MOBILE & WIRELESS NETWORKS

OVERVIEW OF TECHNOLOGIES AND PROTOCOLS FOR MOBILE AND WIRELESS NETWORKS

Peter R. Egli
INDIGOO.COM

Contents

1. Wireless technologies overview (1/5)

Name	Standard	F-Spectrum	Data rate	Range	Power cons.	Applications / comments
WiMAX	IEEE 802.16a, d	Div.	75Mbps	6km	High	Mobile MAN (users with PDAs, nomads). Will probably be supplanted by LTE.
WRAN	IEEE 802.22	54MHz - 862MHz	4.54 to 22.69 Mbit/s	<30km	High	WRAN is a new working group in IEEE for using TV frequency for broadband access (white space spectrum). Work in progress.
WiBro	IEEE 802.16e	2.3GHz	1Mbps	<=1km	Low	South Korean competitor to WiMAX. Mobile (60km/h moving mobile devices).
GSM (2G)	Div.	850/1800/1900	14.4Kbps	15km	Low	2nd generation mobile telephony technology.
CDMA (2G)	Div.	N/A	2Mbps	15km	Low	G2 technology used in US and other countries (competitor to GSM).
EDGE (2.5G)	N/A	850/1800/1900 Mhz	384Kbps	15km	Low	Enhanced Data rates for GSM Evolution (2.5G); technology between G2 (GSM) and UMTS (G3).
EUCH (2.5G)	N/A	N/A	N/A	N/A	N/A	Enhanced Uplink Channel.
CDMA2000 (3G)	N/A	N/A	144Kbps	N/A	N/A	Competitor to UMTS
UMTS (3G)	Div.	N/A	2Mbps	15km	Low	Would-be successor to GSM. Slow adoption rate, but picking up speed.
EV-DO (3.5G)	N/A	N/A	3.1Mbps down 1.8Mbps up	N/A	N/A	Enhancement of CDMA2000, competes with HSDPA (counterpart in UMTS family).
HSDPA (3.5G)	Div.	N/A	<20Mbps	N/A	N/A	High Speed Downlink Packet Access.
LTE (3.9G/4G)	3GPP LTE	Candidate: 2.6GHz	160 Mbit/s (DL) 54Mbit/s (UL)	<30km	N/A	4G technology, potential successor to UMTS. Based on TCP/IP, no TDM. Low latency (<5ms) for IP packets.
iMode	N/A	N/A	N/A	N/A	Low	Japanese packet service for mobile devices (GPRS).
VSAT	N/A	N/A	~0.5Mbps duplex	3000km	High	Very small aperture Satellite
TETRAPOL	ETSI	N/A	N/A	N/A	N/A	Voice and data radio technology for public services (police etc.).

1. Wireless technologies overview (2/5)

Name	Standard	F-Spectrum	Data rate	Range	Power cons.	Applications / comments
DECT	ETSI	1800-1900MHz	552Kbps	100m	Low (by design)	Digital Enhanced Cordless Telephony. TDMA. Well established
WLL	N/A	N/A	N/A	N/A	High	Wireless Local Loop.
IrDA	IrDA	Visible light	1.6Mbps	8m	Low	Infrared; transmission needs line of sight. Mostly used for remote controls.
BlueTooth	BlueTooth	2.45MHz ISM	1Mbps	30m	Medium	Consumer market (mice, PDAs, keyboards). Pretty complex technology.
WiBree	WiBree / BT	2.45MHz ISM	1Mbps	10m	Very low	Derived from Bluetooth; targets very low power applications. Integrated in bluetooth standard in 2007 as ULP (Ultra Low Power). Apps: consumer, medical, sports & wellnes (watches etc.).
ANT+	Proprietary (Dynastream)	2.4GHz	<57Kbps	30m	Very low	See www.thisisant.com. Ultra low power radio technology for watches, sensors etc.
UWB	IEEE 802.15.3a	3.1-10.6 GHz (US) 24GHz (China)	<480Mbps	10m	N/A	Ultra Wide Band. Very high BW for PANs. Discontinued in 2006.
WHDI	WHDI 1.0	5GHz	<3Gbps	30m	High?	Home entertainment. Industry initiative (Sony et.al.). Competitor of WirelessHD.
WiGig	IEEE 802.11MAC 1.0 WiGig	2.4/5/60GHz	<7Gbps	N/A	High?	Home entertainment. Industry initiative by HW vendors (Atheros, Nokia et.al.). Competitor of WirelessHD. Uses 802.11 MAC for compatibility.
Wireless USB	CWUSB	<8m	<480Mbps	10m	N/A	Based on UWB radio technology; USB cable replacement.
WirelessHD	WirelessHD 1.0, IEEE 802.15.3c	57-64GHz	3GBbps	10m	N/A	Wireless PHY and MAC layer for use in HD WVAN (Wireless Video Are Network)
HomeRF	N/A	2.45MHz ISM	20Mbps	150m	N/A	Was competitor to 802.11. Now defunct
WLAN	IEEE 802.11a	5GHz	<54Mbps	100m	High	First 802.11 Phy standard.
WLAN	IEEE 802.11b	2.45MHz ISM	<11Mbps	100m	High	Low cost variant of 802.11; in widespread use.
WLAN	IEEE 802.11g	2.45MHz ISM	<54Mbps	100m	High	To supplant 802.11b.
WLAN	IEEE 802.11n	2.45MHz ISM	100-200Mbps	100m	High	High data rates with MIMO technology.
WLAN	IEEE 802.11ac	5GHz	<1Gbps	N/A	High	Enhancement to 802.11n with higher throughput. Standard in progress.
WLAN	IEEE 802.11ad	60GHz	<7Gbps	<10m	High	Forthcoming standard, possibly based on Wigig standard.
HiperLAN2	HiperLAN	5GHz	54Mbps	100m	High	European competitor to 802.11
WirelessHD	WirelessHD 1.0, IEEE 802.15.3c	57-64GHz	3GBbps	10m	N/A	Wireless PHY and MAC layer for use in HD WVAN (Wireless Video Are Network)

1. Wireless technologies overview (3/5)

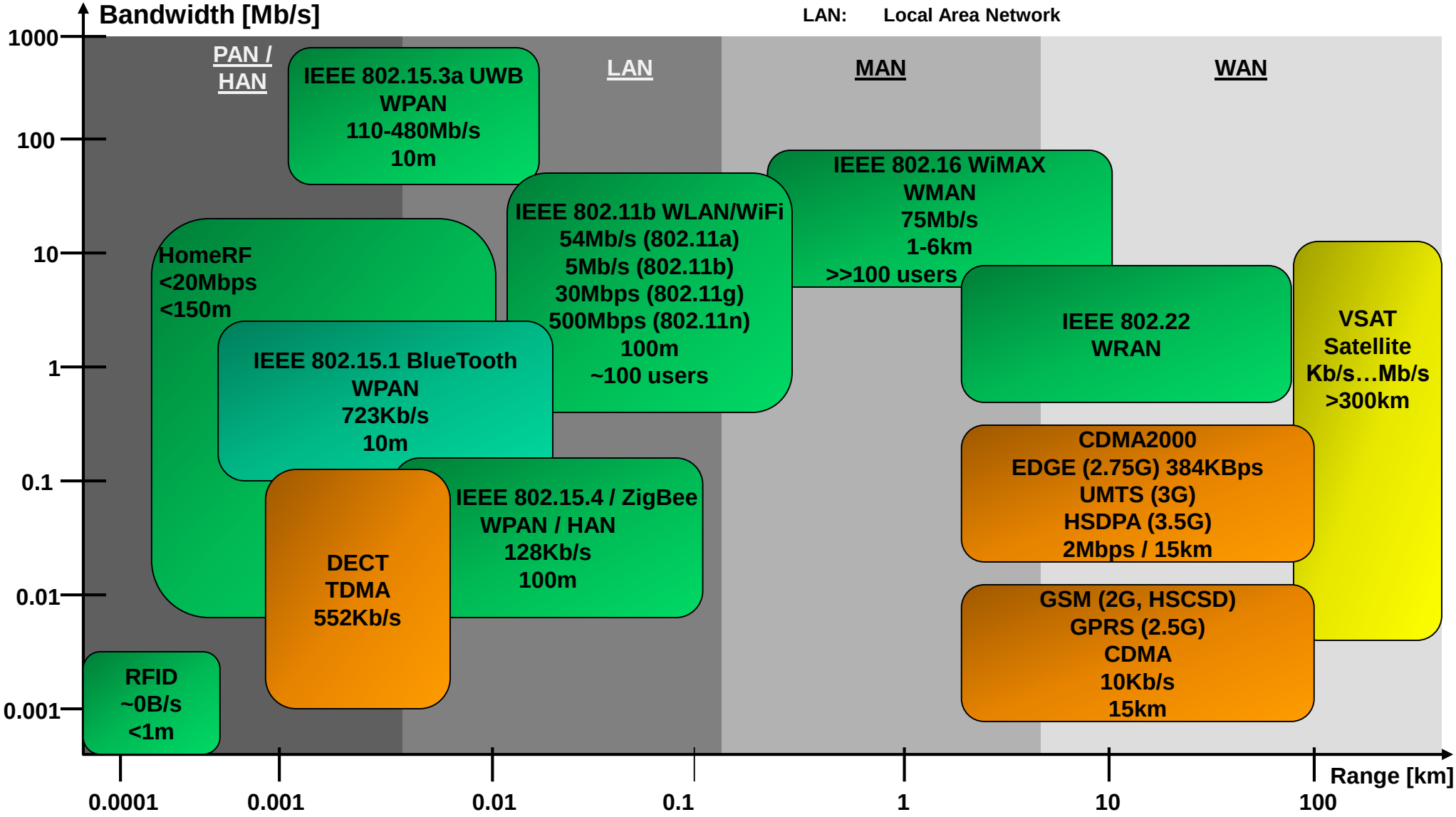
Name	Standard	F-Spectrum	Data rate	Range	Power cons.	Applications / comments
RFID	EPCglobal Gen2 ISO/IEC 18000	Div. (13.56MHz, 135kHz, 2.45GHz, 860 MHz to 960 MHz , 433MHz)	100KBit/s	1m	Zero	Radio Frequency ID tags; wireless access to serial numbers etc.; very low bandwidth and distances. Huge market in the offing.
NFC	ISO/IEC 18092 ECMA 340 ETSI TS 102 190	13.56MHz	< 212KBit/s	0 - 20cm	Pass. & Act.	Near Field Communication.
Transferjet	ECMA 398, ISO/IEC 17568	4.48GHz	375 Mbps	<10cm	N/A	Low proximity high throughput technology.
ZigBee	IEEE 802.15.4, ZigBee standard	2.45GHz 868MHz (Eu) 915MHz (US)	128KBit/s	100m	Low (by design)	Control and monitoring (sensors). Aimed at applications where BlueTooth is too complex and has too much power consumption. Requires certification.
MiWi	IEEE 802.15.4, MiWi	2.45GHz ISM	128KBit/s	100m	Low (by design)	ZigBee alternative from Microchip. Uses IEEE 802.15.4 radio; low cost (licenses!) alternative to ZigBee. No certification required.
Wireless Body Area Networks	IEEE 802.15.6	ISM bands. Low band: 3.5GHz-4.5GHz High band: 6.5GHz-9.9GHz	<10MBit/s	<3m (low data rate)	Extremely low	Wireless Body Area Network (BAN) standard. Hub and spoke network topologies. Target applications: Medical (transceiver close to human body).
Short-Range Wireless Optical Communication	IEEE 802.15.7	Visible light (380 - 780nm)	Low rate: <266KBit/s High rate: <96MBit/s	A few meters	Low	Applications with increased EMC immunity requirements. Traffic signal to vehicle etc.

1. Wireless technologies overview (4/5)

Name	Standard	F-Spectrum	Data rate	Range	Power cons.	Applications / comments
Wireless-M-Bus	EN13757-4, EN13757-3	868MHz	16.4KBit/s	15m-25m	Low	Wireless electrical power meter connectivity. Wireless version of M-Bus.
io-homecontrol	io-homecontrol	868MHz	N/A	N/A	Low	Home automation (light, roller shutter etc.)
Z-Wave	Z-Wave Alliance	908.42Mhz (US) 868MHz (Eu)	9.6KBit/s - 100KBit/s	100m	Low (by design)	Home appliances, sensors. Designed for robustness (crowded frequency bands). MAC and PHY layers standardized by ITU-T (G.9959).
NanoNet	Proprietary	2.45GHz ISM	N/A	N/A	N/A	www.nanotron.com
enOcean	ISO/IEC 14543-3-10	315MHz (US), 868MHz, 902MHz	120KBit/s	N/A	None (energy harvesting)	No power sensors (energy harvesting).
DASH7	ISO/IEC 18000-7	433MHz	200 kbit/s	1000m	Low	RFID technology for worldwide conformance and interoperability.
Wireless HART	IEC EN 62591	2.4GHz	250 kbits/s	30m (indoor) 100m (outdoor)	See 802.15.4	Based on IEEE 802.15.4 MAC
SigFox	ETSI GS LTN 003	868MHz (Eu) 902MHz (US)	10b/s to 1kb/s	Up to 40km	Very low	LPWAN: Wireless technology for IoT sensor networks (alternative to costly 3G, 4G networks).
LoRaWAN	Proprietary	868MHz	10b/s to 10kb/s	Up to 40km	Very low	LPWAN: Wireless technology for IoT sensor networks (alternative to costly 3G, 4G networks).
Weightless-W	Proprietary	54MHZ - 862MHz (TVWS)	N/A	Long range	High	TV Whitespace technology (TVWS).
Weightless-N	Proprietary	868MHz (Eu) 900MHz (US)	10b/s to 10kb/s	Up to 40km	Very low	LPWAN: Wireless technology for IoT sensor networks (alternative to costly 3G, 4G networks) developed from Weightless-W to better suit requirements of IoT.
RPMA	Proprietary	2.4GHz ISM	N/A	<30km	Very low	LPWAN technology by OnRamp Wireless.

1. Wireless technologies overview (5/5)

PAN: Personal Area Network
HAN: Home Area Network
LAN: Local Area Network
MAN: Metropolitan Area Network
WAN: Wide Area Network



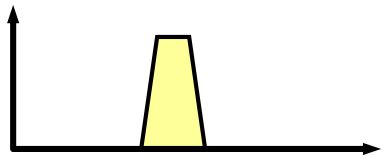
2. Radio technology

➔ **Technological drivers of radio technology:**

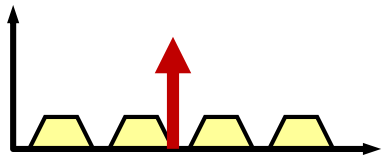
1. Hardware: Better batteries, less power consumption, processors with higher performance.
2. Link: Better / more sophisticated antennas, modulation and coding; DSPs with higher perf.
3. Network: Mobility support; dynamic resource allocation.
4. Application: Adaptive QoS (Quality of Service).
And: Radio is more and more becoming a software technology (DSP, protocols).

➔ **Reuse of spectrum through spread-spectrum:**

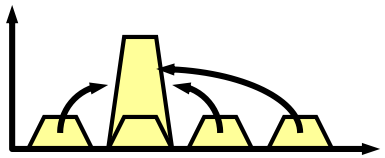
Despite the trend that newer technologies use higher frequencies, radio bandwidth remains limited.
Spread spectrum is a technology used to distribute the signal over a wide frequency range.
Spread spectrum makes the signal less susceptive to interference and noise.



Original signal



The signal is „spread“ over the frequency spectrum.
The spread signal is immune against a jamming signal.
The signal interferes less with other signals due to lower power level.



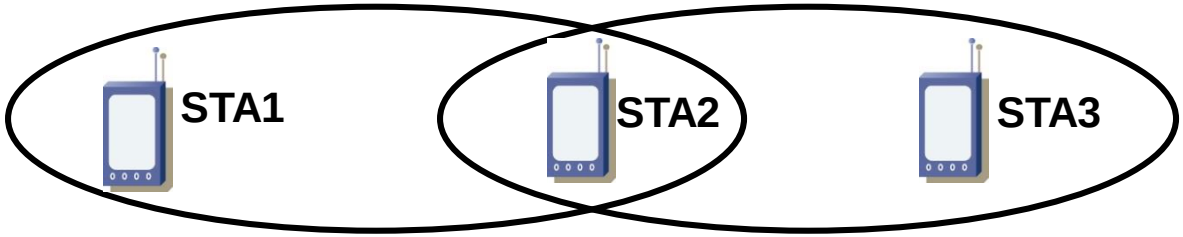
The receiver reconstructs signal.

3. Radio technology problems (1/2)

Radio networks differ from wired networks in a number of aspects. Wireless protocols on layer 1 (physical) and 2 (data link) have to be augmented with the necessary functions to address these issues.

1. Hidden station problem:

A wireless station STA3 does not „hear“ STA1 (hidden station). Both STA1 and STA3 may start sending at the same time thus causing contention at STA2.



2. Eavesdropping:

Wireless networks are inherently open to eavesdropping. This means that wireless networks need protection (strong encryption) right from the start.

3. Reliability of wireless connections:

Wireless networks suffer from interference, reflections, dropouts etc. Thus wireless connections are less reliable. New (wireless) routing protocols can be used to provide multipath routing for better reliability.

3. Radio technology problems (2/2)

4. Power consumption of wireless devices:

Wireless devices inherently suffer from a power problem (wireless = mobile = runs-on-battery). Often wireless technologies (ZigBee 802.15.4, DECT, GSM) are targeted at low power applications. Other technologies like 802.11 or WiMAX 802.16 are not particularly suited for low-power applications.

Usually a greater distance between the antennas requires more transmission power and thus increases the power consumption.

5. Limited bandwidth, need for frequency licensing:

Every country has its own frequency plan that regulates the use or licensing of radio frequencies. Obtaining a license is costly, thus the number of frequency license holders is limited.

In order to allow the use of certain frequencies without a costly and time consuming licensing process, most countries allow using the frequencies in the ISM (Industrial, Science, Medical) bands as defined by ITU-R (International Telecommunication Union – Radio).

In recent years a number of new radio technologies emerged as a consequence of advances in technology (cheaper hardware, new modulation technologies etc.).

Naturally many of these technologies (WLAN, Bluetooth, Zigbee) use the (unlicensed) ISM bands. This in turn means that interferences between different senders become a problem.

4. 802.11 WLAN Wireless LAN (1/10)

WLAN technology:

➔ 802.11 networks use free frequency bands (ISM: Industrial, Science, Medical). Thus everybody can run 802.11 devices without licensing a frequency band.

➔ Different 802.11 standards:

802.11a:	**6, 9, 12, 18, 24, 36, 48, 54 Mbps (5 GHz band).**
802.11b:	**Up to 11Mbps, simple (cheap) technology.**
802.11g:	**Up to 54Mbps.**
802.11n:	**<600Mbps (MIMO=Multiple In Multiple Out antenna technology, uses multi-path transmission for better signal recovery at the receiver).**
802.11ac:	**Forthcoming standard for higher throughput (802.11n enhancements) using 3-8 spatial streams with beam forming.**
802.11ad:	**Standard in progress by WiGig consortium, even higher throughput (<7Gpbs). 802.11ad is targeted at bridging short distances with wireless links, e.g. in data centers (5-10m).**

➔ 802.11 Pros and Cons:

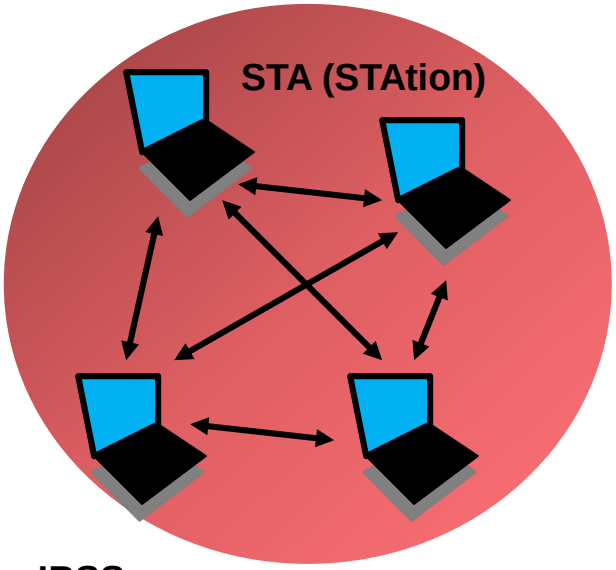
- 🙂 **Mobility**
- 🙂 **Flexible configuration**
- 🙂 **Relatively cheap**
- ☹ **Weak security (WEP Wired Equivalent Protection, but fixed with WPA Wired Protection Access)**
- ☹ **Relatively low bandwidth for data (compared to wired networks)**
- ☹ **Electromagnetic interference with other devices (Bluetooth)**
- ☹ **Simple installation, but high skills needed for exploitation of full potential of technology**

4. 802.11 WLAN Wireless LAN (2/10)

Operation modes of 802.11:

Ad-hoc mode:

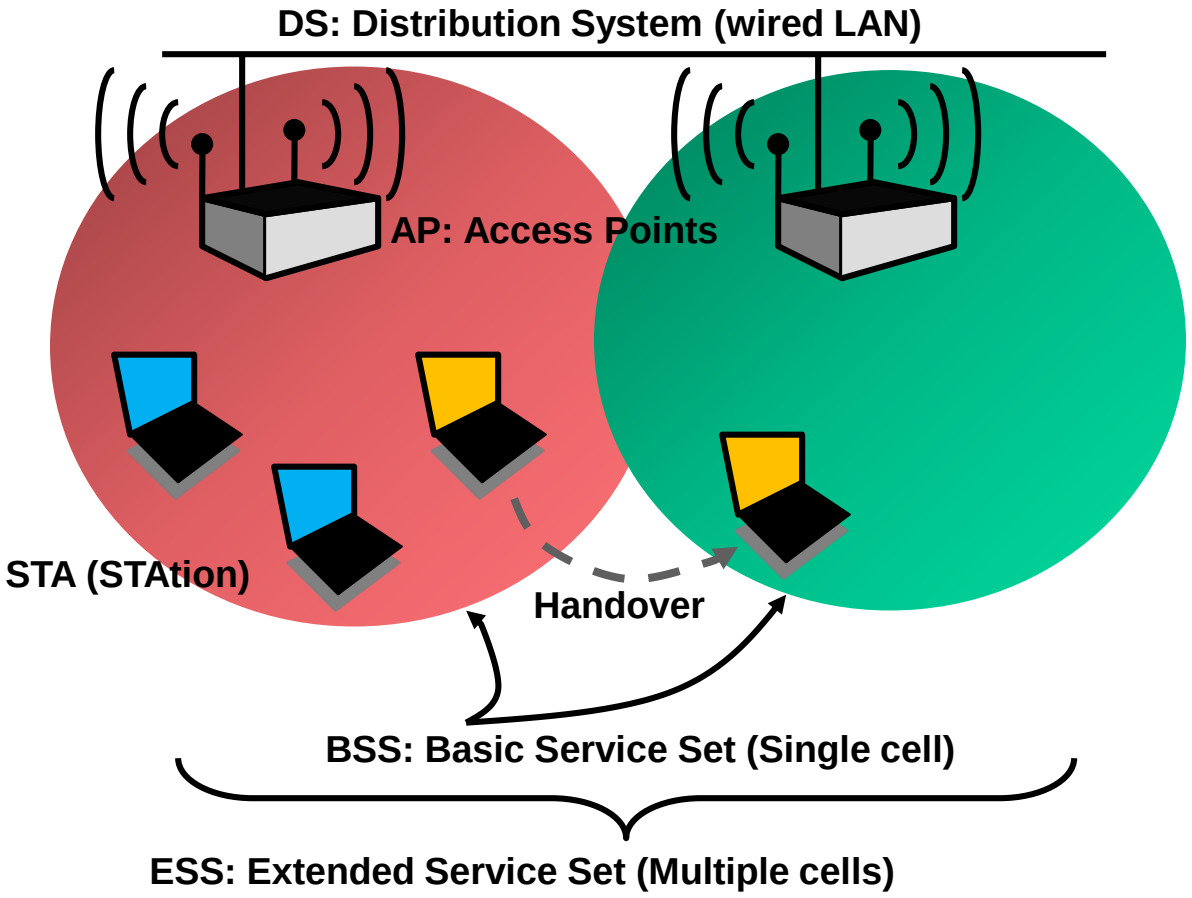
No access points; STAs communicate directly with each other.



IBSS:
Independent Basic Service Set

Infrastructure mode:

Usage of access points interconnected with wired LAN.



4. 802.11 WLAN Wireless LAN (3/10)

802.11 protocol stack:

802.11 Physical layer:

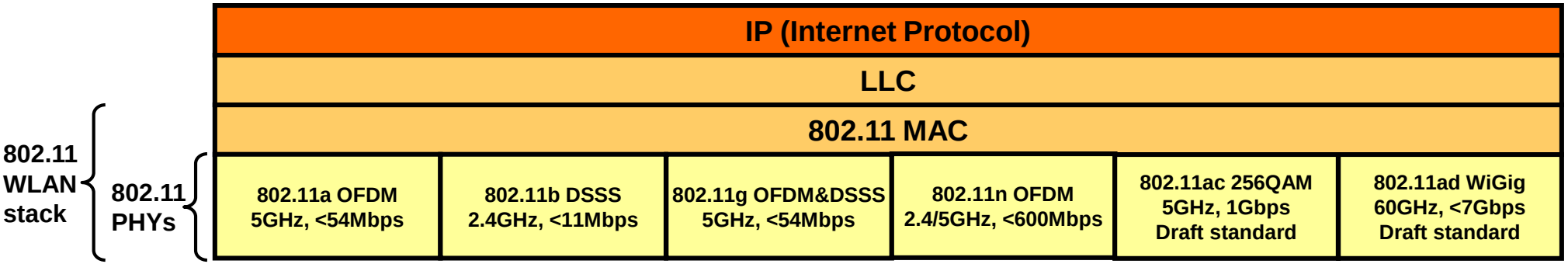
The physical layer is concerned with modulation / demodulation. The different WLAN standards use different modulation techniques (OFDM, DSSS, QAM).

802.11 MAC:

The MAC layer controls the media access (see below).

LLC:

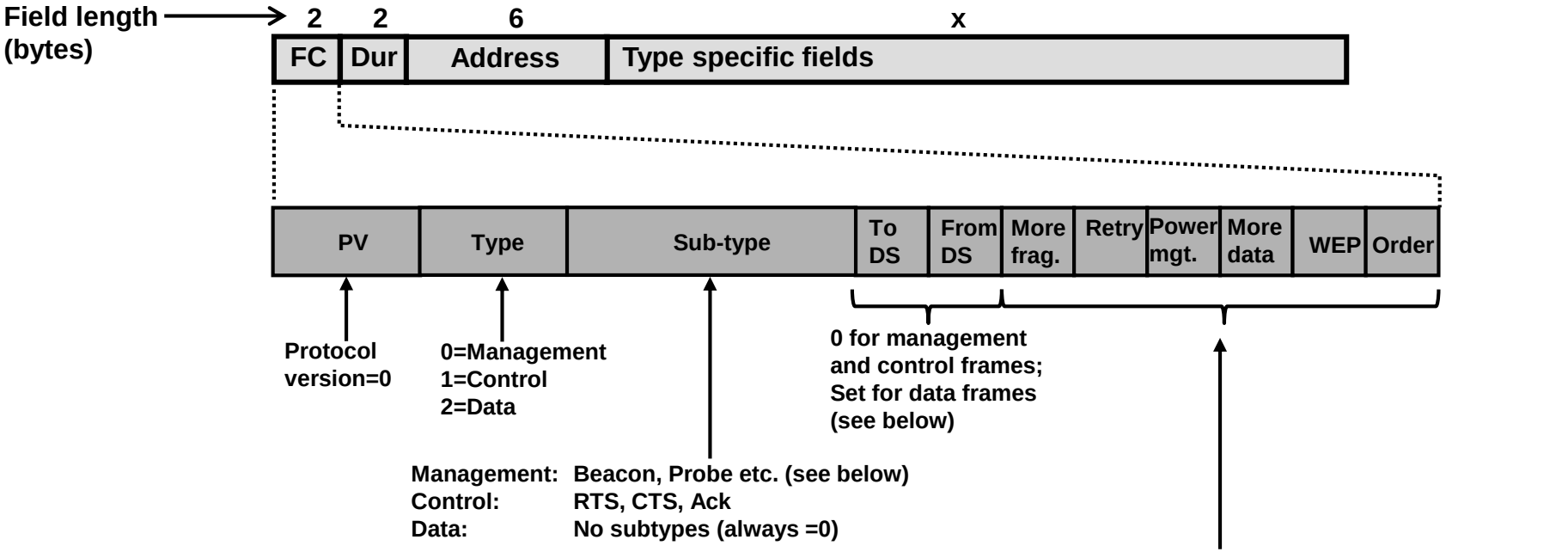
LLC (Logical Link Control) is not part of the WLAN stack, but is often used to provide a generic access layer to the lower (link) layers.



4. 802.11 WLAN Wireless LAN (4/10)

802.11 frame structure:

The 802.11 frame structure depends on the frame type (see below).
The general 802.11 frame structure looks as follows:



Dur: Time in microseconds that the sender needs for sending the frame.
Address: Receiver's MAC address
DS: Distribution System
(wired or wireless „backbone" of WLAN)
FC: Frame Control

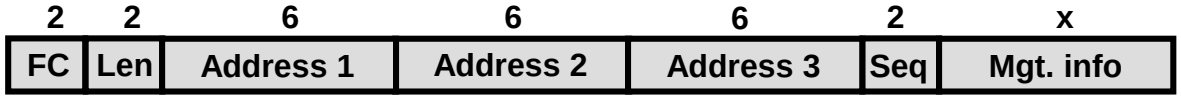
4. 802.11 WLAN Wireless LAN (5/10)

802.11 frame types (1/3):

1. Management frame:

Management frames are used to establish and maintain communication.

Management frame structure:



Management frame suptypes:

The management frames are basically used for associating a STA to an AP (procedure see below).

a. Authentication frame:	Basic authentication, e.g. based on MAC-address.
b. Deauthentication frame	STA sends deathentication frame to terminate communication.
c. Association request frame	STA requests AP to allocate resources for communication.
d. Association response frame	Response of an AP to an association request.
e. Reassociation request frame	Sent by STA when it roams to another AP.
f. Reassociation response frame	Response from the new AP to the reassociation request.
g. Disassociation frame	STA requests disassociation from AP.
h. Beacon frame	AP periodically sends beacon frames with its identity.
i. Probe request frame	When the STA is not associated to an AP, it sends probe request frames.
j. Probe response frame	Reponse from an AP to a probe request frame.

4. 802.11 WLAN Wireless LAN (6/10)

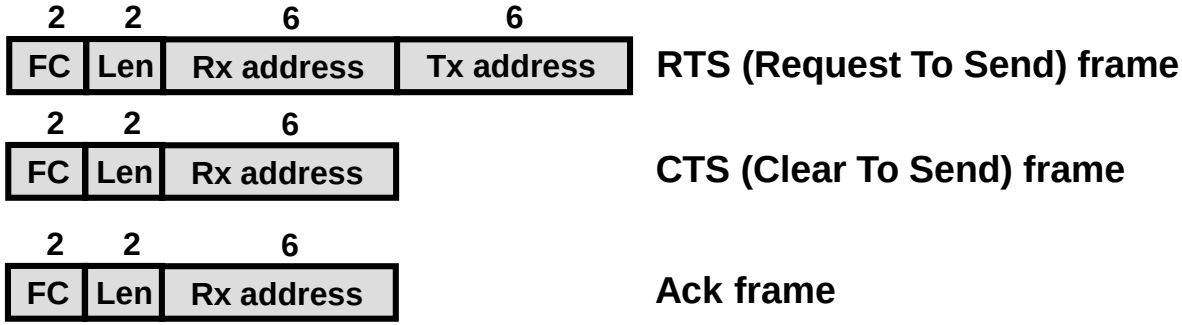
802.11 frame types (2/3):

2. Control frame:

Control frames are optional and are used for assisting in the delivery of data frames between stations.

Control frames are used in a handshake procedure in the CSMA/CA protocol (see below).

Control frame structure:



Rx: Receiver
Tx: Transmitter

4. 802.11 WLAN Wireless LAN (7/10)

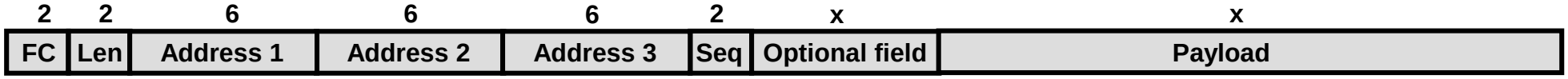
802.11 frame types (3/3):

3. Data frame:

Data frames carry user data. Data frames are acknowledged and retransmitted if they are lost.

Data frame structure:

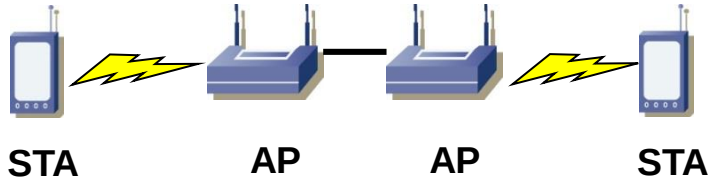
WEP parameters (4 bytes) if data is WEP-protected.
Address 4 (6 bytes) if frame is an AP→AP frame.



Data frame addresses and DS bits:

Since data frames may be transported between APs over a wired distribution system, 2 additional MAC addresses are required in the WLAN frame header.
The DS bits indicate the meaning of the different addresses fields as follows:
Destination = MAC address of final destination node.
Source = MAC address of original sending node.
Sender & receiver: Sending and receiving AP's MAC addresses.

	To DS	From DS	Addr. 1	Addr. 2	Addr. 3	Addr. 4
Client to Client	0	0	Dest.	Source	BSSID	N/A
AP to Client	0	1	Dest.	BSSID	Source	N/A
Client to AP	1	0	BSSID	Source	Dest.	N/A
AP to AP	1	1	Receiver	Sender	Dest.	Source



4. 802.11 WLAN Wireless LAN (8/10)

802.11 MAC (Media Access Control) differs from 802.3 (Ethernet) MAC:

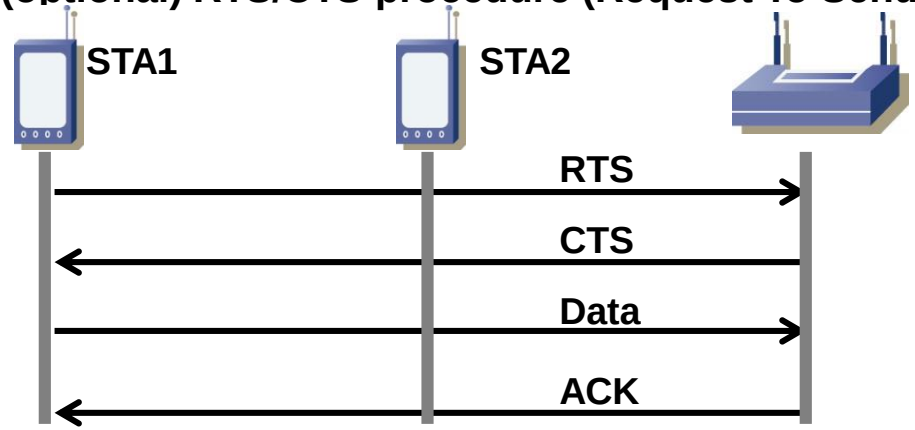
802.3 Ethernet MAC uses CSMA/CD *Collision Detection*:

1. Before sending check if the line is free (nobody else is sending).
2. If the line is free send the data. At the same time monitor the own data on the line. If the data is scrambled, there is a collision (another device is sending at the same time).
3. In case of a collision wait some time (backoff time) and restart at 1.

802.11 WLAN MAC uses CSMA/CA *Collision Avoidance*:

Collisions are costly and difficult to detect in radio networks, thus 802.11 tries to avoid them.

1. Before sending check if the air is free (nobody else is sending).
2. If the air is free send the data. Unlike in wired Ethernet, the monitoring of the own data is useless since the power level of the sender itself is much higher than the power level of another sender. In addition a sender can not detect collisions at the receiver due to the "hidden station" problem.
3. Optionally the sender can reserve the air medium for the transmission of a frame with the (optional) RTS/CTS procedure (Request To Send / Clear To Send) as follows:

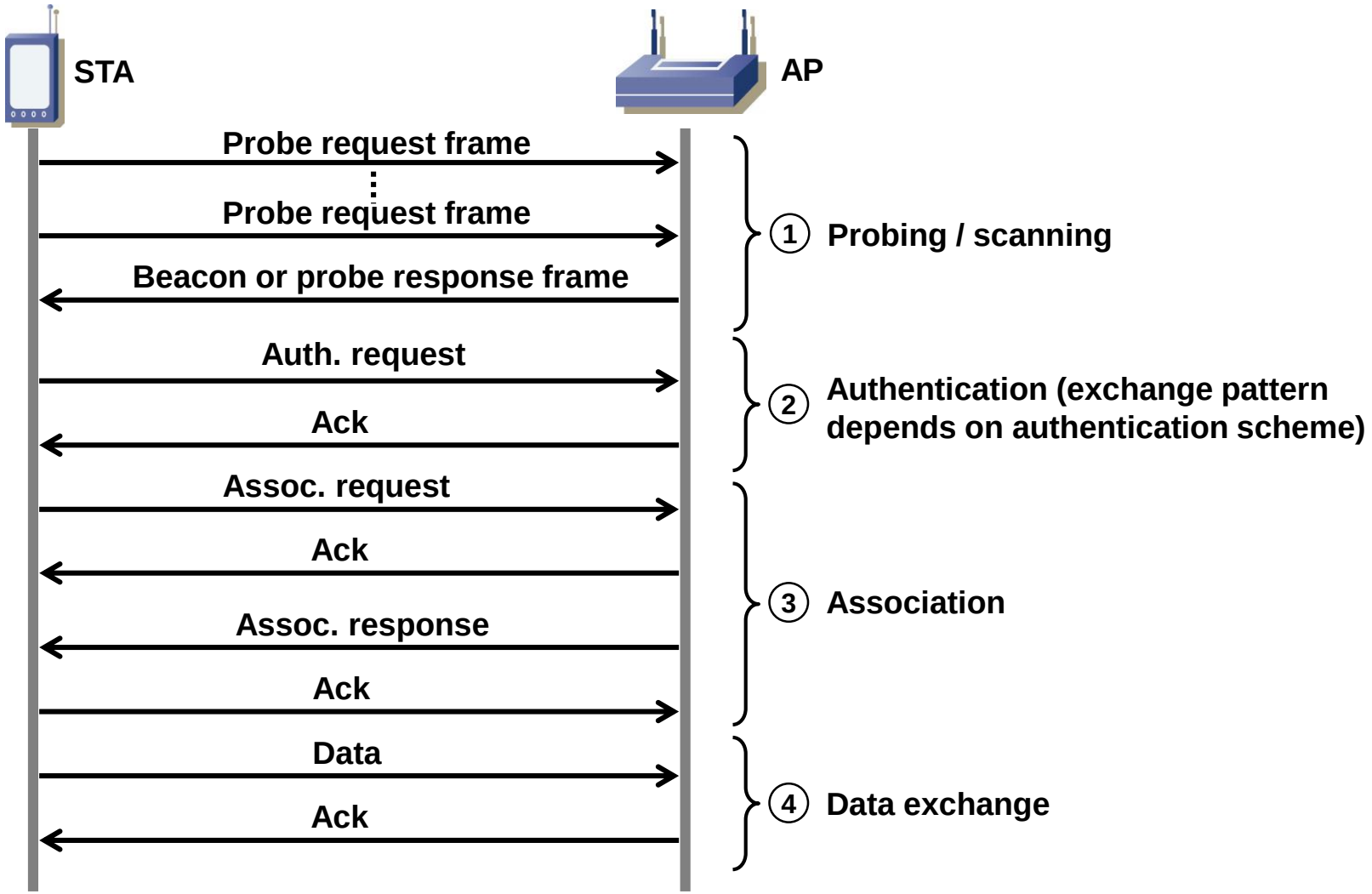


The CTS/RTS procedure is usually only used for small frames.
STA1 requests air interface by sending an RTS frame containing the amount of data to be sent (time interval).
STA2 „hears" RTS and refrains from sending any frames during requested time interval.
AP grants air interface with CTS frame.
STA1 sends data.
AP sends ACK to finish transaction.

4. 802.11 WLAN Wireless LAN (9/10)

802.11 registration with an access point (1/2):

Unlike Ethernet, WLAN stations register with an access point.



4. 802.11 WLAN Wireless LAN (10/10)

802.11 registration with access point (2/2):

1. Probing / scanning:

The STA attempts to find an AP through:

- **a. (Optional) active scanning (probe request frames) or**
- **b. Passive scanning (client waits for AP's beacon frames sent in regular intervals).**

The user then selects to which AP to associate based on the SSID (beacon contains the SSID).

2. Authentication:

STA authenticates with AP.

Possible authentication schemes:

- **a. Open (no authentication).**
- **b. PSK (Pre-Shared Key) with WEP (deprecated).**
- **c. 802.1X EAPOL (EAP Over LAN) used with WPA / WPA2.**

3. Association:

STA enters the service set serviced by the AP. STA informs AP of its supported data rates.
AP allocates buffers and other data structures for the communication with the STA.

4. Send / receive data:

STA starts sending and receiving data (direct or with RTS/CTS mechanism).
N.B.: All frames are acknowledged with WLAN. Lost frames are retransmitted.

5. Public mobile networks (1/4)

Evolution of mobile networks and technologies:

AMPS Analog Mobile Phone Service (e.g. "Natel A – C" in Switzerland).
1G technology: 1st generation mobile cellular networks.

GSM Global System for Mobile Telecommunication.
2G technology: 2nd generation (digital cellular networks).

GPRS Generalized Packet Radio Service, packet service for GSM (2G) networks.
2.5G technology: addition to GSM service.

EDGE Enhanced Data Rates for GSM Evolution; enhancement (data rates) of GPRS service (mainly software based, can be deployed in existing GPRS networks with software upgrades).
2.75G technology: Sometimes also seen as a 3G technology. EDGE is actually a step between GPRS and UMTS.

UMTS Universal Mobile Telecommunication System.
3G technology: Incompatible with 2G and thus requires new network infrastructure. Does the same as GSM so adoption rate is slow (but picking up lately).

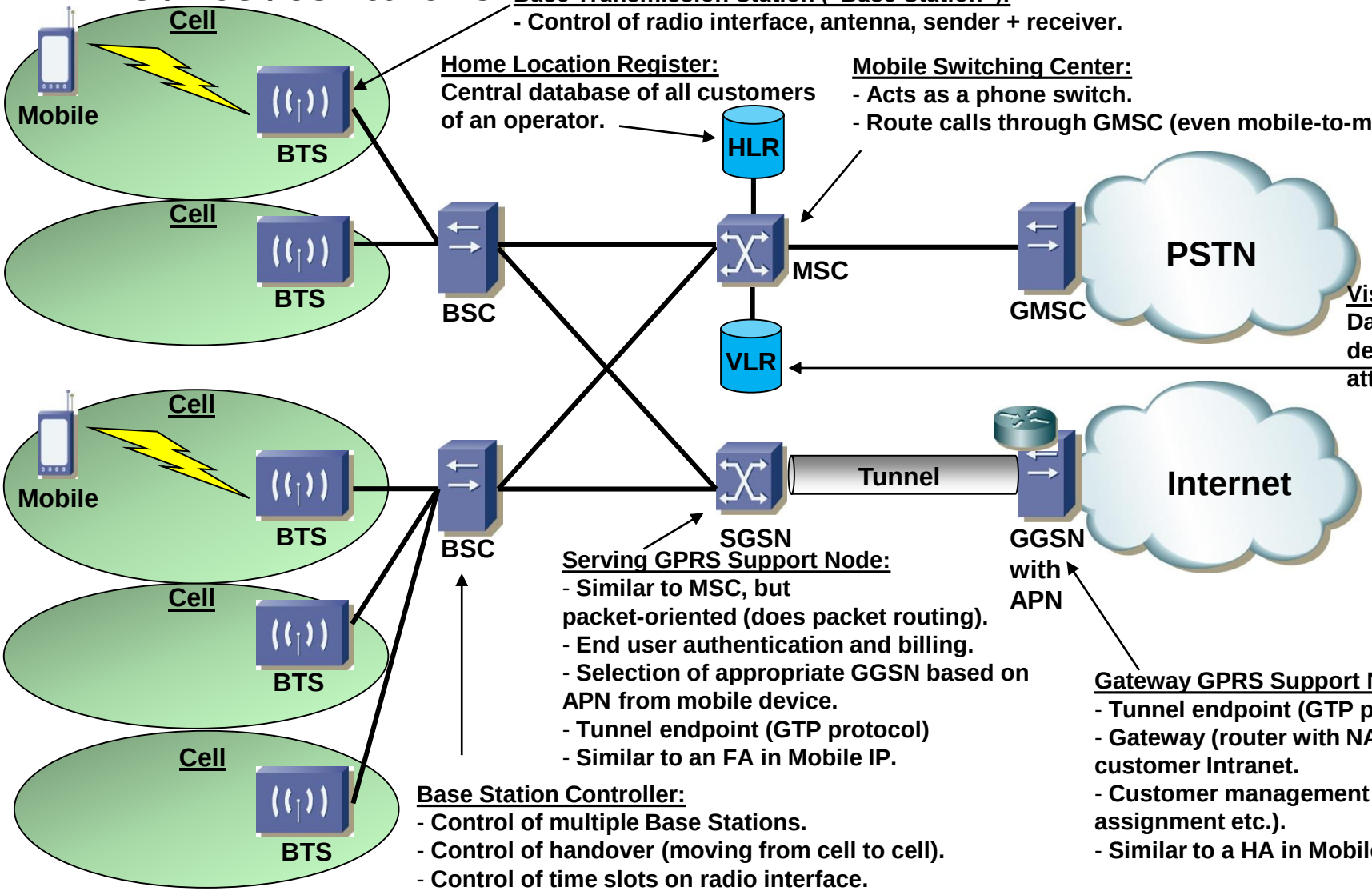
HSDPA High Speed Downlink Packet Access.
3.5G technology: Enhancement of UMTS for higher speeds in Network-to-mobile direction. Mainly a software based improvement over plain UMTS.

HSUPA High Speed Uplink Packet Access.
3.75G technology: Further enhancement (higher speeds in mobile-to-network direction) of UMTS and HSDPA service.

LTE Long Term Evolution.
4G technology, UMTS successor, competitor to WiMAX.
All services are IP-based (no TDM-based voice service anymore).

5. Public mobile networks (2/4)

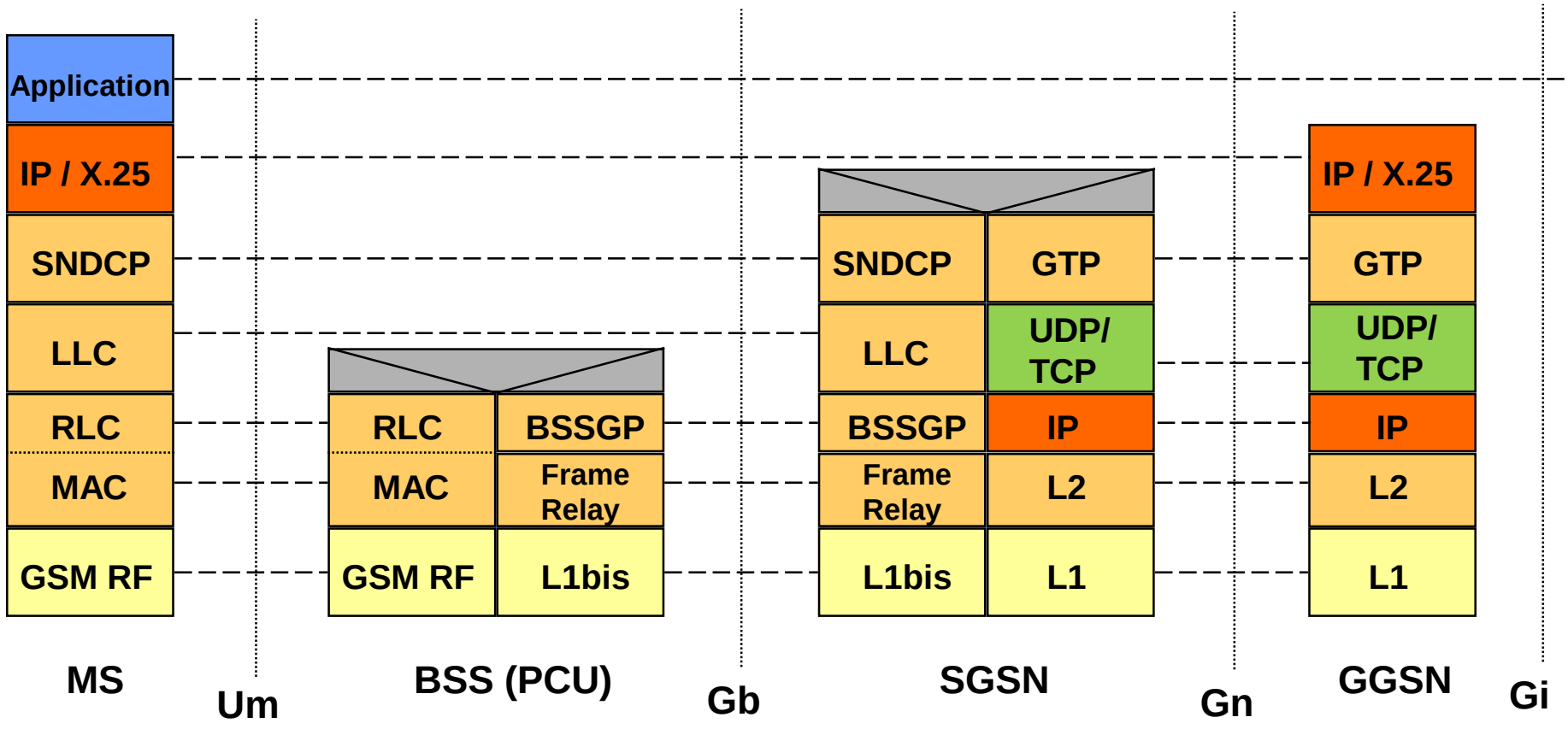
➔ 2G / 2.5G / 3G networks:



5. Public mobile networks (3/4)

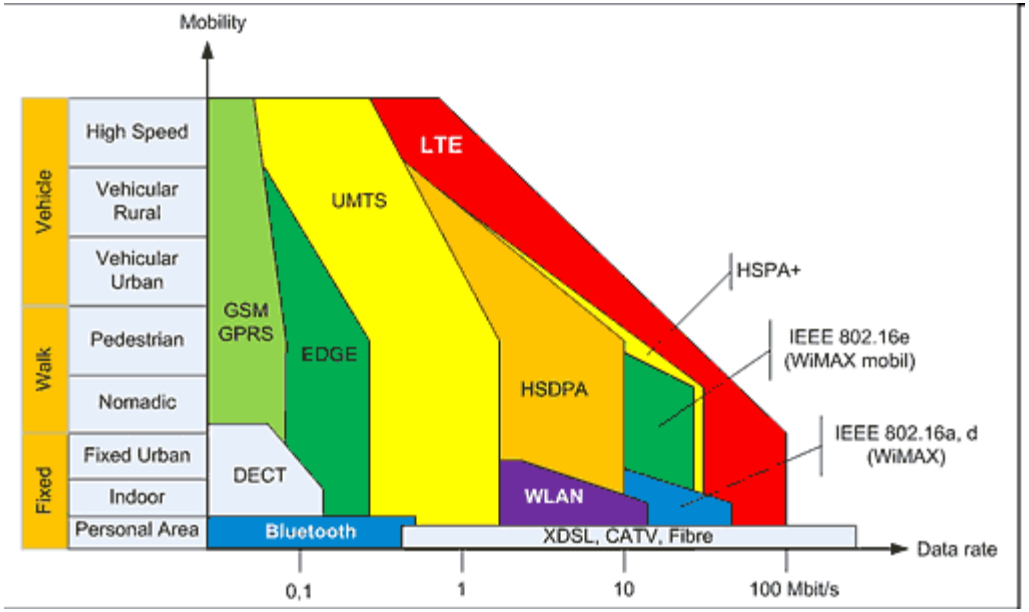
➔ GSM protocol stacks:

The data service (TCP/IP) on GSM networks requires a rather complex protocol stack to achieve transparent mobility (handover between radio cells).
LTE may use a different approach based on PMIPv6 (Proxy Mobile IPv6, RFC5213).



5. Public mobile networks (4/4)

LTE (Long Term Evolution) is the 4th generation of mobile networks to replace G3 networks. LTE provides far greater bandwidths, even for moving mobile devices:



Source: http://www.bakom.admin.ch/dokumentation/Newsletter/01315/02251/02261/index.html?lang=de

LTE features:
- **High bandwidths (< 100Mbps)**
- **Low latency (5ms)**
- **Mobility support (< 500km/h, see above)**
- **High spectral efficiency (3-4 times that of UMTS / HSPA)**

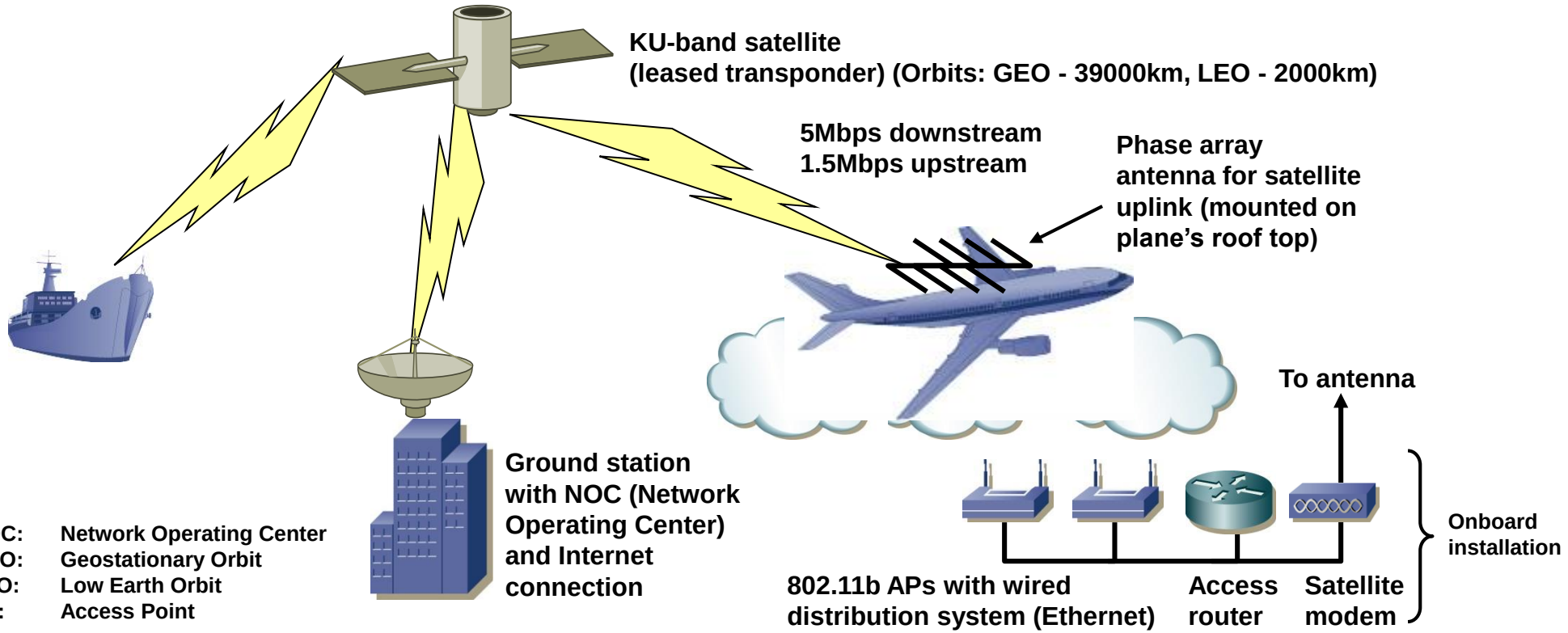
N.B.: First release of LTE is "only" 3.9G as it does not fully meet the 4G criteria (all IP). First version of LTE still supports TDM services.

6. Satellite Internet Access

➔ Satellite Internet access is relatively cheap to deploy in areas where wired Internet access is difficult or impossible (remote areas).

➔ Satellite access is also possible for moving hosts, e.g. Panasonic exConnect for Internet access & GSM phone service aboard long-haul flights.

➔ A satellite system is usually optimized for one-way transmission (TV, radio). Downlink bandwidth is much cheaper than uplink bandwidth.



7. Wireless mobility

➔ **Mobility not only means obtaining an IP address dynamically (PPP, DHCP). Mobility means that a mobile host is always reachable irrespective of its current location (location transparency).**

➔ **Mobility (location transparency) can be implemented at:**

1. Datat link layer (L2):

Examples: IEEE 802.11r Fast Roaming (not widely used) or GSM/CDMA.
Allows to roam between access points (handover).

- ☺ **No changes to clients (mobile nodes) needed.**
- ☹ **Works only for and within specific wireless technologies.**

2. Application layer (L5-L7):

Examples: SIP registrations, DNS/dynDNS.

- ☺ **No changes to clients (mobile nodes) needed.**
- ☹ **Disruptive (an open connection will be dropped), thus only suited for quasi-static attachment to network using PPP, DHCP or PPPoE for obtaining IP address, e.g. once a day).**

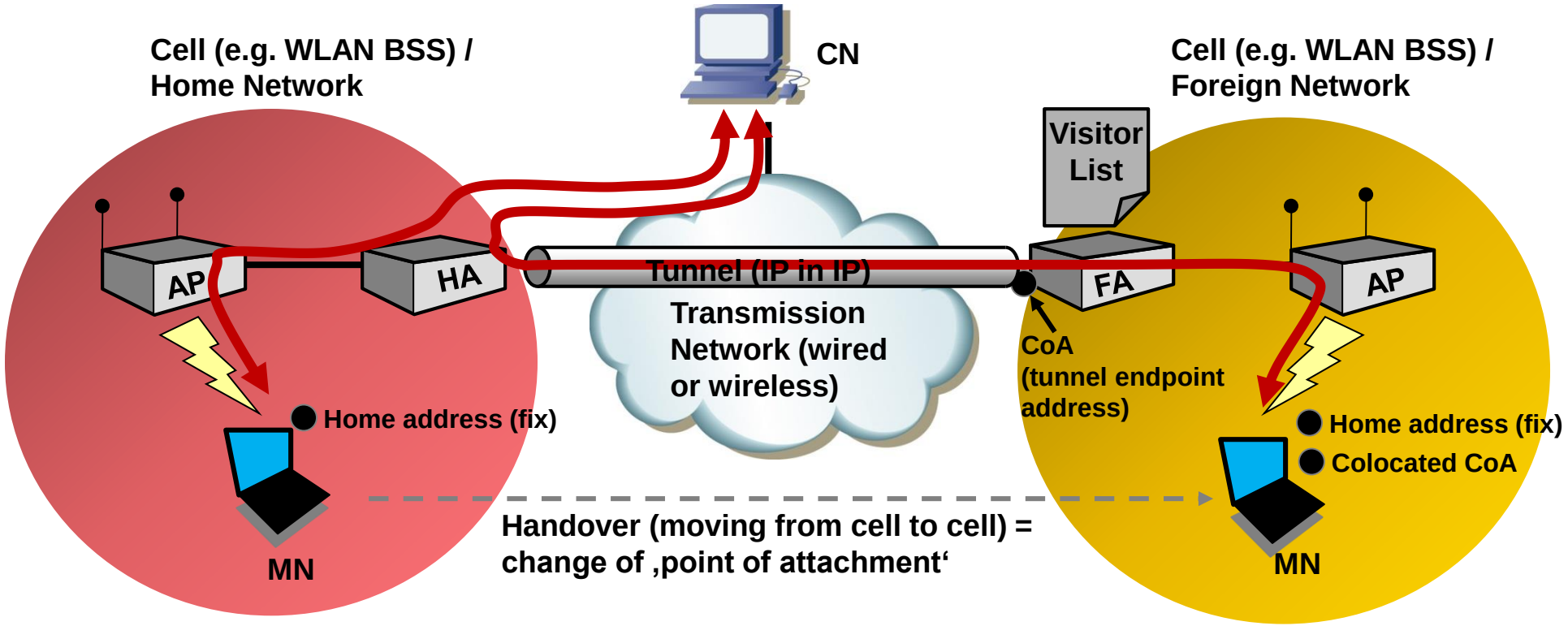
3. Network layer (L3):

Examples: Mobile IP MIP RFC2002 (see below), Proxy MIP RFC5213.

- ☺ **Transparent to transport protocols; thus applications are unaware of changes of network attachment (handover).**
- ☺ **Works for different wireless technologies.**
- ☹ **Changes in OS for mobile nodes required.**

8. Mobile IP RFC2002 (1/5)

➔ Mobile IP model:



➔ HA acts as an ‚anchor point‘
➔ MN has always a relationship to HA (is registered with HA).
➔ FA acts as tunnel endpoint.
➔ N.B.: Mobile IP is not specifically restricted to wireless networks.

MN: Mobile Node
HA: Home Agent
FA: Foreign Agent
CoA: Care of address (c/o)
BSS: Basic Service Set (radio cell)
CN: Correspondent Node (is either Mobile or stationary)

8. Mobile IP RFC2002 (2/5)

➔ **MIP components:**

1. Home Agent HA:

An MN registers with its Home Agent and informs it about its CoA. A HA is a special process running on a router.

2. Foreign Agent FA:

Establishes a tunnel with HA and forwards packets to/from MN from/to tunnel. An FA is a special process running on a router.

3. Correspondent Node CA:

Communication partner for MN; a CA needn‘t have any knowledge about Mobile IP; CA is either a mobile itself or stationary.

4. Mobile Node MN:

Any wireless appliance (handy, PDA, laptop, server aboard an airplane etc.).

➔ **MIP objectives:**

Mobile IP (RFC2002) aims at making the location of machines transparent to applications. If a user moves around the application communication should not be disrupted (TCP connections remain open even though MN obtains new IP address = ‚session continuity‘). Since a TCP connection is defined by the quadruplet {src IP, src port, dst IP, dst port} it is required that the MN retain its IP address when roaming (point of attachment changes). This in turn means that IP tunneling must be used. In a way mobile IP is similar to GSM where a user moves (roams) but can always be called from another phone, irrespective of his current location (handover/roaming even works during a call!).

8. Mobile IP RFC2002 (3/5)

➔ How Mobile IP works:

1. MN Address:
MN has fixed *Home Address* that never changes. A roaming MN is identified/addressed through this *Home Address*.

2. MIP Agent Discovery:
During agent discovery MN finds HA or FA. MIP uses extensions to RFC1256 Router Advertisments. HA and FA advertise their capability to act as HA/FA through broadcasts at regular intervals (*agent advertisments* every few seconds containing a list of CoAs, also called beacons).
If NN does not want to wait for router advertisment it can request a CoA through broad- or multicast (*agent solicitation*).

3. MIP Registration:
MN registers CoA (endpoint address of tunnel that will be initiated by HA) with HA when it changes point of attachment (roams).

4. HA routing:
HA adjusts its routing table to deliver (tunnel) packets destined to MN to make the connections to the MN transparent for applications.
4. Packets from MN to CN are either directly delivered (triangular routing) or the FA routes them back through the tunnel (‘reverse tunneling’).

8. Mobile IP RFC2002 (4/5)

Colocated CoA versus CoA:
The FA either resides on the MN itself (colocated CoA) or on a dedicated device (shared CoA).

1. Colocated CoA:
Mobile Node obtaines IP address through some external means (DHCP, PPP) and uses it as tunnel endpoint address. The MN itself terminates the tunnel, decapsulates the tunnel packets (removes outer header) and delivers (routes, forwards) the packet to the application.

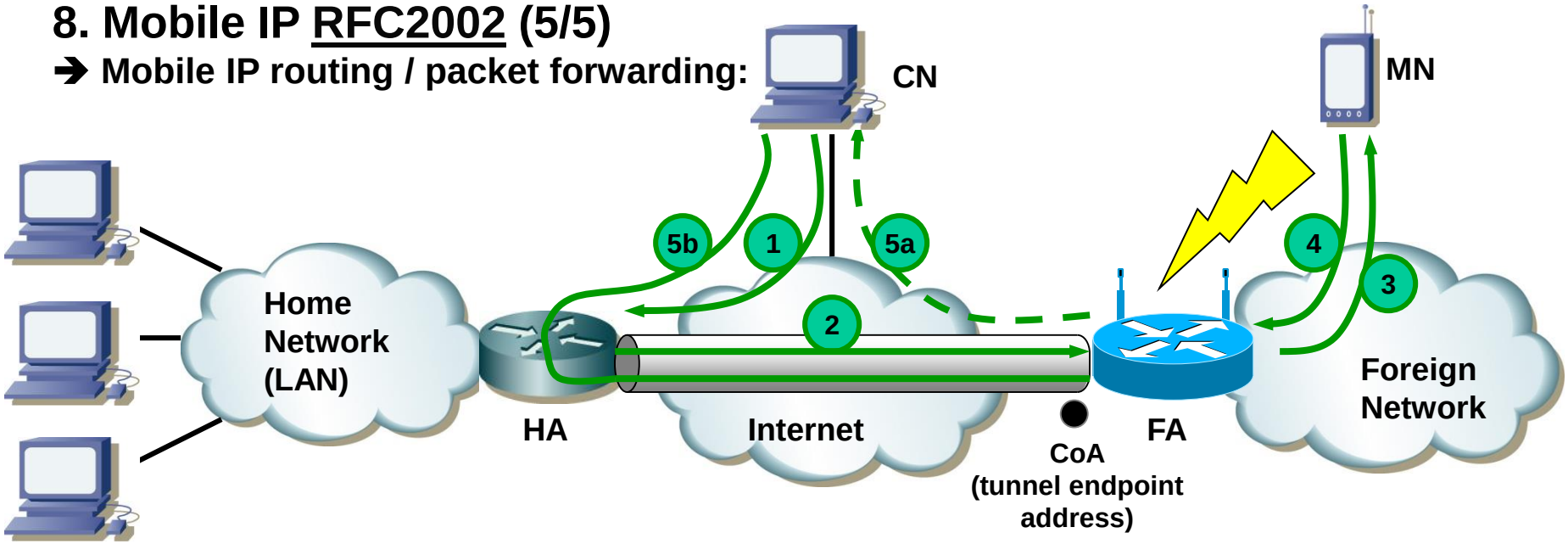
- ☺ **No foreign agent required.**
- ☹ **Multiple IP‘s required to support multiple mobile nodes**

2. Shared CoA:
All MN‘s in a foreign network have the same CoA address. The CoA is simply the IP address of the FA. The FA termates the tunnel, decapsulates the tunnel packets (removes outer header) and delivers the packet to the according MN.

- ☺ **1 IP address for multiple nodes**
- ☹ **FA required**

8. Mobile IP RFC2002 (5/5)

➔ Mobile IP routing / packet forwarding:



1 CN sends packet to MNs home address. HA performs proxy ARP to deliver L2 address on behalf of (absent) MN. When MN leaves home network the HA sends gratuitous ARPs (with HA's link layer address in order to update the ARP caches of hosts in the home network).

2 HA finds out that MN is not on home network but reachable through tunnel (routing entry) and sends packet to CoA (tunnel endpoint address of FA).

3 FA delivers the packet to the MN.

4 MN sends the reply back to the FA.

5a FA sends packet directly to CN (=„triangular routing"); the problem with this approach is that the reply packet does not take a topologically correct route (packet with IP-source=MN-home address comes from FA). Firewalls / packet filters along the way with ingress filtering thus may drop the packet.

5b Instead of directly routing the packet back to the CN the FA routes the packet back to the HA through the tunnel (=reverse tunneling).

➔ N.B.: MN's home address may be private and thus not unique in the foreign network. Thus FA's routing entries must consist of a combination of link layer address (MAC), tunnel identification and MN-IP-address.