SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

IPV4 JA IPV6 PROTOKOLLIEN VERTAILU

Opinnäytetyö

TEKIJÄ: Henri Liekola

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Henri Liekola	
Työn nimi IPv4 ja IPv6 protokollien vertailu	
Päiväys 11.6.2021	Sivumäärä/Liitteet 23
Ohjaaja(t) Veijo Pitkänen ja Pekka Vedenpää	
Toimeksiantaja/Yhteistyökumppani(t) Savonia-amk, tietohallintopalvelut	

Tiivistelmä

Opinnäytetyössäni kerron kahden eri internetin protokollien eroista. Vertailen IPv4 ja IPv6 -versioiden eroavaisuuksia ja miksi nykyisen IPv4 -version on siirryttävä sivuun, kun IPv6 -versio tulee olemaan laajemmin käytetty protokolla.

Opinnäytetyö koostuu eri lähteistä koostettuihin tietoihin, joissa kerron mitä mikäkin tekniikka tarkoittaa ja miten niitä voidaan käyttää hyväksi toteutetussa verkkoratkaisussa. Pyrin kertomaan olennaisimmat kohdat tekniikoista eikä työn ole tarkoitus olla tekniikkakohtaisen aiheen koulutusmateriaali.

Työn tarkoitus on lisätä lukijan tietoisuutta siitä, mikä muuttuu, kun IPv4 vaihtuu IPv6 -versioon ja missä tilanteissa mikäkin tekniikka sopii käyttöön. Työn luettuaan lukija ymmärtää, mitä muutoksessa tapahtuu, vaikka muutos ei näy arjen toiminnoissa esimerkiksi älypuhelimen sovelluksien käytössä.

Avainsanat
IP, IPv4, IPv6, muutos, päivitys

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Valitse kohde.			
Degree Programme Valitse kohde.			
Author(s) Henri Liekola			
Title of Thesis Comparison of IPv4 and IPv6 versions			
Date	11th of June, 2021	Pages/Appendices	23
Supervisor(s) Veijo Pitkänen ja Pekka Vedenpää			
Client Organisation /Partners Savonia-amk, tietohallintopalvelut			

Abstract

In this thesis I will compare two different internet protocols and their differences. I will compare IPv4 and IPv6 - versions differences and explain why presently used IPv4 must setp aside when IPv6 version will be the new widely used protocol

Thesis is consisted from different sources which are mostly web sites from internet. Text will be informal about different methods how and where they are put in effect at network. I will concentrate on essential part of each method. This thesis is not mentioned to be an educate material about different methods.

Thesis meaning is to append readers understaning about on going update in network when IPv4 is being replaced with IPv6 and why different methods are used in different function. I hope reader will understand the underlying chance that is happening in network even though it does not appear in every day life of regular network user.

Keywords

IP, IPv4, IPv6, chance, update

SISÄLTÖ

1 JOHDANTO 6
1.1 Lyhenteet ja määritelmät 6
2 TARVE MUUTOKSELLE 8
3 OSI -MALLI JA YLEISET VERKKOTEKNIIKAT 10
3.1 OSI-malli (Open Systems Interconnection) 10
3.1.1 OSI-mallin historiasta. 10
3.1.2 Fyysinen kerros (Physical) 11
3.1.3 Linkkikerros (Data link) 11
3.1.4 Verkkokerros (Network) 12
3.1.5 Siirtokerros (Transport) 12
3.1.6 Sessiokerros (Session) 12
3.1.7 Esittelykerros (Presentation) 12
3.1.8 Sovelluskerros (Application) 13
3.2 TCP/IP 13
3.3 UDP 14
4 MITÄ MUUTTUU IPV6 JA IPV4 VÄLILLÄ 14
4.1 Yleistä IP-osoitteista 14
4.1.1 IPv4-osoite 14
4.1.2 IPv6-osoite 15
4.2 Osoiteavaruus 15
4.2.1 Osoitetyypit 15
4.2.2 Unicast 16
4.2.3 Global unicast address 16
4.2.4 Link-local unicast address 17
4.2.5 Loopback address 18
4.3 Multicast 18
4.4 Anycast 18
4.5 Lähimmäisten laitteiden etsintä 19
5 MIKSI IPV6 ON PAREMPI 19
5.1 Suurempi osoiteavaruus. 19
5.2 NAT -tekniikan poistuminen 20

5.3 Yksinkertaistettu osoitestruktuuri 20
5.4 Yksinkertaisempi osoite konfigurointi 20
5.5 Yksinkertaistetumpi osoitteen uudelleen numerointi 20
5.6 Broadcast:n poistaminen 21
5.7 Yksinkertaisempi ylätunniste 21
6 IPV6 SAVONIAN TIETOVERKOSSA 21
7 LÄHTEET 22

1 JOHDANTO

Seuraavat sivut sisältävät tietoa eri IP -protokollan toimintatavoista ja sen tekniikoista. Opinnäytetyön tarkoitus on vertailla mikä muuttuu, kun nykyinen IPv4 joutuu siirtymään tulevan IPv6 edeltä. Työssä kerron tulevan version hyödyistä verrattuna vanhempaan eli IPv4 versioon.

IPv6 version laajaa käyttöönottoa odottaa varmasti suuri määtä kuluttajista, mutta operaattoreille muutos voi olla kallis ja hidas, eikä tuo merkittäviä eroja. IPv6:n käyttöönottoon ollaan varmasti valmiita kuluttajapuolen tuotteissa, mutta muutos vaatii paljon ponnistuksia operaattoreilta, kun kaikki verkon laitteet tulee käydä läpi ja tarvittaessa päivittämään/vaihtamaan uuteen laitteistoon.

IPv6 protokollan käyttöönotto ei näy normaalin verkokäyttäjän arjessa suuresti, koska sovellusket toimivat edelleen samalla tavalla. Taustalla kuitenkin tapahtuu asioita, jotka auttavat verkon nopeutta, turvallisuutta, hallintaa ja turvaa verkon laajentumisen myös tulevaisuudessa.

1.1 Lyhenteet ja määritelmät

IP	Internet Protocol, sovittu stantardimalli, kuinka viestit kulkevat internetissä.
IPv4	IP versio 4, vielä yleisimmin käytössä oleva verkkoprotokollan versio.
IPv6	IP versio 6, odotettu korvaaja IPv4 korvaajaksi lähitulevaisuudessa.
IANA	Internet Assigne Numbers Authority, mailmanlaajuinen IP-osoitteiden koordinoija.
Cisco	Suuri verkkolaitevalmistaja ja verkkotekniikan koulutuksia tarjoava yritys.
ISP	Internet Service Provider, eli operaattor,i on verkkoyhteyksiä tarjoava yritys, suomessa tunnetuimmat ovat Telia, Elisa ja DNA
Bitti	Bitti on binäärinen numero, jonka arvo voi olla 1 tai 0. Tätä arvoa käytetään laajalti tietotekniikassa tiedosta sen käsiteltävänä osana.
Reititin	Verkkolaite, joka välittää ja ohjaa viestejä verkossa oikealle päätelaitteelle.
IETF	Internet Engineering Task Force on mailmanlaajuinen avoin ryhmittymä verkon suunnittelijoita, laitemyyjiä ja tutkijoita, joiden tarkoitus on tukea toisiaan yhdessä internetin kehitystä.
DHCP	Dynamic Host Configuration Protocol on yksi IP:n protokollista, jonka tehtävä on jakaa osoitteita verkkoon kytkeytyville laitteille.

NDP	Neighbor Discovery Protocol on protokolla, joka mahdollistaa lähimmäisten laitteiden tunnistamisen ja auttaa viestien nopeampaan välitykseen.
ND	Neighbor Discovery osa NDP protokollaa oleva viesti, jolla tunnistetaan lähimmäinen laite.
NAT	Network Address Translation eli dynaaminen osoitteenmuutos. Käytetään IPv4 protokollana, jotta nykyiset osoitteet riittävät käyttäjille.
ISO	International Organization for Standardization on kansainvälinen toimija, joka määrittelee stantardit, joiden avulla kokonaisuudet toimivat yhdessä.
OSI	Open Systems Interconnection on tapa kuvastaa tiedonsiirtoprotokollien kerrokset ja niiden toiminta.
DSL	Digital Subscriber Line on digitaalinen yhteystapa kuluttajalta operaattorille, tunnetaan myös perinteisesti lankapuhelinverkkona.
TCP	Transmission Control Protocol on IP -protokolla.
UDP	User Datagram Protocol on IP -protokolla
ARP	Address Resolution Protocol jonka tehtävänä oli ylläpitää reitittimellä tietoja muista verkoista, joihin paketti tarvittaessa viesti välittää.

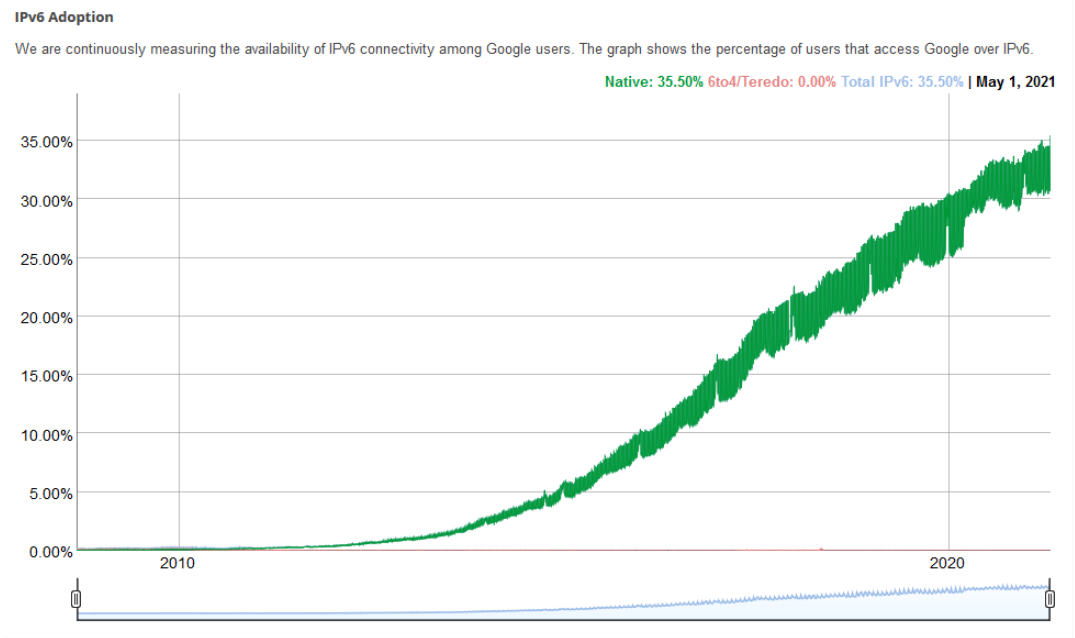
2 TARVE MUUTOKSELLE

Internet laajenee jatkuvasti ja nopeasti. Internetin idea perustuu siihen, että laitteet voivat keskustella keskenään missä tahansa päin verkkoa tai maailmaa. Jotta laitteet kykenevät vaihtamaan tietoa keskenään, tarvitsee jokainen oman osoitteen ja yhteiset säännöt, kuinka tiedonsiirtoa suoritetaan. Siksi on luotu Internet Protocol (IP). IP on protokolla tai ryhmä sääntöjä, joiden avulla tieto voi kulkea eri verkkojen läpi ja saapua oikeaan määränpäähän. (Cloudflare, 2019).

Tunnetuin käytetty protokolla on IPv4, missä v4 tarkoittaa versiota 4. Yleisesti on kuitenkin tiedossa, että IPv4 -osoitteet tulevat loppumaan kesken, kun yhä useampi esine liitetään internettiin, esim. kahvinkeittimet, autot ja teollisuuden sensorit. IPv6 tulee auttamaan osoitteden kanssa, koska IPv6 myötä osoitteiden määrä kasvaa radikaalisti, kun jokaisen laitteen osoitteen koko suurenee 32 bitistä 128 bittiin. IP -osoitteita säätelee ja jakaa Internet Assigne Numbers Authority (IANA). (IANA)

Osoitteiden määrä IPv4 -protokollassa on n. 4.29 miljardia, IPv6:n myötä niitä on 1028 kertaisesti enemmän, eli hyvin paljon enemmän käytettäväksi eri laitteille internetissä pitkäksi aikaa. (Cisco) Osoitteiden määrän kasvessa tarvittiin myös paljon uusia sääntöjä, jotta osoitteiden ja viestiliikenteen hallinnoiminen on mahdollista ja vaatisi vähemmän manuaalityöstävää. (IETF, 1998)

Tarve muutokselle näkyy selvästi verkossa. Vuonna 2012 vain 1% Google käyttäjistä yhdisti palveluihin IPv6:n kautta, mutta 2021 toukokuun alussa IPv6:n kautta käyttäjiä oli jo yli 35% (Google)



KUVA 1. IPv6:n kautta tehdyt yhteydet Google palveluissa. (Google)

Oma pohdintani IPv6:n muutoksesta perustuu sekä kuluttujan, että Internet Service Provider (ISP) eli internetyhteyden tarjoajan kannasta. Kuluttajan kannalta IPv6 voisi tulla vallitsevaksi versioksi, vaikka heti, koska suurin osa nykyisistä laitteista tukee jo IPv6 protokollan toimintaa, esim. tietokoneet ja puhelimet. Tietysti joitain laitteita tulisi päivittää. IPv6 -protokolla tarjoaa käyttäjälle hyödyksi sen, ettei ole aliverkkoja eikä julkisten osoitteiden päälekkäisyyttä. Myös reititys on nopeampaa eli viiveet voivat laskea.

ISP:n kannalta muutos on varmaankin hieman haastavampi. Verkonlaitteiden tulee kaikkien pystyä käsittelemään IPv6 -protokollaa ja välittämään sen protokollan mukaisesti viestejä. Nykyisen, laajan IPv4:n mukaan rakennettu verkko vaatii suuria investointeja ja työtä, ennen kuin IPv6:sta tulee uusi normaali. Yksi ratkaisu olisi hallita ja ylläpitää IPv4 ja IPv6 verkkoja yhtäaikaisesti, mutta sen ylläpitäminen on kallista ja raskasta.

3 OSI -MALLI JA YLEISET VERKKOTEKNIIKAT

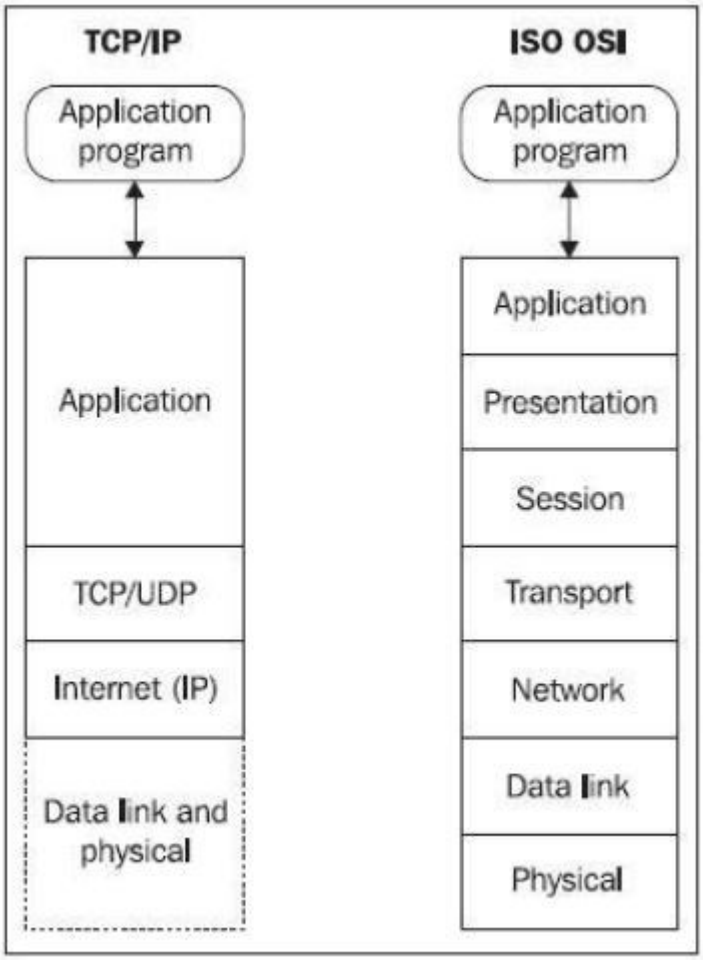
3.1 OSI-malli (Open Systems Interconnection)

Protokollan avulla on määritelty stantardit viestien vaihtoon, eli verkkoliikenteelle eri kerroksien välillä. Yleisesti internetin yhteyksissä käytetty TCP / IP protokolla ei sisällä kaikkia ISO (International Organization for Standardization) OSI -mallin (Open Systems Interconnection) kerroksia, vaan ainoastaan Sovellus-, siirto-, verkko- ja linkkikerrokset. (Stockebrand, 2007)

OSI-malli on luotu International Organization for Standardization:n toimesta, jonka tarkoituksena on stantartoida verkkoliikennettä. Määritelty malli luo kehysikkunat verkkoliikenteen yhteyksien muodostamiseen ja viestien välittämiseen. Stantardissa liikennettä jaetaan eri kerroksiin ja kerroksien välillä on tarkoitus liikkua vain yksi kerros kerrallaan. Jokainen kerros on oma kokonaisuutensa, jonka sisällä tehdäät ennaltamäärätyt toimenpiteet. Tehtyjen toimenpiteiden ansiosta viestin kulku kerroksesta toiselle on virheetöntä ja viesti kulkeutuu perille saakka onnistuneesti. OSI-malli oli tarkoitus korvata kaikki sitä aiemmat kommunikointitavat tietokoneiden väliltä. Sen sijaan OSI -mallista tuli malli kuvailla ja määritellä heterogeenisen verkontekniikan kommunikointia. (Stockebrand, 2007)

3.1.1 OSI-mallin historiasta.

OSI-mallin työstäminen alkoi ensimmäisen kerran 1970 -luvun lopussa. Mallia työsti ensin itsenäisesti International Organization for Standardization (ISO) ja International Telegraph and Telephone Consultative Committee, tai CCITT, jonka lyhenne tulee ranskan kielestä. Heidän työ valmistui vuonna 1983 ja se julkaistiin kaikille käytettäväksi. Työn tarkoituksena oli auttaa myyjiä ja kommunikaatio-ohjelmistojen kehittäjiä tarjoamaan yhteentoimiva verkkotekniikkaa.



KUVA 2. Yleisimmin käytössä oleva TCP/IP -protokollan käyttämät kerrokset. (Alena Kabelová, 2006)

3.1.2 Fyysinen kerros (Physical)

Fyysisen kerros sisältää proseduureja ja kuvailee mekaanisia, elektronisia ja vaadittuja toiminnallisuuksia, joita tarvitaan kokonaisuuden perustamiseen, ylläpitämiseen ja julkaisemiseen. Fyysinen kerros synkronoi lähetettävät bitit ja tarjoaa signaloinin fyysisessä yhteydessä. Fyysinen sisältää esim. DSL -linjan vai valokuidun. (Battu, 2014)

3.1.3 Linkkikerros (Data link)

Linkkikerros välittää datapaketteja, joita kutsutaan myös ”frames” eli vapaasti suomennettuna kehyksinä. Kehys sisältää tietoa esim. lähettäjästä ja vastaanottajasta ja viestin sisällön. Näitä kehyksiä lähetetään linkkikerroksessa fyysisesti toisiinsa yhdistetyissä verkoissa, tunnetuin verkko on Ethernet, jota käytetään mailmanlaajuisen internetin linkkikerroksena. (Stockebrand, 2007)

Linkkikerroksen tärkeä tehtävä on myös pitää tieto ehjänä ja korjata virheelliset bittivirrat, eli kehykset. Linkkikerros myös määrittelee, kuinka kehyksiä lähetetään ja sisältää tiedon fyysisen kerroksen reiteistä. (Battu, 2014)

3.1.4 Verkkokerros (Network)

Verkkokerroksessa eri fyysisest verko yhdistyy ja laitteet voivat kommunikoida tämän läpi. Data kulkee verkkokerroksessa laitteelta toiselle pakatussa linkkikerroksen kehyksessä. Pakattu kehys lähetetään toiselle laitteelle, joka on kytkettynä samaan verkkoon tai reitittimelle, joka hakee paketille uuden verkon tietojensa mukaan ja välittää kehyksen eteenpäin.

Reititin avaa linkkitason kehystä ja selvittää kehyksen tietueista, onko paketti tarkoitettu sen omaan verkkoon vai meneekö eteenpäin seuraavalle reitittimelle. Ennen lähettämistä reititin pakkaa kehyksen takaisin päivittäen osan tietueista. (Stockebrand, 2007)

3.1.5 Siirtokerros (Transport)

Siirtokerroksessa datan kulkemisen mukaan tulee porttinumerot, joita käytetään avuksi paketin ohjaamiseen oikealle laitteelle verkossa. Verkkokerroksen (edellinen) liikenteessä pakettia liikutetaan verkkojen välillä, mutta siirtokerroksessa huolehditaan kahden laitteen välisen tiedonsiirron eheydestä ja jatkuvuudesta. Siirtokerroksessa huolehditaan paketin päätymisestä oikealle portille. Siirtokerroksen protokollat määritellään palvelintasolla. (Battu, 2014)

Yleisin siirtokerroksen tekniikka on TCP (Transmission control protocol). Tämä tekniikka huolehtii jokaisen paketin saapumisesta ja pyytää lähettäjää lähettämään kadonneet tai vajavaiset kehykset tarvittaessa uudelleen.

Toinen tekniikka on User Datagram Protocl (UDP), joka ei huolehdi kehyksien eheydestä tai niiden kaikkien saapumisesta, vaan mahdollisimman nopeasta kehyksien siirrosta lähettäjältä vastaanottajalle. (Stockebrand, 2007)

Siirtokerroksen tekniikoista (TCP ja UDP) kerron vielä tarkemmin tämän kappaleen lopussa.

3.1.6 Sessiokerros (Session)

Sessiokerroksessa tarjotaan kaksi toimintoa: Hallinta ja valvonta. Hallinnassa muodostetaan kahden laitteen yhteys ja sen yhteyden dialogi, mikä määrittelee tietojen vaihdon rajoittamalla ja synkronoimalla tiedonvaihdon tapahtumia, jotka muodostuvat kahdesta kokonaisuudesta (lähettäjä ja vastaanottaja). Tämä kerros myös sisältää tunnistautumisen ja salasanan vaihdon.

3.1.7 Esittelykerros (Presentation)

Esittelymuoto, formatointi, tiivistys, enkryptaus ja jäsenneltyjen tietojen käsittely hyödylliseksi sovellusten käytettäväksi on esittelykerroksen tehtäviä. Sisään- ja ulostulevan liikenteen ja tiedonvaihdon esittely ja hallinta, sekä jäsennöidyn tiedon tarkistus tapahtuu tässä kerroksessa. Tämä kerros mukauttaa eri tiedostoformaatteja, suorittaa tarvittavia koodikäännöksiä ja valitsee

sopivat syntaksit sovellukselle. Esimerkiksi kuvat muutetaan png muotoon tai käännetään ASCII -koodista EBCDIC -koodiin. (Battu, 2014)

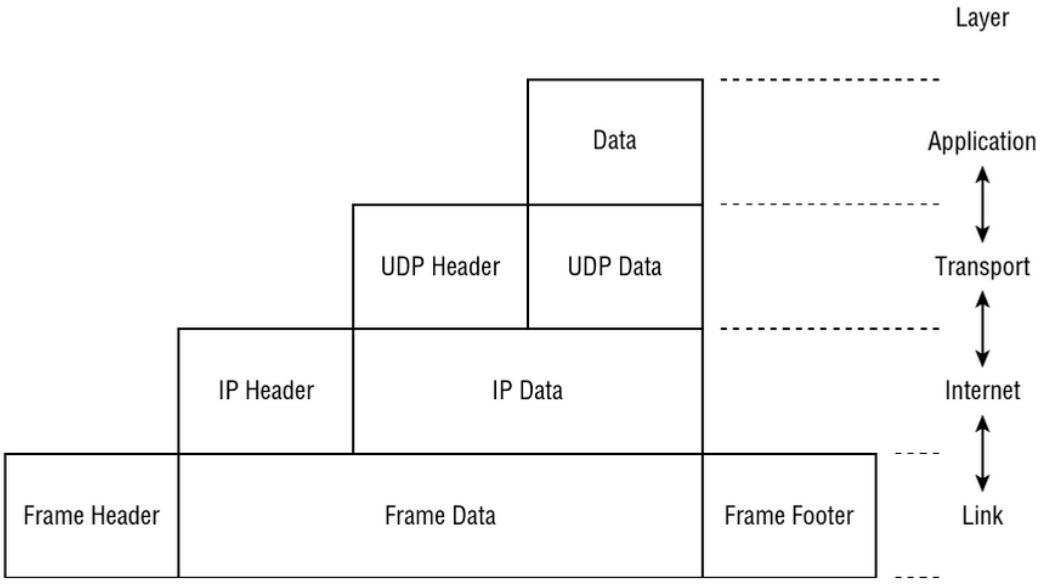
3.1.8 Sovelluskerros (Application)

Application, eli sovelluskerroksen tarkoitus on luoda rajapinta erilaisille tietokoneille ja laitteille, jonka avulla halutut ominaisuudet toimivat. Tämä sovelluskerros alkaa siitä, kun päätelaite saa oman IP-osoitteen ja yhdistää itsensä verkkoon. Sovelluskerroksen aikana on mahdollista tapahtua poikkeus kerrostekniikkaan, eli ei-vierekkäiset kerrokset keskustelevat keskenään. Tämä tapahtuu esimerkiksi DNS-palvelua käyttäessä. Silloin sovellus hakee Transport -kerroksesta asti tiedon.

3.2 TCP/IP

TCP protokolla (Transmission Control Protocol) on yleisimmin käytössä oleva verkkoprotokolla, eli IP (Internet Protocol). Sen tarkoituksena on luoda luotettava, ehjä ja korjaava yhteys laitteiden välille. TCP/IP on yleinen nimitys tälle protokollalle.

TCP/IP malli käyttää edellä mainitusta OSI -mallista 4 eri kerrosta hyödyksi: sovellus-, siirto-, verkko- ja linkkikerrosta. Suuri määrä sovelluksia ja ohjelmia täytyy sovittaa yhteen, jotta ne voivat kommunikoida läpi verkkotekniikan, jonka vuoksi kapsulointia suoritetaan eri kerroksien välillä. Näin taataan itsenäinen viestitys eri sovelluksien tuottamien viestien välillä.



KUVA 3. Esitys TCP/IP kerroksen konseptista.

Kuvan 5. ylin kerros, application eli sovelluskerros, on yksi osa verkkokerroksesta. Se sisältää ylemmän tason protokollat, jotka mahdollistavat sovelluksen kapsuloida tiedon niin, että se voidaan välittää siirtokerrokselle (transport). TCP/IP mallin kirjastot sisältävät kaikki tarvittavat protkollat, joita viestin lähettämiseksi tarvitaan sovelluskerroksessa, koska siinä on yhdistettynä OSI-mallin sovellus-, sessio- ja esityskerros.

TCP/IP mallin siirtokerros kartoittaa viestin kulun suoraan OSI-mallin neljänteen kerrokseen, eli siirtokerrokseen. TCP/IP mallin verkkokerroksesssa toiminta on yleensä suoraan OSI-mallin verkkokerroksesta. TCP/IP mallissa linkkikerros sisältää OSI-mallin linkki- ja fyysisen kerroksen. (Edwards James, 2009)

3.3 UDP

UDP eli User Datagram Protocol (UDP) tarjoaa hallinnollisesti yhteydettömän ja nopean tiedonsiirron mahdollisuuden. Se ei korjaa, pakkaa, järjestele tai uudelleenlähetä viestejä eli viestin välitys on nopeaa mutta ei niin varmaa. UDP -tekniikkaa hyödynnetään esimerkisi verkkopeleissä ja äänipuheluissa, missä tietoa tulee saada nopeasti välitetyksi. UDP sisältämä kehys sisältää paljon vähemmän otsakkeita ja vaatii vähemmän resurssia viestin purkuun ja kapsulointiin. (CCNA)

UDP:n ja TCP:n suurimpia toimintapaeroja on yhteyden muodostaminen, viestien kapsulointi ja niiden käsittely. UDP:n yhteys on prosessilta prosessille, kun taas TCP on laitteelta laitteelle. UDP perustuu parhaimman viestinnän tilaan, missä viestit kulkevat nopeasti. TCP:n toimintamallissa viestien toimitus huolehditaan lähettäjältä vastaanottajalle asti ja mahdollisesti virheelliset paketit lähetetään uudestaan. (TechTarget, 2020)

4 MITÄ MUUTTUU IPV6 JA IPV4 VÄLILLÄ

4.1 Yleistä IP-osoitteista

IP-osoite tarkoittaa yksilöllistä tunnistetta laitteelle, joka on yhdistettynä verkkoon. Osoitteen avulla lähettäjän lähettämä viesti päätyy oikealle vastaanottajalle. Tällä hetkellä käytössä on kaksi eri versiota, IPv4 ja IPv6. Vielä yleisimmin käytössä on IPv4 mutta IPv6 -versio tulee väistämättä tulevaisuudessa olemaan yleisemmin käytössä. (Mooc.fi)

4.1.1 IPv4-osoite

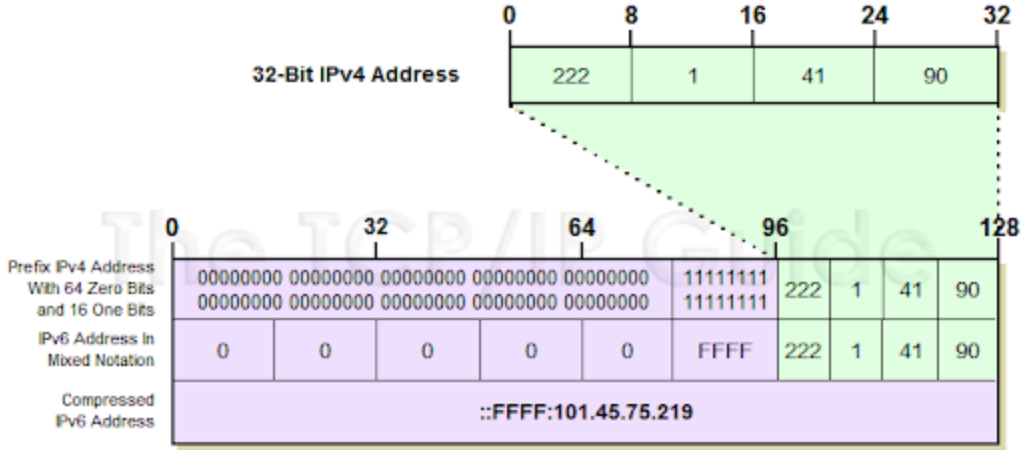
IP-osoite jaetaan kahteen osaan, joista toinen on osoitetta hallinnoivan operaattorin ja toinen on verkon laitteiden tunnistamista varten. Rajapinta näiden kahden välillä on tunnistettavissa verkkopeitteen avulla. Verkkopeite on 32 -bittiä pitkä tietue, jonka alkupään arvo on yksi ja loppupään nolla. Ensimmäiset ykkösen bitit kertovat operaattorin tunnisteen ja nollabitit määrittelevät operaattorin hallinnoimat verkon laitteet.

IPv4 -osoitteita on alun perin tarkoitettu jaettavaksi eri luokkiin: A, B, C ja D. Luokat määriteltiin kaksoispisteiden avulla. Esimerkeiksi osoitteen viimeisen kaksoispisteen jälkeiset bitit (luokka D) oli varattu osoitteiden monilähetykseen, eli multicast -tekniikalle. Tiettyjä osoitearvoja varattiin myös tiettyihin käyttötarkoituksiin. Esimerkiksi 127. -alkava osoite on käytetävänä paikallisena osoitteen yhden verkkolaitteen sisällä. Paikallinen osoite on yleisesti käytössä reitittimellä, josta se jakaa yhteyden internettiin. (Mooc.fi)

4.1.2 IPv6-osoite

IPv6 mahdollistaa paljon suuremman osoiteavaruuden. Osoitteen kokoa kasvatetaan IPv4:n 32 bitistä IPv6:n 128 bittiin. IPv6 osoite ei ole luokallinen kuten IPv4 versiossa oli. IPv6 osoite voi olla mielivaltaisesti luotu ja osoitetta voidaan lyhentää kaksoispisteellä osoitteen keskellä tai lopussa. Esim. osoitteen 2001:0DB8:0000:0000:0006:0600:300D:527B voi ilmoittaa myös muodossa 2001:0DB8::0006:0600:300D:527B, jolloin osoitteen käsittely on nopeampaa ja helpompaa. (Guide) Kahden kaksoispisteen lyhentämistä voidaan käyttää vain kerran osoitteen ilmaisussa

4.2 Osoiteavaruus

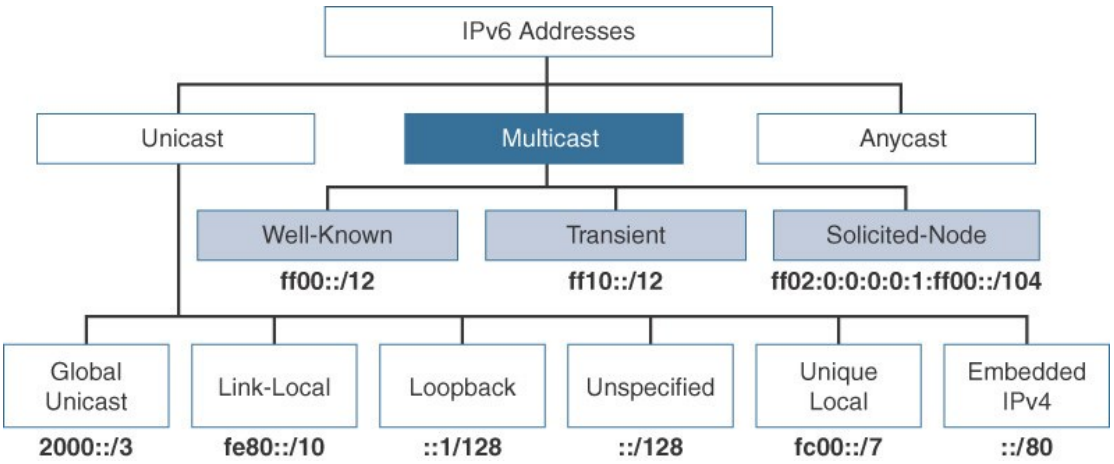


KUVA 4. IPv6 osoitekoko on huomattavasti suurempi, kuin IPv4. (Guide, 2005)

Osoite koostuu kahdeksasta ryhmästä 16 bittisistä heksadesimaaliarvoista, erotettuna kaksoispisteillä, IPv4:n osoite oli suora arvo biteistä, maksimissaan siis 255. IPv6:n osoitteessa huomattavia muutoksia pituuden lisäksi on se, että arvon voi ilmoittaa kirjaimella ja osoitteen eri osat erotellaan kaksoispisteellä. Yksittäinen arvo on siis numeroiden 1-9 tai kirjaimien a-f väliltä. Kirjaimilla voidaan siis osoittaa suurempi numeraalinen arvo, esim b kirjain tarkoittaa desimaaleissa arvoa 11. (CertBros, 2020)

4.2.1 Osoitetyypit

IPv6:ssa on kolme erilaista osoitetyyppiä, Unicast, Anycast ja Multicast. Määrä on vähemmän kuin IPv4 versiossa mutta niillä voidaan kattaa samat käyttötarkoitukset. Näitä kolmea eri osoitetyyppiä voidaan jakaa eri porteille ja eri käyttötarkoitusta varten. Eri osoitetyypit määritellään jokaisen osoitteen käyttöliittymälle, ei reitittimille kuten IPv4 verkossa. Yksittäiseen käyttöliittymään voidaan myös määritellä useampi erilainen osoitetyyppi. (IETF, 2006)



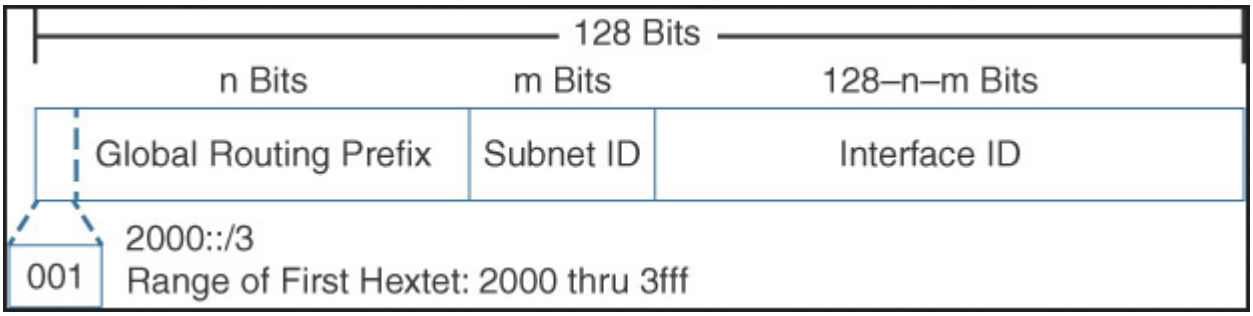
KUVA 5. IPv6:n eri osoitetyypit ja niiden tunnisteet. (Cisco, 2017)

4.2.2 Unicast

Unicast osoitteen tyypeistä merkittävimmät on global unicast ja link local osoitteet. Global unicast osoitetta voidaan verrata IPv4:n julkiseen osoitteeseen. Muita ositetyyppejä on Loopback -osoite, unicast local -osoite ja IPv4 -embedded -osoite (Cisco, 2017) Unicast -osoitetta käytetään yksittäisten laitteiden välillä. Unicast -osoitteelle osoitettu paketti lähetetään osoitteelle tunnistetulle käyttäjäliittymille, eli portille, jossa laite on. (IETF, 2006)

4.2.3 Global unicast address

Global unicast address (GOA) eli global unicast -osoite on mailmanlaajuisesti reititettävä ja saavutettavissa oleva osoite IPv6 -verkossa. Global unicast -osoitteiden merkitys on suuri IPv6 osoitearkkitehtuurissa.



KUVA 6. Global unicast osoitteen rakenne. (Cisco, 2017)

Kuvaan 6. viitaten, Global unicast osoite sisältää kolme eri kenttää. Ensimmäinen vasemmalta on Global Routing Prefix, jonka tarjoaa internet palvelun tarjoaja (ISP). Sen avulla osoitteen käyttämän laitteen verkon sijainti voidaaan tunnistaa. Subnet ID:n avulla voidaan varata omia aliverkkoja kuluttajan puolelta. Toisinkuin IPv4:n julkisen osoitteen kanssa, IPv6:n global unicast osoitteessa ei tarvitse lainata bitti-arvoja Interface ID (päätelaitteen osa) kentästä. Kaikki bittiarvot, jotka jäävät global routing prefix -kentän jälkeen ja ennen interface ID -kentän alkua, voidaan käyttää hyödyksi subnet ID -kentässä, joka yksinkertaistaa ja helpottaa aliverkon luomista ja hallintaa.

Päätelaite voi saada tarvitsemansa global unicast -osoitteen kolmella eri tavalla: Manuaalisesti konfiguroimalla tai automaattisella osoitteen jaolla. Automaattisia osoitejakoja on stateless address autoconfiguration ja statefull DHCP. (Cisco, 2017)

4.2.4 Link-local unicast address

Link-local on toinen unicast -osoitetyyppi. Link-local osoite määritellään yhdelle linkille, eli yksittäiselle aliverkolle. Link-local -osoitteen tarvitsee olla uniikki vain käytössä olevassa verkossa. Muissa verkoissa voi olla saman arvoinen osoite. Tämän vuoksi reitittimet eivät lähetä eteenpäin paketteja link-local -osoitteen perusteella. Link-local -osoitteen voi tunnistaa sen alusta: FE80. Tämä FE80 -arvo osoitteen ensimmäisenä osiona on yleisesti käytettävä ja hyväksytty tapa (RFC 4291). Osoitteen alussa voi käyttää myös muuta arvoa, mutta sen aiheuttamista muutoksista verkon toiminnassa voi aiheutua ongelmia.

Jotta päätelaite voi olla IPv6 -yhteyden valmiudessa, laitteella täytyy olla IPv6 link-local -osoite. Laitteella ei tarvitse olla välttämättä IPv6 global unicast -osoitetta, mutta link-local -osoite täytyy olla. Vain yksi link-local -osoite voi olla määriteltynä yhdelle käyttöliittymälle, eli portille. Päätelaitteet yleensä luovat itse oman link-local -osoitteen käynnistyessä ja yhdistyessä verkkoon. Yleisimmät käyttöjärjestelmät toimivat tällä tavalla, esim. Cisco IOS, Windows, Mac OS ja Linux.

Link-local -osoitteen luominen omalla päätelaitteella tuo suuren helpotuksen laitteen kytkemiseksi verkkoon. Laite voi itsenäisesti luoda itselleen oman uniikin osoitteen, jota se voi käyttää suoraan samassa aliverkossa. Link-local -osoitteen avulla päätelaite saa myös yhteyden lähimpään reitittimeen tai toiseen laitteeseen, josta se saa tiedon, mistä saa yhteyden DHCPv6 -palvelimene, joka taas antaa päätelaitteelle oman global unicast -osoitteen. Tämän jälkeen laite voi yhdistyä internettiin, eli mailmanlaajuiseen verkkoon.

Äsken kerrottu link-local -osoitteen luomisesta itsenäisesti päätelaitteella ratkaisee IPv4 -verkossa ilmennyttä ongelmaa. IPv4 -verkon aikana ongelmana oli, ettei laite saanut IP-osoitetta, jota se tarvitsee verkkoon liittymiseen, ennekuin se sai yhteyden DHCP-palvelimeen. Tämän vuoksi IPv4 -verkossa päätelaite joutui ensin lähettämään paketteja, missä sen täytyi kysyä tietoja muilta laitteilta ja lopulta sai oman osoitteen. Tämä on vienyt aina paljon aikaa sekä vaatinut monimutkaisempia ratkaisuja, verrattuna IPv6 -versiossa.

IPv6 -version dyynamisen liikenteen protokollaviestit lähetetään link-local osoitteen kautta. Päätelaitteet käyttävät reitittimen link-local -osoitetta oletusyhdyskäytävänä.

4.2.5 Loopback address

Loopback on yksi Unicast -osoitteiden tyypeistä, jonka arvo on yleisimmin ”::1”, eli sen bittiarvot on aina 0, paitsi viimeinen. Loopback -osoitetta voidaan käyttää laitteella, kun se haluaa lähettää itselleen paketin/viestin. Tätä käytetään yleisesti TCP/IP -protokollan toimivuuden testaamiseksi. Loopback -osoitteen voidaan valita fyysiselle portille. Loopback -osoiteelle välitettyjä viestejä ei tulisi koskaan lähettää yksittäiseltä laitteelta eteenpäin, koska reitittimien ei tule niitä välittää vaan ne tulee tiputtaa reitityksestä pois heti, kun vastaanottajana on loobpack -osoite. (Cisco, 2017)

4.3 Multicast

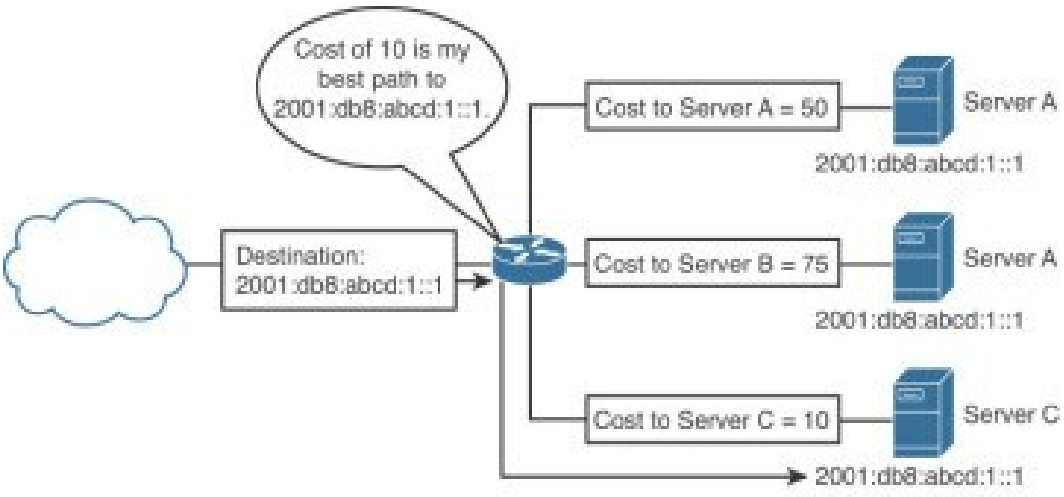
Multicast -osoitetta käytetään ryhmälähetykseen. Multicast -osoite on tarkoitettu laitteiden väliseen viestintään, jossa halutaan lähettää sama yksittäinen viesti useammalle vastaanottajalle. Multicast -osoitteen käyttö oli jo IPv4:n aikaan tehokkaampi tapa, kuin jokaiselle laitteelle erikseen saman sisällön viestiminen erikseen. Ryhmälähetykseen käytetään hyödyksi sille varattuja osoitealueita, esim. IPv4 -verkossa D -luokka on tälle varattu, IPv6 -versiossa vastaavasti FF00:: /12 -osoitetta. (Mooc.fi)

IPv6 -version multicast -osoite määrittelee ryhmän laitteita, jotka tunnetaan ryhmälähetyksen laitteina. Aina, kun multicast -osoitteeseen lähetetään paketti, lähettäjän osoite on unicast -osoite. Multicast -osoite itsessään ei voi koskaan olla lähettäjän osoite. IPv6 -versiossa ei ole IPv4 -version broadcast -osoitetta (yleislähetys), vaan käytössä on well-known- ja solicited-node -osoitteet.

4.4 Anycast

Anycast –osoitetta käytetään erikoistapauksissa, kun unicast- tai multicast -osoitteiden käyttö ei sovi käyttötarkoitukseen. Osoitteella voi olla useita vastaanottajia, mutta viesti päätyy vain yhdelle vastaanottajalle. Lähettäjän kannalta ei ole merkitystä, kuka vastaanottajista viestin saa. Anycast -osoitteen käyttö sopii esimerkiksi internetin nimipalvelun käyttöön. Lähettäjä haluaa osoitetiedon nimiosoitteesta ja lähettää kyselyn usealle eri nimipalvelimelle, mutta vain yhden niistä tarvitsee vastata ja se riittää kyselyn lähettäjälle. (Mooc.fi)

Anycast -osoitteella ei ole erityistä tunnusmerkkiä osoitteen arvossa. Osoite voi olla samankaltainen unicast -osoitteen kanssa, mutta jokaisen anycast -osoitteen jakeluun vastaavan koneen (yleisimmin palvelimen) tulee sisältää sama osoitetieto.



KUVA 7. Anycast osoitteen ryhmä sisältää kuvan esimerkissä eri palvelimia. (Cisco, 2017)

Anycast -osoitteen toimivuus perustuu reitittimen tietoon siitä, mikä anycast -osoitteeseen vastaava laite on lähimpänä ja nopeiten saatavilla. Reititin siis huolehtii siitä, ettei anycast -osoitteeseen lähetetty viesti mene jokaiselle vastaanottajalle, kuten multicast -osoitteissa. (Cisco, 2017)

4.5 Lähimmäisten laitteiden etsintä

IPv4 versiossa yhdyskäytägä (gateway) reititin ylläpiti ARP -taulukkoa (Address Resolution Protocol), jonka avulla reititin tunnisti päätelaitteet MAC-osoitteesta ja tunnisti niiden IP-osoitteet, joka auttoi pakettien reitittämisessä. IPv6 versiossa käytetään NDP -protokollaa (Neighbor Discovery Protocol). NDP -protokollassa reitittimet ja päätelaitteet lähettävät toisilleen Neighbor Discovery (ND) viestejä, joiden avulla voidaan päätellä naapurin linkkitason osoitteet, jotka sijaitsevat yhdistetyssä linkissä. (Networks, 2021)

ND viesteistä pyytämistä ja mainostamista käytetään tuplaantuneiden unicast -osoitteiden korjaamiseen samassa linkissä. IP -osoitteiden automaattinen määritys on riippuvainen linkkien päällekkäisten osoitteiden korjaamisesta. (Networks, 2021)

5 MIKSI IPV6 ON PAREMPI

5.1 Suurempi osoiteavaruus.

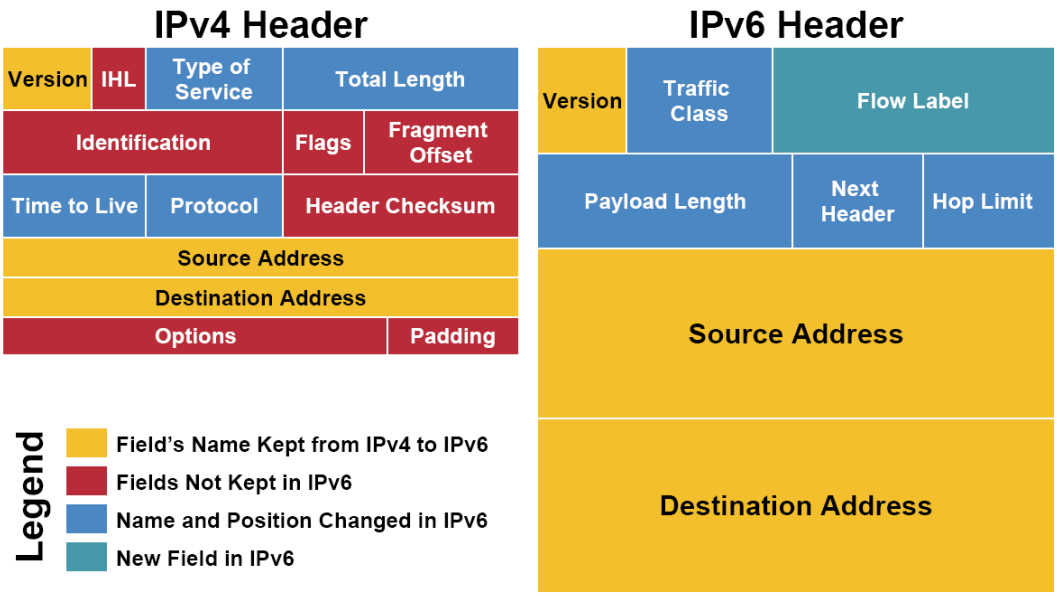
Suuremmalla osoiteavaruudella voidaan poistaa osoitteiden loppumisen uhka, kun laitteita kytketään verkkoon koko ajan suurempi määrä. IPv6 -tekniikassa ylätunnus on muokattu niin, että se on yksinkertaisempi ja nopeampi reitittää. Esimerkiksi IPv6:n struktuurissa osoite jaetaan kahdeksaan (8) osaan, 16 bitin osioihin. Jokainen osio sisältää neljä (4) lukua heksadesimaaleina ja ne erotellaan kaksoispisteellä. Osoitten osioista voidaan poistaa luvut 0, jonka jälkeen osoitteen käsittely on tehokkaampaa. (Tutorialspoint)

5.2 NAT -tekniikan poistuminen

NAT -tekniikan poistamisen jälkeen jokainen laite voi saada oman julkisen osoitteen. Tämän ansiosta yhdistäminen laitteiden välillä on yksinkertaisempaa ja tehokkaampaa. Välistä jää pois esim. aliverkon peiton laskenta, dynaaminen osoitteiden jako DHCP -palvelimelta ja Web Proxy. (Stockebrand, 2007)

5.3 Yksinkertaistettu osoitestruktuuri

Suuren osoitemäärän vuoksi ei ole tarvetta muunneltavalle verkkomaskille, täten verkon konfigurointi on helpompaa ja vähentää virheellisia konfigurointien mahdollisuutta. (Stockebrand, 2007)



KUVA 8. Yleisimmin käytössä oleva TCP/IP -protokollan (verkkokerros) käyttämä kehys. (Alena Kabelová, 2006)

5.4 Yksinkertaisempi osoite konfigurointi

Suurempi osoiteavaruus antaa mahdollisuuden yksinkertaisempaan mekanismiin, tarjoten esim. DHCP:n kaltaisen osoitejaon, mutta ilman kiinteitä tietoja esim. osoitteen laina-ajasta. Kun aiempi DHCP korvataan staattisella mekanismilla, vähenee verkon konfiguroinnin määrä lisää ja vähentää edelleen yleisiä virheita verkossa. (Stockebrand, 2007)

5.5 Yksinkertaistetumpi osoitteen uudelleen numerointi

IPv6:n osoitekonfiguroinilla on täysin mahdollista vaihtaa osoitetta läpi koko verkon, vaikka kesken normaalin toimennon aikana, ilman muutoksia verkossa tai laitteiden uudelleenkäynnistystä. IPV4:ssä jos osoite vaihtui kesken istunnon, täytyi muutoksia tehdä läpi verkon ja tämä vei paljon aikaa ja aiheutti myös tietoturvallisia riskejä. (Stockebrand, 2007)

5.6 Broadcast:n poistaminen

Koska IPv6:ssa multicast toimintaa on laajennettu ja parannettu, ei tarvita enään IPv4:n käyttämää broadcast -toiminnetta. Tämän muutoksen ansiosta IPv6:ssa ei ole enään samaa tietourvallista vaaraa, kuten IPv4:n käyttämässä broadcast tekniikassa oli. Näitä oli esim.”ping bounce” ja ”smurf” palvelunestohyökkäykset. Silti kaikki hyödylliset toimet on saatu pidettyä IPv6:n mukana, joita IPv4 käytti.

Parannellun multicast -tekniikan avulla on myös vähenentty turhaa liikennettä ja kuormaa verkosta, kun broadcast tyylistä jakelua jaetaan vain tarvittaville osoitteille. (Guide, 2005)

5.7 Yksinkertaisempi ylätunniste

IPv6 -osoitteen ylätunnistetta/struktuuria on yksinkertaistettu (katso kuva 8.) Sitä on muokattu niin, että esim. Time to live ja Flags osiot on poistettu. Time to Live tarkoittaa arvoa, jota reitittimet seuraavat paketin saapuessa. Sen arvo vähenee aina yhdellä, kun se lähetetään eteenpäin. Arvon laskiessa nollaan (0), paketti tiputetaan pois. Tällä estettiin IPv4 verkossa eksyneet paketit, jotka turhaan kuormittavat reititystä. Flags osiolla tunnistettiin paketista, saako sitä jakaa osiin vai ei. (Guide)

6 IPV6 SAVONIAN TIETOVERKOSSA

IPV6-osoitteiden käyttövalmius on ollut Savonian tietojärjestelmässä noin 10 vuoden ajan. Osoitteistusta on sallittu joillekin laitteille ja käyttöön tietyillä vlaneilla sisäverkossa, mutta kampustoimintojen keskittyessä ja monien opetustilojen muututtua lähinnä opiskelijoiden omien tietokoneiden käyttöön perustuvaksi, on tällä hetkellä pääosin IPV4-osoitteistus käytössä. Käyttöönotossa ja käyttökokemuksessa ei ole ollut isompia ongelmia.
Laajempikin IPV6-käyttö myös Savonian reitityksessä ulkoverkkoon päin ja nimipalvelussa on mahdollista.

7 LÄHTEET

Alena Kabelová, and Libor Dostálek. 2006. *Understanding TCP/IP.* s.l. : Packt Publishing, Limited, 2006. 9781847190567.

Battu, Daniel. 2014. *New telecom networks : enterprises and security.* s.l. : London, England ; Hoboken, New Jersey : ISTE 2014, 2014. 1-119-00792-5.

CCNA. Study-CCNA. *UDP Explained.* [Online] [Viitattu: 2. June 2021.] https://study-ccna.com/udp-explained/.

CertBros. 2020. IPv6 Addresses Explained | Cisco CCNA 200-301. *Youtube.* [Online] 14. July 2020. [Viitattu: 20. May 2021.] https://www.youtube.com/watch?v=irhS0ASkvy8.

Cisco. Cisco. *IP multicast Routing Configuration Guide, CIsco IOS Release 15.2(2)E (Catalyst 3750-X and 2560-X Switches).* [Online] [Viitattu: 5. May 2021.] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_01.html.

—. 2017. Cisco Press. *IPv6 Address Representation and Address Types.* [Online] 3. October 2017. [Viitattu: 24. May 2021.] https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4.

Cloudflare. 2019. What is the Internet Protocol (IP)? *www.cloudflare.com.* [Online] Cloudflare, Inc., 2019. https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/.

Edwards James, Bramante Richard. 2009. *Networking self-teaching guide OSI, TCP/IP, LANs, MANs, WANs, implementation, management, and maintenance.* s.l. : John Wiley & Sons, Incorporated, 2009.

Google. Google IPv6. *Staticstic.* [Online] [Viitattu: 5. May 2021.] https://www.google.com/intl/en/ipv6/statistics.html.

Guide, Free CCNA study. Free CCNA Study Guide. *13-1 IPv6 Introduction.* [Online] [Viitattu: 23. April 2021.] https://www.freeccnastudyguide.com/study-guides/ccna/ch13/13-1-ipv6-introduction/.

Guide, Ther TCP/IP. 2005. tcpipguide. [Online] 20. September 2005. [Viitattu: 3. May 2021.] http://www.tcpipguide.com/free/t_IPv6IPv4AddressEmbedding-2.htm.

IANA. IANA. [Online] [Viitattu: 3. May 2021.] https://www.iana.org/.

IETF. 2006. *IPv6 Addressing Architcture.* [Online] February 2006. [Viitattu: 3. May 2021.] https://tools.ietf.org/html/rfc4291.

—. 1998. Internet Protocol, Version 6 (IPv6). *Internet Protocol, Version 6 (IPv6).* [Online] December 1998. [Viitattu: 14. November 2019.] https://tools.ietf.org/html/rfc2460.

Learning Center. *ThousanEyes.* [Online] Cisco. [Viitattu: 20. May 2021.] https://www.thousandeyes.com/learning/techtorials/ipv4-vs-ipv6.

Mooc.fi. Osa 4: Verkkokerros. *Tietoliikenteen perusteet.* [Online] [Viitattu: 30. May 2021.] https://tietoliikenteen-perusteet-2-20.mooc.fi/osa-4/1-IPv4-IPv6.

Networks, Juniper. 2021. TechLibrary. *IPv6 Neighbor Sicovery.* [Online] 26. March 2021. [Viitattu: 3. May 2021.] https://www.juniper.net/documentation/us/en/software/junos/neighbor-discovery/topics/topic-map/ipv6-neighbor-discovery.html.

Stockebrand, Benedikt. 2007. *IPv6 in Practice.* s.l. : Springer, 2007.

TechTarget. 2020. SearchNetworking. *UDP (User Datagram Protocol).* [Online] April 2020. [Viitattu: 3. June 2021.] https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol.

Tutorialspoint. Pv6 - Address Types & Formats. *TutorialsPoint.* [Online] [Viitattu: 5. December 2019.] https://www.tutorialspoint.com/ipv6/ipv6_address_types.htm.