LAB University of Applied Sciences

Työelämävalmiudet ICT-asiantuntijan työtehtävissä

LAB-ammattikorkeakoulu
Insinööri (AMK)
2025
Santeri Hietaniemi

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Santeri Hietaniemi	Opinnäytetyö, AMK	2025
	Sivumäärä 27	

Työn nimi

Työelämävalmiudet ICT-asiantuntijan työtehtävissä

Tutkinto ja koulutusala

Insinööri (AMK), Tieto- ja viestintätekniikan koulutus

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Tiivistelmä

Opinnäytetyössä tutustuttiin ICT-asiantuntijan työhön tietoverkkojen häiriönhallinnassa. Työn tarkoituksena oli päiväkirjan avulla seurata kehitystä omissa työtehtävissä. Työssä tutustuttiin ja käytiin läpi myös lähiverkon arkkitehtuuria, protokollia ja aktiivilaitteita, jotka liittyvät olennaisesti työtehtäviin.

Työn tavoitteena oli tuoda esille millaisia taitoja ja vaatimuksia ICT-asiantuntijan työtehtäviin kuuluu. Työssä käytiin läpi esimerkkien avulla työtehtäviin liittyvien ongelmien ratkomista sekä niiden ratkaisut. Esimerkkien tarkoitus oli havainnollistaa lukijalle, kuinka tärkeää lähiverkon laitteiden sekä arkkitehtuurin tuntemus on, mikäli on aikeissa hakeutua vastaaviin työtehtäviin.

Vaikka tieto- ja viestintätekniikan koulutus antaakin hyvät teoreettiset lähtökohdat ICT-asiantuntijan työtehtäviin, varsinaisen työn tuomaa kokemusta on mahdoton korvata.

Asiasanat

lähiverkko, häiriönhallinta, ICT-asiantuntija

Abstract

Author(s)	Type of Publication	Published
Santeri Hietaniemi	Thesis	2025
	Number of Pages	
	27	

Title of Publication

Work-life skills in the task of an ICT Specialist

Degree, Field of Study

Bachelor of Engineering, Information and Communication Technology

Organisation of the client (if the thesis work is commissioned by another party)

Abstract

The thesis introduced the work of an ICT-Specialist in the field of network fault management. The purpose of the thesis was to monitor the development of my own work in the form of a diary. It also explored and discussed the architecture, protocols and active devices of the local area network, which are essential to the job.

The aim of the thesis was to highlight the skills and requirements of an ICT-Specialist. The thesis used examples to illustrate how problems related to the job are solved and how they are resolved. The purpose of the examples was to illustrate to the reader how important it is to have knowledge of local area network equipment and architecture if you are planning to apply for a similar job.

Although ICT education provides a good theoretical basis for the work of an ICT-Specialist, there is no substitute for actual work experience.

Keywords

local area network, incident management, ICT-Specialist

Sisällys

Lyhenteet ja termit

ARP (Address Resolution Protocol) on protokolla, joka auttaa yhdistämään IP- ja MAC-osoitteet toisiinsa.

CAM (Content Addressable Memory) on taulukko, josta näkee mitä porttia pitkin pääsee johonkin tiettyyn MAC-osoitteeseen.

DHCP (Dynamic Host Control Protocol) on verkon laitteiden IP-osoitteiden hallintaan ja jakeluun kehitetty protokolla.

DNS (Domain Name System) on järjestelmä, joka kääntää ihmiselle helppolukuiset osoitteet kuten www.esimerkki.com verkkolaitteiden ymmärtämiksi IP-osoitteiksi.

ICMP (Internet Control Message Protocol) on verkkolaitteiden käyttämä protokolla, jonka avulla pystytään diagnosoimaan verkon ongelmia.

IP-osoite (Internet Protocol) on numeerinen arvo, joka toimii tunnisteena lähiverkon päätelaitteille.

MAC-osoite (Media Access Control) on 48-bittinen verkkokortin yksilöllinen tunniste, jota lähiverkon laitteet käyttävät niiden väliseen kommunikointiin.

NAT (Network Address Translation) mahdollistaa yksityistä IP-osoitetta käyttävien laitteiden yhistämisen julkiseen verkkoon.

OSI (Open Systems Interconnection) -malli, on joukko sääntöjä, jotka määrittävät kuinka eri järjestelmät kommunikoivat tietoverkossa.

SFP (Small Form-factor Pluggable) on verkkomoduuli, jonka avulla voidaan verkkolaitteeseen kytkeä halutulla tekniikalla yhteys.

SNMP (Simple Network Management Protocol) on protokolla, jonka avulla voidaan kerätä tietoa hallittavista verkkolaitteista.

STP (Spanning Tree Protocol) on protokolla, joka ehkäisee silmukoiden muodostumista lähiverkkoon ja mahdollistaa vikasietoisen verkon rakentamisen.

TCP (Transmission Control Protocol) on protokolla, joka muodostaa kahden eri laitteen välille yhteyden ja mahdollistaa niiden välisen kommunikoinnin.

UDP (User Datagram Protocol) on protokolla, jonka avulla voidaan lähettää tietoa laitteelta toiselle, mutta niiden ei tarvitse muodostaa yhteyttä keskenään.

VLAN (Virtual Local Area Network) on verkkojen hallintatekniikka, jonka avulla fyysinen lähiverkko voidaan jakaa loogisiin osiin.

VPN (Virtual Private Network) on palvelu, joka luo suojatun ja kryptatun yhteyden internetin ylitse.

1 Johdanto

Yritykset käyttävät nykypäivänä kasvavassa määrin palveluita, jotka vaativat toimivaa ja vikasietoista tietoverkkoa. Operaattorit ja muut toimijat myyvät palveluita yrityksille, joiden tarkoituksena on huolehtia siitä, että yrityksen verkkoyhteydet sekä tietoturva pysyvät kunnossa. Tätä varten tarvitaan henkilöitä, joiden työtehtävänä on reagoida mahdollisiin tietoverkossa ilmeneviin ongelmiin ja ratkaista niitä.

Opinnäytetyön tavoitteena on kuvata millä tavalla tieto- ja viestintätekniikan insinöörin koulutus palvelee ICT-asiantuntijan työtehtävissä tietoverkkojen häiriönhallinnassa. Opinnäytetyö toteutetaan päiväkirjamallisena, jonka avulla seurataan omaa kehittymistä verkkoarkkitehtuureissa, verkkolaitteiden hallinnoimisessa sekä verkkoprotokollien toiminnan ymmärtämisessä. Päiväkirjan avulla on kirjoitettu kolme esimerkkiä, joiden tarkoitus on avata lukijalle, minkälaisia ongelmia käytännön työelämässä tulee vastaan. Esimerkkitapaukset on valittu siten, että ne tukevat oman kehityksen kohteita. Aluksi käydään läpi teoriaa lähiverkon arkkitehtuurista, protokollista ja laitteista, koska nämä perusasiat kuuluvat olennaisesti ICT-asiantuntijan työtehtäviin häiriönhallinnassa. Lopuksi tarkastellaan, onko oppilaitoksesta saatu koulutus yksinään riittävä näiden ongelmien ratkaisemiseksi. Opinnäytetyö toteutetaan Telia Cygatessa työskentelyn aikana.

Telia Cygate tuottaa yrityksille ICT-palveuita, joista suurimpia ovat tietoverkko- ja tietoturvaratkaisut sekä datakeskuspalvelut. Yrityksellä on tällä hetkellä töissä yli 550 huippuasiantuntijaa, joilla on yli 1000 IT-alan sertifikaattia. Asiakkaiden käytössä on myös ITOC (IT Operations Center), joka palvelee 24/7 vuoden jokaisena päivänä. Pääkonttori sijaitsee Helsingin Pasilassa, ja toimitusjohtajana toimii Matti Eloholma. (Telia Company 2024.) Olen ollut töissä ICT-asiantuntijana Telia Cygatella keväästä 2024 alkaen. Tehtäväni ITOC:ssä on ensisijaisesti häiriönhallinta yritysten tietoverkkoihin liittyvissä ongelmissa. Olen myös usein ensimmäinen henkilö, joka mahdollisesta häiriöstä tietää, sillä ITOC toimii asiakkaille ensisijaisena puhelinkontaktina. Tehtävässä toimiminen edellyttää useiden eri järjestelmien ja laitteiden tuntemista sekä osaamista.

Tieto- ja viestintätekniikan insinöörin opinnot ovat antaneet hyvän pohjan työtehtävässä suoriutumiselle, mutta tähän asti lähes joka viikko on tullut vastaan jotakin uutta. Onneksi työyhteisö on erittäin tukeva ja apua saa lähes jokaiseen tilanteeseen, josta ei itse selviä. Oma-aloitteisuuteen ja itse yrittämiseen kannustetaan, mutta myös apua täytyy osata pyytää, sillä loppuen lopuksi ongelmien ratkaiseminen sekä asiakastyytyväisyys takaavat sen, että töitä on myös jatkossakin.

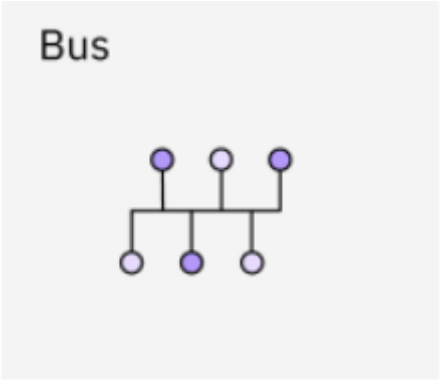
2 Lähiverkko ja aktiivilaitteet

2.1 Lähiverkon arkkitehtuuri

Lähiverkon tarkoitus on yhdistää toisiinsa laitteita, jotka sijaitsevat fyysisesti lähellä toisiaan. Lähiverkon arkkitehtuurilla on suuri vaikutus siihen, miten hyvin liikenne laitteiden välillä kulkee, kuinka vikasietoinen lähiverkko on, miten helppoa ongelmien ratkominen on, kuinka tietoturvallinen verkko on sekä kuinka paljon verkon käyttöönotto ja ylläpito maksavat. Hyvällä suunnittelulla ja toteutuksella on suuri merkitys verkon käytettävyyteen sekä asiakkaan että ylläpitäjän näkökulmasta.Lähiverkossa eri laitteet kytketään toisiinsa eri tavoin. On olemassa valmiita topologioita verkon suunnittelua varten ja näistä jokaisella on hyvät ja huonot puolensa. (Khan ym. 2024.)

Väylätopologia (Bus)

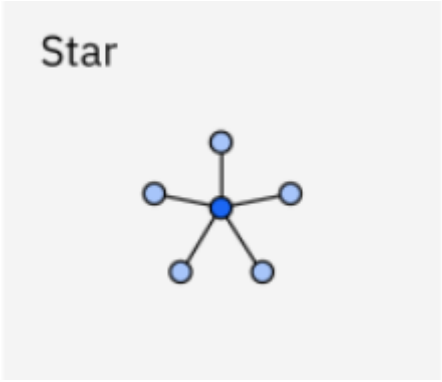
Väylätopologiassa kaikki päätelaitteet ovat kytkettynä yhteen kaapeliin ja kaikki data kulkee pitkin tuota kyseistä kaapelia (Kuvio 1). Jos kaapeliin tulee joku vika, niin kaikki liikenne lakkaa niillä laitteilla, jotka ovat siihen kytkettynä. (Khan ym. 2024.)



Kuvio 1. Väylätopologia (Khan ym. 2024)

Tähtitopologia (Star)

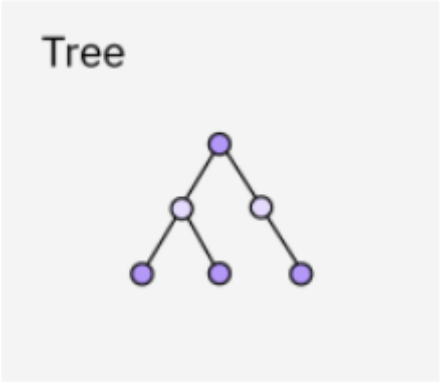
Tähtitopologiassa kaikki päätelaitteet ovat kytkettynä keskitetysti yhteen laitteeseen (Kuvio 2). Tällaisessa verkossa yhden päätelaitteen vianselvitys on helppoa, mutta keskitetyn laitteen vikaantuessa, koko verkko lakkaa toimimasta. (Khan ym. 2024.)



Kuvio 2. Tähtitopologia (Khan ym. 2024)

Puutopologia (Tree)

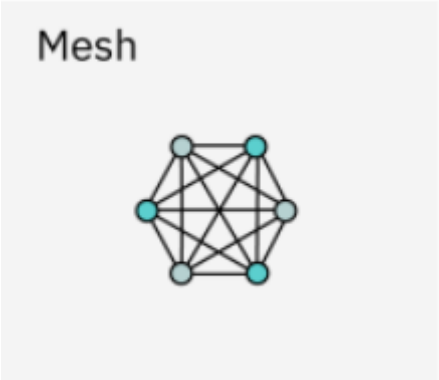
Puutopologia voidaan ajatella väylä- ja tähtitopologioiden yhdistelmänä (Kuvio 3). Sen sijaan, että yhteen keskitettyyn laitteeseen olisi kytketty vain päätelaitteita, kytkeytyykin siihen toisia tällaisia laitteita, kuten kytkimiä. Ongelmaksi tässäkin verkossa muodostuvat verkon solmukohdat, joissa vikatilanteet aiheuttavat yleensä useamman laitteen toimimattomuuden. (Khan ym. 2024.)



Kuvio 3. Puutopologia (Khan ym. 2024)

Silmukkatopologia (Mesh)

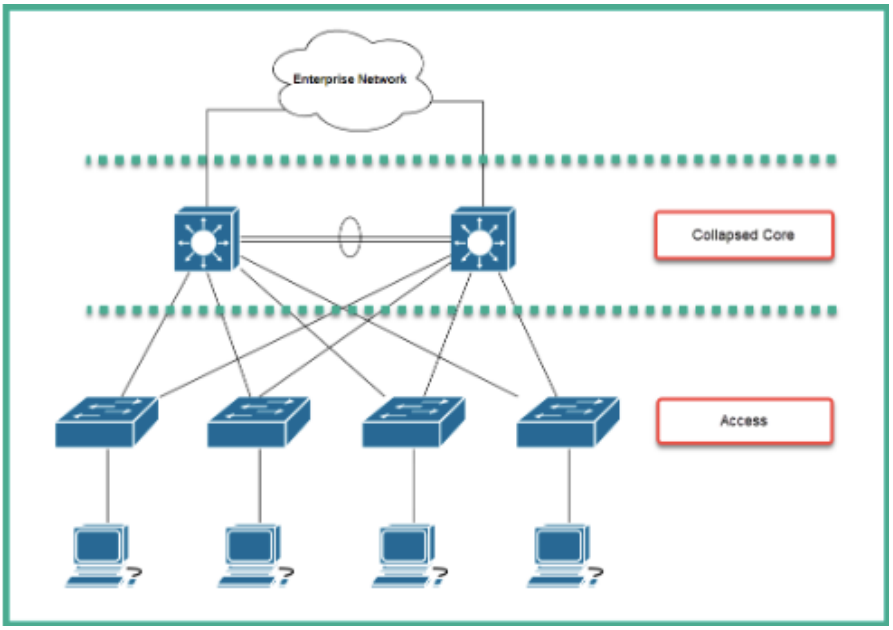
On olemassa kahdenlaisia silmukkatopologioita, osittaisia ja täydellisiä. Täydellisessä silmukkatopolgiassa jokainen laite on kytkettynä kaikkiin muihin verkon laitteisiin, kuten kuviosta 4 voidaan havaita. Osittaisessa silmukkatopologiassa osa laitteista on kytkettynä toisiinsa, mutta osa laitteista joutuu liikennöimään jonkun toisen laitteen kautta. Näistä jälkimmäinen on yleisempi malli kytkeä laitteita toisiinsa. Silmukkatopologialla toteutetut verkot ovat varsin vikasietoisia, mutta niiden toteuttaminen yleensä maksaa enemmän, kuin muulla tavalla toteutetut verkot. (Khan ym. 2024.)



Kuvio 4. Silmukkatopologia (Khan ym. 2024)

Cisco 2 Tier -arkkitehtuuri

Lähiverkon suunnitelussa pitäisi ottaa huomioon hierarkisuus, muunneltavuus, vikasietoisuus ja joustavuus. Tätä varten on luotu valmis arkkitehtuuri, Cisco 2 Tier (Kuvio 5), jota seuraamalla verkkoon tehdään kaksi kerrosta: jakelu (distribution) ja liityntä (access). Jakelu- sekä liityntäverkon laitteet ovat keskenään kytkettynä vikasietoisesti. Vikasietoisuus ei tosin jatku päätelaitteille asti, sillä niissä on yleensä vain yksi verkkokortti. Kyseisessä arkkitehtuurissa jakeluverkosta käytetään termiä collapsed core. (Singh 2020, 60–62.)

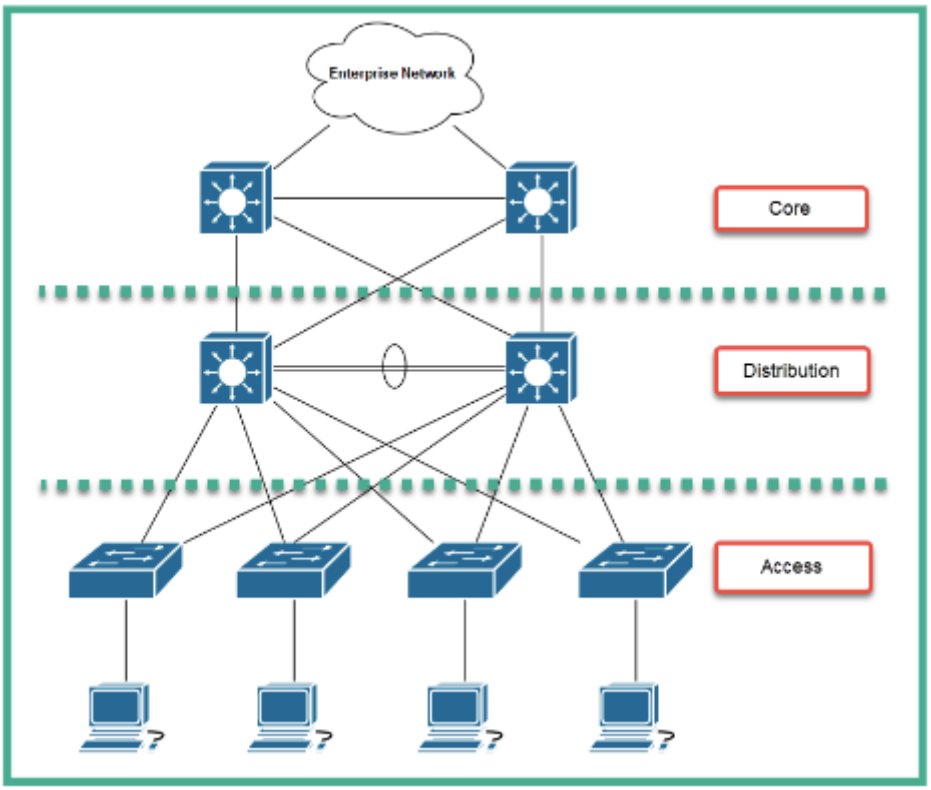


Kuvio 5. Cisco 2 Tier -arkkitehtuuri (Singh 2020, 61)

Cisco 3 Tier -arkkitehtuuri

Tämä arkkitehtuuri pohjaa Cisco 2 Tier -arkkitehtuuriin, mutta siinä on kolme eri kerrosta: ydin (core), jakelu (distribution) sekä liityntä (access) (Kuvio 6). Kaikki verkkolaitteet ovat

vikasietoisesti kytkettynä toisiinsa. Ydinverkon laitteet saattavat sijaita maantieteellisesti eri paikassa kuin jakelu- ja liityntäverkon laitteet, ja niiden kautta voi kulkea liikenne useasta eri toimipisteestä, mikä mahdollistaa verkkoliikenteen eri paikkojen välillä lähiverkkoa pitkin. (Singh 2020, 63–65.)



Kuvio 6. Cisco 3 Tier -arkkitehtuuri (Singh 2020, 63)

2.2 Lähiverkon protokollat

MAC

MAC-osoite (Media Access Control) on 48-bittinen verkkokortin yksilöllinen tunniste, jota lähiverkon laitteet käyttävät niiden väliseen kommunikointiin. MAC-osoite ilmaistaan yleensä muodossa, jossa 12 heksadesimaalista numeroa ovat pareittain erotettuna välimerkillä, esimerkiksi 12:34:DE:AD:BE:EF. Näistä kolme ensimmäistä paria ovat laitteen valmistajalle varatut numerot ja kolme viimeistä ovat valmistajan kyseiselle laitteelle asettamat numerot. (Study CCNA, MAC & IP addresses 2024.)

IP

IP-osoite (Internet Protocol) on numeerinen arvo, joka toimii tunnisteena lähiverkon päätelaitteille. IP-osoitteita on kahta eri versiota 4 ja 6, joista ensimmäinen on 32-bittinen arvo ja jälkimäinen 128-bittinen arvo. Lähiverkoissa yleisimmin käytössä ovat IP-versio 4

osoitteet, jotka ilmaistaan yleensä desimaalimuodossa neljänä lukuarvona välillä 0-255, jotka on erotettu pisteellä toisistaan, esimerkiksi 192.168.0.1. Jokaisella päätelaitteella on oltava IP-osoite määriteltynä, jotta ne voivat kommunikoida toisten laitteiden välillä TCP/IP-verkossa (Transmission Control Protocol/Internet Protocol). Toisin kuin MAC-osoite, joka on fyysinen osoite, IP-osoite on looginen osoite, joka voidaan määrittää halutuksi, kuitenkin niin, että jokaisella verkon laitteella on yksilöllinen osoite. (Vasudevan ym. 2015.)

IP-verkot on jaoteltu julkisiin ja yksityisiin osoiteavaruuksiin, ja näistä yksityiset osoiteavaruudet ovat niitä, joita lähiverkoissa lähtökohtaisesti käytetään. Yksityiset IP-osoitteet eivät reitity internetissä, joten lähiverkon laitteen halutessa kommunikoida verkon ulkopuolelle, reititin käyttää NAT-palvelua (Network Address Translation) kääntääkseen liikenteen kulkemaan julkisen osoitteen kautta. Yksityset IP-osoiteavaruudet on luokiteltu kolmeen eri luokkaan A, B ja C (Kuvio 7). (Singh 2020, 140–144.)

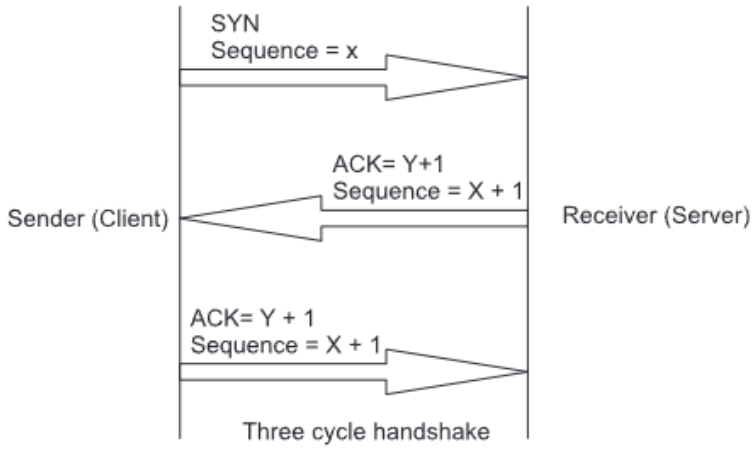
Class	Network Address Block	Address Range
A	10.0.0.0/8	10.0.0.0 - 10.255.255.255
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255
C	192.168.0.0/24	192.168.0.0 - 192.168.255.255

Kuvio 7. Yksityiset osoiteavaruudet ja niiden luokat (Singh 2020, 143)

TCP

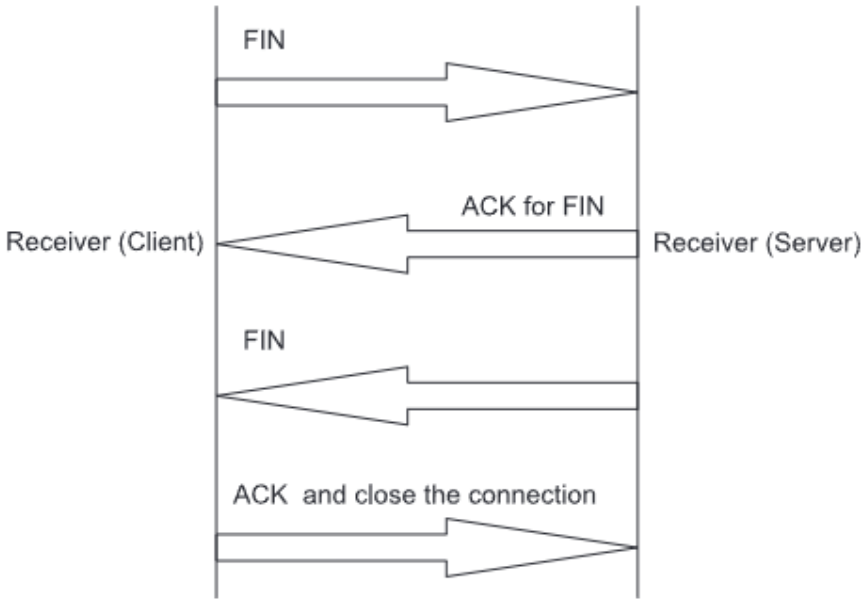
TCP (Transmission Control Protocol) on kaikista käytetyin verkkoprotokolla. TCP on yhteydellinen protokolla, mikä tarkoittaa sitä, että datan siirtämiseksi laitteelta toiselle, muodostavat laitteet ensin keskenään yhteyden, joka pysyy päällä niin kauan, kunnes kaikki data on onnistuneesti siirtynyt. Tämä varmistaa sen, että kaikki data siirtyy, ja tämän takia TCP:tä voidaankin pitää luotettavana tiedonsiirron protokollana. (Vasudevan ym. 2015, 6.2.)

TCP-yhteys muodostetaan kolmivaiheisen kättelyn avulla, jonka aloittaa se osapuoli, joka yhteyden haluaa muodostaa. TCP käyttää eräänlaisia lippuja, joilla se viestii lähetettävän paketin tilasta. Yhteyden ottava osapuoli lähettää ensiksi SYN paketin, johon vastaanottava osapuoli vastaa SYN-ACK paketilla. Lopuksi yhteyttä muodostava osapuoli vastaa vielä takaisin ACK paketilla. Alla oleva kuvio 8 havainnollistaa tätä prosessia. (Vasudevan ym. 2015, 6.4.)



Kuvio 8. TCP-yhteyden kolmivaiheinen kättely (Vasudevan ym. 2015, 6.4)

Vastaavasti TCP-yhteys suljetaan, kun yhteyden muodostanut osapuoli ei sitä enää tarvitse. Lähde lähettää FIN paketin, johon kohde vastaan FIN-ACK paketilla, jonka perään se lähettää FIN paketin takaisin lähteelle, kun yhteys on valmis suljettavaksi. Tämän jälkeen lähde vastaa ACK paketilla ja yhteys suljetaan. Tätä havainnollistaa paremmin alapuolella oleva kuvio 9. (Vasudevan ym. 2015, 6.4.)



Kuvio 9. TCP-yhteyden sulkeminen (Vasudevan ym. 2015, 6.4)

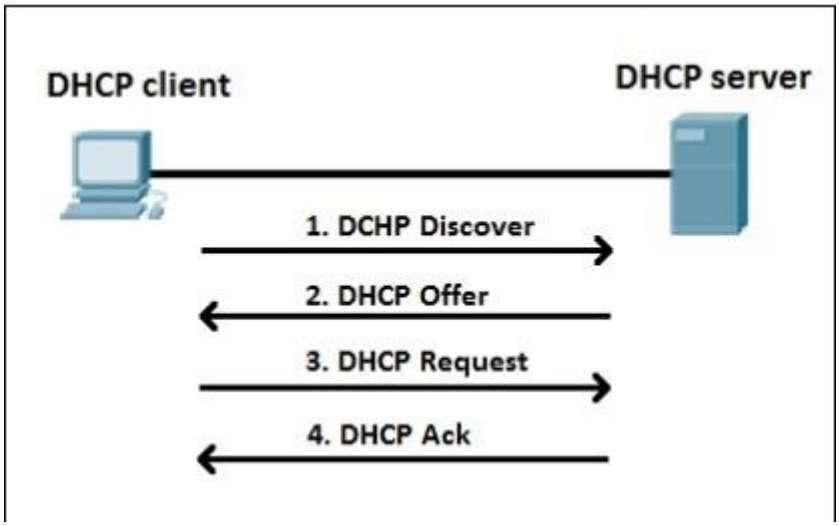
UDP

UDP (User Datagram Protocol), toisin kuin TCP, on yhteydetön protokolla. UDP ei ole luotettava protokolla tiedon lähettämistä varten, koska se ei tarkista millään tapaa onko jokin

paketti saavuttanut jo kohteensa tai ovatko ne saapuneet oikeassa järjestyksessä. UDP on kuitenkin näiden puutteidensa takia paljon nopeampi protokolla, kuin TCP, ja sitä käytetäänkin paljon suoratoisto-ohjelmissa. (Vasudevan ym. 2015, 6.5)

DHCP

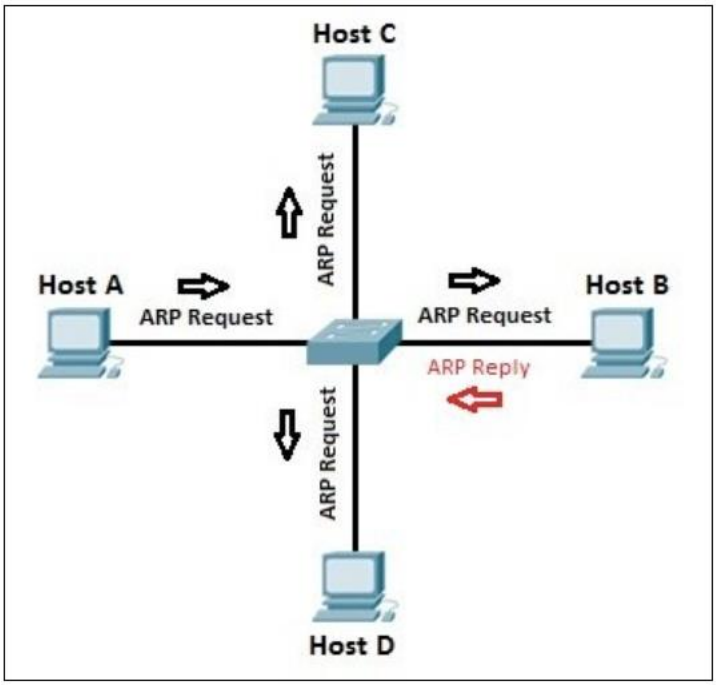
DHCP (Dynamic Host Control Protocol) on verkon laitteiden IP-osoitteiden hallintaan ja jakeluun kehitetty protokolla (Kuvio 10). Sen avulla voidaan automaattisesti jakaa IP-osoitteita verkon laitteille, jolloin laitemääriltään isojen verkkoympäristöjen hallinnointi helpottuu. Se myös pitää huolta siitä, että osoite vapautuu, kun laite ei enää ole verkossa. (Vasudevan, et al. 2015, 5.46-5.47). DHCP-laitteen ja DHCP-palvelimen välillä käydään 4-vaiheinen prosessi, jonka jälkeen laite saa IP-osoitteen, sekä mahdollisesti aliverkon peitteen, oletusyhdyskäytävän, toimialuenimen ja nimipalvelimen. (Study CCNA, DHCP & DNS Protocols explained 2024.)



Kuvio 10. DHCP-prosessi (Study CCNA, DHCP & DNS Protocols explained 2024)

ARP

ARP (Address Resolution Protocol) on protokolla, joka auttaa yhdistämään IP- ja MAC-osoitteet toisiinsa. Se toimii siten, että ARP lähettää broadcast-viestin osoitteeseen FF:FF:FF:FF:FF:FF. Viestissä on mukana lähettäjän MAC- ja IP-osoite sekä kohteen IP-osoite. Broadcast-viesti lähetetään verkkoavaruuden jokaiselle laitteelle. Kun viesti saavuttaa laitteen, se tarkistaa viestistä vastaako kohde IP-osoite kenttä sen omaa IP-osoitetta. Jos vastaa, lähettää se takaisin vastauksen lähettäjälle, jossa on mukana laitteen MAC-osoite. Kuvio 11 havainnollistaa tätä prosessia. (Vasudevan ym. 2015, 5.41.)



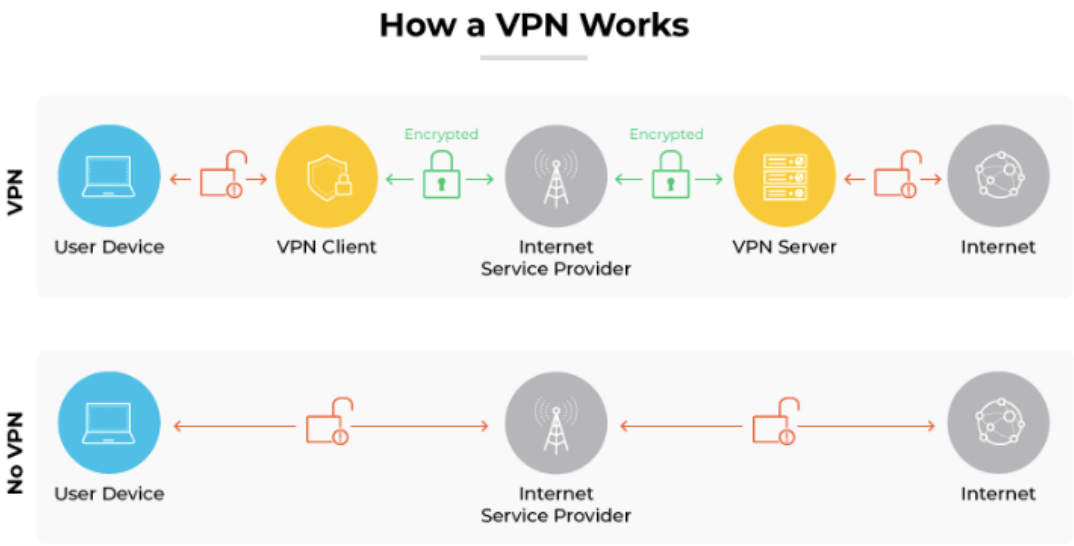
Kuvio 11. ARP-prosessi (Study CCNA, ARP (Address Resolution Protocol) explained 2024)

Spanning Tree Protocol(STP)

Spanning Tree on protokolla, joka ehkäisee silmukoiden muodostumista lähiverkkoon. Kun laitteella on Spanning Tree -protokolla käytössä, silmukan havaitessaan STP estää liikenteen kyseisessä portissa. Tämä mahdollistaa laitteiden kytkemisen toisiinsa vikasietoisesti. On olemassa kolme yleistä STP-standardia, STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) ja MSTP (Multiple Spanning Tree Protocol), joista MSTP on uusin ja kehittynein. (Study CCNA, Spanning Tree Modes: MSTP, PVST+, and RPVST+ 2024.)

Virtual Private Network(VPN)

Virtual Private Network eli VPN on kahden tai useamman laitteen välinen salattu yhteys salaamattoman verkon, eli internetin, ylitse (Kuvio 12). VPN:n muodostamia turvallisia yhteyksiä kutsutaan tunneleiksi ja tätä tunnelia käyttävän laitteen liikenne salataan ja lähetetään tunnelia pitkin. Tällöin liikenne ei näy virtuaalisen verkon ulkopuolelle, yritysympäristöissä liikenne saattaa kuitenkin näkyä yrityksen tietoturvasta vastaaville. (Chauhan 2020, 277; Palo Alto Networks 2025a.)



Kuvio 12. Miten VPN toimii. (Palo Alto Networks 2025b)

Yrityksissä on yleensä käytössä kahdenlaisia VPN-yhteyksiä, käyttäjän ja yrityksen välisiä väliaikaisia etäyhteyksiä (remote access VPN) sekä kahden kohteen yhdistäviä pysyviä VPN-tunneleita (site-to-site VPN). Remote access VPN -tunneli mahdollistaa yritysten työntekijöiden etätyöskentelyn, koska tällöin työntekijä pääsee käsiksi yrityksen tietoihin, sovelluksiin ja työkaluihin, jotka olisivat muuten käytettävissä vain yrityksen oman verkon sisällä. Vaikka liikenne kulkee julkisen verkon yli, kaikki tietoliikenne yrityksen ja käyttäjän välillä on salattua, jolloin liikenteen salakuuntelu ja tarkastelu on lähes hyödytöntä. VPN-yhteydet kuitenkin luovat uuden kerroksen verkkoarkkitehtuuriin, joka taas puolestaan voi vaikuttaa verkon toimintaan. Tämä taas voi johtaa siihen, että jotkut yritykset saattavat oikaista verkon turvallisuudessa etäyhteyksien toiminnallisuuden parantamiseksi. Tätä voidaan ehkäistä oikeaoppisilla ratkaisuilla ja suunnittelulla. (Chauhan 2020, 277-278; Palo Alto Networks 2025c.)

Site-to-site VPN -tunneli yhdistää kahden tai useamman verkon toisiinsa. Tällöin yrityksen eri haarat eri paikoissa voivat liikennöidä toistensa kanssa samassa yksityisessä verkossa. Näin yritys voi myös hyödyntää jo olemassa olevaa julkista internet yhteyttä, jolloin ei ole tarpeen hankkia erikseen yksityistä MPLS(multiprotocol label and switching) -verkkoa. (Palo Alto Networks 2025c.)

2.3 Lähiverkon aktiivilaitteet

Lähiverkon aktiivilaitteisiin kuuluvat kaikki ne laitteet, jotka mahdollistavat tiedonsiirron eri päätelaitteiden välillä. Näitä ovat kytkimet, reitittimet, langattomat tukiasemat ja

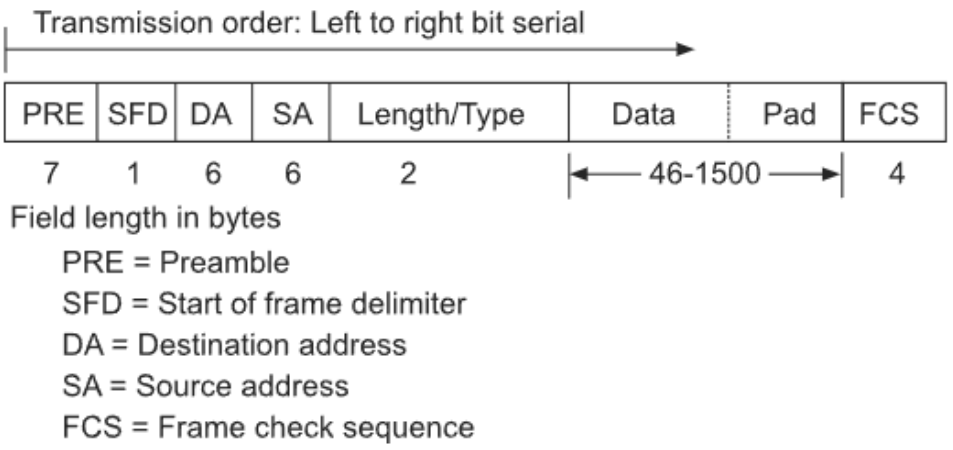
palomuurit. Näistä jokaisella laitteella on oma verkkokorttinsa, jonka kautta laitteet lähettävät ja vastaanottavat datapaketteja. (Singh 2020, 42–58.)

Ethernet

Ethernet on lähiverkon protokolla, joka kehitettiin 1970-luvulla ja on käytössä lähes jokaisessa lähiverkossa. Ethernet on standardi, joka on määritelty IEEE 802.3:ssa. Jokainen Ethernet-verkossa oleva laite on liitetty toisiinsa joko kupari- tai valokaapelilla, kuparikaapelia käytetään yleensä lyhyemmillä välimatkoilla ja valokaapelia pidemmillä. (Singh 2020, 38–41; Vasudevan ym. 2015, 2.21-2.22.)

Ethernetissä laitteet kommunikoivat toistensa välillä käyttäen kehyksiä (Kuvio 13), ja se sisältää seuraavat kohdat (Smith 2024; Vasudevan ym. 2015, 2.21-2.22):

- Preamble: 56-bittinen arvo, jota vastaanottaja käyttää synkronointiin.
- Start Frame Delimiter(SFD): 8-bittinen arvo, joka näyttää mistä kehys alkaa.
- Destination address(DA): 48-bittinen arvo, kohteen MAC-osoite. Arvon ensimmäinen bitti kertoo myös sen, onko kohde yksittäinen laite vai onko kohteena useampi laite. Jos arvo on 0, on kohde yksittäinen laite, jos 1, on kohteena useampi laite.
- Source address (SA): 48-bittinen arvo, lähettäjän MAC-osoite.
- Length/Type: 16-bittinen arvo, kehyksessä olevan datan määrä.
- Data: Vähintään 46-tavuinen ja korkeintaan 1500-tavuinen arvo, sisältää datan.
- Frame Check Sequence (FCS): 32-bittinen arvo, jota käytetään vastaanottavassa laitteessa virheen tarkistukseen.

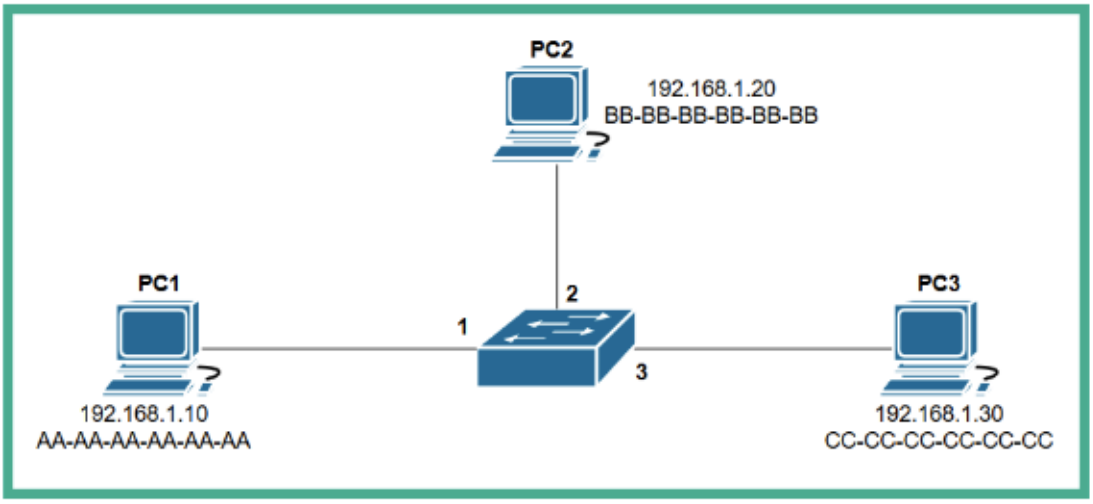


Kuvio 13. Ethernet-kehys (Vasudevan ym. 2015, 2.21)

Kytkimet

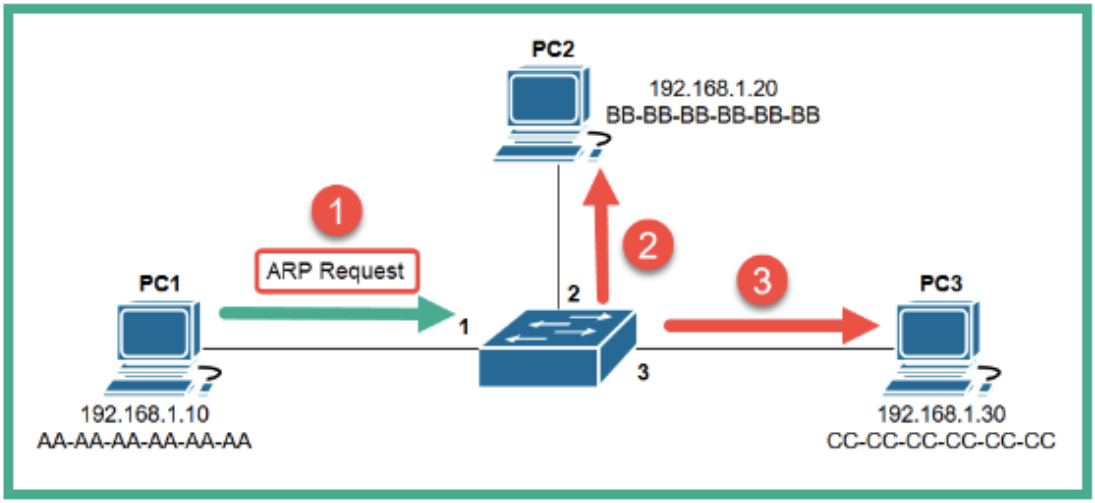
Kytkimet nimensä mukaisesti auttavat kytkemään lähiverkon eri laitteet toisiinsa fyysisesti. Kytkemällä yhteen kaksi tai useampia kytkimiä voidaan lähiverkon kokoa kasvattaa. Kytkin toimii OSI (Open Systems Interconnection) -mallin tasolla 2, joten se vastaanottaa ja lähettää paketteja käyttäen hyväksi MAC-osoitteita. Kytkin tallentaa tiedon MAC-osoitteista CAM-taulukkoon (Content Addressable Memory), josta näkyy missä portissa kukin laite on kytkettynä. (Singh 2020, 45–49.)

CAM-taulukko on kuitenkin aluksi tyhjä ja vasta päätelaitteen yrittäessä kommunikoida toisen lähiverkon laitteen kanssa, saa kytkin tiedon kyseisestä laitteesta. Tiedot tallentuvat CAM-taulukkoon väliaikaisesti ja ne poistetaan, mikäli kyseinen laite ei liikennöi kytkimen kautta jonkin ennalta määritetyn ajan kuluessa. Ciscon laitteilla tuo arvo on oletusasetuksilla 5 minuuttia. Kuvien avulla voidaan havainnollistaa kytkimen toimintaa paremmin (Kuvio 14). (Singh 2020, 45-49.)



Kuvio 14. Laitteet kytketty toisiinsa kytkimen avulla (Singh 2020, 45-49)

Oletetaan, että PC1 haluaa lähettää viestin PC3:lle. Laitteet tietävät toistensa IP-osoitteet, mutta kytkin ei pysty käyttämään hyödyksi tuota tietoa, ellei se ole OSI -mallin tason 3 kytkin, vaan se käyttää ethernet -kehyksissä välitettyä OSI -mallin tason 2 tietoa kohde ja lähde MAC-osoitteista. Laitteet eivät vielä tiedä toistensa MAC-osoitteita, joten PC1 lähettää ARP -pyynnön verkkoon, jossa se pyytää IP-osoitteen 192.168.1.30 sijaintia. Seuraava kuvio 15 havainnollistaa ARP -pyynnön toimintaa kyseisessä esimerkissä. (Singh 2020, 47.)



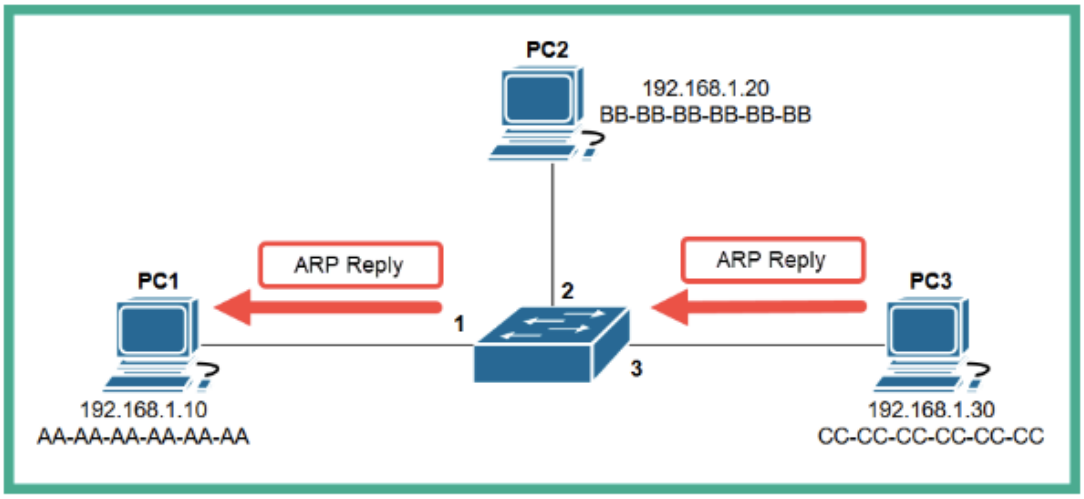
Kuvio 15. ARP -pyyntö (Singh 2020, 47)

Jokainen lähiverkon laite vastaanottaa ARP -pyynnön, ja näin ollen myös kytkin oppii ensimmäisen lähde MAC-osoitteen ja lisää sen CAM-taulukkoonsa (Taulukko 1). (Singh 2020, 47.)

Interface	MAC Address
1	AA-AA-AA-AA-AA-AA
2	
3	

Taulukko 1. CAM-taulukko (Singh 2020, 47)

Seuraavaksi ainoastaan laite, jolla on osoite 192.168.1.30, vastaa ARP -pyyntöön, eli tässä tapauksessa PC3, kuten kuviosta 16 voidaan nähdä. (Singh 2020, 48.)



Kuvio 16. ARP -vastaus (Singh 2020, 48)

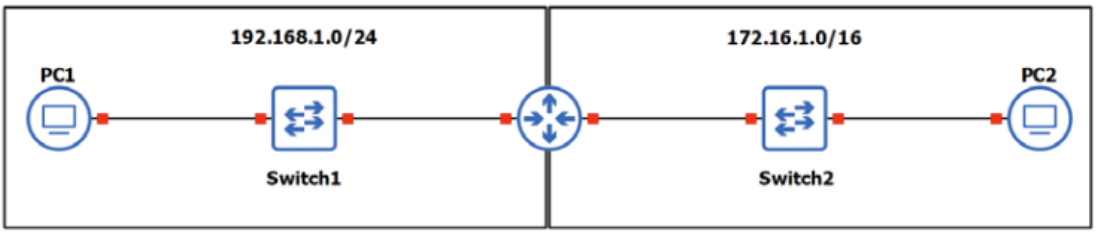
Koska vastaus kulkee kytkimen lävitse, lisää kytkin CAM-taulukkoonsa uuden tiedon porttiin 3 kytketystä laitteesta, kuten voimme havaita taulukosta 2. (Singh 2020, 48.)

Interface	MAC Address
1	AA-AA-AA-AA-AA-AA
2	
3	CC-CC-CC-CC-CC-CC

Taulukko 2. CAM-taulukko ARP -vastauksen jälkeen (Singh 2020, 48)

Reitittimet

Reititin on laite, joka mahdollistaa kahden tai useamman IP-verkon kommunikoinnin keskenään (Kuvio 17). Reitittimet ylläpitävät reititystaulua, johon ne vertaavat tulevan liikenteen kohde IP-osoitteen tietoa, jonka perusteella liikenne ohjataan eteenpäin. Reititin toimii yleensä myös oletusyhdyskäytävänä siinä kytkettynä oleville verkoille, eli kohtana, jonka kautta liikenteen on kuljettava, jotta se voidaan lähettää toiseen verkkoon. (Singh 2020, 50–51.) Reititin toimii usein pienemmissä verkoissa myös DHCP-palvelimena (Singh 2020, 426).



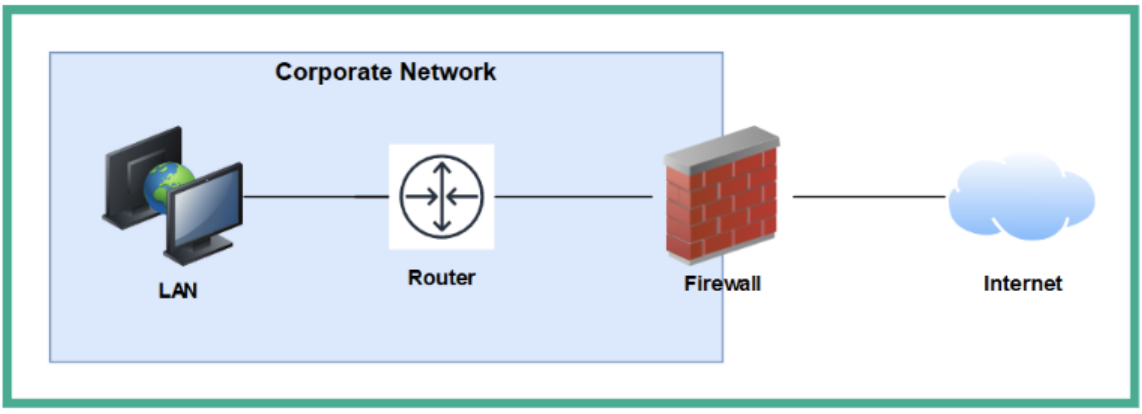
Kuvio 17. Kaksi eri verkkoa kytkettynä toisiinsa reitittimen avulla (Singh 2020, 50)

Langattomat tukiasemat

Langattomat tukiasemat mahdollistavat lähiverkon laajentamisen langattomaksi, jolloinka laitteet, jotka pystyvät hyödyntämään langatonta signaalia, pystyvät liittymään samaan verkkoon. Langattomat tukiasemat käyttävät hyväksi radiotaajuuksia, jotka lähettävät signaalia 2,4GHz:n tai 5GHz:n tajuuden kanavilla. 2,4GHz:n taajuuden signaali yltää pidemmälle, mutta se on hitaampi ja alttiimpi häiriöille, kuin 5GHz:n taajuus, jonka kantama on pienempi, mutta on nopeampi ja vähemmän altis häiriöille. (Singh 2020, 55–56.)

Palomuurit

Palomuuri on laite, jonka tarkoituksena on suodattaa verkkoon saapuvaa sekä lähtevää liikennettä. Palomuuri on yleensä sijoitettuna verkon rajapinnalle, jolloin kaikki liikenne tulee tarkastetuksi (Kuvio 18). Kun palomuurille tulee sellaista liikennettä, jota ei ole sen asetuksissa sallittu, se katkaisee ja estää liikenteen kulun pidemmälle verkkoon. (Singh 2020, 51–53; Vacca & Scott 2004, 7-8.)



Kuvio 18. Palomuurin sijoittelu verkon rajapinnalla (Singh 2020, 52)

Palomuuri voi myös olla asennettuna ohjelmistona itse laitteeseen, kuten tietokoneelle tai palvelimelle. Palomuuri voi myös sijaita verkon sisällä, jolloin sen tarkoituksena ei ole varsinaisesti suodattaa ulkoverkosta tulevaa liikennettä, vaan varmistaa, että verkon sisäinen liikenne on turvattu. Tällöin pystytään estämään mahdollisten

tietoturvapoikkeamien vaikutus pienemmälle alueelle. (Palo Alto Networks 2025d; Palo Alto Networks 2025e; Vacca & Scott 2004, 7-8.)

Palomuurityyppejä on erilaisia:

- Packet Filter palomuuri, sallii liikenteen yksittäiselle paketille mikäli se osuu johonkin sääntöön.
- Web Application palomuuri, suunniteltu suodattamaan erityisesti HTTP -liikennettä.
- Proxy palomuuri, toimii sovellustasolla ja suodattaa liikennettä, joka tulee käyttäjiltä.
- Stateful inspection palomuuri, tarkastelee liikennettä lähettäjän ja kohteen välillä ja sallii tai kieltää niiden välisen yhteyden luomalla ”tilan”. Mikäli kohteiden välillä ilmenee uutta liikennettä, sallitaan liikenne automaattisesti, jos se vastaa aikaisempaa liikennettä.
- NGFW -palomuurit yhdistävät aikaisemmat palomuuritekniikat yhteen uusien menetelmien kanssa, kuten tunkeilijan havaitsemisjärjestelmän (IPS) sekä salatun liikenteen tarkastuksen. (Palo Alto Networks 2025c.)

Palomuureissa ei ole yhtä oikeaa vaihtoehtoa, vaan käyttötarkoitus ja kohde määrittävät sen, minkälainen palomuuri on kyseiseen tehtävään paras. NGFW palomuurit ovat käytössä laajasti yritysympäristöissä, mutta koska niissä on enemmän ominaisuuksia, kuin yksinkertaisemmissa palomuureissa, ne myös maksavat enemmän. (Palo Alto Networks 2025b.) NGFW palomuurit tarvitsevat usein myös maksullisen lisenssin, jotta kaikki sen ominaisuudet saa käyttöön. (Palo Alto Networks 2025d.)

Palomuurit käsittelevät ja tarkastavat suuren määrän verkkoliikennettä, joten niistä voi muodostua pullonkaula, jolloin yrityksen toiminta saattaa kärsiä. Onkin tärkeää, että säännöt suunnitellaan ja testataan huolellisesti, jotta turhilta säännöiltä vältytään ja myös ylläpito on helpompaa. Mitä vähemmän sääntöjä, sitä nopeammin liikenne pääsee jatkamaan eteenpäin. Palomuurit ovat myös alttiita haavoittuvuuksille, joten niiden säännöllinen päivittäminen, varsinkin haavoittuvuuden osuessa käytössä olevaan versioon, on äärimmäisen tärkeää, jotta väärinkäyttö estetään. (Palo Alto Networks 2025d.)

3 Ammatillinen osaaminen ICT-asiantuntijan työssä

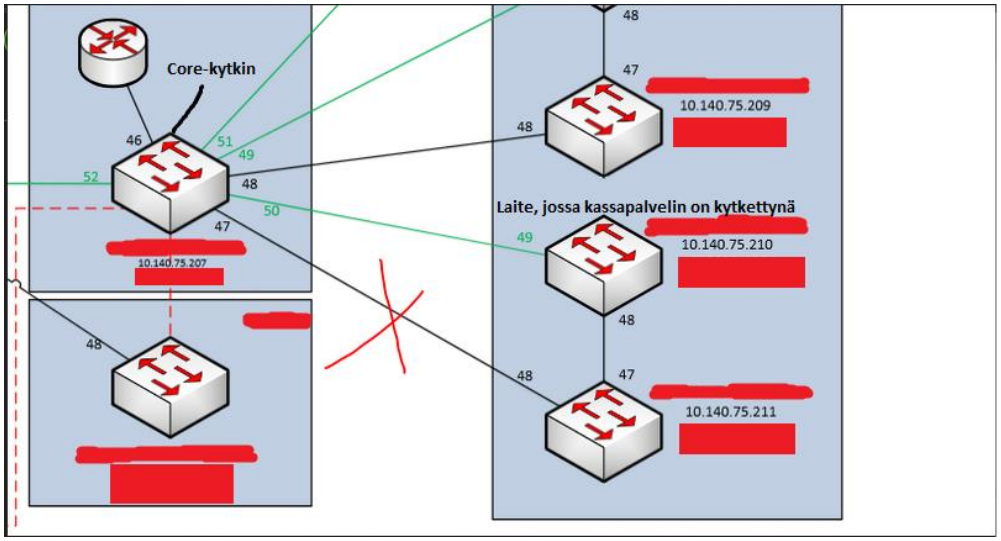
3.1 Tapaus 1: Kassapalvelimen yhteys pätkii

Kassapalvelimen pätkimisestä kohteessa oli ilmoitettu asiakkaan toimesta. Etäyhteyttä palvelimelle oli kokeiltu ja se katkeili säännöllisesti, ja palvelimelta ping-komentoa käytettäessä maksupäätteille yhteys oli hidas. Ongelma näkyi siten, että katevarauksia oli mennyt jonoon. Kassapalvelimen IP-osoite oli saatu asiakkaalta.

Selvitys

Ensimmäisenä piti selvittää, millä laitteella kohteen kassapalvelin sijaitsee. Tätä varten piti ensin etsiä kohteen verkkokuva ja sieltä reitittimen IP-osoite. Toimipisteiden reitittimille ei ollut pääsyä, mutta reitittimille oli sallittu SNMP (Simple Network Management Protocol) -kyselyt komentoriviltä. Snmpwalk -v 2c -c ”communitystring” kohteen-IP ipNetToMediaPhysAddress | grep kassapalvelimen-IP -komennon avulla selvitettiin, mikä on laitteen MAC-osoite.

Kun MAC-osoite oli tiedossa, seuraavaksi verkkokuvasta piti katsoa, mikä on kohteen core-kytkin, eli sellainen kytkin, joka on mahdollisimman korkealla hierarkiassa. Tuolta kytkimeltä piti etsiä MAC-osoitetaulusta komennolla show mac-address-table | inc kassapalvelimen-MAC, missä portissa laite sijaitsee. Tulosteesta voitiin havaita, että laite sijaitsi toisella kytkimellä, johon liikenne kulki core-kytkimen kautta portista 1/1/50. Samaa komentoa käytettiin toisella kytkimellä, jonka jälkeen selvisi, että laite oli kyseisellä kytkimellä portissa 1/1/40.



Kuvio 19. Kohteen verkkokuva

Kytkimen lokitiedoista voitiin havaita tapahtumia, joita kytkimellä oli tapahtunut. Lokitietoja voitiin tarkastella show logging -r -komennolla, joka listasi lokitiedot käänteisessä järjestyksessä uusimmasta vanhimpaan (Kuva 1).

```
2024-09-12T13:39:14.850063+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:39:13.564853+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:39:05.851904+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source [redacted]
2024-09-12T13:39:04.523582+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:54.853250+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:53.932622+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:52.847457+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:51.858336+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:33.851603+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:32.102552+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:30.266327+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:28.845798+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:27.887113+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:14.851825+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:13.369909+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:11.100928+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:05.849751+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:38:04.663763+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
2024-09-12T13:37:50.847447+03:00[redacted]|Topology Change received on port 1/1/49 for CIST from
source: [redacted]
```

Kuva 1. Lokinäkymä

Lokitiedoista näkyi, että kytkimen porttiin 1/1/49 tuli jatkuvasti STP:n (Spanning Tree Protocol) aiheuttamaa ilmoitusta verkkotopologian muutoksesta. Kyseinen portti oli verkkokuvan mukaan linkki core-kytkimelle. Lokitiedot core-kytkimeltä tarkastettiin show logging -r -komennolla (Kuva 2).

```
2024-09-12T14:15:50.748794+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:15:50.033037+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:15:13.598275+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
2024-09-12T14:15:13.341568+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:15:12.479521+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:14:57.633943+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
2024-09-12T14:14:57.279290+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:14:56.496586+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:14:52.871670+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
2024-09-12T14:14:52.622200+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:14:51.790475+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:14:46.798685+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
2024-09-12T14:14:46.523946+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:14:45.746707+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:14:30.993876+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
2024-09-12T14:14:30.607282+03:00[redacted]|1/1|Link status for interface 1/1/50 is up at 1 Gbps with no FEC
2024-09-12T14:14:29.774327+03:00[redacted]|1/1|Link status for interface 1/1/50 is down
2024-09-12T14:14:27.330536+03:00[redacted]NFO|AMM|1/1|CIST - Topology Change generated on port 1/1/50 going in
to forwarding
```

Kuva 2. Lokinäkymä core-kytkimeltä

Core-kytkimen lokitiedoista näkyi, että portti 1/1/50 kävi alhaalla ja tuli takaisin ylös todella usein lyhyen ajan sisällä, ja koska laitteilla oli käytössä STP, se aiheutti jokaisella kerralla verkon topologian muutoksen. Tästä voitiin päätellä kaksi asiaa: Kytkinten välillä oli mahdollisesti viallinen portti tai kaapeli, ja verkkoon syntyi valtavasti turhaa liikennettä jatkuvista topologiamuutoksista.

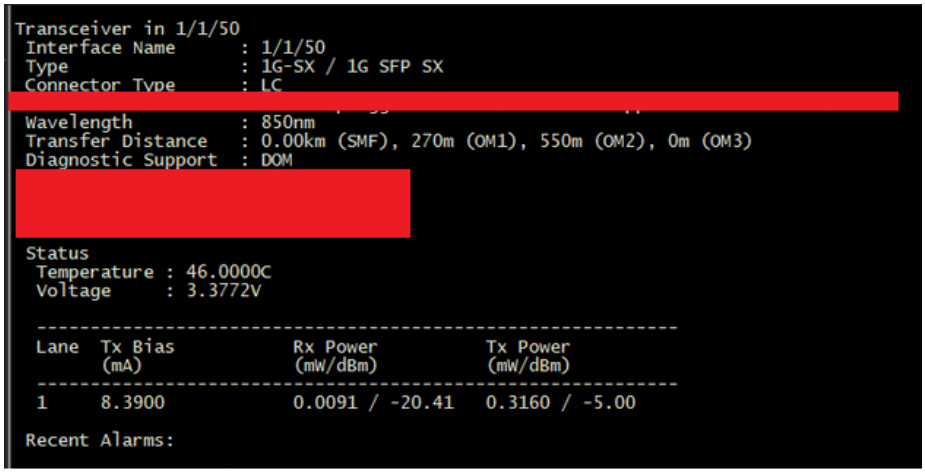
Core-kytkimeltä tarkistettiin vielä portin 1/1/50 tiedot ja kuituarvot, koska kyseessä oli kuituyhteys. Show interface 1/1/50 (Kuva 3) ja show interface 1/1/50 transceiver detail (Kuva 4) -komennolla nämä tiedot voitiin nähdä.

```
Interface 1/1/50 is up
 Admin state is up
 Link state: up for 1 hour (since Fri Sep 13 07:13:57 EEST 2024)
 Link transitions: 77885
 Description:
 Persona:
 Hardware: Ethernet, MAC Address: [redacted]
 MTU 1500
 Type 1G-SX / 1G SFP SX
 Full-duplex
 qos trust cos
 Speed 1000 Mb/s
 Auto-negotiation is on
 Flow-control: off
 Error-control: off
[redacted]
 Rate collection interval: 300 seconds

 Rate                                RX                  TX        Total (RX+TX)
 --------------- -------------------- -------------------- --------------------
 Mbits / sec                   46.59                 1.51                48.10
 KPkts / sec                    5.90                 2.49                 8.39
   Unicast                      5.90                 2.47                 8.37
   Multicast                    0.00                 0.00                 0.00
   Broadcast                    0.00                 0.01                 0.01
 Utilization %                  4.66                 0.15                 4.81

 Statistic                           RX                  TX                Total
 --------------- -------------------- -------------------- --------------------
 Packets                  103779229655          39348270967          143127500622
   Unicast                103759417742          39179184781          142938602523
   Multicast                   1848736             30841506             32690242
   Broadcast                  17963177            138244680            156207857
 Bytes                  103754986294506        2807239753407       106562226047913
 Jumbos                  63884118229           17998109             63902116338
 Dropped                            0                    0                    0
 Pause Frames                       0                    0                    0
 Errors                       2259824                    0              2259824
   CRC/FCS                    2252740                  n/a              2252740
   Collision                      n/a                    0                    0
   Runts                           41                  n/a                   41
   Giants                        7043                  n/a                 7043
```

Kuva 3. Core-kytkimen portin 1/1/50 tarkemmat tiedot



Kuva 4. Core-kytkimen portin 1/1/50 kuituarvot

Portin tiedoista näkyi, että siinä oli valtavasti CRC/FCS (Cyclic redundancy check / Frame check sequence) -virheitä, jotka viittasivat siihen, että data ei välittynyt kyseisessä portissa kuten pitäisi. Kuituarvoista paljastui seuraava mahdollinen ongelmakohta: portin vastaanottoarvo oli aivan liian pieni, jotta yhteys toimisi. Raja-arvo vastaanottovoimalle oli n. -10 mW/dBm.

Seuraavana toimenpiteenä olisi voitu kokeilla sammuttaa portti 1/1/50, koska kassapalvelimen piti olla saavutettavissa toista reittiä pitkin, mutta huomattiin, että verkkokuva oli virheellinen, ja kytkentää core-kytkimen portista 1/1/47 ei ollut koskaan tehty, joten kassapalvelin oli sillä hetkellä vain yhden reitin varassa. Päätettiin soittaa ilmoittajalle asiasta. Tilanne kerrottiin ja myös se, että vikasietoisuutta ei ollut koskaan tehty kohteessa kyseiselle kytkimelle. Sovittiin, että hän menee paikan päälle kytkemään tuon toisen reitin ja kokeillaan sulkea portti 1/1/50 core-kytkimeltä, jonka jälkeen seurataan, poistuuko ongelma.

Tilannetta seurattiin viikonlopun yli eikä ongelma toistunut, kun viallinen reitti oli sammutettuna.

Ratkaisu

Kohteeseen tilattiin asentaja tarkistamaan kytkinten välinen linkki. Puhelussa asentajan kanssa selvisi, että kytkimissä oli käytössä monimuoto SFP (Small Form-factor Pluggable) -portti, ja niiden välille oli laitettu yksmuotokuitua. Asentaja vaihtoi kytkinten välille monimuotokuidun, jonka jälkeen portti 1/1/50 nostettiin takaisin ylös. Tämän jälkeen tilannetta seurattiin yhden päivän ajan, eikä ongelmaa enää ilmennyt. Kassapalvelimen yhteyksien pätkintä johtui siis vääränlaisesta fyysisestä kytkennästä.

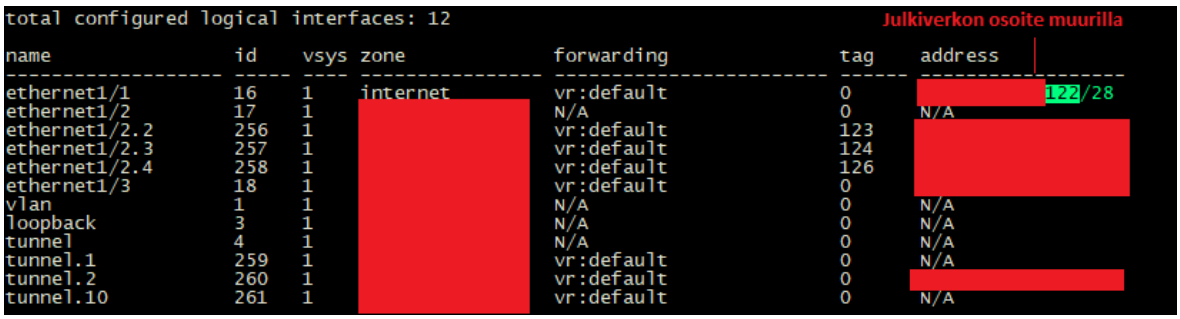
3.2 Tapaus 2: Vierasverkon Wi-Fi ei toimi

Oli saatu ilmoitus asiakkaalta, että vierasverkon Wi-Fi ei toiminut kohteessa. Hetken kuluttua oli tullut myös ilmoitus, että TV-järjestelmien käyttämä verkko ei toiminut. Ongelma oli alkanut hetki sitten.

Selvitys

Tällaisissa tapauksissa on hyvä ensin selvittää, ovatko tukiasemat kohteessa toiminnassa ja mainostuvatko oikeat VLAN (Virtual Local Area Network) -avaruudet kyseisille tukiasemille. Tukiasemien todettiin olevan toiminnassa ja niihin oli yhdistynyt käyttäjiä, mutta jostain syystä vierasverkon sekä TV-järjestelmien verkon käyttäjillä verkkoyhteys ei toiminut. Varmuuden vuoksi tarkistettiin, että kytkimille mainostuvat verkkoavaruudet reitittimeltä asti olivat kunnossa.

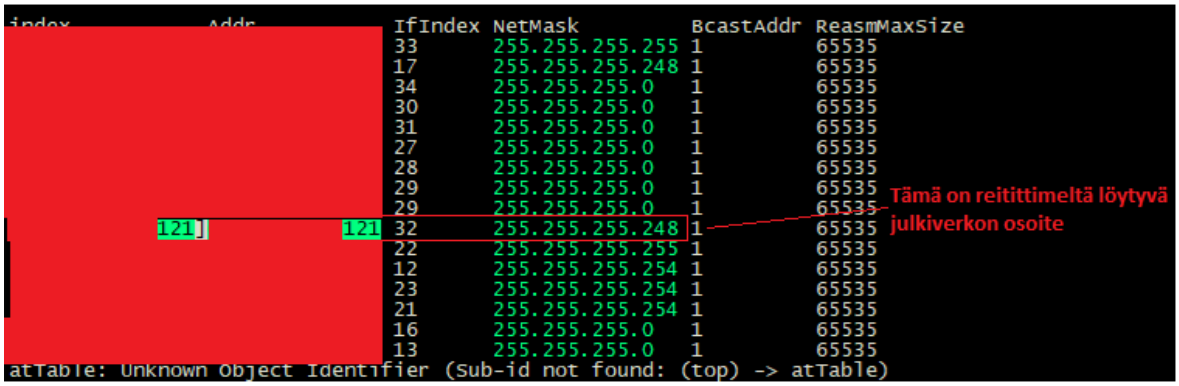
Kohteessa oli käytössä erillinen palomuuri asiakkaan vierasverkon sekä TV-järjestelmien liikenteelle, joten seuraavaksi tarkasteltiin toimipaikkamuurin tilannetta. Ensimmäisenä kokeiltiin ping source vierasverkon-IP host 8.8.8.8 -komennolla ottaa yhteys ulkoverkkoon käyttäen lähteenä vierasverkon yhdyskäytävää. Ping-komento palautti viestinä "request timeout", joka viittasi siihen, että kohde oli määritelty niin, että se ei vastannut ICMP (Internet Control Message Protocol) -viesteihin tai että yhteys jostain kohti verkkoa oli estynyt. Palomuurilta tarvittavat tiedot saatiin show interface logical -komennolla (Kuva 5).



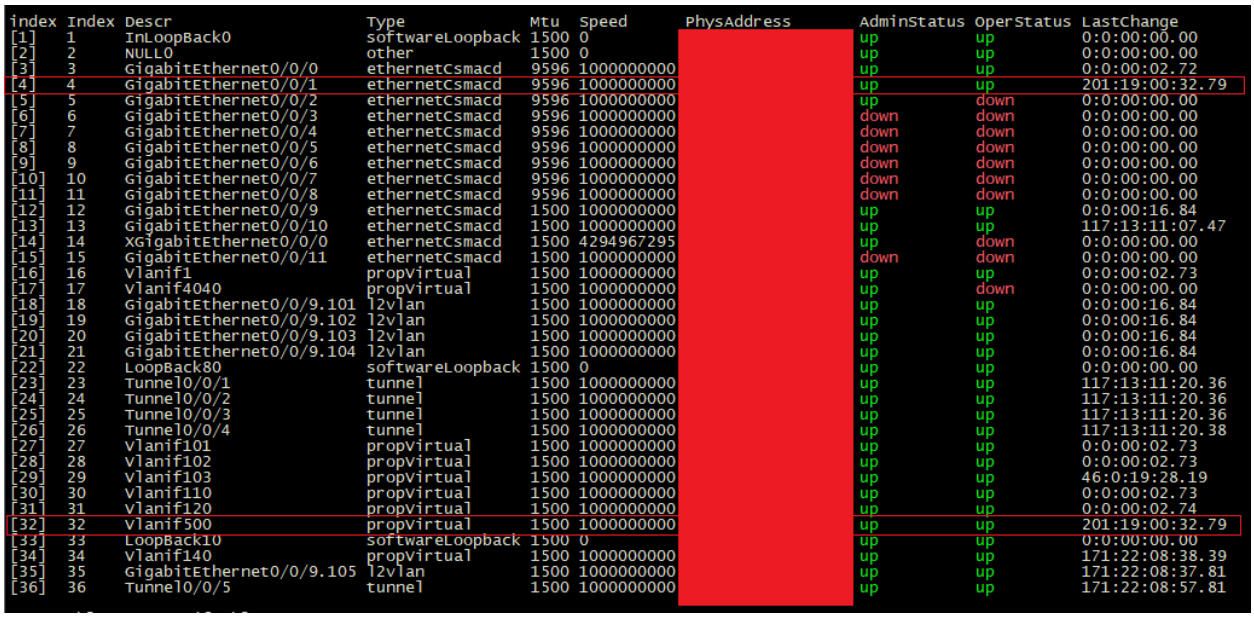
Kuva 5. Palomuurin porttien loogiset osoitteet

Ensin selvitettiin, mikä osoite oli määritettynä palomuurille, jota kautta kohteen ongelmalliset verkot yrittivät yhdistää ulkoverkkoon. Seuraavaksi reitittimeltä haettiin tieto, missä portissa ja mikä IP-osoite sen päässä oli. Tätä varten käytettiin valmista SNMP-skriptiä, joka haki

laitteelta porttien tiedot sekä verkkoavaruudet (Kuvat 6 ja 7).



Kuva 6. Reitittimen verkkoavaruudet



Kuva 7. Reitittimen rajapinnat

Reitittimeltä näkyi, että julkinen IP-osoite sen päässä oli .121 loppuinen ja sillä oli aliverkon peite 255.255.255.248. Tarkistettiin, että palomuurille määritetty julkisen verkon osoite kuului samaan osoiteavaruuteen .121-osoitteen kanssa. Ylemmän kuvan IfIndex-luvun avulla nähtiin, mihin rajapintaan se oli reitittimellä liitettynä, ja alemmasta kuvasta nähtiin, että se osoitti vlanif500. Alemmasta kuvasta nähtiin myös, että portilla GigabitEthernet0/0/1 oli sama aika vlanif500:n kanssa kohdassa "LastChange", joten kyseinen portti oli se fyysinen portti, johon toimipaikkamuurilta oli kytkentä.

Nyt kun reitittimen julkisen verkon IP-osoite ja tieto, että portti oli ylhäällä, olivat tiedossa, voitiin testata yhteys palomuurilta reitittimelle ping source vierasverkon_yhdyskäytävä host reitittimen_julkinen_ip.121 -komennolla. Ping-komento vastasi takaisin onnistuneesti, joten

yhteys reitittimelle asti toimi. Nyt alkoi olla selvää, missä ongelma sijaitsi. Kokeiltiin vielä ping -komennolla ulkoverkkoon vierasverkosta, mutta se ei edelleenkään toiminut.

Ratkaisu

Operaattorille soitettiin, kerrottiin ongelmasta ja mitä oli jo tehty ongelman rajaamiseksi. He ilmoittivat, että alkavat tutkia asiaa. Jonkin ajan kuluttua operaattorilta tuli kuittaus, että reitittimen asetuksia oli korjattu ja että yhteyden pitäisi nyt toimia. Kokeiltiin pingata vierasverkosta ulkoverkkoon ja nyt se onnistui, joten näytti siltä, että ongelma oli saatu korjatuksi. Asiakkaalle kohteeseen soitettiin ja saatiin kuittaus, että yhteydet toimivat taas.

3.3 Tapaus 3: Verkko ei toimi kenelläkään

Ilmoitus oli saatu asiakkaalta, että hallintoverkko ei toiminut kenelläkään. Ongelma koski ilmeisesti langatonta verkkoa. Ongelma oli alkanut jo edellisellä viikolla.

Selvitys

Ensimmäiseksi tarkistettiin, että kohteen laitteisiin pääsi käsiksi. Tämän jälkeen tarkistettiin VLAN-asetukset kytkimeltä. Koska nämä olivat kunnossa, seuraavaksi tutkittiin langattoman verkon laitteiden asetuksia. Asetuksista kävi ilmi, että kaiken piti olla kunnossa ja tukiasemilta nähtiin niihin yhdistyneitä käyttäjiä. Käyttäjät olivat saaneet oikeasta verkkoavaruudesta IP-osoitteet ja liikennettä pystyttiin havainnoimaan tukiaseman GUI (Graphical User Interface) -näkymästä. Palomuurilta nähtiin myös liikennettä kulkevan sekä verkkoon että verkosta pois päin. Päätettiin kokeilla tukiasemien uudelleenkäynnistystä.

Uudelleenkäynnistyksen jälkeen tarkistettiin vielä uudelleen, että verkkoliikennettä kulki sekä palomuurilla että tukiasemilla. Asiakkaalta kysyttiin, auttoiko toimenpide verkko-ongelmaan. Asiakas vastasi seuraavana aamuna, että ongelma ei ollut poistunut, mutta tällä kertaa asiakas osasi tarkentaa, että vierasverkko toimi. Nyt pystyttiin rajaamaan ongelma yhteen verkkoavaruuteen.

Kohteeseen lähetettiin paikan päälle lähituki tutkimaan ongelmaa. Tutkinnassa kävi ilmi, että osa laitteista yhdisti langattoman verkon kautta, mutta ei langallisen. Osa laitteista taas yhdisti langallisen verkon kautta, mutta ei langattoman. Jotkin laitteet toimivat normaalisti molemmissa verkoissa. Kohteen tietokoneisiin päivitettiin verkkokortin ajurit, mutta tällä ei ollut vaikutusta ongelmaan. Tukiasemat käynnistettiin lähituen toimesta vielä uudelleen tuloksetta. Asiakas ilmoitti lähituelle, että tietokone toimi toisessa kohteessa moitteetta.

Seuraavaksi tarkistettiin DHCP (Dynamic Host Control Protocol) -palvelimelta, että laitteet saivat oikeasta avaruudesta IP-osoitteet. Ping-komennolla testattiin laitteiden

saavutettavuutta, osa laitteista vastasi ja osa ei. Tarkistettiin reitittimeltä, että hallintoverkko mainostui kytkimelle asti. Reitittimeltä tarkistettiin myös, että ARP (Address Resolution Protocol) -taulusta näkyivät DHCP-palvelimella näkyneet laitteet, ja että hallintoverkon yhdyskäytävää pitkin kulkeva verkkoyhteys viesti ulkoverkkoon asti. Kaikki näytti toimivan normaalisti.

Tutkintaa rajattiin vielä alemmas verkkoarkkitehtuurissa ja varmistettiin, että kohteen kytkimillä oli varmasti kaikki asetukset kunnossa, ja että kytkennät laitteiden välillä eivät antaneet virheilmoituksia. Tarkistettiin palomuurilta, että verkkoliikennettä kulki yhä molempiin suuntiin. Tutkinnassa ei löytynyt poikkeamia, joten pyydettiin lähitukea tekemään kohteessa testejä ping-komentoa apuna käyttäen. Testeistä kävi ilmi, että toimimattomalla laitteella ping-komento ei toiminut verkon DNS (Domain Name Server) -palvelimiin, julkiseen osoitteeseen 1.1.1.1 eikä hallintoverkon yhdyskäytävään. Toimivalla laitteella kaikki toimivat kuten piti.

Ratkaisu

Ongelmakohdaksi paljastuivat DHCP-palvelimen asetukset. Kohteen verkoissa oli käytössä kaksi DHCP-palvelinta, jotka toimivat keskenään verkkoliikennettä tasaavasti, mutta tutkinnassa oli unohtunut tarkistaa myös toisen palvelimen asetukset. Huomattiin, että toinen palvelin jakoi yhdyskäytävänä aivan väärää verkko-osoitetta. Tämä johti siihen, että kohteen laitteet saivat oikeasta verkkoavaruudesta IP-osoitteen, mutta ne yrittivät liikennöidä verkosta ulospäin väärän osoitteen kautta, mikä näkyi asiakkaalle verkon toimimattomuutena. Palvelimelle korjattiin yhdyskäytävän asetukset, jonka jälkeen saatiin asiakkaalta kuittaus, että verkko toimi jälleen.

3.4 Kehitysprosessini ICT-asiantuntijana

Opinnäytetyötä varten pidetyn päiväkirjan avulla olen pystynyt havainnoimaan itselleni omaa osaamisen kehittymistäni. Olen oppinut verkkoarkkitehtuureista ja tulkitsemaan verkkokuvia. Niiden ymmärtäminen on auttanut rajaamaan lähiverkossa esiintyviä ongelmia. Olen myös oppinut kuinka tärkeää lähiverkon verkkokuvan piirtäminen on, ja että se pyritään päivittämään muutosten yhteydessä. Päiväkirjan pitämisen aikana olen myös kehittynyt verkkolaitteiden hallinnoinnissa. Ongelmien diagnosointi on nopeampaa, kun laitteista saatavaa informaatiota osaa tulkita paremmin. Olen huomannut myös huomattavaa kehitystä laitteiden asetusten muutoksien teossa tai kokonaan uuden laitteen käyttöönotossa. Tiedän mitkä asetukset laitteella täytyy olla ja toiston myötä asetusten muuttaminen on nopeampaa. Verkkoprotokollien toiminnan parempi ymmärtäminen on auttanut mahdollisten vikatilanteiden ongelmien rajaamisessa. Se on saanut myös

tajuamaan sen, kuinka paljon perustyökaluja käytetään osana monimutkaisempien ongelmien selvittämistä.

Päiväkirjan pitämisen aikana olen huomannut itsevarmuuteni ICT-asiantuntijana kehittyneen valtavasti. Pystyn tekemään parempia johtopäätöksiä ja uskallan myös rohkeammin kokeilla omia ratkaisuita ongelmiin. Olen myös huomannut kysyväni vähemmän asioita, joita olen kysynyt aikaisemmin kollegoilta. Kollegat ovat myös kääntyneet minun puoleen joissakin asioissa, joihin olen kaiken lisäksi osannut vastata kattavasti. Myös kokonaisuuksien hahmottaminen on parantunut.

Olen huomannut myös asiakaspalvelutaitojeni kehittyneen ICT-asiantuntijan roolissa. Osaan pysyä rauhallisempana kuin aiemmin, mikäli asiakas on hermostunut ongelmatilanteen johdosta. Osaan myös kysyä oikeita kysymyksiä ongelmaan liittyen, jotta ongelman rajaaminen helpottuu. Itsevarmuus omasta osaamisesta ja sen kehittyminen on auttanut esimerkiksi silloin, kun asiakkaalle täytyy selittää, että ongelma ei johdu verkosta vaan esimerkiksi heidän käyttämästä päätelaitteesta.

Osaamisen kehittäminen ja uusien tekniikoiden hallitseminen on äärimmäisen tärkeää tietoverkkoinsinöörinä. Omat taidot kehittyvät ratkaistaessa erilaisia ongelmia ja jo opitun tiedon soveltaminen helpottuu. Monet laitevalmistajat sekä muut tahot järjestävät kursseja, joilla voi hankkia joko laitteisiin tai laajempiin kokonaisuuksiin liittyviä sertifikaatteja. Nämä sertifikaatit ovat usein maksullisia ja vaativat omaa vapaa-ajan käyttöä niiden suorittamiseen, mutta auttavat työnhaussa tai palkankorotuksesta neuvoteltaessa.

Sertifikaatteihin liittyvistä kokeista täytyy yleensä saada yli 80% kaikista mahdollisista pisteistä. Täten työnantaja näkee mitä kaikkea työntekijä osaa, jos tällä on sertifikaatteja suoritettuna. Mitä tahansa sertifikaatteja ei tosin kannata suorittaa, vaan mieluiten sellaisia, jotka palvelevat omaa työtä, ja jotka ovat arvostettuja ja tunnettuja alan ammattilaisten keskuudessa. Tulevaisuudessa on tarkoitus suorittaa Palo Alton, Fortinetin ja Ciscon sertifikaatteja.

4 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli kolmen esimerkin avulla havainnollistaa minkälaisia ongelmia ja haasteita ICT-asiantuntijan työtehtävissä tulee vastaan, sekä tarkastella kuinka hyvät valmiudet koulutus antaa. Opinnäytetyötä varten pidin päiväkirjaa, johon keräsin tietoja esimerkkejä varten ja seurasin omaa kehittymistäni ICT-asiantuntijana. Päiväkirjamallinen opinnäytetyö auttoi minua huomaamaan missä olen kehittynyt ja missä minulla vielä on kehitettävää.

Päiväkirjan pitäminen osoittautui haastavammaksi kuin luulin. Työtehtävien lomassa ei juurikaan ollut aikaa kirjoittaa erikseen kattavia merkintöjä. Esimerkkeihin tarvittavien tietojen keräämistä varten kehitin itselleni systeemin, jotta pystyin työpäivän jälkeen palaamaan kyseisiin tapauksiin. Muita merkintöjä varten käytin avainsanoja, jotta pysyin palauttamaan mieleen päivän tapahtumat. Päiväkirjan pitäminen osoittautui kuitenkin mainoksi tavaksi seurata omaa kehitystä. Työpäivien aikana vastaan tulleet ongelmat ja ratkaisut jäivät myös paremmin mieleen, kun niitä vielä prosessoi jälkikäteen. Opinnäyetyön kirjoittaminen täten auttoi minua kehittymään ICT-asiantuntijan työssä.

Esimerkkitapauksissa on pyritty havainnollistamaan sitä, miten usein peruskäsitteet tulevat vastaan. Tapauksien avulla havainnollistettiin hieman sitä, mitä kautta erilaisiin johtopäätöksiin ja ratkaisuihin päästiin. Niistä kirjoittaessa on huomannut, että verkkolaitteiden ja -protokollien tuntemuksesta on ollut valtavasti hyötyä ICT-asiantuntijana. Tietoverkkoinsinöörin opintojen ensimmäisellä tietoverkkokurssila käydään läpi esimerkiksi IP- ja MAC-osoitteet, ARP-taulu sekä ping -komento, ja mitä tietoa niistä voidaan saada. Näihin astetta syvällisemmin on päässyt perehtymään koulun kautta kurssilla, jossa käytiin läpi Ciscon CCNA (Cisco Certified Network Associate) laajuiset opinnot. CCNA -opinnot ovat antaneet todella hyvän pohjan uuden oppimiselle.

Opinnäytetyötä työstäessäni olen myös huomannut kuinka tärkeää kollegoilta saama tuki ja yhteiset keskustelut ovat. Kysymällä työkaverilta apua ongelmaan, saadaan se usein miten ratkaistuksi nopeammin kuin etsimällä ja lukemalla dokumentaatioista. Kysymällä on saanut usein myös varsin kattavia selityksiä asioihin sekä vinkkejä vaikkapa tietynlaisten laitteiden kanssa toimimiseen. Samalla olen myös huomannut sen, että lähes kaikki ovat aloittaneet samasta pisteestä kuin mistä itse on aloittanut.

ICT-asiantuntijan työssä osaamiseen vaadittavat taidot ovat varsin laajat. ITOC-työssä häiriönhallinan tehtävissä korostuvat teknisen osaamisen lisäksi ongelmanratkaisukyvyt sekä asiakaspalvelutaidot. Työtehtävissä on myös käynyt selväksi kuinka paljon erilaisia ympäristöjä eri asiakkuuksilla on, ja miten paljon erilaista osaamista vaaditaan kaiken

osaamiseen. Ongelmat saattavat myös päällisin puolin näyttää samanlaisilta, mutta eroavatkin jossain määrin, jolloin niihin ei voi käyttää täysin samaa ratkaisua. Erilaisten verkko-ongelmien ratkaisemista voisikin luonnehtia samankaltaiseksi matemaattisten ongelmien kanssa. Ensin täytyy osata teoria, miten asiat toimivat, mutta tiedon soveltaminen vaatii harjaantumista ja toistoa. Kokemuksen karttuessa ongelmien rajaaminen nopeutuu ja täten myös niiden ratkaiseminen, koska ymmärrys ongelmiin johtavista syistä kasvaa.

Kaiken kaikkiaan koulutus palvelee varsin hyvänä pohjana ICT-asiantuntijatyöhön haluavalle henkilölle. Ylimääräistä harjoitusta itsenäisesti kuitenkin tarvitaan, sillä teoria ei yleensä jää mieleen, eikä sitä välttämättä ymmärrä kunnolla ilman käytännön harjoitusta. Opinnäytetyö oli hyvä osoitus itselle siitä, miten paljon lyhyessä ajassa voi itse kehittyä. Samalla se myös vahvisti tunnetta siitä, että haluan jatkaa kehittymistä kohti syvempää asiantuntijuutta tietoverkkojen maailmassa.

Tulevaisuus tuo tullessaan omat haasteensa. Tekoälyn yleistyessä se tulee vääjäämättä näkymään myös lähiverkon aktiivilaitteissa ja niiden hallintaympäristöissä. Sitä voidaan käyttää apuna ongelmien ennaltaehkäisemisessä sekä ongelmatilanteiden rajaamisessa. Tekoälyn myötä nyt käsin tehtävät asiat saadaan luultavimmin automatisoitua. Moni asia on myös siirtynyt pilveen. Pilvipalveluihin on mahdollista luoda kokonaisia ympäristöjä, jotka ennen luotiin konesaleihin fyysisten laitteiden avulla. Tällaisen ympäristön hallinta vaatii myös omanlaisia taitoja, sillä se tuo tavanomaiseen verkkoympäristöön nähden yhden rajapinnan lisää. Jatkon kannalta onkin tärkeää kouluttautua paitsi lähiverkon laitteiden hallinnoinnissa sertifiointien kautta, myös tekoälyn käytön sekä pilvipalveluiden hallinnoinnin kanssa. Näin voimme hyödyntää teknologian kehityksen tuomat mahdollisuudet ja luoda yhä kestävämpiä ja luotettavampia ratkaisuita tulevaisuuden sukupolvia varten.

Lähteet

Chauhan, S. & Jangra, S. 2020. Computer Security and Encryption: An Introduction. E-Kirja. Mercury Learning & Information. EBook Academic Collection (EBSCOhost).

Khan, T., Jackson, G. & Goodwin, M. 2024. What Is Network Topology. Viitattu 5.10.2024. Saatavissa https://www.ibm.com/topics/network-topology

Palo Alto Networks 2025a. How Does a VPN Work. Viitattu 29.3.2025. Saatavissa https://www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work

Palo Alto Networks 2025b. What is a VPN. Viitattu 29.3.2025. Saatavissa https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

Palo Alto Networks 2025c. What is a Business VPN. Viitattu 29.3.2025. Saatavissa https://www.paloaltonetworks.com/cyberpedia/what-is-a-business-vpn-understand-its-uses-and-limitations

Palo Alto Networks 2025d. What is a Firewall. Viitattu 29.3.2025. Saatavissa https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

Palo Alto Networks 2025e. Types of Firewalls Defined and Explained. Viitattu 29.3.2025. Saatavissa https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

Palo Alto Networks 2025f. Subscriptions You Can Use With the Firewall. Viitattu 29.3.2025. Saatavissa https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/subscriptions/all-subscriptions

Singh, G.D. 2020. Implementing and Administering Cisco Solutions: 200-301 CCNA Exam Guide : Begin a Successful Career in Networking with CCNA 200-301 Certification. E-kirja. Birmingham: Packt Publishing. EBook Academic Collection (EBSCOhost).

Smith, D. 2024. What Is the Destination Address within the Ethernet Frame. Viitattu 5.10.2024. Saatavissa https://sierrahardwaredesign.com/basic-networking/what-is-the-destination-address-within-the-ethernet-frame/

Study CCNA. ARP (Address Resolution Protocol) Explained. Viitattu 2.11.2024. Saatavissa https://study-ccna.com/arp/

Study CCNA. DHCP & DNS Protocols Explained. Viitattu 2.11.2024. Saatavissa https://study-ccna.com/dhcp-dns/

Study CCNA. MAC & IP Addressses. Viitattu 5.10.2024. Saatavissa https://study-ccna.com/mac-ip-addresses/

Study CCNA. Spanning Tree Modes: MSTP, PVST+, and RPVST+. Viitattu 2.11.2024. Saatavissa https://study-ccna.com/spanning-tree-modes/

Telia Company 2024. Telia Cygate - yrityksesi kasvua vahvistamassa. Viitattu 29.3.2024. Saatavissa https://www.telia.fi/telia-yrityksena/telia-cygate

Vacca, J. & Scott, E. 2004. Firewalls: Jumpstart for Network and Systems Administrators. E-Kirja. Chantilly: Elsevier Science & Technology. EBook Academic Collection (EBSCO-host).

Vasudevan, S., Subashri, V., Kothari, D. & Thangaraj, P. 2015. Computer Networking. E-Kirja. New Delhi: Alpha Science Internation Limited. EBook Academic Collection (EBSCOhost).