VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Jouni Henrik Mäkynen

SISÄISEN TIETOVERKON KEHITTÄMINEN JA TIETOTURVAN PARANTAMINEN

Tekniikka ja liikenne

2009

ALKUSANAT

Tämä opinnäytetyö tehtiin Vaasan ammattikorkeakoulun tietotekniikan osaston päättötyönä kevään ja syksyn 2009 aikana. Työ tehtiin työsuhteen aikana vaasalaiselle Winpos Oy -kassajärjestelmätoimittajalle.

Winpos Oy:n yhteyshenkilönä on toiminut verkkovastaava Jari Palomäki. Vaasan ammattikorkeakoulun puolesta työn valvojana toimi lehtori Antti Virtanen.

Kiitokset haluan esittää Winpos Oy:n Jari Palomäelle sekä toisen yrityksen palvelukseen siirtyneelle verkkoasiantuntija Sören Krokforsille.

Vaasassa 8.12.2009

Jouni Mäkynen

VAASAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Jouni Mäkynen
Opinnäytetyön nimi	Sisäisen tietoverkon kehittäminen ja tietoturvan parantaminen
Vuosi	2009
Kieli	suomi
Sivumäärä	29+6 liitettä
Ohjaaja	Antti Virtanen

Tämän opinnäytetyön tarkoituksena oli kartoittaa vaasalaisen Winpos Oy:n sisäverkon tila. Työssä selvitetään, miten tärkeitä ovat tarkat verkkodokumentaatiot sekä tietoturvan tärkeys. Lisäksi kartoitetaan Vaasan toimipisteen verkon rakennetta.

Opinnäytetyössä käydään läpi virtuaalisten verkkojen hyötyjä sekä eri toteutusvaihtoehtoja, keskittyen yrityksessä käytettyyn porttikohtaiseen VLAN-ratkaisuun. Toteutus tapahtuu Zyxel GS-2024 -kytkimellä. Uusien kytkinten johdosta verkon nopeus nousee gigabit ethernetin tasolle. Tästä syystä tehtiin myös verkkokaapeloinnin testaus.

Lisäksi työssä tarkastellaan huomioon otettavia asioita verkon serverin päivityksen suhteen.

Asiasanat verkko, tietoturva, VLAN, verkonhallinta

VAASAN AMMATTIKORKEAKOULU

VAASA UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutusohjelma

ABSTRACT

Author	Jouni Mäkynen
Title	Network Security and Deployment
Year	2009
Language	Finnish
Pages	29+6 Appendices
Supervisor	Antti Virtanen

The purpose of the thesis was to identify the status of Vaasa Winpos Ltd indoor network. The work goes through the importance of the exact network documentation and security. In addition, the Vaasa office network structure was mapped.

The thesis goes through the advantages of virtual networks, and the benefits of various implementation options, focusing on the port based VLAN solution used by the company. The implementation is done using the Zyxel GS-2024 switch. The new switches will increase the network speed to the level of gigabit Ethernet. For this reason, the network cabling was also tested.

In addition the work is to be carefully taken into account relater to issues of the network server upgrading (the work deals with the issues to be taken into account concerning the network server upgrading).

Keywords Network, Security, VLAN

LYHENNELUETTELO

AD (Active Directory)	=	käyttäjätietokanta
BRD	=	Botnia Retail Data -yritys
CAT (Category) 5 & 6	=	tiedonsiirtokaapeleiden laatuluokka
CC(Chain Control)	=	ketjunohjaus
DHCP (Dynamic Host Configuration Protocol)	=	protokolla, joka jakaa IP-osoitteita
DMZ (Demilitarized Zone)	=	demilitarisoitu alue
DNS (Domain Name System)	=	toimialueen nimenhallintajärjestelmä
Ethernet	=	pakettipohjainen lähiverkkoratkaisu
FTP(File Transfer Protocol)	=	tiedonsiirtoprotokolla
IP (Internet Protocol)	=	internetprotokolla
MAC- osoite (Media Access Control)	=	verkkosovittimen yksilöivä osoite
POS	=	Point Of Sale -kassapiste
RJ-45 (registered jack 45)	=	puhelin- ja lähiverkoissa käytetty liitintyyppi
TCP/IP (Transmission Control Protocol/Internet Protocol	=	tiedonsiirtoprotokolla
VLAN	=	virtuaalinen lähiverkko
VPN (Virtual Private Network)	=	näennäinen yksityinen verkko

SISÄLLYS

1 JOHDANTO

1.1 Tavoitteet

Työn tarkoituksena oli kartoittaa Winpos Oy:n Vaasan toimipisteen sisäverkon nykytilanne sekä mahdolliset parannuskohteet ja tietoturva-aukot. Tavoitteena oli kytkinten uusiminen ja verkon nopeuden nostaminen. Lisäksi verkon hallinnoimisen helpottamiseksi haluttiin kartoittaa ja dokumentoida eri verkkolaitteiden sijainnit. Organisaation sisäisten järjestelyjen johdosta verkosta vastaavien henkilöiden tehtävät vaihtuivat. Tämä asetti osaltaan paineita verkon rakenteen selvittämiselle. Osana työn tarkoitusta oli dokumentoida se miten verkkoa yleisesti ylläpidetään kartoittamalla ongelmatilanteita. Winpos Oy:n tyyppisessä yritysverkossa huomioon otettavia asioita ovat tietoturva, helppokäyttöisyys, ja laajennettavuus tekemättä järjestelmästä kuitenkaan liian raskasta ja vaikeasti hallittavaa.

Työn edetessä kävi ajankohtaiseksi ottaa myös tarkasteluun tärkeimmän palvelimen mahdollinen päivitys vanhasta Windows Server 2000:sta uudempaan järjestelmään. Tämän osalta tehtiin kartoitus siitä, miten helposti tarvittaessa pystytään siirtämään tiedot vanhemmasta käyttöjärjestelmästä uuteen järjestelmään.

1.2 Yritysesittely

Oy Winpos Ab on vaasalainen yritys, joka toimii kahdessa toimipisteessä. Toinen sijaitsee Vaasassa ja toinen Helsingissä. Winpos perustettiin 1997 jatkamaan vaasalaisen Oy Botnia Retail Data Ab:n (BRD) toimintaa kassajärjestelmäkehittäjänä. Tämä tapahtui sen jälkeen, kun BRD:n toimintaa pilkottiin asiakaskohderyhmien mukaan vähittäiskauppaosaan (Oy Winpos Ab) ja teollisuusosaan (Oy ISI Industry Software Ab). Toiminta on keskittynyt kaupan ja ravintola-alan sekä julkishallinnon kassajärjestelmiin. Yritys työllistää tällä hetkellä n. 30 työntekijää. Yrityksen kehittämä järjestelmä on Windows-pohjaiseen ohjelmistoon perustuva kassajärjestelmä. Se toimii normaalissa

tietokoneessa, joka on varusteltu erilaisilla lisälaitteilla. Tällä hetkellä yrityksellä on lähes tuhat asiakasta ympäri Pohjoismaita, sekä yksittäisiä kassapisteitä myös Euroopassa. Vuonna 2006 Winpos sai valmiiksi sirukortin käsittelymoduulin ja sen sertifioi hyväksytysti Luottokunta.

Winpos-ohjelmisto tarjoaa mahdollisuudet niin isoille ketjutason myynnin seurannalle kuin pienten yksittäisten myymälöiden kaupan seuraamiseen. Kassajärjestelmä kootaan erilaisista ohjelmistomoduuleista asiakkaan tarpeiden mukaan. Myös laitteistoja on erilaisia vaihtoehtoja riippuen käyttötarkoituksesta: normaalista pc-laitteistosta integroituihin kassa-pc-järjestelmiin.

Winpos-ohjelmiston käyttöliittymä on onnistuttu toteuttamaan varsin helppokäyttöiseksi sekä nopeaksi käyttämällä kosketusnäyttötekniikkaa. Ohjelmistoa ohjataan isoista ja selkeistä painikkeista kosketusnäytön avulla.

Kuva 1. Mallikokoonpano1 /15/

2 TYÖN TEORIATAUSTA

2.1 Johdanto työhön

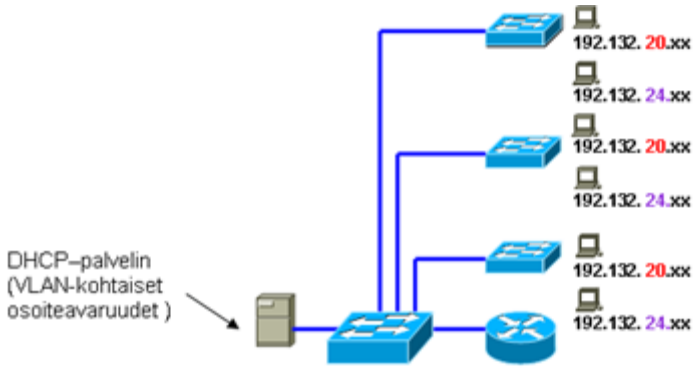
Verkonhallintaa voidaan suorittaa monella eri tavalla käyttämällä erilaisia apuohjelmia tai manuaalisemmin tekemällä liikennemäärien mittauksia. Työssä keskitytään konkreettisempien ongelmien tarkasteluun ja siihen, millaisessa tilassa verkko on tällä hetkellä.

Yhtenä isona tarpeena koettiin verkon osien erottaminen jollain tapaa toisistaan. Tähän on useita erilaisia ratkaisuja mutta yleisimmin käytössä oleva on VLAN eli Virtual Lan.

VLAN-tekniikalla jaetaan fyysisesti samassa kytkimessä olevat koneet eri VLAN-verkkoihin. Tämä vaatii kytkimeltä VLAN-ominaisuuden. Virtuaalisen verkon toteutustavat jaetaan yleisesti ottaen kolmeen eri tyyppiin

- Level 1 VLAN: Kytkimen portteihin perustuva VLAN
- Level 2 VLAN: MAC-osoitteeseen perustuva VLAN
- Level 3 VLAN: Verkko-osoitteeseen tai protokollaan pohjautuva VLAN /13/

VLAN-tyypit voidaan siis määritellä OSI-mallin L2-tasosta aina L7-tasolle saakka. Asetukset siitä, mihin virtuaaliverkkoon käyttäjä kuuluu, määritellään kytkimessä. Jos käytetään verkko-osoitteeseen perustuvaa jakoa, täytyy miettiä VLAN-kohtaiset osoiteavaruudet esimerkiksi kuvan 2 mukaan:



Kuva 2. Osoiteavaruudet /16/

Jokaisella tietokoneella on oma yksilöllinen osoite tai useita osoitteita, jos koneessa on useita verkkokortteja. Osoite voi olla myös vaihtuva osoite, joka annetaan istuntokohtaisesti. IP-osoitteen perusteella koneet tunnistavat toisensa verkossa. IP-osoite esitetään useimmiten neljän desimaaliluvun numerosarjana. Kukin on väliltä 0–255 ja ne erotetaan toisistaan pisteellä, esim. 192.44.62.53. Monessa verkossa osoitteet jaetaan automaattisesti DHCP:tä käyttäen. Dynamic Host Configuration Protocol on palvelu, jolta työasema pyytää osoitetta. Palvelin jakaa osoitteet palvelimen osoiteavaruudeksi määritellyn osoiteavaruuden mukaan. Winpos-yritysverkossa on käytössä sekä kiinteitä osoitteita että DHCP:n jakamia osoitteita. Kiinteät osoitteet ovat käytössä etäyhteyksien reitittämisen helpottamiseksi. /9/

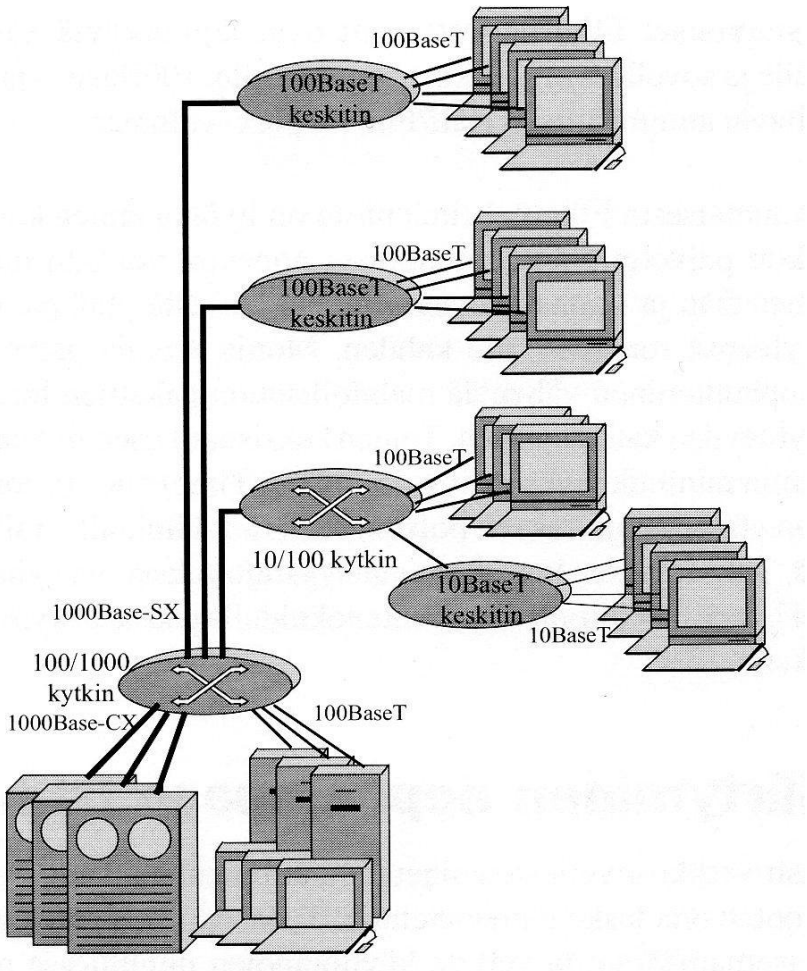
Nämä kiinteät osoitteetkin jakaa tässä tapauksessa DHCP. Palvelimelle on määritelty osoitevaraus tietylle MAC-osoitteelle.

MAC-osoitteeseen perustuvassa VLAN-verkossa määrittelyt siitä mihin verkkoon koneet kuuluvat, tehdään yksilöidyn MAC-osoitteen mukaan. Käytännössä on siis selvitettävä jokaisen koneen verkkokortin MAC-osoite ja syötettävä nämä kytkimelle omiin VLAN-aluesiin. /16/

Koska työssä vaadittiin virtuaaliverkkoa, jouduttiin tekemään kytkinhankintoja, jotka tukevat VLAN-ominaisuutta. Uudet kytkimet mahdollistavat myös verkon nopeuden nostamisen gigabitin tasolle. Tämä asettaa vaatimuksia

verkkokaapeloinnille sekä työasemien verkkokorteille. Gigabit Ethernet on yleisnimitys kaikille 1 Gbit/s siirtonopeuteen kykeneville verkkotekniikoille.

Muutokset 10/100 BaseT -tekniikasta ovat varsin pieniä ja siirtyminen on helppoa. Gigabit Ethernetin perusta kehittää uutta Etherhenetiä alkoi palvelimien tarpeesta nopeammalle sekä suorituskykyisemmälle runkoverkkotekniikalle. Gigabit Ethernet Allianssi (GEA) on laite ja ohjelmistovalmistajien yhteenliittymä, jonka tarkoitus oli tukea uuden verkkotekniikan markkinoille tulemista(kuva 3). Ensimmäiset Gigabit-laitteet julkistettiin vuoden 1997 lopussa. /12/ /1/



Kuva 3. Gigabit Ethernetin tyypillisiä käyttökohteita ovat 100BaseT-verkkot ja nopeat liitännät palvelimiin. Nykyään myös koko verkkoja toteutetaan paljon Gigabit-nopeudellisena. /4/

2.2 Tavoitteet

Työn tavoitteena oli selvittää yrityksen Vaasan toimipisteen verkon rakenne sekä sen ongelmakohdat. Työlle syntyi tarve, kun verkkovastaava siirtyi toisen yrityksen tehtäviin.

Työn tavoitteena oli helpottaa verkon ylläpitoa ja dokumentoida prosessikuvaukset siitä, miten toimipisteen sisäverkko toimii ja mitä se pitää sisällään. Tavoitteena oli myös nopeuttaa verkkoa, koska uusien kytkimien hankkiminen oli ajankohtaista.

Uusien kytkinten avulla olisi tarkoitus parantaa myös tietoturvaa ja rajoittaa verkon käyttöä ottamalla käyttöön VLAN. Lisäksi haluttiin parantaa talossa sisäisesti tapahtuvaa viestintää kehittämällä jokin yhteinen, nopea pikaviestintämuoto, joka kuitenkin olisi salattu ja ilmainen, koska helpdesk-henkilökunta tilajärjestelyistä johtuen siirtyi eri huoneistoihin, ja koettiin että sähköpostin rinnalle tarvitaan jokin helppo ja nopea tapa kommunikoida. Työn edetessä kävi myös ilmi, että verkon toimintoja ylläpitävä serveri on tulemassa tiensä päähän ja sen vaihtaminen tulisi ajankohtaiseksi tulevaisuudessa joka tapuksessa. Verkon tärkeimpiä toimintoja ylläpitävän serverin osalta päädyttiin tekemään selvitystyö siten, että dokumentoidaan domainin tiedot ja tehdään mahdollinen testiympäristö, johon tiedot siirretään testaten näin, miten helposti tiedot ovat siirrettävissä Windows 2008:aan. Lisäksi tutustutaan yleisesti Server 2008 -ympäristöön, koska yrityksessä kenelläkään ei ollut varsinaista kokemusta aiheesta.

2.3 Lähtötilanne

Suurin puute toimipisteen verkkoratkaisussa oli sen dokumentoimattomuus. Periaatetasolla asioita oli varmasti mietitty ja kaikki toimi käytännössä niin kauan hyvin, kunnes verkossa ilmeni jokin vikatilanne. Toimipisteessä on noin 20 aktiivista verkon käyttäjää ja suurin käyttö kohdistuu asiakkailta otettaviin etäyhteyksiin sekä sähköposti- ja intraliikenteestä. Toiseksi eniten ulkoverkosta päin tulevaa liikennettä muodostavat toimipisteen laitetilassa sijaitsevat

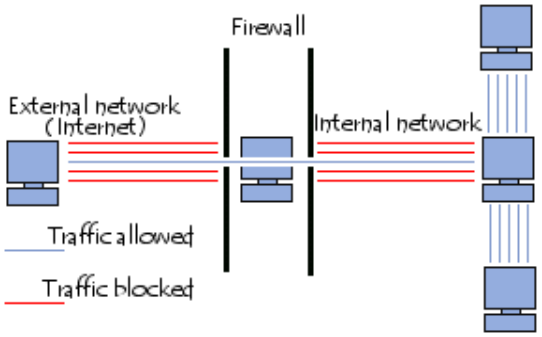
ketjunohjausserverit. Näihin CC-serverihin liikennettä kohdistuu asiakkaiden myyntidatasta sekä tuotteiden ylläpidosta. Ketjunohjaus lyhyesti tarkoittaa sitä, että ketjunjohtaja pääsee ohjausjärjestelmään kiinni mistä tahansa nettiyhteydellä ja pystyy muuttamaan tuotetietoja ja seuraamaan ketjun myyntiä. Lisäksi sisäverkossa hyödynnetään uusien koneiden kloonauksessa image-serveriä, josta saadaan asennettua nopeasti koko levyn image uuteen tai vioittuneeseen koneeseen verkon yli.

Yhtenä suurena parannuskohteena kävi ilmi, että koko toimipisteen kaikki koneet ovat samassa lähiverkossa kiinni. Tämä tarkoittaa sitä, että jos yksi kone saastuu viruksesta, tämä haittaohjelma pääsee leviämään koko verkkoon. Tähän haetaan muutosta eriyttämällä ohjelmistokehitys-, myynti- ja hallinto-osastot eri virtuualiverkkoihin.

Tämä kuitenkin edellyttää kytkimiltä vaatimuksia, joita eivät vanhat kytkimet tue. Lisäksi haluttiin varmistaa uusien kytkinten tehokas toiminta mittaamalla verkon toiminta gigabitin ethernet-nopeudella. Osa verkosta oli vanhaa CAT5-kaapelointia, jossa nopeuteen ei pystytty täysin, mutta lähes jokaiseen huoneistoon saatiin myös CAT6-luokituksen omaava kaapelointi ja pysytyttiin hyödyntämään nopeampaa verkkoa.

2.4 Palomuuri

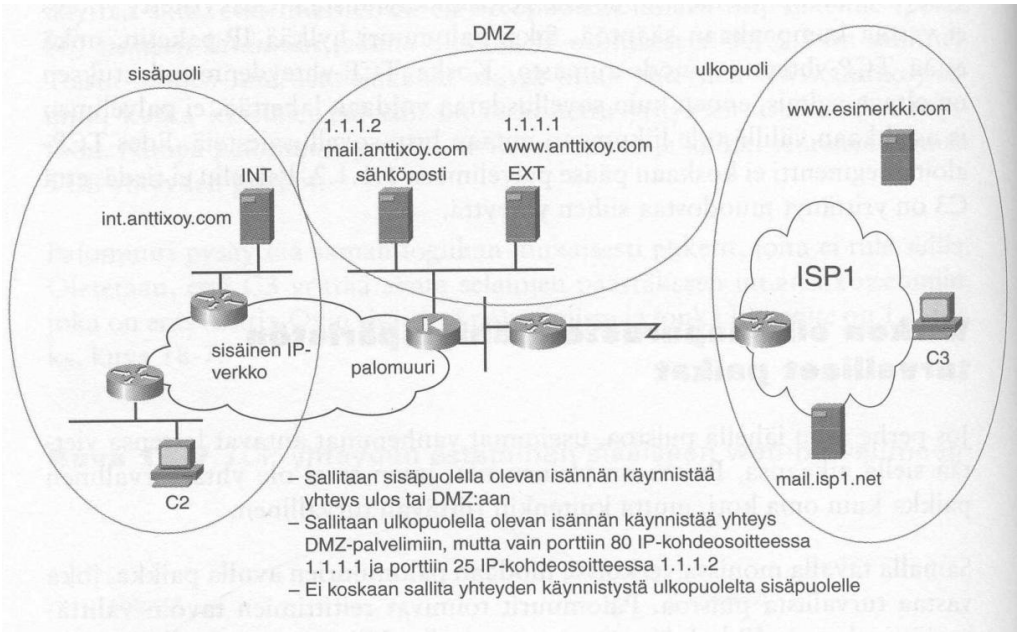
Palomuuri on verkon tärkein tietoturvalaite ja -ohjelmisto. Palomuurin avulla hallinnoidaan sitä miten avoimesta internetistä pääsee yrityksen sisäverkkoon. Palomuuri voidaan toteuttaa laitepohjaisella ratkaisulla tai ohjelmistopohjaisella työasemakohtaisella toteutuksella. Yksinkertaisesti palomuuri suodattaa paketteja, jotka saavat tulla verkkoon ja niitä jotka eivät. Seulonta tapahtuu TCP/IP-pakettien sisältämän lähde- ja kohdeosoitteen sisältöön.



Kuva 4. Palomuurintoiminta /2/

Palomuurit jaetaan yleisesti ottaen kahteen eri luokkaan: tilallisiin (stateful) ja tilattomiin (stateless). Tilaton versio vertaa jokaisen paketin sisältöä sallittujen pakettien listaan, mikäli paketti löytyy listalta, se päästetään eteenpäin. Tilallisessa versiossa pidetään kirjaa yhteyksistä, jotka ovat jo olemassa, ja tällä perusteella saadaan selville yhteyden olemassaolo. Tällöin paketti sallitaan ja päästetään läpi. /2/

Yritysympäristössä on usein useampi palomuuri käytössä tai samassa palomuurissa voi olla ns. DMZ-alue, jonka alaisuuteen sijoitetaan verkon sellaiset palvelut, joihin pääsy on välttämätöntä suoraan ulkoverkosta käsin.



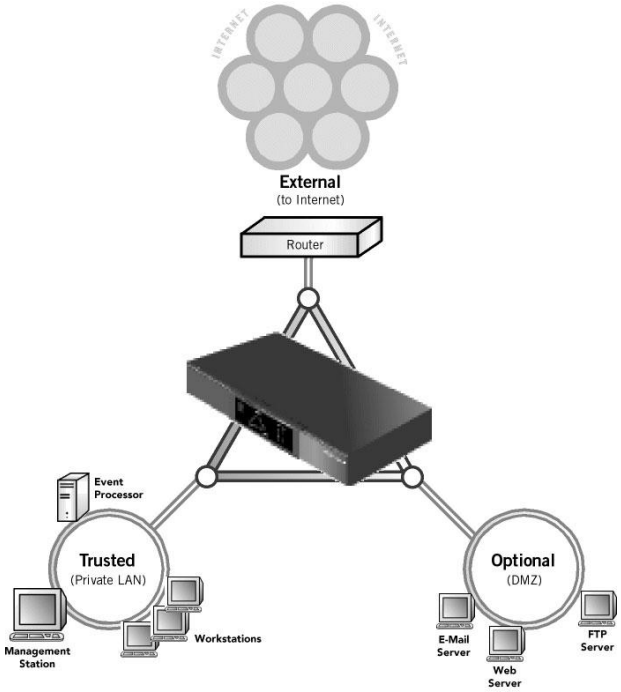
Kuva 5. Esimerkki DMZ-käytännöstä /10/

Toimipisteen palomuurina toimii Watchguard Wg700 –firebox(kuva 6). Tämä malli on tarkoitettu pienille ja keskisuurille yrityksille ja se sisältää VPN-ominaisuudet sekä hyvän hallittavuuden ja ylläpidon. Laite on vanha, mutta toimivuudeltaan ja suojaukseltaan se on ollut tarpeisiin nähden enemmän kuin riittävä.

Prosessorina WG-700:ssa on AMD K6-2 233.0 MHz X86-to-RISC -prosessori.

Kuva 6. WG700 firebox /13/

Palomuurissa on kolme Ethernet-porttia, joista yksi on ns. tuleva portti, yksi suojattu portti ja yks DMZ-portti, johon kytketään kaikki sellaiset palvelut, joihin pitää päästä ulkoverkosta käsiksi suoraan(kuva 7). Tällaisiä DMZ-porttiin tavallisesti kytkettäviä palveluita ovat esim. FTP-palvelin ja WEB-palvelin. Tässä tapauksessa, tähän suoraan ulospäin näkyvään osaan on kytkettynä asiakkaiden web-pohjaiset ketjunohjauspalvelimet eli CC-palvelimet.



Kuva 7. WG700 firebox -porttien käyttö. /12/

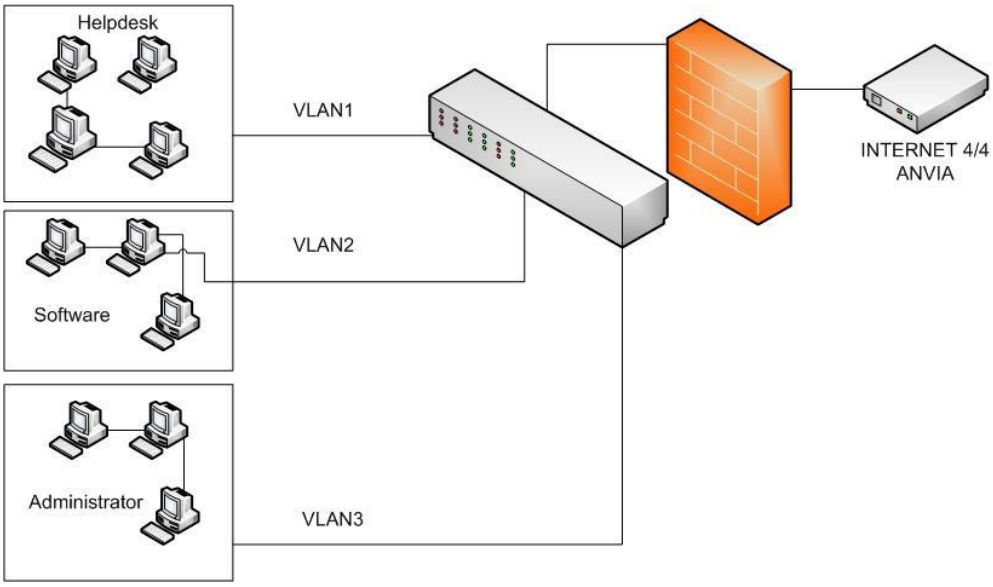
Palomuurin asetuksista ei haluttu tähän työhön ottaa tietoturvasyistä tarkempaa selvitystä yrityksen verkkovastaavan pyynnöstä. Asiasta tehtiin kuitenkin kartoitus: millaisia ’policy’-sääntöjä tällä hetkellä on sekä millaiset VPN-tunnelit muuriin on konfiguroitu.

Lisäksi sovittiin että palomuuriasetuksien muokkaamisesta tehdään eräänlainen versionhallinta ja sovitaan henkilöt, joilla tähän on oikeus. Käytännössä se tarkoittaa verkkovastaavaa sekä yhtä muuta henkilöä.

Palomuurin määrittely -tiedostosta saadaan ohjelmasta otettua helpolla varmuuskopio palautusta varten, jos jotain arvaamatonta tapahtuu. Sovittiin, että ennen jokaista muutosta otetaan varmuuskopio. Lisäksi varmuuskopio otetaan säännöllisesti kuukauden viimeinen päivä joka kuukausi. Lisäksi kävi ilmi, että ylläpitosovellus sekä palomuurin firmware ovat jääneet päivittämättä.

2.5 VLAN

Yhtenä isona tietoturvariskinä nähtiin se, että kaikki verkon laitteet ovat samassa lähiverkossa fyysisesti. Virtuaalinen lähiverkko mahdollistaa samassa kytkimessä olevien verkkolaitteiden rajoittamisen siten, että eri osastojen koneet eivät ole samassa verkossa(kuva 8).

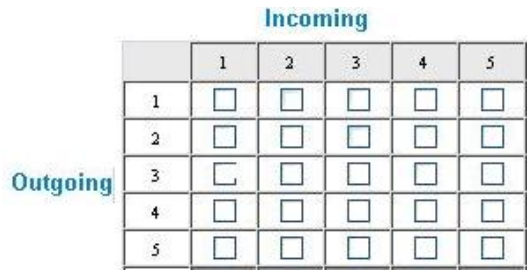


Kuva 8. VLAN-periaatekuva

Koska toimipisteessä olevien verkkolaitteiden määrä on kohtuullisen pieni ja koska käytössä olevat laitteet ovat lähes kaikki pöytäkoneita, joita käytetään vain yhdessä työpisteessä, valittiin kytkimessä yksinkertainen porttikohtaisesti toteutettva VLAN. Näin ollen vältyttiin osoiteavaruuksien muuttamiselta. Suurin osa käytössä olevista osoitteista on reititetty asiakkailta tuleviin etäyhteyksiin läpi palomuurin oikeille asiakaspalveluhenkilöille. Uuden osoiteavaruuden vaihtaminen olisi teettänyt tarpeetonta työtä uudelleenreitityksissä. Jokaisella verkon osastolla on mahdollisuus sulkea toimipisteensä ovi ja näin ollen estää kenenkään ulkopuolisen pääsy fyysisesti oman johdon päähän. Ainoana huonona puolena tässä nähtiin se, että jos kytkimien ristikytkennässä muuttuu jotain, portit voivat sekoittua. Toisaalta verkkoa ylläpitää yksi henkilö, joten tälläinen vaara on hyvin pieni.

Fyysisen tason tietoturvaa parannettiin myös sillä, että vaihdettiin laitetilan oveen lukko, johon vain verkon ylläpitäjällä on avain. VLAN-toteutuksella vältetään se ongelma, että jos esimerkiksi helpdesk-osaston koneista yksi saastuu ja alkaa levittää haittaohjelmaa verkossa, niin koko toimipisteen koneet eivät saastu, vaan ainoastaan yhden osaston, ja ongelmakohta on näin ollen helpompi myös löytää sekä rajata.

Periaate, kuinka portteihin perustuva VLAN tässä valitussa ZyXEL:in GS-2024 -kytkimessä toteuteutetaan, käy ilmi parhaiten alla olevasta kuvasta, joka on otettu suoraan kytkimen konfiguraatioista(kuva 9 & 10).



Kuva 9. Portteihin perustuva VLAN

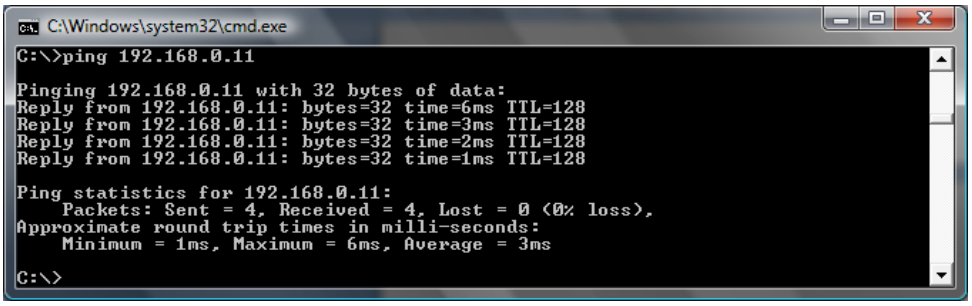
Kuvassa 9 ei ole valittuna vielä mitään porttia, eli yksikään porteista 1−5 ei ole keskenään yhteydessä. Yhteen porttiin voidaan kytkeä esim. palomuurilta tuleva internetyhteys, joka halutaan jakaa kaikille käyttäjille. Lisäksi näkymä voidaan rajata siten, että jokin tietty porttiryhmä näkee vain toisensa kuten alla olevassa kuvassa on.

Kuva 10. VLAN, jossa on määrityksiä.

Tässä kuvan 10 esimerkkitapauksessa portti numero yhdessä on tuleva verkko kaikille nähtävissä ja taas portit 4−5 eivät ole keskenään yhteydessä porttien 2−3 kanssa. /16/ /17/

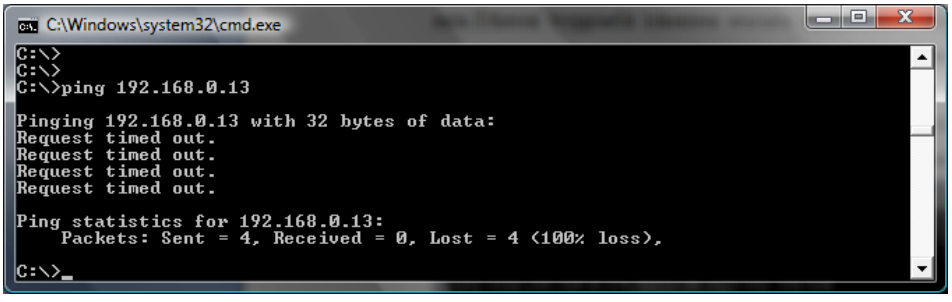
Tälläinen rasteritaulukko on tehty kaikista kytkimen 24 portista, jolloin eri variaatioden tekeminen on helppoa ja yksinkertaista. Lisäksi tässä ei tarvitse kiinnittää huomiota osoiteavaruuksiin.

VLAN:n toimivuutta voitaisiin testata esimerkiksi tutkimalla pakettien kulkua Wireshark-verkkoanalysaattorin tyypisellä ohjelmistolla. Tässä työssä käytettiin yksinkertaista ja tunnettua komentokehoitetyökalua, jolla saadaan selville se, onko laite saatavilla verkossa. Työkalu nimeltään Ping toimii komentokehotteessa ja sisältyy Windowsin perusasennukseen. Ping lähettää ICMP-paketin johon toisessa päässä oleva kone vastaa automaattisesti, jos on saatavilla.(kuva.11)



Kuva 11. Ping- laite saatavilla

Jos kone ei ole saatavilla (kuva 12), vastausta ei tule, eli silloin kone on eri VLAN-verkossa kuin pingaava kone tai etäkoneen palomuuri estää pingin läpipääsyn. Yrityksessä ei ole käytössä konekohtaisia palomuureja.



Kuva 12. Ping- laite ei saatavilla

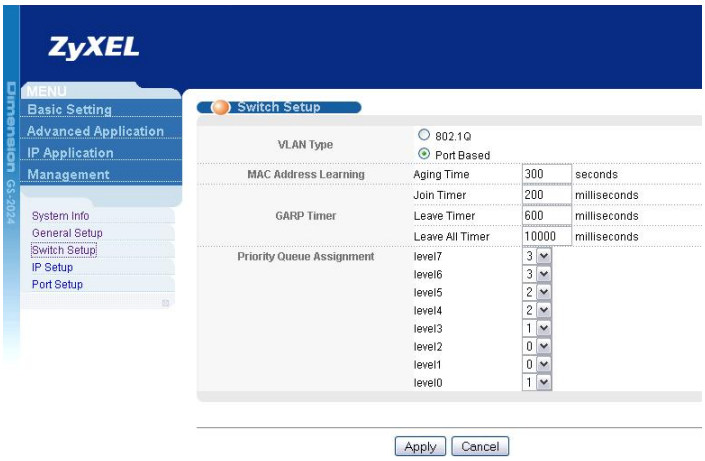
2.6 Kytkin GS-2024

Kytkinten hankinnasta tehtiin laitteistotoimittajalle tarjouspyyntö varsin vapaamuotoisena. Vaatimuksena oli ainoastaan täysin hallittava 24-porttinen kytkin, jossa on VLAN-ominaisuus.

Toimittaja tarjosi kahta erihintaista ratkaisua, ja tässä tapauksessa päädyttiin edullisempaan mutta kuitenkin merkkituotteeseen Zyxelin GS-2024:ään (kuva 13). Tämä laite täyttää vaatimukset, joita oltiin hakemassa. Laite on layer 2 -hallittava kytkin, joka tukee IEEE 802.ab 1000 Base-T Ethernet -standardia, ja siitä löytyy VLAN-ominaisuus. /17/

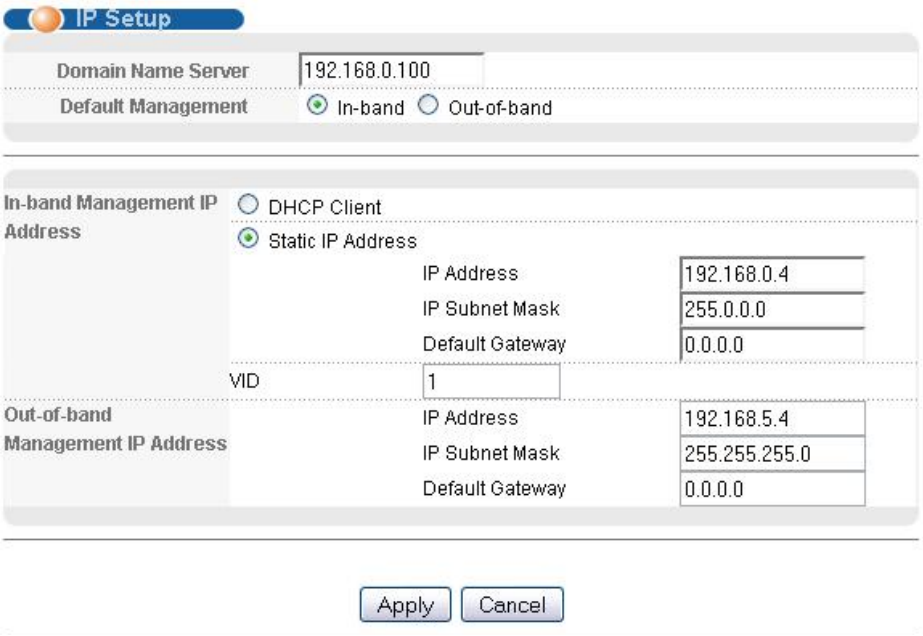
Kuva 13. GS-2024 -kytkin /15/

Kytkimen hallintaan asetettiin salasana ja käyttäjätunnus ja kytkimeen pääsy jokaisesta portista sallittiin. Kytkimen selainpohjainen käyttöliittymä oli varsin selkeä ja helppo ymmärtää alusta lähtien(kuva 14).



Kuva 14. Hallintanäkymä GS-2024 WEB -hallintaosuudesta.

Kytkimen hallinta tapahtuu helposti ja havainnollisesti selaimella. Tarvittavat asetukset on jaettu neljään pääryhmään, joiden alta löytyvät jaetut alaryhmät. Tehdasasetuksilla kytkimeen oli laitettu osoite 192.168.0.1, jonka avulla selaimella pääsi käsiksi kytkimeen. Tämä oli siis kytkimen osoite, joka muutettiin tarkoituksenmukaiseksi(kuva15).



Kuva 15. IP-setup

Yrityksessä on käytössä oma DNS-palvelin, joka pyörii Windows Server 2000:ssa. Lisäksi määriteltiin kytkimelle kiinteä osoite, joka määriteltiin myös serverille siten, että osoite on DHCP-palvelimen osoiteavaruuden ulkopuolella. Tässä ei pääse tulemaan tilannetta jossa osoitteet menisivät päällekkäin.

3 TIETOVERKON DOKUMENTOINTI

3.1 Yleistä

Tietoverkon dokumentointi helpottaa verkon ylläpitoa ja verkossa olevien laitteiden hallintaa. Dokumentointi jaetaan yleensä kahteen eri pääperiaatteeseen: loogiseen osaan ja fyysiseen osaan.

Loogisen osan kuvauksesta ilmenee järjestelmän laitteet. Looginen kuvaus voi olla hyvinkin suurpiirteinen mutta siitä selviää kuitenkin verkon rakenne. Fyysisessä osassa pyritään havainnollistamaan laitteiden fyysinen jakautuminen eri osiin. Fyysisestä osasta ilmenevät tarkemmat yksittäisen laitteen tiedot sekä sijainti verkossa.

Verkon kaikkien laitteiden listaus sekä looginen nimeäminen on erittäin tärkeää. Yksi käytännön kannalta tärkemmistä asioista on verkkorasioiden looginen numerointi ja nimeäminen. /4/ Verkkodokumentointi nopeuttaa ja helpottaa vikatilanteiden ratkaisua.

3.2 Dokumentoinnin nykytila

Vaasan toimipisteessä varsinaista verkon dokumentointia ei oltu tehty. Onneksi verkkorasioiden numerointi oli suoritettu hyvin verkkokaapeloinnin yhteydessä. Laitteista oli eräänlainen listaus ilman tarkempia tietoja, jotta tiedetään mitä laitteita on omassa käytössä. Tämä oli aikoinaan tehty siitä syystä, että voidaan tehdä verotuksellisia poistoja laitteista.

Dokumentointi aloitettiin kartoittamalla verkossa käytössä olevat palvelut ja laitteet. Dokumentointiin käytettiin Microsoftin Visio 2007:ää. Se on monimutkaisten tietojen, järjestelmien ja prosessien havainnollistamiseen tarkoitettu suunnittelutyökalu. Vaikka Visio ei ollut tuttu entuudestaan, oli sen perusominaisuuksien löytäminen helppoa.

Verkon koneista tehtiin kartoitus sisältäen, liitteen kolme mukaiset tiedot. Tämän avulla pystyttiin seuraamaan mitä lisenssejä eri käyttäjillä on. Konekohtainen tarkka dokumentaatio helpottaa myös koneiden päivityskierron seuraamista.

Verkkorasioiden sijainnista oli alun perin tarkoitus piirtää AutoCAD-kuva sisältäen rakennuksen pohjapiirrustuksen. Tämä kuitenkin ratkaistiin tekemällä looginen kuvaus Microsoft Visiolla eri rasioiden sijainneista. Tämän avulla pystytään riittävän hyvin päättelemään rasioiden fyysinen sijainti. Tämä yhdistetty loogisen ja fyysisen dokumentin tyyppi nähtiin riittävän selkeäksi ja toimivaksi ratkaisuksi.

3.3 Verkon palvelut

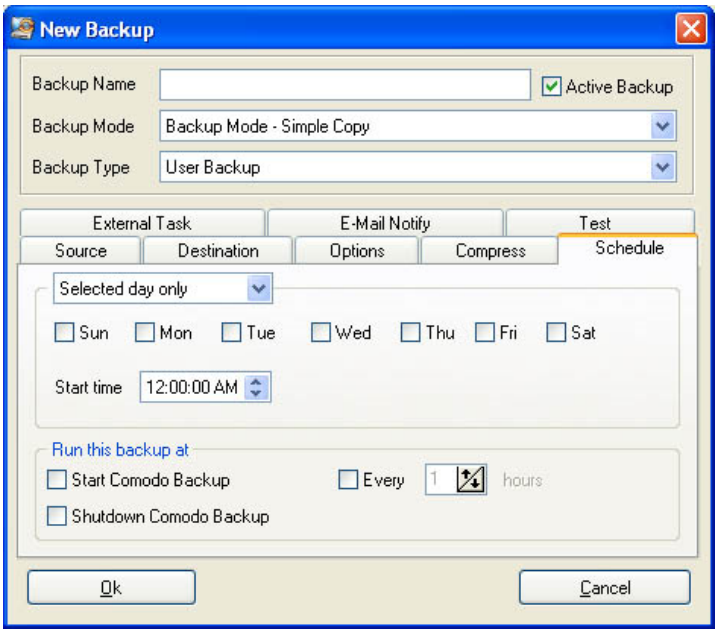
Yrityksessä on käytössä Active Directory (AD) -kirjautumisjärjestelmä, joka on käyttäjätietokanta Microsoft Server -ympäristössä toteutettuna. AD:ssa pystytään luomaan erilaisia ryhmiä sekä antamaan ryhmille erilaisia käyttöoikeuksia verkossa. Tätä yleistä AD:tä kutsutaan nimellä Active Directory Domain Services (AD DS). Tämä palvelu tarjoaa tunnistaumispalvelun, hakemistopalvelut ja tallennuspalvelut. AD DS:ää täydentävät useat muut palvelut, jotka tuovat lisäominaisuuksia kirjautumiseen, levypalveluiden ylläpitoon ja käyttöoikeuksiin. /7/

Nyt verkkoa pyörittää noin kuusi vuotta vanha Server 2000 -ohjelmiston sisältävä tietokone. Tämä laite ja järjestelmä alkavat olla varsin suuri uhka, koska laite alkaa olla teknisesti ja ohjelmallisesti vanhentunut. Tällä palvelimella pyörii toimipisteen DNS-palvelu, DHCP-palvelu ja palomuurin hallinta. Käytännössä tämä tarkoittaa sitä, että jos tämä palvelin jostain syystä rikkoutuu, niin koko toimipisteen verkko on poissa käytöstä. Tämä ei kuitenkaan vaikuta asiakkailta tuleviin etäyhteyspyyntöihin, koska ne on reititetty suoraan asiakaspalvelvelijoiden koneisiin IP-osoitteen perusteella.

Tämän palvelimen osalta käytiin läpi asetukset, jotka se pitää sisällään, eli dokumentoitiin IP-asetukset, DHCP-alue (pool) ja DNS-asetukset. Lisäksi otettiin varmuuskopiot tämänhetkisistä palomuuriasetuksista.

3.4 Varmuuskopiointi

Varmuuskopiointi oli toteutettu Serverillä Comodo BackUp -ohjelmistoon. Comodo on ilmainen ohjelmisto jolla pystytään ajastamaan helposti varmuuskopioinnit(kuva 16). Käytössä on ulkoiset kovalevyt jotka vaihdetaan kerran viikossa ja toiset levyt viedään fyysisesti turvaan, jolloin voidaan taata varmistus vaikka toimitilat tuhoutuisivat palossa tai koko kalusto varastettaisiin.



Kuva 16. Comodo ajastettu varmuuskopiointi

Comodo bacup- varmuuskopionti sisältää varsin monipuoliset ominaisuudet siihen nähden, että se on ilmainen sovellus. Ohjelma ilmoittaa sähköpostitse jos varmuuskopionnissa tulee jokin ongelma tai esimerkiksi kohdelevy on täynnä.

Tämä varmuuskopionti sovellus on todettu varsin toimivaksi ratkaisuksi mutta keskusteltiin myös verkkovarmennuksen käyttöönotosta. Winpos oy tarjoaa asiakkailleen yhteistyössä Storage IT Oy verkkovarmennuspalvelua jota harkittiin myös jossain vaiheessa otettavaksi omaan käyttöön. Verkkovarmennuspalvelussa tiedot kopioidaan verkon yli toisessa tilassa sijaitsevaan verkkopalveluun jossa ne ovat vastaavalla tavalla turvassa. Asiasta keskusteltiin ja päädyttiin kuitenkin

pitämään varmennuspalvelu itsellä. Ulkoiset kovalevyt päätettiin uudistaa Lacien tarjoamiin iskuja sietäviin malleihin(kuva 17).

Kuva 17. Uusi Lacien ulkoinen kovalevy //15

3.5 Kaapelitestaukset

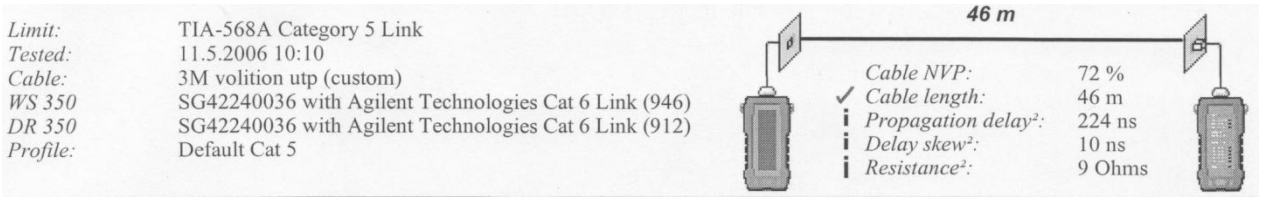
Koko toimipisteen verkko testattiin Agilent WireScope 350 –testerillä (kuva 17), joka suorittaa testauksen varsin automaattisesti, antaen selkeän raportin testatusta kaapelista.

Kuva 18. WireScope 350

Kaapelitestaukset toteutettiin yhteistyössä kaapeloinnin tehneen yrityksen kanssa. Näin varmistuttiin uusien kaapelointien onnistumisesta sekä vanhan kaapeloinnin kunnosta.

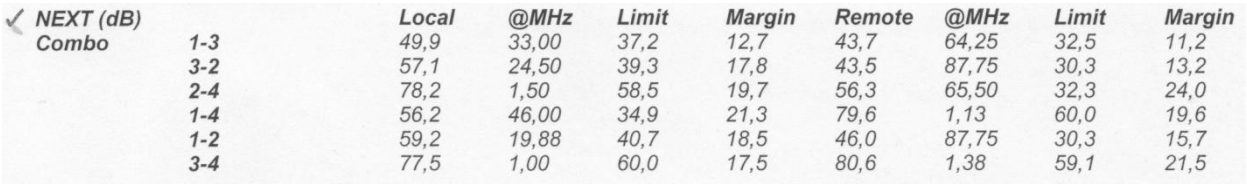
Liitteenä (5) nähdään, millaisen testiraportin laite antaa CAT5-luokitetusta kaapelista sekä CAT6-luokan kaapelista(liite. 6). Testauslaite asettaa tietyt rajat testattavalle kaapelille ja kertoo testin jälkeen, täyttääkö testattu osuus nämä arvot.

Raportin alussa nähdään profiili, joka on asetettu testaukseen, sekä perustiedot kaapelista kuten pituus(kuva 19).



Kuva 19. Testauksen perustiedot

Testiraportista nähdään jokaisen parikaapelin parin asetetut rajat sekä mitatut arvot(kuva 20):



Kuva 20. NEXT-mittaus

Kuvassa 20 nähdään NEXT-testissä olleen kaapelin lähipään ylikuuluminen (near end crosstalk). NEXT tarkoittaa ylikuulumista kaapeliparien välillä lähipäässä. Parikaapelissa on kierrettyjä pareja, joilla pyritään vähentämään tätä ominaisuutta, koska tämä on signaalin siirron kannalta erittäin tärkeää. /5/

Työssä ei tarkasteltu testauksen antamia arvoja tarkemmin. Tyydyttiin siihen, että osa verkosta oli vanhempaa kaapelointia. Vain uusi kaapelointi täytti CAT6-luokituksen.

4 PALVELIMEN PÄIVITYS

4.1 Nykytila

Kuten aikasemmin kävi ilmi, yrityksellä on käytössä Microsoftin Windows 2000 -käyttöjärjestelmä serverinä. Server 2000 -käyttöjärjestelmä julkistettiin Windows NT:n seuraajaksi helmikuussa 2000. Server-versioon on ilmestynyt neljä korjauspakettia (Service Pack), joista viimeisin, versio neljä, on julkaistu 2003. Tämän käytössä olevan serveriversion laajennettu tuki päättyy vuonna 2010. /6/

Laitteisto, jossa ohjelmisto on asennettuna, on myöskin vanhentunut. Tämän vuoksi joudutaan miettimään uusia ratkaisuja tämän suhteen.

Yhtenä vaihtoehtona oli ulkoistaa osa serverin toiminnoista ja ylläpidosta paikallisen puhelinyhtiön Anvian laitetilaan. Yrityksellä oli positiivisia kokemuksia Anvian serveripalveluiden tarjonnasta. Tästä pyydettiin tarjousta. Tarjouksen saavuttua päädyttiin kuitenkin lopputulokseen hankkia tulevaisuudessa fyysisesti oma palvelin. Hintataso oli suhteessa korkea ja haluttiin pysyä vanhassa periaatteessa. Yrityksellä on käytössä hyvä ilmastoitu laitetila, jossa muutkin palvelimet sijaitsevat. Tämä osaltaan tuki oman serverin hankintaa.

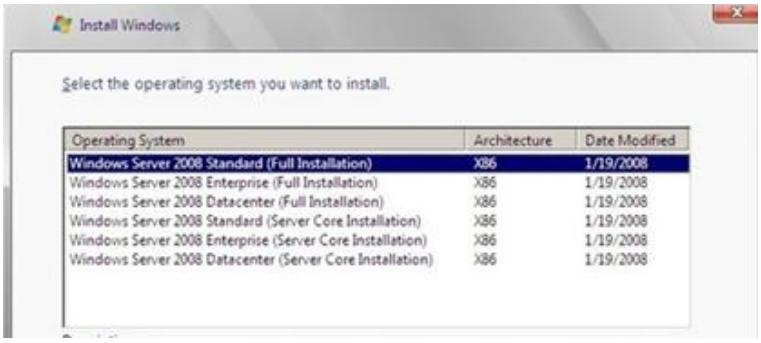
4.2 Toteutus

Alkuperäisessä suunnitelmassa oli tarkoitus asentaa ja toteuttaa täysin toimiva ja vastaava palvelin Windows Server 2008 ympärille, joka nyt on käytössä. Siirtäen käyttäjätietokannan ja muut asetukset uuteen ympäristöön. Tätä ei kuitenkaan kokonaisuudessaan toteutettu vaan serverin tiedot otettiin talteen vienti-ominaisuutta käyttäen. Lisäksi todettiin AD-listalla olevan erittäin paljon sellaisia käyttäjiä joita ei talossa enää ole. Käyttäjät olivat kuitenkin kytketty pois käytöstä. Alkuperäisen suunnitelman mukaan perehdyttiin server ympäristön asennuksen vaiheesiin. Testiympäristö toteutetaan, jossa tutkitaan erilaisten palvelujen perustamista tyhjälle alustalle.

Palvelimelta pyrittiin ottamaan kaikki konfiguroinnit talteen, joita uuden palvelimen perustamisessa tarvitaan. Näin varmistettiin verkon perustietojen varmuuskopiointi siten, että pystytään perustaamaan uusi palvelin, tarvittaessa.

4.3 Testiympäristö

Testiympäristö asennettiin normaaliin pöytäkoneympäristöön. Asennus ei poikkea paljon peruskäyttöjärjestelmän asennuksesta. Asennuksen alussa pitää valita mikä versio ollaan asentamasssa. Tässä tapauksessa käytettiin Windows Server 2008 enterprise- täydellistä asennusta, koska tämä versio tulisi olemaan käytössä todellisessa asennuksessakin (kuva 21).



Kuva 21. Asennettevan version valinta

Asennuksen yhteydessä kysytään koneen nimeä ja järjestelmänvalvojan salasanaa. Kokonaisuudessaan perusasennus on nopea ja yksinkertainen tehdä. Perusasennuksen jälkeen palvelimelle ei ole asennettu mitään rooleja. Roolit ovat komponentteja, jotka tarjoavat palvelintoiminnallisuuksia. Testiympäristössä tutustuttiin roolien asentamiseen Server Manager –hallintakonsolin avulla. Esimerkiksi AD- käyttäjätietokanta on yksi rooli, joka tarjoaa tunnistuspalvelut ja hakemistopalvelut.

Se,mitkä roolit pitää asentaa ja millaiset konfiguroinnit niille pitää suorittaa ei täysin ratkennut koska erittäin vähäinen kokemus aiheesta vaikeutti selvitystä. Tässä kohtaa kuitenkin suurena apuna oli Jyrki Kivimäen kirjoittama seikkaperäinen kirja Windows Server 2008 – Tehokas hallinta. Kirjassa käydään tarkasti läpi miten eri roolit luodaan ja mihin niitä tarvitaan. /7/

5 TULOKSET

Työssä tavoitteena oli kartoittaa vaasalaisen Winpos Oy:n sisäverkon tila. Lisäksi oli tarkoitus parantaa sisäverkon tietoturvaa ottamalla käytöön virtuaalinen lähiverkkoratkaisu.

Työn lopputuloksena yritykseen vaihdettiin uudet kytkimet sekä sisäverkko dokumentoitiin. Uusien kytkimen avulla toteutettiin VLAN-ratkaisu sekä nostettiin sisäverkon nopeutta. Lisäksi käytiin läpi palomuurin säännöt sekä toimintamallit, kenellä on oikeus muuttaa sääntöjä ja miten muutokset merkitään. Verkon nopeuden nostamisen yhteydessä koko Vaasan toimipisteen kaapelointi testattiin WireScope- testilaitteella.

Dokumentoinnin yhteydessä tutkittiin verkkoa ylläpitävän serverin päivitysmahdollisuutta. Tämän osalta tehtiin testiympäristö, johon asennettiin Microsoft Server 2008.Ympäristössä tutustuttiin pintapuolisesti uuden palvelinohjelmiston toimintaan mutta varsinainen pilotointi jäi tekemättä.

6 YHTEENVETO

Työn alkaessa keväällä tilanne oli varsin haastava, kun henkilö, joka oli vastannut pääosin yksin verkon toiminnasta, sanoi siirtyvänsä toisen yrityksen palvelukseen. Tästä lähti työn tilaajan huoli verkon dokumentaatiosta sekä tietotaidon siirtämisestä poistuvalta henkilöltä. Alussa selvitettiin lähinnä fyysisiä verkkorakenteita ja käytiin läpi verkon tarjoamia palveluita. Tässä vaiheessa huomattiin, että verkon dokumentointia ei ollut suoritettu lainkaan tai se oli erittäin puutteellinen. Työn alkuvaiheet menivät varsin nopeasti läpi ja uutta asiaa tuli erittäin paljon vastaan. Tämä kaikki tapahtui tiiviissä tahdissa kahden viikon aikana. Pidimme useita palavereita, joissa kävimme asioita läpi ja kokonaiskuva verkosta alkoi muodostua.

Opinnäytetyön aihe oli hyvin laaja ja sisälsi paljon itsenäistä selvittelyä. Yrityksen verkkopalveluiden ylläpitäminen oli itselleni uutta ja vierasta asiaa. Yritysverkkojen hallinnasta ei koulun kursseilla ollut puhuttu juurikaan mitään, joten pohjatiedotkin olivat hyvin puutteelliset. Olosuhteiden pakosta kuitenkin toiminnallinen osa saatiin vauhdilla käyntiin ja asiat alkoivat selkeytyä.

Työn ensisijaisena prioriteettina oli saada ns. know how pysymään yrityksen sisällä, vaikka henkilöstö vaihtuisi tehtävissä. Lisäksi tarkoituksena oli parantaa tietoturvaa ja estää tilanteita, joissa koko sisäverkko saastuisi yhdestä koneesta. Tämä toteutettiin uusien kytkimien ja VLAN-ominaisuuden avulla.

Kokonaisuudessaan työ oli opettavainen ja tärkeimmät tavoitteet saavutettiin.
Jatkoa työlle seuraa varmasti tutustuessa palvelinympäristön haasteisiin.
Mahdollisen uuden serverin asennukseen työssä tehdyt dokumentit antavat hyvän tuen

LÄHTEET

/1/ DMZ - Demilitarized Zone [online] [viitattu9.11.2009] Saatavilla www muodossa < URL: http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm>

/2/ Firewall [online] [viitattu30.11.2009] Saatavilla www muodossa < URL: http://en.kioskea.net/contents/protect/firewall.php3 >

/3/ Granlund, Kaj: Tietoliikenne 2003 ISBN 951-846-133-3 WSOY

/4/ Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: Docendo.

/5/ Jaakohuhta Hannu Lähiverkot – Ethernet ISBN 951-826-787-1 IT Press 2005

/6/ Introduction to VLAN Article written by Jean-François PILLOU [online] [viitattu 25.10.2009] Saatavilla www-muodossa <URL: http://en.kioskea.net/contents/internet/vlan.php3 >

/7/ Kivimäki, Jyrki: Windows Server 2008 ISBN 978-952-565-578 readme.fi

/8/ Krokfors Sören, Verkkoasiantuntija 24.3.2009. Winpos Oy, Vaasa. Palaveri / Haastattelu.

/9/ NEXT [online] [viitattu9.11.2009] Saatavilla www muodossa <URL http://www.tlu.ee/~matsak/telecom/lasse/testing_of_cabling/mitattavat_parametrit.html

/10/ Pint-of-Sale System Basics for Retailers 2005, What is POS? artikkeli 27.5.2005 [online].[Viitattu 29.5.2009]. Saatavilla www-muodossa <URL: http://www.entrepreneur.com/technology/howtoguide/article77960.html >

/11/ Puska Matti: Lähiverkkojen tekniikka ISBN 951-762-991-5 Suomen Atk-kustannus Oy 1999

/12/ WatchGuard®Firebox System Configuration Guide v.7.4.1 [online] [viitattu 29.5.2009] Saatavilla pdf muodossa <URL:http://www.watchguard.com/help/docs/wfs/75/v75wfsconfigurationguide.pdf>

/13/ WatchGuard®Firebox System HardwareGuide [online] [viitattu 29.5.2009] Saatavilla pdf muodossa <URL: http://www.watchguard.com/help/docs/FBIII+700HardwareGuide.pdf>

/14/ Winpos mallikokoonpano [online] [viitattu30.11.2009] Saatavilla www muodossa <URL: http://www.winpos.fi/Mallikokoonpano.fin.432.html >

/15/ Varmuuskopio levy Lacie [online] [viitattu30.11.2009] Saatavilla www muodossa http://www.lacie.com/fi/products/product.htm?pid=10995

/16/ VLAN-perusteet aliverkotus [online] [viitattu30.11.2009] Saatavilla www muodossa <URL: http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html >

/17/ Zyxel GS-2024 User's Guide v 3.8 20.6.2008 [online].[Viitattu 29.5.2009]. Saatavilla valmisttajan sivulta pdf muodossa <URL: http://www.zyxel.com/web/support_download_list.php?indexflag=20040906173729&ModelIndexflags=0,420041005165244# >

LIITTEET

Liite 1 VLAN konfigurointi

Liite 2 Verkkorasiakuvaus

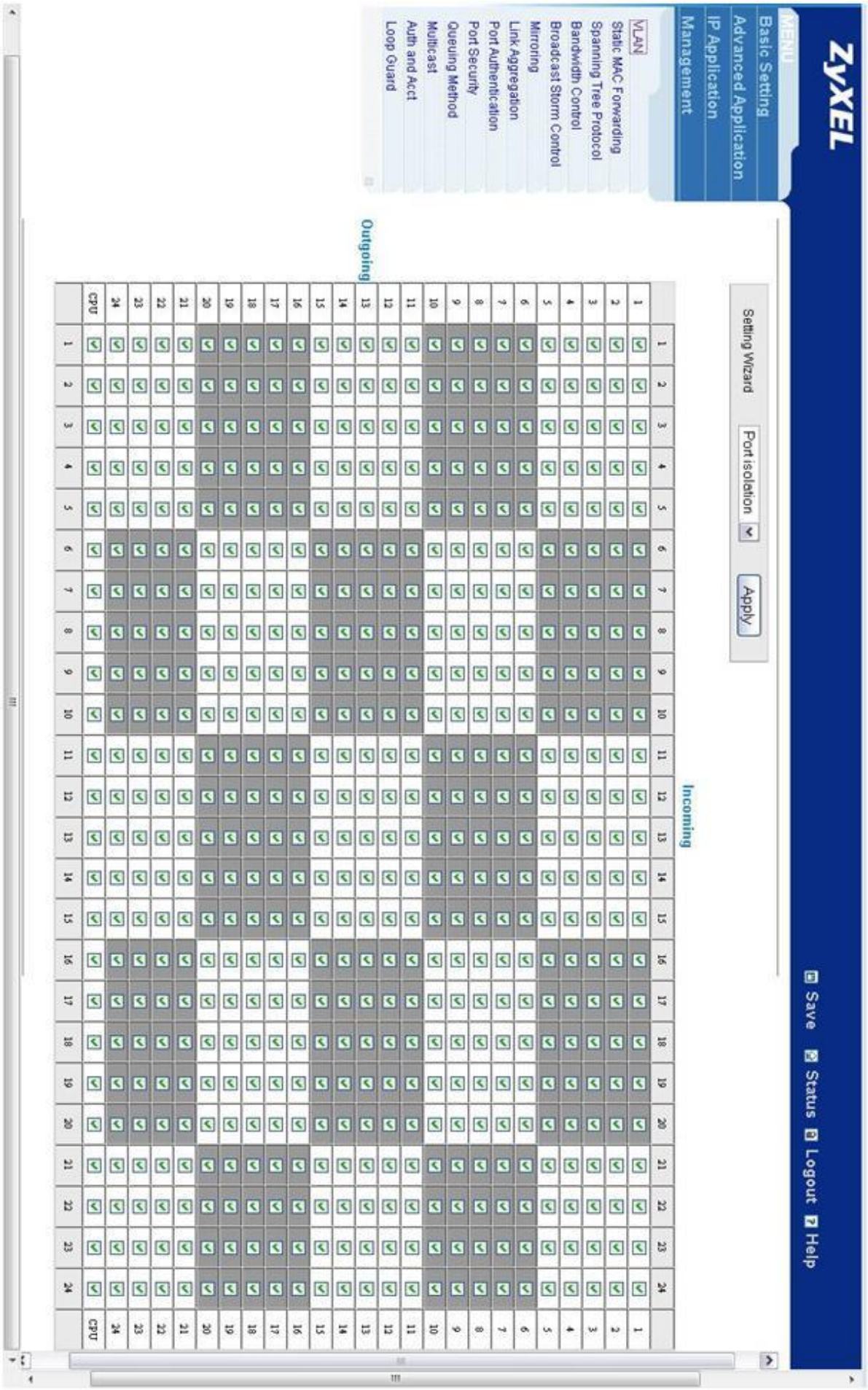
Liite3 Laitekantamalli

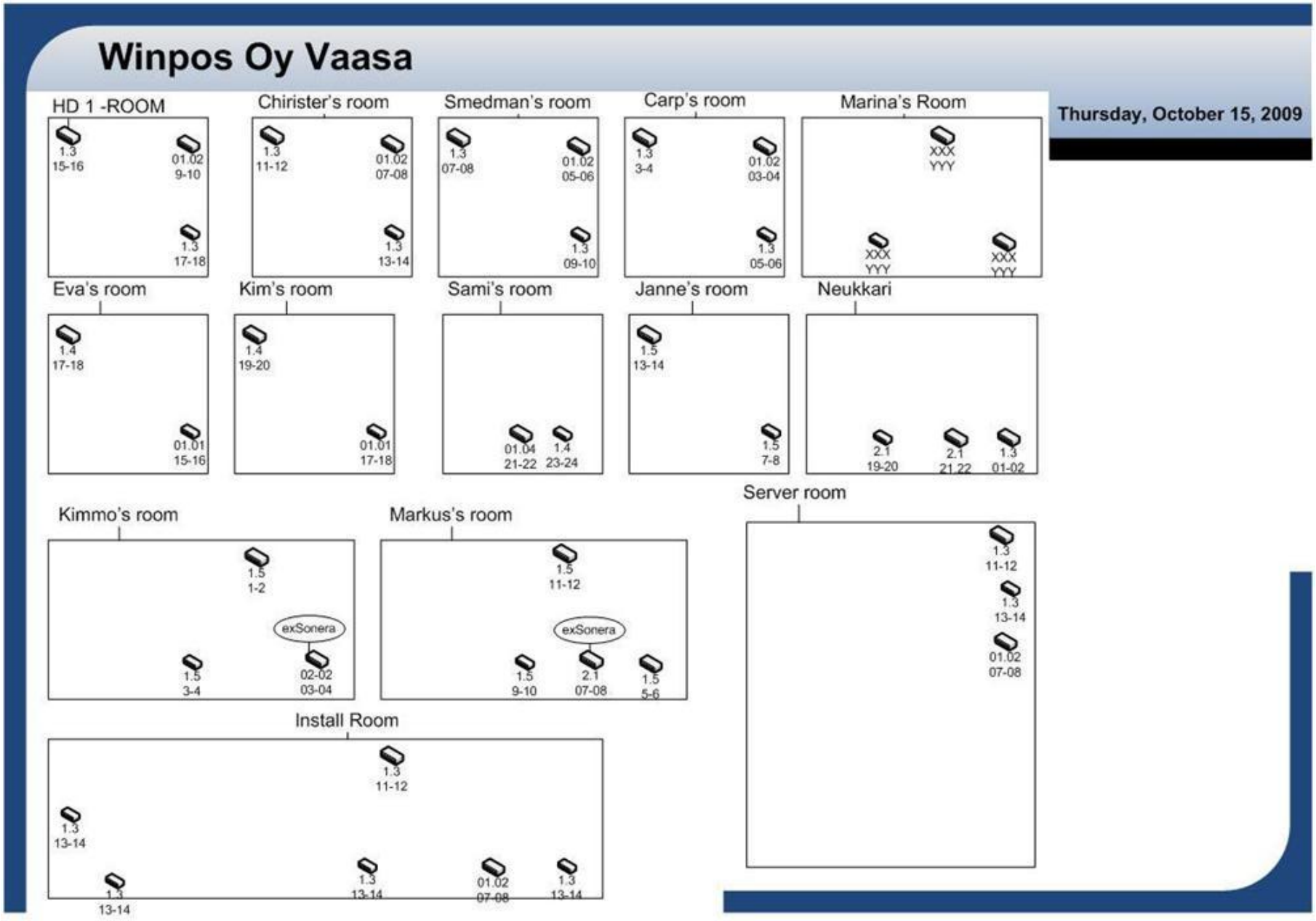
Liite4 GS-2024 tekniset tiedot

Liite5 CAT5 testausraporttiesimerkki

Liite6 CAT6 testausraporttiesimerkki

Liite 1 VLAN konfigurointi





Liite 2 Verkkorasiakuvaus

Laitekanta	
Käyttäjä:	**Käyttäjä N.N**
Laitenro:	**kn2**
Koneen nimi:	**Helpdesk7**
Hardware	
	Carrot tausta G31
Malli:	**core2**
Carrot sarjanro:	**2498**
Valmistettu:	**22.08.08**
Käyttöönotettu:	**1.5.2007**
Prosessori:	**Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz**
Emolevy:	**Intel P35/G33/G31 Revision A2**
Muisti:	**Slot1 1024 MB Slot2 1024 MB yht: 2048MB**
Kovalevy:	**ST380815AS [Hard drive] (80,02 GB)**
IP:	**192.168.x.x**
MAC-osoite:	**00-1A-xx-xx-xx-xx**
Software	
OS:	
Name	**Windows XP Professional Service Pack 2**
Windows Key	**KKKK-KKKK-KKKK-KKKK-KKKK**
Serial Number	**7777-OEM-77777-77777**
Microsoft Office Small Business 2003	**HHHH-HHHHH-HHH6-9YCBR-DTJ7M**

GS-2024

24-port Managed Layer 2 Gigabit Ethernet Switch with 2 SFP Slots

Specification

System Specifications

Standard Compliance

IEEE 802.3 10Base-T Ethernet

IEEE 802.3u 100 Base-Tx Ethernet

IEEE 802.ab 1000 Base-T Ethernet

IEEE 802.3z

IEEE 802.3x Flow control

IEEE 802.1d Spanning tree protocol

IEEE 802.1w Rapid Spanning tree protocol

IEEE 802.1p Class of service, priority protocols

IEEE 802.1Q VLAN tagging

IEEE 802.1x

IEEE 802.3ad Port aggregation

Performance

48Gbps non-blocking switching fabric

35.7 million packet-per-second forwarding rate

Flexible design for both Gigabit copper and Gigabit fiber connectivity

1488000pps forwarding rate for 1000Base-T/1000Base-X connectivity,

148800pps forwarding rate for 100Base-Tx connectivity

Wire-speed performance

MAC and Packet Buffer

8K MAC entries

4Mbits packet buffer

Traffic Management and QoS

IEEE 802.1p

4 egress queues per port for different types of traffic

WRR (Weighted Round Robin) scheduling for different prioritization of packets

SPQ (Strict Priority Queuing) for highest priority packets to get best service

IEEE 802.1Q tag-based and port-based VLAN

256 static VLAN, up to 4K dynamic VLAN

Support GVRP, automatic VLAN member registration

Supports jumbo frame, up to 9K Bytes

Supports IGMP snooping

Congestion control on all ports

Rate Limiting

Supports 14 scales for incremental rate limiting incrementally

Link Aggregation

IEEE 802.3ad compliant

Support LACP, static and dynamic link aggregation

Up to 4 aggregation groups

8 ports per group randomly selected Redundancy for Fault Backup

IEEE802.1w Rapid Spanning Tree Protocol(RSTP) provides rapid convergence of spanning tree independent of spanning-tree timer

User Security and Authentication

MAC filtering per port secures access to each port
Specific MAC forwarding per port: only specified MAC addresses can access the network (port lock)
802.1x port-based security, prevent unauthorized client access to the network
Private VLAN provides security and isolation between ports on a switch, ensures that users can not snoop on each other's traffic
Network Administration Security
User name/password required for web/telnet/local console administrators
Two level security by specific SNMP read/write community
Network Management
Supports ZyXEL iStacking up to 24 switches can be managed by one IP
Web-based management
Telnet CLI
SNMP v2c
RS-232c Local console
IP management: static IP or DHCP client
RMON four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
Port mirroring: supports Source/Destination/Both port mirroring
Hardware Specification
Interface connections
24 100/1000Base-T, auto-negotiation and cross-over
2 shared SFP open slots
1 console port, D-Sub 9 pin Female (DCE)
1 out-of-band management port, RJ-45
Physical Specification
Dimensions: 440 (W) x 300 (D) x 445 (H) mm
Weight: 4 Kg
Power Requirement
Input voltage of AC: 100-240VAC, 50/60Hz
Max power rating of AC: 50 Watt
Environmental Specification
Operating temperature: 0 ~ 45C
Storage temperature: -25 ~ 70C
Operating humidity: 10 ~ 90%, non-condensing

Liite 5 CAT 5 Testaus raportti

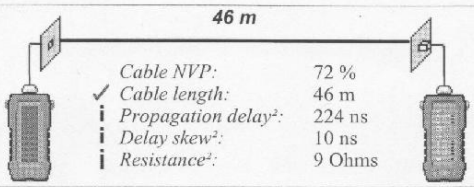
WireScope 350

Site: WINPOS
Rack: 1
Patch Panel: 1
Cable Label: 1-1-1

5
PASS

Cable Certification Report (Pair-to-pair data)

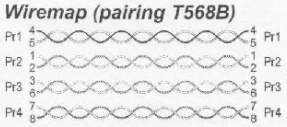
Limit: TIA-568A Category 5 Link
Tested: 11.5.2006 10:10
Cable: 3M volition utp (custom)
WS 350 SG42240036 with Agilent Technologies Cat 6 Link (946)
DR 350 SG42240036 with Agilent Technologies Cat 6 Link (912)
Profile: Default Cat 5



Cable NVP:	72 %	
✓ *Cable length:*	46 m	
¡ *Propagation delay²:*	224 ns	
¡ *Delay skew²:*	10 ns	
¡ *Resistance²:*	9 Ohms	

✓ Attenuation (dB)		Value	@MHz	Limit	Margin
Pair	1 (4,5)	9,4	99,25	21,3	11,9
	2 (1,2)	9,5	99,75	21,4	11,9
	3 (3,6)	9,2	100,00	21,6	12,4
	4 (7,8)	9,1	99,75	21,4	12,3

Wiremap (pairing T568B)



✓ NEXT (dB)		Local	@MHz	Limit	Margin	Remote	@MHz	Limit	Margin
Combo	1-3	49,9	33,00	37,2	12,7	43,7	64,25	32,5	11,2
	3-2	57,1	24,50	39,3	17,8	43,5	87,75	30,3	13,2
	2-4	78,2	1,50	58,5	19,7	56,3	65,50	32,3	24,0
	1-4	56,2	46,00	34,9	21,3	79,6	1,13	60,0	19,6
	1-2	59,2	19,88	40,7	18,5	46,0	87,75	30,3	15,7
	3-4	77,5	1,00	60,0	17,5	80,6	1,38	59,1	21,5

¡ Return Loss² (dB)		Local	@MHz	Remote	@MHz
Pair	1 (4,5)	22,2	1,00	19,3	98,50
	2 (1,2)	21,1	95,25	21,5	44,50
	3 (3,6)	19,5	91,00	17,3	96,25
	4 (7,8)	21,0	90,25	18,8	75,00

¡ ELFEXT² (dB)		Value	@MHz
Combo	1-3	42,8	99,25
	3-2	46,3	58,25
	2-4	52,1	89,50
	1-4	42,5	68,00
	1-2	43,1	97,75
	3-4	45,8	99,50

¡ ACR² (dB)		Local	@MHz	Remote	@MHz
Combo	1-3	34,6	99,25	31,8	100,00
	3-2	38,3	97,25	33,7	100,00
	2-4	49,8	97,50	49,2	65,50
	1-4	46,6	82,25	49,1	81,25
	1-2	40,5	92,75	37,3	87,50
	3-4	46,7	97,25	46,5	84,00

Networks tested

10 Base-T **PASS** *100 Base-Tx* **PASS**

² Not required for selected limit

Liite6 CAT 6 Testaus raportti

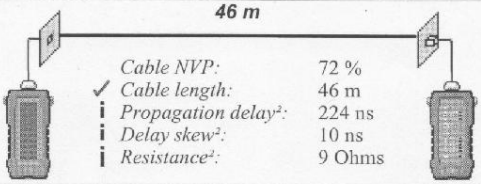
WireScope 350

Site: WINPOS
Rack: 1
Patch Panel: 1
Cable Label: 1-1-1

5
PASS

Cable Certification Report (Pair-to-pair data)

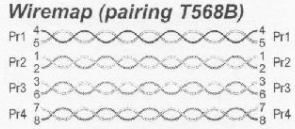
Limit: TIA-568A Category 5 Link
Tested: 11.5.2006 10:10
Cable: 3M volition utp (custom)
WS 350 SG42240036 with Agilent Technologies Cat 6 Link (946)
DR 350 SG42240036 with Agilent Technologies Cat 6 Link (912)
Profile: Default Cat 5



Cable NVP:	72 %	
✓ *Cable length:*	46 m	
¡ *Propagation delay²:*	224 ns	
¡ *Delay skew²:*	10 ns	
¡ *Resistance²:*	9 Ohms	

✓ Attenuation (dB) Pair		Value	@MHz	Limit	Margin
	1 (4,5)	9,4	99,25	21,3	11,9
	2 (1,2)	9,5	99,75	21,4	11,9
	3 (3,6)	9,2	100,00	21,6	12,4
	4 (7,8)	9,1	99,75	21,4	12,3

Wiremap (pairing T568B)



✓ NEXT (dB) Combo		Local	@MHz	Limit	Margin	Remote	@MHz	Limit	Margin
	1-3	49,9	33,00	37,2	12,7	43,7	64,25	32,5	11,2
	3-2	57,1	24,50	39,3	17,8	43,5	87,75	30,3	13,2
	2-4	78,2	1,50	58,5	19,7	56,3	65,50	32,3	24,0
	1-4	56,2	46,00	34,9	21,3	79,6	1,13	60,0	19,6
	1-2	59,2	19,88	40,7	18,5	46,0	87,75	30,3	15,7
	3-4	77,5	1,00	60,0	17,5	80,6	1,38	59,1	21,5

¡ Return Loss² (dB) Pair		Local	@MHz	Remote	@MHz
	1 (4,5)	22,2	1,00	19,3	98,50
	2 (1,2)	21,1	95,25	21,5	44,50
	3 (3,6)	19,5	91,00	17,3	96,25
	4 (7,8)	21,0	90,25	18,8	75,00

¡ ELFEXT² (dB) Combo		Value	@MHz
	1-3	42,8	99,25
	3-2	46,3	58,25
	2-4	52,1	89,50
	1-4	42,5	68,00
	1-2	43,1	97,75
	3-4	45,8	99,50

¡ ACR² (dB) Combo		Local	@MHz	Remote	@MHz
	1-3	34,6	99,25	31,8	100,00
	3-2	38,3	97,25	33,7	100,00
	2-4	49,8	97,50	49,2	65,50
	1-4	46,6	82,25	49,1	81,25
	1-2	40,5	92,75	37,3	87,50
	3-4	46,7	97,25	46,5	84,00

Networks tested

10 Base-T **PASS** *100 Base-Tx* **PASS**

² Not required for selected limit