POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Eetu Räsänen

ETÄHALLINTATEKNIIKAT YKSITYISKÄYTÖSSÄ

Opinnäytetyö
Huhtikuu 2011

OPINNÄYTETYÖ
Huhtikuu 2011
Tietojenkäsittelyn
koulutusohjelma
Länsikatu 15
80200 JOENSUU
p. 050 311 6310

Tekijä
Eetu Räsänen

Nimeke
Etähallintatekniikat yksityiskäytössä

Tiivistelmä

Tämä opinnäytetyö tarkastelee Linux- ja Windows-koneiden, laitteiden ja tietojen etähallintaa verkon yli sekä graafisesti että merkkipohjaisesti. Etätyöskentely on jatkuvasti kehittyvä ja laajeneva työskentelymuoto, jossa käyttäjä ottaa yhteyden haluamaansa työasemaan tai palvelimeen. Etäyhteydet mahdollistavat erinäisten työtehtävien hoitamisen pitkienkin matkojen päästä, jolloin käyttäjän ei itse tarvitse olla käytettävän koneen luona. Näin työasemien etähallinnalla voidaan saavuttaa useita etuja. Työ antaa lukijalle myös kuvan menetelmien vaikeuksista ja käytettävyydestä, jolloin hän voi päätellä itselleen sopivimman ratkaisun työasemansa tai palvelimensa etähallintaan.

Työ on jaettu merkkipohjaiseen etähallintaan Linux-käyttöjärjestelmässä sekä graafiseen etäkäyttöön Linux- ja Windows-ympäristöissä. Supermatrix-projekti on mahdollisesti tuomassa takaisin keskustietokoneympäristö ajattelumallin.

Yhteenvetona tästä työstä voidaan sanoa, että etäkäytön käyttöönotto ei ole nykypäivänä kovinkaan vaikeaa. Lähes jokainen käyttöjärjestelmä tarjoaa omat vaihtoehtonsa etäyhteyksien muodostamiselle.

Kieli
suomi

Sivuja 38

Asiasanat
etäyhteydet, etähallinta, etähallintaprotokollat

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS

April 2011

Degree Programme in Business Information Technology

Länsikatu 15

FIN 80200 JOENSUU

FINLAND

Tel. 358-50 311 6310

Author
Eetu Räsänen

Title
Remote Connection Techniques for Private Use

Abstract

This thesis examines the Linux and Windows machines, devices and remote management of data over the network, graphically as character-based. Remote controlling is a constantly evolving and expanding employment form where the users have access to the desired workstation or server over a distance. Remote connections enable the performance of various work duties over long distances. A number of advantages can be achieved by remote workstation management.

The current thesis examines the difficulties and the availability of methods, which helps a user to select the most suitable solutions for workstations or servers for remote monitoring. The study is divided into character-based remote management of the Linux operating system and graphical remote management in both Linux and Windows environments.

As a conclusion can be stated that remote management is not very difficult today. Almost every operating system provides its own options for remote connections.

Language
Finnish

Pages 38

Keywords

remote connections, remote control, remote protocols

Sisältö

Lyhenteet

IP-NUMERO	Internet Protocol on TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikenne-pakettien toimittamisesta perille Internet-verkossa.
RDP	Remote Desktop Protocol on Microsoftin kehittämä protokolla, joka tarjoaa käyttäjälle graafisen käyttöliittymän toiseen tietokoneeseen.
SCP	Secure Copy on komentoriviohjelma, jolla tiedostoja kopioidaan SSH-protokollan yli.
SSH	Secure Shell on salattuun tietoliikenteeseen tarkoitettu protokolla.
SSL	Secure Sockets Layer on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
TLS	Transport Layer Security on aiemmin tunnettu nimellä Secure Sockets Layer (SSL).
VNC	Virtual Network Computing on protokolla tietokoneen käyttöliittymän etäkäyttöön.

1 Johdanto

Tämä opinnäytetyö tarkastelee Linux- ja Windows-koneiden, laitteiden ja tietojen etähallintaa verkon yli sekä graafisesti että merkkipohjaisestikin. Etätyöskentely on jatkuvasti kehittyvä ja laajeneva työskentelymuoto, jossa käyttäjä ottaa yhteyden haluamaansa työasemaan tai palvelimeen. Etäyhteydet mahdollistavat erinäisten työtehtävien hoitamisen pitkienkin matkojen päästä, jolloin käyttäjän ei itse tarvitse olla käytettävän koneen luona. Näin työasemien etähallinnalla voidaan saavuttaa useita etuja.

Tässä opinnäytetyössä selvitetään käyttäen empiiristä tutkimusmenetelmää yleisimpiä etähallintaohjelmistoja, -protokollia ja -tapoja yleisimmissä käyttöjärjestelmissä. Työ antaa lukijalle myös kuvan menetelmien vaikeuksista ja käytettävyydestä, jolloin hän voi päätellä itselleen sopivimman ratkaisun työasemansa tai palvelimensa etähallintaan. Työ on jaettu kolmeen kokonaisuuteen. Ensimmäisenä on merkkipohjainen etähallinta Linux-ympäristössä. Tämän jälkeen tarkastellaan Linux-palvelimen graafista etäkäyttöä ja viimeisenä etähallintamenetelmiä Windows-ympäristössä.

Linuxin (eli GNU/Linux) vahvuus käyttöjärjestelmänä on sen avoin lähdekoodi. Sen etuja ovat sen mm. maksuttomuus, lupa tutkia, muokata ja kopioida koodia. Kaikkien käyttäjien päästessä ohjelmistojen toiminnalliseen asteeseen käsiksi tietoturva ja käytettävyys hioutuvat huomattavasi käyttäjäystävällisemmäksi kuin suljetun lähdekoodin sovelluksissa. Mainittakoon näistä esimerkiksi Microsoftin Windows-käyttöjärjestelmät. Avoimen lähdekoodin ansiosta myös Linuxin etäkäyttö on hioutunut niin hyväksi kuin se nykyään on. Windows-maailmaan etäkäyttö integroitui vasta Windows XP:n mukana. (Kuutti & Rantala 2007.)

Supermatrix-projektin myötä ollaan ehkä palaamassa enemmän keskustietokone-ympäristöön. Supermatrixin käyttö rajoittuu tällä hetkellä vain projektin omaan valokuituverkkoon, sillä Internetverkko on liian hidas ja ruuhkainen välittämään tietokoneen työpöydän kuvaa.

2 Merkkipohjainen etähallinta Linux-ympäristössä

Komentotulkki eli *terminal* on Linuxin merkkipohjainen työkalu komentojen ajamiseen. Kaikki grafiikka, oli kyseessä sitten käyttäjän työpöytä tai jokin muu graafinen sovellus, tuotetaan erilaisin lisäsovelluksin komentotulkin päälle. Kaikki graafisesti tehdyt muutokset toteutetaan todellisuudessa tulkin kautta merkkipohjaisina komentoina. Komentotulkki on syntaksiltaan eli käskyiltään yksinkertainen ja looginen, mutta komennot on kertaalleen opittava. Siinä, missä graafista ympäristöä pystyy usein käyttämään maalaisjärjellä, esimerkiksi raahaamalla kansion paikasta A paikkaan B, vaatii merkkipohjainen käsittely komentojen opettelun. Manuaalit helpottavat syntaksin ja eri sovellusten parametrien muistamista. (Kuutti & Rantala 2007.)

Merkkipohjaisia Linux-etähallintaprotokollia on kaksi:
TELNET
SSH (SSH-1 ja SSH-2)
Sarjakaapeli, päätelaite ja jokin prosessiprotokolla kirjautumiseen, mutta tämä ei ole mielestäni etähallintaa. Käytännössä sarjakaapeli pitää kiinnittää Linux-koneeseen paikan päällä, jolloin kyseessä on paikallishallinnointia.

TELNET-protokollaa ei käytetä enää juuri lainkaan, heikon tietoturvan vuoksi. Ei ole syytä perehtyä ”kuolevaan” protokollaan sen tarkemmin. TELNETiä on käytetty samanlaiseen etähallintaan kuin SSH:ta. Heikosta tietoturvasta kertovat mm. seuraavat syyt:

- TELNET-protokolla ei autentikoi keskustelevia koneita, joten välimieshyökkäys on mahdollinen.
- Kaikki tieto lähetetään salaamattomana, myös salasanat.
- Lähes kaikista TELNET-sovelluksissa on löydetty vuosien varrella reikiä, joita hyödyntämällä hakkerointi on mahdollista.

(Telnet 2011.)

Vuonna 1995 Tatu Ylönen, tutkija Helsingin yliopistosta, suunnitteli ja kirjoitti SSH:n ensimmäisen version (SSH-1). Tästä lähtien SSH:n suosio on ollut hyvin suurta ja syystä. Vuonna 1996 SSH-1:stä kehitettiin parempi SSH-2-protokolla, joka ratkaisee vaatimattomasti kaikki TELNET-protokollan tietoturvaongelmat. SSH:n suosiosta kertoo myös se, että vuonna 2006 SSH:sta (SSH-2) tuli '*proposed Internet standard*' *IETF:n* (Internet Engineering Task Force) toimesta – eli aiottu uusi standardi. SSH-2-protokolla on siis kaikin puolin turvallinen tapa siirtää tietoa verkkojen välillä. (Dwivedi 2003.)

Vaikka SSH-2-protokolla on jo yli 10 vuotta vanha, eivät kaikki sovellukset tue sitä. SSH-1:n kanssa törmääkin usein salausprotokolliin *SSL (Secure Sockets Layer)* ja uudempaan *TLS:ään (Transport layer Security).* Näiden salausprotokollien avulla SSH-1-yhteys saadaan turvattua. Salauksesta saadaan vahva, eli sen purkaminen on käytännössä mahdotonta. Myös palvelimet voidaan autentikoida vahvasti, eli vastaanottavan pään palvelimella on julkinen avain yleisessä jakelussa ja yhteyden ottavalla päällä oma yksityinen avain. Näiden avulla koneet voivat varmistua ensimmäisen yhteyden jälkeen, että yhteydenotto tapahtuu aina samaan koneeseen. Välimieshyökkäys on siis eliminoitu ensimmäisen yhteyden oton jälkeen. (Secure Shell 2011.)

SSL-/TLS-salausprotokollia voidaan käyttää mm. seuraavissa tapauksissa:

- Julkisten avainten salakirjoittaminen: RSA, Diffie-Hellman, DSA tai Fortezza.
- Symmteriseen salakirjoitukseen: RC2, RC4, IDEA, DES, Triple DES tai AES.
- Yksisuuntaisiin tiivisteisiin: MD5 tai SHA.

(Secure Shell 2011.)

Merkkipohjainen etähallinta ei sinänsä siis vaadi salausta (TELNET-yhteydet salaamattomia), mutta käytännössä yhteys on poikkeuksetta suojattu SSH:lla. Yhteyden muodostaminen kahden koneen välille vaatii siis SSH-protokollaa ymmärtävän ohjelmiston sekä palvelin- (server) että asiakaspäähän (client). Ohjelmistot ovat hyvin vaivattomia asentaa Linuxille (ssh-server ja ssh-client).

On tärkeää ymmärtää, että yhdistämällä Linux-järjestelmä esim. Windows-järjestelmään (SSH+SambaMount) voidaan käytännössä esim. kaikkia sisäverkon koneita ja tiedostoja etähallita turvallisesti sisäverkon ulkopuolelta.

Harva käyttäjä tuntuu ymmärtävän, että SSH-yhteys on VPN-yhteys. Yhteys on tunneloitu suojatusti kahden koneen välille.

2.1 Yleisimmät SSH-sovellukset merkkipohjaisessa etähallinnassa

Yleisimpiin SSH:n merkkipohjaisiin sovelluksiin/käyttökohteisiin kuuluvat:

Komentotulkkien käyttö muiden Linux-koneiden etähallinnassa, esim. Gnome-terminal

SFTP (SSH File Transfer Protocol)
Kansioiden ja tiedostojen etähallinta

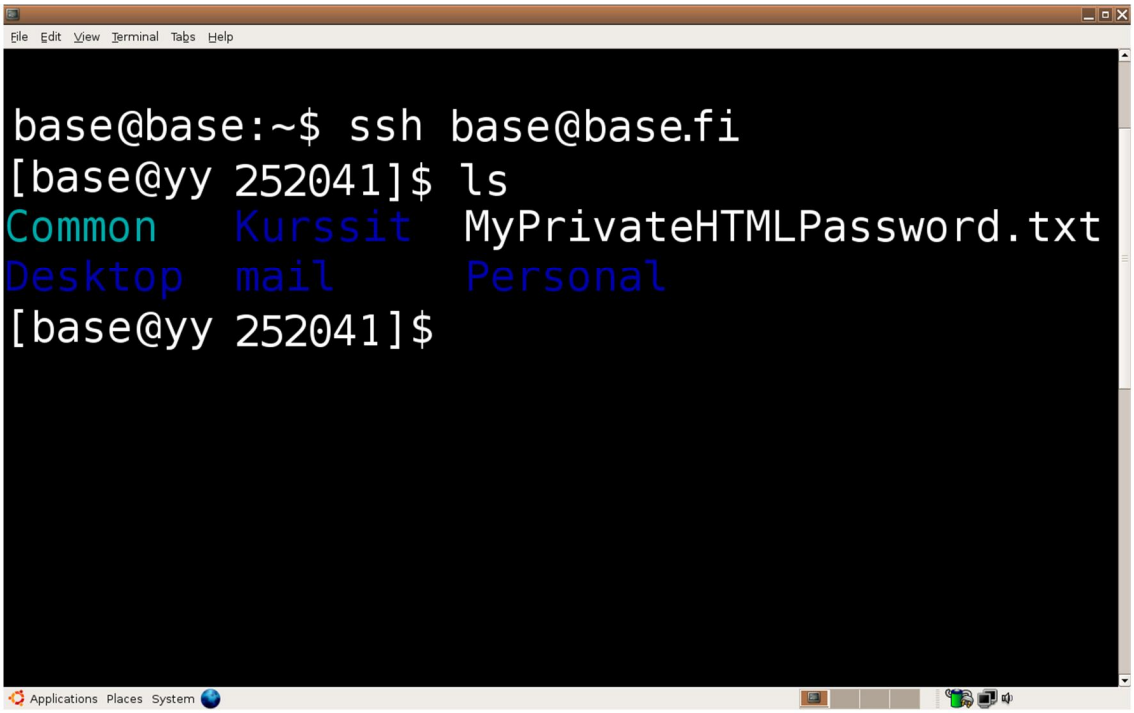
SCP (Secure Copying)
Tiedostojen etähallinta (SFTP syrjäyttänyt pitkälti)

Gnome-terminal (tai vastaava komentotulkki)

Tällä hetkellä lähes jokaisella Linux-komentotulkilla on mahdollista etähallita muita Linux-koneita. Kuvassa 1 on esimerkki SSH:n käytöstä Linux-komentotulkista, jossa SSH-yhteys otetaan seuraavalla komennolla:

```
ssh <käyttäjä>@<palvelin>
```

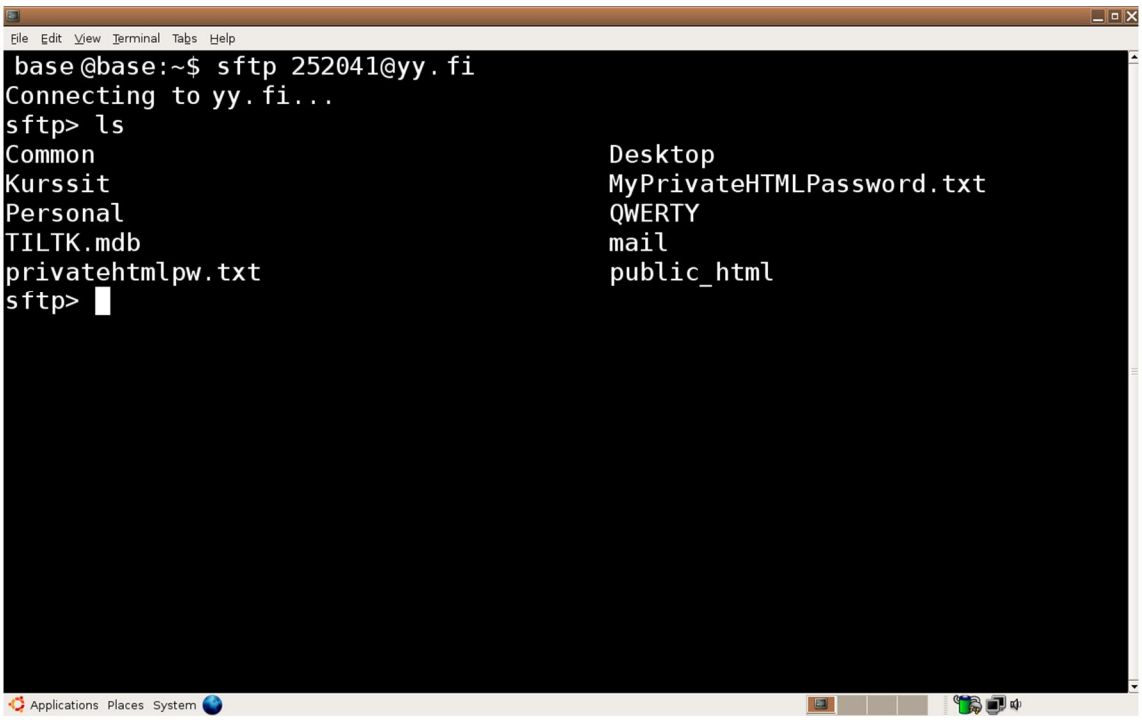
Oikeuksista riippuen käyttäjä pystyy etähallita palvelinkonetta. Jos käyttäjällä on täydet oikeudet tai admin-tason oikeudet muokata käyttäjänsä oikeuksia, pystyy käyttäjä SSH-yhteyden yli tekemään täysin samoja asioita palvelinkoneella kuin omalla koneellaan.



Kuva 1. SSH-yhteys kotipalvelimelta yy-palvelimelle.

SFTP – SSH File Transport Protocol

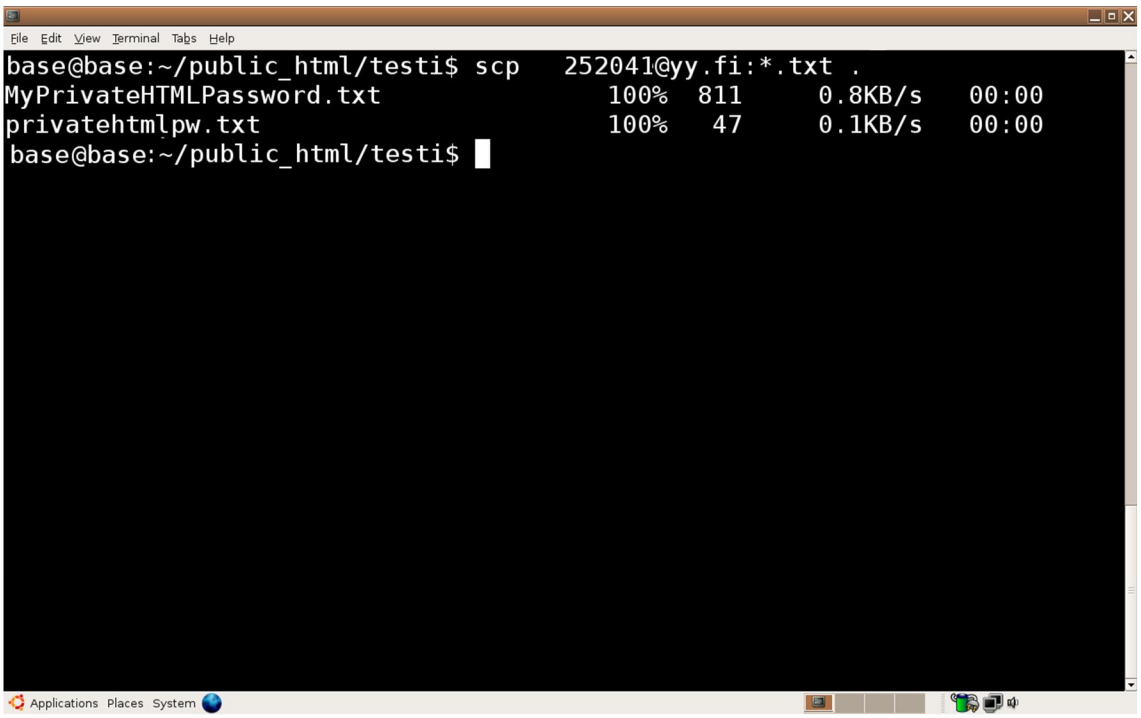
Kuva 2 osoittaa miten SFTP toimii FTP:n tavalla, mutta yhteys on salattu SSH-2-protokollaa käyttäen. SFTP:llä voidaan liikkua kansioiden välillä ja kopioida tiedostoja etäkoneelta palvelimelle ja palvelimelta etäkoneelle. Myös palvelimen sisäinen tiedostojen ja kansioiden hallinta onnistuu.



Kuva 2. SFTP-yhteys kotikoneelta yy-palvelimelle.

SCP – Secure Copying

SCP on verkon yli tapahtuvaa tiedostojen kopiointia SSH-protokollaa hyväksi käyttäen. Kopioitavat tiedostot on tiedettävä edeltä, sillä kopiointi suunnataan suoraan tiedostoihin. Kansioita eikä tiedostoja pystytä 'surffaamaan' kuten SFTPssä tai suorassa SSH-yhteydessä (Gnome-terminal tai vast.) Esimerkki SCP:n käytöstä on osoitettu kuvassa 3.



Kuva 3. TXT-tiedostojen kopiointi SCP:n avulla kirjoittajan kuvitteelliselta yy-kotikansiosta kotipalvelimelle.

2.2 Verkotus SSH-, Samba- ja Web-palvelimia hyödyntäen

Linux-ympäristössä on vaivatonta yhdistää toisen koneen kiintolevyt sisäverkon yli *jaetuiksi resursseiksi*. Toimenpidettä kutsutaan *mounttaamiseksi*. Tällä tavoin on mahdollista yhdistää kaikki sisäverkon koneet yhden palvelimen taakse. Esimerkiksi voidaan toteuttaa Windows-koneen levyjen jaot sisäverkon yli Linux-palvelimelle siten, että sieltä pääsee www-sivujen läpi (Apache2) käsiksi Windows-levyihin. Luonnollisesti levyt ovat salasanan takana ja näkymättöminä ulkopuolisille, mikä pienentää sanakirjahyökkäyksen uhkaa huomattavasti. (Kuutti & Rantala 2007)

Esimerkkinä SSH-palvelimen lisäksi voi yhtäaikaisesti olla Apache2- ja Samba (SMB)-palvelimet pystyssä Linux-koneella. *SMB* eli Server Message Block (nykyisin CIFS, Common Internet File System) on verkkoprotokolla, joka on tarkoitettu tiedostojen, kirjoittimien ja sarjaporttien jakamiseen verkon yli. SMB-palvelin mahdollistaa Windows-koneella olevien verkkojakojen (share) käytön, kuten ne olisivat Linux-palvelimella

sijaitsevia laitteita tai levyjä. SMBMount tapahtuu salaamattomasti ja sitä voi tämän vuoksi käyttää turvallisesti ainoastaan sisäverkossa, jossa salakuuntelu ei ole riski.

Yksittäisen levyn mounttaus verkon yli tapahtuu Linuxissa seuraavalla komentorivillä:

```
sudo mount -o smbfs username=<käyttäjä>,password=<salasana>
//<kohdekoneen IP-osoite>/<kohdekoneen haluttu
kansio/levy/tulostin> /<mounttaavan koneen kansio, johon
kohdekoneen haluttu kansio/levy/tulostin mountataan>
```

...ja sievennettynä esimerkkiarvoilla:

```
sudo mount -o smbfs username=tapio,password=makkara
//192.168.0.2/C$ levyC
```

Koska salasana näkyy tällöin avoimesti komentorivillä ja kyseisen komennon kirjoittaminen on työlästä joka kerta, on hyvä hoitaa mounttaus automaattisesti.

Asian helpottamiseksi voidaan luoda salasanatiedosto *htpasswd*-sovellusta käyttäen. Htpasswd luo tiedoston, jossa selkokielisenä näkyy käyttäjä nimi ja salasanan tiiviste. Haluttu salausalgoritmi voidaan valita muutamasta vaihtoehdosta, esimerkiksi MD5-salausalgoritmi.

Lisätään mount-syntaksi käynnistyksen yhteydessä tapahtuviin laitelisäyksiin:

```
sudo nano /etc/fstab
```

Lisätään fstab-tiedostoon rivit:

```
//<kohdekoneen IP>/<kohdekansio/laite> /<mountattaavan
koneen kansio kohdekansiolle/laitteelle> smbfs (mountattava
tiedostojärjestelmä) credentials=<htpasswd-sovelluksella
luodun salasanatiedoston path> 0 0 (kaksi viimeistä nollaa
```

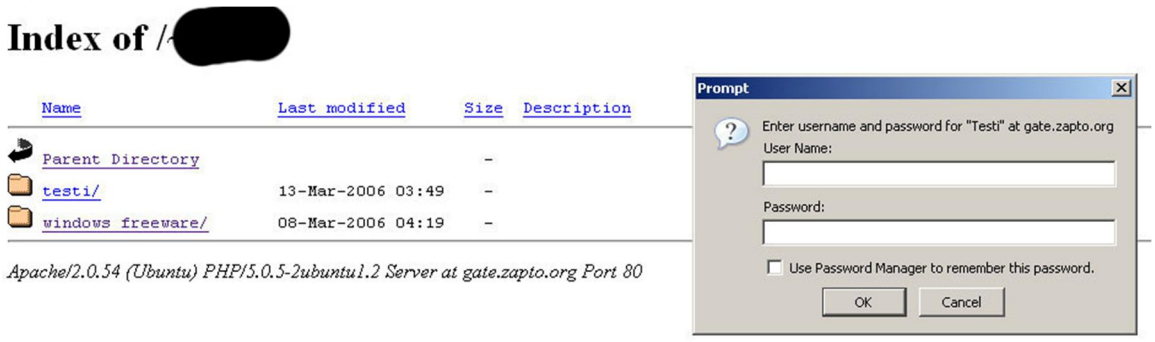
ovat dump- ja pass-parametrien arvot - lisätietoa näistä komennolla man fstab)

...ja sievennettynä esimerkkiarvoilla:

```
//192.168.0.2/C$ /home/tapio/public_html/levyC smbfs
credentials=/home/tapio/salasana.tiedosto 0 0
```

Näin halutut verkkoresurssit saadaan mountattua Linux-palvelimelle käynnistyksen yhteydessä. Koska mounttaukset voidaan tehdä käyttäjien omiin kansioihin, eivät kaikki käyttäjät pääse käsiksi kaikkiin kansioihin edes suoralla SSH-yhteydellä Linux-palvelimeen. Esimerkiksi kuviteltu käyttäjä Jussi voidaan estää pääsemästä /home/tapio-kansioon.

Koska mountatut levyt löytyvät *public_html*-kansiosta, joka todellisuudessa on virtuaalikansio, jolla Web-palvelin (Apache2) määrittelee käyttäjien www-sivut, näkyvät levyt Internetiin *.htaccess*-tiedostoissa määriteltyjen sääntöjen mukaisesti. .htaccess-tiedostossa määritellään kansiot näkymättömiksi ja vaaditaan oikea käyttäjätunnus & salasana, jotta levyihin päästään verkon yli www-sivujen läpi käsiksi.



Kuva 4. Oman Linux-käyttäjäni näkymä Internetin läpi.

Kuvassa 4 nähdään, kuinka yhteys on otettu julkisen verkon yli web-palvelimelle, oman käyttäjäni webbisivuille. Kirjautumisruutu hyppää käyttäjälle, kun .htaccess-tiedostossa on määritykset 'oikein' ja käyttäjä antaa oikean URLin, jossa mountattu levy sijaitsee.

Esimerkiksi:

base.yy.org/~tapio/levyC

Kuvassa 5 näkyy työpöytäni kuvankaappaus, kuinka kirjautuminen on suoritettu onnistuneesti ja mountattu levykohde saadaan näkymään.

Index of /[redacted]

Name	Last modified	Size	Description
Parent Directory		-	
AUTOEXEC.BAT	23-Nov-2005 19:52	0	
AVG7QT.DAT	24-Nov-2005 08:00	12M	
CONFIG.SYS	23-Nov-2005 19:52	0	
Documents/	20-Dec-2005 21:27	-	
IO.SYS	23-Nov-2005 19:52	0	
MISC/	14-Jan-2006 12:10	-	
MP3/	13-Mar-2006 19:26	-	
MSDOS.SYS	23-Nov-2005 19:52	0	
MSOCache/	27-May-2005 15:21	-	
Movies/	01-Mar-2006 22:00	-	
NTDETECT.COM	04-Aug-2004 05:38	46K	
Quickies/	13-Mar-2006 06:29	-	
RECYCLER/	23-Nov-2005 20:18	-	
Software/	12-Apr-2005 03:50	-	
System Volume Inform..>	23-Nov-2005 20:00	-	
boot.ini	11-Feb-2006 20:52	211	
memory.txt	01-Mar-2006 16:08	458	
msdownld.tmp/	07-May-2005 03:50	-	
ntldr	04-Aug-2004 05:59	244K	
xml2.txt	04-Feb-2006 20:48	26	

Apache/2.0.54 (Ubuntu) PHP/5.0.5-2ubuntu1.2 Server at gate.zapto.org Port 80

Kuva 5. Oma C-levynäkymä kirjautumisen jälkeen.

2.3 Merkkipohjaisen etähallinnan edut ja haitat

Merkkipohjaisesta etähallinnasta on valtavasti hyötyä monessa tilanteessa. Käyttäjät pystyvät esimerkiksi käyttämään turvallisesti yrityksen luottamuksellisia tai salaisia tietoja mistä tahansa, missä heillä on nettiyhteys. Käyttäjät pystyvät lisäksi muokkaamaan kotisivujaan ja siirtämään tiedostoja kaksisuuntaisesti palvelimen ja palvelimelle mountattujen levyjen välillä, omaa etäyhteyskonetta unohtamatta.

Vaikka tiedonsiirto on suojattua SSH:lla, on mahdollista, että etäkone itsessään sisältää esimerkiksi *keyboardloggerin* eli sovelluksen, joka tallentaa näppäinpainallukset. Näin ulkopuolinen voi saada käsiinsä salasanat ja päästä käsiksi Linux-palvelimeen ja myös sisäverkkoon. Tällöin murtautuja käyttää olemassa olevaa käyttäjätunnusta ja murtautumisen havainnointi on hyvin vaikeaa. (Kuutti & Rantala 2007.)

Muuttuvalla salasanalistalla (haaste-vaste-menetelmä) pystytään edellä mainittu ongelma kiertämään, mutta sen toteuttaminen on vaikeampaa. Käytännössä aktiivisella etäkoneen virus-, trojalais- ja spywareskannauksilla keyboardloggerit voidaan välttää. (Kuutti & Rantala 2007.)

2.4 Asentaminen, käytettävyys ja kustannukset

Linux-ympäristössä suojatun etähallintaympäristön luonti on hyvin helppoa. Kustannuksia ei tule lisensseistä ollenkaan. Ohjeistusta löytyy netistä valtavasti. Ohjeita löytyy myös monentasoista – aina peruskäyttäjästä ohjelmistokehittäjiin saakka. Windows-ympäristössä CygWinin OpenSSH tarjoaa vastaavan ilmaisen SSH-ympäristön. CygWin kuitenkin emuloi Linux-ympäristöä ja asentaminen on huomattavasti hankalampaa kuin Linuxiin. CygWinin komentotulkkiemulointi ei kuitenkaan vastaa ominaisuuksiltaan Linuxin oikeaa komentotulkkia. (Kuutti & Rantala 2007.)

Windows-ympäristössä verkkoresurssien jakaminen vaatii käytännössä Active Directoryn taakseen ja toteuttaminen on huomattavasti kömpelömpää ja työläämpää. Koska Active Directoryä ei ole normaaleissa Windows-versioissa, vaan ainoastaan palvelinversioissa, tulee vähintään yhden koneen olla erillinen palvelinkone.

Lisenssikustannukset nousevat ja normaalisti palvelinkoneita ei anneta kenenkään käyttäjän normaaliin käyttöön. Linuxissa jokaisesta työasemasta voidaan halutessa tehdä palvelin kustannuksitta.

3 Linux-palvelimen graafinen etäkäyttö

Tässä osiossa tutkitaan Linux-palvelimen etäkäyttöä graafisesti. Palvelin tarkoittaa tässä tapauksessa mitä tahansa Linux-konetta, joka toimii graafisen etäkäytön kohteena. Linux-koneesta on tehtävissä kohtuullisen helposti etäkäytettävä työasema. Käyttäjän vaatimuksista riippuu, tarvitseeko hän graafisen etäkäyttöympäristön vai riittääkö kenties tekstipohjainen etäkäyttö.

Linuxissa on Unix-käyttöjärjestelmästä periytyvä komentopohjainen tila. Kuten edellisessä kappaleessa tuli ilmi, Unix-pohjaista konetta voidaan hallita täysin tekstipohjaisestikin komentotulkin avulla. Nykyään graafiset sovellukset ovat yleistyneet ja kehittyneet, jolloin joissain tapauksissa osoittautuu myös graafinen etäkäyttö hyödylliseksi. Graafisen etäkäytön huono puoli on se, että se vaatii asiakaskoneelta ja palvelinkoneelta enemmän tehoa ja resursseja ja näin ollen kuormittaa myös tietoverkkoa. Tosin graafisen etäkäytön myötä saadaan esille juuri graafinen ympäristö, joka mahdollistaa tarkan graafisen datan esittämisen ja manipulaation etäyhteyksien kautta. (Kuutti & Rantala 2007.)

3.1 Graafisen etäkäytön käyttökohteita

Linux-palvelimen graafiselle etäkäytölle on vaikeampi keksiä käyttökohteita yksityisellä kuin yritystaholla. Yksityisellä taholla käyttökohteita varmasti löytyy niitäkin. Käyttäjä voi esimerkiksi olla vieras Unix- ja Linux-komentojen kanssa, jolloin hän saattaa mieluimmin asentaa itselleen graafisen etäkäyttöpalvelimen. Käyttäjä saattaa myös haluta käyttää joitain graafisen ympäristön erityissovelluksia, joita ei

muuten merkkipohjaisesti voi esittää. Tällaisia kohteita voisi olla kuvien käsittely, videokuvan lähetys ja niin edelleen. (Kuutti & Rantala 2007.)

Selvästi enemmän käyttökohteita löytyy yrityspuolelta, jossa graafinen etäkäyttö on usein käytössä yhtenä ratkaisuna. Yrityspuolella graafista etäkäyttöä käyttää tekninen tuki hoitaessaan työntekijöiden tietokoneongelmia. Tämä on kätevää, sillä tukihenkilö voi ottaa graafisen etäyhteyden omalta koneeltaan käyttäjän ongelmalliseen koneeseen ja käyttää sitä aivan kuin tukihenkilö käyttäisi itse konetta paikan päällä. Tosin verkkoliikenteen ongelmat ovat yleensä sen laatuisia, jotka vaativat tukihenkilön käynnin paikan päällä. Graafisella etäkäytöllä voidaan kuitenkin parantaa teknisen tuen työtehoa, sillä turhaa ajan kulutusta välimatkojen taittamiseen voidaan vähentää. (Kuutti & Rantala 2007.)

Yksi käytetty sovellus on X-ikkunointijärjestelmä, jota voidaan käyttää etähallinnassa ja -työskentelyssä. Tämä aikaisemmin vakituisena työmuotona suosiossa ollut järjestelmä on jäänyt hieman taka-alalle tai muuttanut muotoaan. Nykyään käyttäjille pyritään sovellusten tehon syönnin takia tarjoamaan omat työasemat, joissa jokaisessa on oma kiintolevy ja suoritin. X-ikkunointijärjestelmä voidaan kuitenkin toteuttaa niin, että käyttäjät käyttävät päätettä, johon on asennettu vain yksi ohjelma. Tällä ohjelmalla saadaan yhteys X-palvelimeen, joka tarjoaa graafisen työpöytäympäristön. (Kuutti & Rantala 2007.)

X-päätteissä tulee siis olla jonkin tasoinen grafiikkanäyttö ja ikkunanhallintaohjelma (X-manager). X-manager hoitaa päätekoneen ikkunoiden vaihtamisen ja niiden ulkonäön. X-ikkunointijärjestelmä onkin kätevä siitä, että vanhaksi käyneet päätekoneet toimivat hyvin X-päätteinä. Nykyaikainen työasema pystyy X-palvelinkoneena, käytöstä riippuen palvelemaan jopa 10-20 X-päätettä. Suuremmilla keskustietokoneilla luku on selvästi suurempi. (Kuutti & Rantala 2007.)

Suurin hyöty X-ikkunointijärjestelmässä lienee se, että ylläpito kohdistuu vain keskustietokoneeseen. Myös lisää suoritustehoa haluttaessa päivitys tehdään vain keskustietokoneisiin ja näin ollen päätetietokoneisiin ei tarvitse koskea. X-ikkunointi voidaan toteuttaa Linux-käyttöjärjestelmällä kohtuullisen helposti. Samalla saadaan käyttöön vapaan lähdekoodin tehokkaat työkalut toimistokäyttöön hyvin pienillä kus-

tannuksilla. Joskus voidaan tarvita myös suuren keskuskoneen raakaa laskutehoa, jota tarvitaan esimerkiksi 3D-mallinnuksessa ja raskaissa laskutehtävissä. (Kuutti & Rantala 2007.)

Keskustietokone pystyy suorittamaan tällaisen operaation huomattavasti nopeammin kuin tavallinen työasema. Näin käyttäjälle voidaan toimittaa operaation tulos nopeammin kuin pelkällä työasemalla tehdessä. Ikkunointijärjestelmän käyttöönotto ei välttämättä vaadi edes päätekoneen nykyisen käyttöjärjestelmän poistamista, vaan X-manager ohjelma voidaan käynnistää esimerkiksi käynnistyvältä levykkeeltä tai CD-levyltä (Kuutti & Rantala 2007).

X-ikkunointijärjestelmä vaatii hyvin toimiakseen tehokkaan palvelinkoneen ja nopeat siirtotiet datalle. Verkon ja palvelimien tulee siis kestää hyvin kuormitusta, jotta työskentely tällä tavalla olisi sujuvaa. Keskitetystä toiminnasta voi olla myös haittaa. Varmuuskopiointiin tulee kiinnittää suurta huomiota, sillä jos palvelimeen tulee vikaa, on mahdollista että suuri määrä tietoa katoaa. Myös yhden palvelimen toimintakunnottomuus vaikuttaa useisiin päätekoneisiin, ellei vikatilanteiden hoitoa ole suunniteltu kunnolla. (Kuutti & Rantala 2007.)

3.2 Graafiset etäkäyttöprotokollat

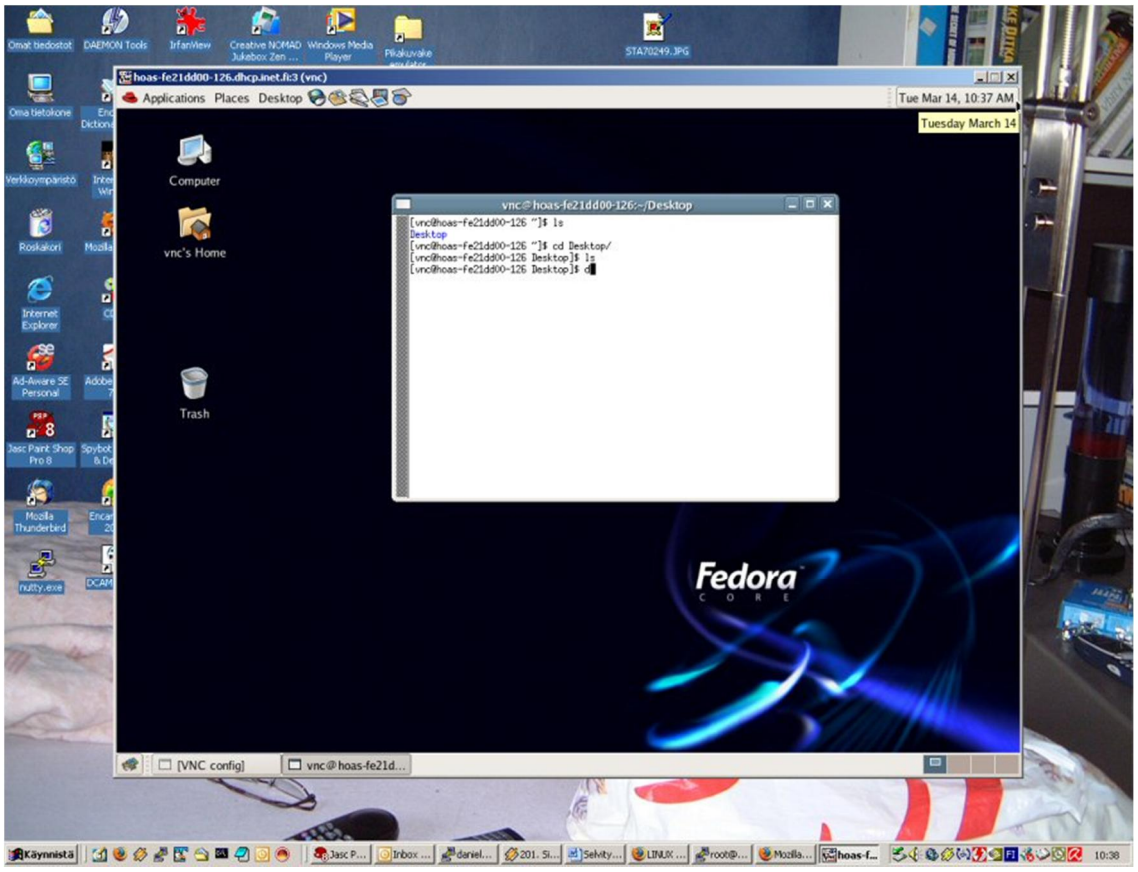
VNC on selvästi eniten käytetty ja dokumentoitu graafinen etäkäyttöprotokolla. Tämän takia Linux-palvelimen graafisen etäkäytön osiossa keskitytään pitkälti tähän tekniikkaan. Linux-palvelimille löytyy myös joitain muita sovelluksia, kuten SSH- ja Java-ratkaisuita. Tärkeimmistä ratkaisuista yritetään tuoda pääpiirteet esille, mutta eniten käyttökohteita ja sanottavaa löytyy kuitenkin siis VNC:n parista. Tässä dokumentissa käydään myös pintapuolisesti läpi VNC-palvelimen pystytys. (VNC Books LLC 2010.)

Virtual Network Computing

Virtual Network Computing eli VNC on varmasti yksi suosituimmista puhtaasti graafisista etäkäyttösovelluksista. Vuonna 1995 sai VNC alkunsa Olivetti research lab-tutkimuskeskuksessa. Kaksi vuotta myöhemmin myös Oracle kiinnostui hankkeesta rahoittaen keskusta. Vuonna 1999 AT&T osti laboratorion, mutta sen toiminta loppui vuonna 2002. Alkuperäinen VNC julkaistiin vapaan lähdekoodin GNU-lisenssin alaisena, josta muodostui useita VNC-pohjaisia järjestelmiä. Näitä ovat muun muassa RealVNC, TightVNC, Ultr@VNC, TridiaVNC ja ZVNC. (VNC Books LLC 2010.)

VNC on ikkunointijärjestelmä, jossa toimii asiakaskone ja palvelin. Palvelinkone tarjoaa käyttäjälle käyttäjäprofiilin mukaisen työpöydän, johon käyttäjä ottaa yhteyttä VNC-asiakasohjelmalla. Tällä tavoin voidaan toteuttaa myös X-ikkunointijärjestelmä, mutta yleensä VNC-asiakaskoneena toimii tavallinen työasema omalla käyttöjärjestelmällään. Niin sanottujen ”kylmien” päätteiden käyttö onkin siis menettänyt suosiotaan. (VNC Books LLC 2010.)

VNC:n hyvänä puolena on se, että se ei ole alustariippuvainen. Esimerkiksi Windows-asiakas voi ottaa yhteyden Linux-palvelimeen ja näin käyttää Linux-työpöytää Windowsin ”päällä”, kuten kuva 6 osoittaa. Samoin voidaan Linux-asiakkaalla ottaa yhteys Windows-palvelimeen. VNC-asiakas- ja palvelinohjelmia löytyykin useille alustoille, kuten Linux, BDS, MS Windows ja Mac OS X. Kaikille käyttöjärjestelmille ei kuitenkaan ole valmistettu tarvittavia ohjaimia.



Kuva 6. Yhteys Windows-koneelta Linux-VNC –palvelimelle.

VNC ja tietoturva

VNC:ssä tulee ottaa huomioon se, että ilman erillisiä toimenpiteitä VNC-liikenne palvelimen ja asiakkaan välillä on täysin salaamatonta. Tämä tarkoittaa sitä, että liikenne on hyvin helposti salakuunneltavissa. Salaamatonta liikennettä ei tulisikaan käyttää kuin korkeintaan kokeilumielessä, tällöinkin on syytä katsoa, ettei esimerkiksi arkaluontoisia salasanoja kulje turvattoman verkon ylitse.

Turvallisen VNC:stä saa kohtuullisen helposti salaamalla VNC-liikenteen jollain verkkoliikenteen salausprotokollalla. Varsinkin Linux-ympäristössä suosituin tapa tähän on tunneloida VNC-liikenne kulkemaan SSH-putkessa. Kuten aikaisemmin on käynyt ilmi, SSH (Secure Shell) on vahva salausprotokolla, joka on hyvin joustava ja sille löytyy monia sovelluskohteita. (VNC Books LLC 2010.)

VNC-palvelimen asennus

VNC-palvelimen asennus Linux-koneessa on kohtuullisen helppoa. Monessa jakeluversiossa VNC-palvelinohjelmisto tulee valmiiksi käyttöjärjestelmän mukana. Jos VNC-palvelinohjelmistoa ei koneelta löydy, sen asentaminen tapahtuu kätevästi Debian-pohjaisissa järjestelmissä komennolla *apt-get install vncserver* tai RedHat-pohjaisissa versioissa komennolla *yum install vncserver*. Komennot täytyy tietenkin antaa käyttäjällä, jolla on oikeudet asentaa ohjelmia. Jos palvelinohjelmaa ei jostain syystä voida asentaa paketinhallinnan kautta, se voidaan kuitenkin ladata Internetistä, tarvittaessa kääntää lähdekoodista ja asentaa palvelinkoneelle normaaliin tapaan.

Kun VNC-palvelin on asennettu, se käynnistetään komennolla */etc/init.d/./vncserver start* . Käytössä tulee tässäkin olla siis esimerkiksi root-oikeudet, jolla komento saadaan suorittaa. Tämän jälkeen voidaan luoda oma käyttäjä VNC-palvelua varten. Jos halutaan luoda käyttäjä nimeltä vnc, tehdään se root-oikeuksilla komennolla *adduser vnc,* ja tälle luodaan unix-salasana komennolla *passwd vnc,* ellei sitä luomisen yhteydessä kysytä.

Nyt käyttäjällä voidaan kirjautua normaalisti sisään, avata käyttäjällä terminaali ja antaa komento *vncserver*. VNC-palvelin lähtee käyntiin, ja yhteyksiä on mahdollista muodostaa VNC-asiakasohjelmalla VNC-palvelimen ilmoittamaan osoitteeseen.

Yksi käyttäjä voi pystyttää useamman ”näytön”, jota hän palvelee. Ensimmäisellä kerralla kun *vncserver*-komento annetaan, VNC-palvelin pystyttää oletuksena näytön 1. Kun komento annetaan toisen kerran, pystytetään näyttö 2 jne. Näytöille voidaan määrittää myös omia numeroita ja aliaksia tarpeen mukaan. Normaalisti VNC-näyttöjä muodostetaan portteihin alkaen luvusta 5901, joka tarkoittaa näyttöä 1. Portille 5902 tulee näyttö 2 jne. Palvelinkoneen palomuurista pitää sallia siis tarvittavat portit, jotta yhteydenotto onnistuisi. VNC-asiakkaan päässä yhteys otetaan perinteisesti seuraavanlaiseen osoitteeseen: *palvelinkoneen-ip:näytön-numero*. Esimerkiksi 123.123.123.123:1, haluttaessa ottaa yhteyden näyttöön 1.

Näin yhteys saadaan kohtalaisen helposti VNC-palvelimeen. Jotta palvelimen käyttö olisi mukavaa, voidaan palvelimeen asettaa haluttuja asetuksia. Näitä voi olla valmiit

ohjelmat, joita käynnistetään yhteyden muodostamisen yhteydessä, käytettävät resoluutiot, värisyvyydet ja niin edelleen.

Jotta VNC olisi turvallinen, se tulee vielä tunneloida SSH-putkeen. Tunnelointi hoituu seuraavan tyylisellä käskyllä:

```
ssh -L 5901:palvelimen-ip:5903 -l <käyttäjätunnus>
palvelimen-ip
```

SSH-ohjelmalla luodaan siis port-forward -tunnelointi parametrilla –L. Tässä esimerkissä portissa 5903 pyörii näyttö, joka tunneloidaan porttiin 5901. Nyt otetaan yhteys näyttöön 1, joka määräytyy tunneloidun portin perusteella. Näin VNC-yhteydestä saadaan salattu.

3.3 SSH:n graafiset ominaisuudet

Yleensä SSH:ta käytetään merkkipohjaisen yhteyden muodostamiseen. Windows-koneilla voi ottaa myös yhteyden Linux-SSH –palvelimiin, mutta Windows-koneissa eivät toimi komentotulkin parametrit niin kuin Linux-koneelta toiselle. Haluttaessa käyttää SSH:n graafisia ominaisuuksia otetaan yhteys Linuxin komentotulkista käsin Linux SSH-palvelimeen. SSH-käskyllä voidaan käynnistää haluttu ohjelma etäkoneelta SSH-tunnelin ylitse graafisesti etäkoneelle. Tätä ominaisuutta kutsutaan myös nimellä X-forward. (Stahnke 2005.)

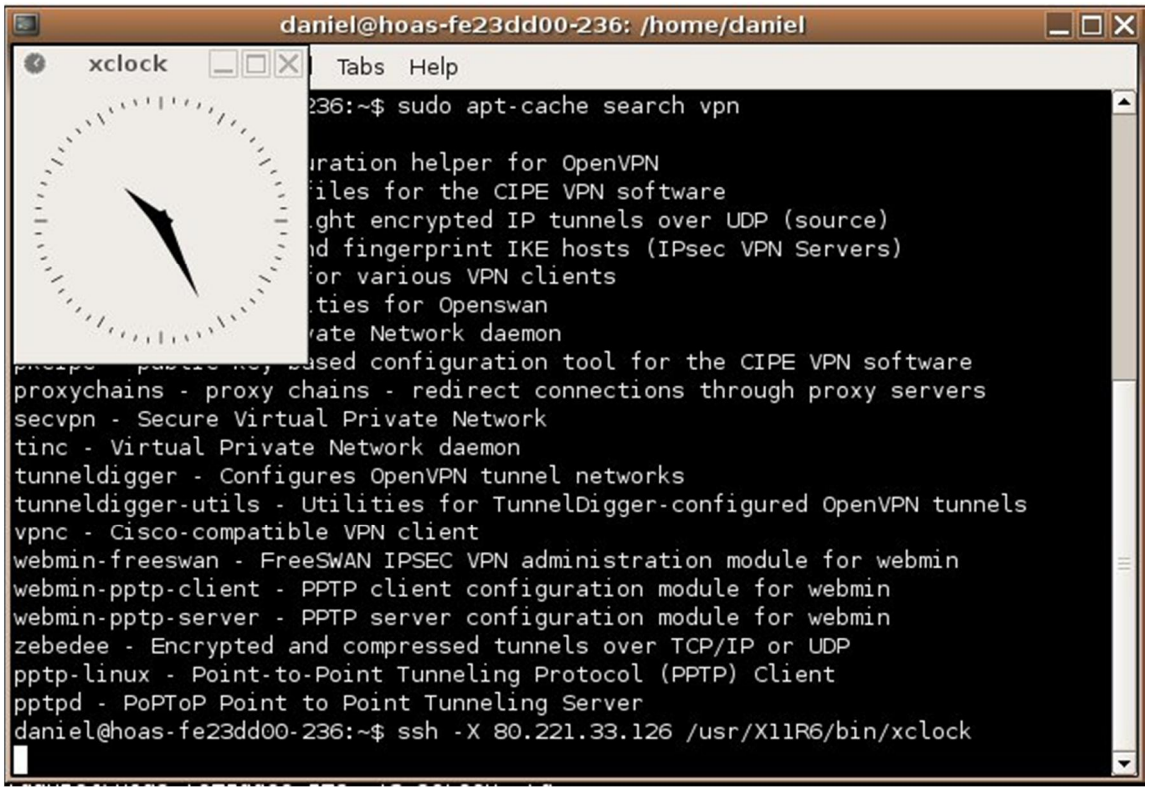
Kuten kuvassa 7 näytetään, komento tapahtuu syntaksilla:

```
ssh -X käyttäjäl@palvelimen-ip /usr/X11R6/bin/xclock
```

Tässä asiakaskone käyttää yhdistämiseen ssh-komentoa. X- parametri kertoo ohjelmalle, että palvelimelta ajetaan graafinen sovellus. Käyttäjä@osoite yhdistää ssh-palvelimelle. Graafinen sovellus, joka ajetaan palvelimen kohdekansiosta */usr/X11/bin* on ohjelma

Xclock. Kun ohjelma sammutetaan käyttäjän päässä sulkemalla ohjelma normaalisti, myös SSH-yhteys palvelimelle sulkeutuu ohjelman mukana.

Käyttäjä voi mahdollisesti löytää joitakin käyttökelpoisia käyttökohteita SSH:n graafisille ominaisuuksille. Yleisesti ottaen ei ole havaittu SSH:n graafisille ominaisuuksille kovinkaan vakavia ja tärkeitä käyttökohteita.



Kuva 7. Graafisesti ajettu ohjelma SSH:n yli.

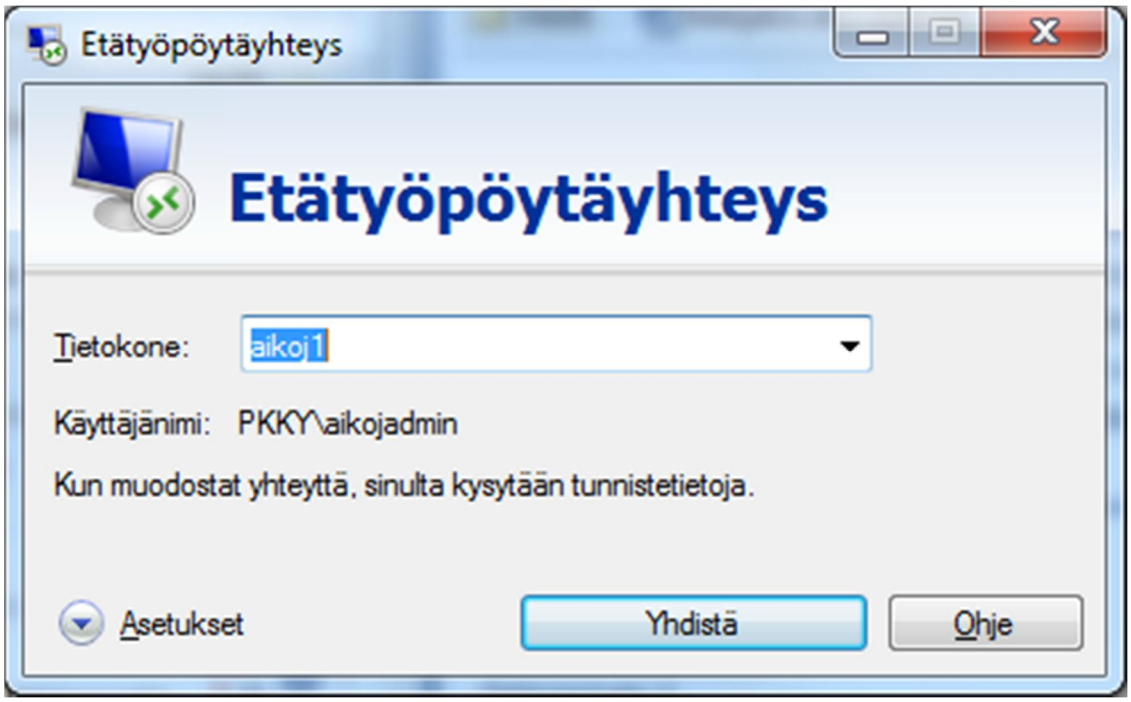
4 Etähallinta Windows-ympäristössä

Tämä osio tarkastelee yleisimpiä Microsoft Windows -tuoteperheen etähallinta-menetelmiä ja etähallintaan liittyviä ohjelmistoja. Windowsissa itsessään on kaksi eri työkalua etäkäyttön mahdollistamiseen. Ensimmäinen näistä on Remote Assistance. Käytännössä tämä on tapa kutsua toinen käyttäjä neuvomaan tietokoneen ongelmien kanssa. (Minasi 2001.)

Toinen tapa taas on ”täysiverinen” etäyhteysmahdollisuus. Sen nimi on Remote Desktop Connection. Se päästää käyttäjän käyttämään etähallittavaa tietokonetta Internetin yli kuin hän käyttäisi omaa tietokonettaan. Tälle yhteystavalle on vaatimuksena se, että etähallittavasta koneesta löytyy Windows XP Professional -käyttöjärjestelmä tai uudempi yritysversio kuten Windows 7 Enterprise. Yhteyden ottajalla voi olla käytössään Windows 95 tai uudempi käyttöjärjestelmä, johon on asennettu etätyöpöytäyhteyden asiakasohjelmisto. (Minasi 2001.)

Yhteys lähiverkossa

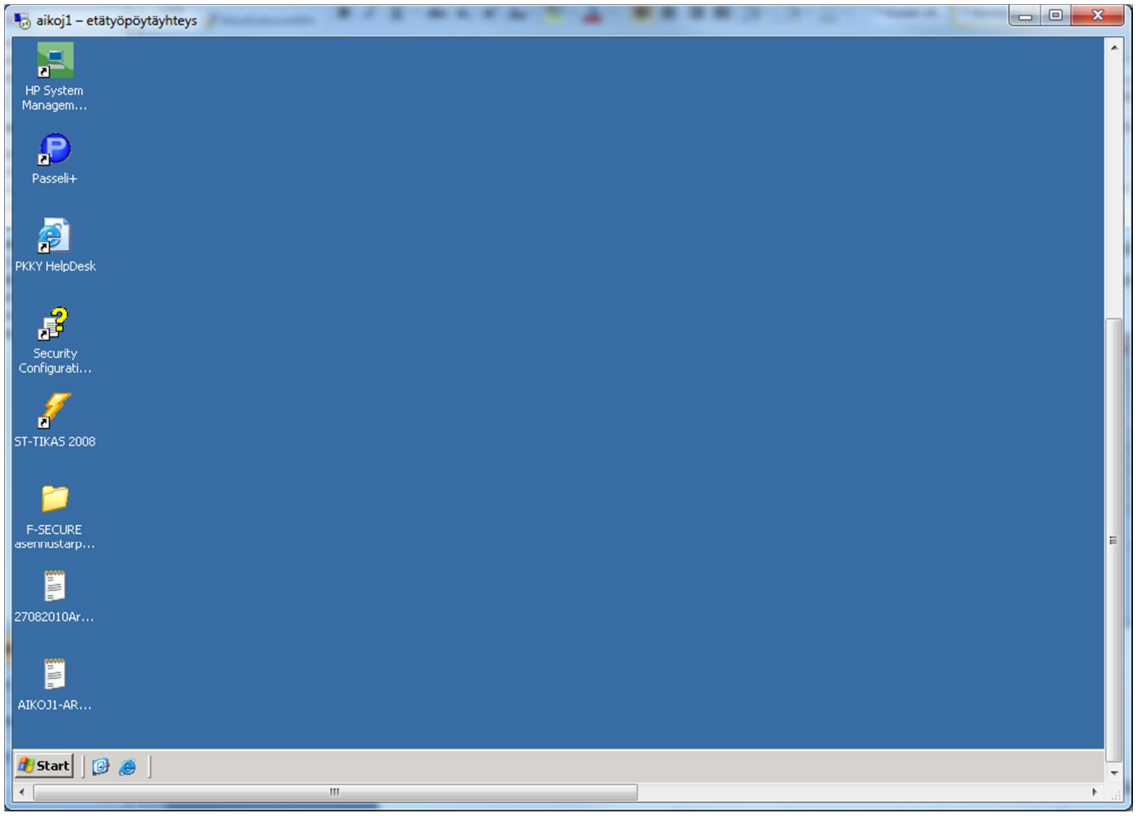
Teoriassa etäyhteyden muodostaminen onnistuu lähiverkon alueelle varsin helposti. Käynnistetään Käynnistä-valikosta löytyvä Etätyöpöytäyhteys-ohjelma, valitaan listasta tietokone ja kirjoitetaan käyttäjätunnus. Kuvassa 8 on näkymä yhteydenotto vaiheesta.



Kuva 8. Yhteyden muodostaminen.

Käytännössä ohjelma ei löydä lähiverkosta koneita kunnolla, vaan useimmiten koneen nimen joutuu syöttämään käsin. Jos kaikki muut asetukset ovat kunnossa, niin käyttäjä pääsee nyt käyttämään kohdetietokonetta kuin omaansa. Kuvassa 9 on näkymä etä-

yhteyden muodostuttua palvelimelle. Kohde koneen näyttö pimenee siksi aikaa, kun joku etäkäyttää konetta.



Kuva 9. Yhteys muodostettu palvelimelle.

Yhteys lähiverkon ulkopuolelta

Etäyhteys lähiverkon kautta on kätevä esimerkiksi yritysten sisällä tai sellaisissa asunnoissa, joissa tietokoneita on useampia. Etätyöpöytäkäyttö on tarkoitettu kuitenkin pääasiallisesti sellaisille yhteyksille, jotka tulevat Internetin yli ja käyttäjä pääsee käyttämään konettaan tai jonkun toisen konetta mistä päin maailmaa tahansa. Jos Internet-yhteyden päässä on vain yksi kone, niin silloin etäyhteyden muodostaminen on teoriassa helppoa. Tarvitaan vain etähallittavan koneen IP-osoite, jonka voi sitten syöttää yhteysohjelmaan. Jos yhteyden tarvitsemat portit ovat auki ja palomuuri sallii niiden käyttämisen, pitäisi yhteyden muodostua aivan samoin kuin lähiverkon ylikin.

Ongelmia tulee, jos Internet-yhteyden päässä onkin toinen lähiverkko, jossa yhteys on jaettu kahdelle tai useammalle koneelle. Tällöin yhteys tarvitsee nettiä jakavan laitteen

asetusten konfigurointia, tai palomuurille pitää määritellä, mille lähiverkon koneelle yhteyspyynnöt välitetään. Nämä asetukset löytyvät yleensä Internet-yhteyttä jakavan laitteen asetuksista, NAT-välilehden alta, osoitteenmuunnosasetukset. Asetuksia ei kuitenkaan kannata mennä ”virittelemään” ennen kuin on täysin varma, että ohjelma tarvitsee niitä.

Etäyhteyden muodostamiseen Internetin yli tarvitaan tietokoneen ulkoinen IP-osoite. Jos kohdetietokone on jonkin sisäverkon ”jäsen”, tarvitaan myös koneen sisäinen IP-osoite. Internet-liittymän ulkoinen IP-osoite näkyy koko Internetin alueelle, siinä missä sisäinen IP-osoite paljastaa, mistä lähiverkon koneesta on kysymys. (Minasi 2001.)

4.1 Remote Assistance

Ensimmäinen asia, joka täytyy tehdä, kun aletaan käyttää Windowsin omia työkaluja, on sallia yhteyksien muodostaminen. Tämä tapahtuu avaamalla Järjestelmäikkuna ja valitsemalla Etäkäyttö-välilehti. Tältä välilehdeltä klikataan päälle mahdollisuus lähettää etätukipyyntöjä sekä vastaanottaa etätyöpöytäyhteyksiä. (Minasi 2001.)

Kun etätukipyyntöjen lähettäminen on sallittu järjestelmäasetusten puolelta, voi pyyntöjä lähettää valitsemalla käynnistä-valikosta löytyvän Etätuki-sovelluksen. Tästä ohjelmasta löytyy linkki ”kutsu toinen käyttäjä auttamaan sinua”. Tätä painamalla pääsee sivulle joka mahdollistaa etätukipyyntöjen lähettämisen sähköpostitse tai Messenger ohjelmalla. Jos kutsu ei jostain syystä lähde eteenpäin, voi sen myös tallettaa tiedostoksi ja lähettää ”manuaalisesti” vastaanottajalle. (Minasi 2001.)

Kun vastaanottaja hyväksyy etätukipyynnön, päästään varsinaisen etäyhteyden pariin. Tukipyynnön vastaanottaja pääsee nyt tarkastelemaan lähettäjän työpöytää ja keskustelemaan hänen kanssaan ongelmasta. Tukipyynnön vastaanottaja voi myös ottaa lähettäjän koneen hallintaansa ja täten päästä korjaamaan mahdollisia ongelmia syvällisemminkin (Minasi 2001).

4.2 Remote Desktop Connection

Etätyöpöytäyhteyden muodostaminen on hieman hankalampaa ja saattaa vaatia enemmän toimenpiteitä ennen kuin se toimii halutulla tavalla. Periaatteessa pitäisi riittää, että järjestelmän asetuksista klikkaa päälle ”Allow users to connect remotely to this computer”-ruudun, mutta käytännössä asetuksia täytyy laittaa kuntoon useamman kerran.

Etäyhteys otetaan tietylle käyttäjätunnukselle, jolle on määriteltävä salasana. Kaikilla järjestelmänvalvoja-luokkaan kuuluvilla käyttäjillä on automaattisesti oikeus kirjautua koneelle, mutta muilla käyttäjätunnuksilla lupa etäyhteyksille täytyy määritellä erikseen. Tämä tapahtuu painamalla ”Select Remote Users” -nappia järjestelmäasetusten Remote-välilehdellä (Minasi 2001).

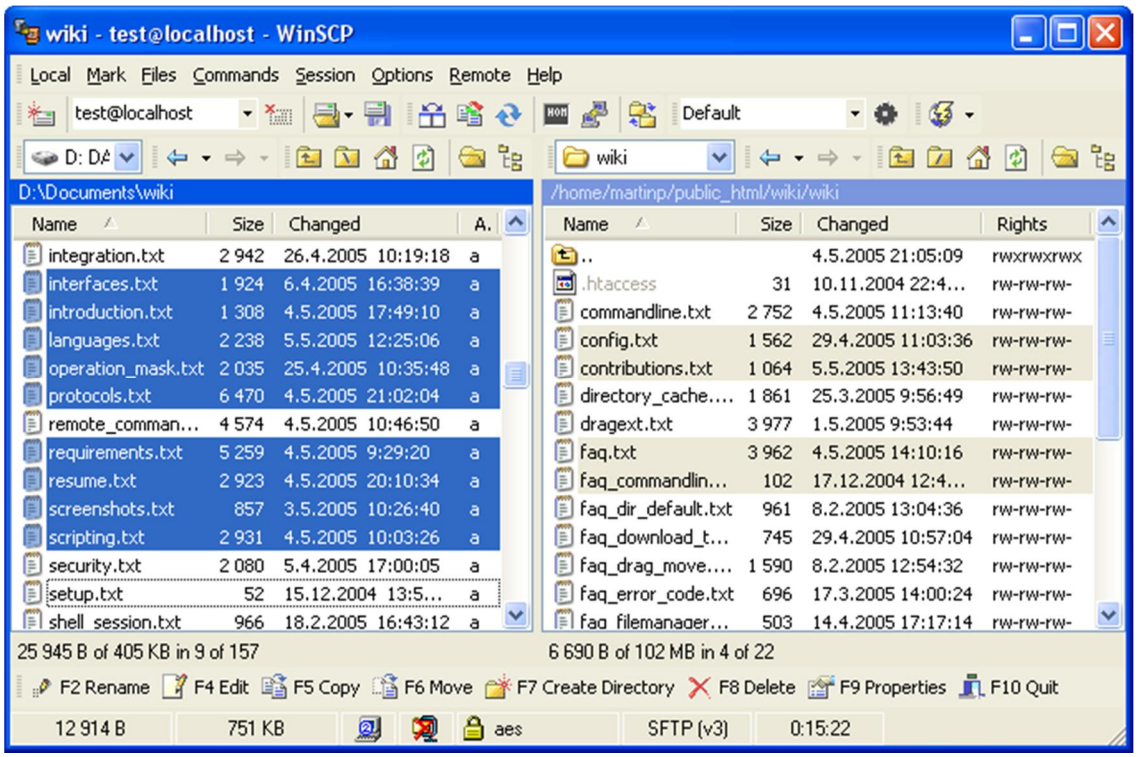
4.3 Kolmannen osapuolen etähallintaohjelmistot

Etähallintaa voi myös suorittaa kolmannen osapuolten ohjelmistoilla, jotka ovat yleensä kevyempiä kuin Windowsin omat integroidut ohjelmistot ja myös joissakin tapauksissa monipuolisempia.

WinSCP3

WinSCP3 on Windowsille suunniteltu ja toteuttu SFTP-ohjelmisto joka käyttää SSH:ta. Sen pääasiallinen tarkoitus on tiedostojen ja kansioiden siirtäminen client-koneen ja remote-koneen välillä turvallisesti. Vaikka WinSCP3 onkin graafinen etäkäyttöohjelmisto (kuva 10), on siinä mukana myös merkkipohjainen toteutus, jonka käyttöönotto vaatii pientä asetusten konfiguroimista. WinSCP3 on siis etäkäyttöön tarkoitettu suojattu resurssienhallintaohjelmisto, jossa on mukana tekstieditori.

WinSCP3 tukee SCP-protokollaa (Secure Copy Protocol) ja SFTP-protokollaa (SSH File Transfer Protocol). SFTP on näistä protokollista uudempi ja yleisemmin käytetty.



Kuva 10. WinSCP3:n graafinen ulkoasu.

RealVNC

RealVNC on itsenäinen etäkäyttöohjelma. Se on kaupallinen ja siitä on versiot niin Windowsille kuin Linuxillekin. RealVNC:n vahvuus on siinä, että se on erittäin kevyt ja helppokäyttöinen. RealVNC käyttää porttia 5900 (ja suurempia), eikä Windows ja Mac-käyttäjien tarvitse kuin avata ko. portti. Palomuuri ja NAT voivat aiheuttaa ongelmia RealVNC:tä käytettäessä. (VNC Books LLC 2010.)

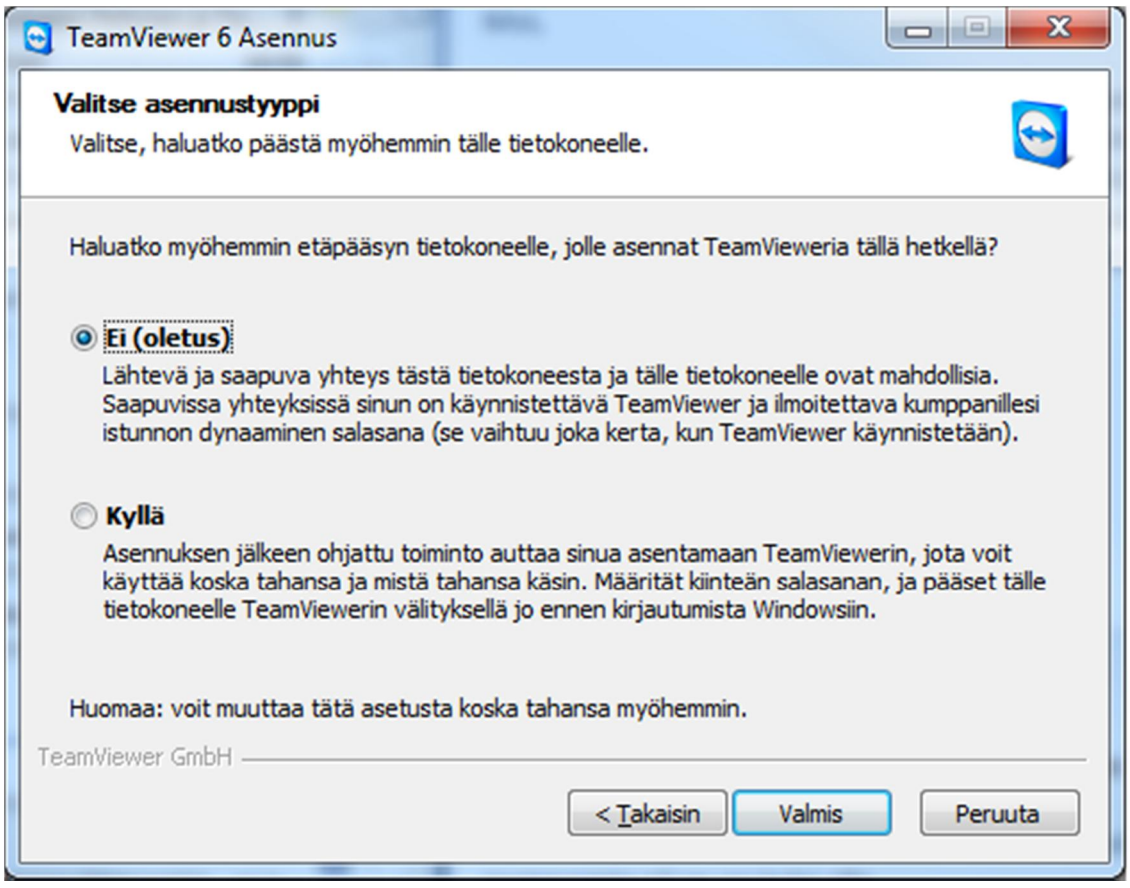
LogMeln

LogMeln on kaupallinen etäkäyttöohjelmisto. Sen vahvuus on siinä, että se ei tarvitse erillistä asiakasohjelmistoa, vaan se mahdollistaa etäyhteydet suoraan nettiselaimen kautta. Käyttö vaatii kuitenkin kirjautumisen LogMeln-palveluun.

LogMeln toimii hyvin, jos molemmat käyttäjät ovat laajakaistayhteyden takana. Koska palvelu on raskas, GPRS- ja modeemi-yhteydet ovat hitaita ja saattavat jäädä myös muodostumatta.

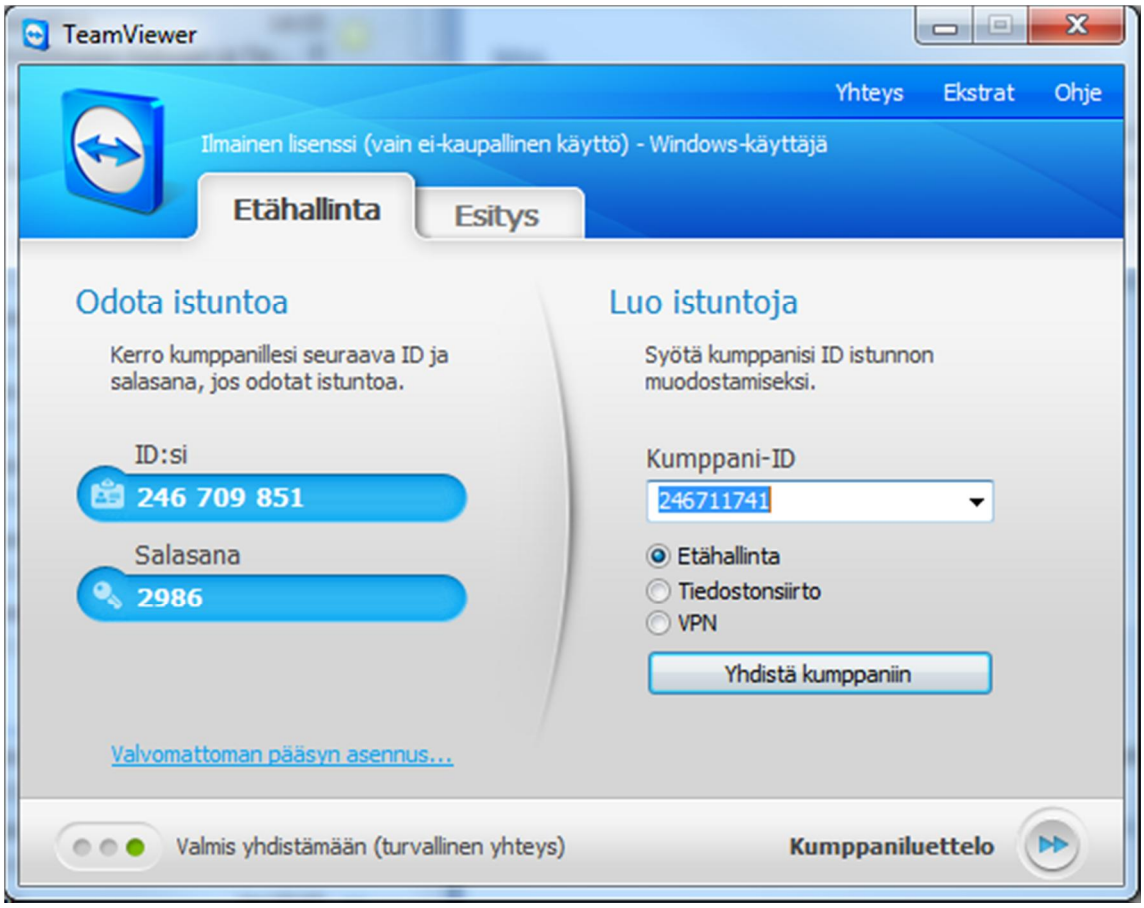
TeamViewer

TeamViewer on myös kaupallinen etäkäyttöohjelmisto. Se on kuitenkin ilmainen, mikäli ohjelmaa käyttää vain yksityiskäytössä. Ohjelma toimii myös suoraan ilman asennusta. TeamViewer -ohjelman yhteydet kulkevat suojattuja datakanavia pitkin 1024 bit RSA -avainsalausprotokollalla ja 256 bit AES -istuntosalauksella (TeamViewer 2011). TeamViewer Web Connector on vaihtoehto, jos ei haluta asentaa itse ohjelmistoa kohde koneelle. Web Connector on toteutettu HTML- ja Flash-pohjaista ratkaisua käyttäen. Kuvassa 11 TeamViewer etähallintaohjelman asennusvaihe, jossa voidaan määrittää oma salaus käyttäen kiinteää salasanaa tai vaihtoehtoisesti istunnon aikaista dynaamista salasanaa, joka on suositus ohjelmistontuottajan taholta.



Kuva 11. TeamViewer:in asennus.

Istunnon muodostamiseen tarvitaan vastaanottajan ID. Tämän jälkeen ohjelma muodostaa halutulla tavalla yhteyden etähallittavaan koneeseen. Kuvassa 12 käy ilmi käyttöliittymän malli.



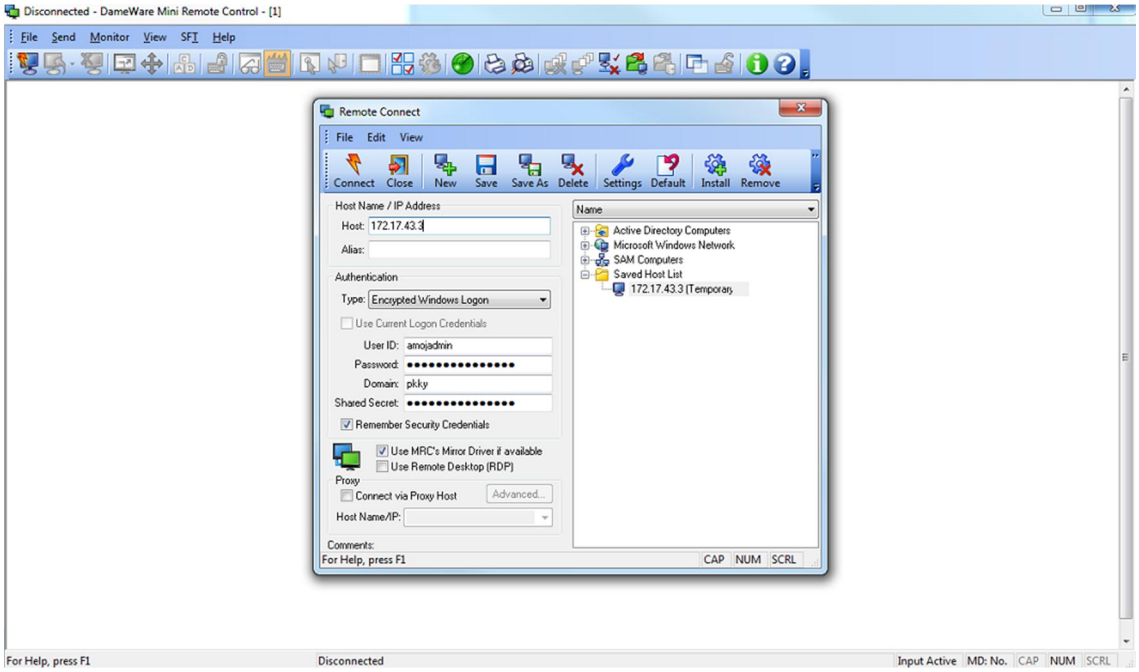
Kuva 12. Yhteyden muodostaminen TeamViewer ohjelmalla.

DameWare

DameWare on kaupallinen etähallintaohjelma, joka soveltuu Windows -palvelimien ja -työasemien etähallintaan ja järjestelmien raportointiin. DameWare -ohjelmisto sisältää monipuolisten hallintaominaisuuksien lisäksi myös DameWare Mini Remote Control -etävalvontaohjelman, jota käytetään myös yritysmaailmassa asiakasrajapinnassa työskennellessä. (DameWare 2011.)

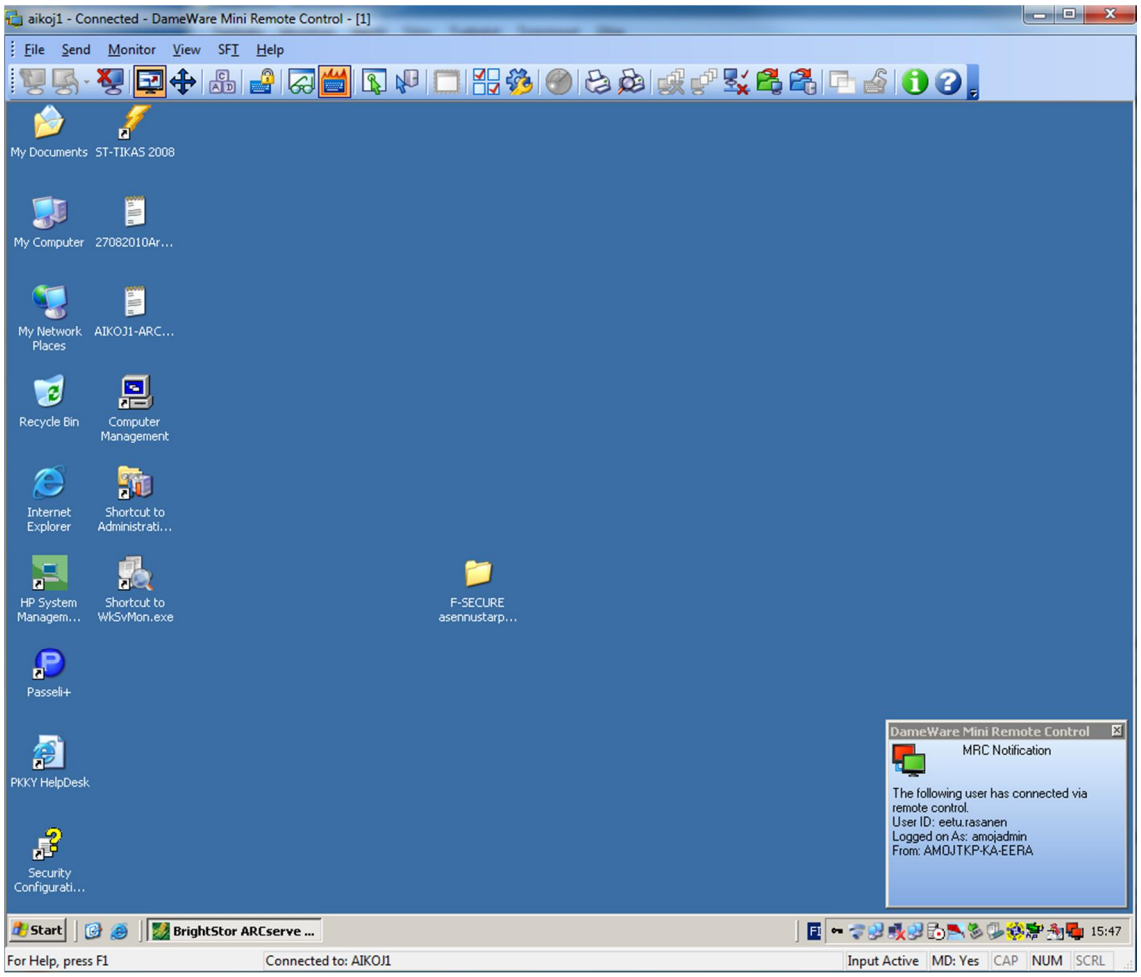
DameWare Mini Remote Control -etähallintaohjelman saa helposti asennettua Windows-työasemille etäasennuksena ilman, että työasemaa tai palvelinta täytyy uudelleenkäynnistää. Tämä helpottaa esimerkiksi teknisen tuen työtä yritysmaailmassa.

Yhteyden muodostaminen työasemaan tai palvelimeen toteutetaan suoralla ip-numerolla tai koneen nimellä. Kuvassa 12 yhteys muodostetaan ip-numerolla palvelimelle. Autentikointi-kenttään syötetään palvelimen kirjautumistiedot ja tässä tapauksessa myös toimialue.



Kuva 12. Yhteyden määrittäminen.

Kuvassa 13 on näkymä DameWare Mini Remote Control -käyttöliittymästä, kun yhteys on muodostettu palvelimelle. Oikean alareunan palkki ilmoittaa kohdekoneella tiedot etäyhteyden ottajasta.



Kuva 13. Yhteys muodostettu palvelimeen.

4.4 RDP – Remote Desktop Protocol

RDP -protokolla tarjoaa graafisen etätyöpöydän koneisiin, joissa on käytössä Microsoft Terminal Service. Windows-koneisiin voidaan ottaa etäyhteys Internetin yli RDP:tä käyttäen, kun konekohtaiset sovellusasetukset ovat kunnossa. RDP julkaistiin Windows NT 4.0:ssä, Terminal Servicen mukana (RDP 4.0), ja myöhemmin Windows 2000 Terminal Service päivitti protokollan versioon 5.0. Terminal Service kuuntelee oletusasetuksilla TCP-porttia 3389. (Minasi 2001.)

RDP sisältää seuraavat ominaisuudet:

- salakirjoitus (Encryption)
- kaistan käytön minimoiminen (Bandwitdth Reduction Features)
- vaeltava yhteyden katkaisu (Roaming Disconnect)

- leikepöydän mappaus (Clipboard Mapping)
- tulostuksen ohjaus (Print Redirection)
- virtuaaliset kanavat (Virtual Channels)
- etäkäyttö (Remote Control)
- kaistan käytön tasaus (Network Load Balancing).

RDP perustuu vanhempiin ITU T.120 -protokolliin, mutta myös laajentaa näitä. RDP on monikanavainen protokolla, joka sallii eri virtuaalikanavien käytön laitekommunikaatiolle ja datan välitykseen palvelimelta. Se myös mahdollistaa näppäimistö ja hiiridatan salakirjoittamisen. RDP tarjoaa myös laajan pohjan ja tukee jopa 64 000 virtuaalista kanavaa datan liikuttelemiseen.

Palvelin puolella RDP käyttää omia video-ajureitaan, joilla se muuttaa ruudulla näkyvän informaation Network-paketeiksi, käyttäen RDP-protokollaa ja lähettäen ne verkon yli asiakkaalle. Asiakaspuolella RDP muuttaa saadut paketit Microsoft Win32 -graafisiksi laite API-kutsuiksi. Palvelimen puolella RDP käyttää sen omia on-screen -näppäimistö- ja hiiri-ajureita jotka osaavat tulkita asiakkaalta tulleet näppäimistö- ja hiiritapahtumat.

RDP käyttää RSA Securityn RC4 -salakirjoitusta, joka on streemaava salakirjoitusmetodi ja joka on suunniteltu tehokkaasti salakirjoittamaan pieniä määriä dataa. R4C on suunniteltu turvaamaan yhteydet verkkojen ylitse. Windows 2000:sta lähtien adminit ovat saaneet päättää, kryptataanko data 56- vaiko 128-bittisella avaimella. RDP tukee monia eri tapoja minimoida kaistan käyttöä. Näihin kuuluvat datan pakkaaminen, jatkuva bittikarttojen asettaminen välimuistiin ja ”glyphien” ja osien asettaminen välimuistiin keskusmuistissa. Jatkuva bittikarttojen ”välimuistittaminen” nopeuttaa yhteyksiä huomattavasti hitailla yhteysmuodoilla.

RDP sisältää Roaming Disconnect -ominaisuuden, joka tarkoittaa sitä, että käyttäjä voi lopettaa etäkäytön, mutta hänen ei tarvitse kirjautua ulos. Kun hän ottaa uudelleen yhteyttä etäkoneeseen, on hän automaattisesti kirjautuneena järjestelmään.

Leikepöydän mappaus -toiminnolla käyttäjä voi poistaa, kopioida, leikata ja liittää tekstiä ja grafiikkaa etäkoneella ja omalla koneella toimivien ohjelmien välillä.

Tulostuksen ohjaus -toimintoa käytetään, mikäli käyttäjä haluaa ohjata tulostuksen omassa koneessa kiinni olevaan paikalliseen tulostimeen. Kummankin koneen tulee olla päällä tulostuksen aikana.

Käyttäen RDP:n virtuaalisten kanavien arkkitehtuuria, nykyisiä ohjelmistoja voidaan kartuttaa ja uusia ohjelmistoja voidaan kehittää lisäämään ominaisuuksia, jotka vaativat kommunikaatiota clientin ja terminal servicen välillä.

Etäkäyttö -toiminnon avulla käyttäjä voi tarkkailla ja ottaa käyttöönsä Terminal Service -sessioita. Jakamalla kahden Terminal Servicen datat voidaan helposti paikallistaa ja korjata mahdollisia ongelmia.

4.5 Supermatrix

Supermatrix-projekti on tuomassa etäkäyttötuotteet koti- ja pienyrityskäyttäjille ensimmäisenä maailmassa. Ongelmana tällä hetkellä on erityisesti HDTV-tason IPTV sekä pelit, jotka asettavat etäkäytön toteutukselle aikaisemmin ratkaisemattomia vaatimuksia. Supermatrix on luonut ongelmaan ratkaisun siten, että näyttöruudun tai television kuva muodostetaan palvelukeskuksen palvelimella ja siirretään käyttäjän näyttöruudulle erittäin nopealla valokuituyhteydellä kevyesti ja nopeasti kompressoituna. Käyttäjällä on vain sovitinlaatikko, joka hoitaa tietoliikennettä oheislaitteiden ja palvelimen välillä. (Supermatrix-projekti 2011.)

Supermatrix siirtää tietokoneiden hallinnoinnin pois kodeista. Näin ollen esimerkiksi eläkeläisen ei tarvitse tietää, mitkä ohjelmat saavat mennä palomuurin ohi, saatikka tietää, mikä on palomuuri. Virtuaaliympäristöt perustuvat usein käyttöjärjestelmän sijaan virtual machine monitor-ohjelmistoon kuten VMWare ESX Server tai Citrix XenServer. Yksinkertainen Supermatrix-ympäristö tulee toimimaan ilman varsinaista virtualisoitua käyttöjärjestelmäympäristöä – ainoastaan käyttäjän asetukset ja tiedostot tallentuvat virtuaaliseen työtilaan. Edistyneimmille käyttäjille on kuitenkin luvassa suosituimpia virtualisoituja käyttöjärjestelmäympäristöjä, kuten Windows 7 tai Linux. (Supermatrix-projekti 2011.)

Valitettavasti Supermatrixin käyttö rajoittuu tällä hetkellä vain projektin omaan valokuituverkkoon, sillä Internetverkko on liian hidas ja ruuhkainen välittämään tietokoneen työpöydän kuvaa. Suunnitteilla on kuitenkin, että käyttäjä pääsisi omaan Supermatrix-tietokoneympäristönsä tietoihin läppärillä tai älypuhelimella. (Supermatrix-projekti 2011.)

5 Yhteenveto

Yhteenvetona tästä työstä voidaan sanoa, että etäkäytön käyttöönotto ei ole nykypäivänä kovinkaan vaikeaa. Lähes jokainen käyttöjärjestelmä tarjoaa omat vaihtoehtonsa etäyhteyksien muodostamiselle. Jatkuva työasemien ja palvelimien verkostoituminen on tuonut vahvasti esille työasemien etähallintaa. Turvattomien verkkojen ylitse työskennellessä tietoturva on otettava hyvin tarkasti huomioon. Palomuurit ovat tärkeitä ohjelmistojen toiminnan ja myös tietoturvan osilta. Yleensä tarvitaan joitain toimenpiteitä käyttäjältä, jotta etäyhteydet päästettäisiin palomuurin lävitse.

Yksityisellä puolella etähallintaan löytyy runsaasti yksilöllisiä vaihtoehtoja kunkin käyttäjän tarpeisiin. Yleensä yksittäinen käyttäjä räätälöikin itselleen sopivan etähallintajärjestelmän, jota hän käyttää lähinnä omaan käyttöönsä. Yrityspuolella käytössä on taas lähinnä koko yritykselle räätälöity etähallintaratkaisu, jota kaikki käyttäjät sitoutuvat käyttämään. Käyttäjien tulee sitoutua myös noudattamaan yrityksen tietoturvakäytäntöjä, jotka ovatkin yrityksen kannalta tärkeitä arvokkaiden tietojen säilymisen kannalta. Usein yritysten etäliikenne on salattua ja tunnistaminen on tehty luotettavaksi.

Työssä huomasin myös sen, että monet etäyhteysratkaisut eivät ole sidottuja vain yhteen alustaan, sillä useat etäyhteysohjelmat toimivat useilla käyttöjärjestelmillä ja mahdollistavat yhteydet näiden välillä. Tämä lisää joustavuutta työskentelyyn, eikä sido käyttäjiä yhteen alustaan edes samassa käyttöjärjestelmässä.

Työssä koin mielekkääksi työskentelyn usean eri käyttöjärjestelmän parissa. Linux-käyttöjärjestelmä on kasvattanut suosiotaan yksityisellä puolella ja tarjoaa käyttäjälle usein ilmaisen version ohjelmista vertailuna Microsoftin-käyttöjärjestelmiin. Ilmaisten ohjelmien vuoksi etäyhteysohjelmien käyttö yleistyy lähitulevaisuudessa. Näen etäyhteyksien helpottavan esimerkiksi vanhempien ihmisten auttamista heidän atk-taitojensa rajoittuessa ongelmien ratkaisuissa. Ongelman ollessa akuutti ei auttajan tarvitse siirtyä paikan päälle ratkaisemaan tilannetta, mikäli vain kone on verkossa ja siihen saadaan muodostettua etäyhteys.

Tulevaisuudessa ollaan ehkä palaamassa keskustietokone -ajattelumalliin, josta hyvänä esimerkkinä on Supermatrix-projekti. Keskustietokone ratkaisun rajoitteena tällä hetkellä on liian hidas Internet-yhteys mikä ei mahdollista graafisen työpöydän näyttämistä asiakaspäätteellä. Mielestäni tämä suunta kehityksessä on paluuta menneisyyteen. Käyttäjällä pitäisi olla tietokone käytettävissä koko ajan ilman pelkoa, että Internet ruuhkautuu ja estää tietokoneen käytön.

Lähteet

1. Dameware 2011. http://www.dameware.com. 28.2.2011
2. Dwivedi, H. 2003. Implementing SSH: Strategies for Optimizing the Secure Shell. Wiley.
3. Kuutti, W. & Rantala, A. 2007. Linux. WSOYpro, Porvoo.
4. Minasi, M. 2001. Mastering Windows XP Professional. Sybex Inc.
5. Secure Shell. http://fi.wikipedia.org/wiki/SSH. 25.1.2011
6. Stahnke, M. 2005. Pro OpenSSH
7. Supermatrix-projekti. http://supermatrix.fi. 28.2.2011
8. TeamViewer. http://www.teamviewer.com. 25.1.2011
9. Telnet 2011. http://fi.wikipedia.org/wiki/Telnet 28.2.2011
10. Virtual Network Computing. http://fi.wikipedia.org/wiki/VNC . 25.1.2011
11. VNC: Comparison of Remote Desktop Software, Virtual Network Computing, Apple Remote Desktop, Realvnc, TeamViewer, Rfb Proto. 2010. Books LLC.