



## **TEKNIikka JA LIIKENNE**

**Tietotekniikka**

**Tietoverkot**

## **INSINÖÖRITYÖ**

### **MICROSOFT OFFICE COMMUNICATIONS SERVER 2007 R2 -KÄYTTÖÖNOTTO**

**Työn tekijä: Jari Silvo**  
**Työn ohjaajat: Marko Uusitalo**  
**Matti Kurki**

**Työ hyväksytty: \_\_\_\_. \_\_\_\_. 2010**

**Marko Uusitalo**  
**lehtori**



## **ALKULAUSE**

Tämä insinööryö tehtiin TimeMill Oy:lle. Kiitän mahdollisuudesta insinööryön tekemiseen. Kiitokset työnohjaajille Marko Uusitalolle ja Matti Kurjelle. Kiitokset Joni Reitamolalle testijärjestelyistä.

Helsingissä 27.5.2010

Jari Silvo

## TIIVISTELMÄ

<b>Työn tekijä:</b> Jari Silvo	
<b>Työn nimi:</b> Microsoft Office Communications Server 2007 R2 -käyttöönotto	
<b>Päivämäärä:</b> 26.4.2010	<b>Sivumäärä:</b> 42 s.
<b>Koulutusohjelma:</b> Tietotekniikka	<b>Suuntautumisvaihtoehto:</b> Tietoverkot
<b>Työn ohjaaja:</b> Lehtori Marko Uusitalo  <b>Työn ohjaaja:</b> Matti Kurki	
<p>Videoneuvottelujärjestelmien kysynnän kasvaessa on ajankohtaista suunnitella myös kattavampaa yhdistetyn viestinnän (unified communications) ratkaisua. Videoneuvottelujärjestelmiä on saatavilla useilta laitevalmistajilta, jotka perustuvat eri standardeihin. Tämän insinööriyön tarkoituksena on luoda Microsoft Office Communications Server R2 -ympäristö, jossa testataan myös yhteensopivuutta Tandbergin videoneuvottelujärjestelmän kanssa.</p> <p>Insinööriyö tehtiin TimeMill Oy:lle tarkoituksena kehittää toimiva ratkaisu yhdistettyyn viestintään. Työssä on tutkittu Office Communications Server -ohjelmistoa ja yhdistettyä viestintää myös testiympäristössä laajemmassa kokonaisuudessa.</p> <p>Insinööriyön teoriaosuus tehtiin kirjallisuustutkimuksena. Teoriaosuudessa selvitetään keskeisten protokollien toimintaa ja Office Communications Serverin ominaisuuksia sekä toiminnallisuutta. Teoriaosuuden lopussa kerrotaan testiympäristön käyttöönotosta, asennusvaiheista sekä tuloksista.</p>	
<b>Avainsanat:</b> Yhdistetty viestintä, OCS, SIP, TLS, Tandberg	

## ABSTRACT

<b>Name:</b> Jari Silvo	
<b>Title:</b> Microsoft Office Communications Server 2007 R2 deployment	
<b>Date:</b> 26.4.2010	<b>Number of pages:</b> 42
<b>Department:</b> Information technology	<b>Study Programme:</b> Data networks
<b>Instructor:</b> Senior Lecturer Marko Uusitalo	
<b>Supervisor:</b> Matti Kurki	
<p>As demand for videoconferencing systems grows, it is useful to design a comprehensive unified communications solution. Videoconferencing systems are available from several device manufacturers, based on different standards. The purpose of this study is to create a Microsoft Office Communications Server R2 environment. This environment is also tested for compatibility with Tandberg videoconferencing system.</p> <p>This study was carried out for TimeMill Oy. The main objective was to create functional solution for unified communications. I studied Office Communications Server and unified communications also in a wider perspective.</p> <p>The theoretical part of the thesis is based on key protocols of Office Communications Server. This part explains SIP and TLS protocols, Office Communications Server features and functionality. The theoretical part also covers deployment of the test environment, Office Communications Server installation steps, and the test results.</p>	
<b>Keywords:</b> Unified Communications, OCS, SIP, TLS, Tandberg	

## SISÄLLYS

### ALKULAUSE

### TIIVISTELMÄ

### ABSTRACT

<b>1</b>	<b>JOHDANTO</b>	<b>1</b>
<b>2</b>	<b>YHDISTETTY VIESTINTÄ</b>	<b>2</b>
<b>3</b>	<b>OFFICE COMMUNICATIONS SERVER</b>	<b>3</b>
<b>3.1</b>	<b>Ominaisuudet</b>	<b>3</b>
3.1.1	<i>Enterprise Voice</i>	4
3.1.2	<i>Group Chat</i>	4
3.1.3	<i>Kuvanlaatu ja koodekit</i>	4
3.1.4	<i>Tarvittava kaistanleveys</i>	6
<b>3.2</b>	<b>Toiminta</b>	<b>7</b>
3.2.1	<i>SIP</i>	8
3.2.2	<i>TLS</i>	11
<b>3.3</b>	<b>Kilpailijat</b>	<b>14</b>
<b>4</b>	<b>TESTIYMPÄRISTÖ</b>	<b>15</b>
<b>4.1</b>	<b>Palvelimien käyttöjärjestelmä asennus</b>	<b>16</b>
4.1.1	<i>Ohjauspalvelimen asennus</i>	17
4.1.2	<i>PKI julkisen avaimen infrastruktuuri</i>	18
4.1.3	<i>OCS-palvelimen asennus</i>	20
<b>4.2</b>	<b>OCS-asennus ja käyttöönotto</b>	<b>21</b>
4.2.1	<i>Active Directoryn valmistelu</i>	21
4.2.2	<i>DNS-tietueet</i>	24
4.2.3	<i>Server 2008:n valmistaminen asennukseen</i>	27
4.2.4	<i>Office Communications Server 2007 R2 Standard Edition -asennus</i>	28
4.2.5	<i>Käyttäjien luonti ja aktivointi</i>	36
<b>4.3</b>	<b>Microsoft Office Communicator R2</b>	<b>37</b>
<b>4.4</b>	<b>Tandbergin yhteentoimivuus OCS-ympäristössä</b>	<b>40</b>
<b>5</b>	<b>YHTEENVETO</b>	<b>42</b>
	<b>LÄHTEET</b>	

## LYHENTEET JA MÄÄRITELMÄT

C20	Tandbergin koodekki.
FQDN	Fully Qualified Domain Name - Täysi domainnimi.
HD	High Definition. Työssä viitataan HD-lyhenteellä videoresoluutioon 1270 x 720 eli 720p.
IM	Instant Messaging. Tekstipohjaiset pikaviestit.
MXP	Erään Tandbergin videoneuvottelujärjestelmän mallinimi.
OCS	Office Communications Server. Microsoftin yhdistetyn viestinnän kulmakivi.
SIP	Session Initiation Protocol. Signaointi protokolla, jolla luodaan IP-pohjaisia istuntoja.
STUN	Session Traversal Utilities for NAT. STUN-protokolla mahdollistaa erilaisten sovellusten toiminnan NAT-osoitteen muunnoksen läpi. STUN havaitsee verko NAT-asetukset. STUN tarvitsee toimiakseen erillisen STUN-palvelimen.
TLS	Transport Layer Security Protocol. IP-verkoissa kulkevien sovellusten salaukseen tarkoitettu protokolla.
TURN	Traversal Using Relay NAT. TURN-protokolla mahdollistaa TCP ja UDP liikenteen palomuurin ja NAT-osoitteen muunnoksen läpi.
UC	Unified Communications. Yhdistetty viestintä
VCS	Tandbergin Video Communication Server. VCS on gatekeeper-laite, joka mahdollistaa vanhalla h.323-standardilla toimivien laitteiden yhteentoimivuuden SIP-ympäristön kanssa.

## 1 JOHDANTO

Useat yritykset ovat ottaneet käyttöönsä erilaisia videoneuvottelujärjestelmiä. Videoneuvottelujärjestelmät ovat osa yhdistetyn viestinnän kokonaisuutta. Yritykset, jotka ovat kokeneet videoneuvottelujärjestelmien tuomat hyödyt, ovat alkaneet kiinnostua laajemmin yhdistetystä viestinnästä. Yksinkertaisten yhdistetyllä viestinnällä tarkoitetaan usean viestintätekniikan lähentymistä yksittäiseksi ratkaisuksi. Viestintätekniikoita ovat muun muassa sähköposti, pikaviestit, ääni- ja videopuhelut, kalenterit ja tekstiviestit. Yhdistetyn viestinnän ratkaisuilla pyritään mm. säästämään kustannuksia, resursseja sekä tehostamaan liiketoimintaa.

Yhdistetyn viestinnän kokonaisratkaisuja tarjoavia suuria yrityksiä ovat Gartnerin mukaan mm. Microsoft, Cisco ja IBM. Nämä yritykset pyrkivät tuomaan omat sovelluksensa mahdollisimman monelle eri alustalle, ja yhteensopivuutta pidetään tärkeänä. Yhdistetyn viestinnän tarjoajat ovat eri mieltä ainakin siitä, mikä alusta on yhdistetylle viestinnälle tärkein. Esimerkiksi Nokialla panostetaan enemmän matkapuhelin sovelluksiin kuin tietokonepohjaisiin sovelluksiin.

Tässä insinööriyössä on tarkoitus luoda Microsoftin Office Communications Server 2007 R2 -ympäristö ja testata sen eri ominaisuuksia ja yhteensopivuutta Tandbergin videoneuvottelujärjestelmän kanssa. Microsoftin Office Communications Server (OCS) on oleellinen osa Microsoftin yhdistetyn viestinnän ratkaisua. OCS:n toiminnallisuuteen kuuluu mm. videokonferenssi, joka mahdollistaa videoneuvottelun usean tietokoneen välillä. Tämän toiminnallisuuden yhteensovittaminen Tandbergin videoneuvottelujärjestelmään on osa tutkimustani.

Teoriaosuudessa käydään läpi yhdistettyä viestintää, Office Communications Serverin toiminnallisuutta ja SIP- ja TLS-protokollien toimintaperiaatteet. SIP- ja TLS-protokollat ovat oleellinen osa OCS:n toimintaa. Tarkoituksena on myös selvittää OCS:n tietoturvaominaisuudet. Insinööriyön loppuosa sisältää testiympäristön luomisen eri vaiheet, testatut ominaisuudet ja testaustulokset.

## TimeMill Oy

TimeMill Oy on vuonna 2008 perustettu helsinkiläinen videoviestintään erikoistunut yritys, joka toteuttaa asiakkailleen kaikenkattavia videoneuvottelupalveluita. TimeTraveller on kokonaispalvelu, johon sisältyvät kaikki videoneuvotteluun tarvittavat komponentit. Tandberg toimittaa videoneuvottelussa käytettävät päätelaitteet, kuten kamerat ja koodekit. TimeTraveller -asiantuntijapalveluita ovat mm. suunnittelu, tilaratkaisut, asennuspalvelut, koulutuspalvelut ja konsultointi.

## Tandberg

Tandberg on vuonna 1933 perustettu norjalainen tietoliikenneyritys, joka on nykyään erikoistunut videoneuvottelujärjestelmiin. Tandberg tarjoaa videoneuvottelu- sekä telepresence-järjestelmien lisäksi mm. henkilökohtaista viestintää ja lisälaitteita.

## Insinööriyön tavoitteet

Tämän työn tavoitteena on rakentaa toimiva Office Communications Server 2007 R2 Standard -ympäristö kehitysmahdollisuudet huomioiden. OCS-ympäristön yhteensopivuutta Tandbergin videoneuvottelulaitteiden kanssa on tarkoitus testata Tandberg MXP 1700, VCS ja C20-laitteilla.

## 2 YHDISTETTY VIESTINTÄ

Yhdistetty viestintä tarkoittaa pääpiirteissään erillisten järjestelmien ja palveluiden yhdistämistä yksittäiseksi ja monipuoliseksi viestintäkokonaisuudeksi. Tällä kokonaisuudella viestitään tehokkaasti teksti-, ääni- ja videoviestein. Viestinnän tulee olla myös mahdollista erilaisten laitteiden välillä, kuten tietokoneiden, matkapuhelinten ja videoneuvottelujärjestelmien.

Yhdistetyn viestinnän (Unified Communications, UC) ratkaisuilla on mahdollista saavuttaa huomattavia säästöjä kustannuksissa ja resursseissa liiketoiminnasta riippuen. Yhdistetyssä viestinnässä viestinnän vaiheita tehostetaan ja täydennetään ohjelmallisesti sekä erilaisilla teknisillä ratkaisuilla. UniComm Consulting mukaan UC:n säästömahdollisuudet voidaan jakaa kolmeen luokkaan:

- välittömien kustannusten pienentäminen



- viestintäinfrastruktuurin yhdistäminen
- inhimillisen pääoman hyödyntäminen.

Välittömällä kustannuksilla tarkoitetaan erilaisia viestintäpalveluita esimerkiksi puhelinlaskuja, isännöityjä ääni- ja videoneuvotteluita sekä niihin liittyviä matka- ja toimistokuluja. Viestintäinfrastruktuurin yhdistämisessä säästöpotentiaali on pienin näistä kolmesta luokasta. Säästöjä perustellaan toimintakustannusten pienentämisellä uusien viestintä ratkaisujen integroiduilla toiminnoilla. Inhimillisen pääoman hyödyntämisen säästöt perustuvat tuottavuuden parantamiseen ja viestinnän turvallisuuteen. Matkakulut ovat yksi suurimmista säästöä tuovista yksittäisistä tekijöistä. Tandbergin mukaan useat organisaatiot ovat onnistuneet vähentämään matkustamista 30 prosenttia tai enemmän kunnollisen videoneuvottelujärjestelmän avulla. [9, s. 1 - 3.]

### **3 OFFICE COMMUNICATIONS SERVER**

Office Communications Server (OCS) on osa Microsoftin yhdistetyn viestinnän ratkaisua. Tähän kokonaisuuteen kuuluu tällä hetkellä myös seuraavat ohjelmistot ja palvelut:

- Microsoft Exchange Server 2010
- Microsoft Office Communicator 2007 R2
- Microsoft Exchange Server Online
- Microsoft Office Communications Server Online
- Microsoft Office Live Meeting
- Microsoft Exchange Hosted Services.

#### **3.1 Ominaisuudet**

OCS on Microsoftin yhdistetyn viestinnän kulmakivi, joka mahdollistaa läsnäolopalvelut, pikaviestinnän, konferenssit ja VoIP-palvelut. Läsnäolotiedot perustuvat kalenterimerkintöihin, kirjautumis- ja aktiivisuus-statukseen sekä käyttäjän asetuksiin. Konferensseilla luodaan virtuaalinen työtila, joka mahdollistaa reaaliaikaisen tiedon, videon, äänen ja tekstin jaon usean osallistujan välillä. Tarkastellaan kahta OCS:n ominaisuuksista tarkemmin. [3.]

### 3.1.1 *Enterprise Voice*

OCS:n VoIP on nimetty Enterprise Voice -palveluksi. VoIP-puheluita voidaan muodostaa Office Communicatorin lisäksi myös muista Office-sovelluksista, kuten Outlookista. Tavanomaisten puheluominaisuuksien lisäksi OCS VoIP:illa voidaan puhua usean osanottajan välillä sekä liittyä videokonferenssiin ilman kuvaa. Puheluasetuksilla voidaan välittää soittajalle useita tavoitettavuustietoja esimerkiksi useamman puhelinnumeron tai henkilön tiedot. OCS VoIP on tuettu myös matkapuhelimissa sovelluksilla Office Communicator Mobile R2 ja Office Communicator Mobile for Java.

Ryhmäpuhelu (Team Calling) on ominaisuus, jossa kaikkien ryhmän jäsenten puhelimet soivat, kun joku jäsenistä saa puhelun. Puhelimen soidessa kaikki jäsenet näkevät soittavan osapuolen tiedot ja ketä tavoitellaan. Puheluita voidaan myös valtuuttaa-avustajille. Valtuuttaja näkee myös, kuka on vastannut hänelle tuleviin puheluihin ja milloin.

Vastausryhmä (Response Groups) -palvelulla voidaan luoda useita vastausryhmiä. Vastausryhmäpalvelu osaa reitittää puhelut perustuen läsnäolotietoihin tai perinteisiin puhelinreititys algoritmeihin. Muita vastausryhmän palveluita ovat jonotus, musiikki ja puheentunnistus.

### 3.1.2 *Group Chat*

Ryhmäviestintä on usean henkilön välistä viestintää, jota säilytetään ja jatketaan pidemmän aikaa. Ryhmäviestintä mahdollistaa osallistujien yhteistyön, vaikka he työskentelevät eri aikoihin. Ryhmäviestinnässä käytetään hyväksi Office Communicatorin läsnäolotietoa ja käyttäjät voivat myös asetuksilla vaikuttaa, miten herkästi Group Chat -viesteistä ilmoitetaan. Tiedostonjako on mahdollista. Federaatio mahdollistaa myös muiden valmistajien chat-huoneiden liittymisen OCS Group Chatiin.

### 3.1.3 *Kuvanlaatu ja koodekit*

Office Communications Server 2007 R2 rajoittaa oletuksena Communicatorien välisien videopuheluiden kuvan VGA-tasolle resoluutiolla 640 x 480. Korkein Office Communicatorin tukema kuvan laatu on High-Definition (HD) -tasoa resoluutiolla 1270 x 720. Kuvan laatuun vaikuttavat asetukset säädetään OCS-palvelimesta. Asetuksilla voidaan myös rajata osallistujia videokuvan laadun perusteella. Office Communicator käyttää Microsoftin omaa RT

Video -koodekkia. Jotta HD-tason neuvottelu onnistuu, molempien osapuolten on tuettava RT-Videota. Testiympäristössä ei ollut tarpeeksi HD-tason videokameroita, joten pystyimme testaamaan vain VGA-resoluutiolla.

Office Communicatorin videopuhelut ovat laadukkaita. Videopuhelu muodostetaan oletuksena CIF-videoformaattilla resoluutiolla 352 x 288. Videon resoluutiota muutetaan Communicatorista vaihtamalla kuvan kokoa. Vaihtoehdot ovat small (CIF), large (VGA) ja full screen (HD).



Kuva 1. Puhelu cif-formaatissa

CIF-formaatilla videokuvan koko on tarpeeksi suuri, jotta henkilöt tunnistavat toisensa. Videon merkitystä lisää mahdollisuus kuvan suurentamiseen. VGA-tasolla kuva parani selvästi ja pysyi korkealaatuisena. Videon tai äänen pätkimistä ei esiintynyt testiympäristön sisäverkossa. Molempien asiakaskoneiden ollessa ulkoverkossa kuvaan tuli ajoittain hiukan pidempi viive, mutta katkon jälkeen videopuhelu jatkui normaalisti. Videon täytettäessä koko kuvaruudun resoluution tulisi olla HD-tasoista. HD-tason saavuttamiseksi työasemassa on oltava HD-tason videokamera ja työaseman on täytettävä riit-

tävät järjestelmävaatimukset. Mikäli työasemalla ei ole mahdollista saavuttaa HD-tason videokuvaa kokoruututila toistetaan VGA-tasolla, jolloin kuva pikselöityy selvästi. Pikselöityminen ei kuitenkaan estä videopuhelua ja käyttäjien kokema haitta on suhteellista.

Point-to-point -yhteyksissä OCS käyttää RT-Audio/RT-Video -koodekkeja. Lyhenne RT tulee sanoista Real-Time eli reaaliaikainen. Koodekit mukautuvat saatavilla olevan verkkokaistan mukaan. RT-Audio pystyy koodaamaan yksikanavaisia äänisignaaleja 16 bitin ääninäytteillä. Koodekki toimii joko kapealla taajuusalueella tai leveällä taajuusalueella. Kapea taajuusalue koostuu 8 kHz:n näytteenottotaajuudesta ja leveä 16 kHz:n näytteenottotaajuudesta. RT-Audiossa on myös Forward Error Correction eli FEC virheenkorjausta varten. RT Video -koodekki perustuu SMPTE VC-1 -koodekkiin, joka määritetään SMPTE 421M -standardissa. VC-1 perustuu diskreettiin kosinimuunnokseen ja Microsoftin mukaan VC-1-koodin purku on huomattavasti tehokkaampaa, kuin H.264-koodekin.

Audiokonferensseissa OCS-käyttää Siren-koodekkia. Koodekin on kehittänyt PictureTel Corporation. Siren-koodekkeja on kolmea erilaista Siren 7, Siren, 14 ja Siren 22. OCS-käyttää Siren 7 -koodekkia, jonka näytteenottotaajuus on 16 kHz. Koodekin tukemat nopeudet ovat 16, 24 ja 32 kbps. Siren 7 -koodekki on melkein identtinen G.722.1-koodekin kanssa.

Kolmen tai useamman henkilön kommunikoidessa on kyse konferenssista. Microsoftin OCS-ympäristössä tarvitaan konferenssiin multipoint control unit (MCU) -laitteisto. Videokonferenssia varten tarvitaan audio/video MCU (AV MCU) ja pikaviestejä varten tarvitaan IM (Instant Messaging) MCU. Tuottaessa MCU-laite OCS-ympäristöön kulkevat signaalintviestit kuten ennenkin, mutta kaikki media kulkee osanottajille MCU-laitteen kautta. AVMCU tukee vain RT VIDEO -koodekkia resoluutiolla 352 x 288 kuvataajuuden ollessa 15 fps (frames per second). Office Communicatorilla voidaan kuitenkin liittyä toisen valmistajan videokonferenssiin HD-tasoisella kuvalla. Kolmannen osapuolen laitteet, jotka rekisteröityvät OCS-palvelimelle, näkyvät OCS-ympäristössä vain yksittäisinä käyttäjinä. [11, s. 7; 52 - 53.]

#### 3.1.4 Tarvittava kaistanleveys

Yksi Office Communicator -käyttäjä varaa videopuhelun aikana verkkokapasiteettia maksimissaan noin 407 kilotavua sekunnissa. RT Audio -koodekin

viidessä 57 kilotavua sekunnissa ja RT Video –koodekin viidessä 350 kilotavua sekunnissa. Tämä laskelma perustuu Microsoftin testeissä saamiin tuloksiin tyypillisestä kaistantarpeesta. Mediavirrassa on huomioitu pakettien kehykset, salausta, IP-reititystiedot ja itse siirrettävä media. Laskelmassa käytetty videoformaatti on CIF (Common Intermediate Format) resoluutiolla 352 x 288. Microsoft ilmoittaa VGA-tasoisesta kuvan kaistantarpeeksi keskimäärin 600 kilotavua sekunnissa ja HD-tasoisesta kuvan 1500 kilotavua sekunnissa.

### 3.2 Toiminta

OCS:n tärkein protokolla on Session Initiation Protocol (SIP), joka on sovellustason merkinantoprotokolla. Viestintäistuntoa hallitaan SIP-protokollalla IP-verkossa. SIP aloittaa, hallitsee ja lopettaa viestintäistunnon. SIP-protokolla on määritelty IETF:n dokumentissa RFC 3261. [4, s. 8.]

OCS käyttää SIP-protokollaa pikaviestintään, konferensseihin, läsnäolotietoihin, videoon ja VoIP-puheluihin. PSTN-verkosta tulevat puhelut signaloidaan SIP-protokollalla PSTN-gatewaylla. SIP-istunnoissa voidaan siirtää monenlaista tietoa, mutta SIP-protokollaa käytetään vain signaalointiin ja itse tieto siirretään jollakin muulla protokollalla.

Toinen tärkeä protokolla OCS:n toiminnassa on Transport Layer Security (TLS). Oletuksena OCS käyttää TLS-protokollaa käyttäjän ja palvelimen välillä sekä mutual TLS (MTLS) -protokollaa palvelimien välillä.

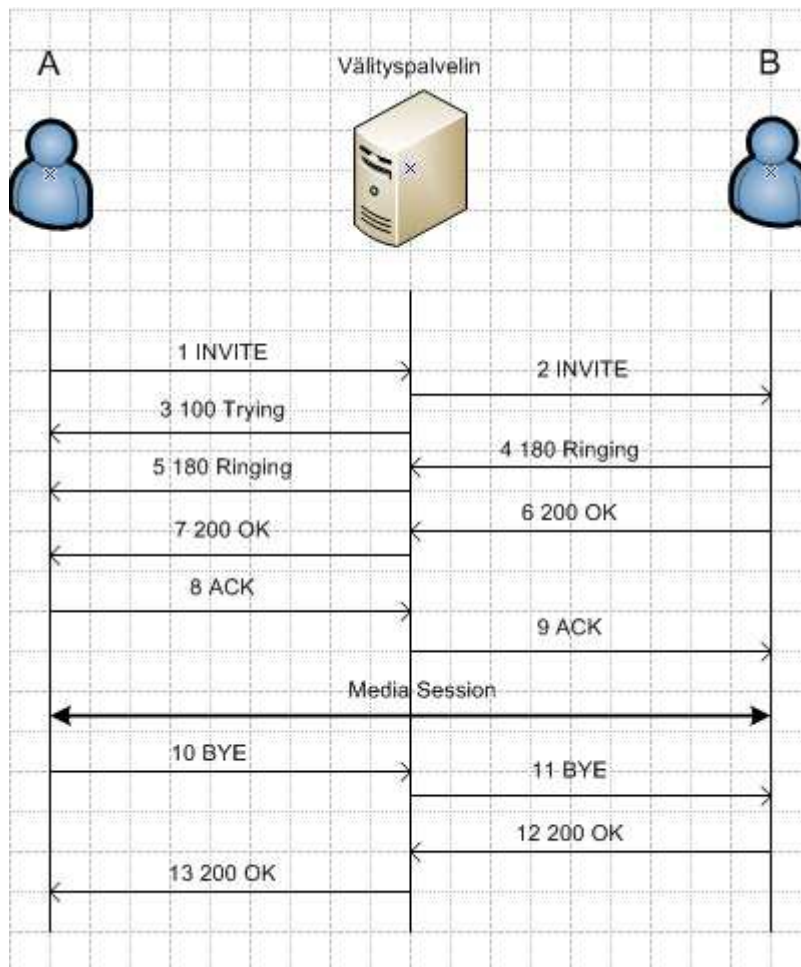
Office Communications Server 2007 R2 -ympäristön muut oleelliset protokollat ovat:

- Hypertext Transfer Protocol (HTTP)
- Centralized Conference Control Protocol (C3P)
- Persistent Shared Object Model (PSOM)
- Secure Real-Time Transport Protocol (SRTP)
- Secure Real-Time Control Protocol (SRTCP)
- Internet Connectivity Establishment (ICE)
- Traversal Using Relay NAT (TURN)
- Session Traversal Utilities for NAT (STUN).

### 3.2.1 SIP

SIP-protokollalla voidaan muodostaa sovellustason istuntoja kahden tai useamman osanottajan kesken. SIP:llä voidaan kutsua osanottajia valmiiseen istuntoon. Myös mediaa voidaan tuoda tai poistaa olemassa olevasta istunnosta. SIP-protokollaa käytetään vain signaalointiin, ja se tarvitsee muita protokollia median siirtoon osanottajien kesken kuten RTP-protokollaa. [5.]

Kuvassa 2 on esimerkki SIP-istunnon muodostamisesta ja purkamisesta. SIP-viestit on numeroitu järjestyksen mukaan 1 - 13 ja molemmat käyttäjät kommunikoivat välityspalvelimen kautta. Käyttäjä A ottaa yhteyden käyttäjään B, jonka SIP uri on sip:b@testi.com. Ensimmäinen viesti yhteyden muodostamisessa on INVITE, joka sisältää tiedon muodostettavan istunnon tyypistä. Onnistuneen yhteyden muodostaminen tapahtuu kolmivaiheisena kättelynä, johon kuuluu viestit INVITE/200/ACK. Viestit 100 Trying ja 180 Ringing ovat väliaikaviestejä, jotka ilmoittavat soittajalle yhteyden muodostuksen etenevän. 200 OK -viesti vahvistaa soittavalle osapuolelle, että vastapuoli on valmis vastaanottamaan dataa tietyssä IP-osoitteessa, portissa ja tietyllä kodekillä. Soittaja vahvistaa olevansa myös valmis ACK-viestillä, jonka jälkeen yhteys on muodostettu. Yhteys puretaan kun, jompikumpi osallistujista lähettää BYE-viestin, johon vastataan 200 OK -viestillä.



Kuva 2. SIP-yhteyden muodostaminen

SIP-viestit:

- INVITE-kutsu istuntoon
- ACK-vastaus kutsuun
- BYE-istunnon lopettaminen
- CANCEL-istunnon muodostamisen lopettaminen
- REGISTER-käyttäjän URI:n rekisteröiminen
- OPTIONS-valintojen kysely
- INFO
- PRACK
- UPDATE-istunnon tietojen päivittäminen
- REFER
- SUBSCRIBE
- NOTIFY
- MESSAGE
- PUBLISH-läsnäolotietojen päivittäminen palvelimelle.

SIP-vastausviestit ovat numeerisia:

- 1xx väliaikaisia ja informatiivisia vastauksia
- 2xx pyyntö suoritettu onnistuneesti
- 3xx uudelleenohjaus, pyyntö tulisi suorittaa toisaalle
- 4xx käyttäjä virhe
- 5xx palvelin virhe
- 6xx globaali virhe.

Esimerkki SIP INVITE -viestistä:

```
INVITE sip:b@testi.com SIP/2.0
Via: SIP/2.0/UDP 192.168.0.5:5060
;branch=z9hG4bK765d
To: UserB< sip:b@testi.com >
From: UserA< sip:a@testi.com >
;tag=34kd92kfs
Call-ID: 4r59899D8g10c3413
Max-Forwards: 70
CSeq: 1 INVITE
Contact: sip:a@192.168.0.5
Content-Length: 126
```

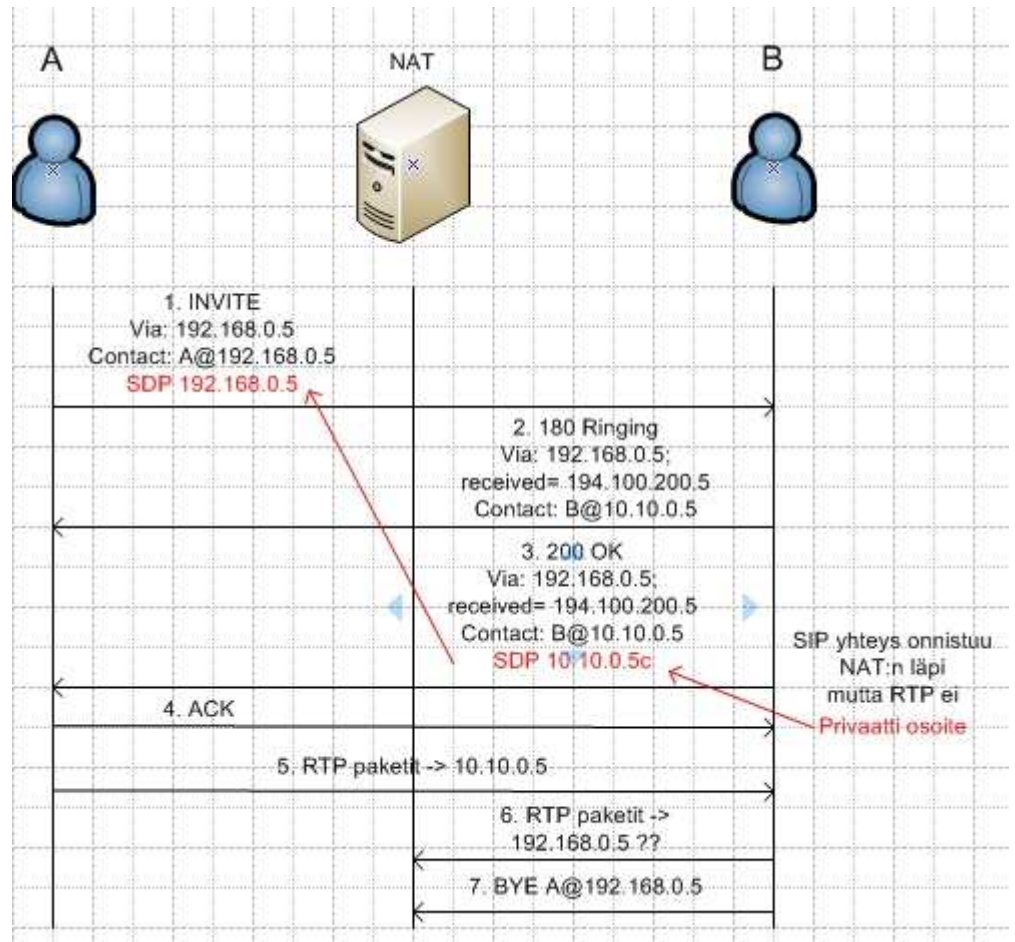
Ensimmäisellä rivillä on viestin nimi INVITE, jonka jälkeen on kutsun kohde URI [b@testi.com](mailto:b@testi.com) ja SIP-versionumero. Toisella rivillä on header via, joka kertoo kuljetusprotokollan, lähettäjän IP-osoitteen ja portin numeron. Call-ID on istunnon ainutkertainen tunniste. Max-Forwards rivi kertoo välityspalvelimien maksimimäärän, jonka kautta viesti voi kulkea. Content-Length kertoo viestin koon. Jos pituus on nolla, viestiä ei ole. [6, s. 102 - 103; 116 - 117.]

Palomuurit ja osoitemuunnokset (NAT) aiheuttavat paljon ongelmia SIP-yhteyden muodostamisessa. Ongelmiin voidaan vaikuttaa eri tavoin esimerkiksi:

- tehdään SIP-välityspalvelimesta sovellustason gateway (ALG)
- muuttamalla palomuri ja NAT SIP tietoisiksi
- käyttämällä P2P-tekniikoita ICE, STUN ja TURN.

SIP-viestit sisältävät osallistujien IP-osoitteet, jos esimerkiksi INVITE-viesti lähetetään sisäverkosta palomuurin ja NAT:n läpi tällöin vastaanottaja saa vain lähettäjän sisäverkon IP-osoitteen. Vastaanottaja ei pysty tavoittamaan kutsun lähettäjää, koska yksityisen sisäverkon osoitetta ei voida reitittää internetin yli. Myös INVITE-viestin sisältämät portit 5060 ja 49170 saattavat vaihtua osoitteenmuutoksen yhteydessä. [6, s. 174 - 176.]





Kuva 3. SIP-yhteyden muodostus NAT:n läpi

Microsoft Office Communications Serverissä käytetään STUN- ja TURN-protokollia ratkaisemaan NAT-ongelmat datan siirrossa. STUN- ja TURN-protokollia käytetään A/V Edge -palvelimissa, jotka sijaitsevat DMZ-alueella.

### 3.2.2 TLS

Transport Layer Security -protokollan tarkoitus on taata yksityisyys ja tiedon eheys kommunikoivien osapuolien välille IP-verkossa. Protokolla on määritetty IETF:n RFC 5246 standardissa. TLS on kuljetuskerroksen protokolla ja korvaa SSL (Secure Sockets Layer) -protokollan. SSL-protokolla oli suunniteltu HTTP-yhteyksien suojaamiseen, mutta SSL- ja TLS -protokollilla voidaan suojata mitä tahansa TCP-yhteyksiä. TLS on riippumaton sovelluksista.

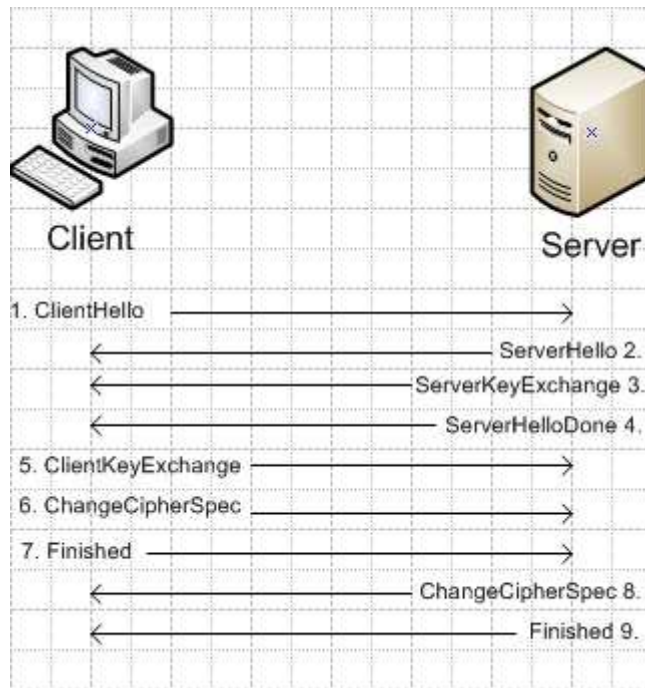
TLS-protokollan toiminta perustuu kahteen ominaisuuteen yksityisyyteen ja luotettavuuteen. Yhteys salataan esimerkiksi symmetrisellä AES-lohkosalausmenetelmällä. Salaukseen tarvittavat avaimet luodaan jokaiselle

yhteydelle erikseen ja avaimet perustuvat erilliseen kättelyprotokollaan esimerkiksi TLS Handshakeen. Viestien luotettavuus tarkistetaan SHA-1-tiivistefunktiolla. TLS-protokolla neuvottelee ja suojaa yhteyden salausalgoritmeilla ennen kuin sovellus on ehtinyt lähettämään tai vastaanottamaan ensimmäistä tavuaan. [7.]

TLS-yhteyden muodostuksessa toinen osapuoli on asiakaskone (client) ja toinen on palvelin. Asiakaskone pyytää suojattua yhteyttä ja palvelin vastaa asiakkaan pyyntöön. Asiakaskone ehdottaa TLS-asetuksia, joista palvelin päättää mitä yhteyden muodostamiseen käytetään. TLS-kommunikoinnissa käytettävät viestit:

- Alert varoittaa toista osapuolta mahdollisesta tietoturvariskistä.
- ApplicationData viesteissä kuljetetaan salattu tieto, joka halutaan välittää.
- Certificate sisältää lähettäjän julkisen avaimen sertifikaatin.
- CertificateRequest palvelin pyytää tällä viestillä asiakkaalta julkisen avaimen sertifikaattia.
- CertificateVerify asiakaskone varmistaa sillä olevan hallussa julkista avainta vastaava yksityinen avain.
- ChangeCipherSPec viesti lähetetään, kun on sovittu käytettävästä salauksesta.
- ClientHello asiakaskone kertoo viestillä mitä turvapalveluita se haluaa ja pystyy käyttämään.
- ClientKeyExchange asiakaskoneen viesti, joka sisältää salausavaimet.
- Finished kertoo salauksen olevan sovittu ja suojatun yhteyden muodostuneen.
- HelloRequest palvelin pyytää tällä viestillä asiakaskonetta aloittamaan tai uudelleen aloittamaan TLS-yhteyden muodostamisen.
- ServerHello palvelin kertoo, mitä salausta käytetään kommunikoinnissa.
- ServerHelloDone kertoo palvelimen suorittaneen kaikki asiakaskonetta koskevat pyynnöt.
- ServerKeyExchange palvelinkoneen viesti, joka sisältää salausavaimet.

Luetelman tarkoitus on selkeyttää TLS-viestien sisältöä seuraavaa yhteyden muodostamis esimerkkiä varten.



Kuva 4. TLS-yhteyden muodostuminen

Salatun TLS-yhteyden muodostamiseen tarvitaan yhdeksän viestiä. Ensimmäinen viesti ClientHello koostuu viidestä kentästä. Ne ovat Version, RandomNumber, SessionID, CipherSuites ja CompressionMethods. RandomNumber-kenttä koostuu satunnaisluvusta, jota käytetään salauksessa. Tämä kenttä luo jokaisesta istunnosta uniikin. Määritelmän mukaan satunnaislukukentän 32 tavusta neljä muodostuu ajasta ja päivämäärästä. Tällä varmistetaan, että asiakaskone ei käytä samaa satunnaislukua useammin kuin kerran. Kun tiedetään, että asiakaskone ei voi käyttää samaa satunnaislukua uudestaan, niin voidaan estää hyökkäykset, joissa kopioidaan vanhat TLS-viestit yhteyden muodostamista varten. CipherSuites-kentällä asiakaskone kertoo, mitä salausta voi käyttää. Palvelin valitsee käytettävän salauksen tästä kentästä. CompressionMethods-kentässä asiakaskone kertoo mahdolliset käytössä olevat pakkaustekniikat.

Toinen viesti ServerHello on vastaus palvelimelta ClientHello-viestiin. ServerHello-viesti koostuu samoista kentistä, kuin ClientHello. Version-kentässä asiakaskone ehdottaa kaikki tukemansa TLS-versiot, ja palvelin valitsee näistä vaihtoehdoista. Jos palvelin ei valitse uusinta versiota, niin asiakaskone voi katkaista yhteyden. Muut kentät toimivat ServerHello-viestissä samalla tavalla ja koostuvat saman tyypisistä arvoista, kuin ClientHello. Asia-

kaskone ehdottaa näillä kentillä käytettäviä palveluita ja palvelin päättää, mitä käytetään.

Kolmannessa ServerKeyExchange-viestissä palvelin lähettää ServerHello-viestin CipherSuite-kentän komplementtiarvon asiakaskoneelle. ServerKeyExchange-viesti sisältää salauksessa käytettävän julkisen avaimen. Asiakaskone käyttää palvelimen julkista avainta istuntoavaimen salaukseen.

ServerHelloDone on neljäs viesti, jolla palvelin kertoo alustavan yhteyden muodostuksen olevan valmis. Viesti ei sisällä muuta tietoa. Asiakaskone voi siirtyä tämän viestin saatuaan yhteyden muodostuksen seuraavaan vaiheeseen.

Viides viesti ClientKeyExchange on asiakaskoneen vastaus ServerHelloDone-viestiin. ClientKeyExchange sisältää tiedon avaimesta, jota molemmat osapuolet käyttävät istunnossa. Tämä viesti on salattu palvelimen julkisella avaimella. Salauksella asiakaskone varmistaa palvelimen pitävän hallussaan julkiseen avaimeen sopivan yksityisen avaimen. Operaatio suojaa hyökkääjiltä, jotka onnistuvat sieppaamaan viestejä ja välittämään niitä eteenpäin asiakaskoneelle. Viestien sieppaamisesta ei ole hyötyä, jos ei tiedä palvelimen yksityistä avainta.

Kuudennella ja kahdeksannella ChangeCipherSpec-viestillä asiakaskone ja palvelin vaihtavat yksityiskohtaiset tiedot käytettävistä salauspalveluista. Viestin lähtiessä järjestelmä aktivoituu kirjoitustilaan ja vastaanottaessa järjestelmä aktivoituu lukutilaan. ChangeCipherSpec-viestien jälkeen molemmat järjestelmät lähettävät Finished-viestin, jolla vahvistetaan yhteyden muodostuksen onnistuneen. Mikäli osapuolet eivät pysty tulkitsemaan Finished-viestiä, tällöin yhteyden muodostus on epäonnistunut. Finished-viestillä vahvistetaan tiedot avaimista, kaikki kättelyyn liittyvät viestit järjestelmien välillä ja kumpi järjestelmistä on asiakas ja kumpi palvelin. [8, s. 37 - 51.]

### 3.3 Kilpailijat

Office Communications Serverin suurimmat kaupalliset kilpailijat ovat IBM Lotus Sametime ja Cisco. Näiden yritysten yhdistetyn viestinnän ratkaisuissa on eroavaisuuksia ja valinta tulisi tehdä käyttötarkoituksen perusteella. Lotus Sametime asiakasohjelma Connect voidaan asentaa useille eri alustoille, ku-

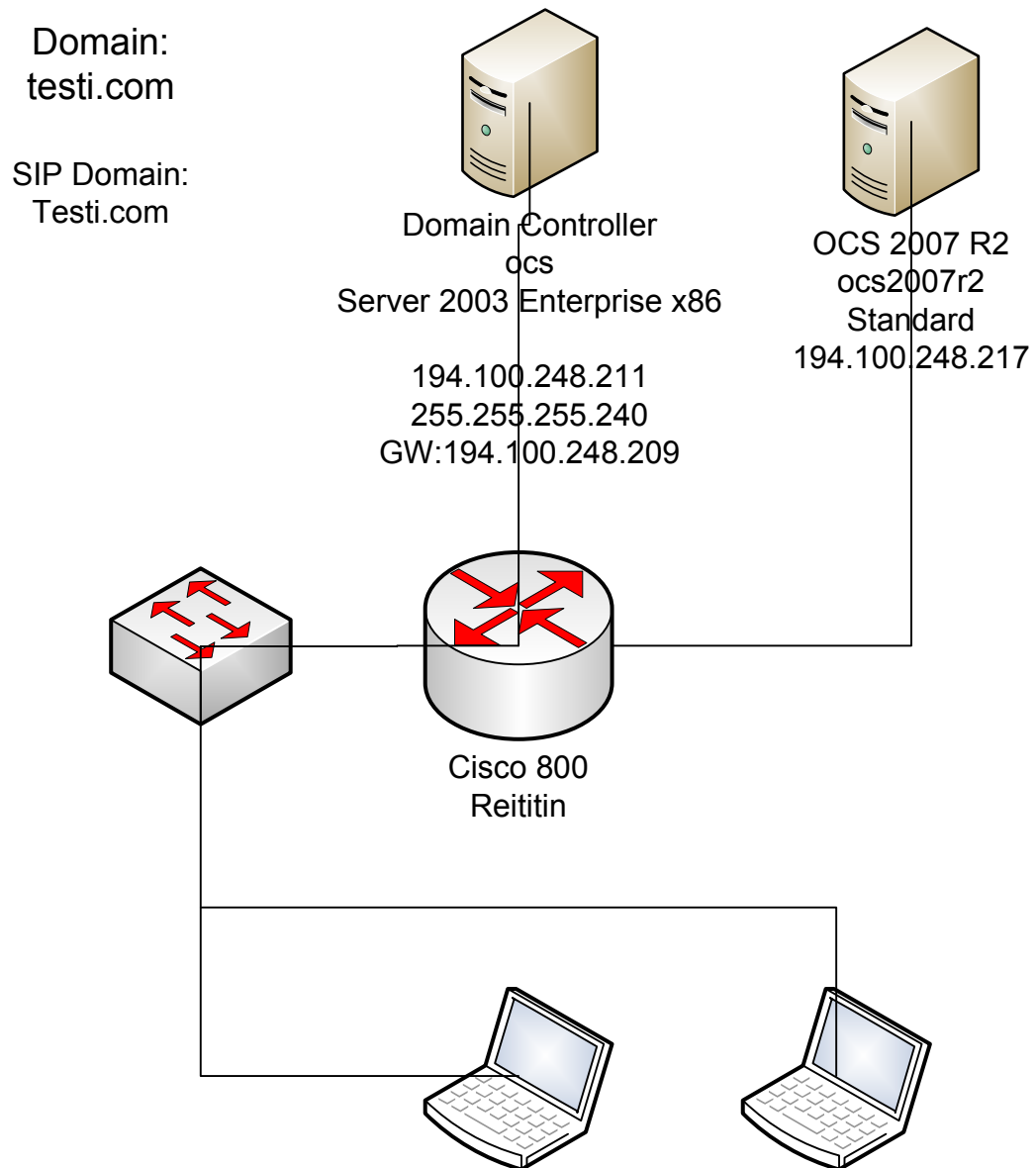
ten Windowsille, Linuxille ja Macille. Connect tukee myös useita mobiilialustoja. Lotus Sametime käyttää Virtual Places nimistä protokollaa, mutta tukee myös standardoituja protokollia, kuten SIP, G.722.1, H.264 ja H.323. Ciscon ratkaisu koostuu useasta eri tuotteesta:

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Express
- Cisco Unified Presence
- Cisco Unity
- Cisco Unity Connection.

Näiden lisäksi Ciscon UC-tuotteisiin kuuluu erilaisia asiakassovelluksia, IP-puhelimia ja hallintasovelluksia. Ciscon ja IBM:n UC-ratkaisuista on vaikeampaa saada kokonaiskuvaa verrattuna Microsoftin OCS-ratkaisuun. Microsoft on panostanut paljon tuotteensa dokumentointiin. OCS:n toiminnallisuuden sekä teknisiin ominaisuuksiin on helppo tutustua. Mielestäni Microsoftin Unified Communications –ratkaisu on kokonaisvaltaisempi ja valmiimpi tuote verrattuna Ciscon ja IBM:n vastaaviin ratkaisuihin.

#### **4 TESTIYMPÄRISTÖ**

Testiympäristö koostuu toimialueesta, jossa on kaksi palvelinta ja muutama kannettava työasema. Toinen palvelimista toimii toimialueen ohjauspalvelimena (domain controller) ja toinen Office Communications Serverinä. Office Communications Serveriä ei voi asentaa ohjauspalvelimeen. Ohjauspalvelimena toimii Dell PowerEdge 2650, jossa on käyttöjärjestelmänä 32-bittinen Microsoft Windows Server 2003 Enterprise. Office Communications Server asennettiin Lenovo TS200 -palvelimeen, jonka käyttöjärjestelmäksi valittiin 64-bittinen Microsoft Windows Server 2008 Enterprise.



Kuva 5. Toimialueen perusrakenne

#### 4.1 Palvelimien käyttöjärjestelmä asennus

Palvelimen asennus aloitettiin Server 2003 -palvelimesta, johon lisättiin kaksi roolia: Domain Controller (Active Directory) ja DNS server. Toimialue nimettiin testi.com ja palvelimen nimeksi annettiin ocs, joten ohjauspalvelimen FQDN (Fully qualified domain name) on ocs.testi.com. Tämän jälkeen palvelimeen päivitettiin Microsoft Update -sivuston kautta uusimmat päivitykset.

OCS 2007 R2 vaatii toimiakseen 64-bittisen palvelimen, jossa on 64-bittinen käyttöjärjestelmä. OCS-palvelimeen asennettiin Server 2008 - käyttöjärjestelmä ja uusimmat päivitykset. Rooleja ei palvelimeen lisätty. Tätä kirjoittaessa OCS ei toimi Server 2008 R2 -käyttöjärjestelmässä. Server 2008 R2 -tuki OCS:lle on kuitenkin ainakin osittain tulossa. Myöskään domain controller -palvelimessa ei saa olla Server 2008 R2 -käyttöjärjestelmää.

#### 4.1.1 Ohjauspalvelimen asennus

Ohjauspalvelimena käytettiin Metropolia Ammattikorkeakoulussa muutaman vuoden palvelutta Dell PowerEdge 2650 -palvelinta. Palvelimen firmware- ja BIOS -päivitykset olivat ajantasalla, joten ainoa huomiota vaativa seikka ennen käyttöjärjestelmän asennusta olivat kiintolevyt. Kiintolevyiksi valittiin kaksi 72 gigatavun kiintolevyä, joista muodostettiin palvelimen levyohjaimella RAID1-levyosio. RAID1-tekniikka peilaa tiedon molemmille levyille, tällöin toisen levyn hajotessa mitään tietoa ei menetetä.

Ohjauspalvelimeen asennettiin Windows Server 2003 R2 Enterprise Edition -käyttöjärjestelmä. Ennen ohjauspalvelimeksi korottamista on oleellista asettaa palvelimelle kiinteä IP-osoite ja yhdistää verkkokaapelit. Ohjauspalvelimeksi muuttaminen sekä DNS-palvelun käyttöönotto tapahtuu Administrative Tools -valikon kohdasta Manage Your Server. Seuraavaksi valitaan Add or remove a role, jolloin käynnistyy Configure Your Server Wizard. Tässä kohdassa valitaan rooliksi Domain Controller (Active Directory) ja painetaan Next kaksi kertaa. Näin käynnistyy Active Directory Installation Wizard, jolla luodaan ohjauspalvelin uuteen toimialueeseen ja toimialue uuteen metsään.

Wizard ajaa DNS rekisteröinti diagnostiikan, joka päättyy virheeseen, koska DNS-palvelinta ei ole toimialueeseen määritetty. Luodaan tässä vaiheessa ohjauspalvelimelle myös DNS-palvelu. Lopuksi tarkistetaan yhteenvedosta tietojen oikeellisuus ja aloitetaan asennus. Palvelin vaatii uudelleenkäynnistyksen ja tämän jälkeen uusi toimialue on valmis.

Windows toimialueiden Active Directoryssä on useita toimintatasoja taaksepäin yhteensopivuuden takia. Pääasiassa toimintatasot määrittelevät muiden ohjauspalvelimien käyttöjärjestelmä vaihtoehdot. Windows Server 2003 -toimialueen toimintatasot ovat:

- Windows 2000 -sekatila (mixed mode)
- Windows 2000 -natiivitila (native mode)

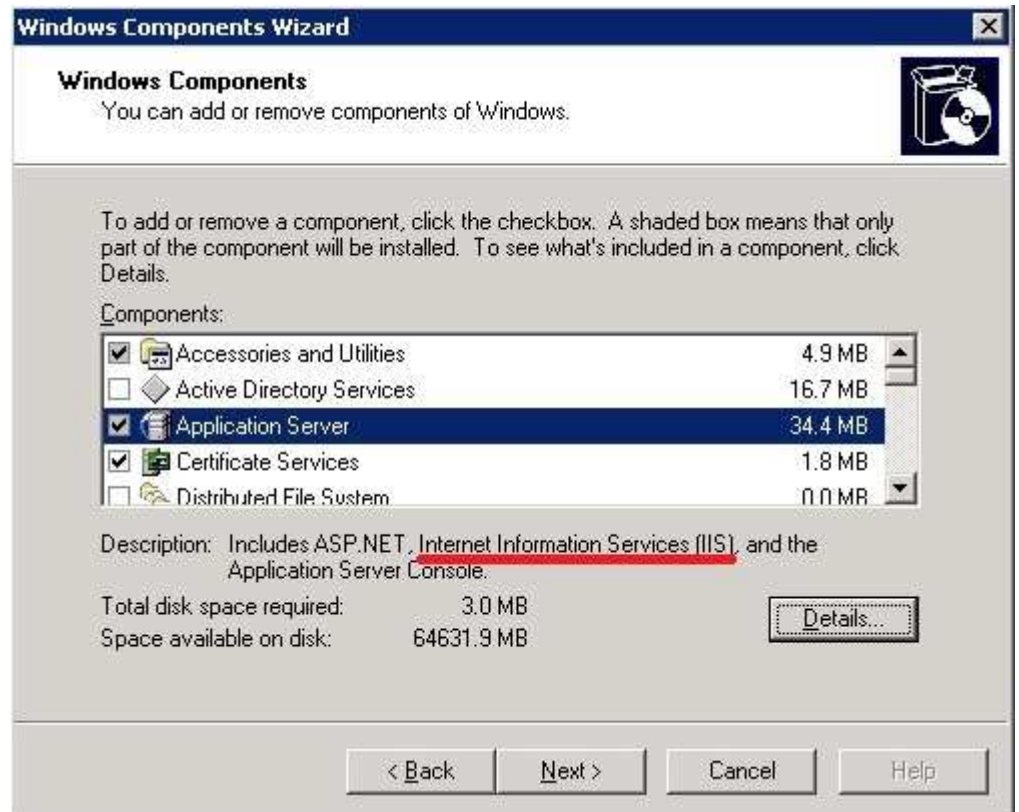
- Windows Server 2003 -välitila (interim mode)
- Windows Server 2003 -tila (Windows Server 2003 mode).

OCS-palvelinta ei voida asentaa toimialueeseen, joka on sekatilassa. Toimialueen on oltava vähintään Windows 2000 -natiivitilassa tai korkeammalla. OCS-palvelimessa käytettävän Windows Server 2008 -käyttöjärjestelmän takia toimialueen toimintataso nostettiin korkeimpaan Windows Server 2003 -tilaan. Toimintatason nosto tapahtuu Active Directory Users and Computers -konsolin kautta valitsemalla toimialue ja Action-valikosta kohdasta Raise Domain Functional Level. Myös metsän toimintatasoa on nostettava. OCS-palvelin vaatii metsän toimintatason oltava vähintään Windows Server 2003 -tilassa. Metsän toimintatason nosto tapahtuu Active Directory Domains and Trusts -konsolin kautta. Konsolista valitaan ensin toimialueen yläpuolelta Active Directory Domains and Trusts, jonka jälkeen Action valikosta Raise Forest Functional level.

#### *4.1.2 PKI julkisen avaimen infrastruktuuri*

OCS vaatii sertifikaatin asentamista kaikkien palveluiden toimivuuden takia. Tämän vuoksi ohjainkoneesta tehtiin juurivarmentaja (Standalone Root Certificate Authority). Ennen Certification Authorityn asentamista on palvelimella asennettava IIS-palvelu. Asennus tapahtuu Add or Remove Programsin kautta, josta valitsemalla Add/Remove Windows Components päästään valitsemaan halutut komponentit.





Kuva 6. IIS-asennus

Windows Components Wizard -ikkunassa valitaan Application Server ja painetaan Details-painiketta. Application Server -ikkunassa valitaan Internet Information Services (IIS) ja painetaan OK-painiketta, jolloin asennus käynnistyy. IIS asennuksen jälkeen voidaan asentaa Certificate Services. Certificate Services asennetaan myös Windows Components Wizard -ikkunasta. Certificate Services asennuksen alussa tulee varoitus toimialueen jäsenyydestä ja tietokoneen uudelleen nimeämiseen liittyvistä rajoituksista. CA tyyppiä kytettäessä valitaan Enterprise root CA ja painetaan Next painiketta. CA Identifying sivulle kirjoitetaan palvelimen yleinen nimi. [10, s. 668 - 670.]

**Windows Components Wizard**

**CA Identifying Information**  
Enter information to identify this CA.

Common name for this CA:  
ocsCA

Distinguished name suffix:  
DC=ocs,DC=com

Preview of distinguished name:  
CN=ocsCA,DC=ocs,DC=com

Validity period: 5 Years

Expiration date: 21.4.2015 8:42

< Back   Next >   Cancel   Help

Kuva 7. CA yleinen nimi

Lopuksi asennus ilmoittaa IIS:n pysäyttamisestä, josta edetään klikkaamalla Yes. Seuraavassa kohdassa asennus kysyy ASP:n käynnistämisestä, joka käynnistetään klikkaamalla Yes. Näin on asennettu ohjainkoneelle Certificate Services ja palvelimesta tehty toimialueen juurivarmentaja.

#### 4.1.3 OCS-palvelimen asennus

OCS-palvelimena toimi Lenovo TS200 kahdella 500 gigatavun kiintolevyllä. Palvelimessa on Intelin 2,4 Ghz:n neliydinsuoritin ja keskusmuistia 8 gigatavua, tämä kokoonpano vastaa OCS-palvelimelle asetettuja minimi vaatimuksia. Asennus aloitettiin palvelimen mukana tulevalla asennuslevyllä, joka mahdollisti RAID-levyosion luonnin. OCS-palvelimessa käytettiin RAID1-levyosiota, joka peilasi molemmat 500 gigatavun kiintolevyt yhdeksi loogiseksi levyasemaksi. Seuraavaksi asennuslevy kysyi asennettavaa käyttöjärjestelmää. Asennuslevyn valikosta valittiin 64 bittisen Windows Server 2008 Enterprise -version, jonka jälkeen vaihdettiin Windows-asennuslevy palvelimeen. Asennuksen jälkeen Windows oli käyttövalmis Lenovon ajurit olivat asentuneet asennuslevyn kautta. Lopuksi asennettiin Server 2008 uusimmat

päivitykset ja tarkistettiin palomuurin asetukset. Palomuurin ollessa päällä OCS asennus osaa tehdä palomuuriin tarvittavat poikkeukset.

## 4.2 OCS-asennus ja käyttöönotto

Office Communications Server -palvelimen asennus aloitetaan domain controllerista. Domain controllerin Active Directory täytyy valmistella OCS-asennusta varten. Valmistelu tarkoittaa Active Directoryn skeeman eli mallin muuttamista.

### 4.2.1 Active Directoryn valmistelu

Active Directoryn valmisteluun kuuluu kolme kohtaa: skeeman valmistelu, metsän valmistelu ja toimialueen valmistelu. Skeeman valmistelu lisää Active Directoryyn tarvittavat luokat ja attribuutit Office Communications Serverille ja siihen liittyville käyttäjille. Metsän valmistelu luo globaalit asetukset ja universaalit ryhmät, joita OCS käyttää. Toimialueen valmistelu lisää oikeudet objekteille, joita universaalien ryhmien jäsenet käyttävät. Active Directoryn valmisteluun riittää toimialueen Administrator-käyttäjätili, joka oletuksena kuuluu Schema Admins- ja EnterpriseAdmins-ryhmiin.

Active Directoryn valmistelu suoritetaan Active Directory Preparation Tools -ohjelmilla. Ohjelmat ovat graafinen SetupSE.exe tai komentorivityökalu LcsCmd.exe. Molemmat ohjelmat löytyvät Office Communications Server -asennuslevyltä. Asennuslevyllä on myös SetupEE.exe Office Communications Server Enterprise Editionia varten. Graafiset ohjelmat SetupSE.exe ja SetupEE.exe ovat käyttökelpoisia yksinkertaisissa yhden metsän ja yhden toimialueen topologioissa. LcsCmd.exe ohjelmalla voi suorittaa Active Directoryn valmistelun myös monipuolisemmassa ympäristössä. Testiympäristössä jouduin käyttämään LcsCmd.exe-ohjelmaa Active Directoryn valmisteluun 32-bittisen ohjainkoneen vuoksi. SetupSE.exe- ja SetupEE.exe-ohjelmia on mahdollista käyttää vain 64-bittisissä ohjainkoneissa. 32-bittisiin ohjainkoneisiin täytyy lisäksi tuoda schema.ldf-tiedosto OCS-asennusmediaalta. Schema.ldf-tiedosto tuodaan Ldifde.exe-ohjelmalla, joka on osa Microsoftin Active Directoryn skeema -työkaluja. Ldifde-ohjelma ajetaan komentoriviltä.

```
ldifde -i -v -k -s ocs -f schema.ldf -c DC=X "DC=testi,DC=com"
-b Administrator testi.com <salasana>
```

Tämä toimenpide tulee suorittaa myös 64-bittisissä ohjainkoneissa, jotka eivät ole schema mastereita.

### OCScore-asennus

Ohjainkoneelle voidaan asentaa OCS-ydinkomponentit `ocscore.msi`-asennuspaketista, joka löytyy OCS-asennusmedialta. Ocscoren mukana asentuu myös AD:n valmisteluun tarvittava `LcsCmd.exe`-ohjelma. `LcsCmd.exe`-ohjelma voidaan vaihtoehtoisesti ajaa suoraan asennusmedialta. 32-bittinen versio OCScoresta asennetaan OCS-asennusmedialta hakemistosta `\support\i386\ocscore.msi`. OCScoren asennus edellyttää palvelimesta löytyvän Microsoft SQL Server Native Clientin, VC++ 2008 Redistributablen ja Microsoft .NET Framework 3.5 SP1. Nämä kolme ohjelmaa löytyvät samasta hakemistosta kuin `ocscore.msi`.

### Skeeman valmistaminen

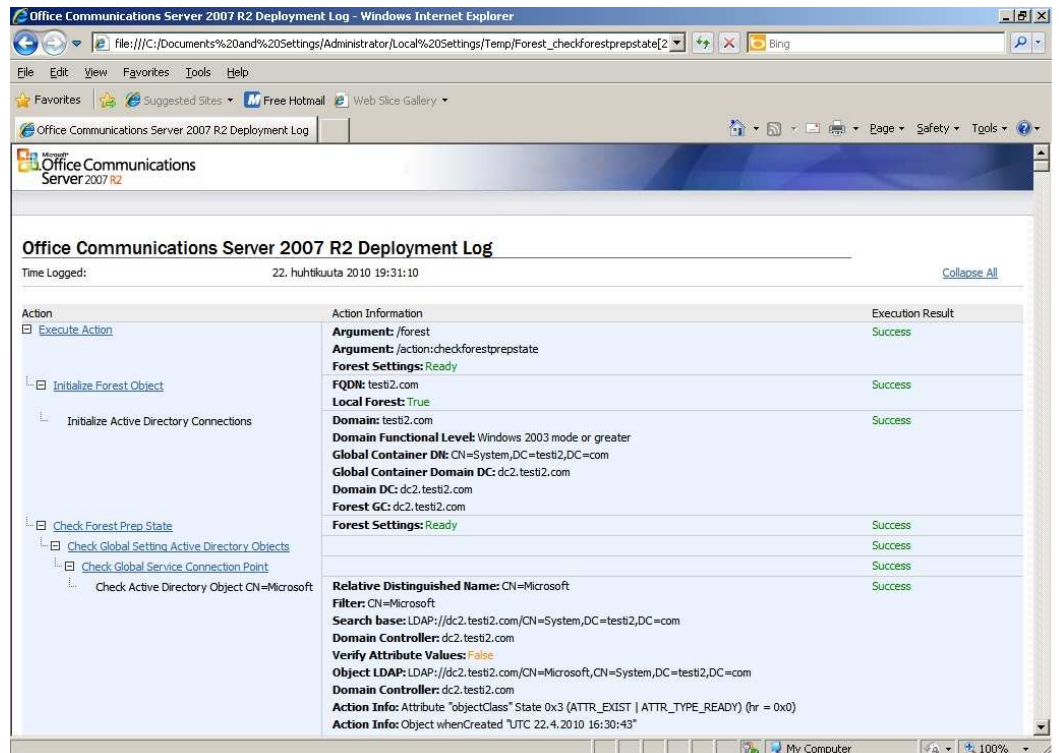
Skeeman valmistaminen tehdään jokaisessa AD-metsässä, johon OCS-palvelin on tarkoitus asentaa. Skeema valmistetaan `LcsCmd.exe`-ohjelmalla, joka ajetaan `schema master` -ohjainkoneessa. Skeema laajennetaan OCS-asennusmedialta löytyvän `schema.ldf`-tiedoston mukaan.

```
LcsCmd.exe /forest /action:SchemaPrep /ldf: d:\setup\amd64
```

Komennon lopussa tulisi lukea "Action completed successfully" ja lokitiedosto löytyy kansiota `c:\documents and settings\administrator\local settings\temp`. Skeeman valmistamisen voi varmistaa seuraavalla komenolla.

```
LcsCmd.exe /forest /action:CheckSchemaPrepState
```

Komento luo yllämainittuun hakemistoon laajemman raportin tehdyistä toimenpiteistä.



Kuva 8. Skeeman valmisteluraportti

Skeeman valmistaminen kestää kauemmin monimutkaisemmissa ympäristöissä, joissa on useita ohjainkoneita. Viive johtuu skeeman replikoinnista ohjainkoneiden välillä. Mikäli skeema ei ole replikoitunut kaikkien ohjainkoneiden välillä, valmisteluraporttiin tulee virheilmoitus. Replikoinnin tulee olla valmis ennen metsän valmisteluun siirtymistä.

### Metsän valmistelu

Metsän valmistelu suoritetaan jokaisessa metsässä, johon OCS-palvelin on tarkoitus asentaa. Metsän valmistelussa luodaan objektit, jotka sisältävät tiedot OCS-asennuksesta ja globaalit asetukset. Globaalit asetukset tallennetaan, joko konfiguraatiosäiliöön tai järjestelmäsäiliöön. Yksinkertaisessa testiympäristössä ei ole merkitystä kumpaan säiliöön globaalit asetukset tallennetaan. Järjestelmäsäiliö sijaitsee juuri toimialueessa, jota ei replikoida. Konfiguraatiosäiliö replikoidaan toimialueiden välillä, joka vaikuttaa suorituskykyyn. Replikointi on oleellisin ero näiden kahden säiliön välillä. Metsän valmistelu suoritetaan komennolla.

```
LcsCmd.exe /forest /action:ForestPrep /global:system
```

/global määrittää globaalien asetusten tallennus-säiliön testiympäristössä käytettiin järjestelmäsäiliötä. Käsky voidaan suorittaa eri toimialueeseen lisäämällä parametri /groupdomain ja antamalla sille haluttu toimialueen kokonimi. Metsän valmisteluun liittyvä loki luodaan komennolla hakemistoon c:\documents and settings\administrator\local settings\temp.

```
LcsCmd.exe /forest /action:CheckForestPrepState
```

#### Toimialueen valmistelu

Active Directoryn valmistelun kolmas ja viimeinen kohta on toimialueen valmistaminen. Toimialueen valmistelu tehdään jokaisessa toimialueessa, johon OCS-palvelin asennetaan. Testiympäristö valmistettiin toimialueen komennolla.

```
LcsCmd.exe /domain:testi.com /action:DomainPrep
```

Paikallinen toimialue voidaan valmistaa myös jättämällä /domain parametri komennosta pois.

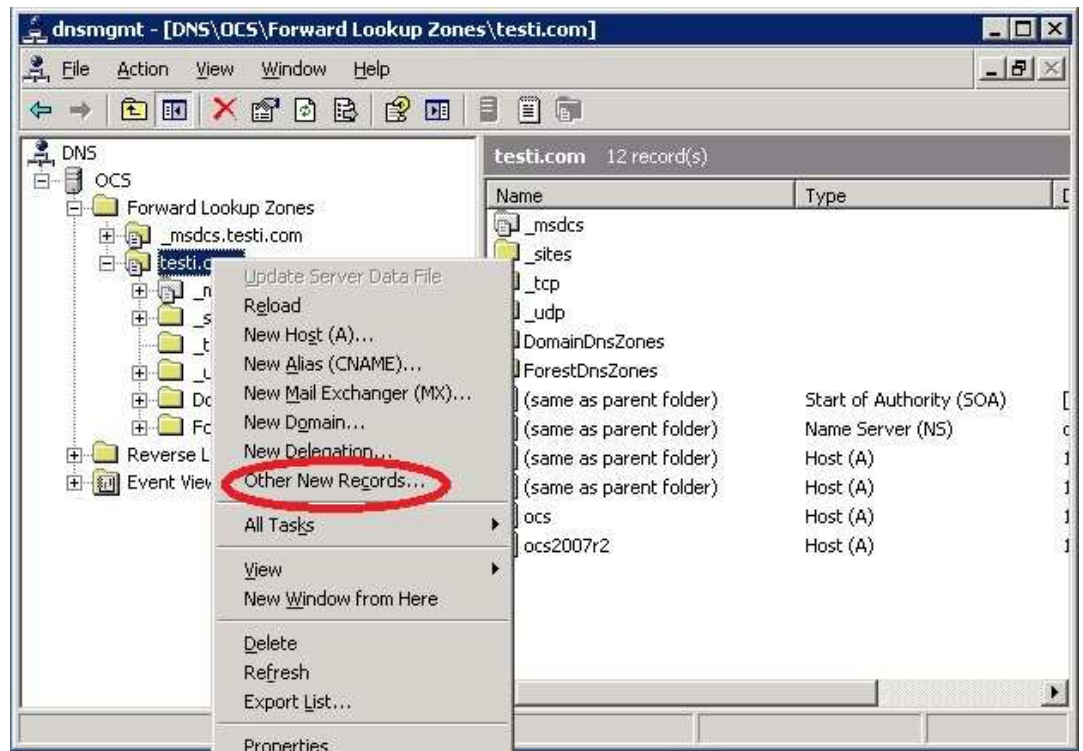
```
LcsCmd.exe /action:DomainPrep
```

Paikallisen toimialueen valmisteluun liittyvä loki luodaan komenolla hakemistoon c:\documents and settings\administrator\local settings\temp.

```
LcsCmd.exe /action:CheckDomainPrepState. [1, s. 5 - 14; 26 - 29.]
```

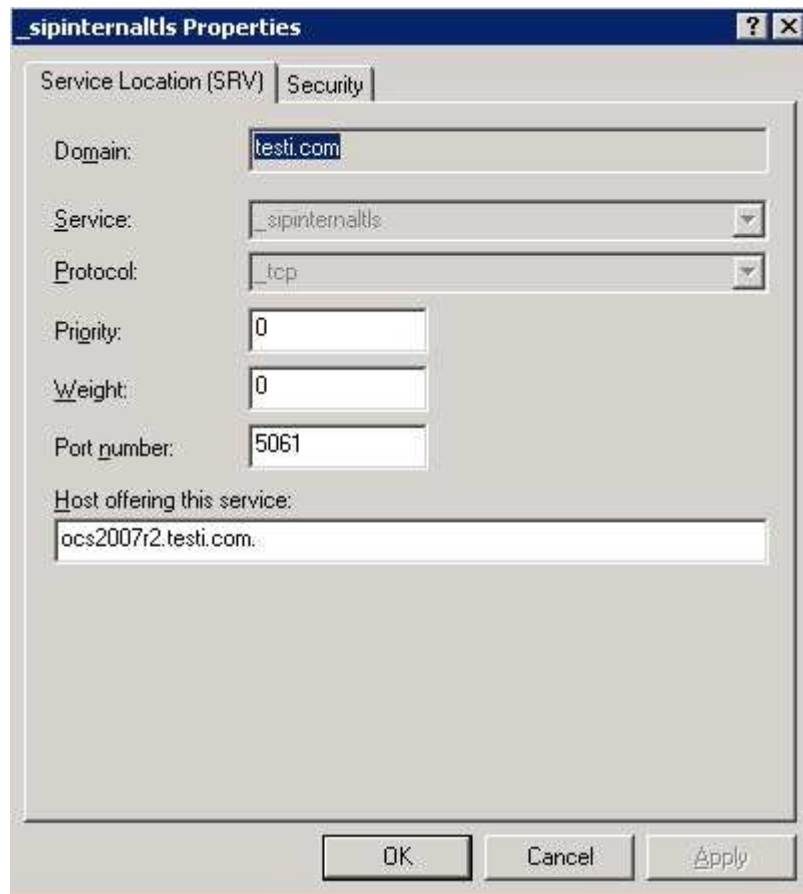
#### 4.2.2 DNS-tietueet

Toimialueen jokaisen OCS-palvelimen täysi toimialuenimi tulee rekisteröidä toimialueen nimipalvelujärjestelmään, jotta käyttäjät voivat yhdistyä palvelimeen. OCS-palvelinta varten tehtiin DNS SRV- ja DNS A-tietueet ohjainkooneen nimipalveluun. DNS SRV -tietue luodaan dnsmgmt-konsolista laajentamalla Forward Lookup Zones ja valitsemalla toimialue, johon OCS-palvelin asennetaan. Toimialue valitaan hiiren oikealla painikkeella ja listasta valitaan Other New Records.



Kuva 9. DNS SRV -tietueen luonti

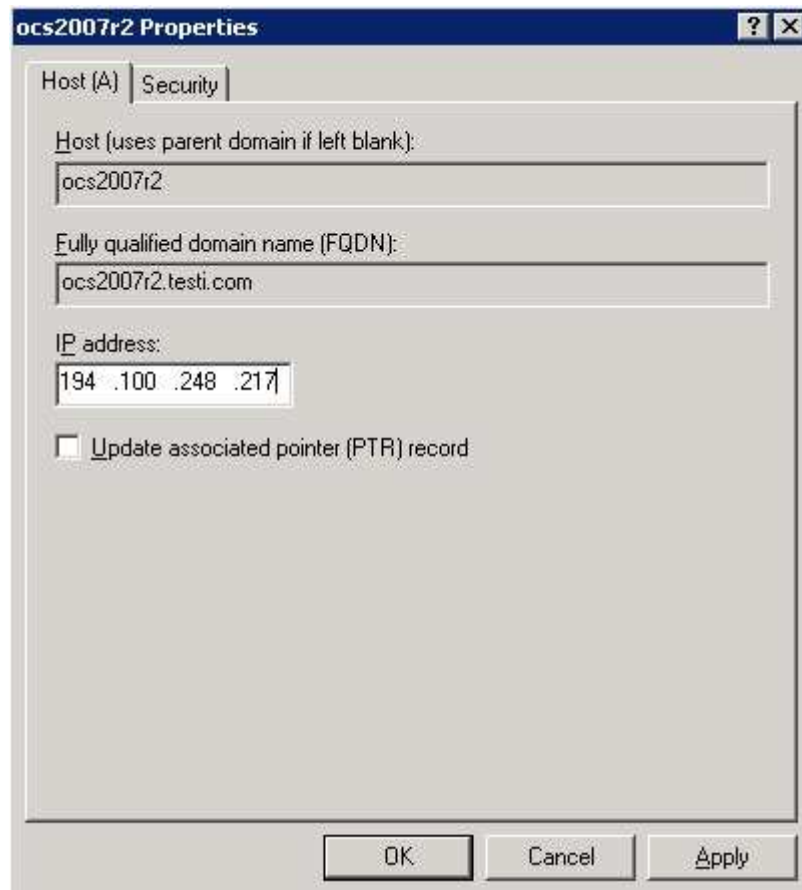
Seuraavaksi aukeaa Resource Record Type -ikkuna, jonka listasta valitaan haluttu tietueen tyyppi eli Service Location (SRV). New Resource Record -ikkunaan valitaan Service kohtaan kirjoitetaan \_sipinternaltls, protokollaksi valitaan \_tcp ja portin numeroksi 5061. Viimeiseen kenttään Host offering this service kirjoitetaan OCS-palvelimen täysi toimialue nimi eli ocs2007r2.testi.com.



Kuva 10. DNS SRV -tietue

Seuraavaksi luotiin DNS A-tietue. Tämä tapahtuu laajentamalla Forward Lookup Zones ja valitsemalla hiiren oikealla painikkeella toimialue ja listasta New Host (A). Name kohtaan kirjoitettiin OCS-palvelimen nimi ocs2007r2. IP Address-kenttään kirjoitettiin OCS-palvelimen ip-osoite 194.100.248.217. [2, s. 6 - 7.]





Kuva 11. DNS A -tietue

#### 4.2.3 Server 2008:n valmistaminen asennukseen

OCS-palvelimena toimiva Windows Server 2008 -käyttöjärjestelmä päivitettiin Windows Updaten kautta uusimmat päivitykset. Muutaman päivityksen tiedettiin mahdollisesti häiritsevän OCS-asennusta, mutta ongelmalliset päivitykset suunniteltiin poistettavan niiden ilmaannuttua. Office Communications Server 2007 R2 vaatii ainakin seuraavat päivitykset ennen asennusta kb953582 ja kb953990. Windowsin palomuuuri on suositeltavaa pitää päällä asennuksen aikana, jotta OCS:n tarvitsemat poikkeukset tulevat voimaan. Mikäli palomuuuri ei ole toiminnassa OCS-asennus ei puutu palomuurin asetuksiin ja poikkeukset on luotava manuaalisesti tai aktivointi suoritettava uudestaan palomuurin ollessa päällä.

#### IIS - Internet Information Services

IIS on Windowsin mukana tuleva web-palvelinohjelmisto, joka tarjoaa FTP-, SMTP-, NNTP-, HTTP- ja HTTPS-palvelut. IIS on otettava käyttöön palveli-

mella ennen OCS-asennusta. Server 2008 käyttöjärjestelmän mukana tulee IIS 7.0, joka tulee asettaa toimimaan IIS 6.0 yhteensopivassa tilassa. IIS asennus tehdään Server 2008 Administrative Tools Server Managerin kautta, josta valitaan Add Roles. Add Roles velhosta valitaan Web Server (IIS). Seuraavaksi valitaan tarvittavat IIS palvelut.

- ASP.NET
- Windows Authentication
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility
- IIS 6 Scripting Tools
- IIS 6 Management Console.

Server 2008 huomauttaa, jos ylimääräisiä palveluita tulee käynnistää, näissä huomautuksissa olevat palvelut tulee myös asentaa. [2, s. 9.]

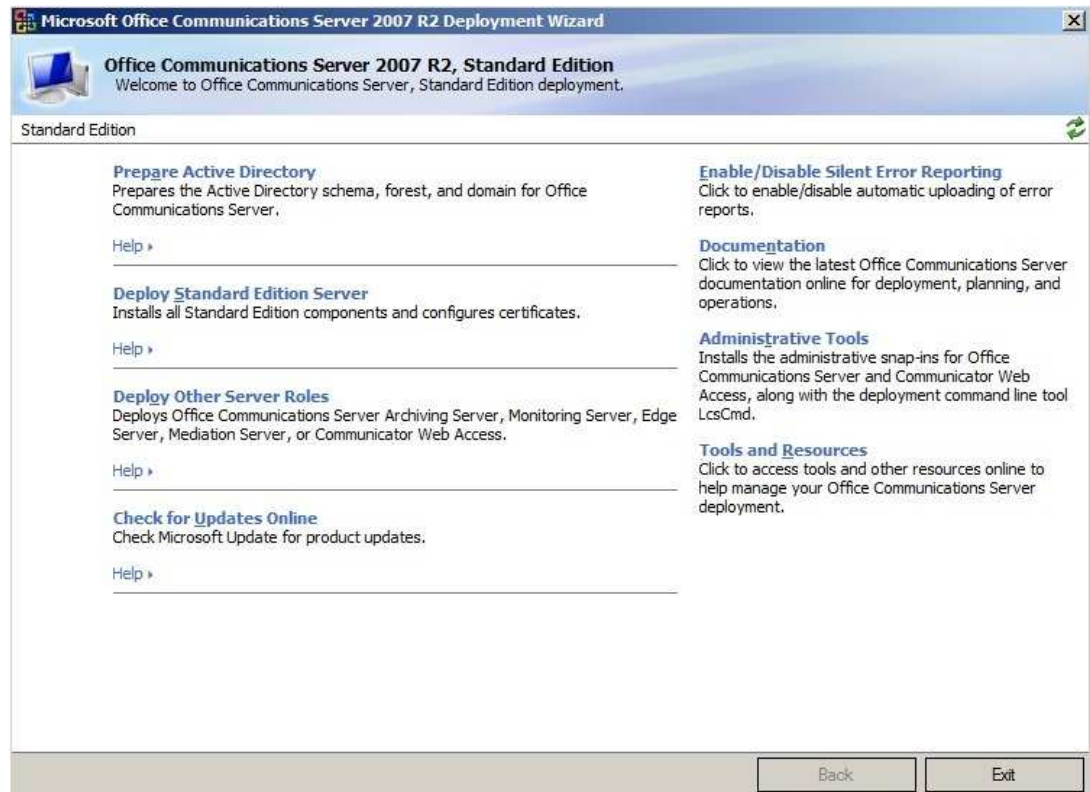
#### 4.2.4 *Office Communications Server 2007 R2 Standard Edition -asennus*

OCS Standard Edition asennuksessa kaikki palvelinkomponentit asennetaan yhdelle fyysiselle tietokoneelle. Asennettavat komponentit ovat seuraavat:

- Microsoft SQL Server 2005 Express Edition SP2
- Front End Server
- Web Conferencing Server
- A/V Conferencing Server
- Web Components Server
- Application Sharing Conferencing Server
- Four unified communications applications.

Ennen OCS-asennusta palvelimessa täytyy olla asennettuna Microsoft Visual C++ Redistributable Package, Microsoft .NET Framework 3.5 ja Windows Media Format Runtime. OCS-asennus huomauttaa näiden ohjelmien puuttuessa ja halutessa suorittaa myös asennuksen OCS-asennusmedialta.

Palvelimelle ocs2007r2 kirjaututtiin toimialueen administrator tunnuksella ja tarkistettiin tunnuksen kuuluvan RTCUniversalServerAdmins ryhmään. Asennus käynnistettiin Office Communications Server 2007 R2 CD -levyltä ja valitsemalla Standard Edition, tämä käynnistää Office Communications Server 2007 R2 asennusvelhon.



Kuva 12. OCS-asennusvelho

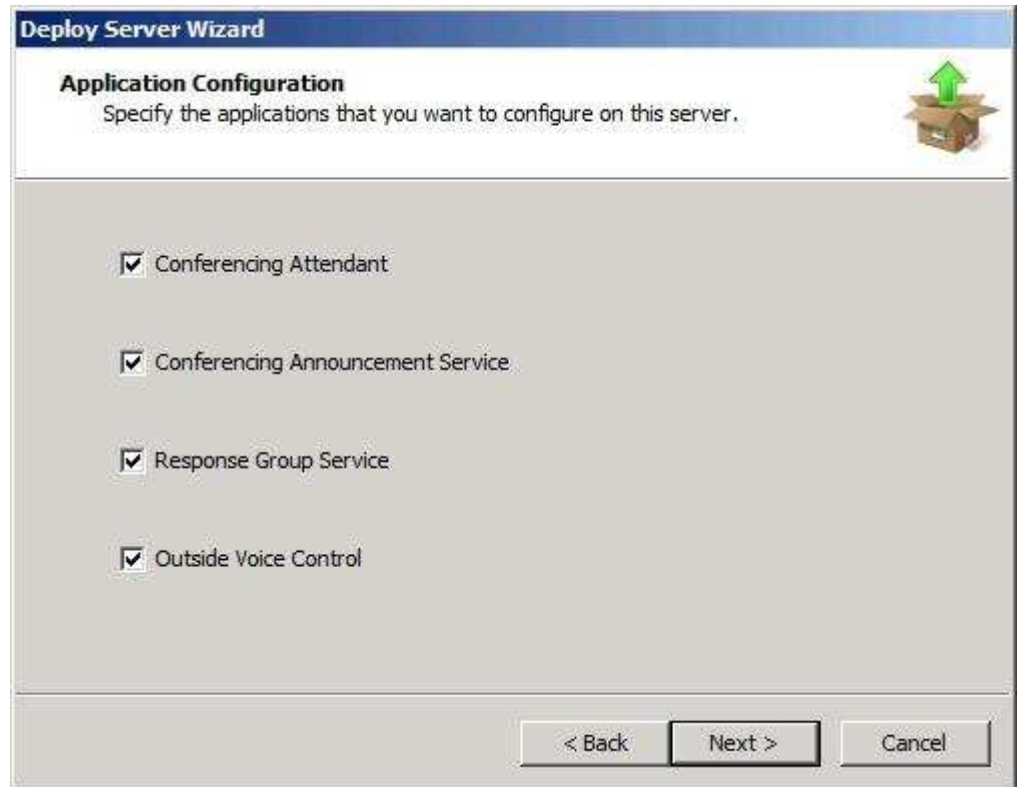
Asennusvelhosta valitaan Deploy Standard Edition Server, joka sisältää seitsämän kohtaa.

- Deploy Server
- Configure Server
- Configure Certificate
- Configure Web Components Server Certificate
- Verify Replication
- Start Services
- Validate Server Functionality.

Nämä asennusvaiheet käydään järjestyksessä läpi.

Deploy Server

Application Configuration kohdassa voidaan valita halutut sovellukset edellä mainitusta Four unified communications -sovelluksesta. Testiympäristöön valittiin kaikki sovellukset aktivoitaviksi.



*Kuva 13. Application Configuration*

Main Service Account for Standard Edition Server -kohdassa asennus kysyy käyttäjätunnusta, joka ajaa OCS-palvelua tällä palvelimella. Uuden käyttäjätunnuksen luonti tällä sivulla tuotti virheilmoituksen, joten käytettiin valmista administrator käyttäjätunnusta. Component Service Account for this Standard Edition Server sivulla asennus kysyy millä käyttäjätunnuksella halutaan ajaa Audio/Video konferenssi- ja Web-konferenssipalveluita. Tässäkin kohdassa käytettiin testiympäristössä administrator käyttäjätunnusta, joka ei ole suotavaa tuotantoympäristössä.

Web Farm FQDN -sivulla asennus kysyy sisäisen ja ulkoisen OCS-palvelimen täyttä toimialuenameä. Testiympäristön asennuksessa kirjoitettiin sisäiseksi FQDN:ksi ocs2007r2.testi.com ja valinnaisen ulkoisen palvelimen nimi jätettiin täyttämättä.

Location for Database Files -sivulla määritetään OCS:n hakemistot käyttäjien tietokannalle ja tapahtuma lokeille.

**Deploy Server Wizard**

**Location for Database Files**  
Select the location where files will be installed.

Each database and transaction log should be placed on a separate physical disk to improve performance. Do not use the system disk or page file.

Database File Location  
Database:  Browse...

Transaction Log Location  
Shared logs:  Browse...

The following two log file locations should not share the same physical location. Please choose different drives for each.

RTCDYN log:  Browse...

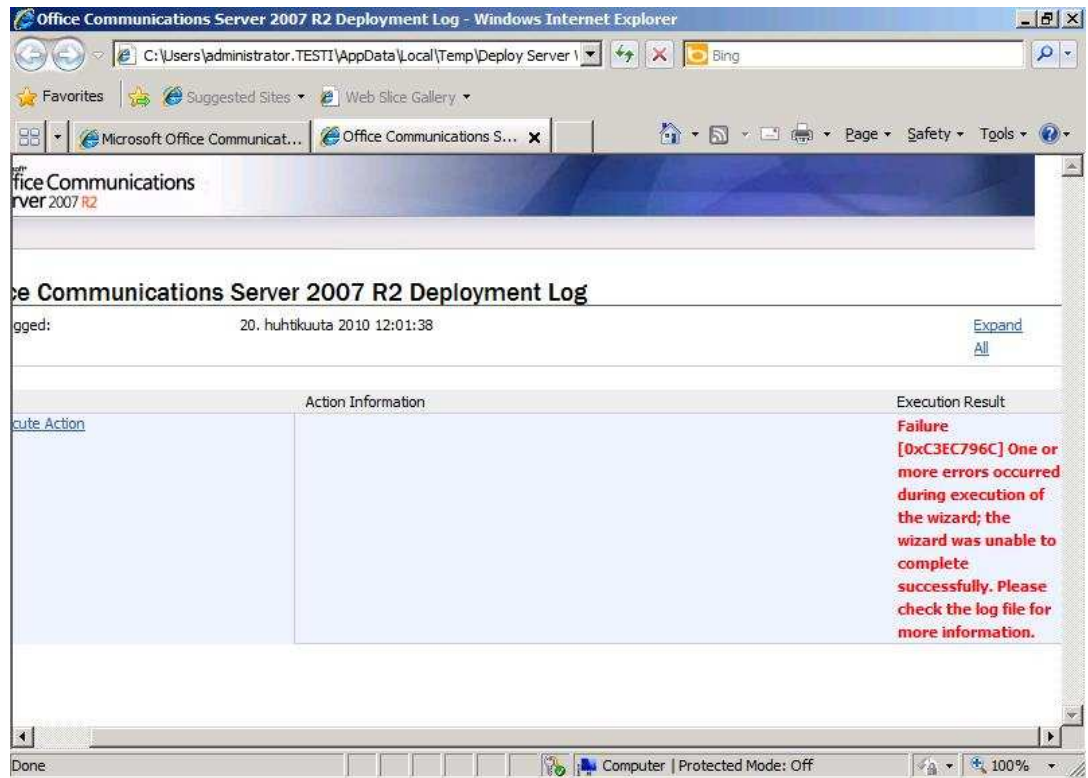
RTC log:  Browse...

< Back   Next >   Cancel

*Kuva 14. Location for Database Files*

Asennus määrittää parhaan sijainnin tietokannalle ja lokeille automaattisesti. Järkevintä suorituskyvyn kannalta on sijoittaa jokainen kansio erilliselle fyysiselle levyllä. Järjestelmälevylle ei tulisi sijoittaa yhtäkään kansiota.

Ready to Deploy Server -sivulta voi käydä vielä yhteenvedon asetuksista ja Next-painikkeella asennus suoritetaan. Ensimmäisellä kerralla testiympäristössä asennus ilmoitti virhekoodin 0xc3ec796c.



Kuva 15. Ensimmäinen asennusvirhe

Windowsin tapahtumalokissa oli virhe tapahtuma ID 30502, joka viittaa palvelimen kellon asetuksiin. Kellon asetukset olivat kuitenkin kunnossa ja synkronoitu palvelimien kesken. Myöhemmin selvisi virheilmoituksen johtuvan Microsoftin turvallisuuspäivityksestä kb974571. Vaihtoehtoina oli poistaa turvallisuuspäivitys tai asentaa Microsoftin ocsasnfix.exe korjaus palvelimelle. Ocsasnfix.exe ohjelmakorjaus asennettiin ja ajoin Deploy Serverin uudestaan OCS-asennuslevyllä. Tällä kertaa asennus onnistui, mutta sain varoitustilmoituksen koodilla 0x03ec78e4. Varoitustilmoitus johtui kahdesta DNS-tietueesta, jotka ocs2007r2-palvelimella oli luotu. Poistin toisen DNS-tietueen, mutta en katsonut tarpeelliseksi ajaa Deploy Serveriä uudestaan.

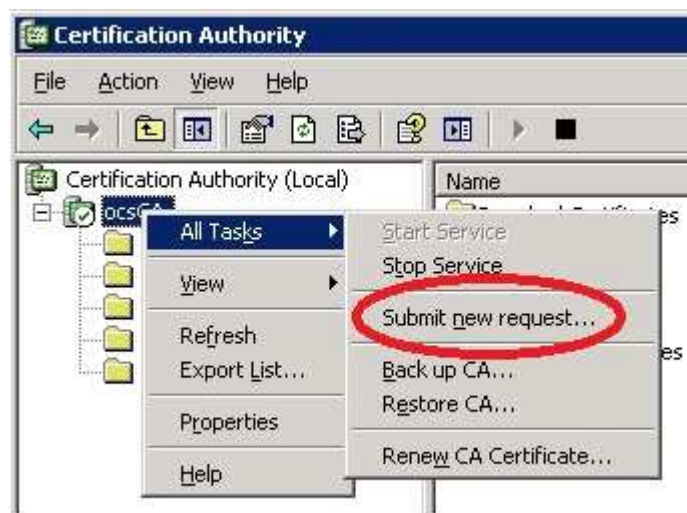
### Configure Server

Kohdassa kaksi konfiguroidaan palvelin. Konfigurointivelho pyytää aluksi valitsemaan konfiguroitavan palvelimen listasta, jonka jälkeen valitaan SIP toimialue. SIP toimialue tulisi olla listassa valmiina valittavana, jos ei ole toimialue tulee lisätä siihen add-painikkeen kautta. Seuraavaksi valitaan asiakaskoneiden kirjautumisasetukset. Asiakaskoneiden haluttiin voivan kirjautua automaattisesti, joten valitsin kohdat Some or all clients will use DNS SRV records for automatic logon ja Use this server or pool to authenticate and re-

direct automatic client logon requests. Tuotantoympäristössä ollessa useita OCS-palvelimia vain yksi palvelin hoitaa automaattisen kirjautumisen. SIP Domains for Automatic Logon -sivulla valitaan toimialueet, jotka halutaan automaattisen kirjautumisen piiriin. Yhteenvetosivun jälkeen velho suorittaa konfiguroinnin.

### Configure Certificate

OCS-palvelimen ja ohjainkoneen välille on muodostettava luottosuhde sertifikaatilla, jotta kaikki OCS-palvelut toimivat oikein. Tällä sertifikaattivelholla on mahdollista luoda uusi sertifikaatti, käsitellä offline sertifikaatti pyyntö tai ottaa käyttöön valmis sertifikaatti. Web Components -palvelu sertifioidaan IIS hallintakonsolin kautta sertifikaatin on oltava sama kuin Configure Certificate Wizardilla tehty. Testiympäristössä sertifiointi toteutettiin tekemällä ohjainkoneesta juurivarmentaja, joka myöntää tarvittavat sertifikaatit.



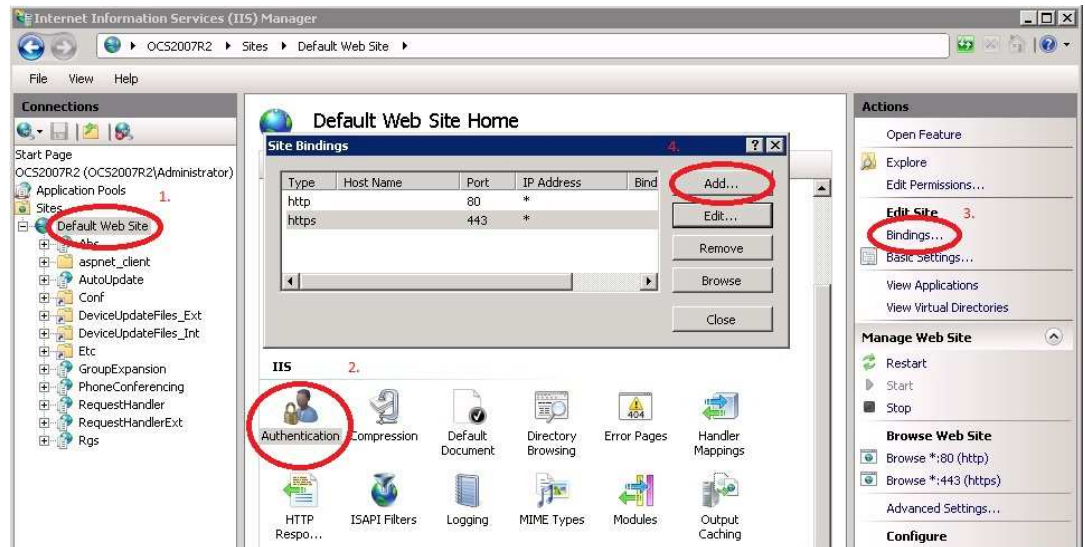
Kuva 16. Sertifikaatin pyyntö

Avattiin ohjainkoneen Certification Authority, josta pyydettiin uusi sertifikaatti. Tämä sertifikaatti tallennetaan tiedostoksi, joka siirrettiin ocs2007r2 palvelimelle.

Configure Certificate on kohta kolme Deploy Standard Edition Wizardissa. Sertifikaatit konfiguroidaan klikkaamalla viereistä run painiketta. Available certificates tasks sivulta valittiin Assign an existing certificate ja tämän jälkeen valittiin sertifikaatti, joka oli juuri tallennettu ohjainkoneesta.

### Configure Web Components Server Certificate

Kohdassa neljä tuodaan sertifikaatti IIS-palvelulle ja tämä tehdään manuaalisesti, kuten aikaisemmin mainitsin. IIS-hallintakonsoli avataan Administrative Toolssin kautta.



Kuva 17. IIS-hallintakonsoli

IIS-hallintakonsolista valitaan ensimmäiseksi ocs2007r2-palvelimen alta Default Web Site. Toiseksi Authentication, kolmanneksi Bindings ja Site Bindingsin alta Add. Tyypiksi valitaan https ja SSL-sertifikaatiksi valitaan sama sertifikaatti, kuin aikaisemmin. IP-osoitteena All Unassigned ja porttina 443.

### Verify Replication

Kohta viisi tehdään myös manuaalisesti, jossa todennetaan aktiivihakemiston replikoinnin tila. Todennus tehdään komentoriviltä komennolla.

```
LcsCmd /server /action:CheckLCServerState /role:se
/PDCRequired:FALSE
```

Komento luo lokin replikoinnin tilasta, jossa tulisi kaikissa kohdissa olla maininta Success. Loki löytyy hakemistosta C:\Users\administrator.TESTI\AppData\Local\Temp.

### Start Services

Kohdassa kuusi käynnistetään asennetut palvelut. Tässä vaiheessa on oleellista pitää Windowsin palomuri päällä, jotta OCS-asennus osaa avata tarvittavat portit palomuriin. Start Services -velho ilmoittaa yhteenvetona,



mitkä palvelut käynnistetään ja klikkaamalla Next-painiketta palvelut käynnistetään. Testiympäristössä käynnistettävät palvelut.

- Front-End
- Telephony Conferencing
- IM Conferencing
- Web Conferencing
- Audio/Video Conferencing
- Application Sharing
- Monitoring Agent
- Conferencing Attendant
- Conferencing Announcement
- Response Group
- Outside Voice Control.

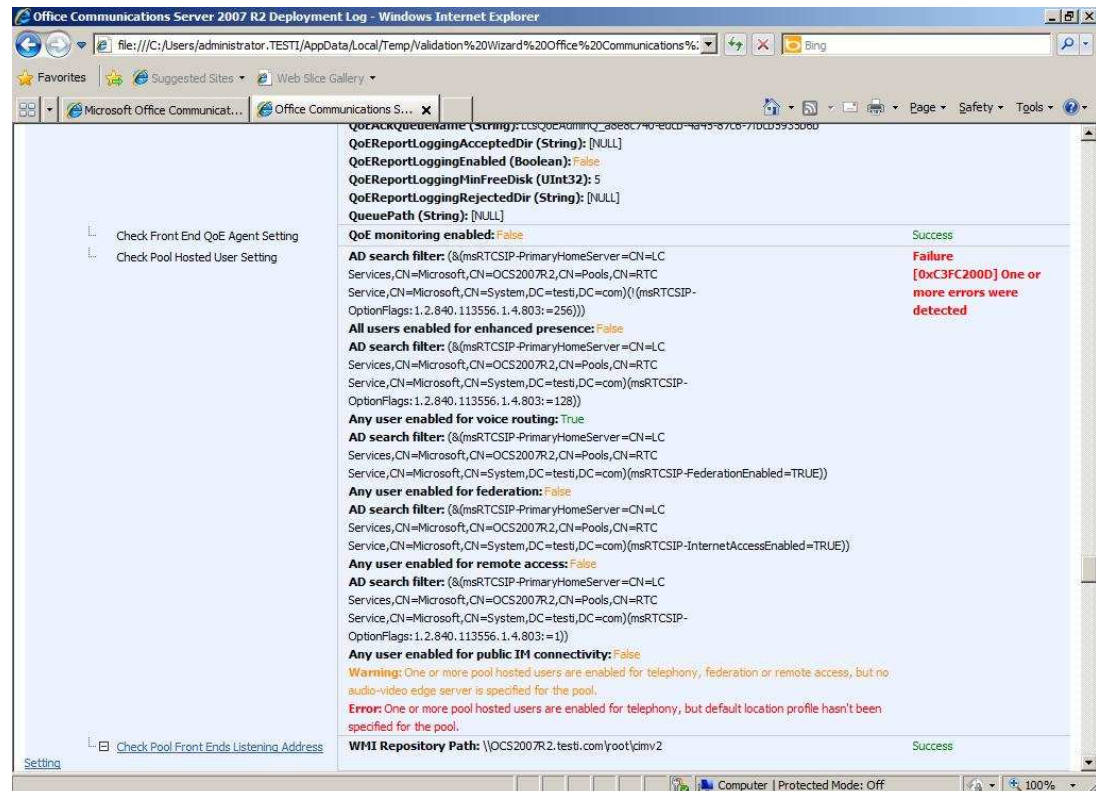
Ensimmäisellä käynnistyskerralla saatiin virheilmoitus 0xc3ec79e6. Virheilmoitus johtuu siitä, että palvelimella ei ole Message Queuing -ominaisuus päällä. Tätä ominaisuutta tarvitsee ainakin Monitoring Agent. Message Queuing asennetaan Server 2008 -käyttöjärjestelmässä Server Managerin kautta. Managerista valitaan Features ja Add Features. Add Features velhosta valitaan Message Queuing ja klikataan Next. Asennuksen jälkeen kaikki palvelut käynnistyivät ongelmitta.

#### Validate Server Functionality

Deploy Standard Edition seitsämäs ja viimeinen askel koostuu useasta kohdasta, joissa OCS velho tarkistaa asetusten toiminnan. Validate Server Functionality kohdat ovat.

- Validate Front End Server Configuration
- Validate Web Components Server Configuration
- Validate Web Conferencing Server Configuration
- Validate A/V Conferencing Server Configuration
- Validate Application Sharing Server Configuration
- Validate Application Functionality.

Validate Front End Server Configuration vahvistaa Front End palvelimen toiminnan. Tämä kohta tuotti virheilmoituksen Failure [0xc3fc200d] One or more errors were detected.



Kuva 18. Front End Server Validation

Virheilmoitus syyksi ilmoitetaan, että yhdelle tai useammalle käyttäjälle on aktivoitu palveluita, jotka tarvitsevat edge palvelimen ja default location profiilen. Default location profiilen määrittäminen ei kuitenkaan poistanut ilmoitusta. Käyttäjää ei myöskään ollut tässä vaiheessa luotu. Käytiin läpi aktiivihakemiston kaikki käyttäjät ja varmistettiin, että yhtäkään käyttäjää ei ollut aktivoitu Office Communicationssia varten. Kaikki muut asetusten vahvistukset onnistuivat ilman virheilmoituksia, joten päätin sivuuttaa Front End palvelimen tuottaman virheilmoituksen. Validate Application Sharing Server Configuration antoi varoituksen koodilla 0x43fc200c. Varoitus liittyy Communicator Web Accessin sisäiseen URL:iin, jota ei oltu vielä määritetty. [2, s. 10 - 32.]

#### 4.2.5 Käyttäjien luonti ja aktivointi

Käyttäjät luodaan OCS:n samalla tavalla kuin normaaliin toimialueeseen aktiivihakemiston kautta. Aktiivihakemistossa olevat käyttäjät aktivoidaan OCS:ää varten. Tämä tapahtuu tuplaklikkaamalla haluttua käyttäjää aktiivihakemistosta ja valitsemalla Communications-välilehti.

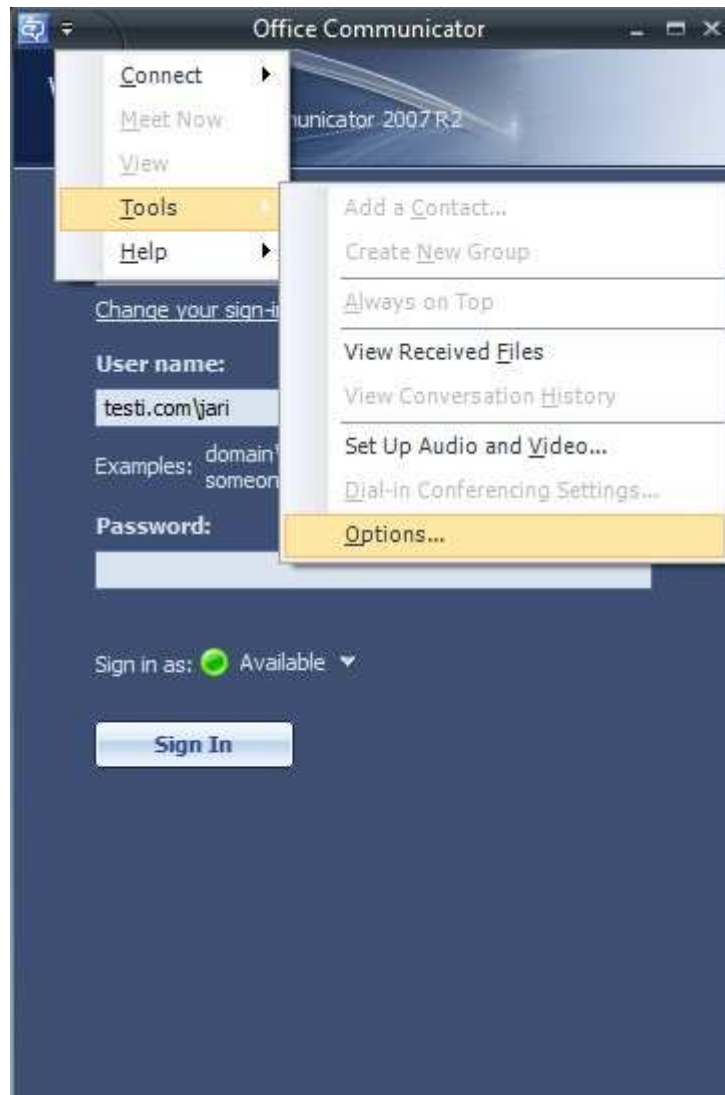


Kuva 19. AD-käyttäjä

Välilehdeltä ruksitaan Enable user for Office Communications Server, kirjoitetaan haluttu kirjautumisnimi, valitaan palvelin ja toimialue. [2, s. 38 - 40.]

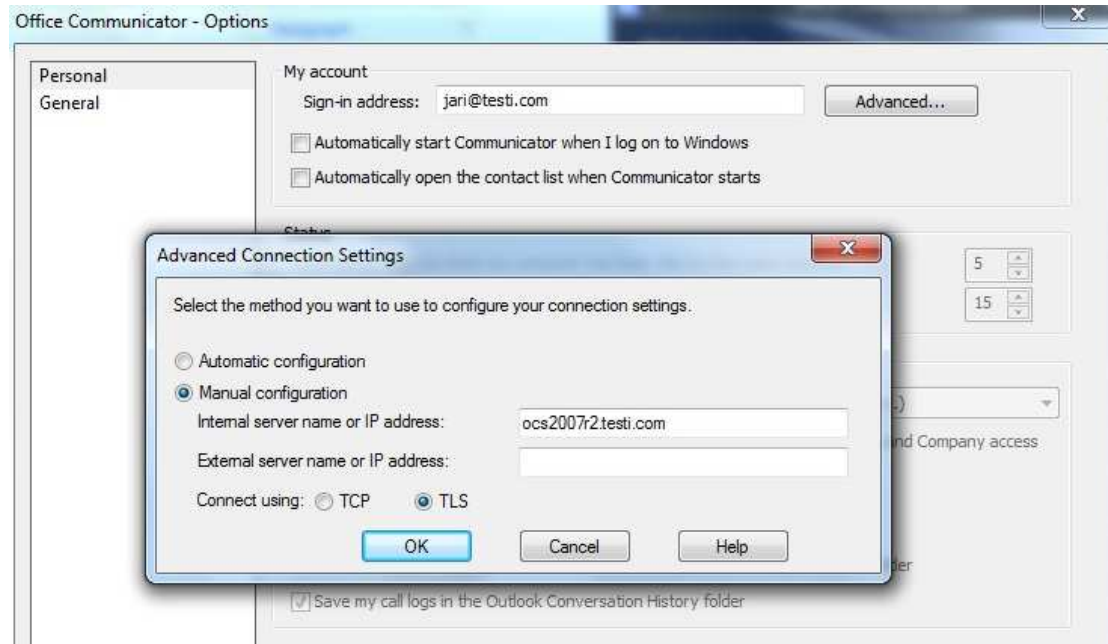
### 4.3 Microsoft Office Communicator R2

Microsoft Office Communicator R2 (MOC) on asiakaskoneisiin asennettava pikaviestinsovellus, joka mahdollistaa viestinnän Office Communications Serverin kautta. Testiympäristöön asennettiin MOC viiteen kannettavaan tietokoneeseen paikallisesti Communicator.msi-asennuspaketista. Paikallinen asennus on hyvin yksinkertainen ja asetukset määritellään vasta asennuksen jälkeen käynnistämällä Communicator ja valitsemalla ylävalikosta Tools ja Options.



Kuva 20. Communicator

Options-valikosta voidaan valita henkilökohtaiset asetukset ja yleiset asetukset.



Kuva 21. Options & Advanced

Oleelliset asetukset ovat Sign-in address ja Advancedin alla Internal server name. Advanced Connection asetuksista kirjoitettiin sisäiseksi palvelimen nimeksi ocs2007r2.testi.com ja yhteydeksi TLS. Aktiivihakemistoon olin luonut käyttäjän Jari, joten käytin sisäänkirjautumisosoitteena [jari@testi.com](mailto:jari@testi.com). Oletuksena MOC asettaa Personal information manageriksi Microsoft Office Outlookin. Tämä kuitenkin antaa virheilmoituksen testiympäristössä, koska Exchange ei ole käytössä. Sisäänkirjautuminen Communicatorilla onnistui ongelmitta asiakaskoneen ollessa toimialueeseen kirjautuneena. Office Communicatorin käyttö onnistuu myös toimialueen ulkopuoliselta tietokoneelta, jos tietokoneeseen on tuotu sertifikaatti toimialueen juuri-varmentajasta.

#### Turva-asetukset

Communicatorin turva-asetuksia on tarkoitus hallita palvelimelta käyttämällä Group Policy Object Editoria (GPO). Testiympäristössä muutettiin turva-asetukset paikallisesti asiakaskoneelta käsin. Tähän tarvitaan Communicator.adm tiedostoa, joka on Administrative Template eli asetusmalli. Communicator.adm tiedosto on ladattavissa Microsoftin verkkosivuilta. Asiakaskäyttöjärjestelmässä Group Policy Object Editor avataan Microsoft Management Consolen (MMC) kautta. GPO lisätään MMC:hen tiedostovalikon kautta. GPO:sta valitaan Computer Configuration ja klikataan Administrative Templates kohtaa oikealla hiiren näppäimellä. Avautuvasta valikosta valitaan

Add Template ja sitten valitaan aikaisemmin tallennettu Communicator.adm tiedosto. Tämän jälkeen Administrative Templates hakemistosta löytyy Microsoft Office Communicator Policy Settings -kansio, josta voidaan muunmuassa turva-asetuksia muuttaa. Turva-asetuksista jouduin laittamaan kuvassa 22 näkyvän turva-asetuksen päälle soitettaessa videopuhelua MXP:n ja Office Communicatorin välillä.

Setting	State
Prevent users from saving instant messages	Not configured
Time out to close IM session due to inactivity	Not configured
Block conversation from federated contacts	Not configured
<b>Specify encryption for computer-to-computer audio and video calls</b>	<b>Enabled</b>
Enables Full Screen Video and video preview disabled for all OC video calls	Not configured
Enables or disables application sharing encryption in peer to peer (2 user) c...	Not configured
Disables sharing control with users in an application sharing session.	Not configured
Enable the state Appear Offline	Not configured

Kuva 22. Communicator turva-asetus

#### 4.4 Tandbergin yhteentoimivuus OCS-ympäristössä

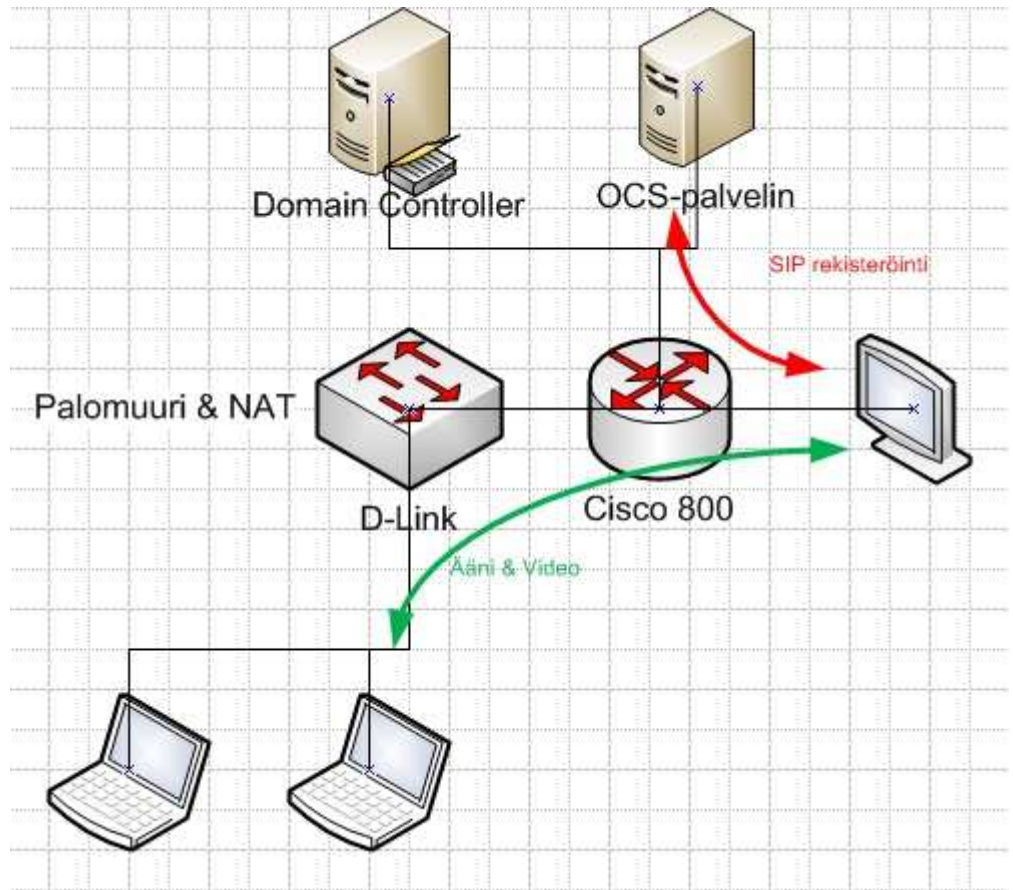
Testasimme Tandbergin MXP 1700 -videoneuvottelulaitteen toimivuutta Office Communications Serverin kanssa. Tandberg on vuosia kehittänyt yhteensopivuutta Microsoftin tuotteiden kanssa. MXP 1700 -päätelaitteen rekisteröinti Office Communications Server -palvelimeen onnistui helposti. Eniten testausta vaikeutti D-link kytkimessä ollut palomuri ja sen vaikutus MXP:n ja OCS-ympäristön välillä. MXP 1700 rekisteröityy Office Communications Serveriin suoraan SIP-viesteillä. SIP-rekisteröinti on edellytys suoraan yhteentoimivuuteen ilman erillistä gatekeeper-laitetta. Tandberg Video Communication Server (VCS) mahdollistaa myös esimerkiksi aikaisempaan H.323 standardiin perustuvien laitteiden yhteentoimivuuden OCS-ympäristössä. VCS-laitteisto kommunikoi OCS-palvelimen kanssa SIP-protokollalla ja kaikki laitteet, jotka rekisteröityvät VCS:ään ovat yhteentoimivia OCS-ympäristössä. Emme onnistuneet testaamaan VCS toimivuutta OCS-palvelimen kanssa koska VCS laitteessamme ei ollut tarpeeksi uutta ohjelmistoversiota. VCS laitteemme versio oli x1.2 ja OCS yhteentoimivuuteen tarvittava toiminnallisuus on vasta versioissa x3 eteenpäin.

MPX

MXP-videoneuvottelulaitteen rekisteröiminen aloitetaan samalla tavalla, kuin Microsoft Communicator -käyttäjien rekisteröinti. Luodaan aktiivihakemistoon MXP-laitteelle käyttäjätili. Käyttäjätilin nimeksi luotiin timetraveller, jonka sip uri on siis <sip:timetraveller@testi.com>. MXP:n asetukset syötetään web-selaimen kautta. Oleelliset asetukset OCS:n ja MXP:n välillä liittyvät SIP-asetuksiin, jotka tulee asettaa seuraavalla tavalla:

- SIP-moodi päälle ja tyyppi Microsoft
- SIP uri [timetraveller@testi.com](sip:timetraveller@testi.com)
- Server Discovery manuaalinen
- Server Address kohtaan tulee OCS-palvelimen ip-osoite
- Transport TLS
- Verify TLS pois päältä
- SIP-tunnistukseen syötetään käyttäjänimeksi ja salasananaksi samat arvot, kuin aktiivihakemistoon.

Kuvassa 23 on kuvattu MXP:n sijainti testiympäristön verkossa, ja SIP-rekisteröinti OCS-palvelimelle. MXP-laite rekisteröityi suoraan OCS-palvelimen kanssa ja läsnäolotiedot päivittyivät oikein, mutta videopuheluiden muodostaminen ei täysin onnistunut. Ensimmäisillä yrityksillä kannettavien tietokoneiden Communicator-ohjelmisto antoi virheilmoituksen: Incompatible security setting. The call could not be completed because security levels do not match. Virheilmoitus postui asettamalla Communicatoriin kuvassa 22 näkyvä turva-asetus päälle. Tämän jälkeen videopuhelu yhteys onnistui toiseen suuntaan. MXP-laite vastaanotti kuvaa ja ääntä normaalisti, mutta Communicator oli puhelunmuodostamistilassa eikä pystynyt vastaanottamaan kuvaa eikä ääntä. Testiympäristön D-Linkissä olevat palomuri ja NAT-osoitteenmuunnos vaikuttivat videopuhelunmuodostukseen. Tämä selvisi sijoittamalla kannettava tietokone myös Cisco 800 -reitittimeen MXP:n kanssa. Molempien osapuolten kommunikoidessa suoraan ilman D-Linkin väliintuloa videopuhelu toimi normaalisti. Kahdella kannettavalla ja MXP-laitteella onnistuimme monipisteneuvottelussa, kun kaikki laitteet olivat Cisco 800 -reitittimessä kytkettyinä.



Kuva 23. Testiympäristön SIP ja media -virrat

## 5 YHTEENVETO

Insinööriyössä otettiin käyttöön Microsoft Office Communications Server 2007 R2 Standard Edition. OCS-ympäristössä on tärkeää ottaa huomioon SIP-protokollan toiminnallisuus ja sen tuomat vaatimukset yritysverkolle. SIP-viestien välittäminen NAT:n ja palomuurin läpi ei ole yksiselitteistä. Myös Tandbergin toiminnallisuutta testattiin OCS-ympäristössä. Tandbergin ja Microsoftin yhteentoimivuus on selvästi hyvin pitkälle vietyä. Tandberg on lisännyt ohjelmistopäivityksillä laitteisiinsa yhteentoimivuuden kannalta tärkeitä ominaisuuksia. Testatut MXP- ja VCS-laitteistot ovat helppokäyttöisiä toimivan web-selainpohjaisen hallinnan ansiosta.

Testausvaiheessa Communicator-sovellusten väliset videopuhelut, pikaviestit ja tiedostojen jako toimivat ilman ongelmia. Communicatorien väliseen viestintään ei vaikuttanut myöskään D-Linkin kytkin millään tavalla. Testauksessa havaittiin ongelmia MXP:n ja Office Communicatorin välisen videopu-



helun muodostamisessa. Ongelmat poistuivat ottamalla D-Linkin kytkin välis-  
tä pois. MXP:n ongelmat liittyvät todennäköisesti, jollain tavalla NAT osoit-  
teenmuutokseen.

Testiympäristöön ei kuulunut Edge-palvelinta, joka vaaditaan sisäverkon ul-  
kopuoliseen viestintään. Ilman Edge-palvelinta ja kunnollista palomuuria  
OCS-ympäristö ei ole tarpeeksi tietoturvallinen käytettäväksi ulkoisen verkon  
yli kommunikointiin. Tandbergin VCS-laitteistolla on kuitenkin mahdollista  
yhdistää turvallisesti julkisen verkon yli Tandbergin laitteistoa Microsoftin si-  
säiseen OCS-ympäristöön. Tässä työssä oleva testiympäristö on varsin yk-  
sinkertainen ja laajennettavissa huomattavasti. Seuraavat toimenpiteet tes-  
tiympäristön kehittämisessä liittyvät Edge-palvelimen ja VCS-laitteiston käyt-  
töön ottoon sekä testaukseen.

## LÄHTEET

- [1] Preparing Active Directory Domain Services for Office Communications Server 2007 R2 [Verkkodokumentti]. 2009. [Viitattu 26.4.2010]. Saatavissa: <http://go.microsoft.com/fwlink/?LinkID=151920>.
- [2] Deploying Office Communications Server 2007 R2 Standard Edition [Verkkodokumentti]. 2009. [Viitattu 26.4.2010]. Saatavissa: <http://go.microsoft.com/fwlink/?LinkID=151911>.
- [3] Microsoft Office Communications Server -kotisivut: <http://www.microsoft.com/communicationsserver/en/gb/capabilities.aspx>. [Viitattu 26.4.2010].
- [4] Microsoft Office Communications Server 2007 R2 Technical Overview [Verkkodokumentti]. 2009. [Viitattu 26.4.2010]. Saatavissa: <http://go.microsoft.com/fwlink/?LinkID=151915>.
- [5] Internet Engineering Task Force. SIP: Session Initiation Protocol [Verkkodokumentti]. 2002. [Viitattu 26.4.2010]. Saatavissa: <http://tools.ietf.org/html/rfc3261>.
- [6] Sinnreich, Johnston. Internet Communications Using SIP. Wiley Publishing 2006.
- [7] Internet Engineering Task Force. The Transport Layer Security (TLS) Protocol Version 1.2. [Verkkodokumentti]. 2008. [Viitattu 26.4.2010]. Saatavissa: <http://tools.ietf.org/html/rfc5246>.
- [8] Thomas. SSL and TLS Essentials Securing the Web. Wiley Publishing 2000.
- [9] Parker, Van Doren. Kustannusten ja resurssien säästäminen yhdistetyn viestinnän ratkaisulla [Verkkodokumentti]. 2009 [Viitattu 26.4.2010]. Saatavissa: [http://download.microsoft.com/download/0/B/A/0BA1D6E7-252E-478C-81B3-D0C3D6696D65/Achieving%20Cost%20and%20Resource%20Savings%20with%20Unified%20Communications\\_FI.pdf](http://download.microsoft.com/download/0/B/A/0BA1D6E7-252E-478C-81B3-D0C3D6696D65/Achieving%20Cost%20and%20Resource%20Savings%20with%20Unified%20Communications_FI.pdf).
- [10] Minasi. Mastering Windows Server 2003. Sybex Inc 2003.
- [11] Tandberg Solution Guide TANDBERG Telepresence and Video Conferencing with Microsoft Office Communications Server 2007 R2 [Verkkodokumentti]. 2010. [Viitattu 1.6.2010]. Saatavissa: <http://www.tandberg.com/collateral/TANDBERG%20Telepresence%20and%20Video%20Conferencing%20with%20Microsoft%20Office%20Communications%20Server%20Solution%20Guide.pdf>.