Kari-Pekka Kauhanen

# ETÄYHTEYDET

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Luonnontieteiden ala
Tietojenkäsittely
1.3.2011

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**OPINNÄYTETYÖ**
**TIIVISTELMÄ**

| | |
|---|---|
| Koulutusala<br>Luonnontieteiden ala | Koulutusohjelma<br>Tietojenkäsittely |
| Tekijä(t)<br>Kari-Pekka Kauhanen | |
| Työn nimi<br>Etäyhteydet | |
| Vaihtoehtoiset ammattiopinnot | Ohjaaja(t)<br>Tarja Karjalainen |
| | Toimeksiantaja |
| Aika<br>1.3.2011 | Sivumäärä ja liitteet<br>43 |


Opinnäytetyön tavoitteena on perehtyä etäyhteyden teoriaan ja tutkia teorian pohjalta erilaisia etäyhteysohjelmistoja. Tutkimuksen tarkoituksena on ottaa selvää etäyhteysohjelmistojen tietoturvaominaisuuksista ja kuinka paljon eri etäyhteysohjelmistot rasittavat tietokoneen resursseja. Tuloksien perusteella valitaan yhteensopivin etäyhteysohjelmisto organisaatiokäyttöön.

Opinnäytetyö käsittää teoriaosan, jossa kerrotaan erilaiset etäyhteysprotokollat. Etäyhteysprotokollista kerrotaan tärkeimmät ominaisuudet ja protokollan toimintaperiaate. Etäyhteysprotokolliin kuuluu esimerkiksi VNC, RDP, X11 ja PcoIP –protokollat. Protokollan tarkka teoriatuntemus auttaa selvittämään eri käyttötarkoituksiin parhaiten sopivan protokollan.

Opinnäytetyö käsittää tutkimusosion, joka tarkastelee VNC- ja RDP-protokollia käyttäviä etäyhteysohjelmistoja, koska VNC- ja RDP-protokolla ovat käytetyimmät etäyhteysprotokollat. Tutkimus käsittää ohjelmistojen asennuksen, yhteyden muodostuksen ja käytettävien tietokoneen resurssien mittauksen.
Asennusvaiheessa etäyhteysohjelmisto asennetaan yhteyden muodostusta varten. Yhteyden muodostuksessa tutkitaan miten yhteys muodostetaan käytettävällä etäyhteysohjelmistolla ja mitä tietoturvaominaisuuksia on valittavana. Resurssien mittauksessa tutkitaan kuinka paljon etäyhteysohjelmisto kuormittaa tietokoneen resursseja. Tietokoneen resursseihin kuuluu prosessorin suorituskyky, keskusmuistin kuormitus ja verkkoliikenteen kuormitus.

Opinnäytetyön tuloksissa esitellään tutkimustulokset ja pohditaan lyhyesti mitä jatkotutkimuksia olisi mahdollista tehdä. Tulokset tietoturvaominaisuuksista kerrotaan lyhyenä vertailuna keskenään. Tulokset resurssien käytöistä esitellään pienessä taulukossa.


| | |
|---|---|
| Kieli | Suomi |
| Asiasanat | Etäyhteys, Opinnäytetyö, Internet, Protokolla, Tietoliikenne |
| Säilytyspaikka | ☒ Verkkokirjasto Theseus<br>☐ Kajaanin ammattikorkeakoulun kirjasto |

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**THESIS ABSTRACT**

| School<br>School of Business | Degree Programme<br>Information Technology |
|---|---|
| Author(s)<br>Kari-Pekka Kauhanen | |
| Title<br>Remote Connections | |
| Optional Professional Studies | Instructor(s)<br>Tarja Karjalainen |
| | Commissioned by |
| Date<br>1.3.2011 | Total Number of Pages and Appendices<br>43 |


The object of the thesis is to get orientated with the theory of the remote connections and to examine various remote connection software by theoretical means. The main object of the research is to determine the security options of remote connection software and how much the recourses of the computer is used by a remote connection software. The most compatible remote connection software for common organization use is chosen based of the research outcome.

Thesis includes a theory section in which all the various remote connection protocols are examined. The most important features and the principle of a remote connection protocol are included in the examination. Various remote connection protocols, for example, are: VNC, RDP, X11 and PcoIP. The exact knowledge of the remote connection protocol assists one to determine the best remote connection software to be used in different uses.

Thesis includes a research section in which several VNC and RDP remote connection software are inspected. Research consists of installing a software, forming a remote connection with specific software and examining security options. First section includes installing a remote connection software and readying the software for forming a remote connection. Second section includes forming a remote connection with different remote connection software and examining all the various security options in the remote connection software. Final section includes monitoring how much all the remote connection software load the resources of the computer. the recourses of a computer are the performance of the processor, the load of the base memory and the load of the network.

All the research results are listed in the result section of the thesis. Furthemore the possible follow-up research are discussed after the results. The results of the security options are listed as a short comparison with themselves. The results of the resource monitoring are presented in a small table.



| | |
|---|---|
| Language of Thesis | Finnish |
| Keywords | Remote Connection, Thesis, Internet, Protocol, Data communication |
| Deposited at | ☒ Electronic library Theseus<br>☐ Library of Kajaani University of Applied Sciences |

SISÄLLYS

SYMBOLILUETTELO

| | |
|---|---|
| ALDP | Appliance Link Device Protocol. Protokolla, joka määrittää käytettvät laitteet, kuten äänet, ALP-protokollassa. |
| ALRP | Appliance Link Render Protocol. Protokolla, joka määrittää grafiikan ALP-protokollassa. |
| ALSP | Appliance Link Session Protocol. Protokolla, joka määrittää istunnot ALP-protokollassa. |
| ALP | Appliance Link Protocol. Sun Microsystemsin kehittämä etäyhteysprotokolla. |
| API | Application Programming Interface. Ohjelmointirajapinta. |
| ARD | Apple Remote Desktop. Applen kehittämä etäyhteysprotokolla. |
| Authentication Scheme | Autentikointiskeema. Määrittää käytettävän autentikointimuodon. |
| Client | Asiakassovellus tai –ohjelmisto. |
| Copy Rectangle Encoding | Yksi VNC-protokollan yhteyden koodausmenetelmistä. |
| CoRRE | Compact RRE. Yksi VNC-protokollan yhteyden koodausmenetelmistä. kts. RRE Encoding |
| DES | Data Encryption Standard. Standardiksi valittu salausmenetelmä. |
| DLL | Dynamic-Link Library. Jaettu kirjasto, joka jakaa ohjelmakoodia usean eri ohjelman kesken. |

| | |
|---|---|
| Encoding | Koodaus. Menetelmä, jolla haluttu tieto muutetaan toiseen muotoon. |
| Flash | Adobe Systemsin kehittämä ympäristö multimediaesityksille. |
| Framebuffer | Kuvapuskuri. Laite, joka tulosta muistipuskurista kokonaisen kuvan. |
| Format | Tiedostomuoto. Tallennetun tiedon rakennetyyppi. |
| GB | Gigabyte. Tuhat miljoonaa tavua (byte). Yleensä ilmaus keskusmuistin koolle. |
| GHz | Gigahertz. Tuhat miljoonaa värähtelyä yleensä sekunnissa. Taajuuden ilmaisin yleensä prosessoreille. |
| GDI | Graphics Device Interface. Rajapinta, joka ohjaa graafiset tiedot näytöille. |
| GPLv2 | GNU General Public License version 2. Vapaiden ohjelmistojen julkaisuun tarkoitettu lisenssi. |
| HD | High Definition. Korkealaatuinen kuva tai ääni. |
| ICA | Independent Computing Architecture. Citrixin kehittämä alustariippumaton etäyhteysprotokolla. |
| IP | Internet Protocol. Protokolla tietoliikennepakettien kuljettamiseen. |
| ITU-T | The Telecommunication Standardization Sector. Standardointijärjestö, joka koordinoi tietoliikennestandardeja. |
| Hextile Encoding | Hextilekoodaus. Yksi VNC-protokollan yhteyden koodausmenetelmistä. |
| Mbit | Megabit. Miljoona bittiä |

| | |
|---|---|
| MIT | Massachusetts Institute of Technology. Cambridgen kaupungissa (USA) sijaitseva korkeakoulu. |
| NX | NoMachinen etäyhteysmenetelmä, joka perustuu X-ikkunointijärjestelmään. |
| OS | Operating System. Käyttöjärjestelmä. |
| PcoIP | Teradicin kehittämä etäyhteysprotokolla. |
| Pixel Data | Pikselidata. Tietue, joka sisältää tiedot käsiteltävistä pikseleistä. |
| RAM | Random Access Memory. Keskusmuisti, jonne ajettavat ohjelmat tallentavat tietoa. |
| RCP | Rich Client Platform. Ohjelmisto, joka sisältää kernelin ja tietyt työkalut sovelluskehittämiseen. |
| RFB | Remote Framebuffer. Yksinkertainen etäyhteysprotokolla. |
| RDP | Remote Desktop Protocol. Microsoftin kehittämä etäyhteysprotokolla, joka on osa Remote Desktop Servicea. |
| RDS. | Remote Desktop Services. Microsoftin kehittämä eätyhteysjärjestelmä. |
| RXP | Rapid X Protocol. Go-Globalin hallinnoima etäyhteysprotokolla. |
| Raw Encoding | Raw-koodaus. Yksi VNC-protokollan yhteyden koodausmenetelmistä. |
| RRE Encoding | Rise-and-run-length –koodaus. Yksi VNC-protokollan yhteyden koodausmenetelmistä. |

| | |
|---|---|
| Roaming | Langattomassa verkossa siirtyminen tukiasema-alueelta toiselle. |
| RC4 | Ron's Code 4. RSA Securityn kehittämä salausalgoritmi. |
| RSA Security | Yhtiö, joka kehittää tietoturvaratkaisuja. Kts. RC4. |
| SPICE | Simple Protocol for Independent Computing Environments. Red Hat:n kehittämä etäyhteysprotokolla laitteistoriippumattomiin järjestelmiin. |
| SSH | Secure Shell. Tatu Ylösen kehittämä verkkoliikenteen salausprotokolla. |
| TERA | TERA Image Engine. PcoIP:n ydinosa. |
| TCP | Transmission Control Protocol. Tietoliikenneprotokolla internetyhteyksien luomista varten. |
| Thin Client | Kevyt asiakaspääte. |
| UNIX | AT&T:n kehittämä laitteistoriippumaton käyttöjärjestelmä. |
| USB | Universal Serial Bus. Sarjaväylä tietokoneessa oheislaitteiden kiinni liittämiseen. |
| VNC | Virtual Network Computing. Alunperin Olivetin kehittämä etäyhteysprotokolla. |
| WAN | Wide Area Network. Laaja-alue verkko, joka peittää isoja alueita. |
| WMI | Windows Management Instrumentation. Ohjelmien valvontaa varten kehitetty laajennusjärjestelmä. |
| X11 | kts. X Window System |
| X | kts. X Window System |

| | |
|---|---|
| X Window System | X-ikkunointijärjestelmä. MIT:n kehittämä UNIX-pohjainen ikkunointijärjestelmä |

# 1 JOHDANTO

Etäyhteyksillä on olemassa lukuisia käyttötarkoituksia, jotka voivat edistää toiminnallisuutta organisaatioissa riippuen siitä, minkälaisesta organisaatiosta on kyse. Tämän opinnäytetyön keskeinen ajatus on siinä, miten etäyhteyksiä voi hyödyntää tehokkaasti organisaatioissa eri käyttötarkoituksiin.

Opinnäytetyön tarkoituksena on ottaa selvää eri vaihtoehdot etäyhteyksille, miten ne toimivat, vertailla eroja ja hakea selvä johtopäätös siitä, että mikä etäyhteysvaihtoehdoista soveltuu mihinkin käyttötarkoitukseen ja tutkia etäyhteysvaihtoehtojen ominaisuuksia. Etäyhteyksien tarkempi kartoittaminen on tärkeää, koska nykyaikana organisaatioissa käytetään kyseistä yhteyskäytäntöä.

Opinnäytetyön keskeisin tutkimustyö sisältää tutkimuksen yleisimmin käytettyjen etäyhteysohjelmistojen ominaisuuksista, verkkoliikenteestä ja tietoturvaominaisuuksista. Tutkimus rajoitetaan etäyhteysohjelmistojen ilmaisversioihin.

# 2 ETÄYHTEYDET JA ETÄYHTEYDEN TEORIA

Etäyhteys on keino saada pääsy johonkin tietokoneeseen tai verkkoon. Etätietokone voi sijaita fyysisesti toisessa maassa tai jopa viereisessä huoneessa. Organisaatioiden henkilöillä voi olla tarvetta päästä organisaation verkkoon matkustuksenkin aikana. Näitä tilanteita varten on kehitetty useita etäyhteyteen soveltuvia protokollia ja ohjelmistoja, jotka käyttävät kyseisiä protokollia. (SearchMidMarketSecurity.com 2009.)

## 2.1 Etäyhteyden toimintaperiaate

Etäyhteyden periaate on yksinkertaisesti yhteyden ottaminen toiseen tietokoneeseen ja etätietokoneen hallitseminen. Etäyhteyssovellukset määrittävät palvelimena toimivan tietokoneen, johon asiakastietokone voi ottaa yhteyttä. Palvelintietokone kaappaa kuvan näytöntilastaan ja pakkaa sen jollakin pakkausmenetelmällä. Seuraavaksi kuva lähetetään asiakastietokoneelle, joka näyttää kuvan etäyhteysohjelmistossa. (Lacoma, T. 2010.)

## 2.2 Protokollat

Etäyhteyksiin on olemassa useita kehitettyjä protokollia, joiden toiminta vaihtelee sen mukaan, mille käyttöjärjestelmälle kyseinen protokolla on kehitetty. Protokollien toiminnat ja ominaisuudet vaihtelevat riippuen protokollan kehittäjästä ja millä tasolla graafinen työpöytä välitetään. Etäyhteysprotokollia ovat seuraavat:

- Virtual Network Computing (VNC)
- Remote Desktop Protocol (RDP)
- Apple Remote Desktop (ARD)
- NX Technology (NX)
- Independent Computing Architecture (ICA)

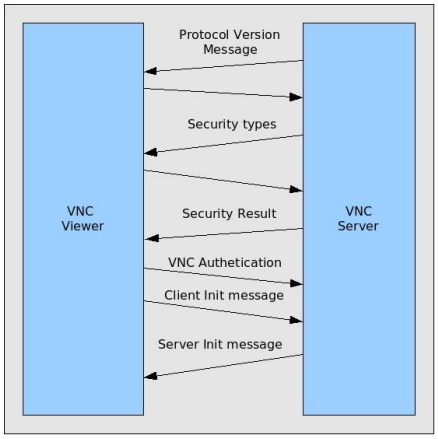
- X Window System (X11)
- Rapid X Protocol (RXP)
- Appliance Link Protocol (ALP)
- Proxy Protocol

(The free dictionary 2010.)

## 2.3 VNC / RFB

RFB (Remote Framebuffer Protocol) on yksinkertainen protokolla graafisen käyttöliittymän etäkäyttöön. Monissa vanhemmissa dokumenteissa ja julkaisuissa VNC-protokollaa on kutsuttu RFB-protokollaksi, mutta nykyään termi VNC on vakiintunut. (Emery, V. 2003.)

VNC koostuu kahdesta erilaisesta osasta. Palvelimesta (server), joka generoi graafista dataa ja asiakassovelluksesta (client), joka piirtää graafisen datan käyttäjän tietokoneelle. Toiminta on esitetty kuviossa 1. VNC:stä puhuttaessa asiakassovelluksesta käytetään nimeä viewer. Palvelin ja asiakassovellus voivat olla eri tietokoneilla ja eri käyttöjärjestelmillä. Sen lisäksi mitään tilaa ei tallenneta asiakassovellukseen, joten datan häviämistä ei tapahdu, jos yhteys katkeaa ja yhteys joudutaan muodostamaan uudelleen palvelimen ja asiakassovelluksen välille. (Richardson, T. 2010.)




Kuvio 1. RFB-protokollan toiminta. (Life's Good 2010.)

Koska RFB-protokolla toimii kuvapuskuri-(Framebuffer) tasolla, sitä voidaan käyttää kaikissa ikkunoiduissa käyttöjärjestelmissä ja sovelluksilla. Näihin kuuluu UNIX-käyttöjärjestelmät, MAC-käyttöjärjestelmät, eri Linux-käyttöjärjestelmät ja kaikki Windows-käyttöjärjestelmät, sekä kaikki sovellukset edellä mainituilla käyttöjärjestelmillä. (Richardson, T. 2010.)

RFB-protokolla on ideaalinen protokolla kevyiden asiakaspäätteiden käytössä. Kevyitä Asiakaspäätteitä käsitellään tarkemmin luvussa kolme. Painotus RFB-protokollan suunnittelussa on asiakassovelluksen vähäisillä vaatimuksilla. Tällä pyritään siihen, että asiakassovellukset voidaan ajaa hyvin laaja-alaisella laitteistolla ja asiakassovelluksen käyttöönotto on mahdollisimman helppoa (Richardson, T. 2010).

RFB-protokolla tekee asiakassovelluksen tilattomaksi. Tilattomalla tarkoitetaan tilannetta, jossa käyttöliittymän tila säilyy ennallaan, kun palvelimen ja asiakassovelluksen välinen yhteys katkeaa ja yhteys muodostetaan uudelleen samaan palvelimeen. Yhteys voidaan myös muodostaa RFB-palvelimelle toisella asiakassovelluksella toisesta päätepisteestä ja graafinen käyttöliittymä säilyy ennallaan päätepisteestä huolimatta. Käyttäjällä on mahdollisuus käyttää paikasta riippumatta omia sovelluksia etäyhteysjärjestelmässä, koska sovellusten tilat säilyvät eri käyttöönottopaikkojen välillä (Richardson, T. 2010).

### 2.3.1 Näyttöprotokolla

Näyttöprotokolla VNC-protokollassa perustuu yksinkertaiseen grafiikkalauseeseen: ”aseta suorakulmio pikselidataa annettuun x- ja y-pisteeseen”. Tämä voi kuullostaa tehottomalta tavalta piirtää useat käyttöliittymän komponentit. Kuitenkin se mahdollistaa erinäiset pikselidatan koodaukset, jotka antavat joustavuutta siinä, miten eri parametrit käsitellään keskenään (Richardson, T. 2010).

Näiden suorakulmioiden sarja tuottaa kuvapuskurin päivityksen (Framebuffer update). Päivitys käsittää tietyn kuvapuskurin tilan siirtymisen toiseen tilaan. (Richardson, T. 2010).

Päivitys lähetetään palvelimelta asiakassovellukseen ainoastaan silloin, kun asiakassovellus sitä pyytää. Tämä mahdollistaa protokollan mukautuvuuden. Mitä hitaammat asiakassovellus ja verkko ovat, sitä harvemmin kuvapuskuri päivitetään. Hitailla asiakassovelluksilla ja/tai

verkoilla lyhytaikaiset kuvapuskurin tilat voidaan jättää huomoimatta, jolloin verkon kuormitus vähenee ja asiakassovellukselle kuvaa piirretään harvemmin. (Richardson, T. 2010).

### 2.3.2 Syöttöprotokolla

Protokollan syöttö perustuu tavalliseen työasematyyppiseen näppäimistöön ja osoittimeen, kuten hiireen. Syöttötapahtumat lähetetään asiakassovelluksesta palvelimelle aina, kun käyttäjä painaa näppäimistöltä jotain näppäintä tai liikuttaa hiiren osoitinta. Epästandardeissa oheislaitteissa voidaan käyttää keinotekoisia syötetapahtumia. Esimerkiksi kynällä käytettävä kirjoituspohjainen alusta voi jäljitellä näppäimistön syötetapahtumia. (Richardson, T. 2010.)

### 2.3.3 Pikselidatan esitys

RFB-palvelimen ja RFB-asiakassovelluksen ensisijaisessa vuorovaikutuksessa käsitellään muodon (format) ja koodauksen (encoding) toiminta pikselidatan lähettämisestä. Neuvottelutoiminta on suunniteltu tekemään asiakassovelluksen tehtävät mahdollisimman helpoksi. Palvelimella täytyy olla mahdollisuus välittää pikselidata siinä muodossa, miten asiakassovellus sen vaatii. Asiakassovellus voi valita muodoista ja koodauksesta parhaimmat valinnat palvelimelle, jos asiakassovellus kykenee tukemaan eri muotoja ja koodauksia. (Richardson, T. 2010.)

Pikselin muoto kuvaa jokaista väriä pikselin arvoina. Useimmat pikselin muodot ovat 32-bittinen, 24-bittinen ja 16-bittinen ”true color”, missä bittikentät pikselien arvoissa kääntyy suoraan punaisen, vihreän ja sinisen voimakkuuksiin. (Richardson, T. 2010.)

Koodaus määrittää sen, miten suorakulmion pikselidataa välitetään. Jokaisessa suorakulmiossa pikselidataan on sisälletty ylätunniste, joka kertoo pikselin X,Y sijainnin näytöllä, suorakulmion leveyden ja korkeuden sekä koodauksen tyypin, jolla pikselidata on koodattu. Tämän jälkeen tulee itse data käyttäen haluttua koodaustyyppiä. (Richardson, T. 2010.)

Protokollaa voidaan laajentaa lisäämällä uusia koodaustyyppejä. Määriteltyjä koodaustyyppejä ovat raw encoding, copy rectangle encoding, RRE (Rise-and-run-lenght) encoding, CoRRE (Compact RRE) ja hextile encoding. Käytännössä normaaleissa työasemissa voidaan käyttää

pelkästään hextile- ja copy rectangle encodingia, koska ne antavat parhaimmat datan pakkaussuhteet. (Richardson, T. 2010.)

### 2.3.4 Protokollaviestit

VNC-protokolla toimii minkä tahansa luotetettavan verkkoliikenteen avulla, joko bittivirrassa tai viestien välityksellä. Protokollaan kuuluu ensikättelyvaihe, jota seuraa normaalit protokollan vuorovaikutukset. Ensikättelyyn kuuluu ProtocolVersion, Authentication, ClientInitialisation ja ServerInitialisation -viestit. Molemmat, sekä palvelin että asiakassovellus, voivat lähettää ProtocolVersion-viestin. (Richardson, T. 2010.)

Protokolla siirtyy normaaliin toimintaan ServerInitialisation -viestin jälkeen. Tässä vaiheessa asiakassovellus voi lähettää palvelimelle haluttuja viestetä ja voi saada vastauksia palvelimelta. Kaikki nämä viestit alkavat viestityyppitavulla (message-type byte), jota seuraa viestikohtainen data. (Richardson, T. 2010.)

### 2.3.5 Ensikäsittelyviestit

Ensikättely alkaa lähettämällä ProtocolVersion-viesti palvelimelta asiakassovellukselle. Viesti ilmoittaa asiakassovellukselle sen protokollan uusimman version, jota serveri tukee. Tämän jälkeen asiakassovellus vastaa samanlaisella viestillä antaen sen version numeron, mitä oikeasti tulisi käyttää. (Richardson, T. 2010.)

Palvelimet ja asiakassovellukset pystyvät tiettyyn pisteeseen asti tukemaan alaspäinyhteensopivuutta. Palvelimien olisi pystyttävä tukemaan alaspäinyhteensopivuutta ja johonkin asti jopa ylöspäinyhteensopivuuttakin. Esimerkiksi, jos asiakassovellus vaati protokollalta 3.1 versiota, 3.0 palvelin voi olettaa, että koodaustyyppien pyyntöjen huomioimatta jättämisen jälkeenkin kaikki toimii normaalisti (Richardson, T. 2010.)

Kun protokollan versio on päätetty, serveri lähettää tietoa siitä, mitä autentikointiskeemaa (Authentication scheme) käytetään. Skeemaan lisätään arvo 0,1 tai 2. Arvo 0 (Connection failed) lisätään tapauksissa, joissa yhteyden muodotus epäonnistuu. Dataan lisätään merkkijono, joka kertoo epäonnistumisen syyn ja serveri katkaisee yhteyden. Arvo 1 (No authenti-

cation) lisätään silloin, kun autentikointia ei tarvita. Protokolla jatkaa ClientInitialisation-viestiin. Arvo 2 (VNC authentication) lisätään silloin, kun käytetään VNC-autentikointia. (Richardson, T. 2010.)

Asiakassovellus kryptaa haasteen DES:n (Data Encryption Standard) avulla käyttäen käyttäjän antamaa salasanaa avaimena ja lähettämällä vastauksen (response). Palvelin lähettää tietoa asiakassovellukselle siitä, oliko autentikointi onnistunut. Jos näin oli, niin protokolla jatkaa ClientInitialisation viestiin. Jos ei, niin palvelin katkaisee yhteyden. (Richardson, T. 2010.)

Kun asiakassovellus ja palvelin ovat varmoja siitä, että voivat keskustella keskenään, niin seuraavaksi asiakassovellus lähettää ClientIntialisation-viestin. Tähän viestiin sisältyy shared-flag -arvo. Arvo on tosi, jos palvelimen pitäisi yrittää jakaa työpyötä säilyttämällä muiden asiakassovellusten yhteydet ja epätosi, jos palvelimen täytyisi antaa halutulle asiakassovellukselle yksinoikeus katkaisemalla muiden asiakassovelluksien yhteydet (Richardson, T. 2010.)

Palvelin lähettää ServerInitialisation-viestin sen jälkeen, kun palvelin on vastaanottanut ClientInitialisation-viestin. Viesti kertoo asiakassovellukselle palvelimen kuvapuskurin leveyden ja korkeuden, pikselimuodon ja työpöydän nimen. Tärkeimpiä arvoja viestissä on server-pixel-format ja bits-per-pixel. (Richardson, T. 2010.)

Server-pixel-format määrittelee palvelimen pikselimuodon. Määritettyä muotoa käytetään, ellei asiakassovellus pyydä käytettäväksi jotain eri muotoa lähettämällä SetPixelFormat-viestiä. Bits-per-pixel on bittien määrä, jota käytetään jokaisessa pikselissä. Tämän täytyy olla suurempi tai yhtä suuri, kuin värisyvyys (depth), joka on käytettävien bittien määrä pikseliarvossa. Tällä hetkellä bits-per-pixel täytyy olla 8, 16 tai 32. (Richardson, T. 2010.)

SetPixelFormat-viesti asettaa pikselille sen muodon, jota pikselin on käytettävä FramebufferUpdate-viesteissä. Jos asiakassovellus ei lähetä SetPixelFormat-viestiä, niin palvelin lähettää pikseliarvot alkuperäisessä muodossa, joka on määritetty ServerInitialisation-viestissä. (Richardson, T. 2010.)

SetEncodings-viesti määrittää koodaustyypin, jolla pikselidata voidaan lähettää palvelimelta. Koodausten järjestys viestissä on viittaus asiakassovelluksen mieltymykseen siitä, mitä koodaustyyppiä haluttaisiin käyttää. Palvelin voi vapaasti valita käytetäänkö viestissä pyydettyä järjestystä vai ei. Pikselidata voidaan aina lähettää käyttäen raw-koodausta (raw encoding), vaikka sitä ei ole viestissä erikseen määritelty. (Richardson, T. 2010.)

FramebufferUpdate pyydetään FramebufferUpdateRequest-viestillä. Viesti ilmoittaa palvelimelle, että asiakassovellus on kuvapuskurissa x- ja y-sijainnin, leveyden ja korkeuden määrittelemällä alueella. Palvelin vastaa tähän lähettämällä FramebufferUpdate-viestin. Yksittäisellä viestillä voidaan vastata kerralla useampaan FramebufferUpdateRequest-viestiin. (Richardson, T. 2010.)

Palvelin olettaa FramebufferUpdateRequest-viestissä, että asiakassovellus säilyttää kopion kaikista tarpeellisista kuvapuskurin osista. Normaalisti palvelimelle riittää inkrementaalisten päivitysten lähetys asiakassovelluksille. Jos asiakassovellus on kadottanut kaikki tiedot tarvitsemastaan alueesta, niin asiakassovellus lähettää FramebufferUpdateRequest-viestin, jossa inkrementaaliarvo on asetettu arvoon 0. Viestillä pyydetään, että palvelin lähettää kaiken haluttua aluetta koskevan sisällön mahdollisimman nopeasti. Aluetta ei päivitetä copy rectangle –koodauksella. (Richardson, T. 2010.)

Jos asiakassovelluksella on tarvitsemansa alueen data tiedossa, niin asiakassovellus lähettää FramebufferUpdateRequest-viestin, jossa inkrementaaliarvo on asetettu johonkin muuhun arvoon, kuin 0. Kun määriteltyyn kuvapuskurin alueeseen tulee muutoksia, niin palvelin lähettää FramebufferUpdate-viestin. Nopeilla asiakassovelluksilla on mahdollista säännöstellä inkrementaalisten FramebufferUpdateRequest-viestien määrää välttääkseen tukkimasta verkkoa. (Richardson, T. 2010.)

KeyEvent-viestissä määritellään näppäinten painallukset ja vapautukset. Down-flag asetetaan joksikin muuksi, kuin nollaksi silloin, kun näppäintä painetaan. Vastaavasti, kun näppäin vapautetaan, niin down-flag asetetaan arvoon 0. Painettu näppäin itsessään haetaan ”keysym”-arvoista, jotka X Window System on määritellyt. Keysym-arvot ovat muotoa 0xffaa, jossa ”aa” on haettu näppäin. Esimerkiksi 0xffbe on F1-näppäin näppäimistöltä. (Richardson, T. 2010.)

PointerEvent-viestillä määritellään osoittimen liikkuminen, tai osoittimen näppäimen painallus tai vapautus. Viestissä määritellään, missä x- ja y-sijainnissa osoitin on ja sen hetkinen osoittimien näppäinten arvo. 0, jos näppäintä ei paineta ja 1, jos näppäintä painetaan. (Richardson, T. 2010.)

FramebufferUpdate-viesti sisältää sarjan suorakulmioita pikselidatasta, jota asiakassovelluksen olisi asetettava kuvapuskuriinsa. FramebufferUpdate-viesti lähetetään vastauksena FramebufferUpdateRequest-viestiin. Viestirakenne sitältää ensimmäisenä viestin tyypin (messa-

ge-type), jota seuraa suorakulmoiden määrä (number-of-rectangles). Jokainen suorakulmio käsittää seuraavat osat:

- X- ja Y-sijainti
- Suorakulmion korkeus ja leveys
- Koodaustyyppi

(Richardson, T. 2010.)

Tämän jälkeen lisätään pikselidata valitun koodaustyypin mukaan. Raw-koodauksessa data sisältää vain korkeus- ja leveysarvot pikseleistä. Arvot esittävät jokaista pikseliä vasemmalta oikealle yhdessä pyyhkäisyviivassa (scanline). Copy rectangle-koodauksessa data sisältää arvot scr-x-position ja scr-y-position. RRE-koodauksessa data alkaa ylätunnisteella, joka käsittää number-of-rectangles- ja background-pixel-value-tietueet. Background-pixel-valuen arvo määräytyy bits-per-pixel-tietueesta ServerIntialisation- tai SetPixelFormat-viestissä. Viimeisenä on number-of-rectangles, joka koostuu seuraavista: subrect-pixel-value, x- ja y-sijainti, leveys ja korkeus. (Richardson, T. 2010.)

CoRRE-koodauksessa ylätunnisteet ja muut tietueet ja tietueiden arvot ovat samoja, kuin RRE-koodauksessa, mutta number-of-rectangles-tietue on nimeltä number-of-subrectangles. Hextile-koodauksessa suorakulmio jaetaan tiileihin (tile), jotka ovat kooltaan 16x16 pikseliä alkaen ylhäältä vasemmalta liikkuen vasemmalta oikealle ja ylhäältä alaspäin. Jos suorakulmion leveys ei ole 16:lla kerronnainen, niin viimeisen rivin jokaisen tiilin leveys on vastaavasti pienempi. Samalla periaatteella, jos korkeus ei ole 16:lla kerronnainen, niin viimeisen rivin jokaisen tiilin korkeus on vastaavasti pienempi. (Richardson, T. 2010.)

Jokainen tiili alkaa subencoding-tyypin tavulla, joka on tietyistä biteistä koostuva maski. Jos raw-bitti on asetettu, niin siinä tapauksessa muut bitit ovat tarpeettomia. Seuraavana on leveys ja korkeus, jotka kuvastavat tiilin leveyttä ja korkeutta. Jos raw-bittiä ei ole asetettu, niin maskin bitit voivat olla seuraavanlaiset: BackgroundSpecified-bitti määrää pikseleiden tausta värin siinä tapauksessa, jos kyseinen bitti on asetettu ja BackgroundSpecified-bitin arvo määräytyy bits-per-pixel tietueesta ServerIntialisation- tai SetPixelFormat-viestissä (Richardson, T. 2010.)

## 2.4 RDS ja RDP

RDS (Remote Desktop Service), joka tunnettiin ennen nimellä Terminal Services, mahdollistaa toiminnaltaan suurtietokonejärjestelmiä vastaavan ympäristön, jossa useammalta päätteeltä muodostetaan yhteys palvelintietokoneeseen. Jokainen pääte välittää kanavan käyttäjän ja palvelintietokoneen välillä input- ja output-tapahtumia varten. Käyttäjä kirjautuu päätteelle, jonka avulla käyttäjä voi ajaa palvelintietokoneelta sovelluksia, käsitellä tiedostoja, tietokantoja ja muita resursseja. Jokainen istunto käyttäjän ja palvelintietokoneen välillä on yksilöllinen ja palvelintietokone osaa hallita tilanteet, joissa monet käyttäjät hyödyntävät samaa jaettua resurssia. (Microsoft 2010 b.)

Suurin ero RDS:n ja tavallisen suurtietokonejärjestelmän välillä on se, että suurtietokonejärjestelmissä ns. ”tyhmät päätteet” välittävät vain kirjainmerkkisiä input- ja output-tapahtumia. RDS:n avulla asiakassovellus tai emulaattori välittää käyttäjälle täydellisen graafisen käyttöliittymän, joka sisältä Windows-käyttöjärjestelmään pohjautuvan työpöydän ja tukee useita erilaisia syöttölaitteita, kuten näppäimistöä ja hiirtä. (Microsoft 2010 b.)

RDS-ympäristössä sovellukset ovat käynnissä ainostaan palvelintietokoneessa ja näin ollen mitään paikallista tiedonkäsittelyä ei tapahdu. Palvelintietokone lähettää tapahtuneesta graafista tietoa käyttöliittymän kautta käyttäjälle asiakassovellukseen. (Microsoft 2010 b.)

### Resurssit RDS-ympäristössä

RDS-ympäristössä useat käyttäjät voivat olla samanaikaisesti kirjautuneena palvelintietokoneeseen. Käyttäjät joutuvat jakamaan laitteisto- ja ohjelmistoresurssit palvelintietokoneessa. Resurssien jakamisesta voi ilmaantua seuraavia tapahtumia:

- Suoritinkäyttö. Jokaisella käyttäjällä on käytössä työpöytäympäristö, jossa käyttäjä voi ajaa minkä tahansa sovelluksen, joka on käytettävissä työpöytäympäristössä. Kuitenkin kaikki käynnissä olevat sovellukset kaikkien käyttäjien kesken käyttävät samaa suoritinresurssia palvelintietokoneesta. Jos jokin käyttäjä ajaa jotain suoritinta rasittavaa ohjelmistoa, niin tällöin ohjelmiston ajaminen mahdollisesti näkyy muilla käyttäjillä suorituskyvyn heikkenemisenä.

- Levyn käyttö. Käyttäjät joutuvat kilpailemaan sovellusten käytöstä ja niistä tiedostoista, jotka ovat riippuvaisia ajettavasta sovelluksesta. Tiedostojen lisäksi käyttäjät joutuvat kilpailemaan levyn käytöstä palvelintietokoneessa. Tämä käsittää esimerkiksi DLL-tiedostojen lataamisen ja muistin vaihdon sivutustiedoston ja fyysisen muistin välillä.

- Keskusmuisti (RAM). Jokainen palvelintietokoneessa käyttäjien kesken ajettava sovellus kuluttaa palvelintietokoneen keskusmuistia. Jos joku käyttäjä ajaa muistia rasittavaa sovellusta, niin sovelluksen ajaminen voi näkyä suoristuskyvyn heikkenemisenä muille käyttäjille.

- Verkon käyttö. Verkon käyttö on luonnollisesti tärkeää RDS-ympäristössä, koska kaikki tapahtumat käyttöliittymässä ja hiiren/näppäimistön tapahtumat kulkevat verkon läpi asiakassovelluksen ja palvelintietokoneen välillä.

- Palvelimen laitteisto. Palvelimen laitteisto, kuten cd-asemat ja leveykeasemat, ovat usein palvelinpohjaisia. Laitteistojen jako asettaa uusia haasteita niiden käyttäjien ja sovellusten välillä, jotka käyttävät näitä laitteistoja.

- Globaalit resurssit. RDS-ympäristössä käyttäjät eivät käytä yksittäisiä kopioita Windows-käyttöjärjestelmästä. Suuri osa ydinkomponenteista on kloonattu, mutta loput komponentit ovat jaettu käyttäjien kesken. Tämä tarkoittaa, että käyttäjät kilpailevat keskenään pääsystä rekisteriin, sivutustiedostoon, järjestelmäpalveluihin ja muihin globaaleihin resursseihin.

(Microsoft 2010 c.)

Monien yllämainittujen tilanteiden vaikutusta voidaan vähentää lisäämällä tarvittava määrä suoritustehoa, keskusmuistia ja levyresursseja vastaamaan käyttäjien tarpeita. Esimerkiksi palvelintietokoneeseen voidaan lisätä useampi suoritin maksimoimaan suoritintehon saatavuutta. Muistin saatavuutta voidaan maksimoida lisäämällä palvelintietokoneeseen lisää fyysistä keskusmuistia. Levynkäytön saatavuutta voidaan edelleen parantaa konfiguroimalla useampia kanavia ja jakamalla käyttöjärjestelmän ja sovellusten kuormat useammalle fyysiselle levyasemalle. (Microsoft 2010 c.)

### RDS-istunnot (Session)

Joka kerta, kun käyttäjä kirjautuu RDS-työpisteeseen, muodostetaan istunto (session). Jokaiselle muodostetulle istunnolle luodaan tunnus. Jokaisella kirjautumiskerralla asiakassovellus saa erillisen istuntotunnuksen, joten käyttäjä kokee vastaavan tilanteen, kun kirjaudutaan useammalle työpisteelle samanaikaisesti. (Microsoft 2010 d.)

Jokaiseen istuntoon liitetään vuorovaikutteinen ikkunatila (interactive window status). Ainoa kelvollinen nimi ikkunatilalle on ”WinSta0”, joten jokaisella istunnolla on oma ”WinSta0”-ikkunatilansa. Tilaan liittyy kolme erilaista työpöytää: Kirjautumisikkuna, näytönsäästäjäikkuna ja vuorovaikutteinen työpöytäikkuna. (Microsoft 2010 d.)

Käyttäjiä, joihin on liitetty vuorovaikutteinen ikkunatila, kutsutaan vuorovaikutteisiksi käyttäjiksi. Asiakassovelluksessa voi olla useita vuorovaikutteisia käyttäjiä sen käyttäjän lisäksi, joka käyttää RDS-konsolia. (Microsoft 2010 d.)

Käyttäjä kirjautuessa ulos asiakassovelluksesta poistetaan palvelintietokoneesta käyttäjään liitetty istunto ja istuntoon liitetyt ikkunatilat ja työpöydät. Kuitenkaan istuntoja ei poisteta RDS-konsoliyhteyksissä, vaikka käyttäjä kirjautuu ulos palvelusta, joten ikkunatilat säilyvät tällöin ennallaan. (Microsoft 2010 d.)

### RDS-ohjelmointirajapinta

Useimmat sovellukset toimivat RDS-ympäristössä ilman minkäänlaisia tarvittavia muutoksia ja konfigurointeja, joten sovellusten ei tarvitse käyttää RDS-API:a. RDS-API (application programming interface) on hyödyllinen asiakas- ja palvelinsovelluksille ja RDS:n ylläpitosovelluksille. (Microsoft 2010 e.)

RDS-API on kokoelma funktiokutsuja Wtsapi32.dll-tiedostoon. Wtsapi32.dll on sisälletty jokaiseen Windows-käyttöjärjestelmään alkaen Windows 2000-käyttöjärjestelmästä. Funkiot eivät toimi aiemmissa Windows-käyttöjärjestelmäympäristöissä. (Microsoft 2010 e.)

RDS-API antaa sovelluksille mahdollisuuden suorittaa seuraavanlaisia toimintoja RDS-ympäristössä:

- RDS-ylläpito, eli etäyhteyspalvelimien hallinta jossain domainissa tai istuntojen ja prosessien hallinta etäyhteyspalvelimella.
- Asiakas/palvelin-sovellusten parannettu käytettävyys RDS-ympäristössä.
- RDS-virtuaalikanavien käyttö asiakassovelluksen ja palvelinmoduuleiden välisessä sovellusten kommunikaatiossa.
- Tietyn käyttäjän tietojen ja asetusten määrittäminen ja hakeminen RDS-ympäristössä.

(Microsoft 2010 e.)

Virtuaalikanavat

Virtuaalikanavat (Virtual Channels) ovat sovellusten laajennuksia, joita voidaan käyttää toimintojen lisäämiseen ja parantamiseen RDS-ympäristön olemassa oleviin sovelluksiin. Esimerkkejä tästä on tuki tietylle erikoislaitteistolle, äänelle tai muita lisäyksiä RDS:n RDP-protokollan toimintoihin. RDP-protokolla itsessään mahdollistaa monipuolisen hallinnan useille virtuaalikanaville saman aikaisesti. (Microsoft 2010 f.)

Virtuaalikanavasovelluksessa on kaksi osaa: asiakasmoduuli ja palvelinmoduuli. Palvelinmoduuli on käyttösovellus, jota suoritetaan palvelintietokoneella. Asiakasmoduuli on DLL-tiedosto, joka ladataan muistiin työpisteellä aina, kun asiakassovellukseen kirjaudutaan. (Microsoft 2010 f.)

Virtuaalikanavat voivat lisätä parannuksia asiakassovelluksiin olematta riippuvaisia RDP-protokollasta. Virtuaalikanavatuella voidaan lisätä uusia ominaisuuksia ilman päivitysten ajamista asiakas- tai palvelinsovelluksiin tai RDP-protokollaan. (Microsoft 2010 f.)

Virtuaalikanavilla on neljä pääkäyttäjää:

- Pääkäyttöiset ydinajurit, kuten tulostinajurit.
- Tiedostojärjestelmän uudelleenohjaus (Tämä on itse asiassa vain erikoistapaus ydinajureista).
- Käyttäjätilasovellukset, kuten leikkaa/liitä-toiminnot etäyhteytenä.

- Äänilaitteisto.

(Microsoft 2010 f.)

RDP

RDP (Remote Desktop Protocol) on Microsoftin kehittämä protokolla etäyhteyksien luomiseen Windows-käyttöjärjestelmissä. Se perustuu ITU-T T.128 protokollaan, joka on luokitukseltaan sovellusjakoprotokolla (Application share Protocol). RDP on monikanavainen protokolla, joka pystyy tuottamaan virtuaalisia kanavia. Virtuaalisten kanavien kautta voidaan kuljettaa laitteistojen kommunikaatiota ja esitysdataa, sekä mahdollistaa koodatut tiedot näppäimistöstä ja hiirestä. (Microsoft 2010 a.)

Palvelinpuolella RDP käyttää omaa näyttöajuria, jonka avulla RDP muodostaa näyttötiedosta paketteja verkkoon ja lähettää ne verkon kautta asiakassovellukseen. Asiakassovellus ottaa paketit vastaan ja tulkitsee verkkodatan sopivaksi ”Microsoft Win32 GDI API”-kutsuiksi. Näppäimistön ja hiiren syötteet ohjataan takaisin Asiakassovellukselta palvelimelle. Palvelimessa RPD käyttää sen omaa ”on-screen”-näppäimistöä ja hiiriajuria, joilla käsitellään syötteet. (Microsoft 2010 a.)

Remote Desktop -istunnossa kaikki ympäristömuuttujat, jotka esimerkiksi vaikuttavat näytön värien syvyyteen ja taustakuvan käyttöön, määräytyvät rcp-tcp yhteyden asetuksissa. Asetukset koskevat kaikkia niitä funktioita ja kutsuja, jotka asettavat ympäristömuuttujia Remote Desktop ActiveX Control Interface ja Remote Desktop Services WMI Provider –luokissa. (Microsoft 2010 a.)

RDP-protokollalla on seuraavanlaisia ominaisuuksia ja toimintoja:

- Kryptaus
- Kaistanleveyden hallinta
- Roaming yhteydenkatkaisu
- Leikepöydän kontrollointi
- Tulostuksenohjaus

- Virtuaalikanavat
- Etäohjaus

(Microsoft 2010 a.)

RDP käyttää kryptaamiseen RSA Securityn RC4 salakirjoitusjärjestelmää, joka on kehitetty pienen tietomäärän tehokkaaseen kryptaamiseen. Se on myös kehitetty verkon turvallisiin yhteyksiin. Windows 2000 -käyttöjärjestelmästä asti on voitu käyttää joko 56-bittistä tai 128-bittistä salausavainta kryptaamiseen. (Microsoft 2010 a.)

RDP tukee erilaisia menetelmiä, joilla kaistanleveyden käyttöä voidaan hallita vähentämällä siirrettävää dataa verkkoyhteyksissä. Näitä menetelmiä ovat pakkaus, bittikartan tallentaminen välimuistiin ja pirstaleiden (fragments) ja symbolien tallentaminen keskusmuistin kautta välimuistiin. Jatkuva bittikartan tallentaminen välimuistiin voi aiheuttaa huomattavan parannuksen suorituskyvyssä hitailla yhteyksillä varsinkin, jos käytetään ohjelmistoja, joissa käsitellään suurikokoisia bittikarttoja. (Microsoft 2010 a.)

Roamingilla RDP:ssä tarkoitetaan, että käyttäjä voi katkaista etäyhteyden kirjautumatta siitä ulos. Käyttäjä kirjataan automaattisesti aikaisempaan istuntoon, kun käyttäjä kirjautuu järjestelmään seuraavan kerran samalta tai eri laitteelta. Jos käyttäjän istunto sammuu verkko- tai palvelinohjelmavian takia, niin käyttäjän yhteys katkeaa, mutta uloskirjautumista ei tapahdu. (Microsoft 2010 a.)

RDP osaa leikepöydän käytön niin, että käyttäjät voivat poistaa, kopioida ja liittää tekstiä ja grafiikkaa paikallisten sovellusten ja etäyhteydessä olevien sovellusten välillä. Samaa menetelmää voi käyttää myös eri istuntojen välillä. (Microsoft 2010 a.)

Tulostuksen ohjaaminen RDP:ssä toimii siten, että käyttäjä voi tulostaa paikalliseen tulostimeen etäyhteydestä. Sama onnistuu myös toisinpäin, eli voidaan tulostaa sellaiseen tulostimeen, joka on yhdistetty käytettävään etähallintatietokoneeseen. (Microsoft 2010 a.)

RDP:ssä virtuaalikanavia ja niiden rakennetta voidaan käyttää olemassa olevien sovellusten kehittämiseen. Kehittämisellä voidaan lisätä uusia ominaisuuksia ja keinoja sovelluksiin, jotka tarvitsevat yhteyttä palvelimen ja asiakassovelluksen välillä. Samaa keinoa voidaan käyttää myös kokonaan uusien sovellusten kehittämiseen. (Microsoft 2010 a.)

RDP:n etäohjauksella voidaan katsoa ja ohjata jotain tiettyä etäyhteysistuntoa. Tämä mahdollistaa sen, että tukihenkilöt voivat etänä määrittää ja korjata etäyhteysistuntoa vaivaavat ongelmat ja viat. (Microsoft 2010 a.)

Ylläolevien ominaisuuksien lisäksi RDP tukee myös seuraavia lisäominaisuuksia:

- Tuki 24-bittiselle värille.
- Parannettu suorituskyky hitailla puhelinverkkoyhteyksillä vähennetyn kaistanleveyden ansiosta.
- Älykorttivarmennus.
- Kyky ohjata erilaisia Windowsin näppäinyhdistelmiä kokoruudussa etätietokoneeseen tai äänien, asemien, porttien ja tulostimen ohjaukset etätietokoneeseen.

(Microsoft 2010 a.)

## 2.5 X11

X11 on UNIX-käyttöjärjestelmille kehitetty protokolla, joka mahdollistaa graafisen etäyhteyden sovelluksiin. Alkuperäinen X-ikkunointijärjestelmä kehitettiin vuonna 1984 MIT:n toimesta. (ToastyTech 2010.)

X-ikkunointijärjestelmää käyttävä laite voi käyttää sovelluksia etähallittavalta laitteelta. Kaikki suorittimen prosessit tapahtuvat etätietokoneessa, mutta käytettävän sovelluksen tiedot näkyvät paikallisen tietokoneen näytöllä. (ToastyTech 2010.)

Vaikka X-päätteet eivät yleistyneet laajoille markkinoille, X-ikkunointijärjestelmä oli kuitenkin standardi graafisten sovellusten paikalliseen ja etäkäyttöön UNIX- ja Linux-käyttöjärjestelmissä. Järjestelmät käyttävät X11-protokollaa graafisen tiedon piirtämiseen paikallisen tietokoneen näytölle. Paikallista näyttöä käsiteltiin etänäyttönä, vaikka näyttö oli käynnissä samalla tietokoneella. (ToastyTech 2010.)

X-ikkunointijärjestelmän sovelluksia voidaan suorittaa etäyhteyden kautta, mutta käyttäjät eivät sitä yleensä tee. Tätä toimintoa usein rajoitetaan turvasyiden takia. X-

ikkunointijärjestelmän rakenteen vuoksi joku ulkopuolinen käyttäjä voisi käynnistää sovelluksen, joka näkyisi omalla näytöllä. (ToastyTech 2010.)

NX

NX on NoMachinen valikoima teknologioita ja työkaluja. Teknologiat ja työkalut ovat suunniteltu verkkotyöskentelyn helpottamiseen. NX pohjautuu X-ikkunointijärjestelmään ja se sisältää palvelinkomponentin, jolla voidaan muuttaa UNIX-pohjainen tietokone palvelintietokoneeksi. Asiakassovelluksia löytyy useille eri käyttöjärjestelmille ja laitteistoille. NX käyttää etäyhteyksissä SSH-salausmenetelmää. (Medialogic 2010.)

NX:n päätavoite on parantaa X:n pakkausmenetelmää, jotta käyttäjät voisivat käyttää mitä tahansa X-työpyötäsovellusta standardeissa X-palvelimissa. NoMachine on kehittänyt oman X-pakkausmenetelmän ja sisällyttänyt siihen välitysagentit, jotka mahdollistavat etäyhteyksien käyttämisen jopa vanhoilla modeemiyhteyksillä. (Medialogic 2010.)

NX:n pakkausmenetelmä toimii kolmessa tasossa X-protokollassa:

- Verkon liikennettä pakataan monilla keinoilla, kuten differentiaalialgoritmeilla, erilaisilla välimuistimenetelmillä ja häviättömällä kuvanpakkauksella.
- Parantaa läpisyöttöä vähentämällä ”round-tripia” verkossa lähes nollaan.
- Sovittaa verkon kaistanleveyttä tarpeen mukaan.

(Medialogic 2010.)

Pakkausmenetelmän suhde on 10:1 ja 100:1 välillä ja enemmänkin riippuen siitä mitä sovellusta käytetään. Tämä on saavutettu heikentämättä verkon suorituskykyä ja etäyhteydet voidaan muodostaa sellaisilla nopeuksilla, jotka ovat verrattavissa paikallisen tietokoneen käyttöön. (Medialogic 2010.)

NX:n käyttö ei rajoitu pelkästään Linux- ja UNIX-käyttöjärjestelmille. NX osaa kapseloida X-protokollaan RDP-protokollan ja VNC-protokollan, joten NX:a voidaan käyttää usealla eri käyttöjärjestelmällä. (Medialogic 2010.)

## 2.6 Citrix ICA

ICA on Citrix:n kehittämä protokolla, jota käytetään pääasiassa työpyötävirtualisointiin useiden käyttöjärjestelmien välillä. Tunnetuimmat ICA-protokollaa käyttävät Citrix:n tuotteet ovat WinFrame ja XenApp, joka tunnettiin ennen nimellä MetaFrame. XenApp:n ja WinFrame:n päätarkoitus on mahdollistaa Microsoft Windows -palvelimilta windows-sovellusten käyttö niille käyttäjille, jotka käyttävät eri käyttöjärjestelmiä, kuten Linux, UNIX ja MacOS (BreakingPoint 2010.)

ICA-protokolla käyttää portteja 1494 ja 2598 käsittelemään asiakassovelluksen ja palvelimen välistä tiedonsiirtoa. Tiedonsiirto asiakassovellukselta palvelimelle sisältää hiiren liikkumisen ja muut tapahtumat ja pyynnöt. Tiedonsiirto palvelimelta asiakassovellukselle sisältää koko ruudun sijasta korkealaatuisen kuvan. Menetelmä säästää näin kaistaa ja vähentää verkkokuormitusta. ICA:n avulla laitteistot, kuten thin clientit, voivat käyttää keskitetyiltä palvelimilta sovelluksia, joita laitteiston käyttöjärjestelmä ei välttämättä tue normaalisti. (BreakingPoint 2010.)

## 2.7 PcoIP

PcoIP-protokolla on Teracidi:n kehittämä protokolla etätyöpöytien käyttöön. PcoIP mahdollistaa lähiverkossa tai WAN:ssa (Wide Area Network) keskitetyn työasemien hallinnan tietokeskuksesta käsin. Keskitetty hallinta mahdollistaa tuen korkeille resoluutioille, 3D-grafiikalle ja HD-medialle, USB-laitteiden täydellisellä yhteensopivuudella. (TeraDici 2010 a.)

PcoIP on näyttöprotokolla, joka mahdollistaa kaikkien IT-resurssien yhdistämisen tietokeskukseen. Keskitys poistaa tarpeet tavallisille työpöytätietokoneille ja mahdollistaa yhteydet useampiin työpöytiin ilman riskejä. (TeraDici 2010 a.)

PcoIP-teknologiaa on saatavissa laitteisto- ja ohjelmistopohjaisina. PcoIP-laitteita on saatavilla laaja valikoima eri kolmannen osapuolen tuottajilta. Näihin laitteisiin kuuluu muun muassa integroidut näytöt, työpyötäportaalit ja palvelinliitännäiset. (TeraDici 2010 a.)

### 2.7.1 Näytönprosessointi

PcoIP:n ydinosa on TERA Image Engine, joka tuottaa näytön tietojen pakkauksen IP-verkkojen kautta. Kyky prosessoida näytön tietoa pikselitarkkuudella mahdollistaa PcoIP:n riippumattomuuden suorittimen ja grafiikkakiihdytyksen suorituskyvystä. PcoIP:tä voidaan käyttää piirisarjoilla integroiduissa näyttölaitteissa tai työasemien näytönohjainten piirisarjojen kanssa. (TeraDici 2010 b.)

Ulkoisen näytönprosessoinnin avulla järjestelmä on riippumaton käytettävistä sovelluksista ja käyttöjärjestelmistä. Järjestelmäylläpitäjät voivat helposti integroida PcoIP:n olemassa olevaan järjestelmään. Integrointi mahdollistaa työasemien keskityksen yhteiseen tietokeskukseen. (TeraDici 2010 b.)

### 2.7.2 Verkkotyöskentely

PcoIP käyttää vähälatenssisia algoritmeja näytön tiedon näyttämiseen IP-verkkojen kautta tavallisissa lähiverkoissa tai WAN:ssa. Nämä algoritmit mukautuvat dynaamisesti verkon ruuhkautumisen aikana estäen käyttäjien kokemia katkoksia palvelussa. (TeraDici 2010 c.)

Yritykset voivat käyttää PcoIP:tä yhdistääkseen yksilölliset työasemat ja kerätäkseen kaikki yrityksen käyttämät sovellukset ja tietokannat yhteiseen keskitettyyn pisteeseen. Keskitetty menetelmä turvaa viruksilta ja tietomurroilta sekä parantaa toimintavarmuutta.. (TeraDici 2010 c.)

### 2.7.3 Turvallisuus

PcoIP:ssä tiedot pysyvät aina tietokeskuksessa ja ainoastaan pikselidata tiedoista välitetään käyttäjille. Käyttäjät voivat käsitellä tietoa, mutta eivät voi omistaa eikä kopioda kyseistä tietoa tietokeskuksesta. Yritykset voivat vähentää vaaratekijöitä ja parantaa immateriaaliomaisuuden ja arvokkaan tiedon kontrollointia. (TeraDici 2010 d).

### 2.7.4 WAN-tuki

Vähäviiveisten kuvanpakkausalgoritmien ja laitekohtaisten WAN-firmwarepäivitysten avulla voidaan parantaa käyttettävyyttä WAN-verkoissa. WAN-parannukset lisäävät huomattavasti käytettävyyttä multimedian, 3D-grafiikan ja äänten parannetulla tuella (TeraDici 2010 e.)

WAN-ominaisuuksia:

- Vähennetty minimikaistanleveys. PcoIP:n minimikaistanleveys WAN-yhteyksille on 1 Mbit/s, koska WAN-yhteydet eivät normaalisti käytä korkeita kaistanleveyksiä. Käytettävä kaistanleveys voi olla pienempi, koska PcoIP ei lähetä muuta kuin näytön tietojen muutokset.

- Paikallinen näppäimistö ja hiiri. Korkeaviiveisissä verkoissa voidaan hiiren osoitin näyttää paikallisella työpöydällä sen lisäksi, että osoittimen tapahtumat lähetetään palvelintietokoneelle. Paikallisella näppäimistöllä estetään näppäinten painalluksien häviämiset verkon viiveiden vuoksi.

- Pakettien järjestely. WAN-yhteyksille tyypilliset järjestymättömät paketit voidaan ketjuttaa PcoIP:n avulla. Järjestymättömät paketit voivat aiheuttaa verkossa viiveitä, jos järjestelymenetelmää ei käytetä.

- Äänten pakkaus kaistanleveyden mukaan. PcoIP lähettää ääntä joko pakattuna tai pakkaamattomana riippuen käytettävissä olevasta kaistanleveydestä.

(TeraDici 2010 e.)

## 2.8 Muut protokollat

Erilaisia etäyhteysprotokollia käsiteltyjen protokollien lisäksi on esimerkiksi MacOS-käyttöjärjestelmille tarkoitettu Apple Remote Desktop (ARD). Se on Applen mukaan paras keino hallita MAC-tietokoneita verkon kautta. ARD:n kautta on helppoa asentaa suoraan halutut Applen ja kolmannen osapuolen sovellukset kerralla kaikille verkon asiakastietokoneille. Sen lisäksi ARD:ssä on sisäänrakennettuna Task Server, joka voidaan ajastaa asentamaan automaattisesti verkon kautta sovelluksia asiakastietokoneille. (Apple Inc. 2010.)

ARD 3:ssa on mukana 40 automaatiotoimintaa, joita voidaan käyttää hallintatehtävien automaatioimiseen. Toimintoja ovat esimerkiksi taustakuvan asettaminen, energiansäästöasetukset ja aikavyöhykkeen asettaminen. (Apple Inc. 2010.)

ARD:n kautta voidaan antaa vaivattomasti etätukea käyttäjille näytön jaon avulla. ”Curtain Moden” avulla voidaan estää paikallista käyttäjää näkemästä mitä ruudulla tapahtuu. Tämä on hyödyllistä silloin, kun halutaan tehdä toimenpiteitä etänä olevaan julkiseen näyttöön. Järjestelmänvalvojat voivat myös Remote Desktop -työkalun avulla tarkastella verkossa olevaa tietokonetta ja mahdollisesti ottaa etänä tietokone hallintaan. (Apple Inc. 2010.)

Appliance Link Protocol (ALP) on Oraclen kehittämä etäyhteysprotokolla Sun Ray -thin clienteihin. ALP on osana ”Sun Ray Sofware” ohjelmistoa, joka on eräänlainen käyttöjärjestelmä Sun Ray -thin clienteissa. Teknisiä tietoja ALP:n ja Sun Ray Softwaren toiminnasta ei ole helposti saatavilla suljetun lähdekoodin vuoksi. On kuitenkin olemassa avoimeen lähdekoodiin perustuva SoftRay, joka on toteutettu Javalla. (Cooper S. 2010.)

ALP:ssä on kolme osaa, jotka ovat Appliance Link Session Protocol (ALSP), Appliance Link Render Protocol (ALRP) grafiikkaan ja ääneen sekä Appliance Link Device Protocol (ALDP). Sun Rayn thin clientit ovat nimeltään ”ultra thin client”, koska ne eivät sisällä muuta, kuin tarvittavat ohjelmistot verkkotoimintoihin. (Cooper S. 2010.)

## 2.9 Suosituimpia etäyhteyssovelluksia

Etäyhteyksien suosion kasvaessa on kehitetty useita etäyhteyssovelluksia vastaamaan käyttäjien asettamia tarpeita. Seuraavana esitellään taulukko 1 käytetyimmistä ilmaisista etäyhteysohjelmistoista. (Wareprise 2010.)

**Taulukko 1: Etäyhteysohjelmistojen vertailu**

| **Ohjelmisto** | **Windows-tuki** | **Linux-tuki** | **MacOS-tuki** | **Yhteyden salaus** | **Tiedostonsiirto** |
|---|---|---|---|---|---|
| Crossloop | Kyllä | Ei | Kyllä | Kyllä | Kyllä |

| | | | | | |
|---|---|---|---|---|---|
| SkyFex | Kyllä | Ei | Ei | Kyllä | Kaupallisessa versiossa |
| YuuGuu | Kyllä | Kyllä | Kyllä | Kyllä | Kyllä |
| LogMeIn Free | Kyllä | Ei | Kyllä | Kyllä | Ei |
| UltraVNC | Kyllä | Ei | Ei | Liitännäisellä | Kyllä |
| TeamViewer | Kyllä | Kyllä | Kyllä | Kyllä | Kyllä |
| Desktop Share | Kyllä | Ei tiedossa | Ei tiedossa | Ei tiedossa | Ei tiedossa |
| NX Free | Asiakassovellus | Kyllä | Asiakassovellus | Kyllä | Ei tiedossa |
| TightVNC | Kyllä | Kyllä | Asiakassovellus | Ainoastaan UNIX | Kyllä |
| Royal TS | Kyllä | Ei | Ei | Kyllä | Kyllä |

# 3 KEVYET ASIAKASPÄÄTTEET

Kevyt asiakaspääte (thin client) on tietokonejärjestelmä, jota käytetään sovellusten ajamiseen tilanteissa, missä sovellusten suoritus tapahtuu verkon kautta yhteydessä olevalla etäpalvelimella. Paikallista tietokonetta, eli asiakaspäätettä, käytetään ainoastaan tapahtumien näyttämiseen niillä tavoin, mitkä muistuttavat sovelluksen suorittamista paikalliselta tietokoneelta. (Yegulalp, S 2010.)

Kevyet asiakaspäätteet itsessään eivät ole uusi asia. Ne ovat yksi nykyaikaisen tiedonkäsittelyn perusasioita. Kevyet asiakaspäätteet tunnetaan paremmin nimellä ”tyhmät päätteet”. Kyseiset laitteistot koostuivat kuvaputkinäytöstä, joka oli koaksiaalikaapelin avulla kytketty haluttuun tietokoneeseen. Päätteellä itsellään ei usein ollut muita toimintoja, kuin tulostukset ja tekstinsyöttö. (Yegulalp, S 2010.)

## 3.1 Sovelluksia kevyille asiakaspäätteille

Teoriassa mikä tahansa sovellus voidaan ajaa asiakaspäätteen kautta, mutta käytännössä sovellus voi vaatia asiakaspäätteeltä ominaisuuksia, joita sillä ei ole. Tämä tarkoittaa sitä, että suoritetusta sovelluksesta ei välttämättä saa kaikkia toimintoja käytettyä. (Yegulalp, S 2010.)

Kevyissä asiakaspäätteissä sovellusten käyttömahdollisuudet ovat riippuvaisia monista eri tekijöistä. Itse asiakaspäätteestä, verkon kaistanleveydestä, mitä ominaisuuksia käytettävä etäyhteysprotokolla tukee, onko laitteiston kiihdytystä olemassa erilaisille toiminnoilla ja niin edelleen. (Yegulalp, S 2010.)

Eri kevyet asiakaspäätteet tukevat erilaisia kuormituksia ja työmäärää. Erimerkiksi VNC-protokolla ei tällä hetkellä suoraan tue videon suoratoistoa. On mahdollista kuitenkin käyttää videontoistosovellusta työpöydällä, jonne on otettu yhteys käyttäen VNC-protokollaa. Kuvantoistonopeus olisi vain noin 1-2 kuvaa sekunnissa riippumatta siitä, miten nopea verkkoyhteys on käytettävissä. (Yegulalp, S 2010.)

## 3.2 Tyypillisiä käyttökohteita

Eri kevyet asiakaspäätteet soveltuvat parhaiten tiettyihin käyttötarkoituksiin, joita ovat seuraavat:

- Korkeille turvaluokituksille tai yleisiin käyttöympäristöihin soveltuvat asiakaspäätteet.
- Pieniin työmäärin soveltuvat asiakaspäätteet.
- Suoritustehoa vaativiin sovelluksiin soveltuvat asiakaspäätteet.

(Yegulalp, S 2010.)

Paikat, joissa turvallisuus on avainasemassa, hyötyvät asiakaspäätejärjestelmästä. Tieto pidetään tallessa palvelintietokoneella ja asiakaspääte näyttää vain ne tiedot, mihin käyttäjällä on mahdollisuus päästä käsiksi. Yritykset tietojen etsimiseen asiakaspäätteeltä johtavat yleensä rikkoutuneeseen laitteeseen varastetun tiedon sijasta. (Yegulalp, S 2010.)

Kevyet asiakaspäätteet ovat myös hyvin soveltuvia julkisille paikoille, kuten kirjastoihin ja nettikahviloihin. Kirjastoissa ja nettikahviloissa monet ihmiset käyttävät samaa konetta ja on tarpeellista estää henkilökohtaisten tietojen jääminen tietokoneeseen. Riskiä ei voi kokonaan poistaa, mutta riskin mahdollisuus pienenee, koska pääte itsessään käsittelee hyvin vähän tietoa. (Yegulalp, S 2010.)

Kevyet asiakaspäätteet soveltuvat hyvin sellaisiin työmääriin, joissa suoritettavat prosessit eivät ole suoritinriippuvaisia ja käyttäjälle riittää vain normaalin Internet-selaimen verran tietoa. Itse asiassa monet asiakaspäätteet voivat olla Internet-selaimia, koska asiakaspäätteet sisältävät tarpeen vaatiessa tarvittavat työkalut käyttäjille. (Yegulalp, S 2010.)

Vanhat tietokoneet voidaan ottaa uusiokäyttöön muuttamalla ne asiakaspäätteiksi. Sovellukset, jotka itsessään eivät toimisi kovin hyvin vanhalla tietokoneella, voidaan näyttää palvelimelta tietokoneelle asiakaspääteyhteyden avulla, jos sovelluksen toiminta ei heikkene tällä menetelmällä. (Yegulalp, S 2010.)

## 3.3 Kevyt asiakaspäätetyypit

Kevyet asiakaspäätteet voidaan jakaa pääsääntöisesti kahteen ryhmään. Nämä ryhmät ovat laitteistopohjainen asiakaspääte ja ohjelmistopohjainen asiakaspääte. (Yegulalp, S 2010.)

### 3.3.1 Laitteistopohjainen kevyt asiakaspääte

Laitteistopohjainen asiakaspääte on laite, joka on luotu pelkästään asiakaspäätesovelluksen suorittamiseen. Tätä voidaan verrata vanhan aikaiseen ”tyhmään päätteeseen”, mutta siinä on kuitenkin joitakin eroavaisuuksia paremman grafiikan näyttämisen lisäksi. (Yegulalp, S 2010.)

Esimerkiksi laitteisto itsessään vaihtelee asiakaspäätemalleissa. Se voi olla vanha tietokone, josta on riisuttu asiakaspäätesovellusten suorittamiseen tarpeettomia ominaisuuksia ja laitteita. Se voi myös olla täysin tilaustyönä tehty laite ottamaan pelkästään etäyhteys palvelimeen ja suorittamaan tarpeelliset näyttötoiminnot. Eräs esimerkkilaitteisto on nimeltään nComputing. NComputing on laitteisto, joka tukee monia käyttäjiä työpöytäympäristössä. (Yegulalp, S 2010.)

Muita laitteistopohjaisten asiakaspäätteiden valmistajia ovat Wyse, Leadtek ja Oracle/Sun. Asiakaspäätteiden ominaisuudet vaihtelevat riippuen laitteiston valmistajasta. (Yegulalp, S 2010.)

Wyse on toiminut päätevalmistajana, mutta on nykyään siirtynyt kevyihin asiakaspäätteisiin. Wysen asiakaspäätteet käyttävät etäyhteyksiin ICA, RDP ja Vmware View -protokollia, mutta myös Wysen omaa flash-pohjaista liitännäistä multimedian näyttämiseen ja useamman näytön tukemiseen samanaikaisesti. Wysen asiakaspäätteisiin on olemassa valikoima eri käyttöjärjestelmiä riippuen siitä, mitä mallia asiakaspäätteestä ollaan käyttämässä. Näitä ovat Linux, Windows Xpe, Windows CE, Citrix XenDesktop ja Wysen oma ThinOS -käyttöjärjestelmä. Wyse ei ole julkaissut ThinOS:n API:a, joten ThinOS on vapaa haittaohjelmista. (Yegulalp, S 2010.)

Leadtek on tunnettu valmistaja näytönohjainten markkinoilla, mutta he valmistavat myös Virtual System Desktop -nimellä kulkevia kevyitä asiakaspäätteitä, jotka käyttävät etäyhteyksiin Teradici:n PcoIP-protokollaa. Leadtekin VP 200H on lisälaite, joka muuttaa tietokoneen helposti PcoIP-asiakaspäätteeksi, kun taas VP 200P on itsessään hyvin vähäisellä virrankulutuksella varustettu asiakaspääte. (Yegulalp, S 2010.)

Oraclen/Sunin asiakaspäätteistä löytyy Sun Ray, joka on suunniteltu toimimaan paikallisessa verkossa ja WAN:in kautta ja hyödyntämään erilaisia asetusmalleja. Sun Ray tukee etäpalvelimena Windowsia, Linuxia tai Solarista. (Yegulalp, S 2010.)

### 3.3.2 Ohjelmistopohjainen kevyt asiakaspääte

Ohjelmistopohjainen asiakaspääte on jokin ohjelmisto, jota suoritetaan niiltä isäntäkoneilta, joilta ohjelmistoa on tarpeellista suorittaa. Ohjelmisto voi etäyhteyden käyttöliittymää parantaakseen hyödyntää paikallisen koneen joitakin ominaisuuksia, kuten esimerkiksi grafiikkakiihdytystä. (Yegulalp, S 2010.)

Isäntäkoneen ei tarvitse kuitenkaan olla järjestelmä, joka on suunniteltu vain pelkästään etäyhteyttä varten. Se voi olla tavallinen kotitietokone, jossa suoritetaan asiakaspääteohjelmistoa muiden suoritettavien sovellusten rinnalla. (Yegulalp, S 2010.)

Ohjelmistopohjaisia asiakaspäätteitä ovat itsessään etäyhteyksien protokollat, kuten X11, RDP, ICA, VNC, ALP ja PcoIP. On myös järjestelmäprotokolla nimeltä SPICE, joka pystyy kommunikoimaan virtuaalikoneessa olevaan virtuaalilaitteistoon käyttäen asiakaspäätteitä ja muita laitteita. Tuet kuvalle, äänelle ja paikalliselle laitteistokiihdytykselle on rakennettu suoraan protokollaan. SPICE:a kehittää Red Hat, joka on ostanut SPICE:n alkuperällisiltä kehittäjiltä ja on muuttanut sen avoimeen lähdekoodiin GPLv2-lisenssillä. (Yegulalp, S 2010.)

Eräs yleisimmistä ohjelmistopohjaisista asiakaspäätteistä voi olla verkkoselain. Esimerkiksi Googlen Chrome OS on yksi esimerkki tällaisesta verkkoselain asiakaspäätteestä, jossa asiakassovelluksella on tarpeeksi toimintoja suorittamaan selain ja tarvittavat huoltotoiminnot, kuten esimerkiksi paikallinen välimuisti tyhjentäminen. (Yegulalp, S 2010.)

### 3.3.3 Rajoitukset

Suurin rajoitus kevyissä asiakaspäätteissä on riippuvuus verkkoyhteydestä. Verkon toimimattomuudella on huomattavia vaikutuksia asiakaspäätteiden toiminnassa, koska kaikki asiakaspäätteen toiminta kulkee verkkoyhteyden kautta. Jos verkkoyhteys hidastelee tai jopa katkeaa kokonaan, niin asiakaspäätteessä voi ilmetä viivettä tai asiakaspääte lopettaa kokonaan toimimasta. (Yegulalp, S 2010.)

Asiakaspäätejärjestelmän tarkalla suunnittelulla voidaan vähentää ongelmia hitaiden verkkoyhteyksien kanssa. Esimerkiksi Internet-selain voi kirjoittaa kaiken lataamansa tiedon välimuistiin. Välimuistin koko kuitenkin voi vaihdella paikallisen koneen laitteistosta riippuen. (Yegulalp, S 2010.)

Kuitenkin asiakaspäätteiden riippuvuus verkkoyhteydestä on aina olemassa. Verkkoyhteyksien hitaus voi monesti olla hitaiden komponenttien syytä jopa suorituskyvykkäimmissä kotitietokoneissa, joiden hintaluokat voivat olla samalla tasolla asiakaspäätelaitteistojen kanssa. (Yegulalp, S 2010.)

# 4 TUTKIMUSELEMENTIN ESITTELY

Opinnäytetyön tutkimusosassa tutkitaan kolmea eri etäyhteysohjelmistoa, jotka käyttävät VNC- ja RDP-protokollia. Tutkittaviin ohjelmistoihin kuuluu seuraavat: TightVNC, UltraVNC ja Remote Desktop Connection. Kyseisiin ohjelmistoihin on päädytty sen vuoksi, koska ne ovat ilmaisia ja helposti saatavilla (Remote Desktop Connection löytyy jokaisesta Windowsista alkaen Windows XP Pro -versiosta ja siitä löytyy täydellinen dokumentointi Microsoftin sivuilta).

Käyttöjärjestelmäympäristö, jossa ohjelmistoja on tarkoitus käyttää, on Windows 7 Professional 32bit:n englanninkielinen versio niin palvelimen kuin käyttäjän tietokoneessa. Molemmat tietokoneet sijaitsevat lähiverkossa, joten tulokset voivat vaihdella tapaukseen, jossa toinen tietokoneista sijaitsee verkon ulkopuolella. Tietokoneen kokoonpano käsittää kaksiytimisen prosessorin 2,6GHz kellotaajuudella ja prosessorin lisäksi 2GB keskusmuistilla.

Tutkimuksen tarkoituksena on kartoittaa ohjelmistojen ominaisuudet, kuten tietoturvaominaisuudet ja yhteysmahdollisuudet, sekä mitata erilaiset rasitukset mitä tutkittava etäyhteysohjelmisto aiheuttaa käytettävässä tietokoneessa ja verkossa. Rasituksiin luetaan verkkoliikenteen määrä tavuissa, suorittimen kuormitus prosentteina ja muistinkäyttö megatavuina.

Verkkoliikenteen mittaamiseen käytetään Windows Task Managerin  Resource monitoria. Suorituskyvyn ja muistin käytöt tarkistetaan Windowsin Task Managerin ja Resource monitorin avulla. Task Manager ja Resource Monitor löytyy Windows 7:sta painamalla CTRL+ALT+DEL ja klikkaamalla ”start task manager”.

Tutkimuksen etenee seuraavasti:

1. Asennus
2. Yhteyden muodostus ja ominaisuuksien merkitseminen
3. Verkkoliikenteen seuraaminen ja resurssitarpeen analysointi

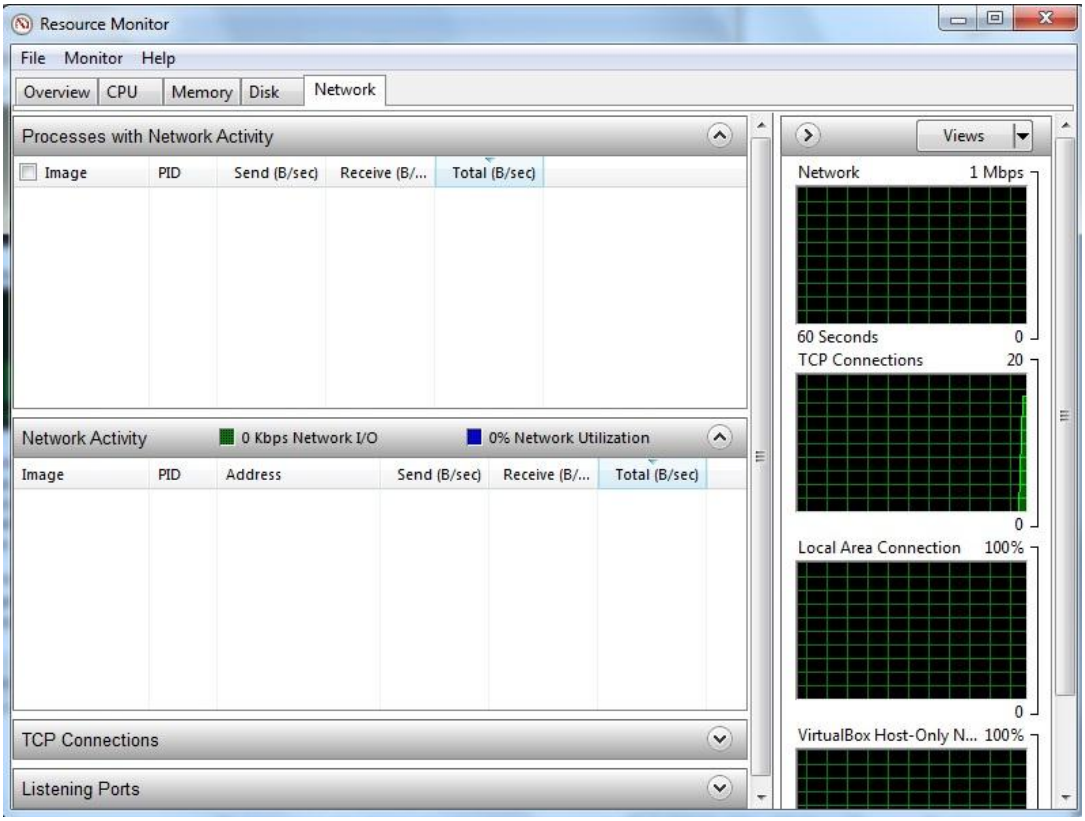
Asennusvaihe käsittää ohjelmistojen asennuksen ja sen mitä ohjelmiston mukana tulee tietokoneelle. Yhteydenmuodostusvaiheessa muodostetaan yhteys etätietokoneelle ja samalla tarkastellaan minkälaisia tietoturvaominaisuuksia etäyhteysohjelmistossa on. Verkkoliikennevaiheessa tarkkaillaan verkkoliikennettä Resource monitorin avulla, eli merkitään ylös kuinka paljon etäyhteysohjelmisto kuormittaa verkkoa yhteyden aikana. Samassa vaiheessa merkitään ylös Task Manageristä ja Resource monitorista, kuinka paljon etäyhteysohjelmisto käyttää suoritinta ja keskusmuistia.

Tutkimuksen tavoitteena on luoda selkeä kuvio ohjelmistojen kuluttamista resursseista, joita käyttötietokoneelta kuluu etäyhteysohjelmiston ylläpitämiseen. Kuvio ilmaistaan selkeänä taulukkona, josta kaikki tutkitut osat ovat hyvin selvillä.

# 5 ETÄYHTEYKSIEN TUTKIMINEN

Tutkimusprosessi käynnistyy asennusvaiheella, joka käsittää ohjelmistojen asennukset ja mitä valintoja asennuksessa on otettava huomioon tutkimustuloksia varten. Kun ohjelmistot on asennettu, niin muodostetaan yhteys etätietokoneeseen ensiksi TightVNC:llä, jonka jälkeen UltraVNC:llä ja lopuksi Remote Desktop Connectionin avulla. Jokaisen yhteyden muodostuksen aikana kirjataan ylös eri tietoturvavaihtoehdot, joita etäyhteysohjelmistolla on käytettävissä. Näitä verrataan tavalliseen VNC-protokollalla muodostettuun yhteyteen, jossa tietoturva käsittää perusautentikoinnin käyttäjätunnuksen ja salasanan avulla, mutta yhteys ei muuten ole suojattu.

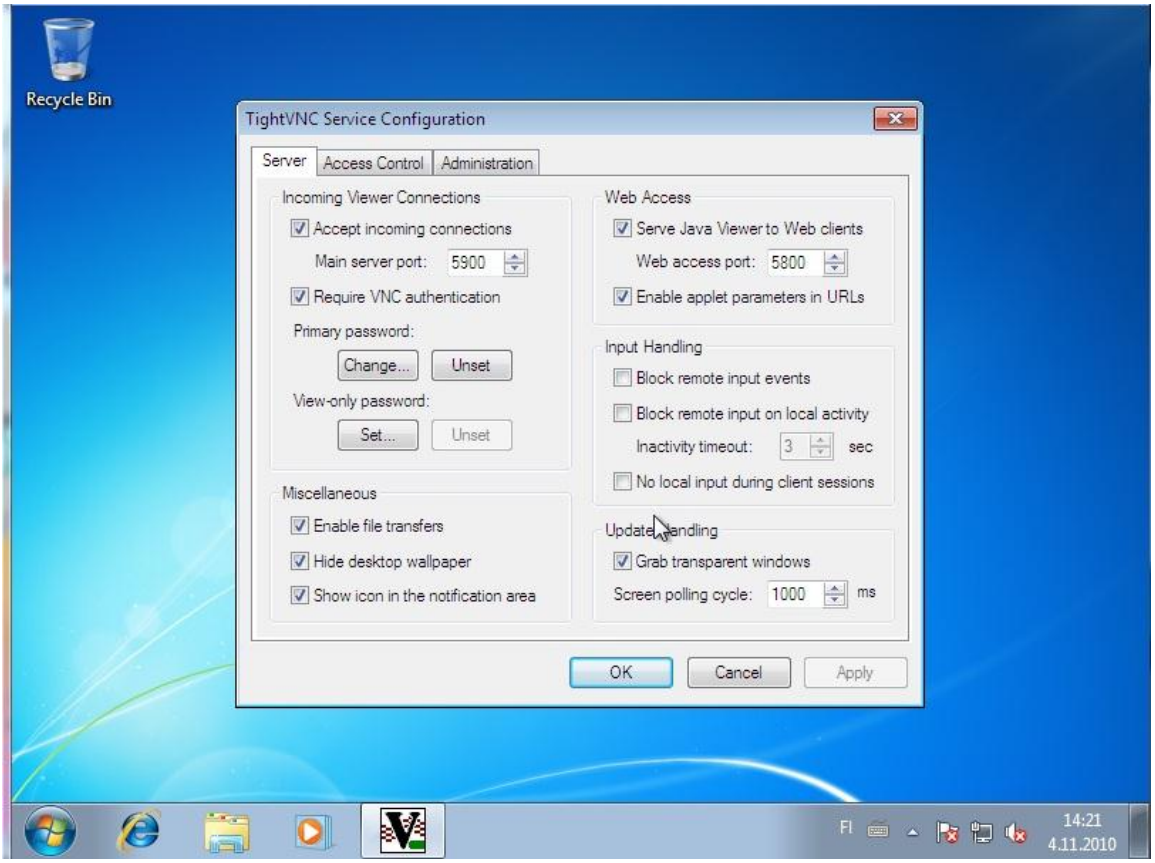
Viimeisenä yhteyden aikaista verkkoliikennettä tarkkaillaan kuvion 2 mukaisen Resource monitorin avulla ja kirjataan ylös verkonkuormituksen määrä. Sen lisäksi tarkkaillaan suorituskyvyn kuormittamista suorittimen ja muistin osalta Task Managerin ja Resource monitorin kautta ja kirjataan ylös kuinka paljon etäyhteysohjelmisto käyttää olemassa olevia resursseja.




Kuvio 2. Resource Monitor

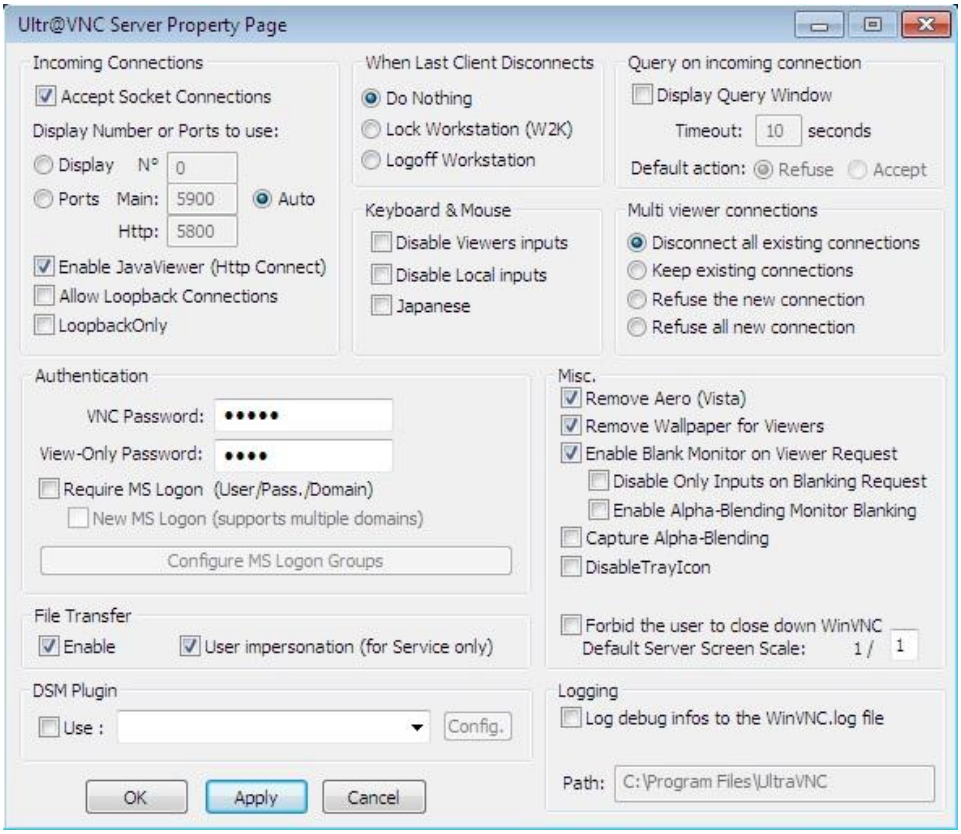
## 5.1 Käytettävät ohjelmistot

TightVNC on VNC:n parannettu versio, joka sisältää lukuisia parannuksia ja uusia ominaisuuksia alkuperäiseen VNC.n verrattuna. TightVNC on VNC:n tapaan ilmainen ja monet käyttäjät ovat sitä mieltä, että TightVNC on kehittynein ilmaisista etäyhteyssovelluksista. TightVNC:tä myös kehitetään jatkuvasti, joten uusia ominaisuuksia ja parannuksia on hyvin todennäköisesti luvassa. TightVNC:n palvelinkomponentti on nähtävissä kuviossa 3. (TightVNC 2010.)




Kuvio 3. TightVNC palvelinkomponentti

UltraVNC on ilmainen ja helppokäyttöinen VNC-etäyhteysohjelmisto, mutta tukee ainoastaan Windows -käyttöjärjestelmiä, joten UNIX-pohjaisissa järjestelmissä on suositeltavaa käyttää jotain muuta ohjelmistoa. UltraVNC tukee Mirror Driver -teknologiaa, joka tehostaa suorituskykyä ja vähentää suorittimen kuormitusta lähiverkkoyhteyksien kautta. UltraVNC tukee myös sisällytettyä tiedostonsiirtoa graafisella käyttöliittymällä ja kattaa laajan kuvion 4 mukaisen asetusvalikon. (UltraVNC 2008.)




Kuvio 4. UltraVNC Palvelinkomponentti

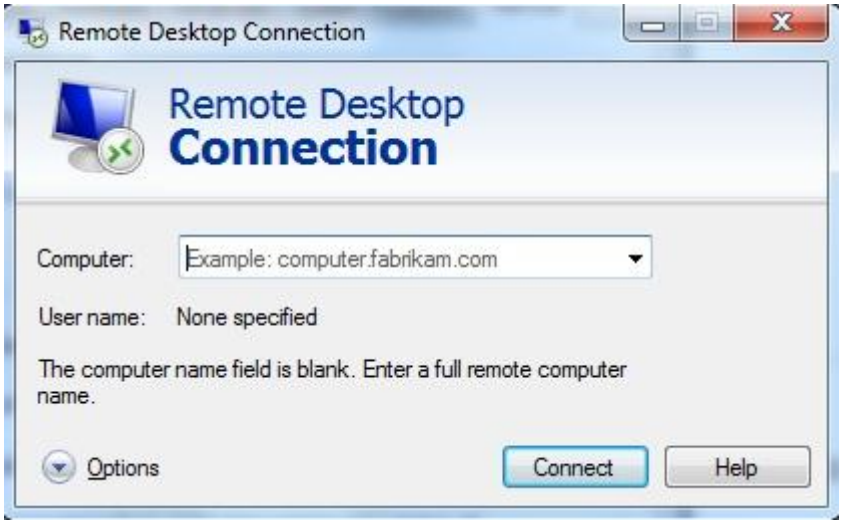
## 5.2 Asennusvaihe

Tutkimisvaihe aloitetaan asentamalla itse etäyhteysohjelmistot tietokoneelle. Koska tutkittavat ohjelmistot ovat ilmaisia ja pienikokoisia, niin ne löytyvät helposti valmistajan sivuilta ja lataus sujuu vaivattomasti hitaimmillakin verkkoyhteyksillä. Tutkimuksessa käytetään uusimpia versioita ohjelmistoista. Ominaisuudet voi vaihdella versiokohtaisesti.

TightVNC:n asennusohjelmisto löytyy TightVNC:n sivuilta osoitteesta http://www.tightvnc.com/download.php. Valittavana on uusin versio (2.0.2) Windows-käyttöjärjestelmille ja vanhempi versio, jos halutaan käyttää TightVNC:tä UNIX-käyttöjärjestelmissä. Asennusvaiheessa etätietokoneelle asennetaan pelkästään palvelinkomponentti toimimaan suoraan windows-palveluna ja paikalliselle tietokoneelle pelkästään viewer-komponentti.

UltraVNC:n asennusohjelmisto on ladattavissa suoraan UltraVNC:n kotisivuilta kohdasta download. Tutkimukseen otetaan mukaan UltraVNC:n 1.0.8.2 ”Full”-versio. Pelkkä päivitysversio ei riitä, koska aikaisempaa versiota UltraVNC:stä ei ole valmiiksi asennettu. Etätietokoneelle asennetaan palvelinkomponentti windows-palveluksi ja paikalliselle tietokoneelle viewer-komponentti.

Remote Desktop Connectionia ei tarvitse ollenkaan asentaa. Windows 7:sta se löytyy suoraan Windows-logon takaa ”accessories”-painikkeen alta. Remote Desktop Connectionin käyttöliittymä on kuvion 5 mukainen.




Kuvio 5. Remote Desktop Connection

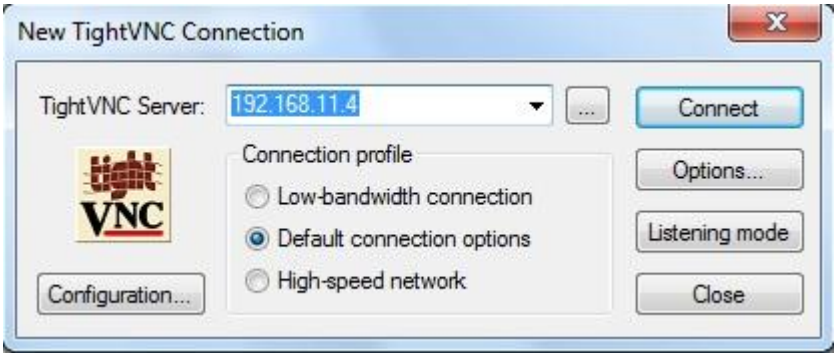
Tämän jälkeen ohjelmistot pitäisi olla asennettuina. Tutkimustulosten selkeyttämiseksi ohjelmistoja käytetään vain oletusasetuksilla ja erityisempiä konfiguraatioita ei tarvita. Tässä vaiheessa voidaan todeta, että ohjelmistojen asennus ei ole vaativaa, kun vain muistaa, mitä komponentteja on asentamassa millekin tietokoneelle.

## 5.3 Yhteyden muodostus ja tietoturva

Seuraava vaihe on muodostaa etäyhteys palvelimelle käyttäen jokaista etäyhteysohjelmistoa vuoron perään. Yhteyden muodostuksen aikana, ja sitä ennen, on tarkoitus tarkastella mitä tietoturvaominaisuuksia on olemassa kyseisessä etäyhteysohjelmistossa.

Ensiksi tutkitaan tietoturvaominaisuudet TightVNC:stä. TightVNC-palvelimen asetusikkunasta löytyvät valinnat vain IP-suodatukseen, joka ohjaa minkä IP-avaruuden IP-osoitteet pääsevät käsiksi etäyhteyspalvelimeen. Tämä on hyödyllinen ominaisuus organisaatioissa, joissa käyttäjille sallitaan pääsy verkkoon vain tietyistä IP-osoitteista. Tämän lisäksi asetuksista löytyy myös valinnat yhteyksien tietojen lokiin kirjauksesta, joka on edelleen hyödyllinen ominaisuus niissä organisaatioissa, joissa halutaan seurata käyttäjien toimintaa etäpalvelimeen. Asetuksista löytyy myös valinta perusautentikoinnille, joka käsittää vain salasanan käytön yhteyden muodostuksessa. Asetusta yhteyden salaamiselle ei löydy TightVNC:stä ollenkaan Windows -versiossa. Tietoturvaominaisuudet ovat näin vain hyvin vähän kehittyneemmät, kuin alkuperäisessä VNC:ssä

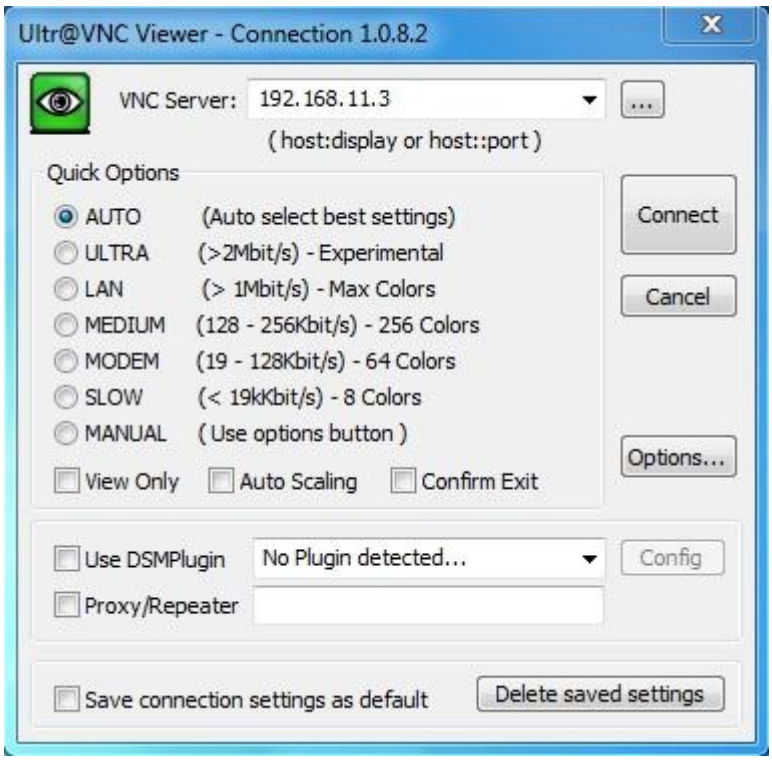
Yhteyden muodostus tapahtuu paikalliselta tietokoneelta käynnistämällä kuvion 6 mukainen TightVNC-viewer ja kirjoittamalla TightVNC Server -kenttään etäpalvelimen IP-osoitteen. Yhteyden muodostuksessa kysytään käyttäjältä salasanaa, jolla päästään kirjautumaan etäpalvelimelle. Tämän jälkeen käyttäjä näkee etäpalvelimen työpöydän paikallisella tietokoneella.




Kuvio 6. TightVNC viewer.

Seuraavaksi tarkastelussa on UltraVNC. TightVNC:n verrattuna UltraVNC:n palvelinasetuksista puuttuu IP-suodatus kokonaan. Ominaisuudeltaan IP-suodatus olisi ollut erittäin hyvä käyttäjienhallintamenetelmä UltraVNC:hen. Myös UltraVNC:stä löytyy mahdollisuus tietojen lokiin tallettamisesta, sekä perusautentikoinnista salasanan avulla. UltraVNC:stä löytyy kuitenkin mahdollisuus salata etäyhteys käyttäen erilaisia liitännäisiä. Yhteyden salaus on tietoturvan kannalta erittäin hyvä ominaisuus ja tärkeintä onkin salata yhteys, jos organisaation verkkoon halutaan käyttäjille sallia pääsy organisaation verkon ulkopuolelta. Salaus toimii luomalla eräänlainen avaintiedosto, joka sijaitsee etäpalvelimella ja paikallisella tietokoneella. Suojaustaso liitännäisissä yltää 128-bittiseen tasoon asti.

Yhteyden muodostus etäpalvelimeen UltraVNC:llä tapahtuu samalla tavoin, kuin TightVNC:llä. Etäpalvelimen IP-osoite kirjoitetaan VNC Server -kenttään yhteyden muodostusta varten. UltraVNC:ssä on valittavana eri yhteysnopeusvaihtoehtoja riippuen esimerkiksi siitä, miten nopea verkko on käytössä. Vaihtoehdot ovat nähtävissä kuviossa 7. Yleensä organisaatioiden verkot ovat nopeita, joten suurinta mahdollista yhteysnopeusvaihtoehtoa voidaan käyttää vaivattomasti. Eri yhteysnopeusvaihtoehdot tosin määrittävät vain sen, kuinka monta väriä on käytössä etätyöpöydällä. Yhteyden muodostuksessa kysytään käyttäjältä salasana, jolla päästään kirjautumaan etäpalvelimelle. Tämän jälkeen käyttäjä näkee etäpalvelimen työpöydän paikallisella tietokoneella.




Kuvio 7. UltraVNC viewer.

Viimeisenä kohteena on Remote Desktop Connectionin tarkkailu. Tietoturvaominaisuuksiltaan Remote Desktop Connection on suhteellisen hyvä. Ennen yhteyden muodostusta kirjataan domain-, käyttäjätunnus- ja salasana-kenttiin halutut tiedot. Käyttäjätunnus on oltava jokin tunnus, mikä esiintyy etäpalvelimella. Sen lisäksi kyseinen tunnus on sallittava erikseen etäyhteyttä varten. Etäpalvelimeen on myös sallittava yleisesti etäyhteyksien muodostus ennen kuin etäyhteyksiä aletaan muodostaa. Yhteyden salaus voidaan asettaa toimimaan 128-bittisella tasolla Remote Desktop Services group policyn kautta.

Yhteyden muodostus onnistuu avaamalla Remote Desktop Connection ”accessories” -kohdan alta Windows-logoa klikkaamalla. Erilaisten asetusvaihtoehtojen puolesta Remote Desktop Connection on hyvä, koska esimerkiksi näytön resoluutiot, äänien ja lisälaitteiden käyttö on helposti säädettävissä yhteyttä muodostaessa. Sen lisäksi etätyöpöydän suorituskykyä voidaan muuttaa valitsemalla parhain tilanteeseen soveltuva yhteysnopeusvaihtoehto, joka kytkee päälle tai pois tiettyjä työpöydän ominaisuuksia, kuten teemat.

## 5.4 Verkkoliikenne ja suorituskyvyn kuormitus

Osin tavoitteena on tarkastella kuinka paljon etäyhteysohjelmistot kuormittavat yhteyden ollessa muodostettuna verkkoa ja paikallisen tietokoneen suoritinta ja keskusmuistia. Tutkiminen alkaa käynnistämällä Task Manager ja muodostamalla ensin yhteys etäpalvelimelle TightVNC:tä käyttäen.

Yhteys muodostetaan TightVNC -viewerillä käyttäen oletusasetuksia. Kun etätyöpöytä on näkyvissä ikkunassa, voidaan tarkastella resurssien käyttöä Task Managerin ja Resource Monitorin avulla. Kaikilla ohjelmistoilla avataan etänäkymästä useampi kansio sekä käynnistetään paint.exe ja piirretään yksinkertainen kuva. Tällä nähdään se miten paljon kuormitusta syntyy kyseisten toimenpiteiden suorittamiseen.

Task Managerista ja Recourse Monitorista huomataan, että prosessorin kuormitus on toimenpiteiden aikana ollut noin 0-8% alueella ja keskiarvoksi saadaan 6.65%. Muistin käytön osalta TightVNC -viewer käyttää noin 2,2Mt keskusmuistia käynnissä ollessaan. Muistin käyttö ei ole muuttunut toimenpiteiden aikana. Verkon kuormitus on Resource Managerin mukaan noin 3 t/s, kun yhteys on muodostettu ja mitään ei tehdä. Kun mainitut toimenpiteet olivat tehty, niin verkon kuormitus nousi 4,6 kt/s:iin (Send: 776 t, Recieve: 3,831 kt) ja pysyi tällä alueella. Voidaan todeta, että käynnissä ollessaan ja tiedostoja käyttäessään TightVNC ei kuormita verkkoa juuri ollenkaan.

Etäpalvelimelta verkon kuormitusta tarkastaessa TightVNC -serveri näytti noin 22 Kt/s kuormitusta toimenpiteiden aikana. Tarkastelusta ei käy ilmi miksi palvelin lähettää enemmän dataa kuin mitä viewer sitä vastaanotti paikallisella tietokoneella.

Seuraavaksi tarkastellaan samoja kuormituksia UltraVNC:tä käyttäen. TightVNC:n tapaan myös UltraVNC:llä yhteys muodostetaan oletusasetuksia käyttäen.

Task Managerista ja Resource Monitorista nähdään, että UltraVNC -viewerin prosessorin käyttö toimenpiteiden aikana oli 0-3% ja keskiarvona 1,44%. Keskusmuistia UltraVNC käyttää 5,5 Mt eikä muistin käyttötarve muutu yhteyden aikana. Verkon kuormitus nousi UltraVNC:llä toimenpiteiden aikana noin 10 kt/s:iin (Send: 1,2 kt, Recieve 8,8 kt). Valmiustilassa kuormitus on TightVNC:n tasolla, eli noin 3 t/s.

Etäpalvelimella UltraVNC -serveri näytti kuormittavan verkkoa jopa 100 kt/s, kun toimenpiteitä suoritettiin. Voidaan todeta UltraVNC:n kohdalla sama kuin TightVNC:n kohdalla, eli palvelin lähettää dataa enemmän, kuin mitä viewer ottaa vastaan paikallisella tietokoneella.

Viimeisenä on vuorossa Remote Desktop Connection. Remote Desktop Connectionista ei välttämättä saa minkäänlaisia arvoja itse etäpalvelimen kuormituksesta, vaan ainoastaan paikallisen tietokoneen kuormituksesta. Yhteys muodostetaan edelleenkin oletusasetuksilla, eli mitään muita asetuksia ei muuteta, kuin kokoruutu tila pois käytöstä.

Etäyhteyden aikana Remote Desktop Connectionilla prosessorin kuormitus oli toimenpiteiden aikana 0-3% ja keskiarvona 1.14%. Keskusmuistin käyttö oli 22 Mt ja pysyi muuttumattomana toimenpiteiden aikana. Verkon kuormitus toimenpiteiden aikana nousi Remote Desktop Connectionissa 44,7 kt/s:iin (Send: 4 Kt, Recieve: 40,7 kt) ja paikallaan ollessa kuormitus oli 2,2 kt/s. Etäpalvelimen kuormituksia ei voitu mitata ollenkaan.

# 6 TULOKSET JA POHDINTA

Etäyhteysohjelmistoja tutkimalla saatiin selkeitä tuloksia tietoturvaominaisuuksista suorittimen, muistin ja verkon kuormituksesta sekä asentamisen helppoudesta. Ohjelmistojen asentamiseen ei tarvita erityistä tuntemusta. Monet ohjelmistot saadaan asennettua painalla ”next”-nappia koko ajan.

## 6.1 Tietoturvan tulokset

TightVNC:llä, UltraVNC:llä ja Remote Desktop Connectionilla on omat tietoturvaominaisuudet, jotka vaihtelevat huomattavasti. TightVNC on ominaisuuksiltaan vain jonkin verran turvallisempi, kuin tavallinen VNC-yhteys, mutta kärsii samoista puutteista, kuten yhteyden salaamattomuudesta. Yhteyden SSH-salaus on tehtävä itse tai käytettävä UNIX-pohjaisia käyttöjärjestelmiä, joissa salaus onnistuu automaattisesti. TightVNC:n IP-suodatus on hyödyllinen ominaisuus organisaatioiden käytössä, kun halutaan sallia vain tietyt IP-osoitteet organisaation verkkoon käyttäen etäyhteyttä.

UltraVNC:stä löytyy erilaisuuksia TightVNC:en verrattuna. UltraVNC:llä pystytään liitännäisillä salaamaan etäyhteys 128-bittisellä salauksella, joten salaus onnistuu myös Windows -käyttöjärjestelmillä. Liitännäisissä on omat ongelmansa, koska liitännäisiä pitää hallita palvelimilla ja paikallisilla tietokoneilla asettamalla tietty salausavain, jolla päästään muodostamaan etäyhteys. IP-suodatus, joka olisi toivottu tietoturvaominaisuus organisaatioiden käytössä, puuttuu UltraVNC:stä kokonaan.

Remote Desktop Connection ei tarjoa laajasti muokattavia tietoturvaominaisuuksia. Etäpalvelimelta on sallittava kuitenkin Remote Desktopin käyttö tietylle käyttäjälle, jolla on käyttäjätunnus etäpalvelimella. Group Policyjen kautta Remote Desktop Connectionin etäyhteys voidaan kuitenkin salata 128-bittiseen salaukseen saakka sekä säätää muita tietoturvaominaisuuksia.

## 6.2 Resurssien käytön tulokset

Jokainen testattu etäyhteysohjelmisto kuormittaa paikalliselta tietokoneelta ja etäpalvelimelta tietyn verran prosessoria, keskusmuistia ja verkkoa. TightVNC:llä huomattiin, että prosessorin kuormitus oli 0-8%, ka 6,65%, keskusmuistin käyttö 2,2Mt ja verkon kuormitus 3 t/s valmiustilassa ja 4,6 kt/s toimenpiteiden aikana. UltraVNC:llä vastaavasti prosessorin kuormitus oli 0-3%, ka 1.44%, keskusmuistin käyttö 5,5 Mt ja verkon kuormitus 3 t/s valmiustilassa ja toimepiteiden aikana 10 kt/s. Viimeisenä Remote Desktop Connectioissa prosessorin kuormitus oli 0-3%, ka 1,14%, keskusmuistin käyttö 22 Mt ja verkon kuormitus 44 kt/s toimenpiteiden aikana ja 2,2 kt/s valmiustilassa.

Kaikki nämä ovat paikalliselta tietokoneelta mitattu. Etäpalvelimelta huomattiin ainoastaan TightVNC:llä ja UltraVNC:llä, että etäpalvelin lähettää enemmän dataa, kuin mitä paikallinen tietokone ottaa vastaan. Mielenkiintoista on se, minne ylimääräinen data häviää.

Tuloksista voidaan todeta, että pelkästään tietoturvaominaisuuksien ja resurssien käytön perusteella on vaikeaa suositella mitä TightVNC:stä, UltraVNC:stä ja Remote Desktop Connectionista olisi parhainta käyttää. Tietoturvaominaisuuksiltaan kaikki olivat samaa tasoa ja resurssien käytöt itsessään eivät olleet isoja yhdelläkään etäyhteysohjelmistolla, joten etäyhteydet onnistuisivat varmasti jopa kymmenen vuoden takaisella tietokoneen kokoonpanolla etäyhteysohjelmistosta riippumatta. Yhteenvetona tuloksista on nähtävissä taulukossa 2.

**Taulukko 2: Tutkimustulokset**

| | TightVNC | UltraVNC | RDC |
|---|---|---|---|
| Suoritin | 0-8%, ka 6,65% | 0-3%, ka 1,44% | 0-3%, ka 1,14% |
| Keskusmuisti | 2,2 Mt | 5,5 Mt | 22 Mt |
| Verkko | 3 t/s, 4,6 kt/s | 3 t/s, 10 kt/s | 2,2 kt/s, 44 kt/s |

## 6.3 Pohdinta

Opinnäytetyössä on käsitelty yksinkertaisesti, mutta selkeästi VNC:n ja RDP:n toiminta ja tutkittu erilaisia etäyhteysohjelmistoja VNC- ja RDP-protokollalle. Tuloksista on hankala sanoa mitä etäyhteysohjelmistoa olisi parasta käyttää, koska opinnäytetyö keskittyi lähinnä VNC- ja RDP-protokollaan ja kyseisiä protokollia käyttävien etäyhteysohjelmistojen ilmaisversioihin. Tuloksissa todettiin, että tietoturvaominaisuudet olivat hyvin samankaltaisia keskenään ja ominaisuudet voisivat vaihdella huomattavasti keskenään, jos testattavana olisi ollut myös maksullisia etäyhteysohjelmistoja. Resurssien käyttökin vaihtelisi varmasti, jos paikallisen tietokoneen kokoonpano olisi esimerkiksi hyvin vanha tai aivan uusi. Jatkotutkimuksena olisi hyvä käydä läpi muiden protokollien etäyhteysohjelmistoja sekä maksullisia etäyhteysohjelmistoja VNC:stä ja RDP:stä.

Etäyhteydet itsessään on suunniteltu vain etätietokoneeseen yhteyden muodostusta varten. Valittavana on kuitenkin monia eri keinoja etäyhteystapoihin. Organisaatioiden tapauksissa olisi varmasti hyvä valita sellainen etäyhteysohjelmisto, joka soveltuu tietoturvaominaisuuksiltaan, muilta ominaisuuksiltaan ja resurssien käytöltään organisaation tarpeisiin.

LÄHTEET

Apple Inc. 2010. Remote Desktop 3. http://www.apple.com/remotedesktop/ (Luettu 22.11.2010).

BreakingPoint. 2010. Citrix ICA Protocol. http://www.breakingpointsystems.com/default/assets/File/data%20sheets/breakingpoint_app_citrix.pdf (Luettu 22.11.2010).

Cooper S. 2010. Thin client appliance link protocol. http://www.ehow.com/facts_7270631_thin-client-appliance-protocol.html (Luettu 22.11.2010).

Emery, V. 2003. VNC over SSH2 – A TightVNC tutorial. http://www.vanemery.com/Linux/VNC/vnc-over-ssh.html (Luettu 1.12.2010)

Lacoma, T. 2010. How Does a Remote Connection Work? http://www.ehow.com/how-does_6016489_remote-connection-work_.html (Luettu 1.1.2011).

Life's Good. 2010. RFB Protocol. http://nagalenoj.blogspot.com/2010/04/rfb-protocol-ii.html (Luettu 1.3.2011).

Medialogic. 2010. NX technology. http://www.nomachine.com/documents/intr-technology.php (Luettu 22.11.2010).

Microsoft. 2010 a. Remote Desktop Protocol. http://msdn.microsoft.com/en-us/library/aa383015(VS.85).aspx (Luettu. 22.11.2010).

Microsoft. 2010 b. About Remote Desktop Services. http://msdn.microsoft.com/en-us/library/aa380400(v=VS.85).aspx (Luettu 1.1.2011).

Microsoft. 2010 c. Resources on a Remote Desktop Session Host Server. http://msdn.microsoft.com/en-us/library/aa383052(v=VS.85).aspx (Luettu 1.1.2011).

Microsoft. 2010 d. Remote Desktop Sessions. http://msdn.microsoft.com/en-us/library/aa383496(v=VS.85).aspx (Luettu 1.1.2011).

Microsoft. 2010 e. Remote Desktop Services API. http://msdn.microsoft.com/en-us/library/aa383459(v=VS.85).aspx (Luettu 1.1.2011).

Microsoft. 2010 f. Remote Desktop Services Virtual Channels. http://msdn.microsoft.com/en-us/library/aa383509(v=VS.85).aspx (Luettu 1.1.2011).

RealVNC. 2010. RealVNC. http://www.realvnc.com/company/index.html (Luettu 22.11.2010).

Richardson, T. 2010. The RFB Protocol. http://www.realvnc.com/docs/rfbproto.pdf (Luettu 1.12.2010).

SearchMidMarketSecurity.com 2009 http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci212887,00.html (Luettu 1.12.2010).

TeraDici. 2010 a. PCoIP. http://www.teradici.com/pcoip/pcoip-technology.php (Luettu 22.11.2010).

TeraDici. 2010 b. Display Processing. http://www.teradici.com/pcoip/pcoip-technology/display-processing.php (Luettu 1.1.2011).

TeraDici. 2010 c. Networking. http://www.teradici.com/pcoip/pcoip-technology/networking.php (Luettu 1.1.2011).

TeraDici. 2010 d. Security. http://www.teradici.com/pcoip/pcoip-technology/security.php (Luettu 1.1.2011).

TeraDici. 2010 e. WAN Support. http://www.teradici.com/pcoip/pcoip-technology/wan-support.php (Luettu 1.1.2011).

TightVNC. 2010. TightVNC. http://www.tightvnc.com/intro.php (Luettu 22.11.2010).

The Free dictionary. 2010. Remote Desktop Software. http://encyclopedia.thefreedictionary.com/Remote+desktop+software (Luettu 22.11.2010).

ToastyTech, 2010. X Windowing System. http://toastytech.com/guis/remotex11.html (Luettu 22.11.2010).

UltraVNC. 2008. UltraVNC. http://www.uvnc.com/index.html (Luettu 22.11.2010).

WarePrise. 2010. List of Free Remote Desktop Software for Telecommuters. http://www.wareprise.com/2008/11/28/list-of-free-remote-desktop-software-for-telecommuters/ (Luettu 1.3.2011).

Yegulalp, S. 2010. Thin Client. http://itmanagement.earthweb.com/netsys/article.php/3865151/Thin-Client.htm (Luettu. 22.11.2010)