



Linkkikerros, tiedonsiirron perusteet

Jyry Suvilehto

T-110.1100 Johdatus tietoliikenteeseen ja
multimediatekniikkaan
kevät 2011

Luennon sisältö

1. Kertausta
2. Linkkikerros
3. Tiedonsiirron perusteet

Osa luennosta perustuu Tuomas Auran, Timo Kiravuon ja Jouni Karvon opetusmateriaaliin

Osa kaavioiden kuvista Public Domainia openclipart.orgin käyttäjiltä ARTMAN ja dur2250

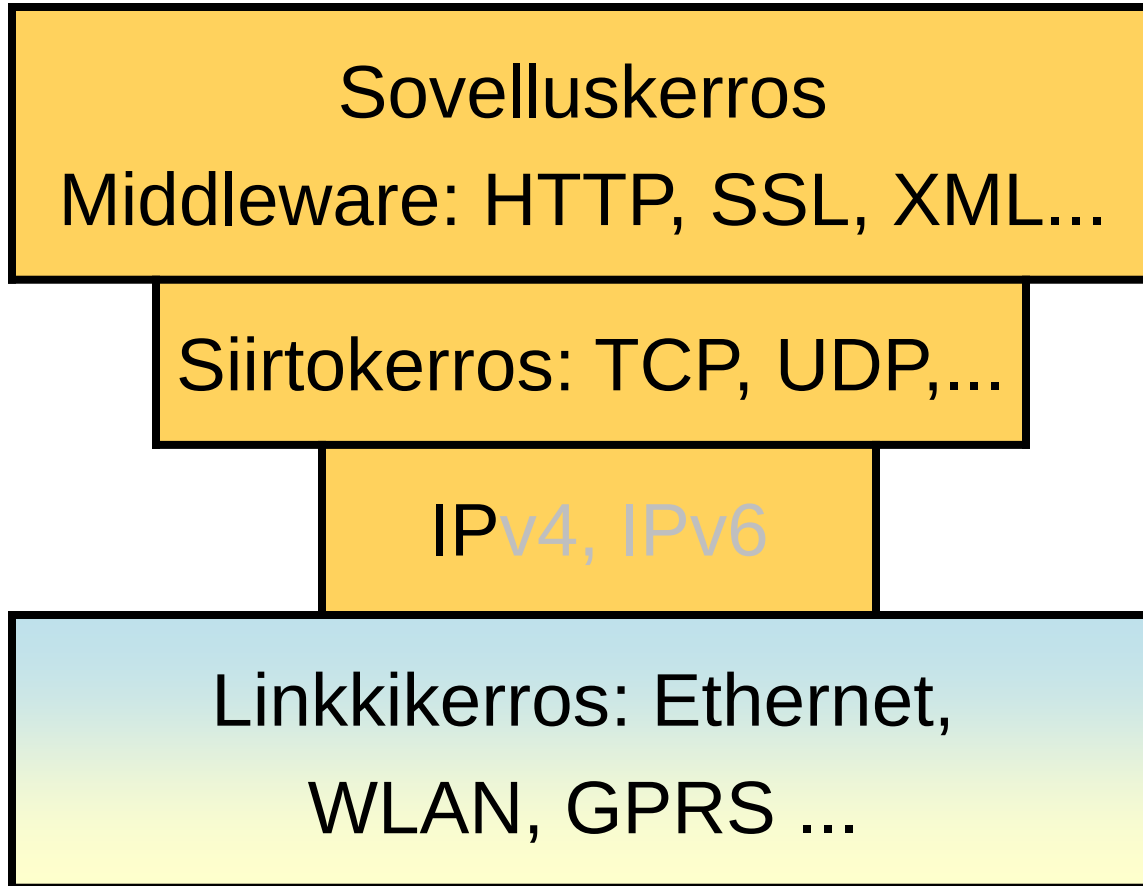
Viime luennolta

- UDP: Universal Datagram Protocol

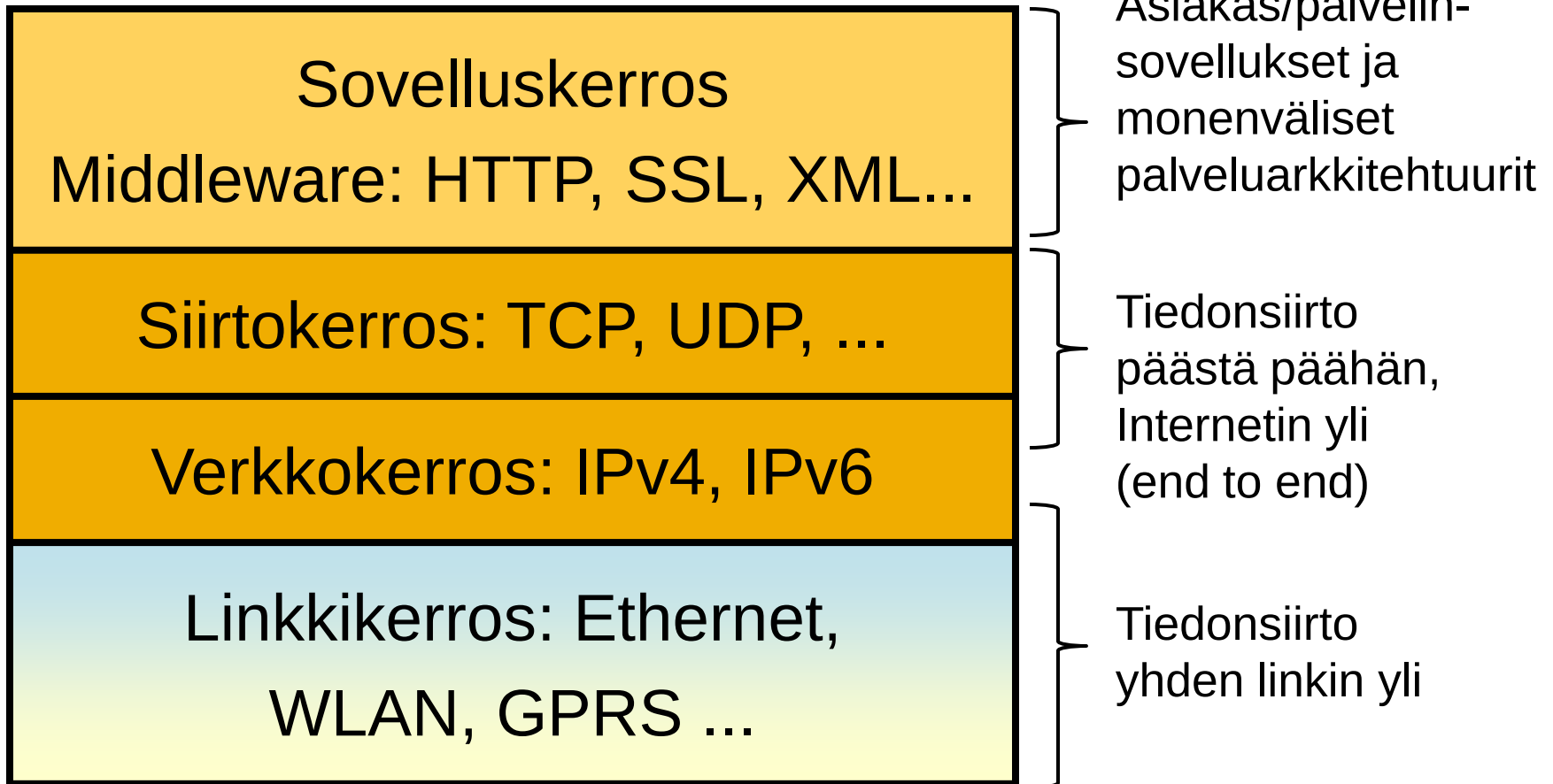
Lähdeportti (ohjelma)	Kohdeportti (ohjelma)
Paketin pituus	Tarkastussumma
Sisältö	

- Tarkastussumma (hash, checksum) lasketaan koko paketista ennaltamäärätyllä tavalla
 - Voidaan havaita jotkin virheet saapuneessa paketissa
- Tarkastussummaa ei ole pakko laittaa lähettäessä

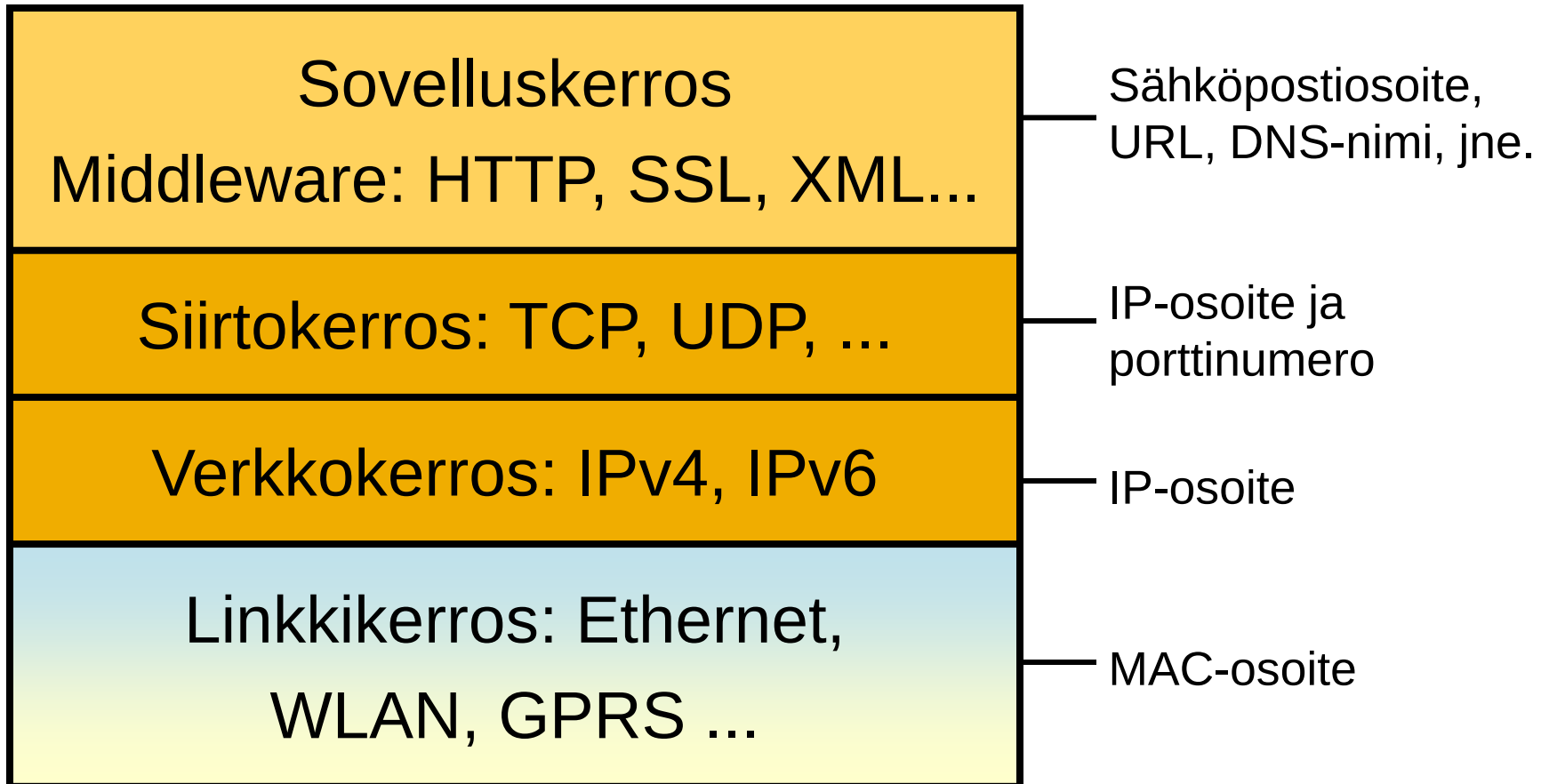
Tarina tähän asti



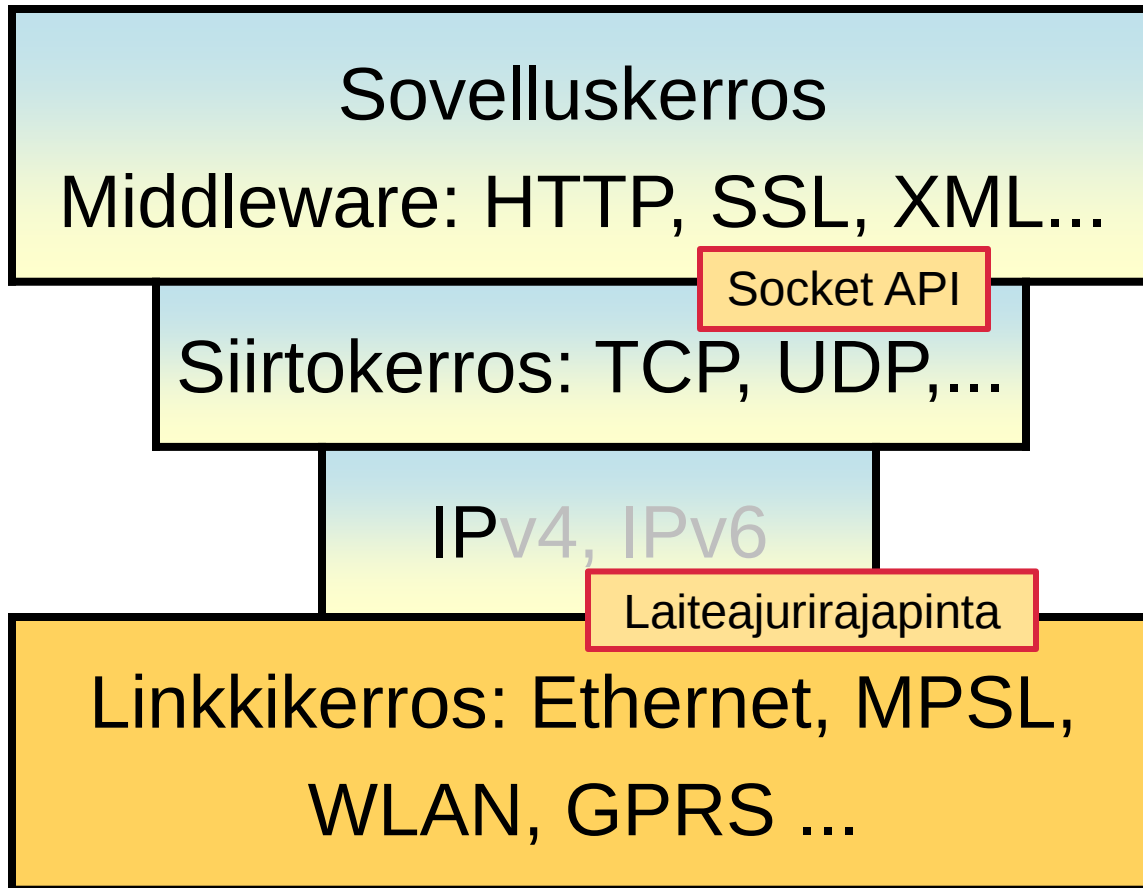
TCP/IP-protokollapino



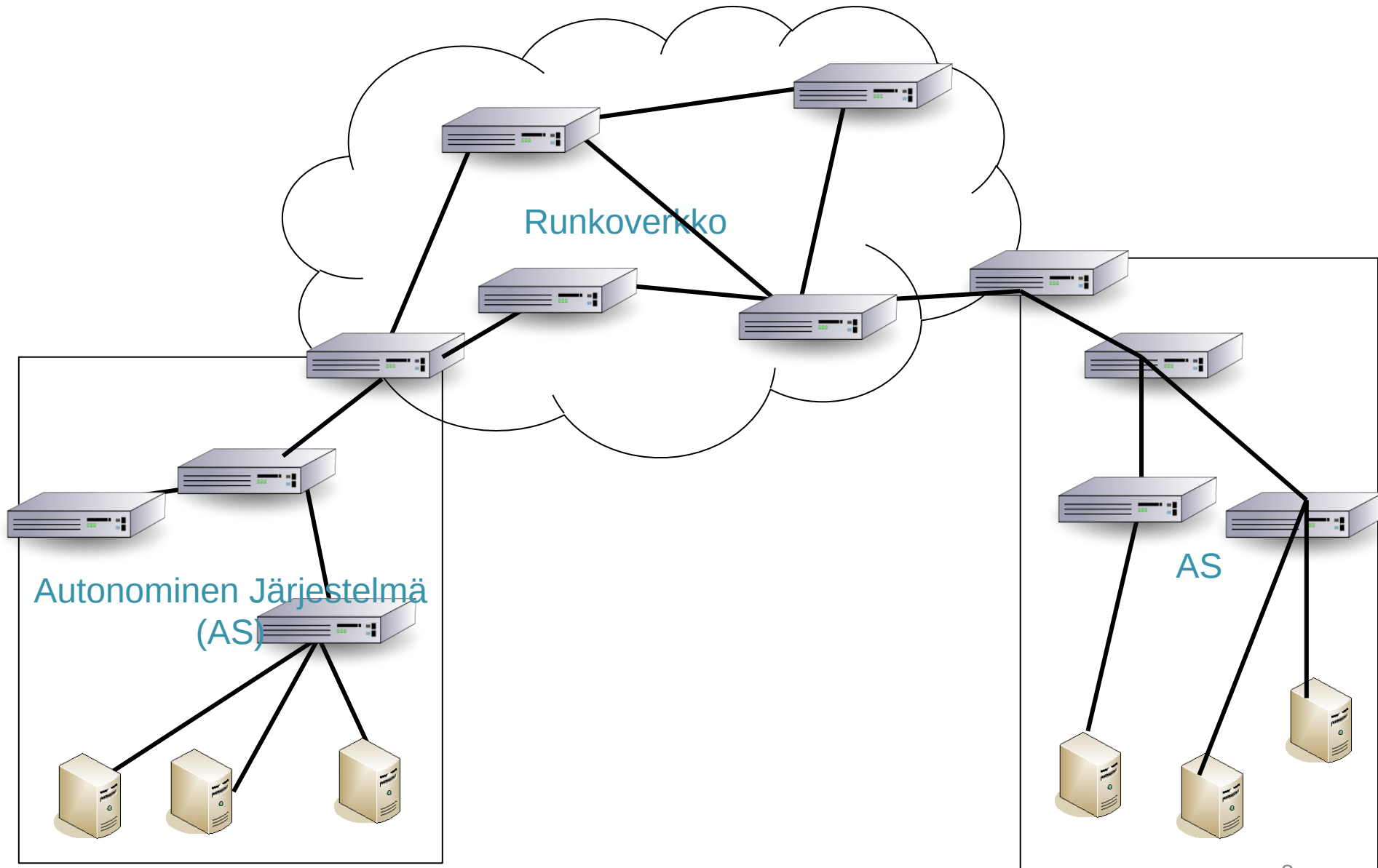
Nimiavaruudet



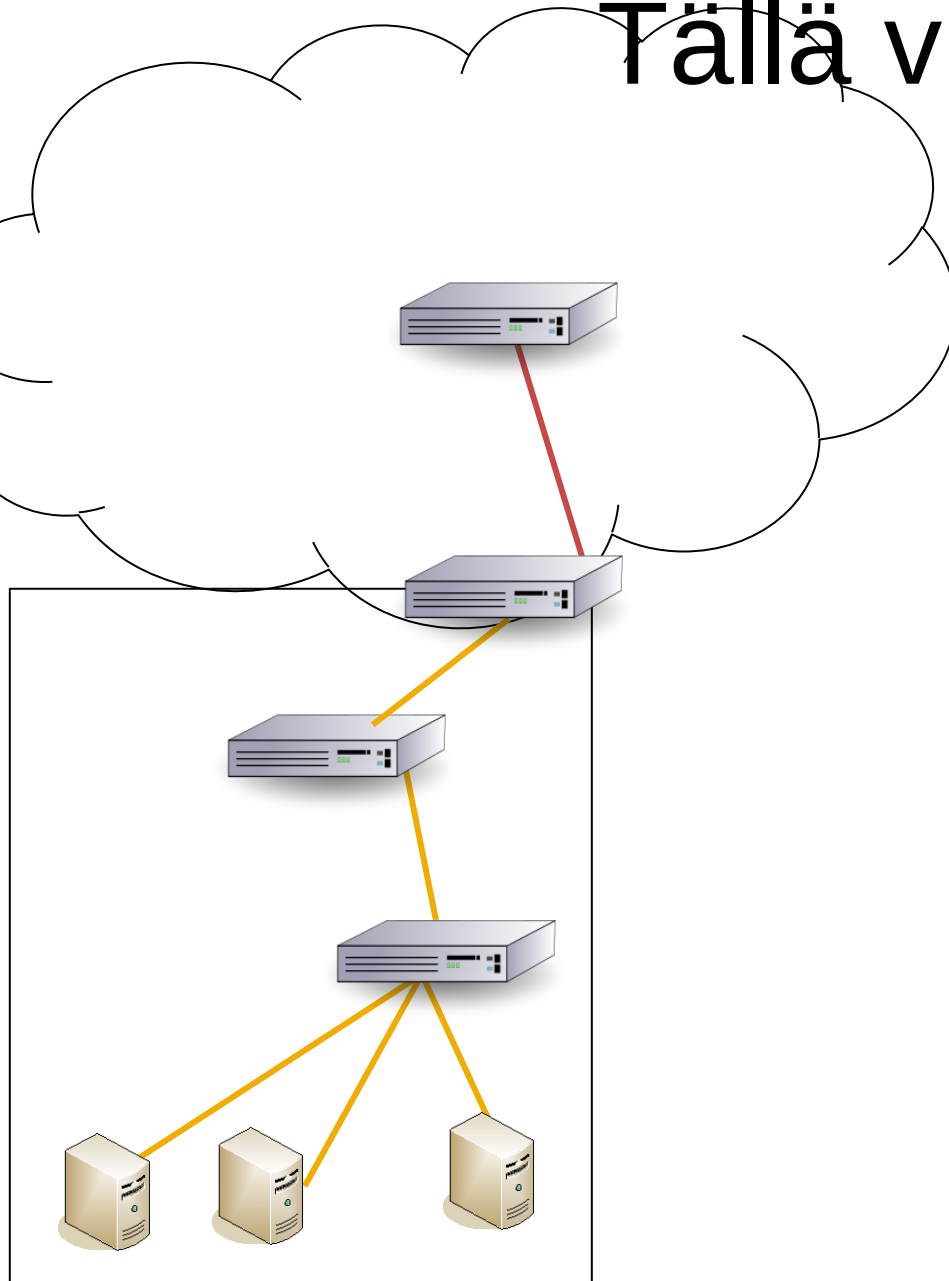
Linkkikerros



Viime viikolla



Tällä viikolla



- Linkkikerros tarjoaa tiedonsiirtoa yhden fyysisen tai loogisen linkin yli
- Ei yksimielisyyttä siitä, kuuluuko fyysinen datan siirto TCP/IP-stäckiin
- Kilpailevassa OSI-mallissa erikseen looginen linkki ja fyysinen linkki
 - Looginen = ”miltä se näyttää käyttäjältä”
 - Fyysinen = ”miten piuhat on vedetty”

Yhteys

- Kahden laitteen välinen yhteys voi olla
 - Simplex: yksisuuntainen. Kaksisuuntaiseen kommunikaatioon tarvitaan 2 simplex-linkkiä.
 - Half-Duplex: kaksisuuntainen, mutta vain toinen osapuoli voi puhua kerrallaan
 - Full-Duplex: samanaikainen kaksisuuntainen
- Full-Duplex-yhteyden voi rakentaa vain kahden pisteen välille
 - N noodin yhdistämiseen $\frac{n(n-1)}{2}$ yhteyttä
 - Yleensä käytetään kytkimiä, toistimia tai muita

Viestin rakenne tähän asti

Verkkokerros	Kuljetuskerros	Sovelluskerros	Varsinaisen data
IP-otsakkeet	TCP/UDP	HTTP, SMTP, VoIP, tjms protokolla luotettavan tavuvirran tai datagrammiyhteyden päällä	Esim. Html-sivu, sähköpostiviesti

- Jokainen protokollataso kuljettaa tiimalasimallissa ylempien protokollien otsake- ja muita tietoja
- Jokainen voitaisiin rakentaa vastaavaa palvelua tarjoavan toisen protokollan päälle
 - <http://tools.ietf.org/html/rfc1149>

Viesti tällä viikolla

Linkkikerros	Verkkokerros	Kuljetuskerr os	Sovelluskerros	Varsnii nen data
Ethernet- kehys, tjms	IP- datagrammi	TCP/UDP- paketti/datagr ammi	HTML, SMTP, jne protokollan otsakkeet	Esim. Html- sivu, sähköpos tiviesti

- Linkkikerros lisää monipuolisuutta monotonisen IP:n alapuolelle
 - Ethernet
 - Wlan
 - DSL
 - ISDN
 - Etc.
- Tiimalasimallin toinen leveä kohta

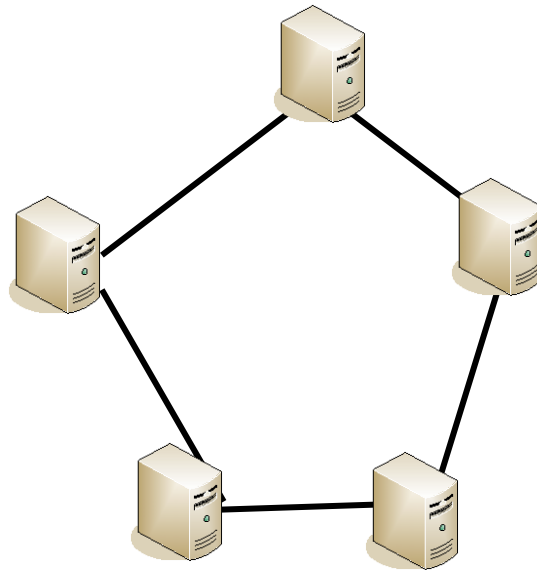
Overhead

Linkkikerros	Verkkokerros	Kuljetuskerr os	Sovelluskerros	Varsinai nen data
Ethernet- kehys	IP- datagrammi	TCP/UDP- paketti/datagr ammi	HTML, SMTP, jne protokollan otsakkeet	Esim. Html- sivu, sähköpos tiviesti

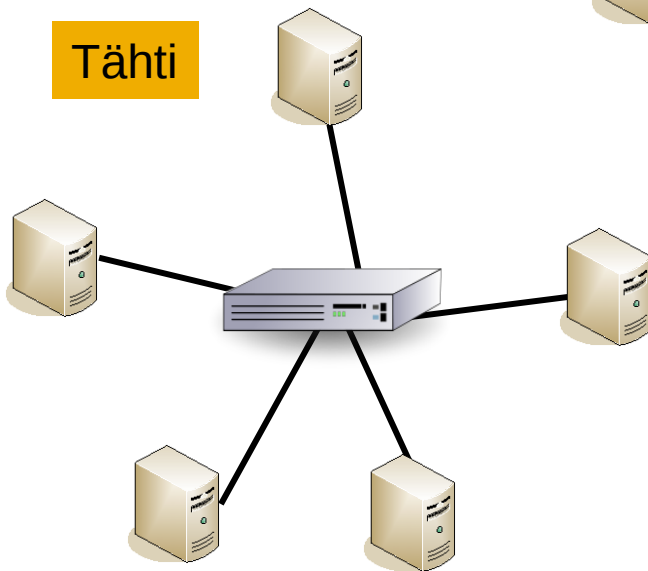
- Jokainen tietoliikenneprotokolla aiheuttaa overheadia (suom. yleiskustannus)
- Overheadia voi olla yllättävän paljon (mahdollinen rästitehtävä)
- Toisaalta overhead on välttämätöntä

Verkkotopologioita

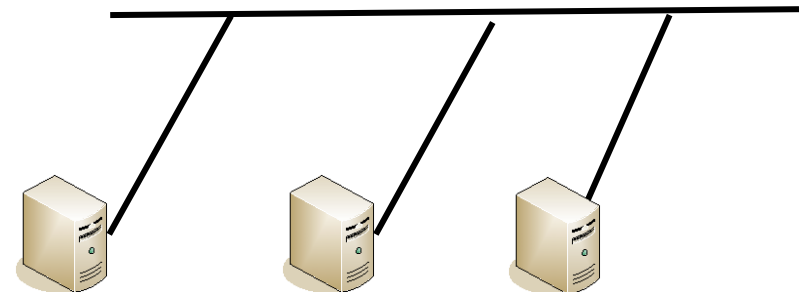
Rengas



Tähti



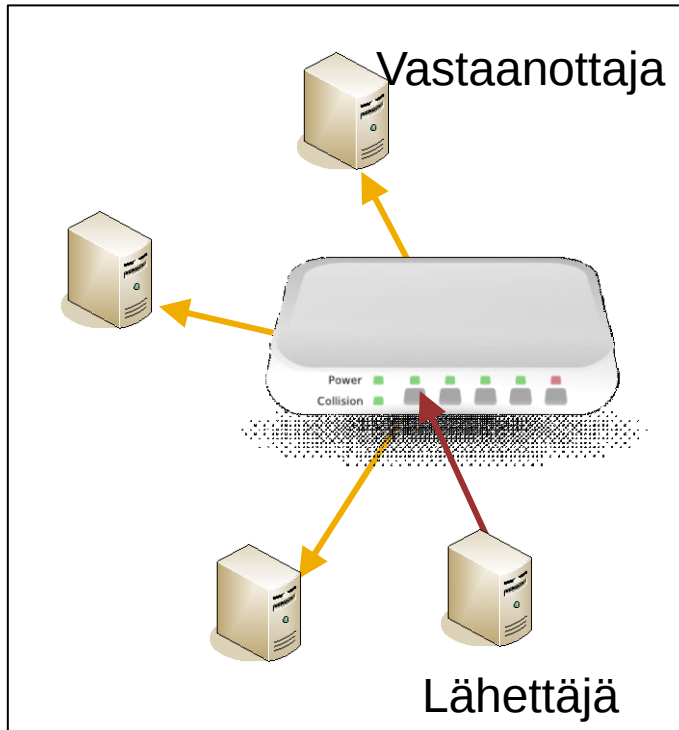
Väylä



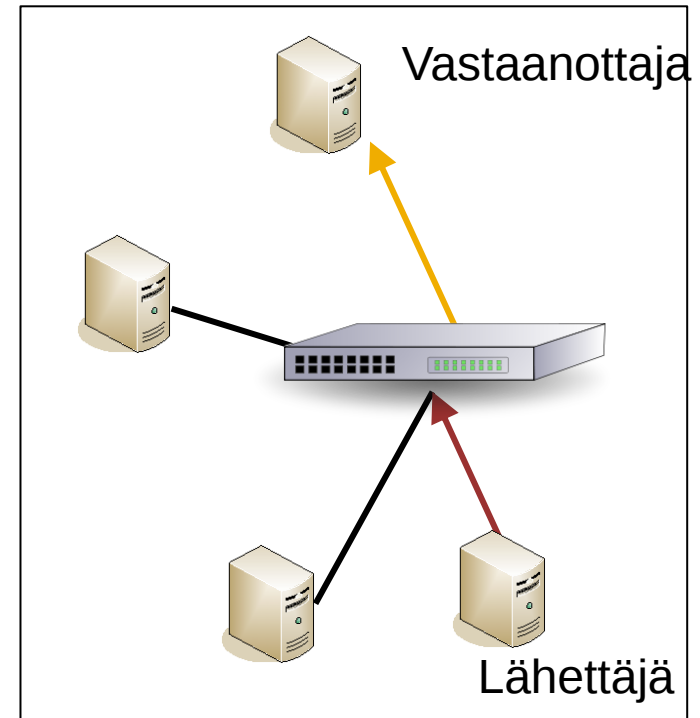
Yleisiä verkkotopologioita

- Johdinverkot ovat rakenteeltaan joko renkaita, tähtiä, väyliä tai edellisten hybridejä
- Rakenteet käytössä kaikessa tiedon siirtämisessä
 - Väylä on yleinen tietokoneiden sisällä
 - Ns. Network on a Chip (NOC) –tyyppiset tietokoneet kuuma tutkimusaihe
- Verkkotopologia voi olla erilainen fyysisesti ja loogisesti
 - Esimerkiksi keskittimellä toteutettu ethernet on fyysisesti tähti, loogisesti väylä

Hub/Switch



- Hub eli keskitin lähettää saamansa kehykset kaikkiin suuntiin



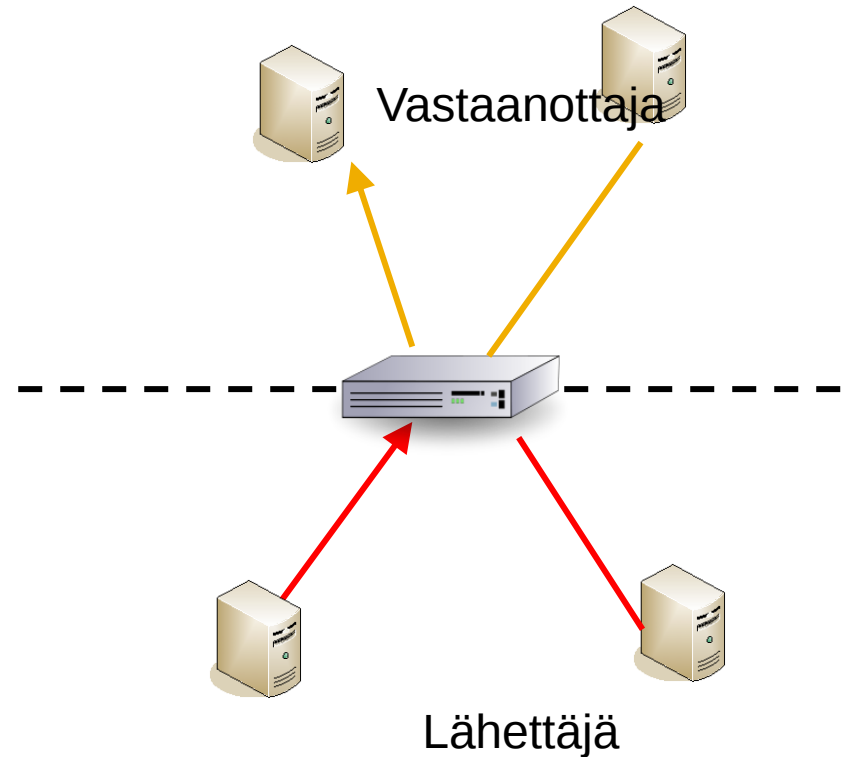
- Switch eli kytkin lähettää saamansa kehykset vain oikeaan suuntaan

Hub/Switch

- Hub on tyhmä toistin
 - Halpa
 - Lörppö
 - Ruuhkautuu helposti (törmäyksiä)
 - Ei kauheasti enää
- Switch on fiksumpi
 - Kalliimpi, pitää muistaa missä mikäkin kone on
 - Ei tarpeettoman lörppä
 - Ruuhkasietoisempi

Router

- Reititin on laite, joka on kiinni kahdessa eri verkossa
- Verkot voivat olla fyysisesti erilaisia (esim. ADSL ja Ethernet, WLAN ja Ethernet)
- Reititin siirtää viestejä verkosta toiseen



Ethernet

- Yleisin lähiverkoissa (Local Area Network, LAN) käytetty teknologia
- IEEE 802.3
- Loogisesti väylä
- Vain yksi laite voi lähettää väylälle kerrallaan
- Laitteet eivät tiedä koska muut haluavat lähettää
- Erillinen protokolla määrittelee miten toimitaan
 - Media Access Control (MAC)

Ethernet-kehys

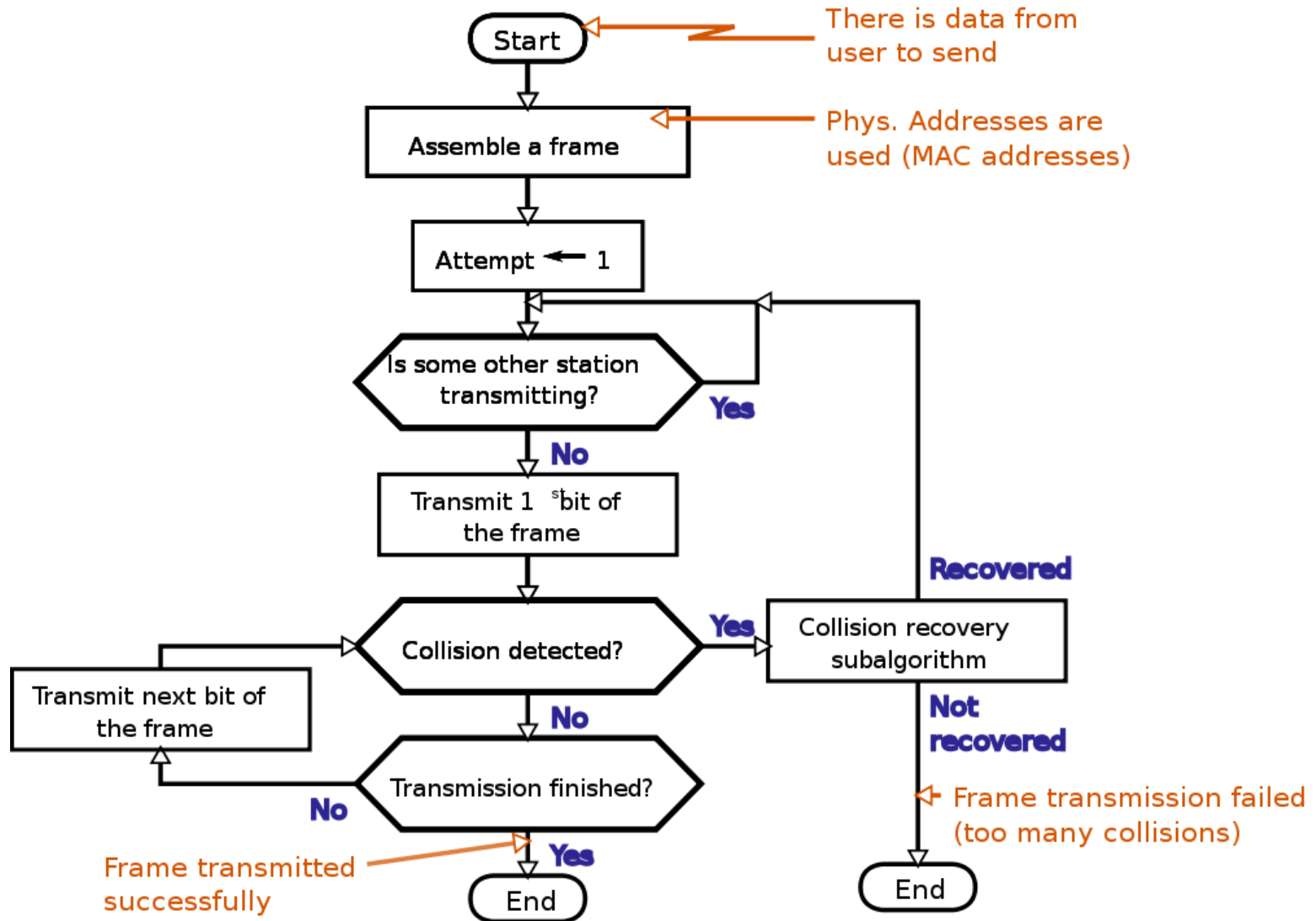
Lähettäjä	Kohde	Kehystetty protokolla	Data	CRC-tarkastussumma
00:26:82:16:df:04	ff:ff:ff:ff:ff:ff	0x0800 (IP)	...	1234

- Ethernet-kehys rikkoo kerrosmallia, koska se on kiinnostunut päälläolevasta protokollasta
- Toisaalta, ethernetin päälle voidaan rakentaa muitakin kuin IP-verkkoja

Media Access Control

- MAC-osoite määrittää yksikäsitteisesti väylän varrella olevan laitteen
 - Uniikki koko maailmassa
 - Jokaisella verkkolaitteella (BT, Wlan, whatnot)
 - Esim. 00-FF-3A-D0-C9-18
 - Tunnetaan myös nimellä Physical Address
- Carrier Sense Multiple Access With Collision Detection (CSMA/CD)-protokolla määrittelee miten Ethernet-verkkoon saa lähettää

CSMA/CD



Token Ring

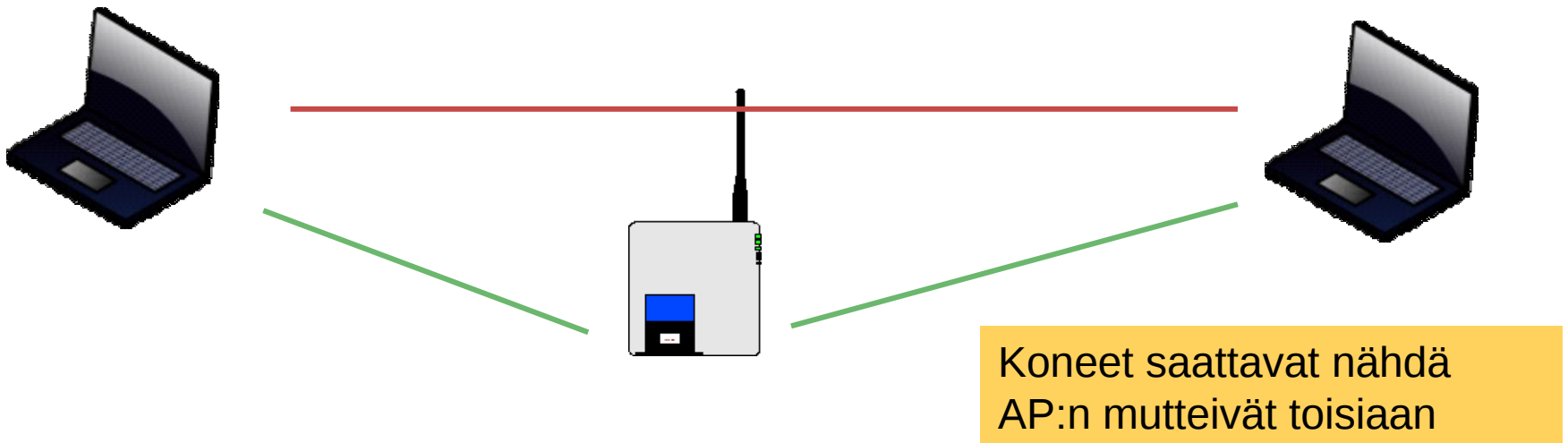
- Ennen Ethernetiä käytettiin yleisesti token ring –lähiverkkoprotokollaa
- Kun kukaan ei lähetä varsinaista dataa, erityistä Token-kehystä lähetetään vuorotellen kaikille laitteille
 - Laite saa lähettää vain silloin kun se on saanut Token-kehysten eikä ole vielä vastannut
 - Laite ilmaisee olevansa valmis lähettämällä Token-kehysten

WLAN

- IEEE 802.11 –perheen protokollat määrittelevät langattoman lähiverkon
- Radioaallot eroavat olennaisesti johtimesta
- Monotonisuuden rikkova tuotemainos
 - <http://www.thinkgeek.com/tshirts-apparel/interactive/bd12/>
- ns. Hidden node –ongelma
- Infrastructure mode kun on tukiasema (Access Point)
- Ad Hoc mode kun halutaan yhdistää ilman AP:tä (harvoin käytössä)

CSMA/CA

- Hidden node –ongelman takia langattoman verkon noodit eivät voi toimia kuten Ethernetissä
- Ratkaisuna jokainen pyytää vuorollaan access pointilta lupaa lähettää



WPA/WEP

- Wlan on ohjaamaton media
 - Kuka tahansa voi kuunnella
- Salausta tarvitaan
- WEP (Wired-Equivalent Privacy) vanha, viallinen ratkaisu
- WPA (Wi-Fi Protected Access) parempi, ei vieläkään täydellinen
- Yksityiskäyttäjille jaettu salaisuus
- Monimutkaisemmissa konteksteissa erillinen autentikaatio
 - eduroam

DHCP

- Dynamic Host Control Protocol mahdollistaa verkkoon liitetyn koneen osoitteen automaattisen määrittämisen
 - Pitää olla osoitteita tarjoava palvelin
- Liitetty kone huutaa linkkikerroksen broadcast-osoitteeseen ja kysyy, haluaisiko joku antaa IP-osoitteen
- Osoitteen mukana usein tulee mm. verkon koko (netmask), oletusreititin, DNS-nimipalvelimien osoitteita

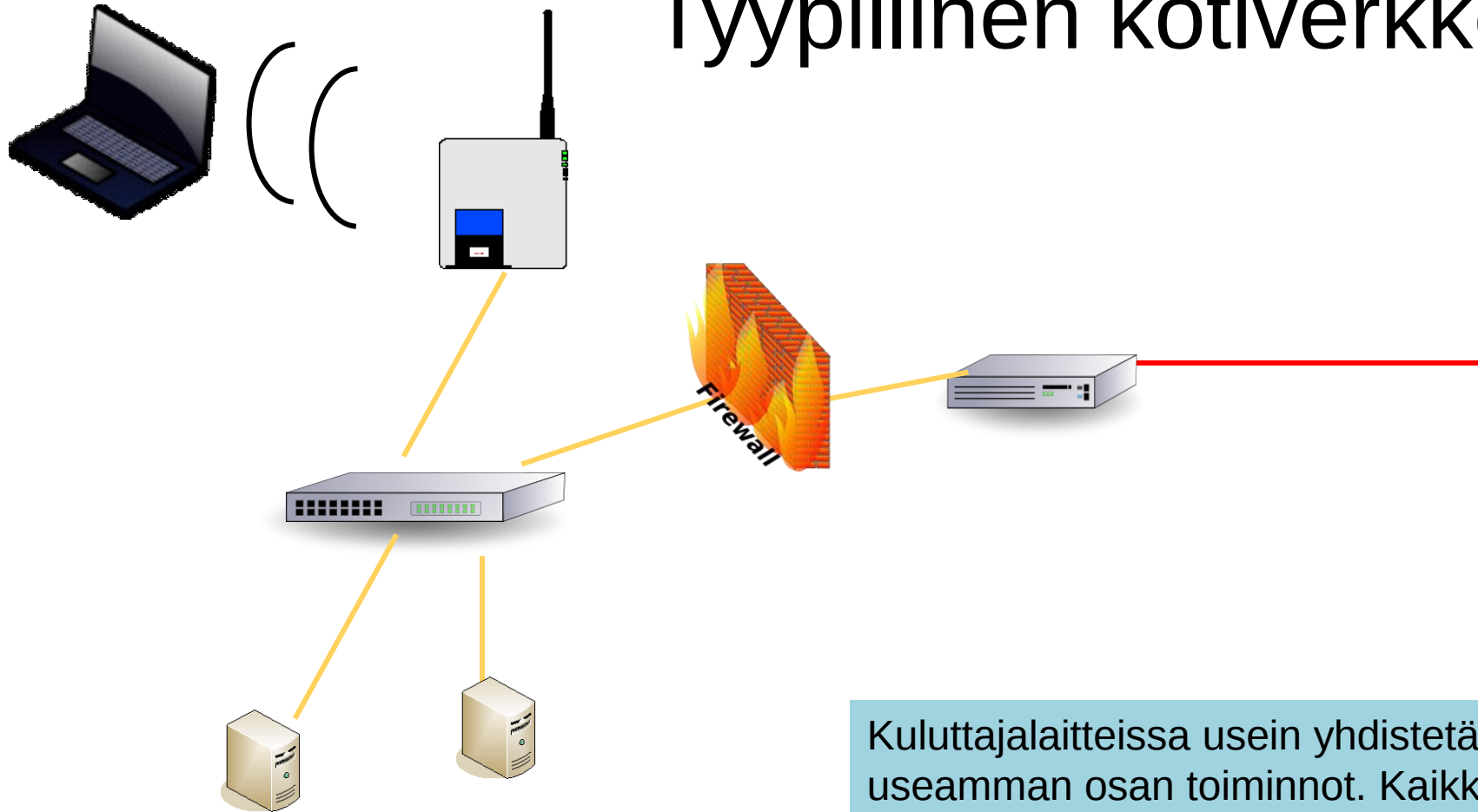
DHCP - ongelmia

- Verkossa voi olla monta DHCP-palvelinta, keneen luottaa?
 - Tietoturvaongelma esim. lentokentillä
 - Ärsyttävää taloyhtiön verkossa
- DHCP:n jakamat osoitteet (usein) vaikeasti ennustettavissa
 - DHCP:llä IP:n saaneen koneen on vaikea olla asiakas-palvelin mallin palvelin
 - Jaetut osoitteet usein yksityisissä IP-avaruuksissa (NAT), porttien edelleenohjaus ja reiät palomuriin iso ongelma
 - Osittain ratkennut UPnP:llä, suurimmalta osalta ei

ARP

- Address Resolution Protocol (ARP) auttaa verkossa olevaa laitetta löytämään IP-osoitetta vastaavan MAC-osoitteen
- Mikäli kohde ei ole samassa verkossa (kone tietää netmaskin), lähettäjä lähettää IP-datagrammin oletusreitittimelle, joka huolehtii sen eteenpäin

Tyypillinen kotiverkko



Kuluttajalaitteissa usein yhdistetään useamman osan toiminnot. Kaikki toiminnallisuudet voi saada yhdessä laitteessa

TIEDONSIIRRON PERUSTEET

Data ja Informaatio

- Data: kuvat, luvut, kirjaimet ilman merkitystä
- Informaatio: datan merkityssisältö (ihmisen kasvot, hinta, geenin emäsparijärjestys)
- Tieto on ihmisen ymmärrystä informaatiosta (tuote on kallis)
- Tämä kalvo tulee uudestaan parin viikon kuluttua

Tiedon esitys

- Tietokoneissa informaatio on esitetty binäärimuodossa
 - Joskus binääri on esitettävissä merkkeinä, esim. tekstipohjaiset protokollat
- Sama informaatio voi viedä vaihtelevan määrän tilaa → Häviötön pakkaus
- Joskus informaatiota ei pyritä säilyttämään kokonaan → Häviöllinen pakkaus
- Tämä kalvo tlee uudestaan parin viikon kuluttua

Tiedon siirto

- Tietoliikenteessä yleensä pyritään siirtämään informaatio häviöttömänä
- Tietokoneille virheetön datasiirto tarpeellista informaation välittymiseksi
 - Ihmisille aina ei
- Esimerkiksi puhe häiriöisen radioyhteyden yli
 - Data saattaa olla korruptoitunutta, mutta viestin informaation sisältö todennäköisesti menee perille

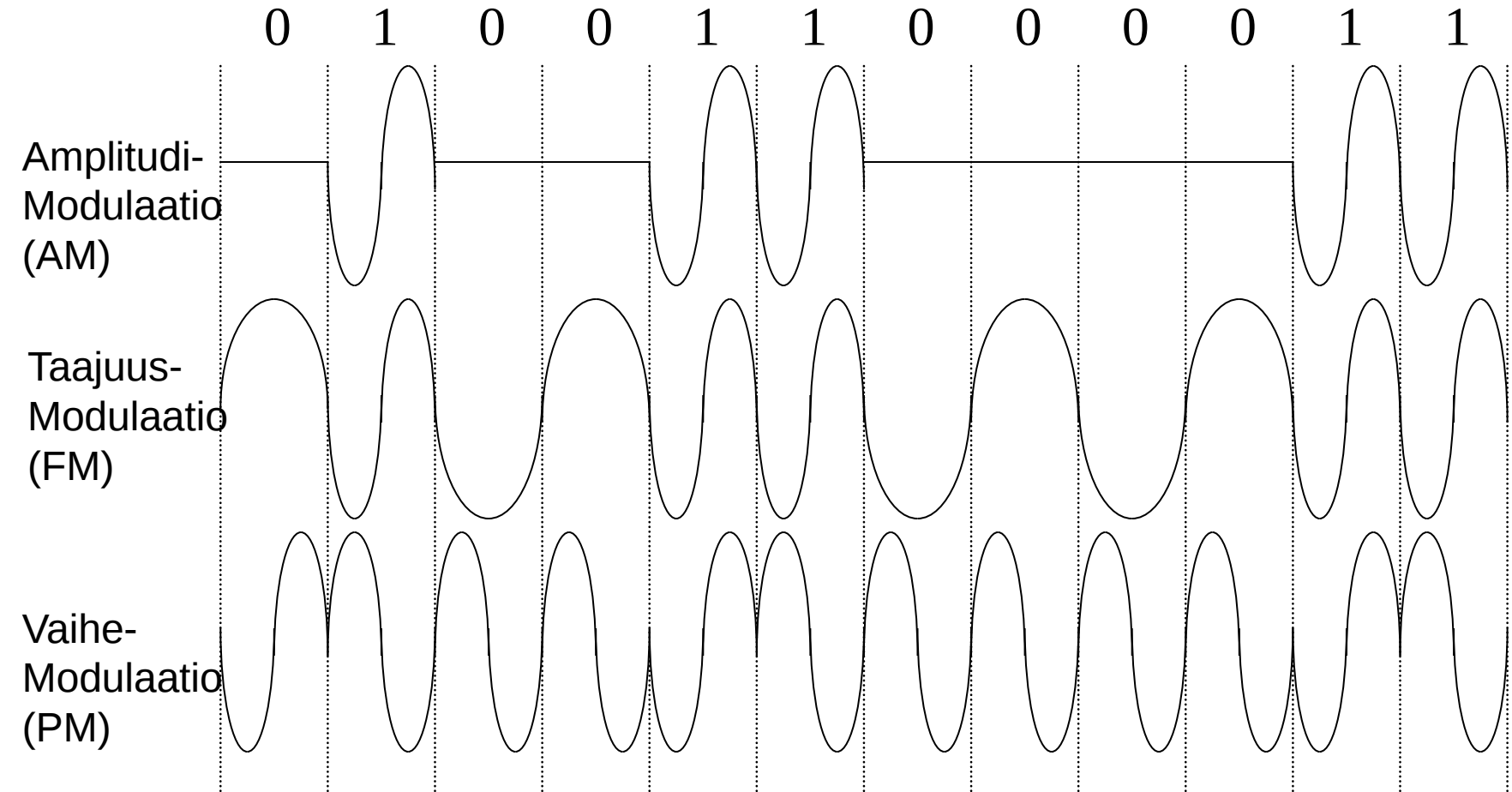
Tiedonsiirtomediat

- Ohjattu media
 - Kuparijohto
 - Parikaapeli
 - Koaksiaalikaapeli
 - Massatallennusvälineet
- Ohjaamaton media
 - Sähkömagneettinen säteily
 - Painevaihtelut (ääni)
- Olennaista:
 - Vastaanottajien määrä
 - Lähetteen ”säteily”

Bitin siirto median yli

- Bitit on koodattava jotenkin
- Kantataajuusmenetelmässä bitit muutetaan suoraan esim. jännitteeksi, toimii yhteyksillä, joissa on suhteellisen vähän häiriöitä
- Häiriöisillä yhteyksillä kantoaalto auttaa erottamaan signaalin taustakohinasta, signaali muokkaa kantoaaltoa
 - Amplitudimodulaatio (AM)
 - Taajuusmodulaatio (FM)
 - Vaihemodulaatio (PM)
- Nykyään on myös monimutkaisempia koodauksia
 - Esim. UMTS:n käyttämä CDMA

Modulaatio



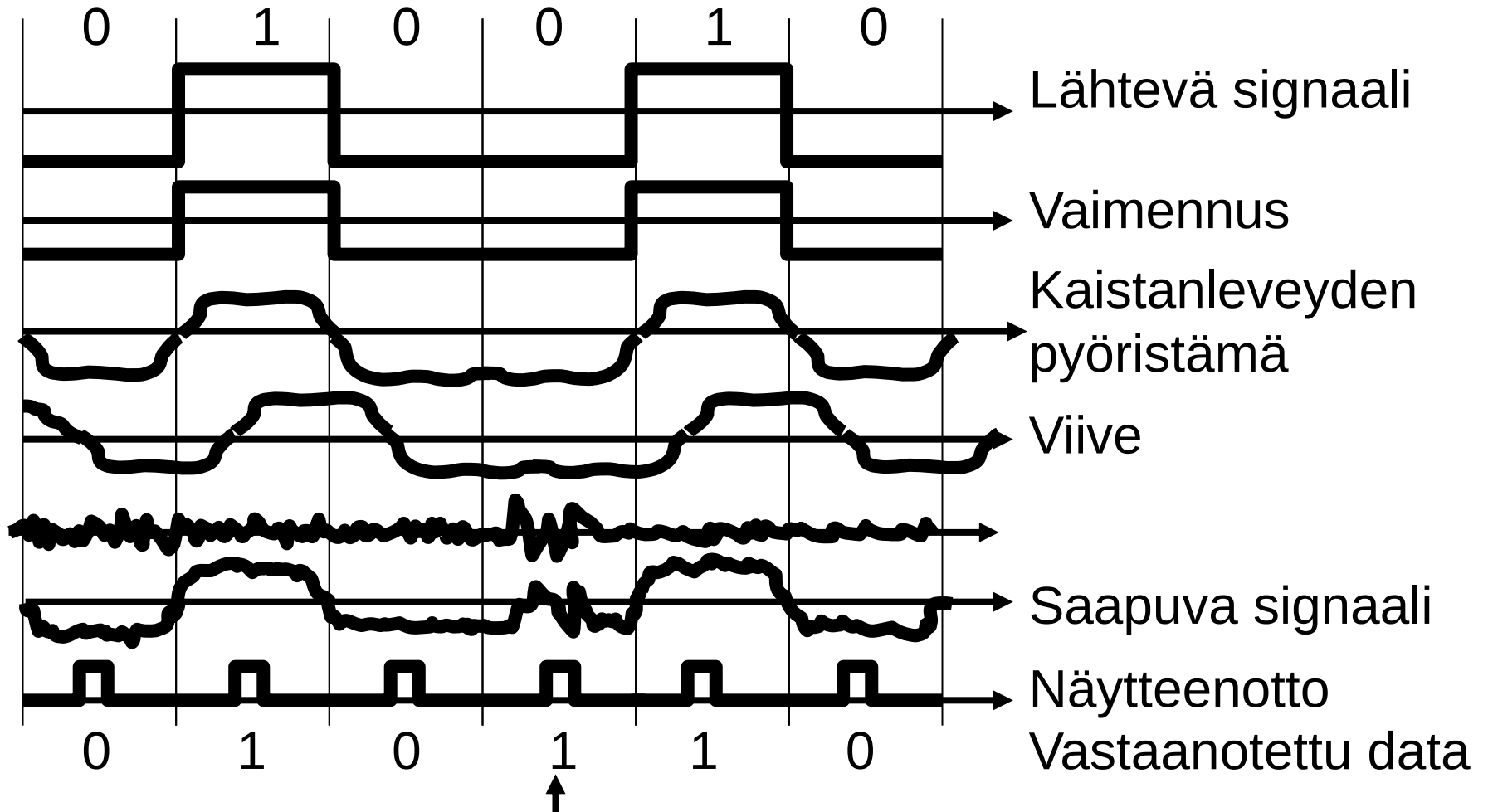
Synkronisaatio

- *Denuntiato solum translata valet* = vain vastaanotettu viesti merkitsee
- Vastaanottajan pitää siis tunnistaa data
- Synkronoimattomassa tiedonsiirrossa vastaanottaja tunnistaa viestin (yksi tavu dataa) alun ja ottaa näytteitä riittävän usein saadakseen viestin
 - Esim. start-bitti, 8 databittiä, pariteetti ja stop-bitti
 - Ethernetissä viesti alkaa ykkösillä
- Synkronoidussa tiedonsiirrossa lähettäjällä ja vastaanottajalla on kellot samassa ajassa, vastaanottaja tietää milloin bitin pitäisi tulla
 - Tehokkaampaa
 - Kellojen synkronointi vaikeaa

Siirtotien laatu

- Kaistanleveys (bandwidth)
 - Käytettävissä oleva taajuusalue
- Kohina (noise)
 - Taustalla olevat häiriösignaalit, joista viesti on erotettava
- Siirtokapasiteetti (capacity)
 - Montako bittiä sekunnissa saadaan siirrettyä (lasketaan edellisistä)
- Virhetaajuus (error rate)
 - Montako databittiä sekunnissa muuttuu
- Viive (latency)
 - Kauanko bitiltä kestää matkata päästä päähän
- Huojunta (jitter)
 - Perättäisten viestien aikavaihtelut
- Vaimennus (attenuation)
 - Kuinka usein signaalia on vahvistettava (riippuu mediasta)

Signaali matkalla



AD

- Vastaanottopäässä tehtävä muunnos analogisesta digitaaliseen
- Sama muunnos tehdään otettaessa digikuvaa, nauhoitettaessa musiikkia tietokoneelle
- Ei käsitellä tässä, koska sopii paremmin toisaalle

Kohinasuhde

- Analogisissa siirtoteissä on aina erilaisia häiriöitä
- Signaalinvoimakkuuden suhde kohinan voimakkuuteen on hyvin tärkeä mitta siirtotien laadulle
 - SNR, Signal to Noise Ratio
- Ilmaistaan yleensä desibeleissä
- Esim. jossain analogisessa puhelinverkossa voidaan mitata signaalin olevan 10 000 kertaa taustakohinaa voimakkaampi
 - Tällöin SNR on $10 \log_{10} 10000 = 40 \text{ db}$
- Ihmiskorva selviää vielä noin 0 db:n SNR:stä

Kaistanleveys ja kapasiteetti

- Kaistanleveys tarkoittaa tietyn kanavan läpäisevää taajuusaluetta
 - Tyypillisesti siirtotien sähköiset ja optiset ominaisuudet määrittävät lähetettävälle pulssille tietyn minimipituuden, jotta se voitaisi havaita luotettavasti vastaanottopäässä
 - Pulssin minimipituudesta saadaan vastaava korkein taajuus, joka voidaan siirtää
 - Ilmaistaan Hertzeinä, Hz
- Kapasiteetti on tietyn kanavan läpi siirrettävän datan määrä
 - Ilmaistaan bitteinä sekunnissa, b/s
- Nyquistin kaava tiedonsiirrolle on
$$r_{\max} = 2 W \log_2 L$$
 - $r_{\max}$ on suurin saavutettava bittien siirtokapasiteetti
 - W on ideaalikanavan kaistanleveys
 - L on signaalitasojen määrä
- Puheessa kapasiteetti sekoitetaan helposti kaistanleveyteen, koska niiden välillä on riippuvuus
- Riippuvuus ei ole kaksisuuntaista

Realistinen kaistanleveys

- Käytännön kanavilla on kohinaa, joka rajoittaa signaalitasojen määrää
- Shannonin kaava kanavakapasiteetille on
$$C = W \log_2 (1 + \text{SNR}) \text{ b/s}$$

C on kanavan siirtokapasiteetti b/s
W on kaistanleveys
SNR on kanavan signaali/kohinasuhde

 - jos ilmaistu desibeleinä: $10^{(\text{SNR}/10)}$

– Signaalitasojen määrä ei vaikuta, kaava määrittelee suurimman mahdollisen bitinsiirtokapasiteetin

Ensi viikolla

- Tietoturvallisuuden perusteet
 - Miksi tietoturva-asiantuntijoilla on aina haus Kempaa?
 - Mistä CIA on lyhennetty?
 - Mikä on Oodin tärkein tietoturvaominaisuus? Entä Nopan?
 - Miksi Aalto-yliopiston uusi salasananpolitiikka on huono?