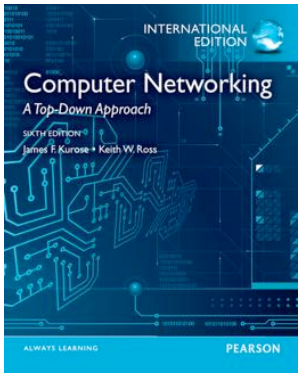
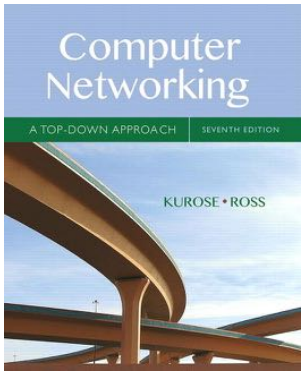
Wireless & mobile networks

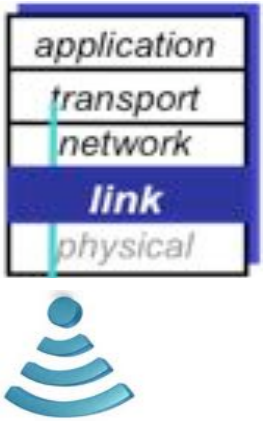
Chapter 6 (6ed) /7 (7ed)

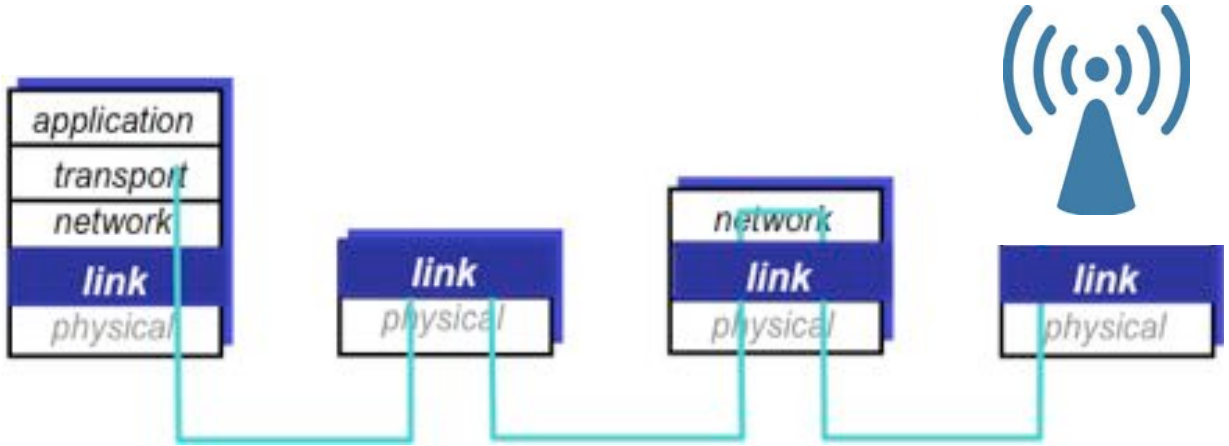
Kjersti Moldeklev, Prof II
Department of Information Security and Communication Technology

kjersti.moldeklev@ntnu.no









The content of many of these slides are based on slides available from the web-site of the book by J.F Kurose and K.W. Ross.

Wireless networks, March 9 and 10

9	**NOTE:**	**No lectures from textbook in week 9.**			
9-10	Mon – Fri 08:15 – 16:00	Project design (KTN1)	P15 - Rall	Assistants/ Norvald	
10	Thursday 12:15 – 14:00	Wireless Networks	R1	Kjersti	Chapter 6
	Thursday 14:15 – 15:00	Theory Assignment 5: *Link Layer*	R1	Assistants/ Ida/Norvald	One must deliver and pass at least 5 of the 8 theory assignments.
10	Friday 09:15 – 11:00	Wireless Networks (cont)	R1	Kjersti	Chapter 6 Chapter 8.8 and 8.8.1
10	**Friday 16:00**	**Deadline** for KTN1 – Project Design		Assistants/ Magnus	Show project design to course assistants for approval, at P15.
11-12	Mon – Fri 08:15 – 16:00	Project implementation (KTN2)	P15 - Rall	Assistants/ Norvald	
11	Thursday 12:15 – 14:00	Multimedia Networking	R1	Kjersti	Chapter 7

NTNU

Chapter 5

The data link layer - wireless

Goals

- understand principles behind data link layer services
  - how **wireless links** differ from wired
  - sharing a radio broadcast channel: **multiple access**
  - **WLAN link layer addressing**
- An overview of network soup ingredients
  - IEEE 802.11 a/b/g/n/ac
  - Mobile 2G (GSM), 3G (UMTS), 4G (LTE)
- Securing Wireless LANs

Wireless networks: Roadmap

6.1 Introduction

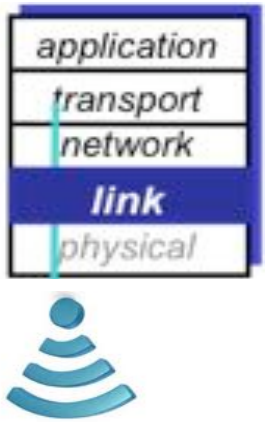
6.2 Wireless links, characteristics
- ~~Code division Multiple Access (CDMA)~~

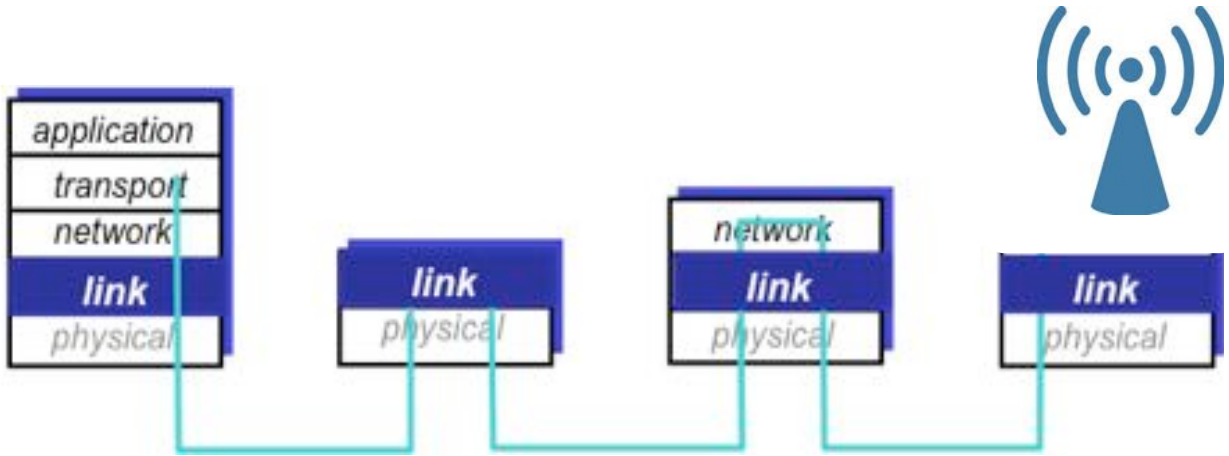
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet Access
- architecture
- standards

8.8 Securing Wireless LANs

8.8.1 Wired Equivalent Privacy





NTNU

Abbreviations in this slide deck...

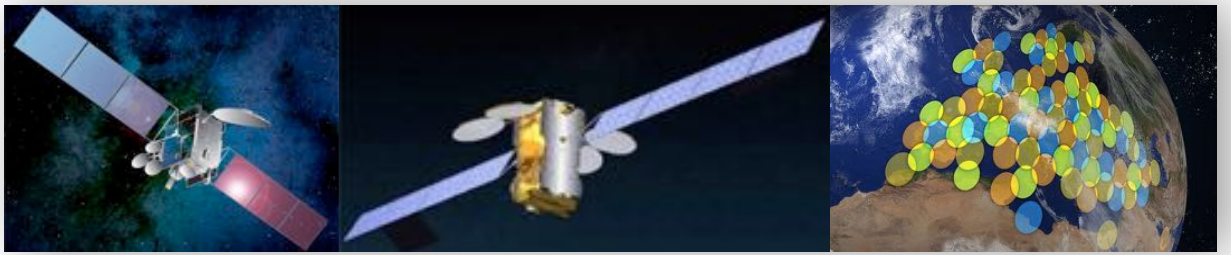
- LAN Local Area Network
- NIC Network interface card
- CPU Central Processing Unit
- MAC Medium Access Control
- TDMA Time Division Multiple Access
- FDMA Frequency Division Multiple Access
- OFDMA Orthogonal Frequency Division Multiple Access
- DSSS direct sequence spread spectrum
- FHSS frequency-hopping spread spectrum
- HR-DSSS High Rate direct sequence spread spectrum using the long preamble and header
- WLAN Wireless LAN
- AP access point
- EIRP Equivalent Isotropic Radiated Power
- CSMA Carrier Sense Multiple Access
- CSMA/CA CSMA/Collision Avoidance
- ECRC Cyclic Redundancy Check

- IP Internet Protocol
- UDP User Datagram Protocol
- Transmission Control Protocol
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System
- FCS frame check sequence
- SSID service set identifier
- BSSID Basic service set identifier
- ESS extended service set
- MIMO multiple input, multiple output
- GSM Global System for Mobile Communications
- GPRS general packet radio service
- HSDPA UL/DLHigh Speed Data Packet Access UpLink/DownLink

Unguided physical media

Radio signals are carried within the electromagnetic spectrum

- no physical “wire”
- bidirectional
- propagation environment effects
  - reflection
  - obstruction by objects
  - interference
- wireless LAN
  - e.g. 11, 54, 300, 600, 750 Mbps
- terrestrial point-to-point microwave
  - e.g. up to 45 Mbps channels
- wide-area (e.g. cellular)
  - 3G: few Mbps, LTE: 100-1000 Mbps
- satellite
  - kbps to 50 Mbps channels
  - delay geostationary 250-280 msec
    low-earth orbit 20-25 msec

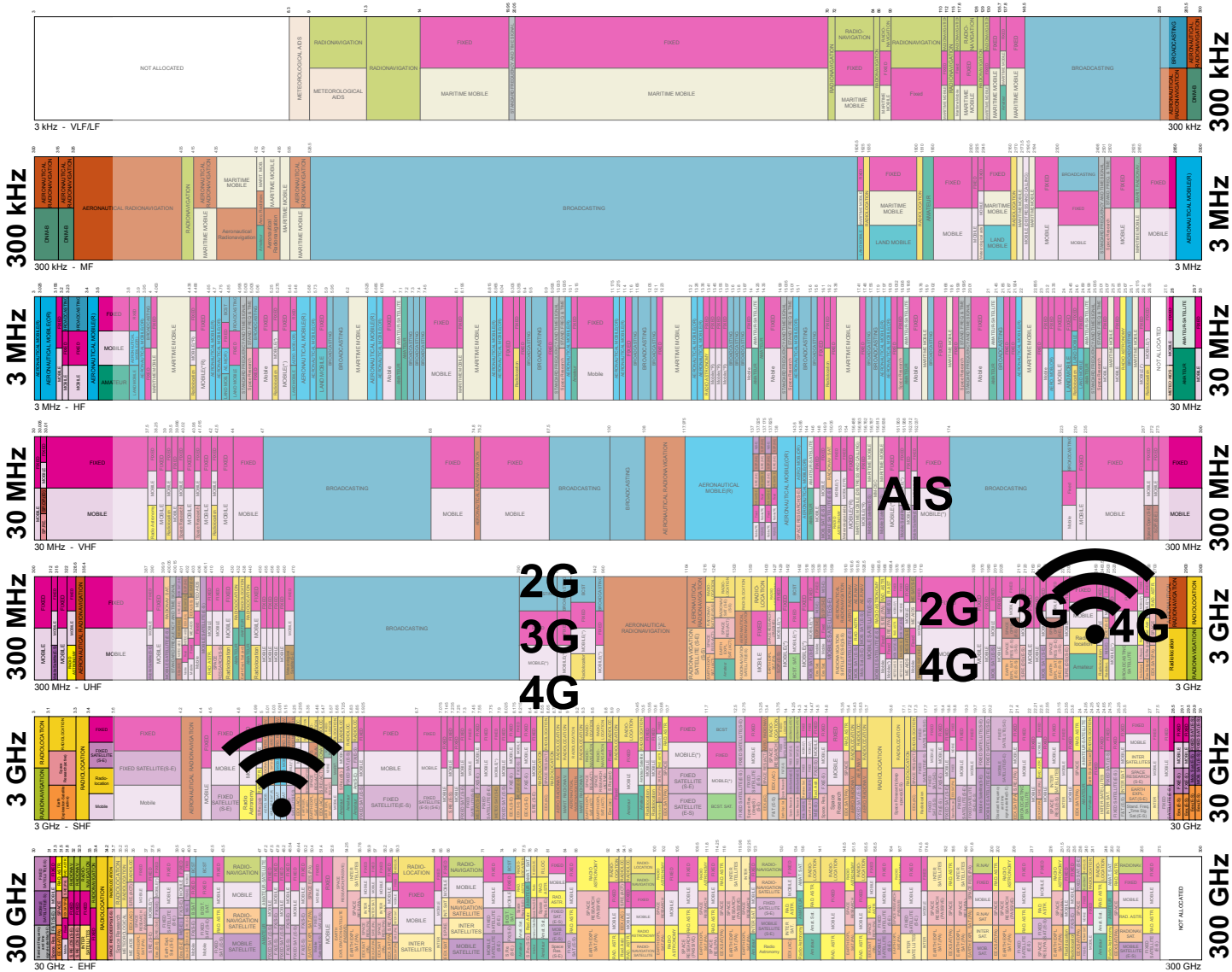


FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

WLAN
unlicensed

2G/3G/4G
licensed



http://http://www.nkom.no/teknisk/frekvens/frekvensstrategi-og-frekvensplan/informasjon-om-nasjonal-frekvensplan

The radio spectrum: A shared resource

2400-2483,5 MHz og 5 GHz allokeringer – ingen lisens påkrevd

2400.0 MHz - 2483.5 MHz	Nasjonal	Non-specific SRDs Short Range Devices	Nkom-Fribruksforskrift	9999999	2099-12-31
2400.0 MHz - 2483.5 MHz	Nasjonal	Radiodetermination applications	Nkom-Fribruksforskrift	9999999	2099-12-31
2400.0 MHz - 2483.5 MHz	Nasjonal	Radio LANs	Nkom-Fribruksforskrift	9999999	2099-12-31
2446.0 MHz - 2454.0 MHz	Nasjonal	RFID Radio Frequency IDentification	Nkom-Fribruksforskrift	9999999	2099-12-31

Frekvensområde	Geografisk område	Bruksvilkår	Innehaver	Tillatelsesnummer	Utløper
5.4 GHz - 5.85 GHz	Nasjonal	Defence systems	Forsvaret	1003425	2030-12-31
5.0 GHz - 6.0 GHz	Nasjonal	GPR/WPR Ground- and Wall-Probing Radar	Nkom-Fribruksforskrift	9999999	2099-12-31
5.725 GHz - 5.795 GHz	Nasjonal	Radio LANs	Nkom-Fribruksforskrift	9999999	2099-12-31
5.725 GHz - 5.795 GHz	Nasjonal	Point-to-Point	Nkom-Fribruksforskrift	9999999	2099-12-31
5.725 GHz - 5.875 GHz	Nasjonal	Non-specific SRDs	Nkom-Fribruksforskrift	9999999	2099-12-31

http://frekvens.nkom.no/Frekvensportalen/index.xhtml

Ulisensierte frekvensbånd

Forskrift om generelle tillatelser til bruk av frekvenser (fribruksforskriften)

§ 1. ***Stedlig virkeområde*** Forskriften gjelder ikke for frekvenser i området 2 GHz–32 GHz i det geografiske området innenfor en radius av 20 km fra Ny-Ålesund sentrum

Kap. IV. Dataoverføring

- ***§ 11.Trådløse nettverk***
- (1) **Frekvensbåndet 2400,0–2483,5 MHz** tillates brukt til dataoverføring med frekvenshopping (FHSS) (frequency-hopping spread spectrum) som interferensreduserende tiltak som beskrevet i standarden EN 300 328. Maksimal tillatt utstrålt effekt er 100 mW e.i.r.p. og 100 mW per 100 kHz e.i.r.p. spektral effekttetthet. For andre spredt-spektrumsteknikker enn FHSS, er maksimal tillatt spektral effekttetthet 10 mW/MHz e.i.r.p.
- (2) **Frekvensbåndet 5150–5350 MHz** tillates brukt til innendørs dataoverføring med maksimal tillatt utstrålt effekt på 200 mW e.i.r.p. slik frekvensbruken er beskrevet i standarden EN 301 893. Ved annen bruk enn innendørs bruk er den gjennomsnittlige spektrale effekttetthet i frekvensbåndet 5150–5350 MHz begrenset til 10 mW/MHz e.i.r.p. i ethvert 1 MHz-område. Trådløse aksessystemer (WAS) (Wireless Access Systems) og radiobaserte lokalnett (RLAN) (Radio Local Area Networks) som opererer i frekvensbåndet 5250–5350 MHz, skal implementere sendeeffektstyring (TPC) (Transmit Power Control) som gir en gjennomsnittlig dempning på minst 3 dB i forhold til maksimalt tillatt utstrålt effekt. Dersom sendeeffektstyring ikke er i bruk, er maksimal tillatt utstrålt effekt 3 dB lavere enn det som følger av første og andre punktum. Radioutstyret skal benytte dynamisk frekvensvalg (DFS) (Dynamic Frequency Selection) som beskrevet i standarden EN 301 893.

LOVDATA

- (3) **Frekvensbåndet 5470–5725 MHz** tillates brukt til dataoverføring med maksimal tillatt utstrålt effekt på 1 W e.i.r.p. Maksimal gjennomsnittlig spektral effekttetthet skal ikke overskride 50 mW/MHz e.i.r.p. i noe bånd på 1 MHz. Trådløse aksessystemer (WAS) og radiobaserte lokalnett (RLAN) som opererer i frekvensbåndet 5470–5725 MHz, skal implementere sendeeffektstyring (TPC) som gir en gjennomsnittlig dempning på minst 3 dB i forhold til maksimal tillatt utstrålt effekt. Dersom sendeeffektstyring ikke er i bruk, er maksimal tillatt utstrålt effekt og spektral effekttetthet 3 dB lavere enn det som følger av første og andre punktum. Radioutstyret skal benytte dynamisk frekvensvalg (DFS) som beskrevet i standarden EN 301 893.
- (4) **Frekvensbåndene 5725–5795 MHz og 5815–5850 MHz** tillates brukt til dataoverføring med maksimal tillatt utstrålt effekt på 4 W e.i.r.p. Maksimal gjennomsnittlig spektral effekttetthet skal ikke overskride 200 mW/MHz e.i.r.p. i noe bånd på 1 MHz. Radioutstyret skal implementere dynamisk frekvensvalg (DFS) som beskrevet i standarden EN 302 502. Radioutstyret skal ha sendeeffektstyring (TPC) som gir en gjennomsnittlig dempning på minst 3 dB. Dersom sendeeffektstyring ikke er i bruk, er maksimal tillatt utstrålt effekt og spektral effekttetthet 3 dB lavere enn det som følger av første og andre punktum. På grensen mellom Norge og naboland skal effekttettheten ikke overstige –122,5 dBW/m² målt med en referansebåndbredde på 1 MHz med mindre noe annet følger av koordineringsavtale.
- (5) **Frekvensbåndet 57–66 GHz** tillates brukt til innendørs trådløs dataoverføring med maksimal tillatt gjennomsnittlig effekt på 40 dBm e.i.r.p. som beskrevet i standarden EN 302 567. Maksimal tillatt spektral effekttetthet er 13 dBm/MHz. Bruk gjennom fast utendørsinstallasjon tillates ikke. Det skal benyttes spektrumaksessteknikker og interferensreduserende tiltak som gir minst samme virkning som teknikker beskrevet i harmoniserte standarder.

0 Endret ved forskrift 28 april 2014 nr. 591.

900 MHz-båndet omfatter 880-915 MHz / 925-960 MHz.

TELENOR

Vil redusere dominans i mobilmarkedet

Når regjeringen i fremtiden skal dele ut lisenser i mobilmarkedet, vil den senke grensen for hvor mye hvert enkelt selskap kan sikre seg. Telenor har over halvparten av mobilmarkedet, mens konkurrenten Telia har en tredjedel. Ice, en operatør som bygger opp et tredje landsdekkende nett, har foreløpig bare 1,6 prosent av markedet. Derfor har de sistnevnte to reagert på taket Nasjonal kommunikasjonsmyndighet har satt når de neste gang skal auksjonere ut mobilfrekvenser. Taket er i dag satt til 2x20 MHz i 900 MHz-båndet. Telia mener at et så høyt tak gir Telenor mulighet til å befeste sin dominans og i ytterste konsekvens svekke konkurransen permanent. Telenor er ikke enig i den beskrivelsen. (NTB)

Aftenposten 25.02.2017

DET KONGELIGE SAMFERDSELSDEPARTEMENT

Nasjonal kommunikasjonsmyndighet
Postboks 93
4791 LILLESAND

NKOM

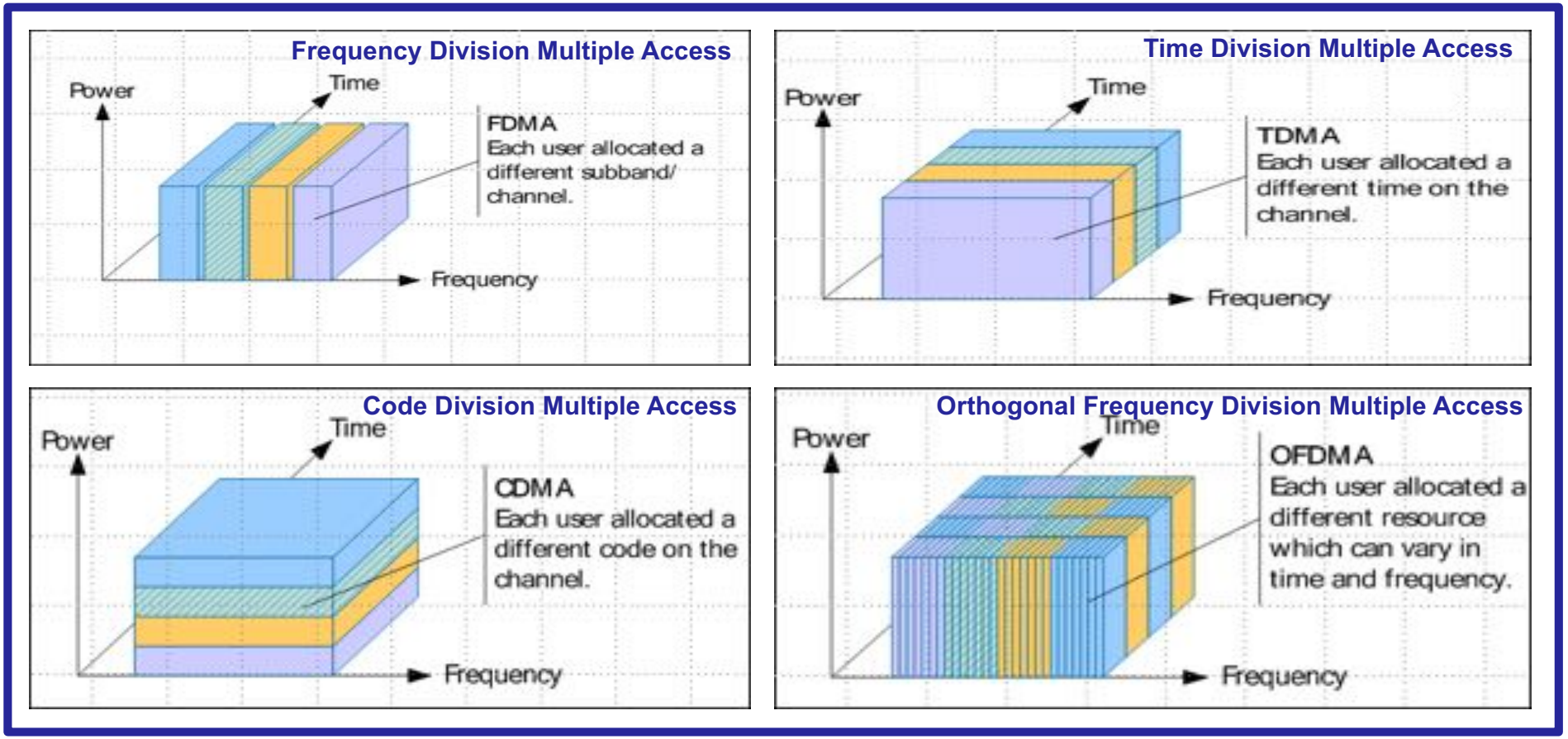
900 MHz-båndet er, og vil i årene fremover, være en spesielt velegnet ressurs ettersom 2G og 3G tjenester fases mer og mer ut og erstattes av 4G. 900 MHz- båndet er av dekningsbåndene best egnet for å understøtte alle tre teknologigenerasjonene 2G/3G/4G. I overgangsperioden der 2G og 3G fases ut må eldre mobiltelefoner og brukerutstyr som f.eks. maskin-til-maskin terminaler fremdeles bruke 900 MHz-båndet. Departementet ser det derfor som svært viktig for konkurransesituasjonen å hindre at én aktør kan sikre seg en for stor andel av denne ressursen i denne avgjørende fasen.

På bakgrunn av markedssituasjonen, Stortingets tilslutning til Ekomplanen, og Ice og Telias innsigelser, har Regjeringen kommet til at *de overordnende rammene* for Nkoms tildeling av frekvensressurser i 900 MHz-båndet bør justeres. Frekvenstaket reduseres fra 2x20 MHz til 2x15 MHz. Øvrige rammer for tildelingen forblir uforandret. Departementet ønsker at en auksjon skal avholdes så snart dette lar seg gjøre etter Nkoms normale prosedyrer og ber samtidig Nkom om å legge frem en plan for snarlig gjennomføring av auksjon av 2x20 MHz i 900 MHz-båndet.

For å legge ytterligere til rette for investeringer og satsninger i det norske mobilmarkedet, ønsker Samferdselsdepartementet å signalisere at frekvensressurser for mobilt bredbånd under 1 GHz vil bli vurdert samlet når det skal fastsettes frekvenstak. Sammen med et redusert frekvenstak i 900 MHz-auksjonen, vil dette gi en helhetlig tilnærming til ambisjonen om tre likeverdige konkurrenter i mobilmarkedet til nytte for norske virksomheter og forbrukere, både gjennom de grep som gjøres i markedsvedtakene og tilrettelegging gjennom frekvensforvaltningen.

I brev fra Samferdselsdepartementet til NKOM, 24.02.2017

Techniques for sharing the radio spectrum



Source: https://www.slideshare.net/toenofmoegan/future-network-lte-for-indonesia

Wireless and mobility are two different things

- **Wireless**: communication over a wireless link
- **Mobility**: handling the mobile user who changes point of attachment to the (mobile/cellular) network

no mobility **high mobility**

wireless user using same access point

mobile user/terminal connecting/ disconnecting from network using DHCP

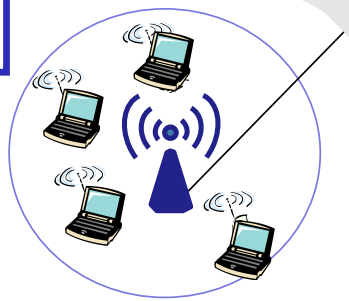
mobile user passing through multiple access points while maintaining ongoing connections – handover/handoff

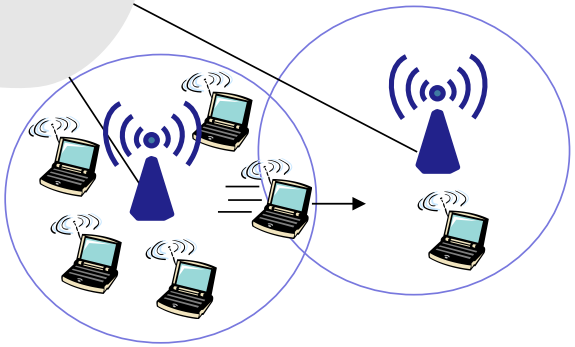
Elements of a wireless network

Base stations and wireless hosts

Base station

- typically connected to wired network
- **relay** - responsible for sending packets between wired network and wireless host(s) in its “area”
  - e.g. cell towers, 802.11 access points





network infrastructure

Wireless hosts

- laptop, phone, smartTV
- **run applications**
- may be **stationary** (non-mobile) or **mobile**
  - wireless does *not* always mean mobile

NTNU

Elements of a wireless network

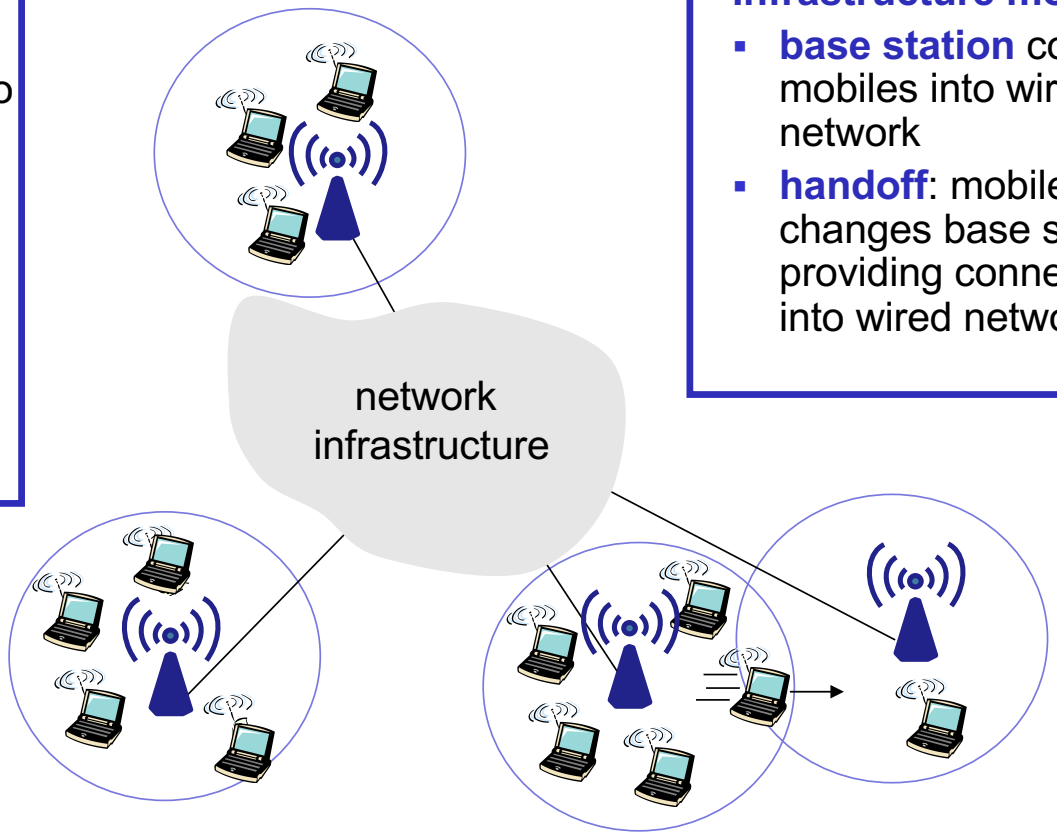
The wireless link

Wireless link

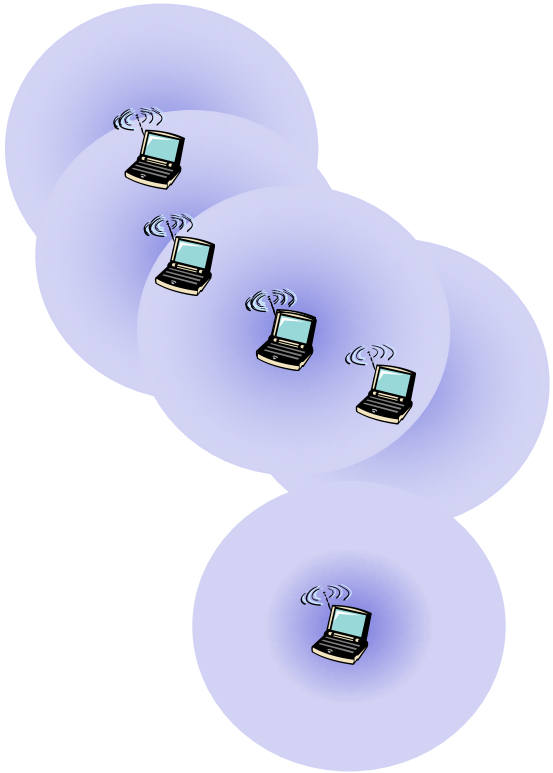
- connect mobile(s) to base station, but also as backbone link
- **multiple access** protocol coordinates link access
- various data **rates**, **transmission distance**

Infrastructure mode

- **base station** connects mobiles into wired network
- **handoff**: mobile changes base station providing connection into wired network



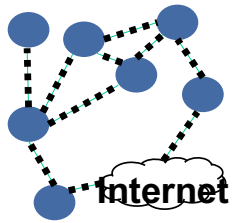
Ad-hoc networks



Ad-hoc mode

- **no base** stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Taxonomy

	Single hop	Multiple hops
Infrastructure (e.g. APs)	 Host connects to base station which connects to larger Internet (WiFi, WiMAX, cellular)	Host may have to relay through several wireless nodes to connect to larger Internet (mesh net) 
No infrastructure	 No base station, no connection to larger Internet (Bluetooth, ad hoc nets)	No base station, no connection to larger Internet. May have to relay to reach a given wireless node (MANET, VANET*)  *Mobile Ad-hoc NETworks, Vehicle Ad-hoc NETworks

Wireless networks: Roadmap

6.1 Introduction

6.2 Wireless links, characteristics

- ~~Code division Multiple Access (CDMA)~~

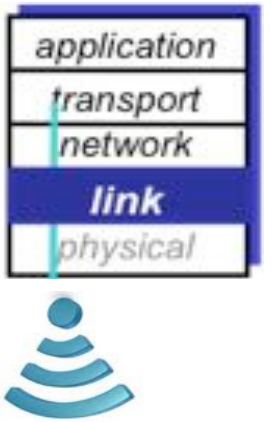
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

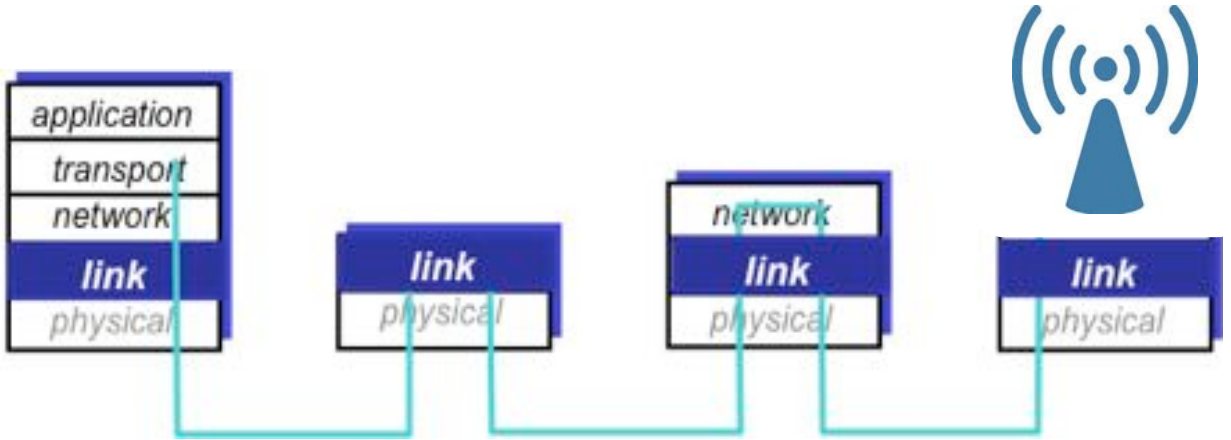
6.4 Cellular Internet Access

- architecture
- standards

8.8 Securing Wireless LANs

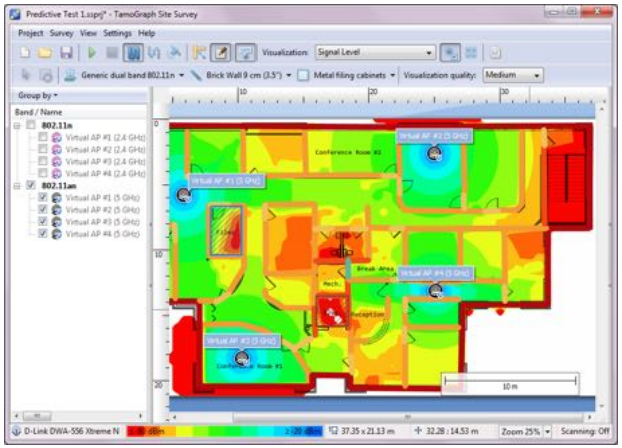
8.8.1 Wired Equivalent Privacy



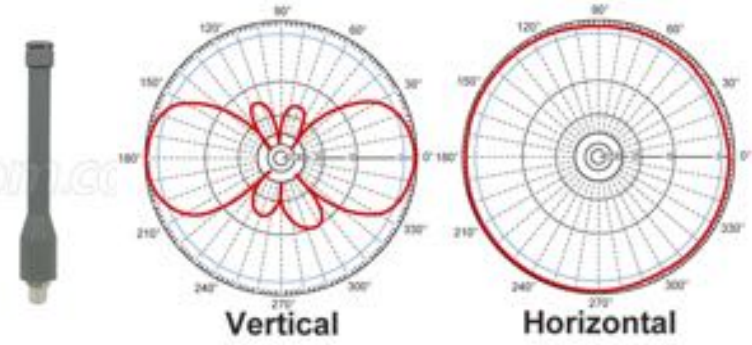


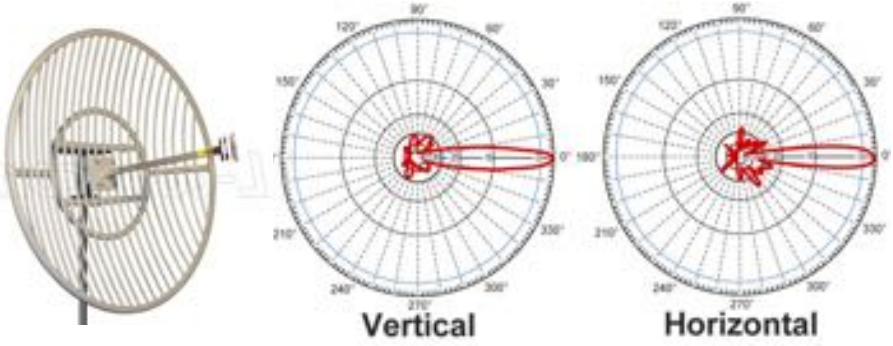
Wireless link characteristics make communication across wireless links more challenging than wired communication

- **Signal spreads as it travels away/propagate from the antenna**
  - Range depends on frequency and radio transmitter power
- **Radio antenna concentrate and directs signals**
  - Antenna´s power gain affects connection range
  - Gain is a measure of how much of the power is radiated in a given direction.
  - Gain (omnidirectional antenna) < Gain (directional antenna)



Source: http://www.tamos.com/products/wifi-site-survey/wlan-planner.php

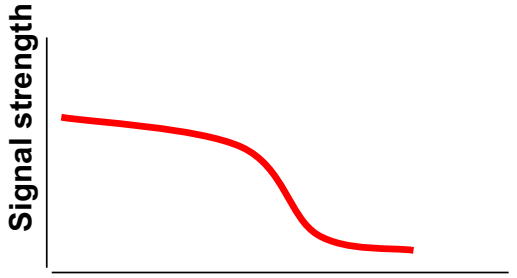


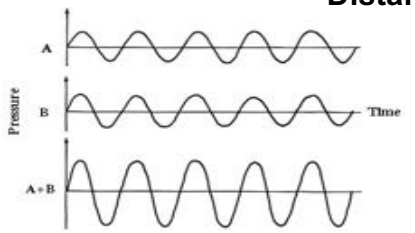


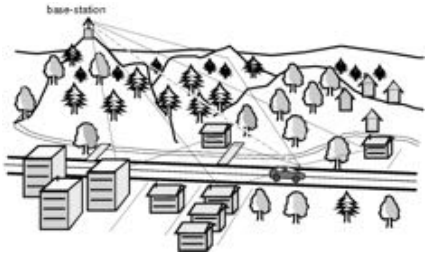
Source: http://www.l-com.com/content/Article.aspx?Type=N&ID=10264

Wireless link characteristics make communication across wireless links more challenging than wired communication

- **Decreasing signal strength (amplitude) due to physical obstruction and distance**
  - radio signal attenuates as it propagates through matter (path loss)
  - lower frequency, larger coverage area
  - signal strength = (distance)$^{1/3}$
- **Interference between signals**
  - Signal phase has an effect on amplitude when receive multiple signals
  - Signal sharing - standardized wireless network frequencies (e.g. 2.4 GHz) shared by other devices (e.g. phone); devices (motors, microwave
  - Frequency harmonics
- **Multipath propagation**
  - Radio signal reflects off objects ground, arriving destination at slightly different times - interference

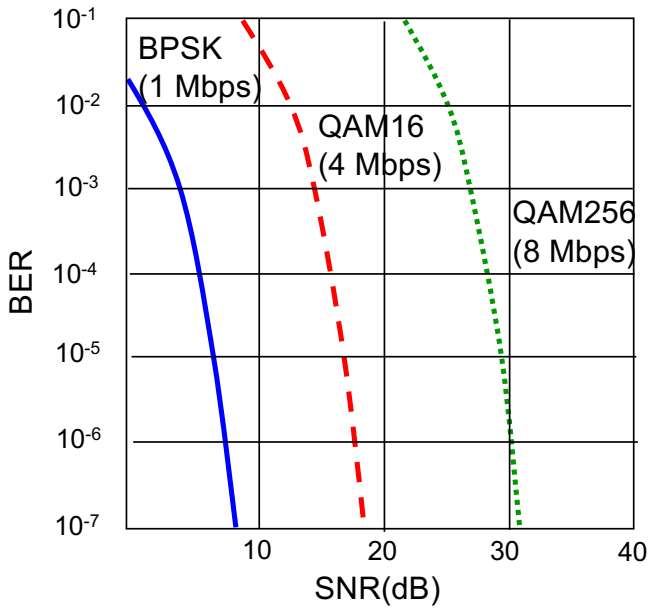






Physical layer adapts to channel conditions

- The **signal-to-noise ratio (SNR)** is a measure of the strength of the received signal
- A higher SNR, a lower bit error rate (BER) – easier to extract signal from noise
  - Given physical layer: increase power -> increase SNR->decrease BER
  - SNR given: a higher bit transmission rate will have a higher BER
- **SNR may change with mobility**: dynamically adapt physical layer (modulation technique, rate) to channel conditions
  - SNR decreases, BER increase as node moves away from base station
  - When BER becomes too high, switch to lower transmission rate but with lower BER



Binary Phase Shift Keying
Quadrature Amplitude Modulation

Wireless networks: Roadmap

6.1 Introduction

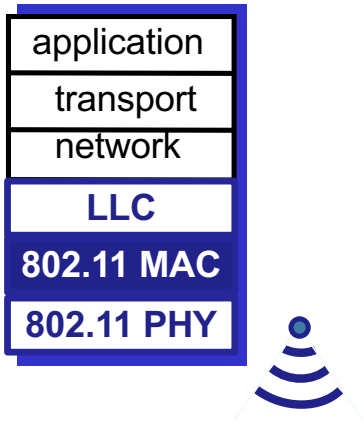
6.2 Wireless links, characteristics
- ~~Code division Multiple Access (CDMA)~~

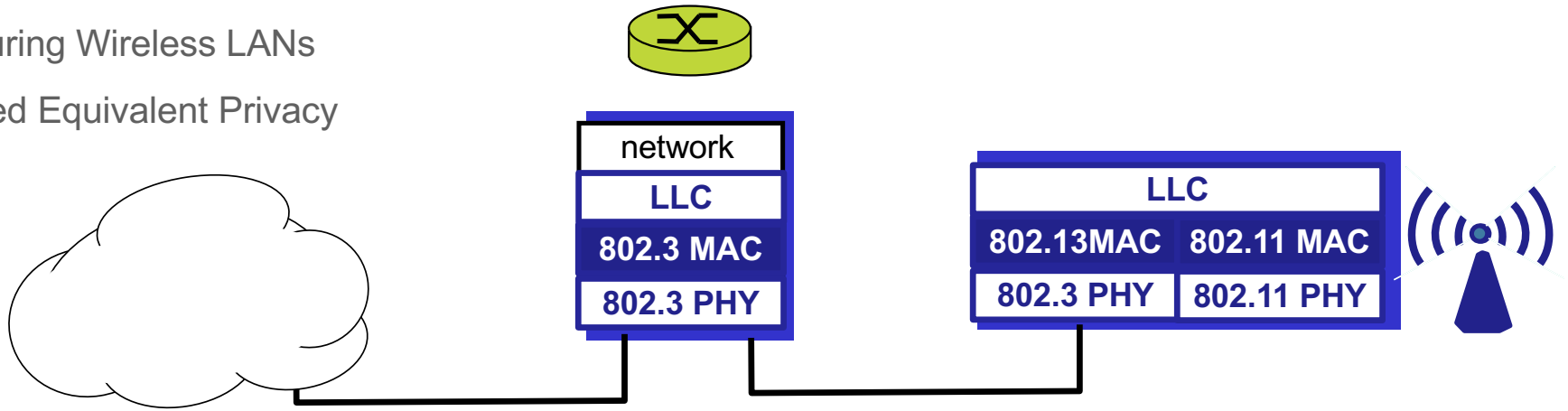
6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access
- architecture
- standards

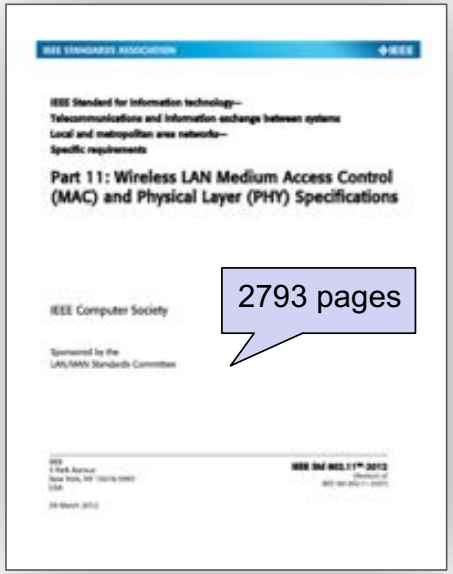
8.8 Securing Wireless LANs

8.8.1 Wired Equivalent Privacy





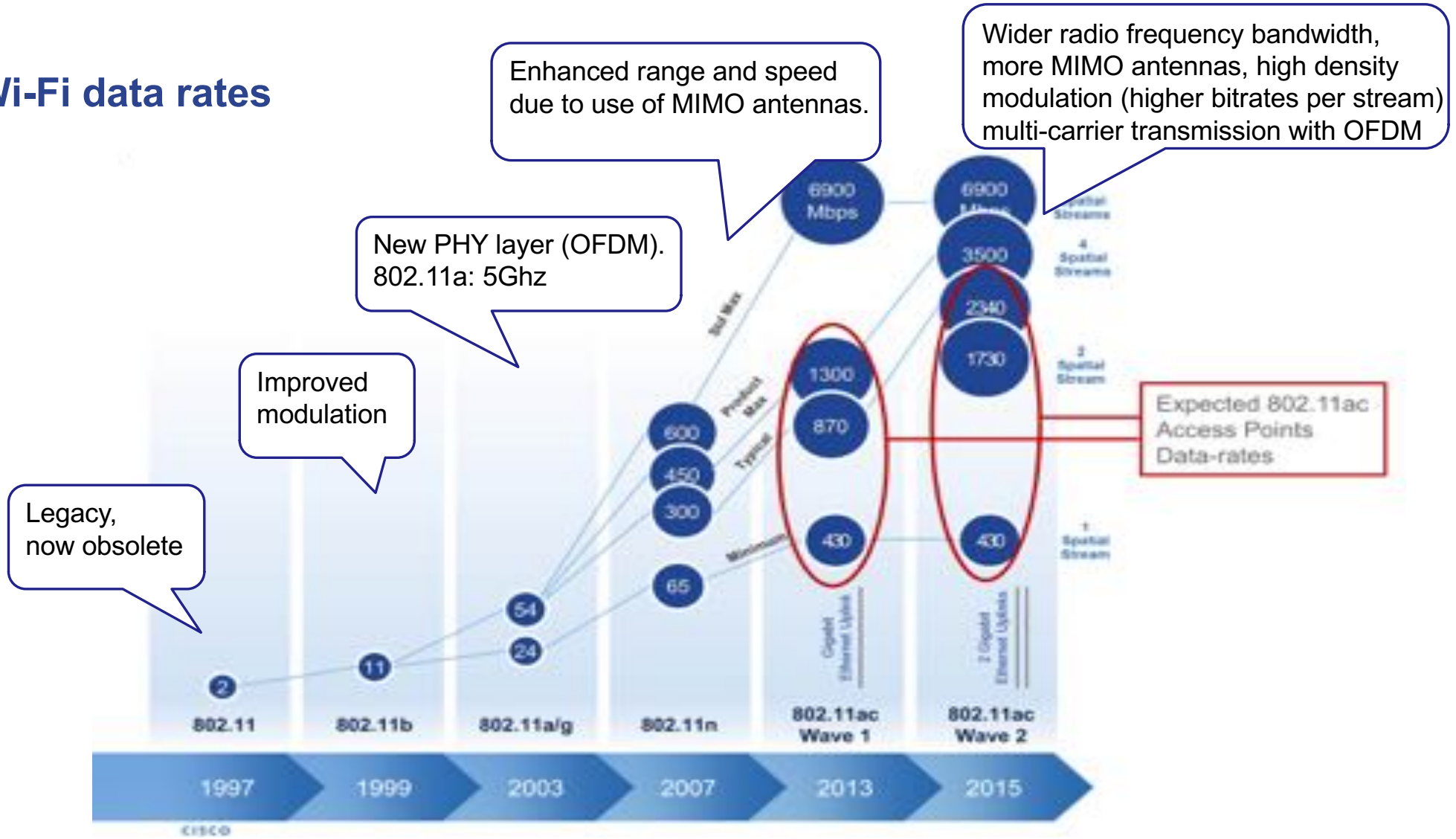
Overview 802.11 WLAN standards



IEEE 802.11 MAC sublayer					
802.11 DSSS/FHSS	**802.11a** OFDM	**802.11b** HR-DSSS	**802.11g** OFDM	**802.11n** MIMO-OFDM	**802.11ac** MIMO_OFDM
2,4 GHz	5 GHz	2,4 GHz	2,4 GHz	2,4/5 GHz	5 GHz
2 Mbps	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1300 Mbps

- A common Medium Access Layer using **CSMA/CS Carrier Sense Multiple Access/Collision Avoidance** – 802.11 MAC
- **Different physical layers based on various spread spectrum techniques** – 802.11 PHY a/b/g/n/ac
- Base station and mobile **dynamically change transmission rate** (physical layer modulation technique) as node moves and SNR (signal-to-noice ratio) varies

Wi-Fi data rates



Source: https://www.wirelessdesignmag.com/blog/2015/10/beyond-byod-and-introduction-80211ac-wave-2-technology

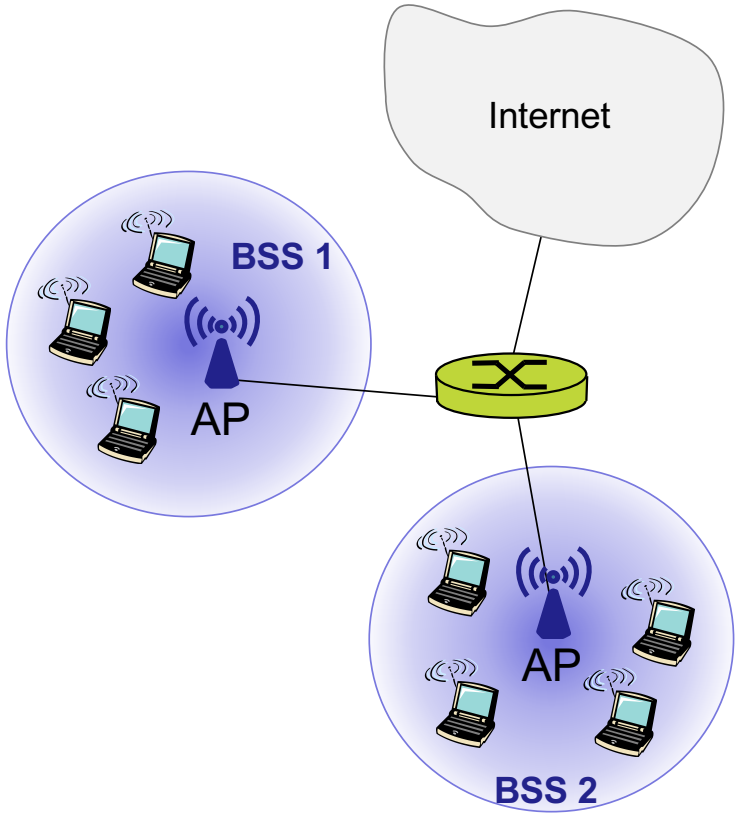
Overview 802.11 WLAN standards

802.11 network PHY standards [hide]

802.11 protocol	Release date[6]	Frequency (GHz)	Bandwidth (MHz)	Stream data rate[7] (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range[citation needed] Indoor (m)	Indoor (ft)	Outdoor (m)	Outdoor (ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38	125	140	460
n	Oct 2009	2.4/5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65 [C]	4	MIMO-OFDM	70	230	250	820[B]
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135 [C]			70	230	250	820[B]
ac	Dec 2013	5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7 [C]	8		35	115[B]		
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180 [C]			35	115[B]		
			80	400 ns GI : 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] 800 ns GI : 29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390 [C]			35	115[B]		
			160	400 ns GI : 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] 800 ns GI : 58.5, 117, 175.5, 234, 351, 468, 702, 780 [C]			35	115[B]		

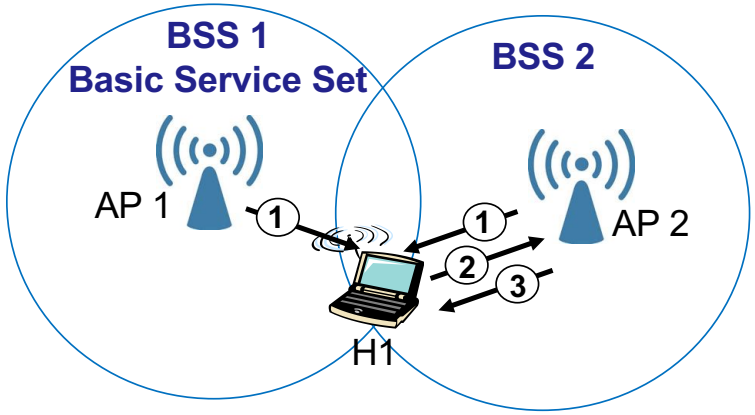
Source: http://en.wikipedia.org/wiki/802.11

802.11 LAN architecture



- **CSMA/CA** for multiple access
- Base station and ad-hoc
  - base station = **access point (AP)**
- **Basic Service Set (BSS)** in infrastructure mode contains
  - wireless hosts
  - access point (AP)
  - ad hoc mode: hosts only
- **Hosts associate with an AP**
  - may perform authentication
  - typically DHCP to get IP address in AP's subnet

802.11: passive/active scanning to associate with an access point

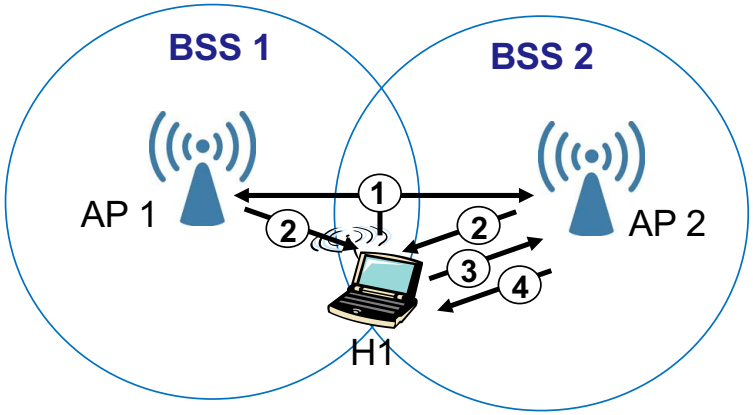


Passive scanning

(1) **Beacon frames** sent from AP with its SSID and MAC address

(2) **Association request** frame from H1 to selected AP

(3) **Association response** frame from selected AP to H1



Active scanning

(1) **Probe request** frame broadcast from H1

(2) **Probe response** frame from APs

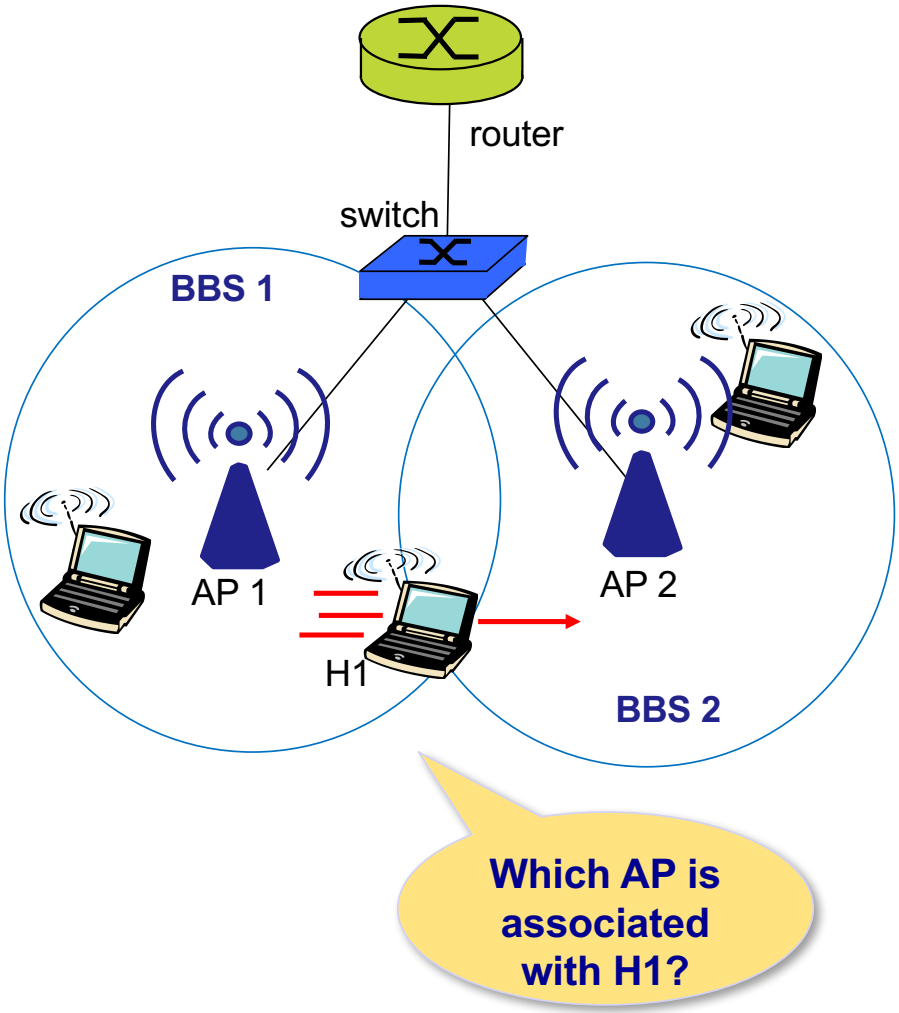
(3) **Association request** frame from H1 to selected AP

(4) **Association response** frame from selected AP to H1

802.11: supports mobility within same subnet

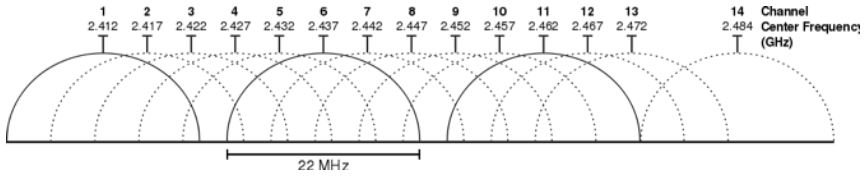
- H1 remains within the same IP subnet:
  IP address can remain same

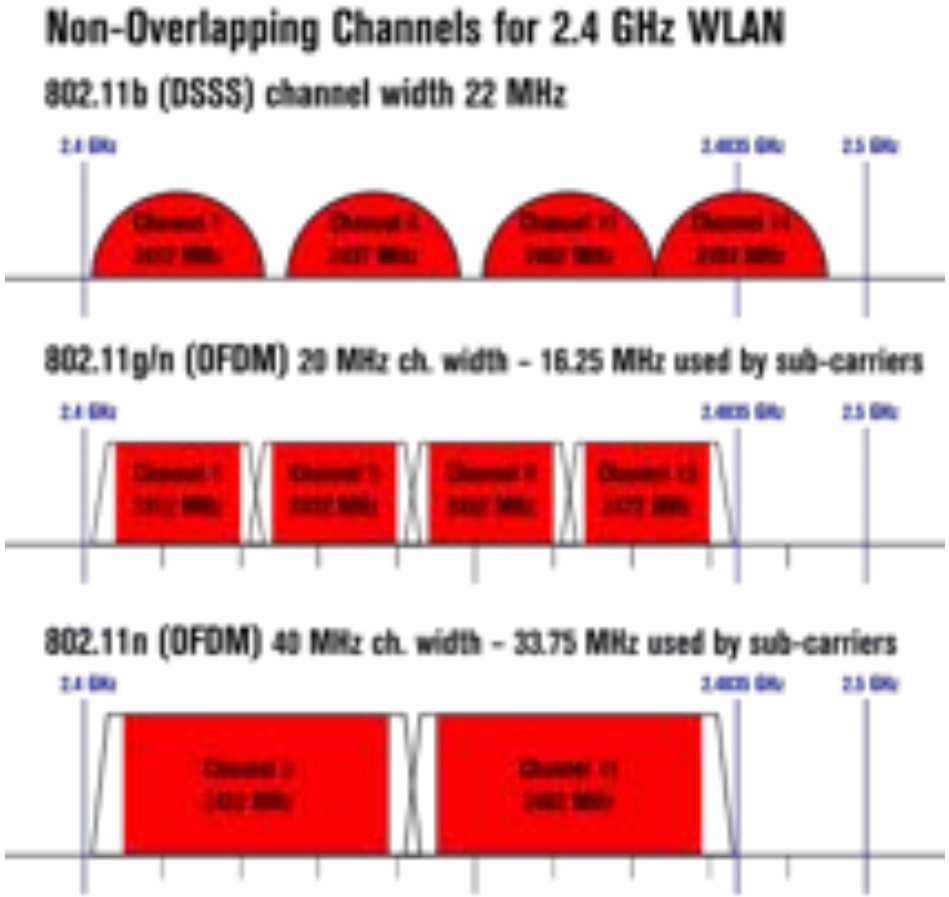
- Self-learning switch will
  see frame from H1 and “remember” which
  switch port can be used to reach



802.11: Access point (AP) and channels

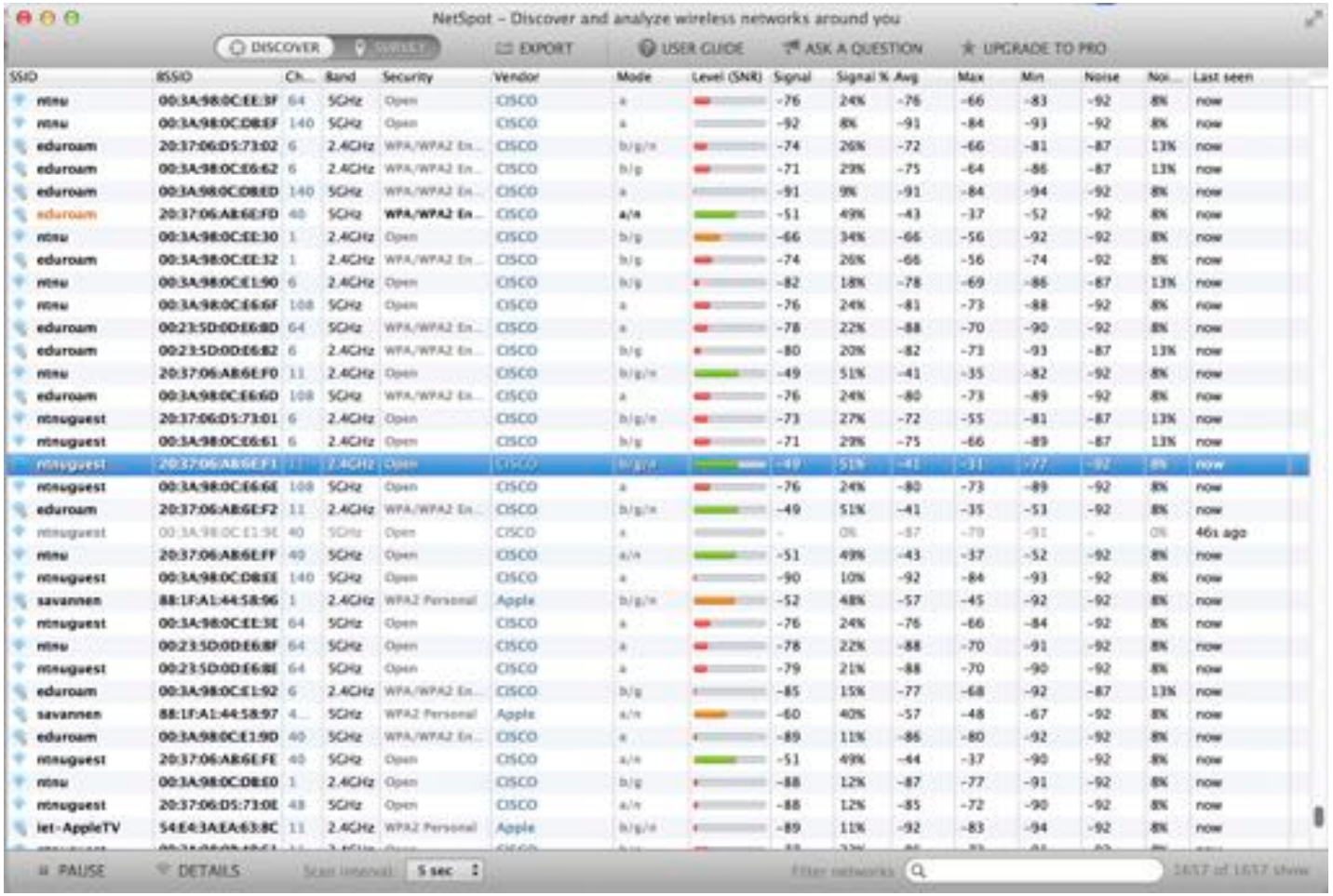
- Frequency for AP chosen by AP or admin
- Spectrum divided into channels
- Interference possible: channel can be same as that chosen by neighbor AP!
- 802.11b channels non-overlapping if separated by four or more channels, eg.
  - 1, 6, 11



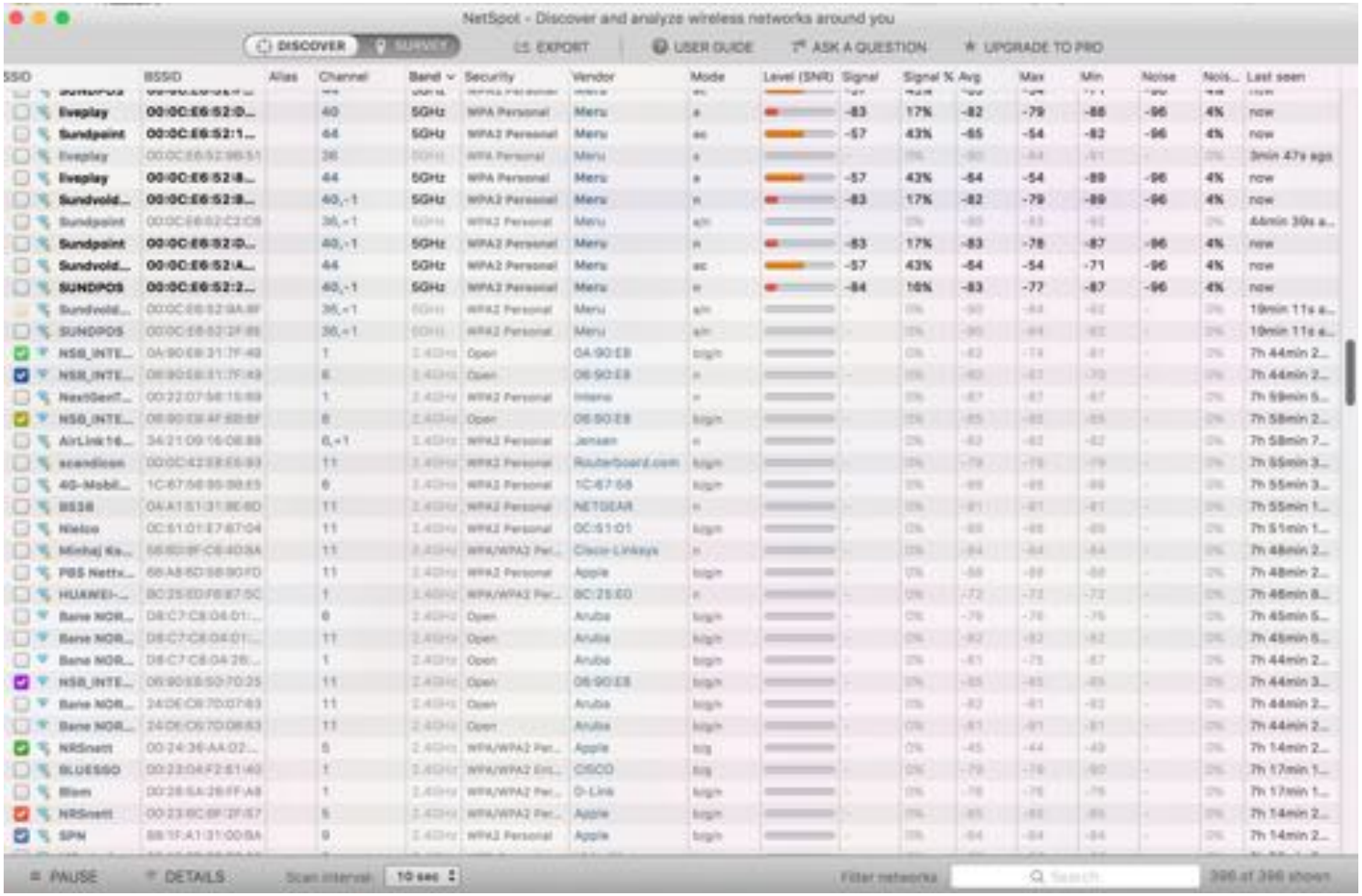


Source: https://en.wikipedia.org/wiki/List_of_WLAN_channels

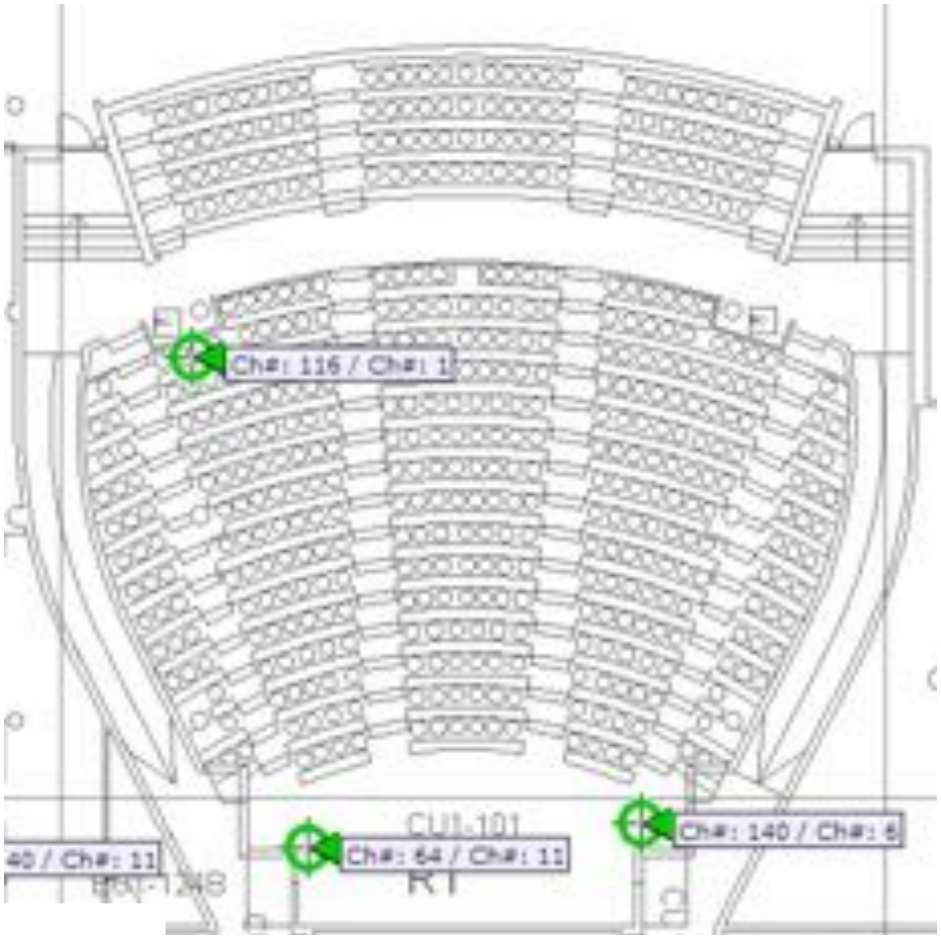
WLAN spotting, March 2013



WLAN spotting March 2017

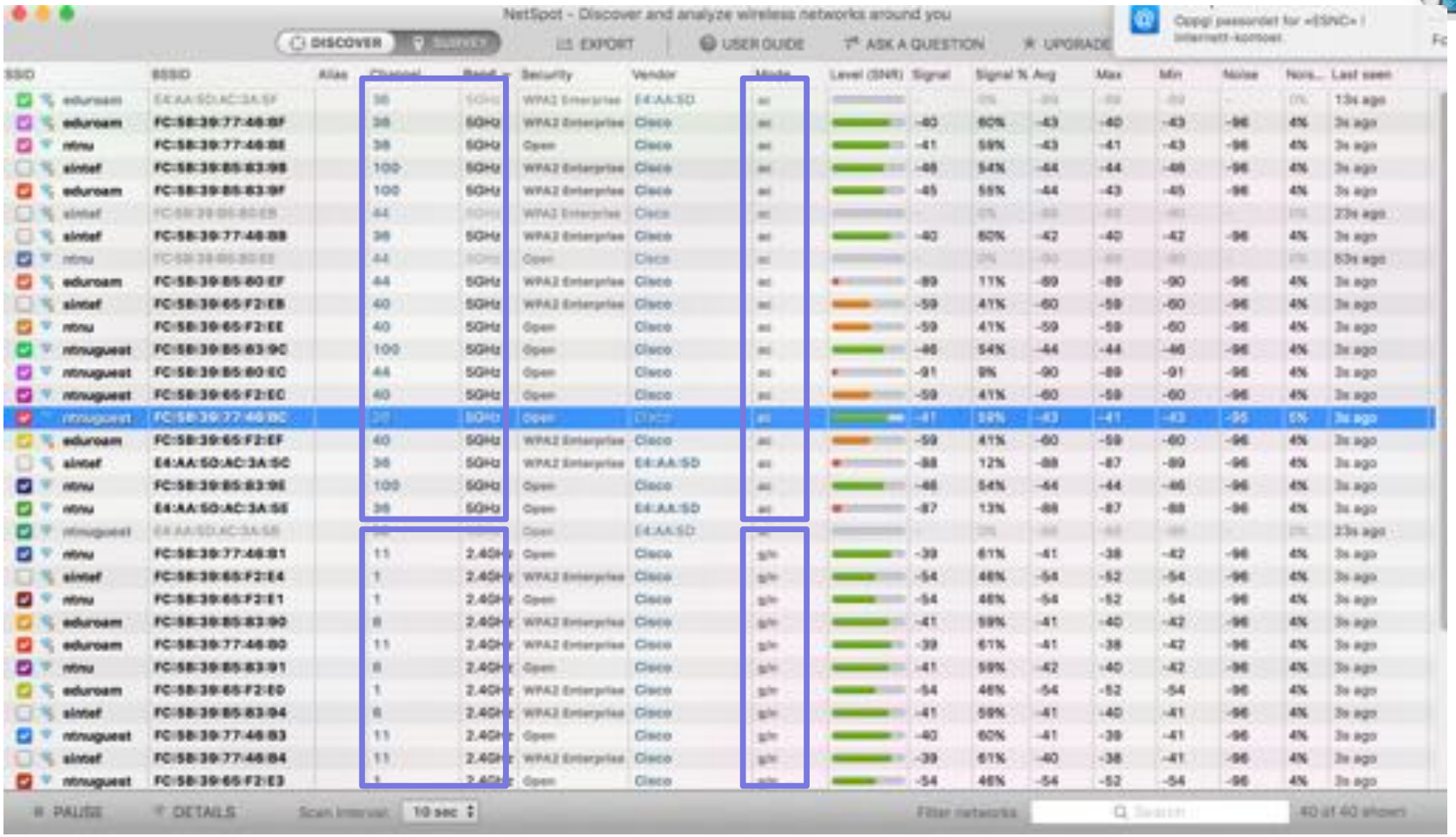


802.11 WLAN in R1

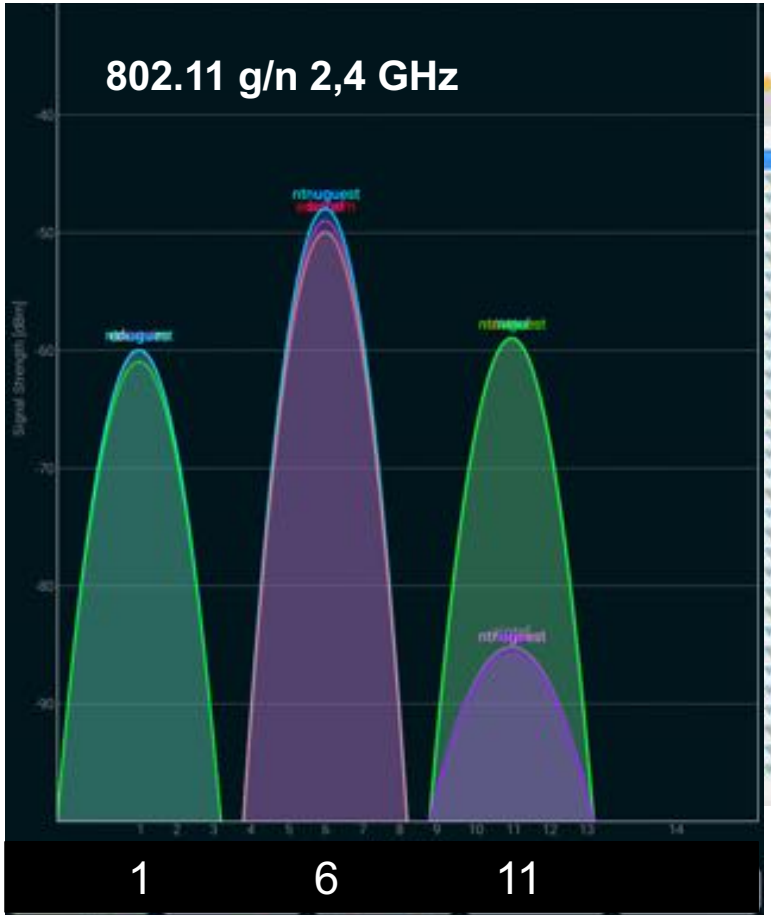


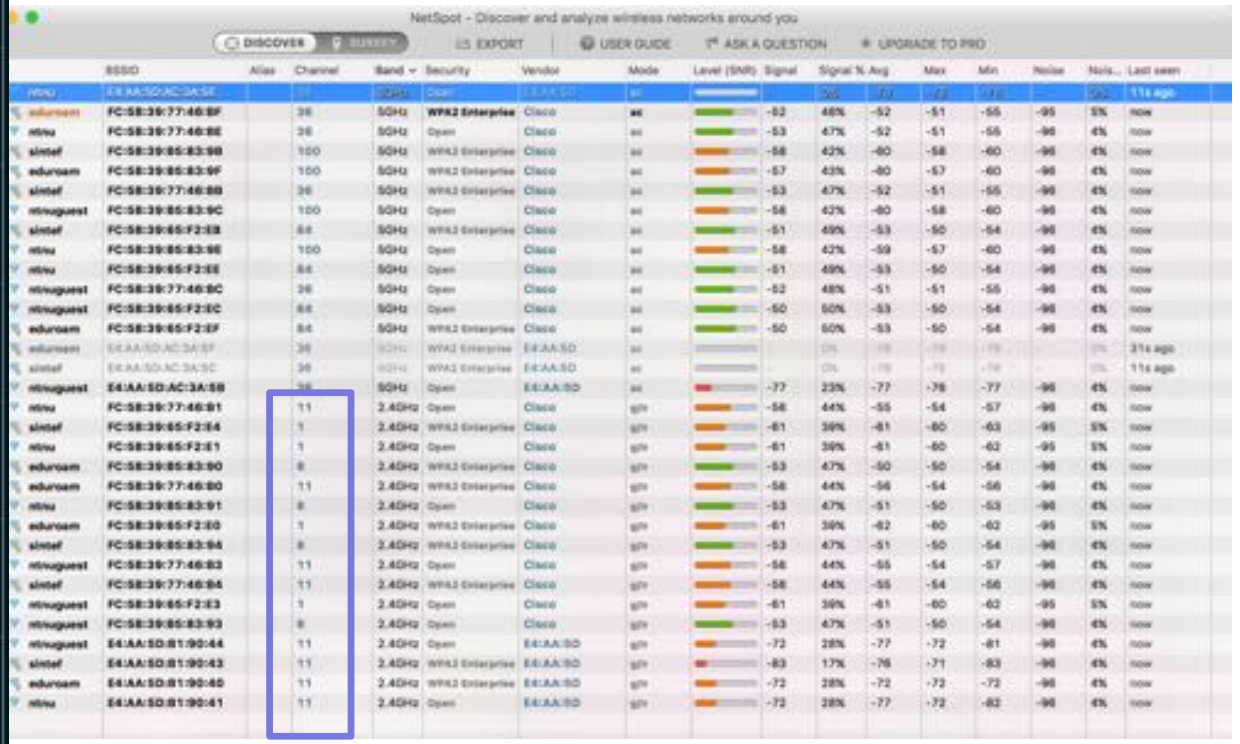
I 2014
5 GHz 802.11a channels 64, 116, 140
2,4 GHz 802.11b channels 1, 6, 11

Access points in R1, March 2017



802.11g/n channels, R1 March 2017

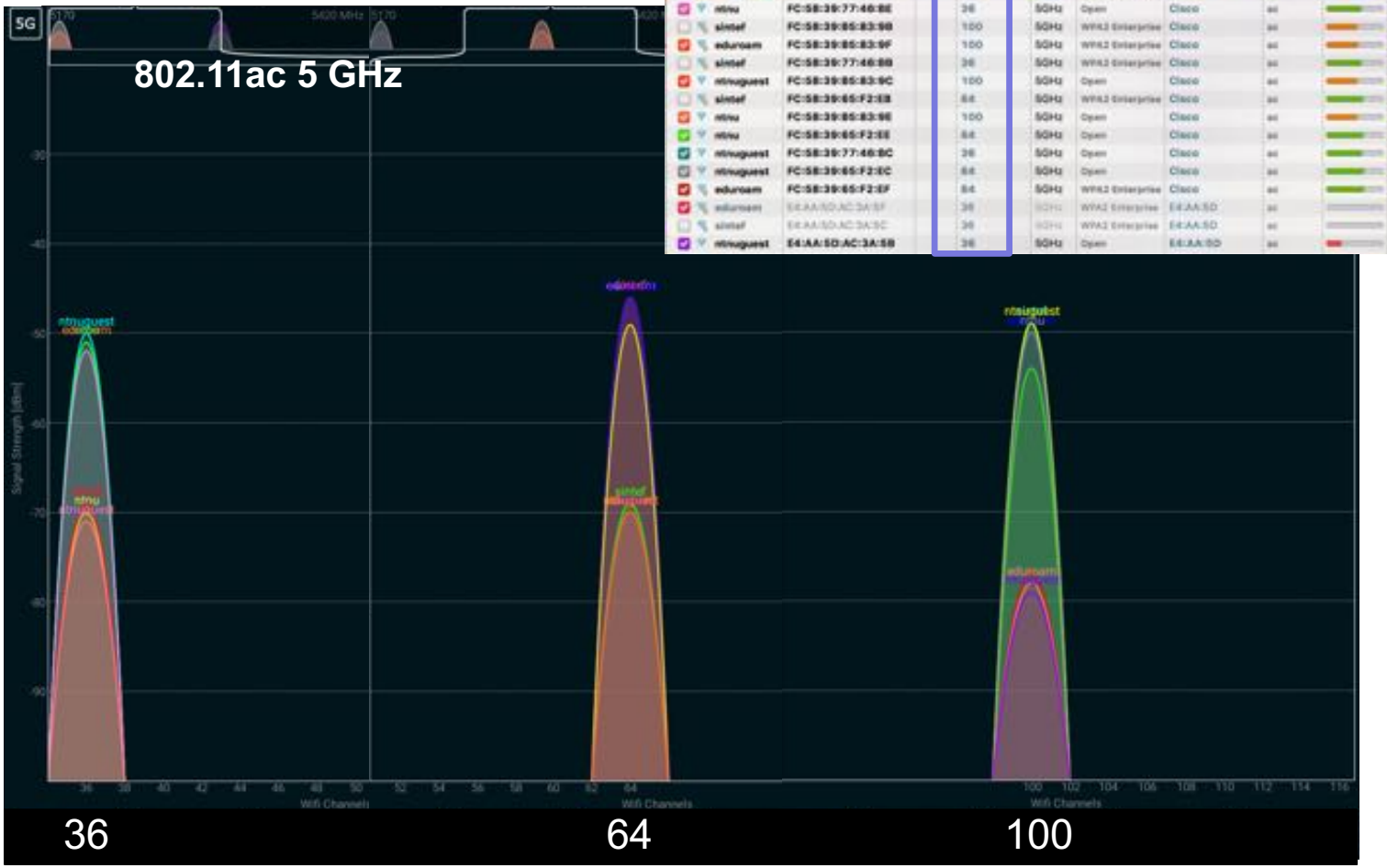




Wifi Analyzer

NetSpot

802.11ac channels



R1, March 2017

Next Generation Gigabit WiFi - 802.11ac

Today's WiFi

3x speed with 802.11ac

2.4GHz WiFi band

- More widespread usage but high interference
- Minimum WLAN feature required for connectivity

802.11ac –5GHz WiFi Band

- Less interference, 8x more channels than 2.4GHz
- Ideal for video streaming or gaming

Today's WiFi

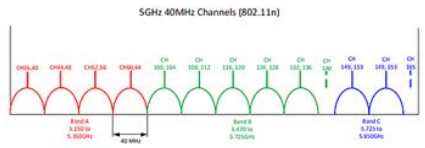
802.11ac Beamforming Technology

NTNU

802.11n

- Supports 20 and 40 MHz channels
- Supports 2.4 GHz and 5 GHz frequency bands
- Supports BPSK, QPSK, 16-QAM, and 64-QAM
  Binary/Quadrature Phase Shift Keying
  Quadrature Amplitude Modulation
- Supports many types of explicit beamforming
- Supports up to four spatial streams
- Supports single-user transmission only
- Includes significant MAC enhancements (A-MSDU, A-MPDU)
  aggregate medium access control (MAC) service data unit /protocol data unit

802.11n channels:
https://en.wikipedia.org/wiki/IEEE_802.11n-2009

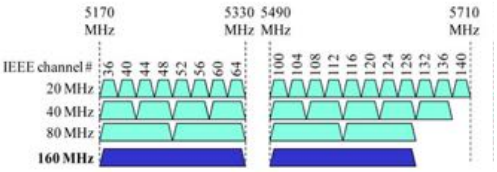


802.11ac

802.11ac data rate increases: more spatial streams (1-8), wider channels (20/40/20/160 MHz) or expansion of encoding rates

- Adds 80 and 160 MHz channels
- Supports 5 GHz only
- Adds 256-QAM
- Supports only null data packet (NDP) explicit beamforming
- Supports up to eight spatial streams (AP); client devices up to four spatial streams
- Adds multi-user transmission
- Supports similar MAC enhancements, with extensions to accommodate high data rates

802.11ac channel
https://en.wikipedia.org/wiki/IEEE_802.11ac

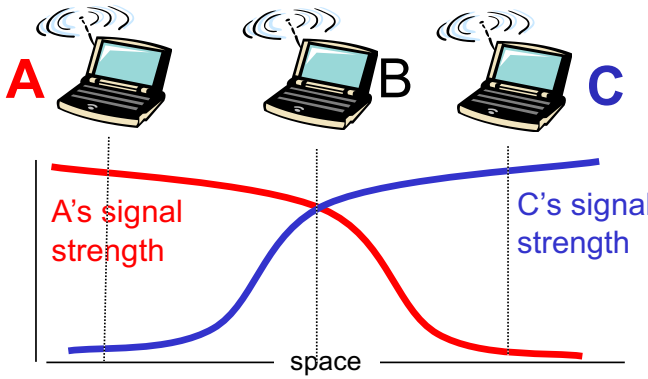


Source: Oreilly 802.11ac survival guide, 2013

IEEE 802.11: CSMA/CA for wireless medium access

carrier sense multiple access / collision avoidance

- **CSMA – carrier sense before transmitting**
  - don't collide with ongoing transmission by other node
- **CA - collision avoidance**
  - may be difficult to receive/sense collisions when transmitting due to weak received signals: **fading**
  - can't sense all collisions: **hidden terminal**



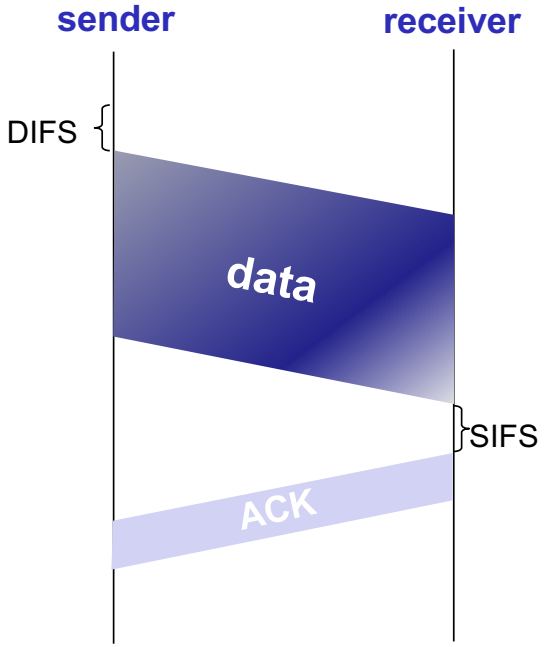
Fading

Hidden terminal

When channel sensed busy – sender back-off

802.11 sender

- If sense **channel idle** for a period (DIFS): transmit frame
- If sense **channel busy**
  - start **random back-off** time
  - timer **counts down while channel idle**
  - transmit when timer expires
  - if no **ACK from receiver**, collision => erroneous frame => increase random back-off interval
  - repeat transmission



802.11 receiver

- if frame received OK: return ACK after a short period of time (SIFS)

DIFS – Distributed inter-frame space, SIFS – Short inter-frame spacing

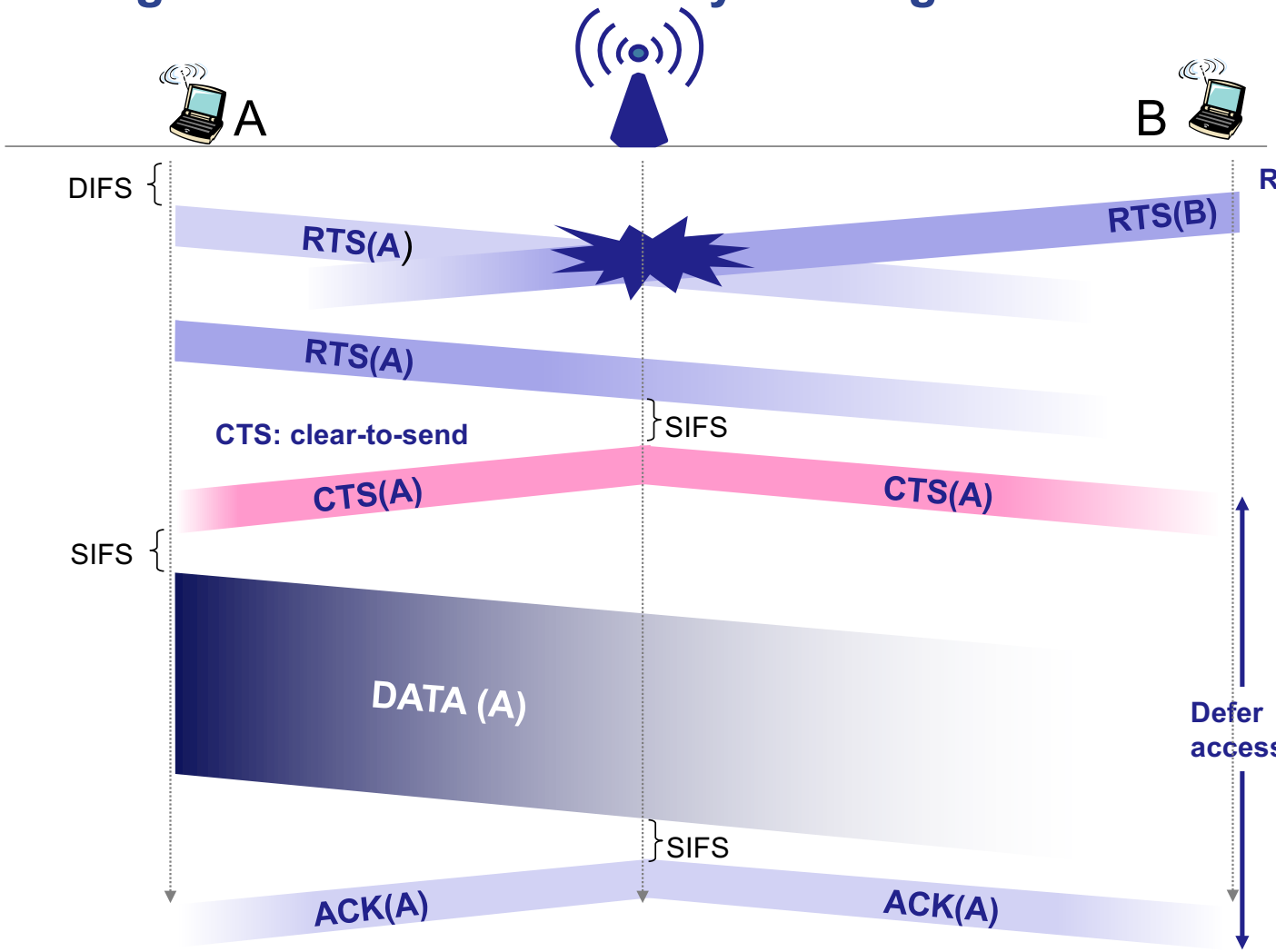
To avoid data frame collisions: small reservation packets

- **Idea:** allow sender to "reserve" channel rather than random access of data frames to avoid collisions of long data frames

- Sender first transmits small **request-to-send (RTS)** packets using CSMA to access point
  - Requests may still collide with each other, but they're short

- Access point broadcasts **clear-to-send (CTS)** in response to RTS request
  - CTS heard by all nodes
- Sender transmits data frame
  - other stations defer transmissions

Avoiding data frame collisions by sending small reservation packets

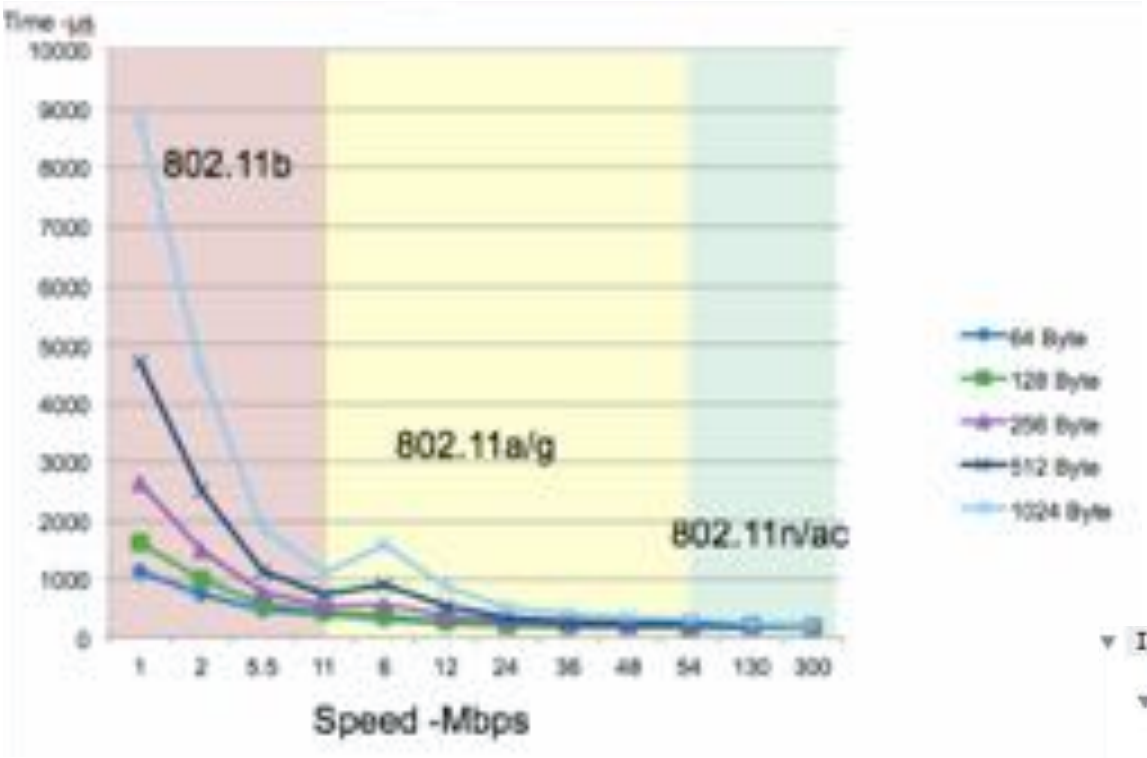


RTS: request-to-send

DIFS – Distributed inter-frame space
SIFS – Short inter-frame spacing
DIFS = SIFS+ (2 * Slot time)

Standard	Slot time (µs)	DIFS (µs)
IEEE 802.11-1997 (FHSS)	50	128
IEEE 802.11-1997 (DSSS)	20	50
IEEE 802.11b	20	50
IEEE 802.11a	9	34
IEEE 802.11g	9 or 20	28 or 50
IEEE 802.11n (2.4 GHz)	9 or 20	28 or 50
IEEE 802.11n (5 GHz)	9	34
IEEE 802.11ac (5 GHz)	9	34

Airtime of Packets by Speed and Size

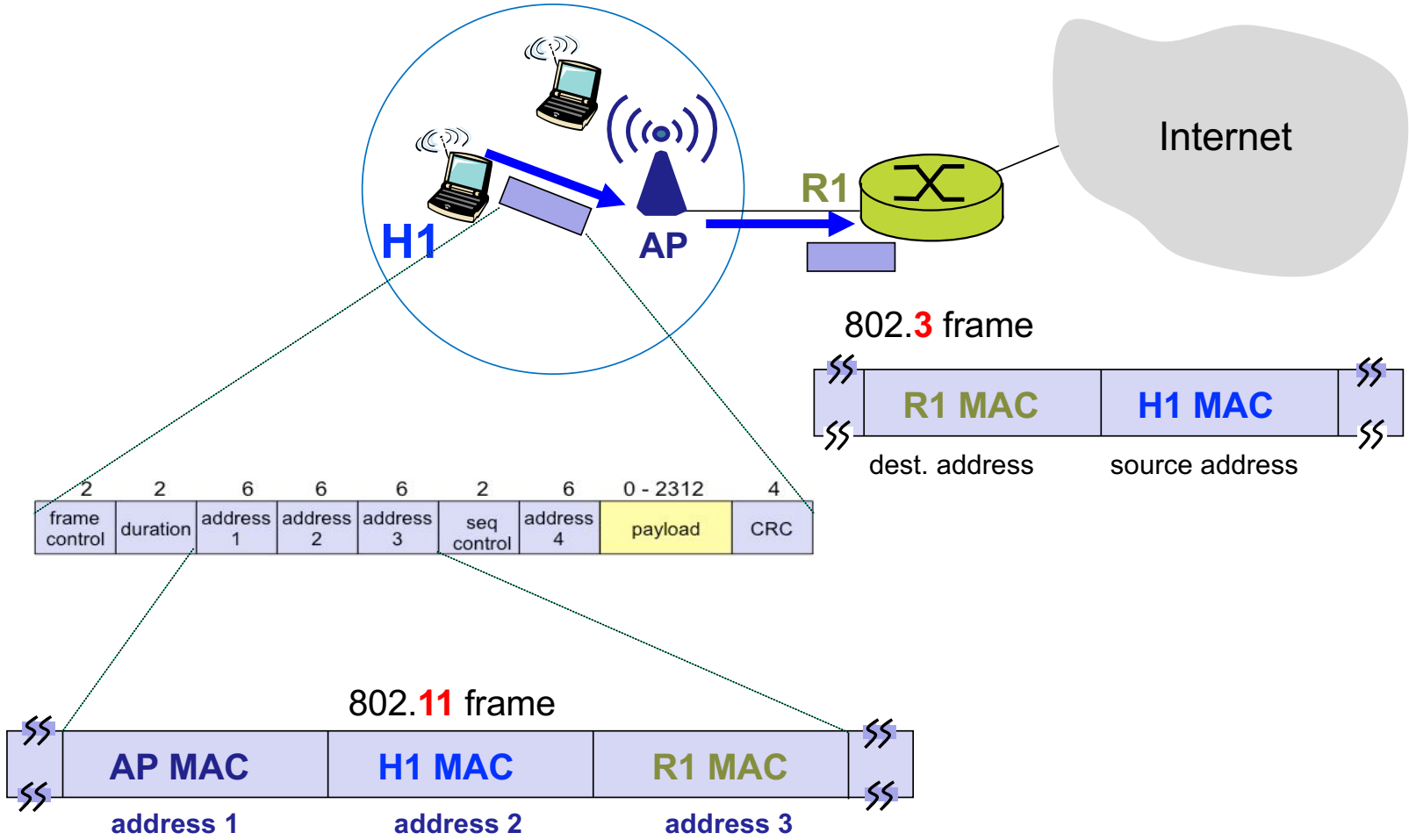


Source: Enterprise Mobility 8.1 Design Guide , Cisco 2016

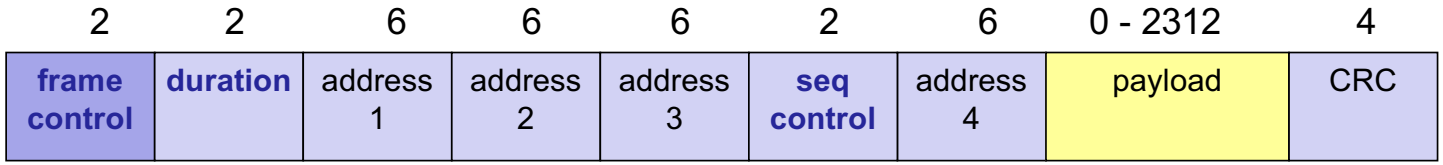
```
   45  Request-to-send, Flags=........C
   39  Clear-to-send, Flags=........C
 1538  [TCP segment of a reassembled PDU]
 1542  [TCP segment of a reassembled PDU]
   57  802.11 Block Ack, Flags=........C
```

```
▼ IEEE 802.11 Request-to-send, Flags: ........C
    Type/Subtype: Request-to-send (0x001b)
  ▼ Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    ▶ Flags: 0x00
    .000 0000 1111 0000 = Duration: 240 microseconds
    Receiver address: Apple_86:72:95 (20:c9:d0:86:72:95)
    Transmitter address: MeruNetw_f2:45:06 (00:0c:e6:f2:45:06)
    Frame check sequence: 0xc3b449bb [correct]
    [FCS Status: Good]
```

802.11 frame: addressing



802.11 frame format – multiple addresses



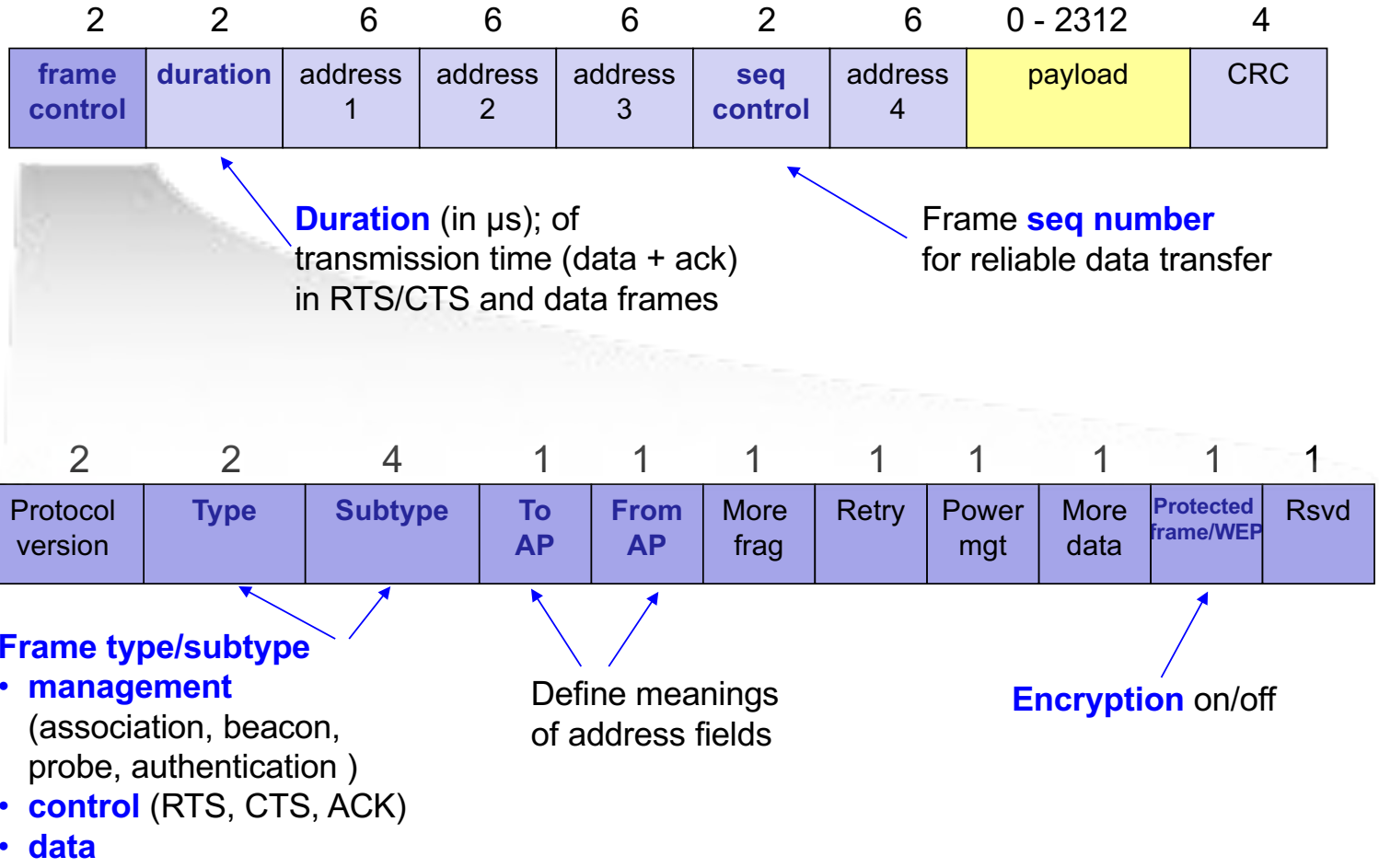
Address 1: MAC address of **destination** – wireless host or AP

Address 2: MAC address of **source** - wireless host or AP

Address 3: MAC address of **router** interface to which AP is attached

Address 4: used only in **ad hoc** mode

802.11 frame: frame control ++



NTNU

Table 7-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Manage	0001	Association response
00	Manage	0010	Reassociation request
00	Manage	0011	Reassociation response
00	Manage	0100	Probe request
00	Manage	0101	Probe response
00	Manage	0110–0111	Reserved
00	Manage	1000	Beacon
00	Manage	1001	ATIM
00	Manage	1010	Disassociation
00	Manage	1011	Authentication
00	Manage	1100	Deauthentication
00	Management	1101	Action
00	Management	1110–1111	Reserved
01	Control	0000–0111	Reserved
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack

Management frames

Control frames

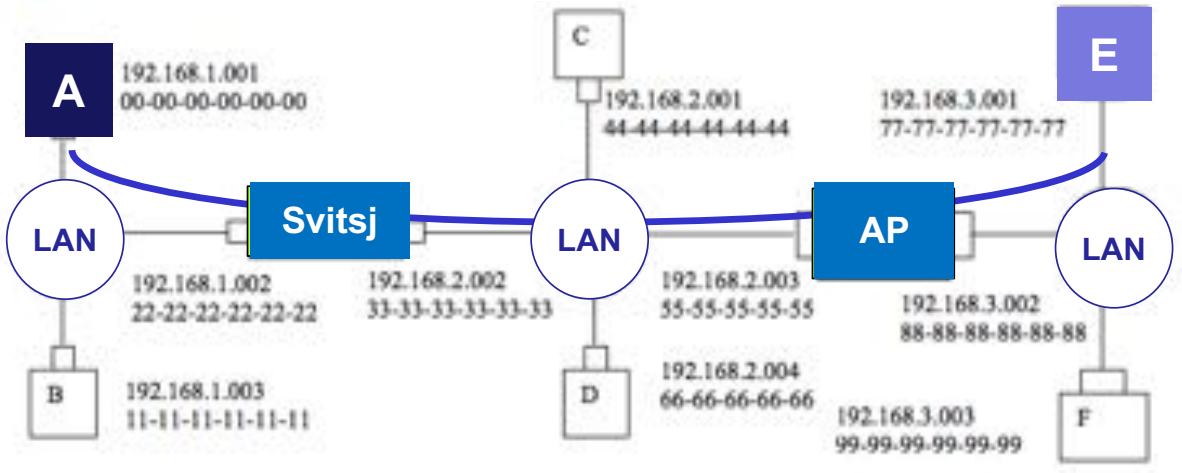
Table 7-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Ack + CF-Poll
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000–1111	Reserved

Data frames

Source: IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *2012*

A sends a datagram to E



Give **destination** and **source** MAC addresses of the frame encapsulating this IP datagram as the frame is transmitted

1) from A to router 1
2) from router 1 to router 2
3) from router 2 to E

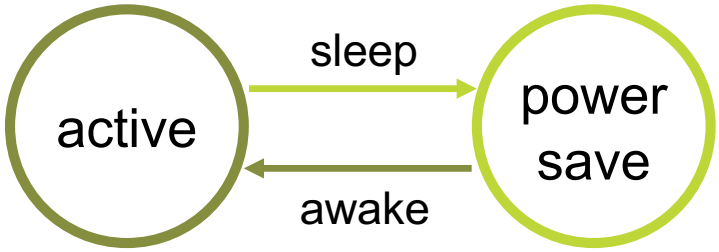
What if Router 1 is replaced by a switch S1, connected to Router 2?

What if Router 2 is replaced by a wireless access point AP1, wired to Router 1?

What are the source and destination IP addresses of the datagram at each of these points?

For battery to last longer: power save mode

- Wireless nodes alternate between active and sleep mode
- Node-to-Access Point: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - Node wakes up before next beacon frame
- Beacon frame contains list of nodes with AP-to-node frames waiting to be sent
  - Node will stay awake if AP-to-node frames to be sent
  - Otherwise sleep again until next beacon frame



Wireless networks: Roadmap

6.1 Introduction

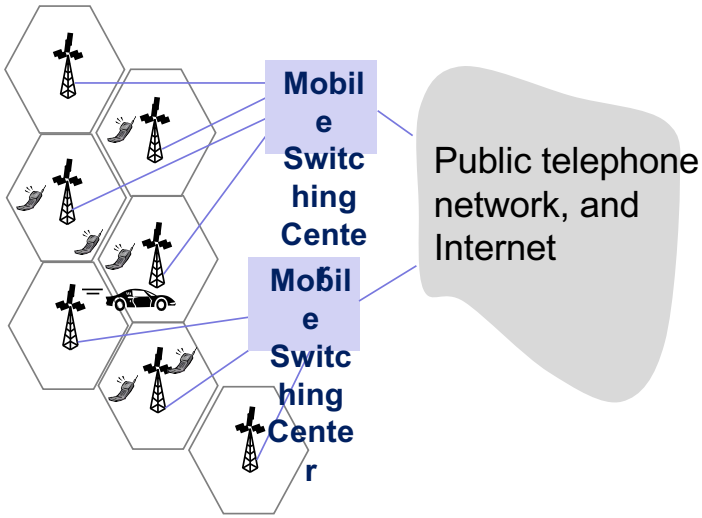
6.2 Wireless links, characteristics
- ~~Code division Multiple Access (CDMA)~~

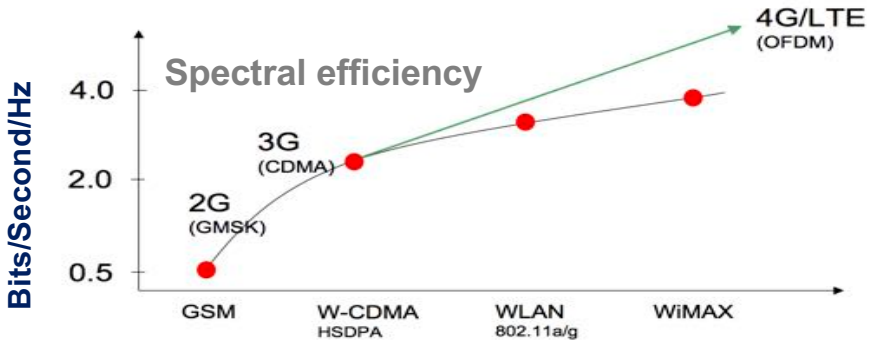
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet Access
- **architecture**
- **standards**

8.8 Securing Wireless LANs

8.8.1 Wired Equivalent Privacy





GSMK Gaussian Minimum Shift Keying, W- CDMA Wideband - Code Division Multiple Access,

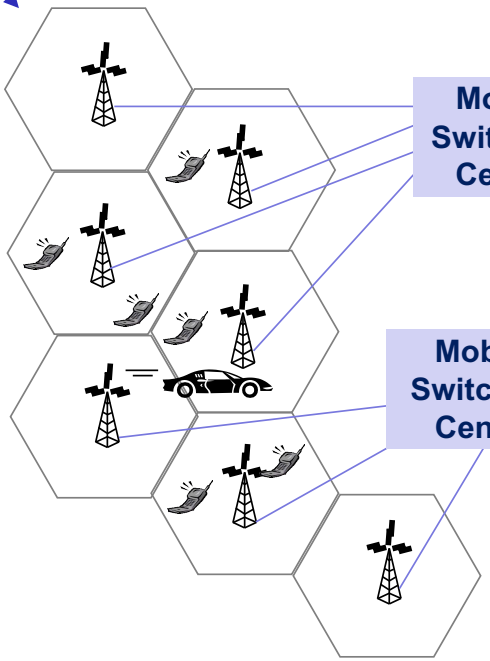
Components of cellular network architecture

Cell

- Covers geographical region
- **base station** (BS) analogous to 802.11 AP
- **mobile users** attach to network through BS
- **air-interface**: physical and link layer protocol between mobile and BS

MSC – mobile switching center

- connects cells to wide area net
- manages call setup
- handles mobility



Mobile Switching Center

Mobile Switching Center

Public telephone network, and Internet

wired network

Cellular network evolution

1G
2.4 kbit/s

- Mobile telephony
- Analog cellular phones, national/regional
- **NMT**, AMPS

2G
64 kbit/s

- Mobile telephony with international roaming, some data (dial-up, SMS)
- Digital cellular phones
- **GSM** (FDMA, TDMA)

2,5 G
250 kbit/s

- Higher data rates (packet switching)
- **GPRS** (2,5G) (FDMA, slotted ALOHA),
  EDGE (2,75G) Enhanced Data rates for GSM Evolution

3 G
2 000 kbit/s

- Voice, data, video telephony, Internet surfing
- **UMTS (**CDMA)
- **HSDPA (Turbo-3G 3,5G 3,6 Mbit/s)**
  HSDPA+ (3,75G 42 Mbit/s dual carrier HDSPA)

4G
100 Mbit/s

- Mobile Internet broadband (voice over IP)
- 4G (OFDMA), **LTE**

4G+
450 Mbit/s

- LTE Advanced (Carrier aggregation)

Evolution of cellular standards

2G systems: voice channels
GSM (global system for mobile communications) combines FDMA/TDMA

were held late last year. Cars equipped with the various technologies on offer were driven around Paris. The winner was a surprise—it was a system called ELAB, that was developed not by a large company but by Trondheim University in Norway. It is based on a 600-kilohertz signal and a choice of 256 or 512 kilobits per second for the data stream. In Madeira the negotiators have the task of deciding whether to ignore the Paris tests or turn down electronics giants such as Ericsson and Standard Elektrik Lorenz in favour of a university laboratory.

Even if an agreement is reached in Madeira, it will be only on how the speech signal should be modulated. The next stage will be for the GSM to draw up a firm specification on the switching control system which is an essential part of cellular radio. If this can be done before the end of 1987, the service could start in 1991.

GSM radioteknologi suveren vinner av Aftenposten leserkåring av Norges beste oppfinnelse

3G systems: mode data, video telephony
A cataclysmic event that drove Europe's mobile system suppliers into recession, set Europe's 3G networks back 5 years and made European governments a great deal of money.

Thursday, 27 April, 2000, 15:56 GMT 16:56 UK

UK mobile phone auction nets billions

BBC

The Internet on the move on the phones of the future

The auction for next-generation mobile phone licences in the UK is over, leaving Chancellor Gordon Brown with a £22.47bn ($35.4bn) windfall.

VG TEKNOLOGI

HSDPA

19-04-2007

I dag åpnes bredbånd på mobilnettet

(VG Nett) Glem 3G og EDGE, i dag åpner NetCom en pilotutgave av bredbånd via mobilnettet. Men bare for hovedstaden.

NetCom lanserte på en pressekonferanse i dag sine planer for mobilt bredbånd. NetCom har kjørt egne tester av HSDPA og fra og med i dag kan alle NetCom-kunder med datakort til PC-en selv teste hastigheten.

Under presselanseringen fikk vi testet linjene og hastigheten lå mellom 1,1 og 1,9 Mbit/s. Det er fire-fem ganger hastigheten man oppnådde med god 3G-dekning. Opplastingshastigheten er raskere enn 3G-nettets nedlasting og ligger på rundt 350 kbit/s.

4G LTE: increased data rate and capacity, better spectrum efficiency, reduced latency and simplified network architecture – all IP

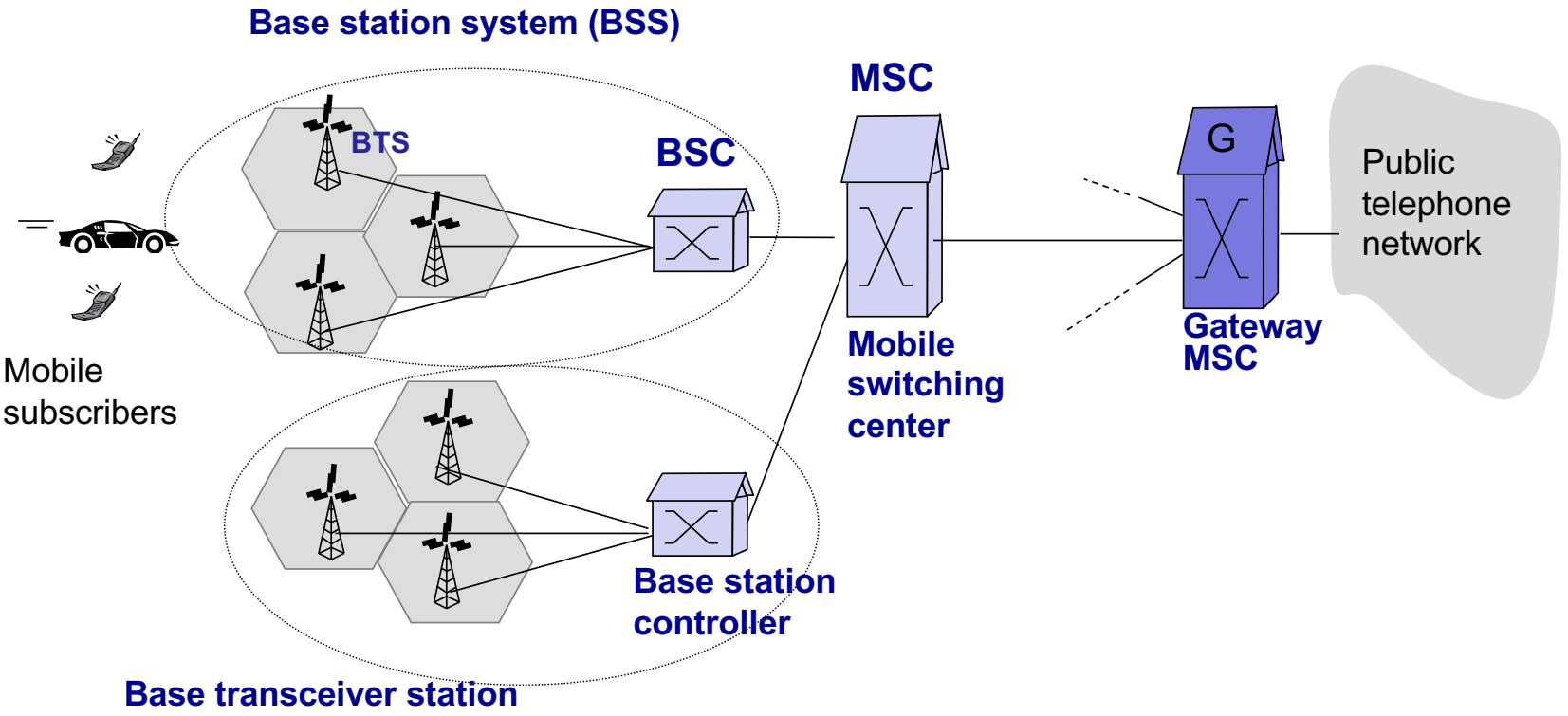
2.5 G systems: voice and data channels

- **GPRS general packet radio service** evolved from GSM, data sent on multiple channels (if available)
- **EDGE** enhanced data rates for global evolution also evolved from GSM, using enhanced modulation, data rates up to 384K

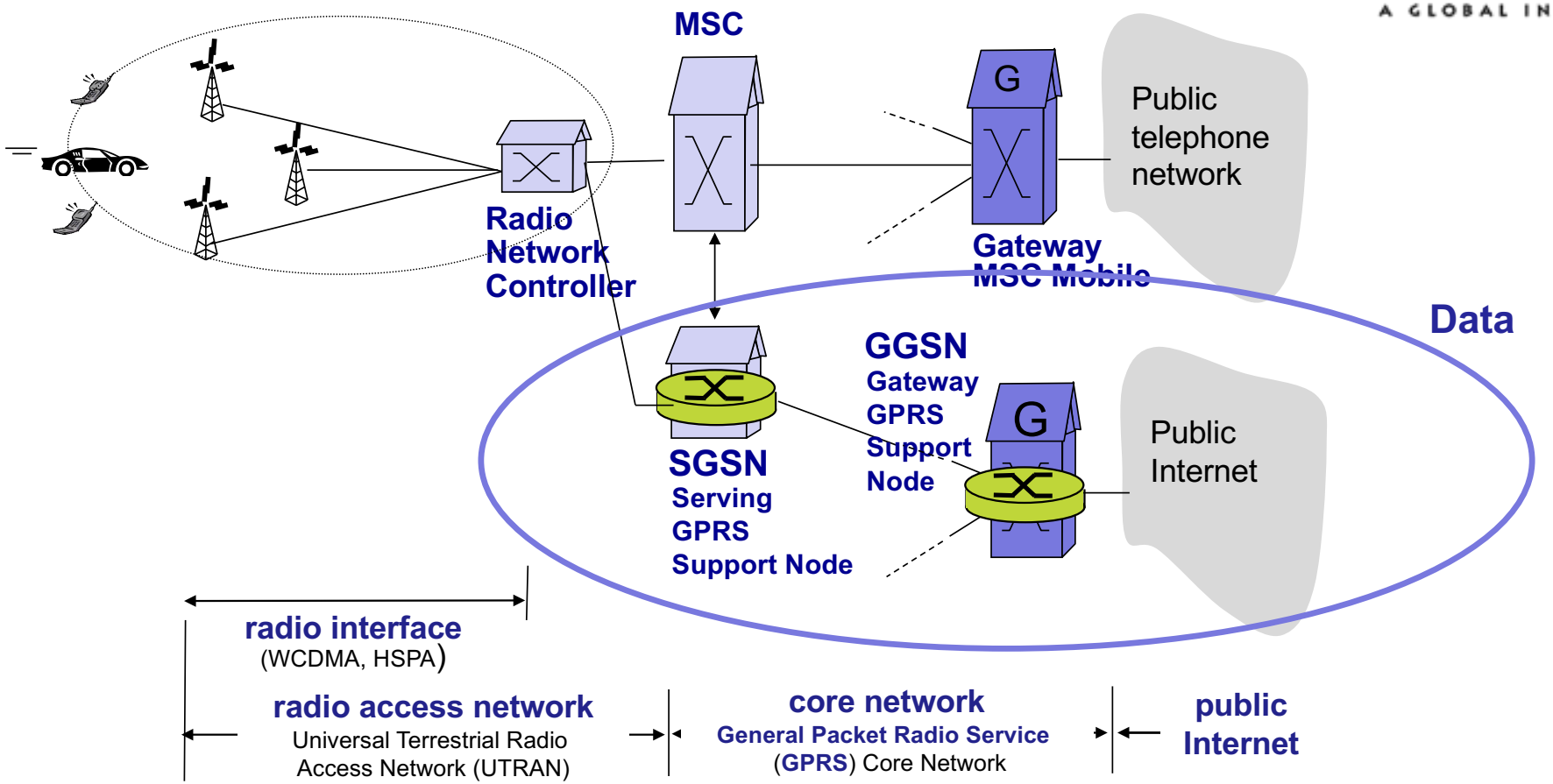
GPRS denne uka Dagbladet

Netcom prøvde å snike seg foran Telenor i GPRS-kappløpet. Me nå ser det ut som Telenor tar siste stikk. 17-01-2001

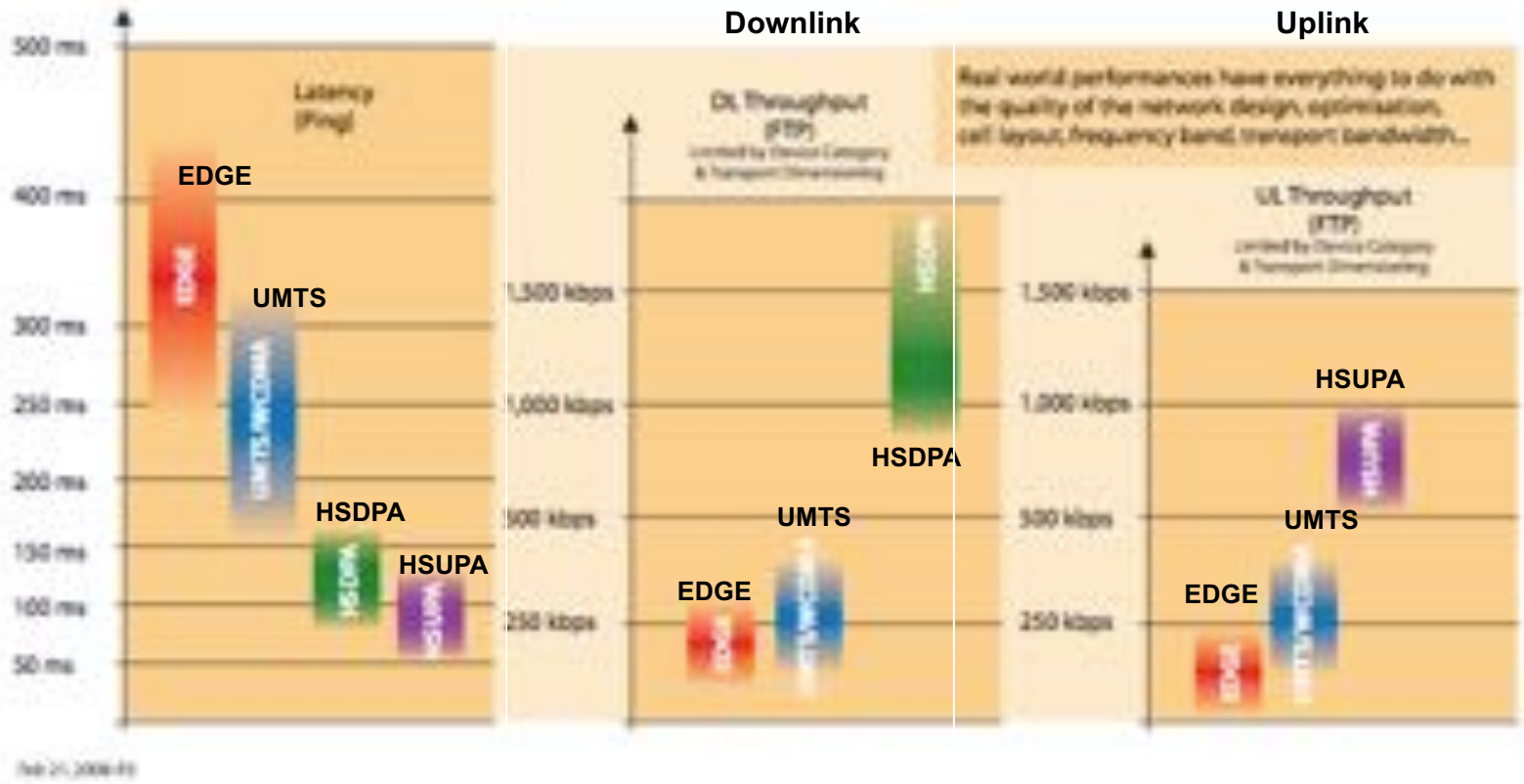
2G (voice) network architecture



3G (voice+data) network architecture

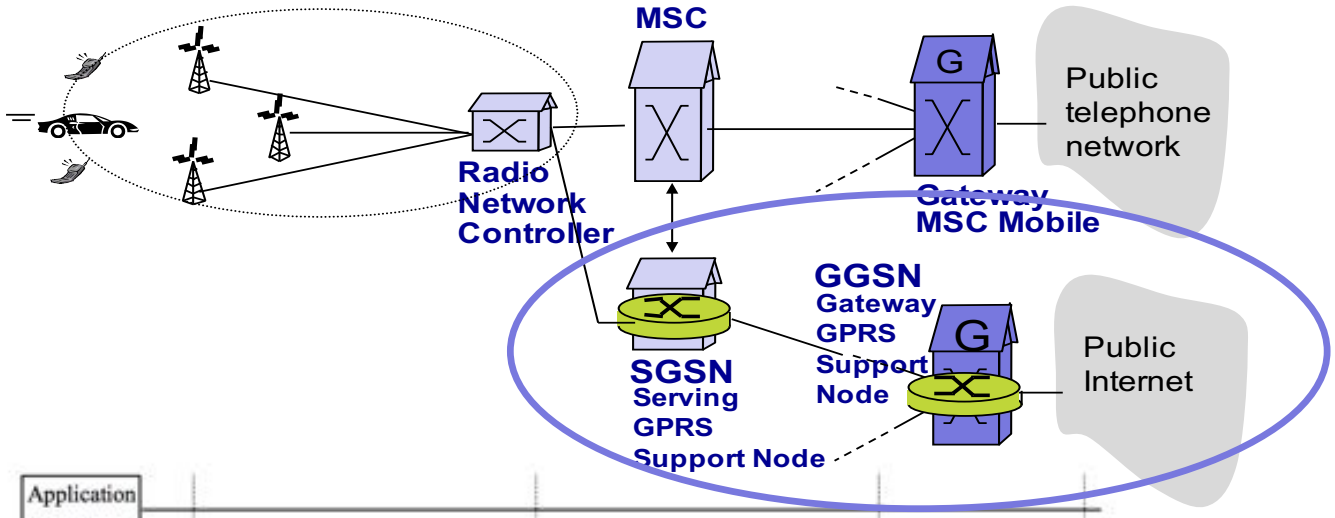


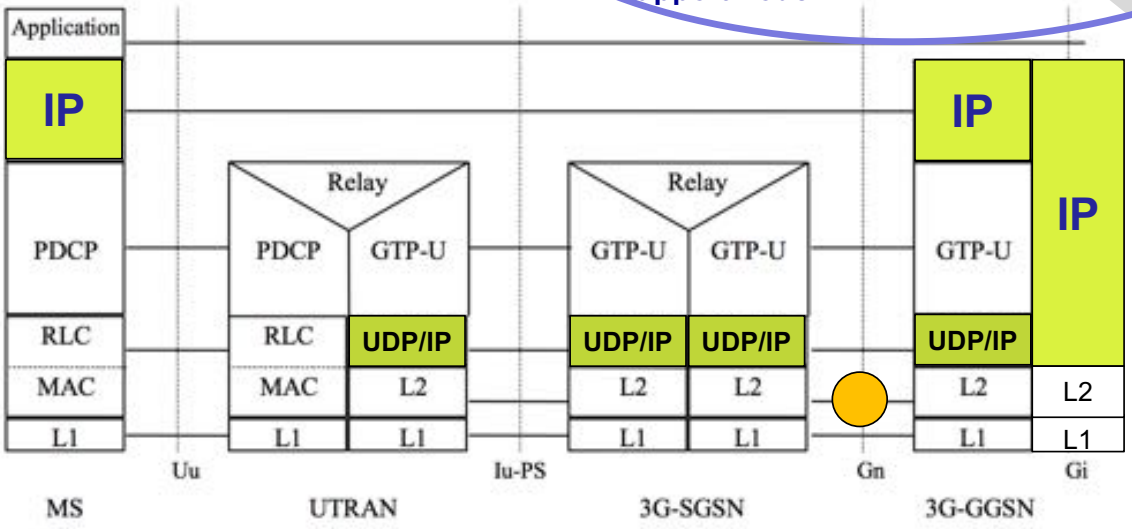
Mobile cellular access technologies – 2G/3G



Data for initial HSPA implementations (2007) under typical load conditions; devices limited to 3.6 Mbit/s in DL and 1.5 Mbit/s in UL.

3G (voice+data) GPRS protocol stack

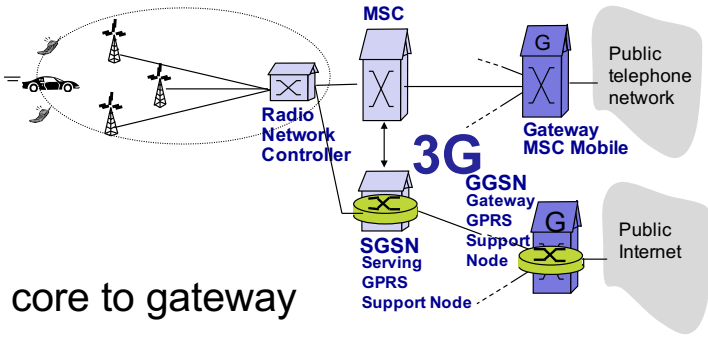




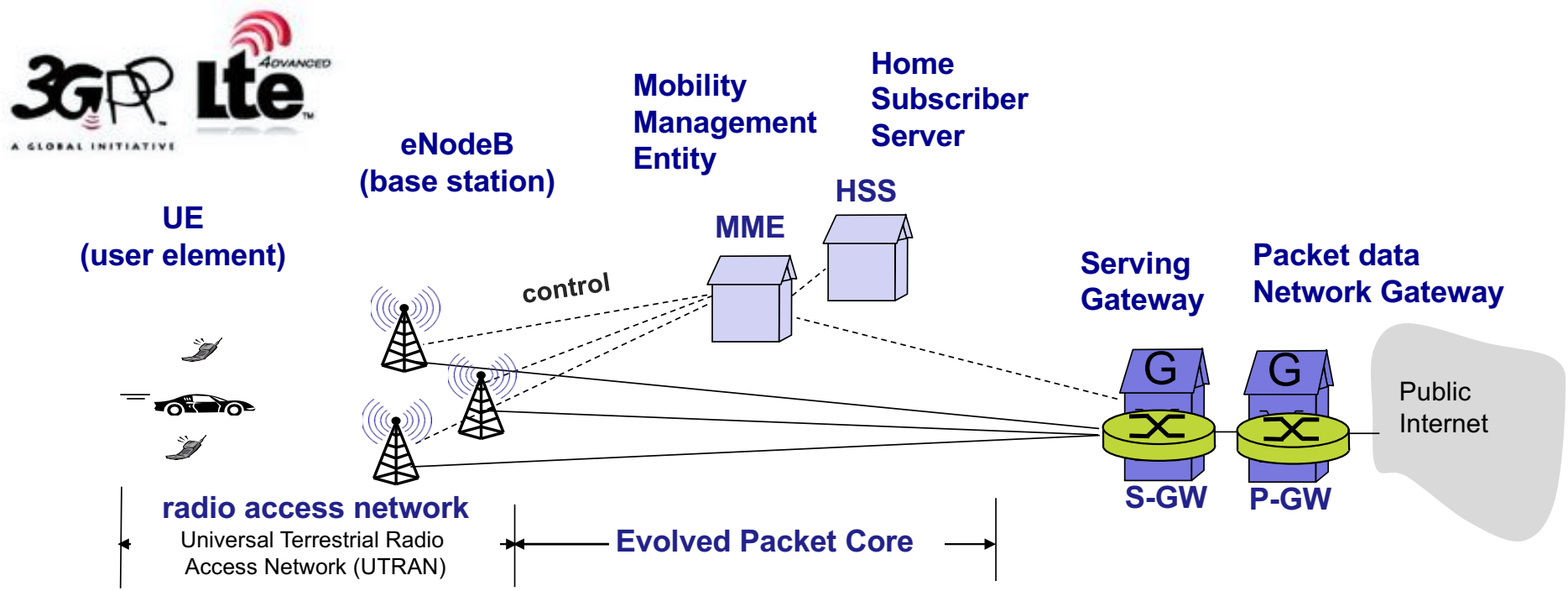
MSC: Mobile Switching Centre
GPRS: General Packet Radio Service
PDCP: Packet Data Convergenc Protocol
RLC: Radio Link Control
MAC: Medium Access Control
GTP-U: GPRS Tunnelling Protoc – User plan
UDP: User Datagram Protocol
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRT Support Node
MS: Mobile Station
BSS: Base

Using IP VPN here gives yet another IP layer!

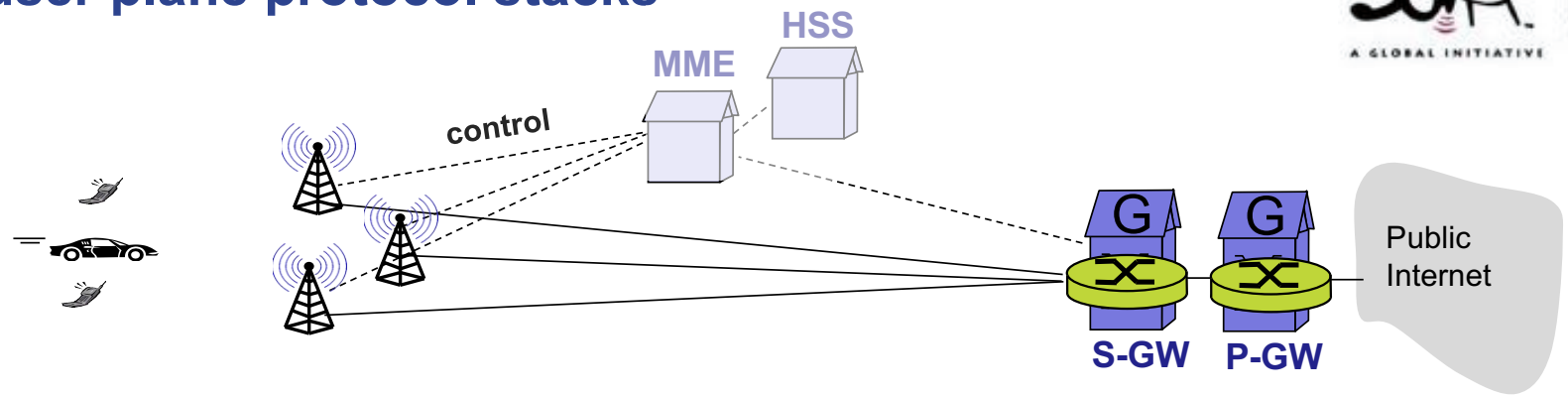
4G LTE network architecture

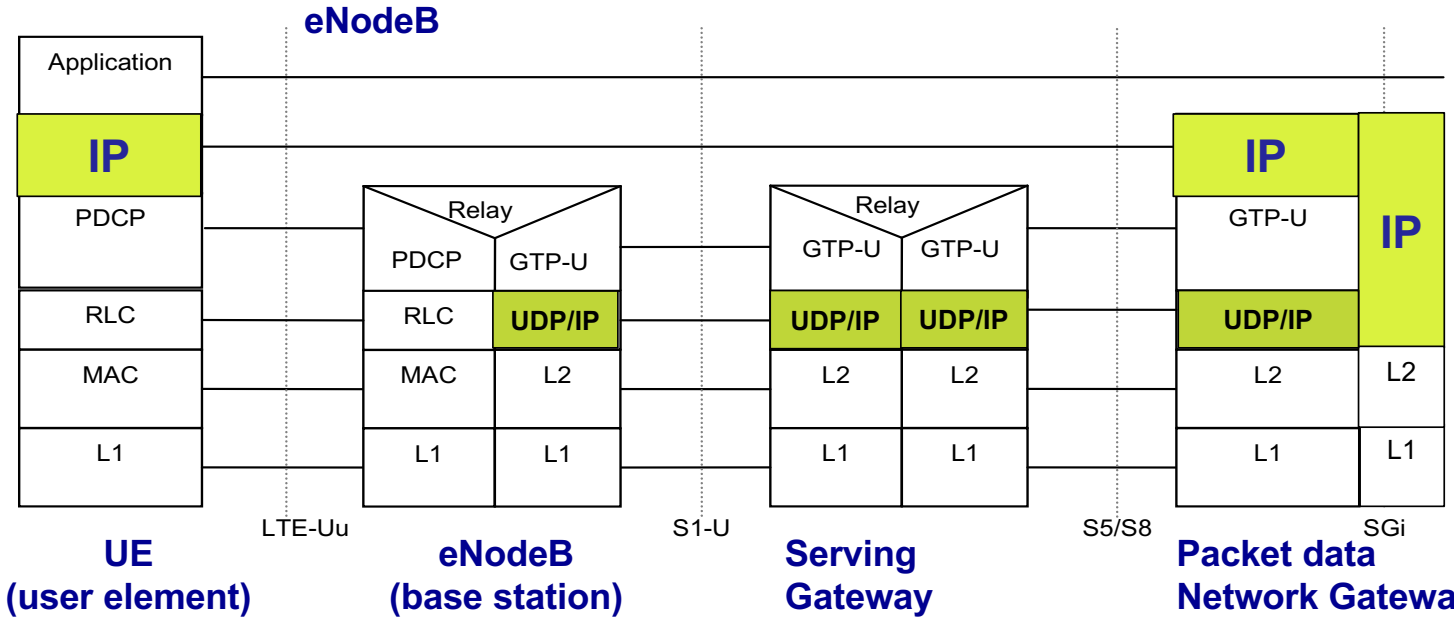


- **All IP core**: both data plane and control plane based on IP
- no separation between voice and data – all traffic carried over IP core to gateway

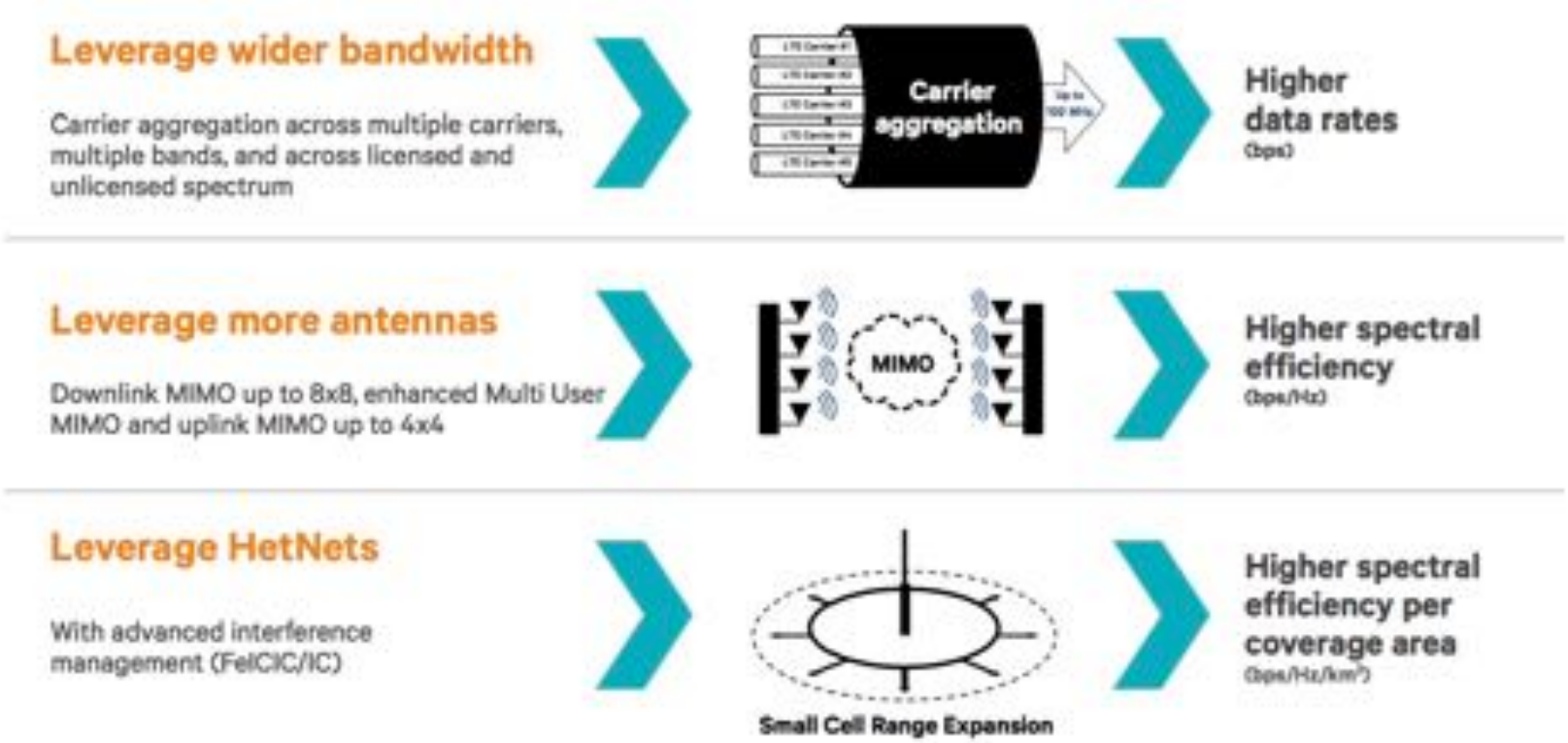


LTE user plane protocol stacks





LTE Advanced brings different dimensions of improvements



Source: Qualcom 2014 LTE advanced: evolving and expanding into new frontiers

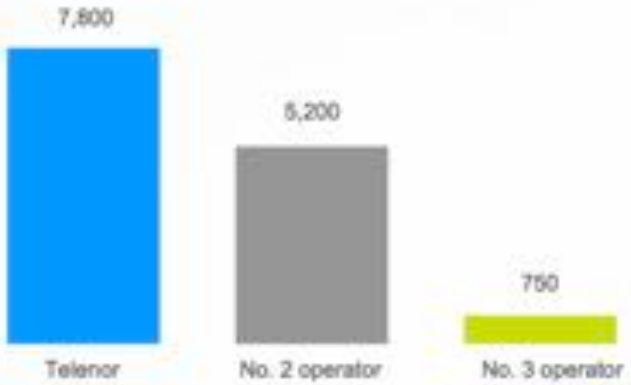
02.08.2017

CMD 2017

INVESTMENTS IN RECENT YEARS HAS RESULTED IN A WORLD CLASS MOBILE NETWORK

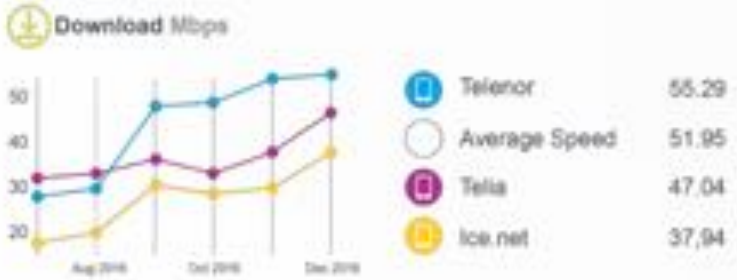
telenor

Highest number of network sites*



- 50% more sites than no. 2 operator
- 97.6% population coverage on 4G
- 91.4% pop coverage on 4G+

Best capacity **



Telenor dekning	Befolkningsdekning	Flatedekning
GSM alle net	99,8%	82%
UMTS (3G)	95%	39,85%
LTE (4g)	52%	3,64%

Jan 2014, http://www.cw.no/artikkel/telekom/fiber-utfordringen-4g-mobil

15

* Network sites as of 1 Oct 2016. Source: finnsenderen.no
** Based on Ookla's analysis of Speedtest Intelligence data from 1 Aug 2016 to 31 Dec 2016, approved by Ookla

telenor

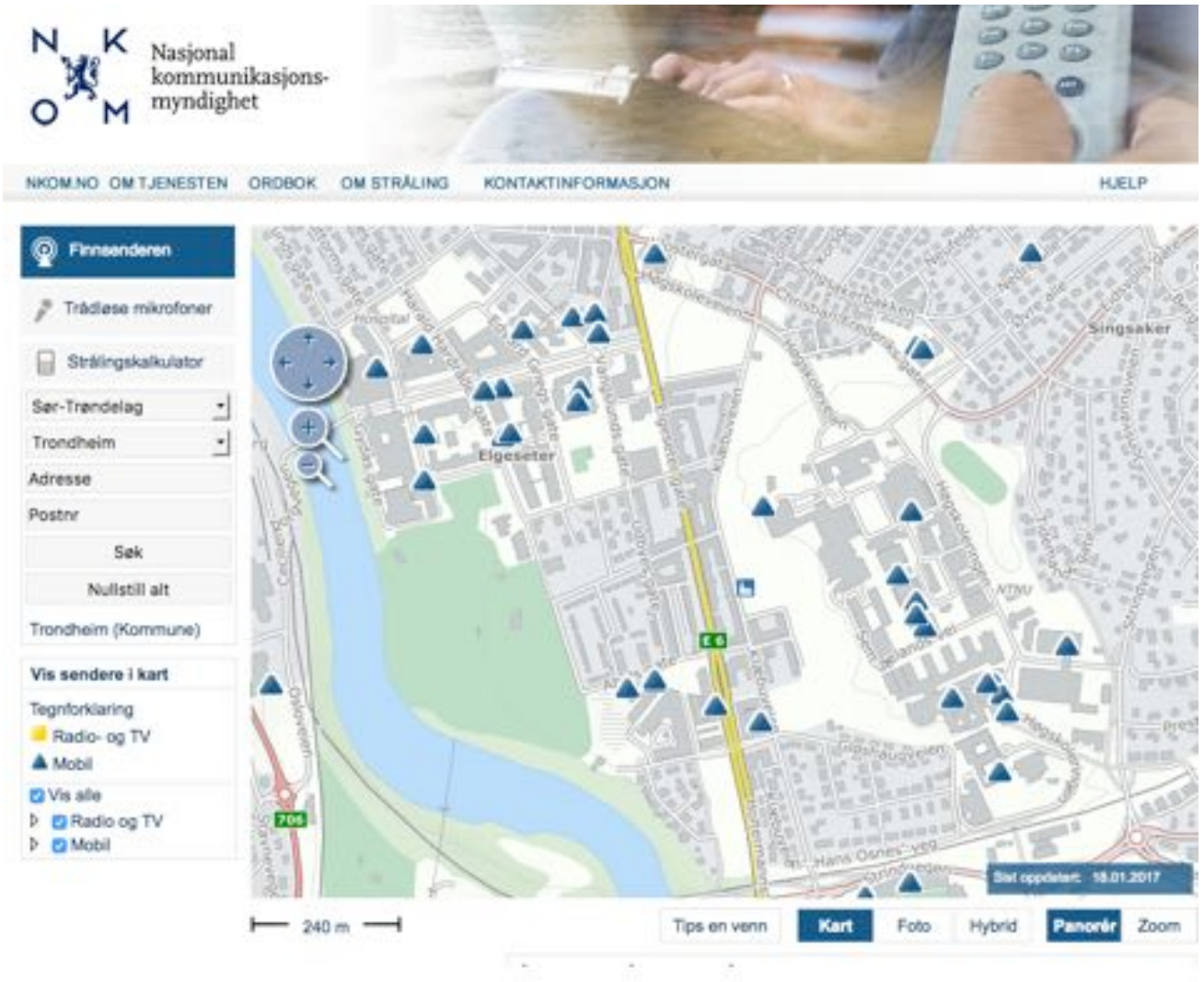
Telenor dekningskart https://www.telenor.no/privat/dekning/
Telia dekningskart: https://telia.no/dekningskart

Telia

Mobilsendere – oversikt

Finnsenderen er en søketjeneste som gir deg oversikt over mobilsendere i Norge, hvor de er plassert, og hvilke selskap som eier og driver dem.

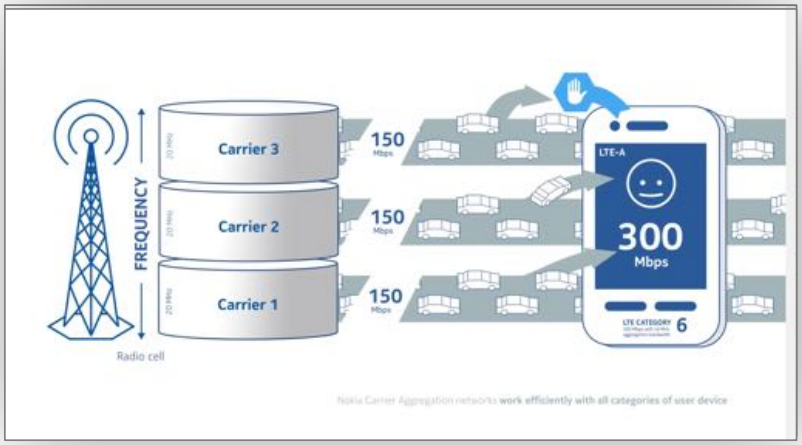
http://www.finnsenderen.no/finnsender



The mobile networks meet the Internet

https://www.youtube.com/watch?v=4YgGuK9cuSU

https://www.youtube.com/watch?v=lNQcSgKVhSk



https://www.youtube.com/watch?v=c4n5SF7Sloc

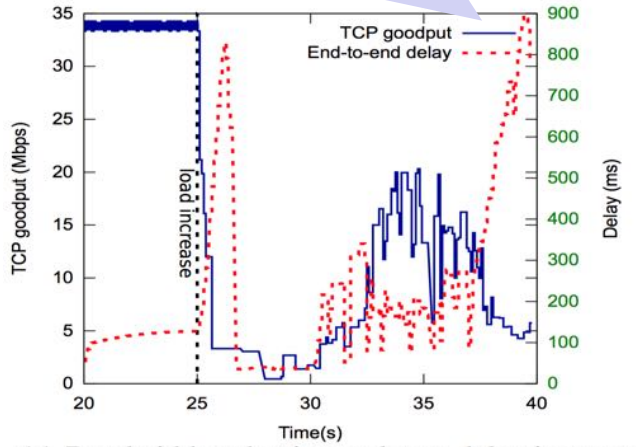
https://www.youtube.com/watch?v=UAKavT8Ux9Q

Wireless & mobility: impact on higher layer protocols

- Logically, impact should be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile networks
- … but
- **performance-wise challenges** due to
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff between base stations
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - TCP uses IP subnet address as part of connection handle – mobility challenge
  - limited bandwidth of wireless links
  - scalability vs wired networks – not all traffic can be put on wireless

Seamless handover causes significant TCP losses while lossless handover increases TCP segments' delay

Load increase in a cell causes dramatic bandwidth reduction on UEs and significantly degrades TCP performance.



(a) Bandwidth reduction and max delay increase

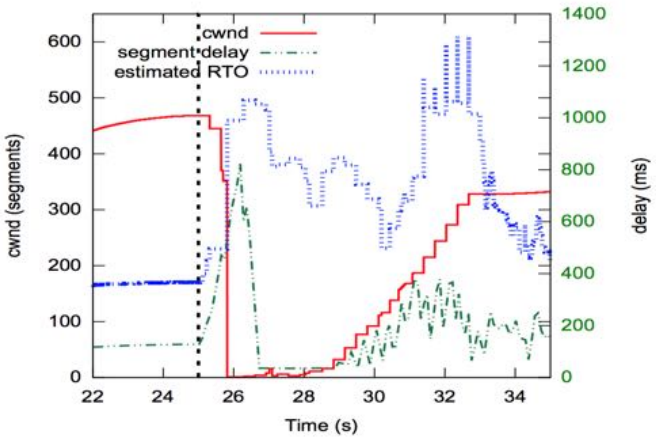


Figure 3: TCP timeout caused by load increase

Source: Nguyen et al: Towards Understanding TCP Performance on LTE/EPC Mobile Networks http://dx.doi.org/10.1145/2627585.2627594 , 2014

Wireless networks: Roadmap

6.1 Introduction

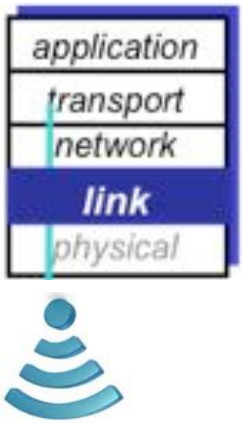
6.2 Wireless links, characteristics
- ~~Code division Multiple Access (CDMA)~~

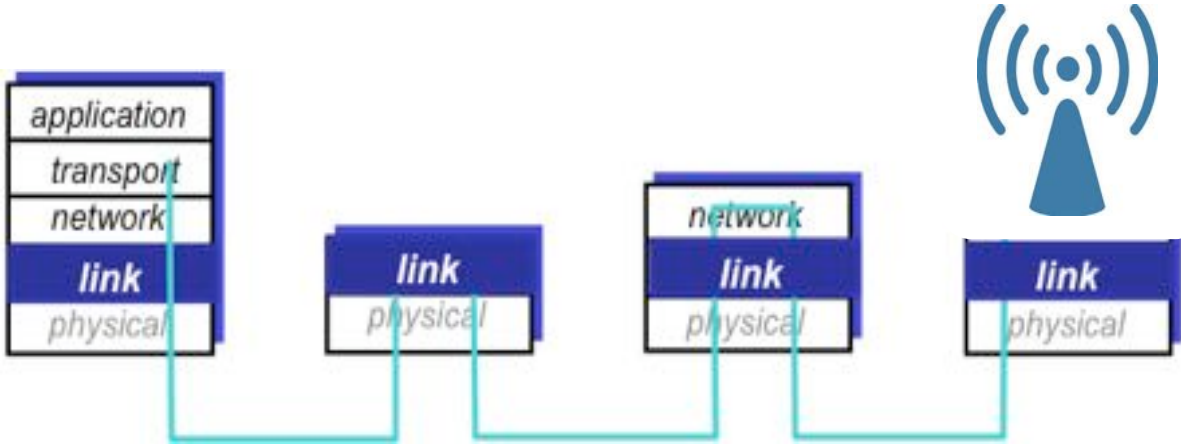
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet Access
- architecture
- standards

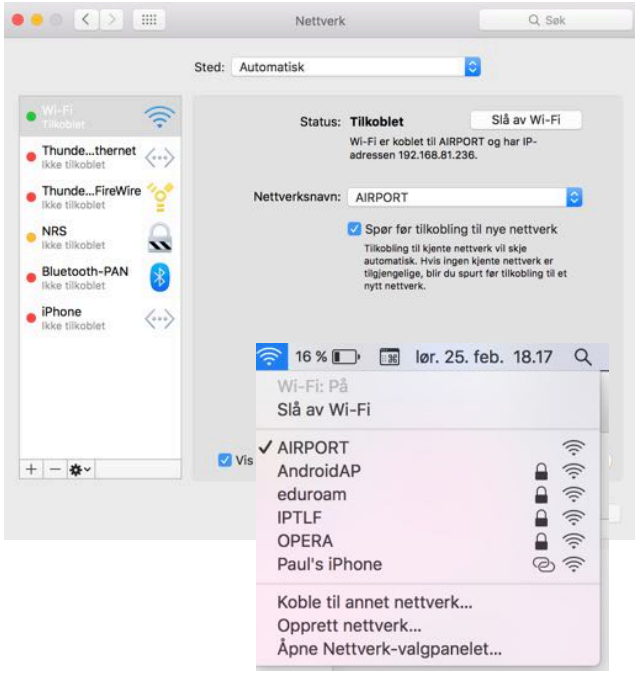
8.8 Securing Wireless LANs

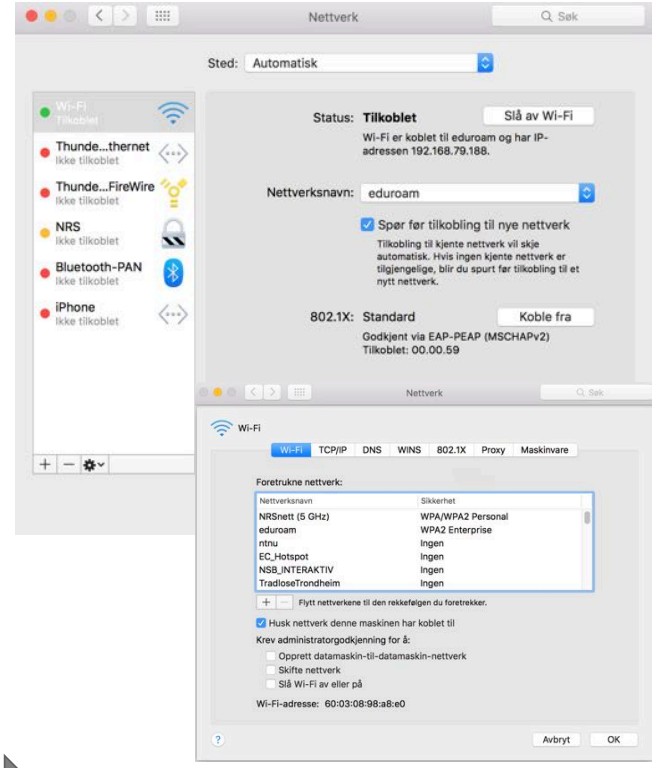
8.8.1 Wired Equivalent Privacy





WiFi Security – From unsecured via Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access (WPA)





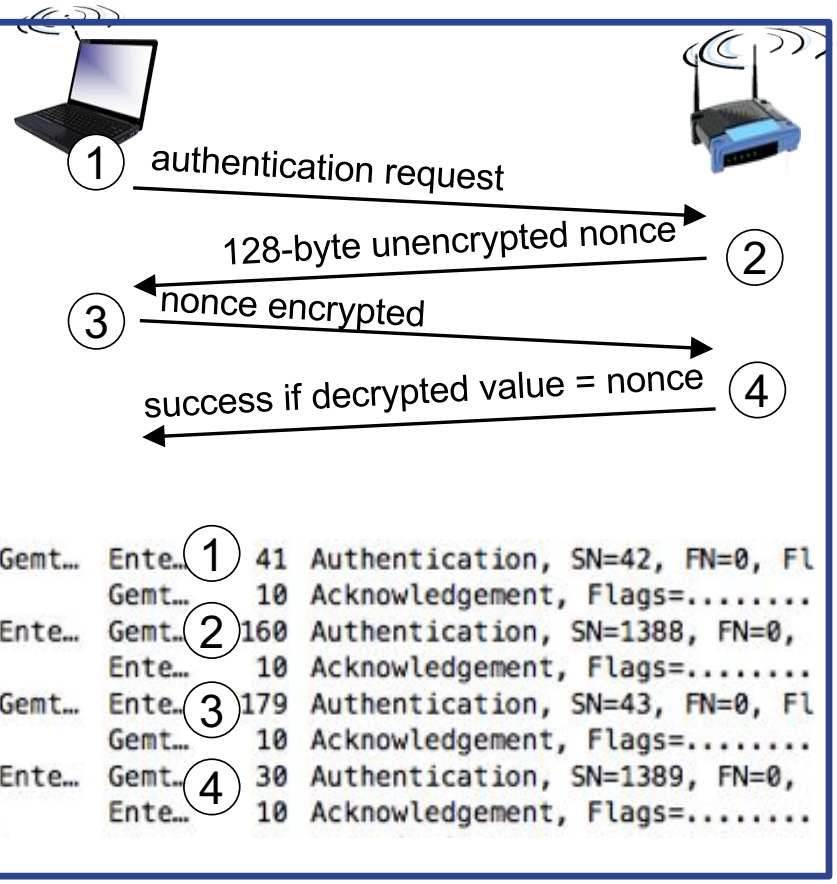
No security

WPA2

Highest security

Wired Equivalent Privacy (WEP) based on symmetric key crypto – goals

- No unauthorized access: end host **authorization**
  - nonce challenge and shared key
  - one way
- No eavesdropping: **confidentiality**
  - per-frame encryption using secret key and Initialization vector
  - IV in clear text in frame
  - Manual configuration of key
- No tampering with messages: Data integrity
  - CRC-32

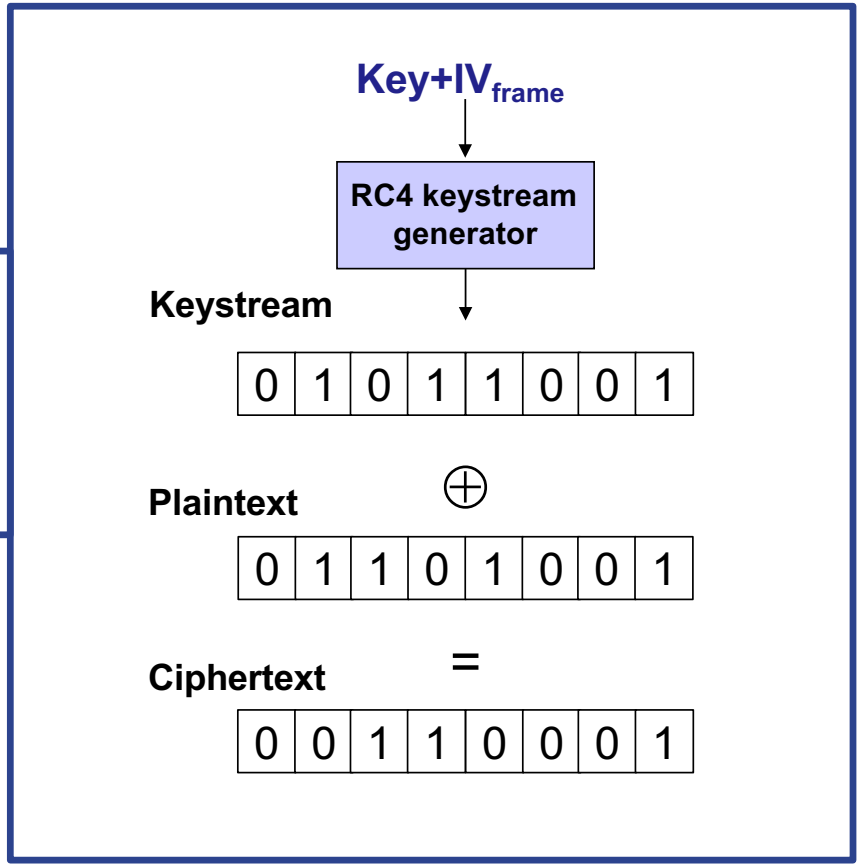


SN Sequence number

Wired Equivalent Privacy (WEP) based on symmetric key crypto

- No unauthorized access: end host **authorization**
  - nonce challenge and shared key
  - one way

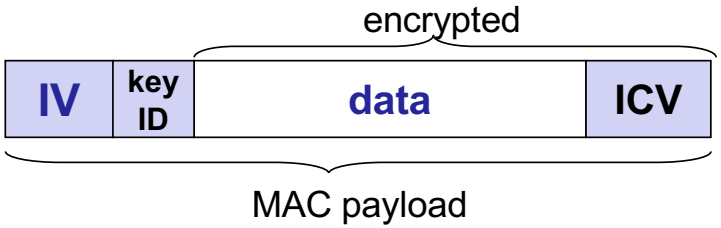
- No eavesdropping: **confidentiality**
  - per-frame encryption using secret key and Initialization Vector (IV)
  - IV in clear text in frame
  - manual configuration of key




```
▼ WEP parameters
    Initialization Vector: 0x17f79e
    Key Index: 0
    WEP ICV: 0xa7f5ea83 (not verified)
▼ Data (350 bytes)
  Data: 3128ea481f7fe1fa1c35a8ef5b00ca0bfc4b1170c9a33f6e...
  [Length: 350]
```

Wired Equivalent Privacy (WEP) based on symmetric key crypto

- No unauthorized access: end host **authorization**
  - nonce challenge and shared key
- No eavesdropping: **confidentiality**
  - per-frame encryption using secret key and Initialization vector (IV)
  - IV in clear text in frame
  - manual configuration of key
- No tampering with messages: Data integrity
  - CRC-32 (error detecting code) = Integrity Check Value



- New 24-bit initialization vector transmitted in in clear-text in each frame
- Short IV -> reuse after 5-7 hours on a busy network: keystream repeats
- CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash: linear function of the -> an attacker can modify an encrypted message and easily fix the ICV

NTNU

R.I.P WEP

Weaknesses

- No key management and short key
- The Initialization Vector (IV) is too small
- The Integrity Check Value (ICV) algorithm is not appropriate
- WEP's use of RC4 is weak
- Authentication messages can be easily forged

- **Passive attacks to decrypt traffic:** based on statistical analysis (keys not changed periodically)
- **Active attacks to inject new traffic from unauthorized mobile stations:** based on known plaintext
- **Active attacks to decrypt traffic:** based on tricking the access point
- **Dictionary-building attacks:** possible after analyzing enough traffic on a busy network

Source: http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf
http://www.dummies.com/programming/networking/understanding-wep-weaknesses/

Table 1. *Timeline of WEP death*

Date	Description
September 1995	Potential RC4 vulnerability (Wagner)
October 2000	First publication on WEP weaknesses: *Unsafe at any key size; An analysis of the WEP encapsulation* (Walker)
May 2001	An inductive chosen plaintext attack against WEP/WEP2 (Arbaugh)
July 2001	CRC *bit flipping attack – Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
August 2001	FMS attacks – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Mantin, Shamir)
August 2001	Release of AirSnort
February 2002	Optimized FMS attacks by h1kari
August 2004	KoreK attacks (unique IVs) – release of chopchop and chopper
July/August 2004	Release of Aircrack (Devine) and WepLab (Sanchez) implementing KoreK attacks

Source: Guillaume Lehembre. Wi-Fi security – WEP, WPA and WPA2, Hakin9 6/2005

WiFi Security – From Wired Equivalent Privacy to Wi-Fi Protected Access 2

WPA addressed WEP flaws. Two modes: personal & enterprise. Use only if WPA2 not available. TKIP no longer considered secure.

”Bruk WPA2-kryptering og skru ned sendestyrken på basestasjonen. Det er ingen grunn til å kringkaste signalet til halve nabolaget.”

WEP has been outdated for years. Easily hacked due to 24-bit IV and weak authentication. Risky choice!

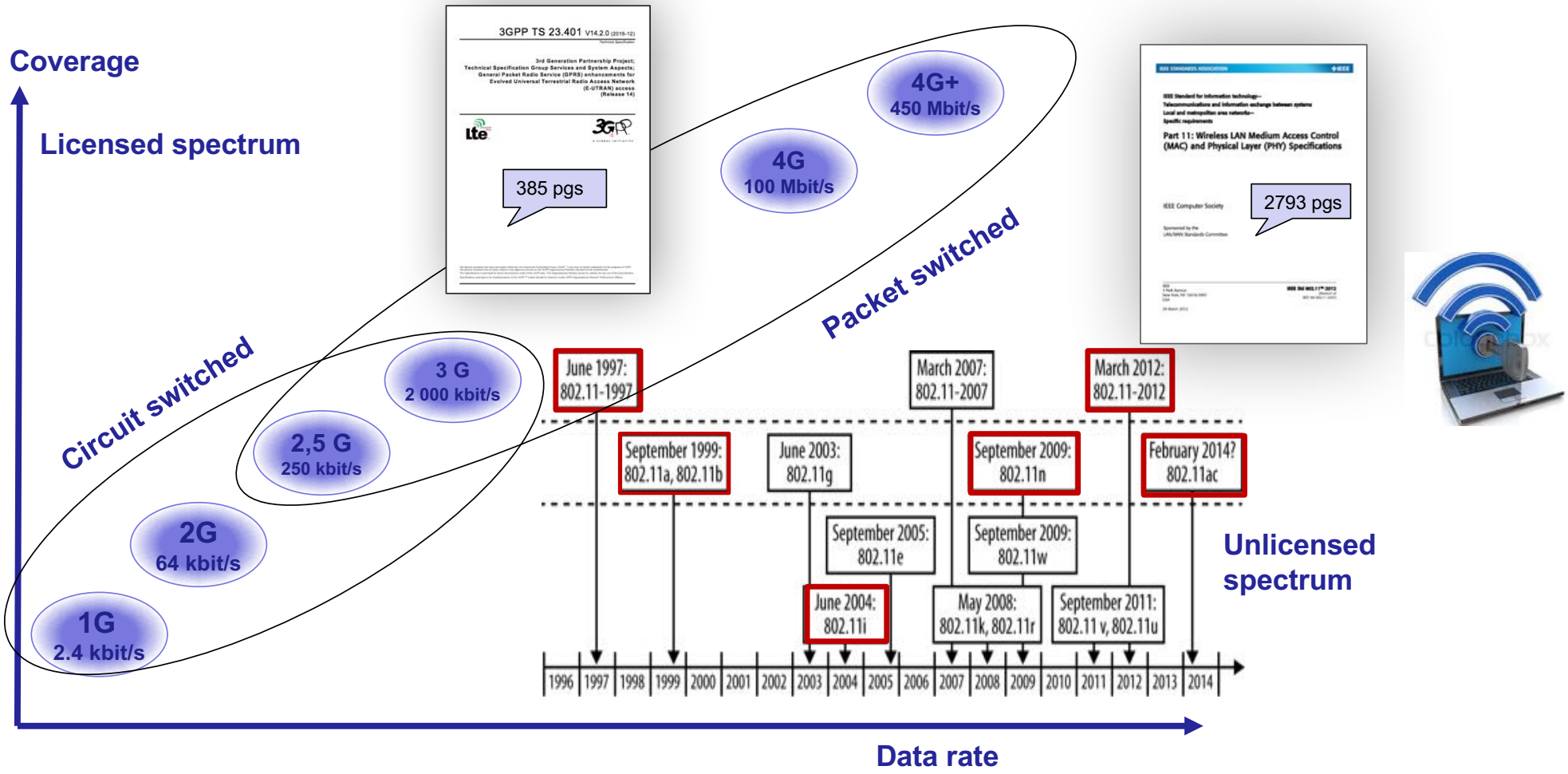
	WEP	WPA	WPA2
Encryption	RC4 (64/128 bit) incl 24-bit initialization vector (IV)	RC4 (64/128/256 bit) 28-bit IV	AES (128 bit)
Key rotation	None, Initial key stream with new (in-clear text) IV per frame	Temporal session keys and per-frame key hashing – Temporal Key Integrity Protocol (TKIP)	Dynamic session keys AES-based CCMP (Counter mode Cipher block chaining Message authentication code Protocol
Key distribution	Each device set manually	Personal (PSK – pre shared key) Enterprise (Radius)	
Authentication	RC4 and same key	Enterprise: 802.1x & EAP extensible authentication protocol	
Integrity	Integrity Check Value (ICV) CRC-32	TKIP 64-bit message integrity check, sequence counter	AES-based CCMP
	1999	draft IEEE802.11i	IEEE 802.11i-2004

Breaking 802.11 WEP encryption: Duplicate key in RC4
The 24-bit initialization vector is a security hole, chosen

- 24-bit IV (Initialization Vector)
  one IV per frame -> IV's eventually reused
  - IV transmitted in plaintext -> IV reuse detected
- Chosen-plaintext attack
  - Trudy causes Alice to encrypt known plaintext $d_1\ d_2\ d_3\ d_4\ \ldots$
  - Trudy sees: $c_i = d_i \oplus k_i^{IV}$
  - Trudy knows c_i and d_i, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence $k_1^{IV}\ k_2^{IV}\ k_3^{IV}\ \ldots$
  - Next time IV is used, Trudy can decrypt!

The IV is too small and in cleartext. It's a 24-bit field sent in the cleartext portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.
The IV is static. Reuse of the same IV produces identical key streams for the protection of data, and because the IV is short, it guarantees that those streams will repeat after a relatively short time (between 5 and 7 hours) on a busy network.
The IV makes the key stream vulnerable. The 802.11 standard does not specify how the IVs are set or changed, and individual wireless adapters from the same vendor may all generate the same IV sequences, or some wireless adapters may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the ciphertext.
The IV is a part of the RC4 encryption key. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack that recovers the key after intercepting and analyzing only a relatively small amount of traffic. Such an attack is so nearly a no-brainer that it's publicly available as an attack script and as open-source code. H
Source: http://www.dummies.com/programming/networking/understanding-wep-weaknesses/

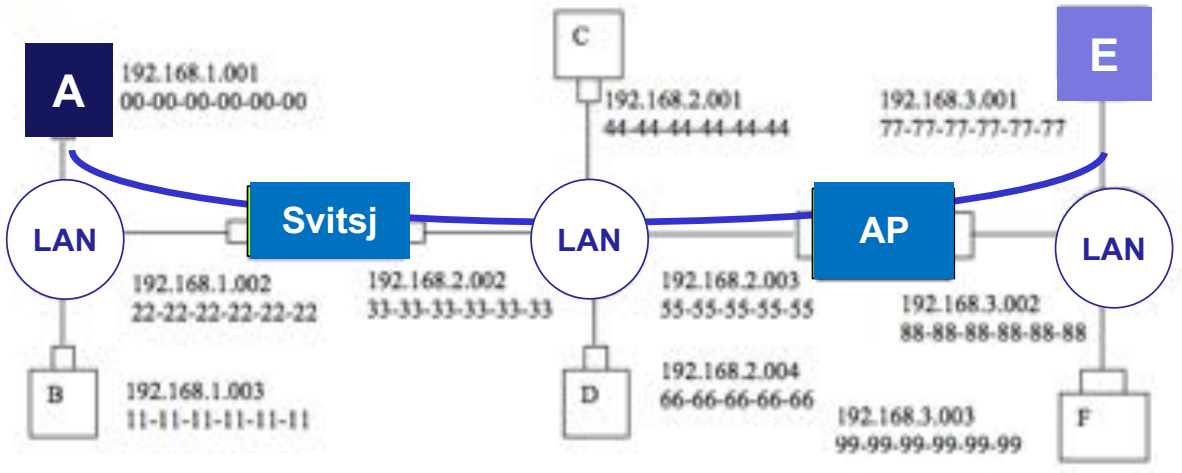
Summary wireless and mobile: significant improvements in radio link bandwidth and efficiency -> Internet access networks



Next lecture multimedia networking, March 16-17

10	Friday 09:15 – 11:00	Wireless Networks (cont)	R1	Kjersti	Chapter 6 Chapter 8.8 and 8.8.1
10	**Friday 16:00**	**Deadline** for KTN1 – Project Design		Assistants/ Magnus	Show project design to course assistants for approval, at P15.
11-12	Mon – Fri 08:15 – 16:00	Project implementation (KTN2)	P15 - Rall	Assistants/ Norvald	
11	Thursday 12:15 – 14:00 Thursday 14:15 – 15:00	Multimedia Networking Theory Assignment 6: *Wireless and Mobile Networks*	R1 R1	Kjersti Assistants/ Ida/Norvald	Chapter 7 One must deliver and pass at least 5 of the 8 theory assignments.
11	Friday 09:15 – 11:00	Multimedia Networking (cont)	R1	Kjersti	Chapter 7
12	**NOTE:**	**No lecture from textbook in week 12.**			

A sends a datagram to E



I Give **destination** and **source** MAC addresses of the frame encapsulating this IP datagram as the frame is transmitted

1) from A to router 1
2) from router 1 to router 2
3) from router 2 to E

x	x	x

What if Router 1 is replaced by a switch S1, connected to Router 2?

What if Router 2 is replaced by a wireless access point AP1, wired to Router 1?

What are the source and destination IP addresses of the datagram at each of these points?