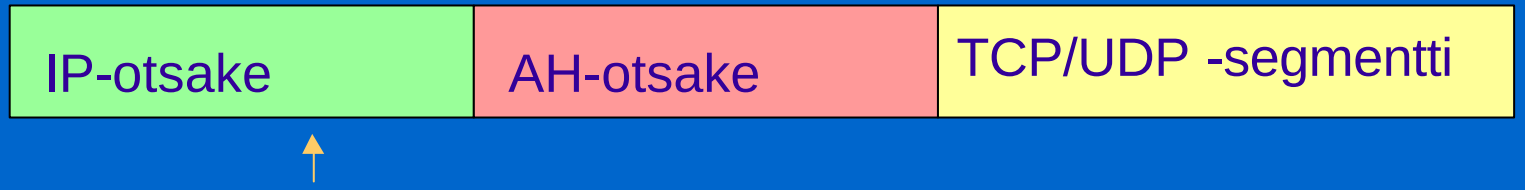
Turvallisuus verkkokerroksella

- **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

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

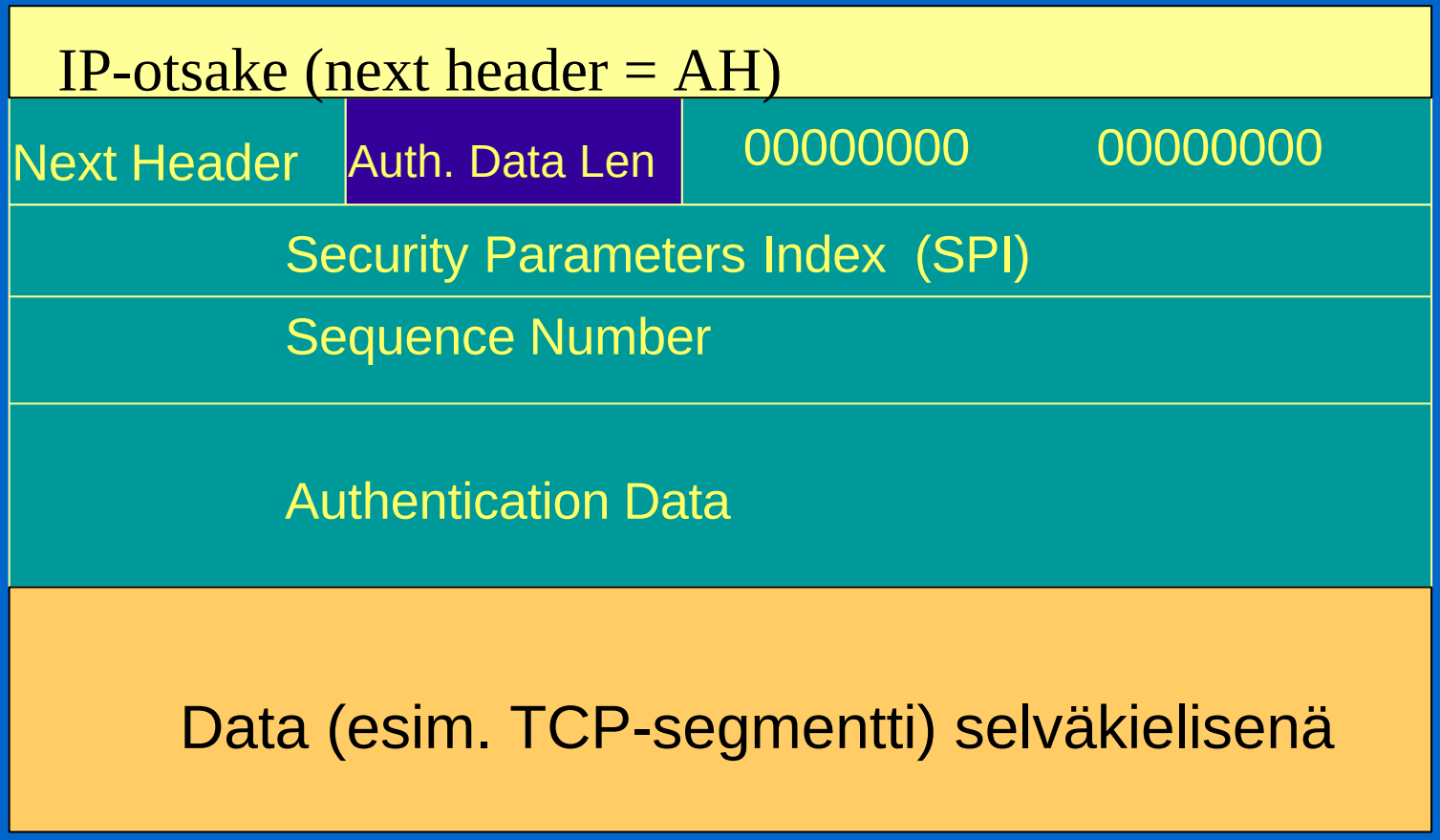


Protokollakenttä (= 51) ilmoittaa, että mukana on AH-otsake eli käytössä AH-protokolla

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)
Next Header
Auth. Data Len
00000000
00000000
Security Parameters Index (SPI)
Sequence Number
Authentication Data
Data (esim. TCP-segmentti) selväkielisenä

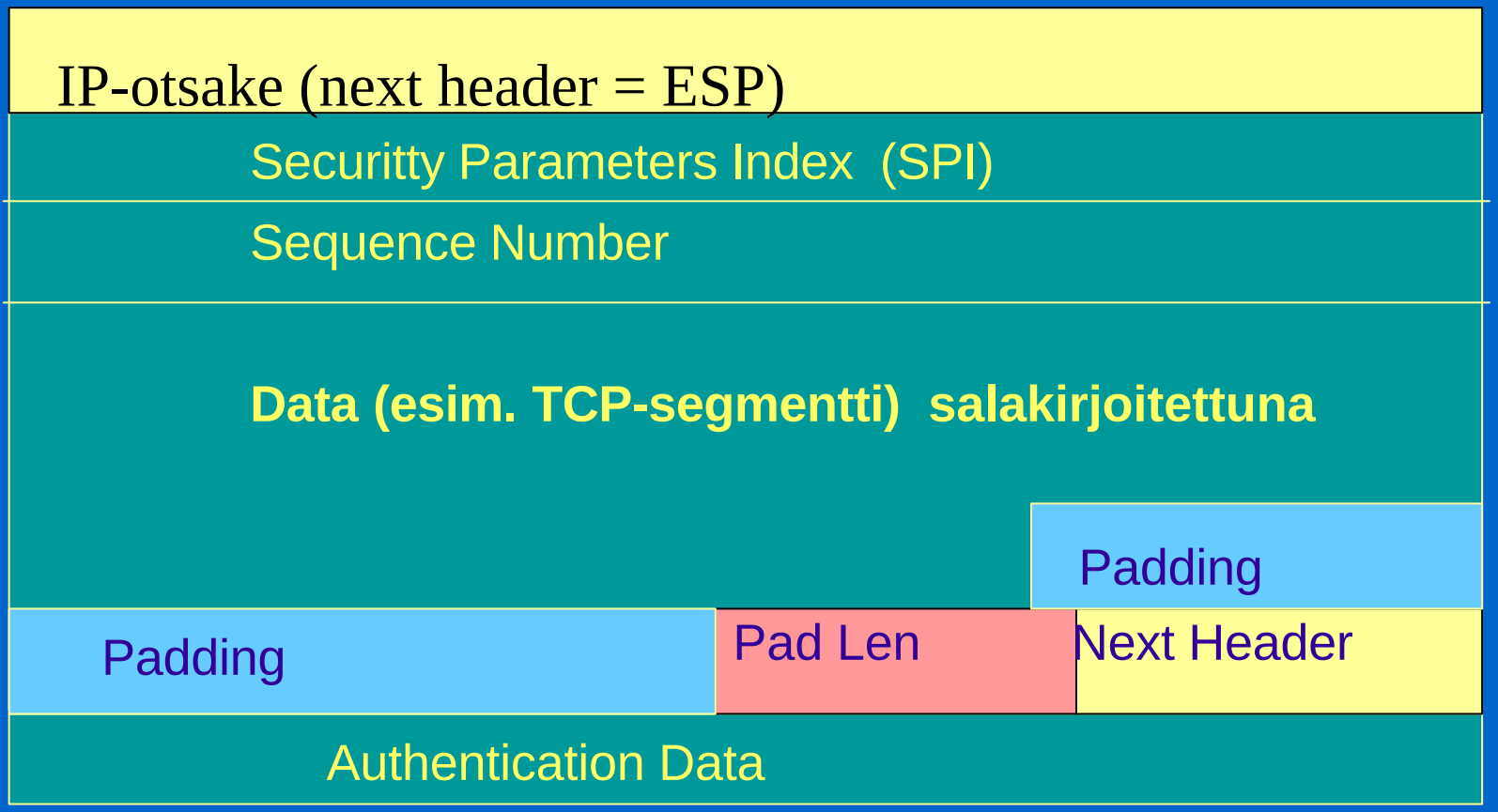
ESP-otsake

- **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)
Sequence Number
Data (esim. TCP-segmentti) salakirjoitettuna
Padding
Padding
Pad Len
Next Header
Authentication Data

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

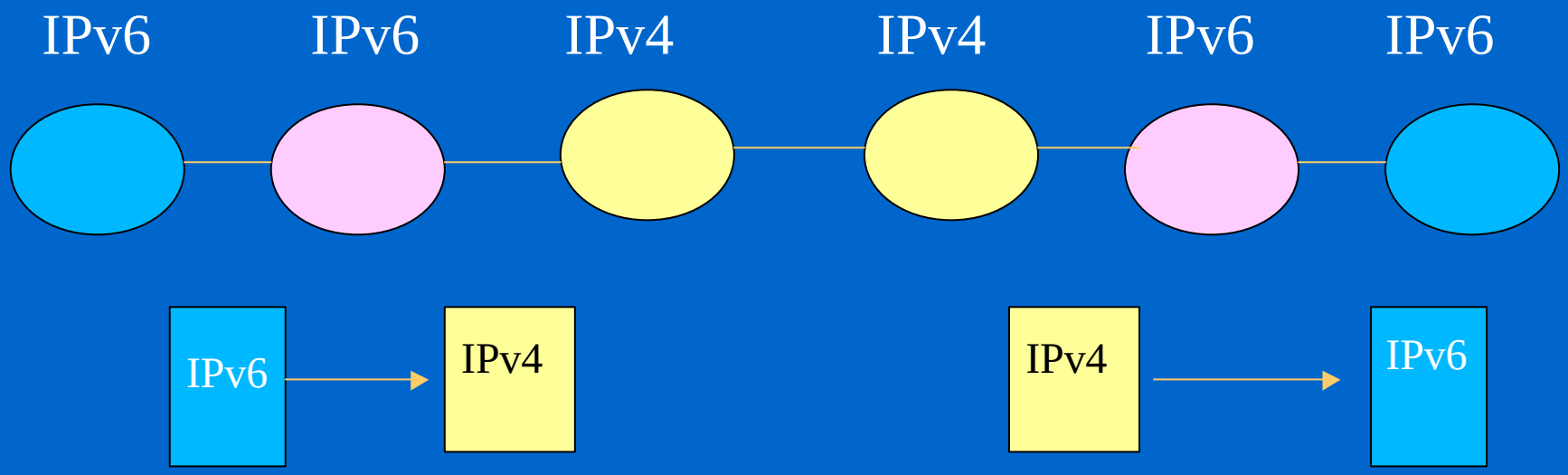
- **kahdeksan neljän heksaluvun ryhmää:**
  - 8000:0000:0000:0000:0123:4567:89AB:CDEF
    - ryhmän alkunollat voi jättää pois
    - 16 nollan ryhmät voi korvava kaksoispisteellä
  - => 8000::123:4567:89AB:CDEF
  - **IPv4-osoitteet => ::193.31.20.46**

- **osoitteita on PALJON!**
- **2**128 => ~3* 10**38**
- **tasaisesti jaettuna noin 7 * 10**23 IP-osoitetta jokaista maapallon pinnan neliömetriä kohden**
  - > Avogadron luku = 6.022 *10**23
    = value of the number of atoms, molecules, etc. in a gram mole of any chemical substance.
- **vaikka jako olisi epätasaisempi, ainakin yli 1000 IP-osoitetta neliömetriä kohden**

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

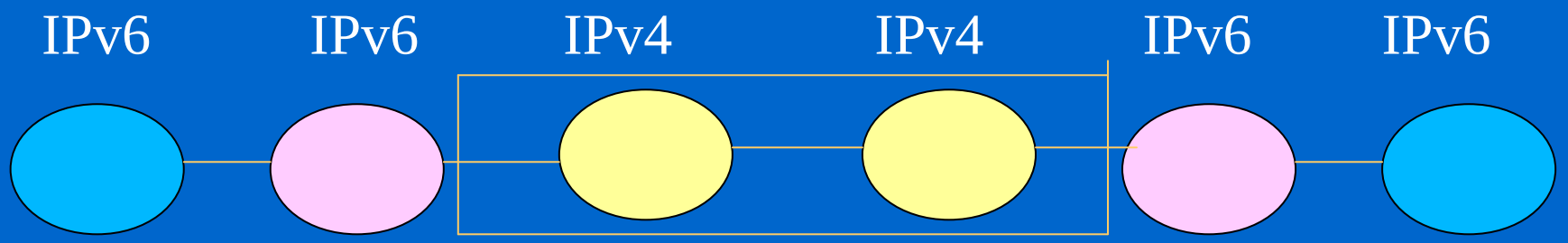
Kaksoispino



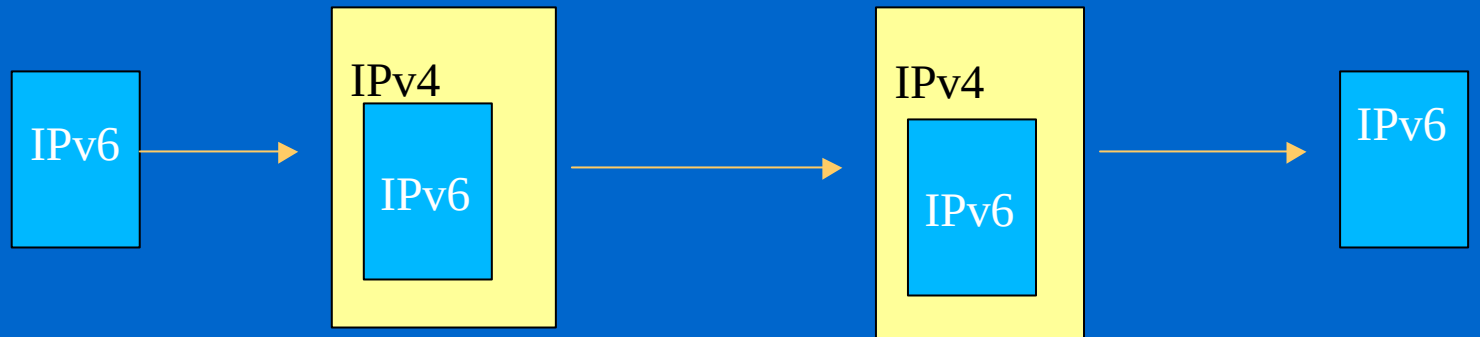
Flow= X

Flow = ??

Tunnelointi



tunneli



Flow= X

Flow = x

Onko IPv6 edes tarpeen?

- **Asiakkaat eivät kysele!**
- **Valmistajat eivät ole kiinnostuneita!**
- **Euroopassa ja Japanissa laajempi kiinnostus**
- **6Bone**

3. 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)

- **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

Type 5: Redirect

Reititin voi pyytää isäntäkonetta lähettämään sanoman toiselle reitittimelle

Code:

0 = Redirect datagrams for the Network.

1 = Redirect datagrams for the Host.

2 = Redirect datagrams for the Type of Service and Network.

3 = Redirect datagrams for the Type of Service and Host

Echo-sanomat

Type 0: echo reply
Type 8: echo request

Echo-pyynnön sanoma tulee palauttaa echo-vastauksessa

- ping-ohjelma lähettää echo-pyynnön koneelle ja pyynnön vastaanottanut kone palauttaa sen

Timestamp-sanomat

type 13: timestamp message
type 14: timestamp reply message

lähettäjä leimaa lähettäessään ja vastaanottaja saadessaan ja uudelleenlähettäessään

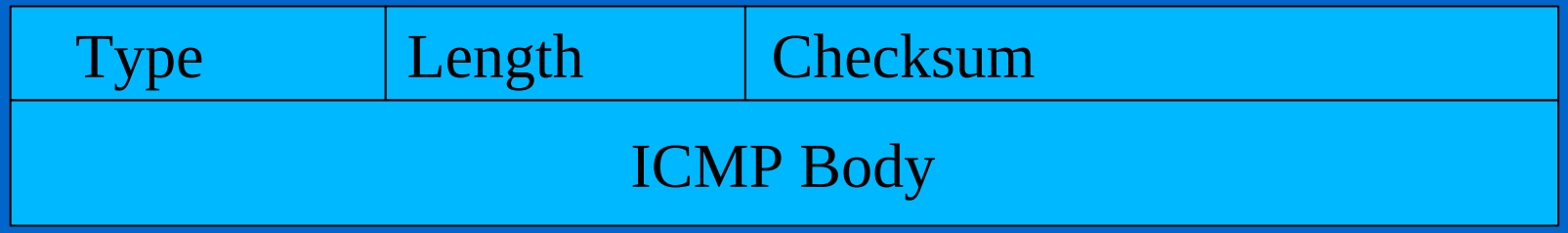
- The timestamp is 32 bits of milliseconds since midnight UT.

Traceroute-ohjelma

- **Lähettää kohdekoneelle ICMP-sanomia, joissa TTL on 1, 2, 3,... sekuntia**
  - reititin, jolla jonkin sanoman TTL loppuu, lähettää tästä ilmoituksen, jossa on reitittimen osoite ja aikaleima
- **Lähettäjä saa näin selville kiertoajan ja reitittimen eli kuljetun reitin lähettäjältä kohdekoneelle**

ICMPv6

- **IPv6:n myötä**
  - virtaviivaistus
    - ‘turhia’ piirteitä pois
    - monilähetysprotokollan toiminnot mukaan (IGMP)
    - isommat kentät IPv6-osoitteita varten



1	Destination Unreachable
2	Packet too Big
3	Time Exceeded
4	Parameter Problem
5	Echo Request
6	Echo Reply

ICMPv6 -sanomat