



VAASAN AMMATTIKORKEAKOULU  
VASA YRKESHÖGSKOLA  
UNIVERSITY OF APPLIED SCIENCES

Petteri Dietz

# ETÄKÄYTTÖYHTEYDET

Liiketalous ja matkailu  
2014



## ABSTRACT

Author	Petteri Dietz
Title	Remote Connections
Year	2014
Language	Finnish
Pages	43
Name of Supervisor	Antti Mäkitalo

---

This thesis studied remote connections between computers and active devices. The focus was on programs, program functions and techniques.

This thesis is meant to be an informative guide on what kind of remote desktops are available and for what kind of use they are most suitable. The work covers the needs of companies and private use, connections over a public network and the use in local area networks. There is a comparison of commercial programs and free programs in the work. Some of the programs are free of charge in private use and chargeable in commercial use. Some are charged in any use.

## KÄSITELUETTELO

AES	Advanced Encryption Standard, salaustekniikka.
Client	Ohjelma tai laite, joka toimii verkkopalvelun käyttäjänä.
DHCP	Dynamic Host Configuration Protocol, IP-osoitteen automaattisen konfiguroinnin mahdollistava protokolla.
DNS	Domain Name System, verkko-osoitteiden muuntaminen IP-osoitteiksi.
Ethernet	Lähiverkkotekniikka.
FTP	File Transfer Protocol, tiedonsiirtoprotokolla.
IP	Internet Protocol, verkon perusprotokolla, IP-osoite.
ISO	International Organization for Standardization, Standardisointijärjestö.
LAN	Local Area Network, lähiverkko.
LTS	Long Term Support, pitkäaikainen tuki.
LTSP	Linux Terminal Server Project, etäkäyttöyhteyskokonaisuus Linux-pohjaisille palvelimille.
MAC	Media Access Control, verkkokortin yksilöllinen osoite.
NAT	Network Address Translation, verkko-osoitteen muutospalvelu.
OSI	Open Systems Interconnect, verkkotekniikan viitemalli.
Palomuuuri	Tietoturvan hallintaan tarkoitettu ohjelma tai laite.
Palvelin	Ohjelma tai laite, joka toimii verkkopalvelun tarjoajana (sama kuin Server).
PXE	Preboot eXecution Environment, mahdollistaa tietokoneen käynnistämisen verkon kautta.
RDC	Remote Desktop Connect, etäkäyttöohjelma.
RDP	Remote Desktop Protocol, etäkäyttöprotokolla.
RDS	Remote Desktop Services, etäkäyttöohjelmakokonaisuus.
RFB	Remote Frame Buffer, etäkäyttöprotokolla.
RJ11	Verkkojohdon liittimen nimi / malli.
RJ45	Verkkojohdon liittimen nimi / malli.
RSA	Julkisen avaimen salausmenetelmä, salaustekniikka.
Server	Ohjelma tai laite, joka toimii verkkopalvelun tarjoajana (sama kuin palvelin).
SSH	Secure Shell, salattu tekstipohjainen etäkäyttöyhteys.
SWOT	Nelikenttäanalyysi, jota käytetään apuna suunnitelmien laatimisessa.
TCP	Tiedonsiirtoprotokolla, verkon perusprotokolla.
TCP/IP	Kahden verkon perusprotokollan yhteisnimitys.
Telnet	Tekstipohjainen protokolla, salaamaton tekstipohjainen etäkäyttöyhteys.
TFTP	Trivial File Transfer Protocol, tiedoston siirtoon tarkoitettu protokolla.
Thin Client	Laitteistoltaan vaatimaton tietokone etäkäyttöä varten.
UDP	Tiedonsiirtoprotokolla, verkon perusprotokolla.
VPN	Virtual Private Network, salattu virtuaalinen lähiverkkotekniikka.

# SISÄLLYSLUETTELO

## TIIVISTELMÄ

## ABSTRACT

1	JOHDANTO.....	4
2	TEKNIIKAT JA PROTOKOLLAT.....	6
	2.1 OSI-malli.....	6
	2.2 TCP/IP.....	9
	2.2.1 TCP-protokolla.....	9
	2.2.2 UDP-protokolla.....	9
	2.2.3 IP-protokolla.....	10
	2.2.4 Portti.....	10
	2.3 DHCP.....	10
	2.4 NAT.....	11
	2.5 DNS.....	11
	2.6 Ethernet.....	11
	2.7 MAC-osoite.....	12
	2.8 Reititin.....	12
	2.9 VPN.....	12
	2.10 SWOT.....	13
3	TOTEUTUS.....	14
	3.1 Tarvekartoitus.....	14
	3.2 Käytettävä palvelinalusta.....	15
	3.2.1 Windows.....	15
	3.2.2 Linux.....	16
	3.3 Käytettävä päätealusta.....	18
	3.3.1 Windows.....	19
	3.3.2 Linux.....	19
	3.3.3 Mobiili.....	19
	3.4 Siirrettävä tieto.....	20
	3.5 Tietoturva.....	20
	3.6 Käyttäjämäärät.....	21

3.7 Käytön helppous .....	21
4 ETÄKÄYTTÖOHJELMAT JA TEKNIIKAT .....	23
4.1 Tekstipohjainen etäkäyttö .....	23
4.1.1 Telnet.....	23
4.1.2 SSH .....	24
4.2 Graafinen etäkäyttö .....	28
4.2.1 VNC (RFB) .....	29
4.2.2 TeamViewer .....	31
4.2.3 Remote Desktop Connection (RDC).....	35
4.2.4 Microsoft Remote Desktop Services (RDS) .....	36
4.2.5 Linux LTSP .....	37
4.2.6 Thin client .....	38
5 YHTEENVETO .....	40
LÄHTEET .....	41

## **KUVIO- JA TAULUKKOLUETTELO**

Taulukko 1. Käyttöjärjestelmien ominaisuusvertailu Windows vs. Linux. s.22

Taulukko 2. Tekstipohjaisten etäkäyttöyhteyksien vertailu. s.31

Taulukko 3. Graafisten etäkäyttöohjelmistojen vertailutaulukko. s.43

Kuva 1. OSI-mallin rakennekuva I. (Colliander. 1999) s.11

Kuva 2. OSI-mallin rakennekuva II. (Kouvolan seudun ammattiopisto) s.11

Kuva 3. SSH-autentikointi julkisella avaimella. (Kuva: RTC Group Inc.) s.29

Kuva 4. Puttyn käyttöliittymä. s.30

Kuva 5. SSH-näkymä etäkoneelta Putty:lla. s.31

Kuva 6. Yksinkertainen RealVNC:n yhdistämiskkuuna. s.34

Kuva 7. Työpöytänäkymä etäkoneelta RealVNC:llä. s.34

Kuva 8. TeamViewer näkymä. Palvelin ja yhdistäminen samasta ikkunasta. s.37

Kuva 9. Työpöytänäkymä etäkoneelta TeamViewerillä. s.37

Kuva 10. RDC yhdistämisenäkymä. s.39

## 1 JOHDANTO

Etäkäyttöyhteyksiä on ollut käytössä jo kymmeniä vuosia erilaisissa muodoissa. Ensimmäiset etäkäyttöyhteydet olivat täysin tekstipohjaisia, koska molemmissa päissä olevat tietokoneet toimivat tekstipohjaisilla käyttöjärjestelmillä. Graafisten käyttöjärjestelmien yleistyessä myös graafiset etäkäyttöyhteydet tulivat mahdollisiksi. Tällöin molemmissa päissä olevat tietokoneet toimivat graafisella käyttöjärjestelmällä, kuten esimerkiksi Windowsilla. Graafisen etäkäytön kohteena olevan tietokoneen näyttämä kuva siirretään tietoverkon yli toiselle tietokoneelle, jolta käsin kohteena olevaa konetta voidaan käyttää, kuten oltaisiin sen läheisyydessä. Graafisen käyttöjärjestelmän yleistyessä ei tekstipohjainen etäkäyttö ole kuitenkaan jäänyt pois. Tekstipohjaista etäkäyttöä tarvitaan muun muassa tietoverkkojen aktiivilaitteiden ja Linux-pohjaisten käyttöjärjestelmien hallintaan. Tekstipohjaisen etäkäytön hyvänä puolena voidaan pitää sen huomattavasti pienempiä laitteistovaatimuksia niin tietokoneen kuin tietoliikennesyhteyksienkin osalta. Tekstipohjainen etäkäyttö on poikkeuksetta vain IT-alan ammattilaisten ja osaajien käytössä.

Graafinen etäkäyttö soveltuu helppoutensa puolesta myös yritys- ja yksityiskäyttöön. Se mahdollistaa esimerkiksi työpaikalla tai kotona olevan tietokoneen käyttämisen hotellihuoneesta käsin. Täten käyttäjän tietokoneella ei tarvitse olla kaikkia samoja ohjelmia ja tiedostoja, joita työpaikalla tai kotona sijaitsevassa tietokoneessa on. Tämä lisää osaltaan myös tietoturvaa tiedostojen ollessa yhdessä paikassa.

Etäkäyttöohjelmat ovat vuosien saatossa kehittyneet tekstipohjaisista graafisiin ja osaan ohjelmista on kehitetty muita helpottavia toimintoja, kuten esimerkiksi reaaliaikainen keskustelu (instant messaging) ja tiedostojen siirto. Lisäominaisuudet tuovat käyttäjilleen tietyissä tilanteissa suurta lisäarvoa.

Etäkäyttöyhteyksiin voidaan lukea myös Citrix-pohjaiset ja -tyyliset ohjelmat. Nämä mahdollistavat ohjelmien käyttämisen miltä tahansa tietokoneelta ilman varsinaista kuvan tai tekstin siirtoa. Tällöin palvelimelle kirjautumisen jälkeen



käytettävä ohjelma ladataan käyttäjän tietokoneelle, tosin vain käyttöliittymän ja pakollisten ohjelmakomponenttien osalta. Ohjelman pääkomponentit sijaitsevat palvelimella. Käytännössä itse ohjelma toimii palvelimella ja käyttäjän koneella on vain ohjelman käyttöliittymä. Käyttäjän käyttöliittymällä tekemät muutokset siirtyvät tietoverkon välityksellä palvelimelle, johon ne tallentuvat.

Työn tarkoituksena on selvittää millaisia etäkäyttöön soveltuvia ohjelmia on olemassa, mihin ne soveltuvat ja minkä hintaisia ne ovat. Ohjelmia vertaillaan keskenään niin hinnan, toiminnallisuuden, saatavuuden, käyttöönoton kuin käytettävyyden osalta. Myös mobiililaitteet on otettu huomioon.

Tutkimus perustuu henkilökohtaisiin kokemuksiin sekä internetistä löytyvään luotettavaan materiaaliin, jota on tarjolla joidenkin ohjelmien osalta varsin niukasti.

Työn on tarkoitus auttaa IT-alan ammattilaisia, harrastajia sekä pieniä ja keskisuuria yrityksiä valitsemaan käyttöönsä kustannustehokkaasti parhaimman käyttöön soveltuvan ohjelman.

Ongelmallisen työstä tekee ohjelmistojen varsin suuri kirjo, verkosta löytyvän luotettavan tiedon pirstaleisuus sekä mahdollisimman tarkan käyttötarkoituksen kuvaaminen. Osassa ohjelmia myös hinta estää niiden käytännön testauksen lopputyötä varten. Näissä ohjelmissa joudutaankin turvautumaan aikaisempiin käyttökokemuksiin, jotka ovat syntyneet työpaikoilla sekä koulussa käytettävistä ohjelmista.

## 2 TEKNIIKAT JA PROTOKOLLAT

Tässä luvussa kerrotaan lyhyesti tietoliikenteessä käytetyistä protokollista, tekniikoista ja malleista.

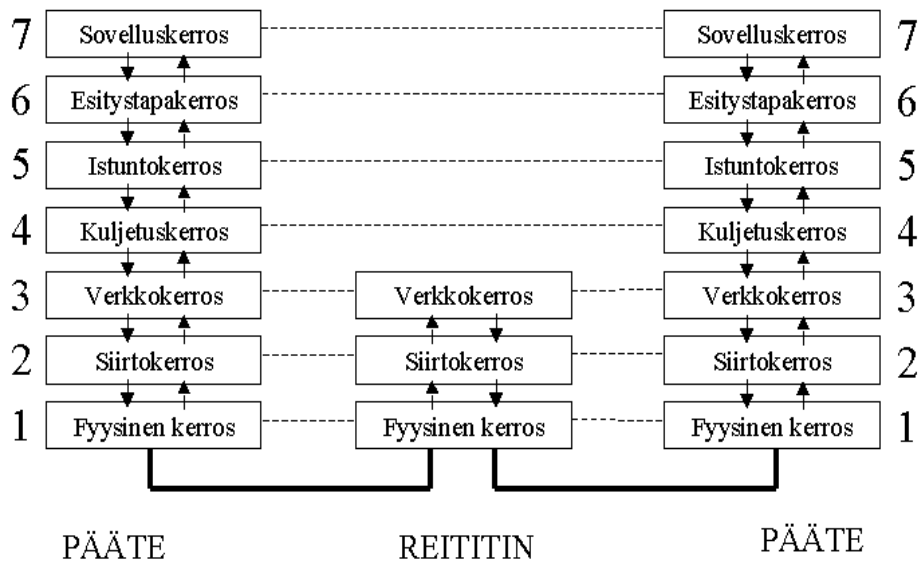
### 2.1 OSI-malli

OSI-malli (Open Systems Interconnect) valmistui vuonna 1984 ja sen kehittäjänä toimi ISO-organisaatio (International Organization for Standardization). OSI-malli kuvaa, kuinka tieto kulkee tietokoneelta toiselle tietoverkon kautta. OSI-malli on viitemalli, joka koostuu seitsemästä kerroksesta, joissa jokaisessa määritellään tietyt verkon toiminnot. Mallin mukaan verkkoliikenteen tehtävät jaetaan seitsemään pienempään osaan, joita on helpompi hallita. Osat ovat itsenäisiä, jonka ansiosta jonkin tietyn verkko-osan kehittäminen voidaan toteuttaa muihin osiin koskematta. (Cisco System Inc.) Osi-mallin rakennetta on esitelty kuvissa 1 ja 2.

OSI-mallin kerrokset ovat:

1. **Fyysinen kerros** (Physical Layer): Määrittää elektroniset, mekaaniset ja toiminnalliset ominaisuudet tietoliikenneverkkojen välille. Ominaisuuksissa määritetään arvot muun muassa jännitetasolle, jännitetason muutoksen ajoitukselle, siirtonopeudelle, siirton maksimipituudelle sekä fyysisille liitäntöille.
2. **Siirtokerros** (Data-Link Layer): Huolehtii tiedon luotettavasta siirrosta fyysistä kerrosta pitkin. Siirtokerroksen määritelmät määrittävät erinäisiä verkko- ja protokolla-arvoja, kuten fyysisen osoittamisen, verkon rakenteen, virheilmoitukset, kehyksien ajoitukset ja vuonohjauksen. Fyysinen osoittaminen määrittää, kuinka verkkolaitteet osoitteistetaan siirtokerroksessa. Virheilmoitus ilmoittaa ylemmälle kerrokselle siirtovirheen tapahtumisesta. Vuonohjaus huolehtii, että vastaanottavalle laitteelle syötetään tietoa vain sen vastaanottokapasiteetin verran.

3. **Verkkokerros:** Huolehtii reitityksestä ja siihen liittyvistä toiminnoista.
4. **Kuljetuskerros:** Huolehtii tiedonsiirron luotettavuudesta tietoverkossa. Tiedonsiirto on ylemmille kerroksille näkymätön. Yleisesti kuljetuskerros sisältää vuonhallinnan, multiplexauksen, virtuaalikanavien hallinnan sekä virheenkorjauksen.
5. **Yhteyskerros / istuntokerros:** Muodostaa, hallinnoi ja sulkee yhteyksiä yhteyskerroksen ja esityskerroksen välillä. Yhteydet koostuvat palvelupyynnöistä ja palveluvastauksista, joita eri verkoissa olevat ohjelmat lähettävät.
6. **Esitystapakerros:** Tarjoaa erilaisia koodaus- ja konversiotoimintoja sovelluskerrokselle. Nämä toiminnot varmistavat, että sovelluskerrokselta lähetetty tieto on vastaanottavan järjestelmän kanssa yhteensopiva. Esimerkkeinä koodaus- ja konversiotoiminnoista ovat muun muassa merkkijärjestelmän, pakkauksen ja salauksen muunnokset ja konversoinnit.
7. **Sovelluskerros:** On lähin kerros loppukäyttäjään nähden. Sovelluskerros ja loppukäyttäjä asioivat molemmat suoraan sovelluksen kanssa. Sovelluskerros tarjoaa liitännärajapinnan sovelluksille, jotta ne voivat käyttää tietoliikenneyhteyksiä. Sovelluskerroksen toiminnot sisältävät yleensä kommunikointikumppanin identiteetin, resurssien saatavuuden sekä kommunikoinnin synkronoinnin. (Cisco Systems Inc. 1998)



Kuva 1. OSI-mallin rakennekuva I. (Colliander. 1999)



Kuva 2. OSI-mallin rakennekuva II. (Kouvola seudun ammattiopisto)

## 2.2 TCP/IP

”TCP/IP (Transmission Control Protocol / Internet Protocol) on usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa. Sen päällä voidaan ajaa useita muita verkko- tai kuljetuskerroksen protokollia, joista TCP-protokolla on yleisin. Se vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hukkuneiden pakettien uudelleenlähetyksestä. Vaikka TCP/IP-protokollaperheeseen kuuluu monia muitakin protokollia, pääosa liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä. Tämän takia protokollaperhe yleensä tunnetaan nimellä TCP/IP.” (Web-opas. Mikä on TCP/IP?)

### 2.2.1 TCP-protokolla

TCP-protokolla luo yhteydet tietokoneiden sovellusten välille käyttäen IP-paketteja. (Web-opas, Mikä on TCP/IP?)

TCP-protokolla paketoii ohjelmien tuottamat tiedot paketteihin, jotka voidaan lähettää verkon yli sekä vastaanottaa paketit verkkokerrokselta. Se hallitsee myös vuonohjausta ja vastaa pakettien perillemenosta varmistamalla, että vastaanottaja on vastaanottanut lähetetyt paketit. Vastaavasti se myös ilmoittaa saapuneiden pakettien vastaanottamisesta pakettien lähettäjälle. (Rouse. 2014)

### 2.2.2 UDP-protokolla

UDP-protokolla on kuljetuskerroksen protokolla, joka on hyvin yleisessä käytössä. TCP-protokollaan verrattuna UDP kuormittaa verkkoa vähemmän, sillä se ei vaadi paketin vastaanottajan kuittausta perille saapuneesta paketista. UDP tarjoaa tarkistussumman, jonka perusteella voidaan todeta onko paketti saapunut kokonaisuutena perille. Käytännössä UDP sopii hyvin muun muassa äänen ja kuvan siirtoon, joissa vähäinen pakettien puuttuminen ei vaikuta olennaisesti siirrettyyn tietoon. (Rouse. 2005)

### 2.2.3 IP-protokolla

IP-protokolla on TCP/IP-protokollan ydin. Verkon aktiivilaitteet, kuten kytkimet ja reitittimet, välittävät tiedon oikealle tietokoneelle / laitteelle IP-pakettien otsikkokenttien tietojen perusteella. Ylempien tasojen protokollat kulkevat IP-pakettien data-osiossa. Täten IP-tasolla toimiva verkko ei ole tietoinen mitä IP-paketin hyötykuormana kulkee. (Web-opas, Mikä on TCP/IP?)

IP-osoitteet on jaettu kahteen erilliseen osaan, julkisiin IP-osoitteisiin sekä sisäverkon IP-osoitteisiin. Julkisella IP-osoitteella operoidaan lähiverkon ulkopuolella ja se on muille internetin käyttäjille näkyvissä. Sisäverkon IP-osoite on käytössä ainoastaan lähiverkossa ja näkyvissä vain samassa lähiverkossa oleville koneille.

### 2.2.4 Portti

Kuljetuskerroksen protokollat käyttävät portteja ohjataksaan paketit niitä odottaville palveluille. Porttia voidaan verrata esimerkiksi puhelinasiakaspalveluiden lisävalintoihin. Ensin soitetaan puhelimella asiakaspalvelun puhelinnumeroon (vastaa IP-osoitetta), jonka jälkeen lisävalinnalla (vastaa porttia) valitaan puhelun yhdistämisestä laskutukseen, myyntiin tai vikailmoitukseen.

Portteja on yhteensä 65535 kappaletta per protokolla. Portit ovat jaettuina eri kategorioihin; järjestelmäportit 0 - 1023, käyttäjäportit 1024 – 49151 ja dynaamiset portit 49152 – 65535. (Service Name and Transport Protocol Port Number Registry.)

## 2.3 DHCP

DHCP (Dynamic Host Configuration Protocol) on protokolla, joka dynaamisesti määrittää verkkolaitteen IP-osoitteen laitteen liittyessä verkkoon. Jaettu IP-osoite on voimassa ennalta määritellyn ajan. DHCP vaatii toimiakseen DHCP-palvelimen ja päätelaitteen, joka tukee DHCP:n käyttöä. IP-osoitteen määrittäminen tapahtuu MAC-osoitteeseen perustuen. (Web-opas. Mikä on DHCP?)

## 2.4 NAT

NAT (Network Address Translation) mahdollistaa lähiverkon laitteiden liikennöinnin lähiverkon ulkopuolelle siten, ettei koneiden IP-osoite näy lähiverkon ulkopuolelle. NAT toteutetaan ohjelmallisesti joko palvelimelta tai verkon aktiivilaitteelta, kuten esimerkiksi reitittimeltä. NAT toimii toisella kädellä lähiverkon parissa ja toisella kädellä julkisen verkon kanssa. NAT suojaa lähiverkon laitteita ulkoverkon suunnasta tulevilta hyökkäyksiltä, sillä hyökkäykset eivät läpäise NAT:tia ilman erikseen tehtyjä porttiohjauksia. Porttiohjauksien avulla tietyn portin tai portit voidaan ohjata lähiverkossa halutulle kohteelle. Tällöin kaikki ko. portteihin saapuva liikenne ohjautuu suoraan sille lähiverkon koneelle, jolle porttiohjaukset ovat osoitettu. NAT:in pääsääntöinen tarkoitus on kuitenkin säästää julkisten IP-osoitteiden määrää, että niitä riittäisi kaikille tarvitseville laitteille ja tahoille.

## 2.5 DNS

Koska tietoliikenne kulkee IP-osoitteiden avulla on DNS (Domain Name System) kehitetty muuttamaan tekstimuotoiset osoitteet IP-osoitteiksi. Esimerkiksi selaimen kirjoitettu www-osoite muuntuu DNS:n avulla IP-osoitteeksi, jotta tiedetään mihin IP-osoitteeseen selaimen on yhdistettävä. DNS hoitaa myös sähköpostin reitittämisen oikealle palvelimelle. (Suomen Hostingpalvelu OY. 2010)

## 2.6 Ethernet

Ethernet on yleisimmin käytössä oleva lähiverkkotekniikka. Aluksi Ethernet toimi koaksiaalikaapeleiden välityksellä, joista luovuttiin niiden heikon suorituskyvyn sekä vikaherkkyuden takia. Nykyään siirtotienä käytetään kierrettyä parikaapelia, jonka tämänhetkinen suurin mahdollinen siirtonopeus on 10 Gbps. Yleisimmät käytössä olevat nopeudet ovat 100 Mbps sekä 1 Gbps. Ethernet-kaapelin suurin mahdollinen pituus ilman signaalin häiriintymistä on 100 metriä. Liittimenä kaapeleissa käytetään kahdeksanpinnistä RJ45-liitintä (puhelimissa käytettävä liitin on neljäpinninen RJ11-liitin). (Axis Communications AB. 2014)

## 2.7 MAC-osoite

MAC-osoite (Media Access Control) on verkkokortin yksilöllinen tunniste. MAC-osoite on aina pituudeltaan 48-bittia ja muodoltaan ”MM:MM:MM:SS:SS:SS”. Ensimmäiset kuusi merkkiä kertovat valmistajan (Manufacturer) ja seuraavat kuusi merkkiä ovat verkkokortin sarjanumeroa (Serial number) varten. DHCP-palvelin käyttää MAC-osoitetta tunnisteena IP-osoitteen antamiseen. (Mitchell)

## 2.8 Reititin

Reititin on verkon aktiivilaite, joka ohjaa IP-pakettien kulkua IP-osoitteiden perusteella. Sen tehtävänä on ohjata paketit perille mahdollisimman nopeaa ja luotettavaa reittiä pitkin. Reitittimen verkkoliitäntäteknikat voivat olla erilaisia lähtevällä ja saapuvalla puolella. IP-paketti voi saapua esimerkiksi ethernet-liitäntää pitkin ja lähteä langatonta verkkoa käyttäen. (IP-location)

## 2.9 VPN

VPN (Virtual Private Network) on tekniikka, jolla voidaan yhdistää kaksi erillään olevaa verkkoa ohjelmallisesti yhdeksi verkoksi, jolloin kaikki verkon palvelut ovat käyttäjän saatavilla. VPN:n suosio perustuu sen monipuolisuuteen ja vahvaan salaukseen.

VPN:ää voidaan käyttää kahdella eri tavalla. Joko tietokoneiden välisesti tai reitittimien välisesti. Tietokoneiden välinen verkko muodostetaan käyttämällä VPN-palvelimena ja VPN-clienttinä tietokoneita. Tämä mahdollistaa yksittäisten käyttäjien yhteydenmuodostuksen milloin vain mistä vain esimerkiksi yrityksen verkkoon. Reitittimien välinen VPN käyttää VPN-palvelimena ja VPN-clienttinä reitittimen omaa ohjelmistoa. Tämä mahdollistaa esimerkiksi koko toimiston kattavan VPN-yhteyden muodostamisen kahden toimitilan välillä siten, ettei käyttäjien tarvitse tietää asiasta mitään. (Koulutus- ja konsultointipalvelu KK Mediat)



## 2.10 SWOT

SWOT-analyysin tarkoituksena on auttaa tunnistamaan suunnitellun strategian tai muutoksen sopivuutta yrityksen tarpeisiin. Analyysissä pyritään selvittämään strategian tai muutoksen vahvuudet (Strengths), heikkoudet (Weakness), mahdollisuudet (Opportunities) ja uhat (Threats). Vahvuudet ja heikkoudet ovat sisäisiä asioita, joihin yritys itse pystyy vaikuttamaan. Ulkoisia asioita ovat mahdollisuudet ja uhat, joihin voivat vaikuttaa monet yrityksen ulkopuoliset asiat. SWOT-analyysi toteutetaan usein nelikenttäanalyysinä, jossa jokaiselle osa-alueelle on oma merkintäkenttensä. (Oulun seudun ammattikorkeakoulu, SWOT-analyysi)

### 3 TOTEUTUS

Päättötyön käytännön toteutus pyritään toteuttamaan mahdollisuuksien mukaan ilmaiseksi ladattavilla Windows- ja Linux-alustaisilla palvelinohjelmistoilla. Loppukäyttäjän pääteohjelmista pyritään saamaan mukaan Windows-, Linux- ja Android-alustaiset ohjelmat. Linux-alustaiset ohjelmat asennetaan tekstipohjaisena Ubuntu Server 12.04 LTS palvelimelle.

Teorian ja aikaisempien käyttökokemusten varassa ovat palvelinohjelmistoista maksulliset ohjelmat sekä Machintosh-käyttöjärjestelmällä toimivat ohjelmat. Loppukäyttäjän ohjelmistoista teoriatiedon ja aikaisempien käyttökokemusten varassa ovat maksulliset ohjelmat, Machintosh, iPad, iPhone sekä Windows Phonella toimivat ohjelmat.

Toteutuksessa on tarkoitus käyttää pääsääntöisesti kirjoittajan omia laitteita ja tietoliikenneyhteyksiä. Tarvittaessa koulun harjoitusluokat ovat myös käytettävissä.

#### 3.1 Tarvekartoitus

Tarvekartoitus on syytä tehdä erittäin suurella huolellisuudella. Sen pohjalta tehdyt päätökset vaikuttavat oleellisesti loppukäyttäjän käyttökokemukseen. Tarvekartoitus vaikuttaa yritysten kohdalla tulevan ylläpidon ja käyttöneuvonnan kustannuksiin ohjelmiston hankinnan kustannuksien lisäksi. Tietoturva-asiat on myös tärkeää ottaa huomioon tarvekartoitusta tehdessä. Tarvekartoituksen periaatteiksi sopivat hyvin kysymykset ”kuka, mitä, millä ja mistä?”

”Kuka?” vastaa kysymykseen; ketkä palvelua käyttävät? Kyseessä voi olla yrityksen sisäinen tai ulkoinen henkilökunta tai yksityiskäyttäjät. Käyttäjien osaamistasoissa on suuria eroja, joten palvelun pitää olla käyttäjälleen helppo käyttää.

”Mitä?” vastaa kysymyksiin; millaisia palveluita on tarkoitus käyttää, käytetäänkö tekstipohjaista vai graafista käyttöliittymää. Onko palveluiden tarkoituksena siirtää kuvaa, käskyjä vai tekstipohjaista tietoa.

”Millä?” vastaa kysymyksiin; millaisilla laitteilla palvelua on tarkoitus käyttää. Onko kyseessä tehokas pöytätietokone, kannettava tietokone, suhteellisen tehoton miniläppäri, tabletti, puhelin vai jokin muu laite. Laitteistojen käyttöjärjestelmät on myös tärkeä tietää ohjelmistosaatavuuden selvittämiseksi.

”Mistä?” vastaa kysymyksiin; millaisesta ympäristöstä palvelua on tarkoitus käyttää. Onko ympäristö turvallinen tietoliikenneyhteyksien osalta vai voidaanko verkkoliikennettä vakoilla helposti. Minkälaisia yhteysnopeuksia on käytettävissä ja kuinka kaukana palvelin on käyttäjästä.

Avuksi kartoitukseen voidaan ottaa myös SWOT-analyysi. Sitä voidaan käyttää kokonaisuuden kartoitukseen tai yksittäisien osa-alueiden tarkempaan tarkasteluun. SWOT-analyysi toteutetaan yleensä nelikenttämallina

## **3.2 Käytettävä palvelinalusta**

Käytettävän palvelimen käyttöjärjestelmä vaikuttaa osaltaan siihen, mitä palveluita voidaan käyttää ja minkä hintaisia ne ovat. Windows-pohjaiset palvelimet ovat helpommin hallittavissa, mutta Linux-pohjaiset taas ovat edullisempia hankintakustannuksiltaan ja ohjelmistojen osalta.

### **3.2.1 Windows**

Windows on käyttöjärjestelmänä erittäin suosittu. Osaltaan sen suosiota selittää se, että se on ylivoimaisesti eniten tehdasasennettu käyttöjärjestelmä uusissa tietokoneissa. Vaikka uutta konetta ostaessa ei hintalapussa ole eritelty käyttöjärjestelmän osuutta hinnasta, on kuitenkin selvää, että jokaisen laitteen hintaan on sisällytetty myös Windowsin lisenssimaksu. Erikseen ostettuna koti- ja toimistokäyttöön tarkoitettujen lisenssien hinnat alkavat noin sadasta eurosta ja voivat nousta tuhansiin euroihin raskaaseen yrityskäyttöön tarkoitettujen versioiden puolella.

Windowsin suosiota edesauttaa sen helppokäyttöisyys sekä valtavan laaja laitteistotuki. Kärjistettynä voikin sanoa, että ei ole sellaista komponenttia tai oheislaitetta, joka ei toimisi Windowsilla. Laitteistovaatimuksen osalta Windows on vaativa käyttöjärjestelmä. Suuri prosessoriteho ja keskusmuistin määrä ovat pakollisia käytettävyyden ja vakauden saavuttamiseksi. Mikäli laitteiston prosessoriteho on riittämätön, on käyttö hidasta. Jos taas keskusmuistia on liian vähän, on käyttö hitauden lisäksi epävakaa ohjelmien tapellessa vapaan muistin käytöstä. Kun laitteiston kokoonpano on kunnollinen, Windows on käyttöjärjestelmänä varsin luotettava. Vakautta ja luotettavuutta kuitenkin häiritsevät jatkuvat ohjelmisto- ja tietoturvapäivitykset, jotka vaativat käyttöjärjestelmän uudelleenkäynnistystä asennuksen päätteeksi.

Turvallisuuden osalta Windows on helposti haavoittuvainen, vaikka virusturvallisuutta ja sisäistä palomuuria onkin vuosin saatossa parannettu huomasti. Suurin osa haittaohjelmista on tehty Windowsia varten. Vakoilu- ja haittaohjelmia tarttuu monella eri tavalla, kuten tiedostojen välityksellä ja nettisivujen kautta. Usein käyttäjä ei edes tiedä klikanneensa linkkiä, jonka kautta käyttöjärjestelmä saastuu. Windowsin sisäänrakennettu www-selain Internet Explorer onkin tunnettu haavoittuvuudestaan, jonka takia sen käyttöä on monesti syytä välttää. Windows käyttöjärjestelmien ominaisuuksia on vertailtu taulukossa 1.

### **3.2.2 Linux**

Linux-pohjaiset käyttöjärjestelmät ovat suosittuja kaikenlaisessa käytössä. Niiden suuren suosion pohjalla on käyttöjärjestelmän erittäin hyvä skaalattavuus sekä maksuttomuus. Laitteistovaatimusten osalta Linuxissa on hyvät ja huonot puolet. Hyvänä puolena voidaan pitää sitä, että tarvittaessa käyttöjärjestelmän tekstipohjaisen tai kevyen graafisen version saa pyörimään hyvinkin vaatimattomalla laitteistokokoonpanolla. Haittapuolena on, että kaikki komponentit eivät ole tuettuja. Tämä tarkoittaa käytännössä sitä, ettei kaikille komponenteille ole olemassa toimivaa ajuria. Komponenttien huolellinen valinta onkin tärkeä osa Linux-pohjaista kokoonpanoa suunniteltaessa.

Linux-käyttöjärjestelmien ohjelmistotarjonta on laajaa ja tarjolla on hyvin paljon ilmaisia ohjelmia, jotka soveltuvat hyvin yritys- ja yksityiskäyttöön. Käyttöjärjestelmän ja ohjelmiston konfiguroinnin osalta Linux on huomattavasti vaikeampi käyttää verrattuna täysin graafisiin käyttöjärjestelmiin. Useat asetukset on helpoin tehdä tekstipohjaisena suoraan tiedostoja editoimalla. Tämä vaatii huomattavan paljon tietämystä ohjelman asetuksista sekä itse käyttöjärjestelmän komennoista.

Linuxien graafinen käyttöliittymä on viime vuosien aikana kehittynyt huomasti ja tätä kautta perusohjelmien asennus onnistuu varsinkin helposti. Siitä huolimatta Linuxin parissa on vaikea välttää joutumasta tekemisiin tekstipohjaisen konfiguroinnin kanssa. Ohjelmiston vakauden kannalta Linux on erittäin hyvä käyttöjärjestelmä. Päivityksiä asentaessa koko käyttöjärjestelmää ei tarvitse käynnistää uudelleen. Päivitetyn ohjelmakomponentin voi käynnistää erikseen uudelleen, jolloin uudelleenkäynnistyksen kesto on yleensä vain muutamia sekunteja. Täten itse käyttöjärjestelmää ei tarvitse käynnistellä uudelleen jokaisen päivityksen yhteydessä. Linux-pohjaiset palvelimet ovatkin tunnettuja todella pitkistä päälläoloajoista. Turvallisuuden puolesta Linux on ollut aina hyvä. Se sisältää erittäin hyvät käyttäjätilien ja -ryhmien hallintaominaisuudet sekä palomuurioinaisuudet. Virus- ja vakoiluohjelmien osalta Linux on huomattavasti paremmassa asemassa, kuin Windows. Haittaohjelmia on huomattavasti vähemmän Linuxille. Syynä on Linuxin merkittävästi pienempi markkinaosuus, käyttäjien valvetuneisuus sekä eri Linux-versioiden kirjo. Käyttötukea Linuxille ei varsinaisesti ole tarjolla, mutta yhteisöjen ja ohjelmistojen valmistajien sivuilta löytyy valtava määrä tietoa ja ohjeita käyttöjärjestelmän sekä ohjelmistojen konfigurointiin. Ongelmatilanteessa keskustelupalstoilta löytyy paljon avuliaita ihmisiä, jotka auttavat parhaansa mukaan ongelmien ratkaisemisessa. Linux käyttöjärjestelmien ominaisuuksia on vertailtu taulukossa 1.

Taulukko 1. Käyttöjärjestelmien ominaisuusvertailu Windows vs. Linux

Ominaisuus	Windows	Linux
Hinta	Jokaisesta asennetusta Windowsista täytyy maksaa lisenssimaksu	Ilmainen yritys- ja yksityiskäytössä
Käytettävyys	Helppokäyttöisempi, kuin Linux. Ei tarvetta tekstipohjaisille komennoille	Vaikeampi käyttää, vaikka vuosien saatossa käytettävyys onkin parantunut huomasti
Luotettavuus	Täytyy käynnistellä usein päivitysten yhteydessä. Alttiimpi viruksille ja haittaohjelmille	Voi olla päällä todella pitkää aikoja ilman uudelleenkäynnistystä. Turvaominaisuudet todella hyvät
Laitteistotuki	Erittäin laaja tuki eri valmistajien komponenteille	Suppeampi laitteistotuki, täytyy tarkistaa laitteiston yhteensopivuus ennen hankintaa
Laitteistovaatimus	Vaatii paljon suoritustehoa laitteistolta. Rääätälöinti hankalaa.	Toimii varsin pienitehoisillakin laitteistoilla. Voidaan rääätälöidä laitteiston tehojen mukaan
Ohjelmiston saatavuus	Erittäin hyvä	Hyvä / Erittäin hyvä
Ohjelmiston hinta	Tarjolla varsin vähän ilmaisia ohjelmia.	Tarjolla erittäin paljon ilmaisia ohjelmia laidasta laitaan
Turvallisuus	Windowsin palomuuuri kehittynyt huomattavasti. Tarjolla useita palomuuureja ja virustorjuntaohjelmia. Altis haittaohjelmille. Automaattiset päivitykset plussaa.	Käyttäjätilien ja -ryhmien hallinta sekä palomuuriominaisuudet erittäin hyvät. Linux viruksia huomattavasti vähemmän liikenteessä. Nopeat tietoturvapäivitykset.
Tuki	Tuki varsin kattava. Netistä löytyy paljon vinkkejä ja ohjeita. Microsoftin omat tukisivut hankalahkot	Tuki muiden käyttäjien varassa. Linux-foorumeilla apua tarjolla erittäin paljon. Osattava etsiä oikea tieto itse.

### 3.3 Käytettävä päätealusta

Käytettävä päätelaite saattaa vaikuttaa käytettävän ohjelmiston ja käyttöjärjestelmän valintaan. Varsinkin suunniteltaessa etäkäyttöä mobiililaitteilla täytyy asiaan

kiinnittää erityistä huomiota. Mobiililaitteiden suuri kirjo laitteiden ja käyttöjärjestelmien osalta tuovat omat haasteensa sopivan etäkäyttöohjelman löytämiselle.

### **3.3.1 Windows**

Tietokoneiden osalta Windows on hyvin tuettu alusta pääteohjelmistojen suhteen. Sille löytyy kaikkiin etäkäyttöyhteyksiin sopivat ohjelmat. Ohjelmien hinnat vaihtelevat ilmaisista varsin arvokkaihin maksullisiin sovelluksiin. Windowsilla voi käyttää hyvin niin graafista kuin tekstipohjaistakin etäkäyttösovellusta.

### **3.3.2 Linux**

Linuxille löytyy myös erittäin kattavasti etäkäyttösovelluksia, ei kuitenkaan siinä määrin, kuin Windowsille. Osa maksullisista ohjelmista ei tue Linuxia ohjelmistojensa osalta. Ohjelmien käytettävyys on graafisella käyttöliittymällä hyvä. Tekstipohjaisen Linuxin kanssa ei graafisia pääteohjelmia voi käyttää. Tällöin tulevat kysymykseen lähinnä SSH- tai Telnet-yhteydet, jotka ovat molemmat täysin tekstipohjaisia. Telnetin käyttöä pitää välttää mahdollisimman paljon, sillä sen tietovirta ei ole lainkaan salattua.

### **3.3.3 Mobiili**

Mobiilialustaiset pääteohjelmat ovat kehittyneet huimasti viime vuosina. Laitteistojen kasvavat tehot sekä nopeat 3G- ja 4G-yhteydet ovat luoneet hyvän pohjan etäkäyttöohjelmien ajamiselle mobiilialustoilla. Mobiilialustojen ongelmana on kuitenkin niiden suuri kirjo ja rajoittuneisuus. Varsinkin Windows Phone ja Applen iOS-käyttöjärjestelmien sovelluskaupat ovat tarkassa valvonnassa valmistajien toimesta. Kilpailevan valmistajan ohjelmistoja ei haluta kauppaan julkaistavaksi, sillä se ei edesauta valmistajan omien ohjelmistojen myyntiä. Vaikuttaakin siltä, että ohjelmistojen myynti on mennyt laitemyyntiin edelle. Mobiilialustojen kirjo on varsin laaja, Apple käyttää omaa iOS-alustaansa, Windows Phone ja Android-alustat ovat laajalti käytössä useiden valmistajien kesken, Androidin johtajana markkinoita ylivoimaisesti. Windows Phone ja Apple iOS ovat tunnettuja siitä, että niille on hankala löytää maksuttomia ohjelmia. Joskin useiden ohjelmien kohdalla hinta on varsin alhainen, muutamalla eurolla saa pienempien ohjelmata-

lojen ohjelmia ja tunnettujenkin ohjelmien kohdalla puhutaan korkeintaan kymmenistä euroista. Androidille on myös tarjolla maksullisia ohjelmia ja monista ilmaisista ohjelmista onkin olemassa myös maksullinen versio. Maksu tuo mukanaan monesti käyttöön ohjelman täydet ominaisuudet tai / ja mainoksettomuuden. Androidille on kuitenkin tarjolla myös varsin hyviä ilmaisia ohjelmia etäkäyttöyhteyksiä varten.

### **3.4 Siirrettävä tieto**

On tärkeä tietää, millaista tietoa etäkäyttöyhteydellä on tarkoitus siirtää. Tämä vaikuttaa suuresti ohjelmiston ja tarvittavan tietoliikenneyhteyden nopeuden valintaan. Tekstipohjaisen tiedon siirtäminen onnistuu käytännössä kaikilla yhteysnopeuksilla pienen datasiirtomäärän ansiosta. Graafisen kuvan, videon ja äänen siirtäminen vaatii huomattavasti enemmän kapasiteettia siirtoverkolta. Tämä tulee ottaa huomioon suunniteltaessa etäkäyttöympäristöä ja laitteistoa. On myös huomioitava, että mobiililaitteilla käytettäessä saattaa esiintyä ylimääräisiä datasiirto-maksuja liikennemäärän ylittäessä tietyn rajan. Rajan ylittyessä myös siirtonopeuden rajoittaminen on mahdollista maksujen sijaan.

### **3.5 Tietoturva**

Tietoliikenneverkon välityksellä tapahtuvassa tiedonsiirrossa on aina huolehdittava riittävästä turvallisuudesta. Tietoturvan tasojen ollessa varsin moniportaiset, tärkeimpinä asioina voidaankin pitää järjestelmää käyttävien henkilöiden opastusta sekä teknisten tietoturvaratkaisujen onnistumista. Tietoturvan saattamiseksi riittävälle tasolle on jokaisen tapauksen kohdalla pohdittava ja huolehdittava erikseen vaaditun tietoturvatason saavuttamisesta. Tarpeellisten toimien määrittämisessä voidaan käyttää apuna SWOT-menetelmää.

Tärkeimpänä teknisenä ominaisuutena on liikenteen salaus. Kaikki etäkäyttöohjelmat eivät tue oletuksena tiedon salausta. Mikäli tietoa ei ole salattu, on se helposti kaapattavissa tietoliikenteen seasta. Tällöin väärin käsiin saattaa joutua esimerkiksi salasanoja ja muuta arkaluontoista tietoa. Joissakin tapauksissa onkin



syytä harkita ohjelmiston ulkopuolisen salaustekniikan käyttämistä. Varteenotettavia tekniikoita ovat esimerkiksi SSH- ja VPN-tekniikat.

Mikäli etäkäyttöyhteyden palvelin on avoinna ulkoverkosta tuleville yhteyspyynnöille, on huolehdittava riittävän vahvasta yhteydenmuodostuksessa käytettävästä salasanasta. Tarvittaessa voidaan käyttää automaattisia sulkulistoja ei-toivottujen kirjautumisyritysten estämiseksi. Myös yksityisen salausavaimen käyttöä voi harkita kohteissa, joissa käyttäjiä ei ole paljon. Tällöin kirjautuminen ei onnistu ilman salausavaintiedostoa. Salausavaimen kryptauksesta on huolehdittava siltä varalta, että salausavain päätyy väärin käsiin. Tällöin salausavaimen käyttäminen ei ole mahdollista ennen salauksen purkamista.

Loppukäyttäjän pääteohjelmistoja hankittaessa, tulee erityistä huomiota kiinnittää ohjelmiston valmistajaan. Ohjelmiston nimi ei vielä kerro riittävästi. On syytä varmistua siitä, että ohjelmiston valmistaja on luotettava. Varsinkin mobiilimarkkinoilla on tarjolla paljon harhaanjohtavasti nimettyjä ohjelmistoja, joiden valmistaja voi olla kuka vain. Tällaisten ohjelmistojen asentaminen saattaa vaarantaa tiedon turvallisen kulun ja tiedon joutumisen väärin käsiin.

### **3.6 Käyttäjämäärät**

Käyttäjämäärät vaikuttavat oleelliselta osalta käytettävän etäkäyttöohjelman valintaan. Pienten yksittäiskäyttöön tarkoitettujen järjestelmien asennus ja ylläpito on helppoa ja edullista. Suurissa käyttäjämäärissä on usein tarve käyttää useita samanaikaisia etäkäyttöyhteyksiä. Tämä asettaa laitteisto- ja tietoliikenneyhteyksille suurempia vaatimuksia. Mikäli käyttäjiä on paljon, eivät edulliset ja helppokäyttöiset etäkäyttöohjelmat ole yleensä ole riittäviä.

### **3.7 Käytön helppous**

Ohjelmistoa valittaessa tulee kiinnittää huomiota ohjelmiston ylläpidon helppouteen sekä loppukäyttäjän kannalta käytön helppouteen. Mikäli ohjelmiston ylläpitoon on käytettävissä vain pienet resurssit, tulisi ohjelmiston olla varsin helppohoitoinen ylläpidon sujuvuuden kannalta. Mikäli ylläpitoon ei ole riittäviä resurs-

seja, saattaa ohjelmiston hallinta jäädä esimerkiksi tietoturvapäivitysten kannalta vaarallisen paljon jälkeen.

Jotta valituista ratkaisuista olisi käyttäjilleen hyötyä, on ohjelmiston oltava riittävän helppokäyttöinen käyttäjälleen. Teknisesti hieno ratkaisu, jota kukaan ei halua käyttää ei ole kenenkään edun mukaista. Onkin syytä kiinnittää huomiota olemassa oleviin pääteohjelmiin ja niiden käyttöalustoihin. Erityisen tärkeäksi käytettävyyden osalta muodostuu mobiililaitteille suunnatut ratkaisut.

Mobiililaitteiden suuri kirjo asettaa omat vaatimuksensa ohjelmiston hankintaan. Kaikilla laitteille ei välttämättä ole tarjolla toimivaa pääteohjelmaa tai toisilla laitteilla käytettävyys on huomattavasti parempi kuin toisilla. Pääteohjelmia tarkasteltaessa tulee myös kiinnittää suurta huomiota pääteohjelman valmistajaan. Osa ohjelmista on hämäävästi nimetty alkuperäisen valmistajan mukaan tai lähelle sitä, pääteohjelman tekijän ollessa jokin ihan muu taho.

## 4 ETÄKÄYTTÖOHJELMAT JA TEKNIIKAT

Tässä luvussa käsitellään etäkäyttöohjelmien toimintoja ja niiden soveltuvuutta erilaisiin käyttötarkoituksiin. Ohjelmien kohdalla on perehdytty niiden ominaisuuksiin sekä tietoturvaan niiltä osin, kuin se on tarpeellista. Ohjelmien tietoturvaominaisuudet on kuitenkin syytä tarkistaa vielä ohjelman asennushetkellä, sillä tulevilla julkaisuilla ne ovat voineet muuttua. Yleensä tietoturva-asioissa muutoksien suunta on parempaan päin. Kuitenkin kaupallista arvoa tavoiteltaessa saatetaan ilmaiseksi ladattavien ohjelmien tietoturvaominaisuuksia karsia siinä toivossa, että käyttäjä siirtyisi ohjelman maksulliseen versioon.

### 4.1 Tekstipohjainen etäkäyttö

Tekstipohjainen etäkäyttö tarkoittaa kohdekoneen käyttämistä tekstipohjaisilla komennoilla. Tämä on yleisin etäkäyttötapa Unix- ja Linux-käyttöjärjestelmissä, joita voidaan hallita täysin tekstipohjaisesti. Myös Windows-koneille voidaan antaa tekstipohjaisia komentoja, pääkäytön tapahtuessa silti graafisesti.

Yksi yleisimmistä tekstipohjaisien etäkäyttöyhteyksien pääteohjelmista on Putty, jonka käyttöä on esitetty kuvissa 4 ja 5.

Tekstipohjainen etäkäyttö on tietoliikenteen kannalta erittäin suotuisa, sillä sen vaatima yhteysnopeus on lähes olematon. Perinteisillä analogisilla modeemeilla ja GPRS-yhteyksillä tekstipohjainen etäkäyttö onnistuu mainiosti.

#### 4.1.1 Telnet

”Internetin protokollat (niin verkkotason TCP ja UDP, kuin sovellustason Telnet, FTP jne.) on tehty alun perin pieneen luotettavaan verkkoympäristöön, jossa oleellista oli käyttäjiin luottaminen, samalla kun protokollien keveys ja palveluiden ohjelmoinnin helppous oli tärkeää.” (Oulun yliopisto. Tietoturvasivut).

Nykyaikaisen tietoturvan puuttuessa on Telnet vähitellen poistumassa käytöstä. Tästä syystä muun muassa Windows7 ei enää asenna Telnet-pääteohjelmaa oletuksena. Telnetin viimeaikainen käyttötarkoitus on ollut lähinnä aktiivilaitteiden

konfiguroinnissa paikallisella yhteydellä (ei tietoliikenneverkkojen yli). Telnet ei tue minkäänlaista salausta, joten sen liikenne on helposti luettavissa suojaamattomassa verkossa. Tämä mahdollistaa esimerkiksi salasanojen ja konfigurointiin liittyvien tietojen varastamisen tietoverkon kautta.

Telnetin puutteellisesta tietoturvasta johtuen sitä ei suositella käytettäväksi lainkaan verkkoliikenteessä. Mikäli sitä kuitenkin on pakko käyttää, on yhteyden salauksesta huolehdittava esimerkiksi SSH-tunnelin tai VPN:n avulla.

On kuitenkin erikoistapauksia, joissa Telnettiä voidaan käyttää ilman salausta. Telnetin ollessa täysin puhdasta tekstiä välittävä protokolla, voidaan sen avulla lähettää muihin tekstipohjaisiin palveluihin komentoja. Tällöin yhteyttä ei ole tarpeellista muodostaa Telnet-palvelimelle, vaan johonkin toiseen tekstipohjaiseen palveluun, johon ei tarvitse siirtää arkaluontoista dataa. Esimerkiksi WWW-palvelimen porttiin 80 voidaan ottaa yhteys Telnetillä ja syöttää WWW-palvelimen ymmärtämiä käskyjä yksitellen. (Fischer. 2014). Telnetin ominaisuuksia on esitetty taulukossa 2.

Viralliset Telnetille määritellyt portit ovat TCP 23 ja UDP 23. Käytännössä oletusporttina on poikkeuksetta TCP 23. (Internet Assigned Numbers Authority Service. 2014)

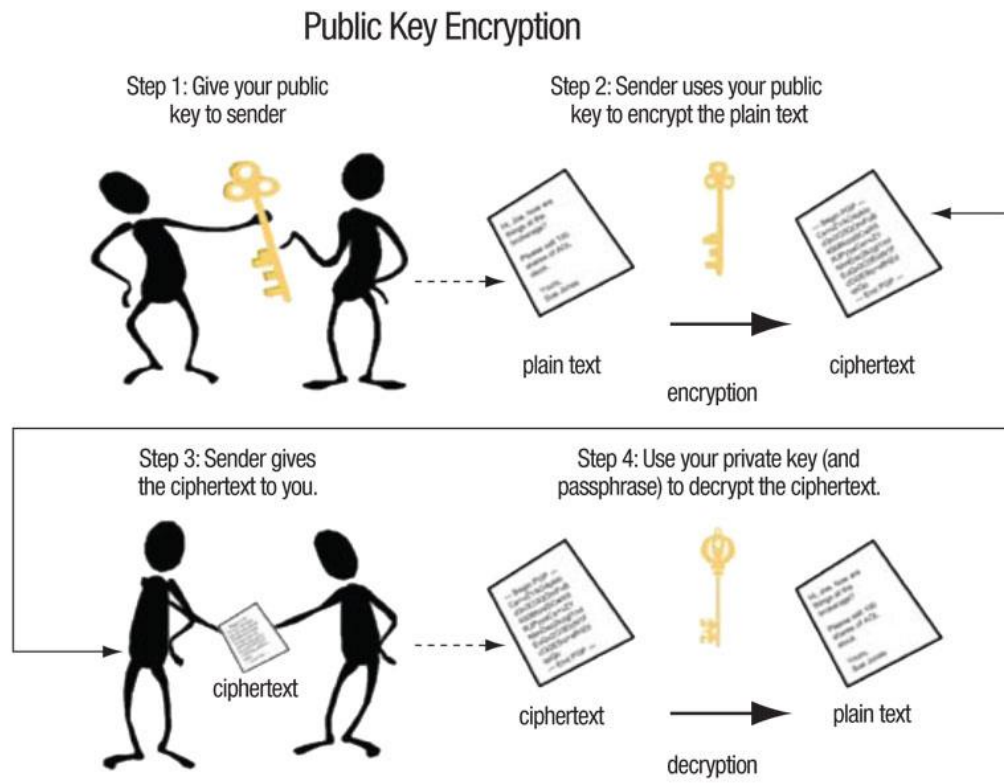
#### **4.1.2 SSH**

SSH (Secure Shell) on kehitetty korvaamaan turvattomat tekstipohjaiset etäkäyttöohjelmistot pääteyhteyksissä ja osittain FTP-ohjelmisto tiedostojen siirrossa. SSH pyrkii paikkaamaan edellä mainittujen ohjelmistojen puutteita esimerkiksi yhteyden salauksella ja palvelimen tunnistamisella. SSH tarjoaa myös mahdollisuuden putkittaa yksittäistä porttia käyttävän TCP-yhteyden salatun SSH-yhteyden yli. Putkitetussa yhteydessä muodostetaan ensin salattu SSH-yhteys kohdekoneeseen, minkä jälkeen SSH-yhteyden turvin käytetään suojaukseltaan heikompaa ohjelmaa, kuten esimerkiksi Telnettiä. Putkitusta voidaan verrata esimerkiksi sähköasennuksissa käytettävään muoviseen suojaputkeen, jonka sisällä

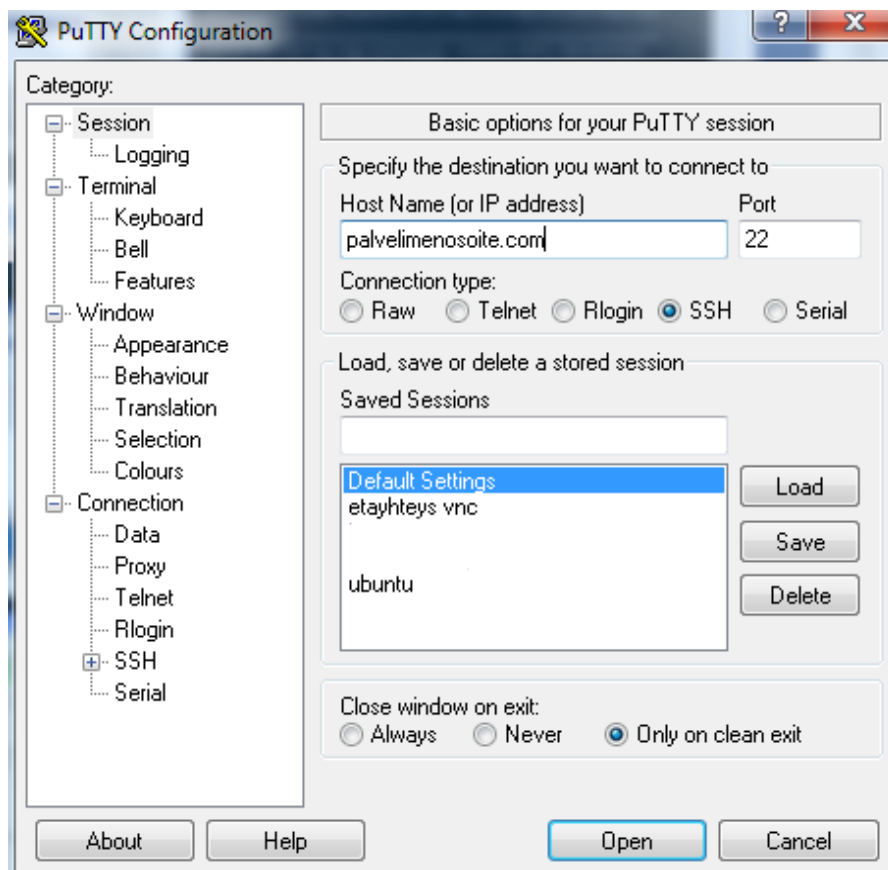
itse sähkökaapelit kulkevat. (Tampereen teknillinen yliopisto. Tieto- ja sähkötekniikan tiedekunta. Lintula 2009).

SSH autentikoi kohdekoneen julkisen avaimen tekniikalla. Se tarkoittaa, että käyttäjän (laitteen) on tunnettava kohdekoneen julkinen avain eli käytännössä ensimmäisellä yhteyskerralla kohdekoneen tarjoama julkinen avain. Käyttäjä autentikoi-tuu tämän jälkeen samalla tavalla, kuin olisi tavallisessa pääteyhteydessä kohde-koneeseen, käytännössä siis salasanalla. (Tampereen teknillinen yliopisto. Tieto-verkot ja tietoturva & Tietoturvallisuuden perusteet & jatko 2010) Julkisen avai-men autentikointia on esitetty kuvassa 3. SSH:n ominaisuuksia on esitetty taulu-kossa 2.

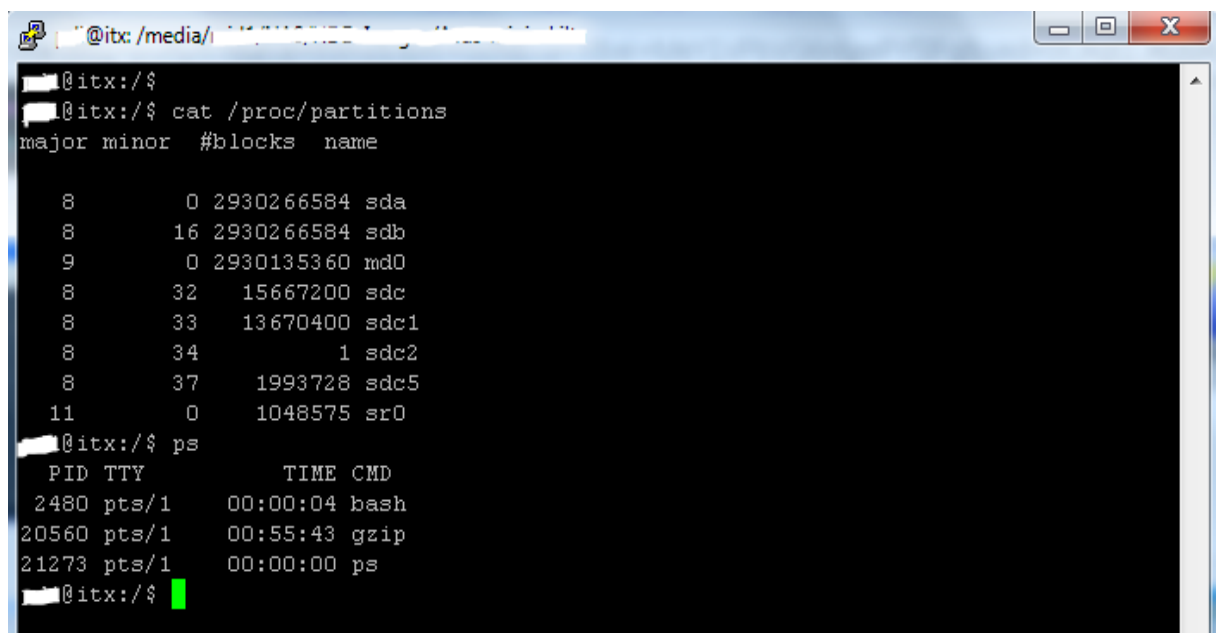
Viralliset SSH:lle määritellyt portit ovat TCP 22 ja UDP 22. Käytännössä oletu-sportti on poikkeuksetta TCP 22. (Internet Assigned Numbers AuthorityService. 2014)



Kuva 3. SSH-autentikointi julkisella avaimella. (Kuva: RTC Group Inc.)



Kuva 4. Puttyn käyttöliittymä.



Kuva 5. SSH-näkymä etäkoneelta Putty:lla.

Taulukko 2. Tekstipohjaisten etäkäyttöyhteyksien vertailu.

Ominaisuus	Telnet	SSH
Tekstipohjainen	Kyllä	Kyllä
Graafinen	Ei	Ei
Turvallisuus	Erittäin turvaton	Hyvä / Erittäin hyvä
Liikenteen tunnelointi	Ei	Kyllä
Siirtonopeusvaatimus	Erittäin matala	Erittäin matala / Matala
Helppokäyttöinen	Kyllä	Kyllä
Tuetut käyttöjärjestelmät pääteohjelmille	Kaikki	Kaikki
Tuetut mobiilikäyttöjärjestelmät pääteohjelmille	Kaikki	Kaikki
Tuetut käyttöjärjestelmät palvelinsovellukselle	Ei tuettu kaikissa, poistumassa käytöstä	Kaikki

## 4.2 Graafinen etäkäyttö

Graafinen etäkäyttö tarkoittaa kohdetietokoneen käyttämistä toisella tietokoneella tietoliikenneverkon yli (client käyttää serveriä). Tällöin serverin käyttöjärjestelmänä on graafinen käyttöjärjestelmä kuten Windows. Serveri-koneen kuva siirtyy tietoverkon välityksellä client-koneeseen, jolta käsin käyttö onnistuu, kuten oltaisiin serveri-koneen läheisyydessä.

Suurempien mittakaavojen etäkäyttö on yleistymässä. Tämä tarkoittaa satojen, jopa tuhansien käyttäjien järjestelmiä, joissa käyttäjät yhdistävät laitteillaan esimerkiksi yrityksen verkkoon. Verkon välityksellä he käyttävät ohjelmia ja virtuaalisyöpyitä suoraan palvelimen resursseilla. Jokaisella käyttäjällä on omat tunnukset, joilla he pääsevät käyttämään omaa virtuaalisyöpöytää. Tämä mahdollistaa edullisten päätelaitteiden hankkimisen ja raskaidenkin ohjelmien suorittamisen keskitetyin laiteresurssein. Keskittäminen parantaa myös huomattavasti yrityksen tietoturva, sillä kaikki tieto on talletettuna keskitetysti palvelimen tietovarastoon.



Kuvan siirtäminen vaatii aina enemmän kapasiteettia siirtoverkolta verrattuna tekstipohjaiseen tiedonsiirtoon. Käytännössä hyvin toimiva yhteys saavutetaan kahden megabitin tai sitä nopeammilla yhteyksillä. Hitailta yhteyksillä, kuten GPRS:llä tai analogisilla modeemeilla käyttö on erittäin hidasta tai mahdotonta.

Taulukossa 3 on vertailtu graafisten etäkäyttöyhteyksien ominaisuuksia.

#### 4.2.1 VNC (RFB)

VNC on pikselipohjaiseen kuvansiirtoon perustuva etäkäyttöprotokolla, joka pohjautuu RFB-protokollaan. Nykyään RFB-protokollaa kutsutaan useasti nimellä VNC.

VNC toimii frame buffer (kuvapuskuri) tasolla, jonka ansiosta se on yhteensopiva kaikkien verkkoyhteydellä varustettujen käyttöjärjestelmien kanssa. Lyhyesti sanottuna frame buffer toimii siten, että serverillä oleva kuva tallennetaan pikselitietona frame bufferiin, josta se lähetetään clientille sen sitä pyytäessä. Tällä tavoin tiedon määrää ja lähetyksenopeutta voidaan säädellä käytettävän laitteiston tehon sekä tietoliikenneyhteyden mukaan. (AT&T Laboratories Cambridge 1999).

VNC ei vaadi client laitteistolta suuria tehoja. Kaikki käytettävät ohjelmat käyttävät serverin resursseja, joten clientin tehotarve keskittyy lähinnä pikselitietojen käsittelyyn. Tämä mahdollistaa suurien ja raskaiden ohjelmien käyttämisen esimerkiksi miniläppäreillä tai mobiililaitteilla. (AT&T Laboratories Cambridge 1999).

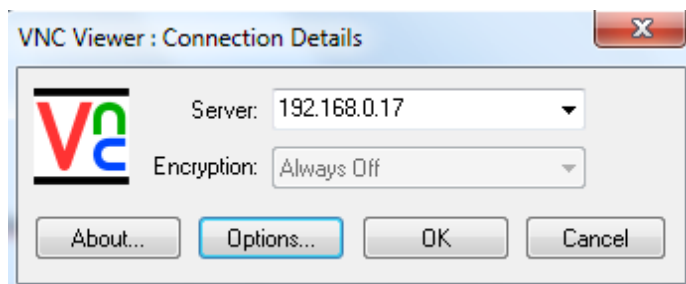
Mikäli yhteys VNC-serveriin jostain syystä katkeaa kesken käytön, ei meneillään ollut sessio nollaannu. Kun yhteys muodostetaan uudelleen serverille miltä tahansa koneelta, voidaan työskentelyä jatkaa siitä, mihin edellinen sessio jäi. (AT&T Laboratories Cambridge 1999).

Copy / paste (leikkaa / liimaa) ominaisuuksiltaan VNC tukee ainoastaan ISO 8859-1, eli Latin-1 merkistöä. Tämän johdosta erikoismerkkejä, kuten dollari-merkki \$ ja euro-merkki €, ei voida kopioida tai liittää clientin ja serverin välillä.

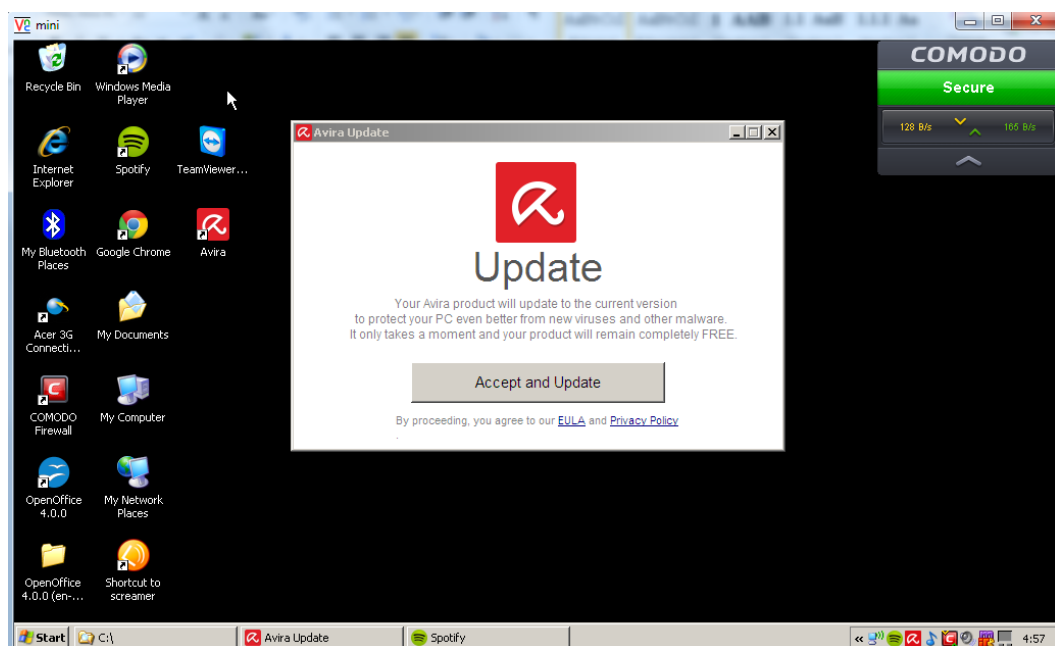
Myöskään kiinalaiset tai venäläiset merkit eivät ole tuettuina. (AT&T Laboratories Cambridge 1999).

VNC:n pohjana oleva RFB-protokolla ei itsessään tue tiedon salausta. VNC-ohjelmat voivat kuitenkin käyttää salausta, joka sovitaan keskenään serverin ja clientin kanssa. Usein ilmaiskäyttöön tarkoitetuista VNC-sovelluksista puuttuu salaus kokonaan. Maksullisissa versioissa salaus saattaa olla varsin hyvinkin ajan tasalla. Salauksen puuttuessa VNC-yhteyksiä ei tule käyttää suojaamattomissa verkoissa lainkaan. SSH-tunnelin kautta salaamatontakin VNC-yhteyttä on kuitenkin mahdollista ajaa luotettavasti. VNC käyttää oletusportina TCP 5900. (Richardson, Levine. 2011. The Remote Framebuffer Protocol; W3Schools. HTML ISO-8859-1 Reference.). VNC:n käyttöä RealVNC:llä on esitetty kuvissa 6 ja 7.

VNC:n (Virtual Network Computing) on kehittänyt alun perin Olivetti Research Lab (ORL) 1990-luvun lopulla. Nykyään kehitystä jatkavat VNC:n alkuperäiset kehittäjät RealVNC Ltd-nimisen yrityksen alaisuudessa. Yritys on perustettu vuonna 2002. (RealVNC Limited. Company background; Richardson, Wood 1998. The RFB Protocol.).



Kuva 6. Yksinkertainen RealVNC:n yhdistämisisikkuna.



Kuva 7. Työpöytä näkymä etäkoneelta RealVNC:llä.

#### 4.2.2 TeamViewer

TeamViewer on osakaupallinen ohjelma helppojen etähallintatoimintojen toteuttamiseen. Ohjelma on yksityiskäyttöön ilmainen ja kaupalliseen käyttöön maksullinen. Kaupallisen käytön lisenssimaksu on kertaluonteinen ja siksi varsin kohutuullinen.

TeamViewer on monipuolinen ja varsin helppokäyttöinen ohjelma. Sen avulla voidaan muodostaa perinteinen etäkäyttöyhteys, tiedostonsiirtoyhteys ja VPN-yhteys helposti. TeamViewer palvelinsovellus voidaan asentaa käynnistyväksi palveluna tietokoneen käynnistyksen yhteydessä tai sitä voidaan käyttää kerta-

luonteisena palvelimena käynnistämällä se yhdestä ainoasta tiedostosta (portable tilassa). Kertaluontoinen menetelmä on erinomainen vaihtoehto annettaessa etä-apua sitä tarvitsevalle käyttäjälle. Käyttäjän ei tarvitse osata, kuin klikata oikeasta ikonista tai osata ladata ja suorittaa tiedosto tietystä osoitteesta.

Vaikka ohjelma on yksityiskäyttöön ilmainen, on se silti monipuolinen ja turvallinen käyttää. Liikenteen salaus tapahtuu kättelyvaiheessa 2048-bittisellä RSA-algoritmin julkisen ja salaisen avaimen parilla. Turvallisen yhteydenmuodostuksen jälkeen liikenne salataan 256-bittisellä AES-salauksella. (TeamViewer 2014a)

RSA-algoritmi perustuu suurien kantalukujen käyttöön, jotka ovat nopeita ja helppoja luoda, mutta erittäin hitaita ja vaikeita muuttaa takaisin alkuperäiseen muotoonsa. RSA-salaus on 2048-bittisenä erittäin turvallinen. (Web-opas. Mikä on RSA?). AES-salaus (Advanced Encryption Standard) on valittu Yhdysvaltojen viralliseksi salausmenetelmäksi ei-salaisten dokumenttien osalta (Rouse. 2011). Normaalioloissa näiden kahden salauksen yhdistäminen luo erinomaisen tietoturvan etäkäyttöyhteydelle.

TeamViewerin palvelinohjelmisto on tarjolla Windows-, Linux- ja Mac-tietokoneille. Pääteohjelma on tarjolla Windows-, Linux- ja Mac-käyttöjärjestelmille sekä mobiilipääteohjelma Android-, iOS- sekä Windows Phone-käyttöjärjestelmille.

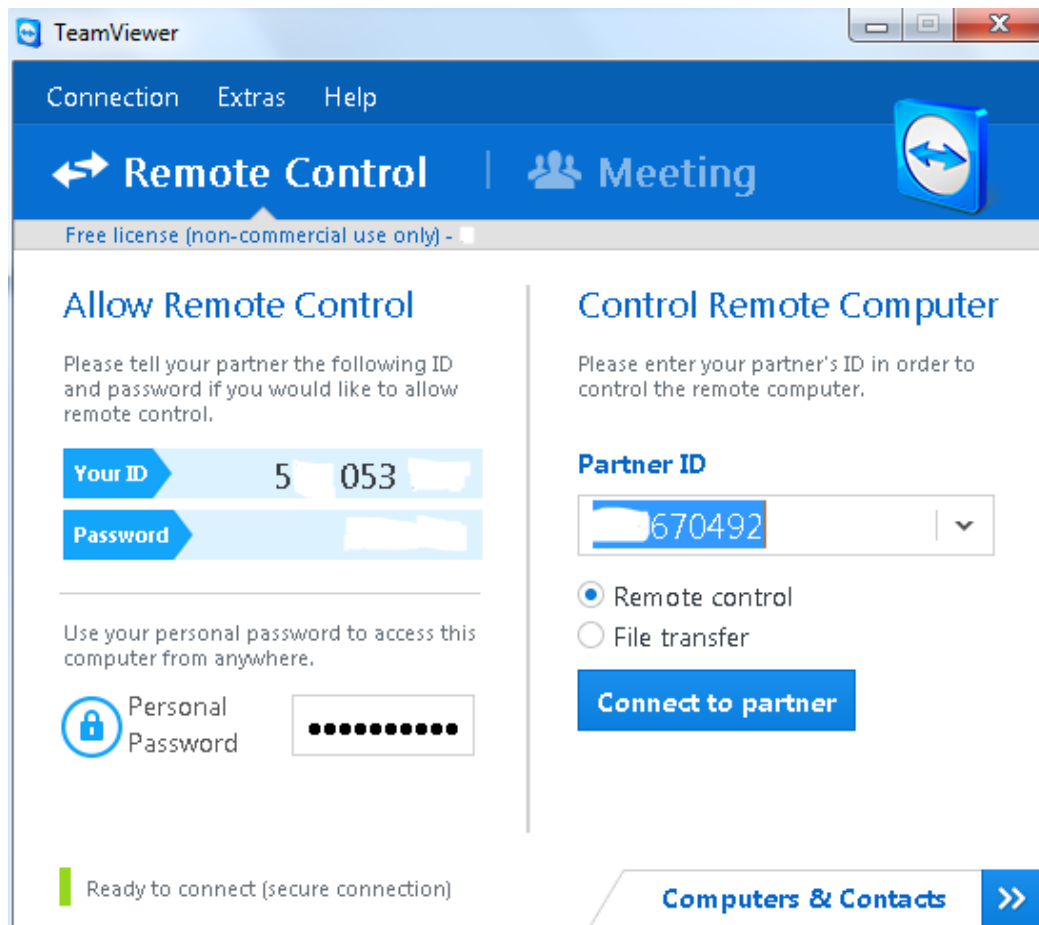
Yksi TeamViewerini kiistaton etu muihin etäkäyttöyhteyksiin nähden on sen kyky toimia palomuurin ja NAT:in takaa ilman konfigurointia. Tämä on mahdollista siten, että asennettu palvelinohjelmisto on jatkuvassa yhteydessä TeamViewerin omiin palvelimiin yhteyden muodostamisen mahdollistamiseksi. Koska yhteys on avattu palvelinohjelmistolta ulospäin, on silloin sisään tuleva vastaus sallittu. Etäkäyttäjän syöttäessä palvelinsovelluksen yhteystiedot, muodostuu yhteys aluksi TeamViewerin palvelimen kautta, jonka kautta ohjattuna yhteys on mahdollista muodostaa jo valmiiksi avoinna olevan keskusteluyhteyden ansiosta.

TeamViewerin kautta on mahdollista käyttää Wake-On-LAN –ominaisuutta, mikäli tietokoneen komponenteissa on tuki kyseiselle ominaisuudelle. Sen avulla

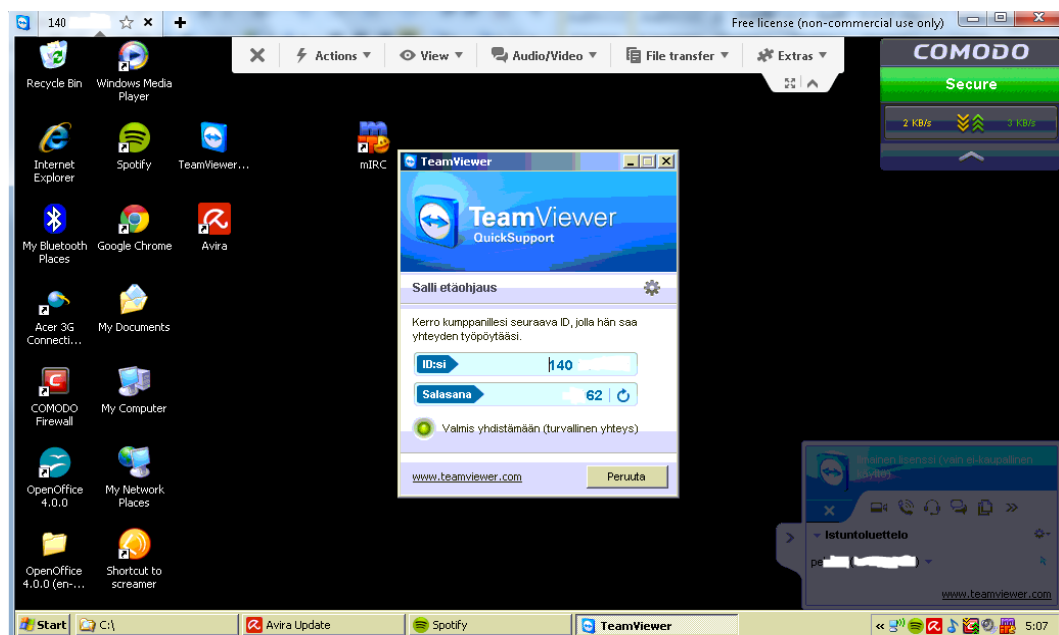
voidaan säästää kuluvia komponentteja sekä energiaa huomattavasti, sillä nukkuva tietokone voidaan käynnistää etänä tietoverkon yli. Ominaisuuden käyttäminen vaatii tietokoneen liittämistä verkkoon ethernetin avulla. (TeamViewer 2013)

Yhteyden muodostus julkisen verkon välityksellä TeamVieweriä käyttäen tapahtuu totutusta DNS-osoitteesta ja IP-osoitteesta poiketen. Ohjelmisto generoi yhdeksännumeroinen tunnuksen ja neljänumeroinen salasanan. Mikäli näitä ei tiedetä, ei yhteyden muodostaminen ole mahdollista.

Asetuksia muuttamalla TeamViewerin saa kuitenkin muutettua toimimaan pelkästään lähiverkossa, jolloin yhteys muodostetaan koneen nimeä tai lähiverkon IP-osoitetta käyttäen. (TeamViewer 2014b) TeamViewerin käyttöä on esitetty kuvissa 8 ja 9.



Kuva 8. TeamViewer näkymä. Palvelin ja yhdistäminen samasta ikkunasta.



Kuva 9. Työpöytä näkymä etäkoneelta TeamViewerillä.

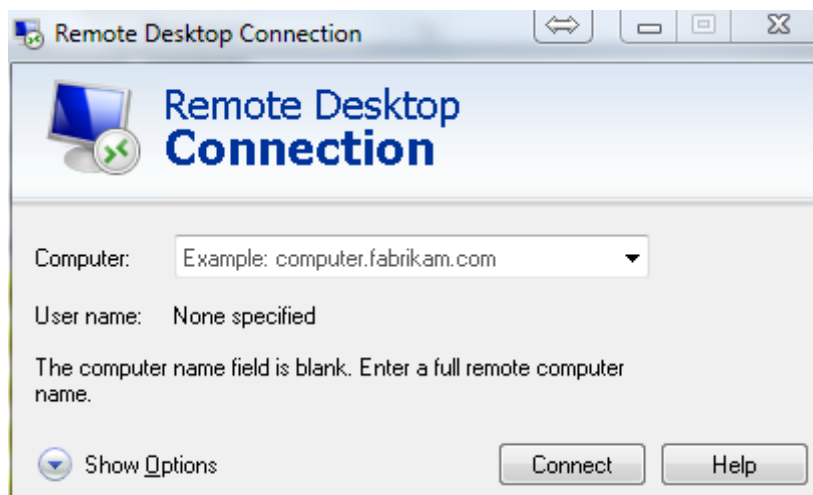
### 4.2.3 Remote Desktop Connection (RDC)

Microsoftin vastine VNC:lle on Remote Desktop Connection. RDC mahdollistaa kohdekoneen käytön tietoverkon yli toisella tietokoneella. RDC:n aikaisempia versioita on kutsuttu nimellä Terminal Server. Terminal Server esiteltiin ensimmäisen kerran Windows NT 4.0 käyttöjärjestelmän yhteydessä. Etäkäyttö on tuettuna kaikissa Windows7-käyttöjärjestelmissä, pois lukien Windows7 Starter ja Windows7 Home versiot, joissa ei ole Remote Desktopin käyttöä mahdollistavaa palvelinta. (Microsoft. 2014a; Microsoft. 2014b)

RDC käyttää Microsoftin kehittämää RDP-protokollaa. RDP mahdollistaa 64000 virtuaalikanavan käytön, joiden avulla RDP-protokollan sisällä voidaan siirtää monenlaista tietoa, kuten ääntä, tulostuskomentoja ja tiedostoja. (Microsoft 2014a; Microsoft. 2014c; Microsoft. 2014d; Microsoft. 2014e)

Oletuksena RDP-protokolla siirtää tietoa salattuna. Yhteensopivuuden takia oletussalaus on ”Client Compatible”, eli asetettu niin, että heikointakin salaussuokkaa käyttävä päätelaite voi muodostaa yhteyden palvelimelle. Tällöin tieto on salattu 56-bittisenä ja vain päätelaitteelta palvelimelle suunnassa. Palvelimelta päätelaitteelle suunta kulkee salaamattomana. Onkin tärkeää asettaa salaussuokka korkeimpaan mahdolliseen, jolloin tiedonsiirto on salattu molempiin suuntiin. Tällöin alemmaa salaussuokkaa tukevat päätelaitteet eivät voi muodostaa yhteyttä palvelimelle lainkaan. 56-bittinen salaus on nykypäivänä erittäin heikko, eikä sitä tulisi käyttää lainkaan. Mikäli alhaisia salaussuokkia joudutaan kuitenkin käyttämään, on suotavaa käyttää tietoturvan tason parantamiseksi muita suojauskeinoja, kuten SSH- tai VPN-yhteyksiä. (Microsoft. 2014f)

RDP käyttää oletuksena virallista porttia TCP 3389. (Microsoft. 2014g). RDC:n yhdistämisenäkymä esitettynä kuvassa 10.



Kuva 10. RDC yhdistämisenäkymä.

#### 4.2.4 Microsoft Remote Desktop Services (RDS)

Microsoft on kehittänyt etäkäyttösovelluksiaan huomattavasti viime vuosina. Aikaisemmin Terminal Services nimellä tunnettu palvelu on saanut uudistunut Windows Server 2008 R2 mukana. Nykyään Remote Desktop Services nimellä kulkeva palvelu, tai paremminkin palvelukokonaisuus, on todella monipuolinen ja kattava etäkäyttöympäristön mahdollistava kokonaisuus.

Perinteisiin VNC- tai SSH-yhteyksiin RDS-ratkaisuja ei voi verrata, sillä ne painivat täysin eri luokissa hinnan, hallittavuuden, käyttöönoton ja laitteistonkin puolesta.

RDS-ominaisuus on parhaimmillaan suurehkoissa ja suurissa yrityksissä. Vaikka RDS toisikin monissa pienissä yrityksissä huomattavia etuja, estävät ohjelmiston hankintakulut ja ylläpidon vaikeus sen taloudellisen käytön yrityksen omana järjestelmänä. Markkinoilla on kuitenkin useita yrityksiä, jotka tarjoavat omilta palvelimiltaan virtuaalipalvelimia tai räätälöityjä RDS-palveluita pienemmille yrityksille.



RDS:llä voidaan toteuttaa etäkäyttösovelluksia muun muassa: työpöytien, virtuaalikonien, ohjelmien, käyttäjähallinnan ja ohjelmistohallinnan osa-alueilla. (Microsoft. 2014h)

Yksi mielenkiintoisimmista ominaisuuksista on RemoteApp. RemoteApp on integroitu käyttäjän tietokoneen työpöytään siten, että etänä käytettävä ohjelma aukeaa tietokoneella kuten se olisi asennettuna itse koneelle. Todellisuudessa ohjelmaa ajetaan serverin resurssein. Käyttö on mahdollista myös www-sovelluksen kautta, jolloin ohjelmaa on mahdollista käyttää myös muilla kuin Microsoftin käyttöjärjestelmillä. (Microsoft. 2014i)

Etäyhteys, jolla käytetään palvelimelle luotua perinteistä työpöytää, on myös mahdollinen. Tämä kulkee nimellä Remote Desktop Session Host (RD Session Host). Työpöytää voidaan käyttää myös suoraan www-selaimella Remote Desktop Web Access -palvelulla. Tällöin käyttäjän koneella ei tarvitse olla erikseen asennettuja sovelluskomponentteja etäkäytön mahdollistamiseksi. Etuna tästä on, että etätyöpöydän käyttö onnistuu miltä tahansa koneelta. (Microsoft 2014 h; Microsoft. 2014j)

RDS-palvelun ominaisuuksia ja suorituskykyä voidaan tarvittaessa lisätä ja parantaa kolmansien osapuolien valmistamilla ohjelmilla. Yksi suosituimmista ohjelmistovalmistajista on Citrix Systems. Citrixin ohjelmien avulla voidaan laajentaa etäkäyttöohjelmien ominaisuuksia varsinkin paljon kuvaa ja ääntä sisältävien ohjelmien etäkäytössä. (TechTarget. 2009.)

#### **4.2.5 Linux LTSP**

Ilmainen Linux-vastine Microsoftin aikaisemmin Terminal Server -nimellä tunnetulle palvelulle on LTSP, eli Linux Terminal Server Project.

LTSP mahdollistaa työpöytien tai pelkkien ohjelmien ajamisen etäkoneella. Varsinainen ohjelmien prosessointi tapahtuu palvelimella, joten päätekone voi olla varsin vanha, joka ei enää välttämättä kelpaa muuhun käyttöön. Tällä saadaan esimerkiksi virastoissa ja julkisissa tiloissa edullisilla (jopa halvoilla) thin client-päätelaitteilla toteutettua asiakkaille käyttöpäätteet asioiden hoitamiseen tai henkilökunnalle työpisteestä riippumattomat työasemat.

Työasemien käynnistys voi tapahtua usealla tavalla. Mikäli laitteisto on yhdistetynä verkkoon langattomasti pitää työaseman käynnistysohjelma käynnistää esimerkiksi CD-levyltä tai disketiltä. Verkkoliitännäiset koneet jotka tukevat PXE (Preboot eXecution Environment) käynnistystä, voidaan käynnistää palvelimella sijaitsevasta käynnistystiedostosta. (LTSPedia 2013)

Käynnistystiedosto sisältää minimaalisen konfiguraation palvelimella olevan ohjelmiston lataamiseksi. Käynnistystiedosto sisältää muun muassa DHCP-palvelimen tiedot ja TFTP-palvelimen tiedot. Ohjelmisto ladataan päätelaitteelle TFTP:n kautta ja tallennetaan päätelaitteen keskusmuistiin. Tämän jälkeen avautuu graafinen käyttöliittymä, jonka tiedot tulevat suoraan palvelimelta. (LTSPedia 2013)

#### **4.2.6 Thin client**

Thin client on laitteistokokoonpanoltaan erittäin vaatimaton PC-tietokone. Laitteiston tarkoituksena on toimia päätteenä etäyhteyden muodostamiseen. Thin clientiin ei tallenneta mitään käyttäjän tietoja tai tiedostoja, vaan ne tallentuvat suoraan palvelimelle. Tämä mahdollistaa esimerkiksi toimistoissa vaihtuvien työpisteiden käytön, koska ei ole väliä mille päätteelle työntekijä asettuu. Kirjautuessaan päätteelle, hänen saa aina oman työpöytänsä käyttöön.

Thin clientien käyttö mahdollistaa edullisten päätteen käytön jokaiselle työntekijälle hankittavan työaseman sijaan. Laitteistoresurssit ja tallennusratkaisut voidaan keskittää yhteen pisteeseen, eli palvelimelle. Nopeiden tietoliikenneyhteyksien ansiosta palvelimen ei välttämättä tarvitse olla samassa tilassa käyttäjien

kanssa. Thin client-päätteitä käytetään yleensä Windows Server-palvelimien kanssa. (DevonIT 2014)

Taulukko 3. Graafisten etäkäyttöohjelmistojen vertailutaulukko.

<b>Ominaisuus</b>	<b>VNC</b>	<b>RDC</b>	<b>TeamViewer</b>	<b>RDS</b>
Graafinen	Kyllä	Kyllä	Kyllä	Kyllä
Tekstipohjainen	Ei	Ei	Ei	Ei
Turvallisuus	Ei ole (ilmainen) / hyvä	Heikko	Hyvä	Hyvä
Asiakasohjelman Helppokäyttöisyys	Helppo	Helppo	Erittäin helppo	Helpohko
Palvelimen helppokäyttöisyys	Helppo	Helppo	Erittäin helppo	Vaikea
Siirtonopeusvaatimus	Suuri	Suuri	Suurehko	Suuri
Käyttäjärühmät	Yksittäiseen käyttöön	Yksittäiseen käyttöön	Yksittäiseen käyttöön	Suurille käyttäjämäärille
Työpöydän etäkäyttö	Kyllä	Kyllä	Kyllä	Kyllä
Ohjelman etäkäyttö	Ei	Ei	Ei	Kyllä
Tiedoston siirto	Ei	Kyllä	Kyllä	Kyllä
Palvelinsovellus Windowsille	Kyllä	Kyllä	Kyllä	Kyllä
Palvelinsovellus Linuxille	Kyllä	Ei	Kyllä	Ei
Palvelinsovellus Macintoshille	Kyllä	Kyllä	Kyllä	Kyllä
Asiakasohjelma mobiililaitteille	Kyllä	Kyllä	Kyllä	Kyllä
Ilmainen yksityiskäytössä	Kyllä	Sis. Windowsin lisenssiin	Kyllä	Ei
Ilmainen yrityskäytössä	Kyllä	Sis. Windowsin lisenssiin	Ei	Ei
Hinta	Ilmainen / edullinen	Sis. Windowsin lisenssiin	Edullinen, kertamaksu.	Kallis

## 5 YHTEENVETO

Opinnäytetyö on tutkimusluontoinen eikä sille ollut toimeksiantajaa. Työn idea lähti liikkeelle tutkiessani erilaisten etäkäyttöyhteyksien ominaisuuksia omaan käyttöön. Havaintojeni perusteella etäkäyttöohjelmia on olemassa varsin paljon, joista osa on jo vanhentuneita. Tarjolla ei ollut suomenkielistä kattavaa vertailua, joka olisi ollut sisällöltään riittävän tekninen ja helposti ymmärrettävä.

Etäkäyttöyhteyksien yleistyminen tulee olemaan nopeaa nopeiden ja kasvavien mobiiliverkkojen sekä -laitteiden ansiosta. Lähtökohtaisesti etäkäyttöyhteyksistä, niiden ominaisuuksista ja soveltuvuuksista on saatavilla koottua tietoa varsin vähän. Tähän opinnäytetyöhön on pyritty keräämään peruspaketti tietoa, jota olisi mahdollista hyödyntää etäkäyttöyhteyksiä suunnitellessaan. Tässä työssä esiteltyjen tietojen lisäksi on kuitenkin syytä vielä perehtyä tarkemmin omiin tarpeisiin ja ratkaisuihin, sillä jokainen etäkäyttöympäristö on erilainen.

Oikeanlaisen etäkäyttöyhteyden valitseminen ja toteuttaminen vaatii varsin paljon tietoa verkko- ja salaustekniikoista. Mikäli tietoa ei ole helposti saatavilla, voi se johtaa pahimmassa tapauksessa suuren tietoturvariskiin huonosti toimivan kokonaisuuden lisäksi. Suurin havaitsemani ongelma löytyikin ilmaiskäyttöön tarkoitettujen ohjelmien tietoturvasta. Osa ilmaisista ohjelmista ei sisällä lainkaan tiedon salausta, jolloin etäyhteys on erittäin haavoittuvainen ja altis vakoilulle.

Maksullisien ohjelmien kohdalla hinnan lisäksi tulee kiinnittää huomiota maksun luonteeseen. Osa ohjelmista on kertamaksullisia ja sisältää oikeuden käyttää myös ohjelman tulevia (päivitettyjä) versioita. Tämän johdosta suhteellisen suuri kertamaksu muodostuu ajan kanssa edulliseksi vaihtoehdoksi, sillä kausiluontoisesti maksettavat lisenssit tapaavat kallistua ajan kanssa.

Onnistuneen ohjelmistovalinnan seuraukset näkyvät helppokäyttöisyytenä sekä ajan ja rahan säästönä tietoturvasta tinkimättä. Ohjelmiston valintaan kannattaakin keskittyä huolellisesti ja tarvittaessa käyttää ammattilaisten apua.

## LÄHTEET

AT&T Laboratories Cambridge 1999. Virtual Network Computing. Viitattu 15.9.2014. [http://www.hep.phy.cam.ac.uk/vnc\\_docs/howitworks.html](http://www.hep.phy.cam.ac.uk/vnc_docs/howitworks.html)

Axis Communications AB. 2014. Local area network and Ethernet. Viitattu 24.10.2014.  
[http://www.axis.com/products/video/about\\_networkvideo/ip\\_networks.htm](http://www.axis.com/products/video/about_networkvideo/ip_networks.htm)

Cisco Systems Inc. 1998.  
<http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm#xtocid166844>

Colliander Andreas. 1999. Viitattu 20.10.2014 [http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Essays/essee\\_OSI.html](http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Essays/essee_OSI.html)

DevonIT 2014. Thin Client Education. Viitattu 29.9.2014.  
<http://www.devonit.com/thin-client-education>

Fischer W. Check TCP Port 80 (http) with telnet. Viitattu 12.9.2014  
[http://www.thomas-krenn.com/en/wiki/Check\\_TCP\\_Port\\_80\\_\(http\)\\_with\\_telnet](http://www.thomas-krenn.com/en/wiki/Check_TCP_Port_80_(http)_with_telnet)

Internet Assigned Numbers AuthorityService 2014. Name and Transport Protocol Port Number Registry. Viitattu 22.9.2014.  
<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

IP-location. What is MAC Address? Viitattu 22.10.2014.  
<http://www.iplocation.net/tools/mac-address.php>

Koulutus- ja konsultointipalvelu KK Mediat. VPN-verkot. Viitattu 20.10.2014.  
<http://www.2kmediat.com/vpn/yhteys.asp>

Kouvolan seudun ammattiopisto. <http://www.koudata.fi/node/598>

LTSPedia 2013. How LTSP Works. Viitattu 28.9.2014.  
<http://wiki.ltsp.org/wiki/Concepts>

Microsoft. 2014a. Understanding the Remote Desktop Protocol (RDP). Viitattu 26.9.2014. <http://support2.microsoft.com/kb/186607>

Microsoft. 2014b. Remote Desktop Connection: frequently asked questions. Viitattu 26.9.2014 <http://windows.microsoft.com/en-us/windows/remote-desktop-connection-faq#1TC=windows-7>

Microsoft. 2014c. Connect to another computer using Remote Desktop Connection. Viitattu 26.9.2014 <http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7>

- Microsoft. 2014d. Developer Network. Remote Desktop Protocol. Viitattu 26.9.2014. [http://msdn.microsoft.com/en-us/library/aa383015\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa383015(VS.85).aspx)
- Microsoft. 2014e. Developer Network. [MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting. Viitattu 26.9.2014 <http://msdn.microsoft.com/en-us/library/cc240445.aspx>
- Microsoft. 2014f. TechNet. Configure Server Authentication and Encryption Levels. Viitattu 26.9.2014. <http://technet.microsoft.com/en-us/library/cc770833.aspx>
- Microsoft. 2014g. Support. How to change the listening port for Remote Desktop Viitattu 26.9.2014. <http://support2.microsoft.com/kb/306759>
- Microsoft. 2014h. Developer Network. Terminal Services Is Now Remote Desktop Services. Viitattu 27.9.2014. [http://msdn.microsoft.com/en-us/library/dd979766\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/dd979766(v=vs.85).aspx)
- Microsoft. 2014i. TechNet. Overview of RemoteApp. Viitattu 27.9.2014. <http://technet.microsoft.com/en-us/library/cc755055.aspx>
- Microsoft. 2014j. TechNet. Remote Desktop Services. Viitattu 27.9.2014. <http://technet.microsoft.com/en-us/library/cc770412.aspx>
- Mitchell B. Introduction to MAC Addresses. Viitattu 1.11.2014 <http://compnetworking.about.com/od/networkprotocols/a/introduction-to-mac-addresses.htm>
- Oulun seudun ammattikorkeakoulu, SWOT-analyysi. Viitattu 23.10.2014 <http://www.oamk.fi/hankkeet/pkk/pakki/nykytila2.htm>
- Oulun yliopisto. Tietoturvasivut. Viitattu 12.9.2014 [http://www oulu.fi/tietohallinto/tietoturva/sisalto/kayton\\_ohjeet/ssh-suojaus.html](http://www oulu.fi/tietohallinto/tietoturva/sisalto/kayton_ohjeet/ssh-suojaus.html)
- RealVNC Limited. Company background. Viitattu 24.9.2014. <http://www.realvnc.com/company/>
- Richardson T., Levine J. 2011. The Remote Framebuffer Protocol. Viitattu 20.9.2014. <http://tools.ietf.org/html/rfc6143>
- Richardson T., Wood K. R. 1998. The RFB Protocol. ORL Cambridge. Viitattu 16.9.2014. [http://www.hep.phy.cam.ac.uk/vnc\\_docs/rfbproto.pdf](http://www.hep.phy.cam.ac.uk/vnc_docs/rfbproto.pdf)
- Rouse M. 2005. UDP (User Datagram Protocol). Viitattu 22.10.2014 <http://searchsoa.techtarget.com/definition/UDP>
- Rouse M. 2014. TCP (Transmission Control Protocol). Viitattu 19.10.2014 <http://searchnetworking.techtarget.com/definition/TCP>
- Rouse, M. 2011. AES (American Encryption Standard). Viitattu 24.10.2014. <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

RTC Group Inc. Viitattu 27.10.2014.

[http://rtcmagazine.com/files/images/2007/rtc1103tc\\_lant1\\_large.jpg](http://rtcmagazine.com/files/images/2007/rtc1103tc_lant1_large.jpg)

Service Name and Transport Protocol Port Number Registry. 2014. Viitattu

20.10.2014. <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Suomen Hostingpalvelu OY. 2010. Viitattu 23.10.2014

<https://www.hostingpalvelu.fi/ohjeet/yleiset-ohjeet/mika-on-domainin-nimipalvelinnimipalvelu-dns/>

Tampereen teknillinen yliopisto. Tieto- ja sähkötekniikan tiedekunta. Lintula.

2009. Viitattu 22.9.2014 <http://www.cs.tut.fi/lintula/software/ssh/teoria.shtml>

Tampereen teknillinen yliopisto. Tietoverkot ja tietoturva & Tietoturvallisuuden perusteet & jatko 2010. Viitattu 22.9.2014.

<https://sec.cs.tut.fi/maso/materiaali.php?id=79>

TeamViewer 2013. TeamViewer 9 Manual. Wake-on-LAN. Viitattu 3.10.2014.

<http://www.teamviewer.com/en/res/pdf/TeamViewer-Manual-Wake-on-LAN-en.pdf>

TeamViewer 2014a. TeamViewer FAQ. How secure is TeamViewer? Viitattu

29.9.2014. <http://www.teamviewer.com/en/help/14-How-secure-is-TeamViewer.aspx>

TeamViewer 2014b. TeamViewer FAQ. Can TeamViewer be used within a local network (LAN) only? Viitattu 3.10.2014.

<http://www.teamviewer.com/en/help/40-Can-TeamViewer-be-used-within-a-local-network-LAN-only.aspx>

TechTarget. 2009. What is Citrix HDX?. Viitattu 28.10.2014.

<http://searchvirtualdesktop.techtarget.com/news/1370602/What-is-Citrix-HDX>

W3Schools. HTML ISO-8859-1 Reference. Viitattu 23.9.2014.

[http://www.w3schools.com/charsets/ref\\_html\\_8859.asp](http://www.w3schools.com/charsets/ref_html_8859.asp)

Web-opas. Mikä on DHCP? Viitattu 23.10.2014

<http://www.webopas.net/dhcp.html>

Web-opas. mikä on RSA? [http://www.webopas.net/mika\\_rsa.html](http://www.webopas.net/mika_rsa.html)

Web-opas. Mikä on TCP/IP? Viitattu 19.10.2014

[http://www.webopas.net/mika\\_tcpip.html](http://www.webopas.net/mika_tcpip.html)