LAUREA

Tutkimus- ja kehitysympäristön lähiverkon suunnittelu ja toteutus – case Laurea Leppävaara

Vehviläinen, Jari

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tutkimus- ja kehitysympäristön lähiverkon suunnittelu ja toteutus – case Laurea Leppävaara

Vehviläinen, Jari
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu 2010

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

Vehviläinen, Jari

Tutkimus- ja kehitysympäristön lähiverkon suunnittelu ja toteutus – case Laurea Leppävaara

Vuosi 2010 Sivumäärä 48

Laurea Leppävaaran laboratorioympäristöön oli aloitettu rakentamaan Laurean omasta sisäverkosta eriytettyä verkkoaluetta T. Viitasen ja D. Vorojeikinin toimesta vuosina 2008 ja 2009.

Laurea Leppävaaran alakerran tutkimuslaboratoriot ja luokkatilat olivat aiemmin liitetty Laurean sisäiseen lähiverkkoon. Oli tarve saada osa tiloista pois Laurean verkosta, IT-hallinnon ylläpidosta, ja saada ne Networks labin ylläpitoon. Näin verkon laitteilla voidaan suorittaa harjoituksia ja opetustilanteita entistä laajemmin vaikuttamatta Laurean lähiverkkoon. Tämä opinnäytetyö on jatkoprojekti Viitasen ja Vorojeikinin opinnäytetöille.

Opinnäytetyön tavoitteena oli suunnitella, laajentaa ja luoda uudistettu verkkoympäristö toimintaan Laurean tiloille. Uudistettuun verkkoon liitettyihin laitteisiin oli myös saatava toiminnallisuus kirjautumiseen opiskelijoiden omilla tunnuksilla.

Verkon vaatimukset ja määritykset kartoitettiin loogisella sekä fyysisellä tasolla. Verkon eri laitteet määritettiin vastaamaan standardeja ja parhaita käytäntöjä. Laitteita olivat Cisco ASA 5510 palomuurireititin, kytkimet, Windows 2003 palvelin sekä työasemat. Kirjautuminen Laurean tunnuksilla mahdollistettiin asentamalla laboratorion palvelimelle Microsoft aktiivihakemisto ja luomalla luottosuhde Laurean aktiivihakemistopalvelimeen.

Tutkimuksen ja kehityksen kautta päästiin opinnäytetyön päätavoitteisiin. Opinnäytetyö kirjoitettiin tieteellisestä näkökulmasta niin, että dokumentointia voidaan käyttää tulevaisuudessa verkon rakenteen selvittämiseen sekä vianmääritykseen.

Työtä tehdessä todettiin että opinnäytetyön jälkeenkin verkkoympäristössä on kehitettävää. Osa-alueista tehtiin dokumentin loppuun kehitysehdotukset käytettäväksi Laurean Learning by Developing jatkoprojekteissa.

Asiasanat aktiivihakemisto, nimipalvelu, verkkosuunnittelu, kytkin, reititin, ASA 5510

Laurea-university of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Programme

Vehviläinen, Jari

Planning and carrying out a new laboratory network layout – case Laurea

Year 2010 Pages 48

During the years 2008 and 2009 Laurea students D. Vorojeikin and T. Viitanen had completed theses about reconstructing a part of the Laurea Leppävaara laboratory environment network.

Laurea Leppävaara first floor laboratories and classrooms were connected to Laurea's own local area network. There was a need to move these study environments out of Laureas IT-administration and get the administration under SIDlab Networks. This thesis is continuation to Viitanen's and Vorojeikin's theses on the same subject.

The objective of this thesis was to design and implement a new network environment using the existing network as a layout. One of the main tasks was to achieve student authorization on the computers so they could log in with their own student ID and password.

Network policies were evaluated on the physical and logical level. Essential network devices were configured to meet the standards and best practices. These devices included Cisco ASA 5510, switches, Windows 2003 Server and workstations. Login possibilities to Laurea's domain were achieved on the computers by installing the Microsoft Active Directory server and creating a trust relationship to Laurea's authenticating server.

By carrying out research on the used devices and software, all the objectives were reached. This thesis was written from a scientific perspective so the Networks lab can use the documentation for debugging and informational purposes on administering the new network.

Upon managing and researching the network and its usage, several improvement possibilities were found. These cases can be used as Learning by Developing opportunities by students in Laurea Leppävaara.

Key words active directory, network design, network configuration, switch, router, ASA 5510

Sisällys

1 Johdanto

Laurean alimman kerroksen laboratoriot ja luokkatilat olivat aiemmin Laurean yhteisessä lähiverkossa ja Laurean IT-palveluiden ylläpidossa. Tavoite oli ollut jo aikaisemmin, että alakerran laboratoriotilojen verkko eriytetään Laurean verkosta ja tuodaan Networks labin ylläpitoon ja erilliseen verkkoon. Eriytetyn verkon toteutuksen lisäksi haluttiin että opiskelijat pääsisivät kirjautumaan koneille omilla käyttäjätunnuksillaan.

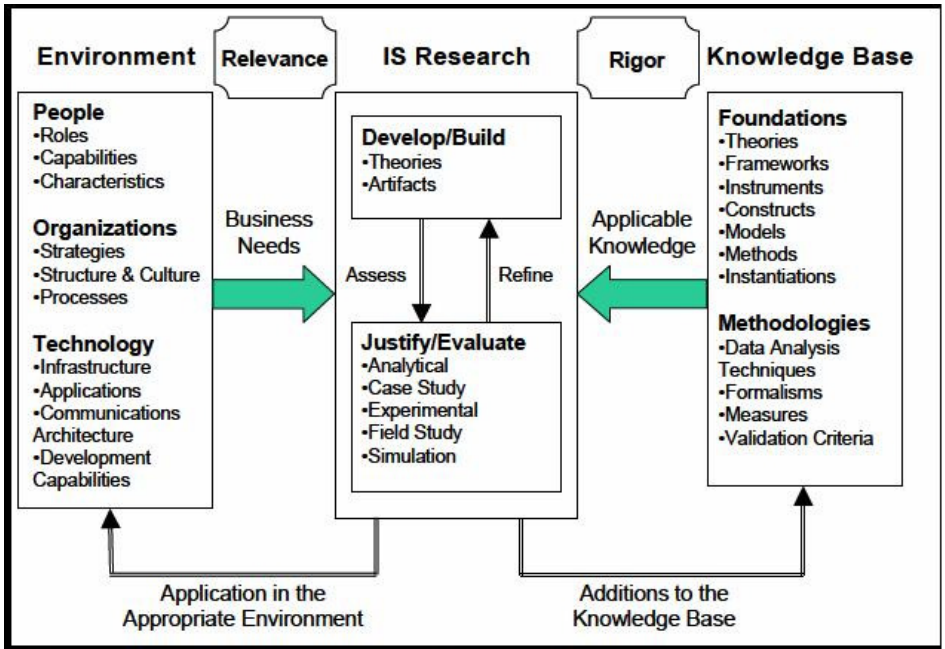
Projektiin liittyy verkon fyysisen ja loogisen rakenteen suunnittelu ja toteutus. Työssä kartoitetaan, mitä palvelimia tarvitaan ja minkälaisia asetuksia ne tarvitsevat. Kaapelointi ja verkon laitteet, kuten kytkimet, palvelimet ja reitittimet dokumentoidaan, sekä suunnitellaan ja toteutetaan laitteisiin asetusten uudelleenmäärittely. Aihe on jatkoa Daniel Vorojeikinin vuonna 2009 valmistuneelle opinnäytetyölle, jossa Vorojeikin suunnitteli aktiivihakemisto- ja DNS-palvelut verkkoon, ja toimii siten jatkoprojektina Vorojeikinin toteutukseen.

Tutkimuksen tieteellinen arvo perustuu tehtyyn suunnitteluun ja käyttöönottoon ympäristössä, johon kyseistä verkkoa ei ole ennen toteutettu. Laboratoriotilat saavat käyttöön oman yksityisen verkkoalueen, joka tulee opiskelijoille ja henkilökunnalle käyttöön, kehittäen Laurea Leppävaaran resursseja ja palveluita.

2 Tutkimusmenetelmä

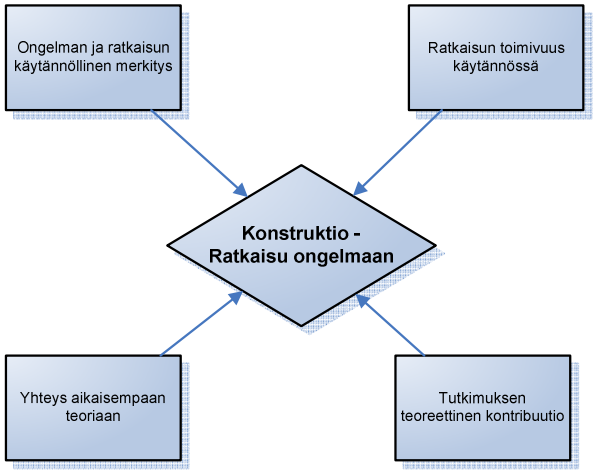
Kuvio 1:n mukaisesti informaatiojärjestelmien tutkimus perustuu ympäristön ja tiedon yhteisvaikutukseen. Ympäristöstä aiheutuu liiketoiminnan tarve kehittää asiaa, joka vaikuttaa tutkimuksen rakentamiseen. Tämä luo teorioita tai niin sanottuja artifakteja, joilla voidaan toteuttaa erilaisia menetelmiä tutkimuksen toteuttamiseen. Näistä voidaan jalostaa ideoita takaisin parempiin teorioihin tai artifakteihin. Kun tutkimus saavuttaa informaatioarvoa, sitä voidaan käyttää hyväksi takaisin ympäristön toimijoihin ja siten jalostaa lisää tutkittavia aiheita. Metodista voidaan käyttää termiä syklitys (Pirinen 2009). Ympäristössä on toimijoina ihmiset, organisaatiot sekä teknologia. Jokin näistä elementeistä tuo tarpeen tutkimukselle. Ihmisten roolit, kyvyt tai luonteenpiirteet voivat olla tarpeen luojia. Tarve voi myös syntyä organisaation strategioista, rakenteesta, kulttuurista tai prosesseista. (Hevner 2004.)

Tutkimus ei ole pelkästään ympäristön vaikutuksen ja organisaation tarpeen tuotos. Tarvitaan myös täsmällistä tietoa, jota voidaan soveltaa tutkimukseen ja näin ollen tutkimuksen kehitysprosessit teorioiden ja artifaktien suhteen on pohjustettu tietoon. Kun tutkimusta luodaan, saadaan lisää tietoa, jota voidaan iteroida ja siitä luodaan perustaa uusille teorioille, kehyksille, malleille, metodeille ja rakenteille. Voidaan kehittää myös metodologioita, joihin liittyy analyysitekniikoita, muodollisuuksia, mittareita ja varmennuskriteereitä. (Hevner 2004.)



Kuvio 1: Informaatiojärjestelmien tutkimustyön kehys (Hevner 2004)

Opinnäytetyössä käytetään konstruktiivista tutkimusmenetelmää, millä voidaan luoda ratkaisuja tutkimusongelmiin sekä kehitettyä käytännön ratkaisuja tutkimuksen ympäristöön. Menetelmä soveltuu uuden käytettävyyden ja ympäristön suunnitteluun olemassa olevien tietojen ja teorioiden pohjalta. (Järvinen & Järvinen 2000.) Tietoperusta haetaan luotettujen, tieteellisten ja teknisten lähteiden kautta. Tätä kautta voidaan konstruoida ratkaisumalli ympäristöön, tieteellisiin ja teknisiin lähteisiin viitaten (Kuvio 2).



Kuvio 2: Ratkaisun konstruointi

Työllä on selkeät teoreettiset ja käytännön tavoitteet, joihin pyritään analyyttisen ja loogisen tuotoksen mukaisesti. Työtä tullaan myöhemmin hyödyntämään verkon vianmäärityksessä tai muuten verkon rakenteen selvittämisessä, joten selkeä ja perustellusti tuotettu teksti on tärkeä. Tieteen tunnuspiirteinä dokumentoinnin tuottamisessa ovat objektiivisuus, kriittisyys, perusteellisuus, johdonmukaisuus, edistyvyys ja autonomisuus (Niiniluoto 2002, 37).

Konstruoinnin eri vaiheet (Järvinen & Järvinen 2000, 105):

- ongelman etsiminen & määrittely
- esiymmärryksen hankinta
- ratkaisumallin konstruoiminen
- ratkaisun toimivuuden testaus.

Tutkimuksen luominen lähtee ongelman etsimisestä ja määrittelystä. Kun aihe on rajattu ja selvitetty mitä toimijoita ja ympäristöjä aiheeseen kuuluu, voidaan luoda teoreettinen tietopohja. Vaihe ei ole suoraviivainen, vaan dokumentteihin ja tutkimuksiin palataan myöhemminkin tutkimuksen edetessä. Tarvittavan esiymmärryksen hankinnan jälkeen voidaan alkaa iteratiivisesti konstruoimaan ratkaisua kehitysympäristöön. Aluksi kehitetty ratkaisumalli voi muuttua iteraatiokierrosten jälkeen. Myös lisääntynyt dokumentaatio tuo arvoa tutkimustyölle (Järvinen & Järvinen 2000).

3 Käsitteet

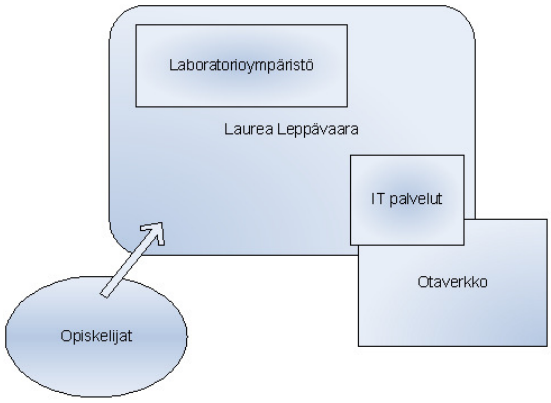
Luvussa käsitellään opinnäytetyössä ja verkkoympäristössä käytettävät termit. Rivi alkaa englanninkielisellä lyhenteellä, minkä jälkeen suluissa on lyhenteestä tulevat sanat. Näiden jälkeen on kirjoitettu lyhyt suomenkielinen selitys termille (Kaario 2002; Free On-Line Dictionary Of Computing 2010.)

- AD (Active Directory): Aktiivihakemisto on Microsoftin kehittämä hakemistopalvelu, joka tarjoaa käyttäjätunnistusta, autentikointia ja resurssien jakamista verkkoihin.
- ACL (Access Control List): Pääsylista on palomuureissa ja reitittimissä yleinen toiminto, jolla voidaan IP-osoitteiden tai muiden heurististen sääntöjen perusteella sallia tai estää liikenteen kulkeminen laitteen porttien läpi.
- AROMI: Logican AROMI ympäristö palvelee Laurean keittiöiden tuotanto-, varasto-, osto-, myynti-, ja laatuprosesseja sekä toiminnan ohjausta ja seurantaa. AROMI–palvelimet kuuluvat Networks laboratorion ylläpitoon.
- ASA (Adaptive Security Appliance): Ciscon kehittämä ja valmistama palomuurireitin, josta löytyy kattavat hallinta- ja tietoturvaominaisuudet. Projektissa on käytössä Cisco ASA malli 5510.
- ASDM: Adaptive Security Device Manager on Ciscon ohjelmisto jolla voidaan hallita ASA–laitetta graafisen käyttöliittymän avulla.
- DC (Domain Controller): Toimialueohjain on toimialueessa toimiva palvelin, joka hallinnoi autentikointia, käyttöoikeuksia, kirjautumista työasemilta ja muita hakemistopalvelun tehtäviä.
- DMZ (demilitarized zone): Demilitarisoitu alue on organisaation verkon alue, missä tietoturvaa on alennettu verrattuna verkon sisäosiin. Demilitarisoidulle alueelle sijoitetaan yleensä palvelut ja palvelimet, joilla on tarvetta päästä julkiverkkoon, esimerkiksi Internetiin.
- DHCP (Dynamic Host Configuration Protocol): DHCP on protokolla, joka jakaa lähiverkkoon kytketyille laitteille IP-osoitteet. Käytännössä DHCP helpottaa verkon hallintaa, koska näin määrityksiä ei tarvitse tehdä jokaiselle verkon koneelle erikseen.
- Windows server domain: Windows-verkkoympäristössä käytettävä toimialue, jota voidaan hallita keskitetysti. Toimii yleensä aktiivihakemiston kanssa ja tarvitsee toimiakseen vähintään toimialueohjaimen sekä nimipalvelimen.
- DNS (Domain Name System): Nimipalvelu on tekniikka, jolla IP-osoitteita voidaan kääntää verkkonimiksi ja toisinpäin.
- Switch: Kytkin liittää verkon tai verkkojen laitteita toisiinsa käyttäen VLAN-tekniikka ja MAC-osoitteiden perusteella tehtyä kytkentää.

- NAT (Networks Address Translation): Osoitteenkäännös on Internet-tekniikka, jolla voidaan muuttaa yksi tai useampi IP-osoite useammaksi osoitteeksi sisäverkkoon. Näin saadaan yhteys ulkoverkkoon, mutta ei käytetä kuin yhtä julkista IP-osoitetta.
- TRUNK (lyhennetään Trk): Kytkimissä käytettävä tekniikka, jolla voidaan jakaa useampia virtuaalilähiverkkoja yhteen fyysiseen porttiin. Verkkojen liikenteet pysyvät erillään ja seuraava kytkin voi jakaa verkot niille määritettyihin paikkoihin.
- VLAN (Virtual Local Area Network): Virtuaalilähiverkko on kytkimissä ja reitittimissä käytettävä tekniikka, jolla voidaan jakaa fyysinen verkko moniin loogisiin osiin. Yleisin VLAN-tekniikka IEEE 802.1Q, jossa käytetään tagging–menetelmää, joka merkitsee datapaketteihin tiedon siitä, mihin virtuaaliseen lähiverkkoon liikenne kuuluu.
- VPN: Virtuaalinen yksityisverkko (Virtual Private Network) on tunnelointi- ja salausprotokollia käyttäen luotu yksityisverkko julkisen verkon päälle.

4 Ympäristö ja yhteistyökumppanit

Opinnäytetyön tarkoituksena on kehittää Laurean oppimisympäristöä sekä parantaa tutkimus-, kehitys- ja innovaatiotyön laatua. Opiskelijat ovat Laurean toiminnan pääkohderyhmä ja näin ollen opinnäytetyön toteutus lähtee opiskelijaprosessien parantamisesta. Ympäristön toimijoiden suhteet voidaan esittää kuvio 3:n mukaisesti.



Kuvio 3: Laurean ympäristö

4.1 Laurea Leppävaara

Laurea Leppävaara käyttää LbD (Learning by Developing) -oppimismallia. Tämän tarkoitus on sitoa opinnot yhteen laajaksi kokonaisuudeksi sekä auttaa opiskelijoita luomaan enemmän yrityskontakteja yhteisten projektien muodossa. Koulutusohjelma painottaa oppimisen tapahtumista oppilaan aloitteista ja luentotyyppinen opetus saa vähemmän resursseja. (Laurea Fakta 2009.)

4.2 Otaverkko OY

Laurea on ulkoistanut verkkopalvelut Otaverkko Oy:lle. He tarjoavat Laurealle aktiivihakemisto–käyttäjäntunnistuspalvelun, verkkolevyt, lähiverkon sekä ulkoverkko eli Internetyhteyden.

Opinnäytetyössä rakennettava verkko kulkee Otaverkon infrastruktuurin läpi, jossa on vielä kaksi palomuuria ennen varsinaista yhteyttä Internetiin. Tästä johtuen projektissa tarvitaan yhteistyötä Otaverkon kanssa reitittimien, aktiivihakemistopalvelimen ja muiden verkon osien yhteensopivuuden määrittelemiseksi.

4.3 IT-palvelut

IT-palvelut vastaavat Laurean tietoteknisestä infrastruktuurista, joihin kuuluu verkko, palvelimet ja työasemat sekä sovellusten kehittäminen ja ylläpito. IT-palvelut osallistuvat laitehankintojen suunnitteluun sekä rekisterin ylläpitoon ja laitteiden poistojen hallinnointiin. (Laurean palvelukuvaus 2010.)

Taulukko 1. Laurean IT-palveluiden toiminnat ja toimijat

TOIMINTA	**TOIMIJAT**
Laurean IT-helpdesk, IT-info ja asiakaspalvelu	ATK-harjoittelijat
Lähituki, Laurean hallinto	Isto Hamina
Lähituki, Leppävaaran Laurea	Petri Miinalainen
Lähituki, Otaniemen Laurea	Sami Ahlgren
IT-hankinnat (laitteet, lisenssit)	Ville Rautiainen
Opintohallinnon tietovarastot	Jori Komulainen
Palvelimet	Jarmo Tapio
Lähiverkot	Mika Salo, Isto Hamina
Ulkoiset tietoliikenneyhteydet	Jarmo Tapio
Yhteislevyalueet, L-asema	Sami Ahlgren
Sähköposti ja levykiintiöt	Timo Leipold

IT-palvelun kanssa tehdään yhteistyötä suorasti tai epäsuorasti. Yhteyshenkilöinä toimivat taulukon 1 mukaisesti kyseessä oleva vastuuhenkilö (tilanteesta riippuen).

4.4 Tutkimuslaboratoriot ja luokkatilat

Laurea Leppävaaran alakerrassa on kolme tutkimuslaboratoriota ja kaksi luokkatilaa joihin projekti toteutetaan: Networks lab, RED lab, NEON lab sekä tietokoneluokat 009 ja 010.

Networks labin toimenkuva on laboratoriolähiverkon ylläpito, sekä erilaiset IT–alan projektit niin opiskelijoiden, kuin henkilökunnankin toimesta. Laboratorioympäristön ylläpitotoiminnasta vastaa Riku Salmenkylä, sekä tutkimus- ja kehitystoiminnasta Jyri Rajamäki. Yksi projekti on TEKES -rahoitteinen ORE (Open Rendering Environment) hanke hajautetusta laskennasta, jonka projektipäällikkönä toimii Julius Tuomisto. Lisäksi Networks labissa toteutetaan opiskelijoille Interconnecting Networks -opintojakson yhteydessä CCNA (Cisco Certified Network Associate) mukaisia kytkin- ja reititinharjoituksia, jossa opiskelijat pääsevät käytännössä kokeilemaan lähiverkon laitteita sekä muokkaamaan niiden asetuksia.

RED lab keskittyy palveluinnovaatioiden suunnitteluun käyttämällä IES (International Expertise Service) mallia. Toiminta tukee ja parantaa korkean koulutuksen T&K-toimintaa, varsinkin kansainvälisten tutkimusharjoittelijoiden osalta.

NEON lab on 16 pöytäkoneen ja usean palvelimen työskentelytila opiskelijoille ja henkilökunnalle, missä he voivat toteuttaa projekteja, käyttäen laboratoriotilassa olevia laitteita.

Luokkatilat 009 sekä 010 ovat 30 tietokoneella, tulostimilla ja videotykeillä varustettuja opetustiloja, joita käytetään opintojaksojen luentojen ja kontaktiopetuksen pitämiseen.

5 Projektin määrittely

5.1 Tausta

Vuonna 2008 Tapani Viitanen suunnitteli NEON labiin Laurean omasta verkosta eriytetyn verkkoalueen, joka tuli silloisen Tietoliikennelaboratorion ylläpitoon. Viitanen toteutti verkon ASA-laitteella toimivaksi, sekä suunnitteli kytkennät. Tästä jatkokehityksenä Daniel Vorojeikin lähti toteuttamaan opinnäytetyönä verkon laajentamista ja aktiivihakemistokirjautumista NEON labiin.

Laboratoriotilat tarvitsivat oman aktiivihakemistopalvelimen omistuksellisista syistä. NEON labin koneet eivät olleet Laurean IT-palveluiden ylläpidossa, joten niitä ei voitu liittää Laurean toimialueeseen verkossa. Aktiivihakemistopalvelimen ja kirjautumisen toteutuksessa ei kuitenkaan teknillisistä syistä onnistuttu. Vorojeikinin mukaan verkon reunareitittimenä toimivan ASA-laitteen osoitteenkäännös aiheutti aktiivihakemistokirjautumisen toimimattomuuden. Vorojeikinin opinnäytetyö kuvasi asetukset, mutta yksi ongelmallisuus tuli

esiin Otaverkon palomuurien ja ASA-laitteen kanssa. Tämä ongelmallisuus kuitenkin korjattiin Laurean IT-hallinnon toimesta, mutta kirjautuminen ei siitä huolimatta toiminut. Vorojeikin toteaa opinnäytetyössään (2009), että toimimattomuuden täytyy aiheutua ASA-laitteesta ja sen asetuksista.

Vorojeikin oli tehnyt verkon luomiseen tarvittavia muutoksia ASA-laitteeseen ja suunnitellut uudistetut verkkokaaviot. Vorojeikinin ja Viitasen opinnäytetöistä saadaan tietoa verkon nykyisestä toiminnasta ja suunnitelluista päivityksistä.

5.2 Tavoitteet

Opinnäytetyön tavoitteena on muuttaa Laurea Leppävaaran Networks lab, NEON lab ja RED lab sekä luokkatilojen 009 ja 010 laitteet Laurean 10.8.0.0 IP-avaruudesta 192.168.0.0 IP-avaruuteen ja näin ollen eriyttää ne Laurean verkosta ja IT-hallinnon ylläpidosta. Verkko haluttiin eriyttää koska haluttiin tarjota kehitysympäristö, mikä mahdollistaa uusien laitteiden ja ohjelmistojen kokeilun tutkimus ja kehitysprojekteissa sekä opetustilanteissa. Laurean lähiverkosta erillään oleva verkkoalue tarjoaa tähän paremmat ja tietoturvallisemmat mahdollisuudet. Tavoitteena oli myös pienentää ylläpidollisia kustannuksia ylläpidon siirtyessä Networks labille. Laboratoriotiloissa toteutetaan erilaisia verkkoprojekteja jotka eivät välttämättä ole täysin valvottuja.

Oli myös tarve että opiskelijat pääsevät kirjautumaan laitteille omilla käyttäjätunnuksillaan. Eriytetyssä lähiverkkoalueessa tämä ei ole suoraan mahdollista yhdistäen Laurean aktiivihakemistopalveluun ja toimialueeseen. Näin ollen tarvittiin laboratorioverkkoalueelle oma aktiivihakemistopalvelin, millä muodostetaan luottosuhde Laurean autentikoivaan aktiivihakemistopalvelimeen ja näin mahdollistetaan opiskelijoiden omien tunnusten käyttö laboratorioverkkoon kirjautumisessa.

Työn käytännön eri vaiheet eivät saa vaikuttaa verkon toimintaan tai lamauttaa laboratoriotilojen tai luokkatilojen verkkojen käytettävyyttä. Lisäksi Networks labissa pidettävät CCNA-harjoitukset (Cisco Certified Network Associate) on päivitettävä uudistettuun IP-avaruuteen.

5.3 Rajaus

Opinnäytetyön suunnitteluun ja toteutukseen kuuluvat kaikki uudistettavan verkon toimintaan liittyvät osa-alueet. Näitä ovat lupien hankkiminen, kaapeloinnin tekeminen ja uudistaminen, uusien kytkimien hankkiminen, työasemien aktiivihakemisto-kirjautumisen mahdollistaminen oikeaan toimialueeseen, aktiivihakemisto- sekä DNS-palvelimen toimintaan laittaminen ja

ASA-palomuurireititimen asetusten uudelleenmäärittäminen. ASA-laitteen asetukset sisältävät DHCP-palvelun, palomuurisäännöt, osoitteenkäännöksen (NAT) ja aktiivihakemisto–kirjautumisen uudelleenohjaamisen.

Opinnäytetyö keskittyy pelkästään Laurea Leppävaaran alakerran verkkoihin ja tiloihin. Verkon muutokset tai toiminta eivät vaikuta Laurean muuhun verkkoon.

ASA-laitteeseen on kytketty myös MentorAid-palvelin. MentorAid-etäluennot eivät ole Networks labin ylläpidossa. Tämän palvelimen ja verkon osan asetuksia ei muuteta ASA-laitteeseen, mutta ne huomioidaan uusia muutoksia tehdessä.

Uudistettu verkko tulee toimintaan Networks labissa, NEON labissa, RED labissa, sekä luokkatiloissa 009 ja 010. Tässä opinnäytetyössä Business- tai Security labia ei liitetä laboratorioverkkoon, vaan ne pysyvät Laurean omassa verkossa ja ylläpidossa. Valmius liittää nämä tilat uudistettuun verkkoon otetaan kuitenkin huomioon suunnitelmissa. Työn lopussa tehdään kehitysehdotus tilojen liittämisestä laboratorioverkkoon.

5.4 Riskit

Erilaisia riskejä projektiin tuovat laitteiden asetusten määrittäminen ja niiden toimivuuden takaaminen. Nämä riskit ovat suoraan verrannollisia toteuttajan pätevyyteen tehdä asetuksia, mutta riskejä voidaan ehkäistä hyvällä ennakkotiedolla ja taidolla muutettavasta laitteesta sekä ympäristöstä.

Edellisessä toteutuksessa Otaverkon palomuurien aktiivihakemiston ja luottosuhteen määrittelyt olivat isona riskinä, mutta Vorojeikinin mukaan (2009) Otaverkon hallinnoimat palomuurit ovat nyt määritetty oikein sallimaan aktiivihakemiston tarvitseva liikenne. Mahdollisuus kuitenkin on, että määritykset joudutaan tekemään uudestaan. Tässä tapauksessa ajallisten resurssien tarve kasvaa. Riskien toteutumisen ehkäisemiseksi luodaan tarvittavissa tilanteissa testiympäristöjä tai prototyyppejä, niin että verkon rakenteeseen ei tarvitse tehdä kokeilemalla muutoksia.

Ympäristön vaatiessa monia laitteita ja laitteistoja, pitää huomioida niiden vikasietoisuus ja toiminnallisuuden takaaminen. Laiterikon sattuessa Networks lab on ylläpidollisesti velvoitettu korjaamaan laitteistot, mahdollisesti tehden yhteistyö IT-palveluiden kanssa.

Luokkatilojen 009 ja 010 kytkimet tullaan vaihtamaan uusiin. Operaatiossa ilmenee riski yhteensopivuuden ja käyttöönoton helppouden suhteen. Mikäli käyttöönotto ei ole sujuvaa,

niin tilausten, fyysisten asennusten kuin ohjelmistopuolen asetusten osalta, projektin aikataulu voi muuttua suunniteltua pidemmäksi.

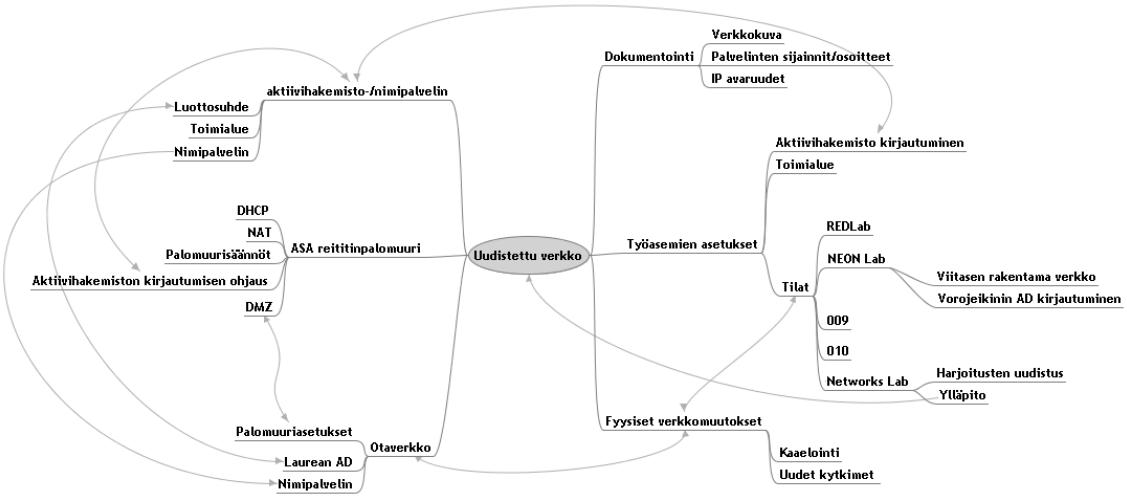
5.5 Tietosuojakäytännöt

Salassapito ja yksityisyydensuoja määriteltiin työn toimeksiantajan, Riku Salmenkylän toimesta. Sisäverkon osoitteistukset eivät vaadi sensuuria julkisesta dokumentista, mutta ulkoiset IP-osoitteet jätettiin julkisesta dokumentista pois. Myöskään käyttäjätunnuksia tai salasanoja ei julkaista missään dokumentissa. Ratkaisu perustellaan tietoturvan ja organisaation salassapidon määrityksin. Salasanat ja käyttäjätunnukset laitteistoon on dokumentoitu Word-tiedostoon Networks labin verkkolevylle, sekä varmuuskopioitu Networks laboratorion varmuuskopiointipalvelimelle.

6 Verkon määrittely

Päätavoitteena on verkon eriyttäminen ja siinä aktiivihakemistokirjautumisen toimintaan laittaminen. Alkuperäisen verkon dokumentaatio oli puutteellista ja joistain verkon osista sitä ei ollut ollenkaan. Tästä johtuen uusittu verkko dokumentoidaan opinnäytetyössä täydellisesti niin, että tulevaisuudessa voidaan tehdä vianmääritystä ja verkkodiagnosointia vaivattomasti.

Kuvio 4 kuvaa projektissa toteutettavat osa-alueet, eri toimijat ja niiden suhteet toisiinsa.



Kuvio 4: Projektin käsitekartta

6.1 Laboratoriopalvelin

Projektissa tarvittiin palvelin tarjoamaan resursseja verkkoon. Networks labilla oli omistuksessa palvelin, joka oli ollut käytössä Vorojeikinin opinnäytetyössä. Koska laite oli

käyttämättömänä, voitiin se ottaa uudelleen käyttöön tässä jatkoprojektissa. Palvelimessa on 1,6 Gigahertsin Intel Xeon prosessori, 2 gigatavua muistia ja 70 gigatavun SCSI kiintolevyt ja näille kuuluva ohjainkortti.

Projektissa käytettävään palvelimeen oli asennettu Windows Server 2003 käyttöjärjestelmä Vorojeikinin toimesta. Palvelimen funktio verkossa on tarjota työasemille aktiivihakemistokirjautuminen Laurean toimialueeseen sekä toimia nimipalveluna.

Viitanen ja Vorojeikin oli määritellyt osan verkon asetuksista, mutta monet asetukset vaativat uudelleenmäärittelyä vastaamaan uudistetun verkon vaatimuksia. Käyttöjärjestelmästä puuttui myös paljon tietoturvapäivityksiä, jotka asennettiin toteutusvaiheessa. Palvelimen nimeksi (hostname) valittiin LABRA-AD.

6.2 Aktiivihakemisto

Aktiivihakemisto (Active Directory, AD) on Microsoftin luoma ohjelmistoympäristö joka mahdollistaa käyttäjien tunnistuksen, autentikoinnin, hakemistopalvelut ja moduulien avulla resurssien jakamisen verkkoon. Näitä palveluita hallinnoidaan kolmella eri tasolla, joita kutsutaan metsäksi (forest), puuksi (tree) ja toimialue (domain). Aktiivihakemistopalvelimen tarkoitus on käyttäjien kirjautumisen mahdollistaminen työasemilta, käyttäjätunnuksien varmennus ja todennus, sekä resurssien tarjoaminen käyttäjille (Llewellyn & Craft 2001, 4).

Microsoftin Aktiivihakemisto on Laurean käyttämä hakemistopalvelu. Hakemistoon voidaan tallentaa erityyppistä tietoa. Nämä voidaan luokitella kolmeen eri kategoriaan: resurssit, palvelut ja käyttäjät. Resursseja ovat komponentit jotka ovat liitetty verkkoon ja niihin pääsy on tehty mahdolliseksi käyttäjille, joista esimerkkeinä IP-osoite, skanneri, tulostin tai levyosio. Palveluilla tarkoitetaan yleensä ohjelmistoja jotka tarjoavat käyttäjille toiminnallisuutta verkon yli. Näitä ovat mm. sähköposti, pikaviestintä tai VPN mahdollisuudet (Llewellyn & Craft 2001,12).

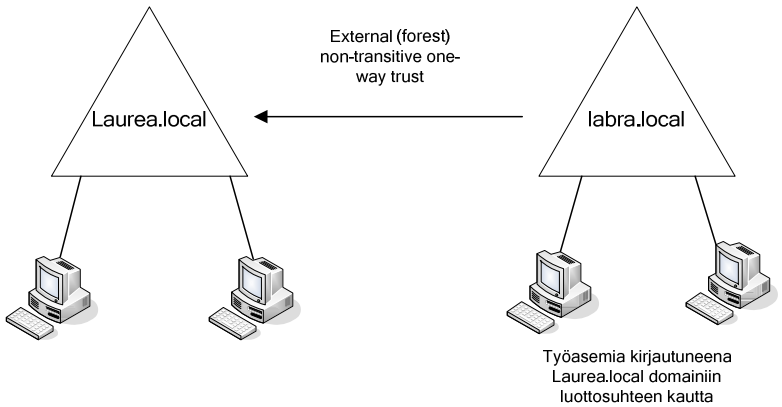
Laboratorioverkon aktiivihakemistopalvelin tulee toimimaan täysin omana yksikkönään, mistä johtuu että hallinnointitasoksi tulee metsä, joka on korkein taso. Aktiivihakemistopalvelimen toimialue on labra.local, Vorojeikinin (2009) määrityksen mukaisesti.

6.2.1 Luottosuhde (Trust)

Käyttäjätunnuksia ei voida luoda erikseen laboratorioverkon aktiivihakemistopalvelimelle, koska halutaan opiskelijoille mahdollisuus käyttää heidän omia tunnuksiaan kirjautumiseen.

Tämän saavuttamiseksi luodaan luottosuhde (trust) laboratoriopalvelimen ja Laurean oman aktiivihakemistopalvelimen välille.

Luottosuhdetyyppejä on eri käyttötarkoituksiin monenlaisia: yksisuuntaisia, kaksisuuntaisia, periytyviä, toimialuetason, metsätason, oikotietyyppisiä ja niin edelleen. Laboratorioverkon aktiivihakemistopalvelin hakee käyttäjätiedot Laurean aktiivihakemistopalvelimelta joka sijaitsee eri toimialueessa. Laurean aktiivihakemistopalvelin ei tarvitse mitään tietoja tai resursseja laboratorion aktiivihakemistopalvelimelta. Tästä johtuen luottosuhteen tyyppi on ”External nontransitive one-way trust” (Kuva 5). Laboratoriopalvelin on luottava (lähde) aktiivihakemisto ja Laurean aktiivihakemisto on luotettava (kohde). (Trust types 2005.)



Kuva 5: Luottosuhde

Vorojeikin oli yrittänyt luoda luottosuhdetta aikaisemmin opinnäytetyössään. Toimimattomuus johtui Vorojeikinin mukaan osoitteenkäännöksestä ja Otaverkon palomuureista, jotka ovat aktiivihakemistopalvelimen ja laboratorioverkon välissä. Tähän Vorojeikin oli ehdottanut yhtä vaihtoehtoista ratkaisua: luodaan VPN tunneli näiden kahden aktiivihakemistopalvelimen välille. Ratkaisu olisi toimiva (Forest or External Trusts Through NATed Firewall 2008).

Käytännön toteutuksellisista ja teknisistä syistä pohdittiin myös muita vaihtoehtoja aktiivihakemiston luottosuhteen toteuttamisen mahdollistamiseen. Yksi vaihtoehto oli asentaa aktiivihakemisto suoraan NAT-laitteen ulkopuolelle staattiselle IP-osoitteelle. Tässä tietoturva laboratorioiden osalta jäisi kuitenkin hyvin vajavaiseksi ja työasemilta toimialueelle kirjautuminen ei toimisi osoitteenkäännöksen yli. Networks lab ei voisi käytännössä hallita mitenkään yhteyksiä ulkomaailmasta laboratorion aktiivihakemistopalvelimelle, muuten kuin paikallisen ohjelmistopalomuurin avulla. Toinen vaihtoehto olisi rakentaa Vorojeikinin ehdotuksen mukaisesti Laurean aktiivihakemistopalvelimen ja laboratoriopalvelimen välille virtuaalinen lähiverkkoyhteys eli muodostaa tunneli. Metodi on kuitenkin haastava koska se vaatii verkkoon muutoksia myös Otaverkon päässä ja heidän osaltaan asennuksia. Virtuaalisen

lähiverkkoyhteyden rakentaminen jätettiin toissijaiseksi suunnitelmaksi ja päätettiin rakentaa verkko mahdollisimman yksinkertaisesti ja helposti hallinnoitavaksi.

Kolmas vaihtoehto oli toteuttaa aktiivihakemistopalvelin demilitarisoidulle alueelle. Tällä menetelmällä ei tulisi osoitteenkäännösongelmaa palvelimelle samassa muodossa missä Vorojeikin oli sen kokenut, koska osoitteenkäännös luodaan staattisesti yhdestä ulkoisesta IP-osoitteesta yhteen sisäiseen osoitteeseen. Metodia kutsutaan 1-on-1 mappaukseksi. Demilitarisoidulla alueella ASA-laitteella voidaan hallinnoida kaikkia portteja ja yhteyksiä mitä sallitaan aktiivihakemistopalvelimelle. Tämä nostaa tietoturvan tarpeelliselle tasolle. DMZ-alueella toteutettaisiin osoitteenkäännös julkisesta IP:stä xxx.xxx.xxx.150 DMZ:n 172.16.30.150 IP-osoitteeseen. Valittiin demilitarisoidulle alueelle toteuttaminen ensisijaiseksi vaihtoehdoksi aktiivihakemistopalvelimen ja luottosuhteen toimintaan saattamiseksi.

Luottosuhteen mahdollisesta toteutuksesta osoitteenkäännöksen yli löytyi hyvin paljon ristiriitaista tietoa. Forumeilla kerrottiin kokemuksista joissa osa oli saanut Microsoftin tuen avulla luottosuhde toimimaan moitteettomasti osoitteenkäännöksen kanssa (Trust With NAT 2007). Muissa paikoissa kuvattiin luottosuhteen muodostamista mahdottomaksi (Forest or External Trusts Through NATed Firewall 2008). Tiedon ristiriitaisuuksista johtuen päätettiin luoda testiympäristö osoitteenkäännöksen ja kahden aktiivihakemistopalvelimen luottosuhteen toimivuuden kokeilemiseksi. Luottosuhteen testiympäristö on dokumentissa luvussa 7.3.

6.2.2 Windows-toimialue

”Windows Server Domain”, eli toimialue on Windows käyttöjärjestelmiin pohjautuva verkkoalue, jota voidaan hallinnoida keskitetysti toimialueen ohjauskoneella (Domain Controller, DC). Toimialue on loogisesti muodostettu ympäristö, jossa voi olla DC palvelin, työasemia, muita palvelimia ja tulostimia. Toimialueen voi nimetä haluamallaan tavalla, mutta yleisenä käytäntönä ja Windowsin ohjelmistoista johtuen, päätoimialue on kaksiosainen merkkijono joiden osat erotetaan pisteellä, esimerkiksi corp1.local. Local on pseudo-ylätason verkkotunnus ja se itsessään määrittää toimialueen luonteen niin, että julkisesta verkosta ei pitäisi olla pääsyä toimialueeseen. Tämän toimialueen alle voidaan luoda alatoimialueita, kuten office1.corp1.local. Windows toimialuetta käytetään aktiivihakemistossa ja yksityisverkoissa ja sitä ei tule sekoittaa verkkotunnukseen, jotka toimivat Internetissä (Llewellyn & Craft 2001, 102).

Vorojeikin oli määritellyt opinnäytetyössään laboratorioverkon toimialueeksi labra.local. Koska aktiivihakemistoympäristö on Laurean sisäisessä käytössä, nimen ei tarvinnut viitata

mitenkään Laureaan tai sen toimintaan. Tästä johtuen päädyttiin pitämään Vorojeikinin suunnittelema toimialuenimi. Toimialueen nimipalveluun voidaan lisätä uusia DNS-tietueita. Esimerkiksi voidaan laittaa palvelinkone1.labra.local osoittamaan opiskelijaprojektin koneeseen, jolloin ei tarvita IP-osoitteiden käyttöä tai muistamista. Ulkoverkkoon laboratorioverkon toimialueella ei ole näkyvyyttä.

6.3 Cisco ASA 5510 Adaptive Security Appliance

”ASA 5500 -sarja tarjoaa kattavat VPN-ominaisuudet, jotka mahdollistavat muun muassa etäyhteydet IPSec- ja SSL VPN-salausprotokollia hyödyntäen. Tuotteet ovat suunniteltu tukemaan kattavasti yritysverkkojen tärkeitä teknologioita ja palveluita kuten QoS, Multicasting sekä IPv6-standardia. Uudet ASA-ratkaisut pohjautuvat markkinoiden johtaviin tietoturvatuotteisiin, PIX Security Appliance, IPS 4200 sekä VPN 3000 Concentrator-tuoteperheisiin. Cisco ASA 5500 -sarja tarjoaa VPN-yhteyksiin IPSec- ja SSL-salausprotokollien toiminnallisuutta. Ne integroituvat yllä mainittuihin ATD-teknologioihin ja turvaavat VPN-yhteyden madoilta, viruksilta ja tietomurroilta. IPSec- ja SSL-VPN-ominaisuudet yhdessä tekevät Cisco ASA 5500 -sarjasta helposti soveltuvan kaikkiin VPN-käyttöympäristöihin.” (Tradec OY - Tietoturva ja VPN 2010.)

Networks labilla on omistuksessa ASA 5510 tietoturvalaite. Laite toimii verkon reunareitittimenä, palomuurina, VPN yhteyden tarjoajana MentorAid luennoille sekä DHCP-palvelimena. ASA-laitteeseen tehdään kaikki aliverkkoihin ja verkon toimintaan liittyvät määritykset. Verkon toiminnan kannalta ASA-laite on verkon kriittisin osa. Kaikki aliverkot ja ulkoverkkoon pääsy ympäristössä toteutetaan ASA-laitteen läpi. Laitteeseen tehtävissä muutoksissa toimii lähteinä Ciscon toimittamat tuoteohjeet ja –oppaat: Cisco ASA 5500 Series Getting Started Guide Version 7.2, Cisco ASDM 5.2 User Guide ja Cisco Security Appliance Command Line Configuration Guide Version 7.2.

Luotiin määritykset ASA-laitteeseen, että hallinta voidaan tehdä ainoastaan Networks ja management verkosta, eikä muilla aliverkoilla ole pääsyä hallintasivulle tai konsoliin telnet yhteydellä. Hallintaosoitteena normaalitilanteessa käytetään 192.168.16.1, joka on sama kuin Networks verkon oletusreitin osoite. Mikäli verkossa käy jotain niin että hallintaosoitteeseen ei pääse, jätetään ASA-laitteen hallintaporttiin IP-osoitteeksi määritys 10.8.4.40/22. Määrittämällä kannettavalle tietokoneelle staattisesti IP-osoitteen edellä mainitusta verkosta ja kytkemällä management portin kaapeli koneeseen, saadaan varmasti hallintayhteys reitittimeen. Hallinta tapahtuu joko Cisco ASDM työkalulla tai web-käyttöliittymällä. Web käyttöliittymään yhdistetään hallinnan IP-osoitteella, mutta yhteys salataan SSL:llä. Tämä tarkoittaa että osoiteriville IP-osoitteen eteen kirjoitetaan https, esimerkiksi https://10.8.4.40 tai https://192.168.16.1.

ASA-laitteen ohjelmisto oli kirjoitushetkellä versiossa 7.2. Ciscon tukisivuilta selvitettiin että laitteeseen olisi saatavilla versiopäivitys versioon 8.2.2, sekä ASDM hallintatyökalu voitaisiin päivittää versiosta 5.2 versioon 6.2.5. ASA-laitteen päivitys toisi muun muassa tuen Cisco AnyConnect VPN Client ohjelmistolle. Aikaisemmin käytetty Cisco VPN Client ei tue laisinkaan 64-bittisiä Windows–käyttöjärjestelmiä, mutta AnyConnect ohjelmisto toisi tuen (Release Notes for the Cisco ASA 5500 Series, 2010). IT-palveluissa työskentelevä ja Laurean lähiverkoista vastaava Mika Salo oli hankkinut päivitykset sekä ohjelmistot Ciscon tuotetuesta. Päivitystiedostot löytyvät Networks labin verkkolevyltä hakemistosta ”ASA ja VPN päivitys”. Ajallisten resurssien puutteen vuoksi, päivitystä ei tehdä tämän opinnäytetyön puitteissa. Päivityksestä tehdään dokumentaation lopussa kehitysehdotus tuleville projekteille (Release Notes for the Cisco ASA 5500 Series, 2010).

6.4 Aliverkot

Salmenkylän mukaan laboratorioverkolle annetaan käyttöön 13 staattista IP-osoitetta. Verkko-osoite on xxx.xxx.xxx.144/28. IP-osoitteesta 28 ensimmäistä bittiä on verkko-osaa, tarkoittaen että aliverkon peite on 255.255.255.240. Yleislähetysosoite on xxx.xxx.xxx.159. Laiteavaruus on siten xxx.xxx.xxx.145 – xxx.xxx.xxx.158. Laiteavaruudesta xxx.xxx.xxx.145 on käytössä Otaverkon palomuurilla/reitittimellä (ASA-laitteen oletusreitti), sekä xxx.xxx.xxx.146 ASA-laitteen ulko-osoitteella, mistä luodaan osoitteenkäännös laboratorioiden ja luokkatilojen IP-avaruuksiin. Käytännössä Networks labin hallinnoimaan verkkoalueeseen saadaan käyttöön 12 julkista IP-osoitetta.

Aliverkon peitteeksi valittiin uusille sisäverkoille 255.255.252.0. Tämä tarkoittaa että verkko vaihtuu kun IP-osoitteen kolmannessa oktetissa lisätään neljä desimaalilukua lisää. Laiteosan kokonaisosuus yhdessä verkossa on siis 10 bittiä, tarkoittaen että yhteen laiteavaruuteen mahtuu 1022 IP-osoitetta (IP Addressing and Subnetting for New Users 1996).

Liite 1 kuvaa verkkojen määritykset. Laiteavaruus määrittelee IP-avaruuden kyseiselle verkolle, jossa sijaitsevat laitteet voivat keskustella keskenään ilman liikenteen kulkemista reitittimen kautta. Broadcast on verkon yleislähetysosoite. Aliverkon peite määrittelee kuinka monta IP-osoitetta aliverkkoon kuuluu. Oletusyhdyskäytävä on reitittimen IP-osoite, johon aliverkon IP-avaruuteen kuulumattomat paketit lähetetään ja reititin ohjaa paketit eteenpäin haluttuun suuntaan. Subinterface on looginen verkkoliitäntä joka luodaan yhteen fyysiseen porttiin ASA–laitteessa. Näin yhdellä fyysisellä liitännällä voidaan luoda monta loogista yhteyttä niiden vaikuttamatta toisiinsa. Subinterfacet vaativat aina virtuaaliverkon määrittelyn (Cisco Security Appliance Command Line Configuration Guide 2008, 5-3).

Aliverkkojen jakaminen laajempiin laiteavaruuksiin selitetään sillä, että saadaan tällöin aliverkon peitettä muuttamalla ja IP-osoitteen uudelleenmäärityksellä tiloissa saadaan koneet käytännössä irti verkosta. Näin luokkatiloissa voidaan luoda oma testiympäristö tulevaisuudessa projekteille ilman kaapelikytkentöjä. Selkeyden vuoksi verkko-osaa pienennetään, eikä suurenneta.

Esimerkkitilanne luokassa 009:
Työaseman IP-osoitteeksi on määritelty 192.168.25.23 ja aliverkon peitteeksi 255.255.252.0. Kokeiluympäristön kone halutaan irti ulkoverkosta. Käyttäjä määrittelee aliverkon peitteeksi 255.255.255.0 ja IP-osoite pysyy samana. Tällöin samasta verkosta ei enää löydy reititintä ja koneet eivät pääse ulkoverkkoon.

Aikaisemmassa ympäristössä NEON lab oli verkossa 192.168.11.0/22. Muita määrityksiä verkolle ei ollut tai ne pysyivät samoina. Verkon määritykset löytyvät dokumentin muista osioista.

6.5 Dynamic Host Configuration Protocol

DHCP (Dynamic Host Configuration Protocol) on verkossa sijaitseva palvelu joka automatisoi verkon IP-osoitteistusta ja jakaa verkkoon liittyville laitteille IP-osoitteet määrityksen mukaisesti. Laitteen liittyessä verkkoon se lähettää yleislähetysosoitteeseen kyselyn löytyykö kyseisestä verkosta DHCP-palvelinta. DHCP-palvelin vastaa kyselyyn ja palauttaa käytettävän IP-osoitteen, aliverkon peitteen, DNS-palvelinten osoitteet, oletusreitin ja muita verkon rakenteeseen liittyviä arvoja (Free On-Line Dictionary Of Computing, 1998.)

Uudistetussa verkossa ASA 5510 toimii DHCP-palvelimena kaikille laboratorioverkon koneille. IP-avaruuksilla ei ollut muuten määrityksiä tai vaatimuksia, mutta Salmenkylän mukaan verkkojen piti olla 192.168.0.0 IP avaruudessa, sekä jokainen tila olisi omassa aliverkossaan.

DHCP-määrityksiin ASA-laitteessa luodaan liite 1:n mukaiset verkot. ASA-laitteen DHCP-palvelu ei kuitenkaan tue suurempaa kuin 254 laitteen IP-avaruutta verkkoliitäntää kohden. Käytetään siis aliverkossa olevat ensimmäiset 254 osoitetta, joka riittää jokaiselle tilalle. Staattisia IP-määrityksiä voidaan tehdä DHCP-palvelun antaman IP-avaruuden ulkopuoleltakin aliverkon mukaisesti.

Palautusviestissä DHCP-palvelin palauttaa laitteille DNS-palvelinten osoitteet. Laboratoriopalvelimen ollessa laboratorioverkkojen DNS-palvelin, määritetään tämän IP-osoite palautettavaksi, joka on 172.16.30.150. On kuitenkin otettava huomioon että

laboratoriopalvelin voi hajota tai tulla muuten toimimattomaksi. Tästä johtuen DHCP-palvelin määritetään myös palauttamaan toissijainen DNS-palvelin, joka on Laurean verkon palvelin IP-osoitteessa 10.2.8.20.

6.6 Osoitteenkäännös

NAT (Network Address Translation), eli osoitteenkäännös, on Internet-tekniikka, mikä mahdollistaa yhden tai useamman julkisen IP-osoitteen muuntamisen moneksi yksityisosoitteeksi. Tekniikasta on hyötyä, kun halutaan yhdistää useita laitteita Internetiin, mutta julkisia IP-osoitteita ei ole tarjolla tarvittavaa määrää tai niitä ei haluta käyttää. Osoitteenkäännös ei pelkästään anna rajattoman määrän koneita kytkeytyä Internetiin yhdelle julkiselle IP-osoitteelle, mutta myös lisää tietoturvaa, koska millään ulkoverkon koneella ei ole suoraa pääsyä sisäverkon koneeseen. (Bradley 2006, 226-228.)

Laboratoriotiloille ja luokkahuoneille toteutetaan osoitteenmuunnos yhdestä julkisesta IP-osoitteesta (xxx.xxx.xxx.146) liitteessä 1 kuvattuihin yksityisverkkoihin. ASA-laitteessa osoitteenkäännös toteutetaan luomalla dynaaminen NAT-sääntö. Jokaiselle verkolle luodaan oma sääntö, josta löytyy tiedot IP avaruudesta, mistä osoitteenkäännös tehdään, sekä julkinen IP-osoite tai osoitteet joka on ulkoverkkoon päin. (Cisco ASA 5500 Series Getting Started Guide, Version 7.2 2006.)

Oli myös tarve toteuttaa liikenteen salliminen laboratoriopalvelimen ja laboratorioaliverkkojen välillä. Toiminnallisuuden toteuttamiseen tarvitaan NAT exempt osoitteenkäännössäännöt, jotka ovat poikkeussääntöjä osoitteenkäännökselle (Cisco ASDM 5.2 User Guide 2008, 26-13). Poikkeussäännön ollessa toiminnassa, määriteltyjen verkkojen tai osoiteavaruuksien välillä ei tehdä osoitteenkäännöstä. Osoitteenkäännöksen sijaan ASA-laite reitittää määriteltyjen verkkojen välillä.

Laboratoriopalvelimelle tehdään osoitteenkäännös ulko-osoitteesta xxx.xxx.xxx.150 sisäosoitteeseen 172.16.30.150. Näin ollen kun esimerkiksi laurea.local aktiivihakemistopalvelin tekee DNS-kyselyn laboratoriopalvelimelta, se palauttaa sisäverkon IP-osoitteen. Tästä johtuen osoitteenkäännöksessä kytketään päälle asetus DNS rewrite, joka uudelleenkirjoittaa osoitteenkäännöstaulun mukaisesti DNS-palvelun vastauksen ulkoverkon IP-osoitteella, jota tarvitaan luottosuhteen muodostamisessa. (Cisco ASDM 5.2 User Guide 2008., 22-3.)

6.7 Kaapelointi ja kytkimet

Kytkimet ovat laitteita jotka yhdistävät verkossa olevia laitteita toisiinsa. Kytkimeen voidaan määritellä virtuaalisia lähiverkkoja, joiden avulla yhden kytkimen läpi voidaan viedä erillisiä verkkoja niiden vaikuttamatta toisiinsa.

IT-palvelut ottavat heidän omistuksessaan olevat vanhat kytkimet käyttöön muissa tarpeissa, joten joudutaan hankkimaan uusia kytkimiä tarpeen mukaan että kaikki tilat ja niiden laitteet saadaan kytkettyä verkkoon. Käytössä oli HP 2626 kytkimiä: Networks labissa, tilassa 040 (laboratorioverkon palvelinhuone) ja kerrosjakamo 01:ssä. Kerrosjakamo 03:ssa oli käytössä Ciscon kytkimiä (liitteet 4 ja 6), jotka eivät myöskään tule käyttöön uuteen verkkoon. Nämä pitää korvata uusilla. Yhteensopivuus kytkimissä VLANien ja muun yhteistoiminnallisuuden kannalta on oleellista, joten uusien hankittavien kytkimien olisi suotavaa olla samalta valmistajalta ja samaa mallia.

Networks labin ylläpitoon kuuluu myös BarLaurealle kuuluvat AROMI palvelimet. Palvelimet sijaitsevat tilassa 040, joka toimii laboratorioverkon palvelinhuoneena. Kytkentöjä tehdessä pitää varmistaa että AROMI palvelimet pysyvät 10.26.0.0 verkossa. Todettiin myös tarve AROMI ylläpitolinjalle Networks labiin, mihin päästään yhdestä portista laboratorion kytkimestä. AROMI laitteet kytketään tilan 040 2626 kytkimen läpi, omassa virtuaalisessa lähiverkossaan ja tuodaan suunnitellun verkkokaavion mukaisesti VLANien avulla Networks labiin.

Verkkoyhteyksien tarve tiloille jakautuu seuraavasti:
RED lab: 3 pöytäkonetta, 9 kannettavaa, 1 palvelin ja tulostin. Yhteensä 12 laitetta. Tulevaisuuden laajennusvaraksi ehdotetaan 15 verkkoyhteyden tuomista tilaan.
NEON lab: 12 pöytäkonetta ja tulostin
Luokkatila 010: 30 pöytäkonetta ja tulostin
Luokkatila 009: 30 pöytäkonetta ja tulostin
Networks lab: 12 pöytäkonetta, 4 kannettavaa, tulostin, verkkolevy. Fyysiseen verkon rakenteeseen ei tarvita muutosta.

Kustannussäästö voidaan saada käyttämällä 48-porttista kytkintä kahden 24–porttisen sijaan. Myös verkon topologia ja hallinta selkeytyy huomattavasti kun kaksi laitetta voidaan korvata yhdellä. Tästä johtuen esitetään hankittavaksi HP ProCurve 2500–sarjan kytkimiä. Ehdotetaan hankittavaksi seuraavat kytkimet:

2x HP ProCurve Switch 2510-48 - Hallittava 48-porttinen 10/100-kytkin. Liitännät: 48x auto-sensing 10/100. Hinta: á 574,90€, verkkokauppa.com.

Yksi kytkin sijoitetaan kerrosjakamo 03:n tuomaan verkko tiloille 009 ja 010, sekä yksi kytkin kerrosjakamo 01:n tuomaan verkko RED- ja NEON labeihin. Siirretään Networks labin omistuksessa oleva vanha Procurve 2626 kytkin kerrosjakamo 01:stä kerrosjakamo 03:n jatkamaan verkkoa tiloille 009 ja 010. Pelkästään yksi 48-paikkainen HP 2510 kytkin ei riitä kaikille laboratorioverkon tilojen laitteille kerrosjakamo 03:sta, toisin kuin kerrosjakamo 01:ssä. Laboratorioverkossa oli kirjoitushetkellä käytössä 3 kpl HP Procurve 2626 kytkimiä. Hankittavat kytkimet ovat HP:n verkkosivujen mukaan yhteensopivia 2600–sarjan kanssa. Hankittavaksi ehdotetut kytkimet sopivat myös Laurean kehikkoihin (HP ProCurve Switch 2510 Series 2010).

Kerrosjakamot ja niiden hallinta on pääsääntöisesti IT-palveluiden ylläpidossa. Ainoastaan laboratorioverkkoon kuuluvat ja suunnitellut kytkimet ovat Networks labin ylläpidossa.

Verkon kytkimet suunniteltiin liite 2:ssa olevan taulukon mukaisesti.

6.8 Aliverkkojen välinen liikenne

Aliverkkojen välistä liikennettä ei tarvita ja siten ollen ei sallita. Laboratorioiden ja luokkatilojen laitteiden on kuitenkin päästävä DMZ-alueella sijaitsevalle laboratoriopalvelimelle nimipalvelukyselyiden ja aktiivihakemistokirjautumisen tarpeesta. Tätä varten luotiin ASA-laitteelle palomuurisäännöt joka mahdollistaa DMZ-alueelle pääsyn.

Mikäli tilojen väliselle liikenteelle on tarvetta tulevaisuudessa, voidaan tätä hallinnoida ASA-laitteesta luomalla NAT exempt -sääntöjä joko verkko- tai IP-osoitteiden perusteella, sekä varmistamalla että pääsylistat päästävät liikenteen verkkojen välillä.

Kuva 6: NAT exempt -sääntö

Pääsylistoilla ASA-laitteessa ei ole estetty verkkoliikennettä aliverkkojen välillä. Liikenne aliverkkojen välillä ei kuitenkaan onnistu, koska ASA-laite yrittää luoda osoitteenkäännöstä verkkojen välille.

6.9 Nimipalvelu

DNS (Domain Name System), eli nimipalvelu mahdollistaa kirjaimin kirjoitetun osoitteen muuttamisen koneen ymmärtämään IP-osoitteen muotoon ja toisinpäin. DNS-palvelimella on lista osoitteista ja niitä vastaavista nimistä, joita asiakaskoneet voivat kysellä. DNS-protokollan perustana ovat hierarkkiset toimialueet. Ylimmältä tasolta Internetissä löytyvät

maatunnukset kuten fi tai com. Toiselta tasolta löytyvät esimerkiksi yritykset, tuotenimet tai oppilaitokset. Tästä alemmat tasot ovat valinnaisia ja käytetään organisaation eri tasojen jakamiseen (Kaario 2002). Tasojen erottamisessa käytetään piste–merkkiä. Mikäli verkko-osoitteita halutaan selvittää toimialuenimen perusteella, sitä kutsutaan forward lookup zoneksi. Kun halutaan tehdä muutos toiseen suuntaan, eli selvittää IP-osoitteen perusteella verkkonimi, käytetään reverse lookup zonea. (Ammann 1999, luku 7.)

Projektissa Windows Server 2003:lle asennettiin nimipalvelu. Tällöin työasemat kysyvät nimipalvelimelta mistä IP-osoitteesta löytyy toimialueen aktiivihakemistopalvelin: labra.local. Työasemat on asetettu kirjautumaan tähän osoitteeseen. Muita DNS-tietueita laboratoriopalvelin ei tarvitse, koska kaikki muut nimipalvelukyselyt uudelleenohjataan Laurean nimipalvelimille 10.2.8.20 ja 10.3.8.20. Näillä palvelimilla on tieto laurea.local aktiivihakemistopalvelimesta. Tieto on tarpeellinen koska luottosuhde muodostetaan toimialuenimen perusteella, eikä IP-osoitteen perusteella (Llewellyn & Craft 2001, 318). DNS-palvelu kerää tietokantaan toimialueeseen liitettyjen laitteiden nimet ja kirjaa myös laitteiden isäntänimiin liittyvät IP-osoitteet. Näin koneita voidaan löytää ja hakea verkosta isäntänimen perusteella. Esimerkkitilanteessa voidaan harjoituspalvelimelle antaa nimi ”palvelin1.labra.local”. Täten muita verkon laitteita käyttävien käyttäjien ei tarvitse käyttää tai tietää IP-osoitetta, vaan isäntänimen käyttäminen riittää.

Projektissa nimipalvelu on aktiivihakemiston toiminnan kannalta välttämätön osa (Microsoft Server TechCenter: Windows Server 2003 2010). Uuden nimipalvelun luominen ei olisi muuten laboratorioverkon toiminnan ja käytön kannalta välttämätön.

6.10 Demilitarisoitu alue

DMZ, eli demilitarisoitu alue on alue organisaation verkossa minne sijoitetaan yleisesti julkiverkkoon tarkoitettuja palveluita. Alue verkosta on yleensä osittain eriytetty sisäverkosta, mutta pääsy ulkoverkkoon on sallittu. Esimerkiksi HTTP- ja sähköpostipalvelimet sijoitetaan usein demilitarisoidulle alueelle (SolutionBase: Deploying domain controllers in a DMZ 2004; Kaario 2002).

ASA-laitteessa demilitarisoitu alue on määritelty ja toteutettu ethernet portista 0/4 verkko-osoitteella 172.16.30.1/16. Tässä projektissa demilitarisoidulle alueelle toteutettiin laboratoriopalvelin, mihin asennettiin aktiivihakemisto- ja nimipalvelu. Demilitarisoidulle alueelle laitettava aktiivihakemisto ei välttämättä ole kannattava valinta yleisen tietoturvan kannalta (Deploying domain controllers in a DMZ 2004). Siitä huolimatta, koska Otaverkko Oy tarjoaa kaksi palomuuria vielä verkon ulkoreunalla, ratkaisu on hyvin perusteltu. Otaverkon palomuurit eivät oletuksena päästä sisääntulevaa liikennettä läpi, ellei sitä erikseen pyydetä.

Tulevaisuudessa demilitarisoidulle alueelle tullaan lisäämään opiskelijaprojekteissa toteutettavia palvelimia, joten tähän mahdollinen liitettävyys ja toiminnallisuus on toteutettava. DMZ-alueelle toteutettavat palvelimet sijaitsevat fyysisesti tilassa 040 sekä NEON labissa, joten ASA-laitteen ja laboratorion välille on toteuttava erillinen yhteys käyttämällä virtuaalista lähiverkkoa. Tällä mahdollistettaisiin palvelinten asetusten muuttaminen, ilman että henkilön tarvitsee fyysisesti olla palvelinhuoneessa 040.

Otaverkon antamasta osoiteavaruudesta määriteltiin viisi IP-osoitetta käytettäväksi DMZ-alueella verkossa (Salmenkylä). Osoiteavaruus on xxx.xxx.xxx.153 – 158, johon voidaan myöhemmin kytkeä ”lennosta” palvelimia DMZ-alueen IP-osoitteella, jotka saavat suoraan ulkoisen IP-osoitteen ja siten voidaan tarjota laboratorioiden toimesta opiskelijaprojekteina laajaverkkopalveluita opiskelijoille tai muille käyttäjille.

IP-osoitteistus DMZ-alueelta ulkoverkkoon tapahtuu muuttamalla IP-osoitteen kolme ensimmäistä oktettia DMZ-alueen vastaavaksi. Esimerkkitilanteessa ulkoiseksi IP-osoitteeksi halutaan xxx.xxx.xxx.155, joten DMZ-alueella sijaitsevalle palvelimelle IP-osoitteeksi määritetään 172.16.30.155. Muut asetukset voidaan määritellä joko liitteiden mukaisesti tai hakemalla asetukset DHCP-palvelusta.

6.11 Henkilökuntaverkko

RED labiin, NEON labiin, Networks labiin sekä luokkatiloihin 009 ja 010 tarvitaan yhteys henkilökuntaverkkoon. Networks labissa puolet tilasta on kytketty henkilökuntaverkkoon kerrosjakamo 04:n kautta. Nämä yhteydet eivät siten vaikuta uudistetun laboratorioverkon suunnitteluun tai toteutukseen. NEON labissa työskentelee Laurean henkilökuntaa, joten noin puolet tilasta pitää kytkeä henkilökuntaverkkoon kerrosjakamo 01:n kautta. Verkon tuominen tilaan voidaan toteuttaa joko IT-palvelun toimesta heidän kytkimiä käyttäen tai Networks labin kytkimiä käyttäen. RED labissa henkilökuntaverkkoon pääsy vaaditaan kahdelta työpisteeltä, mikä sisältää neljä verkkopistoketta. Nämä yhteydet voidaan myös toteuttaa IT-palvelun toimesta heidän kytkimillään tai vaihtoehtoisesti Networks labin kytkimillä.

Luokkatilat 009 ja 010 tarvitsevat yhteyden henkilökuntaverkkoon luennoitsijan koneelta. Seinärasioihin kytkennät tulevat kerrosjakamosta 03 (liite 4). Verkko voidaan tuoda näihin tiloihin samoin mahdollisuuksin kuin edellisessä kappaleessa kuvatuin menetelmin.

6.12 ASA-laitteen palomuurisäännöt

Pääsylistat, eli access-listit, ovat ASA-laitteessa käytettäviä sääntölistoja, joilla voidaan hallita verkkoliikenteen kulkua liitännöissä. Access listejä kutsutaan ASDM hallintatyökalussa nimellä access rule. Säännöt voidaan luoda joko sallimaan tai estämään liikennettä. Ne voidaan määritellä vaikuttamaan kyseisen liitännän ulos- tai sisäänpäin menevään liikenteeseen. Tietoturvan näkökulmasta palomuurin oletusasetuksissa aloitetaan tilanteessa missä ulkoverkosta tuleva liikenne estetään sisäverkkoon (deny). Tästä ylläpitäjä voi jatkaa sallimissääntöjen (permit) tekemistä niille yhteyksille joita tarvitaan. Sisäänpäin tehtävissä yhteyksissä tarvitaan myös osoitteenkäännössääntöihin porttien ohjauksia (Cisco Security Appliance Command Line Configuration Guide 2008).

Opinnäytetyötä aloittaessa ASA-laitteessa oli paljon turhia access-list sääntöjä, jotka eivät vaikuttaneet mitenkään verkkoliikenteeseen muiden sääntöjen ylittäessä ne. Nämä säännöt poistettiin ja lähdettiin luomaan uusia sääntöjä oletusasetuksista.

6.13 Varmuuskopiointi ja varmistus

Verkossa on monia kytkimiä ja laboratoriopalvelin, jotka ovat kriittisiä osia verkon toiminnan kannalta. Mikäli jokin kytkimistä, ASA-laite tai laboratoriopalvelin hajoaa, verkon toiminta voi lakata osittain tai kokonaan. Verkkoon kuuluessa noin 130 laitetta, toiminta poikkeustilanteissa pitää suunnitella kokonaisvaltaisesti. Tilat, mihin verkko tulee toimintaan, eivät ole kuitenkaan ehdottoman kriittisiä toimipisteen yleisen toiminnan kannalta. Laboratoriopalvelimen rinnalle olisi suotavaa luoda toissijainen replikoiva palvelin, jolla on samat funktiot kuin ensisijaisella palvelimella. Näin vikatilanteessa laitteet voivat siirtyä käyttämään varapalvelimia.

ASA-laitteelle voidaan määrittää DHCP-vastaus palauttamaan kaksi DNS-palvelimen osoitetta. Näin ollen voidaan luoda toinen toissijainen laboratoriopalvelin, milloin ensisijaisen palvelimen ollessa saavuttamattomissa tai irti verkosta, työasemat siirtyvät automaattisesti käyttämään toissijaista palvelinta (Kaario 2002). Toissijainen palvelin vaatii kaikki samat tiedot ja määritykset DNS-palveluun kuin ensisijainen palvelin. Aktiivihakemistorakenne voidaan toteuttaa replikoinnilla. Tekniikka on sisäänrakennettu toiminto aktiivihakemistossa, joka kirjaimellisesti kahdentaa palvelimen.

7 Toteutus

Joulukuun alussa 2009 oli kyselty palomuurisäännöistä ja DNS-palvelimista Jarmo Tapiolta, joka vastaa Laurean ulkoisista tietoliikenneyhteyksistä. Saatiin vastaus että voidaan käyttää

Otaverkon DNS-palvelimia, jotka eivät ole 10.0.0.0 verkossa. NEON labissa, jossa edellinen 192.168.11.0/22 verkko oli käytössä, määritettiin yhdellä koneella käytettäväksi saatuja DNS-palvelinten osoitteita xxx.xxx.xxx.14 ja xxx.xxx.xxx.68. Nimipalvelukyselyt toimivat ASA-laitteen läpi näille palvelimille. Palvelin palautti DNS-kyselyissä IP-osoitteet ja Internet yhteys toimi. Tästä johtopäätöksenä uudistettavan laboratorioverkon DNS-palvelu ei vaadi muita asetuksia kuin DNS-kyselyiden uudelleenohjauksen.

Asennettiin testiympäristönä Networks Labissa DNS-palvelu Windows server 2003:n. Asennus onnistui ja saatiin DNS-kyselyiden uudelleenohjaamisen toimintaan. Samana päivänä todettiin että NEON labin verkko käyttää 10.2.8.20 ja 10.3.8.20 nimipalvelimia. Nämä ovat IP-osoitteiden mukaisesti Laurean verkossa. Tästä ilmenikin tutkimusongelma, koska ASA-laitteen kautta kulkevalla liikenteellä ei pitäisi olla pääsyä Laurean sisäverkkoon. ASA-laite teki reitityksen määrityksen mukaisesti, eli oletusreittinä käytetään xxx.xxx.xxx.145 osoitetta.

Traceroute NEON lab koneelta:
oletusreitti: 192.168.11.1 (ASA)
1 hyppy: xxx.xxx.xxx.145
2 hyppy: xxx.xxx.xxx.177
3 hyppy (kohde): 10.2.8.20

Johtopäätöksenä reititys 10.0.0.0 verkkoon tehtiin Otaniemen reitittimissä ja ASA-laitteen kautta toimiva verkko toimii niin kuin pitääkin, eikä laboratorioverkosta ollut pääsyä suoraan Laurean verkkoon.

Haettiin laboratoriopalvelin Networks labiin ja alettiin työstää asetuksia. Muutettiin DNS-palvelu kuntoon niin, että kyselyt ohjataan otaverkon määrittämiin DNS-palvelimiin xxx.xxx.xxx.14 ja xxx.xxx.xxx.68. Tämän jälkeen IP asetukset muutettiin määrityksiä vastaavaksi (kts. liite 3):

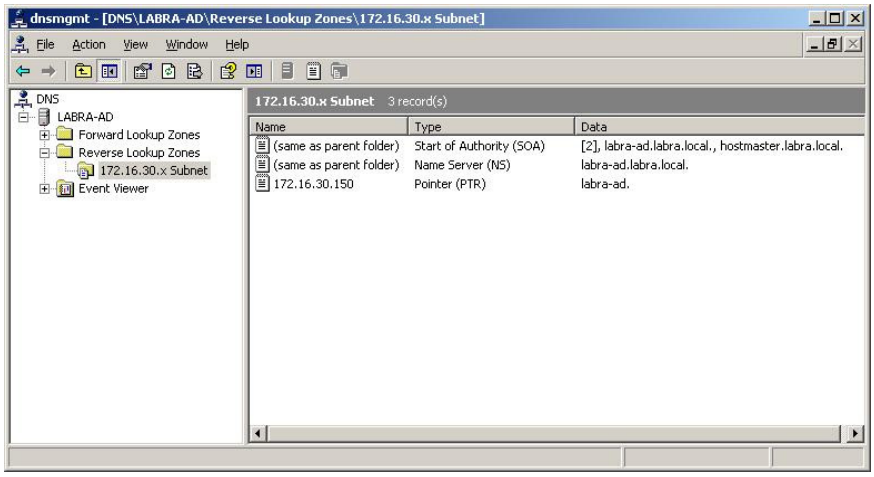
Laboratoriopalvelin vietiin NEON labiin ja kytkettiin DMZ-verkkoon kytkimen läpi. ASA-laite vaati asetusten määrittelyn niin, että liikenne sallitaan DMZ- ja ASA_inside-verkon välillä. Operaation lähteinä toimivat ASA–manuaali, Ciscon forumit ja kolmansien osapuolien forumit. Ongelmallisuutta tuli vastaan, koska ASA-laite tekee oletuksena osoitteenkäännöksen, mitä tässä tapauksessa ei haluttu tekevän. Liikenteen ohjaaminen onnistui luomalla NAT Exempt -sääntö, joka sulkee pois NAT-osoitteenkäännöksen kyseisten verkkojen välillä. ASA-laitteesta laitettiin päälle asetus ”Enable traffic through the firewall without address translation”.

Yksi työasema otettiin käyttöön NEON labissa asetusten ja yhteyksien toimivuuden testaukseen. Työasemalle määritettiin DNS-palvelimen osoitteeksi 172.16.30.150, eli laboratoriopalvelimen IP-osoite. DNS-kyselyt toimivat ja Internet yhteydet toimivat täysin.

Luotiin labra.local aktiivihakemistopalveluun tunnukset testausta varten. Määritettiin tunnukselle oikeudet ryhmään Domain Users aktiivihakemistossa. Tämän jälkeen Networks labin kannettava tietokone liitettiin 192.168.11.0 verkkoon. ASA-laitteen DHCP-palvelin antoi tälle IP-osoitteen, mutta DNS-palvelimen osoitteeksi muutettiin käsin 172.16.30.150. Kannettava kone oli valmis liitettäväksi labra.local-toimialueeseen. Liittäminen onnistui muuttamalla Windows XP asetuksista toimialueen osoitteeksi ”labra.local” ja kirjautumalla edellä mainituilla käyttäjätunnuksilla. Johtopäätöksenä aktiivihakemiston asetukset olivat määritelty oikein ja toimialueeseen kirjautuminen toimi ilman ongelmia ASA-laitteen reitittäessä kaksi aliverkkoa. Lisäksi Windowsin automaattista päivitystenhakua käyttäen asennettiin laboratoriopalvelimen Windows Server 2003 -käyttöjärjestelmään uusimmat tietoturvapäivitykset.

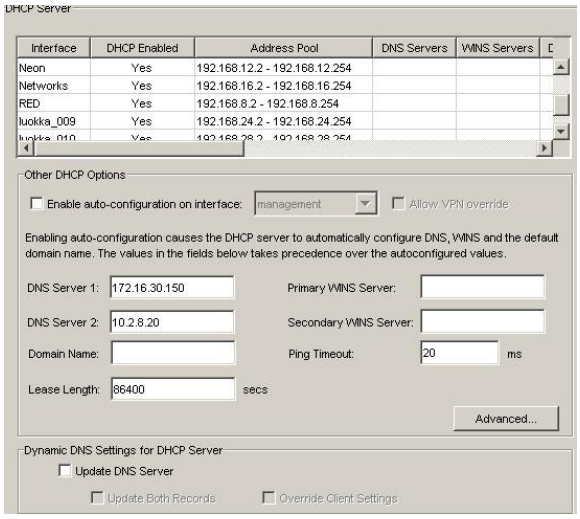
Kun Laurean aktiivihakemistopalvelimeen yritettiin saada yhteyttä käyttäen xxx.xxx.xxx.14 DNS-palvelinta, selvisi, että tämä palvelin ei sisältänyt tietuetta laurea.local IP-osoitteesta. Laurea.local verkkonimessä sijaitsee Laurean aktiivihakemistopalvelin mihin luottosuhde on muodostettava. Ongelma kuitenkin korjaantui muuttamalla DNS-kyselyjen uudelleenohjaus. Luvun alussa mainitut xxx.xxx.xxx.14 ja xxx.xxx.xxx.68 DNS-osoitteet muutettiin 10.2.8.20 ja 10.3.8.20 osoitteiksi. Nämä osoitteet ovat Laurean sisäverkon nimipalvelimia. Tällöin laurea.local verkkonimi löytyy ja luottosuhde voitiin teoriassa muodostaa.

Nslookup komentoa käyttäessä huomattiin että laboratoriopalvelimella ei ole määritelty DMZ-alueen IP-osoitteelle reverse lookup zonea, eli palvelimen IP-osoitteelle ei ole määritetty tietuetta mikä on kyseisen laitteen verkkonimi. Tästä johtuen luotiin uusi reverse lookup zone DNS-palveluun aliverkolle 172.16.30.x (Kuva 7) ja sinne lisättiin tietue jossa IP 172.16.30.150 osoittaa labra-ad verkkonimeen.



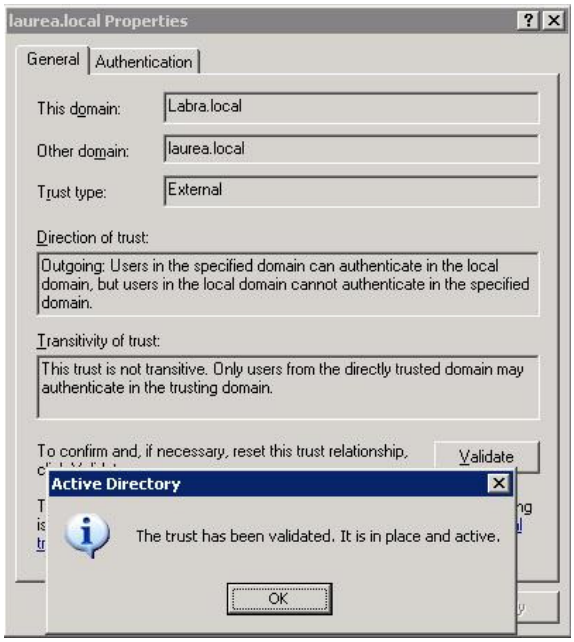
Kuva 7: DNS reverse lookup zone ja tietueet

Aloitettiin asetusten luominen ASA-laitteeseen ja tilojen siirtäminen uudistettuun verkkoon. Luotiin ASA-laitteeseen subinterfacet, NAT-säännöt ja DHCP-palvelu luvussa 6.3, sekä liitteessä 1 määritellyillä asetuksilla (Kuva 9). 040_core ja 008_Networks kytkimiin luotiin VLANit, sekä asetettiin VLANien tagaukset ja trunkkiportit. Lopuksi Networks labista otettiin irti kaikki vanhat yhteydet jotka veivät Laurean verkkoon. Koneet kytkettiin uuteen verkkoon Networks labissa onnistuneesti, niin että DHCP-palvelu antoi IP-osoitteet laitteille. 008_Networks kytkimestä määritettiin portit 22 ja 23 10.8.0.0 verkon VLANille auki verkon laitteiden IP-osoitteiden muuttamista varten. Osoiteavaruuden muuttamisen jälkeen huomattiin että osalla laboratorion laitteista oli määritelty staattiset IP-osoitteet Laurean 10.8.0.0 verkosta. Nämä osoitteet muutettiin 192.168.16.0/22 verkkoa vastaavaksi sekä dokumentoitiin muutokset laboratorion laitelistaan. Laitteita olivat: 008_Networks kytkin, tulostin, labra-palvelin ja verkkolevy.



Kuva 8: ASA-laitteen DHCP-asetukset

Kysyttiin IT-hallinnolta miten toimitaan käytännössä luottosuhteen muodostamisessa. IT-hallinto halusi päästä itse hallinnoimaan laboratoriopalvelinta ja luomaan luottosuhteen koska he joutuvat syöttämään laurea.local palvelimen pääkäyttäjän salasanan luottosuhdetta muodostettaessa. Luovutettiin IT-hallinnolle aktiivihakemistopalvelimen käyttäjätiedot niin, että IT-hallinto sai Remote Desktopilla yhteyden palvelimeen. He ottivat yhteyden aktiivihakemistopalvelimeen ja saivat luotua luottosuhteen labra.local ja Laurea.local-toimialueiden välille (Kuva 10). Luottosuhteen luomisessa ei esiintynyt ongelmia. Luomisen jälkeen kirjautuminen onnistui Laurea.local-toimialueeseen työasemilta, jotka oli liitetty labra.local-toimialueeseen. Muutosten jälkeen luotiin ASA-laitteeseen palomuurisääntö, joka estää kaiken liikenteen muualta Remote Desktop-portteihin paitsi Networks-verkosta. Laboratoriopalvelimelle asennettiin myös F-Secure AV Windows Server-versio.



Kuva 9: Luottosuhde toiminnassa

Liitteen 5 mukaisesti alettiin työstää 040_core kytkimen asetuksia. Siirrettiin kaapelit kuvattuihin portteihin ja muutettiin näille porteille VLANien määritykset. AROMI-VLAN eriytettiin portteihin 1-4. Portti 9 tuo NEON, RED ja DMZ-verkot kerrosjakamo 01:n, mistä kytkin jakaa verkot määriteltyihin tiloihin ja seinärasioihin. Portit 13-18 muutettiin DMZ-VLANiin, joista portti 13 kytkettiin ASA-laitteen ETH1 DMZ-porttiin. Portit 21-24 pysyivät muuttamattomina MentorAid ja VPN yhteyksille. Portti 25 (trunk 1) vie ASA-laitteelle RED, NEON, Networks, luokkatila 009 ja luokkatila 010 verkot tagattuina, joiden liikenteen jakamisen hoitaa ASA laitteen subinterfacet joille on määritetty vastaavat VLANit. Portti 26 vie varayhteyksien kautta kerrosjakamo 03:n tuoden kytkimille DMZ, Networks, luokkatila 009, 010 ja AROMI verkot. Näin ollen Laurean verkko oli täysin eriytetty laboratorioverkosta. Luotiin myös AROMI ylläpitolinja Networks labiin. VLAN-asetukset muutettiin laboratorion 008_networks kytkimeen niin, että portista 24 pääsee AROMI-verkkoon joka on VLANissa 26.

Procurve 2600 –sarjan kytkimissä on oletuksena määritys että maksimimäärä VLANeja on 8. VLANeja tarvittiin ympäristössä enemmän, joten rajoitusta jouduttiin muuttamaan suuremmaksi. Otettiin telnet yhteys 040_core kytkimeen ja suoritettiin komento **max-vlans 15** config-tilassa. Tällä saatiin nostettua VLANien maksimimäärä viiteentoista.

Tehtiin viimeiset tarvittavat asetukset 040_core kytkimeen joita tarvitaan uudistetun verkon käyttöönottoon. Eriytettiin DMZ-VLANit 10.8.0.0 päällekkäisyyksistä ja tuotiin NEON labiin yhteydet 32-01-C4 seinärasiaan mikä tuo DMZ-verkon tilaan aikaisemman NEON ja DMZ-VLANien sekoituksen tilalle. Seinärasiassa on kiinni 8 verkkoliitäntää hallinnoiva kytkin. Kytkimeen voidaan liittää NEON labissa projektipalvelimia tai muita laitteita joille tarvitaan pääsy DMZ-verkkoon.

Koska laboratoriopalvelinta voitiin etähallita täydellisesti, siirrettiin palvelintilaan 040 ja kytkettiin se 040_core kytkimessä DMZ-verkkoon, porttiin 13.

Luotiin loput osoitteenkäännössäännöistä ASA-laitteeseen IP-osoitteille xxx.xxx.xxx.155 – xxx.xxx.xxx.158. Näin DMZ-alueelle voidaan liittää suoraan koneita määrittämällä staattinen IP-osoite 172.16.30.155 - 172.16.30.158 väliltä. Näin laitteet saavat suoraan vastaavan ulkoverkon IP-osoitteen ilman muita tarvittavia asetuksia.

7.1 Laitteiden liittäminen labra.local-toimialueeseen

Ympäristön ollessa liitettynä uudistettuun verkkoon, mahdollistettiin kaikkien verkossa olevien laitteiden liittäminen labra.local-toimialueeseen ja luottosuhteen kautta laurea.local-toimialueeseen.

Liitettiin Networks labista kaksi pöytäkonetta labra.local-toimialueeseen. Toimialueeseen liittäminen toteutetaan Windows käyttöjärjestelmässä ohjauspaneelin kohdasta ”järjestelmä” ja välilehdeltä ”tietokoneen nimi”. Painamalla ”muuta” – painiketta laite voidaan liittää toimialueeseen tai muuttaa toimialuetta.

Todettiin kuitenkin, että Networks labissa sekä NEON labissa kaikissa muissa pöytäkoneissa on asennettu Windows Vista Home Edition. Kyseisessä käyttöjärjestelmässä ei ole tukea toimialueeseen liittämiseen. Tämän opinnäytetyön puitteissa käyttöjärjestelmiä ei uusita, vaan tarpeen vaatiessa käyttöjärjestelmät voidaan uusia muiden projektien puitteissa. Toimialueeseen liittäminen vaatii käyttöjärjestelmien päivityksen Windows Vista Business, Ultimate tai Enterprise versioon tai Windows 7 Professional Enterprise tai Ultimate versioon (Windows Vista: Which Edition Should You Get? 2006; Windows 7: Which Edition Should You Choose? 2009).

7.2 Laboratoriopalvelimen hajoaminen ja kunnostus

Verkon toiminta lakkasi helmikuussa. Todettiin, että laboratoriopalvelin oli sammunut. Palvelin ei enää käynnistynyt useiden kokeilujen jälkeen. Avattiin kotelo ja tarkistettiin johdot. Irrotettiin palvelimesta oheislaitteiden kaapelit (kiintolevyt ja levyasemat), mutta palvelin ei käynnistynyt tästä huolimatta. Johtopäätöksenä todettiin, että palvelimesta hajosi muistit, prosessori, virtalähde tai emolevy. Hajoamisen seurauksena tutkittiin voidaanko toteuttaa laboratoriopalvelimen rinnalle varapalvelin ja millä resursseilla.

Saatiin Networks labin työntekijän virtalähde laboratoriotilaan. Vanha virtalähde irrotettiin laboratoriopalvelimen emolevystä ja uusi virtalähde liitettiin kiinni vanhan tilalle. Palvelin lähti käyntiin uudella virtalähteellä. Voitiin siis todeta, että palvelimesta oli hajonnut ATX-virtalähde. Networks lab ei omistanut testivirtalähdettä, joten tilattiin uusi OCZ ModXStream Pro 600W ATX-virtalähde palvelimeen verkkokauppa.com –liikkeestä. Verkkokaupasta tilattu uusi virtalähde saapui Networks labiin. Kiinnitettiin virtalähde laboratoriopalvelimeen sekä tehtiin virtakaapelikytkennät. Palvelin saatiin käyntiin ja takaisin toimintaan.

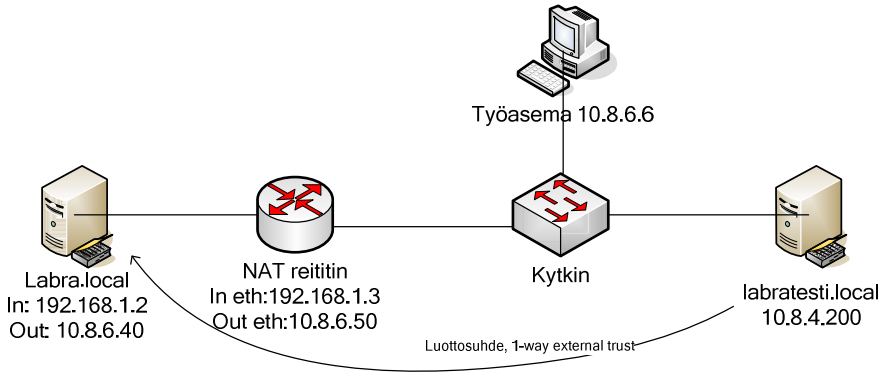
Virtalähteen ja koneen rikkoutumisesta aiheutui se että toimialueeseen kirjautuminen ei toiminut, sekä nimipalvelukyselyt eivät toimineet. Peruskäyttäjälle se näkyi Internet-yhteyksien täydellisenä toimimattomuutena. Luotiin siten ASA-laitteen DHCP-palveluun toissijainen DNS-palvelin osoittamaan IP-osoitteeseen 10.2.8.20. Näin varmistettiin että laitteissa Internet-yhteydet toimivat, vaikka laboratoriopalvelin olisi poissa toiminnasta.

7.3 Testiympäristö luottosuhteelle

Kuten luvussa 5.2.1 kuvattiin, luottosuhteen toimivuus piti varmentaa osoitteenkäännöksen yli. Luotiin Networks labissa 10.8.4.0/22 verkkoon uusi yksityisverkko 192.168.1.0/24. Otettiin käyttöön yksi laboratorion reititin ja luotiin siihen NAT-sääntö tekemään osoitteenkäännös kahden verkon välillä. Tarkennuksena varmistettiin että reititin ei tee normaalia reititystä verkojen välillä. Laitettiin 10.8.4.0 verkkoon työasema IP-osoitteella 10.8.6.6 ja samaan verkkoon pystytettiin ensimmäinen testipalvelin ajamaan aktiivihakemistoa ja nimipalvelua IP-osoitteella 10.8.4.200 ja määritettiin toimialueeksi labratesti.local. Nämä koneet yhdistettiin kytkimen avulla reitittimeen. Reitittimen toiselle puolelle 192.168.1.0 verkkoon luotiin toinen aktiivihakemisto- ja nimipalvelin IP-osoitteella 192.168.1.2 ja toimialueeksi määritettiin labra.local. Sisäisen IP-osoitteen (192.168.1.2) ulko-osoitteeksi määritettiin reitittimelle 10.8.6.40. Reitittimen kaksi käytössä ollutta porttia saivat sisäosoitteen 192.168.1.3 ja ulko-osoitteen 10.8.6.50.

DNS ja aktiivihakemisto asennettiin verkon topologian mukaisesti ja kokeiltiin yksisuuntaisen luottosuhteen muodostamista 10.8.4.200 palvelimelta (luottava), palvelimelle 10.8.6.40

(192.168.1.2). Luottosuhde muodostui onnistuneesti käyttäen DNS-nimiä. Tämän jälkeen liitettiin työasema 10.8.6.6 labratesti.local toimialueeseen. Liittäminen onnistui ja työasemaa käynnistäessä kirjautumisvaihtoehtoina oli labratesti ja labra toimialueet. Labra-toimialueelle kirjautuessa voitiin käyttää labra.local aktiivihakemistoon luotuja testitunnuksia.



Kuva 10: Luottosuhteen testiympäristö Networks labissa

7.4 CCNA-harjoitusten päivitys

Verkkojen eriytys tapahtui verkosta 10.8.4.0/22 verkkoon 192.168.16.0/22. Yksi Networks labin funktioita on tarjota opiskelijoille laboratoriotila reititin- ja kytkinharjoituksia varten. Harjoitukset ovat Niemi Teron toteuttamana tällaisenaan 10.8.4.0/22 verkossa. Koko muu ympäristö muutettiin 192.168.16.0/22 verkkoon, joten harjoitukset eivät suoraan toimineet uudessa ympäristössä. Tehtävänä oli muuttaa kaikki harjoituksiin liittyvät uuteen IP avaruuteen. Muutettavia osa-alueita olivat reitittimet, kytkimet, terminal server, VoIP puhelimet, WLAN tukiasemat, core laitteiden asetukset ja harjoitustekstit.

Yksi vaihtoehto toteuttaa harjoitukset uudistetussa laboratorioverkossa oli tehdä 192.168.16.0 verkon sisälle oma uusi 10.8.4.0 privaattiverkko, millä ei olisi pääsyä verkosta ulos. Näin harjoitukset olisi pystytty suorittamaan edellistä turvallisemmin eriytetyssä verkossa. Käytännössä koneiden piti myös saada yhteys harjoitusreitittimiin ja -kytkimiin. Tämä olisi toteutettu käyttämällä Networks labin pöydillä olevia vaihtoverkkorasioita. Jokaisen koneen olisi voinut muuttaa haluamaansa verkkoon tilanteen mukaan.

Käytännön teknisistä ja toteutuksellisista syistä, edellisessä kappaleessa kuvattu suunnitelma olisi tuonut turhaa vaivaa niin harjoitusten pitäjille, kuin opiskelijoillekin. Päädyttiin siis muuttamaan harjoitukset kokonaisuudessaan uuteen verkkoon. Käytännössä operaatio oli kuviteltua helpompi: tehtiin Microsoft Wordilla search & replace ”10.8.4” -> ”192.168.17” harjoitusteksteihin sekä tallennettuihin asetustiedostoihin. Tämän jälkeen selattiin vielä harjoitukset ja tiedostot läpi ja varmistettiin että kaikki kohdat olivat muuttuneet oikein. Korvaustoimenpiteellä saatiin muutettua kaikki harjoitukset uuteen IP avaruuteen.

7.5 Aikataulu

Opinnäytetyön suunnitteluun ja toteutukseen käytetty aika, sekä viikoille ajoittuneet tehtävät ovat talukossa 2

Taulukko 2. Toimenpiteet viikottain

Viikko	Tehtävät
Viikko 49	▪ Tutkimuksen ja dokumentoinnin aloitus ▪ DNS-palvelimista tietoa IT-hallinnolta
Viikko 50	▪ DNS-palvelun testaus Networks labissa
Viikko 51	▪ Laboratoriopalvelin DMZ-verkkoon ▪ DNS-asetukset ▪ NAT exempt -säännöt ▪ Aktiivihakemistoon testitunnusten luonti ja kirjautuminen ▪ Palvelimen päivitys ▪ DNS-uudelleenohjausosoitteiden muutos ▪ Reverse lookup zonen luominen
Viikko 2	▪ Aloitettiin muutos uudistettuun verkkoon ▪ DHCP-palvelun, subinterfacejen ja NAT-sääntöjen luominen ▪ Kytkinten asetusten muuttaminen ▪ Staattisten IP-osoitteiden muutokset ▪ Luottosuhteen testiympäristö
Viikko 3	▪ CCNA-harjoitusten päivitys ▪ Luottosuhteen luominen aktiivihakemistopalvelimien välille
Viikko 4	▪ 040_core-kytkimen kaapelointi ja VLANit
Viikko 5	▪ DMZ-alueen eriytys yhteen seinärasiaan NEON labissa ja kaapelointi
Viikko 7	▪ Laboratoriopalvelimen hajoaminen ja vian selvittäminen ▪ Uuden virtalähteen tilaus
Viikko 8	▪ Laboratoriopalvelimen korjaus ja takaisin toimintaan laittaminen ▪ Osoitteenkäännössäännöt DMZ-alueelle ▪ Toissijaisen DNS-palvelimen asetus DHCP-palveluun

8 Pohdinta

Kokonaisuutena projekti oli mielekäs suunnitella sekä toteuttaa. Pääsin hyödyntämään tietoa opituilta opintojaksoilta ja harrastuneisuudesta, mutta suuri osa tarvitusta tiedosta piti

opiskella opinnäytetyöhön liittyvistä kirjallisista ja sähköisistä dokumenteista. Verkon suunnittelutyö ei onnistunut minkään oppaan mukaisesti suoraan. Tietoa yhdisteltiin erilaisista lähteistä ja konstruoitiin näistä sopiva ratkaisu muutoksia tekemällä Laurean olemassa olevaan verkkoon ja ympäristöön sopivaksi.

Microsoftin ja Ciscon tukisivustot ja -palvelut olivat erinomaisia erilaisia ratkaisuja pohtiessa ja selvittäessä. Käytännönläheisyys ja toteutuksen suorittaminen toi työlle henkilökohtaista ja yhteiskunnallista arvoa. Työ onnistui suunnitelmien mukaisesti, eikä suurempia ongelmia tutkimuksessa tai toteutuksessa esiintynyt. Virtaviivainen dokumentointi yhdessä tutkimuksen ja toteutuksen kanssa ei tuonut lopun kirjoituspaljoutta, vaan aluksi tehty tutkimustyö dokumentoitiin opinnäytetyöhön heti sekä toteutusvaiheessa kirjoitusprosessi jakautui tasaisesti koko ajalle.

9 Kehitysehdotukset

Luvussa 6.7 ja liitteessä 2 kuvatut 48-paikkaiset kytkimet laitettiin tilaukseen Riku Salmenkylän toimesta. Näitä kytkimiä ei kuitenkaan saatu ajallisten resurssien puitteissa tämän opinnäytetyön toteutukseen. Näin ollen RED labia sekä luokkatiloja 009 ja 010 ei liitetty uudistettuun verkkoon alkuperäisestä suunnitelmasta poiketen. Kun kytkimet saadaan koululle, voidaan tilat liittää verkkoon tämän opinnäytetyön dokumentaation mukaisesti. Salmenkylän mukaan Business- ja Security labit voidaan myös tulevaisuudessa liittää uudistettuun verkkoon. Tehtäviä muutoksessa on kytkinten asentaminen kehikkoihin, kaapeloinnin tekeminen, VLANien määrittelyt kytkimiin, työasemien verkkoasetuksien muuttaminen ja liittäminen labra.local-toimialueeseen sekä tulostimien asetusten muuttaminen uuteen verkkoon. Osa laitteista liitetään Laurean omaan lähiverkkoon tai henkilökuntaverkkoon, mikä vaatii erityisasetuksia tietyille kytkinporteille. Tilojen liittämisessä tehdään yhteistyötä IT-hallinnon kanssa, missä sovitaan eri käytännön asioista verkkojen tuomisesta tiloihin.

Tuotetietoja ja oppaita lukiessa selvisi, että ASA 5510-laittesta löytyy toiminnallisuus Kerberos- ja LDAP-autentikointiin. Nämä ovat samoja protokollia, mitä käytetään aktiivihakemiston kirjautumisessa. Ehdotetaan, että tulevaisuuden projektina voidaan toteuttaa MentorAid VPN- järjestelmään kirjautuminen opiskelijoiden omilla tunnuksilla siten että ASA-laite varmentaa tunnukset laboratoriopalvelimen aktiivihakemistopalvelusta (Cisco Security Appliance Command Line Configuration Guide 2008).

Tutkimusta tehdessä todettiin, että ASA–laitteeseen on saatavilla versiopäivityksiä. Nykyinen ASA–laitteen ohjelmisto on versiossa 7.2 ja ASDM-hallinnointityökalu versiossa 5.2. Päivitykset nostaisivat ASA–laitteen ohjelmiston versioon 8.2.2 sekä ASDM-hallinnointityökalun versioon

6.2.5. Päivitys parantaisi VPN-tukea, IP-liikenteen parempaa hallintaa, botnet-hyökkäysten parempaa suodatusta ja tärkeimpänä laboratorioympäristölle ja opiskelijoille ohjelmistojen päivitys toisi tuen Cisco AnyConnect VPN-ohjelmistolle. AnyConnect-ohjelmisto on ainoa mahdollisuus muodostaa VPN-yhteys 64-bittisestä käyttöjärjestelmästä MentorAid-luentoja varten. Ehdotan, että versiopäivitys tehdään ASA–laitteelle ja näin ollen luodaan opiskelijoille paremmat mahdollisuudet käyttää MentorAid-verkkoluentoja, sekä lisätään verkon yleistä tietoturvaa ja hallintamahdollisuuksia. Tarvittavat päivityspaketit, kuten myös AnyConnect VPN-ohjelmisto löytyvät Networks labin verkkolevyltä hakemistosta ”ASA ja VPN päivitys”. (Release Notes for the Cisco ASA 5500 Series, 8.2. 2010.)

HP Procurve-sarjan kytkimet tukevat keskitettyä hallinnointia (stacking). Määrittämällä kytkinten välille oletus-VLAN voidaan kaikkia verkossa olevia kytkimiä hallita yhden IP-osoitteen kautta. Verkon kytkinten hallinnointi helpottuisi sekä selkeytyisi huomattavasti. Myös uusia kytkimiä voidaan lisätä helposti verkkoon hallittavaksi ilman IP-osoitteiden määritystä tai erikoiskaapeleita. Keskitetty hallinta voidaan toteuttaa tulevaisuudessa joko opiskelijaprojektina tai osana opinnäytetyötä. (HP ProCurve Stack Management 2000.)

Todettiin, että laboratorioverkosta on pääsy Laurean verkkoon ja näin ollen AROMI – palvelimille. Reititys tapahtuu Otaverkon puolella. Traceroute –komennolla selvitettiin, että liikenne AROMI palvelimiin kulkee IP-osoitteiden xxx.xxx.xxx.145 ja xxx.xxx.xxx.177 läpi. Liitteen 6 mukaisesti liikenne AROMI palvelinten ja laurean verkon välillä kulkee erillistä yhteyttä pitkin Laurean verkkoon, joka on viimeinen suora yhteys Laurean verkkoon tilasta 040. Tästä yhteydestä olisi tarve päästä eroon. Ehdotetaan, että AROMI palvelimet siirretään verkossa ASA-laitteen läpi kulkevaksi. Otaverkon suunnasta liikenne voidaan tuoda omaa VLANia pitkin ASA-laitteelle, joka reitittää verkon omaan osioonsa mistä löytyvät AROMI palvelimet. Otaverkon palomuurit vaatisivat määrityksen että AROMI palvelimet löytyvät ASA-laitteen suunnasta, nykyisen Laurean verkon sijaan. Toteutukseen olisi kaksi metodia. Voidaan luoda uusi subinterface ASA-laitteeseen ja sille VLAN-määritys, näin ollen verkkoliikenne kulkisi ASA-laitteen läpi joka reitittäisi liikenteen. Toinen vaihtoehto olisi laittaa kytkin 31-01 G09 liitännän ja ASA laitteen väliin (kts. liite 6), liittää kytkimeen AROMI palvelimet ja määrittää kytkimelle VLAN, missä olisi AROMI -järjestelmään liittyvä liikenne.

10 Yhteenveto

Opinnäytetyö aloitettiin Vorojeikinin ja Viitasen opinnäytetöiden jatkoprojektina. Tavoitteena oli luoda uudistettu ja täysin dokumentoitu verkkoympäristö opettajien ja opiskelijoiden käyttöön Laurea Leppävaaran laboratorioympäristöihin. Tavoitteena oli myös luoda mahdollisuus laajentaa verkkoa tarpeen vaatiessa.

Tutkimusta tehtiin verkon toimijoiden, laitteiden ja ohjelmistojen osalta. Verrattiin eri ratkaisuja olemassa olevaan verkkoon ja luotiin pohja, jonka avulla olemassa oleva verkko voitiin uudistaa parhaiden käytäntöjen mukaisesti. Työn alkuvaiheessa suunniteltiin teoriakokonaisuus uudesta verkkoympäristöstä. Suunnitelman hyväksyi Riku Salmenkylä. Näin ollen pystyttiin siirtymään toteutukseen.

Verkon eri osa-alueet toteutettiin onnistuneesti ja uudistettu verkkoalue saatiin käyttöön laboratorioympäristössä. Osa laboratoriotiloista jätettiin Laurean verkkoon, mutta ne voidaan liittää laboratorioverkkoon muiden projektien puitteissa. Verkkoalue dokumentoitiin ja siirrettiin ylläpito Networks labille Laurea Leppävaarassa.

Lähteet

Ammann, P. 1999. Managing Dynamic IP Networks. McGraw-Hill Osborne.

Bradley, T. 2006. Essential Computer Security. Syngress Publishing.

Cisco ASA 5500 Series Getting Started Guide, Version 7.2. 2006. Viitattu 10.12.2009
http://www.cisco.com/en/US/docs/security/asa/asa72/getting_started/asa5500/quick/guide/5500GSG.pdf

Cisco ASDM 5.2 User Guide. 2008. Viitattu 16.1.2010
http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/ASDMp.pdf

Cisco Security Appliance Command Line Configuration Guide, Version 7.2. 2008. Viitattu 3.2.2010
http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/asacfg72.pdf

Free On-Line Dictionary Of Computing. 2010. Viitattu 13.1.2010
http://foldoc.org/

Forest or External Trusts Through NATed Firewall. 2008. Viitattu 20.1.2010
http://www.eggheadcafe.com/software/aspnet/31760065/forest-or-external-trusts.aspx

Hevner et Al. 2004. Design Science In Information Systems Research. MIS Quarterly Vol. 28

HP ProCurve Stack Management. 2000. Viitattu 20.1.2010
http://www.hp.com/rnd/device_help/help/hpwnd/webhelp/HPJ4121A/configuration_stacking.htm

HP ProCurve Switch 2510 Series. 2010. Viitattu 16.1.2010
http://www.procurve.com/products/switches/ProCurve_Switch_2510_Series/overview.htm

IP Addressing and Subnetting for New Users.1996. Viitattu 3.1.2010
http://road.uww.edu/road/yinl/Cisco-content/ip-addressing.htm

Järvinen, P. & Järvinen, A. 2000. Tutkimustyön metodeista. Tampere: Opinpaja Oy.

Kaario, K. 2002. TCP/IP –verkot. Porvoo: WS Bookwell.

Laurea fakta, 2009. Vantaa: Opintoasiainhallinto.

Laurean palvelukuvaus. 2010. Viitattu 10.2.2010
http://www.laurea.fi/internet/fi/031_laatu/01/03_toiminta/01_lbd_prosessi/04_palvelutoiminnot/palvelukuvaus_2009_06_10_muutokset_vaeliaik2010_2.pdf

Llewellyn, T. & Craft, M. 2001. Windows 2000 Active Directory. Syngress Publishing.

Microsoft Server TechCenter: Windows Server 2003. 2010. Viitattu 15.12.2009
http://technet.microsoft.com/en-us/library/cc706993%28WS.10%29.aspx

Niiniluoto, I. 2002. Tieteen tunnuspiirteet. Helsinki: Gaudeamus.

Pirinen, R. 2009. Research Framework of Integrative Action. Laurea University of Applied Sciences.

Release Notes for the Cisco ASA 5500 Series, 8.2. 2010. Viitattu 24.2.2010
http://www.cisco.com/en/US/docs/security/asa/asa82/release/notes/asarn82.html

SolutionBase: Deploying domain controllers in a DMZ. 2004. Viitattu 15.12.2009
http://articles.techrepublic.com.com/5100-22_11-5238083.html

Tradec OY - Tietoturva ja VPN. 2010. Viitattu 10.12.2009
http://www.tradec.fi/tradec/esivu.php?id=64&kieli=fi

Trust types. 2005. Viitattu 4.12.2009
http://technet.microsoft.com/en-us/library/cc775736%28WS.10%29.aspx

Trust with NAT. 2007. Viitattu 14.1.2010
http://www.winvistatips.com/trust-nat-firewalls-t697951.html

Viitanen, T. 2008. NEON-laboratorion tietoverkon suunnittelu, rakentaminen ja dokumentointi. Espoo: Laurea Leppävaara

Vorojeikin, D. 2009. Neon-laboratorion DNS- ja AD-palvelimen asentaminen, konfigurointi, dokumentointi sekä luottosuhteen muodostaminen Otaverkko- palvelimen välille. Espoo: Laurea Leppävaara

Windows 7: Which Edition Should You Choose? 2009. Viitattu 10.3.2010
http://www.helpwithwindows.com/Windows7/Windows_7_Which_Version.html

Windows Vista: Which Edition Should You Get? 2006. Viitattu 10.3.2010
http://www.helpwithwindows.com/WindowsVista/vista-which-version.html

Kuvat ja kuviot

Taulukot

Liitteet

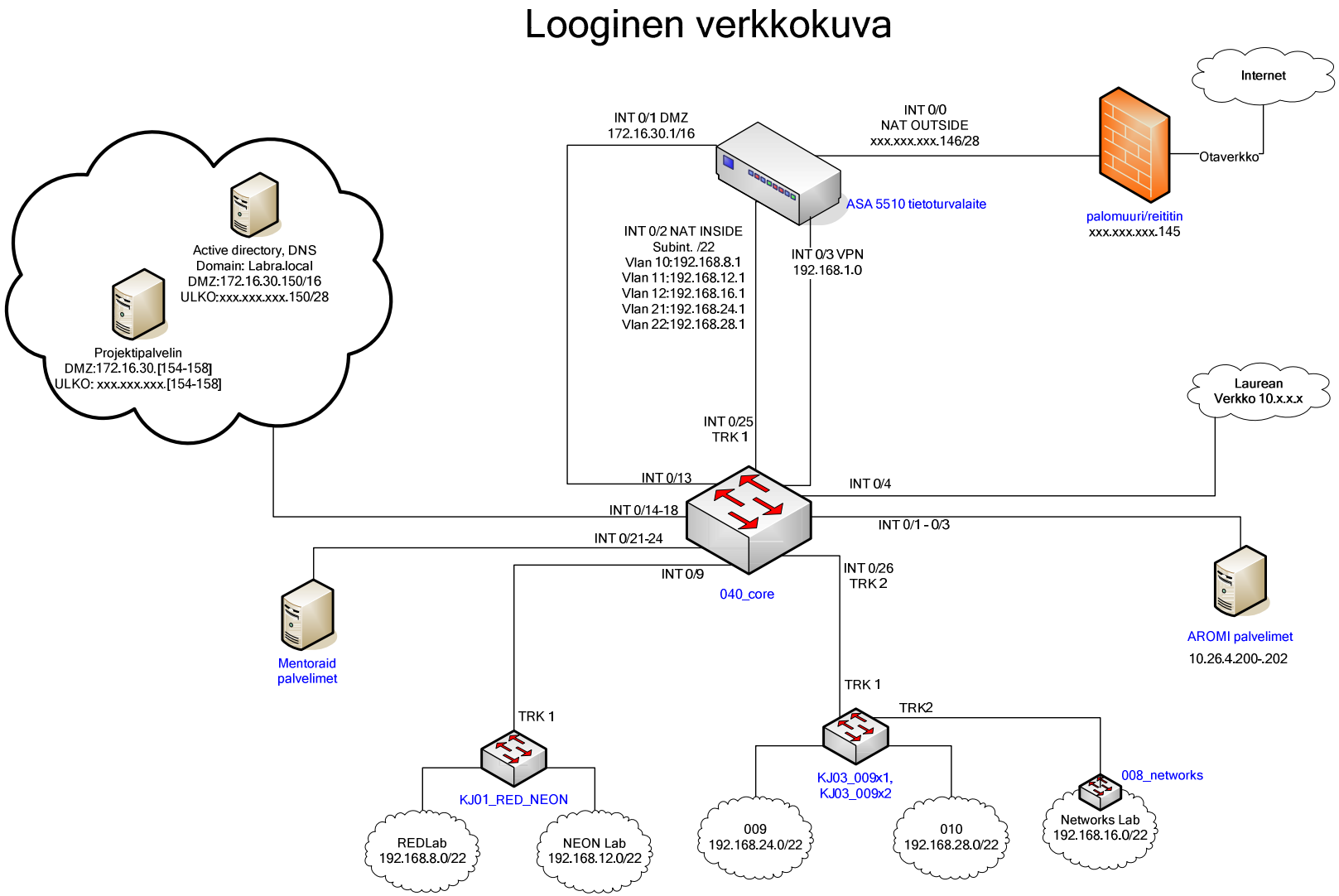
Liite 1 Verkkotaulukko

Verkko	Verkko-osoite	Laiteavaruus	Broadcast	Aliverkon peite	Oletusyhdyskäytävä	VLAN	ASA interface ID	ASA interface nimi
DMZ	172.16.0.0/16	172.16.1.0 - 172.16.255.254	172.16.255.255	255.255.0.0	172.16.30.1	5	4	DMZ
RED lab	192.168.8.0/22	192.168.8.1 - 192.168.11.254	192.168.11.255	255.255.252.0	192.168.8.1	10	2.5	RED
NEON lab	192.168.12.0/22	192.168.12.1 - 192.168.15.254	192.168.15.255	255.255.252.0	192.168.12.1	11	2.2	NEON
Networks lab	192.168.16.0/22	192.168.16.1 - 192.168.19.254	192.168.19.255	255.255.252.0	192.168.16.1	12	2.1	Networks
Luokkatila 009	192.168.24.0/22	192.168.24.1 - 192.168.27.254	192.168.27.255	255.255.252.0	192.168.24.1	21	2.3	luokka_009
Luokkatila 010	192.168.28.0/22	192.168.28.1 - 192.168.31.254	192.168.31.255	255.255.252.0	192.168.28.1	22	2.4	luokka_010
Ulkoverkko	xxx.xxx.xxx.144/28	xxx.xxx.xxx.145 – xxx.xxx.xxx.158	xxx.xxx.xxx.159	255.255.255.240	xxx.xxx.xxx.145		0	ASA_outside
Mentoraid	192.168.1.0/24	192.168.1.1 – 192.168.1.254	192.168.1.255	255.255.255.0	192.168.1.1		3	MentorAid

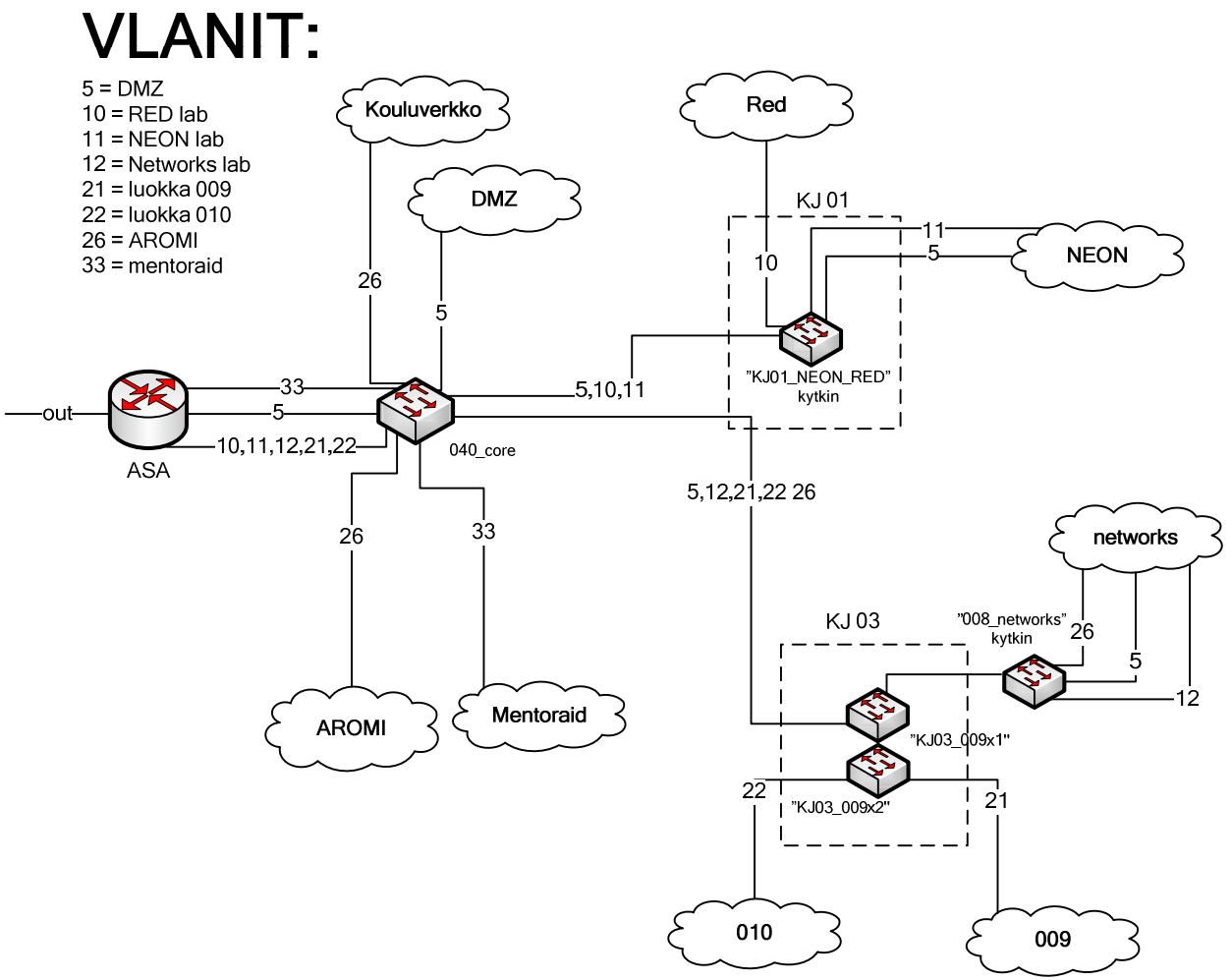
Liite 2 Kytkinsuunnitelma

Sijainti	Portteja	Nimi	Hallinnan IP	VLANIT	Tehtävä
Palvelinhuoneen 040 kytkin	24	040_core	192.168.16.230	5, 10, 11,12, 21, 22, 26, 33	Jakaa verkot eri suuntiin, toimii viimeisenä kytkimenä ennen ASA-laitetta.
Kerrosjakamo 01 kytkin 1	48	KJ01_RED_NEON	192.168.8.230	5, 10, 11	Jakaa REDlabs-, NEON- ja DMZ-verkon niille määritettyihin tiloihin.
Kerrosjakamo 03 kytkin 1	48	KJ03_009x1	192.168.24.230	21, 22	Kytkin luokkatilan 009 ja 010 laitteille
Kerrosjakamo 03 kytkin 2	24	KJ03_009x2	192.168.28.230	22	Kytkin luokkatilan 009 ja 010 laitteille
Networks lab kytkin, tila 008	24	008_Networks	192.168.16.240	5, 12, 26	Tuo networks labin verkon, sekä luo tilaan mahdollisuuden kytkeytyä AROMI- ja DMZ-verkkoon

Liite 3 Looginen verkkokuva

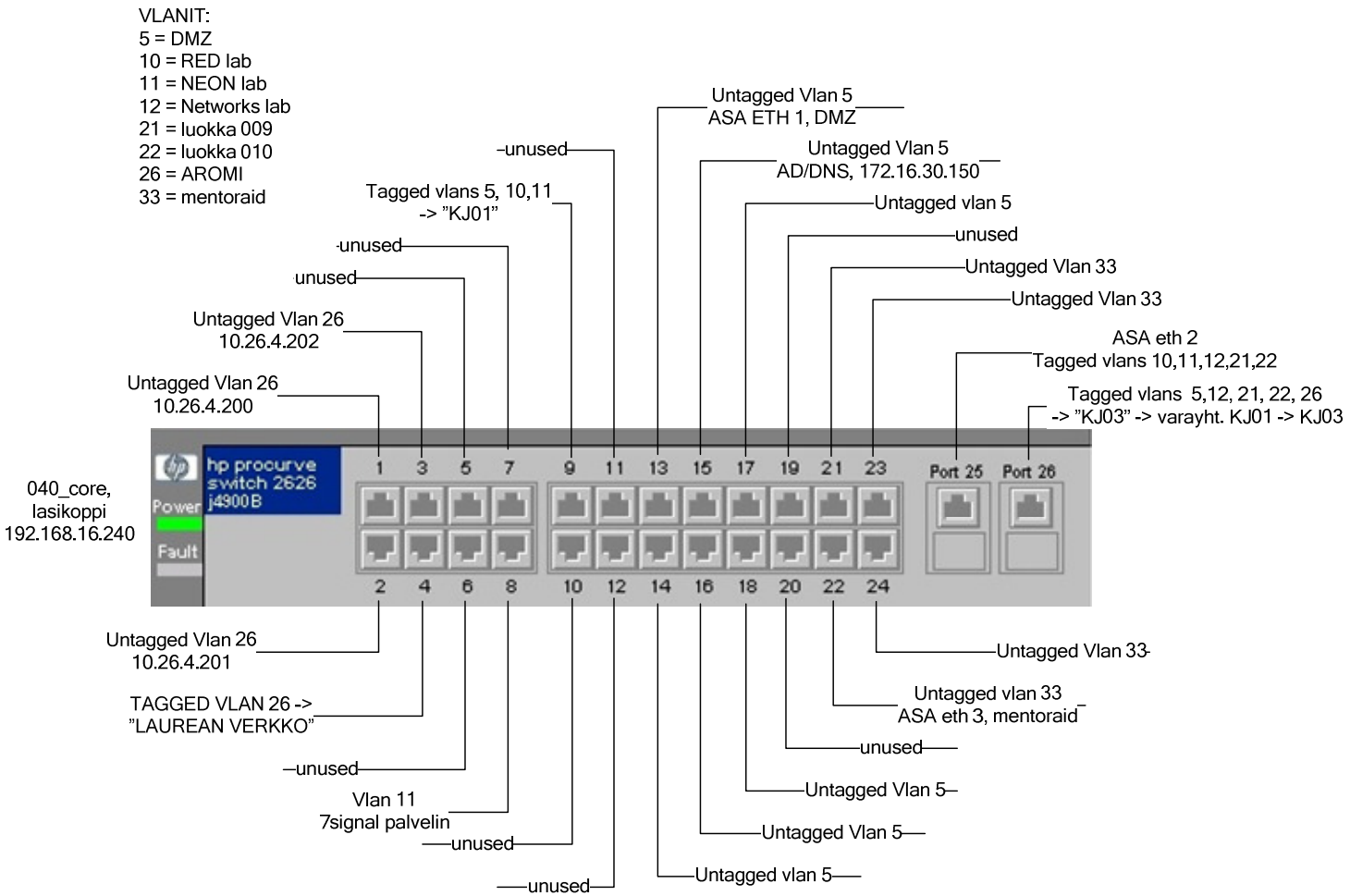


Liite 4 Verkon VLANien kaavio



Liite 5 Kytkinkuva: 040_core

Kytkinkuva: 040_core



Liite 6 Fyysinen verkkokuva

Fyysinen verkkokuva