Jaakko Ylituomaala

IPv4-protokollasta siirtyminen IPv6-protokollaan

Opinnäytetyö

Kevät 2011

Tekniikan yksikkö

Tietotekniikan koulutusohjelma

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Koulutusohjelma: Tietotekniikan koulutusohjelma

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Jaakko Ylituomaala

Työn nimi: IPv4-protokollasta siirtyminen IPv6-protokollaan

Ohjaaja: Alpo Anttonen

Vuosi: 2011 Sivumäärä: 59 Liitteiden lukumäärä: 1

Tässä työssä tutkitaan IPv6-osoiteavaruutta, sekä IPv6-protokollan yhteensopivuutta IPv4-protokollan kanssa. Työssä käydään läpi myös yleisimmät IPv4-yhteensopivat IPv6-reititysmenetelmät.

Tutkimuksessa tutustutaan pääpiirteittäin IPv4-osoiteluokkiin, itse osoitteisiin ja IPv4-headeriin. IPv4 osoiteryhmiä on viisi, jotka ovat A, B, C, D ja E. Lisäksi luodaan katsaus IPv4-headerin eri osioihin ja tutustutaan niiden käyttötarkoituksiin. Työssä käydään läpi myös osittain NAT-toiminto.

Tutkimuksen päätarkoitus on tutkia Internet Protocol version 6 -protokollaa eli IPv6 -protokollaa ja sen toimintoja. IPv6-protokollassa on täysin uudenlainen osoiteavaruus, joka on pituudeltaan 128 bittiä. IPv6-osoitteita voidaan myös supistaa ja näin tehdä osoitteista ihmisystävällisempiä. IPv6-protokollasta löytyy kolmea erilaista osoitetyyppiä, Unicast, Anycast ja Multicast, joita työssä tutkitaan. Työssä tutkitaan myös IPv6:n aliverkottamista ja verkkomaskeja.

Viimeisessä osiossa tutkitaan ja testataan kolmea erilaista IPv4-yhteensopivaa IPv6 reititysmenetelmää, jotka ovat Tunneling, Dual Stack ja Protocol Translation. IPv6-osoitteistusta ja -reititysmenetelmiä testataan myös käytännössä kahdella Ciscon 1841-reitittimellä ja yhdellä HP-merkkisellä Hubilla.

Avainsanat: NAT, IPv6, IPv4, Header, Dual Stack, Tunneling, Protocol Translation, Unicast, Anycast, Multicast.

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Information Network Technology

Author: Jaakko Ylituomaala

Title of the thesis: Transition from Internet Protocol version 4 to Internet Protocol version 6.

Supervisor: Alpo Anttonen

Year: 2011 Number of pages: 59 Number of appendices: 1

The aim of this thesis was to examine the IPv6- address space and transition from the IPv4 protocol to the IPv6 protocol. Another aim was to examine IPv4-compatible IPv6 routing methods.

First the IPv4 address classes, IPv4 addresses themselves and IPv4 headers were studied. There are five different IPv4 classes which are A, B, C, D and E. Also the different partitions of the IPv4 header and its different purposes of use were examined. As well as the functions of NAT.

The main purpose of this thesis was to examine the IPv6 protocol and its functions. There is a completely new kind of address space in the IPv6 protocol whose length is 128 bits. IPv6 addresses can also be shortened and thus the IP addresses are more user-friendly. There are three types of addresses in the IPv6 protocol which are Unicast, Anycast and Multicast that were examined in this thesis. IPv6 sub netting and network masks were also examined.

In the last chapter the three different kinds of IPv4-compatible IPv6 routing methods which are Tunnelling, Dual stack and Protocol translation were researched. IPv6 addressing and routing methods were also tested in practise with two Cisco’s 1841 routers and one HP’s hub.

Keywords: NAT, IPv6, IPv4, Header, Dual Stack, Tunneling, Protocol Translation, Unicast, Anycast, Multicast.

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

ACL	Access Control List, Lista käyttäjistä tai prosesseista jotka saavat palomuurilta luvan päästä läpi.
AfriNIC	African Network Information Centre, organisaatio joka vastaa Afrikan alueen IP-osoitteista. (RIR)
ALG	Application-Level Gateway, protokollamuunnos-tekniikka.
API	Application Programming Interface, toimii porttina erilaisten ohjelmien välillä ja helpottaa niiden käyttöä.
APNIC	Asia-Pasific Network Information Centre, organisaatio joka vastaa Aasian alueen IP-osoitteista. (RIR)
ARIN	American Registry for Internet Numbers, organisaatio joka vastaa Amerikan ja osan Karibian aluiden IP-osoitteista. (RIR)
CATNIP	Common Architecture for the Internet.
CIDR	Classless Interdomain Routing, tarkoittaa verkkomaskin lyhennettyä ja desimaalista muotoa.
CLNP	Connectionless Network Protocol, internetprotokolla.
DHCPv6	Dynamic Host Configuration Protocol version 6, jakaa IPv6-osoitteita verkkolaitteille.
DNS	Domain Name System, nimeämispalvelu, joka muuntaa verkkotunnukset IP-osoitteiksi.
FQDN	Fully Qualified Domain Name, verkkoaluenimi, joka sisältää myös IPv6-osoitetiedot.
HTTP	Hypertext Transfer Protocol, selainten ja WWW-palvelimien käyttämä tiedonsiirtoprotokolla.

IANA	Internet Assigned Numbers Authority, organisaatio joka vastaa maailmanlaajuisesti IP-osoitteista.
ICMPv4	IPv4 Internet Control Message Protocol, verkkolaitteiden käyttämä menetelmä virheilmoituksien lähetykseen.
IETF	Internet Engineering Task Force, internetprotokollista vastaava osrganisaatio.
IPSec	IP Security, protokolla joka mahdollistaa verkkoliikenteen salauksen ja käyttäjän tunnistamisen.
IPX	Internetwork Packet Exchange, internetprotokolla.
IPv4	Internet Protocol version 4, internetprotokolla jonka avulla liikennöidään internetissä.
IPv6	Internet Protocol version 6, uusi internetprotokolla jonka avulla liikennöidään internetissä.
IS-IS	Intermediate System to Intermediate System, reitityspro-tokolla, joka on suunniteltu kuljettamaan informaatiota te-hokkaasti verkossa.
LACNIC	Latin America and Caribbean Network Information Centre, organisaatio joka vastaa Latinalaisen Amerikan ja osan Karibian alueiden IP-osoitteista. (RIR)
MTU	Maximum Transmission Unit, MTU-arvo ilmaisee suurim-man mahdollisen lähetettävän IP-paketin koon.
NAT	Network Address Translation, IPv4-protokollassa käytetty osoitteenmuunnostekniikka
NAT-PT	Network Address Translation Protocol Translation, IP-osoitteiden muunnostekniikka.

NRO	The Number Resource Organization, organisaatio joka edustaa viittä alueellista IP-osoiterekistereistä vastaavaa organisaatiota nimeltään RIR.
NSAP	Network Service Access Point, liityntäpiste internetissä.
PAT	Port Address Translation, IPv4-protokollassa käytetty osoitteenmuunnostekniikka.
Protokolla 41	Tarkoittaa IPv6-kapsulointia.
QoS	Quality of Service, hallitsee ohjelmien, käyttäjien ja data-liikenteen prioriteettejä.
RIPE	Reseaux IP Europeens (European IP Networks), organisaatio joka vastaa Euroopan, Keski-Idän ja osan Keski-Aasian alueiden IP-osoitteista. (RIR)
RIR	Regional Internet Registry, organisaatio joka rekisteröi ja jakaa IP-osoitteita alueellisesti.
SIPP	Simple Internet Protocol Plus.
TCP	Transmission Control Protocol, protokolla jolla luodaan yhteyksiä tietokoneiden kesken internetissä.
UDP	User Datagram Protocol, yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedonsiirron.
TOS	Type of Service, IPv4 Headerin yksi osa-alue.
TUBA	TCP/UDP Over CLNP-Adressed Networks.
TTL	Time to Live, IPv4 Headerin yksi osa-alue.
URL	Uniform Resource Locator, käytetään osoittamaan WWW-sivuja.

(Desmeules 2007.)

1 JOHDANTO

1.1 Työn tausta

Tällä hetkellä käytössä oleva IPv4-osoiteavaruus on loppumaisillaan maailmasta. NRO:n mukaan viimeisetkin IPv4-osoitealueet on jaettu pois. Maailmanlaajuisesti osoitteista vastaa IANA, joka ilmoitti 3. helmikuuta jakavansa loput viisi osoitealuetta AfriNIC:n, ARIN:n, APNIC:n, LACNIC:n ja RIPEN:n kesken. IPv4-protokollan mukaisia IP-osoitealueita ei ole enää jaettavaksi RIReille. IPv4-osoitteiden arvioidaan loppuvan vuoden kuluttua. (Nikulainen 2011.)

IPv6-osoiteavaruuteen siirtyminen on vääjäämätöntä ja tämän on huomannut myös Seinäjoen ammattikorkeakoulu, jonka toimeksiannosta tämä tutkimus tehdään. IPv6 on seuraavan sukupolven internetprotokolla, jossa on paljon suurempi IP-osoiteavaruus kuin IPv4-protokollassa. Tämä mahdollistaa tulevaisuudessa verkkojen lisääntymisen ja kasvun.

IPv6-protokollaan siirtyminen täysin vie vuosia ja sen takia tässä opinnäytetyössä tutkitaan IPv4- ja IPv6-protokollien yhteensopivuutta ja eri toimintoja näiden kahden protokollan välillä.

1.2 Työn tavoite

Työn tavoitteena on tutkia erilaisia IPv6-osoitteistusta, verrata IPv4- ja IPv6-protokollia keskenään, tutkia ja testata IPv4-yhteensopivia IPv6-protokollia. Työssä käytetään protokollien testaukseen apuna kahta Seinäjoen ammattikorkeakoululta saatua Ciscon 1841-reititintä.

Työssä tutustutaan kolmeen erilaiseen reititysmenetelmään, joilla voidaan kommunikoida IPv4- ja IPv6-verkon välillä. Nämä tekniikat ovat Dual stack, Tunneling ja Protocol translation.

Työn lopputavoite on ymmärtää ja osata käyttää IPv6-osoitteita, ja kolmea edellä mainittua reititys menetelmää IPv4- ja IPv6-verkkojen välillä.

1.3 Työn rakenne

Tässä työssä on myös hyvä tuntea IPv4-protokolla, joten ensimmäisenä käsitellään osittain IPv4-osoiteavaruutta ja sen eri luokkia. Tässä osiossa tutkitaan myös IPv4 Headeria ja NAT-toimintoa.

Toiseksi käydään läpi IPv6-osoiteavaruutta ja tutkitaan millainen rakenne on IPv6-osoitteella. Osiossa tutkitaan myös IPv6 Headeria. Lisäksi katsotaan millaisia IPv6-osoitetyppejä on olemassa, ja miten osoitteita voidaan supistaa käyttäjäystävällisemmiksi.

Kolmannessa osiossa tutkitaan kolmea eri IPv6-reititysmenetelmää IPv4- ja IPv6-verkon välillä.

Neljännessä vaiheessa testataan opittuja reititysmenetelmiä kahdella Ciscon 1841-reitittimellä. Tähän osioon sisältyy Ciscon reitittimen eri komentoja, joilla saadaan asetettua reitittimelle IP-osoitteita ja erilaisia reititysasetuksia.

Lopuksi kerrotaan tutkimuksen tulokset ja arvioidaan tutkimus kokonaisuutena.

2 INTERNET PROTOCOL VERSION 4

2.1 Yleistä

Internet Protocol version 4 eli IPv4 perustuu 32-bittiseen osoitejärjestelmään, joka pystyy teoriassa kattamaan kokonaisuudessaan 4 miljardia, tarkalleen 4 294 967 296, verkkoasemaa koko Internetissä. Todellisuudessa osoitejärjestelmä pystyy kattamaan vain 3,2 – 3,3 miljardia verkkoasemaa koko Internetissä johtuen IP-osoitteiden luokittelusta. (Cisco Systems 2006, 1.)

2.2 IPv4-osoitteet

Tämä 32-bittinen järjestelmä jaettiin alunperin viiteen hierarkiseen luokkaan, jota johtaa IANA. Kolme ensimmäistä luokkaa, A, B ja C luokka, ovat käytettävissä globaaleina ainutlaatuisina unicast IP -osoitteina. Nämä luokat asetettiin käyttäjille, joilla on erimittaisia verkkomaskeja. Verkkomaski on sarja 1 bittejä, jotka muodostavat IP-osoitteen verkko-osan. (Desmeules 2007, 6.) Kaksi viimeistä luokkaa ovat D ja E-luokka. Näiden luokkien osoitteet on varattu kokeelliisiin ja multicast tarkoituksiin (Desmeules 2007, 7). Taulukossa 1 näkyy miten osoitteet on jaettu luokittain.

Taulukko 1. Julkiset ja yksityiset IP-osoitteet. (Publick and Private IP Address Classes range [viitattu 22.03.2011].)

Public IP Address Classes range

Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	1-126	**0**0000001-01111110	0.0.0.0	126.255.255.255	**0**	**N.H.H.H**	255.0.0.0
B	128-191	**10**000000-10111111	128.0.0.0	191.255.255.255	**10**	**N.N.H.H**	255.255.0.0
C	192-223	**110**00000-11011111	192.0.0.0	223.255.255.255	**110**	**N.N.N.H**	255.255.255.0
D	224-239	**1110**0000-11101111	224.0.0.0	239.255.255.255	**1110**		
E	240-255	**11110**000-11111111	240.0.0.0	254.255.255.255	**11110**		

Note: Class A address **127.0.0.0** - **127.255.255.255** cannot be used and is for **LOOPBACK** and diagnostic

Private IP Address Classes range

Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	10	**0**0001010	10.0.0.0	10.255.255.255	**0**	**N.H.H.H**	255.0.0.0
B	172	**10**101100	172.16.0.0	172.31.255.255	**10**	**N.N.H.H**	255.255.0.0
C	192	**110**00000	192.168.0.0	192.168.255.255	**110**	**N.N.N.H**	255.255.255.0

2.3 NAT, Network Address Translation

Seuraavassa tarkastellaan NAT-toimintoa ja sen eri muotoja.

2.3.1 Yleistä

NAT syntyi, kun huomattiin IP-osoitteiden olevan loppumassa maailmasta, jossa Internet kasvoi yhtäkkiä odottamattoman paljon. Tarkkaa lukumäärää verkossa oleville verkkolaitteille ei tiedetä mutta arviolta se on 100 miljoonaa isäntälaitetta ja yli 350 miljoonaa käyttäjää koko Internetissä. Kasvuvauhti on ollut niin kova, että Internet kaksinkertaistaa kokonsa joka vuosi. (Cisco Systems 2006, 1.)

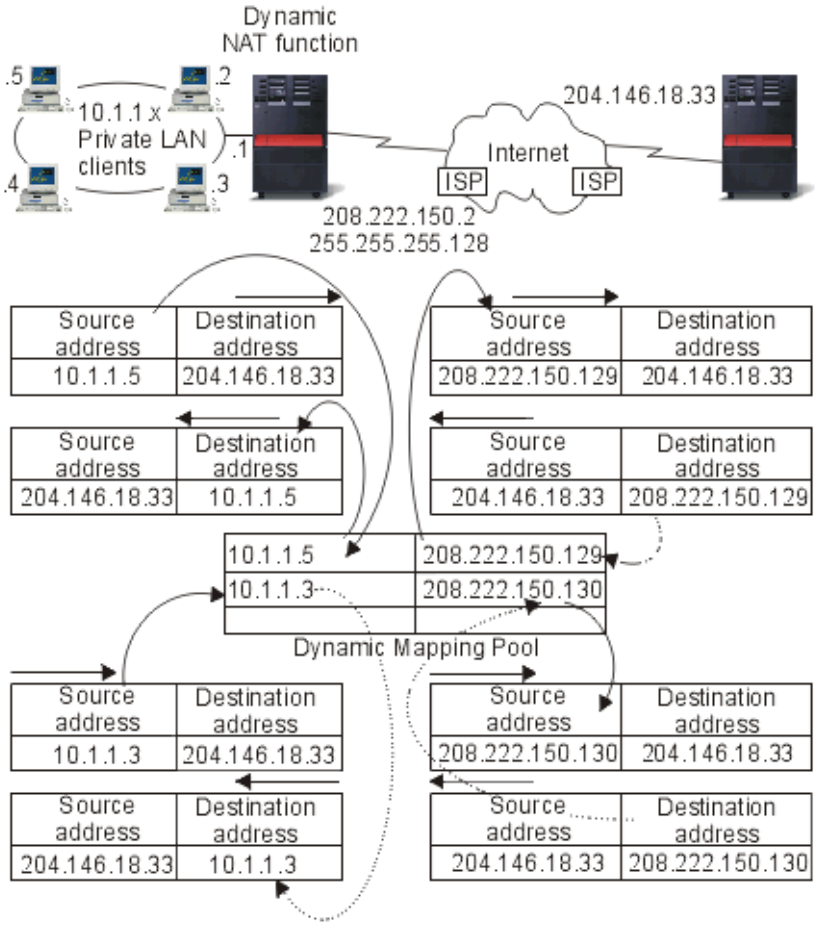
2.3.2 Toiminta

NAT-tekniikka mahdollistaa reitittimen olon ”agenttina” Internetin ja paikallisen verkon välissä. Tämä tarkoittaa sitä, että riittää vain yksi julkinen IP-osoite monelle sisäverkon yksityiselle osoitteelle eli monta yksityistä sisäverkon konetta pystyy liikennöimään Internetissä yhdellä julkisella IP-osoitteella. Lisäksi NAT lisää turvallisuutta ja hallittavuutta. (Cisco Systems 2006, 2.)

2.3.3 Dynaaminen NAT

Kun dynaaminen NAT on käytössä, voidaan muodostaa yhteys ainoastaan yksityisestä verkosta julkiseen verkkoon. Muodostettaessa ulkoinen yhteys jokaiselle yhteydelle noudetaan julkinen IP-osoite osoitealtaasta. Jokainen yhteys saa ainutlaatuisen julkisen osoitteen. Yhtäaikaisia yhteyksiä on mahdollista muodostaa niin monta kuin on IP-osoitteita osoitealtaassa. Dynaaminen NAT mahdollistaa yhteyden muodostamisen Internettiin dynaamisen NAT-osoitteen kautta. (Dynamic NAT. [viitattu 23.03.2011].)

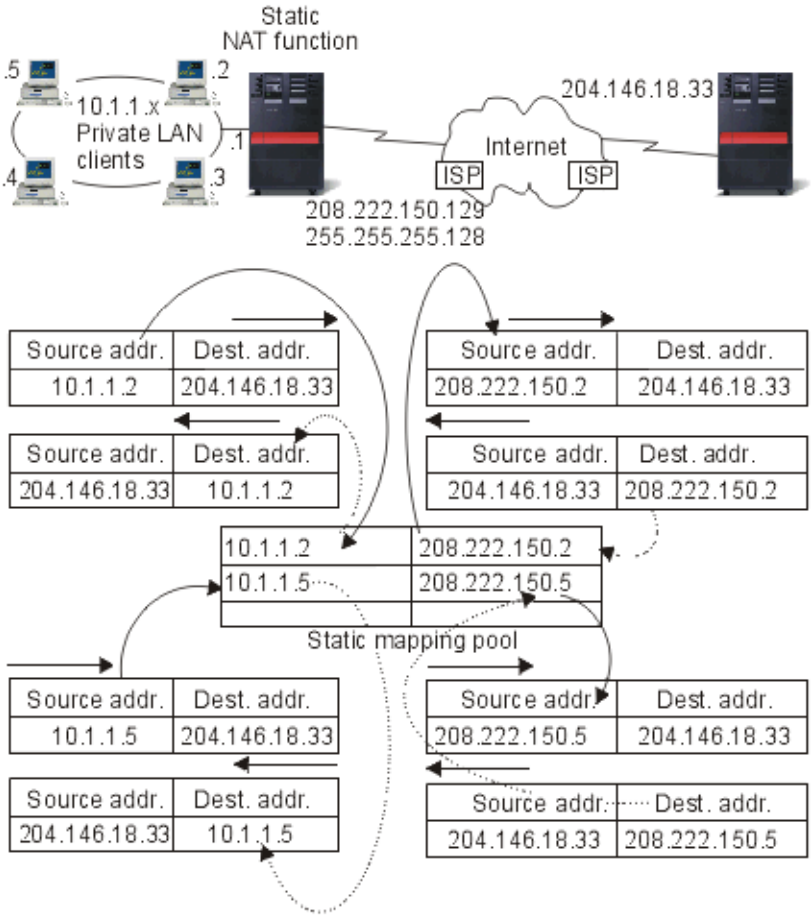
Dynaamisen NAT:in yksi muoto on Overloading, jota kutsutaan myös PAT-tekniikaksi. PAT-tekniikan toiminta perustuu siihen, että se tarvitsee vain yhden tai muutaman julkisen IP-osoitteen eikä paljon julkisia IP-osoitteita. Tähän on syynä se, että PAT erottelee eri istuntoja verkossa porttinumeron perusteella. Jos esimerkiksi käyttäjä haluaa päästä Internettiin sisäisestä verkosta, käyttäjä lähettää pyynnön reitittimelle, jossa NAT-protokolla on käytössä. Tämän jälkeen reititin kääntää paketin IP-osoitteen ja porttinumeron käyttämään reitittimen julkista IP-osoitetta ja samaa porttinumeroa, jos porttinumeroa ei ole varattu jonkun muun käyttäjän toimesta julkisessa verkossa. Tämän muunnoksen jälkeen reititin välittää paketin kohteeseen. Kaikki NAT-porttikartoitukset on tallennettuna reitittimen NAT-tauluun. (DiNicolo 2007.) Kuvassa 1 on esitetty dynaamisen NAT:in toiminta.



Kuva 1. Dynaaminen NAT-toiminta. (Dynamic NAT [viitattu 22.03.2011].)

2.3.4 Staattinen NAT

Staattinen NAT tarkoittaa yksinkertaisesti yhden yksityisen osoitteen ja yhden julkisen osoitteen yhdistämistä. Yhdellä yksityisellä/sisäisellä IP-osoitteella on koko ajan yksi ja sama julkinen/ulkoinen IP-osoite käytössä. Staattisesta NAT-tekniikasta on erityisesti hyötyä, jos yksityisen verkon laitteeseen täytyy päästä käsiksi julkisesta verkosta päin. (Static NAT [viitattu 23.03.2011].) Kuvassa 2 on esitetty staattisen NAT:in toiminta.



Kuva 2. Staattinen NAT-toiminta. (Static NAT [viitattu 23.03.2011].)

2.4 IPv4 Header

Seuraavassa tarkastellaan IPv4 Headerin rakennetta ja sen toimintaa.

2.4.1 Yleistä

IP-paketit kuljetetaan verkossa erilaisten linkkikerrosten yli, esimerkiksi Ethernet (10 Mbps), Fastethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), ja monen muun linkkikerroksen teknologian kautta. Jokaisella linkkikerrosteknologialla on omanlaisensa linkkikerroskehys, joka kuljettaa IP-paketteja. IP-paketilla on kaksi olennaista osaa:

- IP Header

- IP Header sisältää kaikki reitittimen tarvitsemat lähetys- ja vastaanottotiedot. IP Header sisältää tiedot kuten lähettäjä, vastaanottaja, kuljetusprotokolla ja monia muita tietoja. Headerin pituus vaihtelee 20 ja 60 tavun välillä. Suurimmillaan se voi kuitenkin olla 65 535 tavua. Tosin kaikki järjestelmät eivät osaa käsitellä niin suurta headeria, joten suurin mahdollinen toimiva koko voi olla 576 tavua. (Young 2006; Desmeules 2007, 41.)

- Payload
  - Payload tarkoittaa lähetettyä informaatiota eli dataa. (Young 2006; Desmeules 2007, 41.)

Kuvassa 3 on esitetty IP-paketin rakenne.

Kuva 3. IP-paketti. (Young 2006.)

2.4.2 IPv4 Headerin rakenne

IPv4 Header on IP-paketin informaatio-osa, jonka perusteella reititin osaa kuljettaa IP-paketin oikeaan osoitteeseen. IPv4 Header sisältää seuraavanlaiset tiedot:

- Version (4-bit)
  - Tämä osa kertoo internetprotokollan version, joka on tällä hetkellä versio 4. (TCP/IP Suite [viitattu 23.03.2011].)

- Header Length (4-bit)
  - Tämä osa kertoo Internet headerin pituuden 32 bittisinä sanoina. (TCP/IP Suite [viitattu 23.03.2011].)

- TOS (8-bit)

- Tämä arvo osoittaa halutun laadun palvelulle. TOS tarkoittaa sitä että kun kuormitus on kovaa verkossa ja paketilla on tietyn rajan ylittävä prioriteettiluokitus, niin se käsitellään ensimmäisten joukossa verkkoliikenteessä. (TCP/IP Suite [viitattu 23.03.2011].)

- Total Length (16-bit)
  - Tavuina ilmoitettu IP-paketin pituus, johon sisältyy internet-header ja itse data. Tämä osa sallii IP-paketin pituudeksi enintään 65 535 tavua. Suurimmat osat verkoista ja niiden laitteista eivät tue enintään kun 576 tavua suuria IP-paketteja. (TCP/IP Suite [viitattu 23.03.2011].)

- Identifier (16-bit)
  - Lähettäjän asettama osio, jonka tiedot auttavat kasaamaan IP-paketin osat yhteen. (TCP/IP Suite [viitattu 23.03.2011].)

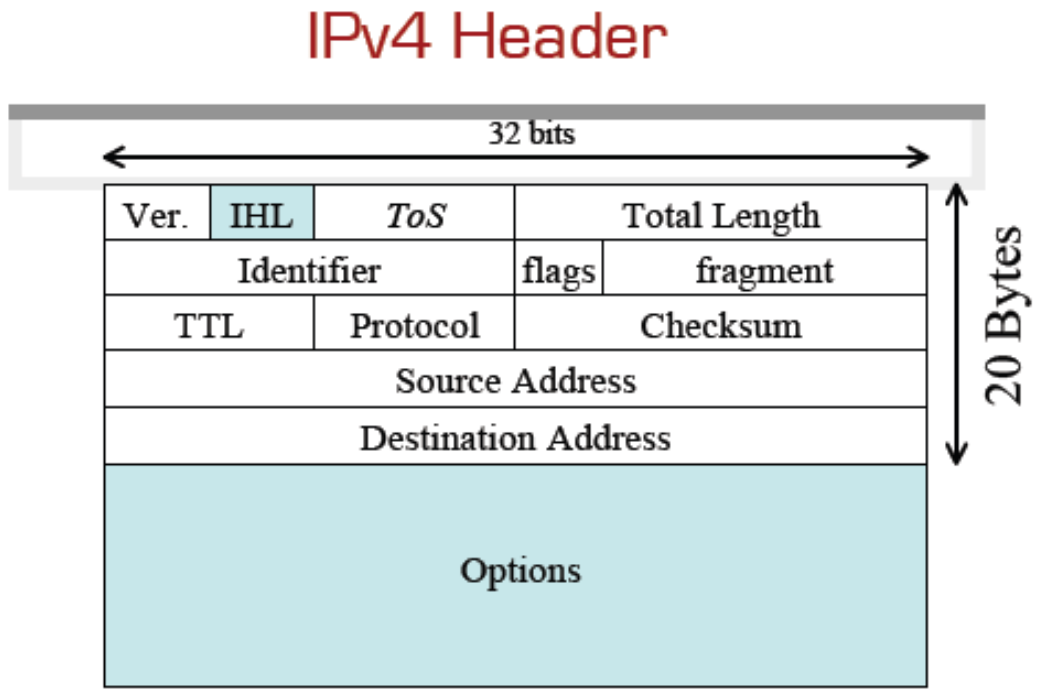
- Flags (3-bit)
  - Osio sisältää kolme bittiä:
    - Bitti 0 on varattu ja sen täytyy olla 0.
    - Bitti 1 on ”Don’t fragment” bitti, jolla on arvot:
      - 0, joka tarkoittaa ”May fragment”.
      - 1, joka tarkoittaa ”Don’t fragment”.
    - Bitti 2 on ”More fragments” bitti, jolla on arvot:
      - 0, joka tarkoittaa ”Last fragment”.
      - 1, joka takoittaa ”More fragments”. (TCP/IP Suite [viitattu 23.03.2011].)

- Fragment Offset (13-bit)

    - Osoittaa mihin mikäkin osa kuuluu IP-paketissa. (TCP/IP Suite [viitattu 23.03.2011].)

- TTL (8-bit)
    - TTL osoittaa ajan kuinka kauan IP-paketti saa olla Internetissä. Jos tämän kentän arvo on nolla, niin IP-paketti on tuhottava. (TCP/IP Suite [viitattu 23.03.2011].)
- Protocol Number (8-bit)
    - Osoittaa seuraavan kerroksen protokollan IP-paketille. (TCP/IP Suite [viitattu 23.03.2011].)
- Header Checksum (16-bit)
    - Tätä osiota käytetään virheiden tarkasteluun. Jokainen reititin, joka reitillä tulee vastaan, uudelleenlaskee ja käy läpi tämän osion. (TCP/IP Suite [viitattu 23.03.2011].)
- Source IPv4 Address (32-bit)
    - Lähettäjän IP-osoite (TCP/IP Suite [viitattu 23.03.2011]).
- Destination IPv4 Address (32-bit)
    - Vastaanottajan IP-osoite (TCP/IP Suite [viitattu 23.03.2011]).
- Options
    - Vapaasti valittava kenttä. Sen koko vaihtelee riippuen siitä miten sitä käytetään. (TCP/IP Suite [viitattu 23.03.2011].)

Edellä käydyssä listassa on käyty läpi kaikki IPv4 Headerin osiot. Kuvasta 4 näkee IPv4 Headerin rakenteen.



Kuva 4. IPv4 Header. (Port 2005.)

3 INTERNET PROTOCOL VERSION 6

3.1 Yleistä

IPv4-osoitteiden hurja kulutus johti siihen, että ajateltiin olevan tarpeeksi aikaa suunnitella ja kehittää kokonaan uusi protokolla päivitetyillä toiminnoilla eikä vain keksiä uutta protokollaa, jolla olisi vain suurempi osoiteavaruus. Vuonna 1993 aloitettiin seuraavan sukupolven protokollan etsintä. Kolmea eri vaihtoehtoa tarkasteltiin lähemmin:

- CATNIP tarkoitti CLNP,IP ja IPX-protokollien muuntamista käyttämällä NSAP-osoitteita.
- SIPP tarkoitti IPv4-osoitteen kasvattamista 64 bittiseksi ja kehittämällä sen IP Headeria.
- TUBA tarkoitti IP:n korvaamista yhteydettömällä verkko protokollalla (CLNP), jossa TCP/UDP ja muut ylemmät protokollat voisivat pyöriä CLNP:ssä ylimpänä. (Desmeules 2007, 11.)

Näistä kolmesta vaihtoehdosta valittiin SIPP, jossa olisi osoitteen kokona 128 bittiä. Uusi internetprotokolla sai nimekseen IANA:n toimesta Internet Protocol version 6. (Desmeules 2007, 11.)

3.2 IPv6 ominaisuudet

Seuraavan sukupolven internetprotokollan kehityksessä huomioitiin kaikki aiemmat ongelmat vanhan protokollan kanssa. Suunnittelijat kehittivät protokollasta sellaisen, että se toimisi vanhan protokollan kanssa hyvin ja samalla se olisi paljon monipuolisempi ja kehittyneempi. Seuraavissa kappaleissa käydään läpi suurimmat parannukset IPv6-protokollassa. (Hogg 2007, 4.)

3.2.1 Yksinkertaistettu Header, jossa on enemmän laajennettavuuta

Kun IPv6-protokollaa kehitettiin, tiedettiin, että vanhassa IPv4-protokollassa on monia käyttämättömiä headerin osia. IPv6-protokollassa on paljon yksinkertaisempi header kuin IPv4-protokollassa. Reititys on täten paljon yksinkertaisempaa ja tehokkaampaa ja samalla se säilyttää ominaisuudet, joita tullaan käyttämään paljon useammin. IPv6-headerissa on paranneltu laajennuksien ja asetuksien tukea, mikä mahdollistaa tulevaisuudessa uusien ominaisuuksien lisäämisen IPv6-protokollaan. Tämä tarkoittaa sitä, että IPv6-protokolla pystyy kehittymään tulevaisuudessa täysin uudenlaiseksi protokollaksi, jollaista ei ole vielä edes keksitty. (Hogg 2007, 4.)

3.2.2 Isompi osoiteavaruus

IPv6-header perustuu 64-bittiseen rakenteeseen, jota on 64-bittisten prosessorien helpompi käsitellä ja hardware-pohjaisten laitteiden nopeampi reitittää eteenpäin. Tämän takia IPv6-headerin koko on 40 tavua (5 * 64 bittiä = 320 bittiä = 40 tavua) ja osoitteiden koko on 128 bittiä. Näin ollen IPv6-osoitteita olisi 2^{128}, joka tarkoittaa sitä että osoitteiden määrä on 340 282 366 920 938 463 463 374 607 431 768 211 456. Kun osoitteiden määrä on näin suuri, niin NAT:in käyttö ei pitäisi olla tarpeellista, koska kaikille verkkolaitteille löytyisi oma ainutlaatuinen IP-osoite. Kun IP-osoitteita on näin paljon, mahdollistuu isojen IP-osoitelohkojen jakaminen erilaisille järjestöille. Käyttäen monitasoista osoitteistusta rekistereiden ja internet palveluntarjoajien kautta, saadaan Internetin reititystaulu pysymään pienenä, mikä nopeuttaa IPv6-pakettien reititystä internetissä. (Hogg 2007, 4 & 5.)

3.2.3 Portaaton autokonfiguraatio

Autokonfiguraatio helpottaa IPv6-protokollaa käyttävän verkkolaitteen konfigurointia. Kun IPv6-protokollaa käyttävä verkkolaite yhdistää IPv6-verkkoon, se tekee kyselyn selvittääkseen tiedon ensimmäisestä 64 bitin prefixistä ja ensimmäisestä paikallisesta reitittimestä. Tämän jälkeen verkkolaite käyttää omaa MAC-osoitetta rakentaakseen itselleen IPv6-osoitteeseen viimeisen 64 bitin pituisen osoitteen

loppuosan. Tätä tekniikkaa kutsutaan nimellä EUI-64. Tällä tavalla jokainen laite pystyy automaattisesti rakentamaan itse itselleen IPv6-osoitteen. (Hogg 2007, 5.)

Kaikki verkkolaitteet eivät kuitenkaan välttämättä hyödy autokonfiguraatiosta, koska laitteilla on valmius käyttää DHCPv6-toimintoa tai portaallista autokonfiguraatiota. (Hogg 2007, 5.)

3.2.4 Multicast

Koska broadcast-toiminnot ovat niin tehottomia, IPv6 tukee ainoastaan unicast-, multicast- ja anycast-liikennöintiä verkossa. Multicast toiminnolla jaetaan verkkolaitteet multicast-ryhmiin ja näin ollen paketteja ei lähetetä broadcast -tyylisesti joka koneelle vaan tietylle multicast-ryhmälle. Näin säästetään verkon kapasiteettia eikä synny niin sanottuja broadcast-myrskyjä, jotka voivat tukkia koko verkkoliikenteen. (Desmeules 2007, 24; Hogg 2007, 5.)

3.2.5 Tuki suuremmille IP-paketeille (Jumbograms)

IPv6 käyttää jumbograms-paketteja parantaakseen suorituskykyä näin tehokkaiden verkkojen yli tehokkaille laitteille. Tällaisilla suurilla IP-paketeilla voidaan lähettää paljon dataa verkon yli, kuten palvelimien varmuuskopioita. (Hogg 2007, 6.)

3.2.6 Verkkokerroksen turvallisuus

IPv6-protokollan extension header -ominaisuus mahdollistaa parempien suojausmenetelmien käytön ja antaa enemmän yksityisyyttä verkkoliikenteeseen. Kyseinen ominaisuus johti myöhemmin IPSec:in kehittämiseen. IPSec on osa IPv6-protokollan pääprotokollista. IPSec toimii IP-verkkokerroksessa, joten sillä voidaan salata kaikki ylemmän tason verkkokerrokset, joita ovat TCP, UDP, ICMP. IPSec-protokollaa voidaan käyttää myös suoraan tietokoneiden välillä kuljetusmuotona. IPv6:n IPSec mahdollistaa paljon suuremman varmuuden siitä, että järjestelmät autentikoidaan ennen yhteyden muodostamista. IPSec tarkistaa yhteyden muo-

dostamisen jälkeen, että yhteys on salattu päästä päähän varmistaakseen luottamuksellisuuden ja koskemattomuuden. NAT:in poistaminen käytöstä vähentäisi myös nimettömyyttä verkossa ja näin ollen turvallisuusriskit ovat helpommin tunnistettavissa. (Hogg 2007, 6.)

3.2.7 Yksityisyyden parannukset

IPv6-tietokoneet pystyvät myös konfiguroimaan IP-osoitteensa 64-bittisen käyttäjäosion bitit satunnaiseen järjestykseen. Tällä tavalla kone pystyy varmistamaan loppukäyttäjän yksityisyyden. (Hogg 2007, 6.)

3.2.8 Parannellut QoS:n ominaisuudet

IPv6-header sisältää 20 bittisen flow labelin, joka tunnistaa erikseen jokaisen yhteyden. Vaikka flow labelia ei ole vielä otettu täysin käyttöön, se on jo osoittanut hyvää kehitystä QoS-tekniikalle. (Hogg 2007, 6.)

3.2.9 Anycast

Anycast on uusi osoiteteknologia, joka on ainutlaatuinen IPv6-protokollassa. Anycast mahdollistaa palvelujen tarjoamisen monesta eri lähteestä yhdellä IPv6-osoitteella. Saman IPv6-osoitteen käyttö useassa koneessa kylläkin rikkoo yksittäisen ja ainutlaatuisen IP-osoitteen sääntöä, mutta se tuo myös varmuutta. Anycast-tekniikka antaa yhtiöiden tarjota palveluita monilta eri palvelimilta, jotka on virtuaalisesti tarjottu datakeskuksilta, jotka taas mahdollistavat katastrofivarmuuskopioiden ja liiketoimien ylläpidon. Anycast kasvattaa palvelujen saatavuutta kokonaisuudessaan. (Hogg 2007, 7.)

3.2.10 Liikkuvuus

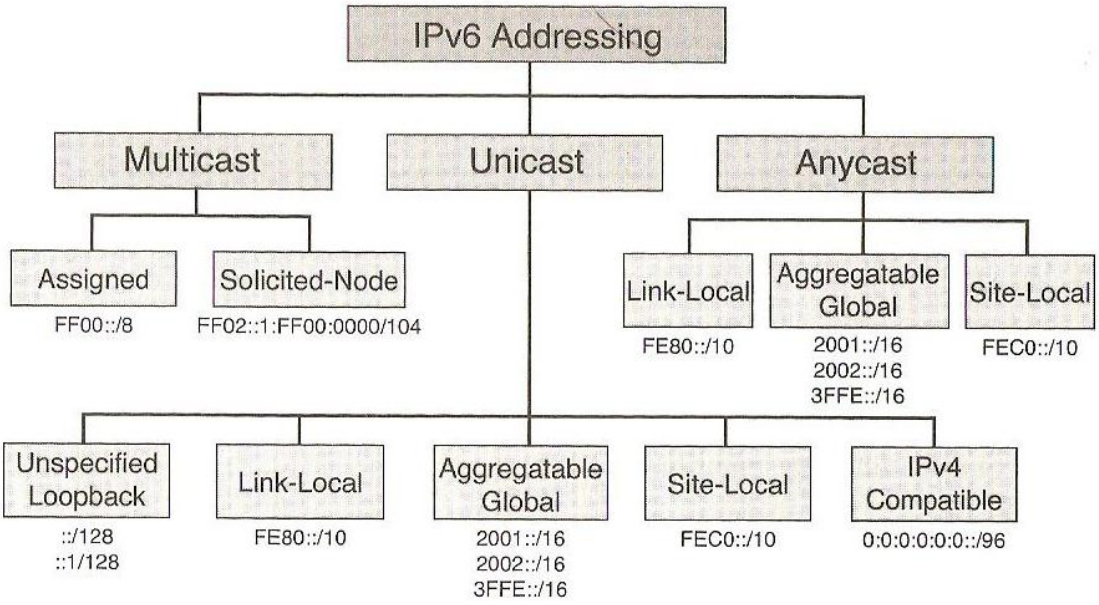
IPv6 käsittelee paljon helpommalla tavalla mobiiliverkkolaitteita. IPv4 tarvitsee paljon monimutkaisemman mobiili IP -rakenteen. IPv6 yksinkertaistaa rakennetta käyttämällä extension header -osaa IPv6-headerissa käsitelläkseen mobiililaitteita silloin, kun ne eivät ole kotiosoitteessa. (Hogg 2007, 7.)

3.3 IPv6-osoitteet

Seuraavassa tarkastellaan IPv6-osoitteistusta ja sen toimintaa. Tarkastellaan myös IPv6-osoitteiden tiivistämistä lyhyempään muotoon, katsotaan millaisia osoiteryhmiä löytyy IPv6-protokollasta ja tutustutaan IPv6-aliverkottamiseen.

3.3.1 Yleistä

Seuraavaksi käydään läpi Internet Protocol version 6 osoitteiden rakennetta ja miten osoitteita voidaan lyhentää. Osoitteet ovat 128 bittisiä ja osoitteella on kaksi osaa. Ensimmäiset 64 bittiä osoitteen alusta merkitsevät osoitteen prefix-osaa ja osoitteen viimeiset 64 bittiä merkitsevät verkkolaitteen Id-osaa. Osoitetyyppejä on kolme eri lajia, unicast, anycast ja multicast. Broadcast-osoiteavaruutta IPv6 ei tunne, vaan broadcasting hoidetaan multicast-osoitteiden avulla. IPv6-osoitteistuksessa, nollat ja ykköset ovat sallittuja missä tahansa kentässä, jos ei toisin mainita. IPv6-osoite esitetään muodossa xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, jossa x on heksadesimaalinen arvo. IPv6-osoitteen yksi solu on 16 bittinen. Tärkeää on myös muistaa, että kun IPv6-osoitetta käytetään selaimessa, täytyy osoite aina merkitä hakasulkujen sisään. Tämä johtuu IPv6-osoitteessa käytettävistä kaksoispisteistä, joilla yleensä erotellaan esimerkiksi porttinumero URL-osoitteessa. (Hinden & Deering 2008.) Kuvassa 5 on esitetty IPv6-osoiteryhmien rakenne.



Kuva 5. IPv6-osoiteryhmien rakenne. (Desmeules 2007.)

3.3.2 IPv6 ja aliverkotus

IPv6-protokollassa verkkomaski esitetään ainoastaan CIDR-muodossa. Vaikka IPv6-osoitteet ilmaistaankin heksadesimaalisena, verkkomaski kuitenkin ilmoitetaan desimaalisena. IPv6-protokollassa ei ole varattuja osoitteita kuten IPv4-protokollassa, eli ei ole varattua broadcast- ja verkko-osoitetta. (Desmeules 2007, 60.) Taulukossa 2 on esitetty prefix- ja verkkomaskiarvoja.

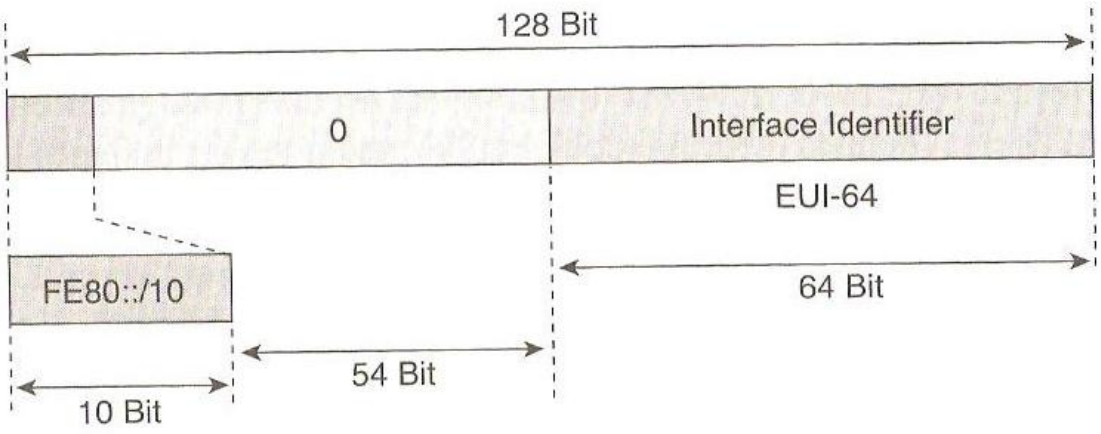
Taulukko 2. Prefix- ja verkkomaskiarvoja. (Desmeules 2007.)

IPv6 Prefix	**Kuvaus**
2001:410:0:1:0:0:0:45FF/128	Esittää aliverkkoa, jossa on ainoastaan yksi IPv6-osoite.
2001:410:0:1::/64	Kyseinen verkko prefix pystyy käsittelemään 2^{64} verkkolaitetta. Tämä on oletus prefix pituus aliverkolle.
2001:410:0::/48	Kyseinen verkko prefix pystyy käsittelemään 2^{16} 64 bitin verkko prefix:iä. Tämä on yhden kohteen oletus prefix pituus.

3.3.3 Osoitetyypit

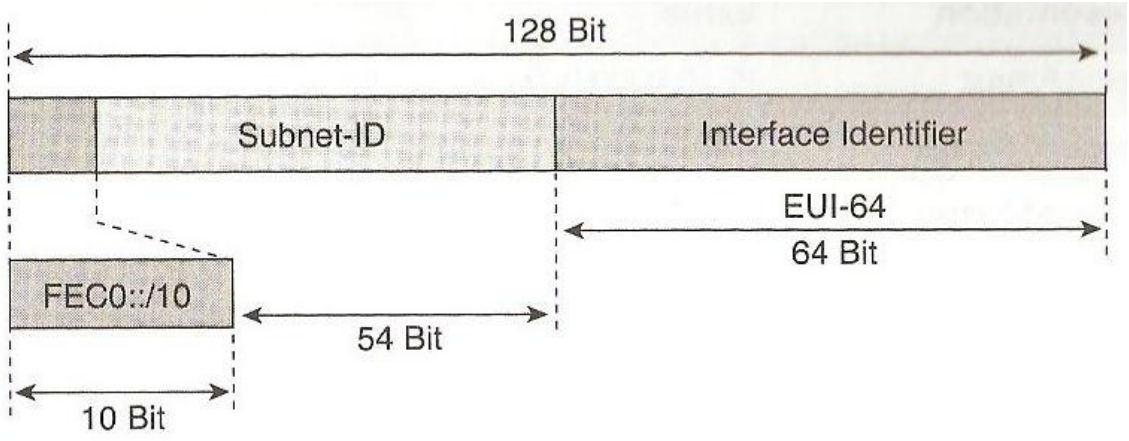
Unicast-osoite on yksittäinen rajapinnan tunniste. Verkkoliittymä voi olla joko yksittäinen kone tai reititin, jonne reititys tehdään mahdollisimman lyhyttä reittiä pitkin. Unicast-osoitteella on monia muotoja. Niitä ovat globaali unicast-osoite, NSAP-osoite, IPX-osoite, site-local-osoite, link-local-osoite ja IPv4-yhteensopiva osoite. IPv6-verkkolaitteilla voi olla vähän tietoa itse IPv6-osoitteen rakenteesta. Verkkolaite voi minimissään luulla, että unicast-osoitteella ei ole sisäistä rakennetta, joten se näkee vain verkkolaitteen osoitteen ja 128 bittiä osoitteessa. (Hinden & Deering 2008.)

Unicast linc-local -osoitetta käytetään verkkolaitteiden välisessä liikennöinnissä, kun laitteet ovat samassa paikallisessa linkissä. Kun IPv6-protokolla on otettu käyttöön verkkolaitteessa, laite saa automaattisesti jokaiseen liitäntäänsä yhden linc-local-osoitteen. Linc-local-osoitetta ei koskaan reititetä aliverkkojen välisessä liikenteessä. (Desmeules 2007, 62.) Kuvassa 6 on esitetty linc-local-osoitteen rakenne.



Kuva 6. Linc-local-osoitteen rakenne. (Desmeules 2007.)

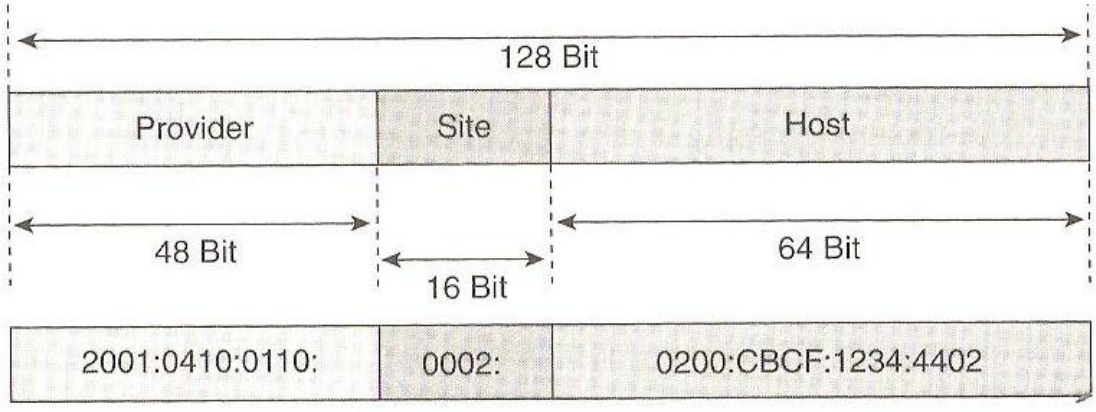
Site-local-osoite on toinen unicast-osoiteavaruuden osa, jota käytetään ainoastaan kommunikoitaessa paikallisessa verkossa. Site-local-osoite täytyy asettaa aina manuaalisesti verkkolaitteeseen. Site-local-osoiteavaruus on samantapainen kuin IPv4-verkon paikallinen privaatti osoiteavaruus. Site-local-osoitteen voi asettaa mihin tahansa verkkolaitteeseen yhdessä kohteessa. Site-local-osoitetta ei koskaan reititetä Internetiin. Osoitteen subnet-ID-osa määrittelee montako aliverkkoa on mahdollista muodostaa jossakin kohteessa, eli kuvan 8 mukaisessa osoitteessa on mahdollista muodostaa 2^{54} aliverkkoa, joiden prefix on 64. (Desmeules 2007, 63.) Kuvassa 7 on esitetty Site-local-osoitteen rakenne.



Kuva 7. Site-local-osoitteen rakenne. (Desmeules 2007.)

Globaali unicast-osoiteavaruus on tarkoitettu liikennöintiin ulkoisessa verkossa eli Internetissä. Globaalit unicast-osoitteet ovat koko IPv6-osoitearkkitehtuurin tärkein

osa. Globaali unicast-osoite on kolmiosainen: prefix-osa, joka saadaan internet palveluntarjoajalta, site-osa ja host-osa. Palveluntarjoajalta saatu prefix pitäisi vähintään olla /48 prefix, jonka on suositellut RFC 3177, IAB/IESG Recommendations on IPv6 Address Allocations to Sites. Site-osa tarkoittaa sitä, että montako aliverkkoa on mahdollista saada kyseiseen osoitteeseen. Tässä tapauksessa prefix on /48 eli aliverkkoja on mahdollista muodostaa 2^{16} , joka on 65 535 aliverkkoa. Osoitteen host-osa määrittelee verkkolaitteen portin ID-numeron. (Desmeules 2007, 65-66.) Kuvassa 8 on esitetty globaalin unicast-osoitteen rakenne.



Kuva 8. Globaalin unicast-osoitteen rakenne. (Desmeules 2007.)

Anycast-osoite on tarkoitettu joukolle verkkolaitteita. Paketti, joka lähetetään anycast-osoitteeseen, menee reititysprotokollan mukaisesti lähimmälle saman anycast-osoitteen omaavalle verkkolaitteelle. Anycast-osoitteet on varattu unicast-osoiteavaruudesta. Kun unicast-osoite asetetaan monelle koneelle, siitä muuttuu anycast-osoite. Verkkolaitteet, joihin osoite asetetaan, täytyy myös asettaa erikseen tietämään, että kyseinen osoite on nimenomaan anycast-osoite. (Hinden & Deering 2008.)

Multicast-osoitteen tunnistaa arvosta FF (11111111), kun taas muut arvot luokittelevat osoitteen unicast-osoitteeksi. Multicast-osoite on verkkolaiteryhmän tunniste. Multicast-osoite mahdollistaa yhden paketin lähetyksen yhdeltä verkkolaitteelta monelle verkkolaitteelle yhtäaikaa. (Hinden & Deering 2008.)

3.3.4 Osoitteiden esittäminen

IPv6-osoitteen voi esittää kolmella eri tavalla. Tavallinen esitystapa on pisin tapa esittää osoite, eli osoitteessa ilmoitetaan kaikki 32 heksadesimaalista lukua. Osoite ilmoitetaan muodossa 0000:0000:0000:0000:0000:0000:0000:0000. (Desmeules 2007, 54.)

Toinen tapa on esittää IPv6-osoite supistetussa muodossa. Supistusmuotoja on kolmea erilaista tapaa. IPv6-osoitteissa on yleistä, että niissä esiintyy paljon nolla-arvoja. Jos osoitteessa esiintyy paljon perättäisiä nolla-arvoja, niin ensimmäisessä supistustavassa nolla-arvot voidaan esittää merkinnällä :: (tuplakaksoispiste). (Desmeules 2007, 55.) Taulukossa 3 on esitetty ensimmäisellä supistustavalla supistettuja IP-osoitteita.

Taulukko 3. Esimerkkejä supistetuista IPv6-osoitteista. (Desmeules 2007.)

Tavallinen esitystapa	**Supistettu muoto**
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::0001
2001:0410:**0000**:1234:FB00:1400:5000:45FF	2001:0410::1234:FB00:1400:5000:45FF
3ffe:**0000:0000:0000**:1010:2a2a:0000:0001	3ffe::1010:2a2a:0000:0001
3FFE:0B00:0C18:0001:**0000**:1234:AB34:0002	3FFE:0B00:0C18:0001:1234:AB34:0002
FE80:**0000:0000:0000:0000:0000:0000**:0009	FE80::0009
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Toisessa supistustavassa osoitteen johtavat nollat supistetaan vain pois. Jos IP-osoitteen 16-bittisen kentän kaikki heksadesimaaliset arvot ovat nollia, niin vähintään yksi nolla täytyy jättää kenttään. (Desmeules 2007, 56.) Taulukossa 4 on esitetty toisella supistustavalla supistettuja IP-osoitteita.

Taulukko 4. Esimerkkejä supistetuista IPv6-osoitteista. (Desmeules 2007.)

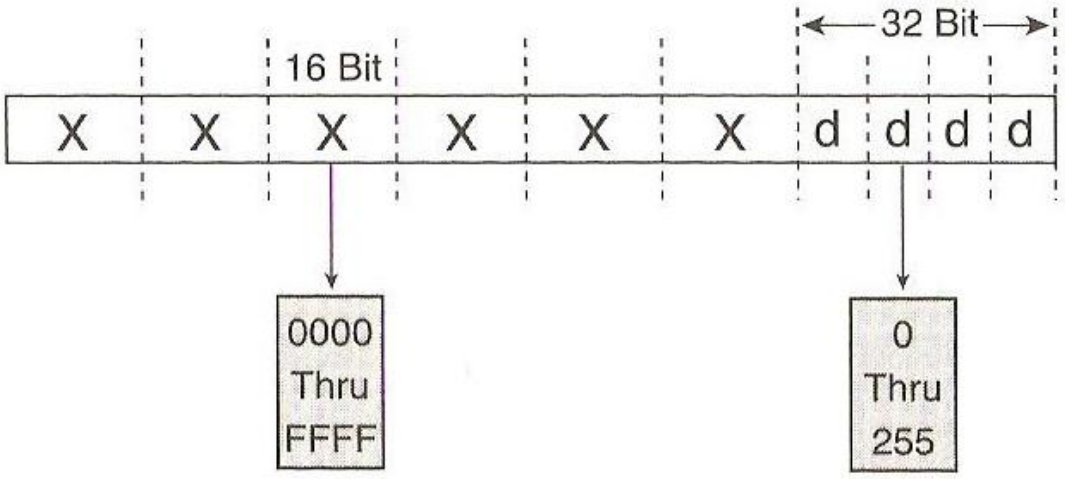
Tavallinen esitystapa	**Supistettu muoto**
0000**:000**0**:000**0**:000**0**:000**0**:000**0**:000**0**:00****0**0	0:0:0:0:0:0:0:0
0000**:000**0**:000**0**:000**0**:000**0**:000**0**:000**0**:00****0**1	0:0:0:0:0:0:0:1
2001:**0**410:**000**0:1234:FB00:1400:5000:45FF	2001:410:0:1234:FB00:1400:5000:45FF
3ffe:**000**0:**000**0:**000**0:1010:2a2a:**000**0:**000**1	3ffe:0:0:0:1010:2a2a:0:1
3FFE:**0**B00:**0**C18:**000**1:**000**0:1234:AB34:**00****0**2	3FFE:B00:C18:1:0:1234:AB34:2
FE80:**000**0:**000**0:**000**0:**000**0:**000**0:**000**0:**000**0:**00****0**9	FE80:0:0:0:0:0:0:9

Kolmannessa supistustavassa käytetään kumpaakin aiemmin esitettyä supistustapaa (Desmeules 2007, 56). Taulukossa 5 on esitetty kolmannella supistustavalla supistettuja IP-osoitteita.

Taulukko 5. Esimerkkejä supistetuista IPv6-osoitteista. (Desmeules 2007.)

Tavallinen esitystapa	**Supistettu muoto**
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::1
2001:**0**410:**0000**:1234:FB00:1400:5000:45FF	2001:410::1234:FB00:1400:5000:45FF
3ffe:**0000:0000:0000**:1010:2a2a:**000**0:**000**1	3ffe::1010:2a2a:0:1
3FFE:**0**B00:**0**C18:**000**1:**0000**:1234:AB34:**000**2	3FFE:B00:C18:1::1234:AB34:2
FE80:**0000:0000:0000:0000:0000:0000:000**9	FE80::9

Kolmas tapa esittää IPv6-osoite on IPv4-yhteensopiva IPv6-osoite. IPv4-osoite on sisällytetty IPv6-osoitteen loppuosaan. Tällaisia osoitteita käytetään vain silloin, kun tiettyjä IPv4-yhteensopivia IPv6-kuljetusprotokollia käytetään. Yhdistelmäosoitteen alkuosa muodostuu kuudesta 16-bittisestä heksadesimaalisesta osasta ja osoitteen loppuosa muodostuu neljästä 8-bittisestä desimaaliosasta. (Desmeules 2007, 58.) Kuvassa 9 on esitetty yhdistelmäosoitteen rakenne.



Kuva 9. Yhdistelmäosoitteen rakenne. (Desmeules 2007.)

On olemassa kahdenlaisia IPv4-yhteensopivia IPv6-osoitteita. Näitä ovat IPv4-yhteensopiva IPv6-osoite ja IPv4-kartoitettu IPv6-osoite. IPv4-yhteensopivaa IPv6-osoitetta käytetään silloin, kun muodostetaan automaattinen tunneli IPv4-verkon yli. IPv4-kartoitettua IPv6-osoitetta käytetään vain paikallisten verkkolaitteiden kesken, kun laitteilla on käytössä dual-stack-toiminto eli laitteilla on sekä IPv4- että IPv6-osoite. (Desmeules 2007, 58.)

Kummallakin yhdistelmäosoitetyypillä on omat esittämistapansa. IPv4-yhteensopiva IPv6-osoite esitetään niin, että osoitteen ensimmäiset 96 bittiä on asetettu nolliksi ja osoitteen loppuosa on 32 bittinen IPv4-osoite. (Desmeules 2007, 58.) Taulukossa 6 on esitetty IPv4-yhteensopivan IPv6-osoitteen esimerkkejä.

Taulukko 6. IPv4-yhteensopivia IPv6-osoitteita. (Desmeules 2007.)

Tavallinen esitystapa	**Supistettu muoto**
0000:0000:0000:0000:0000:0000:206.123.31.2	0:0:0:0:0:0:206.123.31.2 tai ::206.123.31.2
0000:0000:0000:0000:0000:0000:ce7b:1f01	0:0:0:0:0:0:ce7b:1f01 tai ::ce7b:1f01

IPv4-kartoitettu IPv6-osoite esitetään niin, että osoitteen ensimmäiset 80 bittiä on asetettu nolliksi, seuraavat 16 bittiä on asetettu ykkösiksi ja osoitteen loppuosa sisältää 32 bittisen IPv4-osoitteen. (Desmeules 2007, 58.) Taulukossa 7 on esitetty IPv4-kartoitetun IPv6-osoitteen esimerkkejä.

Taulukko 7. IPv4-kartoitettuja IPv6-osoitteita. (Desmeules 2007.)

Tavallinen esitystapa	**Supistettu muoto**
0000:0000:0000:0000:0000:FFFF:206.123.31.2	0:0:0:0:0:FFFF:206.123.31.2 tai ::FFFF:206.123.31.2
0000:0000:0000:0000:0000:FFFF:ce7b:1f01	0:0:0:0:0:FFFF:ce7b:1f01 tai ::FFFF:ce7b:1f01

3.4 IPv6-header

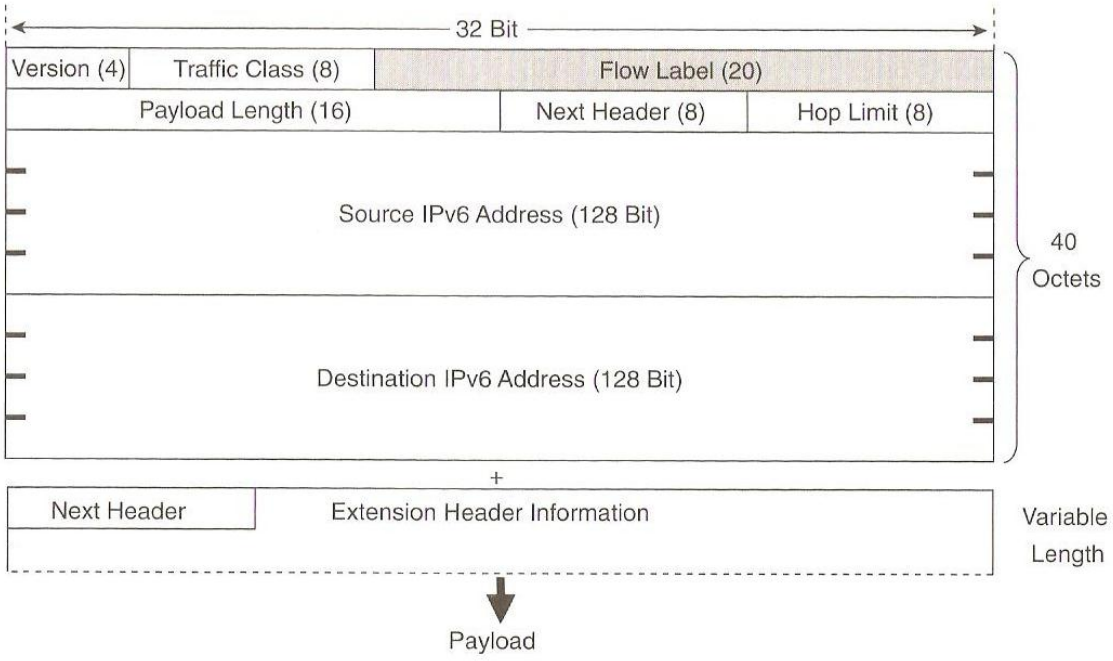
Seuraavassa tarkastellaan IPv6 Headerin rakennetta ja toimintaa.

3.4.1 Yleistä

Tavallinen IPv6-header sisältää kahdeksan kenttää, kun taas IPv4-header sisältää 12 kenttää. IPv6-headerin pituus on 40 tavua. IPv6-header on päivitetty versio IPv4-headerista. (Desmeules 2007, 44.)

3.4.2 IPv6-headerin rakenne

Seuraavaksi käydään läpi IPv6-headerin rakenne ja kerrotaan mikä tehtävä headerin kaikilla osioilla on. Kuvassa 10 on esitetty IPv6-headerin rakenne.



Kuva 10. IPv6-headerin rakenne. (Desmeules 2007.)

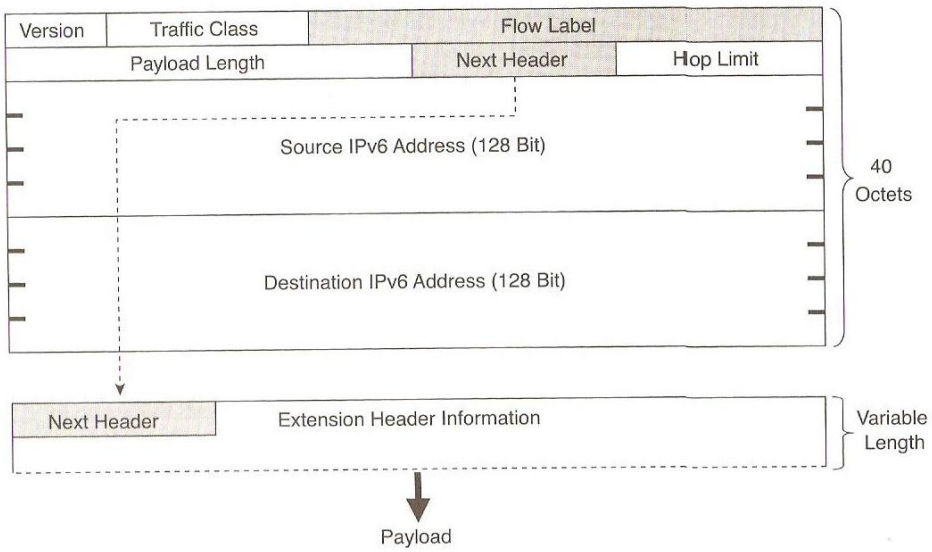
- Version (4-bit)
    - IPv6-version numero. (IPv6, Internet Protocol version 6 1998 – 2011.)
- Traffic Class (8-bit)

- Traffic Class -osio lisää IP-pakettiin tiedon, miten paketti tulisi käsitellä verkkoliikenteessä. (IPv6, Internet Protocol version 6 1998 – 2011.)

- Flow Label (20-bit)
  - Osio on uusi IPv6-headerissa. Osio mahdollistaa IP-pakettien merkitsemisen kuuluvaksi tiettyyn vuohon. Tietyn datavuon paketit saavat näin samanlaisen kohtelun verkon jokaisessa solmussa. (IPv6, Internet Protocol version 6 1998 – 2011.)

- Payload Length (16-bit)
  - Ilmoittaa datan pituuden IP-paketin sisällä. (IPv6, Internet Protocol version 6 1998 – 2011.)

- Next Header (8-bit)
  - Tämä osio ilmoittaa information tyypin, joka seuraa tavallista IPv6-headeria. Tässä osiossa voi olla ylemmän kerroksen protokollia kuten TCP tai UDP, tai se voi olla yksi uusista valinnaisista laajennusheadereista. (IPv6, Internet Protocol version 6 1998 – 2011.) Kuvassa 11 on havainnollistettu kyseinen toiminto.



Kuva 11. Next header -toiminto. (Desmeules 2007.)

- Hop Limit (8-bit)
    - Tämä osio määrittelee hyppyjen määrän, jonka IP-paketti saa maksimissaan kulkea. Hypyn jälkeen arvosta vähennetään aina 1. (IPv6, Internet Protocol version 6 1998 – 2011.)
- Source Address (128-bit)
    - Lähettäjän IPv6-osoite. (IPv6, Internet Protocol version 6 1998 – 2011.)
- Destination Address (128-bit)
    - Vastaanottajan IPv6-osoite. (IPv6, Internet Protocol version 6 1998 – 2011.)

4 IPv4-YHTEENSOPIVAT IPV6-REITITYSMENETELMÄT

4.1 Yleistä

IPv6-protokollaa suunniteltiin alusta lähtien toimimaan IPv4-protokollan kanssa rinnakkain, koska siirtyminen täysin IPv6-protokollaan vie ajallisesti vuosia. Tässä kappaleessa käydään läpi yleisimmät IPv4-yhteensopivat IPv6-tekniikat, jotka ovat nimeltään Dual Stack, Tunneling ja Protocol Translation. Erityisesti nämä tekniikat ovat käytössä Ciscon laitteissa. (Desmeules 2007, 227.)

4.2 Dual Stack

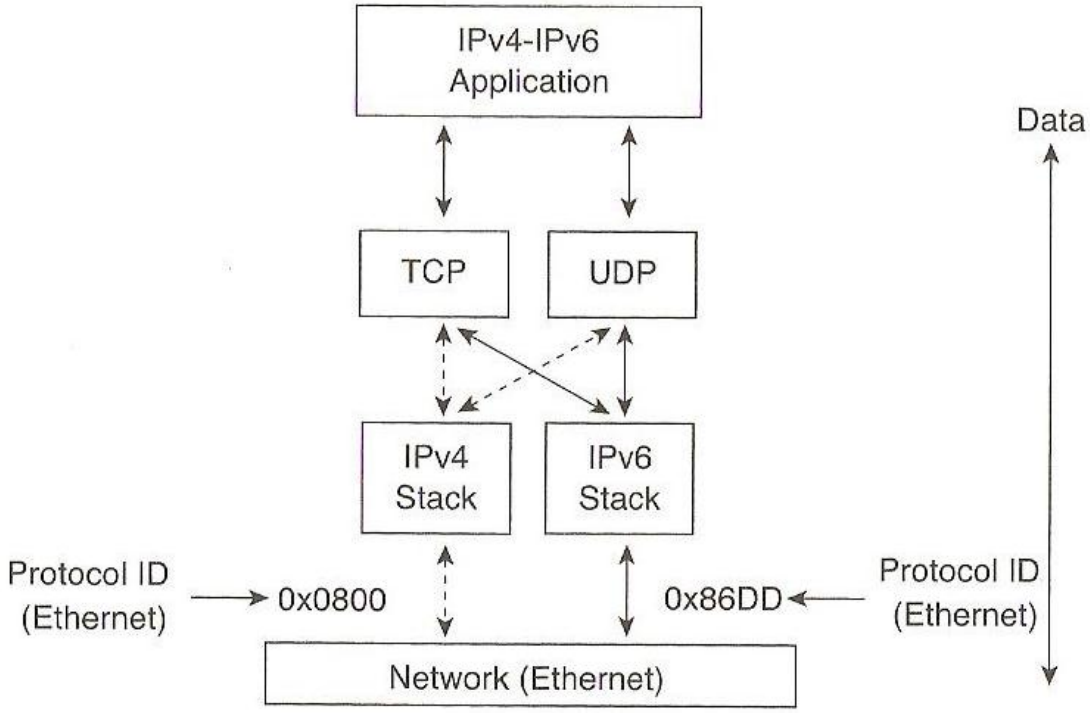
Seuraavassa käydään läpi Dual Stack -tekniikan toiminta.

4.2.1 Yleistä

Dual Stack -menetelmällä on mahdollista käyttää verkkolaitteessa yhtäaikaa IPv4- ja IPv6-protokollaa. Dual Stack luo joustavuutta verkkoon, koska laitteet voivat kommunikoida joko IPv4- tai IPv6-protokollan avulla. (Desmeules 2007, 227.)

4.2.2 Toiminta

Ennen Dual Stack -toiminnon käyttöä täytyy ensimmäisenä muokata IPv4-pohjaiset ohjelmistot tukemaan IPv6-protokollaa. IPv4-ohjelmien API on ohjelmoitu käsittelemään ainoastaan 32 bittisiä IPv4-osoitteita. Protokolla ID IPv4-paketilla on 0x0800 ja IPv6-paketilla 0x86DD. Sen jälkeen kun verkkolaitteiden ohjelmistot on asetettu tukemaan IPv6-protokollaa, ohjelmistot osaavat kutsua oikeaa API-toimintoa, joka tukee 128 bittisiä osoitteita. (Desmeules 2007, 228.) Kuvassa 12 on esitetty sellaisen ohjelmiston toiminta, joka tukee myös IPv6-protokollaa.



Kuva 12. IPv6-yhteensopivan ohjelmiston toiminta. (Desmeules 2007.)

Vaikka ohjelmisto onkin konfiguroitu tukemaan IPv6-protokollaa, itse verkkolaite ei pysty satunnaisesti päättämään kumpaa protokollaa käyttää verkossa liikennöintiin. On olemassa kaksi metodia, joiden avulla verkkolaite saadaan pakotettua käyttämään IPv6-protokollaa, jos sellainen on käytettävissä yhteyden muodostamiseen (Desmeulses 2007, 230.):

- **Käyttäjän manuaalinen syöttö** on ensimmäinen metodi, jota voi käyttää. Tätä menetelmää voidaan käyttää, jos käyttäjä tietää kohdeverkkolaitteen IPv6-osoitteen. Kyseinen metodi ei ole paras mahdollinen päivittäiseen ohjelmistojen käyttöön. Metodia käytetään yleensä vianetsintään. (Desmeulse 2007, 230.)

- **Nimeämispalvelu** on toinen metodi. Tässä menetelmässä konfiguroidaan FQDN-tiedot, jotka sisältävät sekä IPv4- että IPv6-osoitetiedot DNS-palveluun. Tämä tarkoittaa sitä, että DNS-serverit pystyvät jakamaan informaatiota palvelimista ja palveluista joko IPv4- tai IPv6-verkon ylitse. DNS-palvelussa IPv4-osoitteen tunnus on A ja IPv6-osoitteen tunnus on AAAA. (Desmeules 2007, 230.)

Verkkoliikenteessä on olemassa kolme mahdollista DNS-kyselyä:

- **Kysely IPv4-osoitteesta.** Tässä kyselyssä IPv4-protokollaa käyttävä ohjelmisto pyytää DNS-palvelinta kääntämään FQDN-tiedon A-tunnukseksi, eli IPv4-osoitteeksi. A-tunnuksen saadessaan ohjelmisto alkaa kommunikoida kohteen kanssa IPv4-osoitetta käyttäen. (Desmeules 2007, 230.)

- **Kysely IPv6-osoitteesta.** Tässä kyselyssä IPv6-protokollaa käyttävä ohjelmisto pyytää DNS-palvelinta kääntämään FQDN-tiedon AAAA-tunnukseksi, eli IPv6-osoitteeksi. AAAA-tunnuksen saadessaan ohjelmisto alkaa kommunikoida kohteen kanssa IPv6-osoitetta käyttäen. (Desmeules 2007, 230.)

- **Kysely kaikista osoitteista.** Tässä kyselyssä molempia protokollia käyttävä ohjelmistä pyytää DNS-palvelinta kääntämään FQDN-tiedon kaikentyyppisiksi osoitteiksi. Ohjelmisto etsii ensin AAAA-tunnusta. Jos sitä ei löydy, ohjelmisto aloittaa kommunikoinnin kohteen kanssa A-tunnuksen avulla. (Desmeules 2007, 230.)

4.3 Tunneling

Seuraavassa käydään läpi Tunneling-tekniikan toiminta.

4.3.1 Yleistä

Tunnelointia käytetään yleensä kuljettamaan yhteensopimattomia protokollia olemassa olevan verkon ylitse. Tunnelointi mahdollistaa eristyksessä olevan IPv6-protokollaa käyttävän verkkolaitteen kommunikoinnin IPv4-verkon ylitse. Eristyksissä olevat verkkolaitteet voivat jopa muodostaa päästä päähän yhteyden toisiinsa ja käyttää IPv4-protokollaa kuljetuskerroksena. Tunnelointimenetelmällä kapsuloidaan IPv6-paketti IPv4-paketin sisään ja sen jälkeen nämä kapsuloidut IP-

paketit lähetetään IPv4-verkkolaitteelle. Lopuksi verkkolaite dekapsuloi IPv4-paketista IPv6-paketin. (Desmeules 2007, 227.)

4.3.2 Toiminta

Kun IPv6-paketteja tunneloidaan IPv4-verkossa, IPv6-paketin header- ja dataosaa ei muokata. Lähetettävän paketin sisempi header sisältää lähde- ja kohde-IPv6-osoitteet ja ulompi header sisältää lähde- ja kohde-IPv4-osoitteet. Tunnelin kummassakin päässä tapahtuu IPv6-pakettien kapsulointi ja dekapsulointi. Tunnelin kummassakin päässä olevan laitteen täytyy olla molempia protokollia tukeva. (Desmeules 2007, 235.)

Kuten missä tahansa muussakin tunnelointitekniikassa, IPv6-tunneloinnissakin on omat huonot puolensa:

- **Tunnelin MTU ja fragmentoituminen.** Koska IPv6-paketin eteen lisätään 20 tavun IPv4-header, IPv6:n MTU-arvo pienenee 20 tavua. Pienin mahdollinen MTU-arvo IPv6-protokollan linkkikerrokselle on 1280 tavua. Riippuen siitä mitkä MTU-arvot on konfiguroitu IPv4- ja IPv6-linkkikerrokselle, saattaa tapahtua fragmentoitumista IPv4-kerroksessa. Tämä fragmentoituminen vaikuttaa suorituskykyyn tunnelin molemmissa päissä olevissa laitteissa ja vaatii niiltä enemmän prosessointitehoa. (Desmeules 2007, 236.)

- **ICMPv4-virheiden käsittely.** Virhetilanteessa monet vanhemmista reitittimistä palauttavat vain 8 tavua dataa IPv4-paketin headerin yli. Jos virhetilanne tulee, IPv6-lähdeverkkolaitteen tarvitsee tietää IPv6-paketin osoitekentät. (Desmeules 2007, 236.)

- **Protokolla 41:n filtteröinti.** Jos IPv4-verkon palomuurien ja reitittimien ACL-listat ovat hyvin konfiguroituja, tavallisesti nämä laitteet blokkaisivat kaikki IPv4-paketit, jotka käyttävät protokollaa 41. Tämä ongelma liittyy enemmänkin verkonhallintaan. (Desmeules 2007, 236.)

- **NAT.** Kuten muissakin tunnelointitekniikoissa, IPv6-tunneloinnissa ei ole mahdollista muodostaa tunnelia NAT:in läpi, joka on konfiguroitu käyttä-

mään dynaamista porttikääntämistä ja portin uudelleenreititysmoodia. Tunnelointi staattisessa moodissa on kuitenkin mahdollista NAT:in läpi. (Desmeules 2007, 236.)

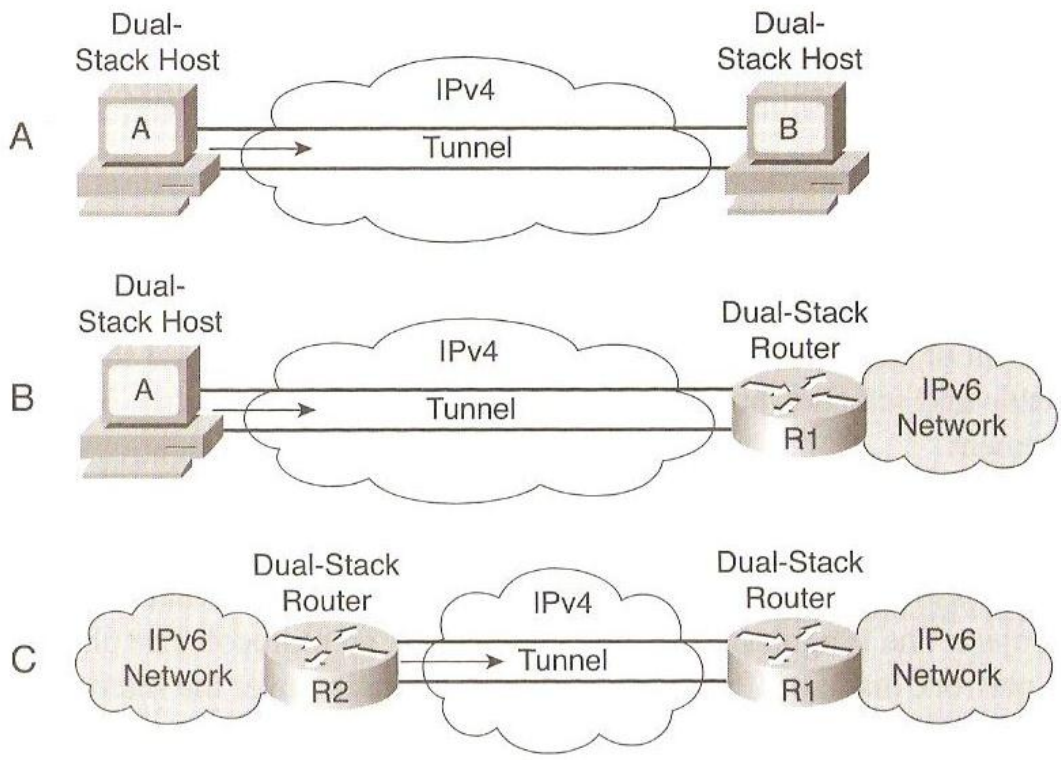
On olemassa kolme erilaista käyttötapaa IPv6-tunnelille IPv4-verkossa:

- **Verkkolaitteelta verkkolaitteelle.** Eristetyt Dual Stack -verkkolaitteet IPv4-verkossa voivat muodostaa tunnelin keskenään. Tämä tapa mahdollistaa kuitenkin vain päästä päähän IPv6-yhteyden koneiden välillä. (Desmeules 2007, 237.)

- **Verkkolaitteelta reitittimelle.** Eristetyt Dual Stack -verkkolaitteet IPv4-verkossa voivat muodostaa tunnelin Dual Stack -reitittimeen. Tällainen menetelmä mahdollistaa IPv6-yhteyden muodostamisen mihin tahansa IPv6-verkkolaitteeseen reitittimen kautta. (Desmeules 2007, 237.)

- **Reitittimeltä reitittimelle.** Dual Stack -reitittimet voivat muodostaa keskenään tunnelin IPv4-verkossa. Reitittimiä voidaan käyttää yhdistämään erillisiä IPv6-verkkolaitesaarekkeita. Näin jokainen IPv6-verkkolaite pystyy yhdistämään kaikkiin IPv6-verkkolaitteisiin. (Desmeules 2007, 237.)

Kuvassa 13 on esitetty erilaisia IPv6-tunneleita.



Kuva 13. IPv6-tunneleita. (Desmeules 2007.)

Seuraavaksi käydään läpi yleisimmät tunnelointitekniikat ja -menetelmät:

- **Configured tunnel.** Tunnelit konfiguroidaan staattisesti Dual Stack -verkkolaitteiden porteille. Tunnelin molemmissa päissä täytyy manuaalisesti konfiguroida IPv4- ja IPv6-osoitteet verkkolaitteiden porteille. (Desmeules 2007, 239.) Seuraavanlaiset osoitteet konfiguroidaan tunnelin portille:

    - **Paikallinen IPv4-osoite.** Paikallinen osoite, josta saa yhteyden paikalliseen Dual Stack -verkkolaitteeseen IPv4-verkon yli. Paikallista IPv4-osoitetta käytetään poistuvan liikenteen lähdeosoitteena. (Desmeules 2007, 239.)

    - **Etäispään IPv4-osoite.** Tästä IPv4-osoitteesta tavoitetaan Dual Stack -kohdeverkkolaite IPv4-verkon yli. Tätä osoitetta käytetään poistuvan liikenteen kohdeosoitteena. (Desmeules 2007, 239.)

- **Paikallinen IPv6-osoite.** IPv6-osoite asetetaan paikallisesti tunnelin portille. (Desmeules 2007, 239.)

- **Tunnel broker.** Tunnel broker on ulkoinen järjestelmä, joka toimii palvelimena IPv4-verkossa. Dual Stack -verkkolaitteet lähettävät tunnelointipyyntöjä Tunnel broker -palvelimelle käyttäen HTTP:tä. Vastineeksi Tunnel broker lähettää verkkolaitteille takaisin IPv4-osoitteita, IPv6-osoitteita ja oletus-IPv6-reittejä tunnelin muodostamista varten. Lopuksi Tunnel broker -palvelin konfiguroi tunnelin reitittimen ja verkkolaitteen välille. (Desmeules 2007, 243.)

- **Tunnel server.** Tunnel server on yksinkertaistettu versio Tunnel broker -tekniikasta. Tunnel server -tekniikka yhdistää broker- ja dual stack -reitittimen samaan systeemiin eli samaan laitteeseen. Tunnel server -tekniikassa tunnelipyynnöt kulkevat myös HTTP:tä käyttäen kuten Tunnel broker -tekniikassa. (Desmeules 2007, 244.)

- **6to4.** IETF on määritellyt 6to4-tekniikan pääominaisuudet, jotka ovat:

  - **Automatic tunneling.** Dynaaminen muoto muodostaa tunneleita IPv6-kohteiden välillä. Tässä toiminnossa ei tarvitse lisätä manuaalisesti lähde- ja kohde-IPv4-osoitteita muodostaakseen tunnelin. Kuten Configured tunnel -tekniikassa, 6to4 kapsuloi IPv6-paketin IPv4-paketin sisälle ja käyttää IPv4-reititysalueita kuljetuskerroksena. (Desmeules 2007, 245.)

  - **Enabled at the edge of the site.** On suositeltavaa, että 6to4 on käytössä eri verkkokohteiden rajareitittimillä, koska 6to4-reitittimen täytyy saada yhteys muihin 6to4-kohteisiin ja 6to4-reitittimiin käyttäen IPv4-reititysrakennetta. (Desmeules 2007, 245.)

  - **Automatic prefix assignment.** Toimittaa yhden julkisen unicast-osoitteen jokaiselle 6to4-kohteelle: (Desmeules 2007, 245.)

        - Kaikki 6to4-osoitteet perustuvat 2002::/16 osoiteavaruuteen, jonka on määrittänyt IANA. (Desmeules 2007, 245.)
        - Jokainen 6to4-kohde käyttää vähintään yhtä julkista unicast-IPv4-osoitetta, joka on asetettu 6to4-reitittimelle. Tämä 32 bittinen osoite muunnetaan heksadesimaaliseksi arvoksi, joka liitetään osoitteeseen 2002::/16. Eli lopullinen osoite on 2002:ipv4-osoite::/48. (Desmeules 2007, 245.)
        - Jokainen 6to4-kohde saa yhden /48-prefixin perustuen kohteen julkiseen unicast-IPv4-osoitteistukseen. Seuraavat 16 bittiä /48-prefixistä ovat avoinna 6to4-kohteen aliverkotukselle reitittimen takana. Täytyy muistaa, että yksi /48 prefiksi sisältää 65 536 /64 prefiksiä eli 2^{16} /64-prefixiä. (Desmeules 2007, 245.)

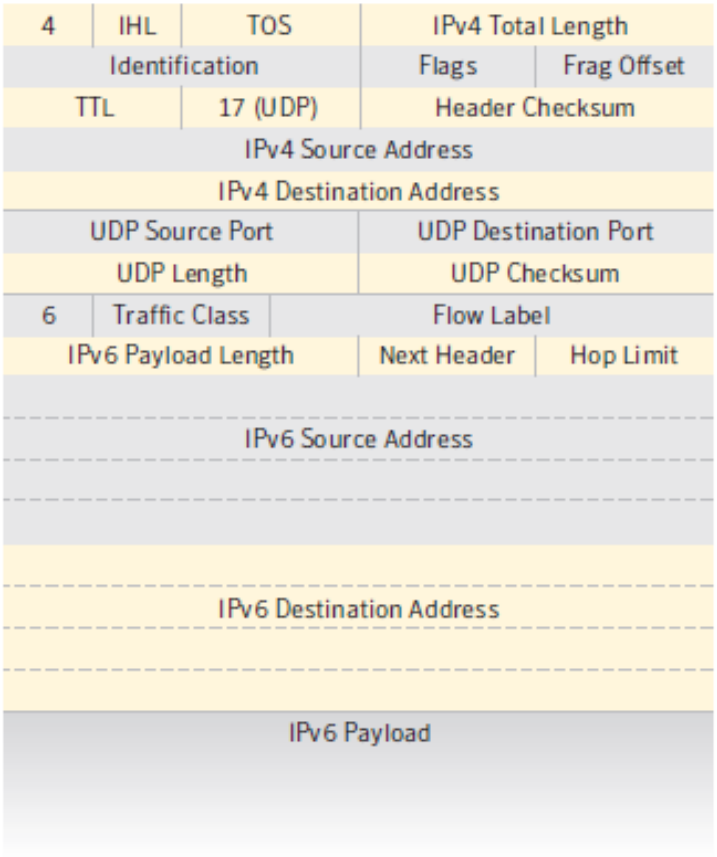
    - **No IPv6 route propagation.** Koska 6to4-prefiksit perustuvat julkisesti ainutlaatuisiin IPv4-osoitteisiin, ei ole tarvetta levittää /48 IPv6-reittejä muiden 6to4-alueiden kesken. (Desmeules 2007, 246.)

    - **6to4 Relay.** Reititin jossa 6to4-mekanismi on käytössä, reitittää IPv6-paketteja IPv4-verkon ylitse mihin kohteeseen tahansa, jolla on prefiksi 2002::/16. Mutta kuten aiemmin on todettu, on olemassa muitakin julkisia unicast-prefixejä, joita käytetään IPv6-verkossa. Tällaisia ovat esimerkiksi 2001::/16 (Production IPv6 Internet) ja 3ffe::/16 (the 6bone). Näin ollen nämä muut prefixit ovat saavuttamattomissa IPv6-verkossa, ellei yhtä IPv4-verkon 6to4-reitittimistä konfiguroida toimimaan kulkuväylänä IPv6-verkkoon. Tällaista reititintä kutsutaan 6to4-relayksi. (Desmeules 2007, 251.)

- **IPv6 over a GRE Tunnel.** GRE-tunneli on hyvin tunnettu tunnelitekniikka, joka on vakaa ja turvallinen tapa muodostaa point to point -yhteyksiä. Kuten Configured tunnel -tekniikassa, GRE-tunnelikin konfiguroidaan staattisesti reitittämään IPv6-paketteja IPv4-verkon yli. GRE-tunneloinnin hyötynä on se, että GRE käyttää domainissa reititysprotokollana IS-IS-protokollaa. Koska IS-IS-protokollan täytyy lähettää linkkikerroksen viestejä vierekkäis-

ten reitittimien kesken, IS-IS-protokolla on ainut tunnelointiprotokolla, joka pystyy lähettämään tämäntyyppistä liikennettä IP-verkon ylitse. (Desmeules 2007, 255.)

- **Teredo Tunneling.** Teredo-tunnelointi, joka tunnetaan myös nimellä shipworm, on tunnelointitekniikka, jonka päätarkoituksena on mahdollistaa IPv6-pakettien reititys dual stack -verkkolaitteille, jotka ovat IPv4-verkossa NAT-laitteiden takana. Teredo-käyttäjät lähettävät ja vastaanottavat IPv4-verkon yli IPv6-liikennettä, joka on tunneloitu UDP-protokollan sisään. (Hoagland 2007, 7.) Kuvassa 14 on esitetty miltä näyttää IPv6-paketti, joka on kapsuloitu UDP-protokollan sisään.



Kuva 14. Teredon kapsuloima IP-paketti. (Hoagland 2007.)

Teredo sisältää kolme pääkomponenttia, jotka ovat clients, relays ja servers. Teredo-client on dual stack -verkkolaite, joka sijaitsee IPv4-verkossa NAT-laitteen takana, josta se lähettää pyynnön teredo-palvelimelle saada IPv6-yhteyden IPv4-verkon yli. Teredo-palvelin sijaitsee sekä IPv4- että IPv6-verkossa, josta se auttaa verkkolaitteita muodostamaan tunneleita IPv6-kohteisiin. Teredo-relay toimii reitittimenä, joka yhdistää IPv4- ja IPv6-verkot teredo-verkkolaitteille, jotka liikennöivät keskenään. (Hoagland 2007, 8.)

4.4 Protocol Translation

Seuraavassa käydään läpi Protocol Translation -tekniikan toiminta.

4.4.1 Yleistä

On mahdollista, että yksinomaan IPv6-verkossa oleva IPv6-protokollaa käyttävä verkkolaite kommunikoi yksinomaan IPv4-verkossa olevan IPv4-protokollaa käyttävän verkkolaitteen kanssa. Nämä toiminnot vaativat protokollan käännöstä molempien verkkojen rajareitittimillä. (Desmeules 2007, 228.)

4.4.2 Toiminta

Tällä hetkellä vain IPv6-protokollaa käyttävien verkkoalueiden täytyy päästä yhdistämään vain IPv4-protokollaa käyttäviin verkkoalueisiin. Täysi toimivuus kahden erityyppisen verkon välillä on pakollista, että voidaan mahdollistaa IPv4- ja IPv6-protokollan yhteensopivuus. Seuraavaksi käydään läpi tavanomaiset esimerkit kahden erityyppisen protokollan kommunikoinnista (Desmeules 2007, 262.):

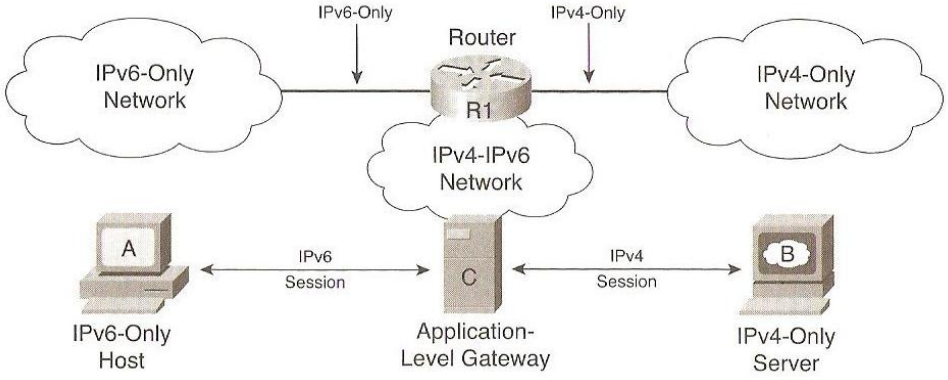
- Verkkolaite IPv6-verkkoalueella voi haluta lähettää sähköpostin verkkolaitteelle, joka on IPv4-verkkoalueella käyttäen SMTP-protokollaa (Desmeules 2007, 262).

- Verkkolaite IPv4-verkkoalueella voi haluta vastata lähde IPv6-verkkolaitteelle IPv6-verkkoalueella (Desmeules 2007, 262).

- Verkkolaitteet IPv4-verkkoalueella voivat haluta muodostaa HTTP-yhteyden IPv6-verkkoalueella olevalle web-palvelimelle (Desmeules 2007, 262).

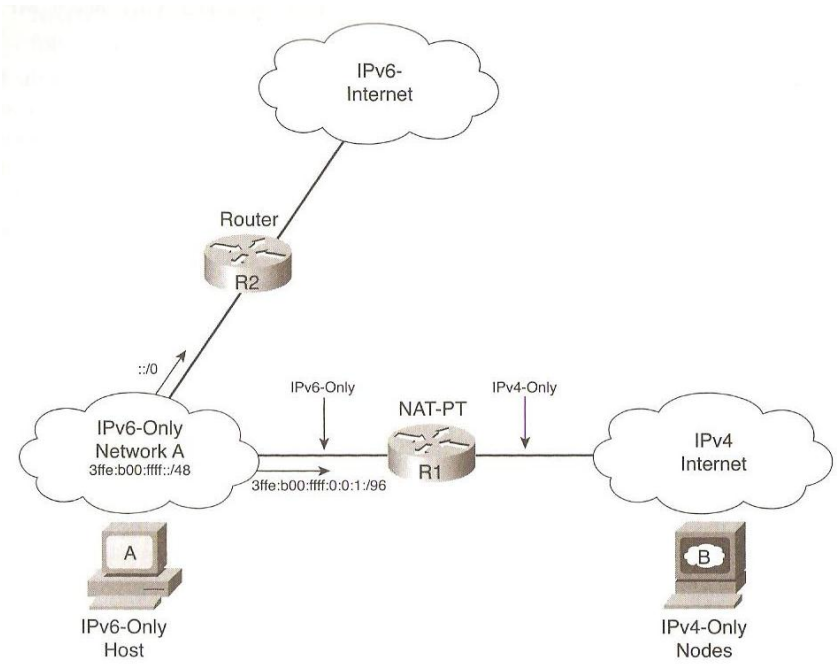
Koska IPv6-protokolla on alusta lähtien suunniteltu toimimaan IPv4-protokollan kanssa rinnakkain, on kehitetty kaksi tekniikkaa, jotka ovat ALG ja NAT-PT (Desmeules 2007, 262).

ALG-tekniikka on verkkorakenne, jonka dual stackia tukevat yhdyskäytävät mahdollistavat IPv6-verkossa olevien IPv6-verkkolaitteiden kommunikoida IPv4-verkossa olevien IPv4-verkkolaitteiden kanssa. (Desmeules 2007, 262.) Kuvassa 15 on esitetty ALG-tekniikan toiminta.



Kuva 15. ALG-tekniikan toiminta. (Desmeules 2007.)

NAT-PT-tekniikka on NAT-tekniikan yksi tyyppi. NAT-PT mahdollistaa liikenteen IPv4- ja IPv6-verkkoalueen kesken muuntamalla IPv6-osoitteen IPv4-osoitteeksi ja toisinpäin. NAT-PT perustuu Stateless IP/ICMP Translator -algoritmiin eli SIIT-algoritmiin. SIIT-algoritmi muokkaa IPv4- ja IPv6-pakettien header-osioita, mukaan lukien ICMP-header. (Desmeules 2007, 264.) Kuvassa 16 on esitetty NAT-PT-tekniikan toiminta.



Kuva 16. NAT-PT-tekniikan toiminta. (Desmeules 2007.)

5 IPv6 KÄYTÄNNÖSSÄ

5.1 Yleistä

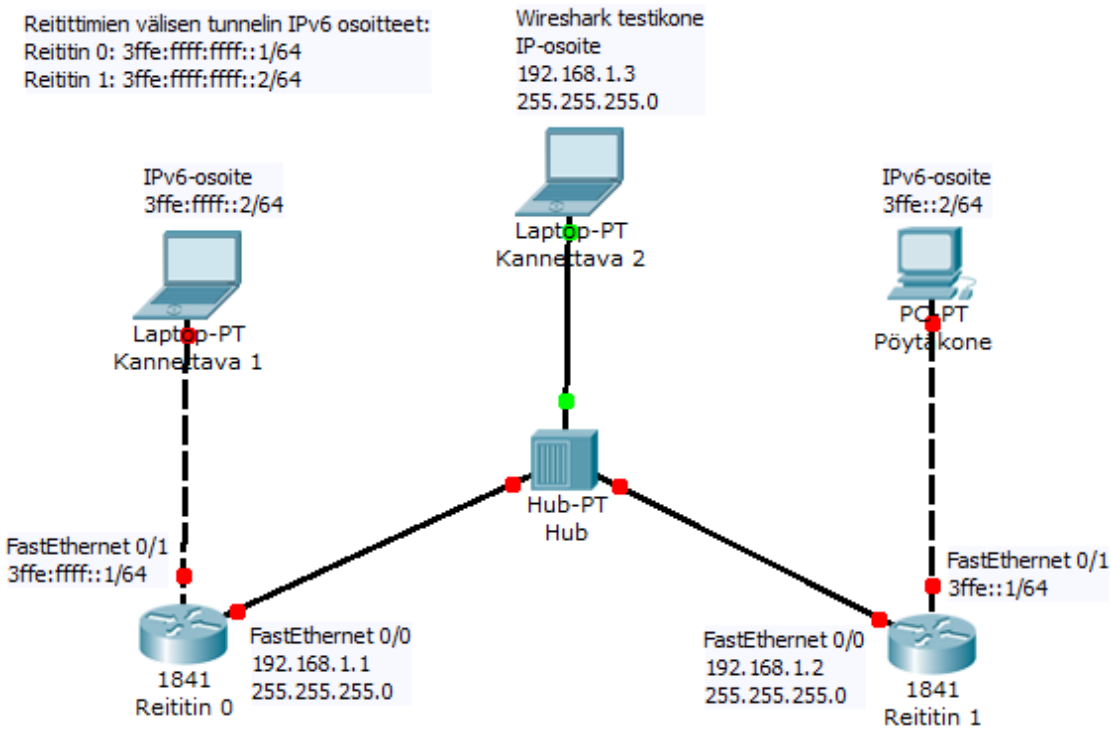
Käytännön testauksessa käytetään kahta Ciscon 1841-reititintä ja yhtä HP-merkkistä Hubia. Testissä kokeillaan IPv6-tunnelointia ja protokollamuunnostekniikkaa Ciscon-reitittimillä ja kolmella tietokoneella. Testauksen yhteydessä käsitellään myös IPv4- ja IPv6-osoitteistusta ja Ciscon-konsolin eri komentoja.

5.2 IPv6-tunnelointi

Seuraavassa testataan käytännössä IPv6-tunnelointia.

5.2.1 Kokoonpano

IPv6-tunneloinnissa käytetään kuvan 17 mukaista kokoonpanoa.



Kuva 17. Kokoonpano, jolla testataan IPv6-tunnelointia.

Kuten kuvassa 17 näkyy, kannettava 1 ja pöytäkone ovat IPv6-verkossa ja molemmista koneista on IPv4-protokolla poistettu käytöstä. Reitittimien 0 ja 1 välissä on IPv4-verkko. Kannettava 2 toimii testikoneena, johon on asennettu Wireshark-ohjelma, jonka tehtävänä on seurata ja näyttää kahden reitittimen välistä verkkoliikennettä. Kokoonpanon tehtävä on muodostaa IPv6-tunneli kannettava 1 -koneesta pöytäkone 1 -koneeseen ja toisinpäin. Kannettava 2 käynnissä olevan Wireshark-ohjelman tulokset löytyvät liitteestä 1.

5.2.2 Cisco-konsolikomennot

Ciscon reitittimissä on oletuksena IPv6-reititys pois käytöstä, joten ensimmäisenä reitittimien konsoliin annetaan komento **ipv6 unicast-routing**, joka mahdollistaa IPv6-pakettien reitityksen eteenpäin. Komentojen syntaksi näyttää seuraavanlaiselta:

```
Router>enable

Router#configure terminal

Router(config)#ipv6 unicast-routing
```

Kun **ipv6 unicast-routing** -komento on annettu reititin 0 ja reititin 1, aloitetaan reititin 0 konfigurointi. Reitin 0:n FastEthernet porteille annetaan kaikki tarpeelliset IP-osoitteet komennoilla:

```
Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdon

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ipv6 address 3ffe:ffff::1/64
```

```
Router(config-if)#no shutdown
```

Reititin 1:n FastEthernet porteille annetaan samanlaiset komennot kuin reititin 0. Täytyy kuitenkin muistaa laittaa kuvan 17 mukaiset IP-osoitteet reititin 1:een. Kannettavalle 1, kannettavalle 2 ja pöytäkoneeseen annetaan IPv6-osoitteet kuvan 17 mukaisesti.

Tarpeellisten osoitteistuksien jälkeen konfiguroidaan IPv6-tunneli reititin 0 ja reititin 1 välille. Reititin 0 komentojen syntaksi on seuraava:

```
Router>enable

Router#configure terminal

Router(config)#interface tunnel 0

Router(config-if)#ipv6 address 3ffe:ffff:ffff::1/64

Router(config-if)#tunnel source 192.168.1.1

Router(config-if)#tunnel destination 192.168.1.2

Router(config-if)#tunnel mode ipv6ip

Router(config-if)#exit

Router(config)#ipv6 route 3ffe::/64 tunnel 0
```

Reititin 1 komentojen syntaksi on seuraava:

```
Router>enable

Router#configure terminal

Router(config)#interface tunnel 1

Router(config-if)#ipv6 address 3ffe:ffff:ffff::2/64

Router(config-if)#tunnel source 192.168.1.2

Router(config-if)#tunnel destination 192.168.1.1

Router(config-if)#tunnel mode ipv6ip

Router(config-if)#exit
```

```
Router(config)#ipv6 route 3ffe:ffff::/64 tunnel 1
```

5.2.3 Konfiguraation tarkastus ja testaus

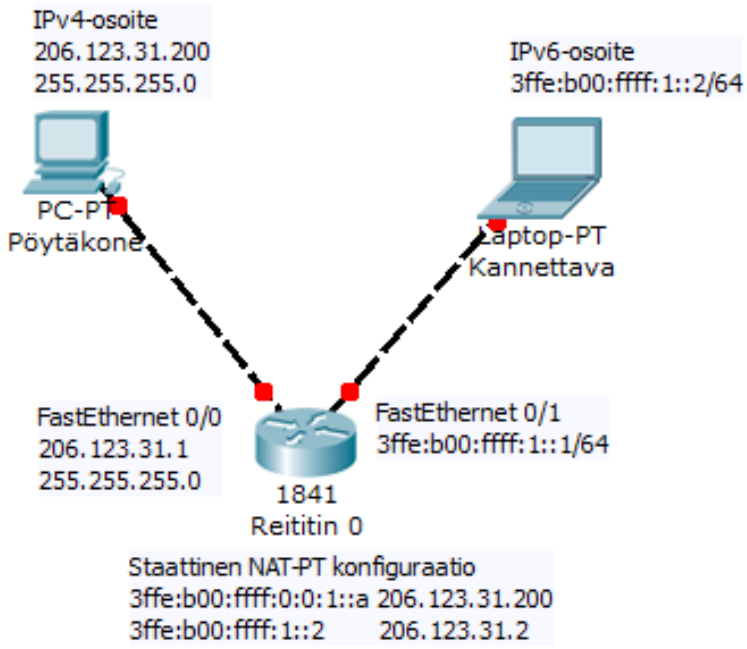
Ciscon reitittimessä voi tarkastella tunnelikonfiguraatiota komennolla **show ipv6 interface tunnel x**. Reitittimen muita asetuksia voi tarkastella komennolla **show running-config**. Yhteyden koneiden välillä voi testata **ping x:x:x:x:x:x:x:x** -komennolla tietokoneiden komentokehotteessa.

5.3 Protokolla muunnos -tekniikka Staattinen NAT-PT

Seuraavasssa testataan käytännössä Protokollamuunnos-tekniikkaan ja lähemmin sen staattiseen NAT-PT-toimintoon.

5.3.1 Kokoonpano

Tässä käytännön testissä käytetään protokollamuunnos-tekniikan staattista NAT-PT-tekniikkaa. Kokoonpano on kuvan 18 mukainen.



Kuva 18. Kokoonpano, jolla testataan staattista NAT-PT-tekniikkaa.

Kuten kuvan 18 kokoonpanosta näkee, pöytäkoneeseen konfiguroidaan IPv4-osoite ja kannettavaan IPv6-osoite. Reitittimen FastEthernet 0/0 -porttiin asetetaan IPv4-osoite ja FastEthernet 0/1 -porttiin asetetaan IPv6-osoite.

5.3.2 Cisco-konsolikomennot

Reitittimien ja tietokoneiden IP-osoitteet asetetaan samalla tavalla kuin otsikossa 5.2.2. Staattisen NAT-PT-tekniikan komentojen syntaksi on seuraava:

```
Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 206.123.31.1 255.255.255.0

Router(config-if)#ipv6 nat
```

IPv6 nat -komento ottaa NAT-PT-toiminnon käyttöön portissa.

```
Router(config-if)#interface fastEthernet 0/1

Router(config-if)#ipv6 address 3ffe:b00:ffff:1::1/64

Router(config-if)#ipv6 nat

Router(config-if)#exit

Router(config)#ipv6 nat prefix 3ffe:b00:ffff:0:0:1::/96

Router(config)#ipv6 nat v6v4 source 3ffe:b00:ffff:1::2 206.123.31.2
```

IPv6 nat v6v4 source -komento pakottaa IPv6-paketin muuntamisen IPv4-paketiksi.

```
Router(config)#ipv6 nat v4v6 source 206.123.31.200 3ffe:b00:ffff:0:0:1::a
```

IPv6 nat v4v6 source -komento pakottaa IPv4-paketin muuntamisen IPv6-paketiksi.

5.3.3 Konfiguraation testaus

Yhteyden testaus suoritetaan tietokoneen komentokehotteen **ping**-komennolla.

6 TULOKSET JA YHTEENVETO

6.1 Tulokset

Opinnäytetyön tarkoituksena oli tutkia IPv6-osoiteavaruutta ja erilaisia IPv4-yhteensopivia IPv6-reititysmenetelmiä. Opinnäytetyössä onnistuttiin hyvin tutkimaan ja löytämään erilaista tietoa IPv6-osoiteavaruudesta ja siitä mitä eroja IPv6-protokollassa on verrattuna IPv4-protokollaan.

IPv4-yhteensopivien IPv6-protokollien testaus suoritettiin kahdella Ciscon reitittimellä ja yhdellä HP-merkkisellä hubilla. Työssä oli tarkoitus tutustua dual-stack-, IPv6-tunneling- ja protokolla muunnos -tekniikoihin. Työssä onnistuttiin testaamaan täysin tunneling-tekniikka ja osittain protokolla muunnos -tekniikka.

Protokolla muunnos -tekniikan testaus epäonnistui, koska Ciscon laitteistoissa ei ollut riittävää IOS-versiota eikä näin ollen kaikkia tarvittavia konsolikomentoja löytynyt.

6.2 Yhteenveto

Opinnäytetyöstä oli henkilökohtaisesti paljon hyötyä, koska työ sisälsi paljon uutta asiaa IPv6-protokollasta, jota täytyi tutkia perusteellisesti erilaisista lähteistä. Työlle asetetut tavoitteet saavutettiin suurimmaksi osaksi.

Haastavinta työssä oli tutkia IPv4-yhteensopivia IPv6-protokollia, koska asiasisältö oli täysin uutta työn tekijälle. Haastavaa työssä oli myös käytännön testaus, johtuen Cisco-reitittimien puutteellisesta IOS-versiosta. Ciscon 1841 -reitittimistä löytyi tuki lähinnä lähiverkon toiminnoille, joten tämän takia työssä onnistuttiin täysin testaamaan ainoastaan tunneling-tekniikka.

IPv6 on erinomainen protokolla tulevaisuutta ajatellen. Jatkuva verkkolaitteiden kehitys ja lisääntyminen takaa sen, että IPv6-protokolla tulee vähitellen käyttöön IPv4-protokollan rinnalle. Muutaman vuoden kuluessa IPv6-protokolla on vallitseva

protokolla ja IPv4 häviää vähitellen. Ennen kaikkea IPv6-protokollan suuri osoiteavaruus on suurin tekijä tulevassa muutoksessa.

LÄHTEET

Cisco Systems. 24.01.2006. How NAT Works. [Pdf-julkaisu]. Cisco Systems [viitattu 22.03.2011]. Saatavissa: http://www.cisco.com/image/gif/paws/6450/nat-cisco.pdf.

Desmeules, R. Syyskuu 2007. Cisco Self-Study: Implementing IPv6 Networks (IPv6). 3. painos. United States of America: Cisco Press.

DiNicolo, D. Tammikuu 2007. NAT Overloading Port Address Translation (PAT). [WWW-julkaisu]. Cisco Systems Inc. [viitattu 23.03.2011]. Saatavissa: http://www.2000trainers.com/cisco-ccna-12/ccna-nat-pat/.

Dynamic NAT. [WWW-dokumentti]. [viitattu 22.03.2011]. Saatavissa: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzajw%2Frzajwdynamic.htm.

Hinden, R. & Deering, S. Heinäkuu 2008. IP Version 6 Addressing Architecture. [WWW-dokumentti]. Cisco Systems. [viitattu 28.03.2011]. Saatavissa: ftp://ftp.funet.fi/pub/standards/RFC/rfc2373.txt.

Hoagland, J. Helmikuu 2007. The Teredo Protocol: Tunneling Past Network Security and Other Security Implications. [Pdf-julkaisu]. Symantec Corporation. [viitattu 06.04.2011]. Saatavissa: http://www.symantec.com/avcenter/reference/Teredo_Security.pdf.

Hogg, S. 2007. Internet Protocol version 6. [Pdf-julkaisu]. Global Technology Resources, Inc. [viitattu 25.03.2011]. Saatavissa: http://www.gtri.com/docs/IPv6%20-%20The%20Next%20Generation%20Protocol%20v1-1.pdf.

Nikulainen, K. 11.02.2011. Viimeisetkin vapaat IPv4-osoitealueet jaettiin. [WWW-dokumentti]. www.ITNyt.fi. [viitattu 22.03.2011]. Saatavissa: http://www.itnyt.fi/node/2465-viimeisetkin-vapaat-ipv4-osoitealueet-jaettiin.

Port, E. Syyskuu 2005. IPv4 Header. [Pdf-julkaisu]. [viitattu 23.03.2011]. Saatavissa: http://www.6diss.org/workshops/saf/ipv6-protocol.pdf.

Publick and Private IP Address Classes range. [WWW-dokumentti]. www.ic.ims.hr. [viitattu 22.03.2011]. Saatavissa: http://www.ic.ims.hr/informaticke_mreze/vlsm/ip_address_range.png.

Static NAT. [WWW-dokumentti]. [viitattu 23.03.2011]. Saatavissa: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzajw%2Frzajwstatic.htm.

TCP/IP Suite. [WWW-julkaisu]. www.protocols.com. [23.03.2011]. Saatavissa: http://www.protocols.com/pbook/tcpip2.htm.

Young, J. H. Helmikuu 2006. IP Packet Structure. [WWW-julkaisu]. Computer science Now. [viitattu 23.03.2011]. Saatavissa: http://www.comsci.us/datacom/ippacket.html.

IPv6, Internet Protocol version 6. 1998 – 2011. [WWW-dokumentti]. Network Sorcery, Inc. [viitattu 31.03.2011]. Saatavissa: http://www.networksorcery.com/enp/protocol/ipv6.htm#Version.

LIITTEET

LIITE 1. Wireshark