Jari Larumo

WINDOWS 2003 PALVELIMEN KÄYTTÖÖNOTTO

Satakunnan ammattikorkeakoulu

Tietotekniikka

Tietoliikennetekniikka

2006

WINDOWS 2003 PALVELIMEN KÄYTTÖÖNOTTO

Larumo Jari Juhani
Satakunnan ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka
Syyskuu 2006
Ari Ekholm
UKK: 004.732, 004.725.5, 651
Sivumäärä: 53

Avainsanat: palvelimet, asennus, suunnitelmat, tietokoneet

Tämän työn tarkoituksena oli korvata yhdistyksen nykyisin käytössä oleva vertaisverkko palvelinpohjaisella verkolla. Lisäksi on pyritty huomioimaan sekä tietoturvallisuus että tiedostojen varmistukset. Lisäksi työssä on tarkoitus tutkia onko tiloissa tulevaisuudessa mahdollisuutta käyttää langatonta tiedonsiirtoa korvaamaan langallinen verkko.

Yksi suunnittelun lähtökohdista oli se, että palvelinverkon käyttö ei saa olla sen monimutkaisempaa kuin nykyisen vertaisverkon käyttö. Tämän seurauksena työhön tuli varsin runsaasti käyttöönottoon liittyvää koulutusta, jossa pääpaino oli peruskäytössä, kuinka tällaiseen palvelinpohjaiseen verkkoon kirjaudutaan, miten ja mistä käyttäjät löytävät omat tiedostonsa, miten tallennetaan palvelimelle omia tiedostoja yms.

Toinen vähintään yhtä tärkeä lähtökohta oli tietoturva ja varmistusten hallittu suorittaminen yhdestä kokonaisuudesta. Vertaisverkon tietoturva oli käytännössä mahdollisen katastrofin varalta heikko, koska verkossa ei ollut mitään varmistusta katastrofin varalta. Varmistusten hallittu tekeminen oli vertaisverkossa teoriassa mahdollista, mutta varmistettavat tiedostot olivat usealla eri koneella ja niiden varmuuskopiointi olisi vaatinut varmistuksen tekijältä kaikkien näiden koneiden läpikäyntiä. Tämäkään ei olisi antanut täyttä varmuutta siitä, että kaikki tarpeellinen tieto olisi tullut asianmukaisesti varmistettua.

IMPLEMENTATION OF WINDOWS 2003 SERVER

Larumo Jari Juhani
Satakunta University of Applied Sciences
Information Technology
Telecommunications
September 2006
Ari Ekholm
UKK: 004.732, 004.725.5, 651
Pages: 53

Keywords: server, installation, plan, computer

The purpose of this work was to replace a charitable association's peer to peer network with a server based network in which the aim was to pay close attention to both data security and data backup operations. In addition, the idea in this work is to study the possibilities to use wireless data transmission in the future.

One of the starting points of planning was that the use of this server based network must not be any more complicated than the present peer to peer network. As a result of that, this work had quite a lot of commissioning training where the main focus was in basic operations. This basic use contains ideas how to sign in the server based system, how and where the users find their files from the server and how to save files in it.

Another equally important point was data protection and controlled backup procedures from one point of operation for the data protection of the network at the moment was in practice quite weak because of lack of backup functions. Taking backups in peer to peer networks is possible in theory but when the files are in several computers around the area it is impossible to know for sure that everything has been backed up properly.

SISÄLLYSLUETTELO

1. LYHENTEET

BITS

Background Intelligent Transfer Service. Tiedostonsiirtoon käytettävä protokolla, joka hyödyntää muilta sovelluksilta vapaaksi jäävää kaistanleveyttä.

DES

Data Encryption Standard. Suosittu, symmetrinen salausmenetelmä, joka käyttää 56-bittistä avainta. DES pilkkoo salattavan tekstin 64:en bitin lohkoihin ja salaa ne erikseen.

DN

Distinguished Name. LDAP-hakemistoissa käytettävä nimeämismenetelmä, joka yksilöi objektin hakemistopuussa.

FQDN

Fully Qualified Domain Name. Verkkolaitteen täydellinen DNS-nimi, joka kertoo laitteen sijainnin verkossa.

GPO

Group Policy Object. Active Directoryn objekti, joka sisältää tietokoneisiin tai käyttäjiin kohdistuvia käytäntöasetuksia. GPO:t linkitetään tiettyihin säiliöobjekteihin, joiden alueella ne vaikuttavat.

GUID

Globally Unique Identifier. Muuttumaton ja yksilöllinen objektitunniste Active Directory-palvelussa.

LAN

Local Area Network. Lähiverkko on yleensä yhden organisaation sisäiset laitteet käsittävä.

LSA

Local Security Authority. Windows-suojausjärjestelmän osa, joka ottaa vastaan käyttäjän syöttämän käyttäjätunnuksen ja salasanan.

MMC

Microsoft Management Console.

Windows 2000/XP/2003 käyttöjärjestelmissä oleva käyttöliittymä, jolla voi suorittaa useita järjestelmän hallintatoimenpiteitä.

PDC/BDC

Primary/Backup Domain Controller. Windows NT-toimialueiden PDC palvelimet ylläpitävät NT4-hakemistotietokannan luku-/kirjoitusversiota ja monistavat hakemiston luettavan kopion BDC-palvelimille.

RDN

Relative Distinguished Name. LDAP-hakemistopalvelussa käytettävä nimitystapa, joka identifioi objektin tietyn varaston sisällä.

SID

Security Identifier. Windows-toimialueen objektin suojaus, joka koostuu kaikille objekteille ja tietokoneille yhteisestä alkuosasta ja yksilöllisestä RID-tunnisteesta.

RID

Relative Identifier. Suhteellinen tunnistenumero, joka tekee Windows toimialueen objektin SID-tunnisteesta yksilöllisen.

SAM

Security Accounts Manager. Windows käyttöjärjestelmän suojaustietokanta, jota käytetään asiakkaiden ensisijaiseen tunnistamiseen Windows NT:ssä.

TCP/IP

Transmission Control Protocol/Internet Protocol. Yleisesti lähiverkoissa liikennöintiin käytetty protokolla. TCP ohjaa datan lähetys- ja vastaanottoprosessia ja IP huolehtii tiedon välityksestä yhteydettömän verkon läpi reitittämällä.

WAN

Wide Area Network. Laajaverkko, joka yhdistää toisiinsa maantieteellisesti etäällä olevat lähiverkot.

WEP

Wired Equivalent Privacy. On ensimmäinen IEEE:n 802.11 standardiin perustuva työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.

WINS

Windows Internet Name Service. Varsinkin NT4-verkoissa käytetty nimenselvityspalvelu, jonka avulla voidaan selvittää NetBIOS-nimiä vastaavat IP-osoitteet.

WPA (Wi-Fi)

Wireless Fidelity Protected Access. On välivaiheen tietoturvatekniikka, joka kehitettiin WEP salauksen ongelmien paljastuttua oletettua vakavammiksi.

GLOBAL CATALOG

On puun tai metsän sisältämien objektien keskitetty säilytyspaikka.

GP

Group policy on joukko palvelimelle laadittuja active directoryn sääntöjä, jotka mahdollistavat automaattisen ja keskitetyn verkon koneiden ja käyttäjien hallinnan

GPO

Group Policy Object. Active Directoryn objekti, joka sisältää tietokoneisiin tai käyttäjiin kohdistuvia käytäntöasetuksia. GPO:t linkitetään tiettyihin säiliöobjekteihin, joiden alueella ne vaikuttavat.

SHEMA

sisältää määritykset AD:n sisällöstä ja rakenteesta.

WSUS

Microsoft Software Update Services on ohjelmisto, jolla hallitaan päivitysten asennusta ja hakua.

WEP

Wired Equivalent Privacy. On ensimmäinen IEEE:n 802.11 standardiin perustuva työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.

WINS (WINDOWS INTERNET NAMINNG SERVICE)

Windows Internet Name Service. Varsinkin NT4-verkoissa käytetty nimenselvityspalvelu, jonka avulla voidaan selvittää NetBIOS-nimiä vastaavat IP-osoitteet. WINS on microsoftin vastine NetBIOS:lle.

WPA

(Wi-Fi) Wireless Fidelity Protected Access. On välivaiheen tietoturvatekniikka, joka kehitettiin WEP salauksen ongelmien paljastuttua oletettua vakavammiksi.

RAID

RAID on tekniikkaa, jolla tietokoneiden kiintolevyjen hakunopeutta ja vikasietoisuutta parannetaan käyttäen useita kiintolevyjä, jotka yhdistetään joko ohjelmallisesti tai ohjainkortilla yhdeksi tai useammaksi levyksi.

Kts. http://fi.wikipedia.org/wiki/RAID

2. ESIPUHE

Tämän työn tarkoituksena oli korvata yhdistyksen nykyisin käytössä oleva vertaisverkko palvelinpohjaisella verkolla, jossa on pyritty huomioimaan sekä tietoturvallisuus että tiedostojen varmistukset. Lisäksi työssä oli tarkoitus tutkia onko tiloissa tulevaisuudessa mahdollisuutta käyttää langatonta tiedonsiirtoa korvaamaan langallinen verkko.

Yhdistyksessä aiemmin käytetyn vertaisverkon historia juontaa siitä ajatuksesta, että sen laajentamisen ja ylläpidon tulee olla helppoa ja yksinkertaista. Tästä syystä yhdistykseen oli päätetty alkujaan rakentaa tietoliikenneverkko mahdollisimman helpolla. Muutosta nykyiseen verkkoon haluttiin, koska haluttiin nostaa verkon turvallisuutta sekä helpottaa varmistusten tekoa.

Yksi suunnittelun lähtökohdista oli se että, palvelinverkon käyttö ei saa olla sen monimutkaisempaa kuin nykyisen vertaisverkon käyttö. Tämän seurauksena työhön tuli varsin runsaasti käyttöönottoon liittyvää koulutusta. Koulutuksen pääpaino oli peruskäytössä eli kuinka tällaiseen palvelinpohjaiseen verkkoon kirjaudutaan, miten ja mistä käyttäjät löytävät omat tiedostonsa, miten tallennetaan palvelimelle omia tiedostoja yms.

Toinen vähintään yhtä tärkeä lähtökohta oli tietoturva ja varmistusten hallittu suorittaminen yhdestä kokonaisuudesta. Verkon senhetkinen tietoturva oli käytännössä mahdollisen katastrofin varalta heikko, koska verkossa ei ollut mitään varmistusta katastrofin varalta. Varmistusten hallittu tekeminen on vertaisverkossa teoriassa mahdollista, mutta varmistettavien tiedostojen ollessa useilla eri koneilla niiden varmuuskopiointi olisi vaatinut varmistuksen tekijältä kaikkien koneiden läpikäymistä. Tällöinkään ei olisi ollut täyttä varmuutta siitä, että kaikki tarpeellinen tieto olisi tullut varmistettua.

3. TARJOUSPYYNNÖT

Tarjouspyynnöissä lähtökohtina olivat seuraavat seikat:

- hankkia riittävän tehokas palvelin, jonka kapasiteetti sekä riittäisi nykyiselle käyttäjämäärälle että sisältäisi mahdollisuuden kasvattaa palvelimen käyttäjäkuntaa ilman suuria investointeja laitteistoon.
- Lisäksi palvelimeen haluttiin mahdollisuus varmistaa tiedot, jotka ovat yhdistyksen kannalta tärkeitä tai vaikeasti korvattavissa.
- Käyttövarmuus ja luotettavuus
- Laitteiston yhteensopivuus palvelinohjelmiston kanssa

Näillä pohjatiedoilla määrittelin palvelimen perusmäärityksiksi seuraavat seikat:

- Soveltuvuus Windows 2003 palvelinohjelmistolle
- Intel / AMD prosessori noin 3 GHz
- Palvelinkäyttöön soveltuvat kiintolevy, piirilevy sekä virtalähde
- Fyysistä muistia 1 Gt
- Levykapasiteettiä vähintään 100 Gt
- Vähintään RAID 5
- Vähintään kaksi verkkoliityntää (sisä- & ulkoverkkoliitynnät)
- Varmistusaseman kapasiteetiksi pakkaamattomana vähintään 36 Gt

Tarjouspyynnöt lähetettiin yrityksille huhti- toukokuun vaihteessa ja vastauksia pyydettiin toukokuun 15. päivään mennessä takaisin.

Tarjouksista suurimmassa osassa oli otettu huomioon varsin hyvin kaikki edellä mainitut minimivaatimukset, joskin varmistusaseman kohdalla oli hajontaa siinä millaista asemaa tarjottiin. Yhdessä oli Iomegan Zip asema ja muissa oli eri versioita nauhavarmistusasemasta. Näiden nauhavarmistusasemien kokohaitari oli pakkaamattomana luok-

kaa 36 Gt:sta tuonne 72 Gt:uun. Osassa tarjouksia oli nauhavarmistusasema sisällytetty suoraan palvelimen hintaan ja joissakin se oli lisälaitteena erillishintaan.

Saaduista tarjouksista parhaiten tarpeita vastasi tarjous, jossa prosessorina oli Intelin 3.2 GHz:in Pentium 4, muistia oli 1024 Mt, levykapasiteettia 200 Gt, RAID varmistuksena 5+10 ja 36/72 Gt:n nauhavarmistusasema. Tämän parhaan tarjouksen tehneen yrityksen kanssa yhdistys päätti jatkaa neuvotteluita parhaan lopputuloksen saavuttamiseksi. Neuvotteluiden lopputuloksena yhdistys päätti hankkia palvelimen tarjouksen pohjalta.

4. ALKUHAVAINTOJA

Tutkiessani senhetkistä järjestelmää ensimmäisiä huomionani oli se että, kaikki käyttäjät olivat järjestelmänvalvojina. Kysyessäni syytä tähän kysyessäni sain vastauksen että, näin he pystyvät käyttämään mitä tietokonetta/kirjoitinta he haluavat. Tätä seikkaa ihmettelin suuresti, sillä se, että pystyykö käyttämään jotakin tietokonetta vai ei, riippuu käyttäjän oikeuksista ainoastaan silloin, kun tämä haluaa asentaa tietokoneeseen uusia ohjelmia. Käyttäjä pystyy rajoitetuin käyttäjän oikeuksin kyllä käyttämään tietokoneeseen asennettuja ohjelmia ja oheislaitteita, mutta niiden lisääminen useimmiten vaatii järjestelmänvalvojan oikeudet.

Lisähuomioista ensimmäinen oli se, että kukin kirjoitin oli jaettu verkkoon paikallisesti, joka vaikeutti sisäverkon käyttöä muuhun. Mikäli joku käyttäjä halusi tulostaa jaetulle kirjoittimelle, joka oli toisen käyttäjän tietokoneeseen asennettu, niin hänen tulostuksensa täytyi ensin saada verkon läpi. Tämän jälkeen kirjoittimen täytyi vielä palauttaa ilmoitus työn valmistumisesta käyttäjälle. Tämä edestakainen liikenne kuormitti verkkoa varsin runsaasti, joten verkon käyttö oli varsin hidasta.

Seuraava asiana johon kiinnitin huomion oli se, että senhetkinen verkko oli ns. vertaisverkko, jossa sisäverkon kaikki liikenne kiersi varsin ruuhkaisen kytkimen kautta. Tällainen tiedostojenjakopolitiikka on varsin sekavaa ja vaikeasti hallinnoitavaa, koska tie-

dostot ovat sekaisin monella tietokoneella. Tämän seurauksena niiden etsintään kuluu tarpeettomasti aikaa ja se on jokaiselle henkilölle varsin vaivalloista.

Tähän kytkimeen oli lisäksi kytketty palveluntarjoajalle lähtevä yhteys ilman, että sisäverkon ja ulkoverkon välissä olisi mitään, mikä estäisi tunkeutumisen sisäverkkoon. Verkon tietoturva oli siis ainoastaan palveluntarjoajan hallinnoiman ja valvoman palomuurilaitteen varassa, mikä ei ole tietoturvan kannalta paras ratkaisu. Halusin kiinnittää heidän huomionsa tähän, sillä mikäli joku onnistuu tunkeutua palomuurin läpi palveluntarjoajan verkkoon, tällöin heidän verkkonsa olisi tämän tunkeutujan käytettävissä verkon kaikkine resursseineen. Tällöin kaikki heidän tiedostonsa olisivat hyökkääjän käytettävissä, miten tämä niitä haluaisi käyttää. Tähän ongelmaan toisi ratkaisun erillinen palomuurilaite, jossa olisi rajoitettu liikennettä molempiin suuntiin erilaisin säännöin ja rajoituksin.

Ennen varsinaista järjestelmän suunnittelua kävin tutustumassa senhetkisen järjestelmän ominaisuuksiin ja mahdollisuuksiin. Lisäksi pyysin käyttäjiä kertomaan, mitä he odottavat tältä uudelta järjestelmältä. Heidän palautteensa oli toivomus helposti käytettävästä verkosta. Näin heillä ei olisi tarvetta miettiä, missä mikäkin tiedosto on vaan, että ne löytyisivät helposti ja nopeasti mahdollisesti vain yhdestä paikasta. Itse kerroin omia ajatuksiani millaiseksi olin itse ajatellut uuden järjestelmän. Tämän keskustelun seurauksena päädyttiin ratkaisuun, jossa kullekin käyttäjälle palvelimelle suunniteltiin hakemistot yleisille tiedostoille, koulutuskäyttöön sekä yhdistyksen omalle lehdelle.

5. ACTIVE DIRECTORY (AD)

AD on integroitu DNS:ään seuraavilla kolmella linkityksellä:

- molemmat käyttävät samaa hierarkkista järjestelmää.
- AD voi säilyttää DNS alueet
- AD käyttää DNS:ää selvittäessään AD:n toimipaikkoja, palveluiden nimiä sekä toimialueiden nimiä IP osoitteiksi

Vaikka AD on integroitu DNS:ään, niin niillä on muutamia tärkeitä eroavuuksia, joista tärkeimmät ovat seuraavat:

- DNS on nimipalvelin, joka muuntaa IP osoitteet helpommin muistettaviksi luettaviksi osoitteiksi ja myös toisinpäin
- AD on hakemistopalvelu, joka tuottaa tallennuspaikan tiedolle, jota voivat käyttää niin käyttäjät kuin sovellutuksetkin.

Active Directoryn ensisijainen tehtävä on olla verkon resurssien tallennuspaikka. Windows 2000 sekatila ja natiivitila ovat käytössä jo Windows 2000:sen AD:ssä. Sekatilassa AD tarjoaa tuen kaikille versioille Windows NT:stä alkaen ja käytössä ovat AD:n perusominaisuudet. Tätä tilaa käytetään, jos halutaan AD:n ohjauspalvelimen välittävän tietoja NT4 palvelimelle ja NT4:n välittävän omia tietojaan takaisin toimialueen sisältäessä sekä Windows 2000 että NT4 palvelimia. Sekatilassa aiempien Windows versioiden koneet käyttävät järjestelmää ikään kuin olisivat osa NT4 toimialuetta, mikäli niissä ei ole AD client ohjelmistoa asennettuna. Myös NT4-työasemat ja palvelimet toimivat, kuten normaalisti toimisivat NT4 toimialueella.

Natiivitilassa Windows 2000:n AD tukee ainoastaan Windows 2000 ja 2003 palvelimia ja työasemia, jolloin toimialueella saadaan käyttöön kehittyneempiä ominaisuuksia, kuten universaalit ryhmät, sisäkkäiset ryhmät, ja ryhmätyypin muunnokset. Otettaessa natiivitila käyttöön, menetetään samalla tuki sille, että Windows 2003 palvelimet pystyisivät välittämään tietoja vanhemmille palvelimille.

Windows Server 2003 tila on Windows Server 2003:en uusia ominaisuuksia. Mikäli halutaan päästä tähän tilaan eli Windows Server 2003 tilaan, ei käytössä saa olla muita kuin Windows Server 2003 palvelimia. Tässä tilassa on mahdollista ottaa käyttöön kaikki AD:n uudet ominaisuudet. Näitä ovat Windows 2000 natiivitilan ominaisuuksien lisäksi esim. helpompi toimialueen ohjauskoneiden uudelleennimeäminen ja kirjautumisleimojen päivitys. Mikäli verkossa on Windows 2000 ohjauspalvelimia, on sekä metsän että toimialueen laitteiden tuettava Windows Server 2003 -tilaa ennen sen käyttöönottoa.

Active Directoryn toimintatasot

Ohjauspalvelimet	
Windows 2000 mixed	Kaikki ohjauspalvelimet
Windows 2000 native	Windows 2000 ja 2003
Windows Server 2003 interim	Windows NT ja 2003
Windows Server 2003	Windows Server 2003

AD metsä voi toimia jossakin kolmesta tilasta. Nämä tilat ovat Windows 2000, Windows Server 2003 interim ja Windows Server 2003, joka on metsän toimintatiloista eniten verkon laitteilta vaativa tila. Harkittaessa metsän tason nostamista ylemmille tasoille, tulee kaikkien toimialueiden olla Windows 2000 natiivi- tai Windows Server 2003 -tasolla.

Metsän tasojen suhteen sallitut käyttöjärjestelmäversiot ovat samat kuin toimialueiden tapauksessa, mutta toimintoihin tulee muutoksia. Windows 2000 tilassa toimiva metsä käyttää oletusominaisuuksia, mutta noustaessa 2003 interim tasolle saadaan niiden lisäksi käyttöön 13 lisätoimintoa yleiseen hakemistoon. Myös hakemiston replikointitoiminta tehostuu, koska käyttöön saadaan LVR (linked-valued replication) replikointi - ja parannetut replikointialgoritmit. LVR replikointi tarkoittaa sitä, että objektien arvojen muutokset siirretään arvo kerrallaan tietokantaan. Tällöin vältetään myös tehtyjen muutosten katoaminen siinä tilanteessa, että kaksi ohjauspalvelinta suorittaa muutoksia samaan hakemistoon samanaikaisesti. Windows Server 2003 tilassa ollessaan metsässä ei voi olla enää muita kuin 2003 palvelimia.

Kun AD asennetaan uuden metsän ensimmäiseen ohjauspalvelimeen, eli ensimmäisen toimialuepuun juuripalvelimeen, tämä palvelin saa kaikki palvelinroolit automaattisesti. Asennettaessa uusia palvelimia olemassa olevalle toimialueelle, eivät nämä uudet palvelimet saa mitään palvelinrooleja ilman käyttäjän toimenpiteitä. Kun toimialueelle lisätään uusi alitoimialue, sen ensimmäiselle ohjauspalvelimelle asentuu PDC emulaattori, RID Master ja Infrastructure Master roolit. Lisättäessä uudelle alitoimialueelle ohjauspalvelimia on tilanne roolien suhteen sama kuin puun juuritoimialueella eli palvelinrooleja ei automaattisesti asenneta uusille palvelimille. Jos taas metsään lisätään uusi

toimialuepuu, saa senkin ensimmäinen ohjauspalvelin vain osan toimialuekohtaisista rooleista. Vaikka global catalog rooli voikin olla jaettuna metsään useammalle palvelimelle, ei metsässä oletuksena ole kuin yksi tätä tehtävää hoitava palvelin. Tämä on kaikkein ensimmäisenä asennettu palvelin ylimmän toimialuepuun juuressa.

5.1. DNS

DNS palvelu on yksi tärkeimmistä palveluista mitä tulee AD:n toimintaan. Se on jopa niin tärkeä, että se tulee ottaa käyttöön palvelimessa jo ennen palvelimen korottamista ohjauspalvelimeksi tai AD:n käyttöönottoa. DNS palvelu voidaan asentaa Manage Your Server automaattitoiminnon avulla tai avaamalla ohjauspaneelin lisää tai poista ohjelmia (Add or Remove Programs) osa, josta valitaan Add/Remove Windows Components. DNS palvelu löytyy muiden verkkopalveluosien tavoin Networking Services kohdan alta. Kun itse DNS palvelu on asennettu, päästään määrittämään palvelun asetukset, jotka riippuvat siitä, mihin tilaan DNS palvelin asennetaan. DNS hallintakonsoli löytyy palvelimen Administrative tools kansiosta. Ensimmäisessä vaiheessa määritetään palvelimen omat asetukset kuntoon. Näitä asetuksia päästään tutkimaan pikavalikosta, joka saadaan esiin palvelimen nimen päällä klikkaamalla. Ensin määritetään palvelimelle Internetin juuritoimialuetta ylläpitävät palvelinosoitteet, joilta kysytään nimenselvitystietoja, mikäli paikallisella palvelimella ei ole osoitteista tietoa. Näiden osoitteet määritetään klikkaamalla hiiren oikealla napilla palvelimen nimen päällä ja valitsemalla valikosta Configure a DNS Server. Aukeavasta valikosta valitaan Configure root hints only ja viedään automaattitoiminto loppuun ohjeiden mukaan.

AD metsän palvelimille voidaan määrittää myös forwarders osoitteita. Nämä osoitteet ovat niiden DNS palvelinten osoitteita, jotka toimittavat DNS palvelimen toiminnot nimikyselyissä, vapauttaen paikallisen palvelimen koko nimenselvitysprosessista. Kaikkien alitoimialueiden nimipalvelimet käyttävät puolestaan forwarder ominaisuudessa AD toimialuepuun juuripalvelimia. Jokaisella toimialueella AD:ssä tulisi mielellään olla vähintään kaksi DNS palvelinta. Näille olisi määritettävä DNS palvelun toiminnan takaamiseksi DNS vyöhykkeet, jotka vastaavat kyseessä olevaa toimialuetta. Vyöhyketiedostot ovat tässä tapauksessa pakolliset, koska AD:ssä jokaisen toimialueen nimipalvelimen on pystyttävä vastaamaan omista DNS vyöhykkeistään, eli pystyvän vastaamaan toimialueensa lähteviin /saapuviin nimenselvityspyyntöihin. Lisäksi tämä

on myös välttämätöntä siksi, että asiakaskoneet löytäisivät toimipaikkatiedot, ohjauspalvelimet ja kaikki eri palvelimilla sijaitsevat palvelut, joista tiedotetaan DNS palvelussa. Jokaisen DNS palvelimen kohdalla on DNS hallintakonsolissa näkyvissä kaksi hakemistoa, jotka ovat normaalin ja käänteisen nimenselvityksen vyöhykkeille tarkoitetut. AD integroiduille vyöhykkeille voidaan määrittää myös replikointikäytäntö, joka hyödyntää Active Directoryn uutta sovelluspartitio ominaisuutta.

Tällöin DNS tietojen replikointi voidaan määrittää siten, että se saadaan kohdistettua vain sille osalle palvelimia, joille se on tarkoitettu. DNS tietojen suhteen politiikka voidaan määrittää sellaiseksi, että DNS palvelimet replikoivat tiedot vain niitä tarvitseville toimialueen ohjauspalvelimille, riippumatta siitä, ovatko ne DNS palvelimia vai ei. Tällöin voidaan varmentaa DNS tietojen säilyminen.

5.2. GLOBAL CATALOG (GC)

Yleinen luettelopalvelu, eli GC palvelu on toimialueen ohjauspalvelimista se, joka muistaa ja samalla ylläpitää kaikkien metsän objektien kattavaa luetteloa. GC on tärkeässä asemassa kaikissa tilanteissa, joissa on tarpeen selvittää jonkin tietyn objektin mahdollinen sijainti metsässä. Tämän luettelon luominen tapahtuu automaattisesti siinä vaiheessa, kun AD replikoidaan. Kuten kaikki ohjauspalvelimet, myös GC palvelin ylläpitää tietojansa oman toimialueensa hakemistoista. Tämä GC:n ominaisuus aiheuttaa tästä syystä palvelimelle lisäkuormaa. Tämä lisäkuorma aiheutuu siitä että, se ylläpitää täydellisen luettelon lisäksi myös osittaista lukumuodossa olevaa versiota oman toimialueensa ja kaikkien metsän muiden toimialueiden hakemistotietokannoista. GC:iin on tallennettuna objekteista ainoastaan niiden yleisimmin käytetyt hakukriteerit, attribuutit ja ne määritteet, joilla voidaan paikallistaa objektin täydellinen kopio metsässä. GC palvelin on apuna käyttäjien tunnistamisessa siinä tapauksessa, että tunnistuspyynnön vastaanottavalla ohjauspalvelimella ei ole tietoa kirjautuvan käyttäjän UPN nimestä.

Mikäli toimialueen taso on vähintään Windows 2000 natiivi, eivät käyttäjät, jotka eivät ole toimialueensa Domain Admins -ryhmän jäseniä, eivät pysty kirjautumaan toimialueelle, mikäli GC ei ole käytettävissä. Tämän aiheuttaa se, että käyttäjän yrittäessä kirjautua toimialueelle, niin tällöin tietokone joutuu tarkistamaan myös käyttäjän uni-

versaalin ryhmäjäsenyyden. Mikäli tätä ei tapahtuisi, käyttäjällä saattaisi olla mahdollista päästä tutkimaan sellaisia tietoja/resursseja, joihin universaalin ryhmän jäsenellä ei ole oikeuksia käyttää. Universaaleilla ryhmillä tarkoitetaan ryhmiä, joihin voidaan lisätä jäseniä eri toimialueiden alueelta. Nämä universaalit ryhmäjäsenyydet ovat ainoastaan GC palvelinten tiedossa. Universaalit ryhmät voidaan kuitenkin ottaa paikallisesti käyttöön määrittelemällä toimipaikassa asetus Enable Universal Group Membership Caching. Mikäli universaalit ryhmät eivät ole paikallisessa käytössä, voivat käyttäjät kuitenkin kirjautua toimialueelle, jos he ovat kirjautuneet sisään jo kerran aiemmin. Tästä seuraa ongelmia varsinkin sellaisissa ympäristössä, joissa käytetään sekä vanhoja että uusia versioita Windowsista, koska tiedosto/resurssikohtainen käyttöoikeus ratkaistaan käyttöjärjestelmä-/tapauskohtaisesti ja tunnistusmenetelmä saattaa vaihdella eri kerroilla. (Stanek)

5.3. DOMAIN CONTROLLER

Ohjauspalvelimen tehtävänä on tarjota AD:n avulla hakemisto-, käyttäjien sisäänkirjautumis-, autentikointipalvelut. Jokaisessa toimialueessa tulee olla yksi tai useampi ohjauspalvelin. Toimialueen ensimmäisestä ohjauspalvelimesta tulee toimialueen juuripalvelin, jolle tulee määrittää DNS nimi & IP osoite sekä NETBIOS nimi. (Tämä on käytössä tietokoneissa, joissa on käytössä joko windows ME tai sitä vanhempi käyttöjärjestelmä).

5.4. GROUP POLICY (GP)

Group policy on joukko palvelimelle laadittuja sääntöjä, jotka mahdollistavat automaattisen ja keskitetyn verkon koneiden ja käyttäjien hallinnan. Näillä asetuksilla hallitaan sekä käyttäjiä että tietokoneita. Näitä käytäntöjä pystytään määrittämään kerralla joko useisiin tai yksittäisiin toimialueisiin, toimialueen organisaatioryhmiin tai paikallisiin järjestelmiin. Paikalliset käytännöt tallennetaan vain paikalliseen tietokoneeseen, kun taas palvelimen käytännöt linkitetään aktiivihakemistopalvelun objekteiksi, joita puolestaan voidaan edelleen linkittää paikallisiksi.

Windows 2003 tarjoaa monia käytäntöjä, jotka toimivat ainoastaan Windows 2000:ssa tai sitä uudemmissa Microsoftin käyttöjärjestelmissä. Uusien käyttöjärjestelmien myötä

mahdollisten käytäntöasetusten määrä on kasvanut, mutta tämä on samalla lisännyt yhteensopivuusongelmia eri käyttöjärjestelmien välille. Vanhempien versioiden käytännöt ovat yhteensopivia ylöspäin, mutta eräitä uusimpia asetuksia ei pysty käyttämään kuin Windows 2000:ssa tai sitä uudemmissa käyttöjärjestelmissä.

Siirryttäessä Windows Server 2003:een ja sen myötä uudempiin käyttöjärjestelmiin työasemissa, saadaan käyttöön nykyistä tehokkaammat ja keskitetymmät hallintamahdollisuudet. Windows Server 2003 järjestelmän eri käytäntöjä ei enää tarvitse erikseen määrittää jokaisessa yksittäisessä työasemassa, vaan ne voidaan määrittää keskitetysti yhdessä paikassa. Käytännöt tallennetaan group policy objekteiksi, jotka ovat asetusten ja määritysten säilytyspaikkoja. Toimipaikat, toimialueet ja organisaatioyksiköt eivät ole sidottuja yhteen yksittäiseen group policy objektiin, vaan niitä voidaan linkittää useampia yhteen ja samaan AD:n osaan. Vastaavasti myös yhden group policy:n linkittäminen moneen paikkaan on mahdollista. Tässä tapauksessa tehdyt muutokset tulevat voimaan kaikissa niissä AD:n osissa, joihin objekti on kytketty. Koska käytännöt ovat objekteiksi tallennettuja, pätevät niihin samat olioajattelun suuret ajatukset kuin muihinkin vastaaviin oliopohjaisiin järjestelmiin, esim. äiti-lapsisuhteet ja periytyminen. AD:n group policy objektin asetukset siirtyvät ylhäältä alaspäin siten, **että ensin sovelletaan toimialueen, sitten palvelinjoukon ja lopulta organisaatioyksikön käytäntöjä.** Tähän tulevat vielä lisäksi Windows NT4:n käytännöt ja paikallisten järjestelmien käytännöt, joita sovelletaan käyttöön kaikkein ensimmäisinä ja mainitussa järjestyksessä, jotka samalla ovat myös kaikista heikoimmat käytännöt.

Käytännöt periytyvät aktiivihakemistossa alaspäin tietyin rajoituksin. Mutta koska organisaatioyksiköiden tasolla määritetyt käytännöt astuvat voimaan viimeisenä, ne muuttavat toimipaikkojen ja toimialueiden käytäntöjen määritykset sellaisten sääntöjen osalta, jotka eroavat AD:n ylemmillä tasoilla määritettyjen asetusten määrityksistä siten, että viimeksi määritetyt käytännöt jäävät voimaan. Eli mikäli toimialueen käytännössä on otettu käyttöön jokin tietty asetus, niin tämä asetus tulee voimaan myös organisaatioyksiköissä, ellei kyseistä asetusta ole määritelty organisaatioyksikön käytännössä muulla tavoin. Tätä ehtoa pystytään kuitenkin muuttamaan, koska alemmilla objekteilla voidaan ottaa käyttöön ehto, jolla estetään tiettyjen käytäntöjen periytymisen ylempää. Tietyn kaltaiset käytännöt saatetaan kuitenkin haluta pakottaa käyttöön kaikissa toimipaikan toimialueissa tai toimialueen organisaatioyksiköissä. Tällöin on mahdollisuus mää-

rittää ylemmän tason group policy objektille ominaisuus, joka pakottaa alemmilta objekteilta perimään ylemmän objektin asetukset eroavuuksista riippumatta

5.5. ACTIVE DIRECTORYN MÄÄRITYKSET

Kun DNS-palvelu on otettu käyttöön ja sen asetukset on määritetty, voidaan palvelimella ajaa dcpromo.exe, joka ylentää palvelimen Active Directorya ylläpitäväksi ohjauspalvelimeksi. Active Directoryssa luottosuhteita luodaan Active Directory Domains and Trusts -konsolissa ja luontiprosessi on samantyylinen automaatin avulla tapahtuva prosessi kuin NT4-palvelimilla. Luottosuhteille täytyy määrittää salasana ja Active Directoryn tapauksessa valita vielä, onko luottosuhteen kautta tapahtuva valtuutus valikoiva vai koko toimialueen laajuinen.

6. VARMUUSKOPIOINTI

Ehkä tärkeimpiä kohtia, mitä varmuuskopioinnin suunnittelussa tulee ottaa huomioon ovat seuraavat seikat:

- mitä kopioidaan ja kuinka usein kopiointi suoritetaan
- minkälaista laitetta käytetään
- paljonko on aikaa varmuuskopioinnin tekemiseen
- minkä tyyppistä varmistusta käytetään

Nämä seikat siksi, että mikäli on tarvetta varmistaa suuria tiedostomääriä, niin niiden varmistamiseen/palauttamiseen menee aina oma aikansa ja jos niihin tehdään muutoksia varmistuksen ollessa käynnissä, niin varmistusohjelma ei voi luotettavasti tarkistaa onko tiedosto kopioitunut oikein. Mikäli tiedostoja on runsaasti, on parempi osittaa varmistus pienempiin osiin ja näin lyhentää siihen kuluvaa aikaa. Se milloin on paras aika suorittaa varmuuskopiointi, taas riippuu siitä milloin tähän on eniten aikaa.

Mediasta taas riippuu kuinka nopeasti varmistetut tiedostot on mahdollista saada takaisin käyttöön. Mahdollisia tallennusmedioita ovat erilaiset nauhavarmistusasemat, MO levyt, ZIP asemat sekä CD/DVD levyt. Todella tärkeät tiedostot tulisi varmistaa sekä CD/DVD levyille että nauhalle, koska magneettisten medioiden tiedot kärsivät / tuhoutuvat, jos tällainen media joutuu voimakkaaseen magneettikenttään pitkäksi aikaa.

Median koosta taas riippuu, minkä verran yhdelle medialle pystytään varmistamaan käyttäjien tiedostoja. Tämä rajoitus tullee vastaan siinä vaiheessa, kun käyttäjien enemmistö on havainnut palvelimella olevien tiedostojen edut verrattuna siihen, että etsisivät tiedostojaan ympäri verkkoa olevista tietokoneista.

Se, mitä varmistetaan riippuu siitä, mitkä tiedostot halutaan olevan käytettävissä mahdollisen onnettomuuden tai vahingon jälkeen. Tälläisiä tiedostoja voivat olla esim. käyttäjien työtiedostot sekä joidenkin ohjelmistojen tiedostot. Lisäksi tulee huomioida se seikka, että kuinka usein ko. tiedostot varmistetaan ja millä menetelmällä ne varmistetaan. Vaihtoehtoja ovat ainakin seuraavat tavat:

- full backup (täysi varmistus)
- differential backup (eroava varmistus)
- incremential backup (lisäävä varmistus)
- daily backup (päivittäinen varmistus)
- normal backup (normaali varmistus)

Differential ja incremential/daily tapojen eroavuus on siinä, että haluttaessa palauttaa tiedostoja niin differential varmistuksen palautus on helpompi tehdä, koska siinä palautetaan ensin viimeisin täysi varmistus, jonka jälkeen palautetaan viimeisin differential varmistus. Incremential ja daily tavalla taas on ensin palautettava viimeisin täysi varmistus ja sen jälkeen kaikki sen jälkeen otetut varmistukset.

Varsinainen varmuuskopiointi päätettiin suorittaa palvelinohjelmiston omalla varmistusohjelmalla. Varmistukset tehdään kerran viikossa siten, että joka perjantai varmistetaan kaikkien käyttäjien henkilökohtaiset hakemistot, molemmat yleiset hakemistot, järjestelmän tilan (sisältäen AD:n ja DNS:n tietokannat, tietokoneen rekisterit, käynnis-

tystiedostot, sysvol hakemiston sekä sertifikaattien tietokannat) sekä asennettujen ohjelmien tiedostot. Varmistusasemana käytetään nauhavarmistusasemaa, joka oli alkuperäisessä suunnitelmassani ensimmäinen vaihtoehto, koska sen käyttö on yksinkertaisinta ja varminta.

Järjestelmän varmistus aloitetaan kello 22 ja tästä lähetetään ilmoitus sähköpostitse järjestelmää ylläpitävälle henkilölle. Samoin lähtee ilmoitus kaikista virheistä järjestelmää ylläpitävälle henkilölle, jotta mahdollisen virheen tapahtuessa siitä olisi tieto käytettävissä heti, eikä vasta kun olisi tarvetta palauttaa jokin tiedosto epäonnistuneesta varmistuksesta.

7. LANGATON LÄHIVERKKO

Langaton lähiverkko toimii käytännössä samoin kuin tavallinenkin lähiverkko, mutta työasemat liitetään siihen langattomasti. Langattomassa lähiverkossa tiedonsiirto tapahtuu ilmatiellä yleensä radioteitse, eikä kaapeleita pitkin, kuten tavallisessa lähiverkossa. Langattomassa lähiverkossa ei siis tarvita mitään kaapelointia, vaan siinä on kuljetustienä ilma. Langattomassa lähiverkossa tietokoneet keskustelevat keskenään käyttäen apunaan erilaisia tekniikoita kuten, mikroaaltoja, infrapuna-aaltoja tai radioaaltoja. Langaton lähiverkko voi koostua pelkistä langattomilla verkkokorteilla varustetuista työasemista tai sitten työasemat voivat olla langattomasti yhteydessä langalliseen lähiverkkoon langattoman tukiaseman kautta.

Langattoman lähiverkon edut tulevat esille viimeistään silloin kun lähiverkko kasvaa, koska uusien koneiden liittäminen verkkoon on suhteellisen yksinkertaista ja helppoa, sillä tällöin ei tarvitse vetää kaapelointeja eikä suunnitella sitä mihin kaapelointi sijoitetaan. Tässä yhteydessä on kuitenkin muistettava langattoman verkon suojaukset, jotta ulkopuoliset eivät pääsisi käyttämään langatonta lähiverkkoa ilman lupaa. Langattomuus säästää sekä rahaa että aikaa, mutta käyttöönotossa on hyvä muistaa se seikka että, näihin laitteisiin ei yleensä ole asetettu turvallisimpia asetuksia oletuksena. Koska langattomat verkot ovat yleensä nopeita suunnitella, rakentaa että ylläpitää niin niillä lienee

hyvät mahdollisuudet kasvaa hyvinkin ripeästi. Ne langattomat lähiverkot, jotka käyttävät radiorajapintaa, muodostetaan tukiasemilla. Näiden tukiasemien välinen etäisyys riippuu sekä käyttäjien määrästä että maastosta. Verkkoon liitettäviin tietokoneisiin asennetaan langattomat verkkokortit, joiden avulla koneesta saadaan yhteys verkkoon. Lähiverkkoon pystytään liittämään tietokoneita lähes rajattomasti, sillä edes verkon ruuhkautuminen ole iso ongelma, koska sitä pystytään hallitsemaan lisäämällä tukiasemia tarpeen ilmaantuessa. Langattomien lähiverkkojen tiedonsiirtonopeus voi olla jopa 108 Mbps ja kantavuus saattaa yltää suotuisissa olosuhteissa jopa noin 300 metrin päähän.

Langattomat verkot yhdistetään kiinteään lähiverkkoon liityntäpisteillä. Liityntäpisteet mahdollistavat pidemmät etäisyydet päätteiden välillä, koska liityntäpisteet pystyvät toimimaan linkkeinä ja edelleen lähettämään toistensa liikennettä. Näitä liityntäpisteitä voi olla yksi tai useampi. Käyttäjän asentaessa langattoman verkkokortin tietokoneeseensa hän pystyy käyttämään langattoman lähiverkon tarjoamia palveluja koko verkon alueella. Langallisen verkon liityntäpiste, jonka kanssa käyttäjän tietokone keskustelee sisäverkossa, voi vaihtua tietokoneen liikkuessa ilman, että yhteys katkeaa tietokoneen ja lähiverkon välillä.

Käyttömahdollisuudet yhdistyksessä

Langattoman tiedonsiirron käyttöönotto yhdistyksen tiloissa on kohtuullisen helppoa, koska tilojen yleisilme on varsin avara. Tästä johtuen tiloissa selvittäneen yhdellä tukiasemalla, mikäli se sijoitetaan tilan keskellä olevan vastaanottopisteen läheisyyteen. Tässä tulee kuitenkin muistaa se, että vanhaa lankaverkkoa voi ja mielestäni tulisi myös edelleen käyttää, koska langatonta verkkoa en ainakaan itse pitäisi ainoana verkkona johtuen niiden häiriöherkkyydestä ja turvattomuudesta.

Siirtymisen kustannukset

Mahdolliset lisäkustannukset siirryttäessä lankaverkosta langattomaan verkkoon ovat n. 30 € /työasema* + verkkokaapelin asennus kytkentäpaneelilta langattoman verkon tukiaseman sijoituspaikkaan. Edellä mainittujen kulujen lisäksi tulee vielä hankittavaksi

langattoman verkon tukiasema, jonka hinta tällä hetkellä on noin 80 €* (54 Mbs siirtonopeus).
* lähteenä käytetty verkkokaupan (www.verkkokauppa.com) tietoja. Hinnat ovat työn tekoajoilta.

Salaustekniikat

Langattomissa lähiverkoissa tietoturvallisuutta on pyritty varmistamaan erilaisilla salaustekniikoilla. Näitä salaustekniikoita on seuraavat kolme:

- WEP (Wired Equivalent Privacy) http://fi.wikipedia.org/wiki/WEP
- WPA (Wi-Fi Protected Access) http://fi.wikipedia.org/wiki/WPA
- WPA 2 http://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva#WPA2_.28AES.29

Käytettäessä radiotaajuuksia kaikki langattoman verkon läpi siirrettävä tieto on käytännössä kaikkien lähialueella olevien kuunneltavissa. Langattoman verkon turvallinen käyttö vaatiikin tämän vuoksi jonkin yllä mainituista salausalgorytmeistä yhteyden salaukseen, mikäli halutaan luotettavuutta ja turvallisuutta langattomaan tiedonsiirtoon.

7.1. WEP (WIRED EQUIVALENT PRIVACY)

WEP on IEEE:n ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä. Tämän oli tarkoitus olla riittävä suojaus estämään salakuuntelu langattomista verkoista ja estää asiattomilta käyttäjiltä pääsy verkkoon. WEP luottaa salaiseen avaimeen, josta alun perin tehtiin U.S.A:n salaukseen liittyvien vientimääräysten vuoksi vain 40-bittinen. Ensimmäisen version jälkeen kehitettyjen 802.11b* ja 802.11g* standardien myötä voidaan käyttää myös 64 tai 128

bittistä salausavainta. Avain hoitaa lähetettävien pakettien salauksen ja sen lisäksi se takaa siirrettävän tiedon eheyden langattomassa verkossa.
*http://fi.wikipedia.org/wiki/802.11

Salauksen turvallisuus

WEP salaus on purettavissa kohtuullisen helposti Internetistä saatavilla ilmaisilla ohjelmilla, joten tämän vuoksi WEP:iä voidaan pitää melko turvattomana ratkaisuna langattomissa verkoissa. WEP salaus estää satunnaiset murtokokeilut langattomassa verkossa, mutta vain, jos samalla alueella on muita vielä heikommin salattuja WLAN verkkoja. Tässä on kuitenkin muistettava WLAN:neista se seikka, että WLAN:it toimivat melko suppealla alueella, joten WEP salausta on lähes hyödytöntä käyttää WLAN:in turvaamisessa, mikäli aikomuksena on rakentaa turvallinen langaton verkko. Toisaalta WEP salattu verkko on kuitenkin haavoittuvainen vain selvästi rikollisille toiminnalle, eli heikon avaimen murtamiselle, mikä tarkoittaa että, WEP salausta ei voida murtaa vahingossa, eikä näin ollen sen murtaja voi sanoa, että en tiennyt, ettei tuota saanut tehdä.

WEP käyttää RSA:n (http://fi.wikipedia.org/wiki/RSA) RC4* salausalgoritmia, jonka toiminnassa on ollut joitain heikkouksia. WEP salauksen yhtenä haittana on ollut (ja on yhä) lyhyet alustusvektorit (*Initialization Vector*). Nämä lähetetään salaamattomina jokaisen kehyksen ensimmäisissä biteissä. Kuuntelemalla tietoliikennettä kahden laitteen välillä ja suunnilleen samoja alustusvektoreita etsimällä pystytään salausavain laskemaan. Samankaltaisten alustusvektoreiden löytymisen jälkeen pystymään langattoman verkon salaus murtamaan melko nopeasti. Kuinka helposti ja nopeasti avain on murrettavissa, on riippuvainen siitä minkä verran tietoa siirretään laitteiden välillä langattomassa verkossa.
* http://fi.wikipedia.org/wiki/RC4

MAC (Media Access Code) osoitteeseen perustuvaa lisäsuojausta on käytetty WEP:n lisänä joissakin tapauksissa, vaikka tämä ei 802.11 standardin alkuperäisiin määrityksiin kuulunutkaan. MAC suojausta käyttävän langattoman verkon tukiasema sallii yhteydenmuodostuksen verkkoon vain niille laitteille, joiden MAC osoitteet se tunnistaa ja ”löytää” omalta sallittujen laitteiden listaltaan. MAC lisäsuojausta ei kuitenkaan voi pitää

riittävänä lisäsuojauksena WEP salatuissa verkoissa, sillä joillekin verkkokorteille on mahdollista sen oman ohjelmiston avulla määrittää itse MAC osoite. Tämä voidaan kaapata kuunnellusta verkosta, ja näin huijata tukiasemaa luulemaan hyökkääjän laitetta joksikin sellaiseksi laitteeksi, jolla on oikeus käyttää langatonta verkkoa. Lisäksi langattoman lähiverkon liikennettä voidaan yrittää kuunnella yrittämättä edes kytkeytyä siihen. Tällöin pyritään etsimään arkaluonteista tai muulla tavoin arvokasta tietoa, jolla sitten pahimmassa tapauksessa voidaan yrittää hankkia rahallista hyötyä. WEP salauksen ongelmien paljastuttua alettiin kehittää WPA salaustekniikkaa, joka on syrjäyttämässä WEP salausta. Tänä päivänä hankittavien uusien tukiasemien tulisi vähintään tukea WPA standardia ja siitä vielä sellaista versiota, jossa on AES salaus, jolloin päivitys tulevaan WPA2 tai 802.11i protokollaan voidaan suorittaa ajuripäivityksellä.

7.2. WPA / WiFi (WIRELESS FIDELITY PROTECTED ACCESS)

WPA tai Wi-Fi (**Wireless Fidelity Protected Access)** on tämän hetken ehkä yksi varmimmista salausalgorytmeistä langattomassa tiedonsiirrossa. Se kehitettiin WEP salauksen ongelmien määrän laajennuttua yhä laajemmiksi. Toinen syy oli se, että langattomien verkkojen määrä kasvoi yhä kiihtyvällä nopeudella. WPA sisältää monia tulevan 802.11i standardin ominaisuuksia, ja se on yhteensopiva niin alaspäin kuin ylöspäinkin, mikä on harvinaista tietotekniikan puolella.

WEP salauksen heikon aloitusvektorin ongelma korjattiin ja sen lisäksi uutena ominaisuutena tuli mukaan salausavaimen vaihto aina 10 000 paketin jälkeen. WPA:ssa on lisäksi käytössä TKIP salaus (Temporal Key Integrity Protocol). Tämä protokolla mahdollistaa WEP avaimen suojaamisen hyökkäyksiltä. TKIP laajentaa langattoman verkon turvallisuutta runsaasti, koska ottamalla TKIP käyttöön saadaan pakettikohtaiset salausavaimet. TKIP salaa liikenteen samalla RC4 algoritmilla kuin WEP, mutta salausavaimen pituus on 128 bittiä. WPAn heikkoutena puolestaan on sen heikko kyky kestää palvelunestohyökkäyksiä. Tämä haavoittuvuus johtuu WPA:n tavasta yrittää selviytyä verkkohyökkäyksistä, joka on sellainen, että WPA sulkee koko verkon noin minuutiksi havaittuaan mahdollisen hyökkäyksen. Tämä tarkoittaa sitä että, verkon lailliset käyttäjätkään eivät saa katkon aikana omaa liikennettään eteenpäin. WPA:ta ollaan korvaamassa IEEE:n 802.11i(WPA 2) protokollalla.

7.3. TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

WAP:n uusi salauskäytäntö poistaa WEP salauksen tunnetut ongelmakohdat, jotka johtuvat WEP:in käyttämästä pysyvästä salausavaimesta. TKIP korvaa WEP:in käyttämän tukiasemaan ja tietokoneen välisen kiinteän 40 bittisen avainparin 128-bittisellä pakettikohtaisella salausavaimella. WEP salauksen purkamisessa oleellisena osana olevan salausavaimen ennustettavuus poistuu TKIP avainpareja käytettäessä, koska avainparit luodaan dynaamisesti paketti- ja yhteyskohtaisesti.

WPA salauksessa on myös pakettien eheyttä valvova MIC (Message Integrity Check) toiminto. Tämä toiminto tarkistaa pakettikohtaisesti, ettei mahdollinen hyökkääjä ole pystynyt muuttamaan paketteja tai niiden sisältämää tietoja. MIC toiminto estää mahdollista hyökkääjää muuttamasta verkossa liikkuvien pakettien sisältöä monimutkaisen matemaattisen yhtälön avulla, jossa sekä lähettäjä että vastaanottaja laskevat jokaisesta paketista tarkisteen ja tätä tarkistetta verrataan keskenään pakettien aitouden varmistamiseksi. Jos tarkistussummat eivät ole samat, paketti hylätään virheellisenä, koska sen oikeellisuutta ei pystytä varmentamaan tarkisteen avulla. MIC:ssä on myös ylimääräinen turvallisuustoiminto. Tämä on sellainen, että havaittaessa epäilyttävä paketti kaikki verkon käyttäjät varmennetaan uudelleen ja kaikki uudet yhteysyritykset estetään minuutin ajaksi.

Käyttäjän kytkeytyessä langattomaan verkkoon käyttäjäksi, joko kirjautumispalvelin tai tukiasema luo yksilöllisen pääavainparin PMK (Pair-wise Master key) käyttäjälle yhteyden ajaksi. TKIP protokolla välittää avaimen sitä haluavalle käyttäjälle. Tämän avainparin avulla TKIP luo automaattisesti pakettikohtaiset avaimet kaikkien verkkoon välitettävien pakettien salaamiseksi.

7.4. WPA 2

802.11i, (WPA2) on langattomien verkkojen tämän hetken viimeisin standardi, jolla pyritään ratkaisemaan langattomissa verkoissa olevat viimeisimmät tietoturvaongelmat. Standardissa määritellään 802.1x:n mukaiset todentamis- ja avaintenhallintakäytäntö sekä näiden lisäksi parannetut menetelmät siirrettävän tiedon salaukseen. 802.11i tar-

joaa käytännössä samat ratkaisut verkkoliikenteen salaukseen kuin aiempi WPA standardi, mutta salaukseen on valittavana aivan uusi salausmekanismi AES (Advanced Encryption Standard). AES salausalgoritmi on tehokkaampi kuin WPA käyttämä RC4, mutta huonona puolena puolestaan on se, että AES vaatii tämän vuoksi enemmän prosessointitehoa. AES pystyy käyttämään eripituisia avaimia, alkaen 128 bittisestä ja suurimman ollessa 256 bittisen. 802.11i standardin yhteydessä käytettiin aluksi 128 bittistä salausta, mutta nykyään käytössä on 256 bittinen avain. Verkon käyttäjät pääsevät sisäverkkoon ja Internetiin vasta onnistuneen tunnistamisen jälkeen.

8. TIETOTURVA

Mitä tietoturva on ? Tämän kysymyksen kuulee jossakin muodossa aika usein, kun siitä yrittää avata keskustelua. On ehkä helpompaa aloittaa kertomalla siitä, mitä tietoturva ei ole. Se ei ole yksittäinen ohjelma, joka asennetaan tietokoneeseen, jonka asennuksen jälkeen voidaan ”unohtaa” kaikki mahdolliset uhkatekijät ja käyttää tietokonetta turvallisin mielin. Tämä tyyli on kuitenkin valitettavan yleinen, johtuen siitä harhaluulosta, joka syntyy monesta eri lähteestä annetusta ohjelmistojen ”idioottivarmuudesta” juuri tietoturvan osalta. Tietoturva ei kuitenkaan ole pelkkää teknologiaakaan, vaan tietoturvan aikaansaavat sekä käyttäjät että ohjelmisto yhdessä. Ilman tätä käyttäjän ja ohjelmiston yhteistoimintaa on mikä tahansa tietoturvaa edistävä toimenpide turha, koska toisen ”unohtaminen” antaa hyökkääjälle aina mahdollisuuden yrittää hyväksikäyttää tätä toista puolta.

Järjestelmän tietoturva on juuri niin vahva kuin sen heikoin lenkki on. Ja valitettavan usein käyttäjän luottamusta väärinkäyttävän oikeudettoman henkilön paras ”ase” on esiintyä esim. järjestelmänvalvojana ja kysyä käyttäjältä tämän tunnukset jonkin tekosyyn nojalla, jonka jälkeen hän pääsee käyttämään järjestelmän ohjelmia ja tiedostoja ilman vaaraa kiinnijäämisestä, koska hänellä on ”viralliset” tunnukset sen käyttöön. Näin ollen tietoturvaan kuuluu se osa jokaisen henkilön toiminnasta, jolla turvataan tietoverkon häiriötön ja turvallinen toiminta.

Asioita, joihin ei voi missään nimessä voi panostaa liikaa, on käyttöjärjestelmän suojauksien asianmukainen ylläpito sekä säännöllinen tiedotus uhista käyttäjille. Ilman säännöllisiä ja jatkuvia tarkistuksia saattavat käyttäjiltä jäädä epähuomiossa suorittamatta jokin tietoturvapäivitys, jonka jälkeen tietokone saattaa olla alttiina hyökkäyksille ja pahimmassa tapauksessa jopa haltuunotolle. Tietoturva siis merkitsee jatkuvaa varuillaanoloa ja tiedotusta uhista ja niiden aiheuttamista vaaroista. Tämän lisäksi tulee kaikille verkon käyttäjille antaa sekä tiedotusta uhista että opastusta siihen liittyvissä kysymyksissä.

Tietoturvassa ei ole tarkoituksena mikään utopistinen täydellisyyden tavoittelu, vaan kyseessä tulisi olla ennalta sovittu tietyn kaltainen toimintatapa, jolla yritetään hallita riskejä ja estää vahinkoja. Tietokoneet eivät ole sen paremmin fyysisesti kuin ohjelmistollisesti ”idioottivarmoja”, koska kyseessä on usein eri tavarantoimittajien osista koottu laite. Tämän kokonaisuuden kokonaisturvallisuus riippuu tietokoneen koonneen yrityksen asiantuntemuksesta ja tietoturvan tiedostamisesta. Lisäksi tulee muistaa se, että käyttöjärjestelmässä, joka tietokoneeseen on asennettu, on mahdollisesti tietoturvaa vaarantavia asioita. Tietoliikenteen riskejä voidaan huomattavasti vähentää, mikäli pystymme vähentämään riskien määrää.

Eräs seikka, johon tulisi kiinnittää huomiota, on se missä säilytetään tiedostojen varmistukset. Sillä näiden anastamisen ollessa tehty liian helpoksi, niiltä saa kaiken tiedon, mitä niihin on varmistettu. Toinen seikka, joka tulee huomioida, on mahdollinen onnettomuus, mikä voi tuhota varmistukset. Näiden syiden vuoksi tulisi olla joko kaksinkertainen varmistusjärjestelmä, jossa toinen puoli varmistuksista olisi muualla kuin siinä paikassa, jossa palvelin sijaitsee tai sitten varmistusmedioiden tulee sijaita sellaisessa tilassa, jossa on riittävät suojaukset mahdollisia uhkia vastaan. Näin ratkaistulla varmistuksella pystytään selviytymään tiedostojen menetykseltä jopa silloin, jos palvelin ja ensisijaiset varmistukset ovat tuhoutuneet esim. tulipalossa.

Ensimmäiseksi tulisi kartoittaa nykyisen verkon tietoturva, jotta saataisiin selville missä voi olla ongelmia. Tästä tulisi tehdä dokumentti, jossa olisi ainakin seuraavat asiat listattuna:

- verkon tietoturvan tila

- sovellusten tietoturvan tila
- käyttäjien tietoisuus tietoturvasta

Lisäksi tätä dokumenttia tulisi päivittää säännöllisesti, jotta siinä olisi koko ajan ajantasainen tieto järjestelmästä ja sen muutoksista. Ilman näin tehtävää jatkuvaa ajan tasalla pitoa sen mahdollinen käyttöarvo työvälineenä heikkenee koko ajan, koska verkon ja/tai sovellutusten muuttuessa niiden mukanaan tuomat riskit muuttuvat myös.

Luvattoman käytön mahdollistavat esim. virukset, laitteiden ja ohjelmistojen tietoturva-aukot, ohjelmien virheitä hyödyntävät hyökkäykset ja käyttäjien huijaukset. Luvattomia käyttäjiä listatessa ensimmäisinä mieleen tulevat hakkerit ja ammattirikolliset, kuitenkaan unohtamatta organisaation omaa henkilökuntaa, koska heillä on usein ”parhaat” tiedot järjestelmästä, jota yrittävät käyttää luvattomasti.

Lisäksi on tiedettävä, miltä halutaan suojautua ja miten se tehdään, unohtamatta mitä halutaan suojata. Järjestelmän suojattavia asioita on ainakin seuraavat asiat:

1. laitteistot (tulipalolta, vedeltä yms.)
2. ohjelmistot (viruksilta, levyrikoilta yms.)
3. sisäverkon liikenteen turvaaminen. (estetään ulkopuolisten pääsy sisäverkkoon)
4. etäyhteyksien riittävän vahva salaus. (esim. VPN:lla)
5. tietokannat ja käyttäjien omat tiedostot
6. tiedon kuljettamiseen käytettävät mediat (CD:t, muistitikut, yms. laitteet)

Käyttäjien tulisi huomioida seuraavat asiat:

1. virustorjunnan ja palomuurin ajan tasalla pito.
2. tietoturva (virukset, s-postimadot, phishing, yms.)
3. käyttäjien ei tule asentaa tuntemattomia ohjelmia tietokoneeseen.
4. Käyttää hyviä salasanoja. (vähintään 8 merkkiä, sisältäen kirjaimia ja numeroita eikä salasanaa tulisi löytää mistään sanakirjasta)
5. Älä avaa liitetiedostoja, joiden nimessä on tuplatunniste. (esim. ohje.doc.exe)
6. Älä avaa liitetiedostoja, joiden lähettäjää et tunne.

7. Älä avaa liitetiedostoja, joiden lähettäjä ei itse viestissä kerro liitteen olemassaolosta.
8. Lue sähköpostit vain teksti muotoisena. Tämä tarkoittaa, että esim. HTML muotoiset viestit muunnetaan "pelkäksi tekstiksi" ennen kuin se näytetään ruudulla.

9. SUUNNITTELU

Uusi 2003 palvelin voidaan asentaa johonkin seuraavista rooleista:

- jäsenpalvelin
- toimialueen ohjauspalvelin
- yksittäinen palvelin

Jäsenpalvelin on nimensä mukaisesti toimialueen jäsen, jolle ei tallennu aktiivihakemiston (AD) tietoja. Tällainen palvelin voi toimia esim. tiedostopalvelimena verkon käyttäjille. Tällainen palvelin vaatii erillisen ohjauspalvelimen, koska ilman ohjauspalvelinta on verkon ylläpito usein melko hankalaa, koska tällöin ei ole keskitettyä verkon tietojen ylläpitoa.

Ohjauspalvelimet eroavat jäsenpalvelimista siinä, että ohjauspalvelimille tallentuu aktiivihakemistojen tiedot. Lisäksi ne hoitavat käyttäjien tunnistuksen ja heidän oikeuksiensa määrittämisen käyttäjän kirjautuessa toimialueelle. Ohjauspalvelimia voi olla yksi tai useampia samalla toimialueella. Kun/jos toimialueeseen kuuluu useampia ohjauskoneita, niin nämä välittävät tietonsa automaattisesti saman toimialueen toisille ohjauskoneille.

Yksittäiset palvelimet hoitavat oman alueensa käyttäjätunnistuksen itsenäisesti ja ilman aktiivihakemistoa. Tämänkaltaiset palvelimet toimivat miltei kuten ohjauspalvelimet, mutta suurin ero on juuri tuo AD:n puuttuminen. Tämä taas johtaa siihen että, näiltä palvelimilta puuttuu mm. käyttäjien oikeuksien hallinta yms. asiat, jotka voidaan tehdä

vain AD:llä. Yksittäinen palvelin toimii työryhmäpalvelimena, joka tarkoittaa sitä että, palvelin on samanlaisessa asemassa kuin työasema, eli on kuin mikä tahansa muu tietokone ko. verkossa.

Tästä johtuen suunnittelin järjestelmän siten, että verkkoon asennetaan yksi palvelin, joka toimii niin kirjautumis-, tiedosto-, ja ohjauspalvelimena hoitaen kaikkien palveluiden hallinnan toimialueella. Johtuen edellisistä tämän palvelimen täytyi olla ensisijainen ohjauspalvelin.

Toimintamoodiksi valitsin toimialueen, koska näin voidaan hieman rajoittaa verkon luvatonta käyttöä. Lisäksi tällä tavoin verkkojakojen käyttö ei onnistu ilman riittäviä oikeuksia toimialueella. Toimialueen nimeksi suunnittelin yhdistyksen nimen, koska se on käyttäjien ”helppo” muistaa. Palvelimen nimeksi määritettiin yksinkertaisesti palvelin1, koska näin palvelimen tunnistaa helposti palvelimeksi.

Lisäksi tuli varmistaa se että, laitteisto vastaa palvelinohjelmiston vaatimuksia. Tämä seikka tuli käytännössä varmistettua sillä, että palvelinta hankittaessa varmistettiin asia kysymällä toimittajalta laitteen soveltuvuus. Toimittaja vahvisti sen, että laitteisto on yhteensopiva palvelinohjelmiston kanssa.

9.1. LEVYJÄRJESTELMÄT

Kiintolevylle suunnittelin omat osiot niin järjestelmälle, asennettaville lisäohjelmille, käyttäjien hakemistoille kuin levyvälimuistille (swap). Osioiden kooiksi määritin järjestelmäosiolle 8 Gt, levyvälimuistille suunnittelin 2 Gt, joka on kaksinkertainen määrä fyysiseen muistiin nähden, asennettaville lisäohjelmille määritin 30 Gt, käyttäjien tiedostoille suunnittelin jättää loput levystä. Näillä asetuksilla levyvälimuisti ei pysty sekoittamaan käyttäjien tiedosto-osiota tai systeemiosiota. Toisaalta, kun järjestelmälle on varattu oma osio, jota ei ole jaettu, niin käyttäjät eivät voi tallentaa systeemiosiolle ja täyttämään sitä tarpeettomilla ja sinne kuulumattomilla tiedostoilla. Levyn osioiden tiedostojärjestelmäksi tuli NTFS järjestelmää, joka on mielestäni ainoa järjestelmä, jota tulee käyttää, koska tällöin on käytössä journaloiva tiedostojärjestelmä. Journaloiva tiedostojärjestelmä pystyy säilyttämään tiedostojen eheyden, vaikka tietokoneeseen tulisi

kesken käytön virtakatko. Eheyttä pidetään yllä pitämällä kirjaa kaikista levylle tehdyistä muutoksista ja tiedot päivitetään vasta, kun tiedoston käyttö lopetetaan.

9.2. LISENSIOINTIPOLITIIKKA

Lisensiointimenettelyksi valitsin konekohtaisen käyttö-oikeuden ja lisenssien määräksi suunnittelin nykyistä työasemamäärää hieman suuremman, koska näin yhdistyksen ei tarvitse hankkia lisää lisenssejä, jos työasemia hankitaan lisää. Mikäli lisensiointitavasta ei ole täyttä varmuutta asennuksen aikana, niin tällöin kannattaa valita vaihtoehto, jossa käyttö-oikeuslisenssit ovat palvelimella, koska tämä voidaan vaihtaa kerran konekohtaiseksi vaihtoehdoksi. Tätä mahdollisuutta vaihtaa ei ole konekohtaisessa asennusvaihtoehdossa.

9.3. VARMUUSKOPIOINTI

Varmuuskopioinnista suunnittelin sellaista, että kerran viikossa suoritettaisiin täydellinen varmistus esim. perjantaina ja muina arkipäivinä suoritettaisiin eroava varmistus, koska näin saavutettaisiin varsin hyvä peitto siinäkin tapauksessa, että järjestelmälle tapahtuisi jokin vahinko jonain arkipäivänä.

9.4. LEVYJEN KÄYTTÖ-OIKEUDET

Levynkäytöstä suunnittelin sellaista vaihtoehtoa, jossa kullekin käyttäjälle määritetään jokin tietty määrä tallennusoikeutta palvelimen henkilökohtaisiin kansioihin. Tätä määrää en kuitenkaan halunnut edeltä käsin rajata, koska minulla ei ollut tietoa kuinka paljon/kuinka suuria tiedostoja käyttäjillä on. Toinen asia, jonka suunnittelin palvelimen levykäytölle, oli se, että palvelimen käyttäjäkohtaisiin hakemistoihin ei ole kirjoitusoikeuksia muilla kuin ko. kansion omistajalla ja järjestelmänvalvojalla. Toinen rajoitus, jonka suunnittelin, oli sellainen, että kenelläkään muulla kuin järjestelmänvalvojalla ei ole kirjoitusoikeuksia juurihakemistoon. Jälkimmäinen ehto siksi, että näin eivät käyttäjät pääse sekoittamaan kansiorakenteita tallentaen sinne tänne.

9.5. VERKKOTULOSTIMET

Verkkotulostimien asennuksen helpottamiseksi suunnittelin niille valmiiksi sekä jakonimet että asetukset. Nimiksi näille verkkokirjoittimille suunnittelin toimisto ja yleinen. Yleisen kirjoittimen suunnittelin sellaiseksi, joka olisi kaikilla oletuskirjoitin. Yleinen kirjoittimen sijoituspaikaksi suunnittelin sellaisen paikan, joka olisi mahdollisimman lähellä kaikkien käyttäjien työskentelypistettä. IP osoitteiksi kirjoittimille suunnittelin 192.168.0.8 ja .9 osoitteet, koska nämä osoitteet olivat suunnitelmassani viimeiset kiinteät IP:t.

9.6. INTRANET

Yhdistyksen henkilökunta esitti toiveen Intranetin käytön mahdollisuuksista ja tuon selvityksen alustava tulos osoitti, että yhdistyksellä saattaisi olla monia tiedostoja mallipohjiksi, jotka voitaisiin mallintaa esim. Adobe Acrobat tiedostoiksi, jotka sitten voitaisiin sijoittaa intranettiin käyttäjien haettavaksi ja käytettäväksi. Näiden tiedostojen lisäksi ko. sivustolle suunniteltiin myöhemmässä vaiheessa lisättäväksi sähköinen ilmoitustaulu, jonne tulisi päiväohjelmat, ilmoitusluonteiset asiat, päivän tapahtumat sekä mahdollisesti henkilökunnan esittelysivut.

Intranetin tiedon ja palveluiden käyttäminen on mitä suurimmassa määrin riippuvainen käyttäjän asenteesta sekä aikaisemmasta tietokoneen käyttökokemuksesta, joka tässä tapauksessa tarkoittaa sitä, että ilman kohtuullista opastusta ko. järjestelmästä ei saada kaikkia sen tarjoamia mahdollisuuksia hyötykäyttöön. Lisäksi joillakin käyttäjillä saattaa olla suuri kynnys opetella käyttämään sellaista asiaa, josta ei ennestään ole aiempaa kokemusta. Tämä voi aiheuttaa muutosvastarintaa tai jopa suoranaista vihamielisyyttä intranettia kohtaan ja tämä asia tulisi ottaa huomioon käytön aloitusta suunniteltaessa. Koulutus uuteen järjestelmään on ensiarvoisen tärkeää, jolloin jokaisella olisi tarvittava tieto intranetistä ja kaikki osaisivat käyttää sen tarjoamia mahdollisuuksia täysimääräisesti ja opastaa uusia käyttäjiä näiden alkaessa käyttämään intranettia. Näin voisi jokainen olla osaltaan rakentamassa intranetin sisältöä, jolloin ei pääsisi syntymään näitä varautumia ja epäonnistumisen pelkoja, jotka saattavat aikaansaada hyvänkin asian hylkäämisen.

9.7. OIKEUSPOLITIIKAT

Varsinaisia oikeusmääritteitä tuli varsin vähän, koska käyttäjäryhmiä muodostui vain kaksi. Nämä ryhmää ovat seuraavat:

1. Ohjaajat
2. Jäsenet

Ryhmälle jäsenet oikeuksia annettiin vain peruskäyttäjän oikeudet, joka tarkoittaa sitä, että tässä ryhmässä olevat käyttäjät pystyvät ainoastaan käyttämään niitä työkaluja ja ohjelmia, joita tietokoneeseen on asennettu heille käytettäväksi, mutta tämän ryhmän jäsenillä ei ole oikeutta asentaa lisäohjelmia tietokoneeseen omilla tunnuksillaan. Lisäksi heille annettiin luku- ja kirjoitusoikeudet joihinkin jaettuihin hakemistoihin palvelimella.

Ohjaajat ryhmän jäsenillä taas on järjestelmänvalvojan oikeudet ja näin ollen he pystyvät asentamaan ohjelmia ilman, että heidän täytyy muistaa erillistä järjestelmänvalvojan tunnusta. Tämän lisäksi he pystyvät kontrolloimaan verkon käyttöä ja sen käyttäjiä paremmin.

9.8. VERKKOMÄÄRITYKSET

9.8.1. IP OSOITTEET

Nämä määritykset olivat sellaiset, joista esitin omana näkemykseni, että tietokoneet toimialueella hakevat osoitteensa DHCP:llä palvelimelta. Täksi osoiteavaruudeksi olin valmiiksi ajatellut 192.168.0.0 / 24 verkkoa, joka riittää yhdistyksen käyttöön. Tämän privaattiverkon osoitesarjan valitsin siksi, että näin jää mahdollisuus laajentaa osoiteavaruutta, mikäli siihen tulee tarvetta tulevaisuudessa.

9.8.2. DHCP PALVELU

IP osoitteet määritettiin siis välille 192.168.0.0 – 192.168.0.255 aliverkon tunnuksen ollessa 255.255.255.0. Osoitteet 192.168.0.1 - 192.168.0.9 määritettiin pois DHCP osoitteista. Loput käytettävistä osoitteista (10 – 254) jakaa DHCP dynaamisesti osoitetta tarvitseville tietokoneille. Osoitteet 1 – 9 päätettiin jättää staattisiksi, koska näin saatiin verkkokirjoittimille ja palvelimelle kiinteät osoitteet.

Näistä kiinteiksi jätetyistä osoitteista päätettiin varata palvelimille osoitteet 192.168.0.1 ja 192.168.0.2. Asia, johon en huomannut varautua oli se, että mikäli halutaan varmennettu verkko-osoitteen saanti, niin tässä tapauksessa olisi pitänyt supistaa tuota DHCP osoitesarjaa jättäen kuitenkin aliverkon tunnukseksi edellä mainitun 255.255.255.0:n, ja asetettu vaihtoehtoisiksi IP osoitteeksi tästä supistetun DHCP alueen ulkopuolelle jääneistä osoitteista tämä vaihtoehtoinen IP osoite.

Toinen ratkaisuvaihtoehto olisi ollut laajentaa käytettävää IP osoitesarjaa toisella C luokan osoitesarjalla käyttämällä aliverkon tunnuksena 255.255.254.0, jolloin käytettävät osoitteet olisivat olleet välillä 192.168.0.0 – 192.168.1.254. Tällöin olisimme voineet antaa tietokoneille vaihtoehtoiset kiinteät IP osoitteet väliltä 192.168.1.1 – 192.168.1.254 ja näin olisimme saaneet varmistettua käyttäjille yhteyden Internetiin.

9.8.3. WINS

WINS tekee NetBIOS kyselyille saman kuin DNS tekee nimikyselyille eli kääntää toimialueen nimen verkko-osoitteiksi. Yksittäinen WINS palvelu pystyy palvelemaan jopa kymmentä tuhatta työasemaa NETBIOS nimikyselyiden osalta.

Mikäli halutaan parantaa viansietoa, tällöin voidaan WINS palvelu kahdentaa kahdelle Windows 2003 palvelimelle, jolloin toinen palvelimista konfiguroidaan backupiksi. Tällöin tulee toinen WINS palvelimista asettaa tilaan, jossa se ”vetää” tiedot toiselta (pull partner), ja toinen WINS palvelimista on asetettava sellaiseen tilaan, jossa se ”työntää” omat tietonsa toiselle (push partner). Näiden palvelimien tietojen replikointi voidaan asettaa joko manuaaliseksi tai automaattiseksi. Tämä valinta tehdään valitsemalla

automatic partner configuration ruutu advanced välilehdeltä replication partner properties valintaikkunassa.

9.8.4. VERKKOJAOT

Verkkojaoiksi alkujaan suunnittelin sellaista ratkaisua, että kullakin käyttäjällä olisi oman kansion lisäksi jokin yhteinen kansio, minne kukin voisi tallentaa sellaisia tiedostojaan, jotka olisivat kaikkien verkon käyttäjien tarkasteltavissa. Tämä suunnitelma kuitenkin oli hieman vajaa, koska yhdistyksellä oli myös ns. yleisiä kansioita, jonne kaikilla tuli olla pääsy. Lisäksi yhdistyksen joillakin toimijoilla oli toiveena saada sellainen kansio, jonne olisi rajoitettu pääsy. Tästä johtuen luotiin kerrosarkkitehtuuri, jossa ylimpänä olivat sellaiset kansiot joissa on vähiten rajoituksia ja mitä syvemmälle kerrosarkkitehtuurissa mennään niin sitä enemmän rajoituksia alkaa olla. Kaikkein suurimmat rajoitukset ovat kunkin käyttäjän henkilökohtaisissa kansioissa, joihin oletussäännöin ei ole oikeuksia kuin ko. kansion omistajalla sekä järjestelmänvalvojalla.

9.8.5. DNS

Palvelimeen määritettiin forwarding palvelu, jossa kaikki ulkoverkon DNS kyselyt ohjataan palveluntarjoajan DNS palvelimelle. Tällä tavoin kaikkien ulkoverkon nimikyselyihin vastaa palveluntarjoajan DNS palvelimella oleva palvelu. Sisäverkon nimikyselyihin puolestaan vastaa verkon oma DNS palvelin.

10.PALVELIMEN ASENNUS

Palvelimen toimittaja oli asentanut käyttöjärjestelmän siten että, se käynnistyi normaalisti. Näin ollen tehtäväkseni jäi palvelimen asetusten ja tarvittavien palveluiden asennus. Palvelimeen asennettiin seuraavat palvelut:

- DNS palvelu
- Domain controller palvelu
- Tiedostopalvelu
- Tulostuspalvelu
- DHCP palvelu
- WINS palvelu

Tarvittavien palveluiden asennus on suhteellisen helppoa, sillä ne voi asentaa kuvan 1 ikkunasta kohdasta Add or remove a role. Tämän ikkunan saa myös avattua käynnistä valikosta kun klikkaa sen kohtaa Manage Your Server.

Tässä kohtaa on kuitenkin hyvä muistuttaa se että, mikäli ei ole aiemmin asentanut ko. palvelimeen vastaavia palveluita, niin sen näennäisen helpon aloituksen jälkeen palvelin kysyy monia yksityiskohtia, joihin vastaamalla puutteellisesti / virheellisesti palvelin saattaa kyllä hyväksyä vastaukset, mutta sitten käytössä antaa käyttäjille virheilmoituksia ja pahimmissa tapauksissa jopa aiheuttaa käyttäjien tietojen katoamista.

Palveluista tulee ensimmäisenä asentaa DNS palvelu, koska AD käyttää DNS:ää ohjauspalvelimen etsintään. Vasta DNS palvelun asentamisen jälkeen tulee asentaa muut palvelut mukaan lukien AD. Näiden muiden palveluiden asennusjärjestyksellä ei ole mitään pakollista asennusjärjestystä, mutta suositeltavin järjestys lienee AD-, DHCP-, WINS-, tiedosto- ja lopuksi tulostuspalvelu.

10.1. DNS JA ACTIVE DIRECTORY

Kuvan 1 kohdassa Add or remove a role kohtaa klikatessa, aukeaa kuva 2, josta valitaan se palvelu, joka halutaan asentaa. Ensimmäiseksi asensin DNS palvelun, koska ennen AD:n asennusta on tarpeen miettiä etukäteen, millaisen nimen valitaan DNS nimeksi, koska tästä nimestä tulee toimialueen nimi. Seuraavaksi asennusohjelma kysyy millaisia tietokoneita toimialueella on. Tätä tietoa tarvitaan, koska tämän tiedon perusteella asennusohjelma määrittää oikeuspolitiikan tason (kuva 3). Lisäksi oli tarpeen selvittää minne AD tallentaa tietokantansa sekä logi tietonsa.

DNS palvelu asennettiin forwarders palveluna, jolloin toimialueen palvelin lähettää ne saamansa DNS kyselyt, joihin sillä ei ole tietoa, palveluntarjoajan DNS palvelimelle. Tämä vaihtoehto oli minusta paras vaihtoehto, koska näin yhdistyksen oman palvelimen kuormaa saadaan tasattua vähimmällä vaivalla. Toinen vaihtoehto olisi ollut se että, toimialueen ohjainpalvelin olisi toiminut myös DNS palvelimena. Tällöin olisi kaikki kyselyt ohjautuneet toimialueen ohjauspalvelimelle, joka olisi saattanut hidastua

Mikäli palvelin on ainoa palvelin toimialueella, kuten oli tässä tapauksessa, niin tällöin siihen tulee asentaa sekä DNS että ohjauspalvelin ensimmäisinä, koska ilman näitä palveluita ei saada käyttöön Active directoryä (AD) ja sen edistyneitä palveluita. Aivan ensimmäiseksi ohjauspalvelun asennusohjelma kysyy hakemistopalvelun (AD:n) palautussalasanaa ja vahvistusta sille.(kuva 4) Tämän jälkeen asennusohjelma tarjosi valintaikkunaa, josta piti valita onko asennettava palvelin uuden toimialueen ensimmäinen palvelin vai tehdäänkö siitä lisäpalvelin jo olemassa olevaan toimialueeseen (kuva 5). Palvelimen roolin valinnan jälkeen asennusohjelma kysyy toimialueen tyypin. Tässä ikkunassa oli seuraavat kolme vaihtoehtoa.(kuva 6)

- uusi toimialue uuteen toimialuemetsään
- alitoimialue olemassa olevaan toimialueeseen
- uusi toimialue olemassa olevaan toimialuemetsään

Näistä vaihtoehdoista sopi ainoastaan ensimmäinen, koska mitään aiempaa toimialuetta ei ollut, johon olisi voinut liittää tämän palvelimen. Näiden perustietojen jälkeen asennusohjelma kysyy toimialueen täydellistä DNS nimeä. (kuva 7) Tästä nimestä tuli samalla myös toimialueen nimi. Seuraavassa ikkunassa asennusohjelma halusi tietää toimialueen NetBIOS nimen. Ohjelma ehdotti täksi DNS nimen alkua, jonka hyväksyin.(kuva 8) Nimien valinnan jälkeen asennusohjelma kysyy Active Directoryn tietokannan ja sen virheilmoitusten tallennuskansion. (kuva 9) Nämä hakemistot olisi ollut hyvä tallentaa omaan osioonsa, mutta kun sellaista ei ollut käytettävissä, niin nämä tiedot päätettiin tallentaa oletuskansioihin. Viimeisessä ikkunassa asennusohjelma kysyy sysvol hakemiston tallennuspaikkaa,(kuva 10) jonka hyväksyin oletusarvolla.

Kuten edellä kävi ilmi, tulee asennusjärjestyksen olla DNS ja AD osalta sellainen, että ensin asennetaan DNS palvelu ja vasta tämän jälkeen AD.

10.2. TIEDOSTOPALVELU

Tiedostopalvelun asennus oli melko suoraviivainen tehtävä, koska windows server 2003 ei esittänyt käytännössä mitään vaihtoehtoja kuin painaa seuraava (Next) painiketta. Ainoa kohta, jossa tuli miettiä tarkemmin oli kohta, jossa asennusohjelma kysyi, millaisia jakopalveluita halutaan asentaa tiedostopalvelun yhteyteen. Asennusohjelma antoi tässä kohtaa seuraavat neljä vaihtoehtoa:(kuva 20)

1. Replicate data to and from this server
2. Manage a SAN (Storage Area Network)
3. Share files with UNIX system
4. Share files with Apple Macintosh computers

Tässä tapauksessa ei ollut tarpeen asentaa mitään yllämainituista kohdista, koska toimialueella ei ollut muita palvelimia, joille olisi ollut tarpeen välittää palvelimen tiedostoja, ei erillisiä tallennuspalvelimia, eikä sen paremmin UNIX kuin Macintosh tietokoneitakaan.

Tällä palvelulla on nimensä mukaisen palvelun lisäksi myös vähemmän tunnettu ominaisuus, joka on se, että tämän palvelun lisäetuna saadaan mahdollisuus määrittää kullekin kansiolle käyttäjäkohtaiset suurimmat sallitut tiedostomäärät. Tämä ominaisuus on melko helppo ottaa käyttöön. Tämä tapahtuu siten, että klikataan hiiren oikealla napilla halutun hakemiston päällä, ja näin aukeavasta ikkunasta valitaan ominaisuudet (properties). Tässä ikkunassa klikataan välilehteä, jossa lukee quota ja tässä välilehdessä voidaan määrittää käyttäjäkohtaiset tallennusrajoitukset ko. kansioon.

10.3. TULOSTUSPALVELU

Verkkotulostimien osoitteiksi päätin jättää osoitevälin 3 – 9. Näistä otettiin käyttöön ensivaiheessa osoitteet 192.168.0.7 - 192.168.0.9. Varsinaisten tulostinajureiden kanssa oli alussa melkoisia vaikeuksia saada ne asennettua siten, että työasemat pystyisivät käyttämään näitä tulostusajureita verkon läpi. Yrittäessäni asentaa verkkokirjoittimia Windows 2003 palvelimelle kirjoittimien ohjaintiedostoja Windows XP:lle ja Windows

2000:lle, niin onnistuin ne kyllä asentamaan palvelimelle ja palvelimelta pystyi tulostamaan verkkokirjoittimille aivan normaalisti. Kun näitä ohjaintiedostoja sitten yritti sitten käyttää XP/2000 työasemilta, niin palvelin vastasi, ettei ko. käyttöjärjestelmän ohjaintiedostoja ole asennettu palvelimelle. Ensin ajattelin, että palvelin tulee käynnistää uudelleen ohjaintiedostojen asennuksen jälkeen, mutta kun uudelleenkäynnistäminenkään ei auttanut, sillä senkään jälkeen käyttäjät eivät pystyneet käyttämään verkkokirjoittimia. Ratkaisu, jolla tämä ongelman ratkaisin, oli se että, lisäsin ohjaimet manuaalisesti palvelimelle.

10.4. WINS PALVELU

Wins palvelu asennettiin siksi, että näin saatiin toimialueen sisäistä liikennettä nopeutettua erityisesti niissä tapauksissa, joissa sekä lähettävä että vastaanottava tietokone on toimialueen sisällä. Tätä palvelua ei välttämättä tarvita, mutta liikenteen sujuvuuden varmistamiseksi asensin sen. Tämänkaltaista sisäistä liikennettä on esim. tulostaminen verkkokirjoittimelle.

Wins palvelimia päätettiin asentaa vain yksi, koska verkon laitteiden määrä on varsin pieni. Wins palvelu pystyy vastaaman n. 300 rekisteröintiin/s tai 350 kyselyyn/s, joten yksi wins palvelin pystyy suoriutumaan kaikista verkkokyselyistä varsin helposti. Lisäksi tässä verkossa ei ole kuin yksi ainoa osoiteavaruus käytössä, joten senkään tehden ei ole tarvetta pitää kahta WINS palvelua verkossa.

Tämän palvelun asennus oli vielä yksinkertaisempaa kuin tiedostopalvelun asennus, koska tässä ei tullut ensimmäistäkään kohtaa, jossa olisi täytynyt valita eri vaihtoehdoista..

10.5. DHCP PALVELU

Varsinaisen DHCP palvelun asennus oli varsin helppo, koska sen asennusohjelmisto antoi varsin hyvät ohjeet, joita noudattamalla pääsi varsin helpolla. Ensimmäiseksi tämän palvelimen asennusohjelma kysyi DHCP:llä jaettavien osoitteiden aloitus ja lopetus osoitteet, joiksi määritin aloitusosoitteeksi 192.168.0.1 ja lopetusosoitteeksi 192.168.0.254.(kuva 12) Aliverkon osoitteeksi määritin 255.255.255.0 eli /24. Tämän

jälkeen ohjelma kysyi, mitä osoitteita edellä määritellystä osoitesarjasta jätetään pois. Näiksi osoitteiksi määritettiin 192.168.0.1 – 192.168.0.9 (kuva 13), jotka näin varattiin sekä palvelimille (osoitteet 192.168.0.1- 192.168.0.2) että verkkotulostimille (192.168.0.3- 192.168.0.9). Seuraavaan asennusohjelman ikkunaan määritettiin kuinka kauan tietokone hallinnoi dynaamista osoitettaan eli kuinka kauan tietty osoite on tietokoneella käytössä, ilman sen uusintapyyntöä(kuva 14). Täksi arvoksi määritin 12 tuntia, koska näin saatiin riittävän pitkä ajanjakso siinäkin tapauksessa, että osoitevaranto alkaa käydä vähiin.

Helpon alun jälkeen ohjelma kysyi, haluanko määrittää lisämäärityksiä, jotka siirretään osoitetietojen mukana työasemalle.(kuva 15) Tähän pystyi vastaamaan vain joko kyllä tai ei. Valitsin, että kyllä haluan määrittää nämä lisäasetukset, koska näin pystyin määrittämään oletusreititimen ja DNS palvelimen osoitteen. Lisäksi pystyin määrittämään WINS palvelussa käytettävän osoitteen ilman, että se täytyi käydä määrittämässä jokaiseen tietokoneeseen erikseen.

Ensimmäisessä varsinaisessa asetusikkunassa ohjelma kysyi oletusreititintä. tähän annoin osoitteen 192.168.0.1, joka on oletusyhdyskäytävän osoite.(kuva 16) Seuraavassa ikkunassa kysyttiin DNS palvelun tietoja. Tähän ikkunaan pystyi antamaan toisen seuraavista tiedoista; toimialueen juuridomainin nimen tai DNS palvelimen nimen / osoitteen. Näistä valitsin palvelimen nimen, koska palvelimen osoite saattaa muuttua, mutta harvemmin muuttuu palvelimen nimi. (kuva 17) Viimeisessä asetuksien antoikkunassa kysyttiin WINS palvelun palvelimen nimeä / osoitetta. Tässä kohtaa syötin nimen edellisen kohdan perusteluiden kera. (kuva 18)

11. PALVELUIDEN HALLINTA

Manage Your server ikkunasta myös hallitaan asennettuja palveluita, jotka on asennettu palvelimeen. Hallinta tapahtuu siten, että ensin klikataan hiirellä palvelun nimeä, jota halutaan muokata. Tämän jälkeen aukeaa valikko, josta klikataan manage this ? server, jossa kysymysmerkin kohdalla on muokattavan palvelun nimi.

Mikäli halutaan poistaa jokin jo asennettu palvelu, niin sekin tapahtuu Manage Your server ikkunan avulla. Palvelun poisto on hyvin pitkälle samanlainen velhon avulla suoritettava toimenpide kuin sen asennuskin. Poistettava toiminto valitaan hallintaikkunasta ja tämän jälkeen asennusohjelma suorittaa ohjatun poiston kysyen tiedot, joita ohjelma tarvitsee.

12.KÄYTTÖOPASTUS

Käyttöönoton ensimmäisessä vaiheessa kävimme läpi aivan perusasioita, kuten miten palvelinpohjaiseen verkkoon kirjaudutaan, miten tiedostoja tallennetaan palvelimella olevaan omaan kansioon ja miten palvelimelle tallennettuja tiedostoja haetaan käytettäväksi. Käyttöönoton ensimmäisessä vaiheessa käyttäjien enemmistö oli varsin epätietoisia siitä, miksi ”hyvä vanha” systeemi tulisi unohtaa. Heillä oli perusajatuksena se että, he eivät millään opi käyttämään uutta systeemiä, koska se vaatii liikaa uusien asioiden opiskelua.

Seuraava asia, joka heille tuli uutena asiana se, että heille oli jokaiselle määritetty henkilökohtainen hakemisto, jonne ei pääse kuin ko. kansion omistaja sekä järjestelmänvalvoja. Tästä syntyi keskustelua, koska tähän asti kaikki olivat päässeet kaikkien käyttäjien kaikkiin tiedostoihin ja nyt siitä tavasta luovuttiin. Edellä mainitusta seikasta johtuen palvelimelle tehtiin tämän seurauksena kansiot, (2 kpl) joista toiseen talletetaan sellaiset tiedostot, jotka ovat kaikkien ohjaajien käytössä ja toiseen kansioon talletetaan sellaiset tiedostot, jotka ovat kaikkien käytettävissä. Käytettyään jonkin aikaa uutta systeemiä, sen käyttö oli muodostunut suurimmalle osasta käyttäjiä lähes rutiinitoiminnoksi.

Ensimmäinen varsinainen opeteltava asia, jonka kanssa käyttäjillä oli miettimistä, oli verkkokirjoittimien asennus koneelle. Asennuksen selvittäminen oli kuitenkin melko nopeasti selvitetty, koska miltei kaikki olivat ennestään asentaneet paikallisia kirjoittimia ja verkkokirjoittimen ainoa merkittävä poikkeama on se, että tällaisen asentamises-

sa tulee ensimmäisessä valintaikkunassa valita kohta verkkotulostin tai toiseen tietokoneeseen kytketty tulostin. Seuraava kohta, jossa on tehtävä valinta, onkin jo sitten halutun tulostimen valinta aukeavasta valikosta.

Vianhaku olikin jo asia, joka oli tarpeen käydä läpi varsin rauhallisesti, johtuen käyttäjien varsin niukasta kokemuksesta ko. asian tiimoilta. Ensimmäiseksi asiaksi tuli näyttää kuinka käyttäjät pystyvät selvittämään, onko heillä yhteyttä palvelimeen. Tämän sain opastettua sillä tavoin, kun kysyin kuinka moni tietää, mikä on ”musta ruutu” ja moniko tietää, mitä kaikkea siinä voi tehdä. Näin sain selvitettyä sen että, miltei kaikki tiesivät ”mustan ruudun”, mutta monikaan ei tiennyt sen monipuolisista käyttömahdollisuuksista vianetsinnässä.

Tämän selvityksen jälkeen olikin sitten komentojen ipconfig ja ping käyttöopastus. Näiden komentojen idean selvittelyn jälkeen oli vuorossa käytännön kokeilua näistä komennoista, siten että pyysin käyttäjiä käymään vaikka kahvilla ja tällä välin kävin ”tekemässä” muutamia ”vikoja” joita he sitten alkoivat itsenäisesti selvittää.

Tämän jälkeen selvitin samalla tavoin kuinka he pystyvät selvittämään, onko heillä yhteyttä oman verkon ulkopuolelle. Mikäli käyttäjä ei saanut yhteyttä palvelimeen, niin ensimmäiseksi annoin muutaman vaihtoehdon, joista yksi oli virheen korjaava. Näin he joutuivat itse miettimään ja selvittämään vikoja, joita heille mahdollisesti syntyy. Tämä oli minusta helpoin tapa opettaa virheenetsintää ja korjausta lähiverkossa.

Seuraava asia, johon he halusivat opastusta, oli miten selvittää mihin heillä oli oikeudet tallentaa työnsä. Tämän ”ongelman” ratkaisun avaimena oli se että, selvitin mikä oli ongelma. Tämä oli epätietoisuus siitä että, nyt heillä olisi kullakin oma kansio varattuna omaan käyttöön, eikä heidän siis tarvinnut enää tallentaa tiedostoa X koneelle Y hakemistoon Z, vaan he voisivat tallentaa kaikki tiedostot yhdelle ja samalle palvelimelle.

13.LOPPUPÄÄTELMÄT

Palvelimen hankinta oli varsin opettavainen kokemus siitä, millainen työmäärä on yhden tarjouskilpailun läpikäynti. Moni sellainen asia, jonka olin pitänyt varsin yksinkertaisena asiana, osoittautui melko paljon aikaa ja työtä vaativaksi, kun hankina on julkinen. Parhaiten asiaa kuvaa ehkä se, että jo tarjouskilpailun suunnitteluvaiheessa tulee kaikkia mahdolliset tarjouskilpailun osanottajia kohdella tasaveroisesti.

Palvelimen käyttöönotto oli melko helppo, koska palvelimen toimittaja oli asentanut palvelimen siihen tasoon, että tämä käynnistyi suoraan normaalitilaan. Tehtäväkseni jäi konfiguroida tarvittavat palvelut käyttövalmiiksi.

Palveluiden konfiguroinnissa suurimmat vaikeudet olivat tarvittavien käyttö-oikeuksien määrittäminen kullekin käyttäjälle, koska osalla käyttäjistä oli tarpeen antaa järjestelmänvalvojan oikeudet, jotta nämä pystyvät hallinnoimaan yhdistyksen verkkoa. Lisäksi vaikeuksia oli DNS palvelun konfiguroinnissa niin, että sen toimivuus olisi riittävän vahvalla pohjalla.

Palvelimen käyttöopastus käyttäjille oli yllättävän monimutkaista, johtuen käyttäjien varsin monitasoisesta kokemuksesta tietokoneen käytössä. Tämän ongelman ratkaisu oli se, että koulutustilaisuuksia pidettiin siten, että kussakin ryhmässä oli suunnilleen saman tietomäärän hallitsevia henkilöitä. Näin saatiin käyttäjien enemmistö suunnilleen samalle tasolle järjestelmän käytön suhteen.

14.LÄHDELUETTELO

Microsoft Windows Server 2003 Active Directory
http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/default.mspx

Windows Server 2003 Tecnical Library
http://technet2.microsoft.com/WindowsServer/en/Library/1fd5b3be-ca29-43d0-b5e2-8a65192d5b781033.mspx?mfr=true

Windows 2003 R2 help
http://technet2.microsoft.com/WindowsServer/en/Library/459af84b-3a3a-42d7-93ed-cc2120b8e9161033.mspx?mfr=true

DNS
http://support.microsoft.com/default.aspx?scid=kb;en-us;825036

WLAN
http://fi.wikipedia.org/wiki/802.11

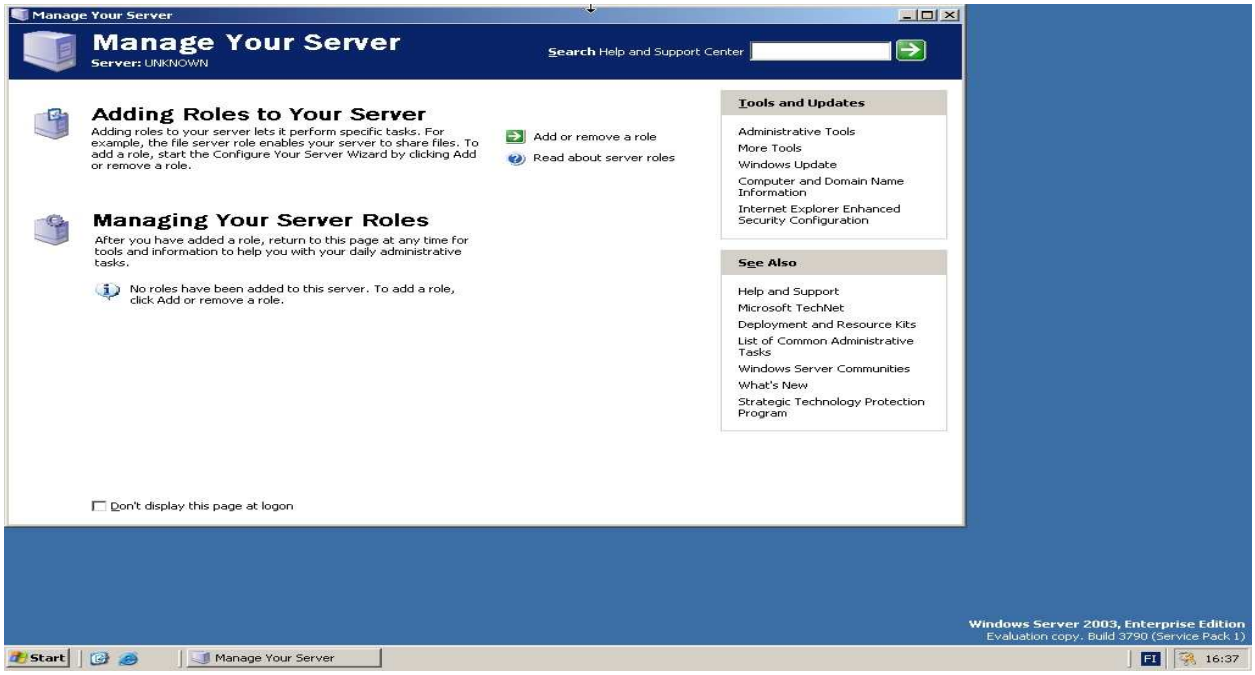
Stanek, William R. 2003. Microsoft Windows server 2003 asiantuntijan käsikirja. Helsinki. Edita Prima OY

Stanek, William R. 2001 Microsoft Windows server 2000 verkonhaltijan käsikirja. Helsinki. Edita

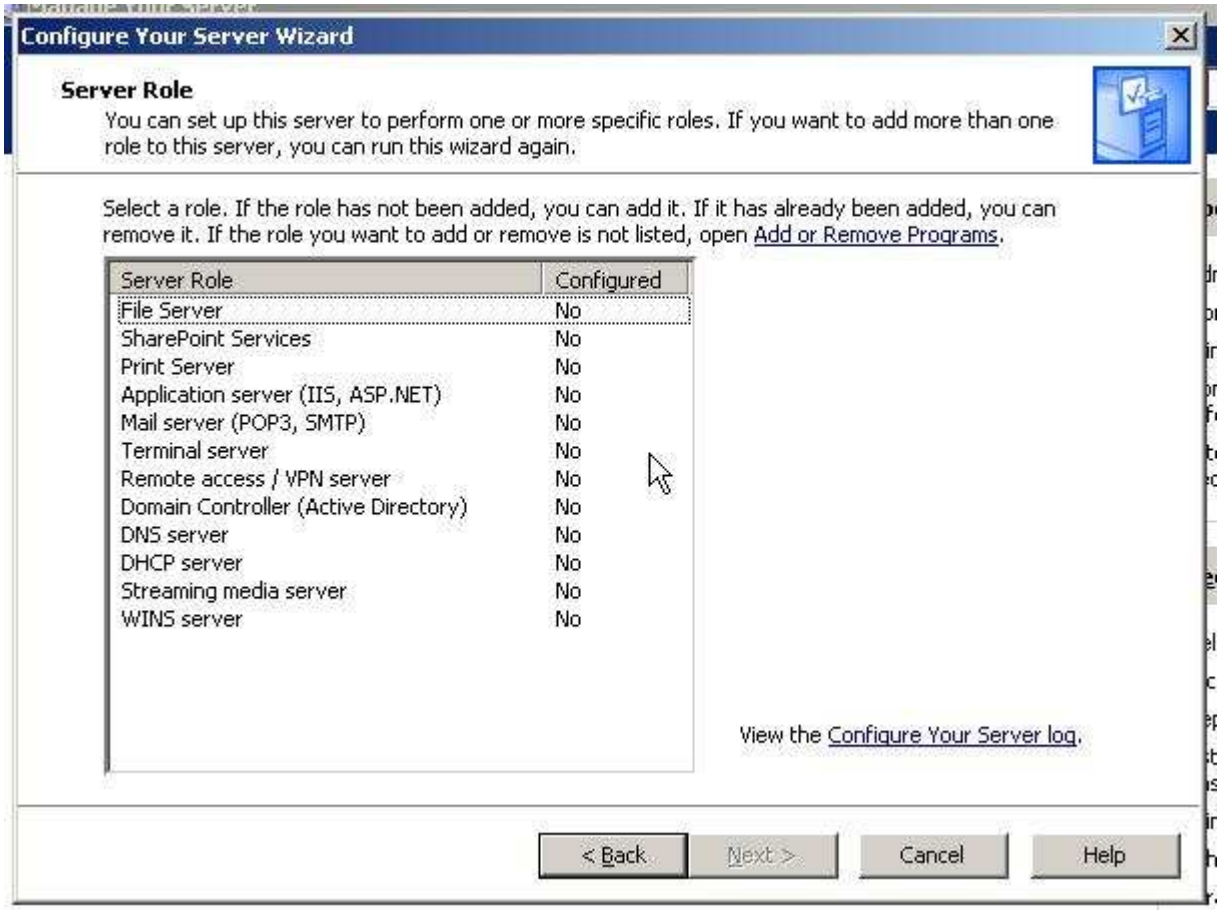
Ruohonen, M. 2002 Tietoturva. Porvoo. WS Bookwell

15. LIITTEET

kuva 1



kuva 2



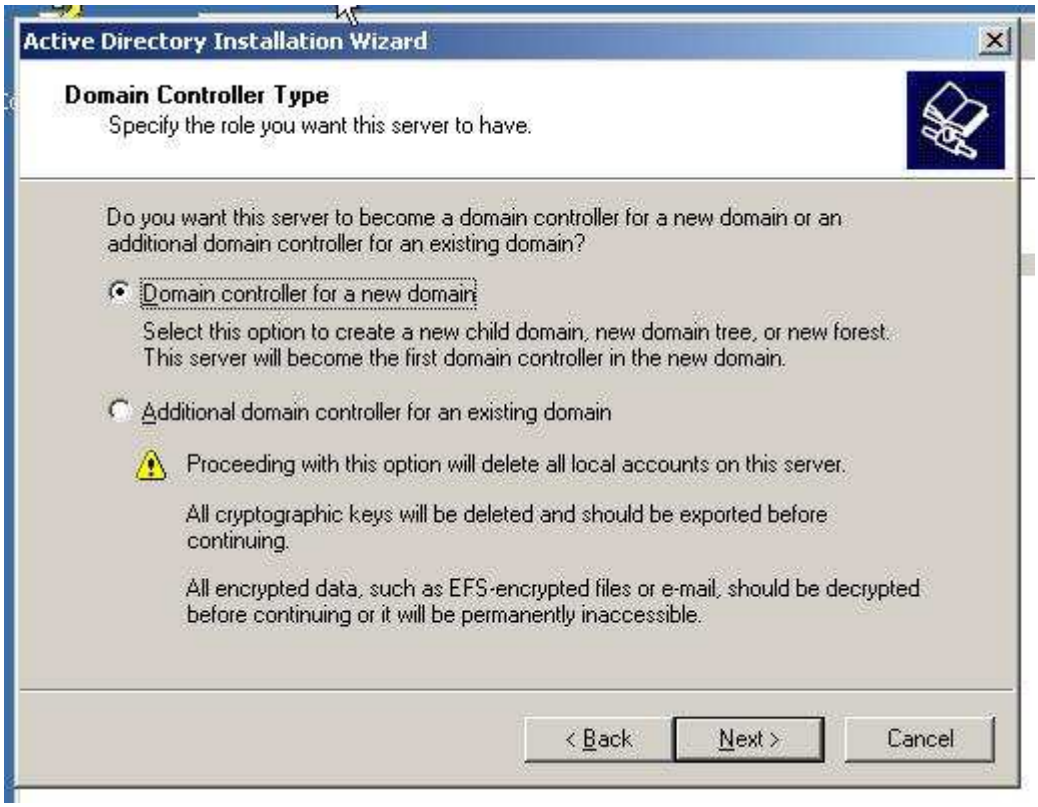
kuva 3


Active Directory Installation Wizard
Permissions
Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< Back
Next >
Cancel

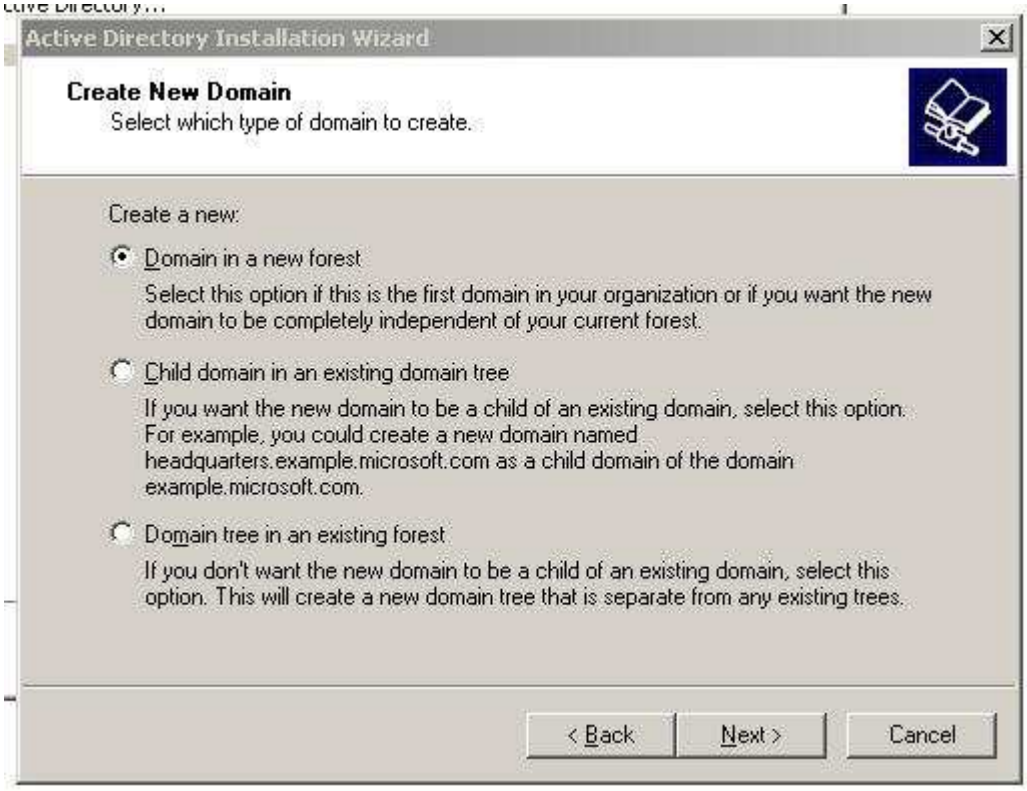
kuva 4


Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see Active Directory Help.
< Back
Next >
Cancel

kuva 5


Active Directory Installation Wizard
Domain Controller Type
Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< Back
Next >
Cancel

kuva 6


Active Directory Installation Wizard
Create New Domain
Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< Back
Next >
Cancel

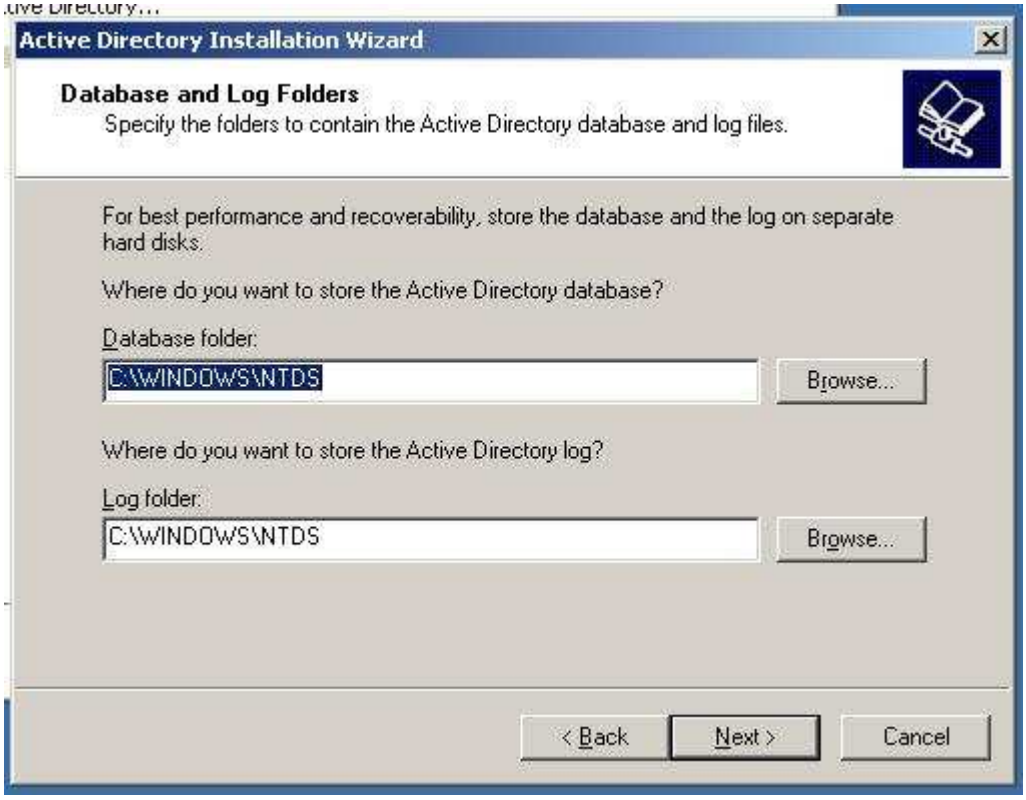
kuva 7


Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
< Back
Next >
Cancel

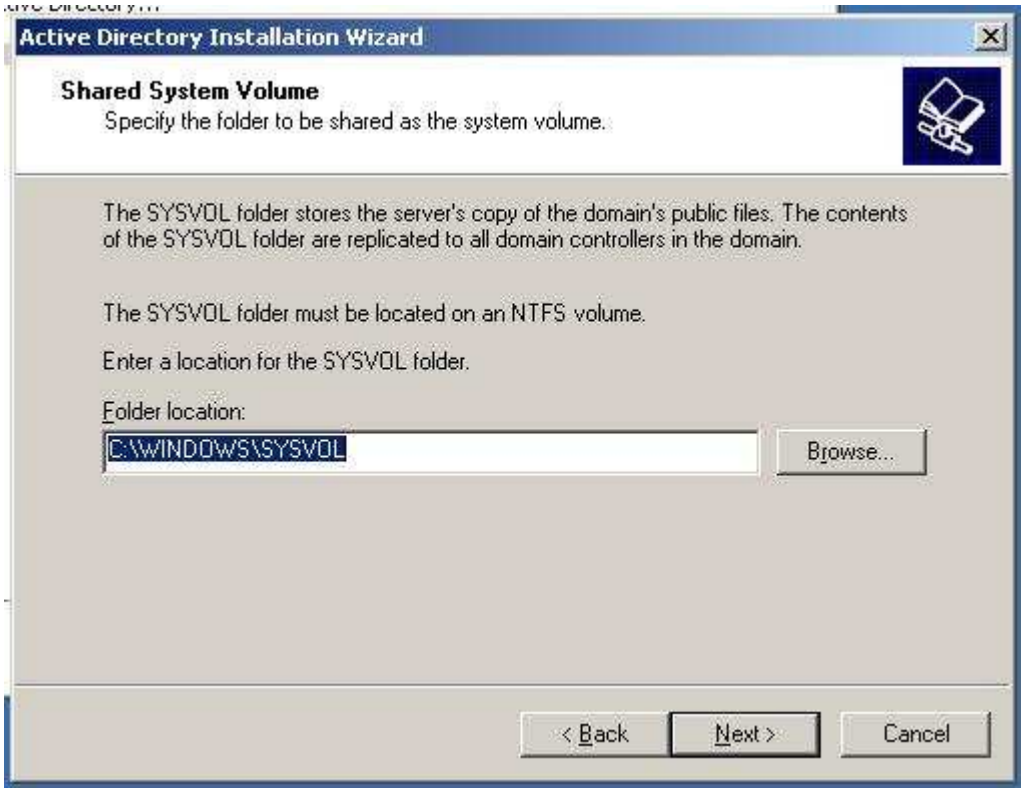
kuva 8


Active Directory Installation Wizard
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name:
TUKIRANKA
< Back
Next >
Cancel

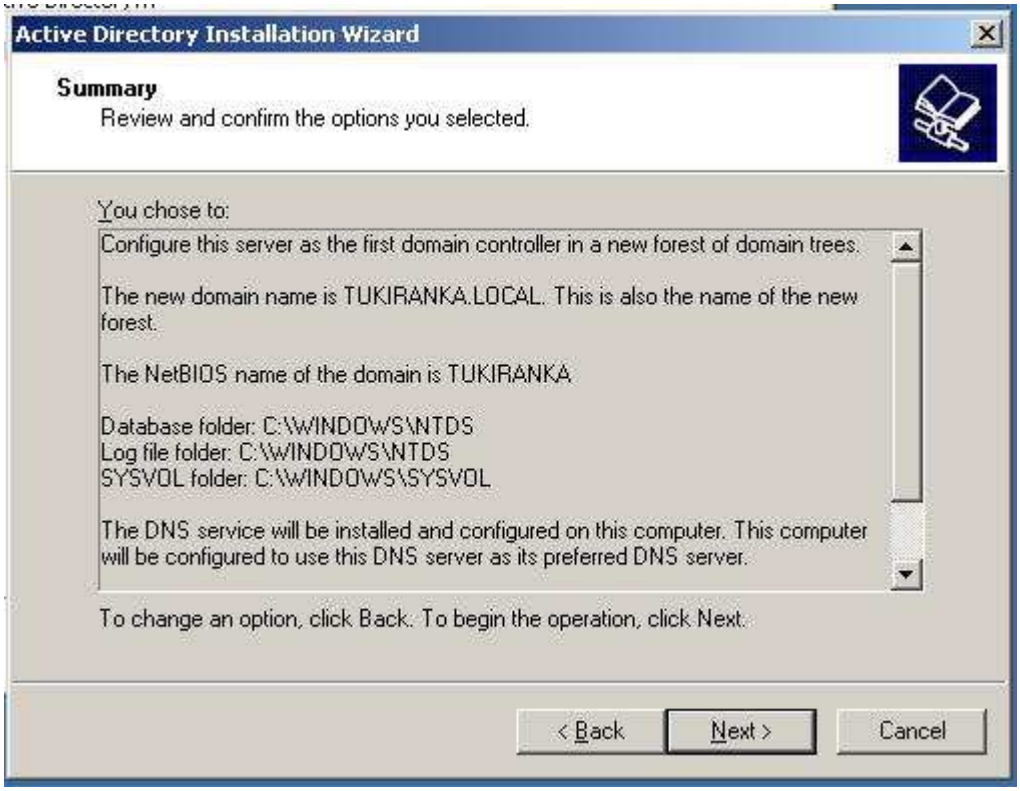
kuva 9



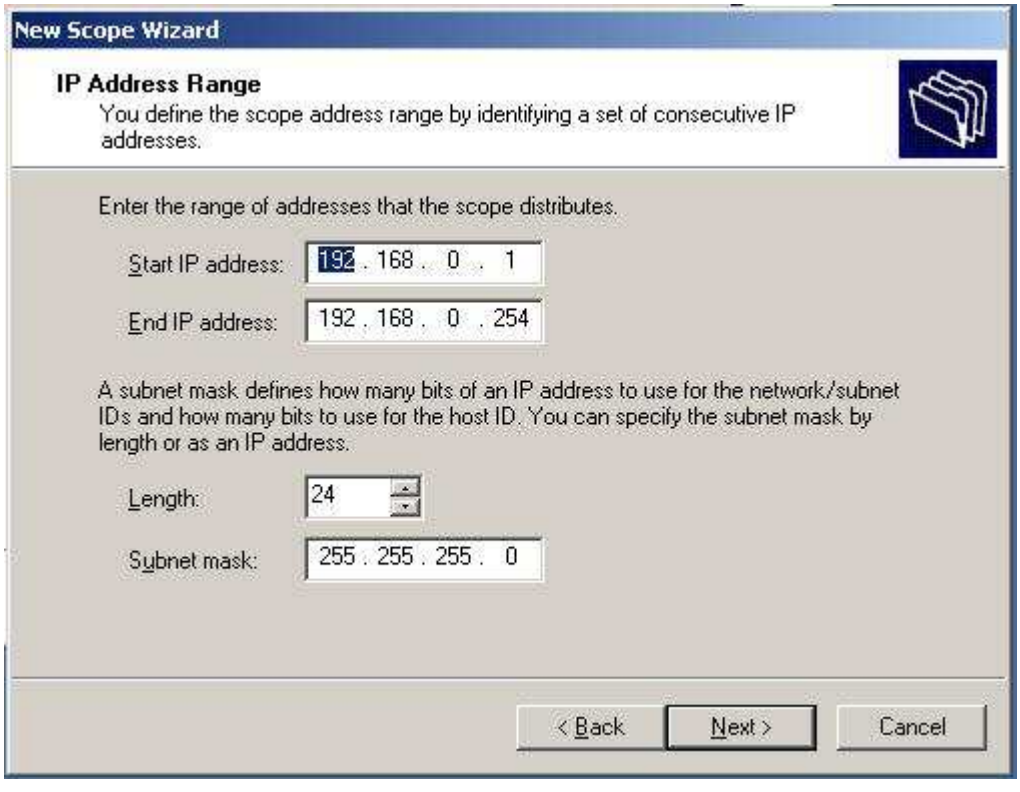
kuva 10



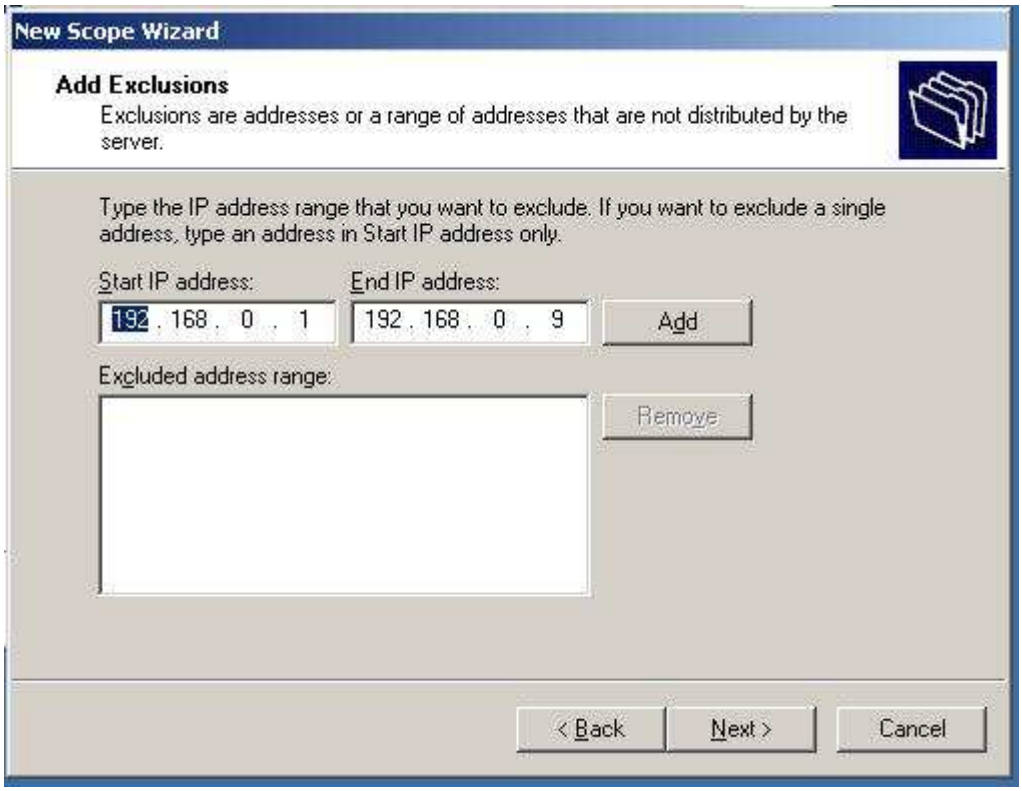
kuva 11



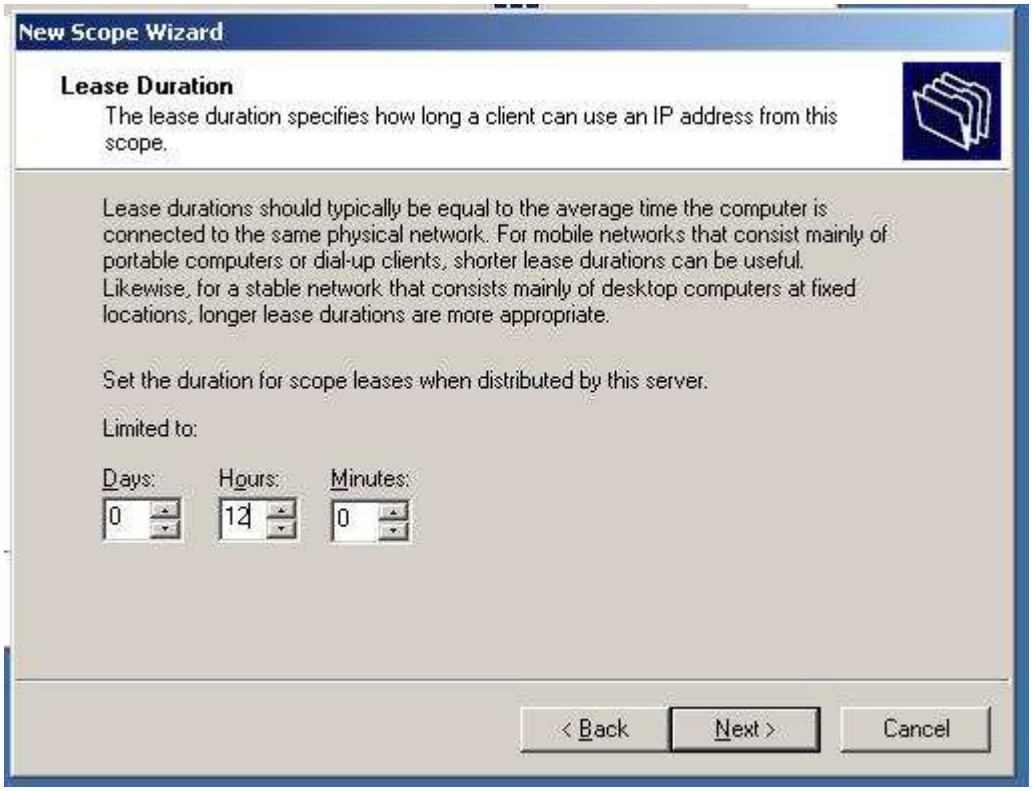
kuva 12



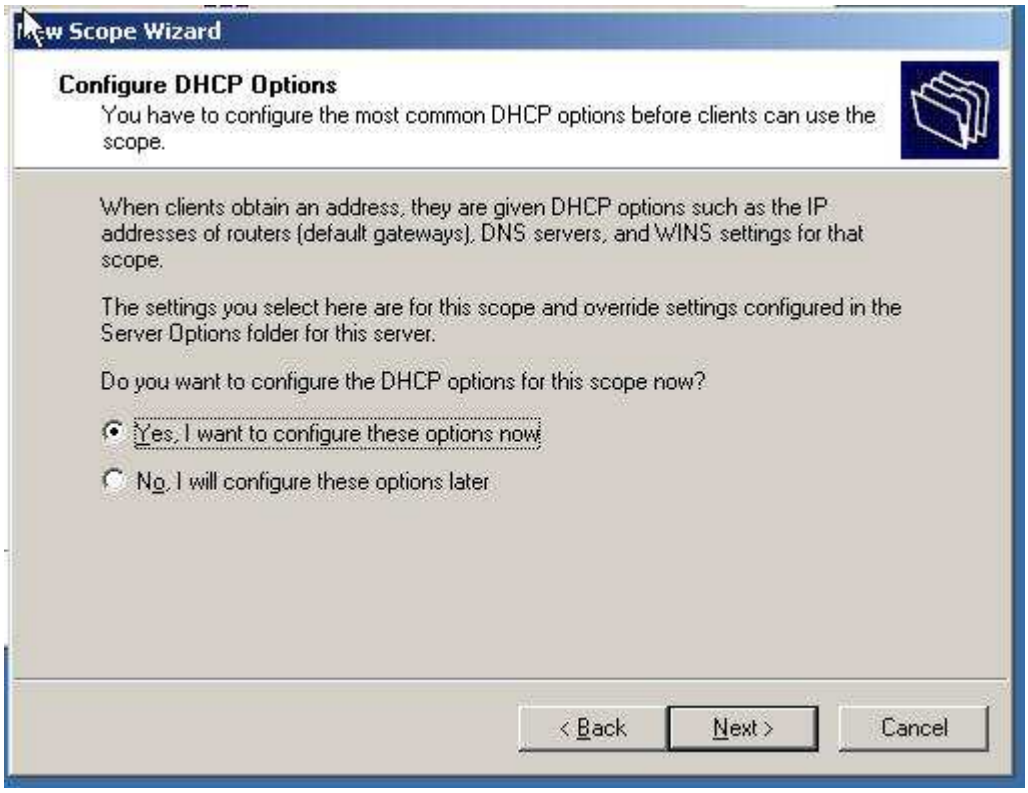
kuva 13



kuva 14

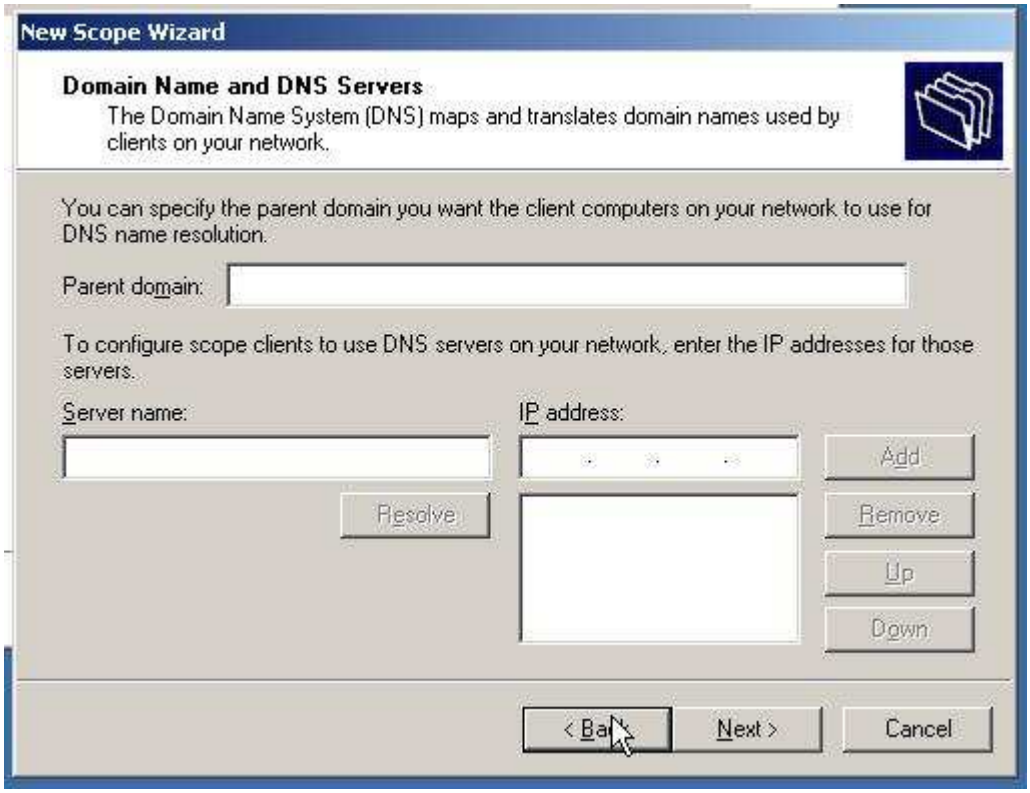


kuva 15



kuva 16

kuva 17



kuva 18

kuva 19

kuva 20