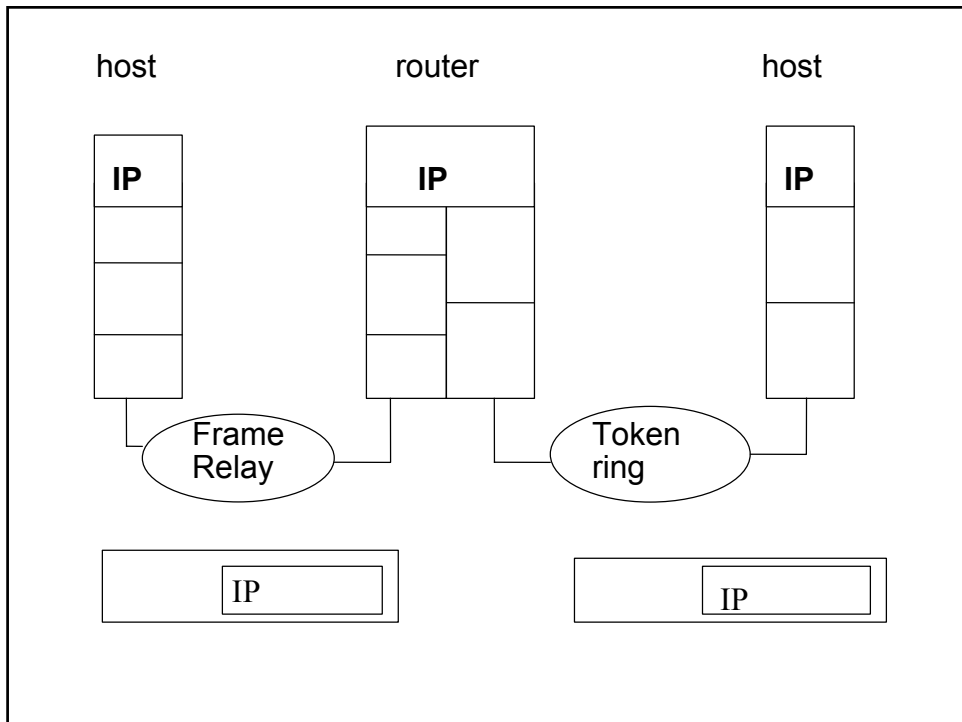


## 2. IPv6-protokolla

- enemmän osoitteita
  - 16 tavua osoitteelle=> osoitteita paljon!
- virtaviivaistettu
  - nopeampi käsittely reitittimissä => tehokkaampi
- uusia piirteitä
  - erilaisten sovellusten tarpeet huomioon
  - turvauspiirteet

## Internet

- Yhdistää hyvin erilaiset verkot yhteentoimivaksi kokonaisuudeksi
  - kaikkien käytettävä samaa **IP-protokollaa**
  - kaikkien käytettävä samaa **IP-osoitustapaa**
- verkkojen tarvitsee osata vain kuljettaa dataa lähettäjältä vastaanottajalle
  - samantekevää kuinka sen tekee
  - verkko=> 'linkkiyhteys' tai tunneli



## Internetin verkkokerros

- Internet
  - on kokoelma ‘itsenäisiä’ aliverkkoja eli autonomisia järjestelmiä (AS, Autonomous Subsystem)
  - joita yhdistävät runkolinjat
- IP-protokolla
  - verkkotason protokolla, joka pitää Internetin koossa
  - tavoite: **kuljettaa paketti (datagram) lähteestä kohteeseen yli kaikkien tarpeellisten verkkojen**

- o
- o
- o

# IP-osoitteet

- jokaisella verkon isäntäkoneella ja reitittimellä on oma yksikäsitteinen osoite muotoa
  - verkon numero
  - isäntäkoneen numero
- IPv4:n osoite on 32-bittinen
  - luokallinen reititys (A-, B- ja C-luokan osoitteet)
  - **CIDR** (Classless Interdomain Routing)
    - verkko-osan pituus vaihtelee : a.b.c.d/'pituus bitteinä'
    - **200.23.16.0/20**

18.9.2003

5

|    | 0     | 8                         | 16         | 24 | 31 |
|----|-------|---------------------------|------------|----|----|
| A: | 0     | verkko-os.                | koneosoite |    |    |
| B: | 10    | verkko-osoite             | koneosoite |    |    |
| C: | 110   | verkko-osoite             | koneos.    |    |    |
| D: | 1110  | monilähetysosoite         |            |    |    |
| E: | 11110 | varattu tulevaan käyttöön |            |    |    |

## IP-osoitteiden luokkamuodot

## IP-osoitteiden luokkajako

- A-luokka: 126 verkkoa, 16 miljoonaa konetta/verkko
- B-luokka: 16382 verkkoa, 65528 konetta/verkko
- C-luokka: noin 2 miljoonaa verkkoa, kussakin korkeintaan 254 konetta
- D-luokka: monilähetysosoite
- E-luokka: varattu tulevaan käyttöön
  
- Luokkajako osoittautui epäonnistuneeksi:
  - C-luokassa koneita liian vähän => useita eri verkkoja
  - B-luokassa koneita liian paljon => hukkakäyttöä, B-osoitteet olivat loppua
  - => CIDR: tehokkaampi osoitevaruuden hyödyntäminen
  - => NAT: osoitteiden yhteiskäyttö

18.9.2003

7

## IPv6

Ratkaise IP:n osoiteongelman + virtaviivaistaa IP:tä

- tavoitteita:
  - biljoonia osoitteita
  - pienempiä reititystauluja
  - yksinkertaisempia protokollia
  - turvallisuutta
  - mukaan palvelutyypit: (tosiaikainen), monilähetys
  - liikkuvien koneiden osoitteet
  - jatkokehitys ja nykyisten protokollien toimivuus

18.9.2003

8

# IPv6

- **16 tavun osoitteet** (= 128 bittia)
  - => 'rajaton' määrä osoitteita
- **yksinkertaisempi otsake-kenttä**
  - kiinteä kehys, jossa vain 7 kenttää
- **valinnaisten piirteiden käsittely**
  - monet ennen pakolliset nyt valinnaisia
  - opitoiden 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                                 | TC | Flow label  |           |
| Payload length                    |    | Next header | Hop limit |
| Source address<br>(16 tavua)      |    |             |           |
| Destination address<br>(16 tavua) |    |             |           |

|                          |            |                          |                             |          |
|--------------------------|------------|--------------------------|-----------------------------|----------|
| Versio                   | IHL        | TOS                      | Datasähkeen pituus (tavuja) |          |
| Tunniste                 |            |                          | Flag                        | Siirtymä |
| Elinaika                 | Protokolla | otsakkeen tarkistussumma |                             |          |
| Lähtäjän IP-osoite       |            |                          |                             |          |
| Vastaanottajan IP-osoite |            |                          |                             |          |
| Optiot (jos on käytössä) |            |                          |                             |          |
| data                     |            |                          |                             |          |

## IPv4 - datasähke

## Otsakekentät

- **Versio (version)**
  - aina 6 IPv6:lle ja 4 Ipv4:lle
- **Liikenneluokka (traffic class) (tai 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: lähdeosoite 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

## IPv6: osoiteavaruus

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



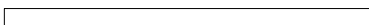
# Osoitteen esitysmuoto

kahdeksan neljän heksaluvun ryhmää:

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



- osoitteita on PALJON!
- $2^{128} \Rightarrow \sim 3 \cdot 10^{38}$
- tasaisesti jaettuna noin  $7 \cdot 10^{23}$  IP-osoitetta jokaista maapallon pinnan neliometriä kohden
  - > Avogadron luku =  $6.022 \cdot 10^{23}$   
= 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 neliometriä kohden

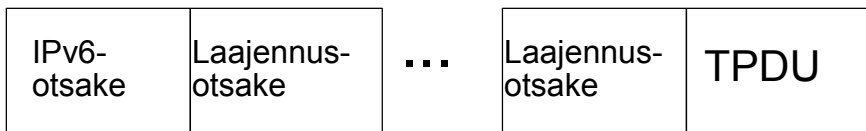


## IPv4:n kentistä puuttuvat

- **paketin paloitteluun liittyvät kentät**
  - kaikki kykenevät käsittelemään ainakin 1280 tavun paketteja
  - lähettäjä huolehtii, että paketti on riittävän pieni
    - reititin ilmoittaa virheestä, jos se havaitsee liian suuren paketin => ohjeet pilkkoa paketti pienemmäksi
    - Lähettäjä paloittelee tarvittaessa itse
- **tarkistussumma**
  - ei lasketa verkkokerroksella
    - luotettavimmat verkot
    - siirtoyhteyskerros laskee / kuljetuskerros laskee

18.9.2003

19



**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

## 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

18.9.2003

21

## Ruuhkavalvottu liikenne

### ❖ Prioriteetit 0- 7

- 0 määrittelemätön liikenne (uncharacterized traffic)
- 1 täyttöliikenne (filler traffic) verkkouutiset, USENET-sanomat
- 2 Iliikenne, jota käyttäjä ei odotele (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

18.9.2003

22

# 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 häiriöääniä linjalla

# Vuonimiö

## • Vuo

- samasta lähteestä samoille vastaanottajille kulkeva peräkkäisten pakettien jono, jota reitittimien halutaan käsittelevän tietyllä tavalla
  - tiedostonsiirto usealla TCP-yhteydellä => yksi vuo
  - multimediakonferenssi => monta erilaista vuota
- lähdeosoite + 20-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 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 reitin 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

- o
- o
- o

# Reititysotsake

| Next Header | Hdr Ext Len | Routing type | Segments left |
|-------------|-------------|--------------|---------------|
|             |             |              |               |

**Routing type** (8 bittiä): reititysotsakkeen tyyppi = 0

**Segments left** (8 bittiä): vielä kuljettavien välisolmujen määrä

## Tyypin 0 reititysotsake

| Next Header | Hdr Ext Len          | 0 | Segments left |
|-------------|----------------------|---|---------------|
| reserved    | Strict/loose bit map |   |               |
| Address1    |                      |   |               |
| ■ ■ ■       |                      |   |               |
| Address n   |                      |   |               |

**Bit map** (23 bittiä): 1 (strict routing) = vastaava osoite on seuraava 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



- o
- o
- o

# Paloittelu-otsake

|                |          |                 |      |   |
|----------------|----------|-----------------|------|---|
| Next Header    | reserved | Fragment offset | res. | M |
| identification |          |                 |      |   |

**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



- o
- o
- o

|         |             |                  |                   |
|---------|-------------|------------------|-------------------|
| 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

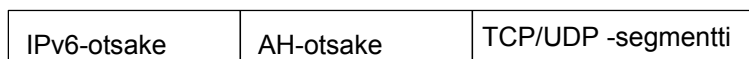
- **kaksi erilaista turvallisuusotsaketta**
  - Autentikointiotsake AH (Authentication Header)
    - varmentaa lähettäjän
    - takaa paketin muuttumattomuuden
    - itse paketti selväkielisenä
  - Salakirjoituksella suojattu –otsake ESP (Encapsulation Security Payload)
    - edellisten lisäksi salakirjoittaa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

18.9.2003

35

# AH-otsake

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



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

18.9.2003

36

# 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 yhteyden varmistus
    - esim. DES, MD5 tai SHA

18.9.2003

37

# AH-otsake

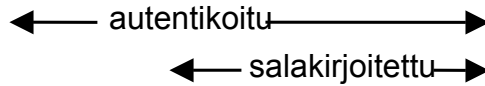
|   |                |          |          |
|---|----------------|----------|----------|
| IP-otsake (next header = AH= 51)                        |                |          |          |
| Next Header   | Auth. Data Len | 00000000 | 00000000 |
| Security Parameters Index (SPI)                     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

18.9.2003

38

# ESP-otsake

- Sanoman salaus ja lähettäjän autentikointi

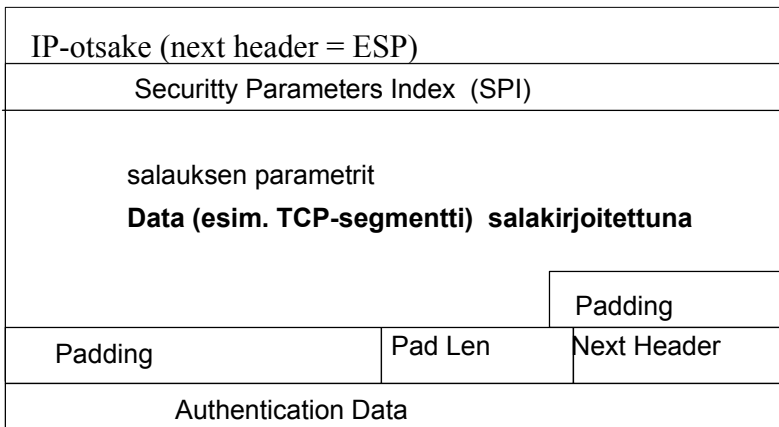


|           |            |               |            |                   |
|-----------|------------|---------------|------------|-------------------|
| IP-otsake | ESP-otsake | TCP/UDP-segm. | ESP-peräke | ESP-autentikointi |
|-----------|------------|---------------|------------|-------------------|

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

Salakirjoituksessa DES-CBC (Cipher Block Chaining)

# ESP-otsake



# 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

18.9.2003

## IPsec ja IPv4 / IPv6

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

18.9.2003

42

## 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) täytetäviä

## Hop-by-hop -optioiden laajennusotsake

|                     |             |  |
|---------------------|-------------|--|
| Next Header         | Hrd Ext Len |  |
| One or more options |             |  |

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

|                                       | otsakkeen<br>(lisä)pituus | option tyyppi | datagrammin<br>pituus<br>4 tavulla |
|---------------------------------------|---------------------------|---------------|------------------------------------|
| next header                           | 0                         | 194           | 0                                  |
| Jumbo payload length ( > 65535 tavua) |                           |               |                                    |

**Maksimikooksi yli 4 Gtavua**

18.9.2003

45

## Otsakkeiden järjestys

- Standardin otsakkeet annetaan sovitussa 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 laajennusotsakkeena.

18.9.2003

46

## Otsakkeiden järjestys

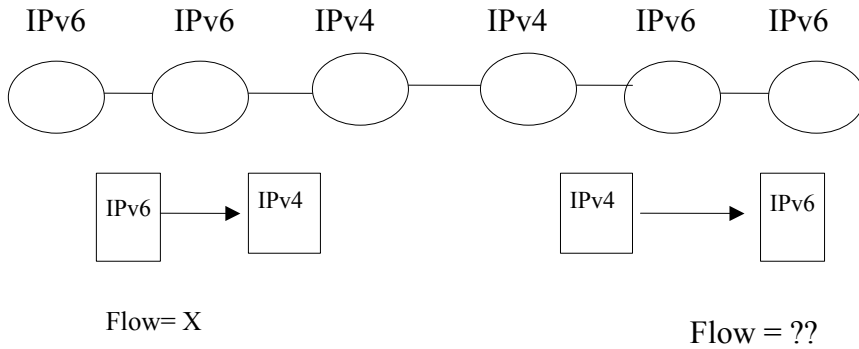
|             |                   |              |                 |                  |                     |              |                  |
|-------------|-------------------|--------------|-----------------|------------------|---------------------|--------------|------------------|
| IPv6-otsake | Hop-by-hop-otsake | Kohde-otsake | Reititys-otsake | Paloitelu-otsake | Autenttointi-otsake | Kohde-otsake | TCP / ODP-otsake |
|-------------|-------------------|--------------|-----------------|------------------|---------------------|--------------|------------------|

## 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



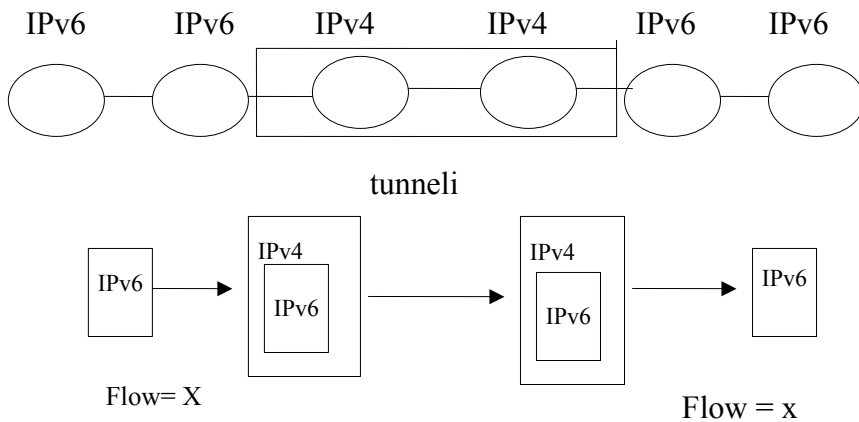
# Kaksoispino



18.9.2003

49

# Tunnelointi



18.9.2003

50

## 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