KOTIREITITTIMEN KÄYTTÖTARKOITUKSET

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu, tietojenkäsittely

kevät, 2019

Dominik Karvonen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittely
Hämeen ammattikorkeakoulu

Tekijä Dominik Karvonen **Vuosi** 2019

Työn nimi Kotireitittimen käyttötarkoitukset

Työn ohjaaja/t Hanna-Kaisa Sulonen, Erkki Laine

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena on selventää lukijan tietämystä kotireitittimen ominaisuuksista, toimintatarkoituksista ja siihen liittyvästä tiedonkeruusta. Työn sisällössä käydään läpi erilaisten kotireitittimen käytössä vastaan tulevien termien ja ominaisuuksien tarkoituksia keskittyen niiden toimintatapoihin kotiolosuhteissa. Työ ohjaa käyttämään kotireititintä monipuolisemmin.

Työ sisältää verkon koostumuksen, kuljetusprotokollat, portit ja muut erilliset kotireitittimeen kuuluvat ominaisuudet. Tämän lisäksi käydään läpi tietoturvaa ja uhkia kotireitittimeen liittyen. Näiden tietojen ja termien läpikäynti varmistaa käytännön osion paremmin ymmärtämisen.

Käytännön osiossa käydään läpi, miten aikaisemmissa teorialuvuissa olevia tietoja voidaan hyödyntää ohjeistamalla kotireitittimeen kirjautumisen ja sen käyttöliittymän selittämisen yksityiskohtaisesti käyttäen esimerkkinä Asus DSL-N55U reitittimen käyttöliittymää. Tämä opinnäytetyö on suunnattu kokemattomammille kotikäyttäjille, mutta voi auttaa myös kokeneimpiakin.

Avainsanat tieto- ja viestintätekniikka, reitittimet, verkkoyhteydet, tiedonsiirto, tietoturva

Sivut 22 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Business Information Technology
Häme University of Applied Sciences

Author Dominik Karvonen **Year** 2019

Subject Uses of the home router

Supervisors Hanna-Kaisa Sulonen, Erkki Laine

ABSTRACT

The purpose of this thesis is to improve the reader's knowledge of the features of the home router, its operational purposes and the related data collection. The content of the work teaches the different terms and features included in the home router and only includes the information about the features that are more useful at home. This thesis teaches better utilization for the home router.

The contents included in the thesis are how the home network is built and how data gets transferred around. Thesis also includes the meaning of many kinds of different network features and terms. There are also subjects about internet security and how it will affect your network if there were a security breach. This information makes it easier to understand the practical part of this thesis.

The Practical section discusses how to use the data in the previous theoretical sections to teach in detail how to log on to the home router and explain its user interface, using the Asus DSL-N55U router interface as an example. This thesis is aimed at inexperienced home users but can also teach the most experienced.

Keywords ICT, routers, network connections, data transfer, data security

Pages 22 pages

SISÄLLYS

1 JOHDANTO 1

2 YLEISTIETOA REITITTIMISTÄ 3

3 TIETOTURVA JA MURROT 4

3.1 Tietoturvan tarkoitus 4
3.2 Tietoturvamurrot ja niiden ehkäisy 5

4 VERKON KOOSTUMUS 6

4.1 Yksityinen verkko, julkinen verkko ja nimipalvelujärjestelmä 6
4.2 IP-osoitteet ja NAT 7

5 KULJETUSPROTOKOLLAT JA PORTIT 9

5.1 Tiedonvälityskerros ja portit 9
5.2 Tiedonvälitysprotokollat UDP ja TCP 10

6 MUUT KOTIREITITTIMEN OMINAISUUDET 12

6.1 Langaton verkko 12
6.2 Verkkoprotokolla DHCP, reititys ja virtuaalinen erillisverkko 12
6.3 Palomuuri, demilitarisoitu alue ja johtopaikan siltaus 13

7 ESIVAIHEITA KOTIREITITTIMEN ASETUSTEN MUUTTOON 15

7.1 Oman yksityisen IP- osoitteen selvittäminen 15
7.2 Kotireitittimeen kirjautuminen 16

8 VERKON ASETUSTEN MUOKKAAMINEN 17

8.1 Langattoman verkon ja lähiverkon asetukset 17
8.2 Laajaverkon asetukset 18

9 KOTIREITITTIMEN MUIDEN ASETUSTEN MUOKKAAMINEN 20

9.1 Järjestelmäloki, järjestelmän valvonta ja liikenteenhallinta 20
9.2 Lapsilukko 21

10 YHTEENVETO 22

LÄHTEET 23

1 JOHDANTO

Joskus kotona alkaa mietityttämään, onko ostetulla internetiä jakavalla laitteella muitakin toimintatarkoituksia ja miten ottaa siitä selvää, niin tästä opinnäytetyöstä on hyvä aloittaa. Valitsin tämän opinnäytetyöaiheen, koska olen usein joutunut kotona tilanteisiin, joissa joudun säätämään kotireitittimeni asetuksia.

Reitittimellä on monenlaisia toimintatarkoituksia, mutta ne tunnetaan yleisemmin kotona olevana laitteena, joka vastaanottaa Internet-yhteyden langattomasti tai kaapelilla ja jakaa kyseisen yhteyden kaikkiin siihen yhdistettyihin laitteisiin. Tässä opinnäytetyössä keskitytään enimmäkseen reitittimen käyttöön kotiolosuhteissa, joten kutsun reititintä nimellä kotireititin, vaikka samaa laitetta voisikin käyttää erilaisessa ympäristössä, kuten yrityksissä.

Ongelmanani on yleensä ollut, että en tiedä mitä suurin osa asetuksista oikein tekeekään, joten en ole uskaltanut koskea mihinkään ilman että otan asiasta selvää, sillä kotireitittimen asetusten muuttaminen väärin voi joskus jopa katkaista koko kotiverkon Internet-yhteyden.

Tämän opinnäytetyön tarkoituksena on käydä läpi kotireitittimen käytössä vastaan tulevien termien ja ominaisuuksien tarkoituksia kotiolosuhteissa, jonka jälkeen käydä läpi, miten niitä käytetään. Opinnäytetyön sisältö on suunnattu kokemattomammille kotikäyttäjille, mutta voi opettaa myös kokeneimpiakin. Näitä tietoja on mahdollista hyödyntää työelämässä, joka liittyy reitittimien hallintaan ja huoltoon.

Tämä opinnäytetyö alkaa selittämällä luvussa kaksi, miltä kotireititin yleisesti näyttää ja selitetään sen ulkoisten painikkeiden ja johtopaikkojen toimintatarkoitukset. Tämän jälkeen luvussa kolme tullaan käsittelemään tietoturvaa aloittamalla sen tarkoituksen selittämisellä, jonka jälkeen aletaan käymään läpi tietoturvamurtojen tarkoitusta, ennaltaehkäisyä ja ehkäisyä.

Luvussa neljä aletaan käymään läpi, miten kotireitittimen verkko ja tiedon kulku toimii käsittelemällä yksityisen ja julkisen verkon merkitykset. Näiden ymmärtämisen selventämiseksi tullaan käymään myös IP-osoitteiden, NATin ja nimipalvelujärjestelmän historiaa ja tarkoituksia.

Luvussa viisi tullaan käymään läpi kuljetusprotokollien ja porttien tarkoituksia. Tämä luku sisältää yleistietoa ja esimerkkejä porteista. Tämän lisäksi selitetään, mitä ovat tiedonvälitysprotokollien UDP ja TCP toimintatapoja ja niiden eroja.

Luvussa kuusi käydään läpi muiden kotireitittimeen kuuluvien ominaisuuksien tarkoituksia, jotta niitä on mahdollista käyttää tulevissa käytännön luvuissa. Aluksi aloitetaan kertomalla langattoman verkon toimintatarkoitusta ja siihen kuuluvia taajuuksia. Tämän jälkeen käydään läpi verkkoprotokolla DHCPn selitystä ja toimintatapaa. Tämän lisäksi käydään läpi staattisen ja dynaamisen reitin tarkoitukset, joiden jälkeen käsitellään myös VPNn tarkoitus. Lopuksi käydään läpi demilitarisoidun alueen ja johtopaikan siltauksen tarkoitukset kotikäytössä.

Luvussa seitsemän aloitetaan käytännön osuus, jossa opetetaan esivaiheet kotireitittimen asetusten muuttamista varten. Luvussa navigoidaan oma yksityinen IP-osoite, jonka jälkeen käydään läpi omaan kotireitittimeen kirjautuminen vaiheittain. Tämän jälkeen siirrytään lukuun kahdeksan, jossa käydään läpi kotireitittimen asetusten muuttaminen. Tämä sisältää langattoman verkon, laajaverkon, lähiverkon ja palomuurin asetusten ja niiden alla olevien ominaisuuksien läpikäynnin ja käyttöönoton ohjeet.

Luvussa yhdeksän käydään läpi vielä muita kotireitittimen ominaisuuksia, jotka eivät yleensä löydy perusasetuksien alta, vaan ovat oma osionsa. Näitä ovat järjestelmäloki, järjestelmän valvonta, liikenteenhallinta ja lapsilukko. Näiden ominaisuuksien toimintatapoja käydään läpi ja opetetaan tarkemmin.

Tutkimuskysymykset:

- Mitä erilaiset termit tarkoittavat?
- Minkälaisia tietoturvariskejä kotireitittimet sisältävät ja kuinka niitä voidaan ennaltaehkäistä?
- Mitä kaikkea kotireitittimellä voi tehdä?
- Kuinka erilaisia toimintoja voi käyttää?

2 YLEISTIETOA REITITTIMISTÄ

Kotireitittimen käyttötarkoituksena on jakaa Internet-yhteys tarvittaville talon laitteille. Tämän lisäksi kotireititin suojaa kodin verkon tietoturvaa siihen määritetyillä asetuksilla, mutta joissain tapauksissa niistäkin voi päästä lävitse tavoin tai toisin. Kotireitittimellä on monenlaisia tietoturvariskejä ja ne voivat vaarantaa jopa kotielämän yksityisyyttä, sillä nykyään todella monella kotilaitteella otetaan yhteyttä omaan kotireitittimeen. (Asus, n.d. a)

Kotireitittimen yhteyden jakaminen on mahdollista langattomasti tai langallisesti käyttäen reitittimen takaosassa olevia Ethernet portteja. Näitä on yleensä neljä. Tämän lisäksi kotireitittimistä löytyy yleensä USB-paikka tulostimien helppokäyttöä varten ja antennipaikkoja kahdesta kolmeen. Antennipaikat mahdollistavat ulkoisen antennin kytkemisen johdoilla kotireitittimeen paremman Internet-yhteyden saavuttamiseksi, mutta nämä joudutaan yleensä ostamaan erikseen. (Asus, n.d. a)

Kotireitittimestä takaosasta löytyy myös ”Reset” –painike, joka on hyvin pieni. Yleensä ”Reset” -painike on jopa pienen reiän alla, joten sitä painaakseen tarvitsee esimerkiksi hammastikun. Kyseistä painiketta tarvitsee pitää pohjassa yleensä noin viisi sekuntia, jotta asetukset palaisivat oletustilaan. Viimeisenä ominaisuutena on kotireitittimen virta painike, jonka avulla on helppo käynnistää kotireititin uudelleen irrottamatta virtajohtoa. Alla olevassa kuvassa 1 on esimerkki kotireitittimen takapaneelista. (Asus, n.d. b)

Kuva 1. Kotireitittimen takapaneeli. (Kuva Asus DSL-N55U reitittimestä)

3 TIETOTURVA JA MURROT

Tämän teoriaosuuden tarkoituksena on käydä läpi mitä tietoturva tarkoittaa, tietoturvan hallintaa ja vahvistamista. Tämän lisäksi käydään läpi mitä ovat tietoturvamurrot, kuinka niitä voidaan ennaltaehkäistä ja kuinka niistä on mahdollista päästä eroon.

3.1 Tietoturvan tarkoitus

Tietoturvalla tarkoitetaan erilaisten tietojen, järjestelmien, palveluiden sekä tietoliikenteen asianmukaista suojaamista. Tietoturva koskee meitä kaikkia, käsiteltiinpä tietojamme sitten suullisesti, paperilla tai tietokoneella. Palveluiden käyttösäännöt tähtäävät siihen, että kaikkien käyttäjien tietoturva toteutuu. Niinpä tietoturvan perussääntöjä on noudatettava, vaikka meillä ei olisikaan omasta mielestämme mitään salattavaa. Tietoturvassa on kyse tiedon luottamuksellisuudesta, eheydestä, käytettävyydestä sekä todentamisesta. Tällä sivulla käsitellään näitä tietoturvan edellytyksiä. (Opiskelijan digitaidot, n.d.)

Luottamuksellisuuden periaatteella tarkoitetaan sitä, että erilaiset tiedot (mm. salasana) ja järjestelmät (mm. sähköposti) ovat vain sellaisten henkilöiden käytettävissä, joilla on oikeus niiden käyttöön. Eheys tarkoittaa sitä, että tietojen ja järjestelmien tulee olla luotettavia, oikeita ja ajantasaisia, eivätkä ne muutu tai ole muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena. Eheyteen voidaan vaikuttaa esim. tietojen päivittämisellä ja ajantasaisella varmuuskopioinnilla. (Opiskelijan digitaidot, n.d.)

Käytettävyydellä tarkoitetaan sitä, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen henkilöiden käytettävissä etukäteen määritellyssä vasteajassa. Todentaminen (autentikointi) tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistettavuutta. Todentamisessa käytetään esim. muuttuvia avaintunnuksia, salasanoja ja sertifikaatteja. Tämä tarkoittaa, että tietoturva on tärkeää pitää hallinnassa kotiverkon hyvinvoinnin ylläpitämiseksi. (Opiskelijan digitaidot, n.d.)

3.2 **Tietoturvamurrot ja niiden ehkäisy**

Tietoturvamurrot saattavat vaarantaa yksityisyytesi tai kotiverkkosi laitteiden hallintakykyä. Esimerkiksi jos joku ulkopuolinen pääsee hallitsemaan kotireititintä, niin hän pystyy myös hallitsemaan kaikkia kotireitittimeen liitettyjä laitteita ainakin jossain määrin. Esimerkiksi tietomurtajan on mahdollista kopioida tietokoneesi tai muun laitteesi tiedostoja omalle laitteelleen, käyttää verkkoon yhdistettyjä videokameroita, käynnistää ja sulkea erilaisia laitteita tai lähettää viruksia verkkosi kautta kaikkiin siihen liitettyihin laitteisiin. Suurin osa näistä oireista ovat huomaamattomia, joten usein ei edes huomaa, jos joku on murtautunut verkkoon. (Traficom, 2015)

Toisaalta tietoturvamurrot ovat melko harvinaisia, mutta siltä varalta, että niitä tapahtuisikin, niin osaan niistä voi jopa vaikuttaakin. Ennaltaehkäisytavoista helpoimpana voisi olla oman kotireitittimen salasanojen vaihtaminen, sillä kaikkien kotireitittimien oletussalasanat voidaan hakea internetistä käyttäen hakusanana reitittimen merkkiä, mallinumeroa tai nimeä. (Traficom, 2015)

Toisena ennaltaehkäisy vaihtoehtona on tarkistaa kotireitittimesi sisältä, että onko sen ohjelmisto päivitettynä. Nämä päivitykset päivittävät laitteen tietoturvaa ja tuovat usein myös lisää toiminnallisia parannuksia. Jos laitteessa ei ole päivityksiä ja se on kovin vanha, niin laite kannattaa vaihtaa uudempaan. (Traficom, 2015)

Viimeisenä ennaltaehkäisynä on sulkea reitittimestä ominaisuudet, joita ei käytetä. Nämä ominaisuudet voivat antaa tietoturvan murtajille helpon pääsyn kotireitittimeen, sillä ne ovat kuin avoimia käytäviä silloin kun niissä ei kulje tietoa. Jokainen ominaisuus ei tietenkään tätä tee, mutta hiljattain opitaan pääsemään eri kautta reitittimien tietoturvan läpi. Useiden laitteiden asetukset on kuitenkin mahdollista säätää oletusasetuksia turvallisemmiksi. (Traficom, 2015)

Jos kotireitittimesi tietoturva on jo murrettu, niin on suositeltavaa käynnistää se uudestaan virtapainikkeella tai virtajohdon irrottamalla virtapainikkeen puuttuessa tai ollessa viallinen. Näin kannattaa toimia esimerkiksi silloin, jos oma verkkoliikenne vaikuttaa hidastuvan. Tämä useimmiten poistaa sinne päässeet haittaohjelmat. (Traficom, 2015)

Jos haittaohjelma on muokannut laitteen asetuksia, voi olla parasta palauttaa laite tehdasasetuksiin painamalla ”Reset”- painiketta muutaman sekunnin. Jos sekään ei jostain syystä toimi, niin aina voi ottaa reitittin kokonaan pois käytöstä. Sen jälkeen kannattaa ottaa yhteyttä asiantuntijaan ja kertoa heille tarkkaan tapahtumat ja pyytää heiltä tarkempia ohjeita. (Traficom, 2015)

4 VERKON KOOSTUMUS

Tämän teoriaosuuden tarkoituksena on käydä läpi IP-osoitteiden, LANin, WANin NATin ja tiedonvälityksen historiaa, tarkoituksia ja toimintatapoja. Tämän lisäksi mainitaan muutamia yleisimpiä esimerkkejä, joita on mahdollista hyödyntää tilanteesta riippuen.

4.1 Yksityinen verkko, julkinen verkko ja nimipalvelujärjestelmä

Yksityistä verkkoa kutsutaan englanniksi nimellä Local Area Network ja on lyhenteeltään LAN. Yksityistä verkkoa voidaan ajatella kodin sisäisenä verkkona, jossa eri laitteilla on otettu yhteys reitittimeen langattomasti tai fyysisesti. Jokainen yhdistetty laite saa oman yksityisen IP-osoitteen reitittimeltä. IP-osoitteet ovat numerosarjoja, joita käytetään verkkoon liitettyjen laitteiden erottamiseen verkossa. (PieterExplainsTech, 2012)

Tämä eroaa MAC-osoitteesta, joka on laitteen oma yksilöivä osoite. MAC-osoitetta käytetään tilanteissa, joissa laitetta ei ole vielä yhdistetty verkkoon ja ei omista vielä omaa IP-osoitetta. Toisaalta joskus MAC-osoitetta käytetään myös kotireitittimen eri asetusten muokkaamisessa. (PieterExplainsTech, 2012)

Kaikki yksityiset IP-osoitteet ovat näkyvissä vain yksityisessä verkossa, joten kukaan ulkoinen taho ei pääse näkemään kyseisiä tietoja, ellei lupaa ole annettu. Yleensä tämä tieto ei ole edes tärkeää yksityisen verkon ulkoisille tekijöille. (PieterExplainsTech, 2012)

Kaikki IP-osoitteet, jotka alkavat sarjalla 192.168.X.X ja 10.X.X.X ovat tarkoitettu yksityisille IP-osoitteille. Näitä IP-osoitteita ei voi käyttää kukaan muu paitsi oman reitittimen sisäiset laitteet, joten ei tarvitse huolehtia, että jokin suurempi yritys käyttäisi niitä jo. (PieterExplainsTech, 2012)

Julkinen verkko on nimensä mukaan julkinen, joka on englanniksi Wide Area Network ja lyhenteeltään WAN. Kaikki julkiset IP-osoitteet ovat suunniteltuja näkymään internetissä, ellei niitä ole piilotettu jollain tavalla. Julkisessa verkossa on mahdollista yhdistää laite erilaisille verkkopalvelimille, joita laitteesi sovellukset käyttävät. (PieterExplainsTech, 2012)

Nimipalvelujärjestelmä on englanniksi Domain Name System, joka on lyhenteeltään DNS. Lyhenteen DNS käyttäminen on yleisempää nykyajan verkkoasetuksissa, joten se on aiheessa käytetty nimitys. DNS etsii haetun Internet-sivuston linkin avulla tarvittavan IP-osoitteen, jonka avulla on mahdollista yhdistää kyseiseen sivustoon. Tätä kutsutaan enemmän nimellä DNS palvelin tai vain käyttämällä lyhennettä DNS. (PieterExplainsTech, 2014)

Jokaisella julkisella DNS palvelimella on yleensä kaksi IP-osoitetta, joista toinen on olemassa siltä varalta, ettei ongelmia tulisi ensimmäisen ylikuormittuessa tai huoltotilanteissa. Nimipalvelujärjestelmässä on mahdollista päättää kenen DNS palvelimia käytetään, määrittämällä itse tietyt IP-osoitteet, mutta jos ne jäävät määrittämättä, niin ne määrittyvät automaattisesti. Yleisimmät DNS palvelimet ovat Googlen 8.8.8.8 ja varapalvelimeksi 8.8.4.4 tai OpenDNSn 208.67.222.222 ja varapalvelimeksi 208.67.220.220. (Google 2019) (Macecraft Software 2019) (PieterExplainsTech, 2014)

4.2 **IP-osoitteet ja NAT**

1970-luvun aikana luotiin IP-osoitteet, mutta niitä luodessa ei oltu varmoja, kuinka pitkiä IP-osoitteita tultaisiin tarvitsemaan. Tämän ratkaisemiseksi täytyi luoda sopiva tasapaino pakettikoon ja IP-osoitteiden määrän välille. IP-osoite on tietokoneen niin sanottu tunnistuskoodi. (PieterExplainsTech, 2012)

Pitkät IP-osoitteet antavat mahdollisuuden useammalle IP-osoitteelle, mutta tekevät siirrettävästä tiedosta raskaampaa. Toisaalta lyhyet IP-osoitteet pitävät tiedon kevyenä ja helposti siirrettävänä, mutta mahdollistavat paljon vähemmän IP-osoite mahdollisuuksia. (PieterExplainsTech, 2012)

1970-luvulla päädyttiin päätökseen käyttää 32-bittisiä IP-osoitteita, joka tarkoittaa määrällisesti 4,294,967,296 IP-osoitetta. Tähän päädyttiin, koska niihin aikoihin internetiä ei käytetty lähellekään niin paljoa, eikä kyseistä lukumäärää uskottu voitavan ylittää. Tämän nimi on IP-versio 4 ja tekniseltä lyhenteeltään IPv4. (PieterExplainsTech, 2012)

Ongelmana on, että maapallolla on noin 7,6 miljardia ihmistä ja mahdollisia IP-osoitteita on vain noin 4,3 miljardia. Tämä tarkoittaa, että jossain vaiheessa IP-osoitteet loppuivat kesken, mutta IPv4 on yhä käytössä. Ratkaisuksi tähän luotiin osoitteenmuunnos, joka on tekniseltä lyhenteeltään NAT (Network address translation). (PieterExplainsTech, 2012)

NATia käytettäessä reitittimellä on yksityinen- ja julkinen IP-osoite, joiden avulla se toimii tiedonvälittäjänä näiden verkkojen välillä. Tietoa hakiessa tietokone lähettää reitittimelle halutun tiedon paketeissa, jotka kertovat mistä tieto pitää hakea ja mistä se on lähetty. Tämän jälkeen reititin jatkaa tiedon haun internetin kautta paketissa lukevaan IP-osoitteeseen. (PieterExplainsTech, 2012)

Paketin saapuessa osoitteeseen verkkopalvelin prosessoi halutun tiedon, asettaa sille sopivan vastauksen ja lähettää sen takaisin lähettäjälle. Ongelmana on, että paketti on lähetetty yksityisestä IP-osoitteesta, joten sitä ei voi lähettää takaisin samalla tavalla. (PieterExplainsTech, 2012)

Tässä kohtaa palataan reitittimen ominaisuuteen vaihtaa paketin tiedoista yksityinen IP-osoite reitittimen omaksi julkiseksi IP-osoitteeksi jo lähetysvaiheessa. Tämän avulla verkkopalvelin kykenee lähettämään vastauksen takaisin reitittimen julkiseen IP-osoitteeseen, jossa reititin muokkaa pakettia jälleen ja lähettää vastauksen eteenpäin yksityistä IP-osoitetta käyttäen takaisin tiedon haluavalle laitteelle. Näiden vaiheiden aikana NAT luo portit automaattisesti kyseiselle lähetykselle, jotta tieto saa luvan kulkea niistä läpi. (PieterExplainsTech, 2012)

5 KULJETUSPROTOKOLLAT JA PORTIT

Tässä teoriaosuuden luvussa käydään läpi perustietoa porteista ja tiedonvälityskerroksesta. Tämän jälkeen käsitellään tarkemmin tiedonvälitysprotokollien UDP ja TCP toimintatapoja, eroja ja niille sopivimpia käyttötarkoituksia. Tämän lisäksi on listattu muutamia yleisimpiä portteja, joiden käyttö on varattu tietyille yhteyksille.

5.1 Tiedonvälityskerros ja portit

Tiedonvälityskerros antaa useammalle sovelluksille mahdollisuuden käyttää samaa Internet-yhteyttä samaan aikaan. Tiedonvälityskerros luo noin 65 000 porttia tietokoneelle tietokoneyhteyttä kohden, joista yleisimpiä esimerkkejä on listattu alla olevaan Taulukko 1 kohtaan. Kyseisiä portteja pystyy varaamaan tietokoneelle erilaisia sovelluksia varten joko automaattisesti tai manuaalisesti. Yksi sovellus voi käyttää yhtä tai useampaa porttia, jos se on tarpeellista tai muuten hyödyllistä. (PieterExplainsTech, 2013a)

Taulukko 1. Yleisimmät portit (Service Name and Transport Protocol Port Nuber Registry n.d.) On olemassa lukuisia vakioportteja, joita on varattu automaattisesti tiettyihin toimintoihin, mutta tässä on muutamia yleisimpiä:

1	TCPMUX
7	ECHO
11	Users
13	DAYTIME
15	NETSTAT
17	QUOTE
18	MSP
19	CHARGEN
20	FTP
21	FTP
22	SSH
23	Telnet

25	SMTP-sähköposti
31	MSG-AUTH
37	TIME
41	GRAPHICS
42	NAMESERV
43	WHOIS
49	LOGIN
53	DNS
67	BOOTPS
68	BOOTPC
80	http
110	POP3-sähköposti

113	ident
143	IMAP-sähköposti
165	XNS-COURIER
179	BGP
194	IRC
199	SMUX
209	QMTP
213	IPX
443	HTTPS
444	SNPP
445	SNB
521	EXEC

545	PRINTER
547	TALK
526	TEMPO
531	CONFERENCE
533	NETWALL
765	WEBSTER
873	RSYNC
1080	SOCKS
6667	IRC
8080	Vaihtoehtoinen HTTP- portti

Tiedonvälityskerros määrittelee tietoa lähettäessä lähtöportin ja vastaanottoportin, pakkaa sen ja lähettää sen Internet-kerrokseen jatkoprosessoitavaksi. Tämän jälkeen pakattu tieto saapuu vastaanottavan tietokoneen tiedonvälityskerrokseen, jossa tarkistetaan vastaanottoportti, puretaan ja ohjataan tieto portille. Tämän lisäksi tiedonvälityskerroksella on kaksi pääkuljetusprotokollaa, jotka ovat UDP ja TCP. Näillä molemmilla on omat hyvät ja huonot puolensa. (Medhi & Ramasamy 2007, 15.)

5.2 Tiedonvälitysprotokollat UDP ja TCP

UDP on lyhenne nimestä User Datagram Protocol. UDPn tiedonvälitysportokollan suurimpana hyötynä on, että sen pakettien koko on vain 8 tavua, joka on noin 60% pienempi kuin TCPn tiedonvälitysportokollan 20 tavua. Tämän lisäksi UDP ei vaadi yhteyden luontia ennen kuin tietoa aletaan lähettää ja sen lähettämisaikaa pystyy kontrolloimaan enemmän. Esimerkiksi streamatessa, joka tarkoittaa tietokoneen tapahtumien jakamista suoratoistona katsojille internetin välityksellä. UDP on sopivampi, koska streamausohjelmat osaavat kompensoida menetettyjä tietoja ja viive pysyy matalampana, joten tulokset ovat reaaliaikaisempia katsojille. (PieterExplainsTech, 2013a)

UDPllä valitettavasti on alkukantainen ongelmanhavainnointi. Se kantaa mukanaan 16 tavun tarkisteen, mutta se ei ole niin luotettava. Kun UDP löytää korruptoitunutta tietoa, palauttamisen sijaan kyseinen tieto poistetaan. Joissain tilanteissa korruptoitunut tieto säilytetään, mutta sovellukselle asetetaan varoituslippu. (Medhi & Ramasamy 2007, 15.)

UDP ei korvaa menetettyjä paketteja kopioilla, vaan menetetty tieto katoaa kokonaan. Tämän lisäksi UDP ei pidä huolta, että paketin tiedot saapuvat oikeassa järjestyksessä, eikä UDP hidasta pakettien lähetystä, vaikka verkko olisi ruuhkainen, jonka seurauksena enemmän tietoa katoaa. UDP on viestisuuntainen, eli sovellukset lähettävät tietoa vain tietynkokoisissa paketeissa, esimerkiksi tekstiviesteinä. (PieterExplainsTech, 2013a)

TCP on lyhenne nimestä Transmission Control Protocol, joka vaatii yhteyden sopimisen ennen kuin mitään voi lähettää ja tätä kutsutaan kolmen käden kättelyksi. Aluksi kysyjä kysyy hyväksyjältä yhteyden aloittamisesta, jonka jälkeen hyväksyjä vastaa myöntävästi ja kysyjä vastaa vielä, että on kuullut hyväksynnän. Tässä kohtaa yhteys on luotu ja yhteyden sulkeminen toimii samalla tavalla. Aina valmiissa yhteydessä tietoa lähettäessä tulee takaisin tieto, että se on vastaanotettu. (PieterExplainsTech, 2013a)

Toinen etu TCPssä on, että kun tiedon vastaanotosta ei tule tietoa, niin lähettäjä olettaa tiedon kadonneen matkalla ja lähettää sen uudestaan. TCPn paketit ovat numeroitu, joka mahdollistaa tietojen saapuessa niiden oikein järjestämisen ennen käyttöönottoa. (PieterExplainsTech, 2013a)

Kolmas etu TCPssä on ruuhkanhallinta, joka lykkää tiedonsiirtoa huomatessaan verkossa olevan liian ruuhkaista. Tämä vähentää verkon rasitusta ja minimoi mahdollisuuden menettää tietoja. Toisaalta tämän seurauksena tieto ei lähde heti liikkeelle, joten viive voi olla pahempi. Puheluissa tämä voi olla ongelma, kun äänet saapuvat toiselle sekunteja myöhässä. (PieterExplainsTech 2013a)

Muina haittapuolina TCPssä ovat, että paketit ovat suurempia, kuin UDPssä. Tämän lisäksi tietoa lähetetään paljon edestakaisin, joten yleiskustannukset ovat suuremmat. TCP on jatkuvaa yhteyttä ja määrittelee pakettien koot ja järjestyksen itse oikeaksi, esimerkiksi puheluna. (PieterExplainsTech, 2013a)

Pääkuljetusprotokollissa tämä riippuu kokonaan sovelluksesta, jota käytät tai luot. Tekstin kommunikaatiossa TCP on selvästi parempi, koska se osaa pitää sanat oikeassa järjestyksessä, mutta UDPta käyttäessä viestin sanat voivat osaksi kadota tai saapua aivan sekalaisessa järjestyksessä. Tämän lisäksi tekstin lähettäminen ei vaadi paljoa viivettä. (PieterExplainsTech, 2013a)

Myös tiedostoja ladatessa TCP on selvästi parempi, koska TCP pitää huolen, että tiedostot lataantuvat ilman, että niistä puuttuu osia. Samoin on myös tietokoneen etähallinnassa, koska kaiken pitää näkyä selkeästi ja kontrollien kuuluu toimia. TCPtä tarvitsee myös, kun sovelluksissa tarvitaan tiedonkuljetuksen varmistusviestejä, mutta tämän voi tehdä manuaalisesti sovellukselle, jos välttämättä haluaa käyttää UDPta. (PieterExplainsTech, 2013a)

Multimedian streamauksessa molemmat tiedonvälitystavat kelpaavat, mutta kyseinen valinta riippuu omista preferensseistä ja joskus rajoituksista. TCP on parempi, jos on kiinnostuneempi laadusta, eikä niinkään viiveestä ja joskus palomuurit estävät UDPn kokonaan suojaussyistä. Toisaalta osalle on tärkeämpää saada mahdollisimman vähän viivettä, kuormitusta on vähemmän ja tiedon menetyksen voi kompensoida. (PieterExplainsTech, 2013a)

6 MUUT KOTIREITITTIMEN OMINAISUUDET

Tässä luvussa käydään läpi muita yleisimpiä ja mahdollisia kotireitittimen ominaisuuksia, mitä ne tekevät ja kuinka ne ylipäätänsä toimivat. Tämä luku sisältää langattoman verkon taajuudet, verkkoprotokolla DHCPn, staattisen reitin, dynaamisen reitin, virtuaalisen erillisverkon siltauksen ja demilitarisoidun alueen selitykset ja toimintatavat.

6.1 Langaton verkko

Langattomasta verkosta puhuttaessa käytetään yleensä lyhennettä WLAN tai Wi-Fi, jonka toimintona on jakaa Internet-yhteyttä langattomasti verkon laitteisiin. Langattoman verkon nopeus riippuu laitteiden etäisyydestä, taajuuksista, seinien tai lattioiden rakenteista ja muista lähellä olevista langattomista verkoista, jotka käyttävät samaa taajuutta ja kanavaa. (Telia, n.d. a)

Langaton verkko sisältää kaksi erilaista taajuutta. Ensimmäinen on 2.4 gigahertsin taajuus ja 5.0 gigahertsin taajuus. Nämä taajuudet eroavat toisistaan niin, että 5.0 gigahertsinen on nopeampi ja vakaampi yhdistetyn laitteen ollessa lähempänä kotireititintä, mutta 2.4 gigahertsinen on vakaampi yhdistetyn laitteen ollessa esimerkiksi toisessa kerroksessa kotireitittimestä. Tämän lisäksi 2.4 gigahertsinen taajuus kantaa pidemmälle, kuin 5.0 gigahertsinen. Langattoman verkon kanava määräytyy yleensä automaattisesti, mutta sen voi myös valita itse. (Telia, n.d. a)

Valitettavasti vanhemmat kotireitittimet ja laitteet eivät tue 5.0 gigahertsin taajuutta, mutta osa kotireitittimistä mahdollistaa molempien yllä pitämisen yhtä aikaa. Molemmilla on omat yhteysasetuksensa, joten ne on mahdollista nimetä eri tavalla ja niille on mahdollista asettaa erilaiset salasanat. Jos siis laitteesi langaton verkko ei havaitse 5.0 gigahertsin nimistä kotireititintä, niin siinä tapauksessa laitteesi ei sitä tue. (Telia, n.d. a)

6.2 Verkkoprotokolla DHCP, reititys ja virtuaalinen erillisverkko

DHCP on lyhenne nimestä Dynamic Host Configuration Protocol, jonka toimintona on antaa automaattisesti jokaiselle lähiverkkoon yhdistävälle laitteille oma IP- osoitteensa ja pitää huoli, ettei useammalla laitteella ole samaa IP-osoitetta. Tämä välttää ongelmien aiheutumista. (PieterExplainsTech, 2013b)

Verkkoon yhdistetty laite pyytää reitittimeltä omaa yksityistä IP-osoitetta, reititin antaa ehdotuksen, laite hyväksyy ehdotuksen ja vasta sen jälkeen reititin asettaa ehdotetun IP-osoitteen laitteelle. Vaikka vaiheita on monta, niin tieto kulkee huomaamattoman nopeasti. DHCPn käyttäminen vaatii

DHCP-palvelimen, joka on sisäänrakennettu kaikilla reitittimillä, ja DHCP tilaaja jokaiselle yhdistettävälle laitteelle. DHCP käyttää UDP portteja 67 ja 68 yhdistämispyyntöjä ja vastaanottamisia varten. (PieterExplainsTech, 2014)

Virtuaalinen erillisverkko on englanniksi Virtual Private Network ja lyhenteeltään VPN. Se mahdollistaa yksityisyyden verkossa muuttamalla IP-osoitteesi muille erilaiseksi, kuin se todella on. Tämä on suosittu ominaisuus, sillä se pitää sijaintisi yksityisenä, datan salassa ja antaa mahdollisuuden olla internetissä tuntemattomana. (vpnMentor, 2017)

Staattinen reitti tarkoittaa, että reititin käyttää pääkäyttäjän käsin syöttämää reittiä pakettien välittämiseen kohdeverkkoon tai lähemmäksi kohdeverkkoa. Jos verkossa tapahtuu muutoksia, niin staattisen reitin asetukset on muutettava uusia asetuksia vastaaviksi. Reitityksen tarkoituksena on määrittää, mitä kautta tieto kulkee verkossa. (Cisco, n.d.)

Staattisessa reitissä täytyy luoda reitti jokaisen verkon laitteen välille erikseen, jos niiden halutaan kommunikoida keskenään. Tämän ominaisuuden käytön tarve on melko harvinaista kotiverkossa, sillä dynaaminen reititys, joka tarkoittaa automaattista reititystä, hoitaa kaikki tarpeelliset reititys-säännöt. (Cisco, n.d.)

6.3 **Palomuuri, demilitarisoitu alue ja johtopaikan siltaus**

Kotireitittimen palomuurin tarkoituksena on suojata reititintä hyökkäyksiltä, se on yleensä oletuksena asetettu päälle. Tämän lisäksi palomuurin asetusten alla saattaa olla erilaisia suodatinasetuksia, joiden avulla on mahdollista estää käyttäjän pääsy erilaisille sivustoille niiden osoitteiden tai niissä käytettyjen sanojen avulla.

Palomuurin kytkeminen pois päältä ei ole ollenkaan kannattavaa, ellei tiedä mitä tekee tai on varautunut toisenlaisella suojauksella. Yleensä palomuurin päällä pitäminen ei ole haitaksi, mutta jos se sattuu olemaan, niin vaikka sen pois päältä ottaminen olisikin helpoin ratkaisu, on olemassa muitakin tapoja päästää tietoa sen lävitse ja vielä turvallisestikin.

Demilitarisoitu alue on englanniksi Demilitarized Zone, joka on lyhenteeltään DMZ. Tämä lyhennettä käytetään suomen kielessäkin kyseisen ominaisuuden selittämisessä. DMZn tarkoituksena on kehittää verkon turvallisuutta erottamalla laitteita erillisen palomuurin taakse ja/tai siirtämällä osan laitteista palomuurin toiselle puolelle. On otettava huomioon, että tietokoneilla ja reitittimellä on jo omat palomuurinsa suojaamassa tietoja. Tämä tarkoittaa, että tämä kolmas palomuuri ei ole välttämätön ominaisuus kotiverkossa. DMZllä voi myös jakaa verkon useampaan osaan. (PowerCert Animated Videos, 2018)

Kotireitittimissä on olemassa hieman erilainen DMZ ominaisuus, joka toimii yksinkertaisemmin. Sen tarkoituksena on avata kaikki laitteen portit, joka mahdollistaa kaiken tiedon kulkemisen vapaasti laitteeseen ja sieltä pois. Tämän toiminnon käyttäminen on yleisintä pelikonsoleilla, sillä se vähentää palomuuri ongelmia pelatessa. Lisäksi on suositeltavaa määritellä pelikonsolille pysyvä IP-osoite, niin DMZ-asetukset eivät siirry vahingossa toiseen laitteeseen tai poistuvat käytöstä pelikonsolin IP-osoitteen vaihtuessa automaattisesti. (PowerCert Animated Videos, 2018)

Siltaus, joka on englanniksi Bridged mode, on DMZ asetusten ominaisuus, jolla voi asettaa Ethernet-johtopaikan siltaavaksi, jonka jälkeen kyseinen johtopaikka päästää tietoa suoraan tietokoneeseen ilman, että kotireitittimen palomuuri vaikuttaisi asiaan. Tämä ominaisuus ei ole mahdollista kaikilla kotireitittimillä, jolloin DMZ on korvaava vaihtoehto. (Telia, n.d. b)

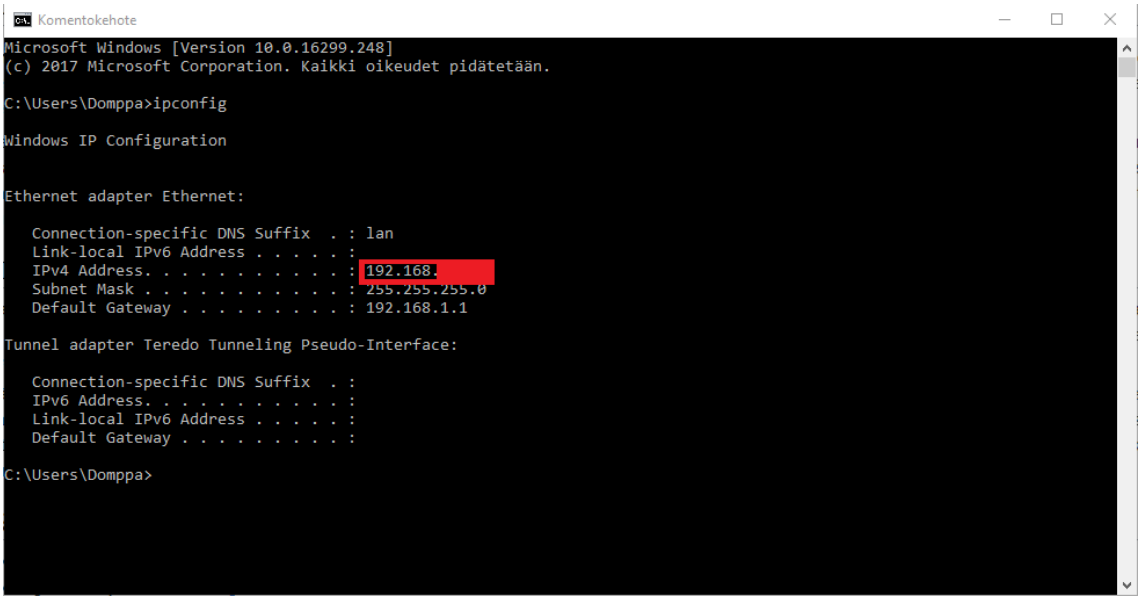
7 ESIVAIHEITA KOTIREITITTIMEN ASETUSTEN MUUTTOON

Tämä luku sisältää käytännön esimerkin oman yksityisen IP-osoitteen selvittämiseen ja kotireitittimen kirjautumiseen käytännössä. Tämä on selitetty mahdollisimman yksinkertaisesti, jotta lukija voi itse käyttää tätä ohjeena ja toteuttaa samat toiminnot itse.

7.1 Oman yksityisen IP- osoitteen selvittäminen

Porttien avaamiseksi täytyy tietää, että miltä tietokoneelta portin avausta käytetään. Laitteiden yksityiset IP-osoitteet kertovat, mikä laite on mikäkin, joten tarvitaan juuri kyseisen tietokoneen yksityinen IP-osoite. Tietokoneesi yksityisen IP-osoitteen saa selville, kun tekee näin:

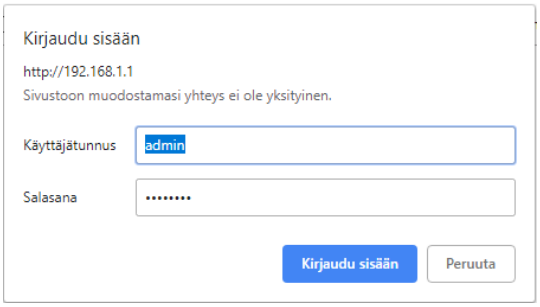
Windows hakupalkkiin kirjoitetaan ”cmd” ja painetaan ”Enter”- painiketta. Tämä aukaisee komentokehotteen, jota voi käyttää lukuisiin asioihin. Seuraavaksi kirjoitetaan komentokehotteeseen ”ipconfig” ja painetaan jälleen ”Enter”- Painiketta. Tämä tuo esille tietoja, joista täytyy löytää tällä hetkellä käytetyn laitteen yksityinen IP-osoite. Se löytyy yleensä nimellä ”IPv4 Address”. Esimerkkinä alla oleva Kuva 2.



Kuva 2. Komentokehotteesta yksityisen IP-osoitteen etsiminen. (Kuvankaappaus komentokehotteesta)

7.2 Kotireitittimeen kirjautuminen

Tässä kohdassa käydään läpi, kuinka kotireitittimen sisälle kirjaudutaan, joka mahdollistaa asetusten muokkaamisen tulevissa kohdissa. Ensimmäiseksi on päästävä oman reitittimen sivulle, joka alkaa kirjoittamalla Internet-selaimen osoitepalkkiin ”192.168.1.1”. Tämä avaa reitittimen kirjautumissivun tai tuo esille pienen kirjautumisikkunan, joka on erilainen reitittimen merkistä riippuen. Esimerkkinä alla oleva Kuva 3.



Kuva 3. Kirjautuminen reitittimen sivustolle. (Kuvankaappaus Asus DSL-N55U reitittimen kirjautumissivusta)

Seuraavaksi annetaan kirjautumistiedot ja kirjaudutaan sisään. (Ensimmäisellä kirjautumiskerralla kirjautumistiedot ovat oletuksella, mutta ovat helppo selvittää operaattorilta tai internetistä). Kirjautuessa aukeaa valinta mennä helppoon tai monimutkaiseen näkymään. Joissakin reititinmalleissa ei ole helppoa näkymää, joten aukeaa suoraan reitittimen asetussivu. Jos saat valinnan helpon ja monimutkaisen näkymän väliltä, niin valitse monimutkainen saadaksesi enemmän tietoa näkyviin.

8 VERKON ASETUSTEN MUOKKAAMINEN

Tämä käytännön luku sisältää kotireitittimen tärkeimmät verkon asetukset ja niiden käytön ohjeet. Verkon asetukset sisältävät langattoman verkon, lähiverkon, laajaverkon ja palomuurin asetukset. laajaverkon asetuksissa käydään tarkemmin läpi ohjeita porttien sallimisesta ja avaamisesta.

Melkein kaikki asetuksista on mahdollista toteuttaa suurimmalla osalla reitittimistä ja mokkuloista, ellei operaattori ole estänyt kyseistä ominaisuutta tai portteja. Ongelmana on, että melkein jokaisella reitittimellä ja mokkulalla vaiheet voivat olla erilaiset. Seuraavan prosessi tehdään Asus DSL-N55U kotireititintä käyttäen.

8.1 Langattoman verkon ja lähiverkon asetukset

Langattoman verkon asetusten alla kaikki muokattavat asiat tulevat vaikuttamaan vain langattomaan verkkoon, ellei siitä toisin mainita. Langattoman verkon yleisosioissa pääsee määrittelemään langattoman verkon perusasetuksia, kuten taajuustyypit kanavat ja niiden kaistanleveydet, langattoman verkon nimi, salaustyyppi ja salasana. Suurin osa näistä ominaisuuksista on määritetty automaattisesti, eikä niiden muuttaminen vaikuta niin paljoa kuin luulisi, mutta tärkeintä on määrittää salasana, jolla verkkoon voi yhdistää langattomasti.

Kaikista nykyajan kotireitittimistä löytyy myös ominaisuus nimeltä WPS, joka on lyhenne nimestä Wi-Fi Protected Setup. Tämä ominaisuus tarjoaa helpon ja turvallisen tavan muodostaa yhteyden langattomaan verkkoon. Sen käyttötapoja on kaksi, jotka ovat kotireitittimen ja yhdistettävän laitteen WPS-painikkeen pitäminen pohjassa reitittimessä kerrotun ajan verran tai käyttämällä PIN-koodia verkkoon yhdistämiseen antamalla yhdistettävän laitteen PIN-koodi reitittimelle. WPS-painike vaihtoehto on yleisempi ja tukee useampaa laitetta.

Lähiverkon eli LAN yleisen osion alla voi määritellä reitittimen IP-asetukset, mutta yleensä ne ovat oletuksina oikein. Tämän lisäksi LAN-asetukset sisältävät muutamia rajoittimen poistoja, jos kyseiset reitittimet niitä tukevat, jotka voi laittaa päälle tai pois nostaakseen reitittimen rajoja ja tehostaakseen Internet-asetuksia sisäverkossa. LAN-asetukset sisältävät myös laajempia osioita.

Esimerkiksi lähiverkon asetukset sisältävät DHCP-palvelimen asetukset. Tämän ominaisuuden asetuksissa tarvitsee määrittää, onko kyseinen ominaisuus päällä vai ei, antaa sille nimi ja DNS palvelin, jota käyttää. Tämä ominaisuus ei ole välttämätön kotiverkossa, ellei henkilökohtaisesti tarvitse sen ominaisuuksia johonkin.

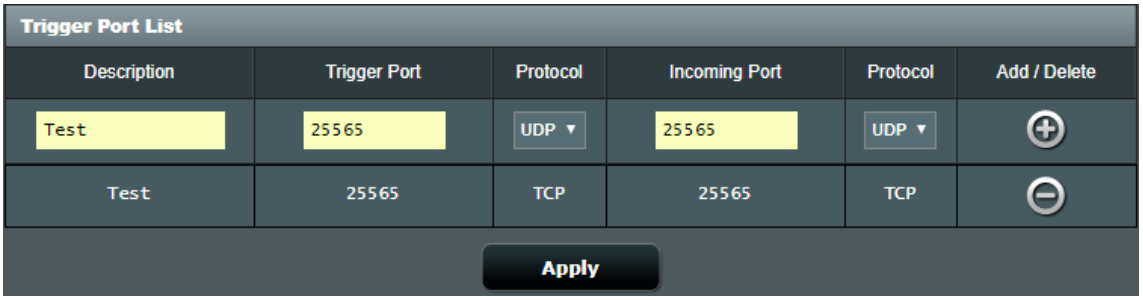
8.2 Laajaverkon asetukset

Laajaverkko on englanniksi Wide Area Network, joka on lyhenteeltään WAN- asetuksista määritetään kaikki asetukset, jotka vaikuttavat kotireitittimen ja laajaverkon välillä. WANin perusasetuksista on mahdollista asettaa päälle tai pois itse WAN kokonaan tai NAT- ominaisuus. Jos WAN-ominaisuuksia halutaan käyttää, niin alla olevat kappaleet käyvät läpi, mitä kaikkia mahdollisia WAN ominaisuuksia kotireititin saattaa sisältää.

WAN- asetuksista voi löytyä siltaus ominaisuus, jolla asetetaan yksi tai useampi kotireitittimen Ethernet-johtopaikka siltaavaksi. Tämä ominaisuus on yleensä vain päälle tai pois valinta. Jos siltaus ominaisuutta ei ole, niin DMZ ominaisuus saattaa olla korvaava vaihtoehto. Tämän ominaisuuden voi myös laittaa päälle tai pois, mutta sen laitettua päälle on määritettävä, mikä verkon laite tulee käyttämään kyseistä ominaisuutta määrittämällä halutun laitteen yksityinen IP-osoite.

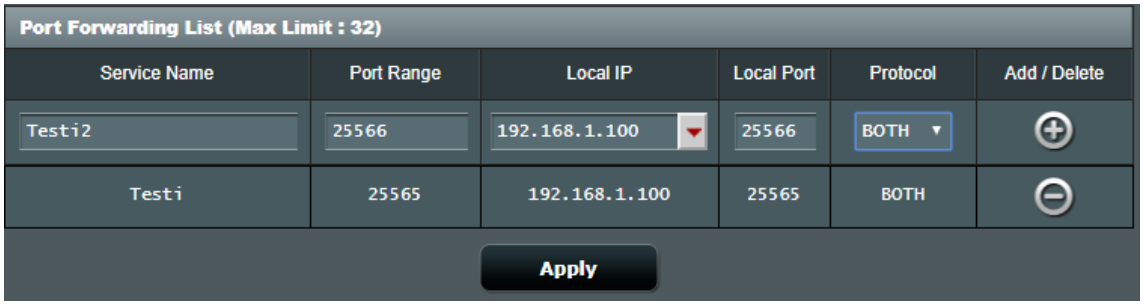
Toisena mahdollisena WAN- asetusten ominaisuutena voi olla porttien käynnistys tai portinsiirto. Porttien käynnistyksen tarkoituksena on avata portti vain, kun lähiverkon laite pyytä kyseisen portin käyttöä. Tämän ominaisuuden ansiosta ei tarvitse syöttää käytetyn laitteen IP-osoitetta, sillä kotireititin ottaa sen talteen, kun haluttua porttia yritetään avata. Tässä tarvitsee itse tietää mikä on haluttu portti, josta tietoa päästetään lävitse. Tämän etsimistä en voi kertoa, koska en tiedä mihin kyseistä porttia käytetään, mutta sen voi yleensä etsiä netistä.

Porttien sallimisen ominaisuus löytyy yleensä joko WAN- asetusten tai NAT- asetusten alta. Se voi olla nimeltään ”Porttien salliminen tai englanniksi ”Port triggering”. Seuraavaksi tulee nimetä kyseinen portti ja määrittää minkä portin halutaan laukaisevan portin aukaisun ja minkä portin aukeavan kyseisestä laukaisusta on suositeltavaa asettaa ne samanlaisiksi, niin ei aiheudu monimutkaisuuksia. Osa kotireitittimistä ei anna mahdollisuutta asettaa UDPta ja TCPtä yhtä aikaa, joten ne saatetaan joutua määrittämään erikseen, mutta tietojen syötön jälkeen painaa vain ”Lisää” painiketta, jonka jälkeen painaa ”Apply” painiketta ottaakseen asetukset voimaan. Esimerkkinä seuraavalla sivulla oleva Kuva 4.



Kuva 4. Porttien määrittäminen ja valmiustilaan ottaminen. (Kuvankaappaus Asus DSL-N55U reitittimen käyttöliittymästä)

Portinsiirron tarkoituksena taas on selittää, kuinka portteja on mahdollista avata. Nämä vaiheet voivat olla erilaiset jokaisella reitittimellä ja mokkulalla. Portinsiirto osion löytää myös yleensä WAN- tai NAT- asetusten alta ja se voi myös olla nimetty eri tavalla kuten nimityksellä ”Virtuaalipalvelin” tai englanniksi ”Port forwarding”. Seuraavana vaiheena on syöttää IP-osoite ja portti/portit ja painaa ”lisää”- painiketta. Joskus nämä ominaisuudet sisältävät vielä oman painikkeensa, joista ne voi laittaa helposti päälle tai pois, mutta joskus riittää vain, että painaa ”Apply”- painiketta, jolla muutokset tallennetaan ja otetaan käyttöön. Esimerkkinä alla oleva Kuva 5.



Kuva 5. Porttien määrittäminen ja avaaminen (Kuvankaappaus Asus DSL-N55U reitittimen käyttöliittymästä)

Jos tilanne on yhä monimutkainen, niin on mahdollista etsiä tietoa internetistä tai muualta. Parhaiten tietoa löytää hakemalla googlesta kirjoittamalla hakupalkkiin ”Port Forwarding.” Porttien avaamisen hyötynä on, että pääsee ylläpitämään julkisia palvelimia omalta kotikoneelta. Tätä voi käyttää esimerkiksi peli- tai keskustelupalvelimilla. Tämän ansiosta ei tarvitse maksaa muille palvelimen ylläpidosta päästäkseen viettämään aikaa ystävien kanssa omalla palvelimella.

Portinsiirto avaa määritetyt portit kokonaan niin pitkäksi aikaa, kunnes se/ne käydään itse sulkemassa. Tätä voi pitää tietoturvauhkana, sillä kuka vain voi käyttää kyseistä porttia pääsynä verkkoon, jos se unohtuu päälle. Suurempana tietoturvauhkana on, että jos avaa liian monta porttia reitittimeltä, on mahdollista päästää läpi tietomurtoja. Toisaalta tämä on todella epätodennäköistä ottaen huomioon porttien määrän verrattuna avattujen porttien määrään. Jos on huolestunut tietomurroista, niin aina voi sulkea portit käytön jälkeen.

9 KOTIREITITTIMEN MUIDEN ASETUSTEN MUOKKAAMINEN

Tässä käytännön luvussa käydään läpi muita kotireitittimen asetuksia ja niiden käyttöä. Näitä ovat muun muassa: järjestelmäloki, järjestelmän valvonta, liikenteenhallinta ja lapsilukko. Nämä ovat yleensä hyvä tietää, mutta eivät välttämättömiä.

9.1 Järjestelmäloki, järjestelmän valvonta ja liikenteenhallinta

Järjestelmälokin tarkoituksena on kerätä ja näyttää kaikki muutokset, mitä reitittimessä on tapahtunut. Järjestelmälokin alla on useampi loki, joista jokainen kertoo erilaisia tietoja. Tämä on hyödyllinen, kun tarvitsee tietää mitä on tapahtunut ja mitä on mennyt pieleen.

Järjestelmän valvonnan osiossa pääsee muokkaamaan itse kotireitittimen tietoja ja asetuksia. Esimerkiksi kotireitittimeen kirjautumisen salasanan ja kotireitittimen käyttämän aikavyöhykkeen. Tämän lisäksi Järjestelmän valvonta osiosta on mahdollista päivittää kotireitittimen ohjelmisto uudempaan, joka pitää sen tietoturvan ajan tasalla. Viimeisenä siellä on mahdollista palauttaa kotireititin tehdasasetuksiin, tallentaa tämänhetkiset tiedot muistiin ja vaihtaa erilaisten valmiiksi määriteltyjen asetusten välillä.

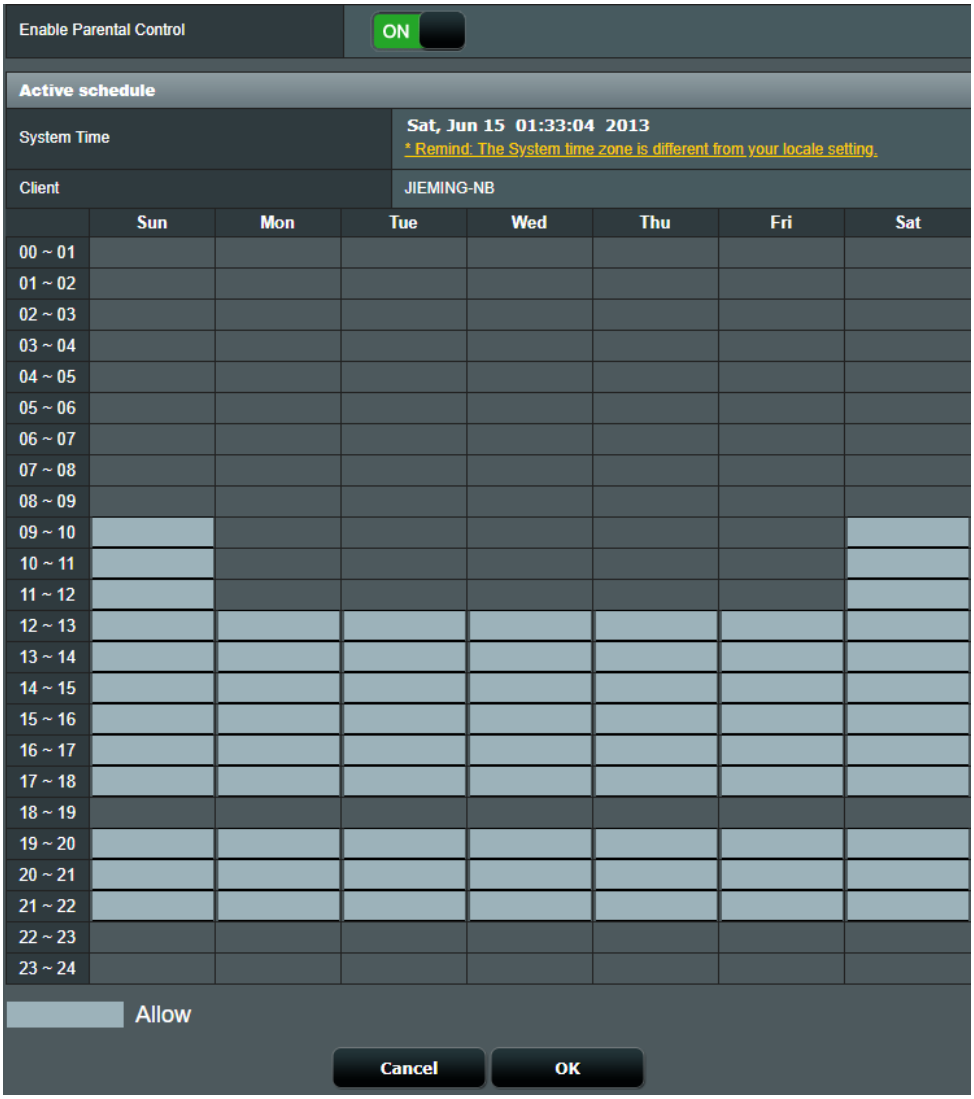
Liikenteenhallinnassa on mahdollista tehdä kaksi asiaa. Ensimmäinen on asettaa Quality of Service (Palvelun laatu) ominaisuus päälle, joka asettaa prioriteetin tietyn tyyppisille tiedonsiirroille. Yleensä oletusasetuksina on parantaa online-pelaamisen kokemusta ja surffaamista netissä.

Toisessa ominaisuudessa voi nähdä kuinka verkon liikenne toimii, kuinka nopeasti tieto kulkee ja lisäksi mikä laite verkossa kuluttaa eniten internetin tehoa. Osassa kotireitittimissä on myös mahdollista säätää tietylle laitteelle prioriteetti verkon kaistan käytössä, sillä myös se on joskus tarpeen.

9.2 Lapsilukko

Lapsilukko ominaisuus mahdollistaa aikarajan asettamisen verkon käyttäjille. Tämä ominaisuus täytyy ensin asettaa päälle, jonka jälkeen tarvitsee asettaa halutun laitteen IP-osoite tai MAC-osoite ja painaa ”lisää” -painiketta.

Tämän jälkeen aukeaa viikon aikataulukko, josta on mahdollista päättää yleensä tuntien tarkkuudella, milloin kyseinen laite saa Internet-yhteyden. Tämä on hyödyllinen ominaisuus vanhemmille, jotka eivät saa lapsiaan tottelemaan pelkällä käskyllä. Esimerkkinä alla oleva kuva 6.



Kuva 6. Lapsilukon ajastuksen asetukset. (Kuvankaappaus Asus DSL-N55U reitittimen käyttöliittymästä)

10 YHTEENVETO

Tässä opinnäytetyössä käytiin läpi yleistietoa kotireitittimistä, tietoturvasta ja tietoturvamurroista ja opittiin, että ne täytyy ottaa huomioon, vaikka ei kotireititintä käyttäisikään monipuolisesti. Tietoturvan osiossa selvitettiin myös tietoturvamurtojen ennaltaehkäisyä ja ehkäisyä tavoin, joihin voi itse vaikuttaakin. Tämän ansioista lukija on oppinut pitämään oman kotireitittimensä asetukset tietoturvallisempana.

Tämän lisäksi opinnäytetyössä avattiin enemmän kotireitittimeen ja internettiin kuuluvaa termistöä ja ominaisuuksia, kuten NAT, IP-osoitteet, portit, TCP, UDP ja eri verkkojen koostumukset ja niiden merkitykset ylipäätänsä. Näitä tietoja käyttäen siirryttiin käymään läpi kotireitittimen ominaisuuksia esimerkein, opettelemalla kotireitittimeen kirjautumisen, avaamaan erilaisia ominaisuuksia ja muokkaamalla niiden asetuksia.

Aluksi käytiin läpi tärkeimmät ominaisuudet ja asetukset, joiden jälkeen siirryttiin muihin asetuksiin. Esimerkiksi liikenteenhallinta ja järjestelmäloki, jotka ovat suurimmaksi osaksi vain luettavaa tietoa. Lisäksi käytiin läpi lapsilukon asetukset, joka ei ole kaikille käyttäjille kovin merkityksellinen ominaisuus, mutta toisille se saattaa olla hyvin tärkeä työkalu.

Sain vastattua tämän opinnäytetyön tutkimuskysymyksiin laajasti ja monipuolisesti, vaikka tutkimuskysymysten määrä olikin mielestäni suppea. Olen tyytyväinen lopputulokseen ja innokas oppimistani asioista. Kaikkia kotireitittimen ominaisuuksia en onnistunut sovittamaan tähän, sillä ne olisivat olleet liian laajoja selittää ja merkitykseltään turhia kotikäytössä.

Seuraavaksi tavoitteeksi asettaisin reitittimien käytön yrityksissä, sillä yrityskäytössä reitittimillä olevia ominaisuuksia on mahdollista hyödyntää paljon monipuolisemmin. Tämä mahdollistaa kaiken mahdollisen tiedon oppimisen reitittimien käyttöliittymistä.

LÄHTEET

Asus (n.d. b). *How to restore the ASUS wireless router to default setting? (ASUSWRT).* Haettu 26.2.2019 osoitteesta https://www.asus.com/support/FAQ/1000925/

Asus (n.d. a). *How do I use the rescue mode of a router? [Wireless]*. Haettu 26.2.2019 osoitteesta https://www.asus.com/support/FAQ/1000814

Cisco® (n.d.). *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*. Haettu 6.2.2019 osoitteesta https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_route.html

Google. Google Inc. (n.d.). *Google Public DNS*. Haettu 31.1.2019 osoitteesta https://developers.google.com/speed/public-dns/

Macecraft Software. Macecraft Inc. (1998-2019). *Set up OpenDNS on your device*. Haettu 31.1.2019 osoitteesta https://www.opendns.com/setupguide/

Medhi, D. & Ramasamy, K. 2007. *Network Routing: Algorithms, Protocols and Architectures. Elsevier Science & Technology*. Viitattu 17.1.2019. Saatavissa Ebookcentral-tietokannassa: https://ebookcentral.proquest.com/lib/hamk-ebooks/detail.action?docID=291644&query=router

Opiskelijan digitaidot. Helsingin yliopisto. (n.d.). *Tietoturvan periaatteet*. Haettu 12.2.2019 osoitteesta https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/

PieterExplainsTech (4.12.2012). *How Network Adress Translation Works*. Haettu 17.1.2019 osoitteesta https://www.youtube.com/watch?v=QBqPzHEDzvo

PieterExplainsTech (24.7.2013a). *UDP and TCP: Comparison of Transport Protocols*. Haettu 19.1.2019 osoitteesta https://www.youtube.com/watch?v=Vdc8TCESIg8

PieterExplansTech (23.10.2013b). *Automatic IP Address Assignment: How DHCP Works*. Haettu 30.1.2019 osoitteesta https://www.youtube.com/watch?v=GlZC4Jwf3xQ

PieterExplansTech (28.8.2014). *Inside The Domain Name System*. Haettu 30.1.2019 osoitteesta https://www.youtube.com/watch?v=GlZC4Jwf3xQ

2016 Portforward, LLC n.d. *How to forward a port.* Haettu 20.1.2019 osoitteesta https://portforward.com/

PowerCert Animated Videos (17.9.2018). *What is a DMZ? (Demilitarized Zone).* Haettu 30.1.2019 osoitteesta https://www.youtube.com/watch?v=dqlzQXo1wqo

Service Name and Transport Protocol Port Nuber Registry (n.d.). Haettu 22.1.2019 osoitteesta https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Telia (n.d. a). *Wifi*. Haettu 26.2.2019 osoitteesta https://www.telia.fi/asiakastuki/net-tiyhteydet/wifi/langattoman-verkkoyhteyden-nopeus

Telia (n.d. b). *TECHNICOLOR TG799 -MODEEMIN KÄYTTÖOHJE*. Haettu 26.2.2019 osoitteesta https://www.telia.fi/asiakastuki/laitteet/modeemit-ja-reitittimet/Technicolor-TG799vac

Traficom Liikenne- ja viestintävirasto (12.10.2015). *Heikosti ylläpidetyt kotireitittimet ovat verkkorikollisten kohteena - osa 1*. Haettu 2.2.2019 osoitteesta https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2015/10/ttn201510121051.html

vpnMentor (12.12.2017). *What is a VPN and How Does it Work?.* Haettu 31.1.2019 osoitteesta https://www.youtube.com/watch?v=_wQTRMBAvzg