SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

YRITYKSEN TIETOVERKKO JA TIETOTURVA

Kartoitus, analysointi ja optimointi

TEKIJÄ: Mirka Koivistoinen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Mirka Koivistoinen	
Työn nimi Yrityksen tietoverkko ja tietoturva - kartoitus, analysointi ja optimointi	
Päiväys 10.5.2016	Sivumäärä/Liitteet 42
Ohjaaja(t) Lehtori Veijo Pitkänen	
Toimeksiantaja/Yhteistyökumppani(t) Yritys X	

Tiivistelmä

Opinnäytetyön tarkoituksena oli kartoittaa yrityksen tietoverkko ja tietoverkossa olevat verkkolaitteet, tehdä laitteista tietokanta yrityksen käyttöön, analysoida tietoverkon rakenne ja tehdä ehdotuksia tietoturvan ja toimintavarmuuden parantamiseksi. Kartoitus tehtiin puhelimitse yhdessä paikallisten teknikkojen kanssa, sähköpostilla ja tutustumalla verkkoon henkilökohtaisesti. Työssä keskityttiin tietoverkon core-, distribution- ja access-kerroksen verkkolaitteisiin.

Lopputuloksena saatiin selkeä kuva yrityksen tietoverkon laitteista, niiden sijainnista ja tilasta, yrityksen tietoverkon rakenteesta sekä tietoturvasta. Kartoituksen avulla saatiin aikaan kustannussäästöjä karsimalla turhia yhteyksiä ja löydettiin verkon turvallisuutta uhkaavia tekjöitä. Lisäksi työssä tuotiin esiin DoS-hyökkäyksiä mahdollistavat puutteet tietoverkossa ja annettiin ehdotuksia siihen kuinka hyökkäyksiä voitaisiin estää.

Avainsanat
Tietoverkko, tietoturva, DoS-hyökkäys

Osittain salainen

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS

Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Computer Science			
Author(s) Mirka Koivistoinen			
Title of Thesis A company's network and network security – Mapping, analysis and optimisation.			
Date	10.5.2016	Pages/Appendices	42
Supervisor(s) Lecturer Veijo Pitkänen			
Client Organisation /Partners Company X			

Abstract

The aim of the thesis was to map out a company's computer network and network equipments, generate a database of the network devices for the company use, analyse the structure of the network and make suggestions as how to improve the strukture and information security in the network. Mapping was done by telephone with local technicians, email and on the spot. The thesis focused on computer networks core- , distribution- and acces layer devices.

As a result the company had a topology of the network and its' devices, locations and state of the equipment and full knowledge of companys computer network and the state of the information security on network devices. Mapping aided the company in redusing the costs and gave ideas in how to improve the network and information security. In addition the thesis brought out deficiensies in the network wich enable DoS-attacks in the network and suggestions how to prevent them.

Keywords

Computer networks, information security, DoS-attack,

Partly classified

SISÄLTÖ

Lyhenteet ja erikoismerkit

Autentikointi = käyttäjän identiteetin tarkistus
bridging loop = verkossa on kaksi OSI-mallin 2-kerroksen reittiä kahden päätepisteen välillä
Cisco = Cisco Systems, yhdysvaltalainen verkkolaitevalmistaja
DNI = Operaattorin käyttämä termi leased-line yhteydelle
Leased line = Yksityinen kuukausihintainen kaksisuuntainen tai symmetrinen yhteys kahden tai useamman kohteen välillä
WAN (Wide Area Network) = tietoverkko joka leviää maantieteellisesti laajalle alueelle
LAN (Local Area Network) = paikallisverkko
EtherChannel = Linkkien yhdistämistekniikka jolla kaksi tai useampi Ethernet-yhteys voidaan yhdistää yhdeksi loogiseksi kokonaisuudeksi.
Ethernet = Verkkoliikennestandardi, joka määrittelee tietoverkoissa käytetyn pakettipohjaisen lähiverkkotekniikan
Konfigurointi = kytkimen asennus. Konfiguraation avulla määritellään kytkimen toiminta
native VLAN
Protokolla = joukko sääntöjä ja toimitatapoja joilla määritelllään liikennöintitapahtuma tietoliikenteessä.
privileged EXEC-mode = salasanasuojattu tila, jossa pystytään tekemään merkittäviä muutoksia laitteeseen
Redundanssi = Viansieto ja toiminnan takaus
Stack = Kytkinpino, jossa on yksi master-kytkin ja muut kytkimet ovat jäsenkytkimiä (member)

1 JOHDANTO

Tietoverkon luotettavuus on tärkeä osa yrityksen toimintavarmuutta ja tuottavuutta. Tämän opinnäytetyön tarkoituksena on kartoittaa, analysoida ja antaa ehdotuksia yrityksen tietoverkon tilan sekä tietoturvan parantamiseksi.

Opinnäytetyössä kartoitetaan yrityksen tietoverkon rakenne ja verkossa olevat laitteet. Kartoitus rajataan koskemaan toimipisteitä, jotka ovat yhteydessä pääkonttoriin dni-yhteydellä. Työssä keskitytään yrityksen core-, distribution- ja access-kerrosten laitteisiin. Kartoituksen lisäksi toimitetaan yrityksen käyttöön verkkotopologian ja tietokanta tietoverkossa olevista verkkolaitteista. Analysoinnin päämääränä on löytää mahdollisia tietoturvaa tai verkon toimintavarmuutta uhkaavia haasteita ja esittää niihin korjausehdotuksia.

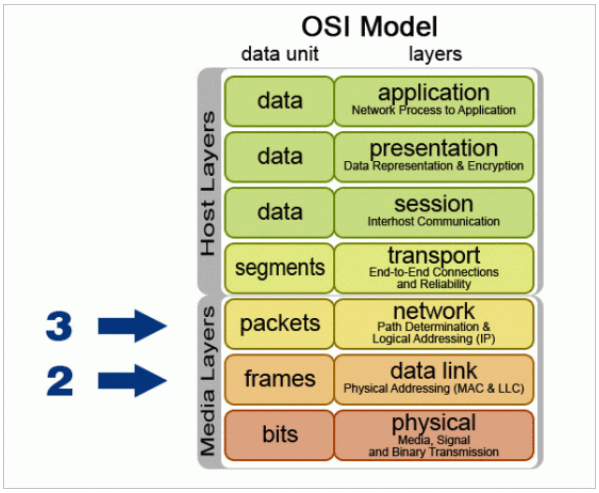
Lopputuloksena pitäisi olla selkeä kuva yrityksen tietoverkon laitteista, sijainnista, tilasta ja yrityksen tietoverkon rakenteesta sekä tietoturvasta. Lisäksi työssä pyritään tuomaan esiin DoS-hyökkäyksiä mahdollistavat puutteet tietoverkossa ja ehdotuksia siitä kuinka hyökkäyksiä voitaisiin estää.

2 TIETOVERKOT

Tietojen välittämiseen voidaan käyttää langatonta lähiverkkoa (tässä Wireless LAN - WLAN) tai langallista verkkoa, joka koostuu useasta point-to-point-linkistä (tässä Ethernet). LAN on yksityinen Ethernet-tietoverkko, jota käytetään yhdistämään toisiinsa erilaisia laitteita sekä vaihtamaan tietoja ja joka on kooltaan rajoitettu. Ethernet-verkon nopeus voi vaihdella 100 Mbps, ja 10 Gbps:n välillä siinä on vähän viiveitä ja virheilyä. (TANENBAUM, A., WETHERALL, D. 2014.)

2.1 OSI-malli

OSI-malli (Open Systems Interconnection) on ollut käytössä jo vuodesta 1984, ja sen alkuperäinen tarkoitus oli luoda joukko standardeja laitteiden valmistajille, jotta laitteet voisivat kommunikoida hyvin keskenään. OSI mallissa on seitsemän kerrosta (kuva 4), joilla jokaisella kerroksella on oma tehtävänsä. Kerrostettu ratkaisu luo useita etuja, kun ongelmien rajaus helpottuu ja uusia protokollia on periaatteessa helppo lisätä kerrostettuun arkkitehtuuriin. (MILLER, R.)



KUVA 1 OSI-malli (SUTTON, G. 2013)

Comment [A1]: ks. ohjeesta, miten kuvat merkitään (otsikon koko, pisteen paikka, viitteen fonttikoko)

Kuviin, taulukoihin ja kuvioihin on AINA VIITATTAVA tekstissä ja asiaa on siis käsiteltävä. Kuva ei voi olla ilman viittausta. Korjaa nämä kaikki, en merkitse jatkossa.

OSI-mallin seitsemän kerrosta ovat seuraavat (OSI-MALLI 2016):

7. Sovelluskerros – kerros, jota sovellukset käyttävät viestintään (application).
6. Esitystapakerros – mm. merkistökoodauksien yhteensovittaminen (presentation).
5. Istuntokerros – yhteydessä kulkevien istuntojen multipleksointi (session).
4. Kuljetuskerros – pakettien välittäminen ja järjestäminen sekä vuonhallinta (transport).
3. Verkkokerros – ylempien kerrosten tietoliikennepaketteja välittäminen tietokoneiden välillä erilaisten verkkoratkaisujen yli (network).
2. Siirtoyhteyskerros – ylempien kerrosten tietoliikennepaketin fyysisen kerroksen kehystäminen siirtoa varten (data link).
1. Fyysinen kerros – Fyysinen media (sähkökaapeli, valokuitu, tms.) bittien siirtämiseen (physical).

2-kerroksella datapaketit kootaan ja puretaan biteiksi. MAC (Media Access Control)-kerros ohjaa tietokoneiden pääsyä verkkoon ja oikeutta välittää tietoja. Lisäksi LLC (Logical Link Control) tarkkailee paketteja, vuota ja virheilyä. 2-kerros on siis vastuussa fyysisestä osoitteistuksesta, virheen korjauksesta ja tiedon valmistelusta siirrettäväksi medialle. 3-kerros on vastuussa kytkennästä ja reitityksestä, ja sillä luodaan reittejä, jotta päätelaitteet voivat lähettää tietoja toisilleen. 3-kerros vastaa reitityksestä, välityksestä, osoitteistuksesta, viankorjauksesta, ruuhkan hallinnasta ja sekvensoinnista. Lisäksi kerroksen vastuulla on looginen osoitteistus sekä IP, ICMP, ARP, RIP ja IGRP reititys. (SUTTON, G. 2013)

Kytkin on laite, joka yhdistää LAN-verkon osia, jotta saadaan muodostettua yhtenäinen OSI-viitemallin 2-kerroksella (siirtoyhteys) toimiva verkko. Usein Ethernet-verkko rakennetaan niin, että jokainen tietokone on kytketty point-to-point-linkillä kytkimen porttiin. Kytkimen tehtävä on välittää paketit verkkoon kytkettyjen koneiden välillä. Suurempien LANien aikaansaamiseksi kytkimiä kytketään toisiinsa niiden porteista. (TANENBAUM, A., WETHERALL, D. 2014; CISCO PRESS 2015.)

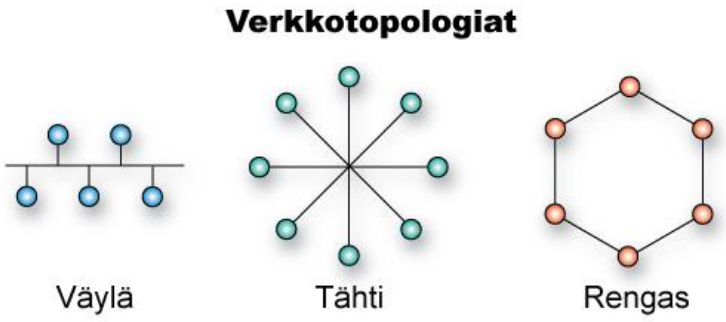
Kytkin tallentaa kytkimen osoitetauluun saapuvan paketin lähettäjän MAC-osoitteen ja portin paketin saapuessa kytkimelle. Sen jälkeen kytkin vertaa paketissa olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää paketin eteenpäin oikeaan porttiin. Mikäli vastaanottajan MAC-osoite ei ole osoitetaulussa tai kyseessä on yleis- tai ryhmälähetys, kytkin lähettää paketin kaikkiin portteihin. Jos vastaanottajan portti on sama kuin lähettäjän portti, paketti hävitetään. (CISCO PRESS 2015.)

2.2 IP-osoite

IP-osoite on 32-bittinen numerosarja, jota käytetään ip-verkkoihin kytkettyjen laitteiden tunnistamiseen. Ip-aliverkon oletusyhdyskäytävä on tietty IP-osoite. Lähetettäessä kehyksiä työasemalta toiselle työasema käyttää ARPia selvittääkseen MAC-osoitteen oletysyhdyskäytävälle. ARP-käännös palauttaa virtuaalisen reitittimen MAC-osoitteen, jotta kehykset voidaan prosessoida ja lähettää eteenpäin. (FRAHIM, E., FROOM, R. 2015, 250–253)

2.3 Verkkotopologia

Tietokoneverkon laitteet voidaan liittää toisiinsa usealla eri tavalla. Fyysisellä topologialla tarkoitetaan sitä, kuinka laitteet on liitetty toisiinsa kaapeleilla. Tarkasteltaessa verkkoa siinä liikkuvan datan kannalta tarkastellaan verkon loogista rakennetta, ei sen fyysistä puolta. Verkon perustopologiat ovat väylä, rengas ja tähti. (VERKKOTOPOLOGIA 2015)

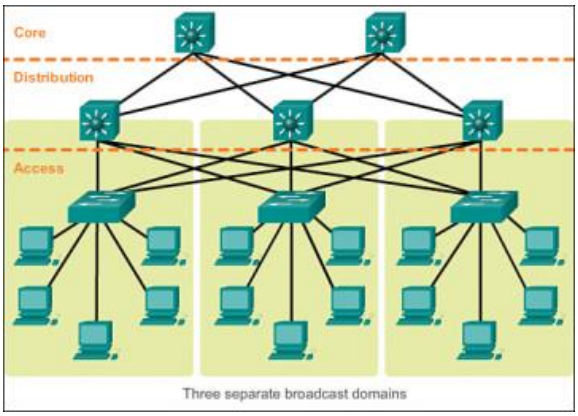


KUVA 2 verkkotopologiat (VERKKOTOPOLOGIA 2015.)

Kuvassa 5 ovat verkkotopologiat, joista väylätopologia on vanhin. Siinä laitteet on kytketty yhteen yhdistävään kaapeliin ja käyttö rajoittuu vain yhdelle laitteelle kerrallaan. Mikäli muut laitteet pyrkivät viestimään väylää pitkin tapahtuu törmäyksiä ja verkko ruuhkautuu. Rengastopologiassa verkosta on muodostettu rengas, joka jokaisessa solmussa on verkkolaite. Verkkolaitteet yhdistyvät verkkoon erillisellä MAU-yksiköllä. Rengasrakenteessa jokaisella verkkolaiteella on kaksi naapuria ja yksi laite kerrallaan käyttää rengasta lähettämään sanoman. Tähtitopologiassa on keskuslaite, johon muut verkon laitteet on kytketty. Tähtitopologia on yleisin käytössä oleva topologia Ethernet-verkoissa. Laajennettu tähtitopologia lisää tähtitopologiaan hierarkian.
(VERKKOTOPOLOGIA 2015)

2.4 Hierarkkinen tietoverkko

Hierarkkinen tietoverkko koostuu kolmesta eri kerroksesta, core-, distribution- ja access-kerros. Jokaisella kerroksella on oma tehtävänsä. Sen lisäksi hierarkkinen tietoverkko jakaa verkon yleislähetysalueisiin (broadcast domain). Paikalliseksi tarkoitettu liikenne pysyy yleislähetysalueella; ainoastaan muihin verkonosiin tarkoitettu liikenne poistuu yleislähetysalueelta. Kuvassa 6 tietoverkko on jaettu kolmeen eri broadcast domainiin. (CISCO PRESS 2014.)



KUVA 3 Hierarkkisen tietoverkon kerrokset. (Cisco Press 2014.)

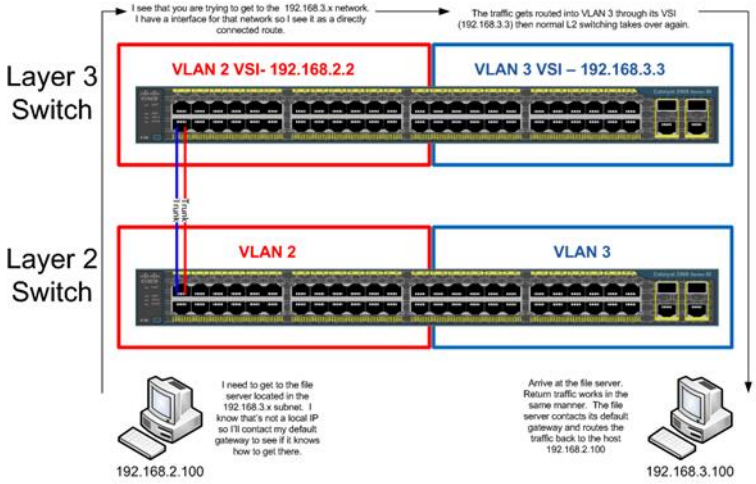
Access-kerroksen tehtävä on luoda mahdollisuus käyttäjille päästä kiinni verkkoon ja siellä oleviin resursseihin. LAN-verkoissa Access-kerroksen kytkimiin liitetään erilaisia laitteita, kuten tietokoneita, tulostimia ja access-points. Access-kerrosta ovat myös sivukonttorit, jotka yhdistyvät pääkonttoriin WAN-yhteydellä. (CISCO PRESS 2014.)

Distribution-kerros liittää yhteen access-tason kytkimet LANissa esimerkiksi laitetilassa. WAN-ympäristössä distribution-kerros liittää yhteen WAN-yhteydet ja luo linjaukset yhteyksille (policy based connectivity). Sen tehtävä on taata yhteys kampusverkolle. (CISCO PRESS 2014.)

Core, jota sanotaan myös tietoverkon selkärangaksi, reitittää paketteja eteenpäin niin nopeasti kuin mahdollista. Sen pitäisi pystyä sopeutumaan muutoksiin nopeasti ja säilyttää silti toimintakykynsä. (CISCO PRESS 2014.)

2.5 2- ja 3- kerroksen kytkimet

Molempien kerrosten kytkimet pyrkivät mahdollisimman nopeaan kytkentään lähettävän laitteen ja kohteen välillä. 2- kerroksen kytkimet käyttävät tähän tarkoitukseen kytkimeen kytkettyjen laitteiden MAC-osoitteita, kun taas 3-kerroksen kytkimet tekevät saman IP-osoitteen perusteella. 2-kerroksen kytkimet pystyvät välittämään paketteja yhden tietoverkon sisällä linjan nopeudella, mutta ne eivät voi priorisoida liikennettä tai taata linjan nopeutta. 3-kerroksen kytkimillä voidaan yhdistää eri tietoverkon osia toisiinsa ja niiden avulla voidaan erotella verkkoa osiin (VLANit). Kytkimissä käytetään usein topologiaperusteista mallia, jossa kytkin rakentaa kytkentätaulukon koko verkosta ja toimittaa paketit perille taulukon IP-osoitetietojen perusteella. Kuvassa 7 tuodaan esiin kytkennän eroavaisuuksia 2- ja 3-kerroksen välillä. (ROUTER-SWITCH.COM 2016)



KUVA 4 eroavaisuudet 2- ja 3- kerroksen kytkennässä (ROUTER-SWITCH.COM 2016)

Cisco Catalyst 2950 ja 2960 ovat tyypillisiä 2-kerroksen kytkimiä, kun taas Cisco Catalyst 3550, 3560, 4500 ja 6500 ovat 3- kerroksen kytkimiä (ROUTER-SWITCH.COM 2016).

3 KARTOITUS JA OPTIMOINTI

Tehtävänä oli selvittää yrityksen tietoverkon rakenne ja verkossa olevat laitteet, toimittaa yrityksen käyttöön verkkotopologia ja tietokanta laitteista. Kartoituksen tarkoituksena oli löytää mahdollisia tietoturvaa tai verkon toimintavarmuutta uhkaavia haasteita ja esittää niihin korjausehdotuksia.

Tietoverkkoon voidaan tehdä muutoksia kahdella eri tavalla: ad-hoc-tyylillä tai suunnitelmallisesti. Ad-hoc-lähestymistavassa määritellään tarve muutokselle ja tehdään haluttu muutos ilman suunnittelua. Tällöin monet muutokset, kuten osoitteistus, reititys ja turvallisuus, konfiguroidaan tarpeen mukaan laitteiden lisääntyessä tai tehtäessä verkkoon muutoksia.

Suunnitelmallisessa lähestymistavassa määritellään tarve muutokselle ja kaikki aloitetaan suunnittelulla. Nykyisen topologian perusteella selvitetään mahdollisia tilanteita joita muutokset voivat aiheuttaa. Tämän jälkeen luodaan suunnitelma ja toimintamalli, joka voi sisältää esimerkiksi muutoksia topologiaan, IP-osoitteisiin, ratkaisuja skaalautuvuusongelmiin, parannuksia linkkien käyttöön ja muihin mahdollisiin verkkoparametreihin. Kaikki yksityiskohdat dokumentoidaan ennen muutosten tekoa. Tietoverkkokohtaiseen informaatioon kuuluvat tietoverkon nykyinen topologia, laitteet ja ohjelmistoversiot, IP-osoitesuunnitelma, skaalautumisvaatimukset (summarointi, stub-alueet jne.), lista mainostetuista verkoista, linkkien käyttö ja vaihtoehtoisten linkkien ominaisuudet. (TEARE, D. 2014, s. 13–16.)

Suunnitelmaa varten

- määritellään asiakkaan tarpeet
- kuvaillaan nykyinen verkko
- suunnitellaan verkkotopologia ja ratkaisut.

Yritykselläei ollut tarvetta tällä hetkellä tehdä muutoksia, mutta IT-päällikkö mielestä oli aika kartoittaa laitteet ja rakenteet, jotta ongelmien sattuessa ja muutoksia tehtäessä voitaisiin jatkossa toimia suunnitelmallisesti ja ottaa huomioon eri vaihtoehdot. Asiakkaan toiveena oli, että työn valmistuttua yritykse käytössä olisi Excel-tietokanta verkkolaitteista dni-yhteydellä olevissa toimipisteissä.

Aloitin kartoituksen yhdessä IT-henkilöiden kanssa ja sain alustavia tietoja yrityksen verkosta. Sain tarkat tiedot yhden toimipisteen laitteista ja tiedon siitä, että jokaisessa dni-yhteydellä toteutetussa toimipisteessä on operaattorin toimittama tai hallinnoima laite, jonka takana oleva verkko ei ole kenenkään kartoittama eikä IT-yksikön hallinnassa. Jokaisessa toimipisteessä on toimipisteen oma henkilökunta laittanut access-kerroksen verkkolaitteet yrityksen verkkoon ja niistä haluttiin saada tarkempi tieto. Tätä varten sain yhteyshenkilöt kuhunkin toimipisteeseen. Sain tietoja sähköpostitse

ja puhelimitse. Mikäli verkko vaikutti monimutkaisemmalta tai selvitys oli mielestäni epäselvä, kävin paikalla henkilökohtaisesti kartoittamassa verkon.

Yrityksen tietoverkkoon on tehty muutoksia pikkuhiljaa ja perittyjä laitteita on lisätty jo olemassa olevaan verkkoon. Muutokset on tehty kiireessä osittain ad-hoc-tyylillä. Nopeasti ilmeni, että ainakin osa operaattorin laitteisiin kytketyistä verkossa olevista laitteista, olivat olleet sinne asennettuna jo kauan ja ne oli suojattu salasanalla, mutta kenelläkään ei ollut tietoa salasanasta. Näissä tapauksissa täytyisi salasana murtaa, jotta päästäisiin katsomaan, mitä muita konfiguraatioita laitteilta löytyi,. Ongelmana oli kuitenkin se, että verkko on tuotantokäytössä ja riski yhteyksien häviämiselle on suuri, mikäli salasanan murtamisen yhteydessä tietoja katoaisi.

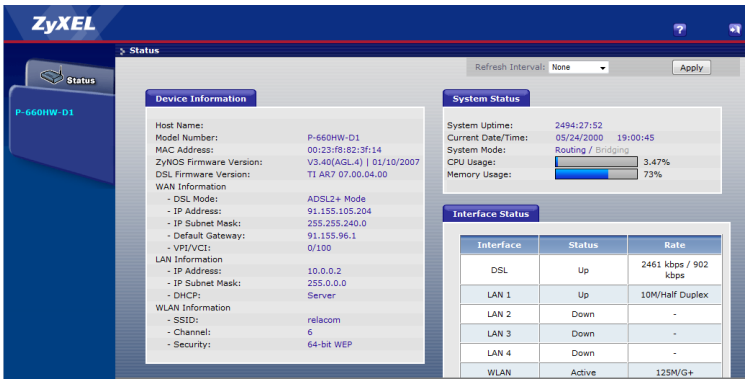
Laitekanta muissa kuin päätoimipisteissä on hieman vanhentunutta. Suurimmaksi osaksi laitteisto koostui dni-yhteyksien päässä Ciscon Catalyst 2960 -kytkimistä, mutta joillakin paikkakunnilla oli myös vanhempaa mallia. Laitteisto toimi hyvin ja on toiminut ilman ongelmia, mutta laitteita voisi päivittää hieman uudempaan.

Kaikkiin laitteisiin ei oltu konfiguroitu salasanoja, joten niistä saatujen tietojen pohjalta päättelin, että laitteille oli laitettu bannerit ja salasana, mutta muita konfiguraatioita laitteilta ei todennäköisesti löydy. Viikoittaisessa tilannekatsauksessa IT-päällikön kanssa sovimme, että toimitan laitetiedot niiltä osin, kuin ne ovat saatavissa, toisin sanoen laitteet ja niiden mallit jokaiselta paikkakunnalta. Tarkemman analyysin tein niiden laitteiden kohdalta, joissa konfigurointeja oli. Keräsin tiedot ja kokosin tietojen pohjalta topologian. Topologiaan merkitsin kunkin paikkakunnan verkossa olevat laitteet ja IP-aliverkon.

Päätoimipisteiden osalta sain muutamien kytkimien running configit etukäteen, jotta pystyin tutustumaan hieman siihen, mitä laitteille on konfiguroituna. Tutkittuani niitä, huomasin että saadakseni paremman kokonaiskuvan joudun ottamaan laitteilta muitakin tietoja. Tämä onnistui parhaiten menemällä paikalle tutkimaan laitteiden kokoonpanoja. Erään toimipisteen laitteisiin oli kaikkiin määritelty telnet-yhteys ja sille salasana, jonka avulla pääsin laitteisiin tutustumaan. Projektipäällikkö tuli paikalle auttamaan kartoituksessa ja vastailemaan kysymyksiini. Otin laitteilta useita eri tietoja erilaisilla show-komennoilla konfiguraatoiden määrittämiseksi, tarkistin kytkinten väliset linkit ja saadun topologian paikkansa pitävyyden. Täydensin verkkotopologiaan kaikkien dni-yhteyksillä toimivien paikkakuntien verkon rakenteen.

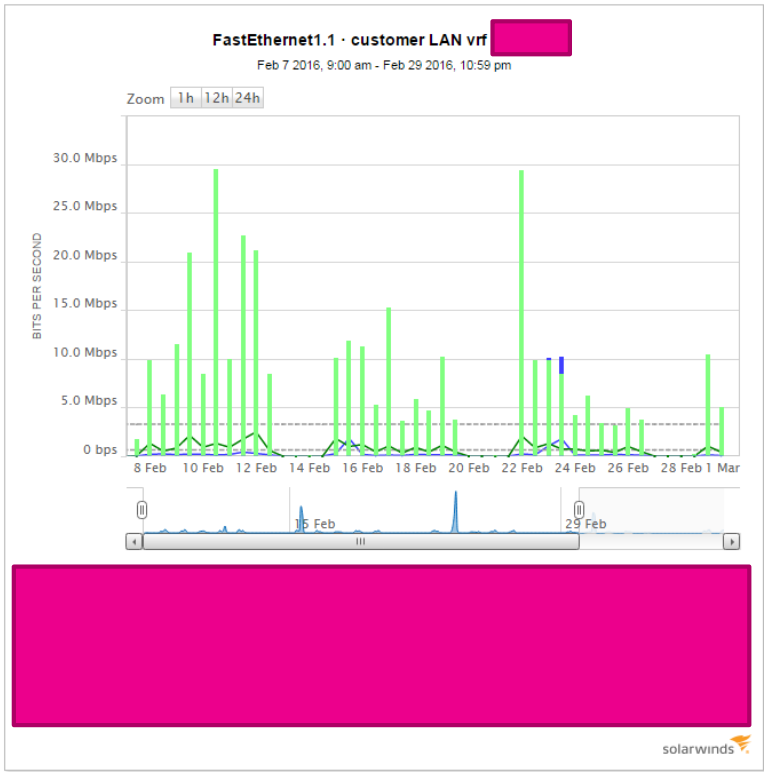
Tarkistuksessa ilmeni, että osa laitteista, jotka saadussa topologiassa oli, ei ollut kytkettyinä verkkoon ja siltä osin piirsin topologian uudelleen. Kytkinten väliset linkit oli muuten dokumentoitu oikein. Palvelimet eivät topologiassa olleet nähtävissä, joten merkitsin myös ne selvyyden vuoksi kuvaan. Portit olivat kaikki GigabitEthernet-portteja, joten niiden nopeus on 1 G. Päätoimipisteen yhteyden nopeus on 30 Mbit, joten tiedonsiirron nopeudessa rajoitusta ei luo sisäverkko vaan pullonkaula on päätoimipisteen yhteydessä.

Joitakin kuluttajaliittymiä oli eri paikkakunnille otettu käyttöön omatoimisesti. Kuvassa 10 oleva laite oli eräällä paikkakunnalla yleisesti käytössä ja julkisella SSID:llä löydettävissä. Laitteessa olivat edelleen oletussalasanat, jotka löytyivät internetistä ja kuten kuvasta näkyy, jaetun verkon salaus WEP ei ole paras mahdollinen. Tällaiset hallitsemattomat verkkolaitteet ovat suuri riski yrityksen tietoturvalle. Samaisessa toimipisteessä yrityksen verkko oli jaettu valmiiksi tiloihin ja kytketty portteihin, joten kuka vain tiloissa liikkuvista henkilöistä pääsisi suoraan käsiksi yrityksen verkkoon. Kuluttajaliittymä oli myös jaettu valmiiksi neuvottelutiloihin. Eri verkot oli merkitty erivärisin johdoin ja tiloissa liikkuville ulkopuolisille henkilöille ohjeistetaan käyttämään tietyn värisiä johtoja internetyhteytenään. Ohjeistus on hyvä ja toteutus selkeä, mutta jos joku haluaa tietoisesti tehdä haittaa verkolle, ohjeet voidaan jättää huomiotta.



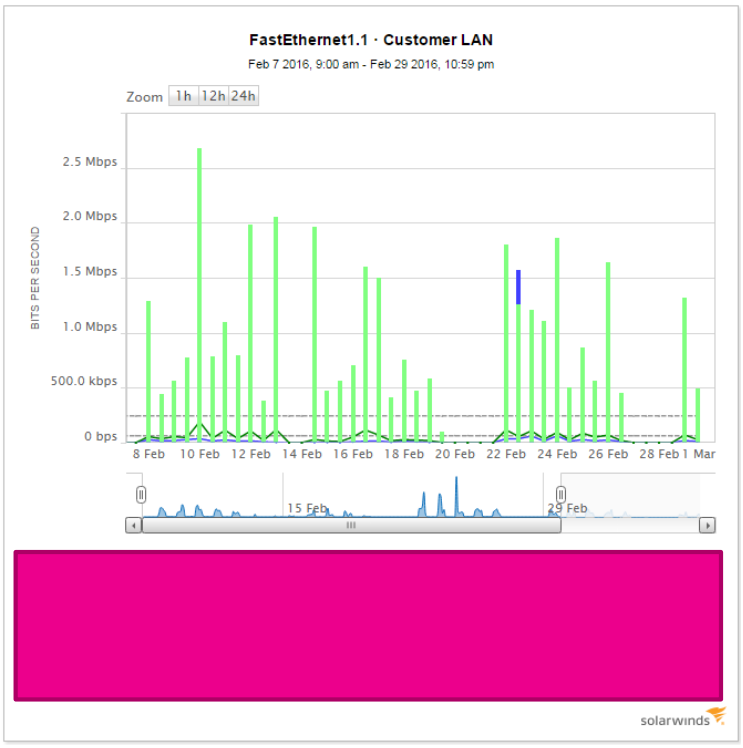
KUVA 5 kuluttajaliittymän konfiguraatiot

Yrityksen verkossa ovat käytössä a-luokan osoitteet ja osoitetiedot tulevat valmiiksi annettuina. Myös käytettävät VLANit ja palomuurien säännöt on määrätty valmiiksi. Yrityksen verkkoa hallitaan ja seurataan toisesta yrityksestä, joten jouduin pyytämään tiedot dni-yhteyksien verkkojen käytöstä sieltä. Sain seurannan ajalta 8.2.–1.3.2016 ja tietojen pohjalta kävin läpi paikkakunnittain yhteyksien nopeuden ja sen ovatko varatut yhteydet riittävät tai oliko jossain ylikapasiteettia. Kuvissa 11-13 on muutamia esimerkkejä saaduista otannoista. Huiput näkyvät kuvassa vihreänä pylväänä ja keskimääräiset lähetys ja vastaanottonopeudet viivana. Seuranta on tehty 24 tunnin ajalta, joten kertomalla kolmella keskimääräisen lähetys- ja vastaanottomäärän saamme todellisemman kuvan kaistan käytöstä.



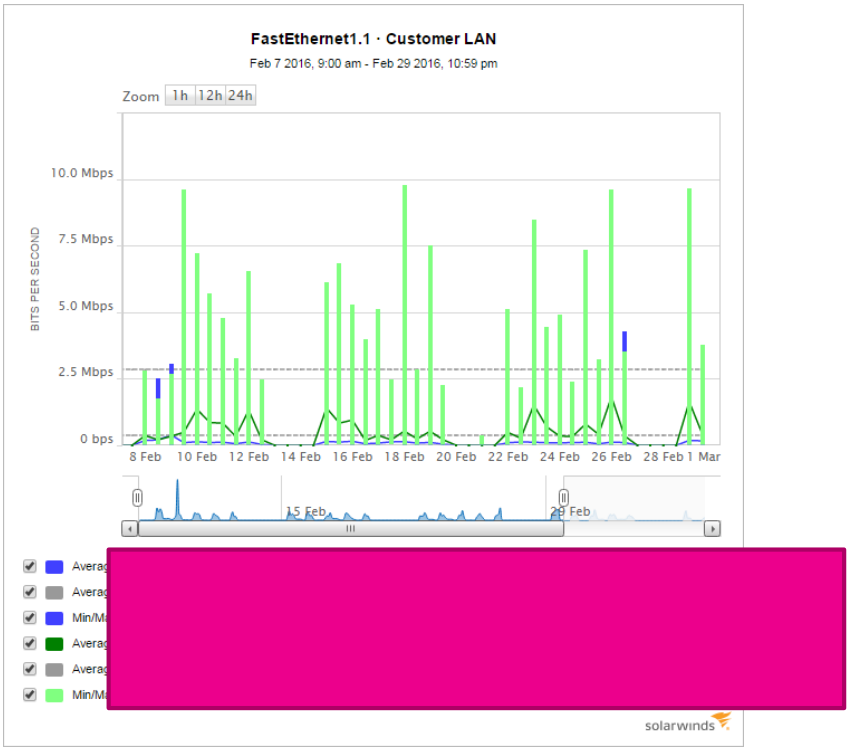
KUVA 6 toimipiste 1 dni-yhteys: datan käyttö

Kuvassa 11 on toimipiste 1 yhteyden käyttö seurannan aikana. Yhteyden nopeus on tällä hetkellä 10Mbit. Huippujen ja keskinopeuksien perusteella heidän yhteytensä voi olla aika-ajoin ruuhkautunut, huiput käyvät parhaillaan jopa 30Mbps:ssä. Tässä tilanteessa kannattaisi käyttäjiltä kysellä, ovatko he kokeneet hitautta yhteyksissä ja tarpeen mukaan nostaa nopeutta.



KUVA 7 toimipiste 2 dni-yhteys: datan käyttö

Joissakin tapauksissa (kuva 12) huomasin, että käytössä oleva kaista on ylimitoitettu. Toimipiste 2:n nykyinen kaistan nopeus on 10 Mbit ja käyttö ei edes huipuissa käy yli 3 Mbit. Tällöin voidaan säästöä hakea laskemalla kaistan nopeutta.



KUVA 8 toimipiste 3 dni-yhteys: datan käyttö

Toimipiste 3:n yhteyden nopeus on 10Mbit. Huiput käyvät usean kerran tarkasteluajan jakson aikana lähellä maksimeja ja keskimääräinen kaistan käyttö lähentelee myös rajoja. Tässä tapauksessa kannattaisi pyytää seurantaa pidemmältä ajalta ja kysellä käyttäjäkokemuksia, jotta voidaan kartoittaa onko nopeuden nostolle tarvetta.

Liittymien käytön kartoituksessa selvisi myös, että joillakin paikkakunnilla kuluttajaliittymä oli ainoa käytössä oleva liittymä vaikka sinne maksettiin myös operaattorin dni-yhteydestä. Näissä tilanteissa kartoituksella saavutettiin säästöjä, sillä ylimääräinen yhteys voitiin katkaista.

WAN-osa yrityksen verkosta on operaattorin ylläpidossa, joka on liittymien toimittaja. Mikäli operaattorin hallinnoima kytkin hajoaa jossakin ylläpidon alaisessa toimipisteessä, paikallinen alihankkija käy korjaamassa tai vaihtamassa laitteen. Liittymät ovat normaalissa yritysliittymäylläpidossa, jolle on tehty oma sopimus.

3.1 Verkkolaitteiden tietoturva

Katsauksessa ilmeni, että usein kytkimille ei ole omaa laitetilaa vaan laitteet saattavat olla toimistotiloissa avoimesti kaikkien kulkijoiden tavoitettavissa. Aina ei ole perusteltua tai kustannustehokasta rakentaa jokaiseen toimipisteeseen omaa lukollista laitetilaa, mutta tällöin olisi hyvä sijoittaa laitteet, niin että ne ovat lukollisessa kaapissa, jonka avain on jonkun luotettavan henkilön hallinnassa. Joillakin paikkakunnilla laitetilaan pääsy oli hyvin valvottu ja avaimia oli vain muutamalla henkilöllä. Laiterikon sattuessa näiden henkilöiden poissa ollessa, voi korjaus hidastua tarpeettomasti ilman sisäänpääsyä.

3.1.1 Salasanat

Salasanojen käyttö ja oikeuksien määrääminen on helpoin tapa hallita terminaali yhteyksiä tietoverkossa. Staattisella salasanalla kontrolloidaan pääsyä privileged EXEC-modeen, mutta lisäturvaksi on hyvä laittaa ”Enable”-salasana. Ilman ”enable secred” – komentoa salasana on kuitenkin nähtävissä selkokielisenä running configissa. (CISCOc.)
Kirjautumis- ja enable-salasana, jolla päästään exec-modeen kytkimellä, oli laitteille päätoimipisteissä konfiguroitu, mutta ne näkyivät running configissa selkokielisenä (Liite 1). Lisäturvan saavuttamiseksi voisi kytkimille lisätä ”enable secret”-komennon. Muilla paikkakunnilla laitteille oli laitettu salasanat, mutta niitä ei ole dokumentoitu, joten henkilöstön vaihtuessa tieto niistä on kadonnut. Jatkossa salasanat olisi hyvä keskittää muutaman henkilön hallintaa, ne voisi yhdenmukaistaa ja niitä kannattaisi vaihtaa aika ajoin.

3.1.2 Käyttöjärjestelmä päivitykset

Kaikissa tutkituissa laitteissa on alkuperäinen käyttöjärjestelmä 12.2. Tämän jälkeen on julkaistu useita eri päivityksiä, joilla on korjattu erilaisia tietoturvauhkia. Ciscolla on olemassa erillinen käyttöjärjestelmän tarkistustyökalu (kuva 14), jolla voidaan tarkistaa jokaisen käyttöjärjestelmän osalta mitä päivityksiä käyttöjärjestelmään on saatavissa. (CISCOa.)

KUVA 9 Cisco käyttöjärjestelmä päivitystyökalu (CISCOa.)

Kuvassa 15 on ote mitä päivityksiä esimerkiksi on saatavissa 12.2 käyttöjärjestelmään. Päivityksiä on saatavissa vuodesta 2004 saakka ja niissä on myös viestintäviraston suosittelemia päivityksiä.

Cisco IOS Software release(s)	Results for all previously published Cisco Security Advisories		
12.2(1)	Security Advisories That Affect This Release	Publication Date	First Fixed
12.2(1)	Multiple Vulnerabilities in ntpd (April 2015) Affecting Cisco Products	2015 Apr 08	15.2(4)M9
	Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerability	2015 Mar 25	15.2(4)M8
	Cisco IOS Software Network Address Translation Vulnerabilities	2014 Mar 26	15.1(4)M8
	Cisco IOS Software DHCP Denial of Service Vulnerability	2013 Sep 25	15.1(4)M7
	Cisco IOS Software Multicast Network Time Protocol Denial of Service Vulnerability	2013 Sep 25	12.4(20)T
	OSPF LSA Manipulation Vulnerability in Multiple Cisco Products	2013 Aug 01	15.1(4)M7
	Cisco IOS Internet Key Exchange Vulnerability	2012 Mar 28	12.4(25g)
	Cisco IOS Software Multicast Source Discovery Protocol Vulnerability	2012 Mar 28	12.4(25g)
	Cisco IOS Software Data-Link Switching Vulnerability	2011 Sep 28	12.4(25e)
	Cisco IOS Software Network Address Translation Vulnerabilities	2011 Sep 28	12.4(25f)
	Cisco IOS Software H.323 Denial of Service Vulnerabilities	2010 Sep 22	12.4(25d)
	Cisco IOS Software Authentication Proxy Vulnerability	2009 Sep 23	12.4(23a) 12.4(25a)
	Cisco IOS Software Tunnels Vulnerability	2009 Sep 23	12.4(23b) 12.4(25b)
	TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products	2009 Sep 08	12.4(18e) 12.4(23a) 12.4(25)
	Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability	2009 Mar 25	12.4(18e) 12.4(23)
	Cisco IOS Software Multiple Features IP Sockets Vulnerability	2009 Mar 25	12.4(18a) 12.4(19)
	Cisco IOS HTTP Server Ping Parameter Cross-Site Scripting Vulnerability	2009 Jan 14	12.4(18e) 12.4(23)
	Multiple Multicast Vulnerabilities in Cisco IOS Software	2008 Sep 24	12.2(26c) 12.2(27c) 12.2(28d) 12.2(29b) 12.2(46)
	Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks	2008 Jul 08	12.4(18b) 12.4(21)
	SNMP Version 3 Authentication Vulnerabilities	2008 Jun 10	12.2(26c) 12.2(27c)

KUVA 10 Ote käyttöjärjestelmään 12.2. saatavista päivityksistä (CISCOa).

Huomioitava on ennen ohjelmistojen päivittämistä, että kaikkia laitteita ei esimerkiksi muistikapasiteetin vuoksi voi päivittää uusimpaan versioon ja sopiva versio on tarkistettava laitteittain. Esimerkiksi Catalyst 2960 -laitteet voi päivittää versioon 12.4.

3.1.3 Siirtoyhteyskerrosten tunnistusprotokolla CDP

CDP on protokolla, jota Ciscon laitteet käyttävät tietojen vaihtamiseen keskenään ja se on automaattisesti päällä kaikilla laitteilla (FRAHIM, E., FROOM, R. 2015, 352). CDP antaa tietoja laitteesta kuten ohjelmistoversio, IP-osoite, alusta, kapasiteetti ja natise VLAN. Hyökkääjä voi suorittaa hyökkäyksen lähettämällä laitteelle virheellisiä CDP-paketteja ja saada niihin vastauksen naapurin laitetiedoilla. Hyökkäys voidaan tehdä myös telnet- tai SNMP-yhteydellä, joten suoraa yhteyttä laitteelle ei välttämättä tarvita. (POPESKIC, V. 2016.)

Kaikissa yrityksen kytkimissä on päällä CDP kaikissa porteissa. Laitteesta, johon ei ole salasanaa, voi silti saada tietoja. Näiden tietojen avulla hyökkääjä pystyy halutessaan erilaisia internetistä vapaasti

saatavia ohjelmia hyödyntäen suorittamaan Dos-hyökkäyksiä. CDP -yökkäyksiltä voidaan suojautua kytkemällä se pois niiltä porteilta, missä sitä ei tarvita.

3.1.4 Hallintayhteydet telnet, ssh ja vty

Dni-yhteyksien päässä olleet yrityksen laitteet eivät olleet etähallittavia ja jokaisessa toimipisteessä oli tehty omia ratkaisuja laitteiden korvaamiseksi laiterikkojen sattuessa. Näkisin, että laitehallinta kannattaisi keskittää yhden organisaation (tässä tapauksessa) IT-hallinnon alaisuuteen. Jotta laiterikon sattuessa voitaisiin paikkakunnilla kuitenkin toimia nopeasti ja verkkoliikenteen toimimattomuusaika saataisiin minimoitua, laitteet voitaisiin jatkossakin korvata paikallisilla laitteilla. IT-osastolla olisi kuitenkin oltava valmiina tekstimuotoinen tiedosto konfiguraatioista, joka voitaisiin etäyhteyden kautta laittaa uudelle kytkimelle, jotta konfigurointi ei vaadi erityisosaamista paikkakunnalta. Etäyhteyttä varten paikkakunnille voisi toimittaa sähköpostitse IP-osoitetiedot teksitimuotoisena konfiguroitavaksi, jotta laitteeseen pääsee kiinni. Sen jälkeen lisätään muut konfiguraatiot. Eri paikkakunnille pitäisi toimittaa selkeät ohjeet laiterikkoja varten sekä selkeästi tuoda ilmi, ettei laitteita ilman IT-osaston lupaa ja konfigurointia enää lisätä verkkoon.

SSH-yhteys (Secure Shell) on käytössä olevaa telnet-yhteyttä salatumpi etähallinnan muoto ja sen käyttö etähallinnassa olisi suositellumpi tapa hoitaa dni-yhteyksien päässä olevia kytkimiä. Luultavasti SSH-yhteys täytyisi kuitenkin ensin sallia kaikissa operaattorin hallinnoimissa kytkimissä, kuitenkin vain yrityksen verkon laitteista, jotta sitä voitaisiin käyttää. Sen jälkeen SSH-yhteys olisi konfiguroitava jokaiselle laitteelle. SSH versiosta 1 on löydetty tietoturvariskejä, joten käytettäväksi olisi hyvä valita versio 2. (FRAHIM, E., FROOM, R. 2015, s. 413.)

SSH-yhteyden käyttöön oton jälkeen kaikilta kytkimiltä pitäisi poistaa telnet-yhteyden mahdollisuus, sillä telnet-yhteydessä liikenne ei ole suojattu, vaan siinä kulkevat kaikki tiedot (esim. käytettävät salasanat ja käyttäjätunnukset) selkokielisenä. Mikäli joku saa kaapattua yhteyden, hän saa myös tietoonsa laitteissa käytettävät tunnukset. Lisäksi olisi suotavaa kytkeä pois päältä web interface-hallinta, mikäli kytkimiä ei hallita sen kautta. Komento ”no ip http server” kytkee pois päältä kytkimen web interfacen. Mikäli hallintaan halutaan kuitenkin käyttää web interfacea, käytettäväksi suositellaan HTTPS-yhteyttä HTTPn sijaan, sillä silloin liikenne on salattua. Sama koskee SNMP-hallintaa; mikäli sen käyttö ei ole välttämätöntä, poistetaan se käytöstä kaikilta kytkimiltä. Jos SNMP-hallintaa kuitenkin halutaan käyttää, suositellaan käytettäväksi SNMPv3-yhteyttä, joka mahdollistaa autentikoitumisen. (FRAHIM, E., FROOM, R. 2015, s. 413.)

Vty-yhteydet tulisi sallia vain tietyistä IP-osoitteista, salasanat vty-yhteydelle oli konfiguroitu.

Comment [A2]: suora käännös on-sanasta. Suomessa ei käytetä. Voidaan korvata tilanteen mukaan eri keinoin (kytkeä, olla käytössä, sytyttää jne.)

Comment [A3]: väli ennen viivaa. Tarkista ja korjaa vastaavat, en merkitse jatkossa.

Comment [A4]: tarkista nämä, en merkitse jatkossa. Tässäkään koko sanaa ei edes tarvita.

Comment [A5]: :n

Comment [A6]: piste

3.2 VLAN

VLAN on yleislähetysalue, joka voi levittyä useille eri LAN-segmenteille. VLANeilla voidaan tietoverkossa luoda segmentaatiota, turvallisuutta ja tietoverkon joustavuutta. Tietoverkossa (switched network) VLANien avulla voidaan rajata 2- kerroksen yleislähetyksiä, jotka kuluttavat verkon resursseja, VLANin sisäisiksi, jolloin ne eivät heikennä koko verkon suorityskykyä. VLANien ollessa käytössä kytkimellä, vain samassa VLANissa olevat laitteet voivat kommunikoida keskenään. Kommunikoidakseen eri VLANien välillä pakettien täytyy mennä joko reitittimen tai 3-kerroksen kytkimen kautta. (FRAHIM, E., FROOM, R. 2015, 42–43.)

Comment [A7]: luoda turvallisuutta?

Comment [A8]: pilkku pois, alussa lauseenvastike. Tarkista kaikki, en enää merkitse jatkossa

Hierarkkisessa tietoverkossa VLANit voidaan suunnitella kahdella eri tavalla: end-to-end VLAN tai local VLANit. Molempien mallien käyttöön on omat syynsä. Trunk-linjat ovat linkkejä kytkinten välillä, jotka kuljettavat tietoja useista eri VLANeista. Trunk-linjoja käytetään, jotta koko verkossa voidaan toimia 2-kerroksen operaatioilla. Esimerkiksi end-to-end VLANit tarvitsevat toimiakseen trunk-linjan. Linjan toimintaan trunk-tilassa kahden kytkimen välillä, vaaditaan sen molempien päiden konfigurointi. Trunk-linjat käyttävät VLAN IDtä erottamaan paketit eri VLANien välillä. Trunk-linjojen konfiguroinnisa voidaan käyttää kahta eri teknologiaa, Inter-Switch Link (ISL) tai IEE 802.1Q. Näistä suositeltavampi on IEEE802.1Q. Jotta kehykset ilman VID-tunnusta pääsevät perille määränpäähänsä trunk-linjojen yli, molempiin päihin täytyy konfiguroida sama native VLAN. (FRAHIM, E., FROOM, R. 2015, 49–51.)

Comment [A9]: mihin viittaa?

Comment [A10]: pois

Comment [A11]: ID:tä

End-to-End VLAN

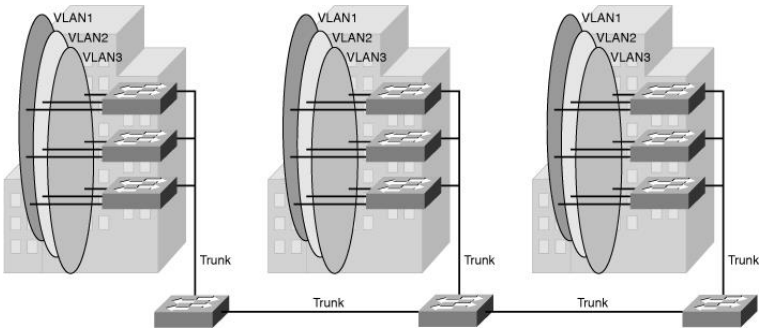
End-to-end VLANilla tarkoitetaan VLANia, joka leviää koko verkon alueelle useille kytkimille. Tällöinen tietoverkko kuljettaa paketteja koko verkon läpi kuten kuvassa. Tyypillistä tälle mallille on, että VLAN levittyy koko verkon alueelle ja käyttäjät ryhmitellään kuulumaan tiettyyn VLANiin enemmänkin hallinnollisista syistä, kuin fyysisestä sijainnista johtuen. Vaikka käyttäjä vaihtaisi eri paikkaan kampuksella, VLAN säilyy samana. Trunk-linjoja käytetään liikennöintiin eri kytkinten välillä kaikkien eri VLANien tietojen kuljettamiseen. (LONG, H. 2006)

Comment [A12]: ?

Comment [A13]: numero

Comment [A14]: pois

Comment [A15]: johtuen on aina väärä. Tässä voi vain jättää pois .

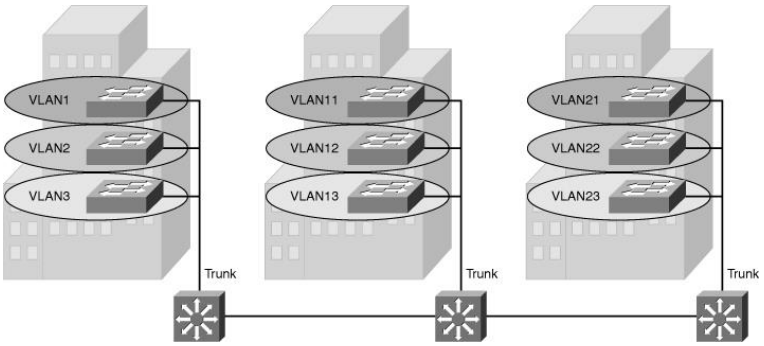


KUVA 11 End-to-end VLAN (LONG, H. 2006)

Siirryin sivulle 30.

Local-VLAN

Tässä mallissa käyttäjät jaotellaan ryhmiin sijainnin, ei tehtävän perusteella. VLANit ovat siis paikallisia yhdellä kytkimellä ja ne yhdistetään trunk-linjalla distribution-kerroksen kytkimeen. Mikäli käyttäjä vaihtaa paikkaa, hänen VLAN jäsenyytensä muuttuu samalla uuden sijainnin mukaan. Paikallisissa Vlaneissa 2-kerroksen kytkentä tapahtuu Access-kerroksella ja reititys distribuution- sekä Core-kerroksella, jotta käyttäjät voivat käyttää tarvitsemiaan resursseja. vaihtoehtoisesti reititys voidaan laajentaa koskemaan myös Access-kerrosta, jolloin linkit Access ja distribuution- kytkimien välillä ovat reititettyjä. (FRAHIM, E., FROOM, R. 2015, s. 45–46)



KUVA 12 Local-VLANs (LONG, H. 2006)

End-to-End VLANilla voidaan ryhmittää käyttäjiä sijainnista riippumatta IP-osoitteen perusteella. End-to-End VLANit luovat myös turvallisuutta, sillä kaikki käyttäjät eivät tarvitse pääsyä kaikkiin verkon osiin tai liikennettä voidaan rajata VLANien sisällä. Palvelujen tasoa voidaan myös määritellä VLAN-pohjaisesti, jolloin tietyssä VLANissa olevalle käyttäjäryhmälle taataan esimerkiksi etuoikeutetumpi pääsy verkon resursseihin. Tämä on tietenkin mahdollista toteuttaa myös ilman VLANeja. Mikäli jonkin käyttäjäryhmän liikenne on suurimmalta osalta liikennettä ryhmän sisällä, end-to-end VLANien käyttö on suositeltavaa, vaikka VLAN jakautuisikin useammalle kytkimelle. End-to-end VLANia voidaan käyttää myös siitä syystä, että sillä on oma erikoistarkoituksensa. Esimerkiksi vieraat voidaan haluta jakaa omaan VLANiinsa, jotta he eivät pääse käyttämään koko verkon resursseja. Yksi syy end-to-end VLANien käyttöön voi myös olla se, että verkko on jo konfiguroitu ja käytössä ja sen ylläpitäjät ovat haluttomia tekemään muutoksia muutoksiin tarvittavasta verkon alasajosta tai poliittisista syistä johtuen. (FRAHIM, E., FROOM, R. 2015, s. 46–47)

Kytkin, jolle päättyy useita VLANeja, yleensä distribution-kytkin, tarvitsee keinoja välittääkseen liikennettä VLANien välillä OSI-mallin 3-kerroksella. Tähän tarkoitukseen voidaan käyttää joko reititintä tai monikerroksista kytkintä. Koska yrityksen verkossa käytetään monikerroksista kytkintä tähän tehtävään, tietojen välittämiseen käytetään SVI:tä. (FRAHIM, E., FROOM, R. 2015, s. 204–205.)

3.3 SVI (Switched Virtual Interface)

SVI on virtuaalinen liityntäportti monikerroksisessa kytkimessä ja se voidaan luoda ainoastaan

VLANeille, jotka ovat kytkimelle konfiguroituna. Virtuaalinen tarkoittaa tässä sitä, että mitään fyysistä porttia ei varata liityntäportille, mutta se pystyy tekemään samat toiminnot VLANeille kuin reitittimen liityntäportti tekisi. Myös sen konfigurointi noudattelee samoja linjoja. (FRAHIM, E., FROOM, R. 2015, s. 212-215).

Ainoastaan VLAN1lle SVI tulee automaattisesti, muille VLANeille se täytyy luoda. Luomisen jälkeen SVIlle voidaan antaa IP-osoite. SVI:tä voidaan käyttää muun muassa toimimaan oletusyhdyskäytävänä liikenteelle VLANista ulos tai sisään ja jotta kytkimeen saadaan yhteys 3-kerroksella. SVIt ovat hyviä käytössä sillä ne ovat nopeita, ulkopuolisia linkkejä ei tarvita reitittämiseen ja kaistaa kytkinten väliseen liikenteeseen voidaan lisätä yhdistämällä linkkejä etherchannelilla.

Yrityksellä oli käytössä end-to-end VLANit. Ryhtyessäni varmistamaan kytkinten porttien osalta VLANien määräytymistä eri portteihin käytin komentoa ”show vlan”. Sen avulla ryhdyin varmistamaan, että VLANien toteutus on saadun dokumentin mukainen. VLANeja oli enemmän kuin mitä dokumentoinnin perusteella oletin, myöskään porttien määräytyminen VLANeihin ei ollut dokumentoinnin mukainen. Tarkistin myös trunk-linjojen konfiguraatiot ”show interfaces trunk”.

Tein vastaavanlaisia tarkistuksia kaikilla kytkimillä ja ilmeni, että VLANien konfiguroinnissa on suuria eroja ja joiltakin kytkimiltä löytyi myös asiakkaan projektissa käytössä olleita konfiguraatioita. Kytkinten toimintaan ylimääräiset VLANit eivät sinällään vaikuta. DTP-statuksen tarkistuksessa ilmeni, että osalla porteista DTP oli pois päältä ja osalla se oli edelleen päällä. Jotta vältytään virheellisesti konfiguroiduilta trunk-linjoilta verkossa, DTP olisi suotavaa ottaa pois päältä kun tietoverkko on vakaa. Mikäli tiedetään, että jollain portilla ei tule olemaan yhteyttä kytkimeen, kannattaa määritellä portti access-modeen, jotta portit eivät omatoimisesti neuvottele trunk-linjaa. Tällä voidaan estetää myös VLAN-hopping hyökkäyksiä (ks. Tietoverkon tietoturva.).

Kytkimillä voisi rajoittaa VLANien määrää, suositeltava määrä olisi kolme VLANia yhdellä kytkimellä. Liki jokaisella kytkimellä on VLANeja, joita ei käytetä joten ne voisi poistaa. Pitäisi käydä läpi monelleko VLANille todella on tarvetta vai riittäisikö yksi VLAN koko päätoimipisteen käyttöön. Kun on päädytty käytettäviin VLANeihin, portit pitäisi määrittää kuulumaan oikeaan VLANiin. Poistettaessa VLANeja pitää ensin muistaa poista porttikytkennät ko. VLANilta ja vasta sen jälkeen poistaa VLAN.

Turvallisuussyistä Liikenne VLAN1:stä pitäisi ottaa pois yrityksen oman liikenteen käytöstä ja sallia ko. VLANille ainoastaan kontrolliprotokollat kuten: DTP, VTP, STP Bridge protokolla (BPDUt), Port Aggregation Protokolla (PAgP), Link Aggregation Control Protokolla (LACP), Cisco discovery Protokolla (CDP). Hallinto VLANina trunk-linjoilla olisi suotavaa käyttää VLANia, joka ei ole muussa käytössä. Rajoittamalla liikenne omaan VLANiin rajataan myös yleislähetysten aluetta ja luodaan turvaa hyökkäysten varalle sekä vähennetään koko verkkoa rasittavia yleislähetyksiä. Tämän lisäksi VLANit ovat tarpeen joidenkin DoS-hyökkäysten turvaominaisuuksien vuoksi. ks. luku 5. Suositeltavaa olisi myös erotella WLANissa liikkuva liikenne omaan VLANiin. Porttien nopeudet ja rajoitukset olisi hyvä tarkistaa ja miettiä ovatko rajoitukset linkeillä tarpeellisia.

3.4 Spanning Tree Protocol

Yritysten toiminnan edellytyksenä on usein yrityksen tietoverkko. Tästä syystä tietoverkon toiminnan varmuus on ensisijainen tavoite. Varmistavat laitteet, linkit ja moduulit luovat varmuutta tietoverkon toiminnalle, kuitenkin luomalla varmistuksia 2. tasolle luodaan myös mahdollisuuksia bridging loopeille, jotka vammauttavat tietoverkkoa. Spanning Tree protokolla (STP) tunnistaa ja estää looppien syntymistä pakottamalla tietyt portit standby-tilaan, jotta ne eivät kuuntele, välitä tai tulvi data kehyksiä. Lähettämällä Bridge Protocol Data Units (BPDU) kehyksiä toisilleen STP ottaakseen selville verkon topologiaa ja määritelläkseen mitä tapahtuu kun verkkolaiteita lisätään tai poistetaan. (FRAHIM, E., FROOM, R. 2015, s. 119–121.)

BPDU

BPDU kehyksissä kytkimet vaihtavat tietoja BID-arvoista ja root path costs. Kytkin lähettää kehyksiä käyttäen portin MAC osoitetta lähetysosoitteena ja kohdeosoitteena STP yleislähetysosoitetta 01:80:C2:00:00:00. BPDU kehyksiä on kahdenlaisia(CISCOb).

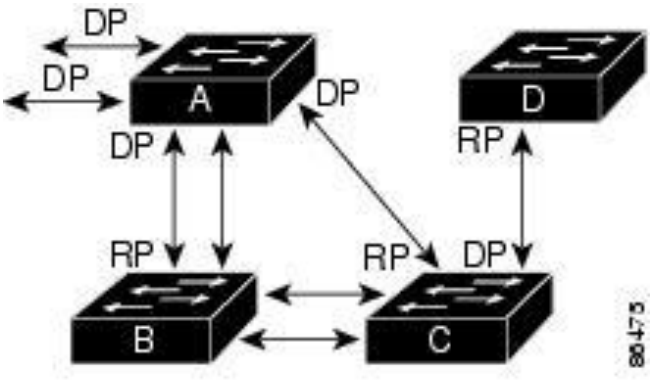
- Konfiguraatio BPDU, jota käytetään spanning tree laskentaan
- Topology Change Notification (TCN) BPDU, joilla ilmoitetaan muuttuneesta topologiasta

BPDU-kehyksiä lähetetään oletusarvoisesti 2 sekunnin välein ja näin kytkimet pystyvät seuraamaan verkon muutoksia sekä lähettämään ja lopettamaan lähetyksen porteilla mikäli tarpeellista. Kun laite kytketään kiinni kytkimeen, se ei ala välittömästi välittämään liikennettä. Portti käy läpi kuusi eri tilaa, joissa se prosessoi BPDU-kehyksiä ja päättelee verkon topologian. (CISCOb.)

- Blocking: tietoja ei välitä, mutta mikäli muut linkit pettävät, STP sallii portin siirtyä forwardin-tilaan. BPDU-kehyksiä vastaanotetaan tässä tilassa ja tila estää bridging loopien syntymisen.
- Listening: Kytkin prosessoi BPDU-kehyksiä ja odottaa uutta tietoa, jonka perusteella se palaa takaisin blockin-tilaan. Ei välitä kehyksiä.
- Learning: Kytkin siirtää osoitetietoja vastaanotettujen pakettien perusteella kytkentä tietokantaan MAC osoite tauluun. Ei välitä paketteja.
- Forwarding: Kytkin lähettää ja vastaan ottaa dataa, STP valvoo saapuvia BPDU-kehyksiä, joiden perusteella se palauttaa portin blocking-tilaan ehkäistäkseen bridging loopeja mikäli tarpeellista.

Ensimmäiseksi STP valitsee ”Root bridge”-kytkimen. Root bridge on se kytkin/reititin jolla on pienin bridge ID (BID), joka lasketaan bridge priorityn ja MAC osoitteen perusteella. Mikäli BID on kahdella kytkimellä sama, se jolla on pienempi MAC-osoite, tulee rootiksi. Sen jälkeen STP määrittelee ”least cost path” root bridgelle. Jokaiselle linkille on oma oletus cost, joka voidaan myös muuttaa manuaalisesti, mikäli halutaan manipuloida STPn käytöstä.

Kun root bridge on valittu, jokainen kytkin määrittelee itse jokaisen reitin arvon root kytkimelle. Se portti, jolta on pienin arvo rootille, tulee ”root port” (RP). ”designated port” (DP) on portti jolta on lyhin matka rootille sillä verkko segmentillä. Kaikki portit, jotka eivät ole RP tai DP-portteja, asetetaan ”blocked port” (BP)iksi. (Kuva 22.)



KUVA 13 Spanning-Tree topologia (CISCOb)

.

Per-VLAN STP Plus (PVST+) on Ciscon oma standartoimaton versio STPstä ja se tarjoaa erillisen spanning-tree ilmentymän jokaista konfiguroitua VLANia kohti. Sen avulla liikennettä voidaan tasata ylimääräisillä linkeillä. Oletuksena Ciscon laitteilla on käytössä PVST+ (Per-VLAN spanning Tree Protocol Plus) vaikka suositellumpaa olisi käyttää joko Rapid PVST+ (RPVST+) tai suuremmissa verkoissa Multiple Spanning tree (MST). (FRAHIM, E., FROOM, R. 2015, s. 119–131).
PVST+

Rapid Spanning Tree Protokolla (RSTP) nopeuttaa verkossa tapahtuvan muutoksen jälkeistä uudelleen laskenta aikaa. RSTP käyttää porttien määrittelemiseen kahta tyyppiä; vaihtoehtoinen tai vara-portti ja kolmea portin tilaa; ”discarding”, ”learning” ja ”forwarding”. STPssä verkon toipumiseen muutoksesta aikaa voi mennä jopa minuutti ja se ei ole riittävän nopea. RSTP mahdollistaa nopean toipumisen kytkimen, portin tai LANin kaatumisesta, sillä uusi root-portti voi siirtyä suoraan forwarding-tilaan. PVRST+, on per-VLAN version RSTP.stä. (FRAHIM, E., FROOM, R. 2015, s. 119–131).

STPssä on lukuisia ominaisuuksia joilla voidaan joko nopeuttaa verkkoa (UplinkFast, BackboneFast, PortFast) tai vakauttaa sitä (BPDU Guard, BPDU Filter, Root Guard, Loop Guard). (FRAHIM, E., FROOM, R. 2015, s. 119.) Alla on esitelty niistä olennaisimmat.

LOOPGUARD

STP toiminta perustuu BPDUiden välittämiseen ja vastaanottamiseen. 2-kerroksen bridging loop syntyy yleensä kun STPn lukitsema portti siirtyy virheellisesti forwarding–tilaan. Tämä johtuu yleensä siitä, että portti ei saa STP BPDUita ja tämän perusteella STP päättelee, että topologia on vapaa bridging loopeista. Tämän jälkeen portin tilaksi vaihtuu designated-tilaan ja sen jälkeen se siirtyy forwarding-tilaan. Bridging loopit voivat syntyä myös access-kerroksen kytkimillä käyttäjän suuntaan useista eri syistä kuten virheellisestä johdotuksesta, väärin konfiguroiduista päätelaitteista tai tahallisesti. (FRAHIM, E., FROOM, R. 2015, s. 164)

ROOTGUARD

Root Guardin avulla vahvistetaan root bridgen sijaintia verkossa. Portit, joissa Root Guard on päällä, menevät ”root-inconsistent STP”-tilaan, mikäli ne saavat BPDUn, joka sisältää tiedon superior STP BPDUsta. Kun portti on ”root-inconsistent”-tilassa, liikennettä ei pääse ulos portista. Tämä toiminta vahvistaa root bridgen asemaa verkossa. (FRAHIM, E., FROOM, R. 2015, s. 164.)

BPDUGUARD

BPDU guard sulkee portin mikäli porttiin, jossa portfast ja BDPU guard on päällä, saapuu BPDU. Tämä estää tehokkaasti porttiin kytketyn laitteen osallistumisen STK-prosessiin. (FRAHIM, E., FROOM, R. 2015, s. 119–131).

PORTFAST

Portfastin ollessa päällä portilla, portti ei joudu läpi käymään kaikkia normaaleja STPn vaiheita, vaan se pystyy vaihtamaan tilan suoraan blocking-tilasta forwarding-tilaan. Portfast portti ei myöskään lähetä TCN BPDU-viestejä portin vaihtaessa tilaa ja tämä säästää verkon kapasiteettia. Portti voi vaihtaa tilaa esimerkiksi silloin, kun siihen kytketty laite (PC) käynnistyy tai sammuu. Mikäli verkossa on paljon PC:itä, voi TCN BPDU-viestejä syntyä paljon. (FRAHIM, E., FROOM, R. 2015, s. 132–133, s. 156).

Yrityksen verkossa on kaikkialla käytössä PVST+. Sen päivittäminen nopeampaan RPVST+/RSTP olisi järkevää, jotta verkko voi reagoida nopeammin muutoksiin. Mikäli halutaan säilyttää VLAN-kohtainen STP, valitaan RPVST+. Tällöin huomioitavaa on, että kaikkien kytkinten muuttaminen rapid-PVST+ ei ehkä onnistu kerralla, mutta koska molemmat käyttävät samaa BPDU formaattia, migraatio voidaan tehdä vaiheissa. Muutos vaikuttaa liikenteeseen, joten on suositeltavaa tehdä se suunnitellusti silloin, kun järjestelmät eivät ole käytössä. UplinkFast ja BackboneFast PVST+ ovat ominaisuuksia, jotka eivät ole käytössä rapid-PVST+ssä ja migraatiossa ne pitäisi ottaa pois käytöstä. Nämä ominaisuudet eivät kuitenkaan ole yrityksen kytkimillä ole käytössä, joten ne eivät vaikuttaisi asiaan. RSTP:n käyttöä taas puoltaa se, että verkossa on käytössä useita VLANeja, mutta vain yksi reitti root-kytkimelle ja internetiin. Käytettäessä RSTP:tä tietoverkko toipuu nopeammin muutoksista. Toisaalta taas silloin ei voida hyödyntää dataliikenteen kuormantasausta.

Loopguard ja Rootguard ovat toisensa poissulkevat, joten samoille porteille ei voi laittaa päälle molempia. Rootguadin voisi ottaa käyttöön kaikissa porteissa, joissa rootia ei odoteta olevan. Rootquard sulkee portin, mikäli joku yrittäisi horjuttaa verkon topologiaa lähettämälle portille hyökkäävältä kytkimeltä BPDUn paremmalla BID-arvolla. Normaalisti tämä johtaisi rootin uudelleen valintaan. Rootguard kuitenkin vaatii toimiakseen Portfastin.

Portfast oli päällä joillakin kytkimillä, mutta sen voisi laittaa päälle kaikkiin access-kerroksen kytkimiin. BPDU Guard ja portfast yhdessä eivät estä kokonaan loopien syntymistä, sillä kaikki laitteet eivät lähetä BPDUita, mutta ne ovat kuitenkin suositeltu turvaominaisuus.

Spanning-treen root bridge olisi hyvä manuaalisesti konfiguroida jokaiselle VLANille, mikäli halutaan säilyttää VLAN-kohtainen STP.

3.5 HSRP

HSRP-protokollaa käytetään merkitsemään kaksi tai useampi reititin vastuulliseksi lähettämään eteenpäin kehyksiä, joita lähetetään yksittäiseen virtuaaliseen IP- tai MAC-osoitteeseen. Tällöin vastuullinen reititin reitittää liikenteen ja fyysisesti reititin, joka ohjaa liikennettä, on näkymätön käyttäjille. HSRP on redundanssi protokolla, joka määrittelee minkä reitittimistä pitäisi ottaa aktiivinen rooli liikenteen välittämiseen. Protokollaan tehtävä on myös vahtia, milloin on otettava käyttöön muu reititin aktiivisena reitittimenä esimerkiksi laiterikon sattuessa. (CISCO.COM 2007.)

Jotta tehokkuus voidaan maksimoida, on muistettava, että STP-topologia ei ole tietoinen HSRP-konfituraatioista, joten HSRPn VLAN-kohtaiseksi aktiiviseksi reitittimeksi on valittava sama reititin, kuin on STP-topologian root-reititin kyseisellä VLANilla. Tällöin 2-kerroksen liikenteen eteenpäin toimitus johtaa suoraan 3-kerroksen laitteelle, joka on HSRPn aktiivinen oletusyhdyskäytävä. (CISCO.COM 2007.)

3.6 Etherchannel

EtherChannel on teknologia joka alu perin kehitettiin yhdistämään monta Fast or Gigabit Ethernet-portteja yhdeksi loogiseksi kanavaksi. Teknologian avulla voidaan nostaa linjan nopeutta sen fyysistä kapasiteettia korkeammaksi. Teknologian eduksi voidaan laskea se, että kytkimiä ei tarvitse vaihtaa porttien nopeuden nostamiseksi. Konfiguraatiot voidaan tehdä EtherChannel-portille, niin ettei jokaista kanavaan kuuluvaa porttia tarvitse erikseen konfiguroida ja liikenteen tasaus on mahdollista linkeillä, jotka kuuluvat kanavaan. Tarve EtherChannelille on ilmeinen, mikäli liikennettä tulee access-kerrokselta enemmän, kuin distribution/core-kerrokselle johtava linkki voi kuljettaa eteenpäin. Tekniikkaa käytettäessä täytyy olla tarkkana konfigurointien yhdenmukaisuudessa ja on kiinnitettävä huomiota siihen, että spanning tree ei lukitse yhtä kanavassa olevaa linkkiä FRAHIM, E., FROOM, R. 2015, s. 94–96.)

Erään toimipisteen kytkimissä ei ollut minkäänlaisia konfiguraatioita, joten myöskään etherchanneleita ei niissä ollut. Toimipisteessä kytkimet oli järjestetty jonoon. Jonoon sijoittamisessa on olemassa riski, että laitteen vikaantuessa vikaantuvan laitteen takana ovat laitteet eivät pääse enää kiinni verkkoon.

Kytkimet dni-yhteyksien päässä ovat kiinni operaattorin kytkimissä ainoastaan yhdellä kaapelilla. Käyttämällä etherchannelia mahdolliset linkkien ruuhkautumisesta johtuvat katkokset tai hajoamisesta voitaisiin välttää ainakin suurelta osalta. Tietenkin, koska linkin toinen pää on kiinni operaattorin hallinnoimissa laitteissa, muutokset täytyisi tehdä yhteistyössä operaattorin kanssa ja varmistaa yhdessä, etteivät konfiguraatiot ole ristiriidassa keskenään.

3.7 VSS

Cisco StackWise-teknologia luo mahdollisuuden usean kytkimen kapasiteetin hyödyntämiseen. StackWise kytkimen käytössä on monia etuja, kuten se, että vaikka kytkimiä voi fyysisesti olla pinossa jopa yhdeksän, hallinnollisesti ne ovat yksi laite. Kytkimet jakavat automaattisesti konfigurointi- sekä reititystiedot ja pinoon voidaan lisätä ja siitä voidaan poistaa kytkimiä, ilman että se vaikuttaa pinon toimintaan. Kun uusi laite lisätään pinoon, master-kytkin automaattisesti konfiguroi uuden laitteen samalla IOSilla ja konfiguroinnilla kuin masterilla on. Tämä mahdollistaa myös toisen laitteen toimimisen masterina, mikäli master-kytkin vikaantuu. Laitteet yhdistyvät toisiinsa erityisellä kaapelilla, joka luo suljetun kaksisuuntaisen linkin (Virtual Switch Link VSL). (FRAHIM, E., FROOM, R. 2015, s. 395–399).

Päätoimipisteessä VSS oli käytössä osittain. Teknologiaa voisi harkita hyödynnettävän muissakin kytkimissä, sillä VSSn käyttö kytkimillä varmistaa vikasietoisen access- ja distribution-tason. Laajentamalla VSS kattamaan koko päätoimipistettä voitaisiin harkita Spanning-Treen ja HSRPn käytön unohtamista, vähentää tarvittavaa konfiguraatiomäärää ja varmistaa koko toimipisteen verkon viansietoisuus.

4 TIETOVERKON TIETOTURVA

Suurin osa yritysten tietoverkkoihin liittyvistä turvallisuustoimista keskittyy yrityksen ulkopuolisten hyökkäysten keskeyttämiseen ja ylemmille OSI kerroksille. Tällöin huomion keskipisteenä ovat kampuksen edge reititys laitteet ja pakettien filtteröinti, joka tehdään 3- ja 4-kerroksen tunnuksen, porttien, tms. perustella ja tapahtuu pääasiassa palomuureilla. Campus access - ja 2-kerroksen liikenne jää huomiotta tai huomioidaan vasta ongelmien sattuessa. Tällöin yrityksen sisäverkko jää haavoittuvaksi sisäisille hyökkäyksille. (FRAHIM, E., FROOM, R. 2015, s. 410)

Päinvastoin kuin palomuuri, jonka tehtävä on oletuslähtöisesti estää liikennettä, kytkinten ja reitittimien tehtävä on oletuslähtöisesti mahdollistaa liikennettä. Tästä syystä laitettaessa laitteita verkkoon ilman konfigurointia ne toimittavat eteenpäin liikennettä, kunnes laite määrätään tekemään muuta. Laitteiden funktio palvella liikennettä aiheuttaa usein sen, että niille päätyy minimaalinen määrä turvallisuusmäärityksiä. Mikäli hyökkäys kohdistetaan sisäiselle 2-kerroksen yrityksen laitteelle, loppu verkko altistuu nopeasti hyökkäykselle. (FRAHIM, E., FROOM, R. 2015, s. 410.)

Kampusverkkoon kohdistuvat erilaiset uhat kuin muuhun tietoverkon osiin. Niistä todennäköisin on luvaton ja valvomaton liikenne eri muodoissa. Kun tietoverkkoon voidaan ilman rajoituksia lisätä omia laitteita (esimerkiksi langattomia tukiasemia) ilman suunnitelmaa tai IT-osaston tietoa valvomattomat laitteet voivat olla suuri tietoturva riski, sillä niihin ei välttämättä aseteta tarvittavaa tietoturvatasoa, vaan ne lisätään verkkoon sellaisenaan. Tällöin niiden kautta kulkeva tieto on helppo kaapata tai ottaa hallintaan koko verkko. (FRAHIM, E., FROOM, R. 2015, s. 414.)

Kun luvaton pääsy verkkoon on saavutettu, verkkoa voidaan häiritä erilaisilla hyökkäyksillä. Hyökkäykset voidaan tehdä ulkopuolelta tai niitä voidaan tehdä luotetusta laitteesta. Seuraavat hyökkäykset kohdistuvat kytkimiin ja 2-kerrokselle (FRAHIM, E., FROOM, R. 2015, S. 415):

- MAC layer attacks
- VLAN attack
- Spoofing attacks
- Hyökkäykset kytkin laitteille.

4.1 DoS-hyökkäykset

Denial of Service(DoS) -hyökkäyksen tarkoituksena on evätä käyttäjältä tai organisaatiolta pääsy palveluihin ja resursseihin. Verkkoon tunkeutuminen tai tietovarkaus eivät ole tyypillisiä DoS-hyökkäyksen muotoja. Tällainen hyökkäys voi pahimmillaan kaataa koko verkon ja aiheuttaa yritykselle suurta haittaa mm. tuottavuuden heikkenemisenä. Tyypillisiä palvelunestohyökkäyksen muotoja ovat esimerkiksi ”SYN flood attac”, ”land attack”, virukset ja madot. Suuri osa näistä hyökkäyksistä perustuu spoofing- ja flooding-tekniikkoihin ja ne hyödyntävät tietoverkon heikkouksia. Hyökkäyksiä vastaan on hankala suojautua, sillä DoS-paketit voivat näyttää aivan normaalin tietoliikenteen paketeilta. (CISCO.COM 2005)

4.1.1 MAC layer attacks

VLAN HOPPING ATTACK

VLAN hopping -hyökkäyksessä hyökkääjää vaihtaa trunk-linjoille saapuvan paketin VLAN ID:tä. Hyökkäyksen alaisena oleva laite voi lähettää paketteja useiden eri VLANien VID-tunnuksella ja näin ohittaa 3-kerroksen tietoturvamääritykset. (FRAHIM, E., FROOM, R. 2015, 416.)

MAC ADDRESS FLOODING

Hyökkäyksessä hyökkääjä lähettää kytkimelle Ethernet-kehyksiä erilaisilla lähde-MAC-osoitetiedoilla pyrkimyksenään kuluttaa loppuun muisti, joka on CAM-taulukon käytössä. CAM-taulukon ollessa täynnä kytkin ryhtyy käyttäytymään hubin tavoin ja lähettää kaikki saamansa kehykset ulos kaikista porteista. Hyökkäyksen lopputulos on se, että hyökkääjä saa käyttöönsä kaiken datan, mitä verkossa liikkuu, ja voi hyödyntää tietoja muiden hyökkäysten tekemisessä(FRAHIM, E., FROOM, R. 2015, 415; CISCO.COM 2016.)

4.1.2 Spoofing attacks

DHCP STARVATION JA DHCP SPOOFING

Hyökkäyksessä käyttäjä ruuhkauttaa yrityksen DHCP-palvelimen DHCP-pyynnöillä väärennetyistä MAC-osoitteista. Kun oikea DHCP serveri on saatu ruuhkautumaan väärennetyllä DHCP-kyselyillä, hyökkääjä laittaa verkkoon väärennetyn DHCP-palvelimen, joka ryhtyy vastaamaan yrityksen sisältä tuleville DHCP-pyynnöille antamalla niille oletusyhdyskäytävä ja IP-osoitetiedot. Hyökkääjän tarkoituksena on pyrkiä toimimaan yrityksen verkossa DHCP-serverinä oikean sijaan. Onnistuneen hyökkäyksen jälkeen käyttäjät saavat hyökkääjän antamat DHCP-vastaukset hyökkääjä voi kääntää kaiken verkkoon suuntautuvan liikenteen ohjautumaan omaan järjestelmäänsä ja näin kaapata yrityksen sisäisiä tietoja.
(CISCO.COM 2007)

SPANNING-TREE RISKIT

Hyökkääjä pyrkii saamaan verkkolaitteen kohdeverkkoon root-bridgeksi spanning-tree protokollassa. Mikäli tämä onnistuu, hyökkääjä voi kaapata verkossa liikkuvia kehyksiä ja saada käyttöönsä yrityksen sisäistä tietoa. (FRAHIM, E., FROOM, R. 2015, s. 415.)

MAC-SPOOFING

MAC-spoofing hyökkäyksessä hyökkääjä muuttaa tehdasasetuksissa määritellyn mac-osoitteensa yrityksen tietoverkosta valitun kohdelaitteen mac-osoitteeksi. Sen jälkeen hyökkäyksen kohteena olevan yrityksen kytkin välittää oikealle laitteelle tarkoitetut kehykset väärennetyllä mac-osoitteella olevaan laitteeseen. (FRAHIM, E., FROOM, R. 2015, s. 417.)

ARP-SPOOFING

ARP-spoofing hyökkäyksessä pyritään myrkyttämään NIC-kortin ARP cache kahdella eri kohdelaitteella. Kun ARP-cache on saatu myrkytettyä, molemmat laitteet lähettävät toisilleen tarkoitetut tietoliikenteen paketit tietämättään hyökkääjälle. Näin hyökkääjä pystyy seuraamaan kohteiden välistä liikennettä.
(KING, J., LAUERMAN, K. 2014)

4.2 DoS-hyökkäyksiltä suojautuminen

Kytkimiin tai käyttäjiin kohdistuvilta DoS-hyökkäyksiltä voidaan suojautua minimoimalla mahdollisia hyökkäykseen mahdollistavia tekijöitä, kuten lähdeosoitteen tarkistusmekanismejä ja liikenteen alkulähteen varmistusta. DoS-hyökkäyksien estossa erilaisilla anti-spoofing mekanismeillä on suuri rooli. Näitä mekanismeja ovat mm:

- Dynamic Host Configuration Protocol (DHCP) Snooping
- Dynamic Address Resolution Protocol (ARP) Inspektion
- IP Source Guard

(CISCO.COM 2005) Näitä tekniikoita voidaan käyttää suojaamaan verkkolaitteita spoofingilta ja ”mies välissä”-hyökkäyksiltä access-kerrokselta ja OSI-mallin kerroksella 2.

4.2.1 DHCP Snooping

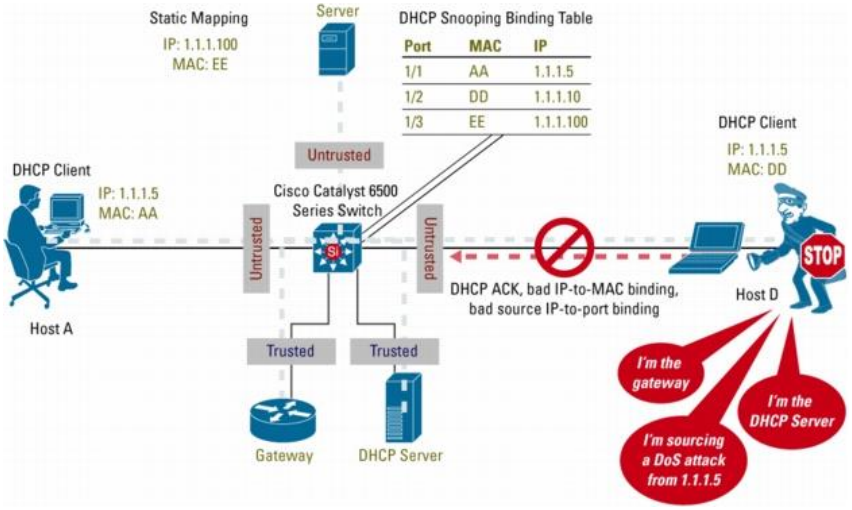
DHCP Snooping varmistaa DHCP tapahtuman ja suojaa käyttäjiä vääriltä DHCP palvelimilta. Kytkimelle ilmoitetaan mitkä portit ovat luotettuja portteja välittämään DHCP-viestejä ja muista porteista tulleet DHCP-viestit hylätään, eikä niitä toimiteta eteenpäin. (CISCO.COM 2005)

4.2.2 Dynamic ARP Inspection (DAI)

Dynamic ARP inspection (DAI) estää hyökkäyksiä missä hyökkääjä lähettää ARP-paketteja isännälle tai oletusyhdyskäytävälle, joissa on virheelliset IP/MAC-siteet tarkoituksenaan ”myrkyttää” ARP-lista kohdelaitteella. DAI sieppaa ARP-viestit kaikista muista kuin luotetuista porteista, tarkistaa tietojen oikeellisuuden DHCP Snooping protokollan tuottaman IP/MAC-listan perusteella varmistaakseen ARP-pakettien oikeellisuuden. Mikäli virheellinen tieto havaitaan saapuneeksi jollekin portille, portti suljetaan. DAI rajoittaa portille saapuvien ARP-pakettien määrä ja näin osaltaan estää DoS-hyökkäyksiä. (CISCO.COM 2005).

4.2.3 IP Source Guard

IP Source Guard estää snooping-hyökkäyksiä välittämällä eteenpäin vain paketit, jotka source address täsmää DHCP Snooping taulussa olevien osoitteiden kanssa. (CISCO.COM 2005.)



KUVA 14 Anti-spoofing ja "mies välissä"-hyökkäyksen esto access-kerroksella (CISCO.COM 2005)

Kuvassa 30 näkyy kuinka kolmen edellä mainitun tekniikan käyttö yhdessä voi estää “mies-välissä ”-hyökkäyksiä. Käyttäjä D pyrkii toimimaan DHCP serverinä ja siirtää liikenteen kulkemaan hyökkääjän laitteiden kautta antamalla väärän oletusyhdyskäytävän tai lähettämään verkkoon ”DHCP release”-viestejä kaikille käyttäjille, jotta he eivät pääse verkkoon. DHCP Snooping kytkimillä estää nämä hyökkäykset luomalla yhteystaulun, jossa on listaus IP- ja MAC-osoiteyhteyksistä porttikohtaisesti. Sama käyttäjä D yrittää suorittaa ARP-hyökkäyksen myrkyttämällä ARP- muistin ja kaapata liikenteen käyttäjä A:lta asettamalla itsensä oletusyhdyskäytäväksi. DAI ehkäisee vertaamalla untursted-portiksi merkitylle tietoja DHCP Snoopingin toimittamaan IP—MAC-osoiteyhteystietoon. Käyttäjä D yrittää vielä suorittaa DoS hyökkäyksen käyttämällä A:n osoitetietoja, mutta IP Source Guard ehkäisee sen jälleen käyttämällä DHCP Snoopingin toimittamia tietoja.

4.2.4 Port security

Port security on muutakin kuin vain rajoitus sallituille MAC osoitteille. Vaikka tämäkin ominaisuus kuuluu porttiturvaan, se voidaan määritellä oppimaan esimerkiksi tietty osoitemäärä, jonka jälkeen jos portille tulee uusia osoitteita, koko kytkin voidaan sulkea, pääsy voidaan rajoittaa tietylle MAC osoitteelle ja lokiin voidaan kirjata virheilmoitus tai pääsy voidaan rajoittaa MAC-osoitteelle ilman virheilmoitusta. (FRAHIM, E., FROOM, R. 2015, s. 419–421.)

STORM CONTROL

Viallinen päätelaite, väärin konfiguroitu verkko tai tarkoituksellinen Dos-hyökkäys voivat olla syynä traffic storms. Ciscon joillakin kytkimillä on käytettävissä storm control ominaisuus, joka rajoittaa myrskyjen vaikutusta ja tarvittaessa toimii oikealla tavalla. Jotta ominaisuutta voidaan käyttää oikein, tietoliikennettä täytyisi seurata, jotta tiedetään normaalit tasot liikenteelle. Access-tasolla oikein konfiguroituna ja käytettynä tämä luo hyvän rajoittimen liialliselle liikenteelle ja hyökkäykselle. Tämän opinnäytetyön aikana saatavilla ei ole porttikohtaista dataa liikenteestä ja liikennemääristä, mutta vaihtoehto on silti hyvä tuoda esiin tulevaisuutta varten.

SECURE UNUSED SWITCH PORTS

Portit, jotka eivät ole missään käytössä pitäisi laittaa kuulumaan VLANiin, jota ei ole sallittu trunkeille tai sulkea ne kokonaan. Suurin osa Ciskon kytkimistä käyttävät oletuksena trunk-linjojen määrittämiseen Dynamik Trunkin protokollaa (DTP). Mikäli porttiin kytketään toinen kytkin, portit omatoimisesti neuvottelelevat käytettävän trunk-protokollaan niiden välille. (FRAHIM, E., FROOM, R. 2015, s. 53.) Hyökkääjä voi hyödyntää tätä ominaisuutta ja neuvotella trunk-linjan itsensä ja kytkimen välille ja saavuttaa sitä kautta pääsyn VLANien tietoliikenteeseen.

5 POHDINTA

Yhtenäiset toimitatavat tietoturvassa, konfiguroinnissa, verkkoon laitettavissa laitteissa ja hallinnassa vaativat selkeän tietoturvasuunnitelman. Yrityksellä ei ollut yhtenäistä toimintamallia verkkolaitteiden hallintaan ja paras lopputulos verkon turvaamiseen saataisiinkin yhdenmukaistamalla toiminta kaikilla paikkakunnilla ja keskittämällä laitehallinta sekä suunnittelu yhden ryhmän hallintaan. Yritykselle pitäisi siis tehdä tietoturvasuunnitelma, joka pohjautuu yrityksen tietoturvapolitiikkaan. Suunnitel-

masta pitäisi käydä selkeästi ilmi mm. henkilöt, jotka ovat vastuussa kustakin osa-alueesta, ja toimintatavat erilaisissa tilanteissa, kuten virhetilanteet, laitteiston päivitys tai uuden laitten lisäys verkkoon. Pääsy kytkimille olisi hyvä olla samanlainen jokaisella paikkakunnalla ja avaimia olisi oltava vain tietyillä luotetuilla henkilöillä.

Laitekanta olisi hyvä päivittää ja korvaaville laitteille voisi ennen niiden toimittamista toimipisteisiin konfiguroida valmiiksi IP-osoitteet ja salasanat, jotta laitteet olisivat jatkossa IT-yksikön hallinnassa. IP-osoitteet, salasanat, VLAN-määritykset ja muut konfiguraatiot voisi jatkossa dokumentoida systemaattisesti. Näin vältyttäisiin verkossa olevilta hallitsemattomilta laitteilta, jotka kuitenkin ovat keskeisessä roolissa yrityksen tietoverkossa ja luovat näin suuren riskin yrityksen tietoverkon toiminnalle.

SSH-yhteyttä pitäisi suosia telnet-yhteyden sijaan. Salasanat olisi hyvä kryptata ja niiden tulisi olla muutaman luotetun henkilön tiedossa. Kytkimiltä voisi poistaa nykyisissä ohjelmistoversiossa automaattisesti päällä olevan internetselaimella suoritettavan hallinnan, mikäli sitä ei käytetä, ja CDP tulisi ottaa pois päältä laitteilta. Trunk-linjoille tulisi sallia vain todellisten käytössä olevien VLANien liikenne ja ylimääräiset VLANit voisi siivota pois kytkimiltä. Käyttämättömät portit pitäisi sulkea tai liittää ne kuulumaan VLANiin, jota ei ole sallittu trunk-linjoille. DTP-pitäisi ottaa pois päältä varsinkin niiltä porteilta, joissa kytkintä ei odoteta olevan.

Kytkimillä ei ollut päällä DoS-hyökkäyksiä estäviä ominaisuuksia, joten ryhdyin miettimään, mikä olisi sopiva taso, joka olisi helppo konfiguroida ja hallita mutta loisi kuitenkin suojaa, mikäli joku haluaisi tietoisesti verkkoa vahingoittaa.

STPn ominaisuuksista käyttöön valitsisin access-kerroksen kytkimille BPDU Guardin ja Portfastin, jotka yhdessä toimivat hyvänä lähtökohtana DoS-hyökkäyksien estossa ja ovat kohtalaisen helppo konfiguroida. RootGuardilla estetään STPn manipulointi.

Dynamic Arp Inspection DAI tulisi laittaa päälle käytössä oleville VLANeille. Globaalisti kytkimillä aktivoidaan DHCP Snooping. Jotta hallinnan ja manuaalisen työn määrä olisi vähäisempi, eri turvien sulkemat portit voisi automaattisesti laittaa takaisin päälle, kun tietty aika on kulunut portin sulkeutumisesta.

Muutokset kannattaisi tehdä vähin erin ja yksitellen, minkä jälkeen pitäisi seurata tilannetta sekä vaikutuksia ennen uuden muutoksen tekoa. Suurimpina riskeinä yrityksen tietoverkon toiminnalle näkisin tietoturvan puuttumisen kokonaisuudessaan tietoverkossa sekä hallitsemattomat laitteet, jotka ovat olennainen osa verkon toimintaa.

Opinnäytetyö oli mielenkiintoinen tehdä ja aiheeseen voisi syventyä enemmänkin. DoS-hyökkäysten määrä ja uutisointi on lisääntynyt, mistä sainkin alun perin ajatuksen opinnäytetyöni aiheeksi. Uskon, että tietoverkoilta vaaditaan jatkossa enemmän sietokykyä, kun yhä suurempi osa palveluista

ulkoistetaan, joten yritysten oman tietoverkon liikenteen nopeus ja laatu tulevat olemaan ratkaisevassa roolissa palveluiden toiminnassa.

LÄHTEET JA TUOTETUT AINEISTOT

CISCOa. Cisco IOS Softwarechecker. [verkkoaineisto]. [Viitattu 10.4.2016]. Saatavissa https://tools.cisco.com/security/center/selectIOSVersion.x

CISCOb. Configuring STP. [verkkoaineisto]. [Viitattu 18.3.2016]. Saatavissa http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swstp.html

CISCOc. Configuring Passwords and Provileges. [verkkoaineisto]. [Viitattu 18.3.2016]. Saatavissa http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

CISCO.COM. 8.8.2005. Protecting the Cisco Catalyst 6500 Series Switches Against Denial-Of-Service attacks. [verkkoaineisto] [Viitattu 26.2.2016]Saatavissa: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd802ca5d6.html

CISCO.COM. 25.5.2006. [verkkoaineisto]. [Viitattu 11.4.2016]. Saatavissa http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

CISCO.COM. 17.1.2007. Layer 2 Security Features on Cisco Catalyst Layer 3 Fixed Configuration Switches Configuration Example. [verkkoaineisto] [Viitattu 16.3.2016] Saatavissa http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html

CISCO.COM. 18.12.2014. [verkkoaineisto]. [Viitattu 11.4.2016]. Saatavissa http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800-series-switches/guide-c07-733457.html

CISCO.COM. 8.2.2016. [verkkoaineisto]. [Viitattu 11.4.2016]. Saatavissa http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/23563-143.html

CISCO PRESS. 9.5.2014. Cisco networking academy connecting networks companion guide: Hierarchical network design. [Verkkoaineisto] [Viitattu 7.3.2016]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

FROOM, R ja FRAHIM, E. Implementing Cisco IP switcherd networks (switch) foundation learning Guide: Network design fundamentals. Cisco Press. [verkkoaineisto]. [Viitattu 11.3.2016]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2

FRAHIM, E., FROOM, R. 2015.

Implementing Cisco Ip Switched Networks (SWITCH) Foundation Learning Guide. Cisco Press. United States of Amerika.

KING, J., LAUERMAN, K. 2014. ARP Poisoning Attack and Mitigation Techniques. [verkkoaineisto] [Viitattu 17.3.2016] Saatavissa http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

Comment [A16]: tämän a-, b-ongelman voisi oikeastaa poistaa tässä niin, että laittaisi ensimmäiseksi tuon aiheen ja vasta sitten CISCO

LONG, H. 2006. Implementing VLANs in campus network. [verkkoaineisto] [Viitattu 11.3.2016] Saatavissa: http://ciscodocuments.blogspot.se/2011/05/chapter-02-implementing-vlans-in-campus.html

MILLER, R. The Osi Model: An Overview [verkkoaineisto]. [Viitattu 26.2.2016] Saatavissa: https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543

OSI-MALLI. 12.2.2016. Wikipedia.org. [verkkosivu]. [Viitattu 1.3.2016]. Saatavissa: https://fi.wikipedia.org/wiki/OSI-malli

ROUTER-SWITCH.COM. 26.4.2013. Tutorial of layer 2 & layer 3 switches and how to choose the best switches for your business? [verkkoaineisto]. [Viitattu 12.4.2016] Saatavissa http://www.cisco1900router.com/tutorial-of-layer-2-layer-3-switches-and-how-to-choose-the-best-switches-for-your-business.html

POPPESKIC, V. 2016. How does internet works. [verkkosivu]. [Viitattu 16.3.2016]. Saatavissa http://howdoesinternetwork.com/2011/cdp-attack

SUTTON, G. 11.9.2013. Small Business Trends. Is the extra layer better? Layer 2 versus layer 3 networking. [verkkoaineisto]. [Viitattu 26.2.2016] Saatavissa: http://smallbiztrends.com/2013/09/osi-model-layer-networking.html

TANENBAUM, A., WETHERALL, D. 2014 Computer Networks. Pearson Education Limited. Essex.

TEARE, D. 2013

Impelenting Cisco IP Routing (ROUTE), Foundation Learning Guide Foundation learning for the ROUTE 642-902 Exam. Cisco Press. United States of Amerika.

TEKIJÄNOIKEUS 2000. Opetusministeriö. [verkkoaineisto]. [Viitattu 12.4.2005].

Saatavissa http://www.minedu.fi/opm/tekijanoikeus/index.html

VERKKOTOPOLOGIA. 27.9.2015. Wikipedia.org.

[verkkoaineisto] [Viitattu 23.3.2016]. Saatavissa https://fi.wikipedia.org/wiki/Verkkotopologia