

SAVONIA

ammattikorkeakoulu

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

SOHO-SISÄVERKON SUUNNITTELU JA TOTEUTUS

TEKIJÄ Roope Taskinen

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Roope Taskinen	
Työn nimi SOHO-sisäverkon suunnittelu ja toteutus	
Päiväys 5.6.2024	Sivumäärä/Liitteet 35
Toimeksiantaja/Yhteistyökumppani(t) Datatiimi Oy	
<p>Tiivistelmä</p> <p>Tämän opinnäytetyön tarkoituksena oli suunnitella ja rakentaa SOHO (Small Office/Home Office) -verkko noin kolmen henkilön yrityksen tarpeisiin. Verkon vaatimuksia ohjasi asiakkaan määrittelemät vaatimukset verkossa käytettävistä laitteista ja ominaisuuksista sekä tietoturvallisuuteen liittyvät rajoitukset.</p> <p>Opinnäytetyössä esiteltiin lähiverkkojen teoriaa sekä niiden tietoturvallisuutta, ja se tarjoaa tilaajayritykselle mallin SOHO-verkkojen itsenäiseen toteuttamiseen ja muokkaamiseen asiakaskohtaisten vaatimusten mukaan. Työssä käytiin läpi verkon suunnittelu, toteutus ja laajentamismallit, keskittyen myös tietoturvaan ja verkon heikkojen kohtien koventamiseen.</p> <p>Lopputuloksena luotiin ja dokumentoitiin toimiva ja turvallinen SOHO-verkko hyödyntäen PPDIIO-elinkaari-mallia. Lopullinen toteutettu verkkoratkaisu vastasi yrityksen toiveita ja tarpeita.</p>	
Avainsanat SOHO-verkot, Tietoturva, LAN, WLAN, VPN	

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author(s) Roope Taskinen	
Title of Thesis Designing and Implementing a SOHO Network	
Date June 5, 2024	Pages/Appendices 35
Client Organisation /Partners Datatiimi Oy	
<p>Abstract</p> <p>The aim of this thesis was to design and build a SOHO (Small Office/Home Office) network to meet the needs of a small company with approximately three employees. The network requirements were guided by the client's specified requirements for the devices and features to be used in the network, as well as security-related restrictions.</p> <p>The thesis presented the theory of local area networks and their security, providing the client company with a model for independently implementing and modifying SOHO networks according to customer-specific requirements. The work covered the design, implementation, and expansion models of the network, focusing also on security and hardening the network's vulnerabilities.</p> <p>As a result, a functional and secure SOHO network was created and documented using the PPDIOO (Prepare, Plan, Design, Implement, Operate and Optimize) lifecycle model. The final implemented network solution met the company's desires and needs.</p>	
<p>Keywords</p> <p>SOHO-networks, network security, LAN, WLAN, VPN</p>	

SISÄLLYS

1	JOHDANTO	7
2	LÄHIVERKKO.....	8
2.1	Johdanto lähiverkkoihin	8
2.2	Lähiverkon historia, nykyisyys sekä tulevaisuus.....	8
2.3	SOHO-lähiverkko.....	8
2.4	Lähiverkon aktiivilaitteet	9
2.4.1	Palomuri.....	10
2.4.2	Reititin	11
2.4.3	Kytkin	11
2.4.4	Langaton tukiasema.....	11
2.5	Lähiverkon etäyhteydet	11
3	LÄHIVERKON TIETOTURVA	13
3.1	Palomuri.....	13
3.2	Segmentointi	13
3.3	Langattomien yhteyksien ja aktiivilaitteiden turvallisuus	14
3.3.1	Salasanat	14
3.3.2	Pääsyn rajoittaminen	15
3.3.3	Verkon salaaminen.....	15
3.3.4	SSID:n suojaaminen	16
3.3.5	Langattoman verkkolaitteiston pitäminen ajan tasalla	16
4	PPDIOO.....	17
5	LÄHIVERKON VALMISTELU JA SUUNNITTELU	19
5.1	Laittevalinnat	21
5.1.1	Reititin	22
5.1.2	Kytkin	22
5.1.3	Langaton tukiasema.....	22
5.1.4	Kustannusarvio.....	22
5.2	Kytkennot.....	22
5.3	Verkon segmentointi	23
6	LÄHIVERKON TOTEUTUS	25
7	VERKON OPEROINTI JA OPTIMOINTI	30

8	YHTEENVETO JA JOHTOPÄÄTÖKSET	32
9	POHDINTA.....	33
	LÄHTEET	34

KUVALUETTELO

Kuva 1	OSI- TCP/IP Mallit (Krimaka (2024) Osi- ja tcp/ip mallit).....	10
Kuva 2	PPDIOO Malli Maggio., A., (2018) Introducing Cisco PPDIOO for Network Design: Cisco PPDIOO is a lifecycle that repeat over time.....	17
Kuva 3	Lähiverkon suunnitelma.....	20
Kuva 4	Yleinen verkon suunnitelma laitteille, kaapeloinnille ja segmentoinnille	21
Kuva 5	Reitittimen ja kytkimen kytkennät	23
Kuva 6	Konfiguroidut VLAN verkot.....	26
Kuva 7	VLAN:eille luodut eriytetyt verkkoalueet	26
Kuva 8	Kytken VLAN-konfigurointi	26
Kuva 9	NAT konfiguraatio	27
Kuva 10	WireGuard konfigurointi.....	28
Kuva 11	VPN-konfiguraatioita.....	28
Kuva 12	VPN-konfiguraatioita.....	29
Kuva 13	WireGuard käyttöliittymän näkymä yhdistetystä tunnelista.	30
Kuva 14	VPN-yhteyden läpi työntekijän kannettavalle työasemalle etänä näkyvä yrityksen verkkolevy	31
Kuva 15	Pingaus testejä eri verkkoalueiden välillä	31

TAULUKKOLUETTELO

Taulukko 1	VPN-protokollien vertailutaulukko (Cruz 2024)	12
Taulukko 2	Kuinka kauan salasanan murtaminen kestää (Drapkin 2023).....	15
Taulukko 3	IP-osoitteistus.....	24

LYHENTEET JA KÄSITTEET

SOHO = Small Office / Home Office

LAN = Local Area Network

WLAN = Wireless Local-Area Network

IP = Internet Protocol

DHCP = Dynamic Host Configuration Protocol

ISO = International Organization for Standardization

ISP = Internet Service Provider

DoS = Denial of Service

MAC = Media Access Control

NAT = Network Address Translation

PoE = Power over Ethernet

SSID = Service Set Identifier

VLAN = Virtual Local Area Network

VPN = Virtual Private Network

WAN = Wide Area Network

WAP = Wireless Access Point

Wi-Fi = Wireless Fidelity

WPA = Wi-Fi Protected Access

ACL = Access Control List

1 JOHDANTO

SOHO eli Small Office/Home Office -verkko tarkoittaa pientä, yleensä korkeintaan 10 käyttäjän lähiverkkoa, joka sisältää toimistolle tarpeelliset verkon ominaisuudet. SOHO-verkot ovat välttämättömiä pienille yrityksille, sillä ne mahdollistavat yrityksen toiminnan kannalta olennaisten järjestelmien, kuten verkkolevyjen, web-palvelimien ja käyttäjähallinnan, toteuttamisen. Näiden verkkojen suunnittelu ja toteutus ovat kustannustehokkaita, ja ne voidaan rakentaa suhteellisen pienellä budjetilla.

Tässä opinnäytetyössä suunnitellaan ja rakennetaan SOHO-verkko noin kolmen henkilön yrityksen tarpeisiin. Työssä esitellään, miten SOHO-verkko suunnitellaan ja toteutetaan yritykselle, ja etsitään paras ratkaisuvaihtoehto verkon toteuttamiselle. Työn tarkoituksena on tarjota tilaajayritykselle malli, jonka avulla he voivat jatkossa helposti itse toteuttaa SOHO-verkkoja asiakkailleen ja mukauttaa niitä kunkin verkon vaatimusten mukaan. Lisäksi opinnäytetyössä käsitellään verkon laajentamismalleja ja sisäverkon tietoturvaan vaikuttavia tekijöitä sekä verkon koventamista.

SOHO-verkon suunnittelun ja toteutuksen teoriaosuudessa käydään läpi lähiverkkojen historiaa, nykytilaa ja tulevaisuutta, esitellään keskeiset aktiivilaitteet, kuten reitittimet, kytkimet ja langattomat tukiasemat, sekä tarkastellaan verkon tietoturvaa, kuten langattoman verkon uhkia, sekä palomuurien ja segmentoinnin merkitystä. Tämän lisäksi työssä hyödynnetään PPDIOO-kehitysmallia, joka tarjoaa rakenteellisen lähestymistavan verkon elinkaaren hallintaan suunnittelusta optimointiin.

Teoriaosuudessa lukija tutustutetaan lähiverkkojen perusteisiin ja niiden merkitykseen nykyaikaisessa työympäristössä. SOHO-verkon suunnittelu ja toteutus tarjoavat käytännön esimerkin siitä, miten pienille yrityksille voidaan luoda tehokas ja turvallinen verkko, joka tukee yrityksen liiketoimintaa ja kasvua.

2 LÄHIVERKKO

2.1 Johdanto lähiverkkoihin

Lähiverkko, josta käytetään termiä LAN (Local Area Network) on tietylle fyysiselle alueelle rajattu tietoverkko, joka yhdistää useita laitteita toisiinsa ja mahdollistaa tiedonsiirron niiden välillä. Lähiverkko voi rajautua esimerkiksi toimistoon, kampukseen tai asuntoon ja se voi yhdistää toisiinsa ja internetiin tietokoneita, tulostimia ja mobiili- tai älylaitteita. Lähiverkko ja sen tarkoituksenmukainen toimivuus on kriittisen tärkeää, sekä kodeissa, että erityisesti työpaikoilla. Lähiverkkoja on hyvin monenlaisia esimerkiksi kodissa lähiverkko voi sisältää vain yhden aktiivilaitteen, joka tukee paria mobiililaitetta, kun taas yrityksen lähiverkko voi koostua jopa kymmenistä aktiivilaitteista ja tukea kymmeniä, ellei satoja päätelaitteita. Tämä työ keskittyy SOHO-lähiverkkoon, jota voisi kuvailla jossakin määrin edellä mainittujen välimalliksi.

2.2 Lähiverkon historia, nykyisyys sekä tulevaisuus

Lähiverkkotekniikka on ollut osanamme jo pitkän aikaa mutta näiden vuosien aikana lähiverkko on saanut muuttua ja kehittyä tehokkaammaksi, sekä paremmin nykyisiä tarpeitamme täyttäväksi apuvälineeksi. Historiassa aiemmin nähdyistä verkkotopologioista huonosti nykyisiin käyttötarkoituksiin ja verkkorakenteisiin soveltuvat ovat saaneet väistyä ja toimivimmat mallit jääneet käyttöön. Nykyään lähestulkoon kaikki tyypillisimmät lähiverkot perustuvat tähtitopologiaan eikä muutosta tälle ole näkyvissä. Lähiverkon peruslaitteet ovat pysyneet melko lailla samanlaisina, joskin ominaisuudet ovat lisääntyneet valtaisesti sekä muuttuneet jatkuvasti yleisemmiksi jopa koti käyttöön tarkoitetuissa laitteissa. Langattomat yhteydet ovat lisääntyneet huomattavasti ja sama suunta jatkuu myös tulevaisuudessa. Kodin ja työpaikkojen lähiverkkoihin liittyy yhä useammin erilaisia IoT- (Internet of Things) tai muita älylaitteita, jotka tuovat lähiverkoille uusia haasteita erityisesti turvallisuuden suhteen. Lähiverkkojen kehittymisen suhteen sekä koti, että työikässä ei siis vielä näy hiljentymisen merkkejä.

2.3 SOHO-lähiverkko

SOHO-lähiverkko tulee englanninkielisistä sanoista Small Office/Home Office Network. Tyypillisesti SOHO-lähiverkossa on 1–10 käyttäjää. SOHO-lähiverkon tarkoitus on ensisijaisesti yhdistää käyttäjät ja laitteet verkkoon, sekä jakaa käyttäjille yritysverkossa toimivia resursseja, kuten tulostimen tai verkkolevyjä. Tämänlaiset verkot ovat nykyään monille yrityksille välttämättömyys, jotta yrityksen tuottavuus pysyy tehokkaana. SOHO-verkon luominen tarjoaa useita etuja. Kustannustehokkuus on yksi niistä, sillä pienehköissä SOHO-verkoissa käytettävät laitteet voivat olla hyvinkin budjettihintaisia. Tähän vaikuttaa SOHO-verkon pienet käyttäjämäärät, jotka pitävät verkkolaitteiden kustannukset alhaisina. Asennus ja konfigurointi ovat usein helppoja, sillä verkkorakenne voi olla varsin yksinkertainen ja ammattilaisen apua ei välttämättä edes tarvita. Joustavuus mahdollistaa verkkojen mukauttamisen yrityksen tai käyttäjien tarpeiden mukaan. SOHO-verkkoihin soveltuvat laitteet on yleensä suunniteltu toimimaan hyvin toimistotiloissa eikä näin ollen ole välttämättä tarvetta erilliselle laitehuoneelle, ja voi mahdollisesti helpottaa kaapelointiratkaisuissa sekä halventaa verkon luomisen hintaa. SOHO-verkot ovat näin ollen tehokas ja helppo ratkaisu pienehkön yrityksen monipuolisen verkon luomiseen jopa hyvin pienellä budjetilla. (QSFPTEK 2022.)

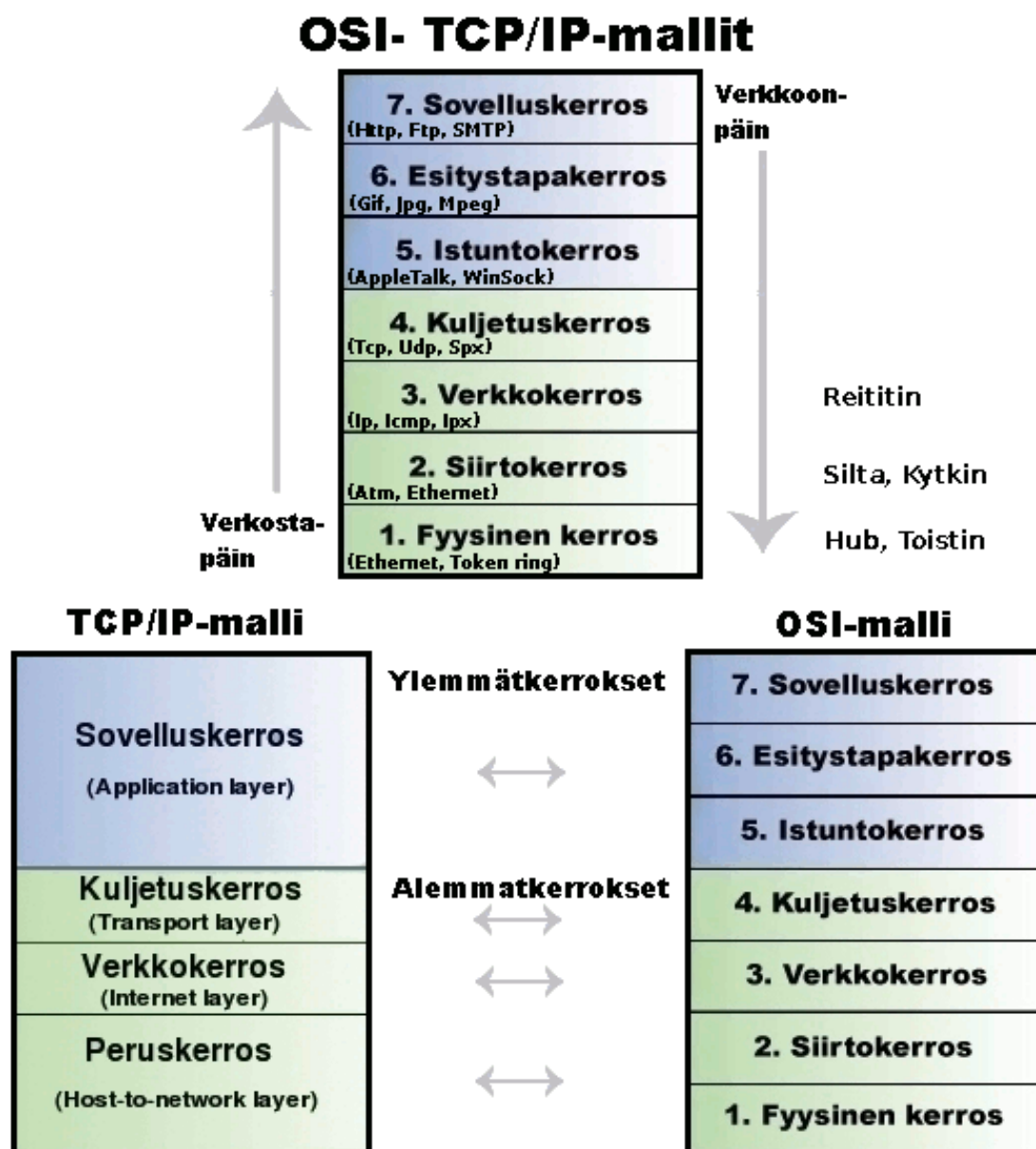
2.4 Lähiverkon aktiivilaitteet

Lähiverkko nykyisessä muodossaan vaatii tiettyjä aktiivilaitteita toimiakseen ja ollakseen käytettävissä päätelaitteille, seuraavaksi listataan laitteita, joita lähiverkko vaatii ja kerrotaan niiden toimintaperiaatteista.

SOHO-verkon luomiseen tarvitaan yleensä seuraavaksi lueteltavia laitteita. Kytkin välittää laitteiden välisen viestinnän paikallisessa verkossa ja tarjoaa tarvittavat portit laitteiden liittämiseksi verkkoon. Reititin mahdollistaa paikallisen verkon laitteiden yhdistämisen Internetiin ja varmistaa verkon turvallisuuden. Langaton tukiasema mahdollistaa langattomien laitteiden yhteyden verkkoon. Päätelaitteet, kuten tietokoneet, tulostimet ja älypuhelimet, tarvitaan työinformaation käsittelyyn ja ne liitetään verkkoon kytkimen tai langattoman verkon avulla. Nämä ovat tyypillisiä laitteita SOHO-verkon luomiseen, ja tarvittavat laitteet voivat vaihdella verkon laajuuden mukaan. (QSFPTek 2022.)

Ennen SOHO-verkon perustamista on tärkeää huomioida ympäristötekijät, kuten laitteiden sijoitus ja ilmastointi, jotta verkon toiminta olisi tehokasta ja luotettavaa. SOHO-kytkimien käyttö ilman tuuletinta vaatii hyvin ilmastoidun tilan, ja UPS:n (Uninterruptible Power Supply) hankinta on suositeltava sähkökatkosten varalta. Lisäksi on otettava huomioon laitteiden suorituskyvyn ja toiminnallisuuksien rajoitukset sekä varmistettava laitteiden yhteensopivuus, jotta verkon toiminta olisi sujuvaa ja häiriötöntä. (QSFPTek 2022.)

Verkon toiminnan ja verkkoliikenteessä tapahtuvien asioiden avaaminen aihealueesta tietämättömälle henkilölle voi olla haastavaa. Verkkolaitteiden toimintaa voidaan avata kerroksellisilla rakennelmalleilla. OSI-malli, joka on lyhenne sanoista Open Systems Interconnection Reference Model, on kansainvälisesti tunnettu ISO:n kehittämä malli, joka kuvaa tietoliikenneverkkojen liikenteen kerroksellista rakennetta. Malli on kehitetty 1980-luvun alussa ja se jakaa verkkoarkkitehtuurin seitsemään kerrokseen, joista jokainen vastaa tietyistä verkkoliikenteessä vaaditusta tehtävästä. OSI-mallin kerrokset ovat: fyysinen kerros, siirtoyhteyserros, verkkokerros, kuljetuserros, istunterros, esitystapakerros ja sovelluserros. Kukin näistä kerroksista käyttää hyväkseen itseään alemman kerroksen tarjoamia palveluita, sekä tarjoaa omia palveluitaan ylemmälle kerrokselle. Täten OSI-mallin kerrokset luovat modulaarisen ja joustavan viitekehiksen, jossa verkon viestintä tapahtuu. Vaikka OSI-malli ei ole saavuttanut yhtä laajaa käyttöä käytännön protokollapinoissa, kuin TCP/IP-malli, se toimii edelleen tehokkaana työkaluna osoittamaan tietoliikenneverkon kerrosten monimutkaisia toimintoja tarkemmalla tavalla. OSI-malli voi auttaa vähemmän verkon toimintaa tuntevia ymmärtämään eri laitteiden ja toimintojen sijoittumista verkossa. Alla olevasta kuvasta 1 nähdään verkkoliikenteen kerrokset sovelluserroksesta fyysiseen kerrokseen ja laitteiden toimintatasoja. On otettava huomioon, että OSI-malli näyttää myös monta kerrosta, jotka eivät suoranaisesti koske lähiverkossa tapahtuvia prosesseja vaan myös sovellusprosesseja, jonka dataa lähiverkko lopulta kuljettaa. (Krima 2024.)



Kuva 1 OSI- TCP/IP Mallit (Krimaka (2024) Osi- ja tcp/ip mallit)

2.4.1 Palomuuuri

Palomuuuri on laite tai ohjelmisto, joka tarkkailee ja rajoittaa verkossa tapahtuvaa liikennettä ja tarvittaessa estää sen väärinkäytösten kohdalla. Palomuuuri suojaa verkossa toimivia laitteita. Laitteisto-palomuuuri on fyysinen laite, joka toimittaa palomuurin tehtävää estämällä haitallista verkkoliikennettä tai luomalla verkolle tietynlaisia rajoja liikenteeseen. Laittepalomuurin lisäksi tietokoneet ja palvelimet omaavat monesti jonkinlaisen ohjelmistopalomuurin, joka rajoittaa verkonkäyttöä vielä itse laitteen päädysssä. Palomuuuri on erityisen tärkeä osa SOHO-verkkoa, sillä montaa eri laitetta ja käyttäjää tukevat verkot ovat vielä suuremmassa vaarassa väärinkäytösten suhteen, kuin pienet kotiverkot. OSI-mallissa palomuuuri voi toimia monella eri kerrokselle riippuen siitä, minkälaisia toimintoja palomuurilla ajetaan. (F-secure.)

2.4.2 Reititin

Reititin on keskeinen laite tietoverkossa, jonka tehtävä on ohjata verkossa paketit eteenpäin oikeaan kohteeseen. Lisäksi reititin ylläpitää reititystietoja. Reititin vastaanottaa saapuvat tietopaketit, tekee päätöksen niiden lähettämisestä eteenpäin reititystaulun avulla, sekä välittää paketin määränpäähänsä. Reitittimen tärkeys korostuu nykyisissä koti- ja yritysverkoissa, joissa sen tehtävä ei ole ainoastaan välittää tietoa ulkoverkkoon ja takaisin vaan tarjoaa myös laajan valikoiman tärkeitä toimintoja. Näitä toimintoja ovat muun muassa verkon turvallisuuden varmistaminen nykyään monesti reitittimeen sisäänrakennetun palomuurin avulla, lähiverkon laitteille IP-osoitteiden jakaminen DHCP:n (Dynamic Host Configuration Protocol) avulla, lähiverkkoon etäyhteyden muodostamisen mahdollistaminen VPN (Virtual Private Network) palvelimen avulla sekä mahdollisuudet monenlaiseen verkkoliikenteen priorisointiin tai hallintaan. Reitittimen sijoittuminen OSI-mallissa osuu kerroksiin 2 ja 3. Lisäksi on huomioitava, että L3 tason kytkin voi toimia myös reitittävänä verkkolaitteena. Linkkikerros käsittelee laitteiden välisen suoran yhteyden, kun taas verkkokerros huolehtii pakettien reitittämisestä sekä niiden eteenpäin välittämisestä laajemmassa verkkostruktuurissa. Voidaan siis todeta reitittimen merkityksen olevan olennainen nykyisten tietoverkkojen toiminnassa ja rakenteessa. (Helsingin yliopisto, 2021.)

2.4.3 Kytkin

Kytkin on tärkeä komponentti lähiverkoissa, jota käytetään kaikkien verkossa langallisesti toimivien laitteiden kytkemiseen verkkoon Ethernet-kaapeleilla ja joka edelleen lähettää paketteja niiden välillä. Kytkin mahdollistaa laitteiden keskinäisen kommunikoinnin. Kytkin toimii OSI-mallin 2. kerroksella eli linkkikerroksella, joka tarkoittaa, että se käsittelee laitteiden välistä viestintää käyttäen hyväkseen laitteiden fyysisiä MAC (Media Access Control) -osoitteita. MAC-osoitteiden ja niistä ylläpidettävän MAC-osoitetaulun avulla kytkin oppii mihin verkkolaitteisiin eri portit johtavat ja täten ohjaa liikennettä verkossa tehokkaasti. (Tietoliikenteen perusteet 2, 2021) Yksi tärkeistä ominaisuuksista, joita kytkin lähiverkossa tarjoaa, on verkon segmentointi. Tämän ominaisuuden kytkin tarjoaa VLAN-tekniikalla. VLAN-tekniikka mahdollistaa fyysisen lähiverkon jakamisen virtuaalisesta useisiin eri osiin. Tällainen lähiverkon jakaminen tuo turvaa sekä tehokkuutta verkon toimintaan. (Netgear 2022.)

2.4.4 Langaton tukiasema

Langaton tukiasema, josta käytetään monesti termiä WAP (Wireless Access Point) on laite, joka kommunikoi lähiverkossa langallisesti Ethernet-yhteydellä ja muuntaa viestinnän 2,4 tai 5 GHz:n langattomaksi signaaliksi mahdollistaen laitteiden yhdistämisen verkkoon langattomasti ja siellä muiden laitteiden kanssa kommunikoinnin. Langattomat tukiasemat ovat nykyisin yksi tärkeimmistä verkkolaitteista useissa verkoissa langattomasti liitettävien mobiililaitteiden määrän lisääntymisen myötä. (Netgear 2022.)

2.5 Lähiverkon etäyhteydet

Lähiverkoissa yleisestikin mutta erityisesti SOHO-lähiverkoissa etäyhteys on nykypäivänä välttämättömyys. Työntekijöillä tulee olla pääsy yrityksen verkkoon myös etäältä useista erillisistä syistä. Näitä syitä voivat olla esimerkiksi yrityksen lähiverkkoon käyttörajoitetut ohjelmat ja yrityksen sisäisten

verkkolevyjen käyttäminen etänä turvallisesti. Tällaisen etäyhteyden luomiseen käytetään nykyään yleisesti VPN-protokollaa. Monesti yritysverkot pitävät sisällään VPN palvelimen, joka mahdollistaa työntekijöille tai verkon hallintaan oikeutetuille henkilöille pääsyn yrityksen lähiverkkoon etänä turvallisesti. VPN on tekniikka, jonka tehtävä on suojata käyttäjän yksityisyyttä suojaamalla verkkoliikenne reitittämällä se suojatun tunnelin läpi kohteeseen. Käytännössä tämä tarkoittaa, että verkkoa käytettäessä data liikkuu loppukäyttäjän ja julkisen verkon välillä palveluntarjoajan luoman erillisen suojatun tunnelin kautta. Monelle yksityishenkilölle VPN on tuttu ulkoiselta palveluntarjoajalta ostettavana palveluna internetin käytön suojaamisen tai suoratoistopalvelujen maantieteellisten alueiden käyttörajoitusten kiertämiseen. Monille yrityksille se on kuitenkin keino yhdistää työntekijät palveluihin sekä yrityksen verkkoon turvallisesti. Monesti suuret yritykset ostavat VPN-palvelun ulkoiselta palveluntarjoajalta käyttäjien suuren määrän ja siitä johtuvan VPN-yhteyksien ylläpidon haastavuuden takia. Pienehköille yritysverkoille VPN yhteyden integrointi omaan verkkoon esimerkiksi reitittämissä toimivana ominaisuutena on kuitenkin tehokas vaihtoehto. Yrityksen verkkoon integroitavaa VPN-palvelua suunniteltaessa on otettava huomioon erilaiset VPN-protokollat. VPN-protokollia on useita erilaisia ja se määrittää kuinka data liikkuu päätelaitteen, VPN-palvelimen ja julkisen verkon välillä. VPN-protokolla määrittää yhteyden suojauksessa käytettävät metodit ja täten myös nopeuden. Luonnollisesti protokollan valinta vaikuttaa paljon myös konfiguroinnin haastavuuteen. Tunnettuja VPN-protokollia ovat seuraavat: PPTP, L2TP, IKEv2, OpenVPN ja WireGuard. Alla olevassa taulukossa 1 näkyy yksinkertaisesti tiivistettynä mainittujen protokollien merkittävimmät erot mitattuna nopeudessa, turvallisuudessa sekä käytön helppoudessa. (Cruz 2024.)

Taulukko 1 VPN-protokollien vertailutaulukko (Cruz 2024)

VPN protocols	Speed	Security	Ease of use
OpenVPN	Moderate	High	High
WireGuard	High	High	Moderate
IKEv2/IPSec	Moderate	Moderate	High
L2TP/IPSec	Moderate	Moderate	Moderate
PPTP	High	Low	High

3 LÄHIVERKON TIETOTURVA

Hyvin suunniteltuna ja turvallisesti toteutettuna lähiverkko on tehokas työväline, mutta se sisältää turvallisuusriskejä, jotka on otettava huomioon, jotta verkko pysyy turvallisena sen käyttäjille sekä organisaatiolle. Perussääntö tietoturvaan on, että mikäli laite on kytkettynä verkkoon, se on haavoittuvainen tietoturvauhille. Lähiverkon tietoturva on erittäin laaja aihealue ja tämä osuus tulee kattaamaan vain valikoidun osan lähiverkon tietoturvallisuuden ympärillä vaikuttavista asioista, jotka . Lähiverkon turvallisuutta koskevista aihealueista tärkeimpinä SOHO-verkkoja koskien pidän seuraavia aihealueita. Palomuuuri on ensimmäinen puolustuslinja verkosta tulevien uhkien ja lähiverkossa sijaitsevien laitteiden välillä. Palomuuuri antaa yleisen suojan verkosta laitteille kohdistuviin uhiin sekä mahdollisesti auttaa käyttäjien aiheuttamiin turvallisuus uhiin rajoittamalla ei-toivottua toimintaa. (Cisa 2023.) Segmentointi on myös erittäin tärkeä osa lähiverkkojen tietoturvaa ja sen merkitys on jatkuvasti kasvanut vuosien varrella verkkoon liitettävien älykkäiden laitteiden määrän kasvaessa. Segmentointi tuo verkkoon turvaa ja hallittavuutta. Yhdeksi isoista riskeistä lähiverkkojen turvallisuudelle nykypäivänä on muodostunut langattomat verkot. Langattomia verkkoja voi olla helpompi hyväksikäyttää väärin konfiguroituina juuri siitä syystä, ettei siihen tarvita fyysistä kontaktia yhteenkään verkkolaitteeseen ja laitteet, jotka on suunniteltu helpottamaan verkkoon yhdistämistä, voivat väärin konfiguroituina helpottaa verkkoon käsiksi pääsemistä myös ei-toivotuille toimijoille.

3.1 Palomuuuri

Palomuuuri on yksi lähiverkon tietoturvan tärkeimpiä palasia. Palomuurilla suojataan laajasti yleisiä uhkia esimerkiksi estämällä dataa tietyistä osoitteista, porteista tai sovelluksista. Lisäksi palomuuuri tarjoaa verkon ylläpitäjälle hälytyksiä uhkia huomatessaan, sekä tietoa mahdollisista uhista, joita verkkoon on kohdistunut. Palomuurin asetukset täytyy muokata verkon vaatimuksia vastaaviksi, mutta mahdollisimman tiukoiksi. Toisaalta palomuurin tulee kuitenkin olla ajantasaisesti ylläpidettävissä. Palomuuureja on sekä laitepohjaisia, että sovelluspohjaisia. Monia SOHO-verkkoja turvaa osittain molemmat, sillä nykyisissä reitittimissä on monesti sisäänrakennettuna laitepalomuurin ominaisuuksia ja lisäksi verkossa toimivia päätelaitteita suojaa lisäksi sovelluspohjainen palomuuuri, kuten Windows-Firewall. On kuitenkin huomioitava, että palomuuuri yksin ei tarjoa täyttä turvaa verkossa vaanivilta uhilta eikä edes hyvin konfiguroidun palomuurin turvin tuudittauduta väärään turvallisuuden tunteeseen. Palomuurit tarjoavat paljon hyviä ominaisuuksia verkon uhkien vähentämiseen, mutta ei itsessään luo täysin kattava suojaa. (Cisa 2023.)

3.2 Segmentointi

Tärkeä asia lähiverkon tietoturvassa on myös segmentointi. Segmentointi tarkoittaa sisäverkossa sitä, että fyysinen verkko jaetaan virtuaalisesti pienempiin loogisiin osioihin. Näin ollen erilleen jaetut verkot eivät voi keskustella toisille alueille jaettujen verkkojen kanssa ja myös verkkojen hallinta helpottuu. Segmentointi tapahtuu monesti pienissä ja yksinkertaisissa verkoissa hyödyntäen VLAN-tekniikkaa. Esimerkkinä voidaan ottaa seuraavanlainen tilanne. Yritys asentaa IP-kameroita verkkoonsa ja ne halutaan eriyttää muista verkossa toimivista laitteista. Tähän löytyy useita eri syitä. Mikäli kamerat joutuisivat hyökkäyksen alaisiksi esimerkiksi niiden ohjelmistosta löytyneen aukon takia, seg-

mentointi turvaisi muuta verkkoliikennettä estämällä kameroita kommunikoimasta muiden verkkolaitteiden kanssa. Lisäksi voidaan haluta estää työntekijöiden pääsy kameroihin ja eriyttää kameroiden vaatimaa kaistaa muusta verkkoliikenteestä. Segmentointia hyödyntämällä myös langattoman verkon käyttäjät voidaan sijoittaa omaan verkko-osoitteeseensa, joka parantaa verkon tietoturvasuutta. (Vmvare 2024.)

3.3 Langattomien yhteyksien ja aktiivilaitteiden turvallisuus

Langattomia verkkoja voidaan pitää vaarallisina väärin konfiguroituina. Väärin konfiguroidut langattomat yhteydet ovat uhka monella tavalla. Näihin uhkiin lukeutuu esimerkiksi verkkoyhteyden luvaton käyttäminen, tietojen urkinta ja DoS-hyökkäykset. Langattomat verkkoyhteydet voivat helposti avata tunkeutujalle tien lähiverkkoon sekä siihen yhdistettyihin laitteisiin. (Cisa 2021.) Langattomiin verkkoihin murtautumista varten on olemassa lukematon määrä helposti saatavilla olevia ja helppokäyttöisiä valmiita hyökkäysmetodeja. Mainittakoon tunnetut Evil Twin Attacks, Deauth-, sekä Handshake capture hyökkäykset. Onneksi näiden hyökkäysten riskiä voidaan minimoida verkon oikeanlaisella konfiguroinnilla. Seuraavaksi luetellaan keinoja, joita tulisi käyttää aina mahdollisuuksien mukaan langattomia verkkoja konfiguroidessa minimoidakseen keinoja hyökätä verkkoon.

3.3.1 Salasanat

Kaikkien verkkolaitteiden vakiokäyttäjätunnukset sekä salasanat tulee vaihtaa aina välittömästi käyttöönoton yhteydessä. Monet vakiotunnukset ovat helposti arvattavissa tai jopa löydettävissä internetistä. Tämän lisäksi helppojen salasanojen murtaminen eri keinoilla on yksinkertaista ja helposti toteutettavissa. Suositeltavaa olisi kriittisten verkkolaitteiden osalta käyttää erittäin monimutkaisia salasanajoja, jotka koostuvat vähintään yhdestätoista merkistä mukaan lukien pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. (Cisa 2021.) Alla oleva taulukko 2 esittää tiivistelmän salasanojen murtamiseen vaaditusta ajasta salasanojen monimutkaisuuden mukaan.

Taulukko 2 Kuinka kauan salasanan murtaminen kestää (Drapkin 2023)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

3.3.2 Pääsyn rajoittaminen

Verkon kriittisiin osiin tulisi päästää vain valtuutettuja käyttäjiä. Tämä on järjestettävissä tekemällä MAC-osoitetaulu sallituista käyttäjistä tietyillä verkonalueilla. Tämä ei ole mahdollista esimerkiksi vierailijaverkkojen kohdalla, joten tällaisissa tapauksissa tulee eriyttää erillinen vierailijaverkko ja rajoittaa verkonkäyttäjien oikeuksia. Monet laitteet tukevat automaattisesti turvallisen vierailijaverkon eriyttämistä muusta verkosta tiukennetuilla turvamenetelmillä. (Cisa 2021.)

3.3.3 Verkon salaaminen

Langattoman verkon salaaminen on yksi tärkeimpiä asioita langattoman verkon tietoturvan suhteen. Salaamiseen on olemassa monia eri protokollia ja jotkin laitteet tukevat useampaa. Vanhat laitteet voivat olla luontaisesti vaarassa, mikäli ne tukevat vain vanhentunutta salaamenetelmää eikä päivityksiä ole tiedossa. Wi-Fi Protected Access on yleisesti käytetty protokolla (WPA), joka salaa liikennettä käyttäjän ja verkkolaitteen välillä. WPA ja WPA2 ovat vanhempia versioita nykyisestä WPA3 salaamenetodista, jota olisi nykyään suositeltavaa käyttää. (Cisa 2021.) WPA ja WPA2 protokollisiin löytyy useita toimivia hyökkäysmalleja, joten mikäli käytetään vanhempia protokollia, olisi erityisesti syytä käyttää huomattavan vaikeaa salasanaa verkon salasana. Täten mahdollisesti salauksen murrettuaan hyökkääjä ei saisi helposti murrettua kaapatusta hash-koodista selkokielistä salasanaa. (HackTrick 2024.)

3.3.4 SSID:n suojaaminen

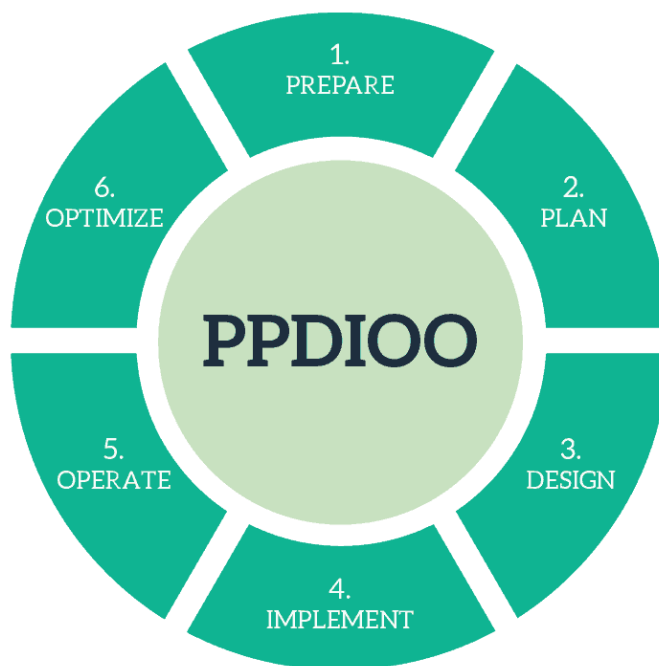
SSID (Service Set Identifier) on julkisesti kaikille langattomia verkkoja hakeville käyttäjille näkyvä verkon tunniste. SSID tulisiikin vähintään nimetä uudelleen siitä syystä, että vakio SSID-tunniste saattaa paljastaa hyökkääjälle verkkolaitteen mallin ja edesauttaa verkkoon murtautumista. Mikäli SSID:n ei ole pakko näkyä julkisesti esimerkiksi verkon ollessa vain yrityksen työntekijöiden sisäisessä käytössä on suositeltavaa piilottaa SSID kokonaan ja ohjeistaa käyttäjät etsimään verkko manuaalisesti. SSID:n piilottaminen ei piilota verkkoa täysin verkkojen monitoroinnilta mutta vaikeuttaa sen havaitsemista. (Cisa 2021.)

3.3.5 Langattoman verkkolaitteiston pitäminen ajan tasalla

Verkkolaitteiden turvallisuudesta löytyy jatkuvasti uusia heikkouksia ja aukkoja, joita hyökkääjät käyttävät hyväkseen. Tämän takia laitteiden ohjelmiston päivitysten pitäminen ajan tasalla on tärkeää. Verkosta vastuussa olevan tahon tulee tarkastella laitteiden päivitysmahdollisuuksia toistuvasti, jotta mahdolliset turvallisuus tai toiminnallisuus päivitykset pysyvät ajan tasalla. (Cisa 2021.)

4 PPDIOO

PPDIOO on Cisco:n kehittämä verkon elinkaarimalli. Tämän opinnäytetyön SOHO-verkon luomisprosessi pohjautuu soveltaen kyseisen elinkaarimallin vaiheisiin ja toimintatapoihin pienen yrityksen ja asiakaskohteen mittakaavassa. Malli on hyödyllinen elinkaarimalli kaikkiin verkon luomis- ja kehitystöihin. Elinkaarimallin käyttäminen on erityisen hyödyllistä suurissa projekteissa ja ympäristöissä, mutta sen soveltaminen myös pienempiin projekteihin ja ympäristöihin on monesti hyödyllinen tapa. PPDIOO malli sisältää mallin nimen kirjainten mukaisesti kuusi vaihetta, jotka ovat Prepare, Plan, Design, Implement, Operate ja Optimize. (Cisco Press 2010.) On tärkeää ymmärtää alla olevassa kuvassa 2 kuvattu verkon elinkaarimalli syvällisesti, jotta suunnittelu voidaan toteuttaa vaihe vaiheelta. Elinkaarimalli antaa hyvän yleisen kehyksen kehitystyölle verkon koosta ja monimutkaisuudesta riippumatta.



Kuva 2 PPDIOO Malli Maggio., A., (2018) Introducing Cisco PPDIOO for Network Design: Cisco PPDIOO is a lifecycle that repeat over time.

Verkon suunnittelussa elinkaariajattelu tuo monia etuja. Tämän menetelmän käyttämisen päätavoitteet ovat vähentää verkon ylläpidon kokonaiskustannuksia, parantaa verkon saatavuutta, lisätä liiketoiminnan nopeutta ja tehostaa sovellusten sekä palveluiden käyttöä. Kustannusten vähentämiseksi on tärkeää tunnistaa ja vahvistaa tekniset vaatimukset etukäteen, suunnitella tarvittavat muutokset infrastruktuuriin ja resursseihin, sekä kehittää verkko, joka täyttää sekä tekniset, että liiketoiminnalliset tarpeet. Verkon saatavuuden parantamiseksi on arvioitava turvallisuustilannetta, pidettävä laitteisto- ja ohjelmistoversiot ajan tasalla, sekä laadittava toimintasuunnitelma ja varmistettava verkko-

toimintojen oikeellisuus. Liiketoiminnan nopeuden lisäämiseksi pitää määritellä liiketoiminnan vaatimukset ja teknologiastrategiat, valmistella sivustoja tukemaan haluttua järjestelmää ja integroida järjestelmäkomponentit asiantuntevasti. Verkon elinkaari nopeuttaa myös pääsyä sovelluksiin ja palveluihin parantamalla toimintavalmiuksia, tehokkuutta ja vaikuttavuutta sekä hallitsemalla ja ratkaisemalla järjestelmään vaikuttavia ongelmia. (Cisco Press 2010; Petryschuk 2024.)

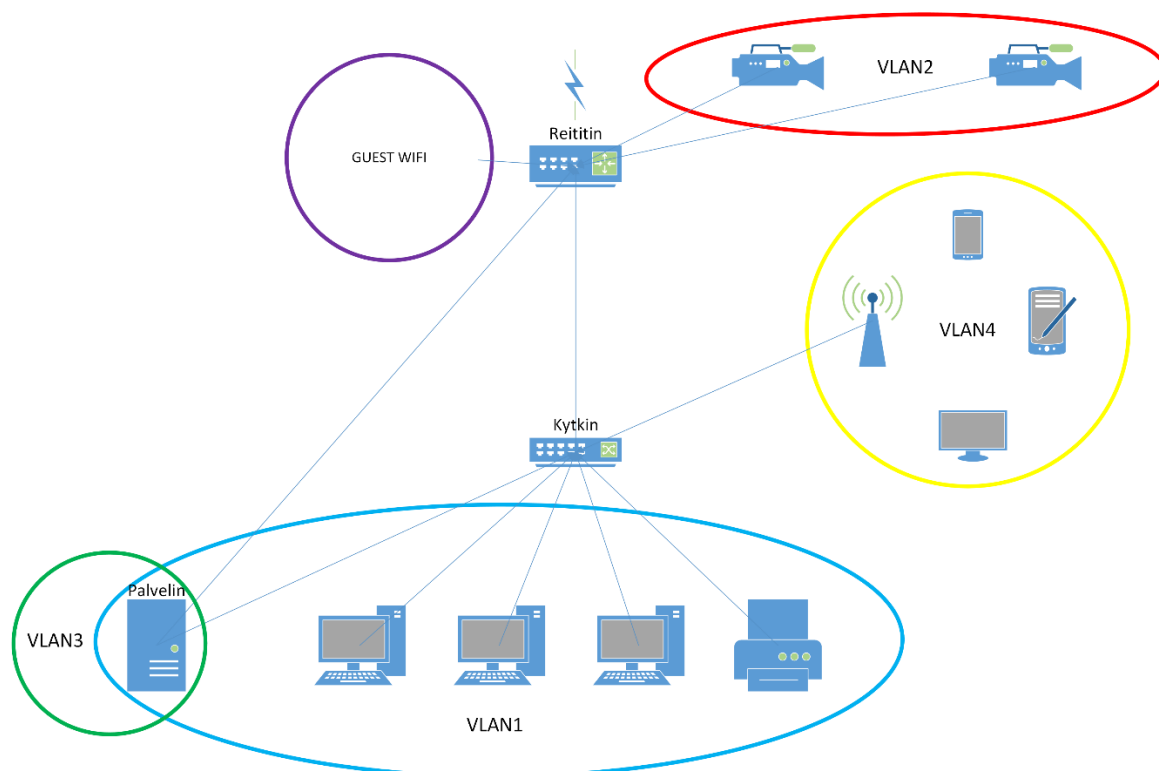
Elinkaarimallin mukainen toimiminen tarjoaa selkeitä etuja erityisesti suurissa projekteissa ja ympäristöissä. Hyvin laadittu toteutussuunnitelma on tärkeä osa onnistunutta projektia. Monimutkaisissa projekteissa varsinaisen suunnittelijan osallistuminen on välttämätöntä, mutta kun suunnitelma on selkeästi kirjoitettu, myös muut työntekijät voivat osallistua ilman, että suunnittelijan tarvitsee olla jatkuvasti paikalla. Suurissa yrityksissä suunnittelijat harvoin osallistuvat itse toteutusvaiheisiin; nämä tehtävät jäävät yleensä verkko-operaattoreiden tai toteutusinsinöörien hoidettaviksi. On myös tärkeää suunnitella, miten toimitaan, jos jotain menee pieleen, jotta voidaan palata takaisin alkuperäiseen tilanteeseen. Parhaita käytäntöjä ovat esimerkiksi vaiheiden esittäminen taulukkona ja yhteistyö kollegoiden kanssa. Toteutus sisältää useita vaiheita, kuten laitteiston asennuksen, järjestelmien määrittämisen ja käyttöönoton. Jokaiseen vaiheeseen tulee liittää tarkat ohjeet ja suunnittelu-dokumentaation viittaukset sekä ohjeet siitä, miten toimia, jos ongelmia ilmenee. Esimerkiksi, kun käyttäjiä siirretään uusiin kampuskytkimiin, suunnitelma esitetään usein taulukkomuodossa. Toteutussuunnitelman muoto ja sisältö voivat vaihdella riippuen organisaation tarpeista. (Cisco Press 2010.)

5 LÄHIVERKON VALMISTELU JA SUUNNITTELU

Lähiverkon valmistelu aloitettiin kartoittamalla kohdeyrityksen tarpeet verkon osalta. Kartoituksen pohjalta aloin suunnitella ja toteuttaa lähiverkkoa seuraavanlaisilla vaatimuksilla. Verkon tulisi sisältää seuraavanlaisia ominaisuuksia ja kykyjä. Palomuuuri, turvallinen vierasverkko, eriytetty sisäverkko henkilöstön mobiililaitteita sekä yrityksen tiloissa viihdekäytössä olevia laitteita varten, verkkotulos-tus, palvelin (jossa Web-Server, verkkolevyt henkilöstölle ja valmius käyttäjienhallintaan), kaksi verk-koon kytkettävää IP-kameraa, vähintään kolmelle henkilölle kiinteästi verkkoon yhdistetyt työpisteet, etäyhdistettävyys (VPN). Muina oletuksina verkon ominaisuuksille voitiin pitää myös staattista IP-osoitetta. Jotkin ominaisuudet, jotka projektissa tullaan luomaan vaativat staattisen IP-osoitteen. Mikäli asiakas ei pystyisi hankkimaan staattista IP-osoitetta, voitaisiin yrittää käyttää jonkinlaista dy-naamista DNS palvelua. Kartoituksen jälkeen suunnittelin alustavan suunnitelman verkon raken-teesta sisältäen yleisellä tasolla ajatuksen verkkoon vaadittavista laitteista, kytkennöistä, sekä mah-dollisesta segmentoinnista ja tietoturvakysymyksistä. Varsinaista budjettia projektiin ei tässä vai-heessa annettu, mutta tarkoituksena oli saada verkkoympäristö aikaiseksi edullisella hinnalla ajatel-len, että asiakas tulisi olemaan pieni yritys.

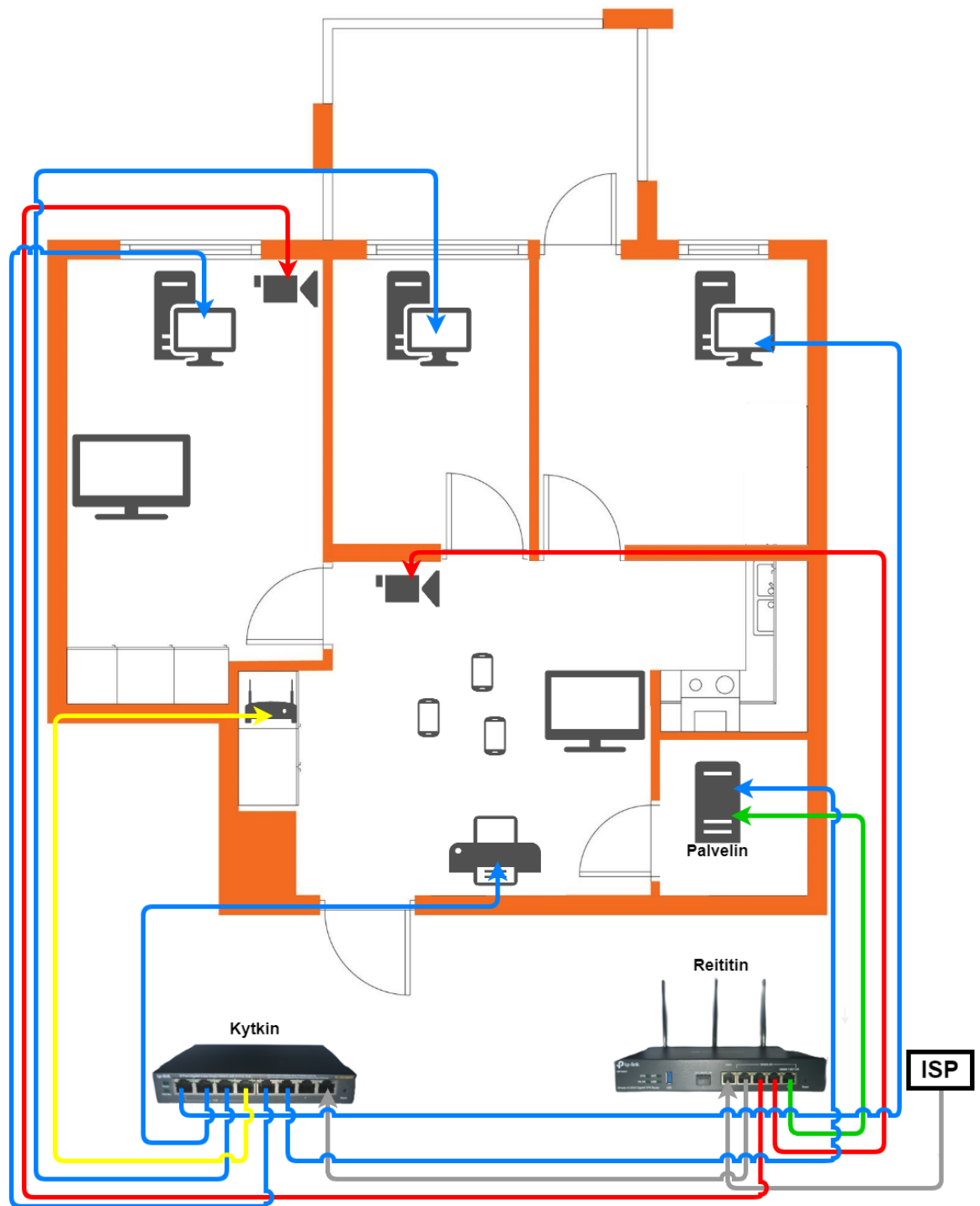
Verkon toteutusta aloitellessa, jo suunnitteluvaiheessa täytyy huomioida rakennettavan verkon vaa-timukset, jotta valitut laitteet toteuttavat vaatimukset. Tähän lukeutuu suuri määrä erilaisia huomioi-tavia tekijöitä. Näitä tekijöitä on muun muassa vaadittujen laitteiden ja ominaisuuksien vaatima porttien määrä. Porttien määrästä toteutettiin kaavio. Kaaviosta nähdään laitteiden vaatima porttien määrä, jotta osataan valita oikeanlaiset verkkolaitteet. Tähän sisältyi tässä prosessissa alustavan käsityksen mukaan kytkimen sekä reitittimen valinta, jotka toimisivat yrityskäytössä ja toteuttaisi aiemmin ilmoitetut vaatimukset. Tässä vaiheessa päätettiin, että erillistä palomuuria ei hankita, vaan reitittimessä täytyy olla sisäänrakennettuna palomuurin toiminnot. Reitittimeltä toivottuja ominai-suuksia oli myös useampi WAN-liitäntä, joista toinen olisi SFP-moduulipaikka, johon voidaan halutta-essa kytkeä valokuituyhteys. Kahden WAN-liitäntän vaatimus oli siksi, että voitaisiin tarvittaessa ot-taa kahdelta eri palveluntarjoajalta verkkoyhteys. Tällainen järjestely toteutetaan silloin, kun tahdo-taan varmistaa, että yrityksellä, työntekijöillä ja laitteilla on aina pääsy verkkoon mahdollisista ope-raattoriin kohdistuvista ongelmista huolimatta. Reitittimeltä tahdottiin ominaisuus langattomaan verkkoyhteyteen sekä tärkeänä ominaisuutena mahdollisuus VPN yhteyksiin, jotta työntekijöiden si-säverkkoon pääsy varmistetaan myös mahdollisina etätyöpäivinä. Tärkeänä määrittävänä tekijänä reitittimelle oli myös laaja konfiguraatioiden mahdollisuus sekä laajentamismahdollisuus mikäli yritys laajenisi ja tarvitsisi uusien käyttäjien tai tilojen seurauksena laajentaa verkkoaan. Lisäksi asiak-kaalta tiedusteltiin tarvetta UPS-laitteiden hankintaan, mutta lopulta ne päätettiin jättää pois tässä vaiheessa ja kartoittaa ensin UPS-tarpeet koko yrityksen kaikkien laitteiden käyttöön yhdellä kertaa.

Tässä opinnäytetyössä lähiverkon toteutukselle hinta ei ollut määrittävänä tekijänä, vaan tarkoituk-sena oli luoda mahdollisimman toimiva lähiverkko. Työssä pyrittiin kuitenkin valitsemaan hinnaltaan edullisia ja käyttötarkoitukseen parhaiten soveltuvia laitteita. Alla oleva kuva 3 havainnollistaa suun-nitelmaa verkon rakenteen, kartoituksen ja alustavan suunnittelun jälkeen. Kuvassa on myös suunni-telma segmentoinnista, kytkennöistä ja joitain verkolta vaadittuja ominaisuuksia.



Kuva 3 Lähiverkon suunnitelma

Alustavan suunnitelman jälkeen luotiin lisäksi kuvassa 4 näkyvä tarkempi verkkokaavio. Tässä kaaviossa verkko on suunniteltu fyysisesti oikeaan tilaan oikeilla laitteilla. Tästä tarkemmasta kaaviosta nähdään myös kytkennät verkkolaitteiden ja päätelaitteiden välillä, sekä suunniteltu segmentointi samoilla värikoodauksilla, kuin aiemmassa lähiverkon suunnitelmassa. Harmaat nuolet kaaviossa kuvaavat tuloliitännät verkkolaitteisiin. Toinen harmaa kaapeli kuvaa tuloliitännää operaattorilta lähiverkon reitittimelle ja toinen tuloliitännää reitittimeltä kytkimelle. Kuvassa sinisillä nuolilla kuvataan VLAN1 kuuluvien toimistolaitteiden kytkentöjä. Punaisilla nuolilla kuvataan VLAN2 kuuluvien IP-kameroiden kytkentöjä. Vihreä nuoli kuvaa palvelimen erillistä julkisen verkon operaatioita käsittelevän verkkokortin kytkentää. Keltainen nuoli kuvaa VLAN4 kuuluvan langattoman tukiaseman kytkentää. Kaaviosta löytyvät päätelaitteet joihin kuvassa ei tule kaapelia ovat langattomasti langattomaan tukiasemaan kytkettäviä laitteita, kuten älytelevisioita sekä työntekijöiden mobiililaitteita. Tällainen kaavio on erittäin hyödyllinen verkon toteutusvaihetta ajatellen ja sen pohjalta on helppo lähteä rakentamaan verkkoa. SOHO-verkon kaavio havainnollistaa niin verkon asentajalle, kuin mahdollisesti myös asiakkaallekin verkon fyysistä suunnitelmaa.



Kuva 4 Yleinen verkon suunnitelma laitteille, kaapeloinnille ja segmentoinnille

5.1 Laitevalinnat

Verkon toteuttamiseksi laitevalinnat täytyi ensin suunnitella huolellisesti. Seuraavissa alakappaleissa käydään läpi kaikki verkon toteuttamiseen vaadittavat aktiivilaitteet ja niiden valintaan vaikuttaneet vaatimukset ja ominaisuudet. Verkkoympäristön laitevaatimukset antoivat jokseenkin vapaat kädet laitteiden valintaan, sillä vaatimuksiin vastaavia laitteita on tarjolla verrattain paljon. Laitteiden valintaan vaikutti muun muassa saatavuus, hinta sekä kokemukset verkkolaitteista.

5.1.1 Reititin

Reitittimeksi valikoitui verkosta ja tukkureiden sivuilta vertailemalla TP-Link ER706W reititin. Kyseinen reititin on yritysluokan reitin, jossa on 2 WAN porttia, joista toinen SFP moduulilla, lisäksi reitittimessä on 4 LAN-porttia. Reitittimessä on sisäänrakennettu palomuuuri, langaton verkko sekä tuki VPN-yhteyksille. Lisäksi TP-Link'in yritystason reitittimet tukevat Omada-pilvihallintaa. Pilvihallittavuus on erityisen tärkeää nimenomaan silloin, jos odotettavissa on, että verkko laajenee tulevaisuudessa. Valinnan yhteydessä vertailtiin myös vastaavien reitittimien hintoja. Reitittimen hintaluokka oli noin 200 €.

5.1.2 Kytkin

Kyttimeksi projektiin valikoitui TP-Link SG108PE. Kyseinen kytkin on 8-porttinen 1000Mbps kytkin ja tukee tärkeimpiä perusominaisuuksia, joita kytkimeltä tarvitaan. Tässä tapauksessa välttämättömät ominaisuudet olivat tuki VLAN ominaisuuksiin, sekä PoE, mikäli IP-kamerat sitä vaatisivat. Kytkimen hintaluokka oli noin 50–100 €.

5.1.3 Langaton tukiasema

Langattomalle tukiasemalle vaatimukset olivat tässä tapauksessa hyvin vaatimattomat. Toiveena oli, että langaton verkko tukisi sekä 2.4GHz, että 5GHz taajuuksia. Lisäksi vaatimuksena oli jossakin määrin kelvolliset konfiguraatio mahdollisuudet, jotta verkosta saa turvallisen. Tässä tapauksessa langattoman tukiaseman rooliin valikoitui Exibel NBG6602. NBG6602 on yksityiskäyttöön suunniteltu reititin ja valikoitui projektiin ylimääräisenä laitteena hyllystä. Laitteen ominaisuudet riittivät käyttötarkoitukseen ja näin saatiin tarjottua edullinen ja tarpeeksi kyvykäs laite projektiin. Langattoman tukiaseman hintaluokka oli 50 €.

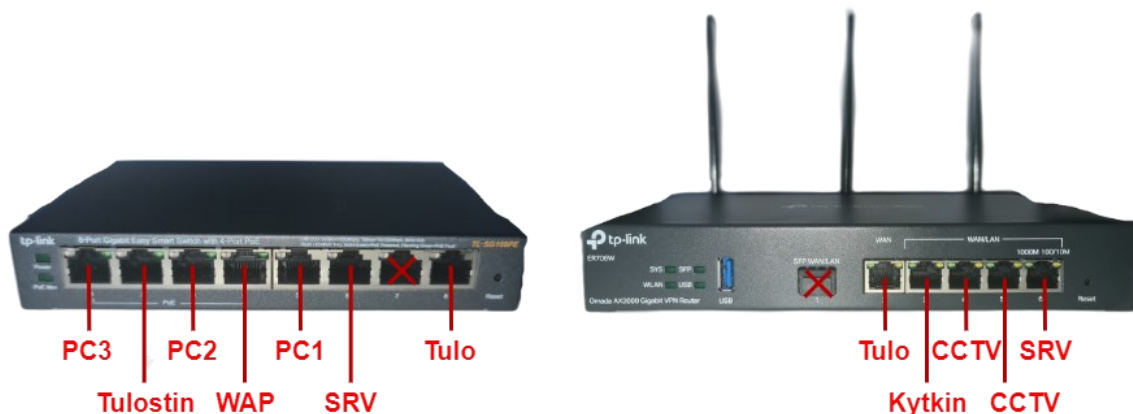
5.1.4 Kustannusarvio

Verkon kustannusarvio muodostui seuraavien tekijöiden mukaan. Laitteiden hinnat, tarvikkeiden hinnat, kaapeloinnin kulut. Tähän kustannusarvioon ei lasketa mukaan suunnittelukustannuksia, tunti-työkorvauksia, tai mahdollisia lisäkuluja eikä näin ollen vastaa projektin oikeaa laskutusta vaan on suuntaa antava arvio itse laitteiden kustannuksista verkon luomisessa. Laitteiden hinnaksi projektissa muodostuu noin 350 €. Tarvikkeiden hinnaksi muodostuu noin 100 €, sisältäen kytkentäkaapelit. Kaikki tämän verkon rakentamisessa käytettävät kaapelit ovat CAT6-luokan kaapeleita. Tässä tapauksessa oletuksena on, että kaapelointitöihin ei jouduta, sillä toimistot sijaitsevat modernissa rakennuksessa, jossa on huomioitu nykyaikaiset vaatimukset verkkoliitännöjen suhteen. Laskennallisesti voitaisiin kuitenkin laskea mahdollisia kaapelointi kuluja koituvaksi 100 € verran riippuen paljolti tiloista joihin verkko rakennetaan. Näistä summista huomataan, kuinka edullista pienelle yritykselle toimivan SOHO-verkkoympäristön rakentaminen on laitteistokuluissa. Laitteiden hinta voi jäädä hyvinkin alle 500 €, tosin se ei vastaa lopullista laskutusta kokonaisvaltaisesta työstä verkon rakentamisesta alusta loppuun.

5.2 Kytkennät

Laitteiden valinnan jälkeen tulee suunnitella, kuinka päätelaitteet kytketään verkkolaitteisiin, jotta lopputuloksessa päästään vaatimuksen mukaiseen verkkoon. Perusperiaatteena suunniteltiin, että

kytkimeen liitetään verkon toimistolaitteet, joita tässä esimerkissä olisi yhteensä kuusi kappaletta (+sisääntulo liitäntä) kolme PC:tä, tulostin, langaton tukiasema, sekä palvelimen sisäverkkoliitäntä. Nämä vievät kytkimen kahdeksasta portista seitsemän, joten kytkimeen jää yksi vapaa portti esimerkiksi yhtä uutta PC:tä varten. Reitittimeen liitettäisiin luonnollisesti verkon sisääntulo liitäntä, lähtö kytkimelle, palvelimen ulko verkkoliitäntä, sekä kaksi kappaletta IP-kameroita. Tämä veisi reitittimen kaikki liitospaikat pois lukien toisen WAN-liitäntän. Kytkentöjä havainnollistavassa kuvassa 4 "X" merkitsee toistaiseksi käyttämättä jätettyä porttia.



Kuva 5 Reitittimen ja kytkimen kytkennät

5.3 Verkon segmentointi

Segmentointi tämän verkon suhteen tulotisiin toteuttamaan seuraavalla tavalla. Reitittimen päässä luodaan kolme VLAN verkkoa. Opinnäytetyössä näytettävät VLAN verkkojen nimet ovat yksinkertaisettuja, siitä syystä, että tilaajan verkkorakenteen kaikkia tietoja ei haluta paljastaa. VLAN1, kytkimeen liitettävälle lähiverkolle. VLAN2 kahdelle IP-kameralle. VLAN3 palvelimen ulko verkkoliitäntälle. Kytkimeen luodaan yksi VLAN langattomalle tukiasemalle. Loput kytkimeen liitettävistä laitteista kuuluvat toimistolaitteille tarkoitettuun VLAN1 verkkoon. IP-osoitteistus laitteille suunniteltiin seuraavalla tavalla. Reitittimelle luotiin kolme erillistä LAN verkkoa, jotka alla olevassa taulukossa 3 on havainnollistettu ja merkattu LAN 1-3. Nuo kolme LAN verkkoa luotiin reitittimen VLAN verkkojen eriyttämistä varten.

Palvelimella on tässä tapauksessa 2 erillistä IP-osoitetta siitä syystä, että palvelimen kaksi verkkokorttia tullaan konfiguroimaan käsittelemään eri liikenteitä. Toinen verkkokortti käsittelee toimistolähiverkon liikennettä ja toinen verkkokortti käsittelee palvelimen ulkoista liikennettä, kuten esimerkiksi Web-palvelimen liikennettä. Guest-verkolle ei tarvittu miettiä erillistä eriyttämistä muusta verkosta, sillä työhön valittu reititin tarjosi automaattisesti ominaisuuden, joka rajoittaa Guest-verkon turvalliseksi muulle verkolle. Tässä tapauksessa langaton tukiasema tulotisiin konfiguroimaan jakamaan käyttäjilleen DHCP:n avulla IP-osoitteita eri osoite alueelta, tässä tapauksessa verkosta 192.168.1.0. Alla oleva taulukko 3 havainnollistaa verkon IP-osoitteistuksen suunnittelua. Laitteet on jaettu kolmelle erilliselle tunnetulle yksityiselle IP-osoitealueelle selkeyden vuoksi.

Taulukko 3 IP-osoitteistus

	Network		IP		Device	
	LAN1		192.168.0.1		Router	
			192.168.0.2		Switch	
			192.168.0.3		WAP	
			192.168.0.5		Server	
			192.168.0.10		PC1	
			192.168.0.20		PC2	
			192.168.0.30		PC3	
			192.168.0.50		Printer	
	LAN2		172.16.0.10		CCTV1	
			172.16.0.20		CCTV2	
	LAN3		10.0.0.10		Server	

6 LÄHIVERKON TOTEUTUS

SOHO-lähiverkon toteutus huolellisen suunnittelun jälkeen alkaa kaapeloinneista. Tässäkin tapauksessa huoneisto jonne verkko rakennettiin, oli jo valmiiksi kaapeloitu, kuten nykyään hyvin usein on uudemmissa huoneistoissa kiinteänä rakennustapana. Tämän takia kaapeloinnin osalta tehtäväksi jäi ainoastaan verkkolaitteiden kytkemiseksi verkonjakotauluun ja päätelaitteiden kytkemiseksi huoneiston seinissä olevien kiinteiden RJ45-rasioiden välille. Kaapeloinnin jälkeen reititin asennetaan ensimmäiseksi laitteeksi verkkoon, kytkemällä verkon tuloliitäntä reitittimen WAN-porttiin. Tämän jälkeen kytketään kytkimen lähtöliitäntä, IP-kamerat sekä palvelimen porttiin kytkettävät kaapelit oikeisiin portteihin verkonjakotaulussa. Kun nämä kytkennät on tehty, aloitetaan laitteiden konfiguraatioiden suorittaminen.

Kun kaapelointi on saatu päätökseen ja verkkolaitteet kytketty oikein, lähiverkon toteutus alkaa useilla kriittisillä konfigurointivaiheilla varmistamaan verkon tehokkuuden ja turvallisuuden. Aluksi suoritetaan yleisten ja turvallisuuteen vaikuttavien asetusten tarkastus, mukaan lukien järjestelmien päivitykset ja tietoturva-asetukset, kuten palomuurin konfigurointi. Tämän jälkeen luodaan uudet hallinnolliset tunnukset kaikkiin laitteisiin, reitittimeen, kytkimeen ja langattomaan tukiasemaan, jotta varmistetaan, että vain valtuutetut käyttäjät pääsevät muokkaamaan verkon asetuksia.

Seuraavaksi konfiguroidaan langattomat verkot; luodaan pääverkon lisäksi erillinen vierasverkko, joka rajoittaa vieraiden pääsyn vain internettiin. DHCP-palvelun asetuksia tarkistetaan, tämä sisältää leasing-listan läpikäyntiä, tunnistettujen laitteiden IP-osoitteiden lukitsemista ja tarvittaessa osoitteistuksen muokkaamista. Samalla tallennetaan tunnettujen laitteiden MAC- ja IP-osoitteet IP-MAC-sidontalistalle, mikä helpottaa laitteiden hallintaa ja turvallisuuden valvontaa.

Lisäksi luodaan verkkoon VLANit (virtuaaliset lähiverkot) eri käyttäjäryhmien tai palveluiden eristämiseksi toisistaan. Tämä parantaa, sekä turvallisuutta, että verkon suorituskykyä. VLAN konfigurointi suoritettiin 802.1Q Encapsulation protokollaa käyttäen. Alla olevassa kuvassa 6 näkyy VLAN lista reitittimeltä. Listasta käy ilmi konfiguroidut VLAN verkot sekä niihin kiinnitetyt portit. Kuvassa 7 näkyy VLAN-protokollan verkkoalueiden määritystaulukko, tuo taulukko määrittää verkkoalueet tietyille VLAN verkoille. Huomioitavaa on, että VLAN konfiguraatiota suoritettiin kahdella eri laitteella. Kuva 8 esittää kytkimen VLAN konfiguraatiota. VLAN-konfiguroinnin lisäksi päädyttiin toteuttamaan ylimääräinen verkkoliikenteen segmentointi palomuurin ACL-säännöillä, estämällä liikenne kuvan 7 mukaisen verkkoalueiden välillä, tällä pyrittiin testaamaan palomuurisääntöjen toimivuutta, sekä varmistamaan verkkojen eriyttäminen mahdollisista osittaisista konfiguraatiomuutoksista riippumatta.

VLAN List							+ Add - Delete	
<input type="checkbox"/>	ID	VLAN ID	Name	Ports	Description	Operation		
<input type="checkbox"/>	1	1	vlan1	3(UNTAG)	LAN1			
<input type="checkbox"/>	2	2	vlan2	4(UNTAG) 5(UNTAG)	LAN2			
<input type="checkbox"/>	3	3	vlan3	6(UNTAG)	LAN3			
<input type="checkbox"/>	4	4094	vlan4094	1(UNTAG)				

Kuva 6 Konfiguroidut VLAN verkot

Network List									+ Add	
<input type="checkbox"/>	ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation		
<input type="checkbox"/>	1	LAN1	1	192.168.0.1	255.255.255.0	Enabled	Disabled			
<input type="checkbox"/>	2	LAN3	3	10.0.0.1	255.255.255.0	Enabled	Disabled			
<input type="checkbox"/>	3	LAN2	2	172.16.0.1	255.255.255.0	Enabled	Disabled			

Kuva 7 VLAN:eille luodut eriytetyt verkkoalueet

TL-SG108PE 2.0

System Switching Monitoring **VLAN** QoS Help

Home

- MTU VLAN
- Port Based VLAN
- > 802.1Q VLAN
- 802.1Q PVID Setting

Global Config

802.1Q VLAN Status: Enable Apply

802.1Q VLAN Setting

VLAN (1-4094):

VLAN Name:

Tagged Ports:

☒1
☒2
☒3
☒4
☒5
☒6
☒7
☒8


Untagged Ports:

☐1
☐2
☐3
☐4
☐5
☐6
☐7
☐8

Apply

VLAN	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete VLAN
1	Default	1-8		1-8	
4	vlan4	4, 8		4, 8	Delete

Kuva 8 Kytken VLAN-konfigurointi

 Muokkaa tunnelia ✕

Nimi:

Julkinen avain:

[Interface]

PrivateKey = SNkXwtXvwgSD4RpSGwOYE/xpDeH/1w9O+yxRJDNRf3s=

Address = 192.168.1.25/24

DNS = 8.8.8.8

[Peer]

PublicKey = JI0p1PRQgrS+lkoPiKyMRH8/+vIVhOH71rOY8JoQUjg=




AllowedIPs = 0.0.0.0/0

Endpoint = 85.23.71.94:51820

☒ Estä tunnelioimaton liikenne (pääatkaisija)

Kuva 10 WireGuard konfigurointi

Wireguard + Add - Delete

<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
--	1	miembros	1420	799.7 MiB	23.7 MiB	939904	163366	51820	Enabled	  

Name:

MTU: (576-1440)

Listen Port: (1-65535)

Private Key: >ref (Optional)

Public Key:

Local IP Address:

Status: ☒ Enable

Kuva 11 VPN-konfiguraatioita

Peers

+ Add

- Delete

<input type="checkbox"/>	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
--	miembros	---	---	192.168.1.0/24	799.6 MIB	24.0 MIB	939640	163185	1 minute ago	Enabled	

Interface:

miembros

Public Key:

uzup2STmCVEEYsNDESxkl

Endpoint:

(Optional)

Endpoint Port:

(Optional, 1-65535)

Allowed Address:

192.168.1.0

/

24

Preshared Key:

(Optional)

Persistent Keepalive:

25

(0-65535)

Comment:

Surface

(0-128 characters)

Status:

☒ Enable

OK

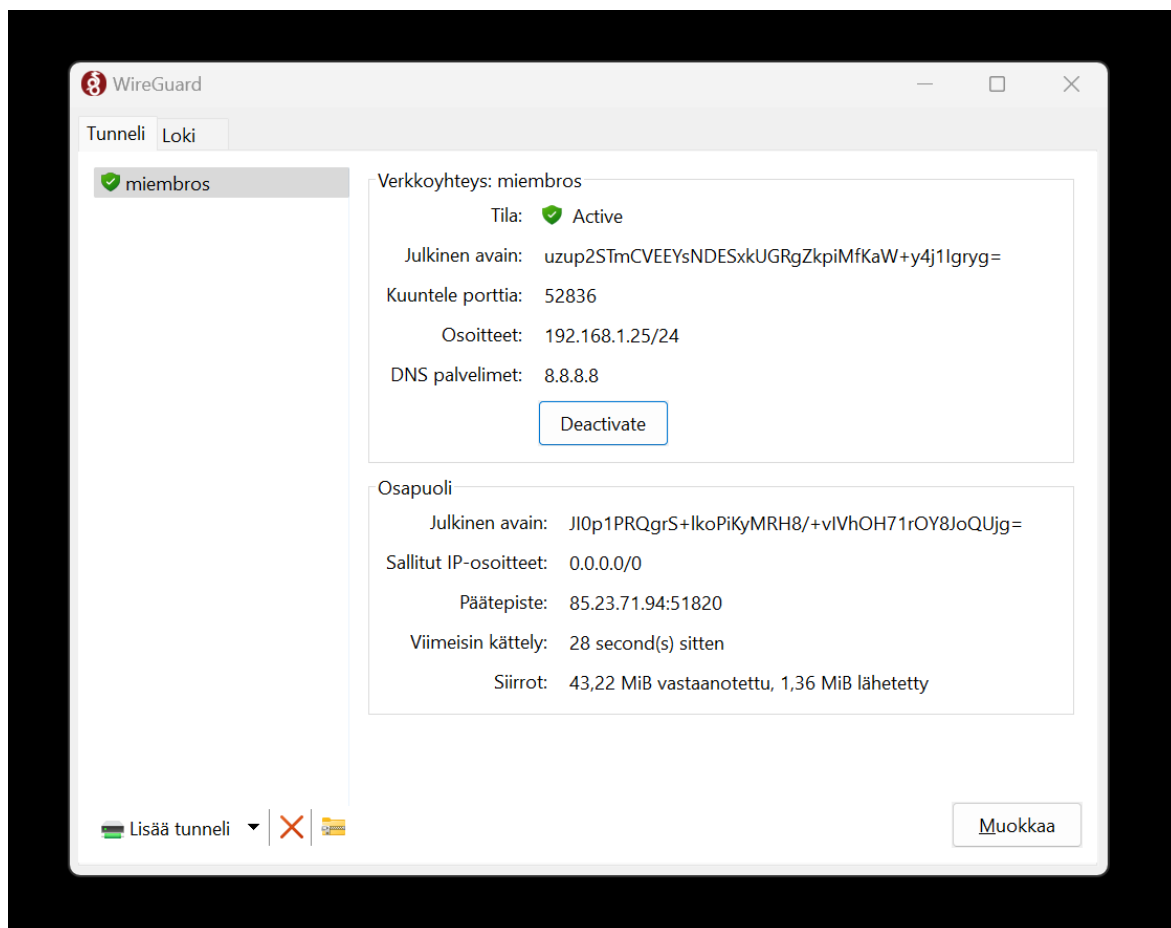
Cancel

Kuva 12 VPN-konfiguraatioita

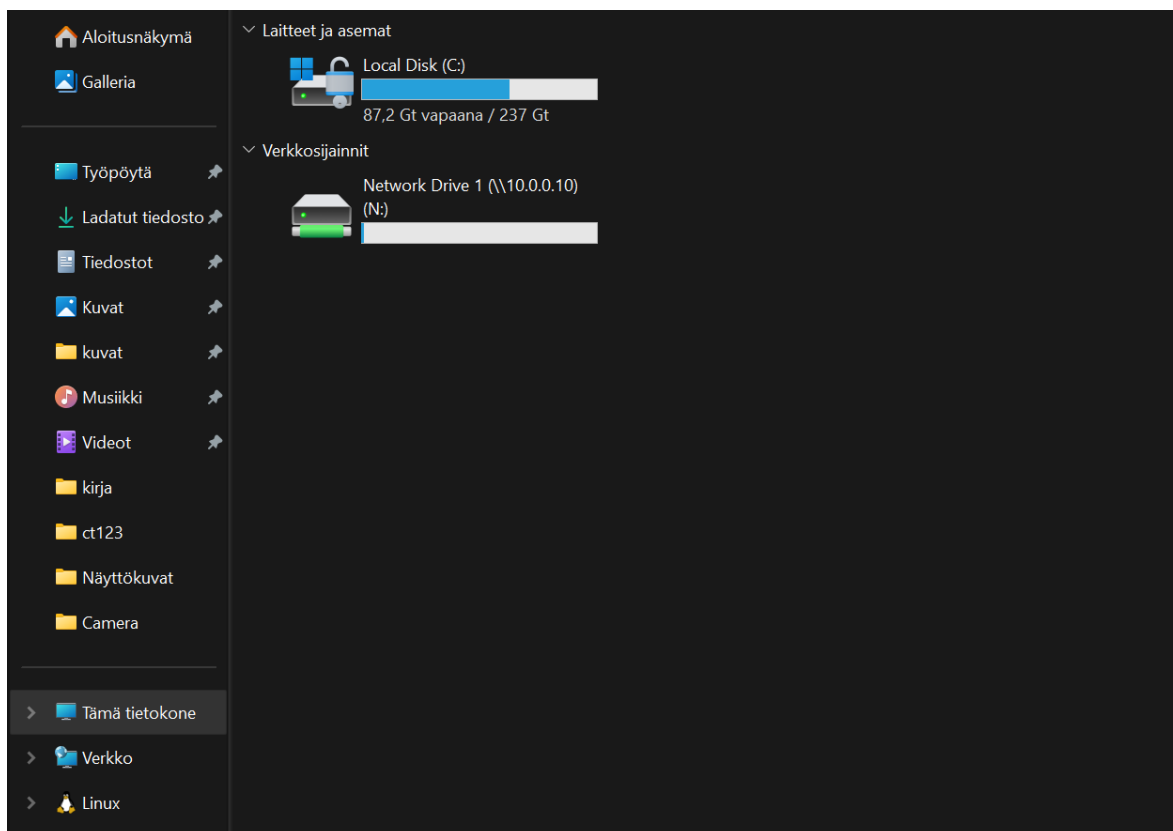
Kun kaikki nämä asetukset on viimeistely, tehdään koko verkon konfiguraatiosta varmuuskopio. Tämä mahdollistaa nopean palautumisen mahdollisista häiriötilanteista ja varmistaa, että kaikki kriittiset asetukset säilyvät muuttumattomina. Näiden toimenpiteiden myötä lähiverkko on valmis käyttöön, optimoitu suorituskyyvyltään ja suojattu mahdollisilta uhkilta.

7 VERKON OPEROINTI JA OPTIMOINTI

Konfiguraatioiden toimivuuden tarkastus voidaan tehdä tarkastamalla, että kaikki laitteet toimivat ja pääsevät verkkoon ja sen jälkeen tehdä pingaustestejä eriytettyjen verkkojen välillä, jotta voidaan olla varmoja, että laitteet ovat eriytetty onnistuneesti. Tässä vaiheessa voimme todeta verkon käyttäytymisen täysin oikein lähiverkkoon kytketyillä laitteilla. Myös VPN-yhteydellä etänä liitetyt laitteet saavat yhteyden lähiverkkoon, sekä pääsevät käyttämään yrityksen palvelimilla toimivia verkkolevyjä. Lisäksi eri verkkoalueita pingaamalla huomaamme, että segmentointi toimii toivotunlaisesti. Tämän jälkeen seuraava vaihe olisi optimointi, jota suoritetaan pitkällä aikavälillä aktiivisesti verkkoa hallinnoimalla ja etupainotteista ongelmanratkaisua suorittamalla. Optimoinnissa otetaan huomioon asiakkaan huomaamia muutostarpeita tai kehitysehdotuksia ja hallinnoidaan verkkoa toimimaan halutulla tavalla. Seuraavat kolme kuvaa kuvaavat verkon operoinnin ja optimoinnin työvaiheita. Alla olevasta kuvasta 13 nähdään että VPN-palvelimeen yhteyden luominen onnistuu toivotunlaisesti. Kuvassa 14 testataan onnistuneesti, että VPN-yhteyden kautta päästään ulkoverkosta käsiksi yrityksen verkkolevyyn toivotulla tavalla. Kuvassa 15 todennetaan pingaustesteillä, että verkkolaitteet on eriytetty toisista verkkoalueista onnistuneesti.



Kuva 13 WireGuard käyttöliittymän näkymä yhdistetystä tunnelista.



Kuva 14 VPN-yhteyden läpi työntekijän kannettavalle työasemalle etänä näkyvä yrityksen verkkolevy

```

Komentokehote
C:\Users\taski>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\taski>ping 172.16.0.10

Pinging 172.16.0.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\taski>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.10: Destination host unreachable.
Reply from 192.168.0.10: Destination host unreachable.
Reply from 192.168.0.10: Destination host unreachable.
Reply from 192.168.0.10: Destination host unreachable.

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\taski>

```

Kuva 15 Pingaus testejä eri verkkoalueiden välillä

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

Yhteenvedona työstä voidaan todeta, että verkon suunnittelussa ja toteutuksessa onnistuttiin toivottulla tavalla. Vaatimukset verkolle olivat melko selkeät, jonka jälkeen kunnollinen suunnittelu tarjosi melko hyvän pohjan verkon luomiselle. Moni asia tässä työssä luodun pienehkön SOHO-verkon luomisessa on hyvin rutiininomaisia tehtäviä mutta jotkin asiat vaativat hieman enemmän suunnittelua ja ongelmien ratkontaa. Tässä työssä merkittävimmäksi työvaiheeksi muodostui VPN konfigurointi. Toki myös muiden konfiguraatiota vaativien ominaisuuksien toteuttaminen vaatii monesti hieman tutustumista laitteen toimintaan uuden laitemallin kohdalla. Jatkokehitysajatuksina työhön, projektia voisi laajentaa ainakin verkkolaitteiden osalta. Laajentaessa käyttäisin Omada-pilvihallintaa tukevia kytkimiä sekä tukiasemia, jolloin verkkoa ja kaikkia sen laitteita voisi konfiguroida ja hallita pilvialinnalla mistä vain helposti ja tehokkaasti.

9 POHDINTA

Tämä opinnäytetyö rajoittui koskemaan vain pienen yrityksen SOHO-verkkoa. Jatkossa aihetta voisi laajentaa suuremmaksi SOHO-verkoksi. Toinen opinnäytetyötä rajoittava tekijä on budjetti. Budjetin suuruus tai pienuus vaikuttaa suoraan niin SOHO-verkon suunnitteluun, kuin toteutukseen.

Opinnäytetyön tekeminen on tarjonnut arvokkaan tilaisuuden henkilökohtaiseen oppimiseen ja kehittymiseen tietotekniikan alalla. Tutkimusprosessin eri vaiheissa olen syventynyt aiheeseen ja hankkinut uutta tietoa ja taitoja. Erityisesti olen oppinut arvioimaan kriittisesti erilaisia tietolähteitä ja soveltamaan niitä tutkimuksen kontekstissa. Lisäksi opinnäytetyön tekeminen on kasvattanut kykyäni itsenäiseen ongelmanratkaisuun ja projektinhallintaan. Prosessin aikana kohtaamani haasteet ovat tarjonneet mahdollisuuden oppia uusia ratkaisumalleja ja kehittää omaa ammatillista osaamistani. Opinnäytetyön tekeminen on myös opettanut minulle paljon itsestäni ja omista vahvuuksistani sekä kehityskohteistani tutkimus- ja kirjoitusprosessin aikana. Kaiken kaikkiaan tämä opinnäytetyöprosessi on ollut merkittävä osa omaa ammatillista kasvuani tietotekniikan alalla.

Tulevaisuudessa teknologian kehitys tarjoaa varmasti uusia mahdollisuuksia myös SOHO-verkoille, kuten nopeammat langattomat tekniikat, esimerkiksi Wi-Fi 6 ja tulevat laajemmat 5G-verkot, jotka parantavat verkkojen suorituskykyä. Myös pilvipalveluiden käyttö yleistyy jatkuvasti SOHO-ympäristöissä. Pilvipalveluiden avulla pienyritykset voivat hyödyntää esimerkiksi kehittyneitä tallennus- ja palveluinfrastruktuureja ilman suuria investointeja. Lisäksi pilvihallintajärjestelmät edesauttavat myös verkkojen hallinnointia. Toimiva SOHO-verkko on kriittinen osa yritysten toimintaa, vaikka monet yritykset siirtävät monien tärkeiden palveluiden toiminnot pilvijärjestelmiin. Pandemian jälkeen nähty etätyön ja etäopetuksen yleistyminen on lisännyt ja lisää edelleen SOHO-verkkojen kysyntää, kun taas älykkäiden laitteiden ja IoT-teknologian yleistyminen lisää verkossa olevien laitteiden määrää. Samalla verkkoturvallisuuden ja tietosuojan merkitys kasvaa, mikä edellyttää entistä kehittyneempiä turvallisuusominaisuuksia ja -ratkaisuja.

LÄHTEET

Cisa (2021) Securing Wireless Networks. Viitattu 24.4.2024. Saatavilla: <https://www.cisa.gov/news-events/news/securing-wireless-networks>

Cisa (2023) Understanding Firewalls for Home and Small Office Use. Viitattu 24.4.2024. Saatavilla: <https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use>

Cisco Press (2010) Analyzing the Cisco Enterprise Campus Architecture. Viitattu 1.4.2024. Saatavilla: <https://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3>

Cruz, B., (2024) Types of VPN Protocols: Explanation and Comparison. Viitattu 27.4.2024. Saatavilla: <https://www.security.org/vpn/protocols/>

Drapkin, A., (2023) How Long Does It Take for a Hacker to Crack a Password? Viitattu 27.4.2024. Saatavilla: <https://tech.co/password-managers/how-long-hacker-crack-password>

F-Secure (2024) Mikä on palomuuuri? Viitattu 7.4.2024. Saatavilla: <https://www.f-secure.com/fi/articles/firewall>

HackTricks (2024) Pentesting wifi. Viitattu 25.4.2024. Saatavilla: <https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-wifi>

Helsingin yliopisto (2021) Tietoliikenteen perusteet 2. Reitin. Viitattu 7.4.2024. Saatavilla: <https://tietoliikenteen-perusteet-2-21.mooc.fi/osa-4/4-reitin>

Krimaka (2024) Osi- ja tcp/ip mallit. Viitattu 7.4.2024. Saatavilla: <https://krimaka.net/tietotekniikka/verkko-ja-ethernet/osi-ja-tcp-ip-mallit.html>

Maggio, A., (2018) Introducing Cisco PPDIOO for Network Design. Viitattu 7.4.2024. Saatavilla: <https://ictshore.com/network-design/cisco-ppdioo/>

Netgear (2022a) Mikä on kytkin? Johdanto. Viitattu 7.4.2024. Saatavilla: <https://kb.netgear.com/fi/232/Mik%C3%A4-on-kytkin-Johdanto?language=fi>

Netgear (2022b) Mikä on virtuaalinen lähiverkko (VLAN) ja miten se toimii hallitun kytkimen kanssa? Viitattu 7.4.2024. Saatavilla: <https://kb.netgear.com/fi/21574/Mik%C3%A4-on-virtuaalinen-l%C3%A4hiverkko-VLAN-ja-miten-se-toimii-hallitun-kytkimen-kanssa?language=fi>

Petryschuk, S., (2024) Network Design and Best Practices. Viitattu 7.4.2024. Saatavilla: <https://www.auvik.com/franklyit/blog/network-design-best-practices/>

Polaridad (2024) Tähtitopologia: Tämän liitännäjäjärjestelmän edut ja haitat. Viitattu 7.4.2024. Saatavilla: <https://polaridad.es/fi/topologia-tipo-estrella-2/>

QSFPTEK (2022) What Is a SOHO Network and How to Set up One? Viitattu 25.4.2024. Saatavilla: <https://www.qsfptek.com/qt-news/what-is-a-soho-network-and-how-to-set-up-one>

Vmware (2024) What is network segmentation? Viitattu 25.4.2024. Saatavilla: <https://www.vmware.com/topics/glossary/content/network-segmentation.html>