Wireless & Mobile Networks

ECE 6607
GATECH Shenzhen, Fall 2022

Dr. Min Luo

1

Outline

- **Introduction**
- Wireless
  - Wireless links, characteristics
    - CDMA
  - IEEE 802.11 wireless LANs (“Wi-Fi”)
  - Cellular Internet Access
    - Architecture
    - Standards (e.g., 3G, LTE)
- Mobility
  - Principles: addressing and routing to mobile users
  - Mobile IP
  - Handling mobility in cellular networks
  - Mobility and higher-layer protocols

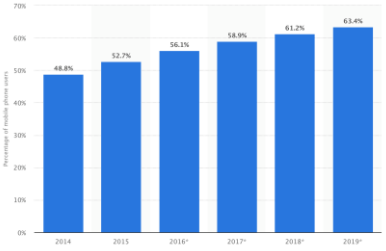
2

Background

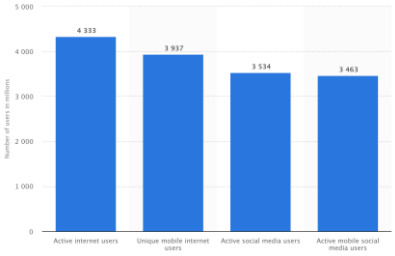
- Impressive Internet Statistics:
  - 3.5+ billion users (> 50%) of the world's population in online; Asian 2 billion
  - 54+%. browsed websites using mobile devices;
  - # wireless (mobile) phone subscribers exceeds # wired phone subscribers (5-to-1)!
    - Laptops, Internet-enabled phones, IOT devices,…
      ➔Anytime anywhere untethered Internet access
  - On avg, mobile internet users spend nearly 3 hours online every day.
    - 50+% of teenagers are addicted to the global network and its endless possibilities.

- Two important (but different) challenges
  - ***Wireless:*** Communication over wireless link
  - ***Mobility:*** Handling the mobile user who changes point of attachment to network

Mobile phone internet user penetration worldwide from 2014 to 2019



Global digital population as of July 2019 (in millions)



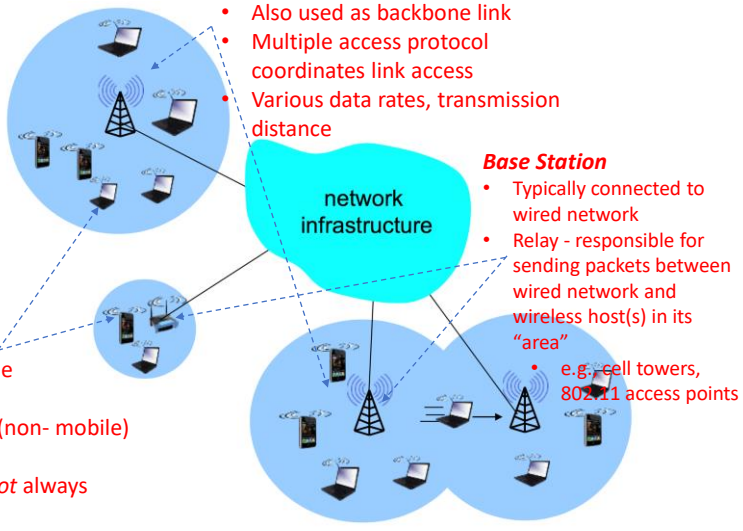
3

WIRELESS NETWORK

- Networks that work *without* wires.
- System transmit data through radio waves.
- Users are mobile, can access information within the range
- E.g. Wireless LAN i.e. ***"Wi-Fi"*** (Wireless Fidelity)

4

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

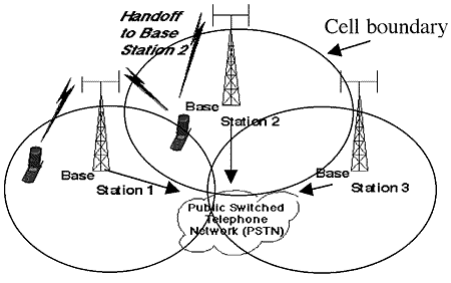
Base Station
- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

Wireless Hosts
- Laptop, smartphone
- Run applications
- May be stationary (non- mobile) or mobile
  - Wireless does *not* always mean mobility

5

Cellular Network

- Base stations transmit to and receive from mobiles at the assigned spectrum
  - Multiple base stations use the *same* spectrum (spectral reuse)
- The service area of each base station is called a *cell*
- Each mobile terminal is typically served by the '*closest*' base stations
  - *Handoff* when terminals move



6

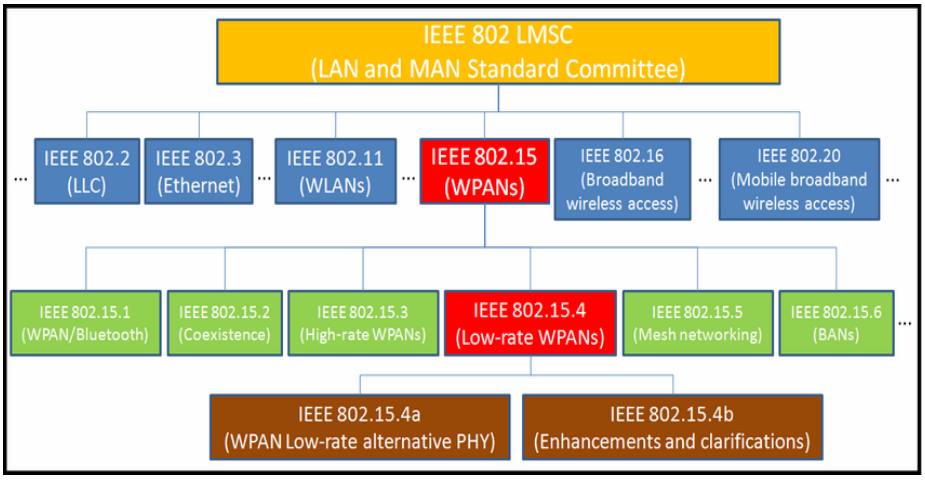
Wireless vs mobile

Possibilities?
- Wireless, not mobile
- Mobile, not wireless
- Both

- *Same*? Often used interchangeably!
- Mobile: Offers all of the resources of a distributed network to something that can go *anywhere*, barring any issues with local reception or technical area coverage
  - Commonly used to describe *portable* devices.
  - A mobile device is one that is made to be taken *anywhere* ➔ Internal battery for power, and must be connected to a mobile network that can help send and receive data *without attaching* to a hardware infrastructure.
  - Mobile devices already have *inherent access* to the Internet or other wireless systems through those cell tower networks that ISPs and telecom companies provide. ➔*Mobile devices don't need Wi-Fi* - they already have their connections!
- Wireless: Provides *a fixed or portable endpoint* with access to a distributed network
  - Traditional computers or other *non-mobile devices* can access wireless networks.
  - Use components of *3G or 4G/5G wireless systems* made specifically for mobile devices ➔ Doesn't mean that the devices on these networks are mobile – need to be plugged in or require proximity to a router or network node.
  - Wi-Fi *hotspot* is typically a resource for someone who has a relatively fixed device, such as a laptop computer that doesn't have its own internal Internet access built in.

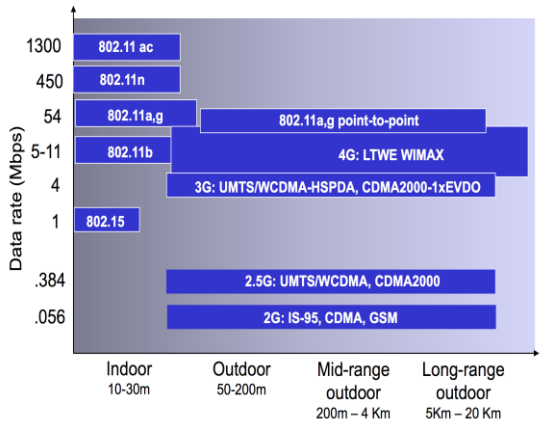
7

IEEE 802 Wireless Standards



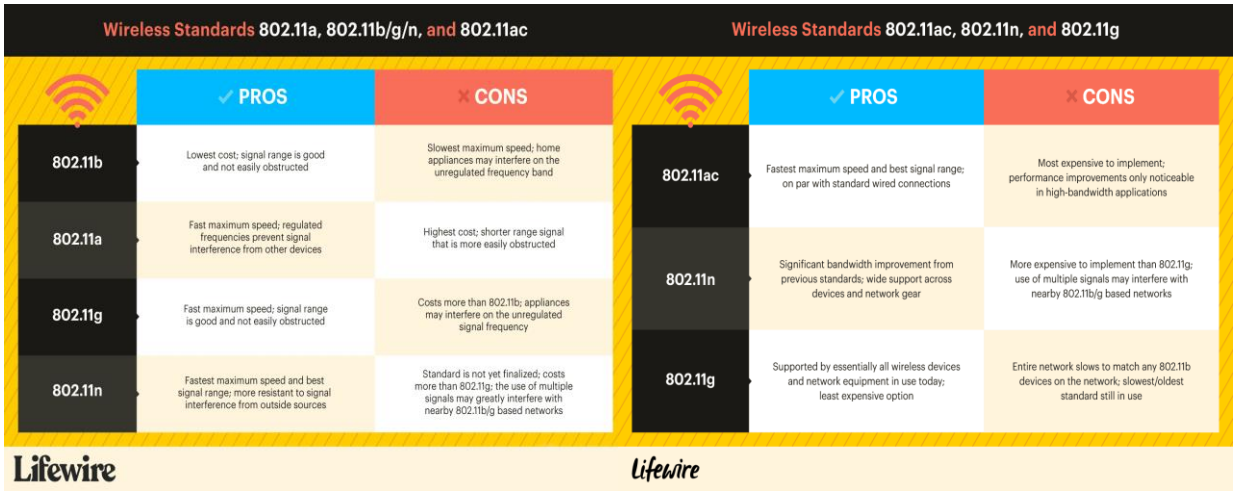
8

Characteristics of selected wireless links



IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

9

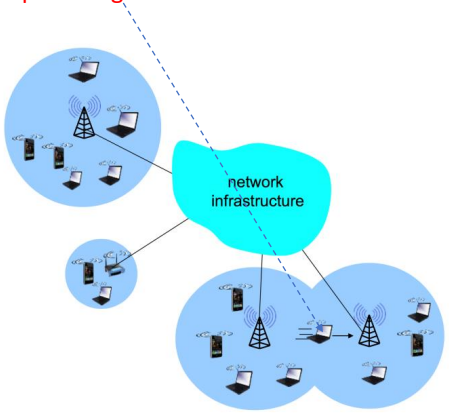


10

wireless network - Infrastructure vs Ad-Hoc

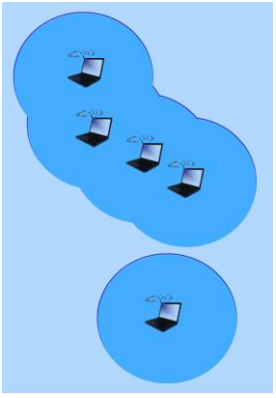
Infrastructure Mode

- Base station connects mobiles into wired network
- Handoff: Mobile changes base station providing connection into wired 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



11

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

Mobile Ad hoc Network (MANET)/ Vehicular Ad hoc Network (VANET)

- Used for communication between vehicles or between vehicles and road-side infrastructure

Characteristics	MANET	VANET
Node Mobility	Low	High
Node Speed	Lower (~ 6 Km/h)	Medium to high (~ 20 to 100 Km/h)
Mobility Model	Random	Regular
Node Density	Low	High
Topology Change	Slow	Fast
Radio propagation model	Close to Ground, LoS is not available for all cases	Close to Ground, LoS is not available for all cases
Power consumption and network lifetime	Energy efficiency protocols	Not needed
Computational Power	Limited	High
Localization	GPS	GPS, AGPS, DGPS
Cost	Inexpensive	Costly
Bandwidth	Hundred Kbps	Thousand Kbps
Range	Upto 100 meters	Upto 600 meters

12

Outline

- Introduction
- Wireless
  - **Wireless links, characteristics**
    - **CDMA**
  - IEEE 802.11 wireless LANs (“Wi-Fi”)
  - Cellular Internet Access
    - Architecture
    - standards (e.g., 3G, LTE)
- Mobility
  - Principles: addressing and routing to mobile users
  - Mobile IP
  - Handling mobility in cellular networks
  - Mobility and higher-layer protocols

13

Wireless Link Characteristics

- *Important* differences from wired link ….
  - *Decreased signal strength:* Radio signal *attenuates as it propagates* through matter (path loss)
  - *Interference* from other sources*:*
    - *S*tandardized wireless network frequencies (e.g., 2.4 GHz) *shared* by other devices (e.g., cell phone);
    - Devices interreference*/noise* (nearby motors, microwave…)
  - *Multipath propagation: R*adio signal *reflects* off objects ground, arriving at destination at slightly different times

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

➔ Bit errors more common : *CRC + RDT at link-level*!

14

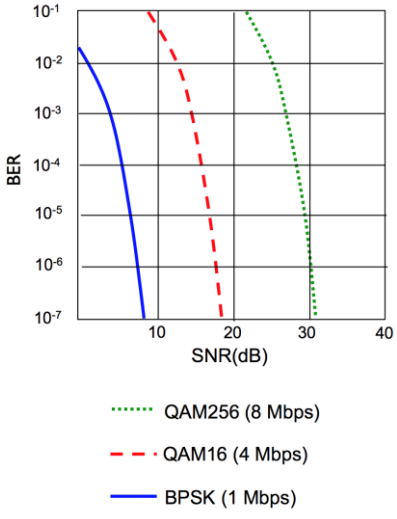
Wireless Link Characteristics

- *Impairments* ➔ Degradation ➔ Bit Error Rate (BER)
- SNR: *signal-to-noise* ratio - A relative measure of the strength of the received signal and the noise
  - Measured in decibels (dB): decibel is a logarithmic unit used to measure sound level.
    - Example: Two sound systems, one with power P_1, and another with power P_2, everything else (how far away, frequency) same: the **difference in sound level,** between the two is defined to be 10 log (P_2/P_1) dB, where the log is to base 10.
    - ***SNR = 20 log (Amplitude of Signal/ Amplitude of noise) dB***
  - *Larger SNR – easier to extract "the signal" from noise*!

15

Wireless Link Characteristics

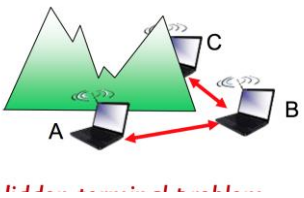
- *SNR versus Bit Error Rate (BER) tradeoffs*
  - *Given physical layer:* ➔ Increase power → increase SNR decrease BER
    - Little/No practical gain in increasing power beyond a certain threshold
    - More power ➔ More energy consumed & more interference!
  - *Given SNR:* Choose physical layer that meets BER requirement, giving highest throughput
  - *Adaptive* modulation and coding: SNR may change with mobility ➔ *Dynamically adapt* physical layer (modulation technique, rate)
    - Used in cellular data systems and in the 802.11 WiFi and 4+G cellular data networks



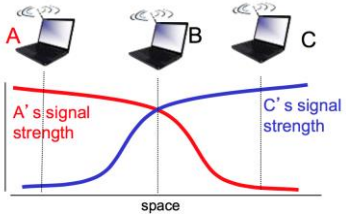
16

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 ➔ A, C unaware of their interference at B



Signal attenuation/fading:
B, A hear each other
B, C hear each other
A, C can not hear each other (power not strong enoug but interfere at B

17

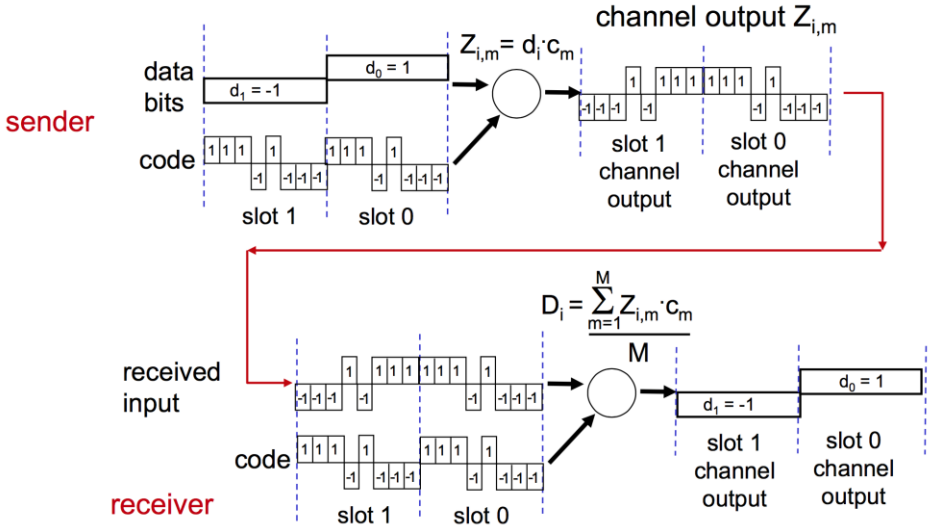
Code Division Multiple Access

- 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

E.g.: *Partygoers* speak in multiple languages!

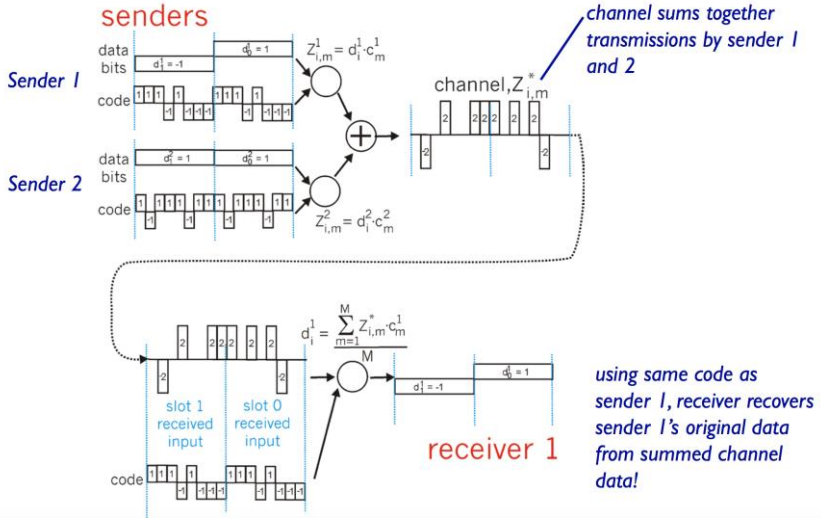
18

CDMA encode/decode



19

CDMA: two-sender interference



20

Outline

- Introduction
- Wireless
  - Wireless links, characteristics
    - CDMA
  - **IEEE 802.11 wireless LANs ("Wi-Fi")**
  - Cellular Internet Access
    - Architecture
    - standards (e.g., 3G, LTE)
- Mobility
  - Principles: addressing and routing to mobile users
  - Mobile IP
  - Handling mobility in cellular networks
  - Mobility and higher-layer protocols

21

IEEE 802.11 Wireless LAN

- **Where? ➔ WiFi**
- Two difference frequency ranges: Range and bandwidth ➔Ability to penetrate solid objects
  - *2.4 GHz* range : 2.4 –2.485 GHz
  - *5 GHz* range: 5.1 – 5.8 GHz
- **All use *CSMA/CA* for multiple access**
- **All have *base-station and ad-hoc* network versions**
- Chipping code: In CDMA, each data bit is encoded by multiplying the bit by a signal (the chipping code) that has a much higher frequency (much faster rate)

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

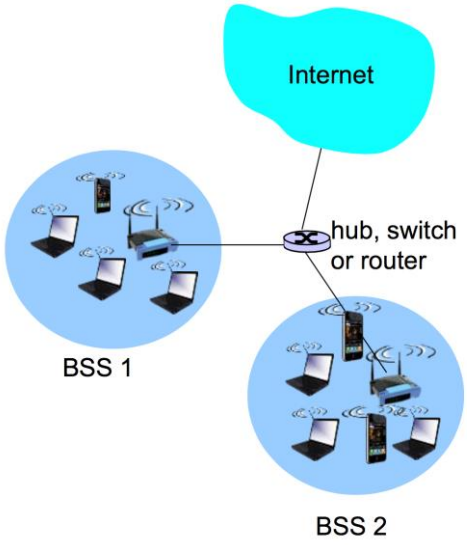
802. 11g
- 2.4-5 GHz range
- Up to 54 Mbps

802.11n: multiple antennas
- 2.4-5 GHz range

22

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



23

802.11: Channels & associatio

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 *partially overlapping* channels at different frequencies
  - AP admin chooses frequency for AP
  - *Interference* possible: channel can be same as that chosen by neighboring AP!
    - Any two channels are *non-overlapping* if and only if they *are separated by **4+** channels*
    - ***1, 6, and 11*** is the only set of three non-overlapping channels :
      - Possible to create a wireless LAN with an *aggregate maximum transmission rate of 33 Mbps* by installing three 802.11b APs at the same physical location, assigning channels 1, 6, and 11 to the APs, and interconnecting each of the APs with a switch.

Table 1 - US/Canada 802.11b/g Channel Frequencies

Channel	Nominal Frequency (MHz)	Minimum (MHz)	Maximum (MHz)
1	2412	2401	2423
2	2417	2405	2428
3	2422	2411	2433
4	2427	2416	2438
5	2432	2421	2443
6	2437	2426	2448
7	2442	2431	2453
8	2447	2436	2458
9	2452	2441	2463
10	2457	2446	2468
11	2462	2451	2473

- For a single AP to provide coverage, use one of 1/6/11
- For multiple APs, you should use two or all three of 1/6/11
- Throughput drops because of interference using more than 3 different channels in a multiple-AP scenario (CISCO)

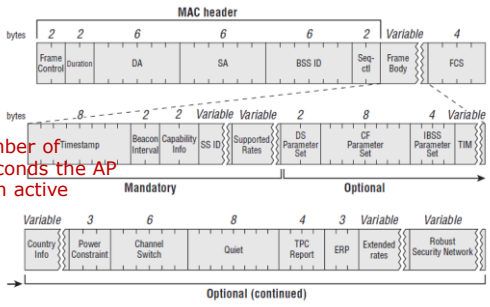
24

802.11: Channels & associati

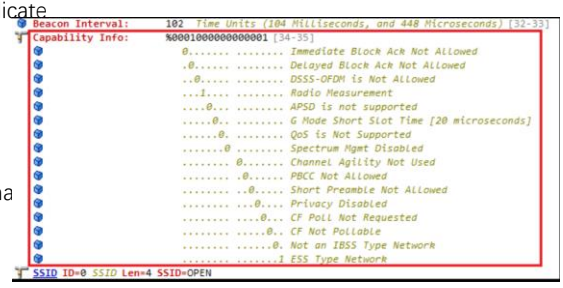
- *Beacon Frames*: Used by the access points (and stations) to communicate throughout the service area the *characteristics of the connection offered* to the cell members.
  - *Beacon* interval *:* Beacons are sent periodically at a time cal Transmission Time (TBTT);
    ➔ The number of time units (TU) between TBTT;
    Default 100: If 1 TU = 1024 microseconds, 100 TU = 10(milliseconds
  - Compatibility Info: A number of subfields that are used to indicate requested or advertised *optional* capabilities
  - "Supported"/"Baisc or Mandatory" Rate
  - Optional …

- Host: Must *associate* with an AP
  - Scans channels, listening for *beacon frames* containing AP's na the *Service Set Identifier* (SSID) and MAC address
  - Selects AP to associate with
  - May perform authentication
  - Will typically run DHCP to get IP address in AP's subnet

FIGURE 4.5 Beacon frame structure

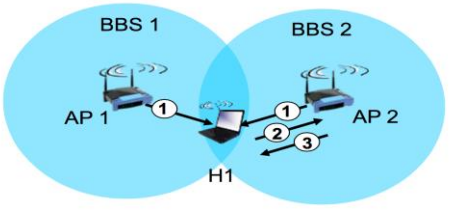


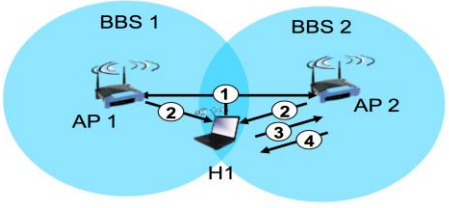
The number of microseconds the AP has been active



25

802.11: passive vs 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

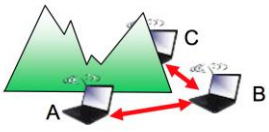
***Active scanning*:**

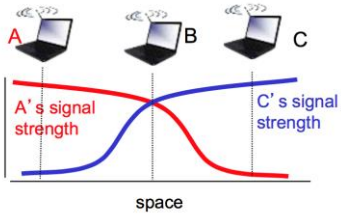
(1) Probe Request frame *broadcast* from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

26

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 nodes
- 802.11: *No* collision detection (remember?)
  - 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: To *avoid collisions* - CSMA/C(ollision)A(voidance)

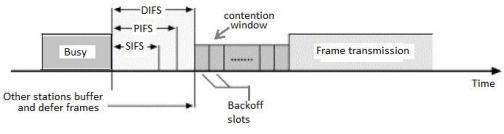




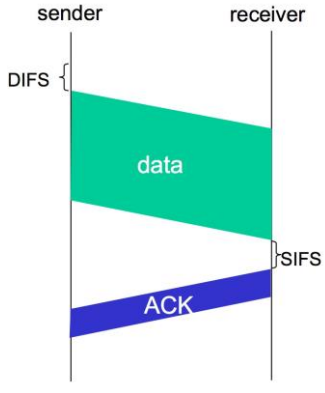
27

IEEE 802.11 MAC Protocol: CSMA/CA

- Interframe spacing: To coordinate access to the common medium that carry 802.11 compliant Ethernet packets.
  ➔ To delay the transmission until medium becomes idle
  ➔ Less delay for high priority traffic
  ➔ To facilitate interoperability between different data rates and vendor products, interframe space is *fixed* for some duration: DIFS, SIFS,



- *802.11 sender*
  1. If channel sensed idle for Distributed Inter-frame Space (**DIFS)** then transmit entire frame (no CD)
  2. If sense channel busy then
     1. Start random backoff time
     2. Timer counts down while channel idle
     3. Transmit when timer expires
     4. If no ACK, increase random backoff interval, repeat 2
- *802.11 receiver*
  1. If frame received OK return ACK after Short Inter-frame Spacing (**SIFS)** (ACK needed due to hidden terminal problem)



28

collision Avoidance

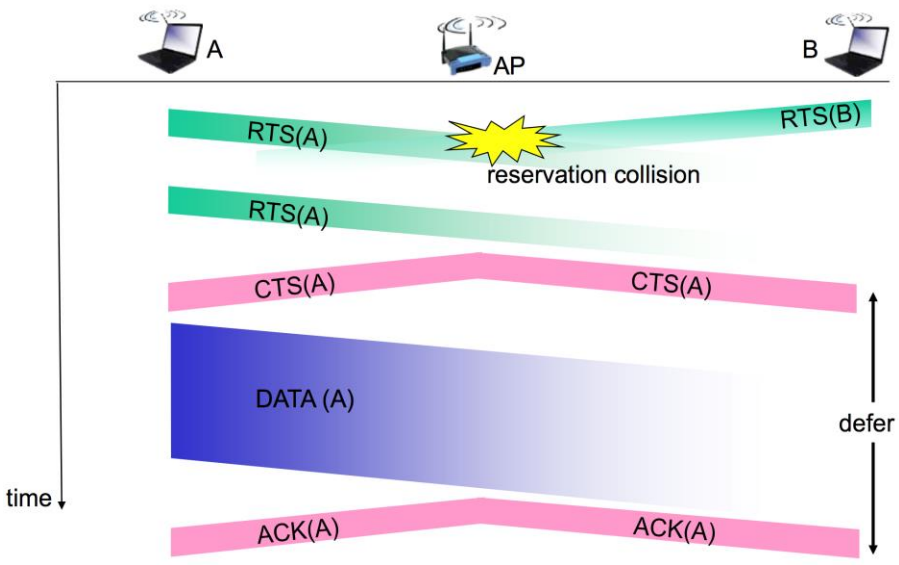
- *Idea:* Allow sender to "*reserve*" channel rather than random access of data frames
  ➔ avoid collisions of long data frames
  - Sender first transmits *small request-to-send* (RTS) packets to BS using CSMA
    - With the total time required to transmit the DATA frame + ACK
    - RTSs may still collide 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!

29

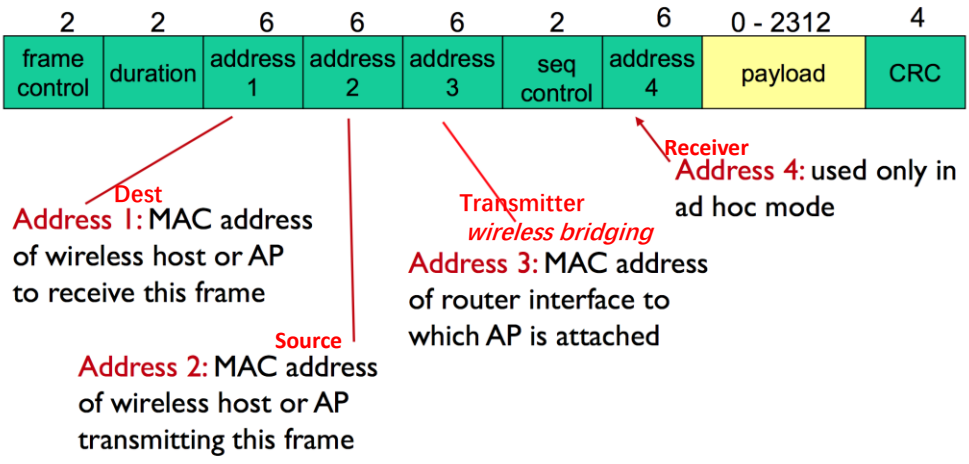
Collision Avoidance: RTS-CTS exchange

Solves the hidden terminal problem!



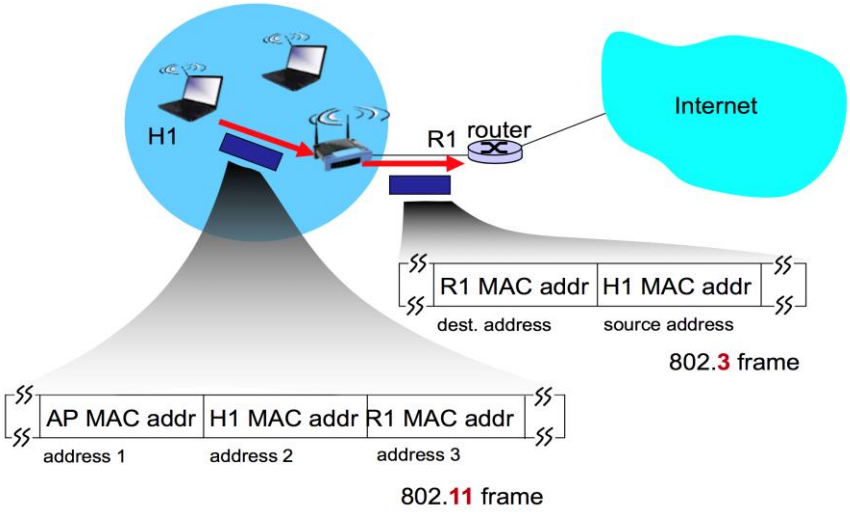
30

802.11 frame: addressing



31

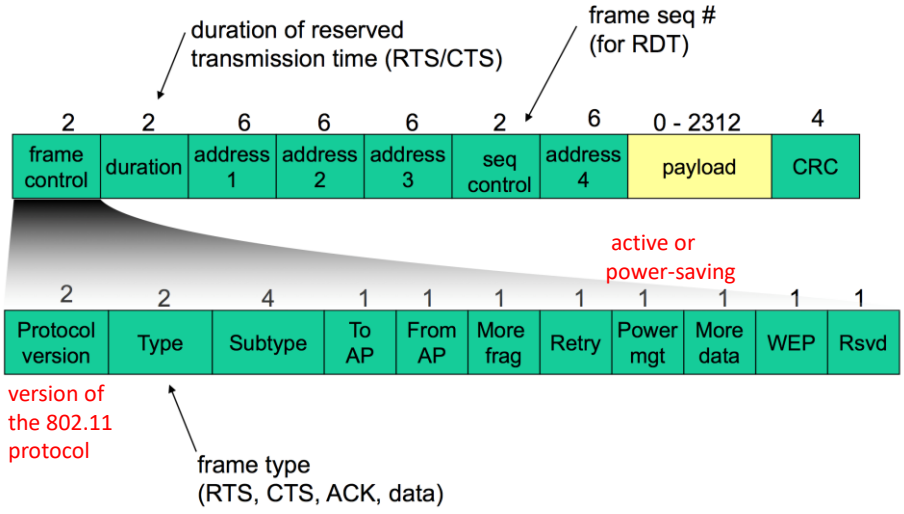
802.11 frame: addressing



32

802.11 frame

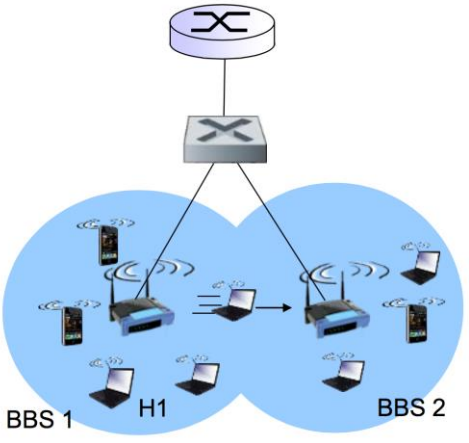
802.11 allows a transmitting station to reserve the channel for a period of time that includes the time to transmit its data frame and the time to transmit an acknowledgment



33

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*: switch will "*see*" frame from H1 and "*remember*" which switch port can be used to reach H1

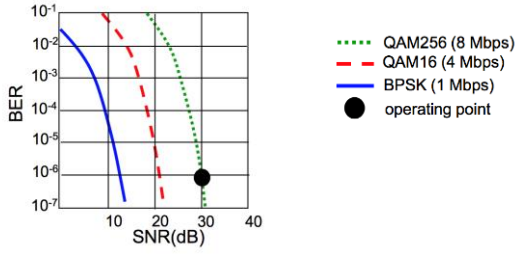


34

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

35

802.11: advanced capabilities

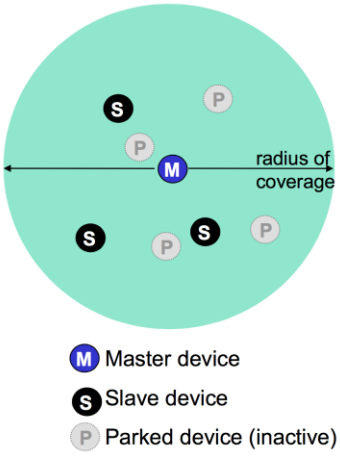
Power Management

- 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

36

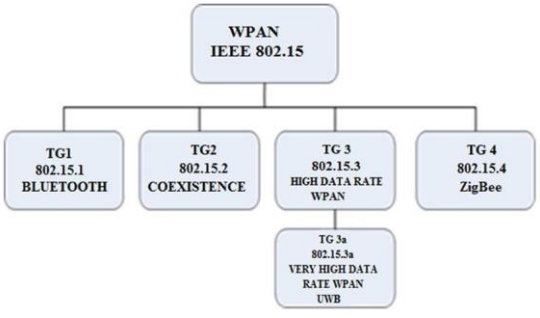
802.15: personal area network (PAN)

- Less than 10 m diameter
- Replacement for cables (mouse, keyboard, headphones)
- *Ad hoc*: no infrastructure vs Master/Slaves
  - Slaves request permission to send (to master)
  - Master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - Up to 721 kbps



37

WPAN Standards and Characteristics



Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low
LoRa	subGhz	< 50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several Miles	Medium	High
NB-IoT	Cellular Bands	0.1-1 Mbps	Several Miles	Medium	High
SigFox	subGhz	< 1 kbps	Several Miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several Miles	Low	Low
Wi-Fi	subGhz, 2.4Ghz, 5Ghz	0.1-54 Mbps	< 300 feet	Medium	Low
WirelessHART	2.4Ghz	250 kbps	~300 feet	Medium	Medium
ZigBee	2.4Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	subGhz	40 kbps	~100 feet	Low	Medium

38

ADVANTAGES OF WIRELESS NETWORK

- **Flexible**: Radio waves can penetrate the obstacles. Sender and receiver can be placed any where.
- **Mobility**: Data can be access from any location.
- **Robustness** : Can survive in disaster (Earthquake, military operations)
- **Scalable**: Can be configured in variety of topologies.
- **Easy Installation**
- **Less Cost**
- **Usage of ISM band**: *ISM (Industrial, Scientific and Medical) band* (2.40GHz to 2.484 GHz, 5.725 GHz to 5.850 GHz) is *available for use by anyone*.
- **No Planning**: Only *Wireless Ad hoc* not required any planning**.**

39

DISADVANTAGES OF WIRELESS NETWORK

- **Quality of Service:**
  - Lower Bandwidth
  - Lower Data Transmission Rate
  - High Error Rates
  - Interference
  - Higher Delay
- **Restrictions:** License-free frequency bands are not same worldwide.
- **Safety and Security**: Interference from other devices (e.g. Hospital. Eavesdropping is possible).

40

Outline

- Introduction
- Wireless
  - Wireless links, characteristics
    - CDMA
  - IEEE 802.11 wireless LANs (“Wi-Fi”)
  - **Cellular Internet Access**
    - Architecture
    - standards (e.g., 3G, LTE)
- Mobility
  - Principles: addressing and routing to mobile users
  - Mobile IP
  - Handling mobility in cellular networks
  - Mobility and higher-layer protocols

41

Why Cellular Internet Access?

- 802.11 hotspot/AP: 10-100m coverage only!
- The cellular telephony is ubiquitous
  ➔ To extend cellular networks to support not only voice telephony but wireless Internet access
  - Reasonably high speed
  - *Seamless mobility*
    - Allowing users to maintain their *TCP sessions* while traveling
    - Maintain video-conferencing sessions while roaming : If UL/DL rate high

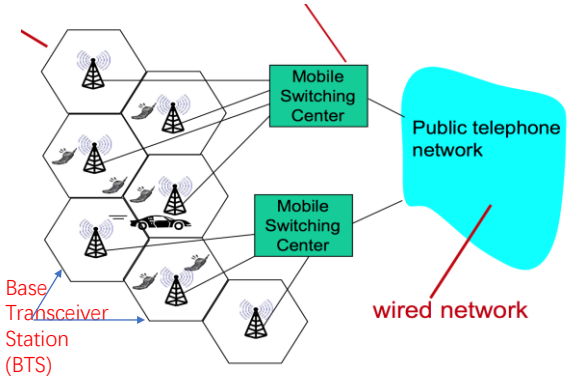
42

Components of cellular network architecture

- *"Cellular": T*he region covered by a *cellular network* is partitioned into a number of *geographic coverage areas*, known as ***cells***

- **Cell**
  - Covers geographical region: Dependent on the transmitting *power* of the BTS, the transmitting power of the user device, *obstructing objects* (buildings, ···) in the cell, and the *height* of base station antennas
  - *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* telephone net.
  - Manages call setup ❖
  - Handles mobility

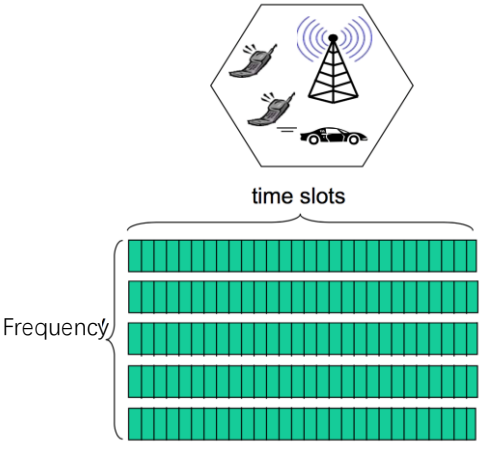


43

Cellular networks: *the first hop*

- Two techniques for sharing *mobile-to-BS* radio spectrum
  - Combined FDMA/TDMA:
    - The channel is partitioned into a number of frequency sub-bands;
    - Within each sub-band, time is partitioned into frames and slots

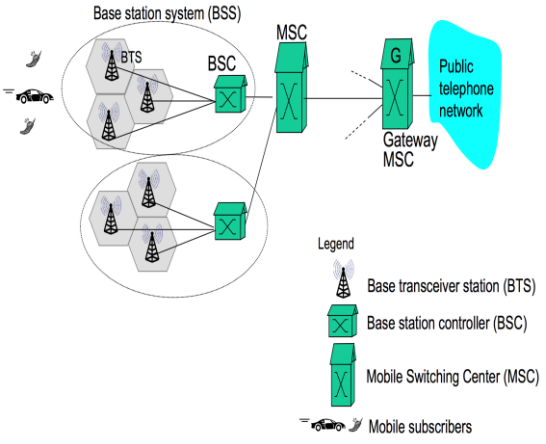
      ➔ If the channel is partitioned into *F* sub-bands and time is partitioned into *T* slots, then the channel will be able to support *F***T* simultaneous calls
  - CDMA: code division multiple access



44

2G (voice) network architecture

- **BSC: T**o allocate BTS radio channels to mobile subscribers, perform **paging (which cell) and handoff** of mobile users
  ➔ Typically service *several tens* of base transceiver stations
- **MSC:** User authorization and accounting, call establishment and teardown, and handoff.
  ➔A single MSC will typically contain *up to five BSCs*, approximately 200K subscribers per MSC
- **GMSC**: Connecting the provider's cellular network to the larger public telephone network



General Packet Radio Services (**GPRS): 2/3G**

- **A** *packet-based wireless 2G* communication service that can provide data rates from *56 up to 114 Kbps* and *continuous connection* to the Internet for mobile phone and computer users.
- Used for 2G data services:
  ➔ 2.5G = 2G cellular technology + GPRS
- GPRS data cannot be sent while a voice call is in progress

45

3G Cellular Data Networks: Extending the Internet to Cellular Subscribers

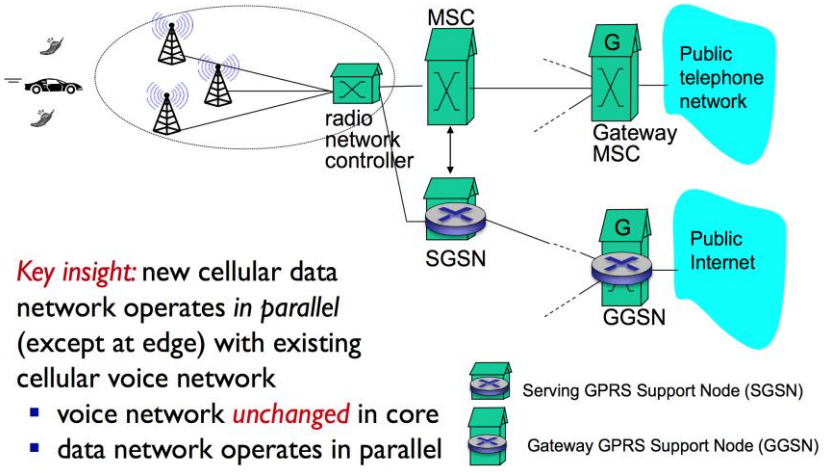
- To read e-mail, access the Web, get *location-dependent services* (e.g., maps and restaurant recommendations), watch streaming video … while traveling (no wifi)?
- Smartphones need to run a full TCP/IP protocol and connect into the Internet via the cellular data network!

- But *no single official body* that sets requirements for 2.5G, 3G, 3.5G, or 4G , … technologies
  - UMTS (Universal Mobile Telecommunications Service): 3G and 4G standards developed by the *3rd Generation Partnership project* (**3GPP**)
    - *3G broadband, packet-based* transmission of text, digitized voice, video, and multimedia at data rates *up to 2 Mbps*.
    - Offers a *consistent set of services* to mobile computer and phone users, no matter where they are ➔ same set of *capabilities*
    - Based on GSM.

*Global System for Mobile Communications (**GSM**)*: most popular cell phone standard; *~80% wireless calls*

46

3G (voice + data) network architecture

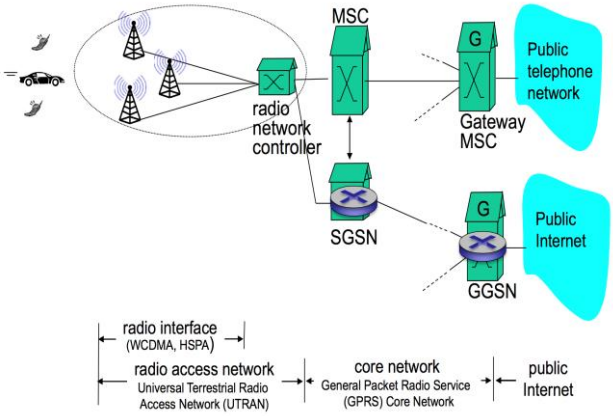


Q: Can/Should we integrate voice & data?

47

3G (voice + data) network architecture

- Universal Mobile Telecom System (UMTS):
  - A mobile cellular system of 3G that is based on GSM and maintained by 3GPP
  - It specifies a complete network system ➔ Freedom of Mobile Multimedia Access (FOMA).



WCDMA - *Wideband* code division multiple access:

- A 3G standard that employs the *direct-sequence CDMA* and the *frequency-division duplexing* to provide high-speed and high-capacity service.
- Most commonly used variant of the UMTS

HSPA - High-speed packet access

- Up to 14.4 Mbit/s down
- Up to 5.76 Mbit/s up
- Also boosts capacity in UMTS networks and provides significant latency reductions.

48

3G Core Network

- Connects radio access networks to the public Internet
- Interoperates with components of the existing cellular voice network (in particular, the MSC)
- Approach taken by the designers of 3G data services : *Leave the existing core GSM cellular voice network as-is, with additional cellular data functionality in parallel*
  ➔ *A*lternative: To *integrate* new data services directly into the core of the existing cellular voice network

Two types of nodes in the 3G core network:

- **Serving GPRS Support Nodes (SGSNs): D**elivering datagrams to/from the mobile nodes .
  - Interacts with the MSC for that area ➔ user authorization and handoff, maintaining location (cell) information, datagram forwarding between mobile nodes in the radio access network and a GGSN

- **Gateway GPRS Support Nodes (GGSNs) :** A gateway, connecting multiple SGSNs into the larger Internet
  ➔ The "*edge*" router

49

3G Radio Access Network: The *Wireless Edge*

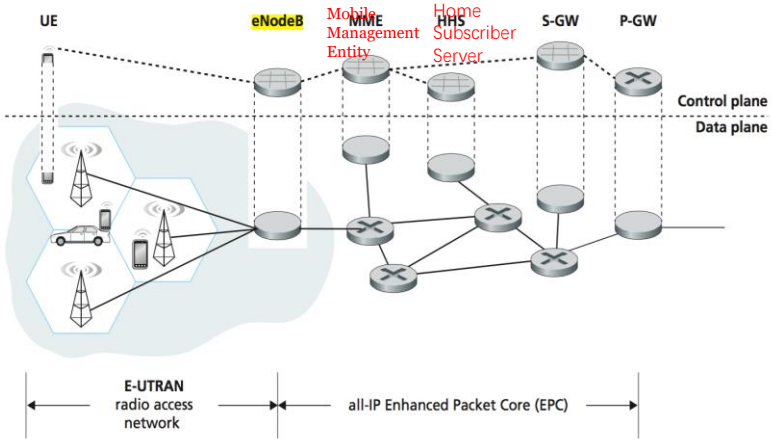
- The *wireless first-hop* network

- **Radio Network Controller (RNC): T**ypically controls several cell base transceiver stations, officially known as "***NodeB***"
  - RNC connects to both the circuit-switched cellular voice network via an MSC, and to the packet-switched Internet via an SGSN.
  - 3G cellular voice and cellular data services use *different core networks*, while sharing a *common first/last-hop* radio access network

- UMTS uses a CDMA technique known as Direct Sequence Wideband CDMA (DS-WCDMA)
- The data service associated with the WCDMA specification is the *High Speed Packet Access* (HSPA) and promises downlink data rates of up to 14.4 Mbps, and uplink rate up to 5.76 Mbps

50

4G network architecture



- A ***unified, all-IP*** network architecture.
- A *clear separation* of the *4G data* plane and *4G control* plane.
- A *clear separation* between the *radio access* network, and the *all-IP-core* network.

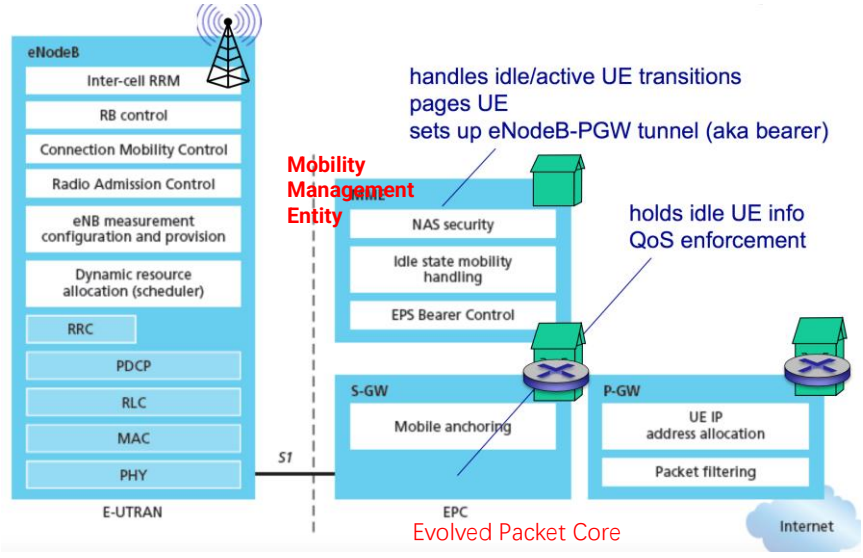
51

4G LTE

- 4G: 10x faster than 3G ➔ Minimum specification of 100 Mbps download speed, …
- "Long-Term Evolution (LTE)" toward the 4G standard!
  - High speed *mobile* and *broadband* data, telephone service, and supports public safety functions.
  - Special features to manage the network
    - Assign *priorities* to customers ➔ Emergency calls; decide which call gets through first and which might be dropped.
    - A *self-organizing* network, meaning that if there is an outage, the calls will be rerouted to another path automatically and once service is restored, the network will revert back to its *optimally designed path*.
- 4G LTE ➔ "upgraded 3G, but worse than *true 4G*"!
  - 4G was defined as the *ideal* standard: No phones actually can reach this standard ➔ LTE.

52

Functional split of major LTE components



https://yatebts.com/documentation/concepts/lte-concepts/

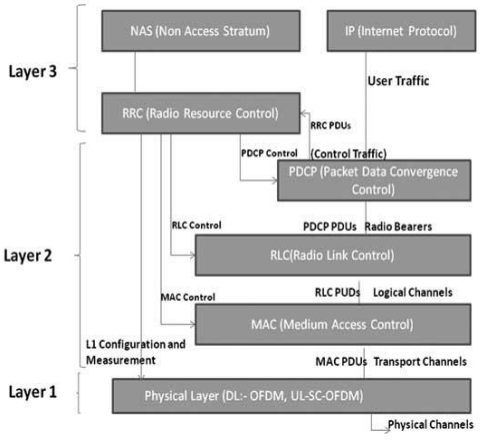
eNodeB: The logical descendant of the 2G *base station* and the 3G *Radio Network Controller* (RNC, a.k.a Node B).
Its data- plane role: T*o forward datagrams between UE (over the LTE radio access network) and the P-GW*
Packet Gateway (P-GW): Allocates *IP addresses* to the UEs and **QoS** enforcement; Encap…

Serving Gateway (S-GW): Data-plane *mobility anchor* point

- all UE traffic will pass through the S-GW
- also charging/billing functions and lawful traffic

53

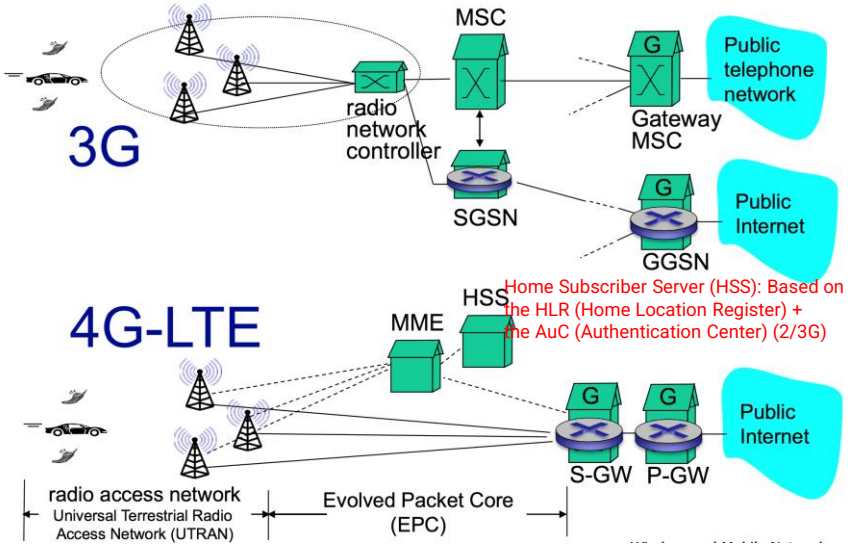
LTE Protocol Stack Layers - E-UTRAN Protocol Stack



- ***Non Access Stratum (NAS) Protocols***: The highest stratum of the control plane between the user equipment (UE) and MME.
  - Support the mobility of the UE and the session management procedures to establish and maintain IP connectivity between the UE and a P-GW.
- ***Radio Resource Control (RRC)***: Broadcast System Information related to the non-access stratum (NAS), the access stratum (AS), Paging, establishment, maintenance and release of an RRC connection between the UE and E-UTRAN; Security functions such as key management, establishment, configuration, maintenance and release of point to point Radio Bearers.
- ***Packet Data Convergence Control (PDCP)***: Responsible for Header compression and decompression of IP data, Transfer of data (user plane or control plane), Maintenance of PDCP Sequence Numbers (SNs), In-sequence delivery of upper layer PDUs at re-establishment of lower layers, Duplicate elimination of lower layer SDUs at re-establishment of lower layers for radio bearers mapped on RLC AM, Ciphering and deciphering of user plane data and control plane data, Integrity protection and integrity verification of control plane data, Timer based discard, duplicate discarding
- ***Radio Link Control (RLC)***: RLC operates in 3 modes of operation: Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM).
  - Responsible for transfer of upper layer PDUs, error correction through ARQ (Only for AM data transfer), Concatenation, segmentation and reassembly of RLC SDUs (Only for UM and AM data transfer).
  - Also responsible for re-segmentation of RLC data PDUs (AM data transfer), reordering of RLC data PDUs (UM and AM data transfer), duplicate detection (UM and AM data transfer), RLC SDU discard (UM and AM data transfer), RLC re-establishment, and protocol error detection (AM data transfer).
- ***Medium Access Layer (MAC)***: Responsible for Mapping between logical channels and transport channels, Multiplexing of MAC SDUs from one or different logical channels onto transport blocks (TB) to be delivered to the physical layer on transport channels, de-multiplexing of MAC SDUs from one or different logical channels from transport blocks (TB) delivered from the physical layer on transport channels, Scheduling information reporting, Error correction through HARQ, Priority handling between UEs by means of dynamic scheduling, Priority handling between logical channels of one UE, Logical Channel prioritization.
- ***Physical Layer***: Carries all information from the MAC transport channels over the air interface. Takes care of the link adaptation (AMC), power control, cell search (for initial synchronization and handover purposes) and other measurements (inside the LTE system and between systems) for the RRC layer.

54

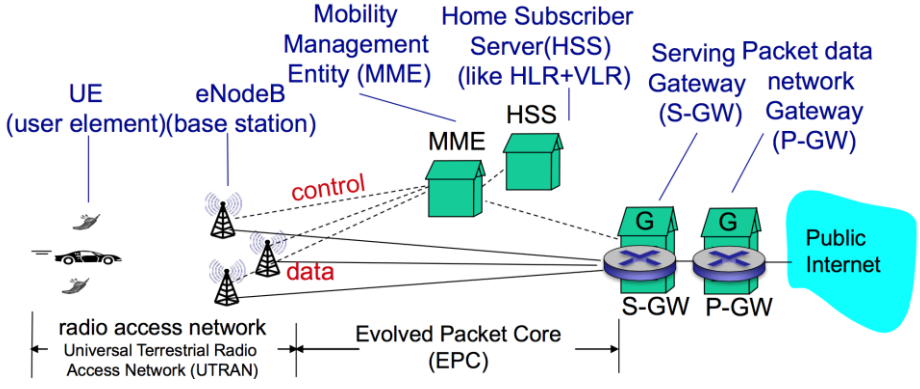
3G versus 4G LTE network architecture



55

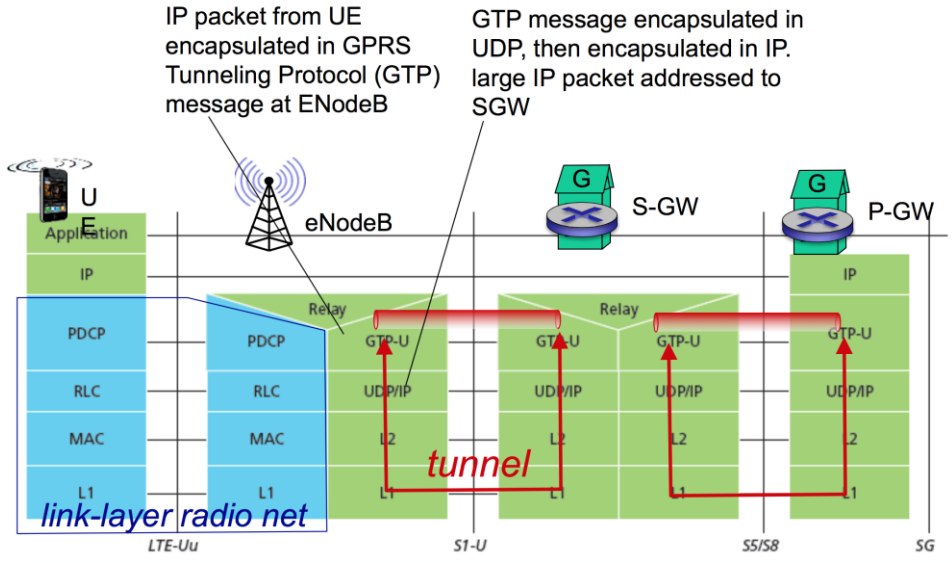
4G - KEY differences from 3G

- 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



56

Radio+Tunneling: UE – eNodeB – PGW



57

Quality of Service in LTE

- QoS from eNodeB to SGW:
  - Min and Max *guaranteed bit rate* (GBR)
  - Delay
  - Loss rate
- QoS in radio access network: Specified with QoS Class Identifier (QCI) values

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100ms	10^{-2}	Conversational Voice
2	GBR	4	150ms	10^{-3}	Conversational Video (Live Streaming)
3	GBR	3	50ms	10^{-3}	Real Time Gaming, V2X messages
4	GBR	5	300ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
65	GBR	0.7	75ms	10^{-2}	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66	GBR	2	100ms	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
75	GBR	2.5	50ms	10^{-2}	V2X messages
5	non-GBR	1	100ms	10^{-6}	IMS Signalling
6	non-GBR	6	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p and the like)
7	non-GBR	7	100ms	10^{-3}	Voice, Video (Live Streaming), Interactive Gaming
8	non-GBR	8	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p and the like)
9	non-GBR	9	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p and the like). Typically used as default bearer
69	non-GBR	0.5	60ms	10^{-6}	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70	non-GBR	5.5	200ms	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)
79	non-GBR	6.5	50ms	10^{-2}	V2X messages
80	non-GBR	6.8	10ms	10^{-6}	Low latency eMBB applications (TCP/UDP-based); Augmented Reality
82	GBR	1.9	10ms	10^{-4}	Discrete Automation (small packets)
83	GBR	2.2	10ms	10^{-4}	Discrete Automation (big packets)
84	GBR	2.4	30ms	10^{-5}	Intelligent Transport Systems
85	GBR	2.1	5ms	10^{-5}	Electricity Distribution- high voltage

IMS: IP Multimedia Subsystem

58

Outline

- Introduction
- Wireless
  - Wireless links, characteristics
    - CDMA
  - IEEE 802.11 wireless LANs (“Wi-Fi”)
  - Cellular Internet Access
    - Architecture
    - Standards (e.g., 3G, LTE)

- **Mobility**
  - **Principles: Addressing and routing to mobile users**
  - Mobile IP
  - Handling mobility in cellular networks
  - Mobility and higher-layer protocols

59

What is mobility?

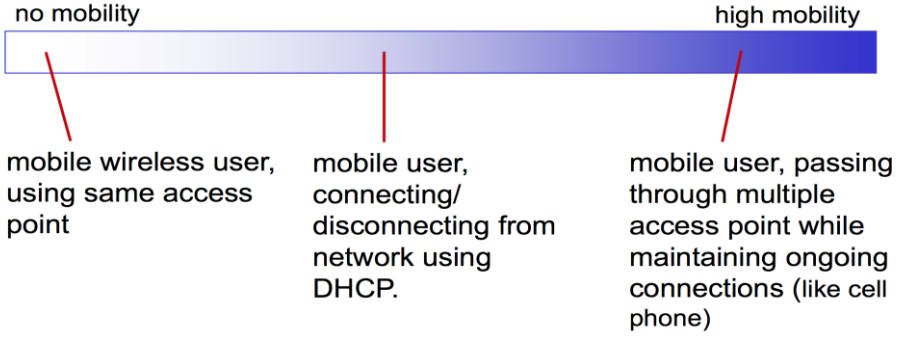
Key Qs:

How Mobile?

Same (IP) address?

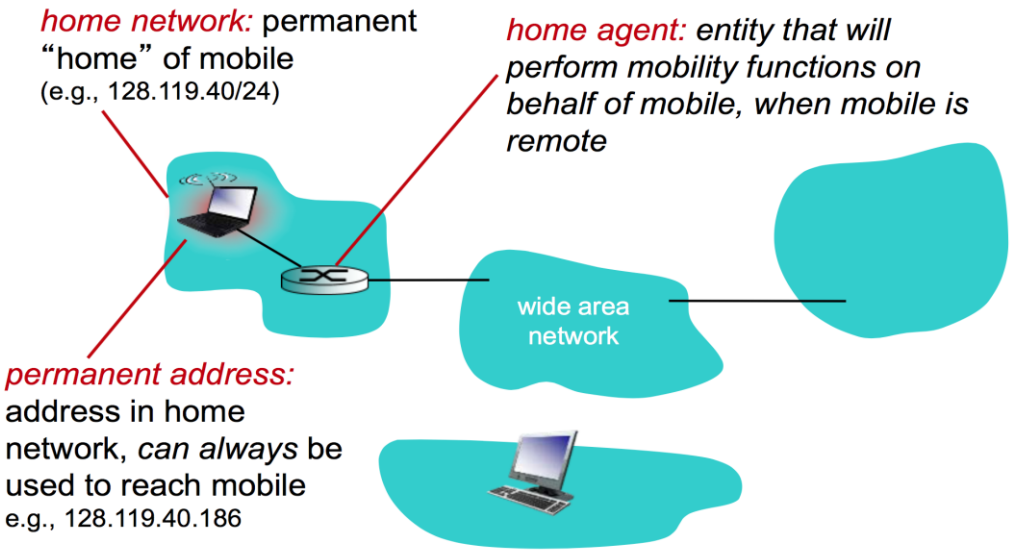
Supporting wired network?
➔ ad-hoc

Spectrum of mobility, from the *network* perspective:



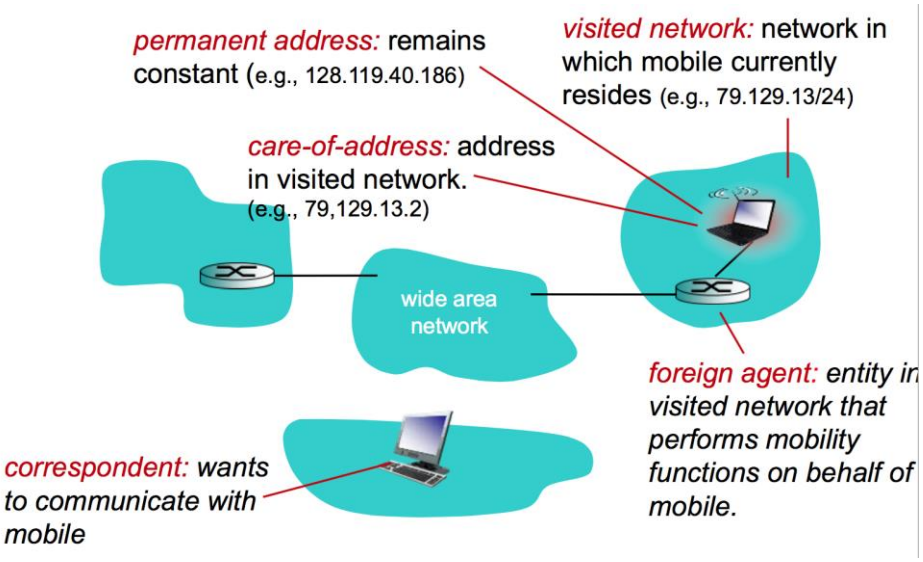
60

Mobility: vocabulary



61

Mobility: Addressing



62

How do *you* contact a mobile friend

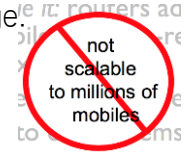
Consider friend frequently changing addresses, how do you find her?

- Search all phone books?
- Call her parents?
- Expect her to let you know where he/she is?
- Facebook/WeChat···?!

63

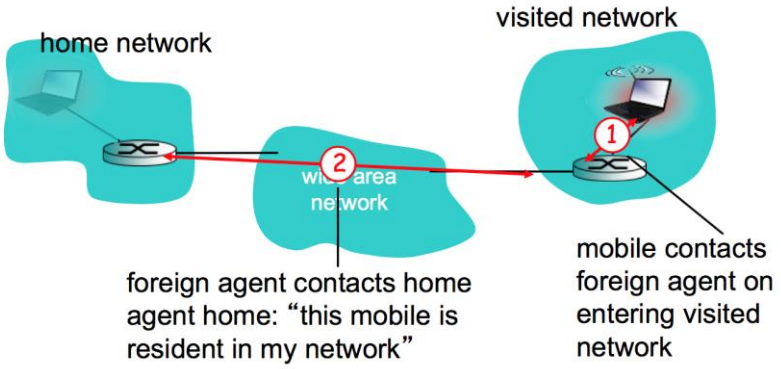
Mobility: approaches

- *Let routing handle it: R*outers 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: C*ommunication from correspondent to mobile goes through home agent, then get forwarded to remote
  - *Direct routing: C*orrespondent gets foreign address of mobile, sends directly to mobile



64

Mobility: registration

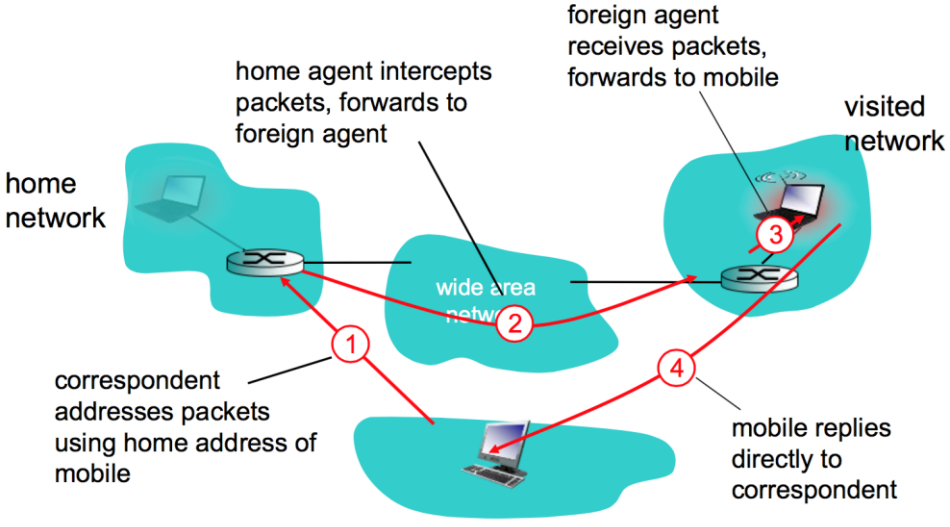


End result:

- Foreign agent knows about mobile
- Home agent knows location of mobile

65

Mobility via indirect routing



66

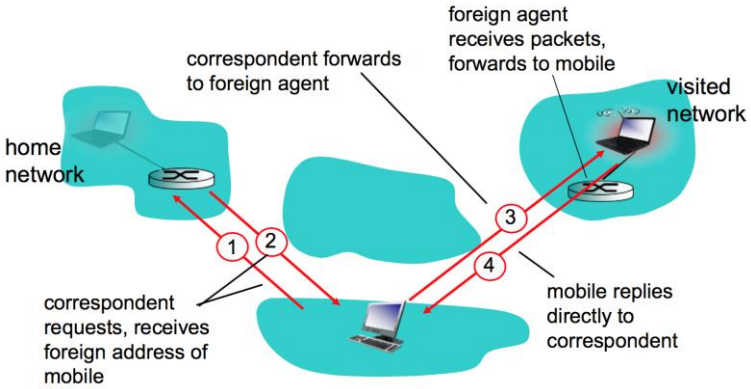
Indirect routing: moving between networks

- 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!*

- 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

67

Mobility via direct routing

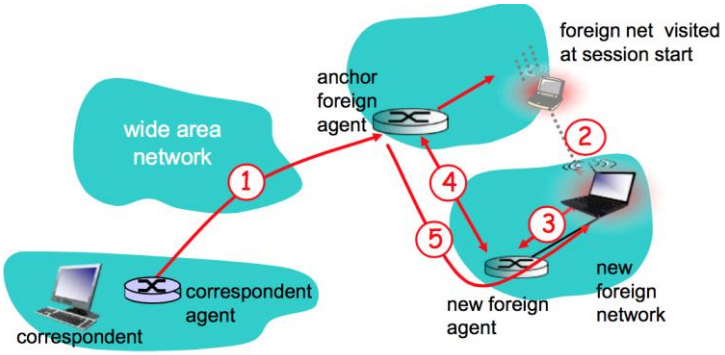


- Overcome triangle routing problem
- *Non-transparent to correspondent:* correspondent must get care-of-address from home agent
  - What if mobile changes visited network?

68

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)



69

Outline

- Introduction
- Wireless
  - Wireless links, characteristics
    - CDMA
  - IEEE 802.11 wireless LANs ("Wi-Fi")
  - Cellular Internet Access
    - Architecture
    - standards (e.g., 3G, LTE)
- **Mobility**
  - Principles: addressing and routing to mobile users
  - **Mobile IP**
  - **Handling mobility in cellular networks**
  - **Mobility and higher-layer protocols**

70

Mobile IP

Internet architecture and protocols for supporting mobility

- RFC 3344: With 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

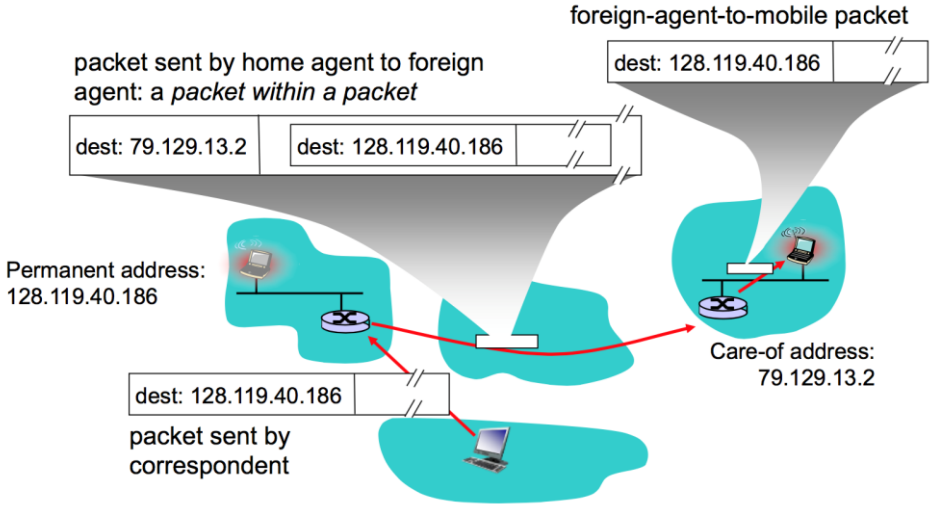
Flexible:

- Supporting many different modes of operation (for example, operation with or without a foreign agent)
- Multiple ways for agents and mobile nodes to discover each other
- Use of single or multiple COAs
- Multiple forms of encapsulation.

But **Complex!**

71

Mobile IP: indirect routing

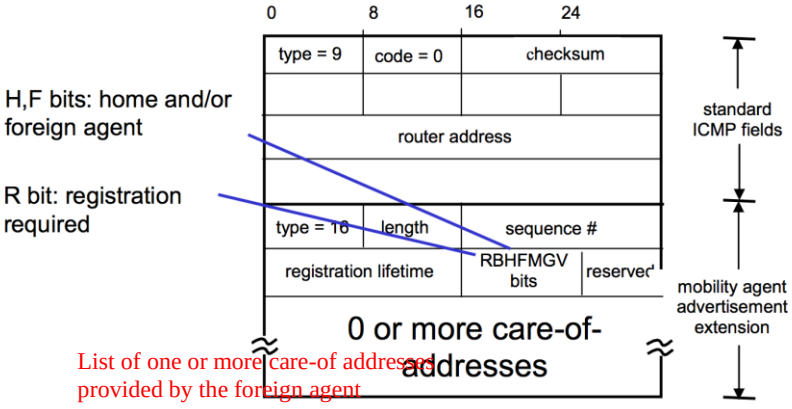


72

Mobile IP: agent discovery

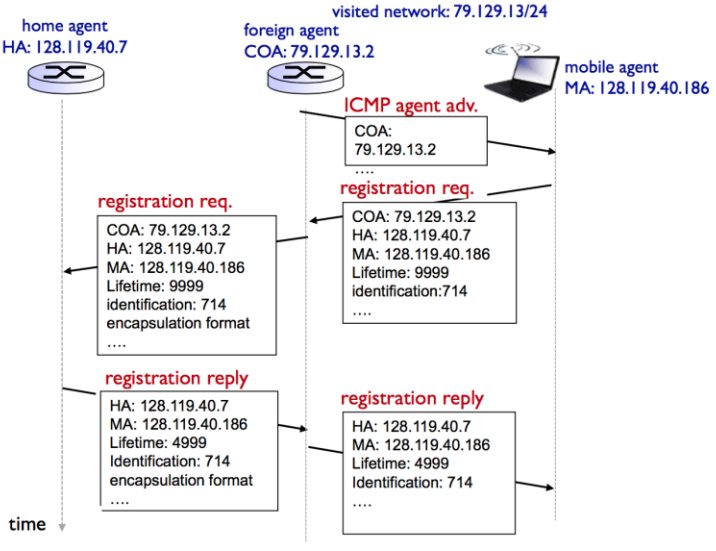
Internet Control Message Protocol(ICMP): An error-reporting protocol network devices (routers) use to generate error messages to the source IP address when network problems prevent delivery of IP packets
➔Supporting protocol for IP stack

- *Agent Advertisement: F*oreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



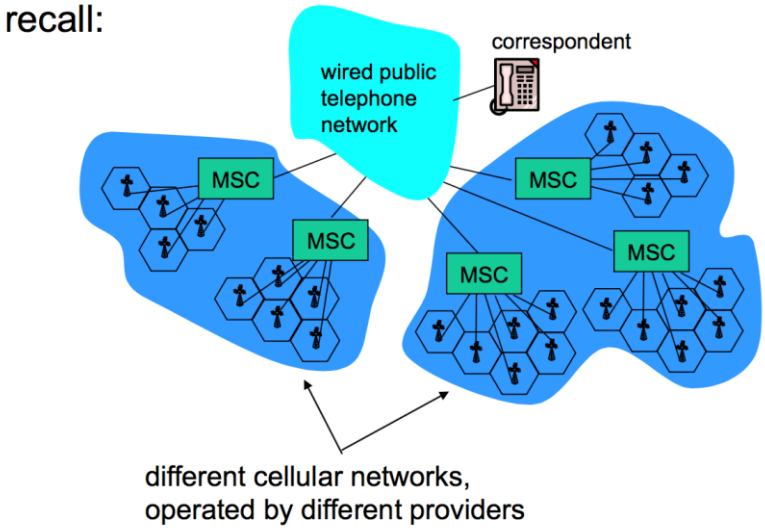
73

Mobile IP: registration example



74

Components of cellular network architecture



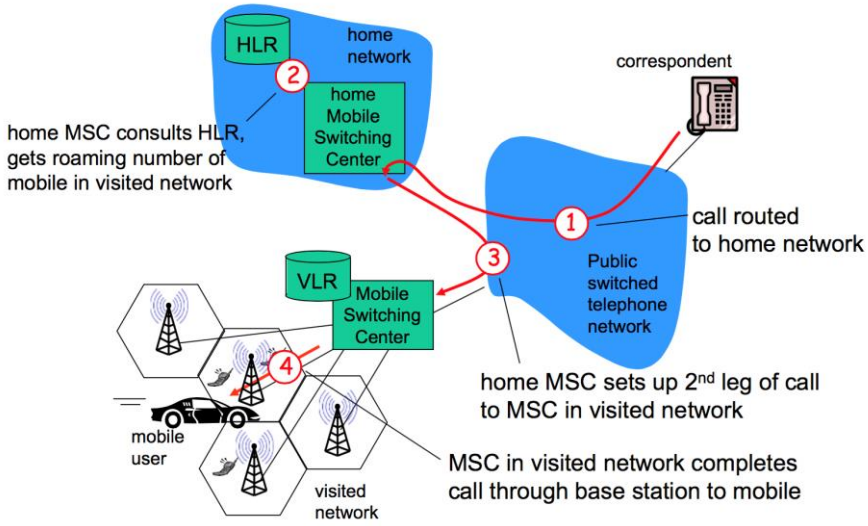
75

Handling mobility in cellular networks

- *Home Network*: Network of cellular provider you subscribe to (e.g., T-Mobile, AT&T, Verizon, Deutch Tel, China Unicom, China Mobile, …)
  - *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)
    ➔ Enough information to obtain an address in the visited network
- *Visited Network: Where* mobile currently resides
  - *Visitor Location Register (VLR):* Database with entry for each user currently in network
  - Could be home network

76

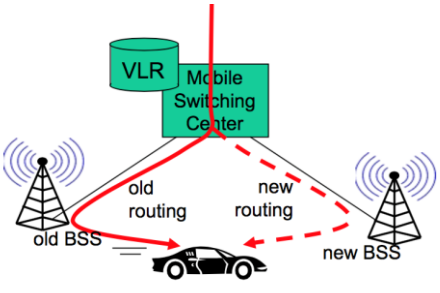
GSM: indirect routing to mobile



77

GSM: handoff with common MSC

- *Handoff: R*oute call via new base station (without interruption), when a mobile station changes its association from one base station to another during a call
- Reasons for handoff:
  - Stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - Load balance: Freeup channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- Handoff *initiated* by old BSS

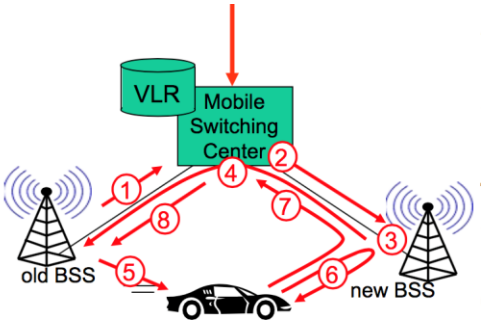


A mobile *periodically* measures the *strength* of a *beacon signal* from its current base station and also beacon signals from nearby base stations

78

GSM: handoff with common MSC

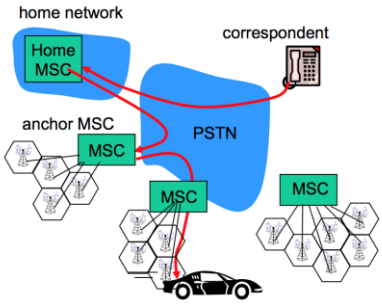
1. Old BSS informs MSC of impending handoff, provides list of 1+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. New BSS allocates radio channel for use by mobile
4. New BSS signals MSC: old BSS is ready
5. Old BSS tells mobile: perform handoff to new BSS
6. Mobile, new BSS signal to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



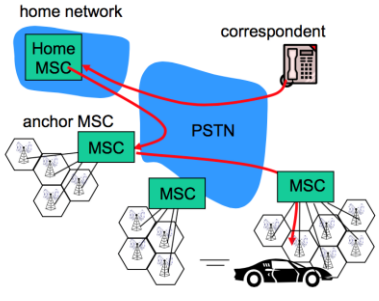
79

GSM: handoff between MSCs

- *Anchor MSC: F*irst 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



(a) before handoff

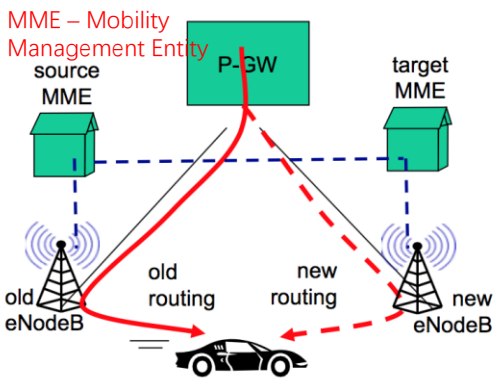


(b) after handoff

80

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: Old BS initiate →Visited MSC setup path → New BS activates channel for Mobile → …
  - Execution phase: Mobile and new BS exchange msgs …
  - Completion phase: Handoff complete to new BS →Visted MSC …



81

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

82

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 unnecessarily
  - Delay impairments for real-time traffic
  - Limited bandwidth of wireless links

83

Summary

Wireless

- Wireless links:
  - Capacity, distance
  - Channel impairments
  - CDM A
- IEEE 802.11 ("Wi-Fi")
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - Architecture
  - Standards (e.g., 3G, 4G L TE)

Mobility

- Principles: Addressing & routing to mobile users
  - Home, visited networks
  - Direct, indirect routing
  - Care-of-addresses (roaming number)
- Case studies
  - Mobile IP
  - Mobility in GSM, LTE
  - Impact on higher-layer protocols

84

Assignments

- Reading: 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Problems: P1, P3, P5, P7, P8, P12, P13, P14, P15