TIETOLIIKENNEVERKON VIKASIETOISUUS

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäen yksikkö, kevät 2015

Ilkka Mäkinen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Tietotekniikka
Tietoliikennetekniikka

Tekijä Ilkka Mäkinen **Vuosi** 2015

Työn nimi Tietoliikenneverkon vikasietoisuus

TIIVISTELMÄ

Teos sai alkunsa henkilökohtaisen kiinnostuksen sekä työelämän haasteiden kautta. Työssä syvennytään verkon toiminnan varmentamiseen, koska sen on voinut käytännössä havaita olevan yksi tärkeimmistä asioista kriittisten tietoliikenneyhteyksien kohdalla. Työn tarkoituksena on toteuttaa suunnittelemani verkkoratkaisu, jossa tutkitaan kahdennetun Internet-yhteyden toimintaa. Toteutus tapahtuu virtuaalisesti sekä tietoliikennelaboratoriossa.

Teoksen alkupuolella perehdytään verkkotekniikkaan sekä siihen liittyviin laitteisiin ja palveluihin. Lisäksi alussa luodaan katsaus verkon toimintaan ja sen keskeisiin käsitteisiin. Työn keskeisimpänä asiana pidetään verkon vikasietoisuutta. Opinnäytetyö koostuu Ciscon sertifikaattioppaiden sekä oman tietotaidon pohjalta luotuun kokonaisuuteen.

Lopputuloksena suunnittelemani verkko saadaan toimimaan halutulla tavalla ja näin ollen syntyy kahdennettu yhteys päätelaitteen ja Internetin välille. Testiympäristössä luodaan mahdollisia käytännön vikatilanteita ja seurataan verkon käyttäytymistä. Verkkotopologia on suunniteltu joustavaksi, mikä mahdollistaa verkon kehittymisen ja tarjoaa avaimet verkon ylläpitoon.

Avainsanat Tietoliikenne, Vikasietoisuus, LAN, STP, HSRP

Sivut 29 s. + liitteet 16 s.

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Information Technology
Information Network Technology

Author Ilkka Mäkinen **Year** 2015

Subject of Bachelor's thesis Network Redundancy

ABSTRACT

The subject of this thesis is based on my personal interests and experiences acquired in the field of IT-business. The thesis focuses on critical technical environments and the network redundancy that comes with them. This thesis contains a solution for implementing a redundant Internet connection in a laboratory environment.

All relevant information about network technology and the equipment used in this project are covered in the theoretical chapter. Technical terminology related to this thesis is also explained in detail to provide the reader a deeper understanding of the field. The main focus here is on network redundancy, as the title suggests. Information used in this thesis is based on the official Cisco Certification Guides and the author's personal knowledge.

A redundant Internet connection was established between a client and the Internet as a final outcome of this thesis. A few possible network faults were developed in the laboratory and the troubleshooting results are presented here. The network was planned considering the required flexibility to adjust and maintain a stable topology in the future.

Keywords Network, Redundancy, LAN, STP, HSRP

Pages 29 p. + appendices 16 p.

SANASTO

BPDU	Bridge Protocol Data Unit. Kytkimien välinen viesti Spanning Tree protokollaa käyttävässä lähiverkossa
DHCP	Dynamic Host Configuration Protocol. Mahdollistaa dynaamisten IP-osoitteiden määrittelyn verkkoon
DNS	Domain Name System. Nimipalvelu, joka muuntaa IP-osoitteet nimiksi ja päinvastoin
ETHERNET	Yleisin käytettävissä oleva lähiverkkotekniikka
FTP	File Transfer Protocol. Tiedonsiirtoprotokolla
HSRP	Hot Standby Router Protocol. Ciscon kehittämä verkon kahdennusprotokolla
HTTP	Hypertext Transfer Protocol. Tiedonsiirtoprotokolla
IEEE	Institute of Electronical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö
INTERNET	Maailmanlaajuinen tietoliikenneverkko, joka koostuu lukuisista pienemmistä tietoverkoista
IP	Internet Protocol. Verkkotason tiedonsiirtoprotokolla
LAN	Local Area Network. Lähiverkko
MAN	Metropolitan Area Network. Alueverkko
OSI-MALLI	Open Systems Interconnection Reference Model. Kerrostettu verkkomalli.
OSPF	Open Shortest Path First. Dynaaminen reititysprotokolla
ROAS	Router on a Stick. Fyysisen portin alle määritellään VLAN kohtaiset loogiset rajapinnat
RPVST+	Rapid Per-VLAN Spanning Tree Plus. VLAN kohtainen nopeasti toimiva STP
RSTP	Rapid Spanning Tree Protocol. Tavallista nopeampi STP
STP	Spanning Tree Protocol. Protokolla, joka estää silmukoiden muodostumisen verkossa
TCP	Transmission Control Protocol. Päätelaitteiden välinen protokolla, joka mahdollistaa tiedonsiirron

VLAN	Virtual Local Area Network. Yhdestä fyysisestä verkosta luotu looginen osa
VOIP	Voice over IP. Äänensiirtoon tarkoitettu protokolla IP-verkossa
WAN	Wide Area Network. Laajaverkko
WLAN	Wireless Local Area Network. Langaton lähiverkko

SISÄLLYS

1 JOHDANTO

Tietoliikenneyhteyksien saumatonta toimintaa ei voida tänä päivänä jättää huomioimatta. Varmennettujen yhteyksien ja vikasietoisten verkkoympäristöjen kysyntä kasvaa jatkuvasti. On yrityksiä, joiden liiketoiminta perustuu täysin tietoliikenteeseen ja tiedonsiirtoon. On myös olemassa palveluita ja ammatteja, jotka toimivat ilman verkkoyhteyksiä, mutta niihinkin lähes poikkeuksetta liittyy Internetin käyttö esimerkiksi mainonnan kautta. Tietoliikenneyhteyksien tarpeellisuudelle ei ole tulevaisuudessa näkyvissä minkäänlaista notkahdusta. Alan kehitys on huimaa, ja uusia palveluita sekä standardeja tulee jatkuvasti.

Mitä kriittisempiä palveluita tietoliikenneverkkojen sekä Internetin avulla rakennetaan ja tarjotaan suuren yleisön käytettäväksi, sitä tärkeämmäksi nousee myös niiden vikasietoisuus ja saumaton toiminta. Rinnakkaisten yhteyksien tärkeys korostuu yritysmaailmassa, jossa varaa virheisiin ei ole ja verkon toiminta on ehdotonta. Varmentavilla yhteyksillä varaudutaan suunnittelemattomiin katkoihin ja mahdollisiin inhimillisiin virheisiin.

2 TAVOITTEET JA RAJAUS

Tässä opinnäytetyössä käydään läpi verkon kahdennukseen liittyviä ratkaisuja ja tekniikoita sekä otetaan katsaus myös verkon perustoimintoihin ja tietoliikenteessä käytettävään termistöön. Työssä keskitytään testiolosuhteissa toteutettuun verkkoympäristöön, sen suunnitteluun ja konfigurointiin.

Tavoitteena on suunnitella ja rakentaa kahdennettu Internet-yhteys. Luodaan vikasietoinen verkkoratkaisu ja seurataan sen käyttäytymistä mahdollisissa käytännön vikatilanteissa. Työ toteutetaan virtuaalisesti sekä työnantajani Cinia One Oy:n tietoliikennelaboratoriossa Riihimäen toimipisteessä.

3 TIETOLIIKENNEVERKOT

Tässä työssä tietoliikenneverkot jaetaan karkeasti kolmeen eri ryhmään niiden käyttötarpeen, koon sekä maantieteellisen sijainnin mukaan. Kaikkien verkkojen toimintaperiaatteena on se, että tieto saadaan siirtymään sen laitteiden välillä. Yhdistämällä pienempiä verkkoja palveluntarjoajien runkoverkkoihin luodaan ja laajennetaan maailmanlaajuista verkkoa eli Internetiä.

Wide Area Network (WAN) eli laajaverkko on maantieteellisesti kattavin verkkotyyppi, ja se koostuu kahdesta tai useammasta alueverkosta tai lähiverkosta. Laajaverkon tarkoituksena on mahdollistaa pienempien verkkojen liittäminen Internetiin. Tämän tyyppiset verkot ovat yleisesti palveluntarjoajien ylläpidossa ja ne rakennetaan valokuidulla, satelliiteilla, puhelinverkoilla sekä vuokrayhteyksillä. Maailman suurin laajaverkko on Internet. (udemy.com, 2014.)

Metropolitan Area Network (MAN) eli alueverkko kohdistetaan usein johonkin kaupunkiin tai kylään. Sen tarkoituksena on yhdistää lähiverkkoja yhdeksi suuremmaksi toteutukseksi. Alueverkko on tavallisesti yhden isomman organisaation ylläpidossa, ja se toteutetaan valokuidulla, jolloin siitä muodostuu lähiverkoille luotettava runkoverkko. (udemy.com, 2014.)

Local Area Network (LAN) eli lähiverkko rajataan pienempiin alueisiin, kuten toimistot, koulut ja kodit. Oikeastaan kaikki nykyaikaiset lähiverkot ja langattomat lähiverkot perustuvat Ethernet-tekniikkaan. Lähiverkon sisäiset tiedonsiirtonopeudet ovat usein suurempia kuin laajemmissa kokonaisuuksissa. Lähiverkko on mahdollista muodostaa kaapeloimalla tai langattomasti. Verkon keskeisenä laitteena toimivat kytkimet, joista yhteydet muodostetaan työasemille kierretyllä parikaapelilla RJ-45-liittimiä käyttäen. (udemy.com, 2014.)

Ethernet (IEEE 802.3) on maailman suosituin lähiverkkotekniikka. Se koostuu useasta IEEE:n (Institute of Electrical and Electronics Engineers) laatimasta standardista. Kyseiset standardit kattavat verkon kaapeloinnin, liittimien, protokollien sekä kaiken muun tarvittavan tiedon Ethernet-verkon rakentamiseksi. (Odom, W. 2013, 46-47.)

Nykyaikainen Ethernet-verkko liikennöi vähintään 100Mbps ja 1Gbps – nopeuksissa. Nopeudet voivat nousta jopa 100Gbps asti.

Ethernet-kytkimen toimintaperiaatteena on vastaanottaa Ethernet-kehyksiä ja tehdä päätöksiä, joiden perusteella kehykset siirretään eteenpäin. Toiminta perustuu MAC-osoitteisiin, joiden perusteella lähettävä ja vastaanottava portti määritellään.

3.1 OSI-Malli

OSI (Open System Interconnection) on kerrostettu verkkomalli, joka koostuu seitsemästä eri tasosta ja niihin kuuluvista tiedonsiirtoprotokollista. OSI-mallia voidaan verrata nykyään yleisesti käytössä olevaan TCP/IP-malliin (Taulukko 1).

Taulukko 1. OSI-mallia voidaan verrata kahteen eri TCP/IP-malliin. (Odom, W. 2013, 35.)

	OSI	**TCP/IP**	**TCP/IP**
7	Application	Application	Application
6	Presentation		
5	Session		
4	Transport	Transport	Transport
3	Network	Internet	Network
2	Data Link	Link	Data Link
1	Physical		Physical

Nykyaikaisen verkkotekniikan terminologian ymmärtämiseksi myös OSI-mallin perusteet täytyy sisäistää. Etenkin kerrokset 2 ja 3 ovat suosittuja verkkodokumentaation yhteydessä.

Taulukko 2. OSI-mallin kerrokset ja avainsanat.

7	**Sovelluskerros.** Tarjoaa rajapinnan ohjelmien väliseen kommunikointiin. Protokollia mm. Telnet, HTTP, FTP, VoIP.
6	**Esitystapakerros.** Tarkoitus määritellä tiedostomuodot ja niiden salaus/purku. Protokollia mm. Telnet, HTTP, FTP, VoIP.
5	**Istuntokerros.** Määrittelee miten eri istunnot aloitetaan, prosessoidaan sekä lopetetaan. Protokollia mm. Telnet, HTTP, FTP, VoIP.
4	**Kuljetuskerros.** Tiedonsiirtoon liittyvät protokollat ja määritykset. TCP ja UDP.
3	**Verkkokerros.** Loogiset osoitteet, reititys ja parhaan polun valinta. Protokollana IP.
2	**Siirtoyhteyskerros.** Määritellään mahdollisuudet pakettien sekä kehysten lähetykseen. Ethernet, kytkimet, modeemit.
1	**Fyysinen kerros.** Kaapelointi, liittimet, sähkönsiirto.

4 VERKON PALVELUT JA LAITTEET

Tietoliikenneverkon toimintaan sisältyy valtava määrä vaihtoehtoja riippuen sen käyttötarkoituksesta. Tässä luvussa käydään läpi tämän laboratoriotyön kannalta keskeisimmät verkkoon liittyvät käsitteet ja laitteet.

4.1 TCP/IP

Transmission Control Protocol / Internet Protocol lyhennetään muotoon TCP/IP, ja se käsittää useamman tietoliikenneprotokollan, joita käytetään liikennöidessä Internetiin. TCP-protokolla on toteutuksen ydin ja sitä käytetään laitteiden välisen tiedonsiirron toteuttamiseen, pakettien järjestämiseen sekä niiden uudelleenlähetykseen. IP-protokollan tehtävä on huolehtia verkon reitityksestä ja laitteiden IP-osoitteista. TCP/IP-protokollaa voidaan kutsua tietoliikenneverkon laitteiden väliseksi kieleksi, jolla kommunikointi onnistuu.

4.2 DHCP

Dynamic Host Configuration Protocol (DHCP) on palvelimen ja työaseman välinen protokolla, joka mahdollistaa IP-osoitteiden automaattisen jakamisen verkossa oleville IP-laitteille. DHCP:n kautta laitteet saavat myös muuta olennaista informaatiota, kuten kyseisen verkon aliverkkomaskin (subnet mask) sekä oletusyhdyskäytävän (default gateway). (microsoft.com, 2015.)

DHCP-palvelimena voi toimia verkossa oleva reititin tai erillinen palvelin. Suuremmissa verkoissa DHCP on käytännössä pakollinen, sillä se minimoi virheet, kuten IP-osoitteiden duplikaatit. DHCP vähentää myös verkon ylläpitäjän tehtäviä huomattavasti.

4.3 DNS

Domain Name System (DNS) on nimipalvelujärjestelmä, joka muuntaa verkon IP-osoitteet numeroista tekstiksi. Jokaisella verkkosivulla tai laitteella on IP-osoite, jonka DNS muuntaa selkokieliseksi nimeksi. Verkkoon tarvitaan julkinen tai sisäinen DNS-palvelin tämän saavuttamiseksi. DNS-palvelimelle on määritelty IP-osoitteita vastaavat selkokieliset nimet. Esimerkiksi Google tarjoaa julkisia DNS-palvelimia, jotka toimivat IP-osoitteilla 8.8.8.8 ja 8.8.4.4. (howtogeek.com, 2012.)

4.4 VLAN

Virtual Local Area Network (VLAN) on tiettyä käyttötarkoitusta varten luotu verkon osa, jolla yksi fyysinen verkko jaetaan eri loogisiin osiin. Saman virtuaaliverkon jäsenet voivat sijaita fyysisesti missä tahansa. Yhdellä fyysisellä verkolla tarkoitetaan verkkoympäristöä, jonka laitteet kuuluvat samaan alueeseen.

Ottamalla käyttöön lähiverkossa useita virtuaaliverkkoja mahdollistetaan työasemien ryhmittely ja käyttöoikeuksien rajaaminen käyttötarpeiden mukaan. Tämä toteutustapa parantaa verkon tietoturvaa ja joustavuutta huomattavasti. Mikäli virtuaaliverkkoja ei ole otettu käyttöön, kytkimen kaikki portit ovat samassa verkossa.

VLAN-tekniikalla on ehdottomasti suurin merkitys yksittäisen kytkimen päätökseen siitä, mihin suuntaan verkossa liikkuvia kehyksiä siirretään. Määrittämällä virtuaaliverkkoja yksilöidään verkon toimintaa ja vähennetään tarpeettomien pakettien määrää. Samalla parannetaan verkon tietoturvaa estämällä näkyvyys eri osioiden välillä. (Odom, W. 2013, 239.)

Virtuaaliverkkojen käyttöönotto yhdellä kytkimellä on suhteellisen yksinkertaista. Luodaan halutut VLAN:t ja määritellään mihin VLAN:iin mikäkin portti kuuluu. Kun kytkinverkko laajenee, täytyy verkkolaitteiden välille ottaa käyttöön *VLAN tagging*.

4.5 VLAN Tagging

Kun lähiverkossa käytetään virtuaalisia verkkoja, täytyy kytkimien välisissä yhteyksissä ottaa käyttöön VLAN tagging. Tämän toiminnon avulla kytkin lisää jokaiseen lähetettävään datakehykseen yhden tunnisteen, joka sisältää virtuaaliverkon tunnuksen (VLAN ID). VLAN ID:n perusteella vastaanottava kytkin pystyy jakamaan eri aliverkoille kuuluvat kehykset oikeisiin osoitteisiin. Tätä hyödyntämällä verkon liikennettä pystytään jakamaan halutulla tavalla. (Odom, W. 2013, 239.)

4.6 Reititin

Reititin toimii OSI-mallin 3. kerroksella. Sen tehtävänä on muodostaa verkkojen väliset yhteydet ja määrittää verkossa liikkuvalle datalle parhaat mahdolliset polut. Reititin ohjaa verkon IP-paketit niille määriteltyihin kohdeosoitteisiin. Tätä kutsutaan *reitityksekseksi*. Reitit voivat muodostua joko kiinteästi konfiguroiduista osoitteista eli ns. *staattisista* reiteistä tai reititysprotokollan luomista *dynaamisista* reiteistä. Dynaamisia reititysprotokollia käytetään varsinkin monimutkaisemmissa toteutuksissa ja niitä ovat esimerkiksi OSPF, BGP sekä EIGRP. Reitittimiä käytetään yhdistämään verkkoja ja lähiverkoissa se tarkoittaa usein yhteyden muodostamista Internetin suuntaan.

4.7 Kytkin

Kytkin on lähiverkon keskeinen laite ja se toimii OSI-mallin 2. kerroksella eli siirtoyhteyskerroksella. Kytkimet välittävät lähiverkossa liikkuvia kehyksiä porttikohtaisesti MAC-osoitteiden perusteella. Kytkimeen voidaan liittää esimerkiksi työasemia, tukiasemia, palvelimia sekä tietysti verkon muita kytkimiä ja reitittimiä. Kytkimen porteissa käytetään tavallisesti pa-

rikaapelia RJ-45 liittimellä tai valokuitua SFP-moduulin avulla. Nykyaikaisissa kytkimissä on ainakin yksi portti valokuitua varten, jota käytetään verkkolaitteiden välisenä kytkentänä. Näitä kutsutaan uplink- tai trunk-porteiksi. Tavallisia työasemaportteja kutsutaan *access*-porteiksi.

4.8 Työasema

Päätelaitteena toimiva työasema on keskeinen osa tietoliikenneverkon tarkoitusta. Päätelaitteet eivät vaikuta millään tavalla verkon toimintaan, mutta niiden takia verkkoja rakennetaan. Ne ovat loppukäyttäjien operoimia tietokoneita, tabletteja, telemaattisia laitteita tai oikeastaan mitä vain laitteita, joilla pyritään keskustelemaan verkossa. Tavallinen verkon käyttäjä ei välitä siitä, kuinka hänen yhteytensä on toteutettu, kunhan se toimii.

5 VARMENNETUT YHTEYDET

Mitä suuremmaksi verkko kasvaa ja mitä kriittisempiä palveluita se sisältää, sitä tärkeämmäksi tulee myös verkon toiminnan varmistus. Palveluntarjoajan näkökulmasta on erittäin tärkeää, että asiakkaan yhteydet toimivat lähes sadan prosentin varmuudella. Lyhytkin katko jonkin kriittisen toimipisteen verkossa saattaa aiheuttaa hyvinkin suuria varatoimenpiteitä, jotka tulevat ylläpitäjälle erittäin kalliiksi.

Verkon toiminnan varmistukseen liittyy monia tekijöitä ja tässä työssä käsitellään muutamaa protokollaa, joiden avulla saadaan teknisesti toteutettua verkkoyhteyksien kahdennus ja varmistavien yhteyksien luonti lähiverkon sisällä. Varmentavia yhteyksiä suunnitellessa ja luodessa täytyy ottaa huomioon riskitekijät, kuten sähkökatkot, kaapelikatkot sekä viallinen laitteisto.

5.1 Hot Standby Router Protocol

HSRP on Ciscon kehittämä verkkotasolle sijoittuva kahdennusmenetelmä, jonka toimintaperiaatteena on luoda tietoliikenteelle useampi reitti käyttämällä rinnakkaisia reitittimiä toisiaan varmentamaan. Tällaisessa toteutuksessa verkko käyttää yhtä reititintä pääyhteyden muodostamiseen ja loput reitittimet ovat passiivisessa tilassa odottamassa, mikäli pääyhteydessä ilmenee vikaa. Näitä voidaan kutsua verkon reunareitittimiksi, jotka tarjoavat yhteyden lähiverkosta palveluntarjoajan runkoverkkoon eli Internetin suuntaan. Tämän kaltaista tekniikkaa tarvitaan, koska työasemille ei ole mahdollista määritellä kuin yksi oletusyhdyskäytävä.

Samaan HSRP-ryhmään kuuluvat reitittimet tarjoavat verkolle vain yhden oletusyhdyskäytävän. Toisin sanoen vikatilanteessa käyttäjät eivät huomaa reittimuutosta lainkaan eikä heidän päätelaitteiden IP-asetuksia tarvitse muuttaa. Saman ryhmän reitittimet jaetaan kolmeen eri tilaan, joista yksi on *aktiivinen*, toinen on *varalla* ja loput reitittimet ovat *kuuntelemassa*. Reitittimet keskustelevat keskenään lähettämällä viestejä tasaisin väliajoin ja ilmoittavat näin olemassaolostaan. Tätä keskustelua käydään vain aktiivisen

ja varalla olevan reitittimen välillä. Mikäli aktiiviselta reitittimeltä ei tule määräaikaan mennessä viestit perille, niin varalla oleva reititin rupeaa automaattisesti ohjaamaan liikennettä ja muuttuu näin ollen aktiiviseen tilaan. (Hucaby, D. 2010, 271-279.)

Oletusarvoisesti reitittimet on ajastettu lähettämään hello-viestejä kolmen sekunnin välein ja mikäli kolmannen paketin jälkeen vastausta ei kuulu, niin varalla oleva reititin ottaa ohjat käsiinsä. Ajastimia on mahdollisuus muokata manuaalisesti timers-komennolla. Reitittimen tila konfiguroidaan sen priority-arvoa muokkaamalla ja suurimman prioorityn omaava reititin on verkon aktiivinen reititin. (Hucaby, D. 2010, 271-279.)

HSRP toteutuksessa on myös ominaisuus, joka mahdollistaa paluun pääyhteydelle automaattisesti vikatilanteen ratkettua. Normaalitilanteessa varalla oleva reititin ei voi ottaa aktiivisen reitittimen roolia ennen kuin senhetkinen pääyhteys katkeaa. Käyttämällä preempt-komentoa on mahdollista määrittää, että alkuperäisesti pääyhteydeksi määritelty reititin valitaan välittömästi aktiiviseksi, kun sen kautta liikenne on mahdollista. (Hucaby, D. 2010, 271-279.)

5.2 Spanning Tree Protocol

IEEE 802.1D eli STP on kytkinverkkoon sijoittuva protokolla, joka mahdollistaa vikasietoisen lähiverkon luomisen. Tämän protokollan toimintaperiaate mahdollistaa kahdennettujen yhteyksien luomisen kytkimien välille ilman *silmukoiden* muodostumista. STP valvoo ja hallitsee kytkinverkkoa niin, että liikenne kulkee vain yhdestä trunk-linkistä kerrallaan, mikäli samaan määränpäähän on luotu useita yhteyksiä. (Hucaby, D. 2010, 128-129.)

Spanning Tree–protokollan toiminta perustuu siihen, että verkossa on aina yksi pääkytkin (root), jonka kautta liikenne kulkee, silloin kun se on mahdollista. Luvun 5.1 L2 verkkokuvan (Kuva 1.) mukaisessa tilanteessa pääkytkimeksi on määritelty CORE-SW1, jolloin STP asettaa CORE-SW2 ja LAN-SW1 välisen trunk-linkin estotilaan ja kaikki liikenne kulkee pääkytkimen kautta.

Verkossa esiintyväksi silmukaksi kutsutaan sellaista tilannetta, jossa kahden kytkimen välinen liikenne pääsee pyörimään loputtomasti. Kumpikaan kytkin ei ole tietoinen toisesta, joten ne jatkavat datakehysten siirtämistä eteenpäin loputtomasti. Tämän kaltaiset silmukat saattavat kuormittaa verkkoa hyvinkin paljon ja johtaa erinäisiin vikatilanteisiin. STP kehitettiin ratkaisemaan tämä ongelma sekä mahdollistamaan kahdennettujen reittien luomisen myös kytkinten välillä. (Hucaby, D. 2010, 131.)

5.2.1 STP-porttien tilat

Osallistuakseen STP:n toimintaan kytkimen jokaisen portin täytyy siirtyä usean eri tilan lävitse. Kaikki portit ovat oletusarvoisesti tilassa *suljettu*, josta ne siirtyvät usean passiivisen tilan läpi välittämään liikennettä, mikäli se sallitaan. Ciscon (Hucaby, D. 2010, 139.) mukaan STP-porttien tilat ovat seuraavat:

Disabled (suljettu) – tilassa olevat portit ovat sellaisia, jotka verkon ylläpitäjä on sulkenut. Tämä on erikoistila, joka ei kuulu STP:n normaaliin toimintaketjuun. Kaikki portit kuitenkin aloittavat oletusarvoiesti tästä tilasta.

Blocking (esto) – tilassa oleva portti ei voi lähettää eikä vastaanottaa dataa eikä myöskään välittää MAC-osoitteita sen MAC-osoitetauluun. Kaikki avatut portit aloittavat tästä tilasta. Ainoastaan BPDU-pakettien välitys on mahdollista, jotta keskustelu onnistuu viereisten kytkimien kanssa. Kaikki varmentavien yhteyksien portit ovat tässä tilassa estääkseen silmukoiden syntymisen.

Listening (kuunteleva) – tilaan portti siirtyy estotilasta, kun sillä on aikomus siirtyä liikennettä välittävään tilaan. Kuuntelevassa tilassa oleva portti ei pysty vielä lähettämään datakehyksiä, mutta se pystyy lähettämään ja vastaanottamaan BPDU-paketteja ottaakseen osaa Spanning Tree -topologian muutoksiin. Mikäli tätä porttia ei valita liikennöiväksi portiksi se palautuu välittömästi estotilaan.

Learning (oppiva) – tilaan siirrytään kuuntelevasta tilasta tietyn viiveen jälkeen. BPDU-pakettien lisäksi portti kykenee välittämään uusia MAC-osoitteita sen osoitetauluun, mikä antaa kytkimelle mahdollisuuden luoda jonkinlaisen kuvan verkossa olevista osoitteista. Datakehykset eivät liiku vieläkään.

Forwarding (liikennettä välittävä) – tila saavutetaan oppivan tilan jälkeen ja se mahdollistaa datakehysten, MAC-osoitteiden sekä BPDU-pakettien välittämisen molempiin suuntiin. Tässä tilassa porttia kutsutaan aktiiviseksi Spanning Tree -topologian jäseneksi.

5.2.2 Rapid Spanning Tree Protocol

IEEE802.1w eli RSTP-standardi on kehitetty käyttämään alkuperäisen Spanning Tree -protokollan toimintaperiaatteita huomattavasti nopeammin ja tehokkaammin. Alkuperäisessä toteutuksessa topologian muuttuessa liikennöivän portin valitsemiseen menee 30 sekuntia, kun portti muuttuu estotilasta liikennettä välittävään tilaan. Teknologian kehittyessä ja verkon palveluiden muuttuessa yhä kriittisimmiksi tämä on aivan liian pitkä aika tuotannossa olevalle verkolle. Kun käytetään RSTP-protokollaa, niin käytännössä porttimuutos tapahtuu niin nopeasti, ettei käyttäjä huomaa liikenteen katkeavan lainkaan. (Hucaby, D. 2010, 198-199.)

5.2.3 Rapid Per-VLAN Spanning Tree Protocol

Jokaista virtuaalista verkkoa kohden on mahdollista ottaa käyttöön oma STP-instanssi. Oletuksena Ciscon kytkimet käyttävät tällaisessa konfiguraatiossa alkuperäistä STP-tekniikkaa, jonka toiminta on todettu liian hitaaksi. Muuttamalla kytkimen konfiguraatiota käyttämään RSTP-tekniikkaa ja yhtäaikaisesti määrittelemällä jokaiselle virtuaaliverkolle (VLAN) oma STP, saadaan tulokseksi Rapid PVST+ (RPVST+). Tuotannossa olevia verkkoja muokatessa pitää muistaa, että STP-tilaa muuttamalla jokainen käynnissä oleva STP-prosessi käynnistyy uudelleen ja portit neuvottelevat tavallisten tilojen läpi, mikä saattaa aiheuttaa muutaman paketin katoamisen. (Hucaby, D. 2010, 205)

Vaikka STP-tilan muutos kuulostaa monimutkaiselta, niin itse kytkimen konfiguraatioon tämä toimenpide ei aiheuta oikeastaan kuin yhden rivin konfiguraatiota:

```
Switch(config)#spanning-tree mode rapid-pvst
```

Per-VLAN STP-tekniikkaa voidaan käyttää kuormanjakoon verkon kytkinten trunk-linkkien välillä. Toisin sanoen portit ovat eri STP-tilassa eri aliverkkojen osalta ja näin ollen liikenne jakautuu määritellyn konfiguraation mukaisesti.

Toisaalta, kun virtuaaliverkkojen määrä kasvaa todella suureksi ja jokaista kohden pyörii oma STP-instanssi, niin tämä aiheuttaa kytkimen prosessorille ja muistille valtavaa kuormaa ja itse liikenteen välitykselle ei välttämättä jää tarpeeksi tehoja. Voidaan todeta, että verkon suunnittelun ja sen tarpeiden kartoituksen pitää vastata käytössä olevaa laitteistoa.

5.2.4 Bridge Protocol Data Unit (BPDU)

Spanning Tree -protokollaa käyttävä verkko käyttää BPDU-paketteja kommunikoidakseen kytkimien välillä. Paketit lähtevät liikkeelle topologian pääkytkimeltä ja niiden avulla kartoitetaan verkossa olevia laitteita. Näiden ansiosta on mahdollista luoda vakaita lähiverkkoja ilman silmukoiden muodostumista. (Hucaby, D. 2010, 182.)

5.2.5 BPDU Guard

Suojautuakseen silmukoiden muodostumiselta ja yllättävien BPDU-pakettien vastaanottamiselta, kytkimissä voidaan ottaa käyttöön BPDU Guard. Tämä toiminto määritellään työasemakytkimen access-porteille, joihin oletetaan liitettävän ainoastaan päätelaitteita, jotka eivät välitä BPDU-paketteja. Nämä portit on tavallisesti määritelty niin, että ne siirtyvät automaattisesti liikennettä välittävään tilaan, mikäli niihin liitetään jokin laite.

Mikäli BPDU Guard on määritelty ja sitä käyttävään porttiin saapuu BPDU-paketteja, kyseinen portti siirtyy automaattisesti *error-disabled* – tilaan. Tässä tilassa portti on suljettu vikatilanteen vuoksi. Verkon ylläpitäjä palauttaa portin toimintakuntoon sitten kun tilanne on normalisoitunut. Portti

voidaan halutessa myös ajastaa niin, että BPDU-pakettien loppuessa se palautuu automaattisesti toimintakuntoon. Portti ei voi päästä pois suljetusta tilasta mikäli BPDU Guard on määritelty ja portti vastaanottaa edelleen BPDU-paketteja.

Tätä toimintoa ei oikeastaan ikinä käytetä kytkimien trunk-porteissa, sillä ne vastaanottavat BPDU-paketteja koko ajan verkon pääkytkimeltä ja portit halutaan säilyttää joko liikennettä välittävänä tai varalla olevana linkkinä.

BPDU Guard otetaan käyttöön porttikohtaisesti alla olevalla komennolla:

```
Switch(config-if)#spanning-tree bpduguard enable
```

6 INTERNET-YHTEYDEN KAHDENNUS TESTIYMPÄRISTÖSSÄ

Tässä laboratoriotyössä luodaan todellista tilannetta kuvaava tietoliikenneverkko, jolla tarjotaan varmennettu Internet-liittymä asiakkaan toimipisteeseen. Toteutukseen sisältyy myös pienimuotoinen lähiverkkoratkaisu. Työ on suunniteltu ja testattu virtuaalisesti Cisco Packet Tracer -ohjelmalla ja tarvittavat verkkokuvat piirretty Microsoft Visiolla. Käytännön toteutus ja verkon varmennusta koskevat kokeet on tehty Cinia One Oy:n tietoliikennelaboratoriossa.

Internet-yhteyden kahdennus toteutuu tässä tapauksessa kahdella reunareitittimellä, joissa käytetään HSRP-tekniikkaa varmentavan yhteyden luomiseen. Tämän ratkaisun periaatteena on se, että lähiverkon ja Internetin välisellä liikenteellä on yksi aktiivinen pääyhteys sekä taustalla toimiva varayhteys. Mikäli liikenne ei pääse jostain syystä kulkemaan pääreittiä pitkin, niin se siirtyy automaattisesti käyttämään sille luotua varayhteyttä. Pääyhteyden korjautuessa liikenne palaa ennalleen eikä verkon käyttäjille ole syntynyt lainkaan katkosta tietoliikenteeseen.

Testiympäristössä Internet-yhteyttä kuvataan reitittimellä hyödyntäen sen Loopback-osoitteita. Internet-reititin toimii myös verkon DHCP-serverinä, joka jakaa IP-osoitteet lähiverkon työasemille. Todellisuudessa tämä reititin olisi osa palveluntarjoajan runkoverkkoa, josta on yhteys Internetiin. Loopback-osoitteita hyödyntämällä voidaan kuitenkin laboratorioympäristössäkin havainnollistaa todellisuutta vastaava tilanne.

Lähiverkko koostuu kahdesta runkokytkimestä ja yhdestä ns. työasemakytkimestä. Runkokytkimet ovat suoraan yhteydessä verkon molempiin reunareitittimiin ja ne luovat vikasietoisen pohjan lähiverkolle. Runkokytkimet varmentavat lähiverkon toimintaa paikallisesti ja jakavat yhteydet muille kytkimille. Lähiverkon runkoon ei tavallisesti liitetä suoraan työasemia, kuten ei tässäkään työssä.

Kytkimissä käytetään Spanning Tree-protokollaa, joka estää silmukoiden muodostumisen sekä mahdollistaa samalla varmentavien kytkentöjen tekemisen lähiverkossa.

Toimipisteen verkko muodostuu kahdesta eri aliverkosta, jotka luodaan käyttämällä VLAN-tekniikkaa. Tämä mahdollistaa käyttäjien jaottelun ja helpottaa huomattavasti esimerkiksi käyttöoikeuksien rajaamista verkon eri palveluihin.

6.1 Verkkotopologia

Hyvän ja helposti ylläpidettävän tietoliikenneverkon rakentaminen alkaa suunnittelusta. Aluksi selvitetään käytettävissä olevat laitteet ja työkalut ja niiden avulla toteutettavissa oleva ratkaisu. Samalla selviävät mahdolliset puutteet ja tarpeet uusiin hankintoihin tai osaamisen kehittämiseen. Hyvän lopputuloksen perusta on, että kaikesta ylläpidon ja jatkokehityksen kannalta merkityksellisestä tehdään kattava dokumentaatio.

Verkon ylläpito ja laajentaminen on huomattavasti helpompaa, kun tarjolla on selkeästi piirretyt verkkokuvat. Verkkokuvia on hyvä pitää ainakin kaksi eri versioita. Toiseen suunnitellaan tulevia muutoksia ja toinen pidetään koko ajan ajan tasalla kuvaamassa verkon nykyistä tilannetta.

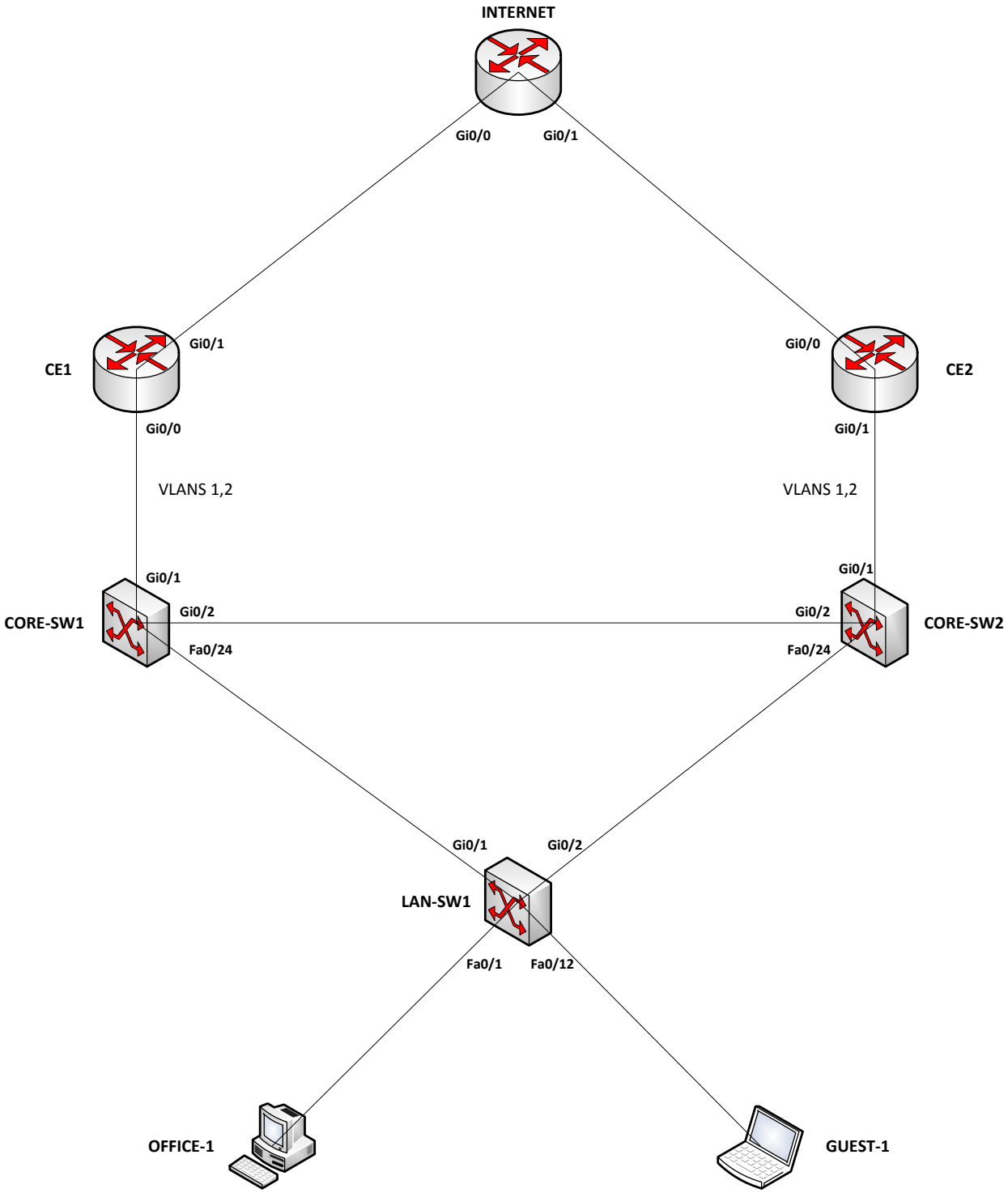
Suunnittelu alkoi tämän työn osalta kynällä ja paperilla, mistä siirryttiin käyttämään Cisco Packet Traceria sekä Microsoft Visiota. Suunnitelmassa on otettu huomioon tietoliikennelaboratorion olosuhteet ja käytössä oleva laitteisto.

Verkkotopologiasta luodaan usein kaksi erilaista verkkokuvaa. Kuten aikaisemmin työssä mainitaan, tietoliikenneverkon toimintaa voidaan kuvata OSI-mallin mukaisesti ja näin ollen tätä voidaan myös hyödyntää verkkokuvia piirrettäessä. Luodaan Layer 2 ja Layer 3 -verkkokuvat.

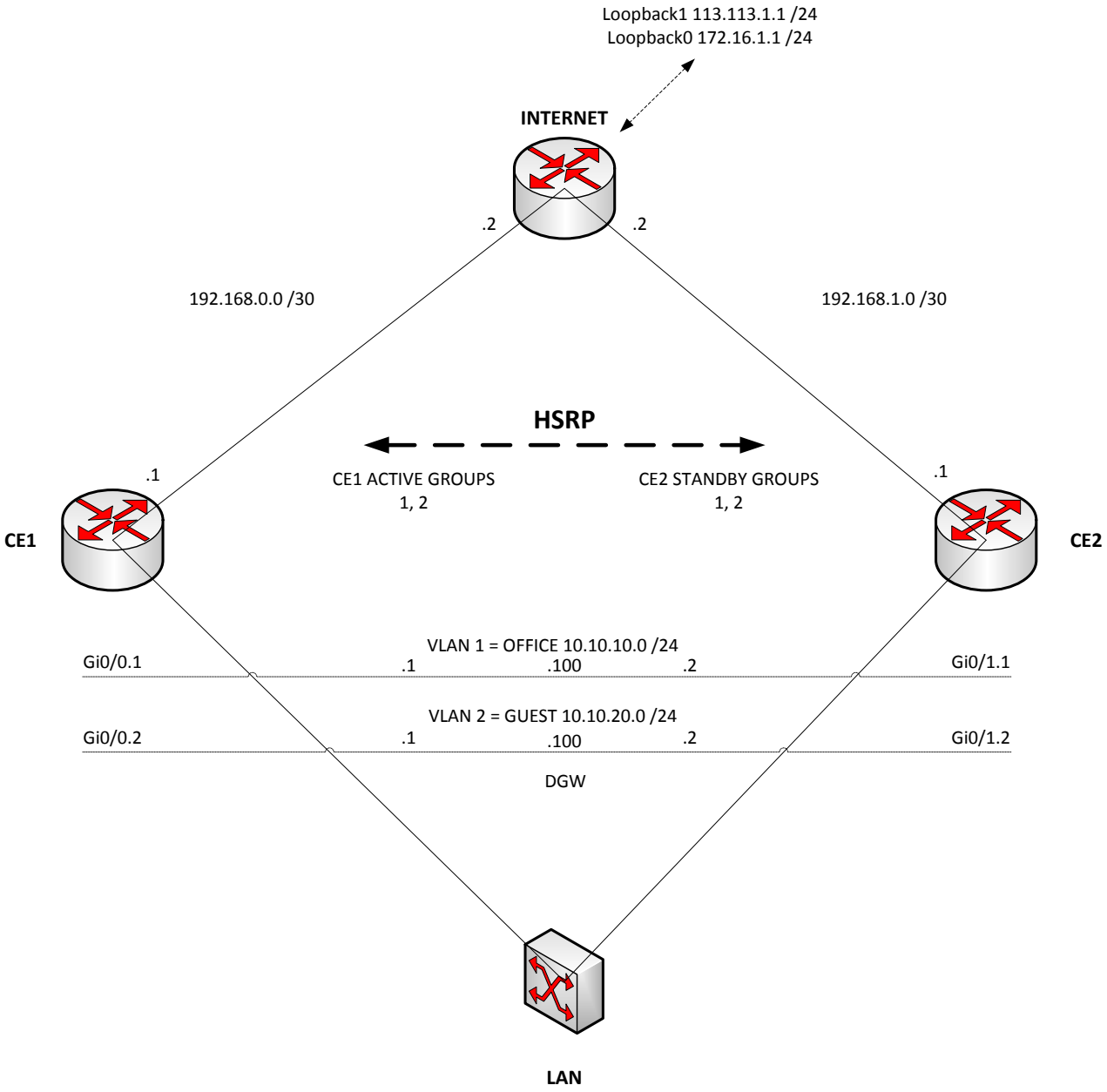
OSI-mallin Layer 2 viittaa siis siirtoyhteyskerrokseen ja tähän kyseiseen kuvaan merkitään verkon aktiivilaitteiden lisäksi kaikki fyysiset kytkennät eli porttitiedot. Kuvaan voidaan merkitä lähiverkkoon kuuluvat työasemat ja muut päätelaitteet, mikäli se on verkon ylläpidon kannalta tärkeää. Suuremmissa toteutuksissa työasemia ei käytännössä merkitä lainkaan. Laajemmissa ympäristöissä verkon aktiivilaitteiden sijaintitiedot ovat elintärkeitä ylläpidon kannalta.

Layer 3 eli verkkokerroksesta piirrettävään kuvaan merkitään verkossa olevat aliverkot, linkkiverkot ja loogiset rajapinnat IP-osoitteineen. Verkon ylläpitäjä voi käyttää tätä kuvaa esimerkiksi reititykseen liittyvissä ongelmissa tutkimalla verkkokuvaa ja reitittimen reititystaulua.

Seuraavassa kahdessa kuvassa esitellään tässä työssä rakennetun tietoliikenneverkon verkkokuvat.



Kuva 1. Internet-yhteyden kahdennus. Layer 2 -verkkokuva



Kuva 2. Internet-yhteyden kahdennus. Layer 3 -verkkokuva

6.2 Työkalut ja laitteisto

Kaikki työssä käytetyt verkkolaitteet ovat Ciscon valmistamia laitteita. Verkon reitittiminä toimii C1900-sarjan malli CISCO1941. Kytkimet ovat puolestaan Cisco Catalyst 2960-sarjan mallia 24TT. Kyseiset laitteet ovat hinnaltaan järkeviä ja sopivat tähänkin ratkaisuun mainiosti. Realistisissa olosuhteissa varsinkin INTERNET-reitittimen paikalla olisi käytetty vielä järeämpää ja vakaampaa laitteistoa, sillä se on osa palveluntarjoajan runkoverkkoa.

Verkko luotiin ja testattiin ensin Cisco Packet Tracer – ohjelmalla, joka tarjoaa virtuaalisen mahdollisuuden luoda tietoliikenneverkkoja. Ohjelmistolla onnistuu laitteiden konfigurointi, niiden välinen kaapelointi sekä työasemien liittäminen verkkoon aivan kuin laboratorioympäristössä. Ohjelmassa voidaan käyttää luonnollisesti vain Ciscon verkkolaitteita. Packet Tracer Student versio on ilmaiseksi saatavilla ja se on erittäin tehokas työkalu suurempiinkin toteutuksiin.

Suunnittelun ja virtuaalisen testauksen jälkeen toteutus siirrettiin työnantajani tietoliikennelaboratorioon. Hyvän dokumentaation ja valmistelujen ansiosta haluttuun tulokseen päästiin ongelmitta. Verkon toimintaa ja vikasietoisuutta testattiin käytännön vikatilanteilla.

6.3 Konfigurointi

Verkon laitteet on konfiguroitu kokonaan komentokehotteesta käyttäen Ciscon käyttöliittymän tarjoamia komentoja. Laitteiden CLI:hin eli komentokehotteeseen päästään paikallisesti kiinni liittämällä työasema eli PC haluttuun verkkolaitteeseen konsolikaapelilla. Väliin tarvitaan myös sopiva adapteri, joka tulee usein laitteen mukana. Konsolikaapelin toisessa päässä on RJ45-liitin ja toisessa päässä DB9-sarjaliitin. Nykyään harvasta koneesta löytyy tuota sarjaporttia, joten väliin tarvitaan USB tai RJ45-sovitin.

Kytkentöjen lisäksi työasemalla tulee olla jokin terminaali-ohjelma, jolla yhteys saadaan muodostettua. Tässä työssä on käytetty Cisco Packet Traceriin sisäänrakennettua terminaalia sekä ilmaista PuTTY-sovellusta.

Laitteiden konfigurointi on tehty konsoliyhteydellä, koska kyseessä oli paikallinen testiympäristössä toteutettu työ. Tuotantoverkossa olevia laitteita pystytään konfiguroimaan etäyhteyden avulla. Etäyhteyden muodostamiseen voidaan käyttää telnet- ja ssh-protokollia.

6.3.1 Verkot ja reititys

Verkon konfigurointi aloitettiin reitittimistä ja niiden välille muodostuvan liikenteen ohjaamisesta eli reitityksestä. Konfiguroinnissa on olennaista hyödyntää aikaisemmin tehtyjä suunnitelmia ja verkkokuvia. Verkkokuvien perusteella (Kuvat 1 ja 2) nähdään reitittimien välille muodostuvat linkkiverkot ja niille allokoidut osoiteavaruudet, joista konfigurointi tulee aloittaa.

```
INTERNET(config)#interface gigabitEthernet0/0
INTERNET(config-if)#description -> CE1 gi0/1
INTERNET(config-if)#ip address 192.168.0.2 255.255.255.252
INTERNET(config-if)#no shutdown

INTERNET(config)#interface gigabitEthernet0/1
INTERNET(config-if)#description -> CE2 gi0/0
INTERNET(config-if)#ip address 192.168.1.2 255.255.255.252
INTERNET(config-if)#no shutdown

CE1(config)#interface gigabitEthernet0/1
CE1(config-if)#description -> INTERNET gi0/0
CE1(config-if)#ip address 192.168.0.1 255.255.255.252
CE1(config-if)#no shutdown

CE2(config)#interface gigabitEthernet0/0
CE2(config-if)#description -> INTERNET gi0/1
CE2(config-if)#ip address 192.168.1.1 255.255.255.252
CE2(config-if)#no shutdown
```

Yllä olevilla riveillä määritellään reitittimien väliset linkkiverkot ja asetetaan kullekin rajapinnalle IP-osoite. Konfigurointiin on lisätty myös kyseiseen porttiin sopiva kuvaus ylläpidon helpottamiseksi. Kaikki linkit nostetaan ylös komennolla `no shutdown` (oletuksena kaikki suljettu). Linkkiverkoissa on käytössä vain kaksi IP-osoitetta, sillä enempään ei ole tarvetta.

Konfiguroidaan INTERNET-reitittimen Loopback-osoitteet, jotka kuvaavat tässä testiympäristössä Internetissä sijaitsevia satunnaisia osoiteavaruuksia. Näiden osoitteiden avulla voidaan verkon toimintaa testata työasemilta ulkomaailmaan ja päinvastoin.

```
INTERNET(config)#interface Loopback0
INTERNET(config-if)#ip address 172.16.1.1 255.255.255.0
INTERNET(config-if)#no shutdown

INTERNET(config)#interface Loopback1
INTERNET(config-if)#ip address 113.113.1.1 255.255.255.0
INTERNET(config-if)#no shutdown
```

Seuraavaksi huomataan, että lähiverkko muodostuu kahdesta virtuaaliverkosta VLAN1 ja VLAN2. Tässä tapauksessa reitittimen fyysisen portin alle luodaan kaksi loogista rajapintaa, joita kutsutaan sub-interfaceiksi. Tätä toteutusta kutsutaan tietoliikennemaailmassa nimellä Router on a Stick (ROAS).

```
CE1(config)#interface GigabitEthernet0/0
CE1(config-if)#no shutdown
```

```
CE1(config)#interface GigabitEthernet0/0.1
CE1(config-subif)#description OFFICE
CE1(config-subif)#encapsulation dot1Q 1 native
CE1(config-subif)#ip address 10.10.10.1 255.255.255.0

CE1(config)#interface GigabitEthernet0/0.2
CE1(config-subif)#description GUEST
CE1(config-subif)#encapsulation dot1Q 2
CE1(config-subif)#ip address 10.10.20.1 255.255.255.0
```

Yllä olevilla riveillä luodaan CE1-reitittimelle molemmille aliverkoille oma rajapinta, johon määritellään verkon osoiteavaruus sekä otetaan käyttöön 802.1Q standardi. Jokaisella 802.1Q –linkillä tulee olla määritelty myös native vlan, joka on tässä tapauksessa VLAN1. Rajapintojen kuvaus asetetaan vastaamaan kyseisen aliverkon nimeä. Rajapintojen numerointi asetetaan myös vastaamaan kyseisen aliverkon VLAN numeroa asioiden selkeyttämisen vuoksi. Tämä ei ole edellytys toteutuksen toimimiselle.

Konfiguroidaan vastaava toteutus CE2-reitittimelle:

```
CE2(config)#interface GigabitEthernet0/1
CE2(config-if)#no shutdown

CE2(config)#interface GigabitEthernet0/1.1
CE2(config-subif)#description OFFICE
CE2(config-subif)#encapsulation dot1Q 1 native
CE2(config-subif)#ip address 10.10.10.2 255.255.255.0

CE2(config)#interface GigabitEthernet0/1.2
CE2(config-subif)#description GUEST
CE2(config-subif)#encapsulation dot1Q 2
CE2(config-subif)#ip address 10.10.20.2 255.255.255.0
```

Toimiakseen tämä toteutus edellyttää, että linkin toisessa päässä olevalle kytkimelle on luotu kyseiset VLAN:t ja että reitittimille menevät portit on konfiguroitu trunkeiksi. Tämä käydään läpi luvussa 5.3.4.

Reitityksen luomiseen käytetään tässä toteutuksessa dynaamista OSPF reititysprotokollaa. Verkon reunareitittimille määritellään myös staattinen oletusreitti, joka ohjaa kaikki tunnistamattomat IP-paketit haluttuun suuntaan.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1

CE2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
```

Kyseiset komennot määrittelevät, mistä portista ohjataan eteenpäin ne IP-paketit, joille ei ole olemassa muuta reittiä. Toisin sanoen kaikki liikenne, jolle ei ole määritelty reittiä ohjataan reunareitittimiltä Internetin suuntaan.

Seuraavaksi reitittimillä otetaan käyttöön OSPF-protokolla, joka luo reitit sellaisten verkkojen välille, johon laitteella ei ole paikallista yhteyttä. Käyttämällä dynaamista reititysprotokollaa säästytään ylimääräiseltä työltä sekä karsitaan inhimilliset virheet pois. Staattisilla reiteillä voidaan luoda pieniä verkkoja, mutta suuremmissa kokonaisuuksissa virheet ovat lähes väistämättömiä. Verkon laajentaminen on myös huomattavasti työläämpää, jos käytössä ei ole reititysprotokollaa.

Konfiguroidaan OSPF, prosessinumero 1, area 0:

```
INTERNET(config)#router ospf 1
INTERNET(config-router)#network 10.0.0.0 0.255.255.255 area
0
INTERNET(config-router)#network 192.168.0.0 0.0.255.255 area
0

CE1(config)#router ospf 1
CE1(config-router)#network 10.0.0.0 0.255.255.255 area 0
CE1(config-router)#network 192.168.0.0 0.0.255.255 area 0
CE1(config-router)#default-information originate
CE1(config-router)#passive-interface GigabitEthernet0/0

CE2(config)#router ospf 1
CE2(config-router)#network 10.0.0.0 0.255.255.255 area 0
CE2(config-router)#network 192.168.0.0 0.0.255.255 area 0
CE2(config-router)#default-information originate
CE2(config-router)#passive-interface GigabitEthernet0/1
```

Prosessinumerolla ei ole toiminnan kannalta mitään merkitystä ja se voi olla vaikkapa eri jokaisella verkon reitittimellä. Network-rivin lopussa oleva area numero täytyy kuitenkin täsmätä niiden verkkojen osalta, joihin OSPF-protokollalla halutaan reitit luoda.

Verkkoja määriteltäessä tavallisen aliverkkomaskin sijaan OSPF-konfiguraatiossa käytetään niin sanottua wildcard-maskia, jolla määritellään, mitä oktetteja verkko-osoitteesta otetaan huomioon. Tämä tarkoittaa sitä, että yllä olevilla riveillä konfiguroidaan kaikki 10.x.x.x ja 192.168.x.x verkot mainostumaan OSPF:n kautta.

Wildcard 0.0.0.0: Huomioi kaikki 4 oktettia. Toisin sanoen numeroiden tulee olla täsmälleen samat.

Wildcard 0.0.0.255: Huomioi ensimmäiset 3 oktettia.

Wildcard 0.0.255.255: Huomioi ensimmäiset 2 oktettia.

Wildcard 0.255.255.255: Huomioi vain ensimmäinen oktetti.

Wildcard 255.255.255.255: Ei huomio mitään. Toisin sanoen kaikki osoitteet täsmäävät network-lauseeseen.

CE1- ja CE2-reitittimelle konfiguroitu `default-information originate` komento ottaa käyttöön aikaisemmin määritetyn staattisen oletusreitin myös OSPF-protokollan alla.

Reunareitittimillä on konfiguroitu myös lähiverkkoon osoittavat portit passiivisiksi. Tämä tarkoittaa sitä, että OSPF ei yritä muodostaa naapureita tai lähettää reititykseen liittyvää informaatiota turhaan lähiverkon suuntaan. Tällä toimenpiteellä vähennetään turhaa työtä ja vähennetään reitittimen kuormaa (cisco.com, 2012).

6.3.2 HSRP-konfigurointi

Hot Standby Router Protocol otetaan käyttöön verkon reunareitittimillä CE1 ja CE2. Käytetään konfigurointiin kahta HSRP-ryhmää 1 ja 2, jotka vastaavat verkossa olevia verkkoja VLAN1 ja VLAN2. Konfigurointi tapahtuu reitittimellä samassa rajapinnassa, jossa aliverkot määriteltiin.

Konfiguroidaan VLAN1:lle HSRP:

```
CE1(config)#interface gigabitEthernet0/0.1
CE1(config-subif)#standby 1 version 2
CE1(config-subif)#standby 1 ip 10.10.10.100
CE1(config-subif)#standby 1 priority 150
CE1(config-subif)#standby 1 preempt
CE1(config-subif)#standby 1 timers 1 4

CE2(config)#interface gigabitEthernet0/1.1
CE2(config-subif)#standby 1 version 2
CE2(config-subif)#standby 1 ip 10.10.10.100
CE2(config-subif)#standby 1 priority 145
CE2(config-subif)#standby 1 preempt
CE2(config-subif)#standby 1 timers 1 4
```

Jokaisella standby-ryhmällä on oma aktiivinen ja passiivinen reititin. Yllä olevilla riveillä määritellään CE1-reitittimen priority-arvo isommaksi, kuin CE2, joten siitä tulee verkon aktiivinen reititin.

Mikäli verkossa tulee ongelmia ja pääyhteys CE1-reitittimen kautta ei jostain syystä toimi, niin priority-arvo laskee oletusarvoisesti 10:llä, jolloin CE2-reitittimestä tulee tässä tapauksessa verkon aktiivinen reititin. Tähän muutokseen vaikuttavat timers-määritykset, jotka ovat yllä konfiguroitu erittäin pienillä arvoilla, jotta muutos tapahtuisi mahdollisimman nopeasti. Preempt-rivi kertoo laitteille sen, että mikäli molemmat laitteet ovat toimintakunnossa, niin suuremman priority-arvon omaava laite on aina aktiivinen. Jos kyseistä riviä ei ole konfiguroitu, niin aktiiviseksi laitteeksi asettuu se, kumpi käynnistyy nopeammin.

Komento `standby 1 ip` määrittelee halutulle aliverkolle virtuaalisen gateway-osoitteen, joka pysyy aina samana riippumatta siitä kumman reitittimen kautta liikenne kulkee. Toisin sanoen kyseisen aliverkon työasemille voidaan määritellä dgw-osoitteeksi aina sama osoite riippumatta siitä, mikä on verkon aktiivinen reititin. Osoitteen tulee toki olla samasta IP-osoiteavaruudesta kyseisen aliverkon kanssa.

Konfiguroidaan vastaavasti VLAN2:lle HSRP:

```
CE1(config)#interface gigabitEthernet0/0.2
CE1(config-subif)#standby 2 version 2
CE1(config-subif)#standby 2 ip 10.10.20.100
CE1(config-subif)#standby 2 priority 150
CE1(config-subif)#standby 2 preempt
CE1(config-subif)#standby 2 timers 1 4

CE2(config)#interface gigabitEthernet0/1.2
CE2(config-subif)#standby 2 version 2
CE2(config-subif)#standby 2 ip 10.10.20.100
```

```
CE2(config-subif)#standby 2 priority 145
CE2(config-subif)#standby 2 preempt
CE2(config-subif)#standby 2 timers 1 4
```

Kuten huomataan, niin myös toisen virtuaaliverkon (VLAN2) osalta verkon aktiiviseksi reitittimeksi määritellään CE1.

6.3.3 DHCP-konfigurointi

Otetaan DHCP-palvelu käyttöön ja määritellään DHCP-alueet verkon INTERNET-reitittimellä. Käytännössä tämä tarkoittaa sitä, että lähiverkkoon kytketyille työasemille jaetaan IP-osoitteet automaattisesti niille määritetyistä osoiteavaruuksista.

```
INTERNET(config)#ip dhcp pool OFFICE
INTERNET(dhcp-config)#network 10.10.10.0 255.255.255.0
INTERNET(dhcp-config)#default-router 10.10.10.100

INTERNET(config)#ip dhcp pool GUEST
INTERNET(dhcp-config)#network 10.10.20.0 255.255.255.0
INTERNET(dhcp-config)#default-router 10.10.20.100
```

Osoiteavaruudet on määritelty ja nimetty vastaamaan käytössä olevia aliverkkoja.

Jotta DHCP-palvelu saadaan toimimaan, täytyy CE1- ja CE2-reitittimen konfiguraatioon lisätä DHCP-palvelimen osoite kunkin aliverkon rajapintaan. Tässä tapauksessahan DHCP-palvelimena toimii INTERNET-reititin.

```
CE1(config)#interface gigabitEthernet0/0.1
CE1(config-subif)#ip helper-address 192.168.0.2
CE1(config)#interface gigabitEthernet0/0.2
CE1(config-subif)#ip helper-address 192.168.0.2

CE2(config)#interface gigabitEthernet0/1.1
CE2(config-subif)#ip helper-address 192.168.1.2
CE2(config)#interface gigabitEthernet0/1.2
CE2(config-subif)#ip helper-address 192.168.1.2
```

Ip helper - osoitteeksi näin ollen konfiguroidaan kunkin reunareitittimen ja INTERNET-reitittimen välisestä linkkiverkosta INTERNET-reitittimen IP-osoite. Kun verkon DHCP on konfiguroitu oikein, työasemat saavat automaattisesti IP-osoitteen liittyessään verkkoon, mikäli työaseman verkkoasetukset on määritelty käyttämään DHCP-palvelua.

Vaikka DHCP-palvelu on käytössä, niin lähiverkossa saattaa olla laitteita, joille halutaan määritellä kiinteä IP-osoite. Tätä varten DHCP serverille voidaan konfiguroida lista IP-osoitteista, joita ei jaeta ollenkaan verkkoon DHCP:n kautta. Tämä lista konfiguroidaan Ciscon reitittimillä `ip dhcp excluded-address`–komennolla. Tässä työssä tälle toiminnolle ei ollut käyttöä, mutta alla esimerkki kuinka tätä olisi voinut käyttää:

```
INTERNET(config)#ip dhcp excluded-address 10.10.10.1
10.10.10.64
```

```
INTERNET(config)#ip dhcp excluded-address 10.10.20.1
10.10.20.64
```

Kyseiset rivit varaavat molemmista aliverkoista ensimmäiset 64 IP-osoitetta staattisiksi ja näin ollen ensimmäinen DHCP:n kautta tuleva osoite olisi 10.10.x.65.

6.3.4 Lähiverkon konfigurointi

Työssä kuvattu lähiverkko koostuu kahdesta runkokytkimestä ja yhdestä työasemakytkimestä. Aloitetaan kytkimien konfigurointi luomalla virtuaaliverkot VLAN1 ja VLAN2.

```
CORE-SW1(config)#vlan 1
CORE-SW1(config)#vlan 2

CORE-SW1(config)#interface Vlan1
CORE-SW1(config-if)#description OFFICE
CORE-SW1(config-if)#no ip address
CORE-SW1(config-if)#no shutdown

CORE-SW1(config)#interface Vlan2
CORE-SW1(config-if)#description GUEST
CORE-SW1(config-if)#no ip address
CORE-SW1(config-if)#no shutdown
```

Samat rivit konfiguroidaan verkon kaikille kolmelle kytkimelle, jolloin koko lähiverkkoon saadaan käyttöön halutut aliverkot. Verkkojen osoiteavaruudet on määritelty reunareitittimien loogisissa rajapinnoissa, joten kytkimillä ei tarvitse kuin luoda VLAN:t, aktivoida ne `no shutdown`–komennolla sekä määrittää niille ylläpidon kannalta järkevät nimet.

Tässä työssä toisena virtuaaliverkkona käytetty VLAN1 on laitteiden oletus VLAN, joka yleensä jätetään tuotantoverkoissa käyttämättä. VLAN1 suljetaan sen takia, ettei työasemia liitetä vahingossa oletusverkkoon. Kytkinportit ovat oletusarvoisesti liitettynä VLAN1-verkkoon. Testiympäristössä VLAN1:n käyttö onnistuu kuitenkin ongelmitta.

Tavallisesti tuotantoverkkoihin on järkevää määritellä myös oma VLAN hallintayhteyksiä varten. Tämä tarkoittaa sitä, että verkon jokaiselle aktiivilaitteelle määritellään hallintaosoite etäyhteyksiä varten. Tämän työn osalta hallintaverkko ei ole tarpeen, sillä laboratorioympäristössä laitteisiin päästään käsiksi konsoliyhteydellä.

Seuraavaksi aktivoidaan fyysiset portit ja määritellään niiden käyttötarkoitus. Työ aloitetaan lähiverkon runkokytkimiltä, joihin ei tässä topologiassa määritellä lainkaan access- eli työasemaportteja.

```
CORE-SW1(config)#interface gigabitEthernet0/1
CORE-SW1(config-if)#description TRUNK to CE1
CORE-SW1(config-if)#switchport mode trunk
CORE-SW1(config-if)#switchport trunk allowed vlan add 1,2
CORE-SW1(config-if)#no shutdown

CORE-SW1(config)#interface gigabitEthernet0/2
```

```
CORE-SW1(config-if)#description TRUNK to CORE-SW2
CORE-SW1(config-if)#switchport mode trunk
CORE-SW1(config-if)#switchport trunk allowed vlan add 1,2
CORE-SW1(config-if)#no shutdown

CORE-SW1(config)#interface fastEthernet0/24
CORE-SW1(config-if)#description TRUNK to LAN-SW1
CORE-SW1(config-if)#switchport mode trunk
CORE-SW1(config-if)#switchport trunk allowed vlan add 1,2
CORE-SW1(config-if)#no shutdown

CORE-SW1(config)#interface range fastEthernet0/1-23
CORE-SW1(config-if)#description VAPAA TRUNK
CORE-SW1(config-if)#switchport mode trunk
CORE-SW1(config-if)#shutdown
```

Yllä olevassa konfiguraatiossa avataan CORE-SW1-kytkimeltä tarvittavat portit ja määritellään ne VLAN-trunkeiksi. Verkon molemmista virtuaaliverkoista sallitaan liikenne kaikkien aktiivisten trunk-porttien läpi. Kaikkiin portteihin lisätään sen käyttötarkoitusta vastaava kuvaus. Kaikki muut tässä vaiheessa tarpeettomat tai muuten käyttöä vaille jäävät portit suljetaan. Samat rivit konfiguroidaan verkon toiselle runkokytkimelle CORE-SW2. Muutetaan ainoastaan porttien kuvaukset täsmäämään niiden käyttötarkoitusta. Ylläpidon kannalta varsinkin runkokytkimiltä on hyvän tavan mukaista sulkea ylimääräiset portit, ettei verkkoon liitetä laitteita niistä ilmoittamatta.

Lähiverkon ainoalla työasemakytkimellä (LAN-SW1) liittymät runkoverkon suuntaan määritellään trunkeiksi. Loput portit jaetaan tasan virtuaaliverkkojen (VLAN1 ja VLAN2) kesken päätelaitteita varten. Trunkportit avataan, jotta liikennöinti aliverkoista onnistuu kytkimeltä eteenpäin:

```
LAN-SW1(config)#interface gigabitEthernet0/1
LAN-SW1(config-if)#description TRUNK to CORE-SW1
LAN-SW1(config-if)#switchport mode trunk
LAN-SW1(config-if)#switchport trunk allowed vlan add 1,2
LAN-SW1(config-if)#no shutdown

LAN-SW1(config)#interface gigabitEthernet0/2
LAN-SW1(config-if)#description TRUNK to CORE-SW2
LAN-SW1(config-if)#switchport mode trunk
LAN-SW1(config-if)#switchport trunk allowed vlan add 1,2
LAN-SW1(config-if)#no shutdown
```

Määritellään portit, joihin kytketyt työasemat halutaan liittää ns. OFFICE-aliverkkoon eli VLAN1:

```
LAN-SW1(config)#interface range fastEthernet0/1-10
LAN-SW1(config-if)#description OFFICE
LAN-SW1(config-if)#switchport mode access
LAN-SW1(config-if)#switchport access vlan 1
LAN-SW1(config-if)#no shutdown
```

Konfiguroidaan halutut portit GUEST-verkkoon eli VLAN2:

```
LAN-SW1(config)#interface range fastEthernet0/11-20
LAN-SW1(config-if)#description GUEST
LAN-SW1(config-if)#switchport mode access
```

```
LAN-SW1(config-if)#switchport access vlan 2
LAN-SW1(config-if)#no shutdown
```

LAN-SW1-kytkimellä on vielä 4 porttia konfiguroimatta, jotka jätetäänkin tällä hetkellä vapaiksi. Vapaaksi jätetyt portit on varattu lähiverkon laajennusta varten ja niitä voidaan käyttää esimerkiksi silloin, jos kaapelointi verkkoon liitettävälle kytkimelle on järkevämpää suoraan tältä kytkimeltä eikä rungon kautta. Pienissä kohteissa tämä on käytännöllistä, mutta tavallisesti työasemakytkimiä ei kannata liikaa ketjuttaa peräkkäin verkon optimoinnin kannalta.

```
LAN-SW1(config)#interface range fastEthernet0/21-24
LAN-SW1(config-if)#description VAPAA TRUNK
LAN-SW1(config-if)#switchport mode trunk
LAN-SW1(config-if)#shutdown
```

STP on olennainen osa vikasietoista lähiverkkoa ja sen avulla pystytään luomaan kytkimien välille varmentavia linkkejä ilman silmukoiden muodostumista. Määritellään CORE-SW1 tämän lähiverkon pääkytkimeksi, mikä tarkoittaa sitä, että liikenne kulkee aina sen kautta, kun se on mahdollista.

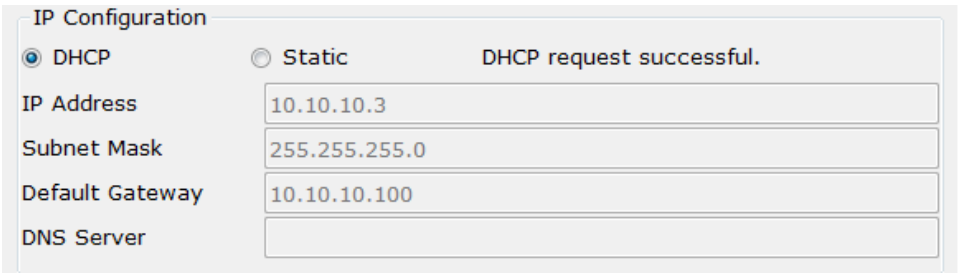
```
CORE-SW1(config)#spanning-tree vlan 1-2 root primary
CORE-SW1(config)#spanning-tree mode rapid-pvst

CORE-SW2(config)#spanning-tree vlan 1-2 root secondary
CORE-SW2(config)#spanning-tree mode rapid-pvst
```

Määrittelyissä käytetään VLAN-kohtaista STP-konfiguraatiota ja muutetaan sen tilaksi rapid eli nopea. `spanning-tree mode rapid-pvst` rivi konfiguroidaan myös verkon työasemakytkimelle LAN-SW1, jotta saadaan verkon kaikki kytkimet samaan tilaan. Yllä olevien konfiguraatioiden perusteella tässä verkkotopologiassa (Kuva 1.) STP asettaa LAN-SW1-kytkimen toisen trunk-portin Gi0/2 estotilaan eikä salli mitään liikennettä sen lävitse. Tämä tilanne säilyy niin kauan, kun CORE-SW1:n suuntaan oleva liittymä Gi0/1 on aktiivinen ja välittää liikennettä.

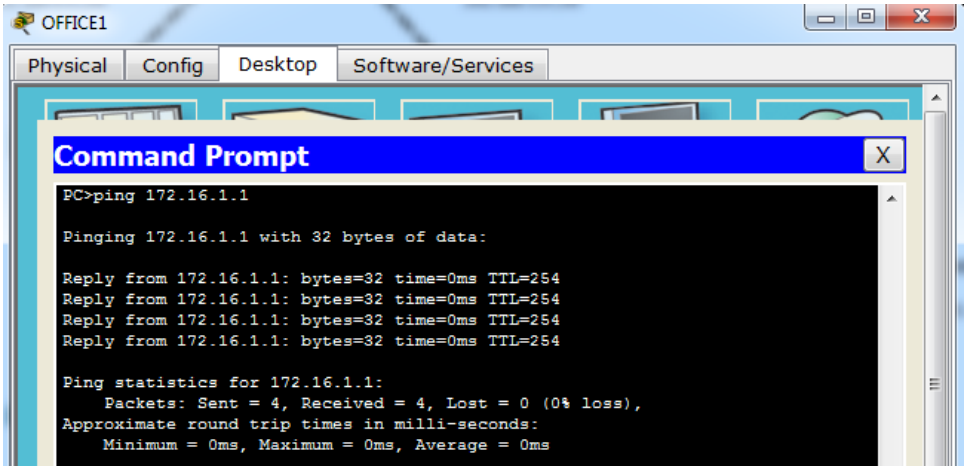
7 TESTAUS JA TULOKSET

Verkon toiminnan varmistamiseen löytyy testiympäristöstäkin muutama erittäin varma keino. Samoja keinoja voidaan käyttää myös tuotannossa oleville verkoille etäyhteyksien avulla. Toteutuksessa otettiin DHCP-palvelu käyttöön, joten liitettäessä työasemia verkkoon, niiden IP-osoitteiden määrittelemisestä ei tarvitse välittää. IP-osoitteiden määrittelyllä tarkoitetaan IP-osoitteen, aliverkkomaskin sekä oletusyhdyskäytävän asettamista päätelaitteelle.

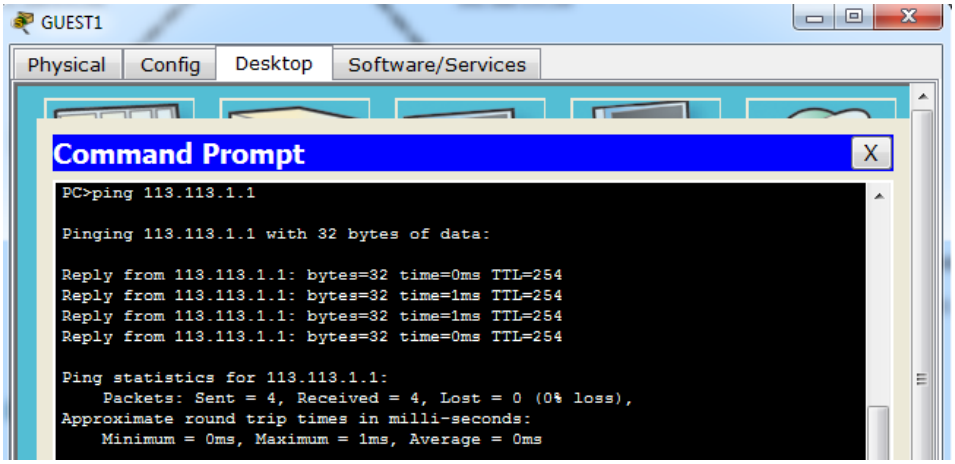


Kuva 3. OFFICE-1 työaseman IP-osoiteasetukset DHCP-palvelun kautta.

Ping-komennolla voidaan yksinkertaisesti testata yhteyksien toimimista. Komento lähettää sarjan ICMP-paketteja haluttuun IP-osoitteeseen. Pakettien lähettämisen tarkoituksena on saada kohteena oleva laite vastaamaan lähettäjän kutsuun. Mikäli yhteys on kunnossa ja jokaiseen kyselyyn tulee vastaus, voidaan todeta, että liikenne kulkee molempiin suuntiin.



Kuva 4. OFFICE-1 työasemalta ping testi Internetiin.

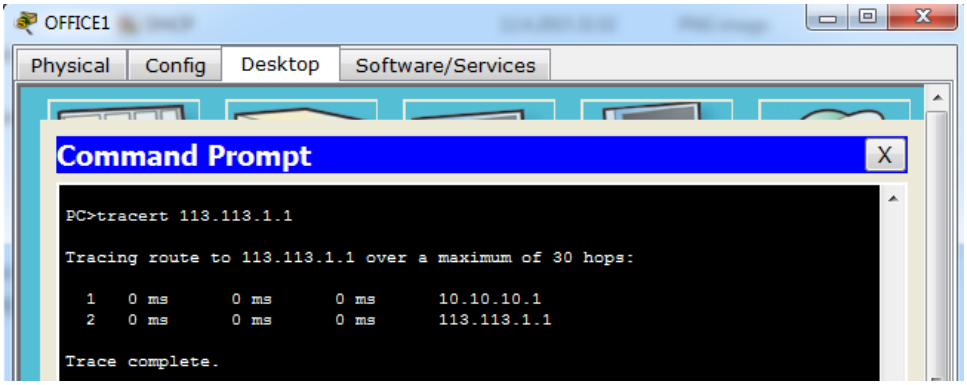


Kuva 5. GUEST-1 työasemalta ping testi Internetiin.

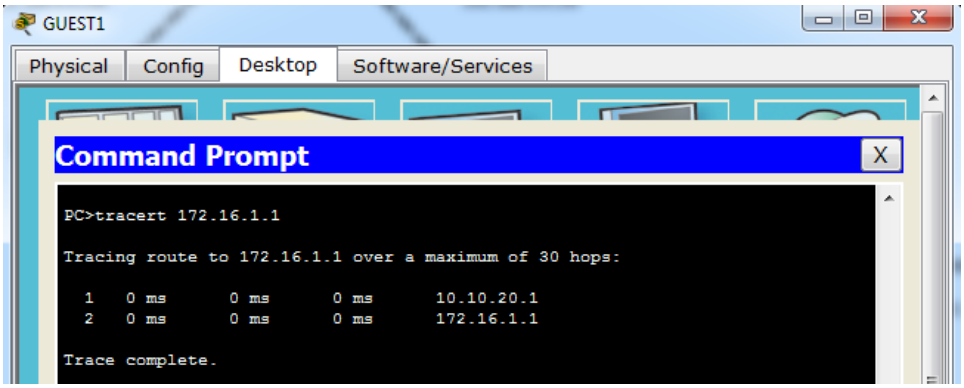
Kuvista 4 ja 5 selviää, että verkon molemmista aliverkoista on tällä hetkellä yhteys INTERNET-reitittimen Loopback-osoitteisiin, jotka kuvaavat tässä ympäristössä Internet-yhteyttä.

Traceroute (tracert) on verkon ylläpitäjälle erittäin hyödyllinen työkalu silloin, kun liikenne ei kulje halutulla tavalla ja ping – kyselyyn ei saada vastausta. Tämä komento helpottaa IP-verkon vianselvityksessä kohdistamaan viat tiettyyn pisteeseen tai laitteeseen. Silloin, kun verkko on kunnossa, niin traceroute – komento tulostaa lähteen ja kohteen välissä olevien reitittimien IP-osoitteet ja näyttää siis reitin, jota liikenne kulkee. Mikäli verkossa on vikaa, niin traceroute – komento näyttää, kuinka pitkälle paketit pääsevät tällä hetkellä kulkemaan.

Kuvissa 6 ja 7 on testattu yhteyttä lähiverkosta Internetiin tracerouten avulla:



Kuva 6. OFFICE-1 työasemalta traceroute Internetiin.



Kuva 7. GUEST-1 työasemalta traceroute Internetiin.

Kuvien perusteella voidaan todeta, että liikenne kulkee suunniteltua reittiä pääyhteyttä pitkin CE1-reitittimen kautta Internetiin. Huomataan, että traceroute – komento näyttää reitittimen VLAN-kohtaisen loogisen rajapinnan gateway-osoitteen, vaikka työaseman IP-määrittelyissä näkyy DHCP:n antama HSRP-osoite. HSRP-osoitetta voidaankin kutsua virtuaaliseksi oletusyhdyskäytäväksi.

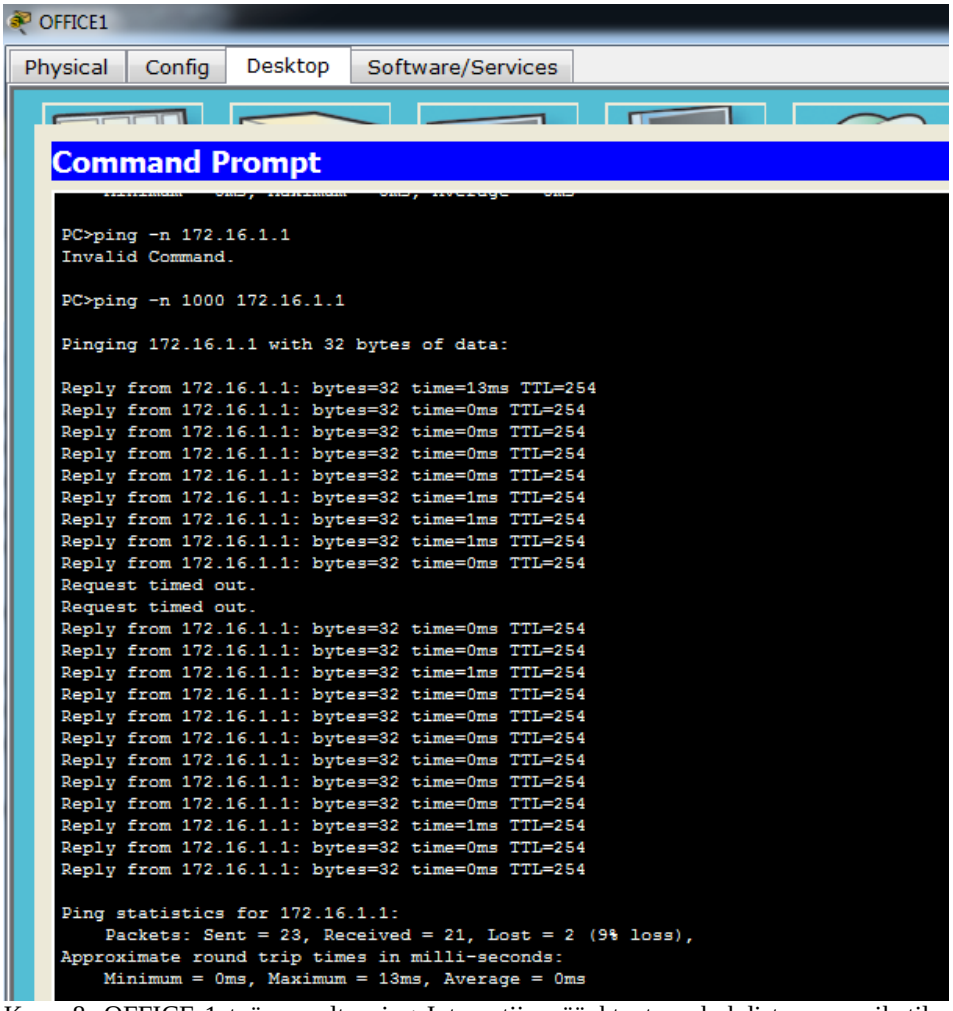
7.1 Vikatilanteet

Tämän varmennetun tietoliikenneverkon tarkoituksena oli luoda kahdennettu yhteys lähiverkosta Internetiin, joten mahdollisten vikatilanteiden testaus on ehdotonta. Luodaan muutama pääyhteyteen kohdistuva vikatilanne ja katsotaan, miten varmennus toimii. Ensimmäinen esimerkkitilanne kohdistuu reitittimiin ja toinen lähiverkkoon.

7.1.1 Laitevika runkoverkossa

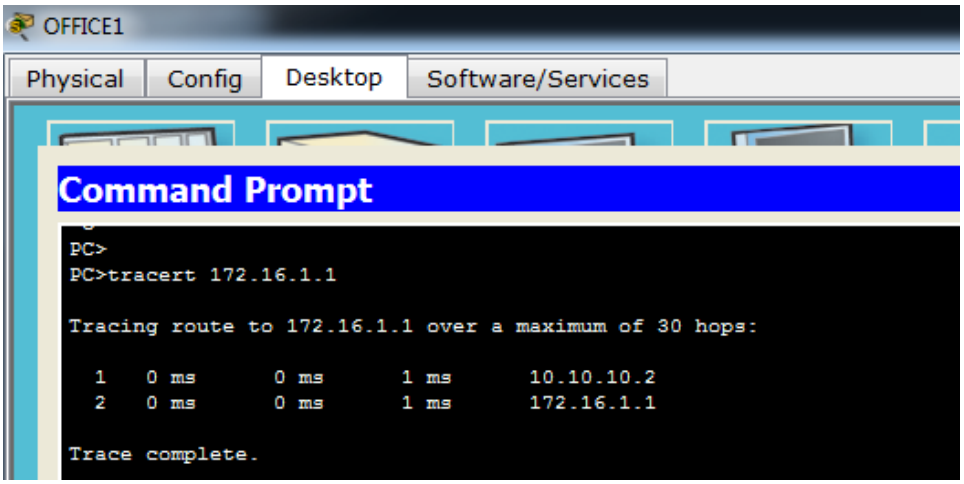
Tämän testin tarkoituksena on kuvata HSRP-kahdennuksen toimintaa reunareitittimien välillä ja seurata miten liikenne kääntyy varayhteydelle esimerkiksi sähkökatkon tai laitevian kohdistuessa CE1-reitittimeen. Tällainen tilanne demonstroi myös pääyhteyteen liittyvää kaapelikatkoa.

Käsketään lähiverkossa olevaa työasemaa pingaamaan Internet-yhteyttä toistuvasti ja otetaan samanaikaisesti CE1-reitittimeltä virrat pois. Ping –komennossa on erittäin paljon tarkentavia käskyjä riippuen käytössä olevasta käyttöliittymästä. Tässä käytetään työaseman komentokehotteen `ping -n [määrä]` syntaksia, jolla pystytään lähettämään mielivaltainen määrä paketteja haluttuun kohteeseen.



Kuva 8. OFFICE-1 työasemalta ping Internetiin pääyhteyteen kohdistuvassa vikatilanteessa.

Huomataan, että yhteyden konvergoitumisen yhteydessä kaksi pakettia menetetään. Näin lyhyttä katkosta käyttäjän on lähes mahdotonta huomata tavallisessa työympäristössä. Tämän jälkeen tehdään vielä traceroute-testi samalta työasemalta Internetiin.



Kuva 9. OFFICE-1 työasemalta traceroute Internetiin yhteyden konvergoitumisen jälkeen.

Yllä olevan tracert – tulosteen perusteella voidaan todeta, että liikenne on siirtynyt onnistuneesti kulkemaan CE2-reitittimen kautta.

Tarkastetaan tilanne vielä CE2-reitittimeltä, josta huomataan, että reititin on siirtynyt verkon aktiiviseksi reitittimeksi.

```
CE2#
%HSRP-6-STATECHANGE: GigabitEthernet0/1.1 Grp 1 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/1.2 Grp 2 state Standby -> Active

CE2#show standby
GigabitEthernet0/1.1 - Group 1 (version 2)
  State is Active
    10 state changes, last state change 00:10:40
  Virtual IP address is 10.10.10.100
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.446 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 145
  Priority 145 (configured 145)
  Group name is hsrp--1 (default)
GigabitEthernet0/1.2 - Group 2 (version 2)
  State is Active
    9 state changes, last state change 00:10:41
  Virtual IP address is 10.10.20.100
  Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.491 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 145
  Priority 145 (configured 145)
  Group name is hsrp--2 (default)
CE2#
```

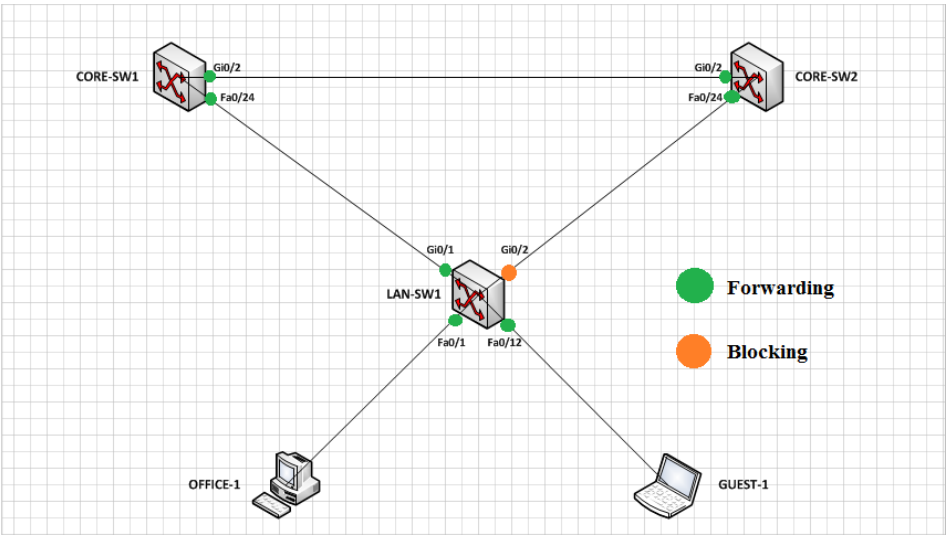
Kuva 10. HSRP tilanne CE2-reitittimellä, kun pääyhteys on poikki.

Yllä olevasta tulosteesta huomataan myös, että varalla olevaa reititintä ei tällä hetkellä ole, sillä CE1-reititin on sammutettu.

7.1.2 Ongelma lähiverkossa

Testi kohdistuu kytkimien välisen linkin katkeamiseen ja Spanning Tree -protokollan toimintaan. Todellisuudessa vika voisi syntyä esimerkiksi kahden laitteen välisen johdon irtoamisesta tai kytkimen trunk-portin sulkemisesta vahingossa.

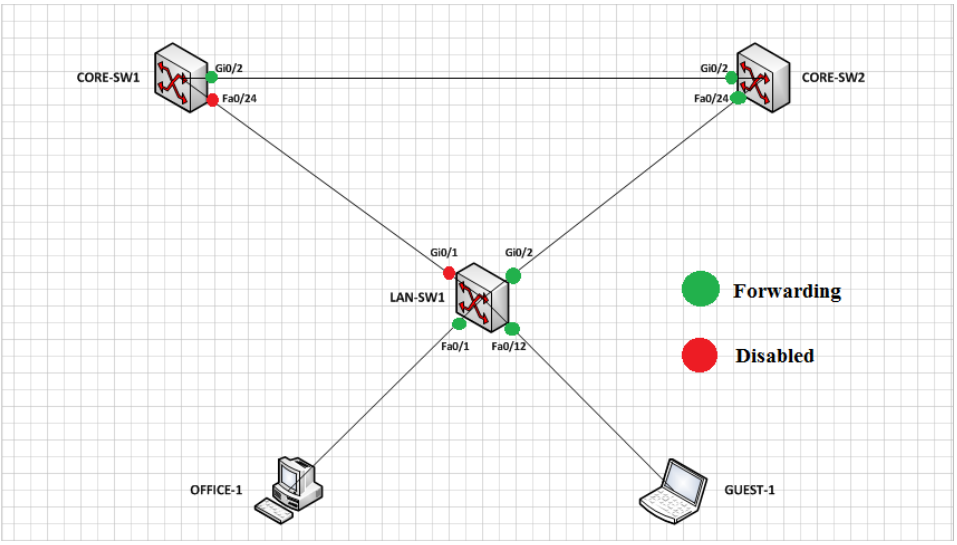
Lähtötilanteessa LAN-SW1-kytkimen Gi0/1 on liikennettä välittävässä tilassa ja Gi0/2 on estotilassa. CORE-SW1 on määritelty verkon pääkytkimeksi.



Kuva 11. Lähiverkon Spanning Tree-protokollan porttitilat lähtötilanteessa.

Laitetaan työasemalta paketteja kulkemaan Internetin suuntaan ja suljetaan LAN-SW1-kytkimen aktiivinen trunk-portti Gi0/1.

```
LAN-SW1(config)#interface gigabitEthernet0/1
LAN-SW1(config-if)#shutdown
```



Kuva 12. Porttien tilat vian kohdistuessa LAN-SW1- ja CORE-SW1-kytkimen välille.

Testistä huomataan, että kytkimen LAN-SW1 Gi0/2-portti on siirtynyt liikennettä välittävään tilaan molempien aliverkkojen osalta eikä tietoliikenteessä havaittu katkosta lainkaan. Porttimuutos tapahtuu erittäin nopeasti, sillä toteutuksessa käytetään RPVST+ - tekniikkaa.

8 YHTEENVETO JA KEHITYSMAHDOLLISUUDET

Työn tarkoituksena oli esitellä tapoja vikasietoisen verkkoympäristön luomiseen. Käytiin läpi tämän työn kannalta keskeiset tekniikat ja protokollat sekä suunniteltiin ja toteutettiin kahdennettu verkkoratkaisu. Testiympäristössä luotu verkkoympäristö saatiin kuvaamaan todellisen työelämän tilannetta kahdennetusta Internet-yhteydestä ja sen toiminnasta.

Projektin edetessä huomattiin jo työelämästäkin tuttu asia, että suunnitelmat ja dokumentit ovat verkon ylläpidon ja hallinnan kannalta todella keskeisiä asioita. Laboratoriotyön tulokset, sekä mahdolliset vikatilanteet saatiin esiteltyä kuvankaappausten kera ymmärrettävässä muodossa. Kiitos myös työnantajalleni Cinia One Oy:lle, joka tarjosi tietoliikennelaboratorion sekä tarvittavat Ciscon laitteet.

Teoksesta syntyi mielestäni ytimekäs ja ymmärrettävä kokonaisuus jokaiselle lukijalle. Työ keskittyy suurilta osin laitteiden konfigurointiin, joten sitä voidaan käyttää myös ohjekirjana. Liitteenä on jokaisen mukana olleen verkkolaitteen täydellinen konfiguraatio.

Kehitysmahdollisuudet tämän kaltaisessa työssä ovat lähes rajattomat. Verkkotopologia on suunniteltu joustavaksi ja sitä olisi mahdollista laajentaa niin lähiverkon kuin runkoverkonkin osalta. Verkon optimoinnin kannalta kehitettävää löytyy myös lähes aina.

Tärkeimpänä kehityskohteena voisin nostaa esille verkon tietoturvan sekä DNS-palvelun käyttöönoton. Tästä opinnäytetyöstä jätetiin kokonaan pois palomuurit sekä niiden vaikutus sisäverkon ja ulkoverkon toimintaan.

LÄHTEET

Hucaby, D. 2010. Cisco CCNP SWITCH 642-813 Official Certification Guide. USA: Cisco Press

Odom, W. 2013. Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide. USA: Cisco Press

VERKKOLÄHTEET:

Cisco 2012. Understanding Passive-Interface Default Command in OSPF. Viitattu 8.4.2015
https://supportforums.cisco.com/document/101591/understanding-passive-interface-default-command-ospf

How To Geek 2012. HTG Explains what is DNS. Viitattu 11.4.2015
http://www.howtogeek.com/122845/htg-explains-what-is-dns/

Microsoft 2015. What is DHCP. Viitattu 11.4.2015
https://technet.microsoft.com/en-us/library/cc781008%28v=ws.10%29.aspx

Udemy 2014. Introduction to LAN, WAN and MAN: Networking Tutorial. Viitattu 11.4.2015
https://blog.udemy.com/lan-wan-man/

Liite 1

INTERNET-reitittimen konfiguraatio

```
Building configuration...

Current configuration : 1486 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname INTERNET
!
!
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
ip dhcp pool OFFICE
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.100
ip dhcp pool GUEST
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.100
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX15244VHI
!
!
!
spanning-tree mode pvst
!
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.0
!
interface Loopback1
 ip address 113.113.1.1 255.255.255.0
!
interface GigabitEthernet0/0
 description -> CE1 gi0/1
 ip address 192.168.0.2 255.255.255.252
 ip ospf hello-interval 1
 ip ospf dead-interval 4
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description -> CE2 gi0/0
 ip address 192.168.1.2 255.255.255.252
 ip ospf hello-interval 1
 ip ospf dead-interval 4
 duplex auto
```

```
 speed auto
!
interface Serial0/1/0
 no ip address
 clock rate 56000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
line con 0
 password admin
!
line aux 0
!
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
!
end
```

Liite 2.

CE1-reitittimen konfiguraatio

```
Building configuration...

Current configuration : 1731 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CE1
!
!
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524BE2I
!
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1
 description OFFICE
 encapsulation dot1Q 1 native
 ip address 10.10.10.1 255.255.255.0
 ip helper-address 192.168.0.2
 standby version 2
 standby 1 ip 10.10.10.100
 standby 1 priority 150
 standby 1 preempt
 standby 1 timers 1 4
!
interface GigabitEthernet0/0.2
 description GUEST
 encapsulation dot1Q 2
 ip address 10.10.20.1 255.255.255.0
 ip helper-address 192.168.0.2
 standby version 2
 standby 2 ip 10.10.20.100
 standby 2 priority 150
 standby 2 preempt
 standby 2 timers 1 4
!
```

```
interface GigabitEthernet0/1
 description UPLINK TO INTERNET
 ip address 192.168.0.1 255.255.255.252
 ip ospf hello-interval 1
 ip ospf dead-interval 4
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 clock rate 64000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
ip flow-export version 9
!
!
!
!
line con 0
 password admin
!
line aux 0
!
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
!
end
```

Liite 3.

CE2-reitittimen konfiguraatio

```
Building configuration...

Current configuration : 1733 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CE2
!
!
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524366H
!
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet0/0
 description UPLINK TO INTERNET
 ip address 192.168.1.1 255.255.255.252
 ip ospf hello-interval 1
 ip ospf dead-interval 4
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.1
 description OFFICE
 encapsulation dot1Q 1 native
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 192.168.1.2
 standby version 2
 standby 1 ip 10.10.10.100
 standby 1 priority 145
 standby 1 preempt
 standby 1 timers 1 4
!
interface GigabitEthernet0/1.2
 description GUEST
 encapsulation dot1Q 2
```

```
 ip address 10.10.20.2 255.255.255.0
 ip helper-address 192.168.1.2
 standby version 2
 standby 2 ip 10.10.20.100
 standby 2 priority 145
 standby 2 preempt
 standby 2 timers 1 4
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
!
!
line con 0
 password admin
!
line aux 0
!
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
!
end
```

Liite 4.

CORE-SW1-kytkimen konfiguraatio

```
Building configuration...

Current configuration : 2891 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CORE-SW1
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1-2 priority 24576
!
interface FastEthernet0/1
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/2
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/3
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/4
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/5
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/6
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/7
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/8
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/9
```

```
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/10
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/11
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/12
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/13
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/14
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/15
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/16
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/17
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/18
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/19
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/20
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/21
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
```

```
!
interface FastEthernet0/22
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/23
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/24
 description TRUNK to LAN-SW1
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface GigabitEthernet0/1
 description TRUNK to CE1
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface GigabitEthernet0/2
 description TRUNK to CORE-SW2
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface Vlan1
 description OFFICE
 no ip address
!
interface Vlan2
 description GUEST
 no ip address
!
!
!
!
line con 0
 password admin
!
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
end
```

Liite 5.

CORE-SW2-kytkimen konfiguraatio

```
Building configuration...

Current configuration : 2891 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CORE-SW2
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1-2 priority 28672
!
interface FastEthernet0/1
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/2
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/3
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/4
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/5
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/6
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/7
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/8
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/9
```

```
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/10
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/11
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/12
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/13
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/14
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/15
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/16
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/17
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/18
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/19
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/20
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/21
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
```

```
!
interface FastEthernet0/22
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/23
 description VAPAA TRUNK
 switchport mode trunk
 shutdown
!
interface FastEthernet0/24
 description TRUNK to LAN-SW1
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface GigabitEthernet0/1
 description TRUNK to CE2
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface GigabitEthernet0/2
 description TRUNK to CORE-SW1
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface Vlan1
 description OFFICE
 no ip address
!
interface Vlan2
 description GUEST
 no ip address
!
!
!
!
line con 0
 password admin
!
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
end
```

Liite 6.

LAN-SW1-kytkimen konfiguraatio

```
Building configuration...

Current configuration : 3877 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname LAN-SW1
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
!
spanning-tree mode rapid-pvst
!
interface FastEthernet0/1
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface FastEthernet0/8
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/9
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/10
 description OFFICE
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/11
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/12
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/13
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/14
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/15
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/16
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/17
 description GUEST
```

```
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/18
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 description GUEST
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/21
 description VAPAA TRUNK
 switchport mode trunk
!
interface FastEthernet0/22
 description VAPAA TRUNK
 switchport mode trunk
!
interface FastEthernet0/23
 description VAPAA TRUNK
 switchport mode trunk
!
interface FastEthernet0/24
 description VAPAA TRUNK
 switchport mode trunk
!
interface GigabitEthernet0/1
 description TRUNK to CORE-SW1
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface GigabitEthernet0/2
 description TRUNK to CORE-SW2
 switchport trunk allowed vlan 1-2
 switchport mode trunk
!
interface Vlan1
 description OFFICE
 no ip address
!
interface Vlan2
 description GUEST
 no ip address
!
line con 0
 password admin
!
```

```
line vty 0 4
 password admin
 login
 transport input telnet
line vty 5 15
 password admin
 login
 transport input telnet
!
!
end
```