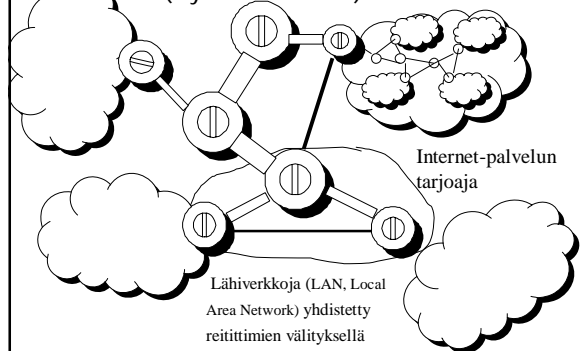


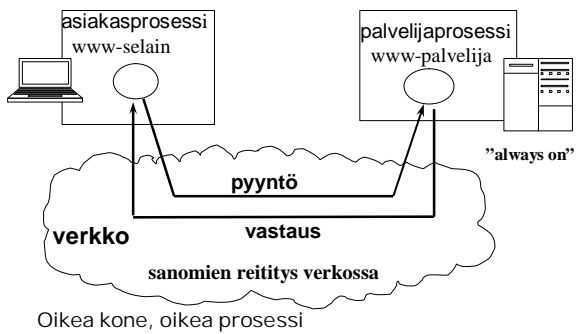
# Tietoliikenteen perusteet

Vähän kertausta

# Internet = verkkojen verkko (löyhää hierarkiaa)

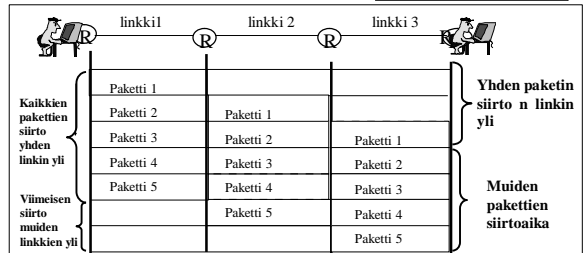


# Asiakas-palvelija-malli



# Pakettivälitys siirto-aika

- Olkoon siirtoaika a:
- a)  $ka + (n-1)a = (k+n-1)a$
  - b)  $na + (k-1)a = (n+k-1)a$

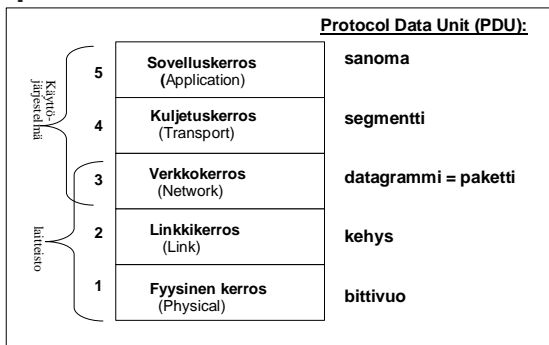


Sanoman siirtoaika, kun sanomassa on k pakettia ja linkejä on n kappaletta

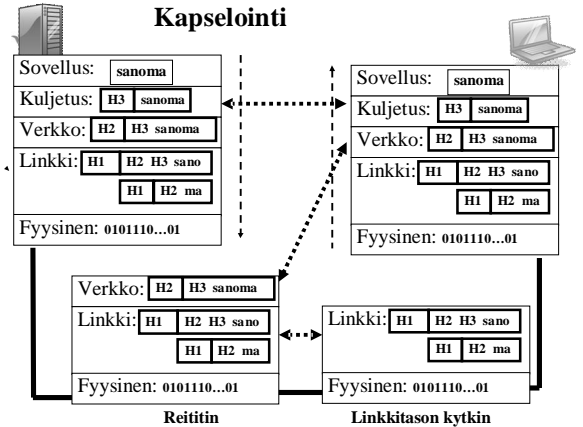
- a)  $k \cdot n$  paketin siirto 1. linkin yli + viimeisen paketin siirto n-1 linkin yli.
- b)  $1 \cdot n$  paketin siirto n:n linkin yli + muiden k-1 paketin siirto yhden linkin li

Animaatio: [http://wps.aw.com/aw\\_kurose\\_network\\_4/63/163034173750/cw/index.html](http://wps.aw.com/aw_kurose_network_4/63/163034173750/cw/index.html)

# Internet-protokollapino



# Kapselointi



## HTTP (HyperText Transfer Protocol)

PC, jossa on Explorer-selain

Palvelin, jossa on Apache-www-palvelija

Linux-kone, jossa on Firefox-selain

**WWW:N sovellusprotokolla**  
Tekstimuotoiset sanomat  
pyyntö - vastaus

**Asiakas**  
Selain: FireFox, Internet Explorer, Opera, Apple Safari, ...  
pyytää, noutaa ja näyttää objektit

**Palvelija**  
etsii objektin (tiedoston) koneen hakemistosta ja lähettää sen vastauksena asiakkaalle

**Tilaton protokolla**  
Palvelija ei muista mitään edellisistä pyynnöistä

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 7

origin servers  
public Internet  
www.herkkutuoto.com  
1.5 Mbps access link  
institutional network  
10 Mbps LAN  
institutional cache

GET /fruit/kiwi.gif HTTP/1.1  
Host: www.herkkutuoto.com

HTTP/1.1 304 Not Modified  
Date: Thu, 14 Jul 2007 15:39:29

GET /fruit/kiwi.gif HTTP/1.1  
Host: www.herkkutuoto.com  
If-modified-since: Wed, 4 Jul 2007 09:23:24

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 8

## Sähköpostin komponentit

User agent  
Mail server  
SMTP  
User agent  
Mail server  
SMTP  
Mail server  
User agent

.....  
Lähtevien sanomien jono

.....  
postilaatikot

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 9

## Hajautettu, hierarkkinen tietokanta

Root DNS Servers  
com DNS servers  
org DNS servers  
edu DNS servers

yahoo.com DNS servers  
amazon.com DNS servers  
pbs.org DNS servers  
poly.edu DNS servers  
umass.edu DNS servers

n **13 juuritason nimipalvelija**  
Replikoituja, kaikilla samat tiedot

n **Yliätason palvelimet maa- ja yleistunnuksille** (n. 265 kpl)  
..., fi, fr, uk, ... edu, net, com, org, ...

n **Autorisoidut aluepalvelimet** (domain) (2-taso) [www.iana.org](http://www.iana.org)  
Isoilla yliopistoilla ja firmoilla omansa, pienet käyttävät jonkun muun ylläpitämää

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 10

## Skaalautuvuus

KuRo08: Fig. 2.24

**Asiakas-palvelinmalli:**  
Palvelimen siirrettävä  $n * F$  bittinä => siirtoaika =  $nF/u_s$   
Hitain asiakas  $d_{min}$  saa tiedoston ajassa  $F/d_{min}$   
Siirtoaika =  $\max(nF/u_s, F/d_{min})$   
Kun n kasvaa, palvelimen kuorma kasvaa ja siirtoaika kasvaa.

**Vertaistoinijamalli** (alussa tiedosto on palvelimella)  
Siirtoaika =  $\max(F/u_s, F/d_{min}, nF/(u_s + V u_1))$

Summaimerkki

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 11

## Pistoke (socket)

n Kuljetuspalvelun ja sitä käyttävän sovelluksen rajapinta isäntäkoneessa  
Sovelluksen tietoliikenne = K:n palvelupyynnöitä  
Pistoke on "palveluluukku"

n **Alunperin Berkeley UNIXin (BSD) mukana**

Sovellus-ohjelmoija  
Käyttöjärjestelmä  
process  
socket  
TCP with buffers, variables  
host or server

internet

process  
socket  
TCP with buffers, variables  
Käyttöjärjestelmä  
Sovellus-ohjelmoija  
host or server

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 12

### UDP: Tarkistussumma

32 bittia

Source port #	Dest. Port #
Length	Checksum

Application data (message)

UDP-otsake

**Lähetys**

- Summaa 16 bittin kokonaisuudet (otsake + pseudo-otsake mukana), ylivuotobitit lasketaan mukaan, talleta yhden komplementtina

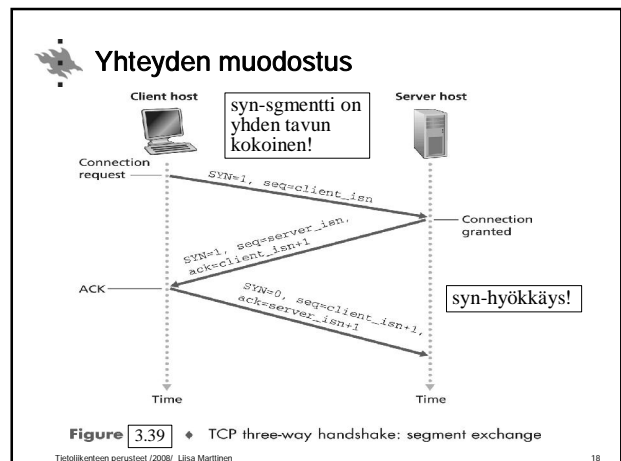
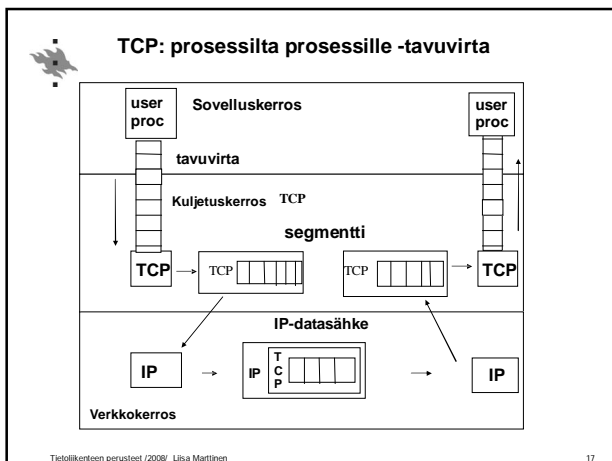
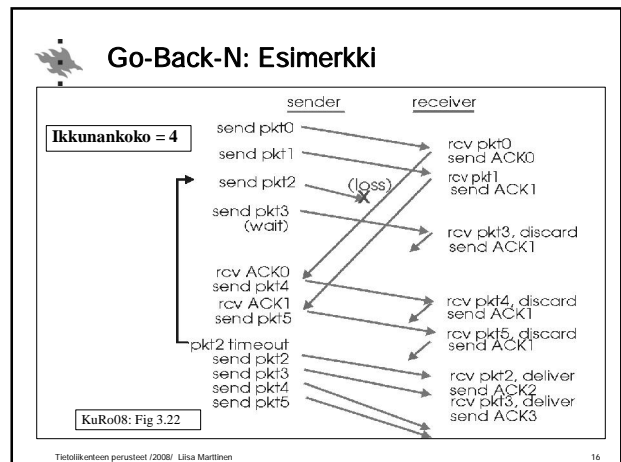
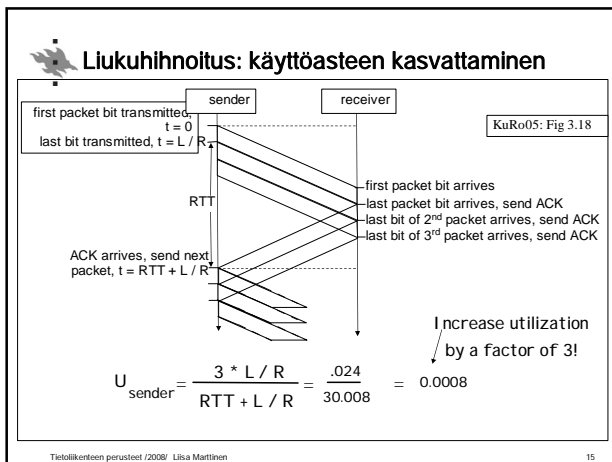
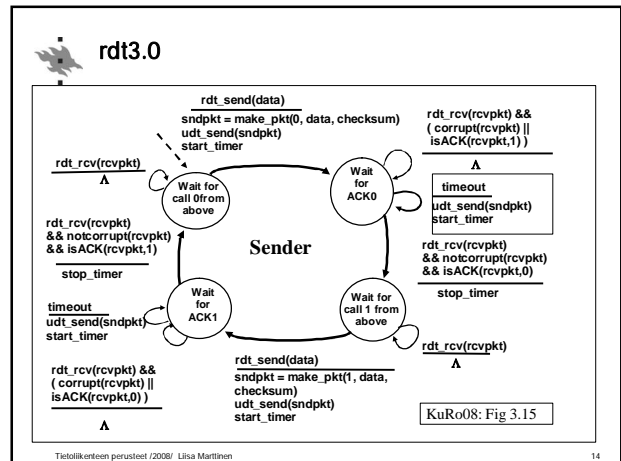
**Vastaanotto**

- Summaa 16 b kokonaisuudet (myös tarkistussumma).
- Jos tuloksena on 16 ykköstä, niin OK!

```

1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
1 0 1 1 1 1 0 1 1 1 0 1 1 1 0 1
0 > 1
1 > 0
Checksum 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1
  
```

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 13



### TCP Reno: Hidas aloitus (slow start) ja ruuhkanvälttely (congestion avoidance)

- Aluksi ruuhkalkkuna = yksi segmentti
  - Alussa hidas siirtonopeus = MSS/RTT
- Kukin kulitus kasvattaa yhdellä ruuhkalkkunan kokoa
  - Ekspontiaaalinen kasvu
  - Ikkinä kaksinkertaistuu yhden RTT:n aikana
- Jos uudelleenlähetys, puolta ruuhkalkkunan koko
  - Multiplicative decrease
- Sen jälkeen kasvata ikkinäa yksi segmentti/RTT
  - Lineaarinen kasvu (Additive increase)
  - Ruuhkan välttely (congestion avoidance)
- Siirtonopeus = CognWin / RTT tavua/sek

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 19

### TCP Tahoe vs. TCP Reno

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 20

### Verkkokerros

- Toimittaa kuljetuskerroksen segmentit vastaanottajalle
- Lähetäjä
  - luo segmenteistä verkkokerroksen IP-paketteja
  - Lisää otsaketietoja: mm. IP-osoitteet
- Reitittäminen
  - Isäntä - reititin ... reititin - isäntä
- Vastaanotto
  - Polsta otsake
  - Anna segmentti kuljetuskerrokselle
- Verkkokerros toimii etenkin reitityksessä
  - Reititin tutkii IP-paketin otsakkeen ja päättää, mihin linkkilin se lähetetään seuraavaksi

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 21

### Reitittimen arkkitehtuuri

- Kaksi tehtävää
  - Välitä paketteja tulolinkeistä ulosmenolinkeihin
  - Suorita reititys algoritmia / -protokollaa
- Portti - verkkokortti
  - Useita portteja niputettu yhteen linjakortiksi (line card)

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 22

### IP-paketin rakenne (IPv4)

Figure 4.13 ♦ IPv4 datagram format

Tietoliikenteen perusteet / 2008/ Liisa Marttinen 23

### IP-pakettien paloittelu (fragmentointi)

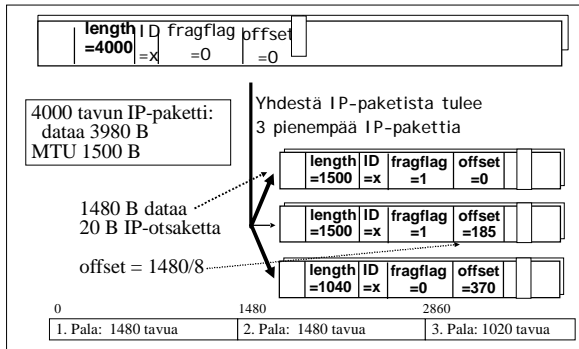
**Maximum transfer Unit (MTU)**  
 suurin mahdollinen IP-paketti eri linkeillä eri koko  
 Esim. Ethernet 1500 B

Liian iso paketti pilkottava reitittimessä pienemmiksi paketeiksi (fragmenteiksi), jotka kohdekone kokoaa voivat kukin kulkea eri reittiä

IP-otsakkeessa kentät yhteenkuuluvien fragmenttien tunnistamiseksi ja kokoamiseksi

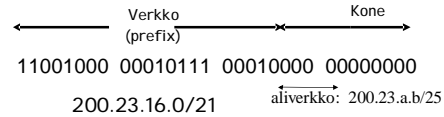
Tietoliikenteen perusteet / 2008/ Liisa Marttinen 24

## Esimerkki



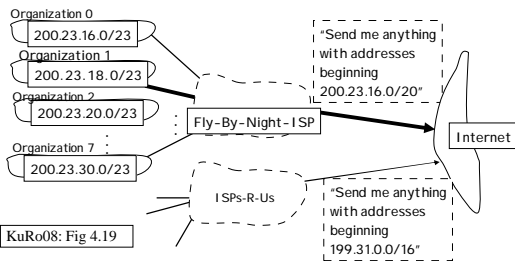
## CIDR: Classless InterDomain Routing

- Verkko-osa voi olla minkä tahansa kokoinen
  - Vanha luokallinen osoite: A-luokka 8 b, B-luokka 16 b, C-luokka 24 b
  - Formaatti: a.b.c.d/x
  - x ilmoittaa verkko-osan bittien lukumäärän (prefix)
- Esim. Organisaatio, jolla 2000 konetta varaa 2024 = 2<sup>11</sup> konenumeroa, jolloin verkko-osaa varten jää 21 bittiä
- Yritys voi vielä itse jakaa viimeiset 11 bittiä aliverkko-osoitteeksi ja koneosoitteeksi. Tämä jako ei näy ulkopuolelle.

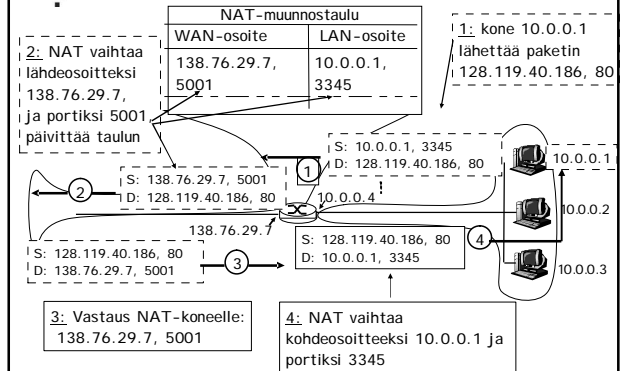


## Hierarkkinen osoite

- CIDR luo reititystä helpottavan hierarkian
- Aggregointi (yhdistäminen): yhteinen alkuosa => samaan suuntaan



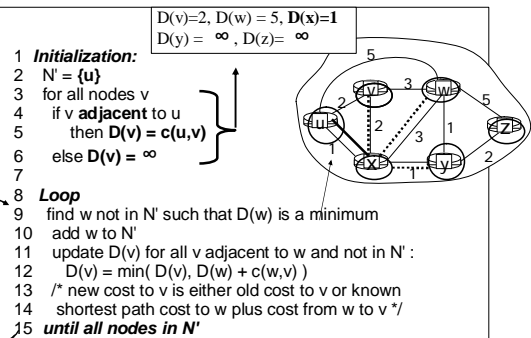
## NAT: Esimerkki



## Reititysalgoritmi

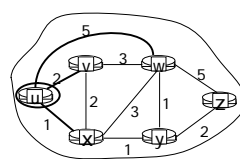
- Etsi edullisimmat reitit lähdekoneelta kohdekoneelle
- Käytetään reititystaulun muodostamiseen
- Mille linkille paketti seuraavaksi siirretään tältä reitittimeltä
- Reititysalgoritmi, joka tarvitsee täydellisen tiedon verkosta
- Ennen laskentaa käytössä koko kuva verkosta:
  - Kaikki linkkiyhteydet solmujen välillä ja niiden kustannukset
  - Käytännössä vain tietyistä autonomisista alueista
- Parhaat reitit lasketaan joko keskitetysti tai hajautetusti
- Linkkiltila-algoritmi (link-state algorithm)
- Reititysalgoritmi, jolle riittää epätäydellinen kuva verkosta
- Aluksi reititin tietää vain niistä koneista, joihin itse on yhdistetty
- Iteratiivinen algoritmi: reititin vaihtaa tietoja naapuriensa kanssa ja saa tietoa muusta verkosta
- Etäisyysvektorialgoritmi (distance vector algorithm)

## Dijkstran algoritmi



### Etäisyysvektoreititys:

#### Esimerkki 1

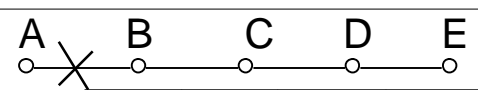


$D_u(z) = 5, D_x(z) = 3, D_w(z) = 3$   
 $D_u(z) = \min \{ c(u,v) + d_v(z), c(u,x) + d_x(z), c(u,w) + d_w(z) \}$   
 $= \min \{ 2 + 5, 1 + 3, 5 + 3 \} = 4$

Kun paketti on matkalla solmusta u solmuun z, se tulee seuraavaksi lähettää solmuun x, joka tuotti tuon minimin => tallenta tieto omaan etäisyysvektoriin (= reititystauluun)

Tietoliikenteen perusteet /2008/ Liisa Marttinen 31

### Huono uutinen etenee hitaasti!



Linkki AB katkeaa => etäisyys äärettömäksi	$D_B(A)$	$D_C(A)$	$D_D(A)$	$D_E(A)$
2	2	3	4	
3	2	3	4	
4	4	3	4	
5	4	5	4	
6	6	5	6	
7	6	7	6	
8	8	7	8	
jne				

Count-to-infinity -ongelma

**Etäisyys A:han**

Tietoliikenteen perusteet /2008/ Liisa Marttinen 32

### Linkkikerros

- Laitetoimintoa
- Siirtää paketin fyysisistä linkistä pitkin koneelta (solmulta (node)) toiselle
  - langallinen / langaton
  - bitit sisään, bitit ulos
- Kapseloi paketin siirtoon sopivaan muotoon
  - Siirtokehys (frame)
- Lähiverkossa linkkejä voi yhdistää keskittimillä tai kytkimillä
  - Käytetään fyysisiä osoitteita
  - 'reititystä' ilman IP-osoitteita

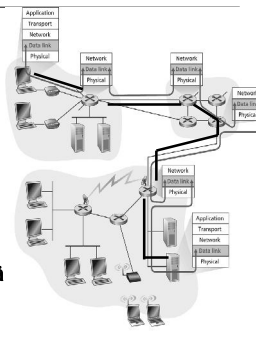


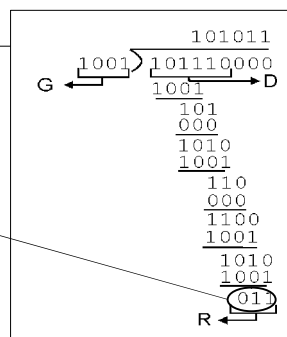
Figure 5.1 • The link layer

Tietoliikenteen perusteet /2008/ Liisa Marttinen 33

### CRC-esimerkki

Data: 101110  
 G: 1001, polynomina  $1*x^3 + 0*x^2 + 0*x^1 + 1*x^0$   
 <D,R>: 101110???

Lähetä: 101110011

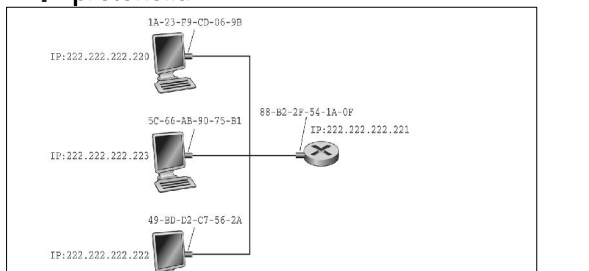


Modulo 2-aritmetiikka vähennyslasku yhteenlaskuja ei lainaamista, ei muistinumeroita = bittitasoin XOR  
 $1+1=0, 1+0=0+1=1, 0+0=0$

KuRo08:Fig 5.8

Tietoliikenteen perusteet /2008/ Liisa Marttinen 34

### MAC-osoitteet ja ARP-taulu, ARP-protokolla



IP-osoite	MAC-osoite	TTL
222.222.222.220	1A-23-F9-CD-06-9B	13:24:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tietoliikenteen perusteet /2008/ Liisa Marttinen 35

### Lähtettäminen toiseen verkkoon (2)

**Lähtettäjä A**  
 Muodosta IP-paketti, jossa Source IP = A, Dest. IP = B  
 Etsi ARP-taulusta reitittimen IP-osoitetta vastaava MAC-osoite  
 Luo siirtokehys, osoitteena reitittimen MAC-osoite (data = IP-paketti).  
 Verkkokortti lähettää siirtokehksen.

**Reititin R**  
 Verkkokortti ottaa siirtokehksen vastaan.  
 Ota IP-paketti kehyksestä ja tutki otsakkeesta kohteen IP-osoite (B)  
 Katso reititustaulusta, mihin verkkoon seuraavaksi (mille reitittimelle)  
 Koska omassa verkossa, etsi kohdeverkon ARP-taulusta kohteen MAC-osoite  
 Muodosta siirtokehys, osoitteena B:n MAC-osoite (data = IP-paketti)

**Vastaanottaja B**  
 Verkkokortti ottaa kehyksen vastaan; ohjaa IP-paketin verkkokerrokselle.

Tietoliikenteen perusteet /2008/ Liisa Marttinen 36

## Ethernet kehys



Tahdistuskuvio (preamble) (8 B)

7 tavussa 10101010 kellojen tahdistusta varten

8. tavu 10101011 kertoo varsinaisen kehyksen alkavan

Kohteen ja lähteen MAC-osoitteet (6 + 6 B)

Type (2 B)

verkko-protokolla, jolle vastaanottaja luovuttaa kehyksen datan

IP, ARP, jokin muu esim, Apple Talk, Novell IPX, ..

Data (46 ... 1500 B)

Ethernet MTU = 1500 B

CRC (4 B)

tarkistusbitit, tahdistuskuvio mukana laskennassa

## CSMA/CD (with Collision Detection)

Asema kuuntelee myös lähettämisen jälkeen

Langallinen LAN: signaalin voimakkuus muuttuu

- Esim. Ethernet

Langaton LAN: hankalaa

Jos törmäys

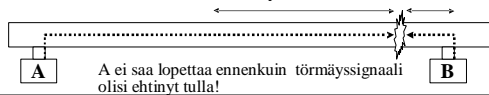
Niin keskeytä heti lähettäminen

ja yritä uudestaan satunnaisen ajan kuluttua

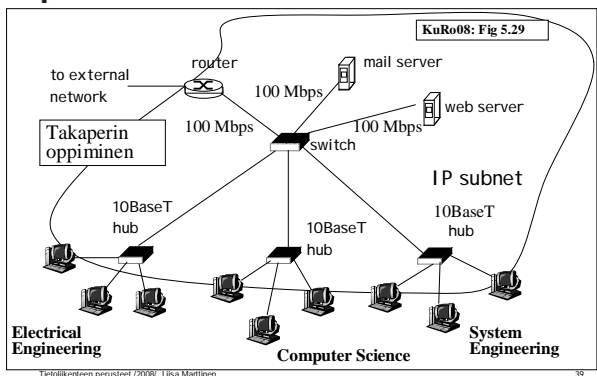
Näin törmäyksen aiheuttama hukka-aika pienenee

Kuanko kuunneltava?

2<sup>n</sup> maksimi etenemisviive solmujen välillä



## LAN, verkkosegmentit



## 802.11: CSMA/CA

**Lähetys**

1. Jos kanava vapaa

Kuuntele DIFS aikayksikköä

Lähetä kehys kokonaan

2. Jos kanava varattu

Käynnistä peruutuslaskuri (backoff)

random(max), jota vähennetään vain

kun kanava on vapaa,

Lähetä, kun laskuri nollassa

Jos ei tule kiitosta, niin yritä

uudestaan max = 2<sup>n</sup> max

**Vastaanotto**

Jos kehys OK

Odotat SIFS aikayksikköä

**Lähetä ACK** (linkkikerroksen ACK)

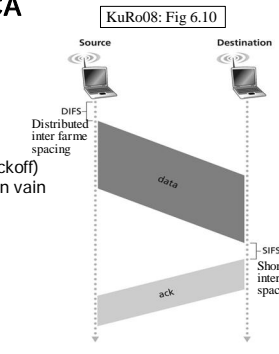


Figure 6.8 ♦ 802.11 uses link-layer acknowledgment

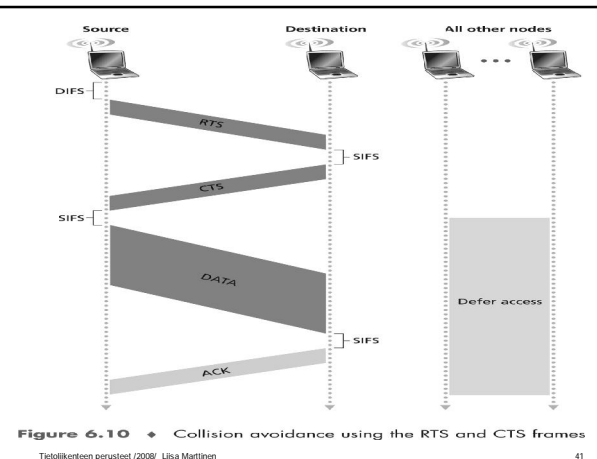


Figure 6.10 ♦ Collision avoidance using the RTS and CTS frames

## Hajautettu DoS-hyökkäys (DDoS)

Hyökkääjä ottaa ensin haltuun ison joukon koneita niiden omistajien huomaamatta

Koputtelee ja löytää turva-aukot

Asentaa hyökkäysohjelman,

joka vain odottelee

käskyä /kellolyömää

Kaapatut koneet aloittavat

samaan aikaan

hyökkäyksen uhrin

kimppuun

Hajautetusti

IP-osoitteet peukaloituina

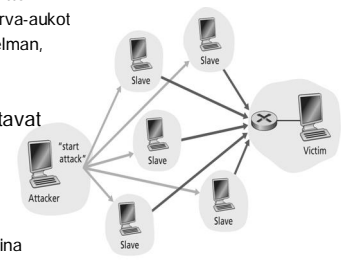
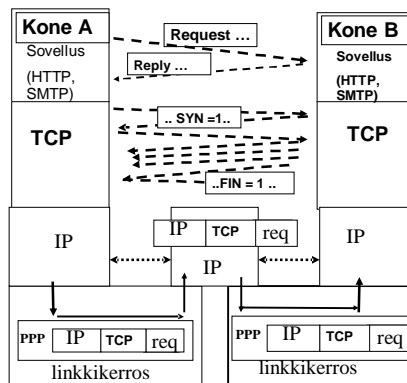
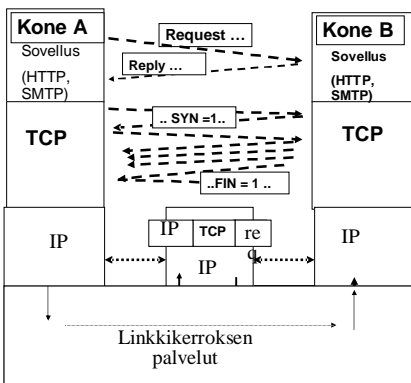
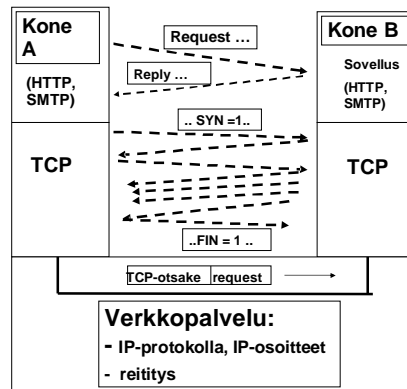
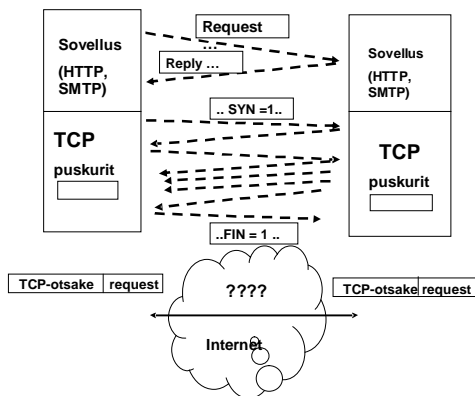
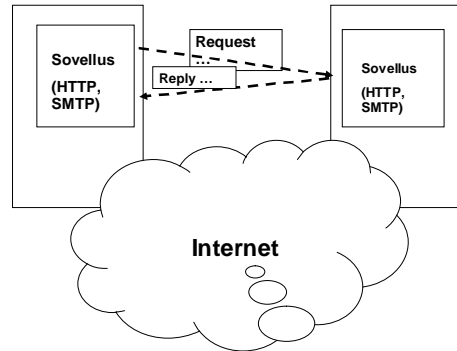
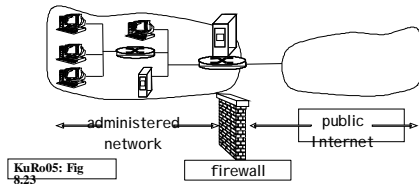


Figure 8.26 ♦ A DDoS attack

# Palomuri (firewall)

- Ohjelmisto + laitteisto
- Suodattaa (filteroi) liikennettä organisaation oman verkon (intranet) ja julkisen Interbetin välillä
- Osa IP-paketeista pääsee palomuurin läpi, osa ei





## Tietoliikenteen perusteet



Siinäpä se!

