystyttämällä palvelin. Palvelin vastaa laboratorioluokan DNS-liikenteestä sekä sisään-kirjautumisesta aktiivihakemistopalvelun avulla. Raportissa avataan lukijalle keskeiset käsitteet ja tekniikat, joita projektissa käytetään sekä palvelimen määritetyt asetukset.

Projektin aikana ilmeni useampi tutkimusongelma yritetäessä muodostaa luottosuhdetta Laurea-palvelimen kanssa, joka fyysisesti sijaitsee Otaverkossa ja kuuluu Otaverkko Oy:in hallinnoitavaksi. Projektin toteutuksesta suuri aika meni tutkimusongelman selvittämiseen. Tutkimusongelmaa selvitettiin Otaverkko Oy:n henkilökunnan kanssa konfiguroimalla palomuureja muun muassa Laurean ASA-reititinpalomuuria. Projektissa paljastui, että luottosuhdetta palvelimien välille ei voi muodostaa ilman VPN-yhteyttä. Johtuen ASA-reititinpalomuurin luomasta IP-osoitemuunnoksesta (NAT). Havainto yllätti niin Otaverkko Oy:n henkilökunnan kuin Laurean opettajatkin. Tästä aiheesta ei löytynyt helposti kirjallista tai sähköistä tietoa.

Projektin huolellisella dokumenttityöllä pyrittiin varmistamaan Labra-palvelimen hallinnointi verkon ylläpitohenkilökunnalle. Raportin lopussa arvioidaan projektin toteutusta sekä käsitellään kehittämismahdollisuuksia tulevaan VPN-yhteys projektiin.

Asiasanat: DNS, AD, Windows Server 2003, Luottosuhde, NAT, Dokumentointi, Tutkimusongelma, tietoverkko

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Programme
Information Systems and Data Communication

Daniel Vorojeikin

Implementing, configuring, documenting of Active Directory and Domain Name Server and establishing a forest trust connection between Neon-laboratory server and Laurea server located in Otaverkko

Year 2009 Pages 35

This is the final report of a thesis completed for Laurea University of Applied Sciences Leppävaara unit during 2008, and concludes the Neon laboratory server project. In the project a name server and an active directory were established on a server located in the Neon-laboratory classroom. The PCs of the Neon classroom were attached to the new domain named "Labra". The main objective of the project was to establish a trust connection between the Neon laboratory server and a Laurea remote server located in the Otaverkko. During the project several research problems were encountered which were solved as the project progressed further. The research problems were related to the network arrangements and the change of the IP address in the ASA-router firewall (NAT). Achieving the main objective requires establishing a VPN connection between the two servers. This was the main discovery whilst solving the research problems. With the Laurea staff and mentors it was decided that the actual process of creating a functional VPN connection is to be executed in another thesis in the future. The Neon laboratory is a part of Laurea's laboratory environment at Leppävaara.

The main goals, interest groups, target organization and research methods are introduced at the beginning of the final report. At the startup of the project the PCs of the Neon laboratory were not part of any domains. This is due to another thesis by Tapani Viitanen in which a separate network was created. A new domain was initiated in the Neon laboratory by establishing a server. The server is in control of the network traffic and logging on in the laboratory classroom via an active directory. The reader is introduced to the essential concepts and techniques which were used in the project in addition to the server's modifiers and settings.

Several research problems were encountered during the project whilst trying to establish a trust connection with the Laurea server, which is physically located in Otaverkko and is managed by Otaverkko Oy. Most of the time in this project was spent solving this research problem. The research problem was solved with the assistance of the Otaverkko Oy staff by configuring firewalls, including the ASA router firewall of Laurea. It was discovered that a connection cannot be established without a VPN connection due to the change of the IP address (NAT) initiated by the ASA firewall. This discovery surprised both the Otaverkko Oy staff and the mentors of Laurea. Finding information of this topic proved very difficult.

By careful documentation of the project further Neon laboratory server management was ensured to the Laurea network administrators. At the end of the report topics such as evaluating the execution of the project, opportunities and ideas for further development for the VPN connection were addressed.

Keywords: DNS, AD, Windows Server 2003, Forest trust, NAT, Documentation, Research problems, Network

SISÄLLYS

1 Johdanto

Opinnäytetyössä raportoidaan nimipalvelimen asentaminen, aktiivihakemiston pystyttäminen Laurea-ammattikorkeakoulun Leppävaaran toimitiloihin sekä luottosuhteen muodostaminen Otaverkossa sijaitsevan Laurean palvelimen välille. Opinnäytetyö on toimintakeskeinen ja itse toteutus on tehty syksyn 2008 aikana Laurea-ammattikorkeakoulun laboratorioympäristössä.

Palvelinprojektin tarve on syntynyt Laurea-ammattikorkeakoulun tietoverkkojärjestelyjen myötä, jonka Tapani Viitanen on toteuttanut opinnäytetyön muodossa keväällä 2008. Tapani Viitanen on rakentanut Laurealle Neon-laboratorioon oman tietoverkon keväällä 2008. Tietokonepäätteet, jotka sijaitsivat Tapani Viitasen luomassa tietoliikenneverkossa, eivät enää muutoksen myötä kuuluneet mihinkään toimialueeseen. Tästä syystä opiskelijat eivät kyenneet kirjautumaan kyseisille päätteille omilla opiskelijatunnuksillaan.

Opinnäytetyön alussa esitellään palvelinprojektin lähtökohdat, tavoitteet sekä projektiin liittyvät sidosryhmät. Opinnäytetyössä avataan lukijalle opinnäytetyön kannalta keskeiset käsitteet ja tekniikat, joita palvelinprojektissa käytetään. Lopussa raportoidaan itse projektin toteutuksesta ja toteutuksen aikana ilmenneistä ongelmista.

Opinnäytetyön tärkein tavoite on pystyttää Laurea-ammattikorkeakoululle laboratorioympäristöön toimiva palvelinratkaisu, jotta opiskelijat voisivat kirjautua omilla käyttäjätunnuksillaan Labran tietokoneisiin. Lisäksi palvelinympäristön tulisi toimia testi,- ja kehitysympäristönä Laurea-ammattikorkeakoulun tietoliikennelaboratorion henkilökunnalle sekä tietojenkäsittelyn opiskelijoille. Opinnäytetyössä dokumentoidaan mahdollisimman tarkasti toteutettu palvelinratkaisu tulevaa hallinnointia varten.

Opinnäytetyön tutkimusongelmaksi muodostuu ennalta tuntematon laboratorioympäristö, johon palvelinprojekti sijoitetaan. Opinnäytetyön tutkimusmenetelmäksi on valittu tästä syystä konstruktatiivinen tutkimusmenetelmä. Laboratorioympäristö verkkojärjestyksineen on haastava ja ennalta tuntematon työympäristö, josta ei löydy kirjallista teoriapohjaa vastaavanlaisesta ympäristöstä. Tarkoituksena on konstruktatiivistä tutkimusmenetelmää käyttäen ratkoa projektin aikana ilmeneviä ongelmia.

2 Kohdeorganisaatio

2.1 Laurea-ammattikorkeakoulu

Laurea-ammattikorkeakoulu (University of Applied Sciences) on Suomen neljänneksi suurin ammattikorkeakoulu, jonka toimipisteet sijaitsevat Espoossa Leppävaarassa ja Otaniemessä sekä Hyvinkäällä, Keravalla, Lohjalla, Porvoossa ja Vantaalla (Laurea Fakta 2008-2009, 15).

Laurea-ammattikorkeakoulussa on 8000 aloituspaikkaa ja 13 suomenkielistä koulutusohjelmaa. Laurea-ammattikorkeakoulu toteuttaa uutta opetussuunnitelmaa (Learning by Developing), jonka tarkoituksena on kouluttaa uudenlaisia osaajia. Kehittämällä oppimisen opetussuunnitelman tarkoituksena on luoda oman alan osaajia, jotka ovat kykeneväisiä myös kehittämään omaa alaansa. Uuden opetussuunnitelman puolesta puhuu se, että Laurea-ammattikorkeakoulu on Suomen paras vastavalmistuneiden työllistäjä (Laurea Fakta 2008-2009, 11).

Laurean tavoite on olla vuonna "2010 täysivaltainen, innovatiivinen, kansainvälinen ammattikorkeakoulu, jonka keskeiset arvot ovat luotettavuus, innovatiivisuus, sosiaalinen vastuullisuus sekä yhdessä tekeminen"(Laurea Fakta 2008-2009, 15).

Laurean ammattikorkeakoulua ylläpitää Laurea-ammattikorkeakoulu Oy, jonka osakkaana ovat kuusi kuntaa, kaksi kuntayhtymää ja yksi yksityinen omistajayhteisö. Laurea-ammattikorkeakoulun toimitusjohtajana/rehtorina toimii Pentti Rauhala vuodesta 1996 lähtien (Laurea fakta 2008-2009, 19).

2.2 Laboratorioympäristö

Opinnäytetyö toteutetaan Laurean Leppävaaran toimipisteessä sijaitsevaan Laurea laboratorioympäristöön. Laboratorioympäristössä toimii toistaiseksi REDlabs, tietoliikennelaboratorio, NEON-laboratorio sekä Business Ecelent center(BEC). Yksiköt toimivat oman alansa omina tutkimus- ja kehittämisyksiköinä, joiden tarkoituksena on luoda hankkeita opiskelijoille (LAUREA 2008).

Kullakin yksiköllä on oma toisistaan riippumaton tietoverkko. Neon-laboratoriossa on Tapani Viitasen rakentama tietoverkko (Tapani Viitanen 2008, 25-26).

Tulevaisuudessa kaikki laboratorioluokat tullaan siirtämään Neon-laboratorion tietoverkon tavoin omiin Otaverkko Oy:stä riippumattomiin tietoverkkoihin (Tuomisto, 2008).

2.3 Neon-laboratorio

Neon-laboratorio sijaitsee Leppävaaran toimipisteessä ja toimii Laurean kehittämislaboratoriona. Laboratorion tarkoituksena on luoda erilaisia projekteja opiskelijoille, joita voi suorittaa muun muassa opinnäytetyön tai työharjoittelun muodossa. Hyviä esimerkkejä Neon-laboratoriossa toteuttavista projekteista ovat RIESCA (Rescuring intelligence Electronics Security Core Applications) ja ORE (Open Rendering Enviroment) projektit (Viitanen 2008, 7).

Neon-laboratorion tietoverkkorakenne poikkeaa muista laboratorioluokista. Se on itsenäinen muista riippumaton tietoverkko, joka on tietoliikennelaboratorion ylläpidossa. Tarkoituksena on, että tulevaisuudessa muut laboratorioluokat siirretään vastaavanlaiseen tietoverkkoympäristöön (Tuomisto, 2008).

3 Projektin tausta ja tarkoitus

3.1 Projektin lähtökohta

Laurea-ammattikorkeakouluun on perustettu vuodesta 2000 lähtien erilaisia tutkimus- ja kehitysympäristöjä, joita kutsutaan laboratorioiksi. Tapani Viitanen opinnäytetyössään (2008) rakentanut Neon-laboratoriolle oman itsenäisen tietoverkon, jonka IP- osoiteavaruus poikkeaa muista Laurean luokista. Neon-laboratorioluokan tietoturvaratkaisut poikkeavat myös muista Laurean luokkien tietoturvaratkaisuista. Ennen Tapani Viitasen opinnäytetyötä Laurean Leppävaaran tietoverkko oli yhtenäinen (10.0.0.0 IP- osoiteavaruudella) . Tietoverkon hallinta ja aktiivilaitteet olivat Laurean IT-palveluiden tarjoajien hallinnassa. Nimipalvelin-(DNS) ,aktiivihakemisto-(AD) ja DHCP-palvelimet sijaitsivat Otaverkon tiloissa ja niiden ylläpito on ulkoistettu Otaverkko Oy:lle. Palvelimien fyysistä hallintaa hoidettiin Otaverkko Oy:ltä käsin, mutta varsinainen hallinta kuuluu Laurean IT-palveluiden hoitajille, ja siitä vastaavat muun muassa Timo Leopold ja Jarmo Tapio . Tapani Viitanen eristi laboratorion verkon omaksi itsenäiseksi verkokseen Laurean muusta tietoverkosta.

Laboratorioiden tietoverkkojärjestelyn tarve muodostui siitä, että haluttiin opiskelijoille tietoverkko, joka on riippumaton Otaverkosta sekä Laurean IT-palvelun tarjoajista. Tämä mahdollistaisi tulevaisuudessa muun muassa omien palvelimien asentamisen, palvelimien hallinnoinnin sekä tietoverkon hallinnoinnin. Laboratoriot toimisivat opiskelijoilla erinomaisena tutkimus- ja kehitysympäristönä. Lisäksi mahdolliset ongelmatilanteet vaikuttaisivat vain laboratorioverkkoihin eikä koko Laurean Leppävaaran tietoverkkoon.

Tapani Viitasen rakentamassa laboratorioverkossa aktiivilaitteet ja tietoverkko ovat tietoliikennelaboratorion hallinnassa. Uuden tietoverkkoratkaisun johdosta Neon- laboratorioverkolla

ei ole aktiivihakemistoa-(AD) eikä omaa nimipalvelinta (DNS). Nimikyselyt on ohjattu laboratorioverkosta Otaverkon nimipalvelimiin. Laboratorioverkossa sijaitsevat päätteet eivät kuulu mihinkään toimialueeseen, ja tämän takia opiskelijat eivät pysty kirjautumaan omilla käyttäjätunnuksillaan näille koneille. Koneille pääsee kirjautumaan vain paikallisilla käyttäjätunnuksilla, jotka ovat Laurean tietoliikennelaboratorion henkilökunnan tiedossa.

3.2 Projektin tavoitteet ja riskit

Projekti koostuu useammasta tavoitteesta. Projektin päätavoite on luoda toimiva työskentelyympäristö Laurean laboratorioluokkiin, mikä mahdollistaisi kaikkien Laurean opiskelijoiden kirjautumisen omilla käyttäjätunnuksillaan laboratorioluokkiin. Tämän tavoitteen onnistuminen koostuu usean eri osan summasta. On kyettävä onnistuneesti pystyttämään nimipalvelin ja aktiivihakemisto Windows server 2003-palvelinalustalle.Lisäksi on pystyttävä määrittämään nimipalvelimen asetukset onnistuneesti sekä luomaan onnistuneesti oma toimialue. Kriittiseksi osaksi muodostuu luottosuhteen muodostaminen Otaverkon palvelimen välille ja tietoturvaasetusten määrittäminen Laurean laboratorioverkoissa.

Toinen tavoite projektissa on pystyttää palvelin, joka olisi tietoliikennelaboratorion henkilökunnan hallinnassa. Tavoitteen onnistuminen vaatii toimiakseen samat toiminnot kuin edellinen tavoite. Lisäksi palvelimelle aktiivihakemistoon on luotava hallintatunnukset tietoliikennelaboratorion henkilökunnalle.

Kolmas tavoite on luoda testiympäristö tietojenkäsittelyn opiskelijoille, jotta he voisivat käyttää projektissa palvelinta työtilanaan. He voisivat tehdä harjoitustehtäviä muun muassa aktiivihakemiston ja nimipalvelimen parissa. Tällä hetkellä Laurea-ammattikorkeakoululla ei ole ollut mahdollista tarjota opiskelijoille tällaista työtilaa harjoitustehtäviä varten. Yksi tavoite on kaiken tämän kattava dokumentointi.

Projektissa on useampi eritason riski. Toteutuksessa tarvittavien taitojen puute on vakava riski. Toteutuksen kannalta vaadittavat taidot ovat: nimipalvelimen toimintafunktioiden ymmärtäminen, aktiivihakemiston sekä toimialueen toiminnan ymmärtäminen ja niiden hallinta sekä kokemuksen saaminen luottosuhteen muodostamisesta. Projekti voisi kariutua näiden osaamisalueiden puuttumiseen. Olen minimoinut riskin vaaroja harjoittelemalla ja toteuttamalla tämän kaiken onnistuneesti työpaikallani pystyttämässäni testiympäristössä.

Vakava riski projektin kannalta muodostuu Laurean laboratorioympäristön tietoverkkorakenteesta. Kukin laboratorioluokka on eri verkossa. Verkkomuutokset on tehtävä ASA-reititinpalomuurista. ASA-reititinpalomuurista joutuu aukaisemaan useamman portin ja käyttämään IP-osoitemuunnosta (NAT) palvelimen yksityisen IP-osoitteen muuntamisen julkiseksi

IP-osoitteeksi. Asetusmuutokset tehdään tietoliikennelaboratorio henkilökunnan kanssa yhdessä. Näiden verkkomuutoksien yhteydessä voi ilmetä vakava ennalta tuntematon ongelma, joka pitää ratkaista. Tämä on suotavaa konstruktatiivisessä tutkimusmenetelmässä.

Kriittisin riski johtuu ulkoisesta sidosryhmästä Otaverkko Oy:stä. Onnistuneen luottosuhteen muodostaminen vaatii heidän teknisen hyväksyntänsä. Heidän on sallittava luottosuhteen muodostus palvelimelta käsin. Ensiksi heidän pitäisi ottaa yhteys labra-palvelimeen, joka sijaitsee fyysisesti Neon-laboratorion verkkoympäristössä. Useista eri pyynöistä huolimatta Otaverkko Oy ei ole vastannut mitään.

3.3 Projektin tutkimusmenetelmä

Opinnäytetyö on muodoltaan toimintatutkimuksellinen eli konstruktiivinen tutkimusmenetelmä. Viitaten Simoniin (1981) ja van Aken (2004) kuvaa, että "suunnittelutieteen tarkoitus on joko luoda tietämystä suunnittelua ja toteutusta varten, siis *konstrukti*o-ongelmien ratkaisemista varten, tai parantaa nykyisten systeemien suorituskykyä, siis ratkaista *parantamis*-ongelmia" (Van Aken 2004; ks. Simon 1981; ks. Järvinen & Vuorinen 2004, 103).

Toimintatutkimustermin on ottanut Järvisen mukaan käyttöön ensimmäisenä Lewin (1946), kun hän tutki ryhmien dynamiikkaa ja muutoksen läpiviemistä ryhmässä (Järvinen 2004, 128).

Konstruktiivinen tutkimus valittiin, koska projektin luonne täytti vahvasti tutkimustietieteelliset ominaispiirteet. Toimintatutkimus on tutkijan toimimista yhtäältä käytännön ongelman ratkaisemiseksi (primääritehtävä) ja samalla toisaalta sellaisen tiedon hankkimiseksi, jolla on tieteellistä mielenkiintoa (sekundääri-tehtävä)(Järvinen 2004, 128).

Toimintatutkimuksen syklit prosesseina: 1. diagnosointi (ongelman tunnistaminen ja määrittäminen) 2. Suunnittelu (eri vaihtoehtojen tarkastelu ongelman ratkaisemiseksi) 3.Toteutus (yhden vaihtoehdon valinta ja toimeenpano) 4. Arviointi (esimerkiksi toiminnan toimivuuden seuraaminen) 5. Oppiminen (Järvinen 2004, 129).

Projektiprosessin tunnusmerkit täyttävät vahvasti toimintatutkimuksellisuuden piirteet. Laboratorioympäristöön ei pääse kirjautumaan opiskelijoiden käyttäjätunnuksilla, eikä tietoliikennelaboratorion henkilökunta hallitse aktiivilaitteita ja tietoverkkoa (tutkimusongelma). Palvelimen asentaminen ja luottosuhteen muodostaminen Otaverkon palvelimen välille ratkaisisivat ongelman (suunnittelu). Palvelimen asentaminen, verkkoasetusten määrittäminen sekä luottosuhteen muodostaminen (toteutus). Projektin ratkaisujen testaaminen sekä toiminnan toimivuuden varmistaminen (arviointi), projektin toteutuksen yhteydessä ilmaantuvien ongelmien ratkaisu (oppiminen).

Projektin toteutuksen dokumentointi on olennainen osa opinnäytetyötä, esittelemällä toteuttamisprosessia ja sen tulosta eli realisaatiota (Järvinen 2004, 131). Tutkijan tehtävä on valita tietyt tekijät realisaation kuvaukseen, sillä kaikkea ei voi kuvata (Tapani Viitanen 2008, 10). Opinnäytetyössä aineiston hankinnassa käytetään erilaisen kirjallisuuden tutkimista sekä näiden lähteiden implementointia Laurean laboratorioympäristöön. Projektin lähtökohtana oli luoda eräänlainen autentikointi ratkaisu sekä lisäarvoa tuova ratkaisu Laurean laboratorioympäristöön. Kirjallisuutta aiheesta on paljon, mutta se on enemmän manuaaliluonteista eikä sitä voi suoraan soveltaa kyseiseen ympäristöön. Tämän johdosta projektitoteutuksen yhteydessä tulee ilmenemään varmasti useita ongelmia, mikä vaatii ratkaisun ennen projektin onnistumista. Ratkaisujen löytäminen ja niistä oppiminen on konstruktatiivisen tutkimusmenetelmän avainasioita.

3.4 Projektin rajaus

Projekti on rajattu kokonaisvaltaiseen tietotekniseen ratkaisun suunnitteluun ja suunnitelman toteuttamiseen. Toteutuksessa on otettava huomioon sidosryhmät, joihin projektin toteuttaja ei voi suoranaisesti vaikuttaa. Projekti vaatii toimiakseen lopullisesti eri sidosryhmien yhteistyötä.

Projektin päätyttyä palvelimen hallinta siirtyy tietoliikennelaboratorion henkilökunnan ylläpitoon. Tulevaisuudessa se vastaa palvelimen toimivuudesta ja mahdollisesta kehityksestä. Aktiivihakemiston hallinta on myös projektin päätyttyä tietoliikennelaboratorion henkilökunnan hallinnassa.

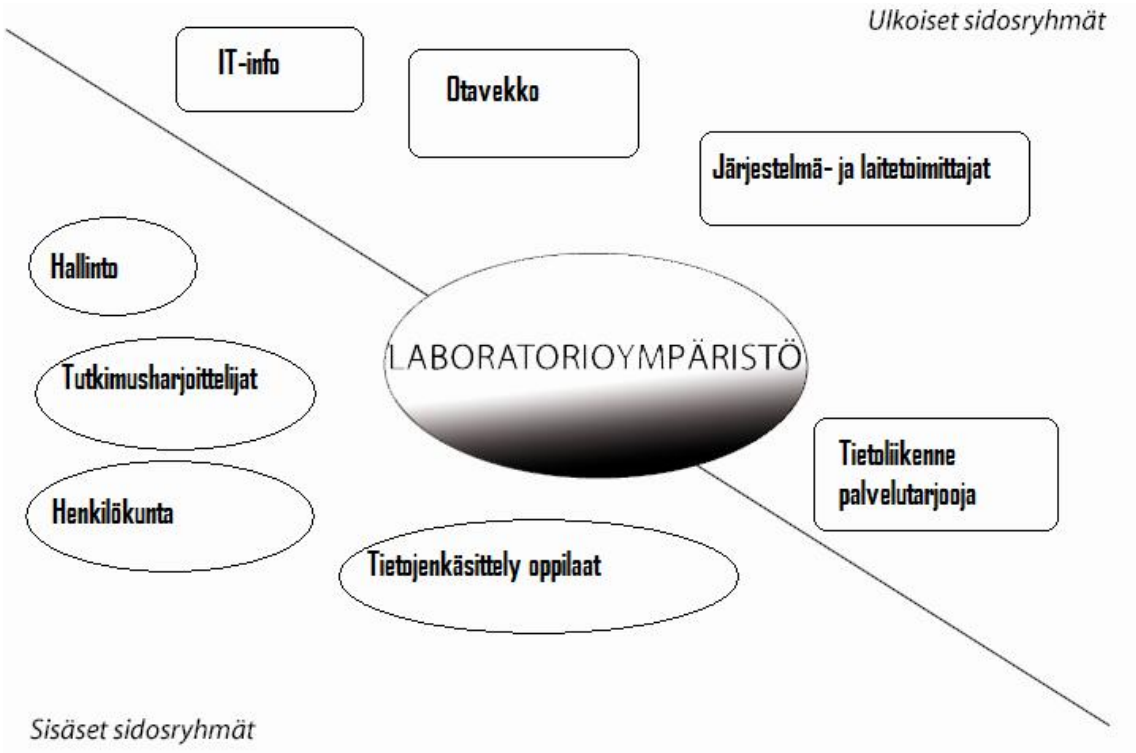
Projektin ulkopuolelle on jätetty mahdollinen tuleva verkkojärjestely, joka yhdistäisi laboratorioluokkien verkot yhtenäiseksi itsenäiseksi tietoverkoksi. Projektin seuraavassa luvussa on avattu keskeisiä käsitteitä, tekniikoita ja protokollia, joita projektissa käytetään. Dokumentaation ulkopuolelle on jätetty tietotekniikan perusasiat , joita lukijan odotetaan tietävän ymmärtääkseen tämän projektin kokonaisuuden.

3.5 Projektin sidosryhmät

Elina Jylhän mukaan yrityksen ja organisaation kenttä on hyvin erilainen, mutta niillä on kuitenkin tiettyjä yhteisiä piirteitä ja toimintaperiaatteita. Näiden ymmärtäminen auttaa ymmärtämään niiden toimintaa markkinoilla ja erilaisissa ympäristöissä. Organisaation toimintaa voidaan tarkastella muun muassa sidosryhmäsuhteiden kautta(Jylhä ym. 1998, 23.).

Sidosryhmät ovat niitä ryhmiä, joiden kanssa yritys on tekemisissä tai yhteistyössä. Ne voivat olla sekä yksityishenkilöitä, yrityksiä että yhteisöjä (Jylhä ym. 1998, 24.). Jylhä jakaa sidosryhmät kahteen pääkategoriaan organisaation ulkoisiin ja sisäisiin sidosryhmiin(Jylhä ym. 1998, 24.). Sidosryhmien ominaispiirteeseen kuuluu, että molemmat osapuolet hyötyvät toisistaan, hyötyminen on niin rahallista hyötymistä, kuin tietoista hyötymistä (Jylhä ym. 1998, 24.).

Projektin läpiviennin kannalta on olennaista ymmärtää laboratorioympäristöön vaikuttavat sidosryhmät. Projektista hyötyvät suoranaisesti Laurean opiskelijat, tietojenkäsittelyoppilaat ja tutkimusharjoittelijat. Tietojenkäsittelyoppilaat ja tutkimusharjoittelijat pääsevät toteuttamaan työtehtäviä uudessa testiympäristössään. Myös kirjautuminen omilla käyttäjätunnuksilla on mahdollista. Tietoliikennelaboratorion henkilökunta saa projektin valmistuessa hallintaansa laboratoriopalvelinympäristön. Projektia ennen palvelinympäristö on ollut ulkoisen sidosryhmän Otaverkon hallinnassa. Projektin valmistumiseen tarvitaan ulkoisen sidosryhmän Otaverkon yhteistyötä. Toiminnan jatkuvuuden kannalta on tärkeää tyydyttää sidosryhmien tarpeet. Organisaation on otettava tämä huomioon strategioita ja toimintasuunnitelmia laatiessaan(Jylhä ym. 1998, 24.).



Kuva 1.Laboratorioympäristön sidosryhmät

3.5.1 Sisäiset sidosryhmät

Laboratorioympäristön sisäisiin sidosryhmiin kuuluu pääasiassa tutkimusharjoittelijat, tietojenkäsittelyoppilaat, Laurea-henkilökunta ja hallinto (kuva1). Projekti on luotu pääasiassa sisäisiin sidosryhmien tarpeisiin. Oppilaille mahdollistetaan sisäänkirjautuminen omilla käyttäjätunnuksilla laboratorioympäristöön. Tietojenkäsittelyn opiskelijoille luodaan testiympäristö kouluprojekteja varten. Tietoliikennelaboratorion henkilökunta saa hallintaansa Otaverkolta haluamansa palvelimen. Hallinnollisesta näkökulmasta tämä projekti tuo lisäarvoa Laurea-ammattikorkeakoululle. Tutkimusharjoittelijat ovat nykyään pääsääntöisesti kansainvälisiä opiskelijoita (Viitanen 2008, 12.). Tutkimusharjoittelijoille projekti mahdollistaa uuden tehokkaamman työskentelytilan.

3.5.2 Ulkoiset sidosryhmät

Laboratorioympäristön ulkoisiin sidosryhmiin kuuluu Laurea IT-palvelu, Otaverkko OY, tietoliikenteen palvelutarjoaja sekä järjestelmä- ja laitetoimittajat. Laurean IT-palvelu on kattava Laurean tietotekniikasta vastaava palvelu, johon kuuluu lähinnä helpdeskinä toimiva IT-info.

Laurea IT-palvelujen tehtävä on vastata Laurean yleisestä tietotekniikan ylläpidosta. Kuitenkin laboratorioympäristön tietoliikenteen hallinta ja tietotekniikan ylläpito on siirretty tietoliikennelaboratorion henkilökunnan hallintaan. Teoreettisesta hallinnon jaosta huolimatta Laurea IT-palvelun tarjoajat on sidottu tavalla tai toisella laboratorioympäristön sidosryhmiin, sillä he tekevät yhteistyötä tietoliikennelaboratorion henkilökunnan kanssa.

Järjestelmä- ja laitetoimittajia ovat 3StepIT, jonka kautta laboratoriossa sijaitsevat tietokoneet on vuokrattu Laurean käyttöön. Hewlett- Packard Oyj on toimittanut laboratorion tulostimet. Työasemakohtaiset virustorjunta- ja palomuuripalvelut on hankittu F-secure Oyj kautta. Sama yritys tarjoaa myös edellä mainittujen ohjelmien päivitys ja tukipalvelut(Tapani Viitanen 2008 Opinnäytetyö, 12.).

Otaverkko Oy tarjoaa Laurealle useita tietoliikennepalveluita, muun muassa DNS, Autentikointi sekä pääsyn julkiseen Internetiin(Tapani Viitanen 2008 Opinnäytetyö, 12.). Projektin kannalta Otaverkko Oy tulee tarjoamaan mahdollisuuden projektin toteutukseen. Ilman Otaverkon teknistä hyväksyntää ei voi muodostaa luottosuhdetta, joka mahdollistaa autentikoinnin laboratorioluokissa. Projektin valmistuessa Otaverkko Oy:n asema ulkoisena sidosryhmänä kasvaa laboratorioympäristössä. Liikenne tulee kulkemaan tulevaisuudessakin Otaverkon kautta, mutta laboratorioympäristö saa oman DNS- ja autentikointi palvelut (Aktiivihakemisto).

3.6 Aikaisempia tutkimuksia aiheesta

Tutkimuksen kokonaisratkaisu koostuu useasta eri ratkaisusta, joita joutuu soveltamaan laboratorioympäristöön. Microsoftilta löytyy paljon kirjallisuutta Windows Server 2003 opuksista, muun muassa luottosuhteen muodostamisesta, nimipalvelimesta sekä aktiivihakemistojen hallinasta. Kirjallisuudessa on fiktiivisiä esimerkkejä organisaatioiden välisistä luottosuhteista ja niiden hallinnasta. Suoranaista verrannon kelpoista aikaisempaa tutkimusta ei aiheesta löydy.

Markus Vuorinen kertoo opinnäytetyössään syyksi vähäisen tiedon määrään yrityksien haluttomuuden paljastaa mitään ylimääräistä omasta ympäristöstään tietoturvasyiden takia(2006, 25).

4 Projektissa käytettävät tekniikat ja protokollat

Seuraavassa luvussa käydään läpi olennaisimmat käsitteet projektin toteutuksen kannalta. Tarkoitus ei ole luoda kaiken kattavaa tietotekniikkaopusta vaan kertoa teoriaa projektissa käytettävistä tärkeimmistä tekniikoista. Lukijalta odotetaan teorian ymmärtämiseen aikaisempaa kokemusta tietotekniikasta.

4.1 Aktiivihakemisto (Active directory, AD)

Termit hakemisto (directory) ja hakemistopalvelu (directory service) viittaavat yleisissä ja yksityisissä verkoissa sijaitseviin hakemistoihin. Hakemisto on verkon objekteja sisältävä tietokanta, johon voidaan viitata monella eri tavalla (Kivimäki 2003, AD,6.).

Kivimäki kertoo opuksessaan, että aktiivihakemisto on hakemistopalvelu ja käyttäjätietokanta. Se sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Aktiivihakemistopalvelu mahdollistaa resurssien jakamisen käyttäjille ja sovelluksille keskitetysti, sillä pystytään hallinnoimaan ja suojata käytössä olevia verkon resursseja. Aktiivihakemistopalvelu kuuluu osana Windows Server 2003 käyttöjärjestelmää (Kivimäki 2003, AD, 6.).

Aktiivihakemiston päätarkoitus on tarjota keskitetty käyttäjätunnistuspalvelu Windows -pohjaisille koneille. Aktiivihakemisto-verkot voivat vaihdella pienestä muutaman sadan objektin ympäristöstä suuriin ympäristöihin, joissa on miljoonia objekteja. Aktiivihakemisto julkis-

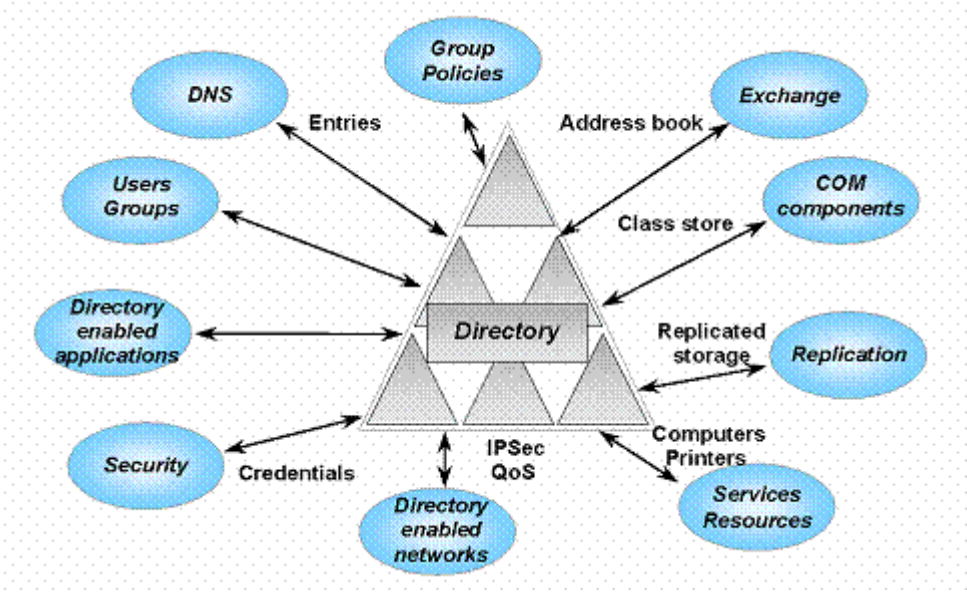
tettiin ensi kertaa vuonna 1996 Windows 200 Server -käyttöjärjestelmässä ja paranneltuna versiona Windows Server 2003:ssa. (www.wikipedia.org) (Active directory)

Aktiivihakemisto on siis palvelu, jota käytetään tiedon tallentamiseen verkon resursseista toimialueella (domain). Aktiivihakemiston rakenne on hierarkinen. Objektit voidaan jakaa kolmeen kategoriaan: resurssit, palvelut ja käyttäjät. Aktiivihakemisto tarjoaa tietoja objekteista, organisoi niitä ja säätelee käyttöoikeudet. (www.wikipedia.org)(Active directory)

Resurssien nimeämiseen käytetään standardin mukaista DNS -nimeämiskäytäntöä. AD:ssa kaikki sellaiset sovellukset ja hakemistot, jotka tukevat LDAP -standardia, pystyvät vaihtamaan tietoja keskenään. (www.itpro.fi)

Kivimäki kertoo, että käytäntöryhmät (Group policy object, GPO) ovat keskeinen aktiivihakemiston tarjoama teknologia käyttäjien ja laitteiden hallitsemiseksi. Käytäntöryhmien avulla voidaan hallita yli tuhatta asetusta objektia kohden. Käytäntöryhmien avulla voidaan yhtenäistää esimerkiksi tietoturva-asetukset, www-selaimen asetukset, käyttöliittymän asetukset sekä käyttöjärjestelmän eri palveluiden asetukset. Näiden avulla on mahdollista saavuttaa mahdollisimman helposti ylläpidettävä työasemaympäristö palveluineen. (Kivimäki 2003, AD, 361,595.).

Aktiivihakemiston päätarkoitus on siis tarjota keskitetty käyttäjätunnistuspalvelu: käyttäjät kirjautuvat työasemilta hakemiston käyttäjiksi, tämä voidaan toteuttaa esimerkiksi käyttäjätunnus / salasana parilla. Tunnistettua käyttäjän tietoa käytetään erilaisten objektien käyttöoikeuksien tutkimisessa: käyttäjän yrittäessä päästä käsiksi haluttuun resurssiin verrataan käyttäjän tietoja resurssiin liitettyyn käyttöoikeusmääritelmään. Resurssien käyttöoikeuksien hallitsemiseen käytetään usein ryhmiä, joille on määritetty tarvittavat oikeudet, joihin käyttäjä lisätään. Käyttöoikeuksia pystytään hallinnoimaan graafisesta käyttöliittymästä: kenellä on pääsy, ketkä pystyvät muuttamaan ja kenellä ei ole oikeutta edes lukea tiettyä resurssia. (www.itpro.fi) (Aktiivihakemisto)



Kuva 2. Aktiivihakemiston toiminnot ja niiden sidosryhmät

Projektissa asennetaan laboratorioympäristöön aktiivihakemisto Windows server 2003 alustalle. Aktiivihakemistoon luodaan hallintatunnukset tietoliikennelaboratorion henkilökunnalle. Aktiivihakemisto on muuten tyhjä käyttäjätunnuksista. Luottosuhteella Otaverkon aktiivihakemistoon mahdollistetaan Otaverkon aktiivihakemistossa sijaitsevien käyttäjätilien käyttö laboratorioverkossa.

4.1.1 Käyttäjäryhmät

Käyttäjätilien avulla käyttäjät voivat kirjautua toimialueella sijaitseviin tietokoneisiin ja käyttää verkon resursseja. Jokainen käyttäjätili on määritelty johonkin ryhmään, mikä mahdollistaa käyttäjälle määritetyt oikeudet (Kivimäki 2003, AD, 385.).

Aktiivihakemistoa pystyttäessä luodaan automaattisesti joitakin oletuskäyttäjätilejä ja -ryhmiä. Tämmöisiä ryhmiä ovat muun muassa järjestelmävalvojat, vieraat ja domain-userit (Kivimäki 2003, 392.). Lisätessään käyttäjätilin esimerkiksi järjestelmävalvojan ryhmään käyttäjä saa järjestelmävalvojaoikeudet. Järjestelmävalvojan oikeuksilla käyttäjä voi tehdä kaikkia konfigurointitehtäviä koneille, jotka kuuluvat samaan toimialueeseen (Kivimäki 2003, AD, 394.).

Eri käyttäjäryhmillä on eri vaikutusalueet: local, global ja universaali. Ryhmien vaikutusalueiden mukaan käyttäjätiliin lisätään security identifier (SID), mistä määräytyy käyttäjien toimialue (Microsoft tech, User Groups). Halutessaan, että he voisivat autentikoitua toisessa toimialueessa, käyttäjien tulisi kuulua Universaaliin käyttäjäryhmään (Microsoft tech, User Groups).

Laurean opiskelijoiden käyttäjätilit sijaitsevat Otaverkon palvelimella. Projektin yhteydessä luodaan uusi toimialue laboratorioympäristöön, josta muodostetaan luottosuhde Otaverkon toimialueen välille. Jotta luottosuhteen avulla autentikointi toimisi, käyttäjien on kuuluttava universaaliin ryhmään.

4.1.2 SID

Security identifier (SID) on käyttäjätilissä ja käyttäjäryhmässä oleva Microsoftin tunnistusmenetelmä. Käyttäjän yrittäessä päästä käsiksi verkon resursseihin Windows vertaa käyttäjän SID tunnusta omiin oikeuksiinsa. Jos ne eivät täsmää, käyttäjä ei pääse resursseihin käsiksi. (Microsoft tech, SID).

Käyttäjät toisesta toimialueesta eivät pääse toisen toimialueen resursseihin käsiksi, jos heillä on toisen toimialueen SID -tunnus. Oletuksena käyttäjät kuuluvat globaaliin tai localiin käyttäjäryhmään. Tällöin heillä on oikeus oman toimialueen resursseihin. Käyttäjätilit, jotka tulevat toisesta toimialueesta on kuuluttava universaaleihin käyttäjäryhmiin SID-tunnistuksen vuoksi(Microsoft tech, SID domain).

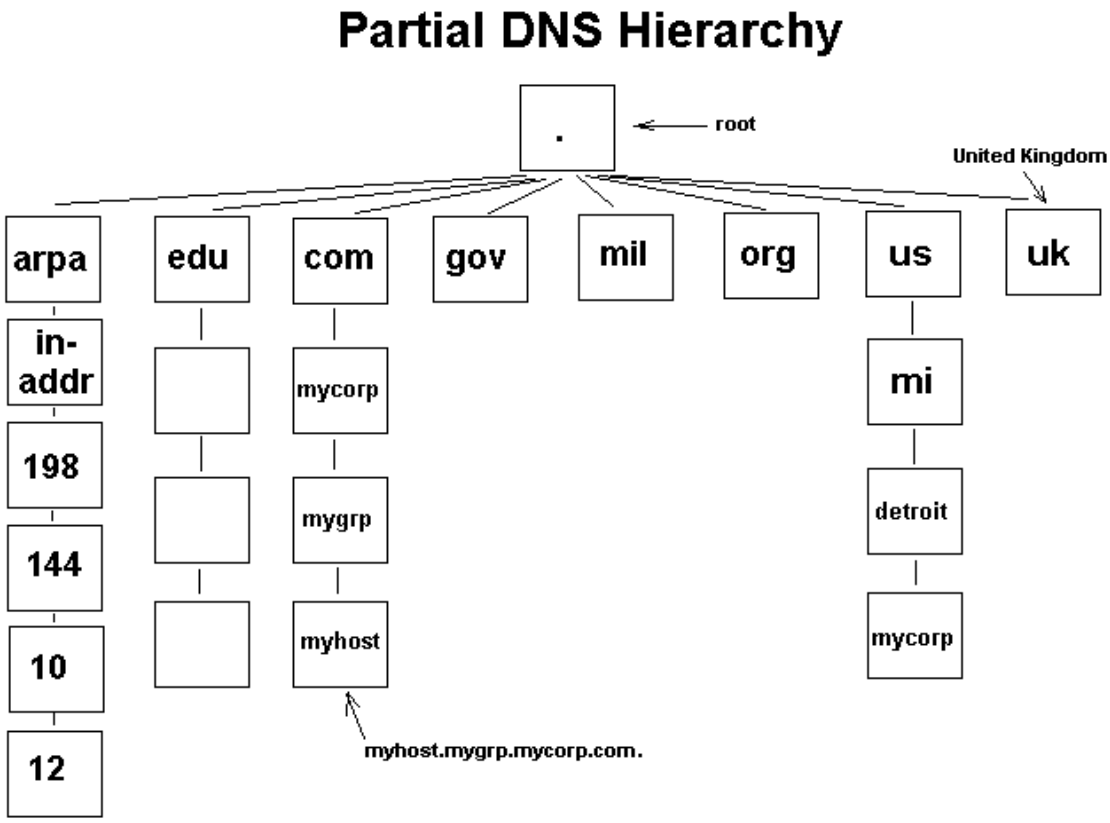
4.2 Nimipalvelin (Domain name system DNS)

Domain name system(DNS) tarkoittaa nimipalvelujärjestelmää. Tarve nimipalvelimelle muodostui jo 1970 -luvulla ARPANET-aikoihin. Tuolloin pieni käyttäjäryhmä, joka muodostui lähinnä tutkijoista, selvitti isännän (host) osoitteita HOSTS.TXT tiedostosta. Nopean tietoverkon kasvun johdosta HOST.TXT ei enää pysynyt kehityksen mukana. 1984 Paul Mockapetris USC tiedeinstituutista kehitti arkkitehtuurin, joka RFC 1034 ja 1035 dokumenteissa määritellään Domain name systemiksi eli nimipalvelujärjestelmäksi (Paul Abitz ym. 1997, 3-4.).

DNS (Domain Name System) on hierarkkinen hajautettu tietokantajärjestelmä, joka vastaa FDQN-nimien rekisteröintiin, kyselyihin sekä staattisten nimien muuntamisesta IP-osoitteeksi. DNS- päätehtävä on muuttaa erillisten verkkoresurssien nimet IP-osoitteeksi. DNS-palvelinta kutsutaan nimipalvelimeksi (Jyrki Kivimäki 2003. server, 958.).

Kaikessa yksinkertaisuudessaan nimipalvelujärjestelmä on tietokanta isäntien osoitteista. Sen tarkoituksena on muuttaa käyttäjäystävälliset isäntä nimet IP-osoitteiksi, koska tietoliikenne toimii IP-osoitteilla(Paul Abitz ym. 1997, 11-12.).

Esimerkiksi selvitettäessä www.wicipedia.org-osoitetta tietokonepääte kysyy omalta nimipalvelimeltaan tietääkö se www.wicipedia.org IP-osoitteen. Jos oma nimipalvelin ei tiedä, lähetetään kysely Root eli juuritason nimipalvelimelle. Juuritason nimipalvelin kertoo missä on .org-nimipalvelin ja lähettää kyselyn .org nimipalvelimelle, joka tietää www.wicipedia.org IP-osoitteen. Käyttäjä saa tietoonsa haluamansa IP-osoitteen, mikä mahdollistaa Internetissä surffaamisen (wicipedia dns).



Kuva 3. nimipalvelujärjestelmän hierarkkinen rakenne

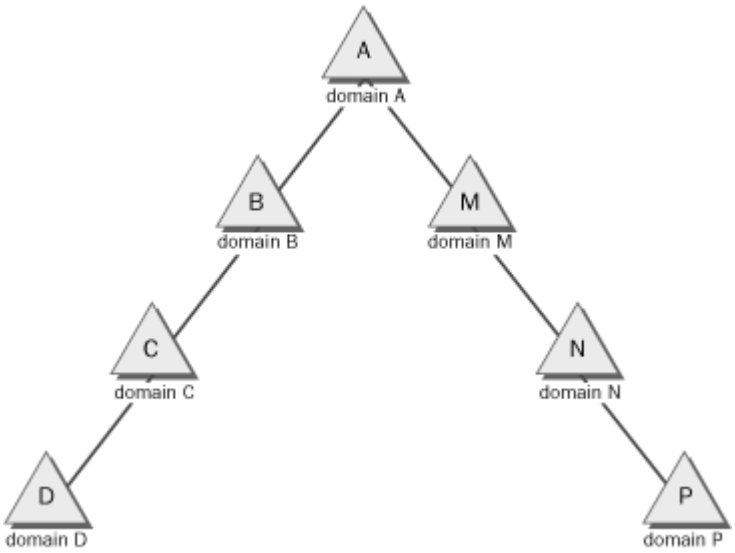
Projektissa pystytetään nimipalvelin laboratorioympäristöön. Laboratorioluokissa sijaitsevien päätteiden nimipalvelukyselyt ohjataan laboratorion nimipalvelimelle. Tämä tarkoittaa, että kaikkien laboratorioympäristössä sijaitsevien tietokoneiden ensisijainen nimipalvelin on *labra*-nimipalvelin. Kaikki kyselyt, joita *labra*-nimipalvelin ei itse tiedä, ohjataan (forwardoidaan) Otavekon päässä sijaitseviin nimipalvelimiin. Projektia ennen laboratorioympäristössä olevien koneiden ensisijainen nimipalvelin sijaitsi Otaverkossa.

4.3 Toimialue (Domain)

Windows 200/2003- palvelinympäristössä toimialue tarkoittaa tietokoneiden ryhmää, joka käyttää yhteistä aktiivihakemistotietokantaa. Aktiivihakemisto on hakemistopalvelu windows 2003 palvelimella ja sitä ylläpitää toimialueen ohjauspalvelimet (Domain Controller) (Jyrki Kivimäki 2003, server, 571.).

Järjestelmävalvojan näkökulmasta toimialue tarkoittaa keksitettyä järjestelmähallintaa, koska kaikki käyttäjätiedot on tallennettu aktiivihakemistoon vain kerran (Jyrki Kivimäki 2003, server, 571.).

Käyttäjien näkökulmasta toimialueeseen liittyminen tarkoittaa sitä, että kaikkiin verkon resursseihin, kuten kirjoittimiin, sovelluksiin ja verkkolevyille päästään käsiksi yhdellä sisäänkirjautumisella. Toimialueessa olevien käyttäjien koneita voidaan hallinnoida tehokkaammin (Jyrki Kivimäki 2003, server, 572.).



Kuva 4. Toimialueen rakenne yksittäisessä metsässä

Organisaation koosta riippuen toimialueita voi olla yksi tai useampi puurakenne hierarkiassa. Eri toimialueilla on määritelty erilaiset käyttäjäoikeudet (www.microsft.com/technet domain).

Projektin yhteydessä luodaan laboratorioympäristöön *labra*-toimialue. Koneet laboratorioympäristössä liitetään *labra*-toimialueeseen. *Labra*-toimialueen aktiivihakemisto on tyhjä käyttäjätileistä. Jotta käyttäjät pääsevät kirjautumaan omilla käyttäjätunnuksillaan *labra*-toimialueeseen, on luotava luottosuhde *Laurea*-toimialueen välille. Tällöin *Laurea*-toimialueen käyttäjätilit ovat *labra*-toimialueen käytössä. Tämä tietoliikenneproseduuri tapahtuu LDAP (Lightweight directory access protocol)-kyselyllä.

4.4 LDAP (Lightweight directory access protocol)

LDAP eli Light Directory access protocol on sovellustason protokolla, joka mahdollistaa kyselyt ja muokkaukset aktiivihakemistossa TCP/IP:een päällä. LDAP:lla voi hakea aktiivihakemistosta sinne määriteltyjä käyttäjätietoja mm. puhelinnumeroita, osoitteita jne. (wikipedia, LDAP).

Ldap-verkkoprotokolla tarjoaa yksinkertaistetun yhteystavan X.500-hakemistopalveluun. Ldap-verkkoprotokolla kulkee TCP:n tai muun luotettavan verkkoprotokollan päällä, mutta tarjoaa vain X.500 -standardin tärkeimmät palvelut. Ldap-verkkoprotokollalla on mahdollista tehdä asiakasohjelmista kevyempiä ja nopeampia toteuttaa: asiakasohjelma voi olla esimerkiksi sähköpostiohjelman osoitemuistio, josta haetaan henkilöitä ja organisaatioiden sähköpostiosoitteita nimen perusteella. (wikipedia, LDAP).

LDAP:ia voi käyttää käyttäjätunnistukseen. Sitä tukee useimmat UNIX-järjestelmät ja Microsoftin aktiivihakemisto käyttää LDAPin pohjalla kerberostunnistusta. LDAP-käyttäjätunnistuskyselyssä LDAP käy tarkistamassa aktiivihakemistosta oliko annettu salasana ja käyttäjätiedot oikein ja palauttaa nämä tiedot käyttäjälle. LDAPin avulla voi myös tarkistaa samalla metodilla käyttäjäoikeudet tiettyyn resurssiin (wikipedia, LDAP).

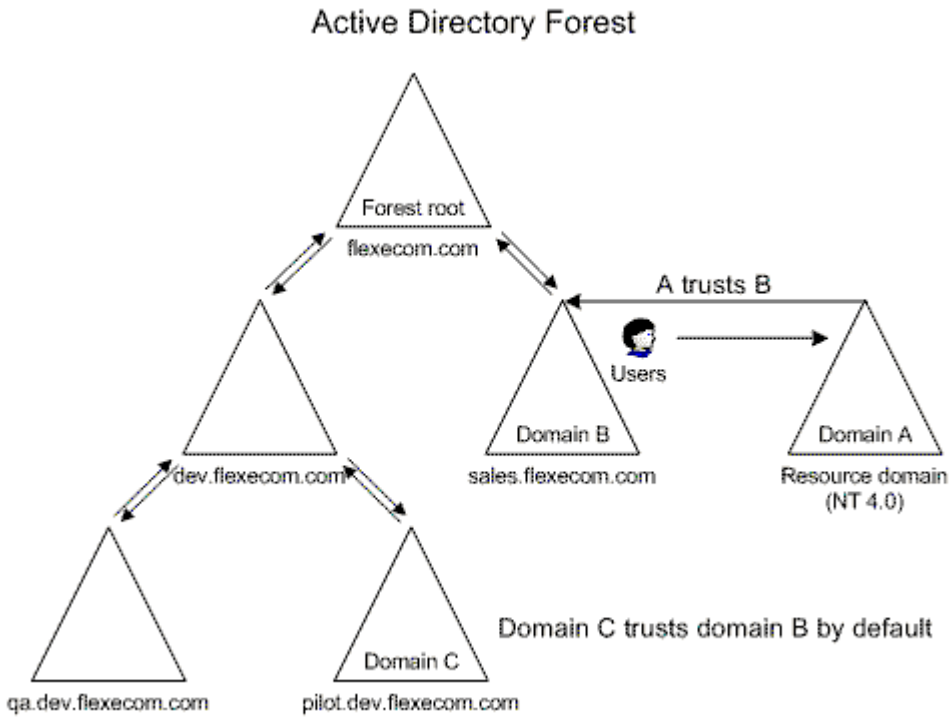
Projektissa LDAPia tullaan käyttämään käyttäjätietojen tunnistamiseen eli autentikointiin. *Labra*-toimialueelle kirjautuvat käyttäjät tarkistetaan LDAP:a käyttäen *Laurea*-toimialueesta. Jotta käyttäjätunnistus toimisi LDAP:a käyttäen on muodostettava luottosuhde kahden toimialueen välille (*labra*-toimialueen ja *Laurea*-toimialueen välille).

4.5 Luottosuhde (trust)

Toimialueiden väliset luottamussuhteet muodostavat luotetun tiedonsiirtokanavan (Secure Channel), jonka avulla tietokone toisessa toimialueessa voi vastaanottaa ja siirtää tietoja toisessa toimialueessa sijaitsevan tietokoneen kanssa. Luottosuhteessa tietokone, joka on luottavassa (trusting) toimialueessa, luottaa luotettavaan (trusted) toimialueeseen ja voi käyttää tämän resursseja. Luottamisella tarkoitetaan uskovan käyttäjätilien ja niiden käyttäjäoikeuksien toisessa toimialueessa olevan sellaisia, joita luotettu väittää(Kivimäki 2003, AD, 981.).

Luottosuhteita on yksisuuntaisia ja kaksisuuntaisia. Yksisuuntaisissa luottamussuhteissa luottamus on yksisuuntaista eli vain toinen osapuoli luottaa toiseen. Kaksisuuntaisissa luottamussuhteissa luottamus on molemminpuolista eli molemmat osapuolet luottavat toisiinsa (Kivimäki 2003, AD, 982-983).

Luottamussuhde voi olla toimialueiden välistä tai metsien välistä luottamusta (metsässä monta toimialuetta). On valittava tarpeidensa mukaan sopivin vaihtoehto (microsoft/tech (Domains trust).



Kuva 5. Luottamussuhteet toimialueiden välillä

Toimialueen kuuluessa samaan metsään heillä on oletuksena luottamussuhde keskenään ja he voivat jakaa keskenään resursseja (katso kuva 5.). Toimialueen kuuluessa eri metsään on luotava luottosuhde metsien välille (microsoft/tech (tust)).

Projektissa *labra*-toimialue on omassa metsässään ja *laurea*-toimialue omassaan. Jotta heidän välisiä resurssejaan voitaisiin jakaa, on muodostettava luottamussuhde. Tarkoituksena on, että l*abra*-toimialueen käyttäjät voisivat autentikoitua käyttäjätunnuksilla, jotka sijaitsevat *Laurea*-toimialueella. Projektissa luodaan yksisuuntainen luottamussuhde, jossa *labra*-toimialue on luottava (trusting) ja *Laurea*-toimialue on luotettu (trusted).

5 Palvelimen asentaminen ja sen konfigurointi

Tässä luvussa käsitellään projektin toteutusta. Tarkoitus on kertoa miten palvelinprojekti on toteutettu sekä dokumentoida mahdollisimman tarkasti palvelinasetukset tulevaa ylläpitoa ajatellen.

5.1 Sijainnin valinta

Projektissa pystytettävä palvelin on pystytettävä laboratorioverkkoon ja koska palvelin tulee olemaan enimmäkseen laboratorioympäristön sisäverkon käytössä, on se hyvä pystyttää sisäverkkoon. Sisäverkko on tietoturvallisempi ratkaisu palvelimelle ja palvelin tulee ensisijaisesti pystyttää sisäverkkoon, jos sitä ei tarvita ulkoverkon käytössä (Jani Aaltonen, 2008).

Palvelimen pystytykseen valittiin Neon -laboratorioluokka, sillä se on Tapani Viitasen rakentama valmis tietoverkko, ja muiden laboratorioluokkien tietoverkkoratkaisut ovat kesken. Tulevaisuudessa pyritään, että muiden laboratorioympäristöluokkien tietoverkkorakenne muistuttaa Neon-laboratorioluokkaa. Nämä muutokset tehdään todennäköisesti tulevaisuudessa opinnäytetyön muodossa(Julius Tuomisto, 2008).

5.2 Windows 2003 serverin asentaminen

Palvelintietokoneeksi valittiin Laurea Leppävaaran omistama Osbornen server -tietokone. Osborne server -tietokone sopi erinomaisesti tähän projektiin. Se on tarpeeksi tehokas Intel Xeon neliydinprosessorilla sekä RAID -ohjaimella varustettu tietokone, joka on tarkoitettu palvelinkäyttöön. Lisäksi tietokone oli käyttämättömänä.

Tietokoneeseen oli asennettu valmiiksi Windows Server 2003, mutta päätteen salasana ei ollut kenenkään tiedossa, joten se jouduttiin asentamaan alusta. Windows server 2003 asennus alkoi 3. syyskuuta 2008 ja kesti koko päivän, sillä siihen jouduttiin asentamaan kaikki alusta, muun muassa ajurit. Palvelimen nimeksi tuli LABRA-AD ja käyttäjätunnukseksi **administrator** salasanalla **admin**.

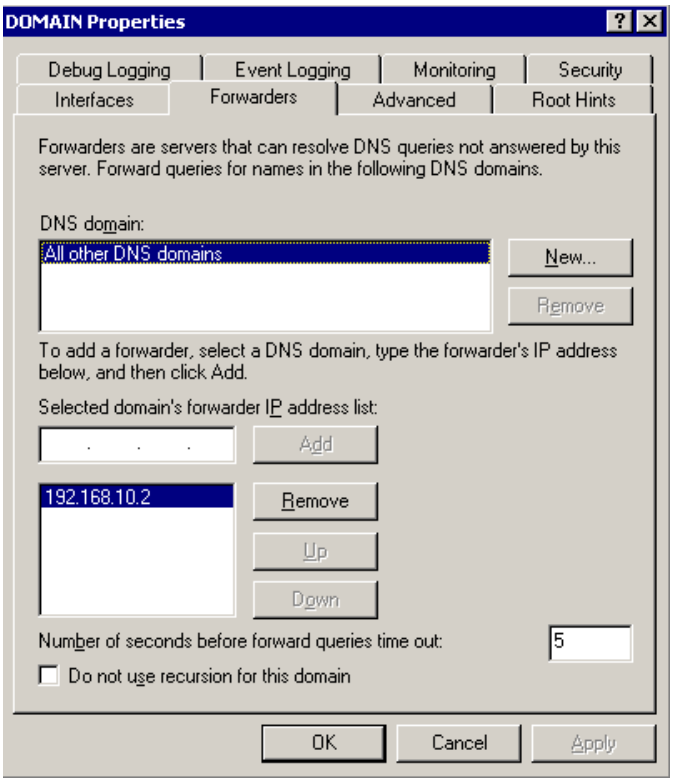
5.3 Palvelimen verkkoasetusten määrittäminen

Tapani Viitasen rakentamassa Neon-laboratoriotietoverkossa päätteet saavat IP-osoitteensa DHCP -palvelimelta, joka sijaitsee Laurean ASA -reititinpalomuurissa. Neon-tietoverkkoon on varattu osoiteavaruudesta 100 IP-osoitetta, joista 50 ensimmäistä on jätetty pysyviä IP-osoitteita varten. Kiinteitä IP-osoitteita kannattaa käyttää laitteissa, jotka käyttötarkoitustensa takia tarvitsevat pysyviä IP-osoitteita. Tällaisia ovat esimerkiksi tulostin ja erilaiset palvelimet(Tapani Viitanen, 25).
Neon-tietoverkon osoiteavaruus on 192.168.11.0 aliverkkopeitteellä 255.255.255.0. Palvelimen IP-osoitteeksi valittiin 192.168.11.10, koska se tulee toimimaan myös nimipalvelimena ja hyviin tapoihin kuuluu, että nimipalvelimille annetaan kymmenen tarkkuudelle IP-osoitteita.

5.4 DNS-palvelimen asentaminen ja konfiguraatio

DNS-palvelin otetaan käyttöön asentamalla DNS-palvelu (DNS Service) Windowsin 2003 -tietokoneeseen ja konfiguroimalla DNS tämän jälkeen. DNS-palvelimelle on määritettävä kiinteä IP-osoite(Jyrki Kivimäki 2003, server, 966).

Windows Server 2003 palvelimelle asennettiin nimipalvelinpalvelu käyttäen Windowsin omaa Configure your server wizardia. Nimipalvelimen IP-osoitteeksi määriteltiin 192.168.11.10 ja isäntänimeksi tuli *labra.local*. Kaikki DNS-kyselyt ohjattiin (forwardoitiin) Otaverkon nimipalvelimiin hedc1.laurea.local 10.3.8.20 ja opdc1.laurea.local 10.2.8.20.



Kuva 6. Nimikyselyiden edelleen ohjaaminen (Forwarders)

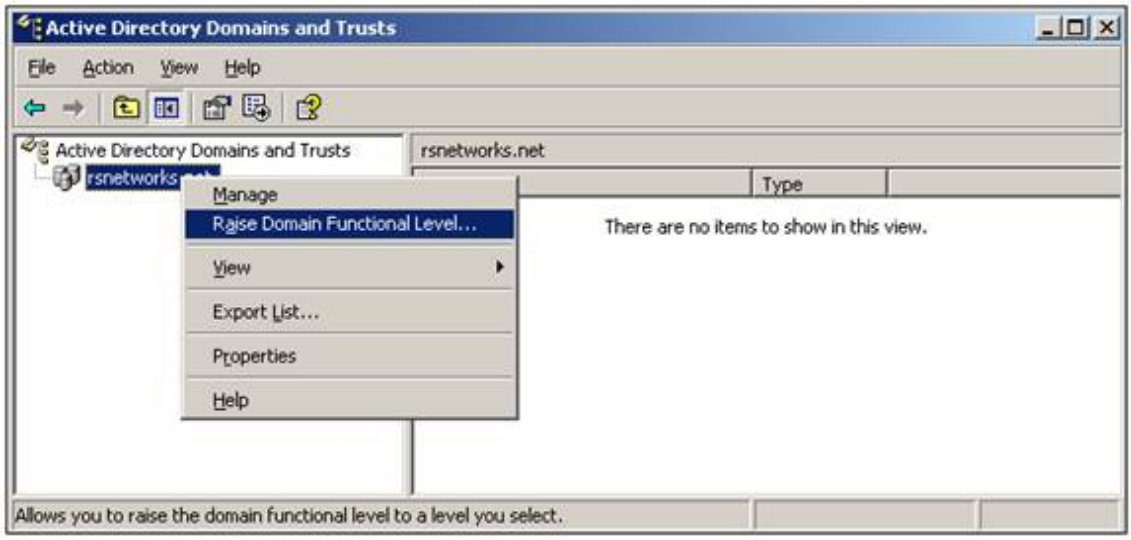
Kaikkien Neon-laboratorioluokassa sijaitsevien tietokoneiden ensisijainen nimipalvelin muutettiin osoittamaan *192.168.11.0 labra.local*, jonka jälkeen Neon-laboratorioluokkien päätteillä surffattiin Internetissä onnistuneesti. Ilman onnistunutta nimipalvelimen asentamista sekä onnistunutta nimikyselyiden edelleen ohjaamista Internetissä surffaaminen ei olisi ollut mahdollista.

5.5 AD-asentaminen ja konfiguraatio

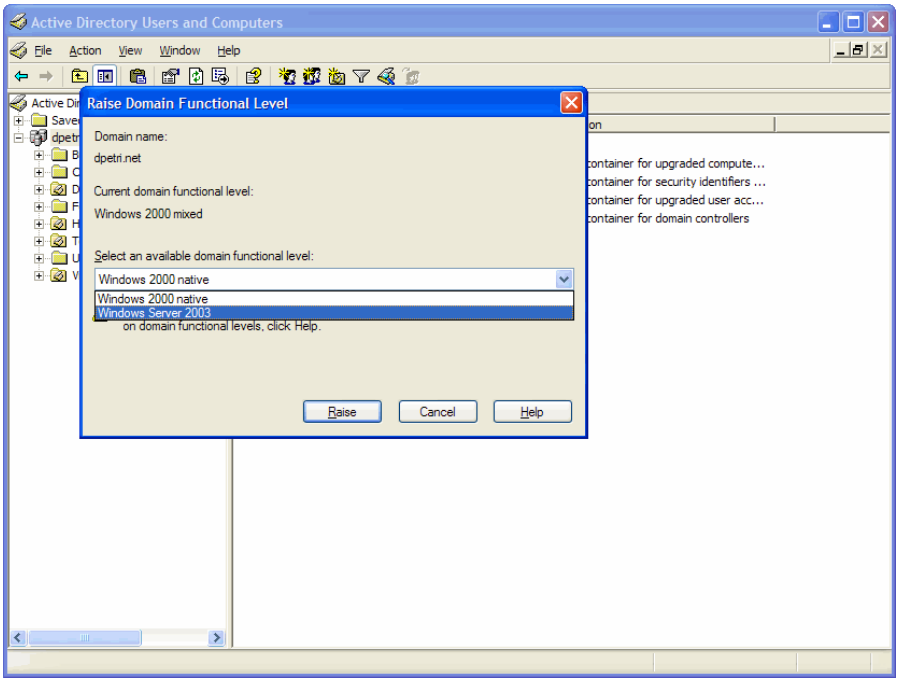
Windows 2003 server, joka on jäsenpalvelimena, voidaan muuttaa ohjauspalvelimeksi. Palvelimen muuttaminen ohjauspalvelimeksi tarkoittaa Active Directoryn (aktiivihakemiston) asentamista palvelimeen. Aktiivihakemisto voidaan asentaa Windows 2003 palvelimelle käyttäen Windowsin omaa asennusvelhoa. Asennusvelho kysyy tarpeelliset kysymykset, jonka jälkeen se muuttaa palvelimen ohjauspalvelimeksi luoden aktiivihakemiston käyttämät tietokannat ja määrittelee tarvittavat palvelut (Jyrki Kivimäki 2003, AD, 20).

Windows server 2003 jäsenpalvelimelle, johon oli aikaisemmin projektin yhteydessä asennettu nimipalvelin, asennettiin aktiivihakemisto käyttäen Windowsin omaa asennusvelhoa. Tulevan laboratorioympäristön toimialueen nimeksi muodostui labra.local. Laboratorioympäristön toimialuenimen valinnasta keskusteltiin Julius Tuomiston kanssa, joka on Laurean tietoliikennelaboratorion henkilökuntaa. Aktiivihakemiston ja palvelimen ylläpito siirtyy projektin päätyttyä tietoliikennelaboratorion hallintaan. Labra.local valittiin nimeksi, koska Laurea.local oli jo Laurean käytössä ja labra.laurea.local ei olisi ollut teknisesti viisas ratkaisu. Päädyttiin nimeen labra.local. Aktiivihakemistoon luotiin muutama testikäyttäjätunnus.

Metsien väliseen luottosuhteeseen vaaditaan molempien metsien olevan toiminnaltaan Windows 2003 tasoa. Oletuksena metsän sekä toimialueen taso on Windows 2000 native. Aktiivihakemistosta korotettiin sekä toimialueen taso, että metsän taso, jotta tulevaisuudessa voidaan muodostaa luottosuhde *laurea.localin* kanssa.



Kuva 7. Toimialueen korotus 1.



Kuva 8. Toimialueen korotus 2.

5.6 NEON-laboratorion toiminnan testaaminen

Kaikki tietokoneet Neon-laboratoriosta liitettiin onnistuneesti *labra.local -toimialueeseen*. Toimialueelle *labra.local* pääsi kirjautumaan luoduilla testitunnuksilla sekä kirjautumisen myötä konetilien nimet ilmestyivät aktiivihakemiston tietokantaan. Tämä todistaa, että aktiivihakemisto ja nimipalvelin on asennettu oikein.

6 Laboratorioympäristön tietoverkkorakenteen ongelmallisuus ja sen ratkaiseminen

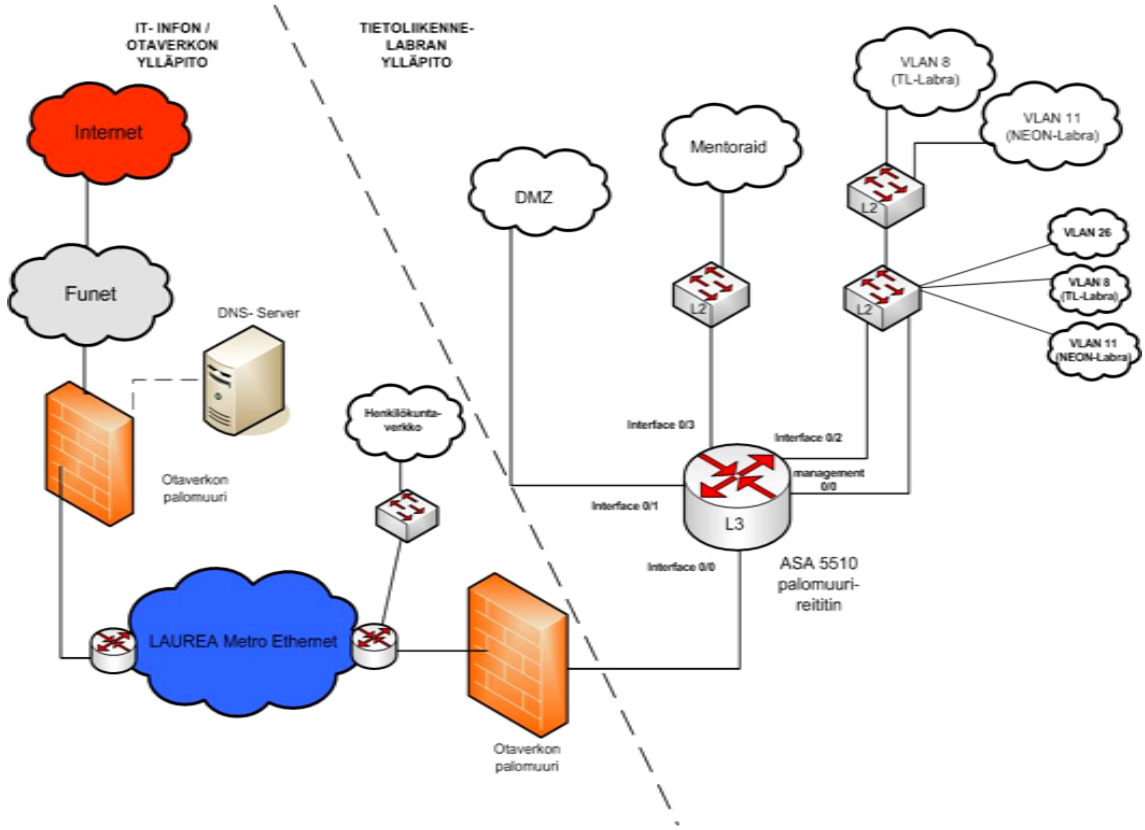
Projektin toteutukseen myötä havaittiin kaksi teknistä ongelmaa, jotka estivät projektia valmistumasta. Luottosuhteen muodostaminen kahden toimialueen välille ei ollut mahdollista, koska yhteyden muodostaminen NEON-laboratoriosta pois ja sisään oli estetty. Lisäksi muiden laboratorioluokkien päätteiden lisääminen *labra.local* -toimialueeseen ei onnistunut. Tämä johtui Tapani Viitasen määrittämistä tietoturva-asetuksista ASA-reititinpalomuurissa.

Luvussa avataan Laurea -Leppävaaran laboratorioympäristön tietoverkkorakenne. Pohjana käytetään Tapani Viitasen opinnäytetyöstä saatuja tietoja. Tapani Viitanen on 2008 tehnyt opinnäytetyön laboratorioympäristön verkkojärjestelyistä. Luvussa esitellään laboratorioympäristön tietoverkon ongelmallisuus projektin suorittamisen kannalta ja dokumentoidaan tulevat verkkomuutokset.

6.1 Laboratorioympäristön tietoverkkorakenne

Tapani Viitanen on hyödyntänyt tietoverkon rakentamisessa koululla olevaa Cisco ASA (Adaptive Security Appliance)-5510 palomuuri-reititintä. ASA palomuuri-reititin on Ciscon tietoliikennelaite, joka tarjoaa palomuuri- ja reititinominaisuudet laboratorioympäristöön. ASA palomuuri-reitittimen kautta laboratorioympäristön tietoliikenne kulkee ulos Laurean rakennuksesta, ilman että liikenne kulkee muiden verkon aktiivilaitteiden kuin Otaverkon tarjoamien palomuuripalveluiden kautta (Kuva 6). Näin mahdollistettiin se, että tietoverkkoon tehdyt mahdolliset muutokset tai ongelmat eivät vaikuta muihin Laurean tietoverkkoihin. ASA reititin-palomuurin hallinta on jätetty tietoliikennelaboratorion ylläpitoon (Tapani Viitanen 2008. opinnäytetyö, 25-26.).

Tapani Viitanen on jakanut Neon-laboratorion ja tietoliikennelaboratorion omiin virtuaalisiin lähiverkkoihin (VLAN), katso kuva 6. Virtuaalilähiverkot mahdollistavat tietoturvallisemman verkkoratkaisun. Ulkoapäin tulevat verkkokyselyt on lähtökohtaisesti estetty ASA -reititin-palomuurilta näihin lähiverkkoihin. Tulevaisuudessa tietoturvatasoon voidaan vaikuttaa ASA:aan tehtyjen palomuurisääntöjen kautta (Tapani Viitanen 2008. opinnäytetyö, 25-26.).



Kuva 9. Tietoverkon rakenne ja aktiivilaitteet

Projektissa toteutettava palvelinratkaisu vaatii, että ulkoapäin tiettyihin portteihin kohdistuvat kyselyt olisivat sallittuja *labra*-palvelimeen sekä tietty ulospäin lähtevä liikenne olisi sallittua. Lisäksi eri lähiverkoissa sijaitsevien tietokoneiden on pystyttävä saamaan yhteys labra-palvelimelle. Tämä vaatii verkkojärjestelyjä ASA reititin-palomuuriasetuksissa.

6.2 Neon-laboratorion tietoverkkorakenne

Tapani Viitanen on rakentanut oman tietoverkon NEON-laboratorioon. NEON-laboratorion tietoverkko saa IP-osoitteensa DHCP-palvelimelta, joka sijaitsee ASA 5510 palomuuri-reitittimessä (Kaavio 6). DHCP-palvelimelle on varattu tietoverkkoa varten 100 kappaletta IP-osoitteita jaettavaksi. Tarvittaessa tätä määrää voidaan kasvattaa tekemällä muutoksia ASA:n konfigurointeihin. IP-osoitteen vuokra-ajaksi on määritelty yksi päivä. Tietoverkkoon sijoitetulle verkkotulostimelle on määritetty kiinteä (staattinen) IP-osoite. Kiinteitä IP-osoitteita kannattaa käyttää laitteissa, jotka käyttötarkoitustensa takia tarvitsevat pysyviä IP-osoitteita. Tällaisia ovat esimerkiksi tulostin ja erilaiset palvelimet. NEON-tietoverkon osoiteavaruudesta on jätetty 50 ensimmäistä osoitetta pysyviä IP-osoitteita varten(Tapani Viitanen 2008. opinnäytetyö, 28.).

Neon-laboratorion verkko on 192.168.11.1 aliverkkopeitteellä 255.255.255.0. Neon-laboratorion koneiden oletusreititin on ASA reititin-palomuuri. Neon laboratorio koneiden nimipalvelimet sijaitsivat Otaverkossa. Neon-laboratorion tietokoneet saivat IP-osoitteet ja DNS-asetukset automaattisesti ASA -reititinpalomuurilta(Tapani Viitanen 2008. opinnäytetyö, 27-30.).

Koska Otaverkolla ei ole tarjota NEON-tietoverkolle kuin rajallinen määrä IP-osoitteita, käytetään laitteiden osoitteina yksityisiä IP-osoitteita. Osoitemuunnokset yksityisten ja julkisten IP-osoitteiden välillä tapahtuvat ASA 5510 palomuurireitittimessä, hyödyntämällä Port Address Translationia (PAT) eli porttimuunnostekniikkaa(Tapani Viitanen 2008. opinnäytetyö, 27.).

Projektissa pystytettiin nimipalvelin Neon-laboratorion verkkoon IP-soitteella 192.168.11.10 Windows Server 2003-palvelimelle asennettiin aktiivihakemisto, jonka mukana toimialue *labra*.local. Kaikki tietokoneet liitettiin *labra*-toimialueeseen sekä tietokoneiden ensisijaiset nimipalvelimet muutettiin osoittamaan *labra*-nimipalvelinta Otaverkon nimipalvelimen sijaan.

Ongelmaksi muodostui se, että *labra*-palvelimen IP-osoite on yksityinen eikä siihen saada yhteyttä muualta, kuin Neon-laboratoriosta pelkästään IP-osoitteen takia. Myös kaikki saapuva liikenne ulkoapäin oli estetty Neon-laboratorion verkkoon. Sekä kaikki lähtevä liikenne Neon-

laboratoriosta oli estetty lukuun ottamatta DNS-kyselyitä. Toimiva ratkaisu saadaan muuttamalla ASA-reititinpalomuurin asetuksia.

6.3 Muiden laboratorioluokkien verkkorakenteet

Muiden laboratorioluokkien IP-osoiteavaruus sekä tietoturvamääritykset poikkeavat Neon-laboratoriosta. Ongelmana näissä luokissa projektin kannalta on, että niitä ei saa liitettyä *labra.local* toimialueeseen ilman verkkoasetusten suurta muutosta. Tulevaisuuden toivetila on, että muiden laboratorioluokkien IP-osoiteavaruus ja tietoturva-asetukset muistuttavat Neon-laboratoriota. Nykyiset laboratorioympäristön verkkoratkaisut ovat keskeneräisiä (Julius Tuomisto, 2003).

Julius Tuomiston kanssa sovittiin, että nämä verkkomuutokset jätetään tämän projektin ulkopuolelle. Tulevaisuudessa joku toteuttaa nämä verkkomuutokset opinnäytetyön muodossa. Muita laboratorioluokkia kuin Neon-laboratorioluokkaa ei liitetä toistaiseksi *labra.local* toimialueeseen. Muut luokat liitetään *labra.local*-toimialueeseen vasta verkkomuutosten jälkeen.

7 Verkkoasetusten määrittäminen sekä luottosuhteen muodostaminen

Tässä luvussa käsitellään sitä miten ASA-reititinpalomuuri ja siihen tehdyt muutokset mahdollistavat luottosuhteen muodostamisen toimialueiden välille. Luvussa käsitellään myös luottosuhteen muodostamista ja siihen liittyvää byrokratiaa.

7.1 Asa-reititinpalomuuri

ASA -palomuurireititin on Ciscon tietoliikennelaite. Se tarjoaa älykkäitä uhkien torjuntapalveluja sekä mahdollistaa turvatut tietoliikennepalvelut, pysäyttäen hyökkäykset ennen kuin ne ehtivät vaikuttaa yrityksen liiketoimintaan. Laitteeseen on yhdistetty palomuuri, hyökkäyksen torjunta ja VPN (Virtual Private Network)-ominaisuudet, joten ASA -reititinpalomuuri pystyy tarjoamaan ratkaisun yritysten tietoturvavaatimuksille. Palomuurireititin reitittää verkkokerroksen tietoliikenteen eri IP-aliverkoissa olevien virtuaaliverkkojen välillä. (Tapani Viitanen, 24.)

Ciscon ASA-reititinpalomuuri 5510 tarjoaa kehittyneitä tietoturva- ja tietoverkkopalveluita pienille ja keskisuurille yrityksille. Ciscon ASA-reititinpalomuuri pienentää yritysten tietoliikennekuluja ja mahdollistaa tietoverkon etähallinnan. Ciscon tietoturva- ja tietoverkkopalveluita voi hallita sekä tarkkailla Ciscon integroidusta Cisco Adaptice Security Device Manager-sovelluksesta. ASA-reititinpalomuurin käyttöliittymää voi hallita joko graafisella sovelluksella

Internet-selaimen päällä tai tekstipohjaisella käyttöliittymällä. ASA-reititinpalomuurissa on viisi ethernet-porttia sekä VLAN-tuki(www.cisco.com, ASA5510).

Kuva 10. ASA-reititinipalomuuri 5510

7.2 ASA-reititinpalomuuriin tehdyt muutokset

ASA-reititinpalomuuriin tehtiin asetusmuutoksia käyttäen Ciscon omaa selainpohjaista graafista käyttöliittymää. Julius Tuomistolla on käyttäjätunnukset, joilla voi hallita ASA-reititinpalomuuria.

Muutoksia tehtiin luottosuhteen muodostamisen mahdollistamiseksi. Lähtötilanne oli se, että kaikki liikenne lukuun ottamatta paluuliikennettä ja DNS-liikennettä oli estetty NEON-laboratorioluokkaan. Toivetilana on, että palvelimelta sallitaan haluttu liikenne ulospäin sekä sallitaan tietty liikenne ulkoverkosta palvelimelle päin.

7.2.1 NAT

Network address translation lyhenne NAT ja suomeksi osoitemuunnos tarkoittaa, että IP-osoitteen voi staattisesti muuttaa reitittimeltä toiseksi IP-osoitteeksi. Tätä hyödynnetään esimerkiksi yrityksissä, koska julkisia IP-osoitteita ei ole jakaa kaikille, useat päätteet voivat kommunikoida ulkomaailmassa samalla IP-osoitteella. NAT-toiminta määritellään tarkemmin RFC 1918 -dokumentissa(www.wicipedia.com, NAT).

Palvelimelle oli määritelty IP-osoitteeksi yksityinen IP-osoite 192.168.11.10. Yksityisen IP-osoitteen johdosta palvelimelle on teknisesti mahdotonta saada yhteyttä ulkomaailmasta. Ciscon ASA-reititinpalomuurista tehtiin osoitemuunnos NAT. Ciscon ASA-reititinpalomuuri muuttaa IP-osoitteen 192.168.11.10 ulos lähtevän liikenteen IP-osoitteeksi 193.166.247.150. Näin palvelimelle saadaan yhteys käyttäen IP-osoitetta 193.166.247.150, jonka ASA-reititinpalomuuri muuntaa 192.168.11.10 IP-osoitteeksi.

7.2.2 ACL

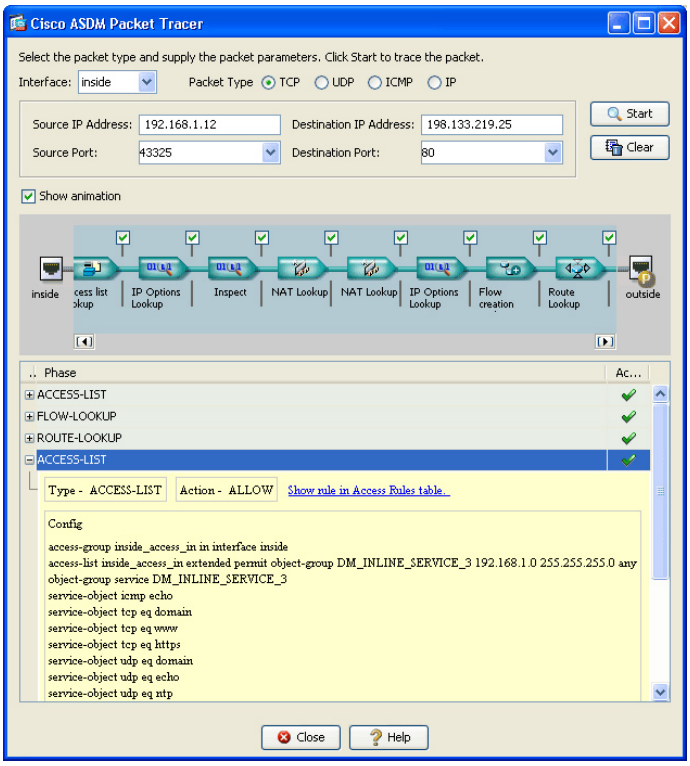
Access control list lyhenne ACL on todennäköisesti kaikkein käytetyin objekti Cisco IOS-käyttöliittymässä. Access control listin avulla voidaan suodattaa paketteja määrittämällä mistä mihin IP-osoitteesta liikenne on sallittua. Extendet access control listin avulla voidaan suodattaa paketteja myös kohde- ja lähtöportin perusteella (http://www.networkclue.com, ACL).

Cisco ASA-reititinpalomuurista sallittiin ACL:n avulla saapuva liikenne LABRA-palvelimelle (193.166.247.150) portteihin LDAP (389 UDP and TCP) Microsoft SMB (445 TCP) Kerberos (88 UDP). Tämä mahdollistaa luottosuhteen muodostamisen. Informaatio tarvittavista aukinaisista porteista luottosuhdetta varten saatiin Microsoft tech -sivuilta osoitteesta: http://technet.microsoft.com/en-us/library/cc756944.aspx.

Lisäksi sallittiin LABRA-palvelimelle saapuva DNS-liikenne portteihin TCP 53 ja UDP 53. Kaikki lähtevä liikenne LABRA-palvelimelta ulospäin sallittiin.

7.3 Yhteyden testaaminen

Ciscon ASA-reititinpalomuurin graafisesta käyttöliittymästä voi virtuaalisesti testata yhteyden toimivuuden määrittämällä lähtö-ja kohde- IP-osoitteen sekä lähettävän sovelluksen. Lopullinen testaus onnistui. Kaikkiin tarvittaviin portteihin saatiin yhteys LABRA-palvelimelle.



Kuva 11. Ciscon ASDM Packet Tracer

7.4 Otaverkkoon palvelupyyntö

Jarmo Tapio neuvotteli Otaverkko Oy:n kanssa sopimuksesta, jotta luottosuhde voidaan muodostaa sen hallitsemalle palvelimelle. Usean eri yhteydenpyynnön jälkeen saatiin Markus Kalliomäki Otaverkko Oy:stä Laurean ammattikorkeakoululle muodostamaan luottosuhdetta palvelimien välille.

7.5 Luottosuhteen muodostaminen

Neon-laboratoriopalvelimelta saatiin yhteys Otaverkossa sijaitsevan Laurean palvelimelle, mutta Laurean palvelimelta ei saatu onnistunutta yhteyttä Neon-labra palvelimelle. Yhteyttä testattiin onnistuneesti ping:in avulla. Tästä pääteltiin Markus Kalliomäen kanssa, että palomuurit estävät yhteydet tarvittaviin portteihin. Palomuureja palvelimien välillä on yhteensä kolme kappaletta, joista kaksi Otaverkko Oy:n hallinnassa ja yksi Laurean tietoliikennelaboratorion hallinnassa ASA-reititinpalomuuri.

Markus Kalliömäen kanssa tarkasteltiin määrittelemiäni ASA-reititinpalomuurin minun tietoturvanasetuksia. Tultiin siihen johtopäätökseen, että ASA-reititinpalomuurin tietoturvasetukset ovat oikein määriteltyjä ja ongelma lienee Otaverkko Oy:n hallitsemissa palomuureissa. Markus Kalliomäki lupasi ottaa asian hoidettavakseen.

Kahden kuukauden kuluttua Markus Kalliomäki ilmoitti Jarmo Tapiolle, että vika on ASA-reititinpalomuurissa eikä heidän hallitsemissaan palomuureissa. He olivat selvittäneet asiaa pitkään ja tehneet kaikki tarvittavat muutokset omiin palomuureihinsa, eikä yhteys luottosuhteenmuodostamista varten siltikään onnistunut.

7.6 Tutkimusongelman selvittäminen

Projektissa muodostui ensimmäinen kunnollinen tutkimusongelma, joka vaati selvittämistä. Projekti oli toteutettu ohjeita noudattaen ja kaiken piti olla kunnossa. Otaverkko Oy:n henkilökuntakaan ei osannut sanoa muuta kuin, että ongelma piili luultavasti Laurean omistamassa ASA-reitinpalomuurissa. Riku Salmenkylä tuli avuksi ongelman selvittämisessä.

Lähdimme Salmenkylän kanssa liikkeelle siitä, että sallimme kaiken liikenteen ASA-reitinpalomuurissa. Lisäksi laitoimme kytkimen ASA-reitinpalomuurin ulkoliitäntään (interface 0/0) kts. kuva 9. Kytkimeen liitimme Rikun kannettavan tietokoneen ja ethernetpiuhan, joka mahdollisti liikenteen ulkomaailmaan. Näin pääsimme suoraan testaamaan onko ongelma ASA-reititinpalomuurissa vai Otaverkon palomuureissa.

Testasimme onnistuneesti, että kaikki tarvittavat portit olivat auki ASA-reitinpalomuurista. Tämän testasimme telnet-komennolla. Lisäksi Salmeenkylän kannettavan tietokoneen ensisijaiseksi DNS-palvelimeksi määriteltiin Labra-palvelin. Salmenkylän DNS-liikenne toimi onnistuneesti. Yritimme liittää kannettavaa tietokonetta Labra-toimialueeseen huonolla menestyksellä. Usean tunnin selvittämisen jälkeen jäljitimme ongelman käyttäen Wireshark-ohjelmaa Salmenkylän kannettavassa. Tapahtui seuraavaa koneenliittämisessä Labra-toimialueeseen:

1. Kone liitetään DNS nimellä Labra.local ip= 193.166.247.150
2. ASA muuttaa IP 193.166.247.150 =192.168.11.10
3. Labra.local vastaa TCP paketissa "minun DNS labra-ad.local on osoitteessa 192.168.11.10"
4.ASA lähettää viestin kannettavalle: "toimialueeseen littäminen ok, IP-osoite AD:lle sama, kuin nimipalvelimellekin 192.168.11.10". Viesti tulee IP-osoitteesta 193.166.247.150
5. Kannettava "hämmentyy" ja yrittää ottaa yhteyttä 192.168.11.10 osoitteeseen tuloksetta.

Tämä prosessi toistuu jatkuvasti. Saimme Salmenkylän kanssa tilapäisesti koneen liittymään toimialueeseen muuttamalla Labra-palvelimelta Labra-ad osoitteen 193.166.247.150. Tämä oli vain hetkellistä, sillä palvelin ei anna AD-IP-osoitteen olla eri kuin sen oma IP-osoitteen eli 192.168.11.10. Palvelin päivittää oman IP-osoitteensa päivitetyn tilalle.

Keskustelin töissä asiasta Jani Aaltosen kanssa. Hän kertoi, että todennäköisesti homma ei tule onnistumaan ilman VPN-yhteyttä. Luin verkosta samanlaisia havaintoja. Verkossa kehotettiin muodostamaan VPN-yhteys palvelimien välille. Huomasin, että useilla eri henkilöillä oli samanlaisia ongelmia, joita he päivittelivät tietokonefoorumeilla. Kaikilla foorumeilla kehotettiin muodostamaan yhteys VPN:n avulla. Linkkejä sivustoille muun muassa http://www.experts-exchange.com (VPN1) ja http://www.computing.net (VPN2)

Riku Salmenkylä oli lukenut samanlaisia kommentteja asiasta ja keskustellut Jarmo Tapion kanssa. Tulimme kaikki siihen johtopäätökseen, että palvelimien välille on muodostettava VPN-yhteys. Tämä tulee olemaan erillinen projekti, joka todennäköisesti toteutetaan opinnäytteen muodossa. VPN yhteydestä pitää tehdä erillinen sopimus Otaverkon kanssa.

7.7 Tutkimusongelman analysointi

Havainto oli mielenkiintoinen. Olen lukenut satoja sivuja Microsoftin ohjeistuksia palvelimen hallinnasta ja luottosuhteen muodostuksesta enkä siltikään löytänyt viitteitä, että IP-osoitemuunnoksen läpi ei voi muodostaa luottosuhdetta ilman VPN-yhteyttä. Lisäksi alan ammattilaiset eivät osanneet kertoa ongelmasta etukäteen, viitaten Otaverkko Oy:ssä työskentelevään Markus Kalliomäkeen. Eikä koulun tietoverkko-opettajatkaan tienneet asiasta.

Tehokkaampana työkaluna It-ongelman selvittämisessä pidän Google hakupalvelua. Tähän johtopäätökseen olen päätynyt tämän projektin aikana. Vaikka It-alasta löytyy yllin kyllin materiaalia verkossa ja kirjallisessa muodossa, tieto on hajanaista ja siinä odotetaan, että lukija ymmärtää tarvitsemansa pohjatiedon. Näin ei kuitenkaan aina ole.

8 Työn arvio ja kehitysehdotus

Tässä luvussa käydään läpi projekti kokonaisuudessaan sekä arvioidaan projektin onnistumista verraten projektitavoitteisiin. Luvussa avataan lukijalle, mitä on projektin aikana opittu. Lopussa on kehitysehdotus, miten tuleva opiskelija voi jatkaa tästä projektista eteenpäin.

8.1 Arvio projektin onnistumisesta

Projektin päätavoite jäi osittain onnistumatta. Neon-laboratorioon ei pääse kirjautumaan kaikilla Laurean opiskelijatunnuksilla. Tämä tavoite koostui useasta eri tavoitteesta, joista kaikki muut onnistuivat lukuun ottamatta luottosuhteen muodostamista. Luottosuhteen muodostaminen vaatii VPN-yhteyden luomista. Tämä projekti tulee tarjoamaan jollekin opiskelijalle tulevaisuudessa opinnäytetyön.

Molemmat sivutavoitteet täyttyivät projektissa. Palvelin on tietoliikennelaboratorion hallinnassa, ja Labra-palvelin tarjoaa testiympäristön tietojenkäsittelyn opiskelijoille ja näin luo lisäarvoa Laurean ammattikorkeakoululle.

Pidän projektia onnistuneena, vaikka päätavoite jäi osittain onnistumatta. Syy tähän oli, että projektin aikana ilmeni tutkimusongelma, joka vaatii selvittämisen. Tutkimusongelman selvittämisen aikana koin monta "ahaa-elämystä" ja opin paljon uutta arvokasta tietoa. Tämä lienee konstruktatiivisen tutkimusmenetelmän tavoite. Se, että projekti olisi mennyt suunnitelman mukaisesti, olisi merkinnyt, että olisin oppinut vähemmän. Tutkimusongelma pakotti opiskelemaan yhä enemmän. Lisäksi Laurean ammattikorkeakoulu saa uuden opinnäytetyön aiheen jollekin opiskelijalle.

8.2 Kehitysehdotus projektin jatkajalle

Luottosuhteen muodostaminen vaatii VPN-yhteyden palvelimien välille. Molempien palvelimien pitää olla samassa verkkoavaruudessa. Tämä lopputyö sisältää kaiken tarvittavan tiedon palvelimen hallinnointia ajatellen ja luottosuhteen muodostamista varten. VPN-yhteyden voi luoda joko suoraan palvelimelta tai ASA-reititinpalomuurista. Se vaatii myös Otaverkon kanssa erillissopimuksen. Otaverkon kanssa työskentelemiseen kannattaa varata aikaa.

Lähteet

Kirjallisia lähteitä:

Järvinen P. & A. 2004. Tutkimustyön metodeista. Tampere: Opinpaja.

Vuorinen M. 2006. Windows 2003- lisäarvoa liiketoiminnalle (Case Esy OY).Espoo Laurea.

Tapani Viitanen 2008. Neon Laboratorion tietoverkon suunnittelu, rakentaminen ja dokumentointi. OpinnäytetyöLaurea.

Jylhä, E., Paasio, A., & Strömmer, R. 1998. Menestyvä yritys. Helsinki: Edita.

Laurea fakta 2008-2009. Laurea ammattikorkeakoulun.

Kivimäki J. 2004. Active Directorin verkonhallinta(AD). Helsinki: IT Press.

Kivimäki J. 2004. Windows 2000 server (server). Helsinki: IT Press.

Albitz P. & Cricret L.1997. DNS and BIND. Tokyo: O`REILLY.

Internet-sivustot ja elektroniset lähteet:

http://en.wikipedia.org/wiki/Active_Directory. (Aktiivihakemisto)

http://itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Active%20Directory.aspx (Aktiivihakemisto)

http://technet.microsoft.com/en-us/library/bb727067.aspx (User Groups)

http://technet.microsoft.com/en-us/library/bb727067.aspx(SID)

http://support.microsoft.com/kb/896593/ (SID domain)

http://en.wikipedia.org/wiki/Domain_name_system (DNS)

http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distrib/dsbb_act_zjfb.mspx?mfr=true (toimialue)

http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol (LDAP)

http://technet.microsoft.com/en-us/library/cc759554.aspx (domain Trust)

http://technet.microsoft.com/en-us/library/bb727050.aspx (Trusts)

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html (ASA5510)

http://en.wikipedia.org/wiki/Network_address_translation (NAT)

http://www.networkclue.com/routing/Cisco/access-lists/index.aspx (ACL)

http://www.experts-exchange.com/Networking/Windows_Networking/Q_22861585.html (VPN1)

http://www.computing.net/answers/windows-2003/join-domain-over-wan/7361.html (VPN2)

Haastateltavat:

Julius Tuomisto Laurea tietoliikennelaboratorion henkilökunta

Jani Aaltonen Salomaa Yhtiöiden palvelin vastaava

Kuva-otsikkoluettelo