



Aalto-yliopisto
Teknillinen korkeakoulu

Kertausluento

Tuomas Aura

T-110.2100 Johdatus tietoliikenteeseen
kevät 2010

Kurssin luennot

- Aloitus: Miten Internet toimii, Tuomas Aura
- Web 2.0 ja uudet sovellustekniikat, Tancred Lindholm
- Sovelluskerros: WWW, email, socket API, Tancred Lindholm
- Tietoturvan perusteet, Tuomas Aura
- Salaustekniikat, Tuomas Aura
- Kuljetuskerros, TCP, Matti Siekkinen
- Verkkokerros, IP, Matti Siekkinen
- Linkkikerros, Ethernet ja WLAN, Jouko Kurki
- Tiedonsiirron perusteet, Jouko Kurki
- Soluverkot, Jukka K. Nurminen
- Puhelinverkot, Jouko Kurki
- Tele- ja tietoverkon laskutus, Sakari Luukkainen
- Liiketoiminta verkkoympäristössä, Sakari Luukkainen
- Yhteenveto/kertaus, Tuomas Aura

Outline

1. Esimerkki protokollista
2. Protokollapino
3. Standardit
4. Internet, tiedonvälitys ja yhteiskunta
5. Tietoliikenneohjelmistojen opiskelu

Webmail

<https://webmail.tkk.fi/>

Mail :: Opetus/T-110.4200 Tietoturva - Mozilla Firefox

File Edit View History Bookmarks Tools Help

tkk.fi <https://webmail3.tkk.fi/index.php?Horde=41029921573f7c3752d4360b8d6ce093>

Mail :: Opetus/T-110.4200 Tietoturva

Open Folder T-110.4200 Tietoturva

Inbox Empty Trash New Message Folders Search Fetch Mail Options Problem Help Log out

Quota status: 337.97MB / 1024.00MB (33.01%)

Opetus/T-110.4200 Tietoturva 1 to 3 of 3 Messages

Select Mark as: Move | Copy Messages to

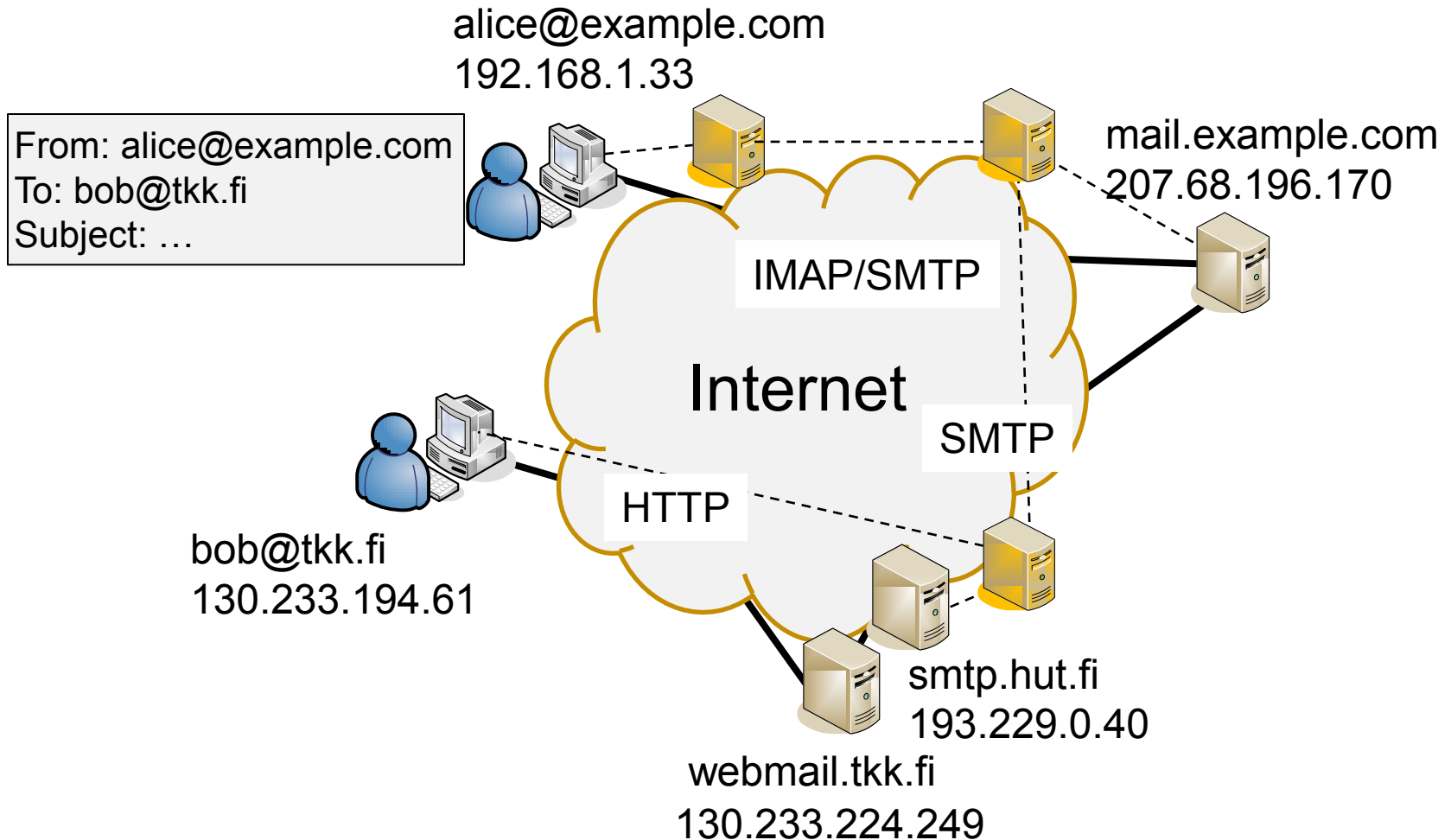
Delete | Forward | View Messages

	#	Date	From	Subject [Thread]	Size
☐	3	8 Oct 2009	Timo Kiravuo	Re: Laitoin kalvot Noppaan	3 KB
☐	2	6 Oct 2009	Timo Kiravuo	Keskiviikon SSL T1 14-16	3 KB
☐	1	9 Jun 2009	Timo Kiravuo	tietoturva syksy 2009 T-110.4200 kehitysajatuksia	3 KB

Unseen Answered Important Deleted Draft Personal

Done

Internetin sähköposti



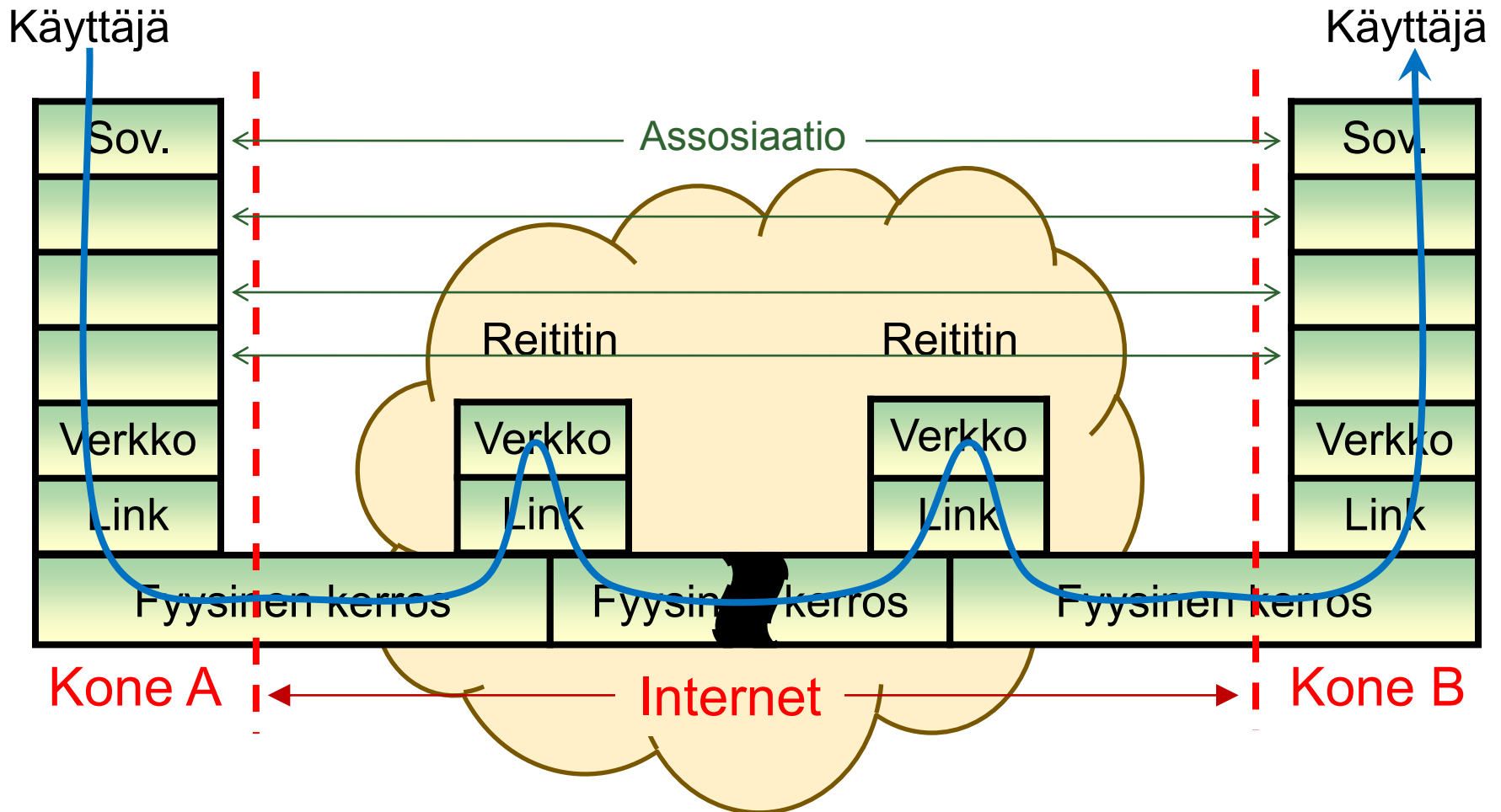
PROTOKOLLAPINO

OSI-malli

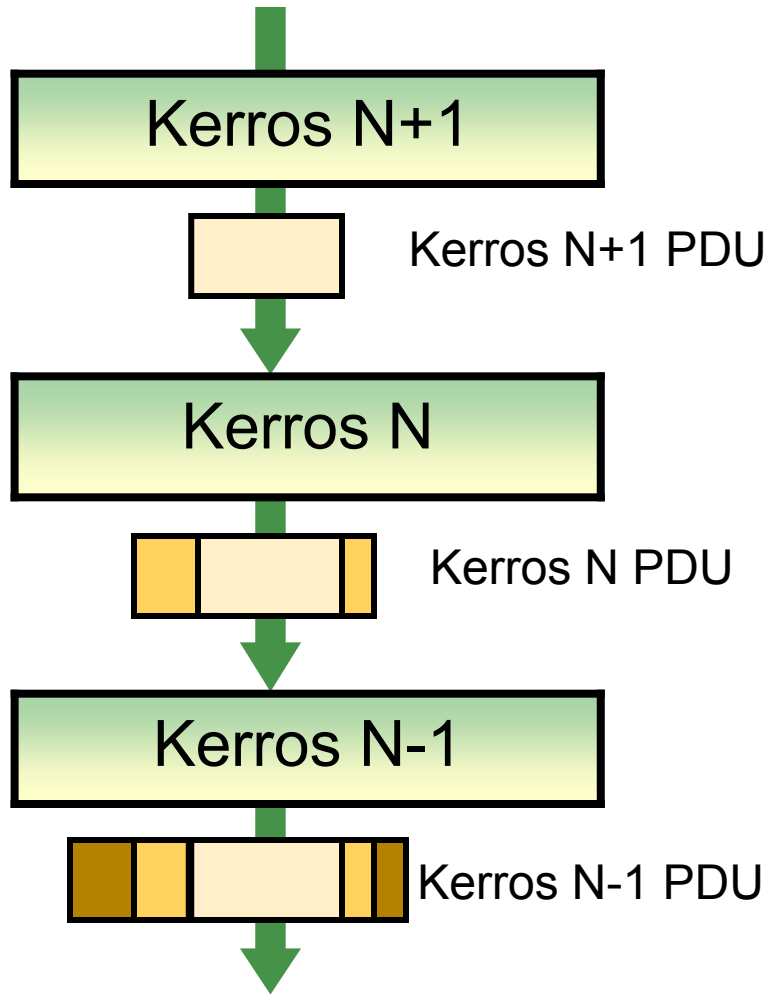


- OSI-referenssimalli
 - ISO-standardi
 - 7 kerrosta
- Kukin kerros käyttää alemman palveluja ja tarjoaa palveluja ylemmälle
- Kerroksissa 4-7 on päätelaitteiden välinen assosiaatio eli jaettu tila

Protokollapinot ja Internet

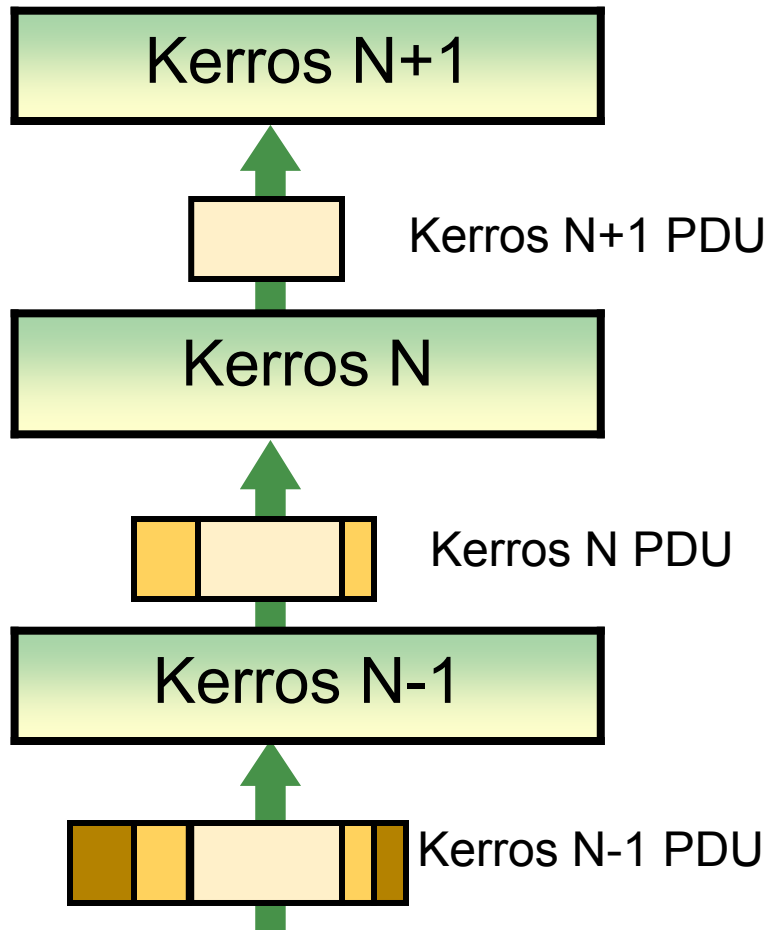


Lähettäjä



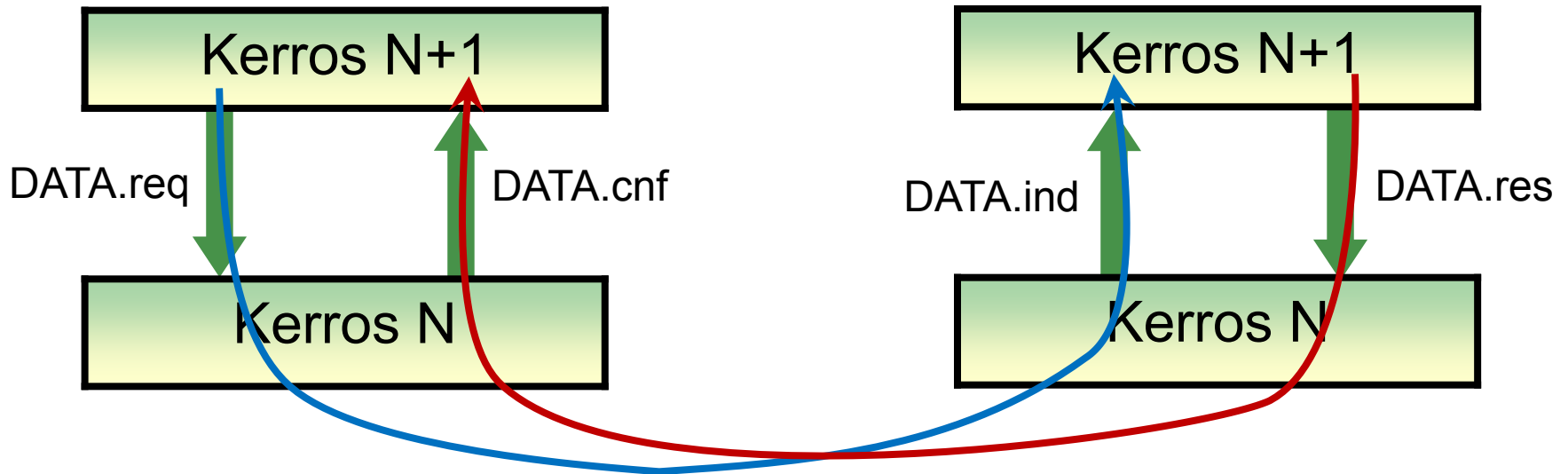
- Protokollatietoyksikkö (PDU)
- Korkeamman kerroksen PDU kapsuloidaan alemman PDU:hun
 - otsake
 - traileri
- Kehys fyysisellä siirtotiellä = 1-kerroksen PDU

Vastaanottaja



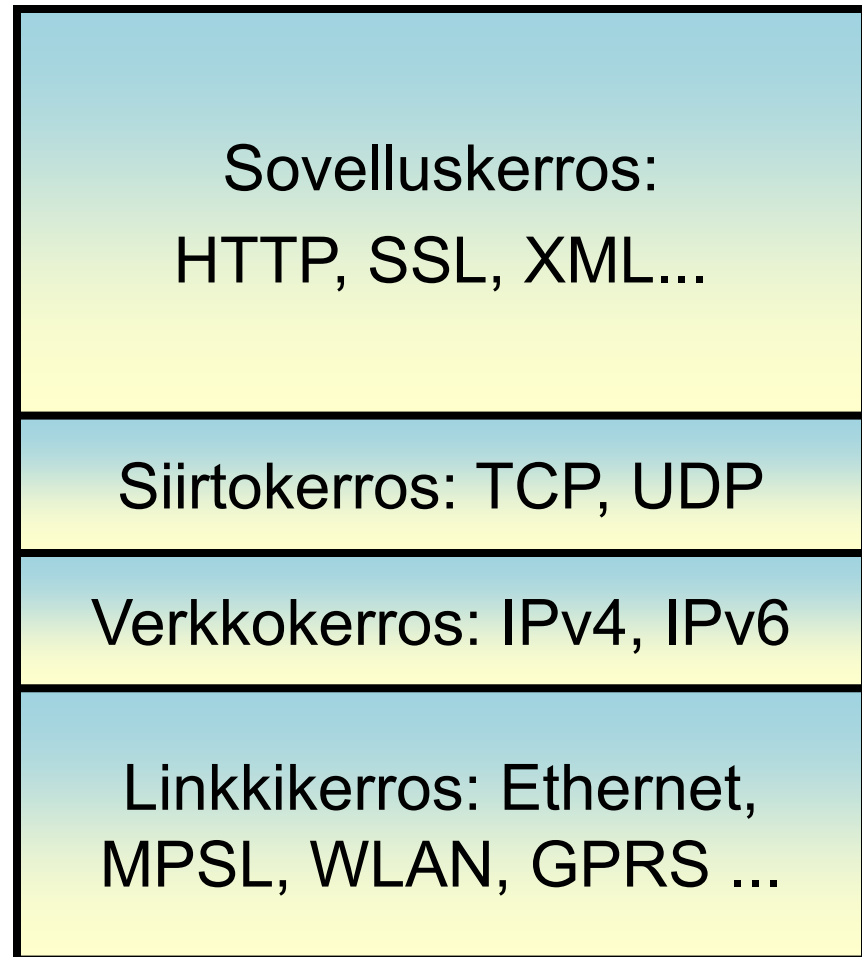
- Esimerkki:
L4 PDU = TCP Packet
L3 PDU = IP Packet
L2 PDU = Ethernet frame

Rajapinnat

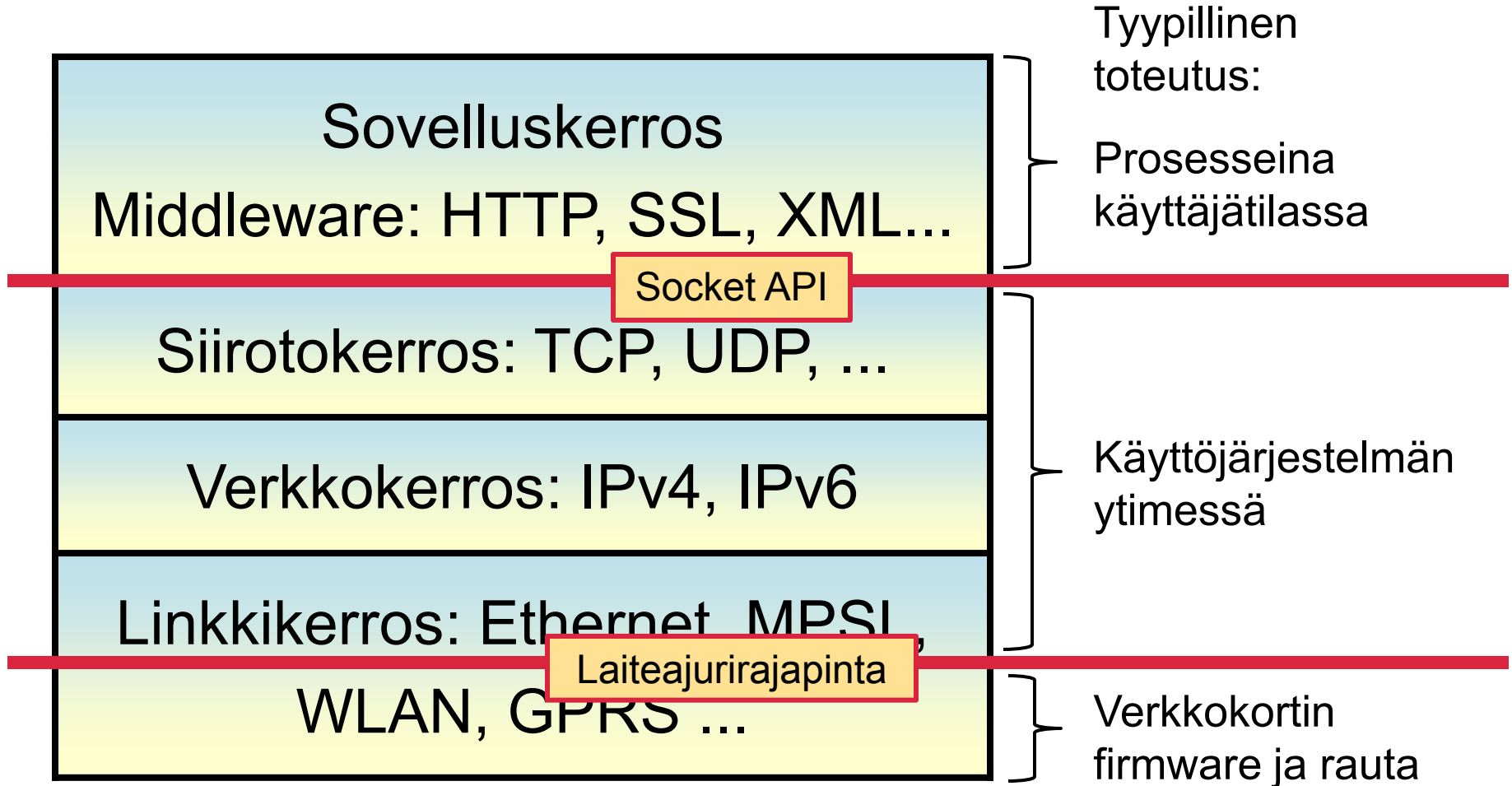


- Kerrosten välissä on palvelurajapinta
 - Kerroksen N ja N+1 rajapinta kuuluu kerrokseen N
- Periaate: kerros N kommunikoi vain kerrosten N ja N+1 kanssa
- OSI-mallin rajapinta:
 - kerroksilla primitiivejä (esim. DATA yllä)
 - pyyntö (req) ja ilmoitus (ind) sisältävät viestin
 - vastaus (res) ja varmistus (cnf) sisältävät kuittauksen

OSI-malli ja TCP/IP-pino



TCP/IP-pinon rajapinnat



Kerrokset käytännössä

- Protokollasuunnittelu on tasapainoilua siistin modulaarisuuden ja optimointien välillä
- Rajapinnat mahdollistavat kokonaisia markkinoita
- Erehdysten seuraukset pitkäkestoisia
 - esim. IP osoitteen käyttö TCP-päätepisteen tunnuksessa
- Kerrosrajoja ylittävät optimoinnit tärkeitä
 - suorituskyky, reaaliaikaisuus, palvelun laatu, energiansäästö, liikkuvuus, turvallisuus, anonymiteetti
 - esim. TCP ja langaton verkko
- Kerrosmallin joustavuus:
 - Alikerrokset, esim. MAC ja LLC, IPsec, TLS
 - Tunnelit, esim. VPN, GPRS tunneling protocol
 - Kokonaan uusia kerroksia ehdotettu, HIP
- Kehitys nopeinta sovelluspäässä

STANDARD OINTI

Standardointi

- **ISO**: OSI-malli, X.509-sertificaatit, Unicode
 - **ITU-T**: puhelinverkot, esim. SDH
 - **3GPP**: UMTS, LTE, GSM/GPRS/EDGE
 - **IETF**: TCP/IP-protokollapino
 - **IANA**: Internetin nimet ja numerot
 - **IEEE**: lähiverkot (IEEE 802)
 - **W3C**: web
 - **OASIS**: WS, XML-pohjaiset protokollat
- ... standardoijat kilpailevat keskenään

IETF

- Internet Engineering Task Force (IETF)
 - määrittelee protokollia: mitä lähetetään langalle
 - IETF-kokoukset, työryhmät, IESG, IAB
 - toiminta julkista: www.ietf.org
 - “running code and rough consensus”
- Standardointiprosessi:
 - Internet-Draft
 - Request for Comments (RFC): informational, experimental, best current practice, standards track (proposed, draft, standard)

IANA

- Internet Assigned Numbers Authority
- Hallinnoi nimiä ja numeroita
 - ylimmän tason DNS-nimet
 - IP-osoitteet ja AS-numerot
 - protokollanumerot, esim.
 - TCP-porttinumerot (80 = HTTP)
 - HTTP-virhekoodit (404 = sivua ei löydy)
- IANA nykyisin yhdysvaltalaisen ICANN-organisaation alaisuudessa

Kuka omistaa netin?

- Kuka päättää?
 - IETF/IANA
 - Verkkooperaattorit, erityisesti Tier-1 ISP:t, esim. TeliaSonera
 - Laite- ja ohjelmistovalmistajat, esim. Cisco ja Microsoft
 - Palveluntuottajat, esim. Google
 - Lainsäädäntö

TIEDONVÄLITYS, IHMISET JA YHTEISKUNTA

Muuttuva kommunikaatio

- Kukaan ei enää kirjoita kirjeitä?
- Väline muuttaa ihmisten välistä vuorovaikutusta
 - fax ja sähköposti
 - matkapuhelimet ja tavoitettavuus
 - sosiaaliset mediat: Usenet, Facebook, Twitter
- **Maailmankylä**, lyhenevät etäisyydet
 - esim. fuksit ja teekkariyhteisö
- Kysymys ei lopulta ole tekniikasta vaan kommunikaatiosta ihmisten välillä

Internet ja vapaus

- Internet ja vapaus
 - villi länsi vs. poliisivaltion väline
 - Kiinan palomuur
- Yksityisyyden suoja
 - valvontayhteiskunta
 - paikkatieto, kamerat, jatkuva nauhoitus

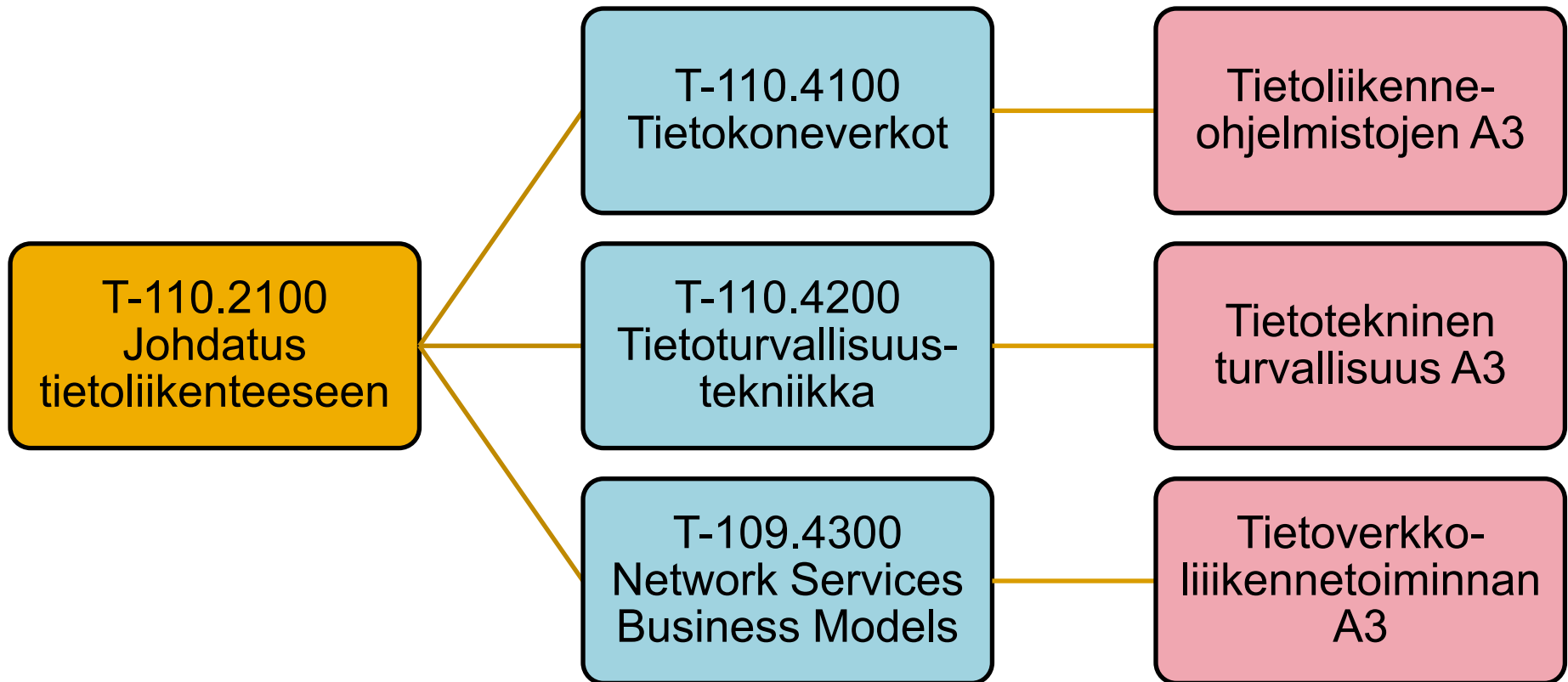
Insinöörin vastuu

- Tekniikan kehittämiseen liittyy arvovalintoja
 - Millaisessa yhteiskunnassa halumme elää?
 - esim. paikkaperustaiset palvelut
- Toisin kuin ydinvoimala tai öljylautta, koodi ei voi tappaa ketään?
 - esim. Iran
- Monitieteellinen näkökulma, Aalto-yliopisto
 - tekniikan vaikutukset käyttäjiin, talouteen ja yhteiskuntaan

TIETOLIIKENNEOHJELMISTOJEN OPISKELU

Tietoliikenneohjelmistojen opintopolku

- JoTi-kurssin jälkeen A1-moduulissa opitaan tietotekniikan DI:lle olennaisia taitoja
- A2-moduulissa kolme kurssia, jotka syveltävät JoTilla sivuttuja teemoja
 - kukin kurssi johtaa omaan A3-moduliin
 - lisäksi Käyttöjärjestelmät ja Ohjelmistokehitysprojekti



Opintojen tavoitteet

- Valmistaa moninaisiin työtehtäviin, R&D ei ainoa urapolku
- Laaja tekninen osaaminen:
 - Internetin ja mobiiliverkkojen teknologiat, palvelut, tietoturva ja liiketoiminta
 - taidot kehittää uutta tietoverkkojen tekniikkaa, palvelualustoja ja sovelluksia
 - kyky kehittää turvallisia ratkaisuja
 - taito hakea tietoa tieteellisestä kirjallisuudesta
- Teknisen osaamisen lisäksi projekti- ja ryhmätyöskentely, kirjoittaminen, esiintyminen
- **Kyky ottaa vastuu avointen teknisten ongelmien ratkaisemisesta**

Mitä muuta tarvitset

- Matematiikka
 - simulointi, tilastotiede, oikeaksi todistaminen, diskreetti matematiikka, koneoppiminen, algoritmit, kryptografia
- Ohjelmointitaito: teoria ja kokemus
- Innovaatioon ja liiketoimintaan liittyvät opinnot
- Assarointia suositellaan: esiintyminen, ihmisten ja asioiden organisointi

Opiskeluympäristö

- Kansainvälinen opiskeluympäristö
 - Tietoliikenneohjelmistojen kansainväliset maisteriohjelmat: *NordSecMob* ja *Mobile Computing—Services and Security*
 - Useimmat kurssit englanniksi
 - Opintojen jälkeen on helppo lähteä ulkomaille ja työskennellä kansainvälisissä yrityksissä
- Opintojen toinen vaihe kahdessa vuodessa on testattu realistinen tavoite kaikille
- Valmistuneilla kova kysyntä