VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Sari Uitto

LÄHIVERKON SUUNNITTELU VIRTUAALISENA YKSITYISVERKKONA

Liiketalous ja matkailu
2011

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Sari Uitto
Opinnäytetyön nimi	Lähiverkon suunnittelu virtuaalisena yksityisverkkona
Vuosi	2011
Kieli	suomi
Sivumäärä	42 + 3 liitettä
Ohjaaja	Christer Karlsson

Tämän opinnäytteen tarkoituksena on selvittää, kuinka voidaan luoda lähiverkko käyttäen virtuaalista yksityisverkkoa. Virtuaalisuus viittaa tässä tapauksessa lähinnä tämän opinnäytetyön toteutustapaan, sillä varsinaista toteutusta ei koskaan tehty. Esimerkkinä käytetään kuvitteellista, fuusioitunutta yritystä, jolla on kolme eri toimipistettä. Tietoturvallisuus mielessä pitäen, työssä esitellään paikallisen palveluntarjoajan yhtä ratkaisua lähiverkon suunnitteluun virtuaalisena yksityisverkkona.

Teorian rooli tässä opinnäytetyössä alustaa lukijaa ymmärtämään lähiverkkojen maailmaa. Siinä on haluttu tuoda esille keskeisimmät käsitteet menemättä kuitenkaan liian syvälle. Käsitteitä löytyy niin laitteiston, tietoturvan että topologioidenkin ryhmistä. Näistä ehkä tunnetuimpia käsitteitä tietoliikenteen puolella ovat reititin, kytkin, protokollat ja IP-osoitteet sekä niiden takana pyörivä logiikka.

Teoria yhdistyy käytäntöön viimeisissä kappaleissa, joissa esitellään yksi ratkaisumalli lähiverkolle. Käytännön työ on tehty mahdollisimman realistisia tietoja käyttäen pohjautuen palveluntarjoajalta saatuihin tietoihin. Vaikka varsinaista lähiverkkorakennelmaa ei toteutettu oikeilla laitteilla, on opinnäytetyössä tuotu esiin mahdollisimman pitkälle asennettu rakennelma käyttäen Ciscon Packet Tracer -ohjelmaa. Sillä pystytään osoittamaan, että rakennetut IP-osoitemaailmat sekä eri tietoturvallisuusasetukset toimivat suunnitellusti.

Avainsanat lähiverkko, tietoliikenneverkot, virtuaalinen yksityisverkko

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Systems

ABSTRACT

Author	Sari Uitto
Title	Designing LAN Using Virtual Private Network
Year	2011
Language	Finnish
Pages	42 + 3 Appendices
Name of Supervisor	Christer Karlsson

The aim of this thesis is to clarify how to create local area network using virtual private network. Virtual in this thesis refers mostly to the way it's been realized since an actual design in real environment was never made. An imaginary company with three different branch offices is used as an example. Keeping data security in mind, this thesis presents a local service provider's model as a solution for this case.

The role of theory in this thesis is to prepare the reader to understand the world of local area networks. Basic terms and concepts are brought up, without going too deep into it.

Theory joins together with practice in the last chapters where the reader is presented one solution model. Practice part is done as realistically as possible, basing itself on the facts provided by the local service provider. The thesis shows the structure of the network using Cisco's Packet Tracer software program. With that it is possible to demonstrate that the IP addresses and different data security settings are working as planned.

Keywords Local Area Networks, data communications, VPN

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

LIITELUETTELO

SANASTO

Packet Tracer	Ciscon tekemä ohjelmisto, jolla voidaan suunnitella ja simuloida verkkoja virtuaalisesti.
Alueverkko	WAN, Wide Area Network, laajemmalle ulottunut verkosto reitittimiä ja kytkimiä sekä niiden alla olevat aliverkot
DMZ	Demilitarized Zone eli alue verkossa, jossa verkon suojaustaso on alempi verrattuna sisäverkon suojauksiin.
SMTP	Simple Mail Transfer Protocol, käytetään sähköpostien välittämiseen palvelimien välillä.
POP	Post Office Protocol, käytetään sähköpostien noutamiseen palvelimilta.
www	World Wide Web, voidaan näyttää eri sivuja joko suojaamattomina tai suojattuina hypertekseinä.
FTP	File Transfer Protocol, yksi käytetyimpiä protokollia tiedostojen siirrossa eri palvelimelta toiselle tai omalle koneelle.
Protokolla	Käytäntö tai standardi, jolla määritellään, miten eri laitteet keskustelevat toistensa kanssa.
OSI	Open Systems Interconnection Reference Model. Standardi, jolla pyritään rakentamaan avoimia järjestelmiä, ja datan liikkuminen voidaan tehdä usean eri laitevalmistajan laitteilla.
MAC-osoite	Ainutlaatuinen jokaisella laitteella oleva heksadesimaalinen osoite.
MPLS	Multi-Protocol Label Switching, jolla mahdollistetaan nimensä mukaisesti monen eri protokollan toiminta saman verkon alaisuudessa.
Wildcard mask	”Jokerimaski”. Saadaan vähentämällä aliverkkomaski luvusta 255.255.255.255.
VRF	VPN Routing and Forwarding. Avainelementti Ciscon MPLS-tekniikassa.
Quad zero	Yleinen nimitys 0.0.0.0 / 0 -osoitteelle.

1 JOHDANTO

Koko opinnäytetyön lähtökohtana oli oma mielenkiinto aiheeseen. Ciscon Certified Network Associate (CCNA) kahdentoista opintoviikon opinnot avasivat tietoliikenteen eri salat hyvin tehokkaasti. Vaikka oli vaikeaa löytää juuri haluamaani yrityshanketta, päätin lopuksi rakentaa itse kuvitteellisen yrityksen. Sen avulla pääsin tutkimaan tarkemmin lähiverkon suunnittelua käytännön työnä.

Halusin ottaa mukaan myös aidon ratkaisun, joten otin yhteyttä paikalliseen palveluntarjoajaan Anviaan. Anvia tarjoaa erilaisia tietoliikenneratkaisuja yrityksille, läheltä ja kaukaa, tarpeen mukaan. Heiltä sain ehdotuksen, miten vastaavanlainen rakennelma voitaisiin toteuttaa heidän ratkaisujen pohjalta. Koska tietoturva on tärkeä asia nykypäivän tietoliikenteessä, on tässä työssä keskitytty siihen, miten Anvia toimittaa virtuaalisia yksityisverkkoja yrityksille. Heillä on myös käytössä Ciscon tekniikkaa.

Opinnäytetyö on rakennettu Ciscon laitteiden ja sovellusten ympärille, kuvitteelliseen ympäristöön. Työssä esitellään kuvamateriaalia tehdystä rakenteesta, kerrotaan toteutusvaiheen kompastuskivistä ja mukaan on liitetty reitittimien sekä kytkinten asetukset, mikäli lukija haluaa rakentaa saman pohjan kokeilumielessä. Yksi toiveeni onkin tämän opinnäytetyön kanssa, että lukija innostuisi aiheesta ja kokeilisi myös itse suunnitella lähiverkkoja.

2 YRITYSKUVAUS

Northern Cloud Oy on kuvitteellinen yritys, jolla on kolme toimipistettä. Kaksi toimipisteistä sijaitsee Suomessa ja yksi Ruotsissa. Yritys muodostui alun perin kolmen yrityksen sulautumisesta yhteen, ja tällä haettiin vahvempaa markkina-asemaa Skandinavian alueella. Kaukaisena tavoitteena on mahdollisesti sulauttaa muita yhteistyöyrityksiä muiden Pohjoismaiden alueelta Northern Cloudin alle ja näin saada suuremmat markkina-alueet käyttöön.

Yritys on erikoistunut media-alan tuotantoon. Graafinen suunnittelu sekä erilaiset videotuotannot kuuluvat pääasialliseen yritystoimintaan. Tuotantoon kuuluu myös www-sivujen tuotantoa. Videotuotanto sisältää DVD-, blu-ray- sekä tavalliset videotuotannot, ja asiakaskunta koostuu lähinnä Euroopan alueella olevista elokuvalevitysyrityksistä. Muita asiakkaita ovat toiset media-alan yritykset ja yritykset, jotka tarvitsevat joko graafista suunnittelua tai videoleikkauspalveluja. Itse videokuvausta ei yritys hoida, vaan materiaali tulee toimistolle raakamateriaalina, jota työstetään tietokoneella.

Toimipisteet sijaitsevat Vaasassa, Helsingissä ja Tukholmassa. Vaasa on erikoistunut graafiseen suunnitteluun ja Tukholma videotuotantoon. Helsinki toimii Suomen alueen myyntikonttorina, sillä suurin osa asiakkaista on pääkaupunkiseudulla. Toimistolla on kuitenkin pieni graafinen osasto käytössä. Tukholmassa on myös oma myyntiosasto, joka hoitaa myynnin Ruotsin alueella. Koko yrityksen talousosasto on pelkästään Vaasan konttorilla.

Opinnäytetyön lähiverkkoihin kuuluvat näiden kolmen toimipisteen lähiverkot, jotka on yhdistetty toisiinsa alueverkon (WAN) kautta. Suoraa fyysistä yhteyttä toimipisteiden välillä ei siis luonnollisesti ole. Yhdistäminen toisiin lähiverkkoihin voidaan hoitaa monella eri tavalla. Helpoin tehtävä on antaa Internet-palveluntarjoajan tehdä omalla reitittimellään tarvittavat yhteysasetukset. Toinen tapa on tehdä asetukset yrityksen omassa reitittimessä ja saada yhteys toimimaan suoraan ilman välikäsiä, mutta tämä voi olla hankalaa ja tietoturvallisuutta ei välttämättä ole otettu kaikilta osin huomioon.

Kaikille toimistoille yhteistä on tietyt tietoturvaan liittyvät seikat, kuten millä koneilla on pääsy kaikkiin sisäverkossa oleviin resursseihin ja keillä taas on rajoitetut resurssit. Lähinnä on eroteltu hallintopuolen verkko työntekijöiden omasta verkosta, koska kaikilla ei ole tarvetta päästä käsiksi esimerkiksi tärkeisiin tietokantoihin. Ajattelumallina on käytetty antamalla verkossa pääsy vain pakollisiin resursseihin, mitä työntekijä työssään tarvitsee.

2.1 Vaasan toimisto

Vaasan toimipiste on päätoimipiste. Siellä sijaitsee normaaliin työskentelyyn tarvittavien laitteiden lisäksi koko yrityksen toimintaan tarvittavat palvelimet. Muutama palvelimista on sijoitettu omalle alueelleen verkkotopologiassa, niin kutsutulle DMZ eli harmaalle vyöhykkeelle. Kirjaimet DMZ tulevat sanoista *demilitarized zone*, jotka viittaavat armeijan termiin alueesta, jossa ei ole aktiivista sotatoimintaa. Tietoliikenteessä tämä vyöhyke ei ole suojattu niin tiukoilla säännöksillä kuin sisäverkko. Tämä siksi, että ulkoa tulevat palvelinkutsut eivät vahingossa tai tarkoituksella jää vastaamatta. Sisäverkko kuitenkin täytyy suojata tarkemmin ulkopuolelta tulevaa liikennettä vastaan.

Vaasan toimistolla on 13 työntekijää. Työntekijät voidaan jakaa neljään eri ryhmään: graafinen, myynti-, talousosasto sekä johtoporras. Koska kyse on mediaalan yrityksestä, tietokoneina käytetään sekä Windows- että Macintosh-tietokoneita. Tästä ei aiheudu suurempaa ongelmaa, sillä kummatkin laitteet tukevat samaa TCP/IP-protokollaa. Graafisella osastolla on käytössä tietokoneiden lisäksi kaksi ulkoista kovalevyä, jotka on liitetty verkkoon omilla IP-osoitteillaan. Jokaisella osastolla on myös oma tulostimensa. Näiden laitteiden lisäksi toimistolla on kokoushuone, jossa on tarvittaessa langaton yhteys kannettaville tietokoneille.

Palvelimet ovat sijoitettu pieneen, lukittuun tilaan. Ulkopuolisilta on pääsy kielletty tähän huoneeseen ja käytännössä vain verkosta vastaavalla henkilöllä on pääsy tilaan. Käytössä ovat SMTP-, www-, FTP-, POP- ja tietokantapalvelimet. Näistä kolme ensimmäistä ovat DMZ -alueella ja loput kaksi ovat sisäverkossa. Tietoturvan kannalta täytyy miettiä, mikä on sallittavaa liikennettä DMZ -alueella. Sähkö-

postiliikenne on eroteltu erillisiksi osiksi lisäämään tietoturvaa. SMTP-palvelin ottaa vain vastaan sähköpostit ja lähettää ne eteenpäin sisäverkkoihin.

2.2 Helsingin toimisto

Helsingissä toimistolla on töissä 8 henkilöä. Toimisto on lähinnä tarkoitettu myyntitoimistoksi, jossa on myös pieni graafinen yksikkö ja johtoportaan tietokoneet. Toimistolle kuuluu lisäksi muutama tulostin ja yksi ulkoinen kovalevy. Toimistolta otetaan tarvittaessa yhteys Vaasan toimiston palvelimiin.

2.3 Tukholman toimisto

Tukholman toimisto on erikoistunut videotuotantoon. Graafiselle suunnittelulle on varattu muutama oma kone. Koska videotiedostot vievät paljon tilaa kovalevyiltä, on Tukholmassa neljä ulkoista kovalevyä. Näillä kaikilla on myös omat IP-osoitteensa. Oma myyntiosasto hoitaa Ruotsin alueen myynnin. Kuten edellisissäkin toimistoissa, Tukholmassa on tulostimet jokaiselle osastolle sekä IP-pohjainen kopiokone.

3 LAITTEISTO

Verkottamiseen tarvitaan erityisiä laitteita, jotta tietoa voidaan kuljettaa, lähettää, vastaanottaa tai säilöä. Laitteita on sekä monimutkaisia että yksinkertaisimpia malleja ja riippuu täysin yrityksestä, millaisia he tarvitsevat käyttöönsä.

Laitteet ja niiden käyttämät protokollat (eli käytännöt) toimivat eri tasoilla tai kerroksilla. 1980-luvulla herättiin siihen tosiasiaan, että tarvittiin yhteiset säännöt ja ratkaisut tietoliikennemarkkinoille. Siihen asti jokainen valmistaja pystyi tarjoamaan vain sellaisia verkotusratkaisuja, jotka olivat yhteensopivia ainoastaan heidän omien laitteidensa kanssa. Yhteiset käytännöt puuttuivat. Tähän ongelmaan saatiin ratkaisu kehittämällä OSI-kerrosmalli. (Granlund 2007, 6)

Kuvio 1. OSI-malli.

Malli on nykyään täysin ISO:n standardisoima kansainvälinen standardi. Sen avulla kuka tahansa laitevalmistaja voi tehdä tietoliikennettä varten tuotteen, ja tuote toimii saumattomasti muiden laitevalmistajien tuotteiden kanssa.

Mallia käytetään myös apuna selvittämään, millä tasolla tietoliikenteessä lähetetyt datapaketit liikkuvat. (Mika Hakala 2005, 138) Tällä on suuri merkitys esimerkiksi ongelmanratkaisussa, jos datapaketit eivät jostain syystä tule perille asti. Tietoliikenneasiantuntija tarkastelee ongelman oireita, osaa sijoittaa ne oikealle tasolle mallissa ja löytää ratkaisun ongelmaan riippuen siitä, minkä kerroksen ongelmasta on kyse. Esimerkiksi fyysisen kerroksen ongelmiin kuuluvat kaikki kaapelointiin

liittyvät ongelmat kun taas verkkokerroksessa otetaan kantaa datapaketin IP-osoitteisiin. Seuraavissa kappaleissa on kerrottu, mihin kerrokseen kyseinen laite mahdollisesti kuuluu ja mikä sen tehtävä on.

3.1 Palvelimet

Palvelin on dataa sisältävä tietokone, jonka tehtävänä on pitää tieto tallessa. Palvelin vastaa ulkopuolelta tuleviin eri palvelinkutsuihin ja lähettää pyydetyt tiedot lopulliselle käyttäjälle. Käyttäjä vuorostaan ottaa tietokoneellaan yhteyttä palvelimeen, kun hän tarvitsee jotain tietoa sieltä. Yhteydenottoon käytetään aina tiettyä ohjelmistoa. (Wikipedia, Palvelin 2011) Ohjelmistoja on monenlaisia, joista käyttäjä voi valita mieleisensä tarvittavilla ominaisuuksilla. Ohjelmistot voivat olla ilmaisia tai maksullisia, mutta tekniikka niiden takana on sama.

Palvelimet ovat fyysisesti suhteellisen samanlaisia toiminnoiltaan, mutta sisältö vaihtelee. Sisältöä käytetään moniin tarkoituksiin ja palvelimia on usein enemmän kuin yksi. Yleisimpiä niistä ovat tiedosto-, sähköposti-, www- ja tietokantapalvelimet, joihin jokainen tietokonetta käyttänyt on tiedostaen tai tietämättään ottanut yhteyttä.

Palvelimiin otetaan yhteyttä tiettyjen porttien kautta. Porttien numerot vaihtelevat käytön mukaan. On olemassa joukko porttinumeroita, jotka on universaalisti valittu ainoastaan yhteen käyttöön. Kuviossa 2 on lista yleisimmistä porttinumeroista, ja mihin palvelinkutsuun ne ovat tarkoitettu.

FTP: 21	Telnet: 23	SMTP: 25
HTTP: 80	POP3: 110	IMAP4: 143
DNS: 53	DHCP: 67	SNMP: 161

Kuvio 2. Yleisimmät porttinumerot.

Yrityksillä on usein monta eri palvelinkonetta hallussaan, joihin on sijoitettu sopivasti sijoitellen eri palveluita. Www-sivut ja sähköpostit voidaan esimerkiksi sijoittaa samalle palvelimelle, koska ne eivät välttämättä yhdessä kuluta niin paljon

tehoja koneelta kuin esimerkiksi tietokanta. Tietokantapalvelin kannattaa pitää erikseen jo tietoturvasyistä, mutta myös koneen tehokkuus saattaa kärsiä, jos sitä kuormitetaan liikaa eri palvelukutsuilla. Palvelinten sisältö kannattaakin miettiä tarkasti.

Nykyään palvelinten sijainti voi olla myös virtuaalinen. (Anvia 2011) Palvelinpalveluja myyvät yritykset voivat tarjota tätä vaihtoehtoa perinteisen fyysisen palvelimen sijaan. Viime kädessä virtuaalipalvelin sijaitsee toki fyysisesti jossain, mutta virtuaalipalvelimia on monta kappaletta samalla fyysisellä palvelimella. Yhteys palvelimelle toteutetaan samalla tavalla kuin normaaliinkin palvelimeen.

3.2 Tietokoneet

Tietokoneet voivat olla tavallisia toimistokäyttöön tarkoitettavia koneita, kannettavia tietokoneita, tehotyöasemia, Macintosh-koneita, kämmentietokoneita tai muita vastaavanlaisia koneita toimistolla. Yleistä niille kaikille on, että ne ottavat yhteyttä reitittimeen lähettääkseen tietopaketteja eteenpäin tai ottaakseen vastaan paketteja haetuilta palvelimilta. Nämä laitteet voivat käyttää eri protokollia päästäkseen käsiksi reitittimeen. Protokollista ylivoimaisesti yleisin on TCP/IP-protokolla, joka toimii kaikenlaisissa ympäristöissä. (Seppänen 2009) Se on oikeastaan joukko erilaisia protokollia, joita käytetään tietoliikenteessä laitteiden välillä eri OSI-kerrosmallin tasoilla. (Wikipedia, TCP/IP 2011)

3.3 Oheislaitteet

Oheislaitteisiin kuuluvat tulostimet, skannerit, ulkoiset kovalevyt, turvakamerat ja niin edelleen. Ne ovat syöttö-, tulostus- tai tallennusvälineitä, jotka auttavat käyttäjäänsä eri tavoin. Oheislaitteita käytetään yleensä tietokoneessa olevan ohjelmiston avulla. Kaikille oheislaitteille tarvitaan oma IP-osoite, mikäli ne ovat yhteisessä käytössä kaikkien tietokoneiden kesken. Tämä on syytä ottaa huomioon IP-osoitteiden lukumäärää laskiessa.

3.4 Reitittimet

Reititin on olennainen osa tietoverkkoa. Ilman sitä ei pystytä siirtämään tietopaketteja eri verkkojen välillä. Sisäisessä verkossa voi olla monta eri aliverkkoa ja, jotta keskustelu kaikkien aliverkkojen välillä on mahdollista, tarvitaan siihen reititin. Luonnollisesti myös kaiken datan liikkuminen alueverkon ja sisäverkon välillä on reititetty. Reititin toimii OSI-mallin kolmannella tasolla ja se osaa liikuttaa paketteja toisille laitteille IP-osoitteen perusteella. (Angelescu 2010, 505)

Reititin tarvitsee topologiatietoja, jotta se voi päättää, mikä reitti on ”lyhin” seuraavaan reitittimeen. Lyhimmällä reitillä ei välttämättä tarkoiteta fyysisesti lyhintä matkaa reitittimeltä toiselle. Mitä korkeampitasoinen reititysprotokolla on valittuna, sen tarkemmin reititin pystyy itsenäisesti päättämään, minne paketit kannattaa seuraavaksi kuljettaa. (Angelescu 2010, 513) Protokollan valinta riippuu kuinka laajalle alalle (lähiverkko, kampusverkko, kaupunkiverkko) sitä on tarkoitus käyttää. Pienissä yrityksissä riittää suhteellisen yksinkertaiset protokollat, joiden avulla tietoa voidaan siirtää suhteellisen helposti reitittimeltä toiselle. Jopa pelkästään staattisesti asetetut osoitteet riittävät pienelle yritykselle. Suuret yritykset voivat käyttää monia erilaisia protokollia, kunhan laitteet vain pystyvät keskenään ymmärtämään niitä.

3.4.1 Protokollat

Reitittäminen voi olla joko staattista tai dynaamista. Staattisessa versiossa tietoliikennehallinnoija asettaa itse kaikki tiedot reitittimiin. Käytännössä tämä on järkevästi mahdollista vain muutaman reitittimen yrityksissä. Hyvänä puolena voidaan pitää sitä, että hallinnoija tietää, miten liikenne on reititetty. Lisäksi reititys ei vie tehoja reitittimeltä, sillä mentävät reitit on jo laskettu sen puolesta. Kuitenkin muutokset liikenteen kulkemiseen täytyy asettaa jokaiseen reitittimeen erikseen, joten hyötysuhde on helposti laskettavissa. Jotta hallinnointi olisi helpompaa, reititykseen on keksitty myös dynaaminen versio. Dynaamisessa versiossa reitittimet puhuvat keskenään ja lähettävät toisilleen tietoja topologioista ja niiden muutoksista automaattisesti asetusten mukaisesti. (Ballew 1998, 114) Tämä mahdollistaa monimutkaisten reititysten teon käytännössä helpoksi.

Dynaamisia reititysprotokollia on kymmenkunta. Protokollat voidaan jakaa muutamaan eri alaryhmään: Etäisyysvektori- (engl. *distance-vector*) ja linkkitilaprotokolliin (engl. *link-state*). On myös olemassa näiden kahden yhdistelmästä tehty hybridiprotokolla. Lisäksi protokollat voivat olla joko ulkoisia (EGP) tai sisäisiä (IGP), riippuen mihin kohtaan verkkoaluetta ne on tarkoitettu. (Ballew 1998, 122) Yleisesti ottaen protokollat ovat sisäisiä, sillä on käytössä lähinnä vain yksi ulkoinen protokolla (*BGP, Border Gateway Protocol*). (Cisco CCNA2 2010)

Suosituimpia sisäisiä protokollia ovat RIP (versiot 1 ja 2), OSPF ja EIGRP. Näistä kaksi ensimmäistä perustuvat yleisiin Internet-standardeihin ja ovat helpompia ottaa käyttöön yrityksessä, jossa on monen eri valmistajan tekemiä reitittimiä. Reitittimet ymmärtävät toistensa lähettämiä viestejä ilman ongelmia. (Mika Hakala 2005, 274) EIGRP on Ciscon kehittämä oma reititysprotokolla, joka toimii ainoastaan Ciscon reitittimissä. Sitä käytetään lähinnä suurissa organisaatioissa, joissa halutaan pitää reitittimien kuormitus alhaisena. (Mika Hakala 2005, 276)

RIP ja EIGRP ovat etäisyysvektoriprotokollia. Tämä tarkoittaa sitä, että reititin laskee, kuinka monen fyysisen hyppäyksen (engl. *hop*) päässä seuraava reititin on. RIP on näistä yksinkertaisin, ja sen rajoitteena on maksimissaan 15 hyppäyksen reitti. Kaikki sen ylittävää matkaa pidetään saavuttamattomana ja tietopakettia ei viedä perille saakka. RIP pitää yllä reititystaulua, jonne se merkitsee reitittimien etäisyyden, IP-osoitteen ja aliverkkopeitteen. Reitittimien taulutiedot lähetetään joka 30:s sekunti eteenpäin. Tämä aiheuttaa ylimääräistä liikennettä verkossa ja saattaa hidastaa sitä.

EIGRP on kehittyneempi versio RIP:stä ja edellisten tietojen lisäksi se ylläpitää naapuritaulua (*neighbour table*) sekä topologiataulua. EIGRP:n maksimihyppäysmäärä on 255, joten sitä voidaan käyttää laajoissakin verkoissa helposti. Se muodostaa tiiviin yhteistyön naapurireitittimien kanssa, ja ne jakavat toisilleen tietoa reitittimistä vain, kun olennaisia muutoksia tapahtuu joissain niistä. Tästä johtuen liikennöinti verkossa ei hidastu pahasti.

OSPF on linkkitilaprotokolla. Sen logiikka on erilainen kuin kahdessa edellisessä. OSPF koostuu eri alueista, joiden sisällä olevat reitittimet keskustelevat toistensa

kanssa lähettämällä pieniä ’tervehdyksiä’ toisilleen (engl. *hello packets*) säännöllisin väliajoin. Ennen tätä reitittimet ovat hyväksyneet toisensa listoilleen ja valinneet reitittimien keskuudesta ’pääreitittimen’ (*designated router, DR*) sekä sen varmuuskopion (*backup designated router, BDR*). Pääreititin saa viestejä toisilta reitittimiltä, mikäli verkossa tapahtuu muutoksia. Tämän jälkeen se lähettää kaikille reitittimille yhtäaikaisesti tiedon muutoksista eteenpäin.

OSPF protokolla käyttää SPF-algoritmia (*Shortest Path First*) laskiessaan lyhimmän reitin. Se sijoittaa reitit topologiapuuhun, jonka juuressa (*root*) reititin itse on. Näin jokainen reititin pystyy itse vertaamaan, mikä on lyhin reitti omasta näkökulmasta määränpäähän. Hyppäysten määrä ei ole ainoa tekijä, mikä ratkaisee, vaan myös käytettävä media linkkien välillä on otettu huomioon. Tämä tekee OSPF:stä suhteellisen tarkan verrattuna muihin reititysprotokolliin.

Reitittimellä voi olla asetettuna useita protokollia kerrallaan. Jos näin tehdään, reititin valitsee lyhimmän reitin protokollan hallinnollisen etäisyyden (engl. *administrative distance, AD*) perusteella. (Cisco CCNA2 2010) Hallinnollinen etäisyys kertoo, kuinka luotettava yhteys on. Mitä pienempi numero on, sitä luotettavampi reitti on käyttää. Nämä ovat ennalta sovittuja arvoja, jotka on listattu taulukossa 1.

Protokolla	Hallinnollinen etäisyys
Suoraan kiinnitetty reitti	0
Staattinen reitti rajapinnasta	1
EIGRP	90
OSPF	110
RIP	120
Tuntematon	255

Taulukko 1. Joidenkin protokollien hallinnolliset etäisyydet

Tietoliikenneasiantuntija voi myös muuttaa reitittimessä asetuksia niin, että tietty reitti saakin suuremman etäisyysarvon kuin sen oletusetäisyysarvo. Tällä varmistetaan, että tieto reitite tään haluttua reittiä pitkin.

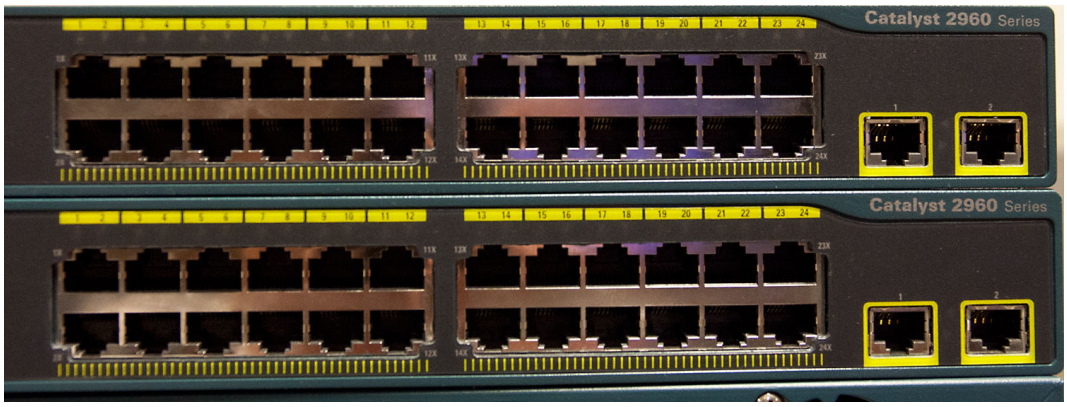
3.4.2 Reitittimen fyysinen rajapinta

Fyysisellä rajapinnalla tarkoitetaan sitä, millä tavalla reititin on liitettynä toisiin laitteisiin tai Internetiin. Sisäverkossa tapahtuva liitäntä on tehty mitä todennäköisimmin FastEthernet- tai GigabitEthernet-rajapintojen kautta. Ulkoisiin yhteyksiin käytetään sarjaliitäntää (engl. *serial port*) tai modeemi/puhelinyhteyksiä. Fyysinen rajapinta määrittelee yhteysnopeuden. Sisäverkko on yleensä nopeampi kuin ulkoinen, ainakin vielä tällä hetkellä. Sisäverkon nopeudet ovat luokkaa 10–1000 Mbps.

Kuvio 3. Reitittimen sarjaportti.

3.5 Kytkimet

Kytkin toimii OSI-kerrosmallin toisella kerroksella. Kytkimen tehtävänä on kuljettaa datapaketteja MAC-osoitteen perusteella laitteelta toiselle. Toisin kuin reititin, kytkin ei pysty siirtämään paketteja aliverkosta toiseen, sillä siihen tarvitaan IP-osoitetta. Kytkimen avulla saadaan liitettyä tietokoneet ja oheislaitteet reitittimeen kätevästi. Kytkimet ovat halvempia hankkia kuin reitittimet, joten hinta per yhteysportti on pienempi kuin reitittimessä. Sen takia kytkimiä voi olla paljon enemmän talossa kuin reitittimiä. (Ballew 1998, 58)



Kuvio 4. Kahden kytkimen portit.

Kytkimet katkaisevat myös ns. törmäysalueen (engl. *collision domain*). Jokainen kytkimeen kiinnitetty kone on oma törmäysalueensa. Törmäyksillä on väliä, sillä jos niitä sattuu paljon jossain verkon osassa, tiedon kulku hidastuu ja koneiden välinen keskustelu toimii ”tahmeasti”. (Mika Hakala 2005, 86)

Kytkimillä on myös oma osansa tietoturvan parantamisessa. Aliverkon sisälle voidaan suunnitella virtuaalinen aliverkko (VLAN), jolla voidaan estää toisen virtuaalisen aliverkon pääsy toiselle. Se toimii samalla tavoin kuin fyysinen aliverkko. (Lammle 2007, 554) Lisäksi MAC-osoitteilla voidaan määrittää, pääseekö jokin tietty laite liitetyn portin läpi verkkoon.

3.6 WLAN-tukiasema

WLAN-tukiaseman tehtävänä on lähettää langattomasti tietoa laitteelle, joka toimii langattomalla yhteydellä. Langattomia yhteyksiä on kätevä käyttää esimerkiksi kokoustiloissa tai muissa paikoissa, joissa liitettäviä koneita vaihdellaan (ulkopuoliset käyttäjät). Langattomalla yhteydellä voidaan nykypäivänä jopa korvata fyysinen yhteys, sillä yhteydet ovat kehittyneet ja nopeutuneet viime vuosina.

Tukiasema käyttää eri standardeja, joita laitteet osaavat tulkita. IEEE:n standardi 802.11 sisältää monia eri alastandardeja. Laitteen ja tukiaseman pitää ymmärtää ja käyttää samaa standardia, jotta ne voivat toimia keskenään. Monet kannettavista laitteista ymmärtävät nykyään 802.11b/g/n -standardeja. (Mika Hakala 2005, 158)

On olemassa myös muita standardeja, mutta edellä mainitut näyttävät valtaavan eniten kaistaa uusissa kannettavissa tietokoneissa.

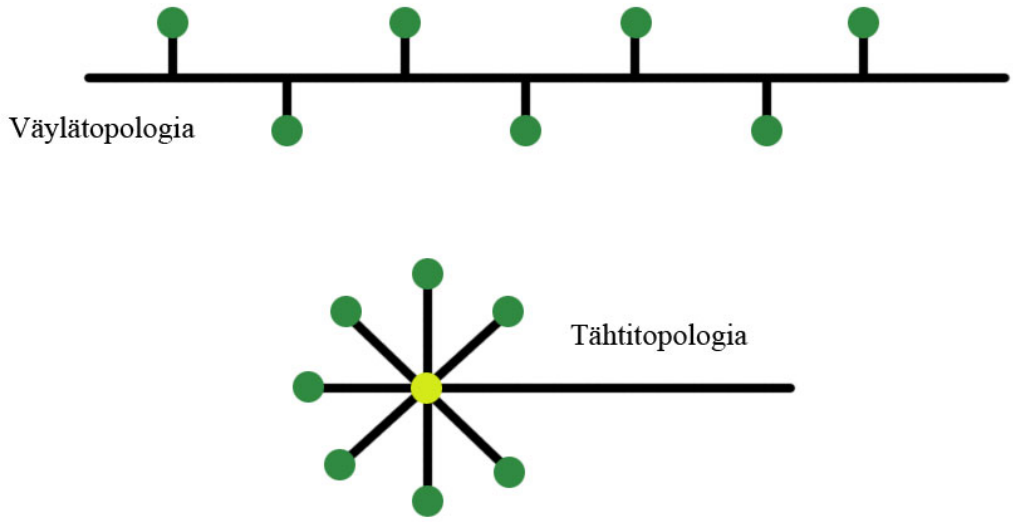
Tukiasema voi olla yksi osa reititintä tai oma laitteensa. Ominaista sille kuitenkin on sen antenni, jota kautta tietoa lähetetään parilla eri taajuusalueella. Sallittuja alueita ovat standardin mukaan joko 2,4 GHz:n tai 5 GHz:n taajuudet. (Mika Hakala 2005, 152)

3.7 Varavirtalähteet

UPS-järjestelmä on suhteellisen tärkeä laite/järjestelmä missä tahansa tietoverkko- ja ylläpitävässä organisaatiossa. UPS on lyhenne sanoista *Uninterruptile Power System* eli suomeksi katkoton tehonsyöttö. Sen päätehtävä on nimensä mukaisesti syöttää virtaa (verkko)laitteille, vaikka sähkökatko katkaisisikin päävirran poikki. Sen toisena tehtävänä on poistaa kaikki yli- tai alijännitteet virrasta, jotka saattaisivat vahingoittaa herkkiä verkkolaitteita. UPS-laitteen virransyöttökapasiteetti riittää lähinnä verkkolaitteen sammuttamiseen tarvittavan määrän virtaa. Tällä kuitenkin autetaan laitetta sammumaan hallitulla tavalla ja ongelmilta vältytään paremmin.

4 TOPOLOGIA

Topologialla tarkoitetaan sitä, miten laitteet on liitetty toisiinsa, muodostaen tietyntyyppisen verkon. Yksinkertaisimmillaan topologiasta voidaan puhua kahden koneen ollessa yhdistettynä toisiinsa johdolla. Tämä on silloin kaksipisteyhteys (engl. *point-to-point*), joka toimii myös kaikkien verkkotopologioiden perustana eri reitittimien välillä. Laajaverkko muodostuu näistä sekä monipisteyhteyksistä. Erilaisia monipisteyhteyksiä ovat mm. tähti-, väylä- ja rengastopologia. (Granlund 2007, 77) Huomattavaa kuitenkin on, että topologiat esiintyvät sekä fyysisinä että loogisina kytköksinä. Looginen topologia ottaa kantaa siihen, miten paketit liikkuvat verkossa, kun taas fyysinen on ainoastaan kiinnostunut verkoston fyysisestä rakenteesta. (Wikipedia, Verkkotopologia 2011) Edellä mainituista tähtitopologia on käytetyin fyysisen verkon rakenne ja loogisissa verkoissa on käytössä lähinnä tähti- ja väylätopologiat. (Mika Hakala 2005, 68)



Kuvio 5. Eri topologiamalleja.

Tähtitopologiasta on lisäksi olemassa pari alaluokkaa, silmuverkko sekä täysverkko (*engl. partial mesh network ja full mesh network*). Nämä liittyvät lähinnä siihen, miten reitittimet ovat liitoksissa toisiinsa fyysisesti. Näillä verkotuksilla voidaan varmistaa tiedonkulku eri reitittimien välillä, vaikka yksi reitittimistä menisi epäkuntoon, sillä aina löytyy yksi tai useampi varareitti. Näiden kahden verkon

ero toisiinsa on, että täysverkossa kaikki reitittimet ovat kiinnitettynä toisiinsa, kun taas silmuverkossa näitä yhteyksiä on vähemmän. (TechTarget 2002) Kuitenkin lopputulos on sama kummassakin: luotettavampi reititysratkaisu muihin topologioihin verrattuna.

Looginen topologia vaatii suunnittelua, jotta pakettien liikkuminen eri laitteiden välillä on sujuvaa ja virheetöntä. Virheitä sattuu esimerkiksi silloin, kun aliverkkojen osoitemaailmat menevät päällekkäin huonon suunnittelun takia. Looginen topologia vaatii tietoliikennesuunnittelijalta ammattitaitoa ja ymmärrystä eri protokollista sekä hierarkkisesta osoitemaailmasta. Aliverkkojen IP-osoitteet jakautuvat loogisesti eri koneiden välille ja niitä suunniteltaessa on otettu huomioon mahdolliset tietoturvaan liittyvät asiat. Näitä ovat esimerkiksi langattomien yhteyksien sekä tietohallintoon liittyvien verkkojen pitäminen erossa muusta verkosta osoitteiden avulla. Mitä suurempaa verkkoa ollaan suunnittelemassa, sitä suurempi syy käyttää hyvin aikaa verkon suunnitteluun. Reitittimet myös voivat kuormittua turhaan pitkistä ja monimutkaisista reititystaulukoista, mikäli reitit ykset on tehty summanmutikassa.

4.1 Tiedonsiirtoverkot

Huomattavaa on, että tiedonsiirtoverkkoihin kuuluvat Northern Cloudin tapauksessa sekä LAN eli lähiverkko että alueverkko (WAN). Lähiverkko on yleensä se alue, mikä on yhden talon sisällä. Koneet ovat fyysisesti samassa osoitteessa toistensa kanssa ja niiden välillä käytetty tekniikka on ominaista lähiverkolle. Näiden kahden verkkotyypin ero on suhteellisen selkeä: alueverkossa olevat reitittimet ovat liitettynä toisiinsa kaksipisteyhteyksillä ja lähiverkkoyhteydet puolestaan monipisteyhteyksillä. Lähiverkoissa tiedonsiirron nopeus on paljon suurempi kuin alueverkossa niiden käyttämien rajapintojen eroavaisuuksien takia.

Lähiverkkomedioita ovat mm. Ethernet, Fast Ethernet ja Gigabit Ethernet. Näiden kolmen median ero on siirtonopeudessa, muut ominaisuudet ovat enemmän tai vähemmän samanlaisia. Nopeudet ovat 10/100/1000 Mbps. Ethernet-verkoissa tieto kulkee paketteina, joita käsitellään eri tavoin OSI-mallin mukaisessa järjestyksessä. (Ballew 1998, 32–33) Ethernet on ehdottomasti suosituin verkkomedia

lähiverkoissa. IEEE on standardisoinut Ethernetiä vuosikausia ja lisää tietoa siitä saa standardista IEEE 802.3.

Alueverkkoliittymissä on käytössä kaksi eri mahdollisuutta liitännästä. Ensimmäisessä yhteys on päällä niin kauan kuin sitä tarvitaan (vrt. puhelinsoitto) ja toisessa se on kiinteästi päällä koko ajan. Jälkimmäinen on kalliimpi vaihtoehto, mutta välttämätön niille yrityksille, jotka tarvitsevat jatkuvaa yhteyttä. Se on myös tietoturvallisempi ensimmäiseen ratkaisuun verrattuna. Jos yhteys ei ole päällä jatkuvasti, on otettava huomioon mahdollinen viive, mitä tulee yhteyden avaamisesta. (Ballew 1998, 35) Jokaisen yrityksen kohdalla joutuu täten miettimään, mitkä ominaisuudet ovat tarvittavia juuri heidän tarpeilleen. Ei ole olemassa yhtä ja samaa verkotusratkaisua kaikille.

Alueverkkomedioita ovat mm. PPP, HDLC, ISDN, X.25 Frame Relay ja ATM. Käytettävä media riippuu siitä, onko kyseessä kiinteä yhteys vai tarvittaessa päällä oleva. Tässä opinnäytetyössä WAN-linkki toteutetaan näistä eriävällä tavalla, joten en paneudu sen tarkemmin näihin medioihin. Alueverkkolinkitys tehdään tässä työssä MPLS-tekniikalla, jonka päälle on vielä laitettu IP-rajapinta. Mutta tästä tarkemmin toteutusosiossa.

4.2 NAT ja PAT

NAT muodostuu sanoista *Network Address Translation* eli suomeksi verkko-osoitteen muunnos. NAT:n avulla säästetään julkisten IP-osoitteiden määrää sekä parannetaan tietoturvaa. Yrityksellä voi olla esimerkiksi muutama julkinen IP-osoite, jotka jaetaan usean eri koneen välillä. Tämä tapahtuu NAT:n kautta dynaamisesti niin, että julkinen osoite muunnetaan yksityiseksi IP-osoitteeksi ja päinvastoin. Yksityisten osoitteiden sallittu lista on listattu ns. pooliin eli varantoon, josta NAT ottaa tarvittavan määrän käyttöön ja vapauttaa ne, kun yhteyttä ei enää tarvita. (Ballew 1998, 238) Lisäksi voidaan määritellä kiinteät yksityiset osoitteet tietyille laitteille kuten FTP-palvelin tai www-palvelin, jotta yhteydenmuodostus olisi varmempaa.

PAT on NAT käytännössä, ja IP-osoitteen muunnoksen lisäksi mukaan kiinnitetään se portti, mistä paketti lähti eteenpäin ja minne porttiin se on matkalla. Näin paketista voidaan tunnistaa paremmin, minne se kuuluu.

Tietoturvan kannalta NAT:n kääntämät yksityiset osoitteet eivät näy ulkomaailmalle. Näin estetään yksittäisten laitteiden näkyminen – ja hyökkäyksen teko vaikeutuu.

5 TIETOTURVA

Tietoturva tarkoittaa luottamuksellisuutta, eheyttä ja käytettävyyttä. Luottamuksellisuus on sitä, että vain oikeutetut henkilöt pääsevät käsiksi tietoverkkoihin esimerkiksi tunnuksien ja salasanojen avulla. Eheydellä varmistetaan, että tieto ei ole muuttunut sen jälkeen, kun se on talletettu kovalevylle. Tähän liittyy sekä fyysinen tuhoutuminen/muuttuminen sekä tahallaan aiheutettu vahinko. Käytettävyydellä vuorostaan viitataan tiedon kulun käytettävyyttä: saadaanko tieto nopeasti ja vaivattomasti vai tapahtuuko matkan aikana tarpeettomia viivästyksiä. Väärin asetetut laitteet aiheuttavat tämäntyyppisiä ongelmia verkkoliikenteessä. (Mika Hakala 2005, 342)

Tietoliikenteessä on erilaisia tapoja poistaa tietoturvariskejä. Fyysiselle tasolle mentäessä on hyvä pitää verkkolaitteet sekä muut, tavalliselle käyttäjälle tarpeettomat laitteet, lukittujen ovien tai kaappien takana. Tilojen hyvästä tuuletuksesta on kuitenkin pidettävä huolta, sillä laitteet kuumenevat käytössä. Laitteisiin pääsee käsiksi vain, jos henkilöllä on tarpeelliset avaimet ja mahdolliset tunnuskoodit. Lisäksi on hyvä pitää huolta paloturvallisuudesta (pölyt pois!) sekä ottaa huomioon mahdolliset vesivahingot tms. yllättävät ongelmat, mitkä voisivat tuhota sähkölaitteita.

Seuraavissa kappaleissa on esitetty useita tietoturvallisuussuojauksia. Suojauksia voidaan asettaa niin reitittimiin kuin kytkimiinkin.

5.1 ACL

ACL on lyhenne *Access Control List* -sanoista. Suomeksi käännettynä puhutaan pääsylistoista. Pääsylistat asetetaan reitittimeen, joko sisään- tai ulosmenevään liikenteeseen. Ne liitetään aina rajapintakohtaisesti, joten listojen huolellinen suunnittelu tekee reitityksestä sujuvan. Väärin asetetut listat pahimmassa tapauksessa estävät tahdotun liikenteen kokonaan tai muuten vain hidastavat liikennettä.

Listoja on kahdenlaisia: vakio (*standard*) ja laajennettu (*extended*). Vakiolistoissa liikennettä säännellään pelkällä IP-osoitteen lähteellä (*source*). Rivien järjestyk-

sellä on merkitystä, sillä reititin käy listan läpi rivi riviltä. Kun jonkin rivin ehto ei täyty, reititin estää liikenteen asetuksen mukaisesti ja lopettaa listan käymisen läpi siihen. Vakiolista kannattaa suunnitella niin, että yksittäiset koneet määritellään ensimmäiseksi, ja sitten aliverkot, laajemmat verkot ja sen jälkeen vasta ulkopuoliset osoitteet. Tämä sen takia, että sisäverkon liikenne liikkuu mahdollisimman nopeasti eteenpäin.

Laajennetuissa listoissa liikennettä voidaan kontrolloida vielä tarkemmin. Lisäehtoja saadaan ottamalla mukaan lähde- ja kohdeosoite, protokollatyyppi (UDP, TCP, jne.), lähde- ja kohdeportit, MAC-osoitteet sekä yhteyden muodostuksen suunta. Lista suunnitellaan kirjoittamalla ensin yksittäiset portit tai protokollat, porttialueet ja lopuksi määrittelemättömät portit ja IP-liikenne.

Yhteistä kummallekin listatyypille on, että sekä lähde- että kohdeosoitteisiin lisätään ns. wildcard mask perään. Se toimii samalla tavalla kuin aliverkkopeite, mutta numerot menevät päinvastaisesti. Wildcard mask lasketaan yksinkertaisesti vähentämällä IP-osoitteen aliverkkopeite 255.255.255.255 osoitteesta ja jäljellejäävä osa on haluttu peite. (Mika Hakala 2005, 248–249) Esimerkiksi komento

```
access-list 13 deny 192.169.12.0 0.0.0.255
```

estää kaikki osoitteet, jotka tulevat aliverkosta 192.169.12.x. Kyseessä on vakiolista. Seuraavassa esimerkissä on laajennettu listatyyppi käytössä:

```
access-list 101 permit ip any any
```

Lista päästää kaiken IP-pohjaisen liikenteen läpi.

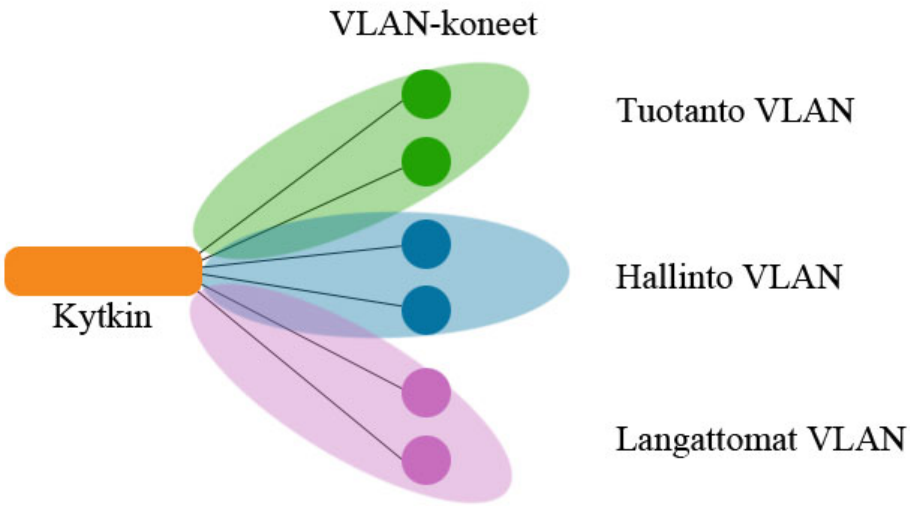
Listoille annetaan aina oma numeronsa, jolla siihen viitataan asetuksissa. Vakiolistoissa käytetään numeroita väleiltä 1–99 ja 1300–1999. Laajennetut listat toimivat numeroväleillä 100–199 ja 2000–2699. Näin riveistä voi helposti päätellä, mihin listaryhmään ne kuuluvat. Huomioitavaa on, että jokainen lista päättyy automaattisesti aina komentoon `implicit deny` ja se estää kaiken liikenteen, mitä ei ole erikseen sallittu listalla. Tämän voi poistaa lisäämällä loppuun aina `permit any` -komennon.

Olennaista listoissa on, että ne kirjoitetaan ensin reitittimelle ja sen jälkeen asetetaan haluttuun reitittimen rajapintaan. Samaa listaa voi siis käyttää monessa eri rajapinnassa. Listaa ei tarvitse erikseen poistaa, jos sen haluaa ottaa pois käytöstä yksittäisessä rajapinnassa.

Vakiolistat kannattaa asettaa mahdollisimman lähelle kohderajapintaa, jotta ne eivät vahingossa estä tarpeellista liikennettä. Laajennetut listat vuorostaan kannattaa lisätä mahdollisimman lähelle lähdettä (Cisco CCNA3 2010)

5.2 VLAN

VLAN on Virtual Local Area Network eli virtuaalinen paikallisverkko. Se vastaa täysin tavallista, fyysistä paikallisverkkoa, mutta liitännät on hoidettu virtuaalisella pohjalla. VLAN:lla pystytään tuomaan lisää tietoturvaa erottamalla verkossa liikkuvan liikenteen omille kaistoilleen, niin että ne eivät ”näe” toisiaan. (Angelescu 2010, 418) Esimerkiksi langattomat verkot on syytä pitää omana itsenäisenä VLAN-yksikkönään sen tietoturvariskin takia. Johtoportaan liikenne ei myöskään ole tavoitettavissa graafisilta koneilta, kun ne ovat omilla kaistoillaan. Kuviossa kuusi on esitelty VLAN:n idea. Kytkimeen on liitetty kuusi eri konetta, ja kolme eri VLAN-verkkoa käyttöön.



Kuvio 6. VLAN:n toimintaperiaate selitettynä kuvan keinoin.

5.3 Palomuuri

Palomuuri estää tietyntyyppisen liikenteen pääsyn sisäverkkoon riippuen asetuksista. Hyvin suunniteltu palomuuri toimii asianmukaisesti, mutta vaatii asentajalta hyvää tietoutta eri asetuksista. Asetusten ei saa olla ristiriidassa reitittimen asetuksien kanssa, jotta haluttu liikenne pääsee läpi. Palomuurit voivat olla joko fyysisiä laitteita tai ohjelmistoja.

5.4 DMZ

Aikaisemmin mainittu DMZ-alue on ns. harmaata aluetta, joka on puoliksi sisäverkossa ja puoliksi ulkoverkossa. Sen tietoturva-asetukset ovat höllemmät, jotta reititintä ei kuormiteta turhaan liikenteen ollessa suuri. DMZ-alueelle laitetaan yleensä FTP-, www- ja SMTP-palvelimet, jotka ovat aktiivisessa käytössä ulkopuolisilta koneilta. Ulkopuolelta tuleva liikenne pysähtyy DMZ-rajalla, josta matka jatkuisi muuten sisäverkkoon. Sisäverkon liikenteeseen pääsee käsiksi ainoastaan sille sallitut laitteet/yhteydet, kunhan palomuuri ja/tai pääsylistat ovat huolella suunnitellut.

5.5 WLAN

WLAN on lyhenne sanoista Wireless Local Area Network. Nimensä mukaisesti se on langaton paikallisverkko. WLAN on hyödyllinen sellaisissa paikoissa, joissa ei muutoin pystyttäisi rakentamaan fyysistä verkkoa. Haittapuolena on sen epävarmuus tietoturvan suhteen. (Mika Hakala 2005, 167) Niinpä sitä kannattaa käyttää harkitusti ja omana aliverkkonaan, jolle on asetettu tarvittavat pääsykiellot muuhun sisäverkkoon. Langattomia yhteyksiä käytetään paljon kokoustiloissa tai muissa suuremmissa huoneissa ja saleissa, joissa on paljon muuttuvia käyttäjiä. Langattomien yhteyksien tietoturva perustuu pitkälti laitteiden tunnistamiseen. Tekniikoita on muutamia erilaisia, ja käytännössä laitteet jakavat yhteisen ”avaimen”, jolla yhteys voidaan avata vain haluttujen laitteiden kesken.

5.6 VPN

VPN eli Virtual Private Network on virtuaalinen suljettu verkko. Laitteet ovat yhteydessä toisiinsa salaisen yhteyden kautta, jonne ulkopuolisella liikenteellä ei ole asiaa. Salaus voidaan tehdä kahdella tapaa: fyysisesti eristämällä liikenne omalle yhteyslinjalleen tai datan liikkuessa julkisissa linjoissa sen voi salata erilaisilla salausprotokollilla. (Wikipedia, VPN 2011)

Opinnäytetyössä on esitelty fyysinen ratkaisu, joten mitään erityisiä salausprotokollia ei tarvitse käyttää. Salausprotokollia ovat mm. IPsec ja PPTP. Näitä protokollia voivat käyttää esimerkiksi koneet, joilla otetaan etäyhteyttä johonkin toimipisteistä ja yhteys pysyy salattuna tällä tavoin.

6 TOTEUTUS

Northern Cloudin lähiverkkojen verkkoratkaisuna on käytetty tähtitopologiaa. Käytännössä se tarkoittaa sitä, että kaikki laitteet on kiinnitetty kytkimeen ja kytkin vastaavasti reitittimeen. Alueverkko on myös toteutettu tähtimäisesti, jossa eri lähiverkot rakentuvat reitittimien ympärille. Kyseessä on siis laajennettu tähtitopologia. Liitteessä 1 on esitelty topologia yksinkertaisessa muodossa. Jokaisesta käyttäjäryhmästä on otettu yksi kone hahmottamaan koko ryhmää.

6.1 Käyttäjäryhmät

Käyttäjäryhmät on jaoteltu työntekijöiden työnkuvan mukaan. Vaasan toimistolla on muita toimistoja enemmän ryhmiä. Ryhmille on annettu omat VLAN-numerot, jotka toistuvat samoina jokaisen toimipisteen alla. Tällä on haettu yhteneväisyyttä toimipisteiden asetusten kanssa niin, että niitä voidaan käyttää hyödyksi muiden toimipisteiden asennuksessa. Samat komennot toistuvat toimipisteiden lähiverkoissa, ainoastaan IP-osoitteet muuttuvat. Alla olevassa taulukossa 2 on esitelty eri ryhmät ja mihin VLAN-numeroon laitteet ovat kytketyt.

Ryhmännimi	VLAN #
Palvelimet	10
Tietokanta	11
Vieras/Guest	20
Grafiikka	30
Myynti	40
Hallinto	50

Taulukko 2. Ryhmäjaottelut ja niiden VLAN-numero toimipisteissä

Hallintoryhmän alle kuuluvat sekä talous- että johtohenkilökunta. Grafiikkaryhmään kuuluvat sekä graafikot ja videotuotannon henkilöstö että heidän tuotannossaan tarvittavat laitteet, kuten ulkoiset kovalevyt. Vaasan toimistolla on käytössä sisäverkossa palvelimille omat VLAN:t, jotta niille menevä liikenne voidaan erottaa tavallisesta sisäverkon liikenteestä.

Eri VLAN-aliverkot on otettu käyttöön lisäämään tietoturvaa. Esimerkiksi tietokantaan (VLAN 11) pääsee käsiksi vain, jos kuuluu VLAN-ryhmään 50, oli käyttäjä missä tahansa toimipisteessä. Grafiikka- ja myyntihenkilöstöillä on pääsy vain heidän omiin resursseihinsa. Hallinto pääsee kaikkiin resursseihin käsiksi. Vierasryhmä on tarkoitettu käytettäväksi kokoushuoneen langattomaan yhteyteen. Vierasryhmällä ei ole pääsyä lainkaan sisäverkon puolelle, vaan vierasverkkoon liitetyt koneet pääsevät ainoastaan näkemään toisensa ja menemään Internetiin. Reitittimiin on laitettu omat pääsylista-asetukset niin, että edellä mainitut kriteerit täyttyvät.

6.2 SMTP-palvelin

Vaasan toimipiste eroaa muista toimipisteistä siten, että sillä on DMZ-alue käytössään. Kyseiseen alueeseen on sijoitettu SMTP ja FTP/www -palvelimet. SMTP toimii tässä tapauksessa vain eteenpäin lähettävänä palvelimena eli ns. smart hostina ja lähettää viestit POP-palvelimelle. POP-palvelimelta ne lähetetään vasta käyttäjien koneille. Tällä varmistetaan myös, että viestit pysyvät sisäverkossa ulkoisen sijaan ja luvattomat eivät pääse näkemään viestejä palvelimelta. Smart host estää lähettäjän palvelimen lähettämästä suoraan vastaanottavaan palvelimeen. Tästä saadaan eri hyötyjä, mm. roskapostien määrää voidaan vähentää ja tietoturvaa kasvattaa.

Smart hostille on tehty pääsylista erikseen DMZ-alueen ja Vaasan sisäreitittimen linkkiin eli RV2, portti f0/1. Sen pääsylistakäsky reitittimellä on seuraava:

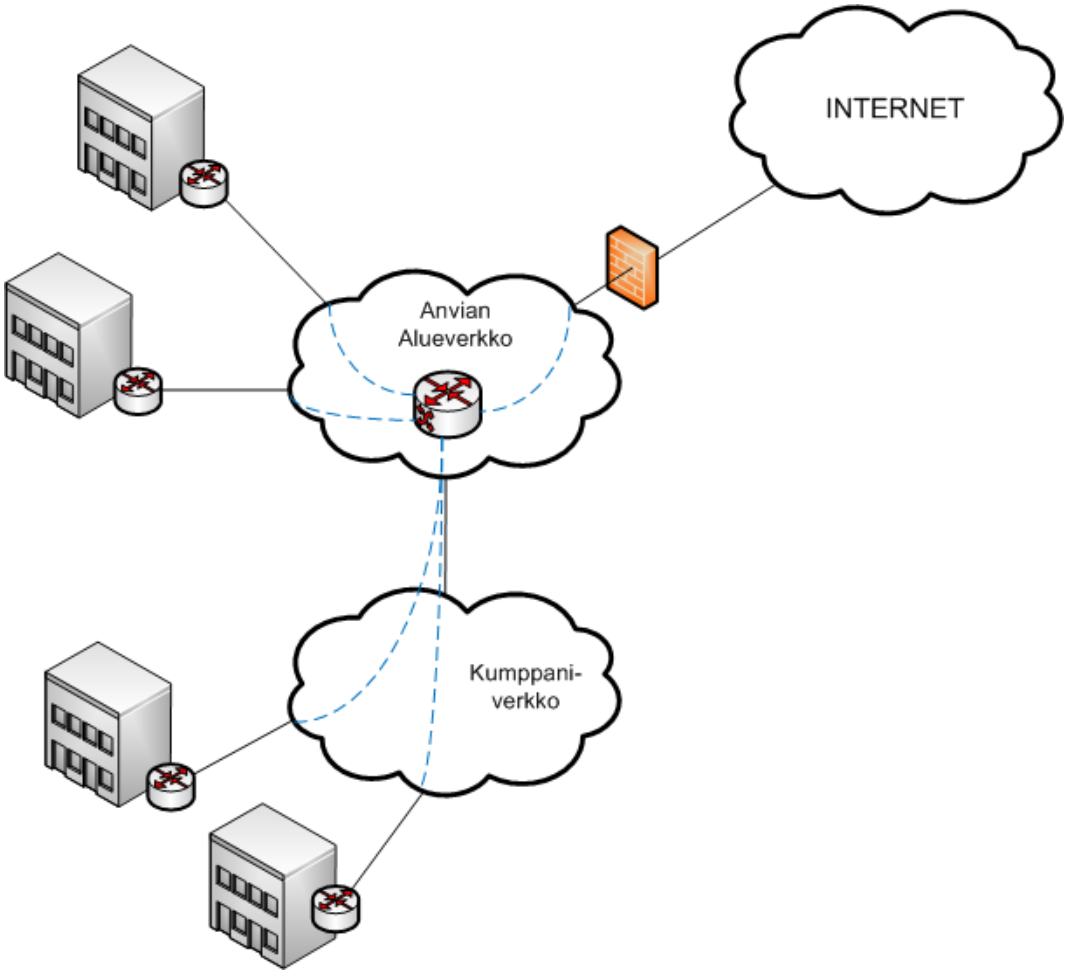
```
RV2(config)#access-list 101 permit tcp host 192.168.10.3 host
192.168.20.2 eq 25
```

6.3 Case Anvia

Anvian ratkaisuehdotuksessa virtuaalisesta yksityisverkosta perustuu Anvian runkoverkon MPLS-tekniikkaan. He kutsuvat tämän tyyppistä ratkaisua Operaattori-VPN:ksi, joka voidaan vielä jaotella VLL (Virtual Leased Line) ja VPLS (Virtual Private LAN Service) ryhmiin. VLL on näistä yksinkertaisempi. Se muodostaa kaksipisteyhteyden kahden toimipisteen välille, eikä runkoverkko ota kantaa välil-

lä kulkevaan liikenteeseen. VPLS -ratkaisu esitellään tässä työssä ja se yhdistää asiakkaan useat toimipisteet yhdeksi verkoksi. Runkoverkko sisältää oman virtuaalisen reitittimen (VRF), joka yhdistää toimipisteet omana ”jalkana” mukaan runkoverkkoon. Kuviossa 7 on esitetty tämä ratkaisu.

Toimipisteiden sijaitessa tässä tapauksessa eri kaupungeissa ei Anvian oma alueverkkokattaus saavuta muiden kuin Vaasan toimipisteen verkon. Anvian oma alueverkkonsa on rajoitettu Pohjanmaan alueelle. He käyttävät muiden kumppaniyritysten verkkoja niin kansallisesti kuin kansainvälisestikin yhdistämään toimipisteet saumattomasti toisiinsa saman virtuaalireitittimen kautta. Mainitaan vielä, että asiakkaiden päätelaitteet eli lähinnä reitittimet ovat Ciscon tuotteita. Anvia toimittaa nämä hyvän laadun takaamiseksi jokaiselle asiakkaalleen.



Kuvio 7. Yksi Anvian tarjoamista verkkoratkaisuista.

Toimipisteiden vähäisen määrän vuoksi ei dynaamisia reititysprotokollia välttämättä tarvita. Halutessa runkoverkossa käytetään OSPF- tai BGP -reititysprotokollia, mutta tässä opinnäytetyössä on keskitytty tekemään kaikki reitityksset staattisesti. Lisäksi sisäverkoissa olisi voitu käyttää RIPin versiota 2, jos näin olisi haluttu tehdä.

Asiakkaan ei myöskään tarvitse itse huolehtia palomuurisuojauksesta, vaan palomuuri sijaitsee Internetin ja VRF:n välissä. Asiakkaan lähiverkot ja virtuaalireititin ovat siis täysin Internetistä ja muista runkoverkossa olevista yrityksistä riippumattomia. Tarvittaessa myös etätyöntekijät voidaan liittää VPN-tunneleilla verkkoon, koska palomuuri on keskitetty. Internet-yhteyttä ei laiteta erikseen kiertämään jonkin toimipisteen kautta, joten kaikki toimipisteet saavat yhtä nopean yhteyden Internetiin.

Huomattavaa vielä on, että NAT-asetukset tehdään ainoastaan Internetin suuntaan, joten niitä ei tarvitse erikseen tehdä suljetulle yritysverkolle.

6.4 IP-osoitteet

Northern Cloudin IP-osoitemaailma on pidetty mahdollisimman loogisena kokonaisuutena. Toimipisteiden osoitemaailma koostuu neljästä eri aliverkosta, jotka ovat toimipisteiden ulkoisten reitittimien takana. Toimipisteiden ulkoisten reitittimien ja Anvian virtuaalireitittimen välillä on käytetty kolmea eri aliverkkoa. Lopuksi vielä yksi verkko-osoite vie liikenteen Internetiin Anvian reitittimen kautta.

Vaasan toimiston kahden reitittimen välillä (RV1 ja RV2) on käytetty IP-osoiteväli on 192.168.10.0 / 24. Vaasan sisäverkossa, eli VLAN-osoitteissa käytetään 192.168.20.0 / 24. Helsingin toimiston VLAN-osoitteet ovat väliltä 192.168.30.0 / 24 ja Tukholmassa 192.168.40.0 / 24. Anvian runkoverkon ja toimipisteiden reitityksset on tehty IP-maailmasta 94.22.64.xx / 30.

Yhdelle ryhmälle on varattu 16 osoitetta, joten aliverkkomaskina on 255.255.255.240. Jokaisesta toimipisteestä löytyy ainakin grafiikan, myynnin ja hallinnon ryhmät. Niinpä esimerkiksi ensimmäinen grafiikkaryhmään kuuluva laite saa IP-osoitteekseen 192.168.xx.34 / 28, jossa xx korvautuu kyseisen toimi-

pisteen aliverkon tunnusnumerolla (20, 30 tai 40). Tarkat IP-osoitteiden listaukset ovat liitteessä 2.

6.5 Asetukset

Tuon muutaman kohdan asetuksista esille, koska niissä on tärkeää informaatiota ymmärtämisen kannalta. Nämä voivat jäädä hyvin aloittelevalta suunnittelijalta huomaamatta.

6.5.1 VLAN-asetukset

VLANien käyttö vaatii asetusten laittamista sekä reitittimeen että kytkimeen. Kytkimessä VLAN:lle annetaan nimi ja minkä tyyppinen, *access* tai *trunk*, portti on kyseessä. Access-tyyppisessä portin kautta menee ainoastaan yhden VLAN:n liikenne. Trunk-portin kautta kulkee monen eri VLAN:n liikenne. (Angelescu 2010, 427) Alla olevassa kytkimeen kirjoitetuissa riveissä nähdään, kuinka viimeiseen f0/24 -porttiin kytkimessä on annettu trunk-käsky. Portti kiinnittyy reitittimeen RV2, ja f0/24 -portin kautta kulkevat kaikkien VLAN:ien liikenne.

```
SW01(config)#vlan 10
SW01(config-vlan)#name palvelimet
SW01(config)#interface f0/1
SW01(config-if)#switchport access vlan 10
...
SW01(config)#interface f0/24
SW01(config-if)#description trunk to router
SW01(config-if)#switchport mode trunk
```

Reitittimen osalta täytyy tehdä muutamia asetuksia. Koska reitittimen portista f0/0 on kytkös kytkimen f0/24 -porttiin, täytyy kaikki VLAN:t jollain tavalla laittaa kulkemaan saman f0/0 -portin kautta. Tämä tapahtuu asettamalla jokainen VLAN omaan aliliittymäänsä (engl. *sub-interface*). (Angelescu 2010, 440) Yleisenä käytäntönä kannattaa käyttää samaa numeroa ja nimeä kuin on käytetty VLAN:ssakin. Eli tässä tapauksessa 10 / palvelimet. Liittymälle täytyy myös antaa jokin kapselointityyppi, eli seuraavalla sivulla on esitelty *dot1q* -tyyppi ja sen jälkeen VLAN:n numero. Vasta tämän asetuksen jälkeen voidaan kirjoittaa aliliittymälle IP-osoite. Joten komentojen järjestyksellä on väliä tässä tapauksessa.

```
RV2(config)#int f0/0.10
RV2(config-subif)#description palvelimet vlan
RV2(config-subif)#encapsulation dot1q 10
RV2(config-subif)#ip addr 192.168.20.1 255.255.255.248
```

Reitittimen f0/0 -porttiin ei laiteta omaa IP-osoitetta! Tämä siksi, koska jokaisella sen aliliittymällä on oma IP-osoitteensa. Ainoa komento, joka tarvitaan laittaa suoraan f0/0 -porttiin on ”*no shutdown*”. Se avaa kaikkien aliliittymien liikenteen käyttöön yhdellä komennolla.

6.5.2 IP route -asetukset

Northern Cloudissa ei ole käytössä dynaamisia reititysprotokollia. Tämä aiheuttaa sen, että reitittimiin pitää erikseen asettaa reittejä toisiin reitittimiin. Se tehdään ip route -komennolla. Jokaisen reitittimen pitää jollain tavalla olla tietoinen, mihin se voi lähettää tulleet datapaketit eteenpäin.

Esimerkiksi Vaasan toimiston RV1-reittimen ip route -komennot ovat seuraavat:

```
RV1(config)#ip route 192.168.20.0 255.255.255.0 192.168.10.14
RV1(config)#ip route 0.0.0.0 0.0.0.0 94.22.64.2
```

Ensimmäisessä komennossa kerrotaan reitittimelle Vaasan sisäisen verkon osoite ja minkä IP-osoitteen kautta kaikki sinne tarkoitettu liikenne voidaan ohjata. Jälkimmäisellä komennolla 0.0.0.0 0.0.0.0 (engl. *quad zero*) mitkä tahansa muut määränpäät (*destination*) siirretään meneväksi ANVIA ROUTERin kautta. Olen yksinkertaisuuden vuoksi sijoittanut kaikkien aliverkkojen reititystiedot Anvian reitittimeen, jotta reititystaulukot jäävät mahdollisimman lyhyiksi muilla reitittimillä. Reititintä ei tarvitse turhaan kuormittaa monilla eri riveillä. Alhaalla vielä esiteltynä Anvian reitittimen asetukset ip route -komennoilla.

```
ANVIA_ROUTER(config)#ip route 192.168.10.0 255.255.255.0
94.22.64.1
ANVIA_ROUTER(config)#ip route 192.168.20.0 255.255.255.0
94.22.64.1
ANVIA_ROUTER(config)#ip route 192.168.30.0 255.255.255.0
94.22.64.6
ANVIA_ROUTER(config)#ip route 192.168.40.0 255.255.255.0
94.22.64.10
```

6.5.3 Pääsylista-asetukset

Northern Cloudin pääsylistoilla on kaksi eri funktiota. Niillä estetään ulkopuolisen liikenteen pääsy sisäverkkoihin. Toisaalta sisäverkoissa tapahtuva liikenne halutaan pitää hallittuna niin, että johtoportaan koneet ja tietokanta ovat eriytetty muista koneista.

Asetukset on tehty lähinnä Vaasan verkkoon ja niitä voidaan soveltaa suoraan myös muiden toimipisteiden reitittimiin. Seuraavilla komennoilla päästetään muista toimipisteistä heidän johtoportaansa näkemään sekä tietokantapalvelimen että muut johtoportaan koneet Vaasan toimistolla.

```
RV2(config)#access-list 10 permit 192.168.30.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.40.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.20.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.20.0 0.0.0.15
```

Edelliset komennot kuuluivat vakiopääsylistoihin. Reitittimeen on laitettu myös laajennettuja pääsylistoja, ja näillä pystytään tehokkaammin päästämään läpi vain tietynlainen liikenne. Viimeisimpänä riveillä on aina jokin portin numero, joka kertoo, millainen liikenne on sallittua.

```
RV2(config)#access-list 120 permit tcp 192.168.20.16 0.0.0.15
206.66.1.0 0.0.0.3 eq 80
RV2(config)#access-list 120 permit tcp 192.168.20.16 0.0.0.15
206.66.1.0 0.0.0.3 eq 443
```

Yllä olevilla riveillä estetään kaikki liikenne vierasryhmän aliverkosta muualle Vaasan sisäverkkoon. Koneet pääsevät ainoastaan Internetiin verkon kautta ja sielläkin he saavat katsoa vain http- ja https-protokolliin perustuvia sivustoja.

```
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any
eq 80
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any
eq 443
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any
eq 25
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any
eq 21
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any
eq 20
```

```
RV2(config)#access-list 101 permit tcp any 192.168.20.0 0.0.0.255
established
```

Viimeinen rivi on muista erilainen ja lopussa oleva ”established” päästää vain sellaisen liikenteen Vaasan sisäverkkoon, mikä on saanut alkunsa sisäverkosta. Jos kutsua ei ole lähetetty sisäverkosta, datapaketit pudotetaan pois käytöstä. Nämä asetukset voidaan laittaa muihin sisäverkkoihin ja ne käyttäytyvät samalla tavoin.

Jotta pääsylistat toimisivat, täytyy ne sijoittaa oikeaan rajapintaan ja oikeansuuntaiseen liikenteeseen. Liitteessä kaksi olevista reititinasetuksista näet tarkasti, miten ne on ajateltu Northern Cloud:n tapauksessa. Esimerkiksi aikaisemmin mainittu laajennettu pääsylista 120 on sijoitettu reitittimen RV2 rajapintaan f0/0.20 ja siitä reitittimen sisäänpäin menevään liikenteeseen. Näin saadaan kaikki vierasryhmästä tulevat yhteydenotot heti käsittelyyn ja poistettua asiattomat yhteysyritykset Internetiin tai sisäverkkoon. Alhaalla ote kyseisistä komennoista:

```
RV2(config)#int f0/0.20
RV2(config-subif)#ip access-group 120 in
```

6.5.4 Muut asetukset

Muita mainitsemisen arvoisia asetuksia ovat kytkimissä olevat käyttämättömät portit. Niille kannattaa antaa komento ”*shutdown*”, jotta ne pysyvät käyttämättöminä ja niistä ei ole pääsyä verkkoon turhaan. Komento lisää tietoturvallisuutta.

Tietoturvallisuutta lisäävät myös salatut salasanat kytkimiin sekä reitittimiin. Asiattomien ei tarvitse päästä käsiksi minkään laitteen asetuksiin!

6.6 Testaus

Koko yrityksen toimipisteet ja niiden välillä olevat reitittimet on testattu virtuaalisesti käyttäen Ciscon Packet Tracer -ohjelmaa. PT:lla voidaan luoda monimutkaisiakin verkkoratkaisuja testausympäristöön. Testauksesta saatuja tietoja voidaan hyödyntää, ennen kuin itse fyysinen verkko rakennetaan.

Suunnittelutyössä PT:sta on paljon hyötyä. Suunnittelijan ei tarvitse yhdistellä johtoja laitteisiin ja taas purkaa niitä. Laitteita on käytössä käytännössä rajaton

määrä, joten ohjelma sopii niin pienten kuin laajempienkin verkkojen suunnitteluun. Erityisen hyödyllinen PT on pääsylistojen suunnittelussa, sillä ne ovat yksi tärkeimmistä asetuksista, jotka on hyvä testata tarkasti.

Testasin eri koneiden välillä olevia yhteyksiä ilman pääsylistoja ja pääsylistojen kanssa niin, että ne vastaavat haluttuja määrittelyjä.

6.7 Ongelmat matkan varrella

Suurin ongelma koko työssä oli loppujen lopuksi eri pääsylistojen suunnittelu. Jouduin miettimään hetken, millä logiikalla ne kannattaa tehdä. Pääsylistat ovatkin hankalia, sillä on helppo laittaa ne väärään rajapintaan päälle tai ajatella väärin, mihin suuntaan liikenne pitäisi estää. Pääsylistojen suunnittelemisessa opin paljon uusia asioita, jotka olivat ennen olleet enemmän tai vähemmän hämärän peitossa. Ciscon CCNA-materiaaleissa oli hyvin kerrottu, kuinka liikenteen suunnan voi helposti ajatella reitittimen kautta. Jos liikenne suuntautuu rajapinnasta ja reitittimestä ulospäin, on asetuksiin laitettava ”*out*” kuvaamaan suuntaa. Päinvastaisessa tapauksessa kirjoitat ”*in*”.

Aluksi verkon suunnittelukokonaisuuden hahmotus oli vaikeaa, koska en ollut aikaisemmin tehnyt vastaavanlaisia verkkosuunnitelmia. Anvialta tulleita tietoja pystyin soveltamaan niin, että ratkaisussani oli otettu mukaan vielä DMZ-alue. DMZ-alueen ymmärtäminen vei myös hetken aikaa sisäistää.

Muita ongelmia, jotka eivät suoraan koske tämänhetkistä tilannetta, mutta tulisivat vastaan yrityksen laajentaessa toimintaa: 16 osoitteen VLAN-aliverkko per ryhmä on liian pieni osoitemäärä. Olisin voinut heti ottaa vaikka 64 osoitteen aliverkon ja pitää verkon mahdollisimman valmiina sen laajentuessa. Pahimmassa tapauksessa aliverkot täytyisi suunnitella uudestaan, mikäli kaikki 16 osoitetta tulevat käyttöön jossain ryhmässä.

6.8 Dokumentointi

Kaikkien toimipisteiden ja laitteiden IP-osoitteet on dokumentoitu Excel-tiedostoon. Laitoin ne mukaan liitteeseen 3. Jos halutaan olla vielä tarkempia do-

kumentoinnin kanssa, laitteiden MAC-osoitteet voidaan laittaa vielä yhteen sarakkeeseen mukaan. Niistä on apua esimerkiksi kytkinten kanssa, joihin jää sitä kautta menneiden laitteiden MAC-osoitteet. Kytkimiin voidaan myös laittaa estot kaikille muille MAC-osoitteille paitsi juuri halutulle laitteelle.

Dokumentointi on tärkeää, sillä tulevaisuudessa on helpompi tarkastella verkon rakennetta, kun siitä on kerran tehty kunnon dokumentointi. Sitä voi verrata esimerkiksi rakennusten piirustuksiin, josta käy ilmi kaikki tarvittavat tiedot. Dokumenttia täytyy muistaa päivittää joka kerta, kun verkkoon tehdään muutoksia.

Dokumentointitapoja on monenlaisia, Anvialla he käyttävät Microsoft Visiolla tehtyä pohjaa dokumentointiin. Pääasia kuitenkin on, että tieto on talletettu jonnekin ja tietoliikennevastaavan ei tarvitse kirjautua jokaiselle reitittimelle erikseen löytääkseen haluamansa informaation.

7 JOHTOPÄÄTÖKSET

Aihe oli mielestäni sopivan haastava tämän tasoiseen koulutukseen, ottaen huomioon sen määrän tunteja, mitä olen käyttänyt Ciscon CCNA-kurssien suorittamiseen. Käytännön työllä vasta nähdään, onko opittu asia mennyt perille ja joutuu miettimään, mitä on tekemässä ja miksi. Olennaisia asioita, jotka täytyy ymmärtää, ovat aliverkkojen rakenne ja miten saat ne tehtyä, että reititys toimii halutulla tavalla.

Verkko on suurimmaksi osaksi mahdollista suunnitella ja testata Packet Tracer -ohjelman kautta. Mielenkiintoista olisi ollut olla mukana aidossa ympäristössä ja nähdä myös muita mahdollisia komentoja, joita reitittimiin joudutaan laittamaan. CCNA-kursseilla kuitenkin käydään läpi vain yksinkertaisemmat asetukset, joita tarvitaan perusasetuksiksi. Tältä osin siis en pystynyt saamaan täydellistä kokonaiskuvaa projektista loppuun asti vietynä.

Monet näistä käymistäni asioista ovat palveluntarjoajien puolesta hyvin pitkälti standardisoidut niin, ettei mikään olennainen asia jää heiltä huomaamatta suunnittelutyössä. Itselleni ainakin jäi hyvä mielikuva niistä kaikista asioista, joita pohdiskelin työtä tehdessäni. Tästä on hyvä jatkaa eteenpäin muilla Ciscon materiaaleilla tulevaisuudessa.

LÄHTEET

Angelescu, Silviu. *CCNA Certification all-in-one for Dummies.* Hoboken, NJ: Wiley Publishing, Inc., 2010.

Anvia. *Virtuaalipalvelimet.* 2011. http://www.anvia.fi/fi-FI/Yrityksille/tietotekniikka/palvelinratkaisut/Sivut/Virtuaalipalvelimet.aspx (haettu 14. marraskuuta 2011).

Ballew, Scott M. *IP-verkkojen hallinta.* Vuosik. 1. painos. Jyväskylä: Suomen ATK-kustannus Oy, 1998.

Cisco CCNA2. *Routers and Routing Basics, Chapter 6.* 2010.

Cisco CCNA3. *Switching Basics and Intermediate Routing, Chapter 8.* 2010.

Granlund, Kaj. *Tietoliikenne.* Vuosik. 1. painos. Porvoo: Docendo, 2007.

Lammle, Todd. *CCNA Study Guide.* Indianapolis: Wiley Publishing, Inc., 2007.

Mika Hakala, Mika Vainio. *Tietoverkon rakentaminen.* Vuosik. 1. painos. Porvoo: Docendo, 2005.

Salonen, Kimmo. ”Toimipisteiden välisen VPN-toteutuksen suunnittelu.” *Tutkintotyöraportti.* Tampere: Tampereen AMK, 2005.

Seppänen, Jari. *Lähiverkon vaatimusmäärittely ja toteutusehdotus kunnostettavassa toimitilassa, Case Tuomarilan VPK.* Laurea Leppävaara, 2009.

TechTarget. *What is mesh network?* 2002. http://searchnetworking.techtarget.com/definition/mesh-network (haettu 10. maaliskuuta 2011).

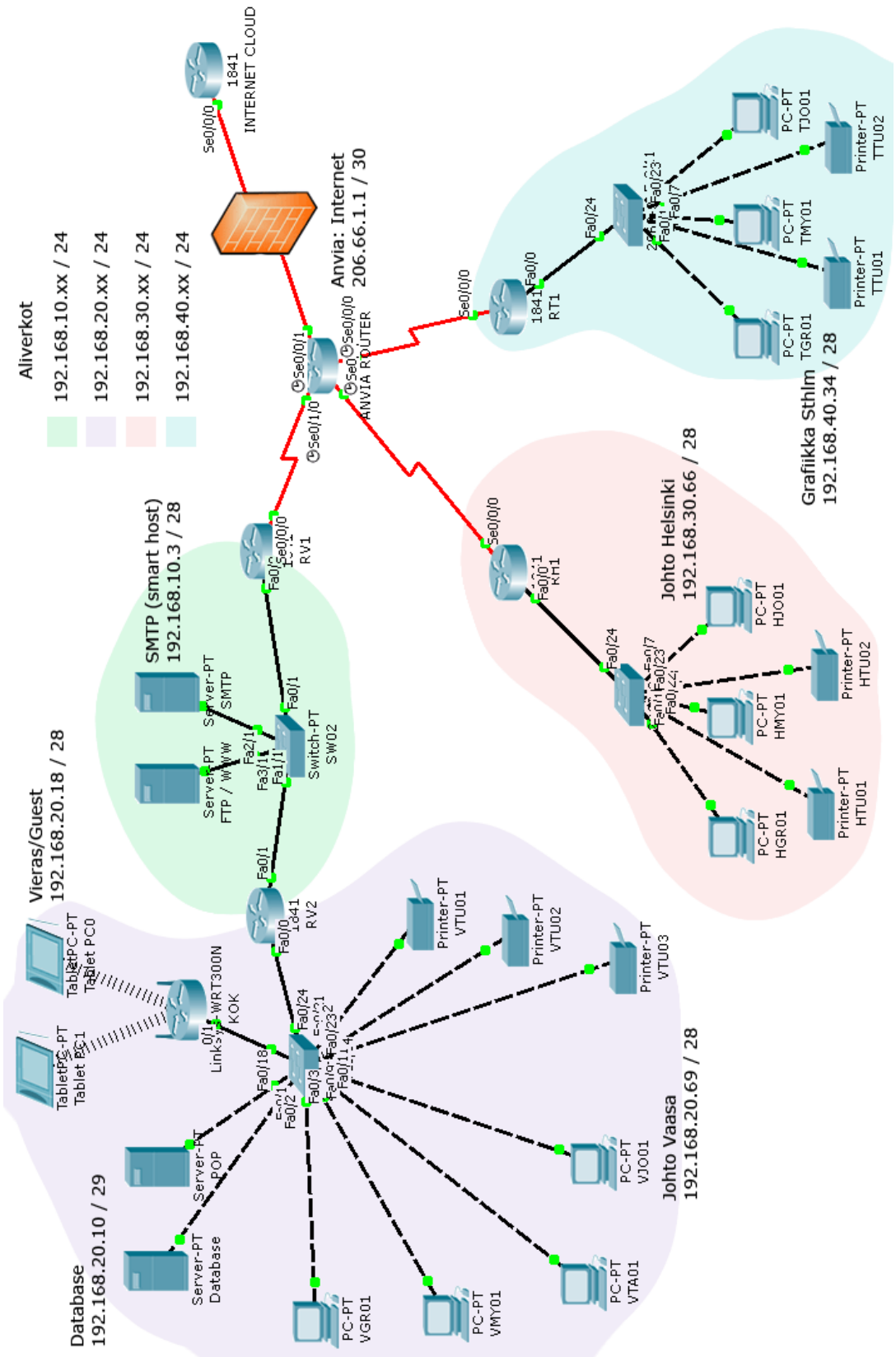
Wikipedia. *Palvelin.* 2011. http://fi.wikipedia.org/wiki/Palvelin (haettu 11. huhtikuuta 2011).

Wikipedia. *TCP/IP.* 2011. http://fi.wikipedia.org/wiki/TCP/IP (haettu 13. huhtikuuta 2011).

Wikipedia. *Verkkotopologia.* 2011. http://fi.wikipedia.org/wiki/Verkkotopologia (haettu 27. helmikuuta 2011).

Wikipedia. *VPN.* 2011. http://fi.wikipedia.org/wiki/VPN (haettu 24. lokakuuta 2011).

Northern Cloud:n verkkotopologia.



Reitittimiin tehdyt komentosarjat:

#####VAASA RV1 (ulkoinen)#####

```
RV1(config)#int s0/0/0
RV1(config-if)#des route to ISP
RV1(config-if)#ip addr 94.22.64.1 255.255.255.252
RV1(config-if)#no shut

RV1(config)#int f0/0
RV1(config-if)#des route to DMZ
RV1(config-if)#ip addr 192.168.10.1 255.255.255.240
RV1(config-if)#no shut

RV1(config)#ip route 192.168.20.0 255.255.255.0 192.168.10.14
RV1(config)#ip route 0.0.0.0 0.0.0.0 94.22.64.2
```

#####VAASA RV2 (sisäinen)#####

```
RV2(config)#int f0/1
RV2(config-if)#ip addr 192.168.10.14 255.255.255.240
RV2(config-if)#no shut
RV2(config-if)#des route to DMZ

RV2(config)#int f0/0
RV2(config-if)#des route to LAN
RV2(config-if)#no shut

RV2(config)#int f0/0.10
RV2(config-subif)#des palvelimet vlan
RV2(config-subif)#encap dot1q 10
RV2(config-subif)#ip addr 192.168.20.1 255.255.255.248

RV2(config)#int f0/0.11
RV2(config-subif)#des database vlan
RV2(config-subif)#encap dot1q 10
RV2(config-subif)#ip addr 192.168.20.9 255.255.255.248

RV2(config)#int f0/0.20
RV2(config-subif)#des kokous vlan
RV2(config-subif)#encap dot1q 20
RV2(config-subif)#ip addr 192.168.20.29 255.255.255.240

RV2(config)#int f0/0.30
RV2(config-subif)#des grafiikka vlan
RV2(config-subif)#encap dot1q 30
RV2(config-subif)#ip addr 192.168.20.33 255.255.255.240
```

```
RV2(config)#int f0/0.40
RV2(config-subif)#des myynti vlan
RV2(config-subif)#encap dot1q 40
RV2(config-subif)#ip addr 192.168.20.49 255.255.255.240

RV2(config)#int f0/0.50
RV2(config-subif)#des hallinto vlan
RV2(config-subif)#encap dot1q 50
RV2(config-subif)#ip addr 192.168.20.65 255.255.255.240

RV2(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1

RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any eq 80
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any eq 443
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any eq 25
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any eq 21
RV2(config)#access-list 111 permit tcp 192.168.20.0 0.0.0.255 any eq 20
RV2(config)#access-list 101 permit tcp any 192.168.20.0 0.0.0.255 established
RV2(config)#access-list 101 permit tcp host 192.168.10.3 host 192.168.20.2 eq
25
RV2(config)#access-list 120 permit tcp 192.168.20.16 0.0.0.15 206.66.1.0 0.0.0.3
eq 80
RV2(config)#access-list 120 permit tcp 192.168.20.16 0.0.0.15 206.66.1.0 0.0.0.3
eq 443

RV2(config)#access-list 10 permit 192.168.30.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.40.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.20.64 0.0.0.15
RV2(config)#access-list 10 permit 192.168.20.0 0.0.0.15

RV2(config)#int f0/0.50
RV2(config-subif)#ip access-group 10 out
RV2(config)#int f0/0.11
RV2(config-subif)#ip access-group 10 out
RV2(config)#int f0/0.20
RV2(config-subif)#ip access-group 120 in
RV2(config)#int f0/0.30
RV2(config-subif)#ip access-group 111 in
RV2(config)#int f0/0.40
RV2(config-subif)#ip access-group 111 in
RV2(config)#int f0/0.50
RV2(config-subif)#ip access-group 111 in
RV2(config)#int f0/1
RV2(config-if)#ip access-group 101 in
```

#####HELSINKI#####

Router(config)#host RH1

RH1(config)#int f0/0
RH1(config-if)#des route to LAN
RH1(config-if)#no shut

RH1(config)#int f0/0.30
RH1(config-subif)#des grafiikka vlan
RH1(config-subif)#encap dot1q 30
RH1(config-subif)#ip addr 192.168.30.33 255.255.255.240

RH1(config)#int f0/0.40
RH1(config-subif)#des myynti vlan
RH1(config-subif)#encap dot1q 40
RH1(config-subif)#ip addr 192.168.30.49 255.255.255.240

RH1(config)#int f0/0.50
RH1(config-subif)#des hallinto vlan
RH1(config-subif)#encap dot1q 50
RH1(config-subif)#ip addr 192.168.30.65 255.255.255.240

RH1(config-if)#int s0/0/0
RH1(config-if)#des route to ISP
RH1(config-if)#ip addr 94.22.64.6 255.255.255.252
RH1(config-if)#no shut

RH1(config)#ip route 0.0.0.0 0.0.0.0 94.22.64.5

#####STOCKHOLM#####

Router(config)#host RT1

RT1(config)#int f0/0
RT1(config-if)#des interface LAN
RT1(config-if)#no shut

RT1(config-if)#int f0/0.30
RT1(config-subif)#des grafiikka vlan
RT1(config-subif)#encap dot1q 30
RT1(config-subif)#ip addr 192.168.40.33 255.255.255.240

RT1(config)#int f0/0.40
RT1(config-subif)#des myynti vlan
RT1(config-subif)#encap dot1q 40
RT1(config-subif)#ip addr 192.168.40.49 255.255.255.240

```
RT1(config)#int f0/0.50
RT1(config-subif)#des hallinto vlan
RT1(config-subif)#encap dot1q 50
RT1(config-subif)#ip addr 192.168.40.65 255.255.255.240

RT1(config)#int s0/0/0
RT1(config-if)#des route to ISP
RT1(config-if)#ip addr 94.22.64.10 255.255.255.252
RT1(config-if)#no shut

RT1(config)#ip route 0.0.0.0 0.0.0.0 94.22.64.9


#####ISP router#####

Router(config)#host ANVIA_ROUTER

ANVIA_ROUTER(config)#int s0/1/0
ANVIA_ROUTER(config-if)#ip addr 94.22.64.2 255.255.255.252
ANVIA_ROUTER(config-if)#no shut
ANVIA_ROUTER(config-if)#clock rate 64000
ANVIA_ROUTER(config-if)#des route to vaasa HQ

ANVIA_ROUTER(config)#int s0/1/1
ANVIA_ROUTER(config-if)#ip addr 94.22.64.5 255.255.255.252
ANVIA_ROUTER(config-if)#no shut
ANVIA_ROUTER(config-if)#clock rate 64000
ANVIA_ROUTER(config-if)#des route to helsinki HQ

ANVIA_ROUTER(config-if)#int s0/0/0
ANVIA_ROUTER(config-if)#ip addr 94.22.64.9 255.255.255.252
ANVIA_ROUTER(config-if)#no shut
ANVIA_ROUTER(config-if)#clock rate 64000
ANVIA_ROUTER(config-if)#des route to stockholm HQ

ANVIA_ROUTER(config-if)#int s0/0/1
ANVIA_ROUTER(config-if)#ip addr 206.66.1.1 255.255.255.252
ANVIA_ROUTER(config-if)#no shut
ANVIA_ROUTER(config-if)#clock rate 64000
ANVIA_ROUTER(config-if)#des route to internet

ANVIA_ROUTER(config)#ip route 192.168.10.0 255.255.255.0 94.22.64.1
ANVIA_ROUTER(config)#ip route 192.168.20.0 255.255.255.0 94.22.64.1
ANVIA_ROUTER(config)#ip route 192.168.30.0 255.255.255.0 94.22.64.6
ANVIA_ROUTER(config)#ip route 192.168.40.0 255.255.255.0 94.22.64.10
```

#####SWITCH 01 (Vaasa)#####

```
Switch(config)#host SW01
SW01(config)#vlan 10
SW01(config-vlan)#name palvelimet
SW01(config-vlan)#vlan 11
SW01(config-vlan)#name database
SW01(config-vlan)#vlan 20
SW01(config-vlan)#name kokous
SW01(config-vlan)#vlan 30
SW01(config-vlan)#name grafiikka
SW01(config-vlan)#vlan 40
SW01(config-vlan)#name myynti
SW01(config-vlan)#vlan 50
SW01(config-vlan)#name hallinto
SW01(config-vlan)#exit

SW01(config)#int f0/1
SW01(config-if)#switchport access vlan 10

SW01(config)#int f0/2
SW01(config-if)#switchport access vlan 11

SW01(config)#int range f0/3 - 8
SW01(config-if-range)#switchport access vlan 30

SW01(config)#int range f0/9 - 10
SW01(config-if-range)#switchport access vlan 40

SW01(config)#int range f0/11 - 15
SW01(config-if-range)#switchport access vlan 50

SW01(config)#int f0/18
SW01(config-if)#switchport access vlan 20

SW01(config)#int range f0/19 - 21
SW01(config-if-range)#switchport access vlan 30

SW01(config)#int f0/22
SW01(config-if)#switchport access vlan 40

SW01(config)#int f0/23
SW01(config-if)#switchport access vlan 50

SW01(config)#int f0/24
SW01(config-if)#des trunk to router
SW01(config-if)#switchport mode trunk
```

```
SW01(config)#int range f0/16 - 17
SW01(config-if)#shut
SW01(config)#int range g1/1 - 2
SW01(config-if-range)#shut
```

#####SWITCH 03 (Helsinki)#####

```
Switch(config)#host SW03

SW03(config)#vlan 30
SW03(config-vlan)#name grafiikka
SW03(config-vlan)#vlan 40
SW03(config-vlan)#name myynti
SW03(config-vlan)#vlan 50
SW03(config-vlan)#name hallinto

SW03(config)#int range f0/1 - 2
SW03(config-if-range)#switchport access vlan 30

SW03(config)#int range f0/3 - 6
SW03(config-if-range)#switchport access vlan 40

SW03(config)#int range f0/7 - 8
SW03(config-if-range)#switchport access vlan 50

SW03(config)#int f0/21
SW03(config-if)#switchport access vlan 30

SW03(config)#int f0/22
SW03(config-if)#switchport access vlan 30

SW03(config)#int f0/23
SW03(config-if)#switchport access vlan 40

SW03(config)#int f0/24
SW03(config-if)#des trunk to router
SW03(config-if)#switchport mode trunk

SW03(config)#int range f0/9 - 20
SW03(config-if-range)#shutdown
```

#####SWITCH 04 (Stockholm)#####

Switch(config)#host SW04

SW04(config)#vlan 30
SW04(config-vlan)#name grafiikka
SW04(config-vlan)#vlan 40
SW04(config-vlan)#name myynti
SW04(config-vlan)#vlan 50
SW04(config-vlan)#name hallinto

SW04(config)#int range f0/1 - 6
SW04(config-if-range)#switchport access vlan 30

SW04(config)#int range f0/7 - 10
SW04(config-if-range)#switchport access vlan 40

SW04(config)#int range f0/11 - 12
SW04(config-if-range)#switchport access vlan 50

SW04(config)#int range f0/18 - 22
SW04(config-if-range)#switchport access vlan 30

SW04(config)#int f0/17
SW04(config-if)#switchport access vlan 40

SW04(config)#int f0/23
SW04(config-if)#switchport access vlan 40

SW04(config)#int f0/24
SW04(config-if)#des trunk to router
SW04(config-if)#switchport mode trunk

SW04(config)#int range f0/13 - 16
SW04(config-if-range)#shut

Dokumentoidut tiedot eri laitteista:

Vaasa

Kytkin	**SW01**			VLAN
fa0/1	CL01	POP server	192.168.20.2 / 29	10
fa0/2	CL02	Database server	192.168.20.10 / 29	11
fa0/3	VGR01	Grafiikka / mac01	192.168.20.34 / 28	30
fa0/4	VGR02	Grafiikka / mac02	192.168.20.35 / 28	30
fa0/5	VGR03	Grafiikka / mac03	192.168.20.36 / 28	30
fa0/6	VGR04	Grafiikka / pc01	192.168.20.37 / 28	30
fa0/7	VGR05	Grafiikka / pc02	192.168.20.38 / 28	30
fa0/8	VGR06	Grafiikka / pc03	192.168.20.39 / 28	30
fa0/9	VMY01	Myynti	192.168.20.50 / 28	40
fa0/10	VMY02	Myynti	192.168.20.51 / 28	40
fa0/11	VTA01	Talous	192.168.20.66 / 28	50
fa0/12	VTA02	Talous	192.168.20.67 / 28	50
fa0/13	VTA03	Talous	192.168.20.68 / 28	50
fa0/14	VJO01	Johto	192.168.20.69 / 28	50
fa0/15	VJO02	Johto	192.168.20.70 / 28	50
fa0/16	-			
fa0/17	-			
fa0/18	KOK	Langaton reititin	192.168.20.28 / 28	20
fa0/19	VHD01	Ulkoinen kovalevy	192.168.20.40 / 28	30
fa0/20	VHD02	Ulkoinen kovalevy	192.168.20.41 / 28	30
fa0/21	VTU01	Tulostin / Grafiikka	192.168.20.46 / 28	30
fa0/22	VTU02	Tulostin / Myynti	192.168.20.62 / 28	40
fa0/23	VTU03	Tulostin / Hallinto	192.168.20.78 / 28	50
fa0/24	x	Linkki kytkimeen RV2		

Helsinki

Kytkin	**SW03**			VLAN
fa0/1	HGR01	Grafiikka	192.168.30.34 / 28	30
fa0/2	HGR02	Grafiikka	192.168.30.35 / 28	30
fa0/3	HMY01	Myynti	192.168.30.50 / 28	40
fa0/4	HMY02	Myynti	192.168.30.51 / 28	40
fa0/5	HMY03	Myynti	192.168.30.52 / 28	40
fa0/6	HMY04	Myynti	192.168.30.53 / 28	40
fa0/7	HJO01	Johto	192.168.30.66 / 28	50
fa0/8	HJO02	Johto	192.168.30.67 / 28	50
fa0/9	-			
fa0/10	-			
fa0/11	-			

fa0/12	-			
fa0/13	-			
fa0/14	-			
fa0/15	-			
fa0/16	-			
fa0/17	-			
fa0/18	-			
fa0/19	-			
fa0/20	-			
fa0/21	HHD01	Ulkoinen kovalevy	192.168.30.46 / 28	30
fa0/22	HTU01	Tulostin / Grafiikka	192.168.30.45 / 28	30
fa0/23	HTU02	Tulostin / Johto + Myynti	192.168.30.62 / 28	40
fa0/24	x	Linkki kytkimeen RH1		

Tukholma

Kytkin	**SW04**			VLAN
fa0/1	TGR01	Grafiikka	192.168.40.34 / 28	30
fa0/2	TGR02	Grafiikka	192.168.40.35 / 28	30
fa0/3	TGR03	Grafiikka	192.168.40.36 / 28	30
fa0/4	TGR04	Grafiikka	192.168.40.37 / 28	30
fa0/5	TGR05	Grafiikka	192.168.40.38 / 28	30
fa0/6	TGR06	Grafiikka	192.168.40.39 / 28	30
fa0/7	TMY01	Myynti	192.168.40.50 / 28	40
fa0/8	TMY02	Myynti	192.168.40.51 / 28	40
fa0/9	TMY03	Myynti	192.168.40.52 / 28	40
fa0/10	TMY04	Myynti	192.168.40.53 / 28	40
fa0/11	TJO01	Johto	192.168.40.66 / 28	50
fa0/12	TJO02	Johto	192.168.40.67 / 28	50
fa0/13	-			
fa0/14	-			
fa0/15	-			
fa0/16	-			
fa0/17	TKK01	Kopiokone (IP)	192.168.40.61 / 28	40
fa0/18	THD01	Ulkoinen kovalevy	192.168.40.43 / 28	30
fa0/19	THD02	Ulkoinen kovalevy	192.168.40.44 / 28	30
fa0/20	THD03	Ulkoinen kovalevy	192.168.40.45 / 28	30
fa0/21	THD04	Ulkoinen kovalevy	192.168.40.46 / 28	30
fa0/22	TTU01	Tulostin / Grafiikka	192.168.40.42 / 28	30
fa0/23	TTU02	Tulostin / Johto + Myynti	192.168.40.62 / 28	40
fa0/24	x	Linkki kytkimeen RT1		

Reititin	**RV2**	**Sisäreititin Vaasa**
fa0/0.10	192.168.20.1 / 28	
fa0/0.20	192.168.20.17 / 28	
fa0/0.30	192.168.20.33 / 28	
fa0/0.40	192.168.20.49 / 28	
fa0/0.50	192.168.20.65 / 28	
fa0/1	192.168.10.14 / 28	
Reititin	**RV1**	**Ulkoreititin Vaasa**
fa0/0	192.168.10.1 / 28	
s0/0/0	94.22.64.1 / 30	
Reititin	**RH1**	**Helsinki**
fa0/0.30	192.168.30.33 / 28	
fa0/0.40	192.168.30.49 / 28	
fa0/0.50	192.168.30.65 / 28	
s0/0/0	94.22.64.6 / 30	
Reititin	**RT1**	**Tukholma**
fa0/0.30	192.168.40.33 / 28	
fa0/0.40	192.168.40.49 / 28	
fa0/0.50	192.168.40.65 / 28	
s0/0/0	94.22.64.10 / 30	

Reititin	**ANVIA**	
s0/1/0	94.22.64.2 / 30	Vaasaan
s0/1/1	94.22.64.5 / 30	Helsinkiin
s0/0/0	94.22.64.9 / 30	Tukholmaan
s0/0/1	206.66.1.1 / 30	Internetiin

Palvelin FTP&WWW	192.168.10.4 / 28
Palvelin SMTP	192.168.10.3/ 28
Palvelin POP	192.168.20.2 / 29
Palvelin Tietokanta	192.168.20.10 / 29