Fortsättning på Internetprotokoll

Maria Kihl

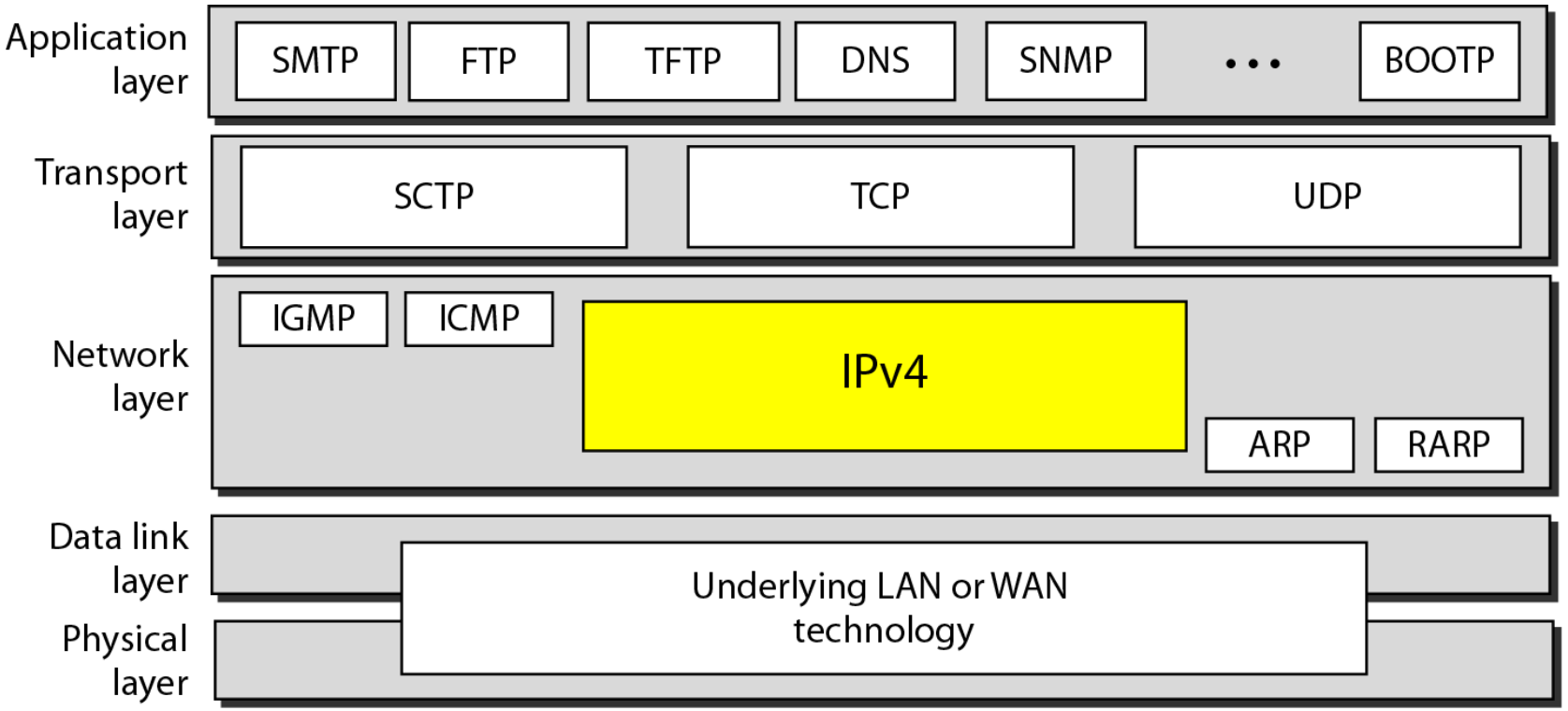
LUND
UNIVERSITY

Läsanvisningar

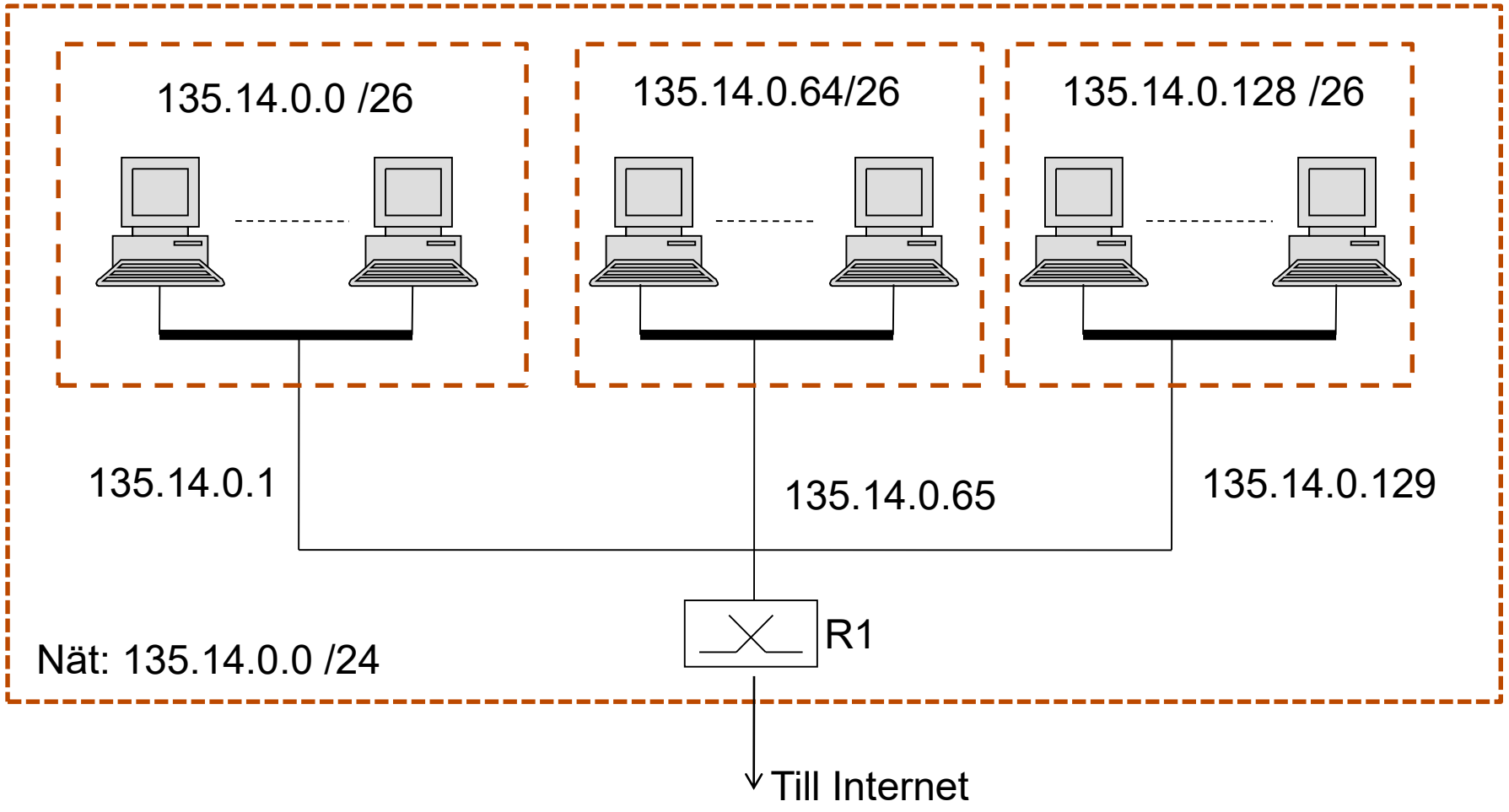
Kihl & Andersson: 7.7, 7.9, 11.1+ intros i 11.2-4, 12.1, 12.4, 17.1, 18.1 (endast ping och traceroute)

Stallings: 14.3 (ICMP), 24.2, 24.3,

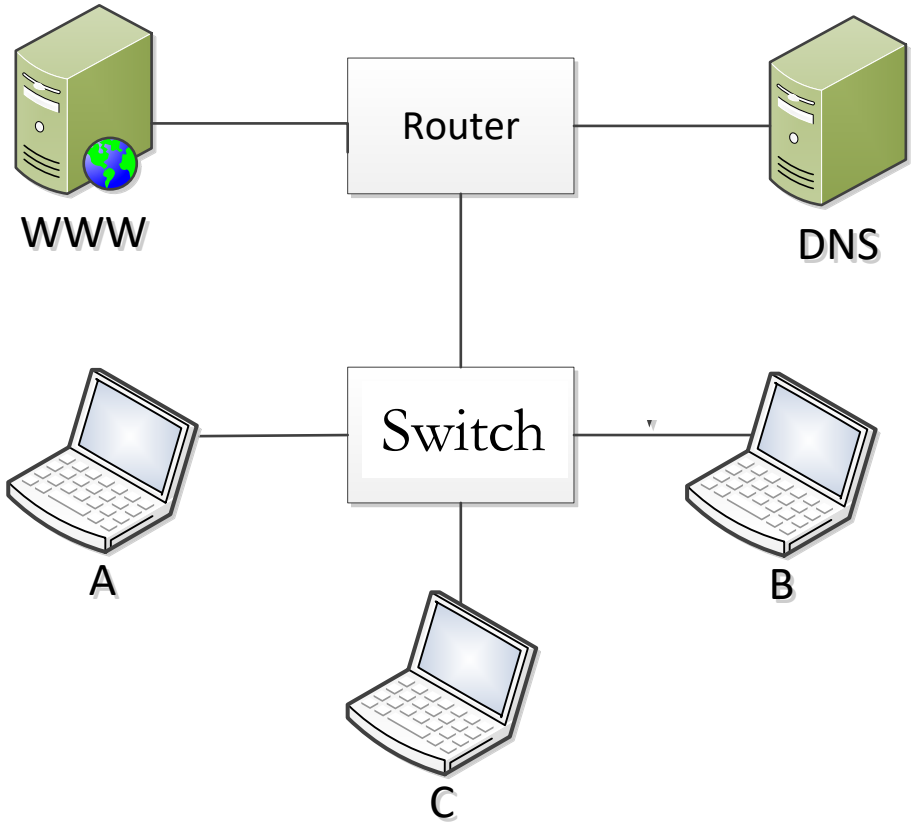
Internetprotokollen



Subnetting, exempel



Tentaexempel



Anta att A vill hämta en websida på WWW-servern och A känner endast till WWW-serverns symboliska namn. Antag att alla adress-cacher är tomma.

Beskriv vilka meddelanden som skickas i nätet!

Datasäkerhet

Det finns tre viktiga koncept vad det gäller datasäkerhet:

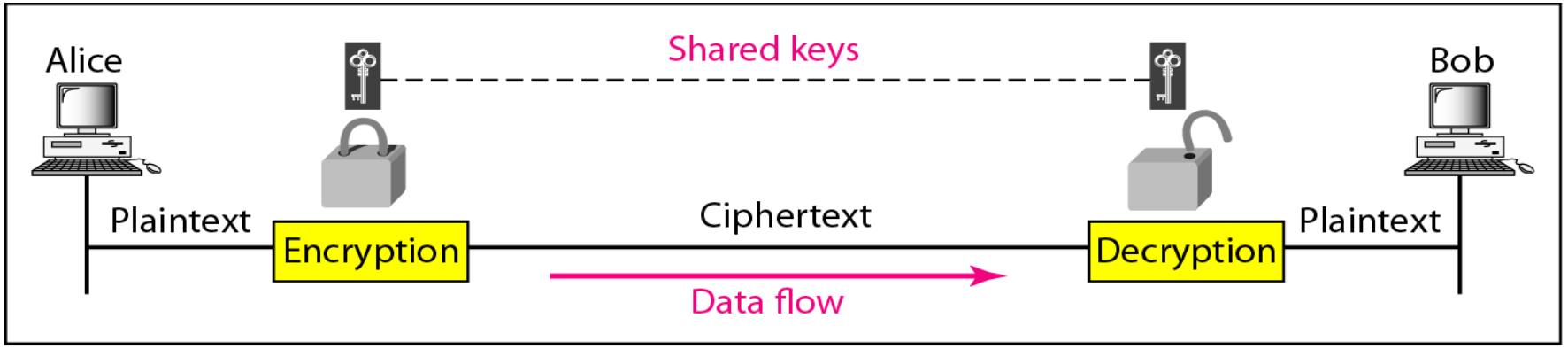
1. Skydd mot avlyssning (Privacy)
2. Skydd mot ändrad data (Integrity)
3. Autentisering (Authentication)

Skydd mot avlyssning (Privacy)

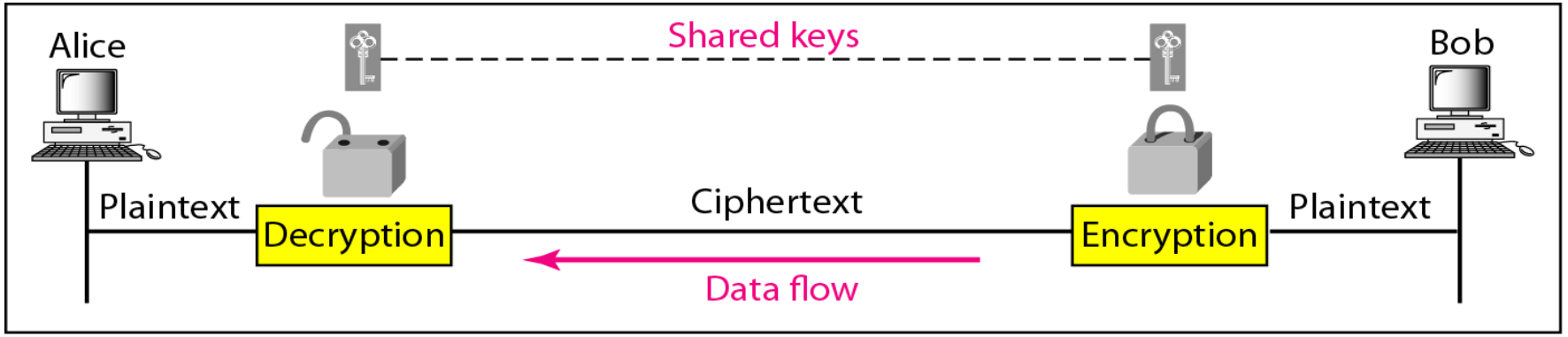
Skydd mot avlyssning (eller privacy) betyder att meddelandet som sänds endast ska kunna förstås av mottagaren. För alla andra ska meddelandet vara oförståeligt.

Privacy löses med kryptering av meddelandet.

Exempel på kryptering



a. A shared secret key can be used in Alice-Bob communication



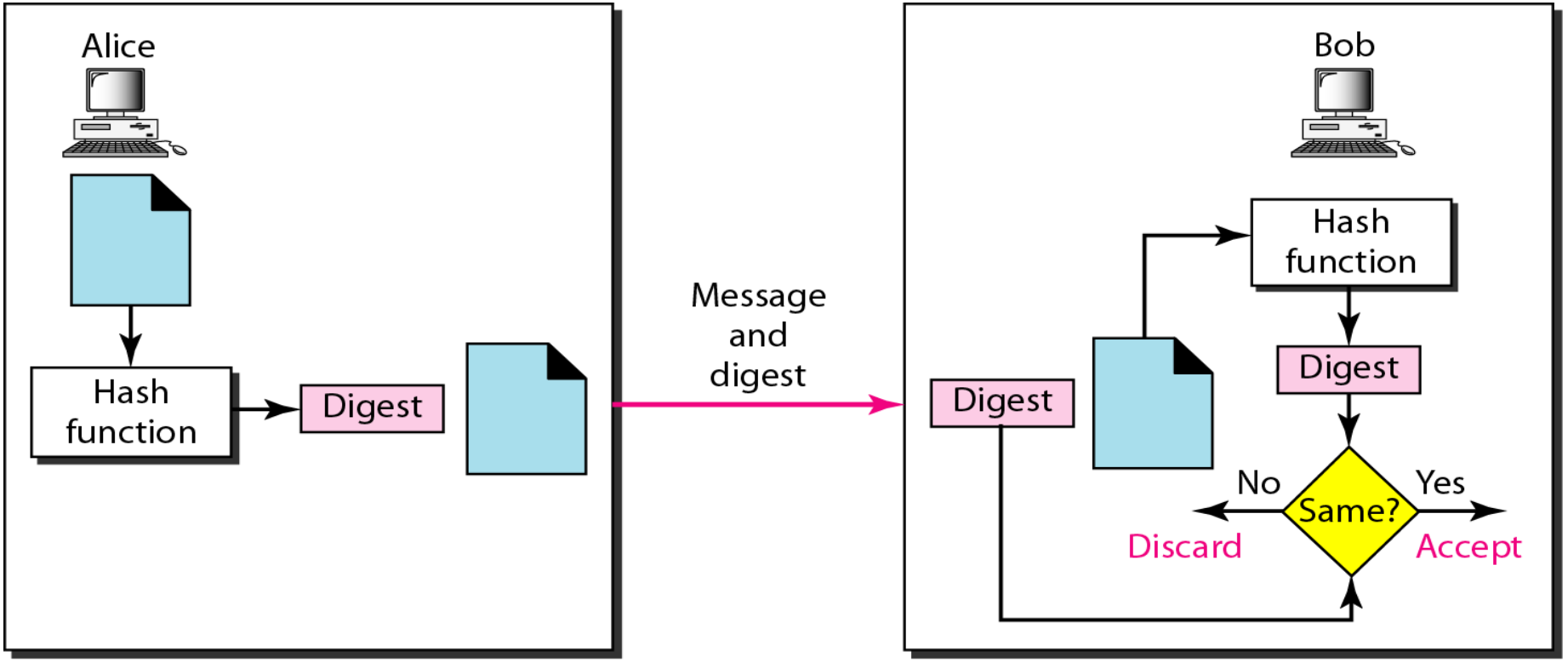
b. A different shared secret key is recommended in Bob-Alice communication

Skydd mot ändrad data (Integrity)

Skydd mot ändrad data (Integrity) betyder att meddelandet måste komma fram exakt så som det var sänt. Det får inte finnas några ändringar i meddelandet.

Integrity kan tillhandahållas med message digests.

Message digest

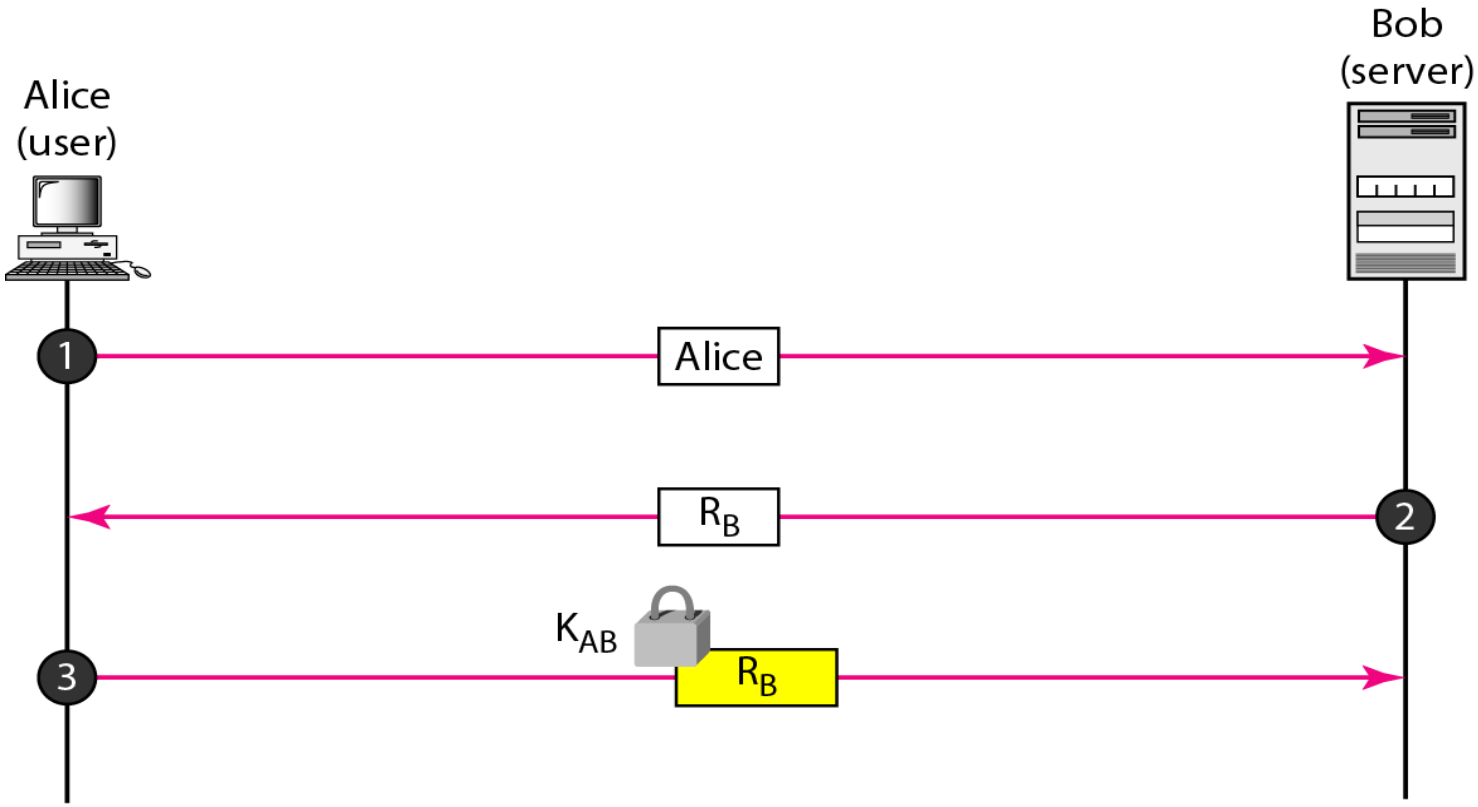


Autentisering (Authentication)

Autentisering (authentication) innebär att mottagaren måste vara säker på sändarens identitet.

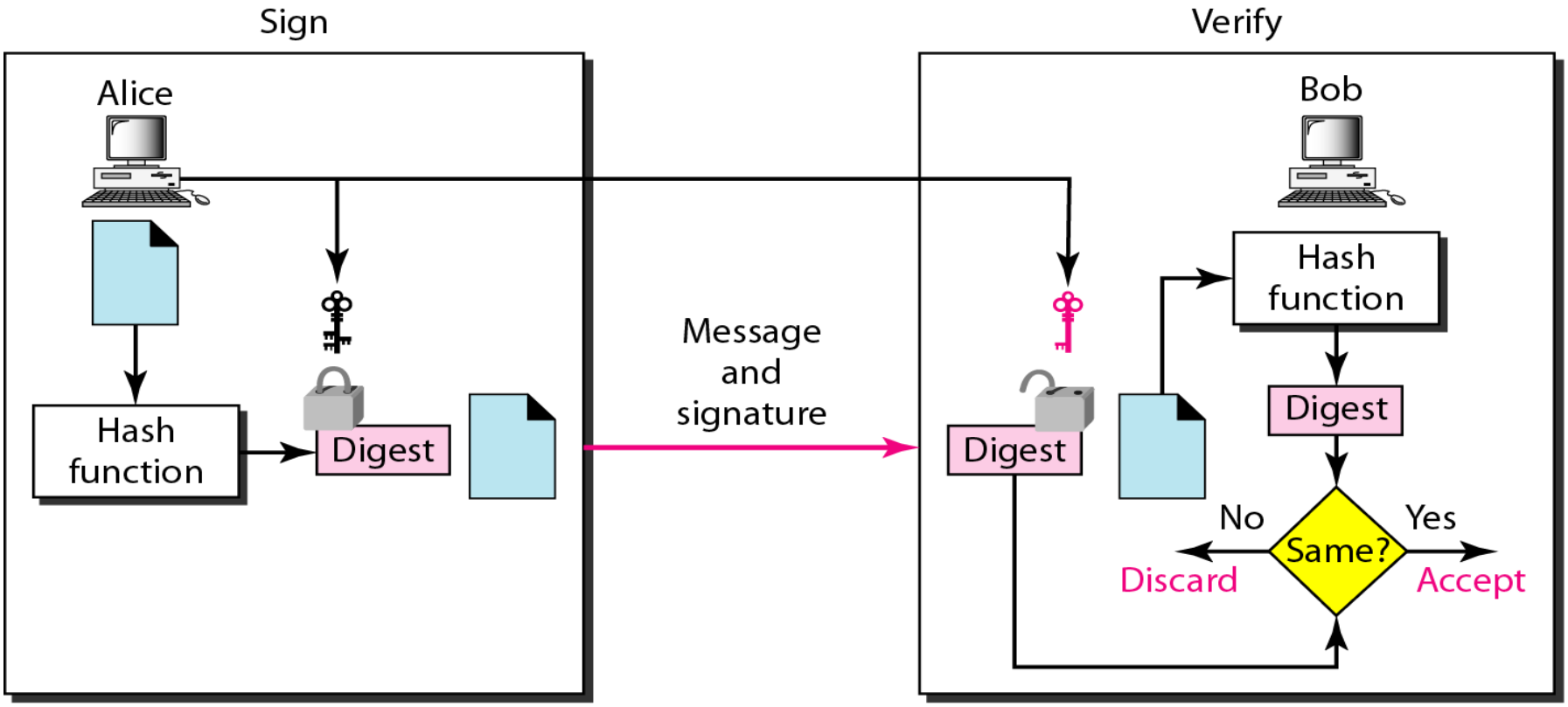
- Autentisering av enheter kan lösas med lösenord eller så kallad challenge-response.
- Autentisering av meddelanden kan tillhandahållas med en digital signatur. En digital signatur är en message digest som är krypterad.

Challenge-response



$\boxed{R_b}$ = Slumptal (Nonce)

Digital signatur



Internet security protokoll

Följande tre säkerhetsprotokoll tillhandahåller privacy, integrity och authentication på olika protokollskikt:

- IPSec: Säkerhetsprotokoll för IPv4.
- SSL/TLS: Säkerhetsprotokoll för TCP.
- PGP: Säkerhetsprotokoll för Email (SMTP).
- HTTPS: Hypertext Transfer Protocol Secure. Använder sig av TLS/SSL

Dessa protokoll kommer att gås igenom i fortsättningskursen Internetprotokoll. För er som går EITF25 så blir det även en föreläsning i webbsäkerhet.

Applikation: WWW

- World Wide Web (WWW) presenterades av Tim Berners-Lee 1989 vid CERN. Syftet med WWW var att möjliggöra för forskare att dela information på ett enkelt sätt.
- Det mer kommersiella WWW startades under tidigt 1990-talet med Netscape och Mosaic.
- Aftonbladet.se startades 1994 som den första stora nättidningen i Sverige.

Grundläggande koncept för WWW

WWW bygger på tre delar:

- Webbsidor
  - HyperTextMarkup Language (HTML) används för statiska webbsidor.
  - Dynamiska webbsidor skapas med script (JSP, CGI, ASP, etc.)
- Universal Resource Locator (URL)
  - Standard för hur man identifierar på vilken webbserver en webbsida ligger.
- HyperText Transfer Protocol (HTTP)
  - Protokoll för att hämta webbsidor från en webbserver.

Universal Resource Locator (URL)

Ett webbdokument har fyra identifierare: Protokoll, Host, Port och Path. En URL är definierad som:

protocol://host:port/path

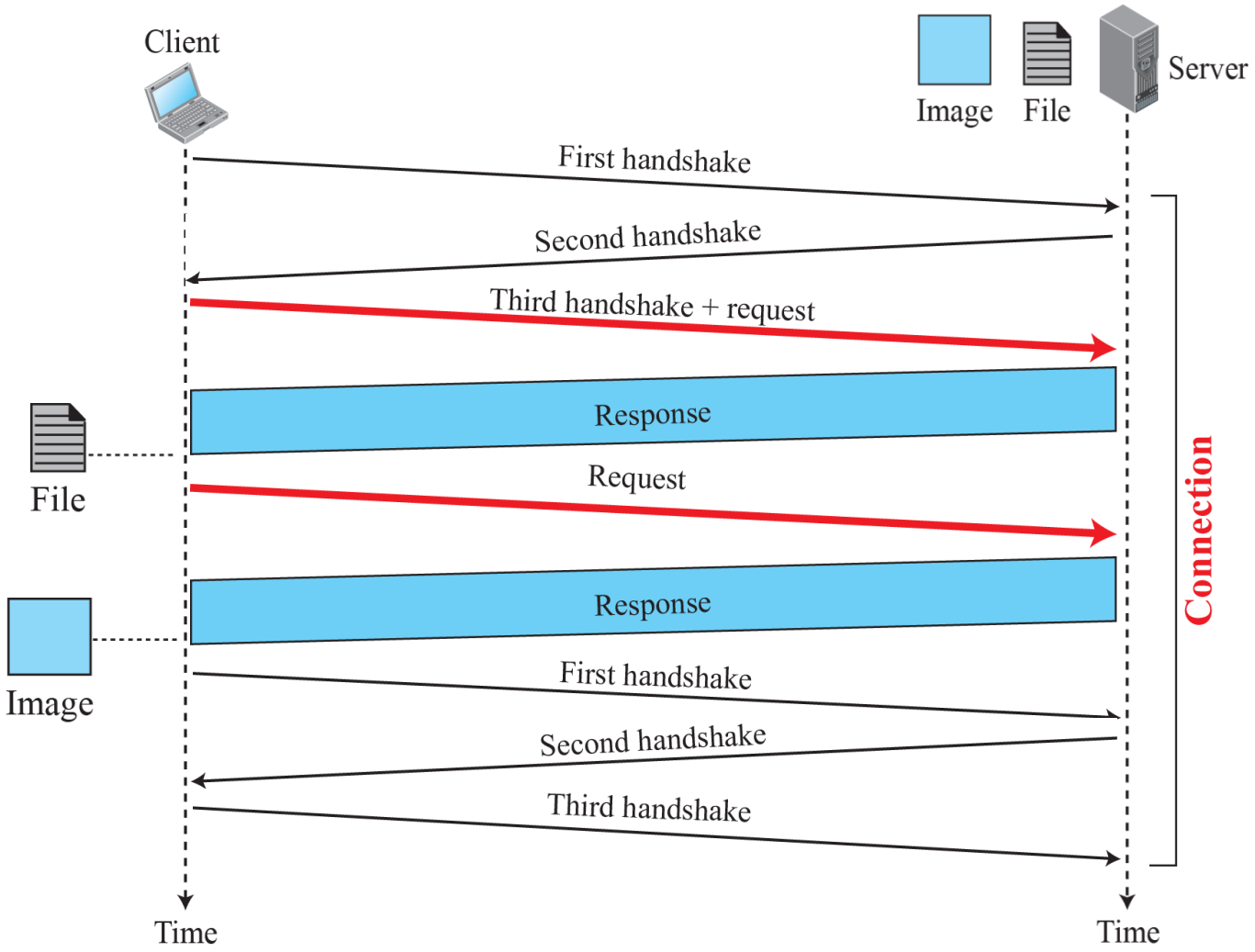
När HTTPs standardport 80 används är den utesluten ur formuleringen ovan, till exempel:

http://www.eit.lth.se/staff/maria.kihl

HTTP

- HTTP är ett textbaserat client/server protokoll med två typer av meddelanden: **Request** och **Response**.
- HTTP använder en TCP förbindelse för kommunikationen mellan klient och server.

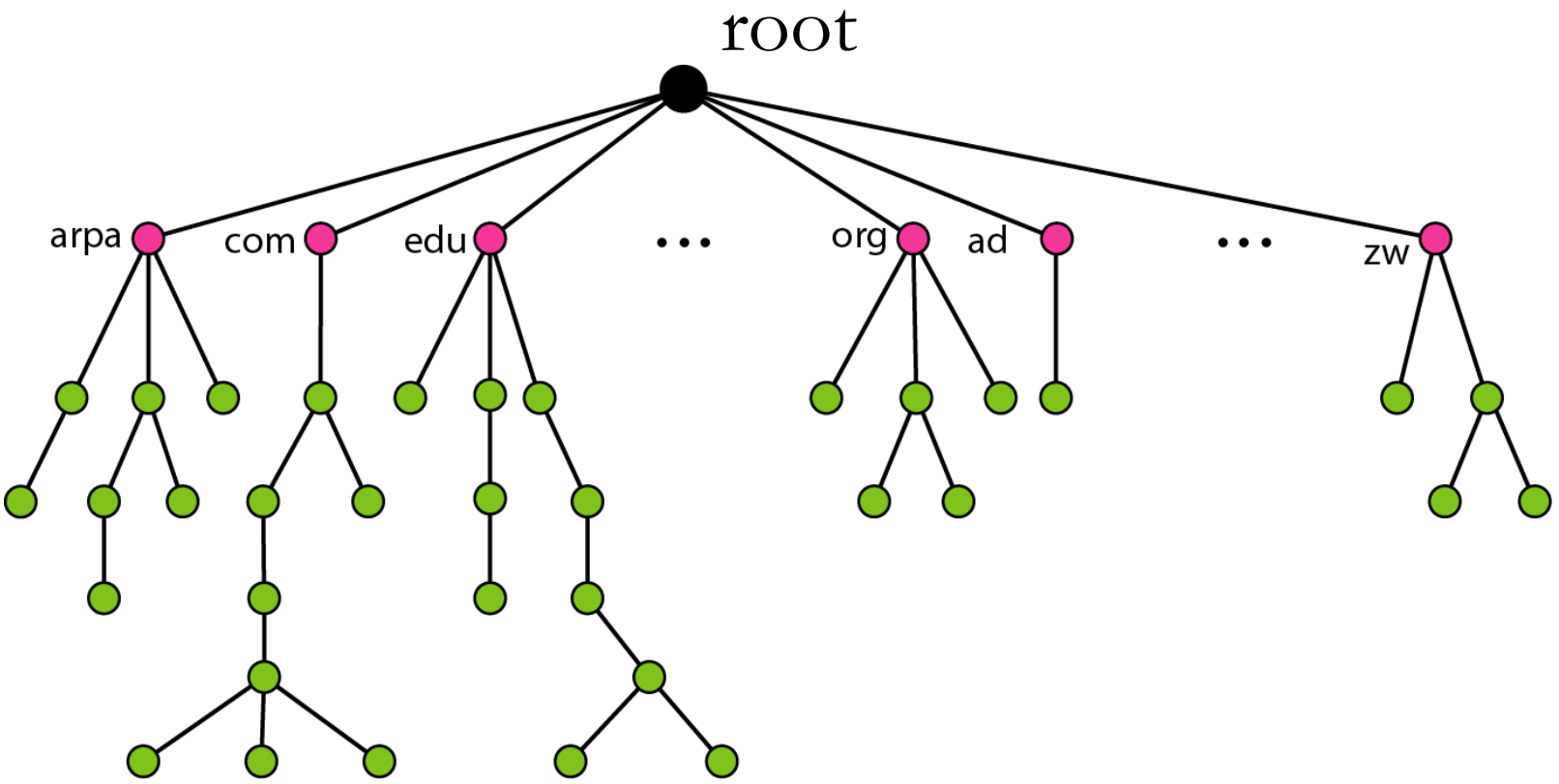
HTTP kommunikation



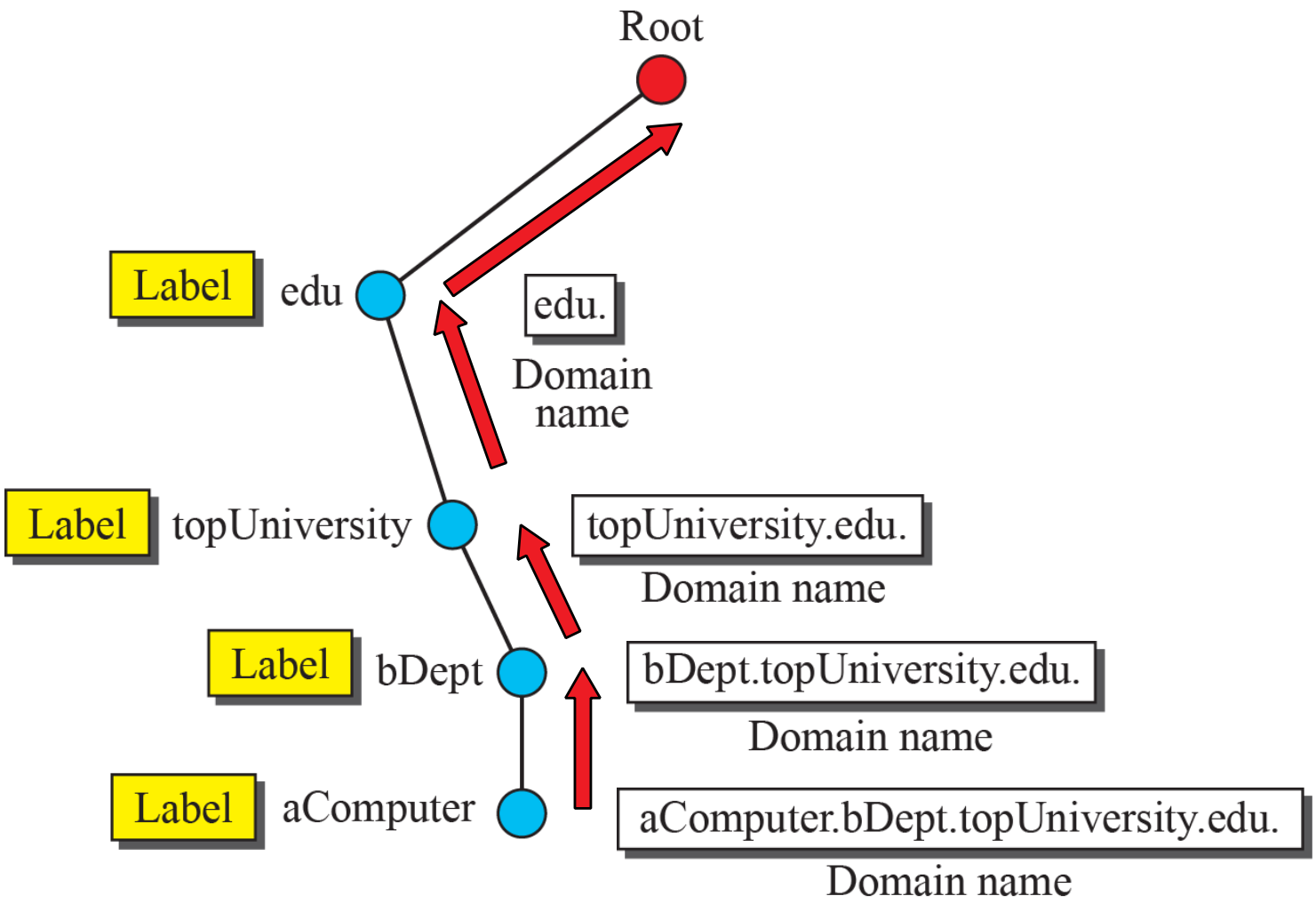
Mappning från URL till IP-adress

- Applikationsprotokoll använder symboliska namn (tex. www.lth.se).
- Mappning från symboliskt namn till IP-adress görs med Domain Name System (DNS).

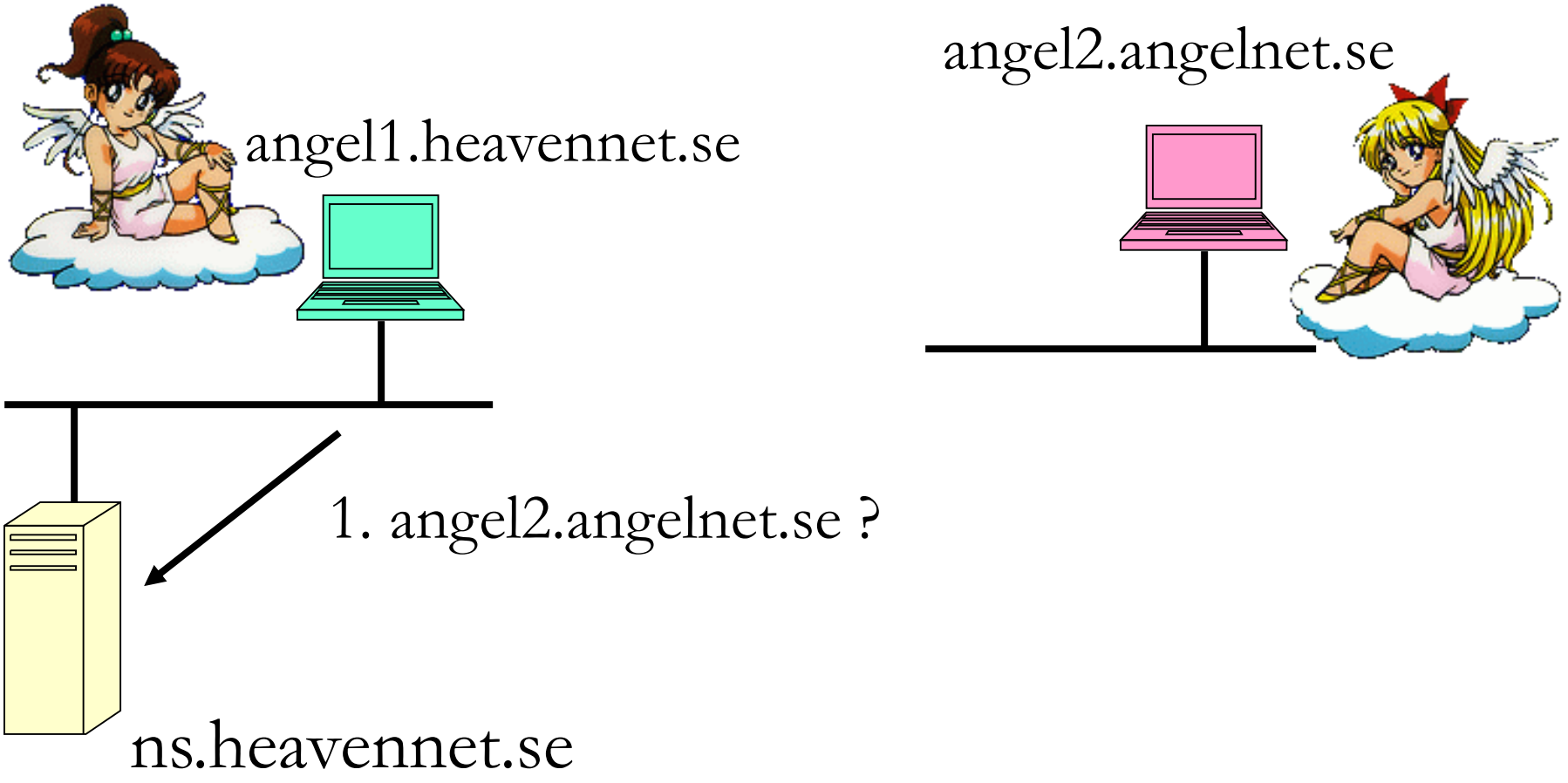
Domän-namn i DNS



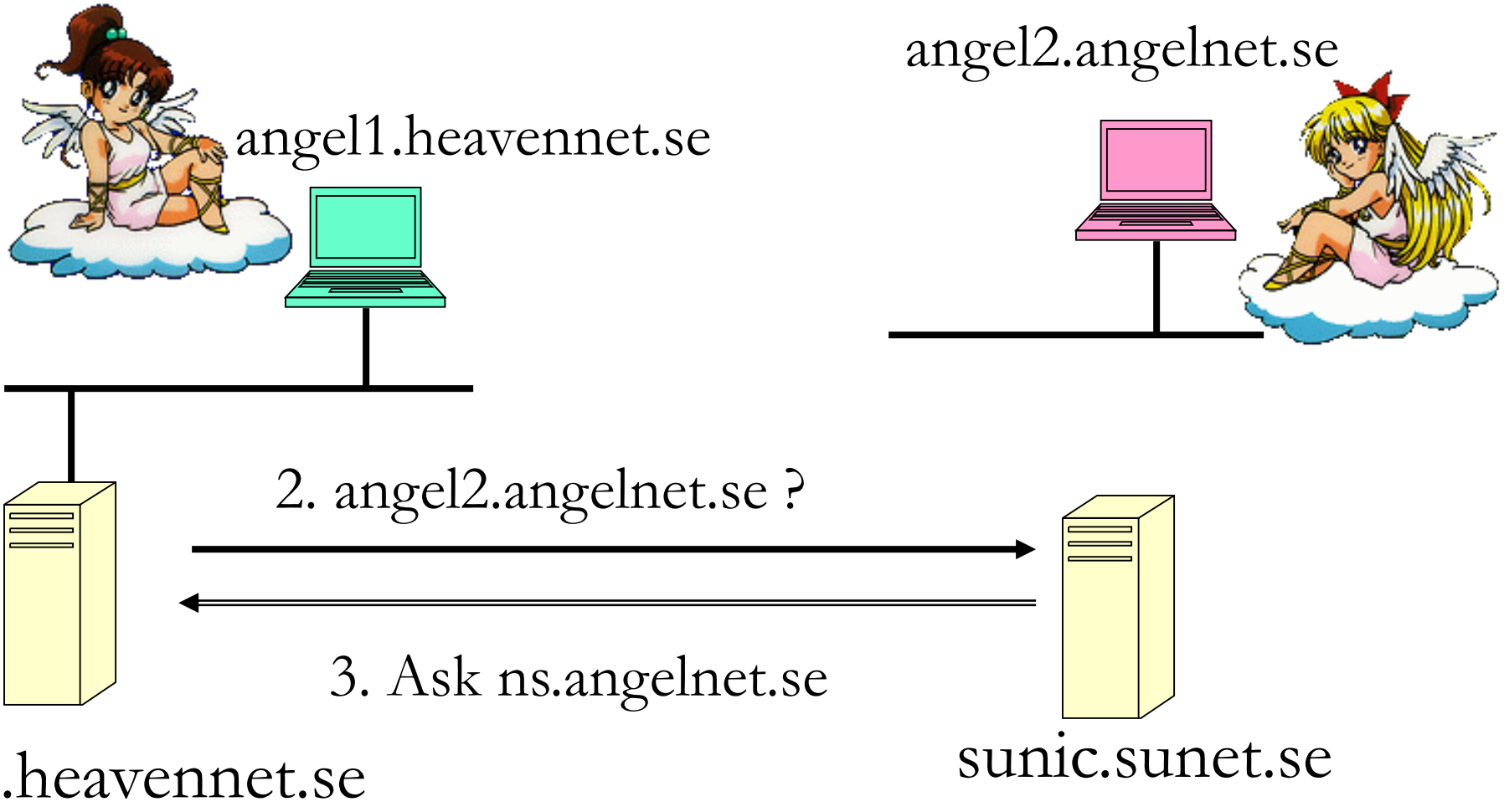
Hierarkisk namn-struktur



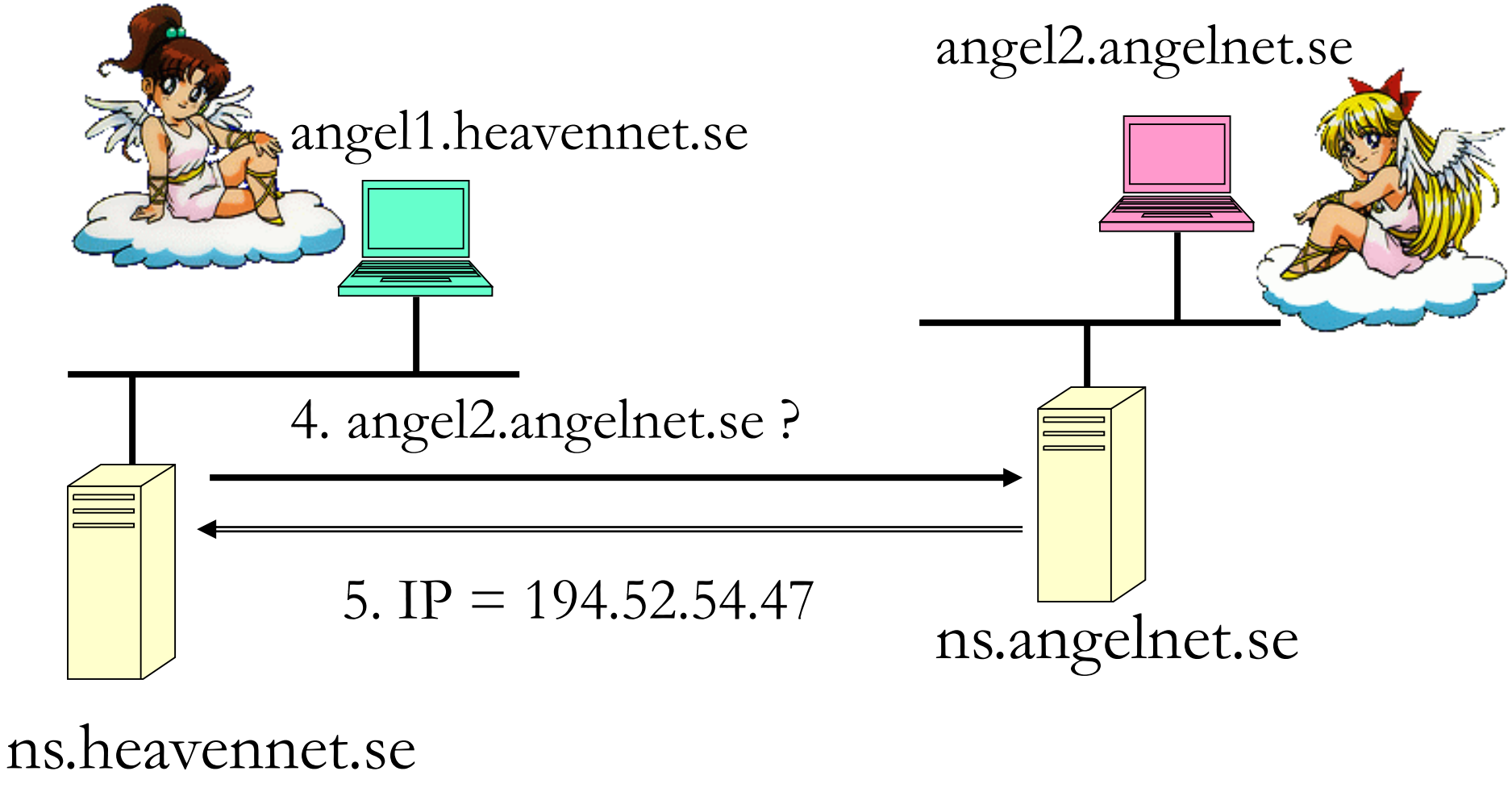
Från namn till adress (1)



Från namn till adress (2)



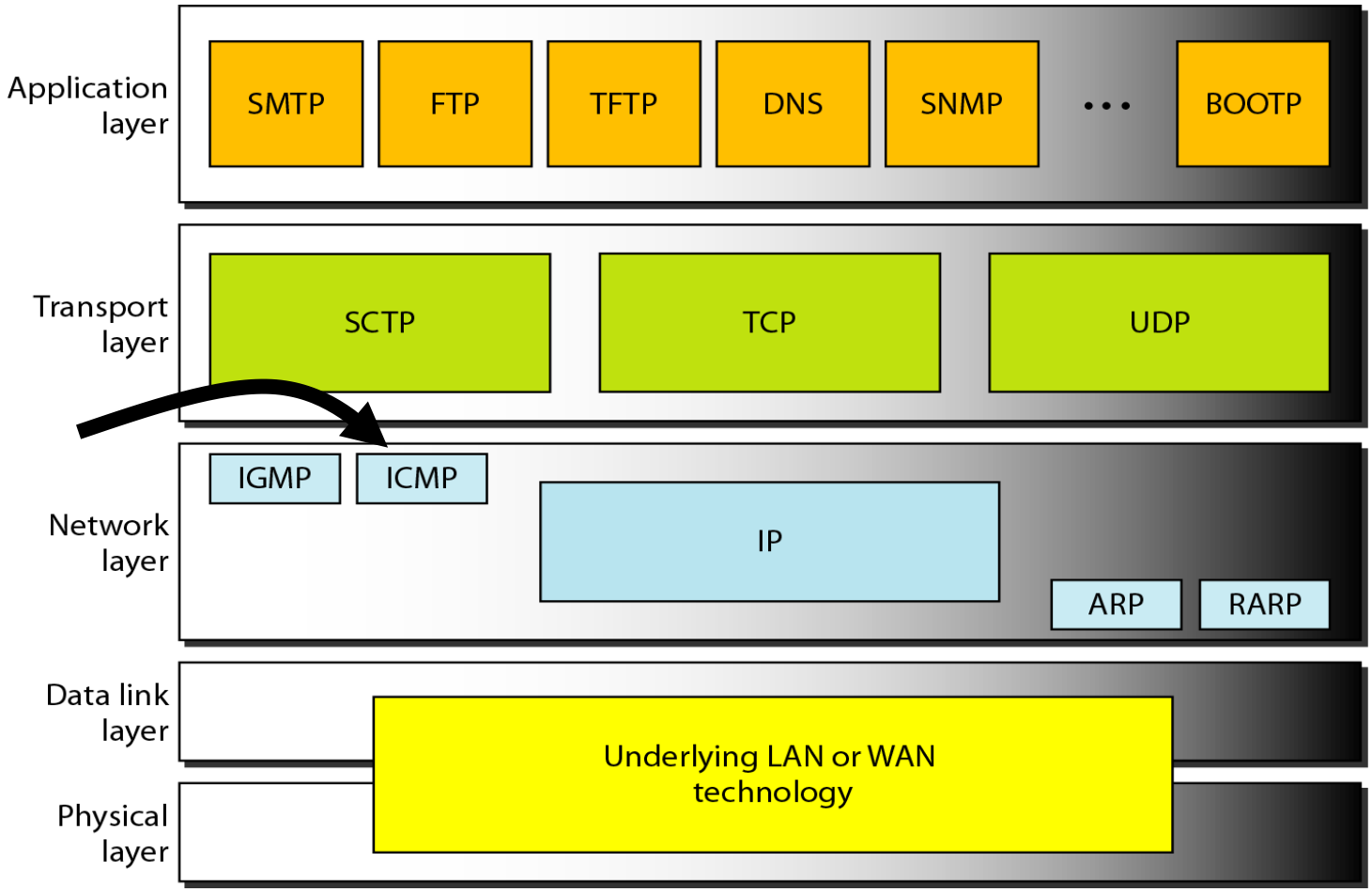
Från namn till adress (3)



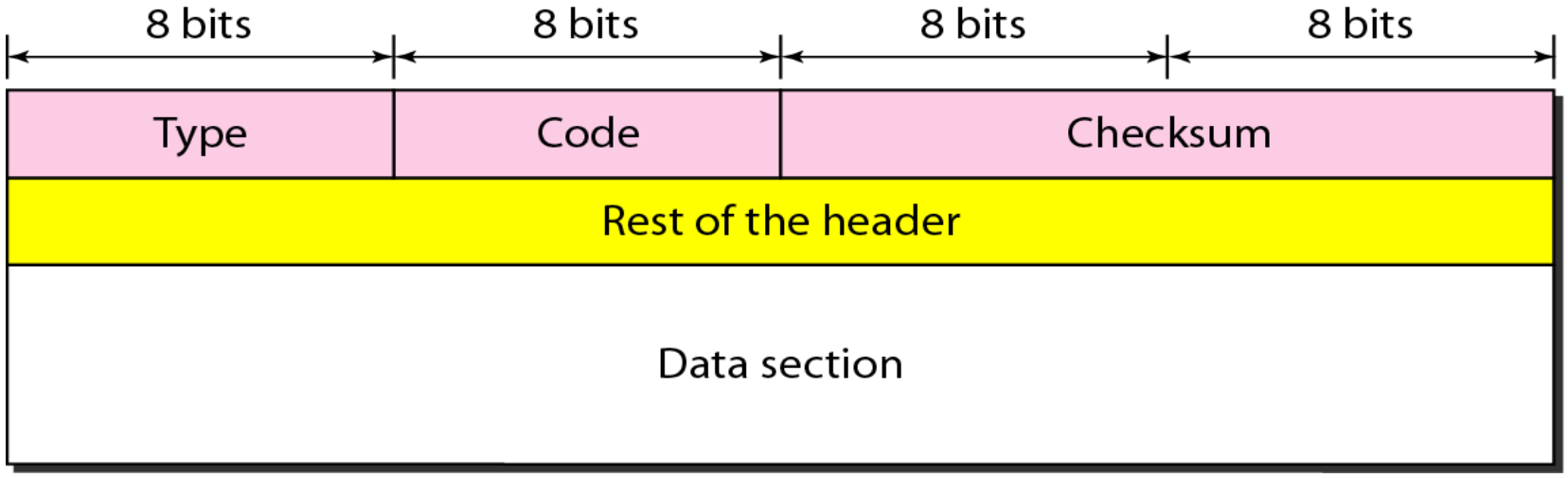
Internet Control Message Protocol (ICMP)

- IP har inga funktioner för felrapportering eller felkorrigering. IP saknar även funktioner för förfrågningar och styrning.
- Internet Control Message Protocol (ICMP) har utvecklats för dessa syften.
- ICMP är ett hjälpprotokoll till IP.

ICMP I TCP/IP-stacken



ICMP-meddelanden



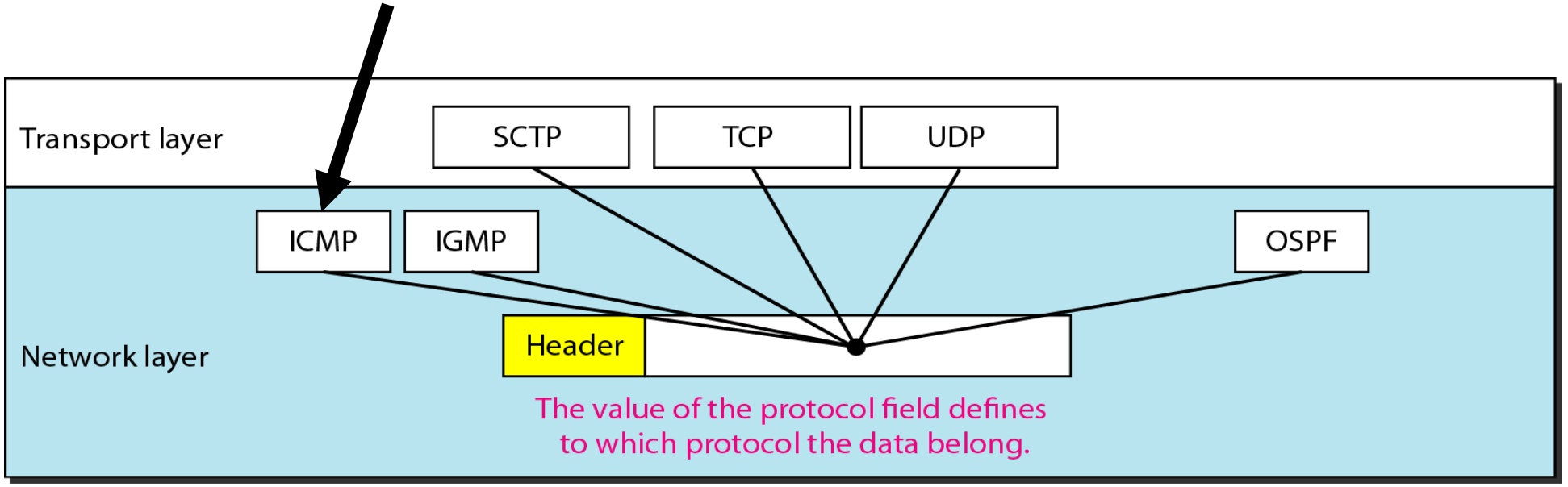
Två typer av meddelanden:

Error-reporting messages (felrapportering)

Query messages (förfrågningar)

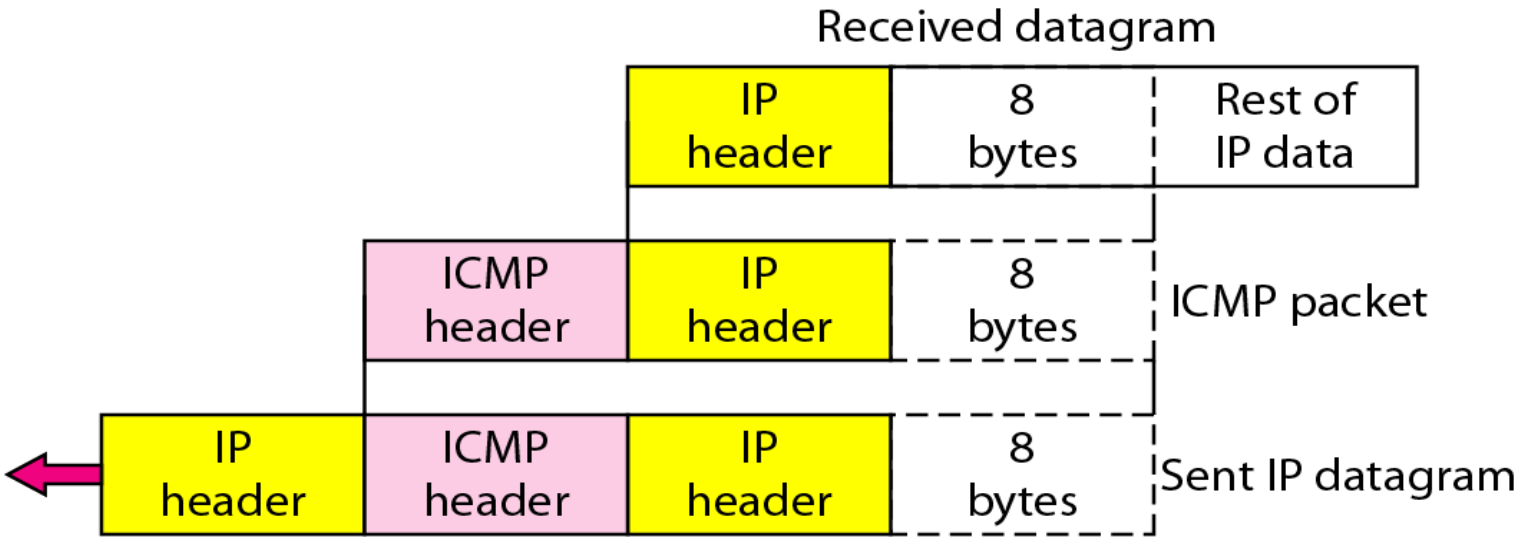
Enkapsulering (Encapsulation)

Ett ICMP-meddelande skickas i ett IP-paket:



Felrapportering (error-reporting)

När ett fel i transporten av ett IP-paket upptäcks, används ICMP för att rapportera felet till sändaren av IP-paketet. Felmeddelandet inkluderar IP-paketets header samt de första 8 bytes data från IP-paketet.



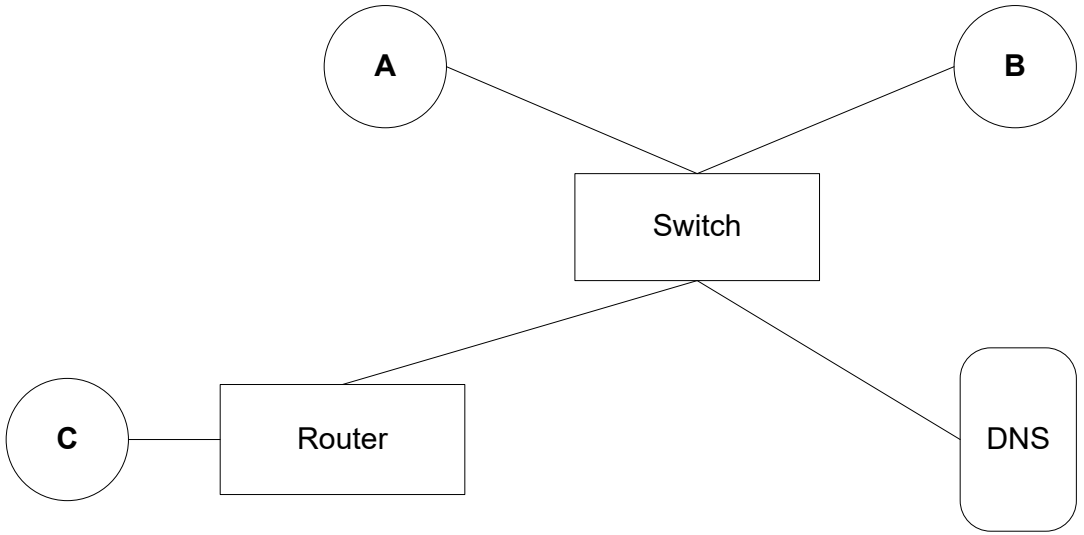
Några felmeddelanden

- Destination unreachable: Skickas när en router inte kan forwarda ett IP-paket eller en host inte kan leverera eller ta emot ett IP-paket.
- Source quench: Skickas när ett IP-paket kastas i en router pga överlast.
- Time exceeded: Skickas när ett IP-paket kastas pga dess TTL-värde har blivit 0 (TTL räknas ner med 1 för varje router-hopp.
- Redirection: Skickas när en host har fel default router, och behöver uppdatera sin routing-tabell.

Några ICMP Query meddelanden

- Echo-request and Reply: Används för att undersöka om två enheter (hosts eller routers) kan kommunicera på IP-nivå
- Timestamp request and reply: Används för att bestämma round-trip time (RTT) mellan två enheter (hosts eller routers).
- Router-Solicitation and Advertisment: Används av en host för att undersöka vilka routers som är kopplade till dess nät.

Tentaexempel



Host A vill skicka en ICMP echo request till host C. Host A kan bara C:s symboliska namn c.citynetwork.se. Förutsätt att alla adress-cacher är tomma. Beskriv vilka meddelanden som skickas i nätet ovan.

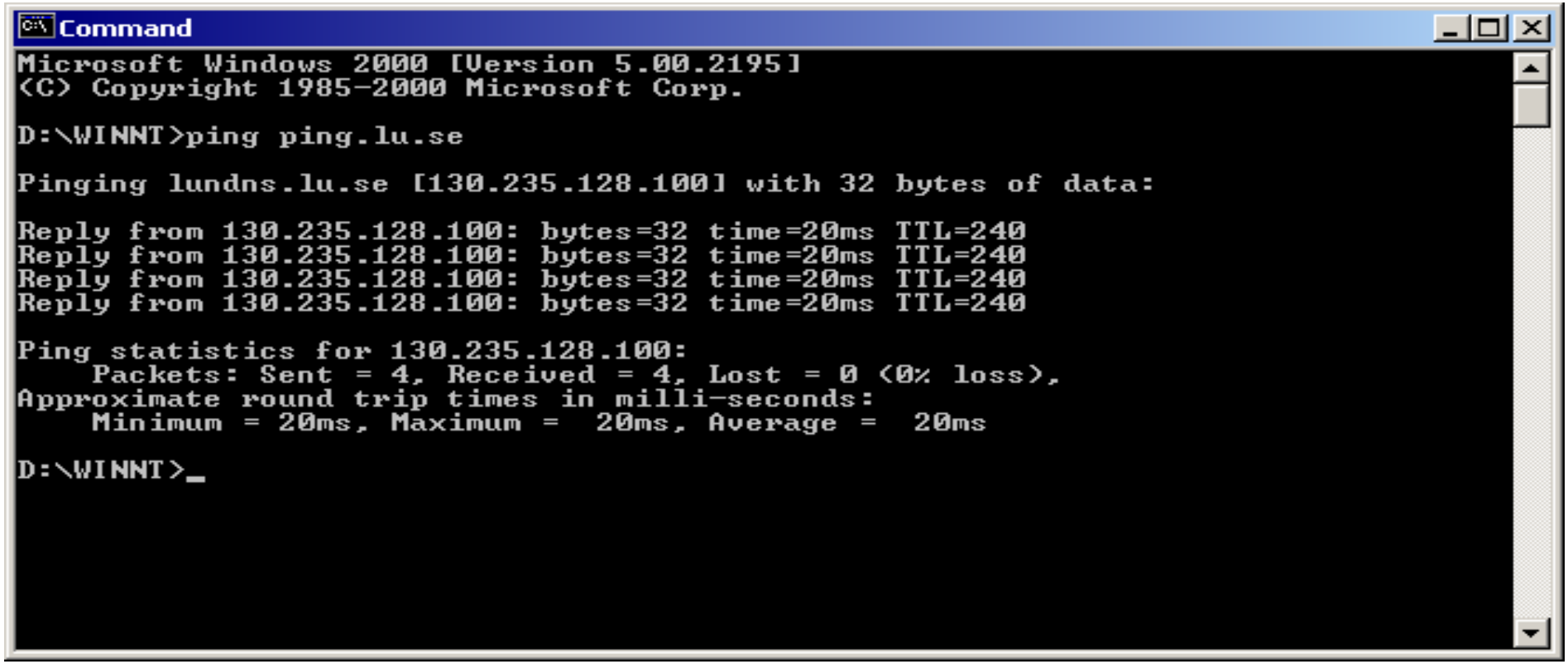
Felhanterings-verktyg (debugging tools)

Det finns flera mjukvarubaserade verktyg som kan användas för att undersöka ett nät tex för att identifiera fel. Två av de enklaste verktygen är:

- Ping
- Traceroute

Ping, exempel

Ping-programmet använder ICMP echo-request and reply meddelanden för att hitta information om en destination.

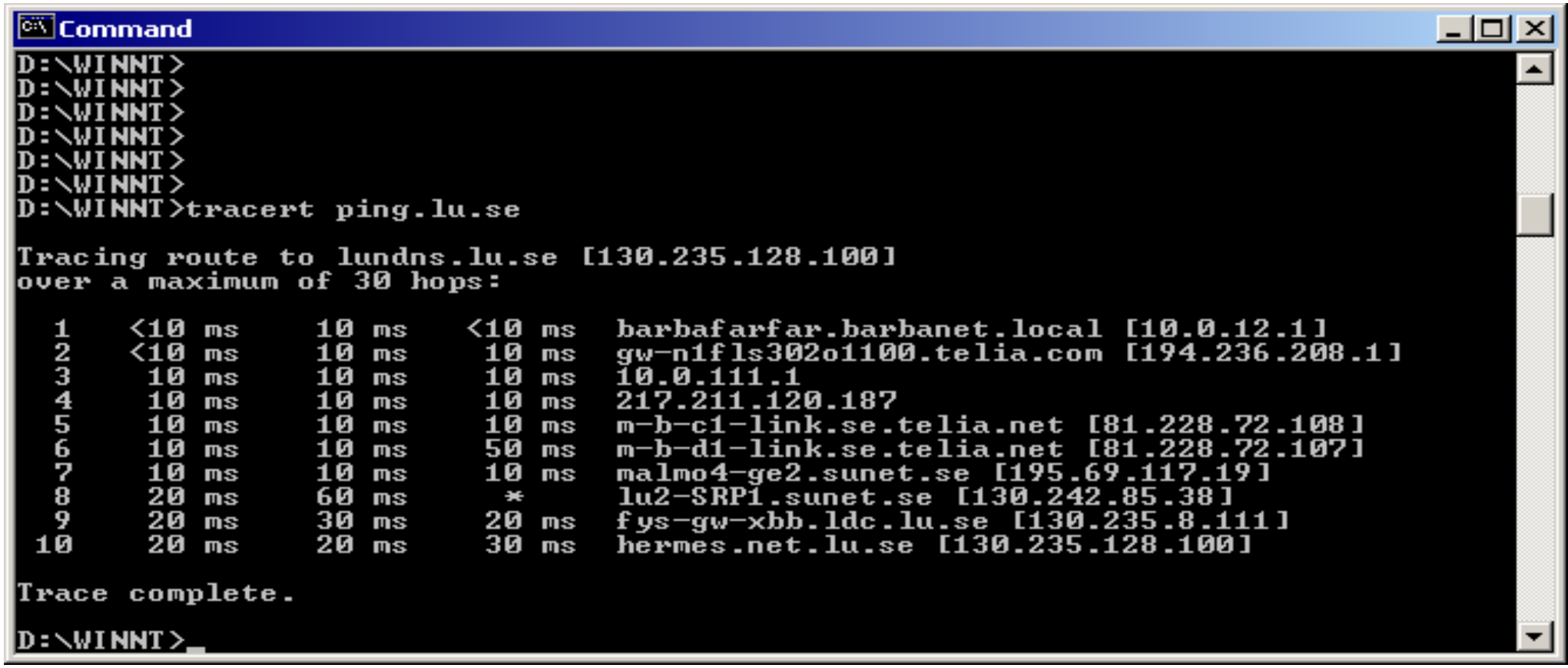


Traceroute

Traceroute (UNIX/Linux) eller Tracert (Windows) används för att hitta "vägen" mellan en sändare coh en mottagare dvs vilka routers ett IP-paket från sändaren till mottagaren kommer att passera.

Programmet använder TTL-fältet i IP-header och två ICMP-meddelanden: Time Exceeded och Destination Unreachable för att bestämma vägen som ett IP-paket tar.

Traceroute, exempel



Tentaexempel

Förklara var i OSI-modellen följande protokoll hör hemma:

HTTP, 802.3, TCP, PPP, IP,UDP, ICMP, ARP

Dina svar ska vara motiverade!

Telenätet och mobila system

Maria Kihl

LUND
UNIVERSITY

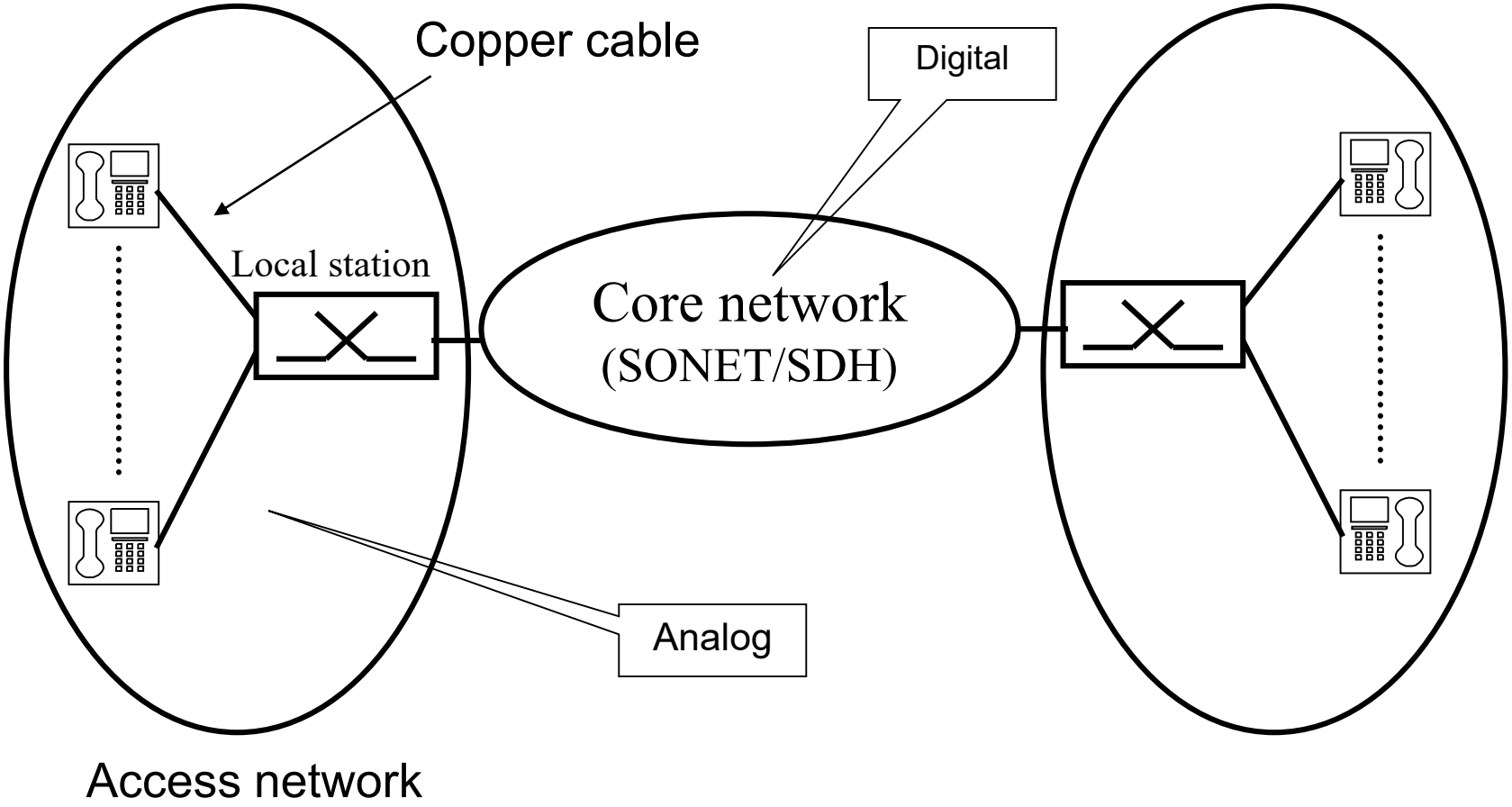
Läsanvisningar

Kihl & Andersson: 13, 14.1-3

Stallings: 8.4, 10.1, 10.2, 10. 3

Läsanvisningarna definieras av innehållet på slides.

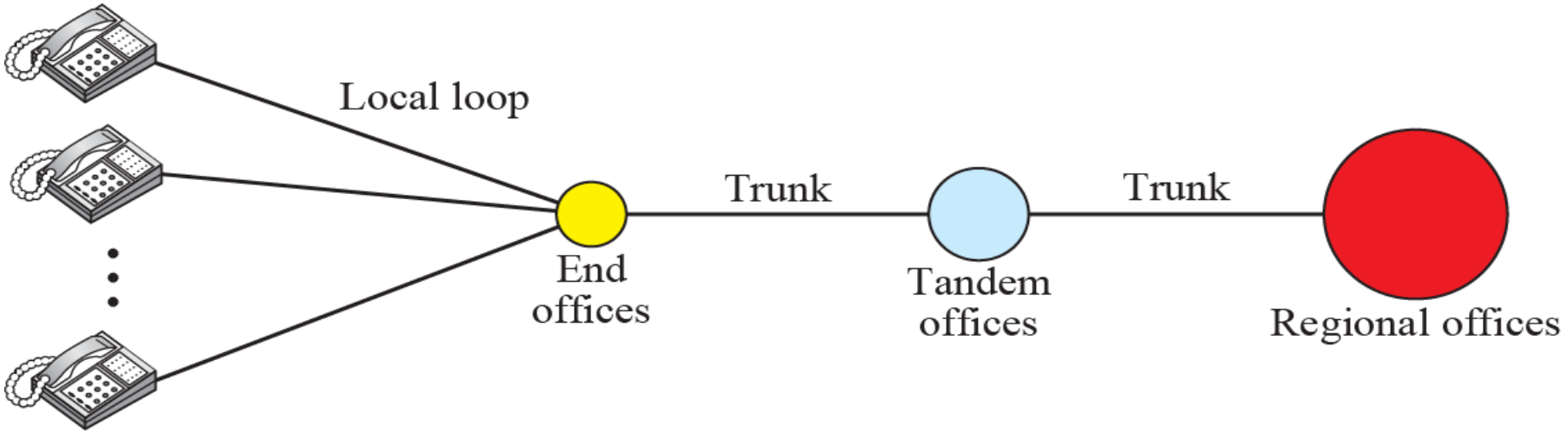
Det publika telenätet (PSTN)



Data transfer in telephone networks

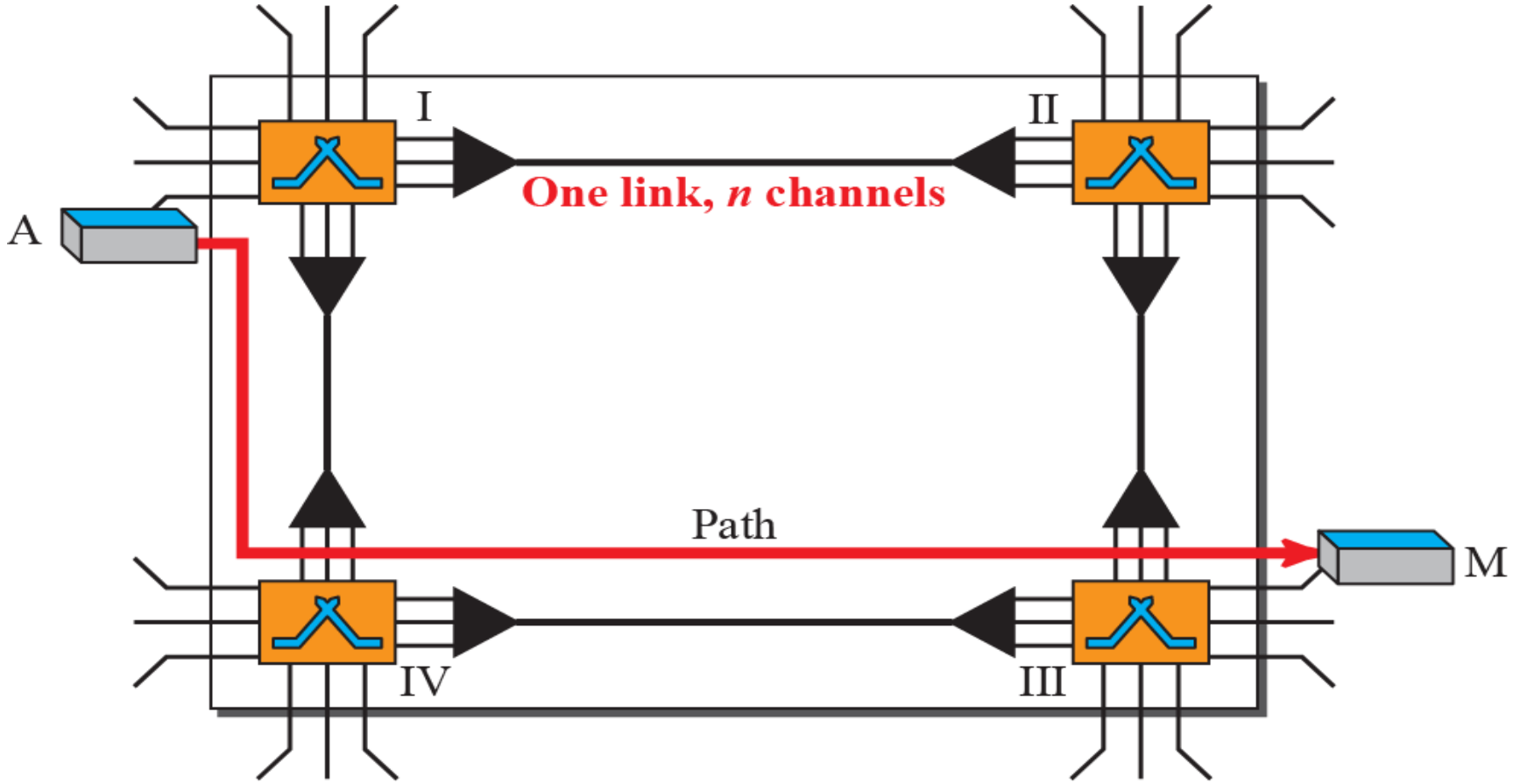
- The telephone core networks are digital.
  - PCM in local stations
  - Data transfer with 8-bits samples.
- The telephone networks use circuit switching.
  - A connection is set up for each call.
- The core networks use Synchronous Time Division Multiplexing.

Hierarchical structure



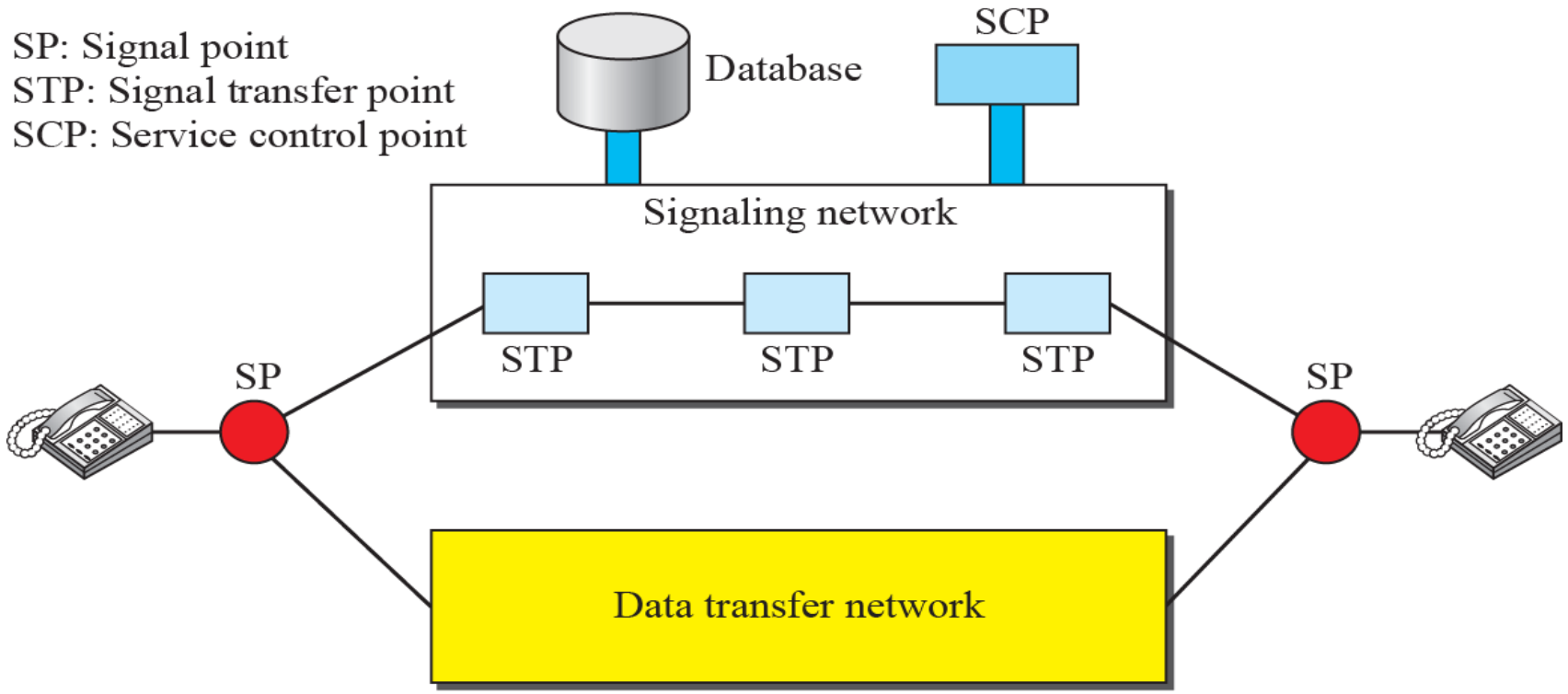
- From the telephone to local station (end office), the analog data is transferred on the 0-4 kHz frequency band.
- In the local station, PCM is used to create 8-bit samples that are coded and transmitted in the network using circuit switching and STDM.
- Also, there are gateways to the Internet and mobile networks.

Circuit switching



Control messages

Switching stations (offices) communicate with standardized protocols using a separate network.



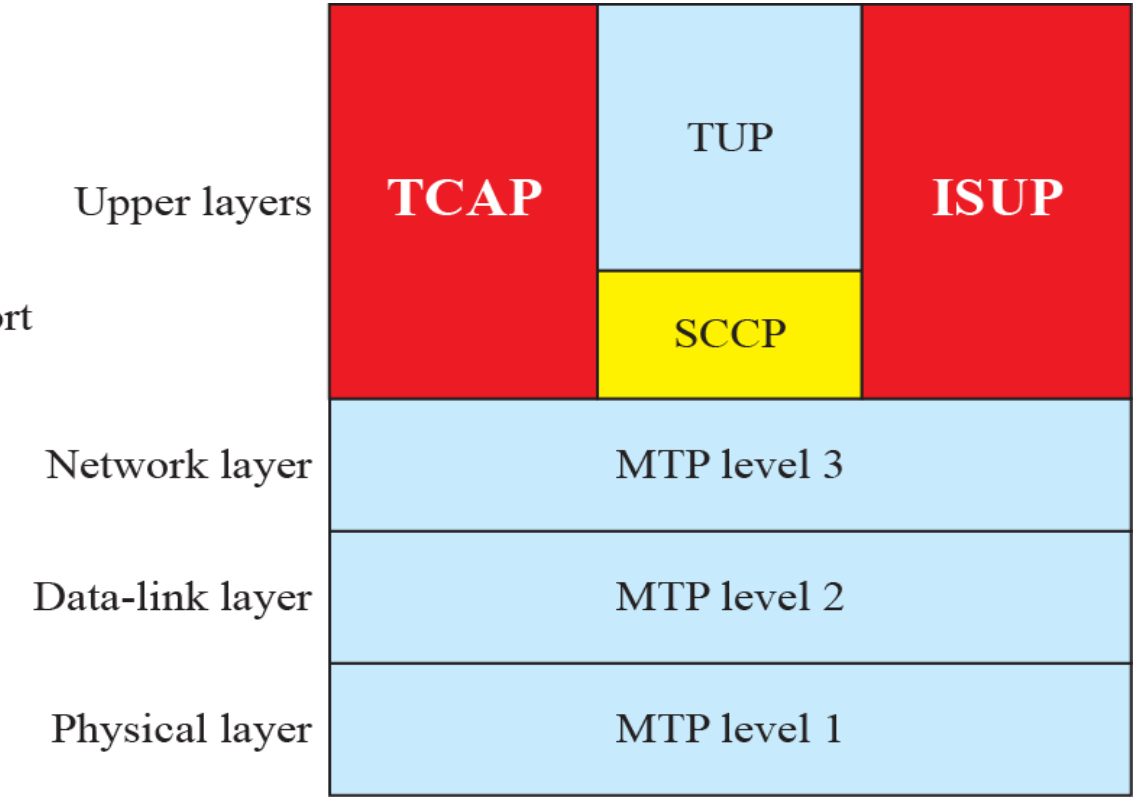
Comparison with the Internet

- In the Internet, control messages are sent the same path as data packets.
  - Special protocols, for example ICMP, ARP, DNS
  - Included in headers of data packets.
- In the telephone networks, the data transfer is separated from the control messages.
  - Delays for setting up and tearing down connections.
  - Very efficient data transfer with circuit switching.

Signaling System No. Seven (SS7)

The protocol stack for telephone networks is called Signaling System No. Seven (SS7).

MTP: Message transfer part
SCCP: Signaling connection control point
TCAP: Transaction capabilities application port
TUP: Telephone user port
ISUP: ISDN user port

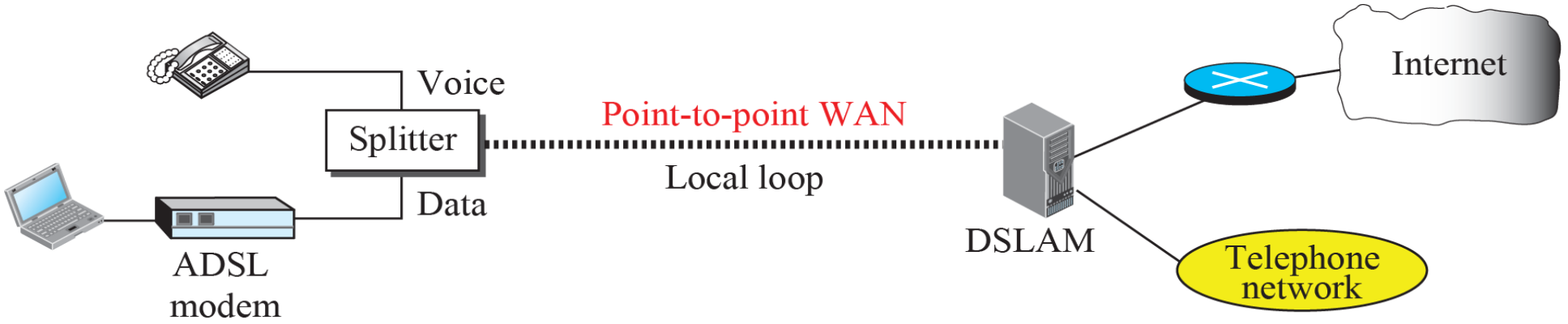


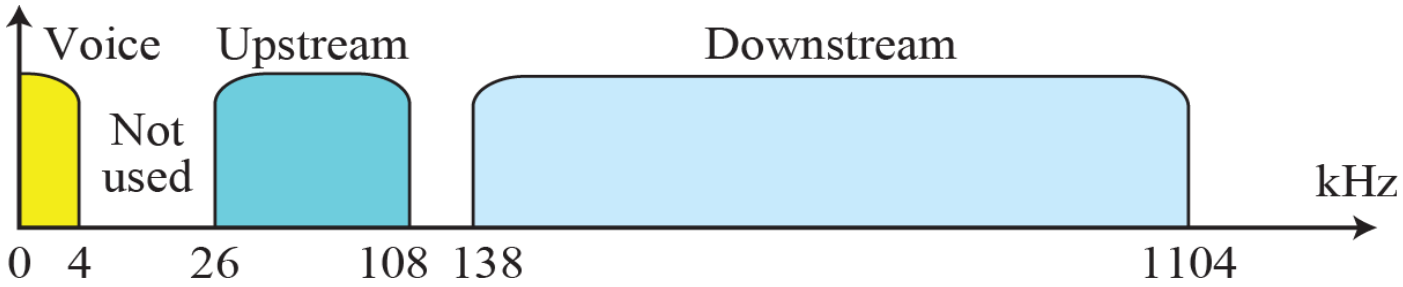
Reliability aspects

- A telephone switching station can be down only 6 minutes during 10 years.
- This means that:
  - All software updates must be performed during runtime.
  - All hardware parts are doubled for redundancy.
  - Much automatic error detection and failure recovery mechanisms.

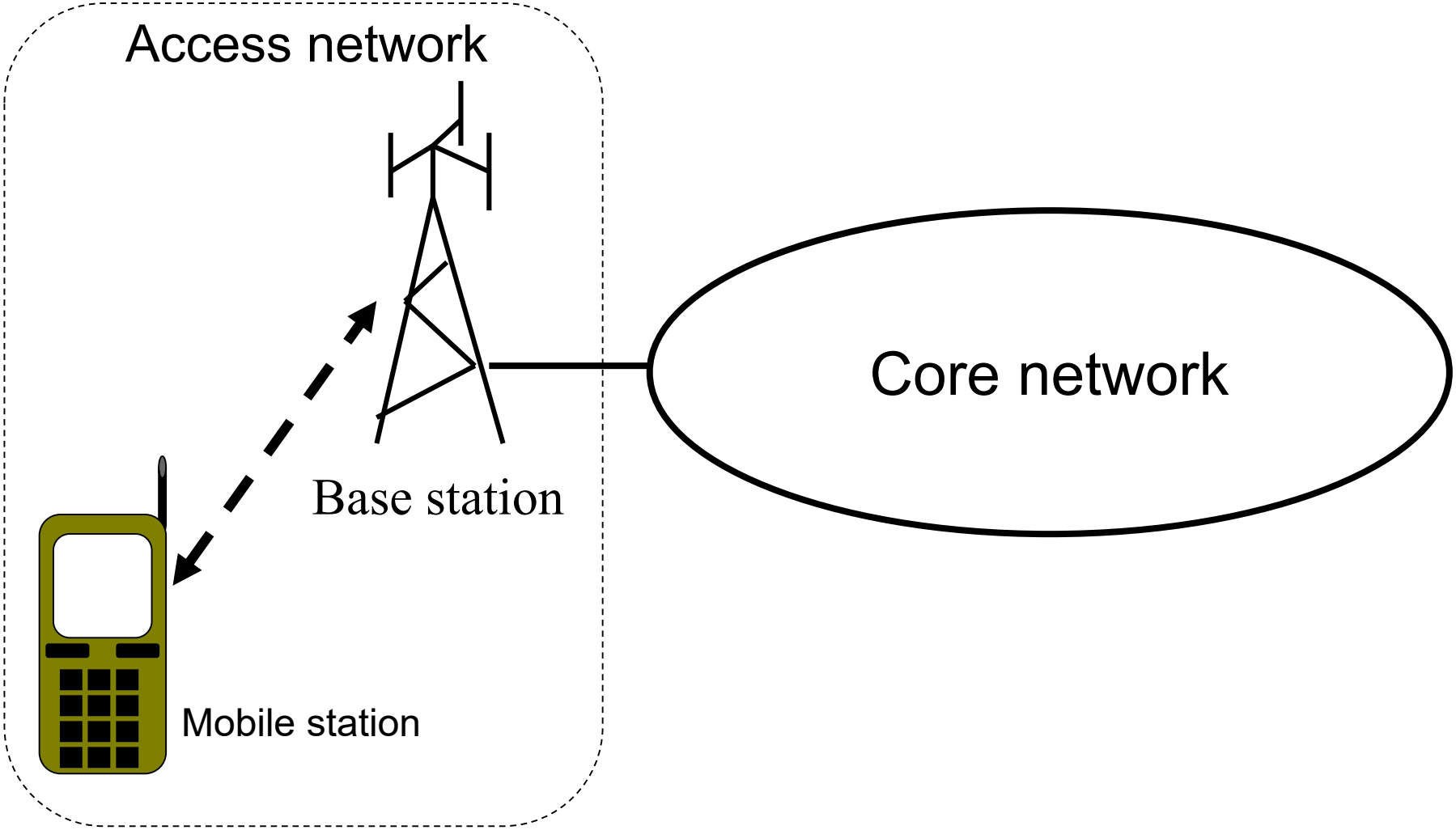
Internet access with xDSL

xDSL (ADSL, VDSL, etc) is used for providing Internet access via the telephone access line.





Mobile cellular (telephone) networks



The Frequency is the main performance problem…

Very Low Frequency (VLF) 0.3-30 KHz

Low Frequency (LF) 30-300 KHz (e.g. submarines)

Medium Frequency (MF) 0.3-3 MHz (e.g. radio stations)

High Frequency (HF) 3-30 MHZ (e.g. radio stations)

Very High Frequency (VHF) 30-300 MHz (e.g. TV stations)

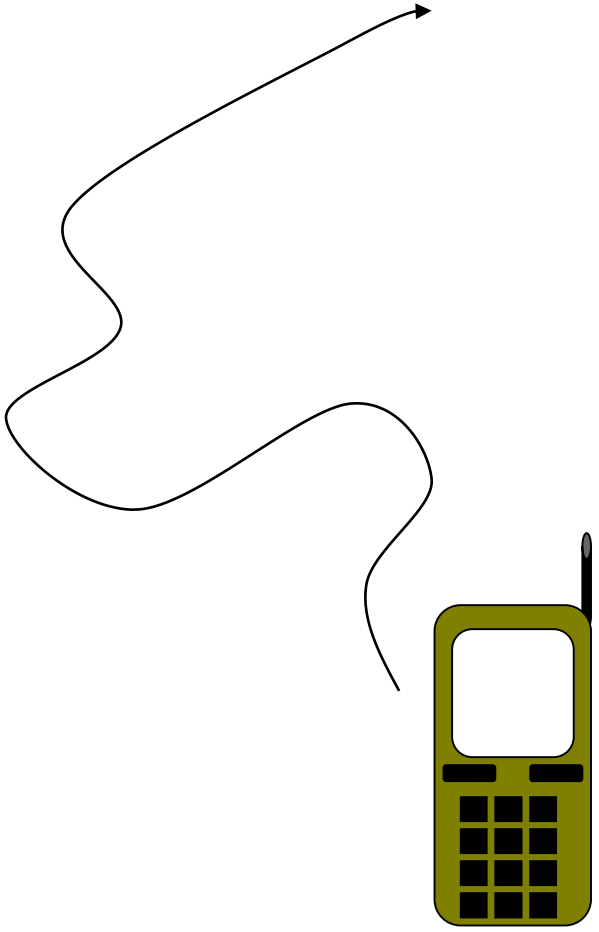
Ultra High Frequency (UHF) 0.3-3 GHz (e.g. mobile telephony)

Super High Frequency (SHF) 3-30 GHz (e.g. WLAN and microwave links)

Extremely High Frequency (EHF) 30-300 GHz

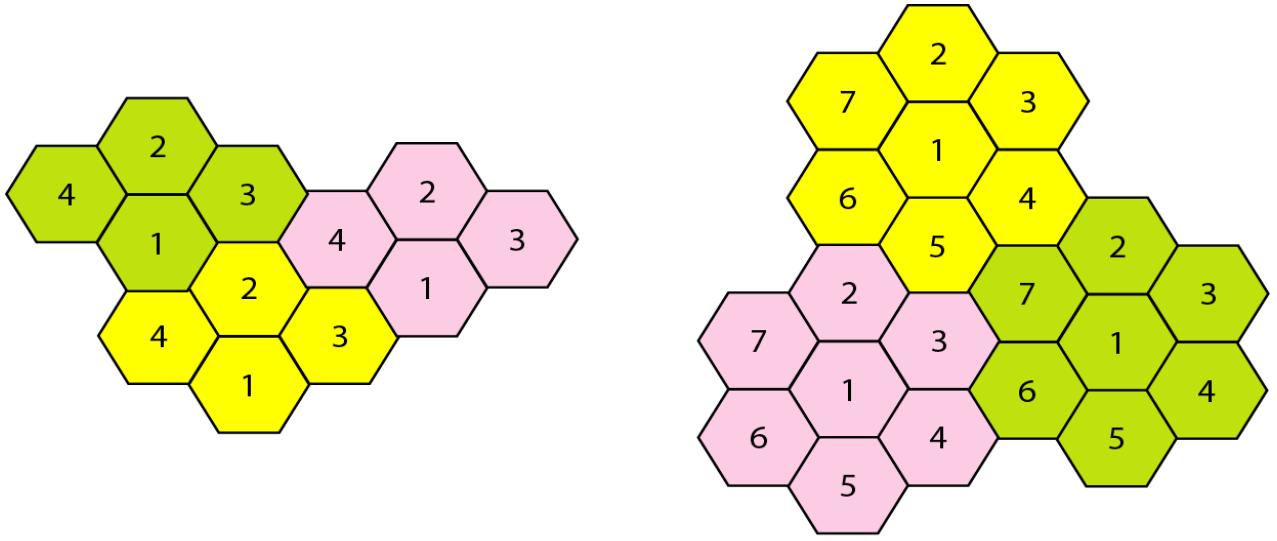
Optical transmission >300 GHz (e.g., IR, visible light, UV)

Together with mobility…



A cellular system should manage to maintain a connection even when the mobile station moves in high speeds, maybe across networks.

Cells and frequency reuse

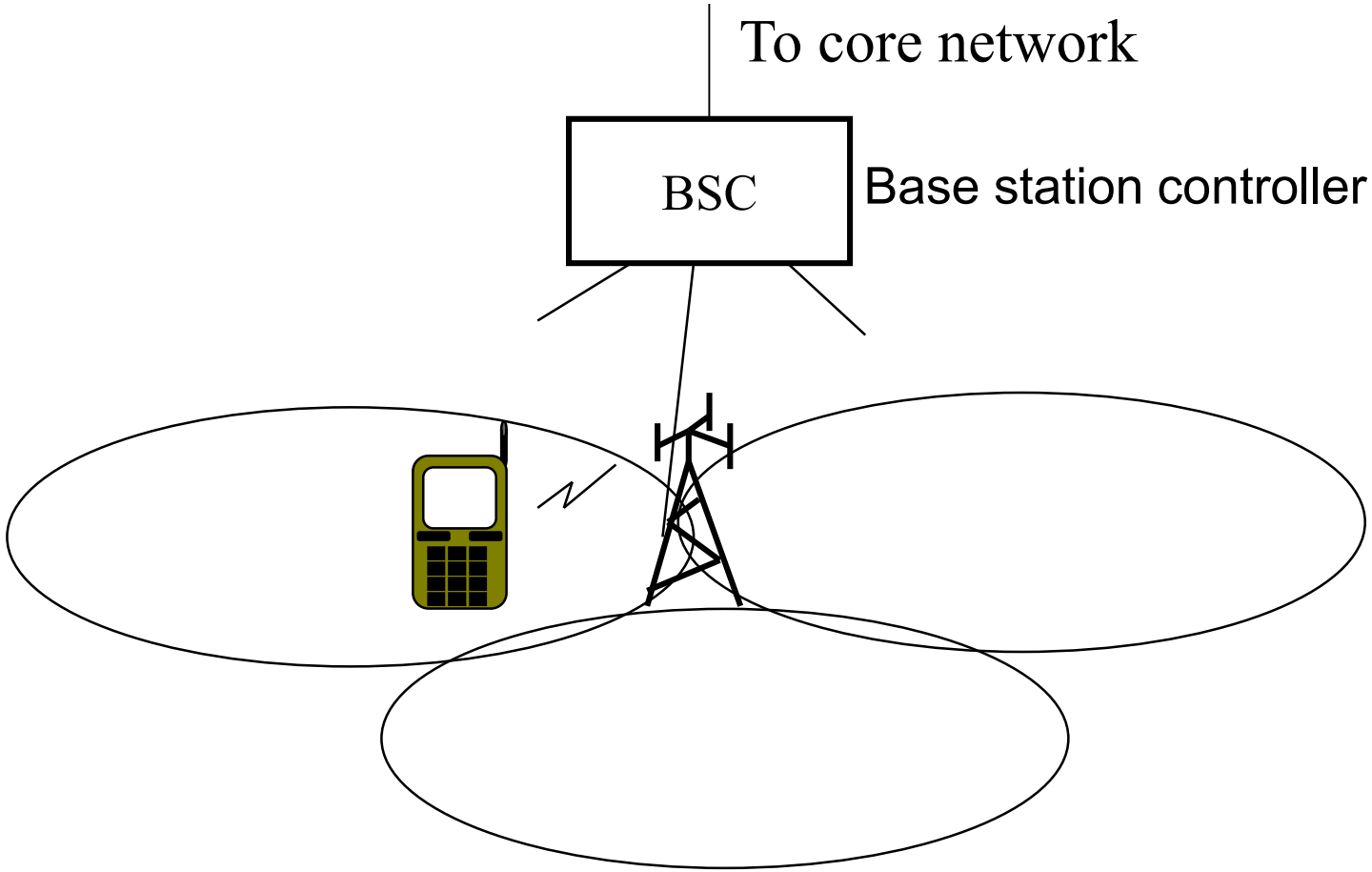


a. Reuse factor of 4

b. Reuse factor of 7

- The network is geographically divided into cells.
- In each cell there is a base station.
- Each cell is given some frequencies. The frequencies are reused in other cells according to a specific pattern.

Cellular access network



Several cells are controlled by one base station controller.

Problems with mobility

The necessary signal strength depends on the mobile station's distance to the base station (*power control*).

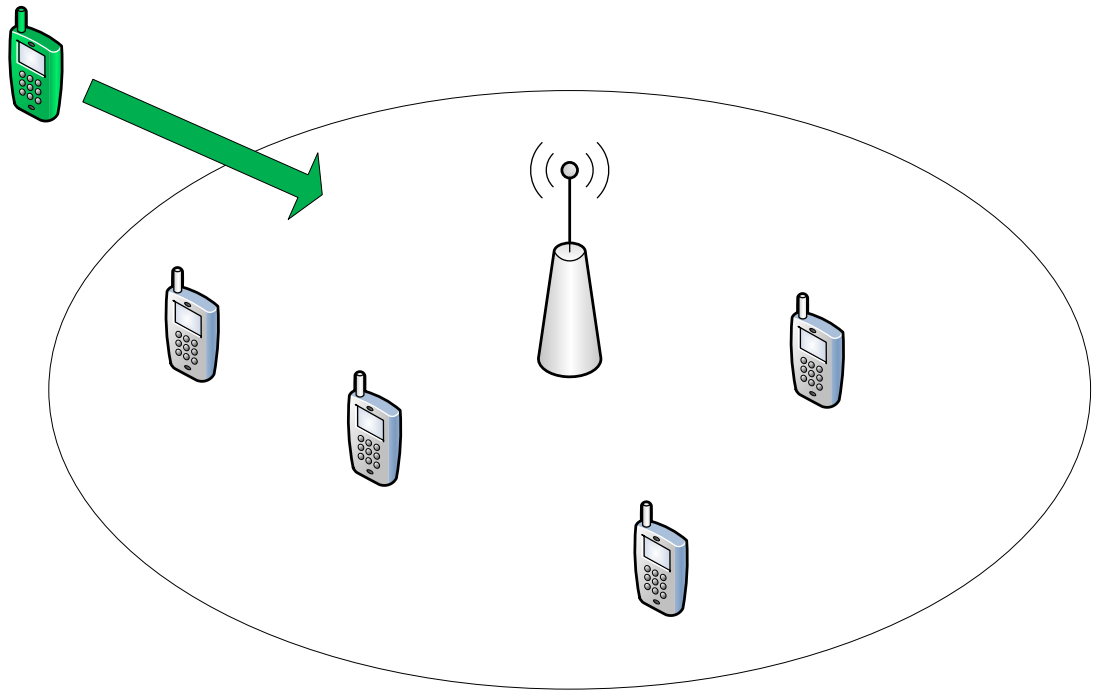
The mobile stations can move to another cell (*handover/handoff*).

The mobile station can move to another network, maybe in another country (*roaming*).

Multipel access

- Flera terminaler ska ha access till samma basstation. Protokoll för multipel access krävs.
- Cellulära nät använder ”Controlled access”. Basstationen bestämmer vilken kanal en terminal får använda.
  - ”Uplink” och ”Downlink”-kanaler kan använda olika metoder för kanaluppdelning.
  - Det finns vanligtvis en gemensam kanal som alla terminaler lyssnar på.

Multipel access i mobila nät



Olika kanaler används med olika MAC-protokoll för att

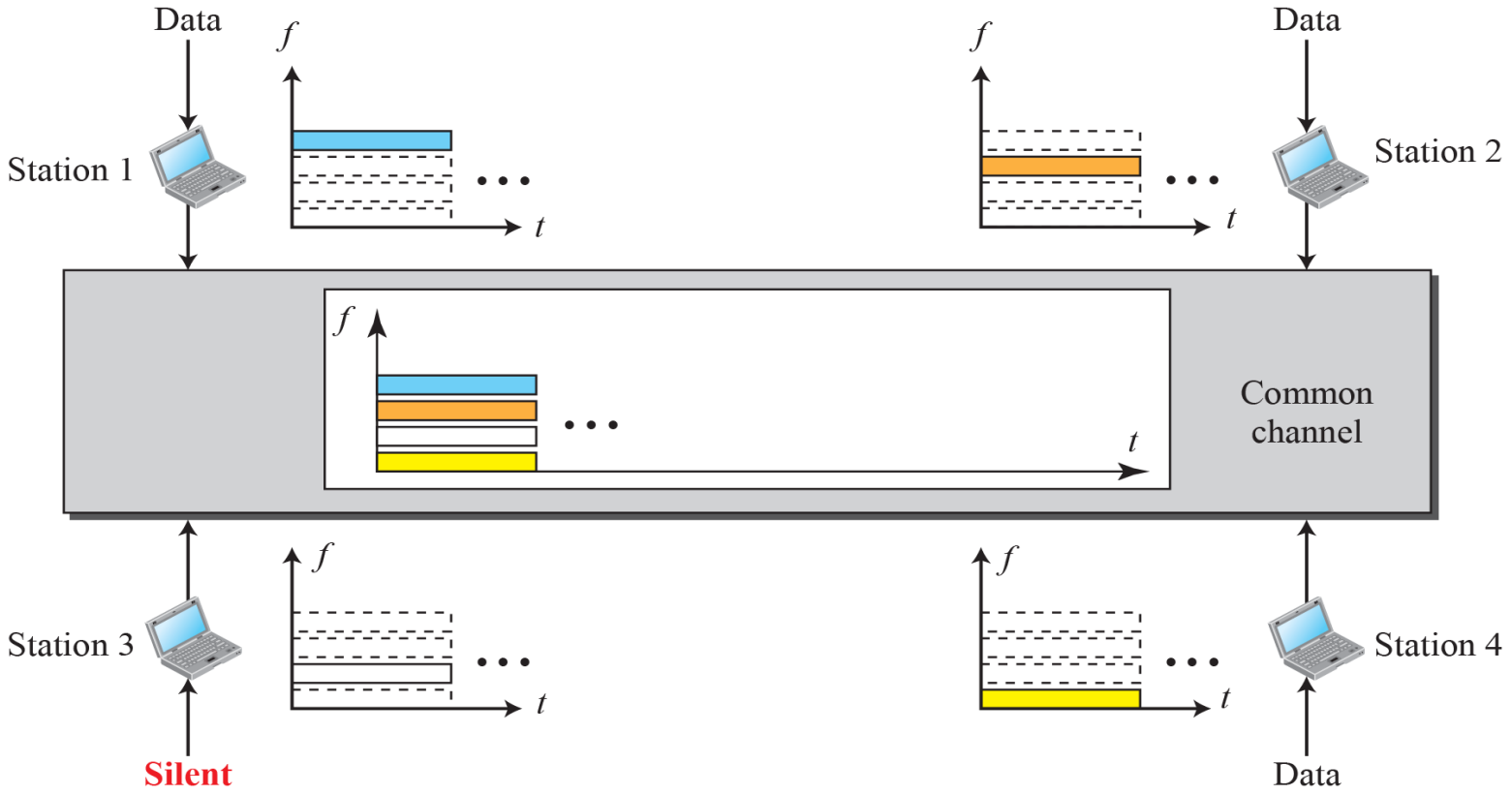
- Hitta en basstation
- Kontrollmeddelanden
- Dataöverföring
- Telefoni
- Etc.

Channelization (Multiple access)

- Three basic so called channelization techniques:
  - Frequency-Division Multiple Access (FDMA)
  - Time-Division Multiple Access (TDMA)
  - Code-Division Multiple Access (CDMA)

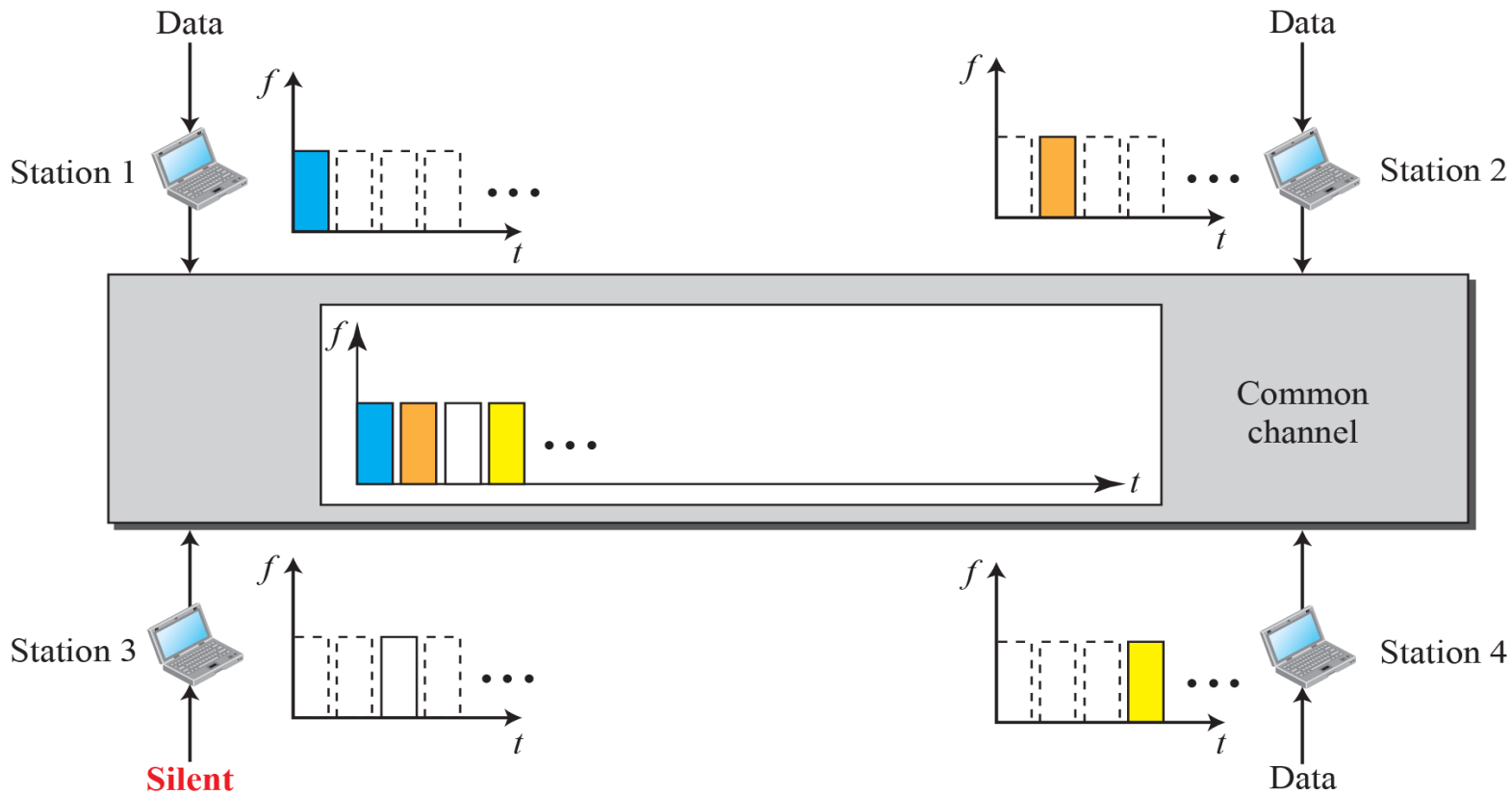
Frequency-Division Multiple Access

In FDMA, the terminals have separate frequency bands.



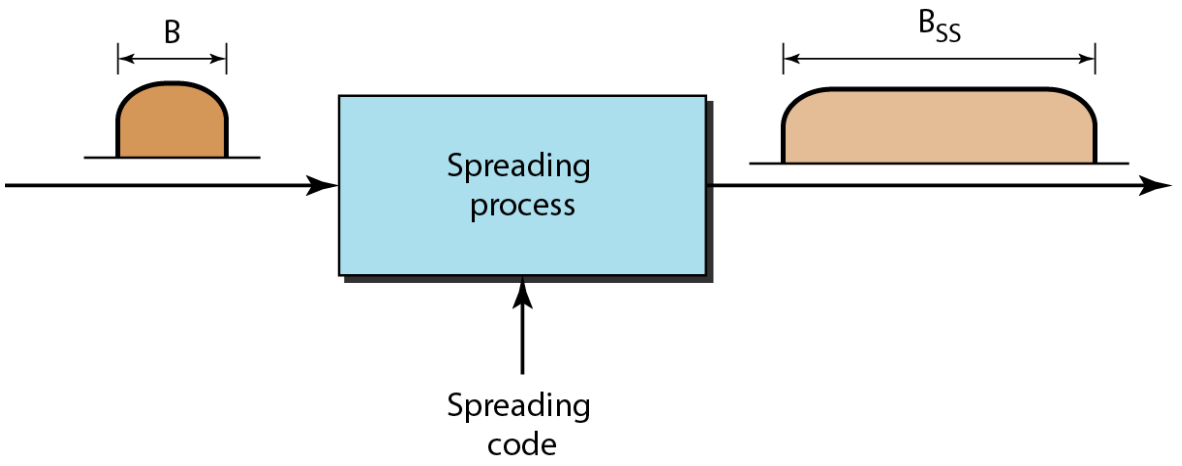
Time-Division Multiple Access

In TDMA, the terminals use separate time slots on a shared frequency band.



Spread Spectrum

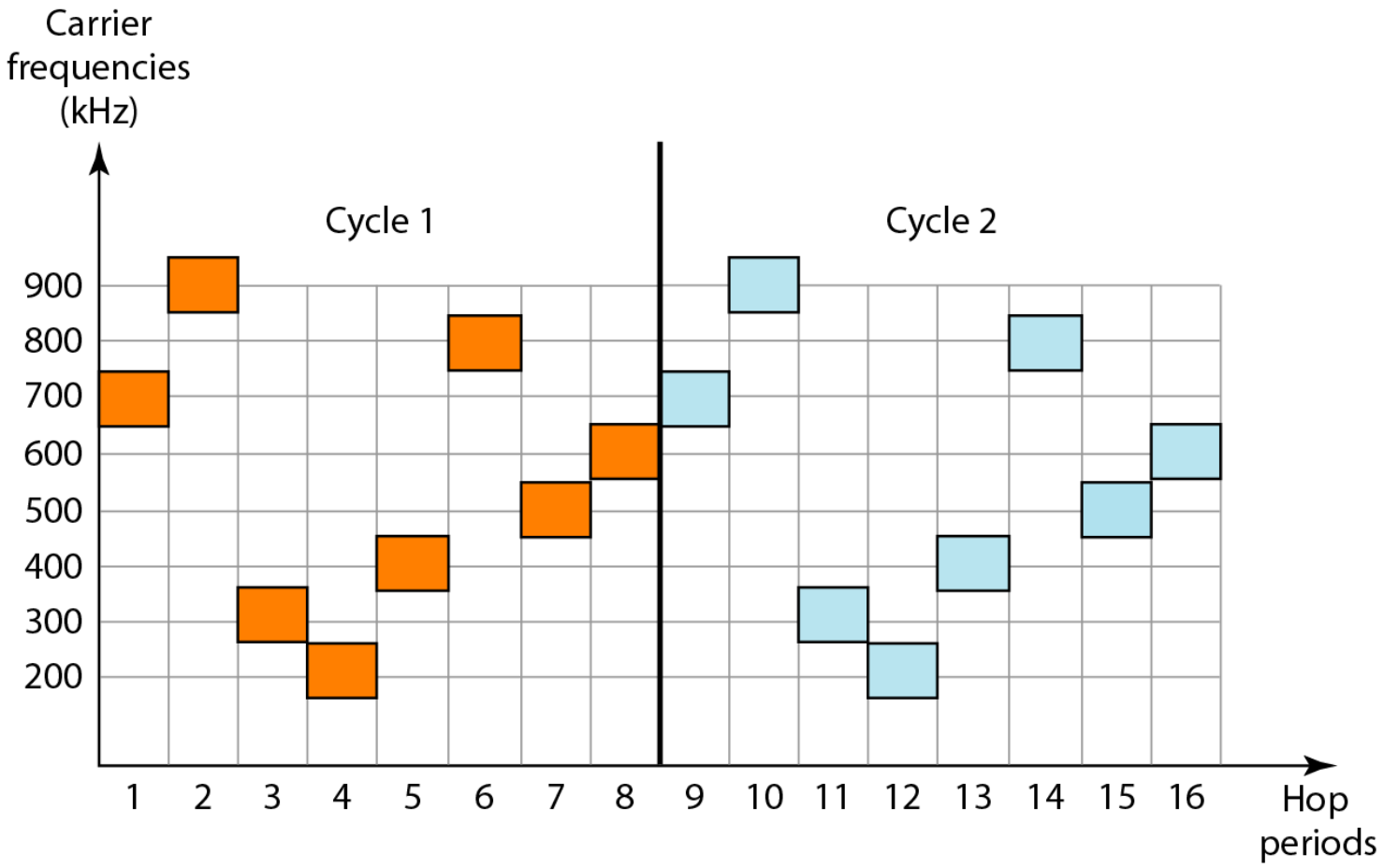
Spread Spectrum (SS), är en teknik för trådlösa länkar med mycket störningar.



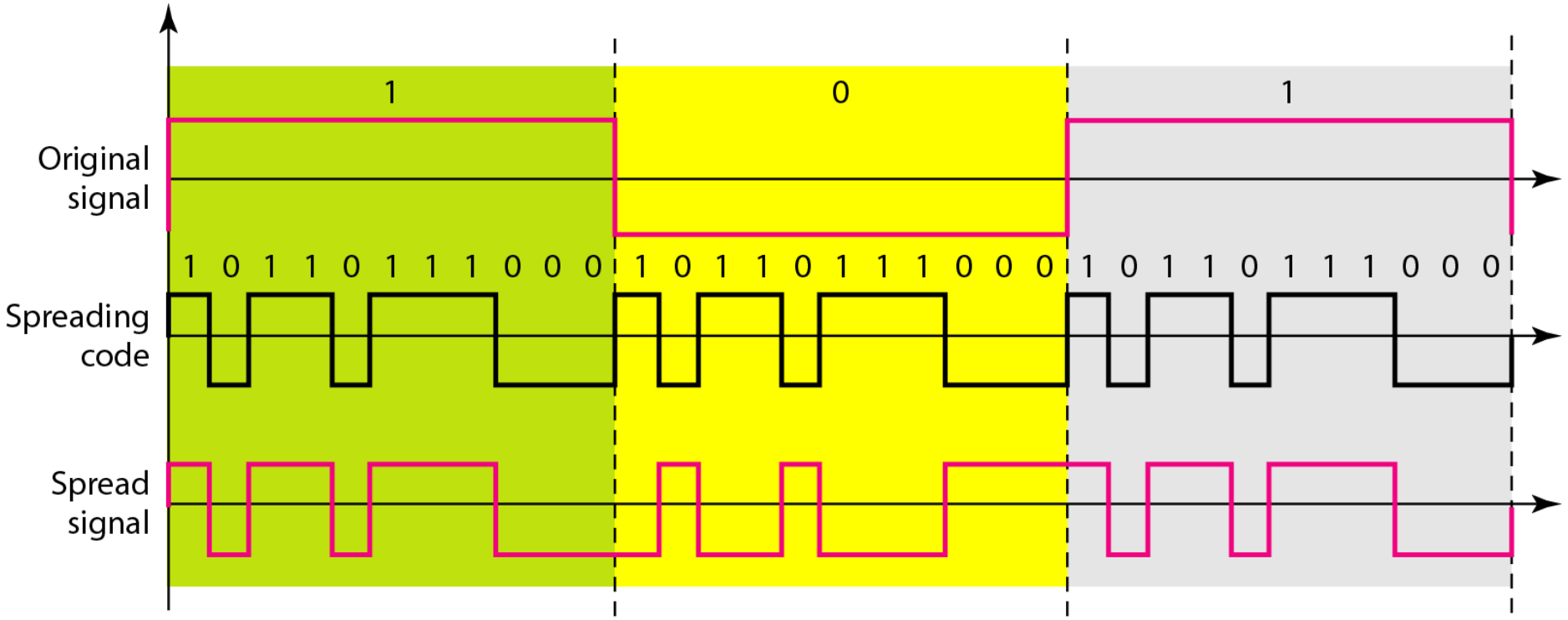
Spread Spectrum metoder

- 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. Spridningskoden är vald så att alla andra källor adderade tillsammans blir som vitt brus och kan filtreras bort.

FHSS-cykler


Carrier
frequencies
(kHz)
Cycle 1
Cycle 2
900
800
700
600
500
400
300
200
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Hop
periods

DSSS exempel



Exempel på DSSS (utan bitfel)

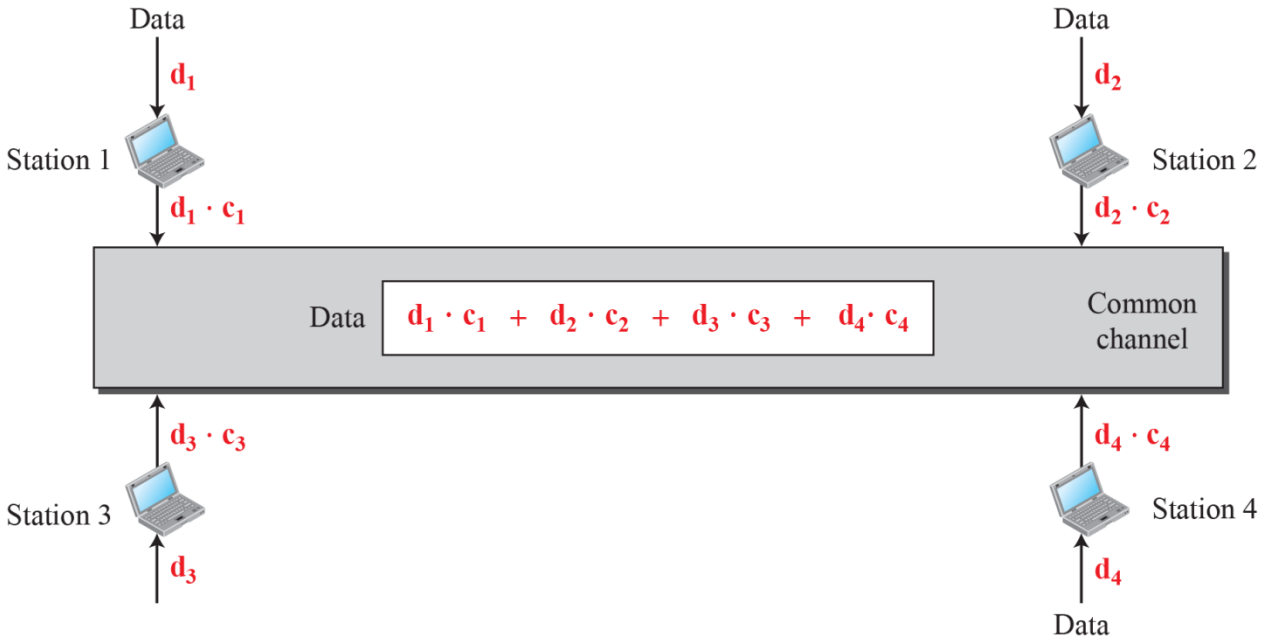
Bit som skall skickas:	0	1
Bitvis modulo-2	0000	1111
med chip-sekvens:	1110	1110
Resultat:	1110	0001
Mottagaren adderar	1110	0001
med chip-sekvens:	1110	1110
Resultat:	0000	1111
Adderas bitvis	0+0+0+0	1+1+1+1
Resultat:	0	4

DSSS-exempel (med bitfel)

Bit som skall skickas:	0	1
Bitvis modulo-2	0000	1111
med chip-sekvens:	1110	1110
Resultat:	1110	0001
Mottagaren adderar	1010	1001
med chip-sekvens:	1110	1110
Resultat:	0100	0111
Adderas bitvis	0+1+0+0	0+1+1+1
Resultat:	1	3

Code Division Multiple Access (CDMA)

Med hjälp av DSSS kan man multiplexera flera kanaler på samma länk. Tekniken kallas Code Division Multiple Access (CDMA) och används i moderna mobilnät.



CDMA

Alla stationer har en egen ”chipping code”. Dessa måste vara matematiskt ortogonala med varandra.

C_1 [+1 +1 +1 +1]

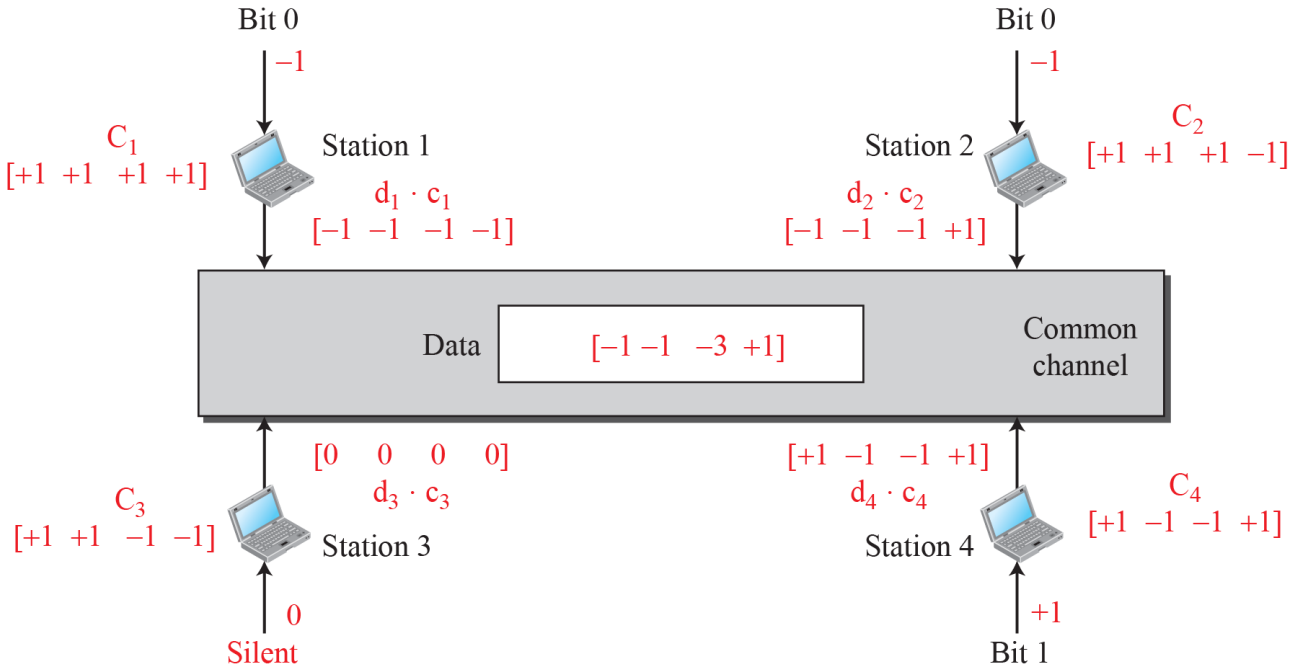
C_2 [+1 –1 +1 –1]

C_3 [+1 +1 –1 –1]

C_4 [+1 –1 –1 +1]

CDMA

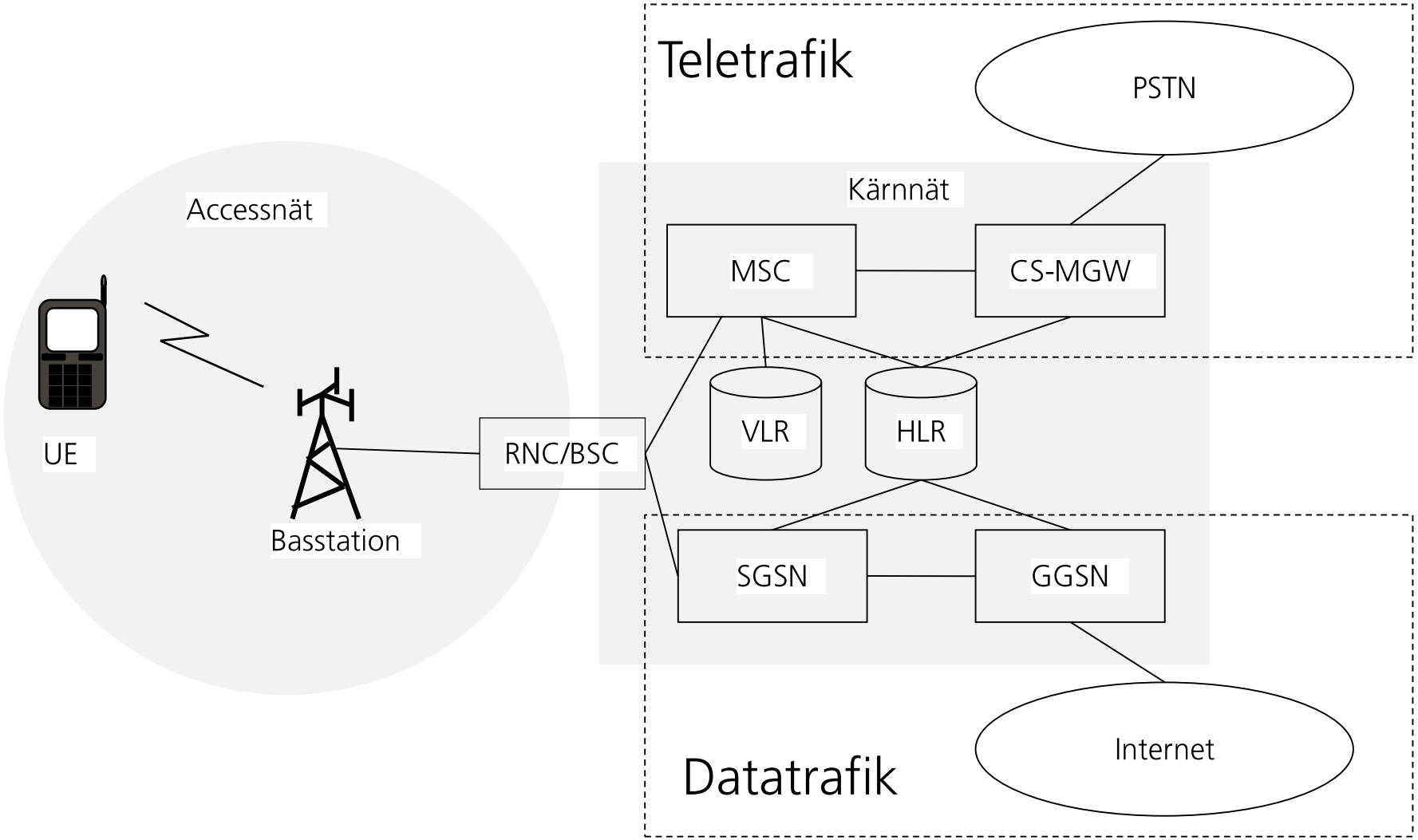
All data skickas samtidigt (synkroniserat) på samma kanal. Mottagaren använder sändarens kod för att filtrera ut dess signal.



2G/3G-system

- GSM (Global System for Mobile Communication) brukar kallas för 2G.
- UMTS (Universal Mobile Telecommunication System) brukar kallas för 3G.
- Gemensamt:
  - Utvecklade främst för telesamtal.
  - Använder liknande arkitektur för kärnnätet.
- Olika:
  - Radioaccessen ger högre överföringshastigheter i UMTS.

Kärnnätet i GSM och UMTS



Förklaring till begreppen

UE=User Equipment

BSC = Base Station Controller

RNC = Radio Network Controller

MSC = Mobile Switching Centre

CS-MGW = Circuit Switched Media Gateway

SGSN = Serving GPRS support node

GGSN = Gateway GPRS support node

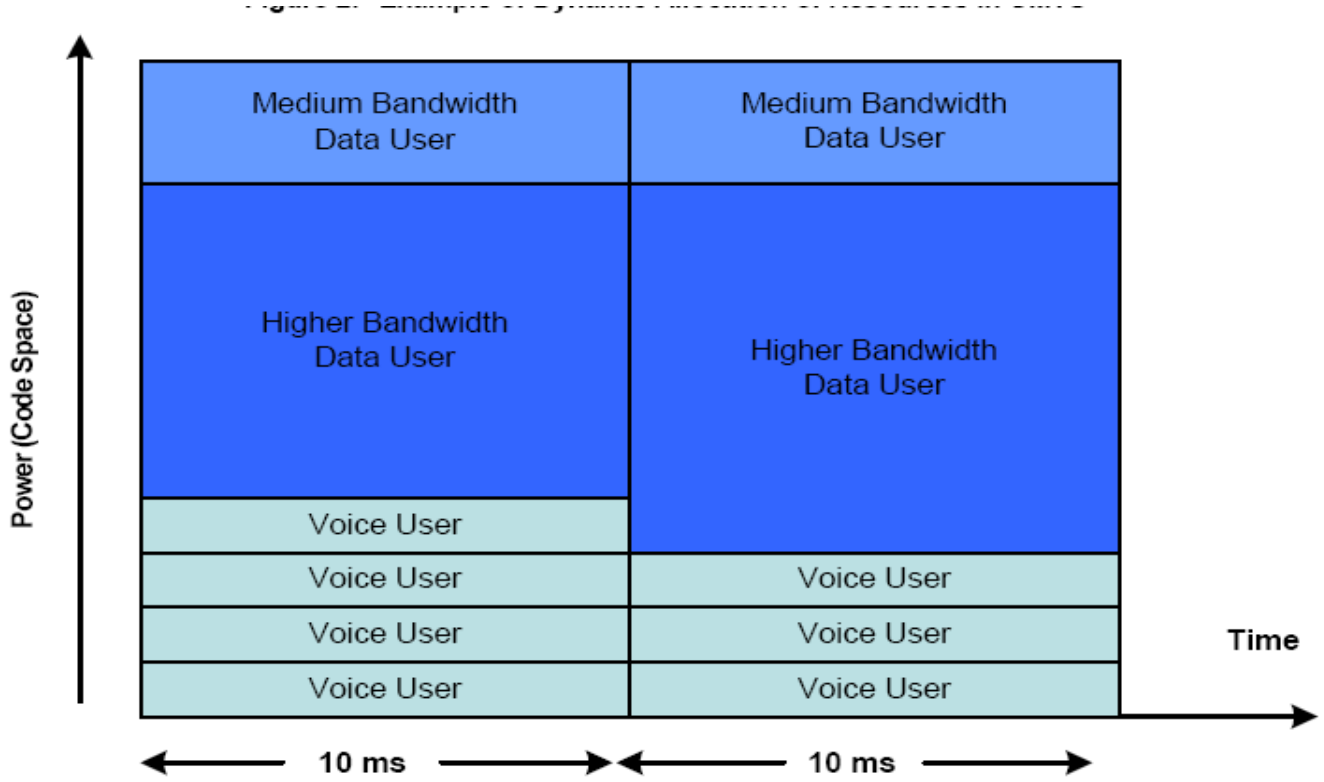
HLR = Home Location Register

VLR = Visiting Location Register

UMTS accessnät (UTRAN)

- UMTS Terrestrial Radio Network
- Använder frekvensmultiplex och CDMA.
- CDMA kräver power control, eftersom alla mobiler måste ha samma signaleffekt vid basstationen. Detta regleras 1500 ggr per sekund.
- Innhåller dynamisk allokering av kapacitet.

Dynamisk resursallokering i UMTS

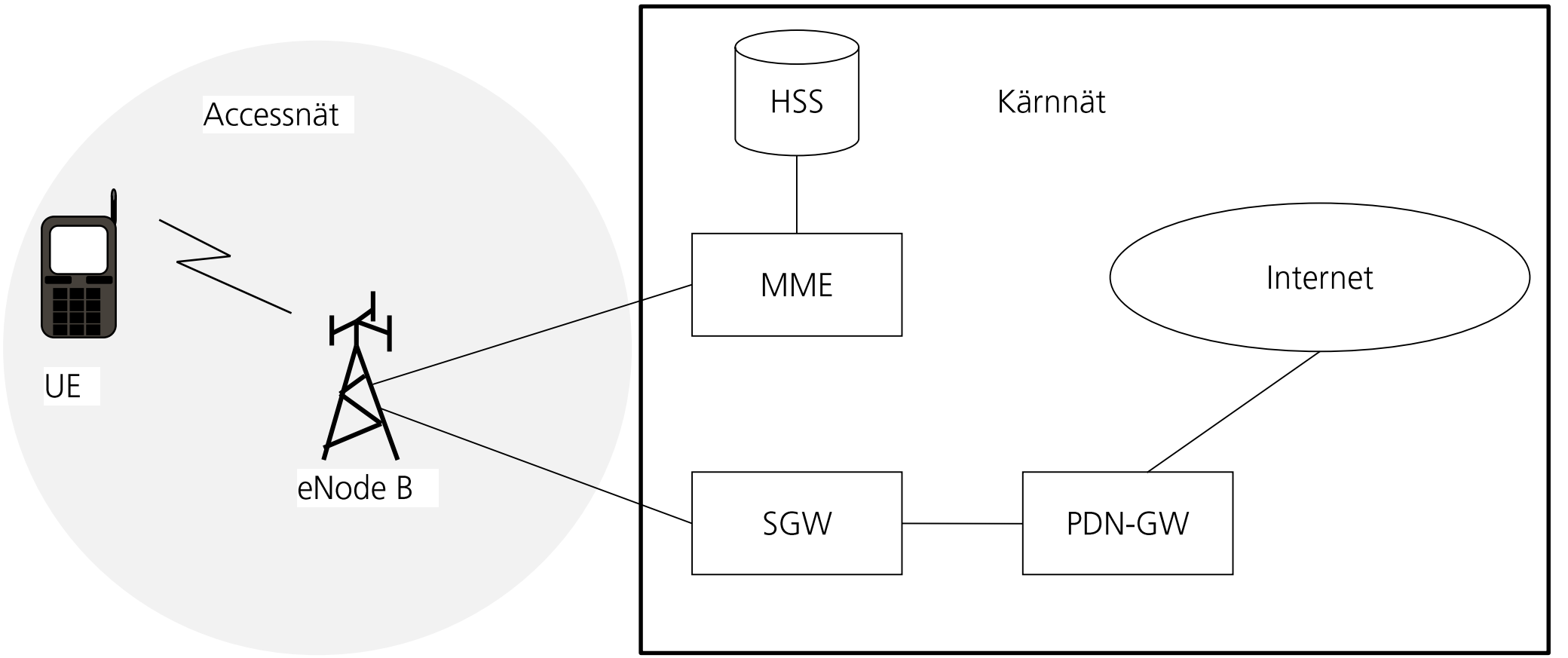


The capacity for each user is dynamically allocated (each 10 ms). This allows for a more efficient use of the frequency band.

Long Term Evolution (LTE)

- 4th generation mobile networks
- Difference compared to GSM/UMTS:
  - Packet-switching!
  - Main service is Internet access, not telephony!
  - Higher data rates (of course)
- Solutions needed to provide Voice over LTE
- Higher data rates require much smaller cells than before, so called pico and femtocells.

Kärnnätet i LTE



Förklaring till begreppen

eNode B: Evolved Node B

MME = Mobility Management Entity

SGW = Serving Gateway

PDN GW = Packet Data Network gateway

HSS = Home Subscriber Server

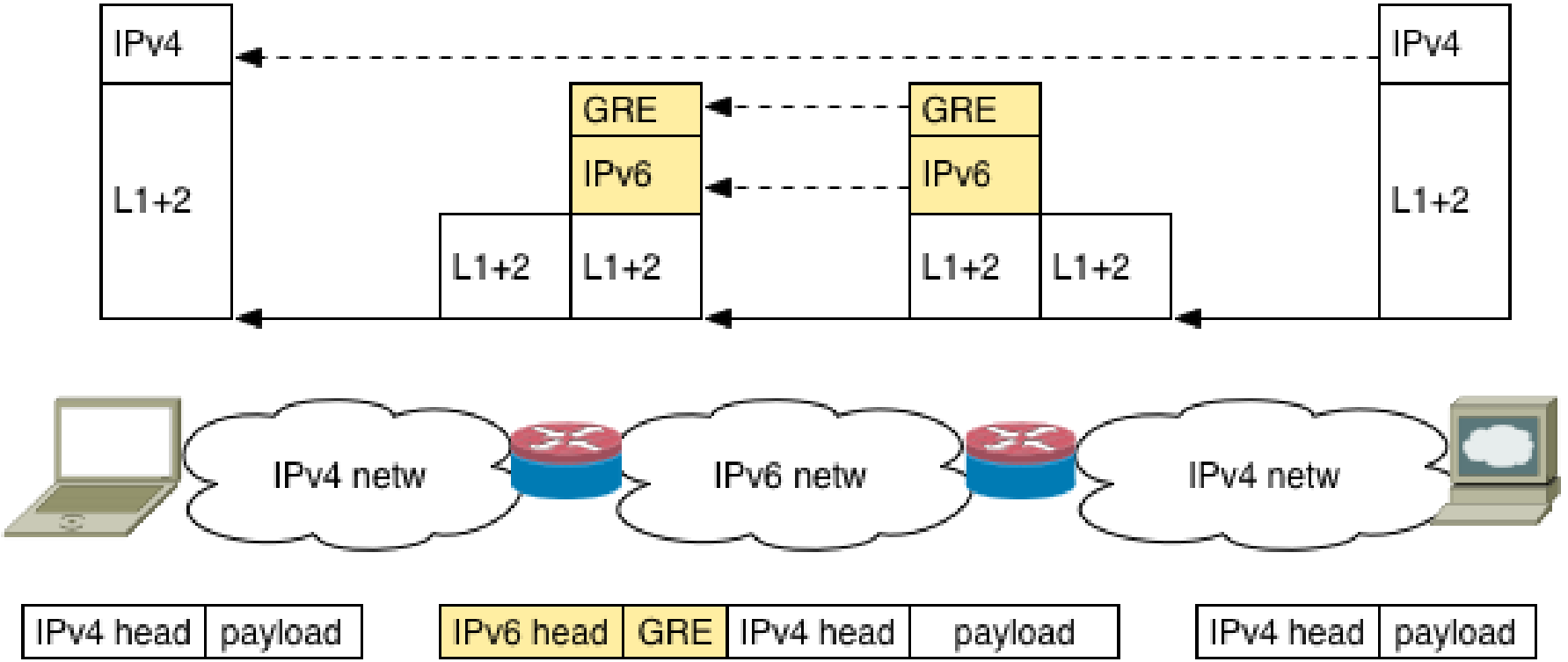
Notera: Det går inte att ringa vanliga kretskopplade telesamtal med LTE:s arkitektur!

Protocol stack and tunneling

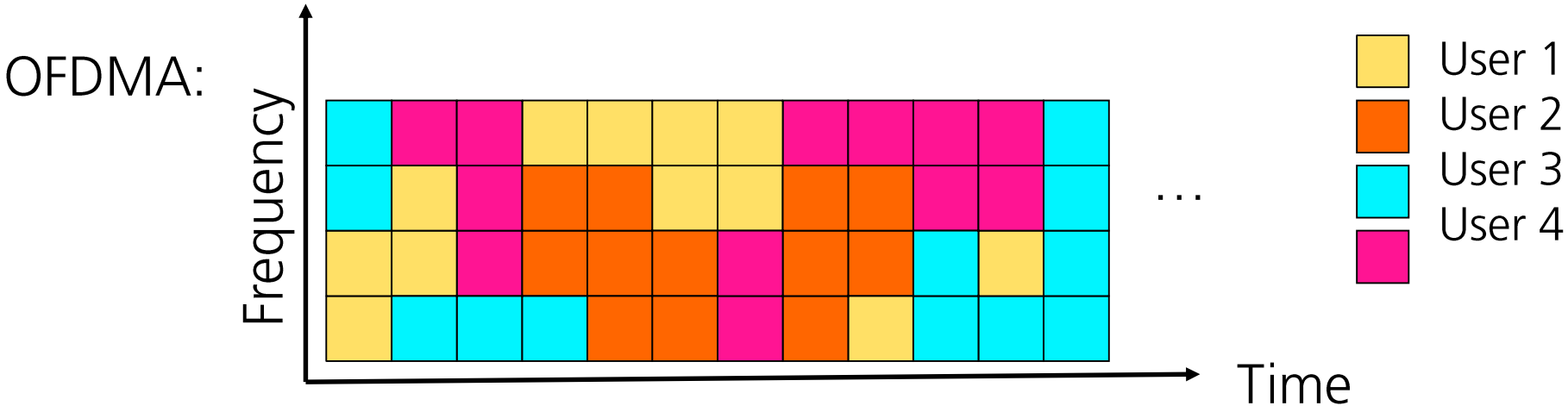
- Traffic is often tunneled over the fix network architecture
- A tunnel is a way to send packets over other types of network. E.g.
  - IPv4 over IPv6 and vice versa
  - IP over IPsec
- GTP: GPRS Tunneling Protocol

Example of tunneling

IPv4 over IPv6 using GRE (Generic Routing Encapsulation)



Time-frequecy multiple access



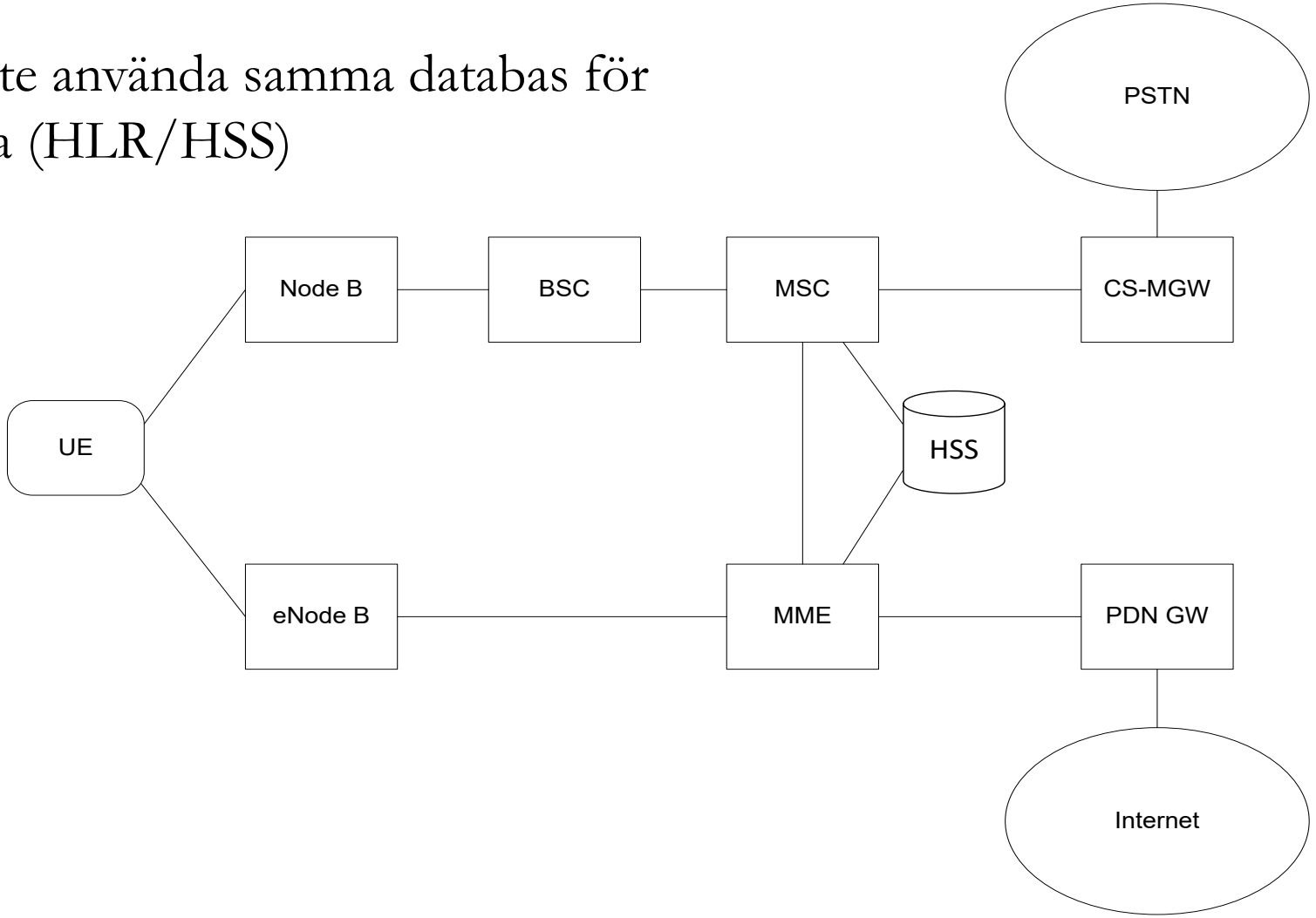
LTE uses OFDMA (Orthogonal Frequency Division Multiple Access) that is a combination of time-division and frequency-division multiple access.

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

Circuit-switched fallback

Näten måste använda samma databas för användarna (HLR/HSS)



ITU: 5G wish list / Requirements