

Tietoliikenteen perusteet

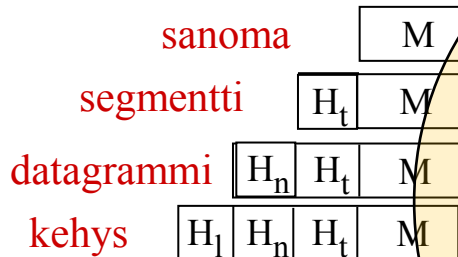


Syksy 2017

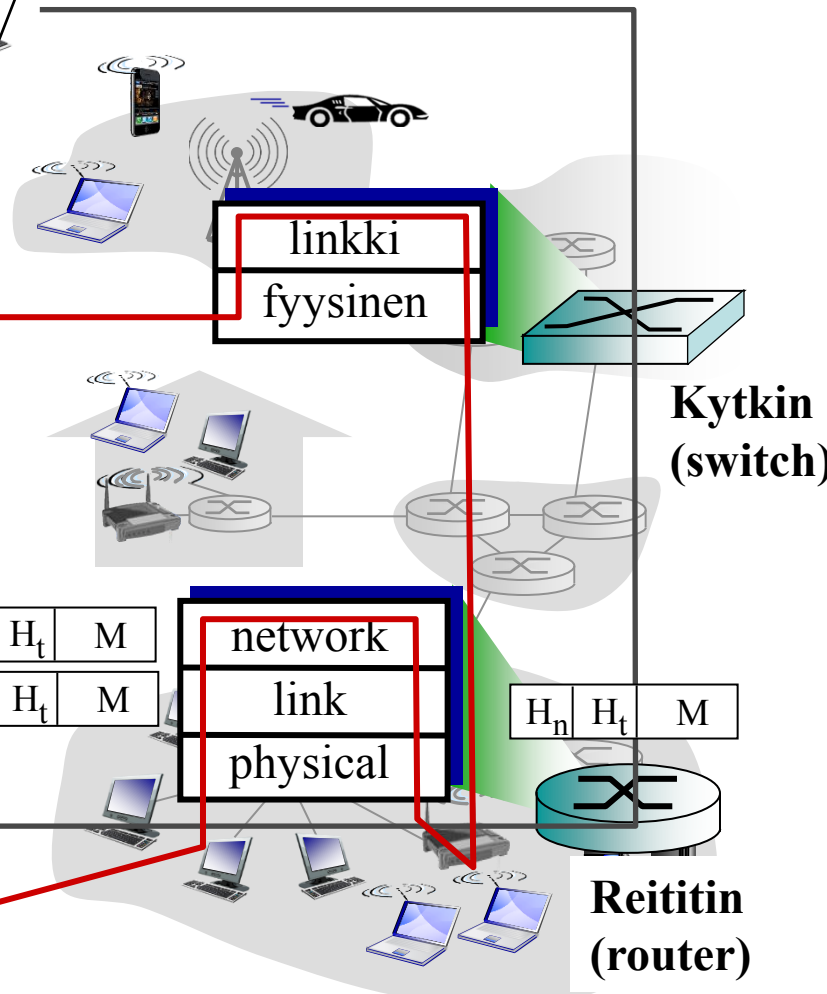
Timo Karvi

Pääasiallisesti kuvien
© J.F Kurose and K.W. Ross, All
Rights Reserved

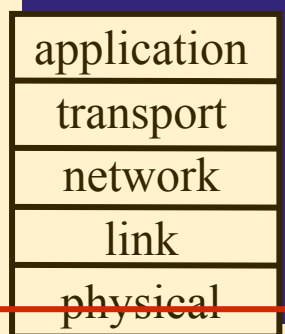
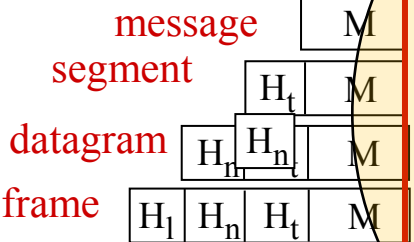
Lähettäjä (source)



Luennon sisältöä



Vastaanottaja (destination)



Sisältöä

- 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**

Oppimistavoitteet:

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

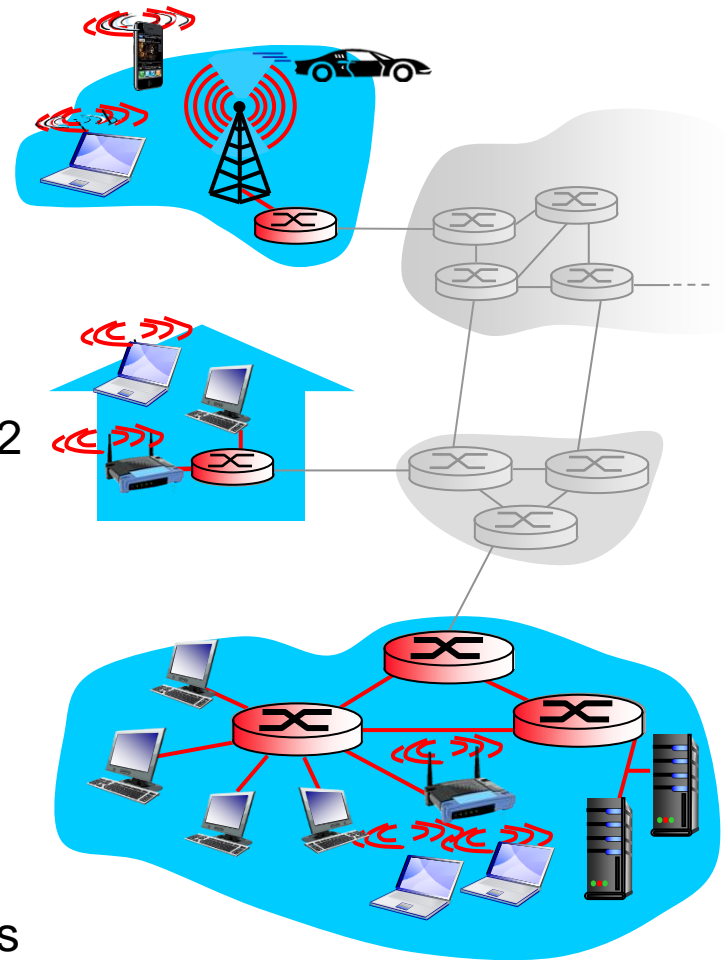




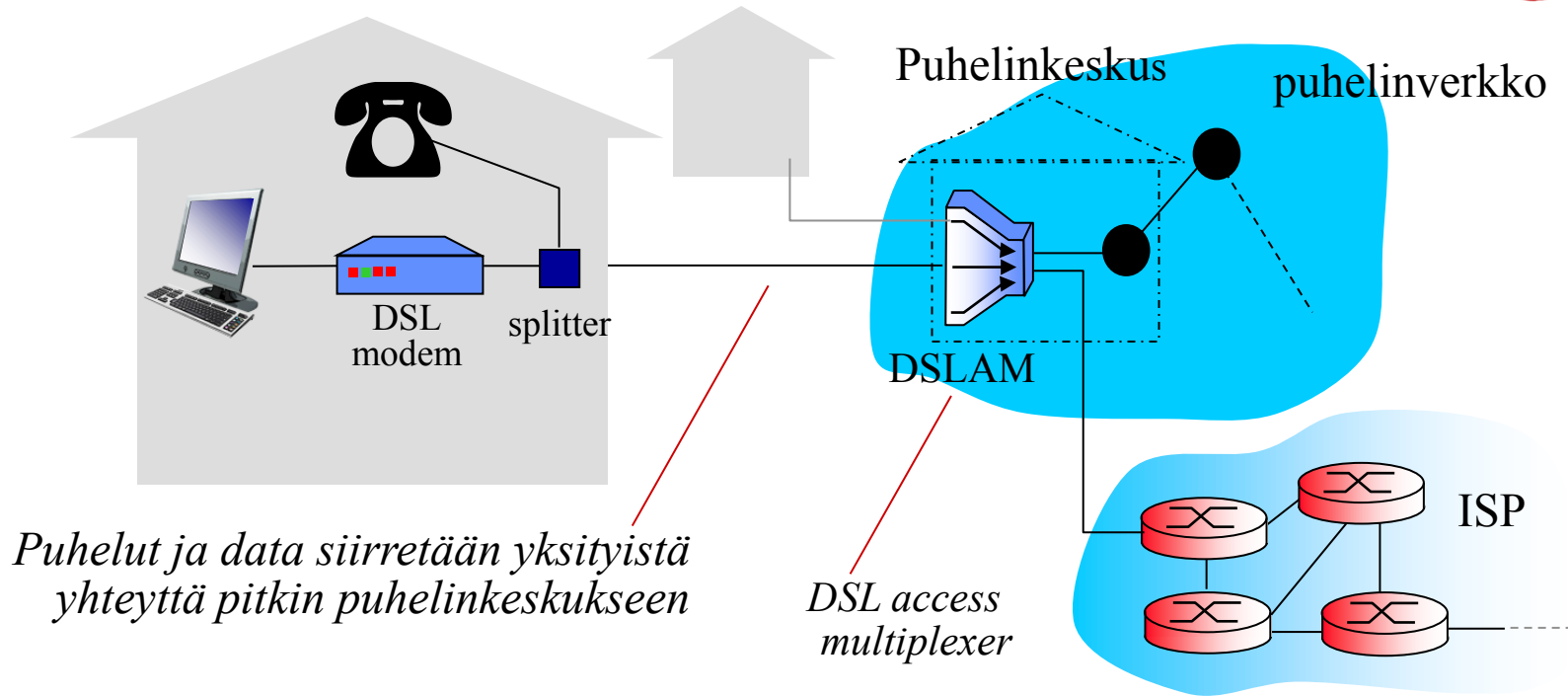
PÄÄSY INTERNETIIN

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 kbps- ~2 Mbps, LTE 50-100Mbps

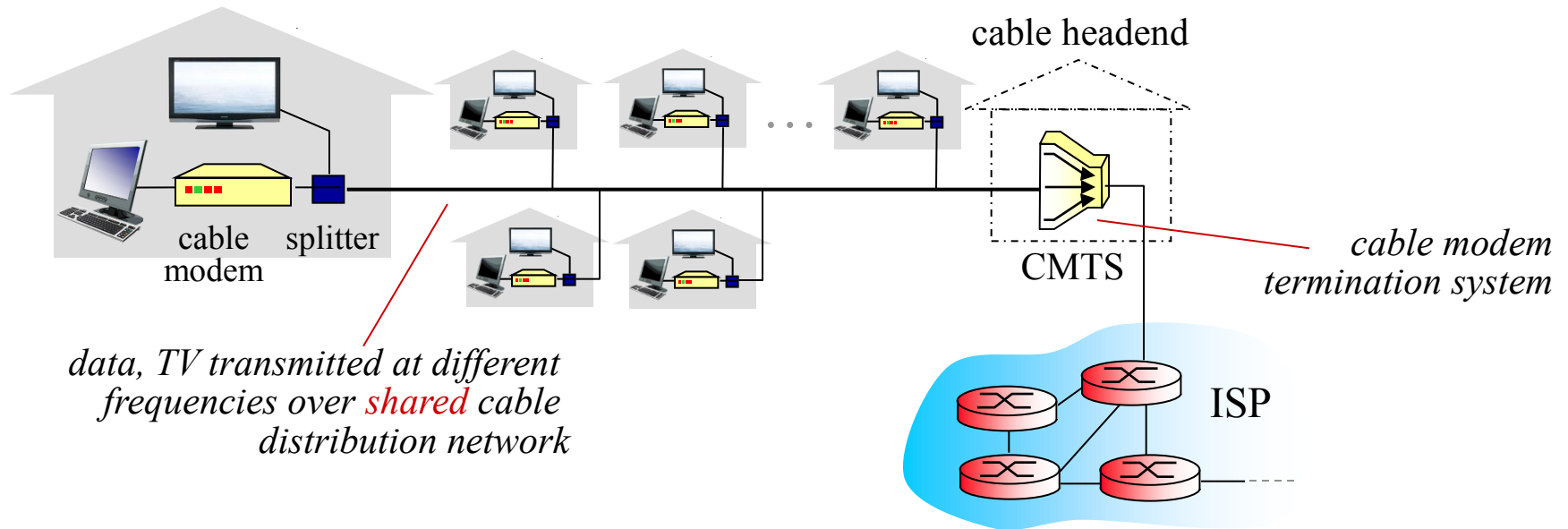


Puhelinverkko: digital subscriber line (DSL)



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

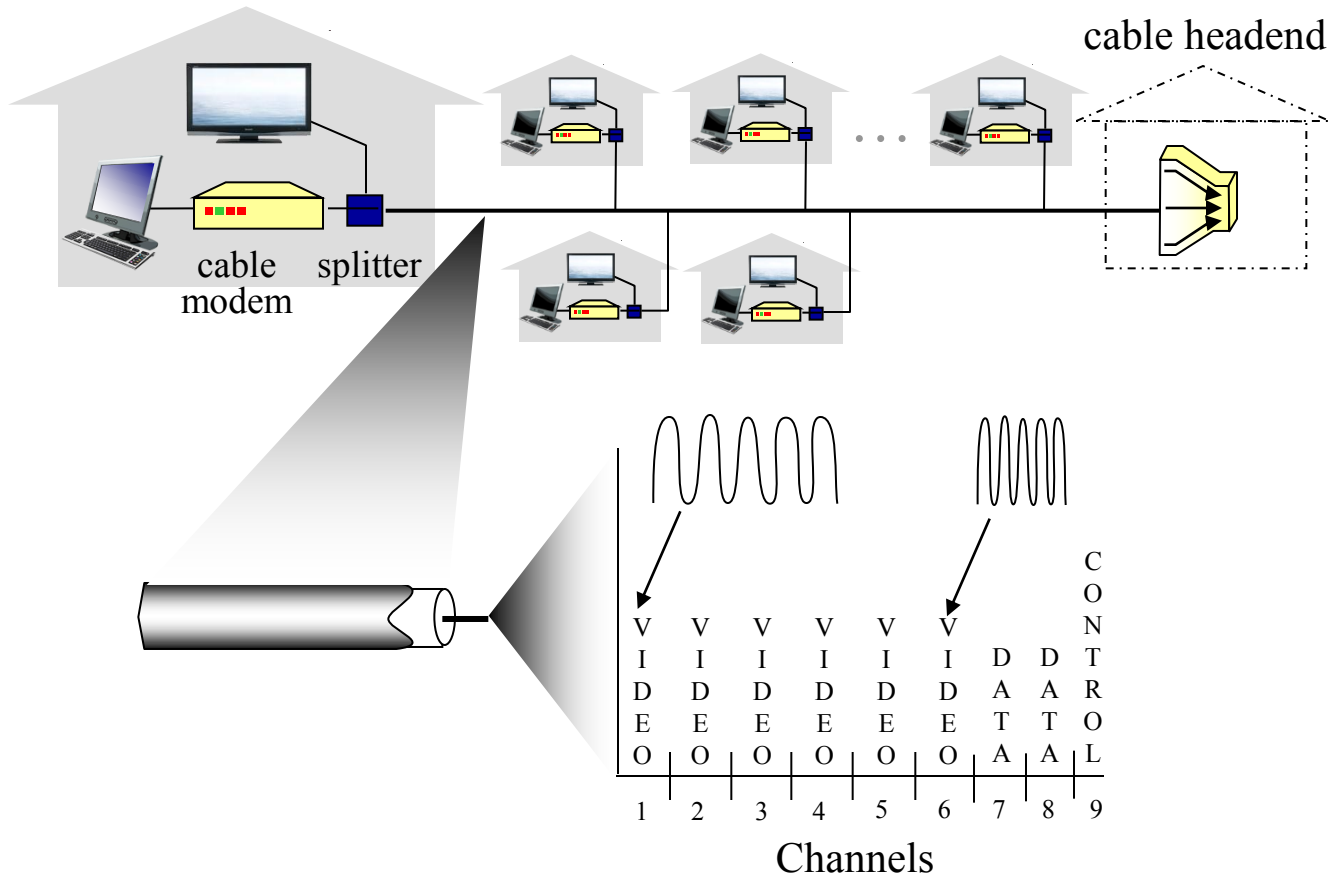
Kaapeliverkko



❖ Asymmetrinen ja jaettu yhteys

- Yleensä koaksiaalikaapeli talojakamoon, jossa ISP reititin
- Huoneistot jakavat saman kaapeliyhteyden toistensa ja TV-lähetysten kanssa

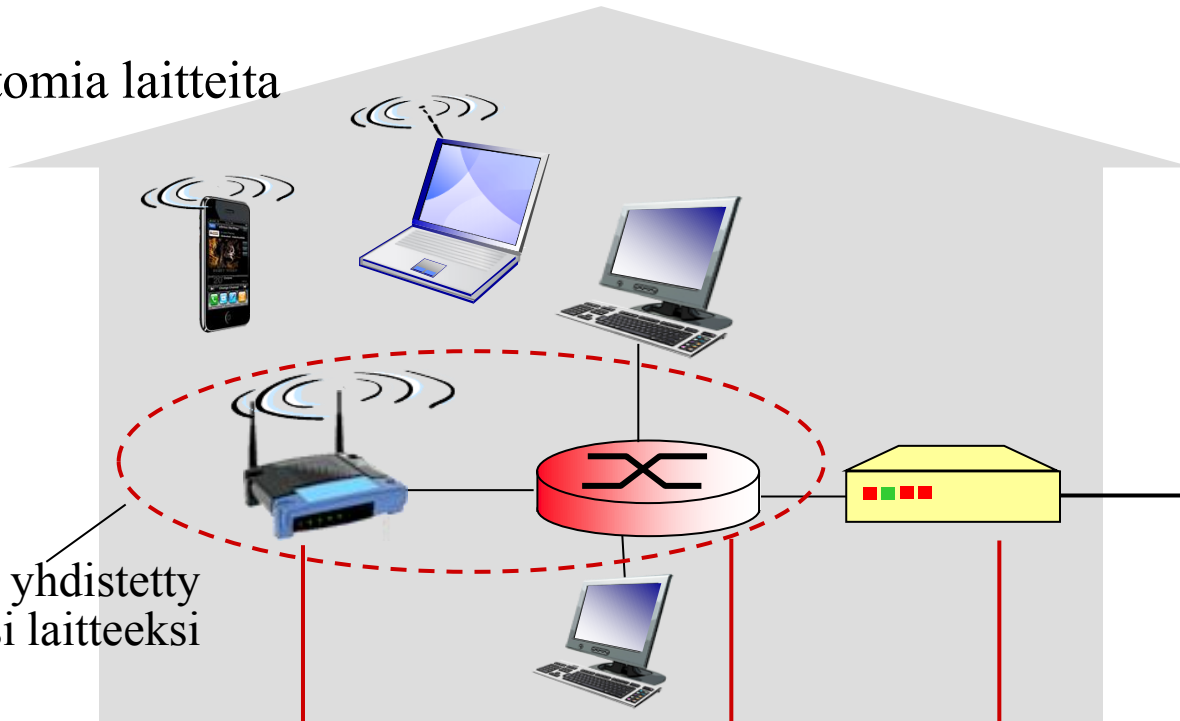
Kaapeliverkko



Taajuusalueet jaettu - frequency division multiplexing:
Eri kanavat siirretään eri taajuusalueilla

Kotiverkko (home network)

Langattomia laitteita



Usein yhdistetty
yhdeksi laitteeksi

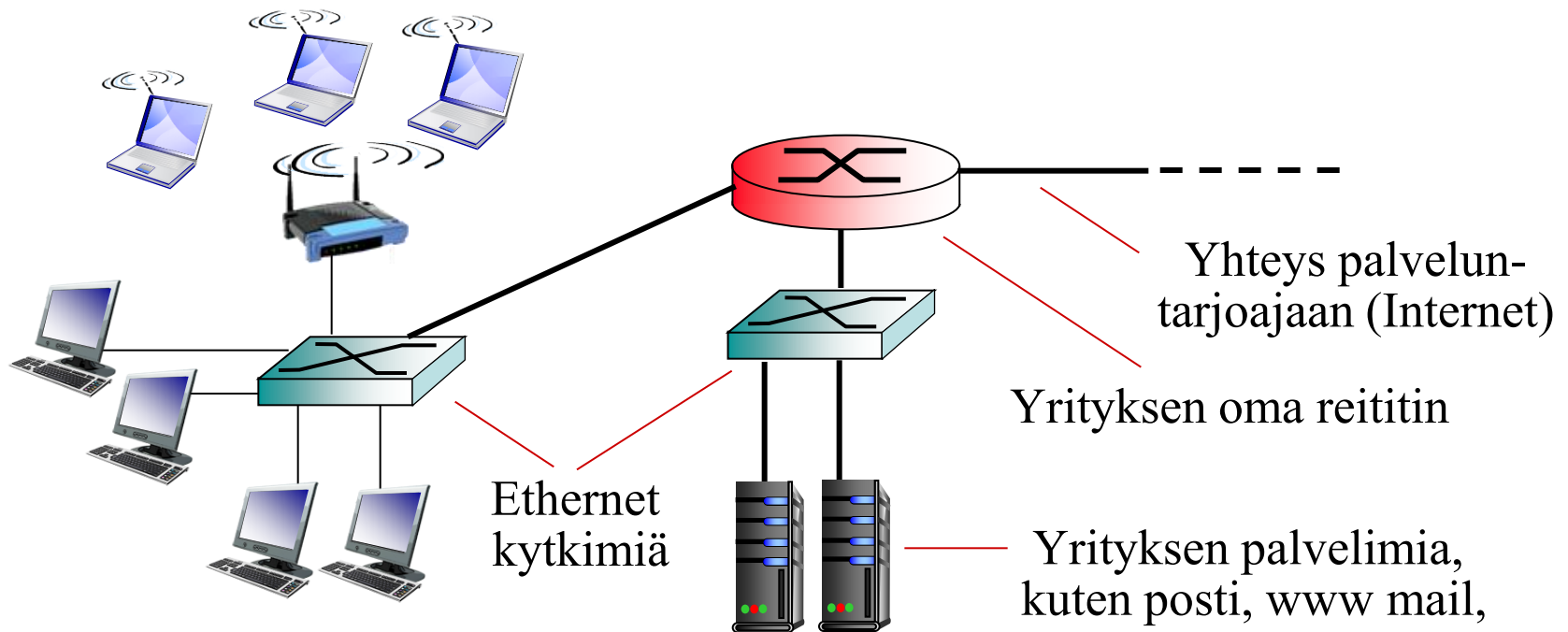
Langaton tukiasema
(54 Mbps)

Reititin, palomuri, NAT
langallinen Ethernet (100 Mbps)

Kaapeli- tai DSL-modeemi

Yhteys palvelun-
tarjoajaan ja sitä
kautta Internetiin

Yritysverkko (Ethernet)



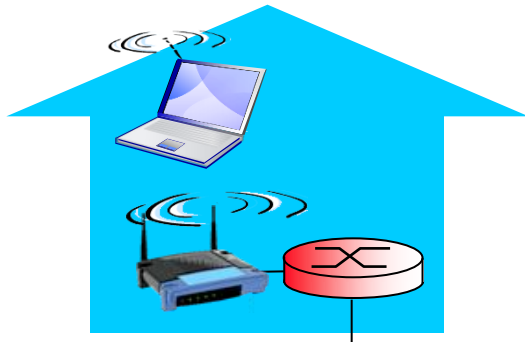
- Tyypillinen yrityksissä, yliopistoissa, jne.
- ❖ Siirtonopeudet 10 Mbps, 100Mbps, 1Gbps, 10Gbps
- ❖ Nykyään päätelaitteet suoraan kiinni ethernet-kytkimissä

Langaton verkko

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

WLAN:

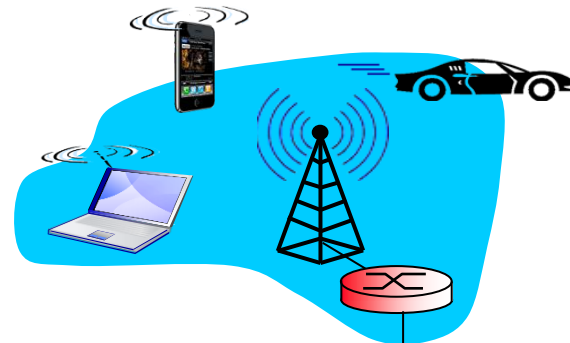
- Rakennuksen sisällä (10 m)
- 802.11b/g (WiFi): 11, 54 Mbps siirtonopeus



to Internet

Mobiiliverkko

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



to Internet

Fyysinen media 1/3

- **Bitti (bit):** siirrettävä yksikkö lähettimen/vastaanotin parin välillä
- **Fyysinen linkki (physical link):** yhteys lähettimen ja vastaanottimen välillä
- **Valvottu siirtotie (media):**
 - Signaali siirretään kiinteään aineeseen välityksellä: kupari, kuitu, koaksiaali
- **Avoin siirtotie:**
 - Signaali siirtyy vapaasti, kuten radio

Parikaapeli (twisted pair, TP)

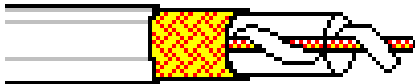
- Kaksi eristettyä kuparijohtoa
 - Category 5: 100 Mbps, 1 Gpbs Ethernet
 - Category 6: 10Gbps



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
 - siirtonopeus 10's-100's Gpbs
- ❖ Vähän siirtovirheitä
 - Toistimet (repeaters) kaukana toisistaan
 - Ei elektromagneettisiä 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

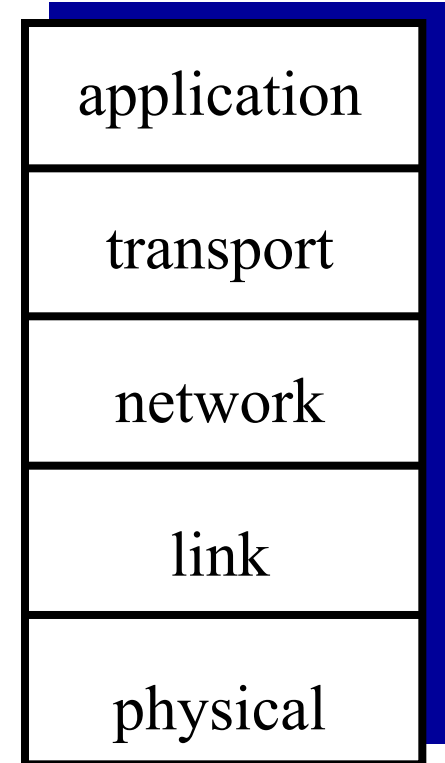
Miksi kerrosrakenne?

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, ..

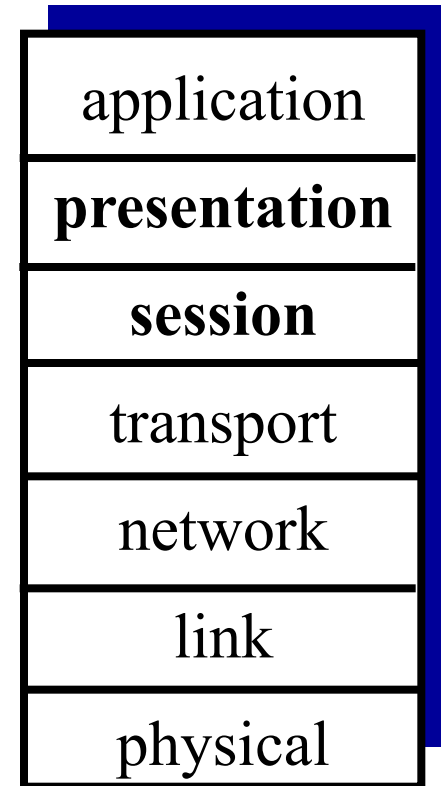
Internet-protokollapino

- **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?

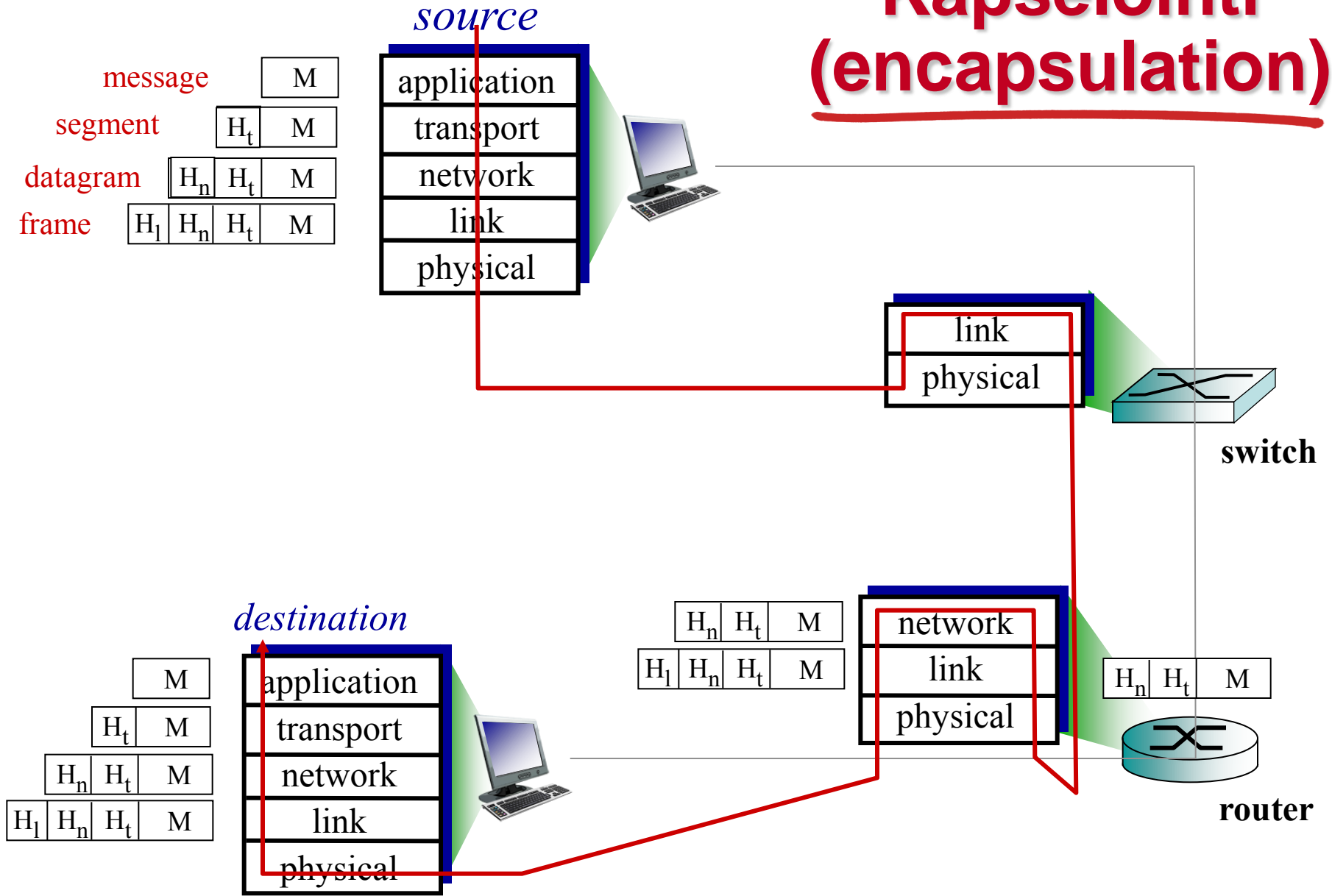


ISO OSI -viitemalli

- *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 (ei kuulu kurssiin)

- 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!

Haittaohjelmia (malware) tietokoneille Internetin välityksellä (ei kurssiin)

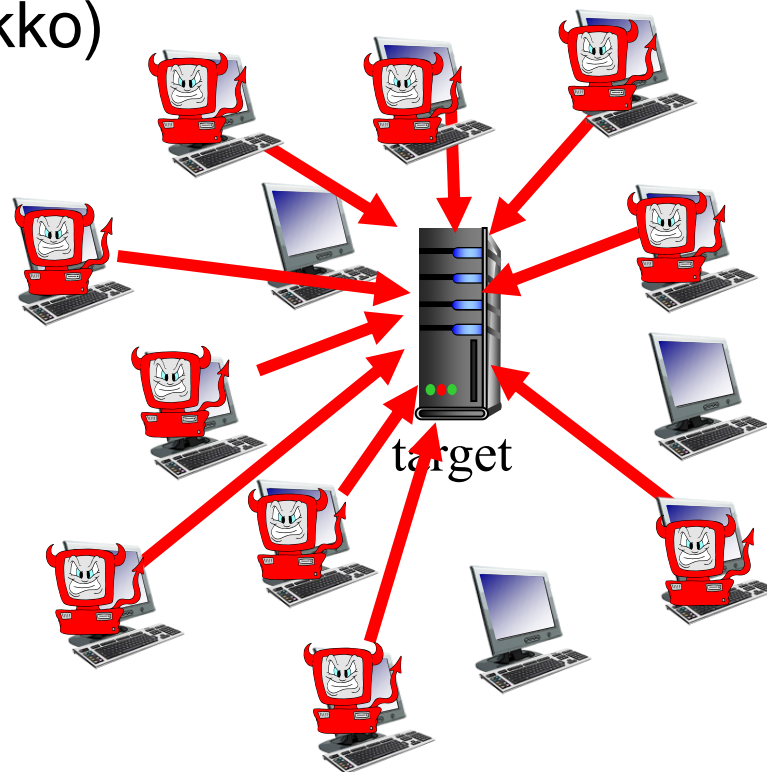
- Haittaohjelma voi tulla usealla tavalla:
 - *virus*: itseään kopioiva ohjelma, joka (aktiivisesti) vastaanotetaan ja suoritetaan (esim. sähköpostin liite, verkosta ladattu koodi)
 - *mato (worm)*: itseään kopioiva koodi, joka saadaan (passiivisesti) vastaanottamalla objekti, joka suoritetaan automaattisesti
- **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 (ei kurssiin)

Palvelunestohyökkäys (Denial of Service (DoS)):

hyökkääjät estävät laillisten käyttäjien käytön tuottamalla runsaasti ylimääräistä liikennettä

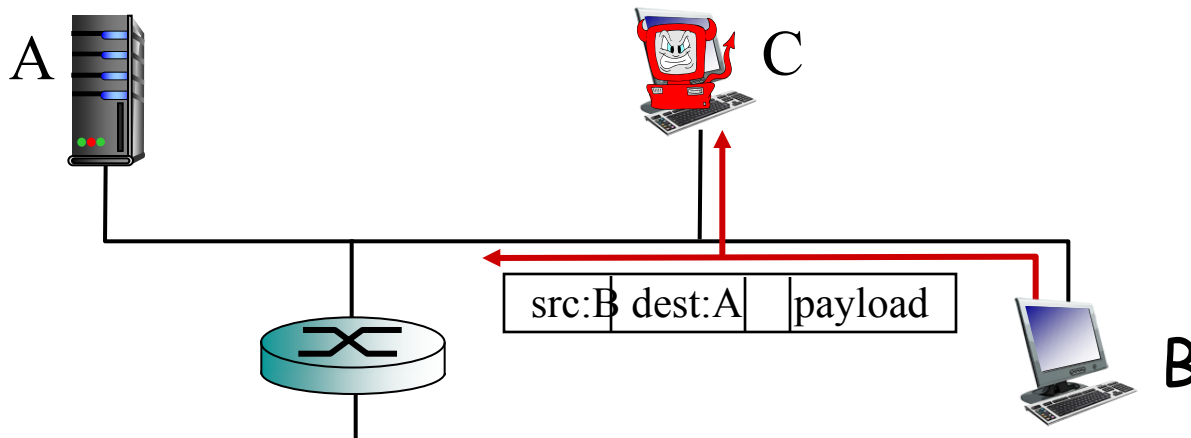
1. Valitse kohde (palvelin, verkko)
2. Rakenna botnet
murtautumalla koneille eripuolilla verkkoa
3. Laita murretut koneet lähettämään paketteja kohteelle



Pakettien kuuntelu (sniffing) (ei kurssiin)

Pakettien kuuntelu:

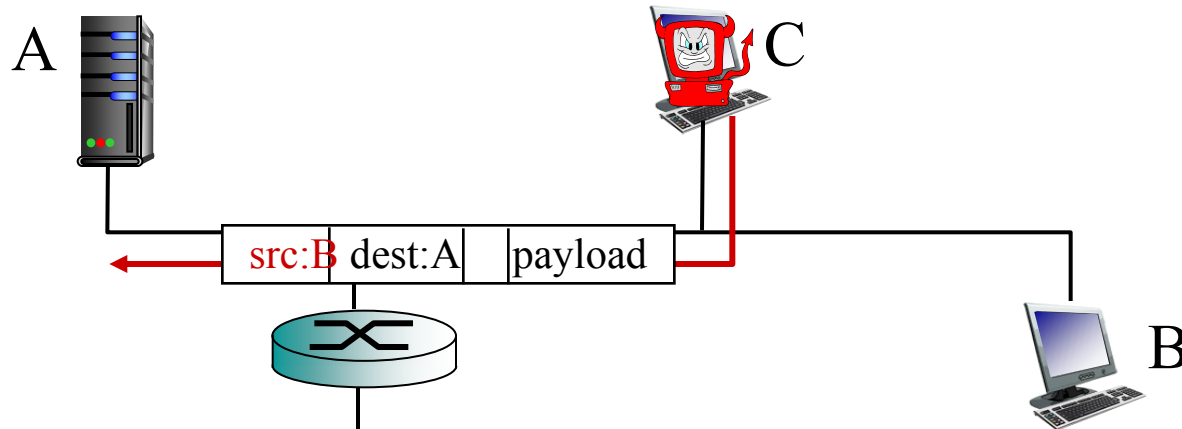
- Yleislähetys kanava (kuten jaettu ethernet, langaton yhteys) – liikenne on kaikkien kuultavissa
- Verkkorajapinta ei valikoi paketteja (ns. promiscuous mode), vaan poimii kaikki kuulemansa paketit (esim. sanasanoja)



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

Osoitteen väärentäminen (fake address) (ei kurssiin)

IP spoofing: lähetä paketti, jossa väärä lähettäjän osoite



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



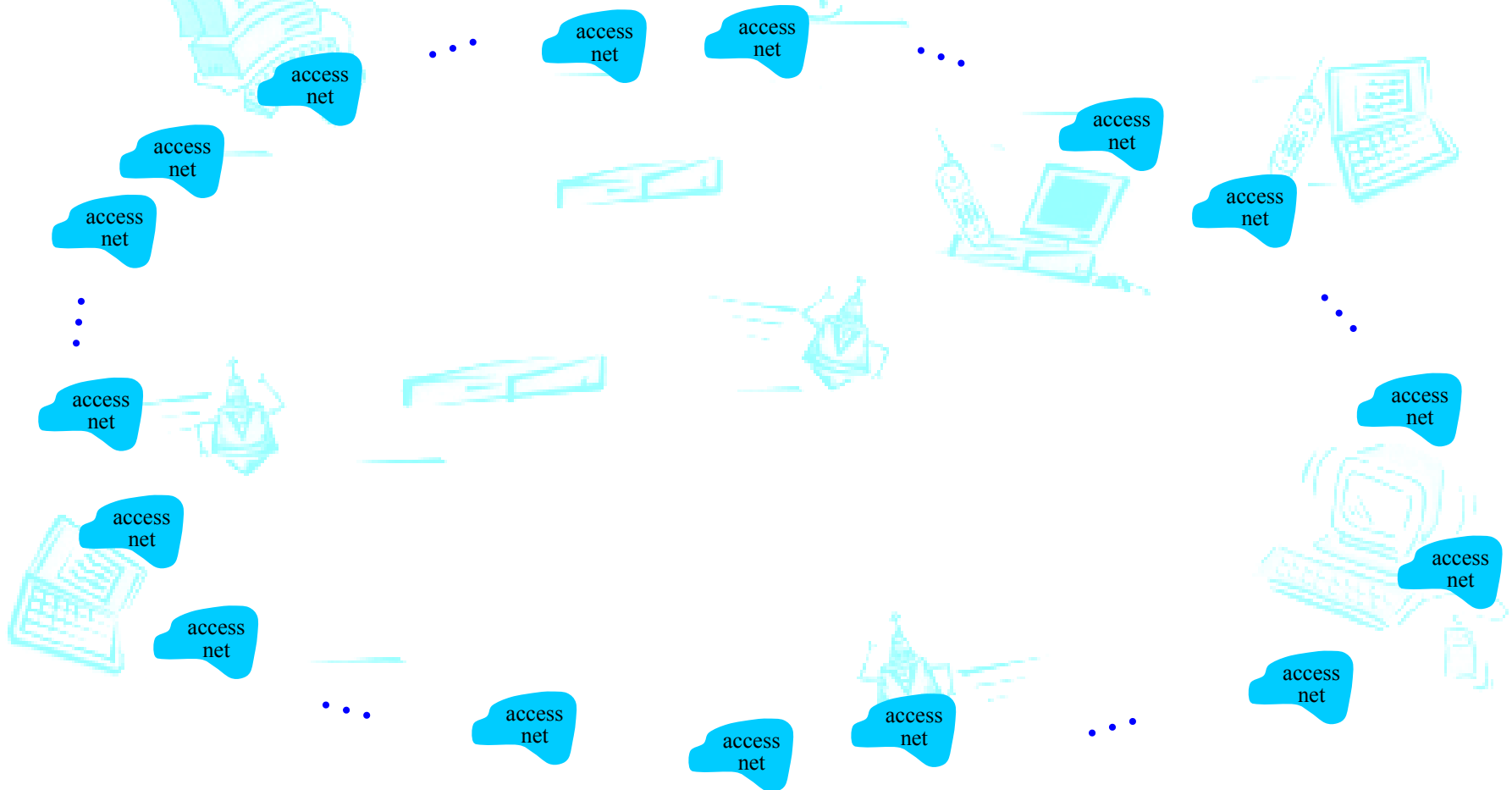
INTERNETIN RAKENNE

Internetin rakenne: Verkkojen verkko

- Pääte-laite 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

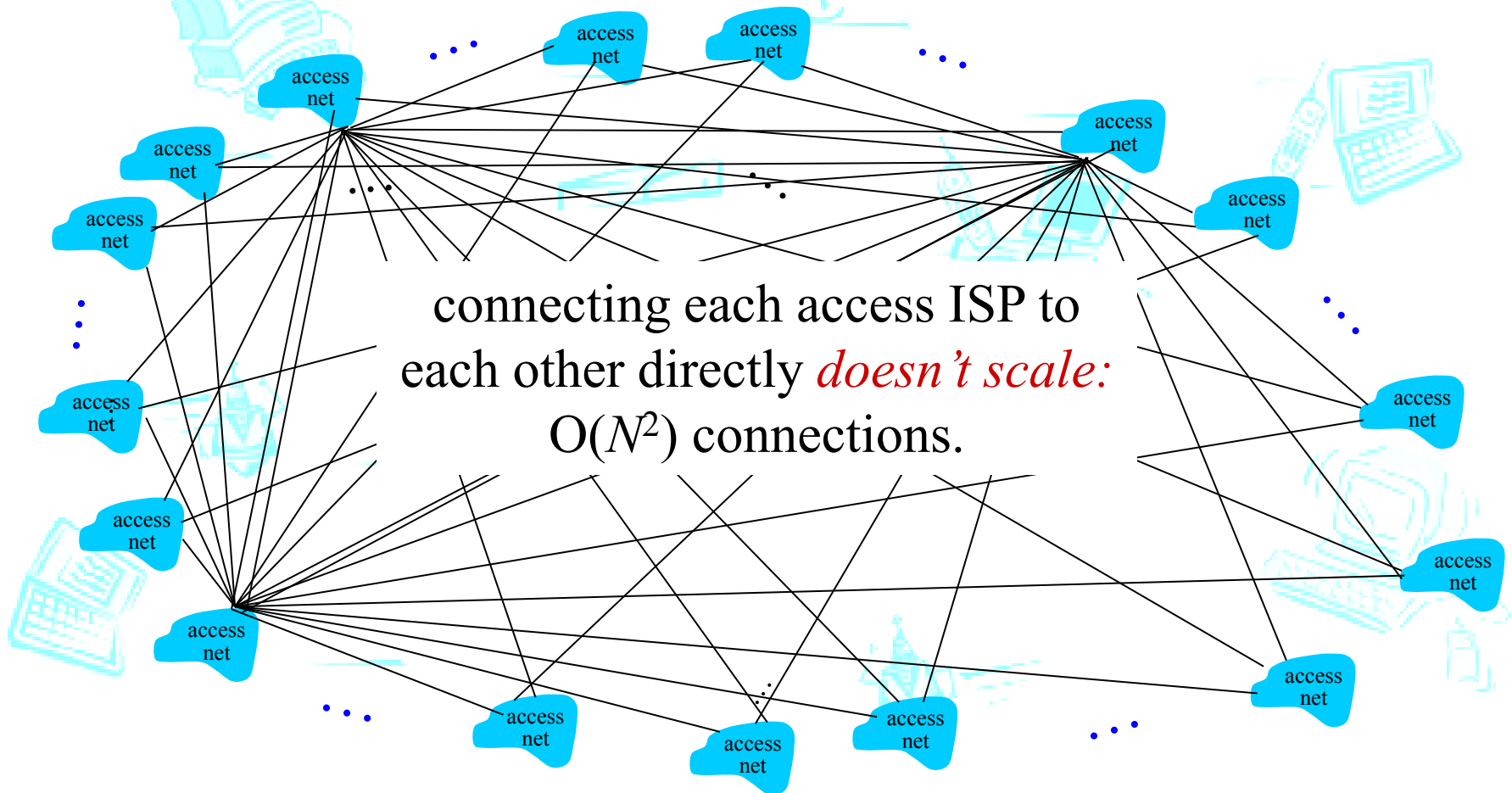
Internetin rakenne: Verkkojen verkko

Ongelma: Miten miljoonat palveluntarjoajien verkot yhdistetään?



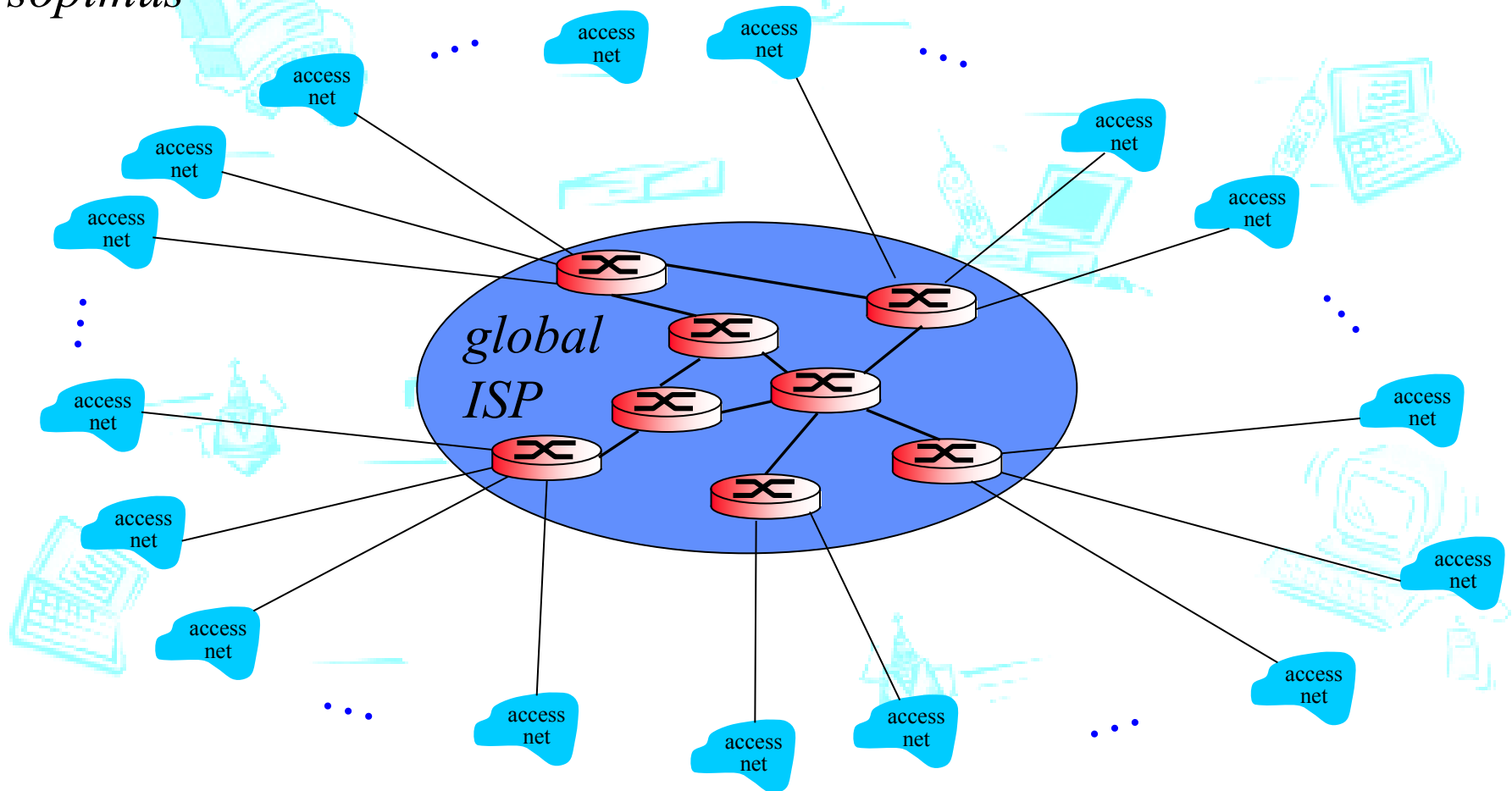
Internetin rakenne: Verkkojen verkko

Vaihtoehto: Yhdistetään jokainen ISP suoraan kaikkiin muihin?



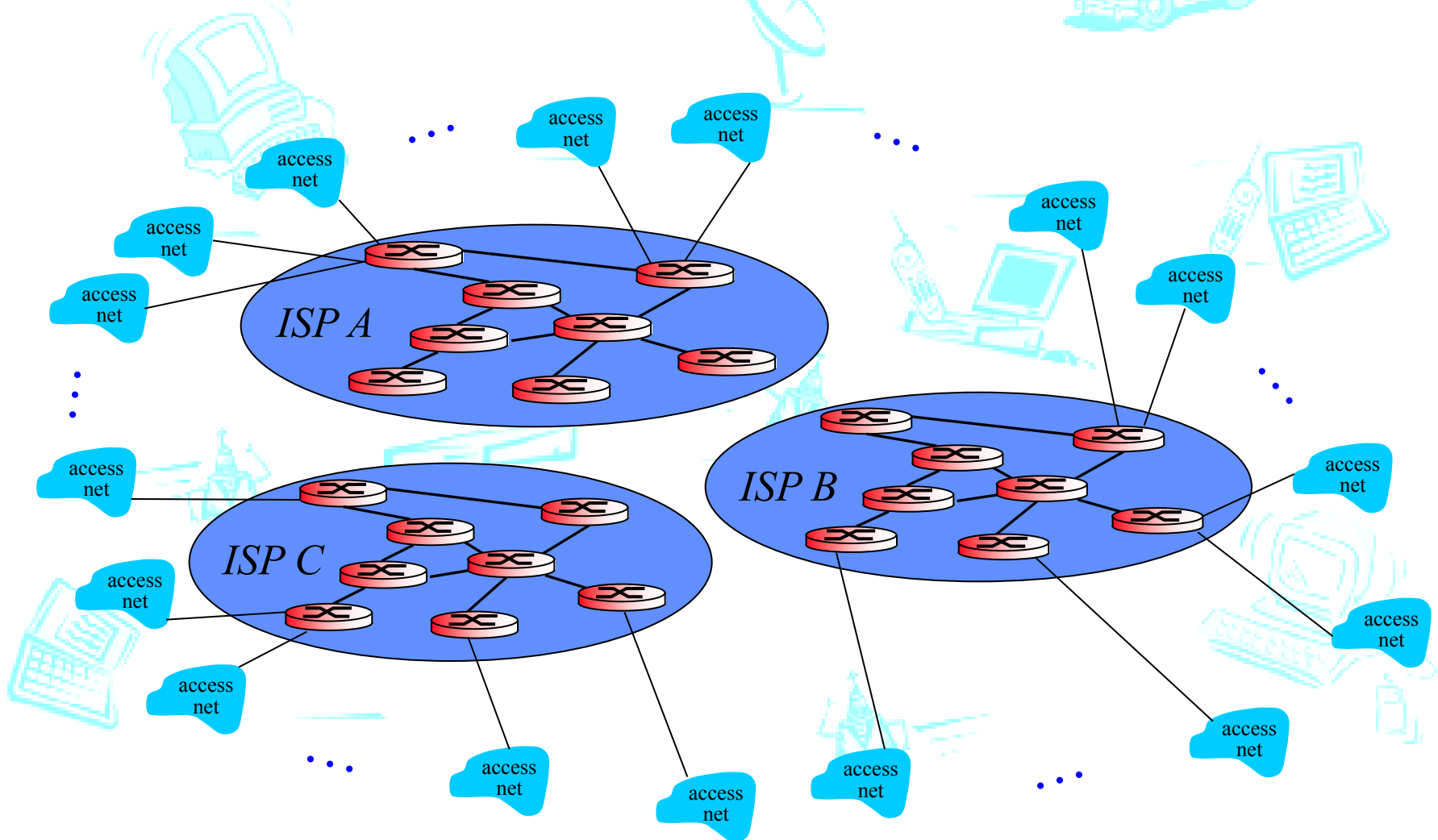
Internetin rakenne: Verkkojen verkko

Vaihtoehto: yhdistetään kaikki yhteen keskitettyyn välitysverkkoon (globaali ISP)? Asiakkailla and palvelun tarjoajalla sopimus



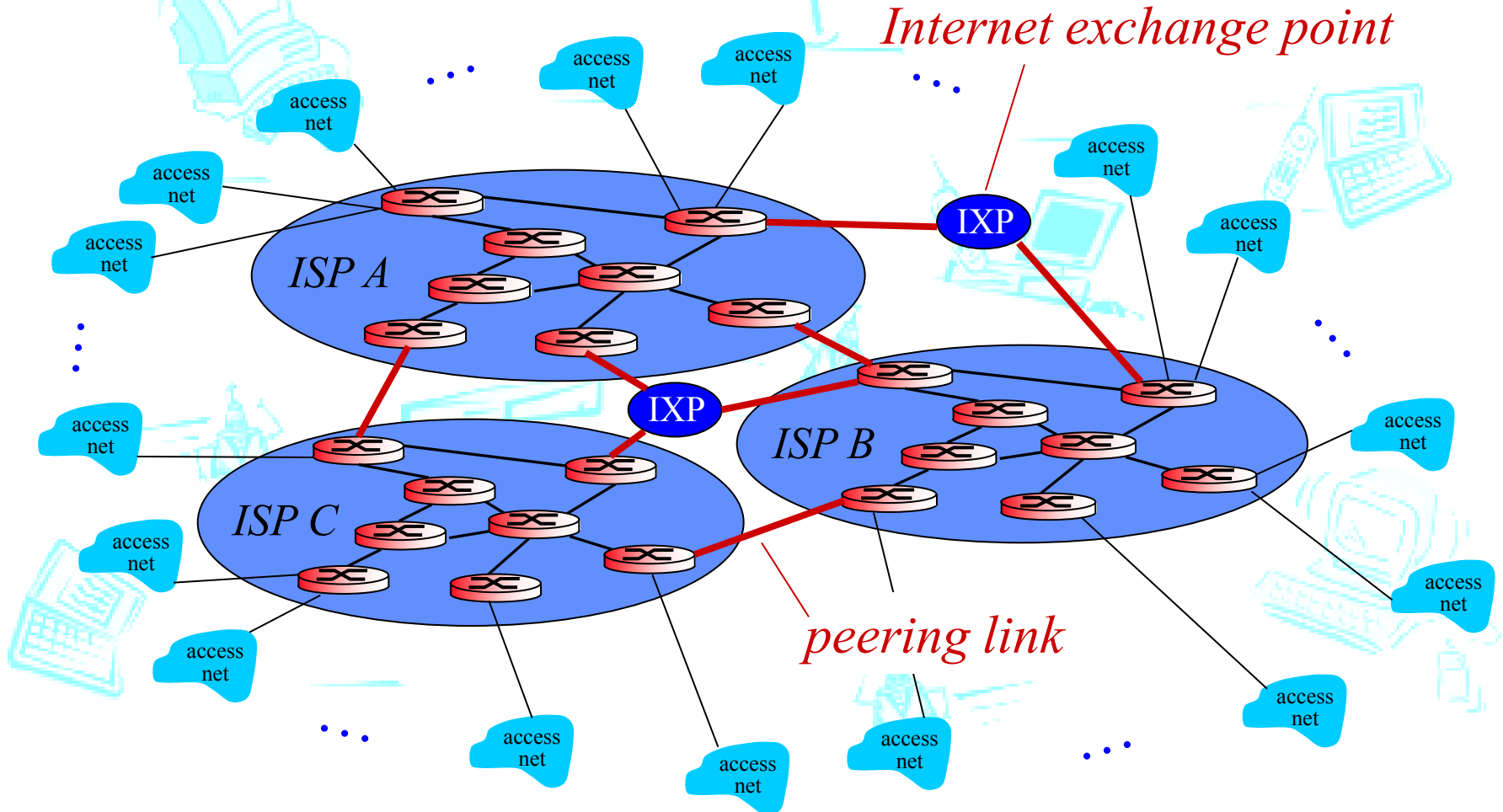
Internetin rakenne: Verkkojen verkko

Mutta: jos välitysverkko tuottaa voittoa, tulee kilpailijoita



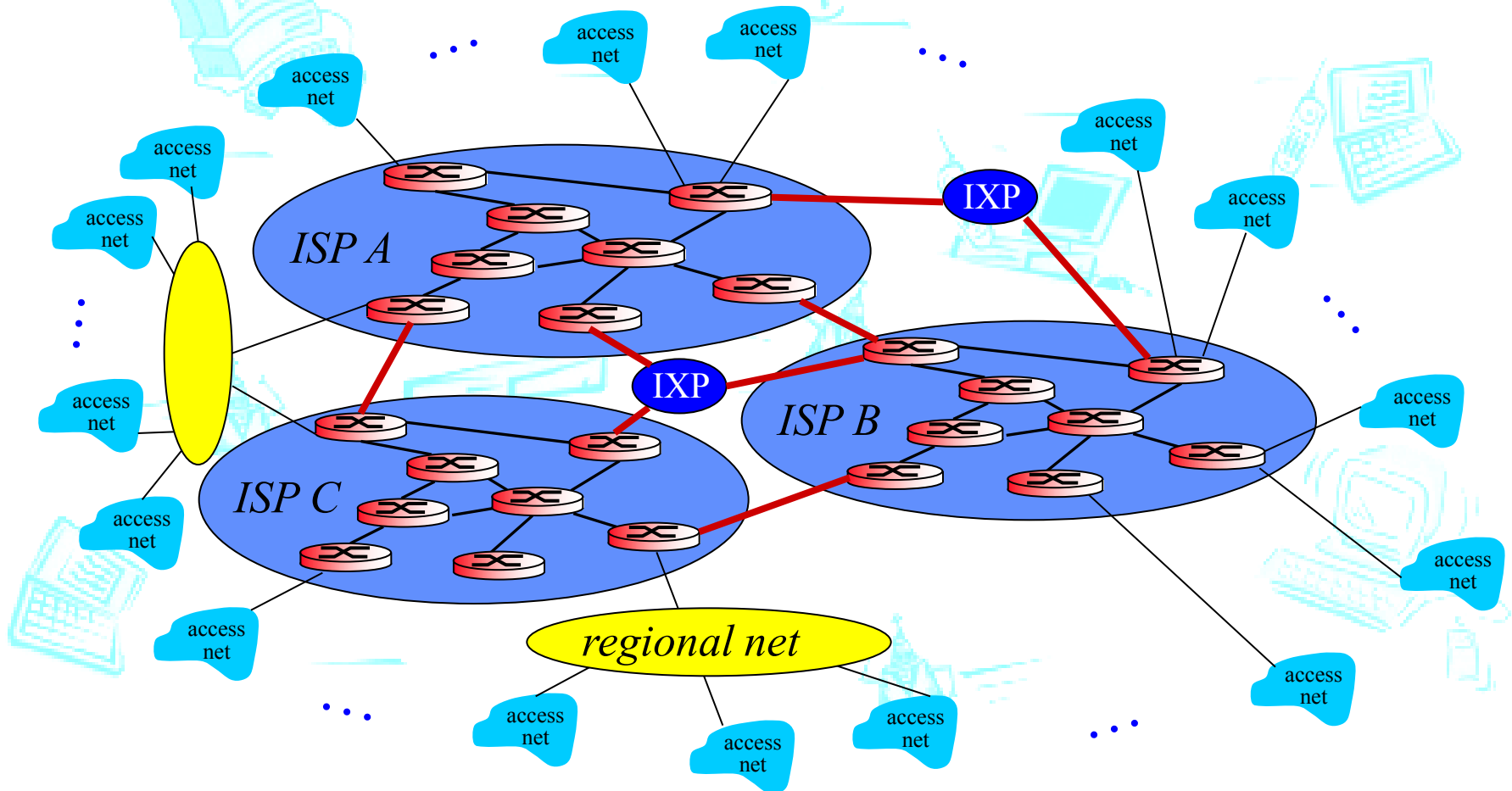
Internetin rakenne: Verkkojen verkko

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



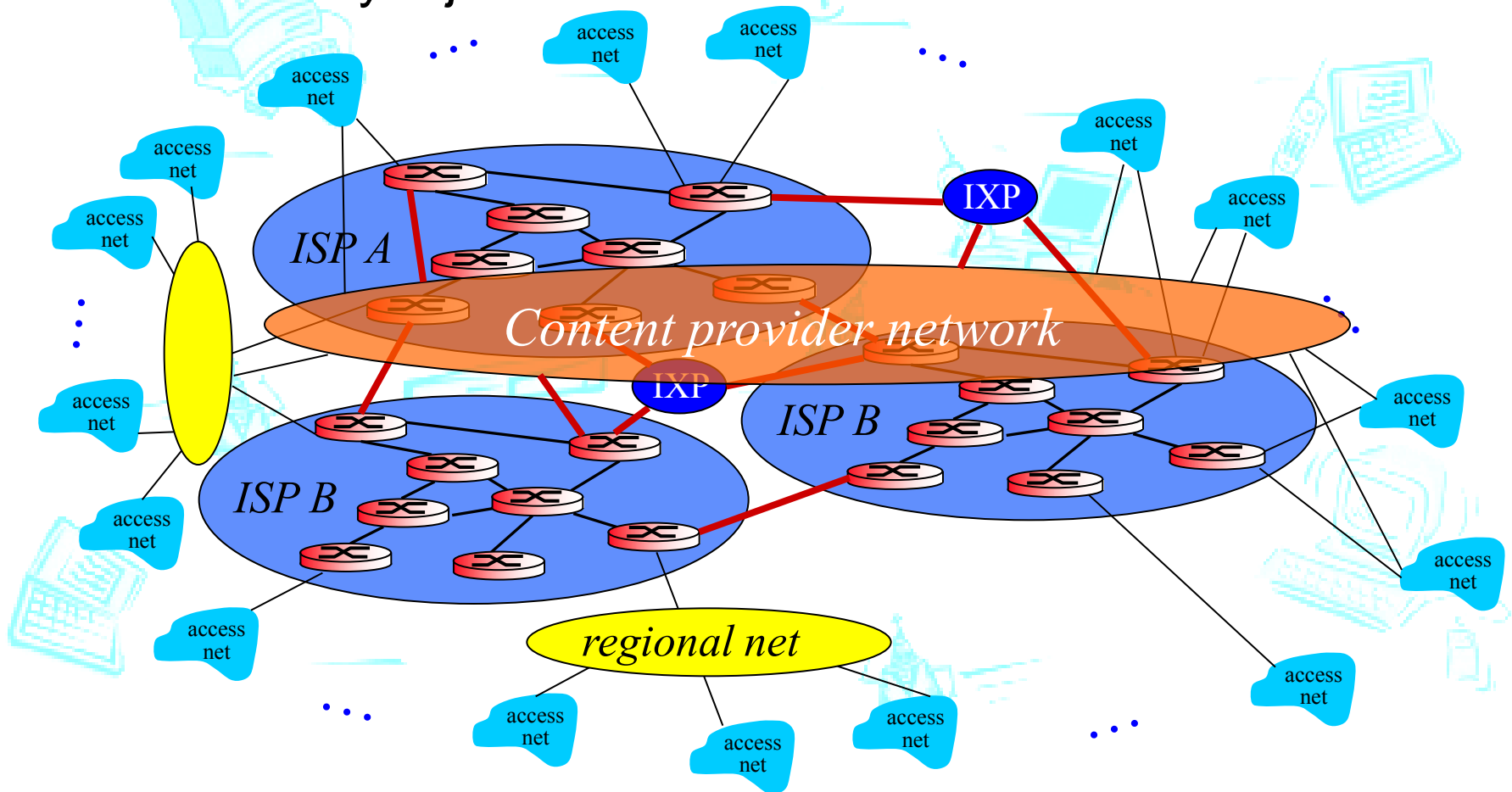
Internetin rakenne: Verkkojen verkko

... ja alueverkkoja (regional net), joiden kautta palveluntarjoajilla yhteydet välitysverkkoihin



Internetin rakenne: Verkkojen verkko

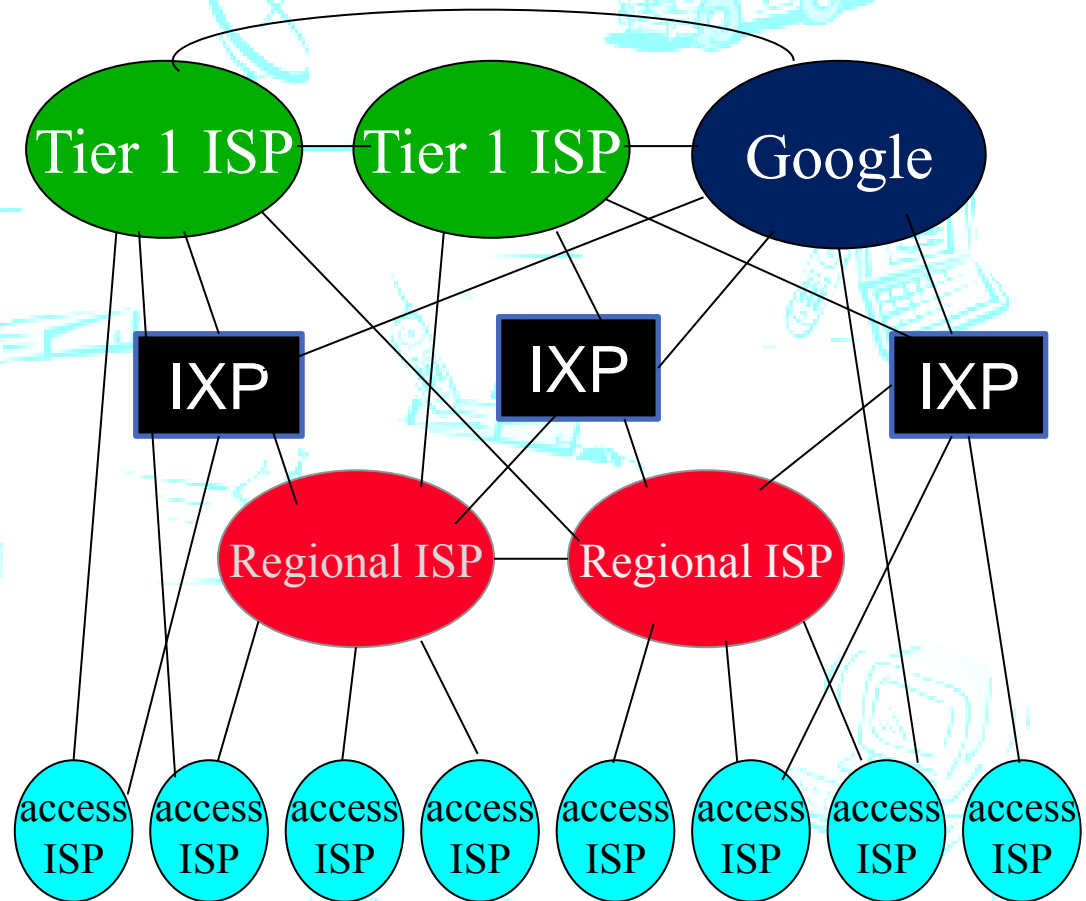
... ja sisällön tuottajien (content provider) (e.g., Google, Microsoft, Akamai) omia verkkoja, joilla palvelut lähemmäs käyttäjiä



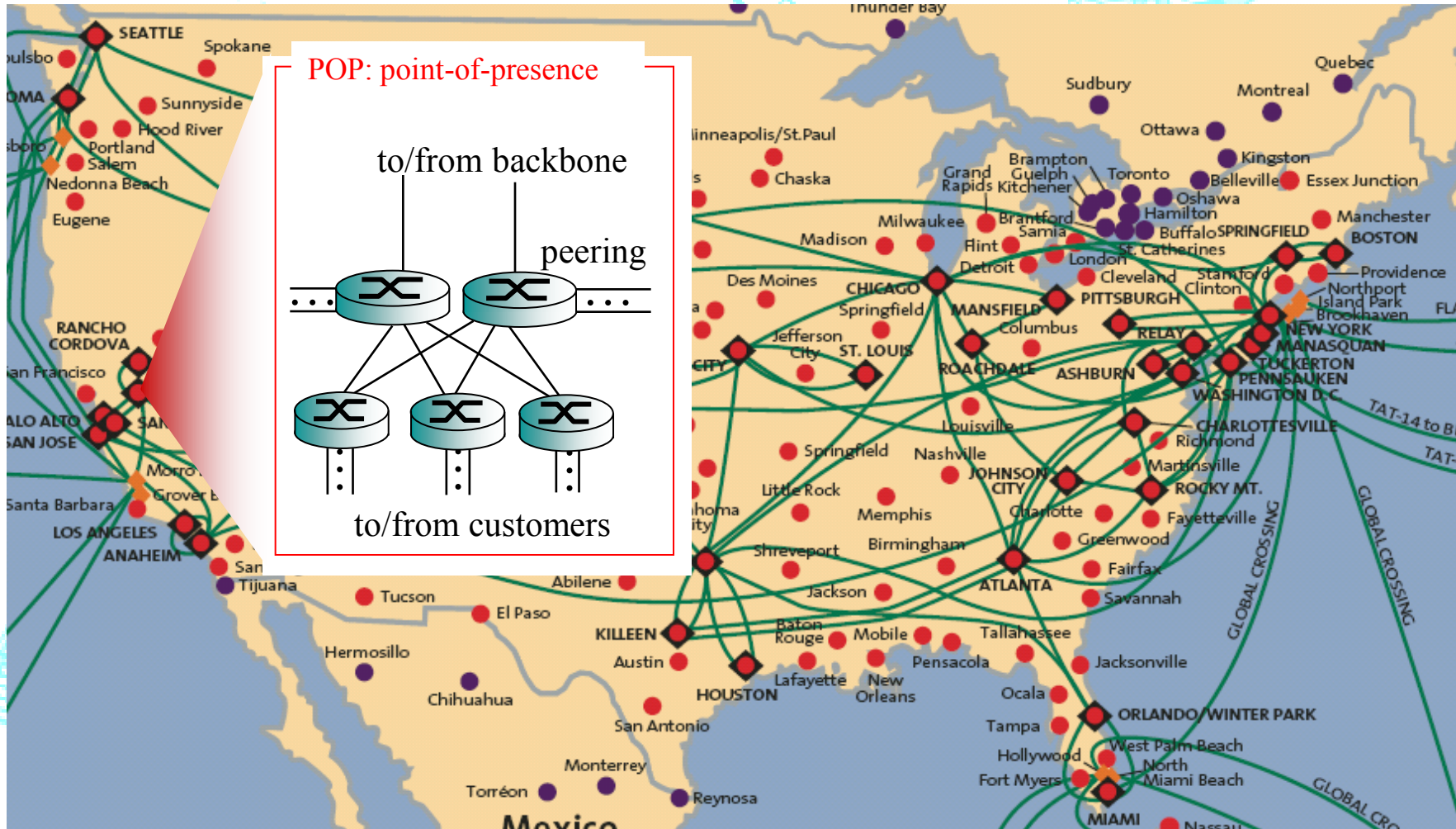
Internetin rakenne: Verkkojen verkko

- 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 ISP:t



Tier-1 ISP: e.g., Sprint



Chapter 1: roadmap

1.1 what *is* the Internet?

1.2 network edge

- end systems, access networks, links

1.3 network core

- packet switching, circuit switching, network structure

1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

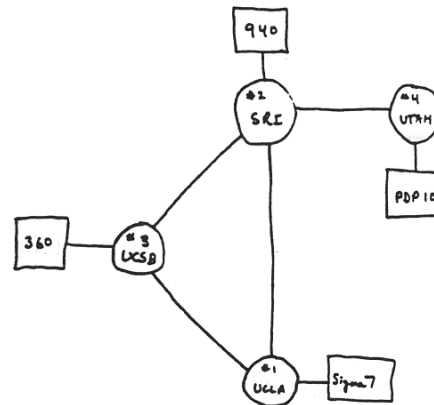
1.6 networks under attack: security

1.7 history

Internet history - Ei kokeessa

1961-1972: Early packet-switching principles

- **1961:** Kleinrock - queueing theory shows effectiveness of packet-switching
- **1964:** Baran - packet-switching in military nets
- **1967:** ARPAnet conceived by Advanced Research Projects Agency
- **1969:** first ARPAnet node operational
- **1972:**
 - ARPAnet public demo
 - NCP (Network Control Protocol) first host-host protocol
 - first e-mail program
 - ARPAnet has 15 nodes



THE ARPA NETWORK

Internet history - Ei kokeessa

1972-1980: Internetworking, new and proprietary nets

- **1970:** ALOHAnet satellite network in Hawaii
- **1974:** Cerf and Kahn - architecture for interconnecting networks
- **1976:** Ethernet at Xerox PARC
- **late70's:** proprietary architectures: DECnet, SNA, XNA
- **late 70's:** switching fixed length packets (ATM precursor)
- **1979:** ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless routers
- decentralized control

define today's Internet architecture

Internet history - Ei kokeessa

1980-1990: new protocols, a proliferation of networks

- **1983:** deployment of TCP/IP
- **1982:** smtp e-mail protocol defined
- **1983:** DNS defined for name-to-IP-address translation
- **1985:** ftp protocol defined
- **1988:** TCP congestion control
- new national networks: Csnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

Internet history - Ei kokeessa

1990, 2000's: commercialization, the Web, new apps

- early 1990's: ARPAnet decommissioned
- 1991: NSF lifts restrictions on commercial use of NSFnet (decommissioned, 1995)
- early 1990s: Web
 - hypertext [Bush 1945, Nelson 1960's]
 - HTML, HTTP: Berners-Lee
 - 1994: Mosaic, later Netscape
 - late 1990's: commercialization of the Web
- late 1990's – 2000's:
 - more killer apps: instant messaging, P2P file sharing
 - network security to forefront
 - est. 50 million host, 100 million+ users
 - backbone links running at Gbps

Internet history - Ei kokeessa

2005-present

- ~750 million hosts
 - Smartphones and tablets
- Aggressive deployment of broadband access
- Increasing ubiquity of high-speed wireless access
- Emergence of online social networks:
 - Facebook: soon one billion users
- Service providers (Google, Microsoft) create their own networks
 - Bypass Internet, providing “instantaneous” access to search, email, etc.
- E-commerce, universities, enterprises running their services in “cloud” (eg, Amazon EC2)