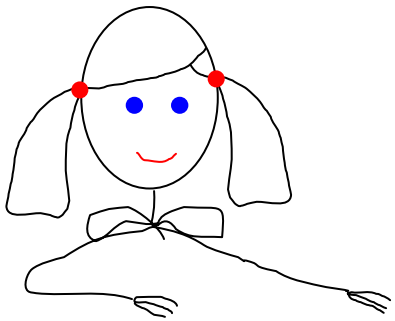
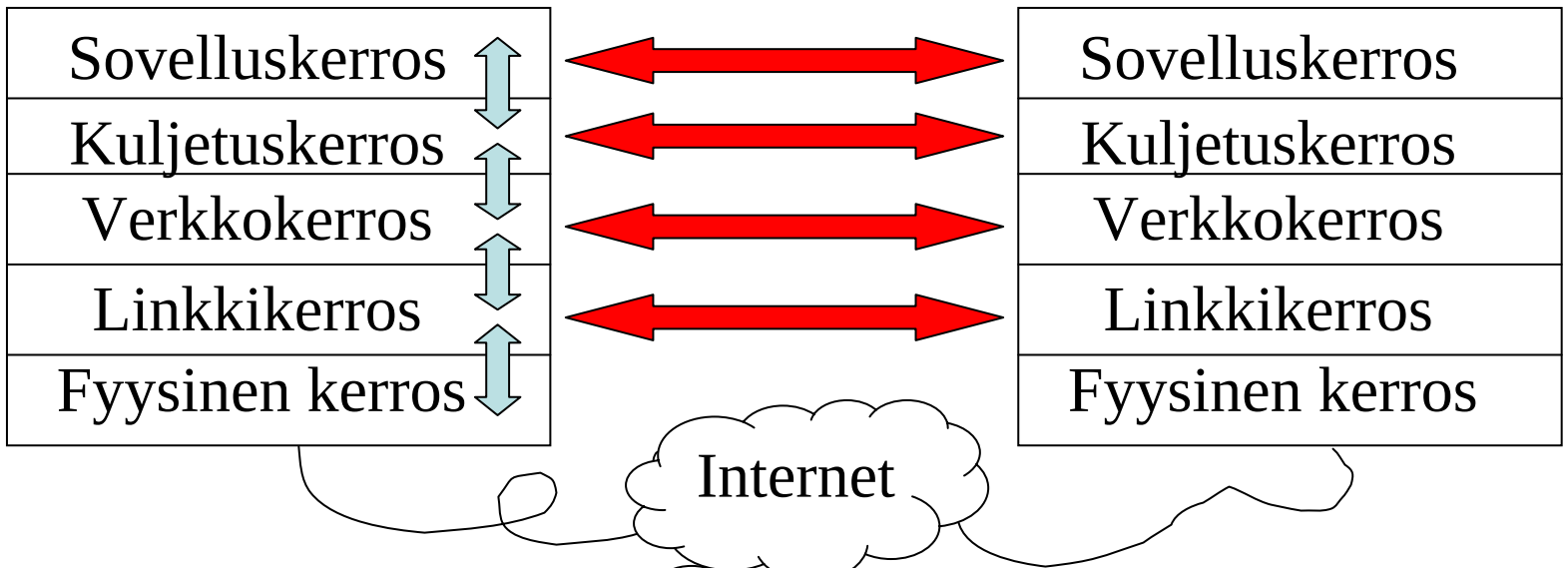
Esimerkkejä lisätyistä kalvoista

Rajapinta ja protokolla

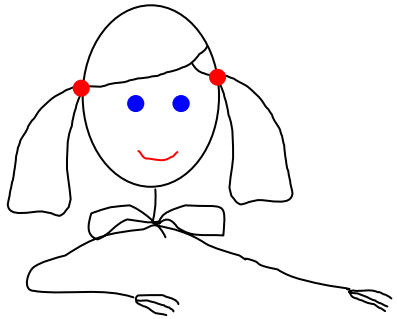
- mitä tehdään esim. kapsulointi

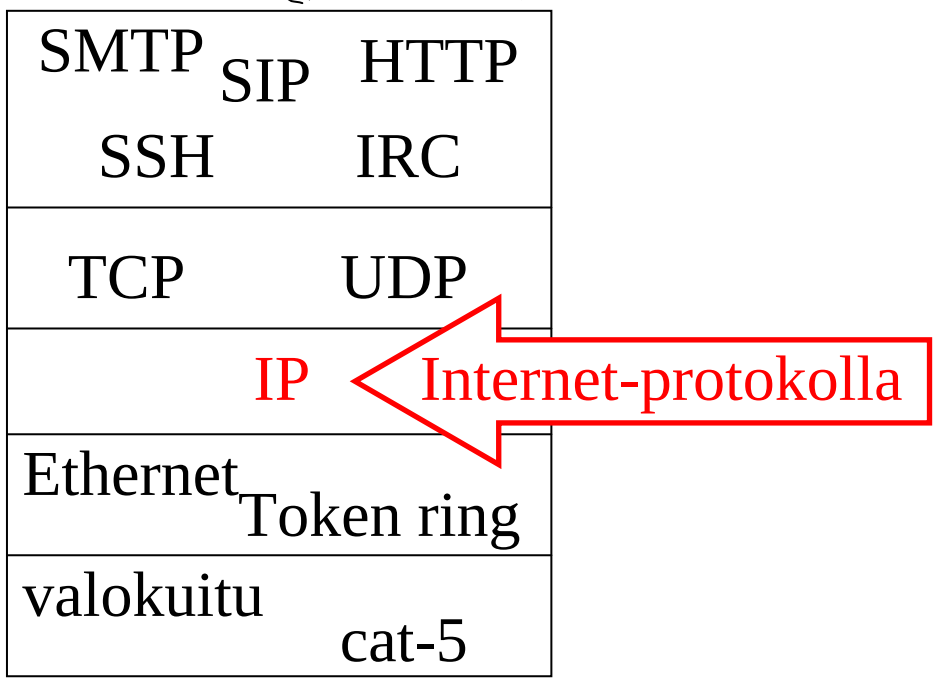
- viestiformaatit
- osapuolten ”tunnistus”
- viestien käyttö





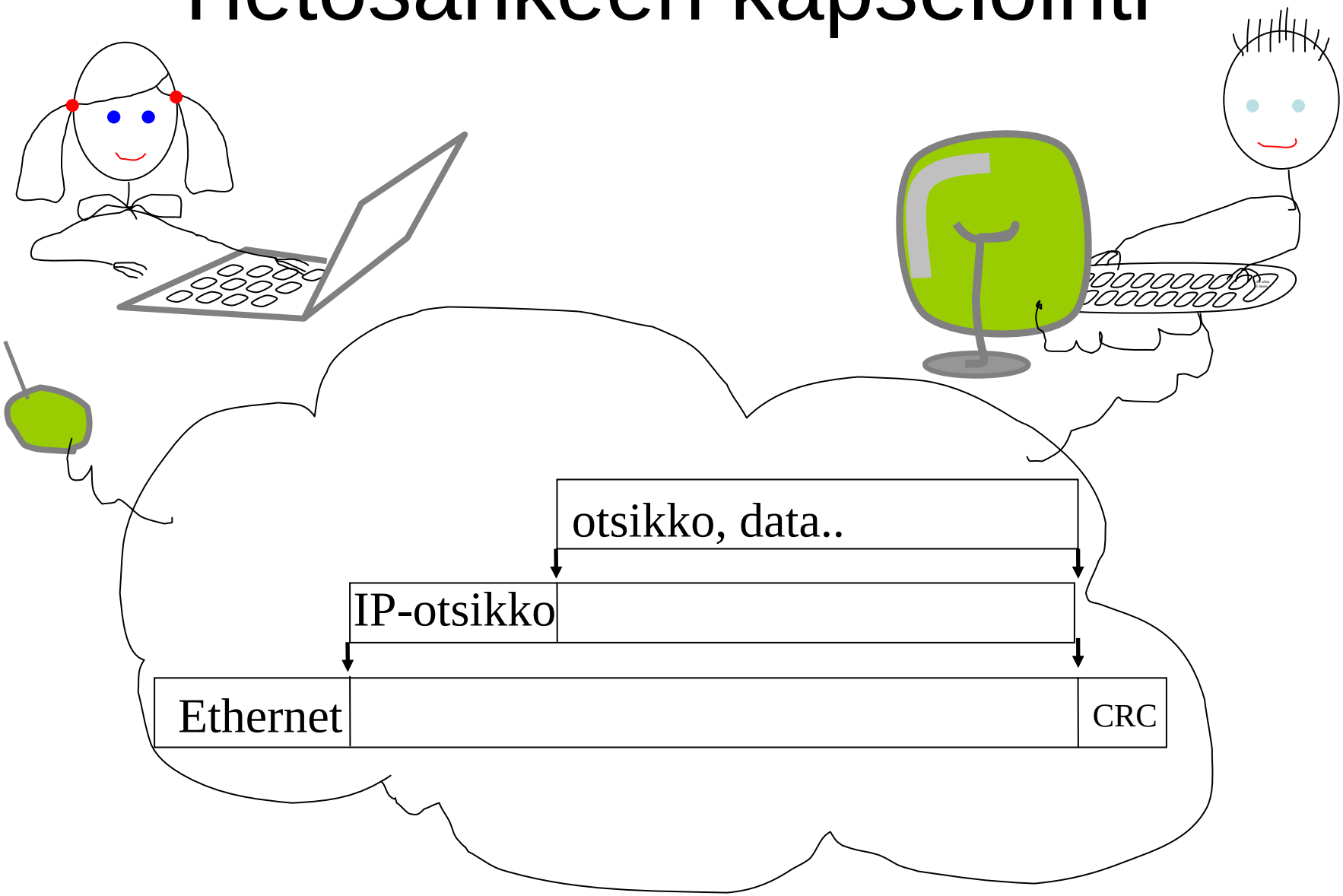
Internet-protokolla



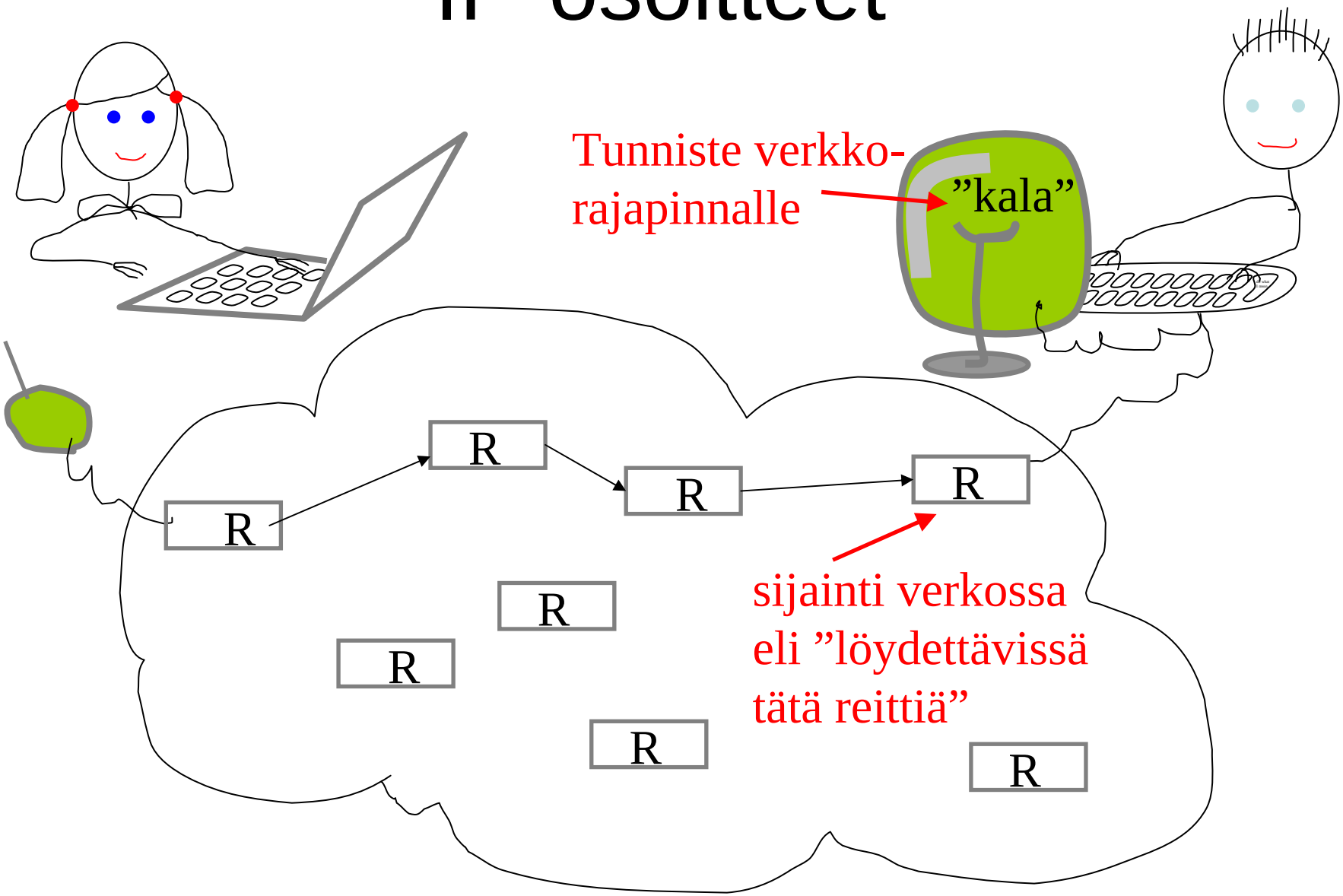


- Internet-protokolla on yhdistävä tekijä kaikkien sovellusten ja kaikenlaisten verkko-teknologioiden välissä

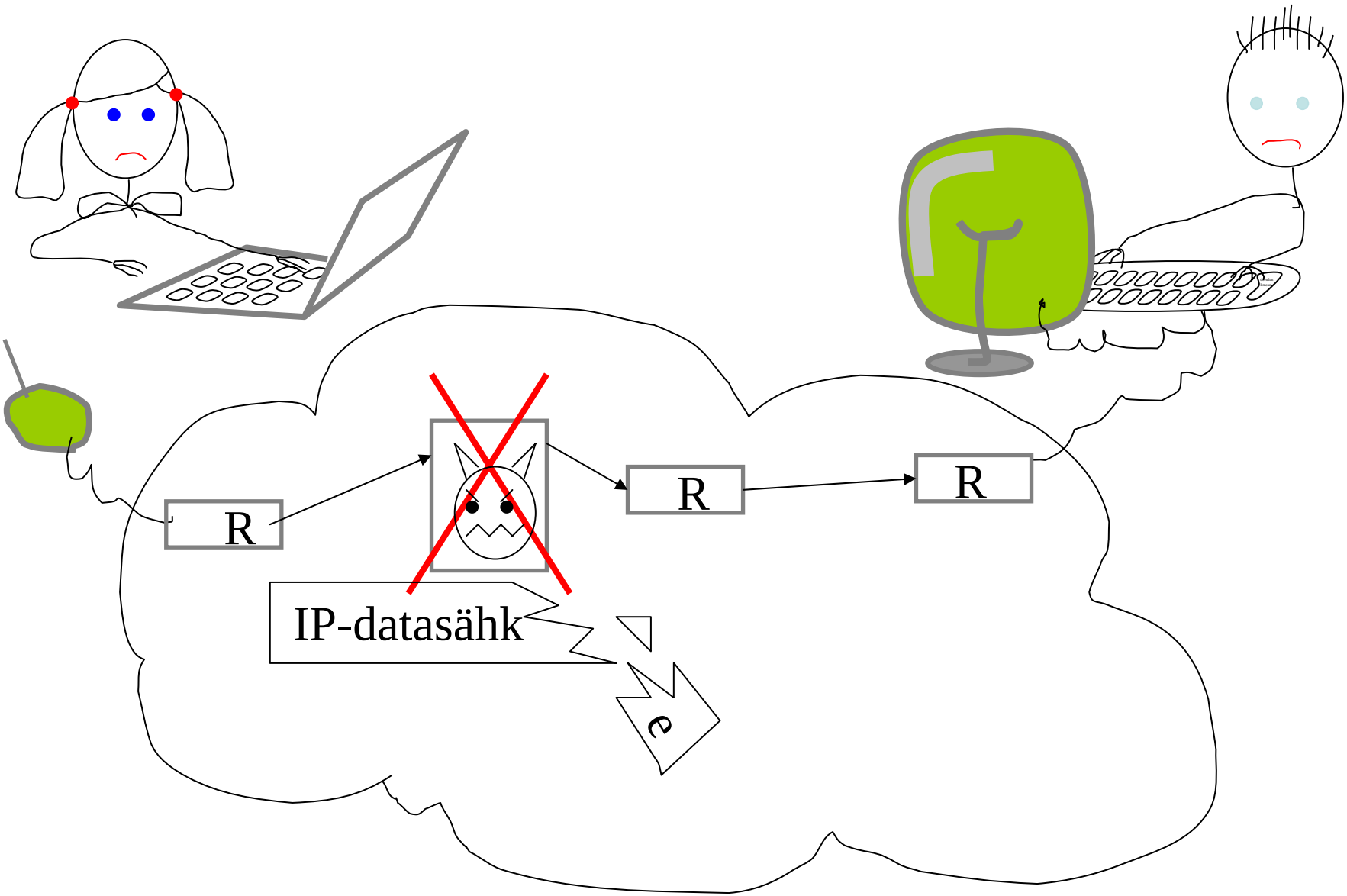
Tietosähkeen kapselointi

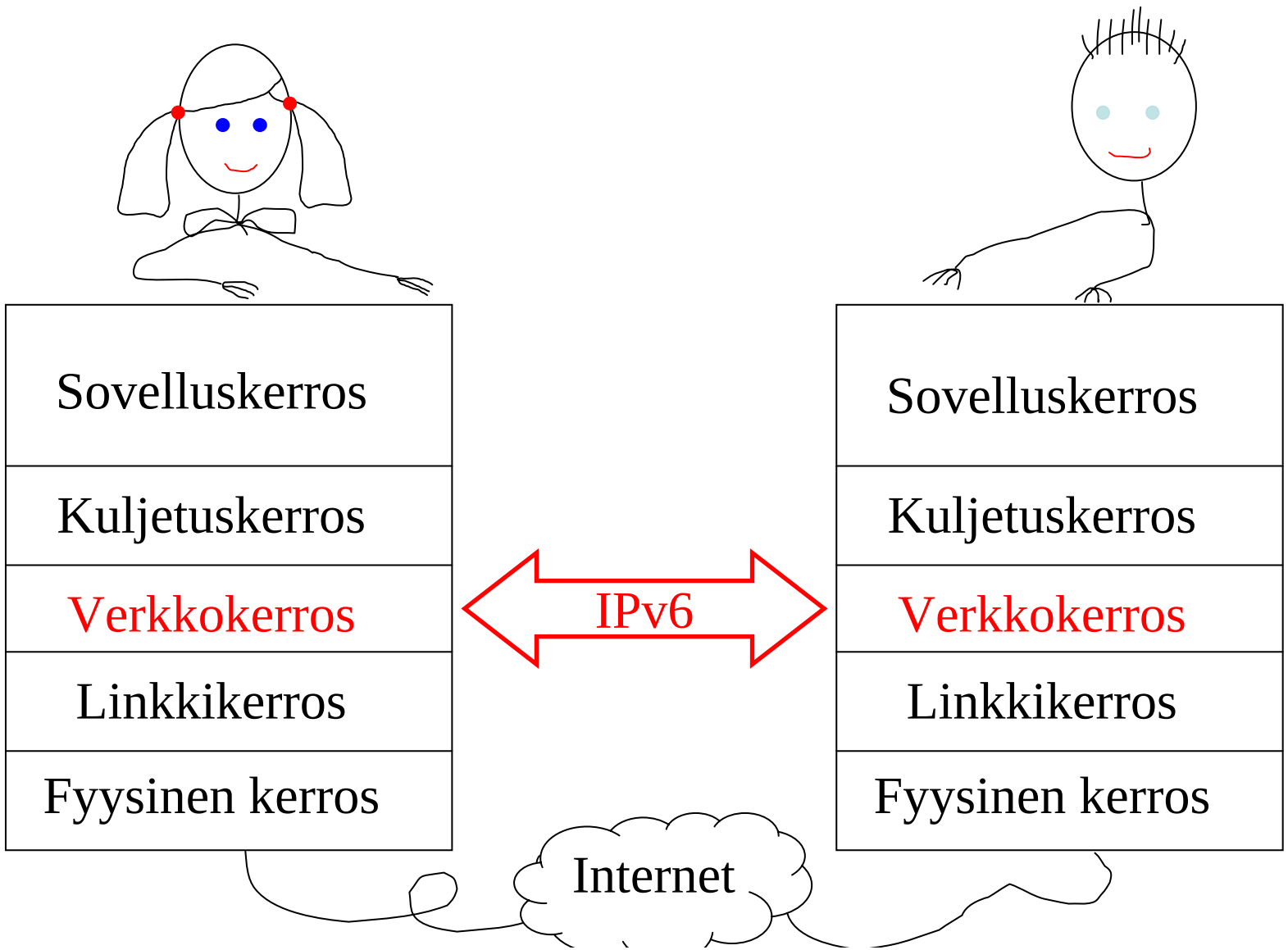


IP-osoitteet

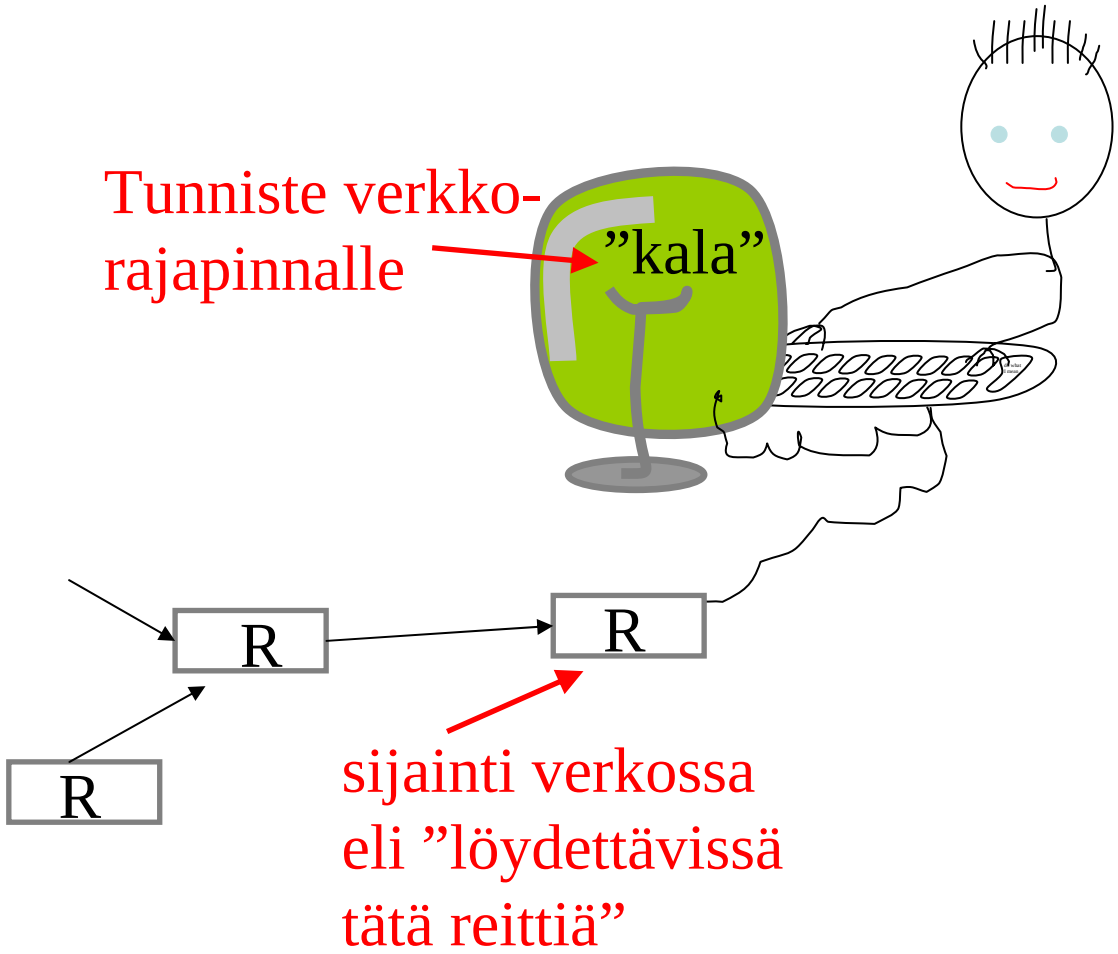


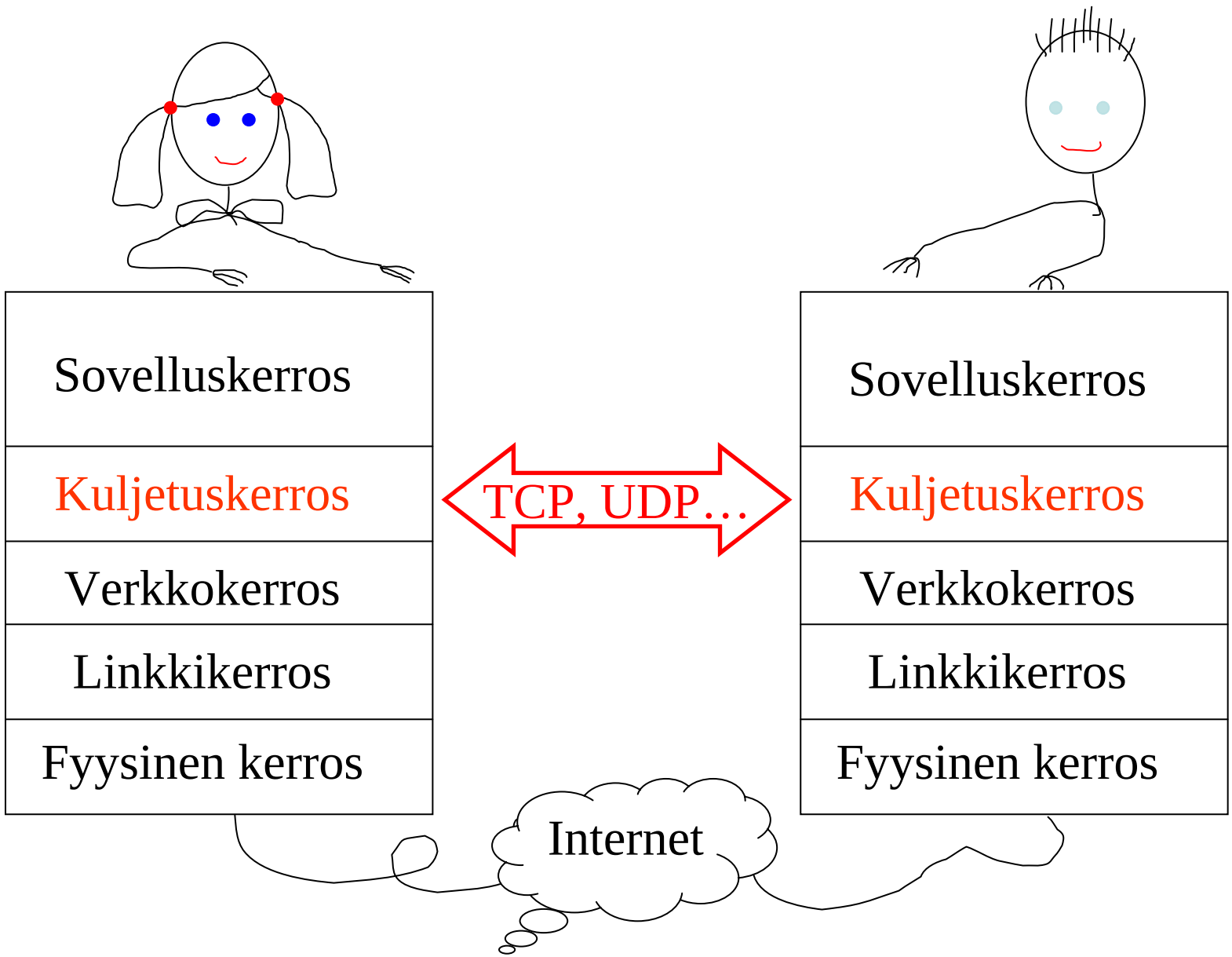
Virhetilanteet




Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
IPv6
Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
Internet

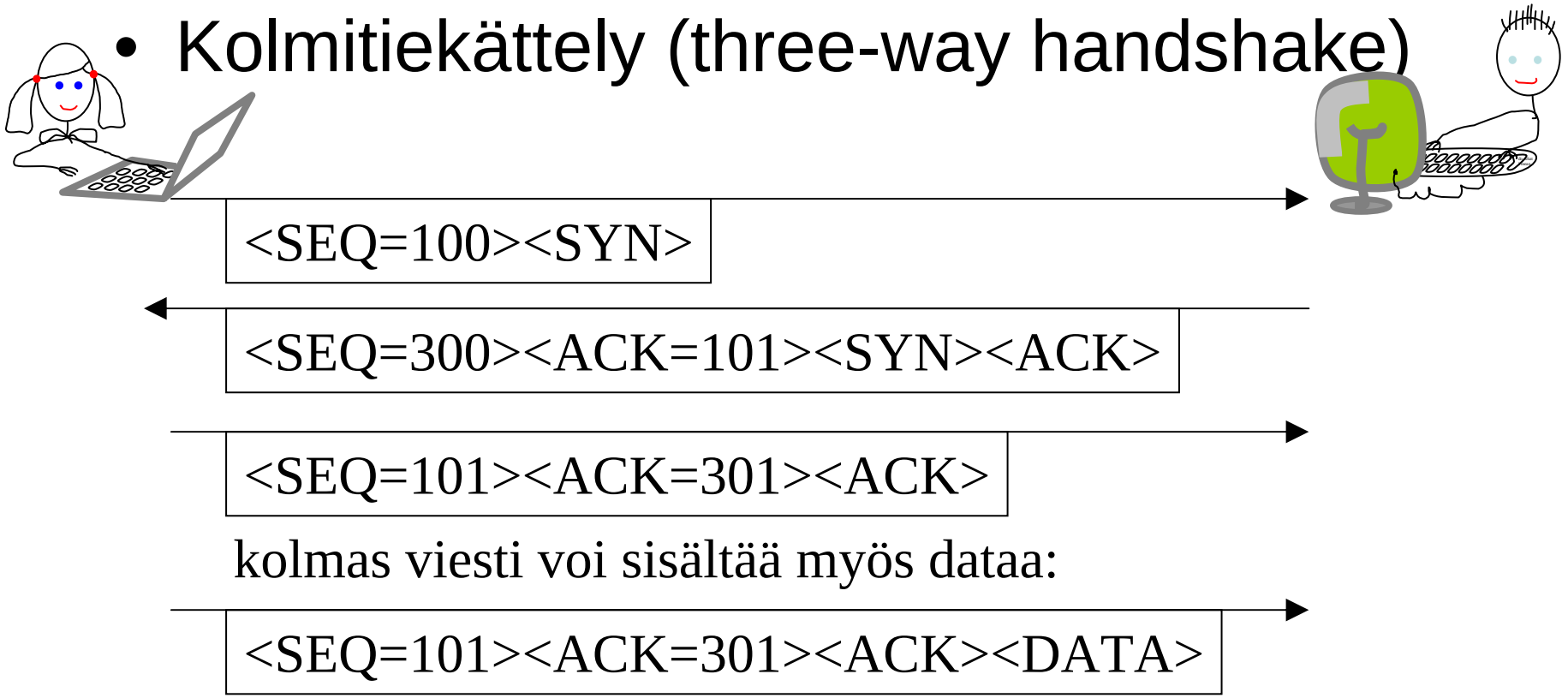
IPv6-osoitteet



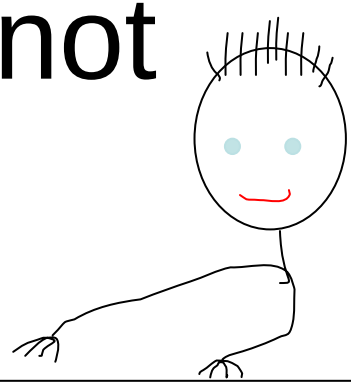

Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
TCP, UDP…
Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
Internet

Yhteyden muodostus

- Kolmitiekättely (three-way handshake)

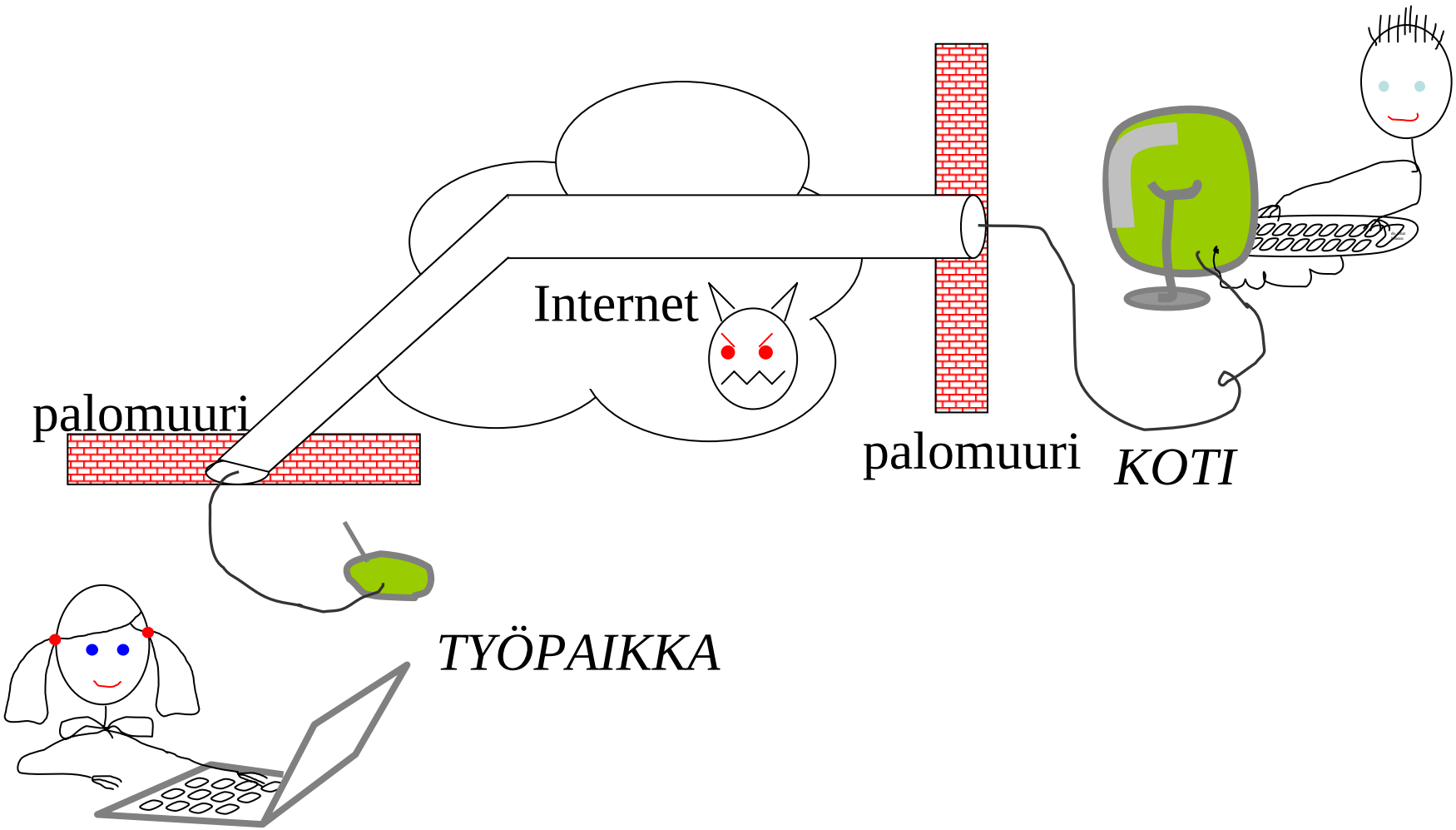


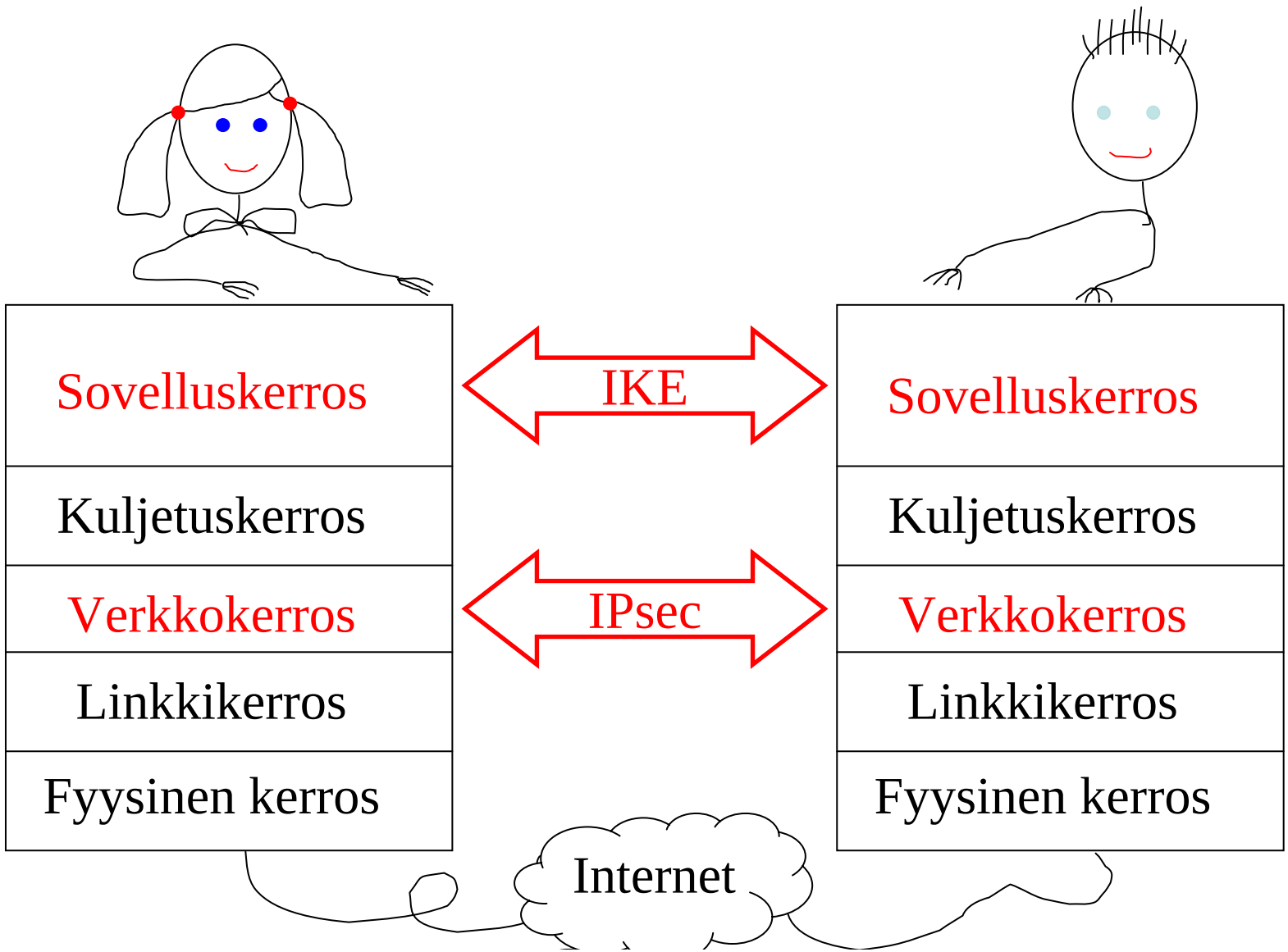
Seuraavat luennot



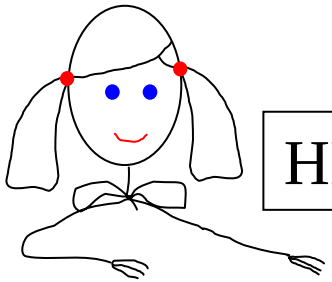
27.9 Nimipalvelu, Bength Sahlin

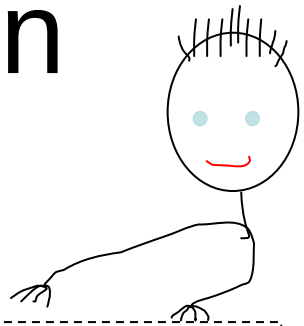
25.9. Reititys, osa 2, Janne Lindqvist


Internet
palomuuri
palomuuri
KOTI
TYÖPAIKKA


Sovelluskerros
IKE
Sovelluskerros
Kuljetuskerros
Kuljetuskerros
Verkkokerros
IPsec
Verkkokerros
Linkkikerros
Linkkikerros
Fyysinen kerros
Fyysinen kerros
Internet

IKE-SA:n perustaminen





HDR	SA_i	KE_i	N_i

→

←

HDR	SA_r	KE_r	N_r	[CERTREQ]

HDR*	ID_i	[CERT]	[CERTREQ]
$[ID_r]$	AUTH	SA_{i2}	TS_i	TS_r

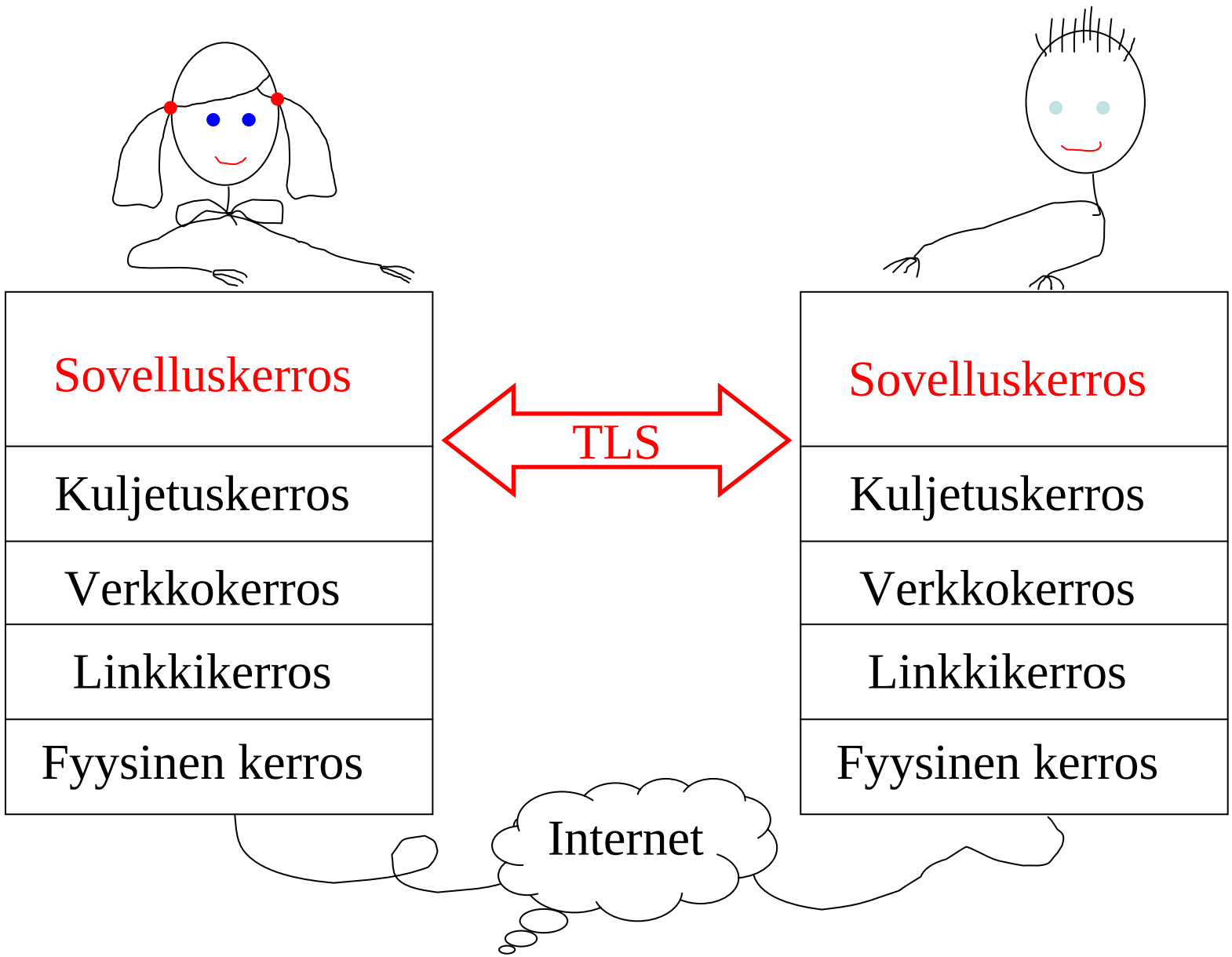
→

←

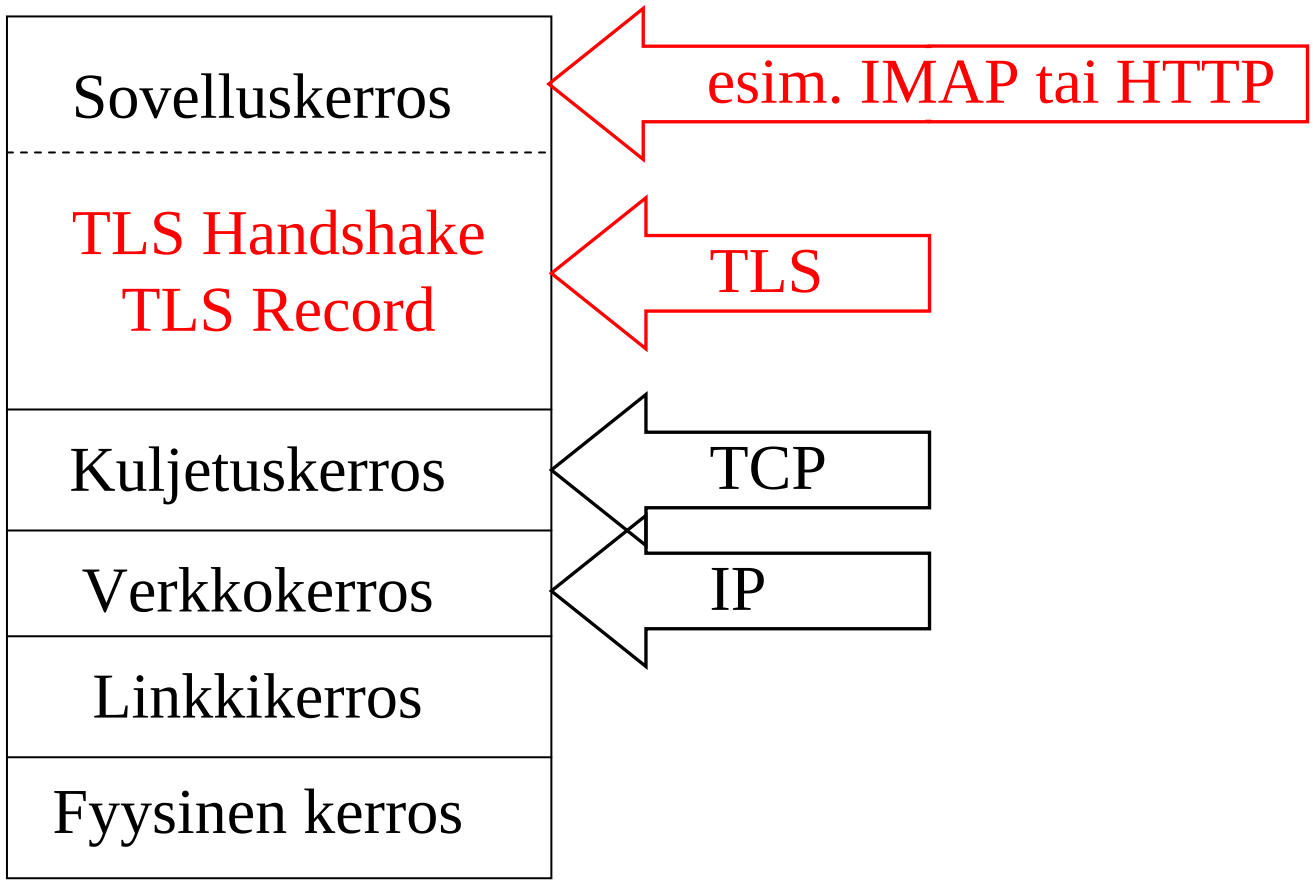
HDR*	ID_r	[CERT]	AUTH
SA_{r2}	TS_i	TS_r	

** kaikki otsikon jälkeen on suojattu*

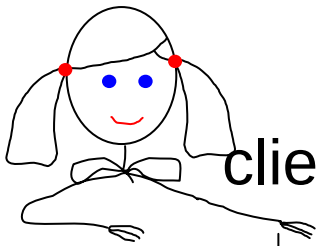
IKE-SA perustettu


Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
TLS
Sovelluskerros
Kuljetuskerros
Verkkokerros
Linkkikerros
Fyysinen kerros
Internet

Protokollapino



TLS Handshake Protocol



client

server

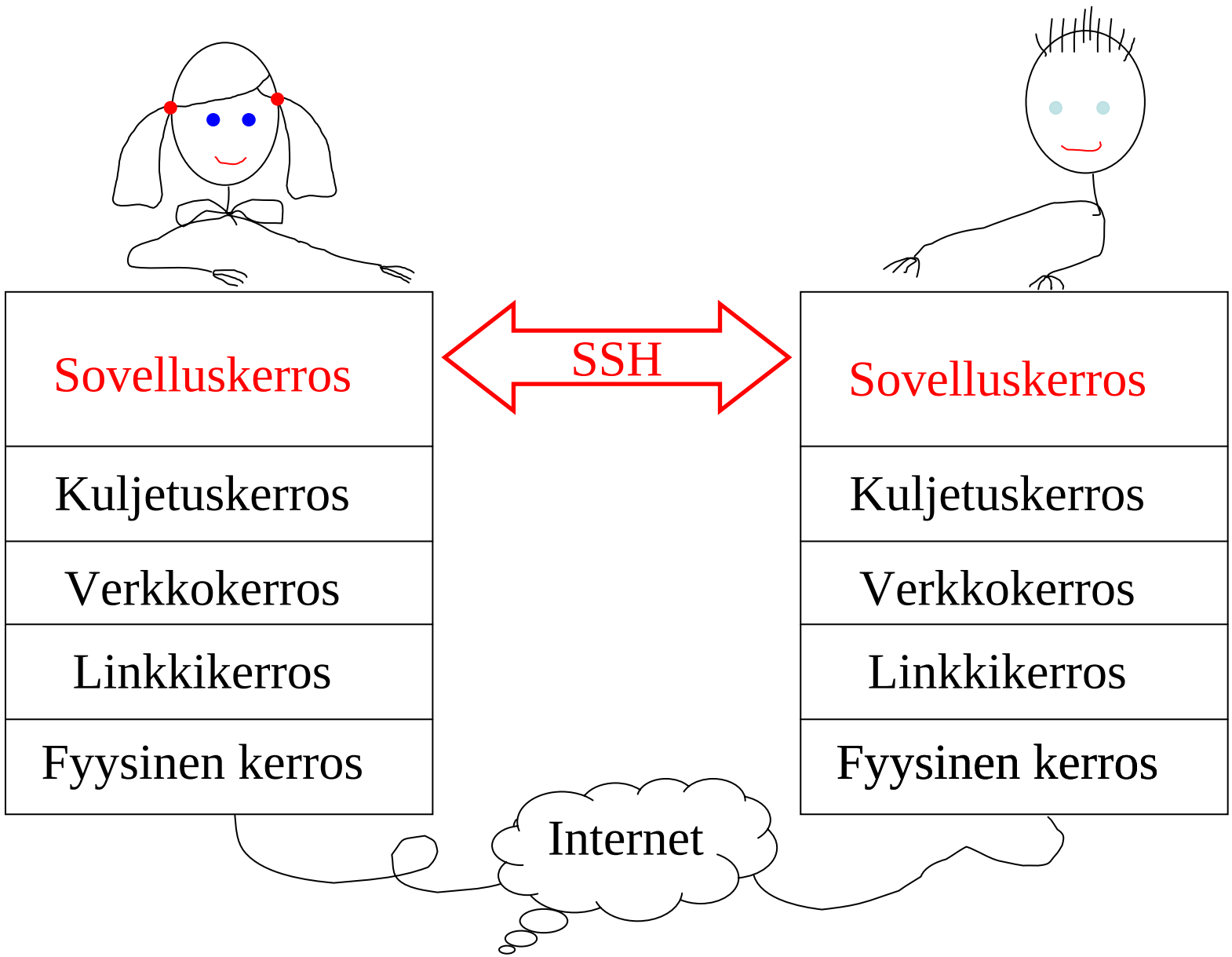
ClientHello

ServerHello [Certificate]
[ServerKeyExchange]
[CertificateRequest]Done

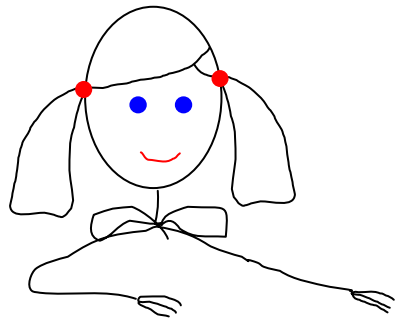
[Certificate]ClientKeyExchange
[CertificateVerify]ChangeCipherSpec*Finished

ChangeCipherSpec* Finished

Sovelluksen viestit turvattua yhteyttä käyttäen


Sovelluskerros
SSH
Sovelluskerros
Kuljetuskerros
Kuljetuskerros
Verkkokerros
Verkkokerros
Linkkikerros
Linkkikerros
Fyysinen kerros
Fyysinen kerros
Internet

	IPsec	TLS	SSH
Molempien tunnistus			
Salaus			
Eheys			
MitM			
Toistohyök.			
DoS			



Käyttäjän sovellukset:
sähköposti (SMTP, IMAP)
WWW (HTTP)
FTP, SSH, …

Infrastruktuuri-palvelut: DNS, SNMP
Tietoturvaratkaisu TLS

Sovelluskerros

Socket-rajapinta ohjelmoinnille

Kuljetuskerros

TCP, UDP, luotettava tiedonsiirto, portit

IP, osoitteet, reititys
tietoturva

Verkkokerros

Linkkikerros

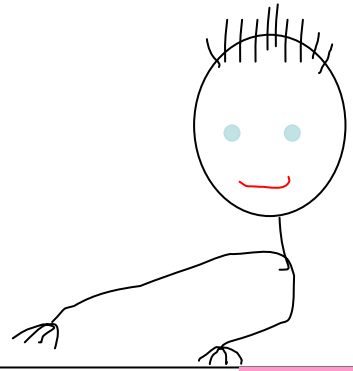
Ethernet, miten IP-osoitetta vastaava ethernet osoite löydetään (ja toistepäin)

Aiheuttaa viiveitä, häviöitä jne.
(out of scope)

Fyysinen kerros

Osatentti 1

Osatentti 2



- DNS& DNSsec
- TCP ja UDP
- IPv4
- IPv6
- Reititys
- Multicast
- osoitteet

Sovelluskerros

Kuljetuskerros

Verkkokerros

Linkkikerros

Fyysinen kerros

Protokollasuunnittelu

- SNMP
- verkko-ohjelmointi
- TLS ja SSH
- IPsec