TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

VERKON KEHITYSPROJEKTI

Jussi Seppälä

Tietojenkäsittelyn koulutusohjelma
lokakuu 2006
Työn ohjaaja: Paula Hietala

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Jussi Seppälä

Koulutusohjelma(t) Tietojenkäsittely

Opinnäytetyön nimi Verkon kehitysprojekti

Työn valmistumis-kuukausi ja -vuosi Lokakuu 2006

Työn ohjaaja Paula Hietala

Sivumäärä: 42

TIIVISTELMÄ

Tämä opinnäytetyö on tehty toimeksiannosta Tampereen ammattikorkeakoululle. Aiheen työlle antoi tietoverkkopalveluiden vastaava opettaja diplomi-insinööri Harri Hakonen. Alkuperäisenä tarkoituksena oli suunnitella ja päivittää tietoverkkopalveluiden opiskelijoiden opetus- ja harjoitteluverkko eli niin sanottu WPK-verkko erillisiin aliverkkoihin, sekä ajanmukaistaa verkon laitteita. Toimeksianto muuttui työn aikana laboratoriototeutukseksi, jossa WPK-verkko suunniteltiin ja rakennettiin segmentoiduksi kokonaisuudeksi, ja käyttöön otettiin sovelletusti nykyisen verkon palvelut.

Opinnäytetyön teoriaosuudessa esitellään nykyinen WPK-verkko, sen laitteet ja niiden tehtävät. Ethernet-lähiverkkojen osalta käsitellään kehityshistoria, toiminta ja laitteet. Koska WPK-verkko suunniteltiin tässä työssä reititetyksi verkoksi, käsitellään teoriaosuudessa myös TCP/IP-protokollaperhettä ja sen toimintaa. WPK-verkko on aina ollut pääasiallisesti Windows–verkko, ja myös tämä työ koostui osaltaan palvelimien asennuksesta ja konfiguroinnista. Siksi myös Windows Server 2003 ja Active Directory esitellään lyhyesti. Työhön kuuluu Cisco Catalyst 3550 –kytkin, jonka käyttöönotto ja peruskonfigurointi myös esitellään.

Opinnäytetyön käytännön osuudessa rakennettiin laboratorioympäristössä aliverkkoihin jaettu uudenmallinen WPK-verkko. Verkon ohjauspalvelimet asennettiin Microsoft Virtual PC 2004 –ohjelman avulla yhdelle PC-tietokoneelle. Palvelimet asennettiin ja konfiguroitiin sovelletusti tarjoamaan samat palvelut kuin nykyisin, mutta räätälöitynä uudenmalliselle WPK-verkolle.

Mikäli WPK-verkko tulevaisuudessa päivitetään tai rakennetaan kokonaan uudelleen, voidaan tätä opinnäytetyötä käyttää käytännössä testattuna pohjana projektille. Opinnäytetyö tarjoaa verkon IP-suunnitelman, kuvauksen työn vaiheista ja ohjeistuksen eri palveluiden perusasennukselle.

Avainsanat Lähiverkot Verkkopalvelut Windows

TAMPERE
POLYTECHNIC

Author(s)	Jussi Seppälä
Degree Programme(s)	Business Information Systems
Title	A Network Development Project
Month and year	October 2006
Supervisor	Paula Hietala

Pages: 42

ABSTRACT

This Final thesis was written as an assignment to Tampere Polytechnic. The subject was assigned by M.Sc. Harri Hakonen, senior lecturer of network services. The original goal for this final thesis was to redesign and update the WPK-network, the training and studying network for the students of network services. The goal was to subnet the network, to update some of the appliances and to reconfigure servers as needed. The assignment however turned into a laboratory implementation. The network was redesigned and built in a laboratory environment as a subnetted network and current services were installed.

In the theory of this final thesis the current WPK-network, its appliances, their roles and all the services are introduced. The history of Ethernet, its functioning and the appliances are introduced. Since the network was redesigned as a routed network, TCP/IP protocol suite is also covered. The WPK-network has always been a Windows network. Therefore Windows Server 2003 and Active Directory are also explained in brief. In the hands-on work a Cisco Catalyst 3550 switch is installed. For the switch there is a basic configuration presented.

In the hands-on work of this final thesis a redesigned routed WPK-network was built. Both domain controllers of the network were installed on a single PC using Microsoft Virtual PC 2004. The servers were then configured to offer the same services as the current WPK-network.

In case the WPK-network is to be updated or completely rebuild in the future, this final thesis can be used as a practically tested foundation for the project. This final thesis offers an IP-plan for the network, a description of the steps of the project and a light tutorial for the basic service installations.

Keywords Local area networks Network services Windows

Sisällysluettelo

LYHENTEET JA KÄSITTEET 5

1 JOHDANTO 7

2 ETHERNET-LÄHIVERKOT 7

2.1 HISTORIAA 7
2.2 LÄHIVERKON VERKKOLAITTEET JA KAAPELOINTI 9
2.2.1 Verkkokortti 9
2.2.2 Keskitin 9
2.2.3 Kytkin 10
2.2.4 Kaapelointi 11

3 TCP/IP 14

3.1 YLEISTÄ JA TAUSTAA 14
3.2 TCP/IP-MALLIN KERROKSET 14
3.3 KULJETUSPROTOKOLLAT TCP JA UDP 15
3.4 REITITIN 16

4 MICROSOFT WINDOWS SERVER 2003 JA ACTIVE DIRECTORY 18

4.1 YLEISTÄ 18
4.2 ACTIVE DIRECTORY 18
4.3 VAATIMUKSET 18

5 NYKYINEN VERKKO 20

5.1 LAITTEET JA NIIDEN TEHTÄVÄT 20
5.2 DHCP 22
5.3 DNS 22
5.4 NAT 22

6 VERKKOSUUNNITELMA JA TOTEUTUS LABORATORIOSSA 24

6.1 SUUNNITTELUN VAIHEET 24
6.2 LABORATORIOYMPÄRISTÖ 25
6.3 CISCO CATALYST 3550 27
6.4 IP-AVARUUS 28
6.5 DHCP 28
6.6 DNS 30
6.7 SOVELLUSPALVELIMET (IIS) 30
6.8 TULOSTINPALVELIN 30
6.9 F-SECURE POLICY MANAGER 32

7 POHDINTAA 33

7.1 YLEISTÄ 33
7.2 TOTEUTUKSESTA 33
7.3 MAHDOLLISIA LISÄYKSIÄ 34
7.4 OMA ARVIO 35

LÄHTEET 36

LIITTEET 37

LIITE1: ETHERNET-STANDARDIT 37
LIITE 2: CATALYSTIN KONFIGURAATIO 38
LIITE 3: VERKON IP-SUUNNITELMA 41

Lyhenteet ja käsitteet

ARP, RARP	Address Resolution Protocol, Reverse Address Resulution Protocol
Cisco IOS	Cisco Internetwork Operating System – Ciscon reititin- ja kytkinkäyttöjärjestelmä
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
Hub	Keskitin, moniporttitoistin. OSI-mallin fyysiselle (1.) kerrokselle kuuluva verkkolaite.
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
LAN	Local Area Network – Lähiverkko
MAC	Media Access Control. MAC-osoite yksilöi verkkolaitteen Ethernet-verkossa.
NAT	Network Address Translation – Osoitemuunnos
NIC	Network Interface Card – Verkkokortti
OSI-viitemalli	Open Systems Interconnection Reference Model. 7-kerroksinen viitemalli tiedonsiirtoprotokollista.
POP	Post Office Protocol
PPP	Point-to-point Protocol
Router	Reititin. OSI-mallin verkkokerrokselle (3.) kuuluva verkkolaite.
SMTP	Simple Mail Transfer Protocol
Switch	Kytkin. OSI-mallin siirtokerrokselle (2.) kuuluva verkkolaite.
Telnet	Protokolla pääteyhteyksiin
TCP	Tranmission Control Protocol
TCP/IP-viitemalli	TCP- ja IP-protokollista nimensä saanut 4-kerroksinen viitemalli tietoliikenneverkkojen kuvaamiseen.
Token Ring	Lähiverkkoteknologia
UDP	User Datagram Protocol
UTP, STP	Unshielded Twisted Pair, Shielded Twisted Pair. Suojaamaton ja suojattu kupariparikaapeli.
Verkkotopologia	Verkon fyysinen perusrakenne. Vaihtoehtoja ovat väylä, tähti ja rengas.
VPN	Virtual Private Network – Tekniikka, jolla luodaan suojattu yhteys julkisen verkon ylitse.

1 Johdanto

Suoritin opintoihini kuuluvan pakollisen harjoittelujakson TAMK:ssa, tietoverkkopalveluiden suuntautumisvaihtoehdon WPK-verkon ylläpitäjänä. Harjoittelu ajoittui kevääseen ja syksyyn 2005. Harjoitteluni aikana käytännön ohjaajani DI Harri Hakonen antoi minulle mahdollisen aiheen opinnäytetyötä varten.

WPK-verkko on tietoverkkopalveluiden opiskelijoiden harjoitteluverkko. Verkossa ja siihen kuuluvissa luokissa opiskellaan useita tietoverkkopalveluiden suuntaavia opintojaksoja ja tehdään opintojaksoihin kuuluvia harjoituksia. Verkko on kasvanut nykyiseen kokoonsa vähitellen, opetuksen tarpeiden kasvaessa, eikä sillä siksi ole monia asianmukaisia ominaisuuksia ja piirteitä. Oppikirjamaisessa verkkosuunnittelussa painotetaan aina käsitteitä vikasietoisuus, skaalautuvuus ja ennakoitavuus. Nämä ominaisuudet saavutetaan jo suunnitteluvaiheessa tiettyjä periaatteita noudattamalla. WPK-verkkoa ei kuitenkaan ole koskaan suunniteltu tällaisen kaavan mukaan, sillä verkon nykymittaista käyttöä ei osattu ennakoida suunnitteluvaiheessa. Ajan mittaan verkkoon on tarpeen mukaan lisätty luokkia, työasemia, tulostimia ja palvelimia. Koska lähes kaikki verkon laitteet ovat samassa aliverkossa, on verkko altis häiriöille ja vikatilanteille. Opiskelijoiden lähes rajoittamaton verkonkäyttö on myös riski.

Opinnäytetyöni aihe alun perin oli suunnitella ja toteuttaa WPK-verkon uudelleenjärjestely. WPK-verkko tuli segmentoida erillisiin aliverkkoihin ja verkon reitittimenä pitkään palvellut PC-tietokone tuli korvata uudella Cisco Catalyst 3550 kytkimellä. Uuden reitittävän kytkimen konfiguraation suunnittelu ja verkon palvelinten vaatimat muutostyöt oli tarkoitus sisällyttää opinnäytetyöhön. Opinnäytetyön ei kuitenkaan ollut määrä liittyä esimerkiksi verkon kaapelointiin, sillä se on tarkoituksenmukainen ja sitä hallinnoi TAMK:n tietokonekeskus.

Työn käynnistyttyä ongelmia alkoi kuitenkin kasaantua. Pian havaittiin, ettei työhön määrätyillä laitteilla olekaan mahdollista toteuttaa suunnitelmaa. Harri Hakosen kanssa käydyn neuvottelun tuloksena sovittiin, että teen työn soveltuvin osin laboratorioympäristössä. Toimeksiantaja päättää aikanaan ryhdytäänkö opinnäytetyöni mukaisiin järjestelyihin ja missä mittakaavassa.

2 Ethernet-lähiverkot

2.1 Historiaa

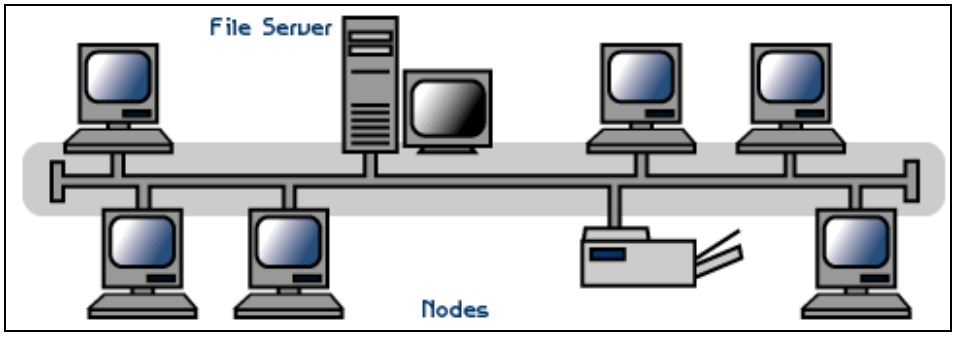
Ethernet on nykyisin yleisin ja laajimmalle levinnyt lähiverkkotekniikka. Ethernetin suosio ei ole kasvanut yllättäen tai nopeasti. Päinvastoin, Ethernetillä on pitkä ja värikäs historia. Suosio perustuu yksinkertaiseen toteutukseen, standardoituihin ratkaisuihin ja edullisuuteen.

Ethernetin varhaishistoria ulottuu 1960-luvun lopulle Havaijin yliopistoon, jossa herrat Abramson, Kuo ja Binder kehittivät Aloha-nimistä radioverkkoa maa-asemien ja laivojen yhteydenpitoon. (Jaakohuhta 2005: 9)

Ethernet sellaisena, kuin se nykyisin ymmärretään, alkoi saada muotoansa 1972. Robert Metcalfe sai Xerox:lla tehtäväkseen liittää Xerox:n ALTO-tietokone Internetin edeltäjään, ARPANET-verkkoon. Metcalfe tutustui Abramsonin ja hänen kumppaneidensa työhön, ja huomasi näiden olleen jo aiemmin samoilla linjoilla. Työtoverinsa David R. Boggs:n kanssa Metcalfe suunnitteli verkon, jolla yhdistettiin ALTO-tietokoneita lasertulostimeen. Verkon alkuperäiseksi nopeudeksi valittiin 2,94 Mb/s. Verkko oli maailman ensimmäinen mikroilla toteutettu lähiverkko. Ensimmäisen kerran verkko toimi 22.5.1973. Samana päivänä Metcalfe antoi verkolle nimen Ethernet. Nimi tuli vanhasta uskomuksesta, jonka mukaan eetterillä oli kyky välittää sähkömagneettista säteilyä avaruuteen. (Jaakohuhta 2005: 11-12)

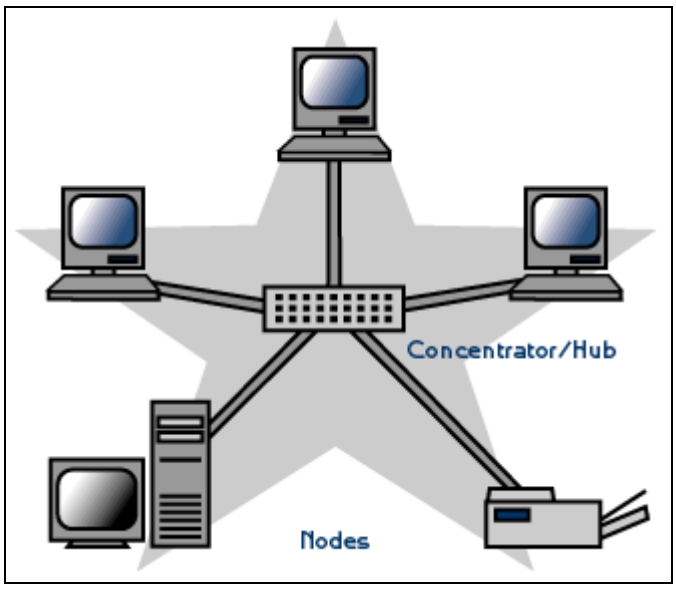
Aluksi Ethernet oli vain yksi monista lähiverkkotekniikoista. Se ei ollut muita nopeampi tai parempi. Ethernetin erotti muista se, että kehittäjä halusi siitä avoimen teollisuusstandardin. Standardi ”IEEE 10Base5” saatiin 1983. Lyhenteessä 10 tulee nopeudesta 10 Mbps, Base sanasta baseband (kantataajuinen siirto), ja 5 verkkosegmentin pituudesta (500 m). Samaa lyhennetapaa käytetään edelleen, nyttemmin tosin jo esim. 1000-Base-T (jossa 1000 = 1 Gb/s ja T = twisted pair, eli kierretty kuparikaapeli). Ethernet sai kansainvälisen ISO-standardinsa 1989. (Jaakohuhta 2005: 13-14)

Ethernet-tekniikkaa on matkan varrella ajanmukaistettu monella tapaa ja moneen kertaan. Muun muassa siirtomediana aluksi käytetty paksu koaksiaalikaapeli muuttui ensin ohueksi koaksiaalikaapeliksi, ”Thick Ethernetiksi”. Koaksiaaliverkko käytti väylämäistä topologiaa (Kuva 1). Kaikki laitteet oli kytketty saman kaapelin varrelle, ja ne saivat lähettää dataa vain yksi kerrallaan. Kaapelointi, verkon päivittäminen ja vianetsintä olivat ymmärrettävästi hankalia tehtäviä.



Kuva 1: Väylätopologia. (An Educator´s Guide.../Topology 2006)

Koaksiaalikaapelointia seurasi tänä päivänä laajimmin käytössä oleva kierretty kupariparikaapeli. Viimeisimpänä Ethernet-standardin on saanut valokaapeli. Siirryttäessä kupariparikaapeliin verkkotopologiaa muutettiin. Käyttöön otettiin tähtitopologia (Kuva 2). Tähtitopologiassa työasemien ”keskellä” on keskitin (hub), johon muut laitteet kytketään. Tämä mahdollistaa väylätopologiaa helpomman kaapeloinnin, vianetsinnän ja laajennettavuuden.



Kuva 2: Tähtitopologia. (An Educator´s Guide.../Topology 2006)

1980-luvun lopulle tultaessa lähiverkoissa oli jo niin paljon laitteita ja liikennettä, ettei kapasiteetti enää tahtonut riittää. Ethernet perustui jaettuun kaistaan. Yksi asema lähetti ja muut kuuntelivat. Kun verkossa oli suuria määriä laitteita, odotusajat pitenivät ja törmäysten määrä kasvoi. Keskittimet eivät auttaneet asiaa, ne lähettivät kaiken vastaanottamansa liikenteen kaikista porteistansa eteenpäin, ja näin itseasiassa vain lisäsivät turhaa liikennettä. (Jaakohuhta 2005: 23-24)

Vuonna 1990 syntyi käsite ”Switched (kytketty) Ethernet”. Kalpananiminen yritys kehitti uuden verkkolaitteen, kytkimen. Kytkin erosi keskittimistä luomalla useita samanaikaisia, toisistaan erillisiä siirtoyhteyksiä. Laite ei keskittimen tavoin enää lähettänytkään kaikkea liikennettä joka suuntaan, vaan ainoastaan oikeaan porttiin itse luomansa ja ylläpitämänsä kytkentätaulun mukaisesti. Vuonna 1993 samainen yritys esitte-

li kaksisuuntaisen (full duplex) Ethernetin. Aiemmin laitteet olivat kyenneet vain joko lähettämään tai vastaanottamaan. Nyt molemmat onnistuivat samanaikaisesti. Full Duplex:n myötä verkon kapasiteetti teoriassa tuplaantui. (Jaakohuhta 2005: 24-25)

Vuonna 1991 heräsi ajatus Ethernetin nopeuden kymmenkertaistamisesta. Perustettiin Fast Ethernet Alliance, jonka tuli luoda tekniikalle standardi. Vuonna 1993 Fast Ethernet Alliance esitteli 100Base-X:n määrittelyn, joka nyttemmin tunnetaan 100Base-TX:nä. Vihdoin maaliskuussa 1995 IEEE antoi 100Mbps Ethernetille standardin nimeltään IEEE 802.3u, eli 100Base-TX (kupari) ja 100Base-FX (valokuitu). (Jaakohuhta 2005: 25)

Nopeuden kasvu ei suinkaan loppunut tähän. 1999 esiteltiin 1000Base-T, 1 Gb/s kuparikaapelissa. Vuonna 2003 seurasi seuraava kymmenkerroin, 10 Gb/s valokaapelissa. Vuoden 2006 aikana odotetaan seuraavaa standardia, 10 Gb/s kuparikaapelissa.

2.2 Lähiverkon verkkolaitteet ja kaapelointi

2.2.1 Verkkokortti

Verkkokortti (NIC, Network Interface Card) on kaikille verkkolaitteille välttämätön osa, jolla laite kytketään verkkoon. Jokaisessa verkkolaitteessa on verkkokortti tai sitä vastaava piiri.

Tietokoneille on olemassa mm. PCI-, ISA-, USB-, PCMCIA- ja CF-liitäntäisiä verkkokortteja, mutta myös emolevyyn integroidut kortit ovat nykyään yleisiä. Jokaisella verkkokortilla on oma, yksilöllinen 48-bittinen MAC-osoitteensa, jonka verkkokortti saa valmistusvaiheessa. Eri lähiverkkotekniikoille kuten Ethernet:lle ja Token Ring:lle on omat verkkokorttinsa.

Verkkokortin tärkein osa on tranceiver-piiri (lähetin-vastaanotin), joka hoitaa verkkoliikenteen välittämisen. Verkkokortilla on myös oma prosessorinsa ja muistinsa. Verkkokortti toimii OSI-viitemallin verkkoyhteyskerroksella (2.). (OSI-viitemalli on standardi, joka havainnollistaa tiedonsiirtoprotokollien yhdistelmän seitsemänkerroksisella mallilla).

2.2.2 Keskitin

Keskitin eli hub on Ethernet-lähiverkoissa toimiva verkkolaite, jonka käyttö käy yhä harvinaisemmaksi. Keskitin on yksinkertainen laite, joka toimii OSI-viitemallin fyysisellä kerroksella (1.).

Keskittimen myötä Ethernetin topologia muuttui väylämäisestä tähdeksi. Keskittimellä varustettu verkko tai verkkosegmentti rakentuu keskitti-

men ympärille. Jokainen verkkolaite segmentissä kytketään keskittimen yhteen porttiin, ja laite lähettää jokaisen vastaanottamansa paketin muuttumattomana ulos jokaisesta portistaan.

Markkinoille tullessaan keskitin helpotti Ethernet-lähiverkkojen aiemmin hankalaa rakentamista ja vianetsintää. Väylätopologiaa käyttävissä verkoissa kaapeloinnin suunnittelu oli ollut ensiarvoisen tärkeätä. Kaapeloinnin muutostyöt saattoivat olla varsin kalliita, koska yhdenkin työaseman fyysinen siirtäminen merkitsi koko verkkosegmentin uudelleenkaapelointia. Tähtitopologiaan siirtyminen merkitsi sitä, että yksittäinen työasema saatettiin irrottaa verkosta irrottamalla se keskittimen portista. Tämä yksinkertainen toimenpide ei vaikuttanut enää millään tavalla verkkosegmentin muiden laitteiden toimintaan.

Keskitintä käyttävä lähiverkkoratkaisu hyödyntää jaettua kaistaa, eikä siksi ole tehokas ratkaisu. Useiden asemien lähettäessä samanaikaisesti syntyy ruuhkaa. Keskitin ei vähennä ruuhkan syntymistä, se päinvastoin pahentaa niitä lähettämällä kaiken liikenteen jokaisesta portistaan.

2.2.3 Kytkin

Kytkintä voidaan raa'asti yksinkertaistaen pitää älykkäämpänä keskittimenä, mutta nykyään se on huomattavasti kehittyneempi verkkolaite. Sen sijaan että kytkin keskittimen lailla lähettäisi kaiken vastaanottamansa valikoimatta joka suuntaan, kytkin tekee päätöksen.

Nykyaikaiset kytkimet ovat kaksisuuntaista liikennettä (dull duplex) tukevia, ja näin ollen tarjoavat jokaiselle liitännälleen maksimaalisen kapasiteetin. Kytkin rakentaa muistiinsa osoitetaulun, johon se tallentaa saapuvista paketeista lähettäjien MAC-osoitteet ja portin, josta ne löytyvät. Keräämiensä tietojen perusteella kytkin osaa lähettää paketit vain niiden oikeille vastaanottajille. Kun kytkin ei tunne saapuvan kehyksen kohdetta, se lähettää kehyksen kaikkiin muihin portteihin, paitsi siihen, josta kehys saapui. Tätä kutsutaan nimellä ”flooding”.

Alun perin kytkimet olivat OSI-mallin 2. kerroksen laitteita, mutta uudemmilla kytkimillä on paljon 3. kerroksen ominaisuuksia (mm. reititys). Vaikka 10 Mb/s verkkoja ei enää rakenneta, on niitä yhä käytössä 100 Mb/s ja 1 Gb/s -verkkojen ohella. Tällaisessa tapauksessa kytkin voi toimia eri nopeuksien välillä puskurina.

Kytkentätavoiltaan kytkimet voidaan jakaa kahteen ryhmään. Kytke ja välitä –kytkimiin (Cut-through) ja varastoi ja välitä –kytkimiin (Store-and forward). Ensiksi mainittu toimii siten, että kehyksen lähettäminen aloitetaan heti kun kohdesoite on saatu luettua kehyksestä. Tämä pitää viiveen minimaalisena, mutta välittää myös vialliset kehykset. Kytke ja välitä –kytkimiä käytetään vain työryhmä- ja työasemakytkimissä. Varastoi ja välitä –kytkimet sen sijaan ottavat koko kehyksen vastaan, ja varmistavat sen eheyden kehyksen tarkastussummasta. Vasta tämän jäl-

keen kytkin lähettää kehyksen kohteeseensa. Varastoi ja välitä –kytkentää käyttävät ainoastaan raskaammat runkokytkimet. (Jaakohuhta 2005: 142)

Erilaisia kytkimiä on kattava valikoima aina 5-porttisesta 10 Mb/s työasemakytkimestä modulaarisiin, räätälöitäviin 10 Gb/s runkokytkimiin.

2.2.4 Kaapelointi

Ethernet-lähiverkkoihin on lukuisia kaapelointiratkaisuja. Näitä, kuten monia muita tietoliikennestandardeja, määrittää ja standardisoi IEEE 802.3-komitea. Kuten Ethernetin historiaa käsittelevässä kappaleessa mainitsen, IEEE on määrittänyt tietyn nimeämistavan verkkotekniikoille ja niiden kaapeloinneille.

Vanhimmat lähiverkot ja kaapelointitekniikat soveltavat erilaisia koaksiaalikaapeleita. Näitä ovat mm. RG-8-koaksiaalikaapeli (Paksu Ethernet), jota käytettiin alkuperäisen 10Base5:n kaapelina ja RG-58-koaksiaalikaapeli (Ohut Ethernet), jota käytettiin 10Base2:n kaapelointina. Vaikka koaksiaalikaapelointia löytynee vielä jostakin, ei sitä enää käytetä uusia kaapelointeja tehtäessä. Tästä syystä en käsittele koaksiaalikaapelointia enempää.

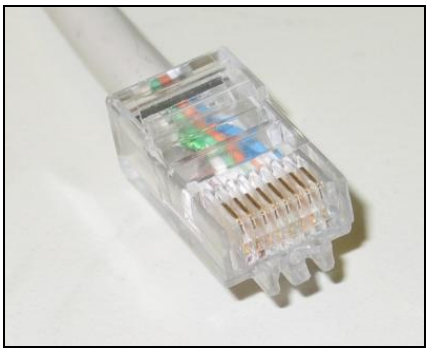
Kierretty kupariparikaapeli oli aikanaan osallisena Ethernet-tekniikan läpimurtoon keskitinten tullessa markkinoille. Tosin jo aiemmin kupariparikaapelia käytettiin muiden lähiverkkoratkaisujen kaapelointina. Samainen kupariparikaapeli on yhä tänäkin päivänä yleisin lähiverkkokaapeli.

Ensimmäinen IEEE:n määrittelemä Ethernet-standardi, joka käytti kupariparikaapelia, oli 10BaseT. Merkintä noudattaa aiemmin tutuksi tullutta kaavaa, jossa 10 tarkoittaa nopeutta 10 Mb/s ja Base kantataajuista siirtoa. Koaksiaalikaapeloinnista poiketen merkinnän viimeinen osa ei tarkoita segmentin pituutta, vaan käytettyä kaapelityyppiä ”(Unshielded) Twisted pair”. Suomeksi ”suojaamatonta kierrettyä kupariparikaapelia”. Alkuperäisen 10BaseT:n mukainen parikaapeli oli kaksiparista, mutta pian ryhdyttiin kaikkialla käyttämään neliparista kaapelia, jolla varauduttiin tulevaisuuden standardeihin. (Meyers 2003: 129)

Suojaamattoman kierretyn kupariparikaapelin, ”UTP:n”, ja suojatun kierretyn kupariparikaapelin ”STP:n” kanssa liittiminä käytetään RJ-45 –liittimiä (kuva 3). Ulkoisesti UTP ja STP ovat samannäköiset. STP-kaapelissa koko kaapeli ja parit suojataan metallivaipalla, joka tarjoaa suojaa häiriöitä vastaan. (An Educator´s Guide.../Cabling 2006)

Useimmissa kaapelointipaikoissa, mm. kotona ja työpisteissä, edullisempi UTP riittää mainiosti. STP tulee lähinnä kyseeseen, jos kaapelointia joudutaan tekemään voimakkaiden häiriölähteiden lähellä. Tällaisia

häiriöitä aiheuttavia lähteitä voivat olla suurijännitteiset sähkölinjat, muuntajat ja muut voimakkaita magneettikenttiä tuottavat laitteet.



Kuva 3: RJ-45-liitin UTP-kaapelissa (ICTP... 2006)

UTP- ja STP-kaapelit on eurooppalaisessa yleiskaapelointistandardissa EN 50173-1 jaettu luokkiin niiden ominaisuuksien mukaan. Luokat alkavat A:sta ja päättyvät tällä hetkellä F:ään. Luokista A on vaatimattomin ja F vaativin. Lähiverkoissa käytetään nykyään ainoastaan luokkien D, E ja F mukaisia kaapeleita. Luokkien sijasta kaapeleista käytetään usein kategoriamerkintää ”Cat”. Kategoriat vastaavat luokkia oheisen taulukon 1 mukaisesti. (Jaakohuhta 2005: 60-76)

Luokkamerkinnällä valmistaja takaa, että kaapeli täyttää vähintään luokan mukaiset laatuvaatimukset. Kaapelin luokan määräytymiseen vaikuttavat mm. seuraavat sähköiset ominaisuudet: kytkentä, pituus [m], heijastusvaimennus [dB], lähi- ja kaukopään ylikuulumisvaimennukset [dB], tasavirtasilmukkaresistanssi [S], kulkuaika [Fs] ja vaimennus [dB]. (Jaakohuhta 2005: 61)

Taulukko 1: Kaapelointiluokat (Jaakohuhta 2005: 60)

Luokka	Kategoria	Ethernet-sovellus
A	-	-
B	-	-
C	3	10Base-T
D	5	100Base-TX
	5e	1000Base-T
E	6	1000Base-T
F	7	10Gbase-T

EN 50173-1 –standardin määrittämiä asioita ovat mm.:
- kaapeloinnin suunnittelu ja mitoitusperiaatteet (maksimipituudet eri paikoissa)
- kaapelointijärjestelmän rakenne ja vähimmäisvaatimukset (mm. järjestelmän osat, kaapelit, ...)
- Yksittäisten siirtoteiden vaatimukset
- Kaapeleiden vaatimukset (mm. luokat)
- Liittämistarvikkeiden vaatimukset (mm. liittimet)
- Testaus

(Jaakohuhta 2005: 50)

Standardi pätee sekä valokuitu-, että kupariparikaapelointiin. Koaksiaalikaapelointiin standardi ei ota kantaa.

Koska opinnäytetyöhöni ei kuulu verkon suunnitteleminen alkutekijöistä, ja opinnäytetyöni ympäristönä käytetään jo olemassaolevaa kaapelointia, en käsittele kaapeloinnin teoriaa enempää.

3 TCP/IP

3.1 Yleistä ja taustaa

TCP/IP on protokollajoukko, joka on saanut nimensä kahdelta ehkä tärkeimmältä protokollalta, TCP:ltä ja IP:ltä.

Verkossa käytettävä kommunikointiprosessi määräytyy TCP/IP:n protokollien mukaan. TCP/IP määrää, mitä pakettien tulee sisältää ja miltä niiden tulee näyttää, jotta laite, joka vastaanottaa ne, osaa käsitellä niitä oikein. (Casad & Willsey 1999: 9)

Periaatteessa edellämainittu mahdollistaa sen, että mitkä tahansa TCP/IP:tä käyttävät laitteet voivat kommunikoida verkossa.

TCP/IP pohjautuu pitkälti Yhdysvaltain puolustusministeriön ARPAnet:iin, jota ryhdyttiin suunnittelemaan 1960-luvun lopulla. ARPAnet:n tarkoitus oli varmistaa, että ohjushyökkäyksen sattuessa tietojärjestelmät ja tietoliikenneyhteydet pysyisivät toimintakunnossa. Perusajatus oli hajautus. Hajautuksen tarkoitus oli varmistaa, että yhden osan tuhoutuminen ei voisi lamaannuttaa koko järjestelmää. Liikenteen tuli siis voida kulkea vaihtoehtoisia reittejä. ARPAnet:ssä toimi protokolla, jonka perustalle TCP/IP on kehitetty. (Casad & Willsey 1999: 10)

3.2 TCP/IP-mallin kerrokset

TCP/IP:lle on nelikerroksinen malli (kuva 4), joka on yleisin tapa kuvata TCP/IP-verkkoa. Malli on samankaltainen kuin ISO:n OSI-viitemalli, mutta suoraviivaisempi ja käytännöllisempi.

Kuva 4: TCP/IP:n kerrokset

Verkkokerros (Link layer) on TCP/IP:n rajapinta fyysiseen verkkoon. Verkkokerroksessa siirrettävä tieto muotoillaan verkkomedian mukaiseen muotoon. Osoitteena käytetään aliverkon fyysisiä osoitteita. Verk-

kokerroksen protokollia ovat mm. Ethernet, PPP ja Token Ring. (Casad & Willsey 1999: 35-36)

Internet-kerros suorittaa loogisen, laitteistoriippumattoman osoitteiden käsittelyn. Tämän ansiosta tieto voidaan siirtää aliverkosta toiseen, siitä huolimatta, että aliverkkojen laitteisto olisi erilainen. Internet-kerros reitittää Internetin (tai pienempien WAN-verkkojen) yli. Internet-kerros yhdistää loogiset ja fyysiset osoitteet toisiinsa. Internet-kerroksen protokollia ovat mm. IP, ICMP ja ARP. (Casad & Willsey 1999: 47-53)

Kuljetuskerros suorittaa tietovuon ohjaamisen, havaitsee virheet ja vahvistaa palvelut internetille. Kuljetuskerros on verkon palveluiden rajapinta. Kuljetuskerroksen protokollia ovat mm. TCP ja UDP. (Casad & Willsey 1999: 86-87)

Sovelluskerros sisältää sovelluksia moneen tarkoitukseen; mm. tiedostonsiirtoon, etähallintaan ja vianetsintään. Sovelluskerroksen protokollia ovat mm. HTTP, FTP, IRC, Telnet ja POP. (Casad & Willsey 1999: 112)

Tiedon liikkuessa tiedon lähettäjäpäässä kerrosten välillä jokainen kerros lisää siihen omat otsikkotietonsa, ”header”:n. Eri kerrosten lisäämät otsikkotiedot kertovat vastaanottajan päässä samalle kerrokselle tietoja toiminnan ohjaamista varten. Vastaanottajan päässä kukin kerros poistaa oman kerroksensa otsikkotiedot ennen tiedon siirtämistä ylemmälle kerrokselle.

Eri kerrosten tietopaketteja kutsutaan eri nimillä. Sovelluskerroksen tietopaketti on sanoma, kuljetuskerroksen tietopaketti segmentti, Internetkerroksen tietopaketti datagrammi ja verkkokerroksen tietopaketti kehys.

3.3 Kuljetusprotokollat TCP ja UDP

Tämän opinnäytetyön kannalta ei ole tarpeellista esitellä kaikkia TCP/IP-perheen protokollia, sillä itse työ rajoittuu enimmäkseen lähiverkon asioihin. Jokunen perusasia muutamasta protokollasta kannattaa kuitenkin mainita.

Kuljetuskerros on verkon ja sovellusten rajapinta. Kuljetuskerroksen avulla tiedoille voidaan osoittaa sovellus, jolle tiedot on tarkoitettu. TCP/IP-järjestelmässä tämä tapahtuu TCP- tai UDP-protokollien porttinumeroiden avulla. Portit ovat ennalta määrättyjä kanavia kuljetuskerrokselta sovellukseen ja toisinpäin. Esimerkiksi HTTP-liikenne käyttää tavallisesti TCP-porttia 80. (Casad & Willsey 1999: 88)

TCP/IP:n porttinumeroita hallinnoi ja ylläpitää Internet Assigned Numbers Authority (IANA). Taulukossa 2 mainitaan muutamia yleisimpiä portteja.

Taulukko 2: TCP/IP-portteja (IANA 2006)

Portti	Protokolla
23 / TCP	Telnet
80 / TCP	http
22 / TCP	SSH
161 / UDP	SNMP
25 / TCP	SMTP

Kuljetuskerroksen kuljetusprotokollat TCP ja UDP eroavat toisistaan suuresti. TCP on yhteydellinen protokolla, joka tarjoaa virheenhavaitsemismekanismin sekä vuonohjauksen. UDP sen sijaan on yhteydetön protokolla, joka sisältää ainoastaan erittäin karkean virheentarkastuksen.

TCP:n virheenhavaitsemismekanismi perustuu TCP-pakettien tarkistussummaan. Vastaanottaja tarkistaa jokaisen paketin eheyden tarkistussumman avulla, ja pyytää lähettäjää lähettämään korruptoituneet paketit uudelleen. Vuonohjaus pitää huolen siitä, ettei vastaanottajan vastaanottokyky ylity.

Yhteydellisyys tarkoittaa sitä, että lähettäjä ja vastaanottaja muodostavat yhteyden ennen datasegmenttien lähettämistä. Yhteyden muodostaminen tapahtuu kolmivaiheisessa kättelyssä. Datasegmenttien vastaanotto kuitataan, ja mahdollisesti hukkuneet tai korruptoituneet datasegmentit lähetetään uudelleen. Kun tiedonsiirto on suoritettu, lähettävä ja vastaanottava kone sulkevat yhteyden siististi.

Yhteydettömällä protokollalla lähettävä kone ei varoita vastaanottajaa aikeistaan lähettää, eikä vastaanottaja kuittaa sitä, onko vai eikö se ole saanut datasegmentin korruptoitumattomana.

Yhteydelliset protokollat ovat luotettavampia, mutta myös hitaampia ja enemmän kapasiteettia vieviä kuin yhteydettömät protokollat.

3.4 Reititin

Aiemmin esitellyt laitteet olivat lähiverkkojen laitteita. Reitittimet ovat laitteita, jotka yhdistävät lähiverkkoja, kaupunkiverkkoja ja laajaverkkoja. Reitittimet eivät välitä liikennettä MAC-osoitteiden perusteella kuten kytkimet, vaan IP-osoitteiden perusteella.

Reitittimet rakentavat ja ylläpitävät jopa kymmenientuhansien rivien mittaisia reititystauluja ja vaihtavat reititystietojaan muiden reitittimien kanssa reititysprotokollien avulla. Näin reitittimet osaavat ohjata liikennettä kymmenien, jopa satojen, kaltaistensa kautta vaikkapa maailman toiselle puolelle.

Reititysprotokollia on kahdenlaisia, linkkitilaprotokollia (link-state) ja etäisyysvektoriprotokollia (distance vector). Reititysprotokollien avulla reitittimet vaihtavat reititystietojaan ja päivittävät reititystaulujaan. Nämä eroavat toisistaan suuresti toiminnaltaan, mutta kaikkien yhteinen

tarkoitus on selvittää nopein ja luotettavin reitti kuhunkin kohteeseen. Reititysprotokollia ovat mm. BGP, RIP, OSPF, IGRP ja EIGRP.

4 Microsoft Windows Server 2003 ja Active Directory

4.1 Yleistä

Windows Server 2003 on toistaiseksi Microsoftin tuorein palvelinkäyttöjärjestelmä. Windows Server 2003:sta on tarjolla useita eri versioita eri tarpeisiin, Small Business Server –perusversiosta Datacenter Edition –lippulaivaan.

Windows Server 2003 korvasi aikanaan Server 2000:n, joten siirtyminen vanhemmasta uudempaan versioon on Microsoftin mukaan saumatonta.

4.2 Active Directory

Microsoft julkisti Active Directoryn (jäljempänä AD) aikanaan Server 2000:een sisällytettynä. AD kuuluu myös Server 2003:een olennaisena osana. AD voidaan suomentaa suoraan aktiivihakemistopalveluksi.

AD on monipuolinen palvelu, jolla hallitaan käyttäjiä, tietokoneita ja resursseja keskitetysti. AD on parhaimmillaan suuressa verkkokokonaisuudessa, jossa tulee keskitetysti hallita käyttäjätilejä, suuria määriä työasemia, verkkotulostimia ja levyjakoja. AD:n avulla hallitaan ohjelmistoasennukset, resurssien tarjoaminen, ryhmäkäytännöt ja lukuisat verkkopalvelut.

Mahdollisia hallittavia resursseja voivat olla tulostimet ja tiedostopalvelimet. Ryhmäkäytännöillä voidaan määrittää suppeammassa tai laajemmassa mittakaavassa mm. salasanapolitiikat, käyttäjien oikeudet työasemiin, työpöydän käyttäytyminen ja ulkoasu sekä keskitetyt ohjelmistoasennukset. Voidaan katsoa, että Active Directory on Windows Server 2000/2003:n ydin.

AD:n ohjauspalvelimet voidaan hajauttaa tehokkuuden ja vikasietoisuuden saavuttamiseksi, kuten tämänkin opinnäytetyön laboratorioosuudessa tehdään.

4.3 Vaatimukset

Mikäli WWW-palvelimeksi tarkoitettua Server 2003 Web Editionia ei oteta lukuun, perusversiona voidaan pitää Server 2003 Standard Editionia. Kuten taulukosta 2 huomataan, voi perusversion halutessaan asentaa jopa melko vaatimattomaan kokoonpanoon. Vastaavasti toisesta ääripäästä löytyy versio, joka vaatii järjestelmältä vähintään 8 prosessoria.

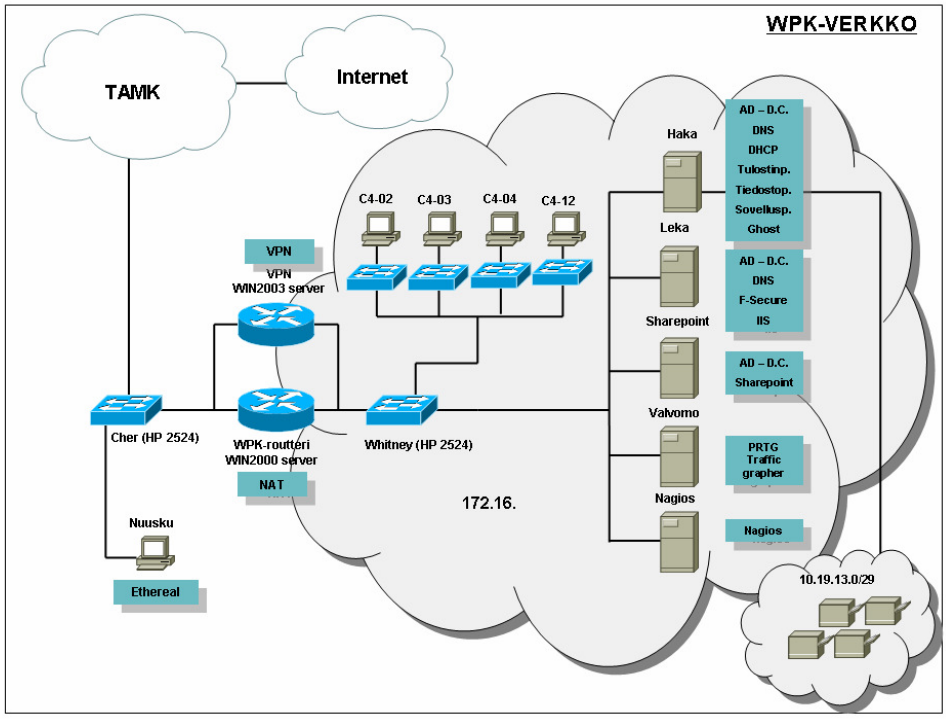
Taulukko 3: Windows Server 2003:n vaatimukset (Microsoft Suomi)

Vaatimus:	Web Edition:	Standard Server:	Enterprise Server:	Datacenter Server:
Suorittimen vähimmäisnopeus	133 MHz	133 MHz	• 133 MHz x85-pohjaisia tietokoneita varten • 733 MHz Itanium-pohjaisia tietokoneita varten	• 400 MHz x86-pohjaisia tietokoneita varten • 733 MHz Itanium-pohjaisia tietokoneita varten
Suositeltava suoritinnopeus	550 MHz	550 MHz	733 MHz	733 MHz
RAM-muistin vähimmäismäärä	128 Mt	128 Mt	128 Mt	512 Mt
Suositeltava RAM-muistin vähimmäismäärä	256 Mt	256 Mt	256 Mt	1 Gt
RAM-muistin enimmäismäärä	2 Gt	4 Gt	• 32 Gt x86-pohjaisissa tietokoneissa • 64 Gt Itanium-pohjaisissa tietokoneissa	• 64 Gt x86-pohjaisissa tietokoneissa • 128 Gt Itanium-pohjaisissa tietokoneissa
Usean suorittimien tuki	1 tai 2	1 tai 2	Enintään 8	• Edellytetään vähintään 8:aa • Enintään 32 x86-pohjaisissa tietokoneissa • Enintään 64 Itanium-pohjaisissa tietokoneissa
Asennuksen edellyttämä levytila	1,5 Gt	1,5 Gt	• 1,5 Gt x86-pohjaisissa tietokoneissa • 2,0 Gt Itanium-pohjaisissa tietokoneissa	• 1,5 Gt x86-pohjaisissa tietokoneissa • 2,0 Gt Itanium-pohjaisissa tietokoneissa

5 Nykyinen verkko

5.1 Laitteet ja niiden tehtävät

Nykyinen WPK-verkko on kuvan 4 mukainen. Palvelimet ja työasemat ovat samassa 172.16.0.0 –verkossa. Verkon reunalla ovat WPK-routteri ja VPN-palvelin. Tulostimia varten on oma 10.19.13.0 -verkkonsa.



Kuva 4. Nykyinen WPK-verkko

Palvelimien IP-osoitteet ovat staattiset, kuten luonnollisesti myös verkkolaitteilla. Verkon työasemat saavat IP-osoitteensa, nimipalvelintiedot ja oletusyhdyskäytävän DHCP-palvelimelta. WPK-verkon DHCP-palvelimena toimii Haka. Sekä Haka että Leka toimivat verkon DNS-nimipalvelimina.

Luokkatilojen kytkimet ovat käytössä ainoastaan lisäporttiensa takia, niillä ei siis ole reititysominaisuuksia.

Luokassa C4-12 olevat reitittimet ovat käytössä erilaisten luokkaympäristövaatimusten vuoksi. C4-12:ssa opetetaan mm. Microsoft- ja StoneGate-kursseja, joita varten asennetaan tietty verkkoympäristö. Koska kyseiset reitittimet eivät kuulu itse WPK-verkkoon, ei niitä ole sisällytetty kuvaan.

Tulostimet ovat omassa 10.19.13.0/29 –verkossaan**,** jotta niihin ei voida tulostaa muuten kuin verkon tulostinpalvelimen kautta. Tulostinpalvelimena toimii Haka. Lisäksi tilan C4-02 lasertulostin on asennettu Hakaan paikallisesti.

Hakan muita tehtäviä ovat Active Directory (ohjauspalvelin, Domain Controller yhdessä Lekan kanssa) ja tiedostopalvelut.

Leka toimii toimialueen toisena ohjauspalvelimena. Tämän lisäksi se on F-Secure Policy Manager -palvelin ja WWW-palvelin. WWW-palvelinohjelmistona on Windows Server 2003:n oma IIS.

Sharepoint-palvelimen tehtävä on nimensä mukaisesti toimia WPK-verkon MS Sharepoint -palvelimena. Microsoft Sharepoint on työryhmäohjelmisto, jolla organisaatiolle voidaan luoda www-sivustoja, joiden avulla voidaan mm. jakaa ja varastoida tiedostoja, pitää online-keskusteluita, ym. Sharepointia käytetään laajalti intranet- ja extranet-sovelluksena. (Microsoft…/SharePoint 2006)

WPK-verkossa Sharepoint toimii henkilökunnan ja harjoittelijan sähköisenä ilmoitustauluna, verkon dokumentaation varastona ja päivityspaikkana. Lisäksi se tarjoaa hypermedian opettajille oman fooruminsa.

Nagios on toiseen opinnäytehön liittyvä palvelin, jossa ajetaan nimensä mukaista Nagios-ohjelmistoa. Nagios on valvontaohjelmisto, joka valvoo mm. verkon aktiivilaitteita, palvelimia ja palveluita. (Nagios)

WPK-routteri on reititin, joka yhdistää WPK-verkon ulkomaailmaan. WPK-routteri on vanha 450/600MHz Pentium III -tietokone, jossa on Windows 2000 Server –käyttöjärjestelmä. Koneella on reitityksen ohella pienimuotoinen DNS-rooli. Lisäksi WPK-routteri tekee osoitteenmuunnoksen, eli NAT:n.

VPN on nimensä mukaisesti VPN-yhteyden verkkoon tarjoava laite. Myös VPN(-kone) on vanha 450/600MHz Pentium III –tietokone. Käyttöjärjestelmänä koneessa on Windows 2003 Server. VPN-yhteys on tarjolla vain valikoiduille henkilökunnan jäsenille, jotka sitä hyödyntäen voivat suorittaa mm. ylläpidollisia toimenpiteitä myös kotoaan.

Koko WPK-verkko on kaapeloitu Cat5- ja Cat6-kaapeleilla, ja kaikki verkkoliitännät toimivat 100 Mb/s nopudella.

5.2 DHCP

WPK-verkon DHCP-palvelimena toimii Haka. Kaikki WPK-verkon työasemat saavat IP-osoitteen, aliverkkomaskin, DNS-palvelimen IP-osoitteen sekä oletusyhdyskäytävän IP-osoitteen DHCP:n avulla. Vain palvelimille, tulostimille ja verkkolaitteille on määritelty staattiset IP-osoitteet.

Koska kaikki fyysiset tilat ja laitteet olivat samassa aliverkossa, ei DHCP-palveluun ole liittynyt ongelmia. Hakan DHCP-palvelun ominaisuuksiin on määritelty edellä osoitevaranto, josta palvelin aina DHCP-pyynnön saadessaan tarjoaa osoitteen. IP-osoitteen laina-aika on määritetty kahdeksaksi tunniksi. Osoitevarannosta on rajattu pois tiettyjä verkkolohkoja, jotka on jaettu tietoverkkopalveluiden opettajille. Näistä lohkoista he saattavat opettamillaan kursseilla antaa harjoituksia varten opiskelijoille staattisia IP-osoitteita ilman, että ne ovat päällekkäisiä DHCP:n jakamien osoitteiden kanssa.

5.3 DNS

WPK-verkon DNS-palvelua ylläpitävät toimialueen ohjauskoneet Haka ja Leka.

WPK-Routterin DNS-määrityksiin on määritetty osoitteet, joihin ulkoverkon puolelta on mahdollista päästä. Nämä ovat www.wpk.tpu.fi, nagios.wpk.tpu.fi, mail.wpk.tpu.fi ja sp.wpk.tpu.fi.

5.4 NAT

WPK-routterin yksi tärkeä tehtävä on tehdä osoitteenmuunnos eli NAT (Network Address Translation). NAT muuntaa verkkojen rajalla sisäverkon salaiset osoitteet julkisen verkon osoitteiksi.

Tätä tarkoitusta varten palveluntarjoajalta eli tässä tapauksessa TAMK:n Tietokonekeskukselta on saatu pieni osoitevaranto (address pool). NAT on määritetty siten, että sisäverkon niille koneille, joille tulee olla pääsy ulkoverkosta, on annettu em. osoitevarannosta julkinen osoite. Kun ulkoverkosta tulee esim. http-pyyntö ”195.148.56.132” (www.wpk.tpu.fi), WPK-routteri ohjaa liikenteen NAT:n mukaiseen sisäverkon osoitteeseen.

NAT tulee kyseeseen myös silloin, kun jokin sisäverkon kone ottaa yhteyttä ulkoverkkoon. Tällöin kyseinen sisäverkon kone näkyy ulkoverkon kohteeseen NAT:n antamalla ulkoverkon osoitteella. Tällaisena tapauksena mainittakoon esimerkiksi opiskelijan selaimella tekemä http-pyyntö http://www.tietokone.fi. Sisäverkon kone lähettää pyynnön omalla sisäverkon osoitteellaan ja NAT muuntaa osoitteen pyynnössä ulkoverkon osoitteeksi. Tietokone.fi:n www-palvelin vastaa pyyntöön, ja lähettää vastauksensa NAT:n mukaiseen ulkoverkon osoitteeseen. NAT

muuntaa jälleen osoitteen sisäverkon vastaavaksi, ja ohjaa liikenteen pyynnön tehneelle sisäverkon koneelle.

6 Verkkosuunnitelma ja toteutus laboratoriossa

6.1 Suunnittelun vaiheet

Opinnäytetyön alkuperäinen tarkoitus oli suunnitella ja toteuttaa käytännössä WPK-verkon jakaminen erillisiin aliverkkoihin. Tarkoitus oli myös poistaa vanha WPK-routteri verkon reunareitittimen roolista. Kummatkin edellä mainitut tehtävät oli tarkoitus saada toteutettua yhdellä ja samalla laitteella, Cisco Catalyst 3550 –kytkimellä.

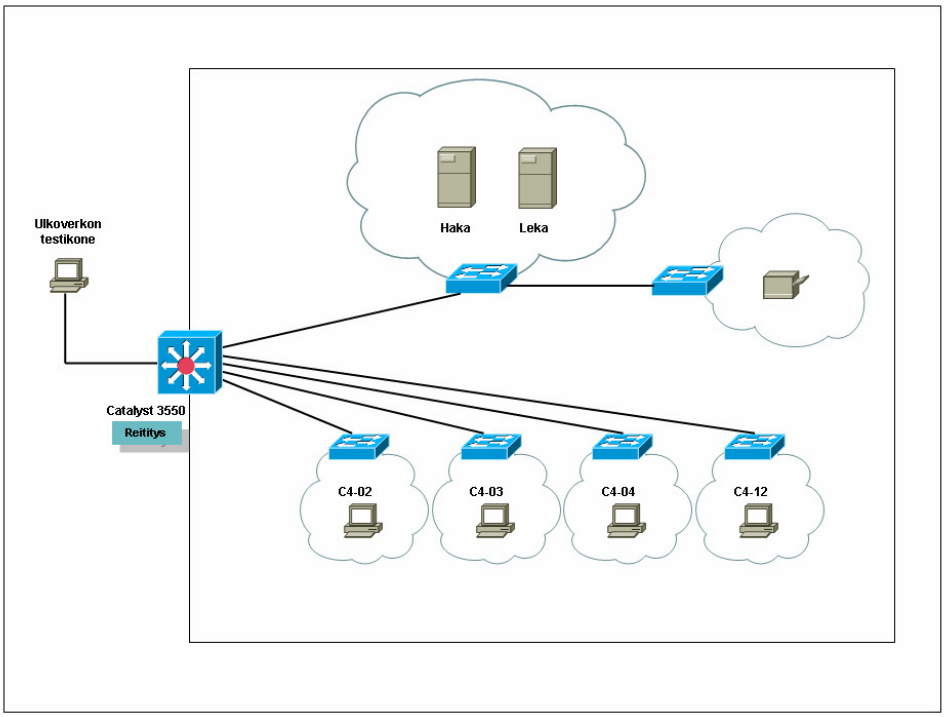
Suunitelmaa jouduttiin päivittämään ensimmäisen kerran kun havaittiin Cisco Catalyst 3550:n tähän tarkoitukseen rajalliset ominaisuudet. Vaikka Cisco Catalyst 3550 onkin reitittävä multilayer-kytkin, ei sille ole siitä huolimatta yhtään IOS-versiota, joka tukisi NAT-toimintoa. (IOS on Ciscon kytkin- ja reititinkäyttöjärjestelmä).

Tämä luonnollisesti teki mahdottomaksi Catalystin sijoittamisen WPK-verkon reunalle. Suunnitelma oli tältä osin pitkään kesken. Yksinkertaisin ratkaisu olisi ollut lisätä Catalystin ja TAMK:n verkon väliin reititin, joka hoitaisi NAT:n.

Verkkoa suunniteltiin jonkin aikaa siltä pohjalta, että reititin lisättäisiin. Kuitenkin toimeksiantajan toiveesta sellaisesta suunnitelmasta luovuttiin, sillä se olisi melko pitkälti tehnyt tyhjiksi uuden verkkomallin tuomat hyödyt. Mikäli suunnitelmaan olisi lisätty reititin, ei verkon laitteiden määrä olisi vähentynyt, eikä verkon hallinnasta olisi tullut lainkaan yksinkertaisempaa ja keskitetympää. Tämä oli kuitenkin yksi projektin alkuperäisiä lähtökohtia.

Toimeksiantaja esitti siksi, että opinnäytetyö tehdään soveltuvin osin laboratorioympäristössä ilman NAT-toiminnallisuutta, ja suunnitelmaa tai sen osia käytetään tarpeen tullen tulevaisuudessa. Tämän opinnäytetyön piiriin ei siis kuulu uuden suunnitelman käyttöönotto. WPK-verkon laboratoriosuunnitelma on kuvan 5 kaltainen.

Laboratorioympäristöstä jätettiin pois useita tämän hetkisen verkon laitteita, sillä niillä ei ollut työn kannalta merkitystä. Samoin pois jätettiin joitakin palvelinten rooleja, sillä niiden lisääminen ei olisi tuonut työlle lainkaan lisäarvoa, vaan ainoastaan lisävaivaa.



Kuva 5: Verkon laboratoriototeutus

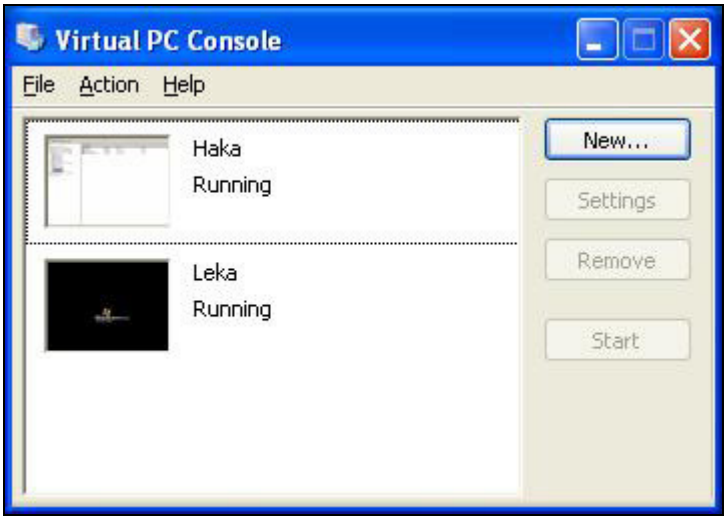
6.2 Laboratorioympäristö

Laboratorioympäristö johon uusi WPK-verkko rakennettiin, oli itse asiassa fyysisesti varsin pieni kokonaisuus. Kaikki tarvittavat laitteet mahtuivat yhdelle suurelle työpöydälle.

Hakaa ja Lekaa ei asennettu erityisille palvelinkoneille, vaan yhdelle ja samalle PC:lle, johon oli asennettu Windows XP Professional (SP2) ja Microsoft Virtual PC 2004 (kuva 6). Itse tietokone oli kokoonpanoltaan 1,8GHz Pentium 4, jossa muistia oli 1Gb. Koneessa oli kaksi verkkokorttia, siis kummallekin virtuaalipalvelimelle omansa. CD-ROM-asema oli molempien virtuaalipalvelimien yhteisessä käytössä.

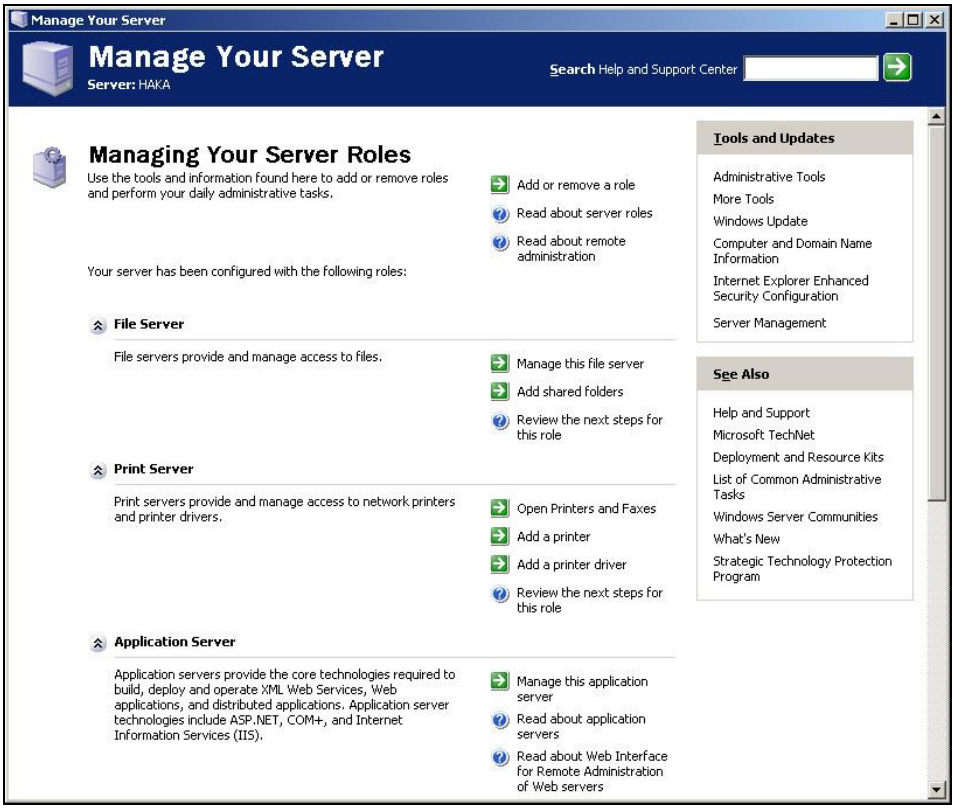
Kone suoriutui kahden virtuaalisen palvelimen ajamisesta varsin kohtuullisesti, sillä mitään muuta erityistä koneella ei samanaikaisesti ajettu. Silloin tällöin molempien palvelimien ollessa käynnissä yhtä aikaa oli huomattavissa pientä tahmeutta. Tämä ei kuitenkaan haitannut työtä.

Palvelinympäristön rakentamisen aloitettiin asentamalla Virtual PC 2004:lle kaksi Windows Server 2003:n peruskokoonpanoa.



Kuva 6: Virtual PC Console

Ensin käsittelyyn otettiin Haka. Manage Your Server –ikkunasta (kuva 7) valittiin ”add or remove a role” ja asennettiin palvelimen oletusominaisuudet. Nämä olivat Active Directory (Domain Controller), DHCP ja DNS. Näistä lisää jäljempänä.



Kuva 7: Manage Your Server -ikkuna

Lekan kanssa ensimmäinen toimenpide oli tuoda se toimialueeseen. Tämän jälkeen se nostettiin Hakan rinnalle toimialueen ohjauskoneeksi (Domain Controller). Tämä tapahtui lisäämällä Lekalle ”Active Directory – Domain Controller” –rooli. Myös Lekan rooleista lisää jäljempänä.

Verkon työasematestaamista varten käytössä oli tavallinen PC, jossa oli asennettuna Windows XP. Kun Active Directory ja DHCP-palvelin oli asennettu, työasema liitettiin toimialueeseen. Tämä onnistui ongelmitta, ja käynnistyksen yhteydessä kone sai DHCP:llä myös oikean aliverkon verkkoasetukset.

Active Directoryn Users and computers –työkalulla tehdyllä tietokonehaulla edellämainittu työasema Kehityslabra2 löydettiin, ja tuotiin asiaankuuluvaan organisaatioyksikköön.

6.3 Cisco Catalyst 3550

Verkon reitittävän Catalyst-kytkimen käyttöönotto oli melko yksinkertainen suorittaa. Laite oli käyttöönotettaessa tehdasuusi ja tuli suoraan laatikosta. Fyysinen käyttöönotto ei vaatinut muuta kuin virtajohdon kytkemisen. Tätä työtä varten kirjoitettu ajettava konfiguraatiotiedosto Catalystille on liitteessä 2.

Cisco Catalyst 3550 (kuva 8) kuuluu Ciscon kytkintuoteperheen Enterprise-luokkaan. Kytkin on konfiguroitava ja pinottava multilayer-kytkin, joka tarjoaa valmistajan mukaan korkean tason turvallisuutta. Kytkimen ominaisuuksiin kuuluu myös QoS (Quality of Service). Cisco Catalyst 3550 –kytkimessä on 24 kpl 10/100 Mb/s –portteja ja 2 kpl Gb/s –portteja. (Cisco…/ Catalyst 3550)

Kuva 8: Cisco Catalyst 3550 (CiscoKits.com)

Kuten kaikki nykyaikaiset Cisco-tuotteet, myös Catalyst 3550 tarjoaa terminaalipohjaisen lisäksi myös selainpohjaisen käyttöliittymän.

Toimeksiantajan kanssa sovittiin, että laitteesta otetaan nyt käyttöön ainoastaan 100Mb/s Fast Ethernet –portteja. Laitteessa olevat kaksi 1Gb/s moduulipaikkaa säästetään reservinä tulevaisuuden käyttöä varten, sillä vaikka TAMK:n rakennukset ovatkin kaapeloitu gigabitin yhteydet mahdollistavalla Cat 6 –kaapelilla, sisäverkko toimii toistaiseksi ainoastaan 100Mb/s nopeudella. Näin ollen kytkimen 1Gb/s –liitännöillä ei saavutettaisi lainkaan lisähyötyä.

6.4 IP-avaruus

Toimeksiantaja halusi, että nyt käytössä oleva 172.16.0.0 –sisäverkko säilytetään myös jatkossa.

Mikäli tämä opinnäytetyö olisi toteutettu alkuperäisen suunnitelman mukaan, olisi selvyyden vuoksi ollut hyvä vaihtaa sisäverkko esimerkiksi 192.168.0.0 –verkoksi. Tällaisessa tapauksessa mm. vianetsintä olisi ollut helpompaa. Säilytettäessä käytössä oleva osoiteavaruus samana, saatettaisiin joutua yhtenään miettimään ”onko tämä IP-osoite jo päivitetty, ja onko se siten uuden mallin mukainen?”. Vaihtamalla toiseen osoiteavaruuteen olisi toisaalta jouduttu tekemään enemmän konfiguraatiotyötä, mutta toisaalta konfiguraatio olisi päästy suorittamaan ”puhtaalta pöydältä” selvemmin.

Toimeksiantajalla oli kuitenkin hyvä syy säilyttää vanha osoitteisto samana. Sekä TAMK:lla, että Tampereen kaupungilla on käytössään 192.168.0.0 –aliverkkoja, joista monet ovat tähänkin saakka olleet ”kiellettyjä verkkoja”. Nämä verkot ovat privaattiverkkoja, joita on vain selvyyden vuoksi syytä välttää. Mikäli 192.168.0.0 –verkkoon olisi siirrytty, olisi sen suunnitteleminen ollut askartelua. Loppujen lopuksi suurin selkeys ja varmuus saavutettiin sittenkin pitämällä sama osoiteavaruus.

Laboratoriototeutuksen IP-suunnitelma on kokonaisuudessaan liitteessä 3.

6.5 DHCP

Toimeksiantaja halusi että myös projektin jälkeen verkon DHCP-palvelun hoitaa Haka-palvelin. Tällä saavutetaan se etu, että mahdollisimman monet verkon palvelut ja resurssit jaetaan keskitetysti. Ylläpitäjän kannalta on helppoa, kun mahdollisesti tarvittavat muutostyöt voidaan suorittaa itse palvelimella tai etäyhteydessä palvelimeen. Kun lisäksi muistetaan että monet verkon palvelut on kahdennettu Hakan ja Lekan kesken, riittää se, että muutokset tehdään yhteen paikkaan.

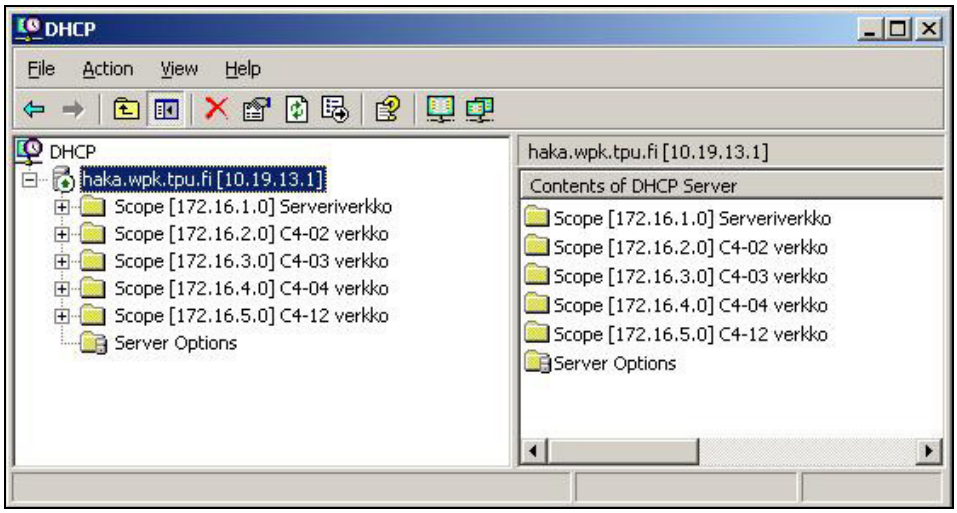
Kivimäen (2005: s. 1279) mukaan ei kuitenkaan olisi suositeltavaa määrittää DHCP-palvelua verkon ohjauspalvelimelle, koska ohjauspalvelimet tallentavat tietoja DNS:ään. Tällaisessa tapauksessa on teoriassa mahdollista, että kuka tahansa verkon käyttäjä pääsee muuttamaan ohjauspalvelimen DNS:ään tallentamia tietoa. DHCP-palvelimet ovat AD:ssa DNSUpdateProxy-ryhmän jäseniä, ja tämän ryhmän DNS:ään luomilla tietueilla ei ole lainkaan suojausasetuksia.

Suunnitelmaan kuuluva Cisco Catalyst 3550 –kytkin olisi myös ollut kykenevä hoitamaan verkon DHCP-palvelua. Mikäli kytkin olisi asetettu kyseiseen tehtävään, olisi DHCP-osoitevarannon (address pool) määrittäminen eri luokille ollut varsin yksikertaista. Koska kukin luokka on kytkimen tietyn portin takana, olisi kytkin ollut helppoa konfiguroida niin, että tietystä luokasta (portista) tulevaan DHCP-pyyntöön olisi vas-

tattu tietyn aliverkon IP-osoitteella. Näin jokaisen luokan työasemat olisivat saaneet oman, määritellyn aliverkkonsa IP-osoitteen.

Kytkimellä suoritettavat muutostyöt, esim. DHCP-osoitevarannon muutokset, vaativat aina ylläpitäjän kirjautumisen laitteelle. Kytkintä voidaan hallita joko selainpohjaisesti, konsolikaapelin avulla tietokoneelta tai verkon kautta telnet- tai SSH-yhteydessä. Viimeksi mainitut vaativat kuitenkin, että kyseisen yhteyden käyttö on mahdollistettu kytkimen konfiguraatiossa.

Laboratoriototeutuksessa DHCP-palvelu rakennettiin siten, että Haka hoitaa edelleen DHCP-palvelun. Palvelimen DHCP-osoitevaranto on jaettu niin, että kullekin tilalle (C4-02, C4-03, C4-04 ja C4-12) on oma osoitealueensa, sekä yksi ylimääräinen osoitealue ”serveriverkko”, josta kuitenkin on poistettu (excluded) staattiset osoitteet (kuva 9).



Kuva 9: Verkon DHCP-palvelu

Catalyst on konfiguroitu siten, että se ohjaa DHCP-liikenteen joka aliverkosta DHCP-palvelimelle eli Hakalle. Koska Broadcast-liikennettä (mm. DHCP-liikenne) ei normaalisti reititetä, piti tämä toteutettaa *ip helper-address* –komennolla. Komento tuli antaa jokaiselle verkkoliitännälle, joista DHCP-pyyntöjä voi tulla.

Catalystin eri verkkoihin (luokat) menevillä verkkoliitännöillä on kyseisen verkon kiinteä IP-osoite. Kun työasema tällaisesta verkosta lähettää DHCP-pyynnön, muokkaa Catalyst pyyntöä niin, että lähettäjän osoitteeksi tulee Catalystin kyseisen verkkoliitännän osoite.

DHCP-palvelin saa näin ollen osoitepyynnön ohella tiedon, mistä aliverkosta pyyntö tulee, ja osaa sen perusteella antaa osoitetiedot oikeasta osoitealueesta. (Kivimäki 2005: 1314)

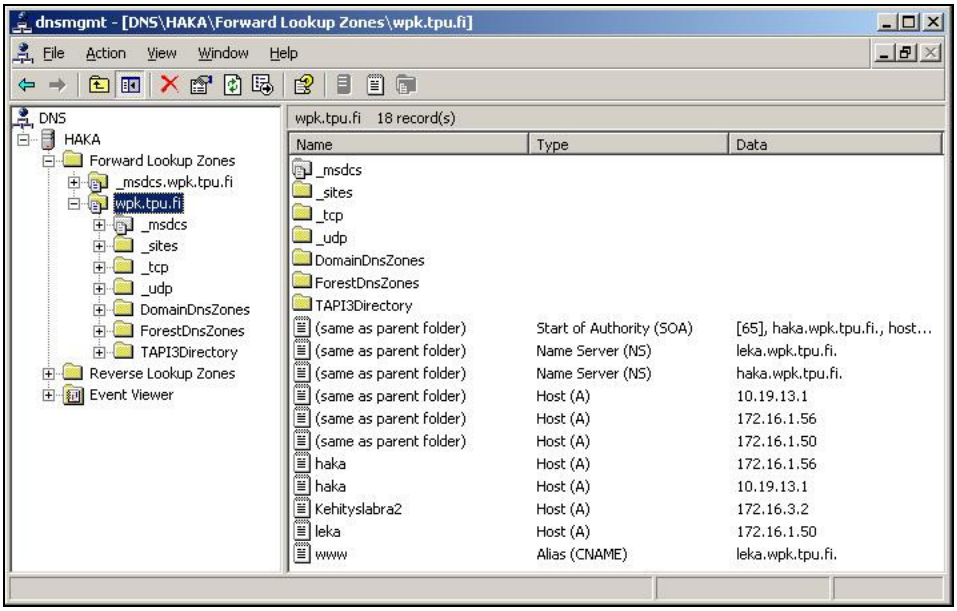
ip helper-address:n määritys Catalystin verkkoliitännöille:

```
Catalyst int# ip helper-address <DHCP-palvelimen osoite>
```

6.6 DNS

Asennettaessa Hakalle palvelimen oletuskokoonpanoa, asentui myös DNS yhtenä oletuspalveluista. Myöhemmin DNS asennettiin varmennustarkoituksella myös Lekalle.

Koska Leka on WPK-verkossa sekä laboratoriototeutuksessa WWW-palvelin, tehtiin DNS:ään alias (CNAME) ”www”, joka osoittaa osoitteeseen leka.wpk.tpu.fi. Näin ollen http://www ja http://www.wpk.tpu.fi johtavat Lekan WWW-sivulle (kuva 10).



Kuva 10: Verkon DNS-palvelu

6.7 Sovelluspalvelimet (IIS)

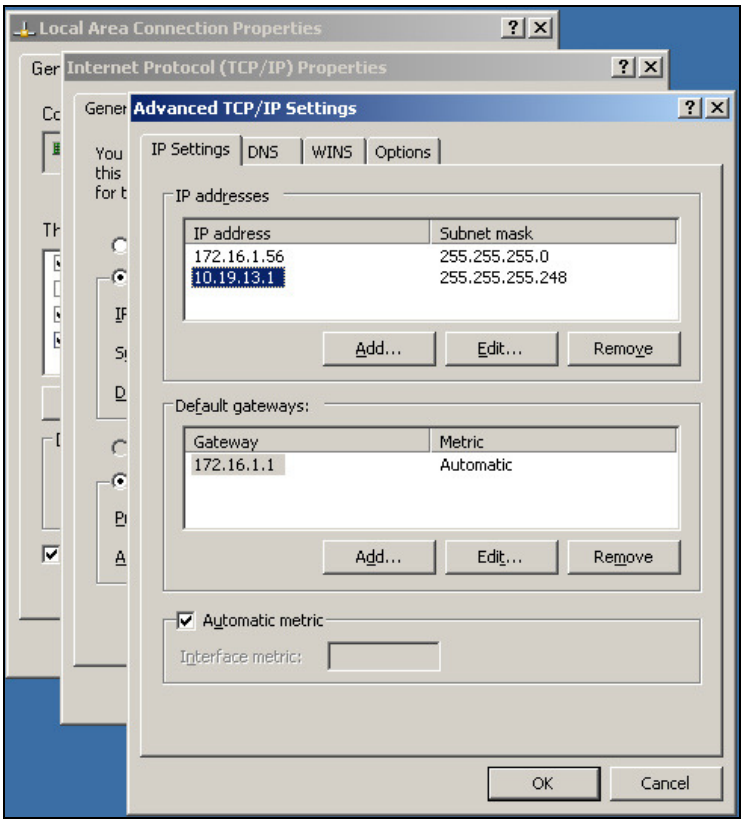
Nykyisessä WPK-verkossa WWW-palvelimena toimii Leka. Tästä syystä myös laboratorioverkon uusi Leka sai saman roolin. Kuten muidenkin palvelinroolien, myös IIS:n asennus suoritettiin Manage your Server –ikkunasta. Valitaan lisättäväksi ”Application server” ja IIS asentuu automaattisesti.

WWW-palvelimen toiminnan varmistamiseksi avattiin Internet Information Services (IIS) Manager. Oletussivuston hakemistoon tehtiin uusi tiedosto, index.html. Kun IIS oli saatu toimintaan, avattiin Kehityslabra2-työasemalla selaimella osoite http://www/index.html. Onnistunut sivuhaku todisti palvelun toimivan.

6.8 Tulostinpalvelin

Verkon tulostinpalvelimena toimii Haka. Myös laboratorioverkossa tulostinpalvelimen rooli annettiin Hakalle. Jo nykyisessä WPK-verkossa käytössä oleva malli, jossa tulostimet ovat omassa erillisessä verkossa Hakan ”takana”, päätettiin säilyttää. Tämä mahdollistaa halutusti sen, ettei verkon tulostimille voida tulostaa muuten kuin tulostinpalvelimen kautta.

Tämänhetkisessä WPK-verkossa tulostimet ovat 10.19.13.0 / 29 –verkossa. Myös laboratorioverkossa tehdään samoin. Hakan verkkokortille annetaan toissijainen IP-osoite, 10.19.13.1 ja aliverkon peite 255.255.255.248 (Kuva 11).



Kuva 11: Hakan IP-asetukset

Verkkotulostin liitetään samaan kytkimeen, jossa Haka on, ja sille annetaan IP-asetuksiksi osoite 10.19.13.6 ja maski 255.255.255.248.

Tämän jälkeen Hakan Manage Your Server –ikkunasta lisätään tulostinpalvelinrooli. Asennusvelho kysyy, asennetaanko paikallinen tulostin vai verkkotulostin. Vastoin logiikkaa valitaan paikallinen tulostin. Tämä siksi, että asennettaessa tulostinta tulostinpalvelimelle, kyseessä on paikallinen tulostin. Annetaan em. tulostimen osoite ja valitaan listalta oikea tulostinajuri kyseiselle laitteelle. Tulostimelle voidaan vielä antaa jakonimi ja sille voidaan lisätä kuvaus.

Työasemalla (tässä kehityslabra2 -kone) avataan asetuksista tulostimet ja lisätään tulostin. Nyt kyseessä on verkkotulostin. Tulostin voidaan etsiä hakemalla se hakemistosta (Find a printer in the directory). Valitaan ”hae”, ja tulostin ilmestyy listalle. Valitaan tulostin ja painetaan ”ok”. Tulostin asentuu oletustulostimeksi.

6.9 F-Secure Policy Manager

F-Secure Policy Manager on keskitettyyn tietoturvahallintaan tarkoitettu ohjelmisto. Sillä voidaan hallita niin suurten kuin pientenkin verkkojen työasemien virustorjuntaa ja palomuureja, päivittää viruskuvaustietokannat automaattisesti ja asentaa työasemille keskitetysti tietoturvasovellukset ja niiden päivitykset. (F-Secure)

Tuotteen tärkeimmät osat ovat Policy Manager Server, joka jakaa ohjelmat, päivitykset ja määritykset verkossa, sekä Policy Manager Console, jolla Serveriä hallitaan. Consolella määritetään työasemien tietoturvamääritykset, asennetaan ohjelmat ja tarkkaillaan hälytyksiä. (F-Secure)

Laboratoriototeutukseen oli tarkoitus asentaa myös tälläkin hetkellä WPK-verkossa käytössä oleva F-Secure Policy Manager. Kuitenkin ilmeni, että TAMK:n lisenssi kyseiseen ohjelmistoon on päättymässä, ja koulu siirtyy Pandan tuotteisiin. F-Securen asennusmediaa ei siis enää ollut saatavilla. Myöskään Pandan tuotetta ei ole vielä otettu käyttöön, joten sitäkään ei ollut saatavilla.

7 Pohdintaa

7.1 Yleistä

Tämän opinnäytetyön tarkoitus oli suunnitella ja toteuttaa laboratorioympäristössä WPK-verkon segmentointi. Segmentointi eli aliverkkoihin jakaminen oli tullut tarpeelliseksi verkon paisuttua nykyiseen kokoonsa. WPK-verkko on ollut olemassa niin kauan kuin tietoverkkopalveluiden opetus on järjestetty Teiskontien toimipisteessä, eikä sitä ole aikanaan suunniteltu tämän mittakaavan käyttöön. Verkkopalveluiden opiskelijamäärät ovat kasvaneet viime vuosina, ja samoin verkkopalveluiden opintojaksojen määrä. Tätä nykyä eräissä WPK-verkkoon kuuluvissa luokissa pidetään lähiopetusta jopa 40 h viikossa.

Ajan mittaan WPK-verkkoon on tuotu tarpeen mukaan uusia luokkia, uusia laitteita ja uusia palveluita. Harjoittelijat ovat päivittäneet konekantaa, ja tilatut opinnäytetyöt ovat tuoneet oman mausteensa verkkoon. Kuitenkin kaikki tämä on tehty yksinkertaisesti lisäämällä kulloinkin tarvitut palaset palapeliin. Siksi nykyinen WPK-verkko ei täytä niitä suunnitteluvaatimuksia, joita alleviivataan verkon luokissa opetettavilla opintojaksoilla. Tämä opinnäytetyö tehtiin WPK-verkon päivittämisen pohjaksi.

Työn suunnittelun ja työstämisen jo alettua tuli vastaan ongelma, joka pakotti muuttamaan suunnitelmaa. NAT-toiminnallisuuden puuttuminen työhön varatusta kytkimestä oli yllätys niin opinnäytetyön tekijälle, kuin toimeksiantajallekin. Asiasta ja ratkaisusta neuvoteltiin toimeksiantajan kanssa, ja päätettiin että työ tehdäänkin laboratoriossa WPK-verkon päivityksen pohjaksi. Opinnäytetyön vaativuuden kannalta työnkuvan muuttuminen vaikutti toisaalta helpottavasti, mutta toisaalta se toi täysin uutta sisältöä työhön. Käyttöönotto, ehkä mittavin ja työläin osa alkuperäistä suunnitelmaa, jäi nyt toteuttamatta. Alkuperäisen suunnitelman mukaan palvelimille olisi pitänyt tehdä pieniä muutostöitä, mutta nyt kaksi palvelinta kaikkine rooleineen tuli asentaa alusta pitäen. Oli kaiken kaikkiaan varsin mielenkiintoista rakentaa oikea, toimiva verkko miniatyyrikoossa. Vaikka verkko rakennettiinkin typistetysti, sisälsi se kuitenkin kaikki oikean verkon osat ja toiminnot; mm. erilliset aliverkot ja reitityksen, kaksi ohjauspalvelinta, työasema(t), verkkotulostuksen ja tiedostopalvelut.

7.2 Toteutuksesta

Kun toimeksiantaja ehdotti laboratoriototeutusta Virtual Server 2004:n kanssa, en tiennyt mitä odottaa. Kuitenkin välittömästi toimeen tartuttuani ymmärsin, että tällä tavalla sovellettu työ oli sekä mielenkiintoinen että erittäin käytännöllinen tapa toteuttaa demonstraatioverkon rakentaminen.

Kaksi palvelinta oli helppoa ja miellyttävää asentaa Virtual PC 2004:n avulla. Ainoa seikka, mikä hieman epäilytti ennen asennuksen aloitta-

mista oli, riittääkö PC:n teho suoriutumaan tehtävästä. Pelko oli kuitenkin turha, sillä riittävästi muistia sisältävä Pentium 4 oli vähintäänkin hyvä työjuhta.

Kuten aiemmin mainittiin, laboratoriototeutus tehtiin sovelletusti. Verkon segmentoinnin tai palveluiden toiminnan kannalta ei ollut välttämätöntä eikä tarpeellista asentaa kaikkia nykyisen verkon laitteita tai palveluita. Nykyisessä WPK-verkossa kaikki keskeiset palvelut on asennettu joko Hakalle tai Lekalle, tai kahdennettu niille molemmille. Siksi laboratoriototeutukseen ei sisällytetty mm. Sharepoint –palvelinta, verkonvalvonnan palvelinta, eikä toisen opinnäytetyön piiriin kuuluvaa Nagios –palvelinta. Kaikki työn ulkopuolelle jätetyt laitteet ja palvelut ovat sellaisia, että ne voidaan verkon päivityksen aikaan uudelleenkonfiguroida melko yksinkertaisesti.

Harjoitteluajallani tutuksi tullut WPK-verkon kehitys- ja tutkimuslaboratorio tarjosi käytännön työlle erinomaiset puitteet. Tarvittavat laitteet, ohjelmistot ja kirjat olivat lähellä ja hyvin saatavilla. Ajan, jonka vietin laboratoriossa, sain enimmäkseen käyttää rauhassa yksin. Kun useamman kuukauden vätystelyn jälkeen viimein ryhdyin käytännön osuuden tekemiseen, ei tehtävä enää tuntunutkaan niin raskaalta kuin aiemmin. Pienen lisäjännityksen työhön kuitenkin toi toteutuksen laajuuden lähes viime metreille säilynyt epämääräisyys. Toimeksiantajan kanssa oli tosin aiemmin keskusteltu seikoista ja palveluista, jotka työhön tulee sisällyttää, mutta vielä loppuvaiheessa niitä uhkasi tulla lisää. Onneksi työ kuitenkin lopulta pysyi siinä mittakaavassa, jollaiseksi olin sen työnkuvan muututtua mieltänyt.

7.3 Mahdollisia lisäyksiä

Käytännön osuuteen olisi ollut erittäin mielenkiintoista sisällyttää keskitetyn tietoturvasovelluksen asennus ja konfigurointi. Valitettavasti se ei kuitenkaan ollut mahdollista tämänhetkisellä työkalulla, sillä kyseisen ohjelmiston lisenssi oli päättymässä. Myöskään uudemman sovelluksen asentaminen ei ollut vielä mahdollista, sillä edes tietokonekeskus ei ollut vielä saanut uutta tuotetta käyttöön.

Olisi toki ollut mahdollista valita ja asentaa Internetistä jokin vapaan lähdekoodin sovellus, mutta se ei olisi ollut tarkoituksenmukaista tämän opinnäytetyön kannalta. Opinnäytetyö tehtiin joka tapauksessa pohjaksi verkon mahdollista päivitystä varten, eikä satunnaisesti valitun ohjelmiston asennusta ja testausta varten.

VPN-yhteys verkon ulkopuolelta on palvelu, jonka nykyinen WPK-verkko tarjoaa. Laboratoriototeutuksessa VPN-palvelun rakentaminen olisi ollut hankalaa useammastakin syystä. Koska laboratoriototeutus tehtiin nykyistä nimiavaruutta käyttäen, ei laboratorioverkkoa voinut noin vain kytkeä ”oikeaan” verkkoon. Tietokonekeskukselta saatu IP-osoitevaranto on myös tätä nykyä niin kovassa käytössä, ettei VPN-palvelun rakentaminen olisi välttämättä ollut edes mahdollinen. Kaiken

kaikkiaan laboratoriototeutus tehtiin niin soveltaen, että myös VPN-palvelu olisi pitänyt tehdä varsin rankasti soveltaen. Aidosta VPN-palvelusta radikaalisti poikkeava ratkaisu ei tässäkään tapauksessa olisi ollut tarkoituksenmukainen. Toimeksiantaja antoi siis luvan jättää VPN-palvelu työn ulkopuolelle.

7.4 Oma arvio

Opinnäytetyöni aihe osoittautui varsin mielenkiintoiseksi. Vaikka itse työ muuttuikin alkuperäisestä paljon, ei käänne suinkaan ollut huonompaan. Työn kirjoittaminen alkoi teoriaosuudella jo kevättalvella 2006, mutta käytännön osuus antoi odottaa itseään syksyyn 2006.

Laboratoriototeutus valmistui melko vauhdikkaasti. Ennen itse työn aloittamista olin valmistautunut hyvin ja suunnitellut varsin tarkasti kaiken mitä teen ja miten ne teen. Suurempia vastoinkäymisiä ei käytännön vaiheessa enää tullut vastaan.

Mikäli WPK-verkkoa jossakin vaiheessa lähdetään päivittämään opinnäytetyöni viitoittamalla tiellä, uskon olevan parasta suorittaa työ vähintään muutaman henkilön voimin. Verkon päivittäinen opetus- ja harjoittelukäyttö sanelevat sen, että työ lienee pakko suorittaa viikonloppuna tai loma-aikaan. Siitä, onko palvelimet syytä päivittää uuden tilanteen mukaiseksi vai peräti asentaa kokonaan uudelleen, voidaan väitellä. Useamman palvelimen asentaminen ja palauttaminen aiempaa vastaavaan tilaan voi olla valtava urakka. Toisaalta tilanne, jossa kaikki lähtee puhtaalta pöydältä, kirkastaa kokonaiskuvan ylläpitäjän kannalta.

Kokonaisuudessaan olen varsin tyytyväinen opinnäytetyöhöni. Aihe oli käytännönläheinen ja työympäristö jo valmiiksi tuttu. Harjoitteluni aikana mietin useasti kuinka mikäkin WPK-verkon tehtävä on toteutettu, ja kuinka ne toteutettaisiin työni kaltaisessa ympäristössä. Opinnäytetyöhöni kaavailemani aikataulu petti perusteellisesti. Alun perin olin suunnitellut saavani työn valmiiksi jo keväällä 2006, mutta syksyyn työn valmistuminen joka tapauksessa venyi. Lopputulokseen olen kuitenkin tyytyväinen.

Lähteet

An educator's guide to school networks. Chapter 4: Cabling. The Florida Center for Instructional Technology College of Education, University of South Florida. [online] [viitattu 5.10.2006]
http://fcit.usf.edu/network/chap4/chap4.htm

An educator's guide to school networks. Chapter 5: Topology. The Florida Center for Instructional Technology College of Education, University of South Florida. [online] [viitattu 9.2.2006]
http://fcit.usf.edu/network/chap5/chap5.htm

Casad, Joe, Willsey, Bob 1999. TCP/IP Trainer. Helsinki: IT Press

CiscoKits.com [online][viitattu 14.9.2006]
http://www.ciscokits.com/images/3550.jpg

Cisco Systems – Cisco Catalyst 3550 24 EMI Switch [online][viitattu 5.4.2006]
http://www.cisco.com/en/US/products/hw/switches/ps646/ps3813/index.html

F-Secure Oyj – F-Secure Policy Manager [online][viitattu 14.9.2006]
http://www.f-secure.fi/tuotteet/fspm

ICTP – Scientific Computer Section Portal. [online][viitattu 22.4.2006]
http://www-scs.ictp.trieste.it/images/rj45.jpg

Internet Assigned Numbers Authority – IANA.org [online][viitattu 22.8.2006]
http://www.iana.org/assignments/port-numbers

Jaakohuhta, Hannu 2005. Lähiverkot – Ethernet. Helsinki: IT Press

Kivimäki, Jyrki 2005. Windows Server 2003 – Tehokas hallinta. Helsinki: Readme.fi

Meyers, Michael 2003. Verkot+-sertifikaatti. Helsinki: IT Press

Microsoft Suomi - Windows Server 2003 [online][viitattu 12.9.2006]
http://www.microsoft.com/finland/products/windowsserver2003/evaluation/choosing/default.mspx

Microsoft Windows SharePoint Services. Microsoft Suomi. [online] [viitattu 27.2.2006]
http://www.microsoft.com/finland/pkinfo/products/online/sp/default.mspx

Nagios.org – About Nagios [online][viitattu 14.9.2006]
http://nagios.org/about/

Wikipedia – Vapaa tietosanakirja. Ethernet. [online][viitattu 27.3.2006]
http://fi.wikipedia.org/wiki/Ethernet

Liitteet

Liite1: Ethernet-standardit

Standardi	Vuosi	Kuvaus
Kokeellinen Ethernet	1972 (paten-toitu 1978)	2,94 Mb/s koaksiaalikaapelissa
Ethernet II (DIX v2.0)	1982	10 Mb/s paksu koaksiaalikaapeli
IEEE 802.3	1983	10BASE5, 10 Mb/s paksu koaksiaalikaapeli
802.3a	1985	10BASE2, 10 Mb/s ohut koaksiaalikaapeli
802.3c	1985	10 Mb/s toistimen määrittely
802.3d	1987	FOIRL (Fiber-Optic Inter-Repeater Link)
802.3i	1990	10BASE-T, 10 Mb/s parikaapelissa
802.3j	1993	10BASE-F, 10 Mb/s valokuidussa
802.3u	1995	100BASE-T Fast Ethernet, 100 Mb/s
802.3x	1997	Full Duplex
802.3z	1998	1000BASE-X, Gigabit Ethernet koaksiaalissa, 1 Gb/s
802.3ab	1999	1000BASE-T, Gigabit Ethernet parikaapelissa, 1 Gb/s
802.3ac	1998	Kehyksen koko 1522 tavua, VLAN-tagit
802.3ad	2000	Linkkien yhdistäminen
802.3ae	2003	10 Gigabit Ethernet kuidussa
802.3af	2003	Tehonsyöttö ja Ethernet samassa 4-parisessa kaapelissa, (Power over Ethernet)

(Wikipedia… Ethernet 2006)

Liite 2: Catalystin konfiguraatio

```
!
enable
!
config terminal
!
enable secret class
enable password cisco
!
hostname Catalyst
!
!
ip subnet-zero
ip routing
!
! DHCP-pyyntojen forwardoinnin mahdollistava
! helper-address (Haka eli 172.16.1.56)
! luokkien liitannoille.
!
interface FastEthernet0/1
 description PALVELIMILLE
 no switchport
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/2
 description LUOKKAAN C4-02
 no switchport
 ip address 172.16.2.1 255.255.255.0
 ip helper-address 172.16.1.56
!
interface FastEthernet0/3
 description LUOKKAAN C4-03
 no switchport
 ip address 172.16.3.1 255.255.255.0
 ip helper-address 172.16.1.56
!
interface FastEthernet0/4
 description LUOKKAAN C4-04
 no switchport
 ip address 172.16.4.1 255.255.255.0
 ip helper-address 172.16.1.56
!
interface FastEthernet0/5
 description LUOKKAAN C4-12
 no switchport
 ip address 172.16.5.1 255.255.255.0
 ip helper-address 172.16.1.56
!
interface FastEthernet0/6
 switchport mode dynamic desirable
!
interface FastEthernet0/7
 switchport mode dynamic desirable
!
interface FastEthernet0/8
 switchport mode dynamic desirable
!
interface FastEthernet0/9
 switchport mode dynamic desirable
```

```
!
interface FastEthernet0/10
 switchport mode dynamic desirable
!
interface FastEthernet0/11
 switchport mode dynamic desirable
!
interface FastEthernet0/12
 switchport mode dynamic desirable
!
interface FastEthernet0/13
 switchport mode dynamic desirable
!
interface FastEthernet0/14
 switchport mode dynamic desirable
!
interface FastEthernet0/15
 switchport mode dynamic desirable
!
interface FastEthernet0/16
 switchport mode dynamic desirable
!
interface FastEthernet0/17
 switchport mode dynamic desirable
!
interface FastEthernet0/18
 switchport mode dynamic desirable
!
 interface FastEthernet0/19
 switchport mode dynamic desirable
!
interface FastEthernet0/20
 switchport mode dynamic desirable
!
interface FastEthernet0/21
 switchport mode dynamic desirable
!
interface FastEthernet0/22
 switchport mode dynamic desirable
!
interface FastEthernet0/23
 switchport mode dynamic desirable
!
interface FastEthernet0/24
 description ULKOVERKKOON
 no switchport
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
 interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 no ip address
 shutdown
!
!
exit
```

```
!
!
ip classless
ip http server
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
!
line vty 5 15
 login
!
!
end
!
!
```

Liite 3: Verkon IP-suunnitelma

172.16.0.0 255.255.255.0 (/24)
254 aliverkkoa, 254 hostia / aliverkko

Taulukossa 30 ensimmäistä käytettävissä olevaa aliverkkoa (sekä viimeinen)

#	ID	Range	Broadcast	Käyttö
1	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255	palvelimet
2	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255	C4-02
3	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255	C4-03
4	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255	C4-04
5	172.16.5.0	172.16.5.1 - 172.16.5.254	172.16.5.255	C4-12
6	172.16.6.0	172.16.6.1 - 172.16.6.254	172.16.6.255	
7	172.16.7.0	172.16.7.1 - 172.16.7.254	172.16.7.255	
8	172.16.8.0	172.16.8.1 - 172.16.8.254	172.16.8.255	
9	172.16.9.0	172.16.9.1 - 172.16.9.254	172.16.9.255	
10	172.16.10.0	172.16.10.1 - 172.16.10.254	172.16.10.255	
11	172.16.11.0	172.16.11.1 - 172.16.11.254	172.16.11.255	
12	172.16.12.0	172.16.12.1 - 172.16.12.254	172.16.12.255	
13	172.16.13.0	172.16.13.1 - 172.16.13.254	172.16.13.255	
14	172.16.14.0	172.16.14.1 - 172.16.14.254	172.16.14.255	
15	172.16.15.0	172.16.15.1 - 172.16.15.254	172.16.15.255	
16	172.16.16.0	172.16.16.1 - 172.16.16.254	172.16.16.255	
17	172.16.17.0	172.16.17.1 - 172.16.17.254	172.16.17.255	
18	172.16.18.0	172.16.18.1 - 172.16.18.254	172.16.18.255	
19	172.16.19.0	172.16.19.1 - 172.16.19.254	172.16.19.255	
20	172.16.20.0	172.16.20.1 - 172.16.20.254	172.16.20.255	
21	172.16.21.0	172.16.21.1 - 172.16.21.254	172.16.21.255	
22	172.16.22.0	172.16.22.1 - 172.16.22.254	172.16.22.255	
23	172.16.23.0	172.16.23.1 - 172.16.23.254	172.16.23.255	
24	172.16.24.0	172.16.24.1 - 172.16.24.254	172.16.24.255	
25	172.16.25.0	172.16.25.1 - 172.16.25.254	172.16.25.255	
26	172.16.26.0	172.16.26.1 - 172.16.26.254	172.16.26.255	
27	172.16.27.0	172.16.27.1 - 172.16.27.254	172.16.27.255	
28	172.16.28.0	172.16.28.1 - 172.16.28.254	172.16.28.255	
29	172.16.29.0	172.16.29.1 - 172.16.29.254	172.16.29.255	
30	172.16.30.0	172.16.30.1 - 172.16.30.254	172.16.30.255	

…..

254	172.16.254.0	172.16.254.1 - 172.16.254.254	172.16.254.255	
Tul.	10.19.13.0 / 29	10.19.13.1 – 10.19.13.6	10.19.13.7	Tulostimet

Laite	Liitäntä	Verkko	ip-osoite	mihin?
Catalyst	fa0/1	172.16.1.0 / 24	172.16.1.1	Palvelinkytkin,

				Palvelimet
	fa0/2	172.16.2.0 / 24	172.16.2.1	C4-02:n kytkin
	fa0/3	172.16.3.0 / 24	172.16.3.1	C4-03:n kytkin
	fa0/4	172.16.4.0 / 24	172.16.4.1	C4-04:n kytkin
	fa0/5	172.16.5.0 / 24	172.16.5.1	C4-12:n kytkin
	fa0/24	*192.168.1.0 / 24*	*192.168.1.1*	*Ulkoverkkoon*
Haka	eth0	172.16.1.0 / 24	172.16.1.56	Palvelinkytkin, Catalyst
		10.19.13.0 / 29	10.19.13.1	Palvelinkytkin, Tulostimet
Leka	eth0	172.16.1.0 / 24	172.16.1.50	Palvelinkytkin, Catalyst
HP Laserjet 5M	eth0	10.19.13.0 / 29	10.19.13.6	Palvelinkytkin, Haka
Nagios	*eth0*	*172.16.1.0 / 24*	*172.16.1.91*	*Palvelinkytkin, Catalyst*
Valvonta /Valvomo	*eht0*	*172.16.1.0 / 24*	*172.16.1.90*	*Palvelinkytkin, Catalyst*
Sharepoint	*eth0*	*172.16.1.0 / 24*	*172.16.1.95*	*Palvelinkytkin, Catalyst*