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

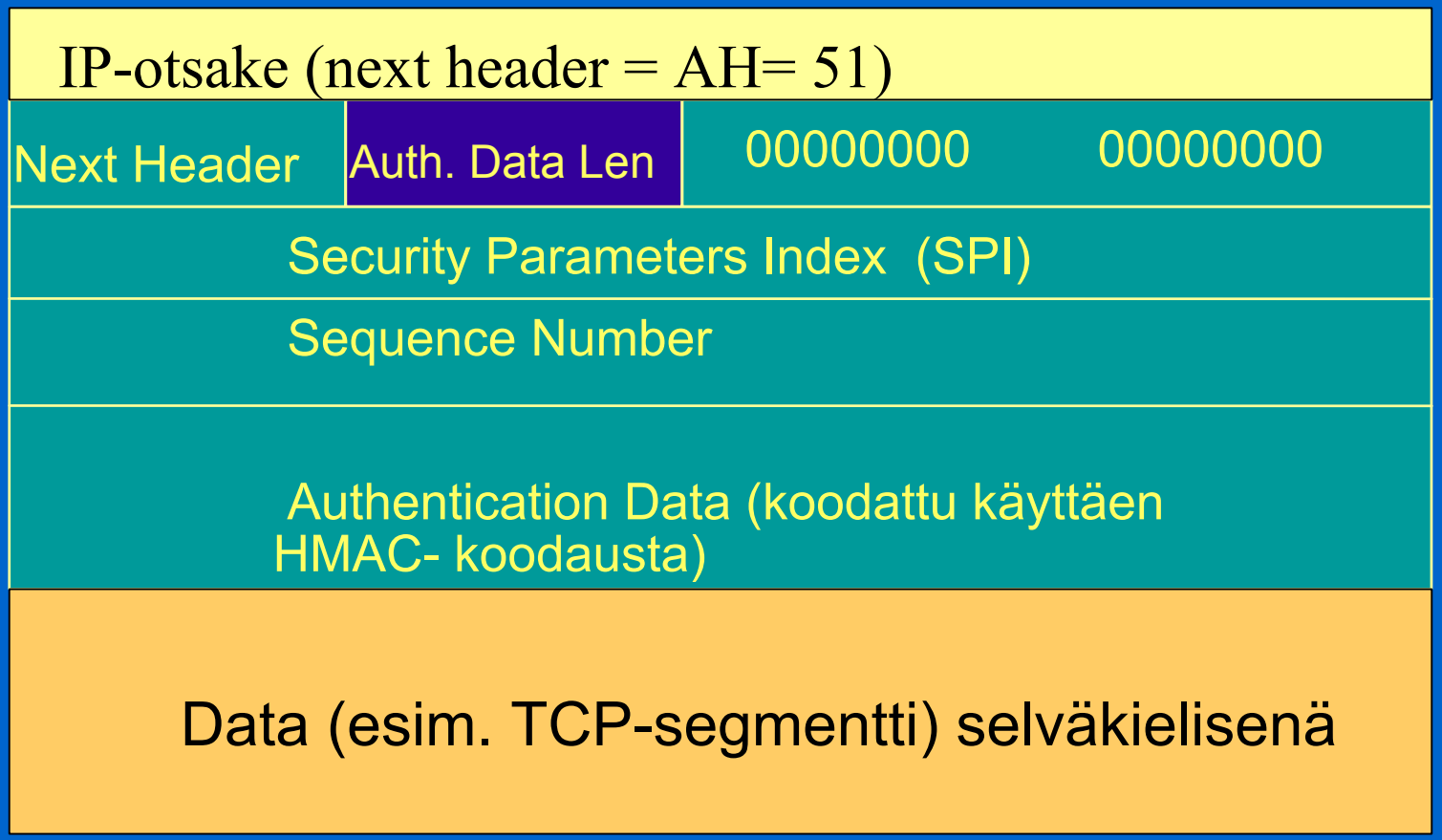
- Varmistaa datagrammin eheyden ja lähettäjän identiteetin
  - " juuri tämä lähettäjä on lähettänyt juuri tämän paketin"
    - kukaan ei väärentänyt lähettäjää
    - kukaan ei ole millaan tavoin muuttanut pakettia

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= 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

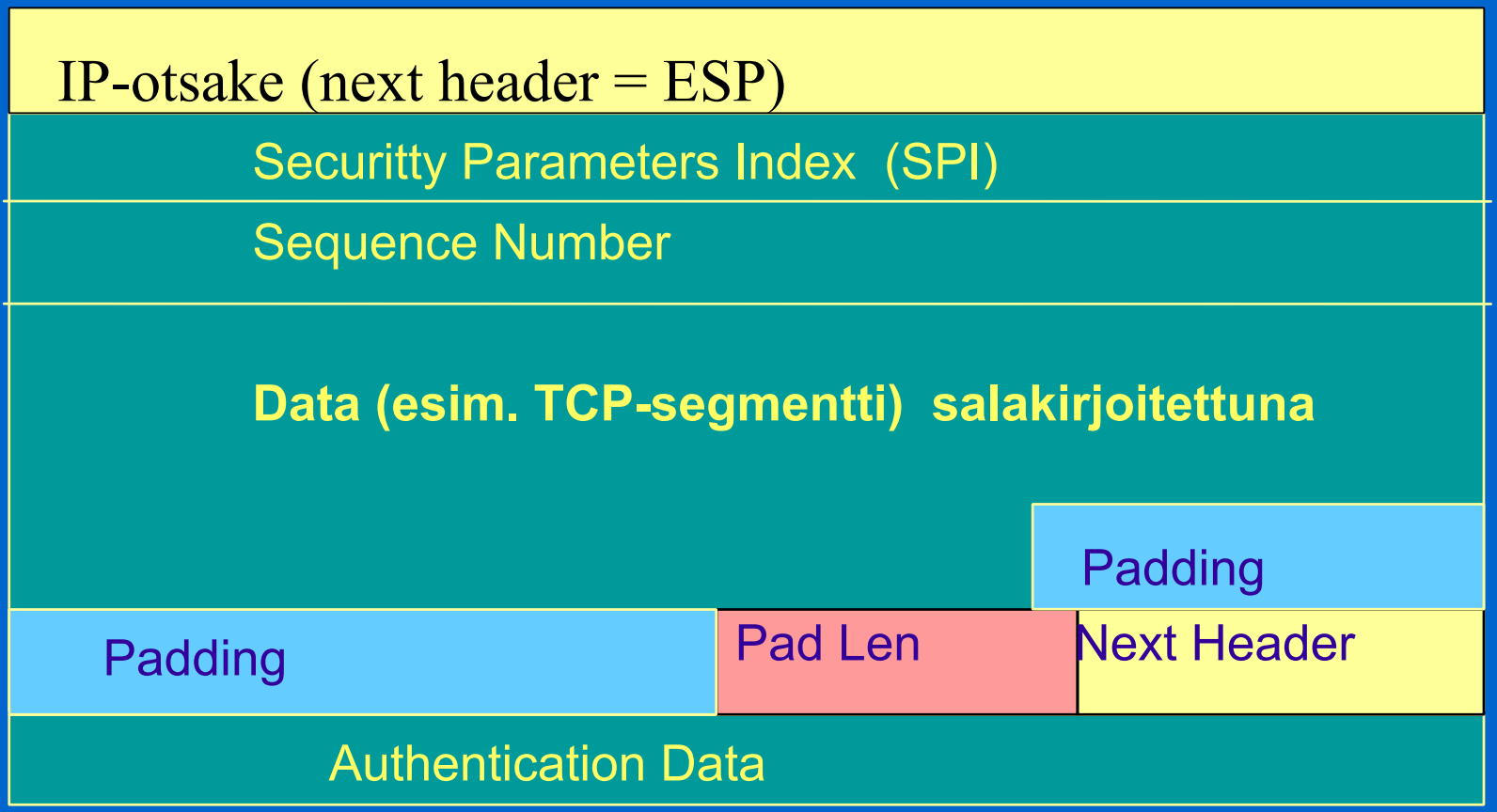
ESP-otsake

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

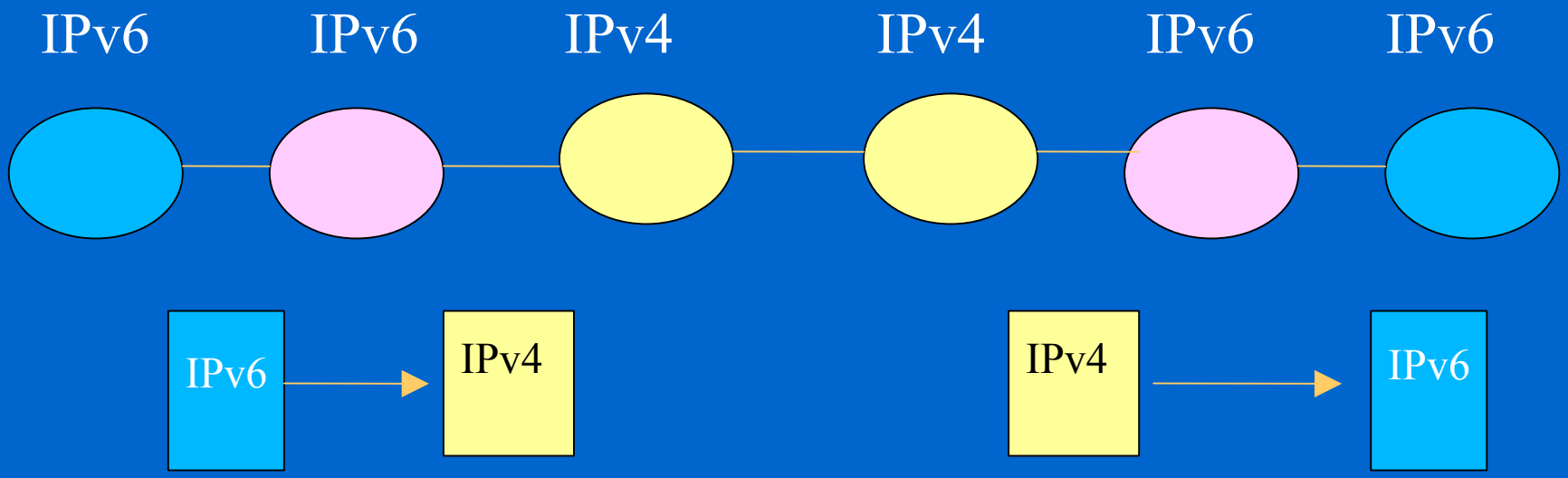
IPsec ja IPv4 / IPv6

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

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

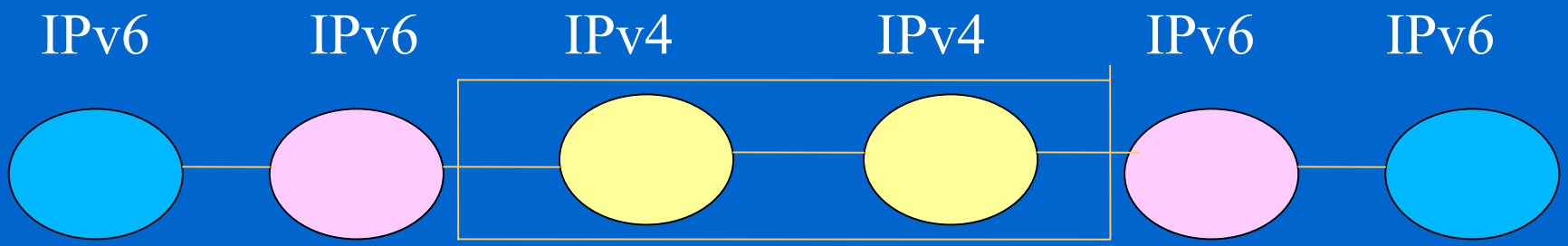
Kaksoispino



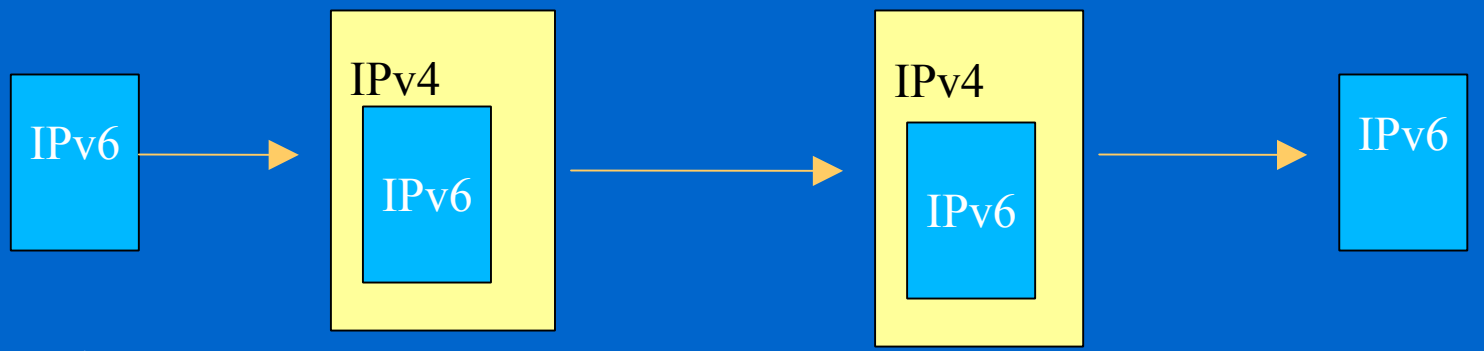
Flow= X

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

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

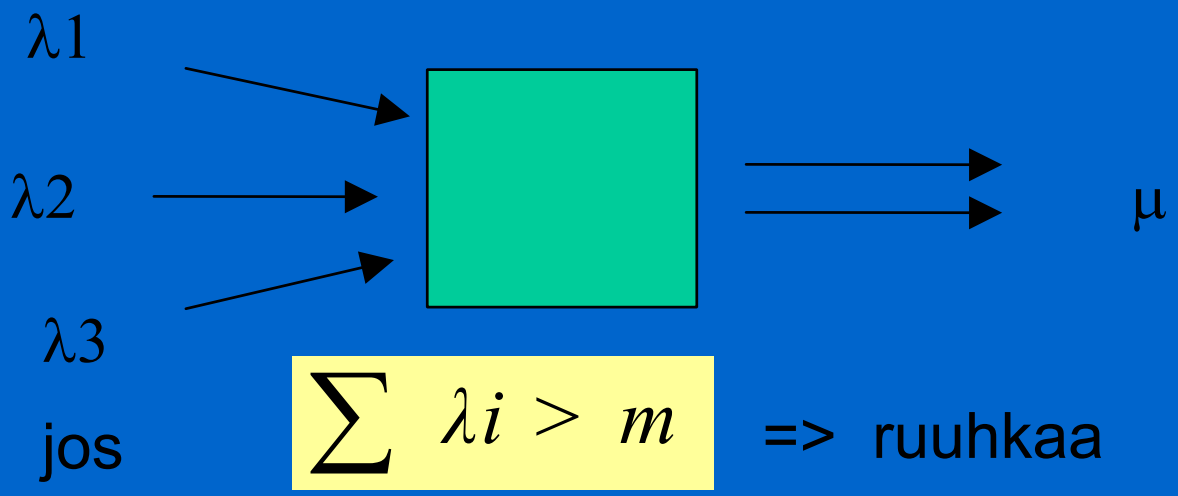
- reititin ei välitä RARP-viestejä
  - joka verkossa oltava oma RARP-palvelin
  - käytetään **BOOTP**-protokollaa
    - käyttää UDP-viestejä, jotka reititin välittää toisiin verkkoihin
    - lisäinformaatiota
      - tiedostopalvelimen IP-osoite
      - oletusreitittimen IP-osoite
      - aliverkkomaski

Ruuhkan valvonta

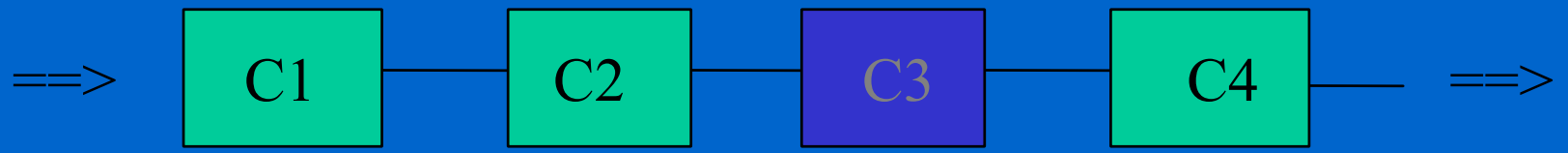
- yleistä ruuhkan valvonnasta
- ruuhkan estäminen
  - liikenteen tasoittaminen
    - vuotava ämpäri, vuoromerkkiämpäri
    - liikennevirran määrittely
- ruuhkan säätely
  - kuorman rajoittaminen
    - pääsyvalvonta, hidastuspaketit
  - kuorman purkaminen
    - pakettien tuhoaminen

Yleistä ruuhkasta

- suorituskyvyn rajat
  - palvelijaketju (reititin, linkki, reititin, …)
  - ketjun maksimiteho korkeintaan hitaimman palvelijan teho
    - suoritusteho: sanoma/aikayksikkö
  - hitain palvelija on pullonkaula
  - jos hitainta tehostetaan => missä / mikä on uusi pullonkaula?



jos $\sum \lambda i > m$ => ruuhkaa



ruuhkan valvonta <=> vuon valvonta

- ruuhkanvalvonta
  - verkon selvittävä tarjotusta kuormasta
  - globaali ongelma
    - monta lähettäjää, monta vastaanottajaa
- vuonvalvonta
  - lähettäjä ei saa lähettää enempää kuin vastaanottaja pystyy käsittelemään
  - kaksipisteyhteys
    - suora palaute vastaanottajalta lähettäjälle

‘open-loop’ control

- järjestelmä suunnitellaan sellaiseksi, ettei ruuhkaa synny
  - uuden asiakkaan hyväksyminen
  - pakettien hävittäminen
  - skedulointiperiaatteet
- järjestelmän tila ei vaikuta päätöksentekoon

‘closed-loop’ control

- palautesilmukka (feed back loop)
- seurataan järjestelmän tilaa
  - puskurien täyttöaste
  - uudelleenlähetysten lukumäärät, viipeet, viipeiden vaihtelu
- ongelman havaitsija ilmoittaa
  - pakettien alkuperäiselle lähettäjälle, kaikille
- reitittimet aktiivisesti kyselevät
  - nopeampi reagointi mahdollista

- lähetyskäyttäytymisen muuttaminen ruuhkan vähentämiseksi
  - liian hidas reagointi => ruuhka kasvaa
  - liian nopea reagointi => heiluriliikettä

Toiminnan säätö ruuhkatilanteessa

- **lisää kapasiteettia**
  - kiintiön nostaminen
  - varajärjestelmän käyttö
- **vähennä kuormaa**
  - ei uusia käyttäjiä, huonompi palvelu, jne
  - sopii hyvin virtuaalipiireihin
    - virtuaalipiirit =>verkkokerroksella
    - datasähkeet => kuljetuskerroksella

Ruuhkanestopolitiikat

- siirtoyhteyskerros
  - uudelleenlähetyspolitiikka
  - epäjärjestyksessä saapuneiden talletuspolitiikka
  - kuittauspolitiikka,
  - vuon valvontapolitiikka,
- verkkokerros
  - virtuaalipiiri <=> tietosähke
  - pakettien jonotuspolitiikka
  - pakettien poistamispolitiikka
  - reititysalgoritmi
  - pakettien elinikä

- kuljetuskerros
  - uudelleenlähetyspolitiikka
  - epäjärjestyksessä saapuneiden talletuspolitiikka
  - kuittauspolitiikka
  - vuonvalvontapolitiikka
  - ajastinaikojen asetukset

Liikenteen tasoitus (traffic shaping)

- liikenne tyypillisesti **purskeista**
  - aiheuttaa ruuhkaisuutta
- tasoitetaan liikennevirtaa puskurilla
  - puskuri toimii jonona
  - vuotava ämpäri
  - vuoromerkkiämpäri
- liikennevirran määrittely
  - määrittelee asiakkaan oikeudet ja velvollisuudet

Vuotava ämpäri (leaky bucket)

- purskeisuutta tasoittaa iso puskuri, josta liikenne valuu tasaisesti
  - ‘vuotava ämpäri’
  - yksi tavu / yksi paketti lähtee jossain aikayksikössä, **jos on lähetettävää**
- jos datapurske mahtuu puskuriin, se aikanaan pääsee matkaan
  - äärellinen jono
  - yläraja saapumistiheydelle

Vuoromerkkiämpäri (Token bucket)

- lähettäminen vaatii vuoromerkin
- vuoromerkkejä generoituu tasaisella nopeudella
- jos ei lähetettävää, merkkejä jää säästöön
  - korkeintaan niin paljon kuin ämpäriin mahtuu
  - => sallii rajoitetut ‘minipurskeet’
- joustavampi kuin vuotava ämpäri
  - purskeet voivat aiheuttaa ruuhkaa => vuotava ämpäri vuoromerkkiämpärin perään

Liikenteen määrittely (flow specification)

- sovitaan liikennevirrasta yhteyttä muodostettaessa
  - asiakas esittää kuorma- ja palvelutoiveet
  - palvelija: ok/ ei käy/ vastaehdotus
  - pyydetty palvelu
    - pakettien katoamisen sietokyky (loss sensitivity): missä määrin asiakas sietää pakettien tuhoamista
    - viiveherkkyys (delay, delay variation)
    - takuu: onko toive vai ehdoton vaatimus
  - asiakas ei aina tiedä mitä todella haluaa

Virtuaalikanavan ruuhkanvalvonta

- pääsynvalvonta (admission control)
  - jos ruuhkaa, ei uusia virtuaalikanavia
  - uusi kanava ok, jos kiertää ruuhka-alueen
- virtuaalikanavaa avattaessa
  - sovitaan liikennekuormituksesta ja palvelun laadusta
  - verkosta varataan tarvittavat resurssit
- resurssien varaus
  - milloin varataan, paljonko varataan
    - liikenne on purskeista
    - turha varaus tuhlaa resursseja

hidastuspaketti (choke packet)

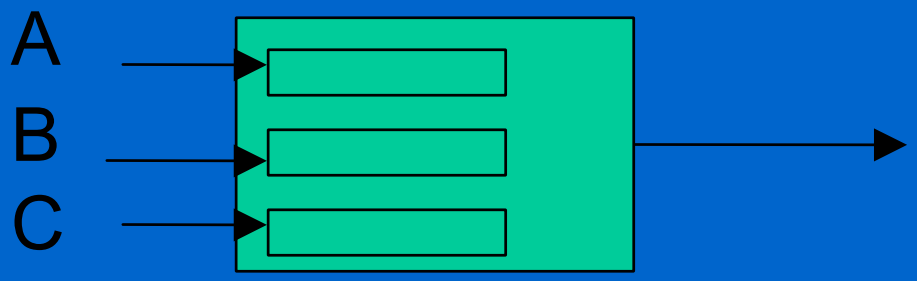
- voidaan käyttää kaikenlaisissa verkoissa
- reititin tarkkailee kuormitusta
  - ulosmenolinjojen käyttöastetta
  - jonopituuksia
  - esim

    Unew = aUold + (1-a)f
    - a kuinka nopeasti aikaisempi historia unohtuu
    - f kuormitettu vai ei (o tai 1)

- jos liikaa kuormaa, reititin huolestuu
  - lähettäjälle hidastuspaketti
  - lähettäjä hidastaa lähetystään
    - vähentää ensin puoleen
    - ja sitten taas puoleen
  - perustuu vapaaehtoisuuteen
    - reilu jonotus
- useita kynnysarvoja
    - lievä, vakava, erittäin vakava varoitus
- muita ruuhkan ‘mittoja’
    - jonon pituus
    - puskurikäyttö

Hidastuspaketin ongelmia:

- lähettäjän hidastus vapaaehtoista
  - reilu jonotus:
    - kullakin lähettäjällä oma jono jokaiseen ulosmenolinjaan



Lähetetään vuorotellen eri jonoista.

- Hidastuspaketin vaikutuksen hitaus pitkillä linjoilla
- Ratkaisu:
  - ei pelkästään lähettäjälle
  - myös välissä olevat reitittimet alkavat hidastaa

Kuorman kevennys (Load Shedding)

- tuhotaan paketteja => kuorma kevenee
  - reititin täyttyy:
    - mitä paketteja tuhotaan?

FTP: tuhotaan 8 => paketit 8-11 uudelleen
tuhotaan 11 => paketti 11 uudelleen

video: ?

- riippuu sovelluksesta
  - viini: vanha parempi kuin uusi
  - maito: uusi parempi kuin vanha
- eriarvoiset paketit
  - perusdata/muutokset
  - teksti / kuva
- käyttäjä ilmoittaa prioriteetin
  - arvokkaita ei tuhota
  - prioriteetin käytön valvonta: hinta/sallitun lähetysmäärän ylittävät paketit
- paketti tuhottu, entä sanoma
  - mitä tehdään ko. sanomalle