T-110.4100 Tietokoneverkot

Sanna Suoranta, TkL
Tutkija, T-laitos, TKK,
Aalto-yliopisto

Tämän kurssin sisältö

- TCP/IP-verkot ja niiden toiminta
- Verkkosovellusten suunnittelu ja ohjelmointi

Tietoa tästä kurssista

- https://noppa.tkk.fi/noppa/kurssi/t-110.4100/
- news://news.tky.hut.fi/opinnot.tik.tietokoneverkot
  (kaikki kysymykset tänne!!)
- IRC: #verkot
- T-110.4100@tkk.fi (henkilökohtaiset kysymykset)
- http://www.cse.tkk.fi/Tietoliikenne/

Esitiedot

- T-110.2100 Johdatus tietoliikenteeseen ja T-106.3101 Ohjelmoinnin jatkokurssi T2
- Eli oikeastaan
  - Tiedonsiirron perusteet
  - Tietotekniikan perusopintojen ohjelmointikurssit

Ilmoittautuminen

- Ilmoittautuminen on avattu WebOodiin
  - Ilmoittautuminen päättyy 21.9.2010
- Tentteihin tulee ilmoittautua erikseen viimeistään viikkoa ennen tenttiä
  - Ilmottautuminen on avattu syksyn tentteihin

Kurssin osasuoritukset ja arvostelu

- Pakolliset
  - Osatentti 1: perus-TCP/IP. 40% loppuarvosanasta
  - Osatentti 2: ohjelmointi, NAT, verkonhallinta jne. 40% loppuarvosanasta
  - Harjoitustyö: 20% loppuarvosanasta (as. 0/3/5)
- Vapaaehtoiset mutta hyödylliset ☺
  - Luennot+muistiinpanot
  - Kirjan lukeminen, jne

Luennot ja harjoitukset

- 1. opetusjakson aikana (7.9.-21.10.) tiistaisin 10-12 salissa T2 ja torstaisin klo 8-10 salissa T2
- Ei harjoituksia, ei vastaanottoa, ellei erikseen sovi assarin kanssa
- Tarkempi aikataulu löytyy kurssin www-sivuilta nopasta

Luennot

• ti 7.9.	Johdanto + IPv4	Sanna Suoranta
• to 9.9.	IPv6	Sanna Suoranta
• ti 14.10.	DNS & DNSsec	Bengt Sahlin
• to 16.9.	Reititys 1 (IGP)	Sanna Suoranta
• ti 21.9.	Reititys 2 (EGP)	Sanna Suoranta
• to 23.9.	Liikkuvuus	Sanna Suoranta
• ti 28.9.	TCP & UDP	Matti Siekkinen
• to 30.9.(9-10)	Harjoitustyö	Pyry Koivisto
• ti 5.10.	Verkko-ohjelmointi	Samuli Sorvakko
• to 7.10.	NAT	?
• ti 12.10.	Verkonhallinta	Jaakko Kotimäki
• to 14.10.	Protokollasuunnittelu	Miika Komu
• ti 19.10.	Uutuudet	proffat
• to 22.10.	Kertaus	Sanna Suoranta

Oppimateriaali

- Douglas E. Comer, Internetworking with TCP/IP, Volume 1, Pearson Prentice Hall, 2006 tai joku muu perusoppikirja
- Opetusmonisteita Nopassa
  - Luennoijien kirjoittamaa materiaalia
  - Linkkejä nettiin
- Kalvot lisätään kurssin luentoaikatauluun
  - pääasiallisesti luennon tukimateriaali, ei oppimateriaali sellaisenaan
  - älkää tulostako niitä TKKn tulostimille!

Tentit

- Tenttipäivät 26.10.2010 ja 14.12.2010 (tarkista oodi!)
  - Tenttiin ilmoittauduttava viimeistään viikkoa ennen tenttiä
- Kaksi osatenttiä
  - Molemmat suoritettava hyväksytysti kurssin läpäisemiseksi
  - Kumpikin osatentti arvostellaan asteikolla 0-5
  - Kaikkina tenttikertoina (tenttikausina) voi tehdä jommankumman osatentin (tai molemmat osatentit yhdellä kerralla)
  - Kumpaankin osatenttiin ilmoittaudutaan erikseen!
  - Vanhoja tenttejä kurssin Noppa- ja arkistosivuilla

Tentti (jatkuu..)

- Perukaa ilmoittautuminen, jos ette tule paikalle!
  - oodissa, tai ilmon sulkeuduttua sähköpostitse
- "Opiskelijan tulee ilmoittautua kokeeseen viikkoa ennen koetilaisuuden järjestämistä, jollei opettaja hyväksy myöhempää ilmoittautumista. Ilmoittautuminen katsotaan kokeeseen osallistumiseksi, ellei sitä ole peruutettu ennen kokeen alkamista. Kokeessa kolmasti hylätyn opiskelijan on neuvoteltava asianomaisen opettajan kanssa kurssin suorittamisesta. "
  (tutkintosääntö)

Harjoitustyö

- Harjoitustyön tehtävänanto julkaistaan viimeistään 30.9.2010 kurssin noppasivuilla
  - Reititystaulun rakentaminen etäisyysvektori ja/tai linkkitilaprotokollan lähettämien viestien perusteella
  - Asiakasohjelma reititystaulun palauttamiseen
- Arvosana 0/3/5, 20% kurssin arvosanasta
- Harjoitustyö tehdään yksin, n. 40-50 tuntia
  - Suunnitelma dl ~pe 15.10. klo 12:00 (keskipäivä)
  - Toteutus dl ~pe 19.11. klo 12:00 (keskipäivä)
  - Demot noin viikolla 47-48

Kysyttävää järjestelyistä?

mitähän te muistatte
edellisistä kursseista..

Jo osattavaa

Käyttäjän sovellukset:
-sähköposti (SMTP, POP, IMAP)
-WWW (HTTP)
-FTP,
-news (NNTP)
-P2P

tietoturvan käsitteet

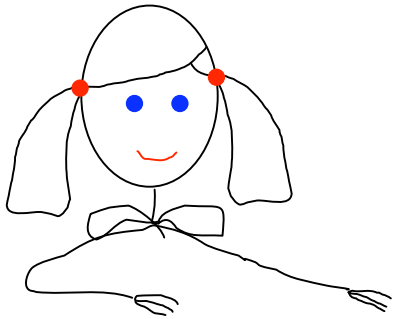
UDP, TCP kuittaukset

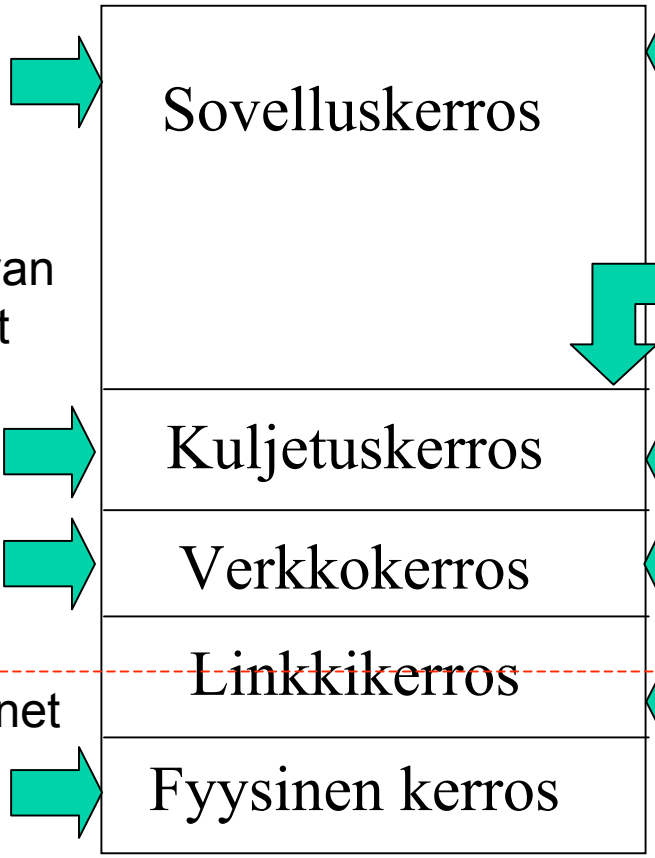
IPv4

ARP

Ethernet

Aiheuttaa viiveitä, häviöitä jne. (out of scope)





Tällä kurssilla

Infrastruktuuri-palvelut: DNS, SNMP, NAT
Tietoturvaratkaisut: TLS, DNSsec
protokollasuunnittelu
verkko-ohjelmointi

Socket-rajapinta ohjelmoinnille

TCP ”kokonaan” eli virhetilanteiden käsittely

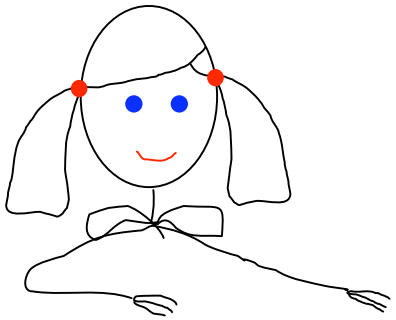
IPv6, reititysalgoritmit, IPsec

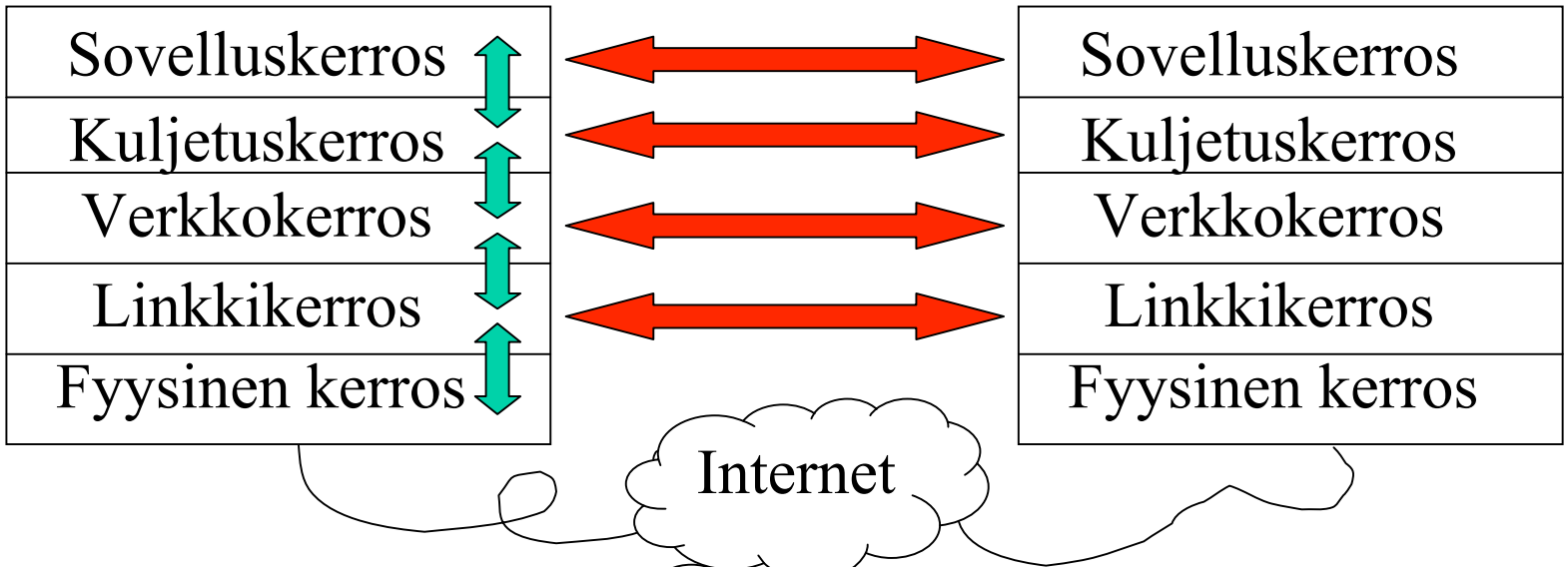
Ethernet, miten IP-osoitetta vastaava ethernet osoite löydetään IPv6:ssa (ja toistepäin)

Rajapinta ja protokolla

- mitä tehdään samassa koneessa esim. kapsulointi

- koneiden välillä
- viestiformaatit
- osapuolten ”tunnistus”
- viestien käyttö





Internet-protokolla versio 4

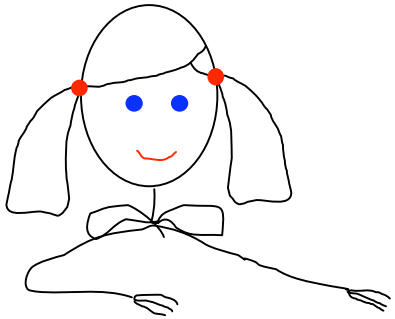
Kertaus

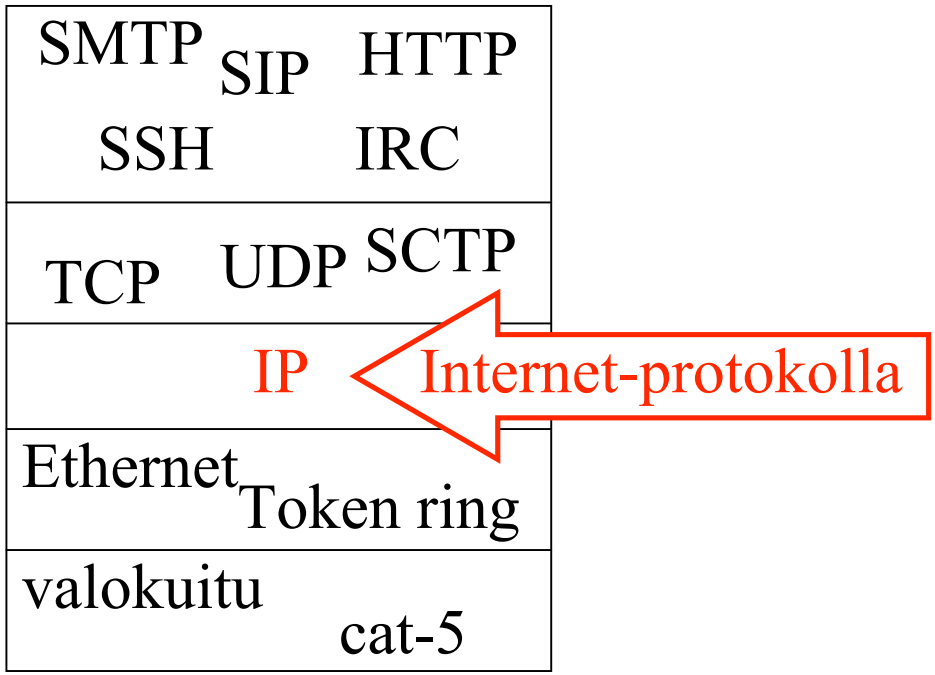
luvut 4, 6, 8, 9, ja 22

Luennon sisältö

- IPv4 ominaisuudet ja tehtävä
- IPv4 otsake ja käyttö
- IPv4 osoitteet
  - Ali- ja yliverkotus
  - Muut ratkaisut: NAT ja DHCP
- ICMP
  - Virhetilanteiden käsittely

Internet-protokolla



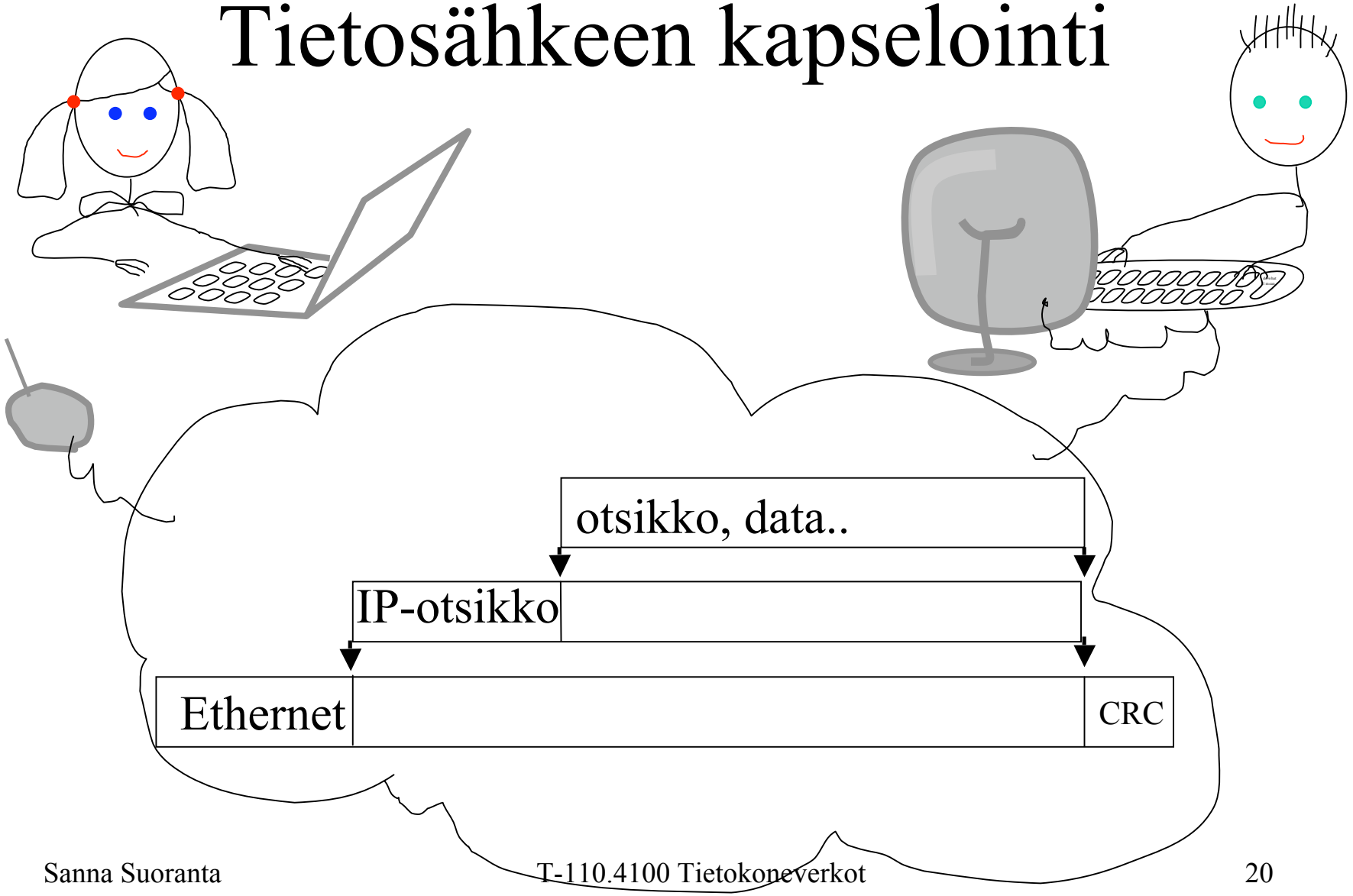


- Internet-protokolla on yhdistävä tekijä kaikkien sovellusten ja kaikenlaisten verkko-teknologioiden välissä

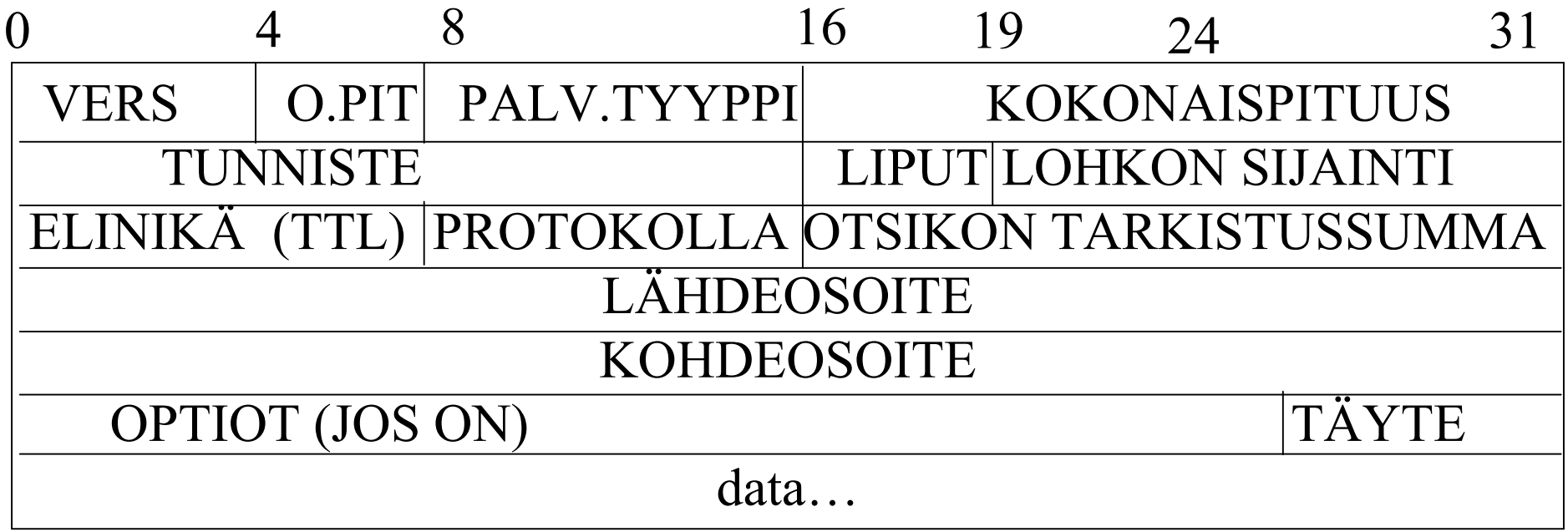
Internet-protokolla (IP)

- Pakettipohjainen (packet oriented)
  - viesti jaetaan paketteihin
- Yhteydetön (connectionless)
  - jokainen tietosähke (datagram) käsitellään itsenäisesti
- Epäluotettava (unreliable)
  - perillemenoa ei taata
  - paketit voivat monistua, viivästyä, järjestys voi vaihtua…
- Päästä päähän (end-to-end)
  - lähettäjän ja vastaanottajan ei tarvitse olla samassa verkossa

Tietosähkeen kapselointi



IP-otsikon rakenne (RFC 791)

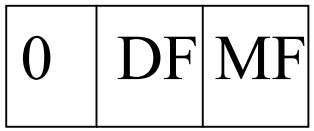


IP-otsikon kentät

- VERSio numero = 4
- Otsikon pituus (O.PIT) 32 bitin sanoina
  - min 5 (5*32 bittiä) + optiot
  - kertoo siis lähinnä optioiden pituuden
- PALVELUN TYYPPI
  - palvelun laadun määrittely, esim DiffServ
  - alunperin toisella tavalla

IP-otsikon kentät

- KOKONAISPITUUS
  - otsikko+data-osion pituus oktetteina
- LIPUT, kolme bittiä:



  - DF: 0 = saa lohkoa, 1 = ei saa lohkoa
  - MF: 0 = viimeinen lohko, 1 = lisää lohkoja
- LOHKON SIJAINTI + TUNNISTE
  - kts. lohkominen

IP-otsikon kentät

- ELINIKÄ
  - maksimi”aika”, jonka paketti saa vaeltaa verkossa
  - alun perin sekunteja; nyt jokainen reititin vähentää vähintään yhdellä
- PROTOKOLLA
  - Ylemmän kerroksen protokolla, joka on data-osiossa
  - Esim ICMP=1, TCP = 6, UDP =17, IPv6=41

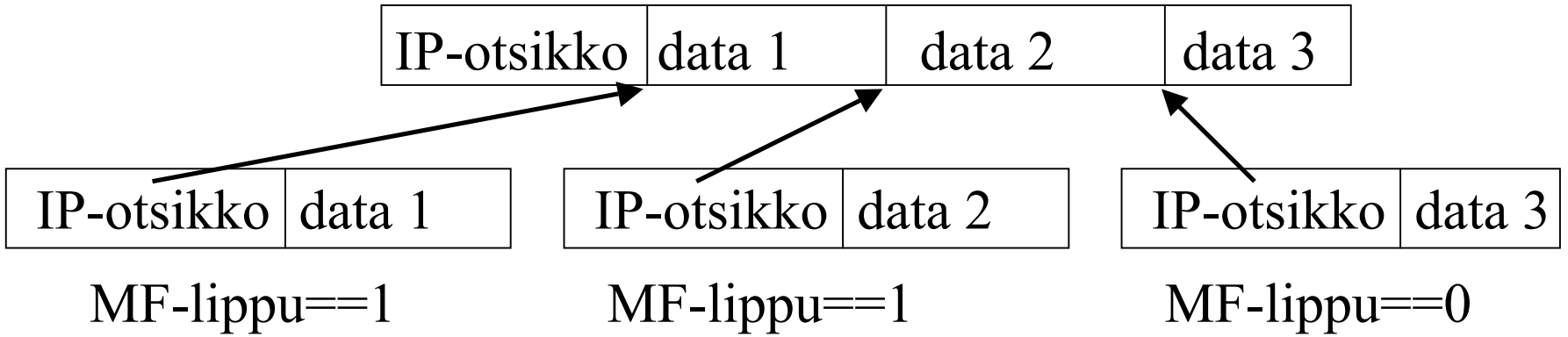
IP-otsikon kentät

- TARKISTUSSUMMA
  - 16-bittinen yhden komplementtisumman yhden komplementti otsikon kentistä
  - kertoo, onko otsikko ehjä
  - ylemmillä kerroksilla omat tarkistussummat
- LÄHDE- ja KOHDEOSOITTEET
  - 32-bittisiä, kts alla

Tietosähkeen lohkominen
(englanniksi datagram fragmentation)

- Tietosähke ei aina mahdu fyysisen verkon kehykseen, joten se pitää lohkoa useampaan palaan
  - tehotonta, joten yritetään välttää selvittämällä verkon enimmäispituus eli MTU (Maximum transfer unit)
- Tietosähke kootaan vasta vastaanottajalla
  - Odotetaan tietty aika, että kaikki lohkot tulisivat perille

Tietosähkeen lohkominen

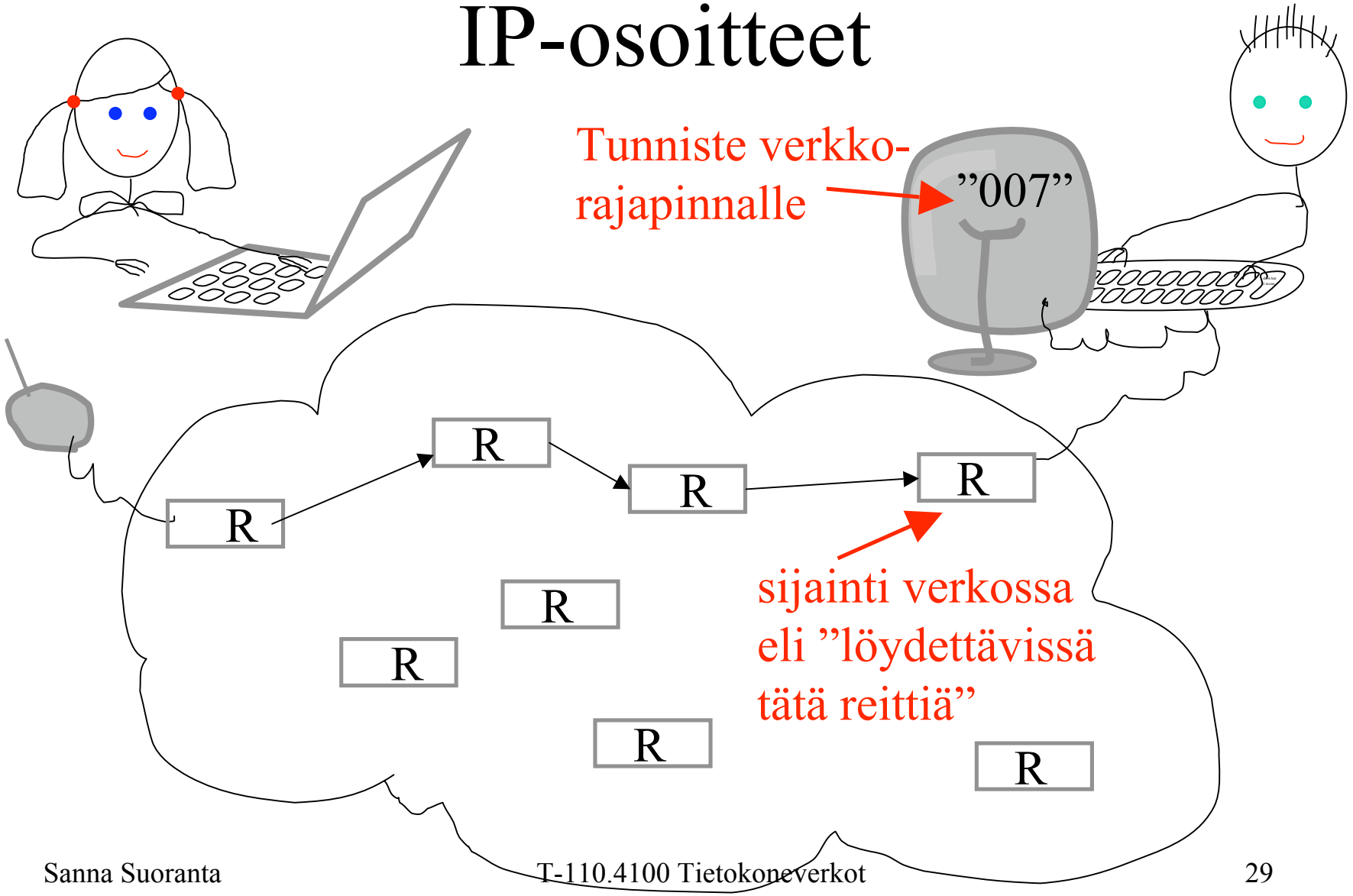


- Jokaisella tietosähkeellä on TUNNISTE, jonka avulla lohkot kootaan takaisin
- Lohkon sijainti: oktettia alkaen alkuperäisen datan alusta
- kokonaispituus: lohkotun sähkeen pituus

IP:n optiot

- Käytetään pääasiassa verkon testauksessa ja vianmäärityksessä (jos siinäkään)
- Ohjeellinen ja täsmällinen lähdereititys, reitin seuranta, jne

IP-osoitteet



IPv4-osoitteet (RFC 796, 1981)

- Alkuperäinen luokallinen osoitteistus

luokka	alku	verkko	laite	osoitteet
A	0	7 bittiä	24	1.0.0.0 - 126.255.255.255
B	10	14	16	128.0.0.0 - 191.255.255.255
C	110	21	8	192.0.0.0 - 223.255.255.255
D	1110	monilähetysryhmä		

- http://www.xkcd.com/195/

Nollien ja ykkösten merkitys

- tämä laite, 0.0.0.0 määrittelemättä

00000000000000000000000000000000

- laite tässä verkossa

00000000000000000000	101010101010

- yleislähetys (tässä verkossa) 255.255.255.255

11111111111111111111111111111111

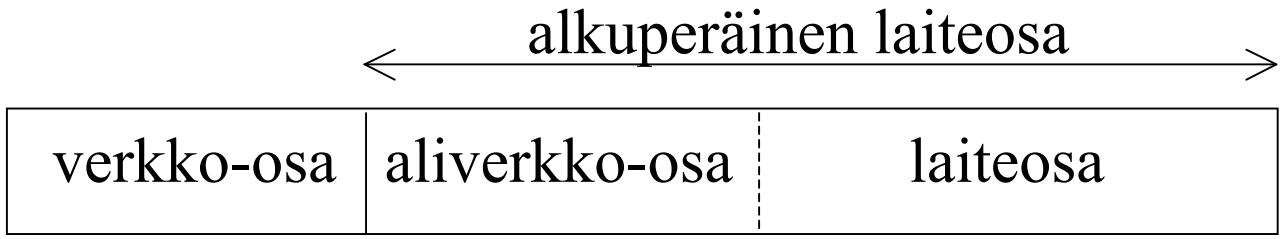
- verkkomaski 255.255.248.0

11111111111111111111	00000000000

- loopback-osoite 127.0.0.1

1111111	nnnnnnn…nnnnnnnnnnnnn

Aliverkotus (RFC 940, 1985)



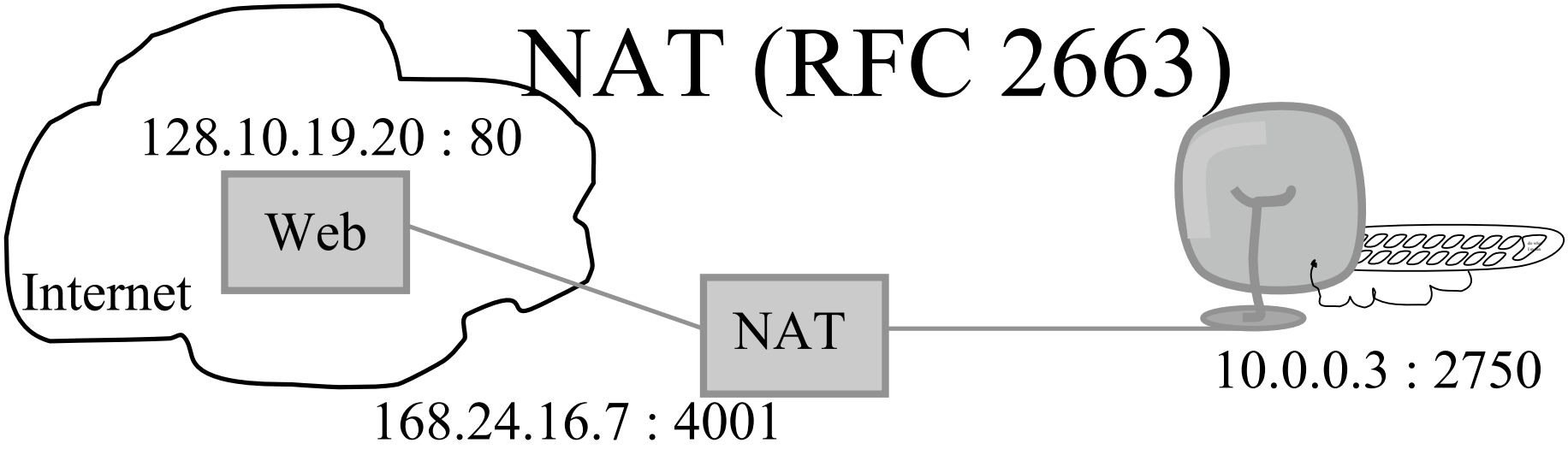
- Saman verkko-osoitteen käyttö useassa fyysisessä verkossa
- Osa laitetunnisteesta määrittääkin aliverkon
- Aliverkko-osan pituus voidaan määrittää verkkokohtaisesti

Luokaton osoitteistus (RFC 1518&1519, 1993)

- Classless InterDomain Routing (CIDR)
- Organisaation verkossa on useita verkkolohkoja
- Osoitelohkon koko voidaan valita vapaasti:
  - verkko-prefix / verkko-osan bittien määrä
  - esim2. 128.211.168.0/21, jossa verkkoa merkitsee 21 ensimmäistä bittiä osoitteesta, koneelle 11 viimeistä bittiä (verkossa tilaa 2048 koneelle)
  - esim 130.233.0.0/16 on tavallinen B-luokan osoite, TKK:n verkko

- IP kerrattu
- NAT, DHCP, ICMP vielä jäljellä

Network Address Translation
NAT (RFC 2663)



- Piilottaa sisäverkon ulkopuolisilta, säästää osoitteita
  - reitittimellä tila kaikille yhteyksille
- Sisäverkossa voi käyttää yksityisiä osoitteita
  - 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12
- Voi aiheuttaa hankaluuksia sovelluksille (lisää 7.10.)

Dynamic Host Configuration Protocol DHCP (RFC2131)

- IP-osoitteen käyttölupa (lease) tietyksi ajaksi
  - automaattisesti (ekan kerran jälkeen aina sama osoite) tai dynaamisesti (joku osoite)
  - myös staattinen jako MAC-osoitteen perusteella mahdollinen
- Samalla muitakin asetustietoja, kuten nimipalvelimen osoite, oletusreitittimen osoite
  - Asiakas täyttää jo kyselyyn mahdollisimman paljon tietoja, ja jättää tyhjäksi (nollaksi), jos ei tiedä

DHCP-asiakkaan tilakone

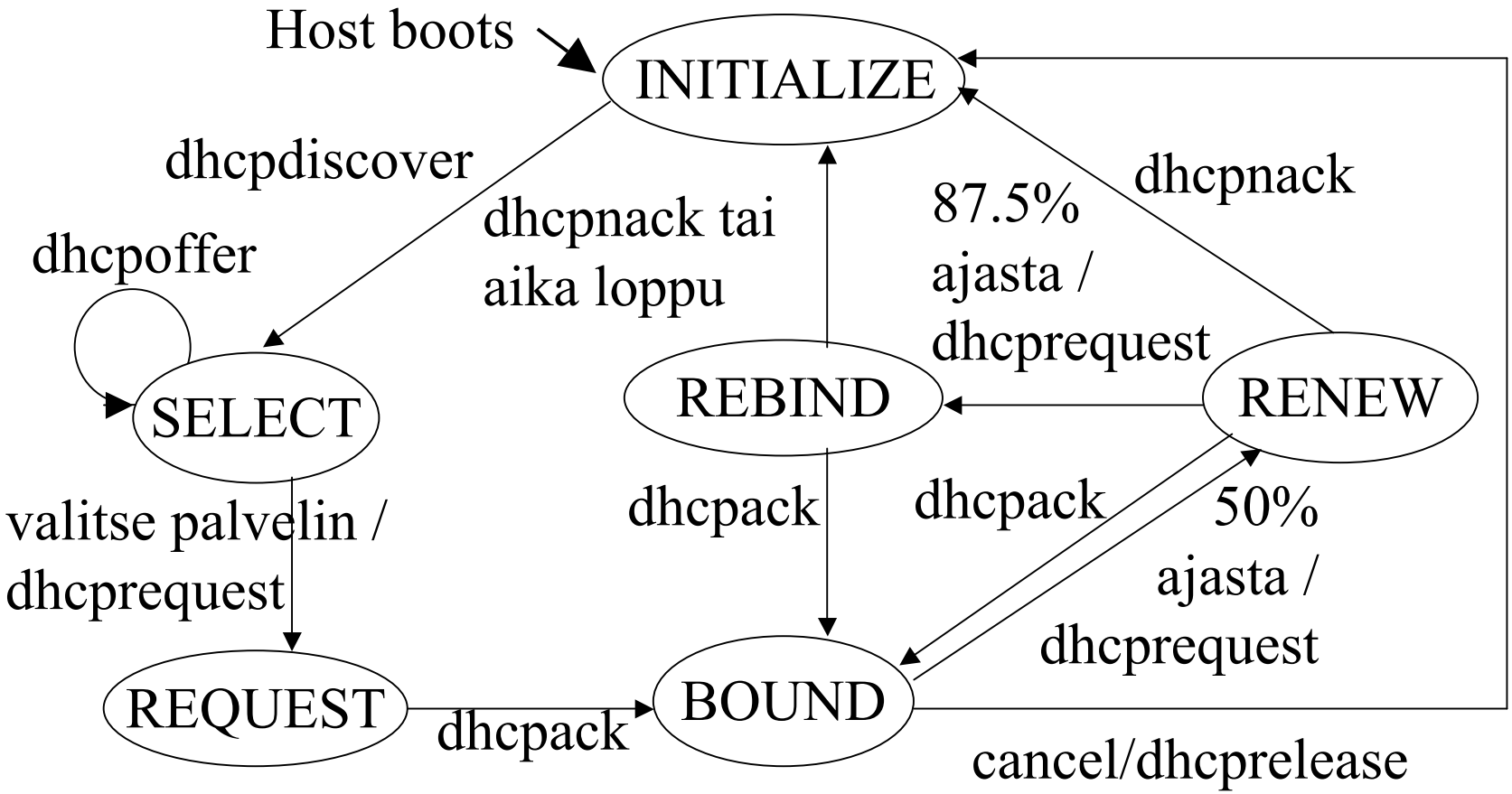
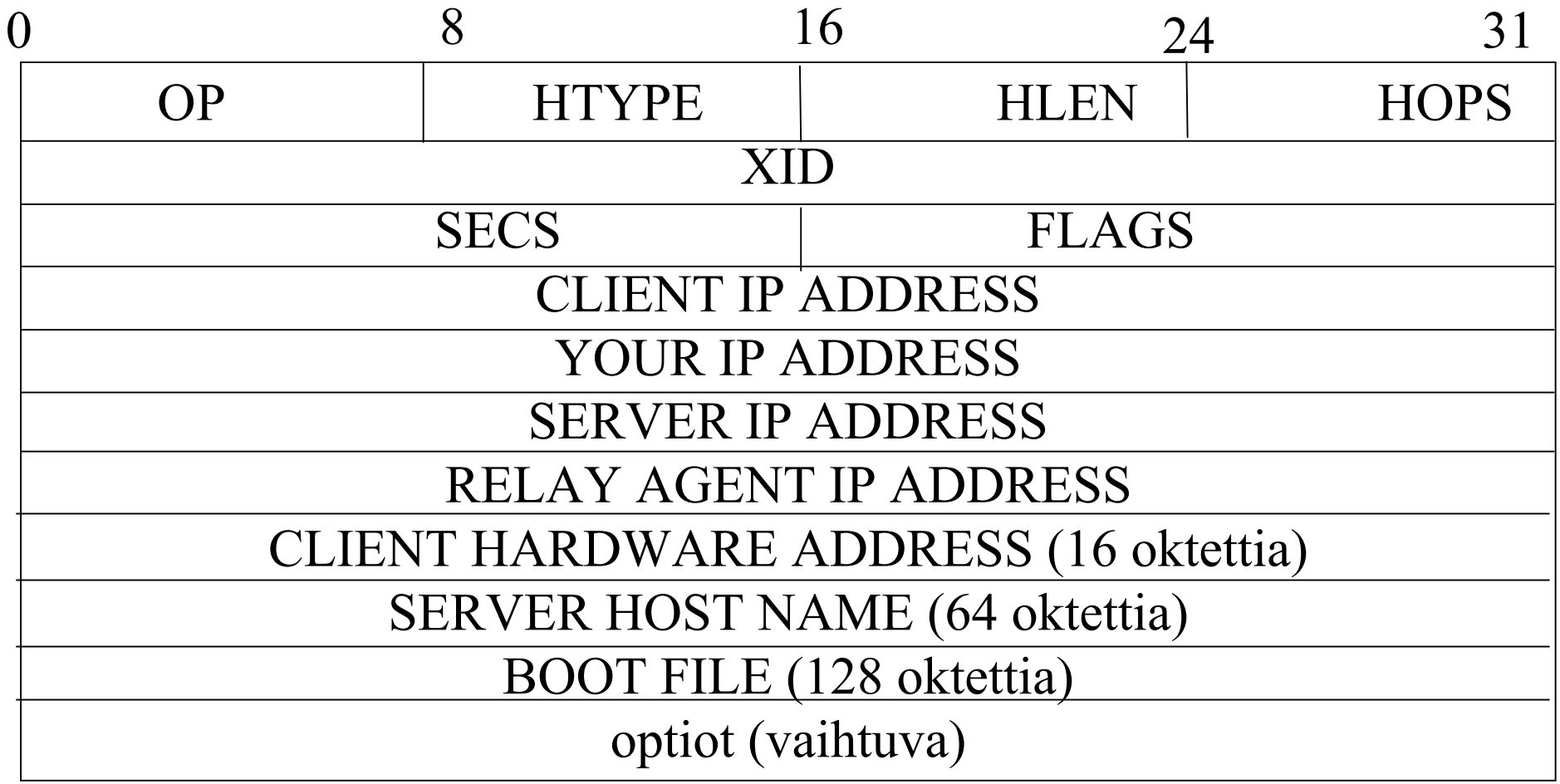


Fig. 22.3 Comerin kirjassa

DHCP-viestit



DHCP-viestit

- OP: 1 = kysely, 2 = vastaus
- HTYPE = linkkikerroksen verkon tyyppi
  - Ethernetille 1
- HLEN = linkkikerroksen osoitteen pituus
  - Ethernetille 6 (eli 6*8=48 bittiä)
- HOPS = asiakas asettaa nollaksi, käytetään kun välissä on välityspalvelin (relay agent)

DHCP-viestit

- XID = asiakkaan luoma tunniste
  - yhdistää kyselyt ja vastaukset
- SECS = sekunttia asiakkaan käynnistämisestä
- FLAGS = käytössä vain ensimmäinen bitti
  - 1 = vastaus lähetetään yleislähetyksenä (asiakkaalla ei vielä IP-osoitetta)
  - 0 = suoraan YOUR-kentän osoitteeseen yksilähetyksenä

DHCP-viestit

- CLIENT-osoite, asiakkaan IP-osoite kun ARPia voidaan käyttää (bound, renew, rebinding-tilat), eli asiakas tietää osoitteensa
- YOUR-osoite, asiakkaan IP-osoite, palvelin lähettää asiakkaalle käynnistyksen yhteydessä
- SERVER-osoite, jota pitäisi käyttää seuraavaksi (palvelin kertoo dhcpoffer- ja -ack-tiloissa), myös jos asiakas haluaa tietyn palvelimen
- RELAY-osoite, jos välissä reititin/agentti

DHCP-viestit

- CLIENT HARDWARE = asiakkaan linkkikerroksen osoite
- Jos asiakas haluaa yhteyden tiettyyn palvelimeen, se täyttää joko palvelimen osoite -kentän tai kentän SERVER NAME = palvelimen dns-nimi

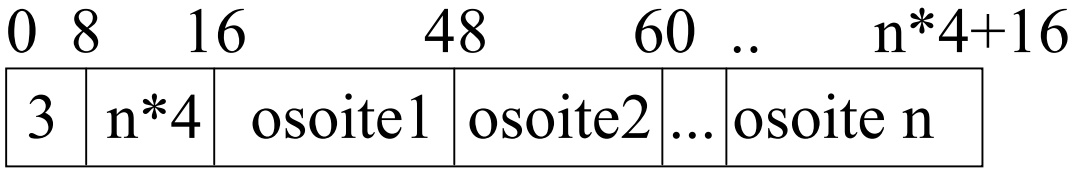
DHCP-viestit

- BOOT FILE = levyttömille koneille alustustiedoston sijainti
  - asiakas voi pyytää tiettyä, esim “unix”
  - palvelin joko antaa pyyntöä vastaavan alustustiedoston sijainnin tai valitsee itse tarvittavan tiedoston
  - asiakas hakee tiedoston esim TFTP:llä
- Optiot: type+length+value-tyylillä
  - RFC 2132 sisältää mahdolliset optiot, lisäyksiä RFC3442, RFC3942, RFC4361, RFC4833, RFC5494

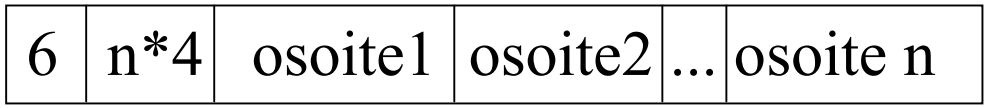
DHCP optiot

- aliverkon peite:

- oletusreititin:
  - voi olla useita
  - preferenssijärjestyksessä

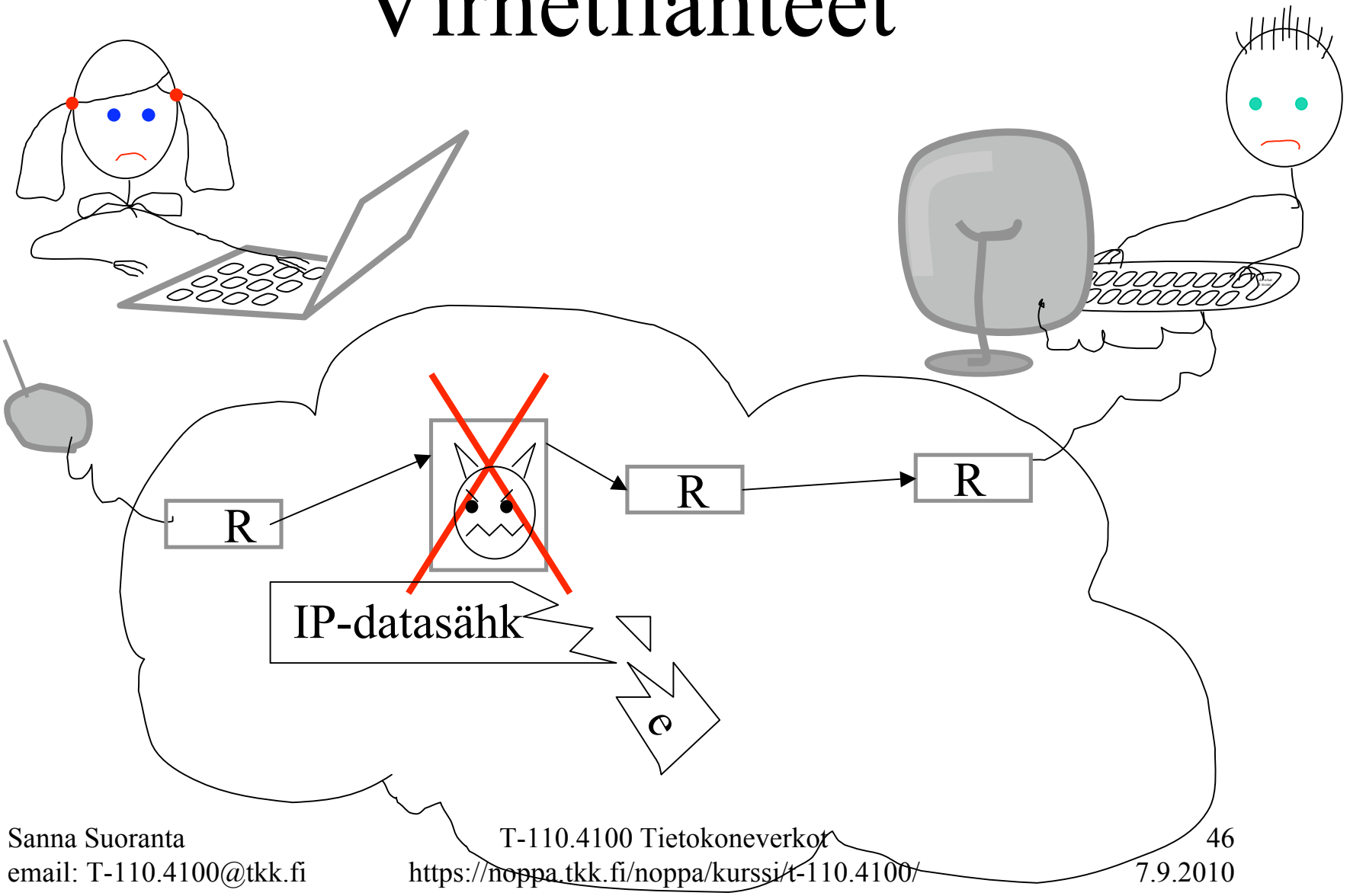


- nimipalvelin:
  - voi olla useita
  - preferenssijärjestyksessä



Vielä jäljellä:
mitä jos jotain
meni pieleen?

Virhetilanteet



Internet Control Message Protocol ICMP (RFC792)

- Ruuhkasta ilmoittaminen
- Uudelleenohjaus (tietoturvaongelma!)
- Elinajan raja saavutettu
- Parametriongelma
- Aliverkon peite
- Reitittimen etsiminen
- Polun pienimmän MTU:n löytäminen

Virhe- ja valvontaviestit

TYYPPI	KOODI	TARKASTUSSUMMA
Riippuu viestin tyypistä		
Ongelman aiheuttaneen paketin IP-otsikko ja 64 bittiä dataa		

- Internet Control Message Protocol (ICMP)
- Virhe- ja ohjaussanomat reitittimille ja tietokoneille
  - Ei virheiden korjausta, vain ilmoittaminen
- Lähetetään alkuperäiselle lähettäjälle

ICMP-viestejä

- Echo request ja echo reply (ping)

TYYPPI (8/0)	KOODI (0)	TARKASTUSSUMMA
TUNNISTE		JÄRJESTYSNUMERO
DATAA (ei välttämätön)...		

- Kohde tavoittamattomissa

TYYPPI (3)	KOODI (0)	TARKASTUSSUMMA
Käyttämätön (oltava 0)		
Ongelmapaketin IP-otsikko ja 64 bittiä dataa		

Lähteet

- RFC 791 Internet Protocol, 1981
- RFC 792 Internet Control Message Protocol, 1981
- RFC 796 Address Mappings, 1981
- RFC 950 Internet Standard Subnetting Procedure , 1985
- RFC 1518 An Architecture for IP Address Allocation with CIDR, 1993
- RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strate, 1993
- RFC 2131 Dynamic Host Configuration Protocol, 1997
- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations, 1999
- RFC 3396 Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), 2002
- RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), 2006

Lisää kursseja aiheesta

- T-110.5110 Tietokoneverkot II
- S-38.2121 Reititys tietoliikenneverkoissa (4 op)
- S-38.3148 Simulation of Data Networks (5 cr)
- S-38.3180 Palvelunlaatu Internetissä (4 op)
- S-38.3184 Verkkoliikenteen mittaus ja analysointi L (5 op)