



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Eemi Oksanen

# Kytkentäisen lähiverkon suojaaminen olemassa olevilla teknologioilla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

1.6.2019

Tekijä Otsikko	Eemi Oksanen Kytkeäisen lähiverkon suojaaminen olemassa olevilla teknologioilla
Sivumäärä Aika	38 sivua 1.6.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tietotekniikka
Ammatillinen pääaine	Tietoverkot
Ohjaajat	Yliopettaja Matti Puska Lehtori Marko Uusitalo
<p>Tässä opinnäytetyössä käsitellään erään suuren monikansallisen tilintarkastusyrityksen kiinteän sisäverkon laitteiden tietoturvamekanismien ominaisuuksia. Työn tarkoituksena oli perehtyä mekanismien toimintaan, testata niiden toimivuus ja soveltuvuus sekä tehdä päätös käyttöönotosta havaintojen perusteella.</p> <p>Yrityksen sisäverkon pohjana käytettiin verkkolaittevalmistaja Juniperin kytkimiä. Käytetyt kytkimet tarjoavat riittävästi kapasiteettia myös tulevaisuudessa, vaikka yrityksen työntekijämäärä kasvaisikin merkittävästi.</p> <p>Käyttöön otettujen tietoturvamekanismien myötä sisäverkon tietoturvaa saatiin parannettua selvästi tiettyjä yleisiä hyökkäystapoja vastaan. Kaikkia tarkasteltuja mekanismeja ei päätetty ottaa käyttöön, mutta tulevaisuutta ajatellen kertyi arvokasta tietoa. Tämän tiedon perusteella on helppo testata asioita myöhemmin uudelleen ja harkita mahdollista käyttöönottoa.</p> <p>Tämän työn tarkoituksena on kertoa yleisesti käytössä olevia asioita yritysten sisäverkoista, sekä antaa tietoa tarkastelluista tietoturvamekanismeista.</p> <p>Työn tulokset olivat mielestäni erittäin hyvät. Tutkituista tietoturvamekanismeista ainoastaan yksi jäi ottamatta käyttöön johtuen yhteensopivuusongelmasta, mutta tästäkin saatiin tärkeää tietoa mahdollista myöhemmin tehtävää käyttöönottoa ajatellen.</p>	
Avainsanat	LAN, DHCP, VLAN, Juniper, verkon tietoturva

Author Title	Eemi Oksanen Securing Switched Local Area Network Using Existing Technologies
Number of Pages Date	38 pages June 1, 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	Communication Networks and Applications
Instructors	Matti Puska, Principal Lecturer Marko Uusitalo, Senior Lecturer
<p>This thesis discusses about a big multinational audit company's internal network security enhancement project using network equipment security mechanisms. The goal was to become familiar with those mechanisms, test their functionality and verify that they are suitable for this specific network. At the end, a decision about deployment was made.</p> <p>The company's LAN is based on network devices manufactured by Junipers. The used devices offer enough capacity in the future, even if company's employee number increases significantly.</p> <p>Due to the deployment of security features LAN security was clearly enhanced against most common attacks. All features were not fully deployed but for the future the IT-department has now quite much useful information and those features can be easily tested later and then consider deployment again.</p> <p>This thesis intends to give information about examined security features and tell about commonly used methods about companies Local Area Networks.</p> <p>In my opinion results of this thesis was great. All inspected security features were implemented except one because of compatibility problems. Related to this security feature we got lots of important knowledge for possible later implementation.</p>	
Keywords	LAN, DHCP, VLAN, Juniper, network security

# Sisällys

## Lyhenteet

1	Johdanto	1
2	Teoria ja haavoittuvuuksia	2
2.1	DNS-nimiselvitys	2
2.2	DNS-järjestelmän tietoturvasta	4
2.3	ARP-osoitteenselvitysprotokolla	5
2.4	ARP-järjestelmän haavoittuvuus	9
2.5	DHCP-osoitejakelu	9
2.5.1	DHCP:n toiminnan perustietoa	9
2.5.2	Omassa ympäristössä toteuttamani DHCP-testi	11
2.6	DHCP:n haavoittuvuuksia	12
2.6.1	DHCP Starvation eli DHCP-palvelimen tukahdutus	12
2.6.2	Rogue DHCP Server eli vihamielinen DHCP-palvelin	12
2.7	VLAN eli Virtual Local Area Network	13
	IEEE 802.1Q ja tagit	13
	Natiivi VLAN (Native VLAN)	14
	Oletus VLAN (Default VLAN)	14
	VLAN-runkoyhteys	14
	Access-portit	14
2.8	VLANien käyttöön liittyvät yleisimmät uhat	15
	Switch spoofing eli kytkimeksi tekeytyminen	15
	Double tagging tai VLAN Hopping eli tuplatagaus tai VLAN hyppyys	15
2.9	Spanning Tree -protokolla	16
2.9.1	Spanning Tree -protokollan toiminta	17
2.9.2	Rapid Spanning Tree -protokolla lyhyesti	17
2.10	Spanning Tree -protokollan haavoittuvuus	18
2.10.1	Root Protection eli Juurivahti	18
2.10.2	Loop Protection eli Silmukkavahti	19
2.10.3	Unidirectional Link Detection (UDLD) eli yksisuuntaisen linkin tunnistus	20
2.11	Virtual Chassis eli virtuaalinen alusta	20
2.12	802.1X-standardi eli porttikohtainen todentaminen	21

2.12.1	Single supplicant mode	23
2.12.2	Single-secure supplicant mode	23
2.12.3	Multiple supplicant mode	24
3	Ympäristön kuvaus	24
3.1	Core-kytkin	24
3.2	Kerroskytkimet	25
3.3	VLAN -verkkosegmentit	25
3.4	Palvelimet	26
3.5	Verkkoyhteydet	26
	Kuvaus lyhyesti	26
	Liikenteen priorisointi	27
4	Tutkimukset	27
4.1	DHCP Snooping	28
4.2	Dynamic ARP Inspection (DAI)	28
4.3	IP Source Guard	29
4.4	Porttikohtainen todentaminen 802.1X	29
4.5	VLAN-liikenteen suodatus	30
4.6	Tietoturvamekanismien testaamiseen käyttämäni työkalut	30
4.6.1	Kali Linux	30
4.6.2	Ettercap	30
4.6.3	Macof	32
4.6.4	Vihamielinen DHCP-palvelin	33
5	Konkreettiset toimenpiteet	33
6	Yhteenveto	34
	Lähteet	36

## Lyhenteet

ARP	Address Resolution Protocol on protokolla, jota käytetään Ethernet-verkoissa ja sen avulla selvitetään IP-osoitetta vastaava MAC-osoite.
BPDU	Bridge Protocol Data Unit on Ethernet-kehys, joka sisältää Spanning Tree -protokollaan liittyvää tietoa, kuten kuittauksen muuttumattomasta verkon tilasta tai tiedon muuttuneesta verkon tilasta.
DHCP	Dynamic Host Configuration Protocol on tekniikka, jonka avulla Ethernet-verkkoon liitetyille laitteille saadaan jaettua IP-osoitteita.
DNS	Domain Name System on järjestelmä, joka muuntaa sanamuotoiset verkotunnukset numeerisiksi IP-osoitteiksi.
IP-osoite	Internet Protocol -osoite, eli Internetin protokollaosoite, jota käytetään IP-verkkoihin kytkettyjen verkkosovittimien yksilöimiseen.
MAC-osoite	Media Access Control -osoite on osoite, joka yksilöi Ethernet-verkkosovittimen.
MPLS	Multiprotocol Label Switching on menetelmä, joka perustuu siihen, että verkkoliikenteen paketit merkitään ja merkinnän perusteella paketti kulkee ennalta määrättyä reittiä pitkin kohteeseen. Näin vältetään aikaa vievät haut reititystauluun.
RARP	Reverse Address Resolution Protocol on protokolla, jota käytetään Ethernet-verkoissa ja sen avulla selvitetään MAC-osoitetta vastaava IP-osoite.
RFC	Lyhenne tulee sanoista Request for Comments ja dokumentit ovat Internetiä koskevia standardeja, jotka on julkaissut IETF (Internet Engineering Task Force).

RSTP	Rapid Spanning Tree Protocol ajaa pohjimmiltaan saman asian kuin STP, mutta vikatilanteissa tämä uudempi protokolla kykenee vaihtamaan liikennöimiseen käytettävää linkkiä parhaimmillaan vain millisekunneissa.
STP	Spanning Tree Protocol on verkkoprotokolla, jonka tehtävä on estää silmu- koiden syntymistä.
UPS	Uninterruptible Power Supply tarkoittaa suomeksi keskeytymätöntä virran- syöttöä. Kyseessä on siis varavirtajärjestelmä sähkökatkon varalle.
Virtual Chassis	Verkkolaittevalmistaja Juniperin käyttämä nimitys tekniikalle, jonka avulla useampi kytkin voidaan liittää yhteen ja konfiguroida käyttä- tymään yhtenä isona kytkimenä.
VLAN	Virtual Local Area Network on virtuaalinen LAN-segmentti.
VPN	Virtual Private Network eli virtuaalinen erillisverkko on menetelmä, jolla yk- sittäisiä työasemia tai kokonaisia verkkoja saadaan yhdistettyä ja näin muodostettua näennäisesti yksityinen verkko.

## 1 Johdanto

Opinnäytetyö tehtiin monikansalliselle tilintarkastusyriykselle, jonka Suomen pääkonttori sijaitsee Helsingissä. Yrityksellä on Suomessa yli 1100 henkilöä, joista Helsingin toimistolla työskentelee noin 800 henkilöä. Yli 300 työntekijää työskentelee maakunnissa sijaitsevilla pienemmissä toimipisteissä, joiden työntekijämäärä vaihtelee vain yhdestä aina lähes sataan saakka. Jokaisella työntekijällä on käytössään vähintään oma kannettava tietokone, mutta joillakin on lisäksi käytössään myös asiakkaiden tietokoneita. Näillä koneilla on tarvittavat sertifikaatit ja VPN (Virtual Private Network) -ohjelmistot asennettuina asiakkaan sisäverkkoon pääsemiseksi, mutta oman yrityksemme sisäverkkoon vaadittavia sertifikaatteja niissä ei ole.

Pääkonttori muutti keväällä 2014 valmistuneisiin täysin uusiin toimitiloihin, jonne päätettiin hankkia verkkolaittevalmistaja Juniperin verkkolaitteet. Tästä syystä opinnäytetyö on kirjoitettu Juniperin laitteiden näkökulmasta, mutta tutkitut turvamekanismit ovat niin perustavanlaatuisia, että ne löytyvät muidenkin verkkolaittevalmistajien tuotteista.

Opinnäytetyön tavoitteena on kartoittaa ja parantaa Helsingin toimiston sisäverkon tietoturvaa. Tästä syystä aloin tutkia ja hankkia ymmärrystä joidenkin verkkokytinten tietoturvamekanismien toiminnasta ja selvittää, mikä tai mitkä niistä olisi syytä ottaa käyttöön Suomen pääkonttorissa. Epäilemättä tuloksia ja havaintoja tullaan käyttämään hyödyksi ja soveltamaan myös muissa toimipisteissä, joissa on siihen mahdollisuus käytettävän laitteiston puolesta.

Toimistossa on myös paljon asiakaskäyttöön tarkoitettuja neuvotteluhuoneita, joissa on tarjolla kiinteä verkkojohto asiakkaiden käyttöön. Tämä on ollut yksi asia, joka on ollut motivaattorina turvallisemman sisäverkon kehittämiseksi. Pelkona ei niinkään ole se, että asiakasorganisaation tai yhteistyökumppanin edustaja haluaisi murtautua verkkoon, vaan se, että kenellä tahansa voi olla jokin haittaohjelma koneellaan josta käyttäjä itse ei edes ole tietoinen.

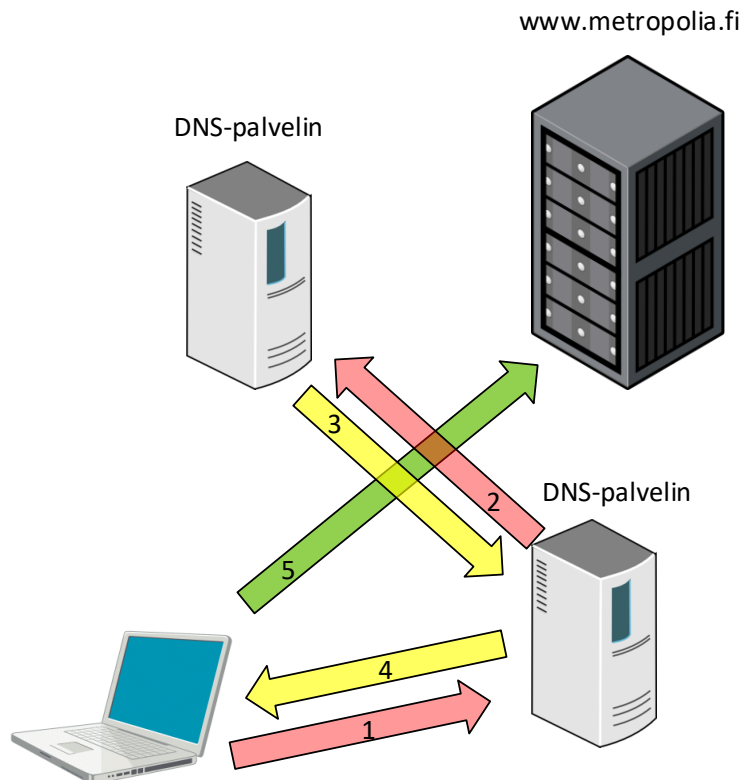


## 2 Teoria ja haavoittuvuuksia

### 2.1 DNS-nimiselvitys

Domain Name System (DNS) on järjestelmä, joka muuntaa sanamuotoiset verkko-osoitteet numeerisiksi Internet Protocol -osoitteiksi. Tätä tarvitaan, sillä ihmiset muistavat helpommin sanamuotoisen verkko-osoitteen kuin laitteiden käyttämän numeromuotoisen IP-osoitteen. Esimerkiksi `www.metropolia.fi`-verkko-osoitetta vastaava IP-osoite on `195.148.144.10`.

DNS-järjestelmä toimii siten, että internetiin liitetty laite, esimerkiksi tietokone, tallentaa omaan DNS-välimuistiinsa sanamuotoiset verkko-osoitteet sekä niitä vastaavat numeeriset IP-osoitteet. Mikäli laitteen DNS-tietokannassa ei vielä ole verkko-osoitetta vastaavaa IP-osoitetta, niin se täytyy ensin kysyä määritellyltä DNS-palvelimelta. Ilman IP-osoitetta laite ei tiedä, minne paketteja pitää lähettää. Saatuaan DNS-palvelimelta IP-osoitteen, voi laite alkaa lähettämään liikennettä halutulle palvelimelle. Tämä DNS-järjestelmän toimintamalli on virallisesti esitetty dokumenteissa RFC 882 ja RFC 883 jo lokakuussa 1983. [1.]



1. Päälaite ei tiedä kohteen [www.metropolia.fi](http://www.metropolia.fi) IP-osoitetta, joten se kysyy sitä DNS-palvelimelta.
2. Ensimmäisellä DNS-palvelimella ei ole kyseistä tietoa tietokannassaan tai väli-muistissaan, joten se kysyy toiselta DNS-palvelimelta.
3. Tieto löytyi toiselta DNS-palvelimelta ja se vastaa takaisin, että [www.metropolia.fi](http://www.metropolia.fi) löytyy IP-osoitteesta 195.148.144.10.
4. Ensimmäinen DNS-palvelin välittää tiedon päätelaitteelle.
5. Päälaite ottaa yhteyden samaansa IP-osoitteeseen.

Microsoft Windows -työaseman komentoriviltä komennolla **ipconfig /all** saa näky-viin paljon olennaista tietoa, kuten esimerkiksi käytettävän DNS-palvelimen. IP-osoit-teessa 8.8.8.8 on Googlen ylläpitämä julkinen nimipalvelin.

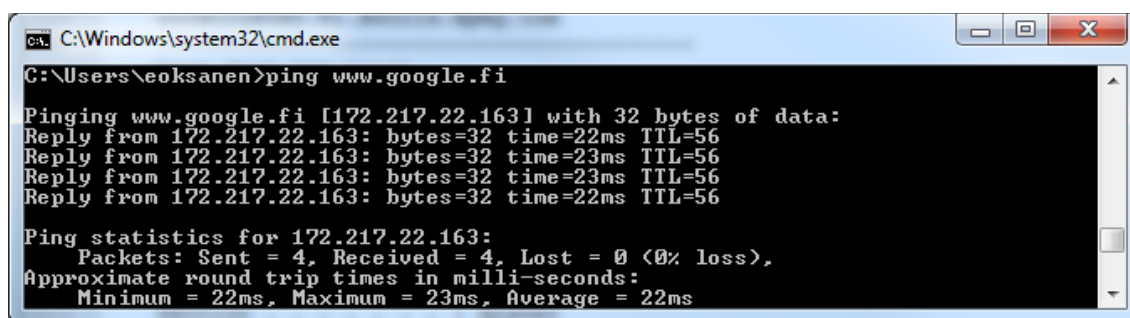
```

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : Kotiverkko
    Description . . . . . : Intel(R) Ethernet Connection I218-LM
    Physical Address. . . . . : EC-F4-BB-3F-21-BF
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.20(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 7. toukokuuta 2017 3:26:57
    Lease Expires . . . . . : 7. toukokuuta 2017 7:26:57
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled

```

Kuva 1. Ethernet-verkkosovittimen tiedoissa näkyy esimerkiksi käytettävä DNS-palvelin.



```

C:\Windows\system32\cmd.exe

G:\Users\eoksanen>ping www.google.fi

Pinging www.google.fi [172.217.22.163] with 32 bytes of data:
Reply from 172.217.22.163: bytes=32 time=22ms TTL=56
Reply from 172.217.22.163: bytes=32 time=23ms TTL=56
Reply from 172.217.22.163: bytes=32 time=23ms TTL=56
Reply from 172.217.22.163: bytes=32 time=22ms TTL=56

Ping statistics for 172.217.22.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms

```

Kuva 2. Komentoriviltä suoritettu ping-komento paljastaa tekstimuotoisen osoitteen taustalla olevan numeromuotoisen IP-osoitteen.

## 2.2 DNS-järjestelmän tietoturvasta

Kuten edellisessä luvussa kerroin, niin DNS-järjestelmä perustuu DNS-palvelimiin, jotka tarvittaessa kertovat sanamuotoista verkko-osoitetta vastaavan IP-osoitteen, jonne IP-paketteja tulisi lähettää. Tässä piilee kuitenkin eräs vaara, jota verkkorikolliset ovat jo onnistuneet käyttämään hyväkseen.

Verkkorikolliset pyrkivät tartuttamaan päätelaitteelle tai suoraan internet-modeemiin haittaohjelman, joka vaihtaa käytössä olevan DNS-palvelimen tilalle rikollisten hallinnassa olevan DNS-palvelimen. Rikollisten hallitsema DNS-palvelin toimii samalla tavalla kuin turvallisten tahojen hallinnoimat palvelimet, mutta sen palauttavat IP-osoitteet saattavat ohjata rikollisten ylläpitämille internetsivuille. Rikollisten ylläpitämiltä sivuilta päätelaitteelle voi tarttua haittaohjelmia tai viruksia, joilla useimmiten tavoitellaan taloudellista hyötyä. [2.]

Eräs tunnettu huijauskeino on ohjata käyttäjä väärässä IP-osoitteessa oleville aidonnäköisille verkkopankkisivuille. Tässä tapauksessa voidaan olettaa verkkopankkitunnusten päätyvän rikollisten haltuun. Mahdollista on myös se, että rikolliset toteuttavat reaaliaikaisen välimieshyökkäyksen, jolloin uhri luulee kirjautuvansa normaalisti omalle verkkopankkitililleen, mutta todellisuudessa rikolliset kirjautuvatkin uhrin tilille uhrin kuvitellessa kaiken olevan normaalisti. Uhrilla ei ole enää tässä vaiheessa hallintaa mihinkään, ja rikolliset voivat siirtää rahaa uhrin tililtä omille tileilleen. [2.]

### 2.3 ARP-osoitteenselvitysprotokolla

Address Resolution Protocol on protokolla, jolla selvitetään Ethernet-verkoissa laitteiden käyttämää IP-osoitetta vastaava Media Access Control -osoite. IP-osoitteesta käytetään monesti tässä yhteydessä nimitystä verkko-osoite ja MAC-osoitteesta nimitystä fyysinen osoite.

IP-osoite on osoite, jota käyttäen paketteja voidaan välittää verkosta toiseen reitittimiä käyttämällä. IP-osoitetta ei voida käyttää liikennöimiseen lähiverkossa (Local Area Network, LAN). Eli ilman IP-osoitteita voisi olla vain lähiverkkoja, mutta lukemattomia eri verkkoja sisältävä internet ei olisi mahdollinen, koska mikään laite ei pystyisi pitämään kirjaa kaikkien muiden verkkoon liitettyjen laitteiden MAC-osoitteista. Lähiverkoissa liikennöinti tapahtuu siis laitteiden fyysisten osoitteiden perusteella. [3.]

ARP-taulun roolina on tallentaa IP-osoitteet ja niitä vastaavat fyysiset osoitteet. Tyypillisesti päätelaite käyttää ARPia selvittääkseen jonkin toisen päätelaitteen fyysisen osoitteen.

Komento `ipconfig /all` antaa seuraavat tiedot ja kuvasta nähdään koneen omat MAC- ja IP-osoitteet seuraavasti:

```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Kotiverkko
    Description . . . . . : Intel(R) Ethernet Connection (4) I219-LM
    Physical Address. . . . . : D4-81-D7-BE-B9-70
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::158a:46c3:9d30:efe2%10(Preferred)
    IPv4 Address. . . . . : 192.168.1.2(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : sunnuntai 21. tammikuuta 2018 1.14.56
    Lease Expires . . . . . : sunnuntai 21. tammikuuta 2018 4.14.55
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 64258519
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-1F-6C-7D-D4-81-D7-BE-B9-70
    DNS Servers . . . . . : 8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled

```

Kuva 3. Listauksesta nähdään kyseisen verkkosovittimen olennaisia tietoja.

Komento **arp -a -n** antaa seuraavat tiedot:

```

C:\Users\eoksanen>arp -a -n 192.168.1.2

Interface: 192.168.1.2 --- 0xa
    Internet Address      Physical Address      Type
    192.168.1.1           00-1c-58-fc-0d-e6    dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

```

Kuva 4. Kuvasta nähdään, että IP-osoitetta 192.168.1.2 käyttävä verkkosovitin on tallentanut ARP-tauluunsa IP-osoitetta 192.168.1.1 vastaavan MAC-osoitteen, joka on Default Gateway, eli palomuurin sisäverkkoon päin oleva verkkosovitin.

Cisco ASA 5505 -palomuurin ARP-taulu:

```

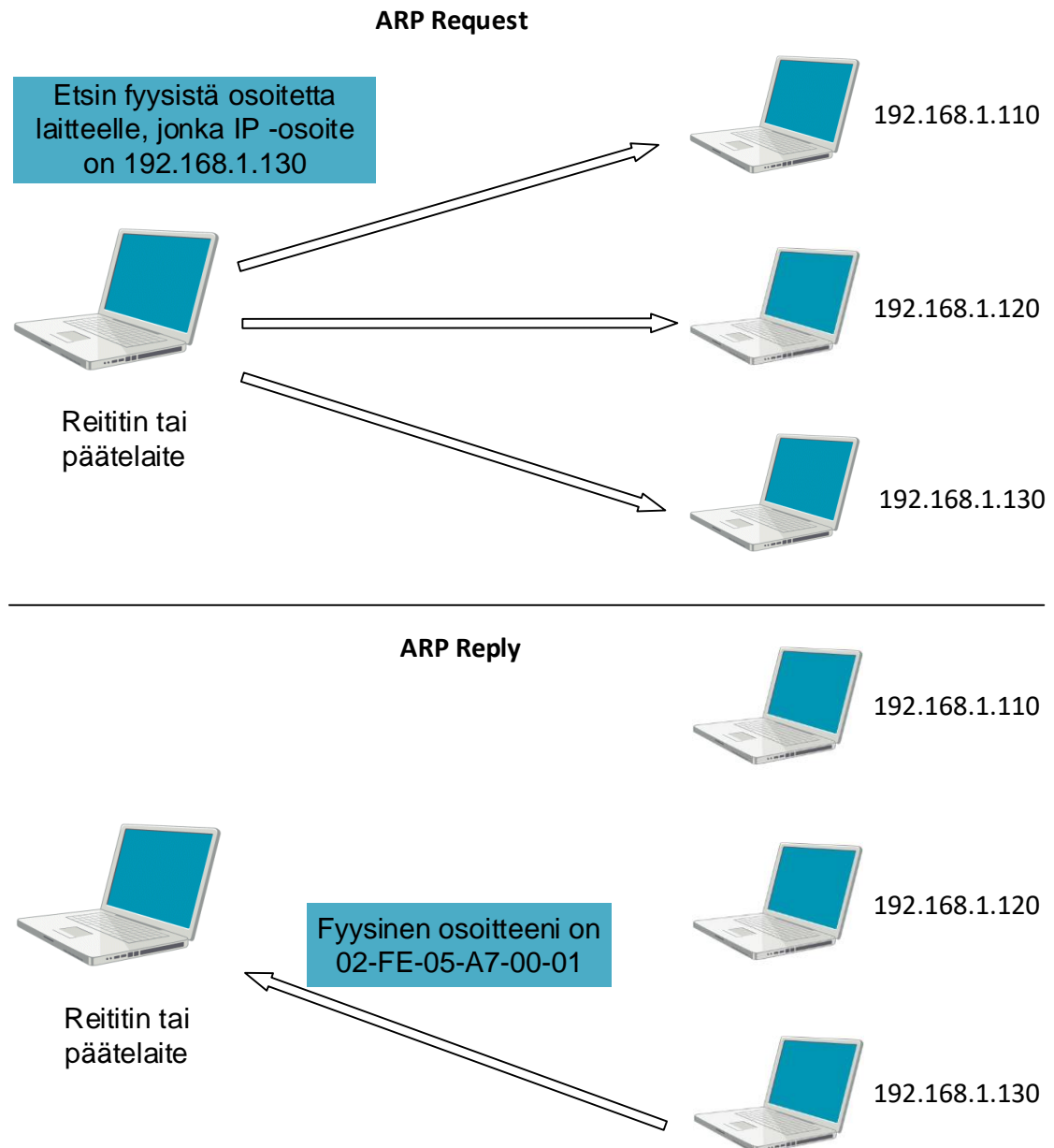
MUURI# show arp
    inside 192.168.1.2 d481.d7be.b970 45
    outside 192.168.0.254 001e.ab02.588f 39

```

Kuva 5. Kuvasta nähdään, että palomuurin ARP-tauluun on tallentunut tieto sisäverkossa olevaa IP-osoitetta 192.168.1.2 vastaavasta MAC-osoitteesta.

Näistä kuvista voidaan todeta, että tietokone on tallentanut palomuurin verkko-osoitetta 192.168.1.1 vastaavan fyysisen osoitteen 00-1c-58-fc-0d-e6 ja palomuuuri on tallentanut tietokoneen verkko-osoitetta 192.168.1.2 vastaavan fyysisen osoitteen d4-81-d7-be-b9-70.

Palomuuuri toimii myös DHCP (Dynamic Host Configuration Protocol) -palvelimena, ja se on asetettu jakamaan sisäverkon laitteille IP-osoitteita väliltä 192.168.1.2 - 192.168.1.100. Palomuuuri on siis itse alun perin antanut tietokoneelle IP-osoitteen ja tallentanut samassa yhteydessä tietokoneen fyysisen osoitteen muistiinsa.



Kuva 6. Ylemmässä osassa havainnollistus siitä, miten pyyntö IP-osoitetta vastaavalle fyysiselle osoitteelle tavoittaa kaikki verkossa olevat laitteet. Alemmassa osassa IP-osoitteen omaava laite vastaa kysyjälle ja kertoo fyysisen osoitteensa, jonka kysyjä tallentaa omaan ARP-tauluunsa.

ARP on kuvattu dokumentissa RFC 826.

## 2.4 ARP-järjestelmän haavoittuvuus

ARP-järjestelmän vaarana on, että vihamielinen taho yrittää syöttää L3-tason kytkimen tauluun väärää tietoa, ja yrittää näin saada uhrien liikenteen ohjattua itselleen. Hyökkäys perustuu siihen, että hyökkääjä lähettää verkkoon väärennetyjä ARP-vastauksia. Väärennetyillä ARP-vastauksilla hyökkääjä pyrkii yhdistämään oman MAC-osoitteensa jonkin jo tiedossa olevan IP-osoitteen kanssa, esimerkiksi oletusyhdyskäytävän, jolloin kaikki ulkoverkkoon tarkoitettu liikenne lähetetäänkin hyökkääjälle. Tällöin hyökkääjä pääsee käsiksi kaikkeen muihin IP-verkkoihin tarkoitettuun liikenteeseen ja voi suorittaa niin kutsutun välimieshyökkäyksen. [4.]

Edistyneempi tapa ARP-väärennöksen tekemiseen on valvoa verkkoa ja odottaa ARP-kyselyitä. Tällöin hyökkääjä lähettää ARP-vastauksen, joka sisältää halutun MAC-osoitteen. ARP-kyselyn lähettänyt laite saa vastauksen ainakin IP-osoitteen oikeasti omistavalta laitteelta sekä väärennetyn ARP-vastauksen lähettäjältä. Vastaanottava laite tallentaa joko ensimmäisen tai viimeisimmän ARP-vastauksen sisältämän MAC-osoitteen riippuen asetuksista. [4.]

Väärennetyillä ARP-vastauksilla on mahdollista aiheuttaa merkittävää haittaa myös ilman salakuuntelua. Mikäli verkossa oleva laite tallentaa keksittyjä tai ristiriitaisia MAC-osoitteita ARP-tauluunsa käytössä olevien IP-osoitteiden kohdalle, niin tällöin kyseisiin IP-osoitteisiin liikennöinti epäonnistuu.

## 2.5 DHCP-osoitejakelu

### 2.5.1 DHCP:n toiminnan perustietoa

Verkkoon liitetty laite lähettää oletuksena automaattisesti levitysviestejä, joihin se toivoo saavansa vastauksen DHCP-palvelimelta. Vastauksessa DHCP-palvelin tarjoaa vapaana olevaa IP-osoitetta määritellyltä osoitealueelta ja ilmoittaa käytettäväksi muita tietoja ja asetuksia. Muita tietoja ja asetuksia ovat esimerkiksi IP-osoitteen laina-ajan pituus, oletusyhdyskäytävän IP-osoite verkosta ulospäin lähetettävälle liikenteelle ja DNS-palvelimen tai -palvelinten IP-osoitteet. Verkkoon liitetty laite pyytää käyttöönsä tarjottua

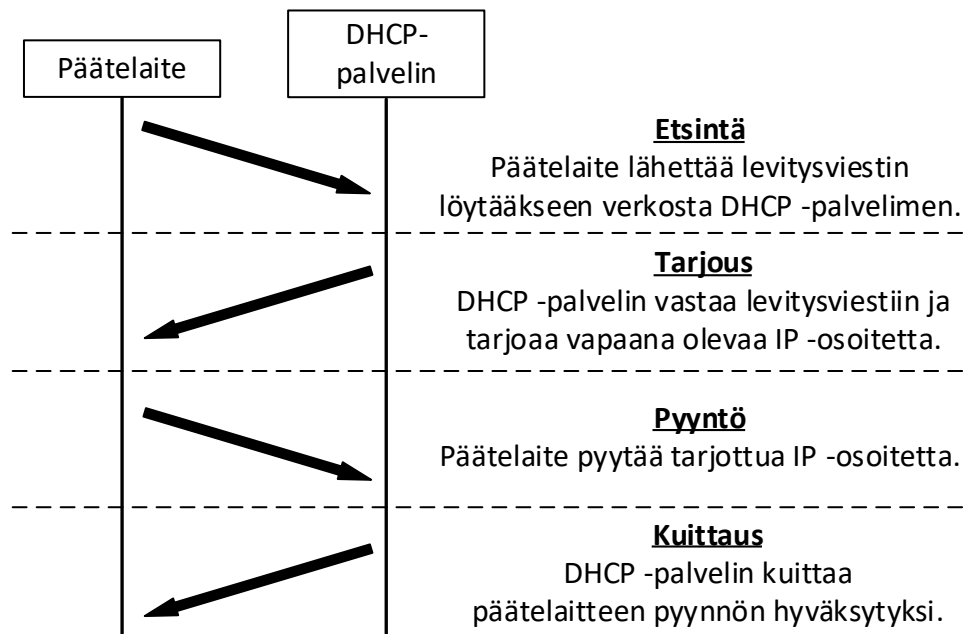


osoitetta. Tämän jälkeen DHCP-palvelin kuittaa hyväksyvänsä pyynnön. Laite ottaa annetun IP-osoitteen käyttöön automaattisesti ja DHCP-palvelin tallentaa tiedon laitteelle annetusta IP-osoitteesta omaan lainatauluunsa (lease table). [5.]

IP-osoitteen laina-ajan pituus riippuu erittäin paljon vallitsevasta ympäristöstä. Ympäristöön, jossa vietetään vähän aikaa ja laitteita on päivän mittaan paljon, on syytä määritellä DHCP-palvelimen käyttöön isompi osoitealue ja lyhyempi laina-aika. Esimerkiksi suosittu kahvilan WLAN-verkkoon voi liittyä päivän mittaan useita satoja laitteita, joten osoitealueen tulisi olla esimerkiksi noin 500 osoitetta ja laina-ajan yhdestä kahteen tuntia. Kotiverkossa sijaitsevan DHCP-palvelimen osoitealueen riittävä koko voisi olla esimerkiksi vain 10 osoitetta, mutta käytännössä liian suuresta osoitealueesta ei ole haittaa. Laina-aika puolestaan voi olla viikkoja tai jopa kuukausia.

Laina-aika ja osoitealueen koko tulisi siis määrittää siten, että osoitealueen osoitteet eivät lopu kesken, koska niiden loppuessa uudet verkkoon liittyvät laitteet jäävät ilman IP-osoitetta, eivätkä tällöin pääse liikennöimään verkossa. Toisaalta taas laina-ajan ollessa liian lyhyt yhteydessä saattaa esiintyä pätkimistä.

Huomion arvoista on kuitenkin se, että DHCP-palvelimelta IP-osoitteen saaneet laitteet yrittävät uusia lainaansa siinä vaiheessa, kun laina-ajasta on kulunut puolet. Mikäli uusimisyritys ei onnistu, niin laite alkaa etsiä verkosta DHCP-palvelinta lähettämällä levitysviestinä DHCPDISCOVER-paketin siinä vaiheessa, kun laina-ajasta on kulunut 87,5 %. Levitysviesti on sama, jonka laite lähettää liitettäessä verkkoon. Tässä vaiheessa laite hyväksyy minkä tahansa verkossa olevan DHCP-palvelimen tarjoaman minkä tahansa IP-osoitteen. [6.]



Kuva 7. Havainnollistava kuva verkkoon liitetyn päätelaitteen ja DHCP-palvelimen kättelyn vaiheista.

DHCP on kuvattu dokumentissa RFC 2131.

### 2.5.2 Omassa ympäristössä toteuttamani DHCP-testi

Kokeilin omassa kotiverkossani asettaa laina-ajan niin pieneksi kuin Cisco ASA 5505 -palomuuuri sen sallii, eli 300 sekunnin mittaiseksi. Asetin päälle jatkuvan pingin Googlen DNS-palvelimen julkiseen IP-osoitteeseen 8.8.8.8 samanaikaisesti kolmella tietokoneella. Havaitsin, että säännönmukaisesti noin kolme sekuntia ennen laina-ajan umpeutumista vastausajan saaminen Googlen DNS-palvelimelta piteni normaalista 20-22 millisekunnista 28-30 millisekuntiin yksittäisen vastauksen osalta ja tämän jälkeen palautui normaaliksi. Pakettien putoamista tai yhteyden katkeamista en havainnut. Käytin tässä kokeessa kahta Windows 7 -työasemaa ja yhtä Windows 10 -työasemaa. Tietenkään koe ei ole absoluuttisen tarkka, koska työasemissa oli sovelluksia auki, eikä niitä ollut optimoitu kyseisiin kokeisiin, mutta mielestäni koe oli erittäin hyvin suuntaa-antava.

Cisco ASA 5505 -palomuurin DHCP-palvelimen oletuslaina-aika on vain 3600 sekuntia, eli yksi tunti. Pisin mahdollinen laina-aika kyseisessä laitemallissa ja käytössä olleella

käyttöjärjestelmäversiolla on 1048575 sekuntia, eli hieman yli 12 vuorokautta. Asetin kokeen jälkeen laina-ajaksi 864000 sekuntia, eli tasan 10 vuorokautta.

## 2.6 DHCP:n haavoittuvuuksia

### 2.6.1 DHCP Starvation eli DHCP-palvelimen tukahdutus

Tässä hyökkäyksessä tavoite on saada DHCP-palvelin lamaantumaan lähettämällä verkkoon DHCP-pyyntöjä (request) väärennetyillä MAC-osoitteilla. Tavoite on lähettää pyyntöjä niin paljon, että DHCP-palvelimen osoitemuisti täyttyy eikä se enää kykene reagoimaan oikeisiin pyyntöihin. Lamaantumisen pituus riippuu käytettävästä DHCP-palvelimen konfiguraatiosta. Tällöin hyökkäävä taho voi käyttää omaa vihamielistä (rogue) DHCP-palvelintaan ja vastata tuleviin DHCP-pyyntöihin. [7.]

### 2.6.2 Rogue DHCP Server eli vihamielinen DHCP-palvelin

Vihamielinen DHCP-palvelin on joko pahantahtoisen hyökkääjän tai tietämättömän käyttäjän verkkoon kytkemä DHCP-palvelin, joka ei ole verkon ylläpitäjien hallinnassa. Vahingossa verkkoon liitetty laite on tavallisesti pieni kytkin tai langaton reititin, jossa on DHCP-palvelin päällä.

Pahantahtoiset hyökkääjät puolestaan pyrkivät omalla DHCP-palvelimellaan tarjoamaan verkkoon liittyville laitteille väärää tietoa, kuten esimerkiksi heidän omassa hallinnassa olevaan laitteeseen osoittavan oletusyhdykäytävän IP-osoitteen tai DNS-palvelimen IP-osoitteen. Tällöin väärää tietoa käyttävä laite lähettää kaiken liikenteen hyökkääjille, jotka voivat halutessaan suorittaa esimerkiksi välimieshyökkäyksen. [7.]

Vaikka vihamielisen DHCP-palvelimen avulla hyökkäävä taho todennäköisesti pyrkiikin suorittamaan välimieshyökkäyksen, on silti syytä muistaa, että virheelliset tiedot uhrikoneella voivat aiheuttaa suuria ongelmia. Uhrikone ei välttämättä pääse liikennöimään verkossa ollenkaan, tai liikennöinti saattaa olla hidasta ja epäluotettavaa. Tällöin kyseessä on jonkinasteinen palvelunestohyökkäys.

DHCP snooping on juuri tätä tarkoitusta varten kehitetty kytkimissä oleva turvamekanismi. DHCP snooping on tarkemmin selitetty luvussa 4.1.

## 2.7 VLAN eli Virtual Local Area Network

Virtual Local Area Network on virtuaalinen LAN-segmentti. Tämä tarkoittaa sitä, että eri VLANeja ajetaan saman verkkoinfrastruktuurin päällä ja ne on myös usein erotettu toisistaan omiksi IP-avaruuksiksi. VLANien avulla on myös mahdollista luoda looginen lähiverkko siten, että eri IP-avaruuksissa olevat laitteet ovat yhteydessä toisiinsa. Haluttaessa VLANien liikennettä voidaan reitittää toistensa välillä tai olla reitittämättä. Esimerkiksi palvelinten tai muiden tärkeiden tai kriittisten laitteiden verkkosegmentti olisi syytä pitää erillään normaalista käyttäjäverkosta.

VLANeja käyttämällä saadaan siis lähiverkon tietoturvaa nostettua, koska esimerkiksi tavalliseen työasemaan tarttunut virus ei pääse leviämään suoraan verkossa palvelinten verkkosegmenttiin.

VLANit helpottavat myös hallinnointia, koska omien segmenttien alle on helppoa ja kätevää niputtaa samankaltaisia laitteita. Esimerkiksi tämän opinnäytetyön kohteena olevassa yrityksessä koko toimiston kattava työntekijöiden tietokoneille tarkoitettu lähiverkko on jaettu rakennuksen kerroksien mukaan, jolloin muodostui sopivan kokoisia noin sadan tietokoneen verkkosegmenttejä. Vianetsintää varten tai tietoturvasyistä johdun näitä segmenttejä olisi helppo eristää tarkempia tutkimuksia varten. [8; 9.]

VLANien konsepti on esitelty RFC-dokumentissa 3069.

### IEEE 802.1Q ja tagit

IEEE 802.1Q on verkkostandardi, joka tukee VLANeja Ethernet-verkossa. Standardi määrittelee useampiakin asioita, mutta tämän työn kannalta oleellisin on Ethernet-pakettien merkitseminen eli tagaaminen. Tagaaminen toimii siten, että Ethernet-pakettiin lisätään yksi neljän tavun kokoinen kenttä, joka sisältää muiden tietojen ohella VLANin numeron, johon kyseinen paketti kuuluu.

### Natiivi VLAN (Native VLAN)

Juniperin termistössä natiivi VLAN tarkoittaa VLANia, johon kytkin olettaa tagaamattomien pakettien kuuluvan ja välittää ne eteenpäin. Paketteja ei tagata eteenpäin välitettäessä. Juniperin kytkimissä ei ole oletuksena natiivi VLANia, kuten Ciscon kytkimissä. Mikäli natiivi VLAN on määrittelemättä, niin tällöin paketit pudotetaan.

### Oletus VLAN (Default VLAN)

Juniperin kytkimissä ei ole samaan tapaan default VLANia, kuten Ciscon kytkimissä. Ciscon kytkimissä default VLAN on oletuksena VLAN 1, joten paketit tagataan siihen kuuluviksi. Juniperin kytkimissä puolestaan default VLAN on sinänsä olemassa, mutta se ei oikeasti kuulu mihinkään VLANiin, eikä siihen tulevaa liikennettä tagata. Tämä voi-kin olla toivottu tilanne pienissä verkoissa, mutta isommissa verkoissa porttiin tuleva liikenne määritetään haluttuun VLANiin.

### VLAN-runkoyhteys

VLAN-runkoyhteys muodostetaan käyttämällä runkoportteja (trunk port). Runkoportit ovat portteja, joiden kautta voi kulkea useamman VLANin liikenne. Käytännössä siis kytkinten väliset portit on asetettava runkotilaan, mikäli halutaan VLAN-liikenteen kulkevan. Mikäli runkoporttiin tulee ilman VLAN-tagia oleva paketti, niin se ohjataan natiivi-VLANiin.

### Access-portit

Access- eli pääsyportit ovat portteja, jotka sallivat kytketyn laitteen liikennöidä vain tiettyyn ennalta määritettyyn VLANiin. Mikäli VLANia ei ole erikseen määritelty pääsyportille, niin liikenne ohjataan oletus-VLANiin, joka on yleensä VLAN1.

## 2.8 VLANien käyttöön liittyvät yleisimmät uhat

VLANien käyttäminen on yleistä ja käytöllä saavutetaan selkeitä etuja niin verkon ylläpidon kuin tietoturvan kannalta. Kuitenkin tietyt tiedetyt hyökkäystavat on syytä ottaa huomioon.

### Switch spoofing eli kytkimeksi tekeytyminen

Tämä hyökkäys perustuu siihen, että hyökkäystä suorittava päätelaite matkii toisen kytkimen runkoporttia käyttämällä lähettämissään paketeissa tagaus- ja trunkkaus-protokollia. Mikäli kytkimestä ei ole asetettu porttia oikeaan toimintamoodiin, niin kytkin alkaa välittää useamman VLANin liikennettä hyökkääjälle. Tästä syystä ylimääräisistä vapaista kytkinporteista tulisi asettaa automaattinen trunkkiprotokollan käyttöönotto pois päältä tai konfiguroida portit vain pääsymoodiin (access mode). Pääsymoodissa portin on sallittua liikennöidä vain yhdessä VLANissa. [10.]

Tämä hyökkäys tosin on mahdollinen vain Ciscon valmistamissa verkkolaitteissa, joissa on otettu käyttöön Ciscon omistama Dynamic Trunking Protocol. Kyseistä protokollaa käyttävät portit pyrkivät automaattisesti määrittämään itsensä joko pääsy- tai trunkkitilaan.

### Double tagging tai VLAN Hopping eli tuplatagaus tai VLAN hypytys

Tuplatagaushyökkäyksessä hyökkäystä suorittava päätelaite lisää lähetettämiinsä paketteihin kaksi VLAN-tagia. Ensimmäinen tagi täsmää siihen VLANiin, johon hyökkääjä kuuluu ja on oikeutettu liikennöimään. Toinen tagi puolestaan on haluttu VLAN, jossa hyökkäyksen kohde sijaitsee.

Hyökkäys pohjimmiltaan rakentuu siten, että ensimmäinen tagi täsmää natiivi VLANiin ja tällöin kytkin poistaa tagin välittäessään paketin eteenpäin. Seuraava kytkin näkee toisen tekaistun tagin, ja tämän seurauksena paketti siirtyy kulkemaan tekaistun tagin osoittamaan VLANiin ja lopulta kohteeseen ohittaen normaalit VLANeja eristävät mekanismit. Tällä hyökkäyksellä tosin on mahdollista vain lähettää paketteja kohteeseen, mutta vastaukset eivät koskaan päädy hyökkääjälle juurikin VLANien käytöstä johtuen. [11.]

Tältä hyökkäykseltä on kuitenkin varsin helppo suojautua esimerkiksi asettamalla kytkinporttien VLANiksi jokin muu kuin oletus-VLAN. Tämä vaikeuttaa hyökkääjän toimia, mikäli tiedossa ei ole käytettävä VLAN, johon hyökkäystä suorittava päätelaite kuuluu. Toinen tapa on määrittää kaikkien runkoporttien natiivi VLANiksi jokin käyttämätön VLAN, jolloin kaikissa runkoporttiin tulevissa paketeissa on oltava jokin tagi.

Kolmas tapa on konfiguroida kytkimestä päälle vaatimus, että myös natiivi VLANiin kuuluvat paketit ovat tagattava. Tagin puuttuessa paketti pudotetaan, eikä sitä välitetä eteenpäin.

Sopivalla ohjelmalla on mahdollista tuplatagata paketteja, jolloin saadaan liikennettä hyppimään VLANista toiseen. Esimerkiksi käyttäjä-VLANista palvelinten VLANiin. On kuitenkin syytä huomata, että palvelimet eivät pysty vastaamaan hyökkääjälle, koska ne eivät käytä tuplatagausta. Tällöin hyökkääjän tavoitteena on käytännössä häiritä verkkoa tai palvelimia, tai saada asennettua jokin haittaohjelma johonkin palvelinverkossa olevaan laitteeseen.

## 2.9 Spanning Tree -protokolla

Tämän protokollan avulla yhteyksiä voidaan kahdentaa ilman vaaraa L2-silmukoiden syntymisestä. Tällöin ensisijaisen yhteyden katketessa redundanttinen linkki tulee automaattisesti käyttöön. Spanning Tree -versioita on useita, mutta päätavoite kaikilla toteutuksilla on estää silmukoiden syntyminen sekä nostaa varalla olevat yhteydet käyttöön tarpeen niin vaatiessa.

Verkkosilmukat ovat ongelmallisia siksi, että ilman Spanning Treetä voi syntyä levitysviestimyrsky (Broadcast Storm). Levitysviesteille ei ole kytkimillä tiedossa tarkkaa kohdetta, joten ne lähetetään eteenpäin kaikista kytkimen porteista paitsi siitä, josta viesti on vastaanotettu. Tällöin kytkimet vain toistavat levitysviestejä toisilleen jatkuvasti ja verkko alkaa hidastua. Verkkoon liitetyt palvelut lakkaavat olemasta saatavilla myrskyn yltäessä riittävän voimakkaaksi, ja esimerkiksi loppukäyttäjän näkökulmasta verkko on tällöin täysin toimimaton. [12.]

Juniperin kytkimissä ajettava tavallinen STP reagoi verkon topologiamuutoksiin noin 50 sekunnissa, kun taas nopeampi RSTP (Rapid STP) kykenee reagoimaan ja konvergoitumaan jopa muutamassa sekunnissa. Topologiamuutoksia aiheuttaa esimerkiksi fyysisen linkin vikaantuminen tai uuden kytkimen lisääminen verkkoon.

Spanning tree on esitelty dokumentissa RFC 2674 vuonna 1999.

### 2.9.1 Spanning Tree -protokollan toiminta

Jokaisella kytkimellä on oma kahdeksan tavun mittainen siltatunniste (Bridge ID), joka koostuu kahdesta siltaprioriteettia (Bridge Priority) sisältävästä tavusta sekä kuudesta MAC-osoitteen sisältävästä tavusta. Siltaprioriteetti on erikseen konfiguroitavissa. Ennen kuin Spanning Tree päättää parhaan reitin juurisillalle (Root Bridge), niin sen on päätettävä kytkin, josta tulee juurisilta. Tämä rooli lankeaa kytkimelle, jolla on pienin siltatunniste. Juurisillan valitsemisen jälkeen muut verkon kytkimet valitsevat portin (Root port), joka on paras juurisillalle lähetettävää liikennettä ajatellen. Portin valintaprosessiin voidaan vaikuttaa, mutta mikäli kytkimissä on eri nopeuksilla toimivia portteja, niin yleensä on järkevintä valita nopein. Tämän jälkeen huomioidaan muut juurisillalle liikennettä lähettämään kykenevät portit ja asetetaan ne suljetuksi. Näin ensisijaisen yhteyden katketessa on jo valmiiksi tiedossa käyttöön otettava yhteys. [12.]

Protokollan toiminta perustuu siihen, että kytkimet lähettävät tietoa itsestään ja linkeistään toisilleen BPDU (Bridge Protocol Data Unit) -paketeilla. Tietojen perusteella protokolla päättää, mitkä linkit jätetään aktiivisiksi ja mitkä linkit suljetaan. Mikäli yhdelläkään kytkimellä ei ole uutta tietoa, niin ainoastaan juurisilta lähettää oletuksena kahden sekunnin välein hello-paketteja. Hello-pakettien ideana on yksinkertaisesti varmistaa verkon toimivuus. [12.]

### 2.9.2 Rapid Spanning Tree -protokolla lyhyesti

Rapid Spanning Tree (RSTP) tekee samaa kuin STP, eli estää silmukoiden syntymistä verkkoon. Se on kuitenkin todella paljon nopeampi konvergoitumaan, mikäli linkki katkeaa tai uusia linkkejä lisätään verkkoon. Kukin kytkin lähettää hello-paketin oletusarvoi-



sesti kahden sekunnin välein. Mikäli ajossa olevassa kytkimessä RSTP huomaa muutoksen verkossa, niin tilanpäivitysviesti lähetetään välittömästi, jotta muut kytkimet osaavat tarvittaessa sopeutua uuteen verkon topologiaan. Juniperin kytkimissä RSTP on oletuksena käytössä ilman erillistä päälle kytkemistä. Juniperin omien sanojen mukaan hyvin suunnitellussa verkossa tätä protokollaa käytettäessä verkon konvergenssiaika voi olla parhaimmillaan vain 0,5 sekuntia. [13.]

## 2.10 Spanning Tree -protokollan haavoittuvuus

Mikäli verkkoon liitetään väärennettyjä BPDU-paketteja lähettävä päätelaite, niin pahimmassa tapauksessa tästä päätelaitteesta tulee uusi juurisilta ja STP saadaan laskemaan verkon reittejä uudelleen ja uudelleen, jolloin yhteydet muuttuvat epävakaisiksi tai saattavat katketa kokonaan. Tällaisen ongelman selvittäminen saattaa tyypillisesti kestää jonkin aikaa, jolloin mahdollinen tuotantokatkos ehtii aiheuttaa paljon haittaa ja kustannuksia.

Suojautuminen tällaista hyökkäystä vastaan on hyvinkin helposti toteutettavissa. Juniperin kytkimissä tuo mekanismi tunnetaan nimellä BPDU-suojaus (BPDU protection), joka tulisi asettaa päälle kaikkiin kytkimen reunaportteihin eli portteihin, joihin kytketään jokin muu laite kuin toinen kytkin. Oletusarvoisesti kyseinen suojamekanismi sulkee portin, johon tulee ulkopuolinen BPDU-paketti, mutta portin sulkemisen sijaan toisena vaihtoehtona on määrittää suojaus ainoastaan suodattamaan ulkopuoliset BPDU-paketit pois. [14.]

### 2.10.1 Root Protection eli Juurivahti

Juurivahdin tarkoitus on yksinkertaisesti estää halutun portin päätyminen juuriportiksi. Juurivahti asetetaan päälle käsin haluttuihin portteihin. STP:n suorittama juuriportin valinta voi joissakin tapauksissa mennä väärin, mutta oikeisiin portteihin asetetun juurivahdin avulla tämä voidaan ehkäistä. Myös pahantahtoinen laite voi lähettää sopivia BPDU-paketteja, joilla juuriportin valinta pyritään saamaan epäedulliseksi verkon kannalta.

Juurivahdin ollessa päällä portti toimii aivan normaalisti ja välittää liikennettä niin kauan, kunnes porttiin saapuu superior STP BPDU. Superior STP BPDU on BPDU-paketti,

jonka vastaanottanut portti asettuu normaalisti juuriportiksi ja liikennettä välittävään tilaan. Juurivahdin vaikutuksesta portti menee kuitenkin estotilaan, eikä välitä mitään liikennettä eteenpäin. Kun estotilaan mennyt portti lakkaa saamasta superior STP BPDU-paketteja, niin se palaa takaisin välittävään tilaan (forwarding state). [15.]

On olemassa Multiple Spanning Tree (MSTP) -protokolla, jonka ideana on se, että luodaan joukko VLANeista riippumattomia spanning tree -instansseja. Samaan spanning tree -instanssiin yhdistetään siis useita VLANeja. Ajettaessa vain yhtä spanning tree -instanssia, säästetään kytkimen resursseja, mutta hyödynnetään verkon linkkien redundanttius dataliikenteen ohjauksella. Mikäli verkossa ajetaan useampia MSTP-instansseja, niin edellisessä kappaleessa mainittu estotila on instanssikohtainen.

Useimmissa tapauksissa verkon suojaamiseksi riittää Juniperin verkkolaitteissa BPDU Protection-tekniikka, joka käytännössä tarkoittaa sitä, että yksittäisiä portteja voidaan määrittää tilaan, jossa ne hylkäävät kaikki niihin tulevat BPDU-paketit. Root Protectionista puolestaan saadaan hyötyä erityisesti silloin, kun verkkoon täytyy liittää kytkin, joka ei ole omassa hallinnassa.

#### 2.10.2 Loop Protection eli Silmukkavahti

Silmukkavahti nimensä mukaisesti estää silmukoiden syntymistä. STP-versiot tekevät sitä myös, mutta silmukkavahti puuttuu peliin esimerkiksi siinä tapauksessa, jos juurisiltaan päin oleva estotilainen portti lakkaa saamasta BPDU-paketteja juurisillalta. Kytkin saa BPDU-paketteja kuitenkin toisesta suunnasta ja mikäli ne eivät sisällä tietoa muutuneesta verkon tilasta, niin estotilassa olevan portin tilaa ei ole syytä muuttaa. Juurisilta saattaa lakata lähettämästä BPDU-paketteja rautavian sattuessa, tai konfigurointivirheen sattuessa jompaankumpaan päähän kyseistä linkkiä. Ilman silmukkavahtia BPDU-pakettien loppuessa estotilainen portti vaihtuisi välittömästi välitystilaan ja pahimmassa tapauksessa verkkosilmukan syntyessä verkossa kulkevat levitysviestit monistuisivat ja lähtisivät kiertämään silmukkaa kumpaankin suuntaan monistuen jatkuvasti. Tämä johtaa äärimmillään verkon kapasiteetin loppumiseen kesken, jolloin verkko on käyttäjän näkökulmasta äärimmäisen hidas tai kokonaan jumissa. [16.]

### 2.10.3 Unidirectional Link Detection (UDLD) eli yksisuuntaisen linkin tunnistus

Ciscon valmistamissa verkkolaitteissa yksisuuntaisen linkin tunnistus toimii siten, että linkin kummassakin päässä olevaan kytkimeen on asetettu UDLD päälle, jolloin kytkimet lähettävät toisilleen paketteja. Tällöin kumpikin osapuoli on tietoinen siitä, että kumpikin kykenee sekä vastaanottamaan, että lähettämään paketteja. Tämän tunnistuksen avulla huomataan helposti optisten kuitujen väärinkytkenät ja laiteviat.

Juniperin valmistamissa EX-sarjan kytkimissä puolestaan on käyttöjärjestelmäversiosta 9.4 lähtien ollut mukana Link Fault Management (LFM) -ominaisuus, jonka avulla voidaan havaita ja hallita verkkolaitteiden välisten linkkien vikatilanteita.

Muissa Juniperin verkkolaitteissa vikatilanteiden havainnointi onnistuu siten, että kaksi fyysistä laitteiden välistä linkkiä yhdistetään yhdeksi loogiseksi linkiksi. Mikäli laite havaitsee, että linkin toisessa päässä oleva laite ei välitä loogisessa linkissä paketteja oikein, niin se poistetaan käytöstä. [17.]

### 2.11 Virtual Chassis eli virtuaalinen alusta

Virtual Chassis on verkkolaittevalmistaja Juniperin nimitys tekniikalle, jolla saadaan useampi kytkin toimimaan ja käyttäytymään kuin yksi iso kytkin. Kyse on siis kytkinpinosta, englanniksi switch stack. Tämän työn aiheena olevassa yritysverkossa käytettyjä kytkinmalleja on mahdollista asettaa pinoon enintään kymmenen kappaletta.

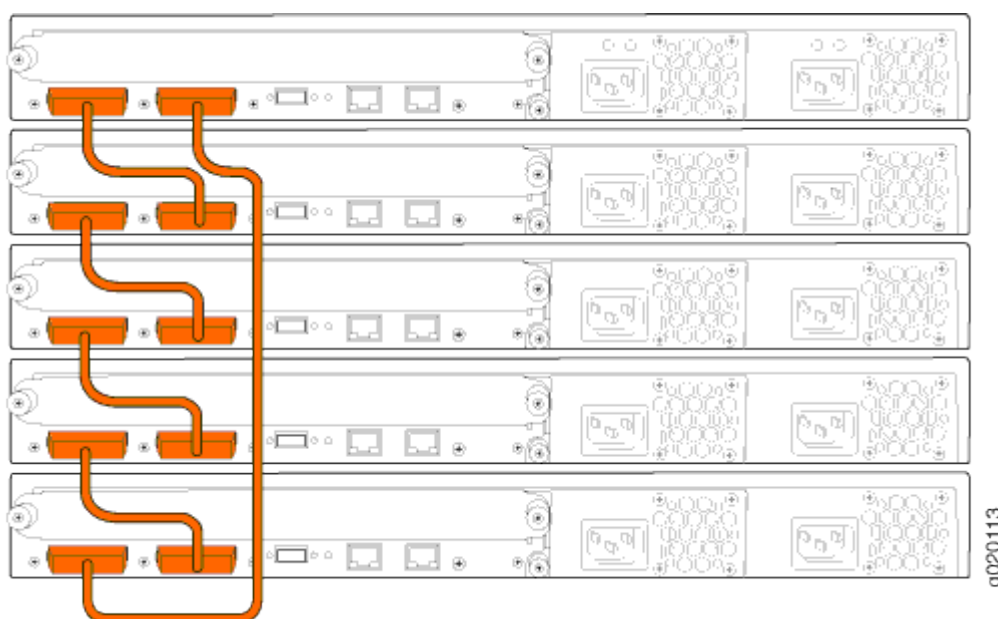
Virtual Chassis -tekniikan oikealla käytöllä on mahdollista saavuttaa merkittäviä hyötyjä ympäristöstä riippuen. Kytkinten konfiguroiminen pinoksi helpottaa ylläpidollisia toimia, sillä jokaista fyysistä kytkintä ei tarvitse konfiguroida erikseen, vaan saman kytkinpinon fyysiset kytkimet käyttäytyvät yhdessä kuin yksi iso kytkin ja toimivat yhden ja saman konfiguraation määrittelemällä tavalla.

Toinen suuri hyöty saadaan tilanteessa, jossa kytkinpinoon on kytketty esimerkiksi kaksi fyysistä yhteyttä keskuskytkinten suuntaan. Toisen uplinkin katketessa kytkinpinon toiminta ei häiriinny lainkaan ja kaikki pinoon liitetyt laitteet, kuten WLAN (Wireless Local Area Network) -tukiasemat ja verkkotulostimet ovat yhteydessä verkkoon jäljelle jääneen

uplink-yhteyden kautta. Virtual Chassis mahdollistaa uplink-yhteyden jakamisen fyysisten kytkinyksiköiden kesken. [18.]

Virtual Chassis -tekniikkaa käytettäessä kytkimet voidaan liittää toisiinsa tavallisilla Ethernet-kuparikaapeleilla tai optisilla kuiduilla alkaen 10 Mbps nopeudesta aina 10 Gbps nopeuteen asti. Täysi kapasiteetti saadaan käyttöön erikseen hankittavilla Juniperin Virtual Chassis -kaapeleilla, jotka tarjoavat 40 Gbps nopeuden kytkinten välille.

Riippumatta kytkinten välillä käytettävästä kaapeloinnista kytkimet liitetään toisiinsa renkaasmaisesti, jolloin kytkinpino sietää yhden linkin tai kytkimen vikaantumisen.



Kuva 8. Juniperin esimerkkikuva kytkinpinossa käytettävien kytkinten välisestä kaapeloinnista. [19]

## 2.12 802.1X-standardi eli porttikohtainen todentaminen

IEEE 802.1X (Port Based Authentication) -standardin tarkoituksena on estää tunnistamattomien päätelaitteiden luvaton liikennöinti yrityksen sisäverkossa. Tämän opinnäytetyön kohteena olevan yrityksen verkossa laitteiden tunnistautuminen tapahtuu työntekijöiden koneille asennetun sertifikaatin perusteella.

Käytännössä sisäverkkoon pääsy tapahtuu niin, että verkkoon kytkeytyvässä laitteessa ajetaan ohjelmistoa, joka tarjoaa käyttäjätunnusta ja salasanaa tai tässä tapauksessa digitaalista sertifikaattia autentikoijalle. Autentikoija on verkkolaite, kuten kytkin, jonka portti on aluksi auktorisoimattomassa tilassa. Autentikoija välittää saamansa tunnukset tai sertifikaatin autentikointipalvelimelle. Autentikointipalvelin tarkistaa vastaanottamiensa tunnuksien tai sertifikaatin oikeellisuuden. Mikäli se toteaa tunnukset tai sertifikaatin validiksi, niin autentikointi on onnistunut ja autentikoija asettaa liityntään käytetyn portin auktorisoituun tilaan. Tällöin normaali liikennöinti sisäverkkoon onnistuu. [20.]

Autentikoinnin epäonnistuessa liityntään käytetty portti pysyy auktorisoimattomana, ja liikennöinti sisäverkkoon ei tällöin onnistu. Riippuen käytettävistä asetuksista ja käyttöjärjestelmästä autentikoinnin uudelleenyritys saattaa tapahtua vasta esimerkiksi 20 minuutin kuluttua. Tässä tapauksessa odottamine ei ole järkevää, vaan nopeampaa on irrottaa verkkojohto ja kytkeä se uudelleen. Ongelmaksi tosin nousee loppukäyttäjien ohjeistus. [20.]

Kun päätelaite kirjautuu ulos, se lähettää uloskirjautumisviestin autentikoijalle, joka asettaa portin jälleen auktorisoimattomaan tilaan. Verkkajohtoon irrottaminen päätelaitteesta katsotaan uloskirjautumiseksi. [20.]

Mikäli verkkoon kytkettävään päätelaitteeseen on asennettu sertifikaatti, niin sille myönnetään pääsy yrityksen sisäverkkoon, kun taas muussa tapauksessa liikennöinti onnistuu vain vierasverkossa.

Esimerkiksi asiakaskäyttöön tarkoitetuissa neuvotteluhuoneissa ongelmana on, että joko ulkopuolinen vierailija tai yrityksen oma työntekijä voi kytkeä verkkojohtoon pienen kytkimen, johon saadaan useampi laite liitettyä. Tässä skenaariossa on luonnollisesti olemassa riskinsä ja riskinhallintaa varten porttikohtaisessa todentamisessa on Juniperin kytkimissä kolme erilaista toimintatilaa, jotka on selitetty tarkemmin seuraavien alaotsikoiden alla.

### 2.12.1 Single supplicant mode

Tässä tilassa autentikointi vaaditaan vain ensimmäiseltä autentikointiporttiin kytketyltä laitteelta. Mikäli autentikointiporttiin on liitettyä verkkoon kuulumaton kytkin ja ensimmäiseen kytkettyyn laitteeseen on asennettu sertifikaatti, niin se pääsee liikennöimään sisäverkkoon. Ongelmana on, että kaikki tämän jälkeen liitetyt laitteet pääsevät myös liikennöimään sisäverkkoon ensimmäisen laitteen siivellä. Positiivista kuitenkin on, että tarvitaan ensin sertifikaatillinen laite avaamaan yhteys. Oletuksena kytkimissä on uudelleenautentikointiasetus päällä, jonka oletusaika on 3600 sekuntia eli yksi tunti. Mikäli sertifikaatillinen laite sammutetaan tai irrotetaan verkosta uudelleenautentikointiasetuksen ollessa päällä, niin yhteys muilta koneilta katkeaa automaattisesti ajan umpeutuksessa. [21.]

Tämä toimintatila ei ole toimiva ratkaisu, koska oletus on se, että yrityksen työntekijöille tarjotuissa tietokoneissa on sertifikaatti asennettuna. Mikäli yrityksessä tai muussa organisaatiossa olisi jostakin syystä sertifikaatilla varustettujen tietokoneiden ohella käytössä myös sertifikaattittomia koneita, niin tämän toimintatilan käyttö voisi olla perusteltua.

On olemassa sellaisia verkkoratkaisuja, joissa omalla hubilla varustettu IP-puhelin on liitetty kytkimeen ja tietokone liitetty IP-puhelimeen. Tällaista toteutusta ei tämän opinäytetyön kohteena olevassa yrityksessä ole, mutta tässä toimintatilassa sertifikaatin tulisi olla IP-puhelimessa, jolloin siihen liitetty tietokone pääsee liikennöimään sisäverkkoon.

### 2.12.2 Single-secure supplicant mode

Tässä tilassa autentikoidaan vain yksi laite kutakin autentikointiporttia kohti. Vaikka autentikointiporttiin olisikin liitettyä ylimääräisen kytkimen kautta useampia laitteita, niin vain ensimmäisenä autentikoitunut kone pääsee liikennöimään verkossa ja kaikkien muiden liikennöinti estetään. Muut laitteet pysyvät estettyinä niin kauan, kunnes autentikoitu laite sammutetaan tai irrotetaan verkosta. [21.]

Tietoturvan näkökulmasta tämä toimintatila on oikein hyvä, mutta ongelmaksi muodostuu juuri kaikkien muiden laitteiden liikennöinnin estyminen.

Mikäli verkossa on edellisessä aliluvussa kuvatus kaltainen ratkaisu IP-puhelimen kautta kytkimeen liitetystä tietokoneesta, niin tässä toimintatilassa sekä IP-puhelimessa että tietokoneessa tulee olla asennettuna sertifikaatti. Tämä siksi, että molemmat laitteet eivät voi olla samaan aikaan autentikoituneena.

#### 2.12.3 Multiple supplicant mode

Tässä toimintatilassa autentikoidaan kukin päätelaite erikseen vaikka ne olisivatkin liitettyinä erillisen kytkimen kautta. Autentikoitavien laitteiden määrää voidaan rajoittaa asettamalla kytkimeen haluttu maksimimäärä. [21.]

### 3 Ympäristön kuvaus

Kuten aiemmin kerroin, niin yritys on monikansallinen ja sillä on Suomenkin sisällä Helsingissä sijaitseva päätoimisto sekä pienempiä erikokoisia aluetoimistoja. Päätoimistolla työskentelee noin 800 henkilöä, ja aluetoimistoissa henkilöstömäärä vaihtelee vain yhdestä noin sataan.

#### 3.1 Core-kytkin

Konehuoneessa oleva Core-kytkin koostuu kahdesta Juniper EX4550-32F L3 -kytkimestä, jotka on kytketty ja asetettu Virtual Chassis -tilaan. Näin kuituyhteys kerroskytkimille ja palvelimille on saatu kahdennettua. VLAN-verkkojen välinen reititys tehdään core-kytkimillä.

Kyseisissä kytkimissä on 32 kappaletta paikkoja, joihin voi asentaa tarpeeseen sopivan moduulin. Käytännössä valittavana on vain 10 Gbps-yhteydet mahdollistava kuituoptiikkamoduuli sekä 1 Gbps-yhteydet tarjoava RJ45-liittimen tarjoava parikaapelimoduuli. Kyseisiin paikkoihin on myös mahdollista asentaa suoraan SFP+ DAC-kuparikaapeli (enhanced Small Form-factor Pluggable Direct Attach Cable), joka mahdollistaa 10 Gbps-yhteydet enintään seitsemän metrin pituisena. Tämän tyyppisiin kaapeleihin on valmiiksi

integroitu kytkimen paikkaan sopiva moduulipää, jolloin erillistä moduulia johdon kytke-miseksi ei tarvita.

Core-kytkinten Virtual Chassis -kytkentään on käytetty Juniperin omia Virtual Chassis -moduuleja ja johtoja, joilla yhteysnopeus on 40 Gbps.

### 3.2 Kerroskytkimet

Uusissa toimitiloissa on seitsemän kerrosjakamoja ja jokaisen kerroksen kerrosjaka-mossa on kaksi kappaletta L3-ominaisuuksilla varustettua Juniper EX3300 -kytkintä, jotka on kytketty ja konfiguroitu Virtual Chassis -tilaan samanlaisella SFP+ DAC-kaape-lilla kuin core-kytkin.

Jokaisen kerroksen kumpikin kytkin on yhteydessä core-kytkimeen omalla 10 Gbps:n kuitulinkillä. Tällöin toisen yhteyden katkeaminen ei vaikuta kyseisen kerroksen verkon toimivuuteen lainkaan.

Toisen kytkimen hajoaminen tai kahdennetun kuitulinkin yhteyden katkeaminen aiheut-taa ongelmia, mutta ei lamauta kyseisen kerroksen verkkoa täysin. Langattomista tu-kiasemista puolet on kytketty toiseen Virtual Chassis -pinon jäseneen ja puolet toiseen. Tällöin toisen kytkimen hajotessa langattoman verkon peittoalue pysyy maksimaalisena, mutta puolet kapasiteetista häviää, mikä mahdollisesti aiheuttaa havaittavaa pätkimistä tai hidastelua käyttäjien verkkoyhteydessä. Kytkimen hajotessa tietenkin kaikki kysei-seen kytkimeen suoraan liitetyt laitteet putoavat pois verkosta, ja tämän vaikutuksen suu-ruus riippuu kerroksesta, sillä jokaisessa kerroksessa on hieman eri määrä toimistoissa käytettäviä verkkolaitteita, kuten WLAN-tukiasemia, tulostimia, infonäyttöjä ja neuvotte-luhuoneiden varaamiseen käytettäviä Evoko Room Managereita.

### 3.3 VLAN -verkkosegmentit

Laajemmissa verkoissa on hallinnan helpottamiseksi ja tietoturvan parantamiseksi useimmiten käytössä VLAN-verkkosegmenttejä. Tämän työn aiheena olevassa toimisto-



verkossa on käytössä useita VLAN-segmenttejä juuri edellä mainituista syistä. Toimistossa jokaiselle kerrokselle on olemassa oma segmenttinsä, joten päätelaite saa langattoman verkon kautta IP-osoitteen kyseisen kerroksen oman VLANin IP-osoitepoolista.

Myös palvelimille ja tulostimille on omat VLAN-segmentit.

### 3.4 Palvelimet

Palvelimet sijaitsevat toimiston kellarikerroksessa olevassa konehuoneessa kahden kulunvalvotun oven takana. Konehuoneessa on yksi iso laitekaappikonaisuus, joka koostuu kuudesta 1200 mm syvästä laitekaapista, joihin voi asentaa laitteita etu- sekä takapuolelle. Laitekaapin sisällä on suljettu ilmankierto, jolloin kaukokylmällä viilennettävä ilmamäärä on huomattavasti pienempi verrattuna koko konehuoneen viilentämiseen. Laitekaapin varusteluun kuuluu hälytysjärjestelmä lämpötilan nousun varalta, sammutuslaitteisto sekä UPS (Uninterruptible Power Supply eli keskeytymätön virransyöttö). Varavirtajärjestelmä on mitoitettu siten, että palvelimet ehditään ajaa hallitusti alas ennen akkuvirran loppumista.

Laitekaappeihin on tällä hetkellä asennettuna kuuden isäntäkoneen VMWare ESXi -ympäristö, joissa on yhteensä ajossa noin 200 virtuaalikonetta. Asennettuna on myös levyjärjestelmä noin 200 teratavun tallennuskapasiteetilla, yksi fyysinen varmistuspalvelin, nauharobotti, palomuureja, VPN-yhteykskeskitin sekä aiemmin mainittu core-kytkin.

### 3.5 Verkkoyhteydet

Kuvaus lyhyesti

Helsingin toimisto on Suomen verkkokeskittymä. Etätoimistoista on käytössä MPLS-yhteys (Multiprotocol Label Switching) vähintään 50/50 Mbps nopeudella Helsingin toimistoon. Helsingin toimistosta on 1000/1000 Mbps yhteys julkiseen internetiin sekä 20/20 Mbps:n yhteys yrityksen globaaliin sisäverkkoon.

## Liikenteen priorisointi

Priorisointia ei tarvitse toimistoiden sisäverkoissa tehdä, koska etätoimistoissakin sisäverkon nopeus on vähintään 100 Mbps ja käyttäjiä on huomattavasti vähemmän kuin Helsingissä päätoimistossa. Päätoimiston sisäverkon kapasiteetti on monitoroinnin perusteella riittänyt hyvin, joten tarvetta priorisoinnille ei ole ilmennyt. Priorisointia ei tarvitse tehdä myöskään etätoimistoiden ja päätoimiston välisissä yhteyksissä, koska yhteysnopeus on riittävä, eikä verkon ruuhkautumista esiinny.

Priorisointia kuitenkin tehdään globaaliin sisäverkkoon johtavalla linjalla. Priorisointia tarvitaan, koska yhteysnopeus on kohtalaisen pieni ja linjaa pitkin kulkee paljon liikennettä. Globaali sähköpostipalvelin sijaitsee Hollannissa, joten koko Suomen sähköpostiliikenne kulkee sitä kautta. Myös videoneuvottelut ulkomaille kulkevat Hollannin kautta.

## 4 Tutkimukset

Kuten johdannossa kerroin, niin tämän työn tavoitteena on kartoittaa ja parantaa Helsingin toimiston sisäverkon tietoturvaa. Tekniikoiden ja protokollien teoriasta ja tietoturvaohjeiden kartoituksesta kerroin luvussa kaksi. Kolmannessa luvussa kuvasin verkkoympäristön ja tässä neljännessä luvussa käyn läpi työkalujen ja -järjestelyiden esittelyt, sekä testit ja niiden tulokset.

Kaikki testit tehtiin hyvien perusperiaatteiden vastaisesti suoraan tuotantoverkkoon yksinkertaisesti siitä syystä, että erillistä testiverkkoa ei ollut. IT-osastolla ei työn tekemisen aikaan ollut laiterikkojen varalta yhtään ylimääräistä Juniperin kytkintä, jota olisi voinut lainata testien suorittamista varten.

Testien vaikutus oli kytkimen asetuksilla rajattu koskemaan vain ensimmäisen kerroksen kytkintä. Ensimmäinen kerros on katutasossa oleva aulakerros, jossa työskentelee säännöllisesti vain noin viisi henkilöä. Kerroksessa on myös auditorio, mutta testien suorittamisen aikaan auditoriota ei oltu varattu koulutuksia tai muita tilaisuuksia varten.

Testit suoritettiin perjantaina ilta-aikaan, jolloin kaikki ensimmäisen kerroksen työntekijät olivat jo lähteneet pois. Tällä ajankohdalla ja vaikutusten rajaamisella vain ensimmäisen

kerroksen kytkimeen pahin mahdollinen skenaario koko kytkimen sekoamisella olisi ollut se, että muussa kerroksessa pääsääntöisesti työskentelevä henkilö olisi tullut jostakin syystä ensimmäiseen kerrokseen ja huomannut langattomien verkkojen kadonneen. Tämän toteutumista pidettiin melko epätodennäköisenä ja mahdollista haittaa arvioitiin vähäiseksi, koska ensimmäisessä kerroksessa ei ole normaaliin työskentelyyn tarkoitettua kalustusta, kuten pöytiä ja tuoleja.

Ennen testejä tarkastin kytkimen lähtötilan kunkin testattavan asian suhteen ja vertasin kytkimen ilmoittamia tietoja testien jälkeisiin tietoihin. Testien jälkeen tarkastin itse kytkimen toimivan normaalisti kytkemällä ja irrottamalla tietokoneita ja testaamalla niiden verkkoyhteyksien toimivuuden. Varmuuden vuoksi IT-osaston järjestelmänsinööri tarkasti kytkimen tilan etäyhteydellä viikonlopun aikana. Kaiken varalta tulin maanantaina töihin normaalia aikaisemmin, jotta mahdollisten ongelmien ilmetessä voitaisiin reagoida välittömästi. Ongelmia kytkimen toimivuudessa ei ilmennyt seuraavalla viikolla.

#### 4.1 DHCP Snooping

DHCP snooping sallii kytkimen monitoroida ja kontrolloida kytkimeen liitetyiltä epäluotetuilta laitteilta tulevia DHCP-viestejä. Kytkin kokoaa ja ylläpitää tietokantaa valideista IP- ja MAC-osoitepareista. Tätä tietokantaa kutsutaan DHCP snooping -tietokannaksi. DHCP snooping siis kaikessa yksinkertaisuudessaan pudottaa DHCP-viestit, jotka ovat peräisin ei-luotetulta DHCP-palvelimelta. [22.]

#### 4.2 Dynamic ARP Inspection (DAI)

Dynaaminen eli reaaliaikainen ARP-seuranta suojaa kytkintä ARP-väärennöksiltä. DAI tutkii ARP-paketteja ja vertaa niiden sisältämää tietoa DHCP snooping -tietokantaan. Mikäli paketin lähettäjän MAC- ja IP-osoite eivät täsmää tietokannassa olevaan tietoon, niin paketti pudotetaan. DAI estää siis tehokkaasti välimieshyökkäyksen onnistumisen. [23.]

### 4.3 IP Source Guard

IP source guard on Juniperin nimitys kytkimen portin tietoturvaominaisuudelle, jonka tarkoitus on eliminoida lähde IP-osoitteen ja lähde MAC-osoitteen väärennyshyökkäystä. Jos IP source guard päättää laitteen lähettäneen paketin, jonka header-tiedoissa on DHCP snooping -tietokantaan sopimaton IP-osoite tai MAC-osoite, niin kytkin ei välitä pakettia eteenpäin. Paketti siis tuhoutuu. Mikäli käytössä on staattisia IP-osoitteita VLANeissa, niin nämä osoitteet tulee lisätä kytkimen DHCP snooping -tietokantaan. [24.]

Tämä estää MAC-tulvituksen, jolla yritetään täyttää kytkimen MAC-taulu ja saada kytkin käyttäytymään kuin hubi (porttitoistin). Porttitoistin nimensä mukaisesti toistaa kaiken siihen saapuvan liikenteen kaikkiin portteihin, vaikka vain yhteen porttiin olisi kytketty laite, jolle liikenne oikeasti olisi tarkoitettu. Tällainen kytkimen käytös tapahtuu siksi, että osoitetaulun muisti on loppunut kesken, eikä kytkin enää tiedä laitteiden tarkkaa sijaintia. Tällöin hyökkääjä voisi helposti nuuskaa ja tallentaa mille tahansa kytkimeen liitetylle laitteelle tarkoitettuja IP-paketteja.

### 4.4 Porttikohtainen todentaminen 802.1X

Tätä tekniikkaa kokeiltiin, mutta johtuen työasemien haittaohjelmasuojauksesta ongelmia ilmeni toimiston omaan verkkoon pääsyssä. Noin kahdeksan kertaa kymmenestä kone päätyi oikeaan verkkoon, mutta noin kaksi kertaa kymmenestä kone päätyi virheellisesti vierasverkkoon. Ilman haittaohjelmasuojauksia onnistumisprosentti oli 100, eikä ongelmia ilmennyt.

Tarkempi ongelman juurisyyn selvittäminen olisi ollut mielenkiintoista, mutta pienen tutkimisen jälkeen ratkaisua ei vaikuttanut löytyvän, joten tämän tekniikan käyttöönotosta päätettiin luopua.

#### 4.5 VLAN-liikenteen suodatus

Juniperin kytkimissä VLANien välistä liikenteen suodatusta varten tulee ensin määritellä kytkimeen prefix-lista, johon määritellään suodatettavat VLANit niiden IP-osoitteiden perusteella. Tämän jälkeen luodaan varsinainen suodatin, johon liitetään haluttu prefix-lista. Suodattimeen määritellään halutut toiminnallisuudet, eli esimerkiksi se, että estetäänkö vai sallitaanko liikennöinti listatuista verkoista.

Suodatusta lähdettiin rakentamaan sillä ajatuksella, että palvelinverkkoon ei tulisi päästä kiinni mistään muualta, kuin erikseen määritellyiltä frontend-koneilta. Suodatus tuli kytkeä päälle myös toiseen suuntaan, koska palvelimien ei ole tarvetta liikennöidä kaikkiin talon verkossa käytettäviin VLANeihin. [25.]

#### 4.6 Tietoturvamekanismien testaamiseen käyttämäni työkalut

Ennalta ei ollut tarkalleen tiedossa, millä tavalla ja mitä työkaluja käyttäen tietoturvamekanismeja olisi mahdollista testata. Melko nopealla etsinnällä löysin Kali Linux -distribuition ja asensin sen USB-massamuistille, jolta käynnistin hyökkäyksiin käytetyn tietokoneen.

##### 4.6.1 Kali Linux

Kali Linux on aktiivisesti ylläpidetty ja päivitetty Linux-distributio, johon on koottu erittäin laaja valikoima työkaluja eri tietoturvallisuuden osa-alueilta. Työkaluja löytyy niin passiiviseen tutkimiseen ja skannaamiseen kuin aktiiviseen hyökkäämiseen, murtamiseen ja tunkeutumiseen.

##### 4.6.2 Ettercap

Ettercap on avoimeen lähdekoodiin perustuva ilmaist työkalu, joka on saatavilla useille Linux-/Unix-pohjaisille käyttöjärjestelmille sekä Microsoft Windowsille. Ohjelmalla voidaan kaapata verkkoliikennettä, vakoilla salasanoja sekä toteuttaa välimieshyökkäys monellakin eri protokollalla.

Ettercap asettaa verkkosovittimen promiscuous modeen (eli kaikki liikenne välitetään prosessorille, eikä vain oikeasti itselle tarkoitettu) ja ARP-myrkyttää kohdelaitteet. Tällöin voidaan suorittaa välimieshyökkäys tai palvelunestohyökkäys. Palvelunestohyökkäys saadaan helposti aikaan, kun onnistuneen ARP-myrkytyksen jälkeen hyökkääjälle päätyvät paketit joko pudotetaan kokonaan tai muuten vain jätetään välittämättä kohteeseen.

Ettercapia käyttämällä onnistuin suorittamaan välimieshyökkäyksen ja sain kaapattua toisen tietokoneen ja reitittimen välille muodostetun salaamattoman Telnet-session. Ettercap sai kytkimen tallentamaan uhrikoneen MAC-osoitteen tilalle hyökkäyksessä käytetyn tietokoneen MAC-osoitteen, ja näin uhrille tarkoitettu liikenne päättyi hyökkäyksen suorittavalle tietokoneelle ja sain hallintaani avoimena olleen komentorivisession.

Tietenkin tässä on syytä muistaa se, että hyökkäystä suoritettaessa ja kokeiltaessa oli runsaasti tietoa kohdeverkosta ennakkoon, eikä aikarajaa tai kiinnijäämisen pelkoa ollut. Mikäli uhrin ja kytkimen välinen sessio olisi ollut salattu, niin tällöin olisin saanut kaapattua liikenteen, mutta salauksen takia en olisi pystynyt lukemaan sen sisältöä.

Kaapattua ja salattua liikennettä käyttämällä on kuitenkin mahdollista suorittaa Replay Attack, eli toistohyökkäys. Hyökkäyksessä lähetetään kaapatut paketit uudelleen kohdejärjestelmään. Tämä hyökkäys on ikään kuin välimieshyökkäyksen pikkuveli, koska salattujen pakettien sisältöä ei välttämättä tiedetä. Tällöin tavoite on lähinnä häiritä kohdejärjestelmiä.

Onnistuneen välimieshyökkäyksen suorittamisen jälkeen asetin kytkimeen päälle DAI. Välimieshyökkäys lakkasi välittömästi toimimasta, juuri kuten odotinkin tapahtuvan. Tämä johtuu siitä, että DAI havaitsee ja tunnistaa Ettercapin lähettämän väärennetyn ARP-paketin, jossa hyökkäävän koneen MAC-osoite on yhdistetty IP-osoitteeseen, jonne uhrikoneelta oli otettu Telnet-yhteys. Vastaanotettu paketti ei täsmää DHCP snooping -tietokannassa olevaan tietoon hyökkäävän tahon IP- ja MAC-osoitteesta, joten paketti pudotetaan.

#### 4.6.3 Macof

Macof on automaattinen MAC-tulvitustyökalu, jolla saadaan lähetettyä verkkoon loputtomasti satunnaisesti generoituja MAC-entryjä. Tältä hyökkäykseltä suojaamaton kytkin tallentaa vastaanottamansa tiedot MAC-tauluunsa, ja taulun täyttyessä se alkaa käyttäytyä kuin hubi eli porttitoistin. Riippuen hyökkäykseen käytetystä laitteistosta, Macof kykenee generoimaan jopa 155 000 MAC-entryä minuutissa.

Tavallisen kytkimen MAC -taulun koko on yleensä asetettu noin 5000–30000 entryyn. Esimerkiksi Juniperin EX3300 -kytkimessä MAC -taulun kooksi on oletuksena määritetty 5120 kappaletta, mutta määrä on konfiguroitavissa välille 16–1048575. Suurta MAC-taulun kokoa käytettäessä on syytä huomioida se, että kytkimestä saattaa loppua resurssit kesken, mikäli käytössä on paljon toimintoja.

Kartoitusvaiheessa tietokone oli kytketty suoraan kytkimeen ja Macofin MAC-tulvitus käynnistettiin. Kytkimen monitoroinnista nähtiin, että MAC-tauluun tallentui nopeasti kymmeniä tuhansia MAC-entryjä ja tässä kohtaa tulvitus kytkettiin pois päältä varmuuden vuoksi. Tulvitushyökkäys todettiin onnistuneeksi.

Onnistuneen tulvitushyökkäyksen jälkeen tyhjensin manuaalisesti kytkimen MAC-taulun kaiken varalta. MAC-taulun entryjen vanhenemisaika on oletuksena 300 sekuntia eli viisi minuuttia. Kokeilin myös tulvittaa varmuuden vuoksi huomattavasti pienemmän määrän MAC-entryjä, eli noin 10 000 kappaletta ja odotin viisi minuuttia, jonka jälkeen ne poistuivat kuten pitikin.

Tulvitushyökkäysten suorittamisen jälkeen asetin kytkimeen päälle IP Source Guard -mekanismin ja testasin tulvitusta uudelleen. Tietoturvamekanismi toimi kuten pitikin, eikä tulvitus onnistunut. Mikään Macofin lähettämistä paketeista ei täsmännyt DHCP snooping -tietokannassa oleviin tietoihin, joten kaikki paketit tulkittiin virheellisiksi ja ne pudotettiin.

#### 4.6.4 Vihamielinen DHCP-palvelin

Kali Linuxissa ei ollut valmiina DHCP-palvelinohjelmistoa ja koska ajoin Kalia USB-massamuistilta, en halunnut lähteä DHCP-palvelinta siihen asentamaankaan. Näistä syistä johtuen päätin asentaa DHCP-palvelinohjelmiston Windows-tietokoneelle.

Verkon kartoitusvaiheessa DHCP-palvelinohjelmisto toimi kuten pitikin, ja se vastasi onnistuneesti kytkimeen liitetyle uudelle laitteelle ja laite otti käyttöön tämän ei-luotetun DHCP-palvelimen lähettämät määrytykset. Mikäli määrytyksissä käytettävät IP-osoitteet ovat täysin väärä, niin tapahtuu jonkinasteinen palvelunestohyökkäys, koska uhrikoneen lähettämät paketit on lähetetty IP-osoitteisiin, joita ei ole olemassa kyseisessä verkossa.

Käyttämissäni määrytyksissä oli asetettu hyökkäävän koneen IP-osoite oletusyhdykäytäväksi, jolloin kaikki ulkoverkkoon tarkoitettu liikenne päätyi hyökkääjälle. Käytin verkkoliikenteen pakettien tutkimiseen tarkoitettua Wiresharkia tutkiakseni verkkosovittimeen saapuvia paketteja ja havaitsin paketteja saapuvan uhrikoneelta. Välimieshyökkäys olisi siis ollut mahdollista toteuttaa.

Tässä vaiheessa asetin DHCP Snoopingin päälle kytkimeen ja liitin verkkoon uuden tietokoneen. Uusi tietokone sai vastauksen verkon oikealta DHCP-palvelimelta, joten enää sillä ei ollut vaaraa joutua välimies- tai palvelunestohyökkäyksen kohteeksi. DHCP Snooping toimi kuten pitikin ja huomasi epäluotettavalta laitteelta tulevat DHCP-viestit ja pudotti ne.

## 5 Konkreettiset toimenpiteet

Tutkimusteni tulosten perusteella DHCP Snooping päätettiin ottaa käyttöön kaikissa tutkimissa, koska sen avulla ei-toivotut DHCP-palvelimet eivät pysty toimimaan, joten niiden aiheuttamista mahdollisista häiriöistä tai ongelmista ei tarvitse huolehtia.



Testaus osoitti DAIn eli reaaliaikaisen ARP-seurannan toimivaksi, ja se otettiin käyttöön kaikissa kytkimissä, koska sen avulla estetään tehokkaasti esimerkiksi välimieshyökkäyksen onnistuminen.

Testauksen perusteella myös IP Source Guard todettiin toimivaksi ja sekin otettiin käyttöön kaikissa kytkimissä, koska sen avulla MAC flooding -hyökkäys saadaan estettyä.

802.1X osoittautui testien perusteella erittäin potentiaaliseksi tekniikaksi mutta liian huonosti yhteensopivaksi tietokoneissa käytetyn virustorjuntaohjelmiston kanssa. Epäluotettavan toiminnan takia tekniikkaa ei päätetty ottaa käyttöön. Mikäli 802.1X:n ja virustorjuntaohjelmiston väliset vaikeudet poistuvat esimerkiksi uusien ohjelmaversioiden tai käyttöjärjestelmäpäivitysten myötä, niin tämän tekniikan käyttöönottoa halutaan varmasti harkita uudelleen. Käyttäjille aiheutuisi yksinkertaisesti liikaa ongelmia ja hämmennystä, mikäli verkkojohtoa kytkettäessä yrityksen oman työntekijän tietokone joutuu väärin perustein vierasverkkoon, ja sisäverkon palvelut ovat saavuttamattomissa

Liikenteen suodatus VLAN-verkkojen välillä otettiin käyttöön, koska se on erittäin tehokas ja käytännöllinen tapa estää liikennöinti verkkojen välillä.

## 6 Yhteenveto

Tämä työ käsitteli pääasiassa vain Helsingissä sijaitsevaa Suomen päätoimistoa, mutta tietoja ja kokemuksia voidaan luonnollisesti hyödyntää myös aluetoimistoissa. Toki aivan pienimmät aluetoimistot eivät kuulu joukkoon, koska pienimmillään aluetoimisto saattaa käsittää vain yhden työntekijän, joka liittyy yrityksen verkkoon mobiililaajakaistalla VPN-yhteyden yli. Hiemankin isommissa aluetoimistoissa on asennettu Juniperin kytkin ja se voidaan määrittää käyttämään DHCP Snoopingia, DAIta ja IP Source Guardia.

Liikenteen suodatus on myös mahdollista ottaa käyttöön Juniperin kytkimellä varustetuissa etätoimistoissa. Tämä tullaan ennemmin tai myöhemmin tekemään, koska etätoimistoissa käyttäjät kuuluvat käyttäjille tarkoitettuun VLANiin samaan tapaan kuin päätoimistonkin käyttäjät. Verkon IP-avaruus tosin on eri, mutta suora liikennöinti palvelinverkkoon on silti tietoturvan parantamisen vuoksi estettävä.

Porttikohtainen todentaminen, eli 802.1X on myös mahdollista ottaa käyttöön etätoimistoissa, joissa on Juniperin kytkin. Tämä tekniikka tullaan varmasti ottamaan käyttöön, mikäli luotettavuusongelmista päästään tavalla tai toisella eroon.

Tämän työn tekeminen osoittautui huomattavasti mielenkiintoisemmaksi kuin ennalta arvelinkaan. Tässä työssä käsitellyt turvamekanismit ovat pohjimmiltaan kohtalaisen helppo ja nopea kytkeä käyttöön erilaisten ohjeiden avulla, mutta syvällisemmän ymmärryksen hankkimiseksi jouduin kyllä opiskelemaan tosissani ja tekemään muistiinpanoja. Työssä oli paljon itsenäistä tutkimista, opiskelua ja testausta, mutta työpaikalla työtä ohjannut järjestelmäinsinööri oli useasti apuna ja nimenomaan ohjaamassa oikeaan suuntaan. Apua sain sitä kaivatessani, mutta en suinkaan suoria vastauksia. Tukena ja apuna oli myös koko sisäinen IT-osasto lähinnä 802.1X-testauksessa.

Työn tekeminen vaati pitkäjänteisyyttä ja huolellisuutta, joita minulta omasta mielestä löytyykin. Oli tärkeää pitää kirjaa tehdyistä muutoksista ja kokeiluista sekä havaituista asioista. Tekeminen ei ollut loppupeleissä kovinkaan nopeatempoista, mutta erittäin johdonmukaisesti etenevää.

Minulle mieluisaa oli työn käytännönläheisyys ja tieto siitä, että työn tuloksia tullaan oikeasti hyödyntämään. Juniperin kytkimiin olin kyllä koulussa päässyt tutustumaan, mutta tämän työn myötä Juniperin käyttämä Ciscon laitteista eroava toimintalogiikka tuli kunnonla tutuksi.

Todella kiinnostavaa oli myös kokeilla turvamekanismien toimivuus käytännössä. Kali Linuxia en ollut aiemmin käyttänyt ja arvioisin, että myöhempää työuraa ajatellen oli erittäin hyödyllistä päästä tutustumaan siihen ja sen sisältämiin työkaluihin. MAC-osoitteiden tulvitus ja välimieshyökkäyksen suorittaminen onnistuneesti tuntui hienolta. Hienoa oli myös todeta turvamekanismien toimivuus niiden päälle kytkemisen jälkeen.

Mielestäni työn tavoitteet saavutettiin hyvin. Verkko on nyt suojattu monella tavalla ja yksinkertaisimmat hyökkäykset eivät enää toimi. Porttikohtaisesta todentamisesta saimme arvokasta tietoa ja käyttäjille tarkoitetut VLANit on eristetty suodatuksella palvelinten käyttämästä VLANista.

## Lähteet

- 1 Cloud Academyn selitys DNS-järjestelmästä <<https://cloudacademy.com/blog/how-dns-works/>> Luettu 19.3.2018.
- 2 Tietoturvayhtiö Kasperskyn selitys DNS Poisoningista ja Spoofingista <<https://www.kaspersky.com/resource-center/definitions/dns>> Luettu 19.3.2018.
- 3 Technopedian selitys ARP-protokollasta <<https://www.techopedia.com/definition/5493/address-resolution-protocol-arp>> Luettu 19.3.2018.
- 4 Veracoden selitys ARP-spoofingista <<https://www.veracode.com/security/arp-spoofing>> Luettu 19.3.2018.
- 5 Lifewiren selitys DHCP-protokollasta <<https://www.lifewire.com/what-is-dhcp-2625848>> Luettu 19.3.2018.
- 6 Serverbrainin selitys DHCP-protokollan laina-ajan uusimisesta <<https://www.serverbrain.org/network-services-2003/how-the-dhcp-lease-renewal-process-works-1.html>> Luettu 25.5.2019.
- 7 Omnisecun selitys DHCP-starvationista ja DHCP-spoofingista <<http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>> Luettu 19.3.2018.
- 8 Lifewiren selitys VLAN-verkoista <<https://www.lifewire.com/virtual-local-area-network-817357>> Luettu 27.5.2019.
- 9 Fiber Optic Transceiver Modulen julkaisema taulukko VLAN- ja aliverkkojen ominaisuuksista <<http://www.fiber-optic-transceiver-module.com/vlan-vs-subnet.html>> Luettu 28.5.2019.
- 10 Omnisecun selitys switch spoofingista ja siltä suojaumisesta <<http://www.omnisecu.com/ccna-security/what-is-switch-spoofing-attack-how-to-prevent-switch-spoofing-attack.php>> Luettu 19.3.2018.
- 11 Omnisecun selitys tuplatagauksesta ja siltä suojaumisesta <<http://www.omnisecu.com/ccna-security/what-is-double-tagging-attack-how-to-prevent-double-tagging-attack.php>> Luettu 19.3.2018.
- 12 Fossbytesin selitys STP-protokollan toiminnasta <<https://fossbytes.com/spanning-tree-protocol-stp-operational-basics/>> Luettu 19.3.2018.

- 13 Juniperin perustason selitys RSTP-protokollasta <[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/stp-rstp-qfx-series-understanding.html](https://www.juniper.net/documentation/en_US/junos/topics/concept/stp-rstp-qfx-series-understanding.html)> Luettu 19.3.2018.
- 14 Tomickin syvälinen selostus STP-hyökkäyksen rakentamisesta <<http://www.tomicki.net/attacking.stp.php>> Luettu 19.3.2018.
- 15 Juniperin dokumentaatio Root protectionista <[https://www.juniper.net/documentation/en\\_US/junos/topics/example/spanning-trees-root-protection-ex-series.html](https://www.juniper.net/documentation/en_US/junos/topics/example/spanning-trees-root-protection-ex-series.html)> Luettu 19.3.2018.
- 16 Juniperin dokumentaatio Loop Protectionista <[https://www.juniper.net/documentation/en\\_US/junos/topics/example/spanning-trees-loop-protection-ex-series.html](https://www.juniper.net/documentation/en_US/junos/topics/example/spanning-trees-loop-protection-ex-series.html)> Luettu 19.3.2018.
- 17 Juniperin selitys yksisuuntaisen linkin tunnistuksesta <<https://kb.juniper.net/Info-Center/index?page=content&id=KB13314>> Luettu 29.5.2019.
- 18 Juniperin Virtual Chassis -ohje <[https://www.juniper.net/documentation/en\\_US/junos/information-products/pathway-pages/qfx-series/virtual-chassis.pdf](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/qfx-series/virtual-chassis.pdf)> Luettu 21.3.2018.
- 19 Juniperin esimerkkejä mahdollisista Virtual Chassis -kaapeloinneista <[http://www.juniper.net/techpubs/en\\_US/release-independent/junos/topics/reference/requirements/cable-ex4200-virtual-chassis-cabling-examples.html](http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/requirements/cable-ex4200-virtual-chassis-cabling-examples.html)> Luettu 21.3.2018.
- 20 Juniperin dokumentaatio porttikohtaisesta todentamisesta <[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/802-1x-authentication-switching-devices.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/802-1x-authentication-switching-devices.html)> Luettu 19.4.2019.
- 21 Juniperin ohjeistus porttikohtaisen todentamisen eri toimintamoodien käyttöön <[https://www.juniper.net/documentation/en\\_US/junos/topics/example/802-1x-pnac-single-supPLICANT-multiple-supPLICANT-configuring.html](https://www.juniper.net/documentation/en_US/junos/topics/example/802-1x-pnac-single-supPLICANT-multiple-supPLICANT-configuring.html)> Luettu 19.4.2019.
- 22 Juniperin dokumentaatio DHCP Snoopingin päällekytkemisestä <[http://www.juniper.net/documentation/en\\_US/junos13.2/topics/task/configuration/port-security-dhcp-snooping-cli.html](http://www.juniper.net/documentation/en_US/junos13.2/topics/task/configuration/port-security-dhcp-snooping-cli.html)> Luettu 19.3.2019.
- 23 Juniperin dokumentaatio Dynamic ARP Inspectionista <[https://www.juniper.net/documentation/en\\_US/junos/topics/task/configuration/understanding-and-using-dai.html](https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/understanding-and-using-dai.html)> Luettu 20.3.2019.

- 24 Juniperin dokumentaatio IP Source Guardista <[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/port-security-ip-source-guard.html](https://www.juniper.net/documentation/en_US/junos/topics/concept/port-security-ip-source-guard.html)> Luettu 20.3.2019.
- 25 Juniperin dokumentaatio Prefix-listoista <[https://www.juniper.net/documentation/en\\_US/junos/topics/example/policy-prefix-list.html](https://www.juniper.net/documentation/en_US/junos/topics/example/policy-prefix-list.html)> Luettu 22.3.2019.