Lappeenrannan-Lahden teknillinen yliopisto LUT
School of Engineering Science
Tietotekniikan koulutusohjelma

Diplomityö

Ilkka Virta

IP-TASON LIIKENTEEN YHDISTÄMINEN KÄYTTÄJÄÄN LÄHIVERKOSSA

Työn tarkastaja(t): Professori Jari Porras
Apulaisprofessori Ari Happonen

TIIVISTELMÄ

Lappeenrannan-Lahden teknillinen yliopisto LUT
School of Engineering Science
Tietotekniikan koulutusohjelma

Ilkka Virta

IP-tason liikenteen yhdistäminen käyttäjään lähiverkossa

Diplomityö 2020

45 sivua, 10 kuvaa, 3 taulukkoa

Työn tarkastajat: Professori Jari Porras
Apulaisprofessori Ari Happonen

Hakusanat: lähiverkko, IP-osoite, Ethernet-osoite, käyttäjän tunnistaminen
Keywords: Local area network, IP-address, Ethernet address, user identification

IP-pohjaisessa verkossa käytetyt osoitteet eivät suoraan yksilöi verkon käyttäjää. Joskus on kuitenkin hyödyllistä löytää tietyn liikenteen lähettäjä. Työssä tarkastellaan lähiverkko-pohjaisen verkon osoitteistusta sekä tarvetta ja tapoja verkko-osoitteen yhdistämiseksi sekä sitä käyttäneeseen laitteeseen, fyysiseen sijaintiin että loppukäyttäjään. Työssä toteutetaan työkalu verkon osoitetietojen keräämiseksi ja tarkastellaan myös aihetta koskevaa lainsäädäntöä ja muuta säännöstöä.

ABSTRACT

Lappeenranta-Lahti University of Technology LUT
School of Engineering Science
Degree Programme in Software Engineering

Ilkka Virta

Connecting IP Traffic with Owning User in a Local-Area Network

Master's Thesis 2020

45 pages, 10 figures, 3 tables

Examiners: Professor Jari Porras
Assistant Professor Ari Happonen

Keywords: Local area network, IP-address, Ethernet address, user identification

Network addresses used in an IP-based network do not inherently identify the end-user. In some situations, it is however useful to identify the traffic sender. This work reviews the addressing systems used in a LAN-based network, and the reasons and ways to connect the network address with the device, physical location, and end-user. A tool is implemented to collect the addresses used in the network, and the relevant legislation and other applicable directives are discussed.

ALKUSANAT

Kiitokset kaikille yliopiston ja AMK:n opiskelijoille kuluneista vuosista, sekä yliopistolle mielenkiintoisista mahdollisuuksista seurata yliopistomaailman kehittymistä.

Erityisesti kiitokset pelikerho Louhin ja Cafe Labran kävijöille, jotka ette varmastikaan ole opiskelujani edistäneet; Manalle henkisestä tuesta ja ymmärtämisestä; LOAS:lle laitteiston lainasta ja oppimismahdollisuuksista Lnet-verkon parissa; sekä Arille tämän ja kandityön ohjaamisesta.

Herttoniemessä, 5.6.2020
Ilkka Virta

SISÄLLYSLUETTELO

LYHENTEET

ARP	Address Resolution Protocol (IPv4:n tukiprotokolla)
ASN.1	Abstract Syntax Notation One
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol (IPv4-osoitteiden jakoprotokolla)
DHCPv6	Dynamic Host Configuration Protocol version 6 (IPv6 –vastine DHCP:lle)
DUID	DHCP Unique Identifier
HPE	Hewlett Packard Enterprise (mm. verkkolaitteita valmistava yritys)
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol (IP:n tukiprotokolla)
IETF	Internet Engineering Task Force
IP	Internet Protocol (verkkokerroksen yhteysprotokolla)
IPv4	Internet Protocol, versio 4
IPv6	Internet Protocol, versio 6
ISO	International Organization for Standardization
L1	Layer 1 (kerrosmallin ensimmäinen taso, fyysinen kerros)
L2	Layer 2 (kerrosmallin toinen taso, linkkikerros)
L3	Layer 3 (kerrosmallin kolmas taso, verkkokerros)
L4	Layer 4 (kerrosmallin neljäs taso, yhteyskerros)
L5	Layer 5 (kerrosmallin viides taso, sovelluskerros)
L7	Layer 7 (vaihtoehtoinen numerointi sovelluskerrokselle)
LAN	Local Area Network (lähiverkko)
LOAS	Lappeenrannan seudun opiskelija-asuntosäätiö
LTKK	Lappeenrannan teknillinen korkeakoulu
LUT	Lappeenranta University of Technology
MAC	Medium Access Control
MAN	Metropolitan Area Network
MIB	Management Information Base (SNMP:ssä)
ND	[IPv6] Neighbor Discovery [Protocol] (IPv6:n tukiprotokolla)
OID	Object Identifier (SNMP:ssä)
OSI	Open Systems Interconnection
RA	[IPv6] Router Advertisement

RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments (mm. Internet-protokollia määrittävä julkaisusarja)
SLAAC	[IPv6] Stateless Address Autoconfiguration (tilaton osoitekonfigurointi)
SNMP	Simple Network Management Protocol (verkkolaitt. hallintaprotokolla)
SMTP	Simple Mail Transport Protocol (sähköpostin siirtoprotokolla)
TCP	Transmission Control Protocol (yhteyskerroksen siirtoprotokolla)
UDP	User Datagram Protocol (myös yhteyskerroksen siirtoprotokolla)
VLAN	Virtual Local Area Network (virtuaalilähiverkko)
WAN	Wide Area Network
WLAN	Wireless Local Area Network (langaton lähiverkko)
WPA2	Wi-Fi Protected Access II (langattomien verkkojen salausprotokolla)

1 JOHDANTO

Tässä opinnäytetyössä tarkastellaan Internet-liikenteen takana olevan käyttäjän tunnistamiseen liittyvää problematiikkaa käyttäen tutkimusesimerkkinä Lappeenrannan seudun opiskelija-asuntosäätiön (LOAS) kampusverkkoa.

1.1 Tausta

Internetissä ja Internet-protokolliin perustuvissa verkoissa verkkoon liittyvät laitteet kommunikoivat keskenään käyttäen IP-protokollan (Internet Protocol) mukaisia verkko-osoitteita. Osoitteet eivät yleensä ole käyttäjäkohtaisia, vaan ne on jaettu lohkoittain verkkoa käyttäville organisaatioille. Siten yksistään verkko-osoitteen perusteella ei voida yksilöidä verkkoa käyttänyttä henkilöä. Yksityisyyden suojan kannalta tämä onkin toivottavaa, mutta joskus on tarpeen kyetä löytämään se käyttäjä, joka on tietystä verkkoliikenteestä vastuussa. Tällaisia tilanteita voivat olla ainakin haittaohjelmista aiheutuneen liikenteen lähteen tunnistaminen, muiden vikatilanteiden selvittäminen, tai erinäiset viranomaispyynnöt.

Tässä työssä selvitetään niitä teknisiä seikkoja, jotka liittyvät verkkoliikenteen haltijan selvittämiseen sekä yleisesti että erityisesti Lappeenrannan seudun opiskelija-asuntosäätiön (LOAS) kampusverkkoa Lnetiä käytännön esimerkkinä käyttäen.

1.2 Tavoitteet ja rajaukset

Työn tavoitteena on kehittää Lnetin käyttöön soveltuva työkalu, jolla voidaan selvittää, kuka verkon loppukäyttäjistä on käyttänyt tiettyä IP-osoitetta tiettyyn kellonaikaan. Samalla tarkastellaan osoitetietojen keräämiseen liittyviä säädöksiä, ja teorian tasolla vastaavan tiedon keräämistä muissa ympäristöissä. Laitekohtaisia ominaisuuksia käsittelevissä kohdissa työssä keskitytään saatavilla olleisiin Dell Networking N2048, Hewlett Packard Enterprise Aruba 2920 ja Cisco Catalyst 4500-X –laitteisiin. Lnet-verkossa pääosassa ovat kaapeloidut yhteydet ja IPv4, joten työssä keskitytään niihin. Langattomia yhteyksiä ja IPv6 -verkkoa käsitellään teoriatasolla.

1.3 Työn rakenne

Työssä on kuusi lukua, joista ensimmäinen on tämä johdanto. Toisessa luvussa käsitellään tarkemmin tarvetta tallentaa osoitetietoja, siihen liittyviä säädöksiä sekä Lnet-verkkoa toimintaympäristönä. Kolmannessa luvussa kuvataan lähiverkon eri protokollakerrosten osoitteita, osoitteiden jakoa, eri kerrosten liittymistä toisiinsa sekä tähän liittyviä protokollia. Neljännessä luvussa käsitellään varsinaisen käyttäjän identifiointia, ja viidennessä luvussa olemassa olevia vaihtoehtoja ja työkaluja edellä mainittujen tietojen konkreettiseksi keräämiseksi. Kuudennessa luvussa keskitytään varsinaisen työkalun toteutukseen, ja seitsemäs luku on yhteenveto, jossa tarkastellaan työn tuloksia.

2 TOIMINTAYMPÄRISTÖ JA TAUSTAA OSOITETIETOJEN TALLENTAMISESTA

Tässä luvussa esitellään lyhyesti LOAS:n Lnet-verkko, jonka rakenne asettaa kehyksen työn käytännölliselle osalle, sekä esitellään niitä tapauksia, joissa tietoja verkon käyttäjistä voidaan tarvita. Koska kyse on käyttäjien yksilöinnistä, tarkastellaan myös lyhyesti asiaa koskevaa lakia ja muita säädöksiä.

2.1 Taustaa Lnetistä

Lnet on Lappeenrannan seudun opiskelija-asuntosäätiön (LOAS) omistama tietoverkko, joka yhdistää säätiön opiskelija-asunnot Funet-verkon kautta Internetiin. Verkon tarkoituksena on tarjota säätiön asukkaille kohtuuhintaiset ja toimivat verkkoyhteydet keskitetysti.

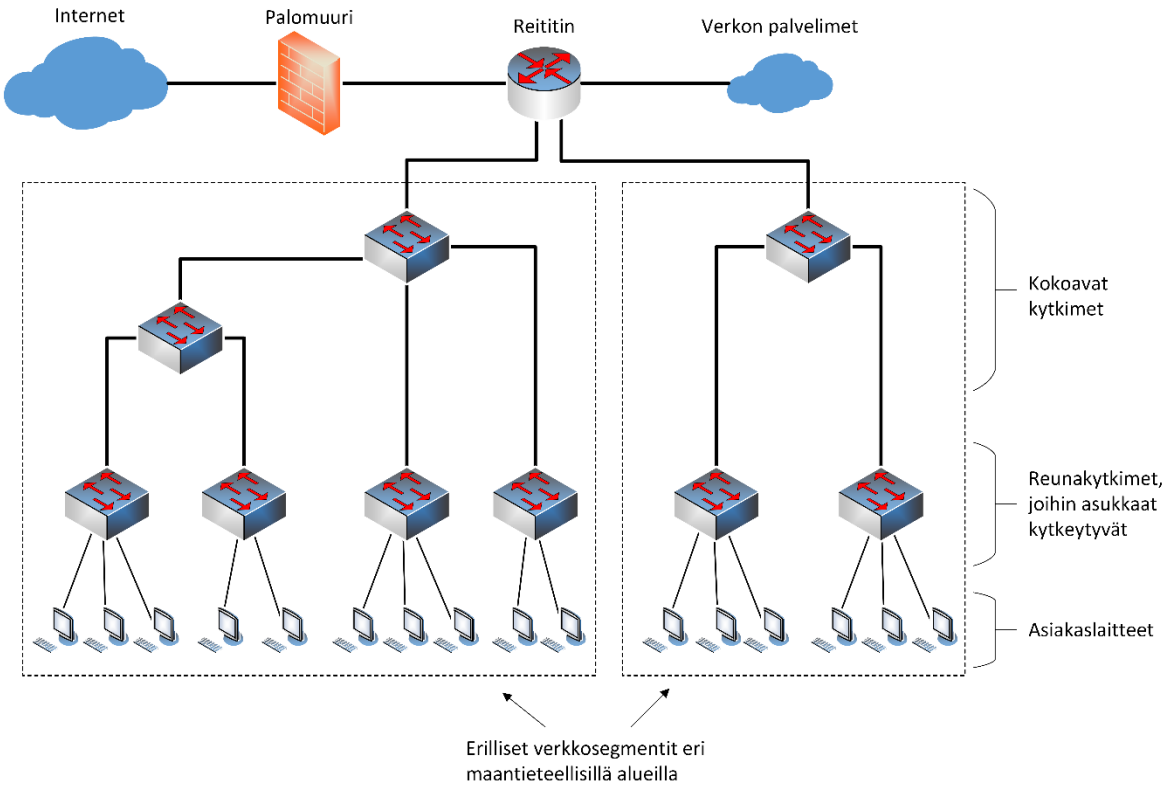
Lnet-verkon rakentaminen aloitettiin jo 90-luvun puolivälissä eräänlaisena teekkareiden harrastustoimintana, ja verkko toimi silloisen Lappeenrannan teknillisen korkeakoulun verkon osana. Alun perin verkkoon oli kytketty vain muutama lähinnä yliopistoa sijaitseva talo. 2000-luvun alkupuolella verkkoon oli kytketty jo pääosa LOAS:n asuntokohteista, ja vuonna 2007 verkko siirtyi pois yliopiston verkosta ja sai oman liittymänsä suoraan Funetiin. Vuoteen 2020 mennessä verkkoon on kytketty n. 80 rakennusta, jotka sijaitsevat Lappeenrannan keskusta-alueen ja Skinnarilan kaupunginosan välillä, pisimmillään n. 8 km etäisyydellä toisistaan.

Verkko on rakennettu lähiverkkotekniikalla, ja käyttää nykyisellään verkkokerroksella IPv4-protokollaa ja linkkikerroksella Ethernet-tekniikkaa. (Näistä enemmän luvussa 3). IP-protokollan uudempi versio IPv6 ei ole Lnetissä vielä käytössä, kuten se ei ole käytössä myöskään nykyisessä Lappeenrannan-Lahden teknillisessä yliopistossa[1]. Lnet-verkon osalta varsinaista tarvetta IPv6:n käyttöönottoon ei ole ollut Funetilta saatujen IPv4-osoitteiden vielä riittäessä. Yleisemmin syitä IPv6 –protokollan hitaaseen käyttöönottoon käsittelee

[1] Yliopiston nimi on muuttunut useamman kerran Lnet-verkon olemassaolon aikana. Yliopiston perustamisesta 1969 vuoteen 2002 asti sen nimi oli Lappeenrannan teknillinen korkeakoulu, 2003-2017 Lappeenrannan teknillinen yliopisto, ja 2018 lähtien ”Lappeenrannan-Lahden teknillinen yliopisto LUT”.

esim. Wahlman [43]. IPv6 –protokollan käyttö kasvaa kuitenkin koko ajan, joten myös sitä käsitellään tässä työssä mahdollisuuksien mukaan.

Verkkoteknisesti Lnet on jaettu maantieteellistä jakoa noudattaen viiteen verkkosegmenttiin ja erilliseen palvelinverkkoon, sekä niitä vastaaviin IP-aliverkkoihin, jotka kytkeytyvät toisiinsa ja ulkomaailmaan yhden reitittimen kautta. Pääosassa verkkoa asukkaille tarjottava yhteys on kaapeloitu lähiverkkoyhteys, mutta osassa rakennuksia tarjotaan sisäkaapeloinnin puuttuessa langattomia WLAN-yhteyksiä. Rakennusten väliset yhteydet ovat valokuitu-yhteyksiä. Kuva 2-1 esittää periaatteellisen kaavion verkon rakenteesta.



Kuva 2-1: Periaatteellinen kaaviokuva Lnet-verkosta

2.2 Tilanteet, joissa osoitetietoja tarvitaan

Verkkoliikenteen taustalla olevan käyttäjän tunnistaminen voi tulla tarpeeseen muutamassa eri tapauksessa. Näistä olennaisimpia ovat verkon vianselvitys, sekä mahdolliset viranomaiskyselyt. Seuraavassa aliluvussa tarkastellaan tarkemmin sitä, mihin tarkoituksiin tietoja on *luvallista kerätä*, tässä keskitytään vain siihen mihin tietoja *voidaan käyttää*.

Haittaohjelmat, väärin konfiguroidut tai vialliset laitteet voivat lähettää verkkoon muita verkkolaitteita häiritsevää liikennettä, jolloin ongelmallisen liikenteen lähde on voitava tunnistaa tilanteen korjaamiseksi. Periaatteessa tässä tapauksessa riittäisi paikallistaa laite verkkoteknisellä tasolla, koska tämän perusteella se voitaisiin sulkea verkosta. Kuitenkin mikäli laitetta käyttävän käyttäjän henkilöllisyys jäisi selvittämättä, ei olisi mahdollisuutta opastaa käyttäjää haittaohjelman poistamiseksi tai konfigurointivirheen korjaamiseksi. Myöskään ei olisi mahdollista edes ilmoittaa käyttäjälle verkkoliittymän sulkemisesta. Käyttäjän henkilöllisyyden selvittäminen on tässä tilanteessa siis vähintään ystävällistä.

Mahdollisen vikatilanteen selvitys voi lähteä myös käyttäjän aloitteesta. Mikäli käyttäjän verkkoliittymä ei toimi tai käyttäjä tarvitsee apua yhteyden käyttöönotossa, on hyödyllistä voida selvittää käyttäjän liittymän verkkotekninen sijainti, jotta voidaan tarkastella miltä osin yhteys toimii ja avustaa käyttäjää tämän perusteella. Tässä yhteydessä myös lokitiedot voivat olla hyödyllisiä, sillä niiden perusteella saatetaan havaita käyttäjän yhteyden toimintaan vaikuttaneita muutoksia.

Hieman erilainen tarve käyttäjän tunnistamiseen syntyy, jos ulkopuolinen taho vaatii tietoa verkon käyttäjästä. Käytännössä kyse on tällöin viranomainen, esim. poliisi, joka voi tarvita tietoja tutkinnallisista syistä. Viranomaisen kiinnostus ei todennäköisesti rajoitu pelkkään asiakaslaitteen verkkotekniseen sijaintiin, vaan myös käyttäjän henkilöllisyyteen. Ulkopuolisista tahoista myös eräät tekijänoikeuksien haltijoiden laskuun toimivat lakiasiaintoimistot voivat olla kiinnostuneita verkkoviestien lähettäjistä. Tässäkin tapauksessa tosin tietojen luovuttamiseen tarvitaan oikeuden päätös.

2.3 Viestien osoitetiedot säädöksissä

Ennen kuin lähdetään varsinaisesti keräämään osoitetietoja, saati luovuttamaan niitä eteenpäin, on tarpeen esittää katsaus siitä, miten lait ja muut säädökset säätelevät asiaa.

Laki sähköisen viestinnän palveluista (7.11.2014/917) lähtee siitä, että yleisesti vastaanotettavaksi tarkoitettua radioviestintää lukuun ottamatta sähköisiä viestejä ja niiden välitystietoja saa käsitellä vain viestinnän osapuolen suostumuksella, tai jos laki erikseen käsittelyn sallii. Tietojen käsittely on myös sallittua ainoastaan käsittelyn vaatimassa laajuudessa, ja tämän jälkeen viestit ja välitystiedot on joko hävitettävä tai anonymisoitava.

Mielivaltainen välitystietojen käsittely on siis yksiselitteisen kiellettyä. [10, 136-137 §] Myös Tietosuojalautakunta on päätöksessään vuonna 2006 katsonut, että IP-osoite (verkko-osoite) on pääsääntöisesti henkilötieto, ja Tietosuojalaki ja yleinen tietosuoja-asetus suhtautuvat henkilötietojen käsittelyyn myös varsin rajoittavasti [40]. Viestejä ja viestien välitystietoja on tietenkin lupa käsitellä viestinnän välittämiseksi, mutta tämä ei ole erityisen kiinnostavaa, sillä tällainen käsittely on välttämätöntä verkon toiminnan vuoksi. Verkkoliikenteen tapauksessa kyse on myös täysin automaattisesta käsittelystä, josta ei jää mahdollisia tilastotietoja kummempaa tallennetta.

Laki määrittelee verkon käyttäjiä seuraavasti: *teleyrityksellä* tarkoitetaan ”sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa”; *viestinnän välittäjällä”* teleyritystä, yhteisötilaajaa ja sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin”; ja *yhteisötilaajalla* ”viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja”. Lain asettamat määräykset teleyrityksille ovat huomattavan erilaisia kuin muille viestinnän välittäjille asetetut määräykset. LOAS on siis lain tarkoittamassa merkityksessä yhteisötilaaja ja viestin välittäjä, ei teleyritys. [10]

Yllä mainitun yleisen käsittelykiellon vastapainoksi laki sähköisen viestinnän palveluista antaa luvan viestien tai niiden välitystietojen käsittelemiseksi tarpeellisessa määrin muun muassa *tietoturvasta huolehtimiseksi* (138 §); *teknistä kehittämistä ja tilastollista analyysia varten* (142 §); sekä *teknisen vian ja virheen havaitsemiseksi ja selvittämiseksi* (144 §). Laki kuitenkin myös vaatii *teleyrityksiä* (mutta ei muita viestin välittäjiä) säilyttämään rikosten selvittämistä varten käyttäjän nimeä, osoitetta ja tietoa, jolla yksilöidä palvelun käyttäjä ja käytön ajankohta yhdeksän kuukauden ajan (157 §). [10] Viime mainitun pykälän vaatimus ei kuitenkaan vaikuta olevan EU-tuomioistuimen näkemyksien mukainen yksityisyyden suojan suhteen [5] [7] [9].

Edellä mainittua tietojen käsittelyä tietoturvan toteuttamiseksi laki määrittää vielä siten, että tässä tarkoituksessa on lupa käsitellä viestejä automaattisesti ja toisaalta teleyrityksen *tai muun viestintäverkon tai laitteen haltijan* on kyettävä tarvittaessa irrottamaan merkittävästi haittaa tai häiriötä aiheuttava laite verkosta. [10, 272-273 §] Myös Viestintäviraston määräys teletoiminnan tietoturvasta vaatii vastaavasti teleyritykseltä mahdollisuutta sulkea haittaa

aiheuttava liittymä verkosta [41, 15-16 §]. Viestintäviraston määräys tosin koskee vain *teleyrityksiä*, ja erikseen rajaa yhteisötilaajat määräyksen ulkopuolelle. Käytännössä lienee kuitenkin selvää, että Internetin globaalin toiminnan kannalta myös yhteisötilaajan olisi hyvä voida turvata verkon toiminta vastaavalla tavalla. Viestintäviraston määräys on myös teknisellä tasolla tarkempi kuin laki, ja sitä voitaneen pitää vähintään kuvauksena hyväksi havaituista teknisistä toimintatavoista.

Käytännön vianselvitystä varten osoitetietoja täytyy tallentaa vähintään jonkin aikaa, sillä ei voida olettaa, että mahdollisiin ongelmatilanteisiin voitaisiin poikkeuksetta puuttua häiriölähteen ollessa vielä verkossa. Tämä vaatisi jatkuvaa päivystystä myös viikonloppuisin ja juhlapyhinä, mikä taas vaatisi kohtuuttomasti resursseja. Myöskään ulkopuolisilta tahoilta tulevat ilmoitukset haittaliikenteestä eivät yleensä myöskään tule välittömästi, vaan havainnon käsittelystä ja edelleen välittämisestä syntyy tietty viive.

2.4 Yhteenveto

Yllä mainitun perusteella voidaan todeta, että on perusteltua tallentaa osoitetietoja vianselvitystä ja haittaliikenteen selvittämistä varten, mutta vain hyvin rajatusti. Näillä syillä ei voida perustella tietojen tallentamista kovin pitkäksi aikaa: mikäli ongelma ei johda toimenpiteisiin n. viikon tai kahden sisällä, on epätodennäköistä, että toimenpiteitä tarvitaan myöhemminkään. Tilanteen pitkittyessäkin vanhat osoitetiedot eivät ole relevantteja, kun tuoreempaakin tietoa on saatavilla. Sinänsä mielenkiintoista on se, että lain perusteella yhteisötilaaja ei edes saa tallettaa verkkoliikenteen osoitetietoja sen enempää viranomaisen suorittamaa rikostutkintaa kuin yksityisen lakiasiaintoimiston suorittamaa tekijänoikeus-valvontaa varten.

Käytännössä vikatilanteiden ja haittaliikenteen selvittämiseksi on siis voitava selvittää:

1. kuka käyttäjä käytti tiettyä verkko-osoitetta (IP-osoitetta) tiettyyn aikaan
2. mistä fyysisestä liittymästä tiettyä verkko-osoitetta käyttävä liikenne tuli, ja
3. mitkä fyysiset liittymät vastaavat käyttäjän asuntoa.

Seuraavissa luvuissa esitellään teknisellä tasolla verkko-osoitteita ja keinoja osoitetietojen keräämiseen, sekä käsitellään niiden soveltamista näitä tavoitteita silmällä pitäen.

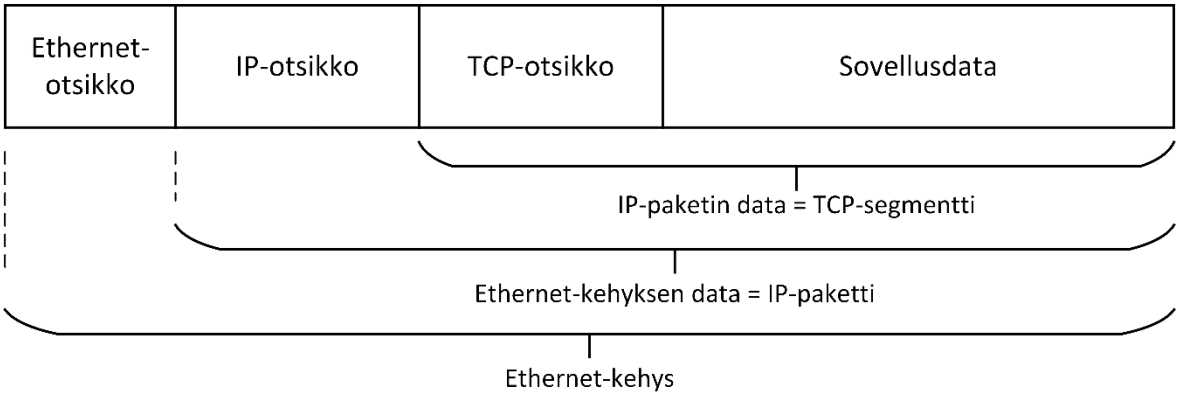
3 LÄHIVERKON OSOITTEET JA PROTOKOLLAT

Tässä luvussa esitellään verkkoliikenteeseen liittyviä teknisiä seikkoja, kuten eri viestintäprotokollia ja niiden muodostamaa kerrosmallia. Olennaisena osana tätä ovat verkon eri tasoilla käytettävät osoitteet, niiden suhde toisiinsa ja se miten verkon laitteet saavat osoitteensa.

3.1 Kerrosmalli

Internet-tyyppisissä verkoissa käytetyt protokollat on suunniteltu siten, että kukin protokolla toimittaa yhden tietyn tehtävän, käyttäen hyväksi muiden protokollien tuottamia palveluja, ja tarjoten omaa palveluaan muille protokollille. Näin eri protokollat muodostavat ikään kuin eri kerroksista koostuvan pinon, jossa abstraktimmat, ylemmän tason protokollat ovat päällä, ja laiteläheisemmät protokollat alla. Jokaisen tason protokollat lisäävät dataan omat ohjaustietonsa, jota alemman kerroksen protokollat kuitenkin käsittelevät vain datana, joka on kuljetettava seuraavaan pisteeseen muuttumattomana. Niiden ei siis tarvitse, eikä kuulu tietää ylemmän kerroksen toiminnasta mitään. Yleensä alemman tason otsikkotietoihin kuuluu kuitenkin jonkinlainen merkintä siitä minkä protokollan mukaista sisältöä sen sisällä on.

Näin muodostuneista kerrosmalleista tunnetuin lienee ISO:n (International Organization for Standardization) kehittämä OSI-malli (Open Systems Interconnection) [8]. Käytännön Internetissä käytetyt protokollat eivät kuitenkaan täysin vastaa OSI-mallin kerroksia, ja Internet-standardien mukaan onkin nimetty niitä vastaava TCP/IP –malli. [39] TCP/IP-mallin nimi tulee kahdesta yleisimmin käytetystä protokollasta: yhteyskerroksen TCP (Transmission Control Protocol), ja verkkokerroksen IP (Internet Protocol). TCP:n ohessa yhteyskerroksella käytetään myös huomattavasti yksinkertaisempaa UDP-protokollaa (User Datagram Protocol), joka tarjoaa vain mahdollisuuden yksittäisten pakettien lähettämiseen ilman varmuutta niiden perille saapumisesta, kun taas TCP tarjoaa pakettien rajoista riippumattoman loogisen ”putken” ja takaa viestien perille saapumisen. Kuvassa 3-1 on havainnollistettu TCP/IP-viestin rakenne ja eri kerrosten sisäkkäin sijoittuvien viestien suhde toisiinsa.



Kuva 3-1: TCP:n yli lähetetty datasegmentti IP- ja Ethernet- viestien sisällä

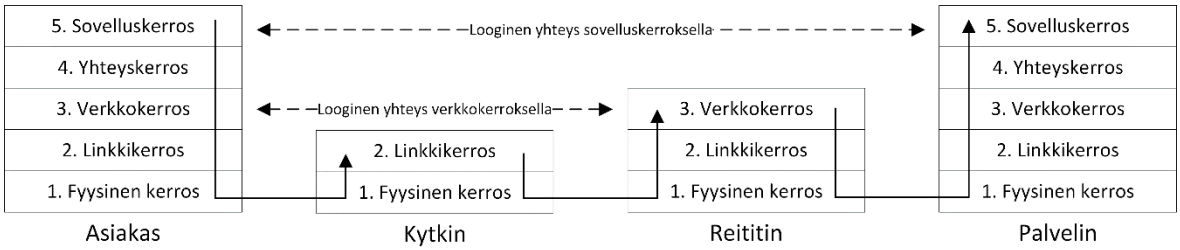
Kerrosten numerointi TCP/IP-mallissa ei ole täysin yksiselitteinen. Esimerkiksi erään kerrosmallin esittävä Internet-standardi RFC 1122 ei numeroi kerroksia lainkaan, ja yhdistää OSI-mallissa erilliset fyysisen ja linkkikerroksen yhdeksi [16]. Sen sijaan Stallings esittää fyysisen ja linkkikerroksen erillään, mutta ei myöskään erikseen numeroi niitä [38]. Tanenbaum esittää saman mallin numeroituna teollisuudessa poikkeuksetta käytettyyn tapaan siten, että Ethernet-kerros sijoitetaan kerrokselle 2 ja IPv4/IPv6 kerrokselle 3 [39]. Tällöin kerrosnumero 1 jää kuvaamaan fyysistä yhteyttä, mitä voidaankin pitää perusteltuna, kun otetaan huomioon esim. radiotien ja kaapeloitujen yhteyksien erot. OSI-malli sijoittaa sovelluskerroksen numerolle 7 ja siitä käytetään ajoittain tätä numeroa myös Internet-verkkojen yhteydessä siitä huolimatta, että OSI-mallin kerroksille 5 ja 6 ei ole vastaavuutta TCP/IP-mallissa. Tässä työssä käytetään Stallingsin ja Tanenbaumin mukaista mallia yllä mainitulla numeroinnilla. Malli on kuvattu taulukossa 3-1 seuraavalla sivulla.

Kerrosmallien eräänä tarkoituksena on, että tietyn kerroksen protokolla voidaan vaihtaa toiseen, ilman että vaihto suuremmin vaikuttaa muihin kerroksiin. Käytännössä verkkokerroksella on kaksi vaihtoehtoa: IP:n kaksi versiota, IPv4 ja IPv6. Samoin lähiverkkotekniikkaan perustuvat verkot käyttävät linkkikerroksella eli yksittäisen verkkosegmentin sisällä pääosin Ethernet-standardin mukaisia kehyksiä. Vaihtelua on lähinnä fyysisellä kerroksella, jolla voidaan käyttää mm. kuparikaapelia, erilaisia valokuituyhteyksiä, ja radioyhteyksiä eri tiedonsiirtonopeuksilla. Tässä työssä rajoitutaan tarkastelemaan Ethernet-protokollaa sekä IPv4- ja IPv6 –protokollia niiden yleisyyden vuoksi.

Taulukko 3-1: TCP/IP -kerrosmallin kerrokset ja niiden tehtävät

Kerros	Merkitys
L5 (L7): Sovelluskerros	Sovellusprotokollien oma liikenne, esim. DNS, HTTP, SMTP.
L4: Yhteyskerros	Looginen yhteyskanava kahden sovelluksen välillä, TCP- ja UDP-protokollat.
L3: Verkkokerros	Pakettiyhteys useamman verkon välillä, hierarkkinen verkkorakenne, reititys. IPv4- ja IPv6-protokollat.
L2: Linkkikerros	Pakettiyhteys verkkosegmentin sisällä, Ethernet-kehykset ja Ethernet-laiteosoitteet eli MAC-osoitteet.
L1: Fyysinen kerros	Fyysinen kaapelointi, liittimet, sähköinen signalointi, tai vastaavasti radiotien tai valokuituyhteyden ominaisuudet.

Kuvassa 3-2 on esimerkinomaisesti kuvattu viestin kulku eri kerroksilla esim. WWW-selaimelta WWW-palvelimelle kytkimen ja reitittimen kautta. Kytkin käsittelee viestiä vain linkkikerrokselle asti (kerros 2), kun taas reititin käsittelee sen myös verkkokerroksella (kerros 3). Verkkokerroksella on suora looginen yhteys asiakaslaitteen ja reitittimen välillä, eikä linkkikerroksesta tarvitse siinä välittää. Vastaavasti alemmat tasot eivät vaikuta sovellustason yhteyteen asiakkaan ja palvelimen välillä, vaan ainoastaan mahdollistavat viestinnän.



Kuva 3-2: Liikenteen kulku erilaisten verkkolaitteiden läpi

3.2 Verkko-osoite, laiteosoite, fyysinen rajapinta ja käyttäjä

Työn tarkoitusta varten on erotettava neljä erillistä asiaa:

- Verkkoa käyttävä henkilö, eli käyttäjä. Tunnistamistarkoituksessa varsinaisesti haluttu tieto.

- Fyysinen rajapinta johon käyttäjän laite kytkeytyy. Tämä voi olla esim. asuntoon vedetty kaapeli ja sitä vastaava portti lähimmässä aktiivilaitteessa, tai langattomassa verkossa laitteen käyttämä tukiasema. Kerrosmallin 1. kerros.

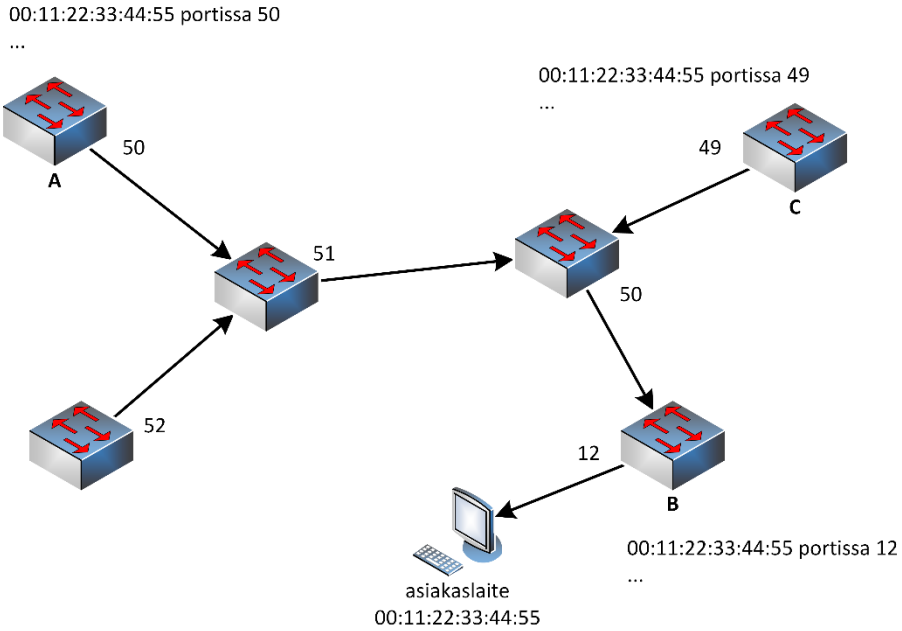
- Käyttäjän laitteen MAC-osoite (Medium Access Control), eli Ethernet-osoite tai laiteosoite, jolla laite liikennöi ja voidaan yksilöidä kytkinverkon sisällä. Kerrosmallin 2. kerros.

- Käyttäjän laitteen käyttämä verkko-osoite, jolla laite liikennöi ja voidaan yksilöidä Internetissä. Kerrosmallin 3. kerros.

Käyttäjän ja fyysisen rajapinnan määritelmät ovat selviä, mutta on paikallaan tarkentaa hieman Ethernetissä käytettävien MAC-osoitteiden ja verkkotasolla käytettävien IP-osoitteiden eroja.

Verkkosegmentin sisällä siihen liittyvät laitteet tunnistetaan laitekohtaisilla, tehdasasennetuilla MAC-osoitteilla. Osoitteet ovat 48-bittisiä ja ne esitetään tavallisesti heksadesimaalinumeroin, kuudessa kahden numeron ryhmässä, esim. 00:11:22:aa:bb:cc. Kunkin osoitteen alkuosa on valmistajakohtainen koodi, ja loppuosa valmistajan laitekohtaisesti jakama. Osoite toimii siis ikään kuin globaalina sarjanumerona ja yksilöi laitteen, jolle se kuuluu. Käytännössä useimmat verkkolaitteet sallivat kuitenkin MAC-osoitteen vaihtamisen ohjelmallisesti, ja esimerkiksi virtuaalikonealustojen on voitava käyttää eri MAC-osoitetta eri virtuaalikoneille. Siten MAC-osoitteet eivät toimi luotettavina tunnisteina pitkällä aikavälillä, mutta ne soveltuvat verkkoon liitetyn laitteen väliaikaiseen yksilöintiin. Pakettien välitys verkkosegmentin sisällä toimii MAC-osoitteiden perusteella siten, että paketin vastaanottaessaan kytkin merkitsee muistiin sen lähettäjäosoitteen sekä fyysisen liittymän, josta paketti saapui. Lähetettäessä paketteja eteenpäin ne ohjataan kohdeosoitteen perusteella siihen liittymään, jossa kyseisellä osoitteella on viimeksi

liikennöity. Yksittäinen kytkin tuntee siis vain seuraavan askeleen reitillä osoitetta käyttävälle laitteelle, mutta kytkinverkkoa kokonaisuutena tarkasteltaessa tiedot muodostavat suunnatun graafin kyseisen laitteen luo. Kuvassa 3-3 on esitetty periaatteellinen kytkinverkko, ja otteet kytkinten A, B ja C osoitetauluista. Kukin kytkin tuntee siis vain oikean suunnan laitteen luo, ei koko reittiä.



Kuva 3-3: Periaatekuva kytkinverkosta ja reiteistä tietyn asiakaslaitteen luo

Verkon toiminnan kannalta MAC-osoitteilla ei siis ole mitään hierarkiaa tai rakennetta, vaan mikä tahansa osoite voi sijaita verkossa missä tahansa ja kunkin kytkimen täytyy pitää kirjaa kaikista näkemistään osoitteista erikseen. Tähän käytettävissä olevan muistin määrä rajoittaa verkon kokoa: tavallisesti MAC-osoitetaulun koko on korkeintaan kymmeniä tuhansia[2], mikä sinänsä riittäisi isollekin yksittäiselle verkolle, mutta ei laajempaan käyttöön. (Käytännössä muut seikat rajoittavat yksittäisen verkkosegmentin kokoa vielä enemmän.)

Siirryttäessä yhdestä verkkosegmentistä eteenpäin, tarvitaan siis myös erilaiset osoitteet. Tätä varten verkkojen välillä ja koko Internetin laajuiseen liikennöintiin käytetään IP-osoitteita, joiden rakenne mahdollistaa hierarkkisen reitityksen. IPv4 -protokollassa osoitteiden pituus on 32 bittiä, ja ne esitetään neljällä desimaaliluvulla, esim.

[2] Esimerkiksi Dell Networking N2048 –kytkin pystyy tallentamaan 25600 MAC-osoitetta, ja Hewlett Packard Enterprise 2920 16000 MAC-osoitetta.

198.51.100.123. IPv6 -protokollassa osoitteet ovat 128-bittisiä, ja ne esitetään kahdeksan 16-bittisen heksadesimaaliluvun ryppäissä, esim. 2001:db8:0:0:1234:5678:90ab:cdef.

Molemmissa IP-protokollan versioissa osoite jaetaan kahteen osaan siten, että osoitteen alkuosa ilmaisee kokonaista verkkoa (osoitteen verkko-osa), ja loppuosa laitteita verkon sisällä (laiteosa). IPv6:n tapauksessa osoitteen laiteosalle lähes poikkeuksetta varataan osoitteen viimeiset 64 bittiä [23] [32], kun taas IPv4:n kohdalla laiteosan pituus voi vaihdella suurestikin [26]. Tämän jaon lisäksi myös eri verkkojen osoitteet ryhmittyvät vastaavasti hierarkkisesti. Verkkojen väliseen reititykseen ei kuitenkaan ole tässä yhteydessä tarvetta syvemmin perehtyä.

Käytännön verkkoliikenteessä tarvitaan sekä verkkosegmentin sisäisiä MAC-osoitteita, että verkkojen välisiä IP-osoitteita. Koko Internetin laajuinen liikenne onnistuu vain IP-osoitteilla, ja myös sovellustason rajapinnat on laadittu siten, että ne käyttävät IP-osoitteita. Verkkosegmentin sisällä viestin välitys perustuu kuitenkin pelkkään MAC-osoitteeseen, jolloin kaikkien laitteiden ei tarvitse kyetä käsittelemään IP-osoitteita ja niihin sisältyvää reititystä lainkaan.

3.3 Verkko-osoitteiden jako ja yhteys laiteosoitteisiin

Kun laite liittyy verkkoon, sillä ei itsessään ole kuin MAC-osoitteensa käytettävissään. Laitteen IP-osoite voidaan konfiguroida käsin, mutta varsinkin asiakaslaitteiden tapauksessa on tavallisempaa, että osoite konfiguroidaan automaattisesti. Tätä varten on omat protokollansa, jotka eroavat jonkin verran IP-protokollan kahden eri version välillä.

3.3.1 IPv4: DHCP ja ARP

IPv4:n tapauksessa tavallisin tapa jakaa verkko-osoitteita asiakaslaitteille on DHCP (Dynamic Host Configuration Protocol). DHCP:ssä verkkoon liittyvä laite lähettää yleislähetyksenä pyynnön saada verkko-osoitteen käyttöönsä, ja verkon haltijan hallinnoima DHCP-palvelin lähettää vastauksena tarjouksen käyttää tiettyä osoitetta tietyn aikaa ja merkitsee kyseisen osoitteen varatuksi kyseiselle laitteelle sen MAC-osoitteen perusteella. DHCP-vastaus sisältää myös muita verkon käyttöön tarvittuja tietoja, kuten verkon reitittimen IP-osoitteen, sekä nimipalvelinten IP-osoitteet. [18]

DHCP-palvelin hallitsee tässä siis täysin mitä verkko-osoitteita asiakaslaitteet käyttävät. Mikäli laitteelle on konfiguroitu verkko-osoite käsin, ei DHCP:tä tarvita, ja tällöin laite voi ohittaa DHCP-palvelimen noudattamat säännöt osoitteiden jaossa. Tämän estämiseksi ammattikäyttöön tarkoitetut kytkimet pystyvät seuraamaan DHCP:n jakamia osoitteita asiakasliittymän reunalla asti, ja estämään muiden kuin DHCP:n jakamien osoitteiden käytön (ns. ”DHCP snooping” -toiminto). DHCP määrää siis miten yksittäinen laite saa oman osoitteensa, mutta ei vielä auta löytämään muita verkossa olevia laitteita. Erityisesti DHCP kertoo ainoastaan verkon reitittimen IP-osoitteen, mutta ei sen MAC-osoitetta, joten liikennöinti reitittimen kanssa ei pelkästään DHCP:n välittämillä tiedoilla onnistu.

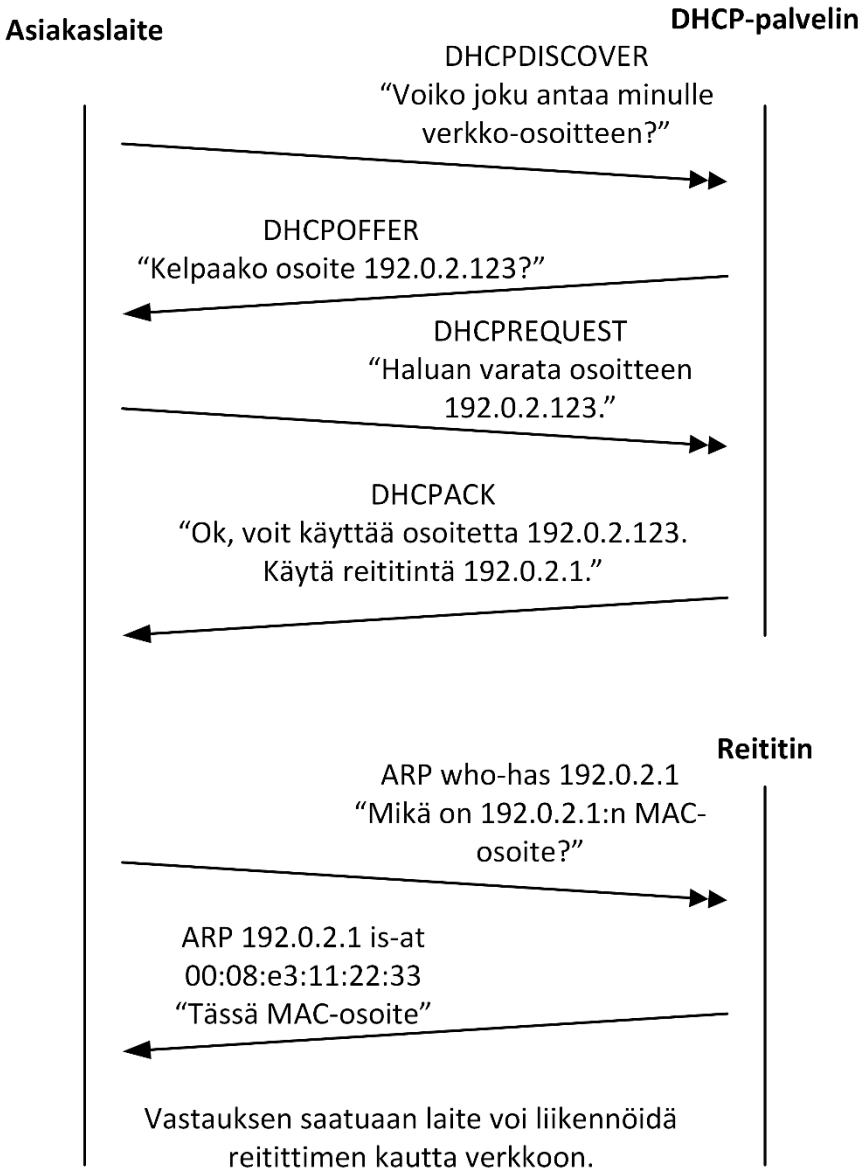
Reitittimen ja muiden laitteiden löytämiseksi verkkosegmentin sisällä käytettään ARP-protokollaa (Address Resolution Protocol). Myös ARP-kyselyt lähetetään yleislähetyksenä koko verkkosegmenttiin ja ne sisältävät yksinkertaisesti IP-osoitteen, jota vastaavan MAC-osoitteen lähettäjä haluaa tietää. Kyseistä IP-osoitetta käyttävä laite poimii kyselystä sen lähettäneen laitteen MAC-osoitteen, ja vastaa siihen kertoen samalla oman MAC-osoitteensa. Tämän viestinvaihdon jälkeen laitteet voivat kommunikoida keskenään. [15] [38, pp.595-596] Kuvassa 3-4 seuraavalla sivulla on esitetty DHCP- ja ARP-viestit asiakaslaitteen liittyessä verkkoon. Asiakkaan lähettämät, kaksoisnuolella merkityt viestit lähetetään yleislähetyksinä koko verkkosegmentille.

3.3.2 IPv6: SLAAC ja ND

IPv6:tta käyttävissä verkoissa osoitejako voidaan tehdä IPv4:n DHCP –protokollaa vastaavalla DHCPv6 –protokollalla, mutta tavallisempi tapa on käyttää ns. tilatonta autokonfigurointia (SLAAC, eli Stateless Address Autoconfiguration), jossa laitteet itse päättävät käyttämänsä osoitteen laiteosan. [29] Osoitteen verkko-osa ja reitittimen tiedot tulevat kuitenkin verkon reitittimeltä erityisellä Router Advertisement -viestillä (RA), eikä verkkoon liittyvä laite niitä voisikaan etukäteen tietää [28].

Alkuperäisessä muodossaan SLAAC käyttää laitteen MAC-osoitetta muodostamaan osoitteen laiteosan, mikä takaa ainutkertaiseen osoitteen kaikille verkkolaitteille. Tällöin MAC-osoitetta ei teoriassa tarvitsisi erikseen edes selvittää, vaan se voitaisiin päätellä suoraan IP-osoitteesta. MAC-osoitteen liittäminen koko Internetin laajuudella käytettävään IP-osoitteeseen on kuitenkin katsottu yksityisyyden suojan kannalta ongelmaksi, erityisesti koska tässä mallissa osoitteen laiteosa pysyy samana riippumatta siitä, mihin verkkoon laite

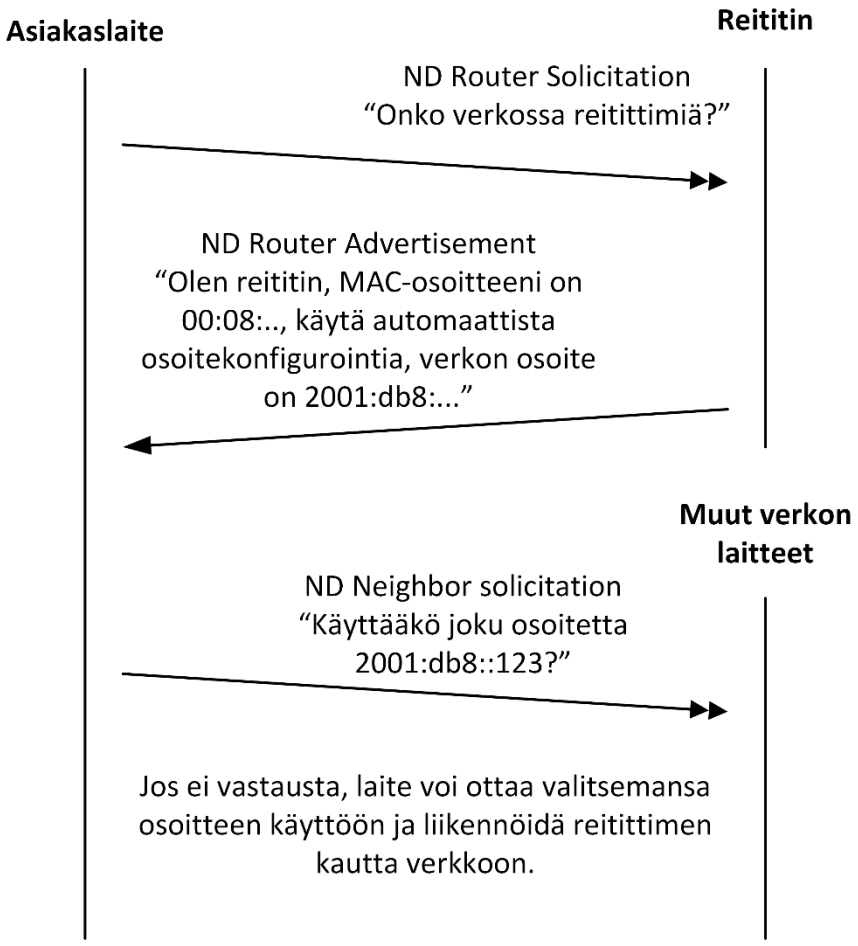
liittyy. [30] Tämän ongelman vuoksi nykyinen suositus on muodostaa osoitteen laiteosa pseudosatunnaisesti erikseen jokaiselle verkolle käyttämättä MAC-osoitetta suoraan [33], tai tämän lisäksi jopa vaihtaa osoitteen laiteosaa säännöllisesti [30]. Muutenkaan mikään ei voi teknisesti valvoa millä tavalla laitteet valitsevat osoitteen laiteosan, joten samaan tapaan kuin MAC-osoitteissa, niitä voidaan pitää pelkkinä tunnisteina ilman suurempaa merkitystä.



Kuva 3-4: Viestinvaihto IPv4-asiakkaan liittyessä verkkoon DHCP:tä käyttäen.

Koska IPv6-osoitteen laiteosa ei siis välttämättä ole sidottu laitteen MAC-osoitteeseen, tarvitaan jokin tapa selvittää muun verkossa olevan laitteen MAC-osoite liikennöintiä varten, samaan tapaan kuten IPv4 -verkossa. IPv6:n tapauksessa tämän toiminnallisuuden toteuttaa Neighbor Discovery -protokolla (ND). ND sisältää myös muita toimintoja, kuten

yllä mainitun reititintietojen välittämisen, mutta tältä osin se toimii jokseenkin samoin kuin ARP. IPv6:n Router Advertisement -viestit sisältävät kuitenkin myös reitittimen MAC-osoitteen, joten erillistä kyselyä ei sitä varten tarvita. Eräänä teknisenä erona ND:n ja ARP:n välillä on se, että ARP-kyselyt lähetetään yleislähetyksinä koko verkkosegmenttiin, kun taas ND perustuu multicast-viesteihin. Kuvassa 3-5 on esitetty ND-viestit asiakaslaitteen liittyessä verkkoon. Reititintiedot saatuaan laite tarkistaa käyttääkö jokin muu laite verkossa jo sen itselleen valitsemaa osoitetta (ns. Duplicate Address Detection, DAD). Tämä kysely lähetetään verkon muille asiakaslaitteille koska mitään keskitettyä osoitehallinta ei tilattomassa autokonfiguroinnissa siis ole. Reititinkysely ja päällekkäisen osoitteen tarkistusviesti lähetetään multicast-viesteinä. [28]



Kuva 3-5: Laite liittyy IPv6-verkkoon automaattista osoitekonfigurointia käyttäen

3.4 Laitteiden paikallistaminen verkossa

Kuten aiemmin luvussa 3.2 mainittiin, kytkinverkon laitteet muistavat havaitsemansa MAC-osoitteet ja fyysisen liittymän, josta kyseistä osoitetta käyttävä laite on liikennöinyt. Tämän tiedon perusteella myös verkon ylläpitäjä voi paikallistaa tiettyä MAC-osoitetta käyttävän laitteen aina fyysiseen liittymään asti. Paikallistamista vaikeuttaa hieman se, että sama MAC-osoite löytyy yleislähetysten myötä verkon jokaisen kytkimen osoitetauluista. Lopullisen asiakaslaitteen löytämiseksi täytyy erotella kytkinten portit joko portin tyypin, asetusten tai viime kädessä numeron perusteella kytkimiä yhdistäviin runkoportteihin ja loppukäyttäjille yhteyttä tarjoaviin asiakasportteihin. Verkkoa käyttävä laite voi näkyä jokaisen kytkimen runkoporteissa, mutta vain sen laitteen asiakasportissa, johon se on välittömästi kytketty. Etenemistä fyysisestä liittymästä varsinaiseen käyttäjään käsitellään seuraavaksi.

4 KÄYTTÄJÄN IDENTIFIOINTI

Edellisessä luvussa käsiteltiin verkkoon liittyvien laitteiden välistä liikennöintiä ja laitteiden sijainnin selvittämistä. Tässä luvussa käsitellään varsinaisen verkkoa käyttävän henkilön tunnistamista.

4.1 Kiinteästi kaapeloitu verkko ja paikkaan sidotut käyttäjät

Kampusverkon tapaisessa verkossa, jossa kiinteä kaapeli tuodaan asuntoon asti, on verkkoa käyttävän henkilön tunnistaminen verrattain suoraviivaista. Voidaan yksinkertaisesti olettaa, että liittymää vastaavan asunnon haltija (tai joku heistä) on myös verkon käyttäjä. Täsmälleen tämä ei pidä kaikissa tapauksissa paikkaansa, koska esim. asunnossa vieraileva henkilö voi myös käyttää asunnon verkkoyhteyttä. Käytännössä tällä ei kuitenkaan ole väliä, sillä asunnon haltijan voidaan olettaa tietävän keitä asunnossa on käynyt, ja viime kädessä vastaavan asunnossa verkkoon liitettävistä laitteista.

Toisaalta, mikäli asunnon verkkoliittymästä tarjotaan esim. avointa WLAN-palvelua, voi verkon käyttäjä olla lähes kuka tahansa. Tällöinkin voidaan esim. haittaliikenteen tapauksessa velvoittaa asunnon haltija estämään liittymän haitallinen käyttö liittymän sulkemisen uhalla.

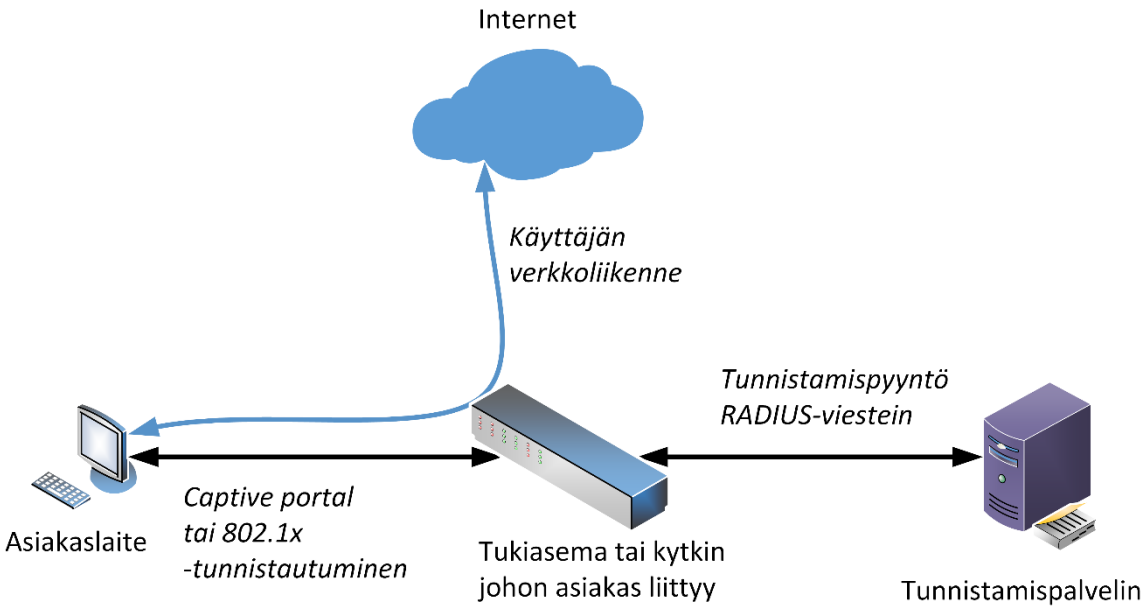
Verkkoon liitetyn laitteen verkkotekninen sijainti (asiakasportin numero) ei kuitenkaan vielä suoraan paljasta sitä vastaavaa fyysistä asuntoa, vaan tätä varten tarvitaan dokumentaatio verkon kytkennöistä. Kytkennät eivät luonnollisesti muutu yhtä usein kuin verkkoon kytketyt laitteet, joten pääosin dokumentaatio tarvitsee tehdä vain kerran. Dokumentaation laatiminen ja siirtäminen ohjelmallisesti käsiteltävään muotoon on kuitenkin erikseen tehtävä, ja merkintöjen ajantasaisuuden varmistamiseksi on merkintöjen päivittäminen oltava huomioituna kytkentämuutoksiin liittyvissä prosesseissa.

4.2 Langaton tai muu verkko, jossa käyttäjät liikkuvat

Verkossa, jossa käyttäjän fyysinen sijainti ei riitä yksilöimään käyttäjää, tarvitaan muita tapoja käyttäjän tunnistamiseen. Käytännössä tällöin tulevat kyseeseen erilaiset järjestelmät, joissa käyttäjä (tai tämän laite) tunnistautuu verkkoon aina yhteyden muodostuessa. Tällaisia ovat esim. 802.1x -protokollan mukainen tunnistautuminen, langattomien verkkojen

WPA2 (Wi-Fi Protected Access II) Enterprise ja erilaiset captive portal -järjestelmät X. Yhteistä näille kaikille on, että ne yleensä ulkoistavat varsinaisen tunnistamisen erilliselle palvelimelle, jolle viestitään RADIUS-protokollan (Remote Authentication Dial In User Service) avulla.

Tunnistamispalvelin saa yleensä käyttäjän antaman tunnuksen ja salasanan lisäksi verkkoon liittyvän laitteen MAC-osoitteen ja verkkoteknisen sijainnin. Näiden perusteella palvelin päättää sallitaanko käyttäjän pääsy verkkoon vai ei. Fyysistä sijaintia ei varsinaisesti tarvita käyttäjän tunnistamiseen henkilökohtaisia tunnuksia käytettäessä, mutta riippuen halutusta toimintalogiikasta, voidaan sitä tietysti käyttää osana pääsynhallintaa, esim. rajaamalla tietyn käyttäjäryhmän pääsy vain tiettyihin verkkoliittymiin. Tunnistautumisen jälkeen käyttäjän varsinainen verkkoliikenne ei enää kulje tunnistamispalvelimen läpi, vaan kytkin tai tukiasema johon käyttäjä liittyi, kuljettaa verkkoliikenteen eteenpäin pitkälti samaan tapaan kuin jos tunnistautumisvaihetta ei olisi. Kuva 4-1 esittää periaatteellisella tasolla 802.1x -tunnistautumisen.



Kuva 4-1: 802.1x -tunnistautuminen

Käyttäjäkohtaista tunnistautumista voidaan käyttää kaapeloidussakin verkossa, mutta sen ongelmana on tarve henkilökohtaisille käyttäjätunnuksille, sekä niiden luomisesta ja jakamisesta aiheutuva työ. 802.1x tarvitsee lisäksi erillistä ohjelmistotukea kaikilta verkkoon liittyviltä laitteilta ja vaikka yleisimmät käyttöjärjestelmät tukevatkin sitä, on kyse

melko harvoin kuluttajaverkoissa käytetystä ominaisuudesta. Varsinaisten tietokoneiden lisäksi myös esim. viihde-elektroniikka, kuten pelikonsolit ja televisiot saattavat kyetä hyödyntämään verkkoyhteyttä, mutta eivät välttämättä tue 802.1x:n kaltaista toimintoa.

Captive portal -ratkaisut taas eivät tarvitse erillistä käyttöjärjestelmätukea, mutta vaativat käyttäjän HTTP-liikenteen kaappaamista, jotta tämä voidaan ohjata kirjautumissivulle. Tämä aiheuttaa huonon käyttäjäkokemuksen ja ikäviä virheilmoituksia uudelleenohjattaessa salattua HTTPS-liikennettä, jota suurin osa WWW-liikenteestä nykyisin on. Lisäksi captive portal -ratkaisut eivät yleensä anna mahdollisuutta automaattiseen kirjautumiseen käyttäjän laitteille tallennetuilla tunnuksilla, jolloin käyttäjän täytyy jokaiselle verkkoon liittymiskerralla erikseen syöttää tunnuksensa. Myöskään captive portal-kirjautuminen ei välttämättä onnistu viihdelaitteilla.

Lnetissä aiemmin käytetty tunnistautumisjärjestelmä oli toteutettu captive portal -kirjautumisella, kuitenkin siten, että verkkoon liittyvän laitteen MAC-osoitteen ja fyysisen sijainnin säilyessä samana, oletettiin kyseessä olevan saman käyttäjän. Tällöin tunnistautuminen vaati toimenpiteitä käyttäjältä ainoastaan laitteen vaihtamisen tai siirtämisen jälkeen [11]. Järjestelmä oli kuitenkin herkkä verkon vikatilanteille, ja lisäksi selaimettomien pelikonsolien ja viihde-elektroniikkalaitteiden rekisteröiminen verkkoon oli epäkäytännöllistä. Näiden syiden vuoksi järjestelmästä luovuttiin vuonna 2017, minkä jälkeen verkossa ei ole käytetty käyttäjän tunnistamista.

5 VAIHTOEHDOT TIETOJEN KERÄÄMISEKSI

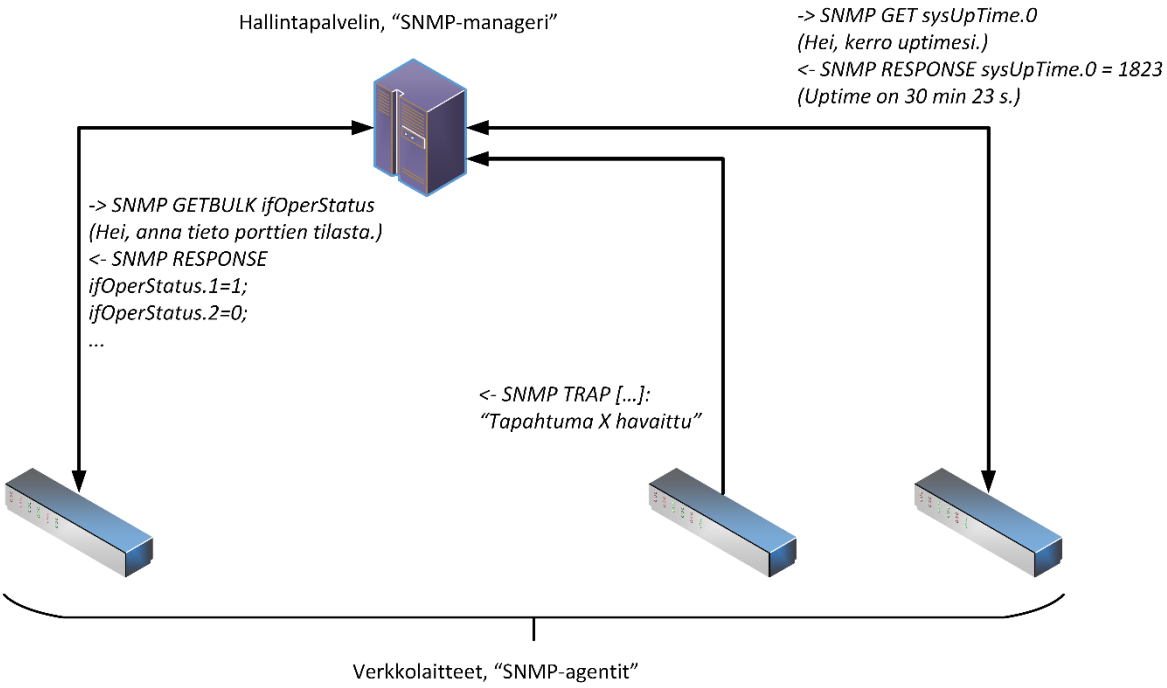
Aiemmissa luvuissa kuvattujen tietojen keräämiseksi on muutamia vaihtoehtoja. Verkkolaitteiden keräämiä tietoja voidaan hakea niiltä SNMP-protokollan avulla, tai voidaan tarkkailla verkon liikennettä ja poimia sieltä eri laitteiden käyttämiä osoitteita, tai käyttää DHCP-palvelimen tietoja jakamistaan osoitteista. Alla tarkastellaan näitä vaihtoehtoja ja niiden keskinäisiä eroja sekä teknisen toteutuksen että saatavilla olevien tietojen suhteen.

5.1 SNMP

SNMP-protokolla (Simple Network Management Protocol) tarjoaa standardoidun työkalun tietojen keräämiseen verkkolaitteista. SNMP:ssä verkkolaitteet (agentit) tarjoavat tietoja kyselevälle valvontaohjelmistolle (manageri) puumaisen tietorakenteen, jossa eri tiedot löytyvät tunnetuista paikoista. Puussa esiintyvät objektit tunnistetaan OID-tunnisteilla (Object Identifier), jotka esitetään tekstimuodossa pisteillä erotettuna sarjana lukuja (esim. 1.3.6.1.2.1.2.2.1.8). SNMP-viestien välittämiseen käytetään UDP-protokollaa, koska TCP:n vaatima yhteydenmuodostus olisi monien yksinkertaisten kyselyjen kohdalla tarpeettoman raskasta. SNMP:n käyttö tilastotietojen keräämiseen lienee selvästi yleisintä, mutta sen avulla voidaan myös rajatusti hallita verkkolaitteiden asetuksia. SNMP ei siis itsessään tarjoa varmuutta pyyntöjen perille saapumisesta, vaan managerin on huolehdittava uusintakyselyistä itse. Sen sijaan SNMP:n uusin versio SNMPv3 tukee autentikointia ja salausta, ja tätä mahdollisuutta onkin syytä käyttää ainakin konfigurointikäskyjä lähetettäessä. Tavallinen SNMP-liikenne ja tietokyselyt lähtevät aina managerin aloitteesta, agenttien vain vastatessa pyydetyillä tiedoilla. SNMP tarjoaa kuitenkin myös agenteille mahdollisuuden lähettää omaehtoisia ilmoituksia (ns. ”SNMP trap”) erityisistä tapahtumista. [37] Kuvassa 5-1 seuraavalla sivulla on havainnollistettu SNMP-liikennettä. Kuvan manageri pyytää kahdelta agentilta erinäisiä tietoja, ja saa kolmannelta pyytämättä ilmoituksen tietystä tapahtumasta.

SNMP:n tietopuu ja siinä esiintyvät tiedot määritellään ASN.1 -kuvauskieltä (Abstract Syntax Notation One) käyttävissä MIB-dokumenteissa (Management Information Base), jotka yleensä kuvaavat yksittäisen haaran puusta kerrallaan. MIB-dokumentit ovat koneellisesti tulkittavia ja esittävät sanalliset nimet puun kaikille solmuille, mikä helpottaa

käyttöä pelkkiin lukusarjoihin verrattuna. Nimen ja OID-tunnisteen lisäksi SNMP-objekteilla on myös tietotyyppi, joka voi olla paljas luku, monotonisesti kasvava laskuri, aikaa kuvaava arvo, merkkijono, tai IP-osoite. [37]



Kuva 5-1: Havaintokuva SNMP-managerin ja kolmen agentin välisestä liikenteestä

Useimpien olennaisten tietojen, kuten verkkolaitteiden portteja koskevien tilatietojen ja liikennelaskurien esitys on määritelty laitevalmistajariippumattomissa standardeissa, mutta puussa on myös valmistajakohtaisia haaroja. Joidenkin tietojen esittämistä on määritetty useammassa eri MIB-dokumentissa, valmistajakohtaisten erojen tai ajan myötä tapahtuneen kehityksen myötä. Tällöin tiedot voidaan joutua lukemaan laitekohtaisesti eri paikoista puuta, mutta olennaista on, että kunkin haaran ja MIB:n sisältämät tiedot ovat aina samat, ja eroa on vain siinä mitä puun haaroja laite tukee. Esimerkiksi alkuperäistä 32-bittistä laskuria käyttävää ”ifInOctets” -taulua (1.3.6.1.2.1.2.2.1.10) tukemaan on lisätty 64-bittistä laskuria käyttävä ”ifHCInOctets” -taulu (1.3.6.1.2.1.31.1.1.1.6) [20].

Yksittäisten objektien lisäksi SNMP tuntee tietotyyppinä kaksiulotteisen taulukon, jonka rivit vastaavat tiettyä loogista objektia, ja sarakkeet näistä objekteista esitettäviä tietoja. Esimerkki tällaisesta taulusta on verkkorajapinnan tietoja esittävä ifTable. Taulun sarakkeisiin kuuluvat mm. rajapinnan nimi (ifName), sen tilaa kuvaavat tiedot (ifAdminStatus ja ifOperStatus), sekä verkkolaitteen sisäinen tunniste rajapinnoille (ifIndex)

jota käytetään taulukon rivien indeksointiin. SNMP:n taulujen hieman erikoinen ominaisuus on siinä, että objektipuussa taulukoiden tiedot on järjestelty sarakkeittain, eikä riveittäin. Siten lukemalla tietty haara puusta voidaan saada esim. kaikkien verkkorajapintojen nimet, mutta tietyn rajapinnan kaikkien tietojen saamiseksi täytyy etsiä oikeaa rajapintaa vastaava indeksi, ja sen jälkeen lukea halutut tiedot erikseen kunkin sarakkeen alta. Esimerkiksi taulukon 5-1 (alla) esittämä kuvitteellinen ifTable -taulu vastaisi puumuodossa kuvan 5-2 (seuraavalla sivulla) mukaista puuta. Esimerkin vuoksi on esitetty vain pieni osa ifTable -taulun sisältämistä tiedoista. Myös yllä mainitut ifInOctets ja ifHCInOctets ovat taulukkojen ifTable ja ifXTable sarakkeita, eivätkä itsenäisiä objekteja. [37] [20]

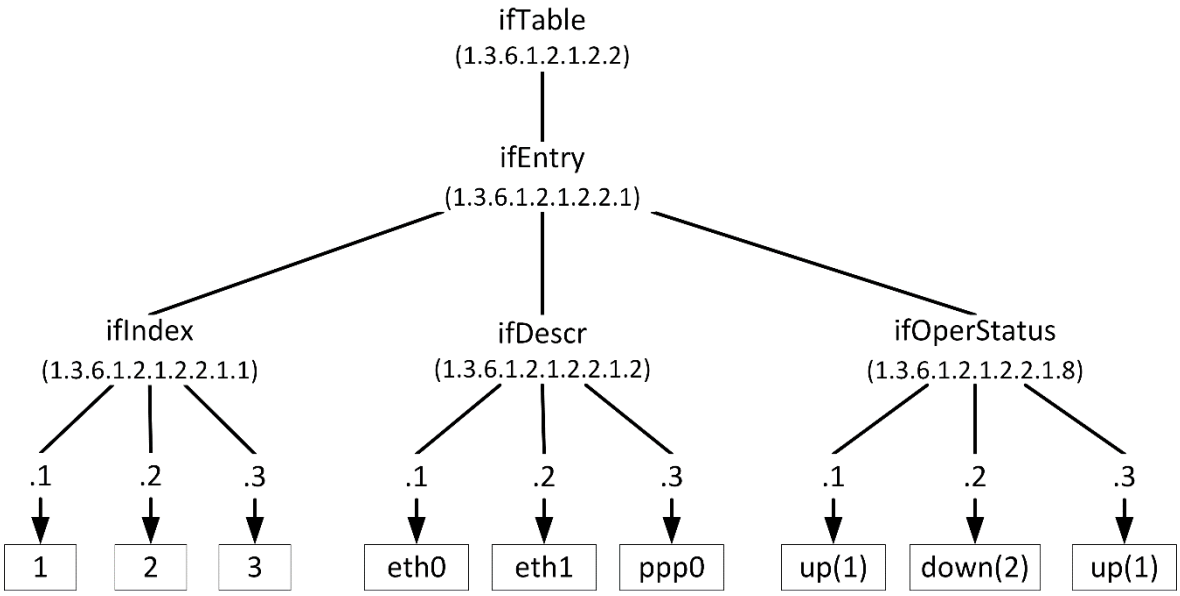
Useimmat kytkimet tarjoavat SNMP:n yli myös tiedot MAC-osoitetauluistaan, sekä tuntemistaan IP-osoitteista ja niitä vastaavista MAC-osoitteista (ARP- ja ND -protokolliin perustuvat tiedot). Molempien tietojen esitys vaihtelee hieman eri valmistajien kytkinten välillä.

Taulukko 5-1: Ote kuvitteellisen laitteen ifTable -taulusta

ifIndex	ifName	ifOperStatus
1	eth0	up(1)
2	eth1	down(2)
3	ppp0	up(1)

5.1.1 MAC-osoitetietojen kerääminen SNMP:llä

Standardoitu tapa MAC-osoitetaulujen esittämiseen on Q-BRIDGE-MIB -tietokanta, joka sisältää 802.1q -standardin mukaisia virtuaalilillähiverkkoja (VLAN, Virtual Local Area Network) koskevia tietoja. Tätä standardin mukaista esitystapaa noudattavat laitevalmistajista ainakin Dell Networking ja Hewlett Packard Enterprise. Q-BRIDGE-MIB sisältää taulun dot1qTpFdbTable, joka esittää MAC-osoitteet ja niitä vastaavat portit sekä osoitteen tilan indeksoituna VLAN-tunnisteella ja osoitteella. Taulun porttinumerot eivät välttämättä vastaa ifTable -taulun numerointia, vaan ne täytyy yhdistää alkuperäiseen BRIDGE-MIB:iin kuuluvan dot1dBasePortIfIndex -taulun tiedoilla. Mainitut taulut lukemalla saadaan melko helposti kerättyä kaikki kytkimen tuntemat MAC-osoitteet. [25] [22]



Kuva 5-2: Sama ifTable -taulu esitettynä puumuodossa

Muista laitevalmistajista poiketen Cisco Systems ei tue useimmissa laitteissaan Q-BRIDGE-MIB -tietokantaa, vaan tarjoaa hieman poikkeavan tavan kerätä vastaavat tiedot vanhempaa BRIDGE-MIB -tietokantaa käyttäen. BRIDGE-MIB ei tue virtuaalilähiverkkoja, joten Cisco on kehittänyt korvaavan tavan, jossa halutun VLAN:in numero upotetaan SNMP-kyselyssä käytettävään käyttäjätunnisteeseen (ns. *community string*). Lukuun ottamatta tätä eroa, BRIDGE-MIB tarjoaa vastaavat tiedot dot1dTpFdbTable -taulussa. [3] [4] (Taulujen nimien alkuosat viittaavat IEEE standardeihin 802.1d ja 802.1q, joista ensimmäinen määrittää kytkinverkkojen toimintaa ja jälkimmäinen erityisesti virtuaalilähiverkkoja.)

5.1.2 ARP- ja ND -tietojen kerääminen SNMP:llä

Verkkokerroksen IP-osoitteiden ja linkkikerroksen MAC-osoitteiden yhteyttä kuvaavia SNMP-tauluja on useita. Alkuperäinen IP-MIB määritteli esityksen vain IPv4 -osoitteille [17], ja IPv6 -osoitteita varten määritettiin erillinen IPV6-MIB [19]. Myöhemmin IP-MIB on päivitetty tukemaan sekä IPv4- että IPv6 -osoitteita [24], ja IPv6-osoitteille luotu erillinen taulu on erityisesti merkitty vanhentuneeksi [34]. Tuki uusimmalle IP-MIB määritykselle oli testatuissa laitteissa vaihtelevaa.

Kaikki testatut laitteet tarjosivat IPv4 -osoitteiden tiedot alkuperäisen IP-MIB:n mukaisessa ipNetToMediaTable -taulussa. Sen sijaan IPv6 -osoitteiden tietojen esityksessä oli vaihtelua. Dell-kytkimet tarjosivat IPv6-tiedot IPV6-MIB:n mukaisessa ipv6NetToMediaTable-

taulussa, kun taas sekä Ciscon että HPE:n laitteet esittivät vastaavat tiedot uudemman IP-MIB:n mukaisessa ipNetToPhysicalTable -taulussa. Kuitenkin vain HPE:n laitteet tarjosivat tässä taulussa sekä IPv4- että IPv6 -osoitteiden tiedot. SNMP:n avulla voidaan siis kerätä kaikista testatuista verkkolaitteista IP-osoitteita vastaavat MAC-osoitteet, mutta IPv6 -osoitteiden kohdalla tietojen keruussa täytyy huomioida laitteiden väliset erot.

5.2 Osoitteiden kerääminen verkkoliikennettä tarkkailemalla

Vaihtoehtoinen tapa osoitteiden keräämiseen on tarkkailla erillisellä ohjelmalla verkon liikennettä, eli ARP- ja/tai ND- viestejä. Kaikki verkossa liikennöivät laitteet joutuvat jollakin tapaa käyttämään näitä protokollia löytääkseen muiden laitteiden MAC-osoitteet, ja viestejä kuuntelemalla voidaan kerätä laitteiden osoitetietoja.

IPv4:n tapauksessa verkkoon liittyvät laitteet joutuvat lähettämään ARP-kyselyn vähintään löytääkseen verkon reitittimen MAC-osoitteen. Koska ARP-kyselyt välitetään yleis-lähetyksinä koko verkkosegmenttiin ja ne sisältävät myös kysyjän tiedot, voidaan näitä viestejä seuraamalla melko helposti kerätä kaikkien verkkosegmentissä olevien IPv4-laitteiden tiedot. IPv4:n ARP-liikenteen kuunteluun on olemassa ainakin *arpwatch* –niminen työkalu, joka löytyy valmiiksi paketoituna monille Linux–jakeluille [12].

IPv6:n tapauksessa laitteet saavat reitittimen MAC-osoitteen jo sen lähettämästä Router Advertisement (RA) –viestistä, joten erillistä kyselyä ei tarvita. Osoitteiden automaattista konfigurointia käytettäessä IPv6–laitteet kuitenkin lähettävät verkkoon kyselyn selvittääkseen käyttääkö jokin muu laite verkossa jo samaa osoitetta, ja näistä kyselyistä voidaan poimia käyttöön otetut osoitteet, joskin vain käyttöönoton hetkellä. Toisin kuin IPv4:n ARP –kyselyt, IPv6:n Neighbor Discovery –viestit lähetetään suoraan halutulle laitteelle, tai tämän ollessa tuntematon, multicast-viestinä sen osoitteesta muodostetulle ryhmälle, ns. Solicited Node -ryhmälle. Siten näiden kyselyjen ei pitäisi levitä kaikille verkon laitteille, mikä hankaloittaisi niiden kuuntelua. [28]

Solicited Node -multicast-ryhmiä muodostuu kuitenkin varsin lukuisia, ja niiden seuraaminen vaatisi verkon laitteilta kohtuuttomasti resursseja. Kaikki käyttöjärjestelmät eivät – määrityksen vastaisesti – edes lähetä viestejä Solicited Node -ryhmiin liittymisestä, joten ryhmiin kuuluvien laitteiden seuraaminen ei edes olisi mahdollista. Käytännössä

kytkinlaitteet eivät tämän vuoksi suodata ND-protokollaan liittyvien multicast-ryhmien liikennettä, vaan välittävät ne kaikille laitteille samaan tapaan kuin yleislähetykset. [14] [42] [44] IPv6:n ND-liikenteen kuunteluun on olemassa ainakin *ndpmon* ja *ndpwatch* -nimiset ohjelmistot [1] [13].

5.3 DHCP:n tietojen hyödyntäminen

Eräs DHCP-protokollan mielenkiintoisista ominaisuuksista on ns. Relay Agent Information –optio, jota käyttäen DHCP-kyselyjä välittävä laite voi lisätä viestiin tiedon siitä fyysisestä verkkoliittymästä josta kysely saapui [21]. Koska DHCP-palvelin saa IPv4:n tapauksessa myös tiedon asiakaslaitteen MAC-osoitteesta ja voi päättää minkä IP-osoitteen sille jakaa, olisi DHCP-palvelimella tällöin saatavilla kaikki tässä työssä tarvitut tiedot.

Vastaava toiminto on olemassa myös IPv6:n kanssa käytettävässä DHCPv6 –protokollassa nimellä Relay Agent Remote-ID [27], mutta ongelmana sen käytössä on se, että DHCPv6:ssa asiakaslaitteita ei tunnisteta MAC-osoitteilla, vaan asiakaslaitteen luomilla DUID –tunnisteilla (DHCP Unique Identifier), joiden sisältö voi vaihdella eikä niistä voida yleisesti päätellä mitään [35]. Alkuperäistä DHCPv6 –määritystä merkittävästi myöhempi RFC 6939 määrittää tosin tavan sisällyttää asiakaslaitteen linkkikerroksen osoite DHCPv6-viestiin, mutta tämä vaatii erillistä tukea DHCPv6-viestejä välittäviltä laitteilta [31], eivätkä esim. tässä testatut Cisco ja Dell-laitteet tue sitä. Toisaalta IPv6:n kanssa käytetään usein DHCP:n sijaan osoitteiden tilatonta autokonfigurointia, jolloin ei ole mitään DHCP-palvelimen kaltaista yksittäistä pistettä, joka tuntisi verkon kaikkien asiakaslaitteiden osoitteet.

DHCP:n saamien tietojen käyttäminen vaatii myös, etteivät asiakaslaitteet voi käyttää muita kuin DHCP:n tarjoamia osoitteita. Mikäli käyttäjä asettaisi laitteelleen IP-osoitteen kiinteästi, ei DHCP-palvelimella olisi tietoa siitä, ja käyttäjä jäisi seurannan ulkopuolelle. Tämän vuoksi ratkaisu vaatii, että verkon kytkinten on kyettävä sekä havaitsemaan verkossa kulkevia DHCP-viestejä, pitämään kirjaa kullekin asiakaslaitteelle myönnetystä IP-osoitteesta, sekä suodattamaan asiakaslaitteiden verkkoliikennettä siten, että vain liikennöinti DHCP-palvelimen myöntämillä osoitteilla on mahdollista. Nämä ominaisuudet ovat sinänsä toivottavia myös muista syistä, pääasiassa estämään asiakaslaitteita käyttämästä verkon reitittimen tai muiden tärkeiden laitteiden osoitteita, mutta niihin tukeutuminen vaatii luottamusta kytkinten suljetun ohjelmiston virheettömyyteen.

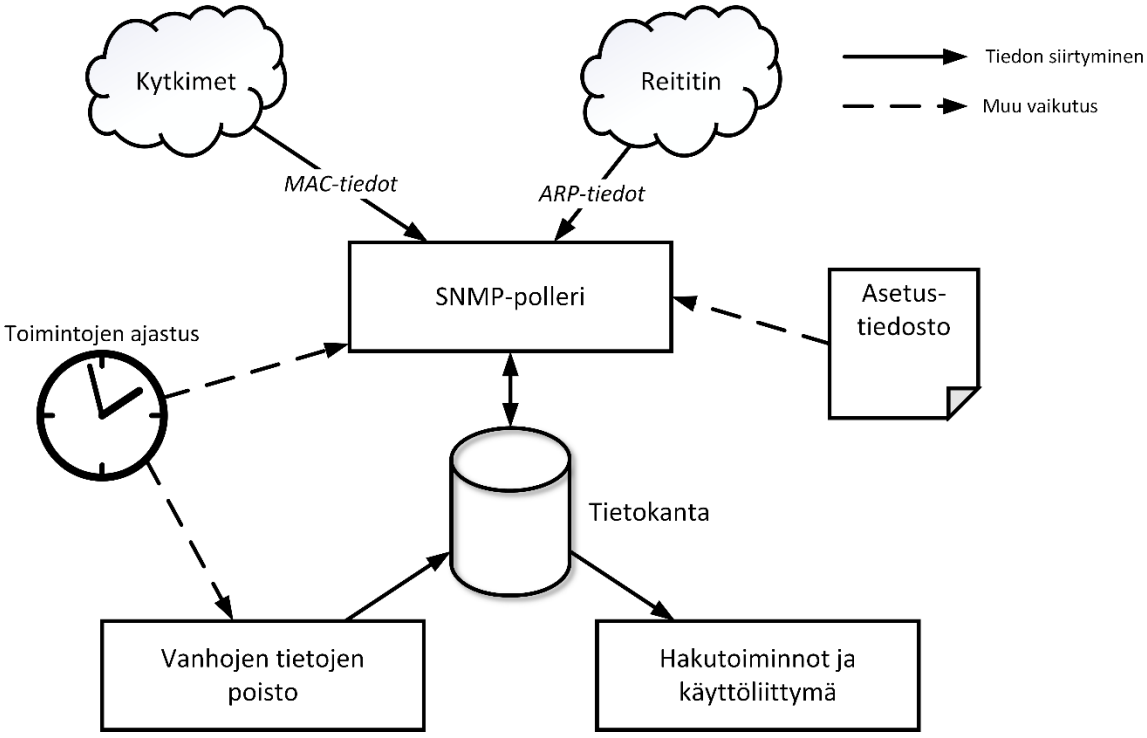
5.4 Yhteenveto

DHCP-palvelimen keräämien osoitetietojen käyttäminen on houkuttelevaa, mutta toimii vain DHCP:tä käyttäviin laitteisiin eikä sovellu erityisen hyvin IPv6-verkkoon. Sen sijaan tietojen kerääminen ARP- tai ND -viestejä kuuntelemalla tai verkkolaitteiden keräämiä ARP- ja ND-tietoja hyödyntämällä saadaan kaikkien verkossa liikennöivien laitteiden osoitetiedot. Kumpikaan näistä vaihtoehdoista ei myöskään vaikuta verkon normaaliin käyttöön mitenkään.

Pelkkien ARP- ja ND -tietojen perusteella ei kuitenkaan voida paikallistaa laitteita fyysisiin kytkinportteihin asti, vaan tätä varten täytyy joka tapauksessa kerätä verkon kytkinten MAC-osoitetaulut SNMP:llä. Kun tämä joudutaan kuitenkin tekemään, ei ole suuri työ kerätä myös ARP- ja ND -tietoja SNMP:llä ja SNMP:n käyttö tietojen keräämiseen vaikuttaa kokonaisuudessaan järkevimmältä. Tietojen keruu SNMP:llä on myös melko tavanomainen toimenpide, ja siihen löytyy sekä valmiita työkaluja että kirjastoja, joiden toimintaa on helppo arvioida. Sen sijaan ARP- ja ND-viestien kuuntelu verkosta on huomattavasti erikoisempi toimenpide, ja olemassa olevien työkalujen soveltaminen käsillä olevaan tarpeeseen voi vaatia muutostöitä.

6 TYÖKALUN TOTEUTUS

Työn yhteydessä toteutettiin prototyyppiluonteinen Python-työkalu, joka kerää SNMP:tä käyttäen verkon reitittimen keräämät ARP-tiedot sekä kytkinten MAC-osoitetaulut ja tallentaa ne hakuja varten. Työhön käytettävissä olevien resurssien rajallisuuden ja testaukseen sopivan IPv6-verkon puuttuessa toteutettiin IP-osoitteiden osalta tässä vaiheessa vain IPv4-osoitteiden keräys. Työkalun yleisluontoinen rakenne on esitetty alla kuvassa 6-1:



Kuva 6-1: Toteutetun työkalun rakenne

Työkalu käyttää SNMP-tietojen keräämiseen snimpy-kirjastoa, joka tarjoaa hyvin helppokäyttöisen tavan hakea SNMP-tietoja Python-ohjelmasta [2]. Verkon kytkimiltä luetaan aiemmassa luvussa mainituista dot1qVlanFdbPort ja dot1dBasePortIfIndex -tauluista kytkimen MAC-osoitetaulu ja osoitteita vastaavat porttinumerot, sekä dot1qPvid- ja ifName -taulut porttien ns. primääri-VLAN:n ja nimen selvittämiseksi. Tietoa porttien primääri-VLAN:eista käytetään erottamaan kytkimen runkoyhteyksien portit havainnoinnin kohteena oleviin VLAN:eihin liitetyistä tavallisista asiakasporteista. Reitittimeltä kerätään vain ipNetToMediaPhysAddress -taulun sisältämät tiedot IP- ja MAC-osoitteiden yhteyksistä. Tiedon tallentamiseen käytetään SQLite-tietokantaohjelmistoa, koska SQL-kieli tarjoaa yksinkertaisen ja laajennettavan tavan tallennettavan tiedon rakenteen

kuvaamiseen, mutta SQLite itse on silti varsin kevyt ja soveltuu myös pienten datamäärien tallentamiseen [6].

Työkalu on suunniteltu keräämään tiedot ajastetusti muutaman minuutin välein esim. cron-sovelluksen avulla. Tietojen hakutahti tulee säätää siten, että se on yhtä pitkä tai hieman lyhyempi kuin aika jonka reititin ja kytkimet säilyttävät tietoja. Useimmat kytkimet unohtavat havaitsemansa laitteet 300 sekunnin (5 minuutin) kuluttua, jolloin tietojen haku olisi hyvä tehdä 4 tai 5 minuutin välein. Koska suurimmassa osassa tapauksia verkkoon kytkeytyvä laite on kytkeytyneenä huomattavasti tätä pidemmän ajan, usein tunteja tai päiviä yhtä mittaa, tallennetaan samanlaisina pysyneet tiedot vain kerran niiden ensimmäisen ja viimeisimmän havaintoajan kera.

Tietojen tallentamisessa päädyttiin yhdistämään verkkoa käyttävän laitteen IP- ja MAC-osoitteet sekä fyysinen sijainti skannaushetkellä ja tallentamaan kokonaisen ”verkkoistunnon” tiedot yhtenä rivinä tietokantaan. Periaatteessa yhtä MAC-osoitetta voi kuitenkin vastata useampi IP-osoite samaan aikaan, joten mainittu ratkaisu ei ole tietokantamallin kannalta normaalimuotoinen. IPv4-verkossa on kuitenkin tavallisinta, että yksittäinen laite käyttää vain yhtä verkko-osoitetta kerrallaan, jolloin kenttien erottaminen toisi tarpeetonta toistoa erityisesti osoitteiden havaintoajoissa. SQL-kieli ja käytännön SQL-toteutukset eivät myöskään tarjoa erityisen hyviä työkaluja aikavälien käsittelylle, jolloin erillään tallennettujen tietojen voimassaoloaikojen vertailu tekisi kaikista hakulauseista tarpeettoman monimutkaisia. Ajan käsittelyn vaikeutta SQL-tietokannoissa käsittelee enemmän esim. Snodgrass [36]. Verkkolaitteilta kerättyjen tietojen lisäksi tallennetaan myös tiedot verkon fyysisistä kytkennöistä. Nämä tiedot on luonnollisesti kerättävä manuaalisesti, mutta niistä tallennetaan myös kytkentöjen olemassaoloaika.

6.1 Työkalun testaus

Työkalua testattiin kytkemällä se tarkkailemaan erään asukasverkon laitteita ja Lnet-verkon reititintä. Testatun verkon laitteina oli 16 kpl Dell Networking N2048 -kytkimiä, sekä Cisco Catalyst 4500-X -reititin. Toimintaa arvioitiin kytkemällä testilaitteita verkkoon tarkoituksellisesti ja varmistamalla niiden tietojen kirjautuvan oikein, sekä myös tarkastelemalla verkon muusta liikenteestä kerättyjä tietoja yleisesti ennalta

odottamattomien havaintojen varalta. Testitapaukset ja niiden tulokset on esitetty alla taulukossa 6-1.

Taulukko 6-1: Verkon osoitteita valvovan työkalun testitapaukset

Testitapaus	**Toivottu tulos**	**Tulos**
A. Laite liittyy verkkoon normaalisti käyttäen DHCP:tä	Työkalu havaitsee laitteen osoitetiedot ja kirjaa uuden istunnon alkaneeksi	ok
B. Laite poistuu verkosta	Työkalu havaitsee laitteen poistuneen ja kirjaa istunnon päättyneeksi	ok
C. Laite liittyy verkkoon käyttäen kiinteää IP-osoitetta	Työkalu havaitsee laitteen osoitetiedot kuten tapauksessa A	ok
D. Laite liittyy verkkoon, mutta ei lähetä IP-liikennettä	Työkalu havaitsee laitteen MAC-osoitteen kytkinportissa	ok
E. Laite liittyy verkkoon ja käyttää useaa IP-osoitetta	Työkalu havaitsee molempien osoitteiden tiedot	ok
F. Laite liittyy verkkoon ja liikennöi, mutta poistuu verkosta nopeasti	Työkalu havaitsee laitteen tiedot kuten tapauksissa A ja B	x (kts. teksti)

Tavanomaisimmissa tilanteissa (testitapaukset A, B ja C) työkalu toimi odotetusti ja havaitsi verkkoon normaalisti liitetyn testilaitteen seuraavalla tiedonhakuajolla. Ajastettuun tiedonlataukseen perustuva työkalu ei tietenkään voi havaita verkkoon liittymisen tarkkaa hetkeä, ja tämä tulee ottaa tietoja tulkittaessa huomioon. Myös hieman poikkeavammat tilanteet, joissa laite liikennöi useammalla IP-osoitteella tai ei käyttänyt IP-liikennettä lainkaan (tapaukset D ja E), tallentuivat toivotulla tavalla. Testilaitteilla tietojen haku kesti n. 8-10 sekuntia, mistä pääosa kului SNMP-kyselyjen vastausten odottamiseen, varsinaisen prosessoinnin ollessa hyvin nopeaa. Koko verkon n. 100 laitteen tietojen keruu kestäisi näin ollen noin minuutin.

Osoitetietojen hakeminen ajastetusti kiinteällä aikataululla aiheuttaa kuitenkin erään ongelmakohdan. Fyysisen linkin sammuessa verkkokytkimet tyhjentävät kyseisen portin osoitetaulun välittömästi, tavallisesta tietojen säilytysajasta riippumatta. Mikäli verkkoon liittyvä laite poistuu verkosta ennen seuraavaa tiedonhakukierrosta (testitapaus F), jää näin

ollen sen fyysinen sijainti havaitsematta. Verkon reititin ei kuitenkaan saa tietoa linkin sammumisesta, ja reitittimen ARP-taulusta saadaan tallennettua laitteen käyttämät IP- ja MAC-osoitteet. Tällainen tilanne on kuitenkin normaalikäytössä harvinainen, ja vaikka ongelma on verkon kattavan seurannan kannalta valitettava, sitä on vaikea korjata muuttamatta työkalun arkkitehtuuria merkittävästi. Lyhytaikaisesti vierailevien laitteiden tietoja voitaisiin kerätä joko DHCP:n antamia tietoja hyödyntäen (kts. luku 5.3), tai muuttamalla työkalun toimintalogiikkaa siten, että verkon kytkinten osoitetaulut luettaisiin säännöllisen ajastuksen lisäksi aina kun verkossa havaitaan uuden laitteen liikennettä. Osoitehaun laukaisijana toimisi tällöin joko verkkoliikennettä tarkkailemalla tehty havainto (kts. luku 5.2), tai verkkolaitteiden lähettämä SNMP trap -viesti.

6.2 Työkalun jatkokehitys

Työkalun jatkokehityksen kannalta olennaisin kohde olisi varmastikin nykyistä prototyyppiluonteista komentorivikäyttöliittymää helppokäyttöisempi, esim. web-pohjainen käyttöliittymä sekä hakutoiminnoille että kytkentäkarttojen ylläpitoon. Työkalun yleiskäyttöisyyttä parantaisi tuki Cisco-kytkinten omalle tavalle esittää MAC-osoitetaulujen tiedot, sekä tulevaisuutta varten IPv6 -osoitetietojen kerääminen. Myös langattoman verkon käyttäjien tietojen keräämistä RADIUS-palvelimelta tulisi

Mikäli aivan kattavaa verkon valvontaa pidetään tarpeellisena, tulisi puuttua myös edellä mainittuun puutteeseen nopeasti verkossa vierailevien laitteiden havaitsemisessa. Tämä vaatisi kuitenkin merkittäviä muutoksia työkalun rakenteeseen. IPv4 -verkossa voitaisiin käyttää DHCP-palvelimella olevia tietoja, mahdollisesti mukaan lukien Relay Agent -tiedot asiakkaan fyysisestä sijainnista. Ilman Relay Agent -tietoja tulisi osoitetietojen haku voida laukaista asynkronisesti tarvittaessa, ja tällöin olisi pidettävä huolta siitä, ettei hakukierroksia ajeta päällekkäin tai muuten verkon kuormituksen kannalta liian usein. Verkon liikennettä seuraamalla voitaisiin myös havaita sekä IPv4- että IPv6 -laitteet niiden kommunikoidessa verkossa. Työkalun rakenteen kannalta tämä sisältäisi olennaisesti samat haasteet kuin DHCP-palvelimen tietojen hyödyntäminen.

Kolmas mahdollinen tapa saada reaaliaikaisempaa tietoa verkon laitteista olisi kytkinten tarjoamien SNMP trap -ilmoitusten hyödyntäminen. Tämä vaatisi toiminnon konfigurointia kytkimiin, sekä SNMP-viestejä kuuntelevaa moduulia hallintatietokoneelle. Useat kytkimet

tarjoavat ainakin mahdollisuuden saada SNMP-ilmoitukset kytkinporttien linkin tilan muuttumisesta. Fyysisen linkin tilan muuttuminen ei kuitenkaan ole sama asia kuin uuden laitteen liittyminen verkkoon, koska yhden portin takana voi olla useita laitteita. Muiden tietojen saatavuuteen SNMP-ilmoituksilla tulisi perehtyä syvemmin, jotta tästä menetelmästä voitaisiin saada merkittävää hyötyä.

Työssä keskityttiin pääosin tietojen hakemiseen verkon laitteilta SNMP:n avulla ja verkkolaitteet tarjoavat SNMP:llä paljon muitakin tietoja, muun muassa verkon liikennemääristä ja linkkien tilasta. Tällaisten tietojen kerääminen on hyödyllistä lähes kaikissa verkoissa, ja työkaluja siihen on runsaasti. Yleiskäyttöiset työkalut eivät kuitenkaan välttämättä sovellu paikallisiin tarpeisiin, ja esimerkiksi tässä työssä mainitut tiedot asuntojen ja kytkinten välisistä kytkentäkartoista voitaisiin haluttaessa yhdistää verkon liikennemääriin ja muodostaa tilastoja verkon käytöstä asuntokohtaisesti.

7 YHTEENVETO

Työssä tarkasteltiin tarvetta käyttäjän tunnistamiseen verkko-osoitteen (IP-osoitteen) perusteella lähiverkkotekniikalla rakennetussa verkossa, ja tähän liittyvää problematiikkaa ja säädöstöä. IP-osoite itsessään ei suoraan yksilöi käyttäjää, mutta käyttäjän tunnistaminen voi olla tarpeen verkon valvontaan ja vianselvitykseen liittyvissä tarkoituksissa. Kiinteästi kaapeloidussa verkossa IP-osoite voidaan yhdistää verkkoa käyttävän laitteen laiteosoitteeseen (Ethernet-osoite, MAC-osoite), ja sitä kautta fyysiseen sijaintiin, joka riittää käyttäjän tunnistamiseen. Tiedot verkossa liikennöivistä laitteista ja niiden käyttämistä osoitteista voidaan kerätä joko verkon laitteilta SNMP-hallintaprotokollaa käyttäen; kuuntelemalla laitteiden liikennöintiä verkossa; tai käyttämällä IP-osoitteita jakavan DHCP-palvelimen tietoja. Vaihtoehtoisesti voitaisiin käyttää jonkinlaista kirjautumisjärjestelmää, mikä onkin myös langattomissa verkoissa käytännössä ainoa tapa käyttäjien tunnistamiseen.

Työssä toteutettiin työkalu sekä IP- että MAC-osoitetietojen keräämiseksi ajastetusti SNMP-protokollalla tavanomaisilta ammattikäyttöön tarkoitetuilta hallittavilta kytkimiltä ja reitittimiltä. Työkalua testattiin Dell Networking -kytkimillä ja Cisco Catalyst -reitittimellä, ja sen todettiin toimivan tavallisimmissa tilanteissa hyvin. Varaa kehitykselle on vielä erityisesti IPv6-verkkojen ja Ciscon SNMP-toteutuksen erityispiirteiden tukemiseksi.

LÄHTEET

[1] Beck, Frederic et al; Neighbor Discovery Protocol Monitor (NDPMon), http://ndpmon.sourceforge.net/ ; viitattu 2020-05-28

[2] Bernat, Vincent et al; Snimpy: interactive SNMP tool, https://snimpy.readthedocs.io/en/latest/ ; viitattu 2020-05-28

[3] Using SNMP to Find a Port Number from a MAC Address on a Catalyst Switch, Cisco Systems 2005-10-26, https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/44800-mactoport44800.html ; viitattu 2020-05-29

[4] SNMP Community String Indexing, Cisco Systems 2005-10-26, https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/40367-camsnmp40367.html ; viitattu 2020-05-29

[5] Court of Justice of the European Union, The Members States may not impose a general obligation to retain data on providers of electronic communications services, 2016-12-21; saatavilla https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf

[6] Hipp, D. Richard et al; SQLite As An Application File Format, https://www.sqlite.org/aff_short.html ; viitattu 2020-05-28

[7] Helsingin sanomat: EU:n tuomioistuin: Valtiot loukanneet yksityisyyden suojaa internetissä – ratkaisulla vaikutuksia myös Suomeen, 2016-12-21; https://www.hs.fi/ulkomaat/art-2000005016509.html ; viitattu 2020-06-01

[8] ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model

[9] Kari, Jussi; Tappoiko EU-tuomioistuin tekijänoikeuskirjeet? ; 2016-12-22, http://www.jussikari.fi/tappoiko-eu-tuomioistuin-tekijanoikeuskirjeet/ ; viitattu 2020-06-01

[10] Laki sähköisen viestinnän palveluista (7.11.2014/917) http://finlex.fi/fi/laki/ajantasa/2014/20140917; viitattu 2020-06-04

[11] Luoto, Sauli; Käyttäjä- ja laiterekisteröinti kampusverkossa, diplomityö. Lappeenrannan teknillinen yliopisto, 2010

[12] Lawrence Berkeley National Laboratory Network Research Group, https://ee.lbl.gov/ ; viitattu 2019-11-05

[13] Lecigne, Clement; NDPWatch – Ethernet/IPv6 address pairings monitor, http://ndpwatch.sourceforge.net/ ; viitattu 2020-05-28

[14] R. Pashby; Simplifying IPv6 MLD Snooping Switches, 2006-04-12, https://tools.ietf.org/html/draft-pashby-magma-simplify-mld-snooping-01 ; viitattu 2020-05-28

[15] David C. Plummer; Request for Comments 826: An Ethernet Address Resolution Protocol, saatavilla: https://tools.ietf.org/html/rfc826

[16] Internet Engineering Task Force, Braden, R. (ed.); Request for Comments 1122: Requirements for Internet Hosts: Communication Layers, saatavilla: https://tools.ietf.org/html/rfc1122

[17] K. McCloghrie (ed.); Request for Comments 2011: SNMPv2 Management Information Base for the Internet Protocol using SMIv2, saatavilla: https://tools.ietf.org/html/rfc2011

[18] R. Droms; Request for Comments 2131: Dynamic Host Configuration Protocol, saatavilla: https://tools.ietf.org/html/rfc2131

[19] D. Haskin, S. Onishi; Request for Comments 2465: Management Information Base for IP Version 6: Textual Conventions and General Group, saatavilla: https://tools.ietf.org/html/rfc2465

[20] K. McCloghrie, F. Kastenholz; Request for Comments 2863: The Interfaces Group MIB, saatavilla: https://tools.ietf.org/html/rfc2863

[21] M. Patrick; Request for Comments 3046: DHCP Relay Agent Information Option, saatavilla: https://tools.ietf.org/html/rfc3046

[22] K. Norseth (ed.), E. Bell (ed.); Request for Comments 4188: Definitions of Managed Objects for Bridges, saatavilla https://tools.ietf.org/html/rfc4188

[23] R. Hinden, S. Deering; Request for Comments 4291: IP Version 6 Addressing Architecture, saatavilla: https://tools.ietf.org/html/rfc4291

[24] S. Routhier (ed.), Request for Comments 4293: Management Information Base for the Internet Protocol (IP), saatavilla: https://tools.ietf.org/html/rfc4293

[25] D. Levi, D. Harrington; Request for Comments 4363: Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions, saatavilla: https://tools.ietf.org/html/rfc4363

[26] V. Fuller, T. Li; Request for Comments 4632: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, saatavilla: https://tools.ietf.org/html/rfc4632

[27] B. Volz; Request for Comments 4649: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option, saatavilla: https://tools.ietf.org/html/rfc4649

[28] T. Narten et al; Request for Comments 4861: Neighbor Discovery for IP version 6 (IPv6), saatavilla: https://tools.ietf.org/html/rfc4861

[29] S. Thomson et al; Request for Comments 4862: IPv6 Stateless Address Autoconfiguration, saatavilla: https://tools.ietf.org/html/rfc4862

[30] T. Narten et al; Request for Comments 4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, saatavilla: https://tools.ietf.org/html/rfc4941

[31] G. Halwasia et al; Request for Comments 6939: Client Link-Layer Address Option in DHCPv6, saatavilla: https://tools.ietf.org/html/rfc6939

[32] B. Carpenter, S. Jiang; Request for Comments 7136: Significance of IPv6 Interface Identifiers, saatavilla: https://tools.ietf.org/html/rfc7136

[33] F. Gont et al; Request for Comments 8064: Recommendation on Stable IPv6 Interface Identifiers, saatavilla: https://tools.ietf.org/html/rfc8064

[34] B. Fenner, Request for Comments 8096: The IPv6-Specific MIB Modules Are Obsolete, saatavilla: https://tools.ietf.org/html/rfc8096

[35] T. Mrugalski et al; Request for Comments 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), saatavilla: https://tools.ietf.org/html/rfc8415

[36] Snodgrass, Richard; Developing Time-Oriented Database Applications in SQL, Morgan Kaufmann 1999

[37] Stallings, William; SNMP, SNMPv2, SNMPv3 and RMON 1 and 2 (3rd ed.); Addison Wesley 1999

[38] Stallings, William; Data and Computer Communications (9th ed.), Pearson 2010

[39] Tanenbaum, Andrew S., Wetherall, David J.; Computer Networks (5th ed.), Pearson 2011

[40] Henkilötieto - Arkaluonteinen henkilötieto (Tietosuojalautakunta 04.04.2006 1/2006) https://www.finlex.fi/fi/viranomaiset/ftie/2006/20060001

[41] Määräys teletoiminnan tietoturvasta (Viestintävirasto 67 A/2015 M) https://www.finlex.fi/fi/viranomaiset/normi/480001/44046

[42] E. Vyncke et al; Why Network-Layer Multicast is Not Always Efficient At Datalink Layer; Internet Engineering Task Force 2014, https://tools.ietf.org/id/draft-vyncke-6man-mcast-not-efficient-01.xml ; viitattu 2020-05-28

[43] Wahlman, Teppo; Miksei vieläkään IPv6? Opinnäytetyö, KyAMK 2016, saatavilla: https://www.theseus.fi/handle/10024/121626

[44] Wheeler, Jeff; Layer-2 Multicast State Problems Caused by IPv6 Neighbor Discovery (ND), https://archive.nanog.org/sites/default/files/tues.general.wheeler.neighbor.12.pdf ; viitattu 2020-05-28