IPv6

- **CIDR on ‘kikkailua’, ei ratkaise IP:n perusongelmia**
- **tavoitteita:**
  - biljoonia osoitteita
  - pienempiä reititystauluja
  - yksinkertaisempia protokollia
  - turvallisuutta
  - mukaan palvelutyyppi (tosiaikainen), monilähetys
  - liikkuvien koneiden osoitteet
  - jatkokehitys ja nykyisten protokollien toimivuus

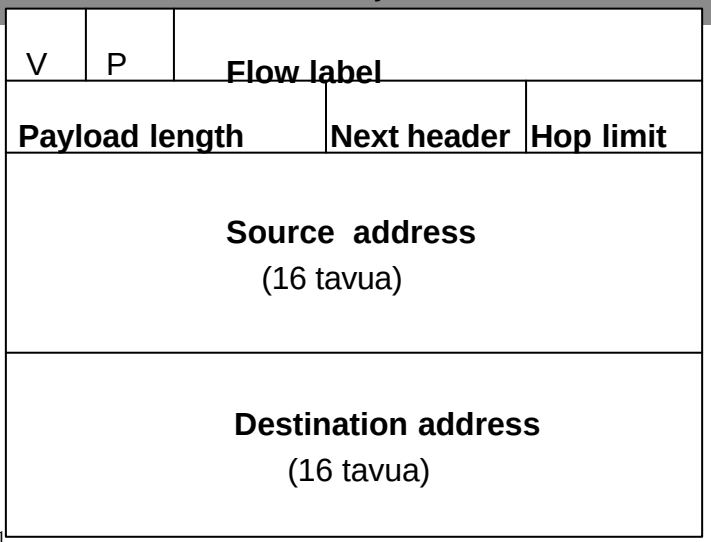
IPv6

- **16 tavun osoitteet**
  - => ‘rajaton’ määrä osoitteita
- **yksinkertaisempi otsake-kenttä**
  - kiinteä kehys, jossa vain 7 kenttää
- **valinnaisten piirteiden käsittely**
  - monet ennen pakolliset nyt valinnaisia
  - opitioiden uusi esitystapa => nopeampi käsittely
- **turvaus**
  - todentaminen
  - yksityisyys

- **palvelutyyppi otettu paremmin huomioon**
  - multimedia
- **yhteensopiva Internetin protokollien kanssa**
  - osoitteiden koko
  - ei ole yhteensopiva IPv4:n kanssa

IPv6-otsake

- V = version, P = Priority



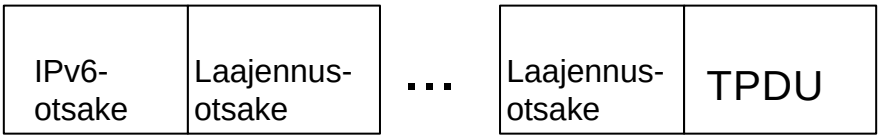
Otsakekentät

- **Versio** (version)
  - aina 6 IPv6:lle ja 4 IPv4:lle
- **prioriteetti** (priority)
  - 0-7 ruuhkatilanteessa voi hidastaa
  - 8-15 tosiaikapaketteja (video/audio)
  - isompi numero, tärkeämpi paketti
- **vuonimiö** (flow label)
  - pseudoyhteys, jolla tietyt ominaisuudet ja vaatimukset (esim. viive, viipeen vaihtelu jne)
  - vuot muodostetaan etukäteen ja niille annetaan tunnus: lähde- ja kohdeosoite ja vuonumero

- **kuorman pituus** (payload length)
  - paketin koko (ilman otsaketta)
- **seurava otsake** (next header)
  - otsikon laajentaminen
  - 6 otsikon laajennusosaa
  - viimeisessä kertoo kuljetusprotokollan (TCP, UDP)
- **hyppyraja** (hop limit)
  - hyppylaskuri, vähenee joka hypyllä
- **source address, destination address**
  - 16 tavun osoitteita

IPv4:n kentistä puuttuvat

- **paketin paloitteluun liittyvät kentät**
  - kaikki kykenevät käsittelemään ainakin 576 tavun paketteja
  - lähettäjä huolehtii, että paketti on riittävän pieni
    - reititin ilmoittaa virheestä, jos se havaitsee liian suuren paketin => ohjeet pilkkoa paketti pienemmäksi
- **tarkistussumma**
  - ei lasketa verkkokerroksella
    - luotettavammat verkot
    - siirtoyhteyskerros laskee / kuljetuskerros laskee



Ei yhtään, yksi tai useita laajennusotsikoita

Seuraava otsake -kenttä (Next header Field)

* ilmoittaa minkä tyyppinen otsakekenttä seuraa IPv6-otsaketta
* seuraaja voi olla jokin laajennusotsake tai ylemmän protokollan, kuten TCP:n tai UDP:n otsake

Laajennusotsikot

- **Hop-By-Hop- optioiden otsake**
  - tietoja reitittimille, käsitellään joka reitittimessä
- **reititysotsake** (Routing header)
  - **laajennettu reititys ~IPv4:n lähdereititys,**
  - **vaadittu reitti tai reitin osa**
- **paloitteluotsake** (Fragmentation header)
  - paloitteluun ja kokoamiseen liittyvää tietoa
- **autentikointiotsake** (Authentication header)
  - **paketin ehyys ja autentikointi (= taattu lähettäjän identiteetti)**
- **turvatun kuorman otsake** (Encapsulating Security Payload header)
  - **pakettien salakirjoitus**
- **kohdeoptioiden otsake** (Destination Options header)
  - paketin vastaanottajille tarkoitettua tietoa

Otsakkeiden järjestys

- **Standardin otsakkeet myös annetaan edellä esitetyssä järjestyksessä**
  - Poikkeuksena ovat kohdeoptioiden otsakkeet
    - Optiot voidaan tarkoittaa myös usealle kohteelle. Tällöin annetaan ensimmäinen osoite kohdeosoitteen kentässä ja muiden kohteiden lista reititysotsakkeessa.
    - Tällainen kohdeoptioiden otsake esiintyy heti hop-by-hop-otsakkeen jälkeen.
    - Jos otsakkeen tiedot on tarkoitettu vain paketin viimeiselle vastaanottajalle. Niin annetaan viimeisenä laajennuksena.

IPv6:n prioriteetit

- **ruuhkavalvottu liikenne (esim. TCP)**
  - viive saa jossain määrin vaihdella
  - pakettien järjestys saa muuttua
- **ruuhkavalvomaton liikenne**
  - tosiaikavideo tai audio
  - vakionopeus ja vakioviive => tasainen pakettivirta
- **prioriteetti suhteessa muihin saman lähteen paketteihin**
- **prioriteetti suhteessa saman liikennetyypin paketteihin**
  - ruuhkavalvotun ja valvomattoman liikenteen välillä ei ole määritelty prioriteettia

Ruuhkavalvottu liikenne

- **Prioriteetit 0- 7**

0 määrittelemätön liikenne (uncharacterized traffic)
1 täyttöliikenne (filler traffic) **verkkouutiset, USENET-sanomat**
2 lliikenne, jota käyttäjä ei dottele (unattended data traffic) **sähköposti**
3 ei vielä käytössä
4 käyttäjän odottama massasiirto (attended bulk traffic) **FTP, HTTP**
5 ei vielä käytössä
6 interaktiivinen liikenne (interactive traffic) **TELNET, X**
7 verkon valvontaliikenne (Internet control traffic) **SNMP, OSPF, BGP**

Ruuhkavalvomaton liikenne

- **Prioriteetit 8-15**

  8 sopivin hävitettäväksi

  esim. teräväpiirtovideo, jossa runsaasti redundanssia

  …….

  15 huonoin hävitettäväksi

  esim. puhelinkeskustelu, jossa kadonneet paketit aiheuttavat äänen pätkimistä ja häiriööääniä linjalla

Vuonimiö

- **Vuo**
  - peräkkäisten pakettien jono samasta lähteestä samoille vastaanottajille, jota reitittimien halutaan käsittelevän tietyllä tavalla
    - tiedostonsiirto usealla TCP-yhteydellä => yksi vuo
    - multimediakonferenssi => monta erilaista vuota
  - lähdeosoite + 24-bittinen vuotunnus identifioi vuon
    - kaikille saman vuon paketeille sama tunnus

- **Reitittimelle vuo on joukko peräkkäisiä paketteja, joita tulee käsitellä tietyllä tavalla**
  - samat resurssivaraukset
  - samat turvallisuusvaatimukset
  - samat säännöt pakettien hävittämiseen
  - samat etuoikeudet jonoissa
  - samat vaatimukset aliverkon palvelunlaadulle
  - sama laskutus

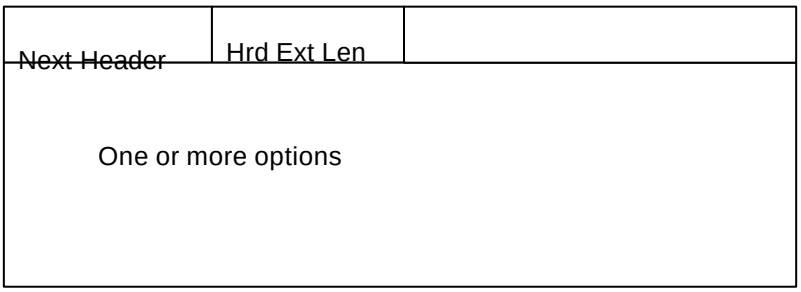
- **Vuonimiö on pelkkä tunniste**
  - on erikseen esitettävä, mitä toimintoja kuhunkin nimiöön liittyy
    - neuvottelemalla etukäteen reitittimen kanssa valvontaprotokollaa käyttäen
    - ilmoittamalla paketteja lähetettäessä otsakkeissa halutut toiminnot
      - Hop-By-Hop -option otsakkeessa
    - voidaan pyytää tiettyä palvelunlaatua (QoS) tai tosiaikaista palvelua

Vuonimiöiden käsittely solmuissa

- Jos ei osaa käsitellä, niin jätetään huomiotta
- jos sama vuonimiö, niin oltava myös
  - **sama kohde- ja lähdeosoite**
  - **sama prioriteetti**
  - **samat hop-by-hop-optiot (jos käytössä)**
  - **samar reititysoptiot (jos käytössä)**

  jotta reititin pystyy käsittelemään paketin pelkän vuonimiön perusteella
- lähde antaa vuotunnisteen ja pitää kirjaa niistä
  - **noin 16 miljoonaa tunnistetta**
  - **valitaan satunnaisesti**
  - **sama tunniste uudelleen käyttöön vasta kun sitä ei enää käytetä**

Hop-by-hop -optioiden laajennusotsake

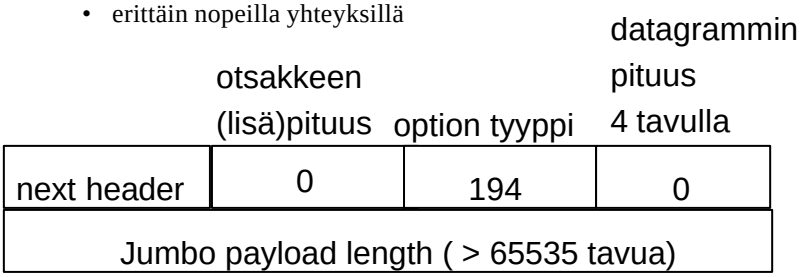


Next Header: seuraavan otsakkeen tyypp

Header Extension Length: otsakkeen pituus 64 bitin osina ensimmäisen 64 bitin lisäksi

jumbogrammi

- **ainoa hop-to-hop- optio toistaiseksi**
- **suuria paketteja tarvitaan**
  - supertietokoneille
  - suurien videopakettien siirrossa
  - erittäin nopeilla yhteyksillä

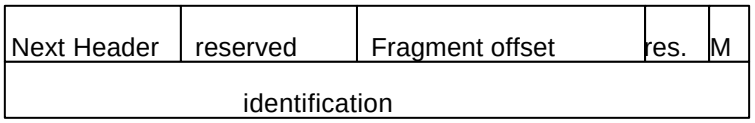


Maksimikooksi yli 4 Gtavua

Paloittelu (fragmentation)

- **IPv6: sanoman paloittelee lähettäjäsolmu**
  - ei enää reititin
  - reititin hylkää liian suuret paketit
- path discovery **-algoritmi:**
  - lähettäjä selvittää reitillä olevan pienimmän MTU:n (Maximum data unit), jotta osaa paloitella sopiviksi osiksi
    - 576 tavun paketti on kaikkien pystyttävä välittämään

Paloittelu-otsake

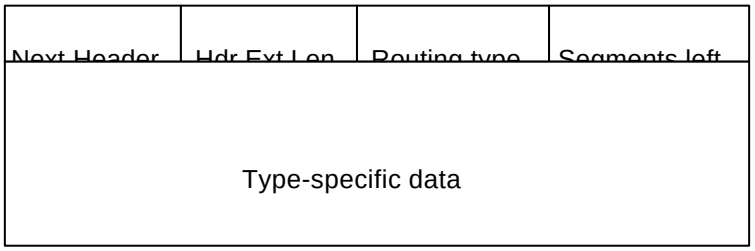


Fragment offset (13 bittiä): osan sijainti, yksikkönä 64 bitin osat

M-lippu: 1 = lisää palasia, 0= viimeinen pala

Identification (32 bittiä): koko sanoman tunniste, kaikissa osissa sama

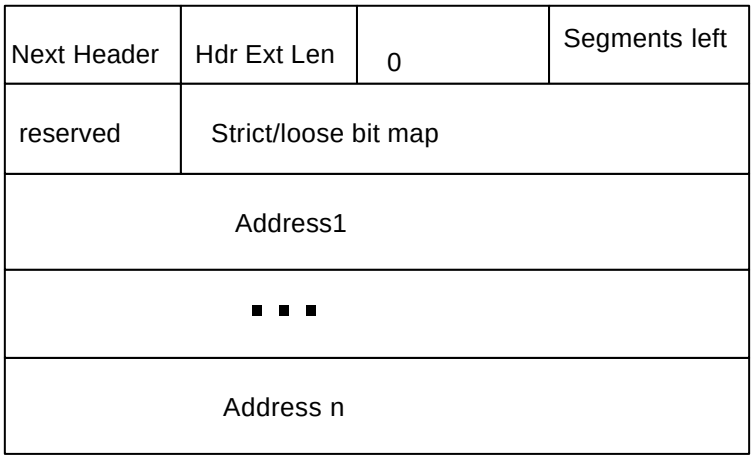
Reititysotsake



Routing type (8 bittiä): reititysotsakkeen tyyppi

Segments left (8 bittiä): kuljettavien välisolmujen määrä

Tyypin 0 reititysotsake



Bit map (23 bittiä): 1 (strict routing) = vastaava osoite on seurava solmu, 0 (loose routing) = ei välttämättä oltava seuraava osoite

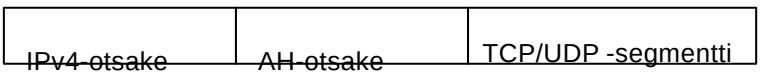
- **Kohteen IP-osoite on osoitelistan viimeinen,**
- **IP-otsakkeessa on ensimmäisen reittilistalla olevan reitittimen osoite**
  - joka vasta tutkii reititysotsikon ja saa selville, minne paketti ohjataan seuraavaksi
  - ja päivittää IP-paketin osoitteeksi seuraavan listalla olevan reitittimen
  - sekä vähentää yhdellä segments left -kenttää

Turvallisuus verkkokerroksella

- **Ipsec**
  - Authentication Header-protokolla **(AH-protokolla)**
  - Encapsulation Security Payload -protokolla (**ESP-protokolla)**
  - ennen käyttöä on luotava kommunikoivien koneiden välille **turvasopimus** SA (Security Agreement)
    - looginen yksisuuntainen yhteys verkkokerroksella
      - käytetty protokolla (AH tai ESP)
      - lähettäjän IP-osoite
      - 32-bittinen yhteystunnus SPI (Security Parameter Index)
        - kaikissa SA:n Ipsec-datagrammeissa sama SPI-arvo

AH-otsake

- **Varmistaa datagrammin eheyden ja lähettäjän identiteetin**
  - " juuri tämä lähettäjä on lähettänyt juuri tämän paketin"
    - kukaan ei väärentänyt lähettäjää
    - kukaan ei ole millaan tavoin muuttanut pakettia

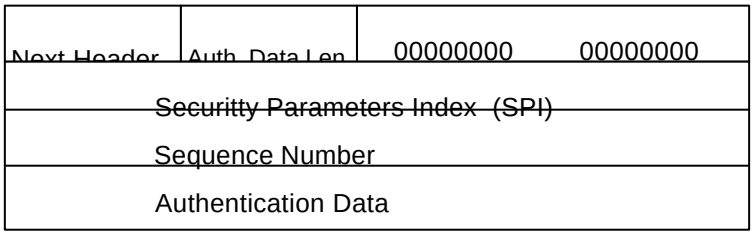


Protokollakenttä (= 51) ilmoittaa, että mukana on AH-otsake eli käytössä AH-protokolla

AH-otsake

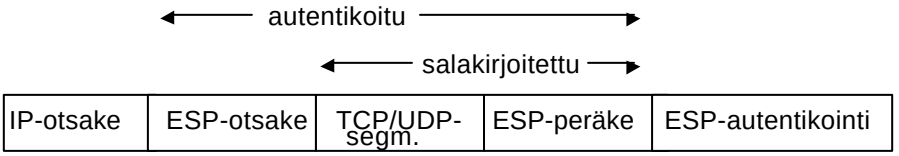
- **Next header**
  - onko data TCP-, UDP-,…. Segmentti
- **SPI eli yhteystunnus**
  - yhdessä lähettäjän IP-osoitteen ja käytetyn protokollan kanssa identifioi yhteyden turvasopimuksen SA
- **Sequence number**
  - järjestysnumero 32 bitillä
- **Authentication Data**
  - sanoman digitaalinen allekirjoitus => lähettäjän identiteetin ja sanoman yheyden varmistus

AH-otsake



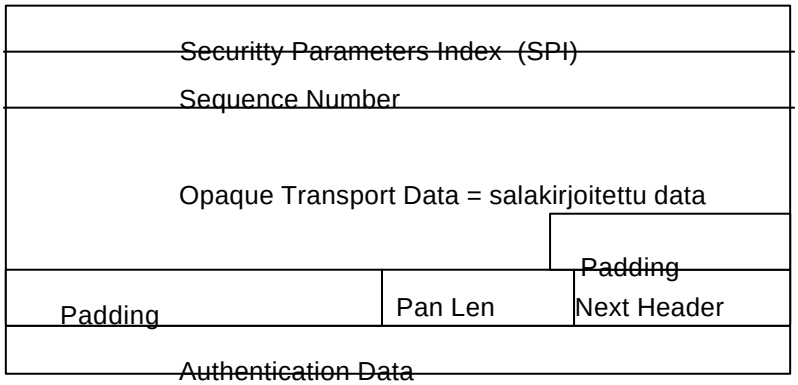
ESP-otsake

- **Sanoman salaus ja lähettäjän autentikointi**



Protokollakenttä (=50): datagrammissa ESP-otsake ja -peräke

ESP-otsake



IPv6: osoiteavaruus

- **jaettu osiin**
  - osa IPv4-osoitteille
- **palveluntuottajapohjainen osa**
  - Internet-palvelujen tuottajille oma osuus osoitteista
  - noin 16 miljoonaa tuottajaa
- **maantieteellinen osa**
  - vastaa nykyista Internetiä

- **Monilähetysosoitteet (multicast)**
  - lippukentän bitti: pysyvä vai tilapäinen ryhmä
  - scope-kenttä rajoittaa monilähetyksen
    - linkkiin
    - solmuun
    - yritykseen
    - planeettaan
- **anycast**
  - osoitteena ryhmä,
  - riittää lähettää jollekin ryhmän jäsenelle

Osoitteen esitysmuoto

- **kahdeksan neljän heksaluvun ryhmää:**
  8000:0000:0000:0000:0123:4567:89AB:CDEF
  - ryhmän alkunollat voi jättää pois
  - 16 nollan ryhmät voi korvava kaksoispisteellä

  => **8000::123:4567:89AB:CDEF**
  - **IPv4-osoitteet => ::193.31.20.46**

- **osoitteita on PALJON!**
  2128 => ~3* 10**38**
- **tasaisesti jaettuna noin 7 * 10**23 IP-osoitetta jokaista maapallon pinnan neliömetriä kohden**
- **vaikka jako olisi epätasaisempi, ainakin yli 1000 IP-osoitetta neliömetriä kohden**

Siirtyminen IPv4 => IPv6

- **Kestää pitkään**
- **syntyvät IPv6-saarekkeet kommunikoivat tunneloinnilla**
- **Dual stack -ratkaisut**
- **IPv6-reitittimet**

Internet-protokollia

- **ICMP (Internet Control Message Protocol)**
- **ARP (Address Resolution Protocol)**
- **RARP (Reverse Address Resolution Protocol)**
- **OSPF (Open Shortest Path First)**
- **BGP (Border Gateway Protocol)**
- **IGMP (Internet Group Management Protocol)**
- **Mobile IP**
- **CIDR (Classless InterDomain Routing)**
- **IPv6**

ICMP (Internet Control Message Protocol)

- **reitittimet ilmoittavat verkon ongelmista toisilleen**
- **yleensä testaukseen**
- **ICMP-sanomat kapseloidaan IP-paketteihin**
- **12 erilaista sanomaa määritelty**

ICMP-sanomia

- **Destination unreachable**
- **Time exceeded**
- **Parameter problem**
- **Source quench**
- **Redirect**
- **Echo request, Echo reply**
- **Timestamp request, Timestamp reply**

ICMP (Internet Control Message Protocol)

- **reitittimet ilmoittavat verkon ongelmista toisilleen**
- **yleensä testaukseen**
- **ICMP-sanomat kapseloidaan IP-paketteihin**
- **12 erilaista sanomaa määritelty**

ARP (Address Resolution Protocol)

- **muuttaa IP-osoitteen siirtoyhteyskerroksen osoitteeksi**
  - lähiverkkoon liitetyt laitteet ymmärtävät vain LAN-osoitteita
    - esim. eetteriverkon 48-bittisiä osoitteita
- **yleislähetys lähiverkkoon**
  - "Kenellä on IP-osoite vv.xx.yy.zz ?"
  - vastauksena osoitteen omistavan laitteen lähiverkko-osoite

- **optimointia:**
  - kyselyn tulos välimuistiin
    - talletetaan muutaman minuutin ajan
  - kyselijä liittää omat osoitteensa kyselyyn
  - alustettaessa jokainen laite ilmoittaa osoitteensa muille
    - kysyy omaa osoitettaan
    - jos tulee vastaus, niin konfigurointivirhe

- **reitittimet eivät välitä ARP-kyselyjä**
  - reititin vastaa itse ARP-kyselyihin (proxy ARP)
  - muihin verkkoihin menevät paketit lähetetään oletuspaikkaan, joka huolehtii niiden lähettämisestä

RARP (Reverse Address Resolution Protocol)

- **muuttaa lähiverkko-osoitteen IP-osoitteeksi**
  - käynnistettäessä levytön työasema
  - asema kysyy IP-osoitettaan yleislähetyksenä
    - "Lähiverkko-osoitteeni on xxxxx..xx. Mikä on IP-osoiteeni?"
    - RARP-palvelin vastaa kertomalla laitteen IP-osoitteen
  - => kaikille laitteille voidaan käyttää samaa aloitustiedostoa

- **reititin ei välitä RARP-viestejä**
  - joka verkossa oltava oma RARP-palvelin
  - käytetään **BOOTP**-protokollaa
    - käyttää UDP-viestejä, jotka reititin välittää toisiin verkkoihin
    - lisäinformaatiota
      - tiedostopalvelimen IP-osoite
      - oletusreitittimen IP-osoite
      - aliverkkomaski