Distributed Computer Systems Engineering

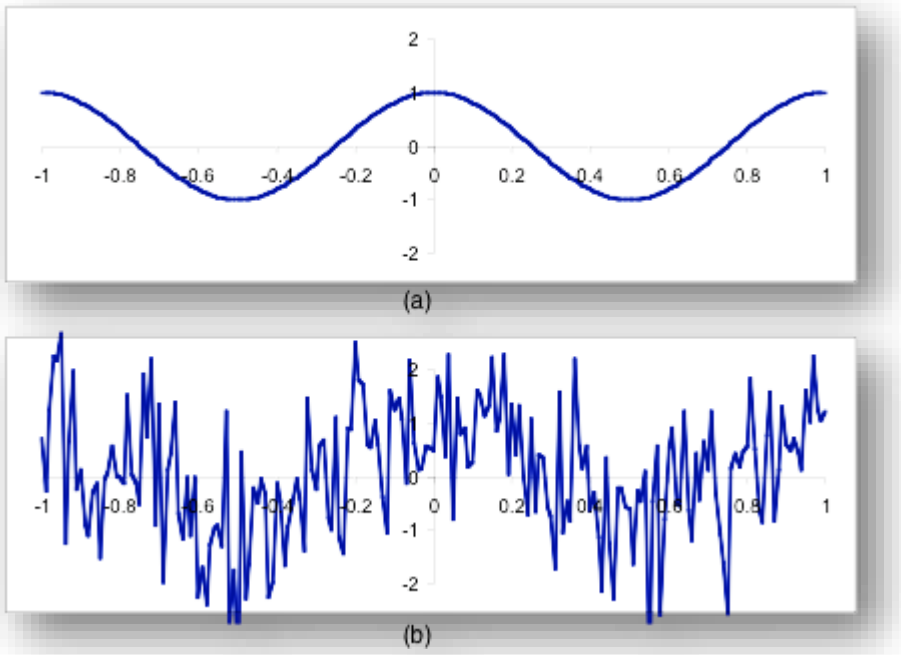
CIS 508: Lecture 5
Wireless & Mobile Networks

Lecturer: Sid C.K. Chau
Email: ckchau@masdar.ac.ae

Wireless Communication

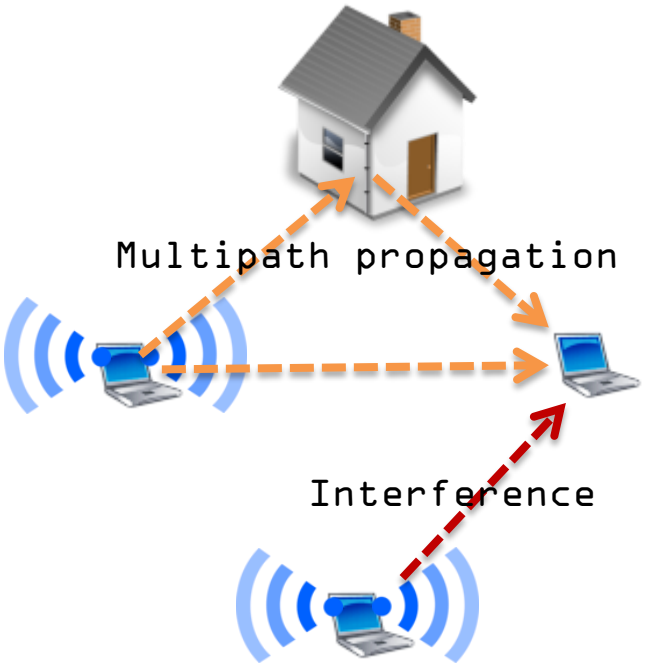
- Tough challenges:
  - ***Noise*** is present everywhere, significantly corrupting the information transmitted across wireless channel
  - ***Shared communication medium***: everyone in your neighborhood can be affected by your transmission (sometimes unawarely)
  - ***Limited spectrum***: usable wireless spectrum is restricted to certain frequency range
  - ***Mobility*** of end-users: wireless nodes are easy to deploy and convenient to move, creating dynamic network topology
  - ***Energy efficiency***: wireless communication is often battery-powered; high-powered antennas are hazardous
- But wireless communication is growing fast; too many important applications

Major Problem: Noise



- Noise is the biggest obstacle
- Electromagnetic wave has alot of background noise (known/unknown)
- Immerse efforts to combat noise to transmit information over wireless
- Other factors affecting reception
  - Antenna power
  - Data rate
  - Distance between transmitters
  - Interference

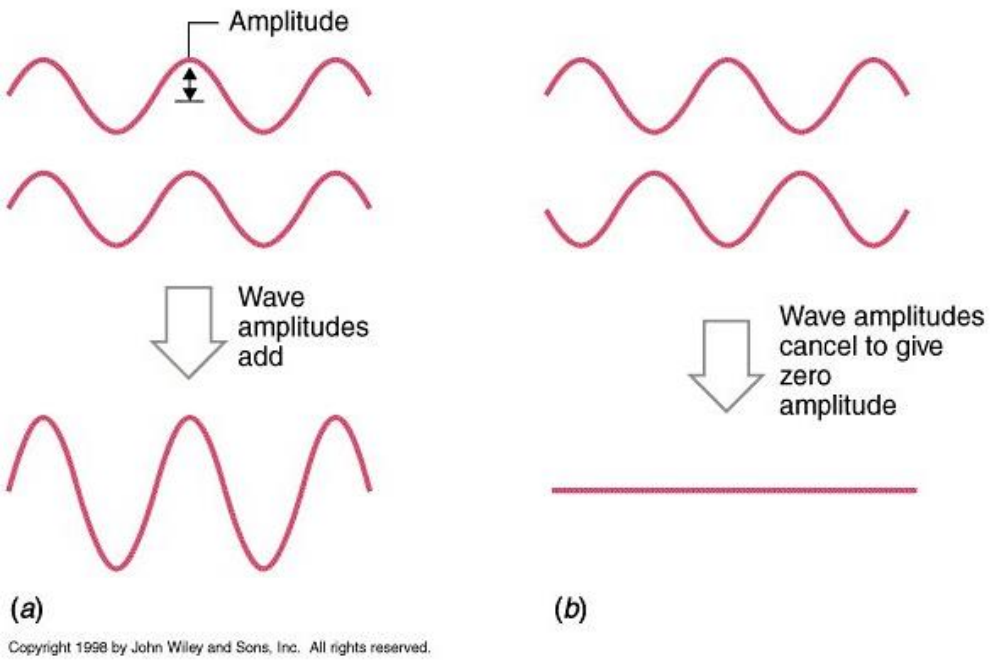
Wireless Link Characteristics



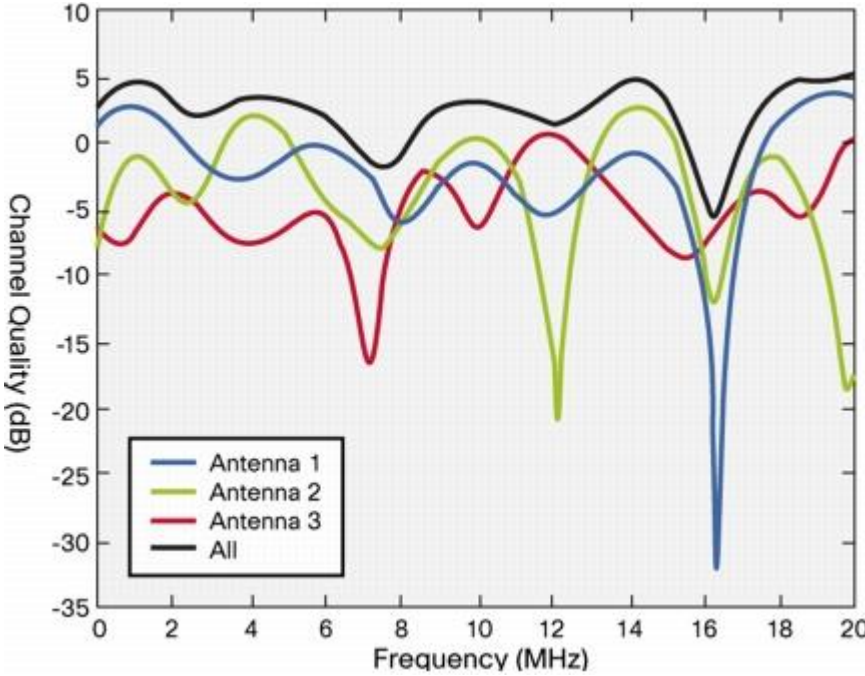
Wireless link is different substantially from wired link

- 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); devices (motors) interfere as well
- Multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

Wireless Link Characteristics

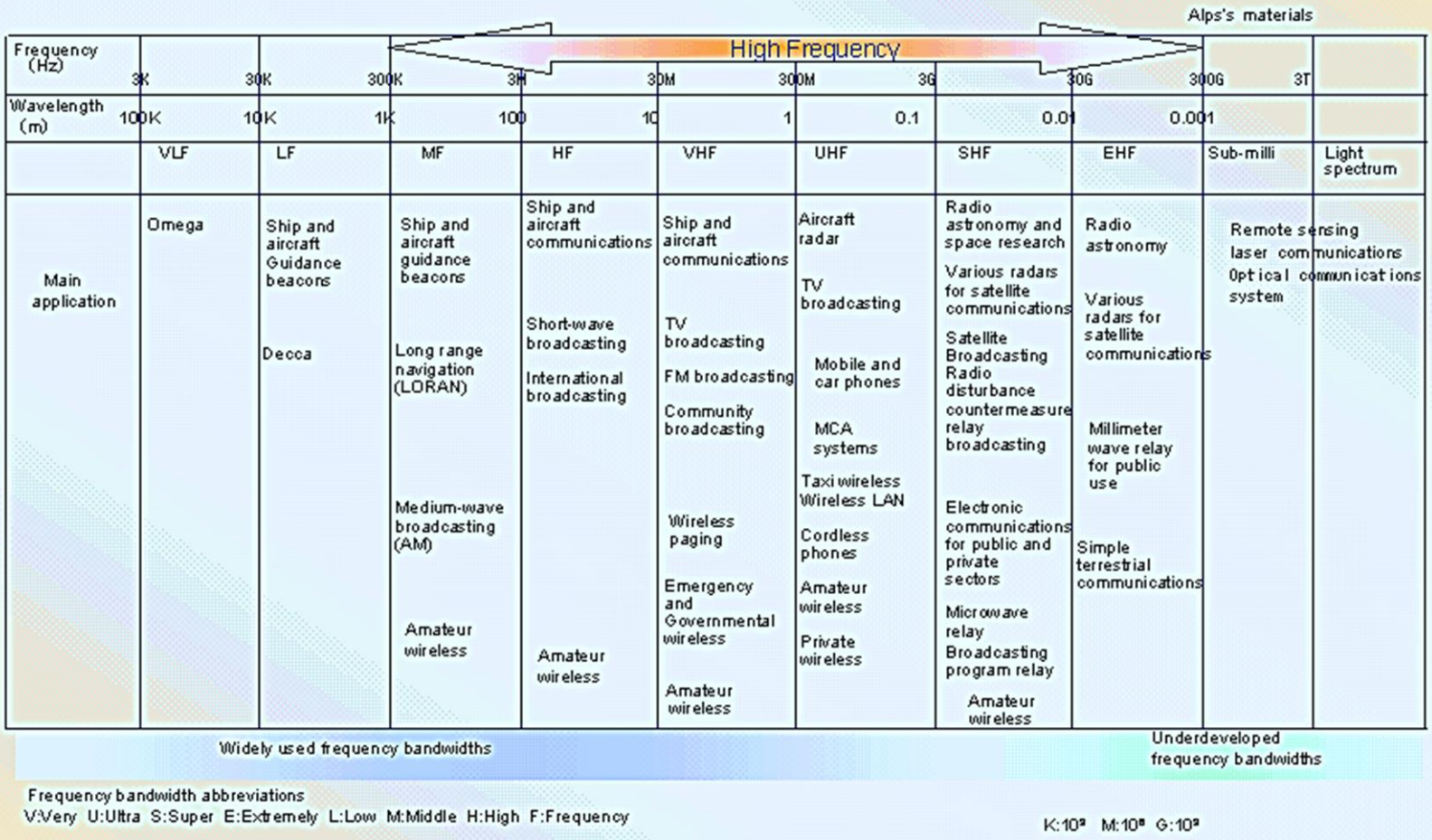


Constructive and destructive interference



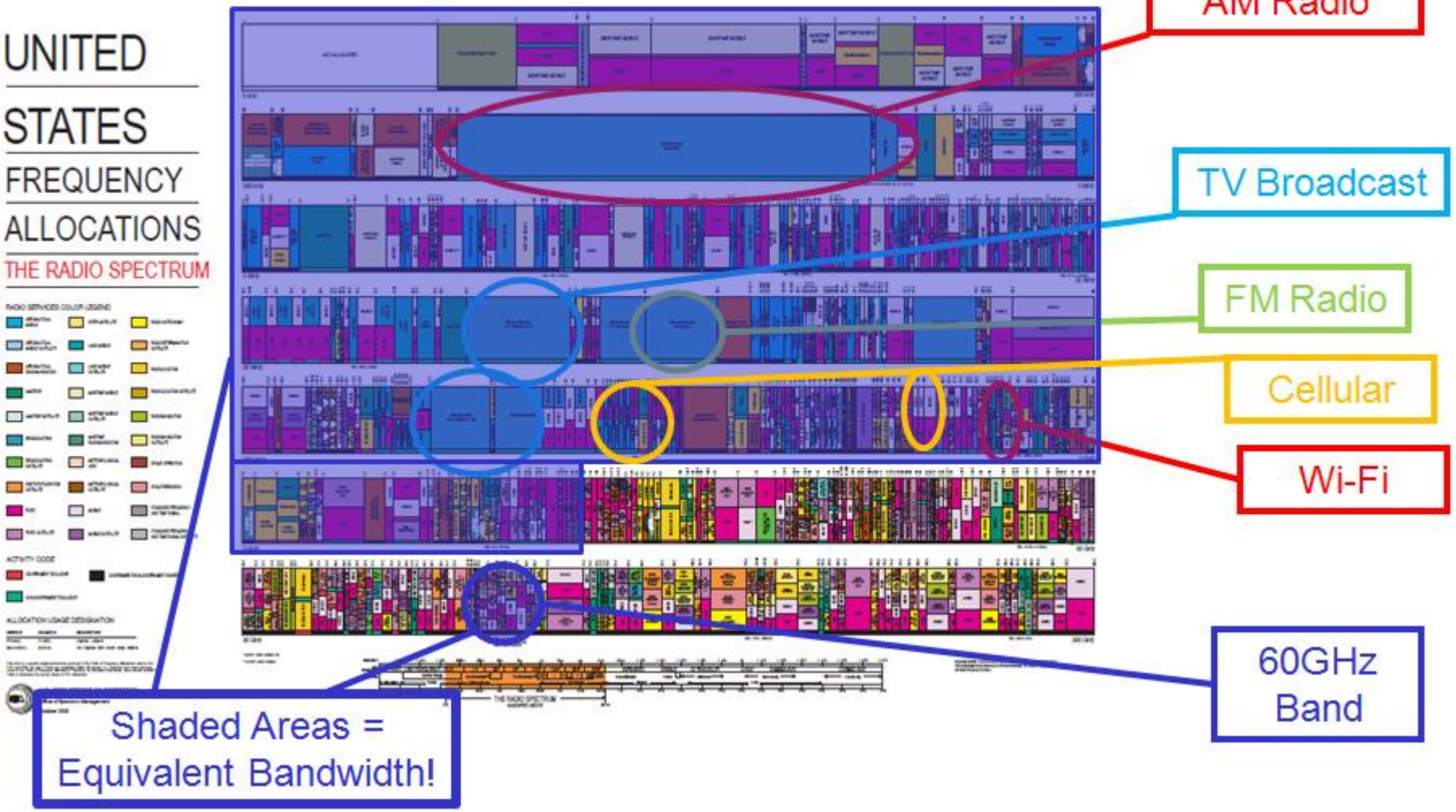
Variation of Signal Quality from Constructive and Destructive Interference

Applications of Frequency Spectrum

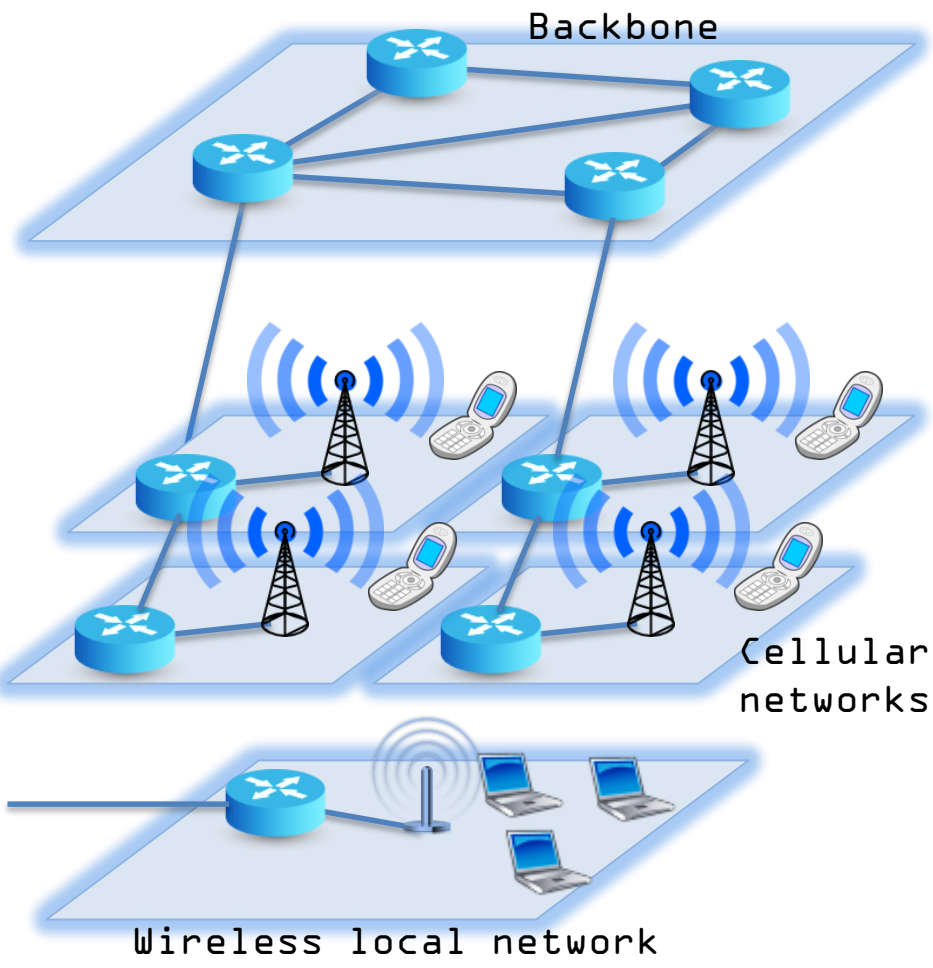


Spectrum Allocation

- Bandwidth can be imagined as real estate

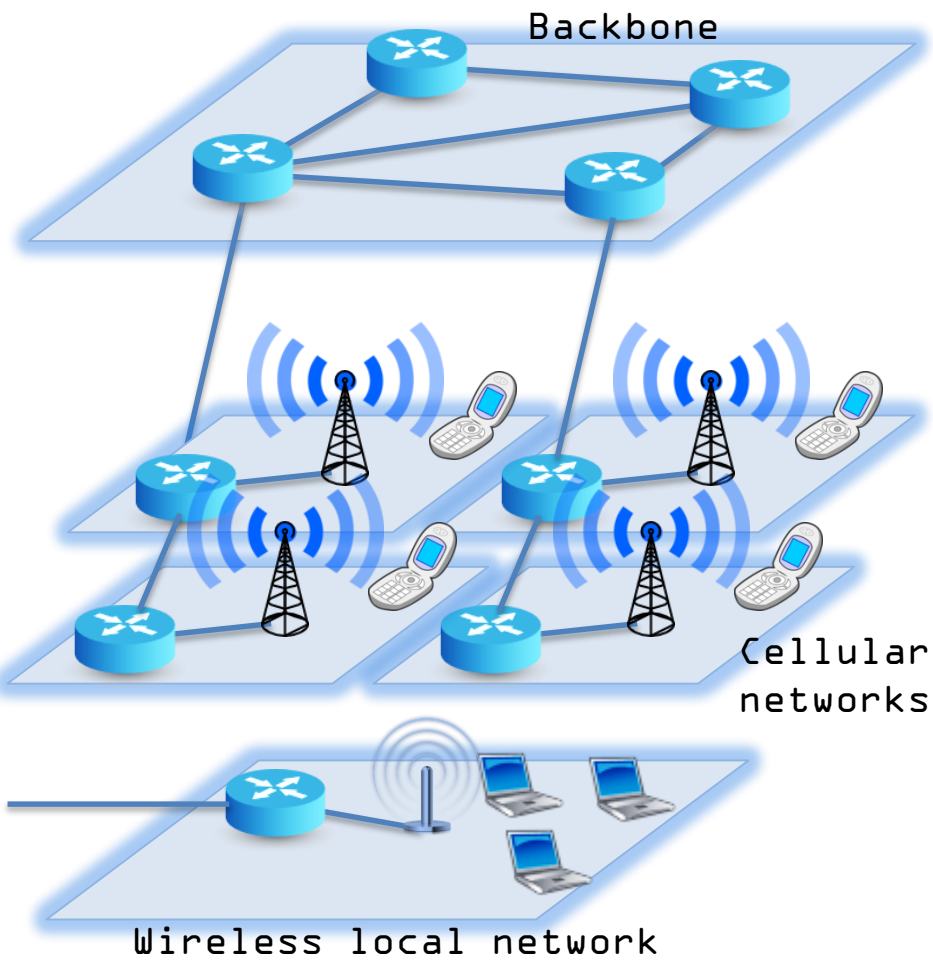


Mobile Network Architecture



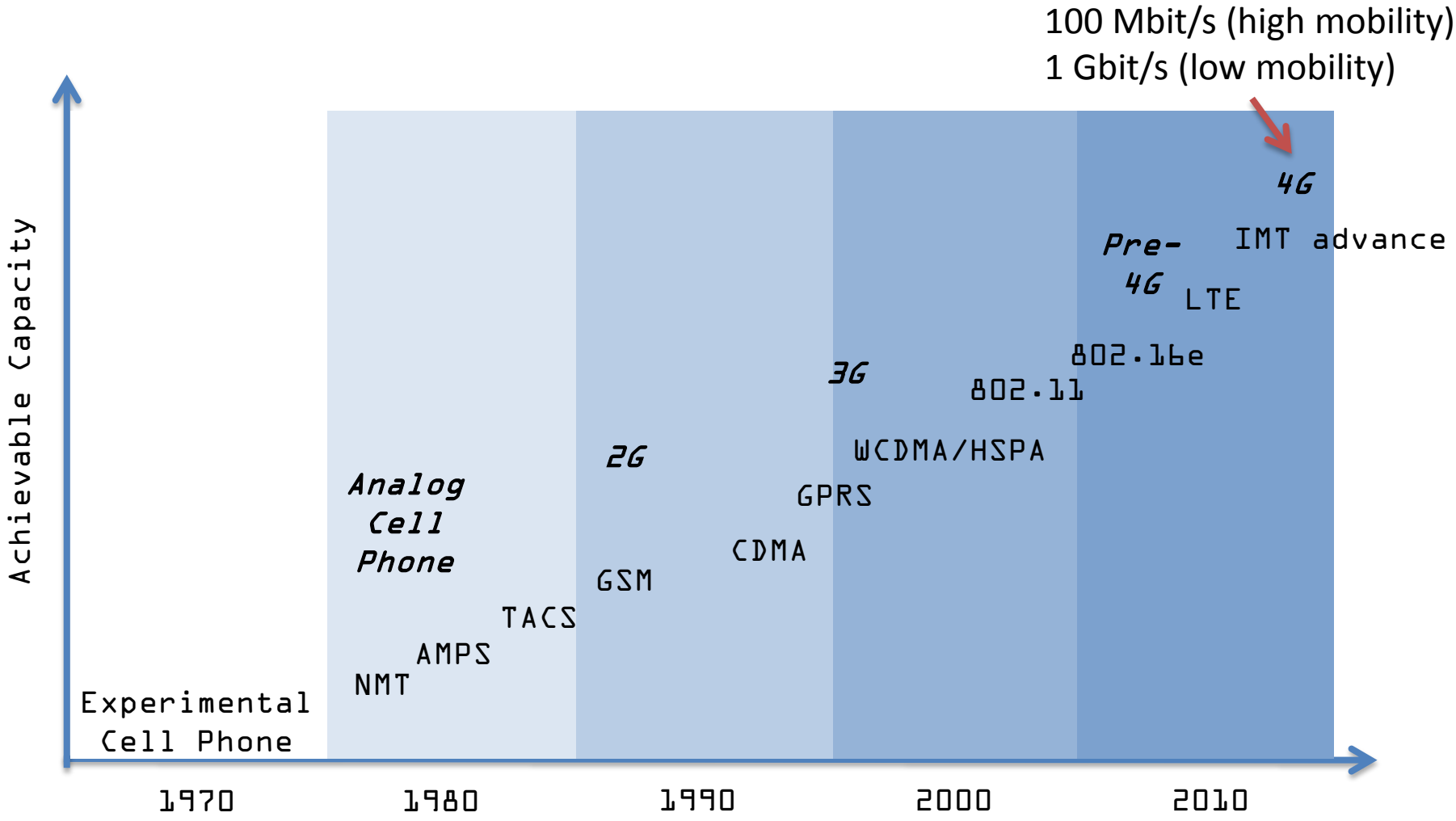
- Wireless hosts
  - Laptops, smartphones, tablets
  - Stationary (non-mobile) or mobile
- Base stations
  - Typically connected to wired network
  - As a relay, responsible for sending packets between wired network and wireless host(s) in its “area”
    - E.g., cell towers, 802.11 access points

Mobile Network Architecture

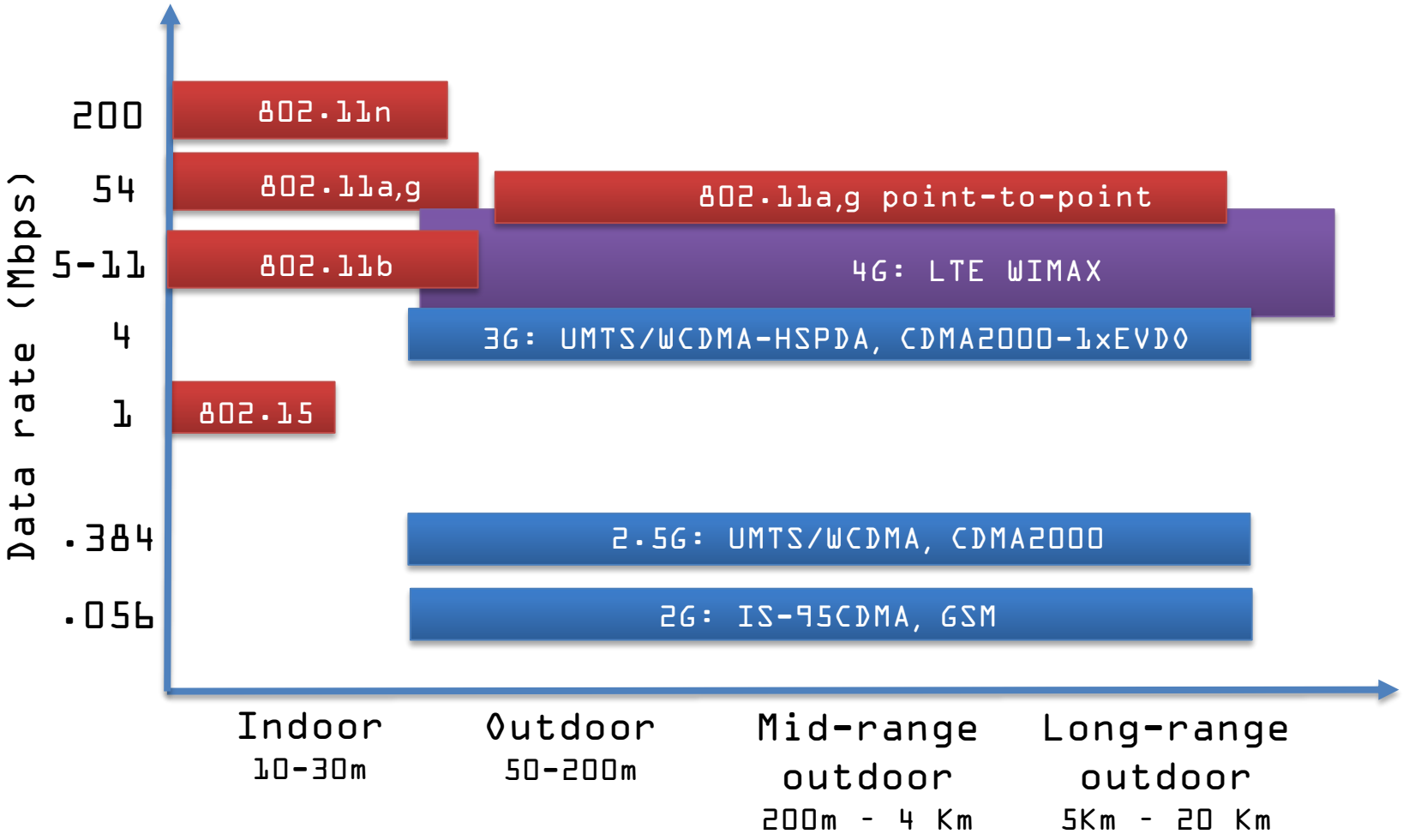


- Wireless links
  - Typically used to connect mobile(s) to base station
  - Also used as backbone link
  - Multiple access protocol coordinates link access
  - Variable data rates, transmission distance
- Infrastructure modes
  - Base station connects mobiles into wired network
  - Handoff: mobile changes base station providing connection into wired network

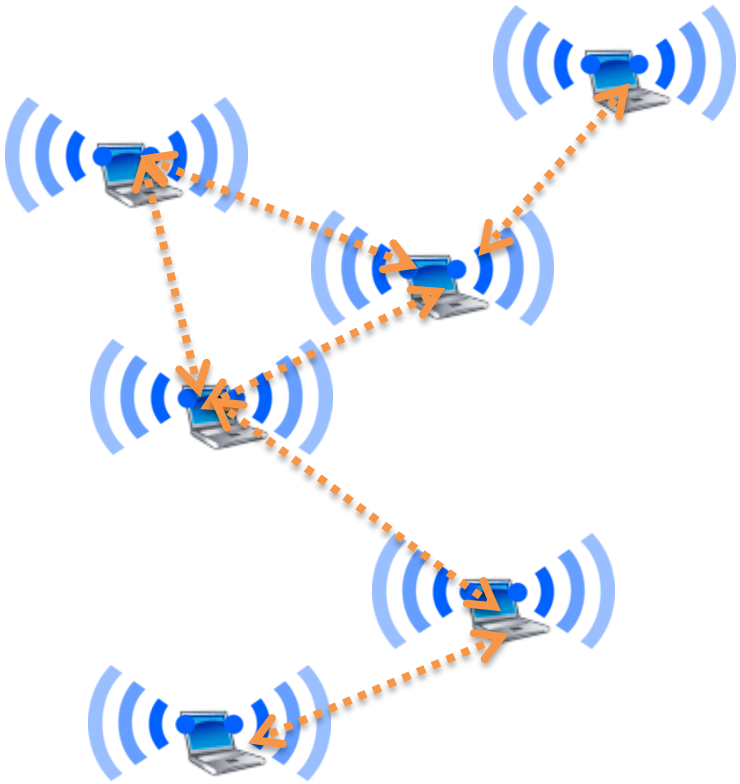
Evolution of Standards



Wireless Communication Standards



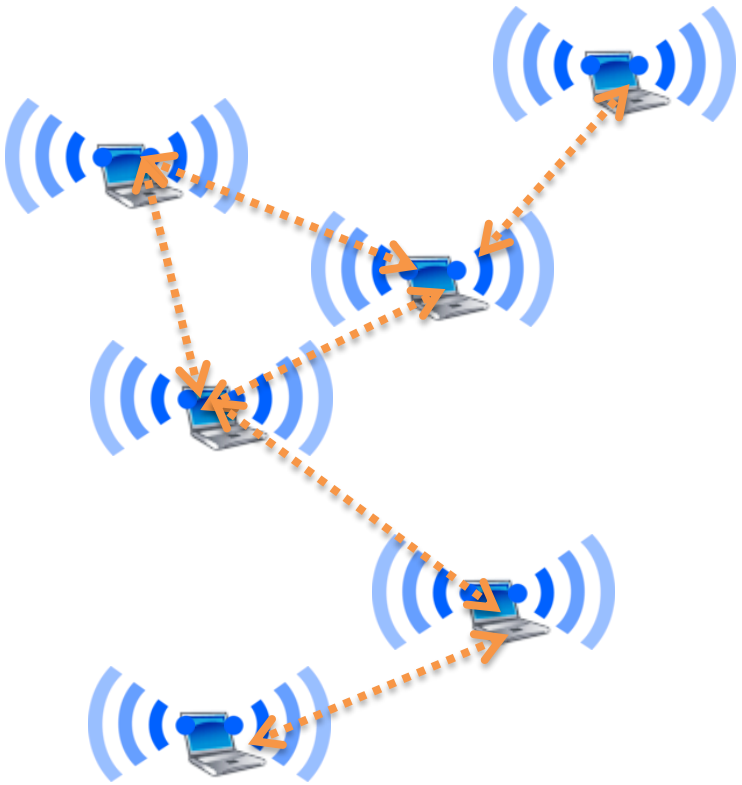
Wireless Ad hoc Networks



Wireless ad hoc network

- Decentralized and self-organizing networks
- No pre-existing Infrastructure support
  - No base stations
  - Nodes can only transmit to other nodes within link coverage
  - Nodes organize themselves into a network, manage route among themselves
- Very challenging problem
  - Too dynamic
  - Too little a-priori information about network state
  - Too few controlling mechanisms

Wireless Ad hoc Networks



Wireless ad hoc network

- Applications
  - Military networks (soldiers, UAVs)
  - Vehicular networks (among cars)
  - Sensor networks (ad hoc deployed)
  - Emergency networks
- A lot of academic results
  - Few implemented wireless ad hoc networks
  - Except military networks

Wireless Network Taxonomy

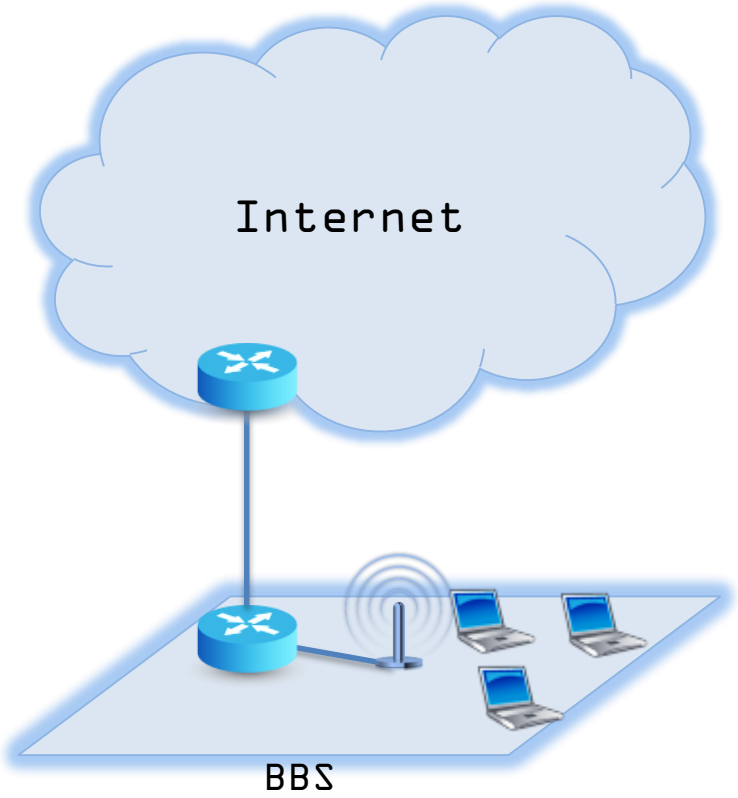
	Single hop	Multiple hops
Infrastructure (e.g., APs)	Host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	Host may have to relay through several wireless nodes to connect to larger Internet: mesh net
No infrastructure	No base station, no connection to larger Internet (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

IEEE 802.11 (Wi-Fi/Wireless LAN)

- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - Up to 11 Mbps
- 802.11g
  - 2.4-5 GHz range
  - Up to 54 Mbps
- 802.11n:
  - Multiple antennas
  - 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

802.11 LAN Architecture

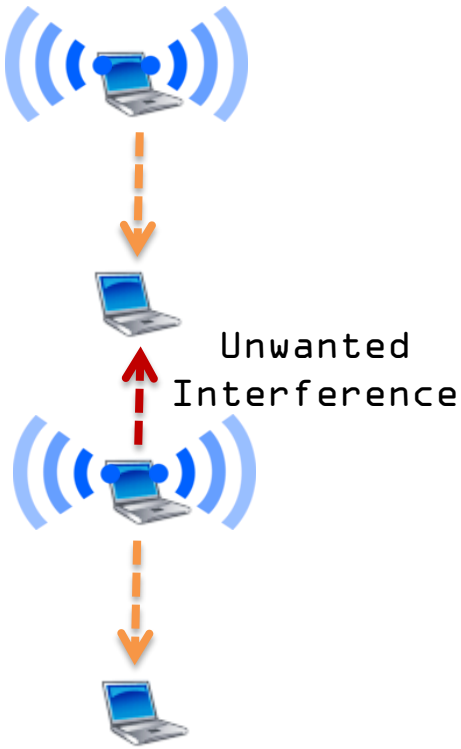


- Wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (known as “cell”) in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP):
    - Base station
  - Ad hoc mode
    - Hosts only

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
  - Will typically run DHCP to get IP address in AP's subnet

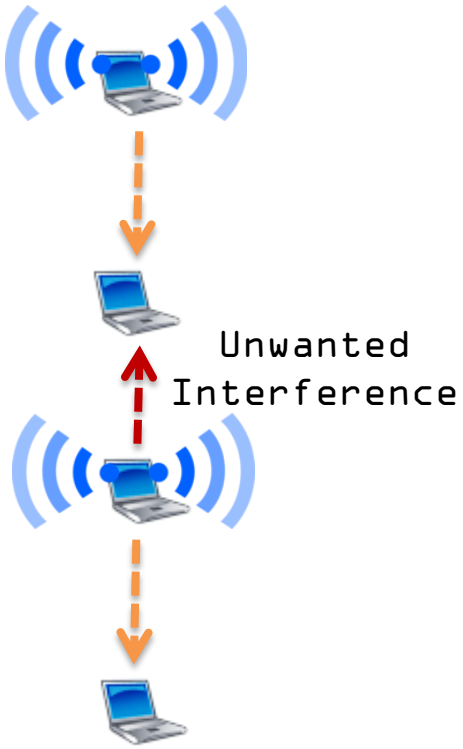
Hidden Terminal Problem



Hidden terminal problem: a major problem in wireless networking

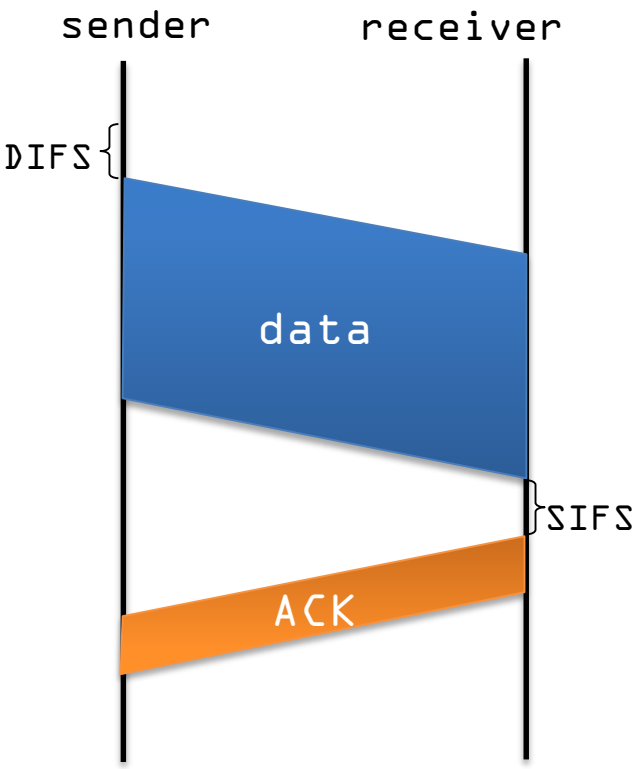
- Wireless is a broadcasting medium
- A node transmitting to its targeted receiver can also generate interference to other untargeted nodes receiving data from an invisible node
- A prominent problem if wireless nodes are closely placed in a region

802.11: Multiple Access



- Avoid collisions: More than two nodes transmitting at same time
- Sensing channel before transmitting
  - Not to collide with ongoing transmission by other node
- *No* collision detection
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Cannot sense all collisions in any case: hidden terminal, fading
  - Goal: *avoid collisions*
    - CSMA/C(ollision)A(voidance)

802.11 MAC: CSMA/CA



Sender

1. If sense channel idle for DIFS then

   transmit entire frame (no CD)

2. If sense channel busy then

   start random back-off time

   timer counts down while channel idle

   transmit when timer expires

   if no ACK, increase random back-off interval, repeat 2

Receiver

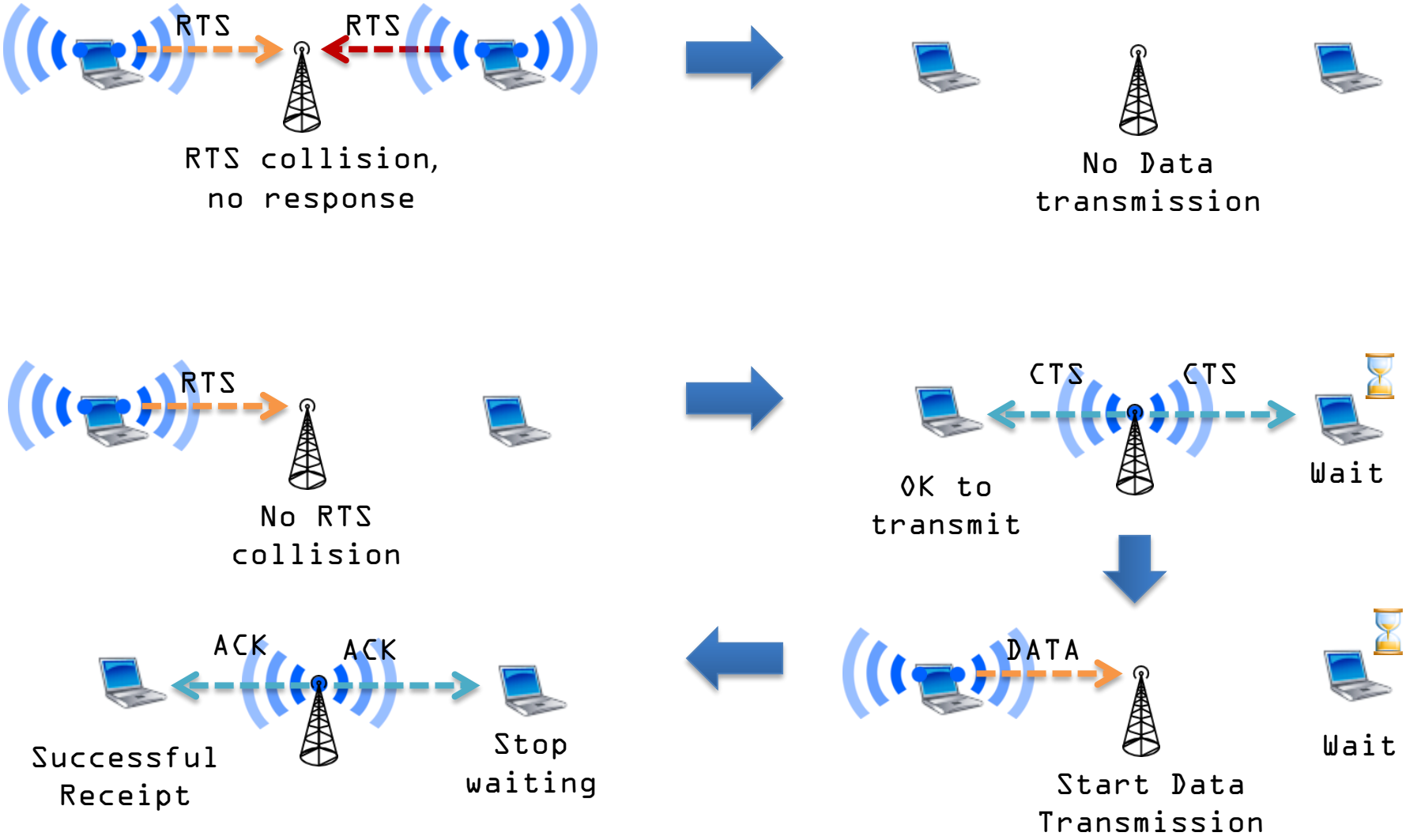
- If frame received OK

  return ACK after SIFS (ACK needed due to hidden terminal problem)

802.11: Collisions Avoidance

- How to resolve hidden terminal problem:
- Basic idea: allow sender to “reserve” channel rather than random access of 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 until hearing ACK

Collision Avoidance: RTS-CTS



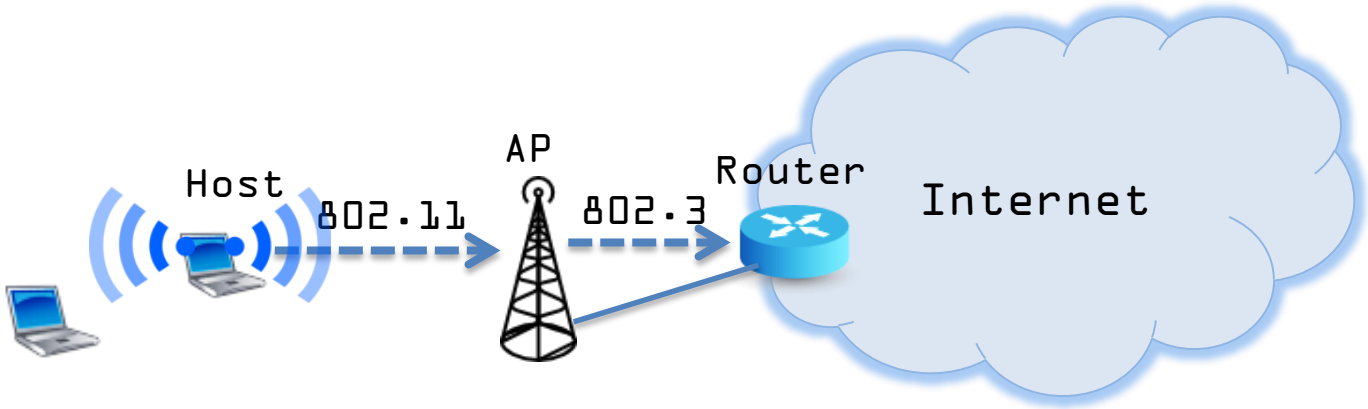
802.11 Frame

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

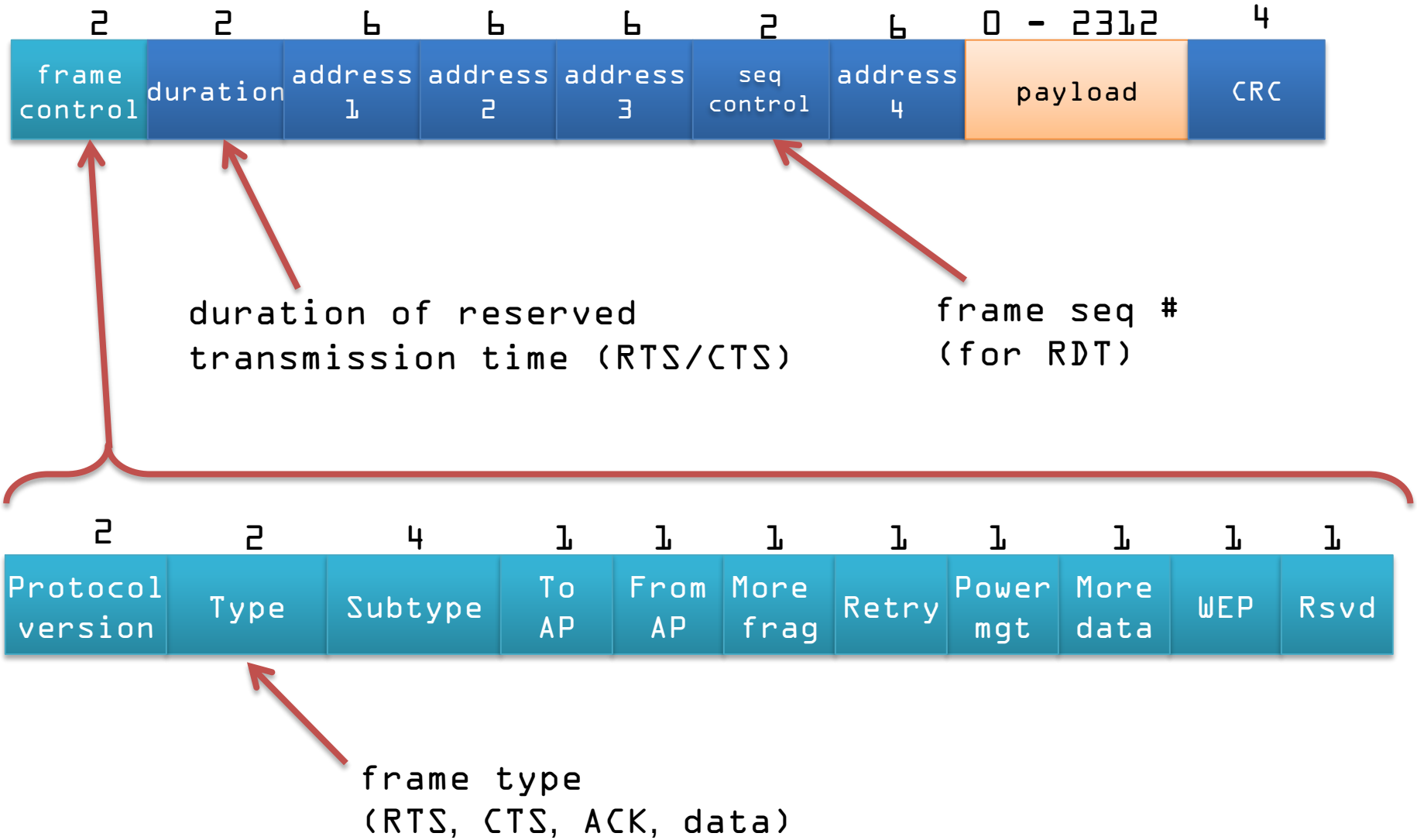
Address 2: MAC address of wireless host or AP transmitting this frame

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

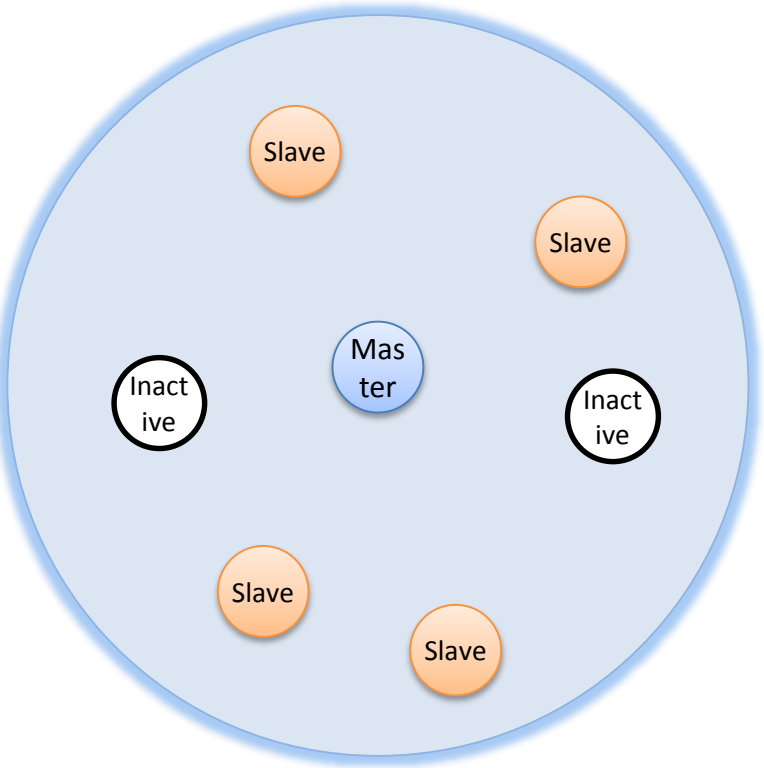
Address 4: used only in ad hoc mode



802.11 Frame


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
duration of reserved transmission time (RTS/CTS)
frame seq # (for RDT)
2
2
4
1
1
1
1
1
1
1
1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power mgt
More data
WEP
Rsvd
frame type (RTS, CTS, ACK, data)

IEEE 802.15 (PAN)

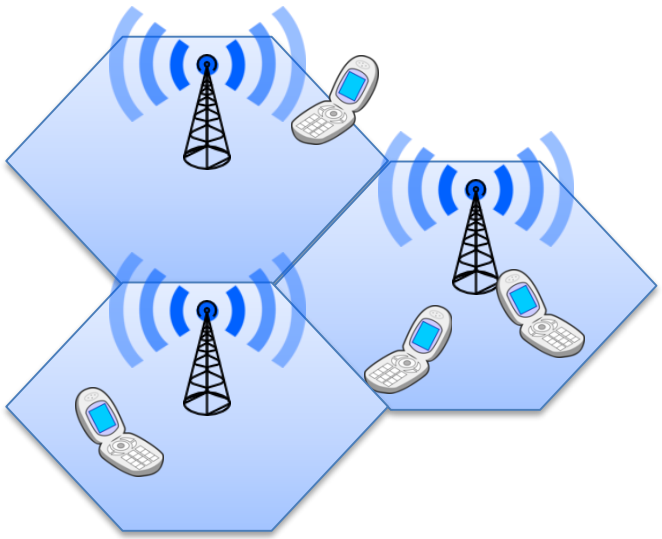


- Wireless personal area networks
  - Less than 10 m diameter
  - Replacement for cables
    - E.g. mouse, keyboard, headphones
  - Ad hoc: no infrastructure
  - Master/slaves:
    - Slaves request permission to send (to master)
    - master grants requests
  - 802.15: evolved from Bluetooth specification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

IEEE 802.16 (WiMax)

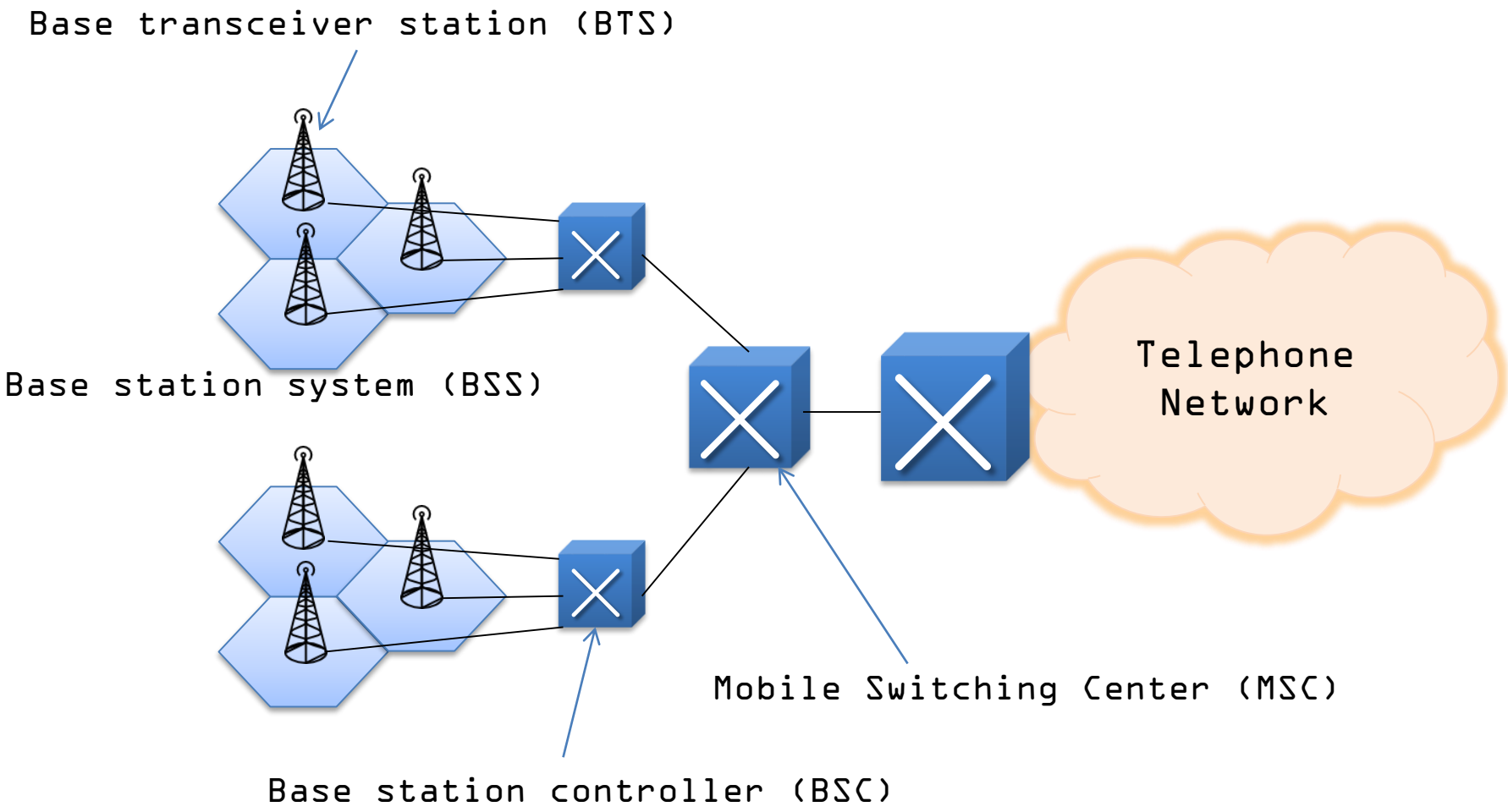
- WiMAX (Worldwide Interoperability for Microwave Access)
  - "Super enhanced Wi-Fi"
  - Up to 1 Gbit/s
  - Competing standard for 4G mobile network
  - Allow hand-over across multiple wireless LAN
  - Support mobility
  - Sprint deployed WiMAX as 4G mobile network in USA

Basic of Mobile (Cellular) Networks

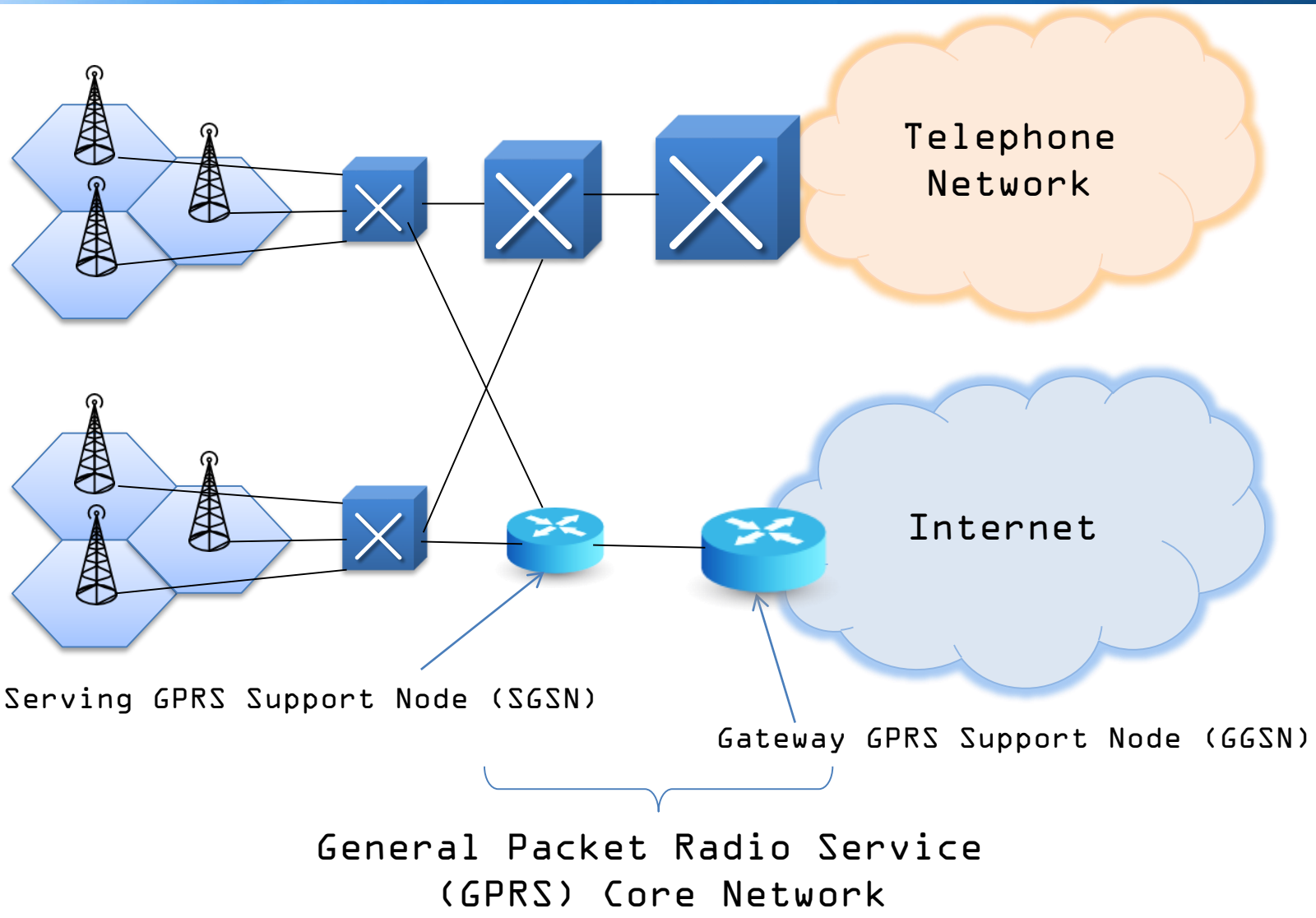


- Cell
  - Basic unit of mobile networks
  - Covers geographical region
  - Base station (BS) analogous to 802.11 AP
  - Mobile users attach to network through BS
  - Air-interface: physical and link layer protocol between mobile and BS
- Connects cells to wired tel. net.
- Manages call setup
- Handles mobility

2G (voice) Network Architecture



3G (data) Network Architecture



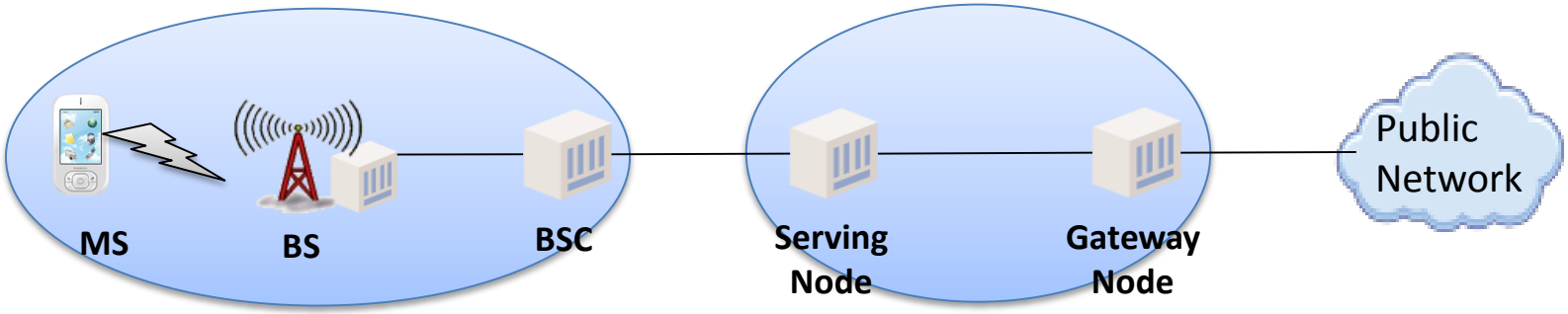
Mobility

- High mobility
  - Mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)
- Routing solution
  - 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
- End-systems solution
  - 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

4G Mobile Networks

- Promising peak speed 100 Mbit/s for high mobility communication and 1 Gbit/s for low mobility communication
- Standards
  - 3GPP: LTE, LTE-Advanced, IMT-Advanced
    - Backed by traditional GSM Telco equipment makers
  - IEEE 802.16m, WiMax
    - Backed by IP network equipment makers
- Advances
  - Higher data rate coding: OFDM
  - Multiple antennas: MIMO
  - Improved network architecture

3G (Cellular Network)



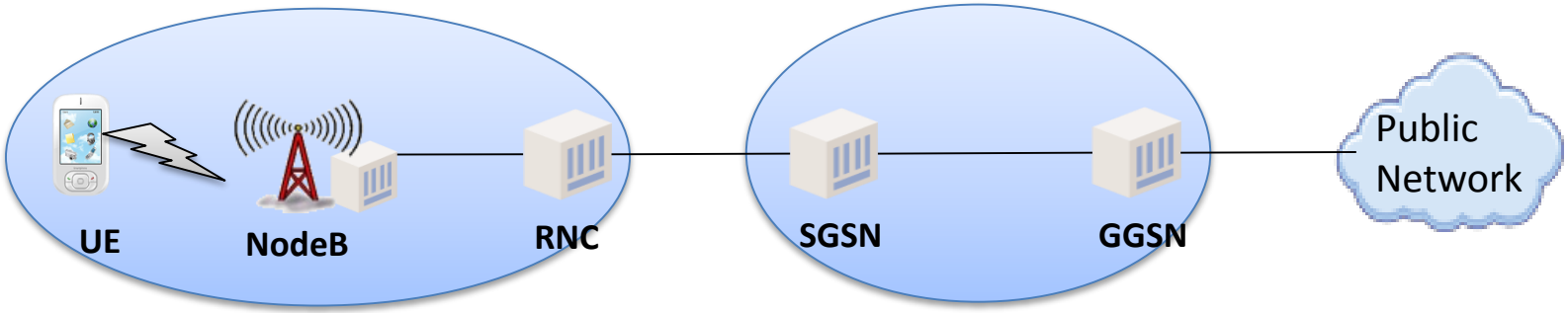
Radio Access Network

- Physical layer
  - Coding, interleaving, modulation, etc.
- Link layer
  - Multi-access, ARQ, header compression
- Radio resource management
  - Handover, power control, interference
- Security
  - Ciphering, data integrity

Core Network

- Subscriber management
- Session management
- Charging and policy control
- Mobility management
- Authentication, Key management
- Connection to external network

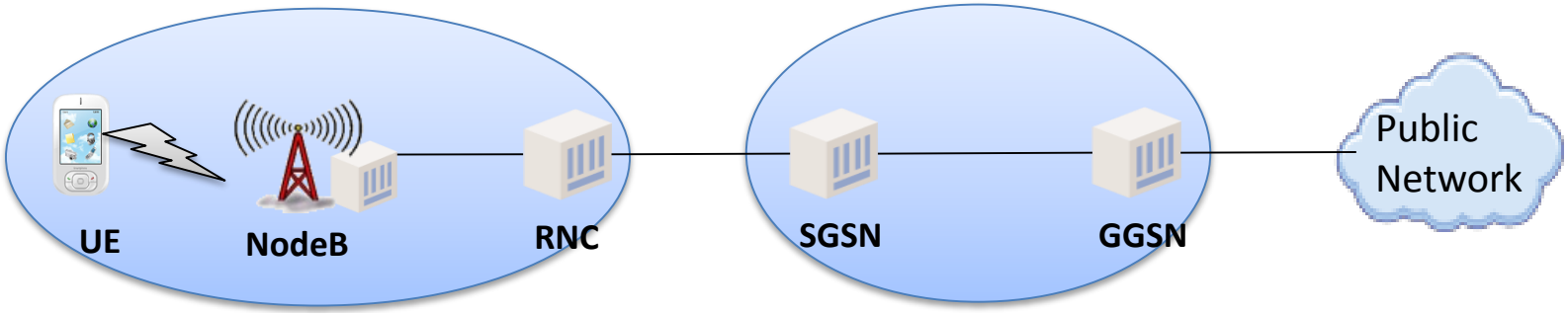
4G (Cellular Network)



Radio Access Network **Core Network**

	Radio Access Network (RAN)			Core Network (CN)		
	3GPP	3GPP2	WiMax	3GPP	3GPP2	WiMax
2G	GPRS (GSM)		N/A	GPRS	PDSN	N/A
	EDGE	CDMA2000				
3G	WCDMA	EVDO				
	HSPA	EVDO Rev.B				
4G	LTE		WiMax	EPC		MIP
	LTE-advanced					

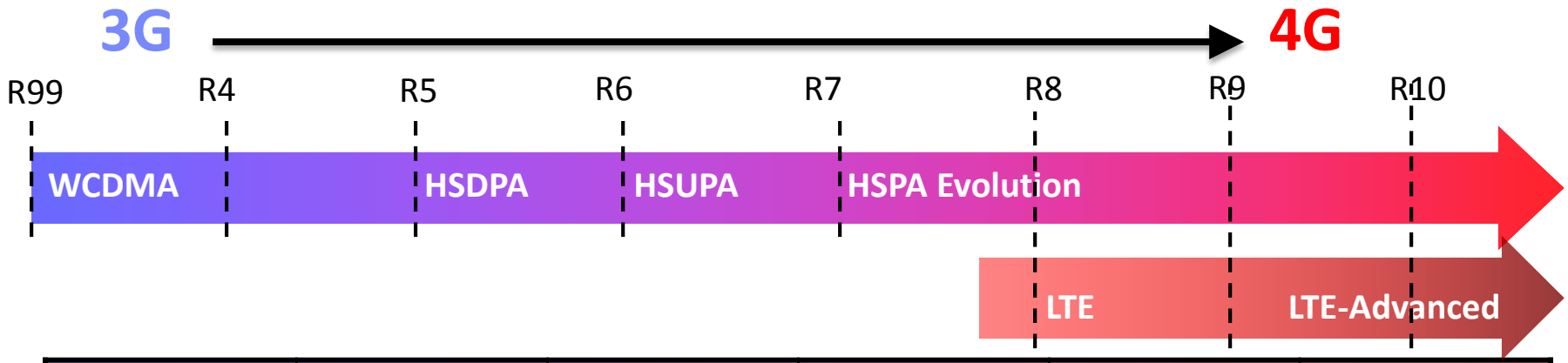
4G (Cellular Network)



GPRSc	MS	BTS	BSC	SGSN	GGSN
WCDMA (3GPP)	**UE**	**NodeB**	**RNC**	**SGSN**	**GGSN**
LTE/EPC	**UE**	**eNodeB**		**S-GW**	**PDN GW**
cdma2000	MS	BTS	BSC/PCF	PDSN(FA)	HA
WiMAX	MS	BS		ASN-GW(FA)	CSN(HA)

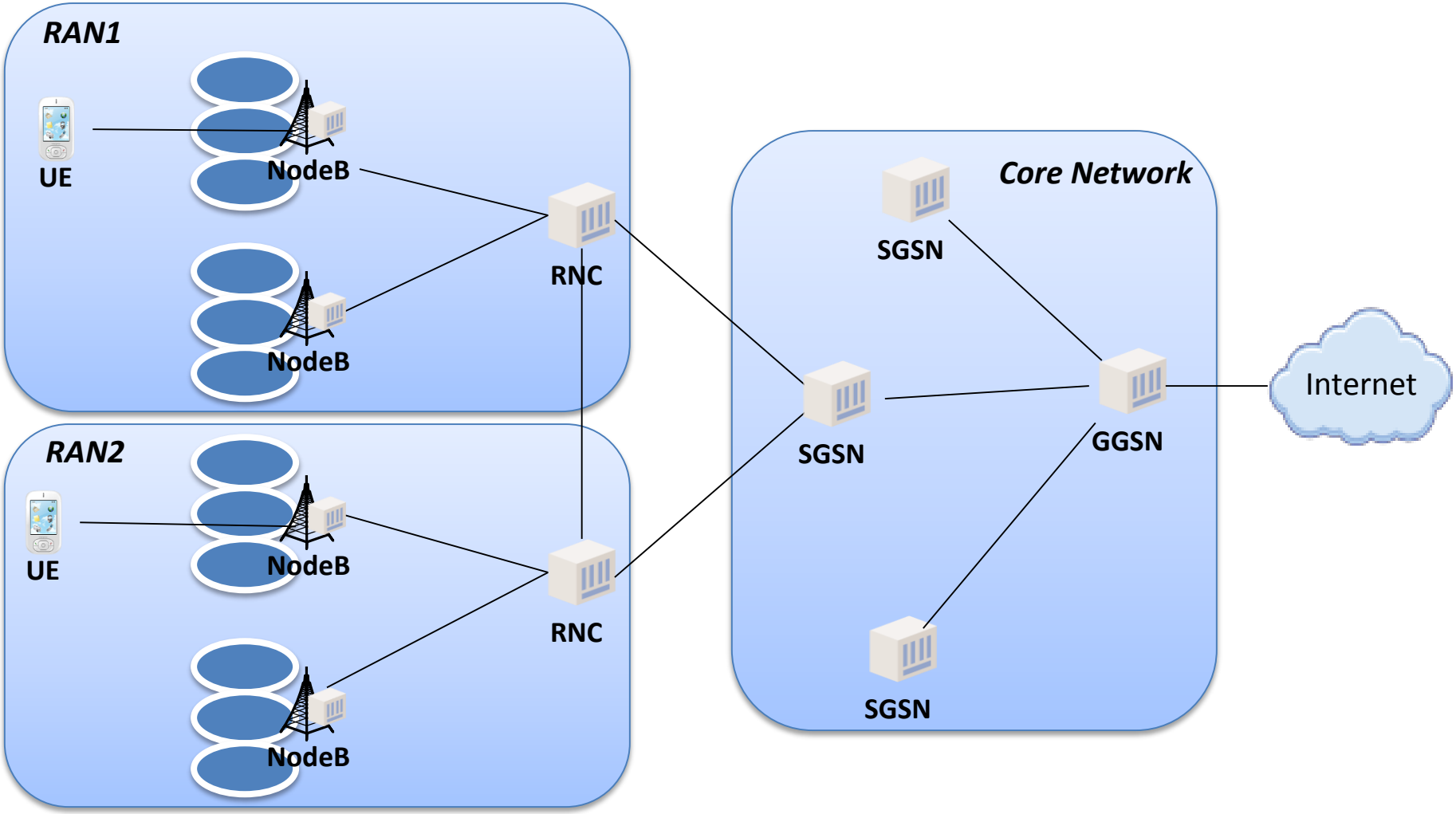
- UE: User Equipment
- RNC: Radio Network Controller
- SGSN: Serving GPRS Support Node
- GGSN: Gateway GPRS Support Node
- UMTS: Universal Mobile Telecommunication System
- eNodeB: Enhanced NodeB
- S-GW: Serving Gateway
- PDN GW: Public Data Network (PDN) Gateway
- LTE: Long Term Evolution
- EPC: Evolved Packet Core

3GPP RAN Technology Evolution



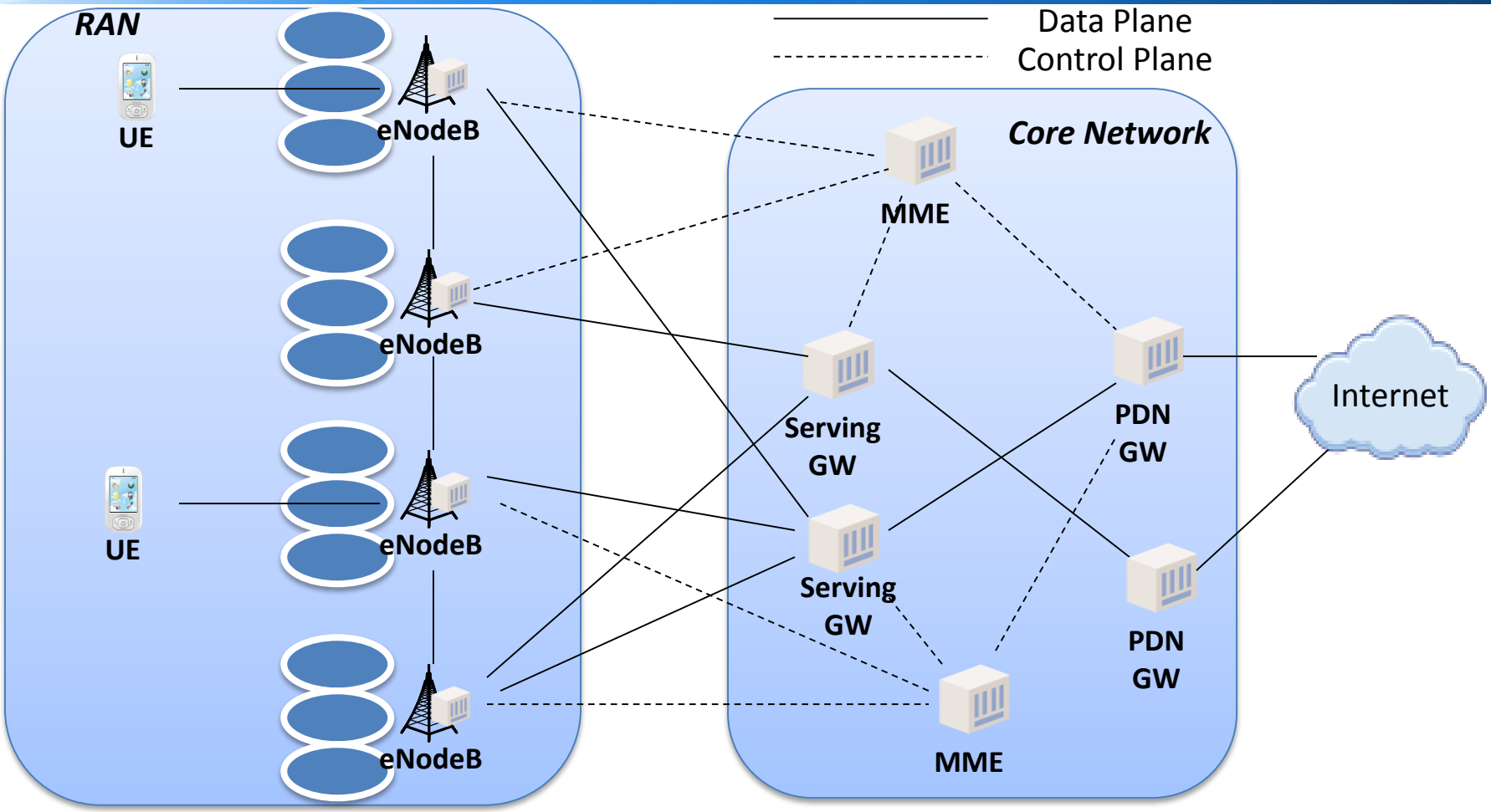
WCDMA	HSDPA	HSUPA	HSPA Evolution	LTE	LTE Advanced
2 Mbps DL 769 kbps UL	14.4 Mbps DL	5.76 Mbps UL	28Mbps DL 11Mbps UL	300 Mbps DL 70 Mbps UL	1.2 Gbps DL 568 Mbps UL
DS-CDMA (5 MHz)	Fast scheduling Rate control 16 QAM H-ARQ	Fast scheduling H-ARQ	64 QAM DL 16 QAM UL MIMO CPC (Continuous Packet Connectivity)	**OFDM** Carrier aggregation (20 MHz) 4x4 MIMO DL	Carrier aggregation (100 MHz) Co-ordinated Multi-Point Inter-cell Interference coordination

3G Hierarchical Network Architecture



- Network entities are connected to each other through static binding.

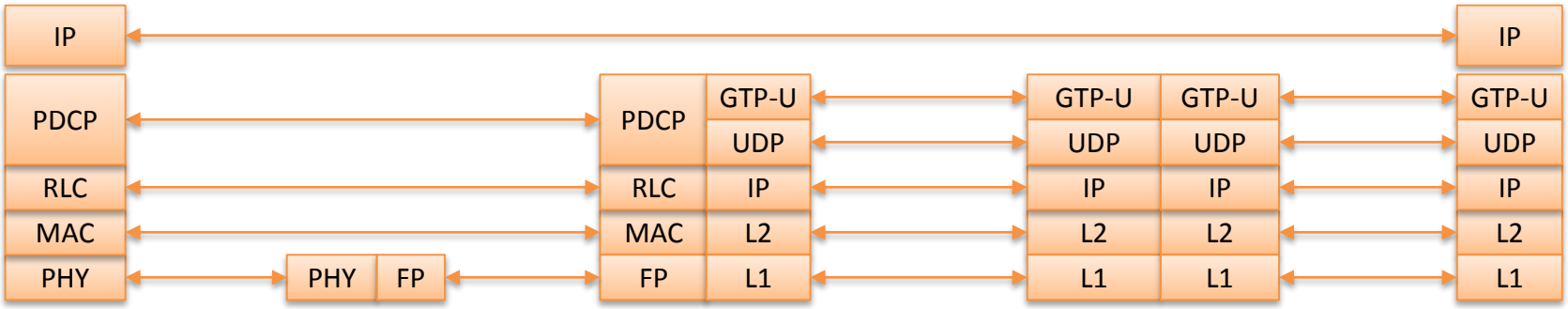
4G "Flat" Network Architecture



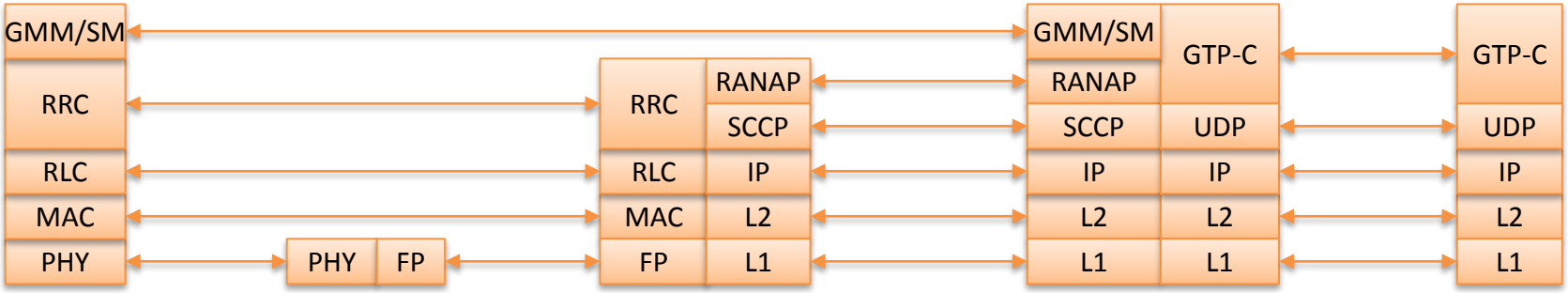
- Network entities are selected on-the-fly for each user separately
- Control-plane and data-plane entities are separated in CN

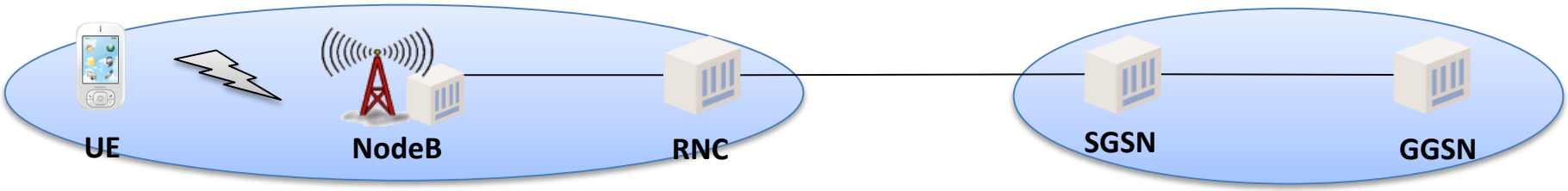
Protocol Architecture (3G/UMTS)

Data plane



Control plane

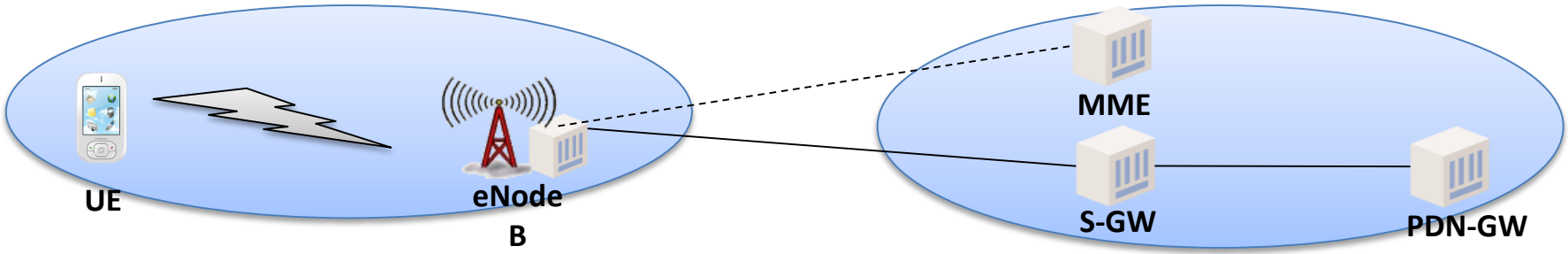




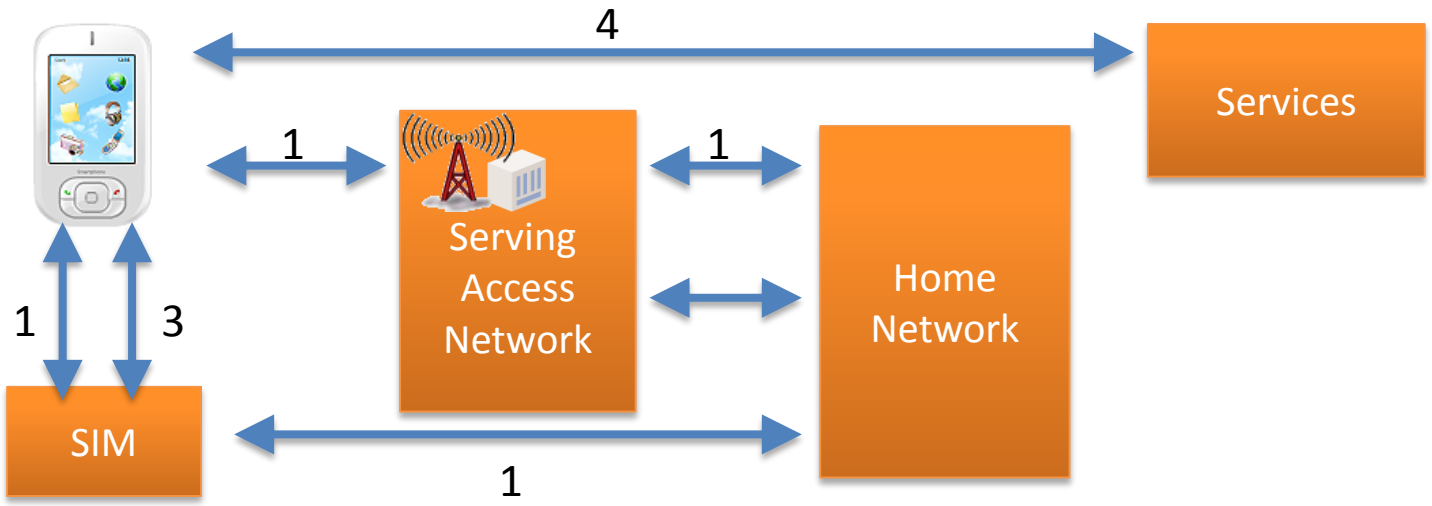
Protocol Architecture (4G/LTE)

Data plane

Control plane



Security Domains



1. Network access security
   - Protection of signaling and user traffic: encryption and integrity protection
2. Network domain security
   - Hop-by-hop secure exchange of data between network entities
3. User domain security
   - Secure access to the terminal
4. Application domain security
   - Application level (end-to-end) security (e.g., HTTPS)