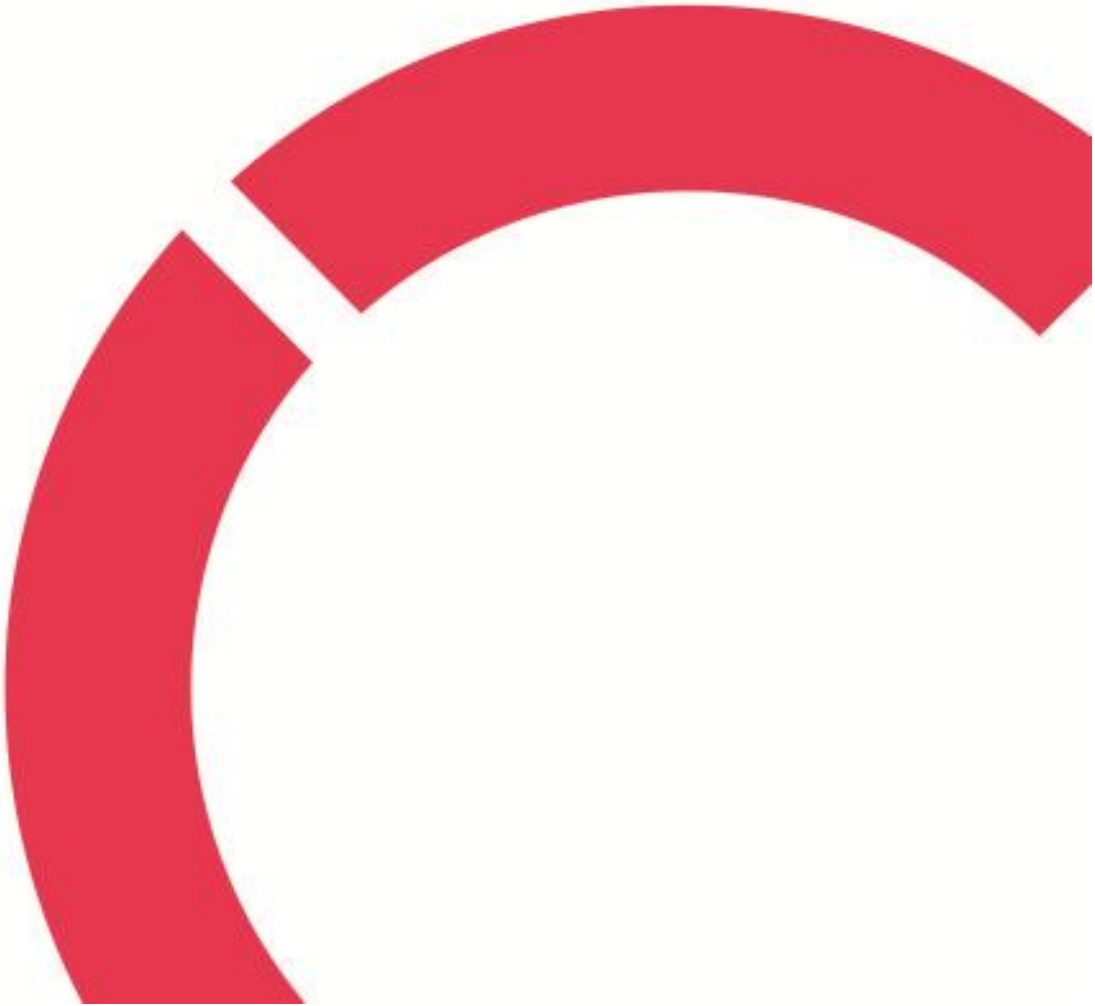
Joni Pesola

VERKON KYTKIMET

L-2 ja L-3 kerrosten kytkimet ja niiden päivittäminen

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikka
Huhtikuu 2025



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Maaliskuu 2025	**Tekijä/tekijät** Joni Pesola
Koulutus Insinööri, Tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi VERKON KYTKIMET L-2 ja L-3 kerrosten kytkimet ja niiden päivittäminen		
Työn ohjaaja Kyösti Marjakangas		**Sivumäärä** 34 + 2

Tämä opinnäytetyö käsittelee verkkokytkimiä keskittyen erityisesti L2- ja L3-kerroksen kytkimiin sekä niiden eroihin ja käyttötarkoituksiin. Työssä tarkastellaan myös kytkinten ohjelmistopäivitysten merkitystä, päivitysprosessia ja siihen liittyviä haasteita.

L2-kytkimet toimivat OSI-mallin datalinkkikerroksella, halliten liikennettä MAC-osoitteiden perusteella, kun taas L3-kytkimet toimivat verkkokerroksella mahdollistaen IP-reitityksen eri verkkojen välillä. Näiden kytkinten ominaisuuksien ymmärtäminen on tärkeää, jotta osataan valita oikeanlainen laite kuhunkin verkkoympäristöön.

Ohjelmistopäivitykset ovat kriittinen osa verkkolaitteiden elinkaaren hallintaa. Päivityksillä parannetaan tietoturvaa, suorituskykyä ja yhteensopivuutta uusien teknologioiden kanssa. Työssä perehdytään erityisesti Cisco 3650- ja 3850-kytkimien päivitysprosesseihin, joissa korostuvat huolellinen valmistelu, varmuuskopiointi ja oikeiden työkalujen käyttö.

Johtopäätöksissä painotetaan ohjelmistopäivitysten merkitystä verkkoympäristön luotettavuuden ja turvallisuuden kannalta. Suosituksina esitetään säännöllistä, mutta harkittua päivittämistä sekä automaattisten päivitysjärjestelmien hyödyntämistä tulevaisuudessa.

Asiasanat
Datalink-kerros, OSI-malli, SSH, USB

ABSTRACT

Centria University of Applied Sciences	Date March 2025	Author Joni Pesola
Degree programme Bachelor of Engineering, Information and Communications Technology		
Name of thesis NETWORK SWITCHES L-2 and L-3 floor switches and their upgrades		
Centria supervisor Kyösti Marjakangas		**Pages** 34 + 2

This thesis focuses on network switches, with a particular emphasis on Layer 2 (L2) and Layer 3 (L3) switches, their differences, and their intended use cases. In addition, the work examines the importance of software updates for switches, the update process itself, and the challenges.

L2 switches operate at the Data Link layer of the OSI model, managing traffic based on MAC addresses. L3 switches, on the other hand, operate at the Network layer, enabling IP routing between different networks. Understanding the functionality and differences of these switches is essential when selecting the appropriate device for a particular network environment.

Software updates are a critical part of the lifecycle management of network devices. Updates improve security, performance, and compatibility with new technologies. This thesis specifically focuses on the update processes of Cisco 3650 and 3850 series switches, highlighting the importance of careful preparation, backups, and the use of correct tools.

The conclusion emphasizes the significance of software updates in ensuring network reliability and security. As recommendations, the thesis suggests regular but well-considered updates, as well as the increased use of automated update systems in the future.

Key words
Datalink layer, OSI-model, SSH, USB

KÄSITTEIDEN MÄÄRITTELY

ACL

ACL (Access Control List) on tietoturvasääntöjen joukko, joka määrittää, mitä liikennettä sallitaan tai estetään verkossa, parantaen näin verkon turvallisuutta ja hallintaa

DATALINK-KERROS

OSI-mallin Datalink-kerros on toinen kerros, joka vastaa fyysisen kerroksen ja verkkokerroksen välistä tiedonsiirtoa. Se käsittelee MAC-osoitteita ja hallitsee liikenteen ohjausta paikallisessa verkossa (LAN).

EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) on dynaaminen reititysprotokolla, joka optimoi reitit verkossa yhdistämällä reititys- ja etäisyysvektoreiden periaatteet, ja se mukautuu verkon muutoksiin nopeasti.

KERROS KYTKIN

Kerroskytkin (Layer 2 switch) on verkkolaite, joka toimii OSI-mallin Datalink-kerroksella. Se pystyy lukemaan ja ohjaamaan liikennettä MAC-osoitteiden perusteella, mikä tekee siitä tehokkaan ja nopean liikenteen reitittämiseen samassa paikallisessa verkossa (LAN).

NETWORK-KERROS

OSI-mallin Network-kerros on kolmas kerros, joka huolehtii verkkoliikenteen reitittämisestä ja ohjaamisesta. Se käyttää IP-osoitteita ja auttaa pääsemään verkkoon toisista verkoista.

OHJELMISTOPÄIVITYS

Ohjelmistopäivitys viittaa verkkolaitteen, kuten kytkimen, käyttöjärjestelmän tai ohjelmiston päivittämiseen uudempaan versioon. Tällaiset päivitykset voivat sisältää turvallisuuspäivityksiä, suorituskyvyn parannuksia tai uusia ominaisuuksia.

OSI-MALLI

OSI-malli on viitekehys, joka jakaa verkkoprotokollat seitsemään eri kerrokseen. Malli auttaa ymmärtämään, miten erilaiset verkkolaitteet ja protokollat toimivat yhdessä.

OSPF

OSPF (Open Shortest Path First) on reitityksprotokolla, joka löytää verkon tehokkaimmat reitit ja mukautuu verkon muutoksiin.

SSH

SSH on salaustekniikkaa hyödyntävä protokolla, jota käytetään etäyhteyksien luomiseen ja turvalliseen etähallintaan verkkolaitteissa, mukaan lukien CISCO-kytkimissä.

VPN

VPN (Virtual Private Network) on teknologia, joka luo suojatun ja salatun yhteyden julkisen internetin kautta. Sen avulla käyttäjät voivat liittää laitteensa turvallisesti etäverkkoon, piilottaen samalla IP-osoitteensa ja sijaintinsa, mikä parantaa yksityisyyttä ja tietoturvaa.

.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVIOT

KUVAT

1 JOHDANTO

Tietoverkot ovat nykypäivän yritysten ja organisaatioiden selkäranka. Kaikki liiketoiminnasta viestintään ja tiedonhallintaan perustuu verkkoyhteyksien toimivuuteen. Kun verkko toimii hyvin, sitä tuskin edes huomaa, mutta heti kun ongelmia ilmenee, ne voivat häiritä koko työyhteisön toimintaa. Viime vuosina verkkojen merkitys on kasvanut entisestään muun muassa etätyön yleistymisen ja pilvipalveluiden lisääntymisen vuoksi. Esimerkiksi pandemian jälkeen hybridityömallit ovat vakiintuneet ja pilvipohjaiset työkalut tukevat joustavaa työntekoa (Tieturi 2024).

Samalla myös tietoturvauhat ovat lisääntyneet ja hyökkäykset verkkoinfrastruktuuriin ovat yhä yleisempiä. Suomessa on havaittu yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa (Kyberturvallisuuskeskus 2024). Erityisesti palvelunestohyökkäykset ja tietojenkalasteluyritykset ovat yleistyneet, mikä on pakottanut organisaatiot panostamaan tietoturvatoimenpiteisiin entistä enemmän. Siksi yritysten on panostettava paitsi verkkojensa luotettavuuteen, myös niiden turvallisuuteen.

Verkkojen toimintavarmuudessa keskeisessä roolissa ovat verkkolaitteet, erityisesti kytkimet, jotka hallitsevat tiedonsiirtoa eri laitteiden välillä. Ilman kytkimiä tietokoneet, palvelimet ja muut verkkoon liitetyt laitteet eivät voisi vaihtaa tietoa keskenään tehokkaasti. Kytkimet ohjaavat liikennettä ja varmistavat, että tieto päätyy oikeaan paikkaan ilman tarpeettomia viiveitä tai tietoturvariskejä. Jotta ne toimivat luotettavasti, niiden ohjelmistoja on päivitettävä säännöllisesti, aivan kuten tietokoneiden ja älypuhelinten käyttöjärjestelmiä (Kuntaliitto 2024a, 2024b).

Tässä opinnäytetyössä tarkastellaan verkkokytkimien ohjelmistopäivityksiä ja niiden merkitystä. Ohjelmistopäivitykset eivät ole vain tapa lisätä uusia ominaisuuksia, vaan ne ovat keskeinen osa verkon tietoturvaa ja suorituskykyä. Päivittämättömät laitteet voivat olla alttiita tietoturva-aukoille, joita hyökkääjät voivat hyödyntää. Esimerkiksi tutkimusten mukaan 60 % tietoturvaloukkauksista johtuu haavoittuvuuksista, jotka olisi voitu estää ohjelmistopäivityksillä (Verizon 2023). Lisäksi vanhentuneet ohjelmistot voivat heikentää verkon suorituskykyä, aiheuttaa yhteensopivuusongelmia ja pahimmassa tapauksessa estää uusimpien verkkoteknologioiden käyttöönoton.

Verkkoympäristöissä käytetään erityyppisiä kytkimiä, joilla on omat roolinsa. Yksinkertaisimmillaan kytkimet siirtävät tietoa laitteiden välillä paikallisessa verkossa, kuten toimiston sisällä, ja ne käyttävät

tähän laitteiden yksilöllisiä tunnisteita. Kehittyneemmät kytkimet voivat hallita myös laajempia verkkoja, ohjata tietoliikennettä eri verkkoalueiden välillä ja jopa tehdä päätöksiä siitä, miten data kulkee tehokkaimmin. Tämä tekee niistä lähes reitittimen kaltaisia, jotka yhdistävät eri verkkoja toisiinsa (Kyberturvallisuuskeskus 2024).

Kun verkkoympäristöt monimutkaistuvat, myös päivitysprosesseista tulee monimutkaisempia. Erityisesti suurissa organisaatioissa ohjelmistopäivitykset voivat vaatia huolellista testausprosessia ennen käyttöönottoa, jotta mahdolliset häiriöt voidaan minimoida.

Tässä työssä keskitytään erityisesti siihen, miten kytkimien ohjelmistopäivitykset voidaan suorittaa turvallisesti ja tehokkaasti. Yksi yleisimmistä ja turvallisimmista tavoista on päivittää laite paikallisesti USB-muistitikun avulla. Tämä menetelmä on varma, koska se ei vaadi verkkoyhteyttä, jolloin riski ulkopuolisista häiriöistä tai tietoturvauhista on pieni. Kaikissa tilanteissa USB-päivitys ei kuitenkaan ole mahdollinen, sillä verkkolaitteet voivat sijaita fyysisesti eri paikoissa – jopa eri maissa. Tällöin etäpäivitys on ainoa vaihtoehto, ja siinä on omat turvallisuushaasteensa (Verizon 2023).

Ohjelmistopäivitysten onnistuminen ei ole pelkästään tekninen kysymys, vaan se vaatii myös huolellista suunnittelua ja valmistelua. Ennen päivityksen suorittamista on varmistettava, että uusi ohjelmistoversio on yhteensopiva verkon muiden laitteiden kanssa ja että päivitysprosessi ei aiheuta tarpeettomia katkoksia. Lisäksi on tärkeää ottaa varmuuskopiot, jotta mahdollisten ongelmien sattuessa laitteet voidaan palauttaa aiempaan toimintakuntoon.

Jotta kytkimien ohjelmistopäivitysten merkitys ja haasteet ymmärretään paremmin, on ensin tarkasteltava, millaisia verkkolaitteita verkossa käytetään ja miten ne eroavat toisistaan. Seuraavassa luvussa käydään läpi verkkokytkimien perusperiaatteet ja niiden rooli nykyaikaisissa tietoverkoissa.

2 KYTKIMET YLEISESTI

Jotta voimme hahmottaa, miten kytkimien ohjelmistopäivityksiä tulisi hallita, on ensin ymmärrettävä, millaisia laitteita ne ovat ja miten niiden tekniset ominaisuudet eroavat toisistaan. Tästä syystä seuraavaksi tarkastellaan L2- ja L3-kerroksen kytkimiä, joiden ymmärtäminen on edellytys oikeanlaisten päivityskäytäntöjen suunnittelulle. Verkkoympäristöjen sujuva toiminta nojaa olennaisesti kytkimiin. Ne vastaavat tietoliikenteen ohjauksesta ja hallinnasta verkossa toimien kuin liikenteenvalvojat, jotka varmistavat, että datapaketit kulkevat oikeiden laitteiden välillä. Kytkimet voivat toimia eri OSI-mallin tasoilla, kuten L2-kerroksella tai L3-kerroksella, riippuen niiden ominaisuuksista ja siitä, mitä tarpeita verkossa on.

Kytkimet ovat avainasemassa erilaisissa verkkoinfrastruktuureissa, olipa kyseessä sitten kotiverkot, yritysten sisäiset verkot, palvelinkeskukset tai internetin runkoverkot. Ne takaavat tietoliikenteen sujuvuuden tehokkuudellaan, nopeudellaan ja luotettavuudellaan, varmistaen, että tiedot päätyvät oikeaan paikkaan oikeaan aikaan. (Kuntaliitto 2024.)

Modernit kytkimet on varustettu myös edistyneillä turvallisuusominaisuuksilla ja hallintamahdollisuuksilla, mikä tekee niistä erittäin soveltuvia monenlaisiin verkkoympäristöihin (Kyberturvallisuuskeskus 2024). Esimerkiksi suojaamattomat tai päivittämättömät kytkimet voivat altistaa rakennusautomaation järjestelmät tietoturvauhkille, mikä korostaa niiden keskeistä roolia verkon suojauksessa (Kyberturvallisuuskeskus 2024).

Kytkimet muodostavat nykyisen tietoverkkoteknologian kulmakiven, mahdollistamalla tiedonsiirron eri verkkojen välillä. Lisäksi ne ovat keskeisessä asemassa varmistamassa kriittisten verkkojen toimintaa, sillä valokuitu- ja kaapeliverkkojen reitittimet, kytkimet, keskittimet ja vahvistimet pystyvät ylläpitämään verkkoyhteyksiä jopa kolme tuntia sähkökatkoksen aikana (Kuntaliitto 2024). Katsotaan seuraavaksi tarkemmin L2-kytkimiä. Kuvassa 1 esimerkki ciscon kytkimestä.

KUVA 1. Cisco Catalyst 2960X-24TS-L 24-porttinen kytkin (Cisco)

2.1 L2-kytkin

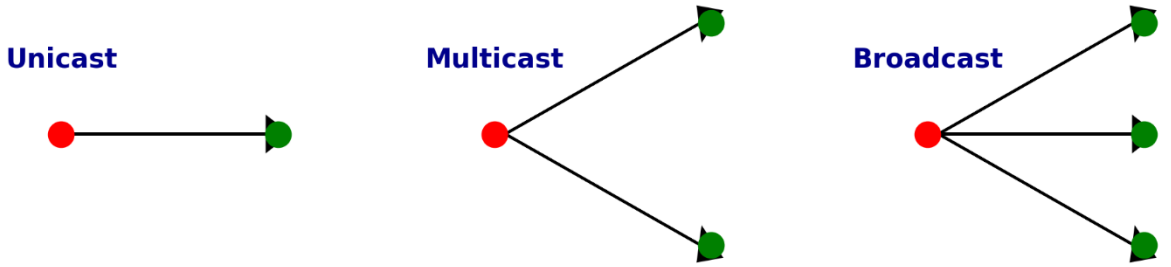
L2-kerroksen kytkin on verkkolaite, joka toimii verkkokerroksen tasolla 2 OSI-mallissa. Sen pääasiallinen tehtävä on ohjata tietoliikennettä fyysisessä kerroksessa MAC-osoitteiden avulla. L2-kytkin on erityisen hyödyllinen paikallisissa verkoissa, kuten LAN-verkoissa, joissa nopea ja tehokas liikenteen ohjaus on välttämätöntä. Tässä on joitain L2-kerroksen kytkimen tärkeitä ominaisuuksia.

L2-kytkimessä on MAC-taulu, joka pitää kirjaa siitä, millä portilla mikäkin laite sijaitsee. Tämä taulu auttaa kytkintä ohjaamaan liikennettä oikeaan suuntaan ja vähentää liikenteen tarpeetonta leviämistä verkkoon. (Cisco Networking Academy 2020, 5.1.1.4.)

L2-kytkimet tukevat Virtual LAN (VLAN) -teknologiaa. VLAN:t mahdollistavat verkon segmentoinnin, jotta voidaan luoda useita virtuaalisia verkkoja yhdelle fyysiselle kytkimelle. Tämä auttaa verkon hallinnassa ja turvallisuudessa.

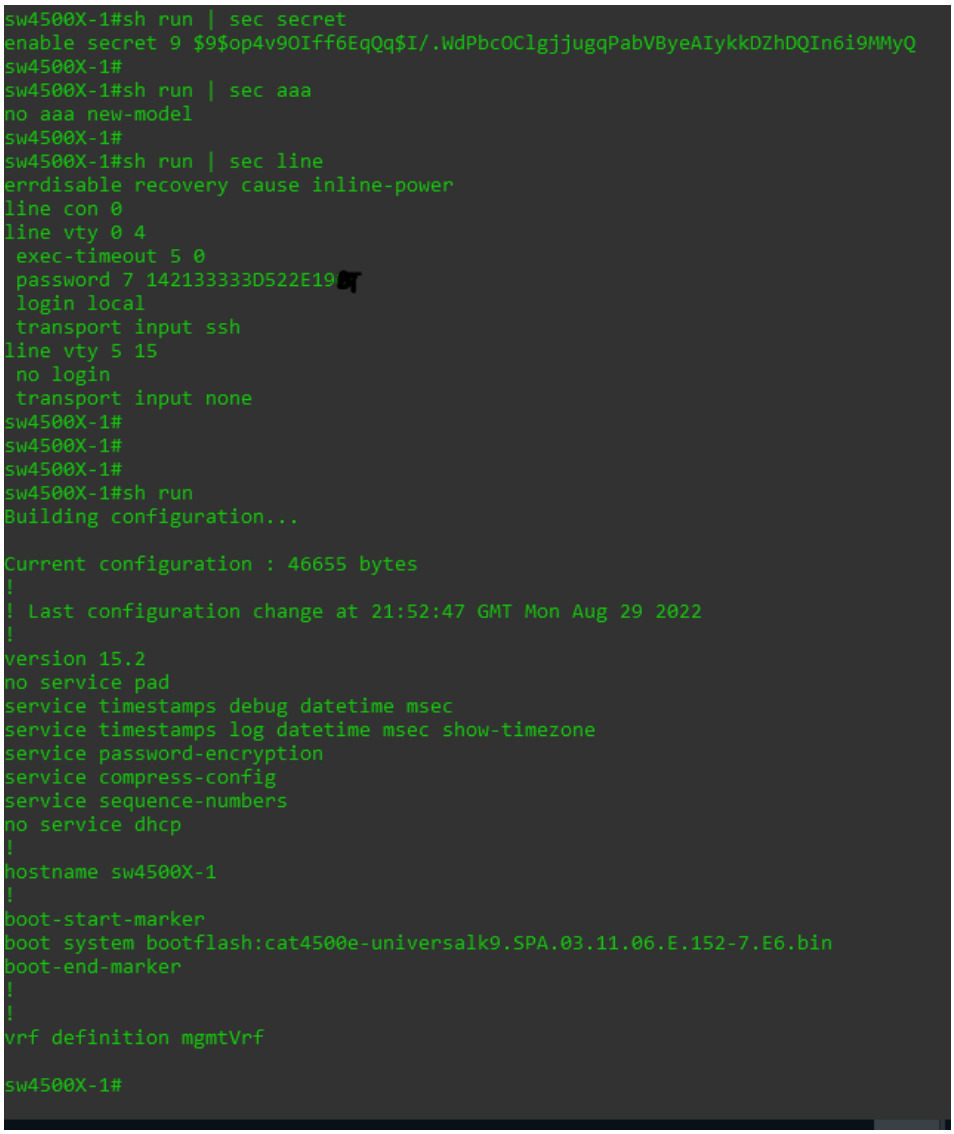
L2-kytkimet ovat yleensä helppoja asentaa ja käyttää. Ne tunnistavat automaattisesti laitteet, jotka on liitetty niihin ja ohjaavat liikenteen oikein ilman monimutkaista konfigurointia.

L2-kytkimet käsittelevät broadcast- ja multicast-liikennettä tehokkaasti. Ne vähentävät näiden tyyppisten tiedonsiirtojen tarpeetonta leviämistä koko verkkoon. Kuviossa 2 havainne näistä liikenteistä.



KUVIO 1. Unicast,Multicast,Broadcast liikenteen havainnekuva (Mukaillen: Castr)

L2-kerroksen kytkimet ovat olennainen osa paikallisia verkkoja ja tarjoavat tehokkaan tavan hallita ja optimoida liikennettä näissä ympäristöissä. Ne sopivat erinomaisesti tilanteisiin, joissa verkon laitteet toimivat samassa fyysisessä verkossa. Liityntäverkon kytkimillä on tärkeä rooli nykyaikaisessa verkkoinfrastruktuurissa, sillä niiden tehtävänä on huolehtia liikenteen ohjauksesta ja hallinnasta. Näiden laitteiden suorituskyky ja toimintavarmuus vaikuttavat suoraan koko verkon toimintaan, koska ne muodostavat monissa tapauksissa liikenteen kulkuväylän päätelaitteiden ja muiden verkon osien välillä (Lehtonen 2017). Alla olevassa kuvassa on näyte erään L2-kytkimen konfiguraation osasta.



KUVA 2. Esimerkki kytkimen konfiguraatiosta (mukaillen: Cisco CLI)

L2-kerroksen kytkin, joka toimii verkkokerroksen tasolla 2 OSI-mallissa, on keskeinen komponentti paikallisverkoissa (LAN). Tämän kytkimen tehokkuus ja toiminnallisuus perustuvat useisiin tärkeisiin ominaisuuksiin, jotka tekevät siitä välttämättömän välineen nykyaikaisissa verkkoinfrastruktuureissa. Tässä alaluvussa tarkastellaan L2-kytkimen keskeisiä ominaisuuksia, jotka vaikuttavat sen suorituskykyyn ja käyttöön.

L2-kytkimien tärkeimpiä perusominaisuuksia on kyky oppia, mihin porttiin kukin verkon laite on liitetty. Kytkin tallentaa jokaisen laitteen MAC-osoitteen omaan tauluunsa ja hyödyntää tätä tietoa ohjatessaan liikennettä eteenpäin. Näin liikenne ei kulje turhaan kaikkien porttien läpi, mikä vähentää verkon kuormitusta ja parantaa tehokkuutta. Tämä ominaisuus on keskeinen osa kytkinten toimintaa ja olennainen perusta koko verkon suorituskyvylle (Immonen 2017).

Modernit L2-kytkimet tukevat VLAN-teknologiaa, jonka avulla sama fyysinen verkko voidaan jakaa useisiin erillisiin loogisiin osaverkkoihin. Tämä parantaa verkon hallittavuutta ja tietoturvaa, koska eri osastojen tai käyttäjäryhmien liikenne voidaan eristää toisistaan. VLANien hallinta ja konfigurointi ovatkin tärkeitä osa-alueita kytkinten käyttöönotossa ja ylläpidossa (Immonen 2017). Tämä eriytys auttaa vähentämään broadcast-liikennettä eli turhia kyselyitä ja parantaa verkon suorituskykyä.

L2-kytkimien yksi vahvuus on niiden kyky sopeutua verkon muutoksiin dynaamisesti. Kun verkkoon lisätään tai siitä poistetaan laitteita, kytkimet päivittävät MAC-taulunsa automaattisesti. Tämä jatkuva sopeutuminen takaa, että verkko pysyy toiminnassa ilman manuaalisia toimenpiteitä. Tällainen joustavuus on erityisen tärkeää nopeasti muuttuvissa ympäristöissä, kuten yritysverkoissa (Immonen 2017). Tämä dynaamisuus takaa, että verkko pysyy toimivana ja tehokkaana erilaisissa olosuhteissa.

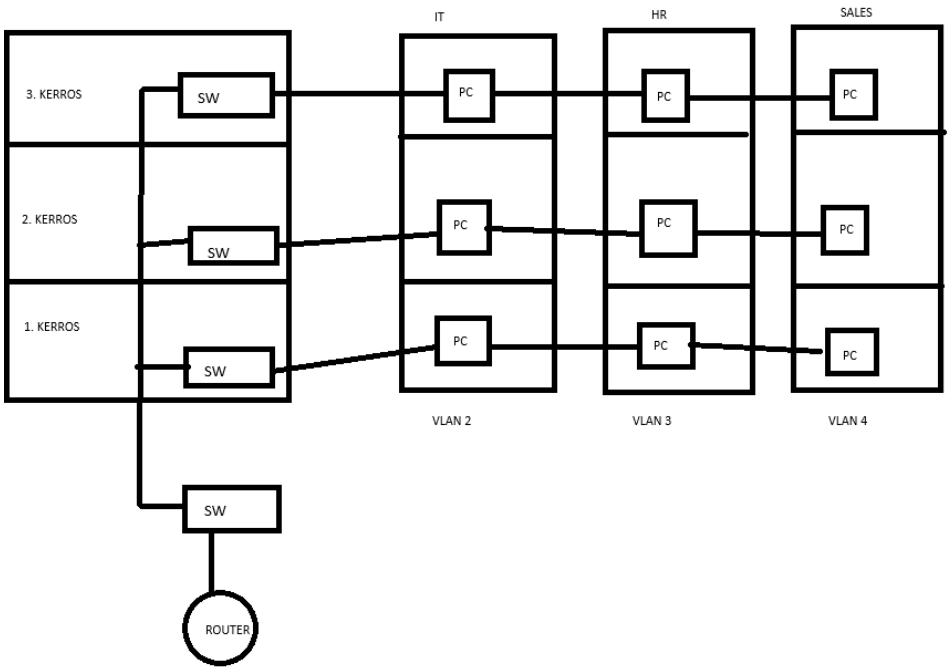
L2-kytkimet on suunniteltu toimimaan monenlaisten laitteiden ja protokollien kanssa, minkä vuoksi ne sopivat hyvin monipuolisiin verkkoympäristöihin. Kun verkko kasvaa ja tietoliikenteen määrä lisääntyy, kytkinten skaalautuvuus varmistaa, että suorituskyky säilyy riittävänä myös tulevaisuuden tarpeisiin. Lisäksi mahdollisuus kytkinten "stackaykseen" antaa lisäkapasiteettia ja parantaa vikasietoisuutta, koska hallinta voidaan keskittää yhteen pisteeseen (Immonen 2017). Tämä tarkoittaa, että useita kytkimiä voidaan hallita keskitetysti yhdestä käyttöliittymästä, mikä yksinkertaistaa hallintaa ja parantaa verkon skaalautuvuutta. Stackays mahdollistaa myös suuremman kaistanleveyden ja parantaa verkon vikasietoisuutta, koska yksi kytkin ei ole enää verkon ainoa kytkin. Kuvassa 4 näette Stackattyjä kytkimiä.

KUVA 3. Stackattyjä ciscon kytkimiä (Cisco)

2.2 L3-kytkin

L3-kerroksen kytkin toimii verkkokerroksen tasolla 3 OSI-mallissa. tämä tarkoittaa, että se pystyy ohjaamaan liikennettä käyttämällä IP-osoitteita. L3-kytkin tarjoaa useita lisäominaisuuksia ja tehokkuutta verrattuna L2-kytkimeen. L3-kytkimen tärkeimmät ominaisuudet ovat.

L3-kytkin pystyy suorittamaan reititystä IP-osoitteiden perusteella. Se voi tehdä päätöksiä siitä, mihin verkko-osoitteeseen liikenne pitää ohjata, jolloin se toimii kuten perinteinen reititin.
VLAN-reititys: L3-kytkin voi suorittaa reititystä VLAN-segmenttien välillä. Se toimii porttina eri VLAN-verkkojen välillä ja mahdollistaa verkkosegmenttien eristämisen ja hallinnan. Jokaista VLAN-verkkoa pidetään erillisenä verkkona. VLAN:in laitteet toimivat ikään kuin ne olisivat omassa itsenäisessä verkossaan, vaikka niillä olisi yhteinen infrastruktuuri muiden VLAN-verkkojen kanssa. Kuten kuviossa 1. (Cisco Networking academy 2023 3.1.1)



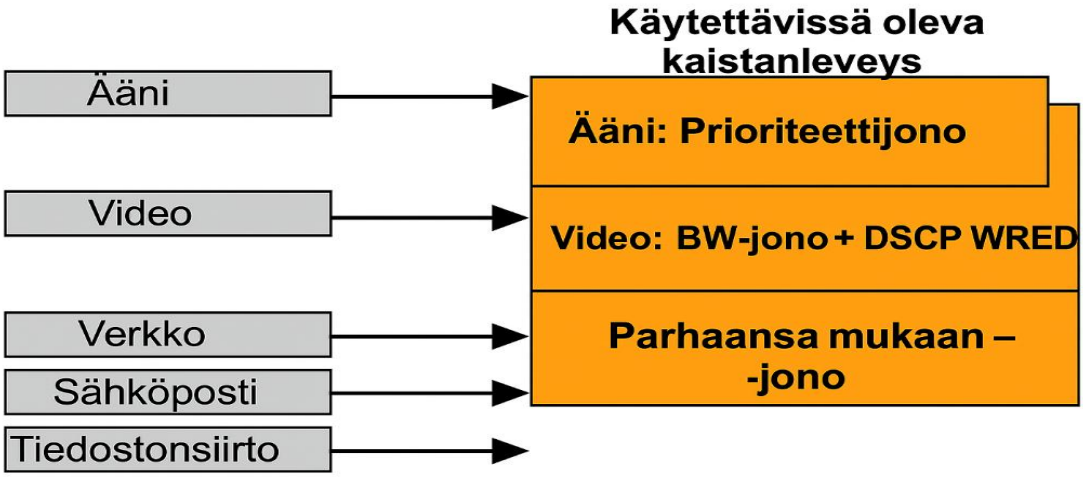
Kuvio 2. VLAN esimerkki. (mukaillen: Cisco Network academy, Switching 3.1.1)

L3-kytkin tukee IP Multicastia, mikä mahdollistaa tehokkaan monipistekommunikaation IP-verkoissa. Se voi ohjata multicast-liikennettä porteille tarvittaessa.

Vaikka L3-kytkin tarjoaa reititys toiminnallisuuden, se on silti erittäin nopea ja tehokas laite. Se pystyy käsittelemään suuria tietomääriä suurella nopeudella, mikä tekee siitä hyvän vaihtoehdon monimutkaisille verkoille.

L3-kytkin pitää taulukkoa IP-osoitteista ja niiden sijainnista verkossa. Tämä mahdollistaa sen, että laite voi ohjata liikennettä tarkemmin ja nopeammin kuin L2-kytkin

Edistynyt liikenteen hallinta: L3-kytkin tarjoaa edistyneitä liikenteen hallintamahdollisuuksia, kuten Quality of Service (QoS) -tuen, joka mahdollistaa priorisoinnin ja tietyn tyyppisen liikenteen optimoinnin. QoS:ia käytetään tyypillisesti verkoissa, jotka kuljettavat liikennettä resurssi intensiivisiin järjestelmiin. Yleisiä palveluita, joita varten sitä tarvitaan, ovat Internet-protokolla-tv (IPTV), online-pelit, suoratoistomedia, videoneuvottelut ja Voice over IP (VoIP). (Fortinet.) Kuviossa 2 havainnollistetaan priorisoitua liikennettä.



Kuvio 3. QoS liikenne (Mukaillen Fiberroad)

L3-kytkimiä käytetään yleensä monimutkaisissa verkoissa, joissa tarvitaan reititystä, segmentointia ja IP-pohjaista liikenteen ohjausta. Niitä käytetään erityisesti yritysverkoissa, palvelimien välisissä verkoissa ja monikerroksisissa verkkoratkaisuissa, joissa L2-kytkimien toiminnallisuus ei riitä.

L3-kytkimissä yksi merkittävimmistä turvallisuuteen liittyvistä ominaisuuksista on mahdollisuus käyttää Access Control List (ACL) -suodatusta. ACL-säännöillä voidaan hallita, millaista liikennettä kytkin sallii ja millaista se estää, mikä tekee siitä tehokkaan työkalun verkon sisäiseen liikenteen suodatukseen. Talvio (2021) tuo esille, että verkon tietoturvan kannalta on tärkeää pystyä rajaamaan ja hallitsemaan liikennettä jo verkkolaitetasolla, sillä se vähentää haitallisen liikenteen leviämistä laajemmin verkossa.

Toinen keskeinen ominaisuus L3-kytkimissä on niiden tuki dynaamisille reititysprotokollille, kuten OSPF ja EIGRP. Dynaamiset reititysprotokollat mahdollistavat sen, että kytkin voi itse oppia ja mukautua verkon topologian muutoksiin ilman manuaalista reititystaulujen ylläpitoa. (Höylä 2012) toteaa, että erityisesti OSPF on laajasti käytetty protokolla yritysverkoissa juuri siksi, että se on joustava ja sopeutuu nopeasti verkon muutoksiin.

L3-kytkimet tukevat myös Layer 3 VPN -ratkaisuja, joiden avulla voidaan rakentaa turvallisia, salattuja yhteyksiä eri toimipisteiden välille julkisen internetin yli. (Lehtonen 2017) korostaa, että monitoimipaikkaisten yritysten verkkoratkaisujen suunnittelussa on tärkeää, että laitteet tukevat suoraan tällaisia VPN-teknologioita, jolloin yhteyksien hallinta on osa verkkolaitteiden perustoiminnallisuutta eikä vaadi erillisiä laitteita.

Lisäksi L3-kytkimet voivat integroida edistyksellisiä verkonvalvontaominaisuuksia, kuten NetFlow- ja sFlow-tekniikoita, jotka keräävät tietoa liikenteen virtauksista verkossa. Tämä tieto auttaa järjestelmänvalvojia ymmärtämään paremmin, miten liikenne liikkuu verkossa, ja optimoimaan verkon suorituskykyä sekä havaitsemaan ja ehkäisemään potentiaalisia ongelmia ennen kuin ne eskaloituvat. L2- ja L3-kytkimet tarjoavat siis hyvin erilaisia toiminnallisuuksia, ja niiden rooli verkkoympäristössä määrittelee pitkälti sen, miten ja kuinka usein niitä tulee päivittää.

3 OHJELMISTOPÄIVITYSTEN MERKITYS JA VALMISTELU

Ohjelmistopäivitykset ovat keskeinen osa verkkolaitteiden ylläpitoa, sillä ne varmistavat järjestelmän suorituskyvyn, turvallisuuden ja yhteensopivuuden uusimpien teknologioiden kanssa. Päivitykset voivat sisältää tietoturvakorjauksia, suorituskykyparannuksia sekä tuen uusille verkkostandardeille ja ominaisuuksille. Ilman säännöllisiä päivityksiä kytkimet voivat altistua haavoittuvuuksille, mikä voi heikentää verkon luotettavuutta ja turvallisuutta.

Jotta päivitysprosessi olisi sujuva ja riskitön, on tärkeää valmistautua huolellisesti ennen päivityksen suorittamista. Tämä sisältää nykyisen ohjelmistoversion tarkistamisen, tarvittavien tiedostojen hankkimisen, järjestelmän varmuuskopioinnin sekä riittävän muistitilan varmistamisen. Tässä luvussa käsitellään ohjelmistopäivitysten merkitystä ja esitetään keskeiset valmisteluvaiheet onnistuneen päivityksen takaamiseksi.

3.1 Miksi ohjelmistopäivitykset ovat tärkeitä

Koska ohjelmistopäivitykset eivät ole vain tekninen rutiini, vaan keskeinen osa laitteiden turvallisuuden ja suorituskyvyn varmistamista, on tärkeää ymmärtää, miksi päivitykset ovat niin kriittisiä ja millaisia riskejä päivitysten laiminlyöntiin liittyy. Verkon kytkimien ohjelmistopäivitykset ovat keskeinen osa verkkoympäristön ylläpitoa ja tietoturvan hallintaa. Yritysverkkojen tietoturva on jatkuva prosessi, jossa verkkolaitteiden ajantasaisuus on merkittävässä roolissa. Monet verkkohyökkäykset kohdistuvat laitteisiin, joiden ohjelmisto on jäänyt päivittämättä, jolloin hyökkääjät pystyvät käyttämään hyväkseen jo tunnettuja haavoittuvuuksia (Talvio 2021). Lisäksi ohjelmistopäivitykset tuovat mukanaan uusia ominaisuuksia ja parannuksia, jotka voivat tehostaa verkon toimintaa.

Ohjelmistopäivitysten tärkeimmät hyödyt ovat:

- Tietoturva: Päivitykset korjaavat tunnettuja haavoittuvuuksia ja vahvistavat verkkolaitteiden suojauksia.
- Parannettu suorituskyky: Uudet ohjelmistoversiot sisältävät optimointeja, jotka voivat vähentää viivettä ja parantaa tiedonsiirtonopeuksia.
- Yhteensopivuus ja uudet ominaisuudet: Päivitykset varmistavat, että verkkolaitteet ovat yhteensopivia uusimpien protokollien ja verkkoarkkitehtuurien kanssa.

- Luotettavuus ja vikasietoisuus: Päivitetty ohjelmisto voi estää järjestelmäkaatumisia ja verkon häiriöitä.

Erityisesti Cisco 3850- ja 3650-sarjan kytkimet ovat laajasti käytettyjä yritysverkoissa, ja niiden ohjelmistopäivitykset tulee suorittaa huolellisesti, jotta verkon toiminta pysyy optimaalisena. Päivitykset voivat olla tarpeen esimerkiksi silloin, kun uusi kytkin lisätään olemassa olevaan stackiin tai kun vikaantunut kytkin korvataan uudella.

Seuraavaksi tarkastellaan, kuinka päivitysprosessi valmistellaan siten, että kaikki sujuu varmasti turvallisesti sekä tehokkaasti.

3.2 Päivitysprosessin valmistelu

Tarkistetaan nykyinen ohjelmistoversio ja lisenssitaso. Ennen ohjelmistopäivityksen suorittamista on tärkeää selvittää, mikä ohjelmistoversio ja lisenssitaso kytkimessä on käytössä. Ohjelmistoversio määrittää, mitä ominaisuuksia ja toiminnallisuuksia laitteella on saatavilla, ja se voi sisältää suorituskykyparannuksia, tietoturvakorjauksia sekä uusia protokollatukia. Lisenssitaso puolestaan määrää, mitkä ohjelmiston ominaisuudet ovat käytettävissä. Esimerkiksi edistyneet reititys- tai tietoturvatoiminnot voivat vaatia korkeamman tason lisenssin

Käytetään komentoa:

show license right-to-use

show version

Varmista, että uuden kytkimen lisenssitaso vastaa stackissä olevien kytkimien tasoa. Jos lisenssitaso on erilainen, aktivoi oikea lisenssi komennolla:

license right-to-use

activate ipbase all

Jos lisenssitaso on jo oikea, tätä vaihetta ei tarvitse tehdä. Oikea lisenssitaso tarkoittaa, että laitteella on käytössä vaadittu ohjelmistoversio ja aktivoidut ominaisuudet, jotka mahdollistavat tarvittavat toimin-

not ilman lisäpäivityksiä tai lisenssilaajennuksia. Esimerkiksi joissakin verkon kytkimissä tietyt edistyneet ominaisuudet, kuten korkeamman tason QoS- tai tietoturvaominaisuudet, vaativat erillisen lisenssin. Mikäli laitteella on jo käytössä vaadittava lisenssitaso, voidaan ohjelmistopäivitys suorittaa ilman lisenssien päivittämistä tai hankkimista.

Varmista, että päivitettävä kytkin on yhteydessä verkkoympäristöön. Vaikka ohjelmistopäivitys suoritetaan USB-tikulta, on tärkeää varmistaa, että kytkin on liitetty verkkoon, jotta se voi tarvittaessa kommunikoida hallintajärjestelmien, lokipalvelimien tai muiden verkonvalvontatyökalujen kanssa. Lisäksi verkkoyhteys voi olla tarpeen päivityksen jälkeisessä tarkastuksessa, esimerkiksi konfiguraation varmentamisessa tai mahdollisten verkko-ongelmien diagnosoinnissa. Jos päivityksen yhteydessä tarvitaan lisätiedostoja tai verifiointia, verkkoyhteys mahdollistaa myös niiden hakemisen keskitetystä hallintajärjestelmästä. Uusi kytkin liitetään verkkoon, ja sille määritetään tarvittavat asetukset ennen päivityksen aloittamista.

Varmista, että ohjelmistotiedosto on valmiina. Tämä tarkoittaa, että USB-tikulle on tallennettu oikea ja yhteensopiva ohjelmistoversio, joka on tarkoitettu päivitettävälle kytkinmallille. On suositeltavaa varmistaa, että tiedosto on ehjä eikä vioittunut, esimerkiksi tarkistamalla sen koko ja vertailemalla sitä valmistajan julkaisemaan tarkistussummaan (checksum, kuten MD5 tai SHA256). Lisäksi on hyvä varmistaa, että USB-tikku on kytkimelle tunnistettavissa ja että tiedosto on helposti löydettävissä kytkimen käyttöjärjestelmästä.

Esimerkiksi:

cat3k_caa-universalk9.16.12.06.SPA.bin

Tarkista tiedoston eheys laskemalla tarkistussumma. Tämä varmistaa, että ohjelmistotiedosto ei ole vioittunut latauksen, kopioinnin tai tallennuksen aikana. Tarkistussumma voidaan laskea käyttämällä tyypillisiä hash-algoritmeja, kuten MD5, SHA-1 tai SHA-256, ja vertaamalla saatu arvo ohjelmistovalmistajan tarjoamaan referenssisummaan.

verify /md5 flash:cat3k_caa-universalk9.16.12.06.SPA.bin

Varmista, että tarpeettomat tiedostot on poistettu. Kytkimen flash-muisti on rajallinen, joten vanhojen ja käyttämättömien tiedostojen poistaminen vapauttaa tilaa ja varmistaa, että päivitystiedosto mahtuu tallennustilaan ilman ongelmia.

Poista vanhat ja käyttämättömät tiedostot flash-muistista, jotta päivitys onnistuu sujuvasti. Tarkista ensin flash-muistin käytettävissä oleva tila ja listaa tallennetut tiedostot:

show flash:

software clean

Kun nämä vaiheet on suoritettu, voidaan siirtyä itse päivitysprosessiin.

4 OHJELMISTOPÄIVITYKSEN SUORITTAMINEN

Ohjelmistopäivitysten suorittaminen on keskeinen osa IT-infrastruktuurin ylläpitoa, ja se varmistaa laitteiden suorituskyvyn, turvallisuuden ja yhteensopivuuden uusimpien teknologioiden kanssa. Päivitysprosessi voi vaihdella laite- ja ohjelmistovalmistajan mukaan, mutta yleisesti se sisältää valmistelun, päivitysten asentamisen ja järjestelmän toiminnan tarkastuksen päivityksen jälkeen. Päivitykset voidaan suorittaa manuaalisesti tai automatisoidusti, ja niiden huolellinen suunnittelu on tärkeää verkon häiriöttömän toiminnan varmistamiseksi

4.1 Päivitys USB-muistilta yksittäiseen kytkimeen

Ennen ohjelmistopäivityksen suorittamista on tärkeää varmistaa, että käytettävä ohjelmistoversio on yhteensopiva muiden kytkimien kanssa. Valmisteluvaihe sisältää seuraavat vaiheet:

Jos päivitys suoritetaan yksittäiseen kytkimeen ilman stackia, voidaan ohjelmistotiedosto kopioida suoraan kytkimen muistiin ja asentaa.

Siirrä ohjelmistotiedosto USB-muistilta kytkimeen

copy usbflash0:cat3k_caa-universalk9.16.12.06.SPA.bin Flash:

Tarkista, että tiedosto on siirtynyt oikein

verify /md5 flash:cat3k_caa-universalk9.16.12.06.SPA.bin

Jos laskettu MD5-tarkistussumma vastaa valmistajan ilmoittamaa arvoa, tiedosto on eheä ja valmis käytettäväksi päivitysprosessissa.

Asenna ohjelmisto ja käynnistä kytkin uudelleen

software install file flash:cat3k_caa-universalk9.16.12.06.SPA.bin new force

reload

Poista vanhat ohjelmistotiedostot komennolla:

install remove inactive

Kun ohjelmistopäivitys on onnistuneesti suoritettu ja kytkin toimii odotetusti uudella ohjelmistoversiolla, voit poistaa vanhat ja käyttämättömät ohjelmistotiedostot vapauttaaksesi flash-muistitilaa.

4.2 Päivitys stackissa oleviin kytkimiin

Jos päivitys koskee stackissa olevia kytkimiä, voidaan hyödyntää automaattista päivitystoimintoa.

Päivitä ohjelmisto stackissä oleviin kytkimiin

software auto-upgrade

Jos käytössä on uudempi ohjelmistoversio (16.x.x), käytä seuraavaa komentoa:

request platform software package install autoupgrade

Tämä komento suorittaa ohjelmistopäivityksen automaattisesti halliten asennusprosessin ja tarvittavat riippuvuudet. Autoupgrade-vaihtoehto varmistaa, että järjestelmä asentaa kaikki tarvittavat paketit ja suorittaa päivityksen mahdollisimman sujuvasti ilman manuaalisia vaiheita.

Varmista, että kaikki kytkimet ovat stackissa ja käynnistä ne uudelleen komennolla:

reload

Poista vanhat ohjelmistotiedostot päivityksen jälkeen. Kun päivitys on onnistuneesti suoritettu ja kytkin toimii odotetusti uudella ohjelmistoversiolla, vanhat ohjelmistotiedostot voidaan poistaa vapauttaakseen flash-muistitilaa ja ylläpitääkseen järjestelmän siisteyttä.

install remove inactive

5 YHTEENVETO JA PÄIVITYKSEN MERKITYS

Ohjelmistopäivitykset ovat keskeinen osa verkon infrastruktuurin hallintaa, ja niiden merkitys korostuu niin tietoturvan, suorituskyvyn kuin yhteensopivuuden kannalta. Päivitykset mahdollistavat uusimpien teknologioiden ja verkkostandardien tukemisen sekä vähentävät haavoittuvuuksia, jotka voisivat altistaa järjestelmän tietoturvariskeille. Lisäksi ne voivat parantaa järjestelmän vakautta ja tehokkuutta, mikä edistää koko verkon luotettavuutta ja käytettävyyttä. Tässä luvussa käydään läpi päivitysten merkitys ja niiden vaikutus verkon toimintaan.

5.1 Ohjelmistopäivityksen rooli verkkoympäristössä

Ohjelmistopäivitykset eivät ole vain pakollinen rutiinitoimenpide, vaan ne ovat olennainen osa verkkolaitteiden elinkaaren hallintaa. Verkkolaitteiden hallittavuus ja niiden päivitettävyys ovat keskeisiä näkökulmia jo siinä vaiheessa, kun uutta verkkolaitteistoa hankitaan. Laitteiden tekniset ominaisuudet ja ohjelmistojen elinkaari vaikuttavat siihen, miten hyvin ne voidaan pitää ajan tasalla tulevaisuudessa. Tämä korostaa tarvetta huomioida päivityskäytännöt osana kokonaisvaltaista elinkaaren hallintaa (Lehtonen 2017; Talvio 2021). Verkkoympäristössä kaikki nämä tekijät voivat vaikuttaa koko organisaation toimintakykyyn.

Keskeiset syyt ohjelmistopäivityksiin:

Tietoturvan parantaminen

Tietoturvapäivitykset suojaavat järjestelmää uusilta uhkilta, kuten haittaohjelmilta, tietomurroilta ja palvelunestohyökkäyksiltä. Päivitykset paikkaavat ohjelmistossa havaittuja haavoittuvuuksia ja estävät hyökkäykset, jotka voivat johtaa tietovuotoihin tai järjestelmän kaatumiseen. Esimerkiksi **CVE-2023-20198**-haavoittuvuus Cisco IOS XE -ohjelmiston web-käyttöliittymässä mahdollisti hyökkääjien luoda järjestelmään korkeimman tason (taso 15) käyttäjätilejä ilman asianmukaista autentikointia. Cisco julkaisi tietoturvapäivityksen estääkseen tämän haavoittuvuuden hyväksikäytön (Cisco 2023). Vastaavasti päivittämättömät järjestelmät ovat alttiina uusille haavoittuvuuksille, joita hyökkääjät voivat hyödyntää.

Toiminnallisuuden ja suorituskyvyn optimointi

Ohjelmistopäivitykset eivät ainoastaan paranna tietoturvaa, vaan ne tuovat usein mukanaan tehokkaampia algoritmeja ja suorituskykyparannuksia, jotka vähentävät viivettä ja lisäävät verkon kapasiteettia. Esimerkiksi Cisco on kehittänyt Extended Fast Software Upgrade (xFSU) -ominaisuuden, joka vähentää liikenteen seisokkiaikoja ohjelmistopäivitysten aikana, mikä parantaa verkkolaitteiden suorituskykyä ja tehokkuutta (Cisco 2025). Päivitetyt laitteet pystyvät näin ollen paremmin käsittelemään kasvavaa tietoliikennettä ja skaalautumaan yrityksen tarpeiden mukaisesti.

Yhteensopivuuden varmistaminen

IT-infrastruktuuri muuttuu jatkuvasti ja uudet ohjelmistoversiot voivat tuoda parannuksia yhteensopivuuteen uusien verkkoprotokollien, palveluiden ja laitteiden kanssa. Päivitysten avulla voidaan varmistaa, että kytkimet tukevat uusimpia verkkostandardeja, kuten IPv6:ta ja uusia QoS (Quality of Service) -ominaisuuksia. Esimerkiksi ohjelmistopäivitykset voivat parantaa järjestelmän suorituskykyä, turvallisuutta ja yhteensopivuutta uusien sovellusten ja teknologioiden kanssa (Buchanan 2024). Päivitetyt laitteet pystyvät näin ollen paremmin käsittelemään kasvavaa tietoliikennettä ja skaalautumaan yrityksen tarpeiden mukaisesti.

Luotettavuuden ja vikasietoisuuden parantaminen

Ohjelmistopäivitykset voivat korjata tunnettuja bugeja ja estää verkon häiriöitä, jotka voivat vaikuttaa kriittisiin palveluihin. Esimerkiksi säännölliset ohjelmistopäivitykset ovat välttämättömiä tietokoneiden, mobiililaitteiden ja tablettien sujuvan toiminnan ylläpitämiseksi, ja ne voivat vähentää tietoturva-aukkoja (Telecom World 101 2023).

Lisäksi uudet versiot voivat sisältää redundanssitoimintoja ja parannettuja diagnostiikkatyökaluja, jotka helpottavat vianmääritystä ja ennakoivaa ylläpitoa. Esimerkiksi Cisco suosittelee hyödyntämään sisäänrakennettuja diagnostiikkatyökaluja linkkien terveyden seuraamiseksi ja mahdollisten vikojen nopeaksi havaitsemiseksi (Ergun 2023).

5.2 Päivitysprosessin haasteet ja riskit

Ohjelmistopäivityksiin liittyy monia riskejä, joista yksi merkittävimmistä on verkkoympäristössä syntyvä käyttökatko. Erityisesti yritysverkoissa tällaiset katkot voivat häiritä liiketoiminnan jatkuvuutta ja aiheuttaa suoria taloudellisia tappioita, mikä tekee päivitysten huolellisesta suunnittelusta välttämätöntä (Talvio 2021). Vaikka ohjelmistopäivitykset ovat välttämättömiä, niiden toteutus voi tuoda mukanaan haasteita, jotka on huomioitava etukäteen. Päivitysprosessi edellyttää usein laitteiden uudelleenkäynnistystä, mikä voi aiheuttaa tilapäisiä käyttökatkoksia. Tätä varten on hyvä suunnitella päivitykset ennalta ja suorittaa ne esimerkiksi öisin tai muina aikoina, jolloin verkon kuormitus on alhainen.
Yhteensopivuusongelmat.
Jos ohjelmistopäivitys ei ole yhteensopiva muun infrastruktuurin kanssa, se voi aiheuttaa yhteysongelmia tai rajoittaa tiettyjen ominaisuuksien käyttöä. Tämän vuoksi on hyvä testata uusi ohjelmistoversio ensin testiverkossa ennen sen käyttöönottoa tuotantoympäristössä.
Konfiguraatiomuutokset ja asetusten nollautuminen.
Joissakin tapauksissa päivitys voi muuttaa kytkimen asetuksia tai palauttaa sen tehdasasetuksiin, mikä vaatii uudelleenkonfigurointia.
Ratkaisu: Tee varmuuskopiot kytkimen nykyisestä kokoonpanosta ennen päivitystä komennolla:
show running-config > backup.cfg
Päivityksen epäonnistuminen
Jos päivitysprosessi keskeytyy esimerkiksi virtakatkoksen tai verkkoyhteysongelmien vuoksi, kytkin voi jäädä toimimattomaan tilaan.
Ratkaisu: Käytä dual boot -ominaisuutta ja varmista, että aiempi ohjelmistoversio on saatavilla palautusta varten.

5.3 Cisco-kytkimien ohjelmistopäivitysten erityispiirteet

Cisco 3650- ja 3850-sarjan kytkimet ovat yrityskäytössä yleisiä laitteita, joiden ohjelmistopäivityksiin liittyy tiettyjä erityispiirteitä:

Stack-päivitys: Jos kytkimet ovat osa stackia, on varmistettava, että kaikki kytkimet päivitetään yhtenäisesti, jotta vältetään versioeroista johtuvat ongelmat.
Tuki useille ohjelmistoversioille: Cisco-kytkimet voivat käyttää install- tai bundle-tilaa, ja päivitysmenetelmät eroavat hieman toisistaan, riippuen käytössä olevasta ohjelmistotilasta.
Päivitysprosessin automatisointi: Cisco tarjoaa mahdollisuuden automatisoituun päivitykseen esimerkiksi komennolla:
software auto-upgrade
Näiden tekijöiden ymmärtäminen auttaa varmistamaan, että päivitysprosessi sujuu suunnitellusti ilman suuria häiriöitä.

5.4 Johtopäätökset ja suositukset

Ohjelmistopäivityksiä käsitteleväss osiossa käytiin läpi Cisco 3650- ja 3850-kytkimien päivitysprosessi sekä siihen liittyvät haasteet ja parhaat käytännöt. Päivitykset ovat olennainen osa verkkoympäristön ylläpitoa, ja niiden merkitys korostuu entisestään organisaatioissa, joissa vaaditaan korkeaa suorituskykyä ja tietoturvaa.

Jotta päivitysprosessi sujuisi mahdollisimman tehokkaasti ja turvallisesti, suositellaan seuraavia toimenpiteitä:

Päivitä säännöllisesti, mutta harkiten.

Päivityksiä ei kannata tehdä liian harvoin, mutta myöskään jokaisen uuden version asentaminen heti julkaisun jälkeen ei ole suositeltavaa. Odota esimerkiksi ensimmäisten käyttäjäraporttien perusteella, että uusi versio on vakaa.

Testaa ensin, ota käyttöön vasta varmistuksen jälkeen.

Käytä testiympäristöä ja varmista, että uusi ohjelmistoversio toimii odotetusti ennen sen levittämistä koko verkkoon.

Dokumentoi päivitysprosessit.

Kirjaa ylös kaikki päivitysprosessin aikana suoritetut vaiheet, jotta mahdolliset ongelmat voidaan jäljittää ja estää niiden toistuminen tulevaisuudessa.

Varmista varmuuskopiointi.

Pidä aina saatavilla edellinen toimiva ohjelmistoversio, jotta voit palauttaa sen nopeasti ongelmatilanteessa.

Ota huomioon verkon käyttäjät.

Ilmoita käyttäjille mahdollisista käyttökatkoista hyvissä ajoin ja suunnittele päivitykset ajankohtiin, jolloin ne aiheuttavat vähiten häiriötä.

Näiden suositusten avulla voidaan varmistaa, että ohjelmistopäivitykset eivät ainoastaan paranna verkon suorituskykyä ja turvallisuutta, vaan myös minimoivat mahdolliset riskit ja käyttökatkokset.

6 POHDINTA

Tämän opinnäytetyön tavoitteena oli perehtyä verkkokytkimiin, erityisesti L2- ja L3-kerroksen kytkimiin, sekä niiden ohjelmistopäivityksiin. Työ lähti liikkeelle tärkeästä kysymyksestä: Miksi kytkimien ohjelmistopäivitykset ovat kriittisiä nykyaikaisessa verkkoympäristössä ja miten päivitykset tulisi suorittaa tehokkaasti ja turvallisesti? Kysymys osoittautui hyvin ajankohtaiseksi, sillä verkkoympäristöjen luotettavuus ja tietoturva on nykyisin tärkeämpää kuin koskaan.

Heti alussa kävi selväksi, että kytkimien ohjelmistopäivitykset ovat paljon muutakin kuin pelkkä tekninen rutiini. Päivitykset kytkeytyvät suoraan organisaation kykyyn suojautua kyberuhilta, ylläpitää verkon suorituskykyä ja varmistaa uusimpien teknologioiden yhteensopivuus. Päivittämättömät kytkimet voivat muodostaa vakavan tietoturvariskin, sillä niissä piilee usein vanhentuneita protokollia, haavoittuvuuksia ja puutteellisia suojausominaisuuksia. Näiden riskien ymmärtäminen toi työlle vahvan käytännön merkityksen.

Perehtyminen L2- ja L3-kytkimiin osoitti, että vaikka nämä kaksi laitetyyppiä kuulostavat perustoiminnallisuuksiltaan yksinkertaisilta, niiden roolit ja tekniset ominaisuudet eroavat toisistaan merkittävästi. Tämä puolestaan vaikuttaa suoraan päivitysprosessin monimutkaisuuteen. L2-kytkimien päivitykset ovat yleensä suoraviivaisempia, sillä ne toimivat yksittäisissä verkkosegmenteissä ja niiden rooli keskittyy MAC-osoitteiden hallintaan. L3-kytkimien kohdalla päivitykseen liittyy huomattavasti enemmän liikkuvia osia, kuten reititystauluja, ACL-sääntöjä ja dynaamisia reititysprotokollia. Tämä havainto selkeytti myös sitä, miksi päivitysten suunnittelu ja esivalmistelu on kriittistä. Kyseessä ei ole vain yhden laitteen päivittäminen, vaan osa koko verkkorakenteen elinkaaren hallintaa.

Opinnäytetyö osoitti, että kytkimien ohjelmistopäivityksissä on kaksi selkeää haastetta. Ensimmäinen liittyy tekniseen suoritukseen: oikean ohjelmistoversion valinta, päivityksen ajastus, varmuuskopioiden ottaminen ja itse päivitysprosessi. Toinen haaste on organisaatio tasoinen: päivitys aiheuttaa lähes väistämättä katkoja ja vaatii huolellista kommunikaatiota eri sidosryhmien, kuten IT-osaston, johdon ja loppukäyttäjien välillä. Tämä organisaatio puoli osoittautui jopa tärkeämmäksi kuin aluksi oletin. Päivityksen tekninen suorittaminen on sinänsä hallittavissa, mutta päivityksen vaikutukset laajempaan verkon toimintaan voivat yllättää, ellei niitä huomioida ennakolta. Jotta ohjelmistopäivitykset sujuvat hallitusti ja tukevat verkon toimintavarmuutta, niiden merkitys tulisi tunnistaa jo verkon suunnittelu-

vaiheessa. Päivityskäytännöt kannattaa miettiä osaksi organisaation ylläpitoprosesseja heti alkuvaiheessa, jolloin voidaan varmistaa, että valitut laitteet tukevat ajantasaisia ja helposti hallittavia päivitysmenetelmiä (Lehtonen 2017; Talvio 2021).

Työn aikana korostui myös se, kuinka monimutkaista ja aikaa vievää ajantasaisen tiedon löytäminen voi olla. Cisco tarjoaa laajan dokumentaation, mutta se on suunnattu pääasiassa kokeneille ammattilaisille, joilla on jo vankka taustatieto laitteiden toiminnasta. Tällaiselle opinnäytetyölle, joka pyrkii palvelemaan myös opiskelijoita ja aloittelevia IT-asiantuntijoita, olisi hyödyllistä, jos vastaavia ohjeistuksia olisi saatavilla yksinkertaistetussa, vaihe vaiheelta etenevässä muodossa. Tämä havainto vahvisti myös sen, että kytkimien päivitysprosessi ei ole vain tekninen operaatio, vaan jatkuva oppimisprosessi.

Pohdin myös, kuinka eri tavoin organisaatiot suhtautuvat päivityksiin. Toisissa organisaatioissa päivityksiä tehdään hyvin systemaattisesti ja säännöllisesti, kun taas joissakin päivityksiä lykätään, kunnes ongelmia ilmenee. Jälkimmäinen lähestymistapa on erityisen riskialtis nykypäivän tietoturvaympäristössä, jossa haavoittuvuudet tunnetaan laajasti ja niitä osataan hyödyntää nopeasti. Tässä mielessä opinnäytetyön anti ei ole vain teknistä, vaan myös kulttuurista: miten organisaatiot voivat rakentaa ennakoivaa ja tietoturvatietoista toimintamallia, jossa päivitykset nähdään osana normaalia ylläpitoa eikä poikkeustilanteena.

Yksi yllättävimmistä havainnoista oli se, kuinka suuri merkitys on käytettävällä päivitysmenetelmällä. USB-päivitys, joka vaikuttaa aluksi vanhanaikaiselta, osoittautui kuitenkin luotettavammaksi kuin verkkopohjaiset päivitykset. Tämä johtuu siitä, että USB-päivitys on vähemmän riippuvainen ulkoisista verkkoyhteyksistä ja sallii päivityksen suorittamisen suljetussa ympäristössä. Tämä havainto tukee ajatusta, että joskus yksinkertaisin ratkaisu on myös turvallisin.

Stackattyjen kytkimien kohdalla opin, että päivitykset monimutkaistuvat huomattavasti. Stackissa yksikin versioero voi aiheuttaa koko ryhmän epävakaan toiminnan. Tästä syystä dokumentointi, versionhallinta ja testaus ovat stack-ympäristössä vielä tärkeämpiä kuin yksittäisissä kytkimissä. Tämä oli itselleni tärkeä oppi, joka liittyy suoraan käytännön työelämään.

Työn pohjalta heräsi myös jatkotutkimusaiheita. Yksi kiinnostava suunta olisi tutkia, miten automaatio ja tekoäly voisivat auttaa päivitysprosessin hallinnassa. Esimerkiksi Cisco DNA Center tarjoaa mahdollisuuden automaattiseen päivityshallintaan, mutta sen käytännön hyödyt ja rajoitukset ovat vielä monille epäselviä.

Toinen kiinnostava aihe olisi vertailla eri valmistajien kytkimien päivitysprosesseja ovatko esimerkiksi Juniperin, HP:n tai Ubiquitin ratkaisut suoraviivaisempia tai käyttäjäystävällisempiä kuin Ciscon?

Kaiken kaikkiaan tämä opinnäytetyö vahvisti ymmärrystäni siitä, että verkkoteknologiat ovat jatkuvasti kehittyvä ja monitahoinen kokonaisuus. Pelkkä tekninen osaaminen ei riitä vaan tarvitaan myös kykyä hallita kokonaisuuksia, arvioida riskejä ja kommunikoida päivitysten vaikutuksista selkeästi organisaation sisällä. Samalla opin arvostamaan ennakoivaa ylläpitoa ja dokumentaation merkitystä. Päivitys ei ole projekti, vaan osa jatkuvaa verkkoympäristön elinkaaren hallintaa.

Lopuksi voidaan todeta, että ohjelmistopäivitykset ovat yksi tärkeimmistä yksittäisistä toimenpiteistä, joilla voidaan vaikuttaa verkon tietoturvaan, suorituskykyyn ja elinkaareen. Ne ovat investointi, joka maksaa itsensä takaisin luotettavana ja turvallisena verkkoympäristönä. Tämä työ tarjosi minulle arvokasta käytännön osaamista ja ymmärrystä, jota voin hyödyntää niin tulevissa opinnoissani kuin työelämässäni.

7 EETTINEN POHDINTA

Verkkokytkimien ohjelmistopäivitykset voivat vaikuttaa pelkästään tekniseltä toimenpiteeltä, mutta niiden taustalla piilee monia eettisiä kysymyksiä, jotka liittyvät sekä vastuulliseen päätöksentekoon että tietoturvan ylläpitämiseen. Yksi konkreettinen osa tätä prosessia on päivitysten suorittaminen USB-tikun avulla. Vaikka kyseessä on yleinen ja teknisesti kätevä tapa, se nostaa esiin myös kysymyksiä tietoturvasta, avoimuudesta ja vastuullisuudesta.

Ensimmäinen eettinen kysymys liittyy itse USB-tikun käsittelyyn ja hallintaan. Kun päivitystiedosto siirretään tikulle, on ensiarvoisen tärkeää varmistaa, että tikku on luotettava, virustarkastettu ja että sen koko historia on tiedossa. Jos IT-ammattilainen käyttää omaa henkilökohtaista tikkuaan tai lataa päivitystiedoston koneella, joka ei ole organisaation hallinnassa, hän vaarantaa päivitysprosessin turvallisuuden. Tämä on suora eettinen ongelma, sillä vastuullinen ICT-ammattilainen huolehtii siitä, että päivityksen lähde ja välineet ovat luotettavia (Duquenoy, P., George, C., Koivisto, R., Walsh, N. & Webb, M. 2018).

Toiseksi eettinen vastuu liittyy siihen, miten USB-tikkuja säilytetään ja käytetään. Jos päivitykseen tarkoitettu tikku on avoimesti kenen tahansa saatavilla, kuka tahansa voisi muokata sen sisältöä tai lisätä siihen haittaohjelmia. Tämä on vakava riski, koska USB-päivityksellä viedään suoraan ohjelmisto kytkimeen, joka on keskeinen osa koko verkkoympäristöä. Turvallinen ja eettisesti kestävä toimintamalli edellyttää, että päivitysmediat säilytetään lukituissa tiloissa, ja että niiden käyttö on dokumentoitu tarkasti (Duquenoy et al. 2018).

Kolmantena, päivityksen dokumentointi itsessään on osa eettistä vastuuta. Jokaisesta päivityksestä tulisi jäädä selkeä kirjaus siitä, mitä versiota käytettiin, kuka päivityksen teki ja milloin. Jos dokumentointi on puutteellista tai sitä ei tehdä ollenkaan, se on vastuutonta toimintaa, koska ongelmatilanteessa kukaan ei voi varmistaa, mitä päivityksen aikana on tapahtunut. (Duquenoy et al. 2018) korostavat, että läpinäkyvyys ja dokumentointi ovat olennaisia osia ICT-ammattilaisen ammattietiikkaa.

Eettistä pohdintaa vaatii myös päätös siitä, milloin päivitys tehdään – tai jätetään tekemättä. Jos organisaatiossa päätetään lykätä kriittistä päivitystä esimerkiksi kiireen, resurssipulan tai mukavuussyiden

takia, päätös ei ole vain tekninen, vaan myös eettinen. Päivittämätön kytkin voi sisältää tunnettuja haavoittuvuuksia, joita hyökkääjät osaavat hyödyntää. Päivityksen lykkääminen on siis tietoinen riski, jossa organisaatio ja sen IT-henkilöstö hyväksyy sen, että tietoturva ei ole ajan tasalla (Duquenoy et al. 2018). Tällöin voidaan kysyä, toimiiko ammattilainen vastuullisesti vai laiminlyökö hän eettistä velvollisuuttaan suojella järjestelmää ja sen käyttäjiä.

Jos päivityksen lykkääminen johtaa tietomurtoon tai muuhun vakavaan tietoturvaongelmaan, eettiset kysymykset muuttuvat vielä vakavammiksi. Kuka kantaa vastuun? Oliko päätöksen taustalla riittävä riskianalyysi, vai oliko kyseessä välinpitämättömyys? (Duquenoy et al. 2018) huomauttavat, että ICT-ammattilaisen ammattietiikkaan kuuluu kyky arvioida päätösten lyhyen ja pitkän aikavälin vaikutuksia. Tässä tapauksessa lyhyen aikavälin mukavuus, eli päivityksen lykkääminen voi johtaa pitkän aikavälin kriisiin, jossa organisaation maine, talous ja tietoturva kärsivät merkittävästi.

Toinen eettisesti arveluttava tilanne voi syntyä, jos päivitystä ei tehdä, mutta organisaation sisällä annetaan ymmärtää, että kaikki on kunnossa. Tällainen harhaanjohtaminen on ristiriidassa avoimuuden ja vastuullisuuden periaatteiden kanssa, jotka ovat ICT-ammattilaisen keskeisiä eettisiä ohjenuoria (Duquenoy et al. 2018). Avoimuus tarkoittaa sitä, että riskit, päätökset ja niiden perusteet tuodaan selkeästi esiin, eikä epämiellyttäviä asioita piilotella.

Eettiset kysymykset ulottuvat myös siihen, miten organisaatiot suhtautuvat työntekijöidensä osaamiseen. Jos päivitysvastuu annetaan henkilölle, jolla ei ole riittävää osaamista tai perehdytystä, kyseessä on sekä operatiivinen että eettinen riski. ICT-alalla ammattietiikkaan kuuluu oman osaamisen ylläpito ja rajojen tunnistaminen. Jos ei tiedä, mitä on tekemässä, on vastuullista pyytää apua (Duquenoy et al. 2018).

Lopulta koko päivitysprosessin voi nähdä osana organisaation tietoturvakulttuuria. Jos kulttuuri suosii hätäilyä, puutteellista dokumentointia ja epävirallisia toimintatapoja, se ruokkii epäeettistä toimintaa. Vastuullinen ICT-ammattilainen ei ole pelkkä tekninen suorittaja, vaan hän myös aktiivisesti rakentaa ja ylläpitää eettisesti kestävää toimintakulttuuria (Duquenoy et al. 2018). Tämä tarkoittaa sekä henkilökohtaisen vastuun kantamista että sen varmistamista, että myös organisaatio tarjoaa puitteet vastuulliselle toiminnalle.

Yhteenvetona voidaan todeta, että verkkokytkimien päivitykset USB-tikulta eivät ole pelkkä tekninen toimenpide, vaan monitasoinen prosessi, johon liittyy runsaasti eettisiä ulottuvuuksia. Vastuullinen

ICT-ammattilainen varmistaa päivitysten turvallisuuden, dokumentoi ne läpinäkyvästi ja viestii niistä avoimesti. Päivitysten viivyttäminen tai huolimattomuus prosessissa voi pahimmillaan vaarantaa koko organisaation tietoturvan ja kyseenalaistaa IT-ammattilaisen ammattietiikan.

LÄHTEET

Buchanan 2024. The Power of System Upgrades in IT Modernization. Saatavissa: 17.3.2025, https://www.buchanan.com/system-upgrades-help-modernize-it-infrastructure/ Viitattu 17.3.2025.

Cisco Networking Academy. Welcome to Switching, Routing, and Wireless Essentials v7.02 (SRWE). Saatavissa: https://lms.netacad.com/course/view.php?id=2127779. Viitattu 18.9.2024.

Cisco Networking academy. Introduction to Networks. 2020 5.1.1.4. Saatvissa: https://www.netacad.com/ Viitattu 18.9.2024.

Cisco Networking academy 2023 3.1.1. Saatavissa: https://www.netacad.com/ Viitattu 18.9.2024.

Cisco 2023. Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature. Saatavissa:, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z Viitattu 17.3.2025.

Cisco support. Upgrade Firmaware on a Switch through the Command Line interface (CLI). Saatavissa: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-550x-series-stackable-managed-switches/smb5566-upgrade-firmware-on-a-switch-through-the-command-line-interf.html Viitattu 7.3.2025.

Cisco (2025). Understand Extended Fast Software Upgrade on Catalyst 9300 Series Switches. Saatavissa: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-series-switches/216837-extended-fast-software-upgrade-on-cataly.html Viitattu 17.3.2025.

Duquenoy, P., George, C., Koivisto, R., Walsh, N. & Webb, M. 2018. Professional ethics: A competency framework for the ICT profession. Computer Science Education, 28(3), 254-275. Saatavissa: https://onlinelibrary.wiley.com/doi/10.1002/cce2.37 Viitattu 7.3.2025.

Mike Schule (2023). Troubleshooting Common Cisco VSS Issues. Saatavissa: https://orhanergun.net/troubleshooting-common-cisco-vss-issues Viitattu 17.3.2025.

Fortinet. What is QoS in Networking. Saatavissa: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service Viitattu 18.9.2024.

Höylä, T. 2012. OSPF-reititysprotokollan ominaisuudet. Theseus. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/51571/Opinnaytetyo_Tero_Hoyla.pdf. Viitattu 3.3.2025.

Immonen, J. 2017. L2-kytkinten ominaisuudet ja konfigurointi: Katsaus Juniperin, Ciscon ja HP:n kytkinten perustoimintoihin. Metropolia Ammattikorkeakoulu. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/123390/Immonen_Juho.pdf. Viitattu 3.3.2025.

Kuntaliitto (2024). Kuntien varautuminen ja turvallisuus. Saatavissa: https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/kuntien-varautuminen-ja-turvallisuus Viitattu 18.3.2025.

Kyberturvallisuuskeskus (2024). Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa Viitattu 18.3.2025.

Lehtonen, T. 2017. Modernin tietoliikenneverkon suunnittelu. Theseus. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/124868/Lehtonen_Tomi.pdf. Viitattu 3.3.2025.

Talvio, A. 2021. Moderniin yritysverkkoon kohdistuvat kyberuhat ja niiltä suojautuminen. Theseus. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/495754/Talvio_Arttu.pdf. Viitattu 3.3.2025.

Telecom World 101 (2023). Network Hardware Maintenance Best Practices. Saatavissa: https://telecomworld101.com/network-hardware-maintenance-best-practices/ Viitattu 17.3.2025.

Tieturi (2024). Pilvipalvelut ja niiden merkitys yrityksille. Saatavissa: https://www.tieturi.fi/en/blogi/pilvipalvelu-suomessa-hyodyt-haasteet-ja-suosituimmat-palveluntarjoajat Viitattu 18.3.2025.

Verizon (2023). 2023 Data Breach Investigations Report. Saatavissa: https://www.verizon.com/business/resources/reports/dbir/ Viitattu 18.3.2025.