samk

Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

JARKKO LEIVISKÄ

Tietoverkon anatomia

TIETOJENKÄSITTELYN KOULUTUSOHJELMA
2021

Tekijä(t) Leiviskä, Jarkko	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Huhtikuu 2021
	Sivumäärä 59	Julkaisun kieli Suomi

Julkaisun nimi
Tietoverkon anatomia

Tutkinto-ohjelma
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli luoda tiivis informatiivinen paketti tietoverkoista ja esitellä niiden suunnittelun ja hallinnan kannalta oleellisimpia pohjatietoja. Työssä käsiteltiin verkkoteknologiaa, topologioita, suunnittelua ja hallintaa.

Työn toteuttamiseksi käytiin läpi runsaasti alan ammattilaisten tuottamaa sisältöä kirjojen ja verkkoartikkeleiden muodossa. Lopullinen sisällön pohjalta kirjoitettu teksti auttaa lisäämään ymmärrystä aihealueesta ja se luo hyvän pohjan aiheeseen syvemmälle perehtymiselle.

Asiasanat
Tietokoneverkot, verkonhallinta, suunnittelu

Author(s)
Leiviskä, Jarkko

Type of Publication
Bachelor's thesis

Date
April 2021

Number of pages
59

Language of publication:
Finnish

Title of publication
Anatomy of a computer network

Degree program
Degree programme in Business Information Systems

Abstract

The purpose of this thesis was to create a concise informative package on computer networks and introduce the most essential information for their design and management. The thesis tackled with the topics of network technology, topologies, design and management.

In order to carry out the thesis, a large amount of content in the form of books and online articles written by professionals was reviewed. The finalized text helps to increase the understanding of the topic and creates a good foundation for deeper familiarization.

Key words
Computer networks, network management, planning and design

SISÄLLYS

1 JOHDANTO

Nykypäivänä tietoverkot ovat läsnä meidän jokaisen arkipäivässä ainakin jossain muodossa, mutta mitä niiden pinnan alla oikeasti tapahtuu ja miksi sillä on meille väliä? Tietoverkko on laaja ja monimutkainen kokonaisuus, joka koostuu useasta eri komponentista. Monimutkaisuudesta huolimatta, sen toiminnan takana on ohjaavia periaatteita ja selkeä rakenne, jotka luovat meille perustan sen ymmärtämiseksi. Eri komponenttien toiminnalliset roolit ja niiden välisten suhteiden ymmärtäminen on välttämätöntä, kun tietoverkkoa aletaan miettiä esimerkiksi sen käyttöönoton, suunnittelun tai hallinnan näkökulmasta. Puutteellisilla tai virheellisillä tiedoilla suunniteltu tai hallittu verkko tulee törmäämään ongelmiin, ilman että edes tiedetään, mistä ongelmat saivat alkunsa. Vaikka ei suoraan työskentelisikään tietoverkkojen parissa, auttaa syvempi tietämys niistä hahmottamaan, miksi joihinkin näkyviin konkreettisiin ratkaisuihin on päädytty.

Opinnäytetyön tarkoituksena on raottaa tietoverkkojen pinnan alle ja toimia niiden ymmärtämisen kannalta oleellisimmat aiheet kattavana tietopakettina. Aluksi luodaan perusta tietoverkkojen takana olevan teknologian ymmärtämiseksi esittelemällä linkkikerroksen ja verkkokerroksen käsitteitä, toimintaa, niiden tärkeimpiä protokollia sekä laitteita. Kolmannessa luvussa esitetään tietoverkkojen asetteluun ja organisoimiseen käytettäviä yleisimpiä verkkotopologioita, jonka jälkeen perehdytään verkkosuunnitteluun ja Ciscon kehittämään suunnittelumalliin. Neljännessä luvussa tietoverkkoa tarkastellaan hallinnollisesta näkökulmasta ja tutustaan samalla sen oleellisimpiin monitorointi ratkaisuihin.

2 VERKKOTEKNOLOGIA

2.1 Lähiverkko

Lähiverkko (eng. Local Area Network, lyh. LAN) on paikallinen verkko, joka on suunniteltu tietokoneiden, oheislaitteiden, tallennuslaitteiden ja muiden tietoteknisten resurssien yhdistämiseen rajatulla alueella. Lähiverkko voi palvella esimerkiksi toimistoa, yhtä rakennuksen kerrosta, koko rakennusta, tai jopa monista rakennuksista koostuvaa kokonaisuutta. Lähiverkot ovat yleensä yksityisiä verkkoja. (Horak 2007, 5; Cisco 2020a.)

Lähiverkot kehitettiin vuonna 1960 vastaamaan korkeakoulujen ja tutkimuslaitosten tarvetta kytkeä tietokoneita toisiin tietokoneisiin. Lähiverkot levisivät laajempaan käyttöön vasta ethernet-teknologian kehityksen, kaupallistamisen ja standardisoinnin jälkeen vuonna 1983. Langattomien lähiverkkojen (eng. Wireless Local Area Network, lyh. WLAN) laajemman käyttöönoton myötä lähiverkot yleistyivät isojen yritysten ja koulujen lisäksi myös muun tyyppisissä ympäristöissä, kuten ravintoloissa, kaupoissa ja kodeissa. (Cisco 2020a.)

Lähiverkot voidaan pääsääntöisesti jakaa kahteen eri tyyppiin: asiakas-palvelin lähiverkkoihin (eng. client/server LAN) sekä vertaislähiverkkoihin (eng. peer-to-peer LAN). Asiakas-palvelin lähiverkoissa laitteet eli asiakkaat ovat yhteydessä keskitettyyn palvelimeen, joka tarjoaa lähiverkon laitteille käyttöön dataa, sovelluksia ja muita erialisia resursseja. Vertaislähiverkoissa ei ole erillistä keskitettyä palvelinta, eivätkä ne pysty käsittelemään asiakas-palvelin lähiverkkojen tapaan suuria työkuormia, joten ne ovat tyypillisesti pienempiä. Vertaislähiverkossa kaikki laitteet ovat asiakkaan ja palvelimen roolissa. Suurin osa kotiverkoista on vertaislähiverkkoja. (Cisco 2020a.)

2.2 OSI-malli

The Open Systems Interconnection (lyh. OSI) malli kuvaa seitsemää kerrosta, joita tietokonejärjestelmät käyttävät kommunikointiin verkon yli. Se oli ensimmäinen standardi malli verkkokommunikaatiolle, ja 1980-luvun alkupuolella sitä käyttivät kaikki

suuret tietokone- ja telekommunikaatioyritykset. Vuonna 1983 suurten tietokone- ja telekommunikaatioyritysten edustajat esittelivät OSI:n, jonka jälkeen International Organization for Standardization (ISO) hyväksyi sen kansainväliseksi standardiksi vuonna 1984. Nykyinen Internet perustuu yksinkertaisempaan TCP/IP-malliin (Transmission Control Protocol/Internet Protocol). OSI-mallia käytetään kuitenkin vielä laajalti, sillä se auttaa visualisoimaan ja kommunikoimaan verkon toimintaa sekä auttaa verkkojen ongelmien tunnistamisessa ja vianetsinnässä. Taulukossa 1 esitellään kaikki OSI-mallin kerrokset ja kuvaillaan lyhyesti kerroksien toimintaa. (Imperva 2020.)

Taulukko 1. OSI-mallin kerrokset (tiedot Thomas ym. 2002, luku 2.1.1.)

Kerros	Kerroksen numero	Kuvaus
Sovelluskerros	7	Sovellukset, joita käyttäjät käyttävät datan vaihtoon toimivat tällä kerroksella.
Esitystapakerros	6	Vastaa vaihdettavan datan muodosta.
Istuntokerros	5	Vastaa kahden ylemmän kerroksen vaatimien yhteyksien avaamisesta istunnon alkaessa ja yhteyksien sulkemisesta istunnon päättyessä.
Kuljetuskerros	4	Pilkkoo datan käytettäviksi segmenteiksi ja päättää, kuinka data lähetetään.
Verkkokerros	3	Vastaa internetin osoitteistuksesta ja siitä, että data päätyy oikealle vastaanottajalle.
Siirtoyhteyskerros	2	Valmistelee datan fyysiselle kerrokselle siirtoa varten.
Fyysinen kerros	1	Määrittää siirtoyhteyskerrokselta saapuvan datan fyysisen siirtotavan.

2.3 Layer 2

Layer 2, joka tunnetaan myös siirtoyhteyskerroksena (eng. Data Link layer) on seitsemänkerroksisen OSI-mallin toinen kerros. TCP/IP-mallissa Layer 2 vastaa ensimmäisenä sijaitsevaa linkkikerrosta. Kaikkia linkkikerroksen protokollaa käyttäviä laitteita kutsutaan solmuiksi (eng. node). Solmuja ovat siis mm. työasemat, reitittimet, kytkimet ja WLAN-tukiasemat. Linkkikerroksen päätehtävinä on mahdollistaa ja tarjota keinot datagrammien siirtoon solmulta toiselle käyttäen linkkejä, mutta se tarjoaa myös useita muita palveluita (Kurose & Ross 2017, 468-470; Juniper 2021a.)

2.3.1 Ethernet

Ethernet on käytetyin langallisen lähiverkon teknologia. Se kehitti Digital Equipment Corporation (DEC), Intel ja Xerox (DIX) 1970-luvulla ja sitä kutsuttiin nimellä DIX Ethernet. Myöhemmin sitä kutsuttiin "paksuksi" Ethernetiksi (viitaten verkossa käytettyjen kaapeleiden paksuuteen), ja sen tiedonsiirtonopeus oli 10 megabittiä sekunnissa. Ethernetin standardia päivitettiin 1980-luvulla uuden toiminnallisuuden lisäämiseksi ja uusi versio nimettiin Ethernet versio 2:ksi. (Sequeira 2013.)

The Institute of Electrical and Electronics Engineers (lyh. IEEE) on tekniikan alan järjestö, joka kehittää verkkostandardeja. IEEE:n kehittämät standardit ovat hallitsevia lähiverkkostandardeja tänä päivänä. 1980-luvun puolivälissä IEEE kehitti uusia standardeja Ethernetin kaltaisille verkoille. Luotuja standardeja kutsutaan Ethernet 802.3:ksi ja se perustuu CSMA/CD-monipääsyprotokollaan. Ethernet 802.3-standradia kehitetään vielä tänäkin päivänä. (Sequeira 2013.)

Ethernet toimii OSI-mallin fyysisellä ja siirtoyhteyskerroksella. Fyysisellä kerroksella se määrittää johdotuksen ja signaloinnin ja siirtoyhteyskerroksella se määrittää kehyksen formaatit ja protokollat. Ethernet käyttää datan siirtoon kehyksiä, jotka sisältävät lähde ja kohde MAC-osoitteet (Media Access Control). (Study-ccna 2020.)

2.3.2 Ethernet-kehyksen rakenne

Bittejä jotka lähetetään Ethernet lähiverkon yli organisoidaan kehyksiksi. Kehykset toimivat lähetettävän datan säiliönä. Kehys koostuu seuraavista kentistä:

- Alkutahdistus (eng. preamble). Koostuu 7 tavusta vuorottelevista ykkösistä ja nollista, jotka synkronoivat kommunikoivien tietokoneiden signaalit.
- Start-of-frame delimiter (SOF). Tämä kenttä sisältää bittejä, jotka ilmoittavat vastaanottavaa tietokonetta, että kehyksen lähetys on alkamassa, ja että tätä seuraava data on osa kehystä.
- Kohdeosoite. Tämä kenttä sisältää tietokoneen verkkokortin MAC-osoitteen, jonne kehys ollaan lähettämässä.
- Lähdeosoite Tämä kenttä sisältää lähettävän tietokoneen verkkokortin MAC-osoitteen.
- Tyyppi/pituus. Kertoo verkkokerroksen protokollatyypin tai data-kentän pituuden.
- Data ja täyte. Tämä kenttä sisältää verkkokerroksen IP-datagrammin, joka lähetetään kohde koneelle. Jos kenttä jää liian lyhyeksi, lisätään siihen lisäksi ns. täytebittejä, jotta kentän 46 tavun minimipituus täyttyy.
- Frame check sequence (FCS). Tämä kenttä sisältää tarkstusmekanismin, jolla varmistetaan, että kehys on siirretty ilman korruptoitumista.

(Sequeira 2013.)

2.3.3 Ethernet-kehyksen lähetystavat

Kommunikaatio verkossa tapahtuu kolmella eri tavalla: täsmälähetyksinä (eng. unicast), yleislähetyksinä (eng.broadcast) ja ryhmälähetyksinä (eng. multicast). (Sequeira 2013.)

Täsmälähetys on kommunikaatiota, jossa kehys lähetetään yhdeltä laitteelta ja osoitetaan yhteen tiettyyn kohteeseen. Täsmälähetyksessä lähettäjiä ja vastaanottajia on kumpiakin vain yksi. Täsmälähetys on lähiverkkojen ja internetin hallitseva lähetystapa. (Sequeira 2013.)

Yleislähetys on kommunikaatiota, jossa kehys lähetetään yhdestä laitteesta kaikkiin muihin laitteisiin. Tässä tapauksessa lähettäjiä on vain yksi, mutta data lähetetään kaikkiin muihin yhdistettyihin vastaanottaviin laitteisiin. Yleislähetykset ovat välttämättömiä, kun on tarve lähettää sama viesti kaikille lähiverkon laitteille. (Sequeira 2013.)

Ryhmälähetys on kommunikaatiota, jossa kehys lähetään tietylle ryhmälle laitteita. Toisin kuin yleislähetyksessä, ryhmälähetyksessä vastaanottavien laitteiden täytyy kuulua ryhmälähetysryhmään vastaanottaakseen dataa. (Sequeira 2013.)

2.3.4 Linkit ja linkkikerroksen toteutus

Tietoliikennekanavia, jotka yhdistävät viereisiä solmuja kutsutaan linkeiksi. Linkit voivat olla joko langallisia tai langattomia. Linkkikerroksen tehtävä on siirtää datagrammeja viereisten solmujen välillä linkin yli. Linkin lähettävä puoli kapseloi datagrammin kehykseen (eng. frame) ja lähettää kehyksen linkkiin. (Kurose & Ross 2017, 468.)

Linkkikerros toteutetaan pääosin jokaisen päätelaitteen verkkokortissa (eng. network interface card lyh. NIC). Verkkokorttiin on erityistä tarkoitusta varten rakennettu siru, jonka tehtävä on toteuttaa linkkikerroksen palveluita. Suurinta osaa linkkikerroksen toiminnoista toteuttaa laitteisto, mutta osaa toiminnoista toteuttaa ohjelmisto, jota suorittaa laitteen prosessori. Täten linkkikerros on yhdistelmä laitteistoa ja ohjelmistoa. (Kurose & Ross 2017, 471-472.)

2.3.5 Kehystys ja vuonhallinta

Kehystys on linkkikerroksen palvelu, joka kapseloi datagrammin linkkikerroksen kehykseen ennen linkkiin lähettämistä. Kehys koostuu linkkikerroksen otsakekentistä ja verkkokerroksen datakentästä. Vuonhallinta on mekanismi, jota käytetään hallitsemaan kahden laitteen välistä tiedonsiirtonopeutta. Tällä estetään lähdelaitetta ylikuormittamasta kohdelaitetta lähettämällä enemmän paketteja kuin kohde pystyy käsittelemään. (Kurose & Ross 2017, 470.)

2.3.6 Virheiden havaitseminen ja korjaus

Linkkikerroksen laitteisto vastaanottavassa solmussa saattaa virheellisesti päättää, että kehyksen bitti on nolla, vaikka lähetettäessä se oli yksi. Tällaisia virheitä aiheuttavat mm. signaalin vaimennus ja sähkömagneettinen melu. Koska ei ole mitään tarvetta ohjata eteenpäin virheellistä datagrammia, monet linkkikerroksen protokollat tarjoavat mekanismeja kyseisten virheiden havaitsemiseen. (Kurose & Ross 2017, 471.)

Virheentunnistus on toteutettu seuraavasti; lähettävä solmu sisällyttää kehykseen virheentunnistusbittejä, jotka vastaanottava solmu tarkastaa. Virheenkorjaus muistuttaa virheentunnistusta sillä poikkeuksella, että vastaanottaja ei vain tunnista virhettä sen tapahtuessa, vaan myös päättelee, missä kehyksen sisällä virhe on tapahtunut ja korjaa tämän virheen. (Kurose & Ross 2017, 471.)

Vialliset verkkokortit tai ominaisuuksiltaan (pituus, impedanssi) sopimattomat kaapelit voivat aiheuttaa ns. myöhäisiä törmäyksiä (eng. late collision). Myöhäisellä törmäyksellä tarkoitetaan verkossa tapahtuvaa törmäystä, joka havaitaan vasta siinä vaiheessa, kun datagrammista on lähetetty jo suurin osa. Tämän seurauksena verkkokortti ei saa tietoa tapahtuneesta törmäyksestä ja virheenkorjaus ja datagrammin uudelleenlähetys jäävät siten ylempien kerrosten tehtäväksi. (Allen 2009, luku 4-18, luku 11-14)

2.3.7 Multiple access links

On olemassa kahdenlaisia linkkejä: pisteestä pisteeseen-linkkejä (eng. point-to-point) ja yleislähetys-linkkejä (eng. broadcast link). Pisteestä pisteeseen linkki koostu yhdestä lähettäjästä ja yhdestä vastaanottajasta. Monet linkkikerroksen protokollista kuten point-to-point protocol (PPP) ja high level data link control (HDLC) on suunniteltu pisteestä-pisteeseen-linkeille. Yleislähetys-linkissä voi olla voi olla useita lähettäviä solmuja ja useita vastaanottavia solmuja, jotka ovat kaikki yhdistetty yhteen samaan yleislähetys kanavaan. Kun mikä tahansa solmu lähettää kehyksen, kanava tekee siitä yleislähetyksen ja jokainen kanavan solmu saa siitä kopion. (Kurose & Ross 2017, 479.)

2.3.8 Monipääsyprotokollat

Kun kaksi tai useampi solmu lähettää kehyksiä samaan aikaan, kaikki solmut vastaanottavat useita kehyksiä samaan aikaan ja kun tämä tapahtuu kaikki lähetetyt kehykset törmäävät vastaanottavissa solmuissa. Törmäyksen tapahtuessa vastaanottajat kuulevat kaikki lähetykset samaan aikaan, eivätkä pysty erottelemaan niitä toisistaan. Törmäyksen aikana lähetetty data menetetään, ja se joudutaan lähettämään uudestaan. Jokainen törmäys siis tuhlaa yleislähetyskanavan kaistaa. Jotta kanava pysyy toimintakelpoisena monen aktiivisen solmun kanssa, on kehitetty protokollia, joilla solmut koordinoivat sitä, kuka kanavaa saa milloinkin käyttää. Tärkeimpänä protokollana CSMA/CD. (Kurose & Ross 2017, 480-481.)

2.3.9 CSMA ja CSMA/CD

CSMA (Carrier Sense Multiple Access)on monipääsyprotokolla, jossa solmu kuuntelee kanavaa ennen lähettämistä. Jos jokin toinen solmu on lähettämässä kehystä kanavalle, solmu odottaa kunnes se ei havaitse enää lähetyksiä lyhyeen aikaan ja aloittaa sitten lähetyksen. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) on CSMA:han pohjautuva monipääsyprotokolla, jossa lisäksi toimintona tunnistaa solmujen välillä tapahtuneita törmäyksiä. Törmäyksen tapahtuessa törmäyksen osapuolet lähettävät muille solmuille häirintäsignaalin, ilmoittaakseen muille solmuille, että on tapahtunut törmäys. Solmut, jotka näkevät häirintäsignaalin käynnistävät algoritmin perääntymistä varten. Algoritmi luo laitteelle ajastimen, jossa on satunnainen määrä aikaa. Ajastin määrää, milloin solmu voi lähettää seuraavan kerran dataa. Ajastimen päättyessä solmut ovat vapaita lähettämään dataa. (Quine 2008; ATIS 2013.)

2.3.10 Fyysinen osoitteistaminen

Linkkikerroksella laitteiden identifioimiseen käytetään MAC-osoitteita. Sen tehtävä on saada kehys viedyksi yhdestä liitännästä toiseen fyysisesti kytkettyyn liitäntään.
MAC-osoitteen pituus on 6 tavua, ja se ilmoitetaan heksadesimaaleina, joissa yksi tavu vastaa yhtä paria heksadesimaali numeroita. MAC-osoite on suunniteltu pysyväksi,

vaikkakin nykyään se on mahdollista muuttaa ohjelmallisesti. Jokaisella verkkoon kytketyn laitteen verkkokortilla on täysin uniikki MAC-osoite. MAC-osoiteavaruutta hallitsee IEEE, jolta verkkokorttien valmistajat ostavat osoitealueita käyttöönsä. (Kurose & Ross 2017, 496-497.)

2.3.11 ARP

Koska verkossa laitteilla on linkkikerroksen fyysisen MAC-osoitteen lisäksi käytössä verkkokerroksen looginen IP-osoite, jota käytetään verkkokerroksen pakettien ohjaamiseen kohdeverkkoon, syntyy tarve tehdä käännöksiä osoitteiden välillä. Kohteen IP-osoitteen tietäminen ei siis riitä, vaan verkkokortin on tiedettävä kohteen MAC-osoite. Tähän tarkoitukseen on kehitetty ARP-protokolla (Address Resolution Protocol), jonka tehtävä on selvittää laitteen loogista IP-osoitetta vastaava fyysinen MAC-osoite. ARP selvittää MAC-osoitteen tekemällä kyselyn verkon kaikille laitteille, jossa se kysyy kuka IP-osoitteen omistaja on. IP-osoitteen omistaja vastaa kyselyyn omalla MAC-osoitteellaan. (Knipp ym. 2002, 43; Fall & Stevens 2012, 165; Conrad ym. 2015, 235; Kurose & Ross 2017, 498.)

2.3.12 Kytkin

Kytkin on linkkikerroksella toimiva laite, jonka tehtävä on varastoida ja välittää Ethernet kehyksiä. Se välittää kehyksiä eteenpäin yhteen tai useampaan linkkiin, riippuen kohteen MAC-osoitteesta. Kytkin on läpinäkyvä laite, mikä tarkoittaa, että verkon muut laitteet eivät ole tietoisia sen olemassaolosta. Kytkin ylläpitää kytkintaulua, jonka pohjalta se päättelee, minne kehykset kuuluu ohjata. Taulu pitää sisällään merkintöjä verkon laitteista. Merkintä sisältää MAC-osoitteen, kytkimen portin, joka johtaa kyseiseen MAC-osoitteeseen ja kellonajan, jolloin merkintä lisättiin tauluun. (Kurose & Ross 2017, 509; Cisco Networking Academy 2016, luku 4.2.1.1.)

Kytkimen eräs hienoimmista ominaisuuksista on se, että kytkintaulu rakentuu automaattisesti, dynaamisesti ja autonomisesti ilman manuaalista konfiguraatiota. Kytkin on siis itseoppiva laite. Kytkin tallentaa jokaisen saapuvan kehyksen lähdeosoitteen,

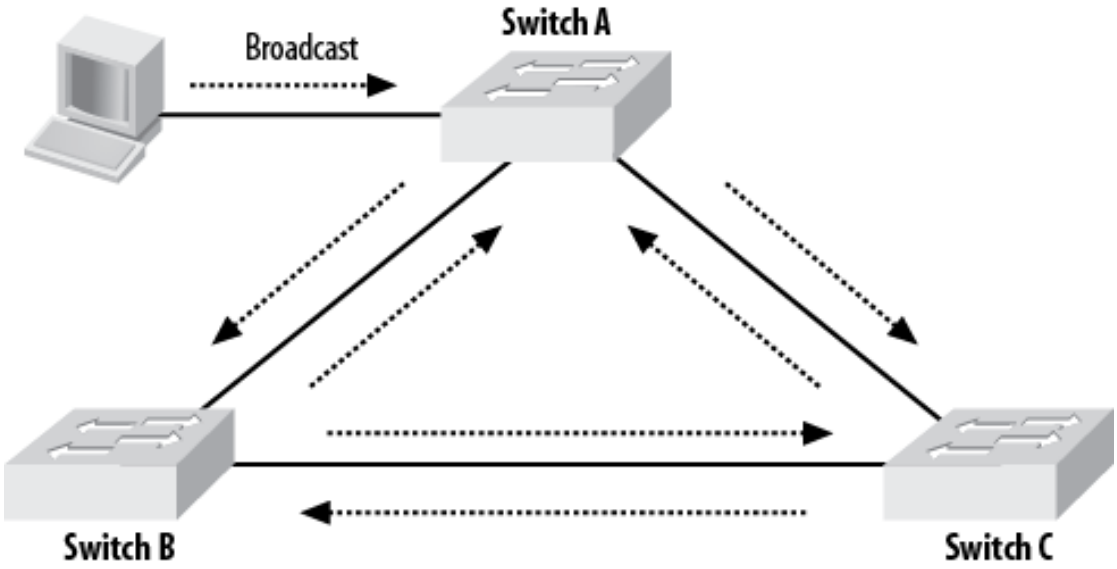
portin ja saapumisajan. Ajallaan taulussa on siis tallennettuna jokainen kehyksiä lähettänyt laite. Kytkin poistaa osoitteita taulusta, mikäli lähdeosoitteen omaavia kehyksiä ei ole vastaanotettu tietyn ajan puitteissa. Esimerkiksi verkosta poistetun tietokoneen MAC-osoite tulee lopulta häviämään taulusta. (Kurose & Ross 2017, 511.)

Kytkimet ovat plug-and-play laitteita. Uuden kytkimen käyttöönotto ei vaadi muuta kuin kaapelien kytkemisen portteihin. Ylläpitäjän ei tarvitse konfiguroida kytkintaulua käyttöönoton aikana tai edes silloin, kun jokin laite poistuu käytöstä. Kytkimet ovat myös kaksisuuntaisia (eng. full duplex) laitteita, joka tarkoittaa, että mikä tahansa kytkimen portti kykenee lähettämään ja vastaanottamaan dataa samaan aikaan. (Kurose & Ross 2017, 512.)

2.3.13 Spanning Tree Protocol

Spanning Tree Protocol (lyh. STP) on protokolla, joka on kehitetty estämään silmukoiden syntymistä siltojen välillä Layer-2 verkoissa. Sillalla tarkoitetaan linkkikerroksen laitetta, joka yhdistää useita lähiverkkosegmenttejä. Muun muassa kytkimet luokitellaan silloiksi. Kun kytkin vastaanottaa yleislähetyksen, se toistaa kyseisen yleislähetyksen jokaisessa portissa, paitsi siinä portissa, jossa yleislähetys vastaanotettiin. Mikäli kytkimet muodostavat silmukan, yleislähetykset jäävät kiertämään kytkinten välillä ikuisesti. Tätä ilmiötä kutsutaan yleislähetys-myrskyksi ja ajallaan se tulee johtamaan koko verkon pysähtymiseen, sen täyttyessä yleislähetyksistä. (Donahue 2011, 81.)

Kuviossa 1 kytkimeen A kytketty PC lähettää yleislähetyskehyksen. Tämän jälkeen kytkin A lähettää kopion yleislähetyksestä kytkimelle B ja kytkimelle C. Kytkin B toistaa yleislähetyksen kytkimelle C, ja kytkin C toistaa yleislähetyksen kytkimelle B, jonka jälkeen kytkin B ja kytkin C toistavat lähetyksen takaisin Kytkimelle A. Sitten kytkin A toistaa kytkimeltä B tulleen yleislähetyksen kytkimelle C ja Kytkimeltä C tulleen yleislähetyksen kytkimelle B. Tätä jatkuu loputtomiin, kunnes silmukka rikotaan jotenkin. Spanning tree on automatisoitu mekanismi, joka on suunniteltu tällaisten silmukoiden löytämiseen ja rikkomiseen. (Donahue 2011, 82.)



Kuvio 1. Yleislähetysmyrsky (Donahue 2011, 82.)

STP valitsee lähiverkosta ns. juurikytkimen (eng. root switch). Juurikytkin on kytkin, joka muiden kytkinten tulee saavuttaa pienimmällä mahdollisella kustannuksella (eng. path cost). STP laskee jokaisen kytkimen jokaisen juurikytkimelle johtavan polun kustannuksen. Pienimmän kustannuksen omaava polku pidetään ja muut polut rikotaan. STP rikkoo polkuja asettamalla kytkinten portteja blocking-tilaan. Jokainen kytkin verkossa, joka tukee STP:tä, lähettää kahden sekunnin välein kehyksiä, joita kutsutaan nimellä bridge protocol data unit (BPDU). Nämä kehykset sisältävät tietoja, joita kytkimet tarvitsevat suorittaakseen STP:n toiminnan kannalta kriittisiä toimintoja, joita käsitellään seuraavaksi. (Froom ym. 2010, luku 3; Donahue 2011, 88-89.)

Juurikytkimen valinta. Jokaisella kytkimellä on oma kytkin ID. Kytkin ID on yhdistelmä kytkimen prioriteettiä ja kytkimen MAC-osoitetta. Kytkimen prioriteettiä on myös mahdollista konfiguroida käsin. Alhaisimman kytkin ID:n omaavava kytkin valitaan juurikytkimeksi. (Froom ym. 2010, luku 3; Donahue 2011, 89.)

Parhaimman juurikytkimelle johtavan polun valinta. Jos juurikytkimeltä saapuvia BPDU:ita vastaanotetaan useammassa portissa kuin yhdessä, on juurikytkimelle useampia polkuja kuin yksi. Paras polku löytyy sen BPDU:n vastaanottaneen portin takaa, jossa kustannukset olivat pienimmät. (Froom ym. 2010, luku 3; Donahue 2011, 89.)

Kytkimen juuriportin (eng. root port) valinta. Juuriportti on kytkimen portti, josta on lyhyin matka juurikytkimelle. Jokaisella kytkimellä on vain yksi juuriportti. Juurikytkimellä ei ole juuriportteja. (Froom ym. 2010, luku 3; Donahue 2011, 89.)

Segmentin nimetyn portin (eng. designated port) valinta. Nimetty portti on portti, joka on olemassa juurikytkimellä ja nimetyillä kytkimillä. Juurikytkimen kaikki portit ovat nimettyjä portteja. Nimetty portti on juuriportista seuraavaksi pienimmän kustannuksen polun juurikytkimelle omaava portti. Segmentillä voi olla vain yksi nimetty portti. (Froom ym. 2010, luku 3; Donahue 2011, 89.)

Segmentin nimetyn kytkimen valinta. Segmentin kytkin, joka omaa nimetyn portin luokitellaan nimetyksi kytkimeksi. Jos segmentissä on useampia kytkimiä, käydään läpi valintaprosessi, jossa alhaisimman kytkin ID:n omaava kytkin valitaan nimetyksi kytkimeksi. (Froom ym. 2010, luku 3; Donahue 2011, 89.)

Liikennettä ohjaamattomien porttien blokkaus. Portit, jotka ovat ottaneet vastaan BPDU:ita, mutta eivät ole nimettyjä portteja tai juuriportteja, asetetaan blokkaavaan tilaan. Hallinnollisesta näkökulmasta portit ovat käytössä, mutta ne eivät ohjaa liikennettä poislukien BPDU-kehykset, joita ne vielä lähettävät ja vastaanottavat. (Donahue 2011, 89.)

2.3.14 Konvergenssi

Konvergenssia tapahtuu kun STP-prosessi on suoritettu (juurikytkin on valittu, juuriportit ja nimetyt portit on valittu ja asetettu edelleenlähettävään tilaan ja liikennettä ohjaamattomat portit blokattu). Dataa ei edelleenlähetetä ennen kuin konvergenssi on ohi ja kaikkien kytkinten tietokannat päivitetty. Konvergenssia tapahtuu siis aina topologian muuttuessa ja se vie aikaa, mutta se on tärkeää, koska se varmistaa, että kaikilla kytkimillä on käytössä sama tietokanta verkon topologiasta. (Lammle 2011, luku 10.)

2.3.15 Rapid Spanning Tree Protocol

STP suunniteltiin silloin, kun konvergenssiin menevä aika ei ollut ongelma. Nykyaikana tämä aiheuttaa ongelmia verkoissa, joissa käytetään reaaliaikaisia sovelluksia. Tähän ongelmaan ratkaisuna IEEE kehitti taaksepäin yhteensopivan RSTP:n (Rapid Spanning Tree Protocol), joka nopeuttaa konvergenssiaikaa huomattavasti. RSTP:ssä porttien tiloja on vain kolme:

- discarding
- learning
- forwarding.

Discarding tilassa oleva portti vastaa STP:n blokcing, listening ja disabled tiloja. Kuten STP, RSTP käyttää vielä juurikytkimiä, juuriportteja ja nimettyjä portteja ja niillä on edelleen samat roolit kuin STP:ssä. RSTP lisää kuitenkin kaksi uutta porttityyppiä, jotka ovat alternate portti ja backup portti. Nämä kaksi porttia ovat samankaltaisia STP:n blocking tilassa olevien porttien kanssa. Alternate porttia voidaan pitää toissijaisena käyttämättömänä juuriporttina ja backup porttia toissijaisena käyttämättömänä nimettynä porttina. (Deal 2008, 454-455.)

2.3.16 Virtuaalilähiverkko

Virtuaalilähiverkkojen ymmärtämisen kannalta on oleellista olla tietoinen virtuaalilähiverkkoja hyödyntämättömien lähiverkkojen puutteista, joita käsittelen seuraavaksi.
Liikenteen eristyksen puute. Ilman virtuaalilähiverkkoja lähiverkon laitteet muodostavat yhden yleislähetysalueen. Tämä tarkoittaa sitä, että kaikki yleislähetysliikenne (esim. ARP) lähetetään koko lähiverkkoon. Yleislähetysliikenteen rajaaminen esim. osastokohtaisesti lisäisi lähiverkon suorituskykyä ja tietoturvaa. (Kurose & Ross 2017, 516; Molenaar 2020.)

Kytkinten tehoton hyödyntäminen. Lähiverkon eri osien eristämiseksi jouduttaisiin hankkimaan reititin, ja jokaiselle osalle jouduttaisiin hankkimaan oma kytkin. Kytkimistä jäisi todennäköisesti myös portteja käyttämättä, mikäli osien laitemäärät ovat pieniä. (Kurose & Ross 2017, 516; Molenaar 2020.)

Haasteellinen käyttäjien hallinta. Jos käyttäjä siirtyy lähiverkon eri osaan, jouduttaisiin fyysistä kaapelointia muuttamaan. Käyttäjät, jotka kuuluvat kahteen eri osaan tekevät tilanteesta vielä haasteellisemman. (Kurose & Ross 2017, 516.)

Virtuaalilähiverkko (eng. Virtual Local Area Network lyh. VLAN) mahdollistaa lähiverkon osien eristämisen ilman erillistä reititintä. Nimensä mukaisesti VLAN:eja tukeva kytkin mahdollistaa useiden loogisten virtuaalilähiverkkojen luonnin yhden fyysisen lähiverkon päälle. Porttiperusteisessa VLAN:issa kytkimen portit on jaettu ryhmiin. Jokainen ryhmä muodostaa oman VLAN:in ja jokainen VLAN muodostaa oman yleislähetysalueen, mikä tarkoittaa, että ryhmään kuuluvan portin lähettämä yleislähetysliikenne lähetetään pelkästään ryhmään kuuluville porteille. Portin lisäksi VLAN-jäsenyys on mahdollista asettaa myös päätelaitteen MAC-osoitteen perusteella. VLAN-jäsenyydet ovat dynaamisia, mikä tarkoittaa, että niitä voidaan vaihtaa koska tahansa tarpeen mukaan. Eri VLAN:ien välisen liikenteen välittämiseen tarvitaan reititin. (Kurose & Ross 2017, 516; Netgear 2020.)

VLAN-kehyksien kuljettamiseen usean fyysisen kytkimen yli käytetään tähän tarkoitukseen konfiguroitavissa olevaa trunk-porttia. Trunk-portti on jokaisen VLAN:in jäsen. Toimiakseen trunk-portin täytyy tietää mihin VLAN:iin siihen saapuva kehys kuuluu. Tätä varten IEEE on kehittänyt laajennetun Ethernet-kehysformaatin trunk-porttien välisille kehyksille, jota kutsutaan 802.1Q:ksi. 802.1Q:n rakenne vastaa normaalin Ethernet-kehyksen rakennetta, mutta sen otsakkeeseen on lisätty 4-tavua pitkä VLAN-tagi, joka pitää sisällään tiedon VLAN:ista, johon kyseinen kehys kuuluu. Lähettävän kytkimen trunk-portti lisää VLAN-tagin kehykseen ja vastaanottavan kytkimen trunk-portti jäsentelee ja poistaa sen kehyksestä. (Kurose & Ross 2017, 516.)

2.4 Layer 3

Layer 3, joka tunnetaan myös verkkokerroksena (eng. network layer) on seitsemänkerroksisen OSI-mallin kolmas kerros. Verkkokerros vastaa siitä, että saapuvat paketit löytävät tiensä määränpäähän. Onnistuakseen tässä verkkokerroksen täytyy tuntea verkon topologiaa (tässä tapauksessa muut reitittimet ja linkit), ja valita sen läpi kulke-

vista reiteistä eri tilanteisiin sopivimmat. Reittiä valittaessa, sen täytyy välttää kuormittamasta joitakin linjoja ja reitittimiä liikaa. Verkkokerroksen täytyy myös osata kuljettaa paketit perille tilanteissa, joissa kohdeosoite ja lähdeosoite sijaitsevat täysin eri verkoissa. (Tanenbaum & Wetherall 2011, 355.)

2.4.1 Internet protokolla

Internet protokollasta (lyh. IP) on käytössä tänä päivänä kaksi versiota IPv4 ja IPv6, mutta tässä työssä IP:stä puhuttaessa viitataan versioon 4 (IPv4). IP vastaa verkkokerroksen datagrammien ts. datapakettien siirrosta kohteesta lähteeseen, käyttäen kiinteän pituuden omaavia osoitteita niiden tunnisteina. Lähetykseen liian suuret datagrammit lohkotaan pienempiin osiin ja kasataan myöhemmin uudestaan. IP luokitellaan epäluotettavaksi palveluksi, sillä se ei takaa, että datagrammit saapuvat perille, eikä se myöskään toteuta virheenkorjausta. IP on myös yhteydetön, mikä tarkoittaa, että se kohtelee kaikkia datagrammeja itsenäisinä, täysin toisistaan riippumattomina kokonaisuuksina. (RFC 791 1981,1-2; Kurose & Ross 2017, 220,357.)

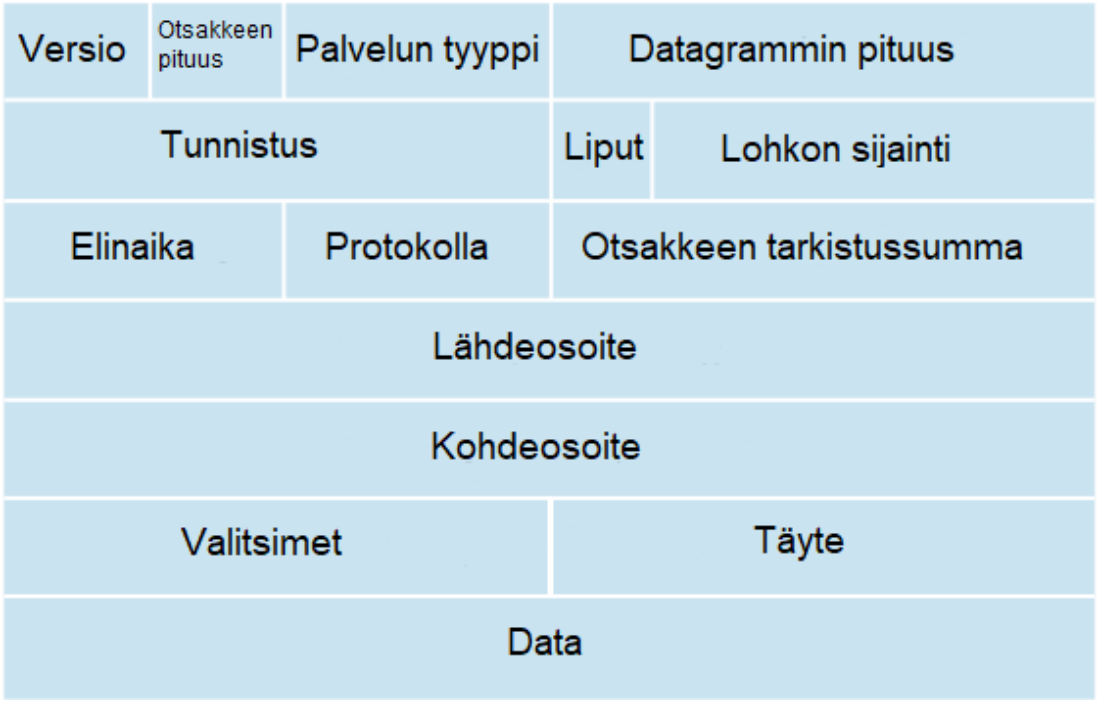
2.4.2 IP-datagrammin rakenne

Verkkokerroksella toimivia paketteja kutsutaan myös IP-datagrammeiksi. IP-Datagrammi koostuu kahdesta osasta; otsakkeesta (eng. header) ja datasta. Datagrammin otsake koostuu lisäksi useista eri kentistä, joiden sisältämä tieto on koko verkkokerroksen toiminnan kannalta erittäin tärkeää. IP-Datagrammi koostuu seuraavista kentistä, jotka visualisoitu kuviossa 2:

- Versio määrittää käytettävän IP:n versio numeron. IPv4 ja IPv6 datagrammien rakenteet eroavat toisistaan, joten reititin katsoo tätä numeroa, jotta se osaa jatkossa tulkita datagrammin loppuosaa
- Otsakkeen pituus kertoo yksiselitteisesti datagrammin otsake-osuuden pituuden
- Palvelun tyyppi-kenttää (eng. Type of service lyh. TOS) käytetään erityyppisten datagrammien erotteluun toisistaan antamalla niille prioriteetti arvo
- Datagrammin pituus kertoo koko datagrammin pituuden, sisältäen otsakkeen ja datan

- Tunnistus-kenttää (eng. identification) käytetään tunnistamaan lohkottujen datagrammien osat
- Liput-kentällä (eng. flags) kerrotaan, että datagrammia ei saa lohkota, tai että datagrammi on lohkottu, ja lisää osia on tulossa
- Lohkon sijainti (fragment offset) kertoo mihin kohtaan lohkottu osa kuuluu datagrammissa
- Elinaika-kenttää (eng. Time to Live lyh. TTL) voidaan pitää datagrammin elinikänä. Sen tarkoitus on varmistaa, ettei datagrammi jää kiertämään verkkoon ikuisesti tilanteissa, joissa se ei löydä määränpäätään. Kentällä on numeerinen arvo, joka pienenee aina yhdellä, kun reititin käsittelee datagrammin. Arvon saavuttaessa nollan, reititin pudottaa datagrammin
- Protokolla kenttää käytetään tyypillisesti vasta datagrammin saavuttaessa päämääränsä. Se määrittää kuljetuskerroksen protokollan, jolle datagrammi luovutetaan. Protokollat ovat tunnistettavissa standardoiduilla numeroilla
- Otsakkeen tarkistussumman arvoa käytetään otsakkeen sisältämän tiedon tarkistamiseen virheiden varalta
- Lähdeosoite kertoo datagrammin lähteen IP-osoitteen
- Kohdeosoite kertoo datagrammin kohteen IP-osoitteen
- Valitsimet (eng. options) on usein tyhjäksi jätetty kenttä, joka mahdollistaa otsakkeen laajentamisen valinnaisilla tiedoilla, kuten esim. aikaleima
- Täyte (eng. padding) varmistaa, että otsakkeen pituus on 32:en bitin monikerta
- Data-kenttä sisältää datagrammissa kuljetettavan korkeamman kerroksen (kuljetuskerroksen) dataa. Joissain tapauksissa kenttä saattaa sisältää myös muun tyyppistä dataa, kuten ICMP-viestejä.

(RFC 791 1981,22; McMillan 2015, luku 4; Kurose & Ross 2017, 358-360.)



Kuvio 2. Datagrammin rakenne (mukaillen McMillan 2015, luku 4; Kurose & Ross 2017, 358.)

2.4.3 IP-osoite

IP-osoitteet ovat verkkolaitteiden verkkoliitäntöjen osoitteita, joita käytetään laitteiden tunnistamiseen verkossa. Toisin kuin fyysiset MAC-osoitteet, IP-osoitteet ovat loogisia osoitteita, joiden implementaatiosta vastaavat verkkojen ylläpitäjät. IP-osoitteita käytetään laitteiden erotteluun toisistaan, ja se toimii arvona, jota käytetään laitteen löytämiseen. (McMillan 2015, luku 7.)

Toinen tärkeä IP-osoitteiden toiminto on laitteiden segmentointi erillisiin lähiverkkoihin. Kun laitteet ovat eri lähiverkoissa, ne eivät voi kommunikoida keskenään ilman reititintä. Vaikka laitteet olisi kytketty samaan kytkimeen, tai jopa suoraan keskenään, ei kommunikaatiota voi tapahtua, jos IP-osoitteet ovat eri verkoissa. Lähiverkkojen segmentointia toteutetaan seuraavista syistä:

- suorituskyvyn parantaminen. Reitittimet eivät ohjaa eteenpäin yleislähetysliikennettä lähiverkosta toiseen. Tämä pitää yleislähetysliikenteen suljettuna lähiverkon sisällä, mikä tarkoittaa pienempiä yleislähetysalueita.
- tietoturvan parantaminen. Laitteiden ollessa eri lähiverkoissa, pääsyä toiseen voidaan rajoittaa reitittimellä. Rajoitus toteutetaan pääsylistoilla (eng. Access list), joissa määritellään, mikä liikenne on sallittua lähiverkkojen välillä ja mikä ei.
- verkkojen laajentaminen. Koska minkä tahansa yksittäisen lähiverkon kasvu tulee jossain vaiheessa ilmenemään suorituskyvyn laskuna, syntyy tarve luoda lisää lähiverkkoja. Kyky luoda lisää reitittimiin kytkettyjä lähiverkkoja mahdollistaa verkon skaalautuvuuden, ilman suorituskyvyn laskua.
- ongelmien eristäminen. Reitittimen segmentoimissa pienemmissä lähiverkoissa verkon ongelmia on helpompi eristää. Koska liikenne on rajattu lähiverkkoon, myös ongelmat ovat rajattu lähiverkkoon. Kytkinten ja reitittimien laiteviat vaikuttavat myös pienempään osaan verkkoa

(McMillan 2015, luku 7.)

IP-osoitteet esitetään ihmisille helpommin ymmärrettävässä desimaalimuodossa, mutta niiden käsittely tapahtuu binäärimuodossa. Binäärimuodossa IP-osoitteiden pituus on 32-bittiä, jotka on jaettu neljään osaan, joita kutsutaan okteteiksi. Jokaisella IP-osoitteella on kaksi osaa, verkon osa ja laitteen osa. Vasemmalta alkava verkon osaa määrittää lähiverkon, josta laite löytyy, ja lopusta löytyvä laitteen osa tunnistaa laitteen kyseisestä lähiverkosta. (McMillan 2015, luku 7.)

Laitteet käyttävät aliverkon peitteeksi kutsuttua arvoa selvittämään, mikä osa osoitteesta kuuluu verkolle, ja mikä laitteelle. Laitteella ei voi olla IP-osoitetta ilman aliverkon peitettä. Jokaisessa lähiverkossa on kaksi IP-osoitetta, joita ei voida ikinä antaa laitteille. Nämä osoitteet on varattu erityisiä rooleja varten. Nämä osoitteet ovat verkon osoite ja yleislähetysosoite. Nämä osoitteet voidaan tunnistaa lähiverkossa osoitteen laiteosan biteistä. Jos kaikki laiteosan bitit ovat nollia, osoite on verkon osoite. Jos kaikki bitit laiteosasta ovat ykkösiä (desimaaleina 255) on kyseessä yleislähetysosoite. (McMillan 2015, luku 7.)

Verkon osoitetta käytetään verkon tunnistamiseen ryhmänä. Se on tärkeä arvo, jota reitittimet käyttävät reititystauluissa. Jos verkon osoitetta ei olisi olemassa, joutuisi reitin tekemään jokaiselle laitteelle oman merkinnän reititystauluun, joka tekisi reititystauluista todella suuria ja koko reititys prosessi hidastuisi merkittävästi. Käyttämällä verkon osoitetta reitin voi reitittää paketteja mille tahansa lähiverkossa sijaitsevalle laitteelle, jonka jälkeen se reitin, joka on fyysisesti yhdistetty kyseiseen lähiverkkoon käyttää ARP:ia löytämään laitteen. (McMillan 2015, luku 7.)

Yleislähetysosoitetta käytetään aina, kun laitteen tarvitsee lähettää paketti jokaiselle laitteelle lähiverkossa. ARP:in lisäksi yleislähetyksiä lähetetään mm. Dynamic Host Configuration Protokollan (lyh. DHCP) yhteydessä, kun laitteet yrittävät löytää DHCP-palvelinta. (McMillan 2015, luku 7.)

2.4.4 DHCP

IP-osoitteet voidaan asettaa käsin manuaalisesti, mutta tyypillisesti tähän käytetään DHCP:tä. DHCP on palvelimen tai reitittimen tarjoama palvelu, jonka tehtävä on automatisoida IP-osoitteiden, aliverkon peitteiden, oletusyhdyskäytävien, sekä muiden verkon asetusten asettaminen. Se auttaa myös estämään konflikteja IP-osoitteiden välillä, pitämällä kirjaa jo jaetuista osoitteista ja jakamattomista osoitteista. (McMillan 2015, luku 7.)

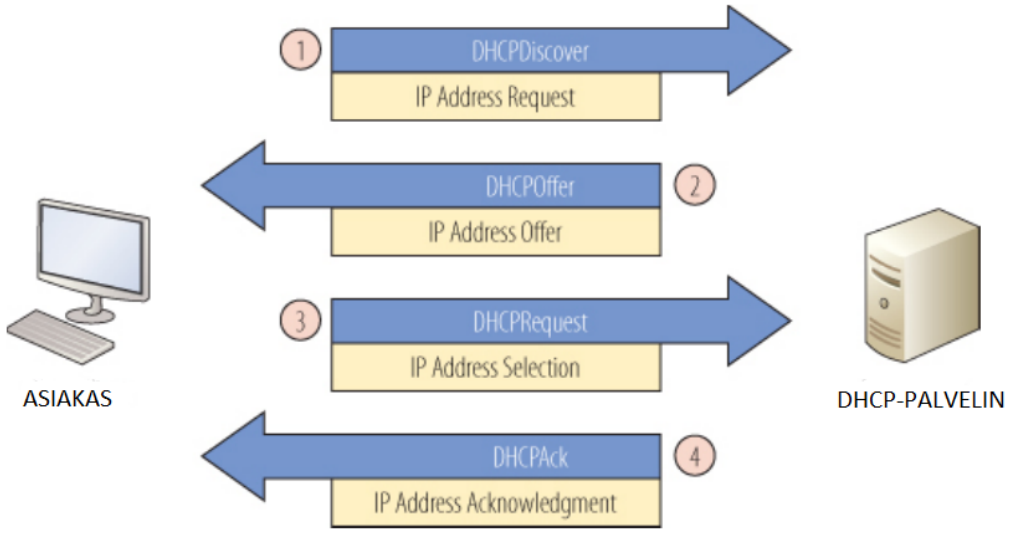
Ennen kuin DHCP-palvelin tai reitin voi toimia, tarvitsee palvelun päälle asettamisen lisäksi luoda IP-osoitealue. Osoitealue on joukko IP-osoitteita, jota DHCP-palvelin tai reitin käyttää osoitteiden jakamiseen. DHCP-palvelin jakaa nämä osoitteet pyyntöjen saapumisjärjestyksessä, ja merkitsee jaetut osoitteet päällekkäisyyksien estämiseksi. DHCP voidaan konfiguroida siten, että tietty laite saa aina saman IP-osoitteen muodostaessaan yhteyden verkkoon. Konfigurointi voidaan toteuttaa myös siten, että laite saa aina väliaikaisen IP-osoitteen, joka vaihtuu aina yhteyttä muodostaessa. (McMillan 2015, luku 7; Kurose & Ross 2017, 370.)

DHCP on asiakas-palvelin protokolla, jossa asiakkaina toimivat verkkoon kytketyt uudet laitteet, jotka haluavat saada käyttöön verkkoasetukset. Kuviosta 3 näemme, että

protokolla on nelivaiheinen prosessi, jossa asiakas ja palvelin vaihtelevat keskenään seuraavaa neljää eri viestityyppiä:

- DHCPDisocver. Ensimmäinen tehtävä, joka uuden laitteen on suoritettava, on löytää verkosta DHCP-palvelin. Tähän tarkoitukseen käytetään DHCPDiscover-viestiä, joka lähetetään yleislähetyksenä kaikille verkon solmuille.
- DHCPOffer. DHCP-palvelin, joka vastaanottaa DHCPDiscover-viestin, vastaa asiakkaalle DHCPOffer-viestillä, joka pitää sisällään asiakkaan pyytämät verkkoasetukset ja ns. vuokra-ajan (eng. lease time). Vuokra-aika määrittää, kuinka kauan pyydetty IP-osoite on voimassa. DHCPOffer lähetetään myös yleislähetyksenä kaikille verkon solmuille.
- DHCPRequest. Mikäli DHCP-palvelimia on useampi, valitsee laite yhden DHCPOffer-viestin saapuneiden tarjouksien joukosta, ja vastaa siihen DHCPRequest-viestillä, joka vastaa sisällöltään valittua DHCPOffer-viestiä.
- DHCPAck. DHCP-palvelin vastaa DHCPRequest-viestiin DHCPAck-viestillä varmistaen pyydetyt asetukset. Kun laite vastaanottaa DHCPAck-viestin, on prosessi ohi, ja laite saa käyttöönsä pyydetyt verkkoasetukset. DHCP tarjoaa myös mekanismin vuokra-ajan jatkamiselle, mikäli laite haluaa pitää saamansa verkkoasetukset vuokra-ajan päätyttyä.

(Kurose & Ross 2017, 370-373.)



Kuvio 3. DHCP-prosessi (mukaillen McMillan 2015, luku 7.)

2.4.5 NAT

Kaikki IP-osoitteet voidaan luokitella kahteen pääryhmään; julkiset IP-osoitteet ja yksityiset IP-osoitteet. Julkiset IP-osoitteet ovat Internetissä reititettäviä globaalisti uniikkeja osoitteita. Jotta laite pääsee kiinni Internetissä sijaitseviin palveluihin, tarvitsee se käyttöönsä julkisen IP-osoitteen. Yksityiset IP-osoitteet ovat paikallisessa verkossa käytettäviä osoitteita, joita ei reititetä Internettiin, eikä niihin voi lähettää liikennettä Internetistä. Yksityiset IP-osoitteet toimivat siis vain sisäverkon sisällä. Jos halutaan yhdistää yksityisen osoitteen omaava laite Internettiin, voidaan tähän tarkoitukseen käyttää osoitteenmuunnosta (eng. network address translation, lyh. NAT). (Keenetic 2019.)

NAT on reitittimissä toimiva tekniikka, jolla yksityisiä osoitteita käyttävät laitteet saadaan yhdistettyä Internettiin. NAT muuntaa sisäverkon yksityiset osoitteet Internetissä toimiviksi julkisiksi osoitteiksi ennen paketin lähettämistä. Reitittimellä on yleensä käytössä yksi palveluntarjoajalta saatu julkinen osoite. NAT:in avulla saadaan tämä yksi osoite edustamaan kaikkia sisäverkon laitteita. Tämä säästää rajallisen määrän omaavia julkisia osoitteita, ja piilottaa sisäverkon yksityiskohtia ulkomaailmalta. (Kurose & Ross 2017, 375; Cisco 2020b.)

2.4.6 ICMP

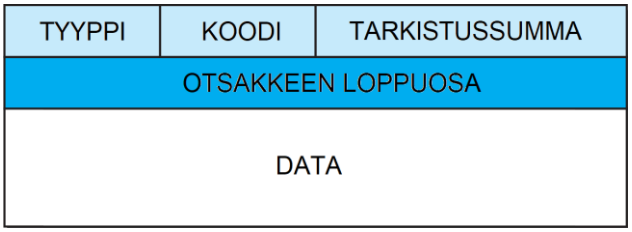
Aikaisemmin kävi ilmi, että IP ei toteuta virheiden raportointia tai virheiden korjausta. Reititin pudottaa datagrammin, koska se ei löydä päämäärään johtavaa reititintä. Datagrammin TTL-kenttä laskee nollaan. Kohdelaite pudottaa datagrammin palaset, koska se ei vastaanottanut niitä kaikkia ajoissa. Nämä kaikki ovat tilanteita, joissa on tapahtunut virhe, eikä IP:llä ole mitään sisäänrakennettua mekanismia huomauttaa lähdelaitetta. IP:llä ei ole myöskään mekanismia toteuttaa kyselyitä. Laitteella on joskus tarve tietää, onko reititin tai jokin toinen laite elossa tai saavutettavissa. Myös verkon ylläpitäjän tarvitsee saada tietoa verkon laitteista. Näitä IP:n puutteita kompensoimaan on kehitetty Internet Control Message Protocol (lyh. ICMP). (Forouzan 2013, 574-575.)

ICMP:n on verkkokerroksen protokolla, jonka tarkoitus on generoida viestejä. ICMP-viestit jaetaan kahteen kategoriaan; virheiden raportointia toteuttavat viestit ja kyselyitä toteuttavat viestit. Virheiden raportointia toteuttavat viestit raportoivat ongelmista, joita reititin tai kohdelaite saattavat kohdata, prosessoidessaan datagrammia. Kyselyitä toteuttavat viestit, jotka toimivat pareina, auttavat lähdelaitetta tai ylläpitäjää saamaan tietoa reitittimestä tai jostain toisesta kohdelaitteesta. (Forouzan 2013, 575.)

ICMP-viestit enkapsuloidaan datagrammin sisälle. Viestin otsakkeen formaatti vaihtelee tyypin mukaan, mutta viestin yleismuoto pysyy samana. Kuviosta 4 näemme, että ICMP-viestin yleismuoto pitää sisällään seuraavat kentät:

- ICMP tyyppi. Määrittää viestin tyypin
- koodi. Määrittää syyn tietylle viestityypille
- tarkistussumma. Käytetään virheiden tarkastusta varten. ICMP:n tapauksessa lasketaan otsakkeesta ja datasta
- otsakkeen loppuosa vaihtelee, riippuen viestin tyypistä
- data-kenttä pitää sisällään tietoa alkuperäisen virheellisen paketin löytämiseksi. Kyselyitä toteuttavissa viesteissä data-kenttä pitää sisällään ylimääräistä tietoa riippuen kyselyn tyypistä

(Forouzan 2013, 575.)



Kuvio 4. ICMP-viestin rakenne (mukaillen Forouzan 2013, 575.)

Koska IP on epäluotettava protokolla, yksi ICMP:n päätehtävistä on raportoida datagrammin prosessoinnin aikana tapahtuvista mahdollisista virheistä. ICMP ei korjaa virheitä, se vain raportoi niistä. Virheiden korjaus on ylemmän tason protokollien vastuulla. Virheviestit lähetetään aina alkuperäiseen lähdeosoitteeseen, sillä ainoat datagrammin reitistä kertovat tiedot ovat lähdeosoite ja kohdeosoite. ICMP käyttää lähdeosoitetta virheviestin lähettämiseen datagrammin lähteelle (lähettäjälle). Tehdäkseen

virheiden raportointiprosessista yksinkertaisen, ICMP noudattaa muutamia sääntöjä. Ensimmäiseksi, virheviestiä ei generoida datagrammille, joka sisältää ryhmälähetysosoitteen tai jonkin muun erikoisosoitteen. Toiseksi, virheviestiä ei generoida vastaukseksi datagrammille, joka kantaa virheviestiä. Kolmanneksi, virheviestiä ei generoioda lohkotulle datagrammille, joka ei ole ensimmäinen lohko. (Forouzan 2013, 576.)

Toisin kuin virheviestien kohdalla, kyselyviestejä voidaan käyttää itsenäisesti ilman suhdetta datagrammiin. Kyselyviestit tarvitsee kuitenkin enkapseloida datagrammin sisälle. Kyselyviestejä käytetään mm. verkon laitteiden hengissäolon testaukseen, kahden laitteen välisen datagrammin kiertoviiveen (eng. round-trip time lyh. RTT) mittaukseen, tai jopa selvittämään, ovatko laitteiden väliset kellot synkronoitu samaan aikaan. Kyselyviestit tulevat pareittain pyyntönä ja vastauksena. Tärkeimpinä kyselyviestejä hyödyntävinä työkaluina voidaan pitää pingiä ja traceroutea. (Forouzan 2013, 577-578.)

Ping on pyyntöjä ja vastauksia käyttävä työkalu, joka on suunniteltu selvittämään jonkin toisen IP-osoitteen saavutettavuus. Pyynnön esittäjä lähettää ICMP echo request –viestin haluttuun osoitteeseen. Mikäli viesti toimitetaan perille, kyseisen osoitteen omaava laite lähettää vastauksena ICMP echo reply -viestin aikaisemmin vastaanotetun viestin sisältämään lähdeosoitteeseen. Vastauksen lähettävä ICMP-moduuli kopioi saapuneen pyynnön sisällön vastaukseen, jotta pyynnön esittäjä voi sovittaa saapuneet vastaukset yhteen lähetettyjen pyyntöjen kanssa. Pingillä saadaan selvitettyä mm. kiertoviive. (Forouzan 2013, 578; Vacca 2017, 245.)

Traceroute on toinen pyyntöjä ja vastauksia käyttävä työkalu. ICMP-moduuli generoi traceroute -pyynnön sen käyttämän kohdeosoitteeseen johtavan polun löytämiseksi. Jokainen reitin, joka käsittelee pyynnön, lisää oman IP-osoitteensa vastaanotettuun pyyntöön, ja välittää päivitetyn pyynnön eteenpäin. Pyynnön saapuessa kohteeseen, kohde lähettää kaiken matkalla kerätyn tiedon takaisin lähdeosoitteeseen traceroute -vastauksessa. (Vacca 2017, 245.)

2.4.7 Reititin

Reititin on verkkokerroksella toimiva laite, joka yhdistää useita eri verkkoja keskenään. Kun reititin vastaanottaa datagrammin jossakin portissa, se päättelee mihin verkkoliitäntään datagrammi kuuluu edelleenlähettää, jotta se saavuttaisi määränpäänsä. Verkkoliitäntä, jonka se valitsee edelleenlähetystä varten, voi olla datagrammin määränpää, tai se voi olla verkko, joka on yhdistetty toiseen reitittimeen, jonka takaa kohdeverkko löytyy. (Cisco Networking Academy 2016, luku 1.1.1.4.)

Jokainen verkko, johon reititin on kytketty, vaatii oman verkkoliitännän. Näitä liitäntöjä käytetään kytkemään sekä lähiverkkoja että laajaverkkoja (eng. Wide Area Network, lyh. WAN). Laajaverkolla tarkoitetaan verkkoa, joka yhdistää useita verkkoja maantieteellisesti laajalla alueella. WAN-yhteyttä käytetään usein lähiverkon yhdistämiseen palveluntarjoajan verkkoon. (Cisco Networking Academy 2016, luku 1.1.1.4.)

Reitittimen päätoimintoina on reititys, eli parhaimman polun määrittäminen lähetettäville datagrammaille ja datagrammien edelleenlähetys kohdeosoitteeseen. Reititin toimii usein verkon laitteiden oletusyhdyskäytävänä (eng. default gateway). Reititin voidaan myös asentaa välietapiksi muiden reitittimien väliin, ilman suoraa yhteyttä verkon laitteisiin. Reityksen lisäksi reitittimet voivat suorittaa myös useita muita toimintoja kuten osoitteenmuunnoksia, pääsylistojen hallintaa tai QoS-tekniikoita (Quality of Service). (Hartpence 2011, 7.)

Reitittimen päätoiminnallisuus koostuu kolmesta komponentista; reititysprosessista, reititysprotokollista ja reititystaulusta. Reititysprosessilla tarkoitetaan datagrammin liikettä yhdestä portista toiseen ja reititystaulu puolestaan sisältää tietoja, joita reititysprosessi hyödyntää. Reititysprotokollia kuten Routing Information Protocol (lyh. RIP) tai Open Shortest Path First (lyh. OSPF) käytetään muiden reitittimien kanssa kommunikoimiseen, jonka seurauksena reititystauluun saattaa asentua uusia reittejä, joita voidaan käyttää reititysprosessissa. (Hartpence 2011, 7-8.)

Kun reititin vastaanottaa datagrammin, se tutkii siitä kohdeosoitteen ja käyttää reititystaulua kohdeosoitteen verkolle johtavan parhaan polun etsimiseen. Reititystaulussa

on ilmoitettu jokaista tiedettyä verkkoa vastaava verkkoliitäntä, jota tulee käyttää datagrammien edelleenlähetyksessä. Kun oikea verkkoliitäntä on löydetty, datagrammi enkapsuloidaan lähtevän verkkoliitännän linkkikerroksen kehykseen ja edelleenlähetetään kohti sen määränpäätä. (Cisco Networking Academy 2016, luku 1.1.1.5.)

Reititystaulut voivat koostua useista erilaisista reittityypeistä; suoraan yhdistetyt, staattiset ja dynaamiset. Suoraan yhdistetyt reitit ovat etusijalla muihin reittityyppeihin nähden. (Hartpence 2011, 8.)

2.4.8 Staattiset reitit

Staattiset reitit ovat reititystaulun merkintöjä, jotka verkon ylläpitäjä on käsin asettanut reitittimeen. Joitakin tiettyjä kohteita varten, pienissä tai muuttumattomissa verkkoympäristöissä manuaalisesti konfiguroidut reitit voivat osoittautua erittäin hyödyllisiksi. Staattisia reittejä käyttämällä, verkon ylläpitäjä on päättänyt polun, jota tiettyyn kohdeverkkoon käytetään. Staattinen reitti menee reititysprotokollien kautta löydettyjen reittien edelle, koska sen hallinnollinen etäisyys (eng. administrative distance) on alhaisempi. Toinen reititykselle tärkeä idea on seuraava hyppy (eng. next hop). Seuraavalla hypyllä tarkoitetaan reititintä, joka on askeleen lähempänä määränpäätä jonkin tietyn reitittimen näkökulmasta. Seuraava hyppy on reititin, jolle datagrammi on tarkoitus lähettää seuraavaksi. (Hartpence 2011, 8-9.)

2.4.9 Oletusreitti

Useissa tapauksissa monia kohteita voidaan saavuttaa samaa polkua käyttämällä. Näissä tapauksissa reititystaulu jatkaa kasvamistaan, vaikka monet näistä reiteistä ovat samankaltaisia. Reititystaulun samankaltaiset merkinnät on mahdollista korvata pienemmällä määrällä reittejä, tästä esimerkkinä oletusreitti. Oletusreitti on erityinen staattinen reitti. Oletusyhdyskäytävästä puhuttaessa ajatellaan yleensä päätelaitteita, mutta myös reitittimillä voi olla oletusyhdyskäytävä. Tapauksissa, joissa reititystaulu on käyty läpi, eikä kohdeosoitteelle löydy vastaavaa verkkoa, käytetään oletusreittiä. Kuten staattisten reittien kanssa, verkon ylläpitäjä olettaa, että seuraavan hypyn reititin tietää, kuinka päästä kohteeseen tai seuraavalle hypylle. (Hartpence 2011, 13-14.)

2.4.10 Dynaamiset reitit

Dynaamiset reitit ovat reittejä, jotka on opittu reititysprotokollia kuten RIP:tä tai OSPF:ää käyttämällä. Verkkoa rakentaessa on tärkeää kiinnittää huomiota siihen, miten reititys toteutetaan. Staattiset reitit vaativat vähemmän prosessointia, mutta topologian muutoksia ei voida ratkaista nopeasti. Jos polku kohteeseen muuttuu tai reititin putoaa verkosta, polut tai reitit menetetään. Staattiset reitit eivät myöskään tarjoa suojaa ylläpitäjän tekemiltä virheiltä. Staattisia reittejä käytetään tyypillisesti, kun topologia on vakaa ja verkon arkkitehtuuri yksinkertainen, eli verkon ehdot ymmärretään hyvin. Usein oletetaan, että jos verkon ylläpitäjää asentaa reititin, sen täytyy olla virheetön. Dynaamiset reititysprotokollat suojelevat näiltä topologian muutoksilta ja ylläpitäjän aiheuttamilta virheiltä. Useimmat reititysprotokollat suojelevat myös reitityssilmukoilta ja vanhalta virheelliseltä tiedolta. Monet toteuttavat myös kuormantasausta ja kykenevät tarjoamaan useita polkuja kohteisiin. (Hartpence 2011, 15.)

2.4.11 IGP ja EGP

Sisäinen yhdyskäytäväprotokolla (eng. interior gateway protocol, lyh. IGP) on suunniteltu reittien ylläpitämiseen autonomisen järjestelmän (eng. autonomous system, lyh. AS) sisällä. Autonomisella järjestelmällä tarkoitetaan ryhmää laitteita, joita ylläpitää yksi organisaatio. Esimerkkinä autonomisesta järjestelmästä voisi olla yritys tai koulu, mutta organisaation ei tarvitse kuitenkaan olla niin laaja, vaan autonomista järjestelmää voisi edustaa pelkkä rakennuksen kerros tai yrityksen osasto. (Donahue 2011, 127.)

Ulkoinen yhdyskäytäväprotokolla (eng. exterior gateway protocol, lyh. EGP) on suunniteltu yhdistämään autonomisia järjestelmiä yhteen. Internet on hyvä esimerkki laajamittaisesta EGP-implementaatiosta. Autonomiset järjestelmät ovat kaikki itsenäisiä ja niitä hallitaan sisäisesti sisäisillä yhdyskäytäväprotokollilla ja ne yhdistetään toisiinsa käyttäen ulkoisia yhdyskäytäväprotokollia (Donahue 2011, 127.)

2.4.12 OSPF

OSPF on IP-reititysprotokollaperheeseen kuuluva sisäinen yhdyskäytäväprotokolla, jota käytetään IP-reititystiedon jakeluun yksittäisen autonomisen järjestelmän verkon sisällä. OSPF on linkkitilareititysprotokolla, joka tarkoittaa, että reitittimet vaihtavat topologian tietoja keskenään lähimpien naapureiden kanssa. Topologian tiedot floodataan autonomisen järjestelmän läpi, jotta jokainen sen sisällä oleva reititin saa kokonaiskuvan kyseistä autonomisesta järjestelmästä. Tätä kokonaiskuvaa käytetään sitten laskemaan autonomisen järjestelmän läpi kulkevat päästä-päähän -polut käyttämällä Dijkstra algoritmia. Tästä syystä linkkitilareititysprotokollassa seuraavan hypyn osoite, johon data edelleenlähetetään on määritetty valitsemalla paras lopulliseen määränpäähän johtava päästä-päähän -polku. (Metaswitch 2021a.)

Tärkein OSPF:än kaltaisen linkkitilareititysprotokollan etu on, että topologian täydellinen tunteminen auttaa reitittimiä laskemaan reittejä, jotka täyttävät joitakin tiettyjä kriteerejä. Tästä voi olla apua suunnittelutarkoituksissa, joissa reittejä rajoitetaan, jotta ne vastaisivat tiettyjä palvelunlaatu vaatimuksia. Linkkitilareititysprotokollan suurin huonopuoli on se, että se ei skaalaudu hyvin, kun reititystoimialueeseen lisätään lisää reitittimiä. Reitittimien lisääminen lisää topologia päivitysten määrää ja niiden lähetystahtia, sekä päästä-päähän reittien laskemiseen menevää aikaa. Tämä skaalautuvuuden puute tarkoittaa, että linkkitilareititysprotokolla ei sovi Internetin yli reitittämiseen, ja tästä syystä johtuen sisäiset yhdyskäytäväprotokollat reitittävät liikennettä pelkästään yksittäisten autonomisten järjestelmien sisällä. (Metaswitch 2021a.)

Jokainen OSPF:ää toteuttava reititin jakaa tietoa sen paikallisesta tilasta (käytettävissä olevat verkkoliitännät, saavutettavissa olevat naapurit ja kunkin verkkoliitännän käyttämisen kustannus) muille reitittimille käyttämällä LSA-viestejä (Link State Advertisement). Jokainen reititin käyttää näitä vastaanotettuja viestejä autonomisen järjestelmän topologiaa kuvaavaan identtisen tietokannan rakentamiseen. Tästä tietokannasta jokainen reititin laskee oman reititystaulunsa käyttäen SPF:ää tai Dijikstra algoritmia. Reititystaulu sisältää kaikki määränpäät, niihin liittyvät seuraavan hypyn IP-osoitteet ja lähtevän liikenteen verkkoliitännät, jotka reititysprotokolla on oppinut. (Metaswitch 2021a.)

Protokolla laskee reitit uudelleen verkon topologian muuttuessa, käyttäen Dijkstra algoritmia ja minimoi reititysprotokollan liikenteen, jota se generoi. Protokolla tarjoaa monitasoiseksi hierarkiaksi kutsuttua aluereititystä, jotta topologiasta kertova tieto on piilotettu autonomisen järjestelmän ulkopuolisilta reitittimiltä. Tämä suojaa reititystä ja vähentää reititysprotokollan liikennettä. Protokolla tarjoaa myös tuen usealle saman kustannuksen omaavalle polulle. Kaikki protokollan kanssakäymiset voidaan autentikoida siten, että vain luotetut reitittimet voivat vaihtaa viestejä autonomisen järjestelmän sisällä. (Metaswitch 2021a.)

2.4.13 BGP

Border Gateway Protocol (lyh. BGP) on IP-reititysprotokollaperheeseen kuuluva ulkoinen yhdyskäytäväprotokolla, jota käytetään reititystiedon jakeluun autonomisten järjestelmien välillä. Ulkoiset yhdyskäytäväprotokollat ovat kaikki vektorireititysprotokollia. Vektoriprotokollissa kuten BGP:ssä, reitittimet vaihtavat verkon saavutettavuustietoja lähimpien naapureidensa kanssa. Toisin sanoen reitittimet kertovat toisilleen osoitteet, jotka ne voivat saavuttaa, sekä seuraavan hypyn osoitteen, johon data tulisi lähettää, jotta se saavuttaisi mainitut osoitteet. EGP-reitittimet vaihtavat reittejä toistensa kanssa, kun taas IGP-reitittimet vaihtavat topologian tietoja ja laskevat omat reittinsä paikallisesti. (Metaswitch 2021b.)

EGP floodaa saavutettavuustietoja Internetin läpi, jotta jokainen EGP-reititin omistaisi reititystaulun, joka pitää sisällään osoitteiden etuliitteet ja seuraavat hypyt, jotka kattavat koko julkisen Internetin. EGP:llä on vähän tai ei lainkaan tietoa päästä-päähän -reitistä, se on tietoinen vain reitin varrella sijaitsevasta seuraavasta hypystä. Tästä syystä johtuen polku, jota käytetään datan edelleenohjaukseen on valittu vertailemalla kaikkia mahdollisia seuraavia hyppyjä. (Metaswitch 2021b.)

Vektorireititysprotokollat skaalautuvat paljon paremmin kuin linkkitilareititysprotokollat, koska parhaimman seuraavan hypyn määrittämiseen menevällä ajalla ei ole mitään tekemistä verkon solmujen määrällä, joka tekee niistä erittäin sopivia Internetin liikenteen reitittämiseen. (Metaswitch 2021b.)

Yksittäinen autonominen järjestelmä, joka haluaa vaihtaa reititystietoja toisten autonomisten järjestelmien kanssa, sisältää tyypillisesti yhden tai useamman BGP-reitittimen. Jokainen BGP-reititin konfiguroidaan niiden BGP-reitittimien osoitteilla, joiden kanssa niiden on tarkoitus vaihtaa reititystietoja. (Metaswitch 2021b.)

Kun yhteys toiseen BGP-reitittimeen on muodostettu, BGP-reititin lähettää kaikki sen paikallisessa BGP-reititystaulussa sijaitsevat reitit kyseiselle BGP-reitittimille käyttäen UPDATE-viestejä. Vastaanottava reititin käyttää näitä viestejä uusien reittien lisäämiseen paikalliseen BGP-reititystauluunsa. Jos BGP-reititin oppii useampia reittejä samoihin kohteisiin, se suorittaa päätösprosessin kilpailevien reittien välillä päättääkseen, mikä reiteistä on parhain. Tämän jälkeen paras reitti asennetaan sen paikalliseen BGP-reititystauluun ja sitä mainostetaan muille BGP-reitittimille. (Metaswitch 2021b.)

BGP-reititystaulun reitit yhdistetään muiden reititysprotokollien (esim. OSPF) kautta opittujen reittien kanssa ja yhdessä nämä muodostavat reitittimen kokonaisen reititystaulun. Tämä reititystaulu sisältää kaikki määränpäät, niihin liittyvät seuraavat hypyt sekä lähtevän liikenteen verkkoliitännät, joista reititin on tietoinen. BGP mahdollistaa reittien muuttamisen ennen kun ne lähetettään vertaisille, käyttämällä implementaatiokohtaisia käytäntöjä. BGP käyttää ajastimia estääkseen nopeasti muuttuvan reitin jatkuvan mainostamisen Internetin läpi. Myös BGP:n kanssakäymiset voidaan autentikoida siten, että vain luotetut reitittimet voivat toteuttaa viestien vaihtoa. (Metaswitch 2021b.)

2.4.14 Layer 3 kytkin

Layer 3 kytkin on verkkokerroksella toimiva laite, joka yhdistää kytkimen ja reitittimen toiminnallisuuksia. Layer 3 kytkimet suunniteltiin alun perin parantamaan reitityksen suorituskykyä suurissa verkoissa. Se kytkee verkon laitteita keskenään ja kykenee IP-reititykseen, mahdollistaen sen toiminnan reitittimenä. Se tukee reititysprotokollia, tutkii saapuvia paketteja ja tekee reitityspäätöksiä käyttäen kohde ja lähdeosoitteita. (Hackernoon 2021.)

Layer 3 kytkimen tarkoitus on tuoda seuraavia hyötyjä:

- VLAN:ien välinen reititys
- parempi vianeristys
- yleislähetysliikenteen määrän vähentäminen
- VLAN:ien konfiguraatioprosessin helpottaminen, sillä VLAN:ien väliin ei tarvita erillistä reititintä
- erilliset reititystaulut, jonka seurauksena paremmin eriytetty liikenne
- vianetsinnän yksinkertaistaminen
- pienempi viive, sillä datan ei tarvitse tehdä ylimääräisiä hyppyjä reitittimelle

(Hackernoon 2021.)

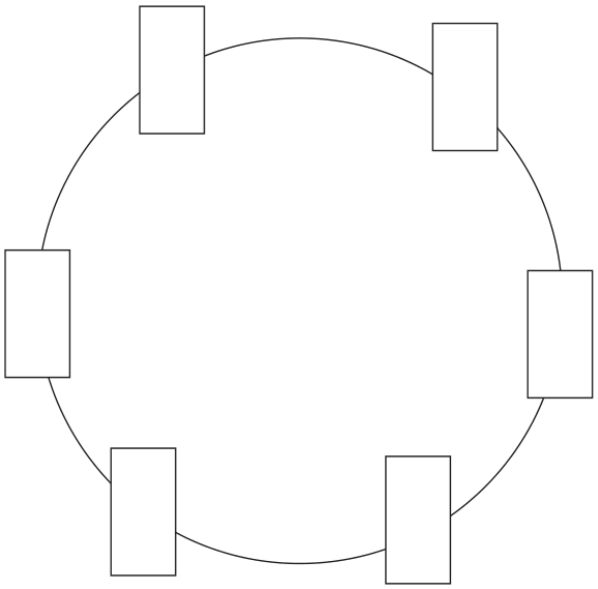
3 TOPOLOGIAT JA SUUNNITTELU

3.1 Verkkotopologiat

Verkkotopologialla tarkoitetaan tietokoneiden ja verkkolaitteiden fyysistä asettelua ja organisointia. Verkkotopologia kuvaa kuinka kaapelointi on fyysisesti toteutettu. Fyysisistä asetelmaa kuvaavia perustopologioita on olemassa neljä; rengas, väylä, tähti ja mesh. (Chapple, Stewart & Gibson 2018, 500.)

3.1.1 Rengastopologia

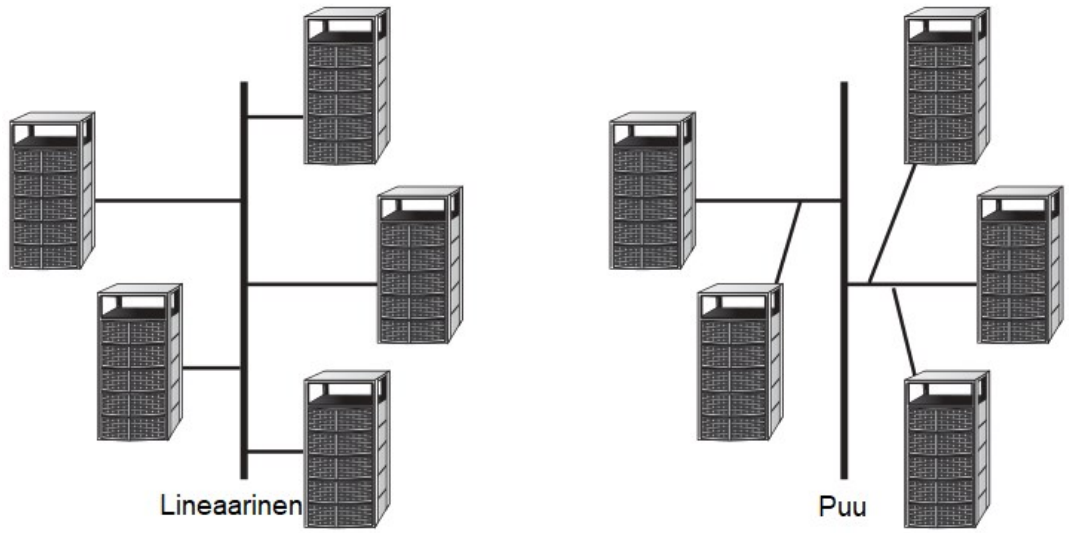
Rengastopologia yhdistää verkon jokaisen solmun kuvion 5 mukaiseksi renkaaksi. Seuraamalla kaapelia solmusta solmuun päädyt siihen solmuun josta aloitit. Vain yksi solmu voi lähettää dataa kerrallaan. Liikenteen hallinta on toteutettu käyttämällä tokenia. Tokenia voitaisiin pitää digitaalisena lupapassina, joka kiertää rengasta kunnes jokin solmuista nappaa sen. Solmu, joka pitää hallussaan tokenia pystyy lähettämään dataa. Data ja token lähetetään tiettyyn päämäärään. Datan matkustaessa silmukan sisällä jokainen solmu tarkistaa kohdallaan, onko se datan vastaanottaja. Mikäli solmu on vastaanottaja, se lukee datan ja mikäli solmu ei ole vastaanottaja, se antaa tokenin eteenpäin. Kun data on vastaanotettu, token vapautetaan ja palautetaan takaisin kiertämään silmukkaa kunnes jokin toinen solmu nappaa sen. Jos mikä tahansa segmentti silmukan sisällä hajoaa, kaikki kommunikaatio sen sisällä lakkaa. Jotkin rengastopologian implementaatiot käyttävät vikasietoisuusmekanismeja, kuten vastakkaisiin suuntiin pyöriviä kaksoissilmukoita estääkseen yksittäisten kohtien vikaantumisen. (Chapple ym. 2018, 500-501.)



Kuvio 5. Rengastopologia (mukaillen Chapple ym. 2018, 501.)

3.1.2 Väylätopologia

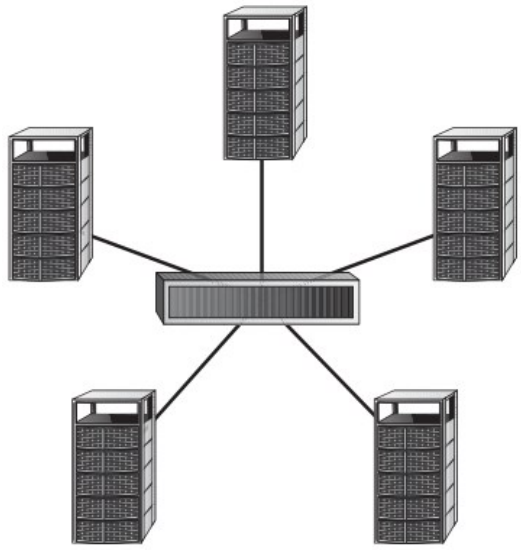
Väylätopologiassa verkon solmut on yhdistetty jonoksi, jossa kaikki väylän solmut voivat lähettää dataa samanaikaisesti. Jos kaapeli hajoaa missä tahansa kohtaa väylässä, koko väylä menee alas. Kuviosta 6 nähdään, että väylätopologioita on olemassa kahta eri tyyppiä; lineaarinen ja puu. Lineaarisessa väylätopologiassa solmut on yhdistetty suoraan runkokaapeliin. Puumallisessa väylätopologiassa runkokaapelilla on oksia, jotka tukevat useampia solmuja. Väylä joudutaan terminoimaan sen kummassakin päässä ja yhteyden katkaisut voivat kaataa koko verkon. Näistä syistä johtuen väylän käyttö nykypäivänä on harvinaista. (Conrad, Misenar & Feldman 2015, 250; Chapple ym. 2018, 501-502.)



Kuvio 6. Väylätopologia (mukaillen Chapple ym. 2018, 502.)

3.1.3 Tähtitopologia

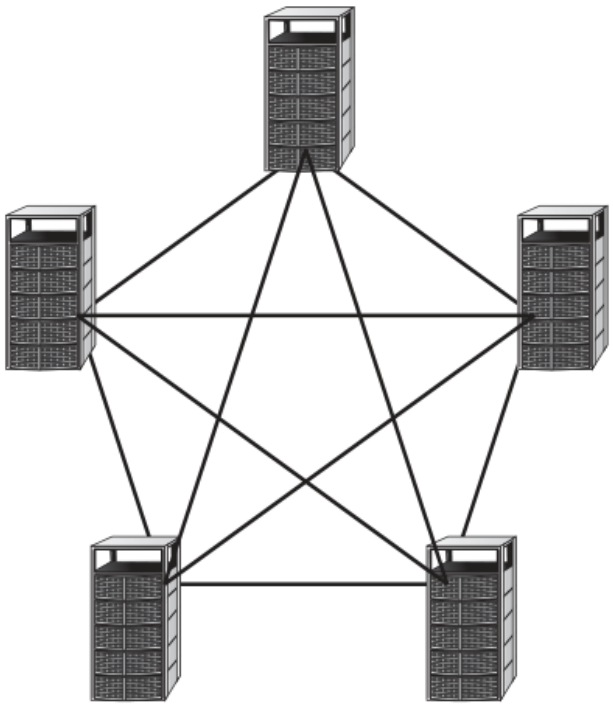
Tähtitopologiassa solmut on kytketty keskitettyyn yhteyslaitteeseen kuten kytkimeen. Jokainen solmu on kytketty kytkimeen siihen dedikoidulla segmentillä. Mikäli jokin segmenteistä vikaantuu, voivat muut segmentit yhä jatkaa toimintaansa normaalisti. Tähtitopologiassa ainoana koko verkon vikaantumiseen johtavana pisteenä on kytkin. Yleensä tähtitopologiassa kaapelointia on vähemmän kuin muissa topologioissa ja vahingoittuneiden kaapeleiden tunnistaminen on helpompaa. (Conrad ym. 2015, 252-253; Chapple ym. 2018, 502.)



Kuvio 7. Tähtitopologia (mukaillen Chapple ym. 2018, 502.)

3.1.4 Mesh-topologia

Mesh-topologiassa solmut on yhdistetty toisiin solmuihin käyttäen useita polkuja. Täys-mesh-topologiassa verkon kaikki solmut on yhdistetty keskenään. Osittaisessa mesh-topologiassa jokaisella solmulla on useita yhteyksiä meshiin, mutta kaikilla solmuilla ei ole yhteyksiä keskenään. Mesh-topologiat tarjoavat korkeaa saatavuutta ja kahdennettuja yhteyksiä. Mesh-topologia sallii useamman solmun vikaantumisen ilman, että se vaikuttaa kriittisesti verkon toimintaan. (Conrad ym. 2015, 253; Chapple ym. 2018, 503.)



Kuvio 8. Mesh-topologia (mukaillen Chapple ym. 2018, 503.)

3.2 Ciscon hierarkinen suunnittelumalli

Verkkojen täytyy kyetä vastaamaan organisaatioiden tarpeita ja tukemaan uusia nousevia teknologioita. Verkon suunnittelun periaatteet ja mallit auttavat verkon ylläpitäjää suunnittelemaan verkon, joka on joustava, kestävä ja helposti hallittavissa. Ciscon hierarkinen suunnittelumalli on alan laajuisesti hyväksytty malli luotettavien, skaalautuvien ja kustannustehokkaiden verkkojen suunnitteluun. (Cisco Networking Academy 2014, 2.)

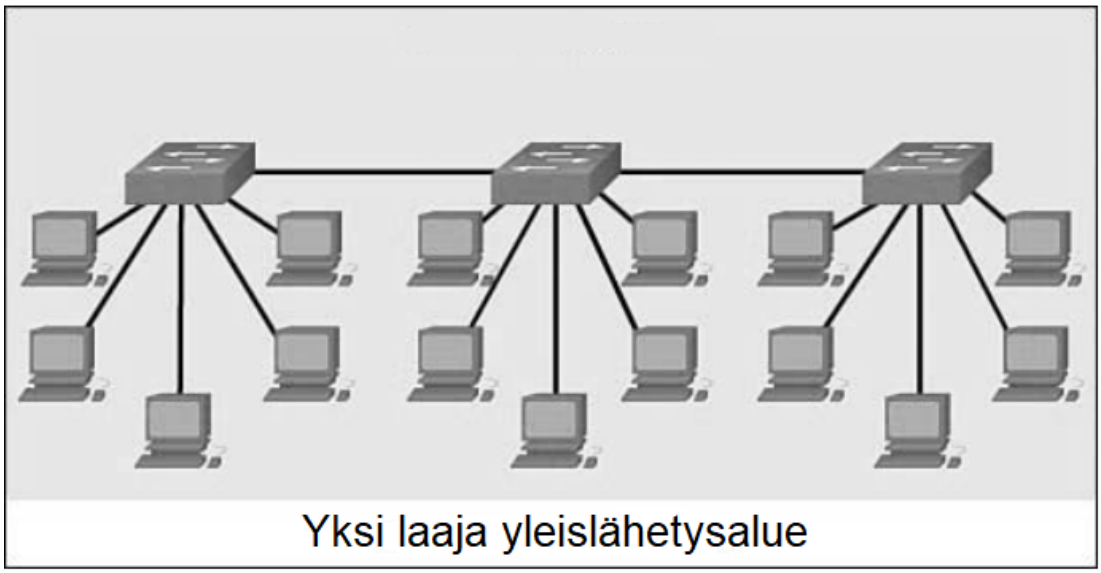
Verkkosuunnittelu vaihtelee, riippuen organisaation koosta ja vaatimuksista. Suuren, paljon laitteita ja yhteyksiä omaavan organisaation tarpeet ovat huomattavasti monimutkaisempia kuin vähän laitteita omaavan pienen organisaation. Koosta ja vaatimuksista huolimatta tärkeimpänä tekijänä onnistuneen verkkosuunnittelun käyttöönoton kannalta, on noudattaa hyviä suunnitteluperiaatteita. Näitä periaatteita ovat:

- hierarkia. Hierarkisen verkon malli on hyödyllinen korkean tason työkalu luotettavan verkkoinfrastruktuurin suunnitteluun. Se rikkoo suunnittelun monimutkaiset alueet pienemmiksi ja hallittavimmiksi kokonaisuuksiksi
- modulaarisuus. Erottelemalla verkossa toimivat eri toiminnot moduuleiksi, tulee verkon suunnittelusta helpompaa
- kestävyys. Verkon täytyy olla käytettävissä normaaleissa ja epänormaaleissa olosuhteissa. Normaalit olosuhteet sisältävät normaaleja tai odotettuja liikennemääriä ja etukäteen sovittuja tapahtumia kuten huoltokatkoja. Epänormaalit olosuhteet sisältävät ohjelmisto- ja laitevikoja, äärimmäisiä liikennekuormia, palvelunestohyökkäyksiä ja muita suunnittelemattomia tapahtumia.
- joustavuus. Kyky muokata verkon osia, lisätä palveluita ja kapasiteettia ilman suurempia laitteiston korvauksia

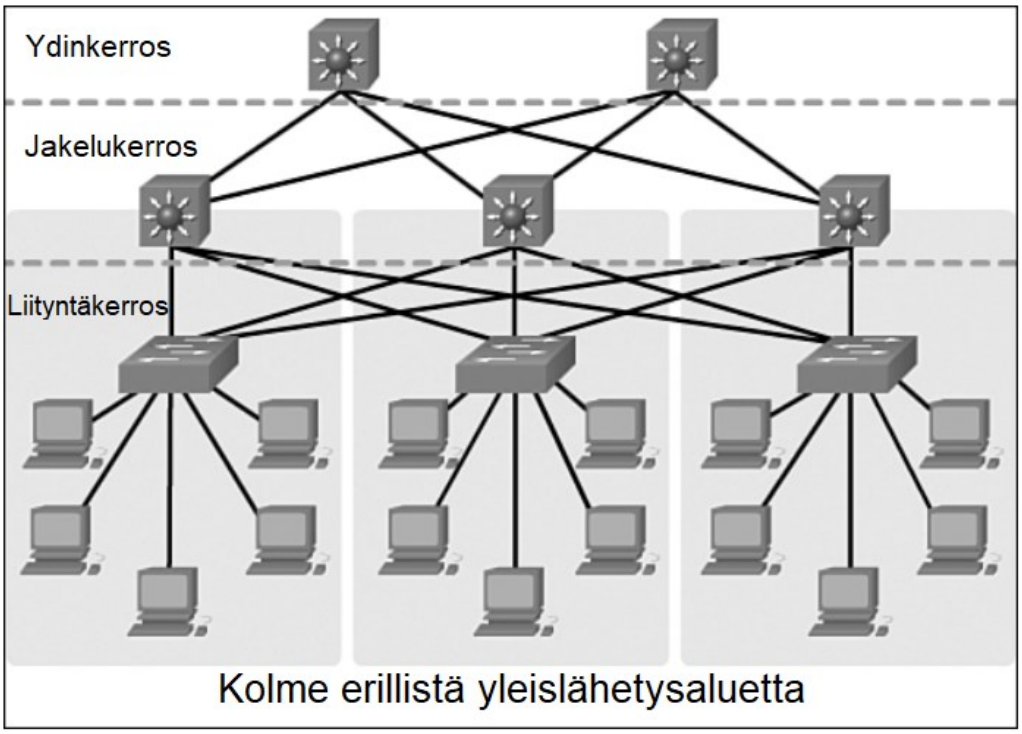
(Cisco Networking Academy 2014, 3-4.)

Ennen verkot otettiin käyttöön käyttäen kuviossa 9 esiteltyä ns. litteää (eng.flat) suunnittelumallia. Suunnittelumallissa kytkimiä lisättiin laitemäärän kasvaessa. Litteä suunnittelumalli tarjosi erittäin vähän vaihtoehtoja yleislähetyksien hallintaan ja eitoivotun liikenteen suodattamiseen. Laitteiden ja sovellusten määrän kasvaessa vas-

teajat kasvoivat, tehden verkosta käyttämättömän. Syntyi tarve paremmalle verkko-suunnittelun lähestymistavalle ja tästä syystä organisaatiot käyttävät nykyään kuviossa 10 esiteltyä hierarkista suunnittelumallia. (Cisco Networking Academy 2014, 4.)



Kuvio 9. Litteä suunnittelumalli (mukaillen Cisco Networking Academy 2014, 5.)



Kuvio 10. Hierarkinen suunnittelumalli (mukaillen Cisco Networking Academy 2014, 5.)

Hierarkisessa suunnittelumallissa verkko on jaettu erillisiin kerroksiin. Jokainen hierarkian kerros tuo jotain tiettyä toiminnallisuutta, joka määrittää sen roolin koko veron sisällä. Tämä auttaa verkonsuunnittelijoita ja arkkitehtejä optimoinnissa, oikeiden laitteiden, ohjelmistojen ja ominaisuuksien valitsemisessa, jotta kerros suoriutuisi sille määritellyissä rooleissa. Hierarkista mallia voidaan käyttää lähiverkkototeutuksissa ja laajaverkkototeutuksissa. (Cisco Networking Academy 2014, 5.)

Jakamalla litteä verkko pienempiin hallittavimpiin lohkoihin paikallinen liikenne pysyy paikallisena. Vain muihin verkkoihin matkalla oleva liikenne siirretään ylemmälle kerrokselle. Kuviosta 6 näemme, että verkko on jaettu kolmeen erilliseen yleislähetysalueeseen. (Cisco Networking Academy 2014, 5.)

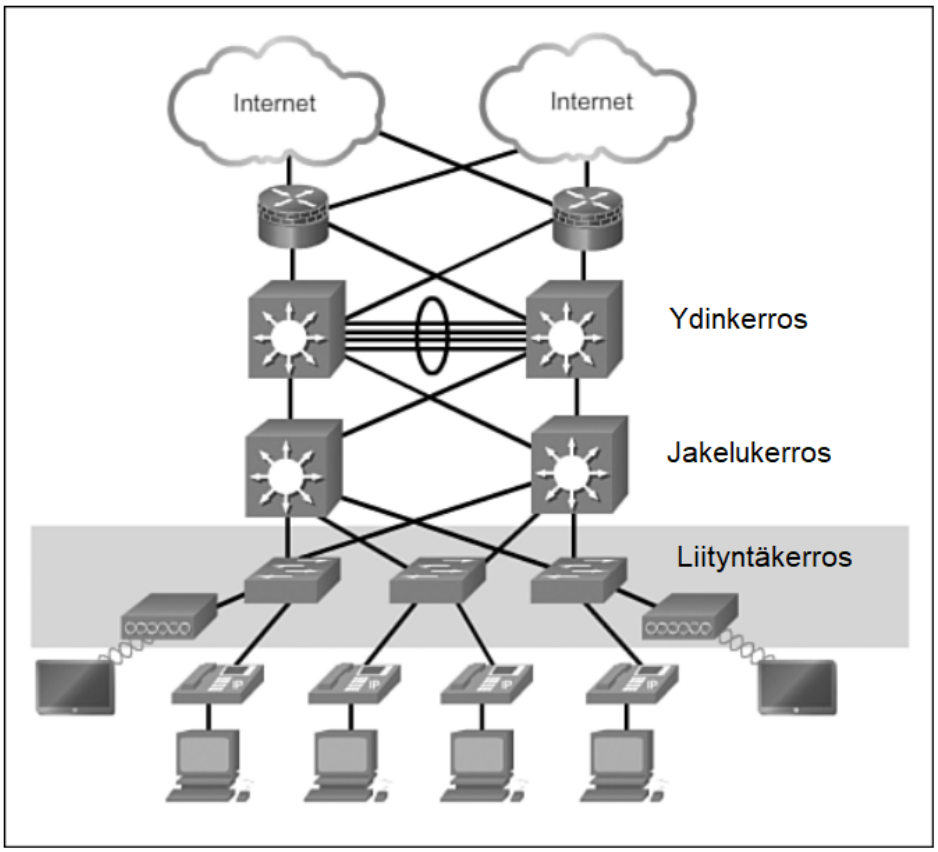
Tyypillinen hierarkinen suunnittelumalli sisältää seuraavat kolme kerrosta:

- liityntäkerros (eng. access)
- jakelukerros (eng. distribution)
- ydinkerros (eng. core)

(Cisco Networking Academy 2014, 6.)

3.2.1 Liityntäkerros

Lähiverkkoympäristössä liityntäkerros tarjoaa laitteille pääsyn verkkoon. Laajaverkkoympäristöissä se tarjoaa etätyöntekijöille ja verkkopaikoille (eng. site) pääsyn yrityksen verkkoon laajaverkkoyhteyksien läpi. Kuten kuviosta 11 nähdään, pienen yritysverkon liityntäkerros sisältää yleensä layer 2 kytkimiä ja tukiasemia, jotka tarjoavat yhteydet työasemien ja palvelimien välille. (Cisco Networking Academy 2014, 6-7.)



Kuvio 11. Liityntäkerros (mukaillen Cisco Networking Academy 2014, 7.)

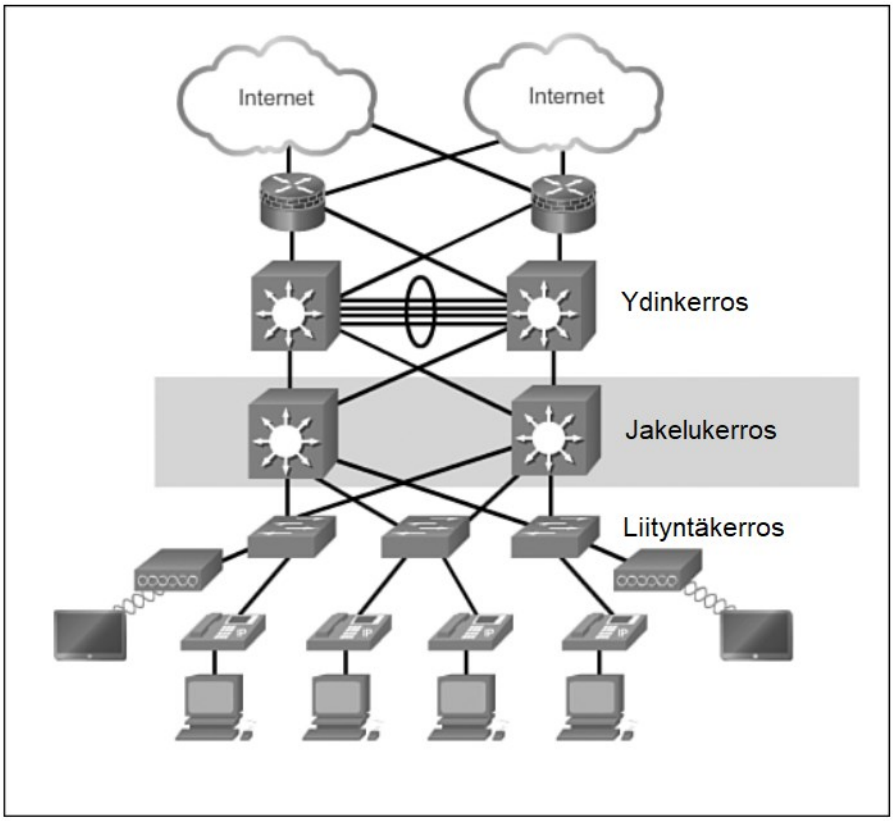
Liityntäkerros tarjoaa muun muassa seuraavia toimintoja:

- layer 2 kytkentä
- korkea saatavuus
- porttien suojaus
- QoS luokittelu ja merkintä
- ARP inspection
- virtuaaliset pääsylistat
- spanning tree
- power over ethernet (lyh. PoE) ja VLAN:it IP-puhetta (eng. Voice over Internet Protocol eng. VoIP) varten

(Cisco Networking Academy 2014, 7.)

3.2.2 Jakelukerros

Jakelukerros yhdistää liityntäkerroksen kytkimiltä saadun datan ennen kuin se lähetetään ydinkerrokselle. Lisäksi se luo vioilta eristävän rajan, joka tarjoaa loogista eristystä liityntäkerrokselta lähtöisin olevilta virheiltä. Jakelukerroksen laitteet ovat tyypillisesti layer 3 kytkimiä. Kuviossa 12 jakelukerros toimii rajana layer 2 toimialueiden ja layer 3 reititettyjen verkkojen välissä. (Cisco Networking Academy 2014, 7-8.)



Kuvio 12. Jakelukerros (mukaillen Cisco Networking Academy 2014, 8.)

Jakelukerroksella toimiva kykenee tarjoamaan seuraavia palveluita:

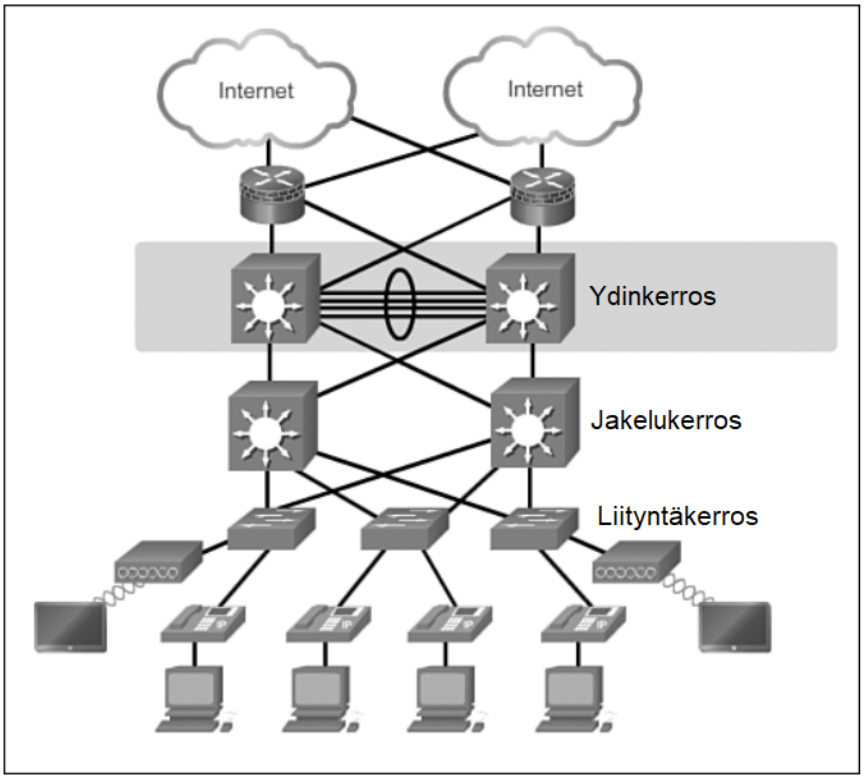
- LAN ja WAN linkkien yhdistäminen
- käytäntöperusteista tietoturvaa pääsylistojen (ACL) ja suodattamisen muodossa
- reitityspalveluita LAN:ien ja VLAN:ien välillä sekä reititystoimialueiden välillä (esim. OSPF)
- varmennus ja kuormantasaus

- yleislähetysalueen hallinta

(Cisco Networking Academy 2014, 8.)

3.2.3 Ydinkerros

Tyypillisessä hierarkisessa mallissa yksittäiset kerrokset on kytketty toisiinsa käyttäen ydinkerrosta. Ydinkerros toimii verkon selkärankana ja kuviosta 13 näemme, että sen rooli on kriittinen jakelukerroksen laitteiden yhteenliittämisessä. (Cisco Networking Academy 2014,9.)



Kuvio 13. Ydinkerros (mukaillen Cisco Networking Academy 2014, 9.)

Ydinkerroksen tulisi omata korkea saatavuus ja olla varmennettu, sillä kaikki muut kerrokset ovat riippuvaisia sen tarjoamista yhteyksistä. Ydinkerros yhdistää kaiken jakelukerroksen laitteilta saapuvan liikenteen, joten sen täytyy kyetä edelleenlähettämään suuria määriä dataa nopeasti. Ydinkerroksen tulisi:

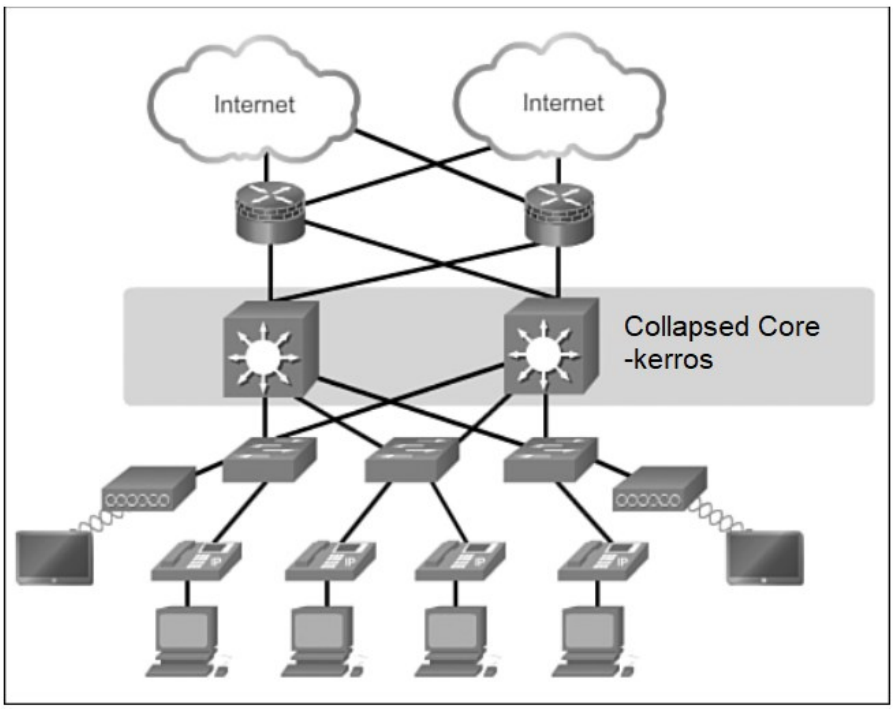
- tarjota nopeaa kytkentää
- tarjota luotettavuutta ja vikasietoisuutta

- skaalautua suosimalla nopeampia laitteita laitteiden määrän sijaan
- välttää tietoturvasta, tarkastuksista ja muista prosesseista aiheutuvaa prosessori-intensiivistä pakettien käsittelyä

(Cisco Networking Academy 2014, 9.)

3.2.4 Collapsed core

Kolmekerroksinen hierarkinen suunnittelumalli maksimoi suorituskyvyn, verkon saatavuuden ja verkon suunnittelun skaalautuvuuden. Kuitenkaan monien pienten yritysten verkot eivät kasva merkittävästi suuremmiksi ajan kuluessa. Tästä syystä kaksikerroksinen hierarkinen malli, jossa ydinkerros ja jakelukerros ovat supistettu yhdeksi kerrokseksi, on usein käytännöllisempi. Tätä kerrosta kutsutaan collapsed coreksi. Collapsed coresssa jakelukerroksen ja ydinkerroksen toimintoja toteuttaa yksi laite. Pääsyy collapsed coren käyttöönotolle on kustannusten laskeminen säilyttäen samalla kolmikerroksisen hierarkisen mallin edut. Kuviossa 14 jakelukerros ja ydinkerros ovat supistettu yhdeksi kerrokseksi, joiden toiminnallisuudesta vastaavat monikerroksiset kytkimet. (Cisco Networking Academy 2014, 10.)



Kuvio 14. Collapsed core (mukaillen Cisco Networking Academy 2014, 10.)

4 VERKONHALLINTA

Tietoverkkoa voidaan pitää modernien organisaatioiden liiketoiminnan elinehtona, sillä sen tarjoama infrastruktuuri mahdollistaa esim. yrityksen liiketoiminnan kannalta tärkeän viestinnän ja tilaukset. Se lisää myös työntekijöiden tapoja tehdä yhteistyötä ja olla tuottavampia. Verkon häiriöt ja katkokset voivat johtaa huomattaviin tappioihin liikevaihdon ja tuottavuuden suhteen. Tästä syistä johtuen on tärkeä pitää huoli siitä, että verkko ja sen tarjoamat palvelut ovat saavutettavissa vuorokauden jokaisena hetkenä. (Singh 2017, luku 10.)

Verkko on dynaaminen kokonaisuus ja se muuttuu aina, porttien tilojen muuttuessa, uusien palveluiden käyttöönotossa ja käytöstä poistaessa, sekä laitteiden tai linkkien vikaantuessa. On tärkeää hallita näitä muutoksia ja varmistaa, että palvelut ovat saatavilla ja, että verkossa ilmenevät ongelmat hoidetaan tehokkaasti. Verkkojen kanssa toimiessa on tärkeää omata järjestelmällinen lähestymistapa, sillä verkon ongelmat voivat olla monimutkaisia, joten niiden rikkominen osatekijöihin ja ratkaiseminen erikseen helpottaa prosessia. (Singh 2017, luku 10.)

4.1 Verkonhallinnan kehykset

Eri organisaatiot ja standardointielimet ovat kehittäneet useita eri lähestymistapoja verkonhallintaan, jotka kaikki keskittyvät eri aspekteihin. Jokainen lähestymistapa johtaa verkon operoinnin ja ylläpidon kannalta hyviin käytäntöihin, joita seuraamalla saadaan tarjottua parempia palveluita. Jokainen lähestymistapa on lähestynyt palveluiden tarjoamista eri soveltamisalojen näkökulmasta, jotka vaihtelevat strategiasta ja muutosten toteuttamisesta itse käyttöönoton ja operoinnin mikromanagerointiin. (Singh 2017, luku 10.)

Yksi aikaisimmista malleista verkonhallintaan on FCAPS-malli, joka on osa ITU-T:n (International Telecommunication Union Telecommunication Standardization Sector) määrittelemää Telecommuncations Management Network -arkkitehtuuria (lyh. TMN). Se jakaa verkon hallinnan viiteen alueeseen; viat (eng. fault), konfiguraatio (eng. con-

figuration), kirjanpito (eng. accounting), suorituskyky (eng. performance) ja turvallisuus (eng. security). FCAPS on lyhenne näistä viidestä alueesta, jotka on määritetty ITU:n M.3400 määritelmässä. Näiden alueiden toiminnot ovat kuvaukseltaan seuraavat:

- vian hallinta. Havaitse, eriytä, ilmoita ja korjaa verkossa ilmenevät viat.
- konfiguraation hallinta. Seuraa hallittavien laitteiden konfiguraatio dataa (esim. konfiguraatio tiedostot, ohjelmistoversiot ja itse laitteet) ja niihin kohdistuvia muutoksia.
- kirjanpidon hallinta. Kerää käyttödataa verkon resursseista kuten kaistanleveydestä linkeissä tai porteissa.
- suorituskyvyn hallinta. Monitoroi ja mittaa palvelutasosopimuksessa (eng. Service Level Agreement, lyh. SLA) määriteltyjä parametreja kuten viivettä, viivevaihtelua, pakettihävikkiä sekä laitteiden muistin- ja prosessorin käyttöä
- turvallisuuden hallinta. Tarjoa suojattu pääsy verkon laitteisiin, resursseihin ja palveluihin niihin valtuutetuille henkilöille

(Sathyan 2010, 33-44; Singh 2017, luku 10.)

Toinen standardi on Information Technology Infrastructure Library (lyh. ITIL), joka on joukko Ison Britannian hallituksen kehittämiä parhaita käytäntöjä. ITIL:in tarkoitus on parantaa tapoja joilla IT toimittaa ja tukee liiketoiminnan palveluita ja se tarjoaa ohjeita teknologian ja prosessien hallintaan ja keskittyy parantamaan henkilöstön, prosessien ja teknologian ominaisuuksia. ITIL V3 määrittelee monia prosesseja ja toimintoja, jotka jakaantuvat seuraavalle viidelle tasolle:

- ITIL Palvelustrategia, joka keskittyy ymmärtämään organisaation tavoitteita ja asiakkaan tarpeita.
- ITIL Palvelusuunnittelu, joka keskittyy kartoittamaan liiketoiminnan tavoitteiden palvelustrategiaa
- ITIL Palvelutransitio, joka keskittyy kehittämään ja parantamaan valmiuksia uusien IT infrastruktuurin palveluiden käyttöönotossa
- ITIL Palvelutuotanto, joka keskittyy palveluiden hallintaan
- ITIL Jatkuva palvelun parantaminen, joka keskittyy operaatioiden ja prosessien virtaviivaistamiseen ja jatkuvaan parantamiseen

(Singh 2017, luku 10.)

Vaikka toisiaan täydentäviä malleja ja ohjeita on olemassa useita erilaisia, ei kaiken kattavaa lähestymistapaa verkon hallintaan ole olemassa, eikä sellaista voi olla edes olemassa, sillä jokainen verkko on suunnittelun, palveluiden ja niiden tavoitteiden suhteen ainutlaatuinen. Nämä ohjeet tarjoavat kuteinkin viitekehyksen yrityskohtaisten spesifien prosessien ja käytäntöjen luomiseen. (Singh 2017, luku 10.)

4.2 Verkonhallinnan tukipilarit

Pohjimmiltaan verkonhallinta keskittyy takaamaan, että palvelut toimitetaan verkon käyttäjille sovitun SLA:n mukaisesti ja tekemään ennakoivia toimenpiteitä SLA:n rikkomisen välttämiseksi tai reagoivia toimenpiteitä palveluiden palauttamiseksi, mikäli niissä havaitaan häiriöitä tai hajoamista. On hyvä pitää mielessä, että SLA:t ovat tyypillisesti epävirallisia organisaation sisällä ja sopimusperusteisia ulkoisille käyttäjille. Tarkastellaan seuraavaksi hieman kolmea tukipilaria, jotka luovat perustan tehokkaalle verkonhallinnalle ja mahdollistavat SLA:n täyttymisen. (Singh 2017, luku 10.)

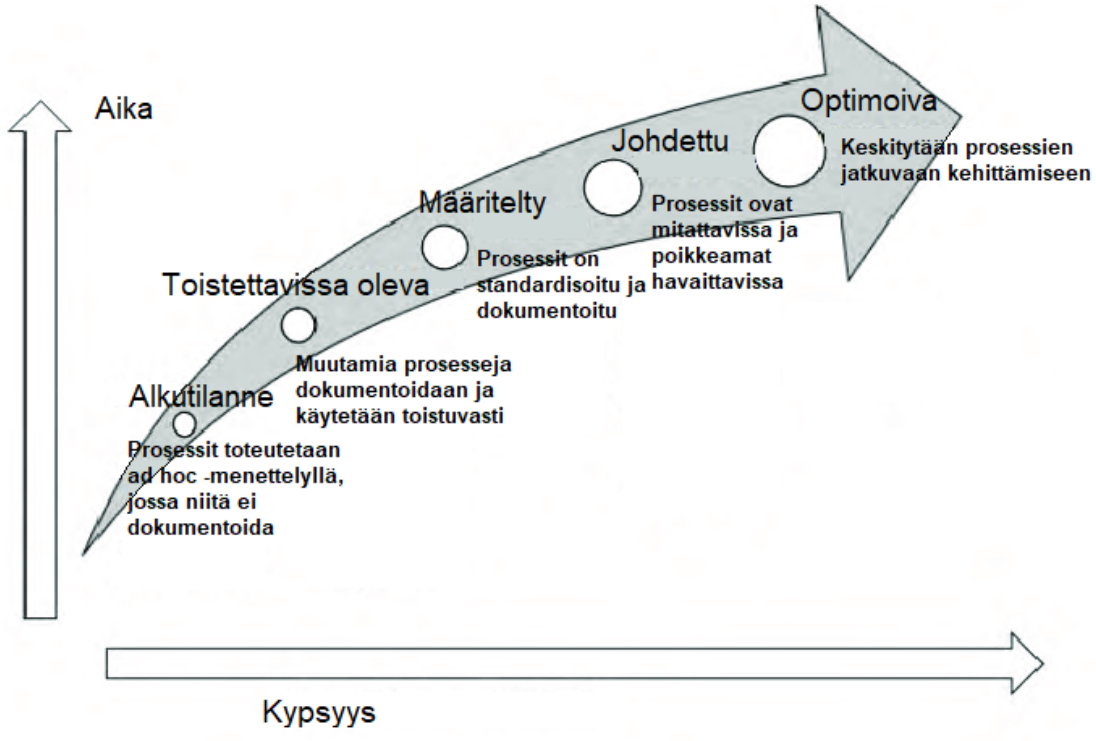
4.2.1 Henkilöstö

Henkilöstö on yksi verkonhallinnan perustavista tukipilareista. Henkilöstön taito määrittää kuinka tehokkaasti he kykenevät käyttämään organisaatiossa saatavilla olevaa teknologiaa ja työkaluja verkonhallintaan ja operointiin. On tärkeää palkata oikeat taidot omaavaa henkilöstöä työskentelemään verkonhallinnan eri tasoilla. Olisi erittäin epätehokasta palkata kaikki työskentelemään samalla tasolla, sillä tehokas verkonhallinta tarvitsee hyvin määritellyn hierarkian. Tehokas verkkotiimi koostuu erilaisista tason 1 ja 2 resursseista, jotka omaavat yleisiä taitoja verkonhallinnassa, monitoroinnissa ja vianetsinnässä. Tason 3 resurssit ovat erikoistuneet tiettyihin palveluihin tai teknologioihin ja hoitavat korkeamman tason vianetsintää vaativia toimenpiteitä. Organisaation verkkotiimiä ovat myös tukemassa erilaisten laite- ja ohjelmistotoimittajien tukitiimit, joiden palveluita organisaatio on tilannut. (Singh 2017, luku 10.)

4.2.2 Prosessit

Taitavat verkkotiimin resurssit tekevät verkon operoinnista tehokasta. Jokainen henkilö on kuitenkin erilainen, omistaa erilaiset taidot ja luonteen. Tästä syystä jokainen henkilö toimii eri tavalla saman tilanteen edessä. Henkilö saattaa kuitenkin kyetä ratkaisemaan verkon ongelman, mutta jokaisella henkilöllä on oma lähestymistapa. Tämä voi johtaa ongelmiin vuorotyötä tekevissä verkkotiimeissä, joissa ongelmat luovutetaan seuraavalle vuorolle. Tämä voi aiheuttaa ongelmia myös verkkodokumentaatiossa, sillä henkilöstö saattaa toteuttaa saman vian korjaavia vaiheita useilla eri tavoilla. Ennalta määritelty prosessi verkon operointiin varmistaa, että henkilöstö seuraa samoja hyväksi todettuja optimoituja vaiheita verkon vian korjaamiseksi. (Singh 2017, luku 10.)

Prosessit voivat olla virallisia tai epävirallisia ja niistä tulee kypsempiä organisaation kehittyessä. Kuviossa 15 esitetty CMM-malli (Capability Maturity Model) kuvaa seuraavat prosessien kypsyyttä esittävät viisi tasoa. Organisaatioiden tulisi pyrkiä nousemaan korkeammalle tasolle ajan kuluessa tehokkuuden lisäämiseksi. (Singh 2017, luku 10.)



Kuvio 15. CMM-malli (mukaillen Hassan 2019.)

4.2.3 Työkalut

Jotta saadaan tarjottua oikeanlaisia syötetietoja olennaisille tiimeille, tarvitaan työkaluja. Työkaluja tarvitaan oikeanlaisten syötetietojen toimittamiseen olennaisille tiimeille. Nämä syötetiedot voivat olla erittäin hyödyllisiä verkon vikojen eristämisessä, verkon palauttamisessa tai ne voidaan jopa antaa suunnittelusta vastaavan tiimin käyttöön erilaisten palvelujen parantamiseksi. Työkalut automatisoivat paljon verkkotiimin suorittamia tehtäviä, jonka ansiosta voidaan keskittyä monimutkaisempiin korkeamman tason tehtävien muodostamiseen. Kun nämä tehtävät on saatu muodostettua, voidaan nekin automatisoida käyttäen uusia työkaluja seuraten jatkuvan kehityksen sykliä. (Singh 2017, luku 10.)

Tehokkaassa verkonhallinta ympäristössä käytetään työkaluja, jotka vastaavat autonomisista hälytyssanomista ja raporteista, jonka lisäksi ne on integroitu vaihtamaan dataa muiden työkalujen kanssa. On olemassa paljon työkaluja, joita hyödynnetään verkon monitoroimiseen käyttäen SNMP:tä (Simple Network Management Protocol). SNMP:llä voidaan pollata verkon laitteita, saada tietoa verkon parametreista, tehdä trendianalyysiä ja sitä voidaan käyttää apuna muita tiimejä avustavien raporttien laatimisessa. (Singh 2017, luku 10.)

4.3 SNMP

Tärkeä aspekti verkon operoinnissa on tunnistaa verkon tapahtumia ja tarjota raportointitapoja, jotka auttavat ennakoivassa ongelmien ja juurisyiden analysoimisessa. Tämä vaati sen, että verkon laitteista kerätään jatkuvasti spesifistä tietoa porttien tiloista, liikenteen kuormituksesta tai esimerkiksi prosessorin käytöstä. SNMP on protokolla, joka tarjoaa viestiformaatin saadakseen tätä tietoa laitteilta. (Singh 2017, luku 10.)

SNMP on sovelluskerroksella toimiva protokolla, joka tarjoaa viestiformaatin SNMP managereiden ja agenttien välisen kommunikaation mahdollistamiseksi. SNMP tarjoaa standardisoidun kehyksen ja yhteisen kielen verkon laitteiden hallintaan ja monitorointiin. SNMP:n kehys koostuu seuraavista komponenteista; SNMP manager, SNMP agent ja MIB (Management Information Base). (Singh 2017, luku 10.)

4.3.1 SNMP Manager

SNMP manager on tietokone, joka on konfiguroitu pollaamaan SNMP agentilta tietoja. Tämä hallintaan keskittynyt komponentti on ydintoiminnoiltaan yksinkertainen, sillä se keskittyy pääsääntöisesti datan pyytämiseen. Managerina voi toimia mikä tahansa laite, joka kykenee lähettämään pyyntöjä SNMP agenteille käyttämällä oikeita pääsytietoja. Joissain tapauksissa SNMP manager otetaan käyttöön osana monitorointipakettia, jota kutsutaan verkonhallintajärjestelmäksi, kun taas toisinaan ylläpitäjä käyttää tähän yksinkertaista apuohjelmaa. Melkein kaikki SNMP-protokollan komennot on suunniteltu managerin lähetettäväksi, mutta se on suunniteltu myös vastaamaan trap ja response -viesteihin. (Ellingwood 2014; Huawei 2020.)

4.3.2 SNMP Agent

SNMP agent on hallittavan laitteen sisällä sijaitseva ohjelmistokomponentti, joka kerää tietoa hallittavasta laitteesta ja säilöö sen kyseltävään muotoon tietokantaan, jota kutsutaan MIB:ksi (Management Information Base). MIB on hierarkinen etukäteen määritelty struktuuri, joka säilöö tietoa, jota voidaan kysellä tai asettaa. Tämä tieto on saatavilla SNMP pyynnöille, jotka ovat peräisin oikeat pääsytiedot omaavalta SNMP managerilta. Agentti laite konfiguroi, millä managereilla on pääsy sen tietoihin. Se voi toimia myös välikätenä laitteiden kanssa, joita ei ole konfiguroitu SNMP liikenteen välittämiseen. SNMP agentit vastaavat suurimpaan osaan protokollassa määritellyistä komennoista, mutta tämän lisäksi agentti on suunniteltu lähettämään trap viestejä. (Ellingwood 2014; Huawei 2020.)

4.3.3 MIB

MIB on tietokanta, joka seuraa globaalisti määriteltyjä standardeja, joita manager ja agentit noudattavat. Se on rakenteeltaan hierarkinen, mutta sallii laitevalmistaja kohtaisia lisäyksiä. MIB:n rakenne voitaisiin nähdä hierarkisena puuna. Jokainen haarautuva oksa on merkitty tunnistenumerolla ja tunnistemerkkijonolla, jotka ovat uniikkeja

kyseisellä hierarkian tasolla. Kun halutaan viitata johonkin puun lehteen, tarvitsee ensin jäljittää polku puun juuresta kyseiselle lehdelle. Lehdelle johtavat tunnistenumerot ja merkkijonot sidotaan yhteen ja ne muodostavat osoitteen. Jokainen hierarkian liityntäkohta on esitetty piste-notaatiolla, joten lopullinen osoite tulee olemaan joukko numeroita tai merkkijonoja, jotka on erotettu toisistaan pisteillä. Tätä lopullista lehdelle johtavaa osoitetta kutsutaan OID:ksi (Obejct Identifier). Laitevalmistajat jotka upottavat laitteisiinsa SNMP agentteja käyttävät joskus omia mukautettuja oksiaan omilla kentillään ja tietopisteillään. Tästä huolimatta jokaisella laitteella on käytössä standardisoituja selvästi määriteltyjä MIB-oksia. (Ellingwood 2014; Huawei 2020.)

4.3.4 SNMP:n komennot

Yksi syistä miksi SNMP on niin laajasti käytetty, on sen saatavilla olevien komentojen yksinkertaisuus. Käyttöönotettavia ja muistettavia operaatioita on vähän, mutta ne ovat tarpeeksi joustavia täyttääkseen protokollan hyödyllisyysvaatimukset. Seuraavassa listassa on käyty läpi kaikki SNMP:n komennot ja niiden toiminnot:

- Get-viesti on managerin agentille lähettämä viesti, jossa pyydetään jonkin tieytyn OID:n arvoa. Tähän pyyntöön vastataan Response-viestillä, joka lähetetään takaisin managerille pyydetyllä datalla
- GetNext-viestillä manager voi pyytää seuraavaa peräkkäistä objektia MIB:ssä. Tällä tavoin voidaan kulkea MIB:n rakenteen läpi ilman, että tarvitsee tietää, mitä OID:tä kysellä.
- Set-viesti on managerin lähettämä viesti agentille, jonka tarkoituksena on muuttaa jonkin agentin muuttujan arvoa. Tätä voidaan käyttää laitteen konfiguraatiotietojen hallintaan tai tilan muuttamiseen. Tämä on ainoa protokollan määrittämä kirjoitusoperaatio.
- GetBulk-viesti on managerin lähettämä viesti agentille, joka toimii ikään kuin monta GetNext-pyyntöä olisi lähetetty samaan aikaan. Vastaus sisältää niin paljon dataa kuin paketin maksimikoko sallii.
- Response-viesti on agentin lähettämä viesti, jota käytetään pyydetyn tiedon lähettämiseen takaisin managerille. Se toimii pyydetyn datan kulkuvälineenä sekä kuittauksena pyynnön vastaanottamisesta. Jos pyydettyä dataa ei voida

palauttaa, sisältää vastaus virhekenttiä, joihin voidaan asettaa lisätietoja. Kaikkiin aikaisemmin esiteltyihin viesteihin ja Inform-viesteihin täytyy vastata Response-viestillä.

- Trap-viesti on yleensä agentin lähettämä viesti managerille. Trapit ovat asynkronisia ilmoituksia, joita managerit vastaanottavat niitä pyytämättä. Agentit käyttävät niitä hallittavien laitteiden tapahtumien ilmoittamiseen managereille.
- Inform-viesti on managerin lähettämä kuittaus vastaanotetusta trap viestistä. Jos agentti ei vastaanota Inform-viestiä, se jatkaa Trap-viestin uudelleenlähetystä.

(Ellingwood 2014; Huawei 2020.)

4.3.5 Versiot

SNMP protokolla on kokenut monia muutoksia sen julkaisun jälkeen. Sen ensimmäinen versio muotoutui RFC (Request for Comments) standardien 1065, 1066 ja 1067 myötä vuonna 1988. Koska ensimmäinen versio on ollut olemassa niin kauan, on se edelleen laajasti tuettu. Versiossa on kuitenkin paljon turvallisuusongelmia kuten autentikointi ilmitekstinä, joten on sen käyttö erittäin epäsuositeltavaa varsinkin suojaamattomissa verkoissa. (Ellingwood 2014.)

Version 2 työstäminen alkoi vuonna 1993 ja se tarjosi merkittäviä parannuksia aikaisempaan versioon. Uutena ominaisuutena esiteltiin osapuoliohjainen turvallisuusmalli, jonka tarkoituksena oli vastata aikaisemman version tietoturva ongelmiin. Uusi turvallisuusmalli ei kuitenkaan ollut kovin suosittu, koska sen ymmärtäminen ja käyttöönotto oli vaikeaa. Tästä syystä johtuen versiosta 2 luotiin muutamia muunnelmia (johdannaisia), jotka kaikki pitivät suurimman osan parannuksista, korvaten kuitenkin monimutkaisena pidetyn tietoturvamallin. Versiossa SNMPv2c esiteltiin uudelleen version 1 yhteisöpohjainen autentikointi ja se oli version 2 suosituin muunnelma. Toinen muunnelma nimeltä SNMPv2U käytti käyttäjäpohjaista turvamallia, joka mahdollisti käyttäjäkohtaiset autentikointi asetukset. Tämä muunnelma ei saanut ikinä paljon suosiota. (Ellingwood 2014.)

Vuonna 1998 esiteltiin SNMP protokollan kolmas ja nykyinen versio. Käyttäjän näkökulmasta merkityksellisin muutos oli käyttäjäpohjaisen turvamallin käyttöönotto. Se tarjoaa seuraavat kolme mallia käyttäjien autentikointivaatimusten asettamiseksi:

- NoAuthNoPriv, jossa yhteyden muodostavia käyttäjiä ei autentikoida mitenkään eikä lähetettyjä ja vastaanotettuja viestejä suojata.
- AuthNoPriv, jossa yhteydet autentikoidaan, mutta viestejä ei salata
- AuthPriv, jossa autentikointi vaaditaan ja viestit salataan.

(Ellingwood 2014.)

Autentikoinnin käyttöönoton lisäksi otettiin käyttöön myös pääsynhallinta mekanismi tuomaan "rakeista hallintaa" (eng. granular control) käyttäjien pääsyyn oksille. Versiolla 3 on myös kyky hyödyntää muiden protokollien, kuten SSH: n tai TLS: n, tarjoamaa turvallisuutta. (Ellingwood 2014.)

4.4 Suoratoisto telemetria

Verkon telemetrian suoratoisto on suhteellisen uusi mekanismi, joka käyttää ns. push-mallia datan lähettämiseen SNMP:n pollaukseen pohjautuvan pull-mallin sijaan. Suoratoisto telemetriassa dataa lähetetään automaattisesti ja jatkuvasti verkon laitteista hallintajärjestelmiin, ilman että sitä tarvitsee pollata erikseen verkon laitteilta. Dataa lähetetään suuremmissa määrissä ja verkon laitteisiin kohdistuva rasitus on parhaimmassa tapauksessa vähäisempää verrattaessa SNMP:hen. (Slattery 2020; Juniper 2021b.)

Data valitaan konfiguroimalla jaksottainen tahti, joka voi olla alle sekunnin tai jostakin tietyistä tapahtumista, kuten jonkin kynnyksen ylitys (esim. korkea virheiden määrä) tai tilan muutos (esim. portin tila muuttuu) käynnistyvä. Suoratoisto telemetriassa data on kuvattu datan mallinnuskieli YANG:illa (Yet Another Next Generation) ja koodattu käyttäen JSON:ia (JavaScript Object Notation), XML:ää (Extensible Markup Language) tai Googe Protocol Buffereita. Data suoratoistetaan käyttäen TCP:tä tai UDP:tä (User Datagram Protocol) tai salattua GRPC:tä (Google Remote Procedure Call). (Blueplanet 2018; Slattery 2020.)

Telemetria datan suoratoistoon on olemassa kaksi tapaa:

- Mallipohjainen telemetria (eng. Model-driven telemetry, lyh. MDT), joka tarjoaa mekanismin datan suoratoistoon MDT:tä tukevalta laitteelta kohteeseen. Suoratoistettavan datan siirto perustuu tilauksiin. (eng. subscription).
- Käytäntöperusteinen telemetria (eng. Policy-based telemetry), jossa telemetria data suoratoistetaan kohteeseen käyttäen käytäntötiedostoa (eng. policy file).

(Cisco 2020c.)

MDT-suoratoiston prosessi koostuu seuraavista komponenteista:

- destination (määränpää), joka määrittää yhden tai useamman kohteen, joista suoratoistettua dataa kerätään
- sensor path määrittää YANG-polun, josta data suoratoistetaan
- subscription (tilaus), joka sitoo yhden tai useamman sensor pathin määränpäihin ja määrittää kriteerit datan suoratoistamiselle
- Transport & encoding (kuljetus ja koodaus), jotka määrittävät datan kuljetuksessa käytetyn protokollan (GRPC, TCP, UDP) ja sen formaatin (XML, JSON, GPB)

(Cisco 2020c.)

Käytäntöperusteisen suoratoiston prosessi koostuu seuraavista komponenteista:

- policy file (käytäntötiedosto) määrittää suoratoistettavan datan ja sen tahdin.
- encoder (kooderi) kapseloi generoidun datan haluttuun formaattiin ja lähettää sen vastaanottimelle
- receiver (vastaanotin) hallintajärjestelmä, joka säilöö telemetria-datan

(Cisco 2020c.)

4.4.1 SNMP vai suoratoisto telemetria

SNMP toimii parhaiten kerättäessä hyvin pitkälle staattisena pysyvää dataa, kuten dataa inventaariosta tai naapurilaitteista. Sen pollaus-mekanismi tekee suurten korkealaatuisten (esim. suorituskyky data) datamäärien keräämisestä haastavaa. SNMP on käytännöllinen verkoissa, joissa on käytössä paljon vanhempia laitteita, jotka eivät tue suoratoisto telemetriaa. Se on myös hyvä suorituskykyä koskemattoman datan, kuten

esimerkiksi laiteinventaariodatan ja NTP-datan keräämiseen. Lisäksi, koska SNMP käyttää UDP:tä ei hallintapalvelinten tarvitse allokoida suuria vastaanottopuskureita, jonka seurauksena muistia vapautuu muuhun käyttöön. (Slattery 2020.)

Suoratoisto telemetria on parempi korkealaatuisen suorituskyky datan, kuten nopeiden verkkoliitäntöjen statistiikan keräämiseen. Siitä on tulossa koko ajan käytännöllisempi, kun yhä useampi laitetoimittaja on alkanut tukemaan teknologiaa. Tämän lisäksi uudemmat RPC (Remote Procedure Call) mekaniikat tekevät suoratoisto telemetriasta tehokkaamman ratkaisun verkon laitteiden datan keräämisen kannalta verrattuna SNMP:hen. Täytyy pitää kuitenkin mielessä, että TCP:tä käyttävä suoratoisto telemetria lisää mahdollisesti vastaanottavien laitteiden vastaanottopuskurien muistinkäyttöä, riippuen implementaatiosta. On hyvä pitää mielessä myös se, että eri valmistajilla on käytössä monia eri YANG-malleja, jonka seurauksena datan analysoimisesta tulee haasteellista. (Slattery 2020.)

Yhdistelmä SNMP:tä ja suoratoisto telemetriaa toimii parhaana ratkaisuna verkoille, joissa on käytössä sekä vanhoja että uusia laitteita. Siirtyminen pelkkään suoratoisto telemetriaan on mahdollista siinä vaiheessa, kun kaikki verkon laitteet tukevat sitä. Riippumatta siitä, käytetäänkö keräyksen keinona SNMP:tä vai suoratoisto telemetriaa, tulee keskeisimmäksi ongelmaksi muodostumaan aina kerättävä data. Hallintajärjestelmän täytyy käsitellä suuria määriä dataa poikkeamien tunnistamiseksi ja kyettävä varoittamaan verkkotiimiä ongelmista. Taulukossa 2 on yhteenveto SNMP:n ja suoratoisto telemetrian merkittävimmistä eroista. (Slattery 2020.)

Taulukko 2. SNMP:n ja suoratoisto telemetrian erot (tiedot Slattery 2020.)

	SNMP	Suoratoisto telemetria
Toimintatapa	Laitteiden dataa kerätään ja palautetaan hallintajärjestelmälle pollaus-mekanismilla.	Laitteiden dataa lähetetään hallintajärjestelmälle jatkuvana virtana.
Käytetyt protokollat	UDP	UDP, TCP tai GRPC

Käyttötapaukset	Staattisen datan, kuten inventaariodatan tai naapurilaite-datan kerääminen.	Korkealaatuisen suorituskyky datan, kuten nopeiden verkkoliitäntöjen statistiikan kerääminen.
Hyödyt	Yksinkertainen protokolla, joka tekee datan keräämisestä helppoa. Tukee suurinta osaa verkkolaitteista ja hallintajärjestelmistä.	Lähettää dataa suuremmissa määrissä, ollen näin tehokkaampi ja käytännöllisempi.
Haasteet	Hallintajärjestelmä joutuu luomaan ja lähettämään pyyntöjä jokaiselle laitteelle.	TCP:tä käyttävä suoratoisto telemetria voi käyttää paljon muistia.

5 LOPUKSI

Kun uusien tai toimintaansa laajentavien yritysten tulee aika suunnitella verkkoa, on tavoitteena usein saada verkko toimintaan mahdollisimman nopeasti. Tällä lähestymistavalla päädytään usein käyttämään erilaisia huonoihin lopputuloksiin johtavia oikoreittejä tai ohittamaan joitakin vaiheita kokonaan. On kuitenkin hyvä huomioida, että kaikkien hyvin onnistuneiden verkkojen takaa löytyy aina hyvä suunnitelma, jonka tekeminen ja toteuttaminen vaativat vahvaa teoreettista ja käytännön osaamista.

Opinnäytetyössä käsiteltyjen aiheiden myötä tuleviksi haasteiksi nousevat mm. vikasietoisuus, tietoruva ja skaalautuvuus. Vikasietoisuuden toteutumiseksi olennaisimpana harkinnan kohteena voitaisiin pitää verkon kahdentamista ja siihen liittyviä toimenpiteitä.. Verkkoon liitettävien laitteiden määrä on kasvanut paljon, ja erityisesti erilaisten IoT-laitteiden (Internet of Things) osuus on huomattava. On kyettävä mahdollistamaan se, että verkkoa voidaan laajentaa vaivattomasti, ilman suurempia koko verkkoon kohdistuvia uudistuksia. IoT-laitteiden tietoturva on myös hyvinkin vaihtelevaa, joten on pidettävä huoli, että verkon tietoturva kykenee estämään niiden käytön mahdollisena hyökkäyspintana.

LÄHTEET

Allen, N. 2009. Network Maintenance and Troubleshooting Guide Field-Tested Solutions for Everyday Problems. 2. painos. Boston: Addison-Wesley. Viitattu 27.1.2021. https://www.oreilly.com/library/view/network-maintenance-and/9780321647672/

ATIS 2013. ATIS Telecom Glossary carrier sense multiple access with collision detection (CSMA/CD). Viitattu 12.12.2020. https://web.archive.org/web/20130313194946/http://www.atis.org/glossary/definition.aspx?id=6102

Blueplanet 2018. What is streaming telemetry?. Viitattu 14.4.2021. https://www.blueplanet.com/blog/What-is-streaming-telemetry.html

Chapple, M., Stewart, J., Gibson, D. 2018. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. 8. painos. Indianapolis: Wiley. Viitattu 4.2.2021. https://www.wiley.com/en-us/%28ISC%292+CISSP+Certified+Information+Systems+Security+Professional+Official+Study+Guide%2C+8th+Edition-p-9781119475873

Cisco Networking Academy 2014. Connecting Networks Companion Guide. Indianapolis: Cisco Press. Viitattu 20.1.2021. https://www.oreilly.com/library/view/connecting-networks-companion/9780133476507/

Cisco Networking Academy 2016. Routing and Switching Essentials v6 Companion Guide. Indianapolis: Cisco Press. Viitattu 12.12.2020. https://www.ciscopress.com/store/routing-and-switching-essentials-v6-companion-guide-9780134669618

Cisco 2020a. What Is a LAN?. Viitattu 12.12.2020. https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

Cisco 2020b. Network Address Translation (NAT) FAQ. Viitattu 17.12.2020.

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Cisco 2020c. Telemetry Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x. Viitattu 15.4.2021. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/telemetry/b-telemetry-cg-ncs5500-62x.html

Conrad, E., Misenar, S., Feldman, J. 2015. CISSP Study Guide. 3. painos. Massachusetts: Syngress Publishing. Viitattu 12.2.2020. https://www.elsevier.com/books/cissp-study-guide/conrad/978-0-12-802437-9

Deal, R. 2008. CCNA Cisco Certified Network Associate Study Guide (Exam 640-802). 3. painos. New York: McGraw-Hill. Viitattu 27.1.2021. https://www.oreilly.com/library/view/ccna-cisco-certified/9780071497282/

Donahue, G. 2011. Network Warrior. 2. painos. California: O'Reilly Media. Viitattu 12.12.2020. https://www.oreilly.com/library/view/network-warrior-2nd/9781449307974/

Ellingwood, J. 2014. An Introduction to SNMP (Simple Network Management Protocol). Viitattu 9.4.2021. https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol

Fall, K. & Stevens, R. 2012. TCP/IP Illustrated, Volume 1. 2. painos. Harlow: Pearson. Viitattu 26.1.2020. https://www.pearson.com/us/higher-education/program/Fall-TCP-IP-Illustrated-Volume-1-The-Protocols-2nd-Edition/PGM69698.html

Forouzan, B. 2013. Data Communications and Networking. 5. painos. New York: McGraw-Hill. Viitattu 19.12.2020. https://www.mheducation.com/highered/product/data-communications-networking-forouzan/M9780073376226.html

Froom, R., Sivasubramanian B., Frahim, E. 2010. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Indianapolis: Cisco Press. Viitattu 12.12.2020.
https://www.oreilly.com/library/view/implementing-cisco-ip/9781587141652/

Hackernoon 2021. An Introduction to Layer 3 Switches. Viitattu 18.1.2021.
https://hackernoon.com/an-introduction-to-layer-3-switches-ys4h34rg

Hartpence, B. 2011. Packet Guide to Routing and Switching. Kalifornia: O'Reilly Media, Inc. Viitattu 5.1.2021.
https://www.oreilly.com/library/view/packet-guide-to/9781449311315/

Hassan, N. 2019. The Effect of Project Management Capabilities on Project Success in Pakistan: An Empirical Investigation. Viitattu 6.4.2021.
https://www.researchgate.net/figure/Levels-of-maturity-in-capability-maturity-model-CMM_fig2_332215821

Horak, R. 2007. TELECOMMUNICATIONS AND DATA COMMUNICATIONS HANDBOOK. New Yersey: Wiley. Viitattu 19.1.2020.
https://onlinelibrary.wiley.com/doi/book/10.1002/9780470399224

Huawei 2020. What Is a SNMP?. Viitattu 9.4.2021. https://support.huawei.com/enterprise/en/doc/EDOC1100086963

Imperva 2020. OSI Model. Viitattu 12.12.2020. https://www.imperva.com/learn/application-security/osi-model/

Juniper 2021a. Layer 2 Networking. Viitattu 26.1.2021. https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/layer-2-understanding.html

Juniper 2021b. Overview of the Junos Telemetry Interface. Viitattu 13.4.2021.
https://www.juniper.net/documentation/us/en/software/junos/interfaces-telemetry/topics/concept/junos-telemetry-interface-oveview.html

Keenetic 2019. What is the difference between a public and private IP address?. Viitattu 17.12.2020. https://help.keenetic.com/hc/en-us/articles/213965789-What-is-the-difference-between-a-public-and-private-IP-address-

Knipp, E., Browne, B., Weaver, W., Baumrucker, T., Chaffin, L., Caesar, J., Osipov, V., Danielyan, E. 2002. Managing Cisco Network Security. 2. painos. Massachusetts: Syngress Publishing. Viitattu 12.12.2020. https://www.elsevier.com/books/managing-cisco-network-security/syngress/978-1-931836-56-2

Kurose, J. & Ross, K. 2017. Computer Networking A Top-Down Approach. 7. painos. Harlow: Pearson Viitattu 26.1.2021. https://www.pearson.com/us/higher-education/program/Kurose-Computer-Networking-A-Top-Down-Approach-7th-Edition/PGM1101673.html

Lammle, T. 2011. CCNA Cisco Certified Network Associate Study Guide. 7. painos. New Jersey: Sybex. Viitattu 26.1.2021. https://www.wiley.com/en-fi/CCNA+Cisco+Certified+Network+Associate+Study+Guide%2C+7th+Edition-p-9780470901076

McMillan, T. 2015. Cisco Networking Essentials. 2. painos. New Jersey: Sybex. Viitattu 12.12.2020. https://www.oreilly.com/library/view/cisco-networking-essentials/9781119092155/

Metaswitch 2021a. What is Open Shortest Path First (OSPF)?. Viitattu 8.1.2021. https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf

Metaswitch 2021b. What is Border Gateway Protocol (BGP)?. Viitattu 11.1.2021. https://www.metaswitch.com/knowledge-center/reference/what-is-border-gateway-protocol-bgp

Molenaar, R. 2020. Broadcast Domain. Viitattu 12.12.2020.

https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/broadcast-domain

Netgear 2020. What is a MAC-based VLAN and how does it work with my managed switch?. Viitattu 12.12.2020. https://kb.netgear.com/21586/What-is-a-MAC-based-VLAN-and-how-does-it-work-with-my-managed-switch

Quine, A. 2008. Carrier Sense Multiple Access Collision Detect (CSMA/CD) Explained. Viitattu 12.12.2020. https://www.itprc.com/carrier-sense-multiple-access-collision-detect-csmacd-explained/

RFC 791. 1981. Internet Protocol. Viitattu 12.12.2020. https://tools.ietf.org/html/rfc791

Sathyan, J. 2010. Fundamentals of EMS, NMS, and OSS/BSS. Florida Auerbach: Publications. Viitattu 20.3.2021. https://www.routledge.com/Fundamentals-of-EMS-NMS-and-OSSBSS/Sathyan/p/book/978142008573

Sequeira, A. 2013. Cisco ICND1 Foundation Learning Guide: LANs and Ethernet. Viitattu 19.1.2020. https://www.ciscopress.com/articles/article.asp?p=2092245&seqNum=2

Singh, H. 2017. Implementing Cisco Networking Solutions: Configure, implement, and manage complex network designs. Birmingham: Packt Publishing. Viitattu 20.3.2021. https://books.google.fi/books/about/Implementing_Cisco_Networking_Solutions.html?id=xplGDwAAQBAJ&redir_esc=y

Slattery, T. 2020. Telemetry vs. SNMP: Is one better for network management?. Viitattu 13.4.2021. https://searchnetworking.techtarget.com/answer/Telemetry-vs-SNMP-Is-one-better-for-network-management

Study-ccna 2020. Ethernet Explained. Viitattu 12.12.2020. https://study-ccna.com/ethernet/

Tanenbaum, A. & Wetherall, D. 2011. Computer Networks. 5. painos. New Jersey: Prentice Hall. Viitattu 26.1.2021. https://www.pearson.com/us/higher-education/program/Tanenbaum-Computer-Networks-5th-Edition/PGM270019.html

Thomas, T., Pavlichek, D., Chowbay, R., Dwyer, L., Sonderegger, J., Downing, W. 2002. Juniper Networks Reference Guide: JUNOS Routing, Configuration, and Architecture. Boston: Addison-Wesley. Viitattu 12.12.2020. https://www.pearson.com/store/p/juniper-networks-reference-guide-junos-routing-configuration-and-architecture-junos-routing-configuration-and-architecture/P100000140089

Vacca, J. 2017. Computer and Information Security Handbook. 3. painos. Massachusetts: Morgan Kaufmann Publishers. Viitattu 5.1.2021. https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7