VIDEONEUVOTTELUJÄRJESTELMÄT

Tietoturvallisuus avoimessa ja suljetuissa verkkoratkaisuissa

LAHDEN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma
Yritysviestintäjärjestelmät
Opinnäytetyö
Syksy 2006
Juho Tietäväinen

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

TIETÄVÄINEN, JUHO:

Videoneuvottelujärjestelmät
Tietoturvallisuus avoimessa ja suljetuissa verkkoratkaisuissa

Yritysviestintäjärjestelmien opinnäytetyö, 32 sivua

Syksy 2006

TIIVISTELMÄ

Tämä opinnäytetyö tutkii erilaisia käytettäviä mahdollisuuksia videoneuvottelun järjestämiseen sekä avoimessa että suljetuissa verkkoratkaisuissa. Teoriaosassa tutkitaan videoneuvottelua käsitteenä, tietoliikenneratkaisuja, millaisia tietoturvallisia ohjelmistoja on olemassa sekä käytettäviä suojausvaihtoehtoja.

Empiirisessä osuudessa perehdytään avoimessa verkossa tapahtuvaan Päijät – Hämeen Koulutus Konsernin L – videonet videoneuvottelujärjestelmään. Siinä selvitetään mitä se sisältää, onko se suojattu riittävän tehokkaasti ja voitaisiinko sitä kenties vielä parantaa. Vertailukohtana opinnäytetyö käyttää Heinolan Opetusalan Koulutuskonsernin suljetussa MPLS – yritysverkossa tapahtuvaa videoneuvottelujärjestelmää.

Lähteinä opinnäytetyössä on käytetty alaan liittyviä internetlinkkejä, sekä käyty paikan päällä haastattelemassa PHKK:n videonetin ja OPEKON henkilöstöä, sekä keskusteltu heidän kanssaan sähköpostin välityksellä. Tietoa on myös hankittu perehtymällä aiheeseen liittyvään kirjallisuuteen.

Tuloksien perusteella voidaan selvästi todeta, että erilaisiin käyttötarkoituksiin soveltuvat hieman erilaiset videoneuvottelun tietoliikenneratkaisut. ISDN-yhteyksillä tulisi suojata neuvottelutilanne palomuureilla, kun taas IP- yhteydellä kannattaa käyttää suojattuja verkkoratkaisuja.

Avainsanat: Videoneuvottelu, tietoturvallisuus, suojaus, ISDN – yhteys, palomuuri, IP- yhteys, verkkoratkaisu

Lahti Polytechnic
Faculty of Business Studies

TIETÄVÄINEN, JUHO:

Video Conferencing Systems
Data security in public and closed network solutions

Professional Development in Education, 32 pages

Autumn 2006

ABSTRACT

This research deals with possibilities of using video conference in closed network and in open network. In theory video conference is examined in common, network solutions and using softwares with enough data security.

In the empirical part we orientate to L- Videonet video conferencing system of Lahti Region Educational Consortium. In that part we examine content of it, if it has enough data security and could it be more secure. In additionally Heinola's National Centre For Professional Development in Education's closed network, MPLS – enterprise network is examined and also what benefits can be gained and how to use that network effectively.

Sources for this thesis are obtained from related hyperlinks. LREC's and NCFPD's organizations have been visited and personnel have been interviewed. Also information has been acquired via E-mail. Furthermore information has been acquired from literature based on video conferencing.

In conclusion we can mention that different video conferencing types excel in different usage. ISDN and IP-connections are researched more specifically and their benefits and deficiencies are explained more accurately.

Key words: Video conference, Data security, ISDN – connection, firewall, IP-connection, MPLS-enterprise network

1 JOHDANTO

Videoneuvottelu on reaaliaikaisesti tapahtuvaa kuvan, äänen sekä mahdollisesti myös tiedostojen välittämistä paikasta A paikkaan B tai useisiin muihin paikkoihin. Tällä mahdollistetaan esimerkiksi kokouksien pitäminen niin, ettei osanottajien tarvitse olla samassa paikassa vaan osanottajat voivat olla vaikka toisella puolella maailmaa. Osanottajat pystyvät siltikin näkemään vastapuolen ilmeet, eleet ynnä muut toimet, jotka saattavat olla ratkaiseva osa kokouksen suorittamisessa. (Kuusinen 2000)

Videoneuvotteluprosessien kehitys lähti nousuun 1990- luvun loppupuolella, jolloin yleistyivät ISDN-yhteydet. Tällöin kuitenkin kuvan ja äänen laatu olivat vielä melkoisen heikkoja. Nykyisin suosiotaan kasvattaneet xDSL-internet laajakaistayhteydet ovat lähes jokaisella videoneuvotteluprosesseja käyttävällä henkilöllä kaapeliyhteyden ohella käytössä. XDSL- sekä kaapeliyhteydellä saadaan tiedonsiirrosta huomattavasti nopeampaa ja kuvan- ja äänenlaadusta entistä parempaa. (Kuusinen 2006)

Videoneuvotteluprosessien kohdalla tapahtunut kehitys on mahdollistanut järjestelmän hankkimisen jokaiseen kotiin. Kustannukset ovat minimaaliset ja laitteisto on kaikkien saatavilla. Erityisesti yritys- sekä opiskelukäyttöön on lisätty ja tullaan lisäämään videoneuvottelujärjestelmiä siitä saatavien säästöjen takia. (Rönkä 2003)

Videoneuvottelujärjestelmät voidaan karkeasti jakaa kahteen eri osaan: Kahden pisteen välillä tapahtuvaan neuvottelutilanteeseen, jossa esimerkiksi luennoitsija omalta työpisteeltään luennoi videon ja äänen välityksellä yhteen koneeseen, sekä monen pisteen väliseen neuvottelutilanteeseen, jossa luennoitsija luennoi useaan eri koneeseen. (Kuusinen 2000)

Tavoitteena videoneuvotteluverkon perustamisessa voisi olla esimerkiksi opiskelijoiden tasa-arvoisuuden parantaminen, jolloin saataisiin opetus kaikkien opiskelijoiden saataville laitoksen toimipisteestä ja maantieteellisestä sijainnista huolimatta. (Kuusinen 2000)

Kaikessa Internetissä käytävässä tiedonsiirrossa, kuten myös videoneuvotteluissa, on omat riskinsä. Erityisesti lähetettäessä tietoa, jota ei haluta saattaa ulkopuolisiin käsiin, on syytä perehtyä videoneuvottelun tietoturvallisuuspuoleen. Videoneuvottelua voidaan pitää joko avoimessa tai suljetussa verkkoympäristössä, ja suojaaminen tapahtuu verkkoratkaisuista riippuen. Erityisesti yritysten, jotka käyttävät videoneuvottelua esimerkiksi kokouksien pitämisessä yhdistäen monen paikkakunnan toimistot ja siirtävät salaista tietoa, tulisi hoitaa datan säilyminen vain asianomaisten keskuudessa. Asianomaiset voidaan tunnistaa esimerkiksi käyttäjätunnusten ja salasanojen avulla. (VIDERA 2006)

2 TUTKIMUSASETELMA

2.1 Tutkimusongelmat

Tämän opinnäytetyön tehtävänä ja tavoitteena on selvittää mitä videoneuvottelujärjestelmä sisältää, millaiset ovat yleisimpiä tietoturvaratkaisuja sekä tutkitaan tietoliikenneverkkoja. Empiirisessä osiossa käydään läpi kahden organisaation käyttämiä videoneuvotteluverkkoja, toinen sisäisessä verkkoratkaisussa, toinen ulkoisessa.

Opinnäyte tutkii ensiksikin avoimessa verkossa käytävän videoneuvottelun suorittamista Virtual Private Networkin avulla. Lisäksi tutkitaan tarvittavia palomuuriasetuksia ja verkon suojaamista käyttäjätunnusten ja salasanojen avulla. Avoimesta verkosta esimerkkinä käytetään Case-osiossa olevaa Päijät – Hämeen koulutuskonsernin L – videonet – videoneuvotteluverkkoa.

Suljetuissa verkoissa tutkitaan lähiverkossa tapahtuvan videoneuvottelukokouksen tietoturvaa. Lisäksi tutkitaan intranetin sekä MPLS – yritysverkon käyttöä. Opinnäytetyö vastaa kysymyksiin onko tietoturva suljetuissa verkoissa riittävää ja millä tavoin sitä voitaisiin mahdollisesti parantaa. Case – osiossa suljetuista verkoista esimerkkinä on Heinolan Opetusalan koulutuskeskuksen suljettu MPLS – yritysverkko.

Videoneuvotteluohjelmistoista opinnäytetyössä esittelee Microsoftin NetMeeting – ohjelmiston, sillä se on yleisesti tunnetuin. Vertailun vuoksi mukaan on otettu Marratech ja Xenex Visual Meeting - ohjelmistot. Opinnäytetyössä tutkitaan ohjelmistojen käytettävyyttä, ominaisuuksia sekä tietysti tietoturvaa.

Tutkimuskohteena on Lahden seudun avoin videoneuvotteluverkko, L-Videonet, johon kuuluvat Päijät-Hämeen Koulutuskonsernin liikelaitoksen yhteensä 17 eri

toimipistettä ja noin 12 000 opiskelijaa. Videoneuvotteluverkon kustannusarvioksi on laskettu 470 808 euroa, rahoituksesta 70% saadaan EU:lta.

Toinen tutkimuskohde on vastaavasti suljetussa MPLS – yritysverkossa toimivan Heinolan Opetusalan koulutuskonsernin videoneuvotteluverkko. Molempien organisaatioiden tietoturvavastaavia on haastateltu ja pohdittu yhdessä heidän kanssaan videoneuvottelujärjestelmiensä tietoturvaratkaisuja.

2.2 Tutkimusmenetelmät

Tutkimukseen on käytetty Internetissä olevaa yleistä videoneuvottelua käsittelevää tietoa, kirjallisuutta, lehtileikkeitä sekä haastateltu ja kuultu casenakin käytettyyn L-Videonetiin ja OPEKO:on liittyvää henkilöstöä.

2.3 Tutkimuksen esittely

Tutkimus alkaa johdannolla, jossa esitellään opinnäytetyön rakenne, selvitetään mitä opinnäytetyö pitää sisällään sekä tutkitaan erilaisia mahdollisia tietoturvallisia yhteystyyppejä. Johdannossa tutkitaan myös videoneuvotteluja käyttävien organisaatioiden henkilökunnan mielipiteitä tietoturvallisuudesta ja mietitään niiden riittävyyttä.

Toisessa luvussa selvitetään tutkimusongelmat sekä – menetelmät ja rajataan tutkimus koskemaan vain tiettyjä asioita. Lisäksi esitetään tutkimus. Lopuksi määritellään ja rajataan tutkimuksen rakenne.

Luvussa 3 perehdytään videoneuvottelujärjestelmiin, millaisia niitä on ja mitä niiltä vaaditaan. Lisäksi käydään läpi ohjelmistoja, erityisesti perehdytään yleisimpään Microsoftin ilmaiseen NetMeeting- videoneuvotteluohjelmistoon ja sen erilaisiin ominaisuuksiin. Vertailun vuoksi mukaan on otettu kaksi muutakin ohjelmistoa, Marratech sekä Xenex Visual Meeting.

Neljännessä luvussa perehdytään videoneuvottelujärjestelmien laitteistoon, mitä vähimmillään sekä enimmillään videoneuvottelulaitteistolta vaaditaan. Samaan lukuun on sisällytetty tietoliikenneratkaisut, joista tutkitaan yhteystyypit sekä niissä käytettävät standardit.

Viides luku tutkii avoimessa verkossa eli internetissä käytävän videoneuvottelun tietoturvaa suojatun ulkoisen tietoverkon, Virtual Private Networkin, avulla ja lisäksi luvussa tutkitaan palomuurien ja salasanojen hyödyntämistä.

Luvussa 6 tutkitaan suljettujen tietoverkkojen ominaisuuksia ja kuinka hyvin niiden avulla voidaan saada tietoturvallinen videoneuvotteluverkko aikaan. Verkkotyypeistä käsitellään erityisen tarkasti lähiverkko (ethernet, token ring) sekä videoneuvottelukäytössä yleistymässä oleva MPLS – yritysverkko. Lisäksi selvitetään intranetin käyttö videoneuvottelukokouksen suojaamiseksi.

Luku 7 on Case-osio, jonka ensimmäisessä alaotsikossa on haastateltu Päijät-Hämeen Koulutuskonsernin tietoliikenne vastaavaa, Pekka Eerolaa koskien avointa L-videonet - videoneuvotteluverkkoa. Luvussa tutkitaan videoneuvotteluverkkoa niin laitteiston kuin tietoturvaratkaisujen osalta.

Samaan lukuun on sisällytetty vertailun vuoksi tietoa Heinolan Opetusalan Koulutuskeskuksen, OPEKOn, käyttämästä suljetusta MPLS - videoneuvotteluverkosta. Haastateltavana on ollut tietoliikennevastaava Jari Nokelainen.

Luvussa 8 suoritetaan opinnäytetyön yhteenveto ja tutkaillaan saatuja tuloksia sekä ovatko ne kaikin puolin riittäviä, sekä selvitetään jatkotutkimuksen tarve.

2.4 Tutkimuksen rakenne ja rajaus

Tutkimus on rakennettu käsittelemään pintapuolista tutkiskelua tarkemmin videoneuvotteluprosesseja niin avoimessa kuin suljetuissakin verkkoratkaisuissa tietoturvallisuuden osalta. Tässä opinnäytetyössä erityisesti kohdistutaan VPN

(Virtual Private Network) -yhteyden tarjoamiin vaihtoehtoihin salauksen varmistamiseksi avoimessa tietoverkossa. Vertailun vuoksi suljetuista verkoista opinnäytetyö tutkii lähiverkon ja MPLS – yritysverkon ominaisuuksia.
Casena tutkimustyössä käytetään kirjoitushetkellä työn alla olevan Lahden seudun avoimen videoneuvotteluverkon perustamisprosessia, jota tutkitaan lähemmin luvussa 7 Case - osuus. Toinen näkökulma saadaan Heinolan Opetusalan Koulutuskeskuksen suljetusta MPLS - videoneuvotteluverkosta.

Tutkimus rajataan koskemaan avoimen verkon osuudessa Virtual Private Networkia sekä käyttäjätunnuksia ja salasanoja tietoturvallisuuden varmistamiseksi. Suljettujen verkkojen osalta tutkimus rajataan koskemaan lähiverkkoa, MPLS – yritysverkkoa sekä intranetiä.

3 VIDEONEUVOTTELUOHJELMISTOJA

Videoneuvotteluohjelmistoja on nykyään markkinoilla aina ilmaisista versioista tuhansia euroja maksaviin videoneuvottelukokonaisuuksiin. Tässä osiossa opinnäytetyö tutkii kolmea videoneuvotteluohjelmaa, Microsoftin NetMeetingiä, Marratechia sekä Xenexin Visual Meetingia.

3.1 Microsoft NetMeeting

Microsoft NetMeeting – videoneuvotteluohjelma on ilmainen ja ladattavissa Microsoftin kotisivuilta osoitteessa http://www.microsoft.com. Ohjelma on myös saatavana Microsoftin kaikissa Windows 95- käyttöjärjestelmää uudemmissa käyttöjärjestelmissä (WINDOWS 98/NT/2000/XP). Ohjelma löytyy lueteltujen käyttöjärjestelmien asennuslevykkeeltä, käyttökieleksi voidaan valita joko suomi tai vaihtoehtoisesti englanti. (Nykänen 1998)

NetMeeting nimensä mukaisesti mahdollistaa kokouksien pitämisen verkon välityksellä, osallistujia voi olla yksi tai useampia samanaikaisesti. Yhteyden muodostaminen on yksinkertaista, joko soittamalla suoraan vastapuolen IP -osoitteeseen tai kirjoittautumalla jollekin NetMeeting – palvelimelle. Palvelimelta voidaan tämän jälkeen valita kokouskumppani. (Nykänen 1998)

Tietenkään MS NetMeetingin käyttö ei ole täysin ongelmatonta. Aina kun ohjelmistoja käytetään vuorovaikutuksessa toisten kanssa, on mahdollisuus toisen koneen tiedostojen poistamiseen, joko vahingossa tai tahallisesti. Myös ohjelman vastapuolen käyttäjän identiteetin varmistaminen voi olla hankalaa. ”Toisen nimellä” voidaan kirjautua palvelimelle, jos vain salasana ja käyttäjätunnus ovat tunkeutujan tiedossa. (Nykänen 1998)

NetMeetingin laajamittainen yhteiskäyttö vaatii myös nopeaa yhteystyyppiä, tietenkin tähän voidaan vaikuttaa äänenlaatua sekä grafiikkaa säätämällä huonommaksi. (Nykänen 1998)

Windowsin eri käyttöjärjestelmät sekä kieliversiot saattavat aiheuttaa ongelmia, välilyönnit hakemistojen nimissä ja erilaiset fontit saattavat aiheuttaa sekaannusta NetMeeting – ohjelmassa ja näin ollen aiheuttaa ohjelman välittömän jumiutumisen ja kaatumisen. (Nykänen 1998)

NetMeetingin avulla kokouskumppanit voivat hoitaa kirjallisen kommunikoinnin Chatilla, sekä Windows-sovellusten jakamisen erityisen Whiteboard -ohjelman avulla.

3.1.1 NetMeeting Chat

NetMeeting Chat mahdollistaa tutun jutustelun kokouksen eri osapuolten välillä. Viestejä on mahdollista lähettää kerralla joko koko ryhmälle tai "salaa" vain yksittäiselle jäsenelle. Keskustelutiedostojen tallettaminen omalle kovalevylle on mahdollista itse määriteltyyn kansioon. (Nykänen 1998)

3.1.2 NetMeeting Videokonferenssi

Videokonferenssi - ominaisuus mahdollistaa point-to-point -tyyppisten videoyhteyksien muodostamisen kokoushenkilöiden välillä. Käytännössä tämä tarkoittaa sitä, että kokous voi enimmillään jakautua kahden jäsenen työryhmiin, joista jokainen on näkö- ja kuuloyhteydessä keskenään vain ja ainoastaan pareittain. Luennointi usealle kuulijalle ei siis peruskokoonpanolla onnistu. Kokouskumppanien dynaamisella vaihtamisella tätä rajoitetta on mahdollista hieman heikentää. Ongelma ratkeaa erilaisten kaupallisten NetMeeting-palvelimien käytöllä. (Nykänen 1998)

3.1.3 NetMeeting Tiedostojen jakaminen

Tiedostojen jakaminen on mahdollista joko koko kaikille kokouksen osallistujille tai vain valitulle osallistujille. Vastaanottajat tallentavat vastaanotetut tiedostot automaattisesti vastaanottajan koneen paikalliseen NetMeetingin kansioon, josta käsin tiedostojen manipulointi on tuttuun Windows-tyyliin mahdollista. (Nykänen 1998)

3.2 Marratech – videoneuvotteluohjelmisto

Marratech – videoneuvotteluohjelmistolla yhteys muodostetaan suojattuun verkkoympäristöön, jossa voidaan siirtää korkealaatuista puheääntä VoIP-yhteydellä, käyttää interaktiivisia työtauluja, jakaa tietoa sekä asiakirjoja ja lähettää Chat - viestejä ryhmissä tai kahden kesken. Käyttäjät ovat näköyhteydessä keskenään web-kameroiden avulla.

Marratech käyttää H.323 –standardin suojausta eli on käytettävissä IP – yhteystyypeissä (xDSL ja kaapeli). Näin ollen yhteyden suojaamiseksi pienen toimiston tarpeisiin tai kotikäyttöön vaaditaan palomuuri. Suurissa yrityksissä suojaustarpeet ovat usein vaativammat, joten silloin vaaditaan yhteydeksi suojattu yrityksen sisäinen verkko. (Marratech 2005)

Ohjelmisto on 5 osaan jaettuna seuraavanlainen: Participants, Video, Whiteboard, Voice over IP ja Chat (KUVIO 1).

3.2.1 Marratech Participants

Marratech – participants –kohdasta näet listalla kirjautuneena olevat käyttäjät. Kaikkien käyttäjien videokuva näkyy reaaliaikaisena pienessä ikkunassa listalla.

3.2.2 Marratech Video

Kun haluat katsella tietyn käyttäjän videokuvaa esimerkiksi puhuessasi juuri hänelle, voit nähdä videokuvan terävämpänä klikkaamalla Participants - kohdasta haluamaasi jäsentä. Näin ollen käyttäjän kuva korostuu videokohdassa, samoin vastaanottajalla näkyy lähettämäsi oma videokuva selkeämmin.

3.2.3 Marratech Whiteboard

Whiteboardin avulla voidaan ladata asiakirjoja kaikkien nähtäville ja jokainen käyttäjä voi tehdä siihen muokkauksia reaaliajassa.

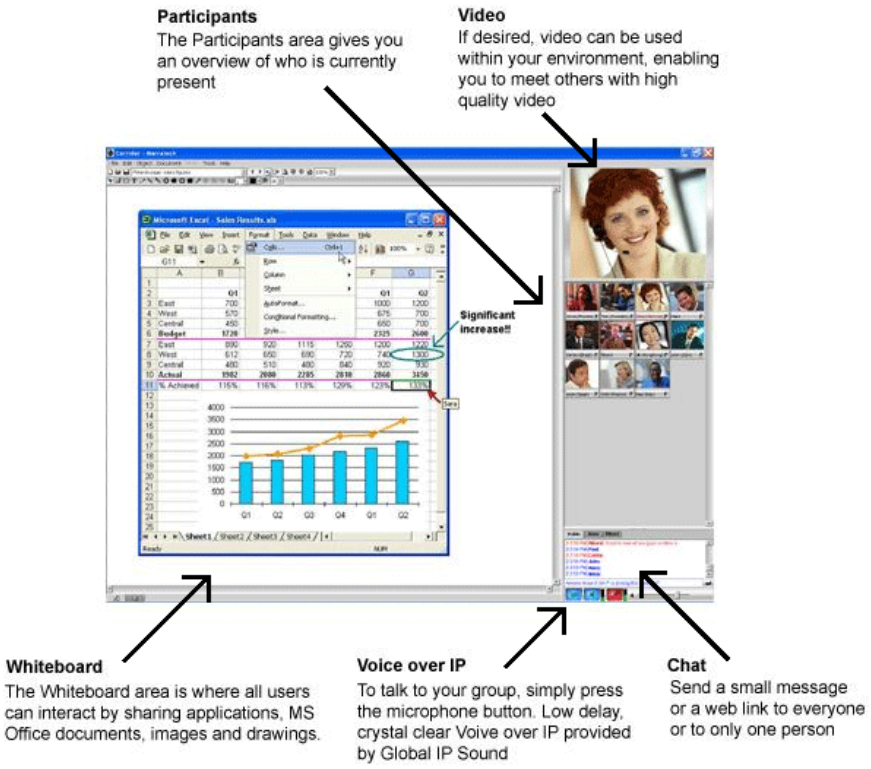
3.2.4 Marratech Voice over IP

Klikkaamalla VoIP –nappia ohjelmiston alakulmasta voidaan mikrofonin välityksellä lähettää myös puheääntä. Ilman napin painallusta ääni ei siis kuulu.

3.2.5 Marratech Chat

Viestitettävä asia kirjoitetaan tekstikenttään ja lähetetään kaikkien osallistujien nähtäville.

KUVIO 1. Marratechissa on seuraavat toiminnot. (Marratech 2005)



3.3 Xenex Visual Meeting (Nettikokous.fi)

Nettikokous.fi tarjoaa mahdollisuuden videoneuvottelun pitämiseen selaimen avulla. Palveluun rekisteröityneet käyttäjät varaavat virtuaalisia neuvottelutiloja palvelimen aulatilasta. Palveluun rekisteröitymättömiä, ulkopuolisia käyttäjiä voidaan kutsua mukaan neuvotteluihin käyttämällä selaimessa toimivan Xenex Visual Meeting – ohjelmiston ”kutsu käyttäjä kokoukseen” - toimintoa.

Laadukkaan äänen ja kuvan lisäksi käyttäjä voi jakaa tiedostoja sekä esittää video- ja äänitallenteita tai PowerPoint - esityksiä. Visual Meeting tukee kaikkia moderneista videoneuvottelujärjestelmistä tuttuja toiminnallisuuksia (Chat, tiedostojenjako, whiteboard) ja täydentää niitä ominaisuuksilla, joita vain Visual Meeting -sovelluksella voidaan toteuttaa. Visuaalinen käyttöliittymä mahdollistaa muun muassa etäältä näytetyn materiaalin tallennuksen ja uudelleenesityksen kätevästi piirto-ominaisuuksin.

Tietoturva nettikokous.fi palvelussa perustuu AES- standardiin. Siksi yhteydenpito myös julkisen laajakaistan yli on turvallista. Ohjelmaan liittyy myös valinnainen tunnelointipalvelin, jonka avulla videoneuvotteluliikenne muunnetaan palomuurien ja osoitemuunnosten ohi tavalliseksi web-selainliikenteeksi naamioituna.(Xenex 2006)

4 VIDEONEUVOTTELULAITTEISTOT JA TIETOLIIKENNERATKAISUT

Videoneuvottelujärjestelmä minimissään koostuu internet – yhteydellä varustetusta tietokoneesta, web-kamerasta, mikrofonista sekä kaiuttimista. Suurimmillaan laitteisto voi kasvaa aina videotykkeihin ja erillisiin videoneuvottelutiloihin asti. (Oulun yliopisto 2003)

4.1 Laitteisto

Videoneuvottelulaitteistot voidaan jakaa karkeasti kahteen eri ryhmään niissä olevien ominaisuuksien mukaisesti: Ryhmäneuvottelulaitteistot sekä henkilökohtaiset videoneuvottelulaitteistot.

Henkilökohtainen videoneuvottelulaitteisto käsittää ensinnäkin PC-tietokoneen, johon lisätään erilaisia osia.

Vastapuolen lähettämää videokuvan toistamista varten tarvitaan videokoodekki -kortti sekä oman videokuvan lähettämiseen web-kamera.
Vastapuolen puhetta sekä äänitiedostoja varten tarvitaan äänikortti, sekä äänen toistamista varten kaiuttimet. Oma puhe välitetään mikrofonilla.
Yhteydenmuodostamista varten tarvitaan tietysti myös Internet-yhteys (xDSL / ISDN / LAN). (Kuusinen 2000)

Ryhmäneuvottelulaitteisto on tarkoitettu esimerkiksi opetuskäyttöön, suurelle ryhmälle suunnattu, jossa laitteisto on yleensä sijoitettu erilliseen videoneuvottelutilaan. Tällaisissa tiloissa muun muassa äänieristyksiin ja ympäristöön on kiinnitetty erityistä huomiota, neuvottelu tapahtuu rauhallisessa ympäristössä, jossa ulkopuoliset äänet on rajattu pois. (Etäopetus ja oppiminen)

Ryhmäneuvottelulaitteisto on hieman monimuotoisempi verrattuna henkilökohtaiseen videoneuvottelulaitteistoon. Peruslaitteisto toki on sama, PC-tietokone yhdistettynä verkkoon, ääni- ja videokoodekki -kortit, sekä kamera ja mikrofoni(t). Tämän lisäksi suurelle joukolle kuvaa ja ääntä toistettaessa on myös näihin laitteistoihin panostettava. Esimerkiksi videotykillä voidaan kuva toistaa valkokankaalle ja äänen toistamiseen paremmat kaiuttimet kuin henkilökohtaisessa videoneuvottelussa. Lisälaitteistoksi voitaisiin lisätä muun muassa tulostin, jos esimerkiksi tekstitiedostoja halutaan jakaa ryhmässä oleville jäsenille. Mahdollista on jokaisella osallistujalla ryhmässä oma kone, jolloin jokainen ryhmän jäsen voisi muutella jaettavia tiedostoja omalta työpisteeltään.(Etäopetus ja oppiminen 22.10.2006)

4.2 Koodekit

Videoneuvottelun tärkeimmäksi osaksi voidaan lukea koodekit. Ne voivat olla kokonaan erillisiä laitteita, tietokoneeseen liitetty koodekkikortti tai ohjelmistokoodekki.

Koodekkien tehtävänä on pakata sekä muuntaa videoneuvotteluissa käytetyt ääni- sekä kuvasignaalit digitaalisiksi datasignaaleiksi, jotka lähetetään tietoliikenneverkkoa pitkin vastapuolen koneeseen. Vastapuolen koneen koodekki vastaavasti muuntaa (dekoodaa) saapuneen datasignaalin jälleen takaisin analogiseen muotoon. (Viestintävirasto 2001)

Juuri koodekit vaikuttavatkin videoneuvottelun reaaliaikaisuuden tunteeseen, miten nopeasti koodekit muuntavat lähettämänsä ja vastaanottamansa signaalit, sekä verkkoyhteyden nopeus ovat hyvän videoneuvotteluyhteyden perusperiaatteet. (Viestintävirasto 2001)

4.3 Yhteystyypit ja –standardit

Tässä osiossa tutkitaan käytettäviä yhteystyyppejä sekä millaisia yhteys – ja tietoturvastandardeja niissä käytetään. Yhteystyyppinä videoneuvottelussa on joko ISDN – tai IP - verkkoyhteys.

4.3.1 ISDN – verkkoyhteys

ISDN-verkkoyhteydet käyttävät modeemien tapaan tavallisia puhelinlinjoja. ISDN (Integrated Services Digital Network) on nopeampi yhteystapa kuin modeemiyhteys ja digitaalisuuden ansiosta myös luotettavampi. Suojaustasoltaan ISDN – yhteys on lankapuhelimeen verrattavissa.(VirtuaaliAMK 2005)

4.3.1.1 H.320 – standardi

H.320-standardi on käytössä ISDN-verkossa toimivissa videoneuvottelujärjestelmissä. Yleisesti ottaen ISDN:ää pidetään vanhana, mutta toimivana ja tietoturvallisena videoneuvottelujärjestelmän ratkaisuna, toisaalta myös se on käyttökustannuksiltaan H.323-standardia kalliimpi. ISDN – yhteyteen luotu videoneuvotteluverkko vastaa tietoturvallisuudellaan lankapuhelimen tietoturvatasoa. (Helsingin yliopisto 2000, standardit)

4.3.2 IP – verkkoyhteys

Internetiin liitetyt verkot voivat olla toiminnaltaan hyvinkin erilaisia, mutta niillä kaikilla on yksi yhteinen tekijä: IP. Tietokoneet kommunikoivat keskenään ottamalla yhteyden toistensa IP – osoitteisiin.

Internetiin liitetyt koneet erotetaan toisistaan IP- eli Internet-osoitteiden perusteella. Jokaisella koneella, joka on liitetty Internetiin, on oma uniikki IP-osoite. Jos laite on kytkettynä useampaan verkkoon, on jokaisella verkkoliitynnällä oma IP-osoite. Tällaisia koneita ovat esim. verkon

solmukohdissa toimivat reitittimet, jotka yhdistävät kaksi tai useampia verkkoja toisiinsa.(Immonen 2000)

4.3.2.1 H.323 -standardi

H.323 on ITU- standardin pakettikytkentäisiin verkkoympäristöihin (LAN, Intranet, Internet) perustuva standardimalli. H.323 on niin kutsuttu sateenvarjostandardi, joka sisältää useita alistandardeja mm. äänen ja videon pakkaamistavoista, yhteyden muodostamisesta sekä tietoturvallisuudesta. Yleisesti ottaen, käytettäessä IP- pohjaista, H.323 standardilla varustettua videoneuvottelujärjestelmää ja yhteyttä ei saada toiseen osapuoleen, on vika todennäköisesti palomuuriasetuksissa. Palomuurit ja palomuuriohjelmistot sulkevat monet videoneuvottelulaitteiden käyttämät tietoliikenneportit, siksi ne tulisikin palomuurin asetuksista erikseen avata ennen yhteyden muodostamista. Verrattuna ISDN – pohjaiseen, H.323- standardia käyttävään videoneuvotteluun IP - pohjaisen videoneuvottelun etuna ovat laitteiston helppo liikuteltavuus sekä halvemmat käyttökustannukset. Miinuksena tuleekin sitten tietoturvallisuuden vaikeampi suojattavuus.

Yhteydenmuodostaminen käytettäessä IP - pohjaista videoneuvottelua tapahtuu soittamalla suoraan vastapuolen IP- osoitteeseen. (Helsingin yliopisto 2000, standardit)

5 TIETOTURVA AVOIMESSA VERKOSSA KÄYTÄVÄSSÄ VIDEONEUVOTTELUSSA

Avoimessa verkossa liikkuva data näkyy aina, ellei sitä ole suojattu. Erityisesti videoneuvottelun aikaansaama suuri datan määrä houkuttelee tunkeilijoita.

5.1 Palomuuri

Internetissä käytävä videoneuvottelu on melkoisen hankala toteuttaa tietoturvallisesti. Tietokoneen tulee olla aina Internet – yhteyteen kytkettynä palomuurilla suojattuna. Kuitenkin kun videoneuvottelulaitteiston kytkee, palomuuri sulkee yleensä videoneuvottelun vaatimat portit, jolloin videoneuvottelu ei pääse läpi. (Talaskivi, 2006)
Palomuurit voidaan kiertää käyttämällä videoneuvottelusiltaa. Sen etuna on, että silloin päätelaitteisiin ei tarvitse avata portteja ulkopuolelle. (VideoFuNet, Palomuuri)

Toinen tapa on tunneloida videoneuvotteluyhteys palomuurin läpi. Tällaiseen ratkaisuun on saatavilla useita kaupallisia vaihtoehtoja, mutta käytännössä sillä ei ole merkitystä palomuurien porttien aukaisuun, sillä siihen tulee joka tapauksessa läpimentävä aukko. (VideoFuNet, Palomuuri)

5.2 Salasanat

Varmin tapa avoimessa verkossa käytävään videoneuvottelun suojaamiseen on ottaa yhteys videoneuvottelusiltaan. tällöin käyttäjä tunnistetaan

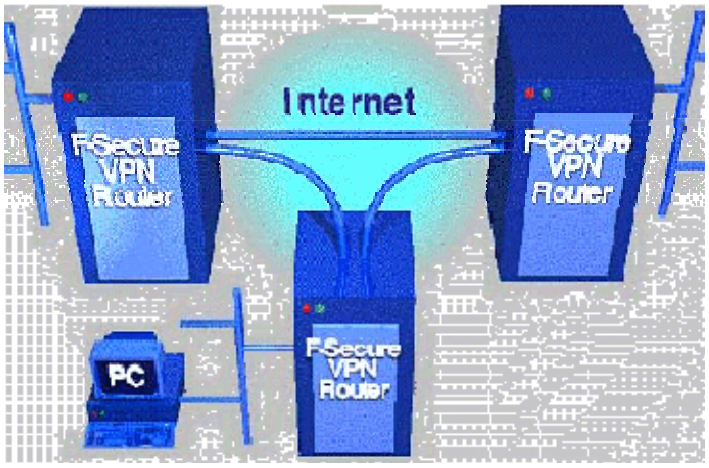
käyttäjätunnuksen ja salasanan avulla. Aina on toki olemassa riski, että tunkeutuja kirjautuu toisen nimellä palvelimelle. (VideoFuNet)

5.3 Virtual Private Networkin (VPN) tarjoamat mahdollisuudet

Avoimen verkon sisään voidaan muodostaa suojattu yhteys soveltamalla rajatun käyttäjäpiirin kesken viestien salakirjoitusta sekä käyttäjien ja viestien todennusta ja aidonnusta. Näin ollen vältetään välitettävän tiedon kulkeutuminen ulkopuolisiin käsiin ilman että heillä olisi vaadittavia salausavaimia.(KUVIO 3) (Viestintävirasto 2001, VPN)

Virtual Private Networkin tarkoituksena on varmistaa, että siirrettäessä tietoa avoimen siirtotien yli ei tieto matkalla muutu, häviä tai joudu kopioiduksi.

KUVIO 3 Virtual Private Networkin toimintaperiaate



Tarkoituksena on luoda "eristetty putki" avoimen siirtotien sisään. Kaikkien VPN-reitittimien välillä on suora point-to-point -yhteys, jonka ansiosta verkkoa voi käsitellä kuten normaalia verkkoa. Kuviossa 3 VPN-reitittimet on konfiguroitu siten, että VPN:n kautta kulkeviksi tarkoitetut viestit lähetetään salattuina VPN-palvelimen kautta toiselle reitittimelle, kun taas muut viestit kulkevat normaalisti avoimeen verkkoon.

5.4 Ekstranet

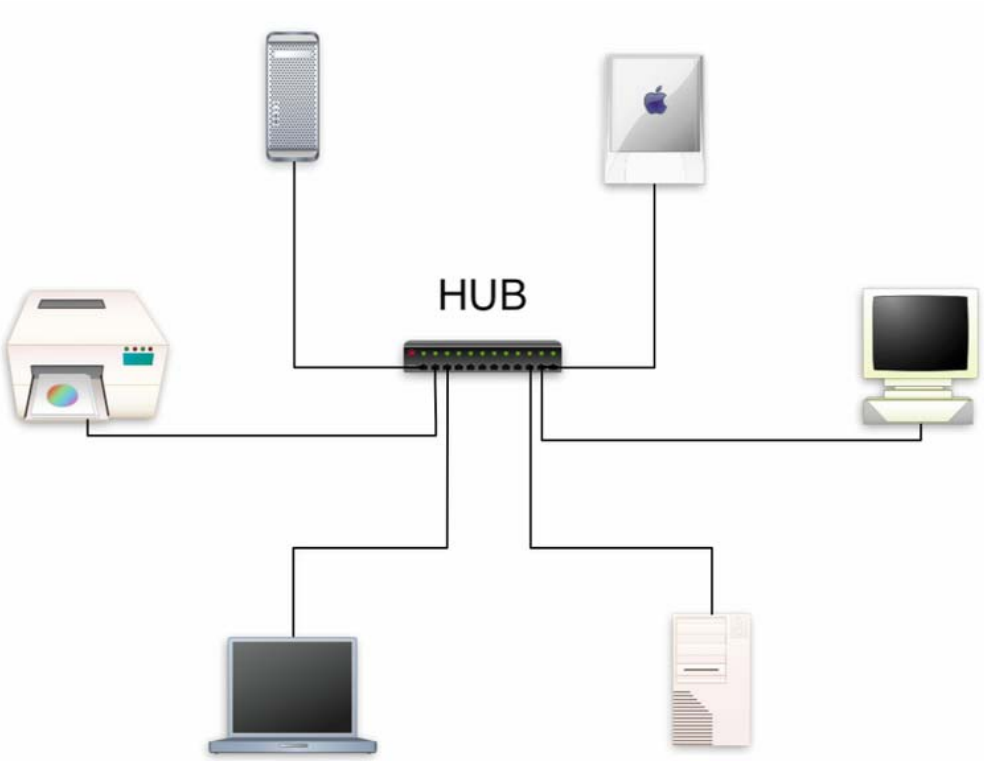
Nykypäivänä yritykset käyttävät ekstranettiä tilausten tekemisiin, sekä asiakkaat esimerkiksi reklamaatioiden tekoon. Videoneuvottelu voidaan myös hoitaa ekstranetin avulla. Perimmältään ekstranetissä on kysymys tietoturvasta. Yksittäistä videoneuvottelua järjestettäessä ei vaivaa kannata nähdä.

Tietoturva voidaan jakaa kolmeen osaan: käyttäjän tunnistaminen, käyttöoikeuksien vahvistaminen sekä liikenteen salaus. Ekstranetin avulla ylläpidetään salasanalla suojattua www-sivustoa sidosryhmille.(Helia 2006)

6 TIETOTURVA SULJETUSSA VERKOSSA KÄYTÄVÄSSÄ VIDEONEUVOTTELUSSA

Tässä osiossa tutkitaan suljetuissa verkoissa tapahtuvan videoneuvottelun suojaamista. Aloitetaan tutkimalla lähiverkkoa.

6.1 Lähiverkko (Local Area Network)

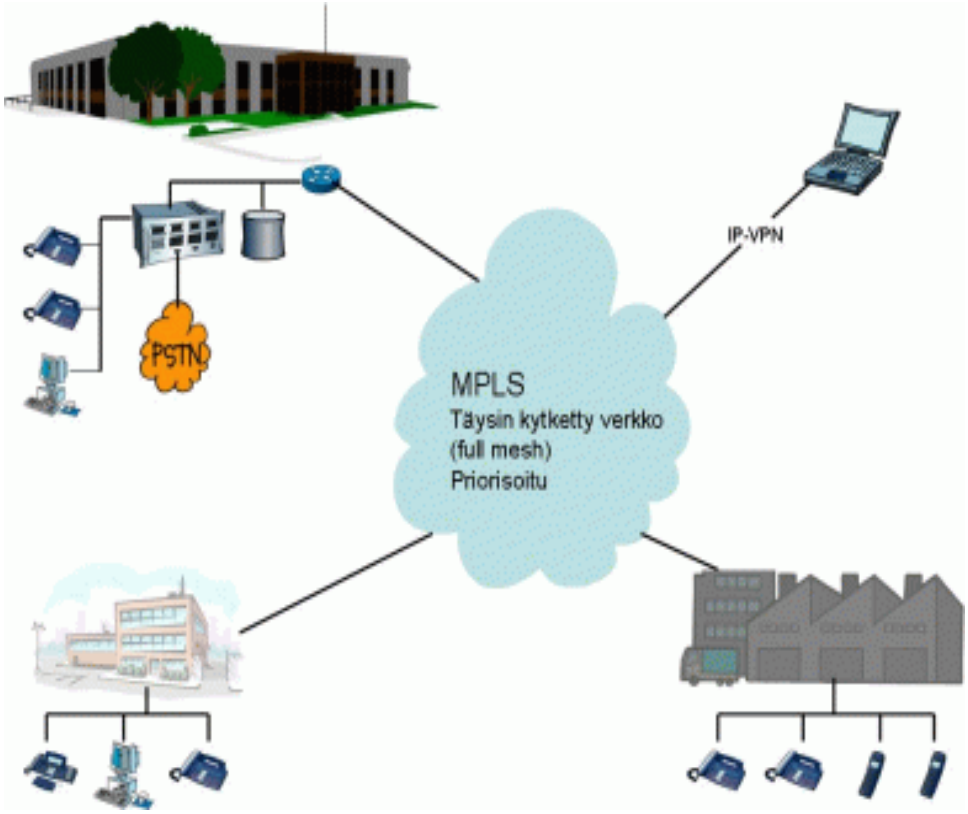


KUVIO 3. Lähiverkon rakenne

Lähiverkko on tietoliikenneverkko, joka toimii rajoitetulla maantieteellisellä alueella (KUVIO 3). Esimerkiksi talossa olevat useat koneet voidaan liittää yhteiseen verkkoon, jolloin tiedostojensiirto ynnä muu kanssakäyminen on täysin turvallista sekä nopeaa. (Wikipedia 2006, LAN)

6.2 MPLS – yritysverkko

MPLS – verkolla organisaatio voi yhdistää kaksi tai useampia toimipisteitä täysin tietoturvalliseksi yritysverkoksi, jolloin informaatio on välittömästi jokaisen käytössä (KUVIO 4). (Finnet 2006)



KUVIO 4

”Esimerkkiratkaisu.

Ratkaisussa puhelinjärjestelmä sijaitsee yrityksen päätoimipaikassa. Yrityksen muut toimipisteet ovat liitetty verkkoon suljetulla MPLS - verkolla. Yrityksen etätyöntekijät ovat yhteydessä suojatulla VPN - yhteydellä. Ratkaisulla voidaan yhdistää koko yrityksen sisäinen tietoliikenne toimipisteiden välillä. MPLS-verkon priorisointi turvaa hyvän äänenlaadun puheluissa, myös yrityksen tietoturva voidaan keskittää hajautettua ratkaisua paremmin.” (Finnet 2006, MPLS)

6.3 Intranet

Intranetistä on yhteys ulkopuoliseen Internet - verkkoon jolloin pitää ulkopuolisten käyttäjien pääsy yrityksen sisäiseen verkkoon estää erilaisin palomuuriratkaisuin.

Intranetiin pääsy yrityksen ulkopuolelta voidaan estää täysin, niin ettei edes yrityksen oma henkilökunta pääse verkkoon yrityksen verkon ulkopuolelta. Usein kumminkin halutaan, että yrityksen työntekijöillä on mahdollisuus päästä käsiksi tietoon myös muualta internetistä. Silloin käyttäjälle pitää antaa asianmukaiset käyttäjätunnukset ja salasanat. Käyttäjä voi siten kirjautua esimerkiksi kotoaan videoneuvottelukokoukseen.(Mensola 2006)

Perinteisten käyttäjätunnusten ja salasanojen tilalle turvallisemmat digitaaliset sertifikaatit tulevat yleistymään seuraavan parin vuoden aikana
Lisäksi verkossa liikkuva tieto halutaan usein salata, vaikka sitä liikutellaankin yrityksen sisäisessä verkossa. Tähän tarkoitukseen voidaan käyttää esim. SSL - protokollaa.(Mensola 2006)

6.3.1 SSL – protokolla (Secure Sockets Layer)

Selaimen verkkopalveluiden välillä lähetettävät sanomat suojataan SSL - salaustekniikalla. SSL mahdollistaa yhteyden vahvan salaamisen käyttäjän www-selainohjelman ja www-palvelimen välillä. Salaus suojaa tietoliikenteen siten, että ulkopuolinen tarkkailija ei yhteyttä seuraamalla pysty näkemään luottamuksellisia tietoja.(Lassila & Tikanoja 2006)

7 CASE – OSUUS

Opinnäytetyö tutkii kahden eri organisaation, Päijät – Hämeen Koulutuskonsernin sekä Opetusalan Koulutuskeskuksen videoneuvottelujärjestelmiä.

Molemmat käyttävät eri yhteystyyppisiä ratkaisuja ja opinnäytetyön tehtävänä on tarkastella molemmista sekä hyviä että huonojakin puolia.

Tiedonkeruumenetelminä on käytetty vierailua organisaatioissa sekä haastattelemalla asianosaisia. Lisäksi tietoa on haettu Internetistä.

Tutkimme ensiksi avoimessa tietoverkossa tapahtuvaa Päijät – Hämeen Koulutuskonsernin L – videonet –järjestelmää.

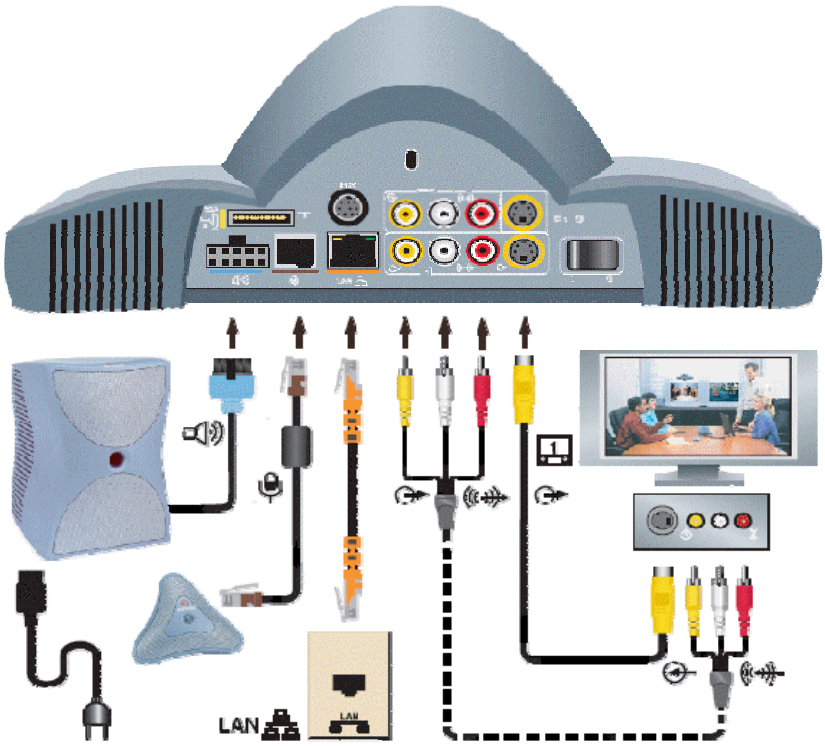
7.1 Päijät – Hämeen Koulutuskonserni, L- Videonet

7.1.1 Laitteisto

Projektia varten hankittiin Polycom VSX 7000 – merkkisiä videoneuvottelulaitteistoja, joiden ohjelmistoversio on 5.1.

Polycom VSX 7000 (KUVIO 5 ja KUVIO 6)
-Varustettu People + Content -optiolla. Mahdollistaa tietokonekuvan jakamisen videoneuvottelun yli
-Videoprotokollat ja standardit: H.261, H.263+, H.263++, H.264, ITU 60-fps full screen
-Audioprotokollat: Polycom Siren 14 Stereo Ready, 14 kHz bw with Polycom Siren 14 audio, 7 kHz bw with g.722, G.722.1, 3,4 kHz bw with G.711, G.728, G.729A

KUVIO 5. Polycom VSX 7000 –laitteisto.



KUVIO 6. Polycom VSX 7000 liitännät.

Näiden lisäksi on hankittu videoneuvottelusilta, joka on Polycom Accord MGC-25 - mallinen. Videoneuvottelusilta on välttämätön monen pisteen välisessä

videoneuvottelussa, sillä kaikki osapuolet ottavat siihen yhteyden syöttämällä käyttäjätunnuksen sekä salasanan. Videoneuvottelusillan tehtävänä on välittää informaatio kaikille osallistujille sopivassa muodossa sekä jakaa puheenvuorot niitä tarvitseville. (Eerola, 14.4.2006)

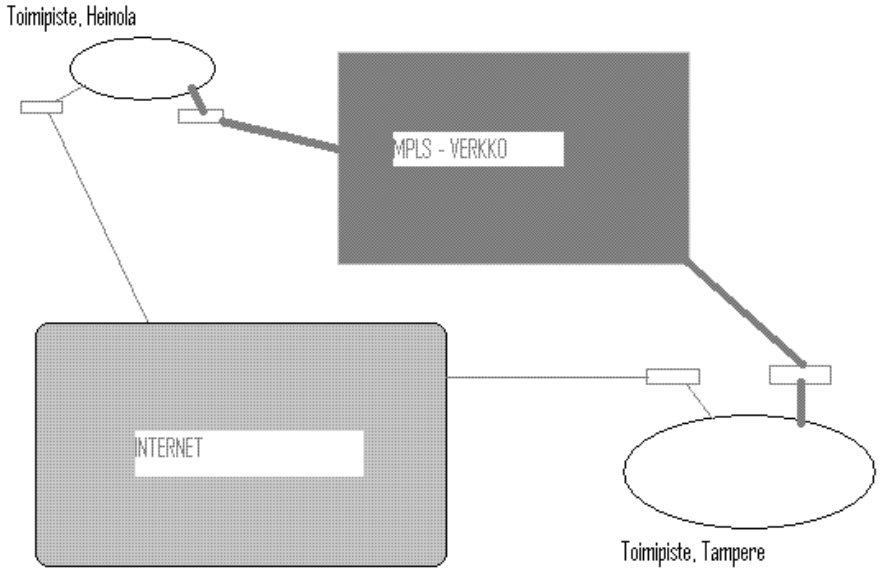
7.1.6 Tietoturvaratkaisut

Tällä hetkellä käytössä ei ole minkäänlaista tietoturvan suojausta, mutta yksi mahdollisuus olisi käyttää AES - salausta. Todennäköisesti salausta käytettäessä, palomuuri tulisi kytkeä pois päältä, jolloin organisaation muu tietoturva olisi puutteellinen. Yhteys on ISDN – pohjainen, joka sinällään on turvallinen. (Eerola, 14.4.2006)

7.2 Heinolan Opetusalan Koulutuskeskus, MPLS - yritysverkko

Heinolan Opetusalan Koulutuskonsernin käytössä on uudenlainen MPLS - yritysverkko, jota käytetään Heinolan ja Tampereen toimipisteiden välisiin videoneuvottelutilanteisiin. Yhteydenmuodostaminen tapahtuu soittamalla vastapuolen videoneuvottelulaitteeseen.(Nokelainen, 20.10.2006)

MPLS – verkon tekee turvalliseksi se, että yhteys on muodostettu suljettuna vain näiden kahden toimipisteen välille. Organisaation muut yhteydet Internetiin tapahtuvat erillisen verkon avulla, joka on palomuurilla suojattu (KUVIO 7). (Nokelainen, 20.10.2006)



KUVIO 7. OPEKOn MPLS –verkkoratkaisu.

8 YHTEENVETO JA POHDINTAA

8.1 Opinnäytetyön tavoitteiden saavuttaminen

Opinnäytetyö saavuttaa tavoitteensa tutkia videoneuvottelujärjestelmien toimintatapaa nykypäivänä, millaisia menetelmiä niissä käytetään ja kuinka onnistutaan luomaan tietoturvallisesti käyttötarpeen mukaisesti toimiva videoneuvottelutilanne sekä millaisia yhteystyyppejä ylipäätään voidaan käyttää. Ulkopuoliselle tarkastelijalle videoneuvottelujärjestelmä voi olla sekavakin kokonaisuus. Tässä opinnäytetyössä asiat pyritäänkin selvittämään vasta-alkavalle videoneuvotteluprosessin käyttäjälle helppoa selkokieltä käyttäen.

8.2 Opinnäytetyön merkitys

Opinnäytetyön tavoitteena on saada niin yritykset kuin yksityisetkin jotka ehkä jo ovat videoneuvottelutilanteisiin tutustuneet, tutkailemaan käyttämiensä neuvottelujen tietoturvallisuusvaihtoehtoja. Voitaisiinko niitä ehkä parantaa ja onko käytössä jo olevat tietoturvallisuusratkaisut riittäviä.
Case -osuudessa luvussa 7 pyrittiin selvittämään Lahden seudulla käytettävää L-videonetin tietoturvallisuuden riittävyyttä ja olisiko sitä kenties voitu parantaa mahdollisesti. Lisäksi OPEKON tietoturvaratkaisuja tutkailtiin.
Parannettavia asioita toki olisi löytynyt, mutta olisiko niillä ollut asian lopputuloksen suhteen merkittävää vaikutusta opiskelukäytössä, ei löydetty mitään mullistavaa vaihtoehtoa. Muutoksiin ei siis tämän opinnäytetyön ansiosta ryhdytty. Molemmissa organisaatioissa tietoliikennevastaavat ovat hoitaneet tietoturva-asiat organisaatioiden vaatimalla tavalla nykypäivän tietoyhteiskuntaa silmällä pitäen.

8.3 Jatkotutkimuksen tarve

Tarvetta jatkotutkimukselle ei ole. Tällä hetkellä käytössä olevaa videoneuvottelujärjestelmää ei tulla muuttamaan olennaisesti. Käytössä olevaa ISDN-pohjaista, H.320-standardia käyttävää yhteystyyppiä tuskin tullaan muuttamaan L -videonetissä, sillä se on havaittu riittäväksi opiskelukäyttöä ajatellen. OPEKOssa samoin, tietoturva-asiat ovat varsin hyvällä mallilla.

LÄHTEET

Elektroniset lähteet:

VideoFunetin videoneuvotteluopas 13.8.2006.
Julk. 2003
<http://www.video.funet.fi/videoneuvotteluopas/?id=9>

VIDERA 14.8.2006.
Julk. 2006
<http://www.videra.com/videra.htm>

Aarno Rönkä 14.8.2006.
Videoneuvottelu etäopetuksessa
<http://www.helsinki.fi/kasv/nokol/projektit/kilpis/kilpi.html>

Aarno Rönkä 14.8.2006.
Videoneuvotteluopas
<http://www.helsinki.fi/kasv/nokol/projektit/kilpis/videoneuvotteluopas.html>

Jussi Talaskivi 20.10.2006.
Videoneuvottelu IP –verkossa.
ATK- suunnittelija, Jyväskylän yliopisto
<http://www.nic.funet.fi/index/FUNET-Club/kokous0206/videoneuvottelu.ppt>

Kati Kuusinen 11.7.2006.
Jyväskylän ammattikorkeakoulu
Tekniikka ja liikenne / IT- Instituutti
Tietoliikennetekniikan harjoitustyö, kevät 2000
<http://www.geocities.com/kati6nen/videosivut.htm>

Helsingin yliopisto 12.8.2006.
Tietotekniikan osasto, julk. 2003
<http://www.helsinki.fi/atk/yhteydet/videoneuvottelu/videoneuvottelu>

Oulun yliopiston Atk- keskuksen tiedote
Julk.04/2001
15.8.2006.
<http://www.oulu.fi/atkk/tiedotus/sessio/sess211/sess211.pdf>

Kuopion yliopisto
Oppimiskeskus
18.9.2006.
<http://www.uku.fi/opk/tilat/videoneuvottelutilat.shtml>

O.Nykänen
NetMeeting – esittely
Julk. 04/09/98
<http://matwww.ee.tut.fi/hmopetus/hypmed01/itseopiskelu/netmeeting/esittely/esittely.htm>

Etäopetus ja oppiminen 22.10.2006.
Internet – pohjainen videoneuvottelu oeptuksessa ja oppimisessa
<http://cc.joensuu.fi/~jptahva/etaopetus/data.html>

Finnet 23.10.2006.
Finnet MPLS verkko
Julk 2006
<www.finnet.fi/default.asp?link=126>

Jyväskylän yliopisto 1.11.2006.
Julk. 2005
<http://virtuaaliyliopisto.jyu.fi/etusivu/tyopakki/viestinta/video>

Helsingin Teknillinen Korkeakoulu 20.10.2006.
Videoneuvottelu, julk. 2000
<http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/19/standardit.shtml>

Viestintävirasto 18.7.2006
VPN, julk. 2001
<http://www.ficora.fi/suomi/tietoturva/vpn.htm>

Chydenius-instituutti - Kokkolan yliopistokeskus 23.10.2006
<http://www.chydenius.fi/verkkoantti/verkostoyo/videoneuvottelu/Videoneuvottelu%20tyokaluna/Johdanto.html>

L & T Verkkopalvelu, 2004
SSL – salaus, 18.11.2006
<https://www.lassila-tikanoja.fi/verkkopalvelut/public/?form=ssl_salaus>

Sami Mensola, 2000
Intranet, 18.11.2006
<http://www.netlab.tkk.fi/opetus/s38116/1997/esitelmat/41748f/>

HELIA, 2006-11-28
Ekstranet, 18.11.2006
<http://myy.helia.fi/~vanvu/tietoliikenne/internet/ekstranet.html>

Mikko Heinonen, Juha Immonen & Ville Koponen, 2000
All Over IP, 18.11.2000
<http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/17/voip.shtml>

VirtuaaliAMK, 2005
ISDN – yhteys, 18.11.2006
<https://www.virtuaaliamk.fi/opintokokonaisuudet/56QfjjzFJ/1100243557888/1100243668895/1100255809319/1100256512812.html.stx>
Haastattelut:

L – VIDEONET –projekti 14.4.2006.
Päijät – Hämeen koulutuskonserni
Pekka Eerola
<http://www.phkk.fi/yhteisetpalvelut/thy/l-videonet/>

OPEKO
Jari Nokelainen 20.10.2006.