



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Active Directoryn suunnittelu ja käyttöönotto kahden kaupungin opetusverkossa

Vepsäläinen, Jarkko

2012 Kerava

Laurea-ammattikorkeakoulu
Laurea Kerava

Active Directoryn suunnittelu ja käyttöönotto kahden kaupungin opetusverkossa

Jarkko Vepsäläinen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2012

Sisällys

1	Johdanto.....	7
2	Projektin teoreettinen viitekehys ja toteuttamisen kuvaus.....	8
	2.1 Active Directory	8
	2.2 Verkkoympäristö	8
	2.3 Testausvaiheen verkko	10
	2.4 Käyttäjätunnukset	10
3	Suunnitteluvaihe	11
	3.1 Projektin taustat	11
	3.1.1 Aktiivihakemisto	11
	3.1.2 Uuden ja vanhan toimialueen erot.....	11
	3.1.3 DNS-nimipalvelu.....	12
	3.2 Active Directory suunnittelua	13
	3.2.1 DNS-nimipalvelu ja WINS	13
	3.2.2 Organisaatioyksiköt.....	14
	3.2.3 Toimipaikat	15
	3.2.4 Nimiavaruus.....	15
	3.2.5 Toimialuerakenne ja luottosuhteet	15
	3.2.6 Ryhmät	16
	3.3 Aktiivihakemistorakenne ja konfiguraatio	17
	3.3.1 Metsä- ja toimialuerakenne	17
	3.3.2 Aktiivihakemiston käyttämien kansioden sijoittaminen	17
	3.3.3 Metsän toimipaikan rakenne	18
	3.4 Organisaatioyksikkörakenne	18
	3.4.1 Juuritoimialueen OU-rakenne.....	18
	3.4.2 Alitoimialueen OU-rakenne	19
	3.5 Nimeämiskäytännöt.....	20
	3.5.1 Nimeämissuunnittelu ja organisaatioyksiköiden nimeäminen	20
	3.5.2 Laiteobjektien nimeäminen ja kustannuspaikan tunnistaminen	21
	3.5.3 Ryhmäobjektien nimeäminen	21
	3.5.4 Käyttäjätunnukset	23
	3.5.5 Lukkiutumiskäytännöt.....	23
4	Käyttöönotto	23
	4.1 DNS-palvelut	23
	4.1.1 DHCP	24
	4.1.2 WSUS.....	25
	4.1.3 Luottosuhteet	25
	4.2 Työasemat.....	26

4.2.1 Suunnittelu ja uusiminen	26
4.2.2 Testaus	26
4.2.3 Siirto uuteen.....	27
5 Projektin tuloksia	27
6 Pohdintaa.....	29
Lähteet	30
Kuviot.....	31
Taulukot.....	32

Jarkko Vepsäläinen

Active Directoryn suunnittelu ja käyttöönotto kahden kaupungin opetusverkossa

Vuosi 2012 Sivumäärä 32

Projektin tavoitteena oli suunnitella ja käyttöönottaa Active Directory kahden kaupungin opetusverkossa. Tästä selviää, mistä opetusverkon Active Directoryn suunnittelu ja käyttöönotto aloitettiin, miten se toteutettiin ja mihin päädyttiin. Kyseessä oli projektihanke, joka kuitenkin itsessään sisältää laadullisen tutkimuksen piirteitä.

Projektidokumentaatiosta voidaan tarkastella mitä ja miten asiat tehtiin ja sen avulla virheet voidaan myöhemmissä projekteissa kartoittaa ja minimoida.

Dokumentaatiossa käydään läpi Active Directoryn suunnittelu vaiheittain sekä osa-alueittain. Suunnitteluvaiheen jälkeen siirrytään käyttöönottoon, joka kertoo lopulliset ja konkreettiset tulokset ja saavutukset.

Jarkko Vepsäläinen

Active Directory design and deployment on education network of two cities

Year	2012	Pages	32
------	------	-------	----

Goal of this project was to design and deployment Active Directory to the two-cities education network. This documentation shows how Active Directory's design and deployment was started, how it was implemented and what were the results. Even though this was project, it incorporates features of qualitative research.

The project documentation can be examined what and how things were done, and it shows mistakes that can be identified and minimized in subsequent projects.

Documentation will take place through the Active Directory design, step by step and by sub-region. After the design moving to the deployment, which provides the definitive and concrete results and achievements.

Keywords: Active Directory, education network, design, deployment, Windows 7

1 Johdanto

Opinnäytetyön aiheeni on uuden Active Directoryn suunnittelu ja käyttöönotto kahden kaupungin opetusverkossa.

Syynä uudistamiseen oli kaupunki X:n ja kaupunki Y:n oppilasverkkojen yhdistyminen. Vanha verkkoympäristö oli suunniteltu pelkästään Kaupunki X:n käyttöön. Toinen syy uudistamiselle oli palvelimien ominaisuuksien riittämättömyys, kun työasemissa siirryttiin Windows7 käyttöjärjestelmiin.

Olin mukana vuonna 2005 nykyisen Active Directoryn (AD) suunnittelussa ja käyttöönotossa, joten minut pyydettiin mukaan projektiin, kun aloitin työharjoittelun tammikuussa 2010. Projektissa oli mukana neljä Kaupunki X:n työntekijää. Oma roolini projektissa oli toimia suunnittelijana, toteuttajana ja testajana. Tarpeena oli uudistaa AD nykystandardeja vastaavaksi, kun koneissa otettiin käyttöön Windows 7.

Projekti alkoi keväällä 2010, kun tuli tieto kaupunkien suunnitelmista yhdistää koulujen ylläpito ja muut käytännöt. Saman vuoden alussa aloitin työharjoittelun kaupunki X:n tietohallinnossa. Viimeinen kaupunki X:n kouluista asennettiin tammikuussa 2012, neljä kuukautta aikataulusta jäljessä. Viivästymisen syy oli laitepulassa eli kouluilla ei ollut tarpeeksi asennukseen sopivaa laitteistokantaa.

Kyseessä on projektiluonteinen tuotantoon tulevan järjestelmän käyttöönottosuunnitelma eli projektin dokumentointi. Kerron, mistä opetusverkon Active Directoryn suunnittelu ja käyttöönotto aloitettiin, miten se toteutettiin ja mihin päädyttiin. Kyseessä on projektihanke, joka kuitenkin itsessään sisältää laadullisen tutkimuksen piirteitä.

Projekti syvensi oman alan ammatillista osaamistani ja oppimista tunnistamaan erilaisia työympäristön kehittämistarpeita ja esittämään ratkaisuehdotuksia.

Projektin toimeksiantaja sai projektidokumentaation, josta voidaan tarkastella mitä ja miten asiat tehtiin, esimerkiksi jos tulee tarvetta tarkastella jo tehtyä tai tehdä samainen uudelleen. Dokumentoinnin avulla virheet voidaan myöhemmissä projekteissa kartoittaa ja minimoida.

Kysymyksen muodossa aiheeni on: *"Miksi ja miten uusi Active Directory toteutettiin?"*. Jatkokysymyksenä on: *"Mitkä ovat uuden AD:n edut vanhaan verrattuna?"*.

2 Projektin teoreettinen viitekehys ja toteuttamisen kuvaus

Tässä työssä käytetyt nimet ja IP-osoitteet eivät ole turvallisuussyistä todenmukaisia.

2.1 Active Directory

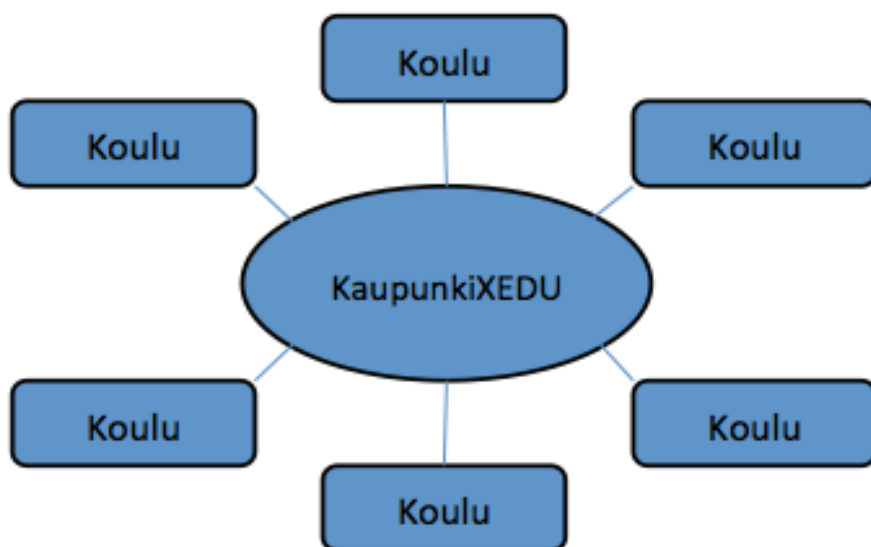
Active Directory on Microsoftin toteutus internet-standardien mukaisesta hakemistopalvelusta (directory service). Perinteisen määritelmän mukaan hakemistopalvelu eroaa hakemistosta (directory) siten, että se sisältää hakemiston tiedot eli tietovaraston (tietokannan) ja se tarjoaa myös palvelut (services), joilla tietovarastoon päästään käsiksi.

Active Directory vähentää ylläpidettävien hakemistojen määrää, koska esimerkiksi käyttäjätilien, tietokonetilien ja jaettujen resurssien hallinta voidaan tehdä yhtenäisillä rajapinnoilla ja työkaluilla (Kivimäki 2009, 651).

2.2 Verkkoympäristö

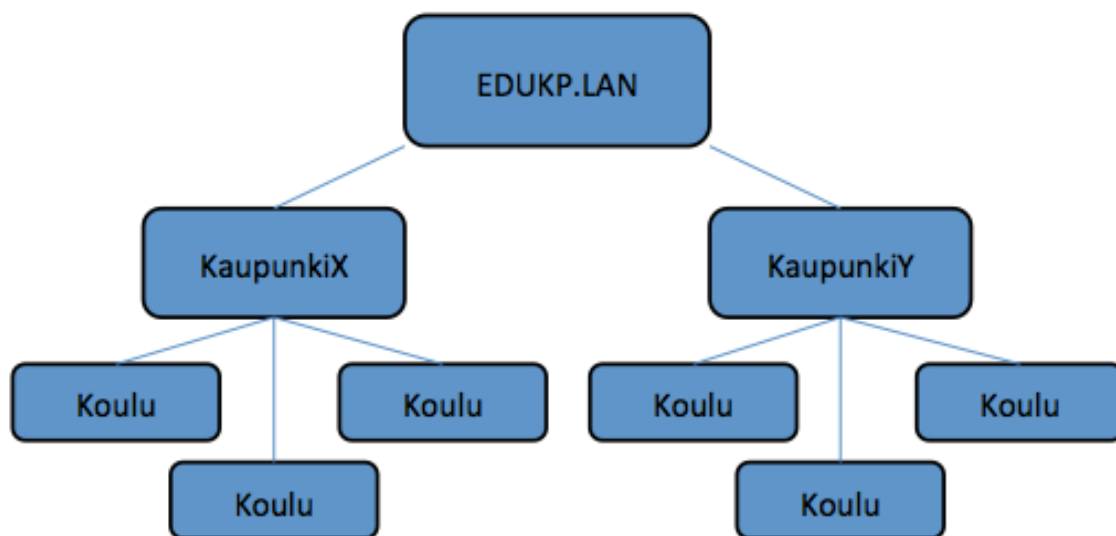
Vanha verkkoympäristö on ollut toiminnassa vuodesta 2005. Tämä verkkoympäristö on suunniteltu Kaupunki X:n käyttöön ja sitä joudutaan nyt uusimaan, koska mukaan tulee Kaupunki Y:n opetusverkko. Toisena syynä uudistamiselle on yksinkertaisesti palvelimien ominaisuuksien riittämättömyys, kun työasemissa tullaan siirtymään Windows7 -käyttöjärjestelmään.

Kaupungeissa oli käytössä kaupunkikohtaiset AD-palvelimet ja opetusverkot, näiden yhdistämisellä ei olisi saavutettu vaadittavia tarpeita ja ne täytyi uudistaa. Vanhassa opetusverkossa koulut olivat keskitetty yhteen paikkaan (Kuvio 1), tätä ei voitu hyödyntää enää uudessa verkossa.



Kuvio 1. Kaupunki X:n opetusverkon verkkoympäristö ennen.

Yhdistämisen jälkeen kaupunkien opetusverkot (kuvio 2) olivat yhtenäiset, hallittavissa ja kaupunkilisäykset mahdollisia.



Kuvio 2. Opetusverkon verkkoympäristö jälkeenpäin.

2.3 Testausvaiheen verkko

Erillistä testausvaiheen verkkoa ei ole olemassa vaan kaikki testaukset suoritetaan tuotanto-verkossa, niin että uuteen ympäristöön ei ole käyttäjillä pääsyä.

IP -alueissa luokat A, B, C ja D ovat luokittelutapoja (A.B.C.D), joiden avulla IP-osoitteet jaetaan ryhmiin suurta, keskinkertaista ja pientä osoitteiden tarvetta varten (Samela 2001, 67). IP -alueet tulevat pysymään muuttumattomina (10.0.x.x). Toimipaikoilla on käytössä C-luokan verkko, isommissa toimipaikoissa on hyödynnetty useampaa C-luokan verkkoa.

2.4 Käyttäjätunnukset

Käyttäjät tulevat saamaan uudet henkilökohtaiset tunnukset. Koko koulun kattavat yleistunnukset poistuvat käytöstä. Luokkatunnukset ovat mahdollisia, tunnuksia valvoo luokan opettaja.

Vanhasta AD:sta ei siirretä tunnuksia eikä oikeuksia uuteen, vaan kaikki käyttäjätunnukset tehdään alusta.

3 Suunnitteluvaihe

3.1 Projektin taustat

Vuonna 2010 kaupunkien tietohallinnot päättivät, että molempien kaupunkien opetusverkon ylläpito ja käytännöt yhtenäistetään. Suunnittelu aloitettiin kartoittamalla molempien kaupunkien nykyiset käytännöt, minkä jälkeen niitä verrattiin keskenään ja mietittiin, mistä käytännöistä voitaisiin/pitäisi luopua. Osasta vanhoista käytännöistä luovuttiin tietoturvasyistä. Suunniteltavina asioina tulisi olla, koulujen yhteiskäyttötunnukset sekä yhteiset yleiset verkkojaot, joihin vanhastaan oli kaikilla käyttäjillä rajoittamaton käyttöoikeus.

3.1.1 Aktiivihakemisto

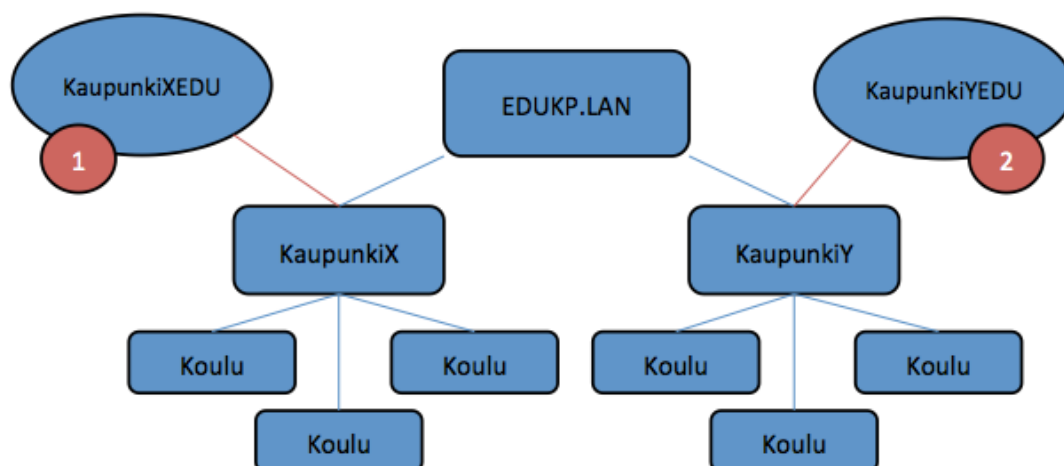
Aktiivihakemiston tekninen suunnittelu määrittä tietohallinnon ja siihen liittyvien kaupunkien aktiivihakemiston rakenteen. Huolellisessa suunnittelussa pyritään huomioimaan mahdolliset ongelmat ja vikatilanteet parantaen samalla käyttäjien tietoturvaa sekä käyttömukavuutta.

Vaatuksina aktiivihakemistolle oli hierarkkinen, puumainen rakenne, että se on hajautettu eri palvelimille sekä mahdollisuus muuttaa hakemiston rakennetta. Objekteina oli käyttäjät, ryhmät, tulostimet ja palvelut.

3.1.2 Uuden ja vanhan toimialueen erot

Koulupuolella nykyisin käytössä oleva Active Directory -toimialue on rakennettu ja käyttöön otettu vuonna 2005. Palvelimien ominaisuudet eivät enää riitä vastaamaan nykyisiä vaatimuksia ja tarpeita, ominaisuuksiltaan sekä laitteitaan ja näin ollen niiden päivitys uudempaan oli tarpeellinen. Palvelimet tullaan päivittämään Windows Server 2003 -käyttöjärjestelmästä Windows Server 2008 R2 -käyttöjärjestelmään. Päivitys tapahtuu myös työasema puolella, Windows XP -ympäristö päivitettiin uuteen Windows 7 -ympäristöön.

Vanhan ja uuden toimialueen välille jätetään luottamussuhde vielä kuukaudeksi (kuvio 3), jonka aikana mahdolliset tärkeät tiedostot säilytetään vanhalla palvelimella, mikäli niiden puuttumista ei ole heti huomattu. Käyttäjiä muistutetaan kuitenkin 2-4 viikon ajan kopiaimaan vanhasta järjestelmästä mahdollisia tiedostoja. Kuuden kuukauden kuluttua vanha toimialue ajetaan alas ja tiedot poistetaan.



Kuvio 3. Uusi verkko ja luottosuhde vanhaan.

Ensimmäisenä uuteen toimialueeseen liitetään Kaupunki X. Kun Kaupunki X:n osilta vanhasta toimialueesta KaupunkiXEDU on siirretty kaikki tarpeellinen ja se on todettu toimivaksi, puretaan Kaupunki X:n luottosuhde KaupunkiXEDU:un ja lisätään Kaupunki Y:n luottosuhde KaupunkiYEDU:un. Tämän jälkeen ruvettiin käymään samaa läpi Kaupunki Y:n osilta.

Sertifikaatit sijaitsevat EDUKP-palvelimella. Mahdollisten uusien kaupunkien lisääminen on helpompaa, koska kaikki palvelimet sijaitsevat kaupunkikohtaisesti EDUKP-palvelimessa. Sertifikaateilla varmennetaan työasema tai käyttäjä, jotta kone- ja käyttäjätilit voidaan varmistaa oikeiksi. Sertifikaatit sijaitsevat EDUKP-palvelimen juuressa, jotta kaikilla on pääsy sinne. Tämä järjestely edesauttaa sitä, etteivät uhat ja tartunnat leviä yli oman toimialueen, kun ne pysäytetään tietoliikenneasetuksilla tai käyttöoikeuksilla.

Uuden toimialueen ja ominaisuuksien myötä saadaan Mac OS X -tuki, jonka avulla organisaatioyksiköt, jotka käyttävät Mac-tietokoneita, saadaan toimimaan samassa toimialueessa.

Suurena etuna saavutetaan etätyöskentelyn mahdollisuus. Kun käyttäjä kirjautuu kotona VPN-yhteydellä verkkoon, saa hän käyttöönsä opetusverkon tarjoamat palvelut. Kone- ja käyttäjätilit on oltava samassa AD-puussa, jotta tunnistautuminen hyväksytään ja kirjautuminen onnistuu.

3.1.3 DNS-nimipalvelu

DNS-järjestelmän tarkoitus on vastaanottaa toimialueen nimi, esimerkiksi www.google.fi tai www.laurea.fi, asiakassovellukselta ja palauttaa sille nimeä vastaava IP-osoite (Samela 2001, 209). DNS-palvelun tehtävä on selvittää verkko-osoitteet IP-osoitteiksi.

DNS on nimenselvityksen menettelytapa, joka on luotu poistamaan tasaisen nimiavaruuden aiheuttamat ongelmat. DNS perustuu hierarkkiseen nimirakenteeseen sekä hajautettuun tietokantaan. (Samela 2001, 203.)

DNS -nimipalvelun rakenne tulee noudattamaan aktiivihakemistorakennetta. Suunnitelmassa käsitellään sisäisen nimipalvelun konfigurointia ja viitataan ulkoiseen nimipalveluun vain sähköpostin tarvitsemien mx-tietueiden osalta.

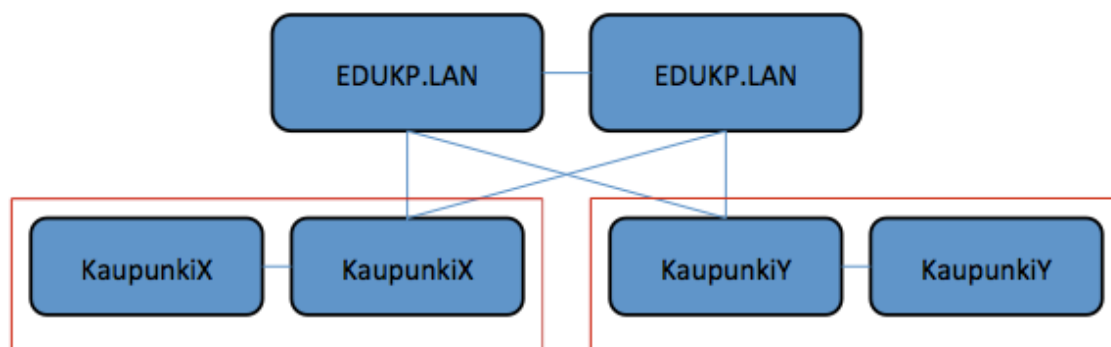
3.2 Active Directory suunnittelua

Suunnitteluvaihe on erittäin tärkeässä roolissa Active Directoryn pystytyksessä. Seuraavassa lainauksessa Kivimäki on hyvin ilmaissut AD suunnittelun perustarpeet. ”Active Directoryn toteutukseen liittyy useita tekijöitä. Ensimmäiseksi on suunniteltava DNS -nimiavaruus, joka sisältää toimialuehierarkian ja luottosuhteet. Lisäksi on suunniteltava organisaatioyksiköt (OU). Yhden toimialueen sisällä käyttäjätilit ja muut objektit voidaan järjestellä käyttämällä soveltuvaa organisaatioyksikköhierarkiaa. Isossa ja laajassa verkossa tulee suunnitella myös toimipaikat (sites), joiden avulla optimoidaan replikointi- ja sisäänkirjautumisliikennettä.” (Kivimäki 2005, 8.)

3.2.1 DNS-nimipalvelu ja WINS

Yhteiseen metsärakenteeseen siirryttäessä, yhteisen aktiivihakemiston, Scheman, konfiguraation ja Global Catalogin lisäksi yhteiseksi tulee myös metsän DNS -nimiavaruus.

Kuntien välinen metsä- ja DNS-nimipalvelurakenne tulee muodostumaan juuritoimialueesta (kuvio 6.) ja lapsitoimialueista (kuvio 7.). DNS-nimipalvelu on yksi aktiivihakemiston kriittisimmistä osista. Näin ollen sen toiminta täytyy varmistaa kaikissa olosuhteissa. Varmistus suoritetaan kaupungin sisäisesti (kuvio 4), eli esimerkiksi kaupunki X varmistuu toisen kaupunki X palvelimen kanssa. Kaupunkien varmistaminen ei mene toistensa kanssa ristiin, vaan varminee niin sanotusti kaupungin sisällä, ilman yhteyttä toisen kaupungin palvelimeen.



Kuvio 4. Replikointirakenne.

Kaupungeilla ei ole toisiinsa suoraa yhteyttä. Toinen kaupunki ei tee toisen kaupungin tiedoilla mitään, mutta koska käyttäjän sisään kirjautuminen voi tapahtua molemmissa kaupungeissa, täytyy niiden kuitenkin olla yhteydessä toisiinsa, tässä tapauksessa EDUKP.LAN palvelimen kautta.

Jokainen kaupunki on vastuussa omasta DNS-palvelusta A- ja SRV-tietueiden osalta samalla tavalla kuin tietohallinto vastaa omasta toimialueestaan näiden tietueiden osalta. Tietohallinto vastaa myös metsän yhteisiä tietoja sisältävän vyöhykkeen (_msdsc) ylläpidosta. A- ja SRV-tietueita ei tarvitse muokata, koska kaupungeilla ei ole opetusverkossa julkisia nimipalveluita.

3.2.2 Organisaatioyksiköt

Organisaatioyksiköt vastaavat kaupungin todellista organisaatiokuvaa.

Organisaatioyksikköjen (OU) tulisi peilata yrityksen liiketoiminnan tai organisaation rakennetta. Organisaatioyksikköjä voidaan luoda, jos halutaan delegoida käyttäjäryhmiä, käyttäjiä ja resursseja koskevia järjestelmänhallinnallisia oikeuksia. Organisaatioyksiköt tulisi järjestellä loogiseksi rakenteeksi, joka sopii yrityksen toimintatapaan ja rakenteeseen. (Kivimäki 2005, 10.)

Organisaatioyksiköinä on lisäksi käyttäjäryhmät, koneryhmät sekä käyttäjätilit. Näiden OU-rakenteet muistuttavat ympäristön fyysistä mallia.

3.2.3 Toimipaikat

Toimipaikkojen (Sites) idea on hallinnoida domainin sisäistä tietoliikennettä. Esimerkiksi eri toimipisteet kannattaa jakaa omiin toimipaikkoihin, jolloin voidaan vähentää turhaa liikennettä esimerkiksi hitaan WAN -yhteyden (WAN = Wide Area Network) yli. Toimipaikat ovat maantieteellisiä ja fyysisiä toimipaikkoja.

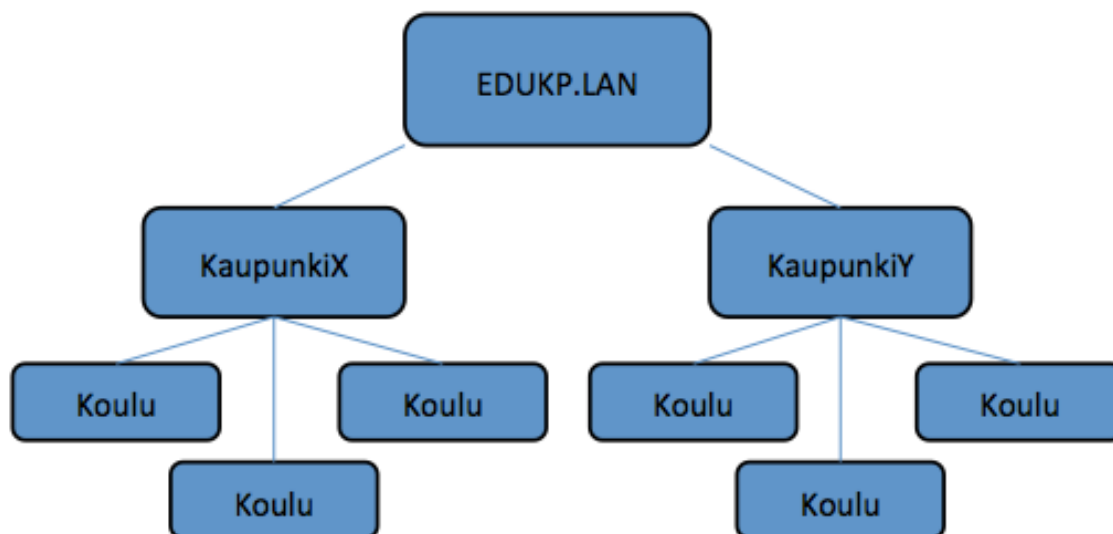
3.2.4 Nimiavaruus

Active Directoryn nimiavaruus määrittää yrityksen ylimmän tason toimialuenimen. Tärkein päätös nimiavaruuteen on se, onko Active Directoryn nimiavaruus sama kuin organisaation käyttöön mahdollisesti rekisteröity DNS-nimiavaruus (Internet-toimialuenimi). Vaihtoehtoina on sisäinen nimiavaruus, eli Intranet, palomuurin sisäpuolella oleva ja ulkoinen nimiavaruus, eli extranet, palomuurin ulkopuolella oleva nimiavaruus. Active Directory -toimialueiden nimeäminen vaikuttaa kaikkiin Active Directoryn objekteihin. Jos käytössä oleva ulkoinen DNS-nimiavaruus on esimerkiksi xyz.fi, Active Directoryn nimiavaruudeksi voidaan valita xyz.fi (Kivimäki 2005, 8.)

Tällä hetkellä ei ole rekisteröityä DNS-nimeä, joten nimiavaruus ei ole julkinen.

3.2.5 Toimialuerakenne ja luottosuhteet

Toimialueina toimivat toimipisteet eli koulut. Toimipisteet sijoittuvat periytymishierarkiassa kaupunkien alle (kuvio 5). Koulujen alla voi olla myös luokkajakoja, jotka sijoittuvat taas koulujen alle. Luottosuhteita voi olla myös ulkoisiin järjestelmiin, esimerkiksi oppilasrekistereihin.



Kuvio 5. Luottosuhteet.

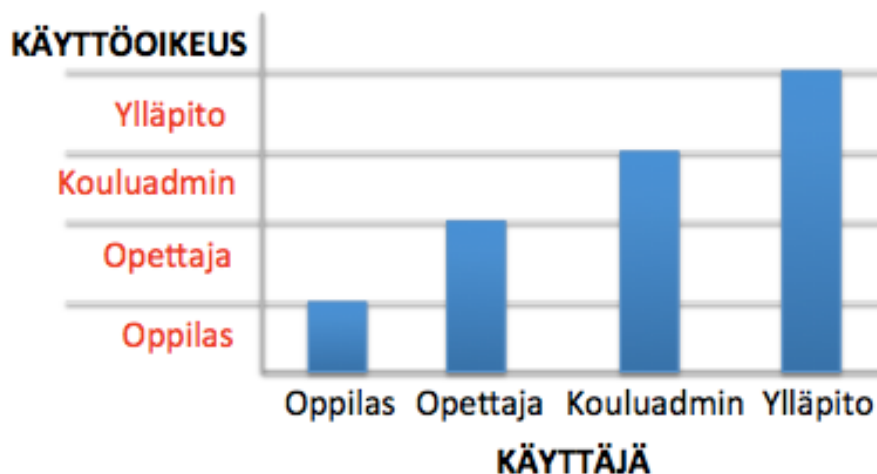
3.2.6 Ryhmät

Ryhmäkäytänteissä suurimpana muutoksena vanhaan Active Directoryyn verrattuna oli se, että vanhat koko koulukohtaiset käyttäjätilit poistuvat. Uuteen Active Directoryyn ei siirretä vanhasta käyttäjätunnuksia, vaan kaikki tehdään alusta.

Käyttäjät saavat uudet henkilökohtaiset tunnukset. Mahdolliset ATK-luokissa käytettävät yhteistunnukset ovat mahdollisia, tunnuksien käyttöä valvovat ATK-opettajat. AD:ssa käyttäjät jaetaan ryhmiin, jolloin saadaan helpommin ja tarkemmin osoitettua tarvittavat oikeudet sekä pääsy tarvittaville verkkoasemille.

Ryhmiä on kahta erilaista: kone- ja käyttäjäryhmät. Hyviä koneryhmä esimerkkejä ovat aula-koneet, joissa on selkeästi rajoitettu käyttöä, sekä isot kokonaisuudet, kuten luokkatilat, joissa on paljon koneita. Ryhmäasetuksilla ja määreillä koneet saadaan samanlaisiksi, asetuksiltaan ja oikeuksiltaan. Ryhmät voidaan pilkkoa vielä paikalliseen domainiin, esimerkkinä pelkkä Kaupunki X, Global, eli koko metsä, tai Universal, joka voi kuulua ulkopuolisiin järjestelmiin.

Erilaisia käyttäjäryhmiä (kuvio 6) ovat opettajat, oppilaat, adminit, kouluadminit, aula, ja ATK-luokat. Oppilaan oikeudet rajoittuvat oppilasoikeusmäärittelyihin. Opettajalla on oppilasoikeuksien lisäksi opettajaoikeudet, jotka lisäävät joitain käyttöoikeuksia. Kouluadmineilla on näiden kahden oikeuksien lisäksi vielä paikallisen adminin ylläpito-oikeudet. Adminien oikeudet kattavat taas kaikki aikaisemmat oikeudet ja lisäksi ylläpito-oikeudet.



Kuvio 6. Ryhmäoikeudet.

3.3 Aktiivihakemistorakenne ja konfiguraatio

Aktiivihakemiston metsärakenne koostuu metsän yhteisistä juuritoimialueista ja kaupunkikohtaisista alitoimialueista. Juuritoimialuetta ja sen palvelimia ylläpidetään yhteisessä tietohallintokeskuksessa.

3.3.1 Metsä- ja toimialuerakenne

Metsä koostuu useista puista, jonka ylin puu on juuritoimialue EDUKP.LAN. Juuritoimialueen alle luodaan kaupunkikohtaisesti omat puut, eli alitoimialueet. Toimialueet ja Metsä nostetaan heti asennuksen yhteydessä Windows Server 2008 -tilaan. Alitoimialueiden nimet tulevat noudattamaan seuraavaa mallia.

Toimialueiden dns-nimet:

Kaupunki Y edukaupunkiy.edukp.lan

Kaupunki X edukaupunkix.edukp.lan

Toimialueiden Netbios-nimet:

Kaupunki Y EDUKAUPUNKIY

Kaupunki X EDUKAUPUNKIX

3.3.2 Aktiivihakemiston käyttämien kansioden sijoittaminen

Domain controllereissa (DC) on aktiivihakemiston suhteen kolme tärkeää kansiota. NTDS, SYSVOL ja Aktiivihakemiston lokit. Oletuksena nämä asentuvat Windows järjestelmäkansioon.

Koska ympäristö on pieni ja tarkoituksena on virtualisoida osa kyseisistä domain controller koneista, kannattaa kanta, SYSVOL ja lokit asentaa oletustallennus paikkoihin. Näin rakenne on yksinkertainen ja toimiva. Pitää kuitenkin varmistaa, että domain controller koneilla on aktiivihakemistoa ja sen varmistamista varten minimissään 10 GT levytilaa järjestelmäosiolla. Tämä levytilavaatimus on tänä päivänä helppo toteuttaa.

3.3.3 Metsän toimipaikan rakenne

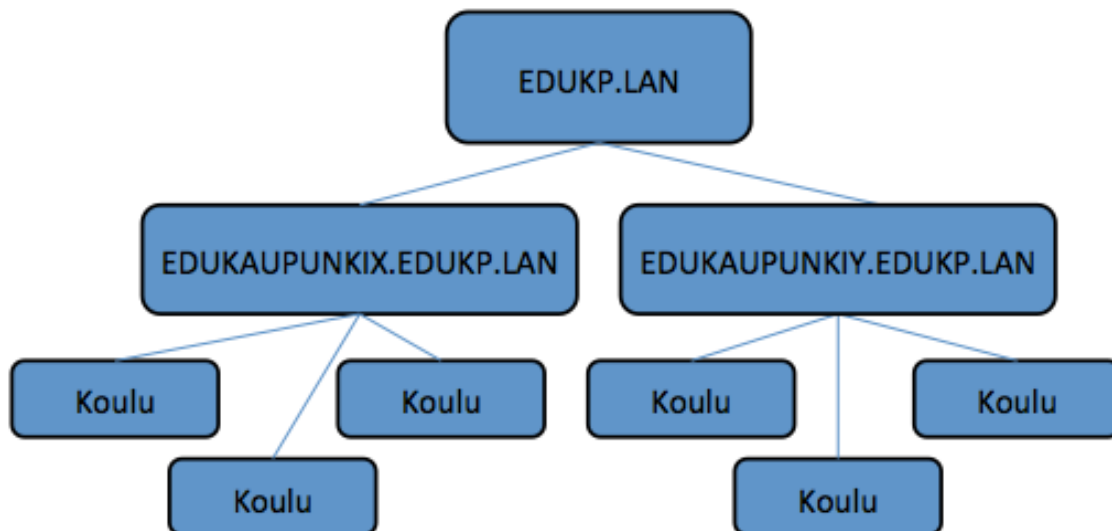
Toimipaikat kertovat aktiivihakemistopalvelulle verkon fyysisen rakenteen, jonka avulla hoidetaan mm. replikointi, autentikointi ja palvelujen paikallistaminen lähimmästä mahdollisesta domain controllerista. Metsän juuritoimialueen ja alitoimialueiden domain controllerit sijoitetaan tietohallintokeskukseen ja toimipisteen nimeksi annetaan EDUKP. Tämä tapahtuu käytännössä uudelleen nimeämällä Default-First-Site-name toimipaikka. Muille toimipaikoille ei ole tällä hetkellä tarvetta, joten luonti on varsin yksinkertainen ja muuta konfiguraatiota ei tarvitse palvelimille tehdä.

3.4 Organisaatioyksikkörakenne

Organisaatioyksikkö rakenne toteutetaan siten, että se mahdollistaa keskitetyn hallinnan ja ylläpidon delegoinnin. OU-rakenne malleja tulee kaksi, toinen tulee juuritoimialueeseen ja toinen kaupunkikohtaiseen alitoimialueeseen. Alitoimialueiden OU-rakenteet toteutetaan samalla mallilla, ainoastaan nimeäminen vaihtelee virastoittain.

3.4.1 Juuritoimialueen OU-rakenne

Juuritoimialueen OU-rakenne pidetään mahdollisimman yksinkertaisena. Omat OU:t luodaan eri palvelintyypeille (sähköpostipalvelimet, sovelluspalvelimet jne.), ylläpitotunnuksille, palvelutunnuksille ja juuritoimialueen mahdollisille työasemille. Tässä määritellään pääpiirteet eli runkotoimialueille, tähän asetetut määräykset periytyvät alaspäin alitoimialueille. Esimerkiksi jos EDUKP.LAN:ssa määritetään salasanan pituudeksi 25 merkkiä, ei sitä voi määrittää alitoimialueissa eli EDUKAUPUNKIX.EDUKP.LAN:issa lyhyemmäksi. Kuvassa (kuvio 7) esitetään miten määrittäykset periytyvät alaspäin EDUKP.LAN:sta EDUKAUPUNKI.EDUKP.LAN:iin ja siitä koulukohtaisiin asetuksiin.



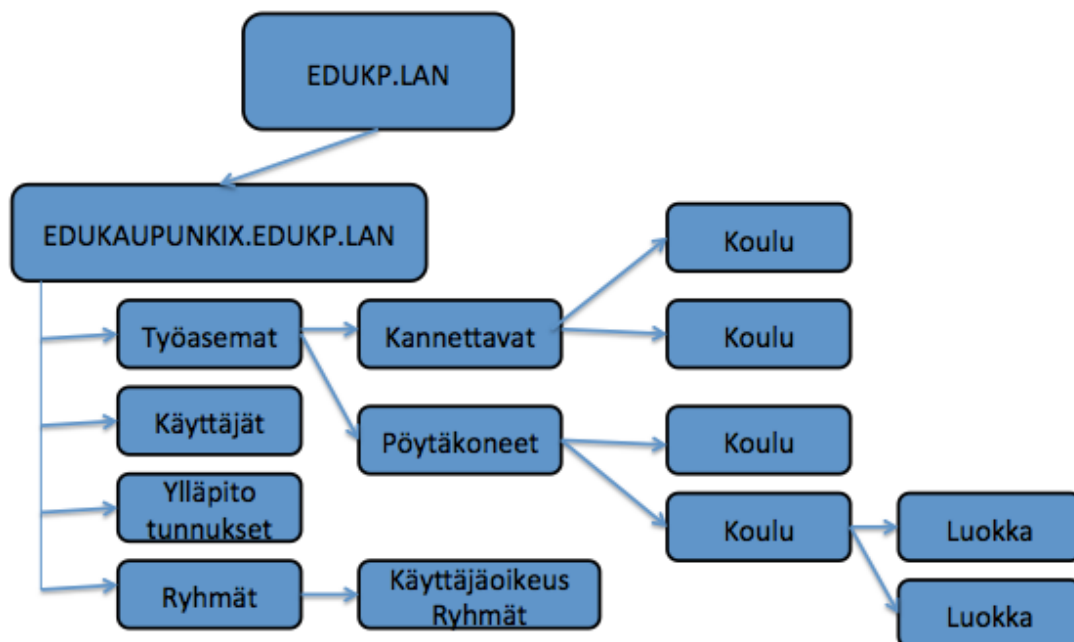
Kuvio 7. Juuritoimialueen OU-rakenne.

Yhteisinä palveluina kaupunki X ja kaupunki Y käyttävät esimerkiksi virustorjuntaa ja VPN-yhteyttä.

3.4.2 Alitoimialueen OU-rakenne

Alitoimialueen rakenne kuvastaa ylläpidettäviä toimialoja (kouluja / oppilaitoksia) ja niiden resursseja. Jokaiselle toimialalle luodaan oma OU, johon tulee vielä tarkentava OU-rakenne.

Alitoimialueen OU -rakenne (kuvio 8) määräytyy siten, että ylimmällä tasolla on EDUKP.LAN, tämän alla EDUKAUPUNKI.LAN. Kaupunkikohtaisen haaran alle tulee työasemat, jotka jaetaan pöytäkoneisiin ja kannettaviin, nämä taas jaetaan koulukohtaisesti. Pöytäkoneet jaetaan vielä luokkakohtaisesti, mikäli kouluissa on isoja tiloja, missä on monta työasemaa.



Kuvio 8. Alitoimialueen OU-rakenne.

Koulukohtaisilla kannettavilla ei ole luokkajakoa, vaan ne liikkuvat käyttäjien mukana koulussa. Koulut, joissa on isoja kokonaisuuksia, jaetaan palasiin, kun taas pienemmissä organisaatioyksiköissä ei jakoa tarvita.

3.5 Nimeämiskäytännöt

3.5.1 Nimeämissuunnittelu ja organisaatioyksiköiden nimeäminen

Nimeämssuunnittelussa tulee ottaa huomioon, ettei työasemien nimistä tule sanoja. Nimestä tulee saada myös selville, mikä työasema on ja missä se sijaitsee, niin ettei Description -kenttää tarvitse katsoa. Nimeämisen tulee olla yhtenäinen ja kaikissa toimipaikoissa sekä kaupungeissa tulee käyttää samaa nimeämispolitiikkaa. Suunniteltu nimeämispolitiikka auttaa työskentelyä. Jos esimerkiksi tulee ongelmia, tarvitsee tietää vain koneen nimi, josta pystytään päättämään, missä se on sekä mihin AD-haarioihin se kuuluu. Koneen nimeä ei käyttäjän tarvitse ymmärtää, tämä voikin käyttäjän silmin näyttää erikoiselta, mutta ylläpito ymmärtää nimeämisen.

Organisaatioyksiköiden nimeämiskäytännössä haetaan kaikille kaupungeille yhteistä mallia, joka tukee kaupunkien mukaantuloa myös myöhäisemmässä vaiheessa. Organisaatiot nimeetään siten, että ne kuvaavat kaupunkien sisäisiä toimialoja, toimialan sijaintia ja/tai resursseja. Nimet tulevat vastaamaan kaupunkien käyttämiä virallisia nimiä.

3.5.2 Laiteobjektien nimeäminen ja kustannuspaikan tunnistaminen

Laitenimeämisessä uuden nimikäytäntö aloitetaan uusista laitteista eri kunnissa olevien eri käytäntöjen takia. Laitteiden nimestä on pystyttävä erottamaan kaupunki, jonka omaisuutta ne ovat, toimipiste/koulu kaupungin sisällä sekä yksikäsitteinen juokseva numerointi. Laitteiden nimeämisessä laitteen tyyppi otetaan huomioon omalla tunnisteella, jolloin nimestä selviää onko laite kannettava vai pöytäkone. Pöytäkoneen tunniste on D-kirjain ja kannettavan tunniste X-kirjain. Numeroinnissa on aina viisi numeroa. Lisäksi opetusverkon kaikkiin laitteisiin laitetaan etukirjaimeksi E-kirjain kuvaamaan opetusverkon laitetta.

Vaihtoehtoina D-kirjaimelle olisi ollut W (workstation) ja X-kirjaimelle L (laptop). Kaupunki X:llä on ollut käytössä pitkään kirjainmerkinnät D ja X. E tarkoittaa EDU:a, lyhenteenä sanasta Education. Alla olevassa taulukossa on purettu laiteobjektien nimeämiskäytäntö tarkemmin osiin.

Kaupunki / lyhenne		Yksikkö / lyhenne		Laitteen malli X = kannettava D = pöytäkone	Juokseva numerointi	Koneen nimi:
Kaupunki X	KX	Koulu	KOU	D	00001	EKXKOUND00001
Kaupunki X	KX	Lukio	LUK	X	00002	EKXLUKX00002
Kaupunki Y	KY	Lukio	LUK	X	00001	EKYLUX00001

Taulukko 1. Laiteobjektien nimeäminen

Palvelimien nimeämiskäytäntö on helpompi, koska niiden nimestä täytyy selvittää, kuuluuko se kaupungille vai tietohallinnolle, sekä palvelimen rooli, virtualisointi ja juokseva numerointi. Palvelimen numeroinnissa käytetään aina kahta numeroa.

Laitteiden kustannuspaikan tunnistamiseen käytetään koneen Description -attribuuttia. Päivitys voidaan tehdä muutostilanteessa Active Directory Users & Computers konsolilla. Sama on myös tulostimien tunnistuksessa, Description -kenttään merkitään koulu- ja tila/huone -merkinnät.

3.5.3 Ryhmäobjektien nimeäminen

Ryhmiä nimeämiskäytännössä noudatetaan samaa kaavaa kuin organisaatioyksiköiden tai laitteiden nimeämisessä. Ryhmien nimikäytännössä käytetään samoja lyhenteitä kuin laitteissa ja organisaatioyksiköissä. Ryhmän nimessä käytetään tavuviivaa välilyönnin tilalla. Yhtei-

sessä metsässä on huomioitava ryhmien käsittelyssä ja nimeämisessä niiden näkyvyys koko metsän alueella. Jos kouluille toteutettaisiin oma sähköpostijärjestelmänsä, niin varsinkin sähköpostijakelulistojen kanssa tietoturvan kannalta on olennaisen tärkeää määritellä, mitenkä käyttäjät tunnistautuvat eri kuntien samojen toimialojen jakelulistat.

Nimestä pitää selvitä seuraavat asiat:

- Ryhmän laajuus (Universal, Global ja Domain Local).
- Ryhmän tyyppi (Security tai Distribution -ryhmä).
- Omistajakaupunki.
- Toimipaikka.
- Ryhmän tarkoitus (annettava käyttöoikeus Domain Local -ryhmiä käytettäessä).
- Distribution-ryhmälle ei ole tällä hetkellä käyttöä, mutta tarpeen tullen nimeäminen tapahtuu mallin mukaan.

Ryhmien nimet muodostuvat ryhmän laajuuden, tyyppin, omistaja kaupungin, toimipaikan, tarkoituksen ja oikeuksien mukaan. Esimerkkinimenä Otetaan Global, security-tyyppinen, KaupunkiX:n omistama, toimipaikkana lukio. Ryhmännimen eteen laitetaan kirjain E, ilmoittamaan, että kyse on opetusverkon ryhmästä, sekä perään omistaja kaupunki, KAUPUNKIX. Väli- viivalla jaetaan toimipaikka, -LUK ja väliviivalla erotetaan myös Global ja Security merkinnät, eli sanojen ensimmäiset kirjaimet, -GS. Näin muodostuu EKAUPUNKIX-LUK-GS, ryhmän nimi.

Ryhmän laajuus	Ryhmän Tyyppi	Omistaja Kaupunki	Toimi- paikka	Tarkoi- tus	Oikeu- det R/M/F	Ryhmän Nimi
Global	Security	Kaupunki X	Lukio	Kooste		EKAUPUNKIX-LUK-GS
Domain Local	Security	Kaupunki X	Lukio	Oikeus	M	EKAUPUNKIX-LUK-DLS-M
Universal	Distribu- tion	Kaupunki X	Lukio	Jakelu- lista		EKAUPUNKIX-LUK-ALL- UD
Universal	Distribu- tion	Kaupunki X	Koko henki- löstö	Jakelu- lista		EKAUPUNKIX-ALL-UD
Domain Local	Security	Kaupunki Y	Lukio	Oikeus	R	EKAUPUNKIY-LUK-DLS-R

Taulukko 2. Malli ryhmäobjektiivien nimeämisestä.

3.5.4 Käyttäjätunnukset

Salaus ja tietoturva on yleisesti rinnastettu usein toisiinsa. Kuvitellaan, että tietoturvan tärkein tavoite on saada pidettyä tiedot salassa ulkopuolisilta, ja että juuri siihen salaus on tarkoitettukin. Tietoturvan tavoitteena on kuitenkin turvata tietojenkäsittelyn toimivuus erilaisia uhkia vastaan, sekä suojata tietoja oikeudettomilta muutoksilta. Osa tietoja tai tiedostoja kohtaavista uhkista on teknisiä, esimerkiksi kiintolevyn hajoaminen joka johtaa pahimmassa tapauksessa tietojen menetykseen ja palvelun keskeytymiseen.

Suurin osa uhista aiheutuu kuitenkin käyttäjän omasta toiminnasta. Ulkopuoliset hyökkääjät pyrkivät saamaan luottamuksellista tietoa tai vahingoittamaan tietojärjestelmien toimintaa. Käyttäjät tekevät kiireen, väliin pitämättömyyden tai osaamattomuuden vuoksi virheitä, joilla voi olla vakaviakin seurauksia. (Järvinen 2003, 29.)

Salasanamäärityksissä tulee olla tarkka rajauksissa ja määrityksissä. Määritykset tulee olla tiukempia mitä korkeampiin virkoihin mennään ja mitä enemmän tärkeitä tiedostoja ja oikeuksia henkilöllä on, tai hän käsittelee. On turhaa käyttää opettajilla ja ala-asteen ensimmäisellä tai toisella luokalla oleville samoja salasana määrityksiä. Ala-asteen oppilas ei voi muistaa mitään 32 merkkistä salasanaa, kun taas opettajalle se on helpompaa. Salasana tulee myös vaihtaa tarpeeksi usein, jotta tietoturva pysyisi ajan tasalla.

3.5.5 Lukkiutumiskäytännöt

Käyttäjätunnukset lukkiutuvat kolmen väärän salasanan jälkeen. Työasemat menevät ajastetusti lukkoon, kun ne ovat olleet käyttämättä kymmenen minuuttia.

Windows Server 2008 -aktiivihakemisto mahdollistaa myös ryhmäkohtaiset salasanapolitiikat. Ylläpitotunnuksille tehdään tiukempi salasanapolitiikka sisältäen salasanan lyhyemmän vaihtovälin, pidemmän salasanavaatimuksen sekä salasanan monimutkaisuus vaatimuksen päälle, eli salasanassa tulee olla numeroita, isoja kirjaimia ja erikoismerkkejä.

4 Käyttöönotto

4.1 DNS-palvelut

DNS-palvelu asennetaan kaikkiin domain controller -koneisiin sekä juuritoimialueen _msdsc.juuritoimialue.fi replikoidaan kaikkiin metsän DNS -palvelimiin. Active Directoryn juuritoimialueen DNS -nimipalvelun vyöhykenimi (Zone) on EDUKP.LAN, jota ei tarvitse sisäisen käytön takia rekisteröidä virallisesti.

Jokainen kaupunkikohtainen aktiivihakemisto (lapsitoimialue) käyttää asennuksen aikana met-sän juuritoimialueen DNS-nimipalvelua aktiivihakemistoa asennuksen aikana. Alitoimialueen luomisen yhteydessä suoritetaan DNS-palvelun delegointi juuritoimialueesta ja luodaan lapsitoimialueen DNS-nimipalvelimiin oikeat vyöhykkeet, (esimerkiksi EDUKAUPUNKIX.EDUKP.LAN aktiivihakemistoon integroituna).

Kaikki työasemat käyttävät joko kiinteillä tai dynaamisilla IP-osoitteilla oman kaupungin nimipalvelimia.

Juuritoimialueen DNS-nimipalvelusta delegoidaan jokaiselle kaupungille oma alidomain, joista jokainen kaupunki on data- ja palvelutasolla itsenäisesti vastuussa. DNS-kyselyt sisäverkosta julkiseen verkkoon määritetään juuritoimialueen aktiivihakemiston DNS-palvelimiin uudelleen ohjaukset (forwarders) kaupungin/kaupunkien omille julkisille nimipalvelimille.

4.1.1 DHCP

Dynamic Host Configuration -protokolla (DHCP) huolehtii tietokoneiden TCP/IP asetuksista automaattisesti. Tietoja vastaanottavaa (konetta) kutsutaan DHCP-asiakaskoneeksi ja tietoja lähettävää konetta DHCP-palvelimeksi. DHCP-palvelin antaa asiakaskoneelle (kaikissa tapauksissa ainakin) IP-osoitteen ja aliverkon peitteen. Lisäksi DHCP voi tehdä muitakin asetuksia, kuten esimerkiksi oletusyhdyksikäytävän sekä DNS- ja WINS-palvelimien IP-osoitteet. (Samela 2001, 279.)

DHCP tekee suuren tietokonemäärän ylläpidon helpommaksi. Tukikustannukset pienenevät, sillä järjestelmänhoitajien ei tarvitse mennä koneiden luokse konfiguroimaan niiden TCP/IP-parametrejä. (Samela 2001, 280.)

DHCP on erittäin hyödyllinen organisaatioissa, joissa käytetään paljon kannettavia työasemia ja työntekijät matkustelevat konttorista toiseen. Manuaalisesti annettu IP-osoite sallisi kannettavan kytkemisen vain tiettyyn verkkoon, josta seuraisi, että IP-osoite olisi muutettava aina uuteen toimipaikkaan tultaessa. DHCP:n ollessa käytössä kaikissa toimipaikoissa työntekijä (yksinkertaisesti) vain kytkee kannettavan verkkoon ja aloittaa työskentelyn saaden käyttöönsä normaalit verkkotoiminnot TCP/IP:n avulla. Kannattaa kuitenkin muistaa, että matkustelevat työntekijät voivat saada muita verkko-ongelmia, kuten esimerkiksi kaksinkertaiset NETBIOS-nimet, kun verkkoon liitettävän kannettavan NETBIOS-nimi on sama kuin jonkun jo verkossa toimivan koneen. (Samela 2001, 280.)

Aliverkko (Subnet) on verkon segmentti, jossa on käytössä osajoukko kaikista verkolle annetun verkkotunnuksen mahdollistamista osoitteista. Aliverkon peite (Subnet mask) on bittijono, jota käytetään erottamaan IP -osoitteista verkon ja isäntäkoneen tunnukset. (Samela 2001, 83.) Alue on DHCP -palvelimen hallinnoima joukko IP-osoitteita, joita se lainaa DHCP -asiakaskoneille. (Samela 2001, 291).

Työasemat käyttävät DHCP:tä, tulostimilla ja verkkolaitteilla on kiinteät IP-osoitteet. Laitteissa, jotka tarjoavat vakituisesti jotain palvelua verkossa, käytetään kiinteää verkko-osoitetta. Jos käytössä on dynaaminen DNS, jonka DNS-tietue ei päivity reaaliajassa, työasemalta lähtevät palvelupyynnöt saattavat ohjautua väärään paikkaan. Kiinteillä IP-osoitteilla pyritään varmistamaan palvelujen pysyvä saatavuus.

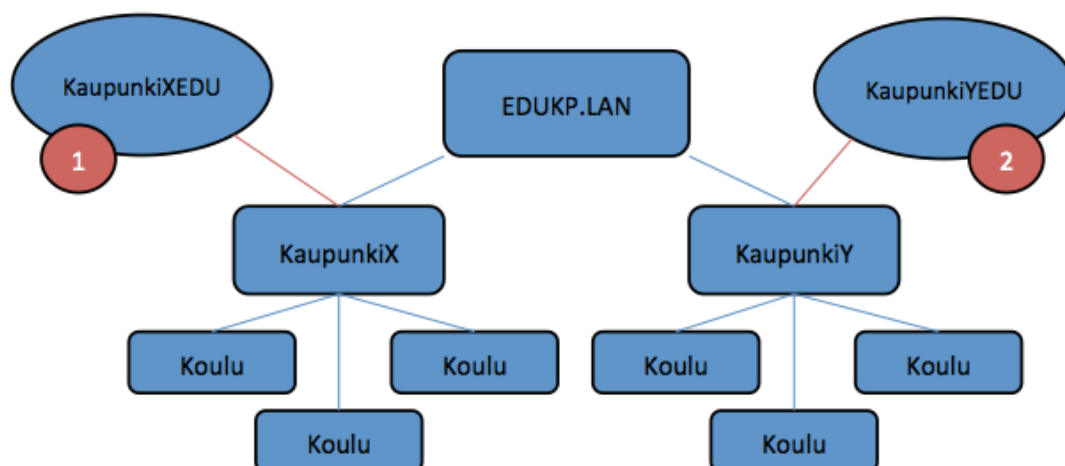
4.1.2 WSUS

WSUS:ia (Windows Server Update Services) käytetään asentamaan työasemien sekä palvelimien päivityksiä. Palvelimelle asennettavan ohjelmiston avulla voidaan valita asennettavat päivitykset ja jakaa ne keskitetysti työasemille. Tällä saavutetaan tarvittavien päivitysten asentaminen ja vältetään turha verkon kuormittaminen sekä ei haluttujen päivitysten asentaminen, joista voi koitua ongelmia. Muihin asennuksiin, kuten ohjelmistojen ja pakettien, käytetään kehittyneempää keskitettyä asennusjärjestelmää. Tässä työssä käytetään SCCM:ää (System Center Console Manager).

4.1.3 Luottosuhteet

Koska kaikkia koneita ei siirretä kerralla, luottosuhteet uuden ja vanhan toimialueen välillä säilytetään kaksisuuntaisella luotolla vielä kuukausi käyttöönotto päivästä (kuvio 9), jotta käyttäjät saavat tiedostonsa siirrettyä,. Näin minimoidaan myös tiedostojen katoaminen ja varmistetaan, että tiedostot ovat varmasti saatavilla.

Edellä mainitun määräajan umpeuduttua vanhat verkkoresurssit siirtyvät vain luku-tilaan, eivätkä käyttäjät voi enää tallentaa vanhoihin verkkoresursseihin. Näin saadaan käyttäjä pakotettua siirtämään vanhat tiedostot uudelle palvelimelle sekä uudet tiedostot heti uuteen verkkoresurssiin, näin vältetään sekaannuksilta sekä siltä, että tiedostoja olisi kahdessa paikassa.



Kuvio 9. Luottosuhteet.

4.2 Työasemat

4.2.1 Suunnittelu ja uusiminen

Suunnittelussa tulee ottaa huomioon että työasemalla on kaikki Windows 7 käyttöjärjestelmään tarvittavat ominaisuudet. Uusissa työasemissa ominaisuudet tulevat olemaan, mutta vanhempien työasemien kanssa tulee selvittää uuden käyttöjärjestelmän yhteensopivuus.

Kaikkein vanhimmat, käytännössä yli viisi vuotta vanhat, työasemat pyritään vaihtamaan uusiin, vanhimmista alkaen. Näin saadaan uusittua samalla laitekanta tuoreempaan ja päivitys hoituu kätevästi muun muutoksen ohella. Uusiminen tulee tehdä myös nyt, ettei vanhoja työasemia jää käyttöön ja saadaan käyttäjille yhtenäinen ympäristö. Vanhimmat koneet vaihdettaisiin muutenkin pian, näin ollen käyttäjille ei tästä koidu enempää keskeytyksiä. Muuten aluksi siirrettäisiin vanha työasema uuteen domainiin ja tämän jälkeen työaseman vaihto uuteen. Tämä aiheuttaisi suuresti turhaa työtä niin käyttäjillä kuin ylläpidolle.

4.2.2 Testaus

Testauksessa pyritään löytämään ei toivotut vaikutukset etukäteen. Testaus kuuluu olennaisena osana pilotointia, joka suoritetaan yhdessä pienessä organisaatiossa. Pilotointi tarkoittaa sitä että koneet asennetaan uuteen domainiin ja loppukäyttäjät pääsevät käyttämään uutta toimialuetta. Tällä tavoin saadaan todennettua mahdollisia oikeita ongelmia, ns. beta-testausta.

Testaus todentaa mahdolliset viat sekä ongelmakohdat ja näin ollen pyritään välttämään pienenkään vian tai ongelman pääsyä massatuotantoon.

Ongelmiksi voi nousta käyttäjä- tai koneoikeudet, laitteisto, verkko, verkkoasemat, tulostimet, lähestulkoon kaikki mikä vain on kytköksissä toimialueeseen tai voi olemassa olollaan vaikuttaa johonkin toiseen laitteeseen tai ominaisuuteen.

Pienellä testausympäristöllä vian selvitys on helpompaa, nopeampaa ja täsmällisempää kuin se että lähdettäisiin selvittämään koko organisaation laajuisesti, jolloin muuttujia olisi paljon enemmän. Mahdollinen ongelma voi aiheuttaa myös sen että koneimageet täytyisi tehdä uudelleen, jolloin tästä koituisi turhaa työtä käyttäjälle sekä ylläpitäjille, kun koneimage pitäisi asentaa koneisiin uudestaan.

Kun pilotointi on saatu valmiiksi, jatketaan toimialueen käyttöönottoa toimipaikka kerrallaan, jokaisen toimipaikka lisäyksen jälkeen kartoitetaan mahdolliset esiin tulleet ongelmat ja korjataan ne ennen siirtymistä uuteen. Näin ollen, mikäli vikoja vielä esiintyy, saadaan ne aina seuraavaan toimialueeseen siirryttäessä korjatuksi.

Testausaikatauluun vaikuttaa ympäristön laajuus, ylläpidon resurssit sekä huomiona se, että testausta suoritetaan muun ylläpidon ohessa.

4.2.3 Siirto uuteen

Uudet työasemat ovat varustettu Windows 7 -käyttöjärjestelmällä. Vanhat käytössä olevat Windows XP työasemat tullaan asentamaan uudelleen, Windows 7 -käyttöjärjestelmällä. Vanhoja Windows XP koneita ei siirretä uuteen domainiin, vaan aloitetaan tyhjältä pöydältä ja asennetaan koneet uudestaan.

Joissakin organisaatioyksiköissä käytetään Mac tietokoneita sekä niissä OS X käyttöjärjestelmää. Nämä organisaatioyksiköt tullaan uudistuksen ja uuden toimialueen myötä siirtämään samaan domainiin kuin Windows-käyttöjärjestelmälliset työasemat.

Henkilökunnalle viralliseen tiedottamiseen on varattu kaksi viikkoa aikaa, sitä ennen kuukautta aikaisemmin ilmoitetaan yksikön vastuuhenkilölle.

5 Projektin tuloksia

Vanhojen kokemusten perusteella tiedettiin, että projekti tulee olemaan kiireinen.

Projektin keskeisemmäksi tulokseksi saatiin kokemusten ja palautteen pohjalta, että

- Siirtymä oli onnistunut Kaupunki X:n ja Kaupunki Y:n välillä.
- Dokumentointi oli kattava ja selkeä.

- Dokumentointiani pystytään käyttämään oppaana, mikäli muita kaupunkeja tai kuntia liittyy Kaupunki X:n ja Kaupunki Y:n kanssa samaan opetusverkkoon.

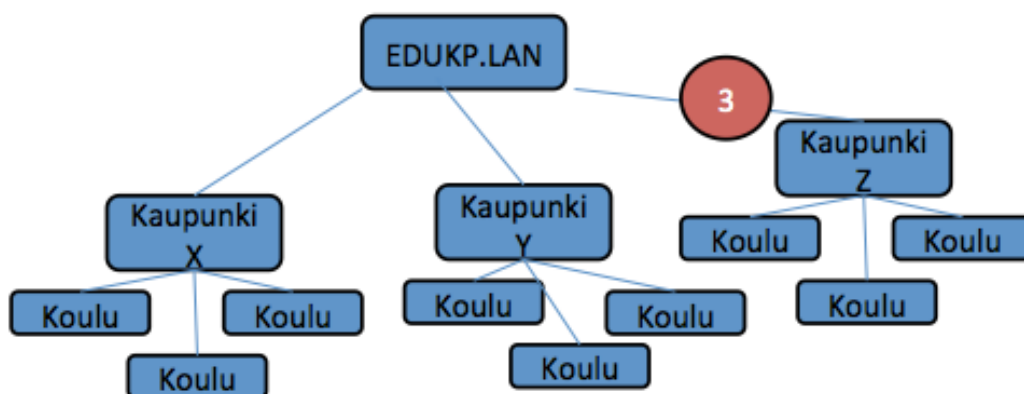
Tässä työssä käytetyt nimet ja IP-osoitteet eivät olleet turvallisuussyistä todenmukaisia. Kaupunki X:lle olen tehnyt kattavamman dokumentoinnin yksityiskohtineen ja nimineen.

Yleisinä haasteina projektissa oli oheislaitteiden, kuten tulostinten, toimiminen vaaditulla tavalla. Ongelmaksi koitui, kun käyttäjäryhmäkohtaisesti kohdistetut tulostimet eivät pysyneet määritettyinä ryhmän jäsenillä. Ongelmaksi nousivat esimerkiksi Aula-käyttäjien pakotetut profiilit ja niiden toimivuus. Käyttäjillä oli ongelmia verkkolevyjen kanssa, levyjaot eivät aina näkyneet tai pysyneet näkyvinä käyttäjillä.

Projekti vietiin loppuun resurssien puitteissa vastaamaan tarpeita ja odotuksia. Viimeinen kaupunki X:n asennettavista kouluista asennettiin tammikuussa 2012, neljä kuukautta aikataulusta jäljessä.

Viivästymisen syy oli laitepulassa, eli kouluilla ei ollut asennukseen sopivaa laitteistokantaa tarpeeksi laajalti, jotta asennusta olisi voitu tehdä. Viivästymiseen vaikutti se, että projektia tehtiin muiden ylläpitötöiden ohella.

Huolimatta aikataulumuutoksista ja vastoinkäymisistä tulee oppilasverkkoon liittymään vielä Kaupunki Z tammikuussa 2012 (kuvio 10).



Kuvio 10. Kaupunki Z:n liittyminen.

6 Pohdintaa

Tämä projekti on ollut laaja ja omia resursseni sitova. Projektin onnistuneeseen läpivientiin tarvittiin projektin alkuvaiheessa tehty työsuunnitelma ja valmentautuminen, toimeksiantajan tuki ja kannustus sekä suurimpana apuna dokumentoinnin kannalta auttaneet väliarviointit mentorini kanssa.

Projektin aiheen laajuus, työn rajaaminen ja turvallisuussyyt aiheuttivat minulle haastetta dokumentoinnin kannalta. Toimeksiantajani palaute Active Directoryn käyttöönotosta sekä käyttäjäytyytyväisyys toimi mittarina projektin onnistuneesta läpiviennistä. Projekti edesauttoi minun ammatillista kehittymistäni. Olen saanut varmuutta pitkäaikaisen ja muutoksia aikaansaavan projektin kirjaamiseen ja läpiviemiseen.

Kokonaistavoitteiden huolellinen pilkkominen osatavoitteisiin ja osa-alueisiin on ollut ratkaisevan tärkeää projektin eteenpäin viemisessä ja omassa jaksamisessa. Uuteen aiheeseen ja haasteeseen tarttumisen olen kokenut mielenkiintoiseksi. Projekti on antanut kokonaisnäemyksen projektiluontoisesta työskentelystä ja projektiin sisältyvistä työskentelytavoista sekä menetelmistä.

Projektin keskeisenä saavutuksena pidän kokemusta aiheesta, työskentelystä sekä varsinkin dokumentoinnista. Kokemuksena projektista opin, että työsuunnitelma tulee tehdä tarkasti, tarpeeksi pilkotusti ja miettiä kaikkia mahdollisia ongelmia sekä vastoinkäymisiä ennakkoon. Hankkeelle on myös varattava oma aika ja resurssija. Projektin edetessä nousi esiin tietotekniikan nopea kehittyminen sekä sen mahdollistaminen projektin vieminen seuraavalle asteelle.

Isot projektit, kuten tämäkin, poikii aina uusia ajatuksia ja mielenkiinnon kohteita, eikä tämä projekti ollut poikkeus. Yksi mielenkiintoinen jatko projekti voisi olla tässä selvitys siitä, miten vanha ja uusi eroavat sekä mitä hyötyjä saavutettiin siirtymällä uuteen.

Keskustelut mentorin kanssa ovat erittäin tärkeitä ja pidänkin niitä tämän työn selkärankana.

Lähteet

Casad, J & Willsey, B. 2011. TCP/IP Trainer. Suom. Salmela, J. Helsinki. IT Press.

Järvinen P. 2003. Salausmenetelmät. Porvoo. Docendo Finland.

Kivimäki, J. 2005. Windows Server 2003 Active Directory. Jyväskylä. Readme.fi

Kivimäki, J. 2009. Windows Server 2008 Tehokas hallinta. Hämeenlinna. Readme.fi

Kuviot

Kuvio 1. Kaupunki X:n opetusverkon verkkoympäristö ennen.....	9
Kuvio 2. Opetusverkon verkkoympäristö jälkeenpäin.	9
Kuvio 3. Uusi verkko ja luottosuhde vanhaan.	12
Kuvio 4. Replikointirakenne.	14
Kuvio 5. Luottosuhteet.	16
Kuvio 6. Ryhmäoikeudet.	17
Kuvio 7. Juuritoimialueen OU-rakenne.	19
Kuvio 8. Alitoimialueen OU-rakenne.	20
Kuvio 9. Luottosuhteet.	26
Kuvio 10. Kaupunki Z:n liittyminen.	28

Taulukot

Taulukko 1. Laiteobjektien nimeäminen	21
Taulukko 2. Malli ryhmäobjektiivien nimeämisestä.	22