Aalto-yliopisto
Teknillinen korkeakoulu

Linkkikerros, Ethernet ja WLAN

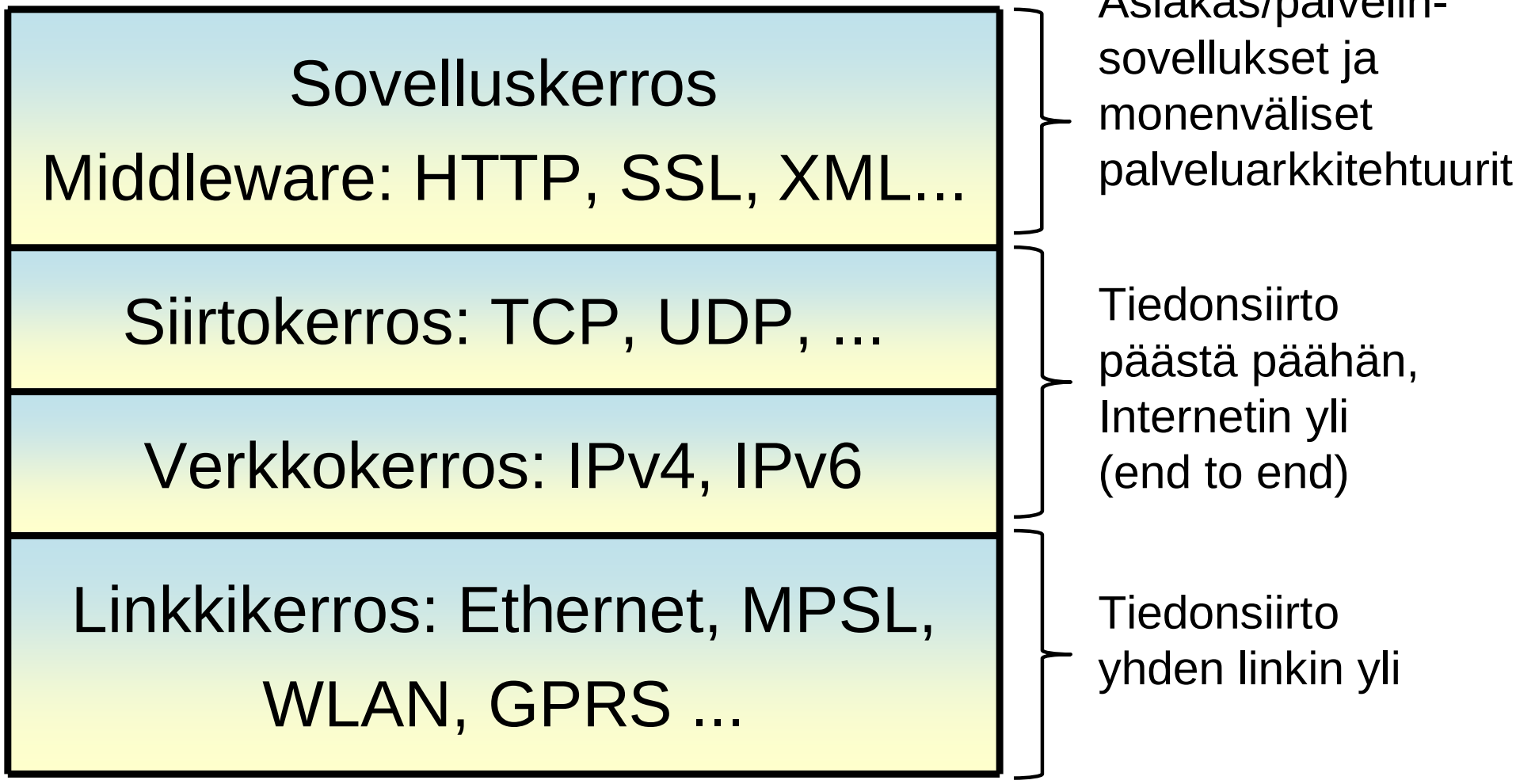
Jouko Kurki

T-110.2100 Johdatus tietoliikenteeseen
kevät 2010

Viime luennolla

- Verkkokerros on nykyään Internetarkkitehtuurissa käytännössä IP
  - Tällä hetkellä versio 4, versio 6 tulossa
- IP toteuttaa epäluotettavan ja tilattoman kuljetuspalvelun Internetissä
  - Ylemmät protokollat hoitaa tarvittaessa luotettavuuden ym.
- IPv4-osoitteet ovat hallinnoitu luonnonvara
  - Voidaan jakaa aliverkoiksi bittirajojen kohdalta
  - NAT helpottaa hyödyntämällä yksityisiä osoiteavaruuksia
- Reitittimet siirtelevät IP-paketteja verkossa
  - Forwardointi
  - Reititys

TCP/IP-protokollapino



Luennon sisältö

- Linkkikerros, Ethernet ja LAN (Local Area Network)
  - Miten IP paketti siirretään päätelaitteesta/reitittimestä toiseen Ethernet tai muun linkkikerroksen kehyksen (frame) sisällä
  - Ethernet
  - Kurose, Computer Networking, kappaleen 5 mukaan
- Linkkikerros ja monipääsyprotokollat langattomissa lähiverkoissa Wireless Local Area network, WLAN (IEEE standardi 802.11)
  - Kurose, Computer networking, kappaleen 6 mukaan

Tämän luennon jälkeen…

Ymmärrätte:

- Tietokoneet käsittelevät tavuja (Byte), IP-kerros paketteja (packet), fyysinen kerros bittejä (bit)
  - Linkkikerros yhdistää nämä *kehystämällä (framing)* ja *kapseloimalla* ylemmän tason datan siirrettäväksi fyysisen median ylitse
- Linkkikerroksen tehtävän ja toiminnan
  - Ethernetin toiminta ja osoitteistus
  - Virheiden havaitsemisen ja korjaamisen periaate
  - Kanavavaraus (CSMA/CD)
  - Mitä on kytkin ja mitä se tekee
  - Langattoman siirron aiheuttamat erityispiirteet ja WLAN:in ominaisuuksia

- Tiedostatte
  - Jaetun median käyttöön liittyvät haasteet. Piirikytkentäisyyden ja pakettikytkentäisyyden eron.
  - Siirtoviiveet ja niiden vaikutus reaaliaikapalveluihin

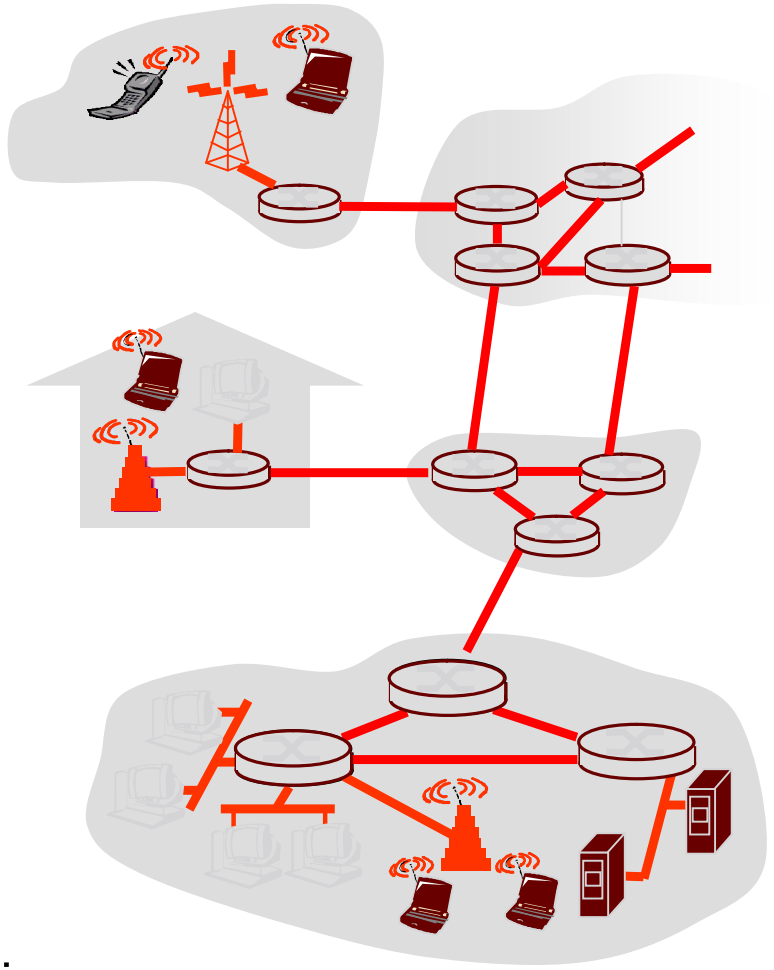
Linkkikerros (Data Link Layer)

- Tällä kerroksella toteutetaan
  - Lähiverkot
    - Ethernet, WLAN, Token Ring, ATM (paikallinen)
  - Pisteiden väliset yhteydet (point-to-point)
    - Tietokoneita tai lähiverkkoja yhdistävät
    - HDLC, PPP, SLIP, ATM
    - Perinteinen tele-infra: Sonet, SDH, PDH, ATM
      - Periaatteita käsitellään tiedonsiirron perusteet luennolla, tarkemmin tietoliikennetekniikan kursseissa
- Myös
  - Kampusverkot tai MAN (Metropolitan Area verkko)
    - FDDI, HIPPI, ATM, optiset renkaat
  - Langattomat mobiiliverkot
    - GPRS, UMTS
  - Ja muuta teknologiaa
    - Kaapelimodemit, Bluetooth

Linkkikerros: Johdanto

Vähän terminologiaa:

- Verkossa tietokoneet ja reitittimet ovat **solmuja**
- Tietoliikennekanavia, jotka yhdistävät viereisiä solmuja pitkin reittejä kutsutaan nimellä **linkki**
  - langalliset yhteydet
  - langattomat yhteydet
  - Lähiverkot (Local Area Network, LAN)
- Linkkikerroksen ”paketti” on **kehys**

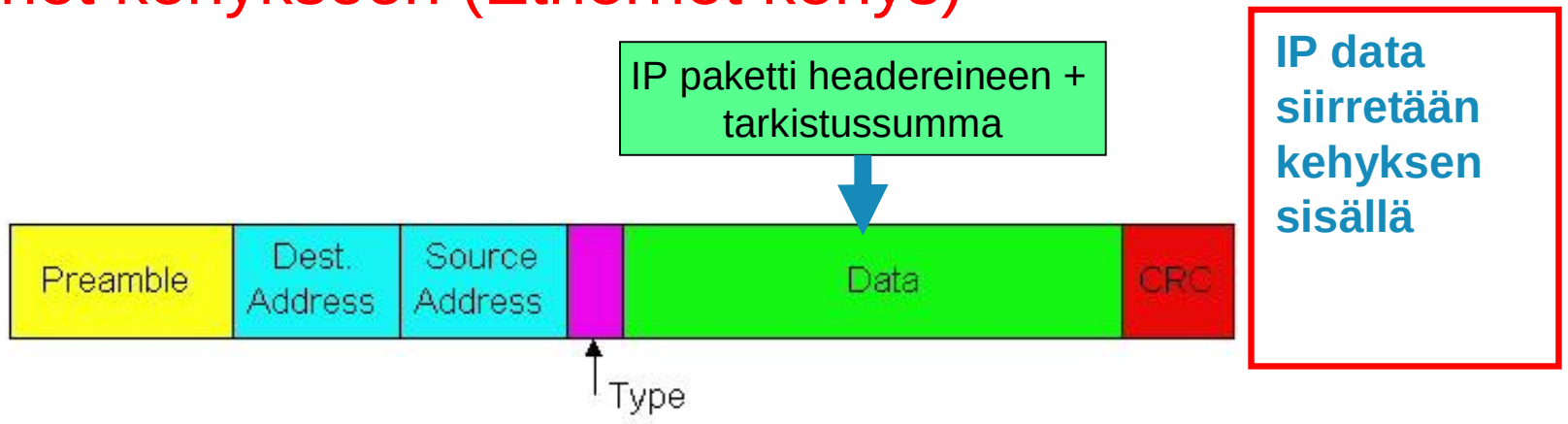


data-linkkikerroksen vastuulla on siirtää datagrammi yhdestä solmusta viereiseen solmuun linkin yli

Kuvissa ——— = Linkki

Linkkikerroksen esimerkki: Ethernet tekniikka

Lähettävän koneen verkkokortti kapseloi IP datagrammin (tai muun verkkoprotokollan paketin) Ethernet kehykseen (Ethernet kehys)



Kehyksen alussa aina tahdistusosa (Preamble):

- 7 tavua jossa bitit menevät sekvenssissä 10101010. Tätä seuraa yksi tavu “10101011” (SD)
- Tällöin vastaanottaja tietää milloin varsinainen tieto alkaa, ja osaa synkronoida nopeuden (kellotaajuuden)

Linkkikerros: Mistä on kyse ?

- Datagrammi siirretään eri linkkiprotokollia käyttäen eri linkkien kautta:
  - Esim., Ethernet ensimmäisellä linkillä, kehys releoidaan seuraavilla (Frame Relay), 802.11 WLAN viimeisellä linkillä
- Jokainen linkkiprotokolla tarjoaa erilaisia palveluita, esim., voi tarjota tai olla tarjoamatta luotettavan tiedonsiirron

Matkustusanalogia:

Matka Princetonista Lausanneen

- limusiini: Princetonista JFK-lentokentälle
- Lento: JFK -> Geneve
- Juna: Geneva -> Lausanne

- Turisti = datagrammi
- Matkan osa = (tietoliikenne) linkki
- Matkustustapa = linkkikerroksen protokolla
- Matkatoimisto = reititysalgoritmi

Linkkikerroksen palvelut

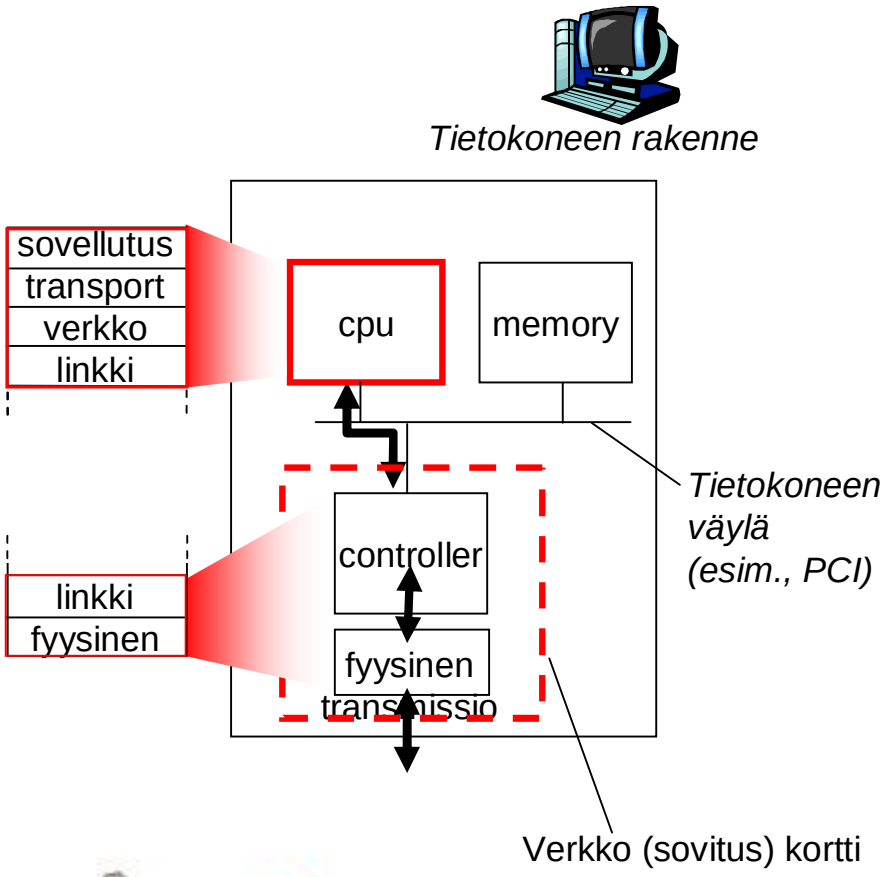
- *Kehystys, siirtotielle pääsy (kaapeli, langaton):*
  - kapseloi datagramnin kehykseen, lisää kehyksen otsikon osoitteineen, loppuosan
  - siirtokanavalle pääsyn kontrolli (tai ei!) jos jaettu media
  - ”MAC"-osoitteita käytetään kehyksen otsikoissa tunnistamaan lähde, ja kohde
    - eri kuin IP-osoite!
- *Luotettavan siirron toteutus vierekkäisten solmujen välillä*
  - Harvoin käytössä luotettavien linkkien välillä (kuitu, jotkut kierretty pari ratkaisut)
  - Langattomat linkit: suuret bittivirhetodennäköisyydet
    - Kysymys: miksi sekä linkkitason, että päästä päähän end-to-end luotettavuus?

Linkkikerroksen palvelut (lisää)

- *Vuon ohjaus:*
  - Odottelu vierekkäisten vastaanottajien ja lähettäjien välillä
- *Virheiden havaitseminen ja korjaus*:
  - Virheitä aiheutuu signaalin vaimennuksen, kohinan, ylikuulumisen (esim. vierekkäinen radiokanava häiritsee) yms.
  - Vastaanotin havainnoin virheiden olemassaolon:
    - Tieto lähettäjälle tai pudotetaan kehys (jolloin ylemmällä tasolla pyydettävä uudelleenlähetyksiä)
- Virheiden korjaus:
  - Vastaanotin ilmaisee ja korjaa bittivirheen/virheet pyytämättä uudelleenlähetystä
- *Puoli-duplex (Half-Duplex) tai koko-duplex (Full-Duplex) (siirtosuuntien hallinta)*
  - Puoli-duplex:illa: lähetys vuorotellen; koko-duplex, molemmat päät voivat vastaanottaa ja lähettää samaan aikaan

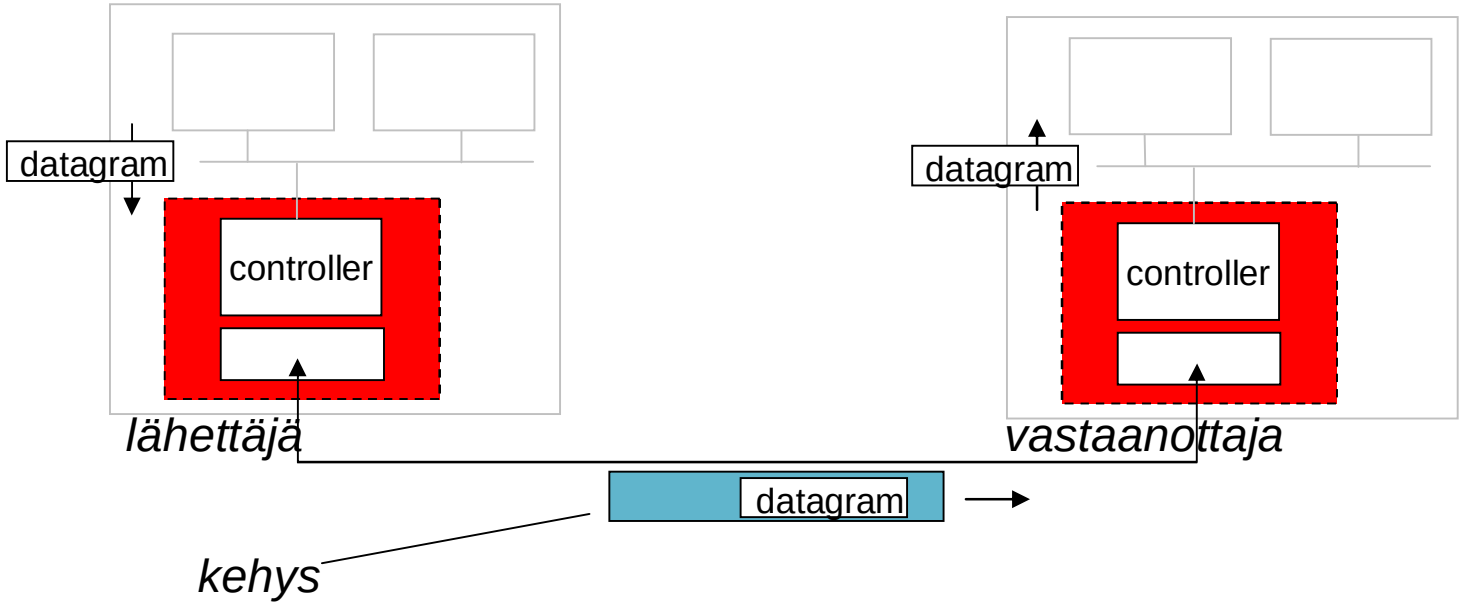
Missä linkkikerros on toteutettu?

- Jokaisessa tietokoneessa
- Linkkikerros käytännössä adapterissa eli “verkkokortissa” (Network Interface Card, NIC)
  - Ethernet kortti, PC-kortti, 802.11 kortti tai adapteri
  - Toteuttaa linkki- ja fyysisen kerroksen
- Asennetaan tietokoneen väylään
- Yhdistelmä rautaa, softaa ja sulautettua ohjelmistoa



Esimerkkejä verkkokorteista

Adapterit (verkkokortit) kommunikoivat

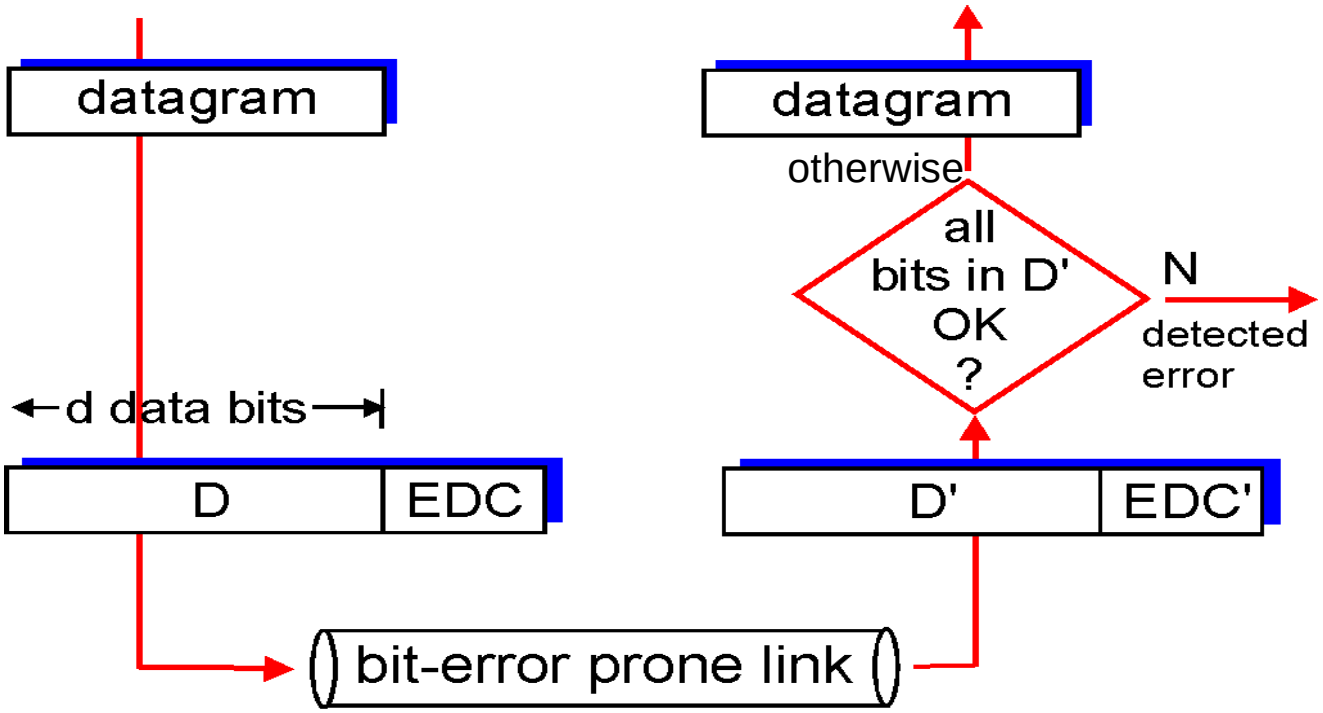


- Lähettävä puoli:
  - Kapseloi datagrammin kehykseen
  - Lisää virheenkorjausbitit, rdt, vuon ohjaus, jne.
- Vastaanottava puoli
  - Tutkii mahdolliset siirtovirheet, rdt, vuon ohjauksen, jne.
  - Kaivaa datagrammin, ja antaa sen ylemmille kerroksille vastaanottopäässä

Virheenkorjaus

EDC= Error Detection ja Correction bittejä (redundanssi)
D = Data suojattu virheen tarkistuksella, saattaa sisältää otsakekenttiä

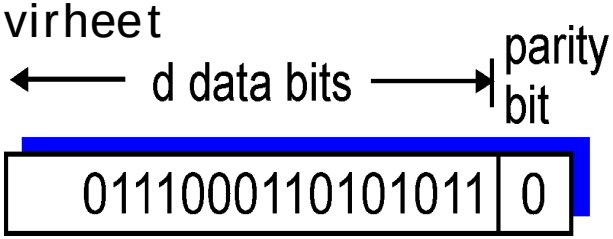
- Virheen havaitseminen ei ole 100% luotettavaa!
  - protokolla saattaa jättää joitain virheitä huomaamatta, mutta harvoin.
  - Isompi virheenkorjauskenttä (EDC kenttä) antaa paremmat mahdollisuudet virheiden havaitsemiseen ja korjaamiseen



Pariteettitarkistus

Yhden bitin pariteetti:

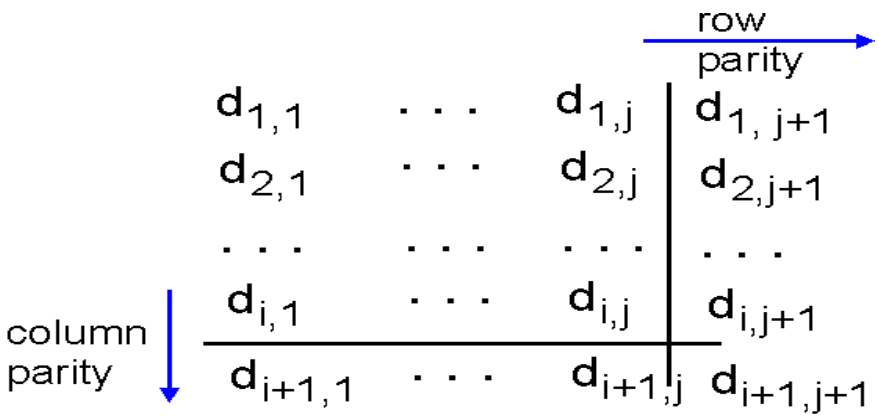
Huomaa yhden bitin virheet

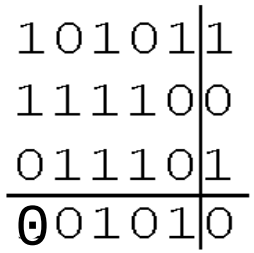


- Yhden bitin pariteettitarkistus huomaa yhden muuttuneen bitin, mutta ei tiedä mikä bitti on väärin, eli ei pysty korjaamaan virhettä.
- Kaksidimensionaalinen tarkistus mahdollistaa yhden bitin virheenkorjaamisen.
- Erityisesti langattomilla linkeillä siirtovirheitä tulee paljon ja tarvitaan huomattavasti kehittyneempiä virheenkorjausmenetelmiä. Tällöin virheenkorjaukseen saatetaan tarvita jopa puolet kaikista siirrettävistä biteistä!

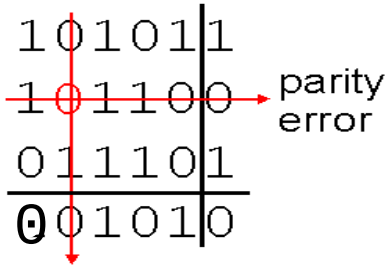
Kaksidimensionaalinen bittipariteetti:

Huomaa ja korjaa yhden bitin virheet





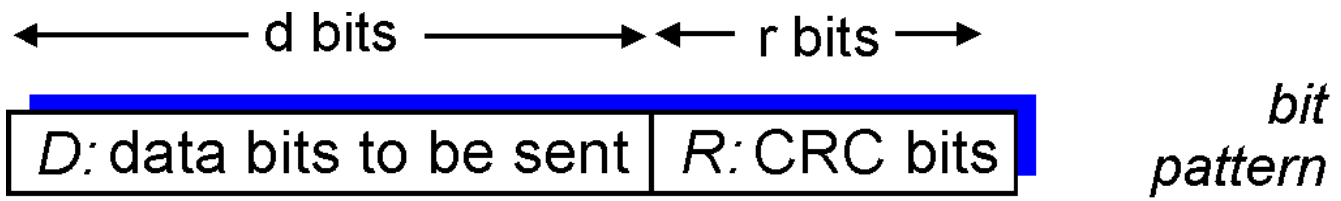
no errors



correctable single bit error

Tarkistussumman laskeminen: Cyclic Redundancy Check (CRC)

- tarkastellaan databittejä, D, binäärinumerona
- valitaan r+1 bittikuvio (generaattori), G
- tavoite: valitaan r CRC bittiä (R ao. Kuvassa), siten, että
  - <D,R> täsmälleen jaettavissa G:llä (modulo 2), eli jakojäännös nolla
  - vastaanottaja tietää G:n, jakaa <D,R> G:llä. Jos nollasta poikkeava jakojäännös: havaittu virhe!
  - voi havaita kaikki purskeiset virheet, joita vähemmän kuin r+1 bittiä
- Laajasti käytetty todellisuudessa (Ethernet, 802.11 WiFi, ATM), Ethernetissä CRC-32 (32 bittiä)



$D * 2^r \quad XOR \quad R$

mathematical formula

CRC Esimerkki

Halutaan:

$D \cdot 2^r$ XOR R = nG

Vastaa, että:

$D \cdot 2^r$ = nG XOR R

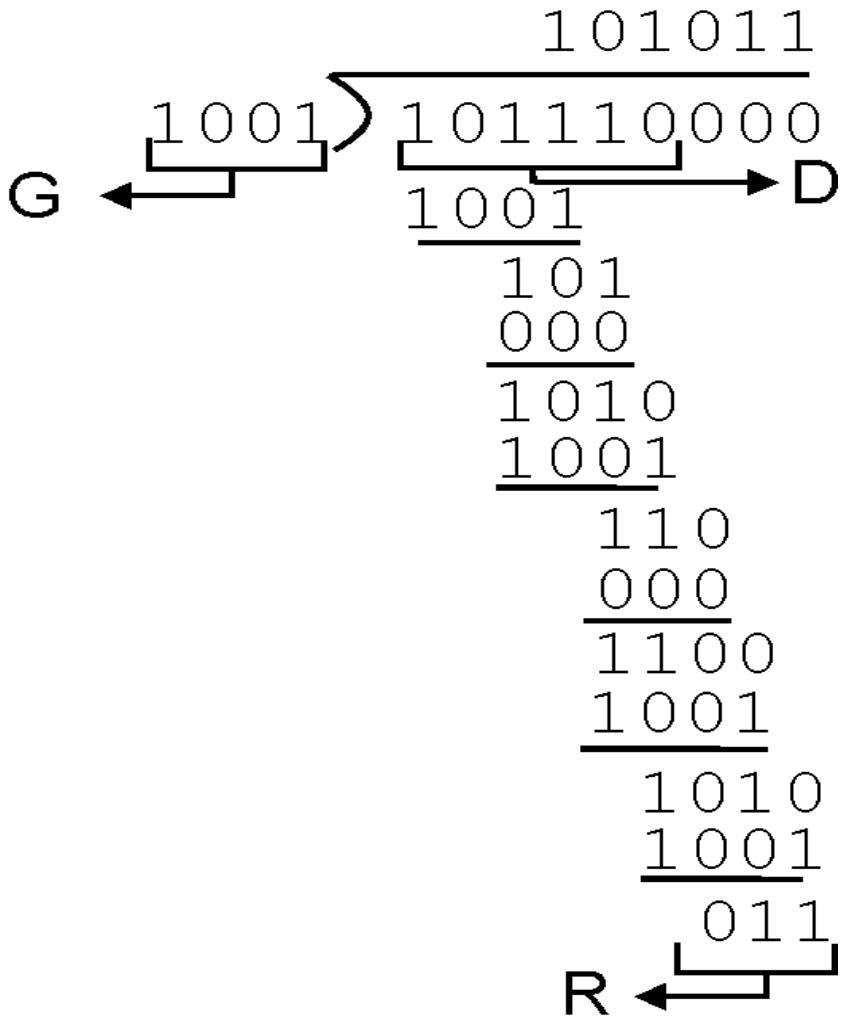
On yhtä kuin:

jos jaamme $D \cdot 2^r$ G:llä, saadaan jakojäännös R

Lähetettäessä jakojäännös pistetään datan perään

Vastaanottaja jakaa koko datan samalla G:llä, ja jos jakojäännös nolla (kaikki bitit nollia), ei havaittuja siirtovirheitä

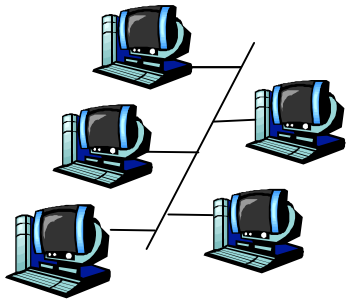
$$R = \text{jakojäännös}\left[\frac{D \cdot 2^r}{G}\right]$$



Monipääsy (Multiple Access) ja Protokollat (Kurose kpl 5.3)

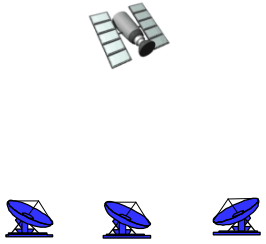
Kahdentyyppisiä “linkkejä”:

- Pisteestä-pisteeseen (point-to-point)
  - PPP linkit modeemiyhteyksille, esim. ADSL
  - point-to-point linkit Ethernet kytkimen ja tietokoneiden välillä
- “Yleislähetys” (broadcast) (jaettu johto tai radiotaajuus)
  - “Vanhanaikainen” Ethernet (jossa työasemat kiinni samassa kaapelissa)
  - 802.11 WLAN eli langaton lähiverkko



Yhteinen (jaettu) kaapeli (esim., kaapeloitu Ethernet)

Jaettu RF-taajuus (esim., 802.11 WiFi)



jaettu RF (satelliitti)

ihmiset cocktail kutsuilla (jaettu ilmatila, akustinen)

Monipääsyprotokollat

- Yksi jaettu lähetyskanava
- Jos kaksi tai useampia lähetyksiä samaan aikaan
  =>Törmäys ja tieto menetetään

Monipääsyprotokollan tehtävät ja tavoitteet:

- Hoitaa koordinaation, kuka saa käyttää jaettua kanavaa ja käyttää itse samaa kanavaa! (ei kaistan ulkopuolista kanavaa koordinointiin)
- Ideaalinen monipääsyprotokolla:
  - Antaa koko kaistan yhdelle käyttäjälle, jos käyttäjiä on vain yksi, eli bittinopeus on R b/s, jossa R on kanavan koko kapasiteetti, esim. 100 Mb/s. Vaihtoehtona piirikytkentäisessä tietoliikenteessä kapasiteetti jaetaan esim. aikaslotteihin (aikaväleihin), yksi käyttäjä saa vain osan kaistaa (mutta toisaalta saa sen varmasti).
  - Kun M solmua haluaa lähettää ne saavat keskimäärin R/M b/s kaistan
  - Ei kellojen synkronointia, aikavälejä
  - Täysin hajautettu: Ei erikoissolmua joka koordinoi lähetyksiä ja joka vikaantuessaan estäisi koko verkon toiminnan
  - Yksinkertainen ja halpa

MAC kanavanvarausprotokollat

Kolme isompaa luokkaa:

- Kanavan osittaminen
  - Jaetaan kanava pienempiin osiin (aikavälejä, taajuuksia, CDMA-koodeja)
  - Allokoidaan yksi osa tietyn solmun yksinomaiseen käyttöön
  - Esim. piirikytkentäinen tietoliikenne: Puhelinverkko, GSM, 3G..
- Satunnainen pääsy (Random pääsy)
  - Kanavaa ei jaeta, sallitaan törmäykset
  - “toivutaan” törmäyksistä
  - Esim. Ethernet ja WLAN
- “Vuorottelu”
  - Solmut saavat vuoroja lähettää, mutta solmut joilla on enemmän lähetettävää saavat pidempiä vuoroja
  - Esim. IBM Token-Ring (ei enää käytössä)

Satunnainen pääsy (Random pääsy)

- Kun solmulla on paketti lähetettävänä
  - Lähetetään täydellä kanavan nopeudella R (Mb/s).
  - Ei etukäteen (*a priori)* koordinointia solmujen välillä
- Yksi tai enemmän lähettäviä solmuja => “törmäys”,
- Satunnaispääsy MAC protokolla määrittelee:
  - Kuinka törmäykset tunnistetaan
  - Kuinka törmäyksistä toivutaan (esim. viivästettyjen uudelleenlähetysten avulla)
- Esimerkkejä satunnaispääsy MAC protokollista:
  - aikajaettu ALOHA ja pelkkä ALOHA (vanhoja)
  - CSMA, CSMA/CD, CSMA/CA,
    - Tässä termit: CSMA = Carrier Sense Multiple Access, CD= Collision Detection, CA = Collision Avoidance
    - Näitä käytetään Ethernetissä ja WLAN:issa

CSMA (Carrier Sense Multiple Access)

CSMA: Ennen lähetystä kuunnellaan onko siirtotiellä signaalia:

- Jos kanava on vapaa:
  - lähetetään koko kehys
- Jos kanava on varattu:
  - viivästetään lähetystä

- Ihmisanalogia keskustelussa: Älä keskeytä toista!

CSMA törmäykset

Vaikka siirtotie on lähetettäessä vapaa törmäyksiä voi silti tulla:

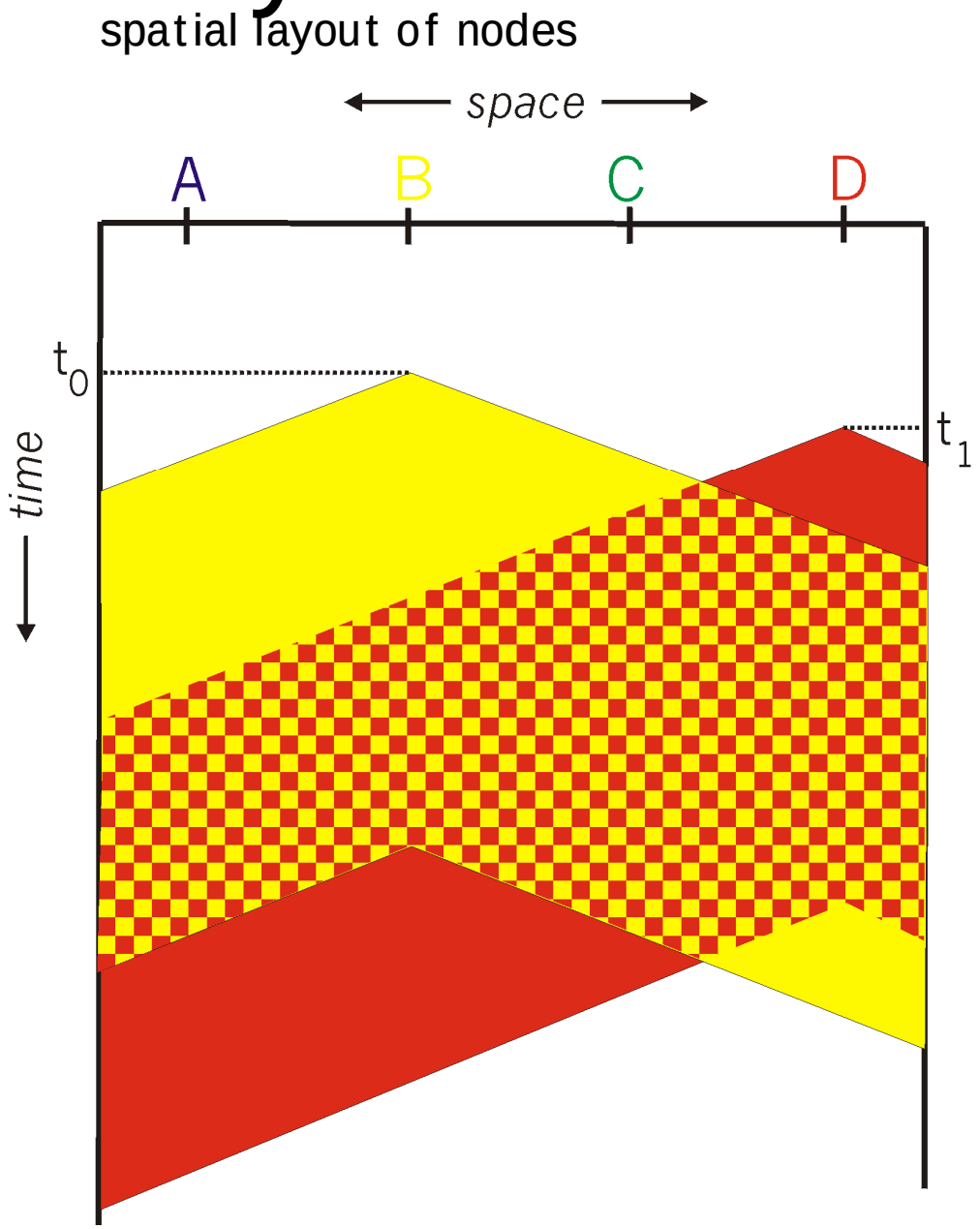
Etenemisviiveen takia solmut eivät tiedä, että toiset ovat jo ehkä lähettäneet kehyksen

törmäys:

Koko paketti tuhoutuu

Huom.:

Etäisyys ja etenemisviive määräävät törmäystodennäköisyyden



CSMA/CD (Törmäysten ilmaisu)

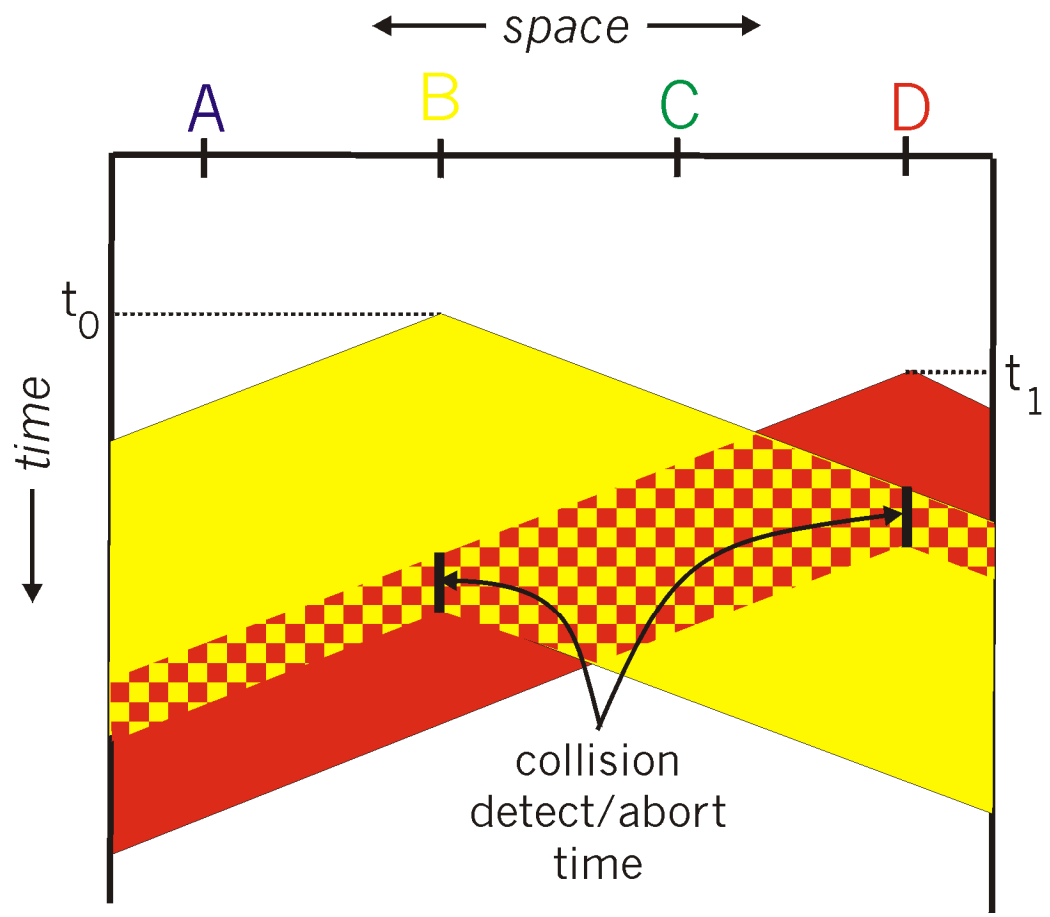
CSMA/CD: kanavan kuuntelu, viivästetään lähetystä kuten CSMA:ssa

- törmäykset ilmaistaan lyhyessä ajassa
- siirto keskeytetään heti törmäyksen jälkeen, jolloin kanavan hukkakäyttö pienenee

§ Törmäysten ilmaisu (=CD Collision Detection= törmäysten ilmaisu):

- helppoa langallisissa LAN:eissa: mitataan signaalin voimakkuutta ja verrataan lähetettyyn
- vaikeaa langattomissa LAN:eissa (WLAN): vastaanotetun signaalin taso vaihtelee hyvin laajoissa rajoissa
- ihmisanalogia: kohtelias keskustelija; lopeta puhuminen, jos toinen jo ehti aloittaa

CSMA/CD törmäysten ilmaisu



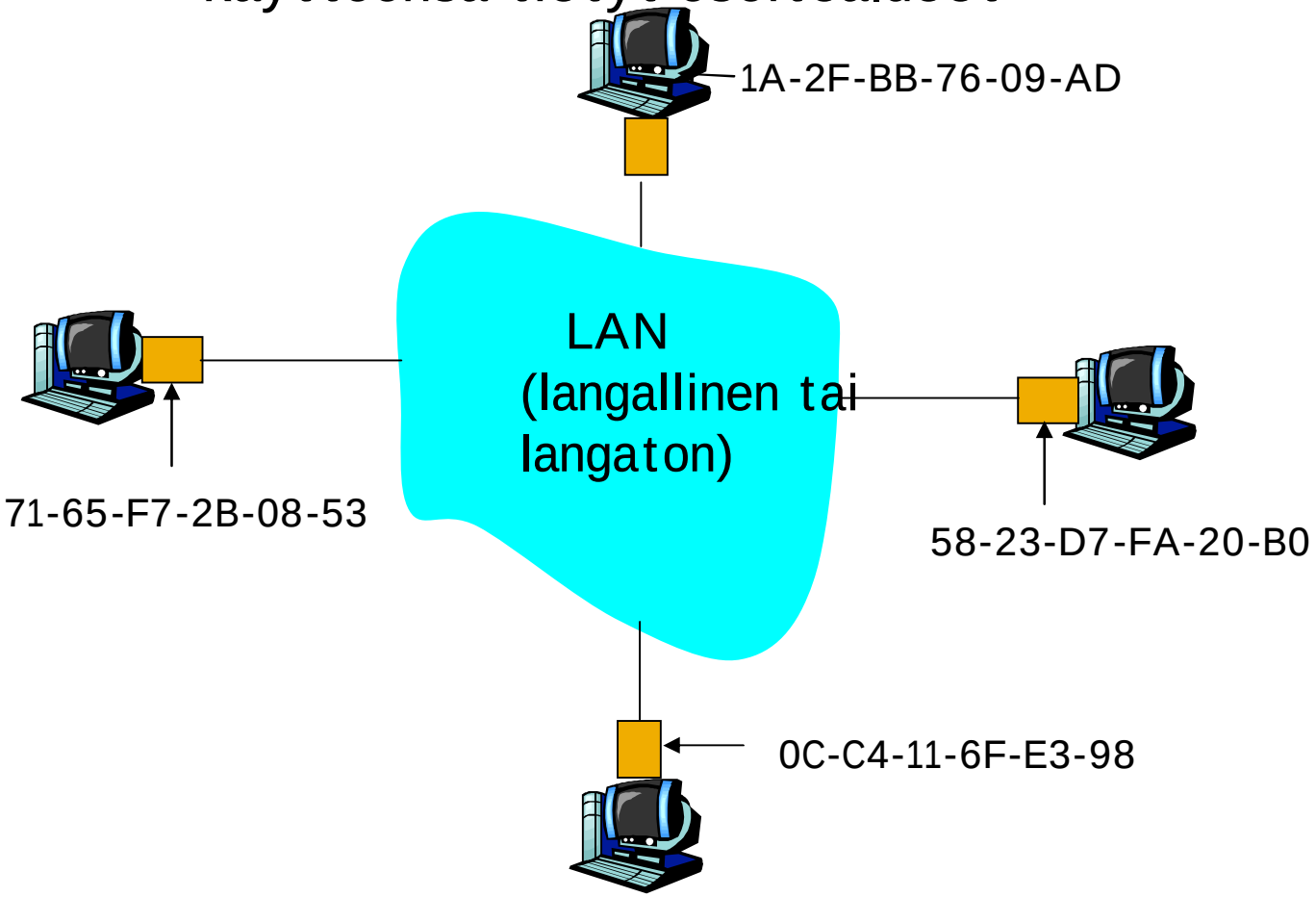
MAC osoite ja ARP (Kurose, kpl 5.4)

- IP osoite on 32-bittinen :
  - *Verkkotason* osoite
  - käytetään siihen, että datagrammi saadaan kohdeverkkoon
- MAC (eli LAN eli fyysinen eli Ethernet) osoite:
  - tehtävä: saada kehys viedyksi yhdestä liitännästä toiseen fyysisesti kytkettyyn liitäntään *(sama verkko)*
  - 48 bittinen MAC osoite (useimmissa LAN:eissa)
    - poltettu verkkokortin (NIC) ROM:iin, joskus ohjelmallisesti muutettavissa

LAN osoite

Jokaisella verkkoadapterilla (kortillla) on uniikki LAN (MAC) osoite.

Verkkokorttien ja tietokoneiden valmistajat saavat käyttöönsä tietyt osoitealueet



Broadcast osoite =
FF-FF-FF-FF-FF-FF
(kaikki bitit ykkösiä)
Kaikki vastaanottavat
broadcast-kehykset

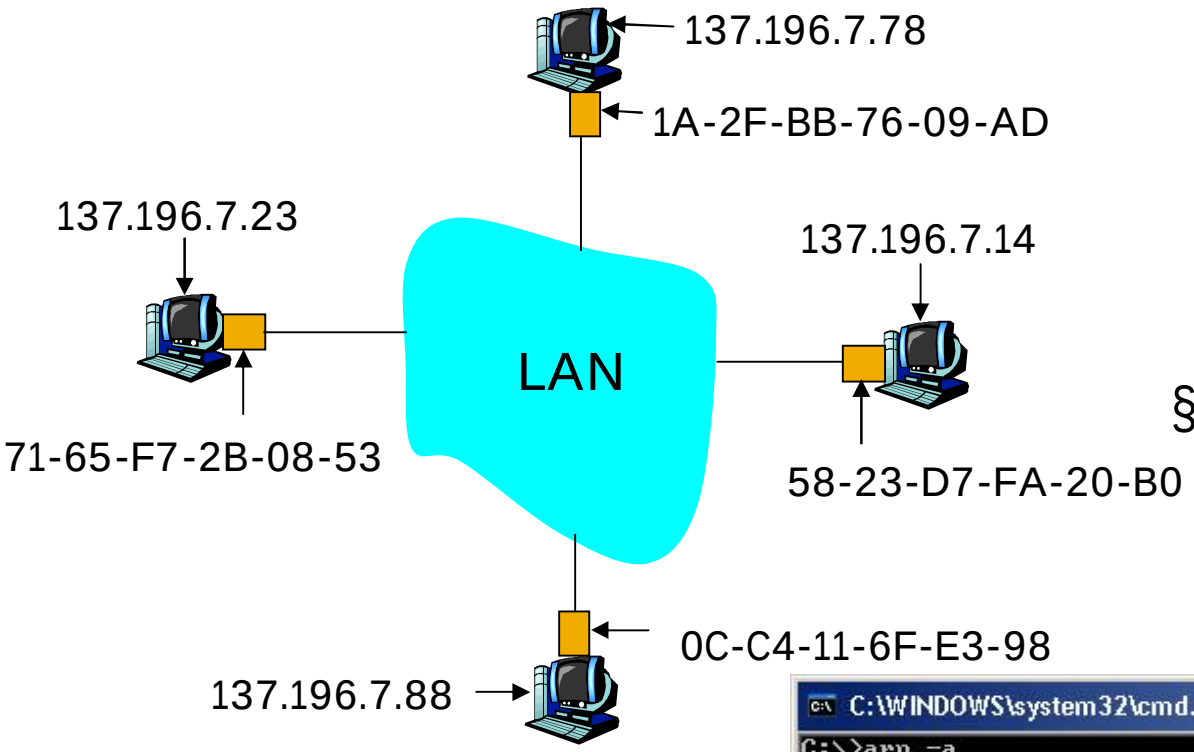
= adapteri

LAN osoite (lisää)

- MAC osoitteiden allokaatiota hallinnoi IEEE
- Valmistajat ostavat jonkun osan MAC osoiteavaruudesta (jotta varmistetaan yksikäsitteisyys)
- analogia:
  - (a) MAC osoite: kuten sotu-numero
  - (b) IP osoite: kuten postiosoite
- MAC: yksikäsitteinen osoite (flat osoite) -> siirrettävyys
  - LAN kortin (ja tietokoneen) voi viedä LAN:ista toiseen
- IP:n hierarkkinen osoite EI OLE SIIRRETTÄ
  - Osoite riippuu IP-aliverkosta, mihin laite on kytketty

ARP: Osoitteenselvitys protokolla (Address Resolution Protocol)

Kysymys: **Kuinka selvitetään B:n MAC osoite kun tiedetään B:n IP-osoite?**



- Jokaisessa IP-laitteessa (tietokone, reititin) LAN:issa on ARP taulu
- ARP taulu: IP/MAC osoitteiden mappaus LAN solmuille

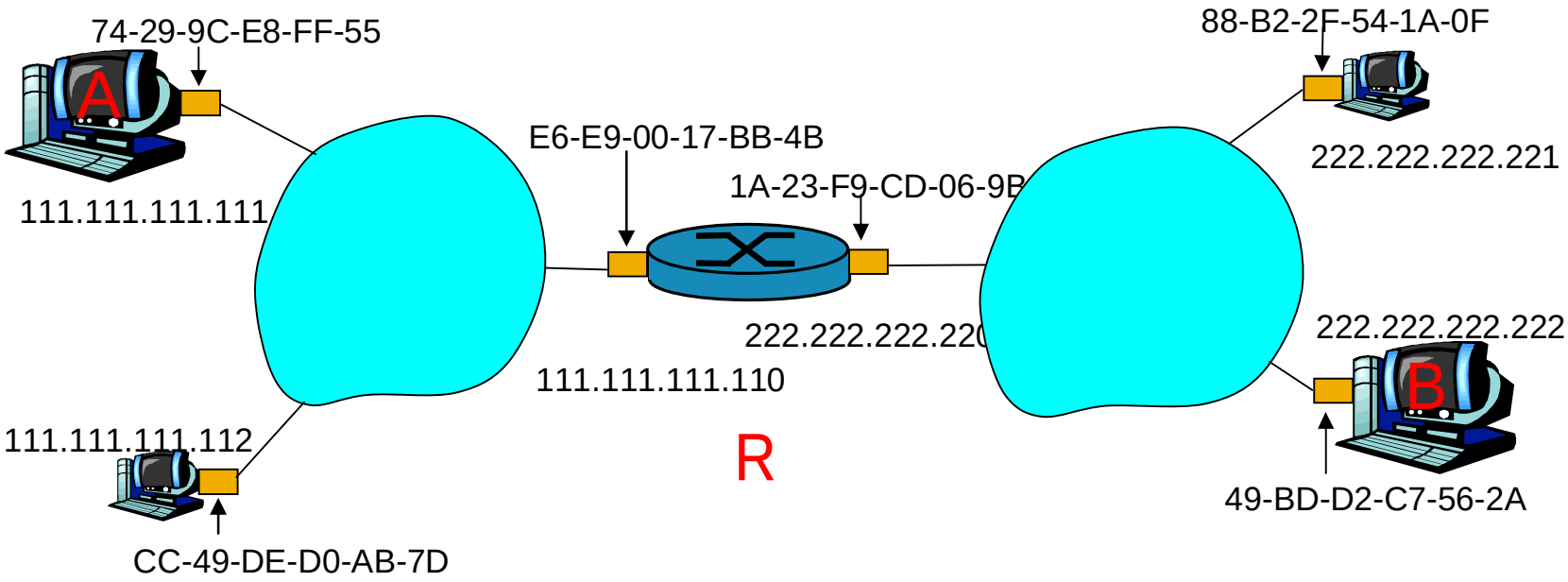
  < IP osoite; MAC osoite; TTL>
  - TTL (Time To Live): aika jonka jälkeen osoitteiden kytkentä unohdetaan (tyypillinen 20 min)
- Esim. Windowsissa, komento arp –a näyttää koneen IP ja MAC osoitteen kytkennän

ARP protokolla: Sama LAN (verkko)

- A haluaa lähettää datagarmmin B:lle, mutta B:n MAC osoite ie ole ARP taulussa.
- A lähettää ARP kyselypaketin, jossa B:n IP osoite
  - kohde MAC osoite = FF-FF-FF-FF-FF-FF
  - LAN:in kaikki koneet vastaanottavat ARP kyselyn
- B vastaanottaa ARP paketin, vastaa A:lle omalla (B:n) MAC osoitteellaan
  - kehys lähetetään A:n MAC osoitteeseen (unicast)
- A tallentaa IP-to-MAC osoiteparin ARP-tauluunsa siihen asti kunnes tieto vanhenee (aika loppuu)
  - Informaatio ei käytettävissä (times out) jollei sitä virkistetä
- ARP on “plug-and-play”:
  - Solmut tekevät omat ARP taulunsa *ilman verkon administriaattorin sekaantumista*

Osoitteistus: reititys toiseen LAN:iin

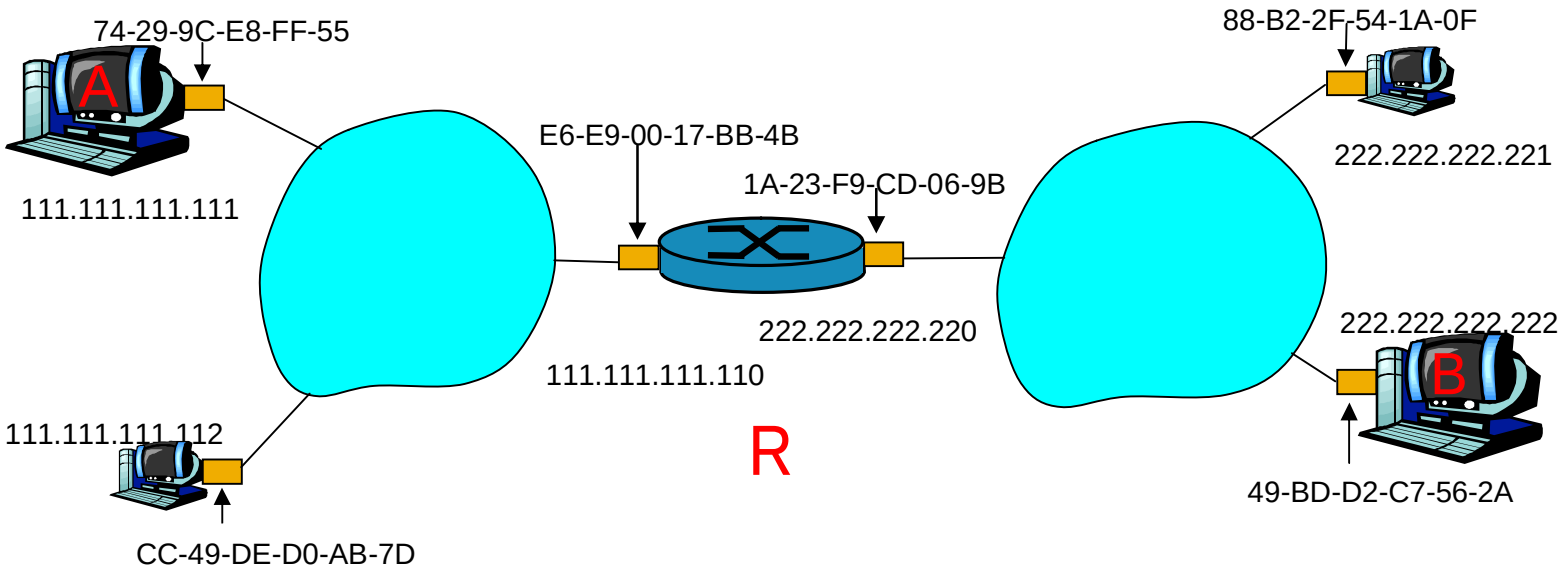
Tutkitaan esimerkki: lähetetään datagrammi A:sta B:hen R:n kautta
oletetaan, että A tietää B:n IP-osoitteen



§ kaksi ARP taulua reitittimessä R, yksi kummallekin IP verkolle (LAN)

- A tekee IP datagrammin lähdeosoitteena A, kohdeosoitteena B
- A käyttää ARP:ia saadakseen selville R:n MAC osoitteen 111.111.111.110
- A tekee linkkikerroksen kehyksen, jossa R:n MAC osoite kohdeosoitteena; kehys sisältää lähetettävän A-B IP datagrammin
- A:n NIC lähettää kehyksen
- R:n NIC vastaanottaa kehyksen
- R poistaa IP datagrammin Ethernet kehyksestä, ja näkee, että sen määränpää on B
- R käyttää ARP:ia saadakseen B:n MAC osoitteen
- R tekee kehyksen, jossa A-B IP-datagrammi ja lähettää sen B:lle

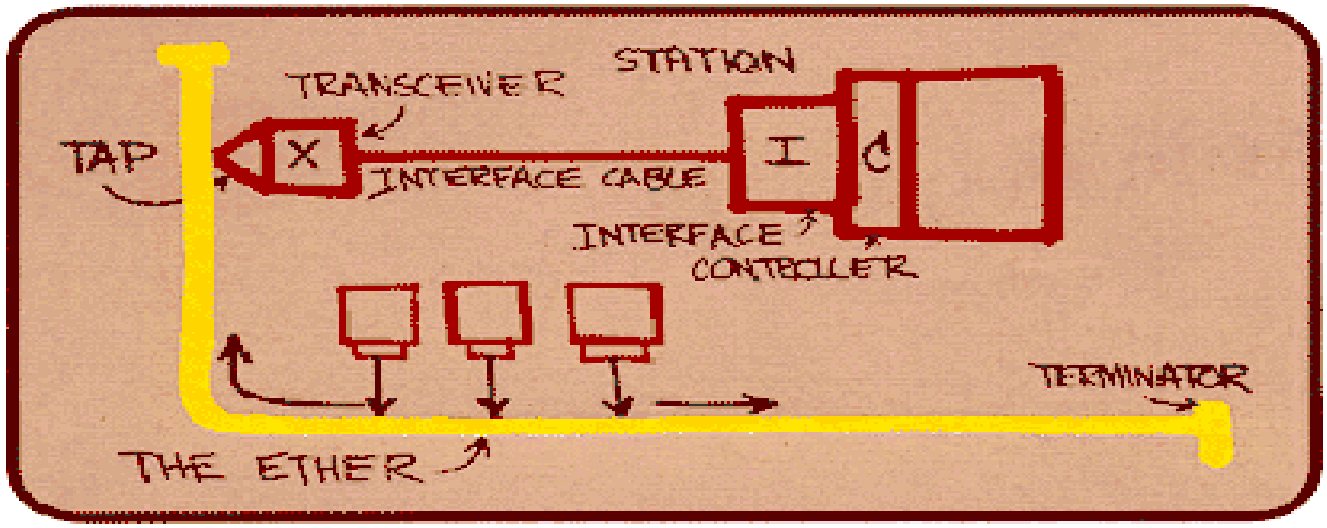
Tämä on todella tärkeä esimerkki – varmista, että ymmärrät!



Ethernet ja vähän historiaa…

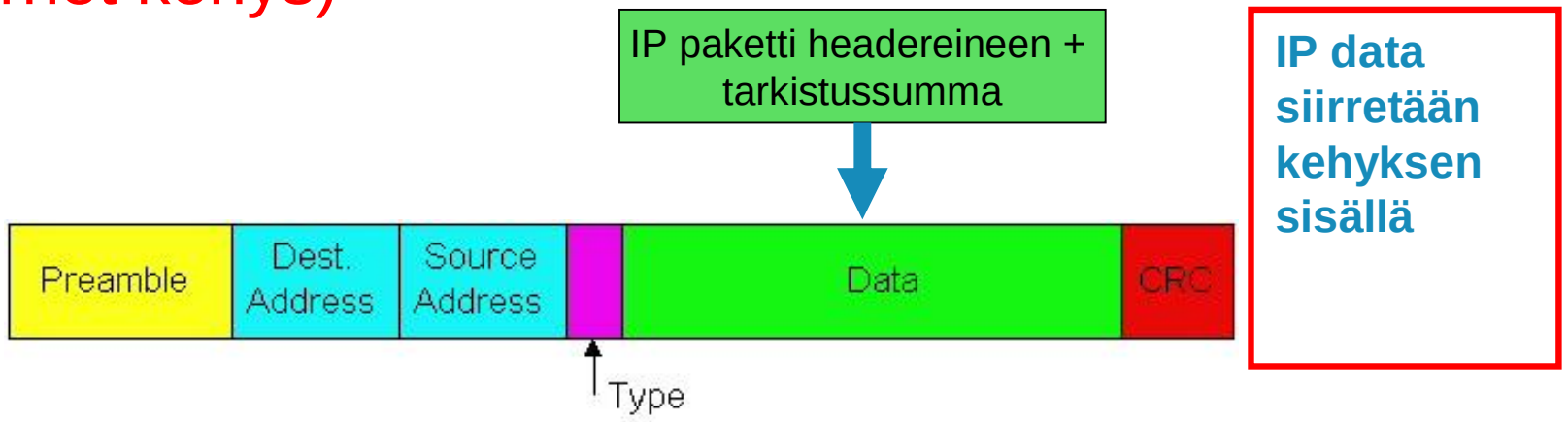
- Nykyään dominoiva langallinen LAN teknologia
- Historiaa:
  - 1970 ALOHAnet radioverkko käyttöön Hawajin saarilla
  - 1973 Metcalf ja Boggs kehittävät ideasta Ethernetin, kilpavarausverkon
  - 1979 DIX Ethernet II Standardi (Digital, Intel, Xerox ->DIX)
  - 1985 IEEE 802.3 LAN Standardi (10 Mbps)
  - 1995 Fast Ethernet (100 Mbps)
  - 1998 Gigabit Ethernet
  - 2002 10 Gigabit Ethernet
- Tänään Ethernet on hallitseva lähiverkkostandardi. Ethernet on pysynyt mukana nopeuskilpailussa: 10 Mbps – 10 Gbps -100 Gb/s (tulossa) sekä hintakilpailussa

Metcalf:in Skitsi:



Ethernet kehyksen rakenne

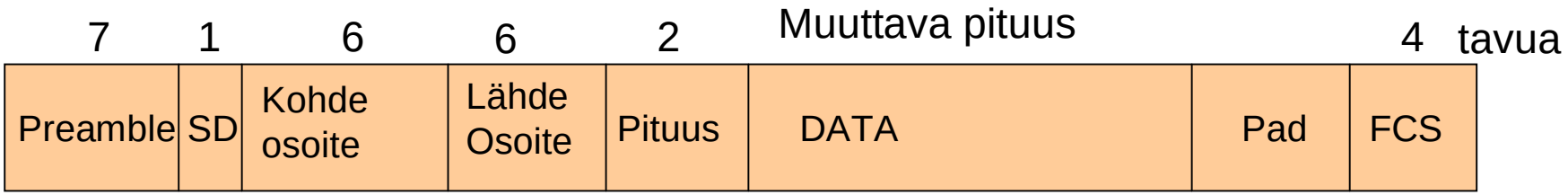
Lähettävä adapteri kapseloi IP datagrammin (tai muun verkkoprotokollan paketin) in Ethernet kehykseen (Ethernet kehys)



Kehyksen alussa aina tahdistusosa (Preamble):

- 7 tavua jossa bitit menevät sekvenssissä 10101010. Tätä seuraa yksi tavu “10101011” (SD)
- käytetään vastaanottimen synkronointiin lähettäjän kellon nopeuteen

IEEE 802.3 – Kehysrakenne tarkemmin



Yhteensä 64 - 1518 tavua

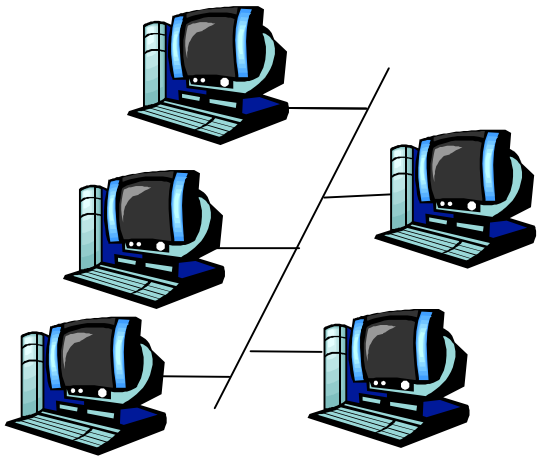
- Preamble (Alkutahdistus) toistaa 10101010-kuviota
- SD aloittaa itse kehyksen tavulla 10101011
- Vastaanottajan ja lähettäjän osoitteet ovat 6 tavua
- Pituus on informaatio-kentän pituus tavuissa
- DATA, lähetettävä tieto (esim. IP-paketti)
- Padding (täytebitit) varmistaa, että kehys on vähintään 64 tavua
- Tarkistussumma on CCITT 32-bit CRC kattaen osoitteen, pituuden, informaation ja paddingin (täytebitit)

Ethernetin osoitteet

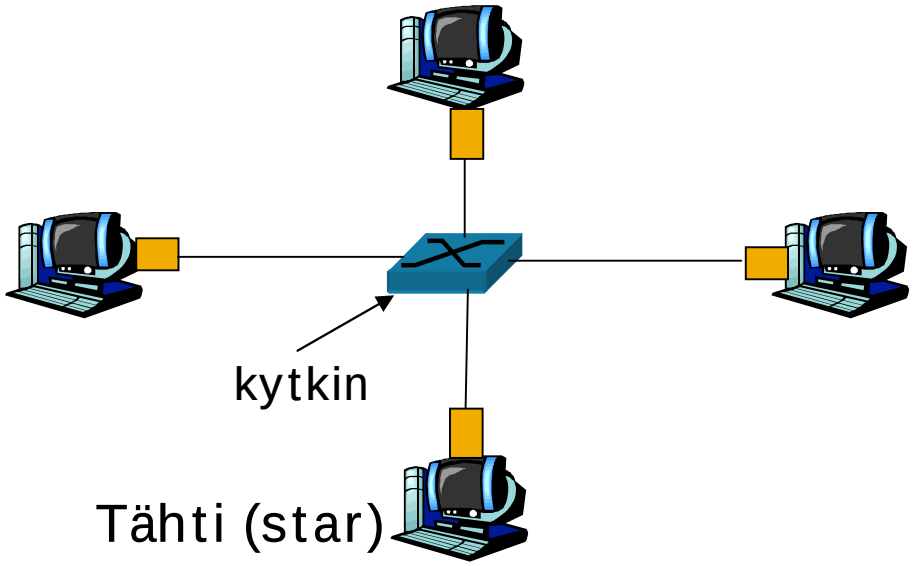
- Jokaisella verkkokortilla (NIC) on uniikki osoite (MAC-osoite)
  - valmistajan kiinteästi asettama tai ohjelmistollisesti vaihdettava
  - 1. bitti kertoo onko kyseessä täsmälähetys (0) vai ryhmälähetys (1)
  - 2. bitti kertoo onko kyseessä paikallinen (0) vai globaali (1) osoite
  - 3 ensimmäistä tavua (miinus kaksi ensimmäistä bittiä) on Organizationally Unique Identifier (OUI)
  - 3 viimeistä tavua on valmistajan valittavissa
  - yleislähetys on osoitteelle ff:ff:ff:ff:ff:ff (kaikki bitit 1)
  - saman osoitteen sattuminen kahdelle verkkokortille samassa verkossa on harvinaista, mutta mahdollista
- Asema voi lähettää täsmälähetyksiä (unicast), ryhmälähetyksiä (multicast) tai yleislähetyksiä (broadcast)
  - IP ja muut protokollat tarvitsevat yleislähetyksiä muiden samassa lähiverkossa olevien asemien (ARP) tai verkkoasetuksia tarjoavien palveluiden (DHCP) löytämiseen
  - Tavallinen liikenne on täsmälähetyksiä

Ethernet topologia: Tähti (Star)

- Bussitopologia (yhteinen jaettu kaapeli) suosittu 90-luvun puoliväliin asti
  - Kaikki solmut samassa “mediassa” ja törmäyksiä sattuu)
- Tänään: Käytännössä tähtitopologia (star)
  - Aktiivinen *kytkin* keskellä *kytkin*
  - Jokainen osallistuja (“haara”) käyttää omaa Ethernet protokollaa (solmut eivät törmää keskenään)



bussi: koaksiaalikaapeli



Ethernet: Epäluotettava, yhteydetön

- yhteydetön: No kättelyä (handshaking) lähettävän ja vastaanottavan NIC:in välillä
- epäluotettava: vastaanottava NIC ei lähetä kuittauksia (ack / nack) lähettävälle NIC:ille
  - virta datagrammeja välitetään verkkokerrokselle ja siinä voi olla aukkoja (puuttuvia datagrammeja)
  - aukot täyttyvät, jos sovellutus käyttää TCP:tä
  - muutoin, sovellutus ei saa kaikkea dataa vastaan (näin tapahtuu esim. VoIP puheluissa, jotka käyttävät yhteydetöntä UDP-protokollaa)
- Ethernetin MAC protokolla: ei aikajaettu vaan CSMA/CD

Ethernet CSMA/CD algoritmi

1. NIC vastaanottaa datagrammin verkkokerrokselta, ja tekee kehyksen
2. Jos NIC huomaa, että kanava on vapaa, se lähettää kehyksen. Jos NIC huomaa, että kanava on varattu, se odottaa kunnes kanava on vapaa, ja lähettää sitten
3. Jos NIC pystyy lähettämään koko kehyksen ilman, että se linjalla muuta transmissiota, NIC saa kehyksen perille !
4. Jos NIC huomaa toisen transmission sillä aikaa kun se lähettävää, se lopettaa lähetyksen ja lähettää kanavaan jam signaalin (jumissa signaali)
5. Lopetettuaan NIC menee **exponentiaaliseen peruutustilaan (exponential backoff)**: *m*:nnen törmäyksen jälkeen, NIC valitsee *K:n siten, että arvotaan* satunnainen arvo väliltä $\{0,1,2,\ldots,2^m-1\}$. NIC odottaa $K \cdot 512$ bitin aikaa, ja palaa sitten vaiheeseen 2

NIC = Network Interface card = Verkkokortti tai adapteri

Ethernet:in CSMA/CD (lisää)

Jumitussignaali (Jam signal): varmistetaan, että kaikki muut lähettäjät ovat selvillä törmäyksestä; 48 bittiä

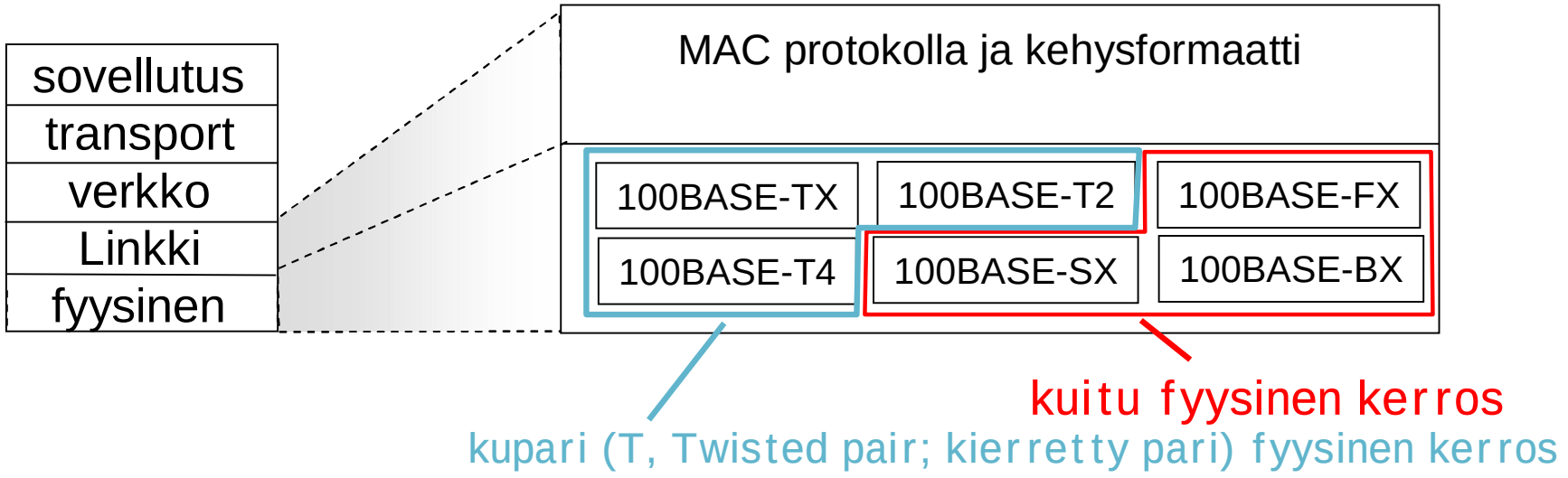
Bitin aika: 0.1 microsekuntia 10 Mbps Ethernetissä ; kun K=1023, odotusaika on noin 50 millisekuntia

Exponential Backoff (**exponentiaalinen peruutustila)**:

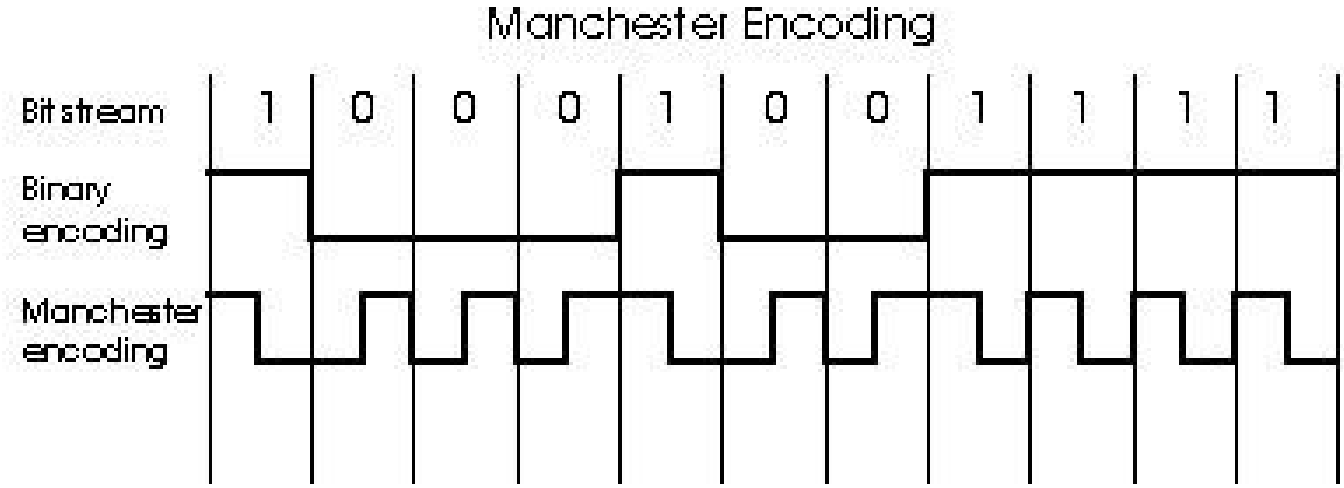
- *Tavoite*: adaptoida uudelleenlähetysyritykset arvioituun silloiseen kuormaan
  - Suuri kuormitus: satunnainen odotus on pidempi
- ensimmäinen törmäys: valitaan K väliltä {0,1}; viive on K· 512 bitin siirtoaikaa
- Toisen törmäyksen jälkeen : valitaan K väliltä {0,1,2,3}…
- Kymmenennen törmäyksen jälkeen, valitaan K väliltä {0,1,2,3,4,…,1023}

802.3 Ethernet Standardit: linkki & fyysinen kerros

§ *monia* erilaisia Ethernet standardeja
- yhteinen MAC protokolla ja kehysformaatti
- erilaisia nopeuksia: 2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps
- Monia erilaisia siirtoteitä (media): kuitu, kaapeli



Bittien fyysinen siirto Ethernet:issä Manchester koodaus



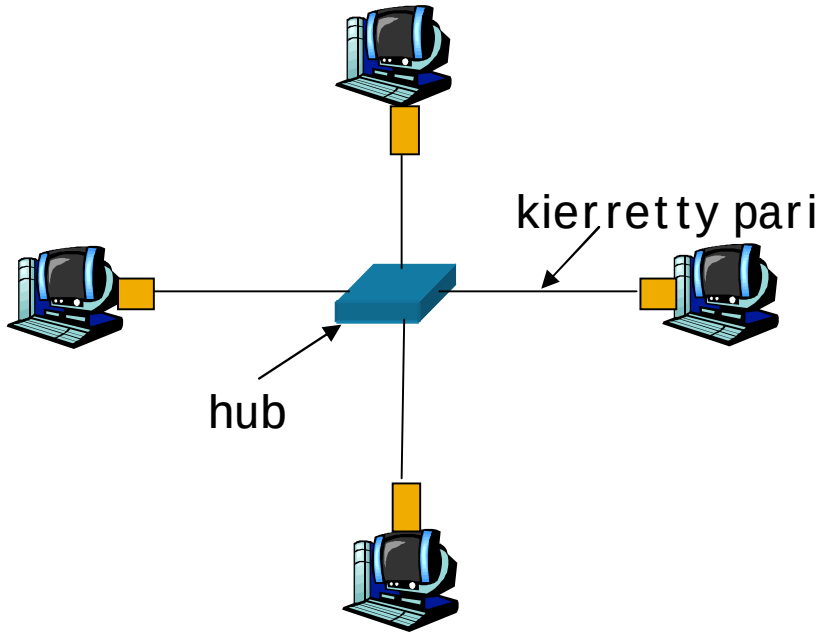
- Ethernet kehykseen kuuluvat bitit siirretään fyysisellä kerroksella jännitteinä (tai valon intensiteettivaihteluna kuidussa), mutta ei ihan siten, että looginen “1” vastaa esim. -1 V ja looginen “0”=0V.
- 10BaseT:ssä (10 Mb/S Ethernet) käytetään Manchester koodausta
  - Tällöin jokainen bitti kokee siirtymän: 1-bitti lähetään siten, että jännite menee loogisesta ykkösestä loogisen nollaan lähetettävän bitin AIKANA (siirtymä) 1->0, Vastaavasti 0-bitille siirtymä:0->1
  - 100 Mb/s käyttää NRZI koodausta ja 1 ja 10 Gb/s Ethernetissä 5/16-tasoista PAM koodausta tehon lisäämiseksi
- Manchester koodaus sallii mm. kellojen lähettävässä ja vastaanottavassa solmussa synkronoitua jokaisella bitillä
  - Ei tarvetta keskitettyyn, globaalin kelloon solmujen kesken!
- Muuten: tämä on fyysisen tason juttua, mutta otetaan tässä kokonaiskuvan selkiinnyttämiseksi!

Linkkikerros: Pakettien välitys ja kytkimet, Kurose kpl 5.6

Hubit (Hub)

… fyysisen-kerroksen (“tyhmät”) toistimet:

- Hub on yksinkertaisin tapa yhdistää useita tietokoneita. IP data voi liikkua kunhan koneilla on sama verkko-osoite. Kahden koneen välillä voi myös käyttää cross-over kaapelia, jossa lähetin (TX) ja Vastaanotin (RX), on kytketty ristiin kaapelia valmistettaessa
- bitit jotka tulevat sisään yhdestä linkistä menevät ulos *kaikkiin* muihin linkkeihin samalla nopeudella.
- Paketit kaikista linkeistä, jotka kytketyt hub:iin voivat törmätä keskenään
- Ei kehysten bufferointia
- ei CSMA/CD hubissa: tietokoneiden NIC:it havaitsevat törmäykset

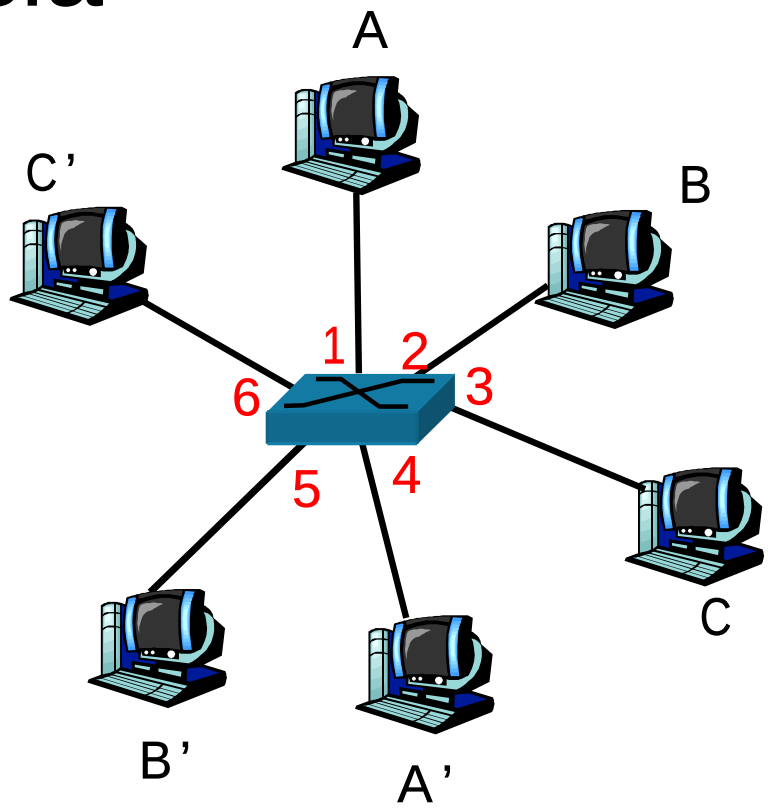


kytkin

- Linkkikerroksen laite: fiksumpi kuin hub, toimii *aktiivisessa* roolissa
  - Varastoi ja välittää Ethernet kehyksiä
  - Tutkii sisääntulevan kehyksen MAC osoitteen, ja välittää kehyksen selektiivisesti yhteen tai useaan ulosmenevään linkkiin.
  - kun kehys pitää välittää segmenttiin, käytetään CSMA/CD algoritmia kontrolloimaan pääsyä segmentille
- *läpinäkyvä*
  - tietokoneet eivät tiedä kytkinten olemassaoloa
- *plug-and-play, itseoppivia*
  - Kytkimiä ei tarvitse konfiguroida

kytkin: sallii *useita* samanaikaisia lähetyksiä

- Tietokoneilla on omat suorat liitäntänsä kytkimeen
- kytkimet bufferoivat (varastoivat) paketteja
- Ethernet protokollaa käytetään *jokaisessa* sisään tulevassa linkissä, mutta ei törmäyksiä; full duplex
  - jokainen linkki on oma törmäys alueensa
- *kytkeminen:* A-A’ ja B-B’ yhtä aikaa, ilman törmäyksiä
  - ei mahdollista tyhmällä hubilla



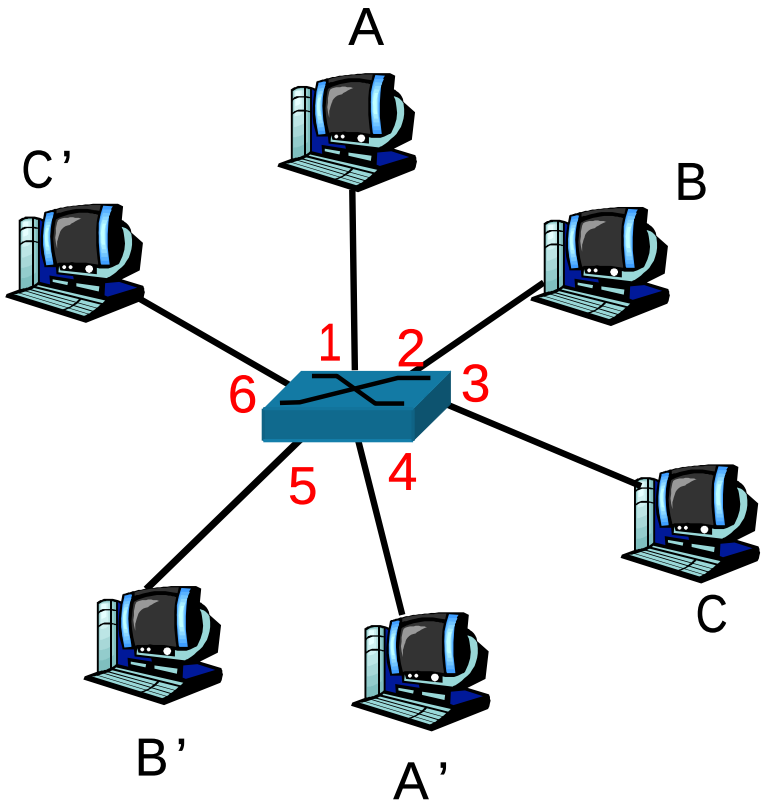
kytkin jossa kuusi liitäntää (1,2,3,4,5,6)

Kytkintaulu

- *Kysymys:* miten kytkin tietää että A' saavutettavissa liitännän 4, ja B' saavutettavissa via liitännän 5 kautta?
- *Vastaus:* jokaisella kytkimellä on kytkintaulu (Switch Table), jokainen rivi:
  - (laitteen MAC osoite, liitäntä jonka kautta saavutetaan tietokone, aikaleima)
- näyttää reititystaululta!

Kysymys: Kuinka kytkintaulun rivit luodaan, ylläpidetään kytkintaulussa?

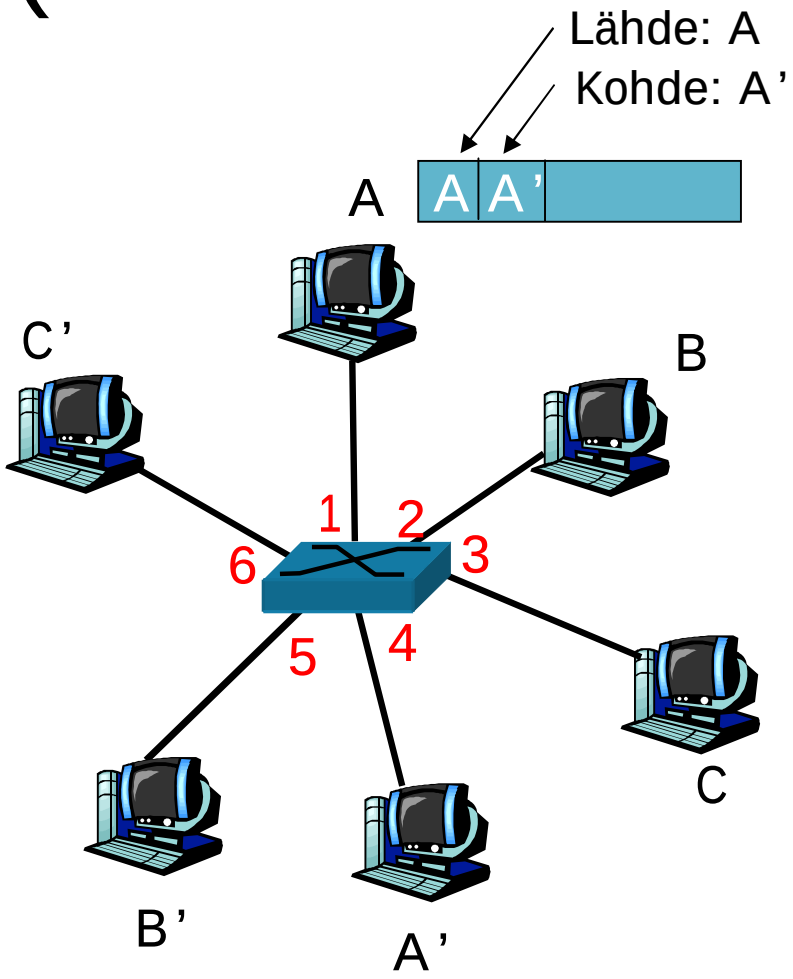
- kuten reititysprotokolla – vai ?



kytkin jossa kuusi liitäntää (1,2,3,4,5,6)

Kytkin: itse-oppiva (self-learning)

- kytkin *oppii* mitkä tietokoneet voi voi saavuttaa minkäkin liitännän kautta
  - Kun kehys vastaanotetaan, kytkin “oppi” lähettäjän sijainnin: sisääntuleva LAN segmentti
  - Kytkin pistää lähettäjä/sijainti parin kytkintauluun (Switch Table)

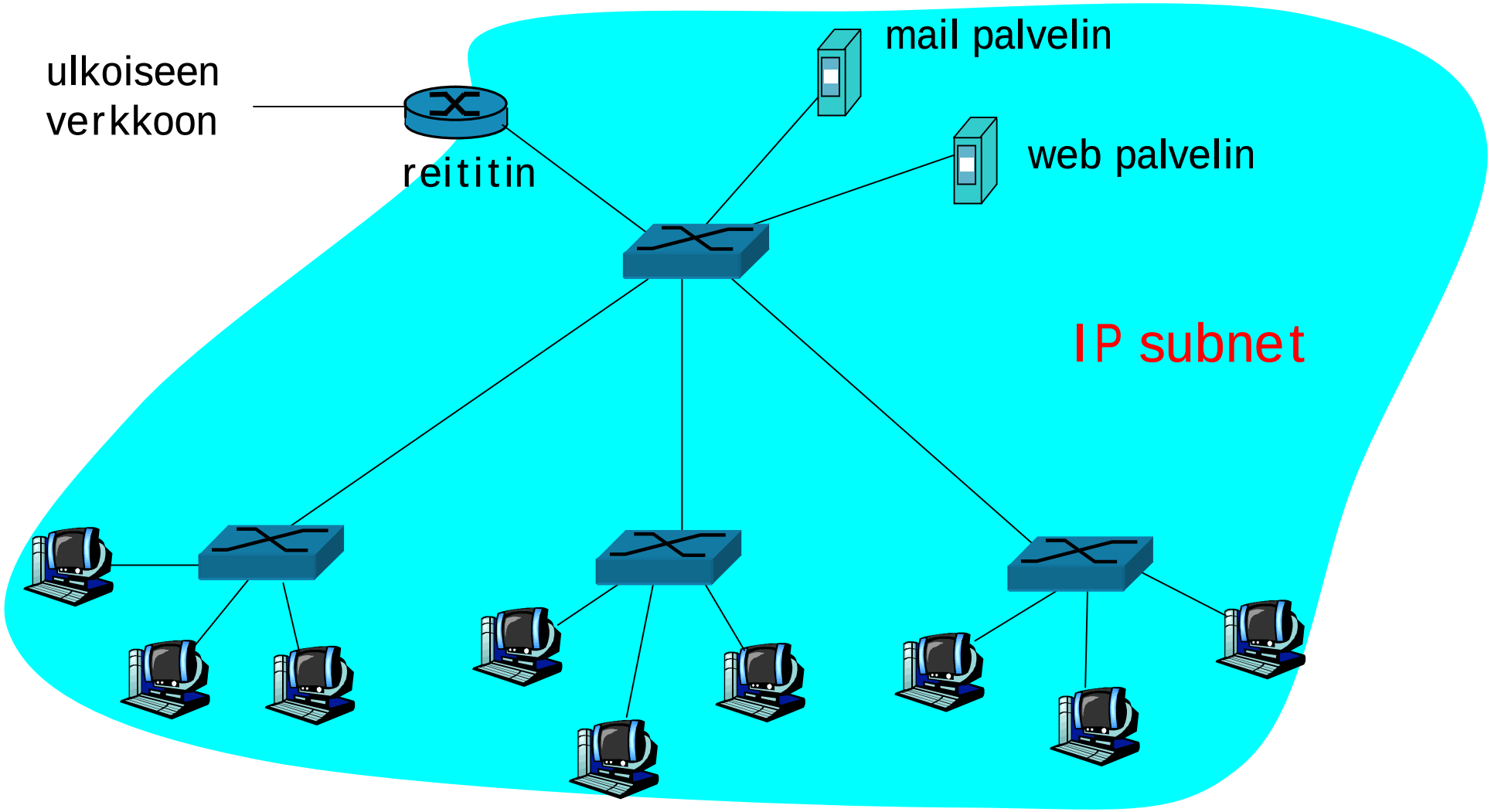


MAC osoite	liitäntä	TTL
A	*1*	*60*

kytkin taulu (Switch Table)

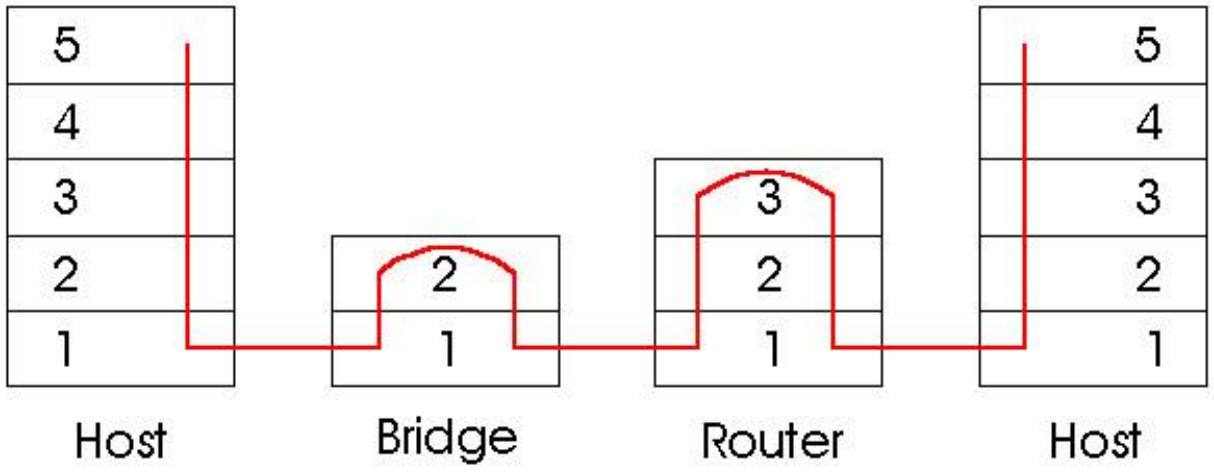
(alunperin tyhjä)

Institutionaalinen verkko



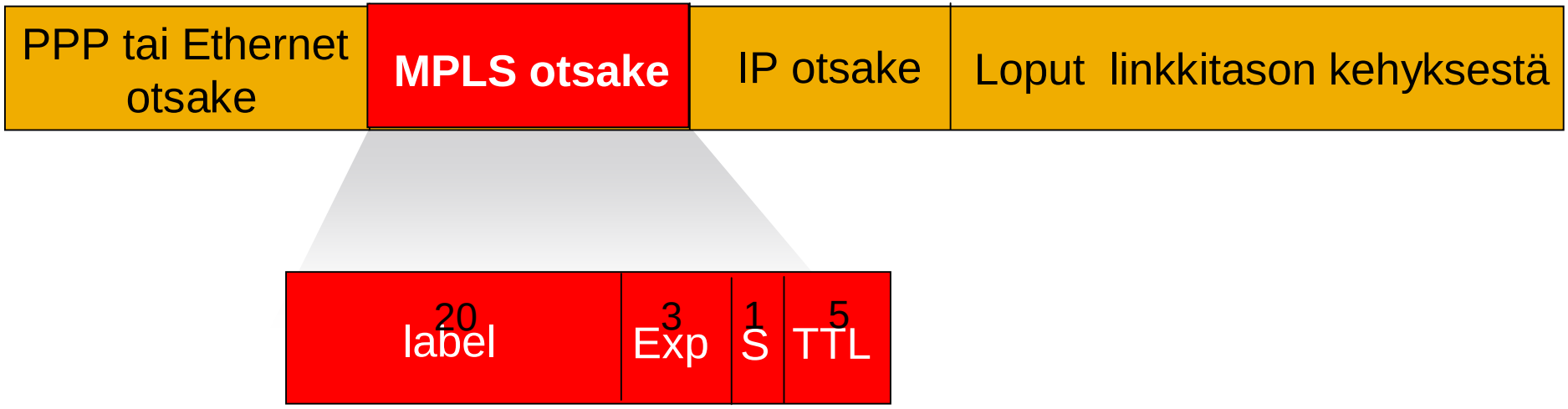
Kytkimet ja reitittimet, vertailu

- Molemmat varastoi-ja-välitä (store-and-foward) laitteita
  - reitittimet: verkkokerros laitteita (tutkivat verkkokerroksen otsakkeen/osoitteen)
  - Kytkimet ovat linkkikerros laitteita
- reitittimet ylläpitävät reititystaulua, toteuttaa reititys algoritmit
- kytkimet ylläpitävät kytkintaulu, toteuttaa suodatusta, oppivat algoritmit



Multiprotocol Label Switching (MPLS)

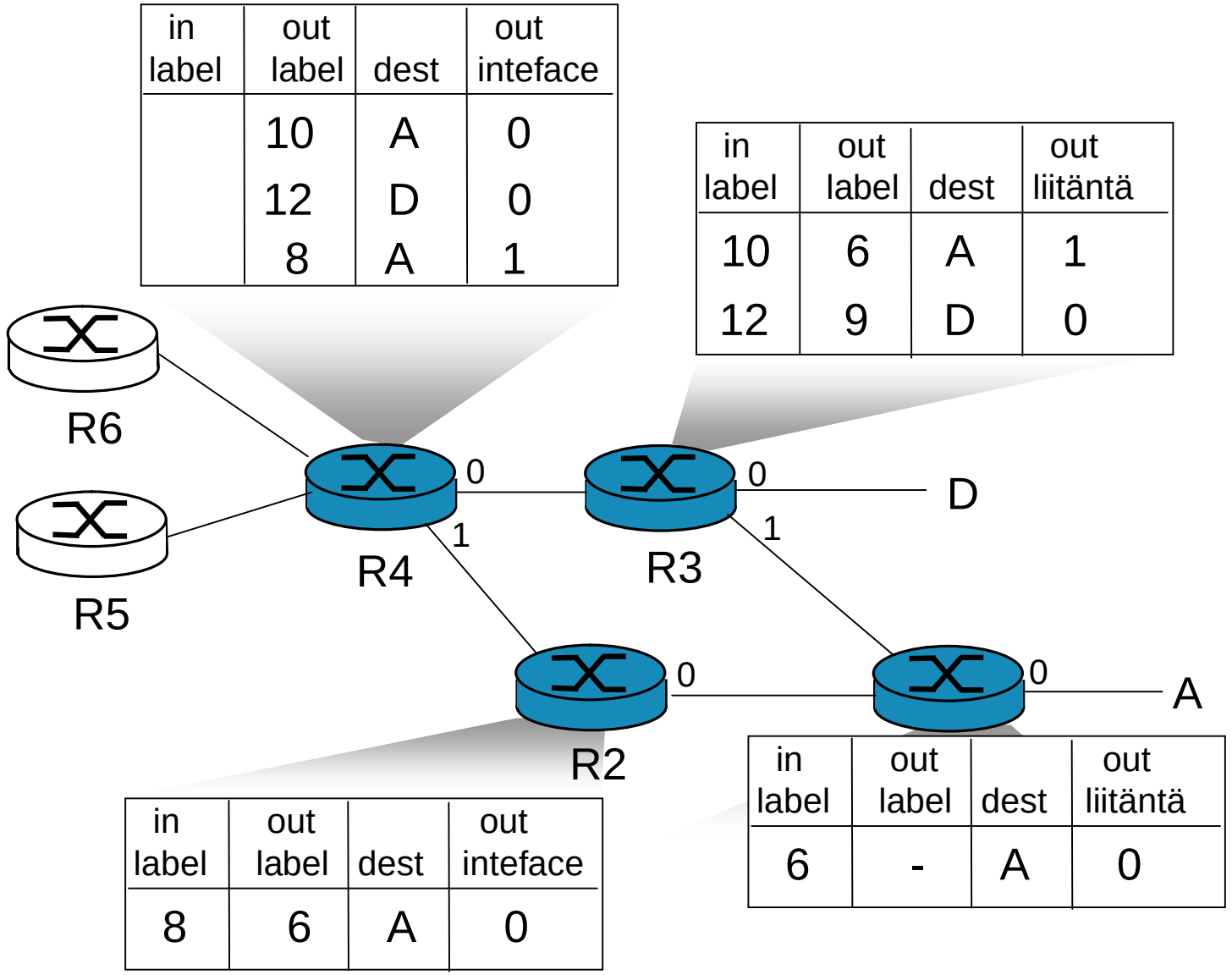
- Ideana: laitetaan IP-paketin alkuun pieni ”osoite” (label, tag). MPLS toiminnalla varustettu reititin katsoo vain leiman ja välittää paketin sen perusteella eteenpäin
- Tavoite: nopeus suurempi kuin IP välityksessä käyttämällä kiinteän pituuden pituus leimaa (label) IP osoitteen sijaan tekemään pakettien forwardointi
  - Lainaa ideoita Virtuaalipiiri (Virtual Circuit ,VC) ajatustavasta
  - Mutta IP datagrammi säilyttää silti IP osoitteen!



MPLS kykenevät reitittimet

- Eli: label-kytketty reititin
- Välittää paketit ulosmenevään liitäntään perustuen vain label arvoon (ei tutki IP osoitetta)
  - MPLS forwardointi taulu; erillinen IP forwardointi taulusta
- signalointiprotokolla tarvitaan asettamaan forwardointi
  - RSVP-TE
  - forwardointi mahdollista sellaisiakin polkuja pitkin joita IP yksin ei sallisi (esim., lähde-spesifinen reititys) !
  - MPLS:ää käytetään liikenteen suunnitteluun (traffic engineering)
  - Laajasti käytössä televerkoissa jo tänä päivänä (IP-core)

MPLS forwardointi taulu

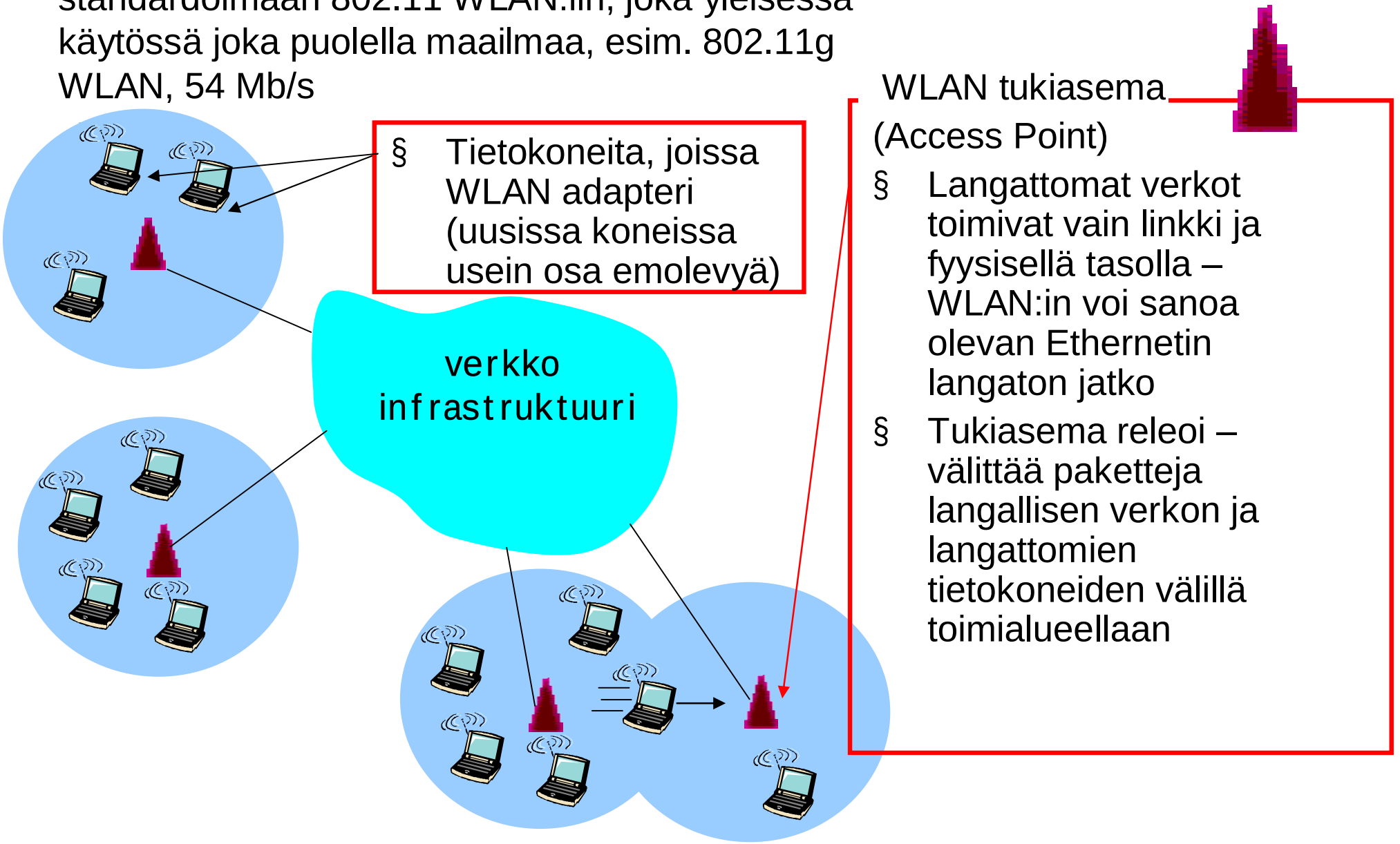


Langattomat Lähiverkot – Wireless LAN (WLAN) Linkkitason kannalta

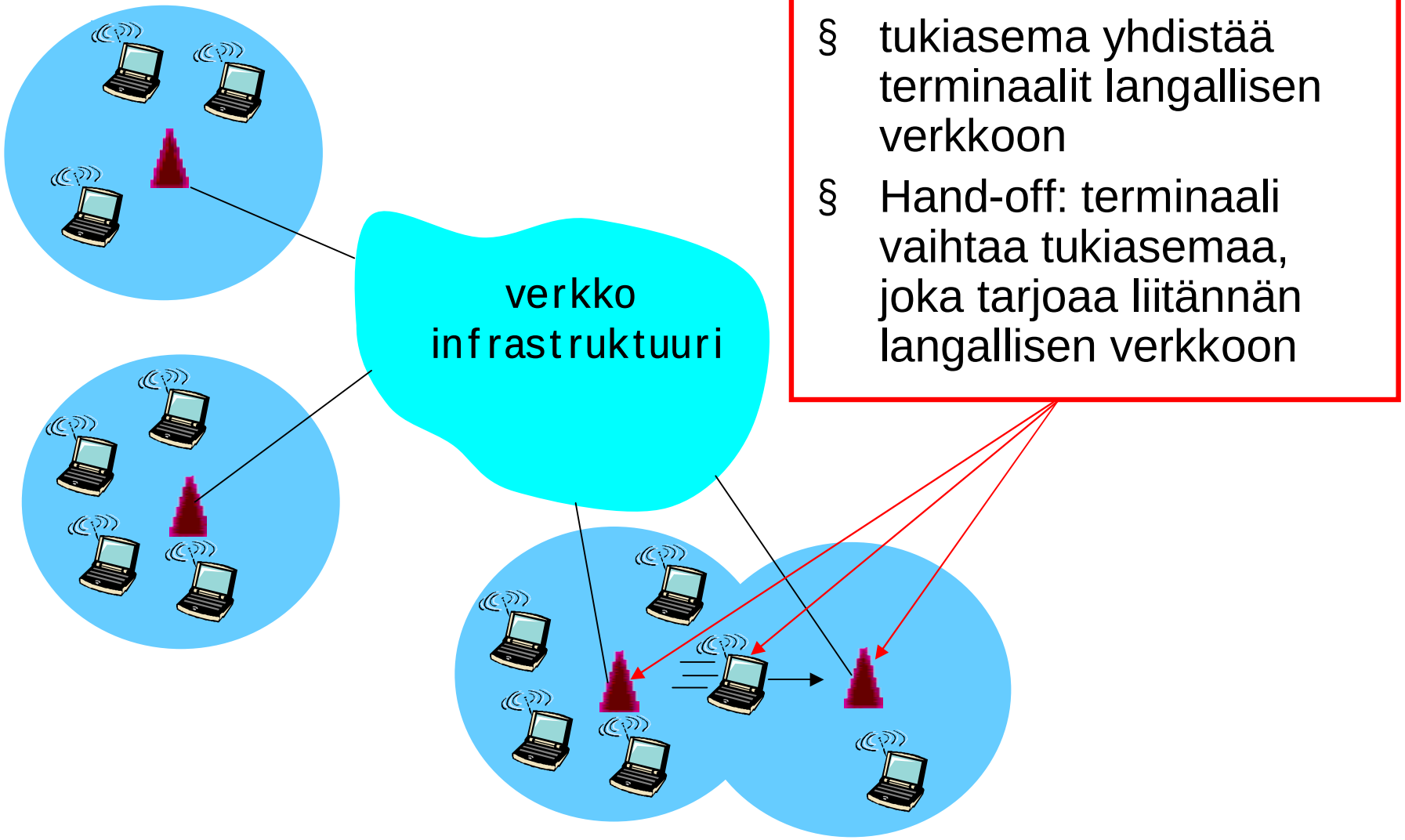
Kurose: Computer Networking, kappale 6

Langattoman verkon (WLAN) käsitteitä

Tässä esityksessä keskitytään vain IEEE:n standardoimaan 802.11 WLAN:iin, joka yleisessä käytössä joka puolella maailmaa, esim. 802.11g WLAN, 54 Mb/s



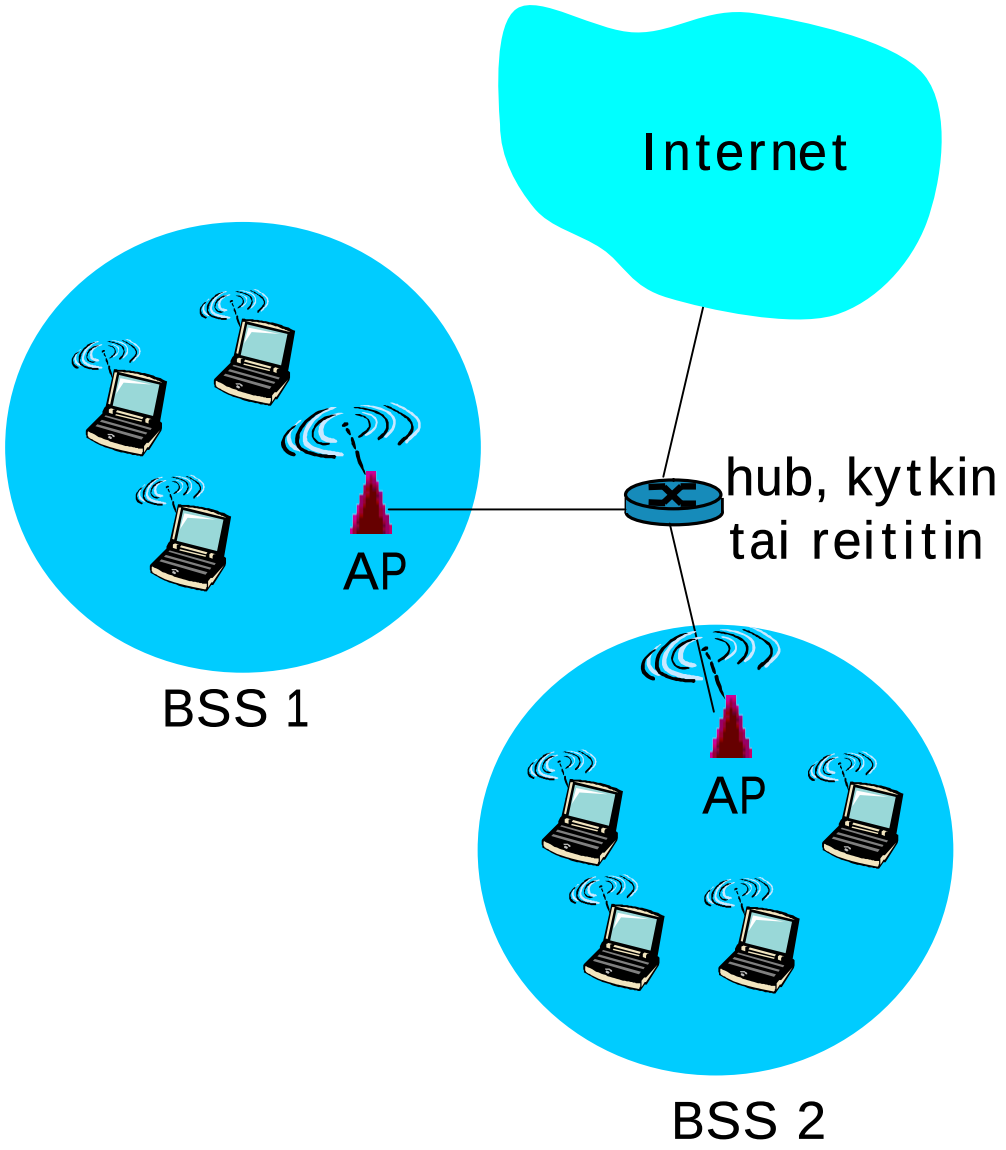
Langattoman verkon (WLAN) käsitteitä



infrastruktuuri moodi

- tukiasema yhdistää terminaalit langallisen verkkoon
- Hand-off: terminaali vaihtaa tukiasemaa, joka tarjoaa liitännän langallisen verkkoon

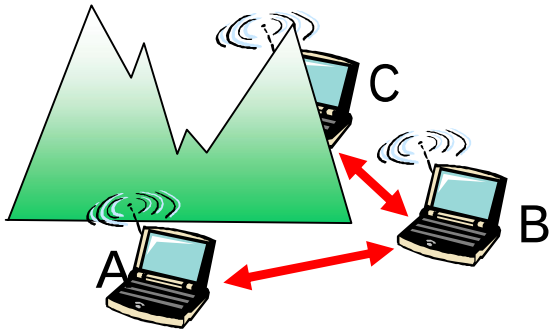
802.11 WLAN arkkitehtuuri (Infrastruktuuri verkko)

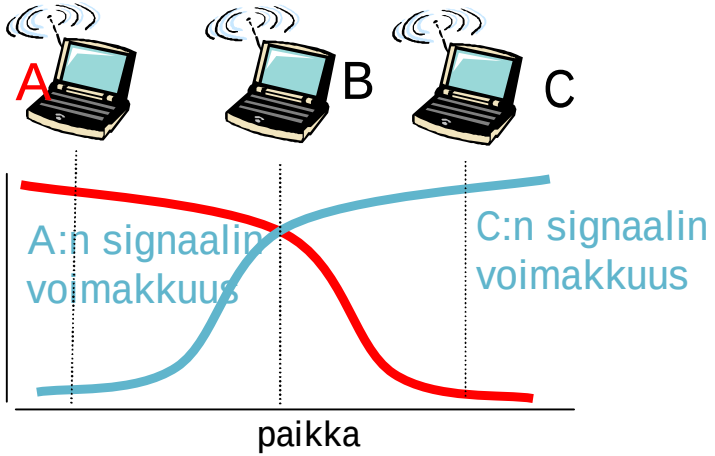


- Langaton laite kommunikoi tukiaseman kanssa: kaikki liikenne aina tukiaseman kautta
  - tukiasema = Access Point (AP)
- Basic Service Set (BSS) (eli “solu”) infrastruktuuri moodissa sisältää:
  - langattomia laitteita
  - tukiasemia (AP)
  - ad hoc moodi: vain tietokoneita, joka kommunikoivat suoraan keskenään
  - Extended Service Set (ESS), BSS:t liitetty toisiinsa jakelujärjestelmän kautta (Distribution System), käytännössä Ethernet

IEEE 802.11 WLAN: monipääsy

- Vältetään törmäyksiä (CA= Collision Avoidance): 2 asemaa lähettävät samaan aikaan
- 802.11: CSMA - havaitaan ennen lähetystä
  - ei törmätä meneillään olevaan transmissioon
    - 802.11: *ei* törmäyksen havaitsemista!
  - vastaanottajan on vaikea havaita törmäyksiä kun vastaanotettu signaali heikko (fading =häipymä)
  - kaikkia törmäyksiä ei havaita joka tapauksessa : piilotettu terminaali, fading eli tavoite: *vältetään törmäyksiä:* CSMA/C (collision Avoidance)





IEEE 802.11 MAC protokolla: CSMA/CA

802.11 lähettäjä

1 jos havaitaan vapaa kanava **DIFS:n ajan, lähetetään** koko kehys (ei CD)

2 jos havaita kanava varatuksi,

Asetetaan satunnainen odotus (backoff) aika (laskurille määrätty satunnaisluku)

Kun laskuri päässyt nollaan ja kanava vapaa voidaan lähettää

jos ei ACK, lisätään satunnainen backoff väliaika, toistetaan 2

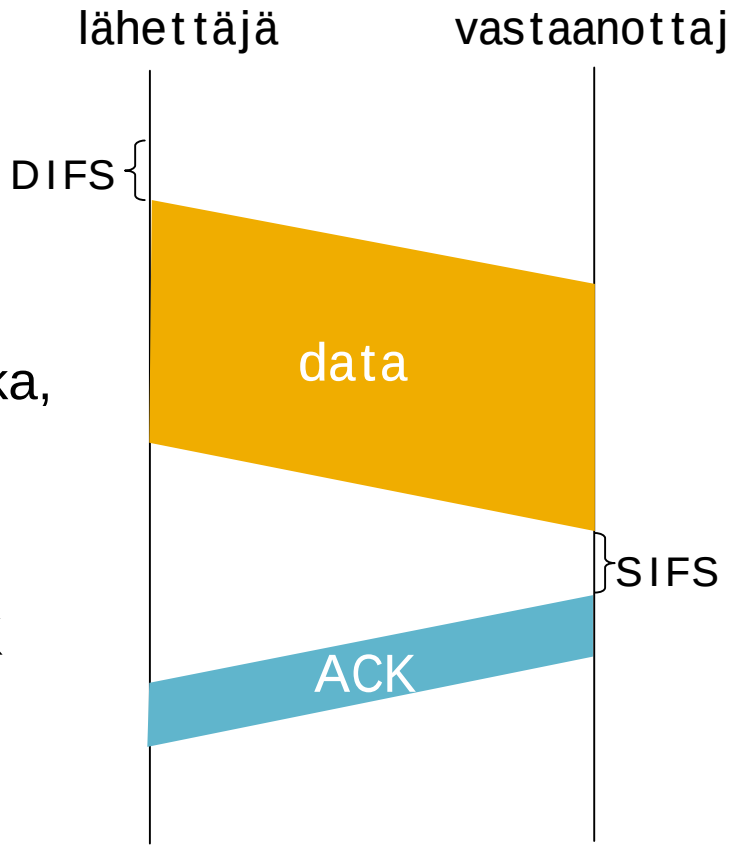
802.11 vastaanottaa

- jos kehys vastaanotetulle datalle OK

palautetaan ACK **SIFS odotusajan jälkeen** (ACK tarvitaan piilotetun terminaalin ongelman takia. SIFS <DIFS, jolloin lyhyet kuittaukset (ACK/NACK) saavat prioriteetin

DIFS = Data Interframe Spacing

SIFS = Short Interfarme Spacing



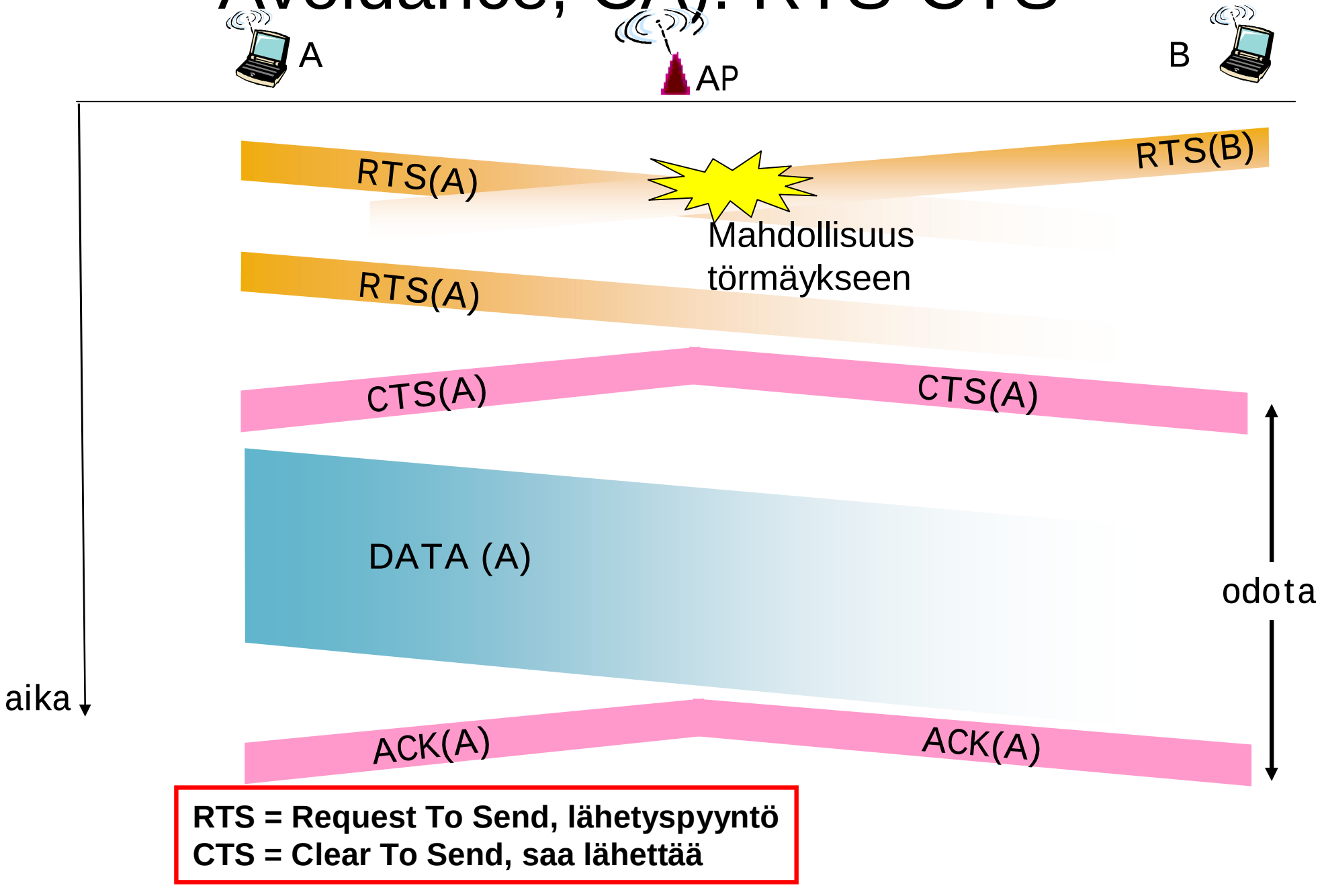
Törmäysten välttäminen (lisää)

idea: sallii lähettäjä “varata” kanava satunnaisen pääsyn sijasta: vältetään isojen datakehyksien törmäyksiä

- lähettäjä lähettää ensin pienen Request-To-Send (RTS) paketin tukiasemalle käyttäen normaalia kilpavaraustekniikka (CSMA)
  - RTS kehykset voivat silti törmätä jokaisen muun kehyksen kanssa (mutta RTS kehykset ovat lyhyitä, eli todennäköisyys pienehkö)
- Tukiasema lähettää Clear-To-Send CTS kehyksen vastauksena RTS:ään
- kaikki aseman kuulevat CTS signaalin (oletetaan, että tukiasema “keskellä”)
  - lähettäjä lähettää datakehyksen
  - Muut asemat viivästävät lähetyksiä

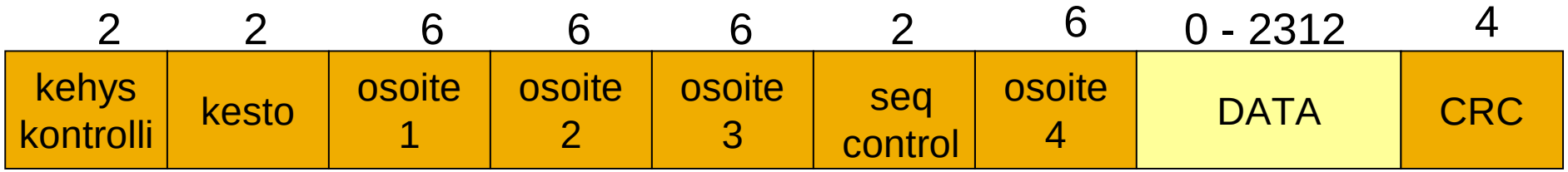
Vältetään datakehyksien törmäykset kokonaan käyttämällä pieniä varauspaketteja!

Törmäysten välttäminen (Collision Avoidance, CA): RTS-CTS



RTS = Request To Send, lähetyspyyntö
CTS = Clear To Send, saa lähettää

802.11: Kehys ja osoitteistus



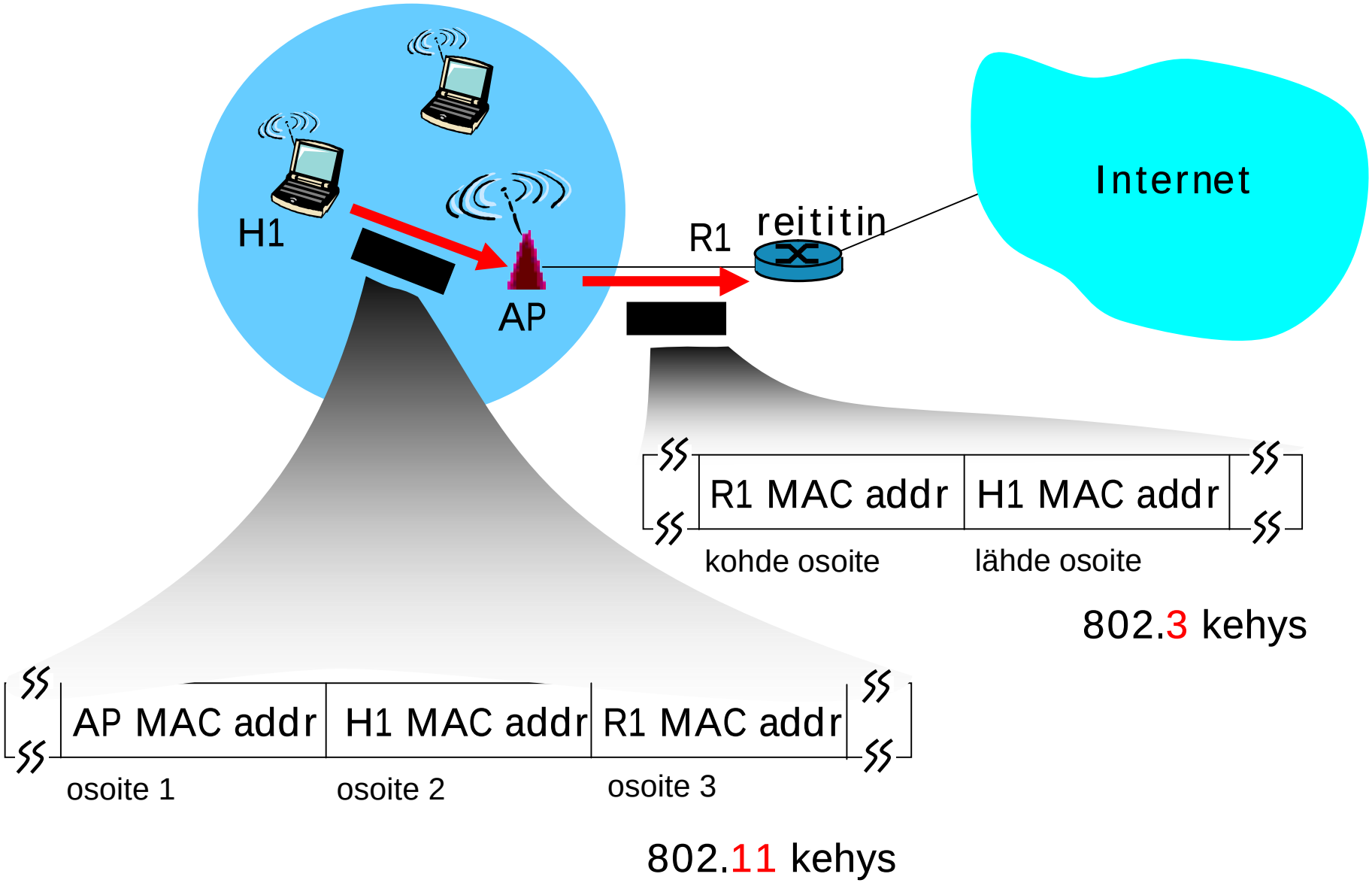
Osoite 1: Langattoman tietokoneen MAC osoite tai sen AP:n osoite, joka vastaanottaa kehyksen

Osoite 2: Langattoman tietokoneen MAC osoite tai kehyksen lähettävän AP:n MAC osoite

Osoite 3: MAC osoite reitittimelle, johon AP liitetty

Osoite 4: käytetään ad hoc moodissa (Ei AP:tä)

802.11: Kehys ja osoitteistus



Yhteenveto

- Periaatteet data linkki kerroksen palveluissa:
  - virheiden ilmaisu, korjaus
  - Jaettu (broadcast) kanava: monipääsy
  - linkki kerroksella oma osoitteistus
- Eri linkkikerros standardeilla omat toteutusteknologiat
  - Piirikytkentäiset järjestelmät
  - Ethernet
  - kytketyt LAN:it
  - Virtualisoitu verkko linkkikerroksena: MPLS
- Langattomissa verkoissa tarvitaan uusia menetelmiä törmäysten hallintaan: törmäysten välttämistä - CSMA/CA
- Virheiden havaitseminen ja korjaaminen tärkeää verkon liian kuormittumisen välttämiseksi. Langattomissa verkoissa erityisen tärkeää ja siellä käytössä hyvin kehittyneet virheenkorjaustekniikat.

Ensi luennolla

- Tiedonsiirron perusteita ja fyysinen kerros
  - Miten kehykset siirretään kaapeleissa, kuidussa ja radioaalloilla solmusta seuraavaan (linkkien väli) – pitkiäkin matkoja
- Signaalin (puheen) näytteenotto ja koodaus, 64 kb/s puhelinsignaali
- Kanavanjako / multipleksointi: Aikajako, taajuusjako, koodijako
- Siirron rajoitukset: Kohina, häiriöt radiotaajuuksien tai kaistan riittäminen
- Yhteys linkkikerroksen ja fyysisen kerroksen välillä
- 2 Megan tietoliikennesignaali, optinen siirto: PDH/SDH,WDM

Tenttikysymyksiä

- Miksi Ethernet-kaapelilla on maksimipituus?
- Miksi linkkikerroksen protokollissa on alku- ja loppumerkkejä?
- Miksi Ethernet:ille riittää törmäyksien tunnistaminen, mutta WLAN-verkossa on pyydettävä lupa lähettämiseen?