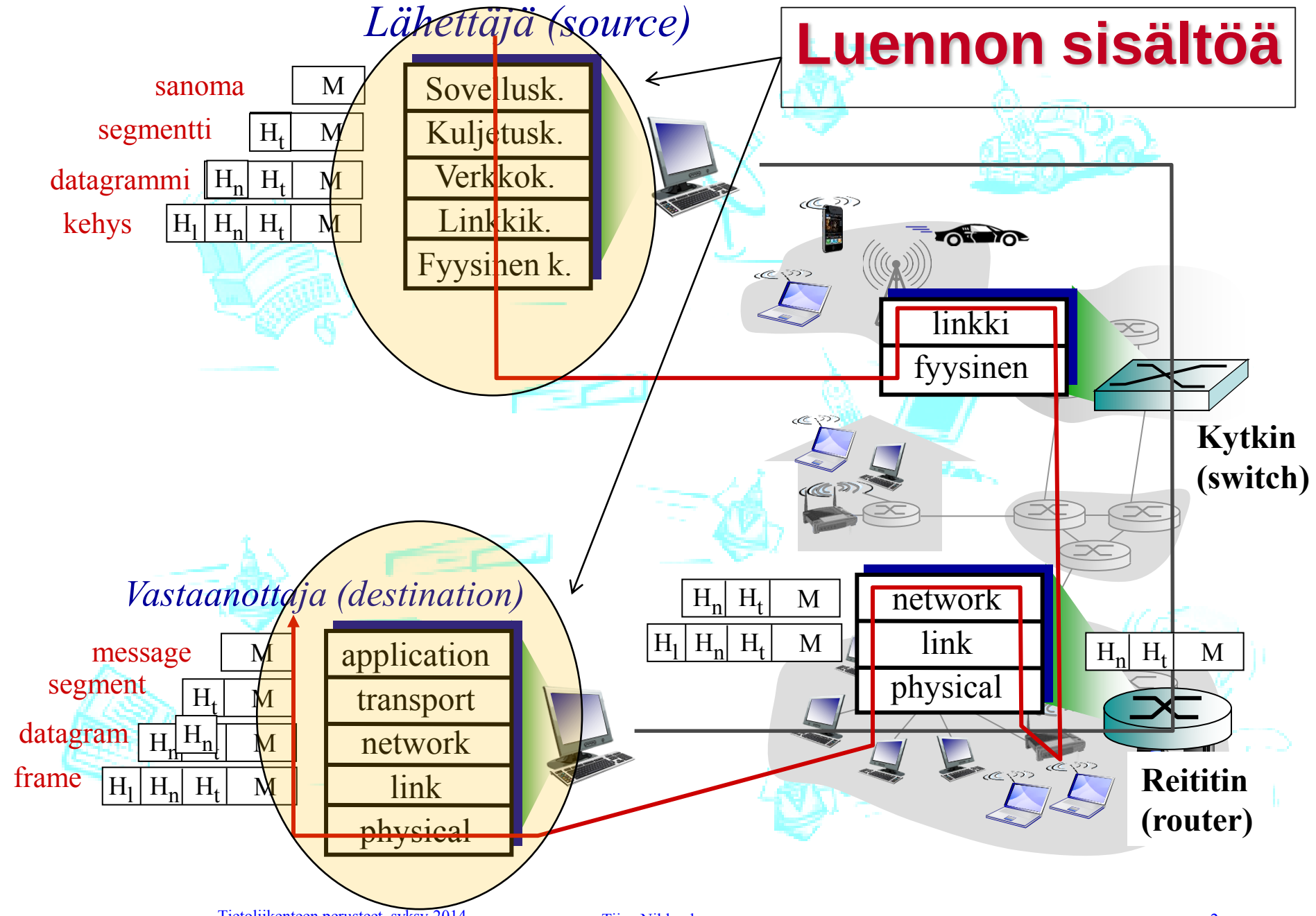
Tietoliikenteen perusteet

Luento 2

Syksy 2014, Tiina Niklander

Luennon sisältöä



Sisältöä

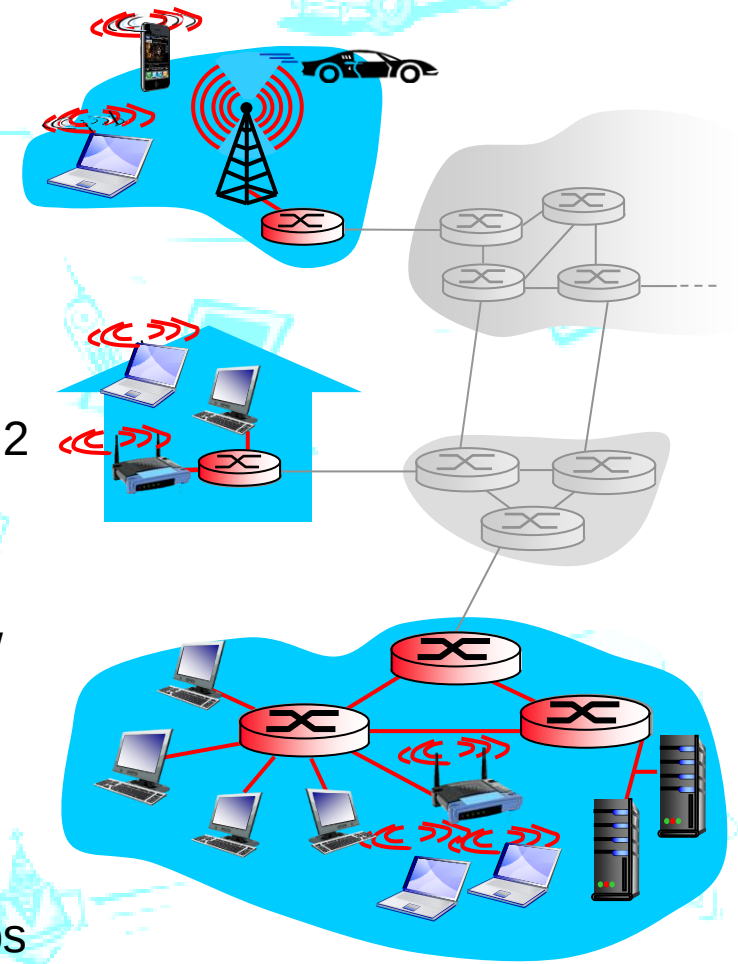
Oppimistavoitteet:
- Perusterminologia tutuksi
- Yleiskuva Internetistä
  - rakenne
  - toiminnallisuus
- Internetin protokollapino ja sen eri kerrosten tehtävät

- Internet
- Verkon reunalla:
  - asiakkaat ja palvelimet,
  - yhteydetön ja yhteydellinen palvelu
- **Pääsy Internetiin, fyysinen media**
- Verkon sisällä
  - Piirikytkentäinen, pakettikytkentäinen verkko
  - Datasähkeverkko, virtuaalipiiriverkko
- Viivytykset ja katoamiset siirrossa
  - Mitä viipeitä? Miksi dataa katoaa
- **Protokolla ja protokollapino**
- **Kerrosarkkitehtuuri**
- **Internet-protokollapino: kerrokset ja sanon**
- **Internetin rakenne**
- **Tietoturva: hyökkäyksiä**

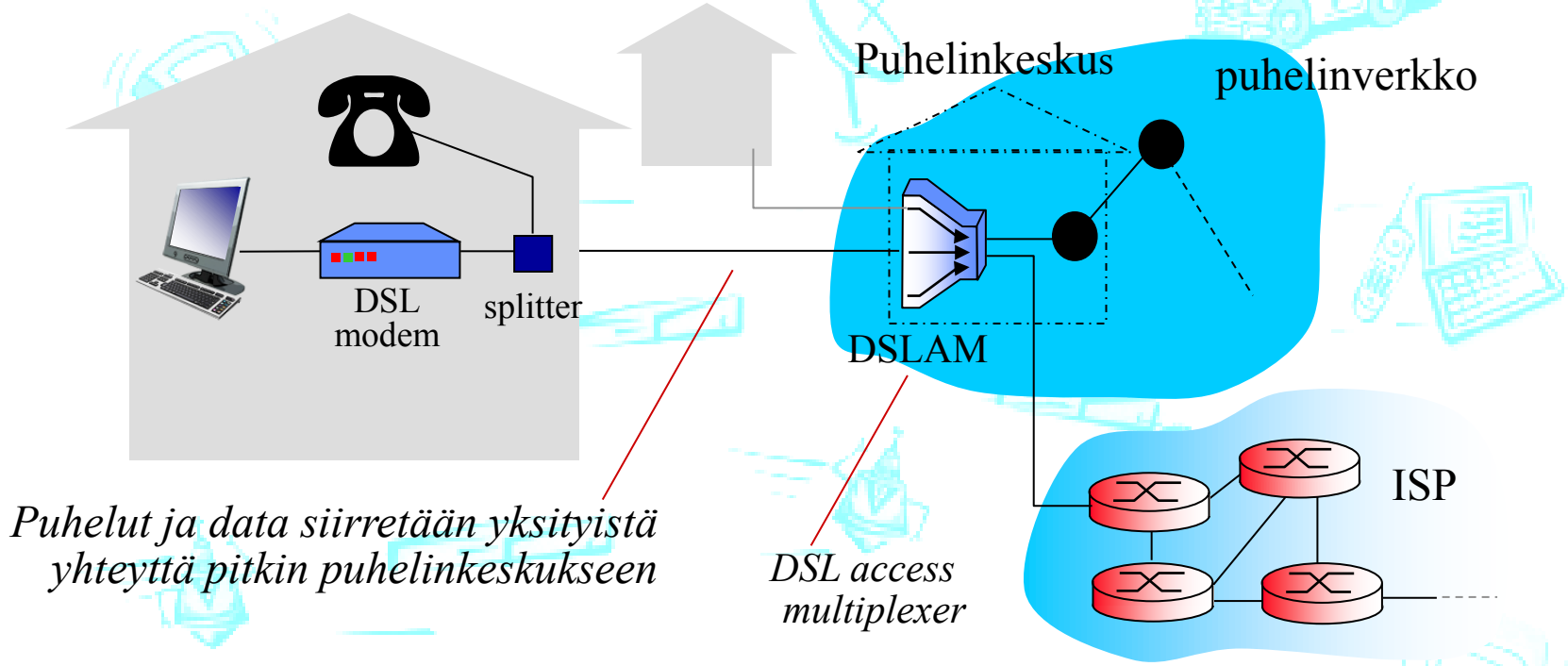
PÄÄSY INTERNETIIN

Pääsy internetiin ja fyysinen siirtotie

- DSL
  - ADSL (Asymmetric Digital Subscriber Link): 8/1 Mbps,
  - ADSL2+: 24/1.4 Mbps (teoreettinen)
  - SHDSL (Symmetric High-Bitrate Digital Subscriber Link): 44/44 Mbps
- Kaapelimodeemi
  - TV, yleislähetys, down ~ 30 Mbps, up ~ 2 Mbps, 100-110 Mbps
- Lähiverkko (Local Area Network)
  - Ethernet: 10 Mbps /100 Mbps / 1 Gbps / 10 Gbps / 100 Gbps
- Langaton yhteys
  - @450: 1 Mbps
  - WLAN (WiFi, WiMax): 11 Mbps, 54 Mbps
  - WAP/GPRS, 3G/UMTS: 384 kpbs- ~2 Mbps, LTE 50-100Mbp

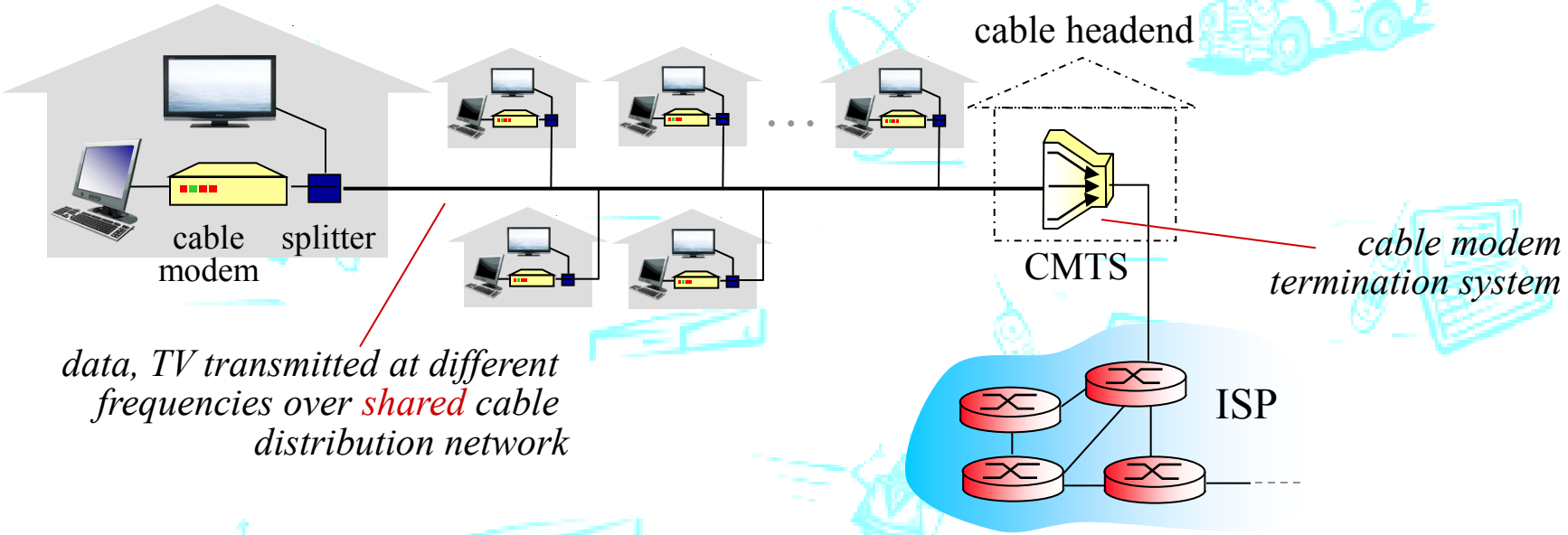


Puhelinverkko: digital subscriber line (DSL)



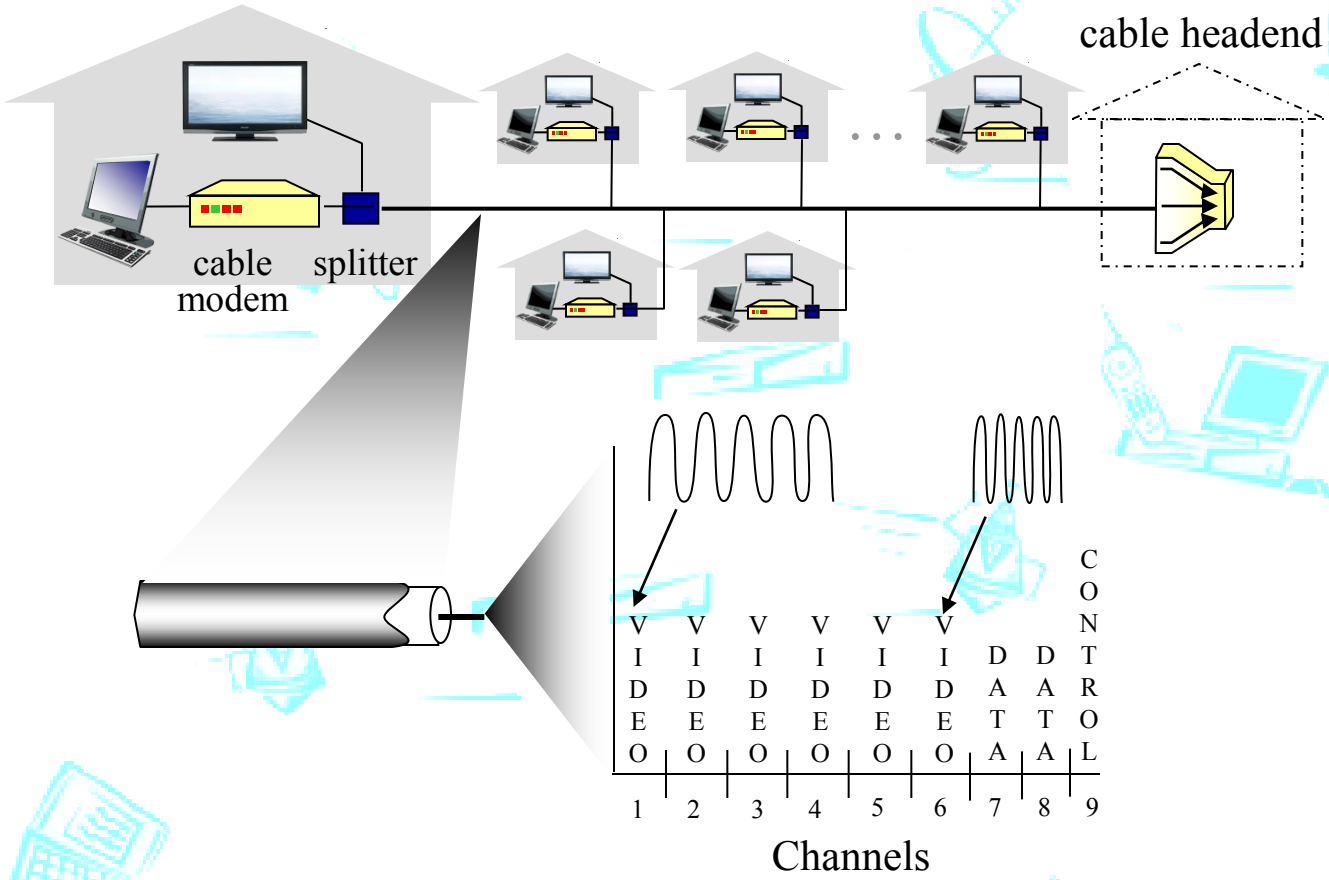
- Käyttää olemassaolevaa puhelinkaapelointia DSLAMille asti
  - data erotetaan ja ohjataan internetiin
  - Ääni erotetaan ja ohjataan puhelinverkkoon

Kaapelivekko



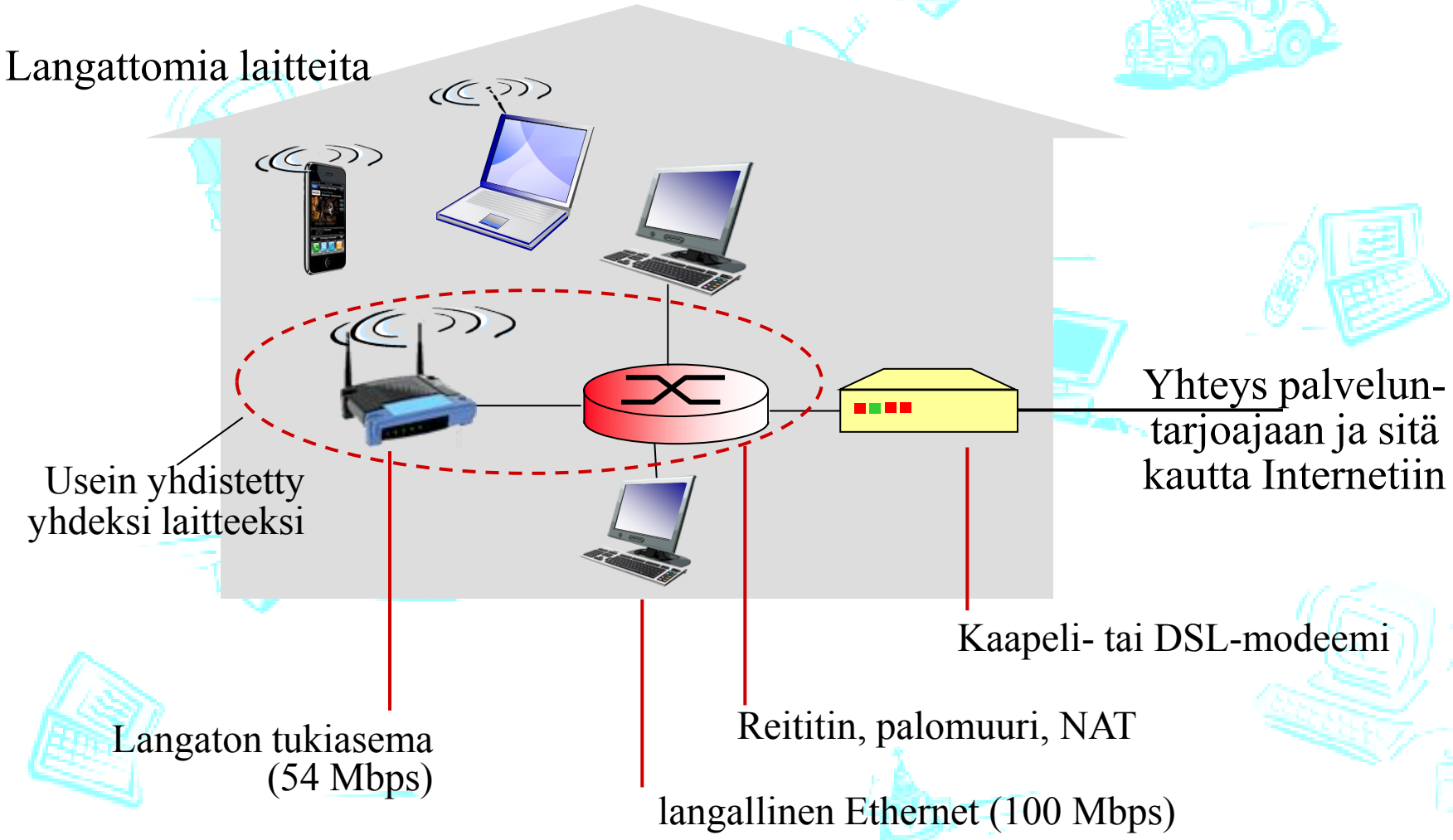
- Asymmetrinen ja jaettu yhteys
  - Yleensä koaksiaalikaapeli talojakamoon, jossa ISP:n reititin
  - Huoneistot jakavat saman kaapeliyhteyden toistensa ja TV-lähetysten kanssa

Kaapeliverkko

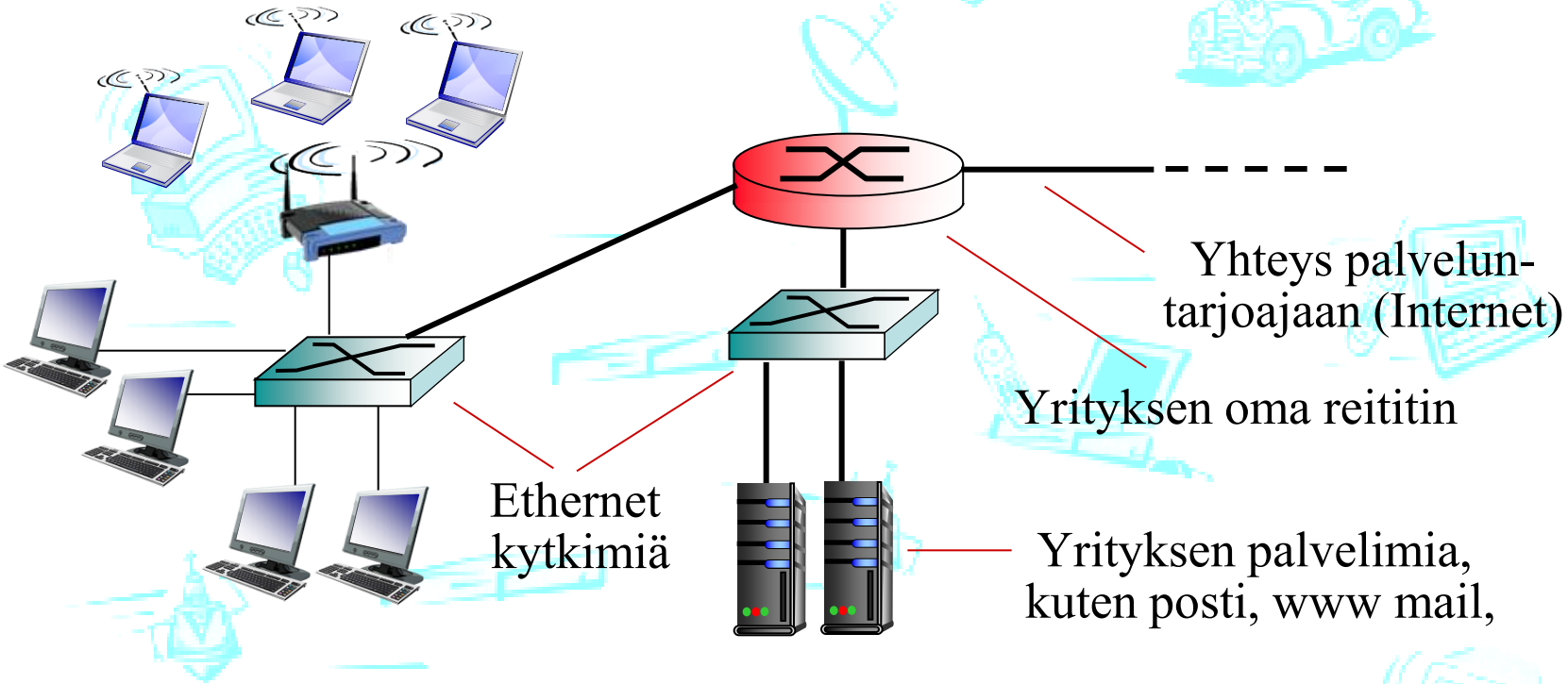


Taajuusalueet jaettu (frequency division multiplexing):
Eri kanavat siirretään eri taajuusalueilla

Kotiverkko (home network)



Yritysverkko (Ethernet)



- Tyypillinen yrityksissä, yliopistoissa, jne.
  - Siirtonopeudet10 Mbps, 100Mbps, 1Gbps, 10Gbps
  - Nykyään päätelaitteet suoraan kiinni ethernet-kytkimissä

Langaton verkko

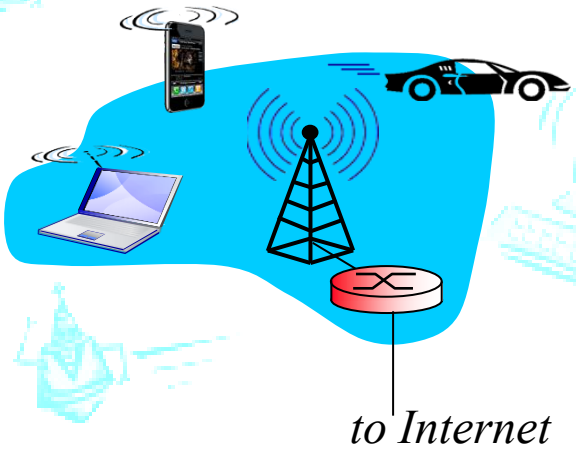
- Jaettu langaton verkko yhdistää päätelaitteet reitittimeen
  - Langaton yhteys tukiasemaan (base station, “access point”) asti

WLAN:

- Rakennuksen sisällä (10 m)
- 802.11a,g,n,ac (WiFi): 11,54,150 Mbps siirtonopeus

Mobiiliverkko:

- Teleoperaattorin tarjoama, 10’s km
- Siirtonopeus 1-50 Mbps
- 3G, 4G: LTE



Fyysinen media 1/3

- Bitti (bit): siirrettävä yksikkö lähetin/vastaanotin parin välillä
- Fyysinen linkki (physical link): yhtyes lähettimen ja vastaanottimen välillä
- Valvottu siirtotie (media):
  - Signaali siirretään kiinteän aineen välityksellä: kupari, kuitu, koaksiaali
- Avoin siirtotie:
  - Signaaali siirtyy vapaasti, kuten radio

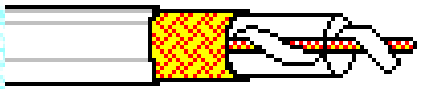
Parikaapeli (twisted pair, TP)

- Kaksi eristettyä kuparijohtoa
  - Category 5: 100 Mbps, 1 Gpbs Ethernet
  - Category 6: 10Gbps

Fyysinen media 2/3

Koaksiaalikaapeli (coaxial cable):

- kaksi sisäkkäistä kuparijohdinta
- kaksisuuntainen
- Laaja kaista:
  - useita kanavia samassa kaapelissa
  - HFC



Valokuitu (fiber optic cable):

- Lasinen kuitu johtaa valopulsseja, jokainen pulssi vastaa bittiä
- Nopea päästä-päähän yhteys
  - siirtonopeus10's-100's Gpbs
- Vähän siirtovirheitä
  - Toistimet (repeaters) kaukana toisistaan
  - Ei elektromagneettisia häiriöitä

Fyysinen media 3/3

Langaton:

- Signaali siirretään elektromagneettisella taajuudella/säteilyllä
- laaja näkymättömän valon spektri
- Ei fyysistä yhteyttä
- Kaksisuuntainen
- Ympäristön vaikutuksia:
  - heijastukset
  - estymiset (= ei kuulu)
  - Interferenssi

radiolinkkityyppejä:

- Maanpäällinen mikroaalto
  - jopa 45 Mbps kanavat
- LAN (e.g., WiFi)
  - 11Mbps, 54 Mbps
- mobiiliverkko
  - 3G cellular: ~ joitain Mbps
- satelliitti
  - 1 Kbps - 45Mbps kanava (tai useita hitaita kanavia)
  - 270 millisekunnin viive
  - Geostationaarinen vs. matalammalla maata kiertävä

PROTOKOLLAPINO

Protokollien kerrostaminen

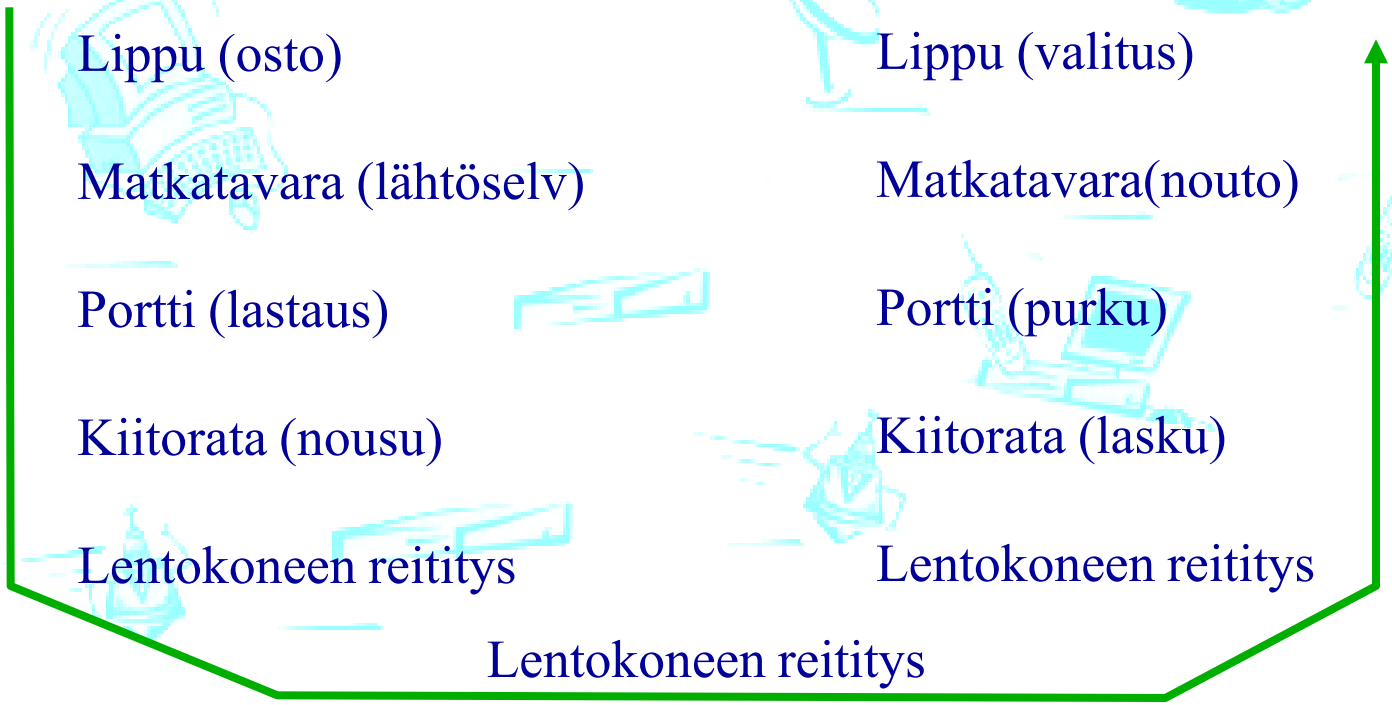
- Protokolla = yhteyskäytäntö
  - Mitä sanomia, missä tilanteessa ja missä järjestyksessä lähetetään
  - Miten saatuihin sanomiin reagoidaan
  - Sanomien syntaksi ja semantiikka
- Protokollapino = protokollien kerrosrakenne
  - Toiminnot on jaettu kerroksiin järkevästi
  - Alemman kerroksen toiminnot ovat ylemmän käytössä
  - Palvelu ja sen toteutus erotettu
- Kukin protokolla toimii yhdellä kerroksella ja toteuttaa tämän kerroksen jonkin palvelun

Miksi kerrosrakenne?

Monimutkaisuuden hallinta

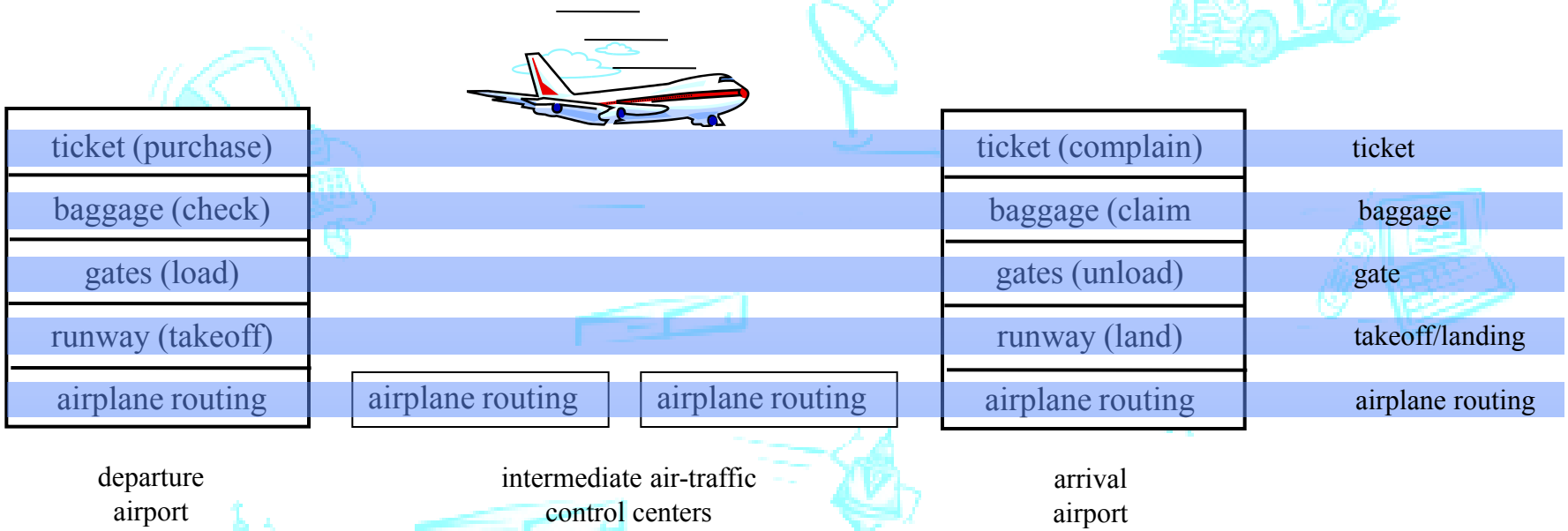
- Kerroksittainen viitemalli *(reference model)* helpottaa asiakokonaisuuksiin viittaamista
  - Kullakin kerroksella omat selkeät tehtävänsä
  - Kerroksissa omat ’lisä’toiminnot
- Voi käyttää olemassaolevia alemman kerroksen toimintoja
- Kerrosten rajapinnat *(interface)* hyvin määriteltyjä
  - Kaksisuuntainen ’palveluluukku’: mitä tekee, kuinka on käytettävissä
- Joustavuus
  - Pino koottavissa erilaisista protokollista
  - Kerroksen toteutusta voi muuttaa, kunhan rajapinnat ennallaan
- Jos kerroksia on paljon, se voi vaikuttaa suorituskykyyn
  - Sama työ toistamiseen,
  - esim. virhetarkistus
  - Kutsumekanismi: kopiointia paikasta toiseen, ..

Esimerkki: lentomatkustus



- Useita vaiheita, jotka tehtävä järjestyksessä

Lentoyhtiön toiminnan eri kerrokset

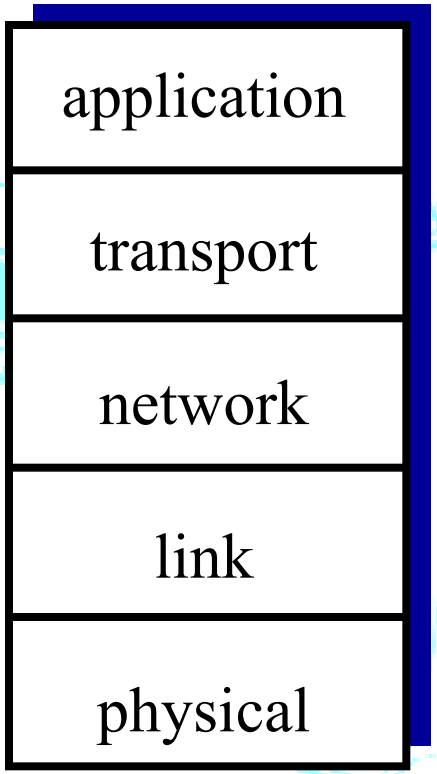


Kerrokset (layers): kukin kerros toteuttaa jonkin palvelun

- Oma palvelurajapinta ja sisäinen toiminta
- Käyttää alemman kerroksen palvelua oman toteuttamiseen
- Tarjoaa omaa palveluaan ylemmälle kerrokselle

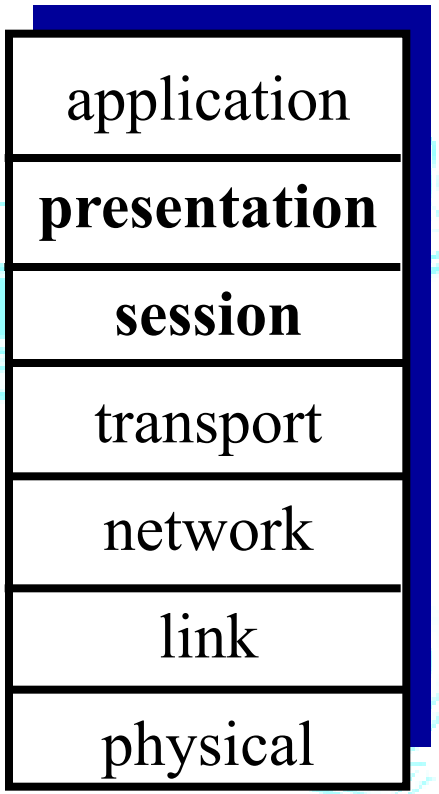
Internet-protokollapino

- *Sovellus:* verkkosovellusten omat protokollat
  - FTP, SMTP, HTTP, DNS,…
- *Kuljetus:* segmenttien siirto prosessilta toiselle (“päästä-päähän”)
  - TCP, UDP
- *Verkko:* pakettien reititys ja siirto verkossa lähettäjältä vastaanottajalle
  - IP, routing protocols
- *Linkki:* siirtää paketit kehyksinä kahden verkkolaitteen välillä
  - Ethernet, 802.111 (WiFi), PPP
- *Fyysinen:* generoi, siirtää ja vastaanottaa bittejä koneelta toiselle



ISO OSI -viitemalli

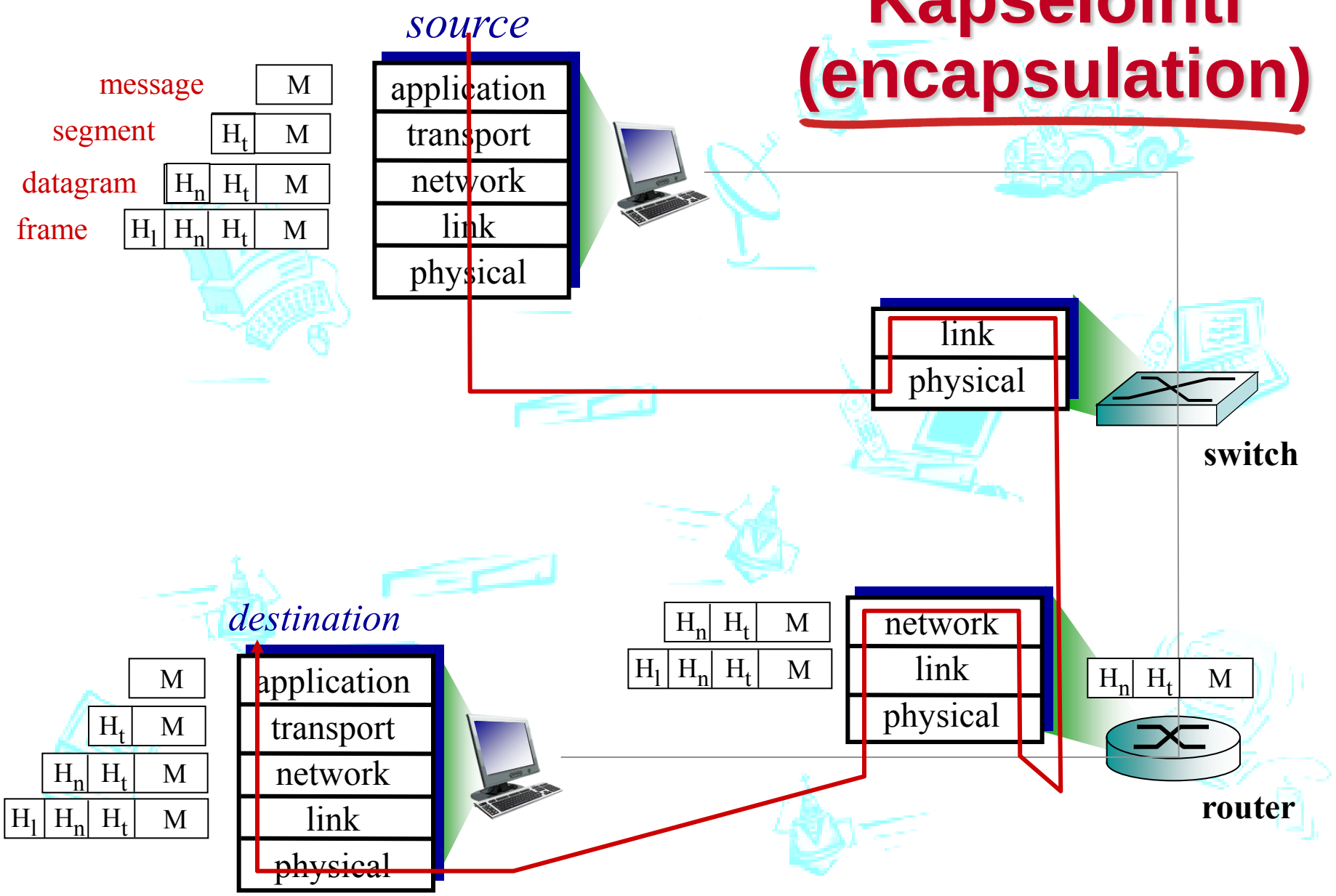
- 7-kerroksinen malli
  - ISO = International Standardization Organization
  - OSI = Open Systems Interconnection
  - yhdistää koneita, jotka ‘avoimia’ kommunikointiin toisten kanssa
- Käsitteellisesti ehjä malli,
  - 1978 -> 1982 viitemalli
  - 1983 -> toiminnallisia standardeja
  - 1995 uudistuksia
  - mutta ei paljoakaan käytössä
- Katoavaa kansanperinnettäkö? Vai vasta tulossa?



ISO OSI -viitemalli

- *Esitystapakerros (presentation):* data esitysmuodon tulkinta (erilainen esitystapa eri koneissa!), siirtosyntaksista sopiminen, salaus ja tiivistys haluttaessa
- *Istuntokerros (session):* kommunikointitavasta sopiminen, synkronointi, tahdistuspisteet ja toipuminen,
- Puuttuvat Internet-protokollapinosta
  - Toteutettava sovelluskerroksella joko sovelluksessa tai mieluummin väliohjelmistona (middleware)

Kapselointi (encapsulation)



TIETOTURVASTA

Verkon tietoturva

- Tietoturvan näkökulmia:
  - Kuinka tietokoneverkkoihin hyökätään
  - Kuinka voimme suojata verkkoja hyökkäyksiltä
  - Miten suunnitella arkkitehtuureja, jotka sietävät hyökkäyksiä
- Internetiä ei suunniteltu turvalliseksi
  - *Alkuperäinen idea:* “luotetaan muihin käyttäjiin, toiminnot läpinäkyviä ” ☺
  - Protokollien suunnittelijoiden täytyy nyt korjata asia
  - Tietoturva huomioitava kaikilla kerroksilla!

Porinatuokio

- Keskustelkaa pienissä ryhmissä (2-4 henkeä) verkon tietoturvasta 2-3 minuuttia

Millaisia uhkia/hyökkäyksiä tiedät tapahtuneet tai osaat arvella mahdollisiksi?

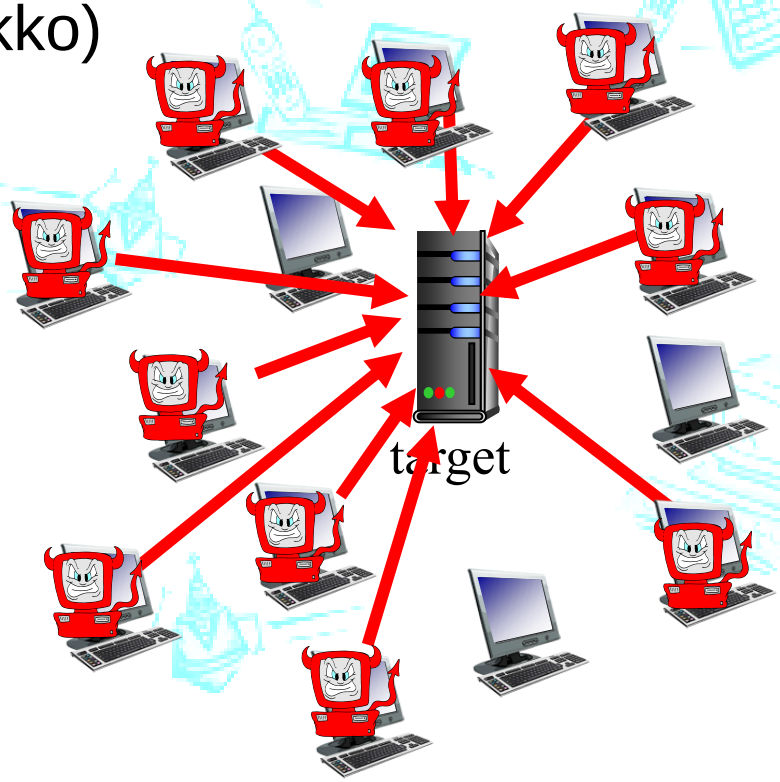
Haittaohjelmia (malware) tietokoneille Internetin välityksellä

- Haittaohjelma voi tulla usealla tavalla:
  - *virus:* itseään kopioiva ohjelma, joka (aktiivisesti) vastaanotetaan ja suoritetaan (esim. sähköpostin liite, verkosta ladattu koodi)
  - *mato (worm):* itseään kopioiva koodi, joka saadaan (passiivisesti) vastaanottamalla objekti, joka suoritetaan automaattisesti
- Vakoiluohjelmat (spyware) voivat tallentaa näppäinpainalluksia tai www-sivu historiaa ja kopioida/tallentaa nämä tiedon omaan palveluunsa Internetissä
- Saastuneita koneita (infected host) voidaan käyttää osana botnettiä lähettämään roskapostia tai osallistumaan DDoS hyökkäyksiin

Hyökkäys tiettyjä palvelimia tai aliverkkoja vastaan

Palvelunestohyökkäys (Denial of Service (DoS)):
hyökkääjät estävät laillisten käyttäjien käytön tuottamalla runsaasti ylimääräistä liikennettä

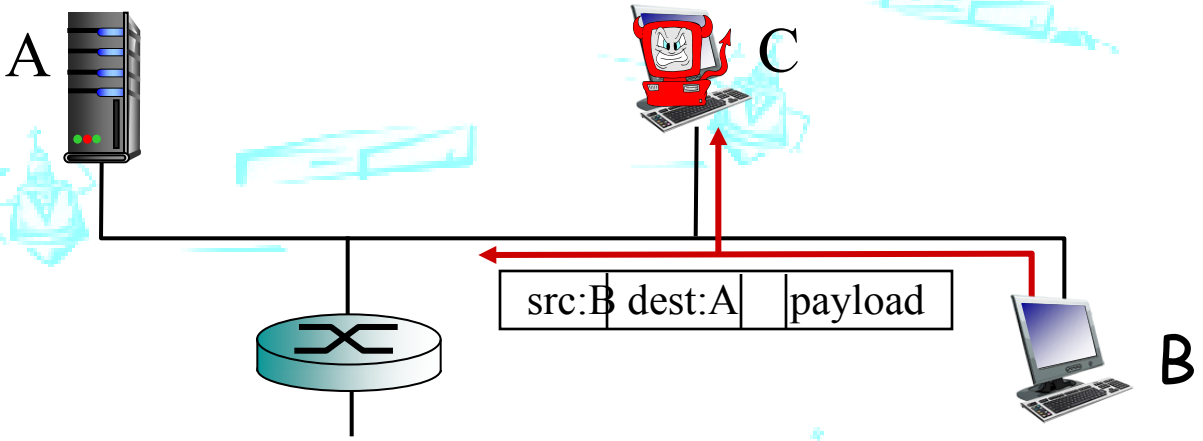
1. Valitse kohde (palvelin, verkko)
2. Rakenna botnet
   murtautumalla koneille eripuolilla verkkoa
3. Laita murretut koneet
   lähettämään paketteja kohteelle



Pakettien kuuntelu (sniffing)

Pakettien kuuntelu:

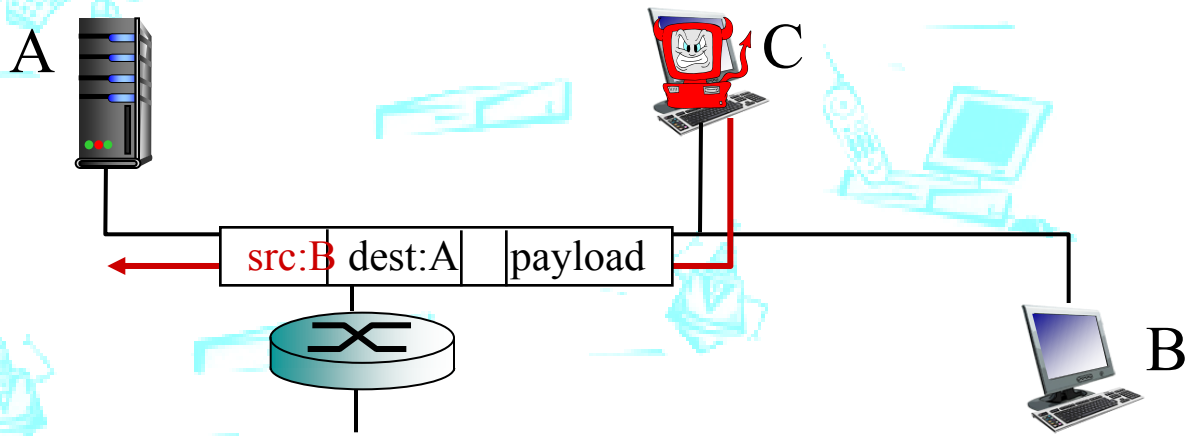
- Yleislähetys kanava (kuten jaettu ethernet, langaton yhteys) – liikenne on kaikkien kuultavissa
- Verkkorajapinta ei valikoi paketteja (ns. promiscuous mode), vaan poimii kaikki kuulemansa paketit (esim. sanasanoja)



- **wireshark** on ilmaisohjelma pakettien kuunteluun (kaappaamiseen)

Osoitteen väärentäminen (fake address)

IP spoofing: lähetä paketti, jossa väärä lähettäjän osoite



… paljon muutakin tietoturva-asiaa
pitkin kurssia, erityisesti luennot 11&12 (kirjan luku 8)

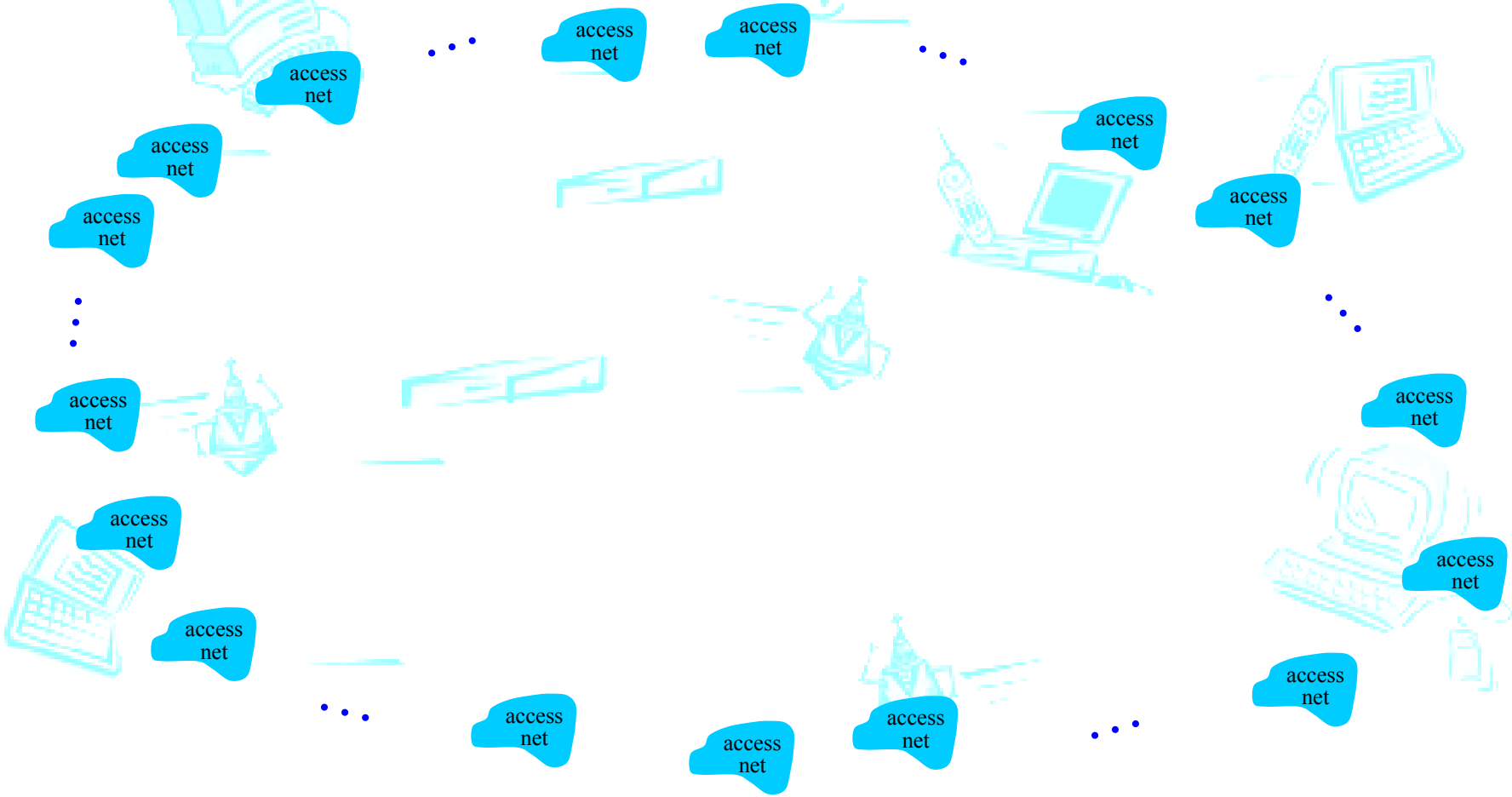
INTERNETIN RAKENNE

Internetin rakenne: Verkkojen verkko

- Päätelaite on kytketty palveluntarjoajan (Internet Service Provider, ISP) verkon kautta Internetiin
  - engl. access network
- Palveluntarjoajien verkot on kytketty edelleen toisiinsa.
  - Näin kaksi Internetiin kytkettyä laitetta voi lähettää paketteja toisilleen
- Tällainen verkkojen verkko on monimutkainen
  - Taustalla sekä talous että kansalliset politiikat
- Tarkastellaan rakennettu pala palalta

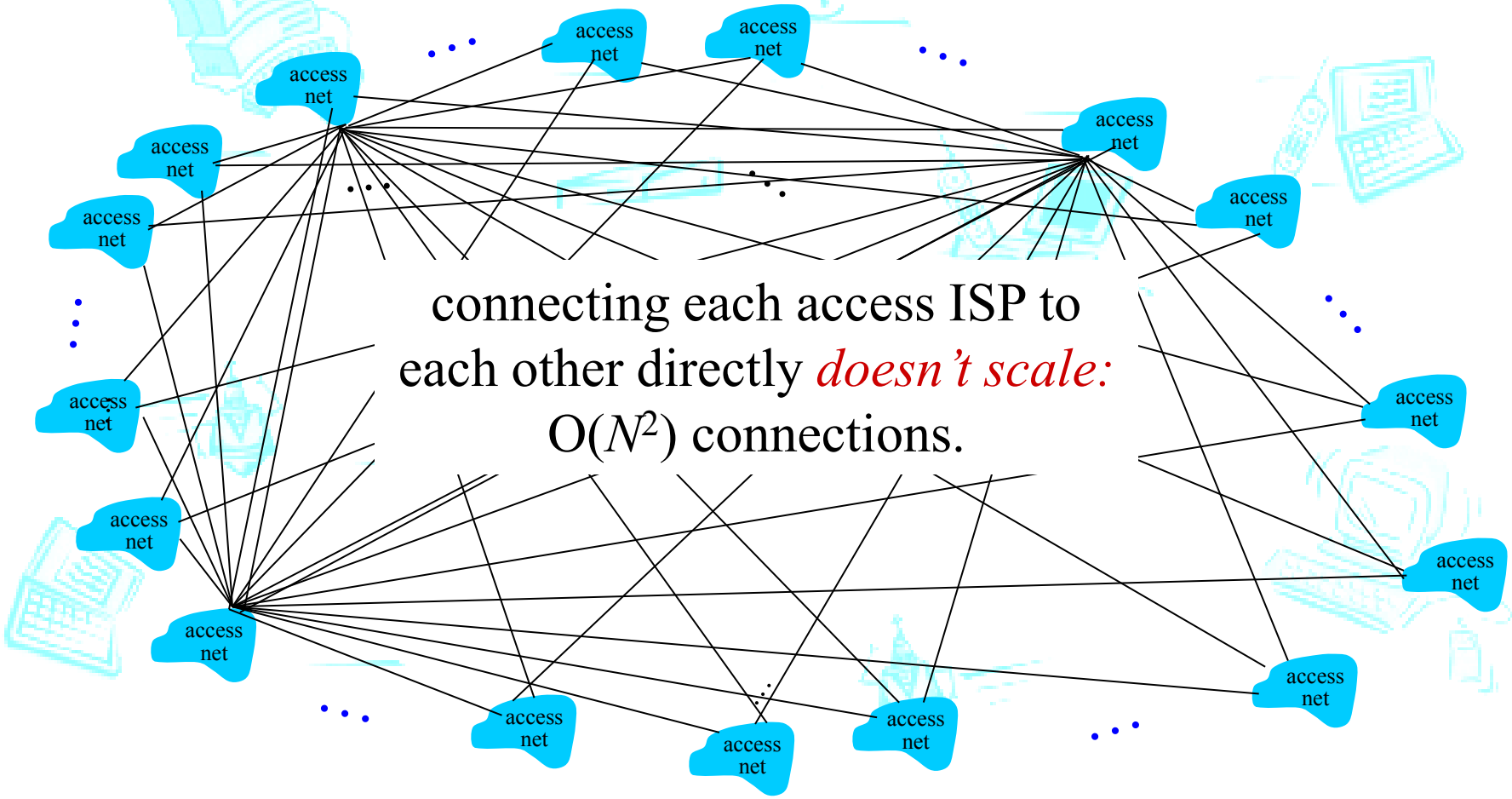
Internetin rakenne: Verkkojen verkko

Ongelma: Miten miljoonat palveluntarjoajien verkot yhdistetään?



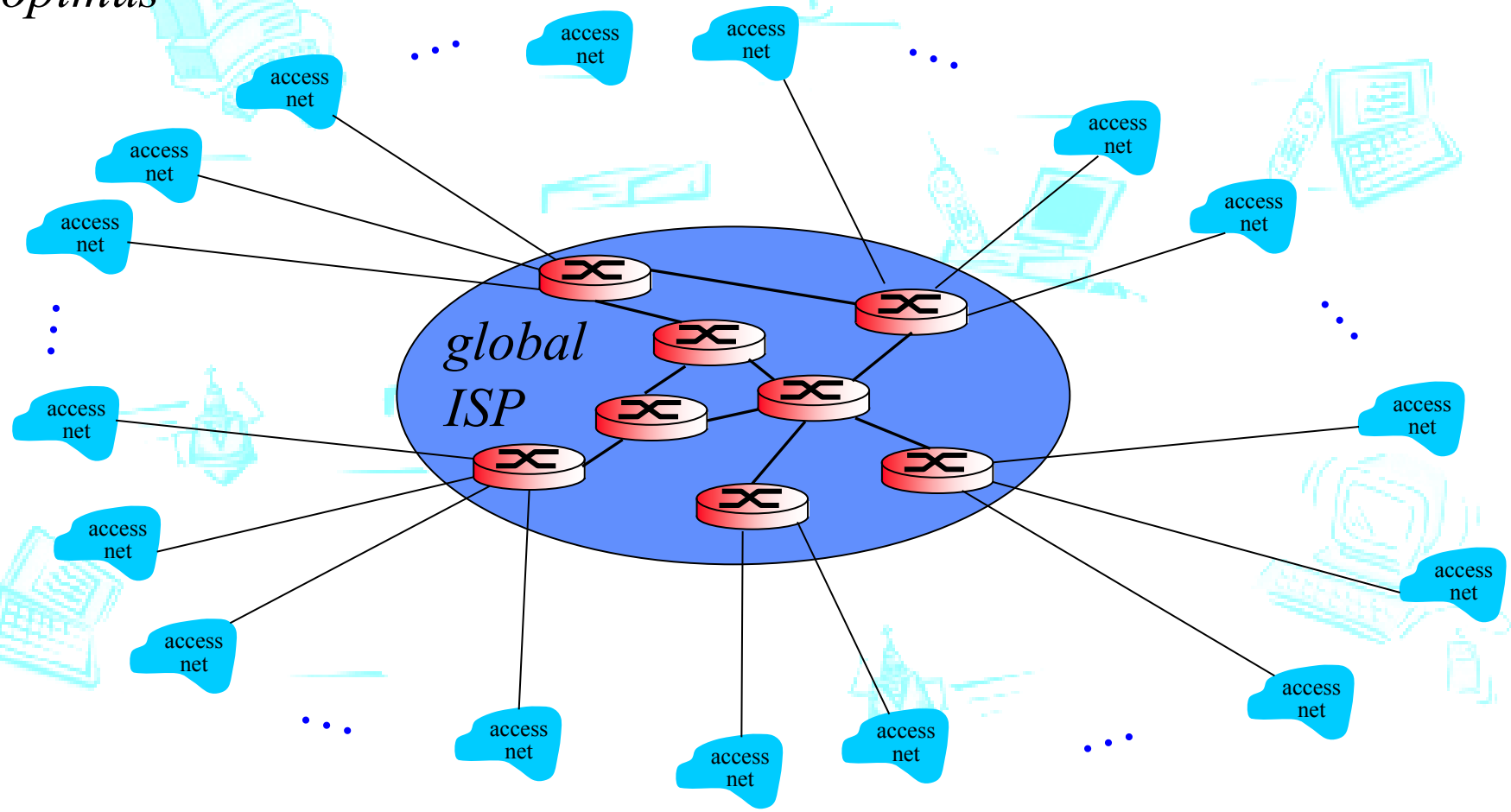
Internetin rakenne: Verkkojen verkko

Vaihtoehto: Yhdistetään jokainen ISP suoraan kaikkiin muihin?



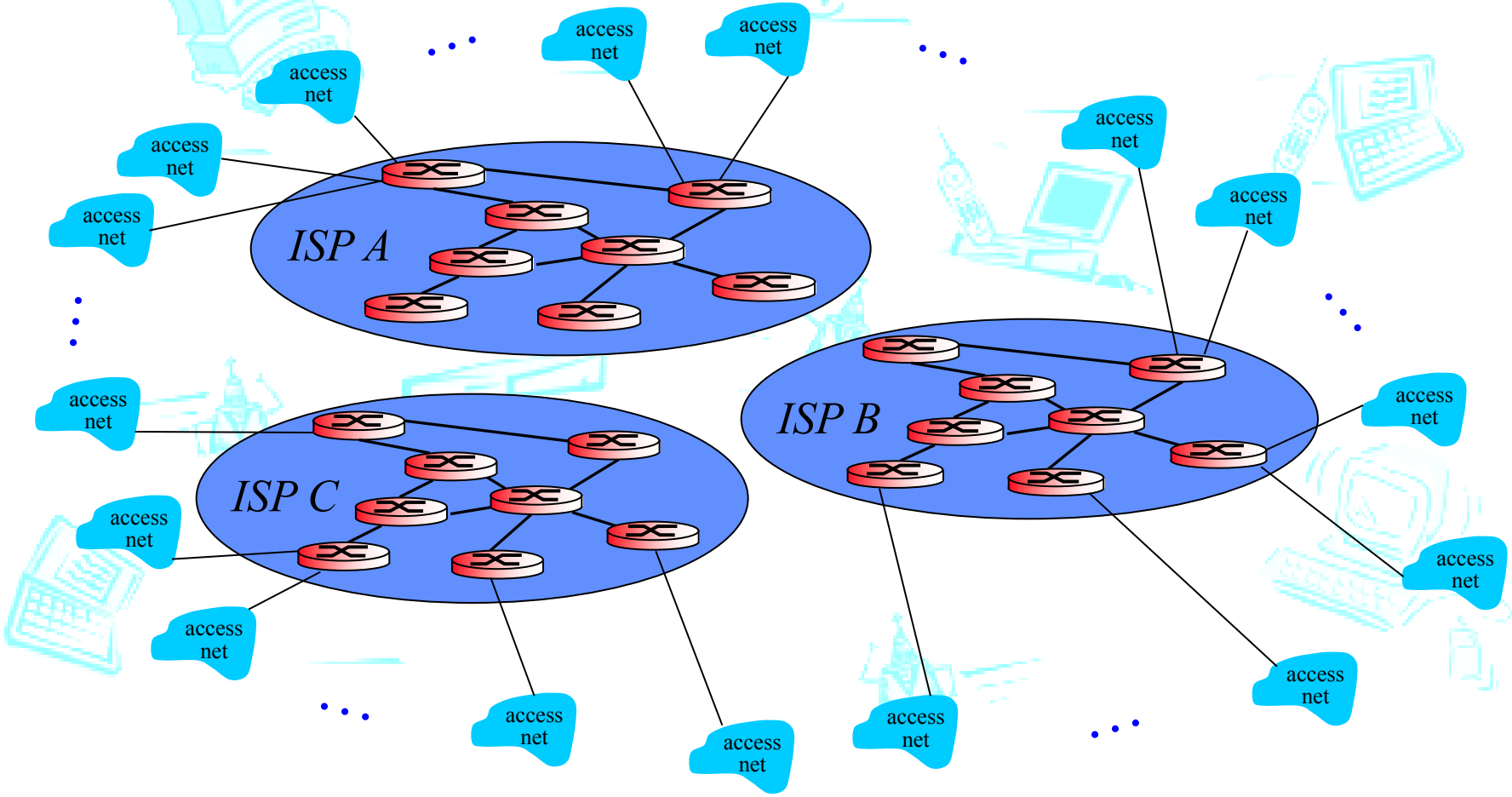
Internetin rakenne: Verkkojen verkko

Vaihtoehto: yhdistetään kaikki yhteen keskitettyyn välitys-verkkoon (globaali ISP)? Asiakkailla ja palvelun tarjoajalla sopimus



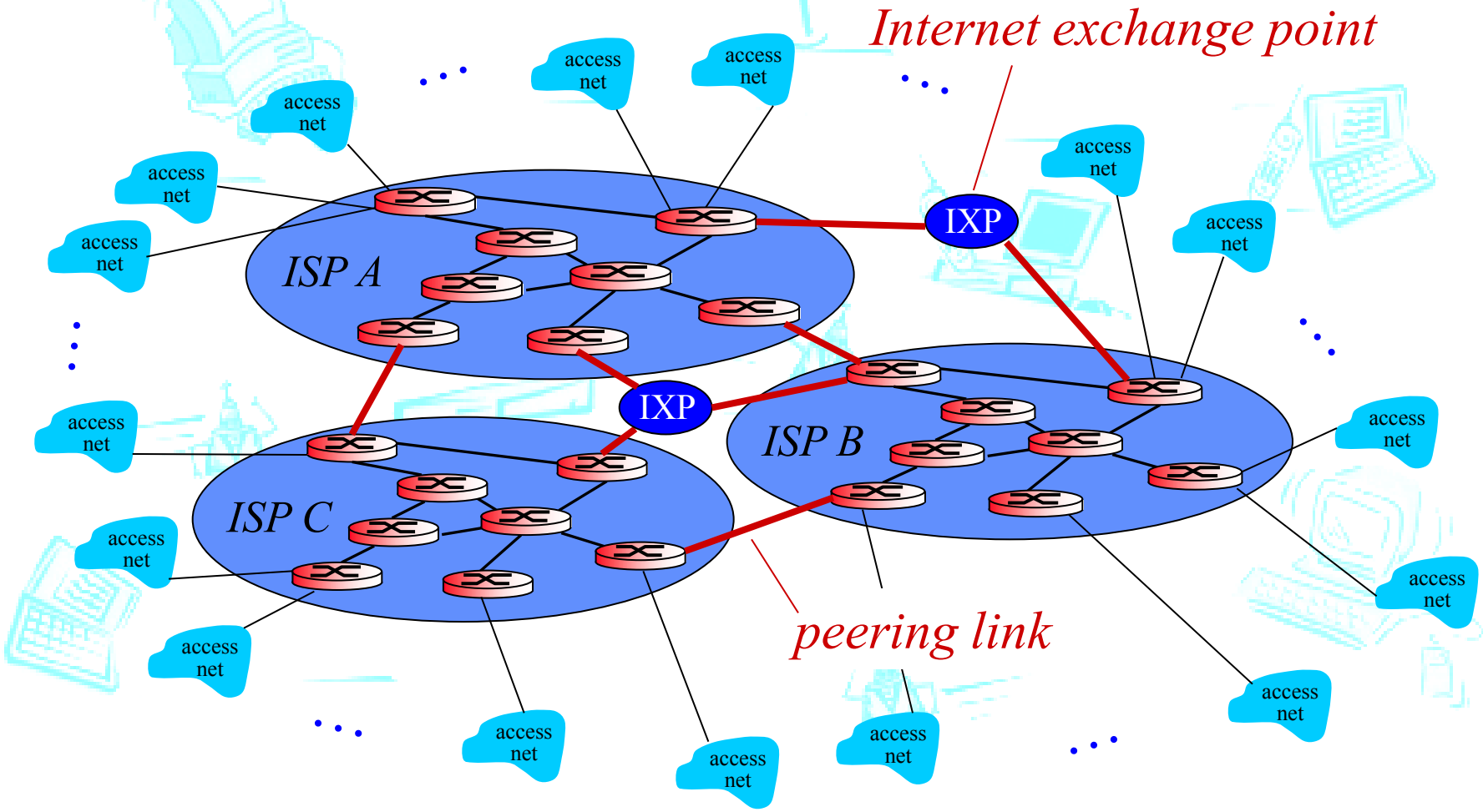
Internetin rakenne: Verkkojen verkko

Mutta: jos välitysverkko tuottaa voittoa, tulee kilpailijoita ….



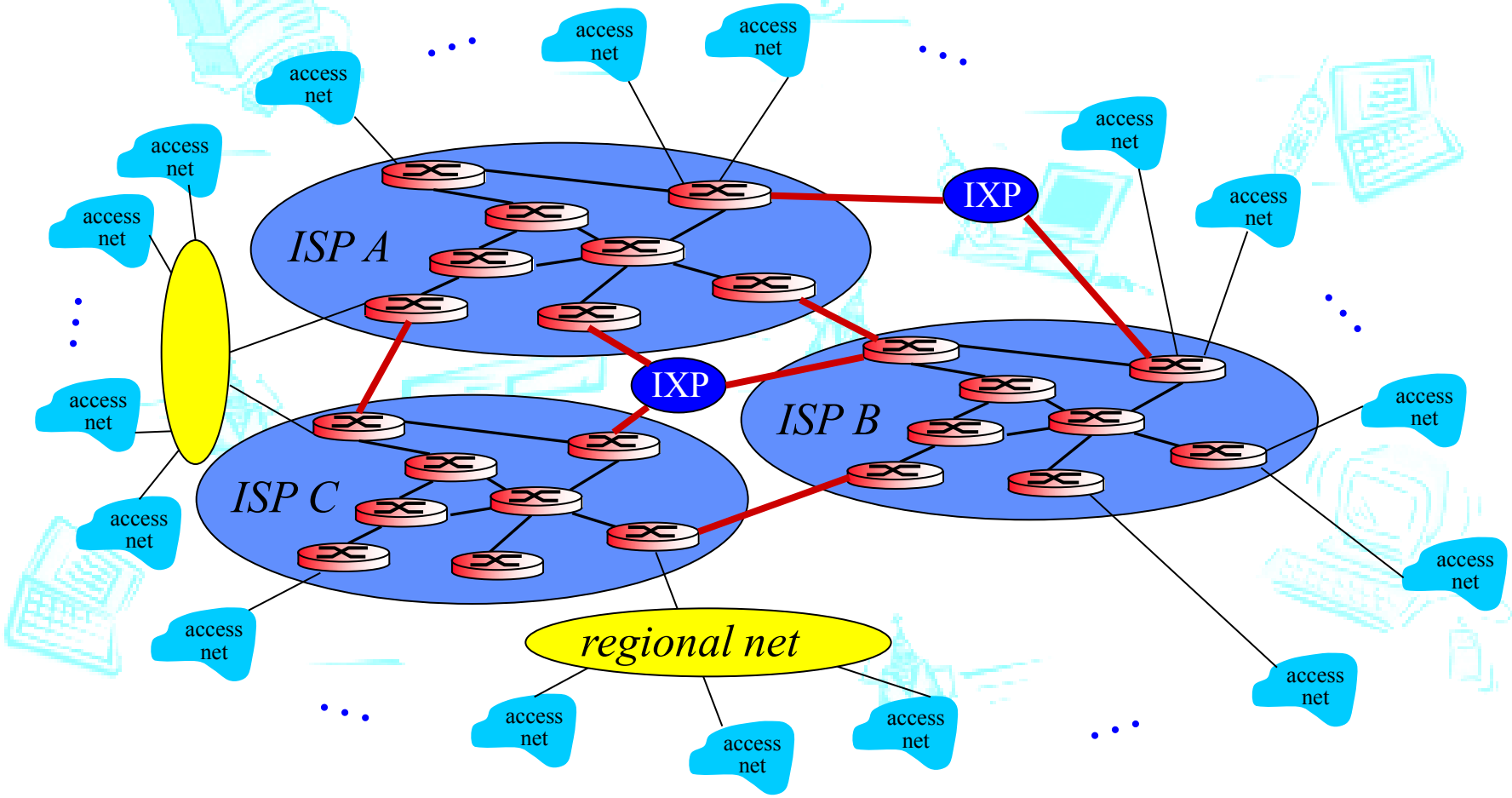
Internetin rakenne: Verkkojen verkko

Mutta: jos välitysverkko tuottaa voittoa, tulee kilpailijoita …. jotka pitää yhdistää toisiinsa!



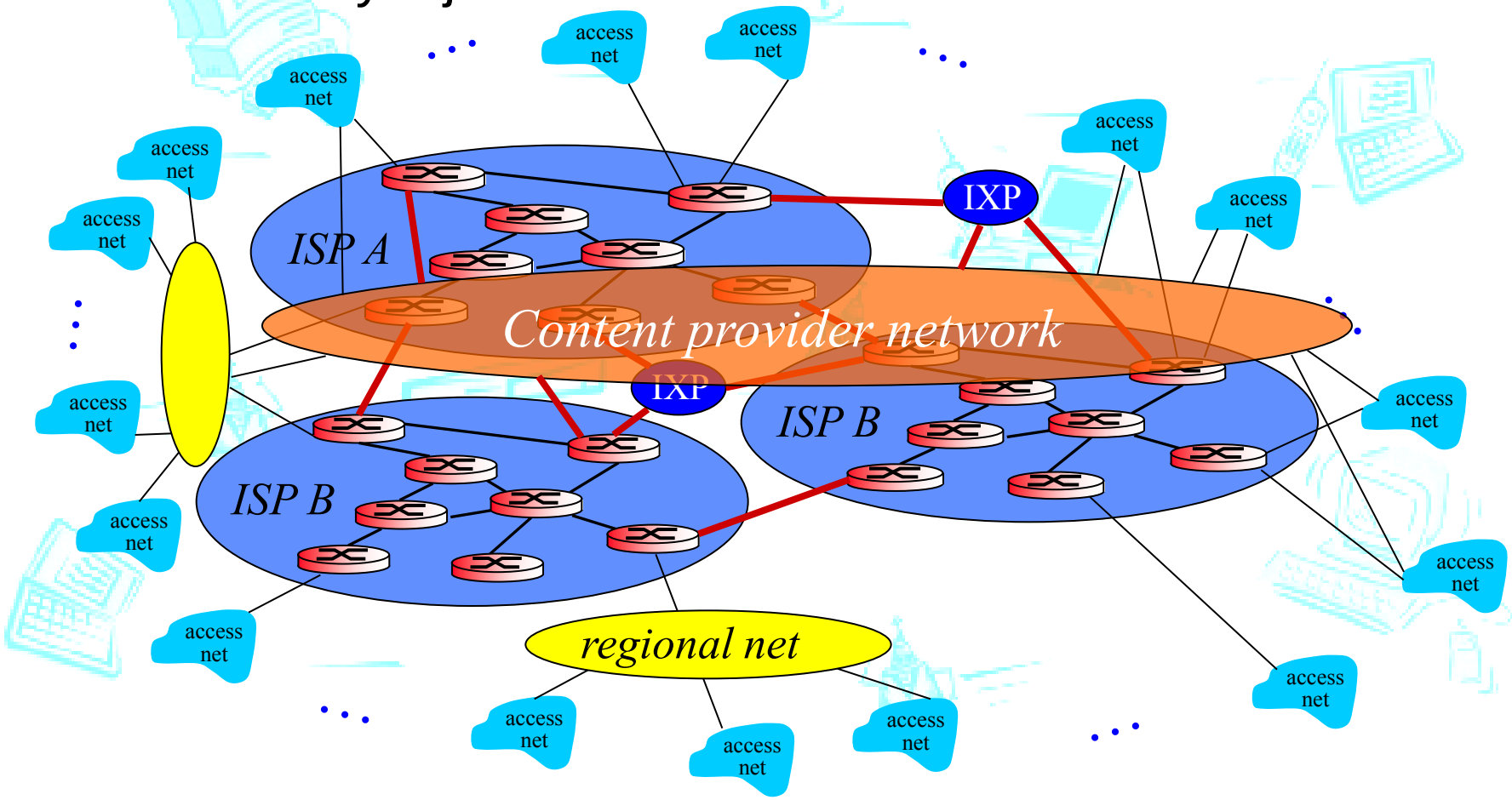
Internetin rakenne: Verkkojen verkko

… ja alueverkkoja (regional net), joden kautta palveluntarjoajilla yhteydet välitysverkkoihin



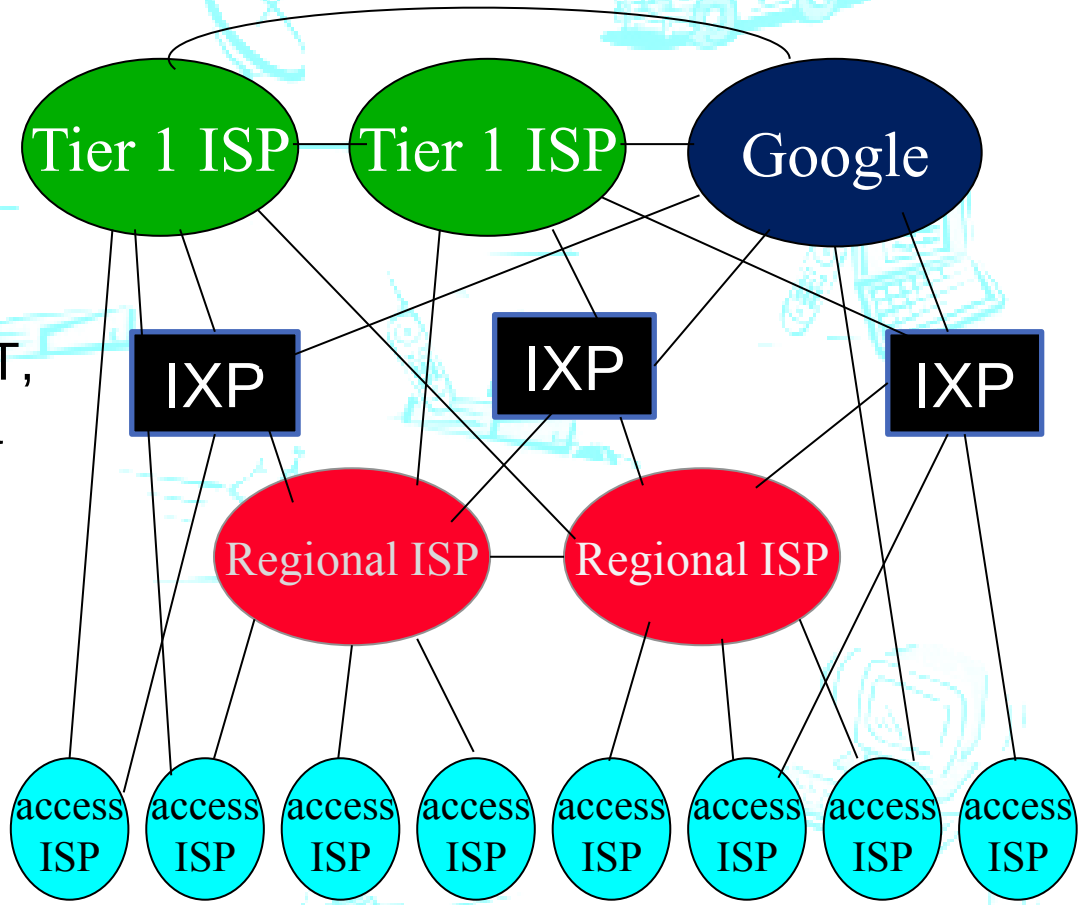
Internetin rakenne: Verkkojen verkko

… ja sisällön tuottajien (content provider) (e.g., Google, Microsoft, Akamai) omia verkkoja, joilla palvelut lähemmäs käyttäjiä

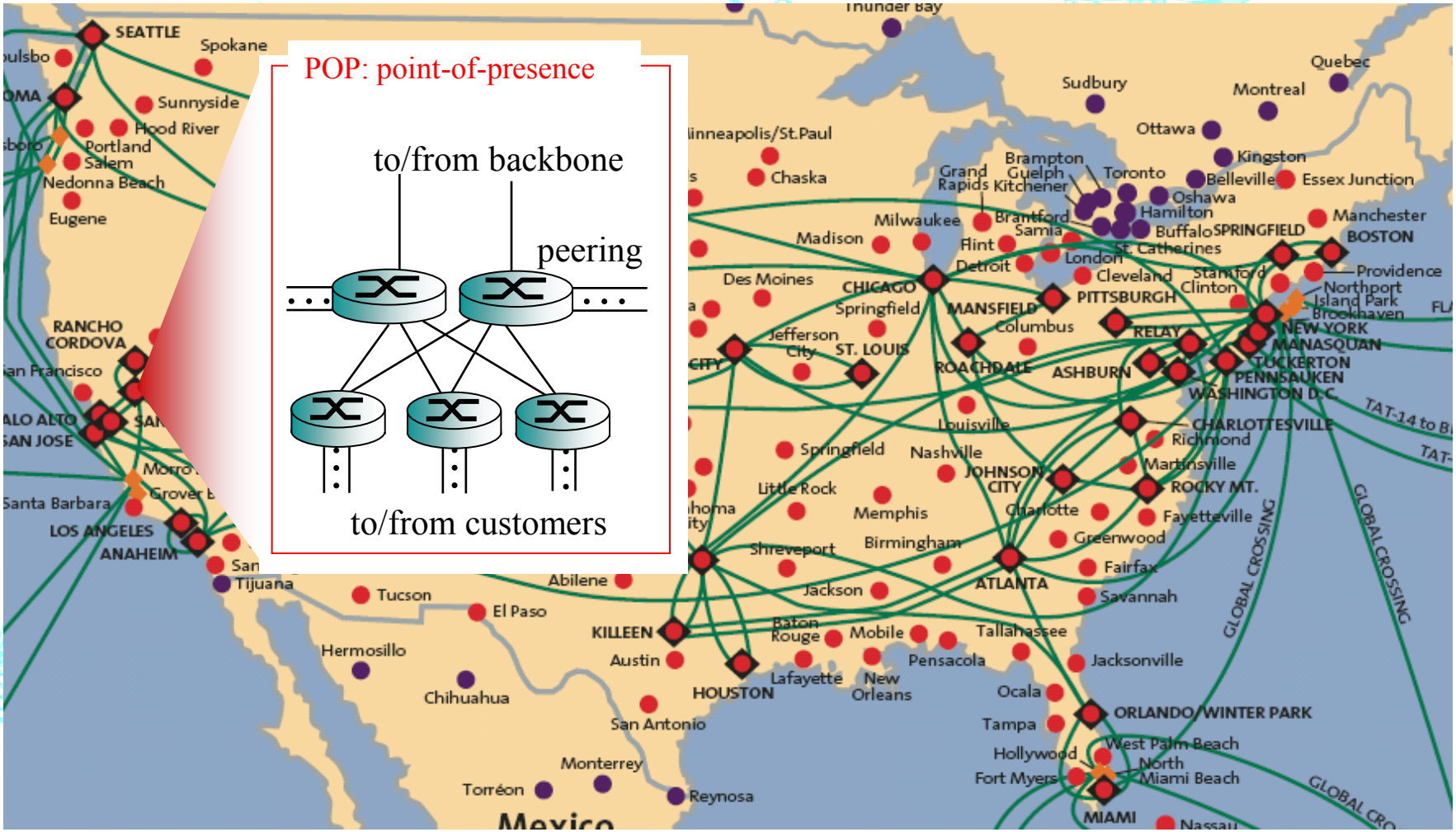


Internetin rakenne: Verkkojen verkko

- sisimpänä: pieni joukko maailmanlaajuisesti hyvin kytkeytyneitä verkkoja
  - “tier-1” kaupalliset ISPs (e.g., Level 3, Sprint, AT&T, NTT), kansainvälisiä, hyvä kattavuus (coverage)
  - Sisällön tarjoajan verkko (content provider netw.) (e.g, Google): yksityinen verkko,joka yhdistää palvelinkeskuksia internetiin, usein ohittaa kokonaan tai osittain tier-1 ISPt



Tier-1 ISP: e.g., Sprint



Yhteenveto

- Protokolla pino
- Internetin rakenne
  - Tietokoneet reunalla
  - Reitittimet muodostavat ytimen
- Erilaisia verkkotekniikoita
  - Tiedonsiirto sähköllä, valolla, säteilyllä
- Pakettien siirtoviipeet ja katoamiset
  - Siirto linkki kerrallaan reitittimeltä toiselle