Ch. 6: Wireless and Mobile Networks

Background:

- Number of wireless (mobile) phone subscribers now exceeds number of wired phone subscribers (5-to-1 or more)!
- Number of wireless Internet-connected devices equals number of wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

Chapter 7 outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

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

67.4 Cellular Internet Access
- architecture
- standards (e.g., 3G, LTE)

Mobility

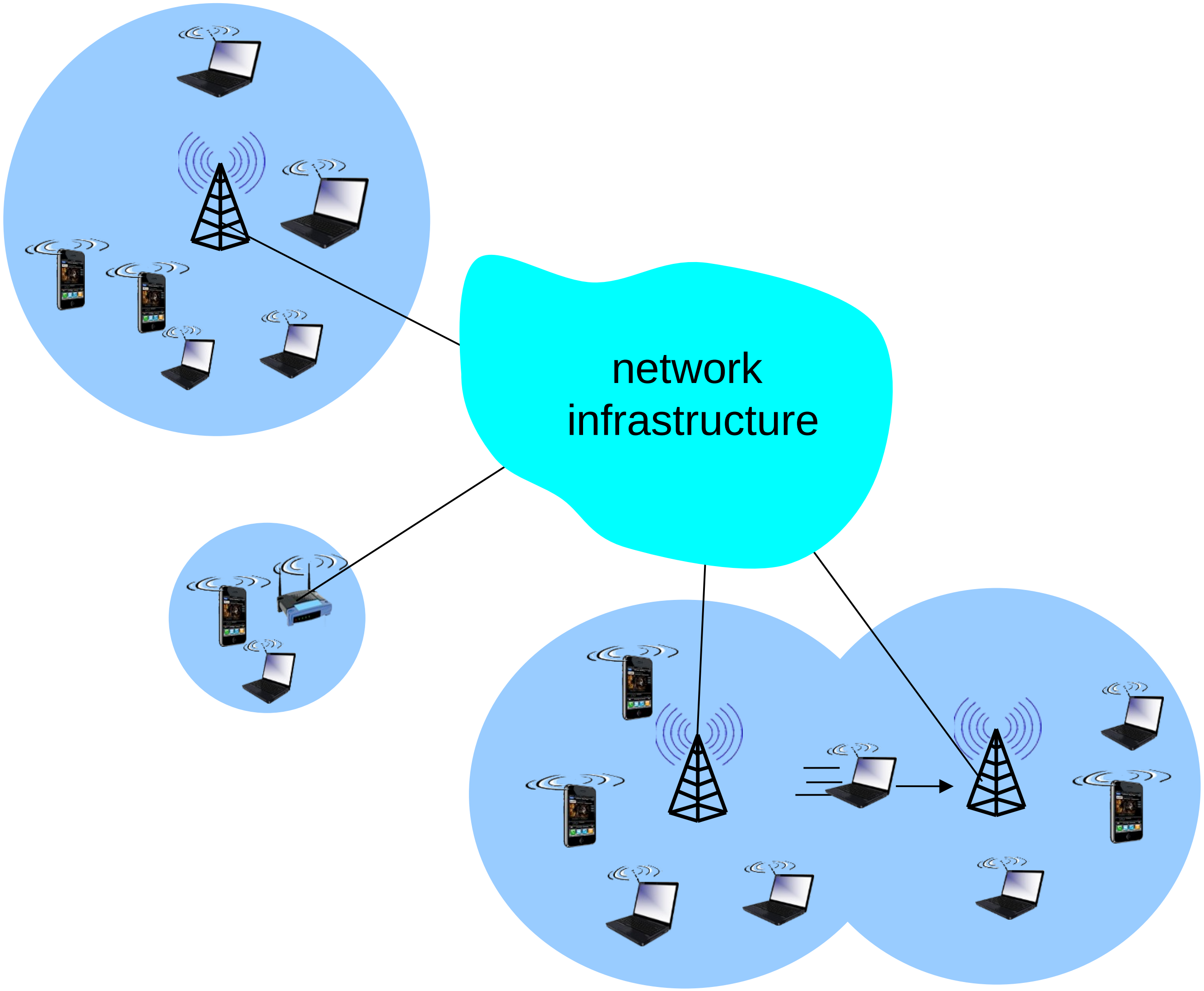
7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

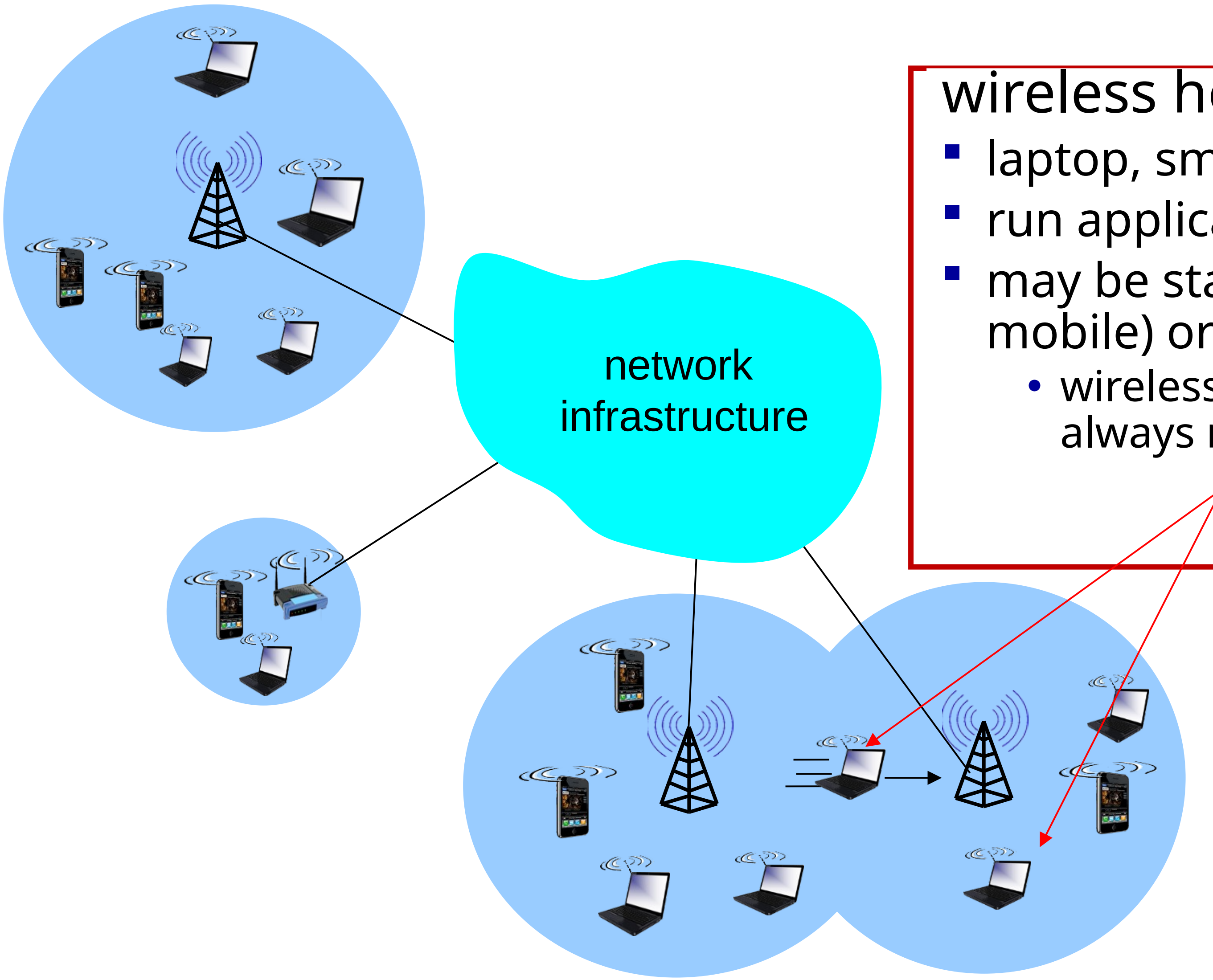
7.7 Handling mobility in cellular networks

7.8 Mobility and higher-layer protocols

Elements of a wireless network



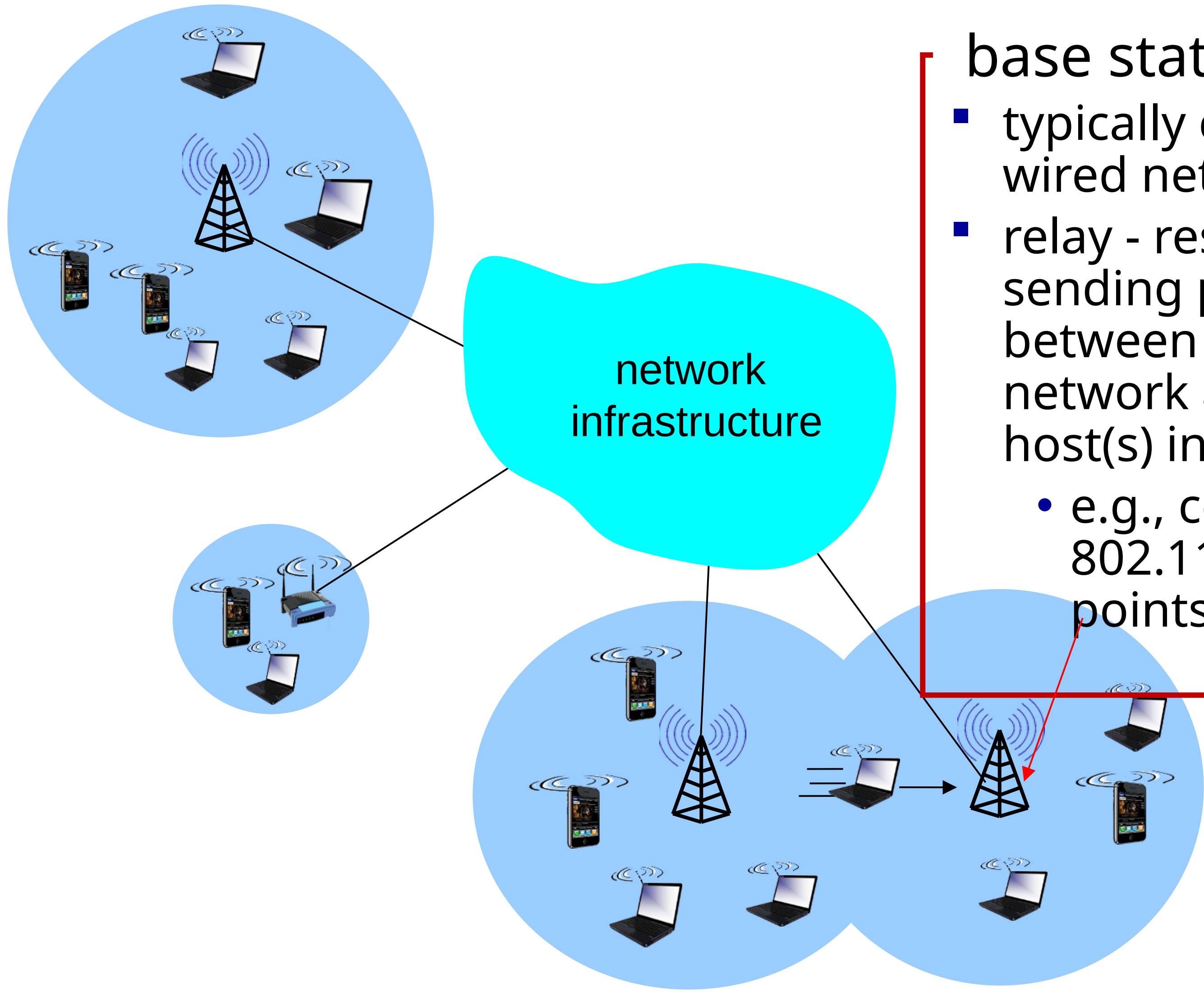
Elements of a wireless network



wireless hosts

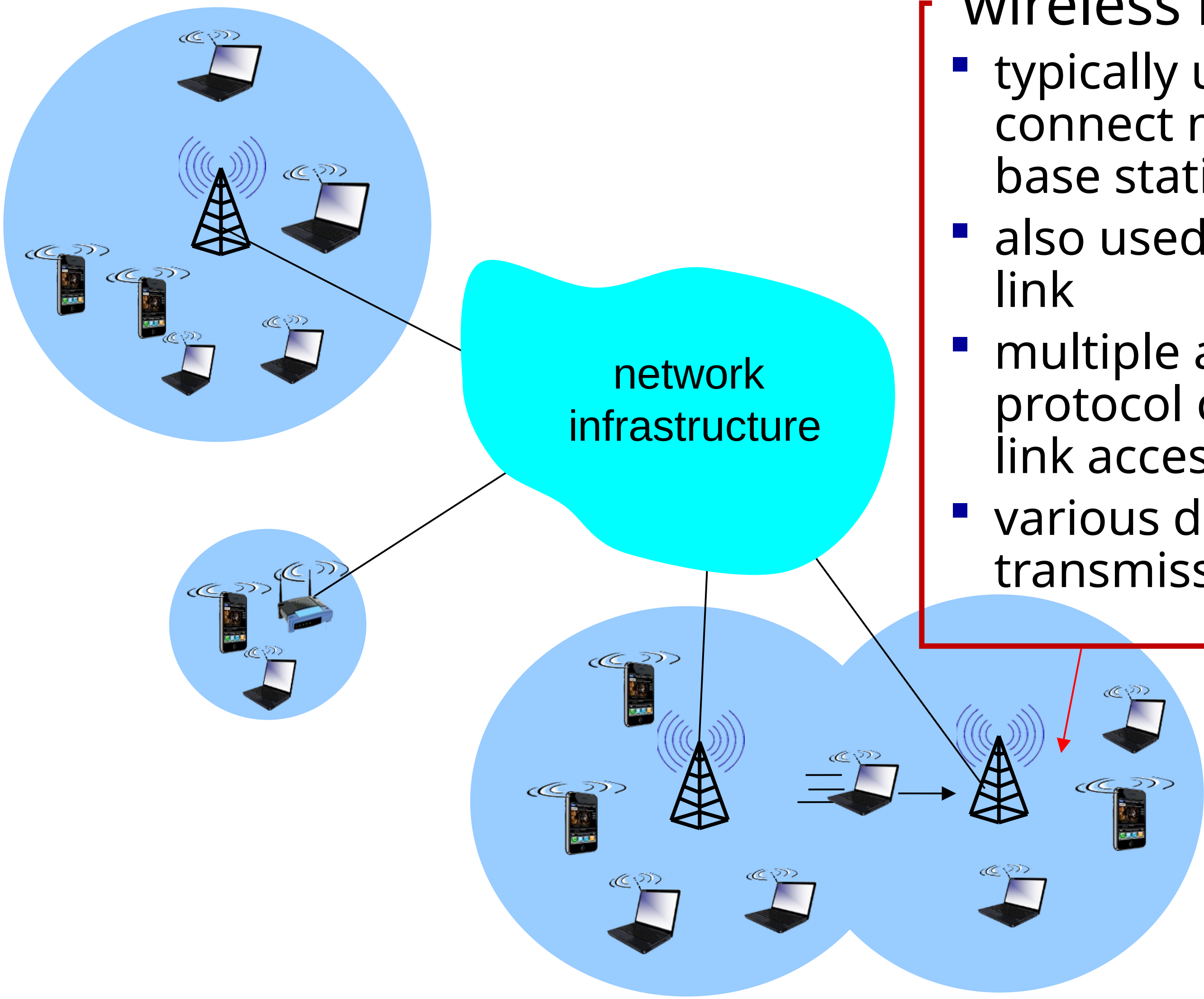
- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Elements of a wireless network



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

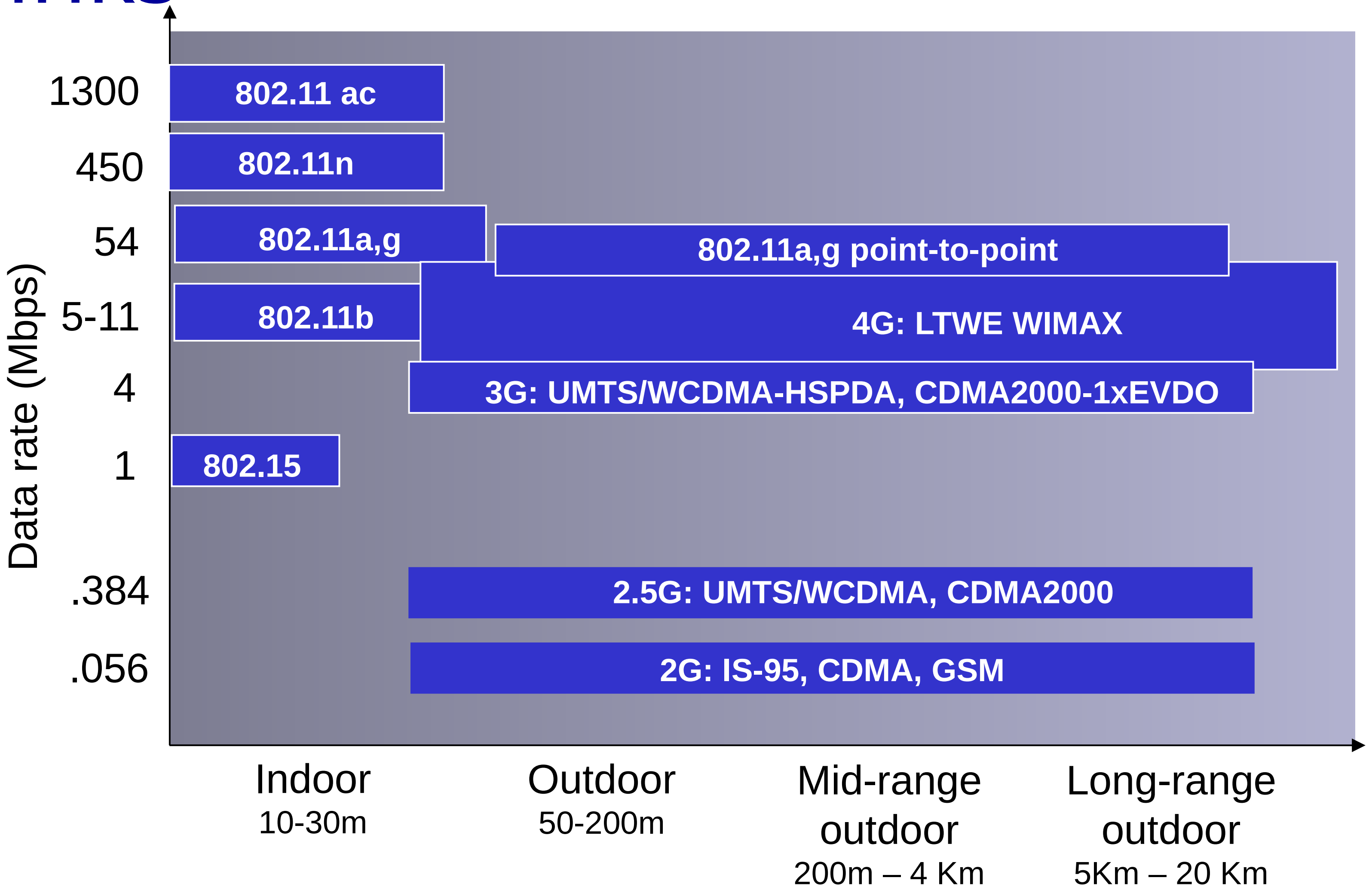
Elements of a wireless network



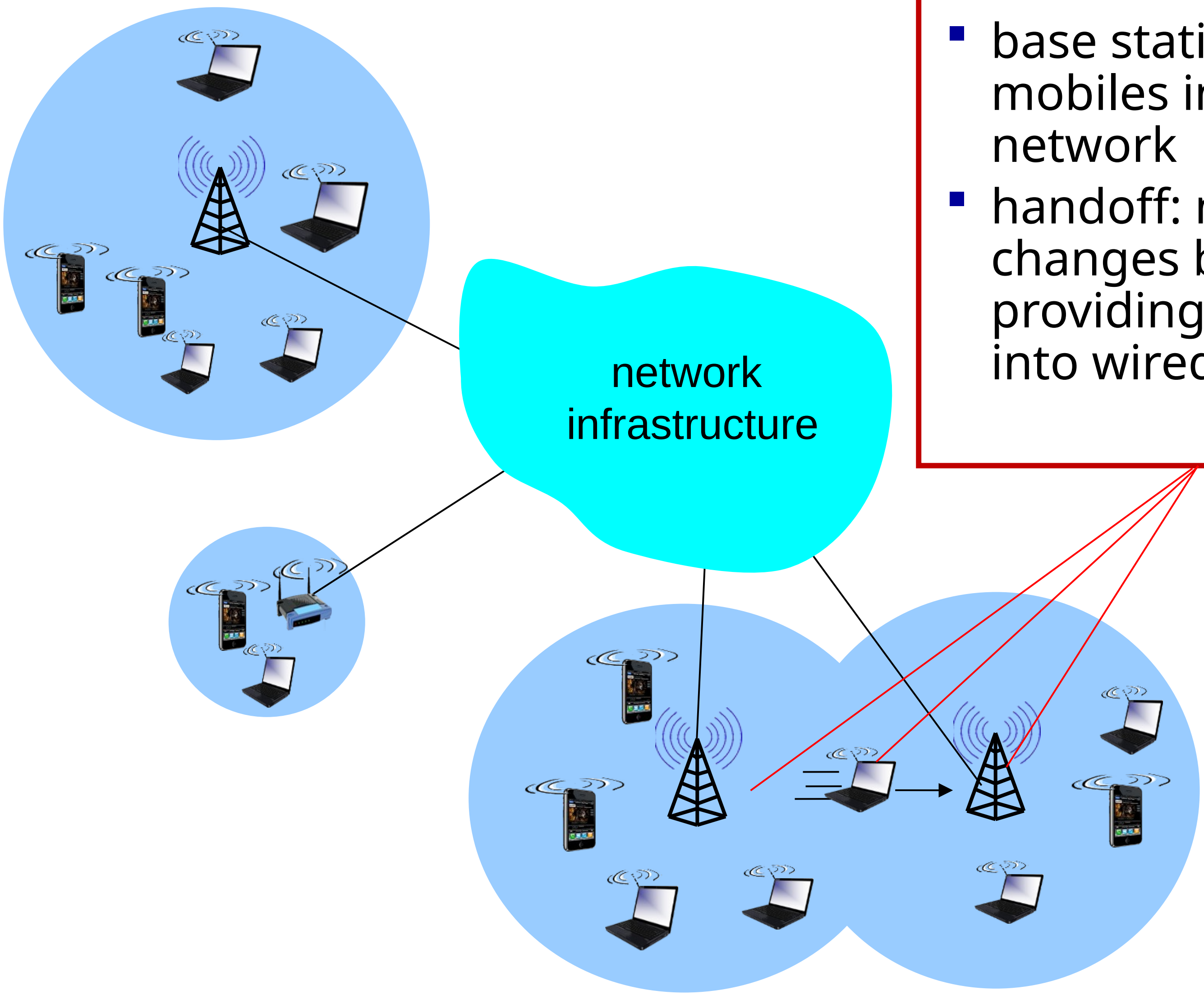
wireless link

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

Characteristics of selected wireless links



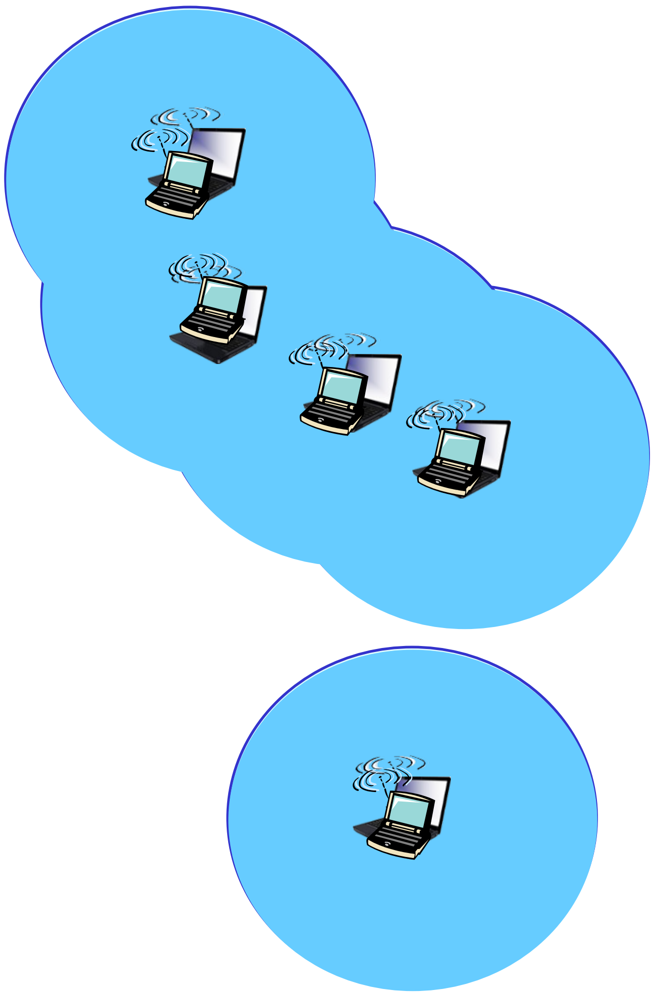
Elements of a wireless network



infrastructure mode

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

Elements of a wireless network



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

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	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 other a given wireless node MANET, VANET

Chapter 7 outline

Wireless Link Characteristics (1)

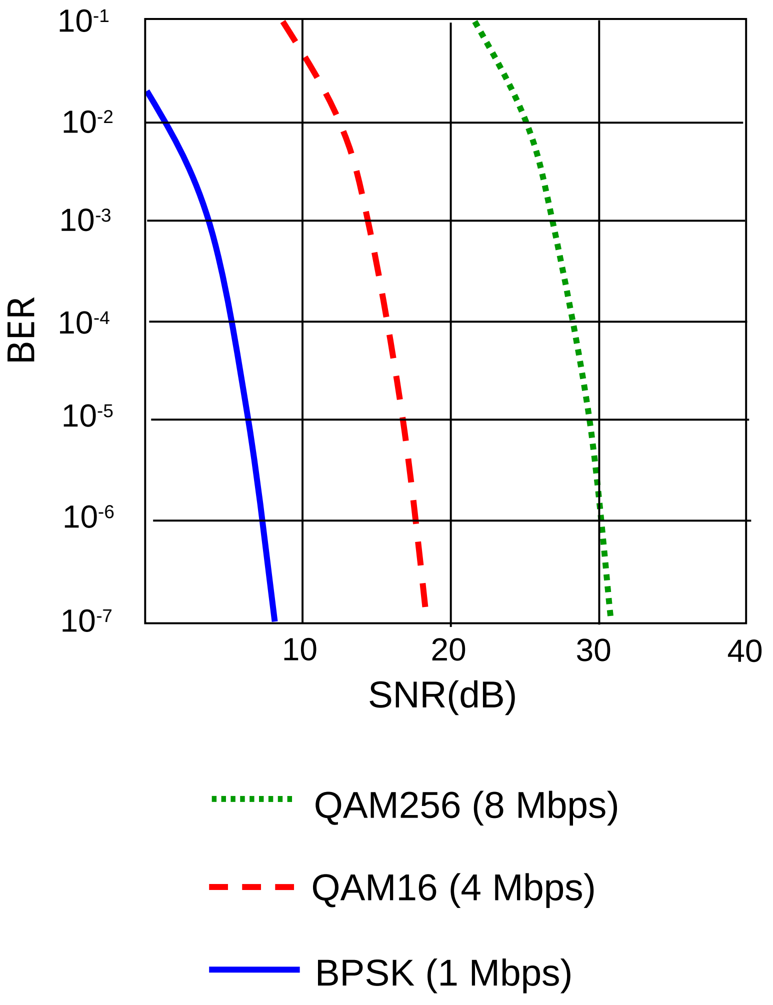
important differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone, microwave); devices (motors) interfere as well
- *multipath propagation:* radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more “difficult”

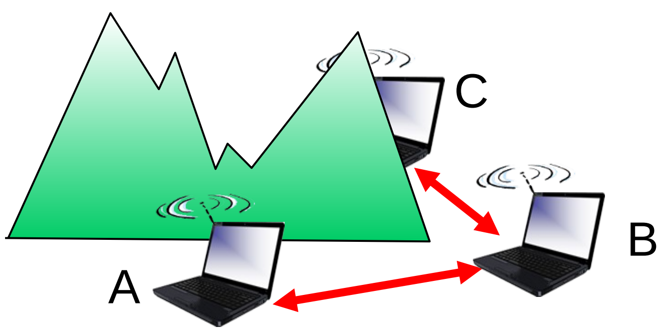
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- BER: bit error rate
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



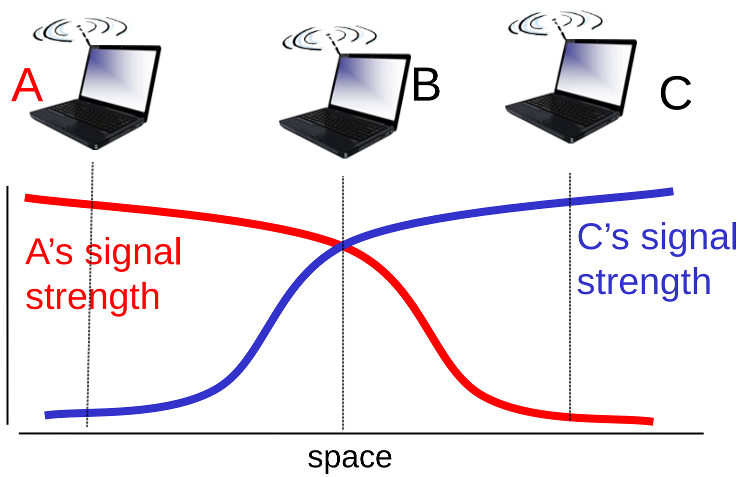
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Chapter 7 outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

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

7.4 Cellular Internet Access
- architecture
- standards (e.g., 3G, LTE)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

7.7 Handling mobility in cellular networks

7.8 Mobility and higher-layer protocols

IEEE 802.11 Wireless LAN

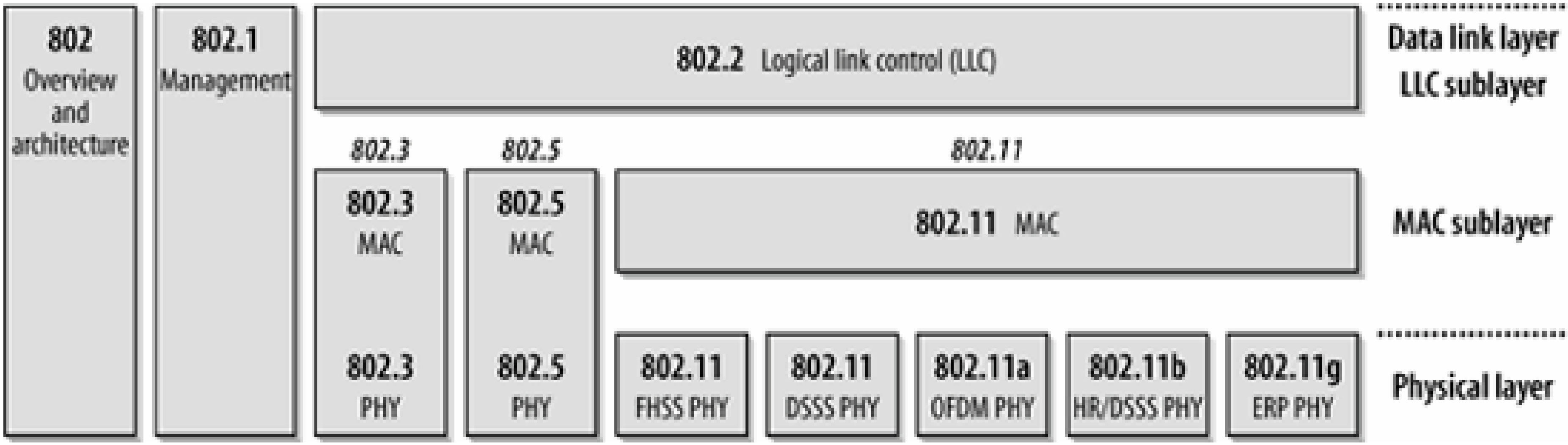
802.11b
- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

802.11a
- 5-6 GHz range
- up to 54 Mbps

802.11g
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae
- 2.4-5 GHz range
- up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions



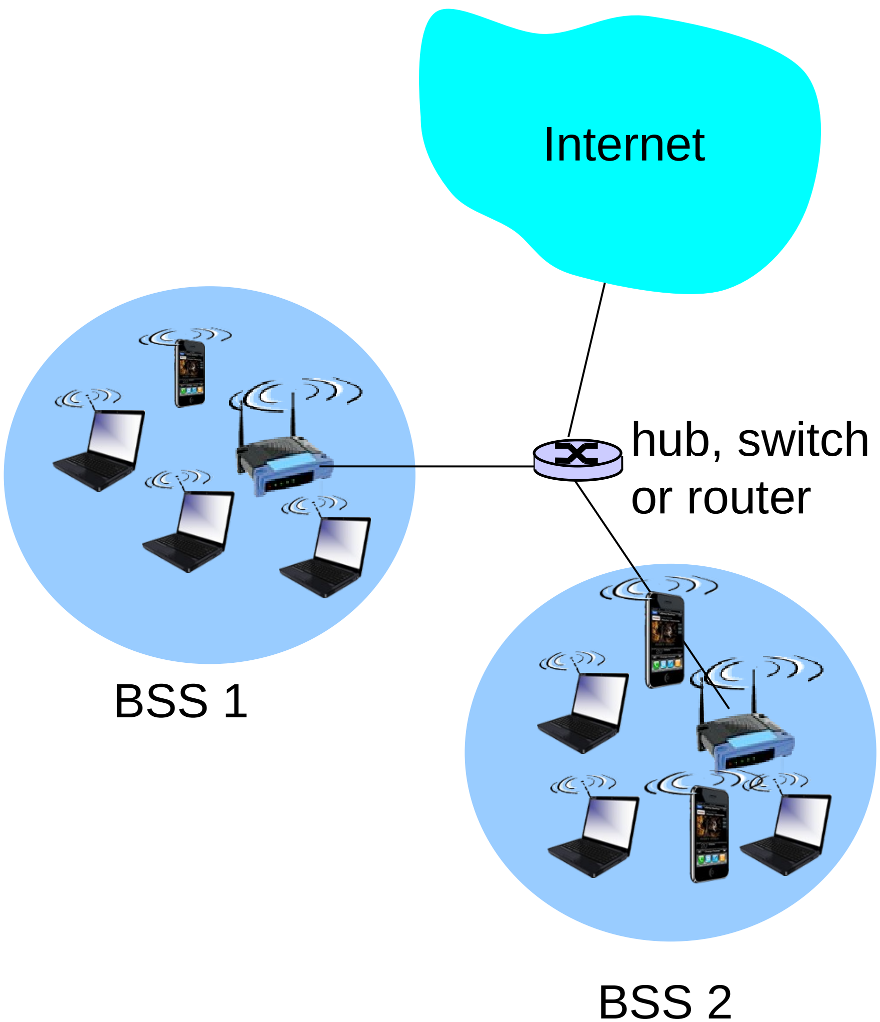
IEEE 802 Standards

802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

Overview of protocols

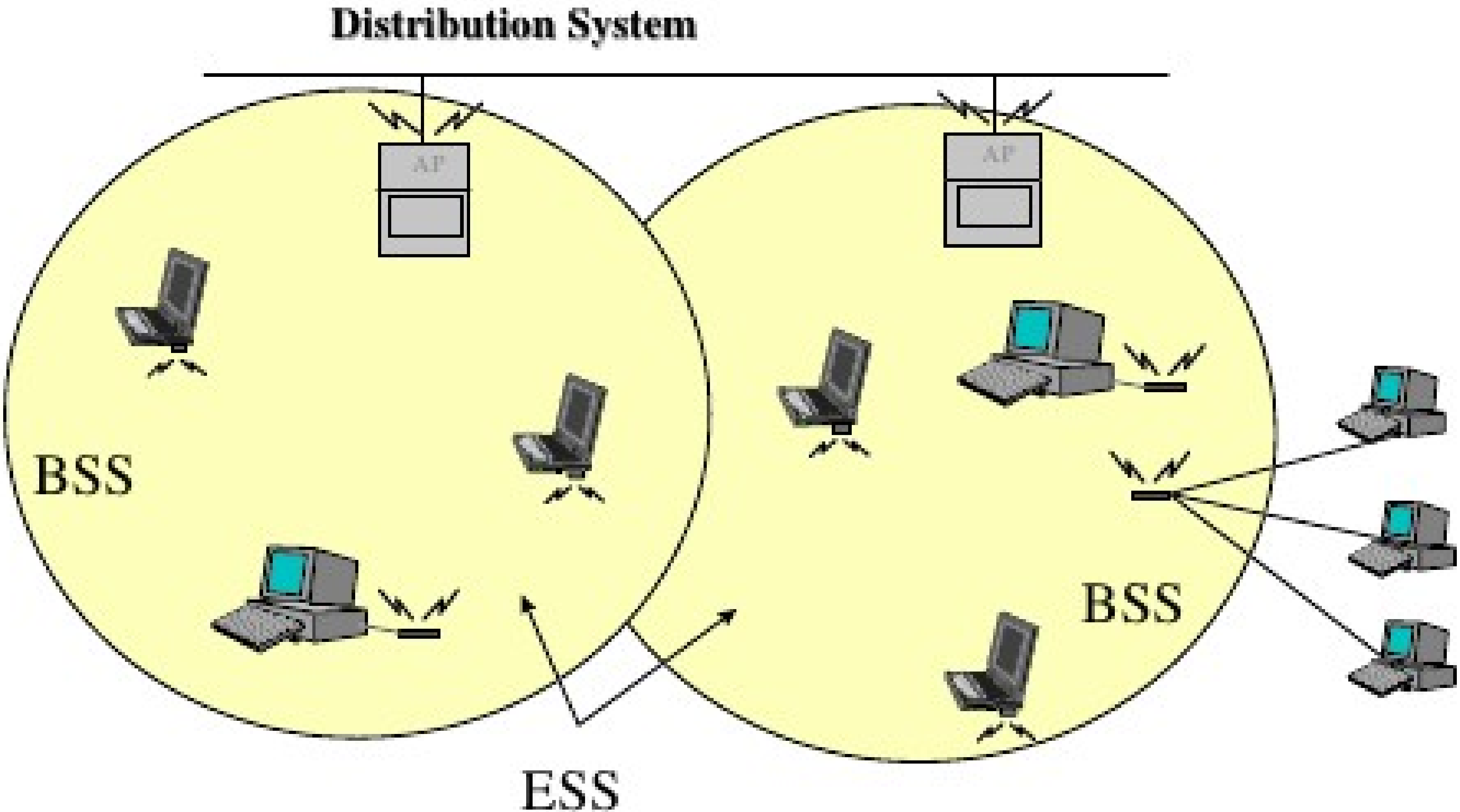
https://en.wikipedia.org/wiki/IEEE_802.11#Protocol

802.11 LAN architecture



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

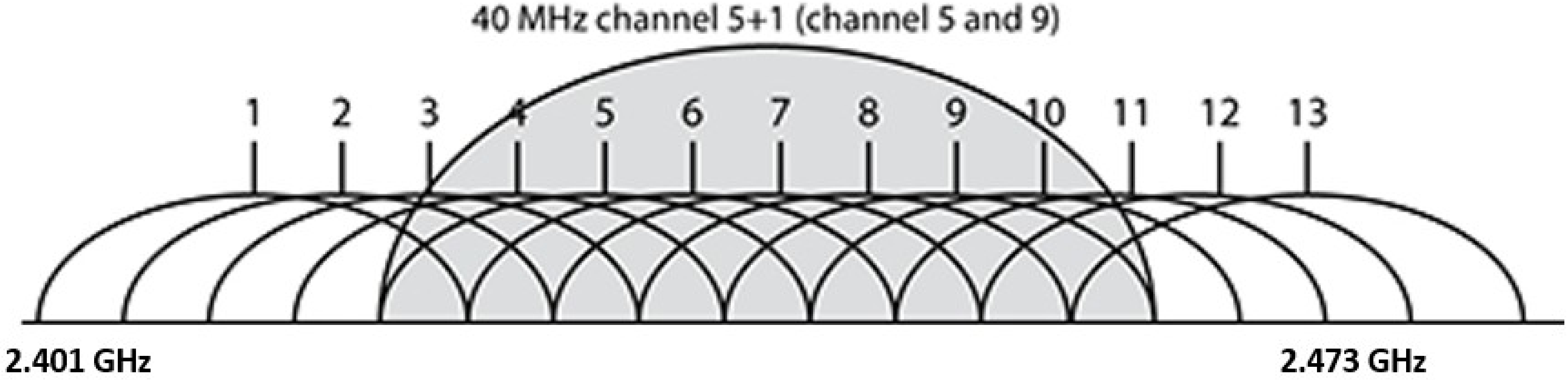
ESS and BSS

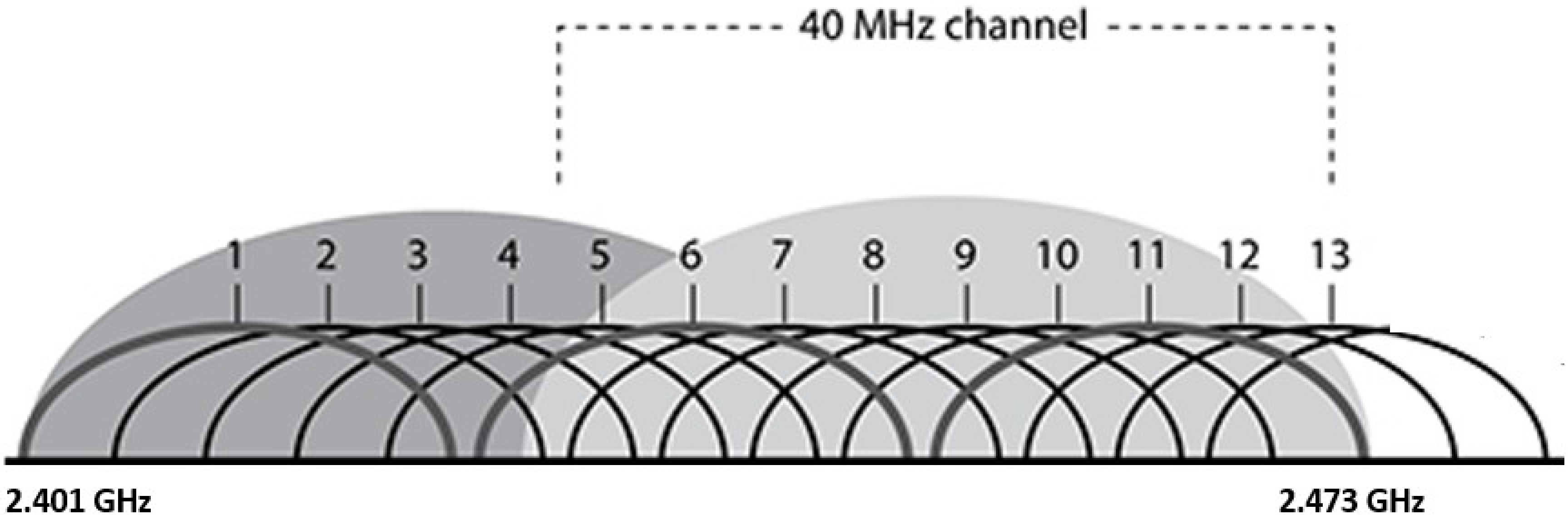


Service	Station or distribution service?	Description
Distribution	Distribution	Service used in frame delivery to determine destination address in infrastructure networks
Integration	Distribution	Frame delivery to an IEEE 802 LAN outside the wireless network
Association	Distribution	Used to establish the AP which serves as the gateway to a particular mobile station
Reassociation	Distribution	Used to change the AP which serves as the gateway to a particular mobile station
Disassociation	Distribution	Removes the wireless station from the network
Authentication	Station	Establishes station identity (MAC address) prior to establishing association
Deauthentication	Station	Used to terminate authentication, and by extension, association
Confidentiality	Station	Provides protection against eavesdropping
MSDU delivery	Station	Delivers data to the recipient
Transmit Power Control (TPC)	Station/spectrum management	Reduces interference by minimizing station transmit power
Dynamic Frequency Selection (DFS)	Station/spectrum management	Avoids interfering with radar operation in the 5 GHz band

802.11: Channels, association

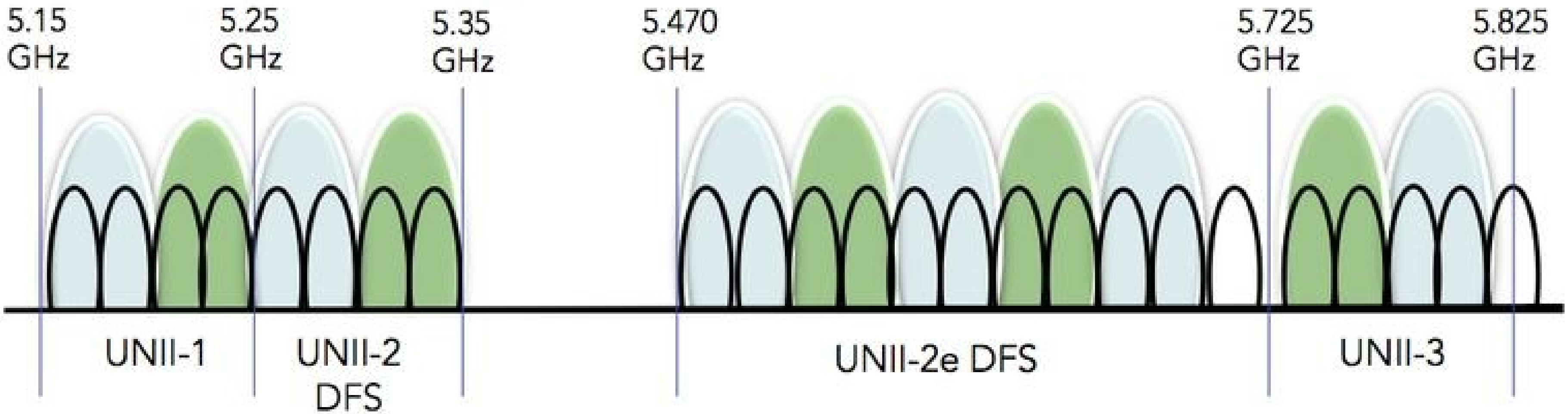
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication [Chapter 8]
  - will typically run DHCP to get IP address in AP's subnet

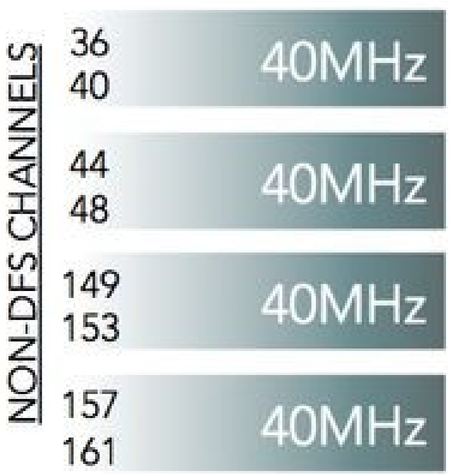




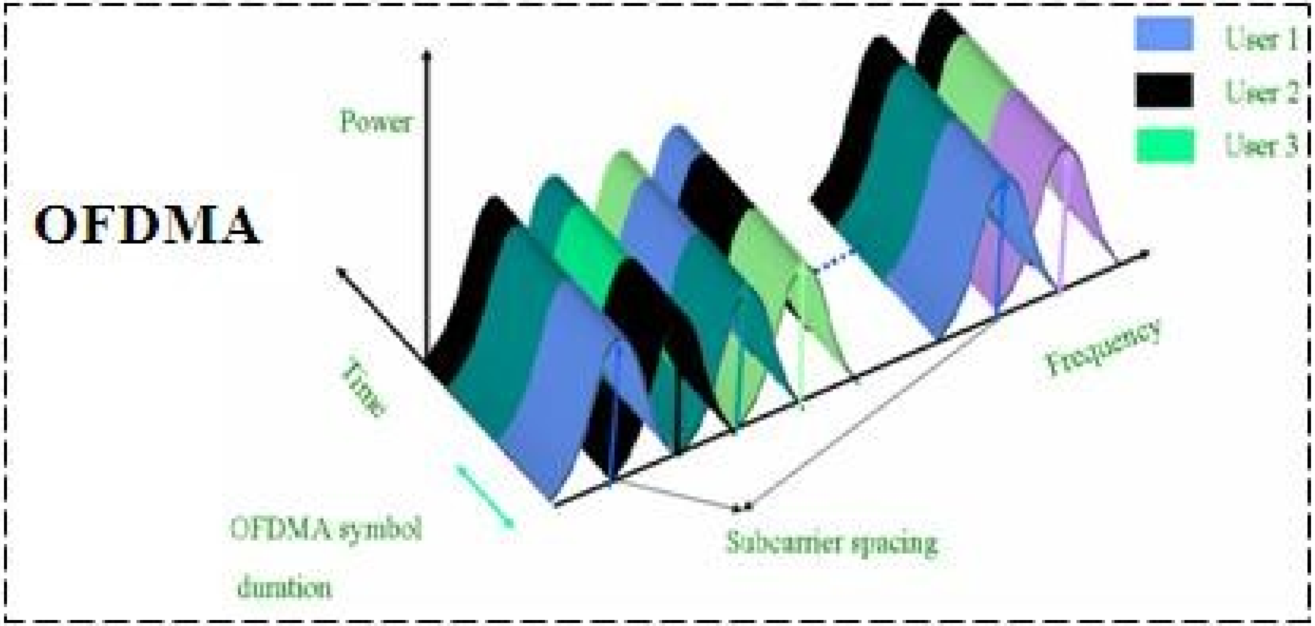
Source: Wescott, et al. CWAP Official Study Guide, Wiley Publishing, Inc. 2011.

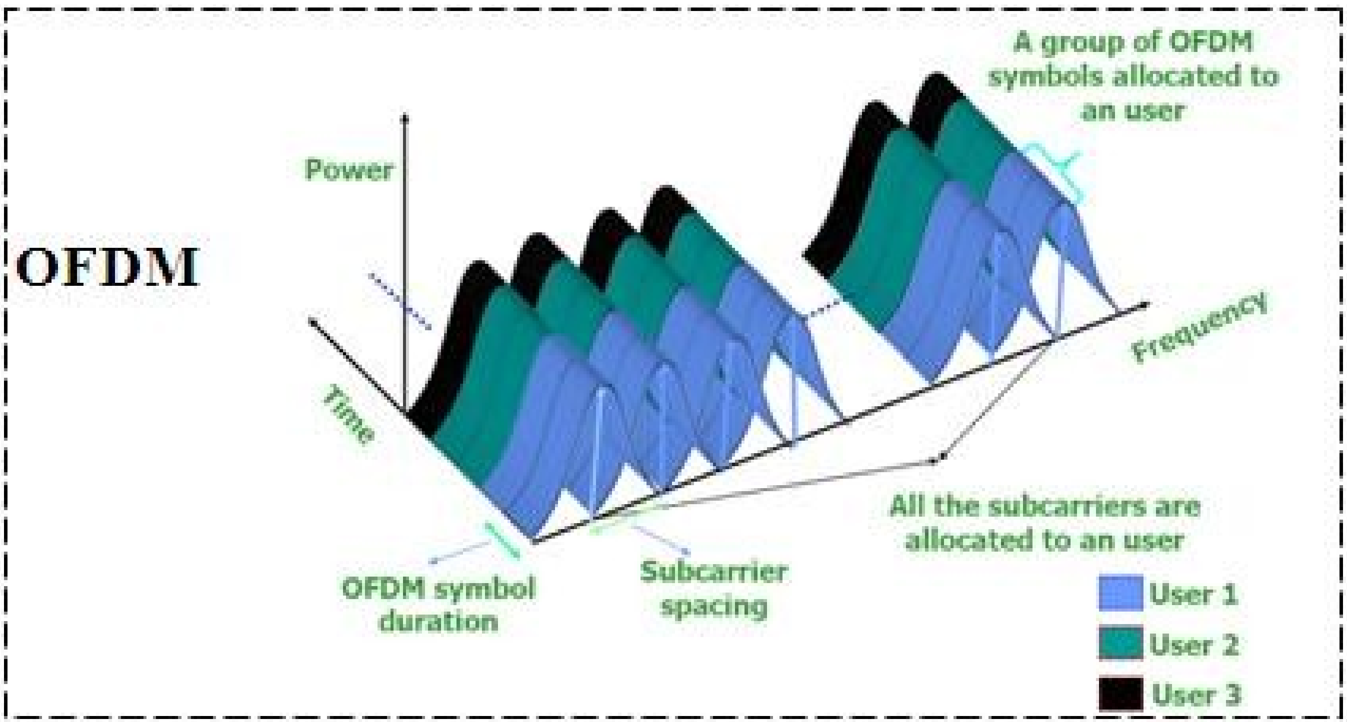
The Wi-Fi Spectrum: 5GHz



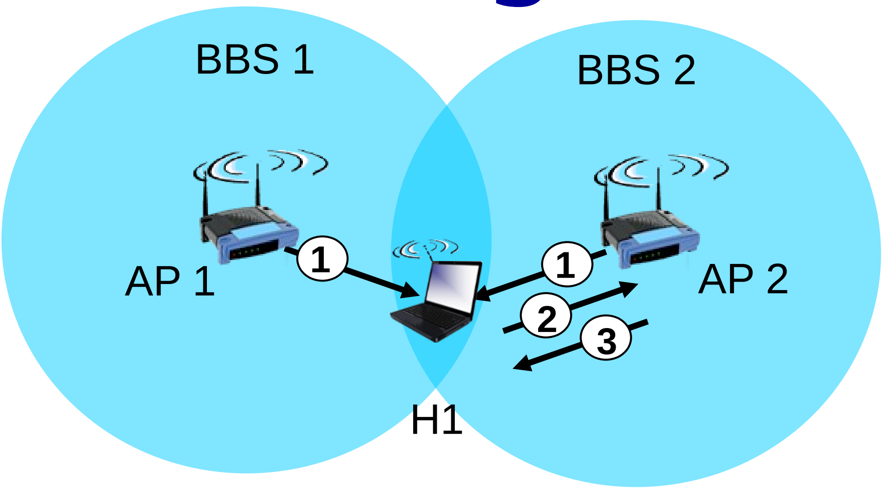


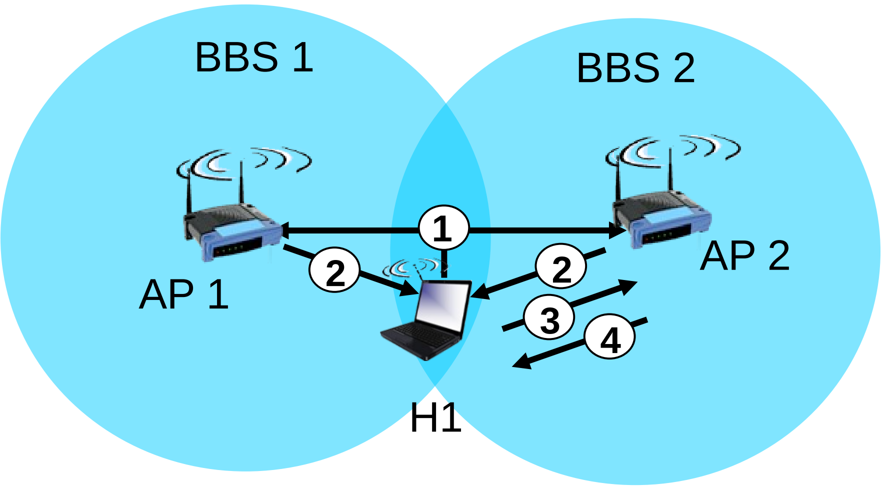
- 21 non-overlapping 20 MHz channels
- 9 non-overlapping 40 MHz channels
- Only 4 non-DFS channels for bonding
- Creates channel planning problems similar to 2.4 GHz
- 5 GHz isn't a panacea, RF management is still king


OFDMA
Power
User 1
User 2
User 3
Time
Frequency
OFDMA symbol
duration
Subcarrier spacing


OFDM
A group of OFDM symbols allocated to an user
Power
Time
Frequency
All the subcarriers are allocated to an user
OFDM symbol duration
Subcarrier spacing
User 1
User 2
User 3

802.11: passive/active scanning





passive scanning:

(1) beacon frames sent from APs

(2) association Request frame sent: H1 to selected AP

(3) association Response frame sent from selected AP to H1

***active scanning*:**

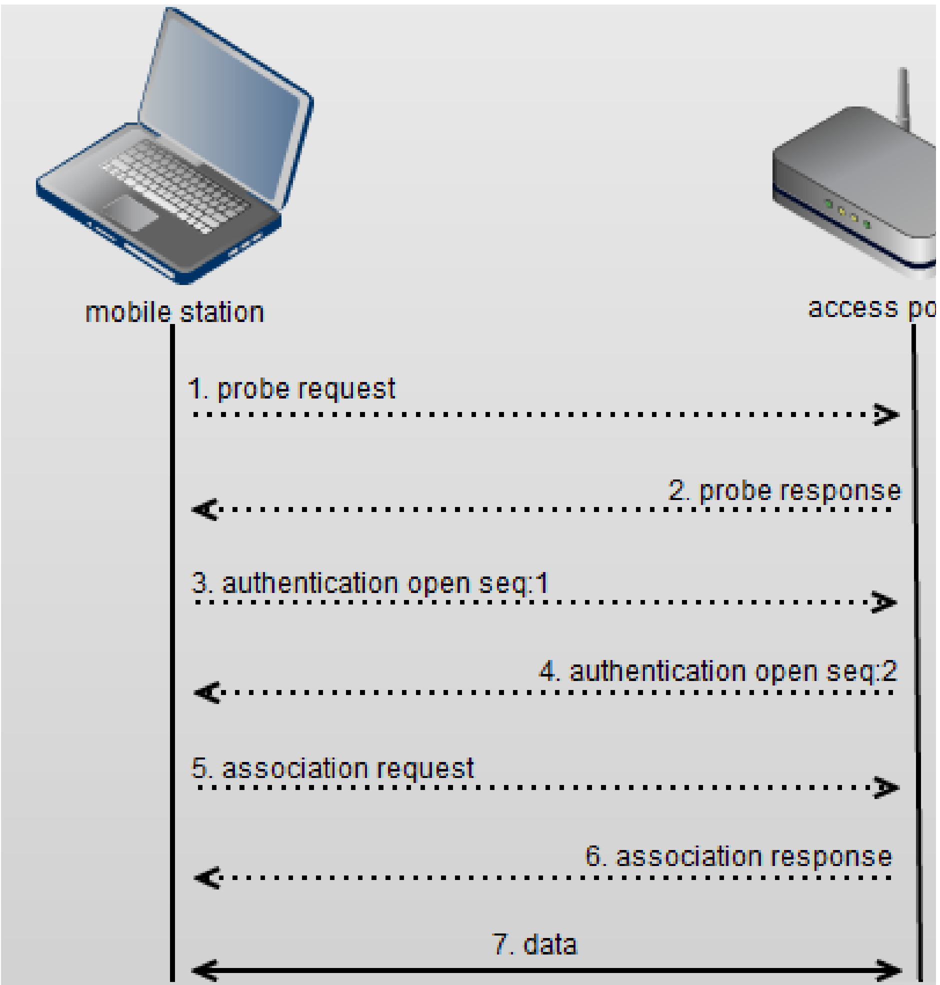
(1) Probe Request frame broadcast from H1

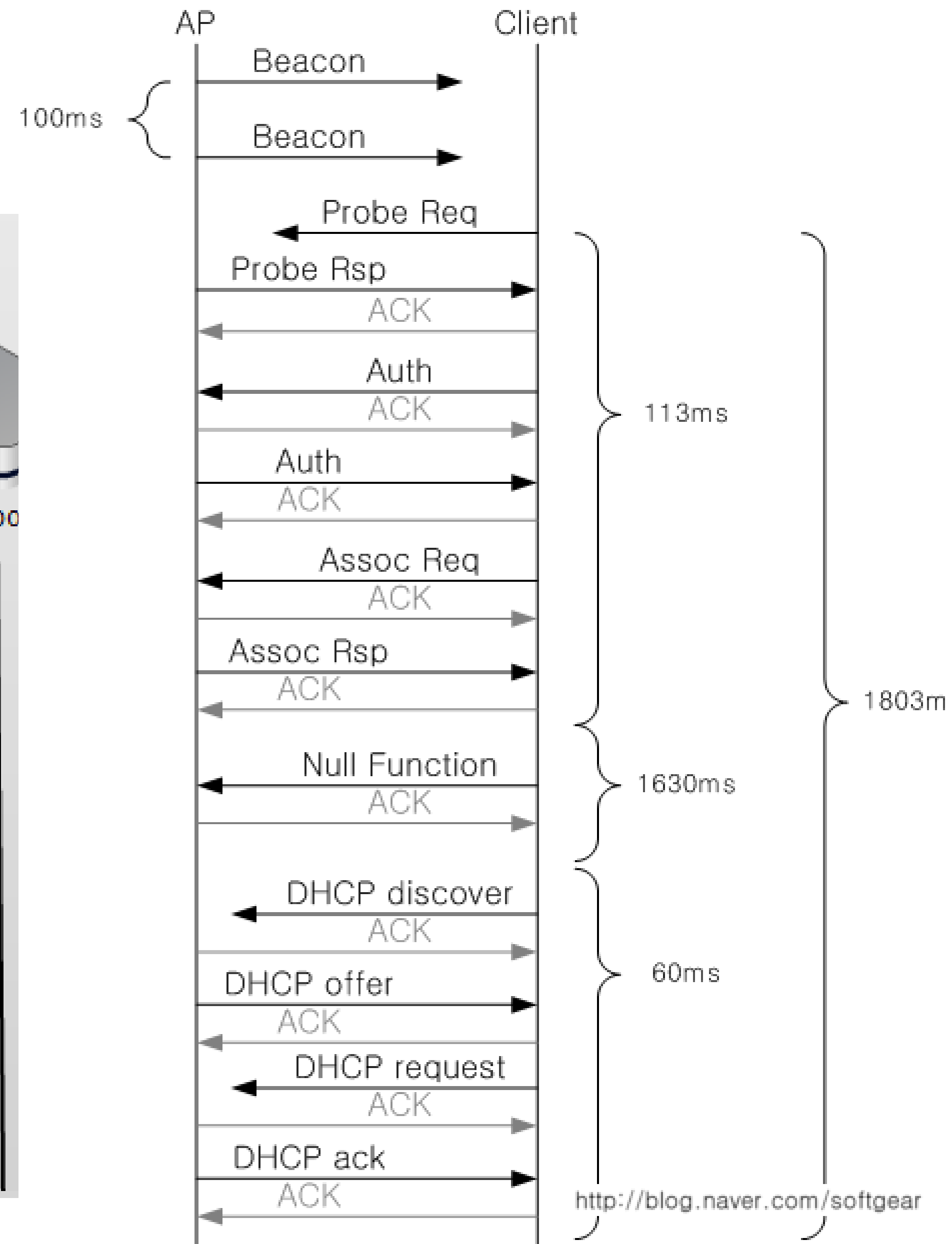
(2) Probe Response frames sent from APs

(3) Association Request frame sent: H1 to selected AP

(4) Association Response frame sent from selected AP to H1

Association





BSSID and SSID

Basic service sets are identified by BSSIDs, which are 48-bit labels that conform to MAC-48 conventions. Logical networks (including extended service sets) are identified by SSIDs, which serve as "network names" and are typically natural language labels.

In open authentication the station sends an authentication request to the access point and the access point replies. About all the station needs to know is the SSID of the access point, though it is usually possible to configure the access point to restrict admission to stations with MAC (physical) addresses on a predetermined list. Stations sometimes evade MAC-address checking by changing their MAC address to an acceptable one, though some Wi-Fi drivers do not support this.

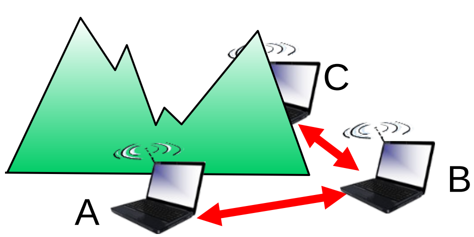
Because the SSID plays something of the role of a password here, some Wi-Fi access points are configured so that beacon packets does not contain the SSID; such access points are said to be hidden. Unfortunately, access points hidden this way are easily unmasked: first, the SSID is sent in the clear by any other stations that need to authenticate, and second, an attacker can often transmit forged deauthentication or disassociation requests to force legitimate stations to retransmit the SSID.

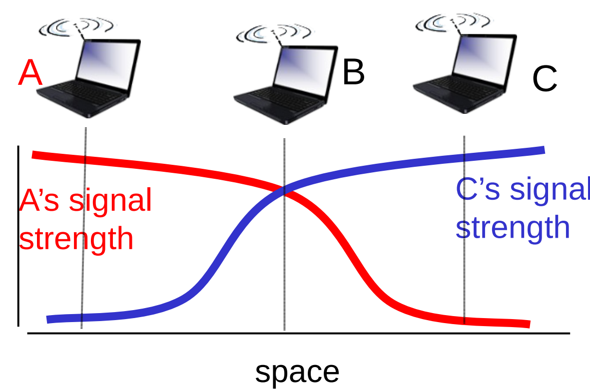
Beacon frames

- Access points periodically broadcast their SSID in special beacon packets.
- These broadcasts allow stations to **see a list of available networks**; the beacon packets also contain other **Wi-Fi network parameters** such as radio-modulation parameters and available data rates.
- Beacons support the **power-management doze mode**. Some stations may elect to enter this power-conservation mode, in which case they inform the access point, record the announced beacon-transmission time interval and then wake up briefly to receive each beacon. Beacons, in turn, each contain a list (in a compact bitmap form) of each dozing station for which the access point has a packet to deliver.
- Ad hoc networks have beacon packets as well; all nodes participate in the regular transmission of these via a distributed algorithm.

IEEE 802.11: multiple access

- avoid collisions: 2$^+$ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

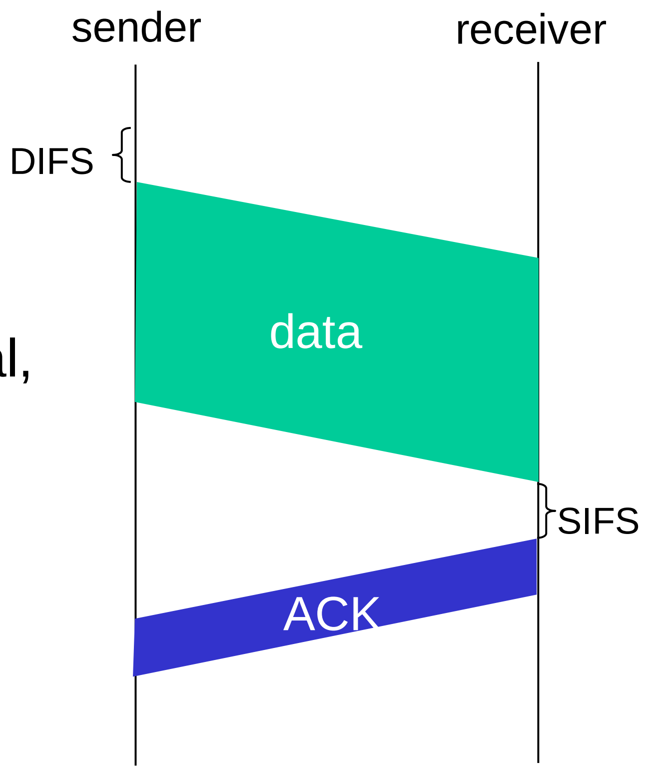
802.11 sender

1 if sense channel idle for **DIFS** then
  transmit entire frame (no CD)

2 if sense channel busy then
  start random backoff time
  timer counts down while channel idle
  transmit when timer expires
  if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)



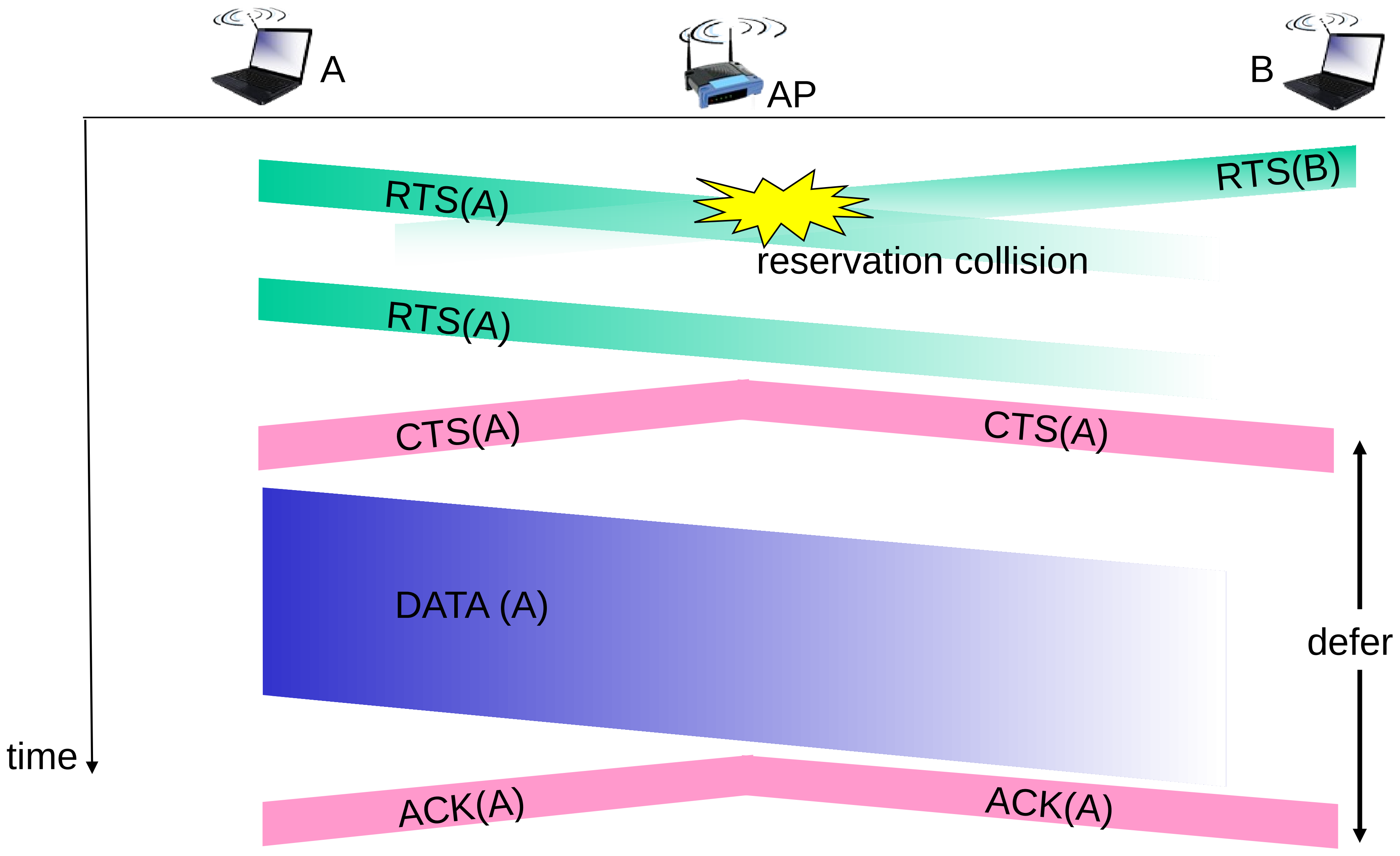
Avoiding collisions (more)

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

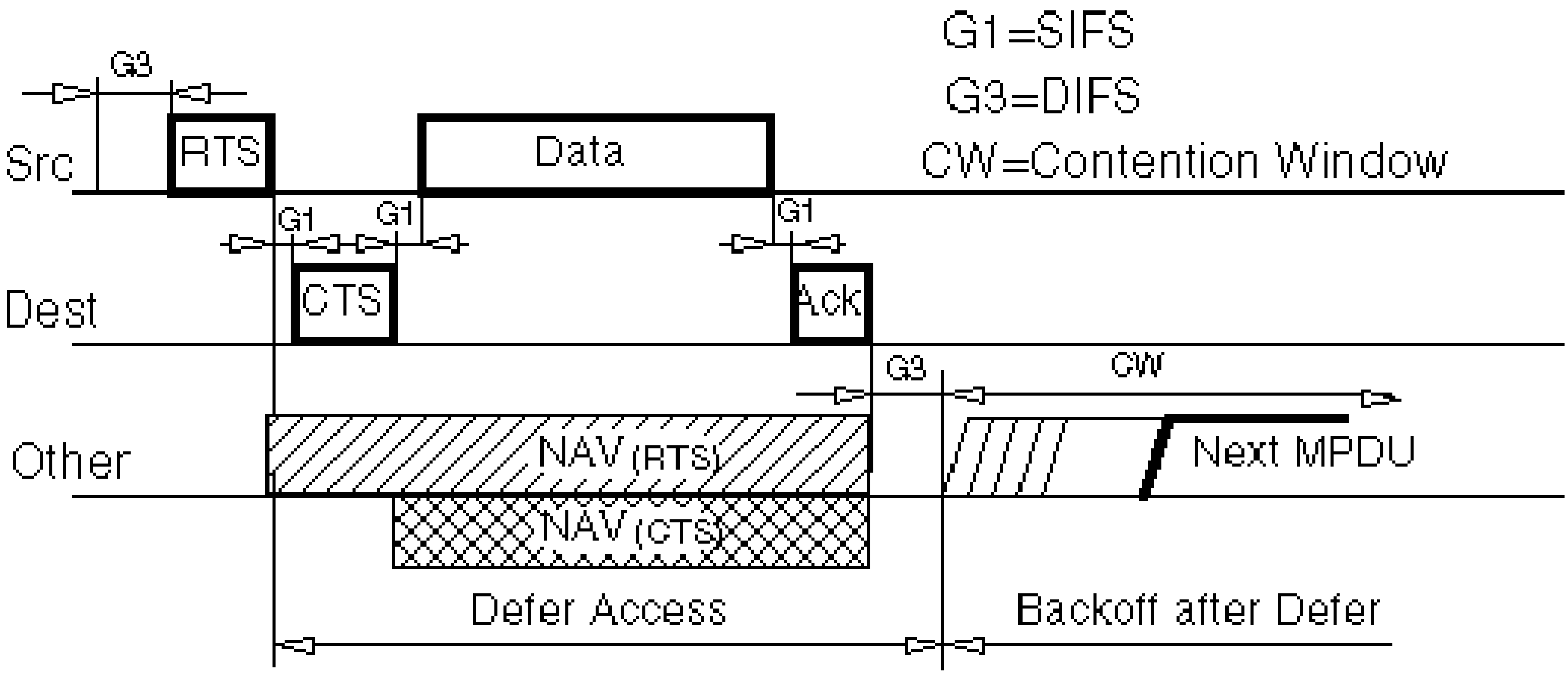
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

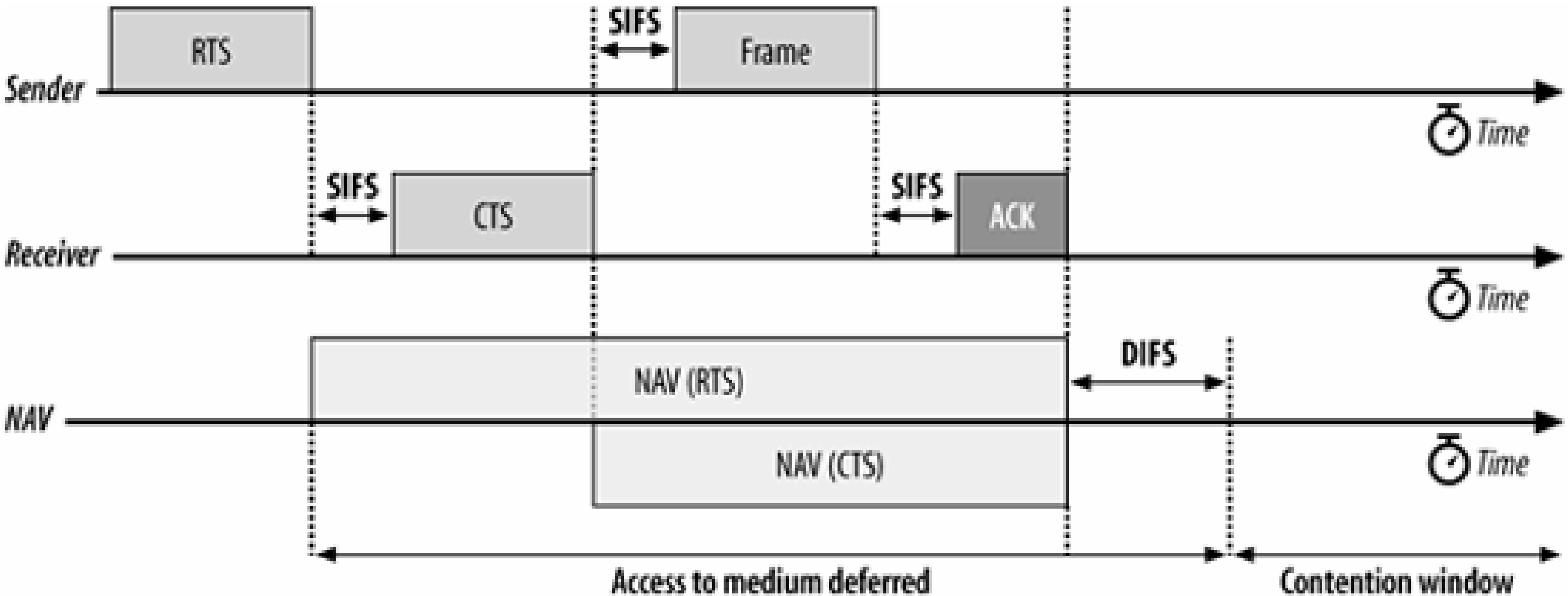
Collision Avoidance: RTS-CTS exchange



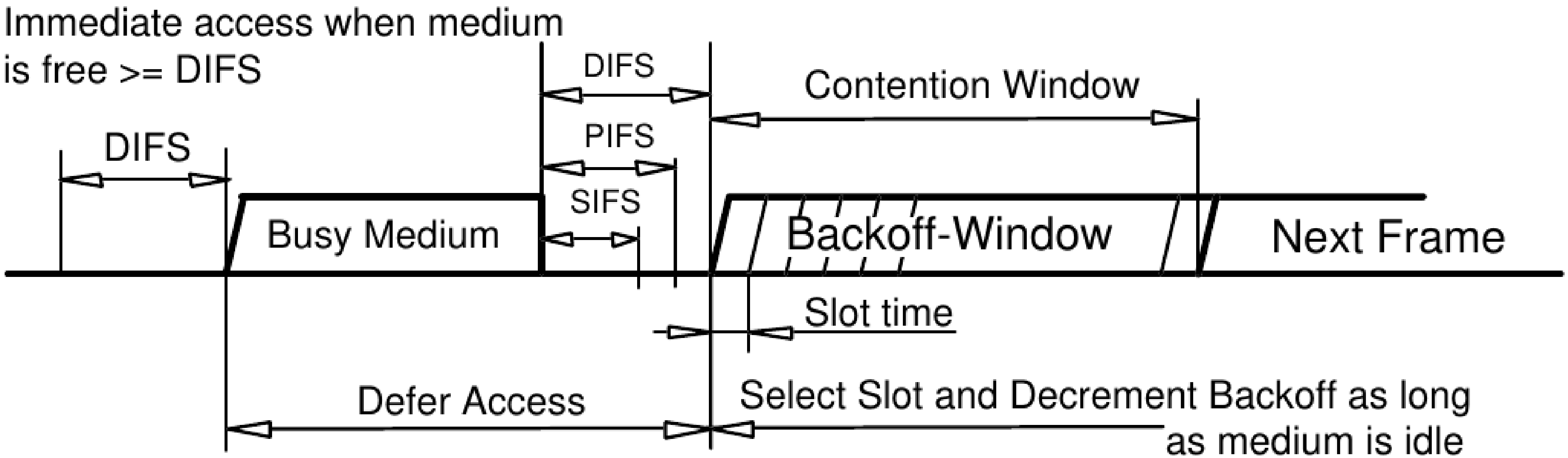
Virtual busy "sensing"



The NAV State is combined with the physical carrier sense to indicate the busy state of the medium.

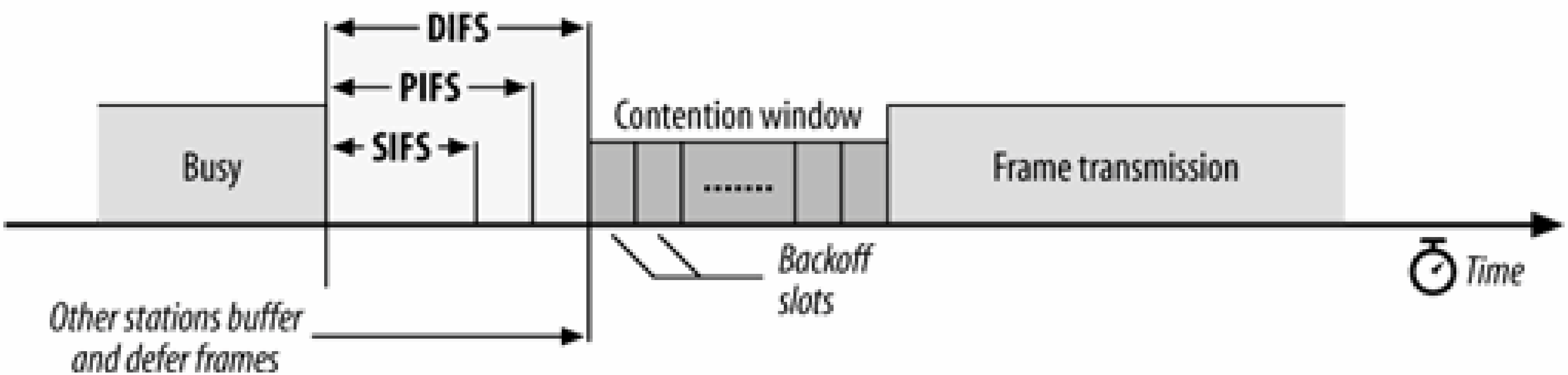


RTS
SIFS
Frame
Sender
Time
SIFS
CTS
SIFS
ACK
Receiver
Time
NAV (RTS)
DIFS
NAV
NAV (CTS)
Time
Access to medium deferred
Contention window



The 802.11 standard defines an **Exponential Backoff Algorithm**, that must be executed in the following cases:

- If when the station senses the medium before the first transmission of a packet, and the medium is busy,
- After each retransmission, and
- After a successful transmission


DIFS
PIFS
SIFS
Busy
Contention window
....
Frame transmission
Backoff slots
Time
Other stations buffer and defer frames

Pre-mac physical layer headers

Preamble	PLCP Header	MAC Data	CRC

Preamble
This is PHY dependent, and includes:

Synch: An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing, and SFD: A Start Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define the frame timing.

PLCP Header
The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information that will be used by the PHY Layer to decode the frame, and consists of:

PLCP_PDU Length Word: which represents the number of bytes contained in the packet, this is useful for the PHY to correctly detect the end of packet,
PLCP Signaling Field: which currently contains only the rate information, encoded in 0.5 Mbps increments from 1 Mbit/s to 4.5 Mbit/s, and Header Error Check Field: Which is a 16 Bit CRC error detection field

Keeping Synchronization

The AP transmits periodic frames called Beacon Frames, these frames contain the value of the AP's clock on the moment of the transmission (note that this is the moment when the transmission really occurs, and not when it is put in the queue for transmission, since the Beacon Frame is transmitted using the rules of CSMA, the transmission may be delayed significantly).

The receiving stations check the value of their clock at the receiving moment, and correct it to keep synchronizing with the AP's clock, this prevents clock drifting which could cause loss of synch after a couple of hours of operation.

802.11 frame: addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

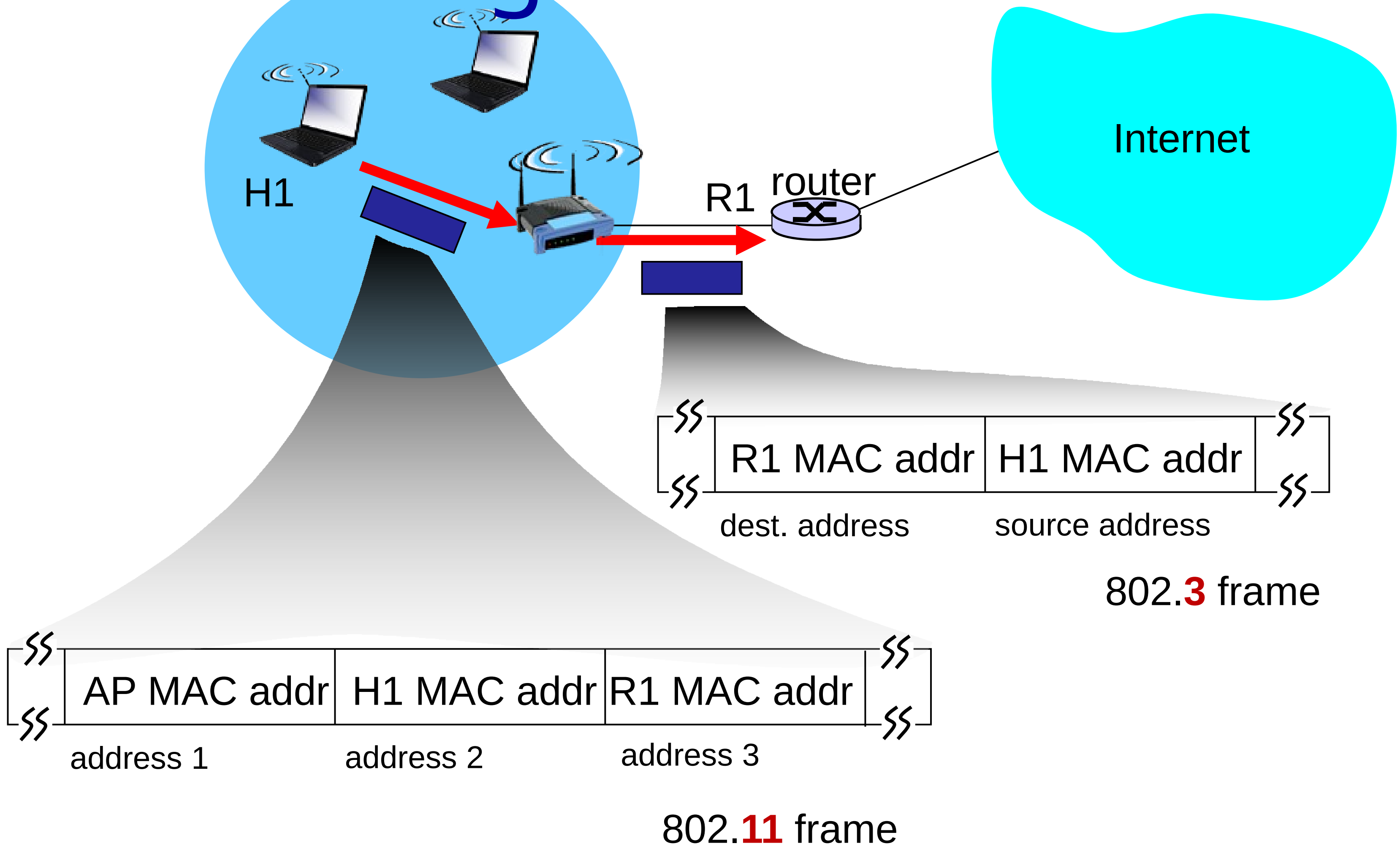
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

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

Address 4: used only in ad hoc mode

802.11 frame: addressing



Address Fields

A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:

Address-1 is always the Recipient Address (i.e. the station on the BSS who is the immediate recipient of the packet), if ToDS is set this is the Address of the AP, if ToDS is not set then this is the address of the end-station.

Address-2 is always the Transmitter Address (i.e. the station who is physically transmitting the packet), if FromDS is set this is the address of the AP, if it is not set then it is the address of the Station.

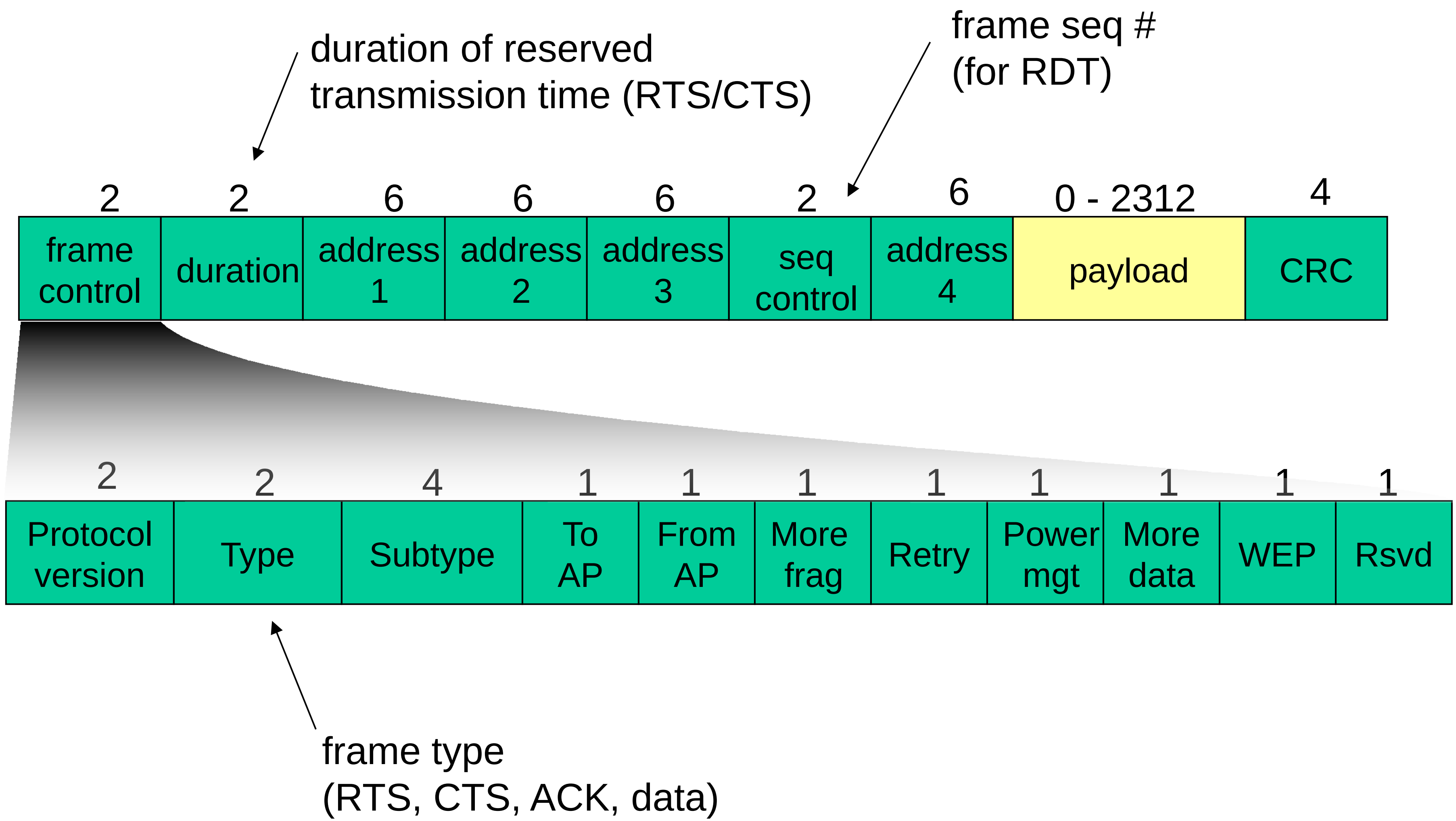
Address-3 is in most cases the remaining, missing address, on a frame with FromDS set to 1, then the Address-3 is the original Source Address, if the frame has the ToDS set then Address 3 is the destination Address.

Address-4 is used on the special case where a Wireless Distribution System is used, and the frame is being transmitted from one Access Point to another, in this case both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.

The following Table summarizes the usage of the different Addresses according to the ToDS and FromDS bits setting:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

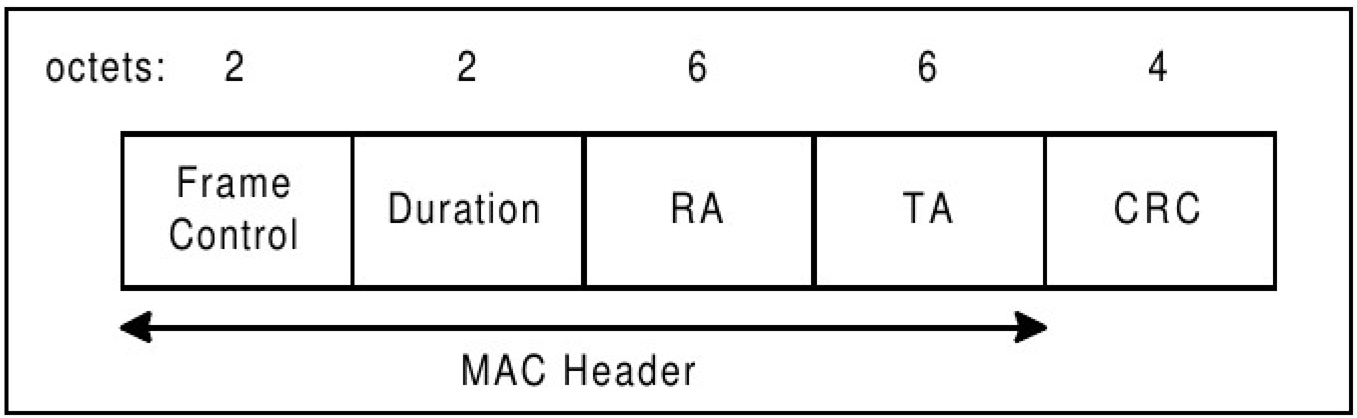
802.11 frame: more



Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
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
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 Function (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	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

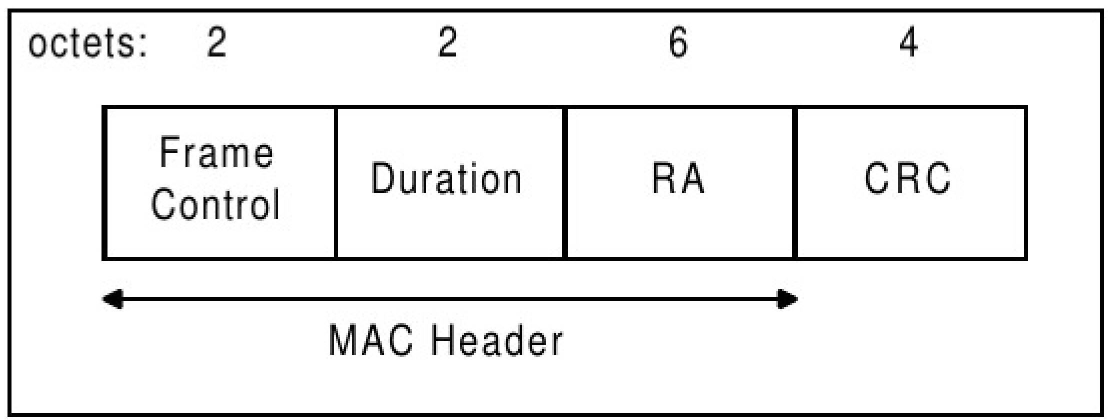
RTS Frame Format

The RTS frame looks as follows:



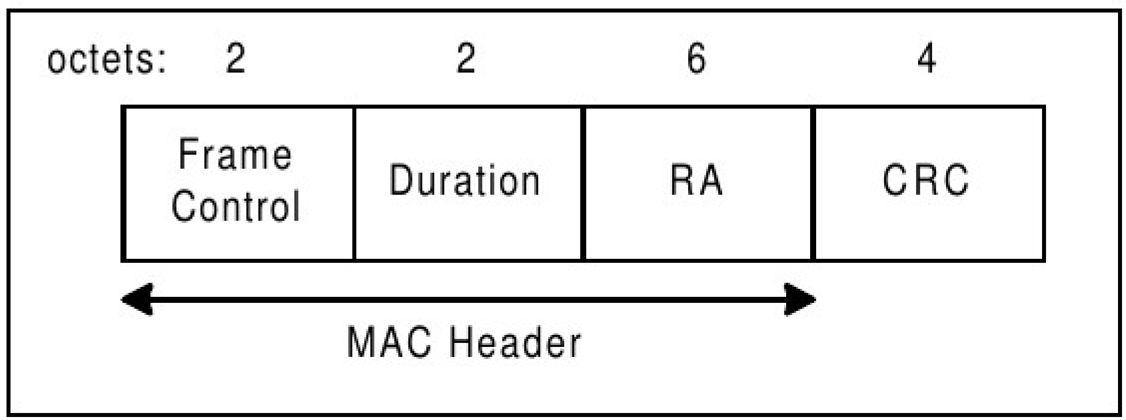
CTS Frame Format

The CTS frame looks as follows:

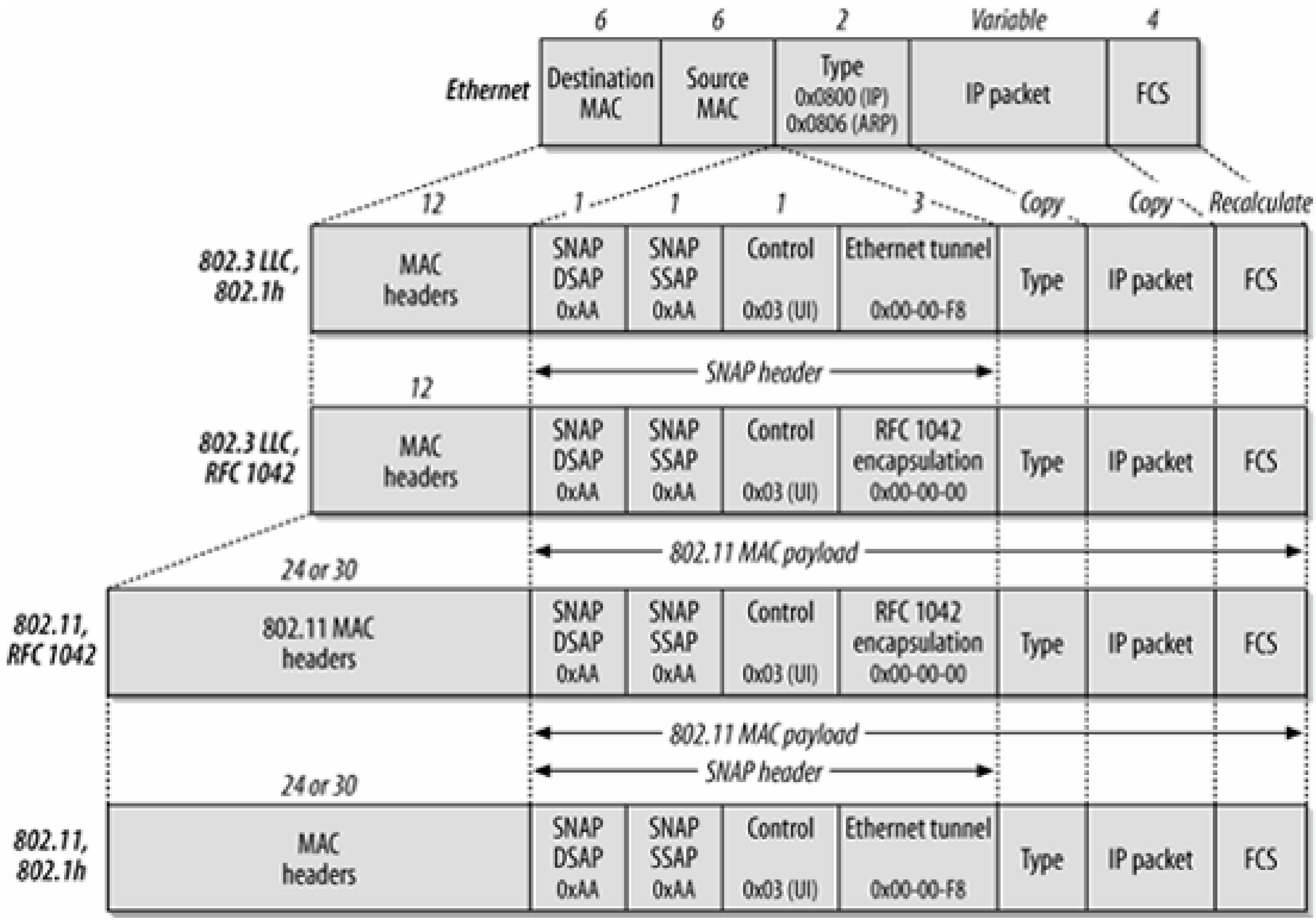


ACK Frame Format

The ACK frame looks as follows:.



Logical Link Control (layer 2.5)

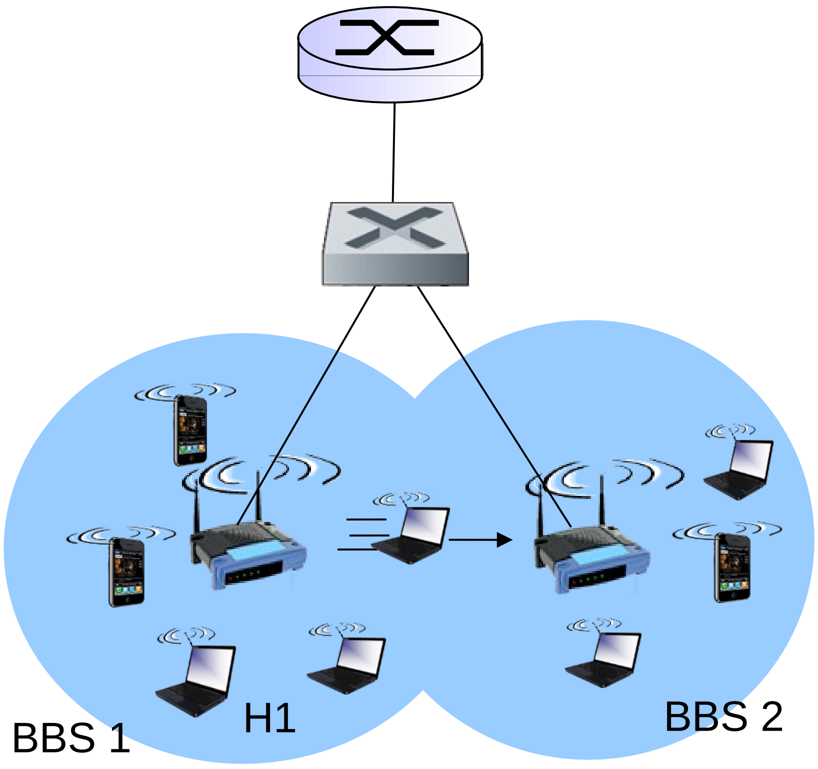


Wireshark and Other materials

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

802.11: mobility within same subnet

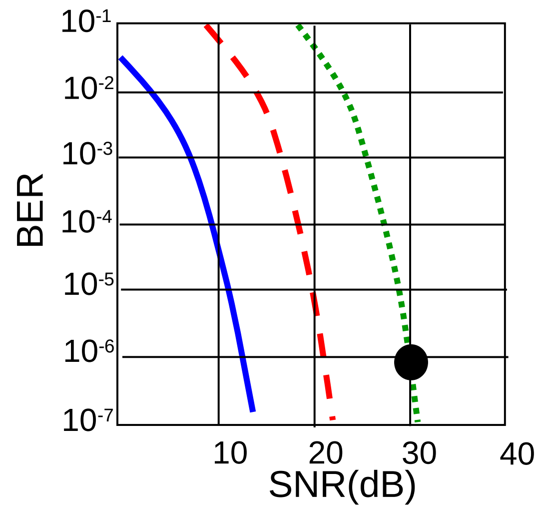
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and “remember” which switch port can be used to reach H1

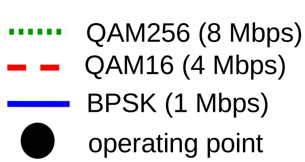


802.11: advanced capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies





1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

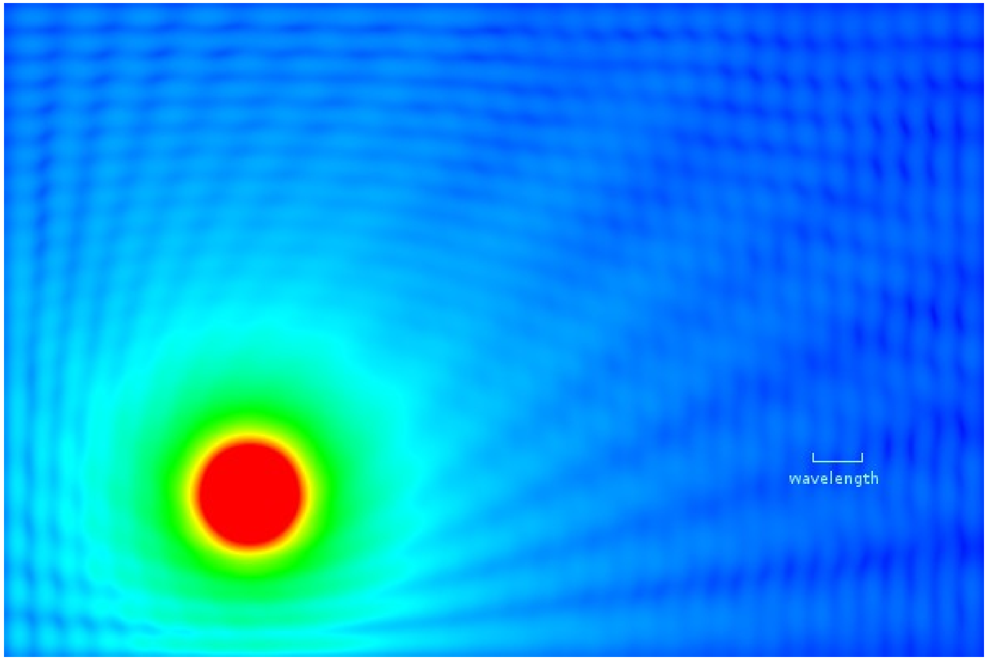
802.11: advanced capabilities

power management

- node-to-AP: “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 mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

MIMO and multipath issues

Warbles are about 3 meters with 2.5ghz



MAC address randomization

- Most Wi-Fi-enabled devices are configured to transmit Wi-Fi probe requests at regular intervals (and on all available channels), at least when not connected.
- These probe requests identify available Wi-Fi networks, but they also reveal the device's MAC address.
- This allows sites such as stores to track customers by their device.
- Probe requests are generally sent when the device is not joined to a network.
- To prevent tracking via probe requests, the simplest approach is to change the MAC address used for probes at regular, frequent intervals.
- A device might even change its MAC address on every probe.
- Changing the MAC address used for actually joining a network is also important to prevent tracking, but introduces some complications. RFC 7844 suggests these options for selecting new random addresses:

1) At **regular time intervals**
2) **Per connection**: each time the device connects to a Wi-Fi network, it will select a new MAC address
3) **Per network**: like the above, except that if the device reconnects to the same network (identified by SSID), it will use the same MAC address

Ad-hoc and mesh networks

https://en.wikipedia.org/wiki/IEEE_802.11s
https://en.wikipedia.org/wiki/Wireless_ad_hoc_network

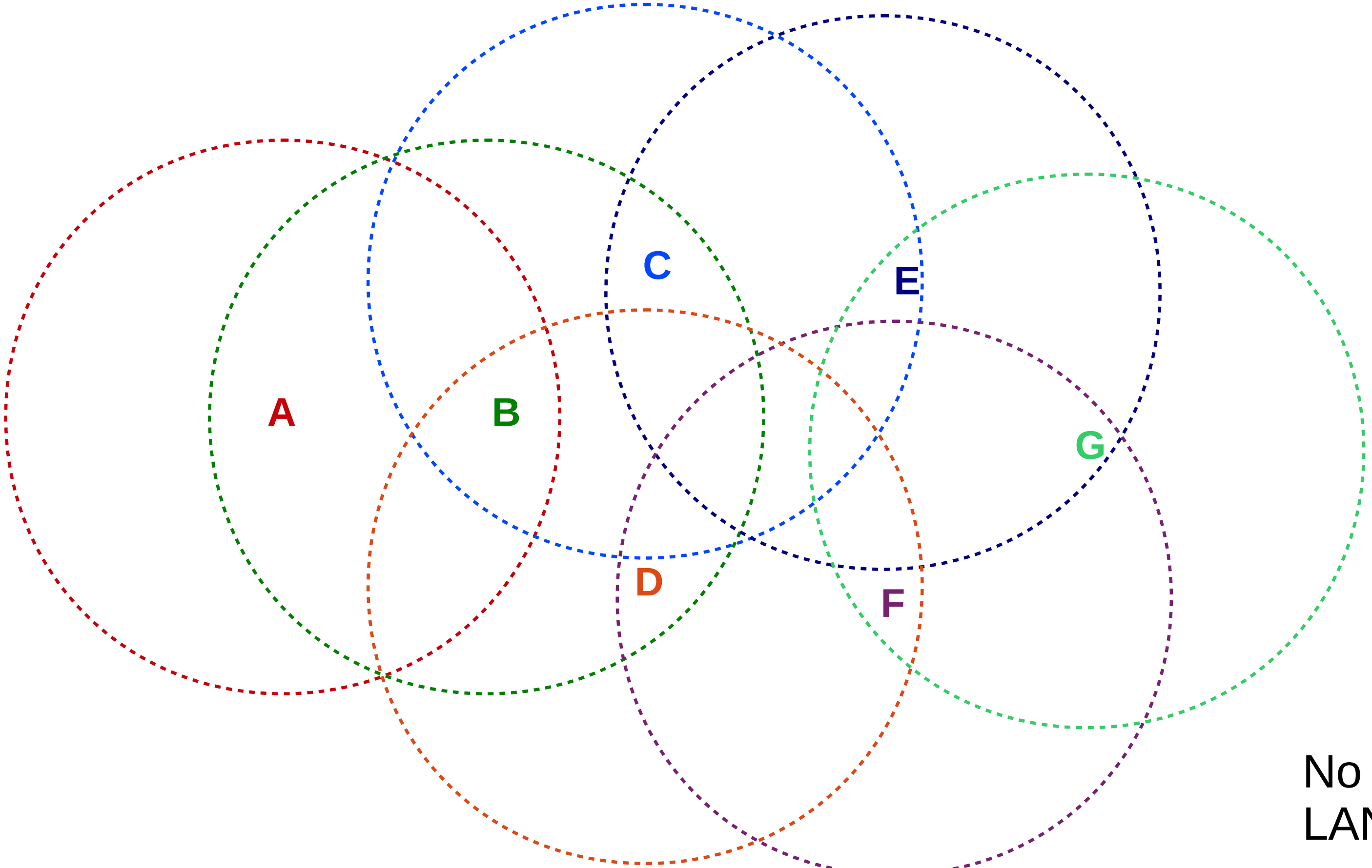
In creating a mesh network with a Wi-Fi distribution system proprietary or 802.11s the participating access points must address the following issues:

- They must authenticate to one another
- They must identify the correct access point to reach a given station B
- They must correctly handle station B’s movement to a different access point
- They must agree on how to route, through the mesh of access points, between the station and the connection to the Internet

If a packet is routed through the mesh BSS from station A to station B, then more addresses are needed in the packet header. The ultimate source and destination are A and B, and the transmitter and receiver correspond to the specific hop, but the packet also needs a source and destination within the mesh, perhaps corresponding to the two access points to which A and B connect. 802.11s handles this by adding a mesh control field consisting of some management fields (such as TTL and sequence number) and a variable-length block of up to three additional addresses.

MANETs

The MANET acronym stands for mobile ad hoc network; in practice, the term generally applies to ad hoc wireless networks of sufficient complexity that some internal routing mechanism is needed to enable full connectivity.

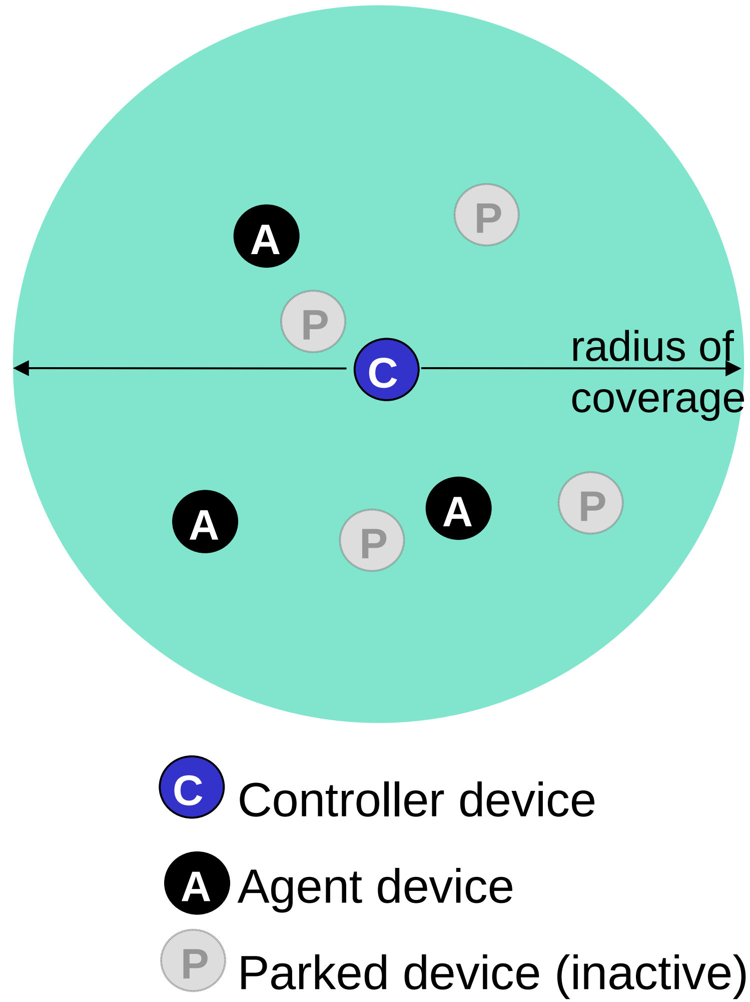


No broadcast
LAN routing hard

Typical MANET in which the radio range for each node is represented by a circle around that node. A can reach G either by the route A—B—C—E—G or by A—B—D—F—G.

802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- controller/agent:
  - agent request permission to send (to master)
  - controller grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps



Chapter 7 outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

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

7.4 Cellular Internet access
- architecture
- standards (e.g., 3G, LTE)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

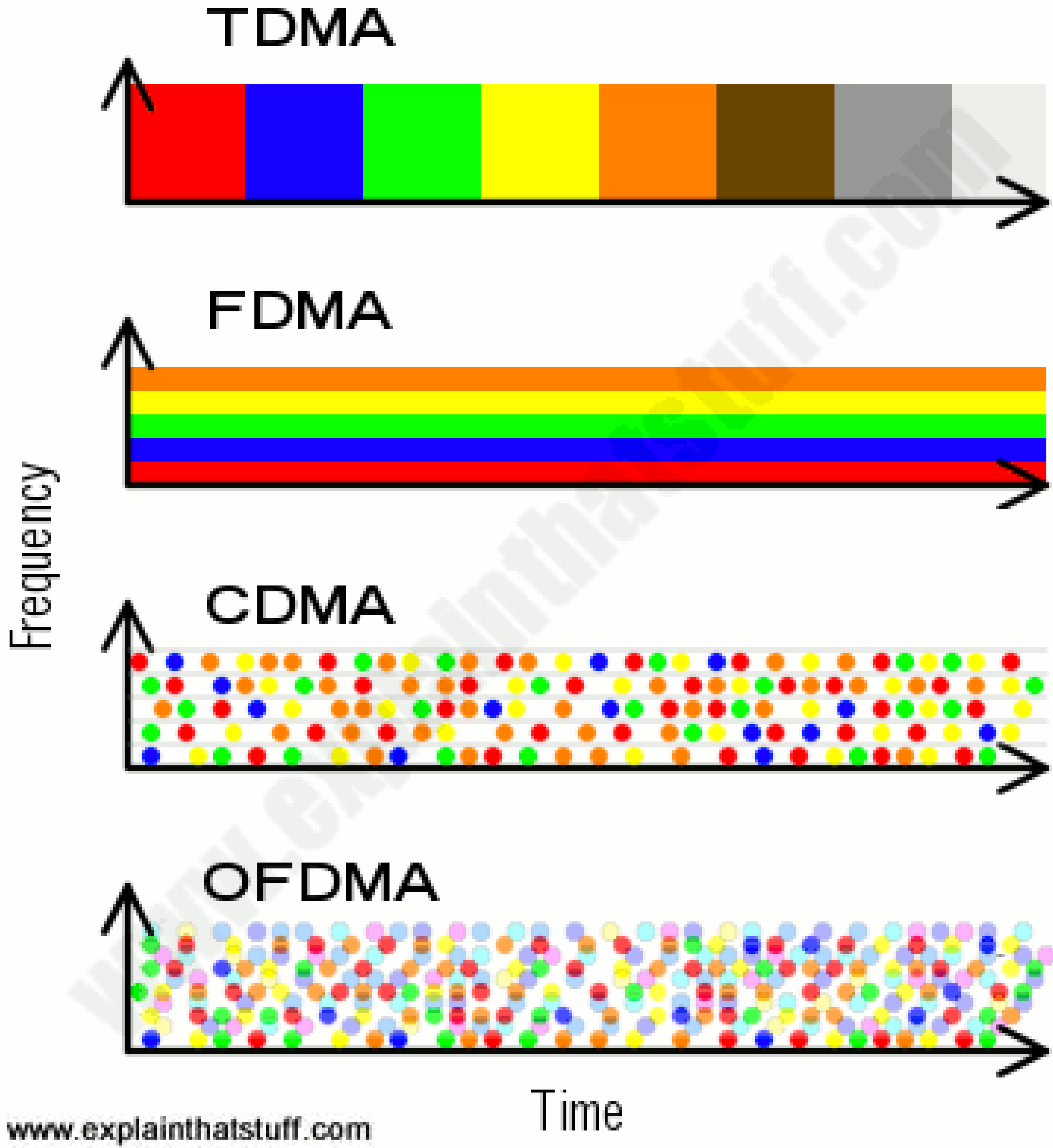
7.7 Handling mobility in cellular networks

7.8 Mobility and higher-layer protocols

List of mobile phone generations		
0G radio telephones (1946)		MTS · IMTS · Altai · OLT · MTA - MTB - MTC - MTD · AMTS · Autotel (PALM) · ARP · B-Netz · AMR
1G (1979)	**AMPS family**	AMPS - N-AMPS · TACS - ETACS
	Other	NMT · C-450 · Hicap · Mobitex · DataTAC
2G (1991)	**GSM/3GPP family**	GSM · CSD - HSCSD
	3GPP2 family	cdmaOne (IS-95)
	AMPS family	D-AMPS (IS-54 and IS-136)
	Other	CDPD · iDEN · PDC · PHS
2G transitional (2.5G, 2.75G)	**GSM/3GPP family**	GPRS · EDGE/EGPRS - Evolved EDGE
	3GPP2 family	CDMA2000 1X (TIA/EIA/IS-2000) · CDMA2000 1X Advanced
	Other	WiDEN · DECT
3G (2001)	**3GPP family**	UMTS (UTRA-FDD / W-CDMA (FOMA) · UTRA-TDD LCR / TD-SCDMA · UTRA-TDD HCR / TD-CDMA)
	3GPP2 family	CDMA2000 1xEV-DO Release 0 (TIA/IS-856)
3G transitional (3.5G, 3.75G, 3.9G)	**3GPP family**	HSPA (HSDPA · HSUPA) · HSPA+ (DC-HSDPA) · LTE (E-UTRA)
	3GPP2 family	CDMA2000 1xEV-DO Revision A (TIA/EIA/IS-856-A) · EV-DO Revision B (TIA/EIA/IS-856-B) · EV-DO Revision C
	IEEE family	Mobile WiMAX (IEEE 802.16e) · Flash-OFDM · iBurst (IEEE 802.20) · WiBro
	ETSI family	HiperMAN
4G (2009) **IMT Advanced** (2013)	**3GPP family**	LTE Advanced (E-UTRA) · LTE Advanced Pro (4.5G Pro/pre-5G/4.9G)
	IEEE family	WiMAX (IEEE 802.16m) (WiMax 2.1 (LTE-TDD / TD-LTE) · WiBro)
5G (IMT-2020) (under development)	**3GPP family**	NR · NR-IIoT · LTE-M · NB-IoT
	Other	DECT-5G

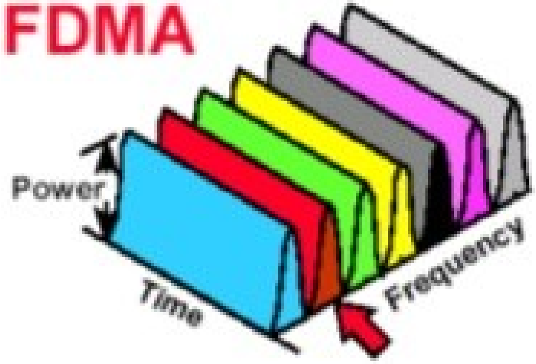
	GSM/ GPRS	WCDMA (UMTS)	HSPA HSDPA / HSUPA	HSPA+	LTE
Max downlink speed bps	10-150 k	384 k	14 M	28 M	100M
Max uplink speed bps	10-150 k	128 k	5.7 M	11 M	50 M
Latency, time approx	600 ms	150 ms	100 ms	50ms (max)	~10 ms
3GPP releases	Rel 97	Rel 99/4	Rel 5 / 6	Rel 7	Rel 8
Approx years of initial roll out	1991	2003 / 4	2005 / 6 HSDPA 2007 / 8 HSUPA	2008 / 9	2009 / 10
Access methodology	TDMA/ FDMA	WCDMA	WCDMA	WCDMA	OFDMA / SC-FDMA
Bandwidth	200 KHz	5 MHz	5 MHz	5 MHz	1.4 ~20MHz
Modulation types supported	GMSK, 8-PSK	QPSK	QPSK, 16-QAM	QPSK, 16-QAM	QPSK, 16QAM, 64QAM
Mobile/UE output power (dBm)	30~33	21	21	21	23

bytebeats.com


TDMA
FDMA
CDMA
OFDMA
Frequency
Time
www.explainthatstuff.com

Wireless Multiple Access Methods

FDMA



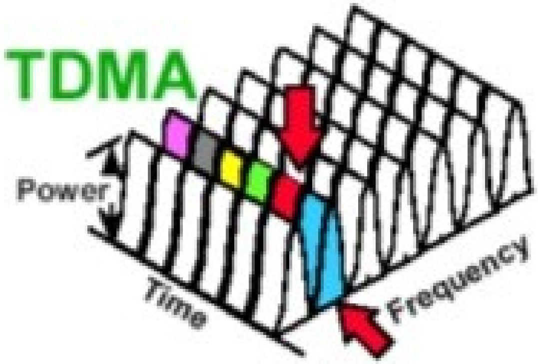
Frequency Division Multiple Access

•A user's channel is a private frequency

Time Division Multiple Access

•A user's channel is a specific frequency, but it only belongs to the user during certain time slots in a repeating sequence

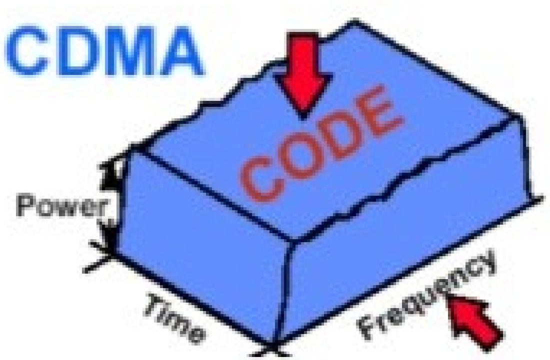
TDMA

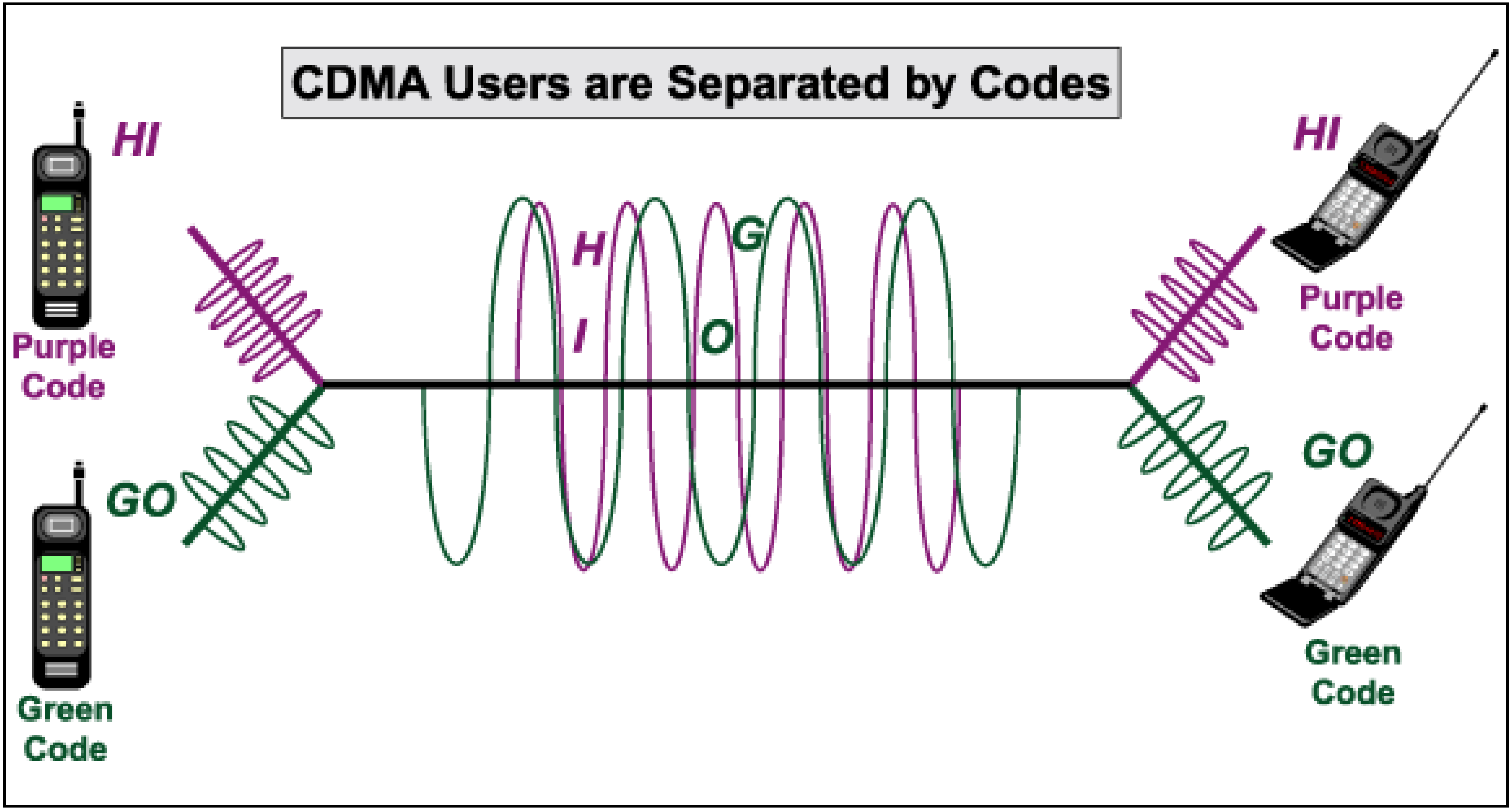


Code Division Multiple Access

•Each user's signal is a continuous unique code pattern buried within a shared signal, mingled with other users' code patterns. If a user's code pattern is known, the presence or absence of their signal can be detected, thus conveying information.

CDMA



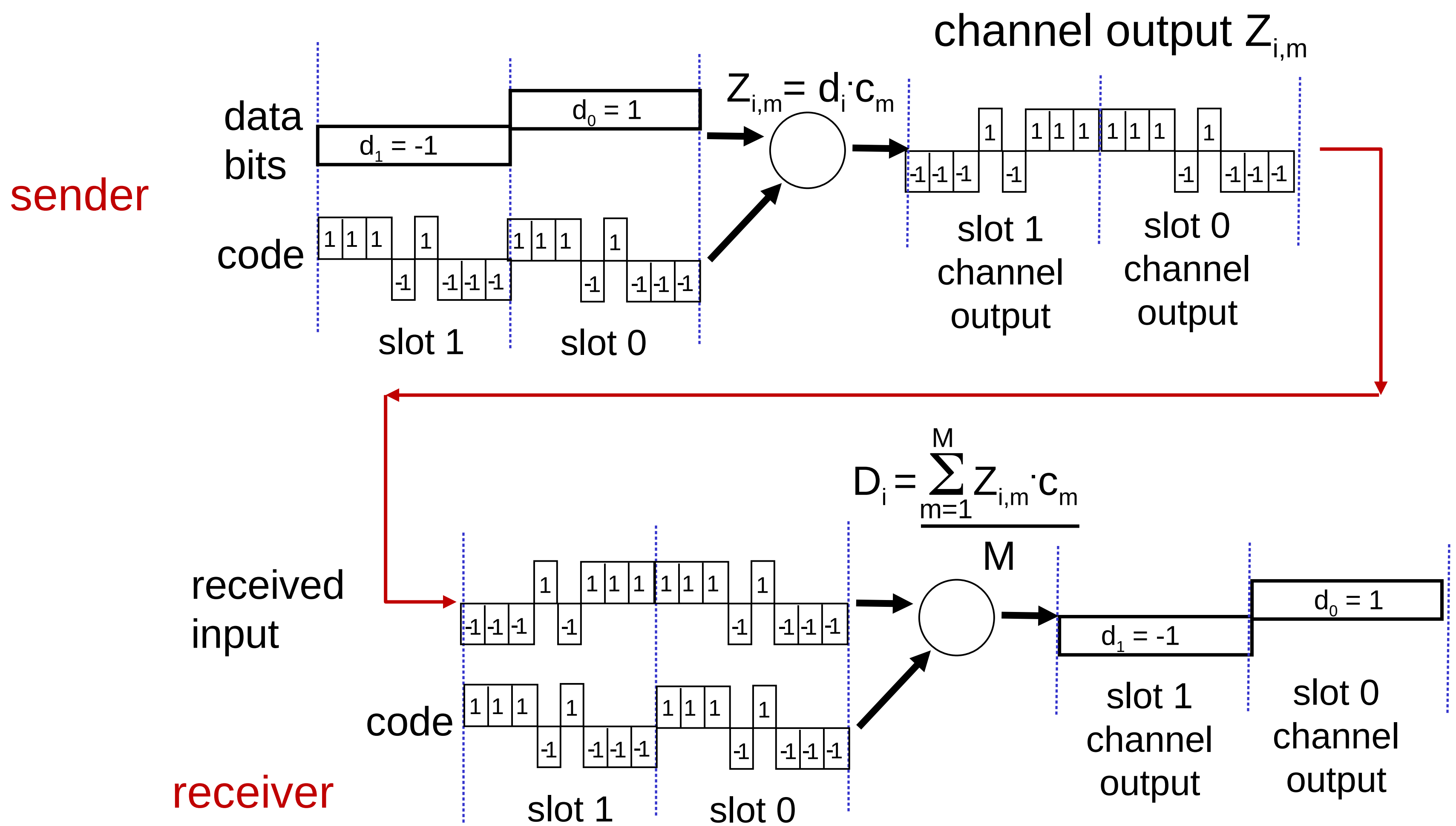


CDMA Users are Separated by Codes
HI
Purple Code
GO
Green Code
H
I
G
O
HI
Purple Code
GO
Green Code

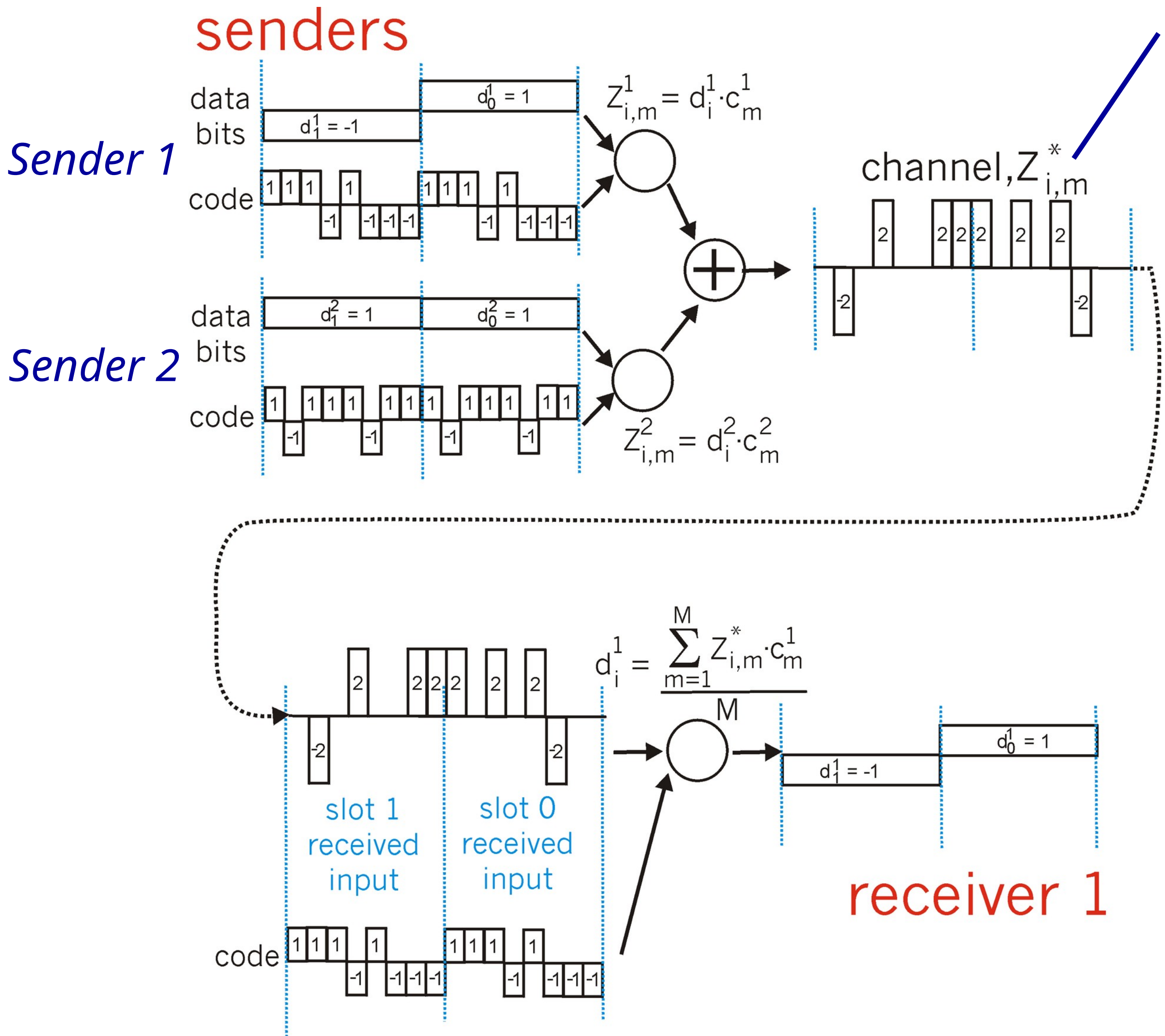
Code Division Multiple Access (CDMA)

- unique "code" assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
  - allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence

CDMA encode/decode



CDMA: two-sender interference



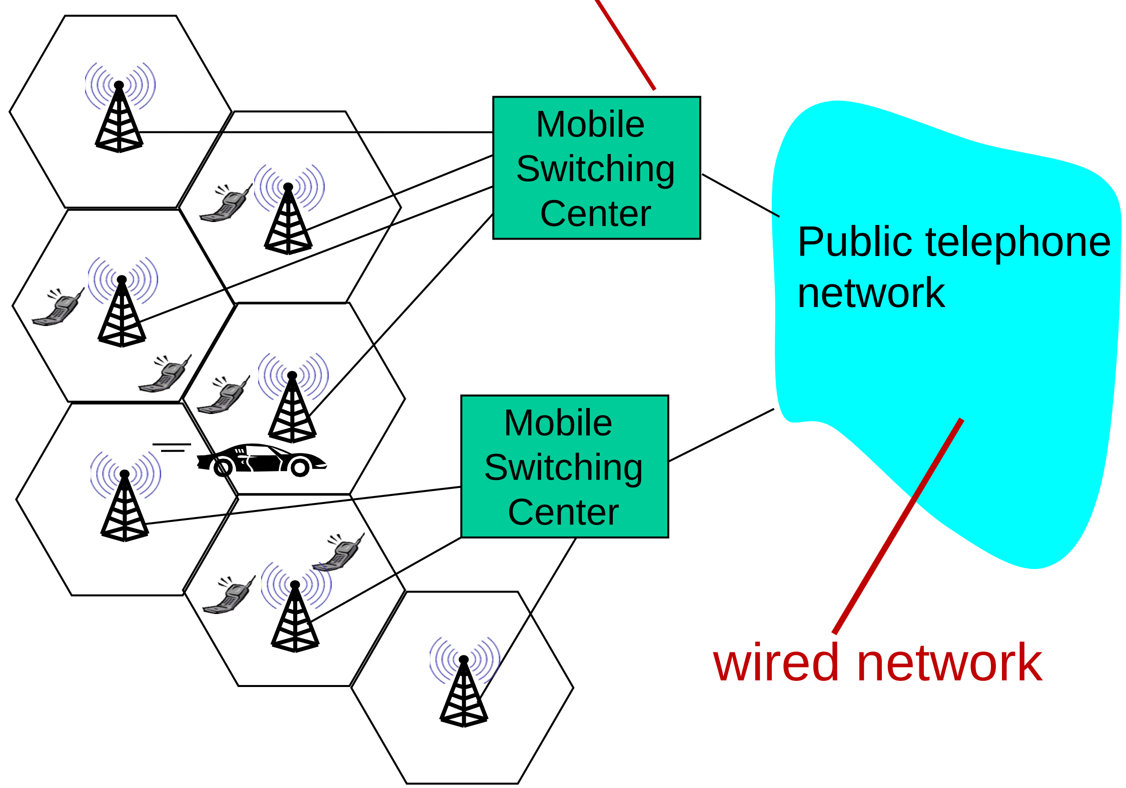
channel sums together transmissions by sender 1 and 2

using same code as sender 1, receiver recovers sender 1's original data from summed channel data!

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

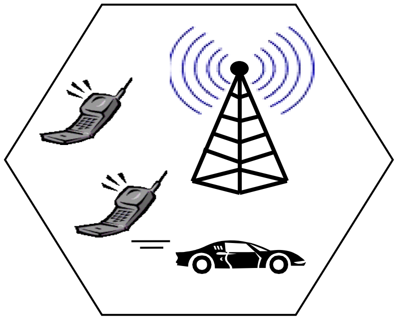
MSC
- connects cells to wired tel. net.
- manages call setup (more later!)
- handles mobility (more later!)

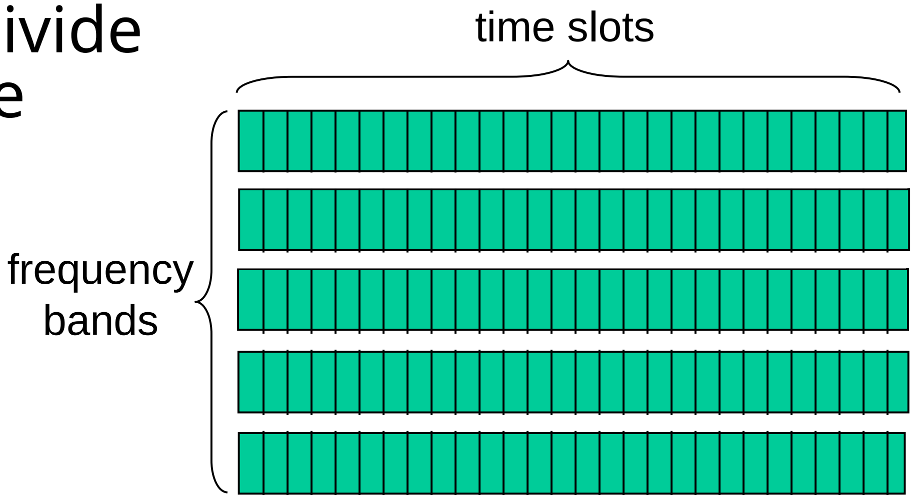


Cellular networks: the first hop

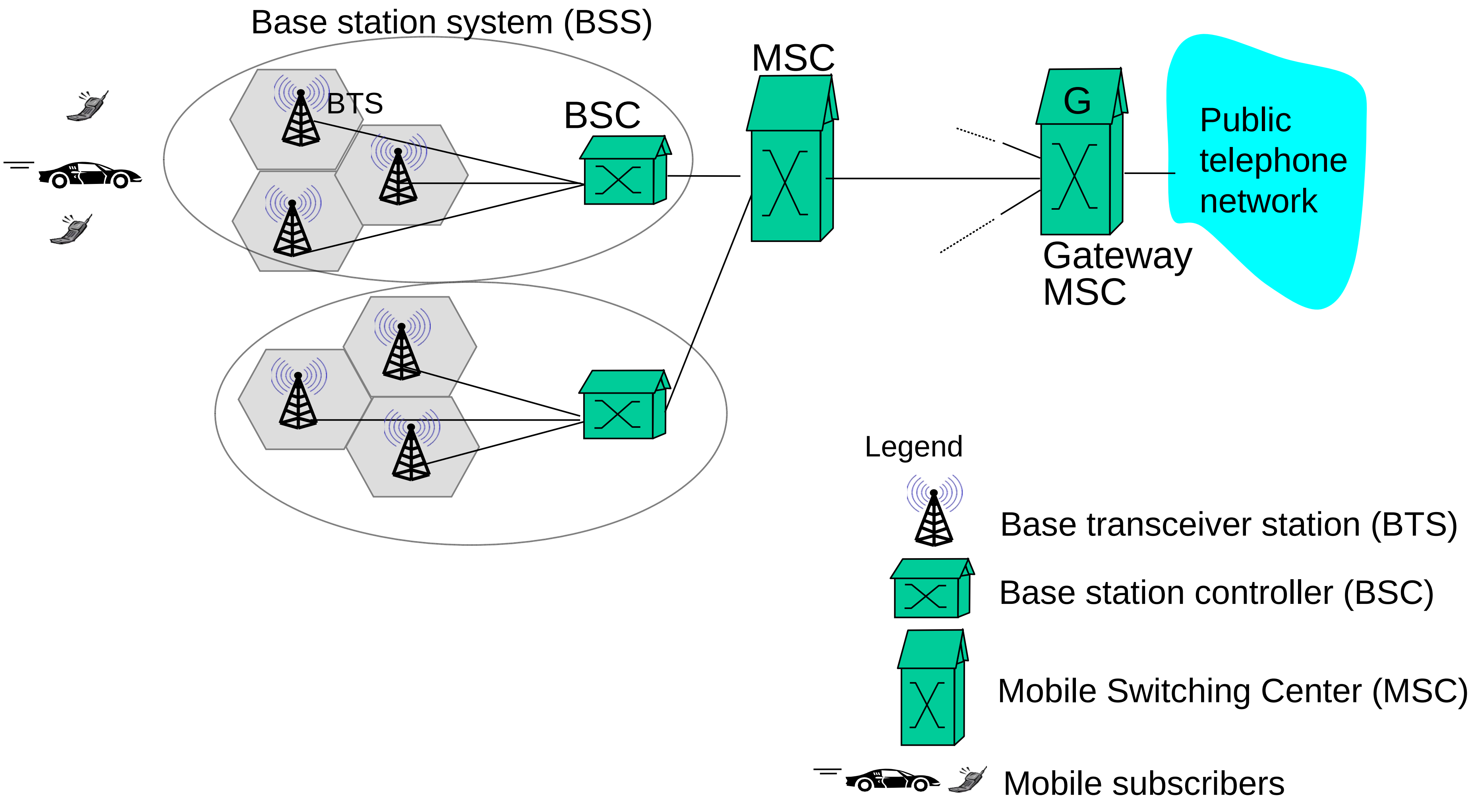
Two techniques for sharing mobile-to-BS radio spectrum

- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access

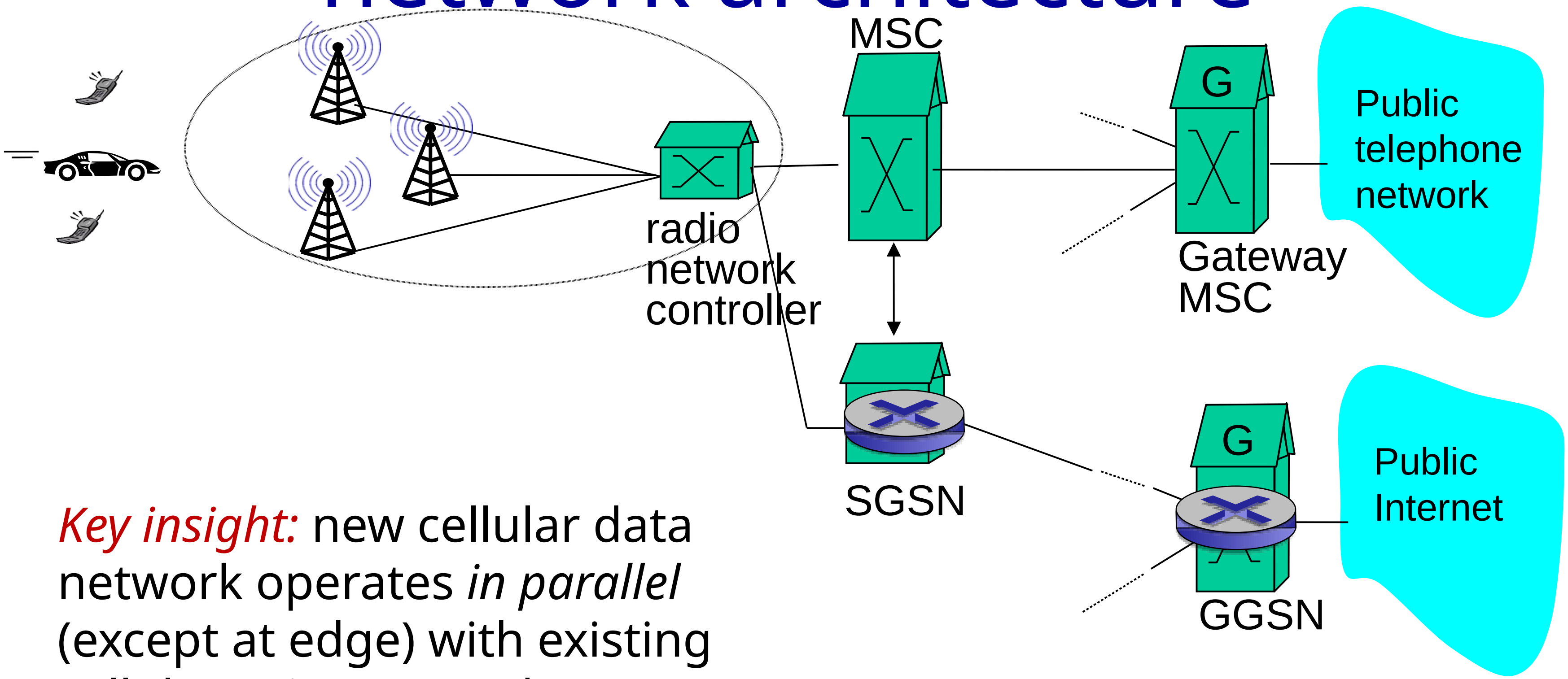




2G (voice) network architecture

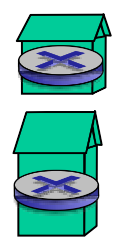


3G (voice+data) network architecture

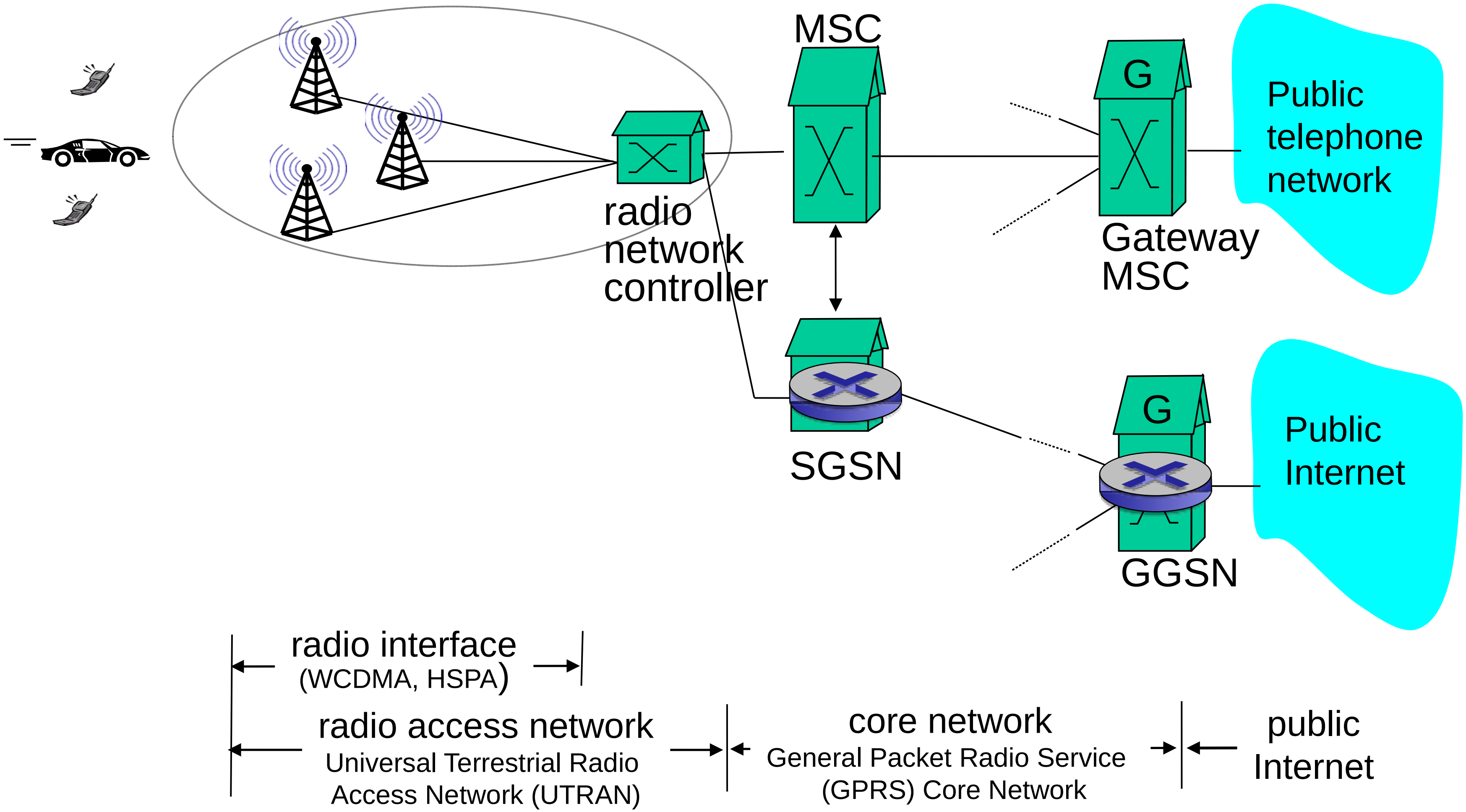


Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

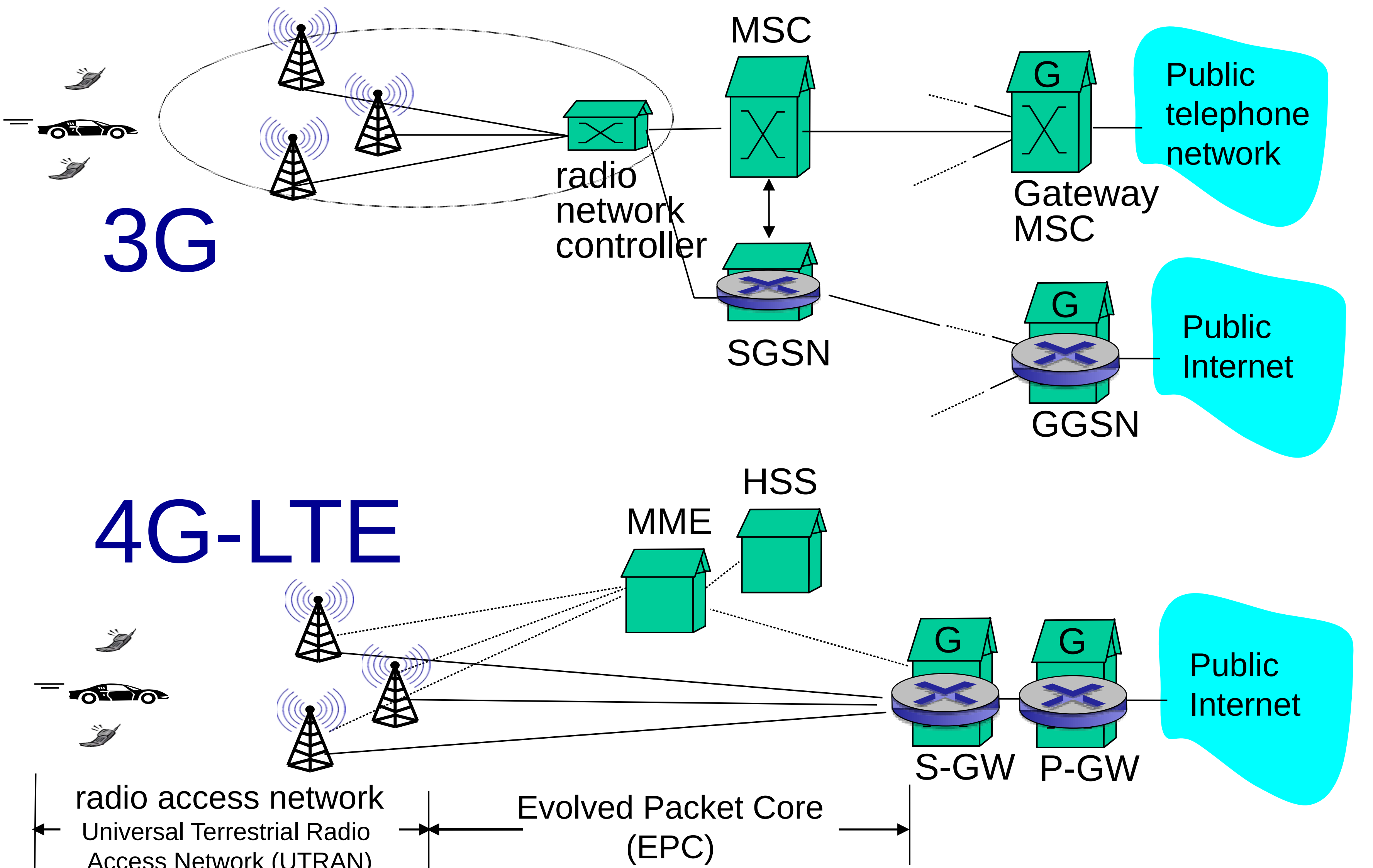
- voice network *unchanged* in core
- data network operates in parallel



3G (voice+data) network architecture

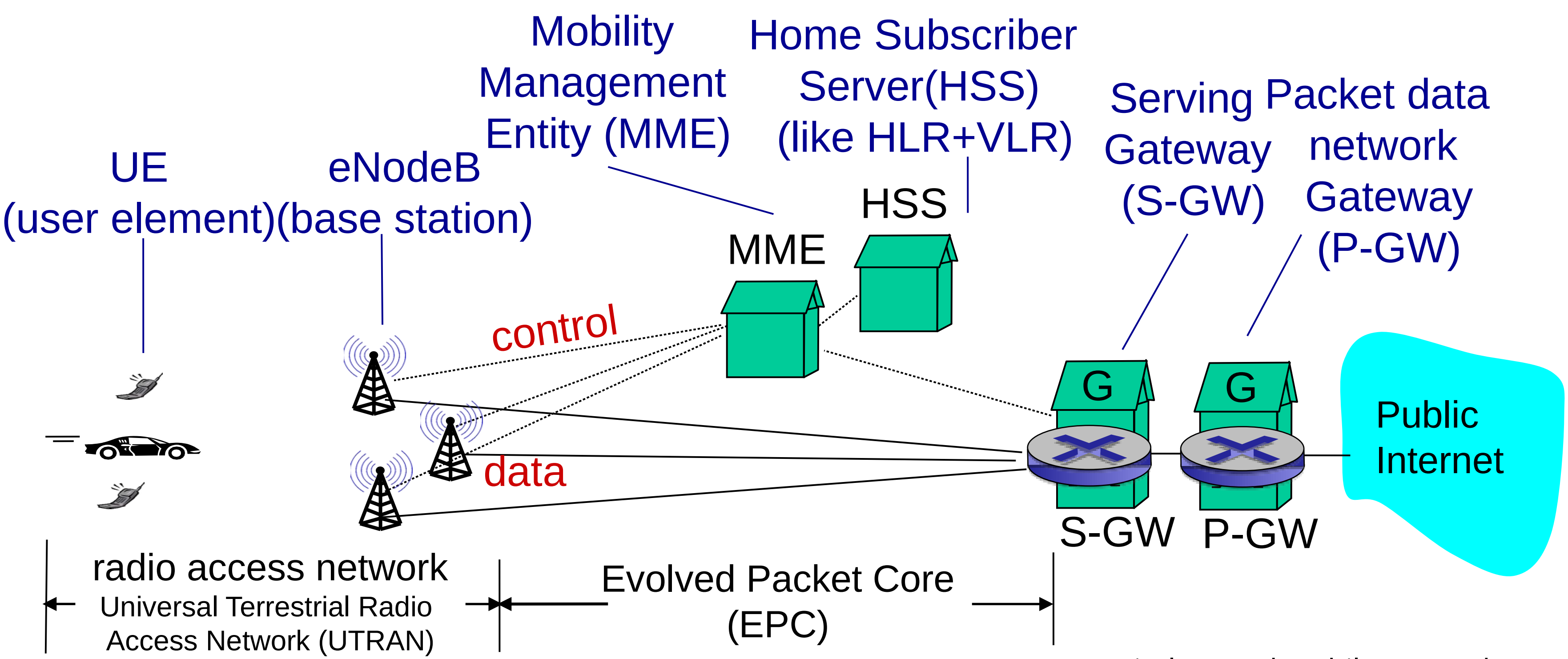


3G versus 4G LTE network architecture



4G: differences from 3G

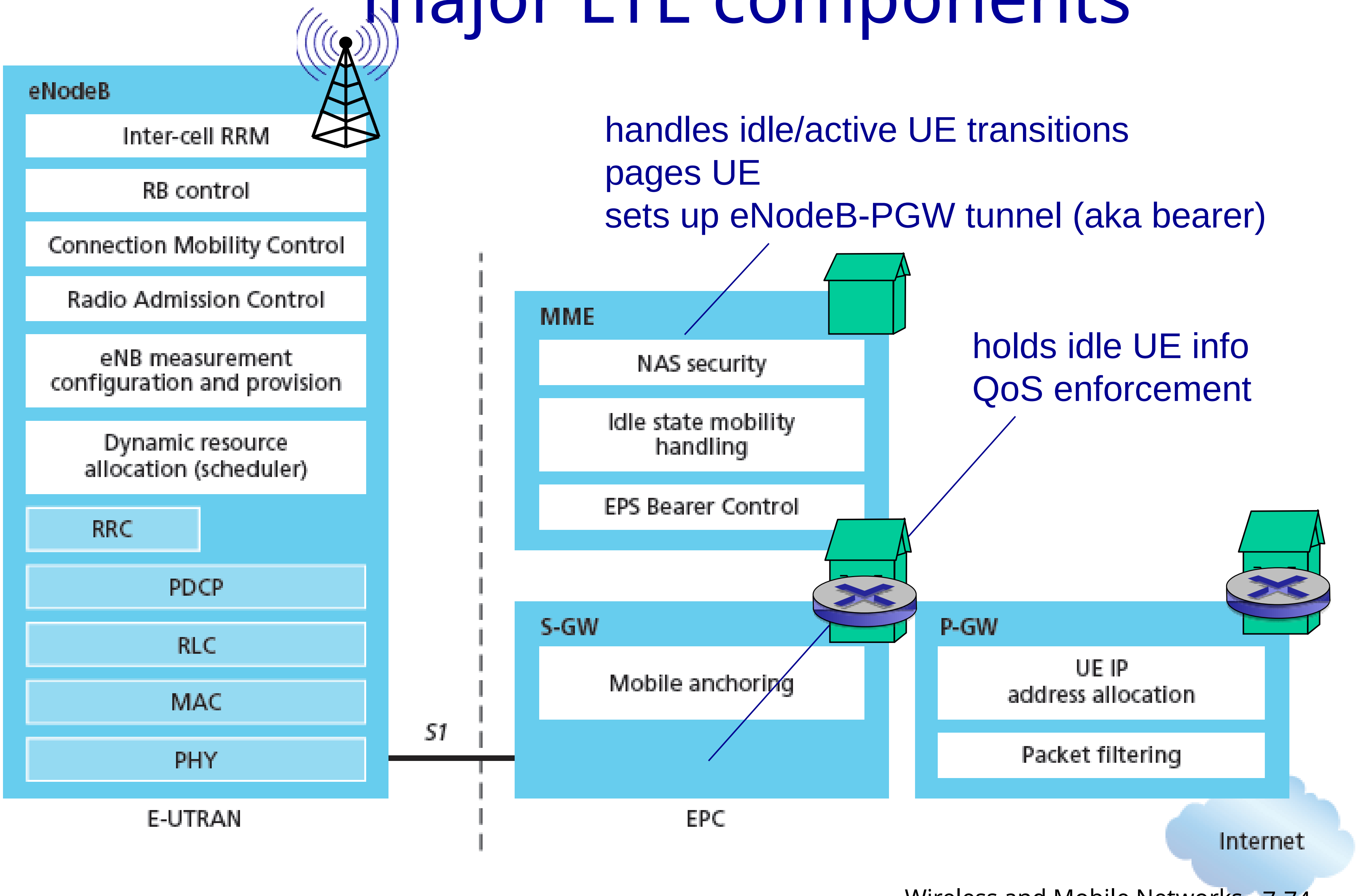
- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway



Functional split of major LTE components

handles idle/active UE transitions
pages UE
sets up eNodeB-PGW tunnel (aka bearer)

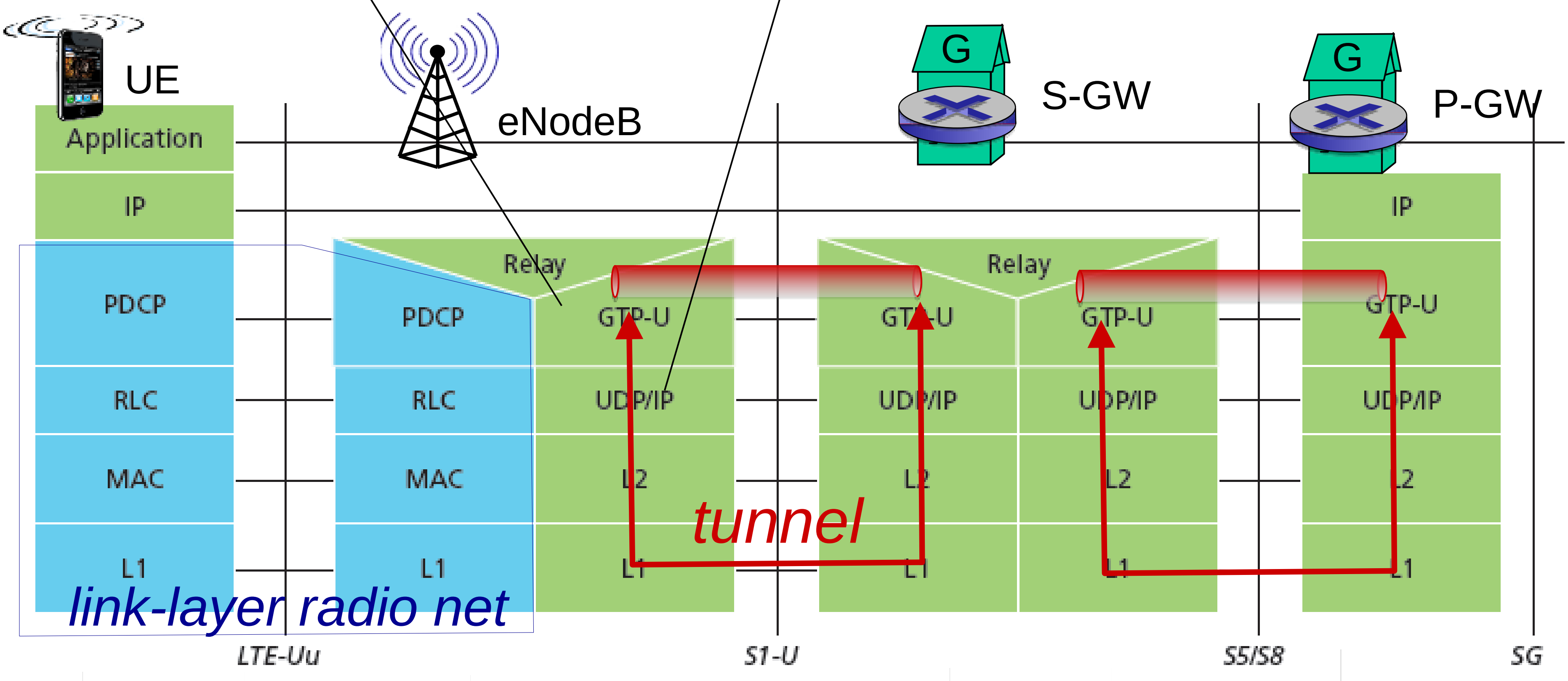
holds idle UE info
QoS enforcement



Radio+Tunneling: UE – eNodeB – PGW

IP packet from UE encapsulated in GPRS Tunneling Protocol (GTP) message at ENodeB

GTP message encapsulated in UDP, then encapsulated in IP. large IP packet addressed to SGW



Quality of Service in LTE

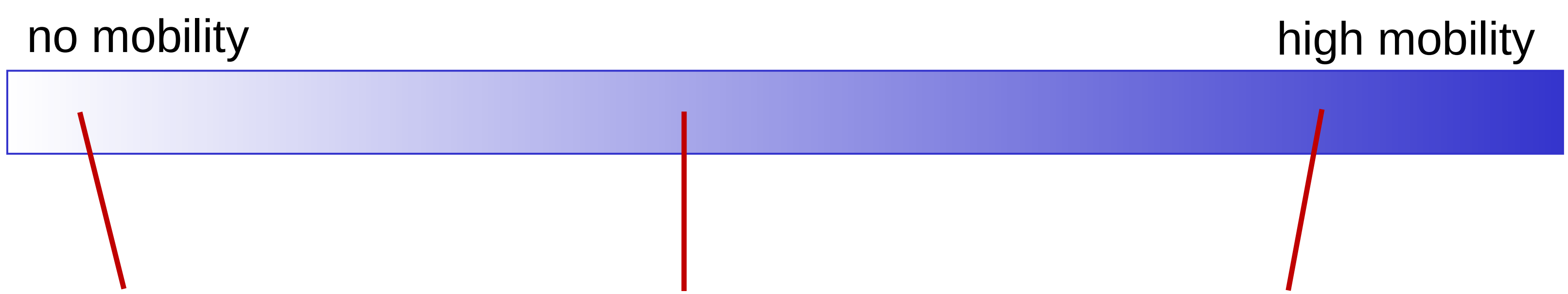
- QoS from eNodeB to SGW: min and max guaranteed bit rate
- QoS in radio access network: one of 12 QCI values

QCI	RESOURCE TYPE	PRIORITY	PACKET DELAY BUDGET (MS)	PACKET ERROR LOSS RATE	EXAMPLE SERVICES
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real-time gaming
5	Non-GBR	1	100	10^{-6}	IMS signaling
6	Non-GBR	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (for example, WWW, e-mail), chat, FTP, p2p file sharing, progressive video and others
9	Non-GBR	9	300	10^{-6}	

Chapter 7 outline

What is mobility?

- spectrum of mobility, from the *network* perspective:



mobile wireless user, using same access point

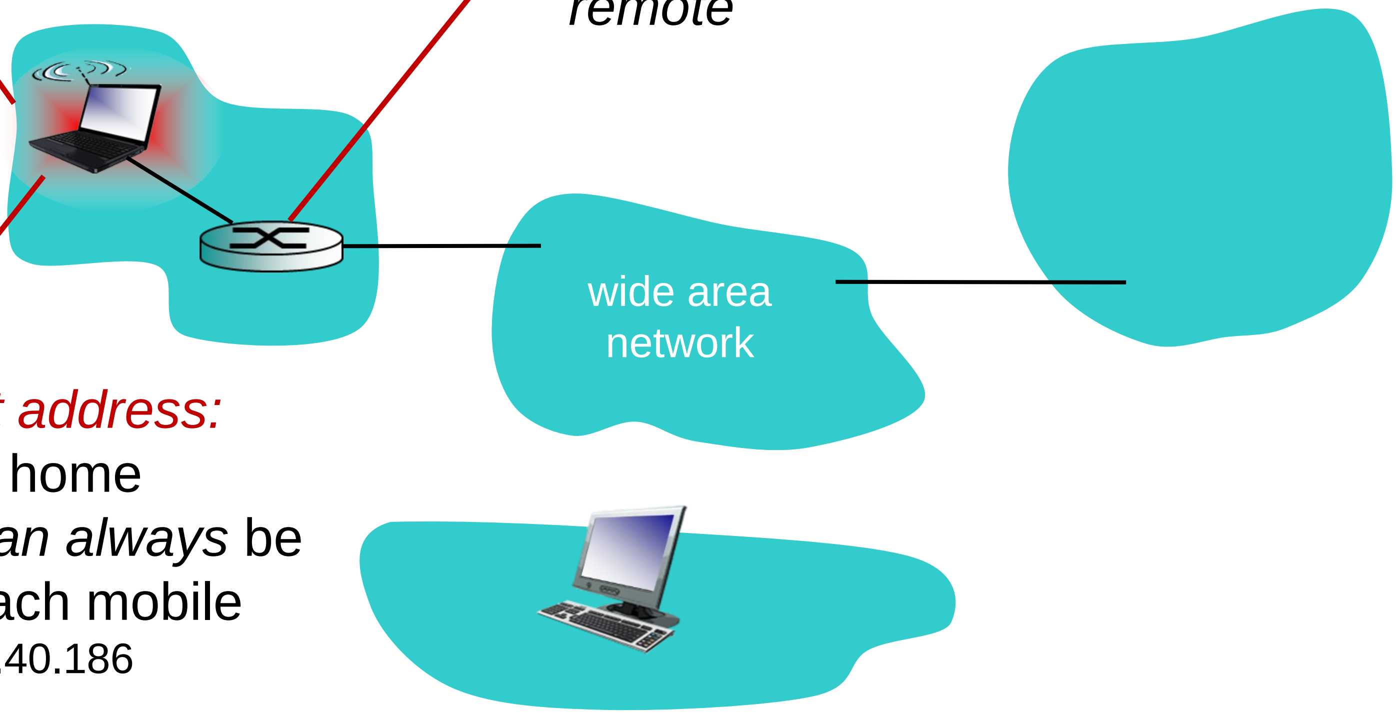
mobile user, connecting/ disconnecting from network using DHCP.

mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)

Mobility: vocabulary

home network: permanent "home" of mobile
(e.g., 128.119.40/24)

home agent: entity that will perform mobility functions on behalf of mobile, when mobile is remote



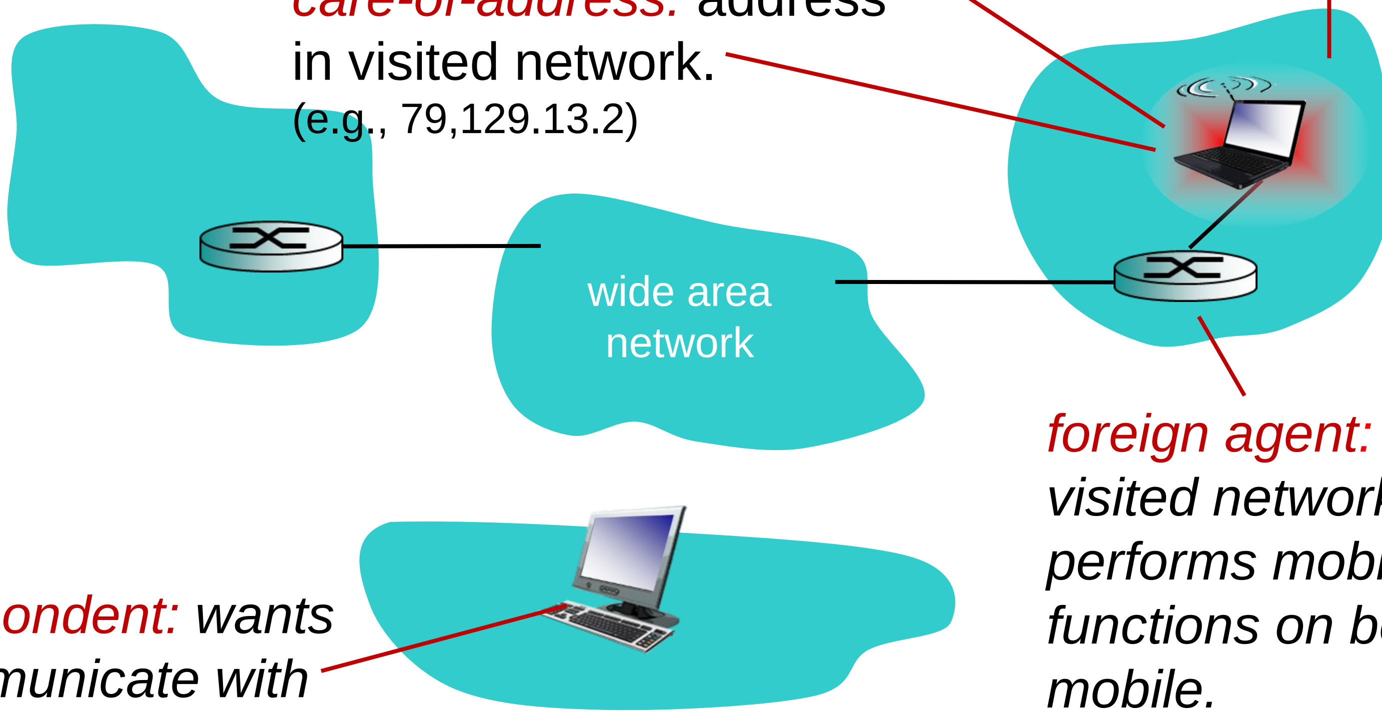
permanent address: address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: more vocabulary

permanent address: remains constant (e.g., 128.119.40.186)

visited network: network in which mobile currently resides (e.g., 79.129.13/24)

care-of-address: address in visited network. (e.g., 79,129.13.2)



foreign agent: entity in visited network that performs mobility functions on behalf of mobile.

correspondent: wants to communicate with mobile

How do *you* contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents (isp)?
- expect her to let you know where he/she is?

Mobility: approaches

- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

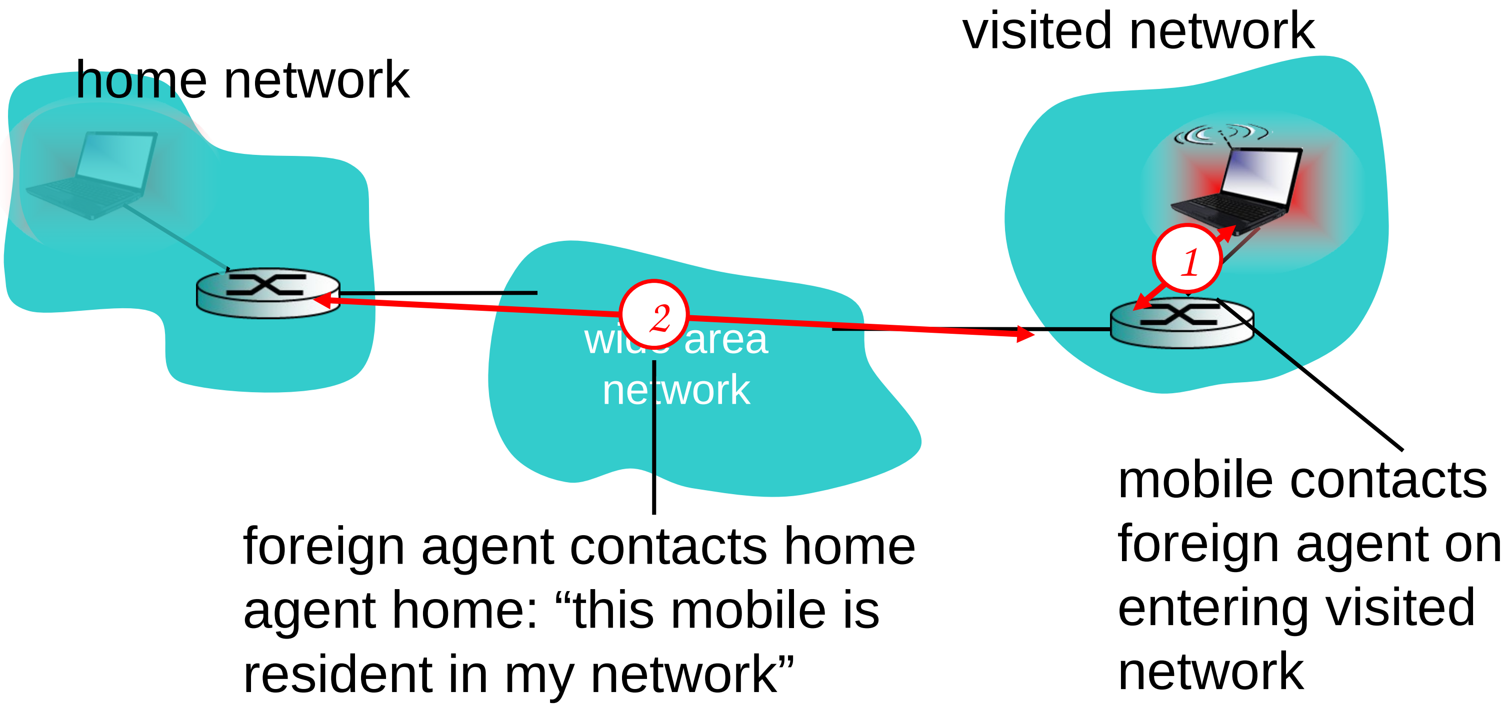
Mobility: approaches

- *let routing handle it:* routers advertise permanent ad[...] mobile-nodes-in-residence via [...]ng table exchange.
  - routing tab[...] where each mobile located
  - no changes to end-systems

not
scalable
to millions of
mobiles

- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

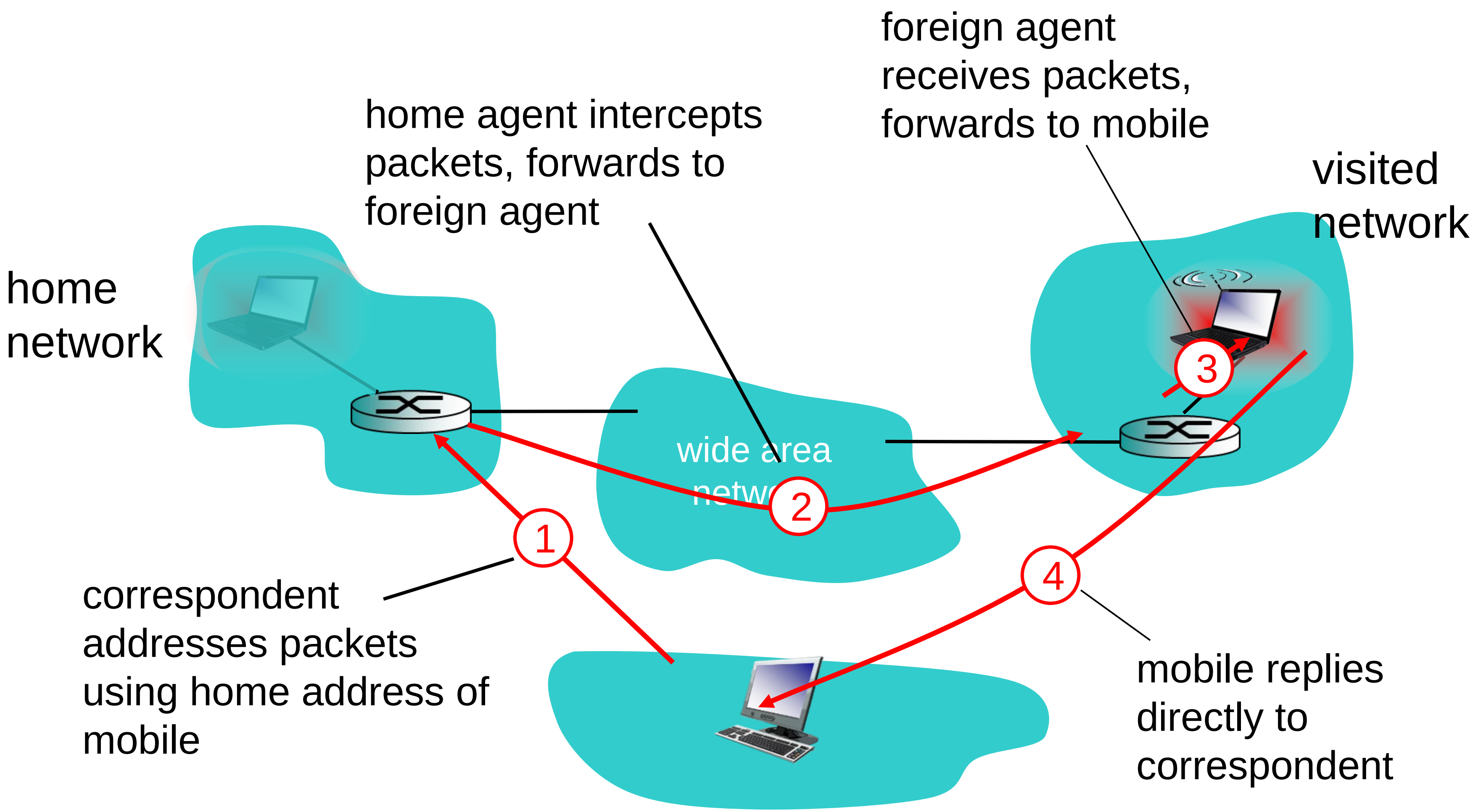
Mobility: registration



end result:

- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via indirect routing



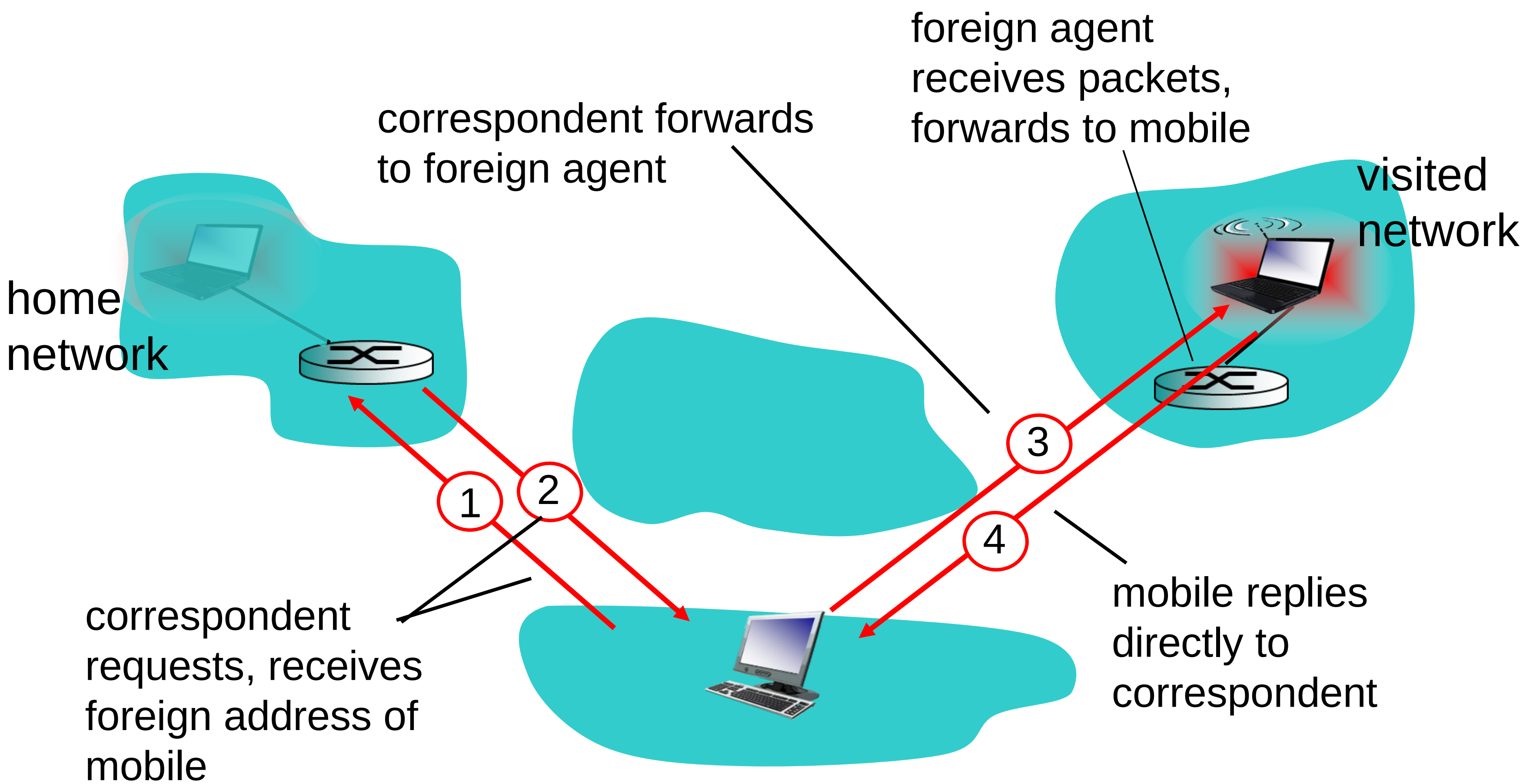
Indirect Routing: comments

- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network

Indirect routing: moving between networks

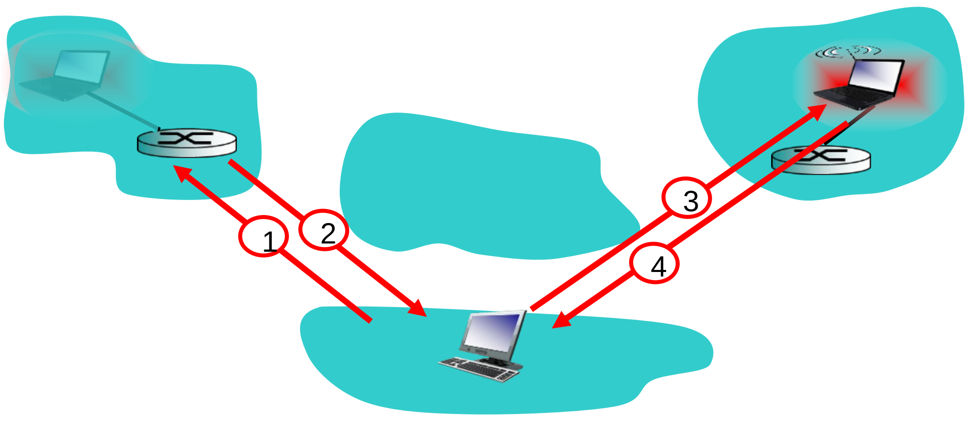
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

Mobility via direct routing



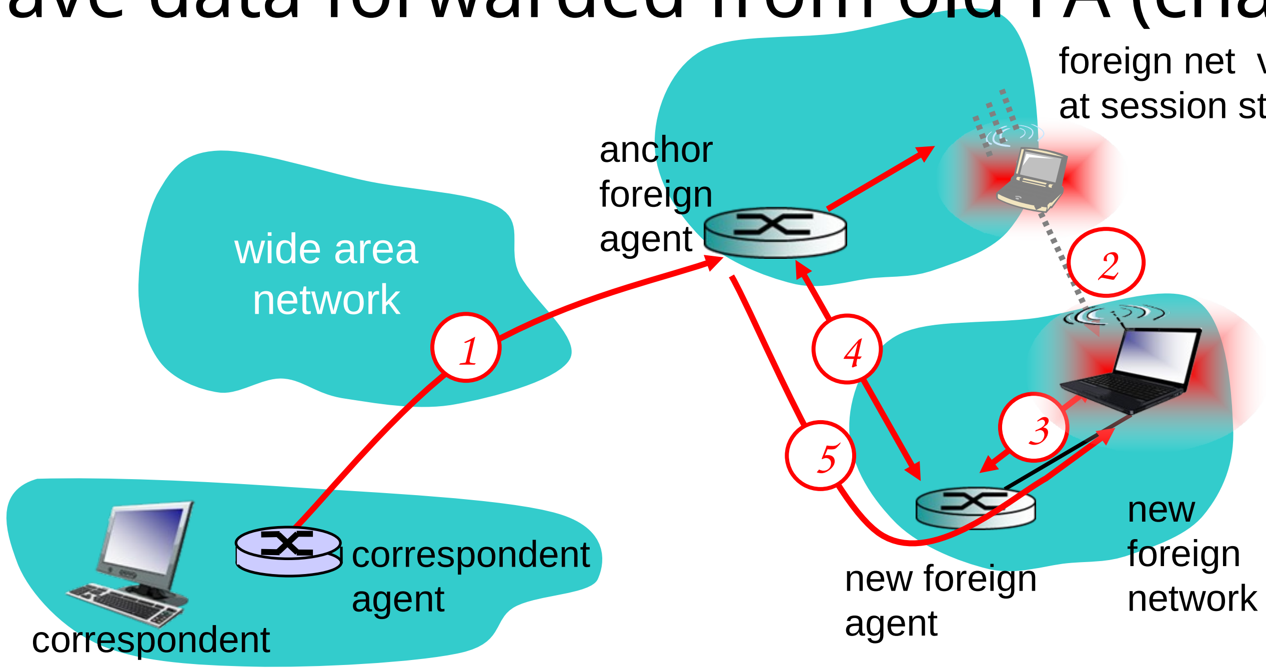
Mobility via direct routing: comments

- overcome triangle routing problem
- *non-transparent to correspondent:* correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Chapter 7 outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

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

7.4 Cellular Internet Access
- architecture
- standards (e.g., 3G, LTE)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

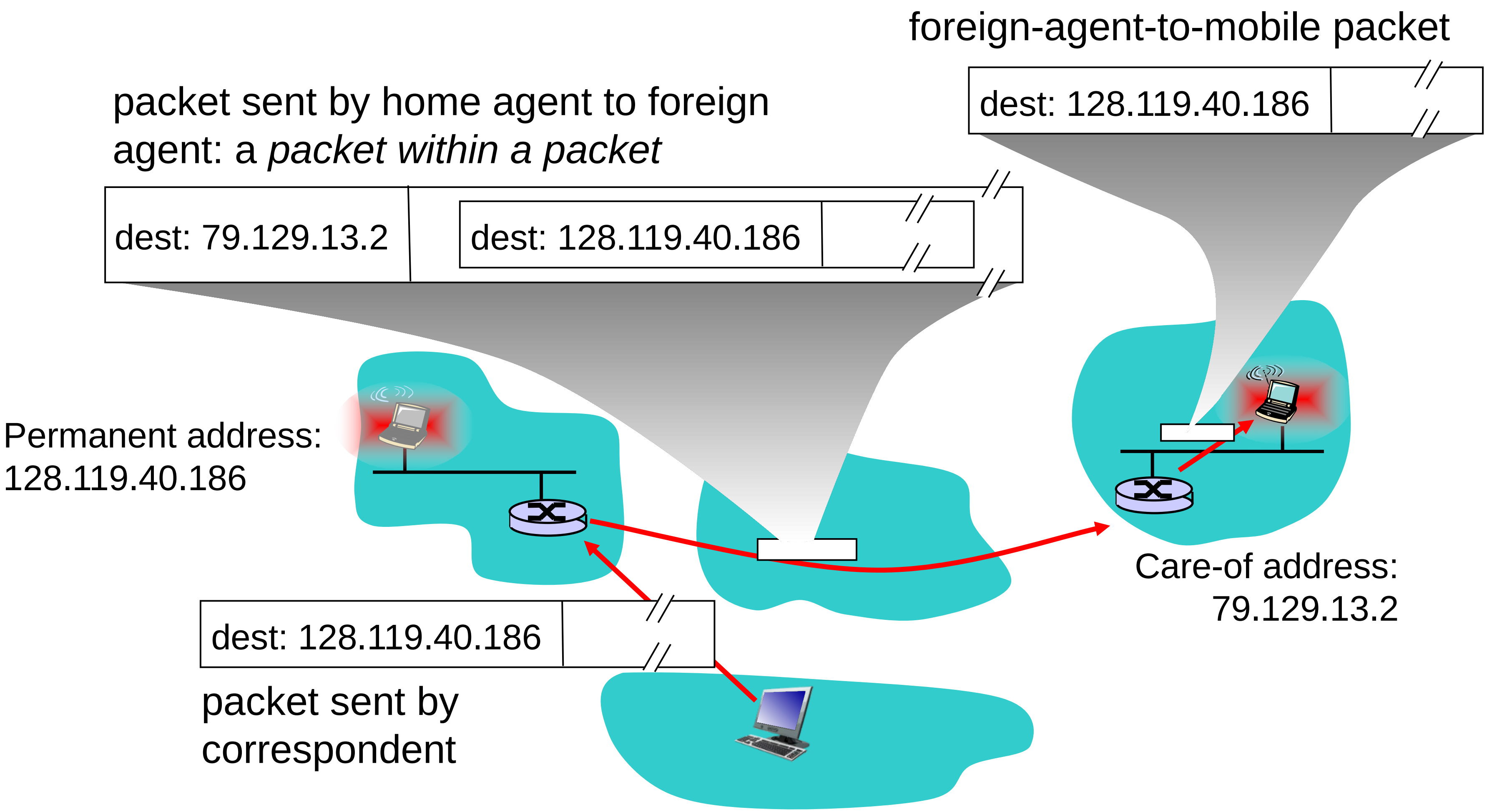
7.7 Handling mobility in cellular networks

7.8 Mobility and higher-layer protocols

Mobile IP

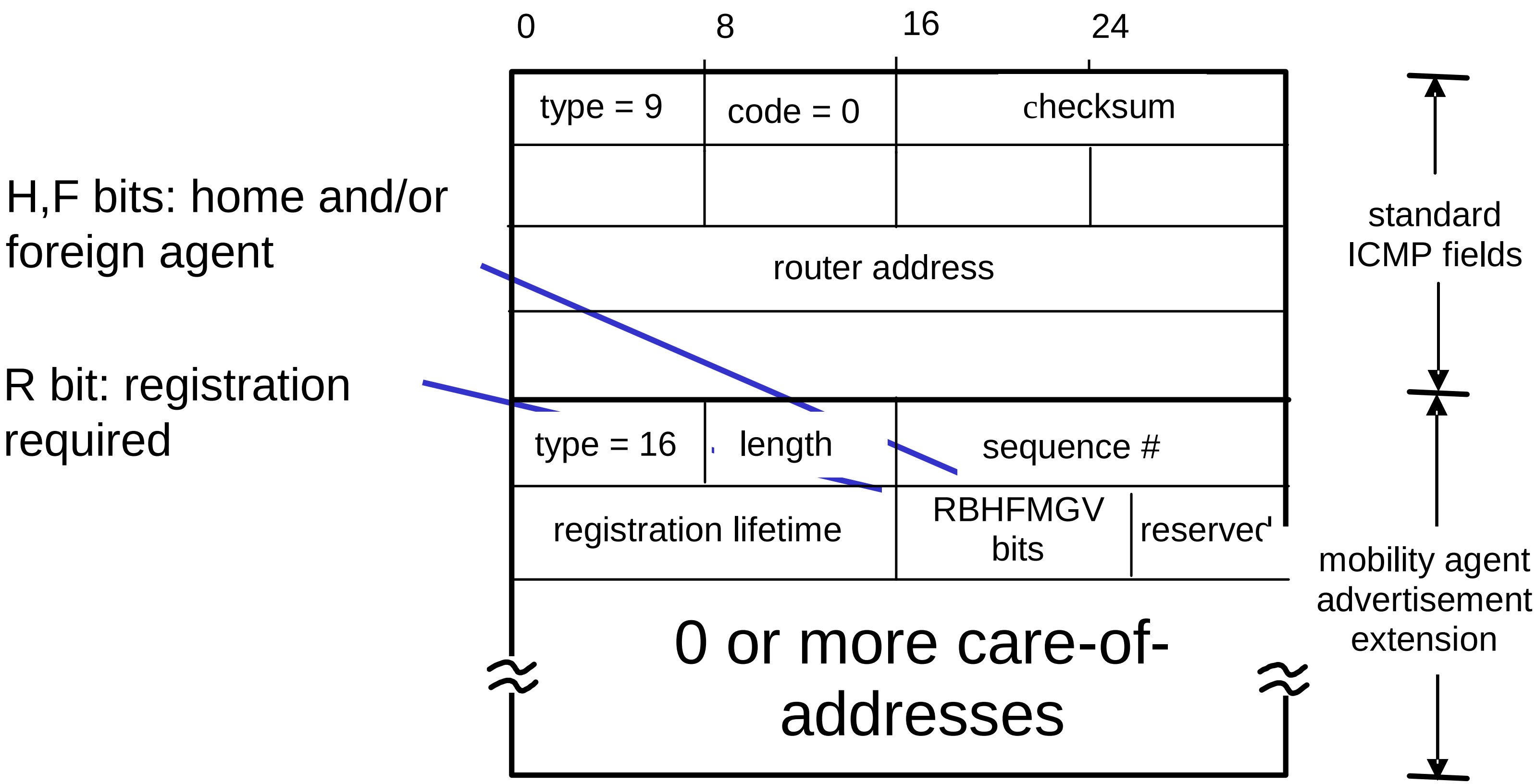
- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: indirect routing

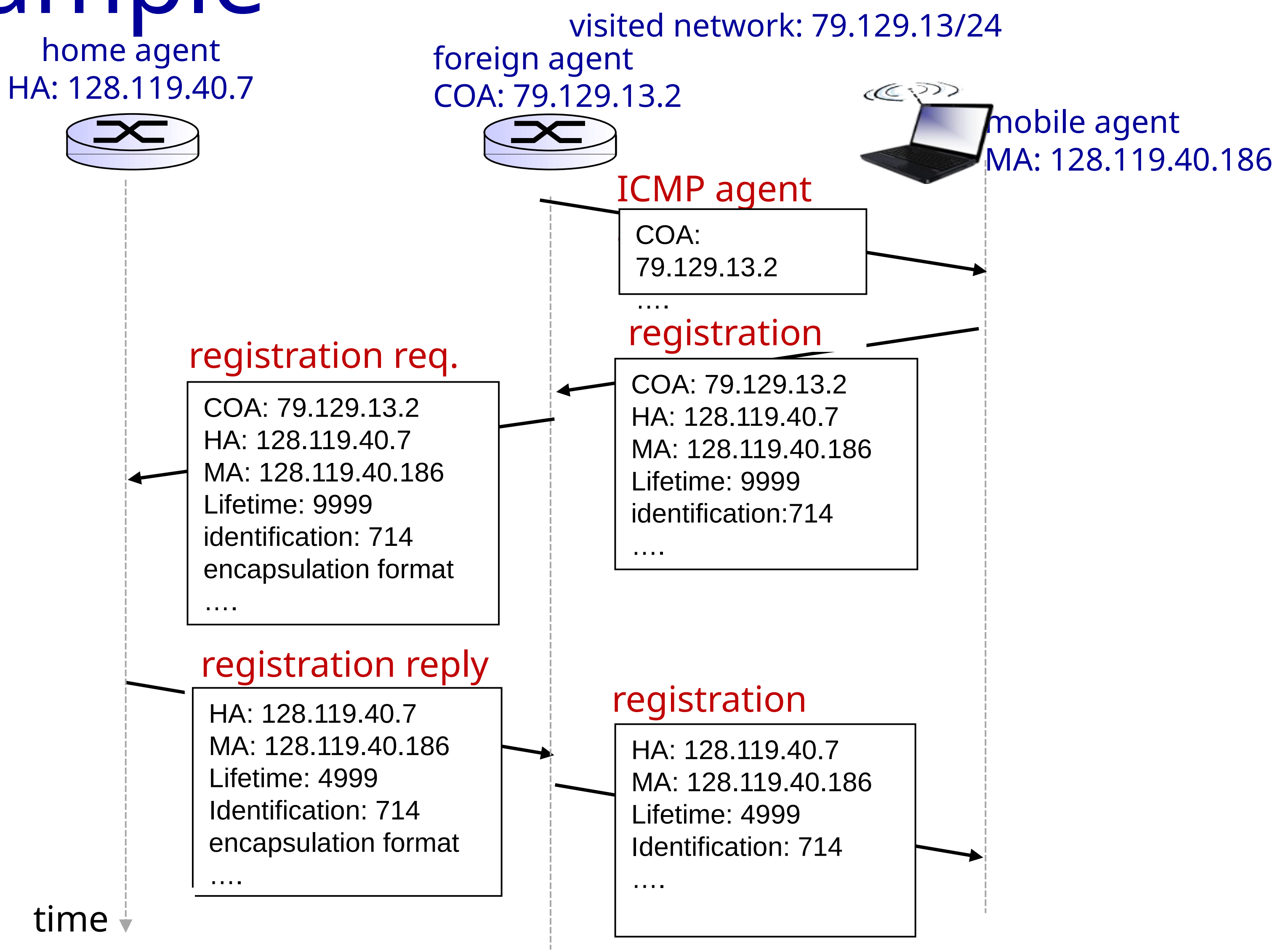


Mobile IP: agent discovery

- *agent advertisement:* foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

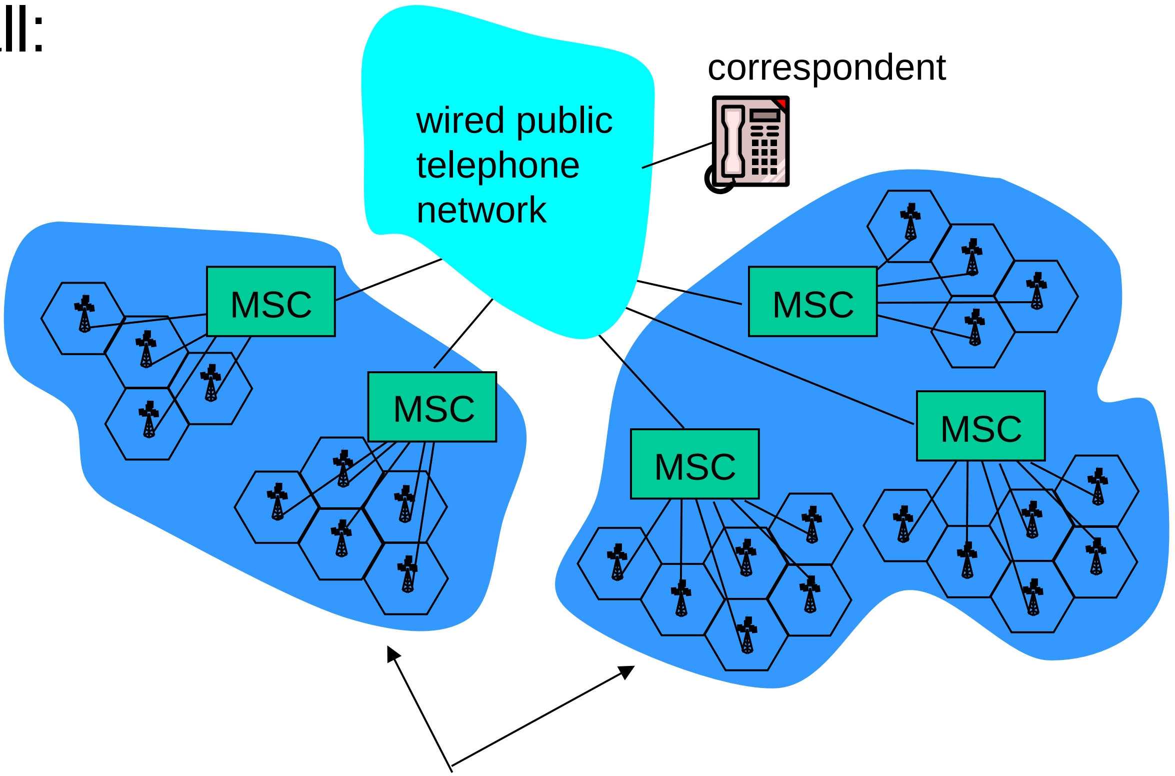


Mobile IP: registration example



Components of cellular network architecture

recall:

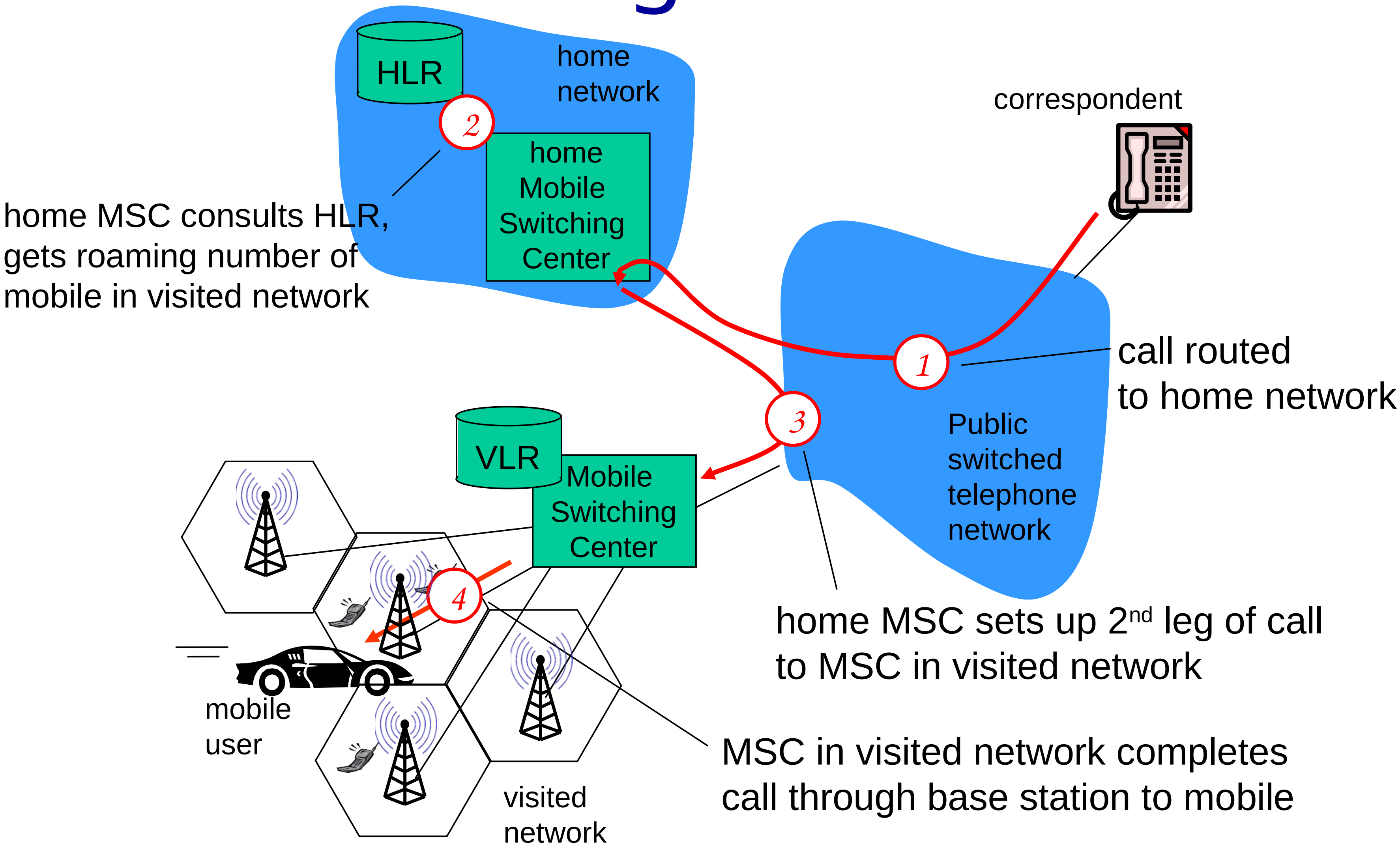


different cellular networks,
operated by different providers

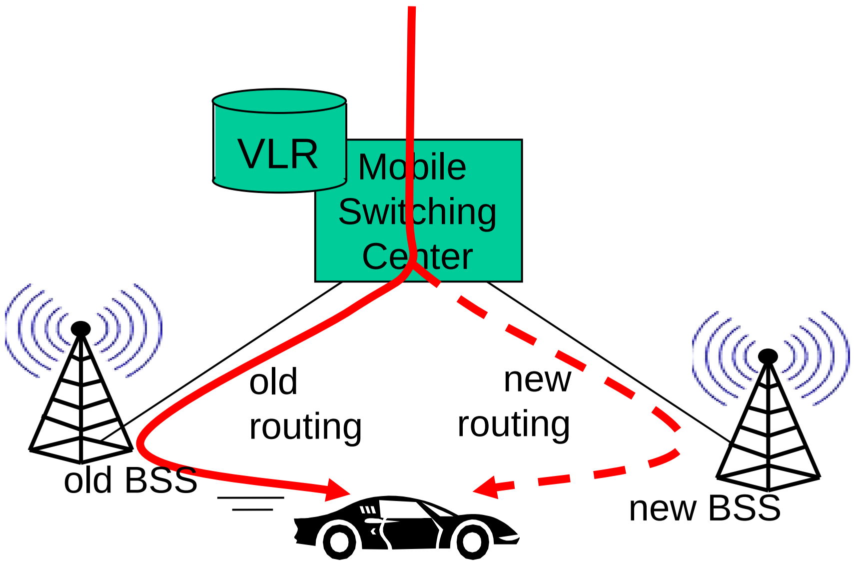
Handling mobility in cellular networks

- *home network*: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- *visited network:* network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network
  - could be home network

GSM: indirect routing to mobile

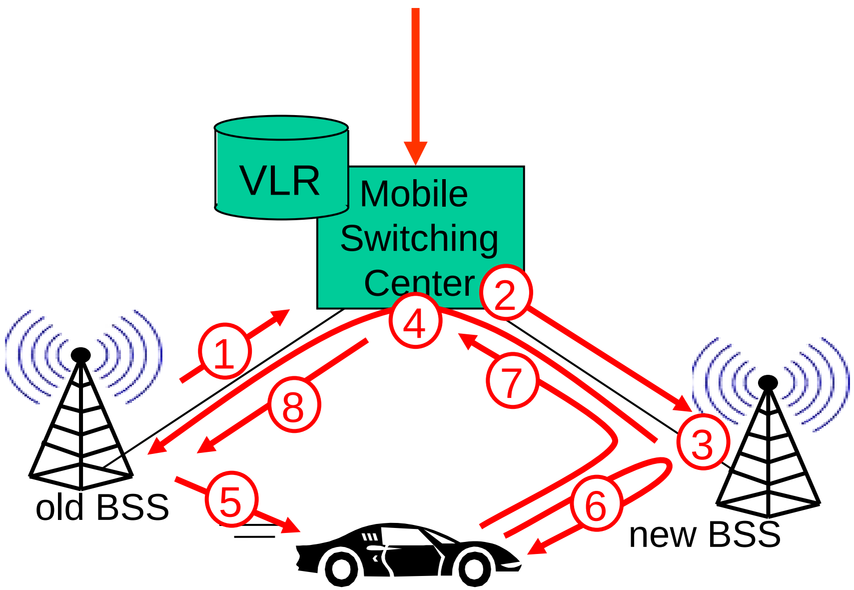


GSM: handoff with common MSC



- *handoff goal:* route call via new base station (without interruption)
- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

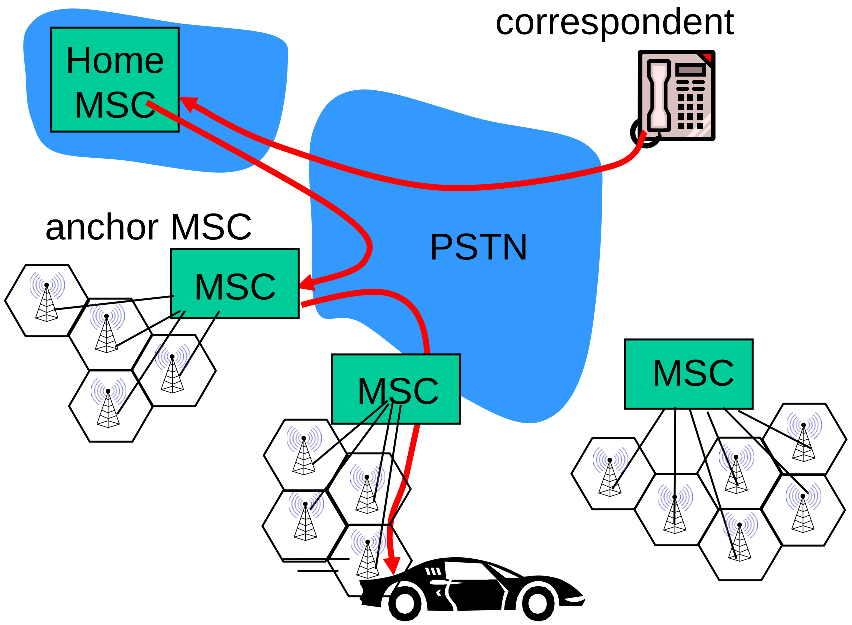
GSM: handoff with common MSC



1. old BSS informs MSC of impending handoff, provides list of 1⁺ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

8 MSC-old-BSS resources released

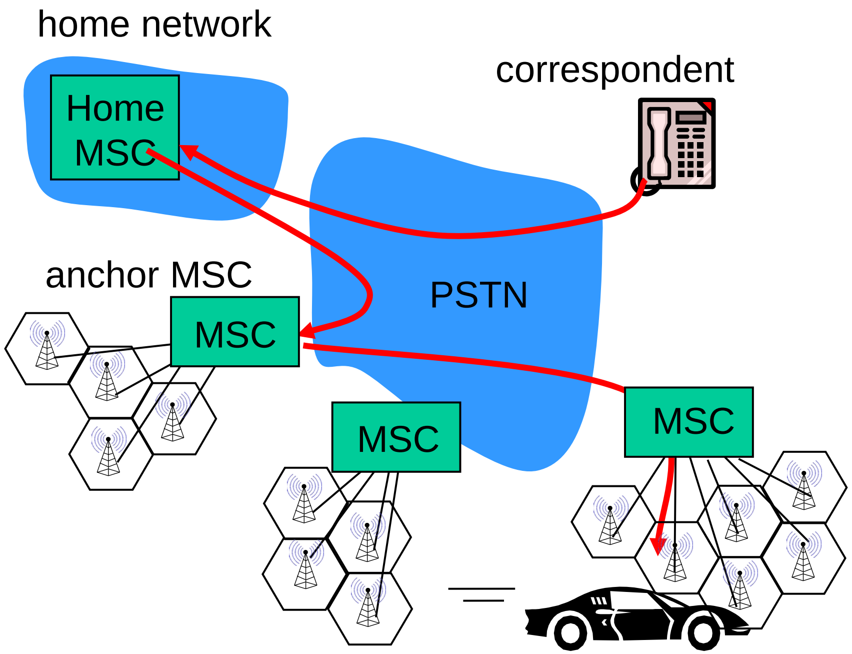
GSM: handoff between MSCs



(a) before handoff

- *anchor MSC:* first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

GSM: handoff between MSCs

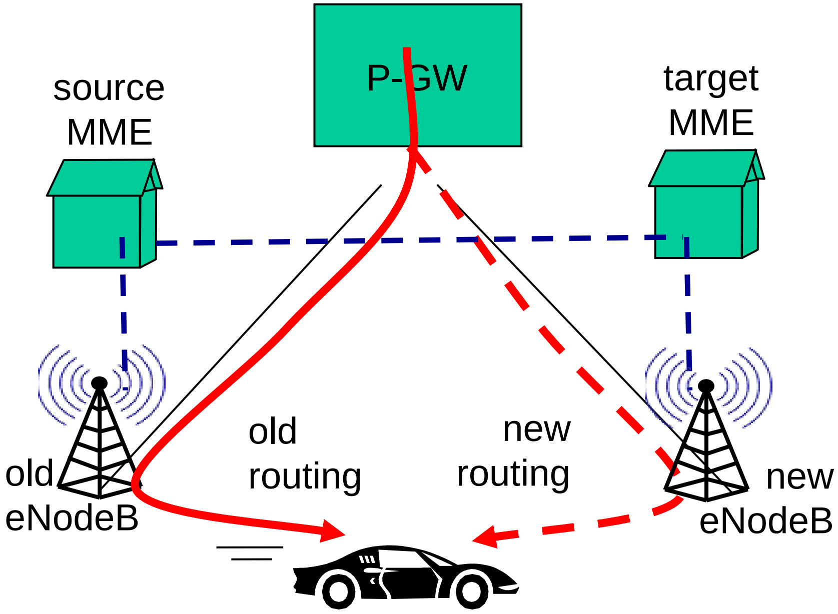


(b) after handoff

- *anchor MSC:* first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

Handling Mobility in LTE

- Paging: idle UE may move from cell to cell: network does not know where the idle UE is resident
  - paging message from MME broadcast by all eNodeB to locate UE
- handoff: similar to 3G:
  - preparation phase
  - execution phase
  - completion phase



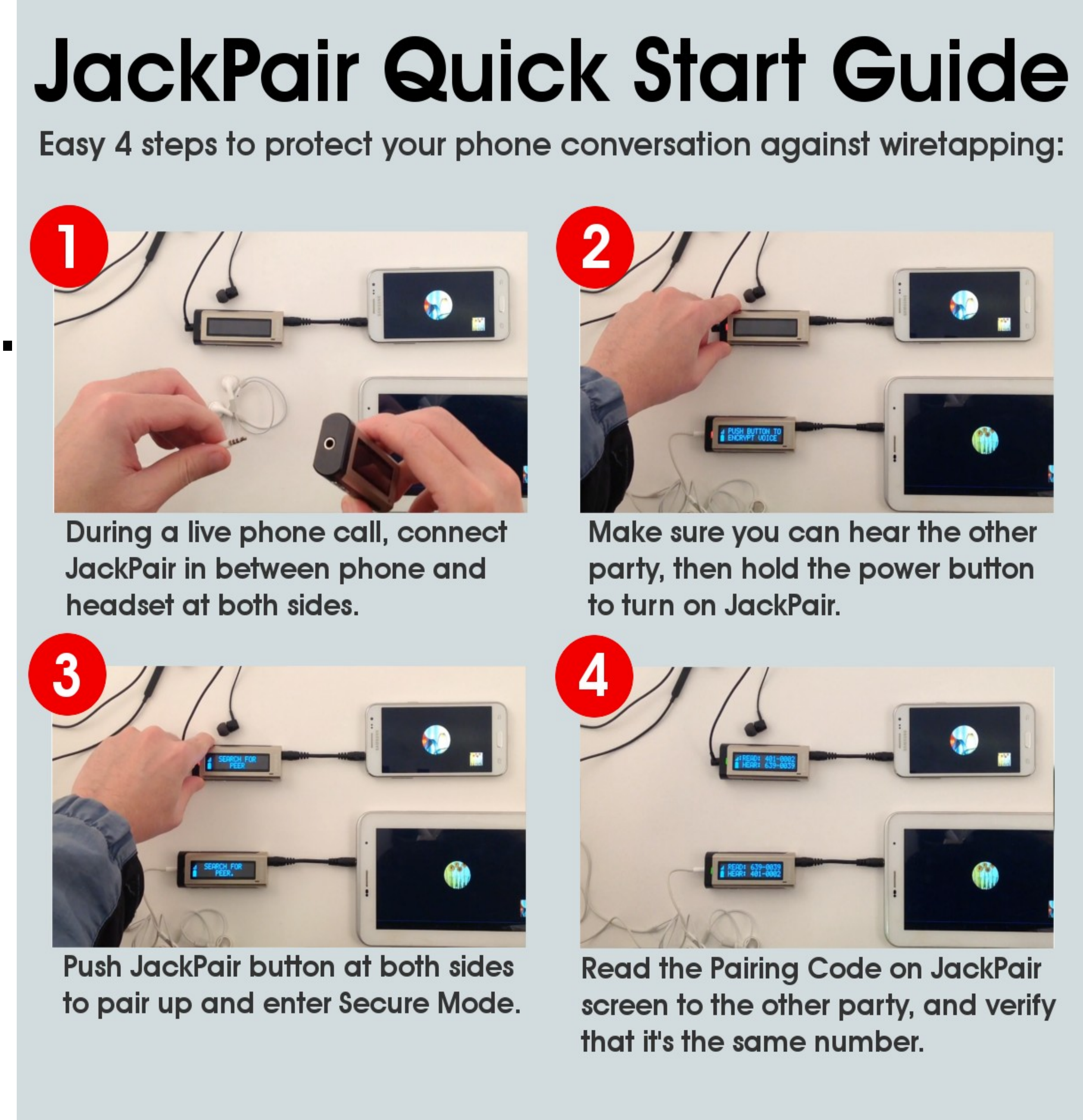
Mobility: cellular versus Mobile IP

cellular element	Comment on cellular element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

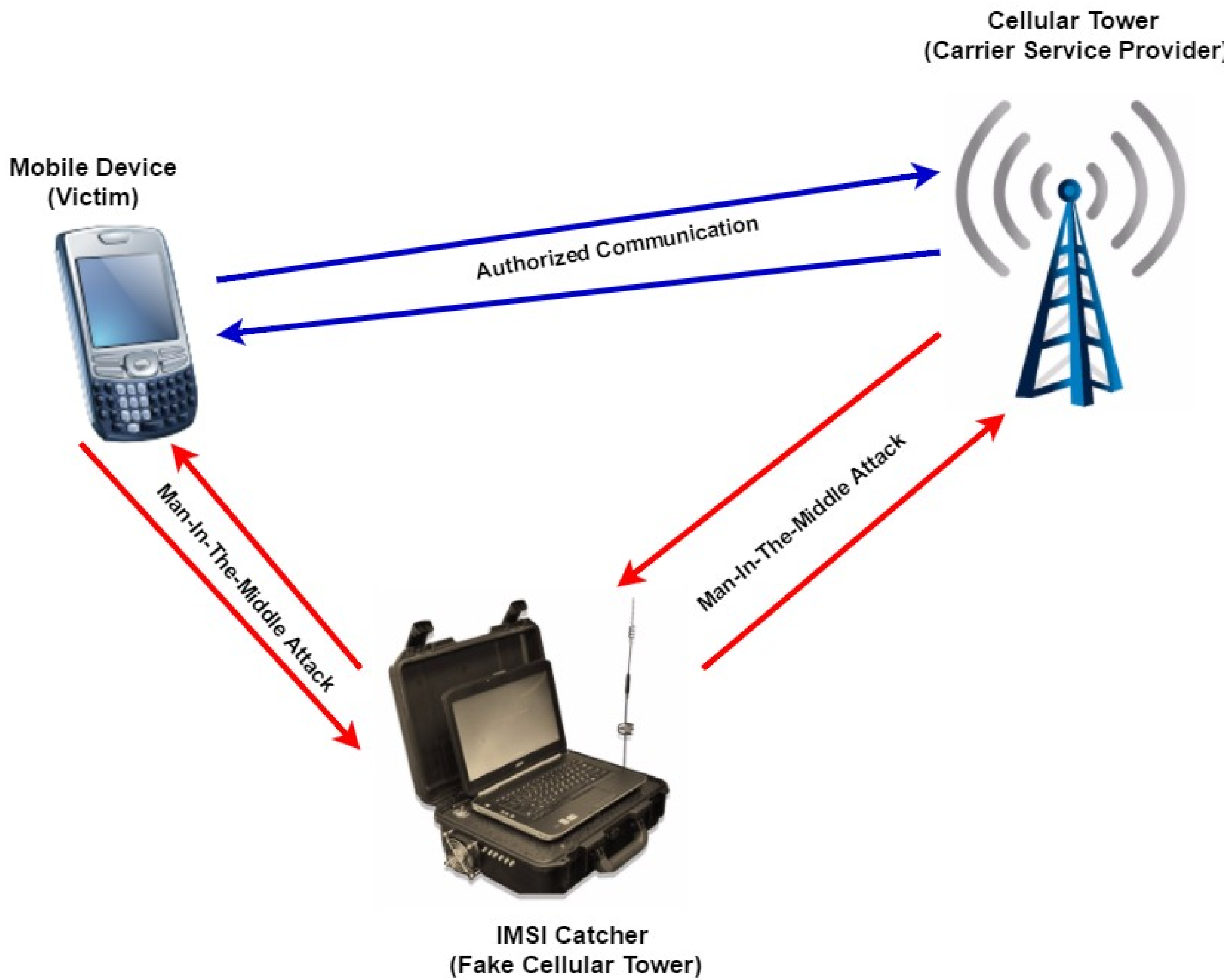
Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links

Security:
Not much.
DIY.



Security



Cellular Tower
(Carrier Service Provider)
Mobile Device
(Victim)
Authorized Communication
Man-In-The-Middle Attack
Man-In-The-Middle Attack
IMSI Catcher
(Fake Cellular Tower)

Chapter 7 summary

Wireless

- wireless links:
  - capacity, distance
  - channel impairments
  - CDMA
- IEEE 802.11 (“Wi-Fi”)
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - architecture
  - standards (e.g., 3G, 4G LTE)

Mobility

- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP
  - mobility in GSM, LTE
- impact on higher-layer protocols