

Sammanfattning av kursen

Maria Kihl



LUND
UNIVERSITY

Internet för er (innan kursen)

facebook

Spotify

Google™



STAR CRAFT



ANDROID

iTunes



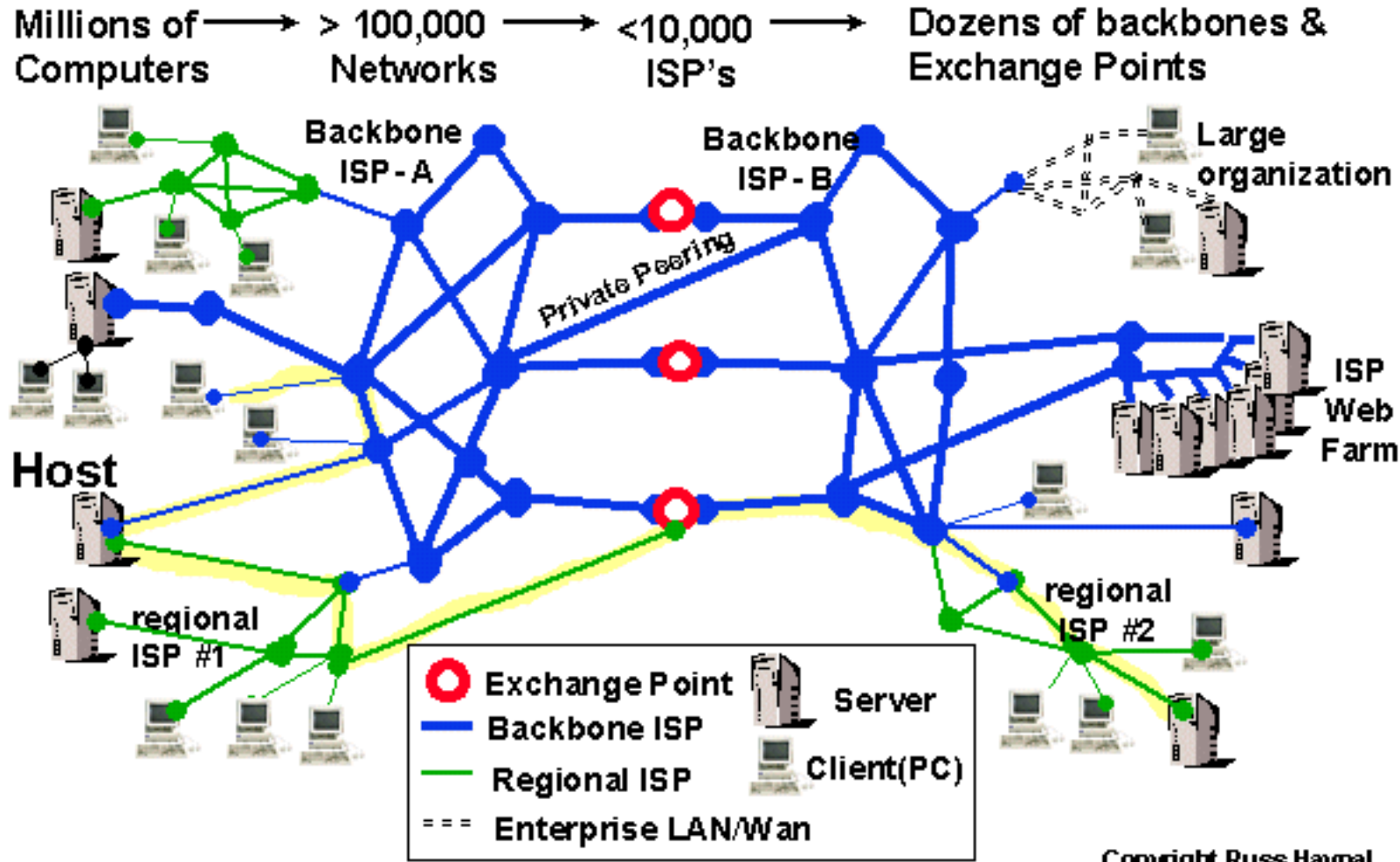
You Tube



amazon.com



Internet för er nu (?)

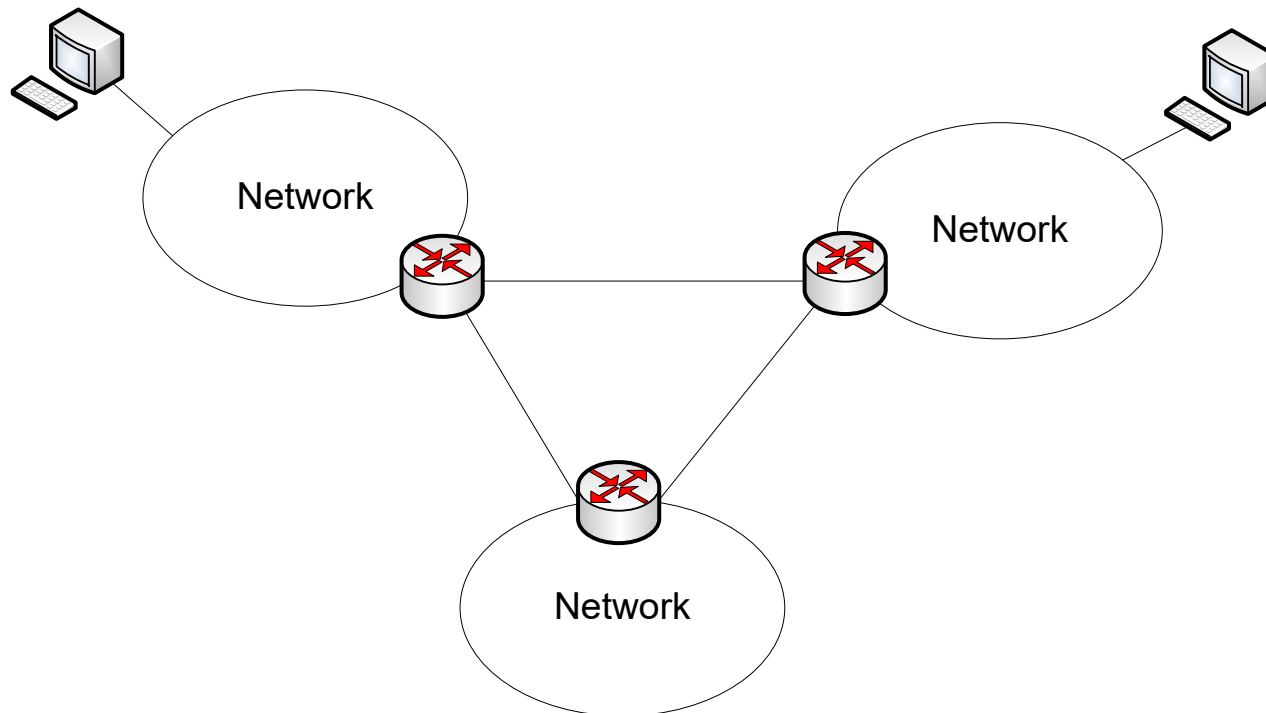


Information Flows over MANY Paths

Copyright Russ Haynal
<http://navigators.com>

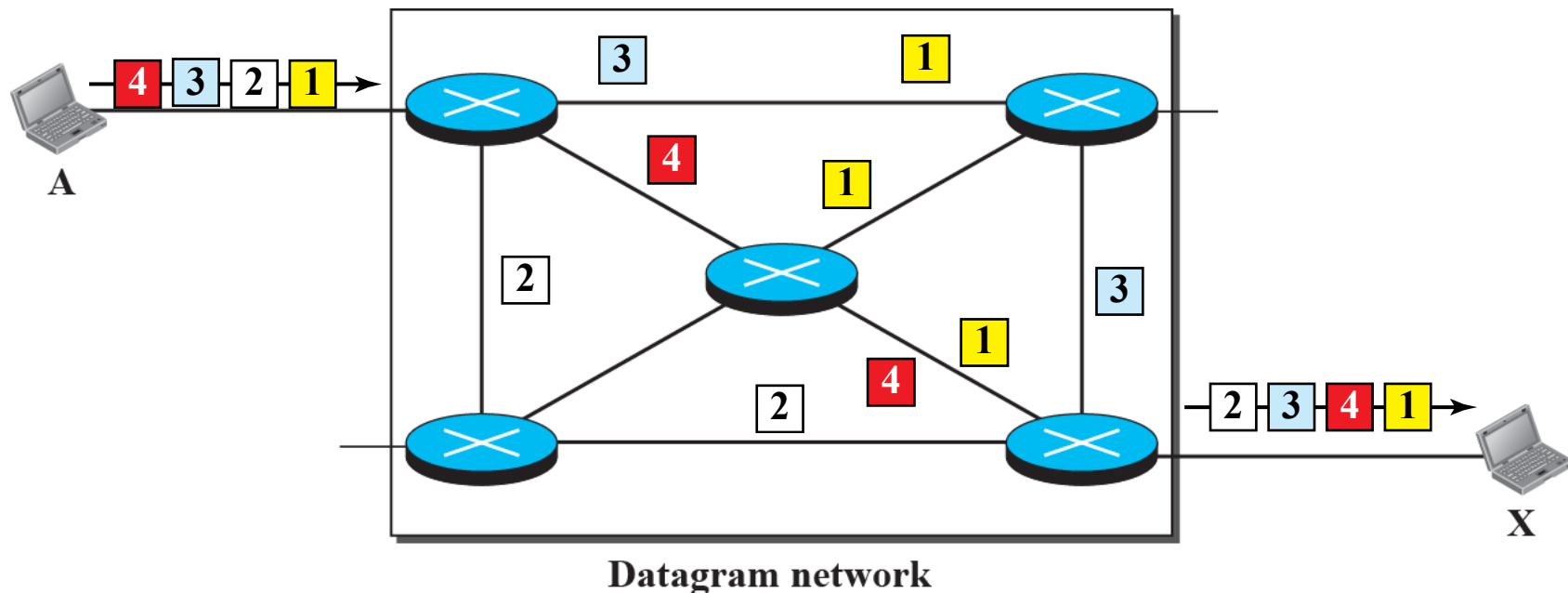
Internetworking

De protokoll och funktioner som behövs för att skicka data över olika nät.

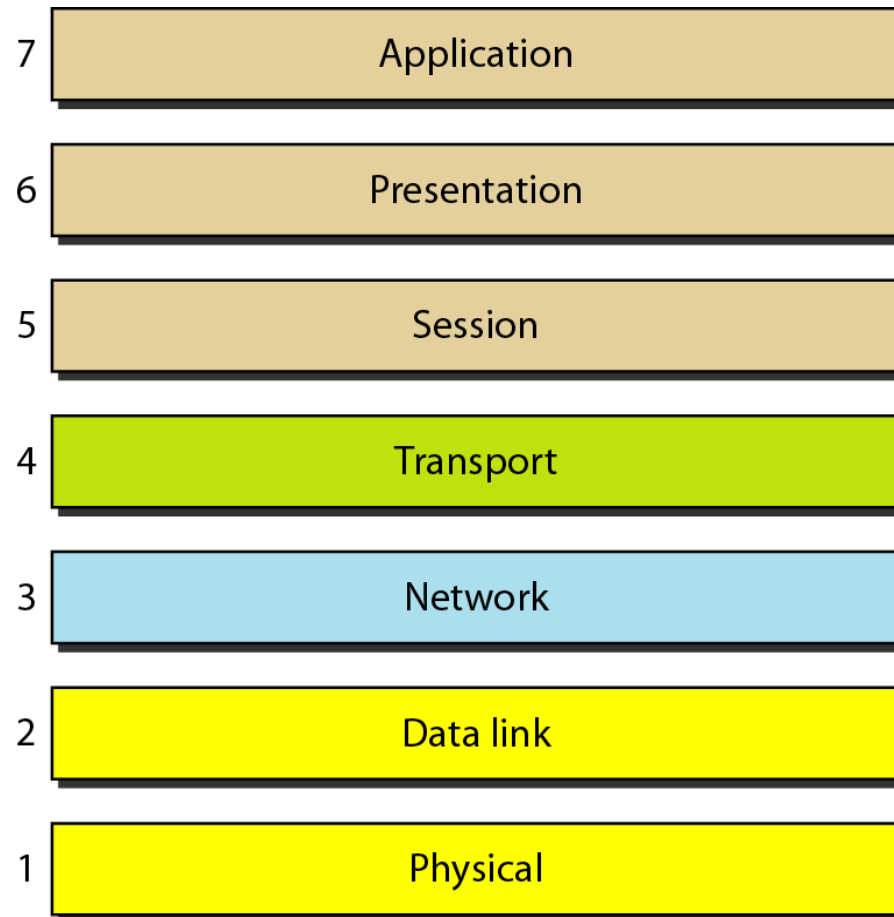


Paketförmedlande nät

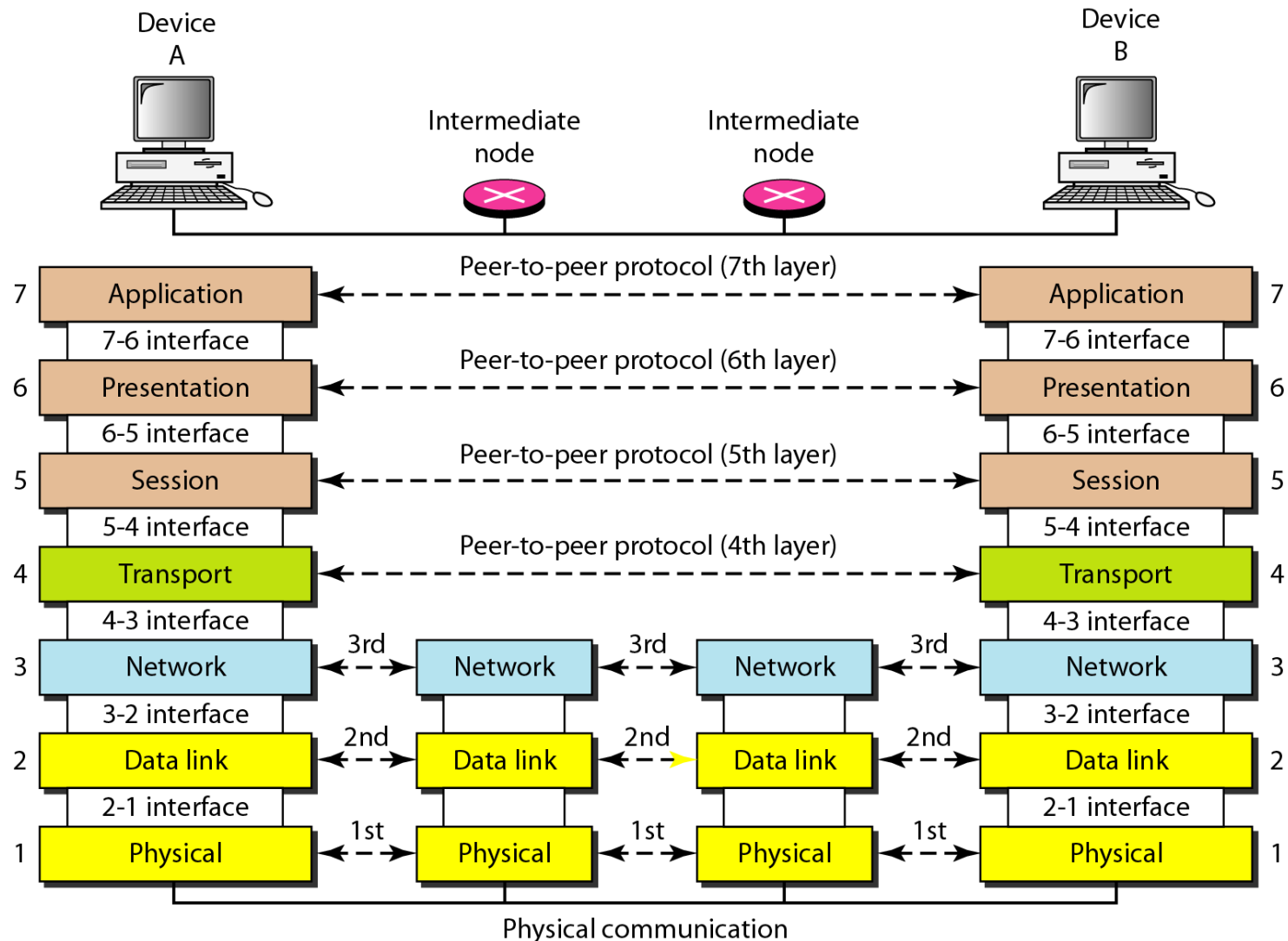
Denna kurs handlar till största delen om paketförmedlande nät där varje paket behandlas oberoende av varandra.



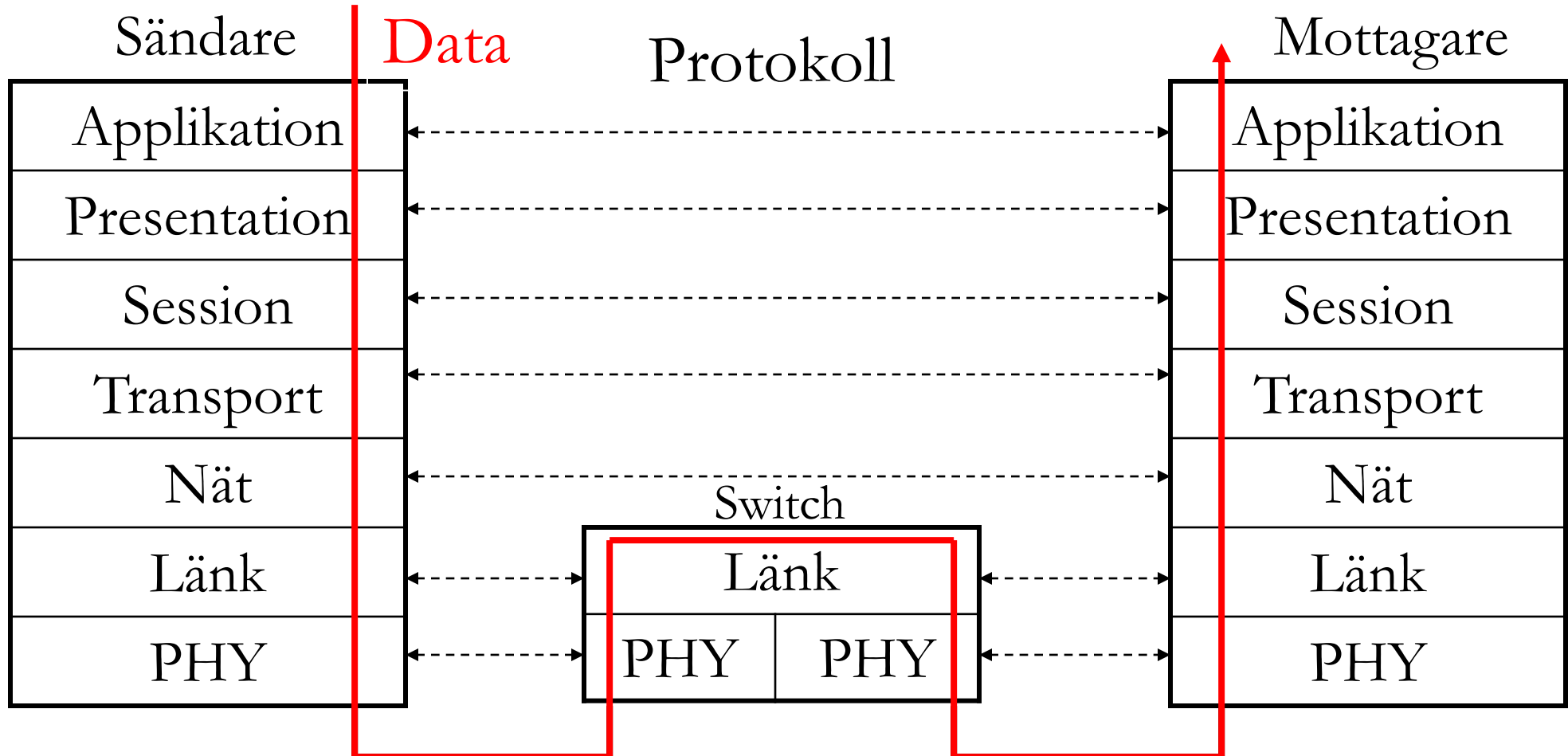
OSI-modellen



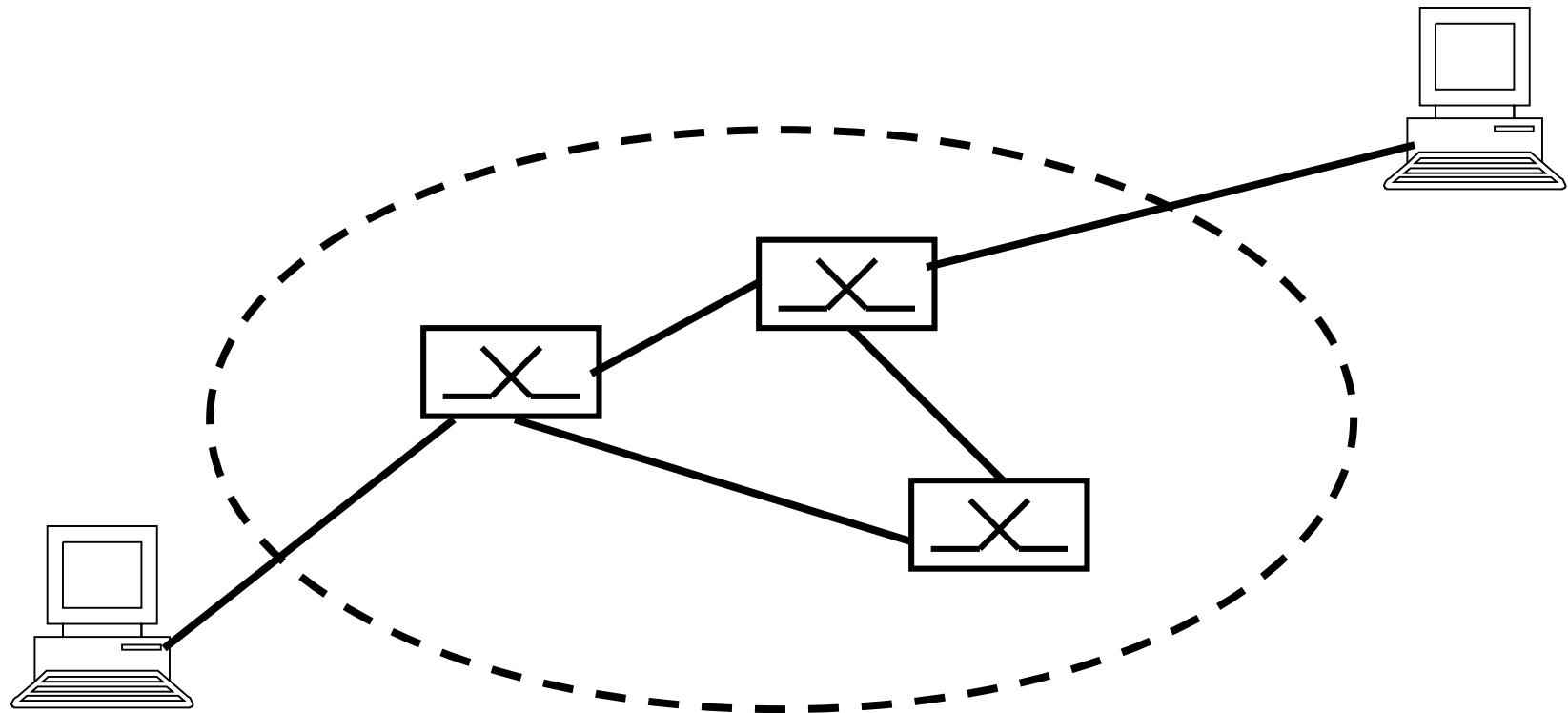
Protokollhantering i flera skikt



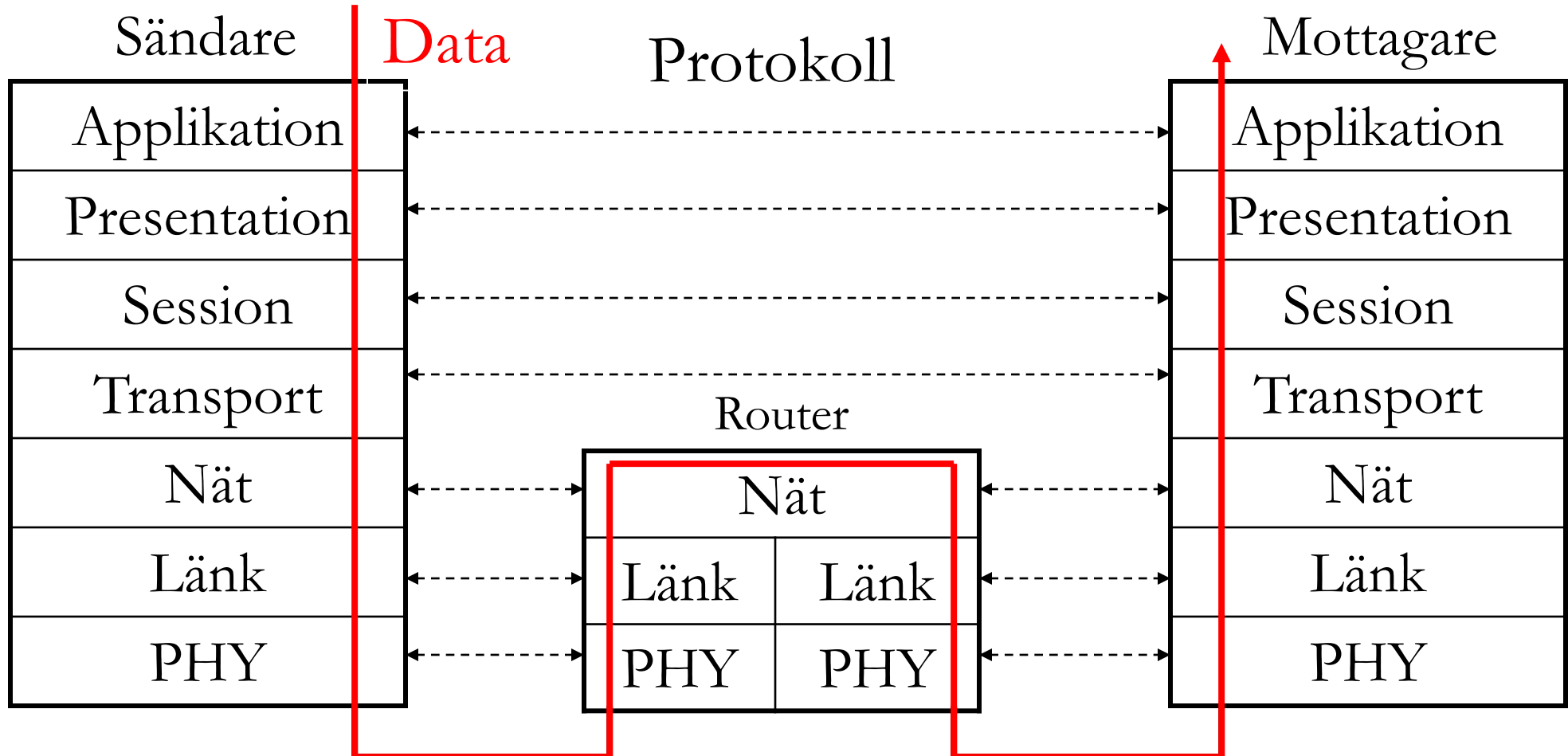
Vägväljare (1)



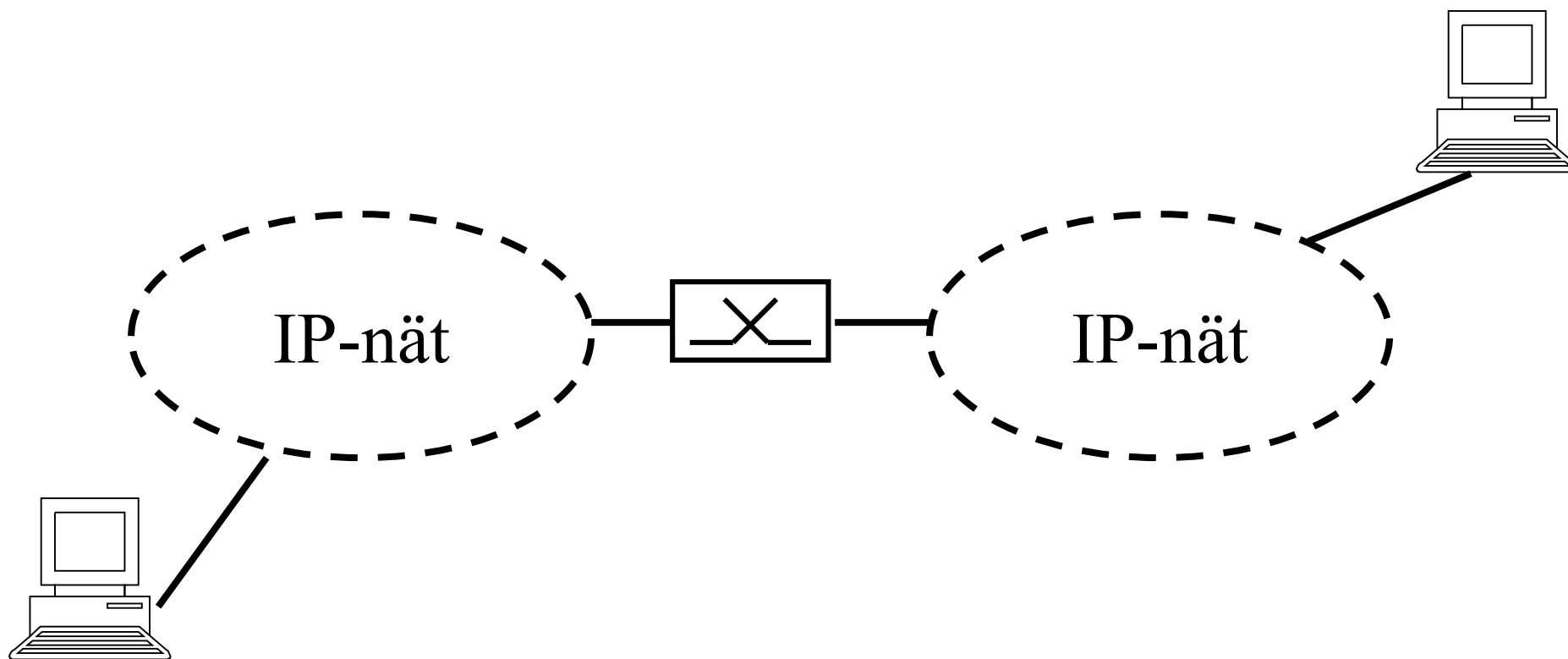
Switchar används inom nät



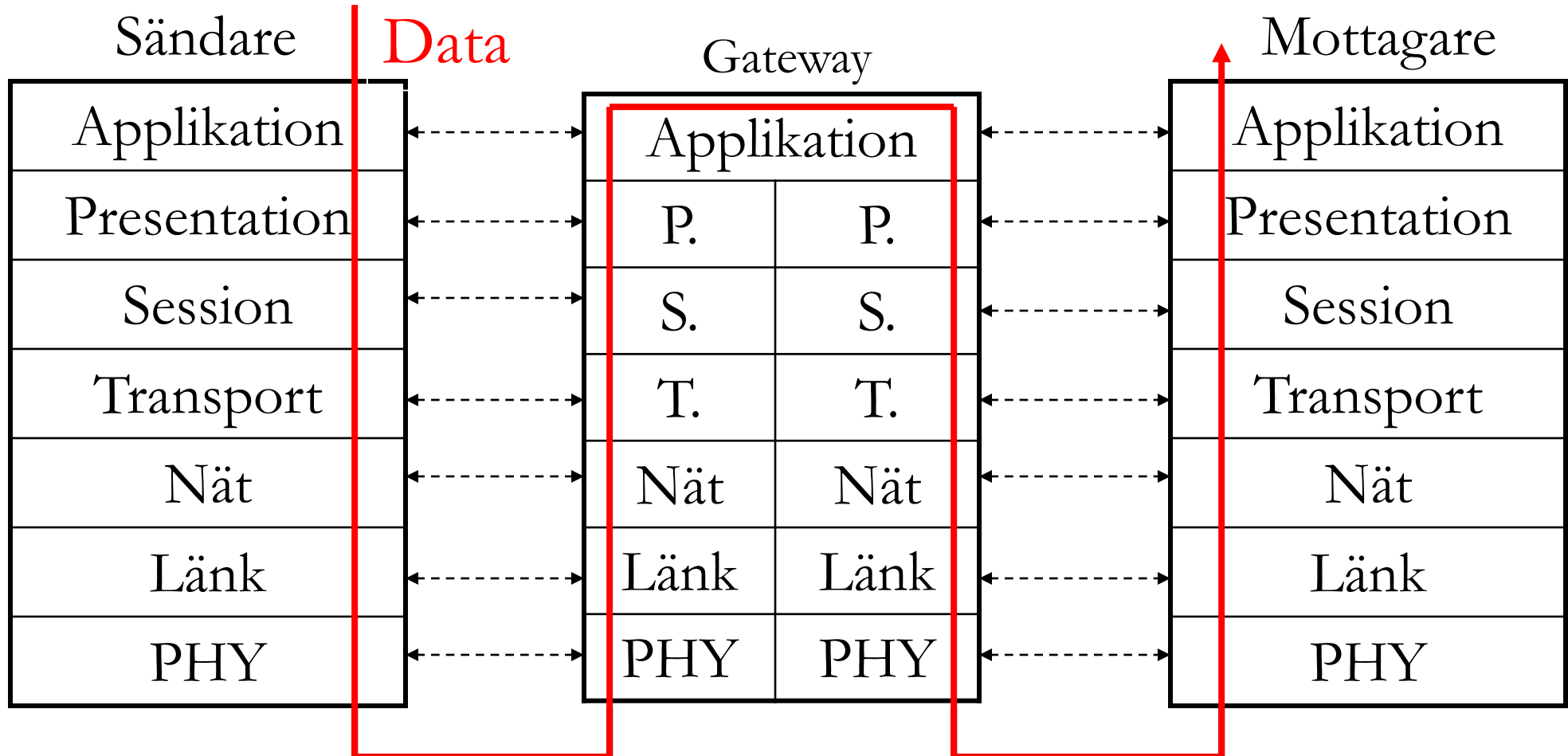
Vägväljare (2)



Routers används mellan olika nät med samma nätprotokoll

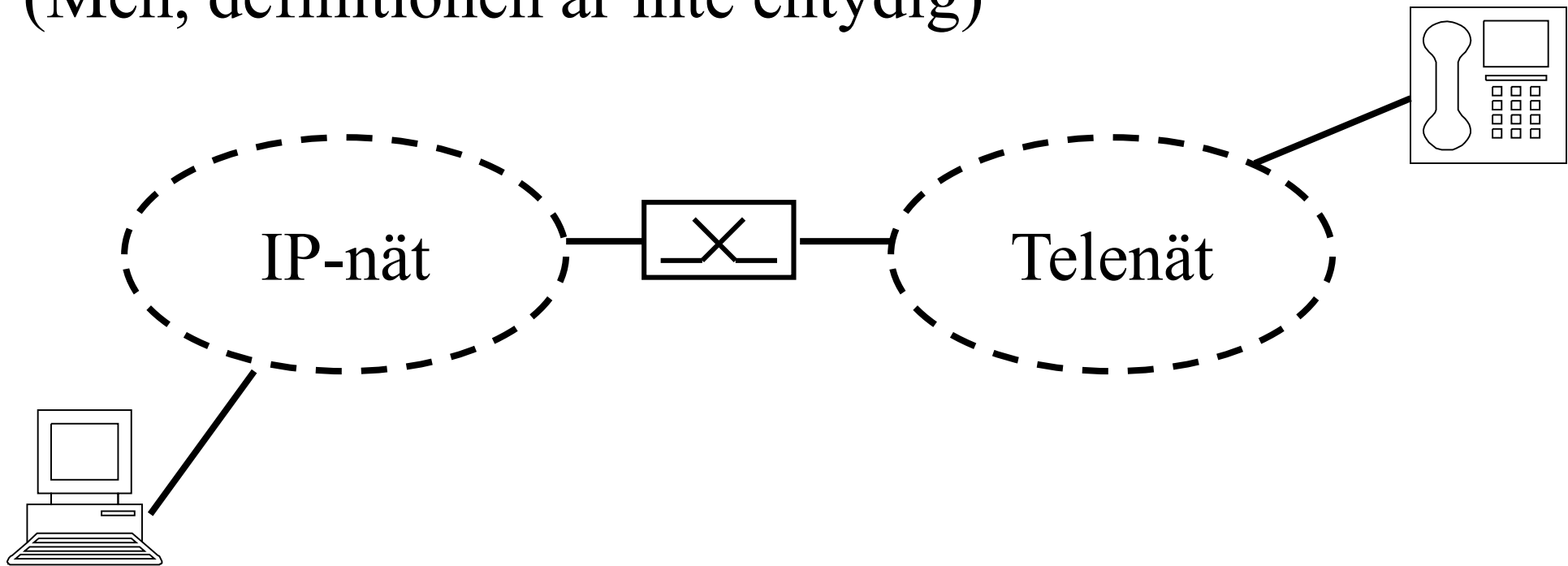


Vägväljare (3)



Gateways används mellan nät av olika typ

(Men, definitionen är inte entydig)



Datasäkerhet



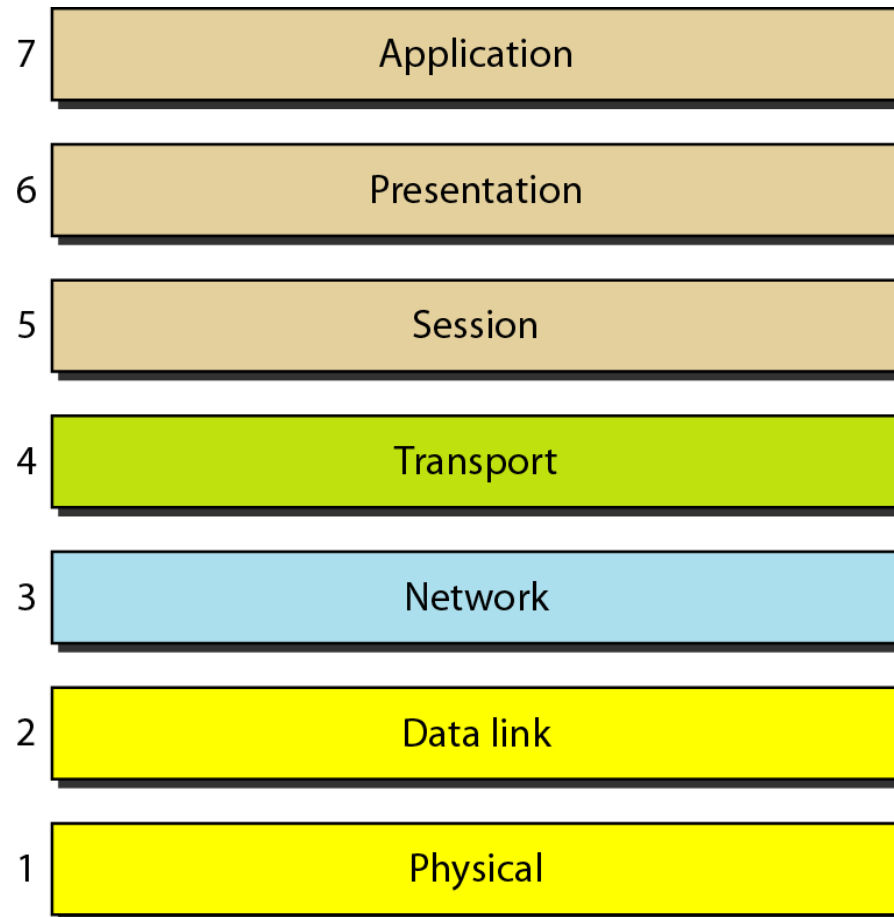
Datasäkerhet handlar om hur man säkerställer att sändare och mottagare vet vem det är de pratar med, samt hur man säkerställer att meddelandet inte kan läsas eller ändras av någon på vägen.

Datasäkerhet

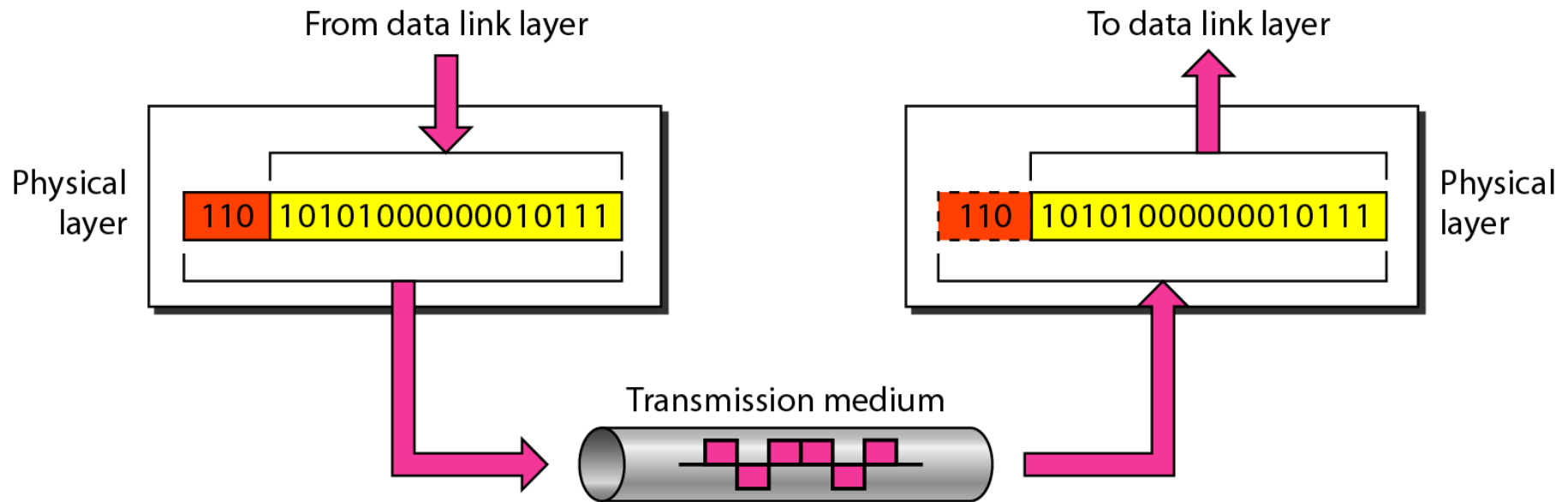
Det finns tre viktiga koncept vad det gäller datasäkerhet:

1. Skydd mot avlyssning (Privacy)
 - Kryptering
2. Skydd mot ändrad data (Integrity)
 - Message Digest
3. Autentisering (Authentication)
 - Challenge-response (enheter)
 - Digital signatur (meddelanden)

OSI-modellen



1. Fysiska skiktet (Physical layer)



Det fysiska skiktet är ansvarigt för att skicka bitar mellan två noder som är kopplade via en fysisk länk.

Data och signaler

Data = Informationen vi vill överföra.

Signal = Så som data är representerat när det skickas över en länk.



Bandbredd

- Analog definition: Frekvensbandet på kanalen (mäts i Hz).
- Digital definition: Antalet bitar per sekund som kanalen kan överföra (mäts i bps). Kallas också för *bit rate*.

Störningar

När en signal färdas över en länk kommer den att försämrats pga störningar (transmission impairments).

- Dämpning (attenuation): Energiförlust
- Distortion: Signalförändring
- Brus (noise): Signalen blir förstörd tex av termiskt brus eller överhörning (crosstalk).

$$\text{Signal-to-noise ratio (SNR)} = \frac{\text{Average signal power}}{\text{Average noise power}}$$

Prestanda

- **Throughput**: “Verkliga” transmissionskapaciteten mellan en sändare och mottagare (bitar/sekund).
- **Fördröjning (Latency)**: Tiden det tar att skicka ett meddelande mellan sändare och mottagare. Summa av *utbredningstid*, *transmissionstid*, *kötid* och *betjäningstid*.

Att skicka data över en länk

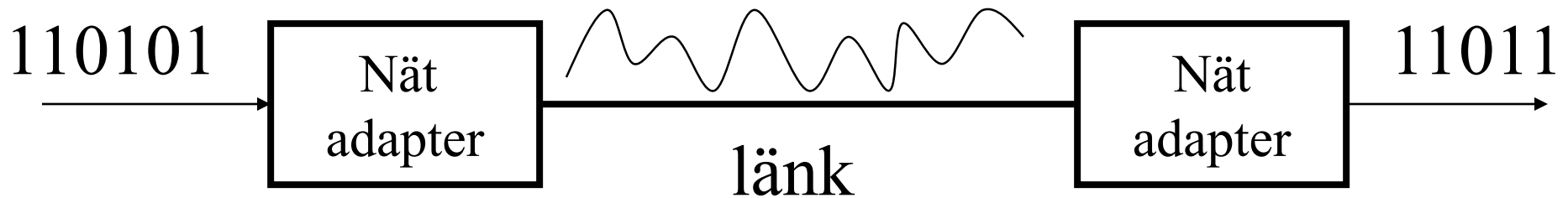


Bitströmmen måste representeras av signaler när den ska skickas över en länk.

Sändare och mottagare måste använda samma regler!

➔ Protokoll för Fysiska skiktet (Physical layer protocol).

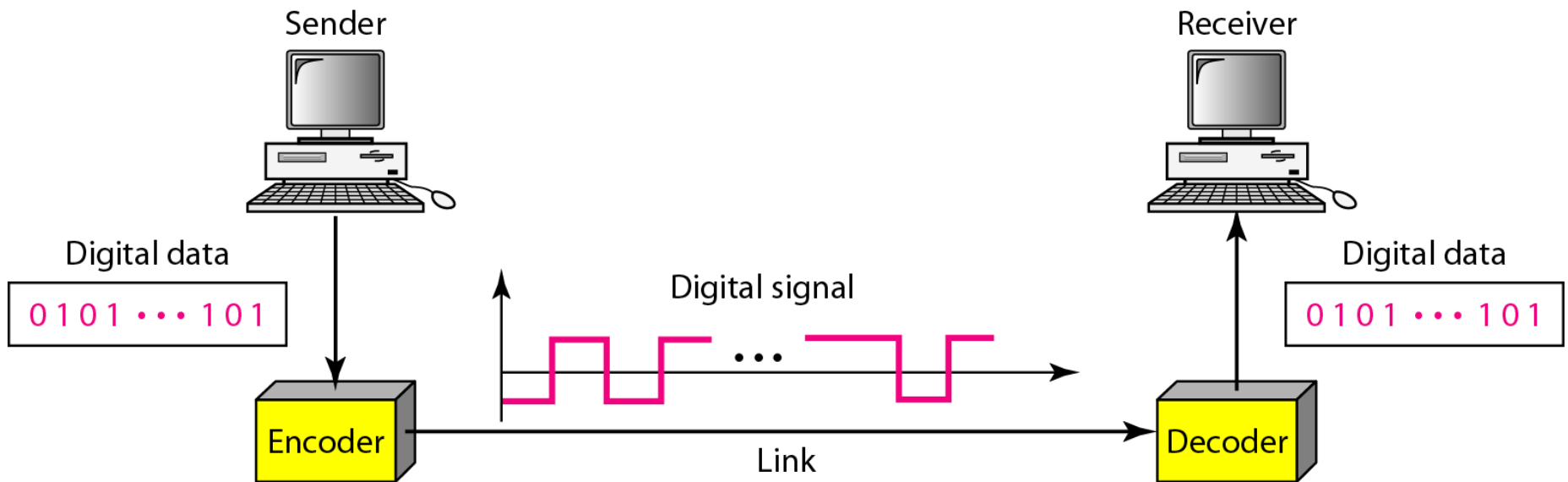
Digital kommunikation



- Digital transmission: Bitarna är representerade av digitala signaler (olika spänningsnivåer).
- Analog transmission: Bitarna är representerade av analoga signaler (modulerade sinusvågor).

Digital transmission

Linjekodning kallas processen att konvertera digital data till digitala signaler. Bitarna representeras av olika spänningsnivåer.

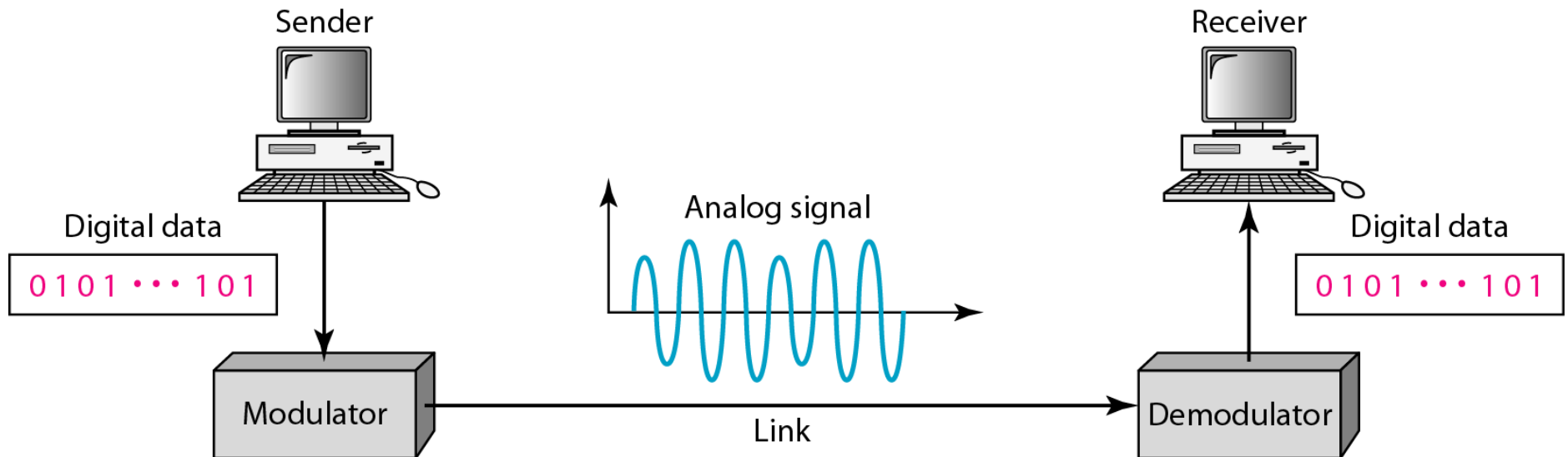


Tre metoder för linjekodning

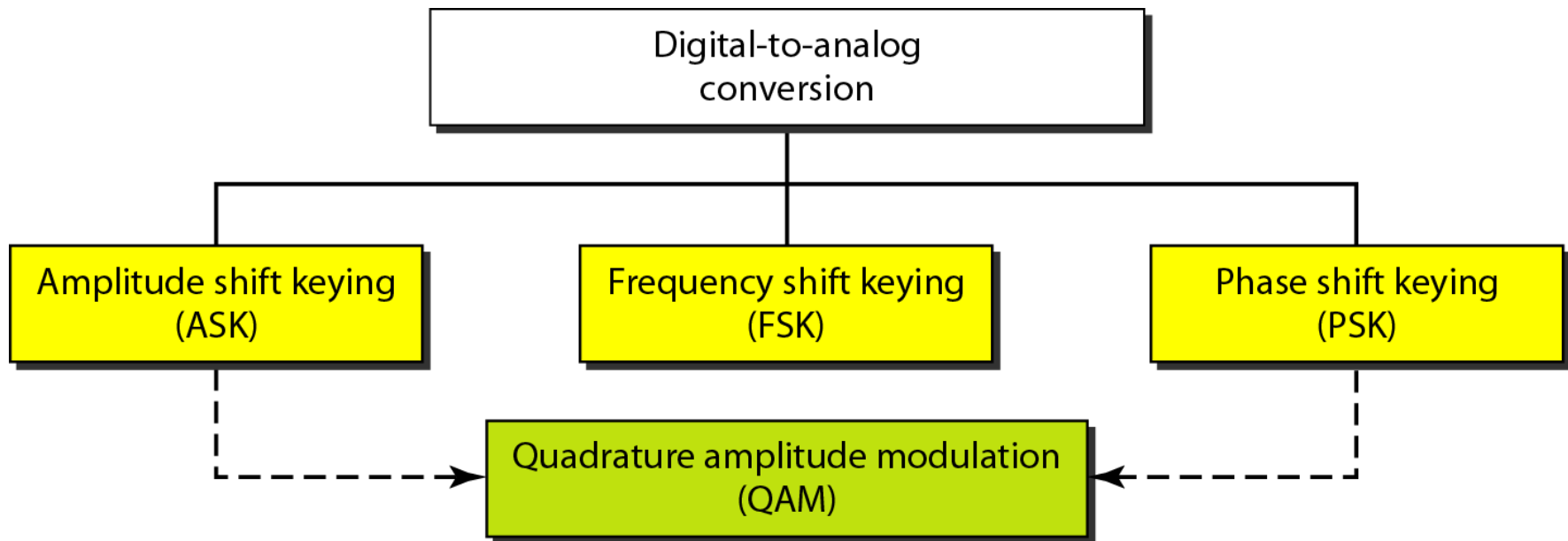
- Non-Return-to-Zero Level (NRZ-L)
- Manchester
- Differential Manchester

Analog transmission

Analog transmission använder **modulering**. Digital data representeras av sinusvågor med en viss **bärfrekvens**.

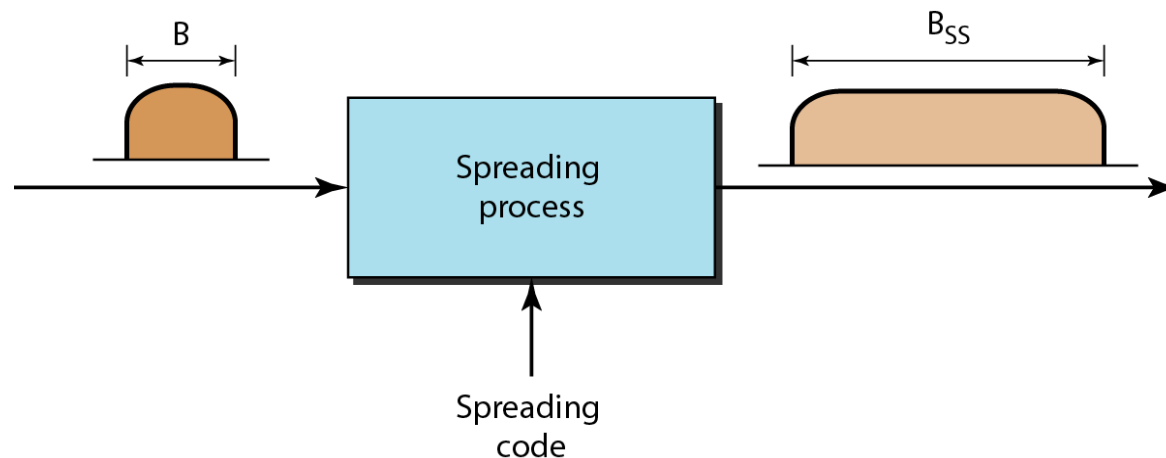


Metoder för Modulering



Spread Spectrum

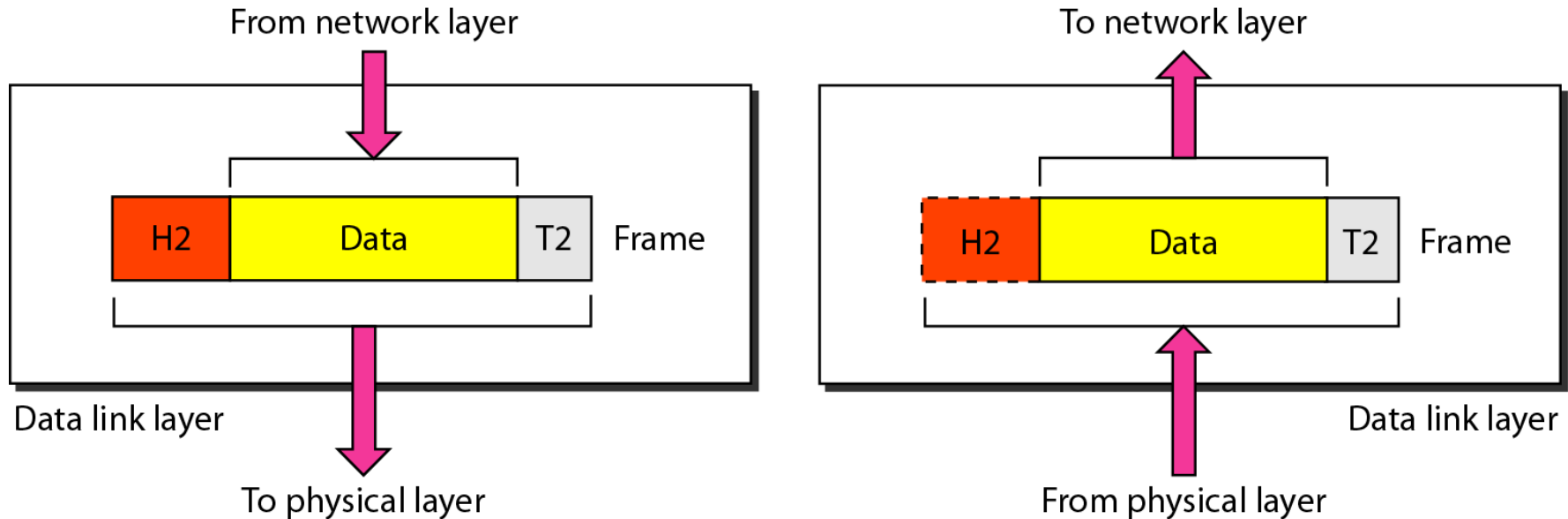
Spread Spectrum (SS), är en teknik för trådlösa länkar med mycket störningar och används bland annat i mobilnät, Bluetooth och vissa versioner av IEEE 802.11.



Spread Spectrum metoder

- Frequency Hopping Spread Spectrum (FHSS)
 - En källa använder många bärfrekvenser. En bärfrekvens används i taget, men bärfrekvensen ändras ofta (tex. 1000 gånger per sekund).
- Direct Sequence Spread Spectrum (DSSS)
 - Varje databit är kodad med n bits (kallade chips) med en unik spridningskod som är förutbestämd av sändare och mottagare.

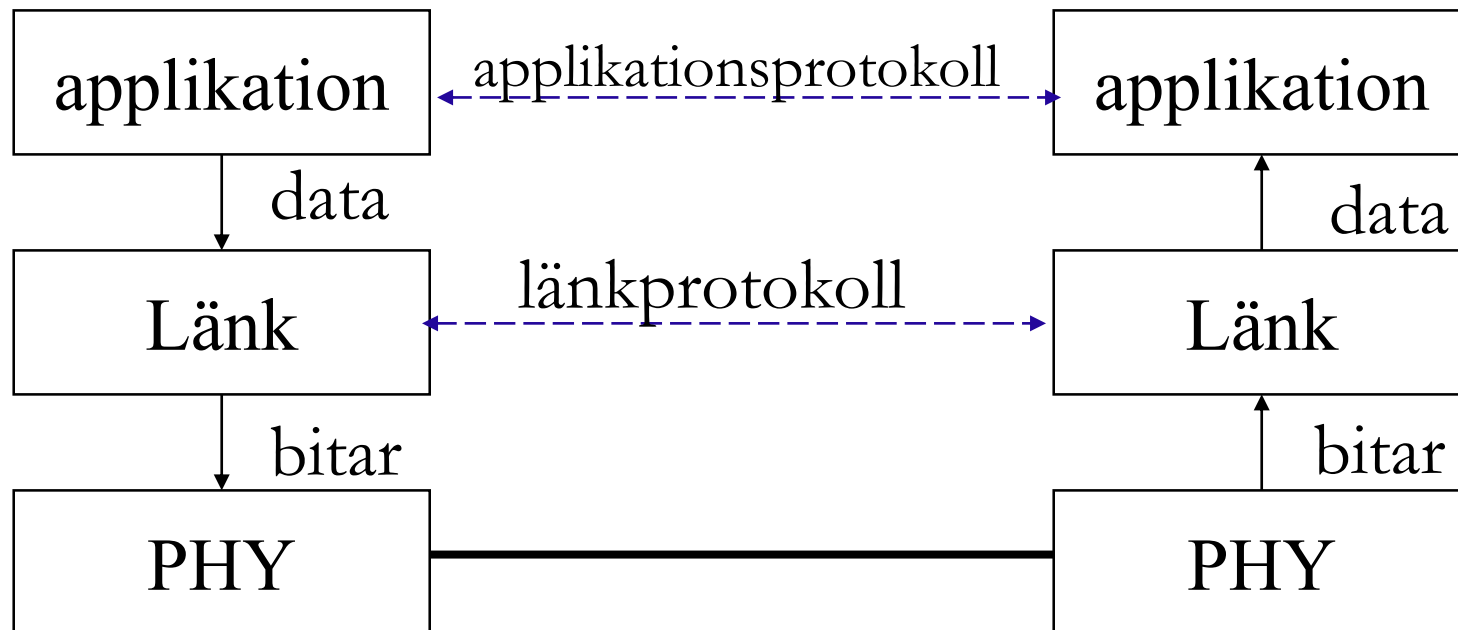
2. Länkskiktet



Länkskiktet är ansvarigt för att överföra ramar från en nod till nästa nod över en länk.

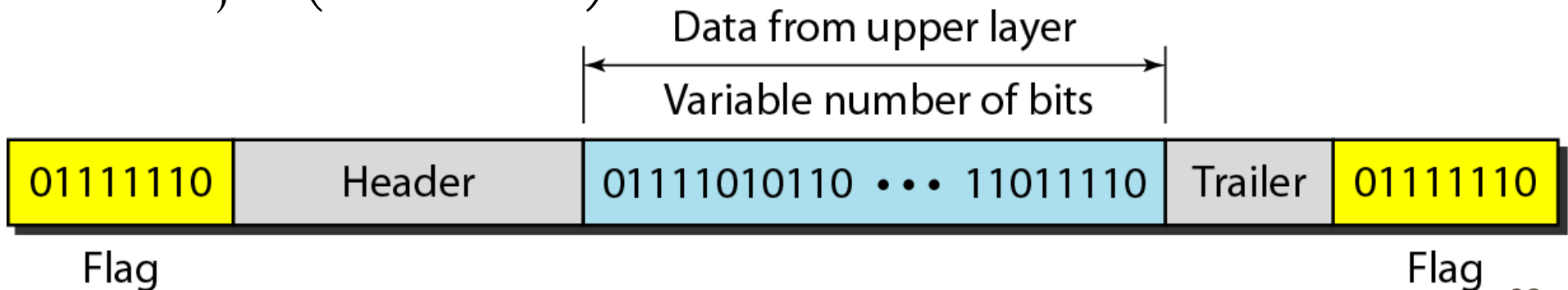
Länkprotokoll

Länkprotokollet tillhandahåller funktioner för att hantera en länkförbindelse, samt feldetektering, felhantering, och flödeskontroll för data som skickas över denna förbindelse.



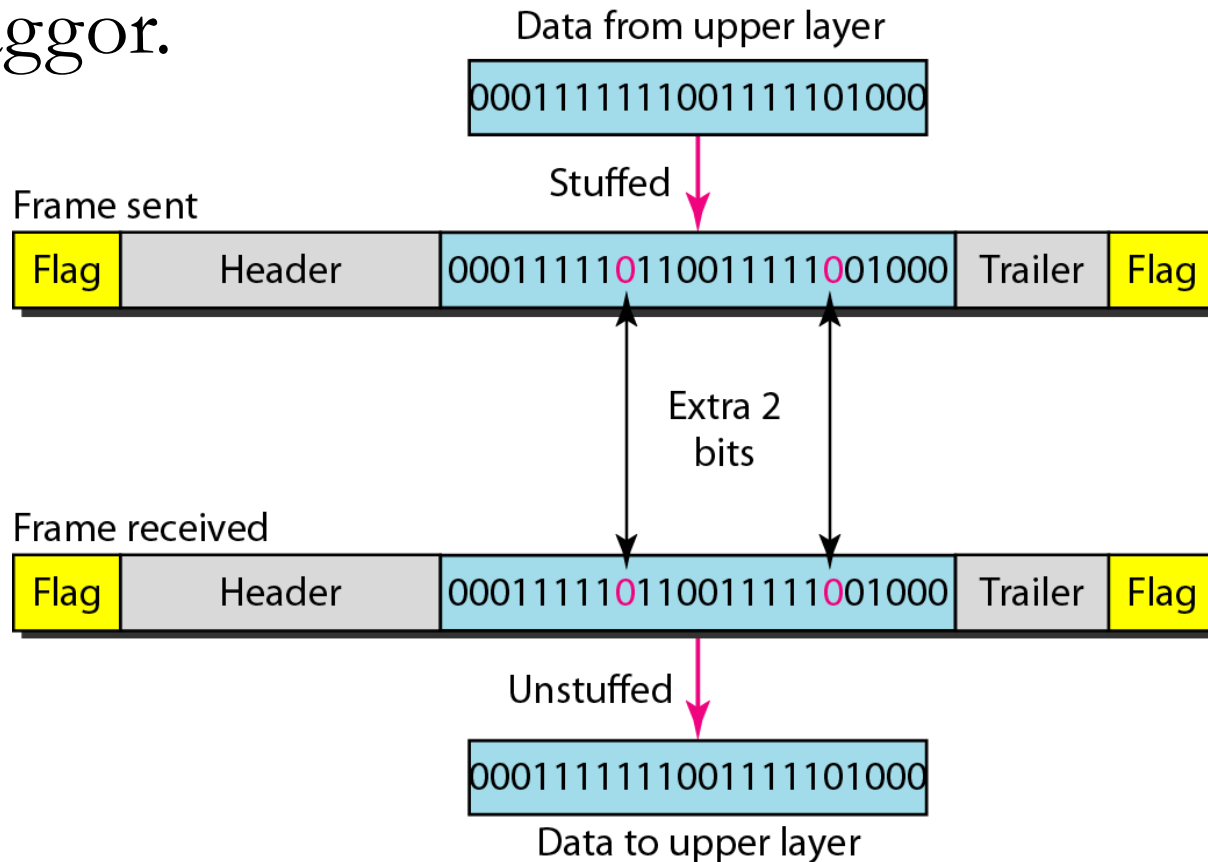
Framing

- Protokollet för det fysiska skiktet hanterar en bitström. Mottagarens länkprotokoll måste kunna identifiera ramar i denna bitström.
- Länkprotokollet paketerar data i ramar med hjälp av flaggor så att mottagaren kan veta var nästa ram börjar (och slutar).



Bitstuffing

Bitstuffing används så att data inte ska kunna förväxlas med flaggor.



Feldetektering

För att kunna detektera bitfel, adderas redundanta bitar till meddelandet på ett smart sätt.



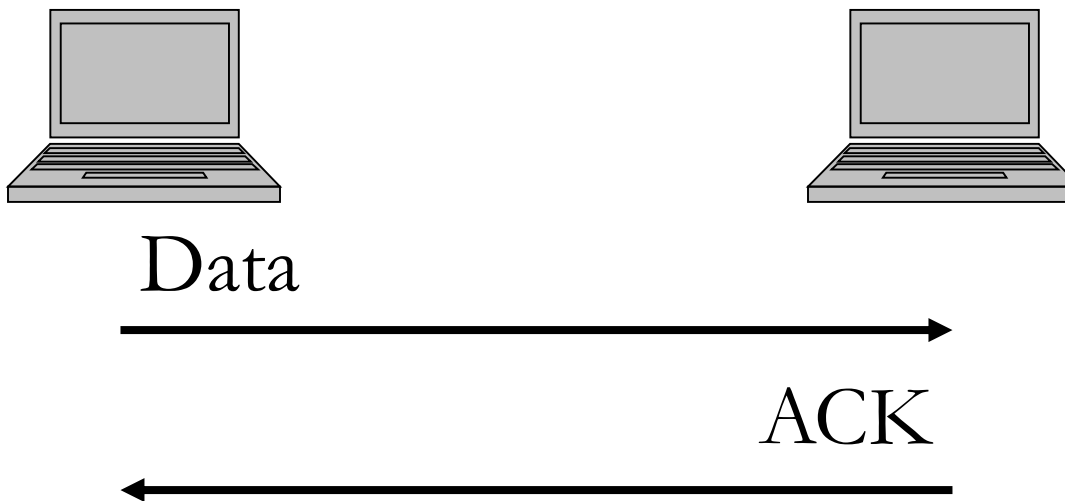
Värdet på extrabitarna beror på data.

Metoder för fel-detektering

- Paritetsbit (Simple Parity-Check Code)
- Cyclic Redundancy Check (CRC)
- Kontrollsumma (Checksum)

Felhantering

- Mottagaren skickar bekräftelse (ACK) för alla korrekt mottagna paket.
- Regler för omsändning när sändaren inte får förväntade ACK.



Metoder för Automatic Repeat Request (ARQ)

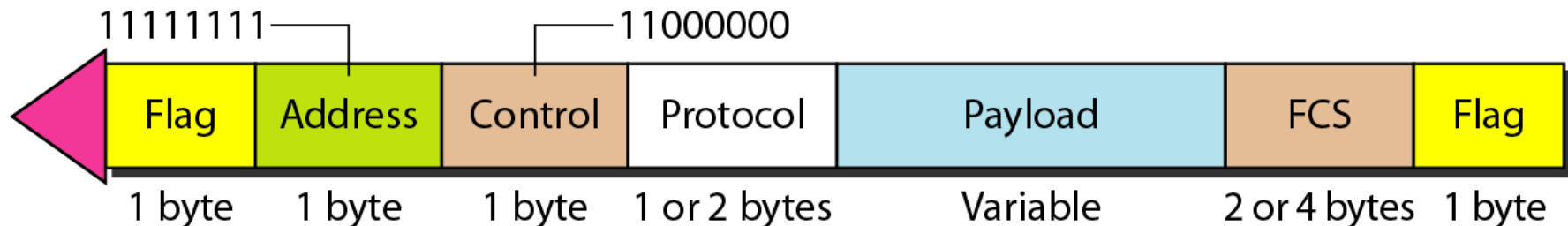
- Stop-and-wait ARQ
- Go-back-N ARQ
- Selective Repeat ARQ

Point-to-Point Protocol (PPP)

Point-to-point protocol (PPP) används som ett exempel på hur ett länkprotokoll kan fungera.

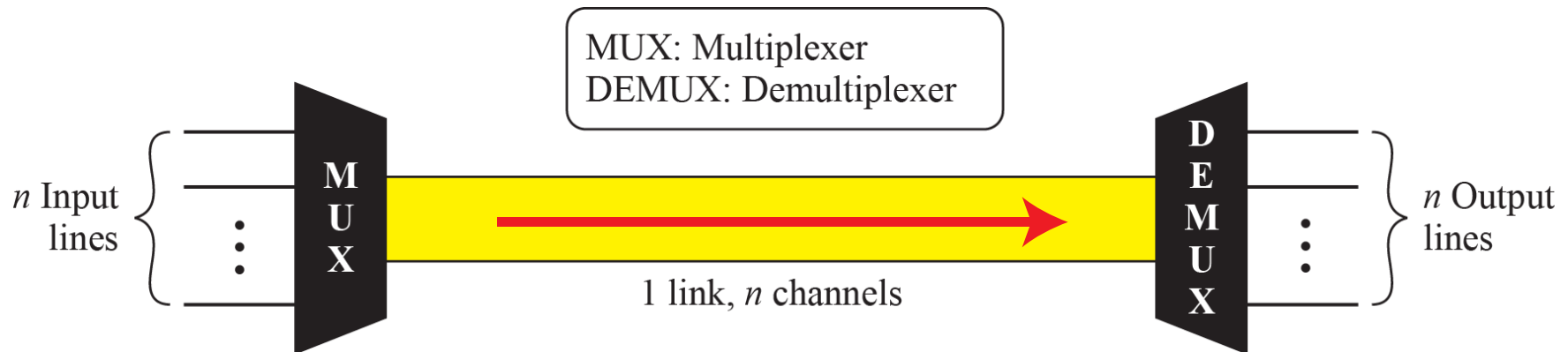
PPP är ett **byte-baserat** (character-oriented) protokoll, vilket innebär att all data i en ram hanteras i bytes (använder även **byte-stuffing**).

Ramformat:



Multiplexering

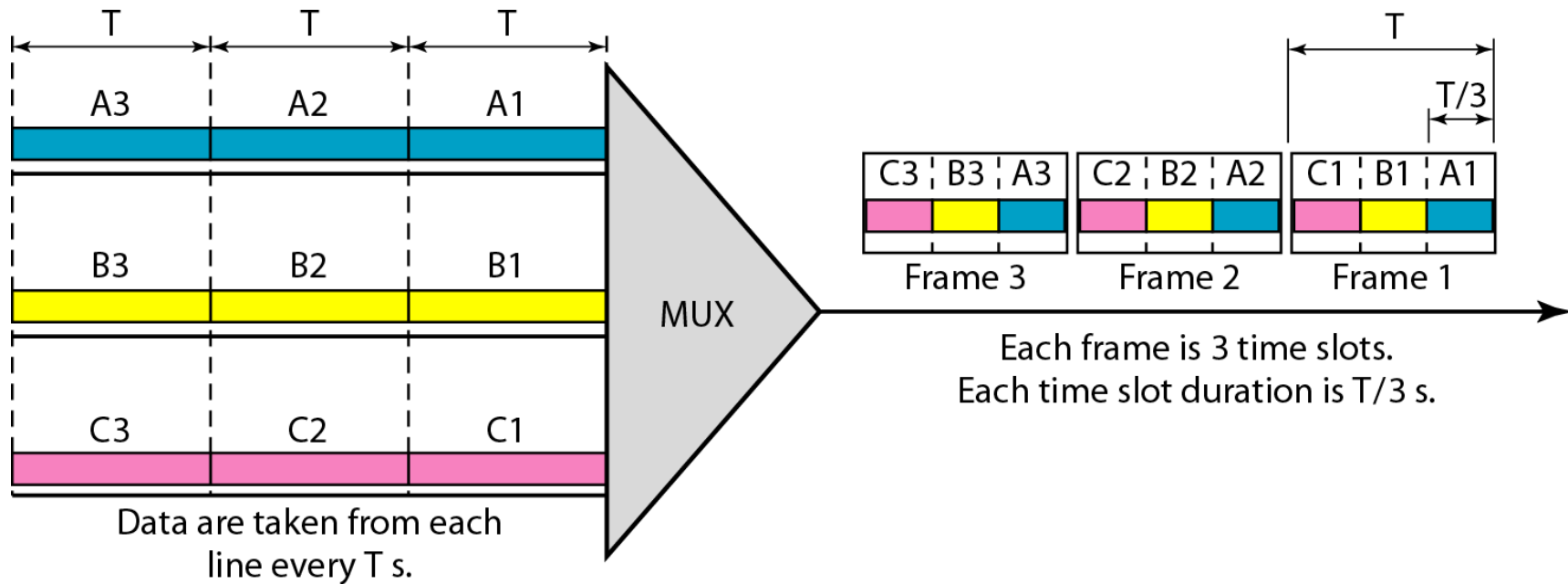
Fysiska länkar behöver delas av flera förbindelser. Detta kallas *multiplexering*. En fysisk länk delas upp i flera *kanaler*.



Metoder för multiplexering

- ⌘ Frekvensmultiplexering (Frequency-Division Multiplexing, FDM)
- ⌘ Tidsmultiplexering (Time-Division Multiplexing, TDM)
 - ⌘ Synkron tidsmultiplex (STDM)
 - ⌘ Statistisk multiplexering

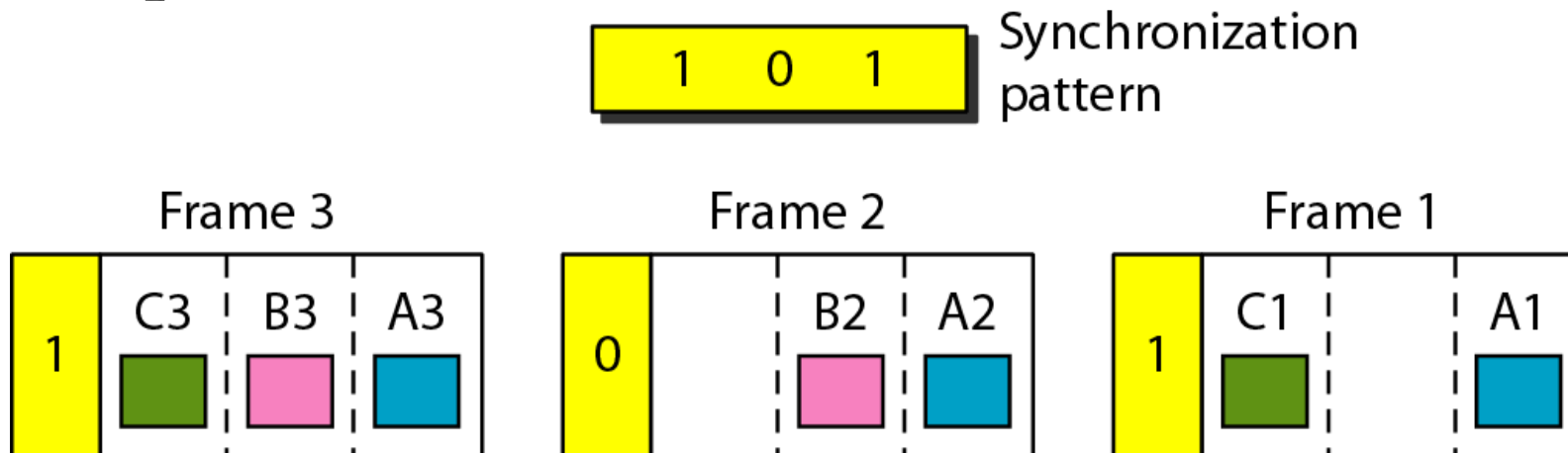
Synkron tidsmultiplex (STDM)



Om en kanal inte har något att skicka så kommer tidsluckan att vara tom!

Synkronisering av ramar i STDM

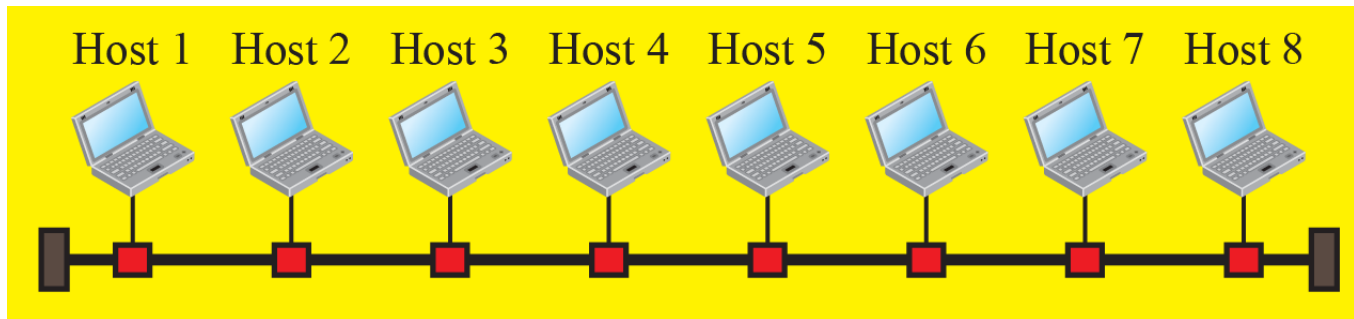
Om multiplexor och demultiplexor inte är synkroniserade i STDM, kan bitar hamna på fel kanal. Därför används synkroniseringsbitar (**framing bits**) i början av varje ram (jämför med flaggor i länkprotokoll).



Lokala nät

- Ett lokalt nät (Local Area Network, LAN) är ett datanät med en begränsad storlek.
- Kan i sin enklaste form bestå av endast *en* fysisk länk som flera datorer är kopplade till.
- Kan också bestå av flera fysiska länkar som är sammankopplade med så kallade bryggor.

Grundprincip för ett delat utbredningsmedium

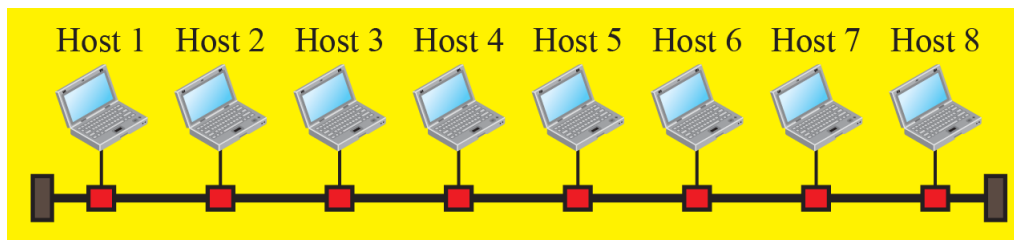


a. LAN with a common cable (past)

Idag delar vi oftast inte på ett trådat utbredningsmedium, utan istället trådlösa länkar. Men grundprincipen är fortfarande den samma (så i alla bilder med en trådad länk kan du tänka dig en trådlös länk istället)

Egenskaper för ett enlänks-LAN

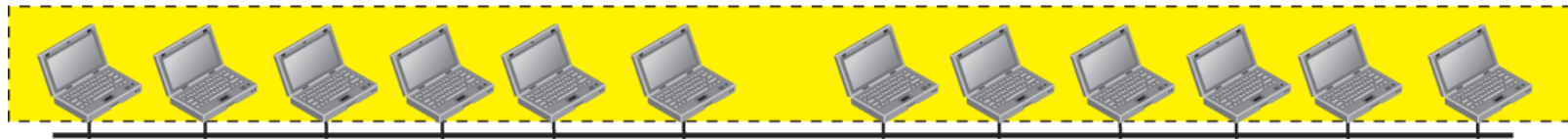
- All data som skickas på länken når alla terminaler (**broadcast**).
- På grund av dämpningen på länken så har nätet en begränsad geografisk storlek.
- Länken kan förlängas med en **repeaterare (repeater)** som förstärker signalen.
- Den del av länken där en kollision kan inträffa kallas för **kollisionsdomän**.



Kollisionsdomän

Alla hosts som delar samma länk tillhör samma *collision domain*. Detta medför begränsningar i hur många hosts som kan tillhöra samma länk.

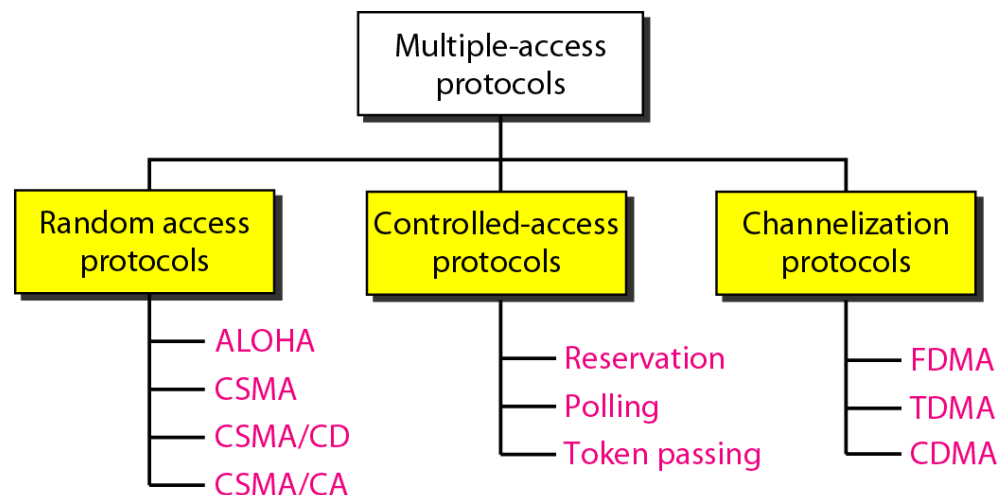
Domain



a. Without bridging

Medium Access Control (MAC) Protokoll

- Alla hosts som delar en länk måste ha samma regler för att skicka och ta emot data.
- Detta kallas för **Multiple-Access Protocol** eller **Medium access control (MAC) protocol**.



Metoder med “Controlled access”

I metoder med **controlled access**, kommer terminalerna överens om vem som ska skicka när. En terminal får inte skicka data om inte de andra har godkänt det.

Denna typ av accessmetoder används i olika delar av de mobila näten samt i andra typer av nät, tex i fordon och produktionssystem.

Exempel: *Reservation, Polling, Token ring, FDMA, TDMA*

Metoder med “Random access”

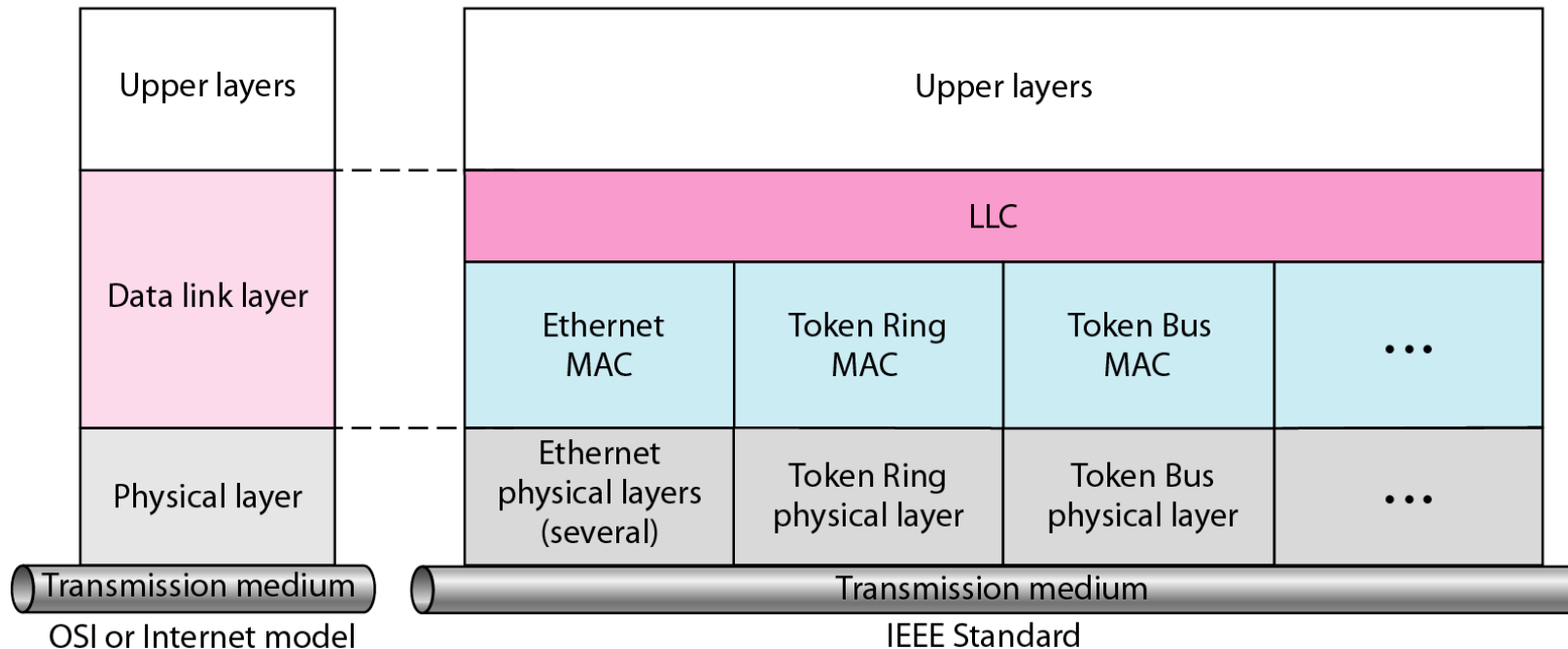
I metoder med **random access** eller **contention**, bestämmer ingen terminal över de andra. Alla terminaler sköter sig själva och tar egna beslut om när de ska skicka.

Varje terminal använder en förutbestämd procedur för att ta beslut om huruvida den ska sända data eller ej.

Exempel: Aloha, CSMA/CD, CSMA/CA

IEEE standardiseringsprojekt 802

LLC: Logical link control
MAC: Media access control



IEEEs projekt 802 startade 1985.

Fysisk adress (MAC-adress)

06 : 01 : 02 : 01 : 2C : 4B

└──┘
6 bytes = 12 hex digits = 48 bits

Alla terminaler med ett nätverkskort för IEEE 802.x fysisk adress, kallad MAC-adress. Har terminalen flera nätverkskort har den flera MAC-adresser.

Unicast och Broadcast-adresser

- Dataöverföringen sker normal i *unicast*, dvs det finns en sändare och en mottagare.
- En del ramar skickas i *broadcast*, vilket innebär att en sändare skickar till alla terminaler inom nätet.
- I 802-nät, är broadcast-adressen satt till bara 1:or (FF:FF:FF:FF:FF:FF).

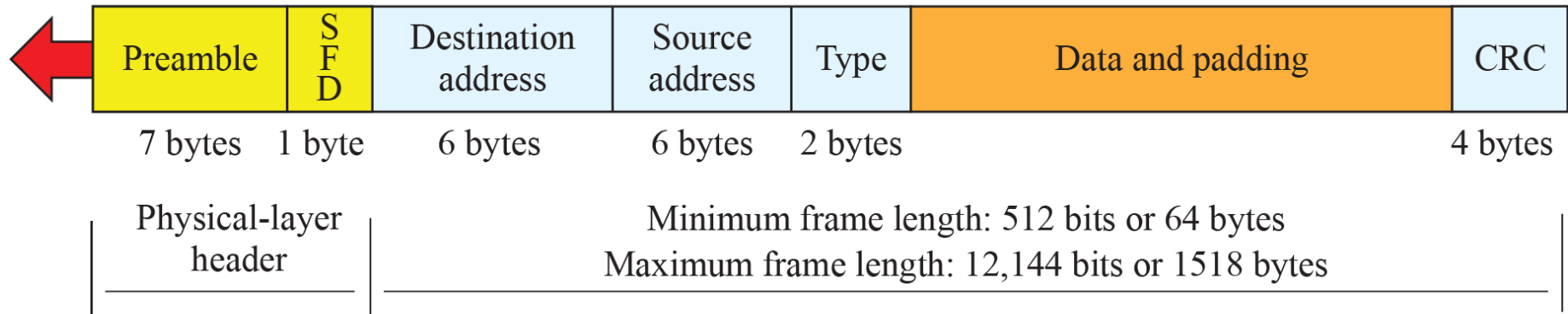
Ethernet

Ethernet är den dominerande (enda?) standarden för trådade LANs.

Preamble: 56 bits of alternating 1s and 0s

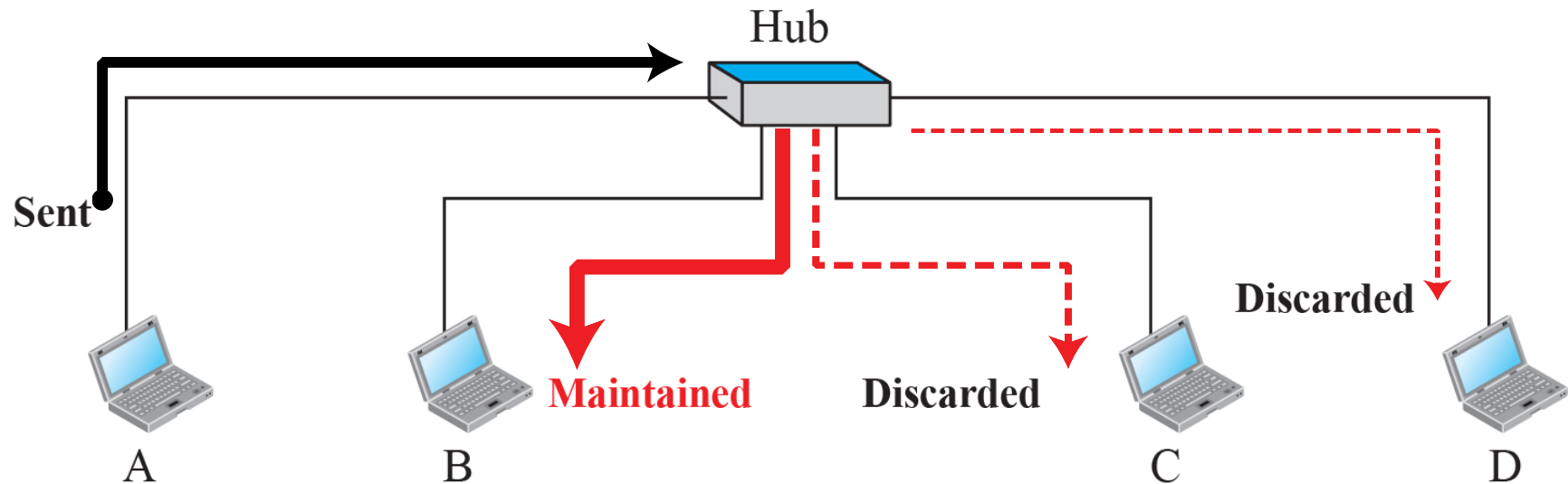
SFD: Start frame delimiter, flag (10101011)

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes



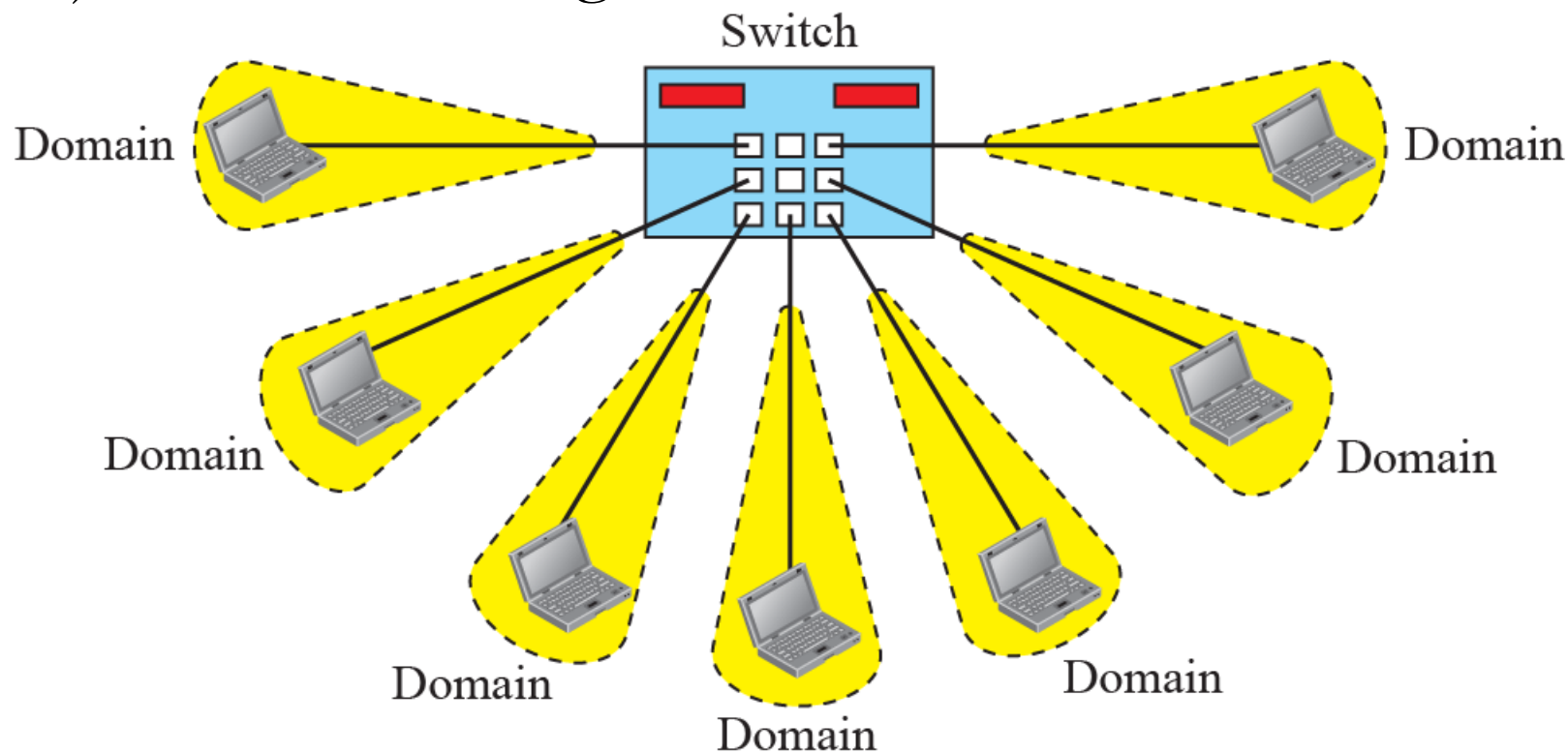
Hubs

Senare versioner av Ethernet använde hubs (nätnav). En hub skickar data från en inkommande länk till alla andra länkar. Den arbetar därför på det fysiska lagret.



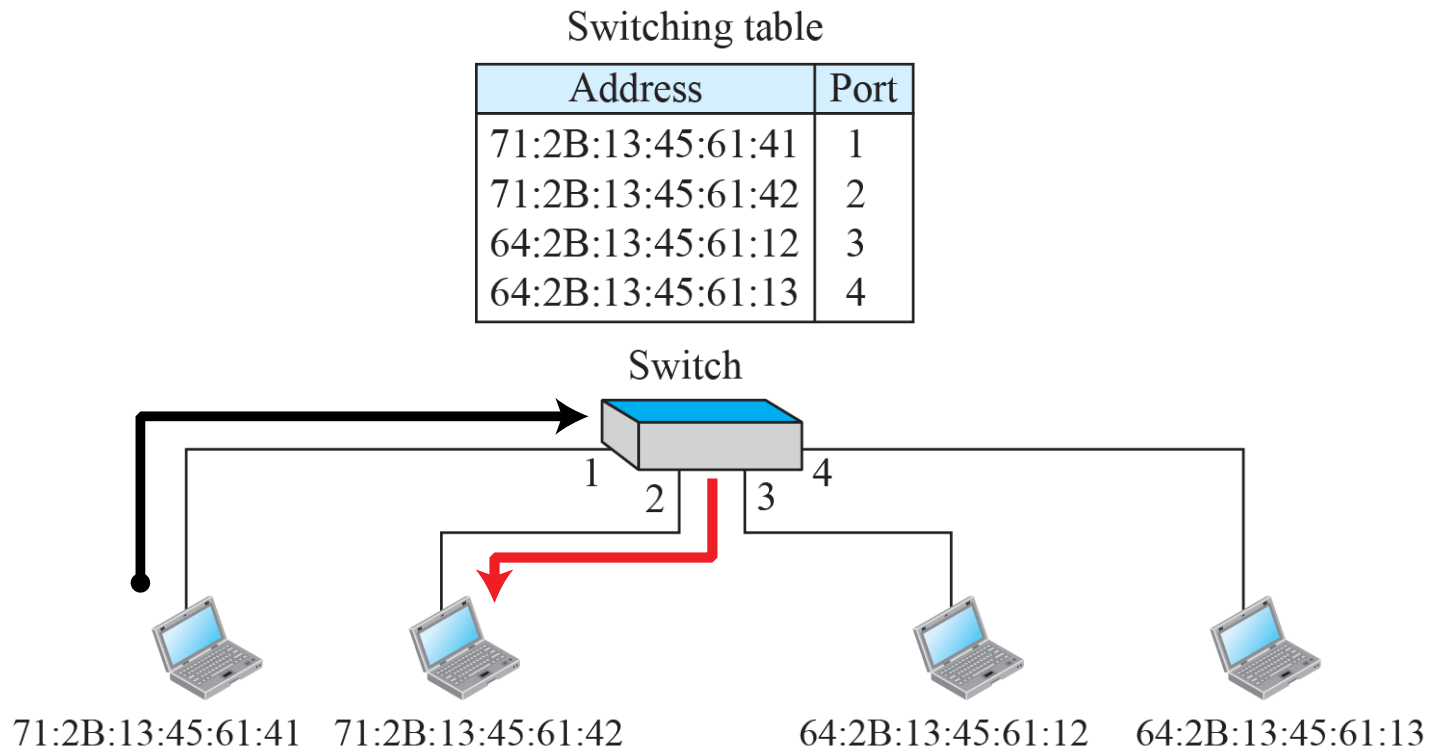
Switchat Ethernet

Moderna Ethernet-implementationer är switchade.
Varje host har sin egen länk.



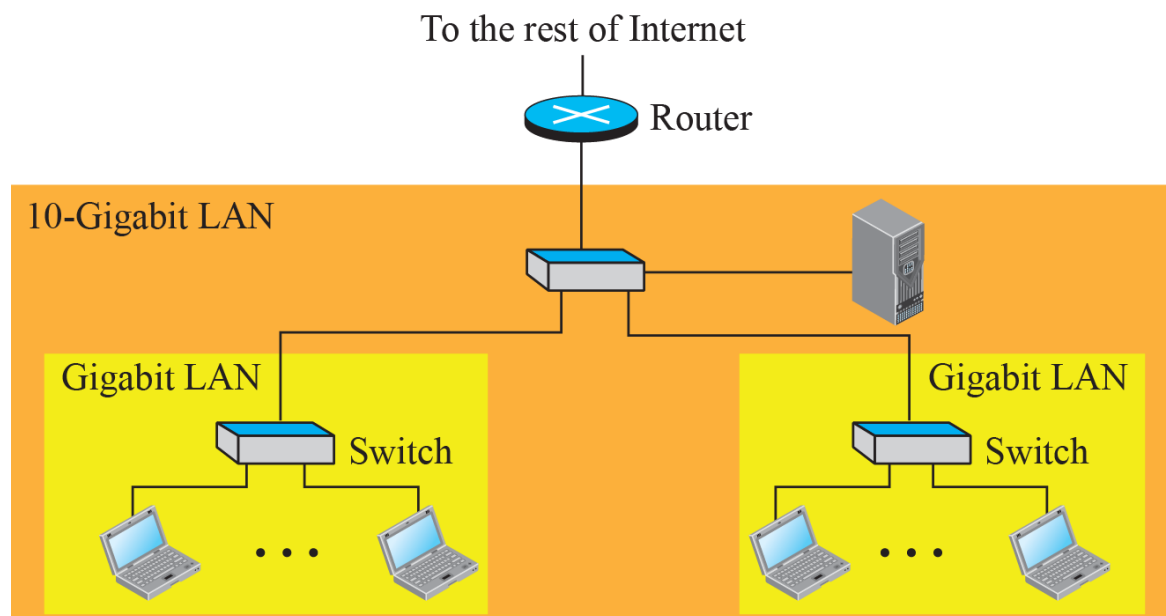
Grundfunktion för en brygga/switch

En brygga/switch har en adresstabell för att kunna skicka vidare ramar till rätt mottagare. Bryggan/Switchen är **lärande**, vilket innebär att den lär sig adresser den ”ser”.



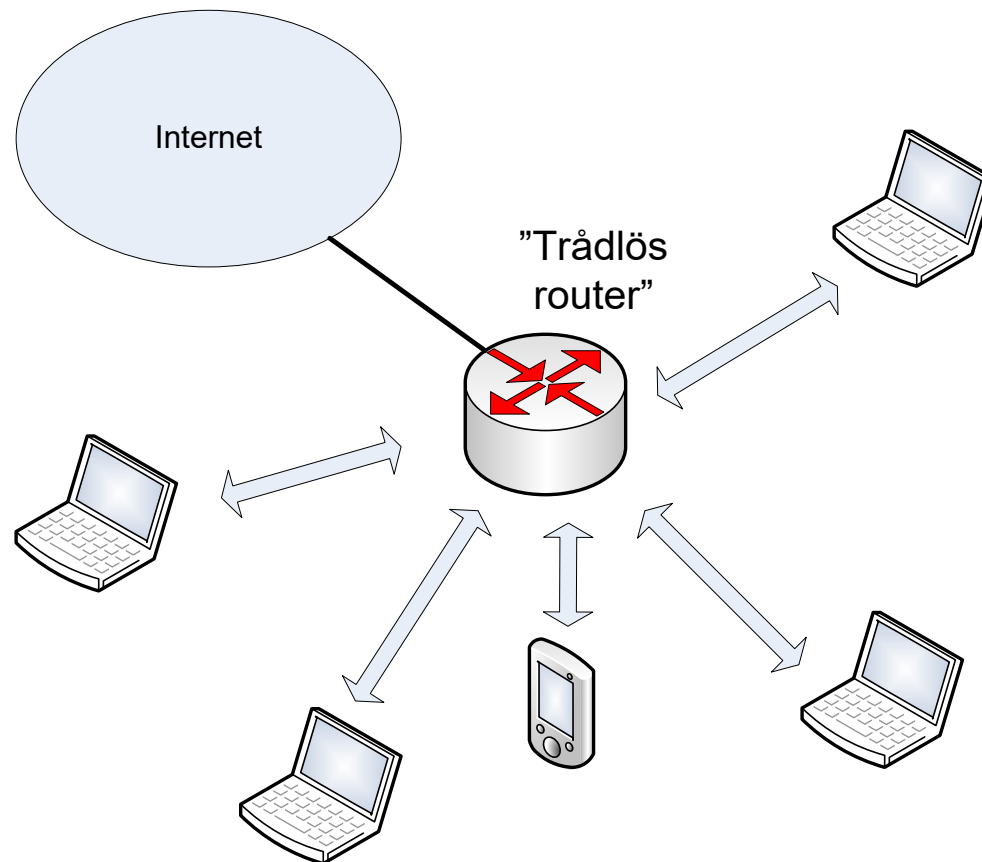
Switchade Ethernets

Ethernet-switchar kan användas för att bygga större nät. Broadcast-ramar skickas till alla hosts inom samma nät (nätet avslutas med en router).

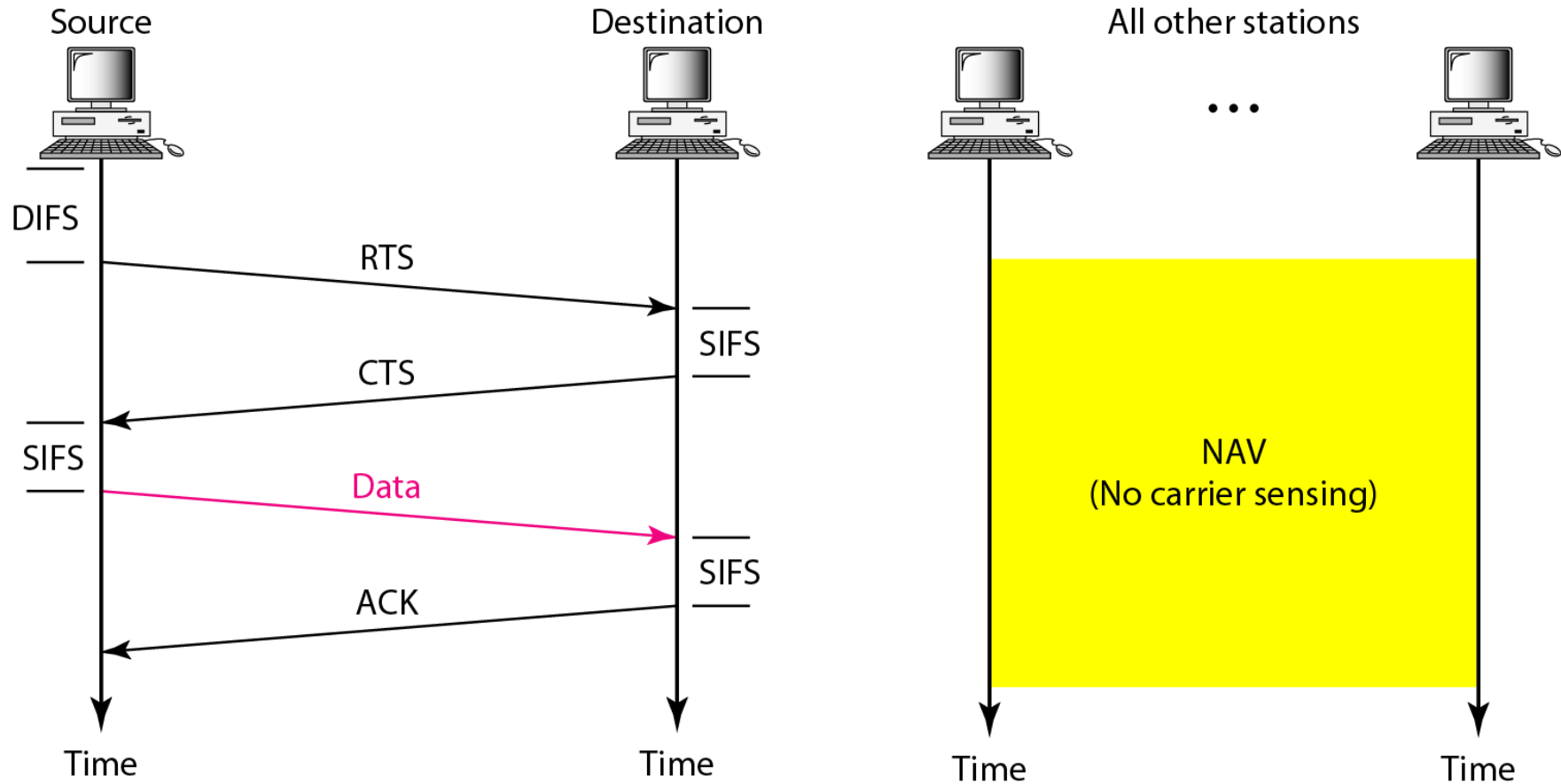


Trådlös access (WiFi), IEEE 802.11

Nätaccess sker ofta trådlöst med IEEE 802.11
WLAN

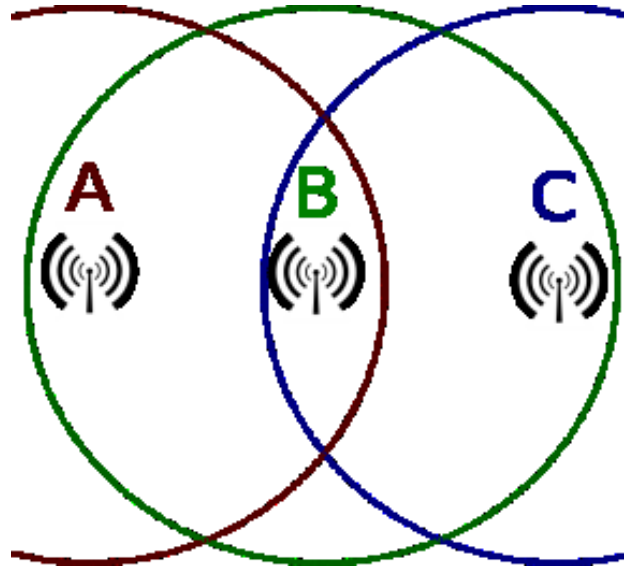


802.11 DCF används hemma



CSMA/CA kombinerat med en reservationsmetod (RTS/CTS)

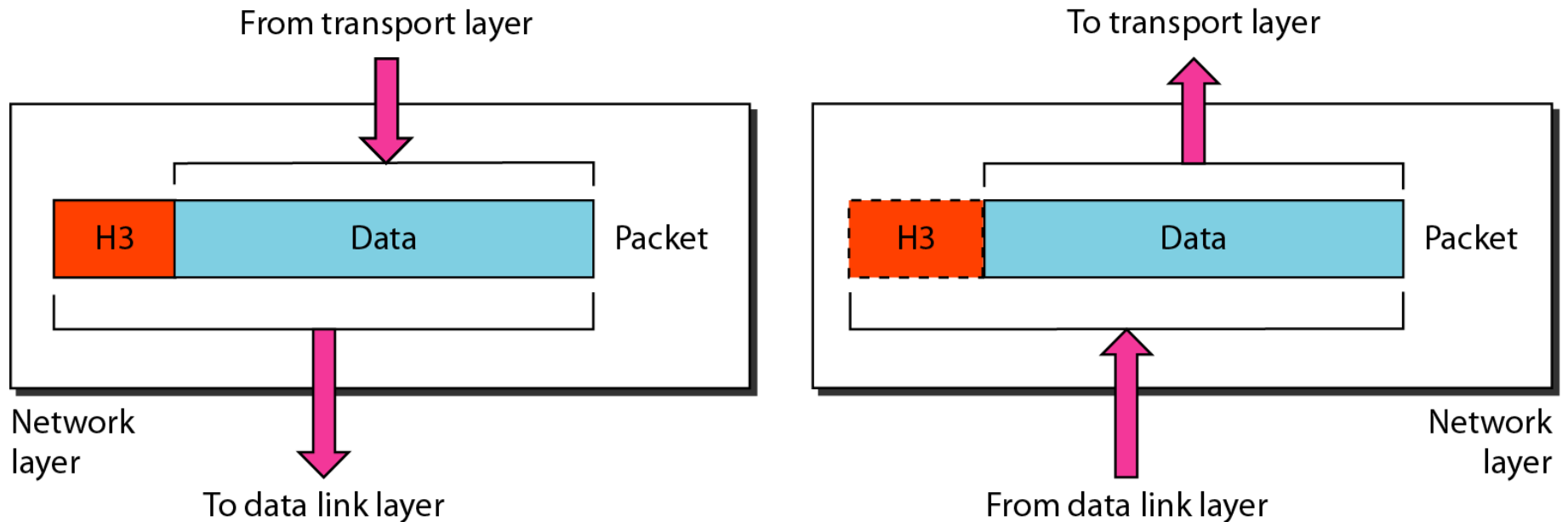
Hidden terminal problem



B = Basstation/
Accesspunkt

RTS/CTS löser problemet med "hidden terminals", dvs
att två terminaler kan höra basstationen men inte varandra.

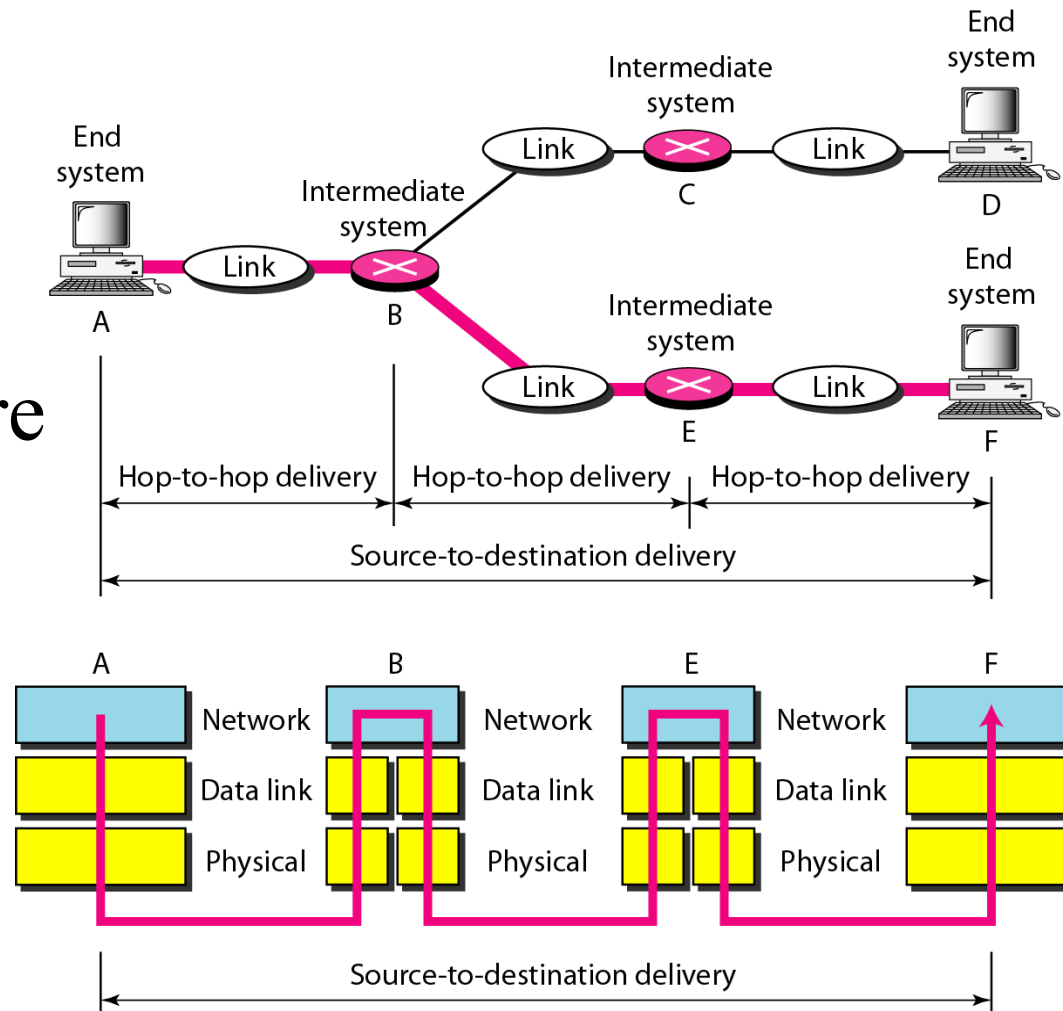
3. Nätskiktet (Network layer)



Nätskiktet är ansvarigt för att skicka paket mellan en sändar-host och en mottagar-host (som kan vara kopplade på olika nät).

Host-to-host delivery

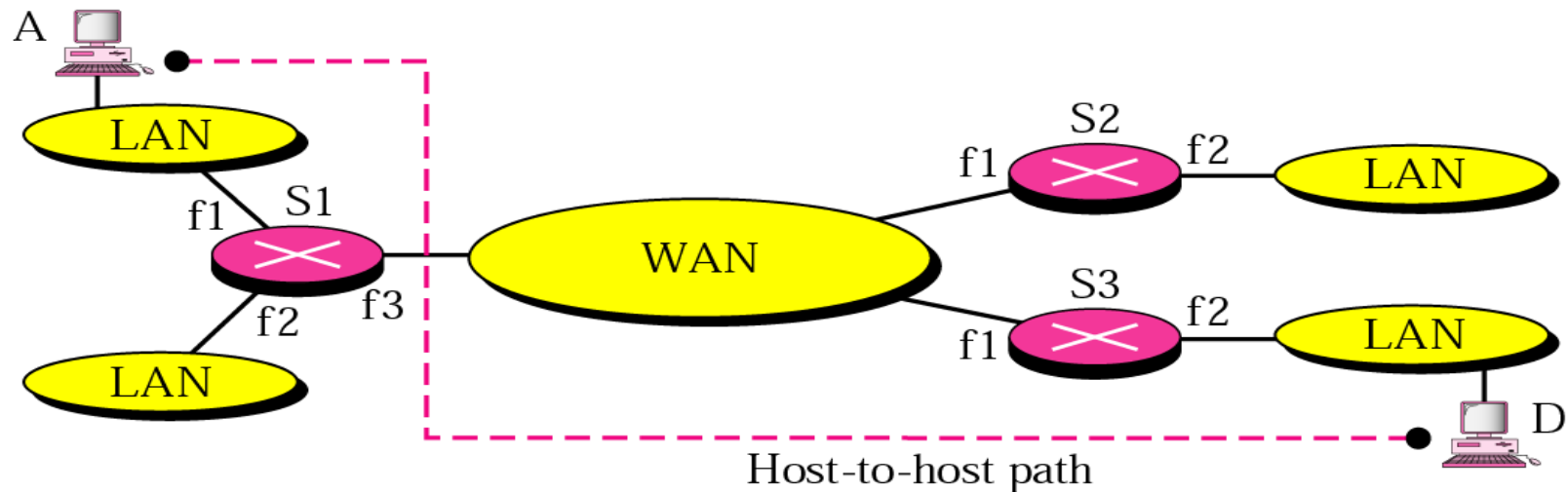
Nätprotokollet har ansvar för att skicka ett paket från en sändare till en mottagare över flera nät, så kallad host-to-host delivery.



Adressering och routing

- Vi behöver en adressering som är gemensam för alla nät. Detta kallas för **nätadress**.
 - Nätadressen måste bestå av en nät-id och en host-id, jämför med postadresser.
- Vi behöver regler för hur data skickas mellan nät till destinationen. Detta kallas för **routing**.
- Vi behöver en nätenhet som är kopplade till flera nät och som kan skicka data mellan näten. Denna enhet kallas för **router**.

Behovet av routrar



Router

En router förmedlar paket mellan nätverk baserat på nätadresserna.

- En router gör ”intelligenta” beslut om bästa väg för paketets vidare leverans mot slutdestinationen.
- Routing-beslut fattas utifrån nät-identitet, inte värd-identitet (*host id*)
 - Sista steget (för att hitta rätt host inom ett nät) görs med hjälp av fysiska adressen eftersom det är länkprotokollets uppgift.

Ett nätprotokoll: IP

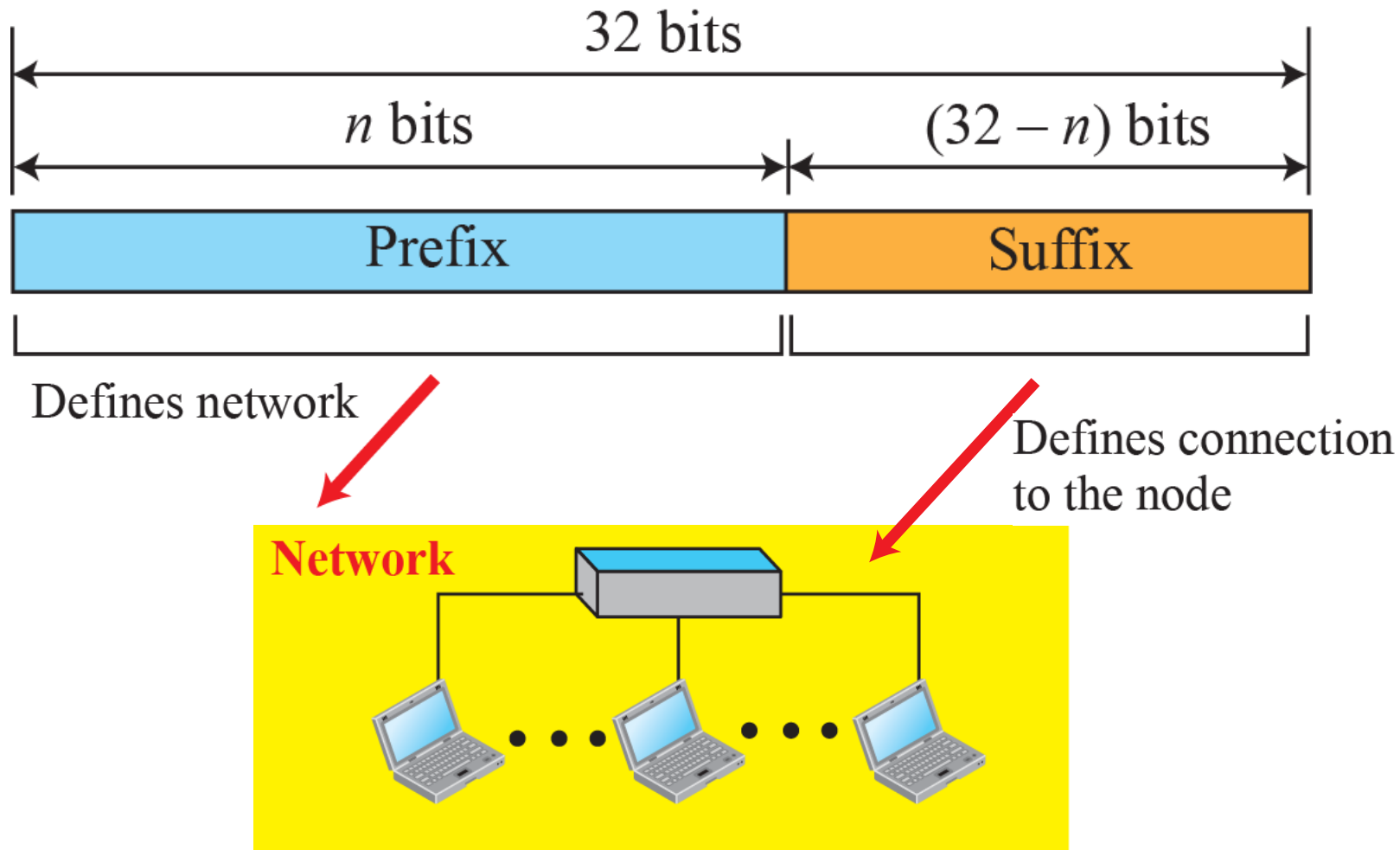
- **Internet protocol (IP)** är det enda nätprotokoll som får användas på Internet.
- Två versioner: IPv4 och IPv6.
- Adressering med IP-adresser
 - Exempel: **130.235.18.158** (IPv4)
- Data skickas som IP-paket (eller datagram)
- Förbindelsefri dataöverföring
- Checksum används men ingen felhantering eller flödeskontroll.

IPv4-adresser

IPv4-adressen består av två delar:

- **Nät-id** (netid, prefix) identifierar det nät som enheten är kopplad till.
- **Värd-id** (hostid, suffix) identifierar enheten själv inom detta nät.

IPv4-adresser



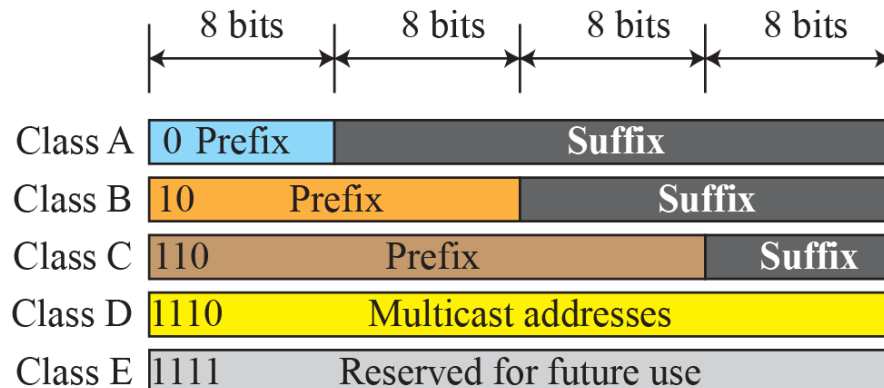
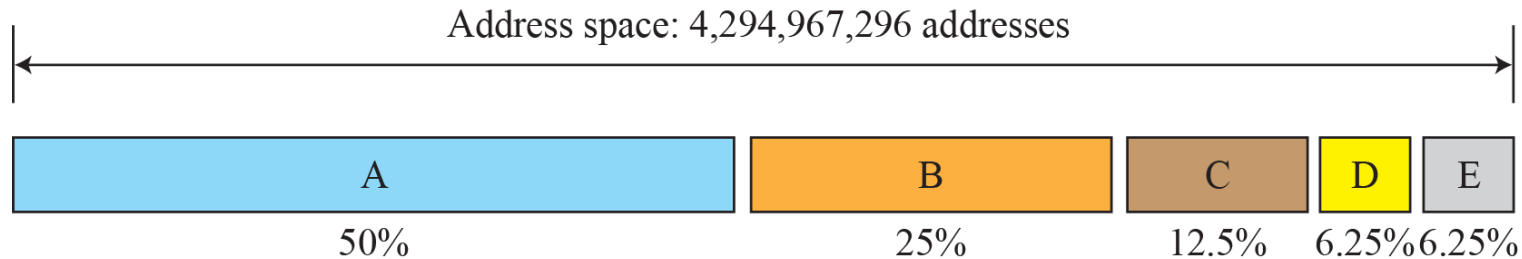
Adress-metoder

Det finns två sätt att definiera adresser:

- Klassindelad adressering (Classful addressing)
- Klasslös adressering (Classless addressing)

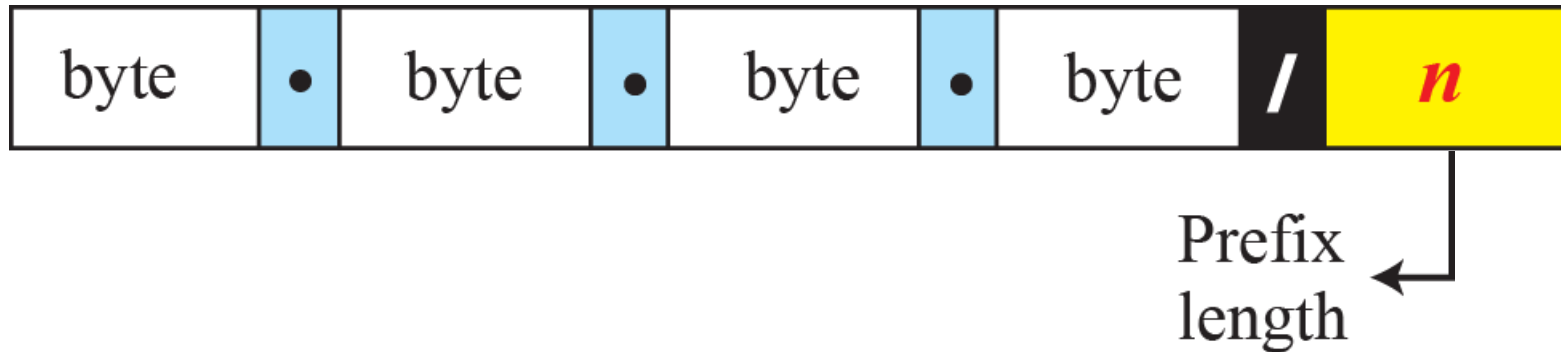
Klassindelad adressering

Fem adressklasser: A, B, C, (D, and E)



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Klasslös adressering (CIDR)



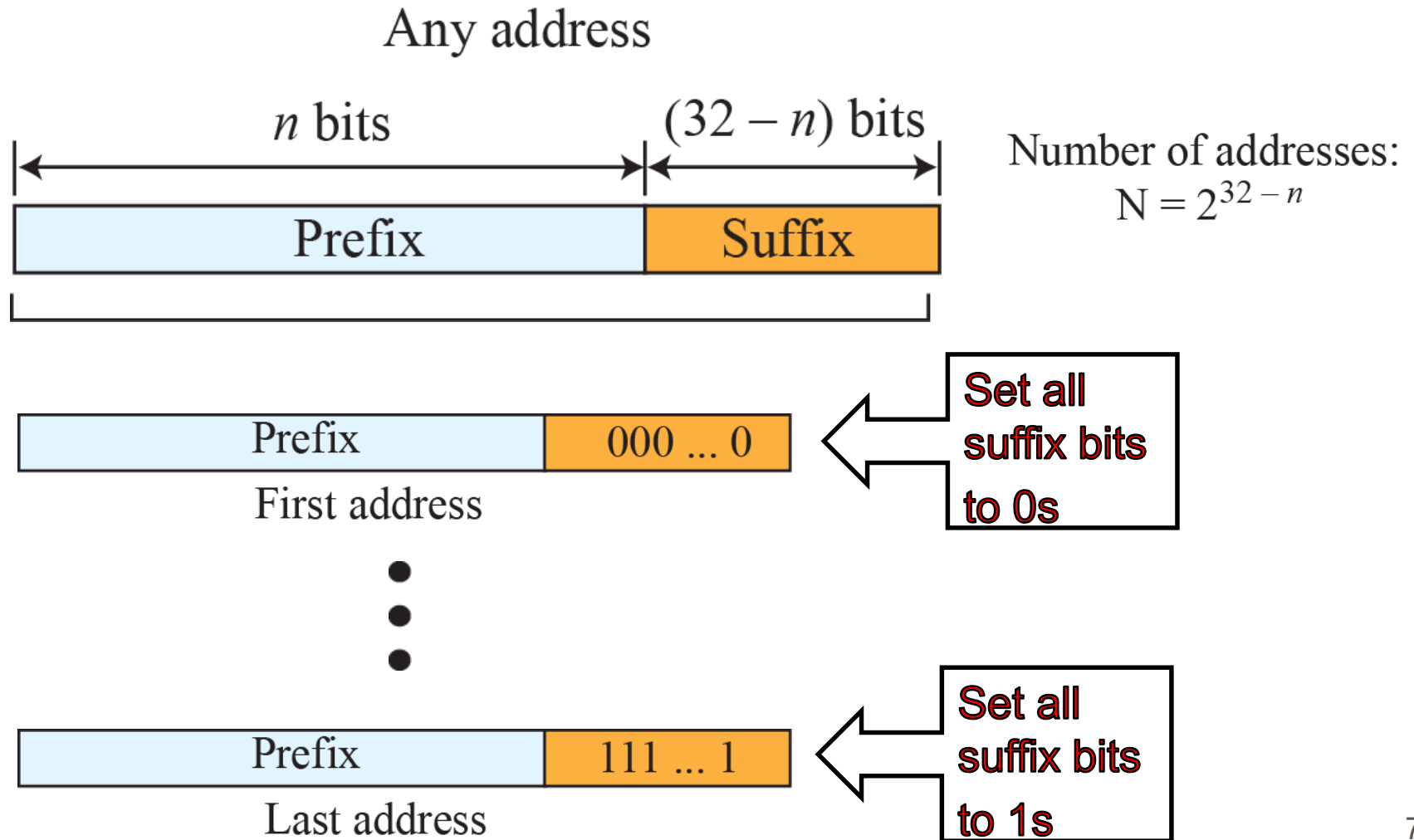
Examples:

12.24.76.8/**8**

23.14.67.92/**12**

220.8.24.255/**25**

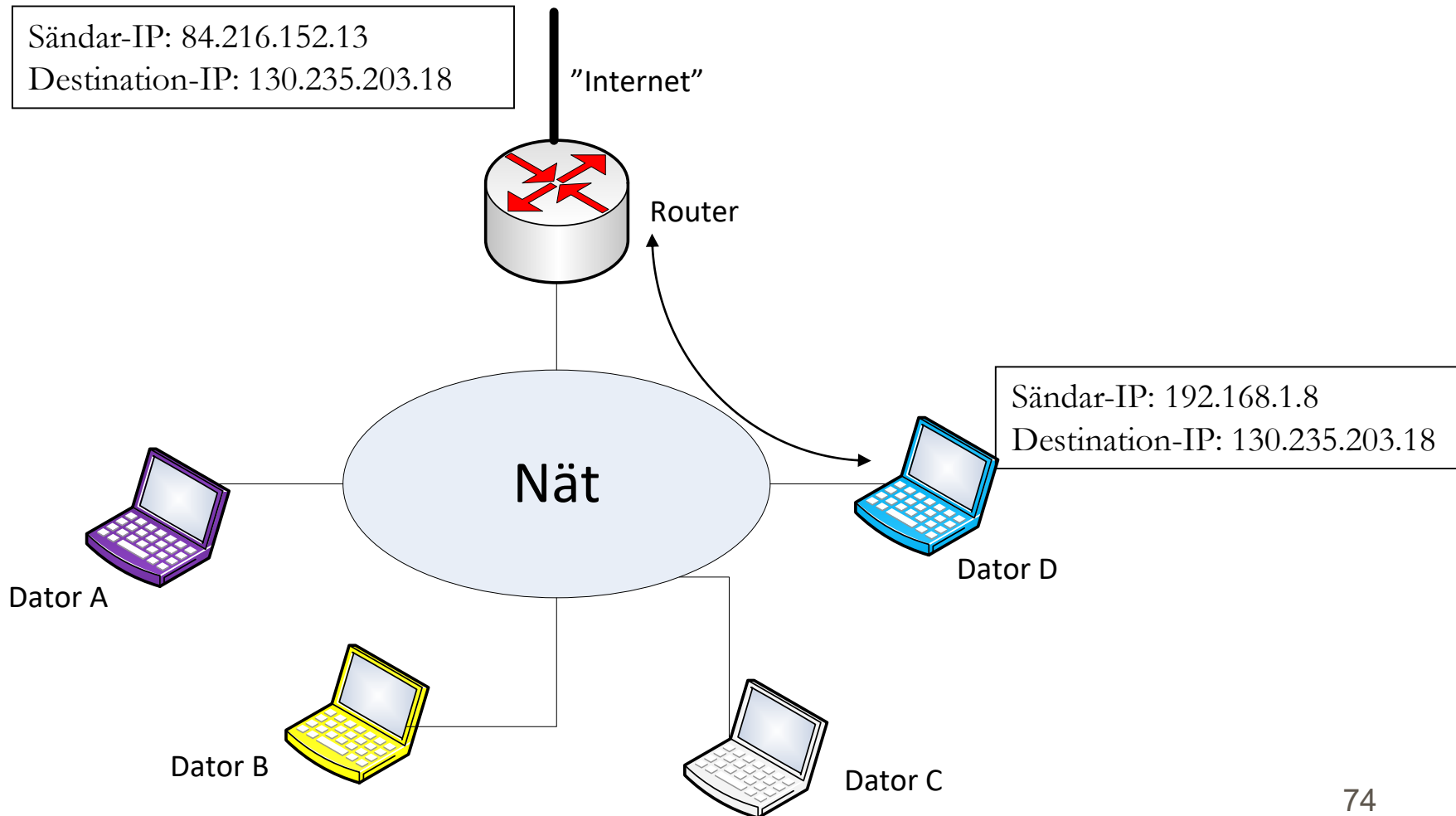
CIDR addressblock



Privata och publika IP-adresser

- Idag är IPv4-adresserna slut eftersom det finns fler anslutna enheter än det finns möjliga adresser.
- Därför används ett system med **privata** och **publika** IP-adresser.
- Inom ett lokalt nät (tex hemma) används en privat adress inom följande adressområden:
 - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
 - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
 - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

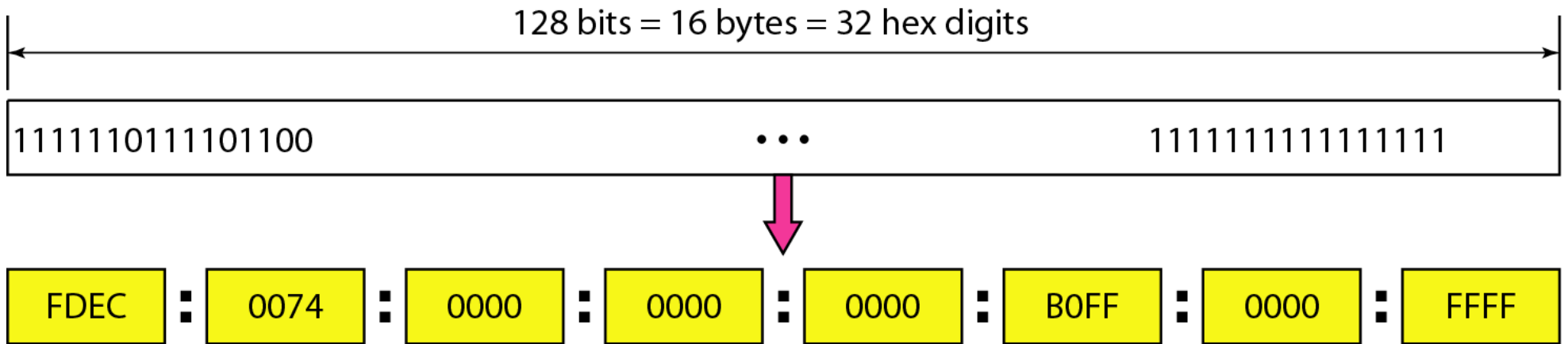
Network Address Translation (NAT)



Några fördelar med IPv6

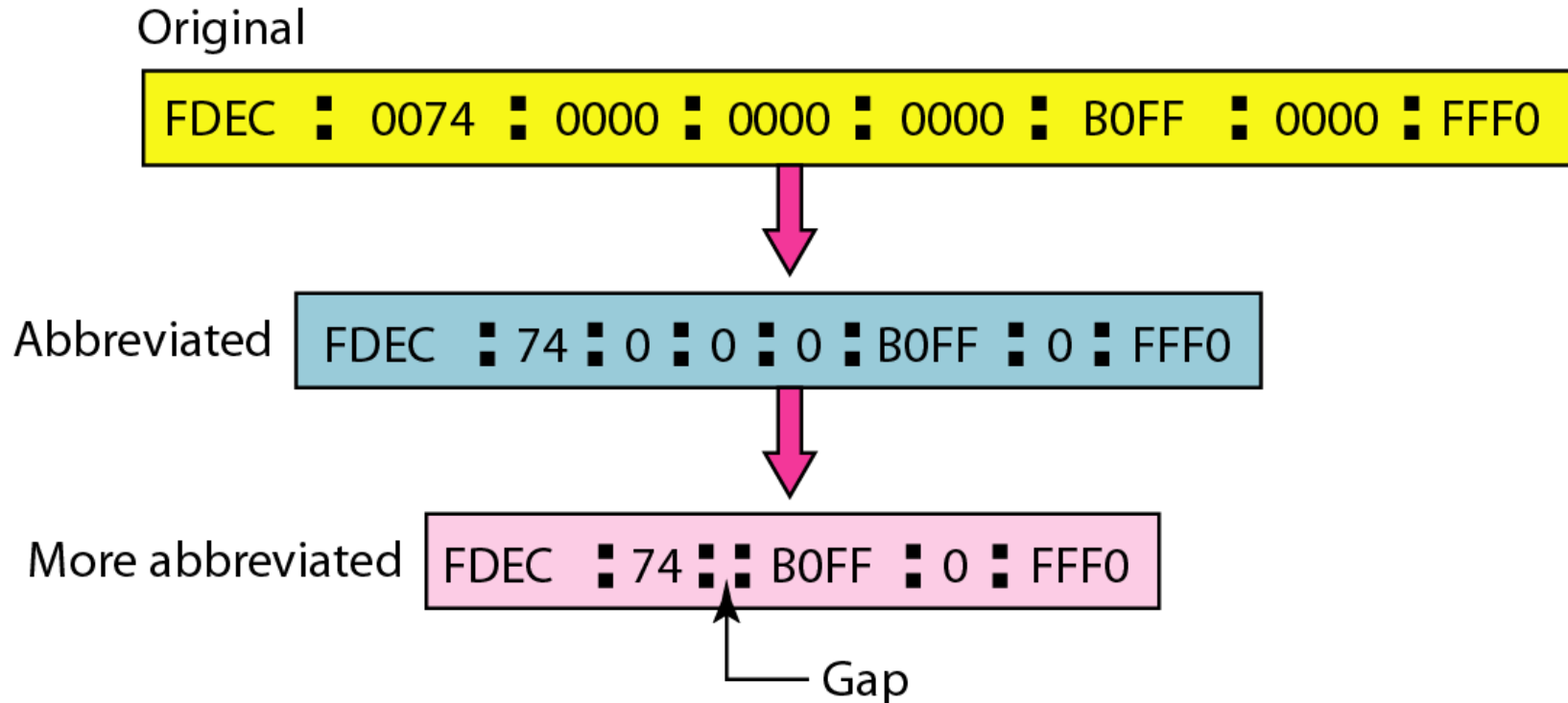
- Mycket fler adresser: 128 bitars adresser.
- Bättre headerformat: Basheader på 40 bytes vilket gör forwarding lättare.
- Stöd för datasäkerhet: IPv6 innehåller funktioner för kryptering och autentisering.
- Stöd för realtidsapplikationer: Prioritet i routrar av streaming-datagram kan begäras (flödeshantering).

IPv6-adresser



Hexadecimal colon notation

Förkortning av IPv6-adresser



Man kan bara ta bort hela sektioner av 0:or en gång.

Att få en IP-adress

Dynamic Host Configuration Protocol (DHCP):

1. När en terminal kopplas in i ett nät skickar terminalens DHCP-klient ett broadcast meddelande med en DHCP-förfrågan.
2. DHCP-servern i nätet (tex routern) svarar med ett erbjudande om IP-adress och annan information (tex nätverksadress, Default gateway, DNS-server etc.).
3. Terminalen kan tacka ja till detta erbjudande och får därmed en IP-adress som gäller en viss tid.

Att mappa IP-adresser mot MAC-adresser

För att en host/router ska kunna hitta en annan host/router inom samma nät måste IP-adressen ”översättas” till en fysisk adress.

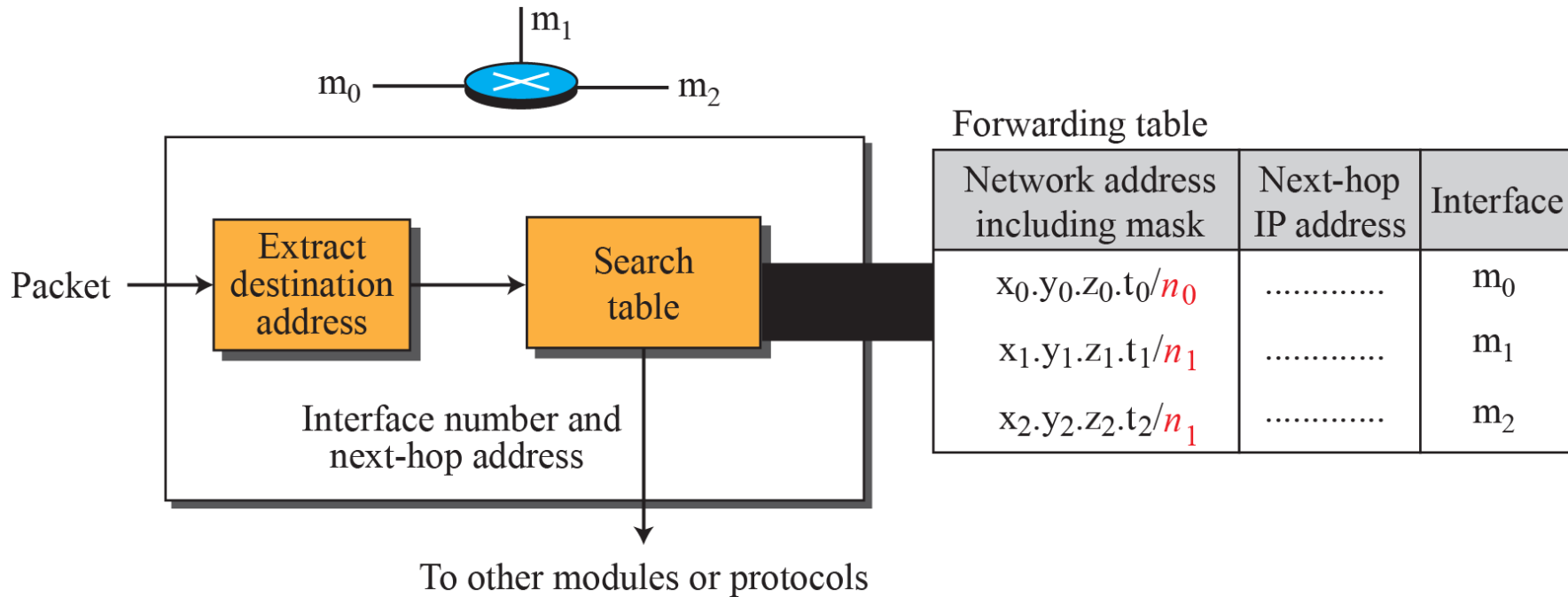
Adress Resolution Protocol (ARP) används för att mappa IP-adresser mot MAC-adresser inom ett LAN.

En host i ett LAN vet alltid IP-adressen till den router (default router/gateway) som är kopplad till ”resten av Internet”.

ARP

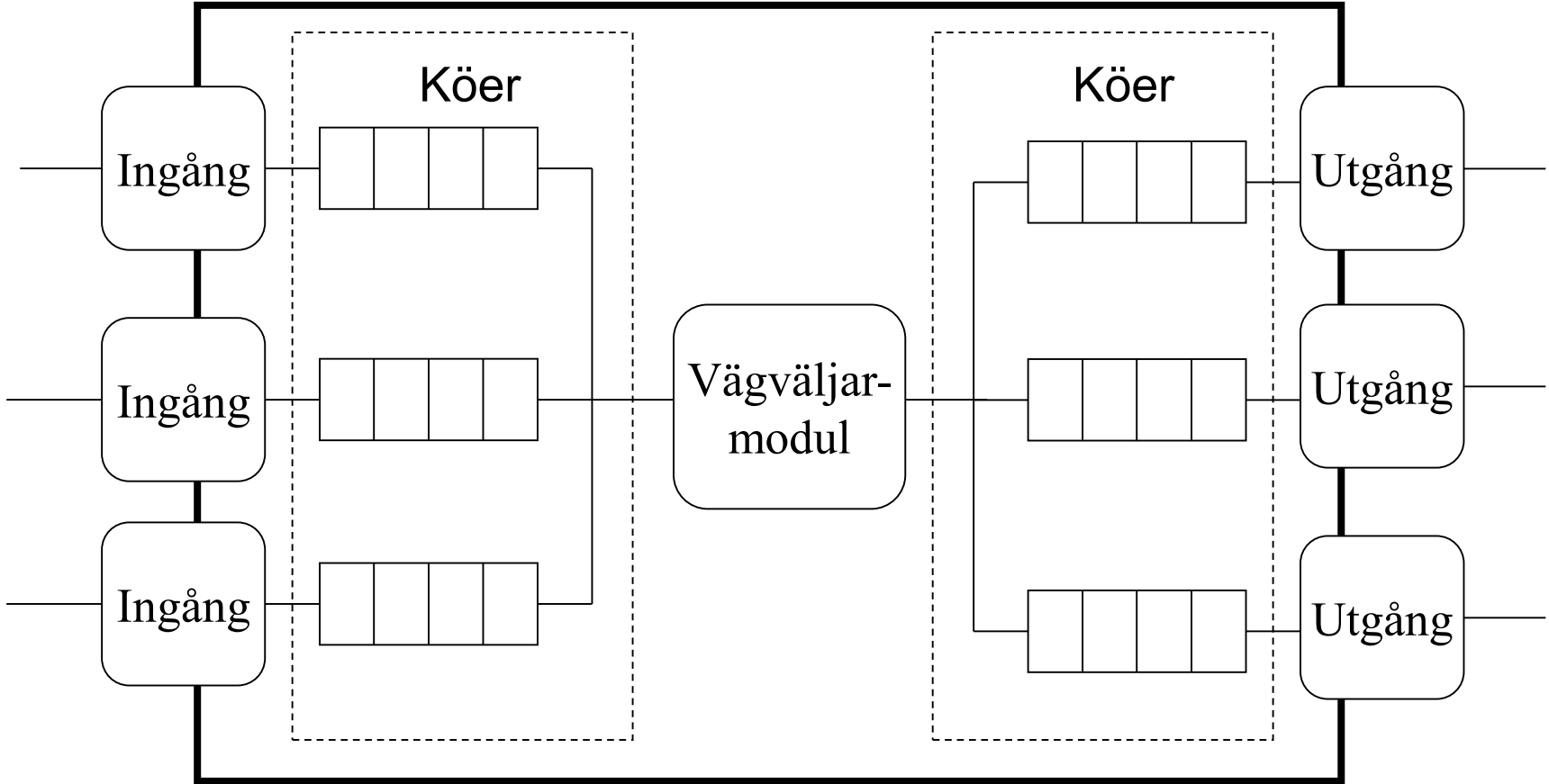
- Varje host/router har en ARP-cache (tabell) som används för att lagra MAC/IP-adresspar.
- En host/router broadcastar en **ARP query packet** varje gång den behöver mappa en IP-adress mot en MAC-adress.
- Den host som har IP-adressen svarar med en **ARP response packet**.

Routrar använder nätadressen

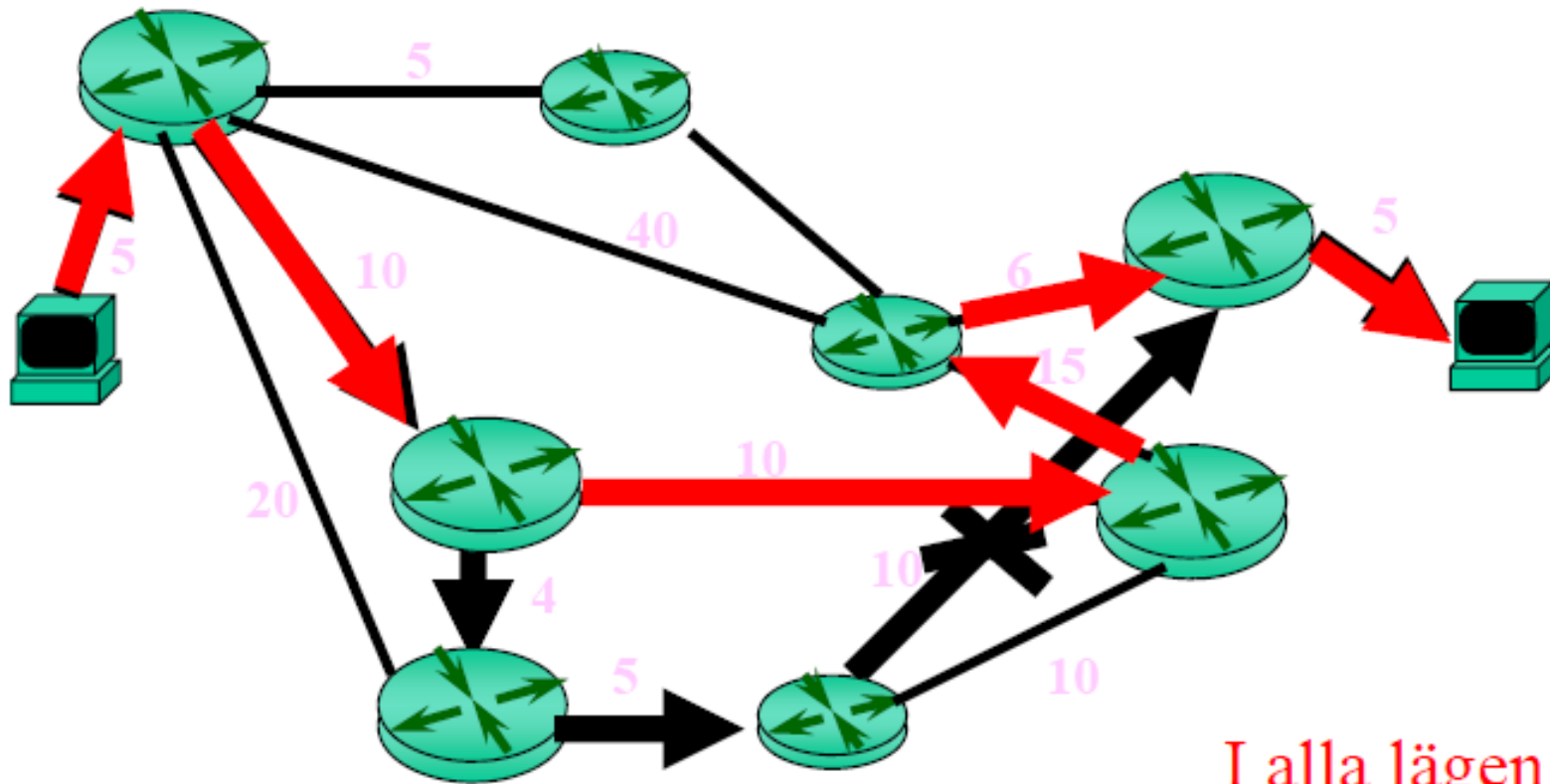


Alla routrar måste kunna så kallad **forwarding**, dvs skicka vidare paket baserat på nätadressen.

Illustration av en router



Routing: Välj bästa väg!



Distribuerad routing

- Distance Vector
 - Varje nods information om bästa vägar distribueras till nodens grannar
 - Bästa väg end-to-end fås fram genom jämförelse med alla möjliga *next hop*
 - Enkelt, låga krav på processor och minne
- Link State
 - Lokal information om topologi flödas (*flooding*) till alla noder
 - Bästa väg end-to-end till alla noder beräknas lokalt i varje nod (trädbyggnad)
 - Komplicerat med krav på processorkraft och minne

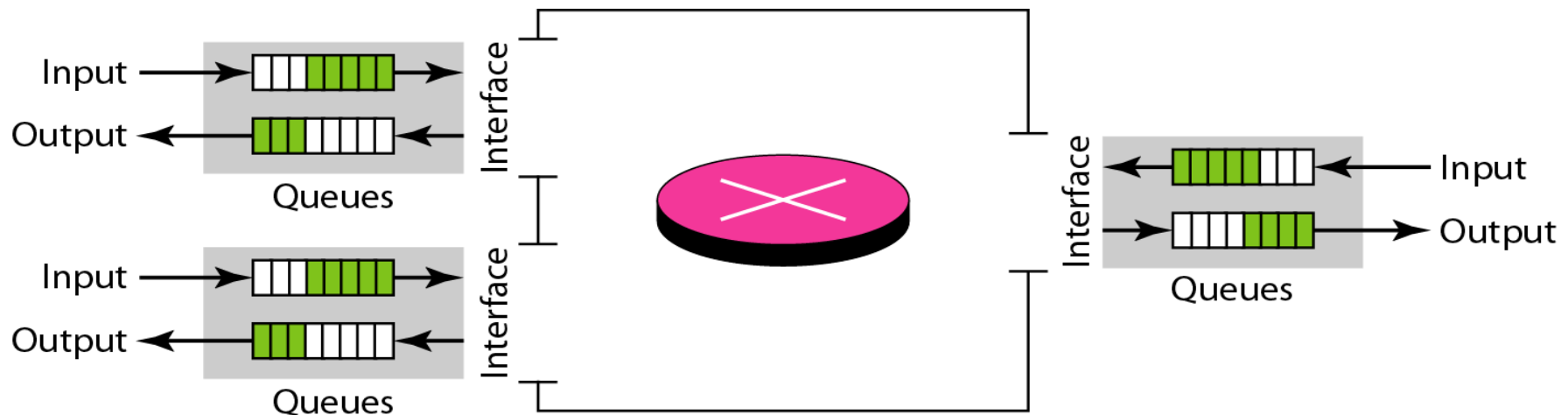
Länkkostnad

Länkkostnaden kan bero på flera saker:

- Kapacitet
- Belastning
- Sträcka
- Utbredningsmedium
- Osv..

Vad händer när något går fel i IP?

Alla routrar har buffertar där paket lagras i väntan på processering. När lasten ökar i nätet fylls buffertarna, och paketfördröjningen ökar. Till slut kan paket kastas på grund av överfulla buffertar. Eftersom IP inte har någon felhantering måste ett annat protokoll ta hand om detta.

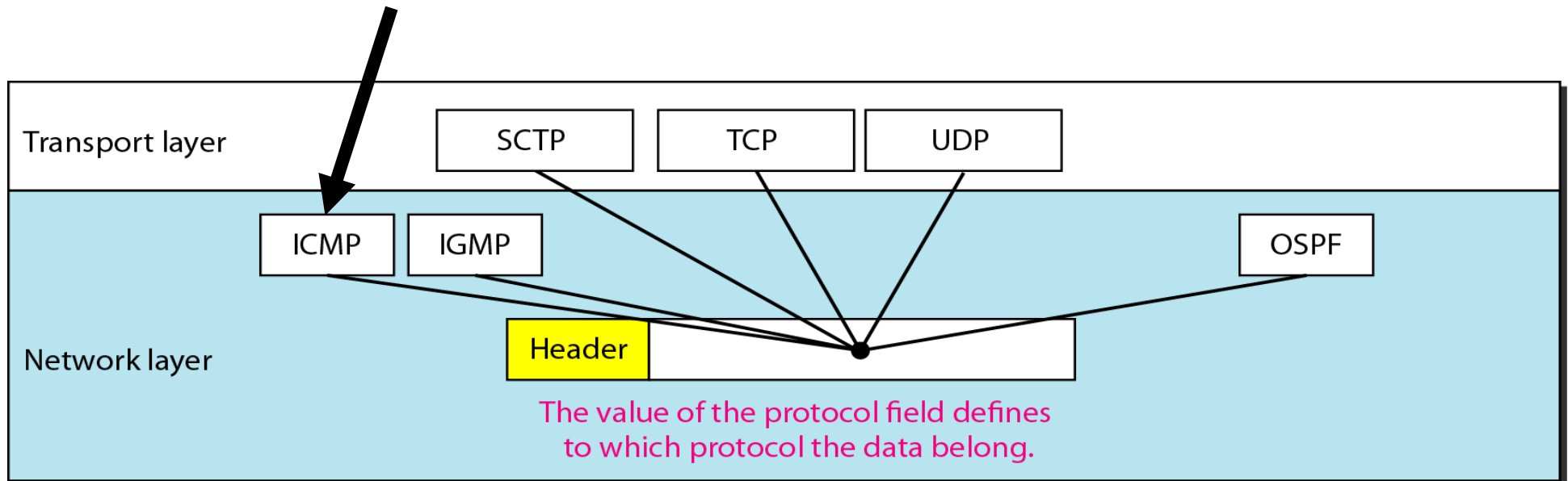


Internet Control Message Protocol (ICMP)

- IP har inga funktioner för fel-rapportering eller fel-hantering. IP saknar också funktioner för förfrågningar till/från hosts och routrar.
- Internet Control Message Protocol (ICMP) har utvecklats för att kompensera för detta.
- Man brukar säga att ICMP är ett hjälpprotokoll till IP.

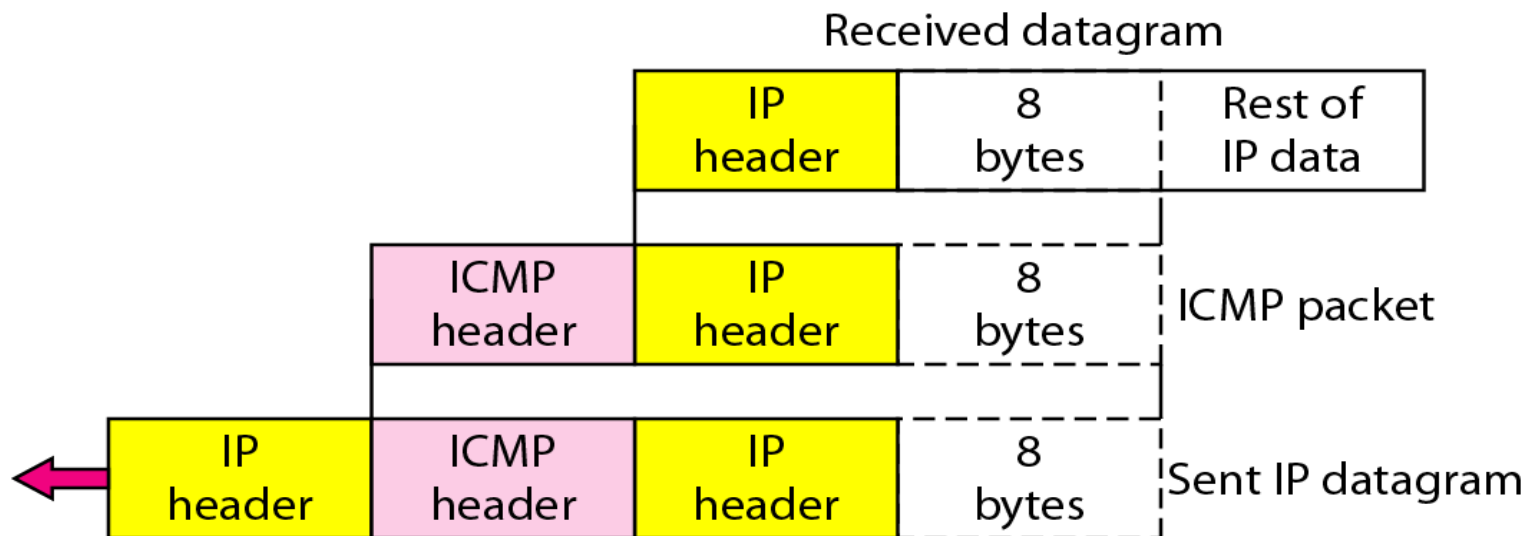
Encapsulation

Ett ICMP-meddelande skickas i ett IP-paket:



Fel-rapportering

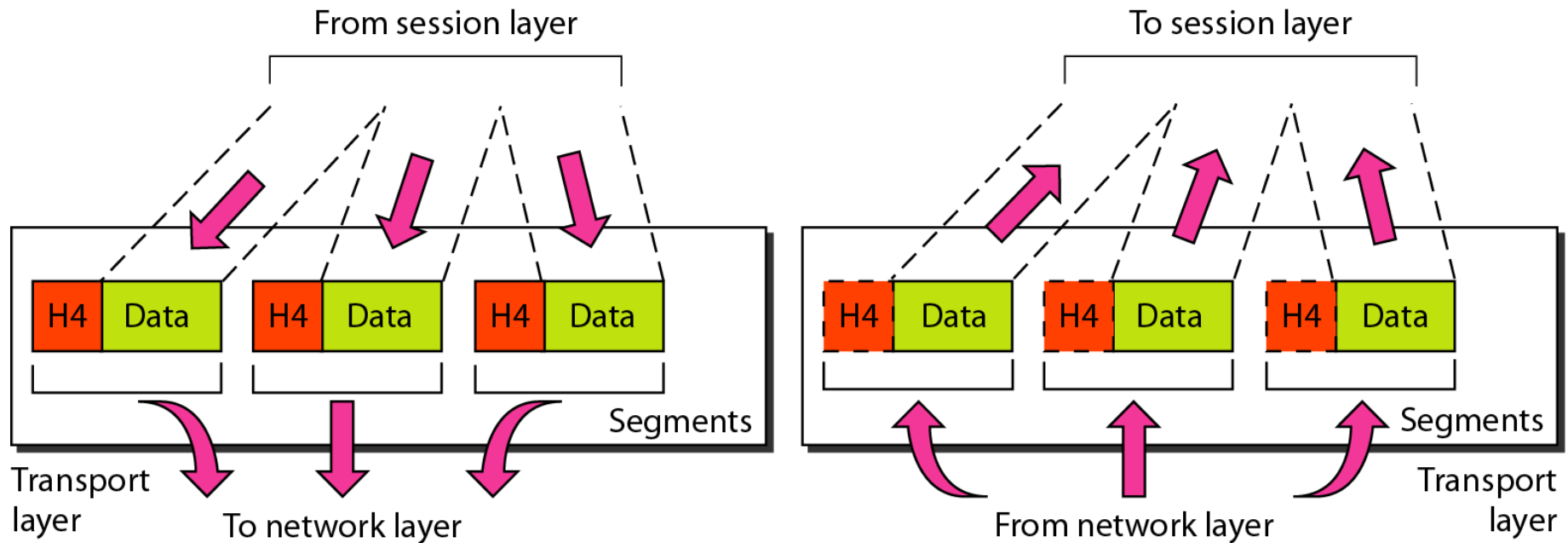
När ett IP-paket inte kan komma fram till sin destination, används ICMP för att rapportera felet till sändar-hosten. Felmeddelandet innehåller IP-headern + de första 8 byten av det ursprungliga IP-paketet.



ICMP Query medelanden

- En host/router kan skicka en ICMP query till en annan host/router:
 - **Echo-request and Reply**: Används för att kolla om två hosts/routers har en fungerande kommunikation på IP-nivån (tex. ping).
 - **Timestamp request and reply**: Används för att estimerera round-trip time (RTT) mellan två hosts/routers.
 - **Router-Solicitation and Advertisement**: Används av en host för att identifiera vilka routers som sitter på samma nät.

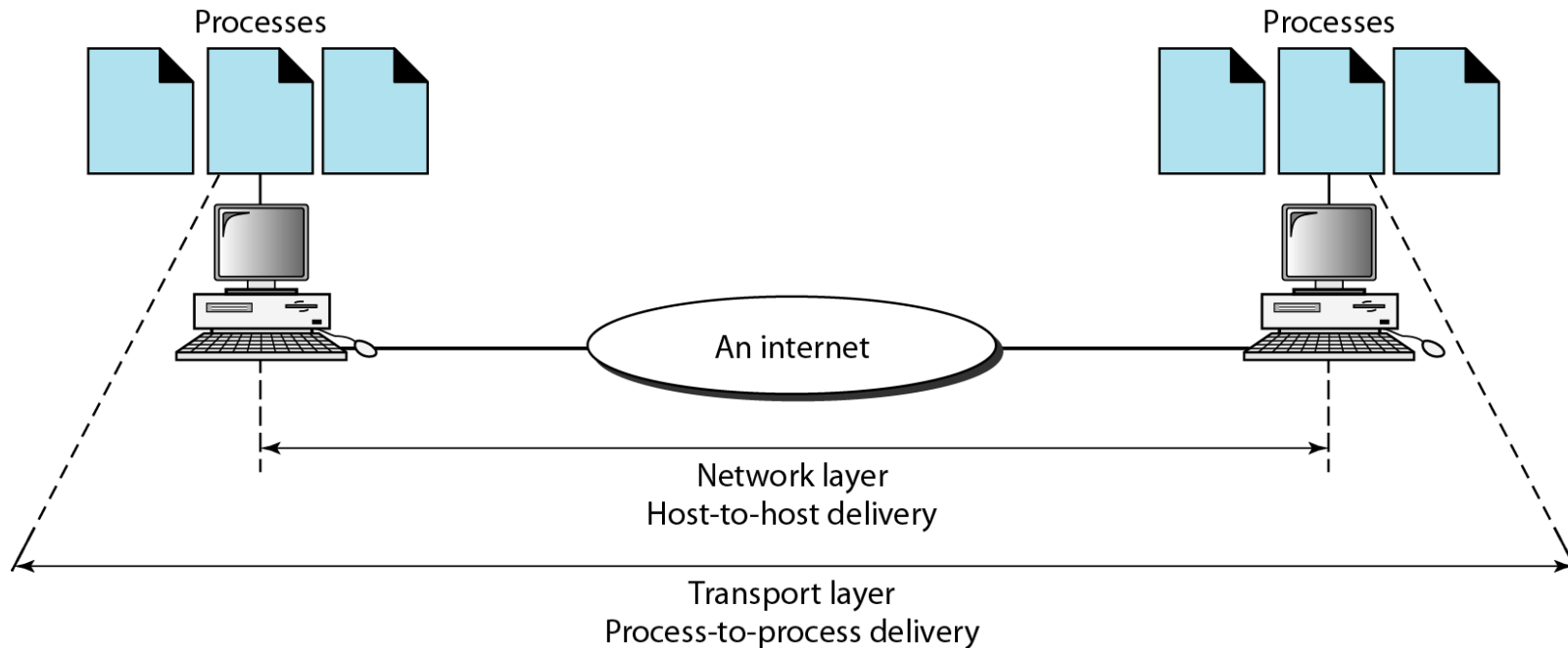
4. Transportskiktet (Transport layer)



Transportskiktet är ansvarigt för att skicka meddelanden mellan två applikationsprocesser.

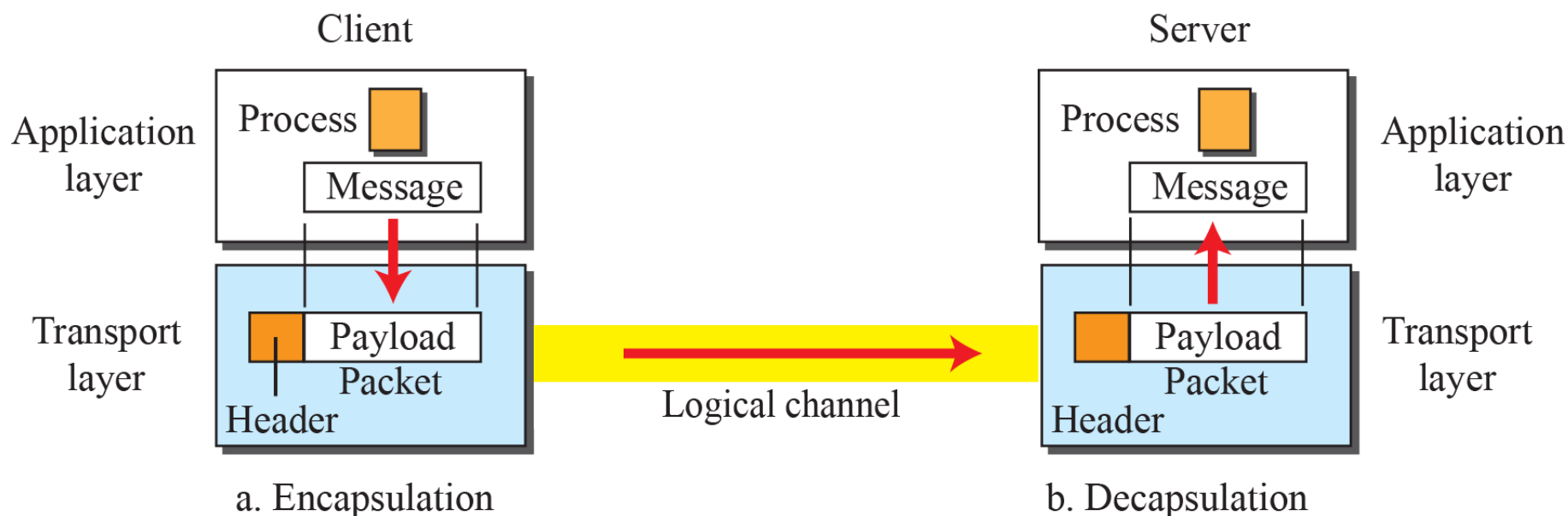
Process-to-process delivery

Transportprotokollet sköter **process-to-process delivery**.



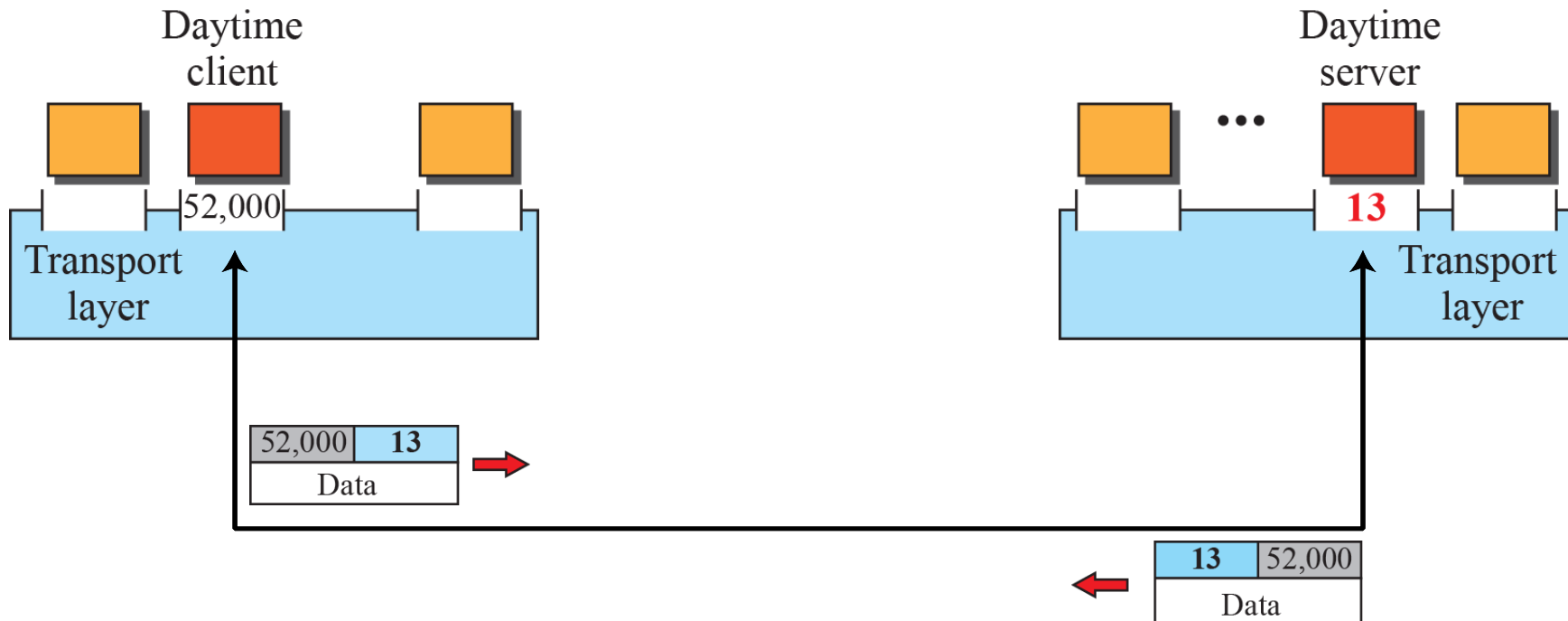
Transportprotokollet

Transportprotokollet ”packar in” (enkapsulerar) data från applikationen och ser till att det skickas till rätt mottagarapplikation. Mottagarens transportprotokoll ”packar upp” datan igen.



Portnummer

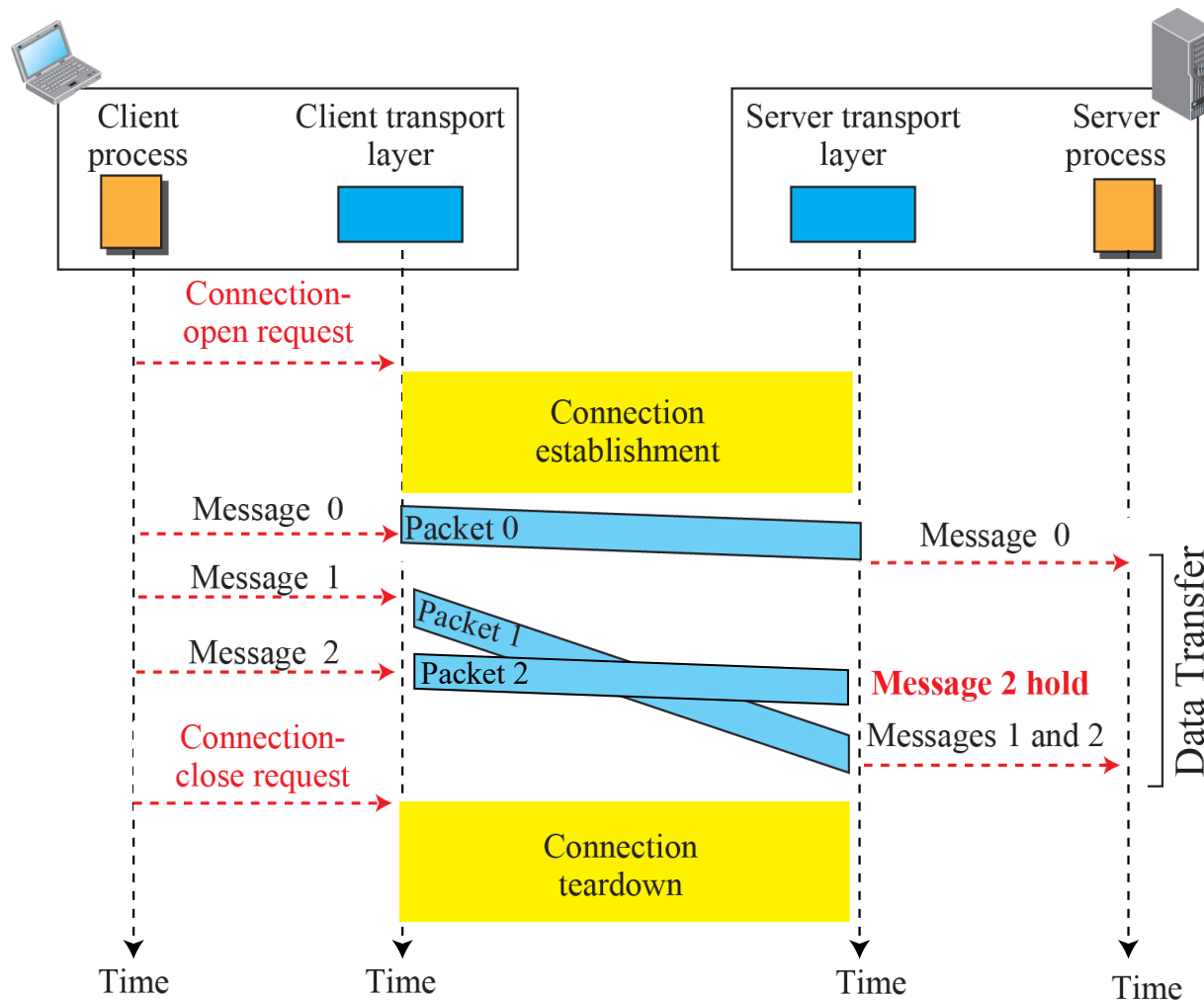
Transportprotokollet använder **portnummer** (portadresser) för att separera applikationer på en viss host.



Ett transportprotokoll: TCP

- Transmission Control Protocol (TCP) är ett av de transportprotokollen som används på Internet.
- Tillhandahåller en förbindelseorienterad dataöverföring med felhantering och flödeskontroll.
- TCP använder Checksum och en Go-back-N ARQ algoritm.

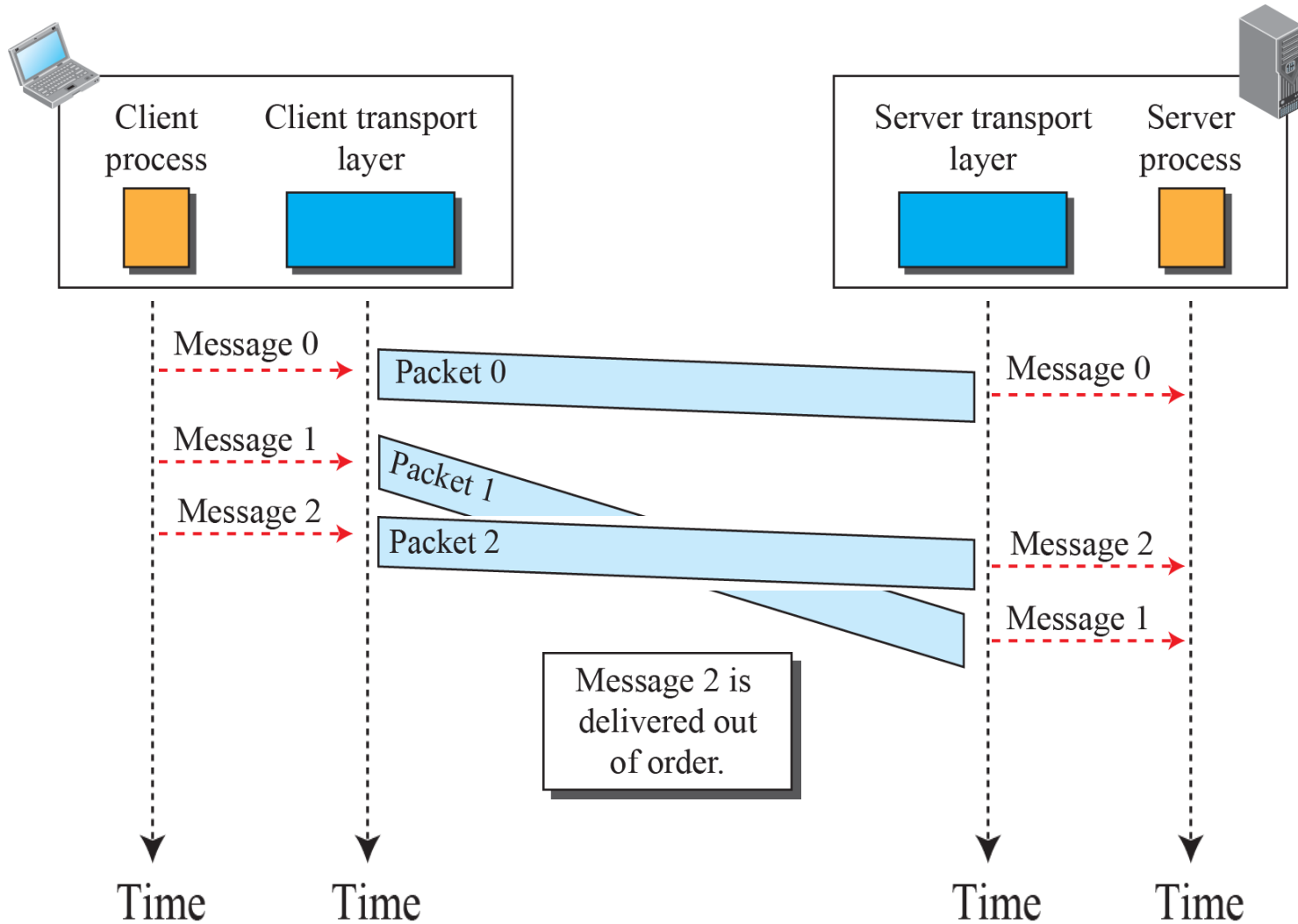
TCPs förbindelseorienterade dataöverföring



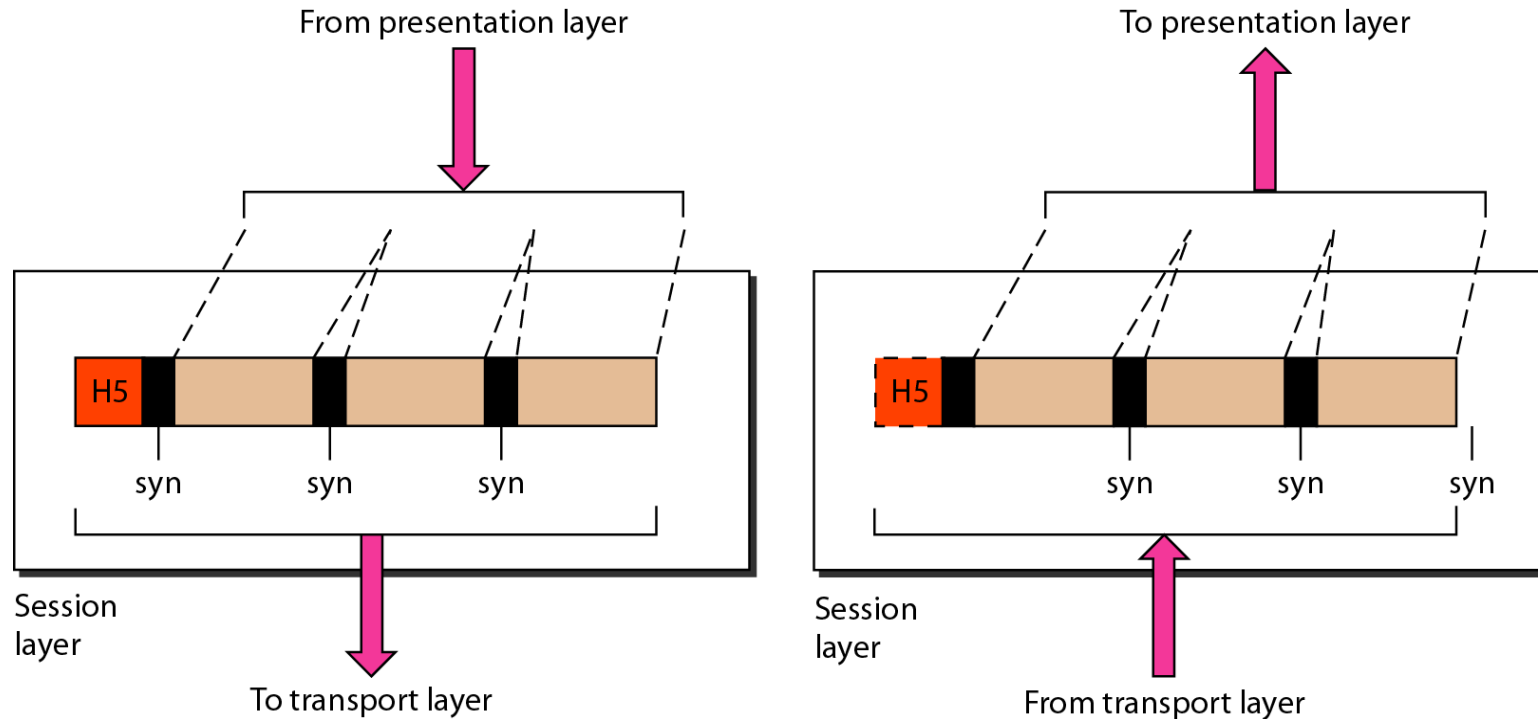
Ett transportprotokoll: UDP

- User Datagram Protocol (UDP) är ett annat transportprotokoll som används på Internet.
- UDP tillhandahåller en förbindelsefri dataöverföring utan felhantering eller flödeskontroll.
- UDP använder en Checksum.

UDPs förbindelsefria dataöverföring

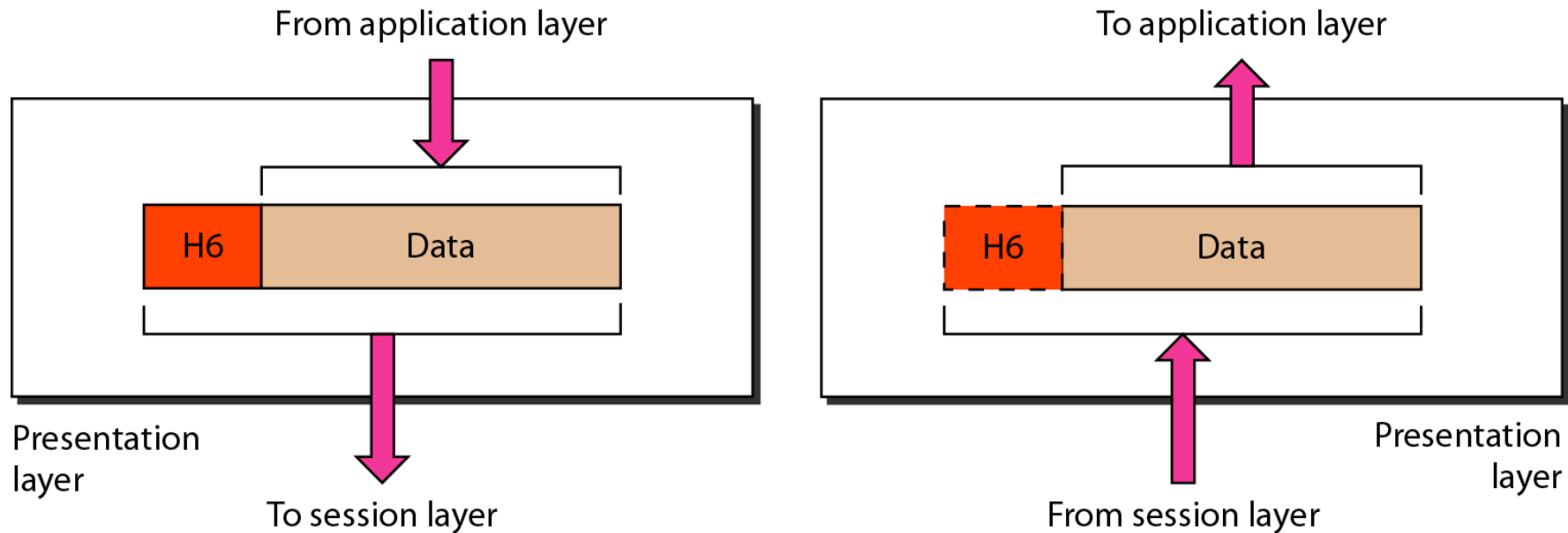


5. Sessions-skiktet (Session layer)



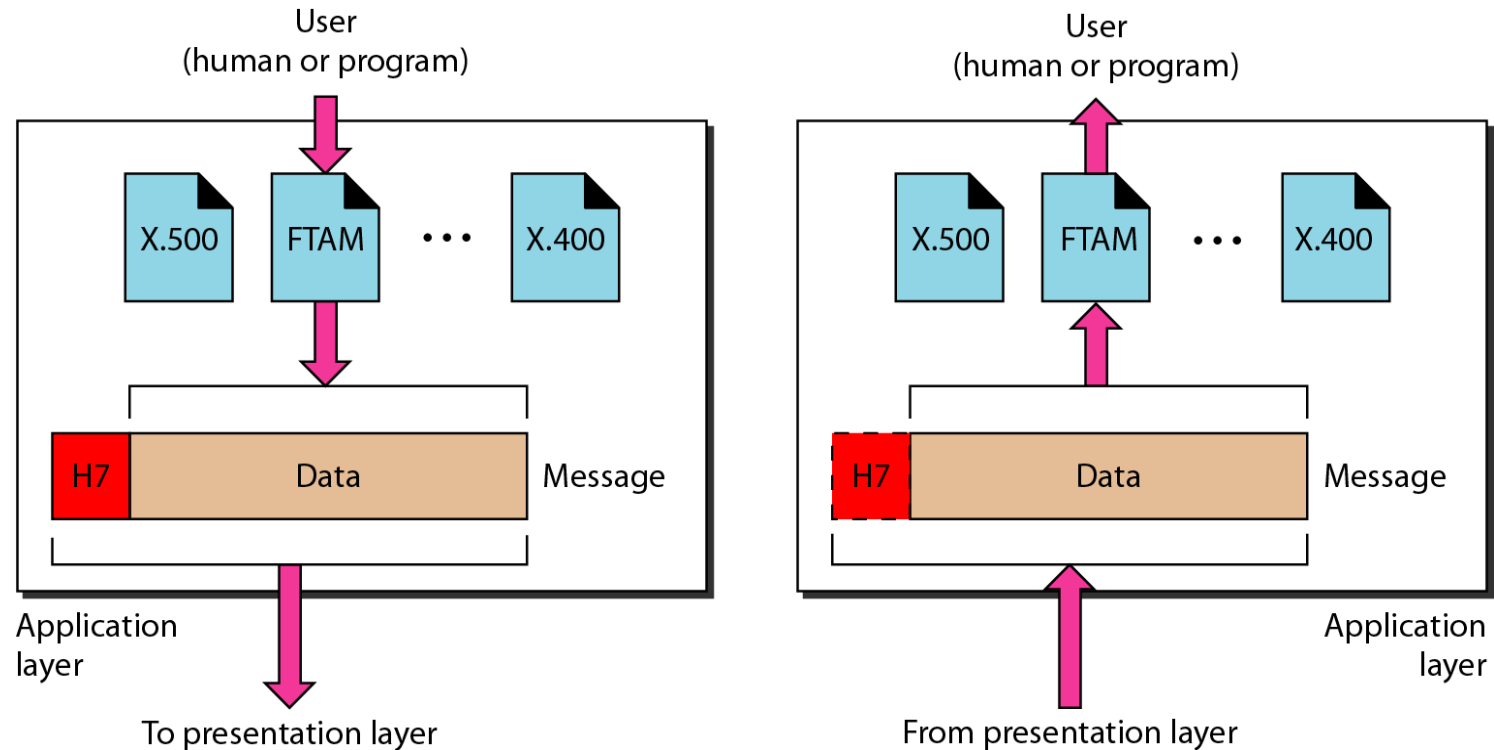
Sessions-skiktet är ansvarigt för styrning och-synkronisering av dialogen mellan sändar- och mottagarprocess.

6. Presentations-skiktet (Presentation layer)



Presentations-skiktet är ansvarigt för översättning, komprimering och kryptering av applikationsdata.

7. Applikations-skikt (Application layer)



Applikations-skiktet är ansvarigt för att tillhandahålla användartjänster.

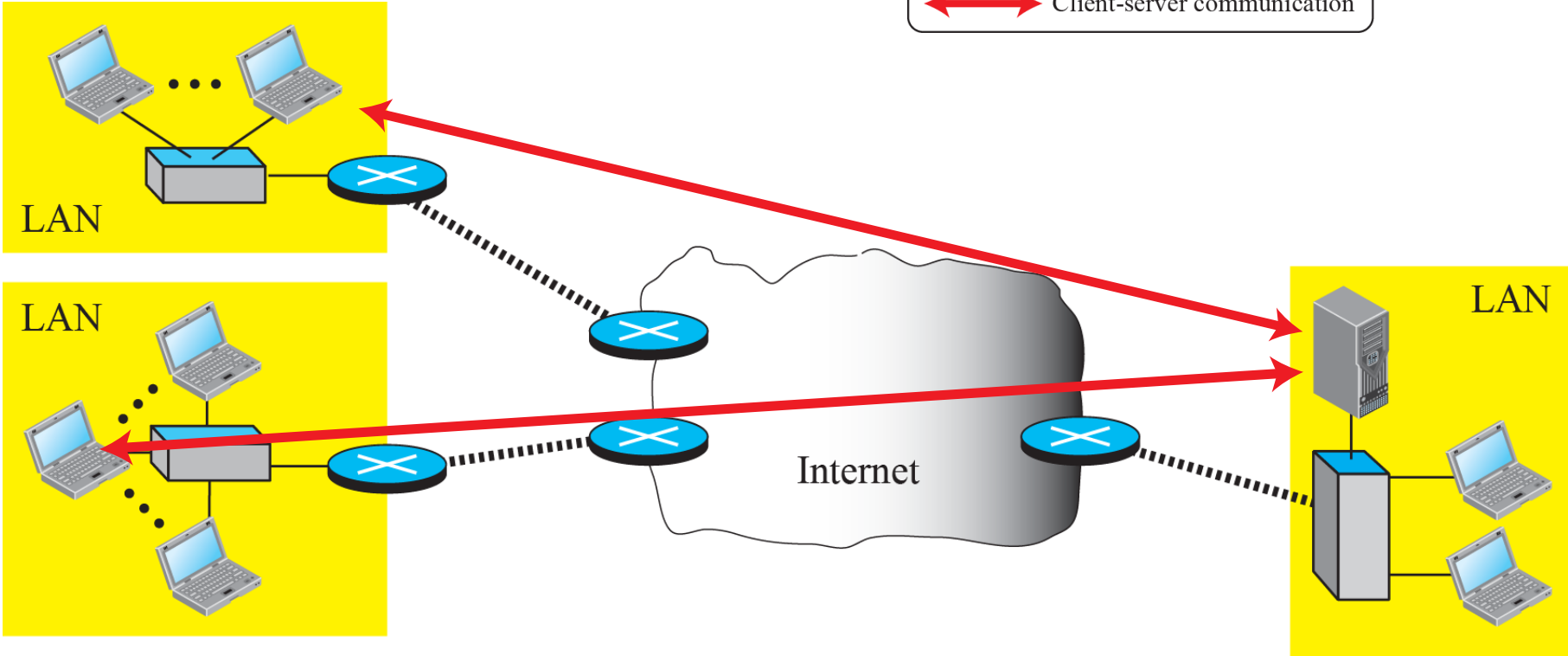
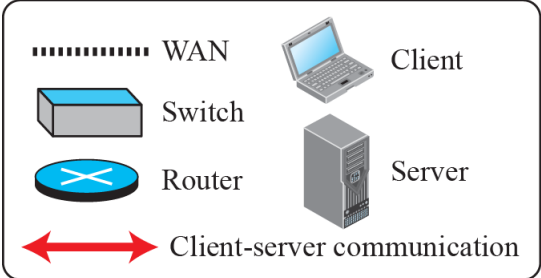
Användarmodeller för applikationer

Det finns två grundläggande användarmodeller för applikationer:

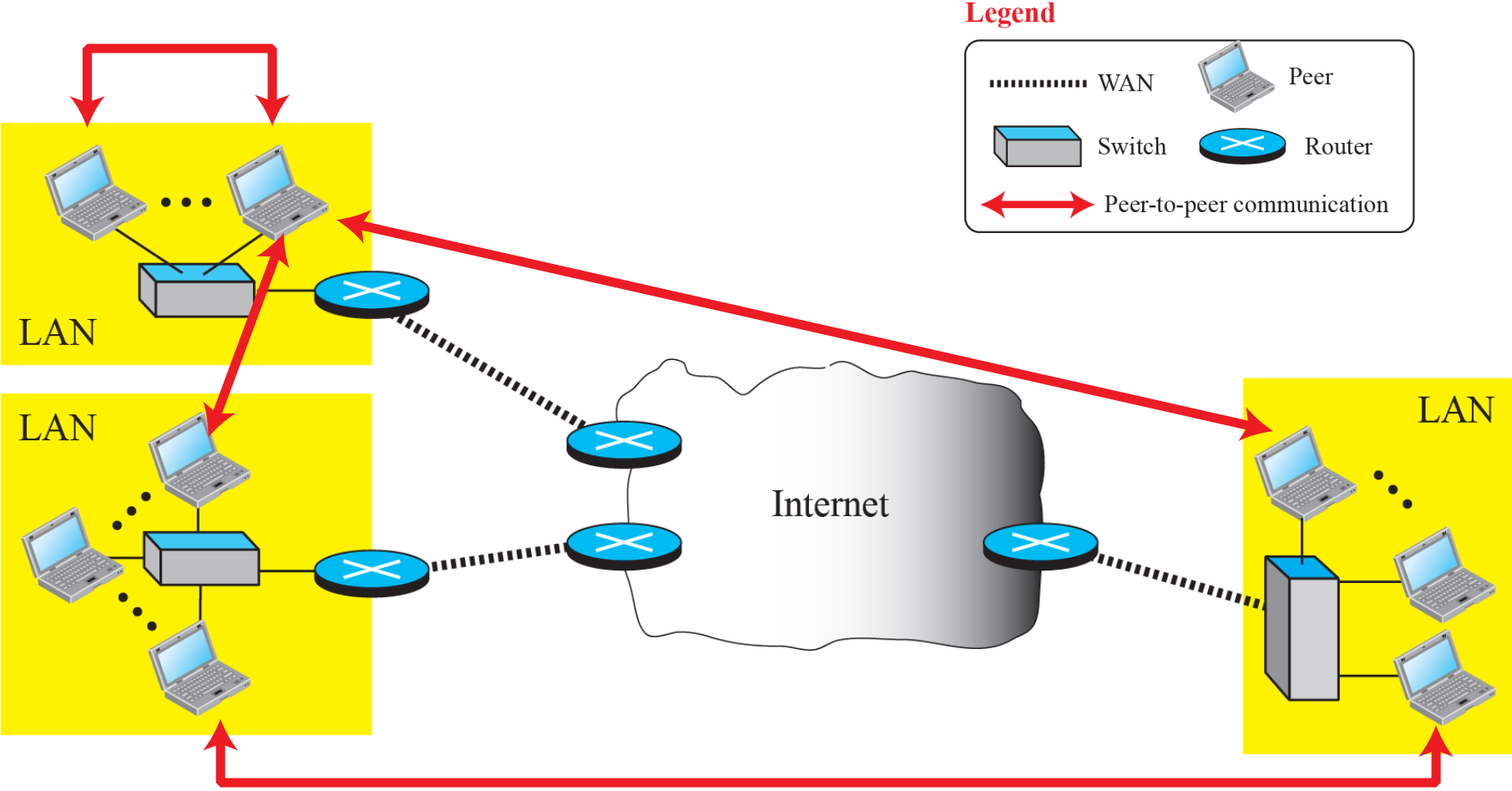
- Client-server modellen
 - Tex. WWW, Online-spel, Web TV, Facebook
- Peer-to-peer modellen
 - Tex. BitTorrent, Vodder, Skype
- En del applikationer använder en kombination av dessa modeller, tex Spotify.

Client-server modellen

Legend



Peer-to-peer (P2P)-modellen

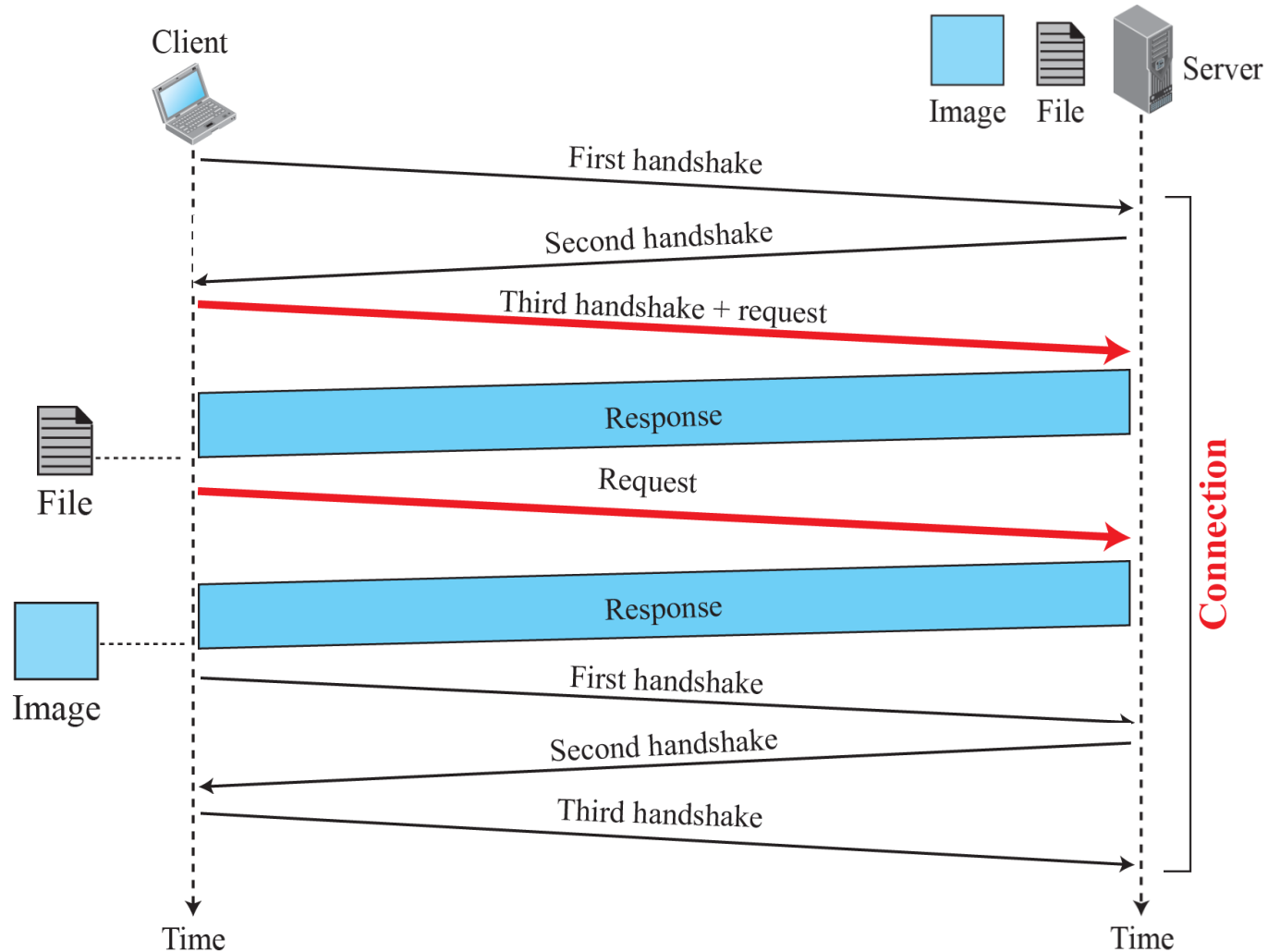


World Wide Web (WWW)

WWW består av tre delar:

- Webbssidor (web pages)
 - HyperTextMarkup Language (HTML) används för statiska webbsidor
 - Dynamiska webbsidor skapas med något scriptspråk (JSP, CGI, ASP, etc.)
- Universal Resource Locator (URL)
 - Standard för att namnge webbsidor.
- HyperText Transfer Protocol (HTTP)
 - Applikationsprotokoll för att hämta webbsidor från en webbserver.

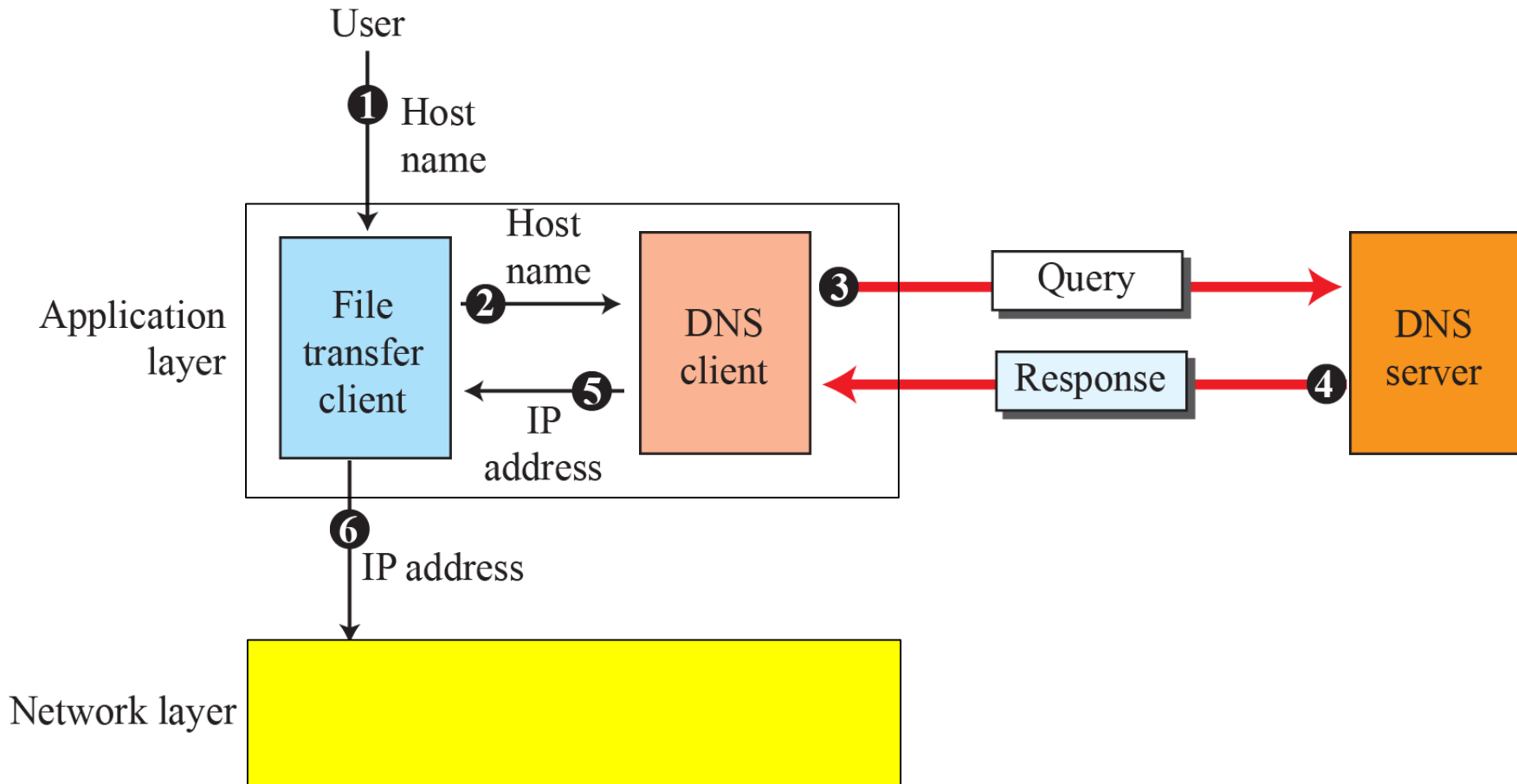
HTTP använder en TCP-förbindelse



Från host-namn till IP-adress

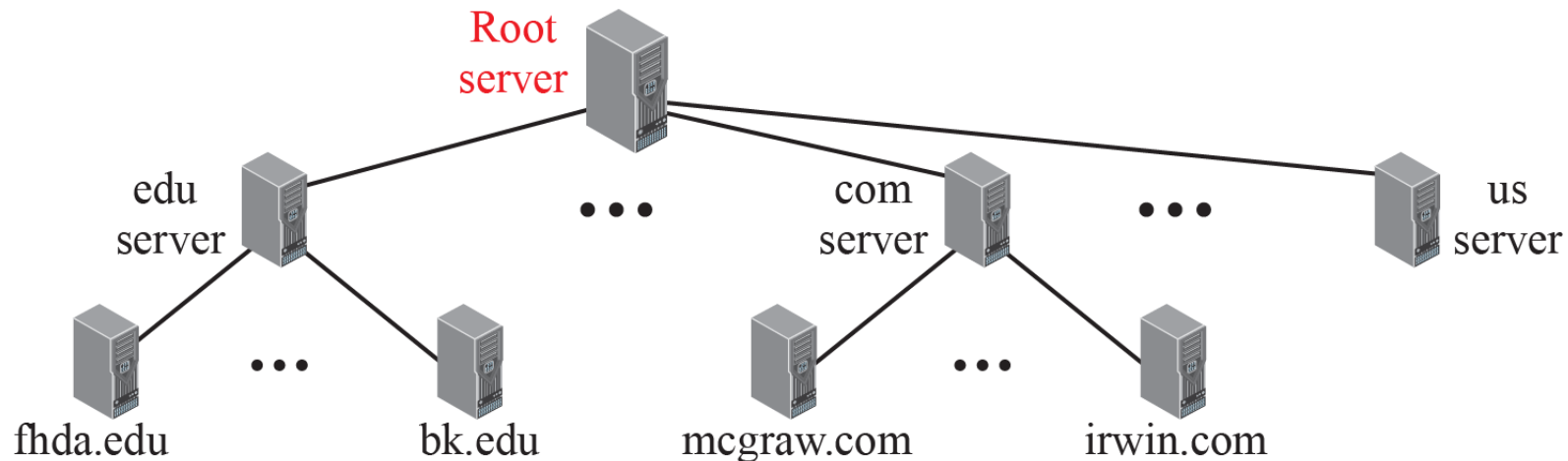
- Applikationsprotokoll, tex HTTP, använder host-namn (tex. www.lth.se).
- Men, TCP/IP använder IP-adresser.
- **Domain Name System (DNS)** sköter mappningen från ett host-namn till en IP-adress.

DNS



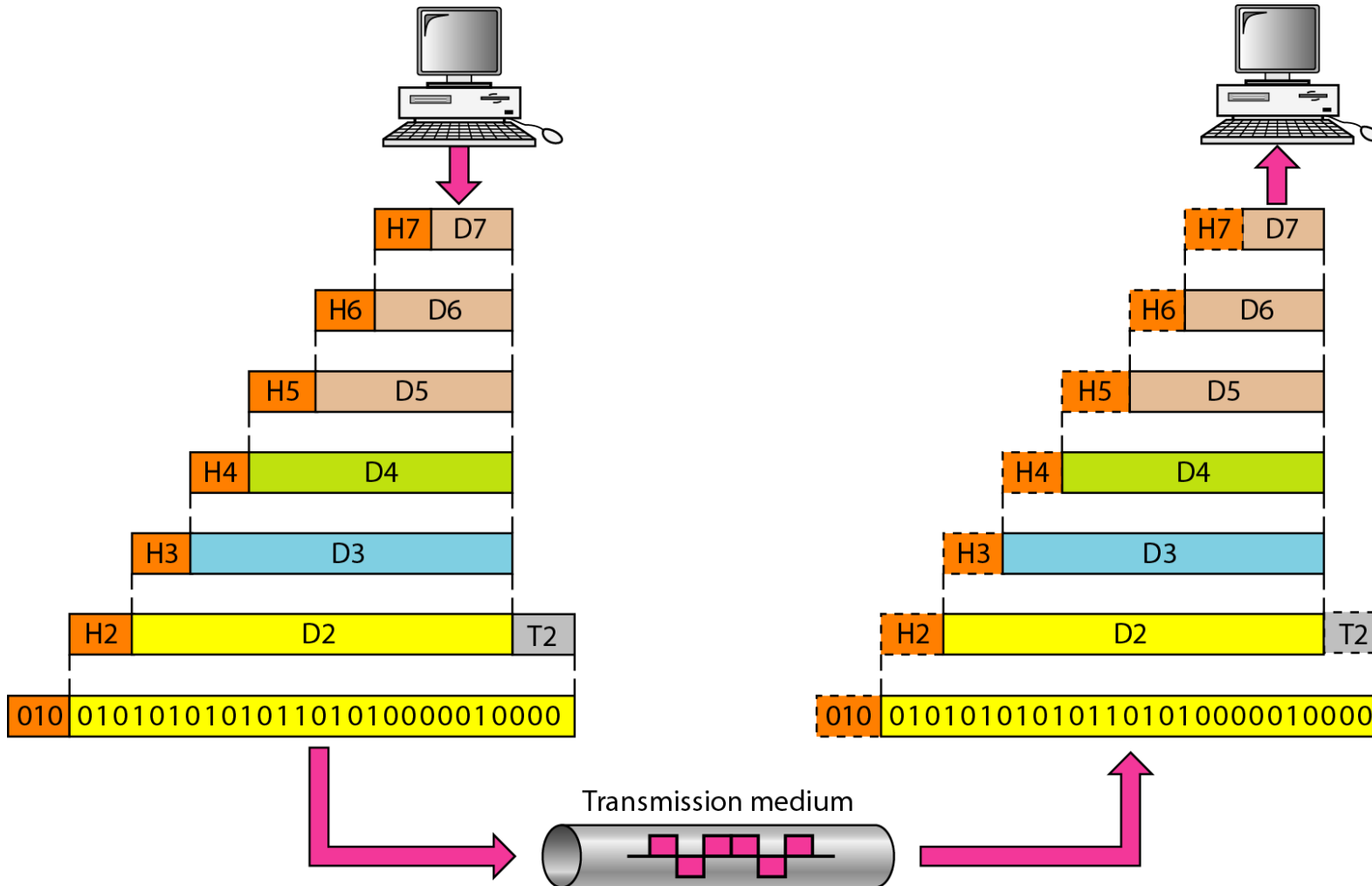
Domain Name Servrar

DNS servrar finns i alla domäner och de kommunicerar med varandra för att kunna mappa host-namn mot IP-adresser.



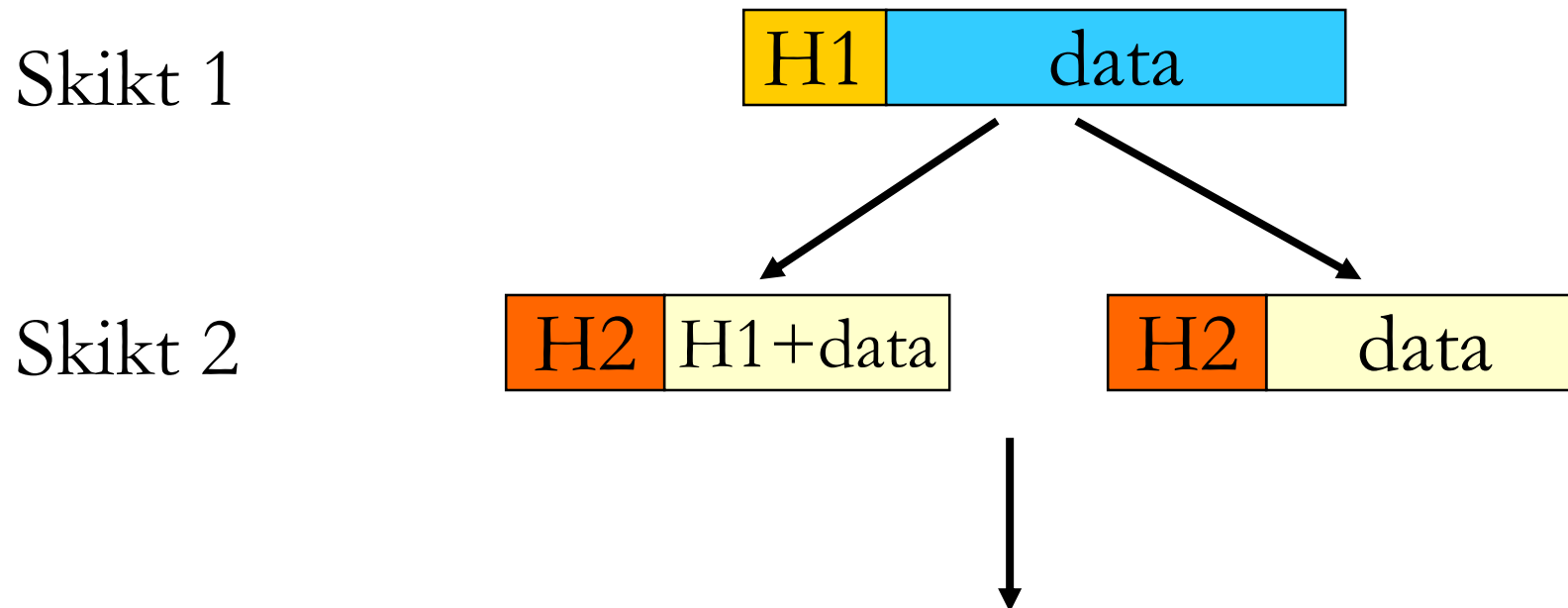
En host vet alltid IP-adressen till sin närmaste DNS-server.

Datakommunikation i flera skikt



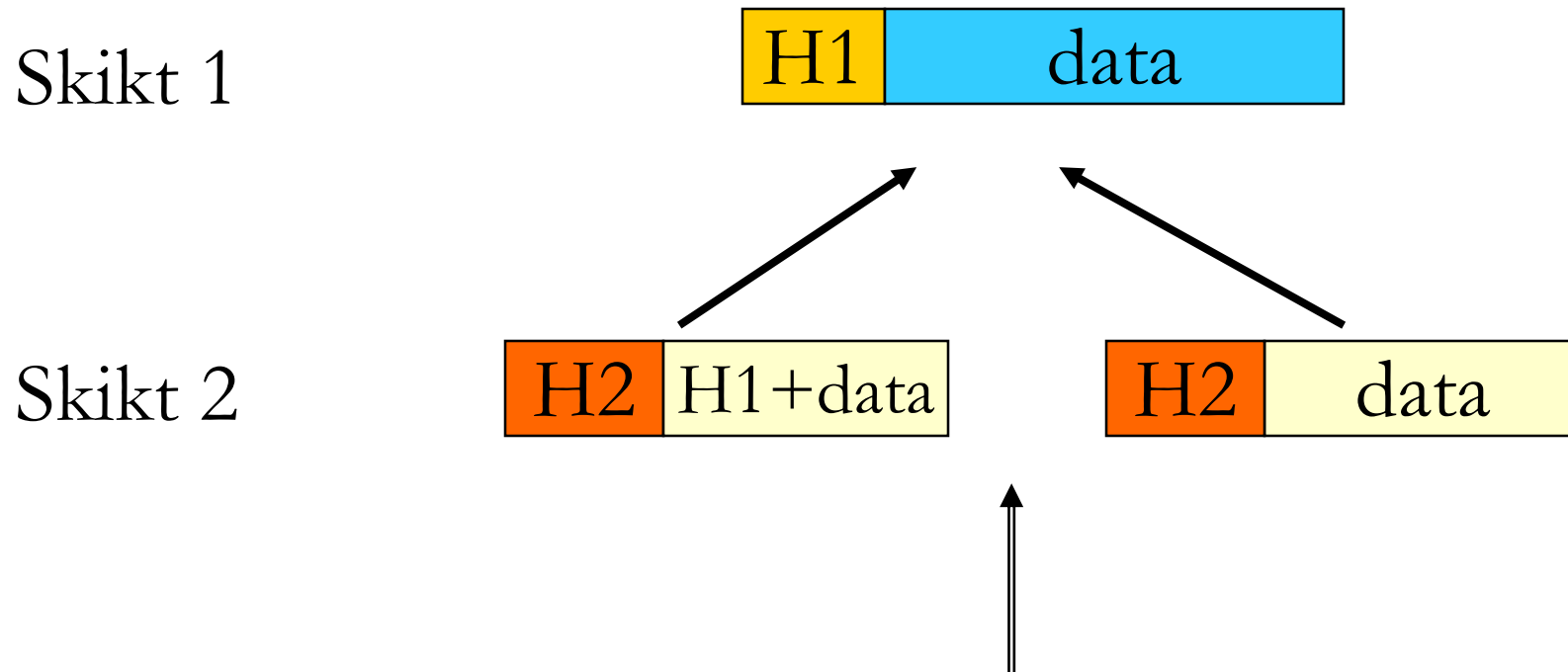
Fragmentering

Om det kommer data från ett övre skikt som inte får plats i ett enda datapaket sker så kallad **fragmentering** (enligt förutbestämda regler).



Hopsättning

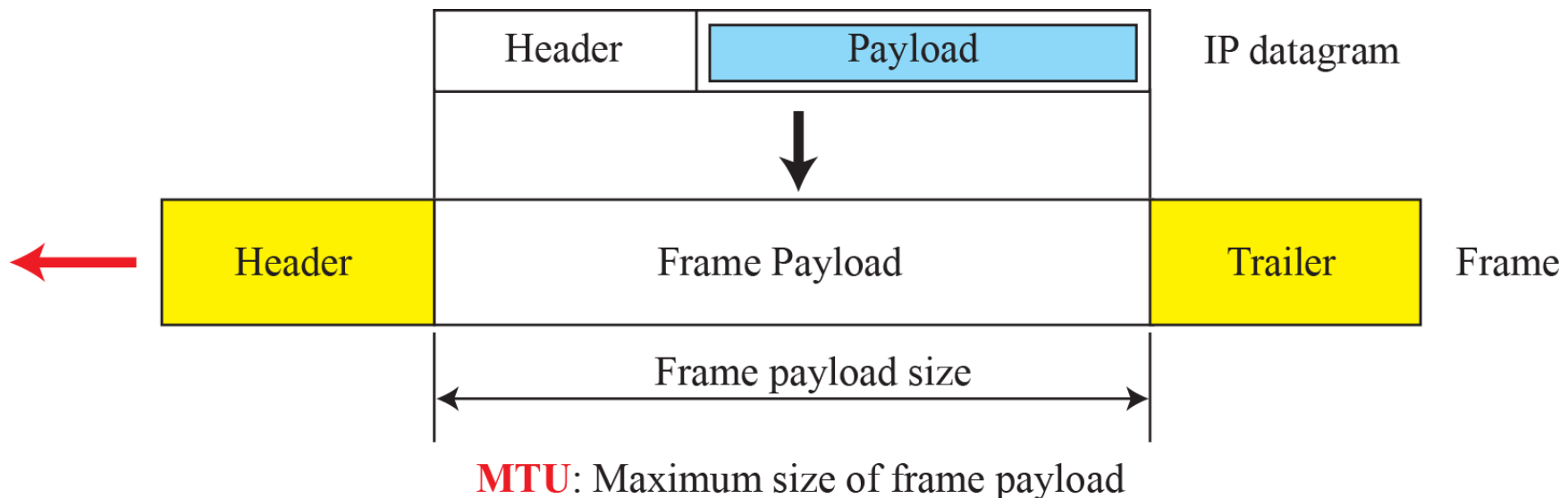
På mottagarsidan sätts datan ihop igen.



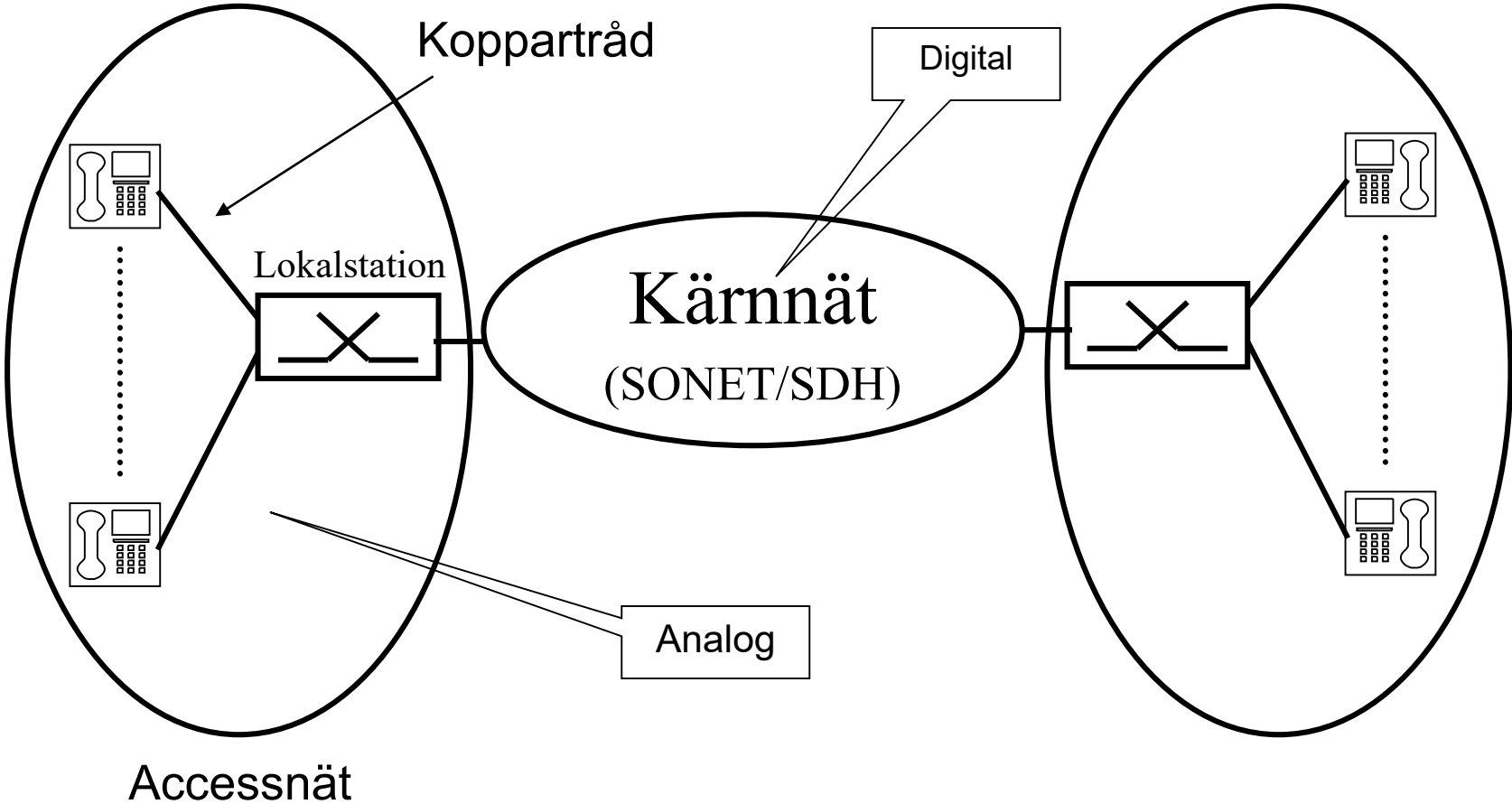
Maximum transfer unit (MTU)

Ett protokoll kan specificera en Maximum Transfer Unit (MTU) som sätter en maxlängd på den payload som kan skickas med protokollet.

Exempel:



Public Service Telephone Network (PSTN)



Dataöverföring i telenätet

- Accessnäten är analoga
 - Från telefonen till lokalstationen överförs talet analogt i frekvensområdet 0-4 kHz.
- Kärnnäten är digitala.
 - ◆ PCM i lokalstationerna
 - ◆ Dataöverföring med 8-bitars sampel.
 - ◆ Kretskoppling (circuit switching) med Synchronous Time Division Multiplexing (STDM).

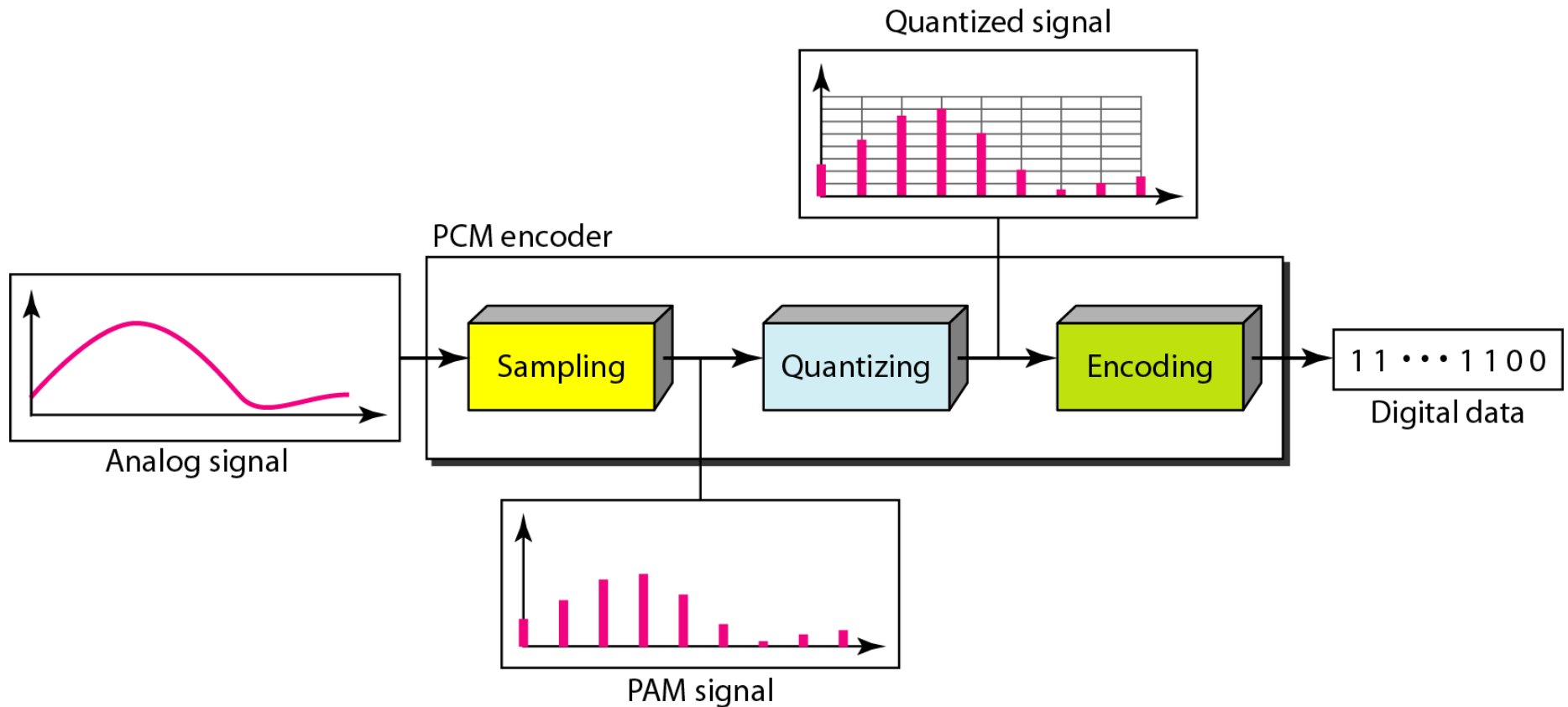
Digitalisering av ljud

Omvandling av ljud till binär data sker i tre steg:

1. Sampling
2. Kvantisering
3. Kodning

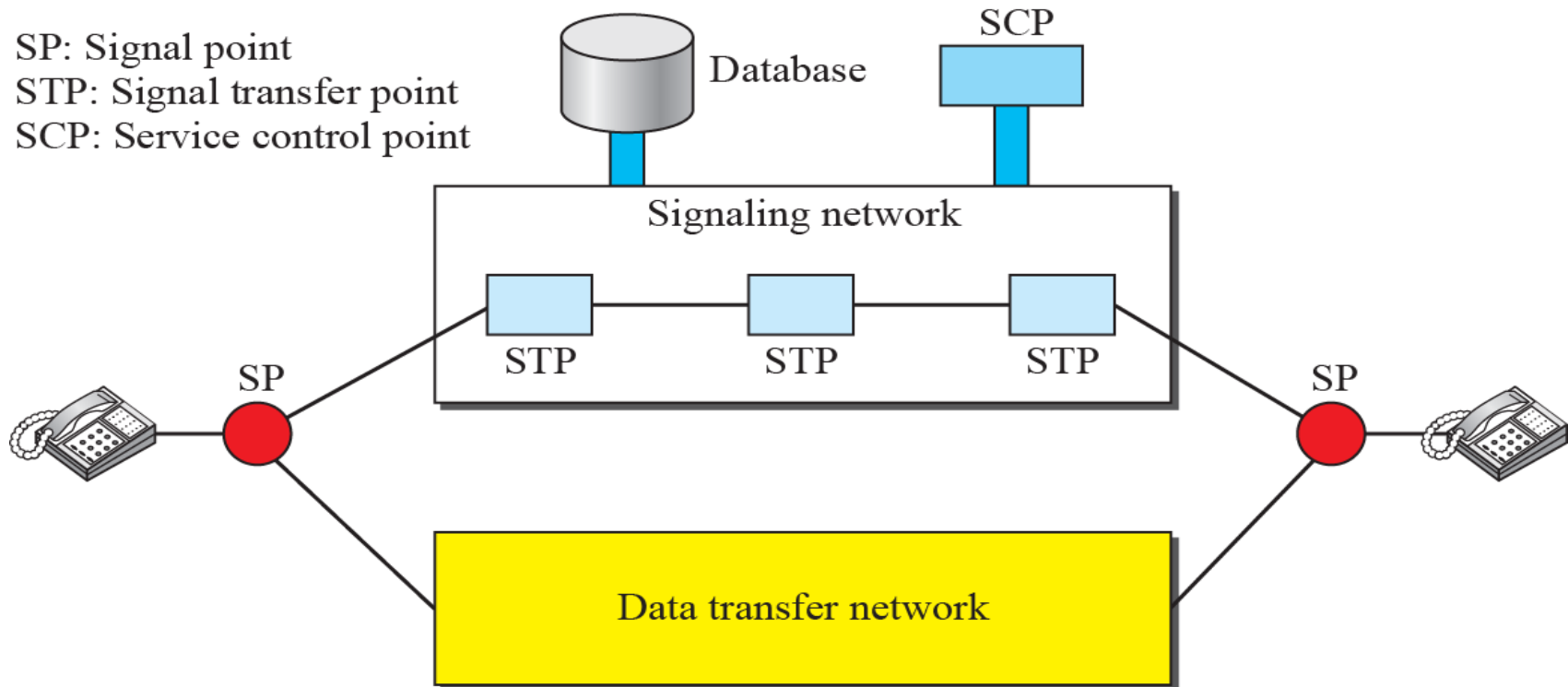
Detta kallas för **Pulse Code Modulation (PCM)**.

Pulse Code Modulation (PCM)



Protokollinformation

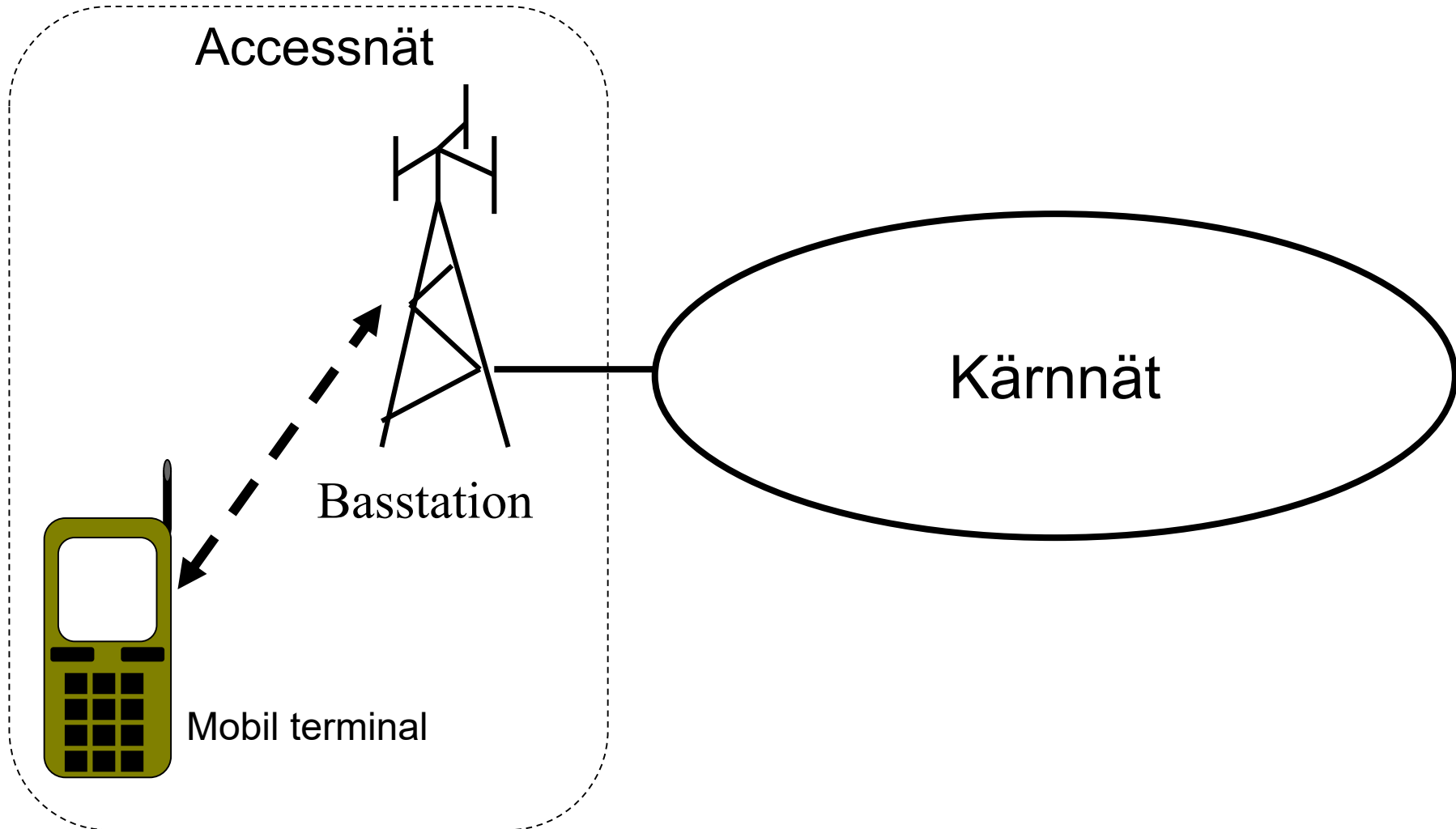
Telestationer övre hela världen kommunicerar med standardiserade protokoll (Signalling System #7) via ett separat datanät.



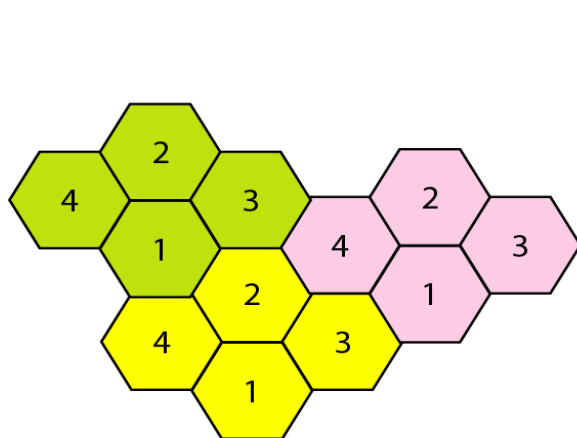
Jämförelse med Internet

- På Internet, skickas protokollinformation på samma nät som data.
 - Oftast som en del av headern i datapaketen.
 - Några speciella protokoll, tex ICMP, ARP, DNS
- I telenätet, är dataöverföringen separerad från överföringen av protokollinformation.
 - Medför fördröjningar för att sätta upp och ta ner förbindelser.
 - Väldigt effektiv dataöverföring med kretskoppling.

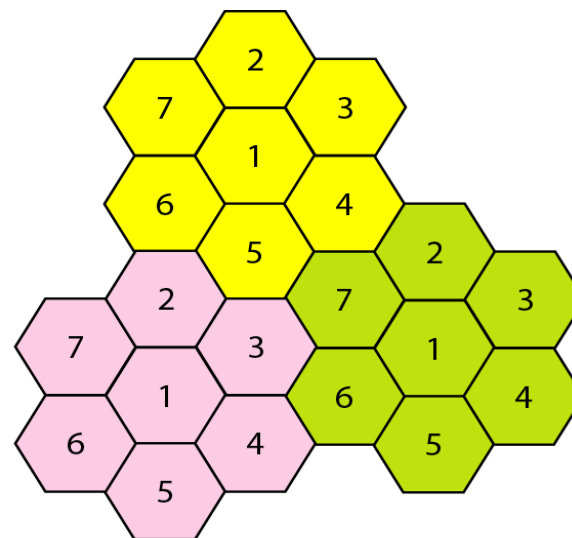
Cellulära nät (mobilnäten)



Celler och frekvenser



a. Reuse factor of 4



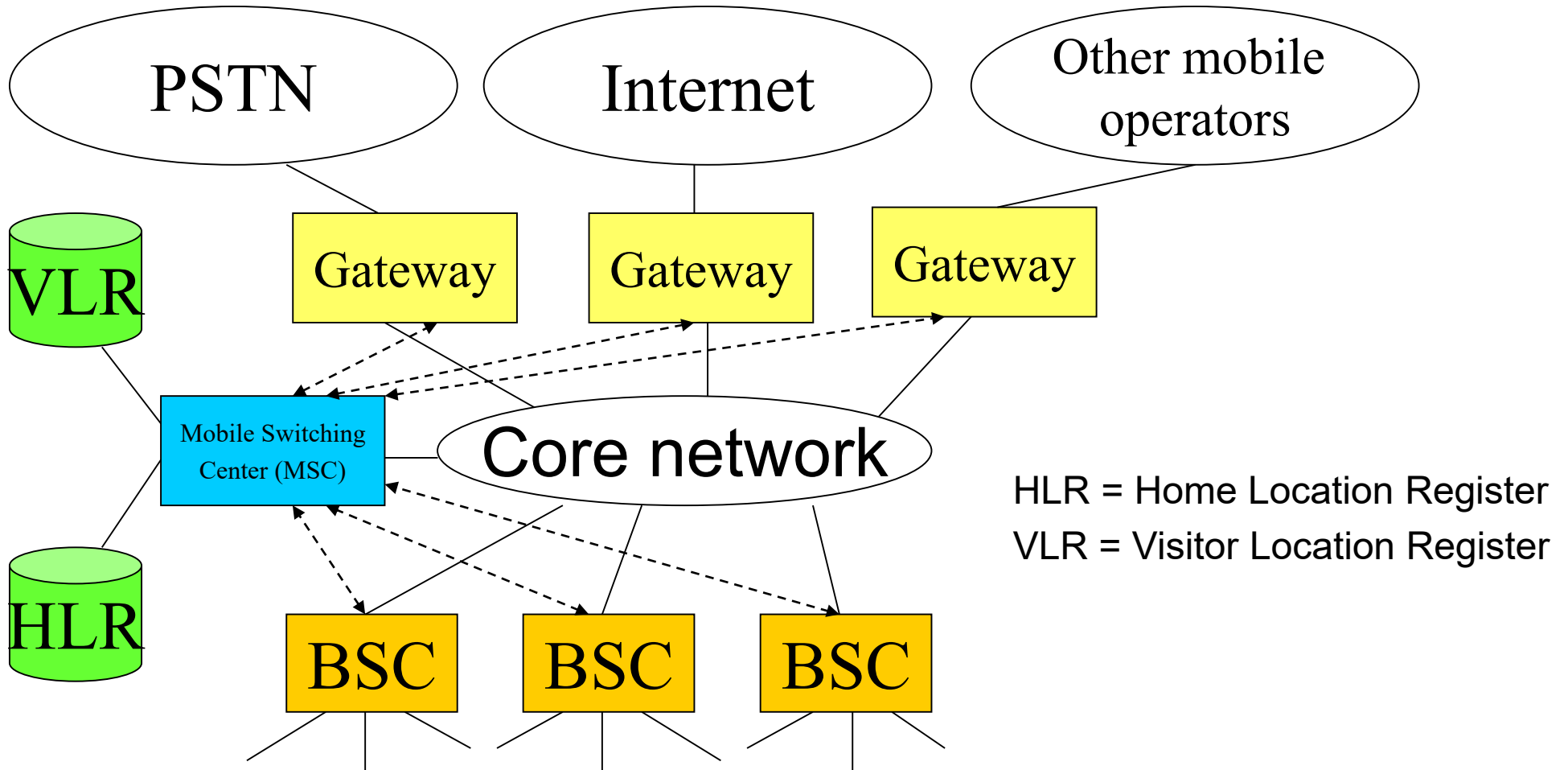
b. Reuse factor of 7

- Nätet är geografiskt indelat i celler.
- I varje cell finns det en basstation.
- Varje cell får ett visst frekvensband. Frekvensbanden återanvänds i andra celler enligt vissa mönster som ska minimera interferens.

Multipel access (channelization)

- Flera mobilterminaler måste dela på samma frekvensband i en cell.
 - Metoder för multipel access behövs.
- I mobilnäten används tre metoder (ofta kombinerat):
 - Frequency-Division Multiple Access (FDMA)
 - Time-Division Multiple Access (TDMA)
 - Code-Division Multiple Access (CDMA)
- All access i mobilnäten är ”Controlled”

GSM/UMTS kärnnät



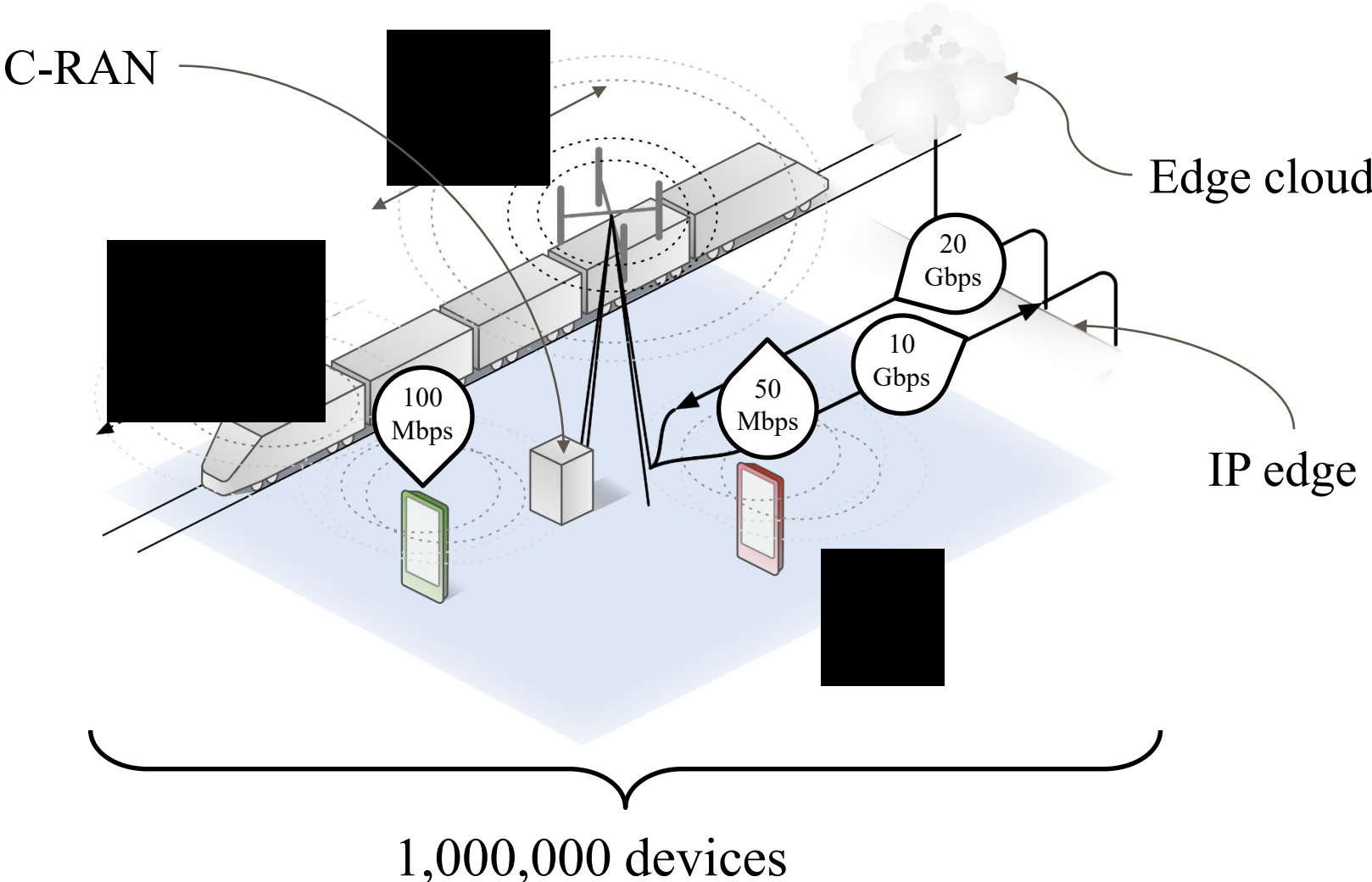
Long Term Evolution (LTE)

- 4:e generationen mobilnät
- Skillnader mot GSM/UMTS:
 - Paketförmiddlad kommunikation!
 - Utvecklat för Internet-access, inte telefoni!
 - Högre överföringskapacitet (såklart)
- Lösningar krävs för ”Voice over LTE”
- Högre bandbredd kräver mycket mindre celler än tidigare, så kallade **pico** och **femtoceller**.

Circuit-switched fallback

- Circuit-switched fallback används i de svenska LTE-näten och innebär att telesamtal kopplas via GSM/UMTS-nätet.
- Kräver kommunikation mellan LTE och GSM/UMTS

ITU: 5G wish list / Requirements



Det var allt för i år!

