Wireless Network Security and Privacy

Wireless Network Basics

Xiaoyu Ji 冀晓宇

Department of Electrical Engineering
Zhejiang University

2024 Autumn

Outline

- Network Basics
  - A high level perspective
- Wireless Fundamentals
  - Important Terms
  - Modulation
  - MAC layer
  - Physical layer
- Popular standards and the corresponding wireless networks:
  - 802.11 Wi-Fi
  - 802.15 Bluetooth
  - 802.15 Zigbee
  - 5G☺☹
- New emerging wireless communications and applications
  - 60G Hz
  - Li-Fi
  - Low power wide area network: NB-IoT, Lora

Part 1： Network Basics

What's the Internet: "nuts and bolts" view

PC

server

wireless laptop

cellular handheld

access points

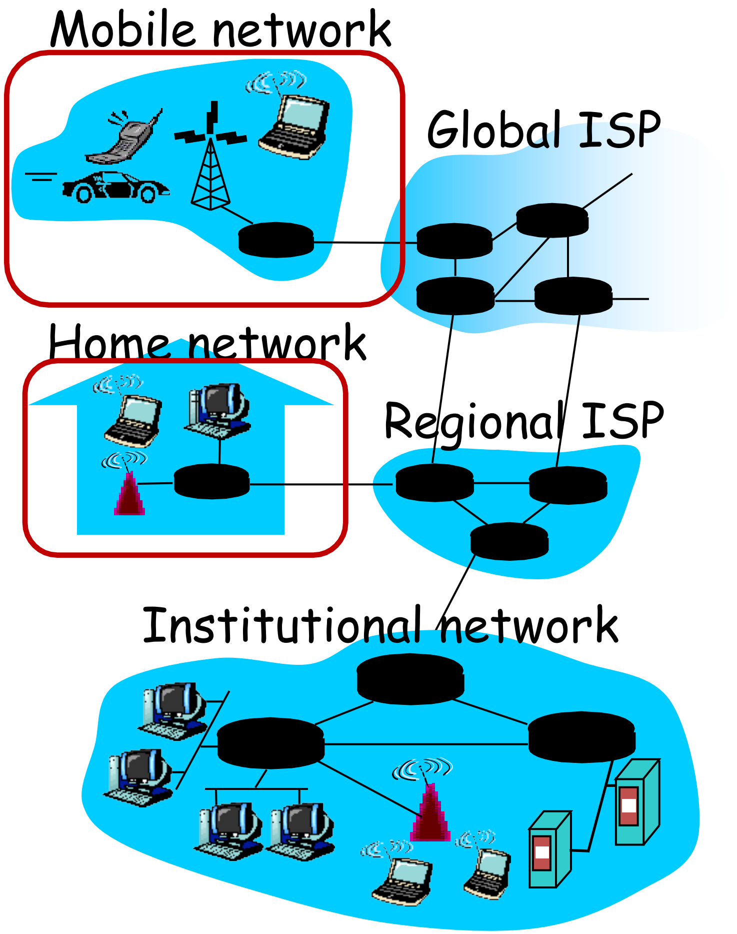
—— wired links

● router

- millions of connected computing devices:
  - *hosts = end systems*
  - running *network apps*

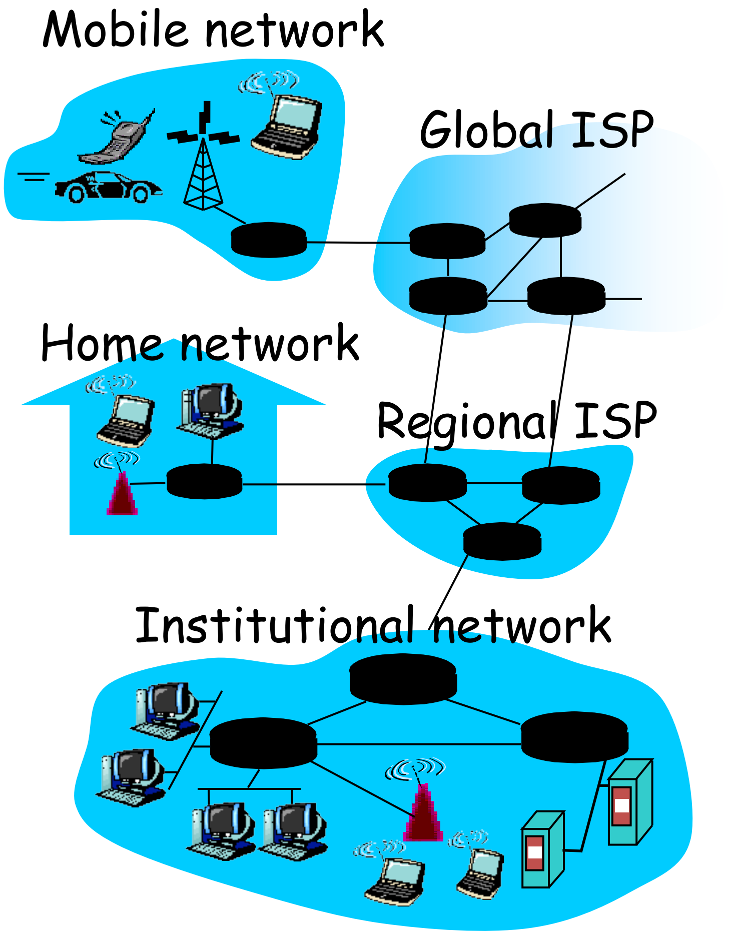
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = *bandwidth*

- *routers:* forward packets (chunks of data)



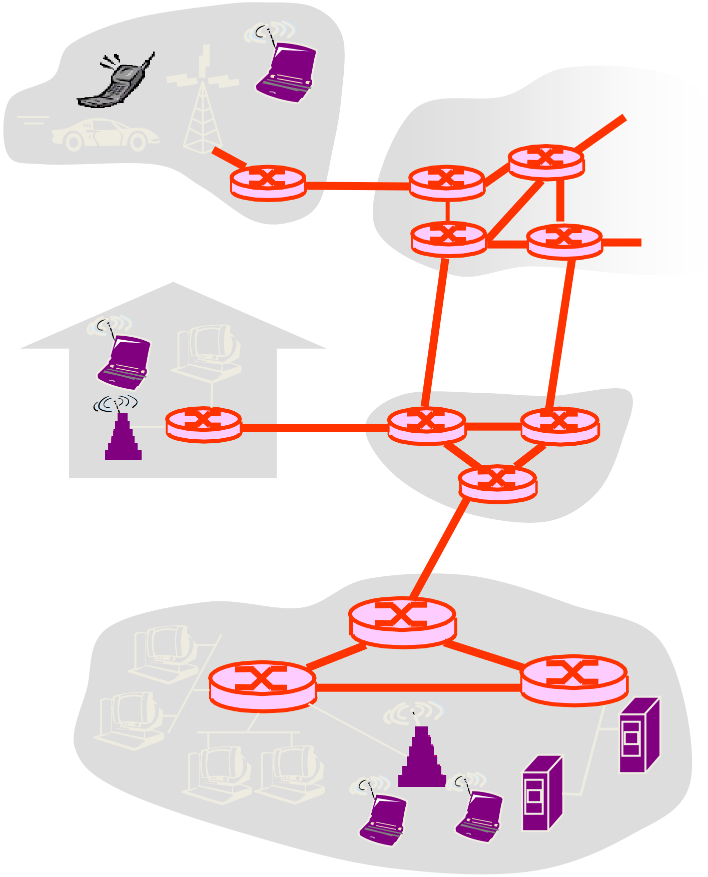
What's the Internet: "nuts and bolts" view

- *protocols* control sending, receiving of messages
  - e.g., TCP, IP, HTTP, Skype, Ethernet
- *Internet:* "network of networks"
  - loosely hierarchical
  - public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



The Network Core

- mesh of interconnected routers
- *the* fundamental question: how is data transferred through net?
  - circuit switching: dedicated circuit per call: telephone net
  - packet-switching: data sent thru net in discrete “chunks”

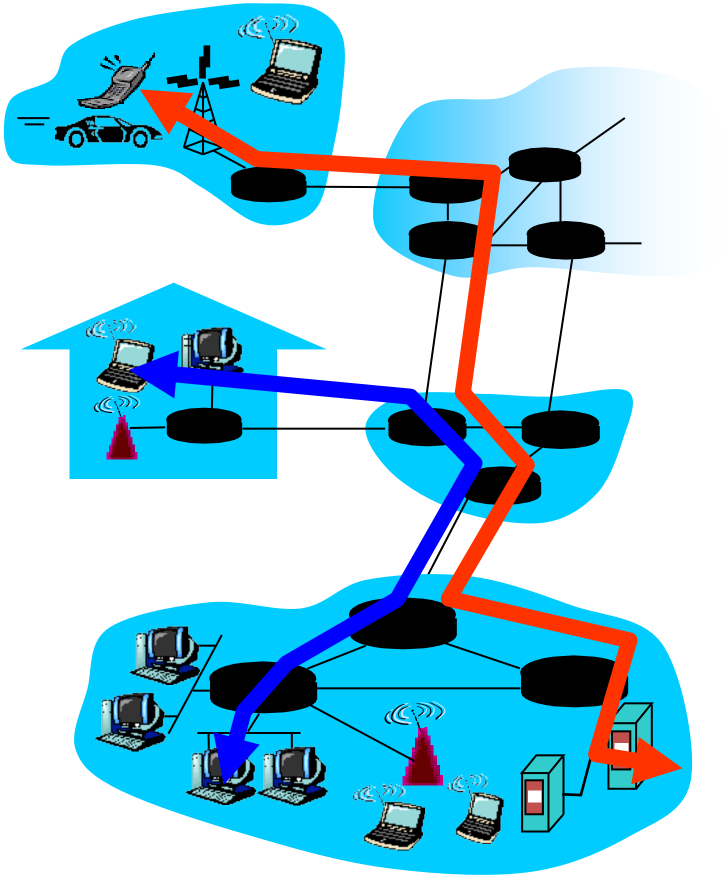


Network Core: Circuit Switching

End-end resources reserved for "call"

- link bandwidth, switch capacity
- dedicated resources: no sharing
- circuit-like (guaranteed) performance
- call setup required

Q: Cons and Pros?



Network Core: Packet Switching

each end-end data stream divided into *packets*

- user A, B packets *share* network resources
- each packet uses full link bandwidth
- resources used *as needed*

Bandwidth division into "pieces"

~~Dedicated allocation~~

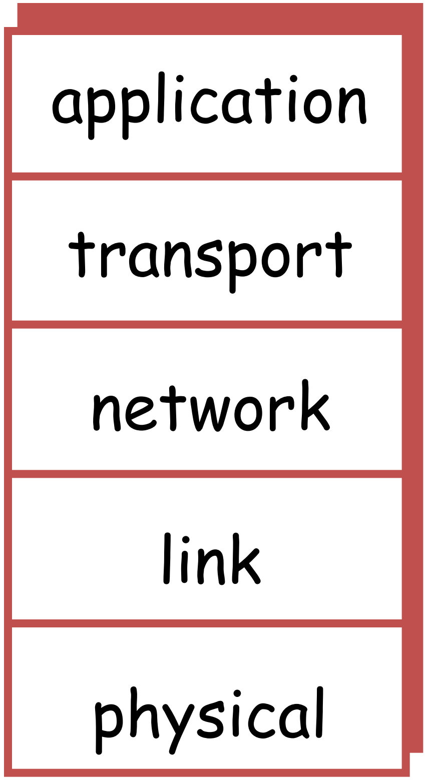
~~Resource reservation~~

resource contention:

- ❑ aggregate resource demand can exceed amount available
- ❑ congestion: packets queue, wait for link use
- ❑ store and forward: packets move one hop at a time
  - Node receives complete packet before forwarding

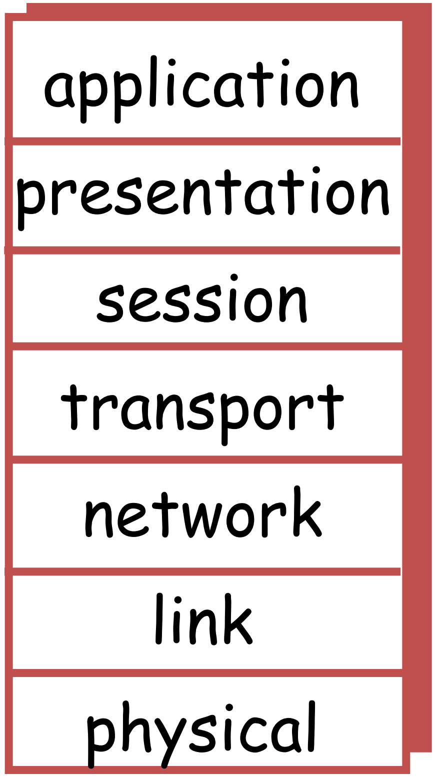
Internet protocol stack

- application: supporting network applications
  - FTP, SMTP, HTTP
- transport: process-process data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - PPP, Ethernet
- physical: bits “on the wire”

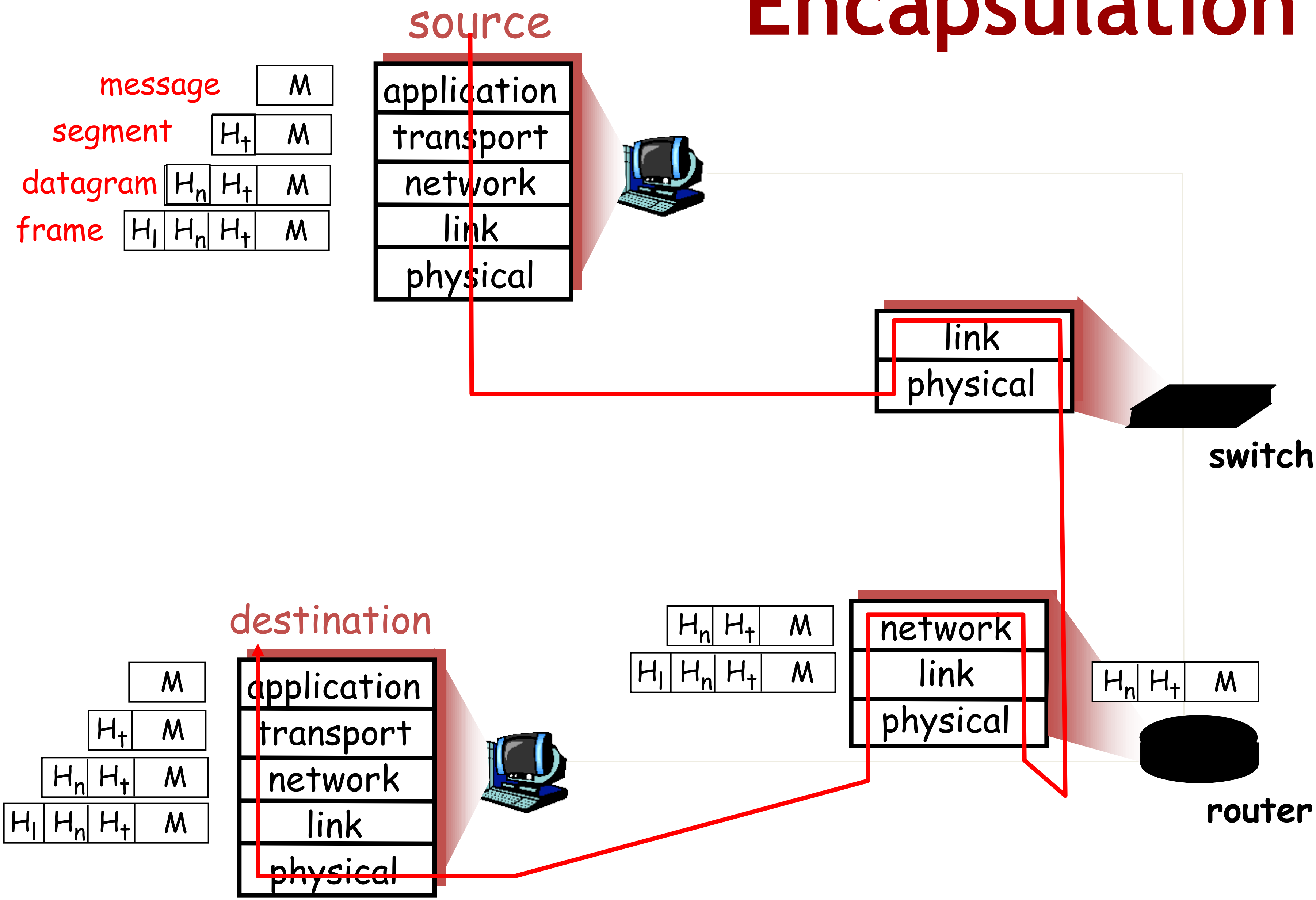


ISO/OSI reference model

- presentation: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- *session:* synchronization, checkpointing, recovery of data exchange
- Internet stack "missing" these layers!
  - these services, *if needed,* must be implemented in application
  - needed?



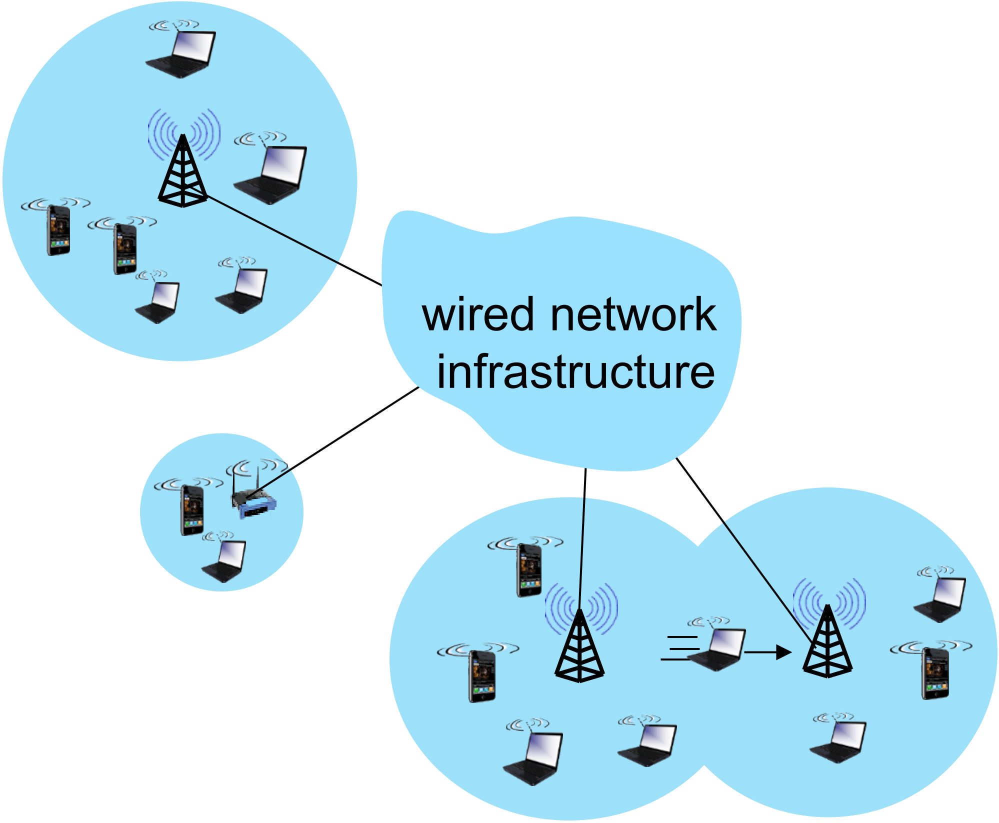
Encapsulation



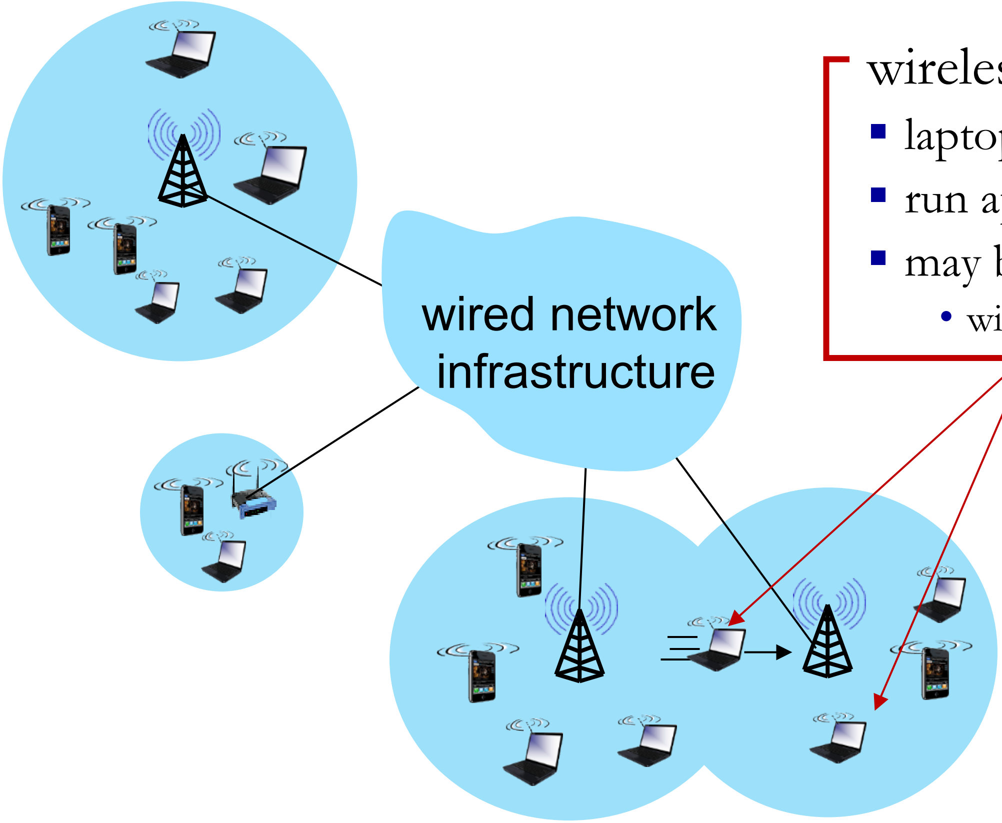
Part 2: Wireless Network Basics

INTRODUCTION TO WIRELESS NETWORK

Elements of a wireless network



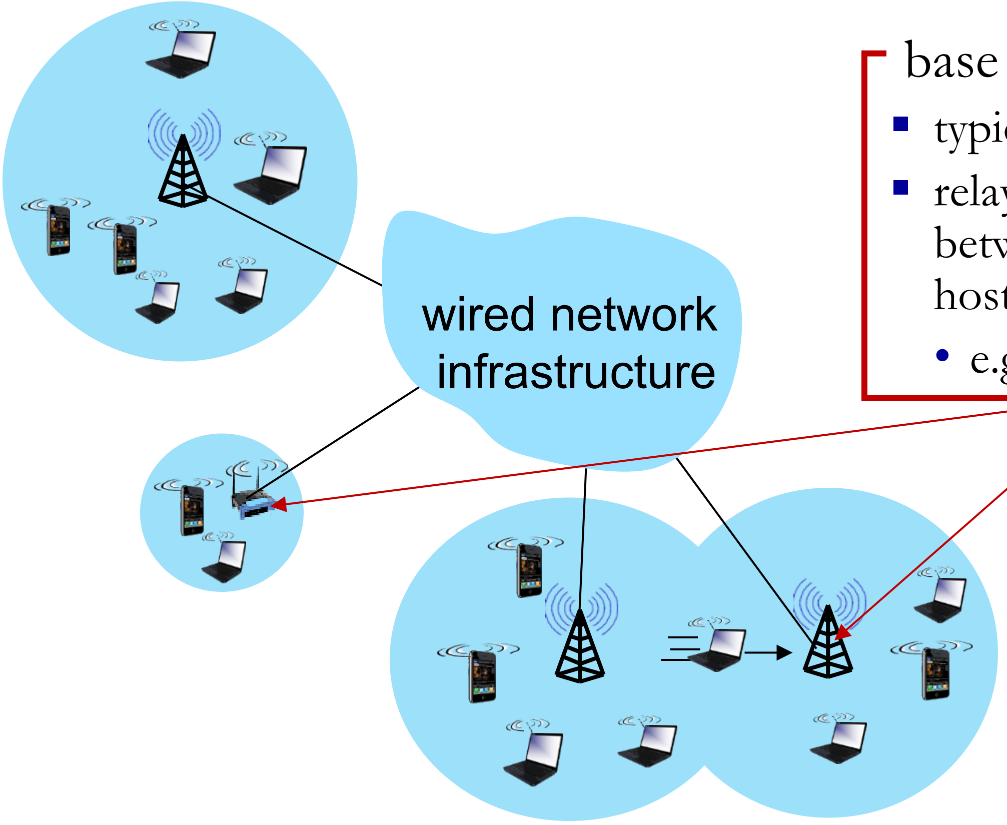
Elements of a wireless network



wireless hosts

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

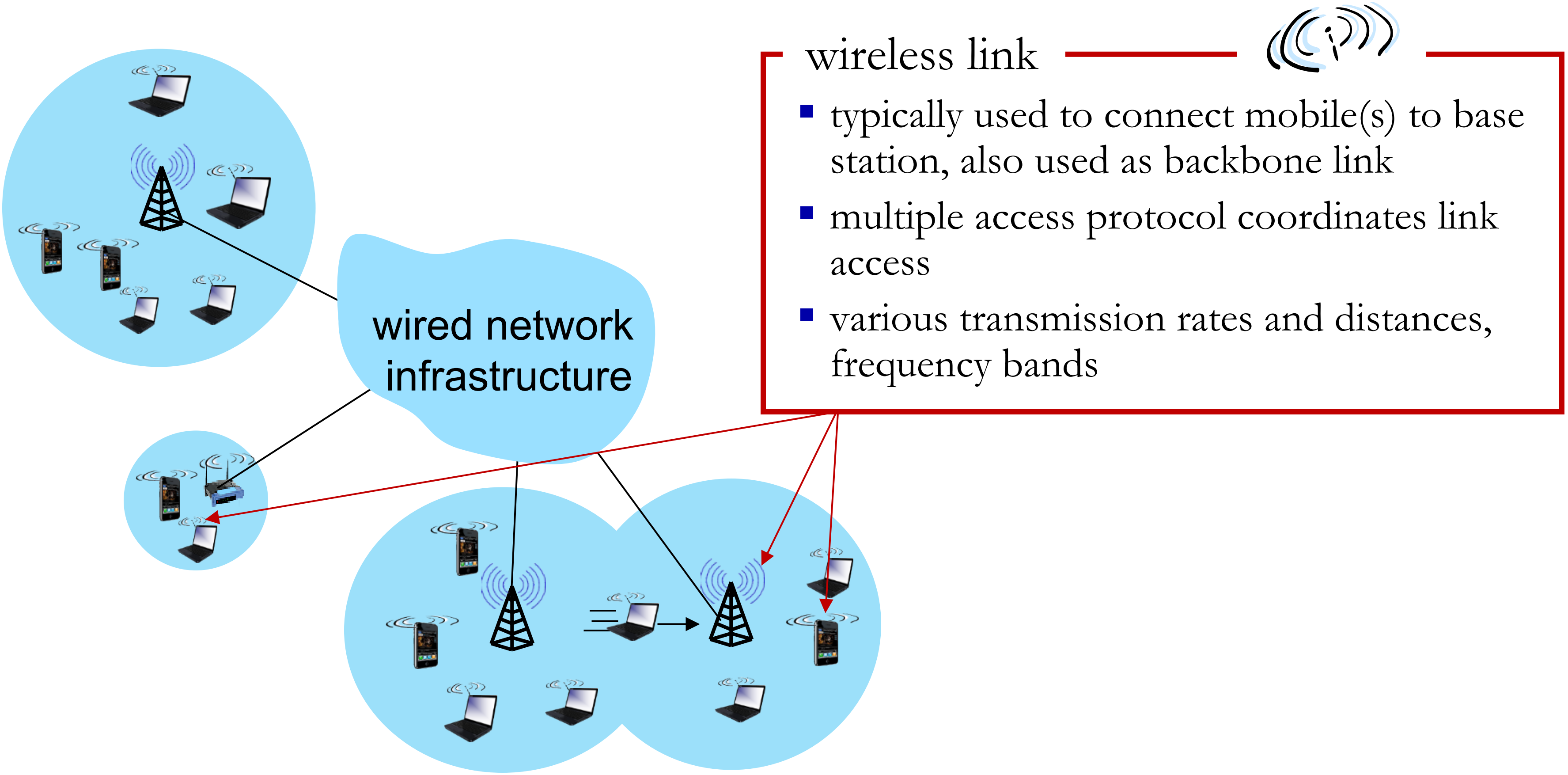
Elements of a wireless network



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

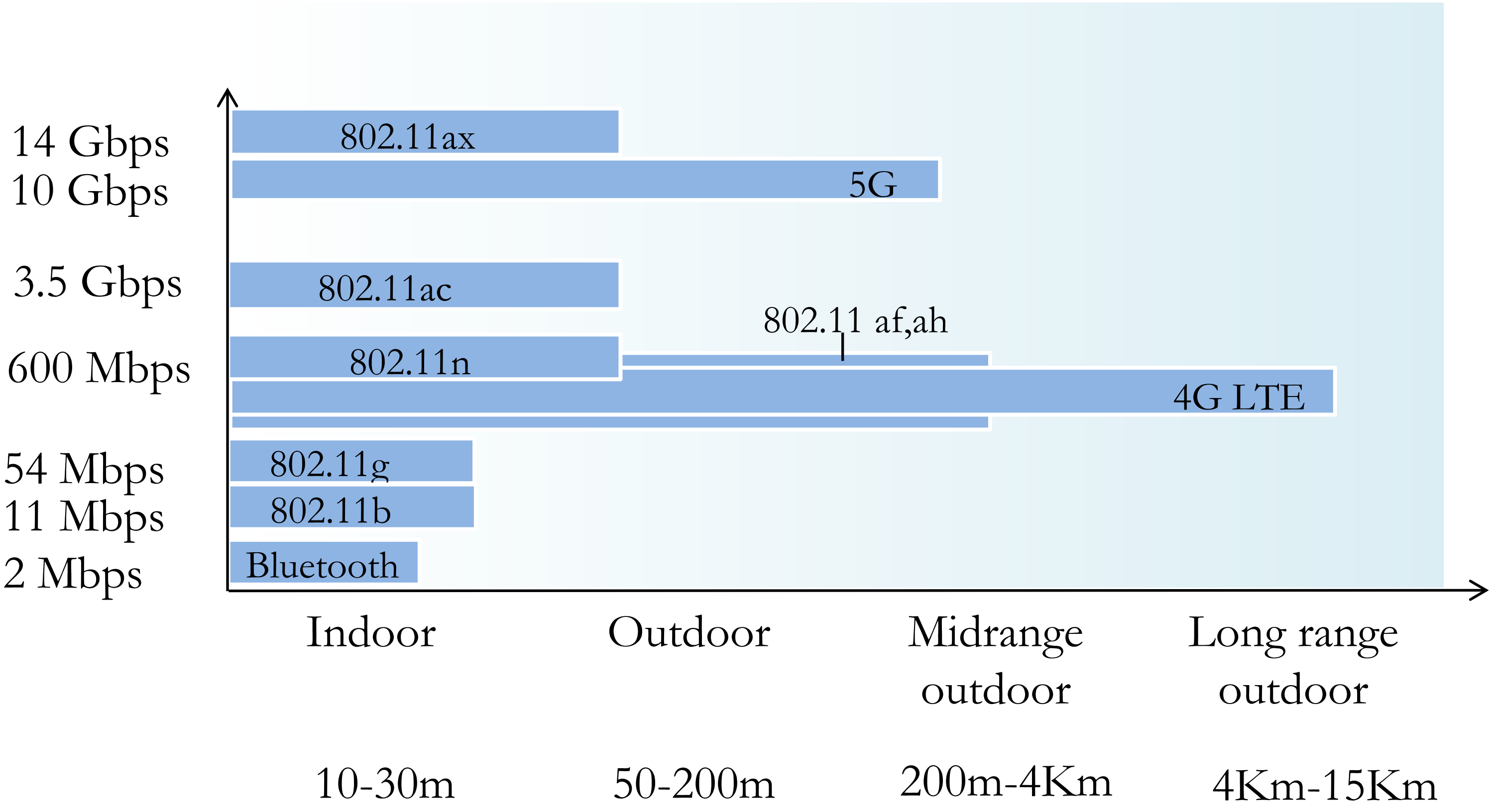
Elements of a wireless network



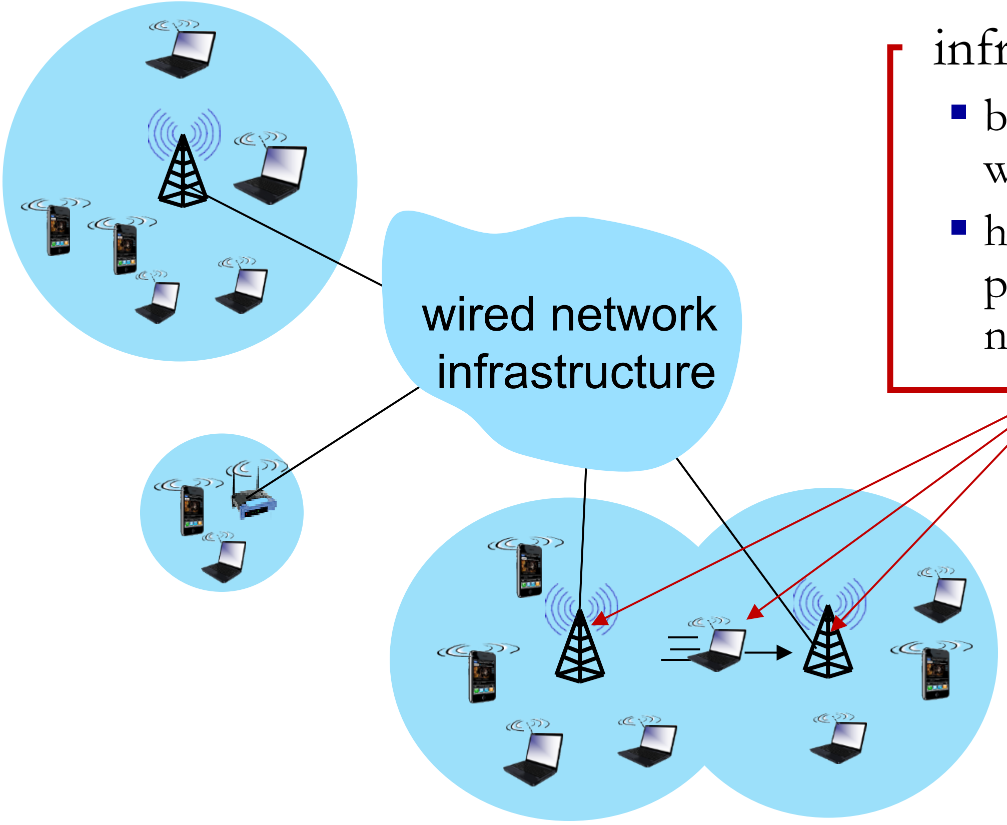
wireless link

- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

Characteristics of wireless links



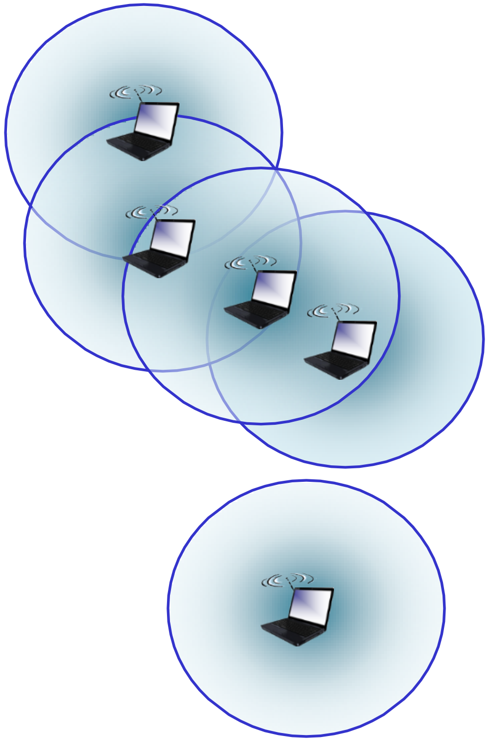
Elements of a wireless network



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

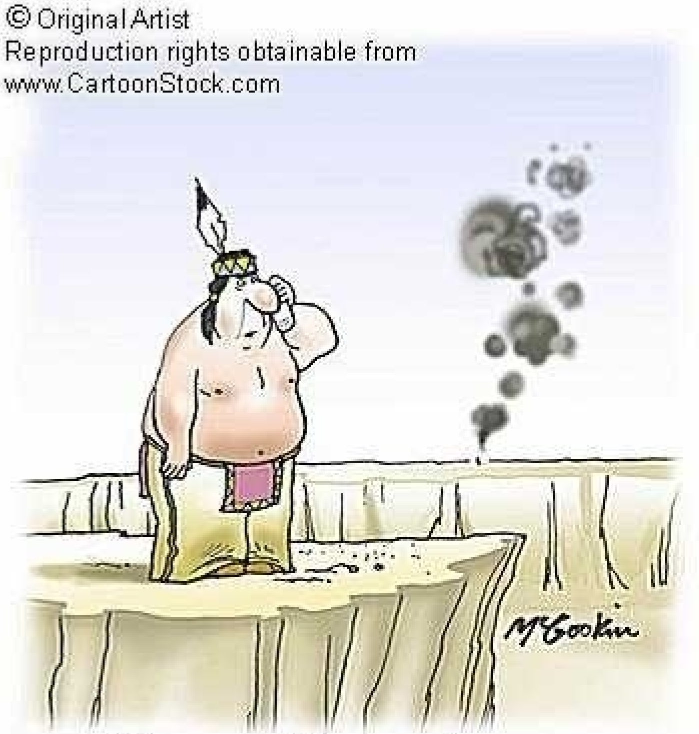
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves
- Example: wireless sensor networks

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, 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(车联网）

Wireless networks

- Why wireless?
- **Wireless networks**
  - “*any* type of network whose interconnections between nodes is implemented without the use of wires.”
  - “generally implemented with some type of remote information transmission system



Oh bugger tradition - next time text me.

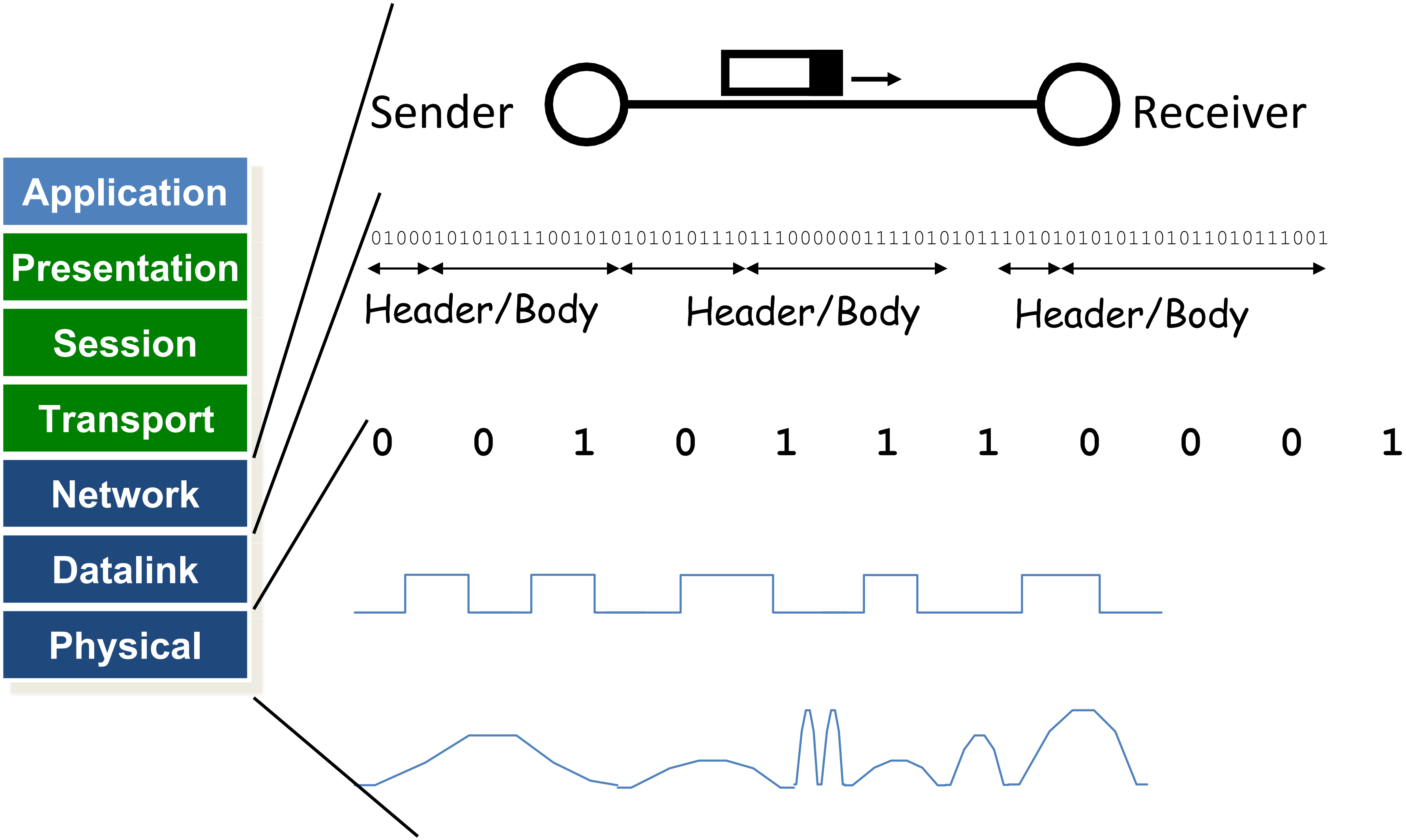
Transferring Information

- Information transfer is a physical process

- In this class, we generally care about
  - Electrical signals (on a wire)
  - Optical signals (in a fiber)
  - More broadly, EM waves

- Information carriers can also be
  - Sound waves
  - Quantum states
  - Proteins
  - Ink & paper, etc.

From Signals to Packets



Sender

Receiver

Application

Presentation

Session

Transport

Network

Datalink

Physical

0100010101011100101010101011101110000001111010101110101010101101011010111001

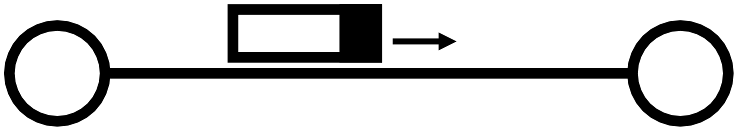
Header/Body Header/Body Header/Body

0 0 1 0 1 1 1 0 0 0 1

From Signals to Packets

Packet Transmission

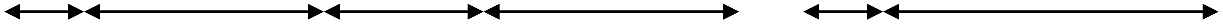
Sender



Receiver

Packets

010001010101110010101010101110111000000111110101011101010101011010110101111001

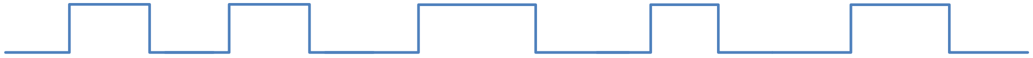


Header/Body Header/Body Header/Body

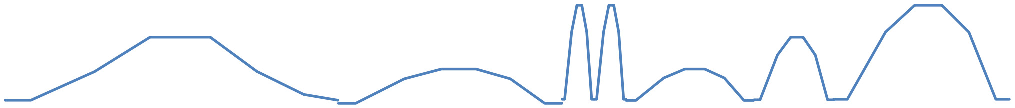
Bit Stream

0 0 1 0 1 1 1 0 0 0 1

"Digital" Signal



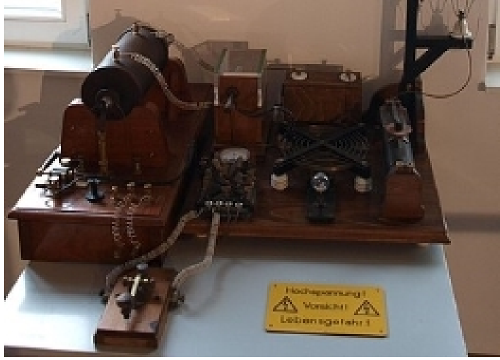
Analog Signal



Radio Frequency Communication

- RF = “portion of the electromagnetic spectrum in which electromagnetic waves can be generated by alternating current fed to an antenna”

Some History



- 1873 – “*A Dynamical Theory of the Electromagnetic Field.*” by James Clerk Maxwell
- 1887 - Heinrich Hertz demonstrates spark-gap transmitter – didn't think it is very useful!
- 1890 - Edouard Branly demonstrates practical coherer
- 1893-97 - Nikola Tesla, Oliver Lodge, Jagdish Chandra Bose, Alexander Popov, Guglielmo Marconi demonstrated “lab” models of their “wireless devices”
- 1897 - Wireless Telegraph and Signal Company, Ltd. In London
- 1901 – successful transmission across the Atlantic Ocean (“a bit more” power and bigger antennas)

Some History (contd)

Q: What do they have to do with radio?

A: Nothing but after Titanic, spark-gap transmitters quickly became universal on large ships

- Radio Act of 1912 – all ships must maintain 24-hour radio watch and keep in contact with nearby ships and coastal radio stations
  - → interference → tuning → modulation
- Radio Act of 1927 – created Federal Radio Commission to regulate radio use “as the public convenience, interest, or necessity requires.”
- Communications Act of 1934 – established Federal Communications Commission (FCC)
- Telecommunications Act of 1996, 2006

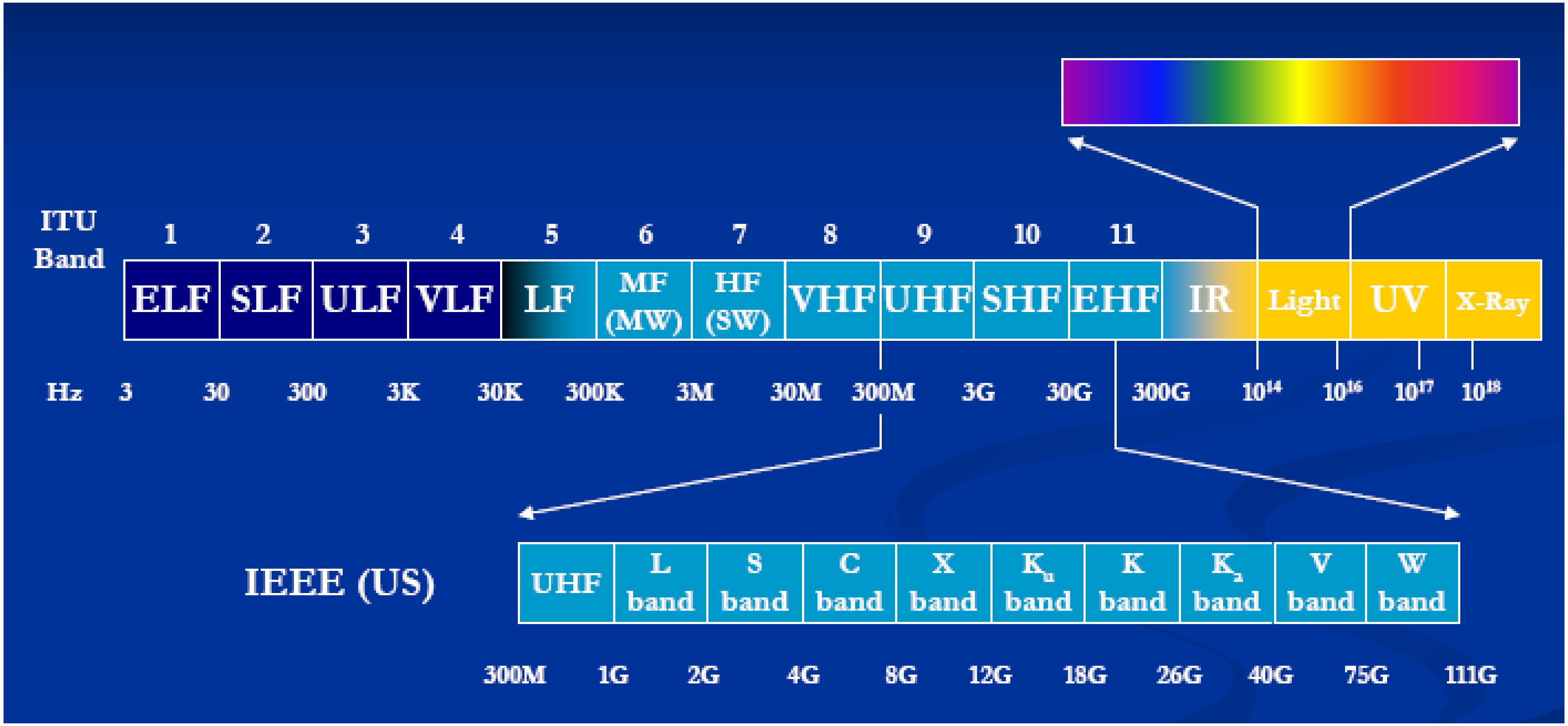
IMPORTANT TERMS

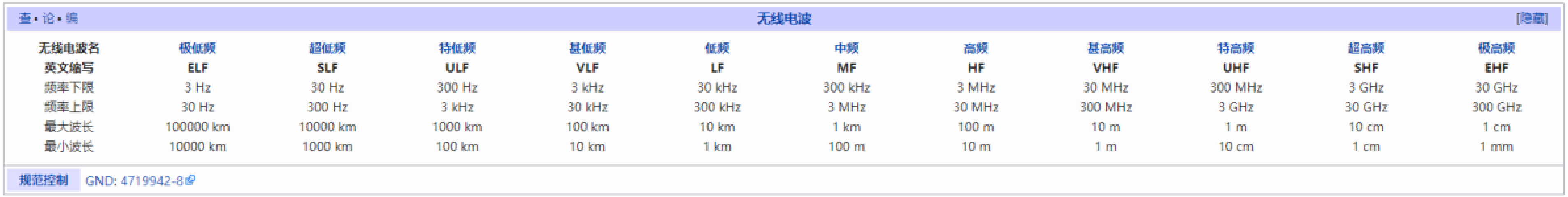
Spectrum

- EM waves have medium dependent properties such as: speed (refraction折射), resonance (absorption吸收), reflection反射, scattering散射
- Propagation in atmosphere:
  - f < 2 MHz: ground-waves (waves follow the contour of the earth)
  - 2 MHz < f < 30 MHz: sky-wave propagation (reflections from ionosphere)
  - f > 30 MHz: line-of-sight (atmospheric scattering)
- Jamming can happen
- In vacuum:

atmospheric scattering

Spectrum Classification





查 • 论 • 编 无线电波 [隐藏]

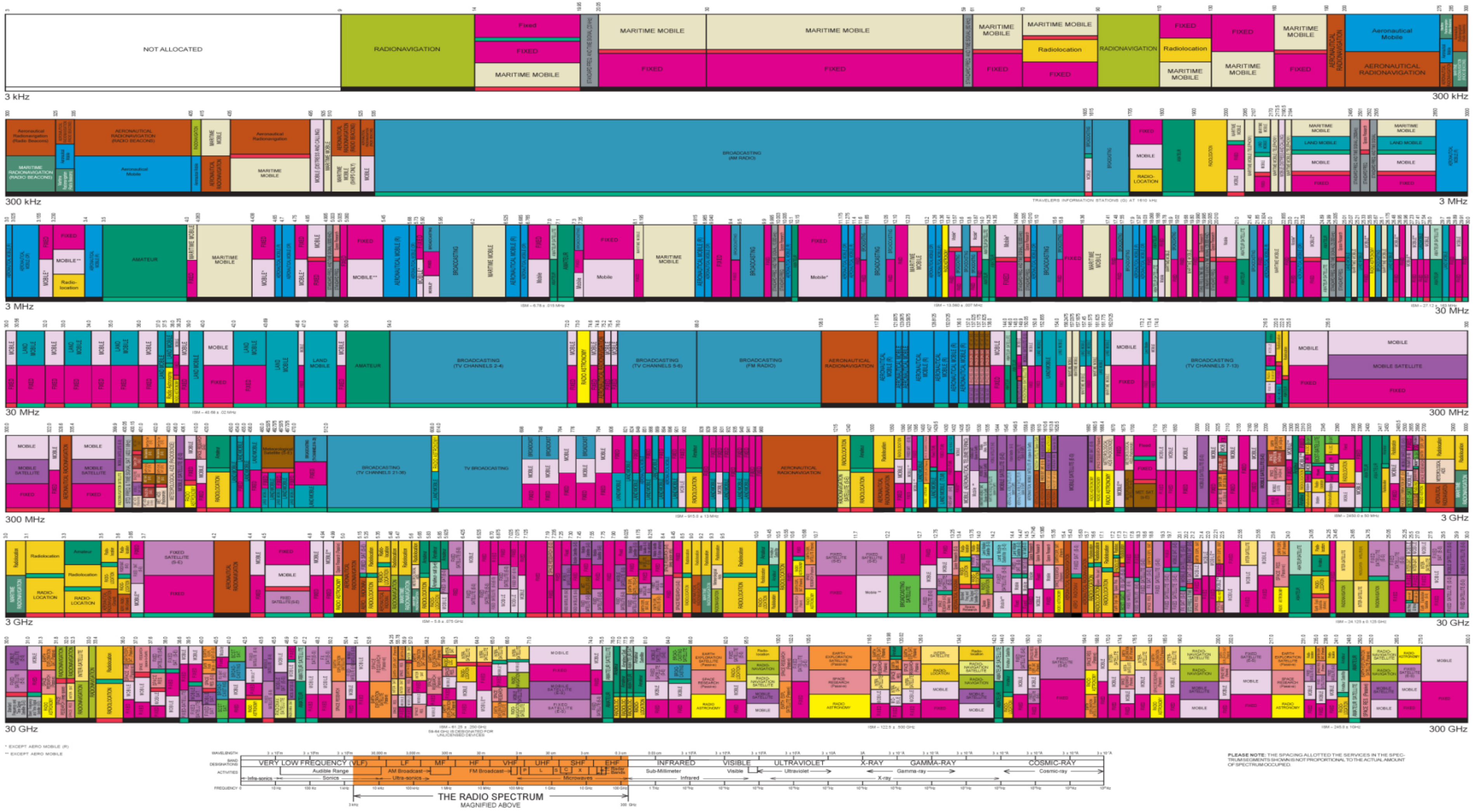
无线电波名	极低频	超低频	特低频	甚低频	低频	中频	高频	甚高频	特高频	超高频	极高频
英文缩写	ELF	SLF	ULF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
频率下限	3 Hz	30 Hz	300 Hz	3 kHz	30 kHz	300 kHz	3 MHz	30 MHz	300 MHz	3 GHz	30 GHz
频率上限	30 Hz	300 Hz	3 kHz	30 kHz	300 kHz	3 MHz	30 MHz	300 MHz	3 GHz	30 GHz	300 GHz
最大波长	100000 km	10000 km	1000 km	100 km	10 km	1 km	100 m	10 m	1 m	10 cm	1 cm
最小波长	10000 km	1000 km	100 km	10 km	1 km	100 m	10 m	1 m	10 cm	1 cm	1 mm

规范控制 GND: 4719942-8

Spectrum Allocation

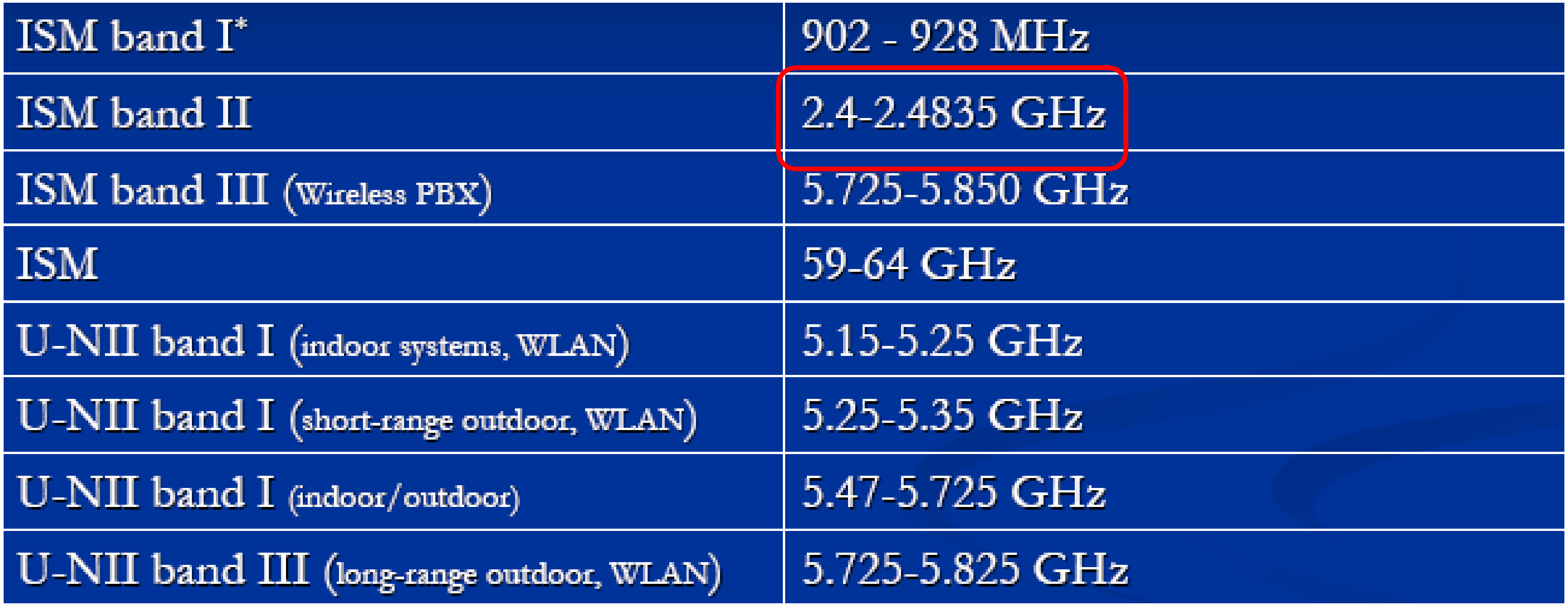
- Spectrum – national resource under government control (usually split between commercial and military)
  - US: Federal Communications Commission (**FCC**) and Office of Spectral Management (**OSM**) in US
  - EU: European Conference of Post and Telecommunications Administrations (**CEPT**)
    - European Communications Office (ECO) -> Electronic Communications Committee (ECC)
  - Japan: Ministry of Public Management, Home Affairs, Posts and Telecommunications (**MPHPT**)
  - China:无线电管理局（国家无线电办公室）
- International Telecommunications Union (**ITU**: ITU-T,ITU-R)
- Commercial allocation
  - Fixed
  - Auctions
  - Unlicensed
  - Secondary market and spectrum leasing
- Policy shift: Cognitive radio - a transceiver can intelligently detect which communication channels are in use and which ones are not

Spectrum Allocation (cont’d)



Spectrum Allocation

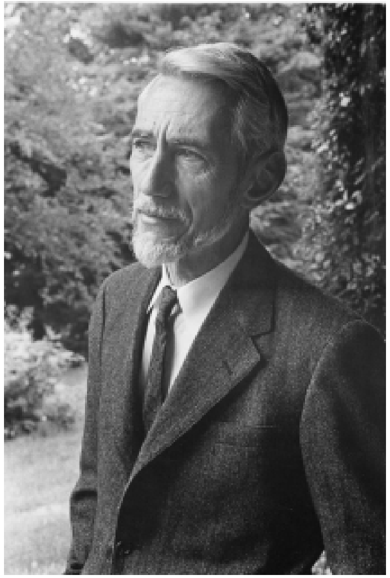
- Unlicensed spectrum (US)



ISM band I*	902 - 928 MHz
ISM band II	2.4-2.4835 GHz
ISM band III (Wireless PBX)	5.725-5.850 GHz
ISM	59-64 GHz
U-NII band I (indoor systems, WLAN)	5.15-5.25 GHz
U-NII band I (short-range outdoor, WLAN)	5.25-5.35 GHz
U-NII band I (indoor/outdoor)	5.47-5.725 GHz
U-NII band III (long-range outdoor, WLAN)	5.725-5.825 GHz

ISM = Industrial, Scientific and Medical
U-NII = Unlicensed National Information Infrastructure

Shannon Capacity



- **Claude Shannon**（克劳德·艾尔伍德·香农）(1916-2001)

$$C = B\log_2(1+\frac{S}{N})$$

- Upper bound on achievable communication rate in AWGN environments (1948)
  - C is the channel capacity in bits per second;
  - B is the bandwidth of the channel in hertz;
  - S is the signal power, measured in watt or volt^2;
  - N is the noise power
  - S/N is the signal-to-noise ratio (SNR)
- Example:
  - Local loop bandwidth: 3200 Hz
  - Typical S/N: 1000 (30db)
  - What is the upper limit on capacity?
    - 3200 x $\log_2(1 + 1000)$ = 31.895 kbits/s

Bandwidth

- Bandwidth is **width of the frequency range** in which the Fourier transform of the signal is non-zero. (At what frequencies is there energy)

- Sometimes referred to as the channel width. Or, where it is above some threshold value (Usually, the half power threshold, e.g., -3dB)

- dB
  - Short for decibel
  - Defined as 10 * $\log_{10}(P_1/P_2)$
  - When used for signal to noise: 10 * $\log_{10}(P_S/P_N)$

Noise

- "Any unwanted input" that limits systems ability to process weak signals
- Measure of the signal "noisiness" = signal-to-noise ratio (frequency dependant)
- Noise sources:
  - External
  - Atmospheric
  - Interstellar
- Receiver internal
  - Thermal
  - Flicker noise (low frequency)
  - Shot noise
- Noise is not always bad!

EXAMPLES:

- Random noise in resistors and transistors
- Mixer noise
- Power supply noise

Antennas

- “Interface” between the transmitter (receiver) and channel

- Can the wires inside devices be antennas?

Multipath

- Non Line-of-sight

- Objects in the environment
  - Reflection
  - Diffraction
  - Scattering

- Multiple signal copies added together
  - Attenuated
  - Delayed
  - Phase shifted

$$d(t) = h_1 s(t - \Delta_1) + h_2 s(t - \Delta_2) + \ldots + h_m s(t - \Delta_m)$$

- Frequency selective fading
- Flat fading
- Ultimately causes inter symbol interference (ISI) which limits performance

Wireless link characteristics (1)

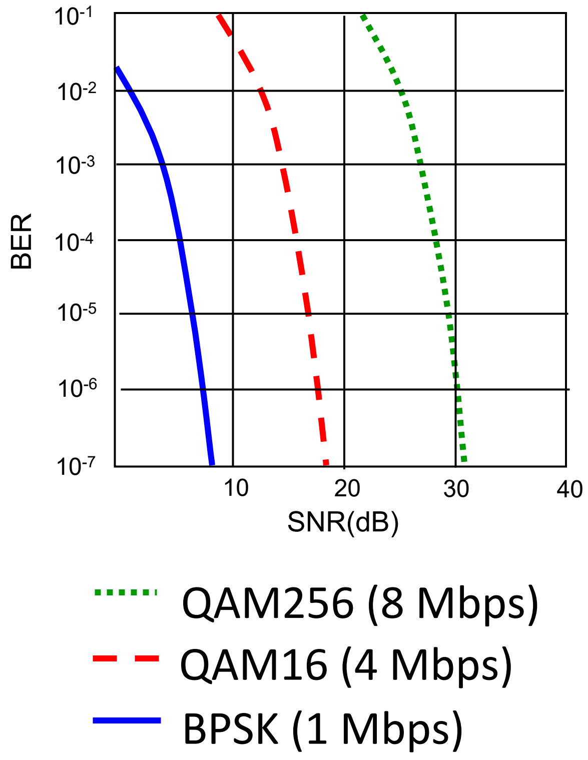
important differences from wired link ….

- decreased signal strength*:* radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
  - Cross-technology communication (CTC)
  - E.g., WiFi and Zigbee/Bluetooth
- multipath propagation: radio 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"

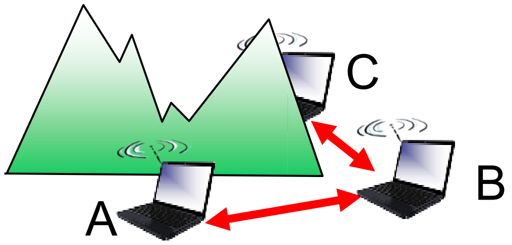
Wireless link characteristics (2)

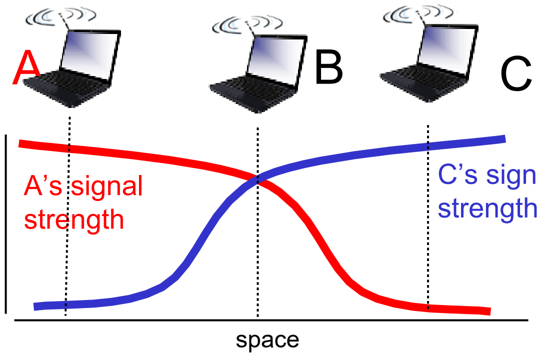
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR versus BER tradeoffs
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR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



Wireless link characteristics (3)

- Multiple wireless senders, 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, resulting in interfering at B

How to deal with a noise or imperfect wireless channels?

MODULATION

Baseband vs. Carrier Modulation

- **Modulation**: is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a separate signal called the modulation signal that typically contains information to be transmitted.

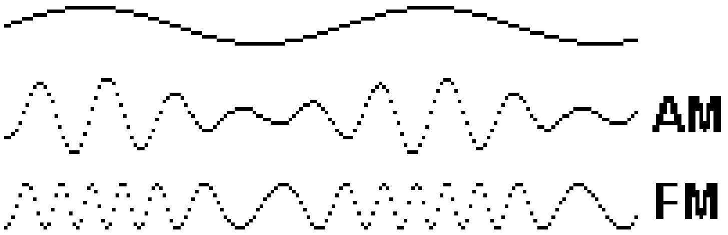
- Baseband modulation: send the “bare” signal

- Carrier modulation: use the signal to modulate a higher frequency signal (carrier).
  - Can be viewed as the product of the two signals
  - Corresponds to a shift in the frequency domain

Modulation

- Changing a signal to convey information

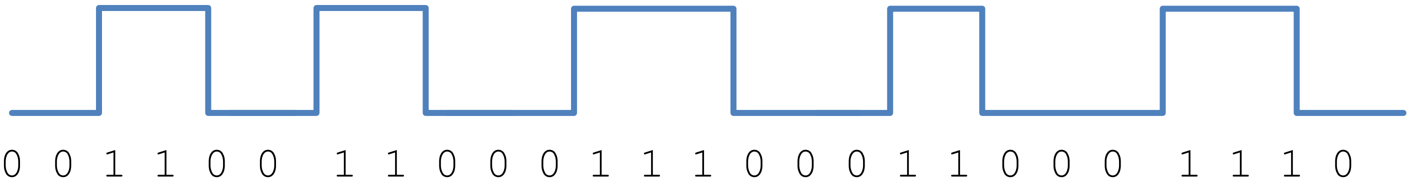
- Ways to modulate a sinusoidal wave
  - Volume: Amplitude Modulation (AM)
  - Pitch: Frequency Modulation (FM)
  - Timing: Phase Modulation (PM)

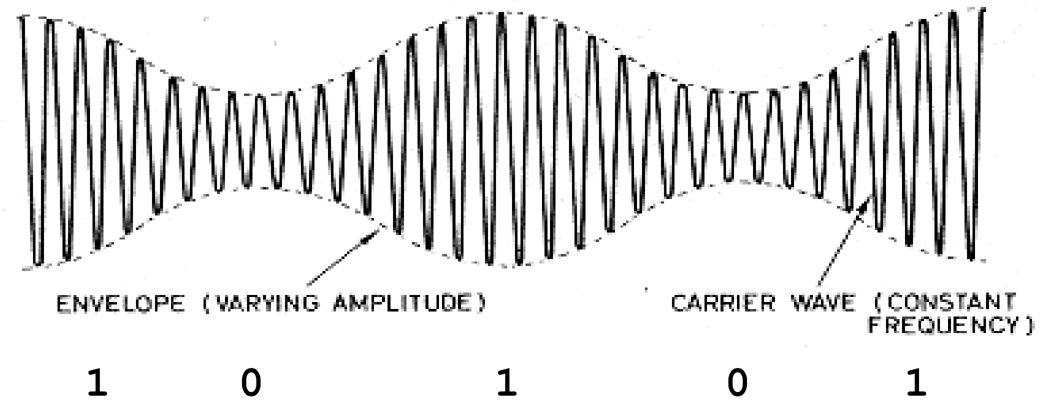


- In our case, modulate signal to encode a “0” or a “1”. (multi-valued signals sometimes)

Amplitude Modulation

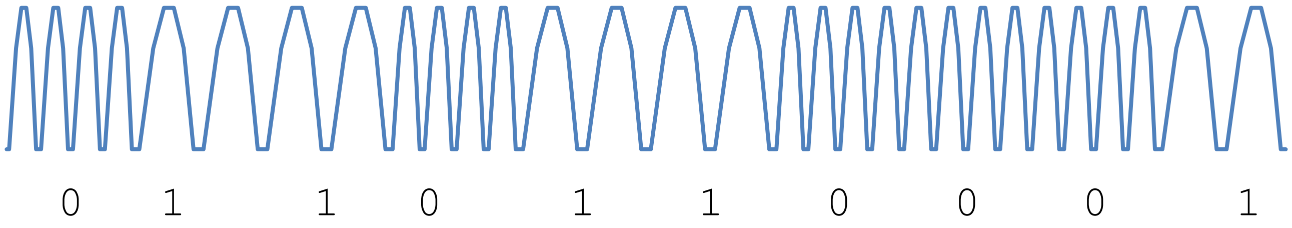
- AM: change the strength of the signal.
- Example: High voltage for a 1, low voltage for a 0

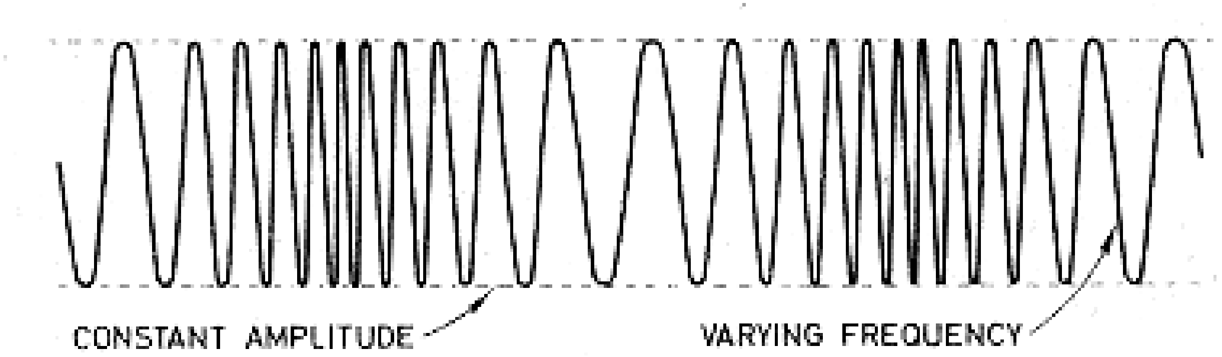



ENVELOPE (VARYING AMPLITUDE)
CARRIER WAVE (CONSTANT FREQUENCY)
1 0 1 0 1

Frequency Modulation

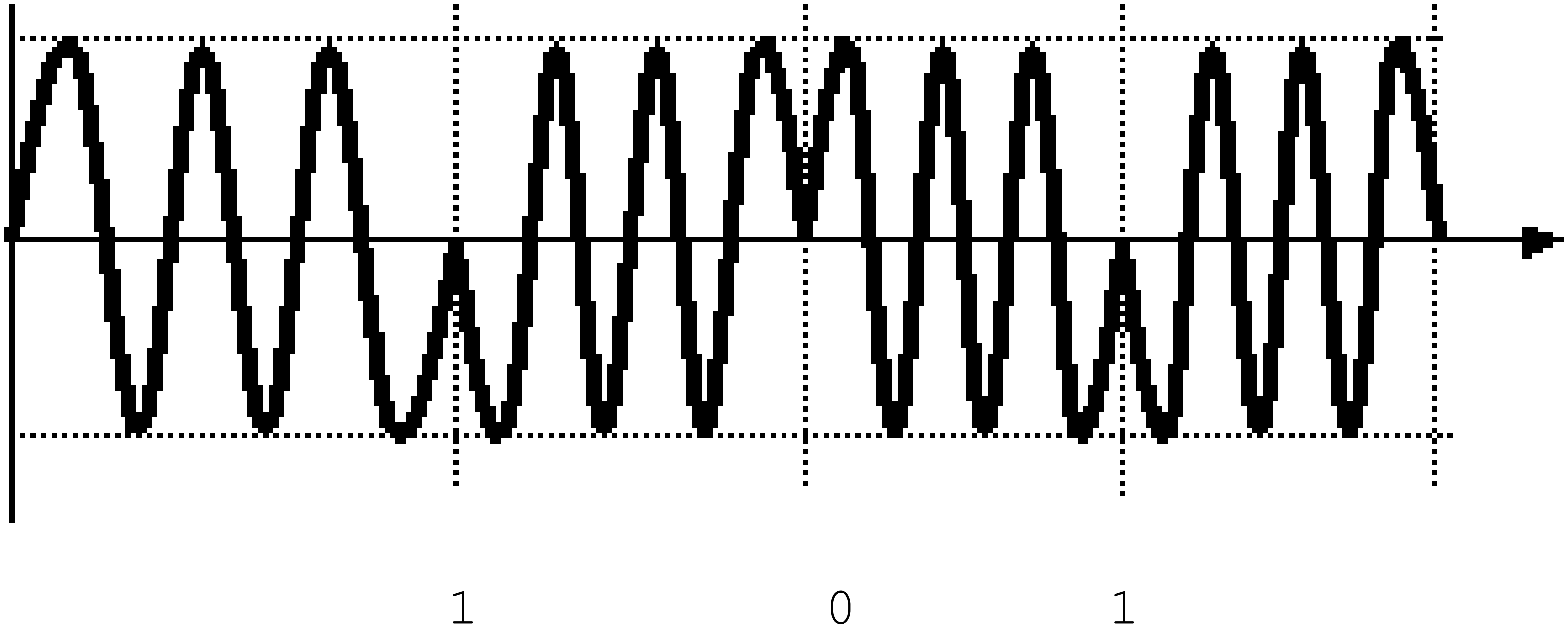
- FM: change the frequency





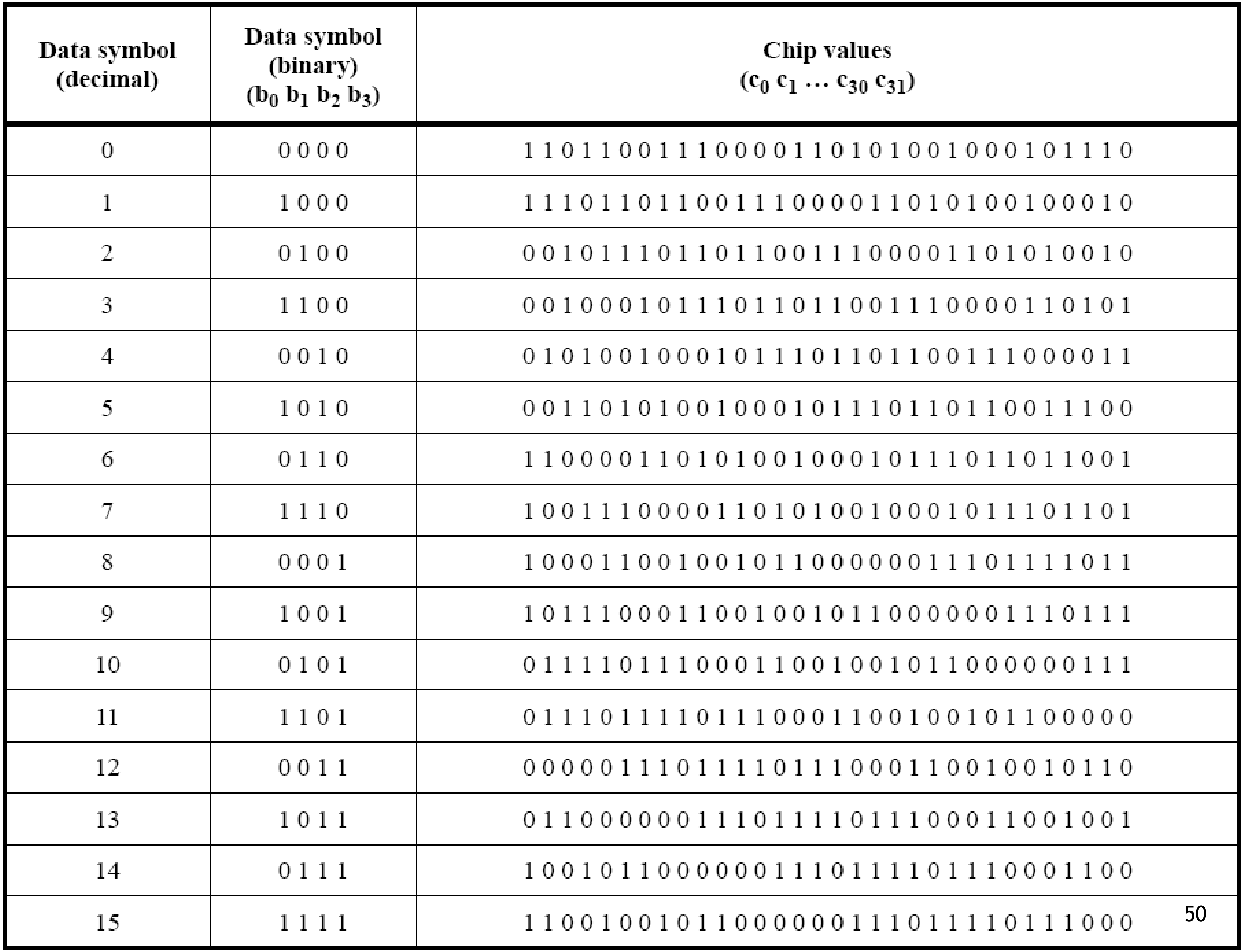
Phase Modulation

- PM: Change the phase of the signal



Direct Sequence Spread Spectrum (DSSS)

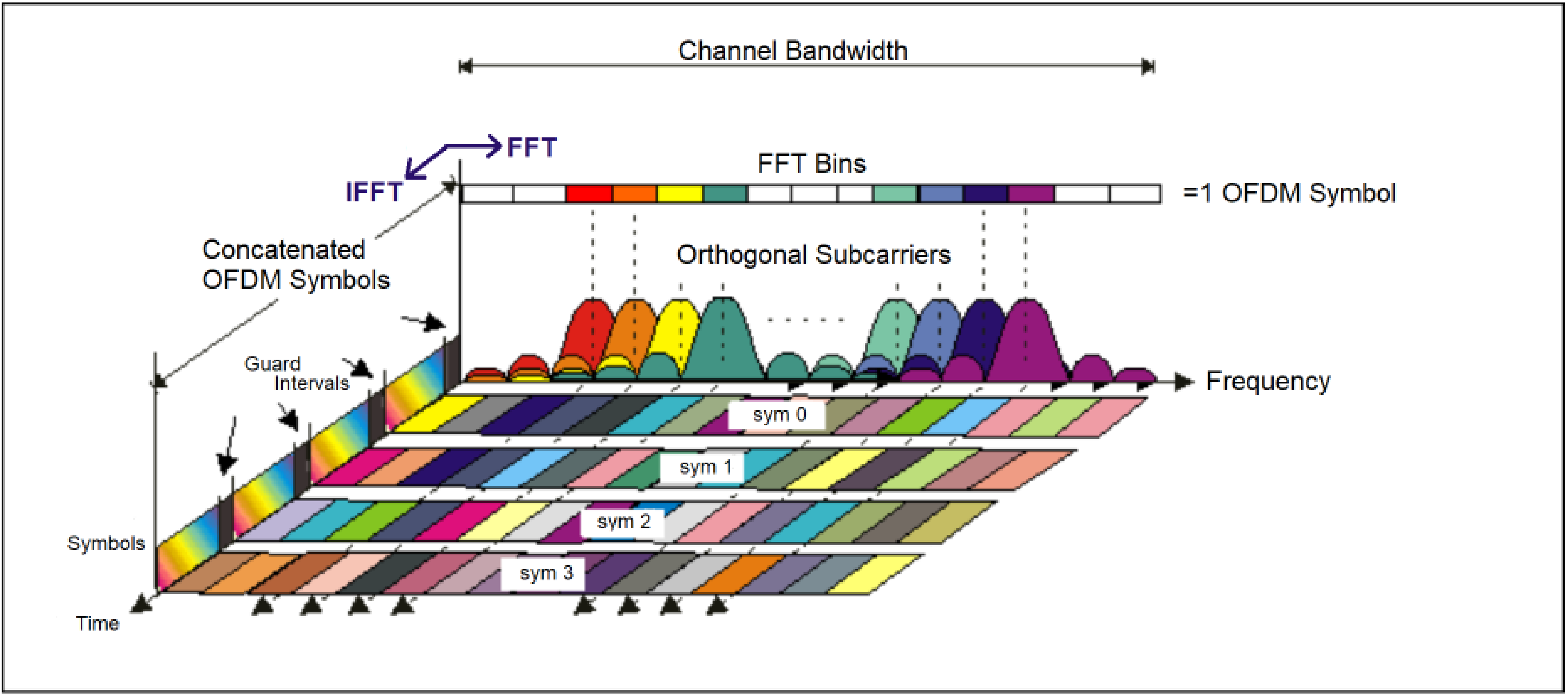
- Widely used in Wi-Fi
- Each bit in original signal is represented by **multiple bits** in the transmitted signal
- Spreading code spreads signal across a wider frequency band
  - Spread is in direct proportion to number of bits used
- One technique combines digital information stream with the spreading code bit stream using exclusive-OR



Data symbol (decimal)	Data symbol (binary) (b_0 b_1 b_2 b_3)	Chip values (c_0 c_1 … c_{30} c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

OFDM

- Mostly used in Wi-Fi
- The OFDM scheme differs from traditional FDM in the following interrelated ways:
  - **Multiple carriers** (called subcarriers) carry the information stream
  - The subcarriers are **orthogonal** to each other, and
  - A guard interval is added to each symbol to minimize the channel delay spread and intersymbol interference.



Frequency-Time Representative of an OFDM signal

How wo regulate wireless vendors?

WIRELESS STANDARDS

Standards

- **Availability of interoperable equipment from multiple vendors**
- **Prevents a “Tower of Babel” situation**
  - Equipment from different vendors will interoperate if it complies with the standard
  - Alliances and certification bodies assure interoperability
    - Wi-Fi for 802.11
- **Lowers costs to consumers**
  - Both through competition and economies of scale
- Fight for standards from countries, e.g, in 5G.

IEEE 802 Standards

Maintained by IEEE 802 LAN/MAN Standards Committee (LMSC):

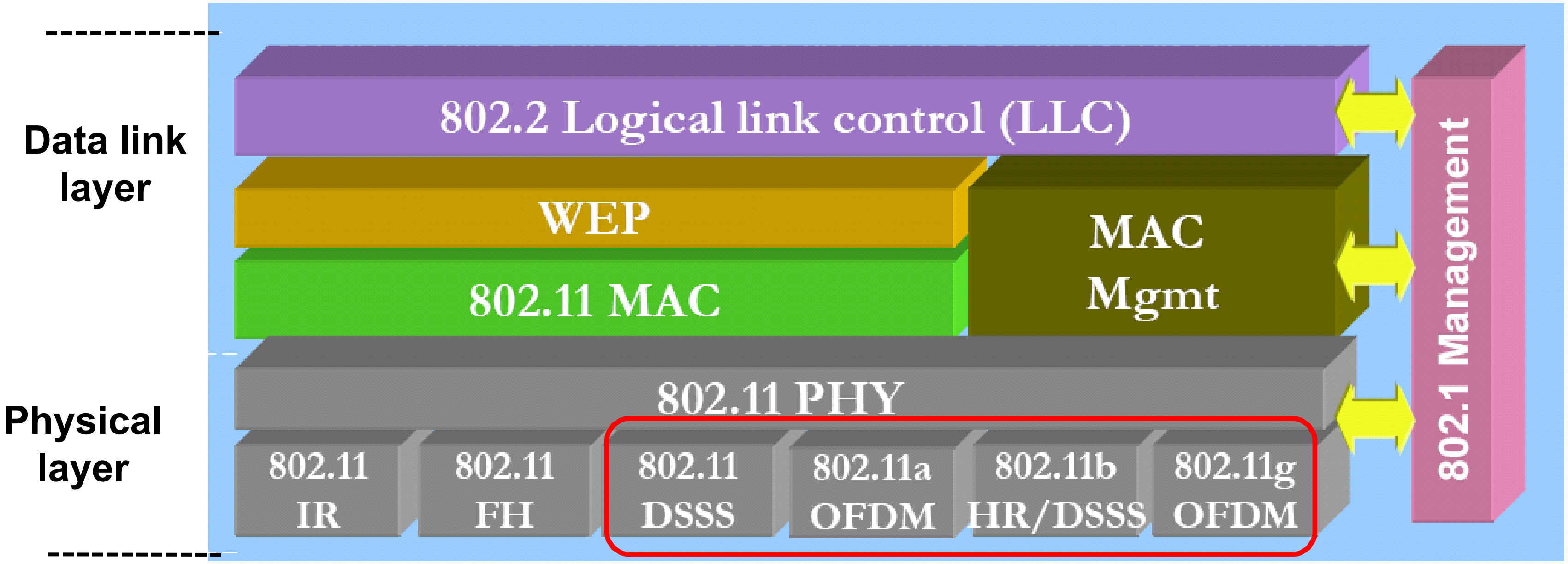
- 802.1 Overview, Architecture, Internetworking and Management
- 802.2 Logical Link Control
- **802.3 Ethernet (CSMA/CD PHY and MAC)**
- 802.5 Token Ring PHY and MAC
- **802.11 Wireless LAN-Wi-Fi**
- 802.12 Demand Priority Access
- **802.15 Wireless PAN**
- **802.16 Broadband Wireless Access**
- 802.17 Resilient Packet Ring
- 802.18 Radio Regulatory
- 802.19 Coexistence
- **802.20 Mobile Broadband Wireless Access**
- 802.21 Media Independent Handoff
- 802.22 Wireless Regional Area Network

Typical Standards and Protocols

802.11 Wi-Fi as an example

802.11

- 802.11 data link and physical layer have a lot of members…



Wireless “Alphabet Soup”

- Q: What is Wi-Fi?
- A: Wi-Fi is a family of wireless network protocols based on the IEEE 802.11 family of standards, especially with specially designed physical layers, including:
- 802.11b:
  - Most common wireless protocol. Uses 2.4GHz frequency, with 1, 2, 5.5,11 Mbps bandwidth. (5 Mbps is more typical).
- 802.11a:
  - Uses 5.5GHz range, 54 Mbps bandwidth (~20 Mbps is typical performance). Produces too much radio power to be certified in medical areas.
- 802.11g:
  - Uses 2.4GHz band and is compatible with 802.11b. Also 54 Mbps bandwidth (~20 Mbps typical)
- Almost a~z are all used!

802.11 Range

802.
11b

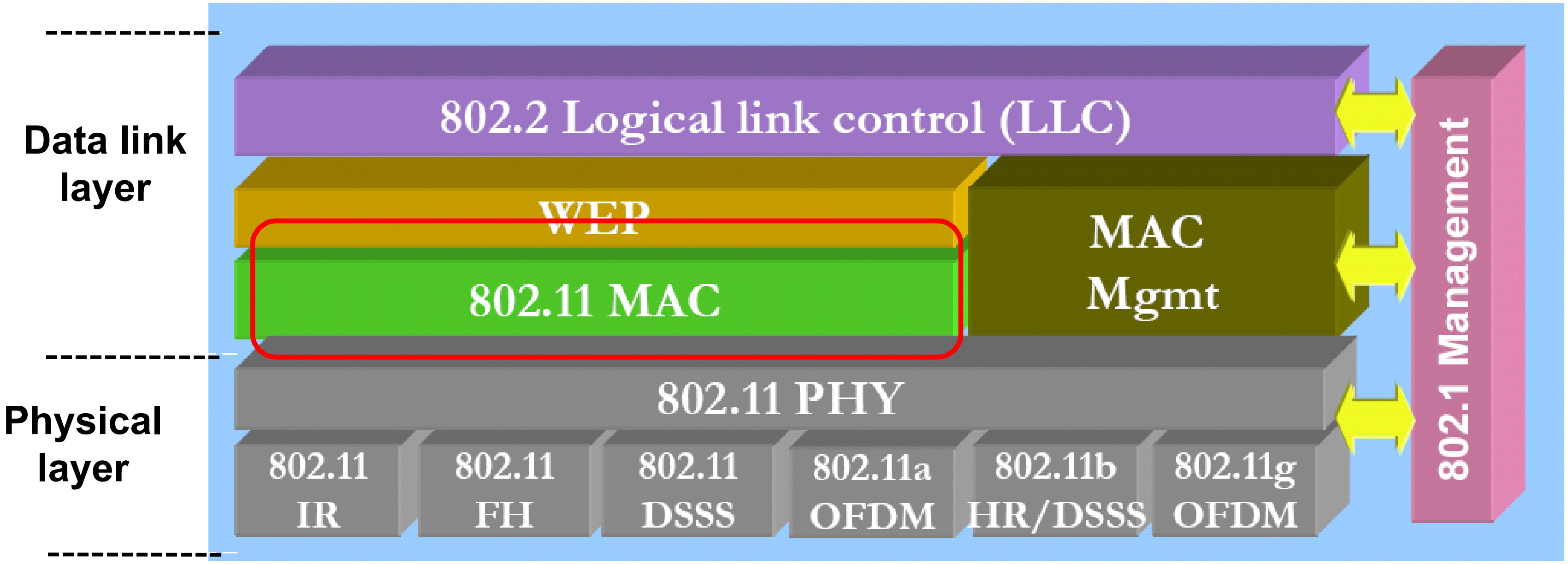
802.
11g

802.
11a

802.11 MAC

802.11

- Member of IEEE 802 family (Specifications for Local Area Networks)



Wireless Access Control

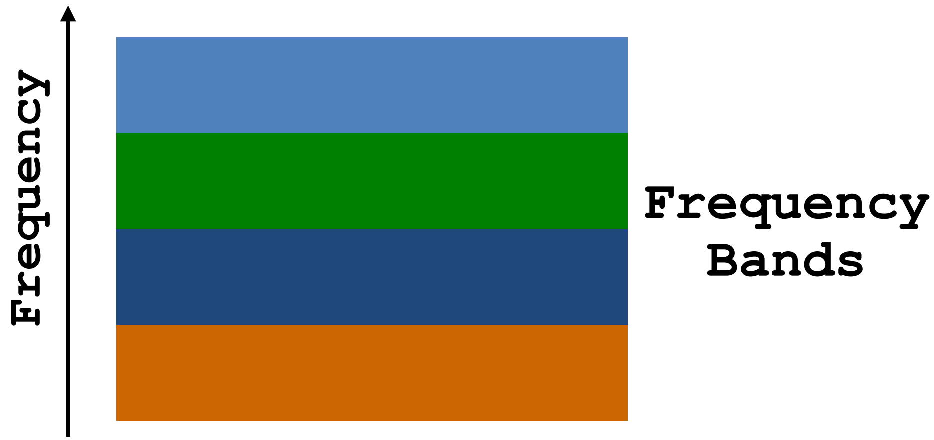
- Recall packet switch: Sharing instead of dedicated resource

- Data is divided into chunks – packets:
  - Each packet fights for resources
  - Each packet can be routed independently

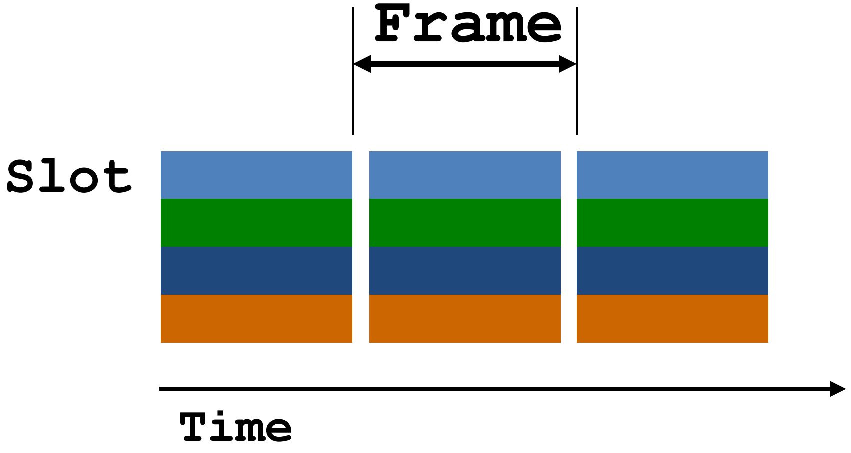
- Resource allocation (switching)
  - DMA: TDMA, FDMA
  - ALOHA:
    - unslotted (pure), slotted
  - Carrier-sense :
    - non-persistent, p-persistent, CD, CA

Frequency vs. Time-division Multiplexing

- With FDM different users use different parts of the frequency spectrum.
  - I.e. each user can send all the time at reduced rate



- With TDM different users send at different times.
  - I.e. each user can send at full speed some of the time
  - Example: time-share condo



- The two solutions can be combined.

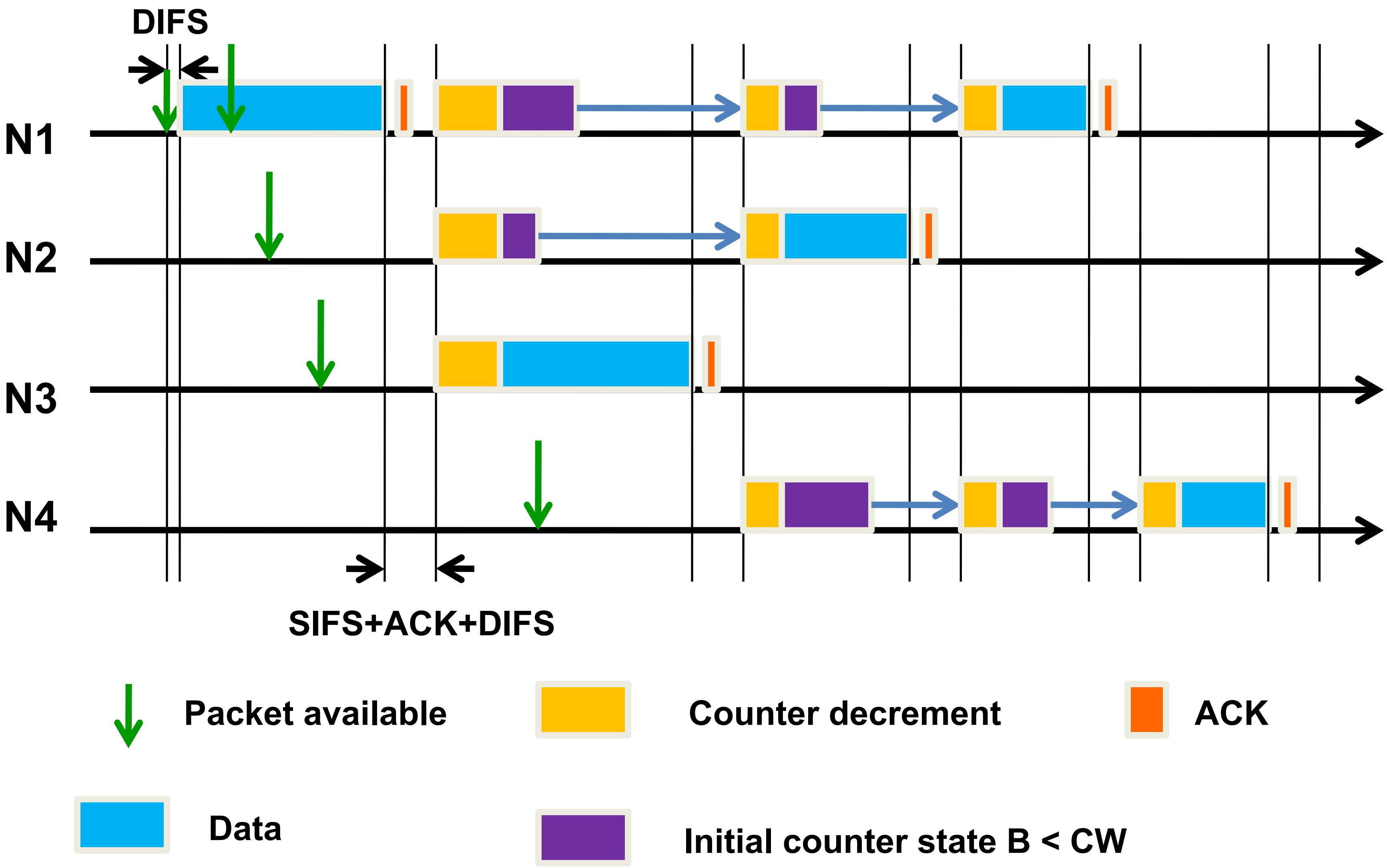
CSMA/CA

- Use CSMA with Collision Avoidance
  - Based on carrier sense function called Clear Channel Assessment (CCA)
- Why not collision detection in wired networks?
- Reduce collision probability where mostly needed
- Possible to implement different Efficient backoff algorithm stable at high loads

1-Persistent CSMA (Ethernet)

- Sense the channel
  - If busy, keep listening to the channel and transmit immediately when the channel becomes idle.
  - If idle, transmit a packet immediately.
- If collision occurs
  - Wait a random amount of time and start over again.
- Greedy algorithm

Basic access in absence of collisions

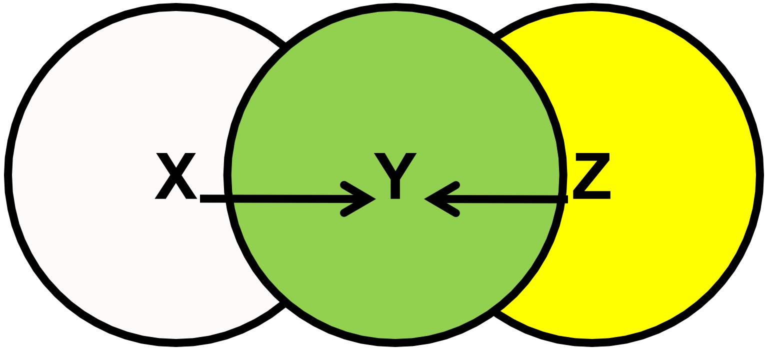


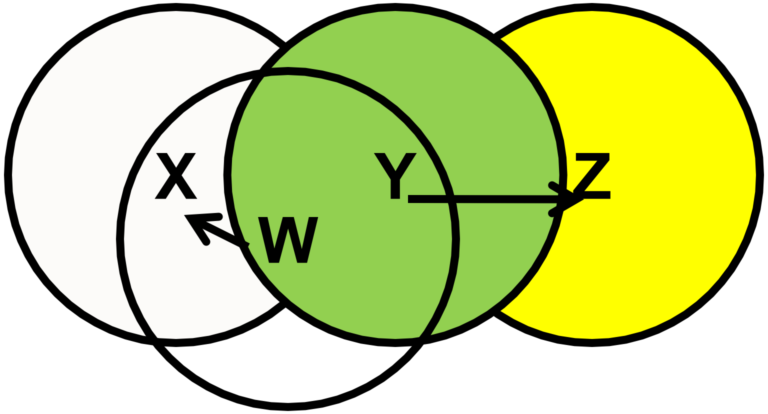
Q: Why is your Wi-Fi always slow?

Binary random backoff

- initial counter state:
  $B = U[0, CW - 1]$
- contention window size:
- k: # of contentions
- example: 802.11b DSSS
  $CW_{min} = 32$, $\hat{k} = 5$, and $CW_{max} = 1024$

Problems with Carrier Sensing





- Hidden terminal problem
  - Z does not hear X; hence transmits to Y and collides with transmission from X
  - No carrier does not mean you can send
- Exposed terminal problem
  - W hears Y but can safely transmit to X
  - Carrier may not imply you can not send

802.11 Media Access Control

- Handshaking to infer collisions
  - DATA-ACK packets
- Collision Avoidance
  - RTS-CTS-DATA-ACK to request the medium
  - Duration information in each packet
  - Random Backoff after collision is determined
- Two carrier sensing functions:
  - Physical carrier-sensing
  - Virtual carrier-sensing

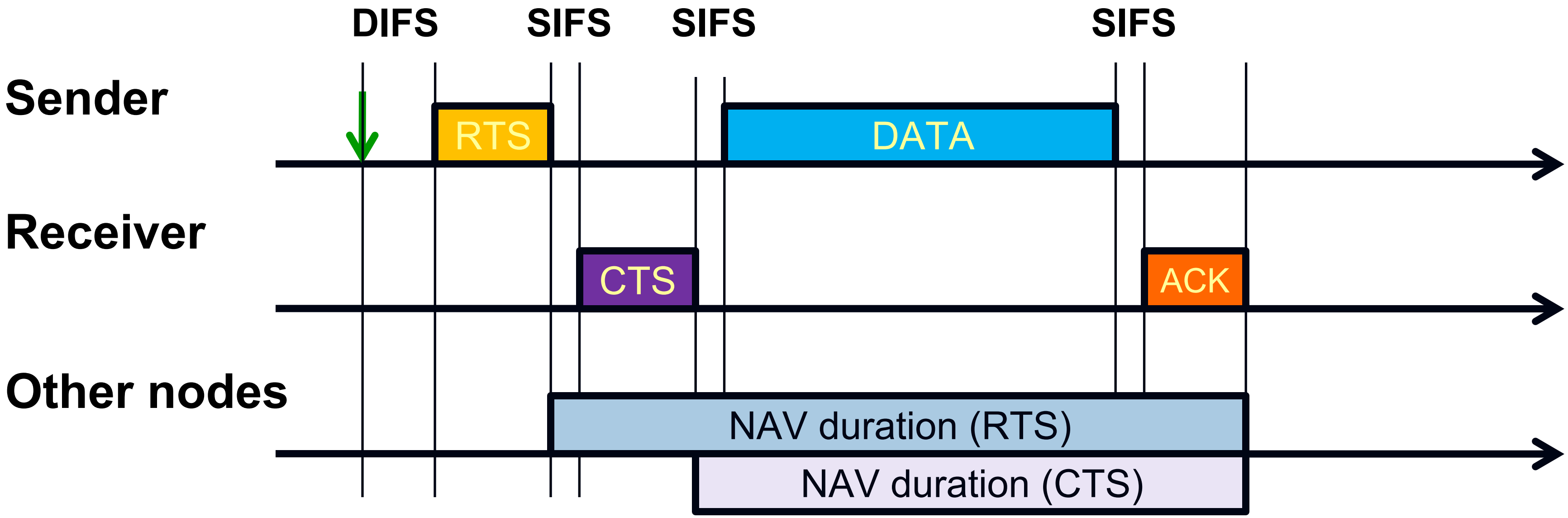
802.11 DCF

- Uses CSMA/CA
- Uses random backoff to avoid collisions
- Can use RTS/CTS to lower collision probability
- Uses positive acknowledgements and sender initiated retries
- DCF state machine can get quite complex
- Incremental NAV-based reservations (virtual carrier sense)

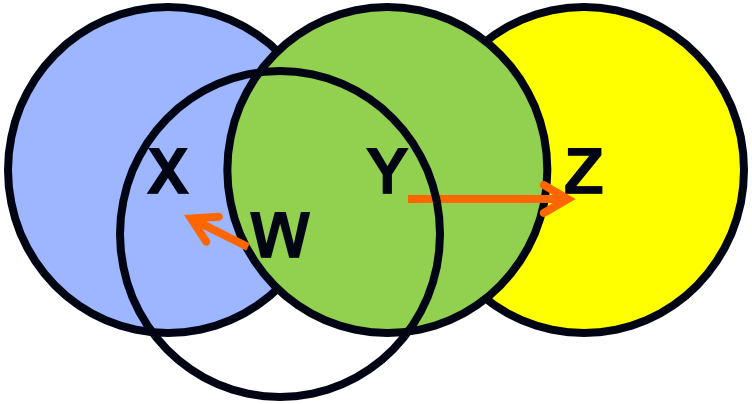
Use of RTS, CTS

- Sender sends a small packet **RTS (request to send)** before sending data
- Receiver sends **CTS (clear to send)**
- All potential senders hearing RTS waits until a CTS is heard from some receiver
- If no CTS, transmit
- If CTS, wait for a time for sender to send data
- Hear RTS, but no CTS, then send
  - Exposed terminal case
- Don’t hear RTS, but CTS receiver is close, don’t send
  - Hidden terminal case

RTS/CTS access method



- Solves hidden node problem ☺
- Introduces exposed node problem ☹
- Reduces time penalty for collisions ☺
- Introduces additional overhead ☹



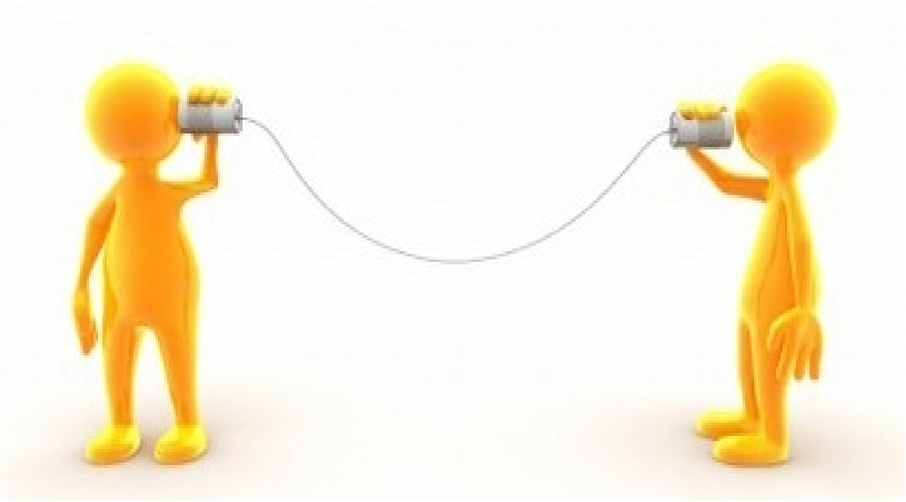
Wireless Network Threat Model

Welcome to the Party

Wireless networking is analogous to a cocktail party

Open Invitation

- Anyone can “talk”, anyone nearby can “listen”
  - We can control connectivity in wired networks, but not in wireless



A Dynamic Occasion

- Everyone is free to move around as they please
  - Physical mobility - that's why we lost the wires, right?
  - Logical mobility – connecting with different peers at different times
- Conversation quantity/load/demand varies
  - Nobody really talks constantly all the time…
- Party conditions change over time
  - Noise, humidity/temperature, obstacles, reflections
- Others: services, roles, energy, …

Limited Engagement

- Each attendee has a limited amount of energy
  - Wireless devices are ideally battery-powered, otherwise why go wireless?

- Not all attendees have the same capabilities:
  - Some are less capable of processing what others say (e.g., less computation capability, 8-bit processors)
  - Some have limited memory (e.g., less storage)
  - Some have a limited vocabulary or speak a different language (e.g., different communication standards)
  - Some are quieter than others (e.g., shorter range of communication)

Coordination?

- Larger social gatherings probably don't have a single coordinator in charge of controlling conversations
  - This type of control is usually more distributed, if existent at all
  - In wireless, APs and gateways act as local controllers, providing access to the cloud, but not controlled by it

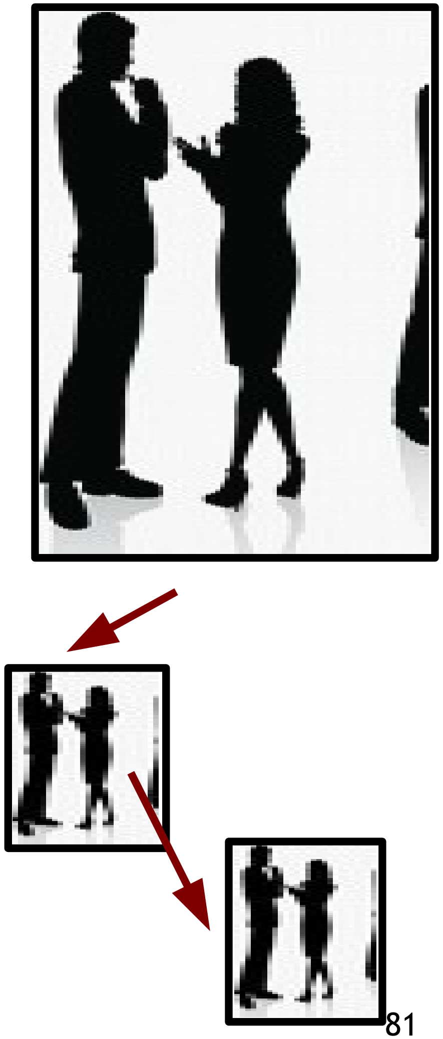
- Competition among (in)dependent sub-groups
  - Think of how many WiFi APs you've seen at once...

How do we deal with these challenges?

“Simplify, Simplify, Simplify”

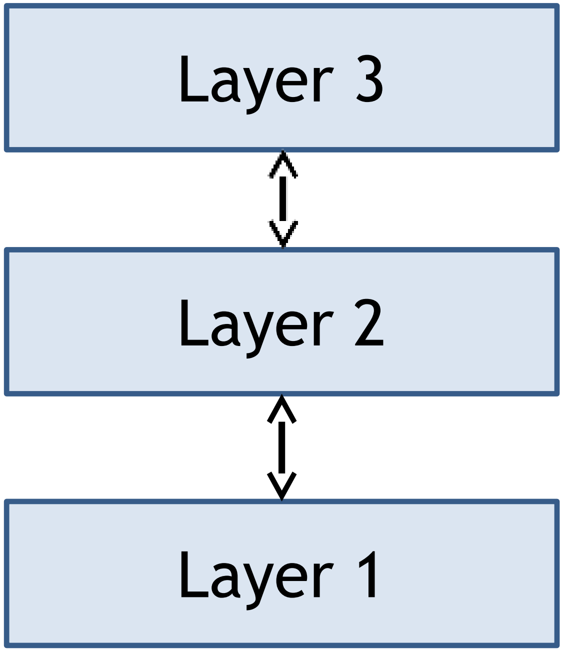
- Thoreau

- Instead of trying to solve all of the possible problems of cocktail party conversation, we decompose the problem into manageable steps
  - Communicating efficiently and effectively to a neighbor
  - Correcting mistakes, repeating, or re-stating
  - Relaying messages to a distant person
  - Making sure messages reach the intended recipient quickly, correctly, efficiently, etc. without annoying the messenger



Layering

- **Layering simplifies network design**
- Layered model:

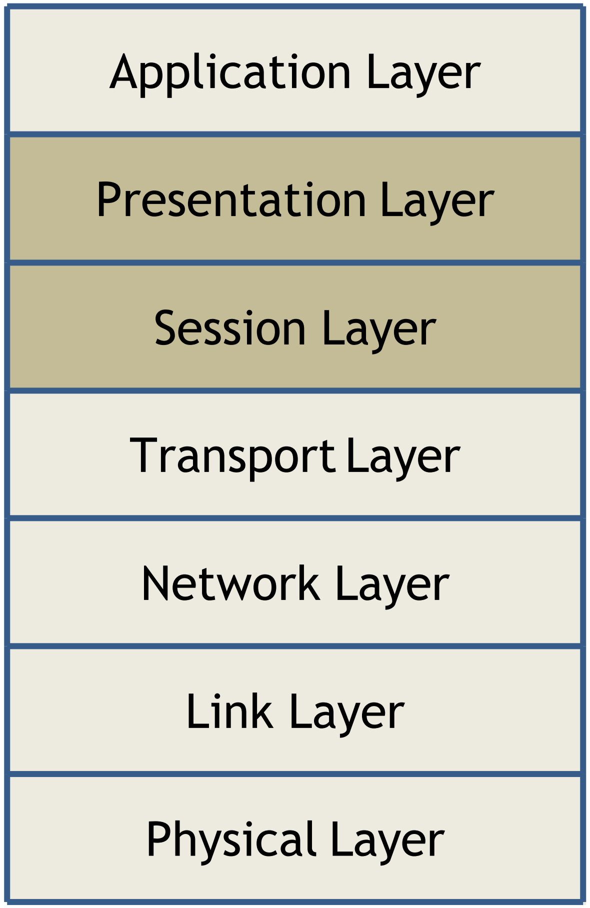


Lower layer provides a service to higher layer

Higher layer doesn’t care (or even know, sometimes) how service is implemented: **lack of transparency**

Layering Standards

- Standard layered model
  - Typically we talk about network layering using the 7-layer ISO Open Standards Interconnection (OSI) Model
  - Other models exist, but everyone seems to like ISO OSI



Application Layer

Presentation Layer

Session Layer

Transport Layer

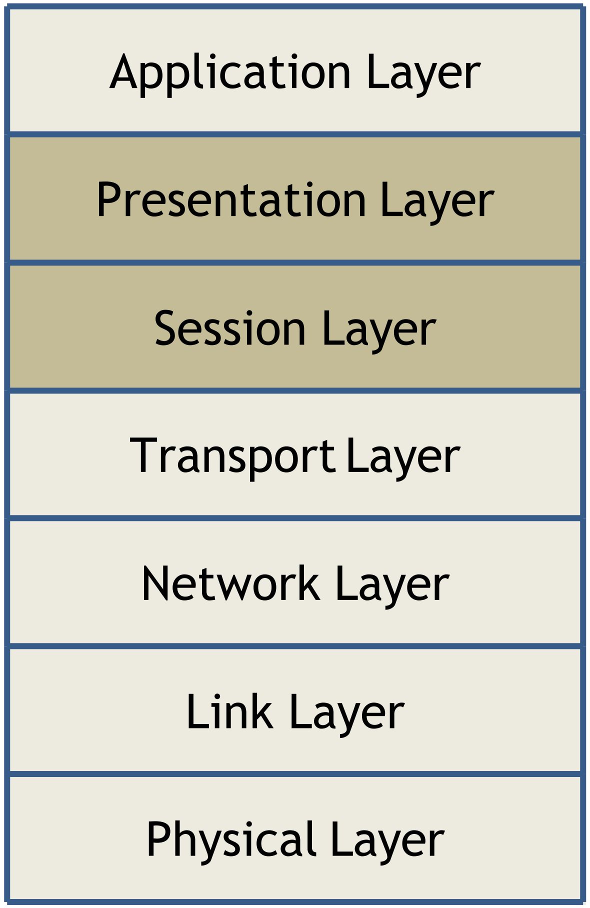
Network Layer

Link Layer

Physical Layer

Layer Functionality

- Application Layer – support network applications
  - Presentation Layer - Compression, encryption, data conversion
  - Session Layer - Establish & terminate sessions
- Transport Layer - *Reliable* end-to-end data transfer
  - Multiplexing, error control, flow and congestion control



Application Layer

Presentation Layer

Session Layer

Transport Layer

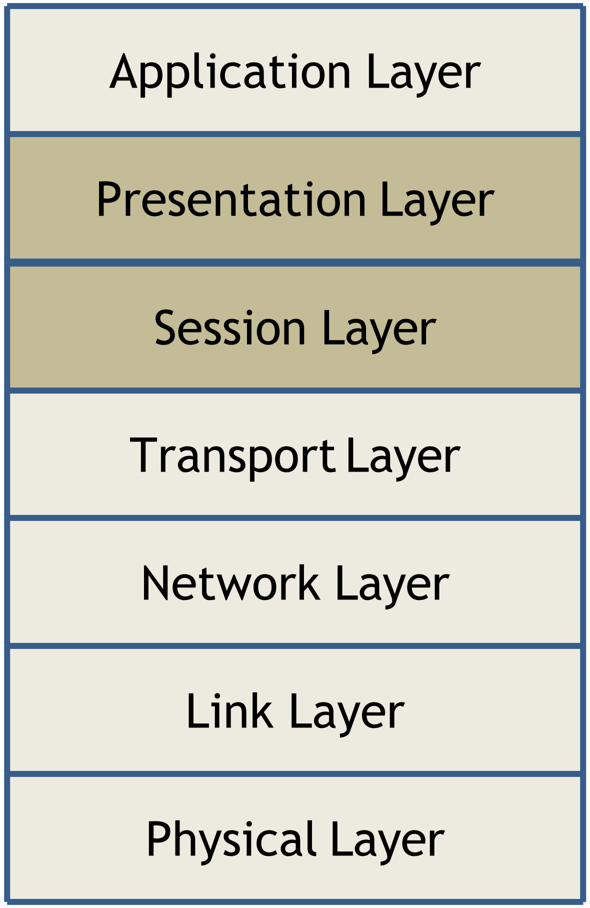
Network Layer

Link Layer

Physical Layer

Layer Functionality

- Network Layer – Addressing and routing
- Link Layer – *Reliable* single-hop data transfer
  - Framing, error detection, medium access control (MAC) sub-layer
- Physical Layer – Moves bits
  - Bit synchronization, modulation & demodulation, physical connections



Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

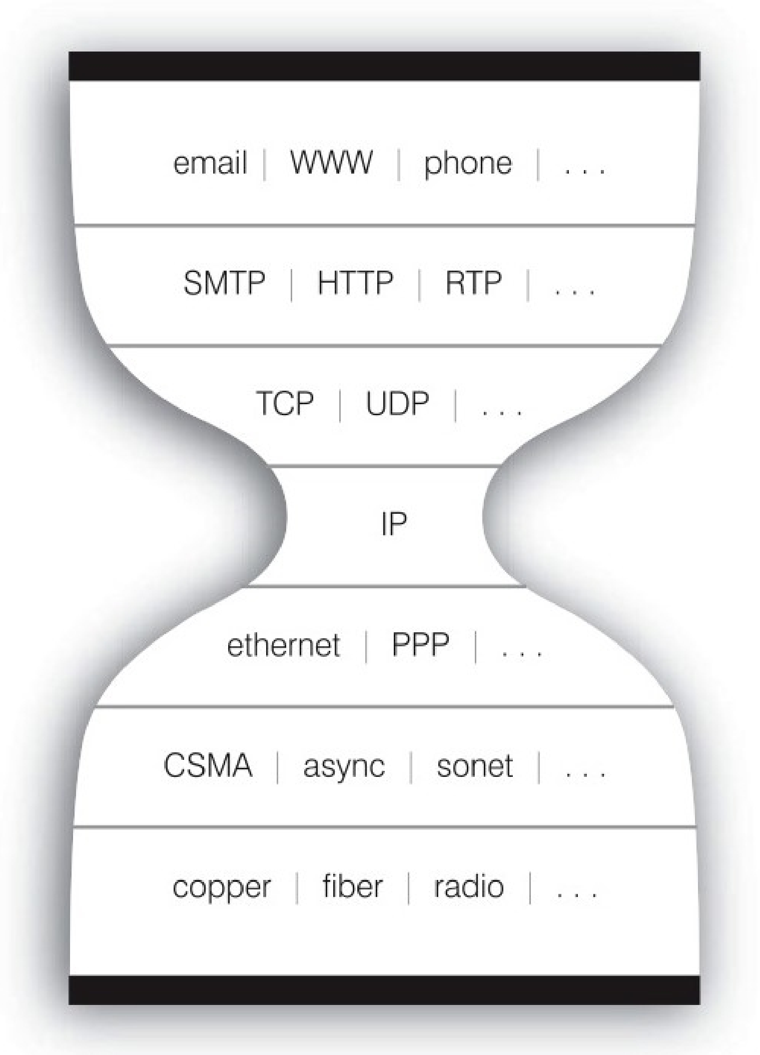
Link Layer

Physical Layer

Internet Layering

- Layered protocols have been the basis of network design for decades

- Layers work great in some scenarios

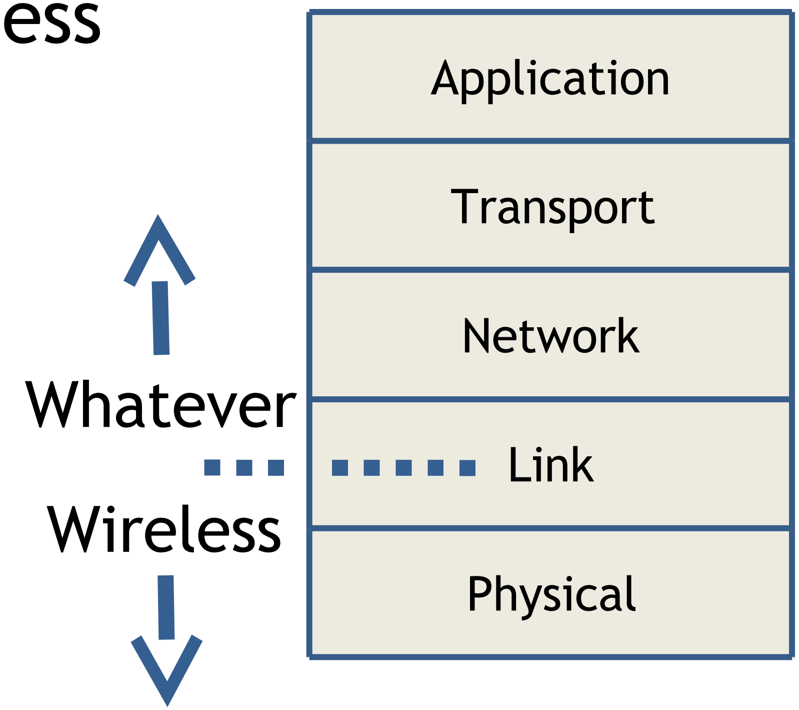

email | WWW | phone | . . .
SMTP | HTTP | RTP | . . .
TCP | UDP | . . .
IP
ethernet | PPP | . . .
CSMA | async | sonet | . . .
copper | fiber | radio | . . .

Layering in Wireless

- Below a certain point, things can be designed for wireless communication

- Above that point, the medium doesn't matter…
  - Or does it?
  - Or should it?

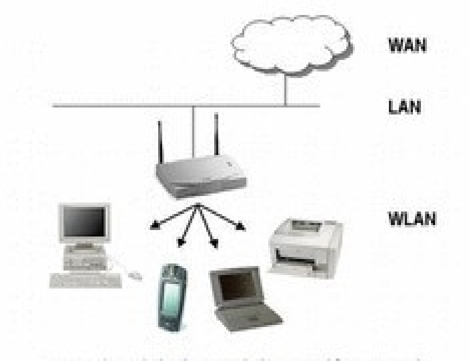
- Trade-offs…



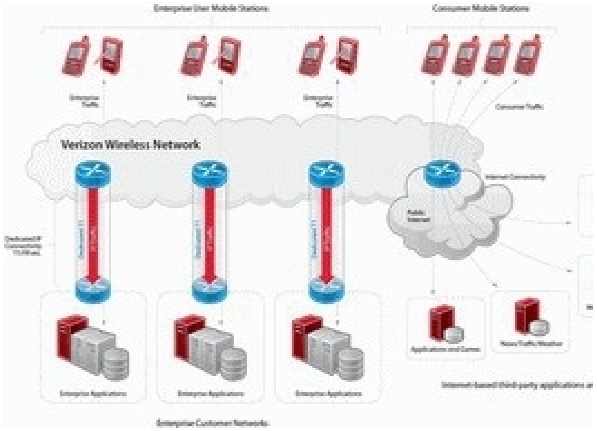
What types of wireless networks are we going to talk about?

Wireless Networks

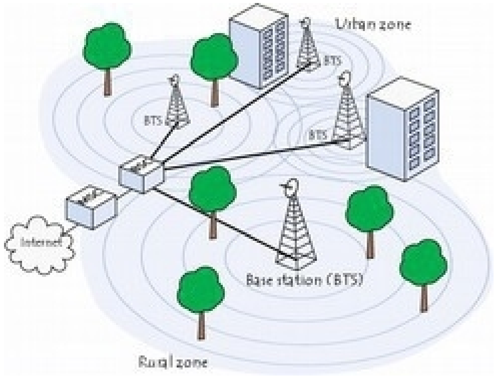
Wireless Internet

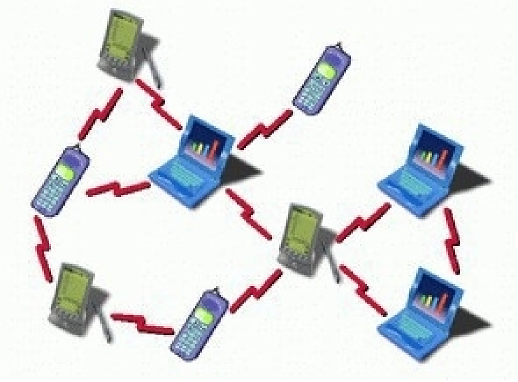


Enterprise Wireless

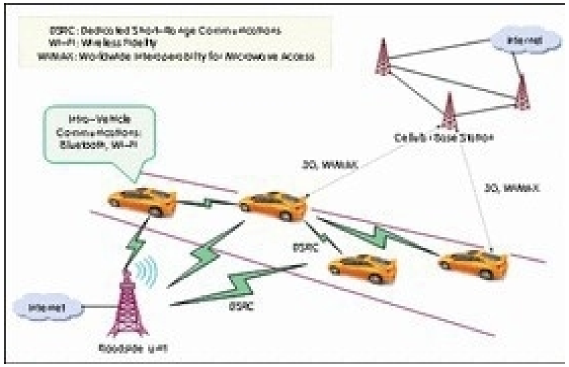


Telecommunications

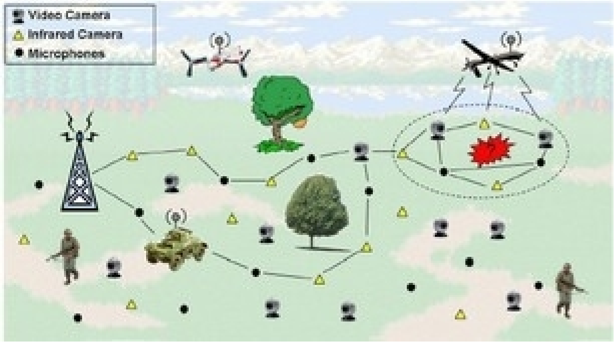




Ad Hoc / Mesh


DSRC : Dedicated Short-Range Communications
Wi-Fi : Wireless Fidelity
WiMAX : Worldwide Interoperability for Microwave Access
Internet
In-Vehicle Communications: Bluetooth, Wi-Fi
Cellular Base Station
3G, WiMAX
3G, WiMAX
DSRC
DSRC
Internet
Roadside unit

Vehicular Networks

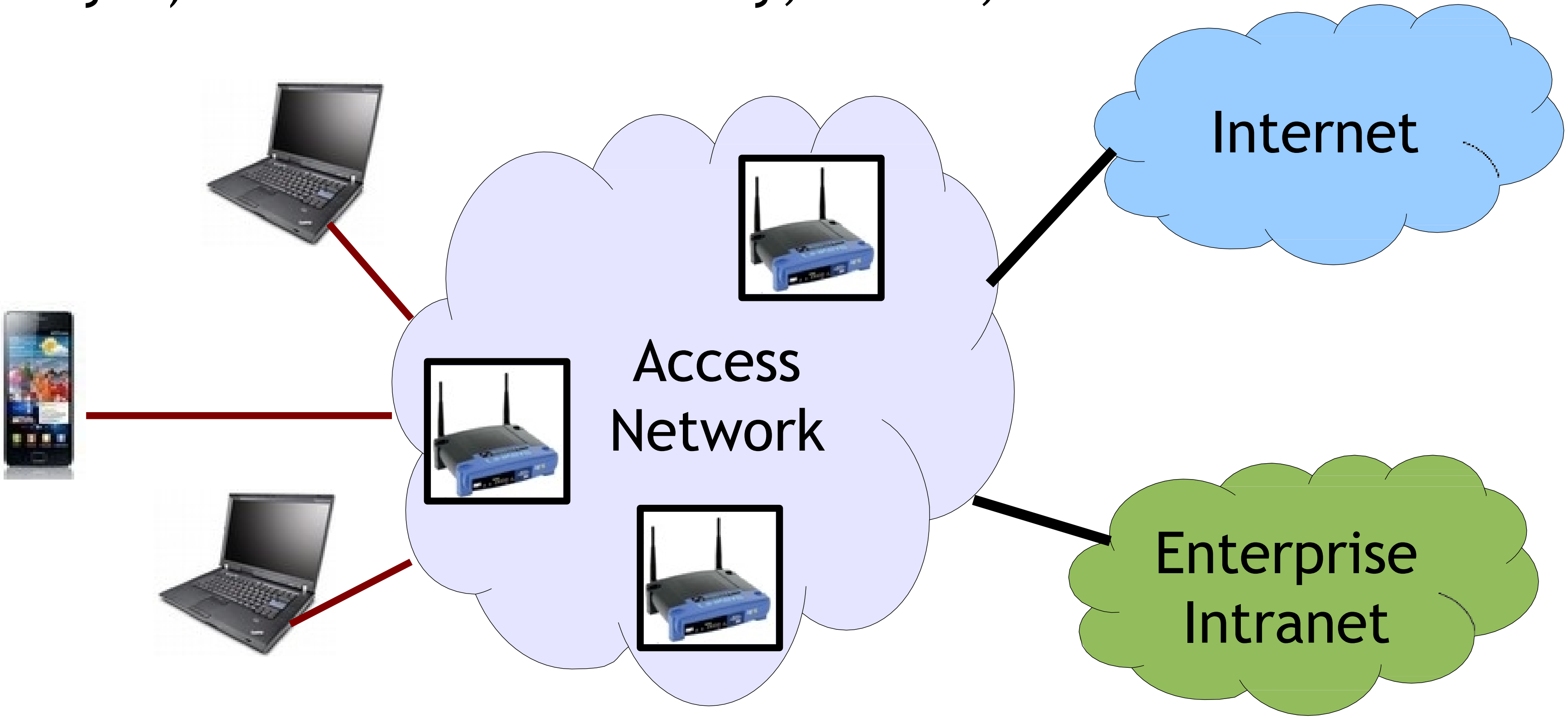


Sensing / Control Systems

And more...

WLAN Systems

- Almost every WLAN system in existence uses the IEEE 802.11 "WiFi" standard
  - 802.11 defines lower-layer services (physical, link, MAC layer) for WLAN connectivity, access, and services

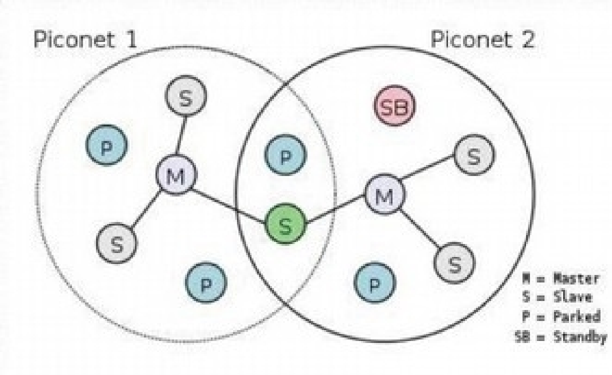


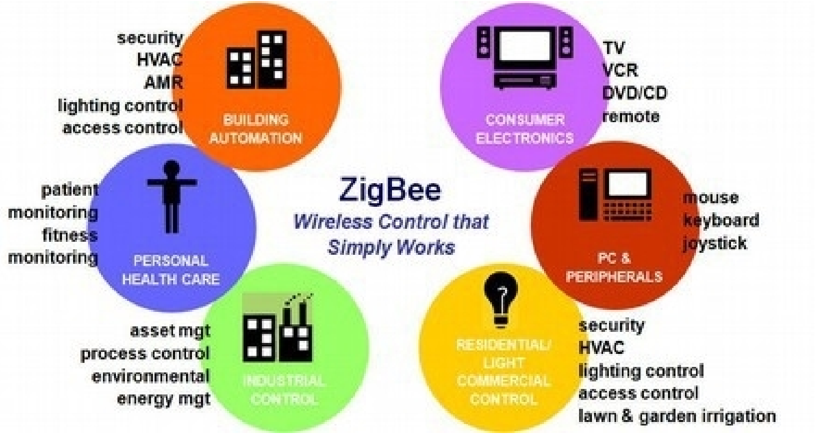
Telecom/Mobile Networks

- Mobile networks have evolved from providing voice connectivity to the PSTN to providing all forms of connectivity to the Internet
  - AMPS first introduced in 1978
  - GSM developed through the 1990s- 2000s
  - 3G/4G standards emerged with full data support, looking more like a WLAN/WMAN

Personal Area Networks

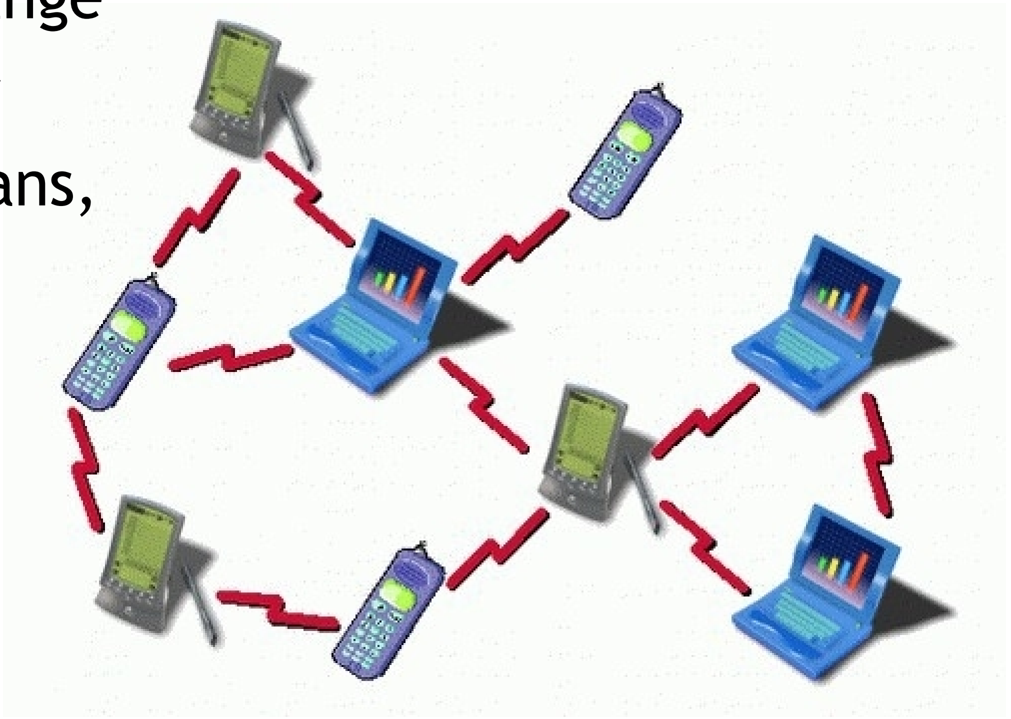
- Local "device-to-device" networking using the 802.15 family of standards
- Typically short range, few devices, low power
- Commonly used for home, personal, office





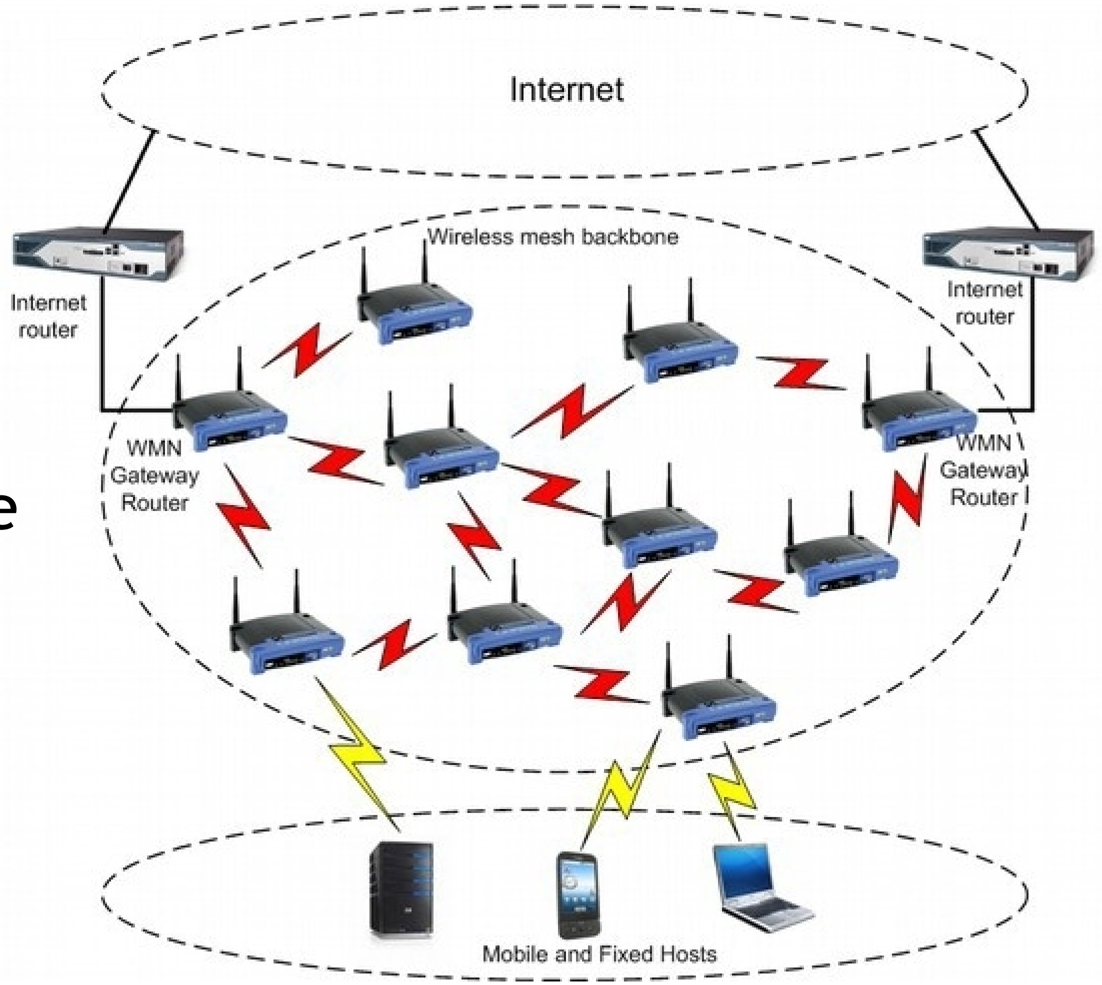
Mobile Ad Hoc Networks

- Mobile ad hoc networks (MANETs) typically connect local/offline devices with no Internet connection
  - Device-to-device, no APs
  - Peer-to-peer data exchange
  - In-network services only
  - Sometimes involve humans, but sometimes don't
  - No central server
  - No authority
  - No backhaul



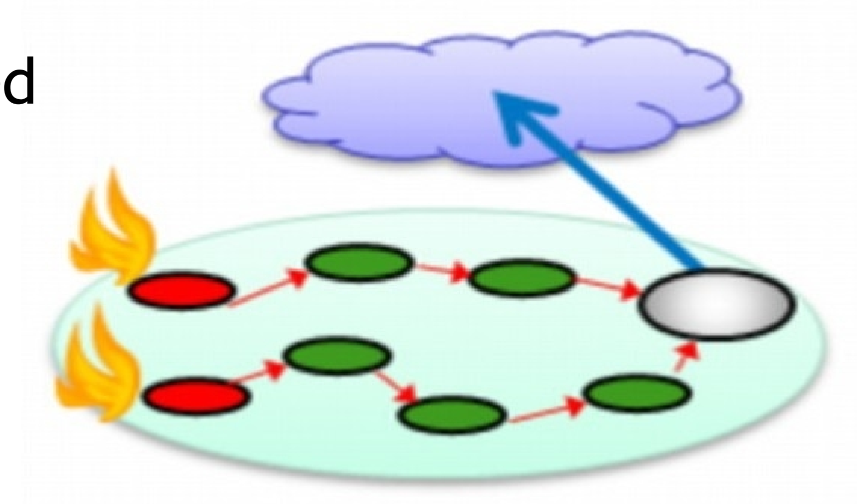
Wireless Mesh Networks

- Mesh networks provide multi-hop wireless connections to a backhaul
  - Mesh routers can be fixed or mobile, serve as multi-hop Internet connectivity
  - Hosts are typically mobile, hand-off to mesh routers



Sensor Networks

- Mostly use ZigBee (based on 802.15.4) or WiFi depending on requirements
  - Sensor networks are typically closer to a mesh architecture: multi-hop to one/many APs
  - Intermittent low-rate traffic, mostly sensor readings from nodes back to APs
  - Heavily resource-constrained
  - Designed for life-time

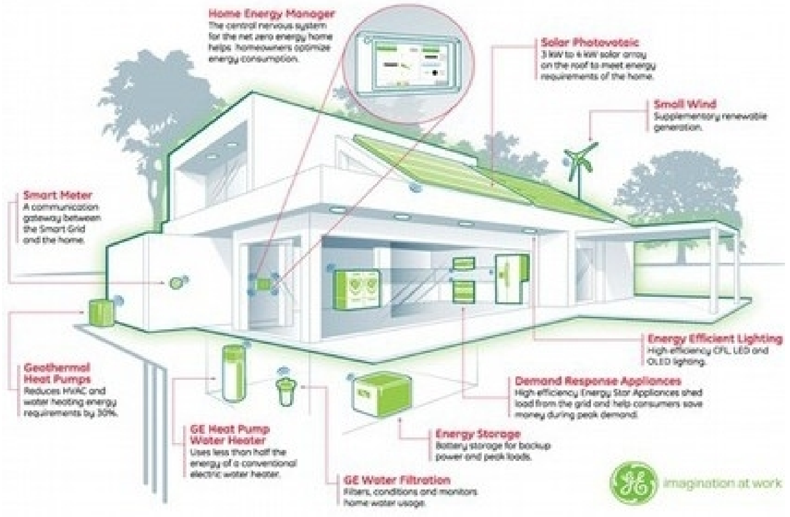


Home Networks

- In-home networked systems (Smart Home)
  - Entertainment/media
  - Appliances, etc.

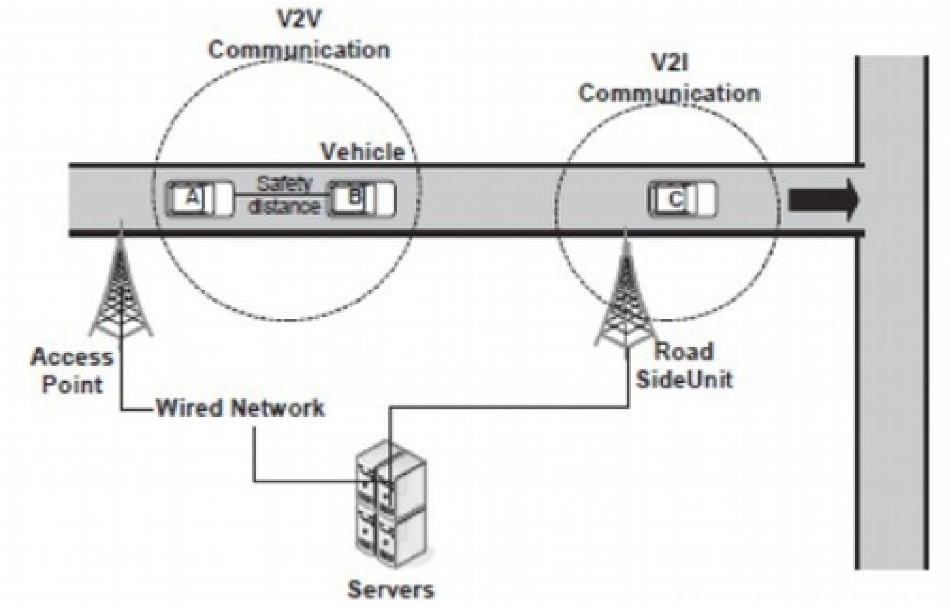
- Home energy networks
  - The home side of the smart grid, between the smart meter and user
  - Mostly wireless (802.15.4, etc.)

AUTO CURTAIN
HOME ENTERTAINMENT
COMMUNICATION
MOODS
HOME AUTOMATION
GARAGE
AUTO SPRINKLERS
ON OFF
AUTO LIGHTING
HOME BACK UP SYSTEM
SECURITY
eCAM


Home Energy Manager
The central nervous system for the net zero energy home helps homeowners optimize energy consumption.
Solar Photovoltaic
3 kW to 4 kW solar array on the roof to meet energy requirements of the home.
Small Wind
Supplementary renewable generation.
Smart Meter
A communication gateway between the Smart Grid and the home.
Energy Efficient Lighting
High efficiency CFL, LED and OLED lighting.
Geothermal Heat Pumps
Reduces HVAC and water heating energy requirements by 30%.
Demand Response Appliances
High efficiency Energy Star Appliances shed load from the grid and help consumers save money during peak demand.
GE Heat Pump Water Heater
Uses less than half the energy of a conventional electric water heater.
Energy Storage
Battery storage for backup power and peak loads.
GE Water Filtration
Filters, conditions and monitors home water usage.
imagination at work

VANETs

- VANET = Vehicular ad hoc network
  - Cars talk among each other and with roadside infrastructure

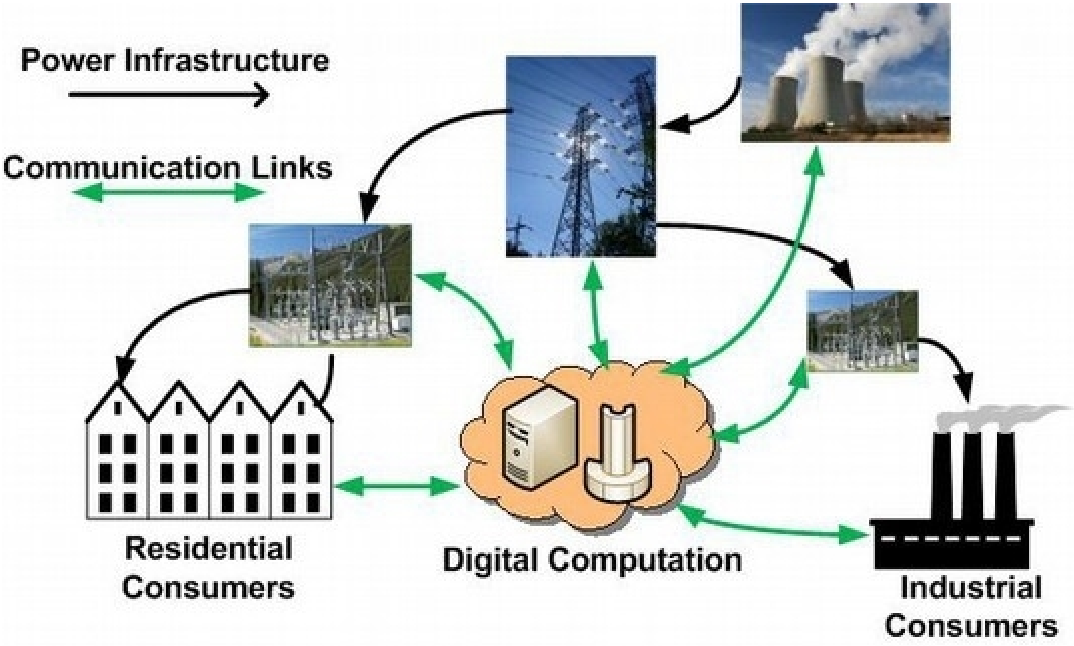


- Applications of interest:
  - Automated driver safety management
  - Passive road quality / condition monitoring
  - In-car entertainment
  - Navigation services
  - Context-aware rec's:
    - “This alternate route would be faster, and it would go past your favorite Primanti Bros.”

Smart Grid

- The Smart Grid incorporates hybrid wired/wireless communications into the energy grid

- Applications of interest:
  - Dynamic pricing
  - Improved efficiency
  - Home energy mgmt.
  - Disaster/outage recovery



What is Wireless Network Security?

A probabilistic guarantee that a wireless network does a particular job as expected, even when faced with a variety of threats.

E.g., Confidentiality, Integrity, Authenticity…

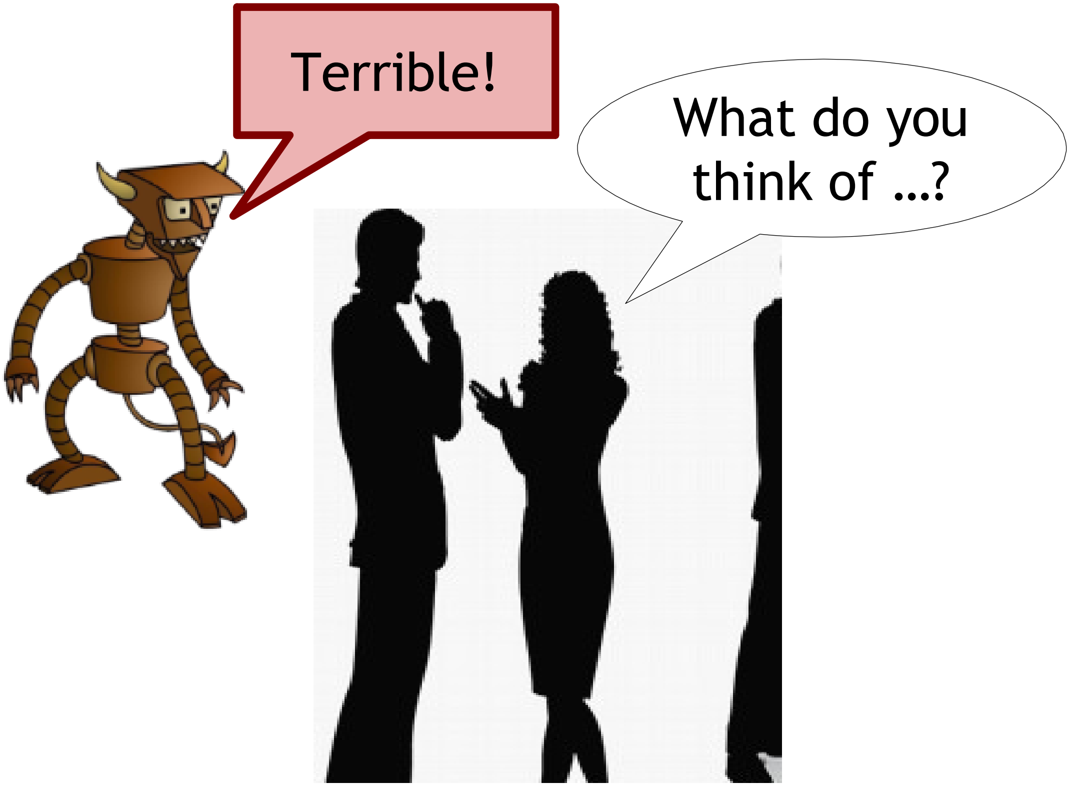
Threats of Interest

- Many different types of threats faced in wireless
- Including (but not limited to) threats to:
  - Information content, source, etc.
  - Availability of wireless connectivity
  - Performance of network protocols
  - Proper use of scarce resources (energy, bandwidth, …)
  - Proper use of command/control messages
  - Correct representation of devices
  - …
- All of these are composed of certain primitives

Eavesdropping

Interference

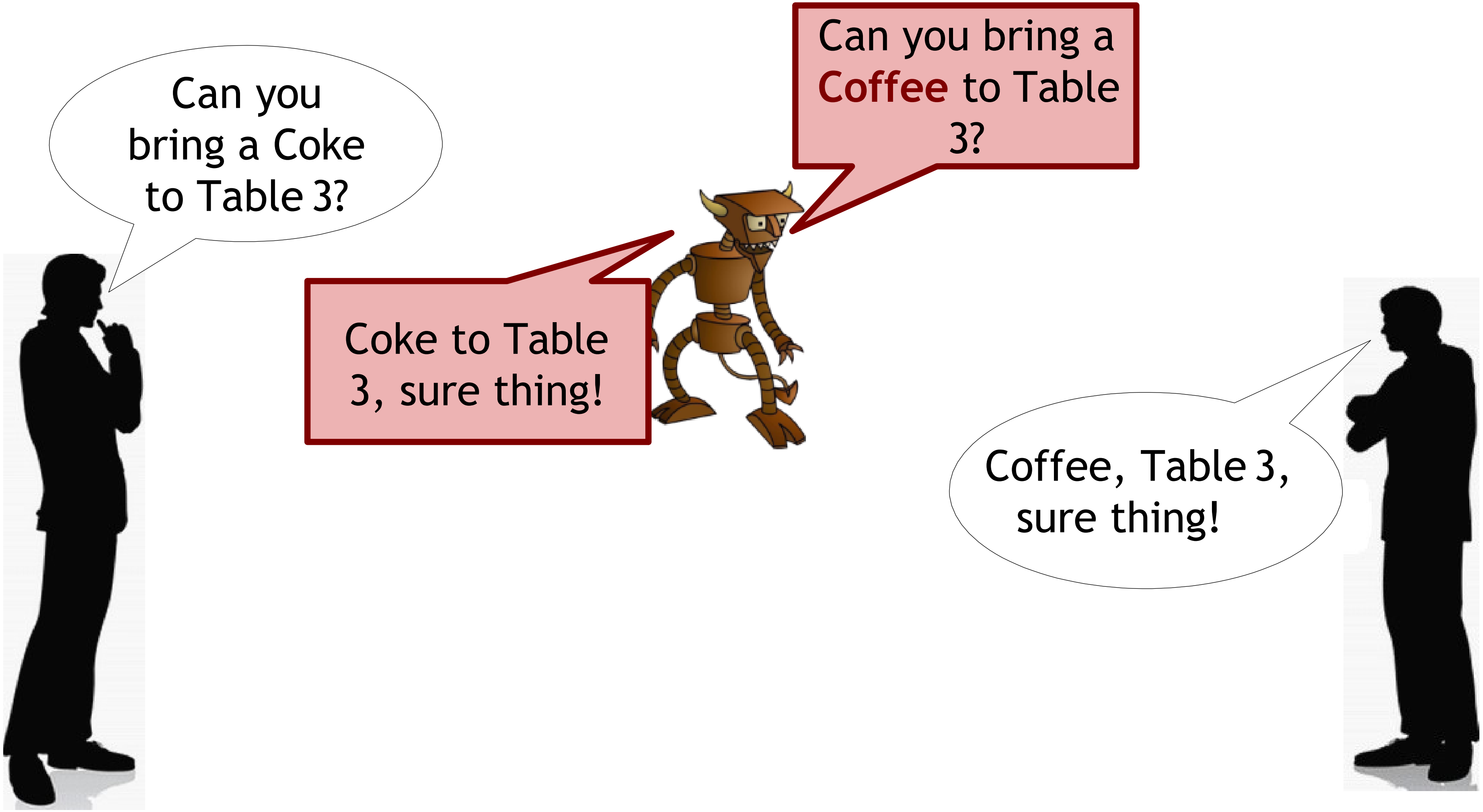
Msg/Pkt/Signal Injection/Replay



Can you speak up?
Can you speak up?
Can you speak up?
Can you speak up?

Spoofing

Man-in-the-Middle Attack



Can you bring a Coke to Table 3?

Coke to Table 3, sure thing!

Can you bring a **Coffee** to Table 3?

Coffee, Table 3, sure thing!

Byzantine Threats

- Byzantine threat is sort of like insider threat
- Basically, an authenticated / valid / trusted group member stops following the rules

And Many More...

- Denial/Degradation of Service
- Exploiting Composition Issues
- Context Manipulation
- …

Our plan.

We‘ll study how these various threats manifest at different layers and in different types of wireless systems.