Internetprotokollen forts.

Maria Kihl

LUND
UNIVERSITY

Repetition (ipconfig kopplad till EITs Ethernet)

Connection-specific DNS Suffix . : eit.lth.se
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : B8-6B-23-F2-88-17
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::40a8:6879:79c9:c00e%2(Preferred)
IPv4 Address. . . . . : 130.235.201.172(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : den 26 november 2018 08:36:23
Lease Expires . . . . . : den 27 november 2018 08:36:22
Default Gateway . . . . . : 130.235.200.1
DHCP Server . . . . . : 130.235.63.228
DHCPv6 IAID . . . . . : 62417699
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-92-81-0B-B8-6B-23-F2-88-17
DNS Servers . . . . . : 130.235.63.228
130.235.63.232

Tentaexempel

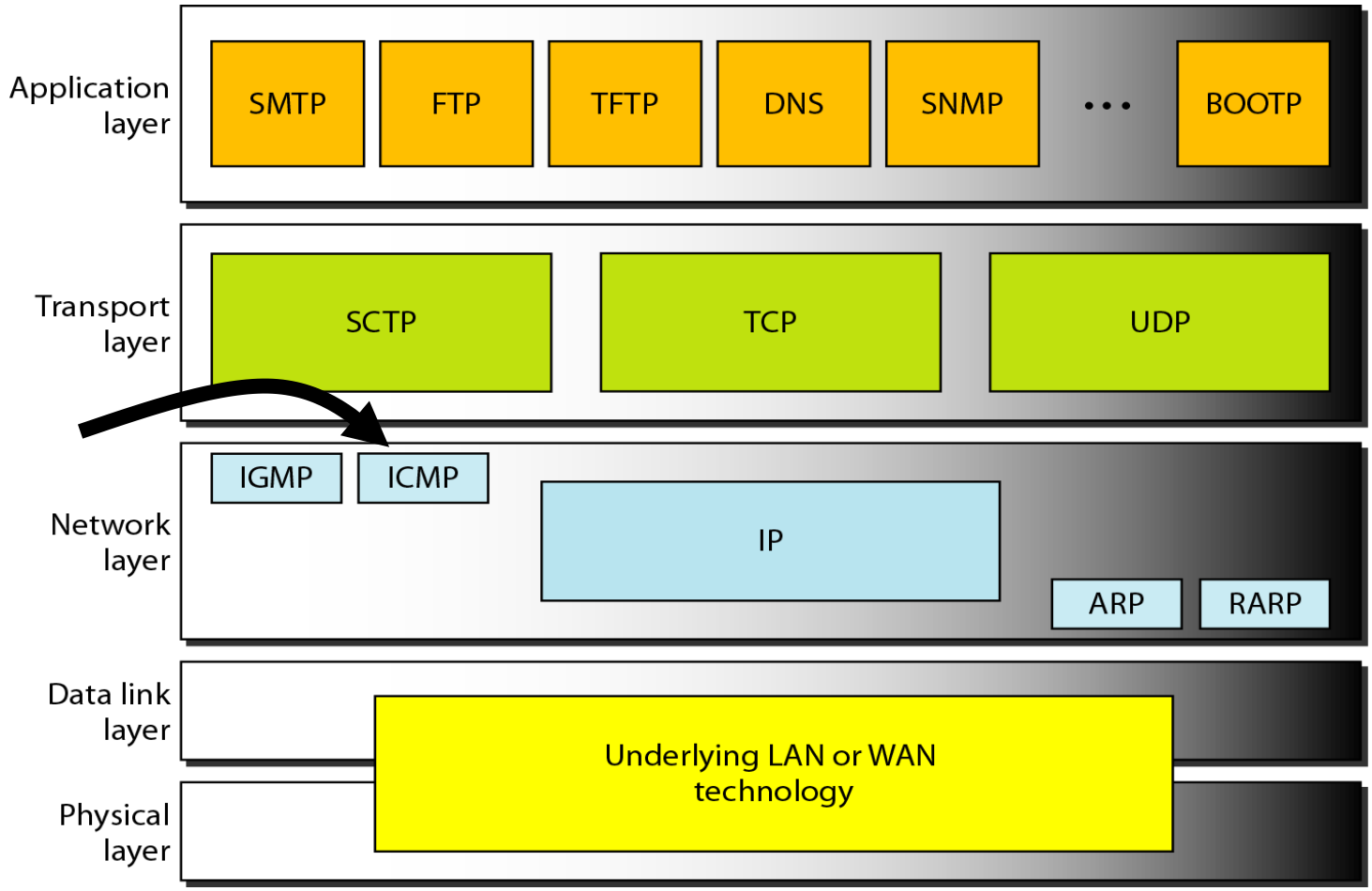
Följande Ethernet-ram bär ett TCP-segment (Preamble, SFD och CRC borttagna). Vad är destinationens portnummer?

```
00 00 0c 07 ac 01 00 08 74 41 af a7 08 00 45 00
00 30 88 14 40 00 80 06 d5 dc 82 eb 12 bd 82 eb
84 43 09 93 00 17 f2 d2 7a 29 00 00 00 00 70 02
40 00 2f a2 00 00 02 04 05 b4 01 01 04 02
```

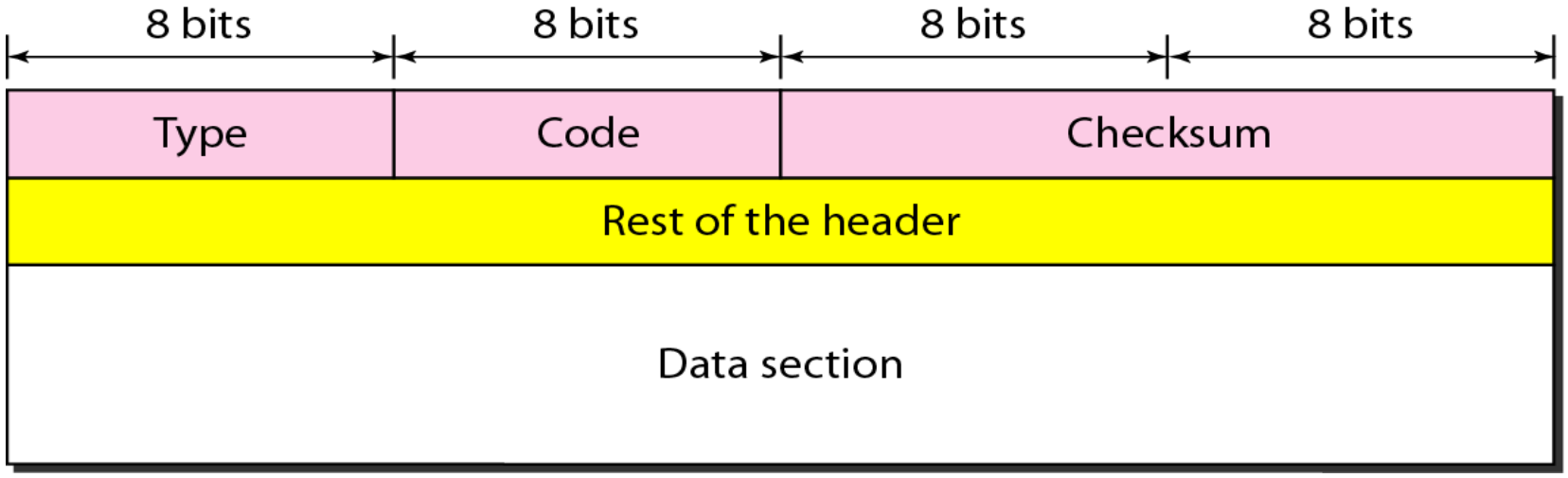
Internet Control Message Protocol (ICMP)

- 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



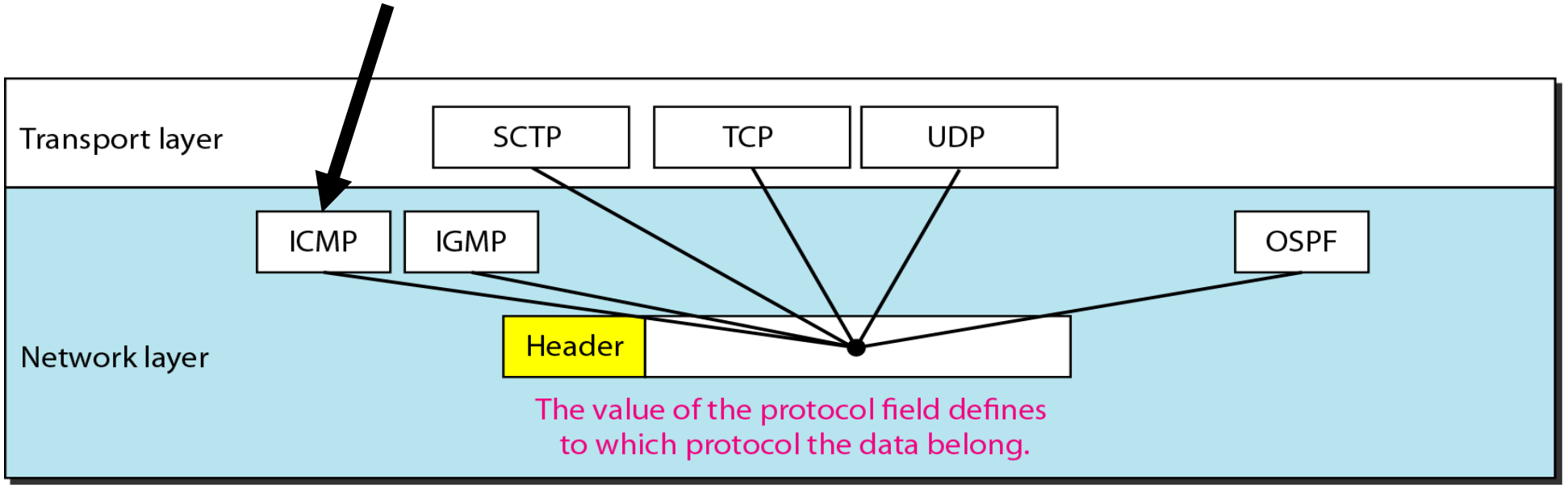
Två typer av meddelanden:

Error-reporting messages (felrapportering)

Query messages (förfrågningar)

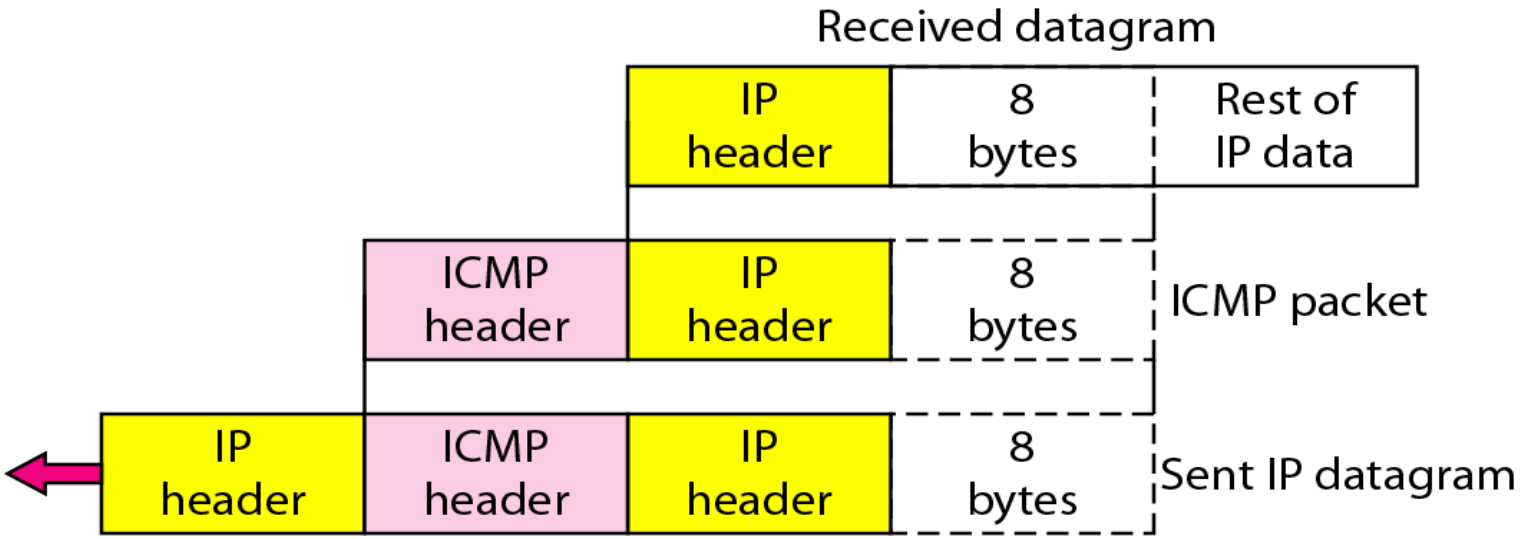
Enkapsulering (Encapsulation)

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.

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:

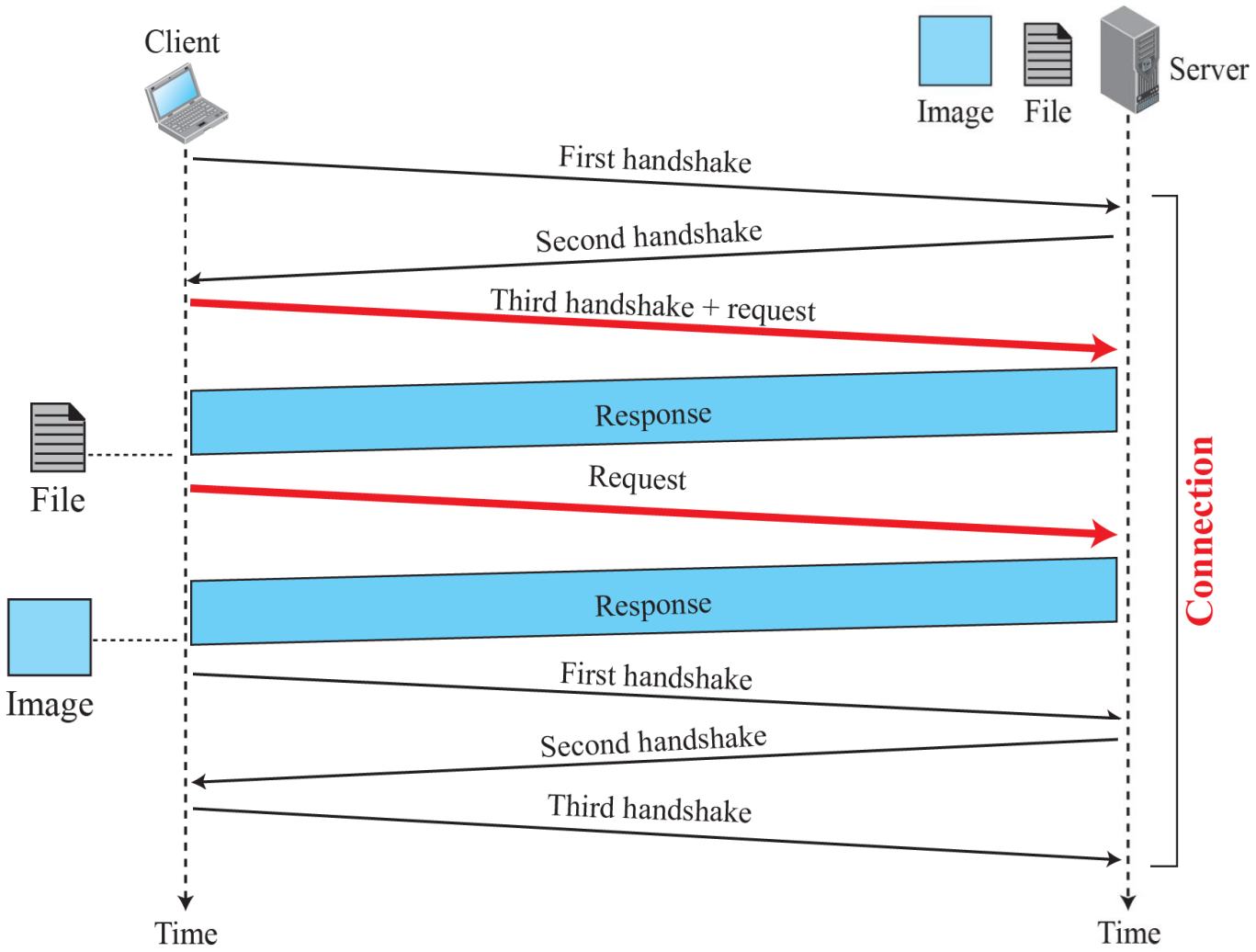
  http://www.eit.lth.se/staff/maria.kihl

- Mappning från symboliskt namn till IP-adress görs med Domain Name System (DNS).

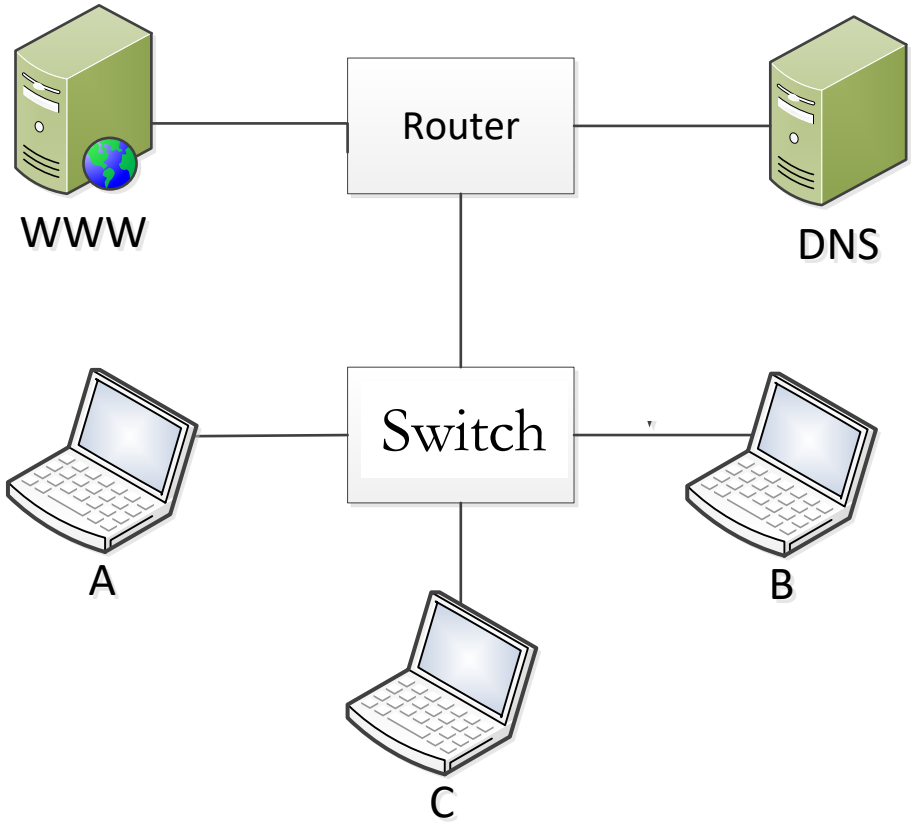
HTTP

- HTTP är ett textbaserat client/server protokoll med två typer av meddelanden: **Request** och **Response**.
- HTTP använder för närvarande TCP förbindelser för kommunikationen mellan klient och server.
- HTTP finns just nu i tre versioner:
  - HTTP/1.0 - en TCP-förbindelse (med keep-alive), en request i taget.
  - HTTP/1.1 – tillåter multipla requests till en server.
  - HTTP/2.0 – innehåller komprimering av web content
- Nästa version 3.0 kommer att använda QUIC-protokollet (utvecklat av Google). QUIC använder UDP som transportprotokoll.

HTTP kommunikation (v1.0-2.0)



Tentaexempel



Antag att A vill hämta en websida på WWW-servern och A känner endast till WWW-serverns symboliska namn (samt de IP-adresser som förutsätts i kursen). Antag att alla adress-cacher är tomma.

Beskriv vilka meddelanden som skickas i nätet samt MAC-adresser och IP-adresser för varje meddelande.

Datasäkerhet

Det finns tre viktiga koncept vad det gäller datasäkerhet:

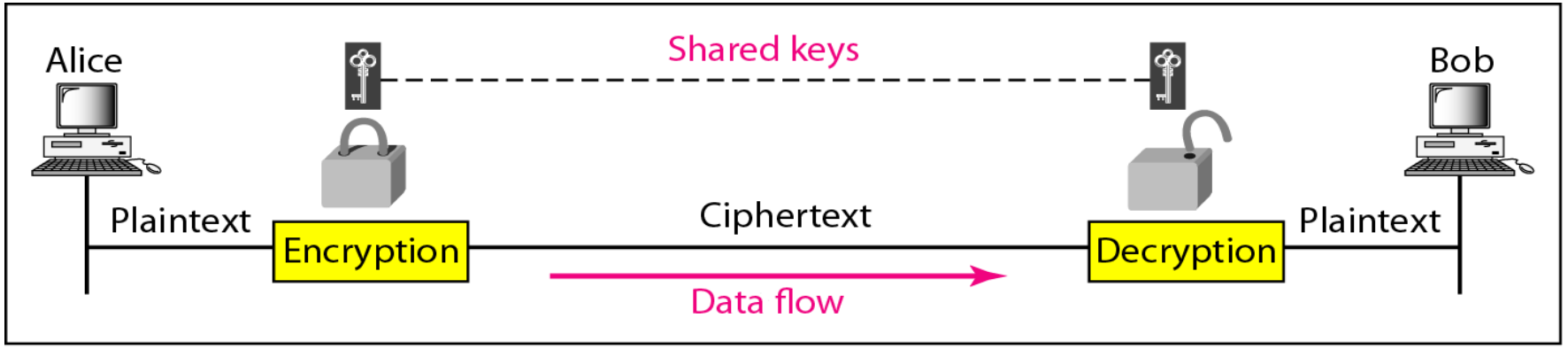
1. Skydd mot avlyssning (Privacy)
2. Skydd mot ändrad data (Integrity)
3. Autentisering (Authentication)

Skydd mot avlyssning (Privacy)

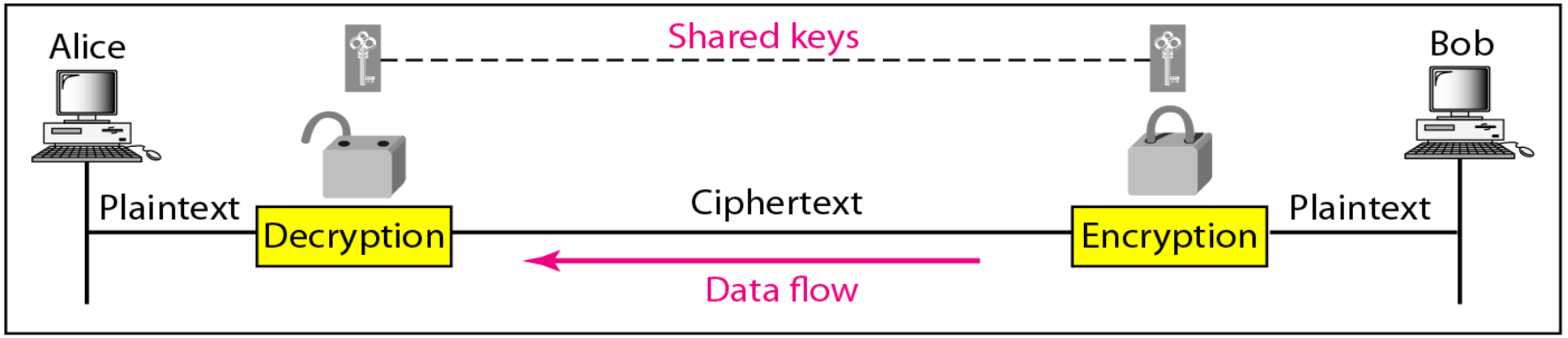
Skydd mot avlyssning (eller privacy) betyder att meddelandet som sänds endast ska kunna förstås av mottagaren. För alla andra ska meddelandet vara oförståeligt.

Privacy löses med kryptering av meddelandet.

Exempel på kryptering



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



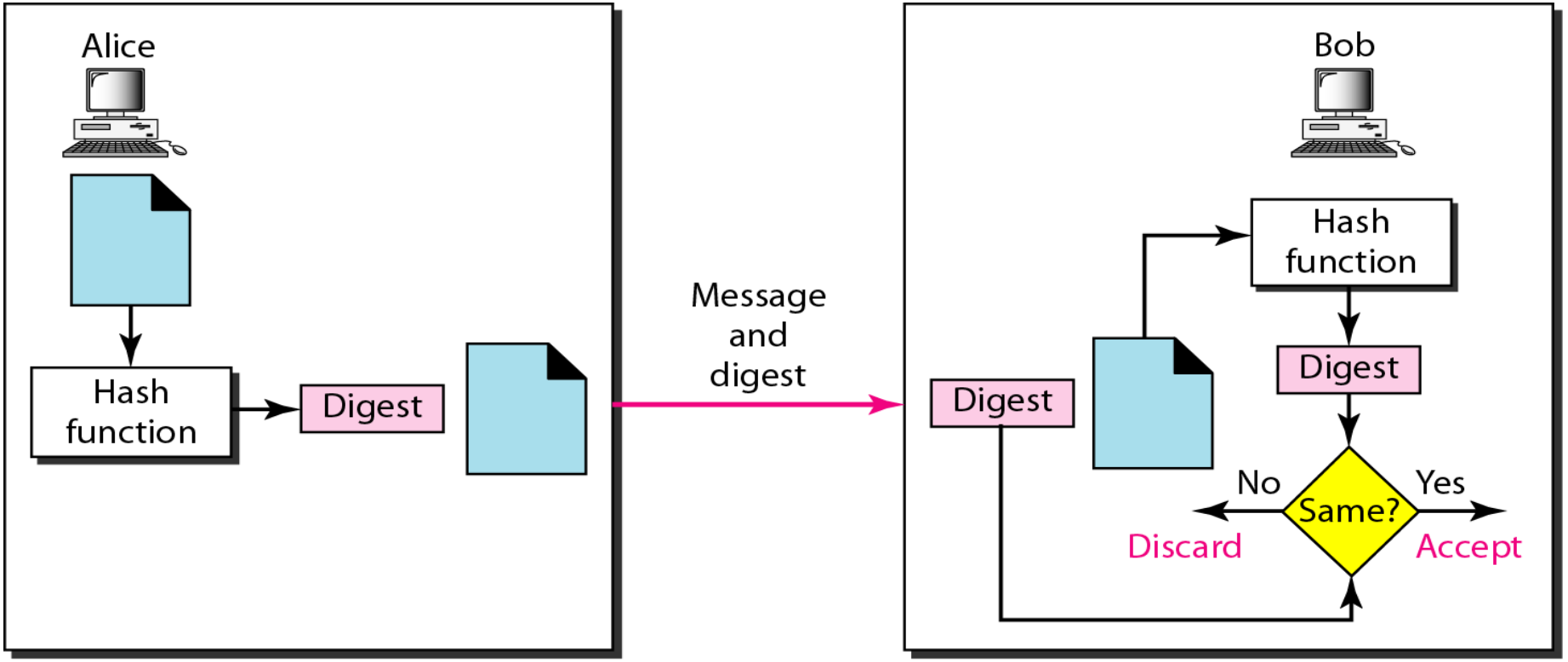
b. A different shared secret key is recommended in Bob-Alice communication

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

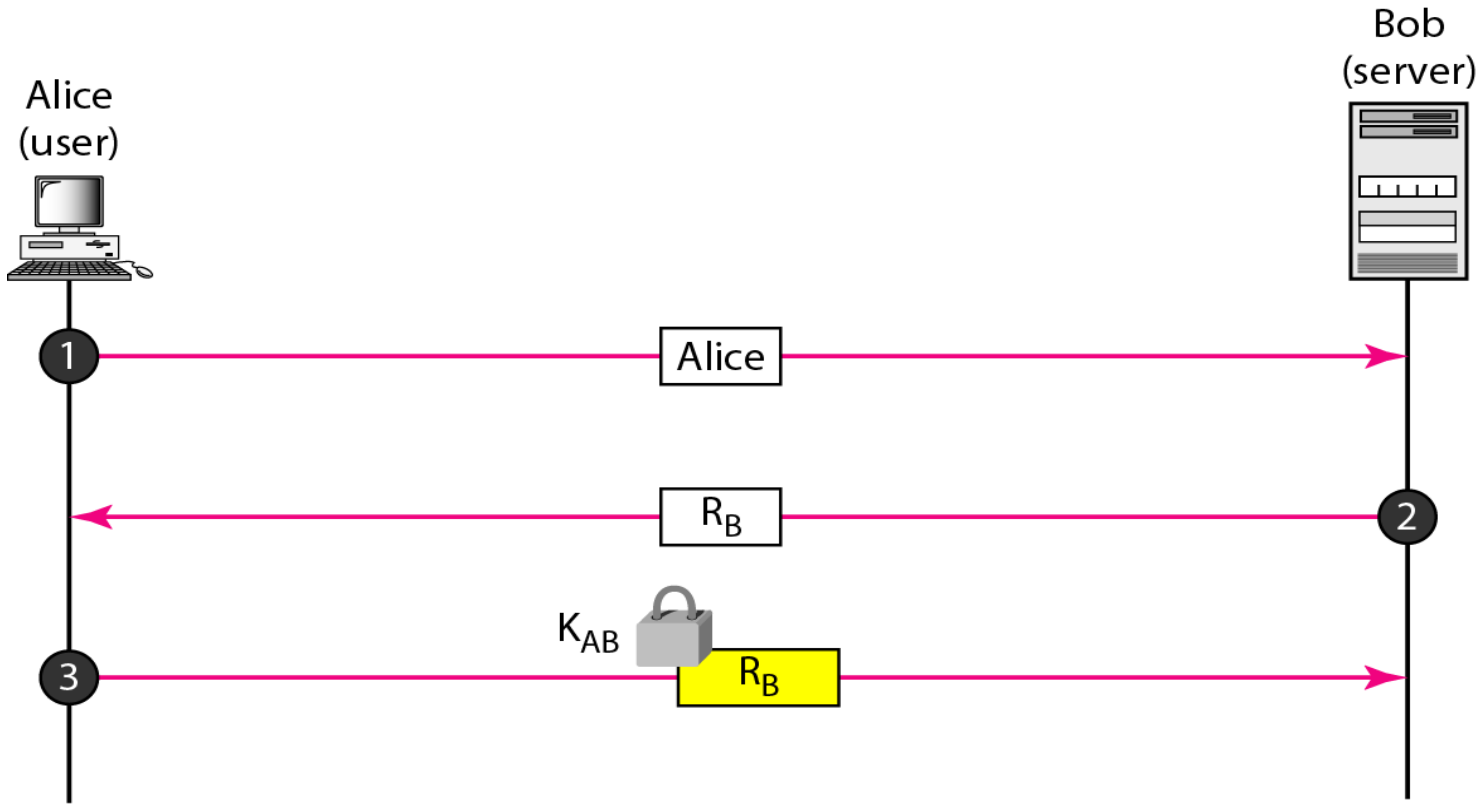


Autentisering (Authentication)

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

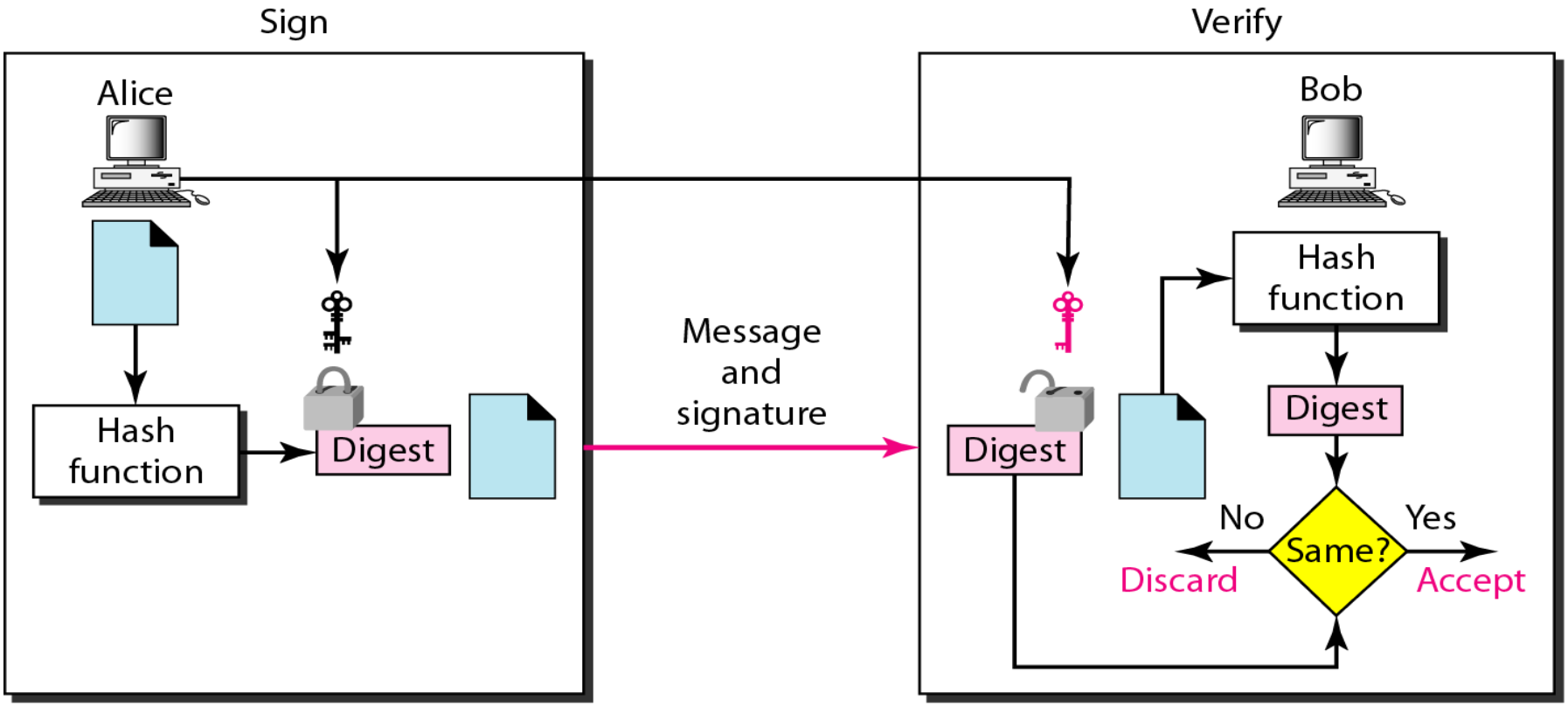
- Autentisering av enheter kan lösas med lösenord eller så kallad challenge-response.
- Autentisering av meddelanden kan tillhandahållas med en digital signatur. En digital signatur är en message digest som är krypterad.

Challenge-response



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).

Dessa protokoll kommer att gås igenom i fortsättningskursen Internetprotokoll.

HTTPS

- Utvecklades av Netscape för säkra transaktioner.
- Skickar krypterad data med TLS.
- Använder portadress 443 istället för 80 (HTTP).
- Baseras på **digitala certifikat** som webservern skapat hos en betrodd tredje part.

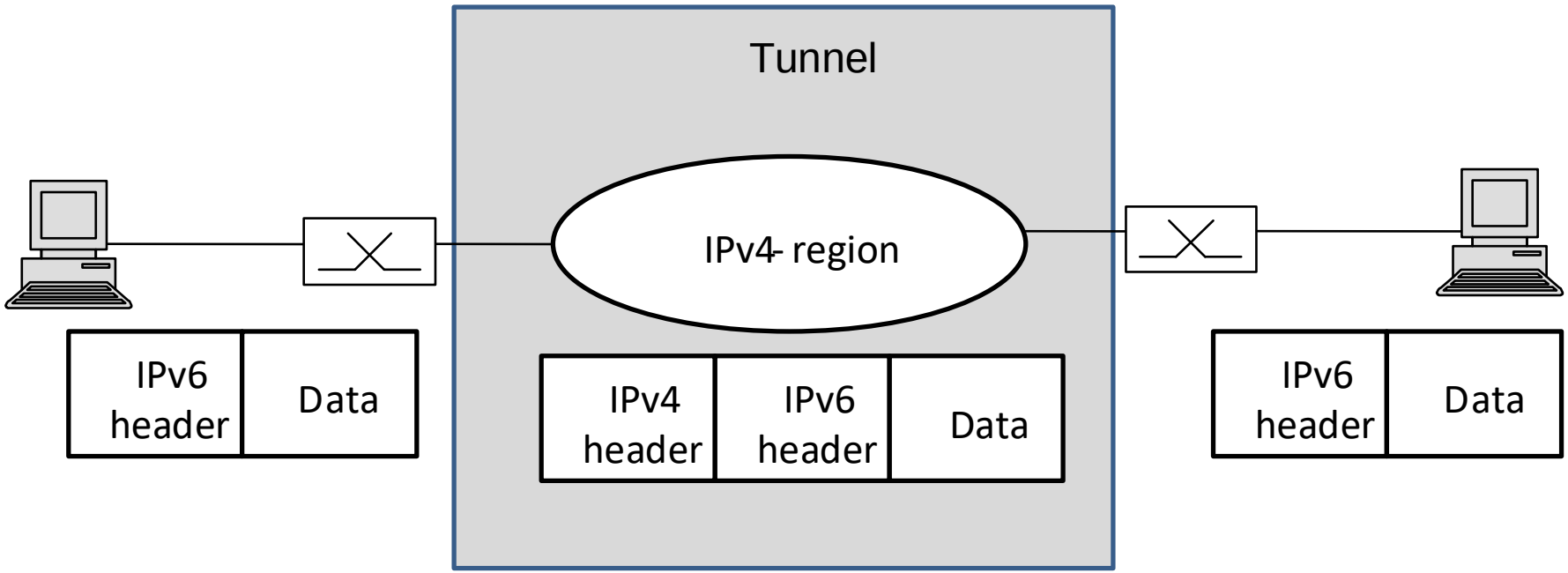
Källa: https://sv.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

Tunnling (tunneling)

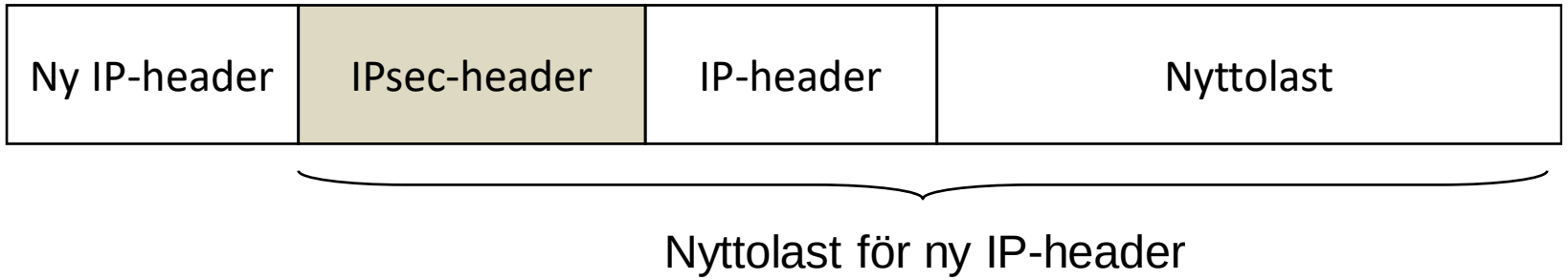
- Trafik kan tunnlas över ett nät som den del tex ett säkerhetsprotokoll.
- Exempel på när trafik tunnlas:
  - IPv6 över IPv4
  - IP över Ipsec
  - VPN (Virtual Private Network), kan tex använda IPsec

    https://sv.wikipedia.org/wiki/Virtual_private_network

Exempel på tunneling: IPv6 över IPv4



Exempel på tunnling: IP över IPsec



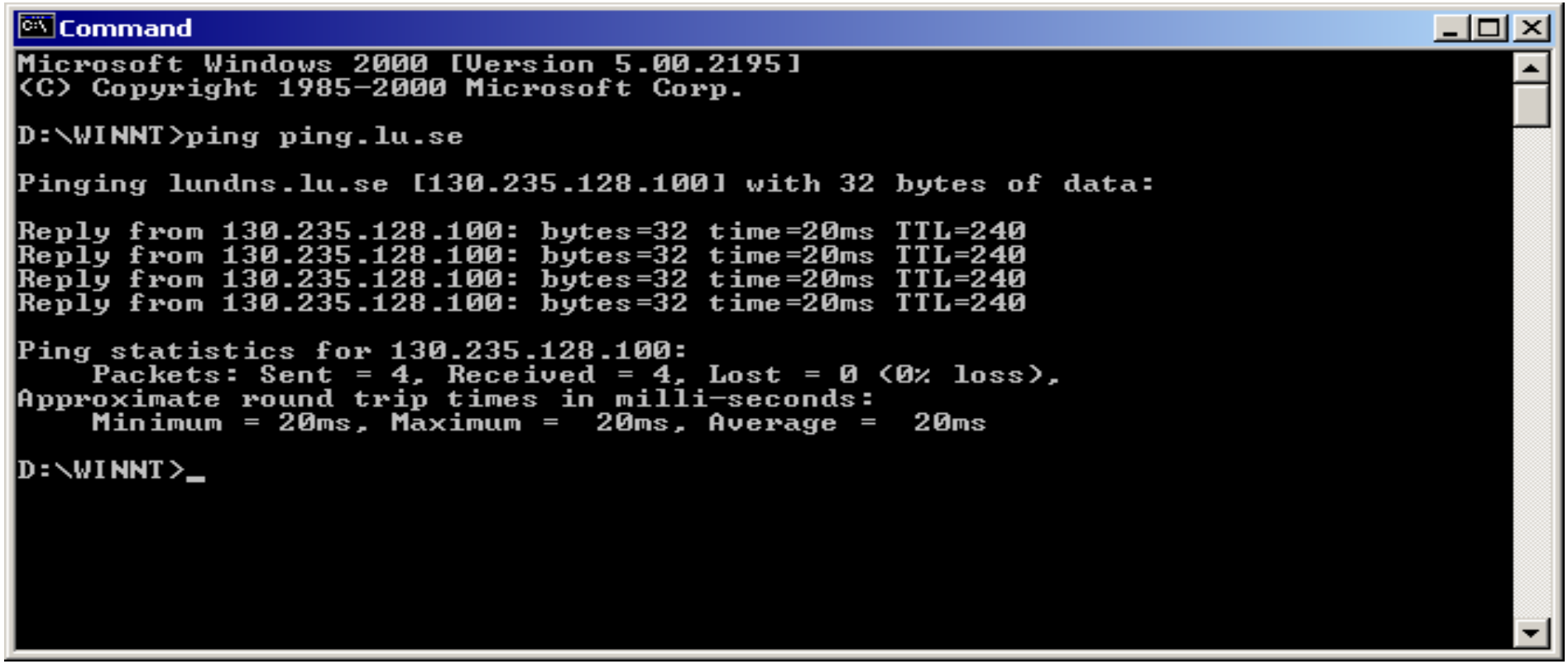
Felhanterings-verktyg (debugging tools)

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

U:\>tracert www.google.com

Tracing route to www.google.com [172.217.19.196] over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	defgw-a190.eit.lth.se [130.235.200.1]
2	9 ms	<1 ms	<1 ms	r1-f0b-vd-eit.net.lu.se [130.235.217.197]
3	<1 ms	1 ms	<1 ms	jr1a-r1a.net.lu.se [130.235.217.60]
4	14 ms	13 ms	12 ms	lund-lnd88-r1.sunet.se [130.242.6.90]
5	6 ms	1 ms	1 ms	malmo-mcen1-r1.sunet.se [130.242.4.71]
6	1 ms	1 ms	2 ms	dk-ore.nordu.net [109.105.102.122]
7	7 ms	7 ms	6 ms	de-hmb.nordu.net [109.105.97.57]
8	6 ms	5 ms	5 ms	google.ham.ecix.net [193.42.155.46]
9	17 ms	17 ms	17 ms	108.170.253.69
10	17 ms	17 ms	17 ms	216.239.63.49
11	13 ms	13 ms	13 ms	172.253.50.100
12	14 ms	16 ms	14 ms	72.14.237.99
13	13 ms	12 ms	13 ms	209.85.255.231
14	12 ms	12 ms	12 ms	108.170.241.193
15	13 ms	13 ms	13 ms	72.14.238.245
16	**14 ms**	**13 ms**	**12 ms**	**ams16s31-in-f4.1e100.net [172.217.19.196]**

Trace complete.

Traceroute example

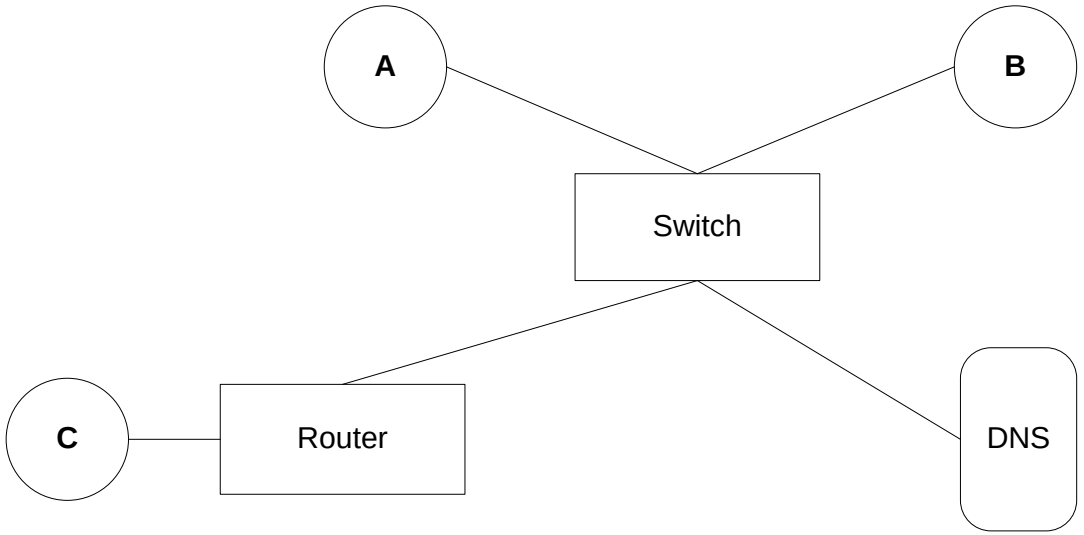
U:\>tracert www.aftonbladet.se

Tracing route to www.aftonbladet.se.cdn.cloudflare.net [104.20.54.70]
over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	defgw-a190.eit.lth.se [130.235.200.1]
2	<1 ms	<1 ms	<1 ms	r1-f0b-vd-eit.net.lu.se [130.235.217.197]
3	1 ms	<1 ms	<1 ms	jr1a-r1a.net.lu.se [130.235.217.60]
4	<1 ms	<1 ms	1 ms	lund-lnd88-r1.sunet.se [130.242.6.90]
5	2 ms	1 ms	<1 ms	malmo-mcen1-r1.sunet.se [130.242.4.71]
6	5 ms	1 ms	1 ms	dk-ore.nordu.net [109.105.102.122]
7	1 ms	2 ms	1 ms	dk-bal.nordu.net [109.105.97.117]
8	3 ms	3 ms	2 ms	as13335-10g-gc1.sthix.net [185.1.88.20]
9	**7 ms**	**2 ms**	**2 ms**	**104.20.54.70**

Trace complete.

Tentaexempel



Host A vill skicka en ICMP echo request (ping) till host C. Host A kan bara C:s symboliska namn c.citynetwork.se (samt de IP-addresser som förutsätts I kursen). Förutsätt att alla adress-cacher är tomma. Beskriv vilka meddelanden (med tillhörande addresser) som skickas i nätet ovan.

Cellulära nät och lite IoT

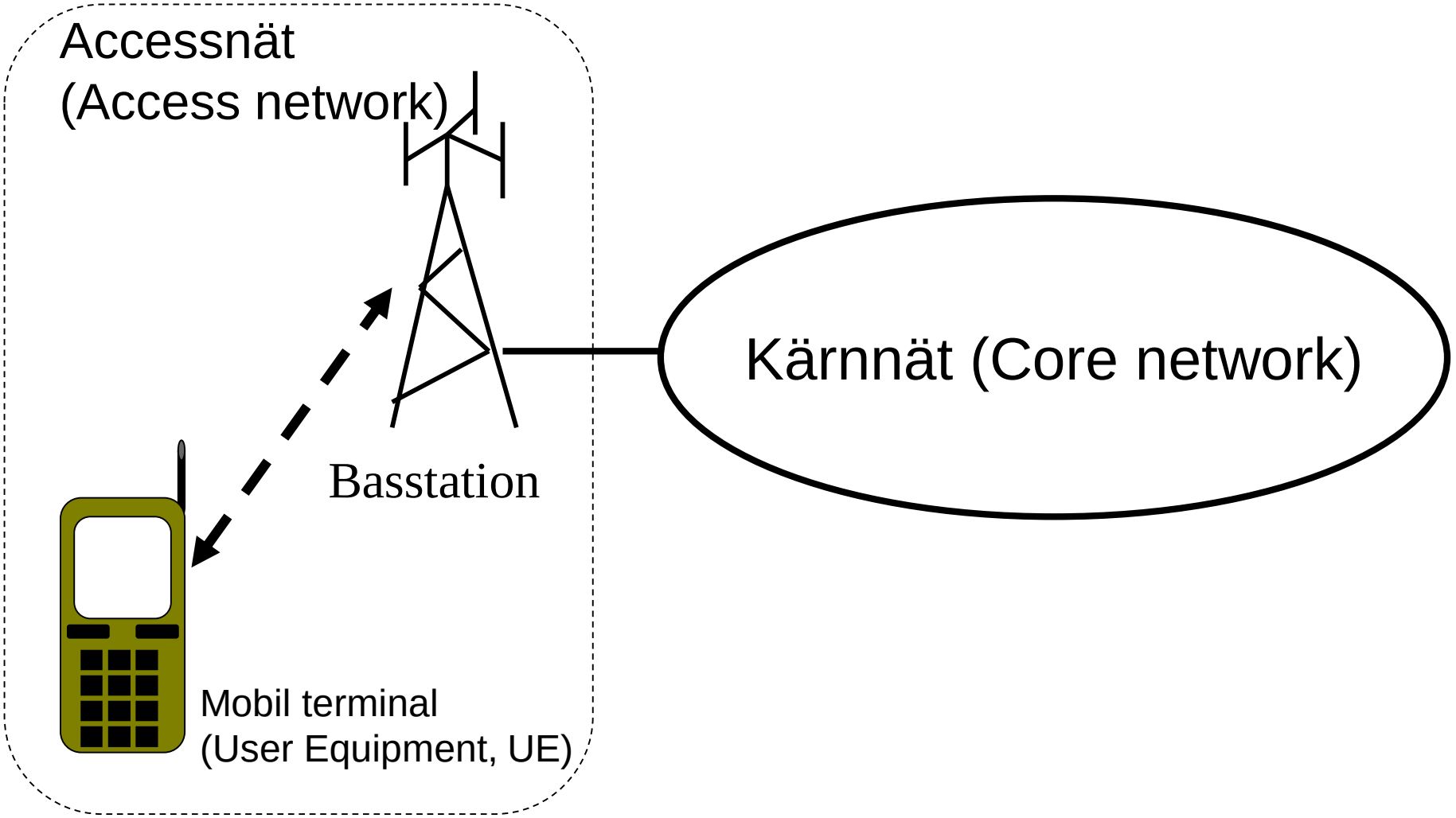
Maria Kihl

LUND
UNIVERSITY

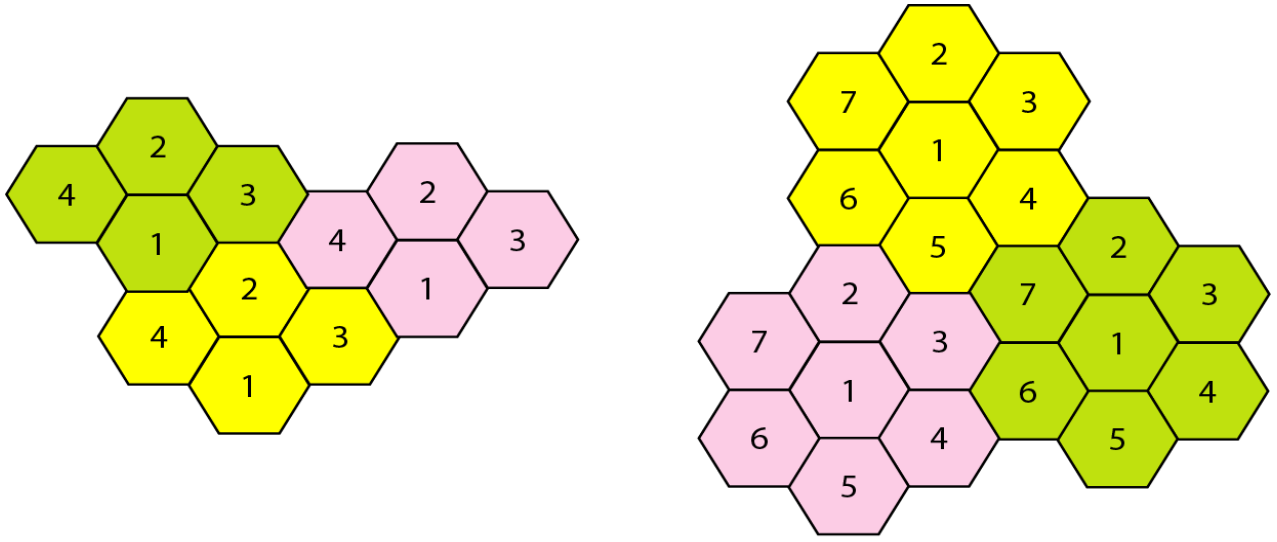
Läsanvisningar

Läsanvisningarna definieras av innehållet på slides.

Cellulära nät



Celler och frekvenser



a. Reuse factor of 4

b. Reuse factor of 7

- Ett cellulärt nät är geografiskt indelat i celler.
- Till varje cell hör en basstation.
- Varje cell får ett visst frekvensband. Frekvensbanden delas ut så att intilliggande celler inte ska störa ut varandra.

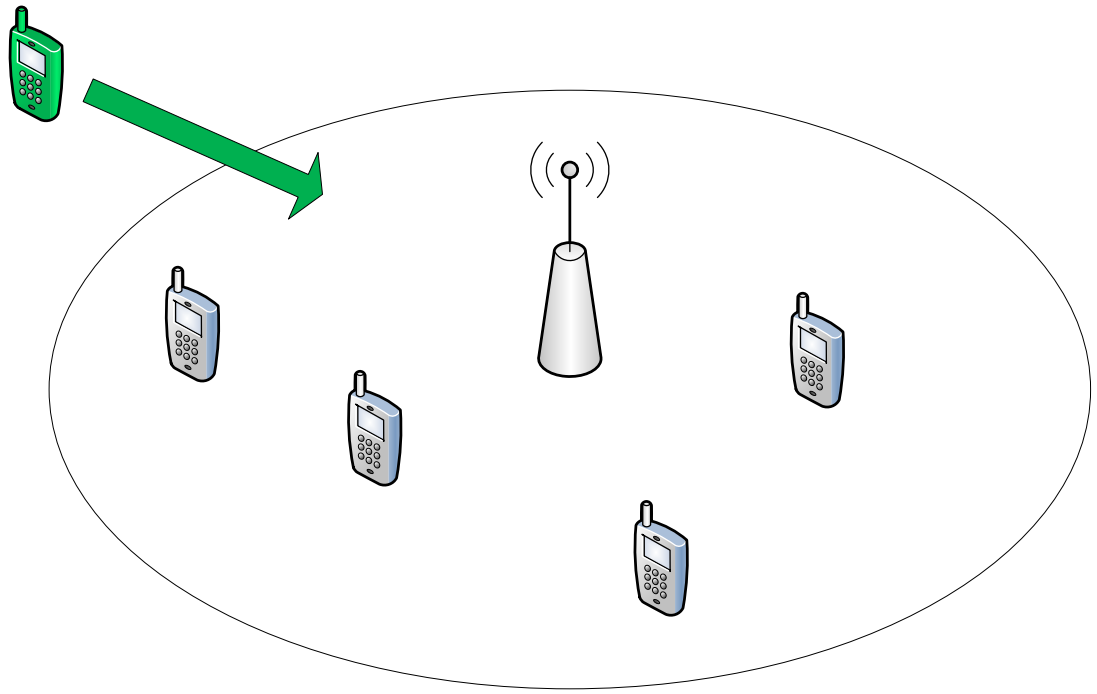
Mobiliteten måste lösas

- Signalstyrkan som en mobil terminal (User equipment, UE) skickar med kan bero på avståndet till basstationen (*power control*).
- En mobil terminal ska kunna byta cell (*handover/handoff*).
- En mobil terminal ska kunna byta nät när den flyttar sig till ett annat land. (*roaming*).

Multipel access

- Flera terminaler ska ha access till samma basstation inom samma frekvensband => Protokoll för access till mediet behövs (MAC).
- Alla cellulära nät använder ”Controlled access” metoder där basstationen bestämmer vilken kanal en terminal får använda och hur den får skicka.
  - ”Uplink” och ”Downlink”-kanaler kan använda olika metoder för kanaluppdelning.
  - Det finns vanligtvis en gemensam kanal som alla terminaler lyssnar på och där nån typ av Random access metod används.

Multipel access i mobila nät



Olika kanaler med olika MAC-protokoll

för att

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

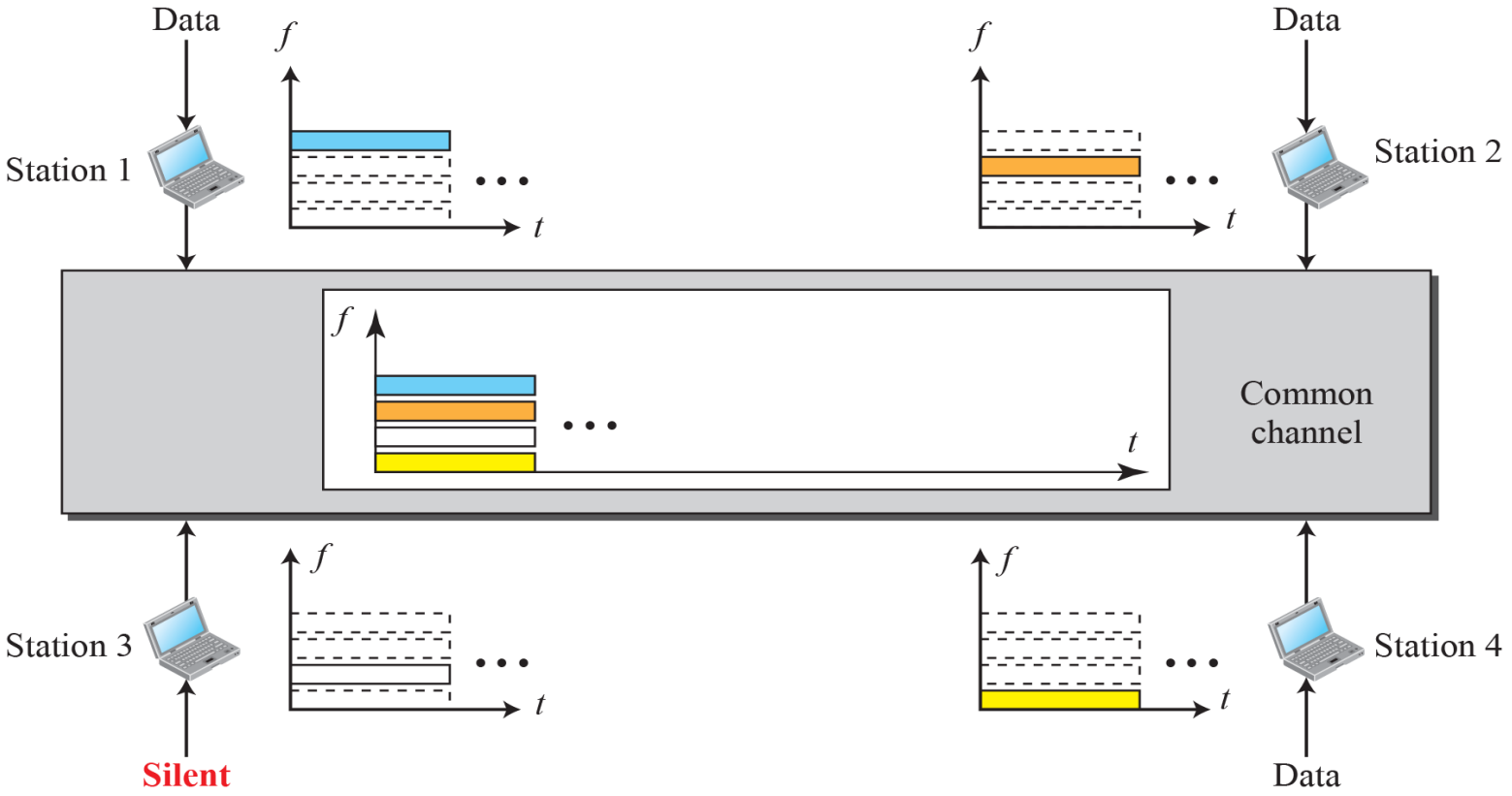
Channelization (Multiple access)

Några grundläggande channelization tekniker:

- Frequency-Division Multiple Access (FDMA)
  - Bygger på Frekvensmultiplexering.
- Time-Division Multiple Access (TDMA)
  - Bygger på tidsmultiplexering.
- Orthogonal Frequency-Division Multiple Access (OFDMA)
  - Kombinerar FDMA och TDMA.
- Code-Division Multiple Access (CDMA)
  - Bygger på Direct Sequence Spread Spectrum (DSSS)

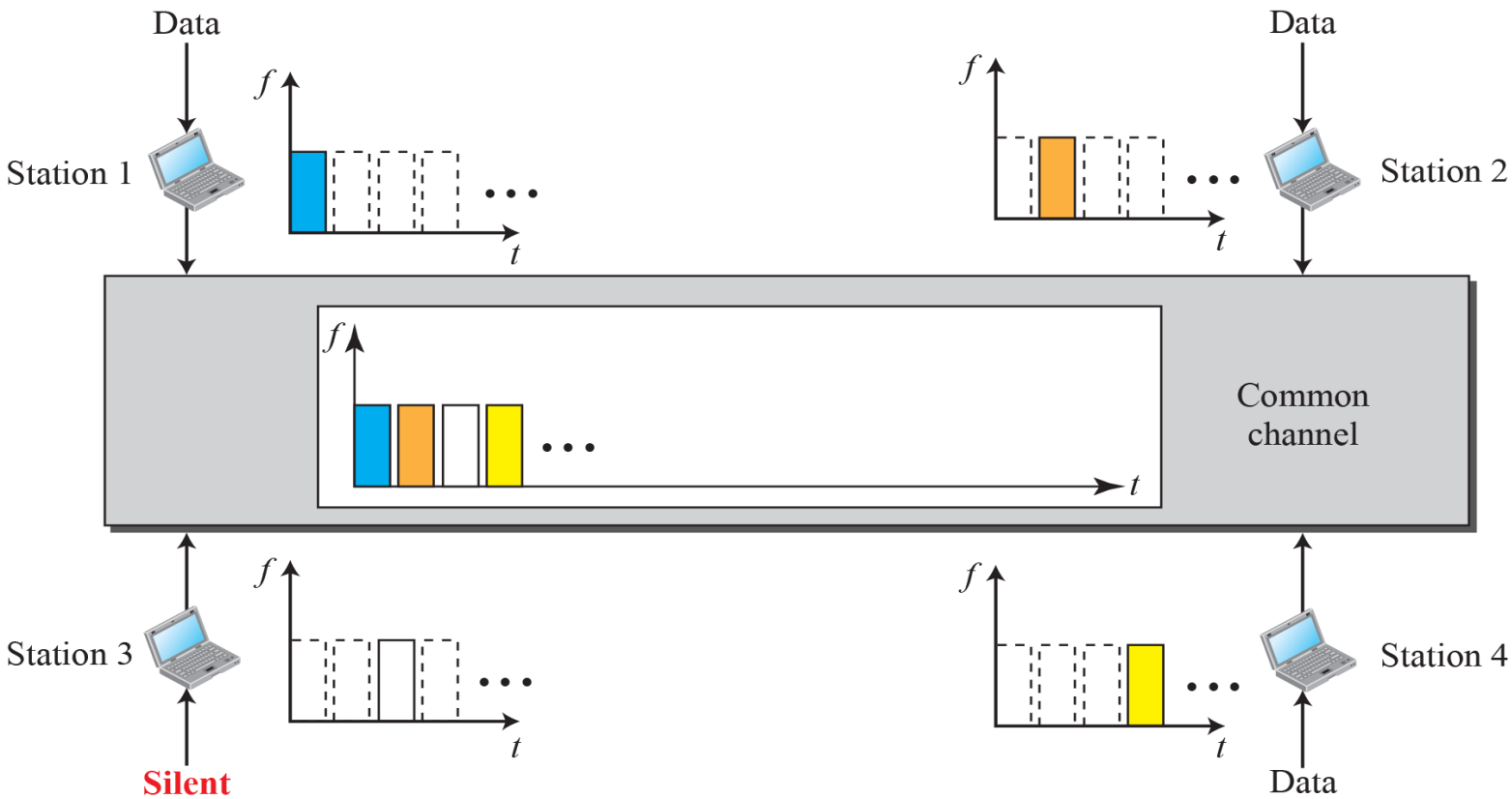
FDMA

I FDMA har alla terminaler har separata frekvensband.

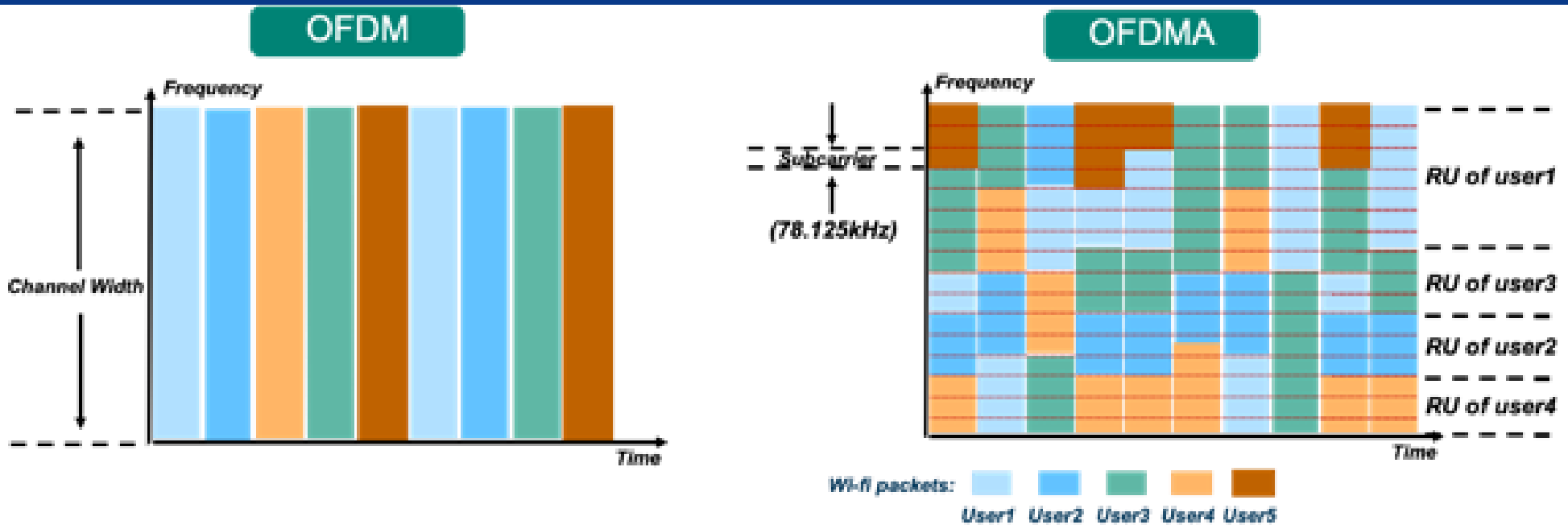


TDMA

I TDMA har varje terminal separata tidsluckor på ett delat frekvensband.



OFDMA



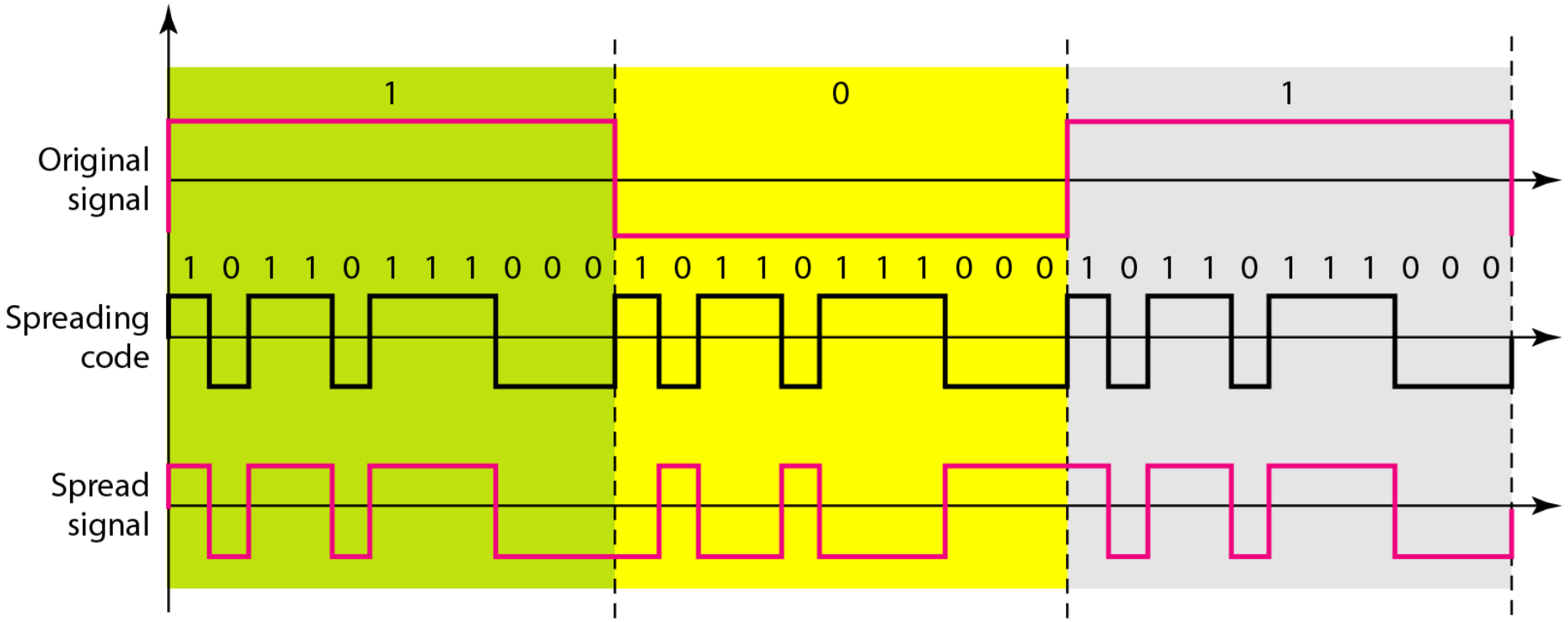
I OFDMA kombineras FDMA med TDMA. Här får varje användare ett flertal tidsluckor på flera (smala) frekvensband och data delas upp på ett intelligent sätt för att motverka störningar. Används i moderna cellulära nät och IEEE 802.11ax (WiFi 6).

Källa: https://blogs.arubanetworks.com/solutions/whats-the-difference-between-ofdma-and-mu-mimo-in-11ax/

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.

DSSS exempel



Exempel på DSSS (utan bitfel)

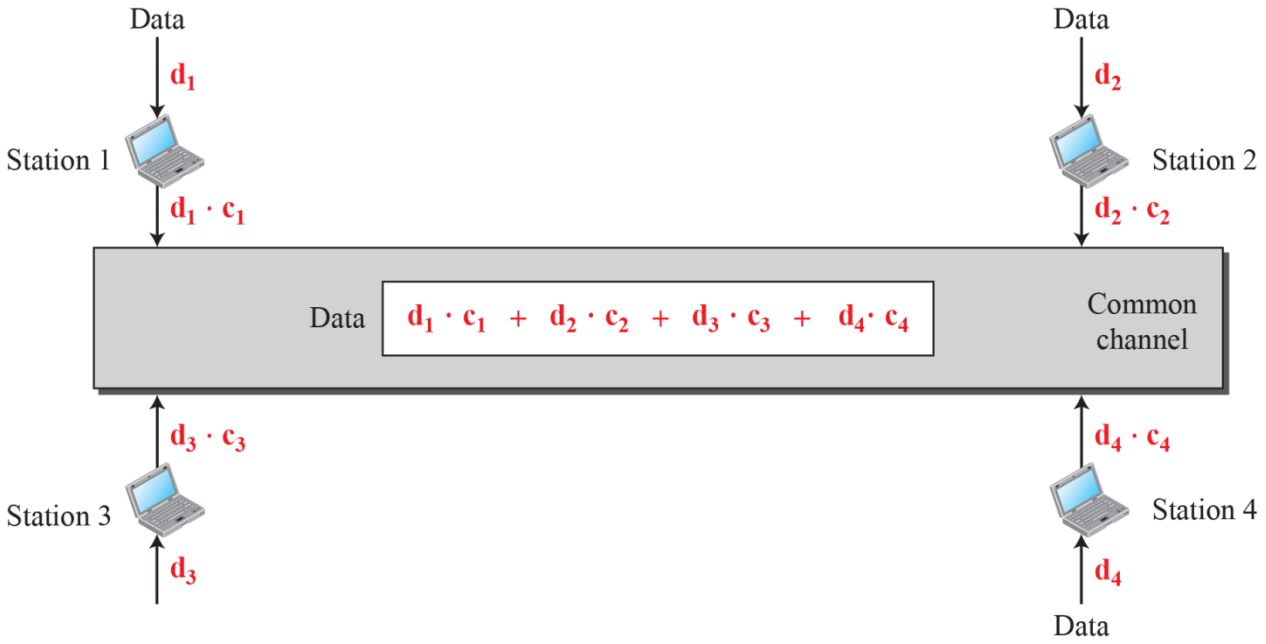
Bit som skall skickas:	0	1
Bitvis modulo-2	0000	1111
med chip-sekvens:	1110	1110
Resultat:	1110	0001
Mottagaren adderar	1110	0001
med chip-sekvens:	1110	1110
Resultat:	0000	1111
Adderas bitvis	0+0+0+0	1+1+1+1
Resultat:	0	4

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

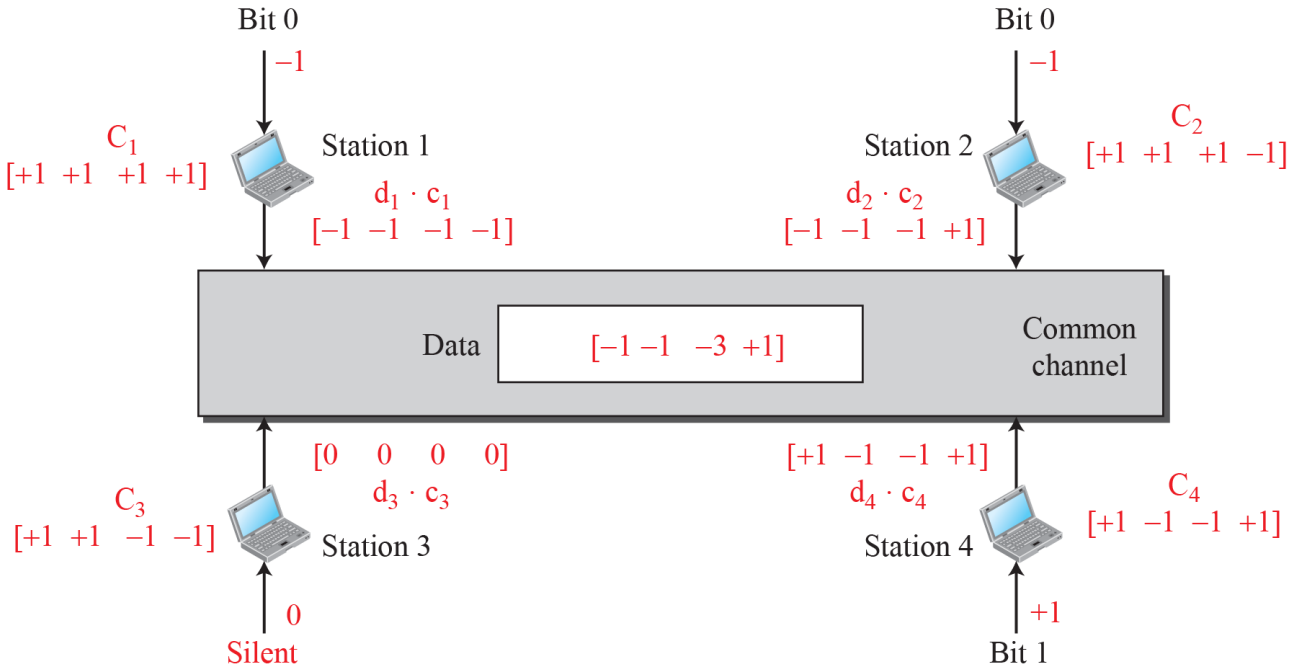
[+1 +1 –1 –1]

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.



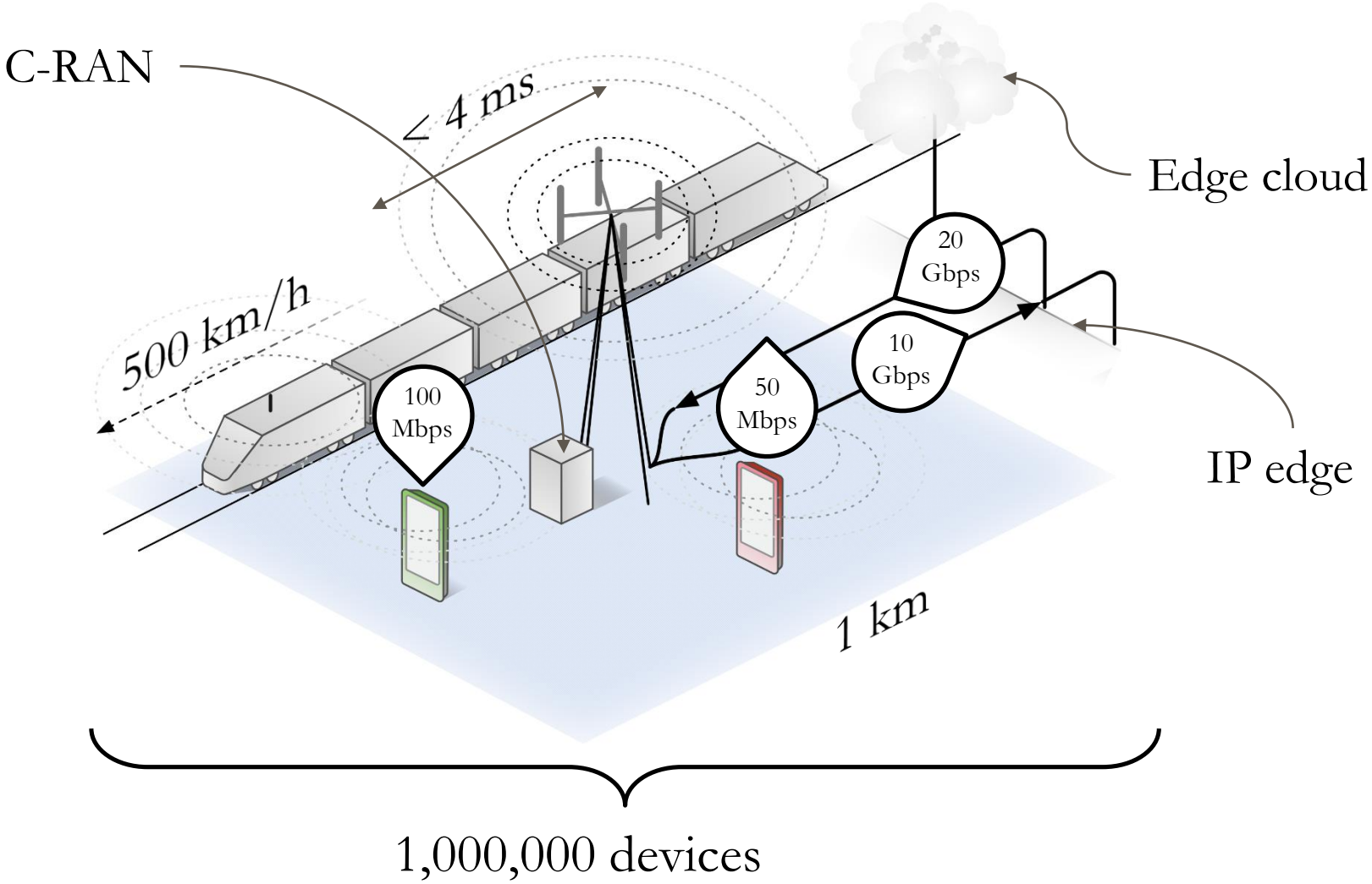
2G/3G-system

- GSM (Global System for Mobile Communication) brukar kallas för 2G.
  - GSM använder främst TDMA/FDMA.
  - Frekvensband: 900 MHz, 1.8 GHz.
- UMTS (Universal Mobile Telecommunication System) brukar kallas för 3G.
  - UMTS använder främst CDMA.
  - Frekvensband: 900 MHz (GSM), 2.1 GHz
- GSM/UMTS är utvecklade främst för telesamtal och använder liknande arkitektur för kärnnätet.

Long Term Evolution (LTE), 4G

- Skillnader jämfört med GSM/UMTS:
  - Paketkopplat nät!
  - Byggt för Internetaccess, inte telefoni!
- Frekvensband: 800MHz, 900MHz (GSM), 1.8 GHz, 2.6 GHz.
- Högre datahastigheter med OFDMA istället för CDMA.
- Kräver lösningar för telefoni
  - Circuit switched fallback: Telesamtal kopplas via 3G-nätet.
  - VoIP, typ andra Internet-appar för telefoni.
- Högre datahastighet och högre frekvenser innebär mycket mindre celler än 2G/3G.

ITU: 5G wish list / Requirements



5G-nät utmanar fiberanslutning

■ Fasta fiberanslutningar får en allvarlig utmanare när nya telenäten 5G kommer på bred front nästa år. Kapacitetsmässigt är de båda ungefär lika bra för en villaägare som står i valet och kvalet.

– Allt handlar i slutändan om hur man dimensionerar, hur många hushåll kommer att kopplas upp, säger Patrik Cerwall, chef för strategisk marknadsföring på Ericsson.

Ju fler hushåll per radiobasstation desto slöare uppkoppling.

I dag kan en fiberdragning för fast, snabbt bredband till en villa gå lös på 10 000–20 000 kronor som en engångskostnad. En ganska dyr affär, men vad som blir bäst är svårt att ge något generellt svar på, enligt Patrik Cerwall.

I dag saknar runt hälften av världens befolkning en fast bredbandsuppkoppling. Ericsson räknar i sin årliga Mobility Report med att 5G kan bli ett bra komplement för dessa.

I telekomvärlden handlar mycket om den nya generationens tele- och datanät 5G som nu kommer på bred front och som Ericsson förstås vill sälja mer av. USA ligger i front än så länge, men under 2019 räknar Ericsson med en större utbyggnad i Västeuropa och då också i Norden, även om det är teleoperatörerna som sitter på den makten.

Nya mer avancerade telefoner, inga av dagens telefoner har någon glädje av 5G, kommer att kunna erbjuda ännu fler finesser (som många kanske inte behöver och än mindre använder), varav själva uppkopplingen är en del. 5G-telefonerna väntas komma ut på marknaden andra kvartalet 2019 även om det inte är säkert att de kommer att finnas tillgängliga på den svenska marknaden, enligt Cerwall.

Huvudorsaken till 5G:s framväxt är att datatrafiken i telenäten håller på att nå taket.

– Och 5G kommer även att avlasta och ge mer utrymme i 4G-nätet, säger Cerwall. TT

OLLE LINDSTRÖM

FAKTA

5G snabbare på flera vis

■ I slutet av 2024 väntas det finnas 1,5 miljarder 5G-abonnemang. Tillväxten av 5G beräknas därmed gå fortare än vad tillväxten av 4G gjorde.

■ Mellan tredje kvartal i fjol och tredje kvartalet i år har datatrafiken i mobilnäten ökat med 79 procent, den högsta tillväxttakten på fem år.

■ I dag finns ungefär 7,9 miljarder mobilabonnemang, fler än vad det finns människor i världen. Men många är inaktiva. Antalet abonnenter beräknas uppgå till omkring 5,6 miljarder.

■ Källa: Ericsson Mobility Report

Frekvensband för 5G

Radio Spectrum Policy Group (RSPG), är rådgivande till EU-kommissionen i spektrumfrågor, och de föreslår tre pionjärband för att möjliggöra 5G.

- 700 MHz för där stor yttäckning skall nås
- 3.4-3.8 GHz för kapacitetskrävande tjänster i stad och tätort
- 26 GHz för extremt höga datahastigheter (mm-wave)

Källor: https://www.induo.com/5g-fakta/
https://www.pts.se/sv/nyheter/radio/2017/pts-nu-finns-tillgangligt-utrymme-for-5g-tester-i-sverige/

Användarscenarios (User scenarios) för 5G

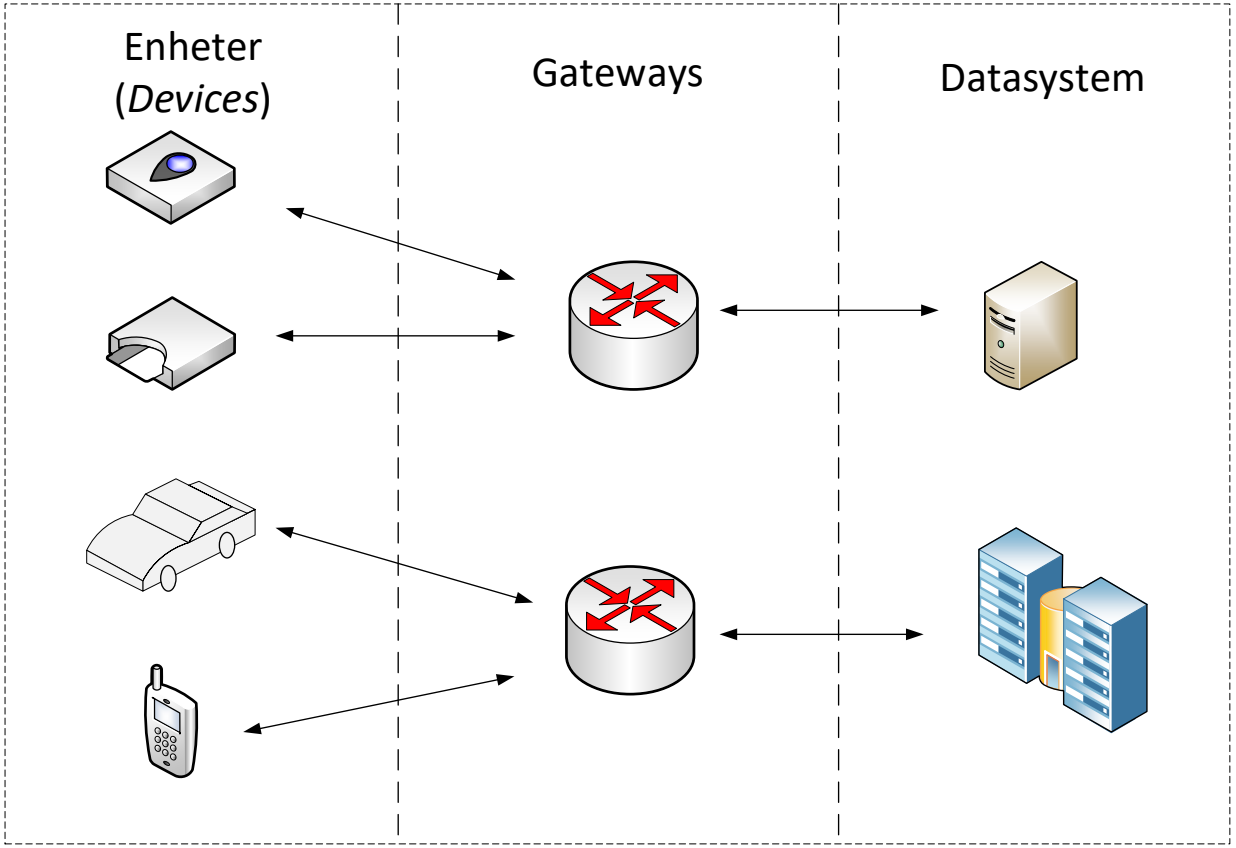
- **Enhanced Mobile Broadband (eMBB):** ”Vanligt” användande, med högre datahastighet.
- **Ultra-reliable Low Latency Communication (URLLC)**: För extremt tidskritiska applikationer, till exempel ”Control over the cloud” och självkörande bilar.
- **Massive Machine Type Communication (mMTC)**: Riktat mot Internet of Things (IoT).
- 5G ska kunna ha 1 miljon uppkopplade enheter per kvadratkilometer med fördröjningar på millisekund-nivå för att möjliggöra URLLC- och IoT-applikationer.

Internet of Things (IoT)

Väldigt brett område som idag saknar gemensamma standarder. Två typer av IoT-system med standarder:

- Low-Power Wide Area Networks (LPWAN)
  - System som ska kunna skicka med låg datahastighet över stora avstånd med extremt låg energiförbrukning.
  - Exempel: LoRaWAN, NB-IoT (föreslaget för mMTC i 5G)
- Personal Area Networks (PAN)
  - System som kopplar ihop enheter på väldigt korta avstånd.
  - Exempel: Bluetooth, Zigbee

Generell arkitektur för LPWAN



NB-IoT: Basstationen är gateway.

Utmaning: Applikationens enheter ska ha så låg energiförbrukning som möjligt.

Några tekniker för låg energiförbrukning

- Ultra-low power electronics: Elektronik med extremt låg energiförbrukning.
- Sleep-metoder: Enheter ”sover” när de inte behövs.
- Energy harvesting: Enheter kan hämta energi från omgivningen (sol, vibrationer, magnetfält etc).
- Data aggregation and edge clouds: Genom att data aggregeras på intelligent sätt och sedan behandlas i edge clouds (distribuerad moln-kapacitet i tex gateways) kan enheterna spara energi.