

INF105 - 09
Sende data: nettverk

David Grellscheid

Q&A

https://www.inf105.org/notater/



Storytime - DeCSS

- Content Scrambling System - Kopibeskyttelse på DVD
- DVD kan bare spilles på lisenserte enheter
- dvs. ikke på Linux / BSD
- DeCSS publisert i 1999

Storytime - DeCSS

DeCSS was devised by three people, two of whom remain anonymous. It was on the Internet mailing list LiViD in October 1999. The one known author of the trio is Norwegian programmer Jon Lech Johansen, whose home was raided in 2000 by Norwegian police. Still a teenager at the time, he was put on trial in a Norwegian court for violating Norwegian Criminal Code section 145,[1] and faced a possible jail sentence of two years and large fines, but was acquitted of all charges in early 2003. On 5 March 2003, a Norwegian appeals court ruled that Johansen would have to be retried. The court said that arguments filed by the prosecutor and additional evidence merited another trial. On 22 December 2003, the appeals court agreed with the acquittal, and on 5 January 2004, Norway's Økokrim (Economic Crime Unit) decided not to pursue the case further.

https://en.wikipedia.org/wiki/DeCSS

Storytime - DeCSS

- WIPO copyright treaty / DMCA / §99 åndsverksloven
  - no circumvention of effective copy-protection measures

- hva er "effective measures"? etc...

- f.eks fra en sak i USA (2000):
  deling av utførbar kode forbudt, men beskrivelse er OK

  - https://www.cs.cmu.edu/~dst/DeCSS/Gallery/

  - https://www.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html

  - https://t5k.org/curios/page.php?number_id=1214

Fortsatt aktuelt

- Til slutt skal brukeren se filmen
- Signalet er tilgjengelig ett sted i PCen
- Introduksjon av HDCP (high-bandwidth digital content protection)
  https://en.wikipedia.org/wiki/High-bandwidth_Digital_Content_Protection
- datakilde ber om autorisert avspilling,
  sender kryptert signal bare mellom autoriserte enheter
- "autorisert enhet" bare hvis sikret mot kopering
  (skjermdeling <-> se på film)

Fortsatt aktuelt

Trusted Computing / TPM brikker

- Combined with the other technologies, this provides a more restricted path for the music: encrypted I/O prevents the user from recording it as it is transmitted to the audio subsystem, memory locking prevents it from being dumped to regular disk files as it is being worked on, sealed storage curtails unauthorized access to it when saved to the hard drive, and remote attestation prevents unauthorized software from accessing the song even when it is used on other computers.

https://en.wikipedia.org/wiki/Trusted_Computing

Copyright og brukerrettigheter

- Første copyright-lov hadde noen få år med beskyttelse
  -> ble skiftet mer og mer i favør av produsentene

- Nå: diskusjon rundt TPM brikker:

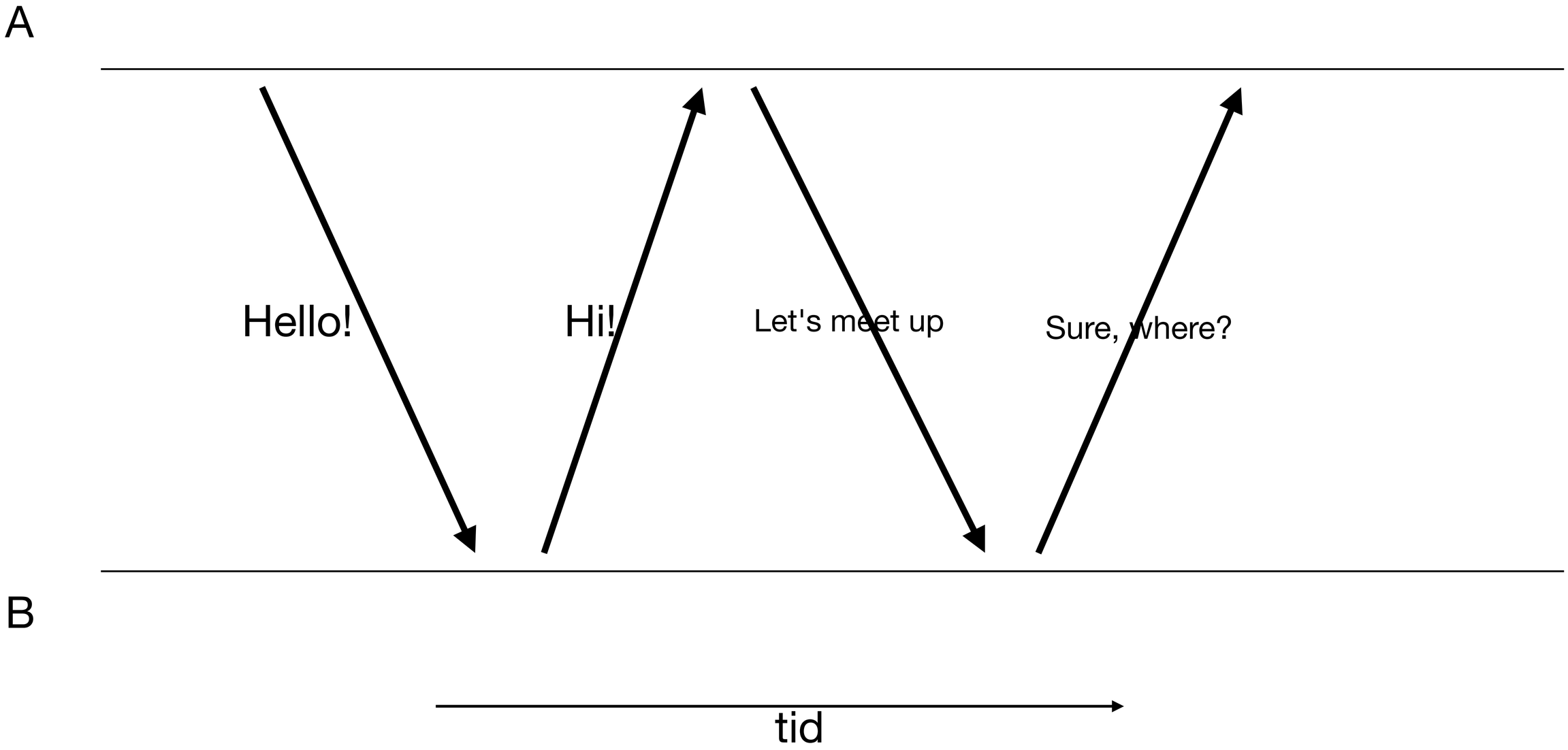
  TPM kan muligens stoppe installasjon av uautorisert OS

- https://en.wikipedia.org/wiki/Digital_rights_management
  https://en.wikipedia.org/wiki/Trusted_Computing
  https://en.wikipedia.org/wiki/Defective_by_Design

- hvem kontrollerer hva du kan gjøre med enhetene dine?

Sende data

Utveksling av meldinger



Over lang distanse...

- røyk, tromme, duer, bål, ...
- 1790: Semaphores
- fra 1800-tallet: elektriske systemer
- telegraf (morse: 1837)
  (1851: 30000 km i USA)
- 1. atlanterhavskabel 1866
- telefon 1878 / 1879
- radiotelegraf 1894

Terry Pratchett, "Going Postal" :-)

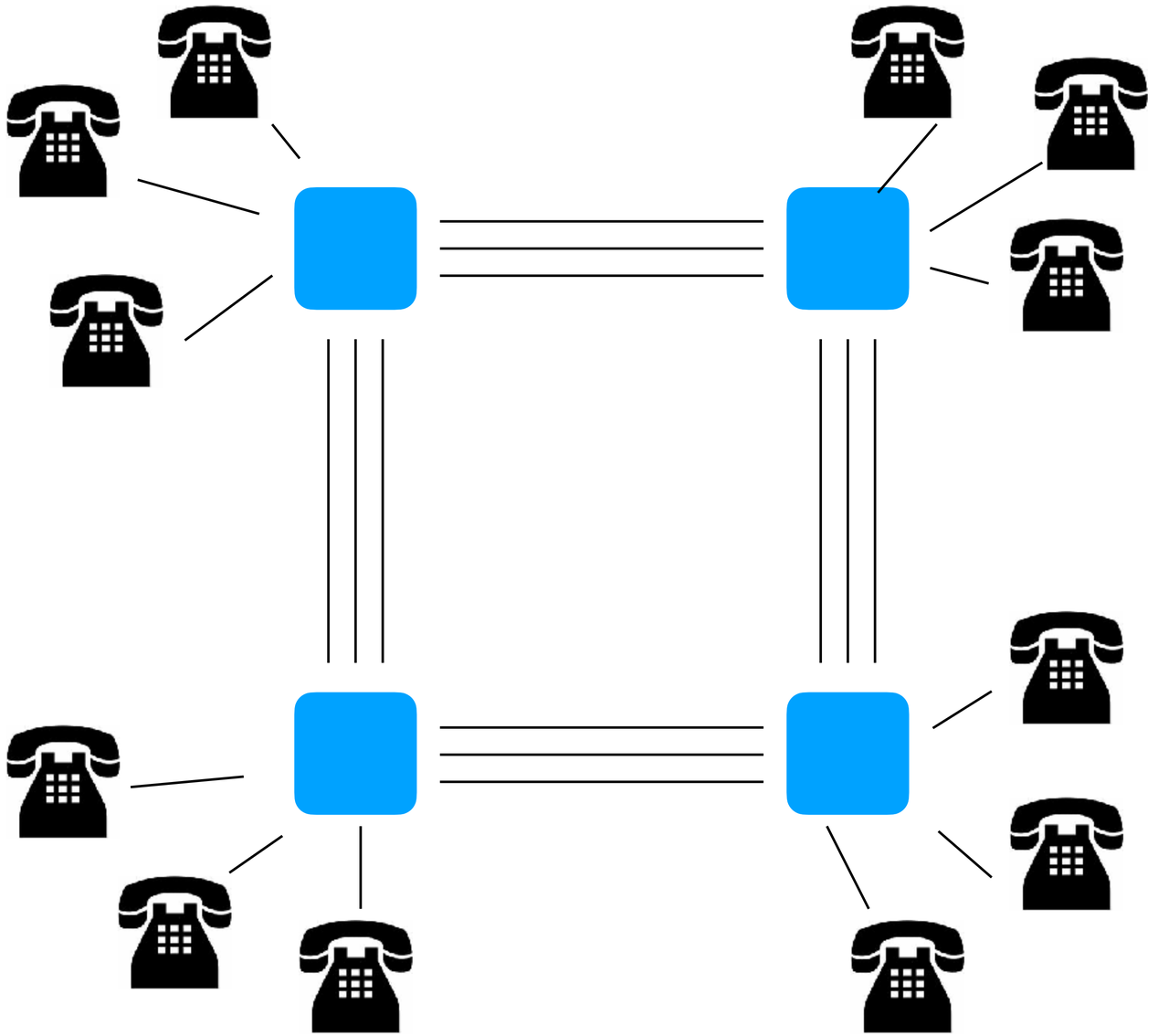


https://en.wikipedia.org/wiki/History_of_telecommunication

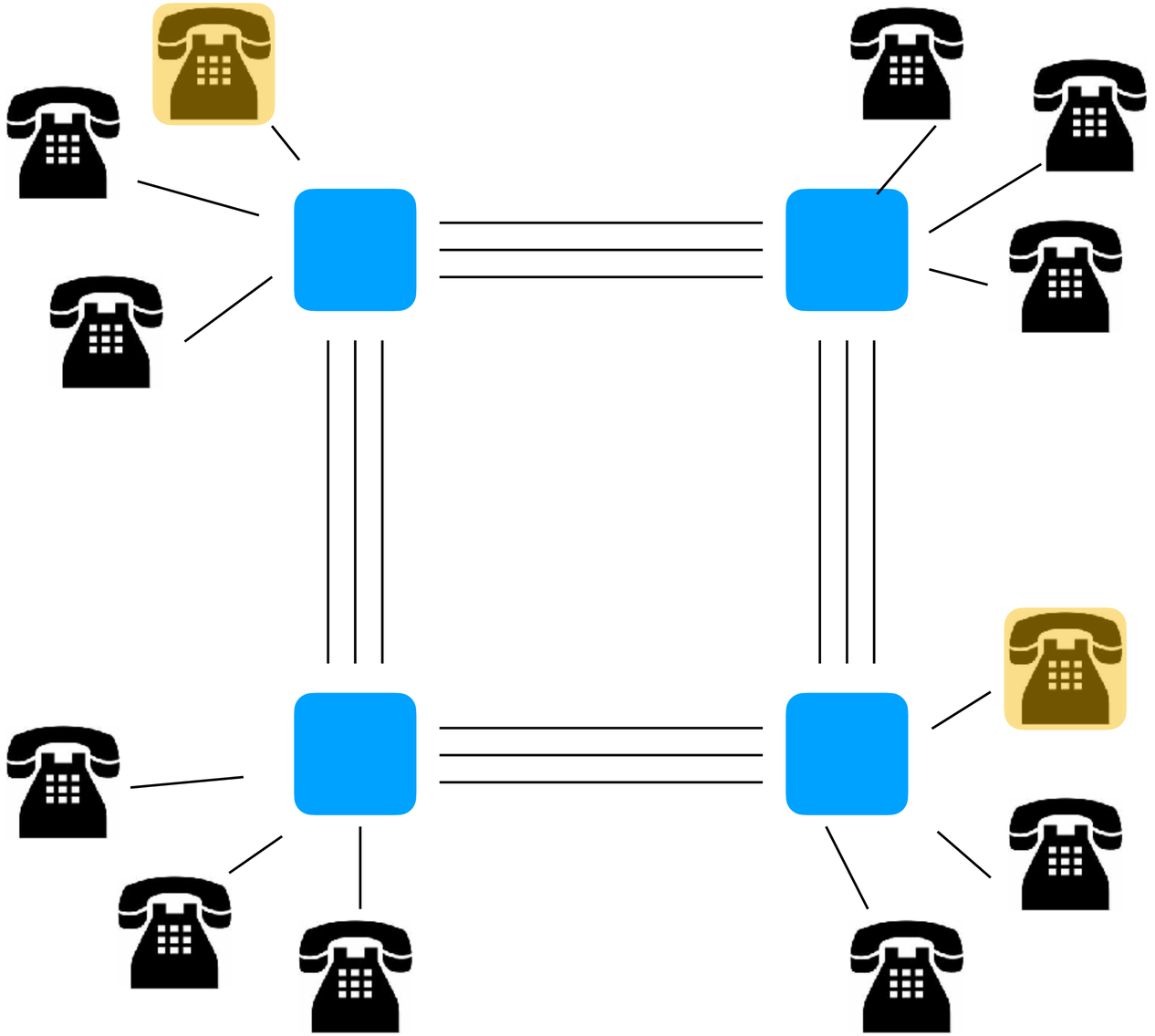
Circuit switching

- Analoge telefonsignaler brukte ***circuit switching***
- Garantert lenke fra A til B

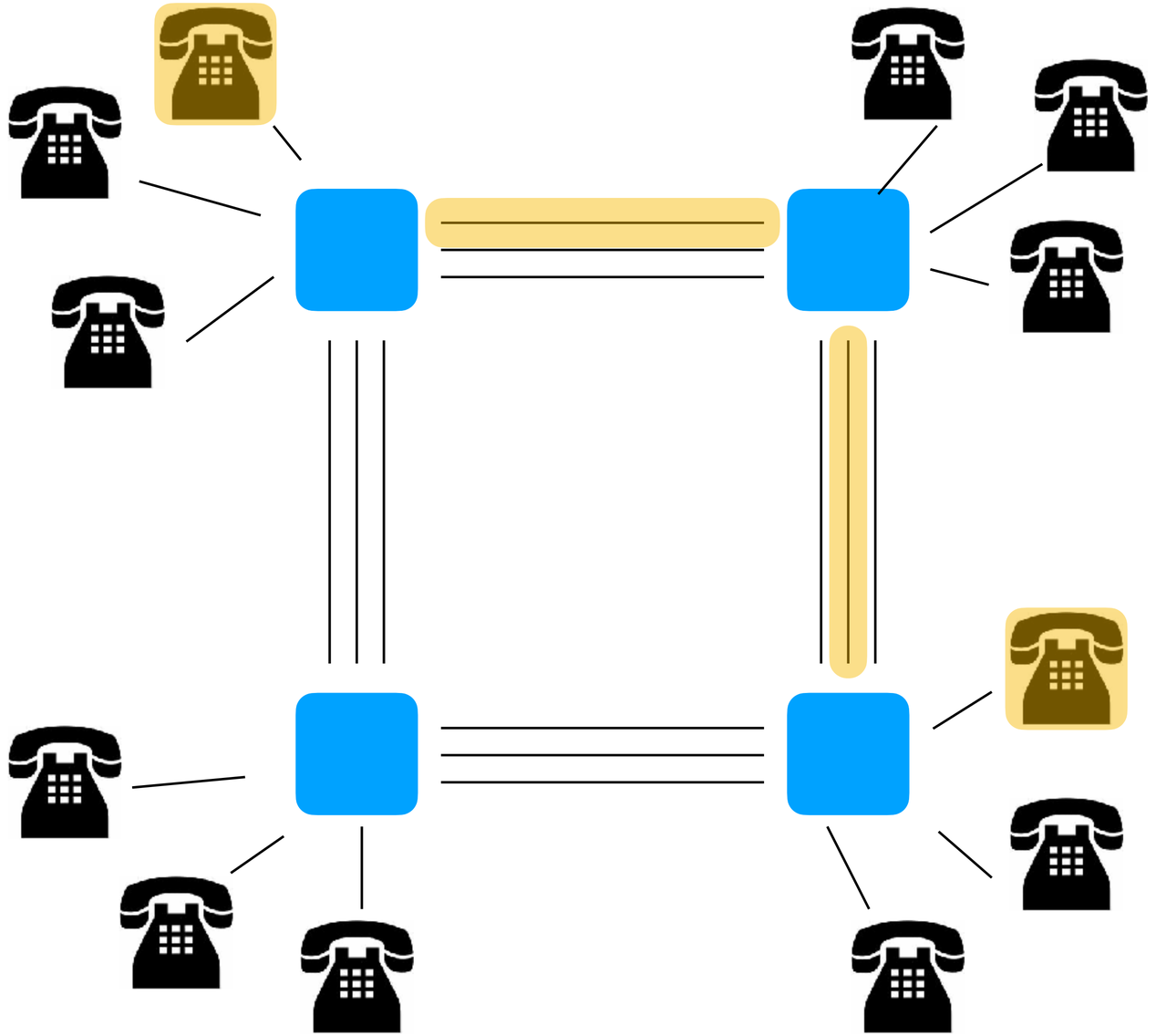
Circuit switched network



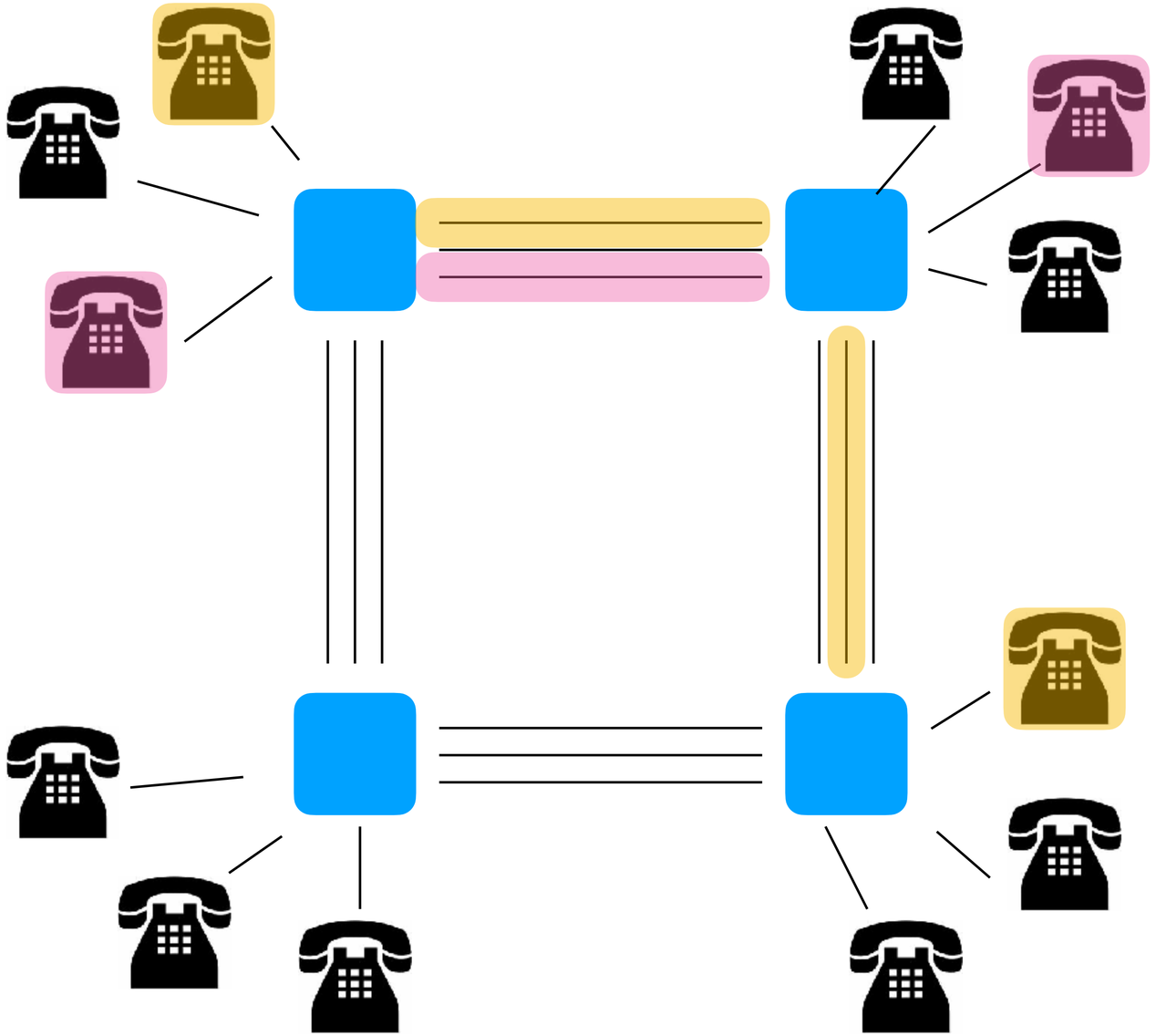
Circuit switched network



Circuit switched network

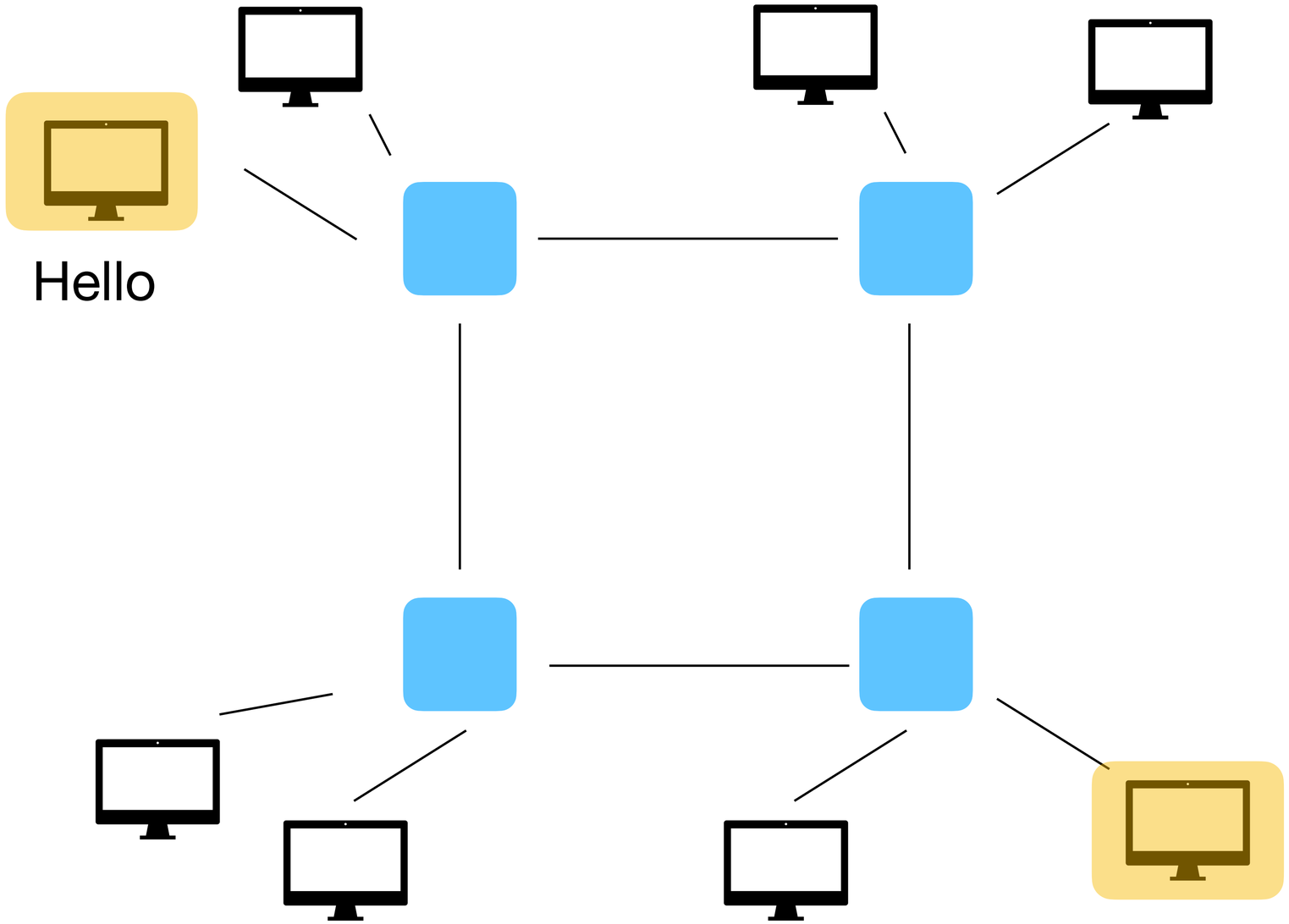


Circuit switched network

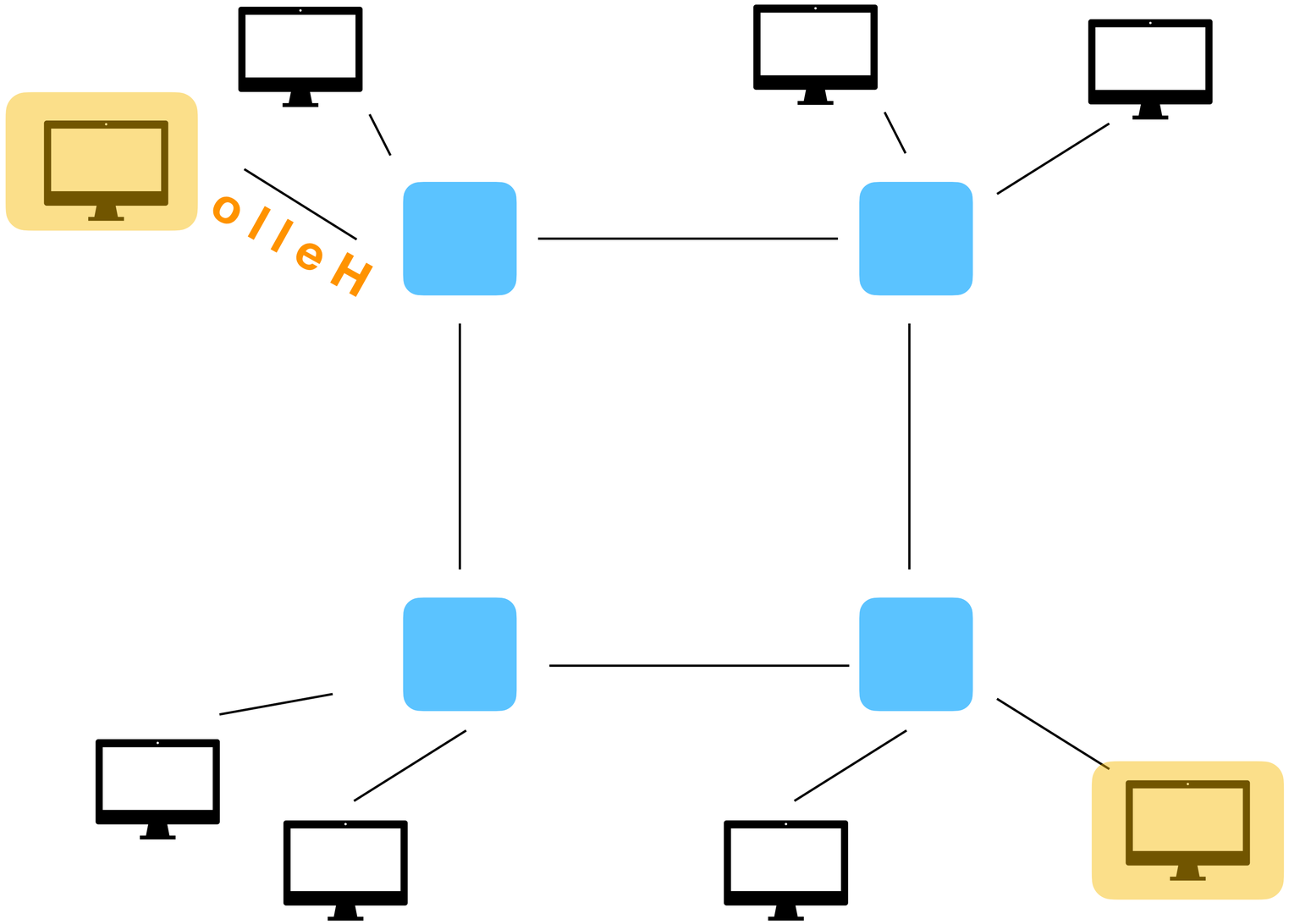


- Digitale signaler kan deles opp
- **Packet switching - 1960-tallet**
- Store and forward

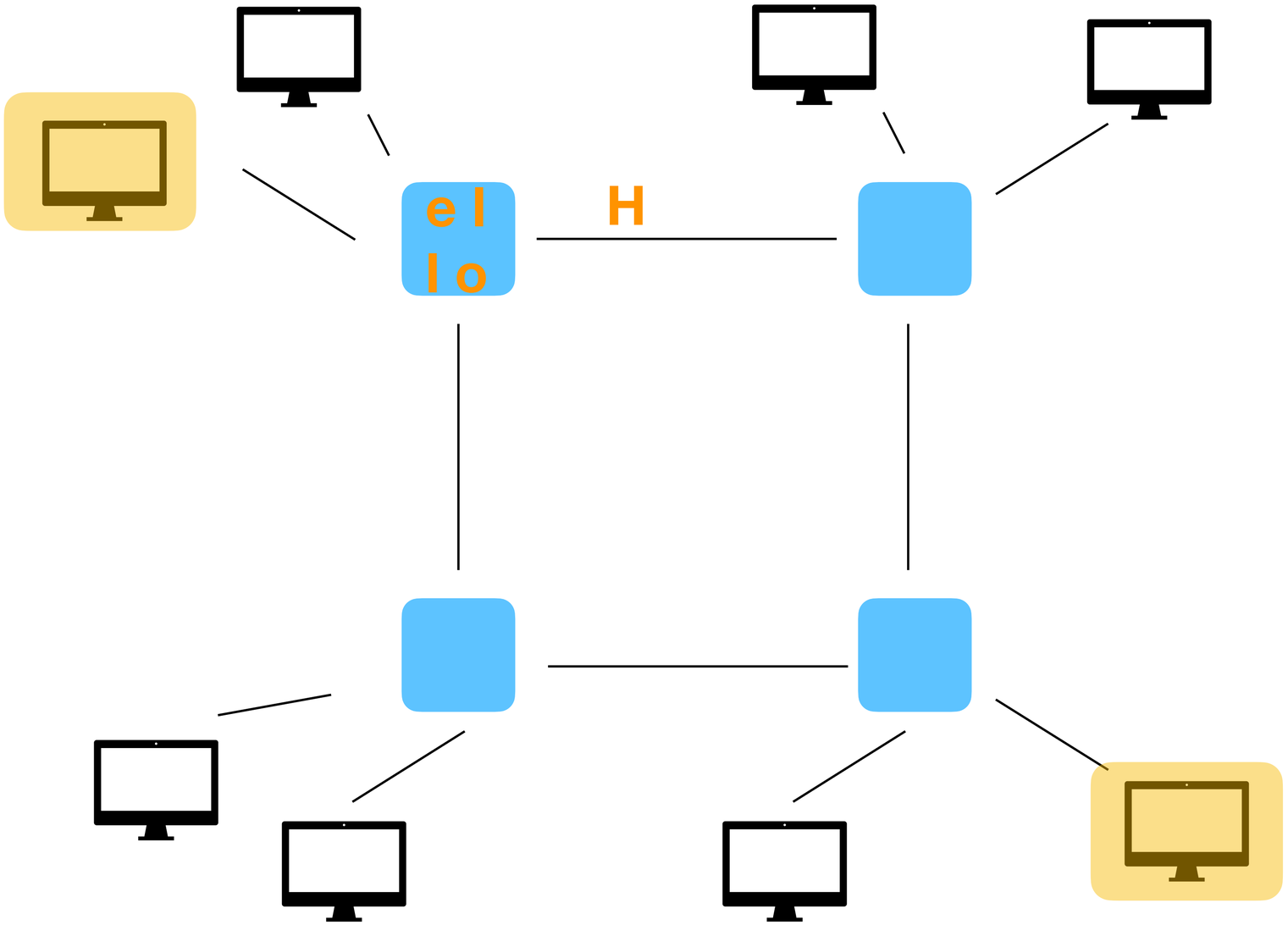
Packet switched network



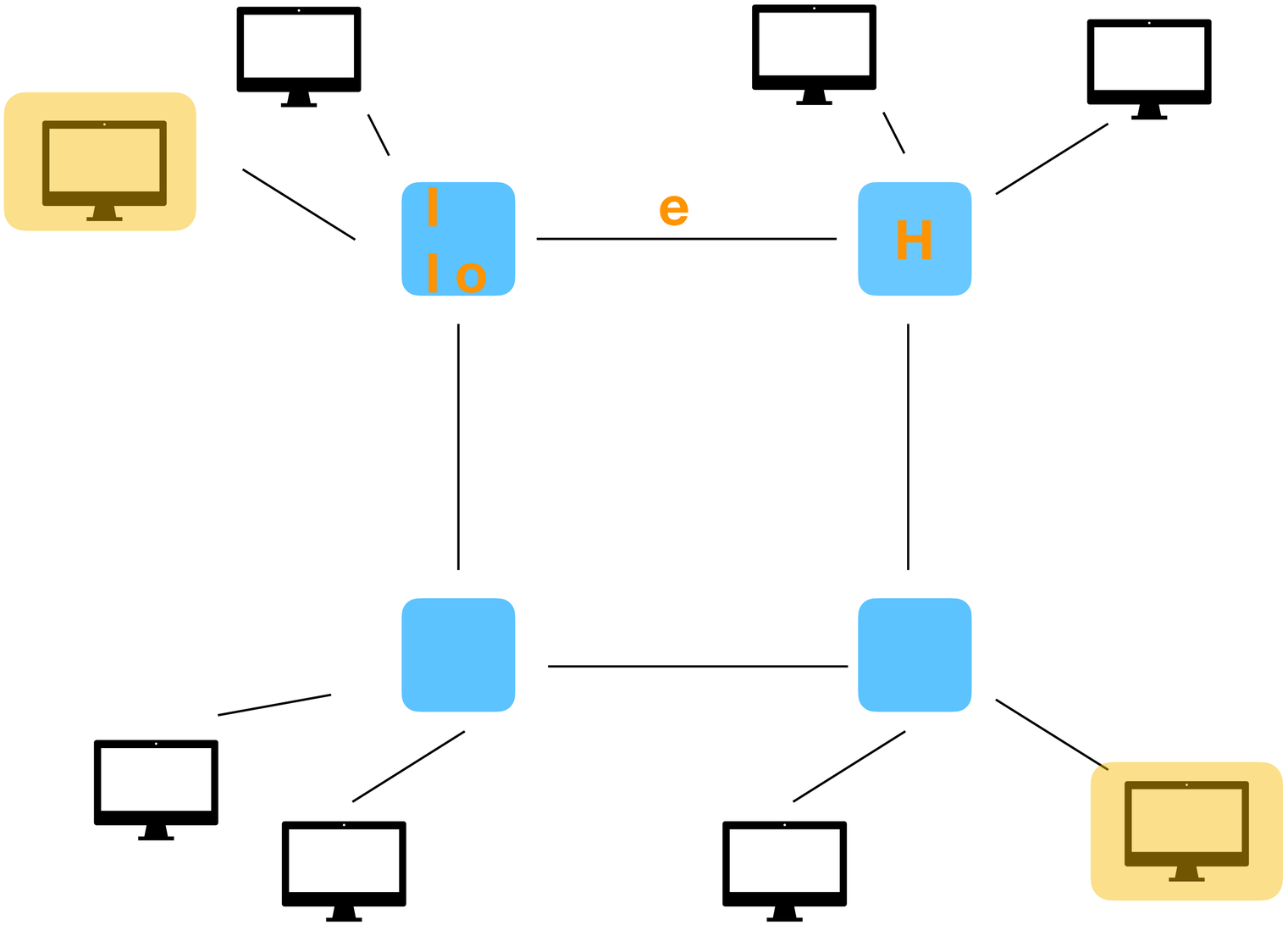
Packet switched network



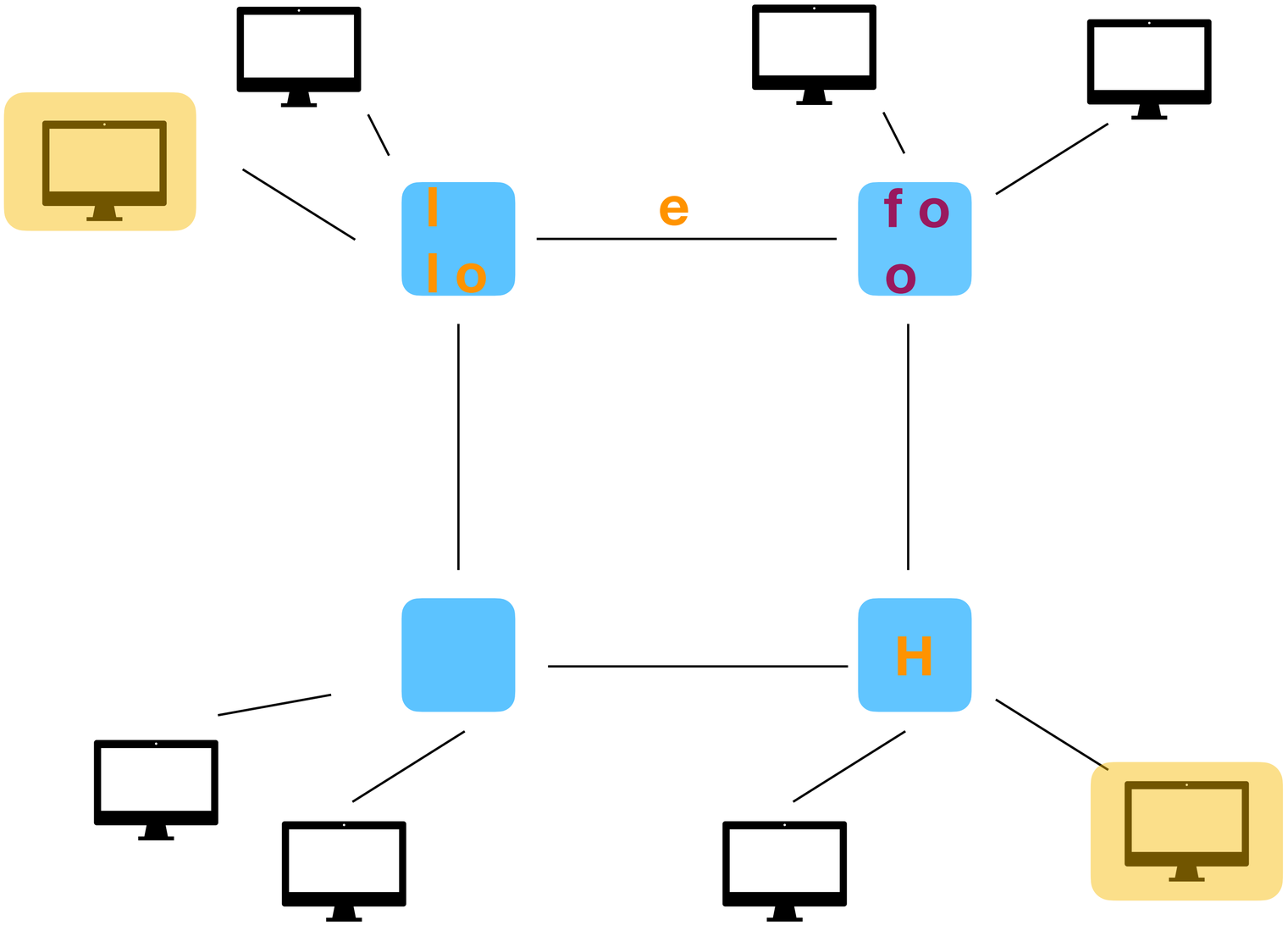
Packet switched network



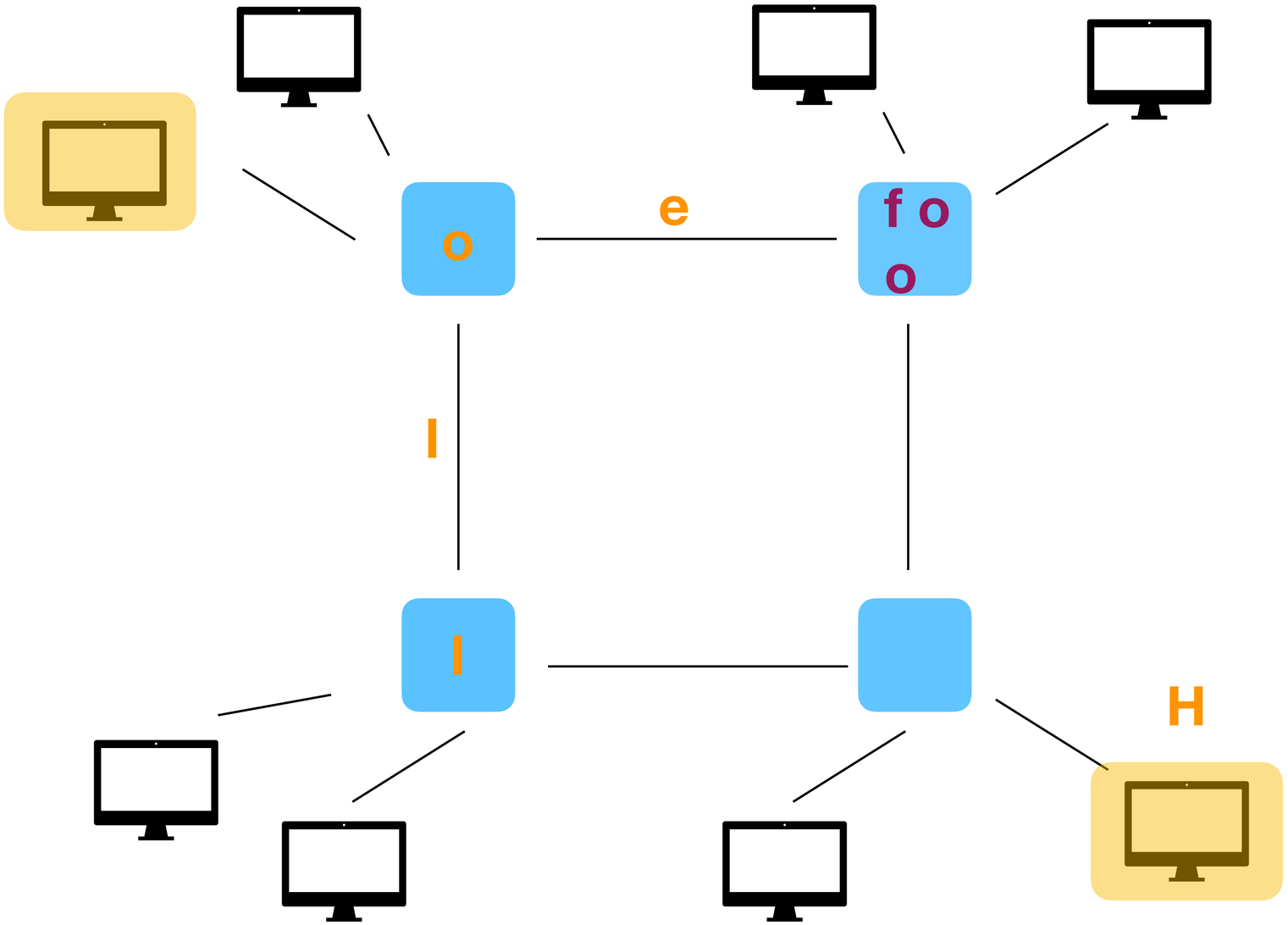
Packet switched network



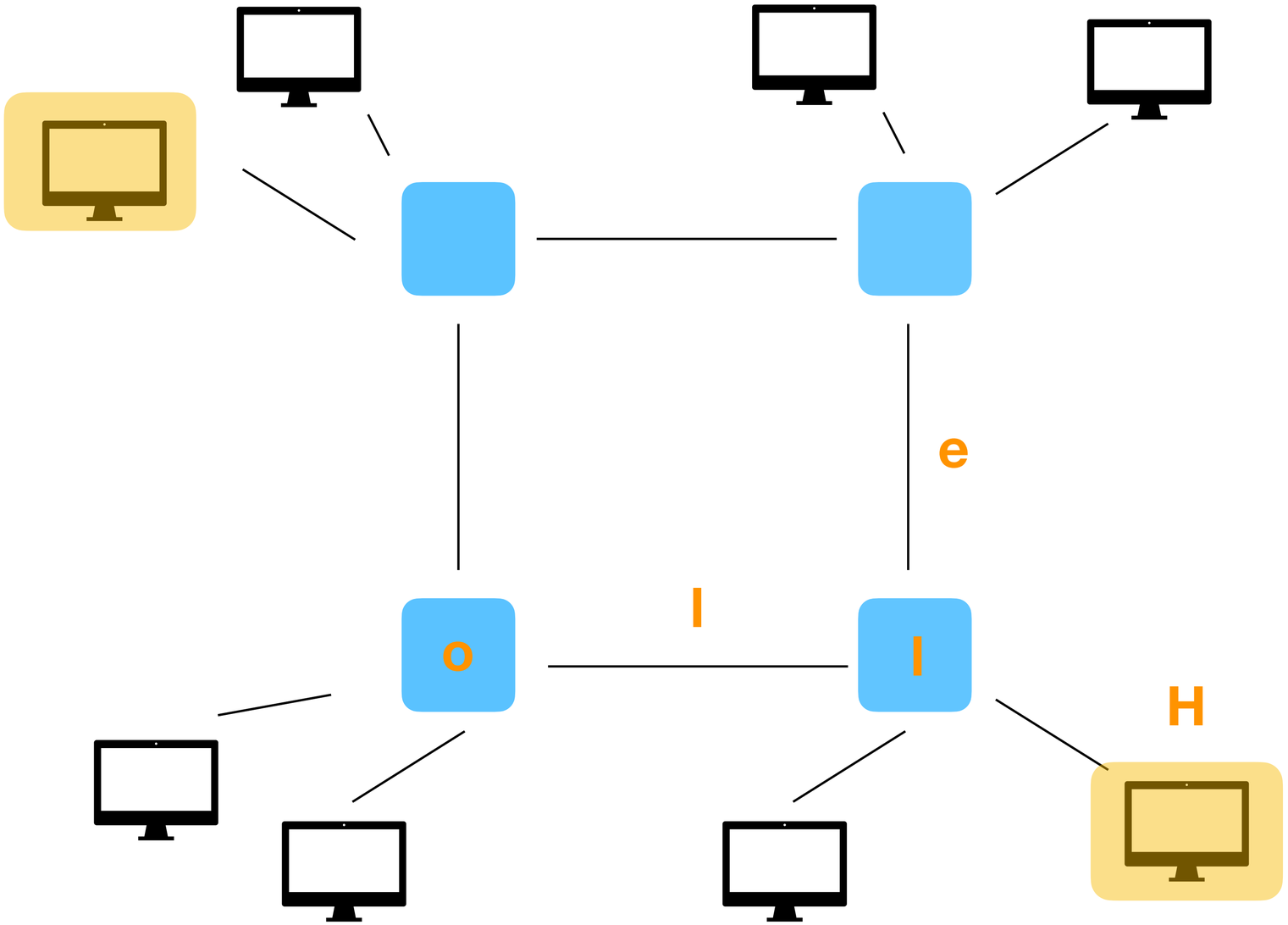
Packet switched network



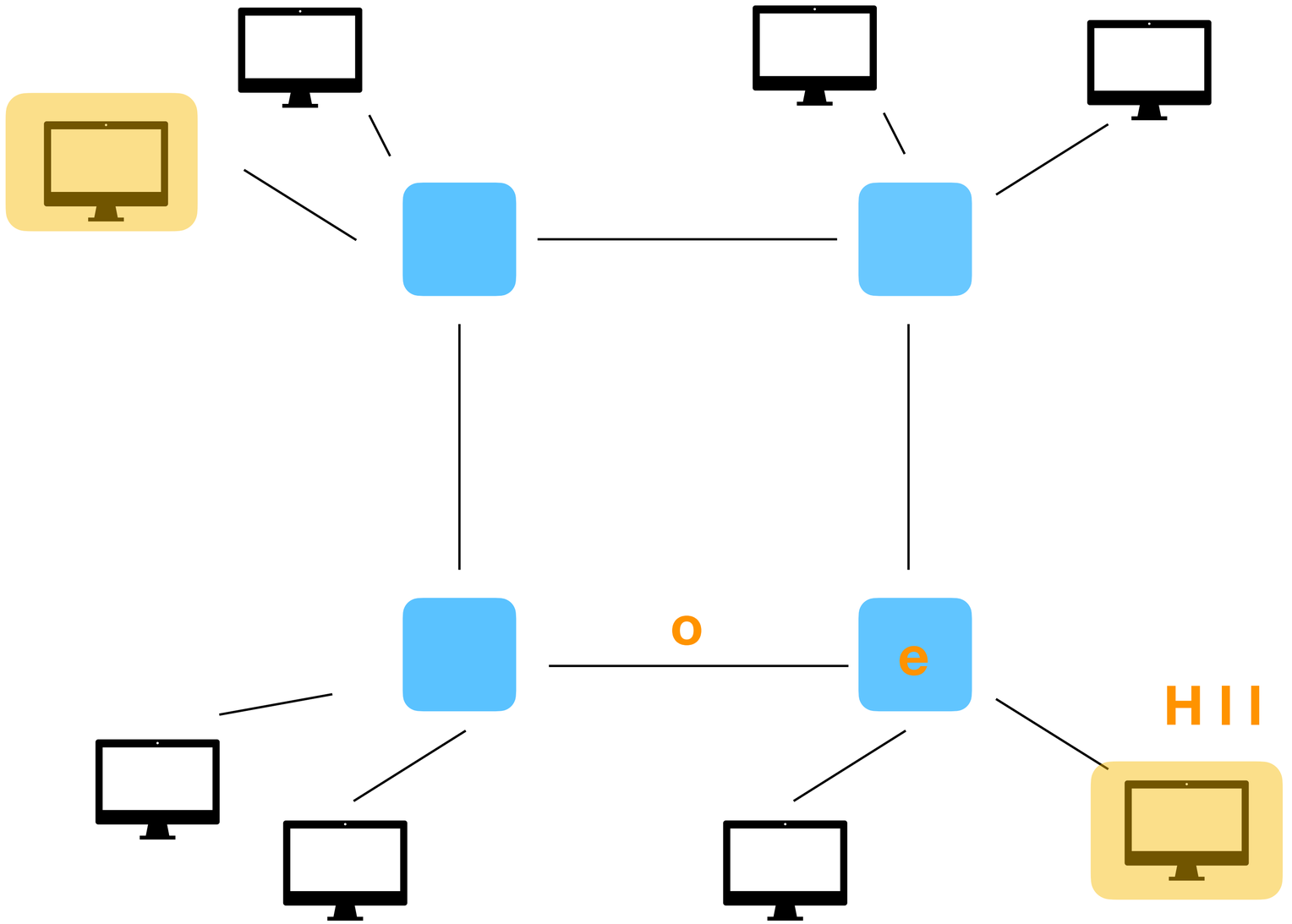
Packet switched network



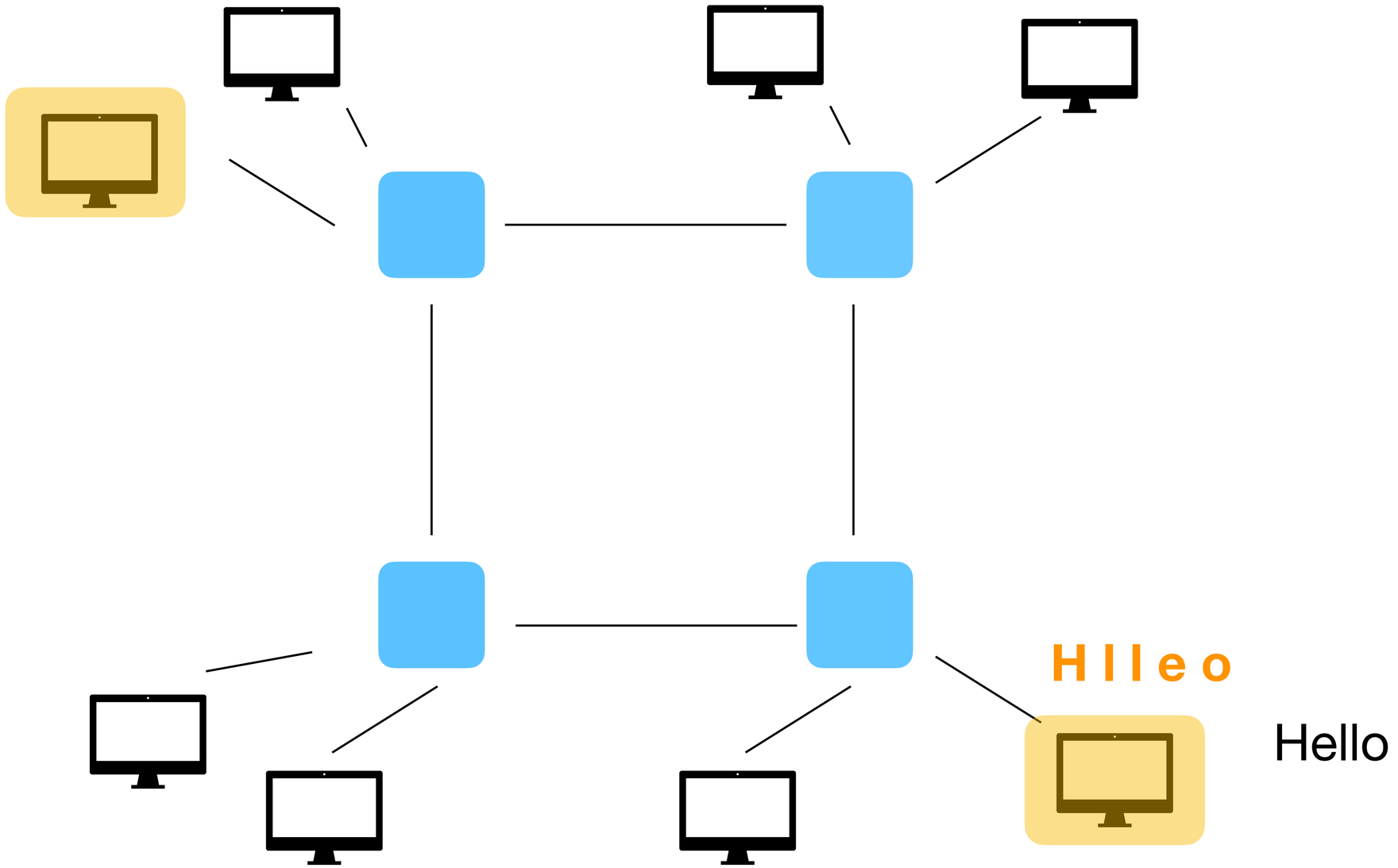
Packet switched network



Packet switched network

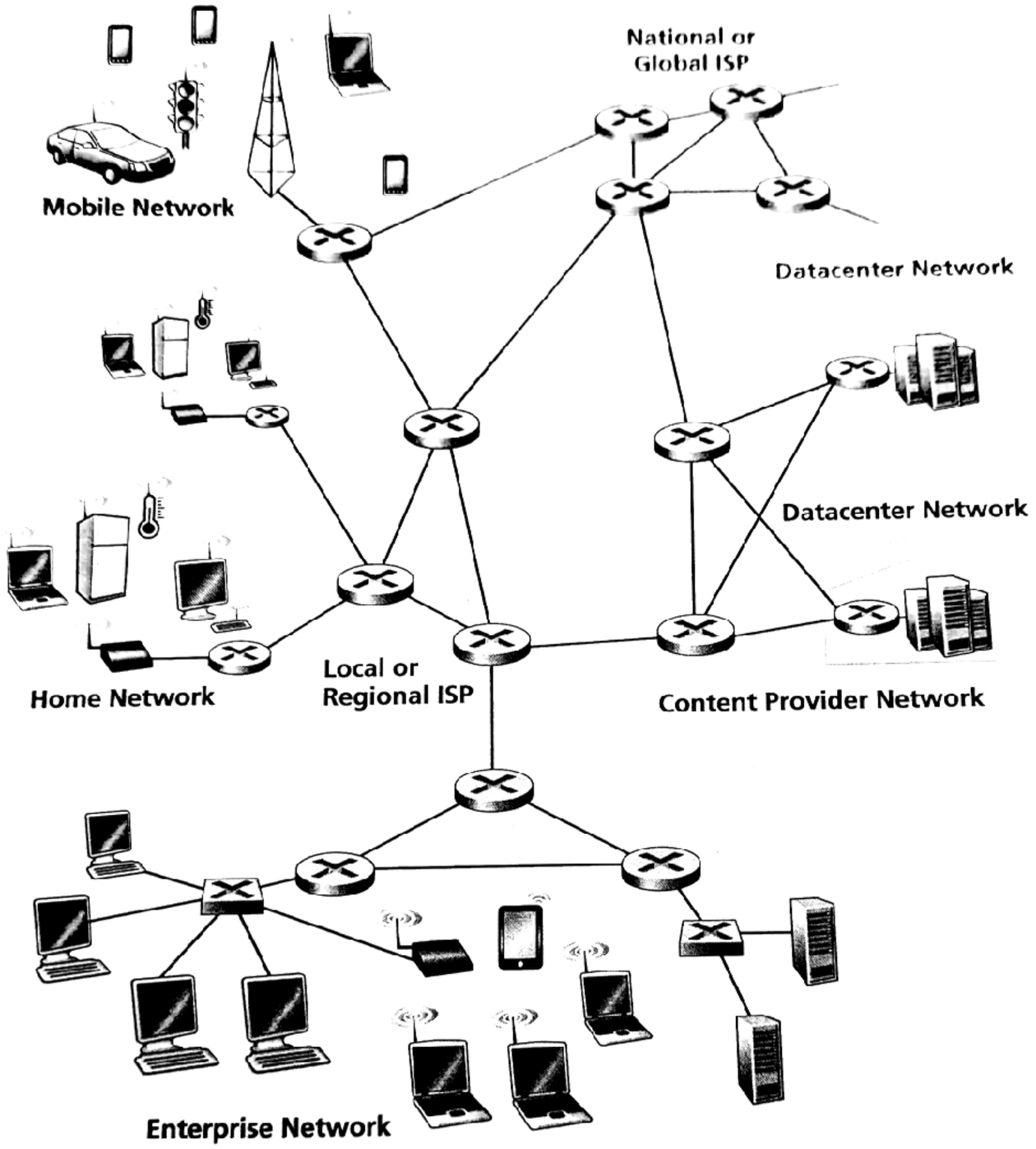


Packet switched network



- Packet switching - tidlig 1960-tallet
- ARPAnet 1969: 4 nodes, 1972: 15 nodes
- første epost: 1972
- Mange uavhengige nettverksløsninger i 1970-tallet
  krever felles utvekslingsprotokoll
- TCP / UDP / IP på plass i slutten av 1970-tallet
- Felles bytte til TCP/IP : 1983-01-01
- Slutten av 1980-tallet: 100000 nodes, f.eks NSFNET kobling blant US-universiteter
- 1991: kommersiell bruk av NSFNET tillat
- 1989-1991: utvikling av WWW (HTML/HTTP/server/browser) hos CERN
- fra 1995: tilgang til WWW er standard for studenter
- 1995 - 2001: økonomisk boble

Internet er et nettverk av nettverk



Kurose/Ross,
"Computer Networking,
a top-down approach",
Pearson 2022

5-layer model

- Application: **HTTP**, SMTP, FTP, SSH, DNS
  lett å lage nye protokoller her
  end system <-> end system
- Transport
- Network
- Link
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: **TCP** (connection) eller **UDP** (connectionless)
  sender "segments" fra end system <-> end system
- Network
- Link
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: **IP** (ingen andre valg på Internet)
  sender "datagrams / packets"
  mellom end systems fra en router til den neste
- Link
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: IP
- Link: Ethernet, WiFi, PPP
  sender "frames" fra en enhet til den neste
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: IP
- Link: Ethernet, WiFi, PPP
- Physical: elektriske signaler, radiosignaler, ...
  sende bits fra en enhet til den neste

OSI modell - 7 layers

OSI model

Layer			Protocol data unit (PDU)	Function[27]
Host layers	7	Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP.
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/ decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet, Datagram[28]	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

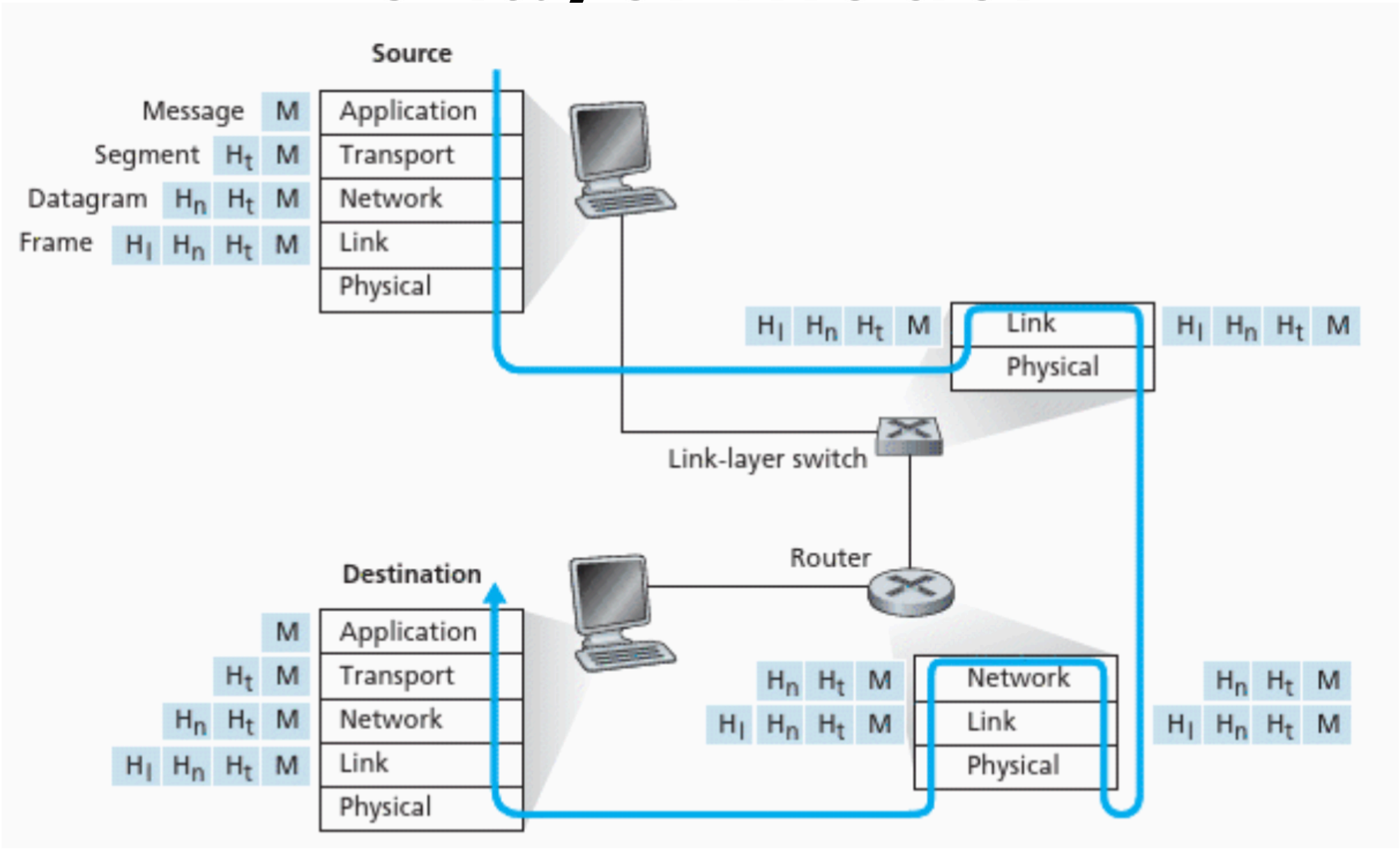
Application

https://en.wikipedia.org/wiki/OSI_model

5-layer model

- Application: innhold, filnavn, domenenavn, ...
- Transport: TCP/UDP-ports
- Network: IP-adresse
- Link: MAC-adresse
- Physical

5-layer model



se på packets

- curl / nc demo

Vi starter top-down med HTTP