



Kytkimen tietoturva

Kytkeisiin kohdistuvilta hyökkäyksiltä suojautuminen

Daniel Honkanen

OPINNÄYTETYÖ
Joulukuu 2021

Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

HONKANEN, DANIEL:
Kytkimen tietoturva
Kytkimeen kohdistuvilta hyökkäyksiltä suojautuminen

Opinnäytetyö 39 sivua, joista liitteitä 1 sivu
Joulukuu 2021

Opinnäytetyön tarkoituksena oli esitellä lähiverkon toimintaa, kytkimeen kohdistuvia hyökkäyksiä lähiverkon sisältä sekä hallittavasta kytkimestä löytyviä asetuksia, joilla voidaan estää kytkimeen kohdistuvia hyökkäyksiä ja parantaa lähiverkon tietoturvaa.

Monet lähiverkon käyttämät protokollat ovat tietoturvanäkökulmasta katsottuna hyvin heikkoja, sillä ne eivät sisällä minkäänlaisia autentikointimenetelmiä. Hyökkääjän on mahdollista käyttää näitä heikkoja protokollia hyväkseen aiheuttaakseen vahinkoa verkolle ja sen käyttäjille. Hyökkääjät tyypillisesti kohdistavat hyökkäyksen ensimmäisenä kytkimeen, sillä se tarjoaa suoran pääsyn organisaation verkkoon. Ilman oikeanlaisia tietoturva-asetuksia hyökkääjä voi aiheuttaa vahinkoa jo kytkemällä oman koneensa johdolla suojaamattoman kytkimen porttiin.

Hallittavat kytkimet tarjoavat ominaisuuksia, joilla voidaan suojautua siihen kohdistetuilta hyökkäyksiltä. Tässä opinnäytetyössä on esitelty Cisco Catalyst 2960-sarjaan kuuluvalla kytkimellä löytyviä tietoturva-asetuksia, joilla voidaan vahvistaa sekä kytkimen että lähiverkon tietoturvaa ja torjua työssä esiteltyt hyökkäykset. Työssä on annettu esimerkkejä asetusten käyttöönottamisesta.

ABSTRACT

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

HONKANEN, DANIEL:
Switch Security
Defending Against Attacks on Switches

Bachelor's thesis 39 pages, appendices 1 page
December 2021

The purpose of the thesis is to present the operation of the local area network (LAN), attacks on the switch from inside the local area network and settings found in the managed switch, which can be used to prevent attacks on the local area network and improve security of the local area network.

Many of the protocols used by the LAN are very weak from a security point of view, as they do not include any authentication methods. It is possible for an attacker to take advantage of these weak protocols to harm the network and its users. Attackers typically attack the switch first, as it provides direct access to the organization's network. Without the right security settings, an attacker would need to connect their own machine to an unprotected switch port and cause damage.

Managed switches provide features to protect against attacks against it. This paper introduces the security settings found on the Cisco Catalyst 2960 Series Switch to strengthen the security of both the switch and the LAN and to prevent the attacks presented in this work. The paper provides examples of how to apply the settings.

Key words: switch security

SISÄLLYS

1	JOHDANTO	7
2	LÄHIVERKON TOIMINTA.....	8
2.1	Lähiverkko.....	8
2.2	MAC- ja IP-osoitteet.....	8
2.3	Ethernet-kehys.....	9
2.4	Liikenteen muodot.....	9
2.4.1	Unicast	9
2.4.2	Broadcast	10
2.4.3	Multicast	10
2.5	Protokollat	11
2.5.1	ARP	11
2.5.2	DHCP	12
2.6	Kytkin	13
2.6.1	Kytkin tyypit	14
2.6.2	Komentotilat	14
2.6.3	VLAN.....	16
2.6.4	Trunk	17
2.6.5	Native VLAN	18
2.6.6	DTP	18
2.7	STP.....	19
3	KYTKIMIIN KOHDISTUVAT HYÖKKÄYKSET	22
3.1	DHCP-palvelimen spooffaus	22
3.2	IP-osoitteiden näännyttäminen.....	23
3.3	MAC flooding.....	23
3.4	ARP-spooffaus	24
3.5	STP-hyökkäys.....	25
3.6	VLAN-hyökkäykset.....	26
3.6.1	Double tagging	26
3.6.2	Kytkimen spooffaus	27

4	HYÖKKÄYKSILTÄ SUOJAUTUMINEN	28
4.1	Käyttämättömien porttien sulkeminen	28
4.2	Port Security.....	28
4.2.1	Port Security rikkomus.....	29
4.3	DHCP snooping	30
4.4	DAI	32
4.5	PortFast BPDU Guard.....	33
4.6	Suojautuminen VLAN-hyökkäyksiltä	34
5	JOHTOPÄÄTÖKSET	35
	LÄHTEET	36
	LIITTEET	39
	Liite 1. Kytkinten välinen trunk-linkki	39

LYHENTEET JA TERMIT

ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CDP	Cisco Discovery Protocol
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DTP	Dynamic Trunking Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MITM	Man-In-The-Middle
STP	Spanning Tree Protocol
VLAN	Virtual LAN

1 JOHDANTO

Tällä hetkellä käytetyin langallinen lähiverkkoteknologia on IEEE 802.3 standardiin perustuva Ethernet teknologia. Ethernetin suosioon ovat vaikuttaneet mm. sen hinta ja yksinkertaisuus. Yksi tärkeä laite Ethernet teknologiaan perustuvan lähiverkon toiminnan kannalta on ethernet-kytkin. Kytkin on lähiverkossa käytettävä verkkolaite, jolla voidaan yhdistää muita samassa lähiverkossa olevia verkkolaitteita ja ohjata liikennettä kohteena olevalle osapuolelle. Hallittava kytkin tarjoaa sitä käyttäville yrityksille ja organisaatiolle keinon parantaa verkon toiminnallisuutta ja hallinnointia.

Monet lähiverkon toiminnan kannalta välttämättömät protokollat eivät ole suunniteltu tietoturva mielessä ja ovat alttiita erilaisille hyökkäyksille. Kyseiset protokollat tarvitsevat jonkin ulkoisen keinon suojatakseen niiden toimintaa. Hallittavat kytkimet tarjoavat useita tietoturva-asetuksia, joilla voidaan estää lähiverkon sisältä tapahtuvat hyökkäykset. Väärin konfiguroituna tai ilman konfiguraatiota ollessaan, kytkin voi aiheuttaa organisaatiolle tietoturva riskin, sillä kuka tahansa pystyy kytkemään oman laitteensa kytkimen porttiin, pääsemään käsiksi verkkoon ja aiheuttamaan vahinkoa verkon toiminnalle ja sen käyttäjille.

Työn tarkoituksena on esitellä hallittavista kytkimistä löytyviä tietoturva-asetuksia, joilla voidaan suojautua tyypillisimpiä lähiverkon sisältäpäin tapahtuvia hyökkäyksiä vastaan. Työssä esitellään lisäksi lähiverkon ja kytkinten käyttämiä tärkeimpiä protokollia ja niiden toimintaa, sekä niissä piileviä heikkouksia, joita hyökkääjät käyttävät hyväkseen. Työssä näytetyt esimerkit konfiguraatiot on toteutettu Ciscon Catalyst 2960-sarjaan kuuluvalla kytkimellä.

2 LÄHIVERKON TOIMINTA

Tässä kappaleessa esitetään lähiverkon ja kytkimen toimintaa. Kappaleessa kuvataan kuinka laitteet viestivät toistensa kanssa ja mitä protokollia ne käyttävät.

2.1 Lähiverkko

Lähiverkko (LAN) on tiettyyn fyysisesti rajattuun paikkaan kuten rakennukseen tai kotiin sijoittuva tietokoneverkko, joka sisältää tietokoneita, kytkimiä, reitittimiä, johtoja ja muita laitteita sekä komponentteja, mitkä mahdollistavat kommunikoinnin samassa lähiverkossa olevien laitteiden sekä muiden lähiverkkojen kanssa Internetin kautta. Lähiverkon koko voi vaihdella yhdestä käyttäjästä koostuvasta kotiverkosta jopa tuhanteen käyttäjään koostuvasta koulun verkosta.

(What is a LAN? n.d.)

Tyypillisimpiä keskisuuren tai suuren yrityksen lähiverkosta löytyviä laitteita ovat mm. pöytäkoneet, palvelimet, palomuuuri, tulostimet, langaton tukiasema ja reititin.

2.2 MAC- ja IP-osoitteet

Lähiverkossa toimivat laitteet kommunikoivat toistensa kanssa IP- ja MAC- osoitteiden avulla. MAC- osoite (Media Access Control) on jokaiselta verkossa viestintään kykenevän laitteen verkkokortilta löytyvä yksilöllinen fyysinen osoite. MAC-osoite on kooltaan 12 heksadesimaalia, joista ensimmäiset 6 desimaalia on laitteen valmistajakohtainen tunniste ja viimeiset 6 heksadesimaalia laitteen yksilökohtainen tunniste. MAC- osoitteet voivat saada arvoja väliltä: 00-00-00-00-00-00 – FF-FF-FF-FF-FF-FF. (Burke & Partsenidis 2021.)

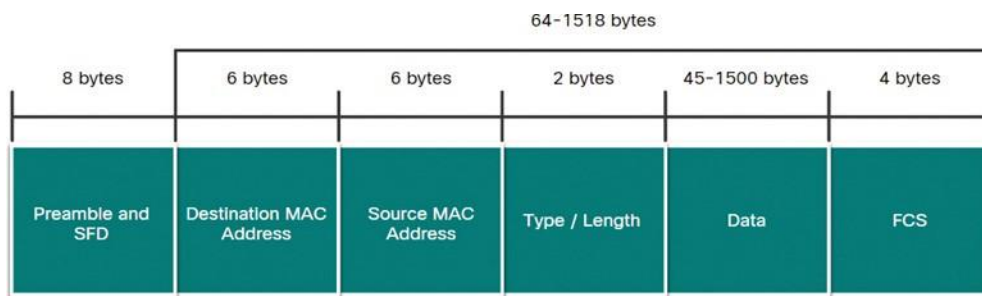
IP-osoitteet (Internet Protocol) ovat loogisia osoitteita, jotka kuvaavat sekä laitteen, että verkon osoitetta, jossa laite sijaitsee. IP-osoitteet ovat 32- bittisiä osoitteita, jotka voivat saada arvoja väliltä: 0.0.0.0 - 255.255.255.255. (Burke & Partsenidis 2021.)

2.3 Ethernet-kehys

Lähiverkossa laitteet viestivät toistensa kanssa lähettämällä verkkoon kehyksiä. Tavallinen Ethernet-kehys on kooltaan 64–1518 tavua ja sisältää seuraavat kentät:

- Preamble ja SFD: Käytetään lähettävän ja vastaanottavan laitteen synkronisointia varten.
- Destination MAC Address: Sisältää viestinnän kohteena olevan laitteen MAC-osoitteen.
- Source MAC address: sisältää lähettävän laitteen MAC-osoitteen.
- Type /length: Kuvaa ylemmän tason protokollan versiota.
- Data: Sisältää ylemmän tason protokollan kapseloitua dataa.
- FCS: Virheentarkistusta varten luotu arvo.

(Ethernet Switching 2020)



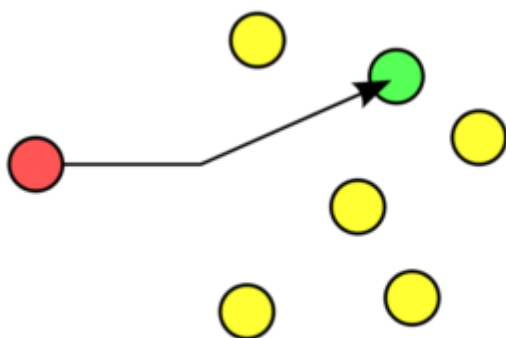
Kuva 1. Ethernet-kehys (Ethernet Switching)

2.4 Liikenteen muodot

Lähiverkossa liikenne laitteiden välillä voi tapahtua kolmella tavalla.

2.4.1 Unicast

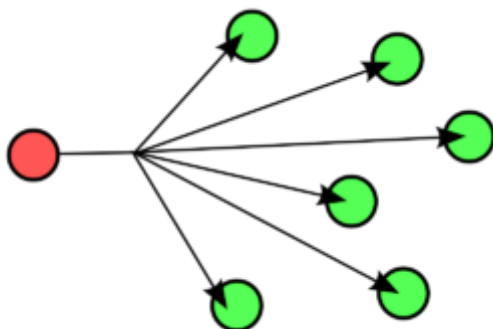
Unicast liikenne tapahtuu kahden laitteen välillä ja on tyypillisin verkossa tapahtuva liikennöinnin muoto. Lähettävä laite kommunikoi vastaanottavan laitteen kanssa lähettämällä tälle kehyksen, mikä sisältää vastaanottavan laitteen MAC-osoitteen. Muut laitteet eivät vastaanota kehyksiä. (Fiber Optical Networking 2018)



Kuva 2. Unicast-liikenne (Fiber Optical Networking 2018)

2.4.2 Broadcast

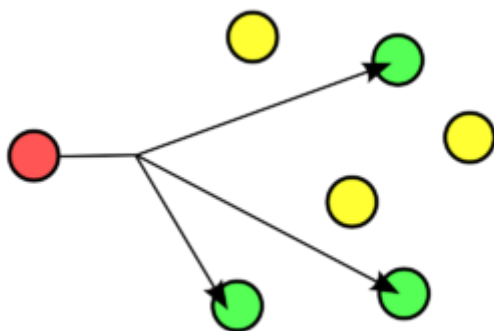
Broadcast liikenteessä lähettävä laite lähettää kehyksen kaikille lähiverkossa oleville laitteille. Broadcast liikenne käyttää MAC- osoitetta FF:FF:FF:FF:FF:FF. (Fiber Optical Networking 2018)



Kuva 3. Broadcast-liikenne (Fiber Optical Networking 2018)

2.4.3 Multicast

Multicast-liikenteessä lähettävä laite lähettää liikenteen kaikille multicast ryhmään kuuluville laitteille. (Fiber Optical Networking 2018)



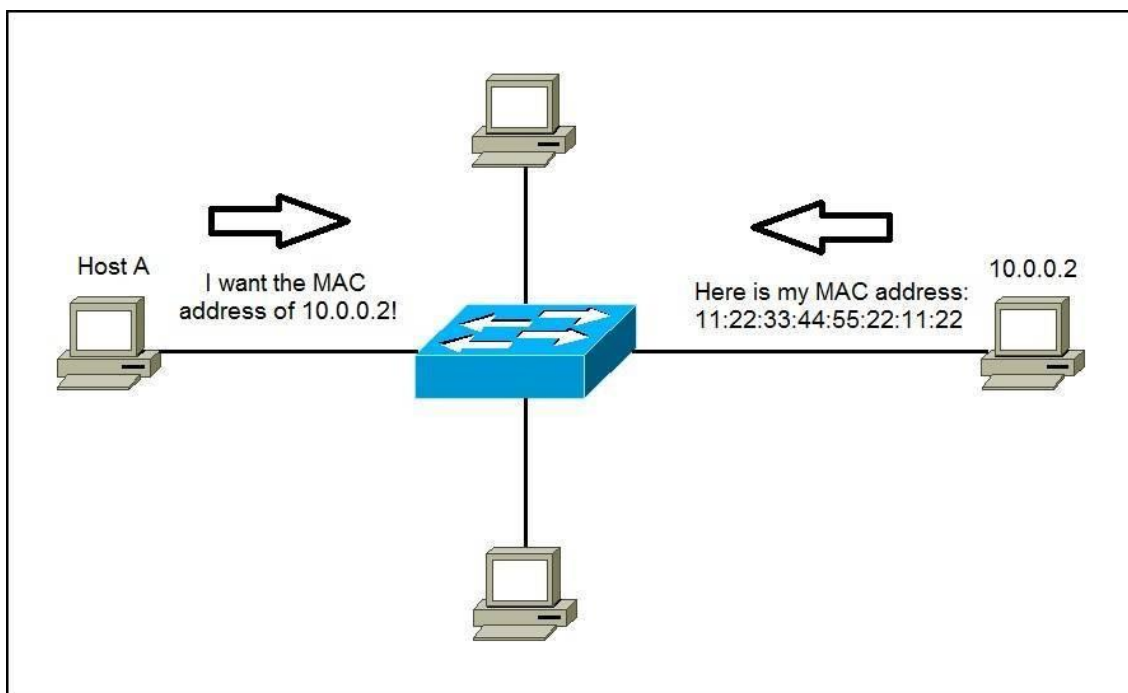
Kuva 4. Multicast-liikenne (Fiber Optical Networking 2018)

2.5 Protokollat

Protokollat ovat sääntöjä, joita verkossa toimivat laitteet noudattavat, jotta viestintä toisten laitteiden kanssa olisi mahdollista. Lähiverkon toiminnan kannalta kaksi keskeistä protokollaa ovat ARP ja DHCP.

2.5.1 ARP

ARP (Address Resolution Protocol) protokollaa käyttävät lähiverkossa toimivat laitteet, jotka haluavat viestiä toistensa kanssa verkossa. Jotta laitteet pystyisivät viestimään toistensa kanssa, laitteiden on IP-osoitteen lisäksi tiedettävä laitteiden MAC-osoite. Laite selvittää kohteen MAC-osoitteen lähettämällä verkkoon ARP-kyselyn broadcast lähetyksenä, jossa se pyytää tietyn IP-osoitteen omaavaa laitetta vastamaan takaisin ja ilmoittamaan oman MAC-osoitteen. Laite, joka tunnistaa kyselyssä olevan IP-osoitteen omakseen lähettää oman MAC-osoitteen unicast-lähetyksenä takaisin kyselijälle. Laitteet pitävät osoitetietoja ylhäällä omassa välimuistissaan tietyn aikaa, jotta verkko ei kuormittuisi turhaan liiallisista kyselyistä. (IBM n.d)

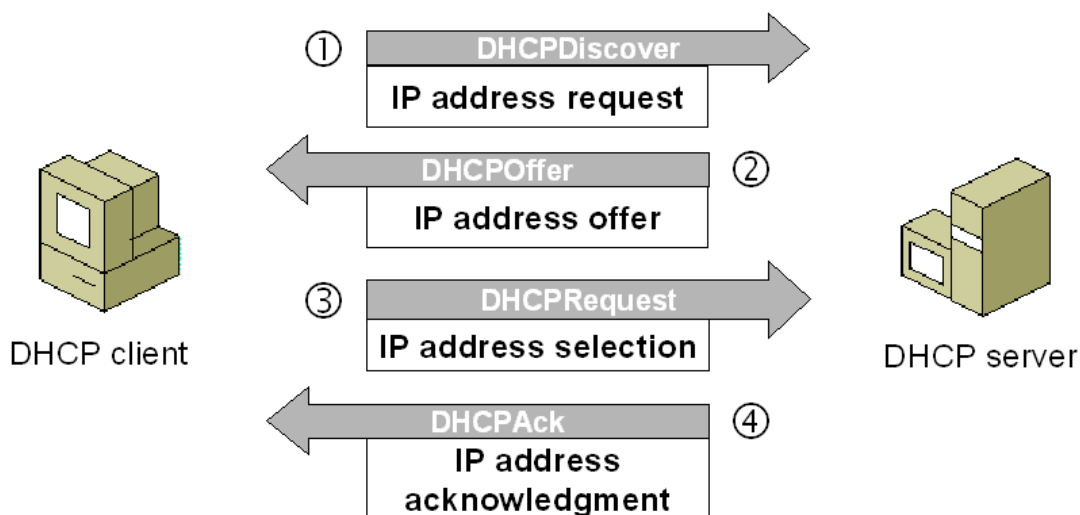


Kuva 5 ARP-protokollan toiminta (Geek University n.d.)

2.5.2 DHCP

DHCP protokolla (Dynamic Host Configuration Protocol) on yleinen lähiverkossa käytetty protokolla, jonka tarkoituksena on tarjota tietyksi aikaa IP-osoite sitä tarvitseville verkkoon liittyneille laitteille dynaamisesti, ilman, että IP-osoitetta täytyisi konfiguroida laitteelle manuaalisesti.

Päätelaitteet saavat IP-osoitteen lähettämällä verkkoon DHCPDISCOVER-paketteja broadcast liikenteenä löytääkseen verkossa toimivan DHCP-palvelimen ja saadakseen siltä lainatuksi IP-osoitteen. Vastauksena DHCP-palvelin lähettää DHCPOFFER-paketin, jossa palvelin tarjoaa asiakkaalle mm. IP-osoitteen ja oletusyhdyksytävän osoitteen. Jos verkossa on useita DHCP-palvelimia, on mahdollista, että ne kaikki vastaavat asiakkaalle ja tarjoavat DHCPOFFER-paketteja. Asiakkaat tyypillisesti vastaavat palvelimelle, jolta asiakas on saanut ensimmäisenä vastauksen. Asiakas vastaa palvelimen lähettämään tarjoukseen DHCPREQUEST-paketilla, jossa se hyväksyy palvelimen tarjoamat asetukset. Viimeisenä vaiheena palvelin kuittaa hyväksymisviestin DHCPACK-paketilla, jolloin asiakas on valmis käyttämään saatua IP-osoitetta. (Vyncke & Paggen 2008)

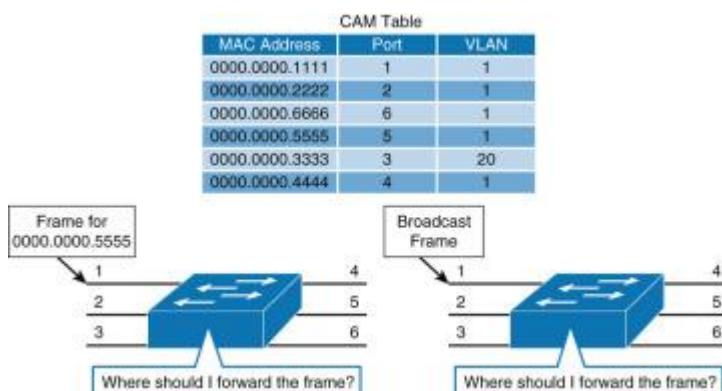


Kuva 6. DHCP-prosessi (ComputerNetworkingNotes 2020)

2.6 Kytkin

Kytkin on lähiverkossa toimiva verkkolaite, joka yhdistää toisiinsa lähiverkossa toimivia laitteita kuten päätelaitteita, reitittimiä, tulostimia ja muita kytkimiä.

Kytkin vastaanottaa ja lähettää sille saapuvia Ethernet kehyksiä, joita lähiverkon laitteet käyttävät viestimiseen toistensa kanssa. Kun kehys saapuu kytkimelle, sen tehtävänä, on lähettää se eteenpäin oikean portin kautta, jossa kehyksen vastaanottava laite sijaitsee. Kytkin tarkastaa sen muistissa sijaitsevaa CAM (Content Addressable Memory)-taulua, johon on tallennettuna tieto siitä missä portissa kohdeosoite sijaitsee. Kytkin rakentaa CAM taulua saapuvien kehyksien MAC-osoitteiden ja laitteen porttisijainnin perusteella. Jos kytkimellä ei ole tiedossa missä portissa viestinnän kohteena oleva laite sijaitsee, se lähettää saapuneen kehyksen kaikkien samassa VLAN:issa olevien porttien paitsi sisään saapuneen kehyksen portin kautta. (Grandmetric 2018)



Kuva 7. Kytkimen CAM-taulu (Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Network Design Fundamentals 2015)

2.6.1 Kytkin tyypit

Kytkimiä on olemassa monenlaisia ja ne eroavat toisistaan esimerkiksi koon, porttien lukumäärän sekä kytkimen tarjoamien nopeuksien perusteella. Kytkimet voidaan jakaa niiden tarjoamien ominaisuuksien mukaan hallittaviin, ei-hallittaviin ja älykkäisiin.

- Hallittavat kytkimet tarjoavat eniten toiminnallisuutta, tarjoten mm. Komentorivin, VLAN ominaisuuden sekä paremman tietoturvan. Hallittavat kytkimet ovat kalliimpia ja niitä käytetään yleensä yrityksissä.
- Ei-hallittavat kytkimet ovat yksinkertaisimpia kytkimiä, jotka eivät tarjoa erikoisominaisuuksia, eikä mahdollisuuksia konfiguroida asetuksia. Kyseiset kytkimet ovat halpoja mutta eivät sovellu yritysten käyttöön.
- Älykkäät kytkimet tarjoavat enemmän ominaisuuksia kuin ei-hallittavat kytkimet mutta vähemmän kuin hallittavat. Tyypillisesti myös hallittavan kytkimen kaltaiset ominaisuudet ovat rajoitetumpia. Kytkimiä on mahdollista konfiguroida Web-käyttöliittymän avulla. Kytkimet ovat hintaluokaltaan halvempia kuin hallittavat kytkimet ja ne soveltuvat pienyritysten käyttöön.

(Shaw 2020)

2.6.2 Komentotilat

Tässä työssä esimerkkikonfiguraatiot on toteutettu Ciscon Catalyst 2960-sarjaan kuuluvalla kytkimellä. Kytkin sisältää Ciscon IOS-ohjelman, jolla voidaan konfiguroida kytkimen asetuksia komentoliittymän avulla. Tiettyjen asetusten toteuttamisen saattaa vaatia käyttäjää olemaan korkeammassa salasanalla suojatussa tilassa. Ciscon IOS-ohjelma sisältää 6 komentotilaa:

- User EXEC: Oletusarvoinen tila kytkimen käynnistyessä. Sallittujen asetusten määrä rajallinen. Tilan tunnistaa kytkimen nimen jälkeen tulevasta nuolimerkistä (>).

```
Switch>
```

Kuva 8. User EXEC-komentotila

- Privileged EXEC: Mahdollistaa järjestelmäkohtaisten asetusten toteuttamisen kuten laitteen uudelleenkäynnistämisen. Tila voidaan salasana suojata. Tilaan pääsee user EXEC-tilasta komennolla: "enable". Tilan tunnistaa ristikkomerkillä (#).

```
Switch>enable
Switch#
```

Kuva 9. Privileged EXEC-komentotila

- Global Configuration: Tila mahdollistaa tehdä asetuksia, jotka vaikuttavat miten laite tulee toimimaan. Tilaan pääsee Privileged EXEC-tilasta komennolla: "configure terminal".

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Kuva 10. Global Configuration-komentotila

- Interface Configuration: Tässä tilassa voidaan tehdä asetuksia kytkimen porteille. Tilaan pääsee Global Configuration tilasta komennolla: "interface [portin nimi]". Jos esimerkiksi haluttaisiin tehdä asetus kytkimen fastEthernet0/1 portille, olisi komento: "interface fastEthernet0/1". Kyseiseen tilaan voidaan myös valita useampi portti kerralla.

```
Switch(config)#interface fastEthernet0/1
Switch(config-if)#
```

Kuva 11. Interface Configuration-komentotila

- VLAN Configuration: Tila mahdollistaa tehdä VLAN kohtaisia asetuksia. Tilaan pääsee Global Configuration tilasta komennolla: "vlan [vlan numero]", esimerkiksi: "vlan 50".

```
Switch(config)#vlan 50
Switch(config-vlan)#
```

Kuva 12. VLAN Configuration-komentotila

- Line configuration: Tilaa käytetään vty-yhteyksien, kuten telnet- ja SSH-yhteyksien asetusten muokkaamiseen. Kyseiseen tilaan pääsee Global Configuration-tilasta komennolla “line vty [vty numero]”, esimerkiksi komento “line vty 0 15” valitsee asetusten kohteeksi vty- linjat 0–15.
(Command Reference 2016)

```
Switch(config)#line vty 0 15
Switch(config-line)#
```

Kuva 13. Line Configuration-komentotila

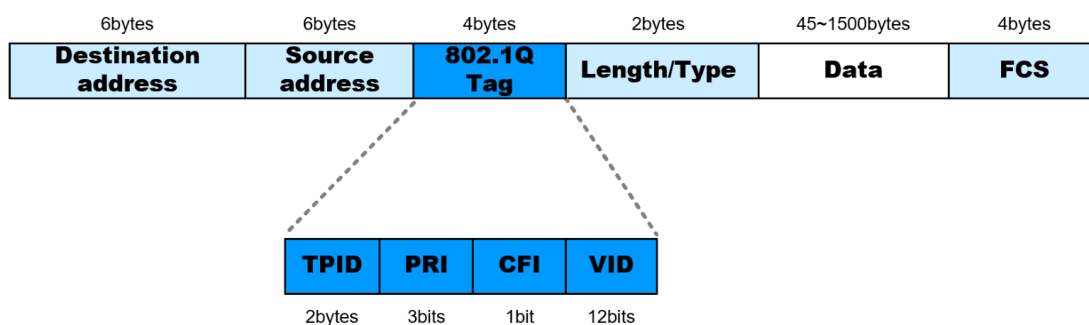
2.6.3 VLAN

VLAN (Virtual LAN) on hallittavista kytkimistä löytyvä ominaisuus, mikä mahdollistaa fyysisen verkon segmentoinnin pienempiin loogisiin broadcast toimialueisiin. Kytkimen portit konfiguroidaan kuuluvaksi tiettyyn VLANiin, mikä määrittää toimimaan tietyssä aliverkossa. Samassa VLANissa olevat portit jakavat saman broadcast- osoitteen ja eivät pysty kommunikoimaan toisten VLANien kanssa ilman reititintä. (Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture 2015)

IEEE 802.1Q standardiin perustuva VLAN-protokolla lisää tavalliseen ethernet-kehukseen 4-tavuisen tag- kentän, mikä sisältää kentät:

- Tag Protocol Identifier (TPID): kuvaa kehyksen tyyppiä. Arvo 0x8100 kertoo, että kyseessä on 802.1Q kehys.
- Priority (PRI): kuvaa kehyksen tärkeyttä. Käytetään datan priorisointiin.
- Canonical Format Indicator(CFI): Kertoo onko MAC-osoitteet kapseloitu. Ethernet verkoissa arvo aina 0.
- VLAN ID(VID): kuvaa VLAN arvoa, johon kehys kuuluu. Vois saada arvon väliltä 1–4094.

(Huawei 2021)

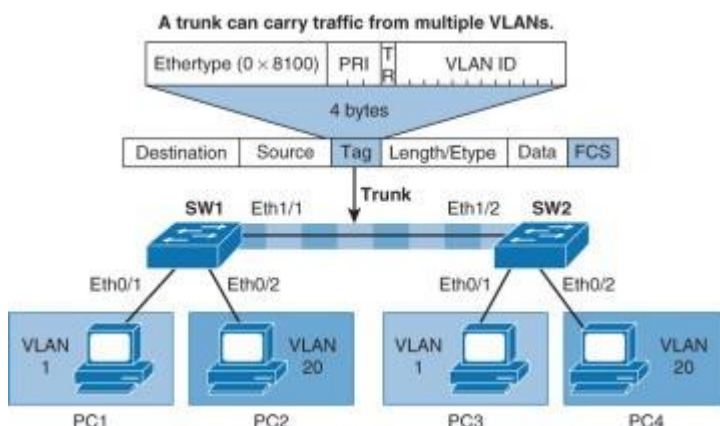


Kuva 14. VLAN-kehys (Huawei 2021)

VLAN tarjoaa keinon parantaa verkon kaistaa, segmentoimalla fyysisen lähiverkon verkon käyttämä broadcast- alue pienempiin VLANin käyttämiin broadcast-alueisiin. VLANit parantavat myös verkon tietoturva, sillä hyökkääjä ei pysty kaappaamaan koko verkon liikennettä. Lisäksi verkon segmentointi on halvempaa kytkinten tarjoamalla VLAN ominaisuudella, kuin jos segmentointi toteutettaisiin kalliimmilla reitittimillä. (Advantages of Virtual Local Area Network (VLAN) n.d.)

2.6.4 Trunk

Samat VLANit voivat sijaita useammissa kytkimissä ja jotta samassa VLANissa olevat laitteet pystyisivät kommunikoimaan toisessa kytkimessä olevan laitteen kanssa, on niille konfiguroitava trunk-linkki. Trunk-linkki konfiguroidaan kytkinten välille ja sen tarkoituksena on kuljettaa VLANien dataa linkin välityksellä. 802.1Q lisää linkille saapuvan kehykseen 4-tavuisen tag-kentän, minkä viimeiset 12-bittiä (VLAN ID) sisältävät kehyksen lähettäneen laitteen VLANin. Vastaanottava kytkin käsittelee saapuvan kehyksen ja poistaa VLAN ID kentän ennen kuin lähettää kehyksen vastaanottavalle laitteelle. (Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture 2015)



Kuva 15. TRUNK (Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture 2015)

2.6.5 Native VLAN

IEEE 802.1Q mahdollistaa myös sellaisten kehysten kulkemisen trunk-linkillä, mitkä eivät sisällä tag-kenttää. Kytkin laittaa tällaiset kehykset kuuluvaksi native VLANiin, mikä on Ciscon kytkimissä oletusarvoisesti VLAN 1. Trunk-linkin muodostavilla kytkimillä on oltava sama native VLAN konfiguroituna, jotta yhteys ongelmia ei syntyisi. (Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture 2015)

2.6.6 DTP

Ciscon kytkimistä löytyvä Dynamic Trunking Protocol (DTP) toiminto mahdollistaa toisiinsa kytkettyjen laitteiden porttien neuvotella trunk-tila.

Ciscon kytkimet tukevat 5 eri trunk-asetusta:

- Access: Pyrkii neuvottelemaan ei-trunk yhteyden kytkinten välille ja asettaa portin pysyvään ei-trunk tilaan.
- Trunk: Pyrkii neuvottelemaan trunk yhteyden kytkinten välille ja asettaa portin pysyvään trunking tilaan.

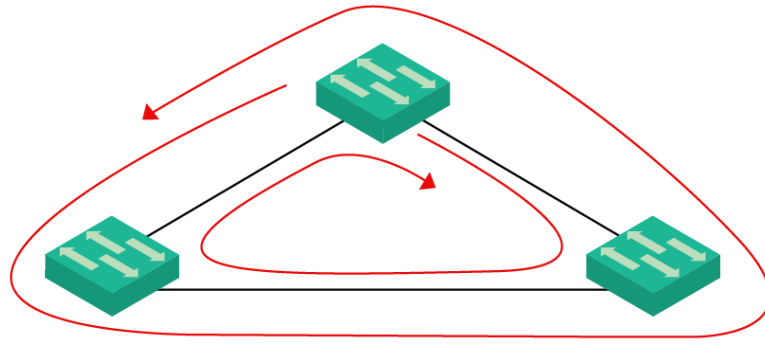
- **Nonegotiate:** Estää porttia lähettämästä DTP kehyksiä. Jos asetus on päällä, niin trunk-yhteyden muodostamiseksi portit on konfiguroitava manuaalisesti.
- **Dynamic desirable:** Portti pyrkii aktiivisesti muodostamaan trunk-yhteyden. Trunk-yhteys muodostetaan, jos vastapuolen kytkimen portti on tilassa trunk, desirable tai auto.
- **Dynamic auto:** Portti on valmis muodostamaan trunk-yhteyden, jos vastapuolen portti on tilassa trunk tai desirable. Oletusasetuksena Ciscon kytkimissä.

(Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture 2015)

2.7 STP

IEEE 802.1D standardiin perustuva STP (Spanning Tree Protocol) on kytkimissä toimiva protokolla, jonka päätarkoituksena on estää silmukoiden syntyminen ja mahdollistaa kytkinten välille vaihtoehtoinen reitti vikatilanteessa.

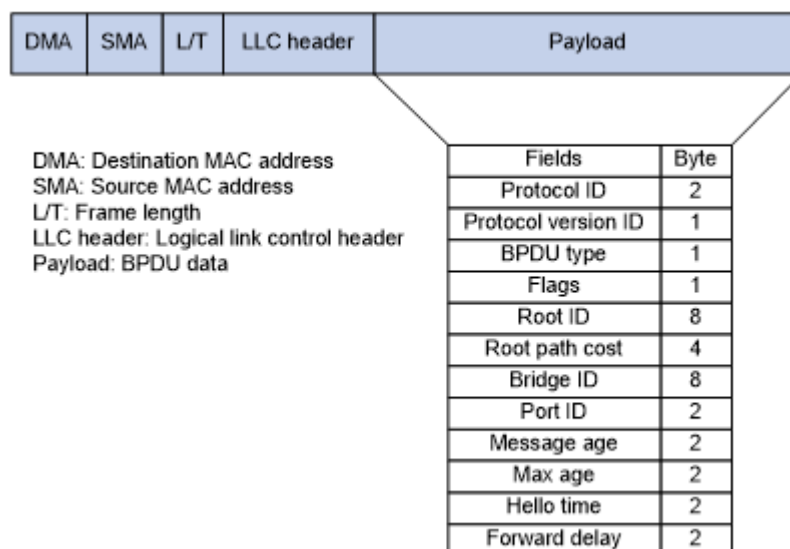
Silmukka voi syntyä, jos lähiverkkoon on liitettynä useampi kytkin toisiinsa ja verkossa oleviin päätelaitteisiin on olemassa useampi reitti. Jos verkossa on silmukka, verkossa toimivat päätelaitteet saattavat saada kopioita samasta viestistä useaan kertaan ja verkkolaitteet saattavat oppia saman päätelaitteen MAC-osoitteen usealla eri portilla. Silmukka voi tehdä verkon toiminnasta hyvin epävakaa. (STP and MST 2013)



Kuva 16. Silmukan syntymisen mahdollistava topologia (Maggio 2017)

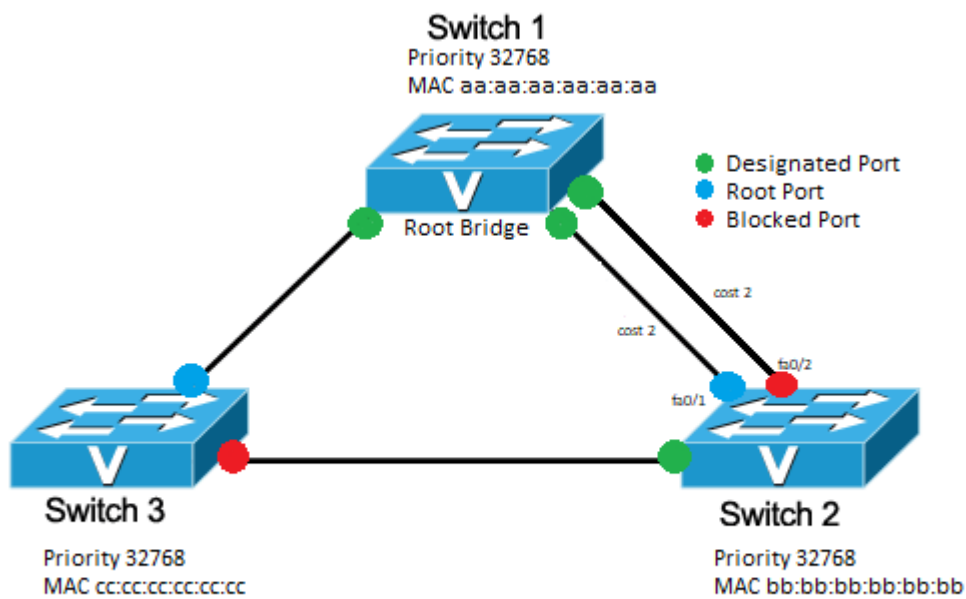
Jotta silmukka ei syntyisi, vain yksi aktiivinen reitti voi olla olemassa kytkinten välillä. STP käyttää hyväkseen algoritmia, mikä laskee verkossa parhaan mahdollisen reitin kytkinten välillä ja estää muita portteja lähettämästä dataa.

STP käyttää silmukka vapaan topologian rakentamisessa hyväkseen BPDU (Bridge Protocol Data Unit) -kehyksiä, jotka sisältävät tietoa lähettävästä kytkimestä ja sen porteista. Spanning tree-algoritmi valitsee ensin kytkimistä juurisillan (Root Bridge) mikä toimii hallinnollisena keskuksena silmukka vapaan reitin laskemiseksi. Valinta perustuu kytkinten valintaprosessissa mainostamasta BPDU-kehuksesta löytyvän 8-tavuisen BID (Bridge ID) arvon perusteella. Kytkin, jolla on pienin BID valitaan juurisillaksi. BID on oletusarvoisesti 32768, joten tasapeli tilanteessa se kytkin, jolla on pienin MAC-osoite, valitaan juurisillaksi. (STP and MST 2013)



Kuva 17. BPDU-kehiksen rakenne (STP protocol frames 2017)

Juurisillan valinnan jälkeen STP valitsee muiden kytkinten porteista yhden juuriportin (root port), joka johtaa kohti juurisiltaa ja sen määrättyä porttia kohti (designated port). STP pyrkii luomaan topologian, joka olisi verkon toiminnan kannalta tehokkain ja suosii reitin rakentamisessa portteja, jotka toimivat suuremmilla data nopeuksilla. Vain määrättyt- ja juuriportit voivat lähettää dataa kytkinten välillä. Muut portit STP asettaa tilaan blocked, ja sallii ainoastaan BPDU-kehysten kulkea niiden kautta, näin luoden silmukka vapaan topologian. (Vyncke, E. & Pagen, C. 2008)



Kuva 18. STP:n luoma silmukka vapaa topologia

3 KYTKIMIIN KOHDISTUVAT HYÖKKÄYKSET

Kytkimeen kohdistuvat hyökkäykset vaativat hyökkääjän laitteen olemaan fyysisesti kytkettynä kytkimeen. Ilman minkäänlaista tietoturva-asetusta hyökkääjän ei tarvitse muuta kuin kiinnittää oma tietokone johdolla kytkimestä löytyvään porttiin, niin hänellä on pääsy verkkoon, mahdollistaen hänen suorittaa lukuisia hyökkäyksiä lähiverkkoon.

Tyypillisimmät kytkimeen kohdistuvat hyökkäykset ovat niin sanottuja “spoofing” hyökkäyksiä, joissa hyökkääjä yrittää esittää olevansa joku toinen. Hyökkäykset ovat tyypillisimpiä, sillä lähiverkon käyttämät protokollat eivät sisällä sisäänrakennettuja autentikointimenetelmiä. Spoofing hyökkäykset voivat johtaa MITM (Man in the Middle) hyökkäykseen, jossa kahden osapuolen väliseksi tarkoitettu liikenne, kulkee kolmannen osapuolen (hyökkääjän) kautta, mahdollistaen mm. arkaluontoisen datan varastamisen.

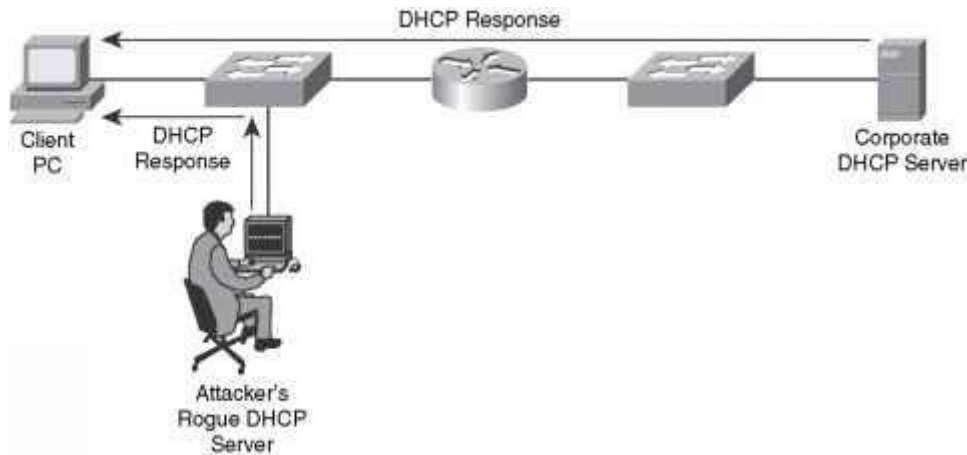
Hyökkääjän motiivina voi myös olla tehdä verkko tai verkossa toimiva palvelu käyttökelvottomaksi muille käyttäjille DoS- (Denial of service) kaltaisten hyökkäysten avulla.

Tässä kappaleessa esitetään tyypillisimpiä yllä mainittujen kaltaisia hyökkäyksiä, joita hyökkääjät kohdistavat kytkimeen.

3.1 DHCP-palvelimen spoofaus

DHCP-palvelimen spoofauksessa hyökkääjä yrittää esittää olevansa verkossa toimiva virallinen DHCP-palvelin. DHCP-palvelin toimii normaalisti palvelemalla asiakkaita antamalla mm. IP- osoitteen, verkon DNS-palvelimen ja oletusyhdyskäytävän. DHCP-palvelimia voi olla verkossa useampia, ja kun asiakas pyytää palvelimelta esimerkiksi IP- osoitetta, se käyttää sen palvelimen tietoja, joka vastaa pyyntöön nopeitten. Jos hyökkääjä onnistuu asentamaan lähiverkkoon oman DHCP-palvelimen, se kuuntelee DHCPDISCOVER viestejä ja palvelee asiakkaita samalla tavalla kuin verkon oikea DHCP-palvelin, mutta tarjoaa asiakkaalle

vääriä osoitetietoja, mitkä voivat johtaa MITM- hyökkäykseen. (DHCP Starvation attacks and DHCP spoofing attacks n.d.)



Kuva 19. DHCP-hyökkäys (Ccexpert 2021)

Yllä olevassa kuvassa hyökkääjän DHCP-palvelin on fyysisesti lähempänä kuin verkon oikea DHCP-palvelin, mikä lisää todennäköisyyttä, että hyökkäys onnistuu.

3.2 IP-osoitteiden näännyttäminen

DHCP-palvelin pystyy tarjoamaan rajatun verran IP- osoitteita asiakkaille. Jos osoitteet loppuvat kesken DHCP- palvelin pystyy palvelemaan uutta asiakasta vasta kun käytössä oleva osoite vapautuu. Hyökkääjän on mahdollista tehdä verkkoon DoS-hyökkäys varaamalla DHCP- palvelimelta kaikki tarjolla olevat IP- osoitteet, jolloin muut käyttäjät eivät pääse käyttämään verkkoa. Hyökkääjä varaa IP- osoitteet esimerkiksi Gobblersin kaltaisella ohjelmalla, mikä lähettää verkkoon monta DHCPDISCOVER pakettia satunnaisella MAC-osoitteella ja nopeaan tahtiin. Palvelin ei osaa erottaa hyökkääjän tekemiä pyyntöjä oikean käyttäjän tekemistä pyynnöistä. (Vyncke, E. & Paggen, C. 2008)

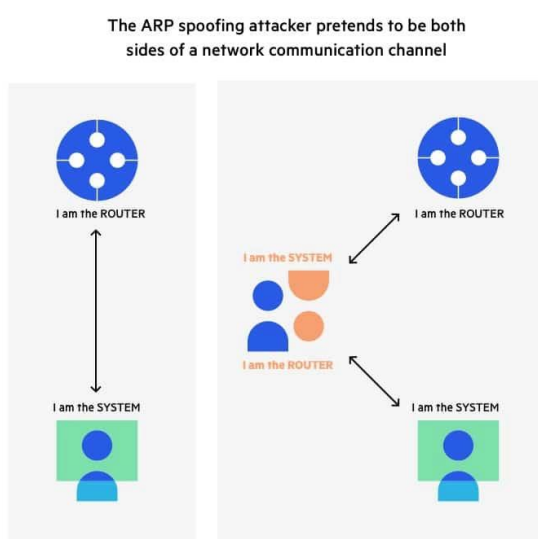
3.3 MAC flooding

Kytkeymen muistissa sijaitseva CAM-taulu voi pitää sisällään rajatun määrän arvoja kytkimen tyypistä ja mallista riippumatta. Hyökkääjä voi käyttää hyväkseen

tätä tietoa lähettämällä kytkimille suuria määriä kehyksiä, jotka sisältävät vale MAC-lähdeosoitteita, kunnes CAM-taulu on täynnä eikä pysty enää lisäämään uusia merkintöjä. Taulu pysyy täynnä niin kauan kuin, kun hyökkääjä lähettää kehyksiä verkkoon. Tämän seurauksena kytkin ei enää pysty suoriutumaan sen olennaisesta tehtävästään, vaan lähettää kaikki sille saapuvat kehykset ulos jokaisesta sen portista. Tämä mahdollistaa hyökkääjän kaapata verkossa tapahtuvaa liikennettä. Vaikka hyökkäys kohdistettaisiin vain yhteen kytkimeen, sen seurauksena myös muiden verkossa olevien kytkinten CAM-taulut täyttyvät. Kyseisessä hyökkäyksessä käytetyt ohjelmat pystyvät lähettämään, jopa satoja tuhansia valekehyksiä minuutissa. (Popeskic, V 2011)

3.4 ARP-spooffaus

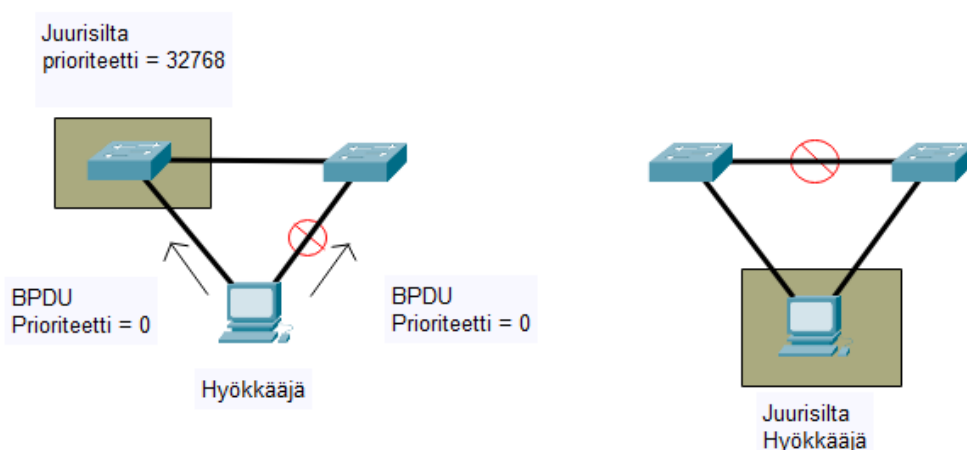
ARP-protokollan heikkoutena on, että se ei pysty varmistamaan, että ARP-kyselyyn on vastannut oikea osapuoli. Se mahdollistaa myös osapuolen hyväksymään ARP-vastauksia, vaikka tämä ei olisi lähettänyt kyselyä. Tämä protokollassa piilevä heikkous mahdollistaa ARP-spooffauksen. ARP-spooffaus on MITM-hyökkäys, jossa hyökkääjä sieppaa liikennettä kahden laitteen väliltä. Hyökkääjä lähettää ARP-vastauksen kohteelle, jossa väittää olevansa verkon reititin ja reitittimelle ARP-vastauksen, jossa väittää olevansa kohde. Sekä kohde että reititin päivittävät ARP-välimuistin uusilla osoitetiedoilla ja kommunikoivat hyökkääjän laitteen kanssa eivätkä suoraan toistensa kanssa. (Imperva n.d.)



Kuva 20. ARP- spoofing (Imperva n.d)

3.5 STP-hyökkäys

Spanning tree protokolla ei sisällä itsessään minkäänlaista suojaus tai autentikointi mekanisme ja hyökkääjää pystyy vaikuttamaan juurisillan valintaan esimerkiksi Yersinian kaltaisella hyökkäysohjelmalla. Yersinia kuuntelee kytkinten lähettämiä BPDU- kehyksiä ja informoi sen käyttäjää mm. nykyisen juurisillan BID- arvon. Hyökkääjän on mahdollista muuttaa verkon topologiaa väittämällä olevansa juurikytin, mikä pakottaa STP:n uudelleen laskun. Tämä onnistuu lähettämällä muille kytkimille BPDU- kehyksiä, joissa BID- kentän arvo on pienempi kuin sen hetkisen juurikytimen BID tai samalla BID- arvolla mutta pienemmällä MAC-osoitteella. Hyökkäyksen onnistuttua hyökkääjän on mahdollista kaapata kehyksiä, joihin hänellä ei aikaisemmin ollut pääsyä. (Vyncke, E. & Paggen, C. 2008)



Kuva 21. STP-hyökkäys

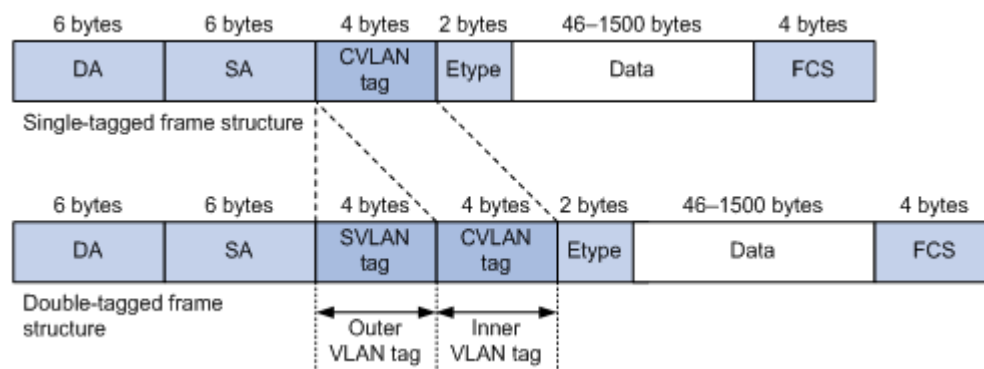
Hyökkääjän on myös mahdollista suorittaa verkkoon DoS-hyökkäys, lähettämällä kytkimelle tuhansia BPDU-kehyksiä sekunnissa, jolloin kytkimen prosessori ylikuormittuu, eikä pysty palvelemaan muuta liikennettä. Kyseistä hyökkäystä voi olla vaikea havaita, sillä STP ei varoita suurista määristä kehyksistä, joita se käsittelee. (Vyncke, E. & Paggen, C. 2008)

3.6 VLAN-hyökkäykset

VLANeihin kohdistuu kahdenlaisia hyökkäyksiä verkon sisältä: Double tagging ja kytkin spoofaus hyökkäyksiä

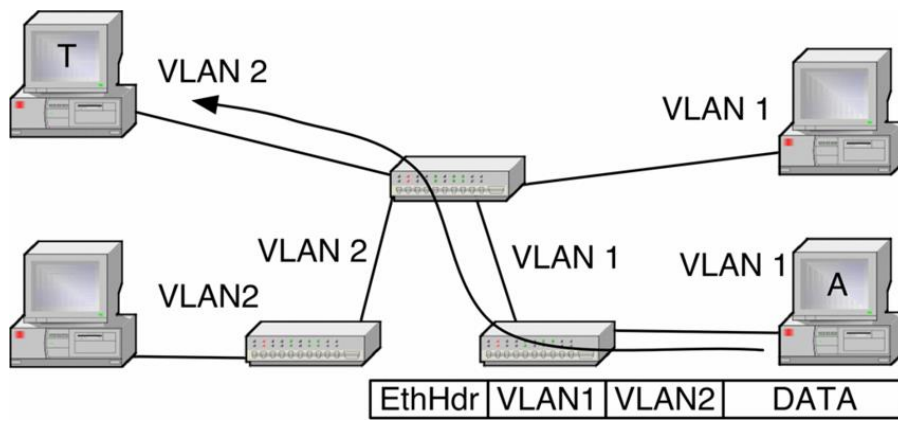
3.6.1 Double tagging

802.1Q standardi sallii ethernet-kehyksissä olevan useampia tag- kenttiä. Hyökkääjän on mahdollista käyttää tätä ominaisuutta hyväkseen niin sanotussa Double tagging- hyökkäyksessä, jonka tarkoituksena on hyökätä eri VLANissa sijaitsevaan laitteeseen. Kyseinen hyökkäys on mahdollista vain siinä tapauksessa, että hyökkääjä on samassa VLANissa kuin kytkimen native trunk VLAN. (Alsouqi 2019)



Kuva 22. (How QinQ works 2017)

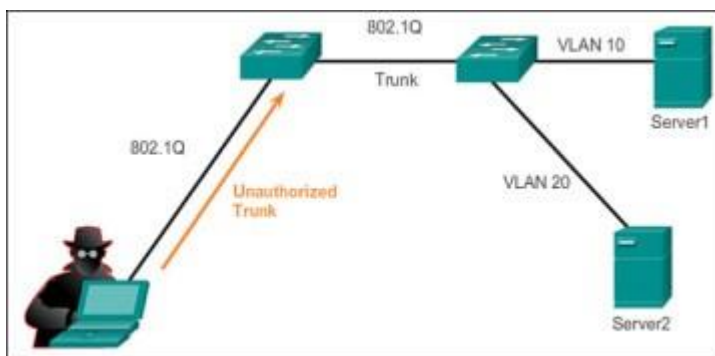
Double tagging-hyökkäyksessä hyökkääjä lisää ethernet-kehukseen normaalin tag- kentän sijaan kaksi tag-kenttää: sisäisen (Inner) ja ulkoisen (Outer) tag-kentän. Sisäinen kenttä sisältää hyökkäyksen kohteena olevan laitteen VLAN ID-arvon ja ulkoinen kenttä sisältää hyökkääjän VLAN ID-arvon, mikä on sama kuin native VLAN. Kun hyökkääjä lähettää suoraan liittyneelle kytkimelle double tag-kehysten, kytkin poistaa kehyksestä ulkoisen tag- kentän ja lähettää kehyksen eteenpäin kaikkien saman native VLANin sisältävien porttien ja trunk-linkin kautta. Koska kyseessä on native VLAN, lähettävä kytkin ei enää lisää uutta tagia kehykseen vaan jäljelle jää yksi sisäinen tag-kenttä. Kun kohteena olevan laitteen sisältävä kytkin vastaanottaa kehyksen, se lukee kehyksen sisältävän tag-kentän VLAN ID-arvon ja lähettää kehyksen oikealle laitteelle. (Alsouqi 2019)



Kuva 23. Double Tagging- hyökkäys (Kiravuo, Särelä, Manner 2013, 1481)

3.6.2 Kytkimen spooffaus

Kytken portit ovat oletusarvoisesti tilassa Dynamic auto, trunk liityntöjen muodostamisen helpottamiseksi verkossa. Hyökkääjän on mahdollista esittää olevansa kytkin lähettämällä hyökkäysohjelmalla DTP- ja 802.1Q-kehäksiä oikealle kytkimelle, joilla se yrittää muodostaa trunk- linkin hyökkääjän tietokoneen ja kytkimen välillä. Jos hyökkäys onnistuu, hyökkääjällä on pääsy kaikkiin trunk-portilla sallittuihin VLANeihin. (Cisco Networking Academy's Introduction to VLANs 2014)



KUVA 24. Luvaton Trunk-yhteys (Cisco Networking Academy Switched Networks Companion Guide: VLANs 2014)

4 HYÖKKÄYKSILTÄ SUOJAUTUMINEN

Tässä kappaleessa esitetään hallittavista kytkimistä löytyviä asetuksia, joilla voidaan suojautua edellisessä kappaleessa esitetyiltä hyökkäyksiltä. Kappaleessa käytettyjen esimerkki konfiguraatioiden on tarkoitus antaa yleiskuva niiden toimivuudesta erilaisia hyökkäyksiä vastaan.

4.1 Käyttämättömien porttien sulkeminen

Oletusarvoisesti kaikki kytkimen liitinportit ovat päällä, mikä mahdollistaa luvattomien käyttäjien liittyä verkkoon helposti. Turvallisuuden kannalta on hyvä sulkea portit, joita ei käytetä ja lisätä ne omaan VLANiin. Suljetuiksi valitut portit voidaan sulkea manuaalisesti Interface Configuration-tilassa komennolla: "shutdown".

```
Switch(config)#interface range fa0/5 - 24
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down
```

Kuva 25. Porttien sulkeminen

4.2 Port Security

Kytken port security ominaisuudella voidaan rajoittaa sallittujen laitteiden määrää portissa MAC-osoitteiden perusteella. Toiminnoilla voidaan mm. varmistaa, että kytkimen portteihin on liitetty vain sille tarkoitettut laitteet, sekä suojautua MAC-flooding kaltaista hyökkäystä vastaan.

Port security ominaisuus voidaan ottaa päälle portilla Interface Configuration komentotilassa komennolla: "switchport port-security". Toimiakseen portin on oltava access modessa.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

KUVA 26. Port Security asetuksen käyttöönotto valitulla portilla

Sallittujen laitteiden määrää porteissa voidaan konfiguroida "maximum" komennolla.

```
Switch(config-if)#switchport port-security maximum 4
```

Kuva 27. Sallittujen laitteiden määrän konfiguroiminen portilla.

Port security voidaan konfiguroida kolmella eri tavalla:

- Dynaamisesti: Kytkin tallentaa porttiin kytketyn laitteen MAC osoitteen osoitetauluun, mutta se häviää, kun kytkin suljetaan tai uudelleen käynnistetään. Oletusarvoisesti päällä, kun port-security käynnistetään portilla.
- Staattisesti: Antamalla manuaalisesti sallitun laitteen MAC osoite portille. Osoitteet tallentuvat osoite tauluun ja pysyvät kytkimen muistissa.

```
Switch(config-if)#switchport port-security mac-address 029b.b0cb.aafc
```

KUVA 28. Sallitun laitteen konfiguroiminen MAC-osoitteen perusteella

- Sticky: Sama kuin dynaamisesti opittu mutta tallentaa osoitteen kytkimen muistiin. Voi sisältää myös staattisesti määritettyjä osoitteita.

```
Switch(config-if)#switchport port-security mac-address sticky
```

Kuva 29. Sticky asetuksen määrittäminen portilla

4.2.1 Port Security rikkomus

Kytkimen porttiin voidaan määrittää kolme erilaista rikkomustyyppiä, jotka määrittävät miten portin tulee toimia, jos rikkomus on tapahtunut. Rikkomus aiheutuu, jos porttiin sallittujen MAC-osoitteiden määrä täyttyy tai jos porttiin kytkeytyy laite, jonka MAC-osoite ei vastaa portissa sallittua osoitetta. Rikkomus tyyppi voidaan konfiguroida porttiin komennolla: "switchport port-security-violation [rikkomuksen tyyppi]".

- Protect: Pudottaa muiden kuin sallittujen MAC osoitteiden omaavien laitteiden kehukset. Vähiten turvallinen vaihtoehto.

```
Switch(config-if)#switchport port-security violation protect
```

Kuva 30. Protect rikkomuksen asetus

- Restrict: Toimii kuten Protect mutta lisäksi kasvattaa Security violation count arvoa yhdellä ja lähettää syslog viestin.

```
Switch(config-if)#switchport port-security violation restrict
```

Kuva 31. Restrict rikkomuksen asetus

- Shutdown: Shutdown rikkomus on oletusarvoisesti päällä, jos muuta tilaa ei määritellä. Portti menee error-disabled tilaan, sulkee portin ja nostaa violation counteria. Toimiakseen portti on manuaalisesti nostettava takaisin ylös.

```
Sl(config-if)#switchport port-security violation shutdown
```

Kuva 32. Shutdown rikkomuksen asetus

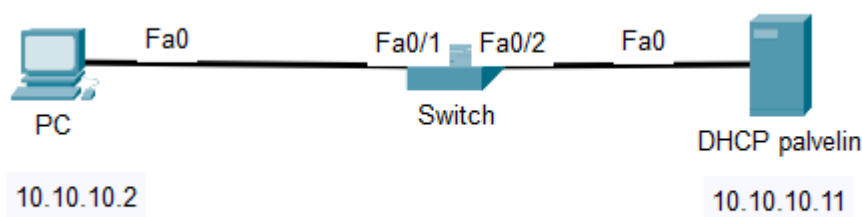
4.3 DHCP snooping

DHCP-spooffaus ja osoitteiden näännyttämisyrityksiä voidaan estää Ciscon kytkimiltä löytyvän DHCP snooping toiminnon avulla. Kytkimen portit voidaan konfiguroida luotetuiksi (trusted) tai ei-luotetuiksi (untrusted). Luotetut portit pystyvät vastaanottamaan DHCPDISCOVER ja DHCPREQUEST paketteja mutta ei-luotetut portit suodattavat ne pois. Jos hyökkääjä yrittää lähettää DHCP-vastauksen verkkoon, ei-luotetulla portilla DHCP snooping sulkee kyseisen portin. Luotetuiksi porteiksi konfiguroidaan portit, joihin verkon virallinen DHCP-palvelin on kytkeytyneenä, ei-luotetuiksi taas ne, jotka sisältävät tavallisia käyttäjiä kuten access-portit. (Vyncke, E. & Paggen, C. 2008)

DHCP snooping käyttää hyväkseen kytkimen muistissa olevaa DHCP binding-taulua, mikä sisältää tietoa mm. DHCP-palvelimen laitteille lainatuista IP-osoit-

teista ja kyseisen laitteen MAC-osoitteista. DHCP snooping vertaa portille saapuvassa DHCP-viestissä olevia osoitetietoja portin binding-taulussa oleviin tietoihin ja hylkää paketin, jos tiedot eivät täsmää. (Vyncke, E. & Paggen, C. 2008)

DHCP snooping ominaisuus voidaan ottaa käyttöön Global Configuration komenttilassa komennolla "ip dhcp snooping". Oletusarvoisesti kaikki kytkimen portit ovat ei-luotettuja, joten luotetut portit on määriteltävä manuaalisesti komennolla "ip dhcp snooping trust". Ominaisuudella voidaan myös rajoittaa DHCP kyselyiden määrää per sekunti ei-luotetuissa porteissa komennolla: "ip dhcp snooping limit rate (määrä)". Alla olevassa kuvassa on yksinkertaiseen VLAN 10 topologiaan konfiguroitu DHCP snooping.



Kuva 33. Esimerkki VLAN 10 kuuluvien laitteiden topologia.

```

Switch(config)#ip dhcp snooping
Switch(config)#interface fa0/2
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#interface range fa0/1, fa0/3 - 24
Switch(config-if-range)#ip dhcp snooping limit rate 5
Switch(config-if-range)#exit
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#end
  
```

Kuva 34. DHCP Snooping konfigurointi

Kytkin portti fastEthernet0/2 (fa0/2) sisältää linkin verkon DHCP palvelimelle mikä on määriteltä luotetuksi. Kytkimen kaikki muut portit ovat oletuksineen ei-luotettuja, ja niiden lähettämiä DHCP kyselyiden nopeutta on rajoitettu viiteen kyselyyn per sekunti. DHCP snooping on konfiguroitu toimimaan VLAN 10 sijaitseville laitteille. Kytkimen DHCP snooping binding taulua voidaan tarkastella Privileged EXEC tilassa komennolla: "show ip dhcp snooping binding".

```
Switch#show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN
Interface
-----
00:E0:F9:48:51:25  10.10.10.2      86400      dhcp-snooping  10
FastEthernet0/1
Total number of bindings: 1
```

Kuva 35. Snooping Binding-taulun keräämät osoitteet

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface      Trusted      Rate limit (pps)
-----
FastEthernet0/9      no          5
FastEthernet0/5      no          5
FastEthernet0/12     no          5
FastEthernet0/1      no          5
FastEthernet0/3      no          5
FastEthernet0/7      no          5
FastEthernet0/2      yes         unlimited
FastEthernet0/4      no          5
FastEthernet0/6      no          5
```

Kuva 36. DHCP Snooping-asetukset

4.4 DAI

DAI (Dynamic ARP Inspection) on ominaisuus kytkimillä, joilla voidaan suojautua ARP-spooffausta vastaan. DAI varmistaa ei-luotetuilla porteilla kulkevan ARP liikenteen vertaamalla lähettäjän MAC- ja IP- osoitetta sen DHCP snooping binding-taulussa kirjattuihin osoitteisiin. Jos osoitteet eivät vastaa toisiaan, DAI pudottaa ARP-kehukset. DAI ominaisuus saadaan päälle Global Configuration tilassa komennolla: "ip arp inspection vlan [vlan numero]". Toimiakseen kytkimessä on ensin oltava konfiguroituna DHCP snooping ominaisuus.

```
Switch(config)#ip arp inspection vlan 10
Switch(config)#interface fa0/2
Switch(config-if)#ip arp inspection trust
```

Kuva 37. FastEthernet0/2 portin asettaminen luotetuksi

Yllä olevan kuvan esimerkissä DAI on konfiguroitu kuvan 33 topologialle, jossa DHCP snooping on jo määritelty. DHCP palvelimelle määritetty portti fa0/2 määritetään luotetuksi komennolla "ip arp inspection trust".

Määriteltyjä asetuksia porteilla voidaan tarkastella Privileged EXEC tilassa komennolla "show ip arp inspection interfaces".

```
Switch#show ip arp inspection interfaces
```

Interface	Trust State	Rate(pps)	Burst Interval
-----	-----	-----	-----
Fa0/1	Untrusted	15	1
Fa0/2	Trusted	15	1

Kuva 38. DAI-asetukset

DAI rajaa oletusarvoisesti sisään tulevat ARP-kehykset 15: toista per sekunti (Rate(pps))), sillä se käyttää kytkimen prosessoria saapuvien ARP-kehysten oikeellisuuden tarkastamisessa, ja estää hyökkääjää toteuttamasta DoS-hyökkäystä. (Configuring Dynamic ARP Inspection 2016)

4.5 PortFast BPDU Guard

BPDU Guard on ominaisuus, jolla voidaan estää hyökkääjää vaikuttamasta juurisillan valintaan ja STP topologian muuttamiseen. BPDU Guard konfiguroidaan tyypillisesti kytkin porteille, joilla on PortFast ominaisuus käytössä. PortFast mahdollistaa portin siirtyä suoraan lähettämään dataa, ja ohittaa monta vaihetta, joita STP prosessi sisältää. PortFast konfiguroidaan tyypillisesti tavallisia käyttäjiä sisältäviin access portteihin. BPDU Guardilla konfiguroitu kytkin hylkää kaikilta PortFast porteilta vastaanotetut BPDU kehykset ja sulkee portit estäen niitä lähettämästä enempää dataa. (Spanning Tree PortFast BPDU Guard Enhancement 2005)

BPDU Guard-asetus saadaan päälle kaikilla PortFast asetuksen konfiguroiduille porteille Global Configuration komentotilassa komennolla: "spanning-tree portfast bpduguard default".

```
Switch(config)#spanning-tree portfast bpduguard default
```

Kuva 39. BPDU Guard-asetuksen päälle ottaminen

Privileged EXEC komentotilassa komennolla: “show spanning-tree summary”, voidaan tarkastaa, että BPDU Guard ja PortFast toiminnot ovat päällä, eli enabled tilassa.

```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID          is enabled
Portfast Default            is enabled
Portfast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default           is disabled
EtherChannel misconfig guard is disabled
UplinkFast                  is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                          Blocking Listening Learning Forwarding STP Active
-----
```

Kuva 40. Konfiguroitujen asetusten tarkistaminen

4.6 Suojautuminen VLAN-hyökkäyksiltä

VLAN hyökkäyksiä vastaan on tärkeää olla jättämättä DTP oletusasetuksia päälle. Kytkin-spooffaus yrityksiä vastaan tulisi jokainen käytössä oleva kytkimen porttiliitäntä konfiguroida manuaalisesti joko access- tai trunk-tilaan, sekä sulkea DTP-asetus kokonaan jokaisessa portissa Interface Configuration komentotilassa komennolla: “switchport nonegotiate”. (Att 2019)

```
Switch(config)#interface range fastEthernet0/1-fastEthernet0/12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport nonegotiate
```

Kuva 41. Valittujen porttien asettaminen acces-tilaan ja DTP:n pois kytkeminen

Paras keino suojautua double tagging-hyökkäyksiltä on varmistaa, että käyttäjäkohtaisten porttien native VLAN on eri kuin trunk- porttien native VLAN. (Att 2019)

5 JOHTOPÄÄTÖKSET

Tässä opinnäytetyössä on esitetty hallittavista kytkimistä löytyviä asetuksia, joilla voidaan vahvistaa kytkimen tietoturvaa. Työssä on myös esitetty lähiverkon toimintaa, lähiverkon käyttämiä protokollia ja kuinka nämä tietoturvan näkökulmasta heikot protokollat voidaan vahvistaa kytkinten tarjoamien tietoturva-asetusten avulla. Lisäksi työssä on kuvattu keinoja, joita hyökkääjät käyttävät aiheuttamaan vahinkoa lähiverkolle ja sen käyttäjille.

Tietoturvan merkitys on jatkuvasti kasvamassa ja hyökkäysten toteuttaminen on entistä helpompaa sillä hyökkääjien ei enää tarvitse olla teknisesti taitavia vaan pystyvät käyttämään valmiita ohjelmia yhden napin painalluksella.

Lähiverkon ja kytkinten tietoturvan merkitys on erityisesti noussut, sillä monet yritykset ulkoistavat palveluitansa pilveen, jolloin yritysten ei itse tarvitse ostaa ja konfiguroida verkkolaitteita, vaan sen hoitavat pilvipalveluiden tarjoajat. Kyseisten tarjoajien verkkolaitteet kuitenkin toimivat samalla tekniikalla ja ovat alttiita samoille hyökkäyksille mutta hyökkäyksen aiheuttamat vahingot voivat olla paljon suurempia.

LÄHTEET

What is a LAN? n.d. Cisco. Verkkosivu. Viitattu 11.10.2021.

<https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html>

Burke, J & Partsenidis, C. 2021. What's the difference between a MAC address and IP address? Verkkosivu. Viitattu 11.10.2021. <https://www.tech-target.com/searchnetworking/answer/What-is-the-difference-between-an-IP-address-and-a-physical-address>

Ethernet Switching. 2020. Cisco Press. Verkkosivu. Viitattu 10.10.2021.

<https://www.ciscopress.com/articles/article.asp?p=3089352&seqNum=4>

Fiber Optical Networking. 2018. Unicast vs Multicast vs Broadcast: What Are the Differences? Verkkosivu. Viitattu 10.11.2021. <https://www.fiber-optical-networking.com/unicast-vs-multicast-vs-broadcast-differences.html>

IBM. n.d. Address Resolution Protocol. Verkkosivu. Viitattu 8.9.2021.

<https://www.ibm.com/docs/en/aix/7.1?topic=protocols-address-resolution-protocol>

Geek University. n.d. Address Resolution Protocol (ARP). Verkkosivu. Viitattu 10.11.2021.

<https://geek-university.com/ccna/address-resolution-protocol-arp/>

ComputerNetworkingNotes. 2020. How DHCP works Explained with Examples.

Verkkosivu. Viitattu 7.11.2021. <https://www.computernetworkingnotes.com/ccna-study-guide/how-dhcp-works-explained-with-examples.html>

Vyncke, E. & Paggen, C. 2008. LAN Switch Security: What Hackers Know About Your Switches. 1. st ed. Indianapolis, Indiana: Cisco Press. Viitattu 10.11.2021.

Vaatii käyttöoikeuden. <https://www.amazon.com/LAN-Switch-Security-Networking-Technology-ebook/dp/B0015KGXCI>

Grandmetric. 2018. How does a switch work? Verkkosivu. Viitattu 17.9.2021.

<https://www.grandmetric.com/2018/03/08/how-does-switch-work-2/>

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning

Guide: Network Design Fundamentals. 2015. Cisco Press. Verkkosivu. Viitattu 13.11.2021.

Verkkosivu. <https://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2>

Maggio, A. 2017. Understanding Spanning Tree Protocol (STP). Verkkosivu. Viitattu 8.11.2021.

<https://www.ictshore.com/free-ccna-course/stp-understanding-spanning-tree/>

STP protocol frames. 2017. HPE. Verkkosivu. Viitattu 16.11.2021. https://tech-hub.hpe.com/eginfolib/networking/docs/switches/5980/5200-3921_l2-lan_cg/content/499036672.htm

Shaw, K. 2020. What is a network switch, and how does it work? Verkkosivu. Viitattu 14.10.2021. <https://www.networkworld.com/article/3584876/what-is-a-network-switch-and-how-does-it-work.html>

Command Reference. 2016. Cisco. Verkkosivu. Viitattu 20.11.2021. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_2_e/command/reference/cr_2960/intro.html

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture. 2015. Cisco Press. Verkkosivu. Viitattu 27.8.2021. <https://www.ciscopress.com/articles/article.asp?p=2348266>

Huawei. 2021. Understanding of VLAN - Basic Concepts of VLAN. Verkkosivu. Viitattu 21.11.2021. <https://forum.huawei.com/enterprise/en/understanding-of-vlan-basic-concepts-of-vlan/thread/745891-861>

Advantages of Virtual Local Area Network (VLAN). n.d. Omnisecu. Verkkosivu. Viitattu 12.11.2021. <https://www.omnisecu.com/cisco-certified-network-associate-ccna/advantages-of-vlan.php>

STP and MST. 2013. Cisco. Verkkosivu. Viitattu 8.11.2021. <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/spanningtree.html#wp1020362>

How QinQ works. 2017. HPE. Verkkosivu. Viitattu 26.10.2021. https://tech-hub.hpe.com/eginfolib/networking/docs/switches/5950/5200-2216a_l2-lan_cg/content/472583750.htm

Ccexpert. 2021. Combating DHCP Server Spoofing. Verkkosivu. Viitattu 10.11.2021. <https://www.ccexpert.us/configuration-mode/combating-dhcp-server-spoofing.html>

DHCP Starvation and DHCP Spoofing attacks. n.d. Omnisecu. Verkkosivu. Viitattu 20.9.2021. <https://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>

Meraki. 2021. Spanning Tree Protocol (STP) Overview. Verkkosivu. Viitattu 24.11.2021. [https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_\(STP\)_Overview](https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview)

Popeskic, V. 2011. Verkkosivu. MAC Address Flooding – MAC address table overflow attacks. Verkkosivu. Viitattu 11.10.2021. <https://howdoesinternet-work.com/2011/mac-address-flooding>

Imperva. n.d. What is ARP Spoofing (ARP Poisoning). Verkkosivu. Viitattu 28.9.2021. <https://www.imperva.com/learn/application-security/arp-spoofing/>

Kiravuo, T., Särelä, M. & Manner, J. 2013. A Survey of Ethernet LAN Security. IEEE Communications Surveys & Tutorials (Volume: 15, Issue: 3, Third Quarter 2013, 1477 – 1491. Viitattu 19.11.2021. DOI: 10.1109/SURV.2012.121112.00190

Cisco Networking Academy's Introduction to VLANs. 2014. Cisco Press. Verkkosivu. Viitattu 2.10.2021. <https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=10>

Alsouqi, A. 2019. VLAN1 and Vlan Hopping Attack. Blue Network Security-blogi. 1.8.2019. Viitattu 14.10.2021. <https://bluenetsec.com/vlan1-and-vlan-hopping-attack/>

Cisco Networking Academy Switched Networks Companion Guide: VLANs. 2014. Cisco Press. Verkkosivu. Viitattu 2.10.2021. <https://www.ciscopress.com/articles/article.asp?p=2208697&seqNum=6>

Configuring Dynamic ARP Inspection. 2016. Cisco. Verkkosivu. Viitattu 22.11.2012. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swdynarp.html

Spanning Tree PortFast BPDUGuard Enhancement. 2005. Cisco. Verkkosivu. Viitattu 22.11.2012. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html>

Att. 2019. VLAN Hopping: How to Mitigate an Attack. At&t kyberturvallisuus-blogi 19.12.2019. Viitattu 24.11.2021. <https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation>

LIITTEET

Liite 1. Kytkinten välinen trunk-linkki

