Tampereen ammattikorkeakoulu

# Verkkosuunnittelun periaatteita

Hiski Hämäläinen

OPINNÄYTETYÖ
Toukokuu 2022

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

**TIIVISTELMÄ**

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

HÄMÄLÄINEN, HISKI
Verkkosuunnittelun periaatteita

Opinnäytetyö 33 sivua, joista liitteitä 1 sivu
Toukokuu 2022

---

Opinnäytetyö kertoo yleismuotoisesti katsaustyyppisesti verkkosuunnittelussa huomioitavista osa-alueista ja periaatteista. Erityisesti keskitytään erityyppisiin tarpeisiin ja vaatimuksiin, joiden perusteella mihinkin suunnitteluratkaisuun päädytään ja joita verkolta odotetaan vaatimusanalyysin muodossa. Verkolta odotetut vaatimukset listataan SLA:han eli palvelutasosopimukseen, joka määrittää asiakkaan haluaman verkon ominaisuudet, esimerkiksi skaalautuvuuden tai luotettavuuden osalta. Opinnäytetyössä tarkastellaan myös verkkosuunnittelua hallinnoinnin kautta. Tämä sisältää katsauksen menetelmistä sekä viitekehyksen verkkohallinnoinnin havainnollistamiseen ja toteutukseen. Edellytyksenä verkkosuunnittelulle ja sen todentamiselle on jatkuva verkon monitorointi. Verkkomonitoroinnin osalta käydään läpi työkaluja ja protokollia, joilla palvelutason parametrit ja verkon ongelmatilanteita pystytään tunnistamaan.

Opinnäytetyössä ei niinkään keskitytä tiettyihin teknologioihin tai niiden yksityiskohtaiseen toimintaan tarkasti, vaan enemmän pyritään luomaan kokonaiskuvaa verkkosuunnittelun toteutuksesta. Lähtökohtaisesti työssä keskitytään pienten ja keskikokoisten, kymmenien ja satojen koneiden yritysverkkoihin, joskin monet käsitellyistä periaatteista skaalautuvat muihinkin kokoluokkiin.

---

Asiasanat: verkot, verkkosuunnittelu, verkkohallinnointi

## ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

HÄMÄLÄINEN, HISKI
Network Design Principles

Bachelor's thesis 33 pages, appendices 1 pages
May 2021

---

The thesis provides a general overview of the network design principles, focusing on the different types of demands and requirements the network should fulfill. The requirements expected from the network are listed in the service level agreement, which defines the characteristics of the network that the customer wants, for example in terms of scalability or reliability. The thesis also examines network management as a part of the network design cycle. This includes an overview of the methods and a framework for management functionalities. Continuous network monitoring is a prerequisite for successful network design and its validation. Lastly, the thesis goes through network monitoring tools and protocols used to identify service level parameters and network problem situations.

The thesis does not focus so much on certain technologies or their detailed operation, but rather on creating an overall picture of the network design with the emphasis on the enterprise networks, on a scale of small and medium-sized networks, consisting of tens and hundreds of endpoints. Although many of the principles discussed also scale to other size classes.

---

Key words: networks, network design, network management

**SISÄLLYS**

## LYHENTEET JA TERMIT

| | |
|---|---|
| ACL | Access-control list, käyttöoikeuslista |
| FCAPS | Fault, Configuration, Accounting/Allocation, Performance and Security Management, verkkohallinnan malli |
| ICMP | Internet Control Message Protocol, kontrolliprotokolla |
| IOT | Internet of Things, esineiden internet |
| ITU-T | International Telecommunications Union Telecommunication Standardization Sector |
| IP | Internet Protocol, verkkokerroksen viestintäprotokolla |
| LAN | Local Area Network, lähiverkko |
| M2M | Machine-to-machine, laitteiden välinen viestintä |
| MIB | Management Information Base, hallintatietokanta |
| MTBF | Mean time between failures, keskimääräinen kulunut aika järjestelmän vikojen välillä. |
| MTBCF | Mean time between critical failures, keskimääräinen kulunut aika järjestelmän kriittisten vikojen välillä. |
| MTTR | Mean time to repair, keskimääräinen kulunut aika järjestelmän kuntoon saamiseksi. |
| OID | Object Identifier, SNMP-protokollan objektin tunniste |
| SLA | Service Level Agreement, palvelutasosopimus |
| SNMP | Simple Network Management Protocol, verkonhallintaprotokolla |
| TMN | Telecommunications Management Network, verkkohallintamalli |
| WAN | Wide Area Network, laajaverkko |

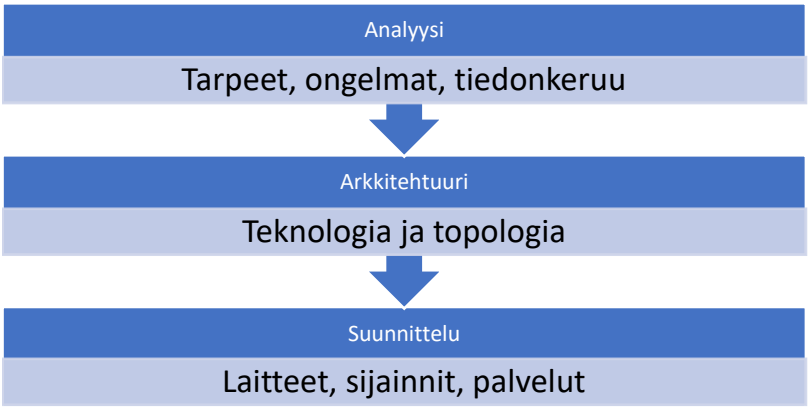
# 1 Johdanto

Erilaisten tietoverkkojen merkitys on jatkuvassa kasvussa, eikä vain liiketoiminnan tehostamisessa, vaan ylipäätänsä se mahdollistamisessa monella alalla. Verkon lyhytaikaisetkin katkokset ja palvelunlaadun ongelmat voivat olla merkittävä kustannustekijä, minkä vuoksi toimiva onnistunut verkkosuunnittelu voi olla avainkilpailutekijöitä monelle yritykselle. Siispä verkon nykyisten ja tulevien palveluiden ja sovellusten lisäksi, myös liiketoiminnan tarpeet tulee ottaa huomioon suunnittelussa.

Verkon rakennus-, päivitys- ja ylläpidolliset toimenpiteet tapahtuvat alati muuttuvassa maailmassa, mikä edellyttää kokonaisvaltaisempaa ja pitkän aikavälin suunnittelua. Vaikka kaikkea tulevaa ei pystytäkään tehokkaasti ennustamaan, ja odottamattomia tilanteita tulee väistämättä vastaan, on kumminkin monia verkkosuunnittelun eri periaatteita luotettavan ja toimivan verkon luomiseksi. Opinnäytetyössä on tarkoitus pohtia haasteita ja verkkosuunnittelun osa-alueita, joita esiintyy yritystoimintaympäristöissä.

## 2 Strateginen suunnittelu

Verkon suunnittelun vaiheita voidaan havainnollistaa vaikkapa jakamalla ne verkon analysointiin, arkkitehtuuriin ja suunnitteluun, kuten kuviossa 1. Vaiheet ovat yhteydessä toisiinsa niin että muutokset yhdessä vaikuttava oleellisesti seuraavan vaiheen ratkaisuihin ja kokonaisuuden toimintaan. Analyysivaihe on eräänlainen ongelmien määrittely, joihin myöhemmissä vaiheissa haetaan ratkaisut. Analyysivaiheessa tarkastellaan olemassa olevan verkon tilaan, käyttäjien tarpeita, liikennevirtoja, nopeuksia ja monia muita verkon toimintaan vaikuttavia tekijöitä, joiden pohjalta verkon arkkitehtuurin valinnat muodostetaan. (McCabe 2007.)




KUVIO 1. Verkkosuunnittelun prosessit (McCabe 2007, muokattu).

Verkkoarkkitehtuurivaiheessa analyysinvaiheen pohjalta muodostettuihin ongelma- ja tarvekuvauksiin valitaan niiden tarpeet täyttävät teknologiat ja topologiaratkaisut. Prosessiin sisältyy myös laitteiden ja verkkojen välisten reititysten, tietoturvan ja palvelunlaadun ratkaisujen sovittamista verkon toimintaympäristön reunaehtoihin (McCabe 2007). Tyypillinen arkkitehtuuritason päätös voi olla, vaikka päätös laitteiden omistamisen ja pilven välillä.

Lopulliseen suunnitteluvaiheeseen kuuluu suunnittelu- ja arkkitehtuurivaiheen toteuttaminen fyysisillä laitevalinnoilla ja niiden konfiguroinnilla, sekä palveluntarjoajin valinnalla. Prosessiin sisältyy myös kustannusten tasapainottamista haluttujen verkolta haluttujen ominaisuuksien kanssa. Verkon kustannukset muodostuvat laitehankintojen lisäksi ohjelmistolisensseistä, ylläpito- ja tukisopimuksista, testauksesta, sekä koulutus- ja henkilöstökuluista.

Verkkoon tehtyjen muutosten jälkeen ei prosessi jää siihen vaan verkon käyttötarpeet sekä ympäristö missä se toimii, ovat alati muutoksessa, on verkon suunnittelu syklinen, iteratiivinen kokonaisuus, eikä vai väliaikainen tila sen alkuvaiheessa.

# 3 Vaatimusanalyysi

Joka verkolle on aina olemassa joukko vaatimuksia. Vaatimukset ovat kuvauksia verkon toiminnoista ja suorituskyvystä, joilla vastataan verkon käyttäjien ja verkkoa hyödyntävien sovellusten tarpeisiin. Yritykselle vaatimukset verkolle ovat taloudellisiin seikkoihin perustuvia kuten verkon käyttökustannusten vähentämistä ja tuottavuuden parantaminen verkon kehittämisen kautta. Kustannustehokkuus onkin arvioita asia verkkosuunnittelun joka kompromississa ja priorisoinnissa laitevalinnoista arkkitehtuuriin.

## 3.1 Asiakkaan tarpeet

Asiakkaan edellyttämät verkon palvelutason vaatimukset, jotka verkon tulee täyttää, määritellään palvelutasosopimuksessa (SLA). Palvelutaso muodostuu joukosta pääsääntöisesti mitattavissa olevista toiminnallisista tai ei-toiminnallisista vaatimuksia, joista toiminnalliset vaatimukset kuvaavat nimensä mukaisesti verkolta odotettua toimintaa. Ne määrittävät halutut tekniikat, kuten esimerkiksi vaatimus SD-WAN-yhteydestä muihin organisaation toimipisteisiin tai toimitilat kattavasta AX-standardin WLAN:sta tai hajautetusta verkonhallinnasta. Ei-toiminnalliset, tai tekniset vaatimukset puolestaan toimivat reunaehtoina toiminnallisten vaatimusten tekniselle toteutukselle. Saatavuus, kapasiteetti, ylläpidettävyys, turvallisuus ja skaalautuvuus ovat kaikki tietoverkoille ominaisia ei-toiminnallisten vaatimusten osa-alueita. Aikaisemman esimerkin WLAN-tuen tapauksessa tämä voisi tarkoittaa vaatimuksia esimerkiksi tietyn käyttäjämäärän palvelemiseen tietyllä nopeudella, tietyllä viiveellä ja tietyn kokoisessa tilassa. Kyseiset vaatimukset samalla toimivat perusteina tietynlaisia laitteita valittaessa. Ovatko viiveen ja kapasiteetin vaatimukset kyllin suuria oikeuttamaan useamman nelikaistaisen tukiaseman käyttöä vai riittääkö muutama halvempi vähäenerginen malli?

Vaatimuksia voivat myös esimerkiksi olla tiettyjen turvallisuusstandardien täyttäminen, verkon skaalautuvuuden tai tukipalvelujen huomiointi. Palveluntason tavoitteet laaditaan asiakkaan liiketoiminnan tarpeiden ja kustannusrajoitteiden perusteella, mahdollisesti verkon useamman eri

käyttäjäryhmän erityistarpeet huomioiden. Esimerkiksi tietyn käyttäjäryhmän pääsy verkkoon voi olla liiketoiminnan kannalta kriittisempää kuin jonkin toisen ja näin edellyttää nopeammin toimivia tukipalveluja ja luotettavampaa verkkoa. Sovittu palvelutaso toimii verkkosuunnittelun tavoitteena, jota vasten verkkosuunnittelun onnistumista voidaan verran. Palvelutason ylläpito edellyttää verkonhallintaa, jonka vastuualueet voidaan myös kirjata palvelutasosopimukseen ylös. Lisäksi SLA:ta laatiessa mahdolliset sanktiot ja korvausmenettelyt on syytä huomioida tilanteissa, joissa verkko ei pääsekään tavoiteltuun palvelutasoon. (Service Level Management: Best Practices 2022.)

Yrityskäyttöön suunnitellut verkot voivat alasta ja käyttökohteestaan riippuen lisäksi edellyttää erilaisia verkon suunnitteluun vaikuttavia standardeja ja sertifikaatteja, eikä pelkästään tietoturvan tason vuoksi vaan myös sen todistamiseksi. Tyypillisiä standardeja ovat muun muassa tietoturvallisuuden hallintajärjestelmien ISO/IEC 27000-sarjan standardit, kuten ISO/IEC 27033-standardi, joka ohjaa verkon suunnittelua, tekniikoita ja valvontaratkaisuja tietoturvan kautta (IsecT Ltd. ISO 27033. 2021), tai esimerkiksi tiedon varastointia käsittelevä ISO/IEC 27040-standardi (IsecT Ltd. ISO 27040 2021.)

### 3.2 Skaalautuvuus

Yritykselle verkon skaalautuvuus ja joustava rakenne voivat olla tärkeitä yrityksen tulevaisuuden suunnitelluissa tai ennalta odottamattomissa muutostilanteissa, kuten henkilömäärän kasvun, toimipisteen lakkautuksen tai yhdistymisen tapahtuessa. Joustamaton verkko voi muutostilanteessa olla monimutkainen kaapelointien ja hallittavuuden suhteen, mikä puolestaan laskee kustannustehokkuutta sen sitoessa työvoimaa ja ollessa epäoptimaalinen uudessa toimintaympäristössään. Verkon rakenteen joustavuutta voidaan edistää suunniteltaessa sitä modulaarisemmaksi.

Modulaarisessa suunnittelussa verkko pyritään jakamaan useampaan moduuliin tai lohkoon, joista jokainen palvelee tiettyä roolia verkossa. Lohko on yleensä tiettyyn paikkaa sidoksissa oleva fyysinen verkko, kuten esimerkiksi palvelinkeskus suurten tietomäärien käsittelyyn ja varastointiin tai reunaverkko

verkon ulkopuolisen liikennöintiin. Modulaarisuuden on tarkoitus tehdä verkon suunnittelusta ja ylläpidosta yksinkertaisempaa, ja sitä kautta halvempaa, kun moduuleita voidaan lisätä, poistaa ja muokata muun verkon arkkitehtuuriin puuttumatta. Moduulien ollessa itsenäisiä kokonaisuuksia, modulaarisessa verkossa lohkon vikatilanteessa vika rajoittuu vain kyseisen lohkon toiminnallisuuksia koskevaksi, eikä verkon toiminta muilta osin esty. (Al-shawi 2015.)

Verkoissa korkeisiin skaalautuvuuden ja joustavuuden vaatimuksiin voidaan vastata pilviteknologioita hyödyntämällä. Pilveen sijoitettuina verkkoresursseja, kuten laskentakapasiteettia tai tallennuskapasiteettia, voidaan dynaamisesti allokoida hyvinkin nopeasti pilvipalvelutarjoajan asiakkaiden välillä tarpeen mukaan ilman verkkopalveluiden keskeytymistä. Verkon kustannusten skaalautuminen on toinen pilvipalvelun käytön etu, kun yrityksen ei välttämättä tarvitse rakentaa omaa investointeja edellyttävää verkkoinfrastruktuuria. Sen sijaan pilven verkkoresurssien käyttöperusteinen laskutus mahdollistaa myös pienemmillä yrityksillä suorituskykyisten ja hallinnoitujen korkeatasoisten verkkojen hyödyntämisen. (Fox, R. Hao, W 2018.)

### 3.3 Topologia

Verkon topologiaa, eli verkon laitteiden ja linkkien sijoittumista verkossa suhteessa toisiinsa, voidaan kuvata fyysisesti (Liite 1) tai loogisesti (Liite 2). Fyysisessä topologiassa verkon laitteet ovat yhteydessä toisiinsa kaapeilla, mikä vastaa sitä miltä verkko myös todellisuudessa näyttää silmin tarkasteltuna, mutta sen pohjalta ei voida vielä päätellä mitä reittiä paketti pääsee verkkolaitteelta toiselle. Looginen topologia näyttää puolestaan laitteiden välisen tiedonkulun reitit verkossa, jotka eivät välttämättä vastaa fyysistä verkkoa. Verkon topologia muodostaa verkon perustan, ja eri topologiamalleilla on eroja verkon toiminnan ja kustannusten kannalta, minkä vuoksi verkon topologia toimii verkon suunnittelua ohjaavana tekijänä.

Melkein joka kodin lähiverkosta tutussa tähtitopologiassa verkon päätelaitteet ovat kytkettynä kytkimeen tai reitittimeen, jonka kautta kaikki liikenne ohjataan

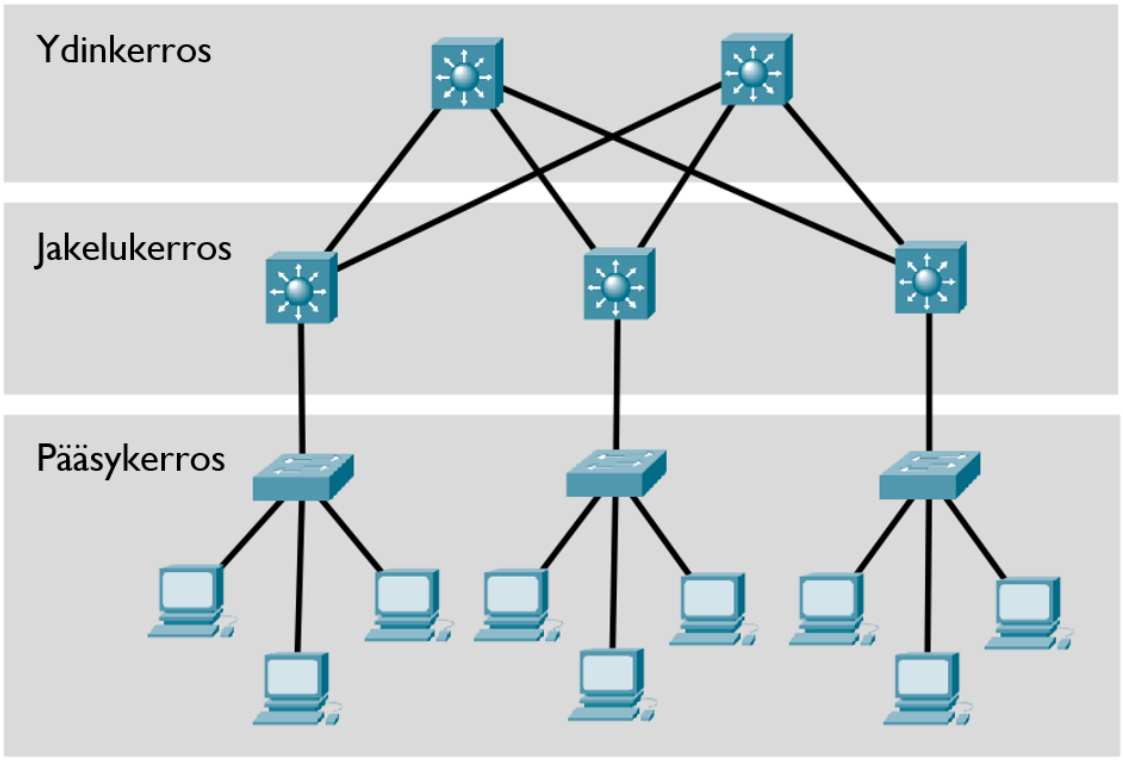
muille päätelaitteille tai ulos verkosta. Päätelaitteen hajoaminen ei vaikuta muuhun verkkoon, mutta vika keskuspisteen laitteessa, jonka kautta kaikki topologian liikenne kulkee estää liikenteen kaikkien siihen kytkettyjen laitteiden välillä. Perinteisen tähtitopologian skaalautuvuuden rajat tulevat kuitenkin äkkiä vastaan, kun päätelaitteita tulee verkkoon satoja tai tuhansia. Tällöin jo pelkkiä neljänkymmenenkahdeksan portin kytkimiä tarvitaan verkkoon lukuisia.

Tyypillinen suunnitteluperiaate ratkaisuksi on tehdä verkosta hierarkkinen. Hierarkkisuudella tarkoitetaan verkon jakamista eri kerroksiin ja verkkoliikenteen johtamista tiettyjen verkon sisäisten liitäntäpisteiden kautta kulkevaksi. Verkon eri hierarkkisilla kerroksilla on omat roolinsa, joita suorittamaan voidaan valita parhaiten juuri niihin soveltuvat verkkolaitteet ja ohjelmistot. Hierarkkinen arkkitehtuuri suunnitellaan lähtökohtaisesti modulaariseksi ja skaalautuvaksi. (Graziani 2014.)

Tyypillinen kolmikerroksinen hierarkkinen arkkitehtuurimalli (kuvio 2) koostuu core-, distribution-, ja access-kerroksista. Access-, eli pääsykerros tarjoaa pääsyn verkkoon sen päätelaitteille ja palvelimille. Kerros on hierarkkisen mallin alin ja lähimpänä verkon käyttäjää. Suurin osa verkon kytkimistä sijaitsee pääsykerroksella, jolloin ei niiden välttämättä tarvitse olla erityisen nopeita tai porttimääriinsä suhteutettuina kalliita laitteita, sillä niiden kautta ei ohjata koko verkon liikennettä, eikä niiltä edellytetä ylempien kerrosten kytkimien kaikkia toiminnallisuuksia kuten verkkokerroksen protokolia (IP, VLAN, ym.)

Distribution-, eli jakelukerros, josta käytetään myös nimeä aggregointikerros, on arkkitehtuurin välikerros, joka kokoaa WAN- ja pääsytason LAN-liikenteen ja hoitaa sen reitityksen. Laitteiden välisiä yhteyksiä myös rajoitetaan ja suodatetaan pääsylistoilla (ACL) porttien ja IP-osoitteiden perusteella tai QoS-tekniikoilla. Jakelukerroksella verkko luotettavuutta tai tavoitettavuutta voidaan kasvattaa sen redundanssia lisäämällä. Tämä tarkoittaa ylimääräisten reitittimien, kytkinten, kaapelien tai yhteyksien lisäämistä verkkoon, mikä luo vaihtoehtoisia yhteysreittejä vika- ja virhetilanteiden varalta. Mikäli yrityksen verkolle yhteys ulkopuoliseen maailmaan on erittäin kriittinen, voi sillä olla useampi WAN-portti käytössään (Graziani 2014).

Core-kerros eli ydinkerros yhdistää verkon jakelukerroksen kytkimet toiseensa. Kerroksella sijaitsevat yleensä verkon nopeimmat ja tehokkaimmat kytkimet ja reitittimet liikenteen siirtämistä varten, eikä kerroksella ei tulisi olla liikennettä tuottavia laitteita, tai tarvetta pakettien käsittelylle, joka voisi turhaan hidastaa kerroksen toimintaa.

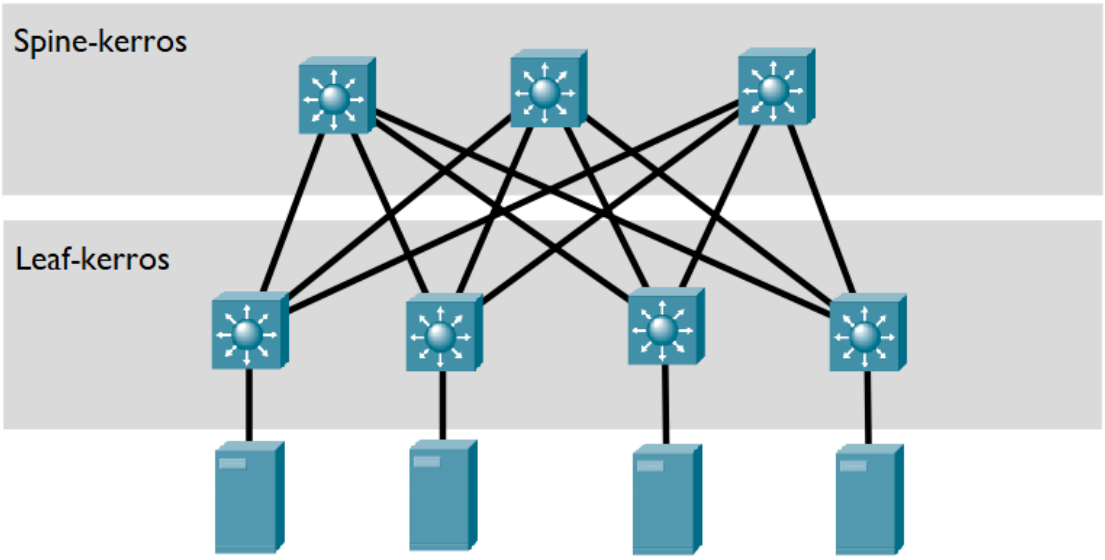



KUVIO 2. Kolmikerroksinen hierarkkinen arkkitehtuurimalli (Connecting Networks Companion Guide 2014, muokattu)

Pienemmän kokoluokan verkoissa voidaan soveltaa yksinkertaisempaa ja laitteistokustannuksiltaan halvempaa kaksikerroksista mallia, jossa ydin- ja jakelukerros ovat yhdistetty yhdeksi ja samaksi collapsed core –kerrokseksi. Ilman eriytettyä ydinkerrosta malli ei skaalaudu isommaksi verkoksi ilman suorituskyvyn alenemista. (Graziani 2014.)

Toinen kaksikerroksinen malli on spine and leaf -malli (kuvio 3), joka on kehitetty erityisesti datakeskusten horisontaalisten, sisäisten palvelimelta palvelimelle kulkevien liikennevirtojen palvelemiseen, kun taas vastaavasti perinteisempi hierarkkinen kolmikerrosmalli on suunniteltu enemmänkin vertikaalista, verkosta ulos suuntautuvaa liikennettä varten. Malli koostuu ylemmän spine-kerroksen reitittävistä kytkimistä ja leaf-kerroksen kytkimistä, joka ovat yhteydessä

jokaiseen spine-kerroksen kytkimistä mesh-tyyppisesti. Näin miltä leaf-kerroksen kytkimeltä tahansa on kahden hypyn helposti ennakoitava viive millä tahansa toiselle leaf-kerroksen kytkimelle, joihin myös verkon päätelaitteet ja palvelimet ovat kytkettyinä. Verkon sisäisen liikenteen reitti voi olla satunnaisesti valittu, jolloin kuormitus jakaantuu spine-kerrokselle tasaisesti. Mallissa verkon laajetessa sisäisten yhteyksien määrä kasvaa nopeasti ja edellyttää valtavaa määrää fyysisiä kaapeleita.




KUVIO 3. Kaksikerroksinen Spine and leaf -arkkitehtuurimalli (Sheldon & Younger 2020, muokattu)

### 3.4 Liikenne

Verkkoa hyödyntävillä sovelluksilla on erilaisia suorituskykyvaatimuksia verkon suhteen, jotka sovelluksien, käyttäjien ja laitteiden sijaintien lisäksi muodostavat perustan arvioitaessa missä, minkä suuntaista, miten paljon ja minkälaista liikennettä verkon läpi kulkee. Liikennevirtojen tunnistaminen on oleellista verkkoarkkitehtuurin ja verkkosuunnittelun kannalta, jotta verkko voidaan mitoittaa kustannustehokkaasti ja sovellusten tarpeita vastaavaksi (McCabe 2007). Liikennevirtojen arvioinnin rinnalla onkin olemassa erityisiä liikenteen seuraamiseen kehitettyjä protokollia, kuten NetFlow tai IPFIX.

Liikenteen osalta trendinä verkkolaitteiden määrän kasvun myötä maailmassa myös M2M-tyyppisten, koneelta koneelle tapahtuvien yhteyksien ja IOT-laitteiden osuus kasvaa muihin laitetyyppeihin nähden, kuten PC:siin tai älypuhelimiin. Ciscon vuosittaisessa ennusteessa arvioidaan kotitalouskohtaisten M2M-yhteyksien osuuden nousevan 33 %:sta 50 %:iin. (Cisco Annual Internet Report 2021.)

M2M-laitteet, kuten älysensorien, puettavan teknologian tai vaikka autotelemetriikan sovellukset, ovat verkkoliikenteensä vaatimuksiltaan kovin erilaisia suoraan ihmisen ohjaamaan teknologiaan verrattuna. IOT:tä runsaasti hyödyntävissä verkoissa toisilleen viestivien laitteiden määrä voi olla valtava, mutta samalla taas laitekohtaiset tiedonsiirtomäärät voivat olla varsin pieniä, Lähetykset ovat tyypillisesti säännöllisen väliajan lyhyen käyttöjakson uplink-painotteisia purskeita. M2M-viestit ovat samantyyppisten laitteiden välillä usein samankaltaisia ja tiedonsiirtomalli helpommin ennustetavissa. (M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic, S. Krco 2014.)

M2M-tyyppistä liikennettä varten langattomissa ympäristöissä on olemassa *LPW*A-verkkoja *(*low-power wide-area), kuten esimerkiksi LoRa-verkot tai matkapuhelinverkossa toimivat NB-IoT. Laajempaa langatonta kaistaa vaativat sovellukset, kuten liikkuvan kuvan siirtäminen videovalvontajärjestelmissä tai lyhyttä viivettä edellyttävät robotiikan, liikenteen tai terveysteknologian sovellukset voivat toimia WiFi-rajapinnassa tai ulkoympäristössä toimiessa matkapuhelinverkossa, esimerkiksi 5G:tä hyödyntäen.

### 3.5 Olemassa oleva verkko ja toimintaympäristö

Verkkosuunnittelussa harvemmin suunnitellaan uutta verkkoa tyhjästä, vaan yleensä toimitaan jonkin olemassa olevan verkon kanssa, johon tahdotaan muutoksia, kuten ominaisuuksien tai lohkojen lisäämistä, käytetyn teknologien päivittämistä tai muita päivityksiä. Olemassa olevan verkon arkkitehtuuriset ratkaisut, käytetty teknologia ja muut ominaisuudet vaikuttuvat myös tulevan verkon suunnittelussa (McCabe 2007). Esimerkiksi kun olemassa olevan verkon arkkitehtuuri on suunniteltu valmiiksi helposti skaalautuvaksi, verkon laajennus

voi hoitua verkkolaitteita vain lisäämällä. Vastaavasti esimerkiksi verkon laitteiden ollessa jo vanhoja ilman suunnitelmaa niiden vaihtamiseksi, saattaa verkossa aiheutua ongelmia uusien ominaisuuksien tai protokollien käyttöönotossa, kun vanhat laitteisto eivät näitä tue.

Olemassa olevat verkot sisältävät lukuisia erilaisia käytänteitä kuten IP-osoitesuunnitelmat, reititysprotokollien valinnat ja konfiguraatiot sekä nimeämisstrategiat, joita joko noudatetaan sellaisenaan tai päivitetään verkkosuunnittelun myötä. Lisäksi verkossa oletettavasti toimii monia erilaisia tukipalveluita, kuten verkon tietoturva-, monitorointi- ja hallinnointipalveluja, joiden toimintaa voidaan joutua määrittään verkon muutostöiden jälkeisiin puitteisiin. (McCabe 2007.)

Myös monet verkon ulkopuoliset tekijät, joihin ei verkkosuunnittelulla voida välttämättä puuttua mitenkään, vaikuttavat suoraan tai epäsuorasti suunnittelun reunaehtoihin. Tällaisia tekijöitä ovat esimerkiksi budjettirajat, sijainti, aika, henkilöstö ja lainsäädäntö. Verkon fyysinen sijainti voi estää kuituinfrastruktuurin saatavuutta ja näin rajoittaa linkkikapasiteettia ja lisätä viivettä. Verkkosuunnittelun tavoitteet pyritään saavuttamaan sille varatun aikaikkunan sisällä ja aikataulussa pysyminen voi edellyttää yksinkertaisemman arkkitehtuurin tai tekniikan valitsemista verkolle. Verkkoa ylläpitävän henkilöstön määrä tai osaaminen voi olla rajoittava tekijä uusien teknologioiden ja monimutkaisten protokolien käyttöönotossa, mihin voidaan vaikuttaa aika- ja kustannusrajoitteiden puitteissa joko henkilöstön koulutuksella tai lisähenkilöstöllä. (Al-shawi 2015.)

### 3.6 Verkon luotettavuus, ylläpito ja saatavuus

Verkon luotettavuutta voidaan mitata vikatiheydelle ja ennakoimattomien katkosten määrällä. Luottavuuden mittareina toimivat esimerkiksi MTBF (Mean time before failure) ja MTBCF (Mean time before critical failure), joista MTBF ilmaisee keskimääräistä verkon ylhäälläoloaikaa vikatilanteiden välillä ja MTBCF vastaan samaa ottaen huomioon vain verkon kannalta kriittiset viat. (McCabe 2007.)

Verkon ylläpidettävyydellä tarkoitetaan sen kykyä palautua vikatilanteista ja sen mittarina toimii yleensä MTTR (Mean time to repair). MTTR kuvaa keskimääräistä aikaa verkon vikatilanteesta toimintakykyiseksi palautumiseen, mikä sisältää vian toteamiseen, ongelmakohdan löytämiseen ja vian korjaamiseen, kuten viallisen laitteen vaihtamiseen kuluvan ajan. (McCabe 2007.)

Saatavuudella tai käytettävyydellä verkossa tarkoitetaan verkon kykyä taata pääsy sen palveluihin ja verkkoresursseihin. Sitä voidaan kuvata verkon suunnitellun toiminta-ajan ja siihen lisätyn kaikkien mahdollisen vikatilanteiden vaatiman korjausajan suhteella (1). Verkon laskennallista saatavuutta ei laske suunnitellut huolto- ja ylläpitotoimet, jotka voidaan ajoittaa verkon käytön kannalta sopivaan kohtaan ja laitteille, joita juuri silloin ei välttämättä tarvita.

$$A = \frac{MTBF}{MTBF + MTTR} \quad (1)$$

Jossa A on verkon saatavuus.

Tyypillisesti käytettävyyttä ilmaistaan prosenttiluvulla, kuten vaikka 99,99 % tai 99,999 %, joka ilmaisee verkon toiminta-ajan osuutta vuodessa. Saatavuustason ollessa 99,999 % sallitaan verkolle noin viiden minuutin verran käyttökatkoksia vuotta kohden, mikä saavuttaminen verkolle edellyttää verkolta huomattavaa redundanssia linkkien, laitteiston ja palvelimien suhteen, ylimääräistä kapasiteettia varavirransyöttöä, valvontaa, henkilöstön koulutusta ja muita investointia. Oleellista onkin pohtia kuinka haitallisia verkon käyttökohteen kannalta katkokset ovat ja minkä mittaisina ne ovat vielä hyväksyttäviä verkossa liiketoiminnan häiriintymättä. (McCabe 2007.)

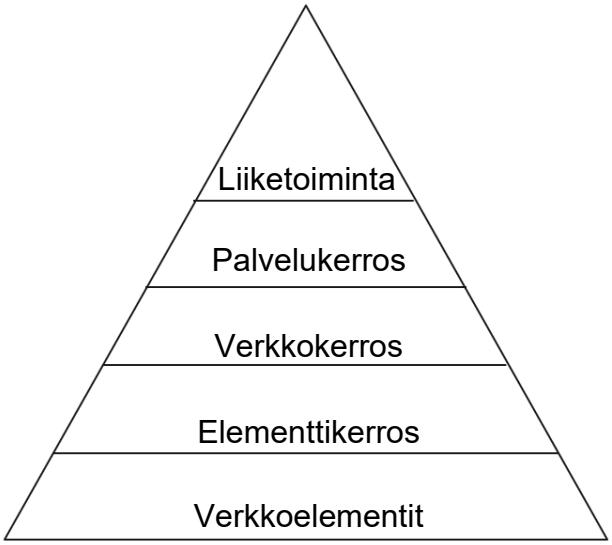
# 4 Verkkohallinnointi

Verkon pitäminen toimintakykyisenä edellyttää verkkohallinnointia. Verkkohallinnointi kattaa verkon operatiiviset päivästä päivään tapahtuvat ylläpidolliset toimenpiteet, tiedonkeruut ja järjestelmät, joilla verkko pidetään käyttäjiensä hyödynnettävä ja turvallisena. Verkkohallinnointia voidaan pitää osana verkkosuunnittelun iteratiivista prosessia. Aivan pienimmissä muutaman laitteen verkoissa verkkohallintaa voidaan hoitaa keskitetysti suoraan reitittimen komentoliittymästä, mutta vähänkään isommissa verkoissa hallinta edellyttää jonkinlaista suunnitelmallista verkkohallinnan strategiaa.

Hierarkkisissa kerroksissa tarkasteltuna verkkosuunnittelu voidaan jakaa eri osiin niiden toiminnan teknillisyyden tason ja abstraktiuden perusteella (kuvio 4), esimerkiksi tapahtuuko hallinto koottujen raporttien ja käytäntöjen perusteella vaiko yksittäisten laiteparametrien ja mittarien. Aina ylemmälle tasolle siirryttäessä edellisen tason hallinnointitiedot kootaan ja käsitellään abstraktimmassa, helpommin käsiteltävässä ja jollain tapaa rajatussa muodossa. Korkealla tasolla hallinnointi tapahtuu liiketoiminnan näkökulmasta eli budjetin ja resurssienhallinnan kautta, sekä sopimuksilla, esimerkiksi verkko-operaattorien kanssa. Palvelukerroksella hallinnoidaan verkkoa palveluna asiakkaalle ja käyttäjille, eli se vastaan verkossa asioista, kuten SLA:n palvelutason toteutumisesta, palvelunlaadusta, käyttäjänhallinnasta ja asiakasrajapinnasta. Verkonhallintakerros keskittyy kaikkien verkkoelementtien, eli verkkolaitekokonaisuuksien, hallintaa koko verkon laajuudella. Se käsittelee esimerkiksi verkkotopologiaa, reititystä, kapasiteettia ja lukuisia muita osa-alueita, jotka eivät välttämättä näy verkon käyttäjällä muuna kuin toimivana tai toimimattomana verkkona. Pohjalla elementinhallintakerroksessa hallinnoidaan yksittäisiä verkkoelementtejä, niiden asetuksia sekä tilastojen ja lokien keräystä. (ITU-T 2000.)

Kyseinen hierarkkinen malli on osa kansainvälisen televiestintäliiton (ITU) TMN-viitekehystä, jossa perusajatuksena on standardisoida arkkitehtuuri, liitännät ja protokollat erityyppisten verkkolaitteiden ja järjestelmien yhteenliittymiseksi organisoidulla tavalla (ITU-T 2000). Vaikka TMN:tä ei käyttäisikään suunnittelun tavoitteena tai kyseinen malli ei sellaisenaan sopisi

täysin suunniteltavaan verkkoon, voidaan sitä viitekehyksenä hyödyntää yhtenäisen terminologian ja verkon tasojen selkeyttämisen osalta hiukan samalla tavalla kuin OSI-malliakin.




KUVIO 4. Verkonhallinnan tasojen hierarkia. (Abeck ym. 2009, muokattu)

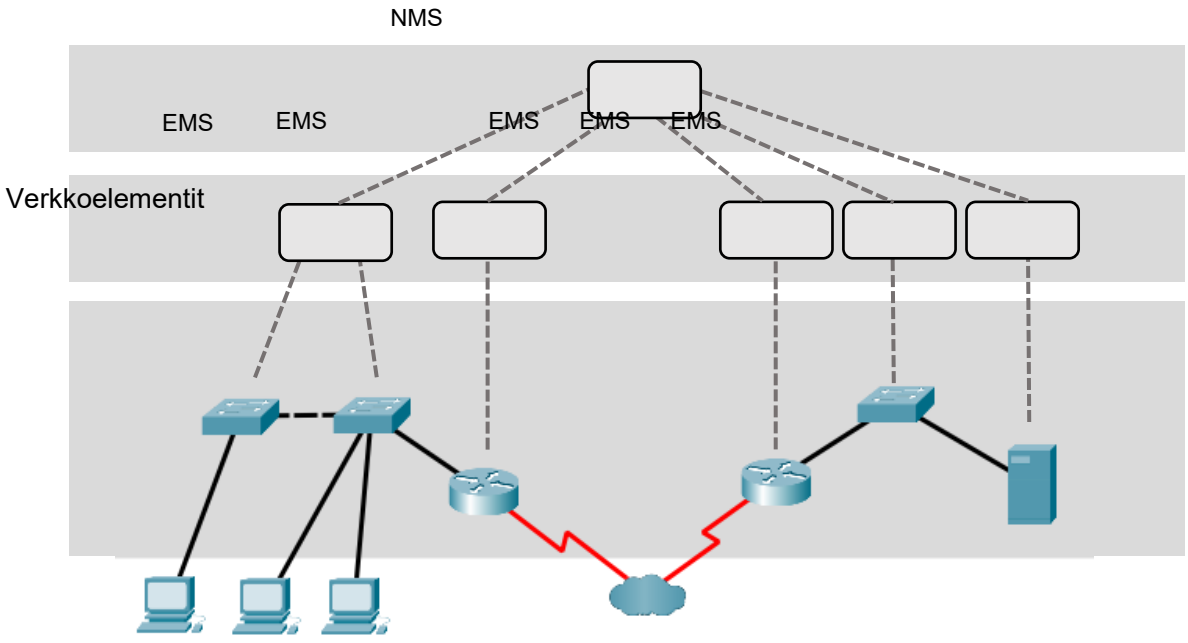
### 4.1 Hallintajärjestelmät

Verkkohallintaa toteutetaan joukolla sovelluksia ja järjestelmiä, jotka koostavat verkonhallintajärjestelmästä (NMS), elementtihallintajärjestelmistä (EMS) ja verkkoelementeistä, eli yksittäisistä hallittavista verkkolaitteista. (Abeck ym. 2009)

Elementinhallintajärjestelmät hoitavat verkossa matalantason laitteistokohtaisen hallinnoinnin, kuten laitteistokonfiguraatioiden latauksen laitekohtaisesti, eivätkä esimerkiksi seuraa laitteiden välistä liikennettä. Jokaista verkkoelementtiä hallitsee sen elementinhallintajärjestelmä, jotka tukevat tavallisesti vain tietyn laitevalmistajan yhtä tai rajattua joukkoa verkkolaitteita, mahdollisti käyttäen laitevalmistajan omia protokollia laitteiden kanssa viestimiseen. Verkon elementinhallintajärjestelmät ovat yhteydessä puolestaan niitä hallinnoivaan verkonhallintajärjestelmään tavallisia teollisuusstandardeja (SysLog, NetFlow, SNMP, ym.) käyttäen. (Mehmet, T 2015)

Verkonhallintajärjestelmä toimii verkossa pisteenä, joka toimii yhteisenä rajapintana verkon elementinhallintajärjestelmille. NMS:stä on näkyvyys koko verkkoon, ja sen kautta ohjata ja konfiguroida joka verkkoelementtiä kautta ilman tarvetta lukuisille eri ohjelmille.

Hallinta-asemia voi olla verkossa useita hajautetusti tai yksi keskitetysti (kuvio 5), jonka kautta kaikki hallintatiedot kulkevat. Keskitetyssä mallissa verkkoarkkitehtuurista muodostuu yksinkertaisempi ja edullisempi, mutta myös ruuhka-alttiimpi kaiken hallintatiedon suuntautuessa yhteen pisteeseen verkossa, eli järjestelmä ei skaalaudu isompiin verkkoihin. Hajautetussa mallissa hallintatietoliikenne jakautuu verkossa tasaisemmin ja verkon redundanssi on parempi, kun järjestelmässä ei ole yksittäistä pistettä, jonka toimintahäiriö keskeyttäisi koko palvelun. Hajautetun mallin voi toteuttaa myös hierarkkisesti, jolloin verkonhallinta-aseman toiminnot, kuten tiedon keräys, käsittely ja varastointi, eriytetään omille laitteilleen. Tarkoituksena on pyrkiä prosessoimaan osa laitteilta kerätyistä tiedoista jo ennen niiden päätymistä varastointiin tai verkon hallinnoijan tutkittaviksi, mikä oleellisesti vähentää siirrettävän tiedon määrää, sekä hallintalaitteiden keskinäistä riippuvuutta toisistaan. (Abeck ym. 2009). Verkkohallinta voidaan myös hoitaa palvelujakelumallilla (SaaS tai NMaaS), jossa pilvipalveluntarjoaja isännöi verkkohallintajärjestelmää omilla palvelimillaan ja asettaa ne loppukäyttäjien saataville internetin välityksellä.

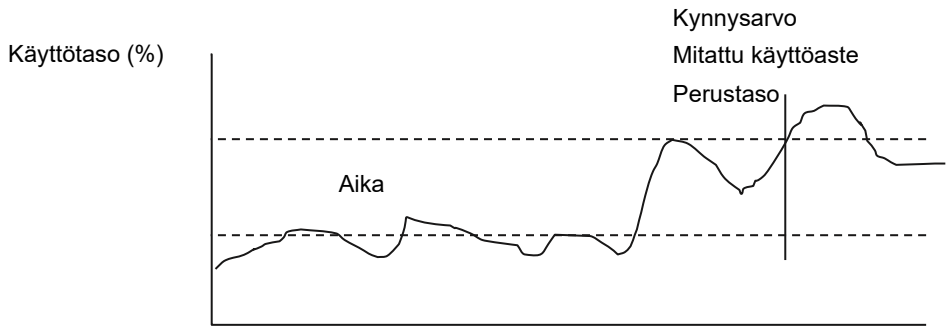



KUVIO 6. Verkkohallinnan tasojen hierarkia yhdellä keskitetyllä verkonhallintajärjestelmällä.

## 4.2 Palveluprosessit

SLA:ssa, eli palveluntasosopimuksessa, on määriteltynä toimenpiteet, joilla palvelutasoa sovituin vastuualuein pidetään yllä. Määritetyt tukitoimet sisältävät sekä reaktiivisia että ennakoivia menetelmiä, joista reaktiiviset palveluprosessit määrittävät kuinka verkkohallinnoinnissa reagoidaan verkon ongelmatilanteisiin niiden ilmettyä tyypillisesti käyttäjäpalautteen, tikettijärjestelmän tai verkkomonitoroinnin kautta. SLA:ssa voidaan määritellä kriteerit erityyppisten ongelmien vakavuustasolle, joidenka perusteella tarjotun tuen aste määräytyy. Tavoitteena on kriittisempien ongelmien nopeampi käsittelyn aloittaminen, ongelman ratkaisu ja mahdollinen eskalointi seuraavalle tukitasolle. (Service Level Management: Best Practices 2022.)

Ennakoivat palveluprosessit pyrkivät ratkaisemaan verkon ongelmat jo ennen niiden esiintymistä, mikä on tärkeää erityisesti korkeaa saatavuutta edellyttävissä verkoissa. Ennakoivat menetelmä perustuvat verkon laitteilta ja linkeistä kerättyjen tietojen analysointiin ja vertaamiseen ennalta määritettyihin, verkon poikkeustilaa indikoiviin kynnysarvot. Kynnysarvona voi toimia esimerkiksi 70 %:n reitittimen prosessorin käyttöaste, jonka arvoa mitataan minuutin välein ja jonka ylittyessä verkkohallinto saa ilmoituksen (kuvio 7). Samoin mittauksia pitkältä ajanjaksolta kerättynä voidaan käyttää trendianalyysissä ja verkon perustason (eng. baseline) määrittelyssä. (Service Level Management: Best Practices 2022)




KUVIO 8. Verkon käyttöasteen monitorointi, käyttöasteen nouseva trendi ja kynnysarvon ylitys. (McCabe. 2007, muokattu)

Verkon perustaso on analyysi verkon normaalista toiminnasta, jota voidaan kuvata tilastona verkkolaitteiden suorituskyvyn, kapasiteetin ja saatavuuden keskiarvoista tietyltä aikaväliltä. Perustaso toimii viitekohtana, kun verkkoa monitoroidaan poikkeavuuksien varalta ja määritettäessä poikkeamia indikoivia kynnysarvoja. Tämän vuoksi perustason määrittelyssä onkin tärkeää huomioida otoksen edustavuus. Jos perustaso on määritetty verkon käytön kannalta epätyypillisessä tilanteessa, kuten esimerkiksi laitevian aikana, jossa verkon palvelukapasiteetti voi näyttäytyä normaalia matalampana. Myös verkkosuunnittelun toimenpiteiden, kuten uuden teknologian käyttöönoton onnistumista voidaan seurata vertaamalla verkon tilaa muutosta edeltävään tilaan. (Service Level Management: Best Practices 2022.)

Myös itse verkkohallinnoinnin prosessit voivat olla vajavaisia tai suunniteltua hitaampia, mistä syystä niiden toimintaa ja onnistumista on myös syytä mitata. Esimerkiksi viallista verkkolaitetta vaihdettaessa uuteen voi kulua suunniteltua enemmän aikaa esimerkiksi henkilövajauksen tai jonkin tuntemattoman vuoksi, mikä laskee verkon saatavuuden tasoa vian korjausajan (MTTR) pidentyessä. (Service Level Management: Best Practices, 2022.)

### 4.3 FCAPS

Osana TMN-viitekehystä verkkohallinnoinnin päätehtävät jaetaan vikatilanteiden, konfiguraatioiden, käytön, suorituskyvyn ja turvallisuuden hallintaan, eli FCAPS-malliin. FCAPS:ia voidaan pitää jonkinlaisena suuntaa antavana mallina, joskaan sen luomishetkenä ei pilvipalvelumallit ja verkkoautomaatio olleet yhtä ajankohtaisia kuin nykyään.

FCAPS:in vikatilanteiden hallinta käsittää verkon mahdollisten häiriöiden ja toimintaa haittaavien poikkeavien tilojen tunnistamisen, paikantamisen ja korjaamisen. Jatkuvan verkkomonitoroinnin, kynnysarvoilla ja aikaisempien virhelokitietojen avulla monia virhetiloja pystytään ennenaikaisesti ehkäisemään. Vikatilanteen havaitsemisen lisäksi, ennen varsinaisten korjausten aloittamista, tarvitaan diagnoosi virheen synnystä (Clemm, A. 2007). Esimerkiksi yksinään hälytys verkon ruuhkautumisesta ei kerro vianhallinnalle ongelman juurisyytä.

Onko mahdollisesti jonkin kriittinen linkki poikki vaiko onko verkossa vain liikaa ruuhkaa? Yhdestä viasta voi vianhallinnalle tulla myös useita päällekkäisiä ilmoituksia. Verkon ongelmat voivat aiheutua ohjelmistojen ja laitteiston lisäksi myös verkon virransyötön, jäädytysjärjestelmien ja muissa verkkoa tukevista, mutta sen ulkopuolisista järjestelmistä.

Konfiguraatiohallinta ylläpitää ja käsittelee verkon laitteiden, kytkentäkaappien, kaapelien ja ohjelmien tietojen, jotka laiteparametrien lisäksi voivat kattaa laitteiden fyysiset ja loogiset sijainnit verkossa, oletusasetuksia sekä versiohallintaa ja päivityshistoriaa. Konfiguraatiohallinnassa verkon tilasta ja siihen tehdyistä muutoksista pidetään kirjaa, mikä on tärkeää vikatilanteiden selvittämisessä ja verkon muutostöissä. Verkossa, jossa halutut tiedot ovat selkeästi luettavassa muodossa saatavilla, syntyy vähemmän virheitä verkon muutosten yhteydessä, kun vaikutukset muihin verkon komponentteihin on helpommin huomioitavissa. Vikatilanteen tapahtuessa esimerkiksi ohjelmistopäivityksen yhteydessä konfiguraationhallinnasta tulisi löytyä varmuuskopiot verkon päivitystä edeltävistä, mahdollisesti toimivista, asetuksista. Verkkolaitteen rikkoutuessa toimivan konfiguraatiohallinnan verkosta löytyy vanhan verkkolaitteet laiteparametrit valmiina syötettäväksi uuteen korvaavaan laitteeseen ja näin verkon vikatilanne jää lyhyemmäksi. (Zola 2021.)

Käytönhallinta vastaa verkon resurssien jaosta verkon käyttäjien, sekä näiden palvelutasoista ja käyttöoikeuksien hallinnasta. Käytönhallintaan kuuluu myös verkkoliikenteen ja verkkoresurssien käytön monitorointi, tyypillisesti laskutuksen tueksi. (Zola 2021.)

Suorituskyvyn hallinnan vastuualueena on nimensä mukaisesti verkon suorituskyvyn seuraaminen ja tehostaminen. Suorituskyvyn seuraaminen voi tapahtua linkkien, koko verkon tai siinä toimivien sovellusten tasolla. Verkosta pyritään löytämään liikenteen ongelmakohdat, joiden korjaamisesta verkon suorituskyky parantuisi eniten. Myös suorituskyvyn seuranta perustuu jatkuvaan verkon datan keräykseen ja tilastolliseen käsittelyyn. (Zola 2021.)

Tietoturvahallinta toteuttaa yhtenäisen tietoturvapolitiikan puitteissa, joka määrittää organisaatiokohtaiset verkon turvaamisen tavoitteet ja toteutuskeinot. Verkkoon kohdistuvat turvallisuusuhat ovat monesti verkon käyttökohteesta ja sitä hyödyntävästä organisaatiosta riippuvaisia, mutta lähtökohtaisesti tietoturvaan kuuluu verkon liikenteen ja tietojen säilyminen ulkopuolisten tahojen käytön ulkopuolella, luottamuksellisina ja eheinä, mutta samalla niiden ollessa oikeiden käyttäjien hyödynnettävinä. Tietomurtojen ja haittaohjelmien lisäksi verkkoturvallisuutta voivat vaarantaa vialliset tai väärin konfiguroidut laitteet ja ohjelmat, tai henkilöstön tietoturvakoulutuksen puute. (McCabe 2007.)

Juuri kyseisen verkon kannalta oleellisimpiin turvallisuusuhkiin keskittyminen edellyttää uhka-analyysiä, jonka periaatetta on havainnollistettu kaaviossa 2. Uhka-analyysissä arvioidaan säännöllisin väliajoin erityyppisten uhkien, kuten palvelusestohyökkäysten, murtojen tai datavarkauksien todennäköisyyttä ja vaikutusta eri verkon osa-alueisiin. (McCabe 2007.)

| Vakavuus/ Todennäköisyys | Matala | Vakava | Kriittinen |
|---|---|---|---|
| Harvinainen | 1 | 2 | 3 |
| Mahdollinen | 2 | 3 | 4 |
| Todennäköinen | 3 | 4 | 5 |

KAAVIO 1. Yksinkertainen riskimatriisi uhkien mahdolliseen pisteytykseen.

| Kohde/ Uhka | Laitteisto | Palvelimet | Ohjelmistot | Tiedot |
|---|---|---|---|---|
| Luvaton pääsy | 4 | 3 | 4 | 4 |
| Palvelunesto | 3 | 3 | 3 | 2 |
| Varkaus | 2 | 2 | 2 | 3 |
| Haittaohjelmat | 2 | 2 | 3 | 2 |
| Fyysinen vahinko | 2 | 2 | 1 | 1 |

KAAVIO 2. Yksinkertaistettu esimerkki uhkanalyysimatriisista.

Uhka-analyysin perusteella voidaan määrittää miten ja minkälaisia suojauskäytäntöjä verkossa sovelletaan ja miten ne kohdistetaan verkossa. Suojauskäytännöt ovat verkon ja sen tietojen pääsyä ja käyttöä rajoittavia säädöksiä turvallisuusuhkien minimoimiseksi. Verkon loppukäyttäjällä nämä ilmenevät esimerkiksi erilaisina ohjelmien, salasanojen, etäyhteyksien ja

henkilökohtaisten laitteiden käyttöön liittyvinä säädöksinä ja ohjeistuksina. (Paquet 2013).

Verkon yli pilvessä toimivien sovellusten ja palvelujen osalta pilvipalveluiden tarjoajalla tulee olla edellytyksen edellytykset ja standardit tietojen turvalliseen käsittelyyn ja varastointiin. Tietojen salauksen ja käyttörajoitusten merkitys korostuu, kun asiakkaalla ei välttämättä ole näkyvyyttä tai tarkkaa tietoa pilven toiminnasta.

# 5 Monitorointi

Toimivan verkkohallinnan edellytyksenä on jatkuva verkon monitorointi ja tiedon keruu verkon laitteista ja linkeistä. Verkon monitorointi on oleellisena osana monia eri verkonhallinnan osa-alueita ja SLA:n toteutumisen seurannassa. Verkkomonitoroinnilla tarkoittaa verkon ongelmakohtien havaitsemista ja palvelutason parametrien seurantaa, sekä kerätyn tiedon käsittelyä ja arkistointia. (McCabe 2007.)

## 5.1 Passiiviset ja aktiiviset menetelmät

Verkon liikennettä voidaan mitata joko passiivisin tai aktiivisin menetelmin. Verkon tilasta parhaiten saa tietoa passiiviset ja aktiivisten menetelmien yhtäaikaisella käytöllä. Passiivisilla mittausmenetelmillä kerätään valitusta pisteistä, kuten verkkolaitteen SPAN-portista, TAP-laitteesta ja kopioidaan verkkoliikennettä tai tilastotietoa siitä. Passiiviset menetelmät eivät itse tuota verkkoon liikennettä ja ovat luvattomassa käytössä hankala havaita. Passiivisia monitorointia menetelmiä ovat muun muassa erilaiset pakettianalysaattorit.

Aktiiviset mittausjärjestelmät puolestaan lähettävät verkkoon omia, todellista liikennettä emuloivia testipakettejaan, joiden liikkeistä, viiveestä, katoamisesta ja muusta toiminnasta voidaan tehdä koko verkkoa koskevia päätelmiä. Aktiivisin verkonmonitorointimenetelmin verkosta saadaan lähes reaaliaikaista tietoa ilman todellisten käyttäjien liikenteen keräämistä, mistä on hyötyä verkkoresurssien saatavuuden ja vasteaikojen mittaamisessa ennen kuin verkon käyttäjä edes huomaa mahdollista ongelmaa. Kun menetelmä ei ole verkon muusta liikenteestä riippuvainen, voidaan sitä käyttää jatkuvaan mittauksien tekemiseen automatisoidusti myös silloinkin, kun todellista liikennettä verkossa ei ole. Esimerkiksi ping on aktiivisen monitoroinnin työkalu, jossa mitataan toiselle verkkoelementille lähetetyn ICMP:n echo request-paketiin vastaamiseen kuluvaa aikaa. (Clemm 2007.)

## 5.2 Työkalut

Monitorointiin on olemassa lukuisia eri tarkoituksiin soveltuvia työkaluja. Verkkoliikenteestä tiedonkeruu tapahtuu pakettianalysaattoreilla, kuten Wiresharkilla. Niitä käytetään tarkastelemaan ja analysoimaan verkon sen hetkistä liikennettä tarkoituksena ymmärtämään verkon toimintaa ja diagnosoimaan tiettyjä ongelmia. Pakettianalysaattorit kaappaavat ja tarpeen tullen purkavat paketteja, jotka kulkevat verkkolaitteen, kuten reitittimen tai kytkimen, portin yli ja esittävät ne luettavassa muodossa. (Clemm 2007.)

Verkkoliikenteen reittien, määrien, lähtö- ja pääpisteiden, eli verkkoelementtien muodostamien yhteyksien seuraamiseen ja analysointiin on kehitytty omat erikoistuneet protokollansa, kuten NetFlow tai IPFIX. Yhteyksien, eli tietystä osoitteesta ja portista tiettyyn kohteeseen suuntautuvien pakettivirtojen, seuranta on käyttäjäkohtaisesti tärkeää varsinkin silloin, kun verkon käytöstä laskutetaan käytön mukaan. Aktiivisella liikennevirtojen seuraamisella voidaan myös tunnistaa verkon ruuhkautumispisteet ja pullonkaulat, sekä tunnistaa mitkä protokollat ja sovellukset vievät eniten kapasiteettiä tietyillä linkeillä. (Clemm 2007.)

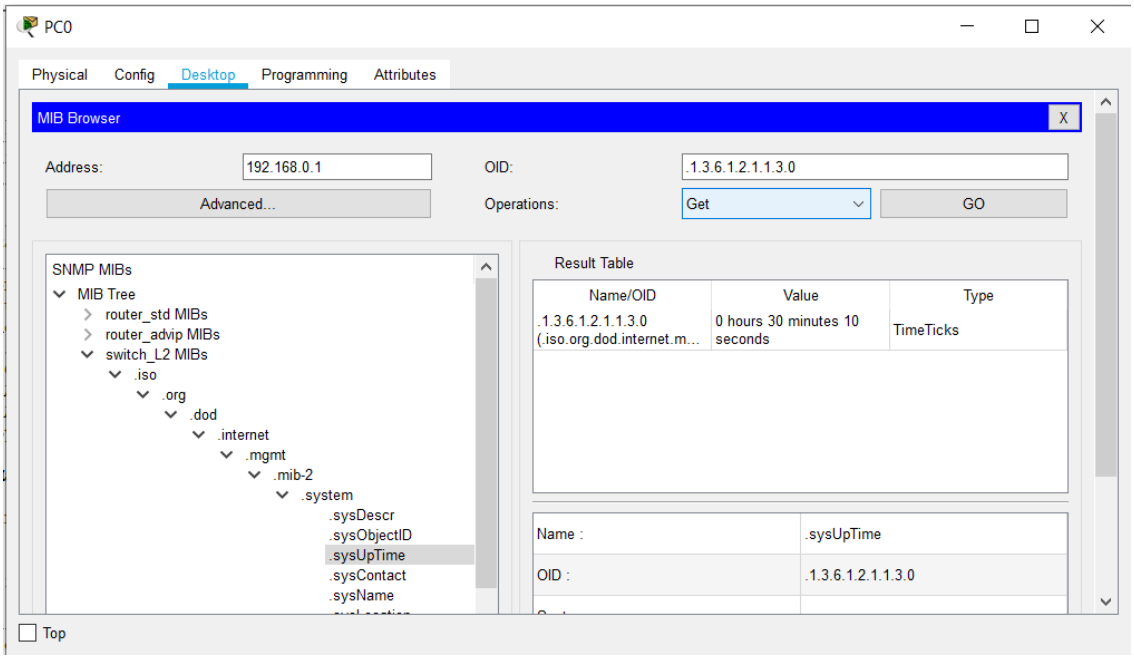
Yksittäisistä verkkolaitteista itsestään voidaan kerätä tietoa suoraan niiden komentoliittymistä (CLI) tai esimerkiksi standardisoiduilla syslog-protokollalla ja SNMP:llä (simple network management protocol). Useammasta verkkoelementistä tiedon yhtäaikaiseen keräämiseen on olemassa lukuisia eri valmistajien julkisia ja kaupallisia verkonmonitorointijärjestelmiä, jotka yleensä hyödyntävät SNMP- ja muita protokollia toiminnassaan.

### 5.2.1 SNMP

SNMP on yksinkertainen, varsin laajassa käytössä oleva, matalilla muisti- ja prosessointivaatimuksilla toimiva verkonhallintaprotokolla. SNMP-hallinnoitu verkko koostuu hallinta-asemasta ja hallinnoitavista SNMP:tä tukevista verkkolaitteista. Hallinnoitavissa laitteissa toimii SNMP-agenttiohjelma, joka vastaa hallinta-aseman tiedonkeruupyyntöihin, kerää hallittavalta laitteelta tiedot

ja lähettää ne SNMP-yhteensopivassa muodossa (kuvio 7). Hallinta-asema voi myös muokata hallinnoitujen laitteiden arvoja, sekä asettaa näille ehtoja, joiden perusteella hallinta-asema saa tietoa poikkeavista tilanteista. Hallittavat laitteet voivat olla mitä vain SNMP:tä tukevia verkon laitteita, kuten printtereitä, palvelimia, tietokoneita tai IOT-laitteita. (McCabe 2007).

SNMP:n kautta käytettävissä olevat parametrit on ryhmitelty hallintatietokantoihin eli MIB:ihin, joista löytyy laitteen toimintaa säätelevät parametrit ja agenttiohjelman laitteesta keräämä tieto. Haluttu parametri löytyy tietokannasta joka parametrin yksilöivän osoitetunnisteen, eli OID:n avulla. Jokainen SNMP:tä tukeva laite ylläpitää yleistä hallintatietokantaa, kuten MIB-II:tä, joka sisältää yleisimpiä ja joka laitteen kannalta oleellisia parametreja, kuten esimerkiksi laitteen IP-osoitetietoja tai verkkoliittimien määrän. Eri valmistajien laitteilla löytyy tavallisesti myös näiden omat yrityskohtaiset hallintatietokantaansa.




KUVIO 9. Cisco Systemsin Packet Tracer -verkkosimulaattorissa luotu SNMP-protokollan GET-viesti ja vastaus siihen. Vasemmalla näkyvissä valitun MIB:n hierarkkinen rakenne ja oikealla ylhäällä käytetty OID, joka kuvion tilanteessa viittaa laitteen käynnissäoloaikaan.

# 6 Pohdinta

Opinnäytetyön aihe verkkosuunnittelun periaatteista on valtavan laaja aihe, jonka yksityiskohtainen tarkastelu ilman oleellisien osien poisjättämistä nykyisellä laajuudellaan ei helposti onnistuisi. Tarkoituksena kumminkin oli enemmänkin havainnollistaa kokonaiskuvaa verkkosuunnittelun pidemmän aikavälin periaatteista takertumatta liikaa juuri tämän hetken teknologioihin tietoverkkojen maailmassa, missä muutos tavallisesti nopeaa ja uusia teknologioita otetaan käyttöön ja vanhoja hylätään jatkuvaa tahtia.

Lähdemateriaaleissa mainituista teknologioista osa ei enää alkuperäisessä muodossaan ole relevantteja verkkosuunnittelun kannalta, sen sijaan iso suunnittelun periaatteista, kuten skaalautuvuuden ja hallinnan hierarkiat tuntuvat pätevät yhä verkoissa. Iso osa työskentelystä kohdistuikin lähdemateriaalin ajankohtaisuuden arviointiin ja sisällön rajaukseen. Suurin osa käytetystä lähdemateriaalista on tietoliikenneyritysten osittain markkinalähtöisin perustein tuottamaa, joka voi vaikuttaa opinnäytetyön sisältöön, joskin vaikutusta pyrittiin tietoisesti välttämään.

Opinnäytetyön hyöty ilmeni lähinnä oppimiskokemuksena aihepiiristä, jota tutkinto-ohjelmassa on käsitelty enemmän teknisellä tasolla painottaen protokollien ja verkkolaitteiden konfigurointien. Aiheen jäsennyksen myötä moni asia on verkkosuunnittelussa huomattavasti selkeämpää, mistä on varmasti hyötyä verkkojen kanssa jatkossa työskennellessä.

**Lähteet**


Panko, Raymond R. 2009. *Business data networks and telecommunications*. Pearson Education International

McCabe, James D. 2007. Network Analysis, Architecture, and Design. Burlington: Morgan Kaufmann Publishers

Fox, R. Hao, W. 2018. Internet Infrastructure - Networking, Web Services, and Cloud Computing. CRC Press

Cisco Annual Internet Report (2018–2023) White Paper. Cisco. Viitattu 30.8.2021. www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Network Topology Diagrams: Enterprise Networking, Security, and Automation. n.d. Cisco. Viitattu 15.6.2022. https://contenthub.netacad.com/ensa/12.1.2

Service Level Management: Best Practices White Paper. 2005. Cisco. Viitattu 10.3.2022. www.cisco.com/c/en/us/support/docs/availability/high-availability/15117-sla.html

Paquet, Catherine. 2013. Network Security Concepts and Policies. Cisco Press. Viitattu 10.3.2022. https://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3

Al-shawi, Marwan. CCDE Study Guide. Cisco Press. Viitattu 5.2.2022. https://community.cisco.com/legacyfs/online/ccde_9781587144615_chapter1.pdf

Zola, Andrew. 2021. FCAPS (fault, configuration, accounting, performance and security). Viitattu 5.2.2022. https://www.techtarget.com/searchnetworking/definition/FCAPS

Moozakis, Chuck. 2018. Network management system. Viitattu 15.3.2022. https://www.techtarget.com/searchnetworking/definition/network-management-system

Abeck, S., Bryskin, I., Evans, J., Farrel, A., Filsfils, C., Hegering, H., McCabe, J., Morrow, M., Nadeau, T., Neumair, B., Ramaswami, R., Sivarajan, K., Strassner, J. & Vijayananda, K. 2009. Network Management Know It All. Burlington: Morgan Kaufmann Publishers

Mehmet, T. (toim.) 2015. Cable networks, services, and management. Hoboken: John Wiley & Sons, Inc

Graziani, R. 2014. Connecting Networks Companion Guide. Indianapolis: Cisco Press

Clemm, A. 2007. Network Management Fundamentals. Indianapolis: Cisco Press

M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic, S. Krco. 2014. Traffic models for machine-to-machine (M2M) communications: types and applications. Viitattu 15.3.2022. https://www.eurecom.fr/en/publication/4265

ITU Telecommunication Standardization Sector (ITU-T). Principles for a telecommunications management network (M.3010). 2000. Viitattu 15.3.2022. https://www.itu.int/rec/T-REC-M.3010

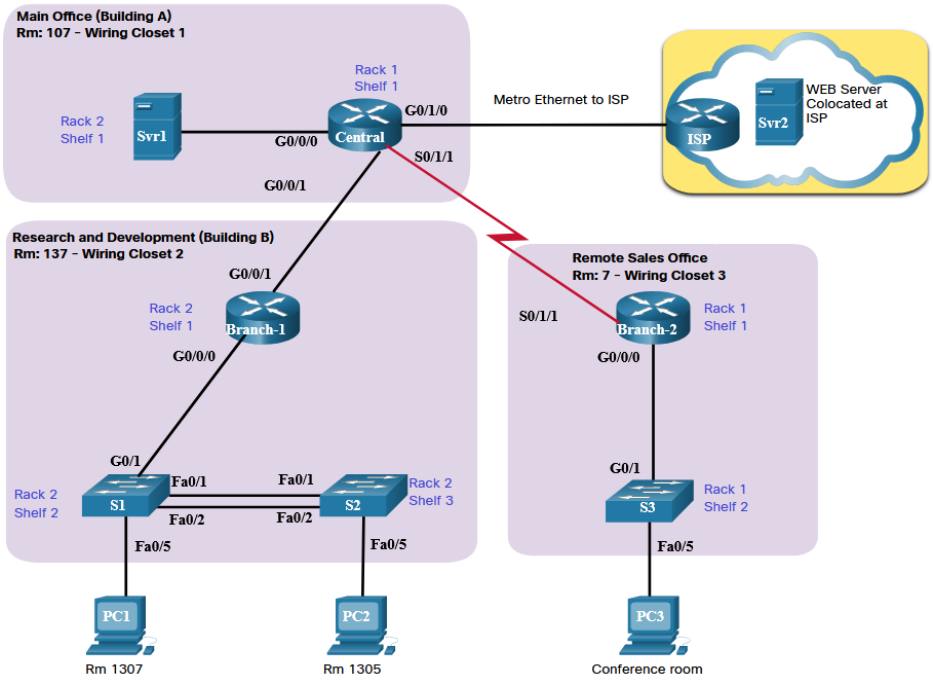
IsecT Ltd. ISO 27033 Tietoturvastandardin kuvaus. Viitattu 14.8.2021. https://www.iso27001security.com/html/27033.html

IsecT Ltd. ISO 27040 Tietoturvastandardin kuvaus. Viitattu 14.8.2021. https://www.iso27001security.com/html/27040.html

Sheldon, D. & Younger, R. 2020. Comparing Two-Tier and Three-Tier Data Center Networks. World Wide Technology. Viitattu 14.12.2021. www.wwt.com/article/comparing-two-tier-three-tier-data-center-networks#two-tier-data-center-networks

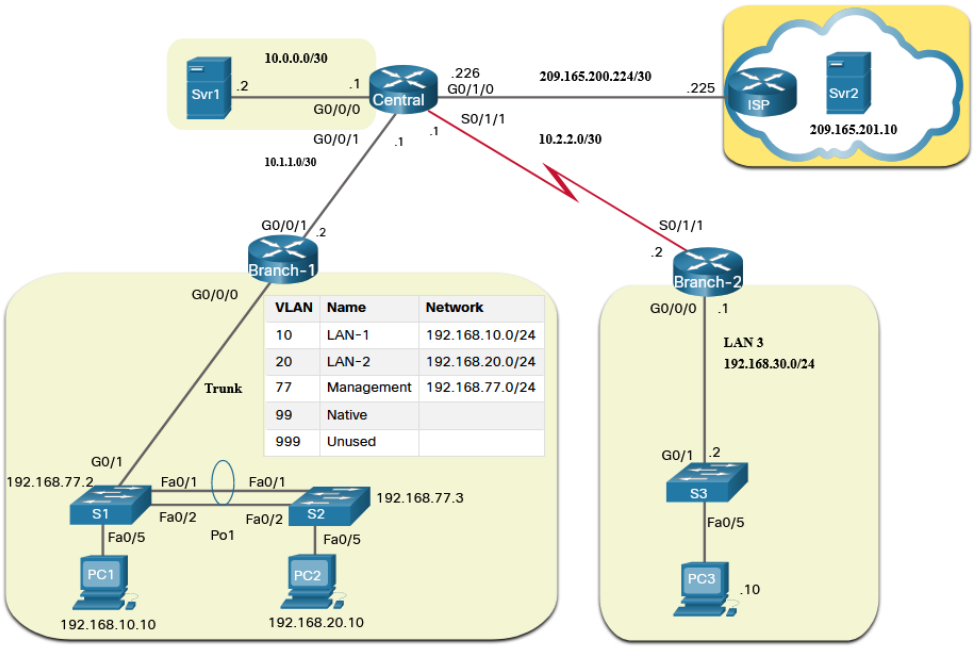
## Liitteet

Liite 1. Fyysinen topologia




LIITE 1. Fyysisessä topologiakuvassa on näkyvissä esimerkiksi verkkolaitteiden nimet, fyysiset sijainnit ja portit. (Network Topology Diagrams n.d.)

Liite 2. Looginen topologia




LIITE 2. Loogisessa topologiakuvassa on nähtävissä esimerkiksi verkkolaitteiden tunnisteet, IP-osoitteet ja virtuaalilähiverkot. (Network Topology Diagrams n.d.)