- 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

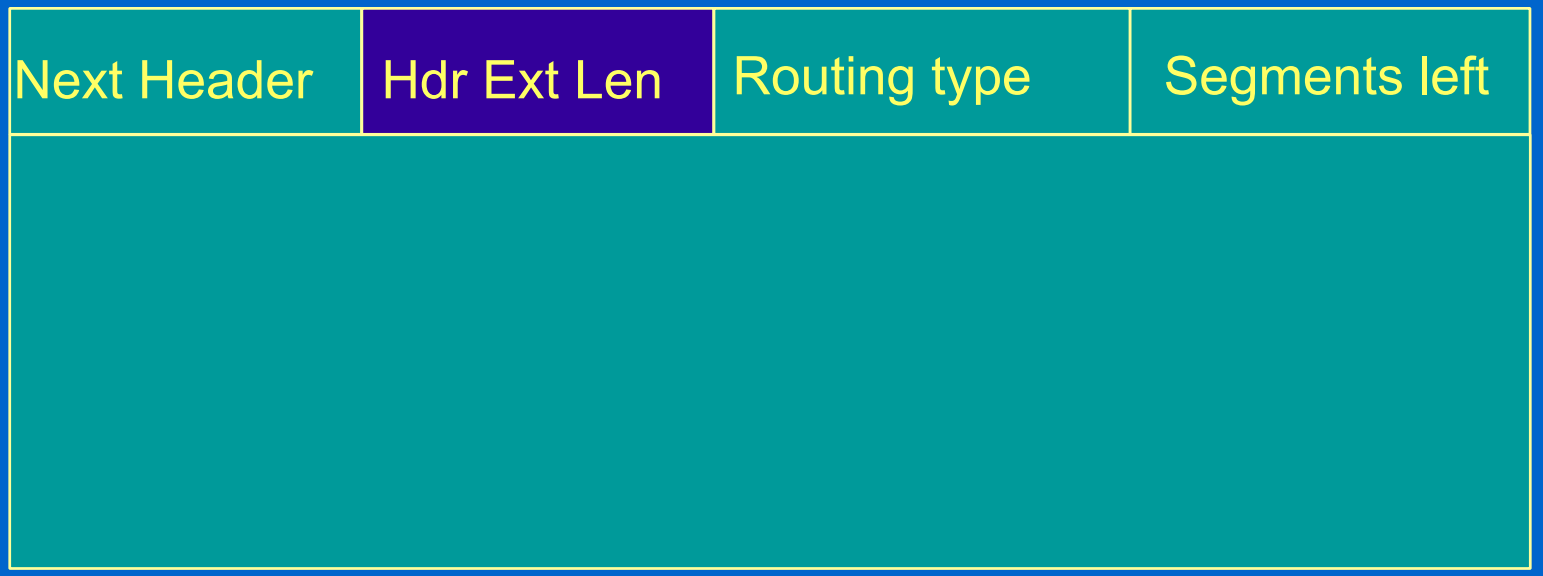
Vuonimiöiden käsittely solmuissa

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

Laajennusotsakkeet

- **reititysotsake** (Routing header)
  - laajennettu reititys ~IPv4:n lähdereititys,
  - vaadittu reitti tai reitin osa
- **paloitteluotsake** (Fragmentation header)
  - paloitteluun ja kokoamiseen liittyvää tietoa
- **Turvaotsakkeet => IPSec**
  - salausotsake ESP ja autentikointiotsake AH
- **kohdeoptioiden otsake** (Destination Options header)
  - paketin vastaanottajille tarkoitettua tietoa
- **Hop-By-Hop- optioiden otsake**
  - tietoja reitittimille, käsitellään joka reitittimessä

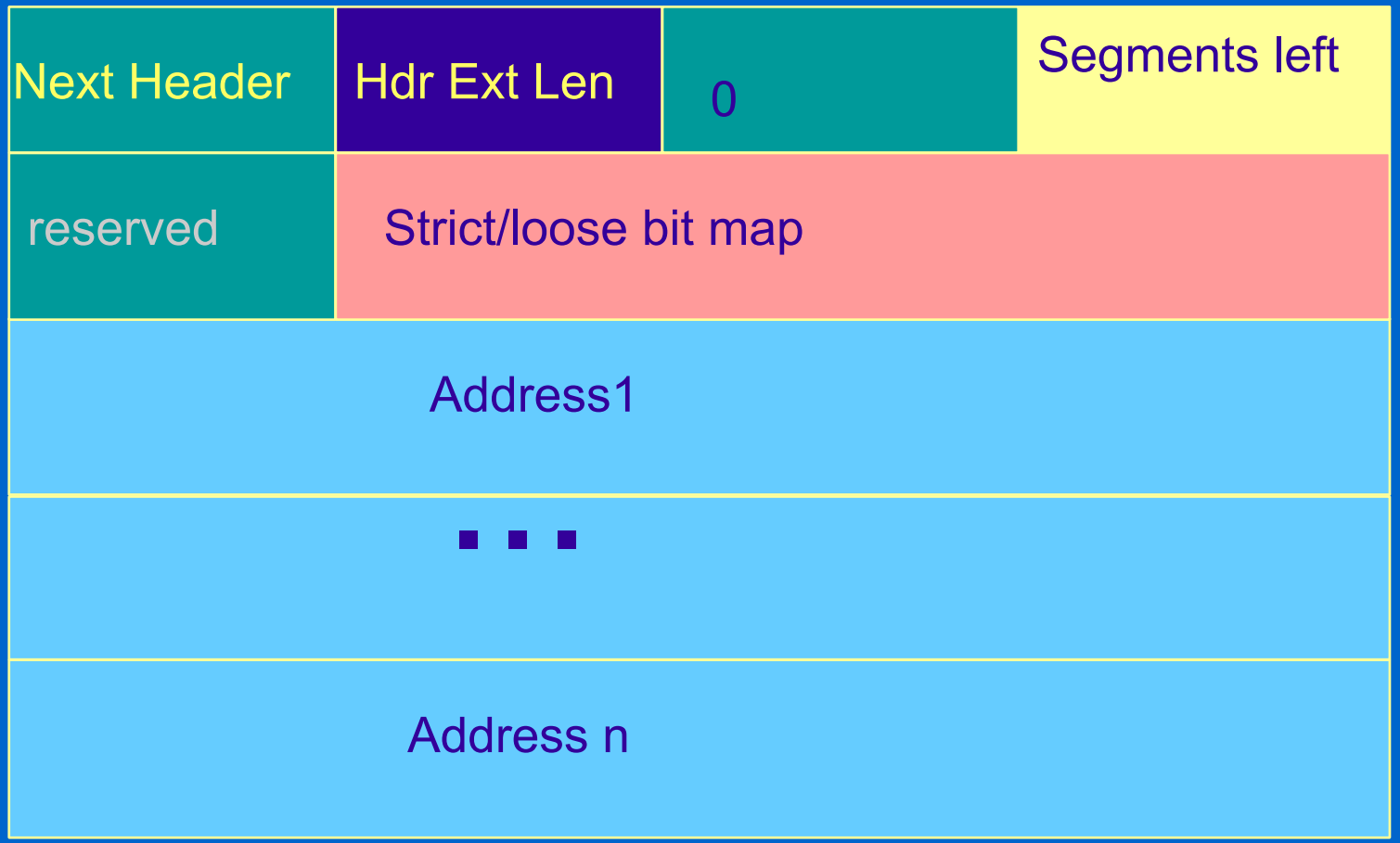
Reititysotsake



Routing type (8 bittiä): reititysotsakkeen tyyppi = 0

Segments left (8 bittiä): vielä kuljettavien välisolmujen määrä

Tyypin 0 reititysotsake



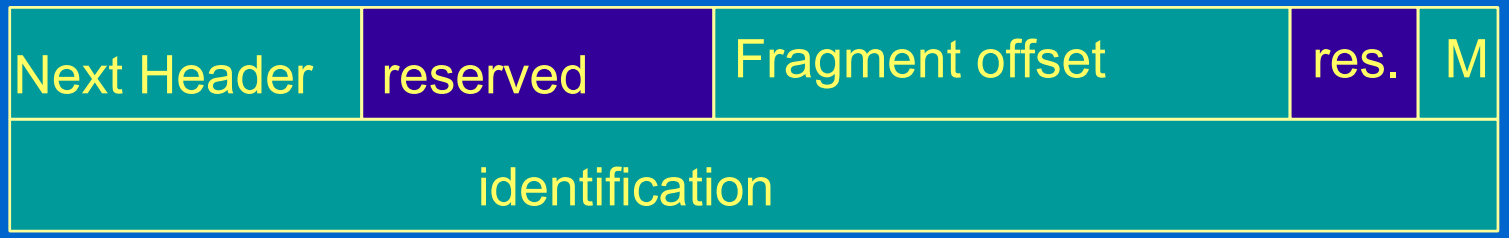
Bit map (23 bittiä): 1 (strict routing) = vastaava osoite on seurava solmu, 0 (loose routing) = ei välttämättä oltava seuraava osoite

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

Paloittelu (fragmentation)

- IPv6: lähettäjäsolmu paloittelee sanoman
  - 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
    - 1280 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

1. pak.	IPv6-otsake	paloitteluotsake	UDP-otsake + data
2. pak.	IPv6-otsake	paloitteluotsake	UDP-otsake + data
3. pak.	IPv6-otsake	paloitteluotsake	UDP-otsake + data
4. pak.	IPv6-otsake	paloitteluotsake	UDP-otsake + data

Turvallisuusotsakkeet

- **kaksi erilaista turvallisuusotsaketta**
  - Autentikointiotsake AH (Authentication Header)
    - varmentaa lähettäjän
    - takaa paketin muuttumattomuuden
    - itse paketti selväkielisenä
  - Salakirjoituksella suojattu –otsake ESP (Encrypted security payload)
    - edellisten lisäksi salakirjoittaa kuorman

AH-otsake

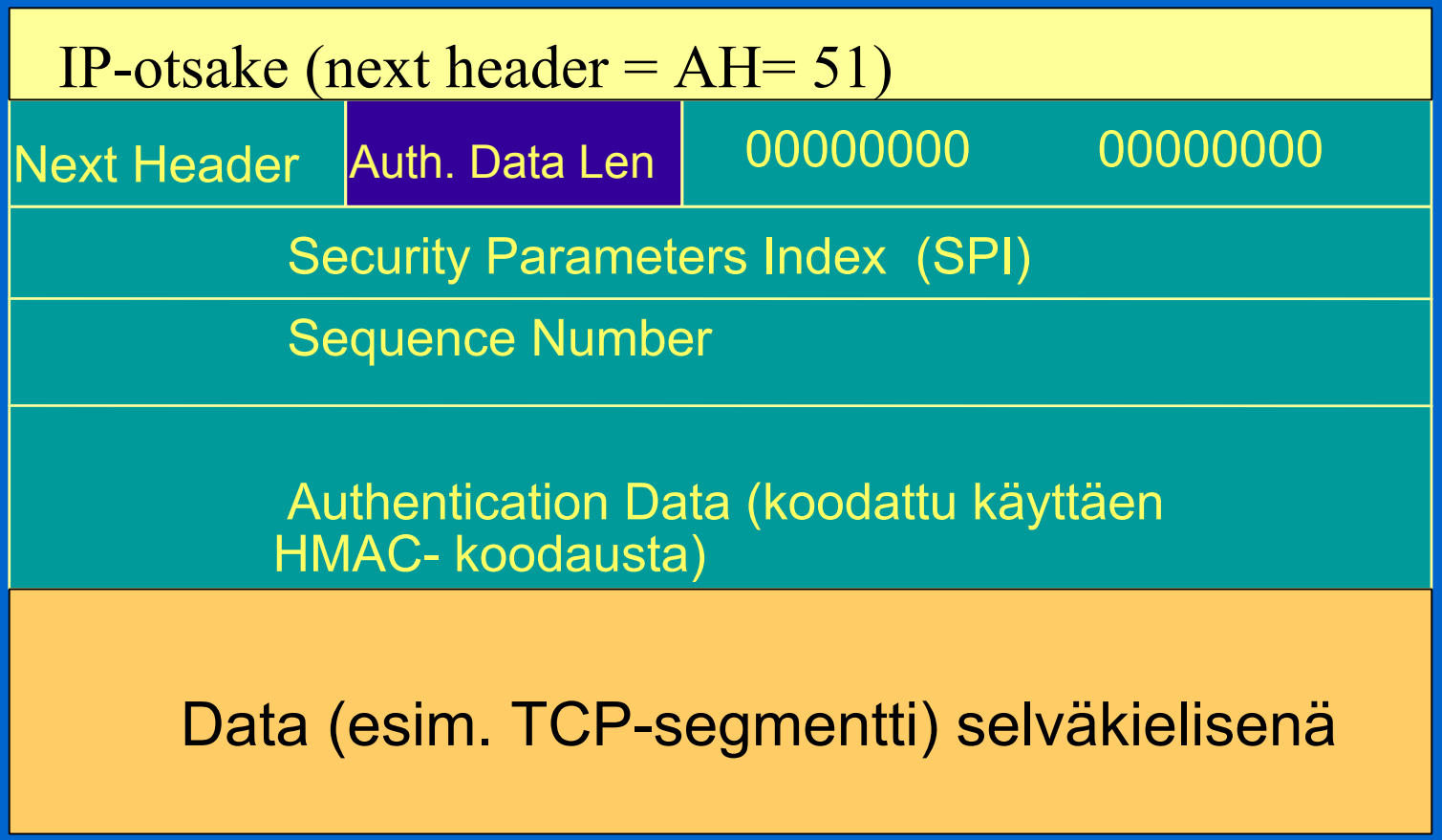
- Varmistaa datagrammin eheyden ja lähettäjän identiteetin
  - "juuri tämä lähettäjä on lähettänyt juuri tämän paketin"
    - kukaan ei väärentänyt lähettäjää
    - kukaan ei ole millaan tavoin muuttanut pakettia

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, yhteyden alussa 0
- Authentication Data
  - sanoman digitaalinen allekirjoitus => lähettäjän identiteetin ja sanoman yheyden varmistus
    - esim. DES, MD5 tai SHA

AH-otsake


IP-otsake (next header = AH= 51)
Next Header
Auth. Data Len
00000000
00000000
Security Parameters Index (SPI)
Sequence Number
Authentication Data (koodattu käyttäen HMAC- koodausta)
Data (esim. TCP-segmentti) selväkielisenä

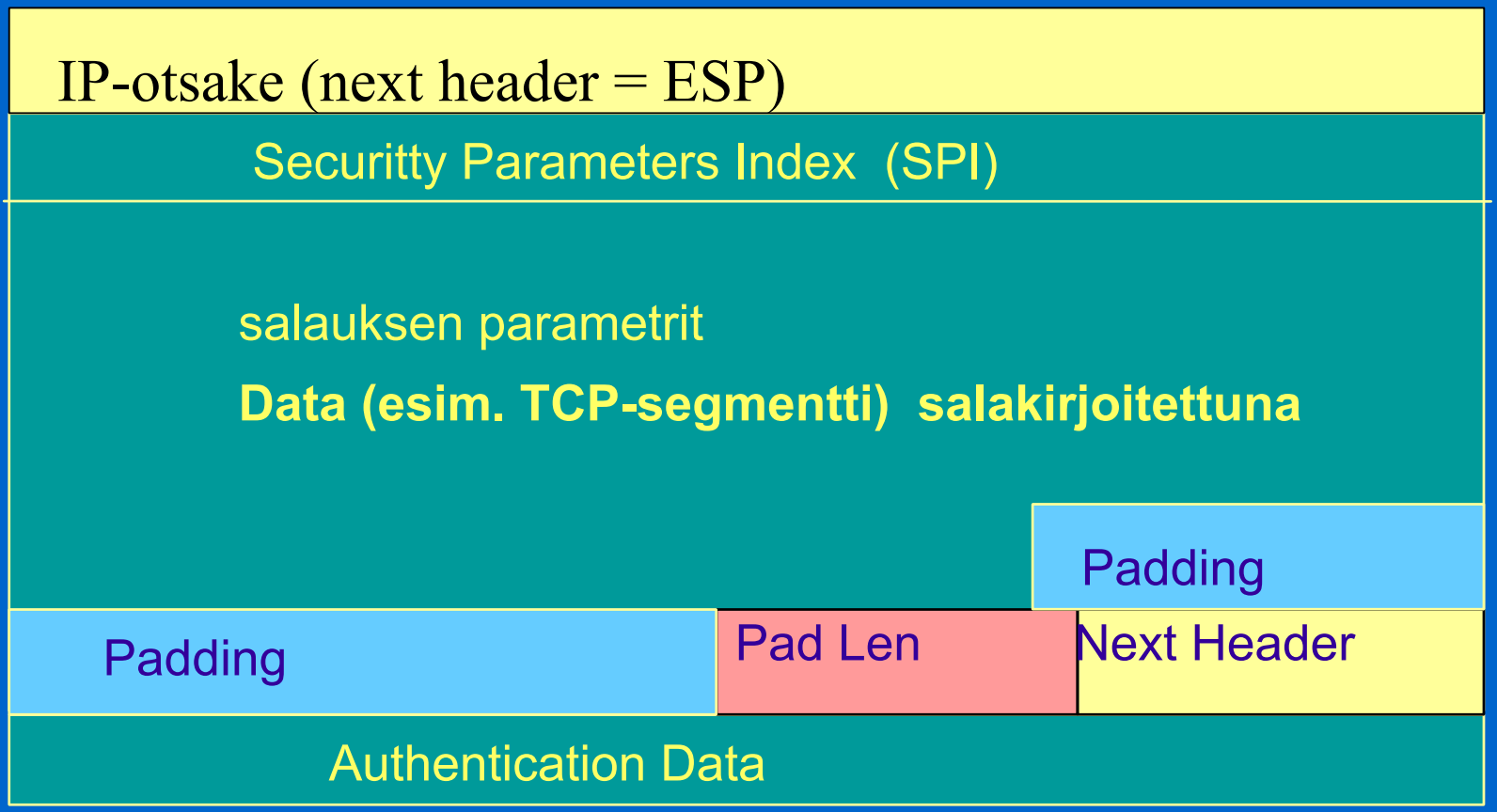
ESP-otsake

- Sanoman salaus ja lähettäjän autentikointi

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

Salakirjoituksessa DES-CBC (Cipher Block Chaining)

ESP-otsake


IP-otsake (next header = ESP)
Securitty Parameters Index (SPI)
salauksen parametrit
Data (esim. TCP-segmentti) salakirjoitettuna
Padding
Padding
Pad Len
Next Header
Authentication Data

Turvallisuus verkkokerroksella

- IPsec
  - **Authentication Header (AH) -protokolla**
  - **Encapsulation Security Payload (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 saman SA:n IPsec-datagrammeissa sama SPI-arvo
  - ISKMP (Internet Security Association and Key Management Protocol)
    - muodostaa ja purkaa SA-yhteyksiä
    - IKE (Internet Key Exchange) -algoritmi avainten hallintaan

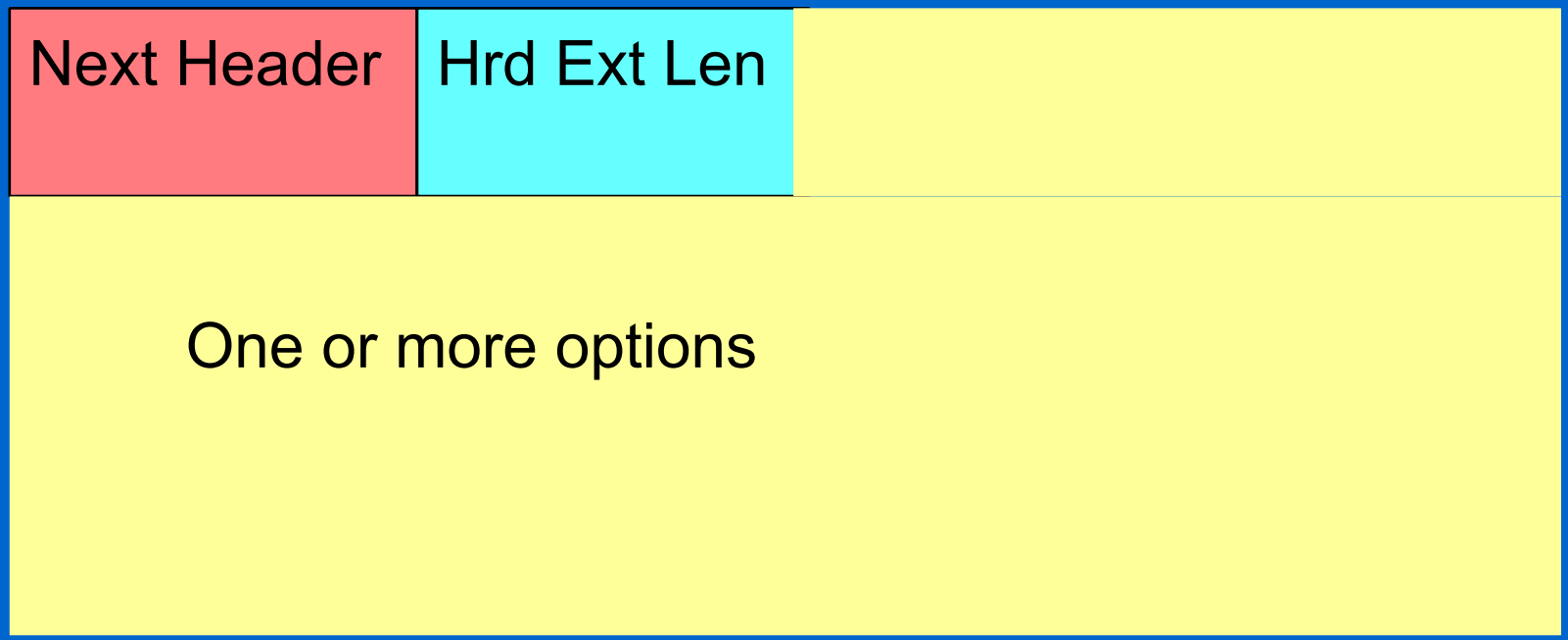
IPsec ja IPv4 / IPv6

- IPsec toimii sekä IPv4:n että IPv6:n kanssa

Kohdeoptioiden otsake

- **käsitellään vasta kohteessa**
- **geneerinen kohdeoptio-otsake**
  - säästää tyyppinumeroita (vain 256 kpl)
  - parametreinä voi olla useita yksittäisiä kohdeoptioita
  - toistaiseksi käytössä vain PAD-optiot
    - lisää yhden (Pad1) tai n kappaletta (Padn) täytetavuja

Hop-by-hop -optioiden laajennusotsake

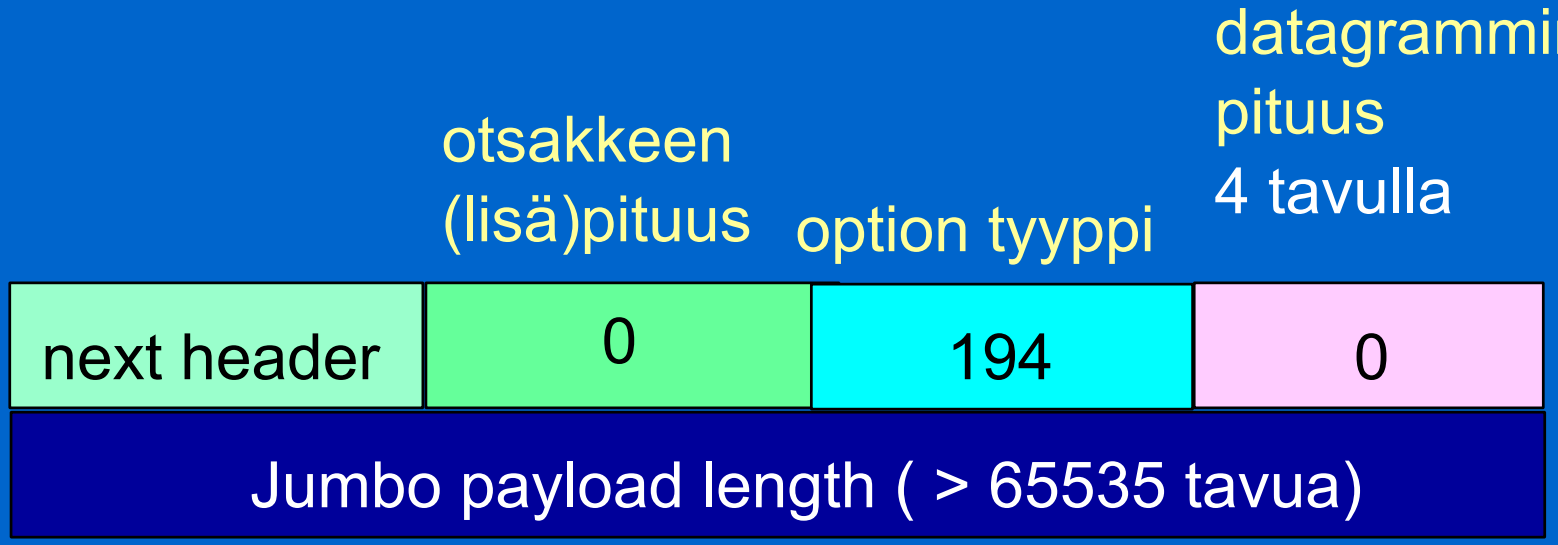


Next Header: seuraavan otsakkeen tyyppi

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

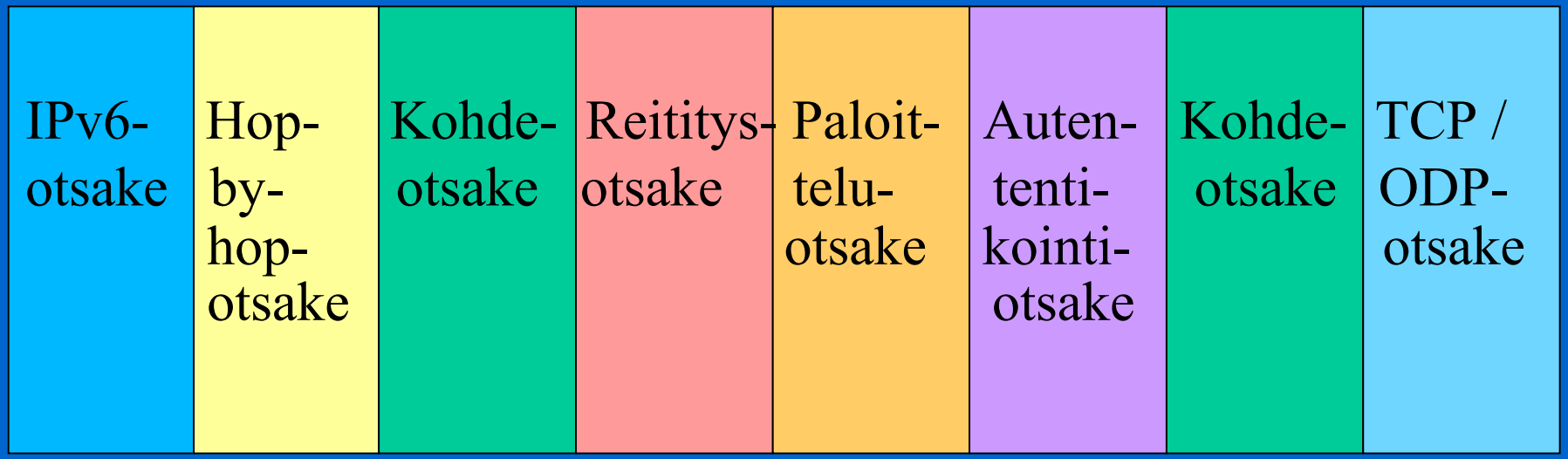


Maksimikooksi yli 4 Gtavua

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.

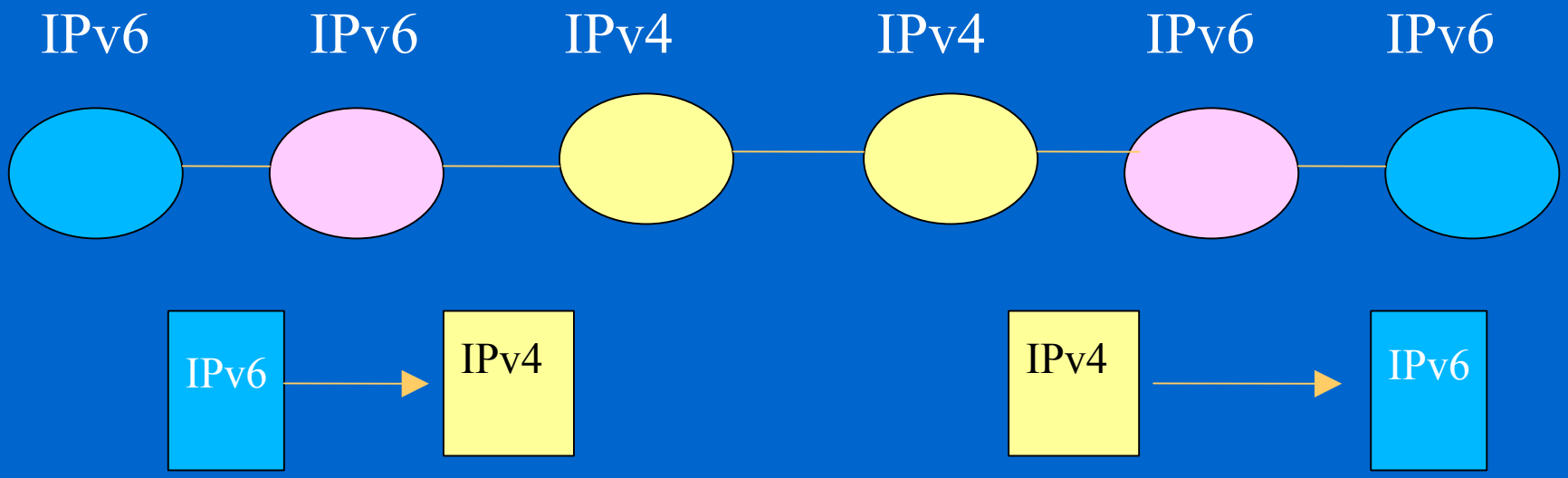
Otsakkeiden järjestys



Siirtyminen IPv4 => IPv6

- Kestää pitkään
  - edellinen suuri muutos NCP--> TCP 20 vuotta sitten ja silloin Internet oli paljon pienempi!
  - Nyt satoja miljoonia koneita ja miljoonia verkon ylläpitäjiä
- Ratkaisuja
  - kaksoispino (Dual stack)
    - IPv6-solmut toteuttavat myös IPv4:n toiminnot
  - tunnelointi (tunneling)
    - IPv6-saarekkeet kommunikoivat IPv4-verkkojen läpi kuin minkä tahansa muun verkon läpi
    - lähettävät IPv6-sanomat ‘kapseloituina’ IPv4-sanomien sisällä

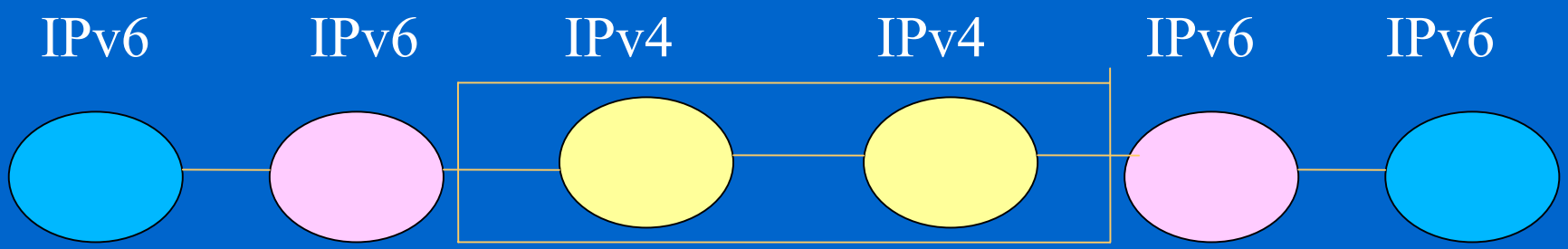
Kaksoispino



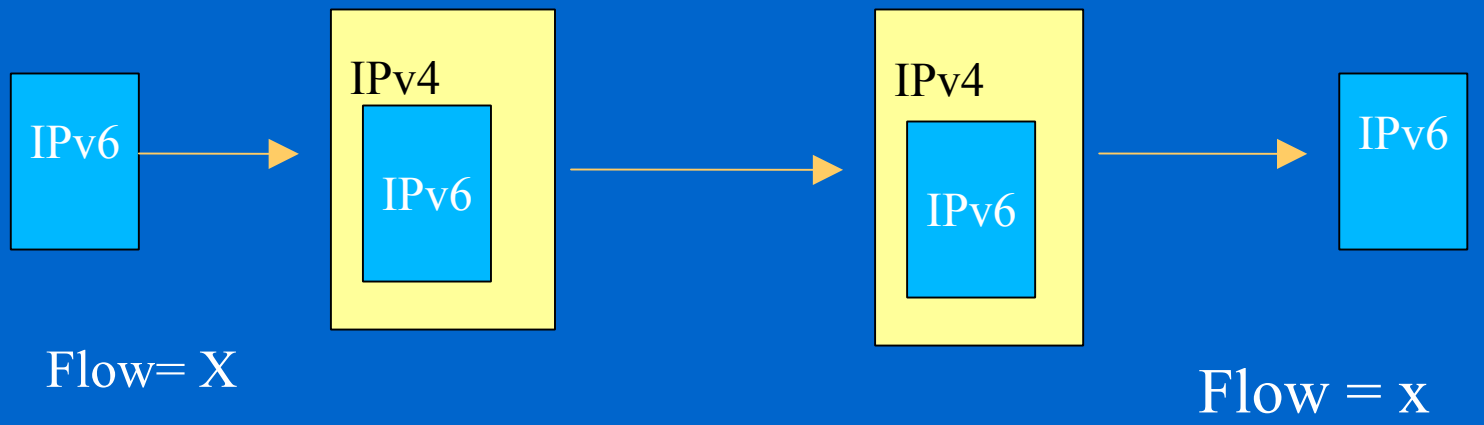
Flow= X

Flow = ??

Tunnelointi



tunneli



Onko IPv6 edes tarpeen?

- Asiakkaat eivät kysele!
  - **CIDR** (Classless Interdomain Routing), **DHCP** (Dynamic Host Configuration Protocol), **NAT** (Network Address Translation) **ratkaisseet osoiteongelman**
- Valmistajat eivät ole kiinnostuneita!
- Euroopassa ja Japanissa laajempi kiinnostus
- 6Bone

3. Verkkokerroksen muita protokollia ja mekanismeja

- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- CIDR (Classless InterDomain Routing)
- NAT (Network Address Translation)

- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)
- IGMP (Internet Group Management Protocol)
- Mobile IP

3.1. ICMP (Internet Control Message Protocol)

- Verkkoinformaation välittämiseen isäntäkoneiden ja reitittimien välillä
  - reitittimet ilmoittavat verkon ongelmista toisilleen
  - reitittimet ilmoittavat lähetysten kohtalosta isäntäkoneille
    - "Destination network unreachable"
  - testauspakettien lähettäminen

- ICMP-sanomat kapseloidaan IP-paketteihin
  - TCP- ja UDP-segmenttien tavoin
  - IP-paketin protokollakentässä 'ICMP'
  - => paketti annetaan ICMP:n käsiteltäväksi
- ICMP-sanomassa
  - tyyppi + koodi kertovat sanoman
  - 8 tavua sanoman aiheuttaneesta IP-paketista
    - jotta lähettäjä tietää, mikä paketti aiheutti sanoman

ICMP-sanomia

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

Summary of Message Types

- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 11 Time Exceeded
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply

Type 3: Destination unreachable

Code

0 = net unreachable;

1 = host unreachable;

2 = protocol unreachable;

3 = port unreachable;

4 = fragmentation needed and DF set;

5 = source route failed.

6 = network unknown

7 = host unknown

Type 11:Time-To-Live exceeded

Sanoma hävitettiin, koska sen elinaika ehti kulua umpeen

Code

0 = time to live exceeded in transit;

1 = fragment reassembly time exceeded.

Type 12: Parameter problem

Virhe IP-otsakkeessa

- Sanomassa osoitin, joka kertoo virheellisen
- kohdan
  - ilmoittaa virheellisen tavun
  - esim. osoittimen arvo 1 kertoo, että vika on TOS-kentässä
- Sanoma lähetetään vain, jos IP-sanoma joudutaan virheen takia hävittämään

Type 4: Source quench

Tällä voidaan ilmoittaa lähettäjälle, että sen tulee vähentää lähettämistään

- reititin joutuu hävittämään paketteja puskuristaan
- vastaanottaja ei ehdi käsitellä paketteja sitä vauhtia kun niitä tulee

HUOM! Käyttöä ei suositella

- TCP-ruuhkanvalvonta
- TCP-vuonvalvonta