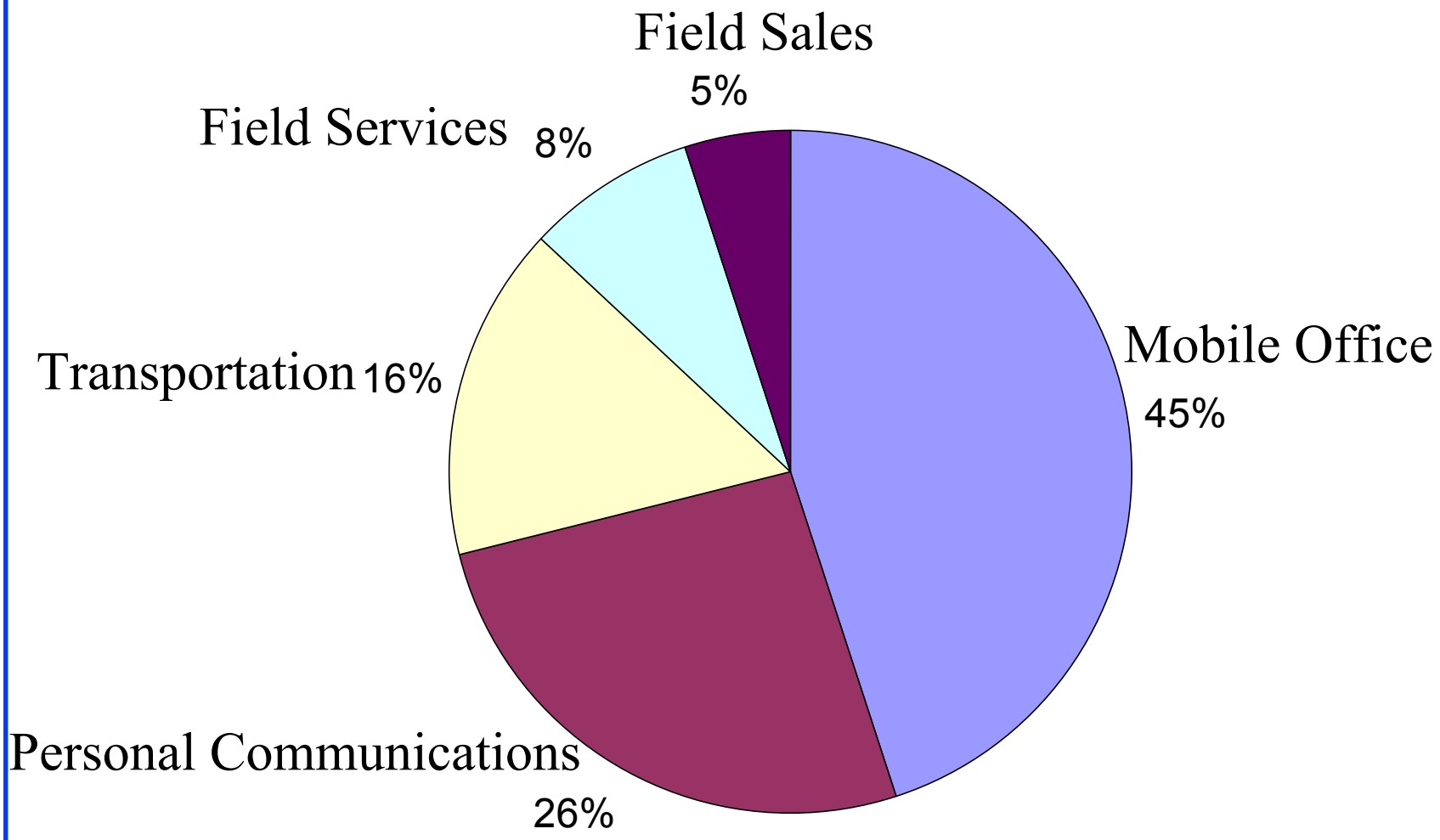
Wireless Data Networking IEEE 802.11 & Overview of IEEE 802.11b

Dr. Arian Durresi
The Ohio State University
Columbus, OH 43210
durresi@cis.ohio-state.edu

- Wireless Application Market
- Wireless WANs
- Wireless LANs
- ISM band
- Spread Spectrum
- Wireless LAN standard: IEEE 802.11
- Overview of IEEE 802.11b

.

Mobile Application Market by 2005



[Dayem 97]

Wireless WANs

- Data over Analog and Digital Cellular, ARDIS, RAM Mobile Data, Cellular Digital Packet Data (CDPD)
- 4.8 kbps to 19.2 kbps nominal,
- Packetized short transmission, Email, stock quotes, weather, Wired backbone
- 3G Goals:
  - Multi-rate: 2Mbps indoor, 384 kbps pedestrian, 144 kbps mobile
  - Multi-service: Mobile Internet, Multimedia, packet and circuit switched services
  - Multi-cell: Seamless coverage across pico-, micro-, and macro-cells

Wireless LANs

- High speed: > 1Mbps
- Real time voice not supported
- About 50 m coverage radius
- Pedestrian speed
- Industry Scientific Medical (ISM) band LANs
  - Use Spread Spectrum not to interfere with primary users
  - IEEE 802.11, IEEE 802.11a, IEEE 802.11b, Hiperlan
- Infrared LANs: Limited applications
- Unlicensed Personal Communication Services (UPCS): will use dedicated bandwidth: 1910-1930MHz

Wireless WANs versus LANs

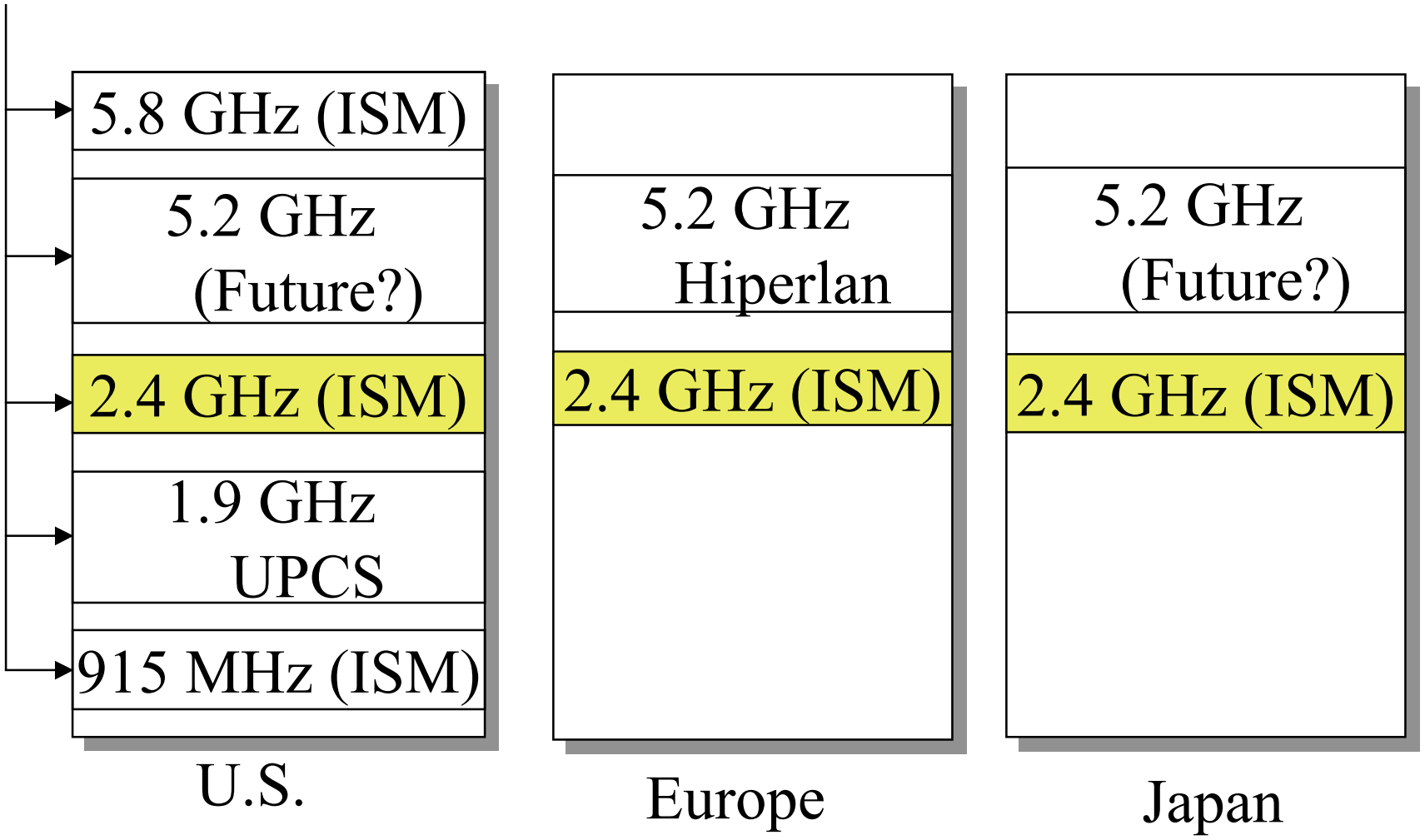
- Different from wired WANs versus LANs
  - In wireless direct competition
  - Wired LANs: high bandwidth, cheap, everywhere
- Business issues
  - Services
  - Coverage
  - Price
- Technical Issues
  - Bandwidth, capacity, mobility
  - Security
  - Software applications

ISM band in US

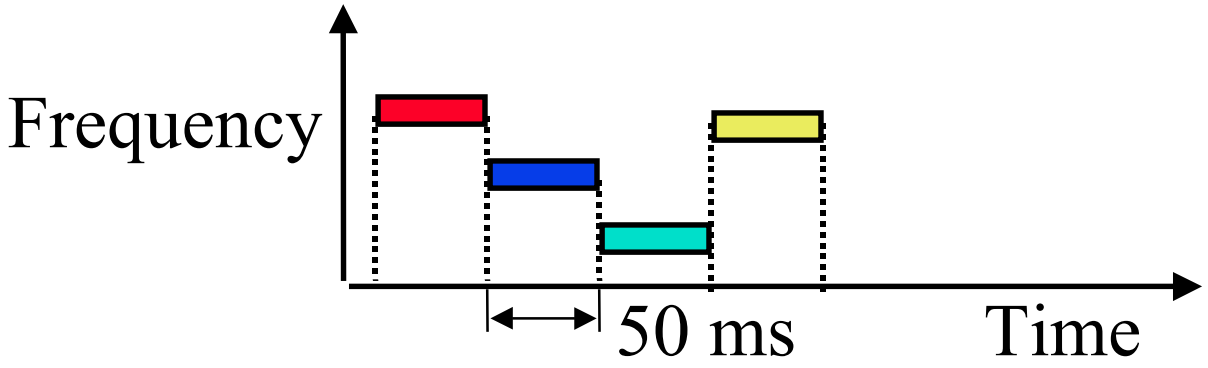
Band (GHz)	Bandwidth MHz	Power Level	Spread Spectrum
0.902	26	1W	FHSS, DSSS
2.4	83.5	1W	FHSS, DSSS
5.725	125	1W	FHSS, DSSS
24	250	50mv/m @3m	NA

Why 2.4 GHz?

IEEE 802.11

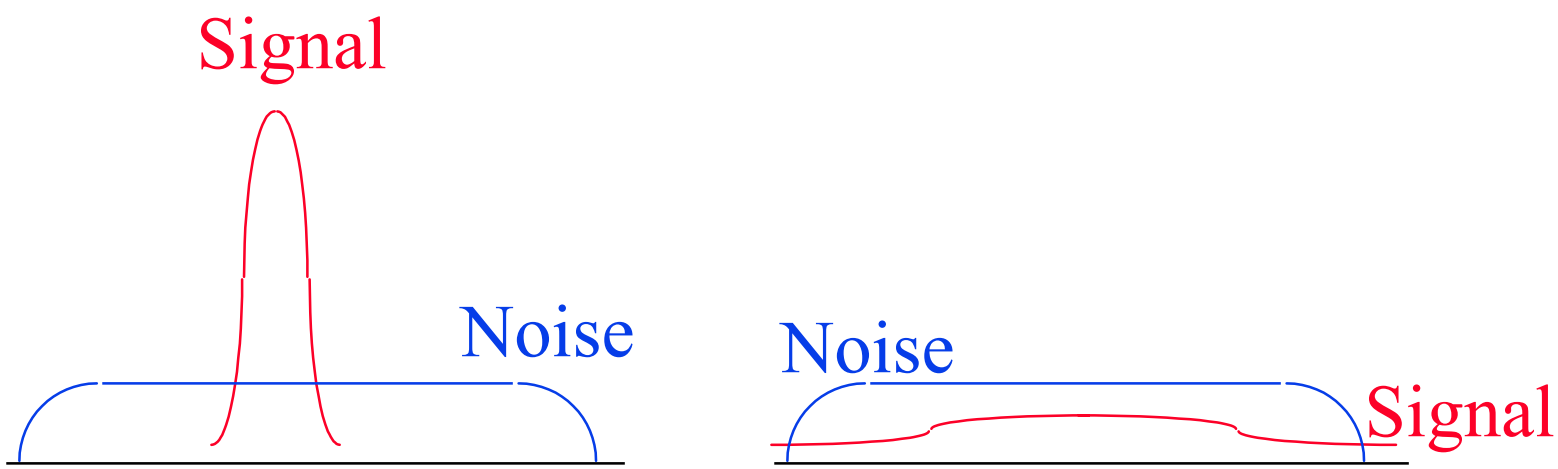


Frequency Hopping Spread Spectrum



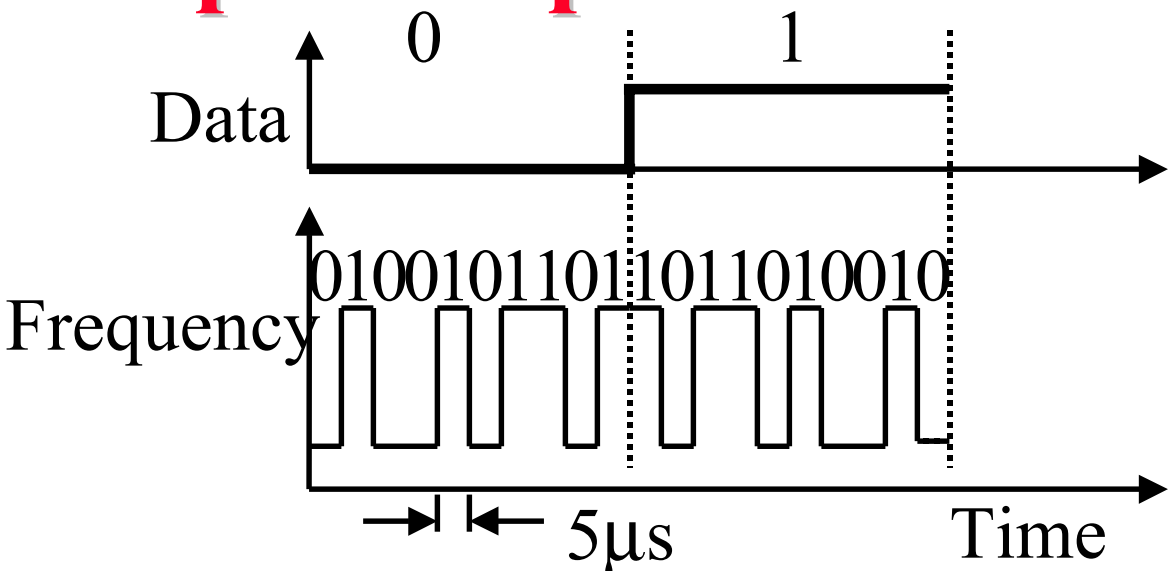
- Pseudo-random frequency hopping
- Spreads the power over a wide spectrum
  $\Rightarrow$ Spread Spectrum
- Developed initially for military
- Patented by actress Hedy Lamarr
- Narrowband interference can't jam

Spectrum



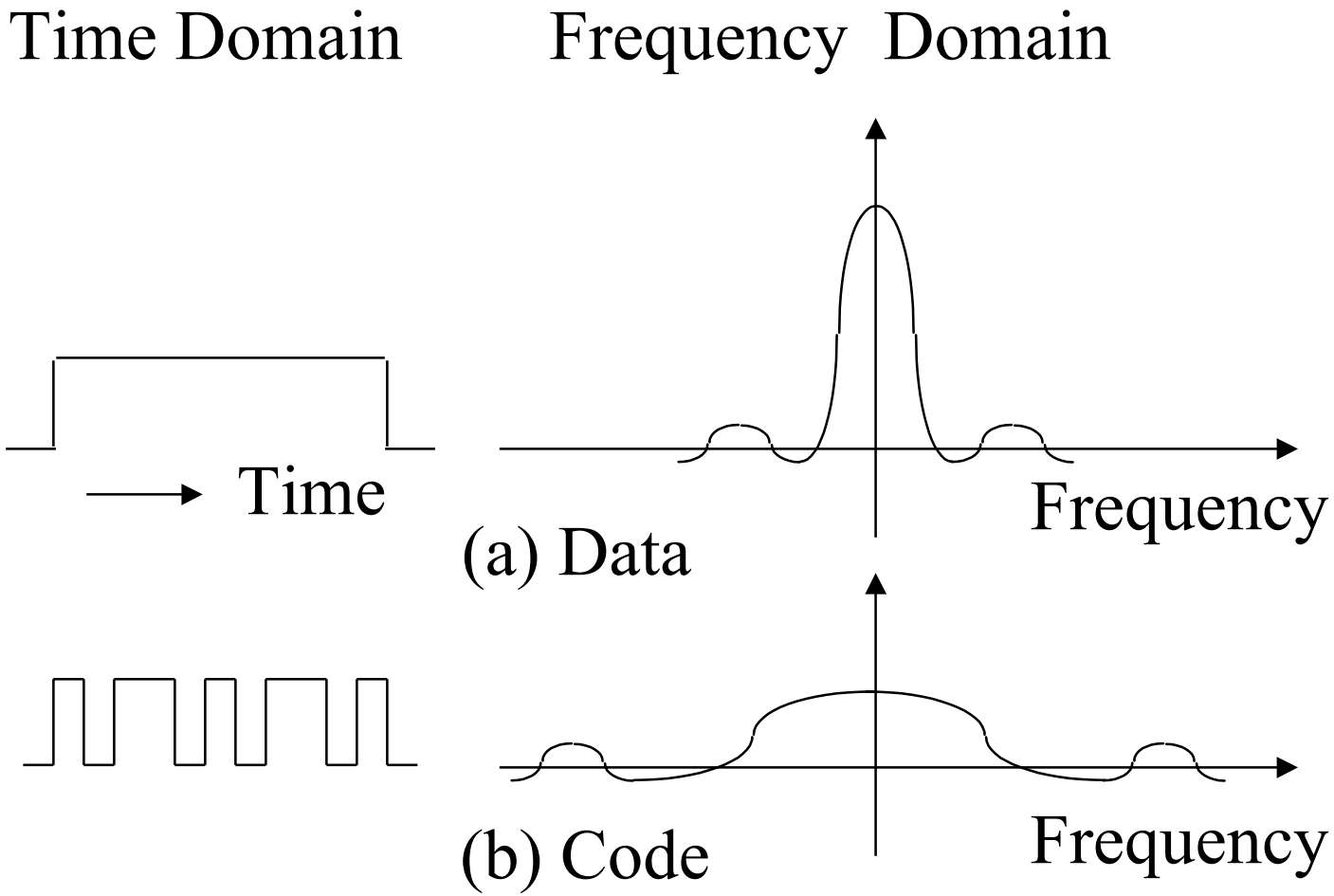
(a) Normal (b) Frequency Hopping

Direct-Sequence Spread Spectrum



- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒Interference⇒ Orthogonal

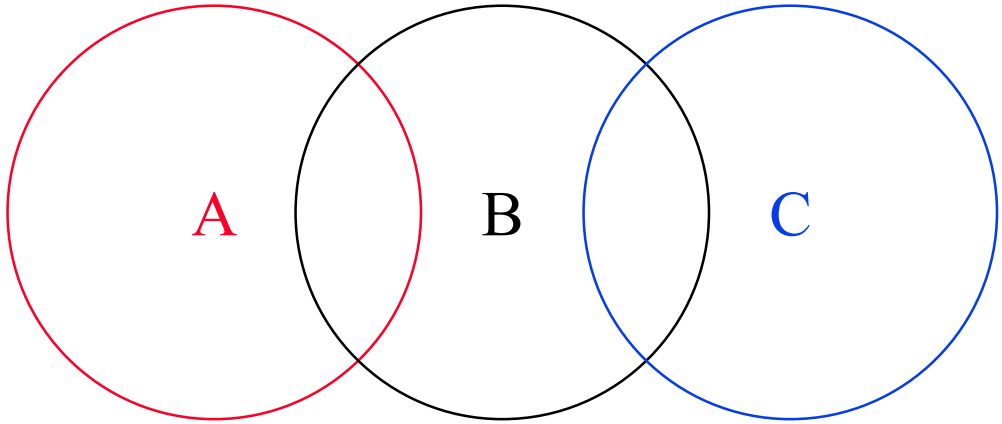
DS Spectrum


Time Domain
Frequency Domain
Time
Frequency
(a) Data
(b) Code
Frequency

IEEE 802.11 Features

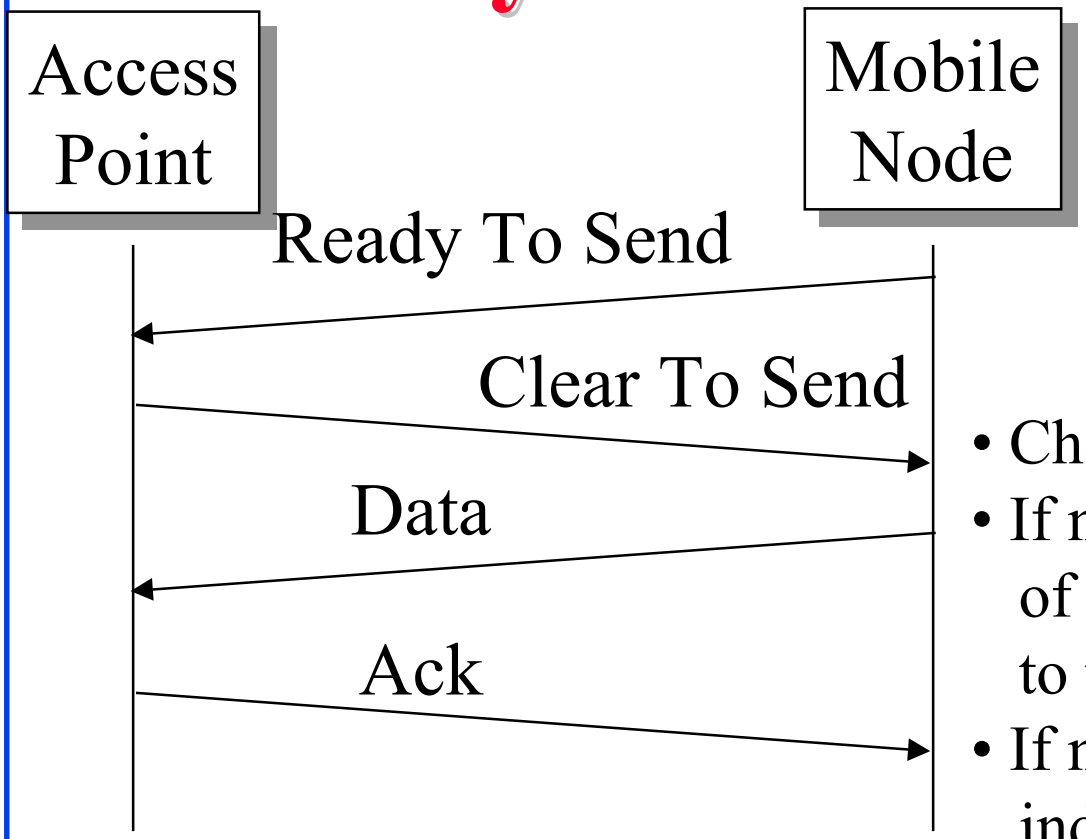
- Standard for WLANs approved by IEEE 802.11 Working Group in June 1997
- 1 and 2 Mbps
- Asynchronous, connectionless service
- Supports both Ad-hoc and base-stations
- Spread Spectrum ⇒ No licensing required.
  Three Phys: Direct Sequence, Frequency Hopping, 915-MHz, **2.4 GHz** (Worldwide ISM), 5.2 GHz, and Diffused Infrared (850-900 nm) bands.
- Supports multiple priorities
- Supports time-critical and data traffic
- Power management allows a node to doze off

Hidden Node Problem



- C cannot hear A.
  It may start transmitting while A is also transmitting
  $\Rightarrow$ A and C can't detect collision.
- Only the receiver can help avoid collisions

4-Way Handshake



- Check if carrier is present
- If no carrier, check the table of CTS if anyone is going to transmit at that time
- If no carrier and the table indicates the medium free then transmit

IEEE 802.11 MAC

- Two access methods:
  - Distributed Coordination Function
  - Point Coordination Function
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Ethernet CSMA/CD Collision Detection
- Collision Detection not suitable for wireless:
  - Need full duplex radio => increase the price
  - Not all stations can hear each other
- CA: Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- CA: Can not detect collision $\Rightarrow$ Each packet is acked

IEEE 802.11 MAC (cont.)

- MAC level retransmission if not acked
- Virtual Carrier Sense: Avoids collision by sending a short message: Ready To Send (RTS):
  - Contains source and dest. addresses + duration of message. Tells everyone to backoff for the duration.
- Destination sends: Clear To Send (CTS)
- All stations receiving RTS and/or CTS set their timer: NAV (Network Allocation Vector) for the given duration
- RTS/CTS short=>reduced overhead of collisions

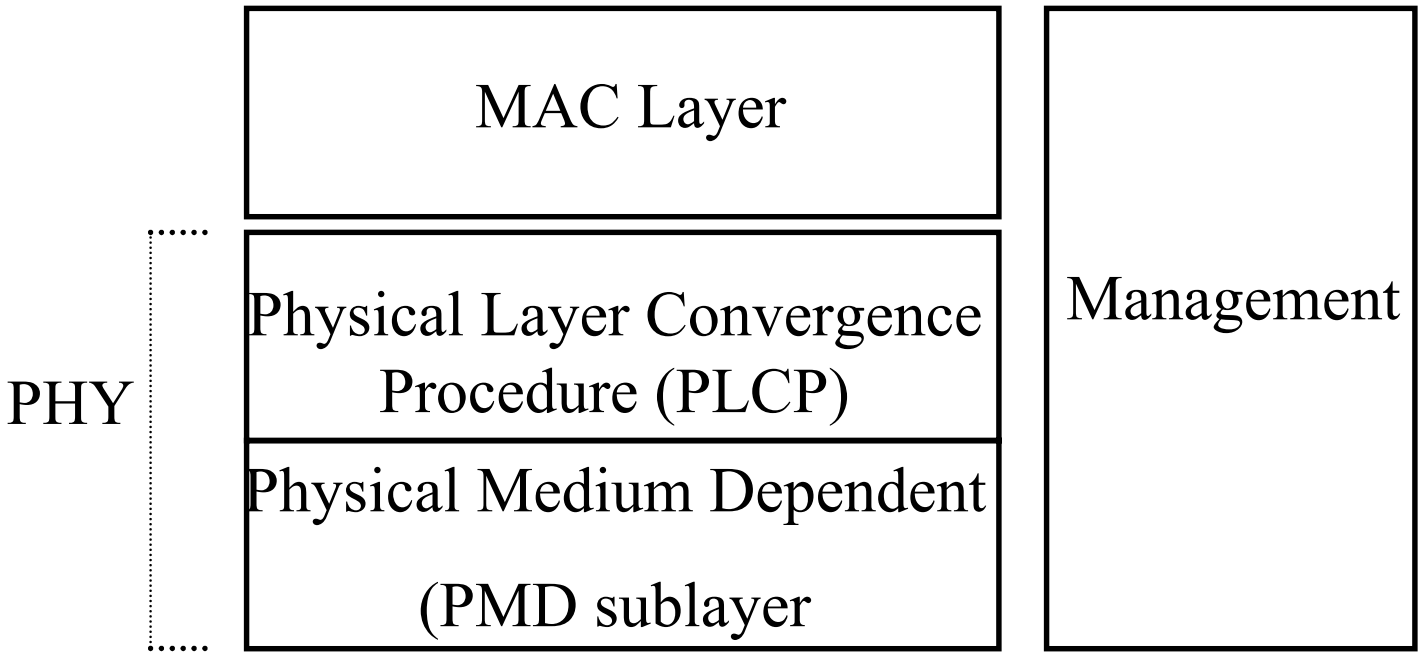
IEEE 802.11 MAC (cont.)

- Why shorter packets than wired?
  - Higher BER=>increased probability of packet corruption
  - In case of packet corruption, smaller the packet-less overhead by retransmission
  - In Frequency Hopping (jump every 20 msec) better short packets
- To be able to deal with Ethernet packet=> Fragmentation and Reassembly
  - Send and wait for each fragment
  - Can transmit to others while waiting

Peer-to-Peer or Base Stations?

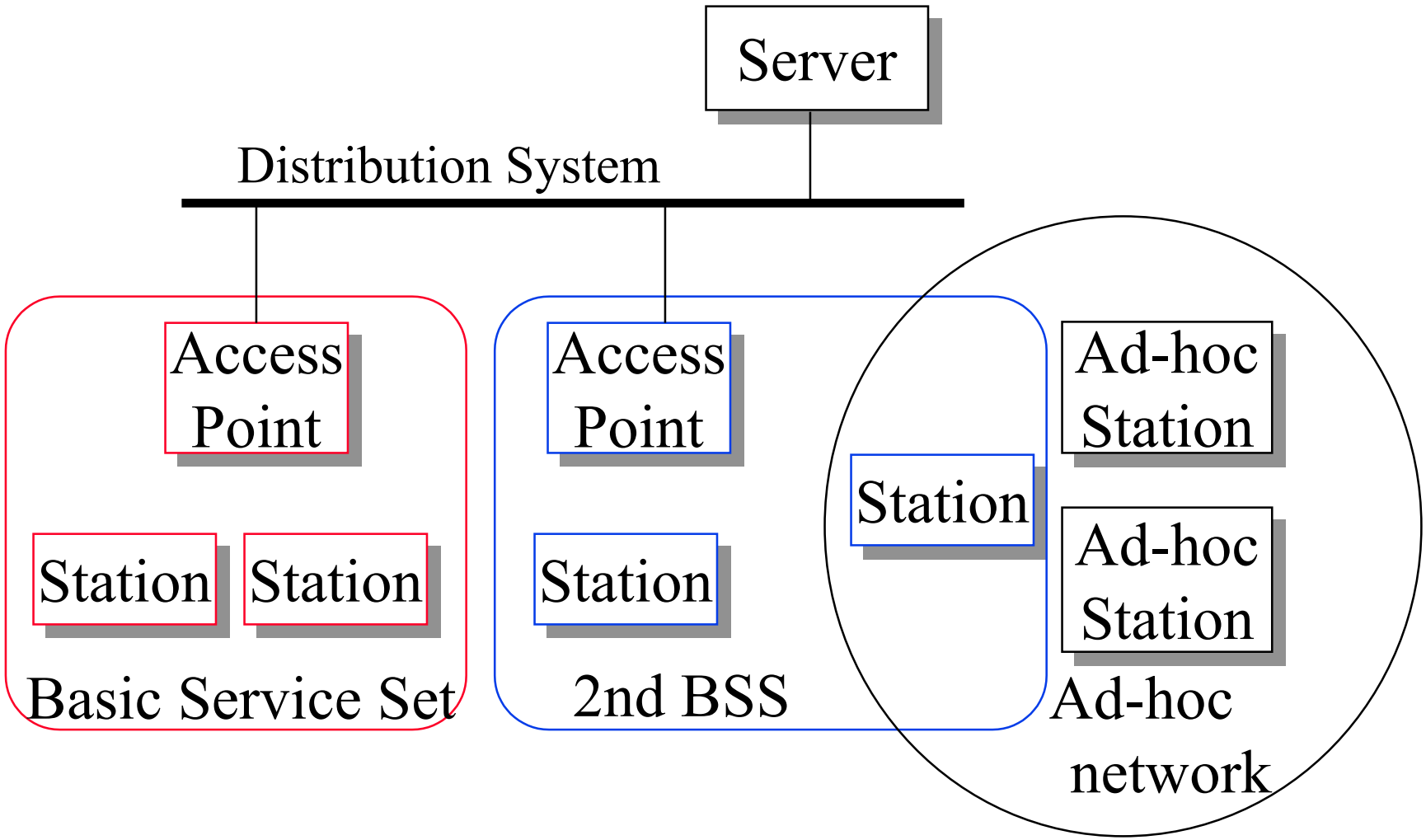
- Ad-hoc (Autonomous) Group:
  - Two stations can communicate
  - All stations have the same logic
  - No infrastructure, Suitable for small area
- Infrastructure Based: Access points (base units)
  - Stations can be simpler than bases.
  - Base provide connection for off-network traffic
  - Base provides location tracking, directory, authentication ⇒ Scalable to large networks
- IEEE 802.11 provides both.

Architecture of 802.11



- PLCP simplifies the interface to MAC
- PMD provides a clear channel assessment mechanism, a transmission and a reception mechanism

IEEE 802.11 Architecture



BSS Services

- Coordination Function: distributed in ad hoc or in AP
- Join a BSS, needs to get synchronization information from AP:
  - Passive Scanning: waits to receive a Beacon Frame sent periodically from AP
  - Active Scanning: tries to locate an AP by transmitting Probe Request Frame and wiats for Probe Response from AP
- Authentication: a station convinces an AP or other station of its identity exchanging passwords
- Association: exchange information about station and BSS capabilities and allow the network to know the location of the station

BSS Services (cont.)

- Roaming: Handover of a station from one AP to another without losing connection. Similar to cellular handover with two differences:
  - In LANs the handover is easier because between packet transmission
  - A temporary disconnection reduce significantly the performance in LAN, for voice no problem
- Keeping Synchronization: necessary for hopping, power saving + etc.
  - AP periodically transmits Beacon Frames, which contain the value of AP's clock when transmitted
  - The stations correct their clocks

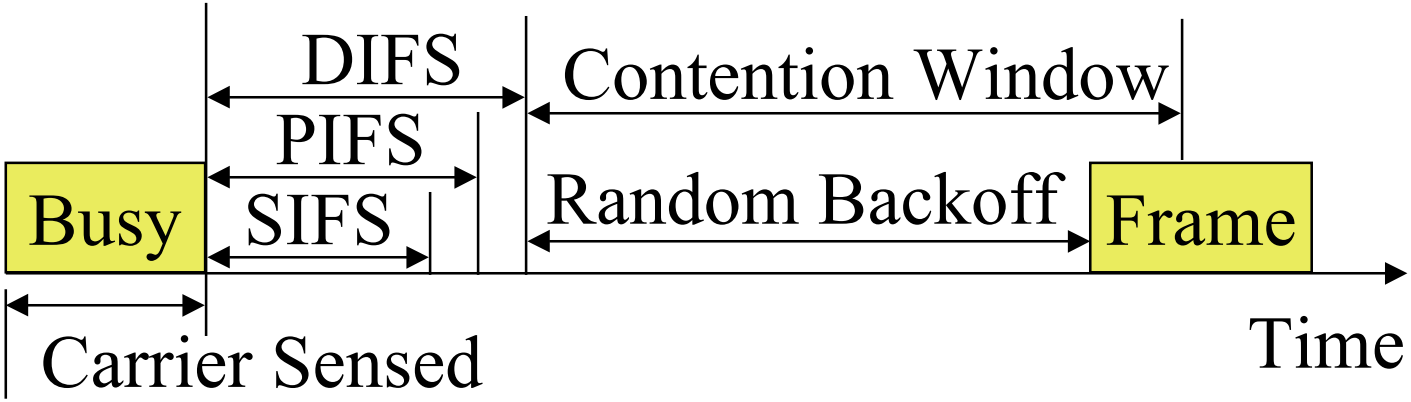
BSS Services (cont.)

- Security: one of the first concern in wireless.
- Protect the Access to network by using authentication mechanisms: needs to prove knowledge of the current key
- Avoid Capture of wireless traffic: Use WEP Encryption algorithm
- Power Saving: in wireless battery is a scarce resource.
- A station can be in one of three states:
  - Transmitter on
  - Receiver only on
  - Dozing: Both transmitter and receivers off, timer may be on.

BSS Services (cont.)

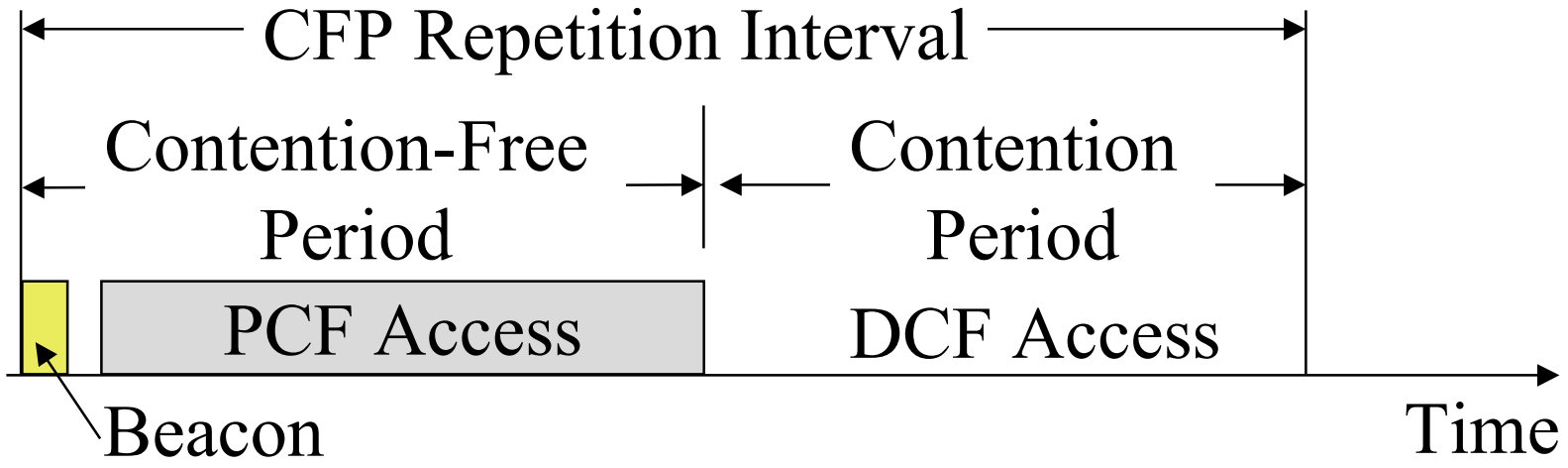
- Access point (AP) maintains record of stations working in Power Saving mode and buffers traffic for them until the stations ask by polling or change mode.
- AP announces which stations have frames buffered. Traffic Indication Map (TIM) included in each beacon. All multicasts/broadcasts are buffered.
- Dozing stations wake up to listen to the TIM in beacon. If there is data waiting for it, the station sends a poll frame to get the data.

IEEE 802.11 Priorities



- Initial interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (SIFS)
- Medium priority time-critical frames use “Point Coordination Function IFS” (PIFS)
- Asynchronous data frames use “Distributed coordination function IFS” (DIFS)

Time Critical Services

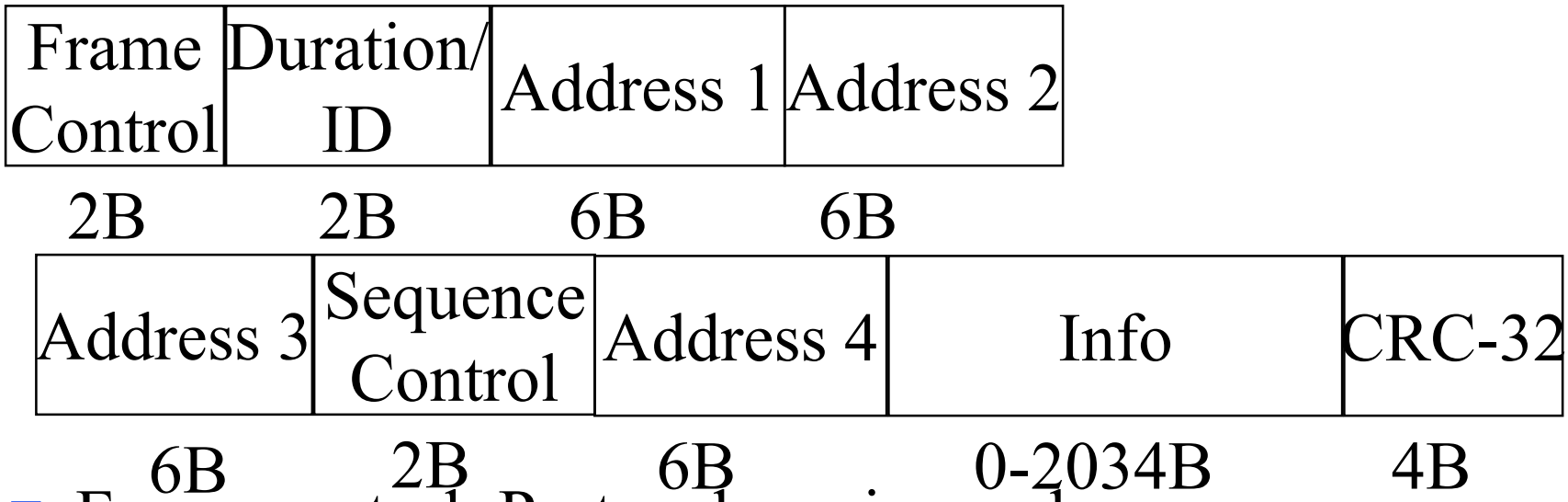


- Timer critical services use Point Coordination Function
- The point coordinator allows only one station to access
- Coordinator sends a beacon frame to all stations. Then uses a polling frame to allow a particular station to have contention-free access
- Contention Free Period (CFP) varies with the load.

Types of frames

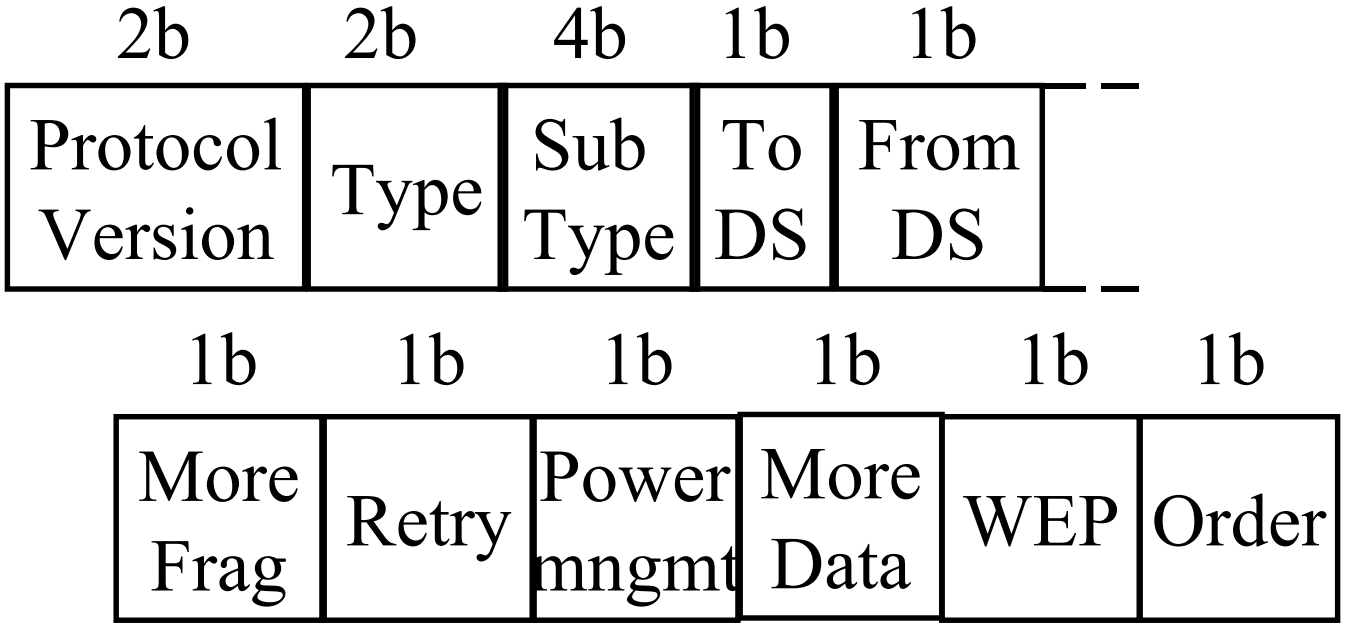
- Asynchronous Data
- Control
  - RTS, CTS, ACK
- Management
  - Beacon, Association Request, Association Response, Reassociation Request, Reassociation Response, etc

MAC Frame Format



- Frame control: Protocol version and frame type: management, data, control
- Duration in Power Save Poll: Network Allocation Vector (NAV) in other frames
- Address: Source, Destination, AP, Transmitting, Recv.
- Info: 0-2304 bytes long

Control Frame



- To DS, From DS: AP present, no as hoc
- Retry: this is retransmission
- WEP: encryption
- Using Strict-ordered service class

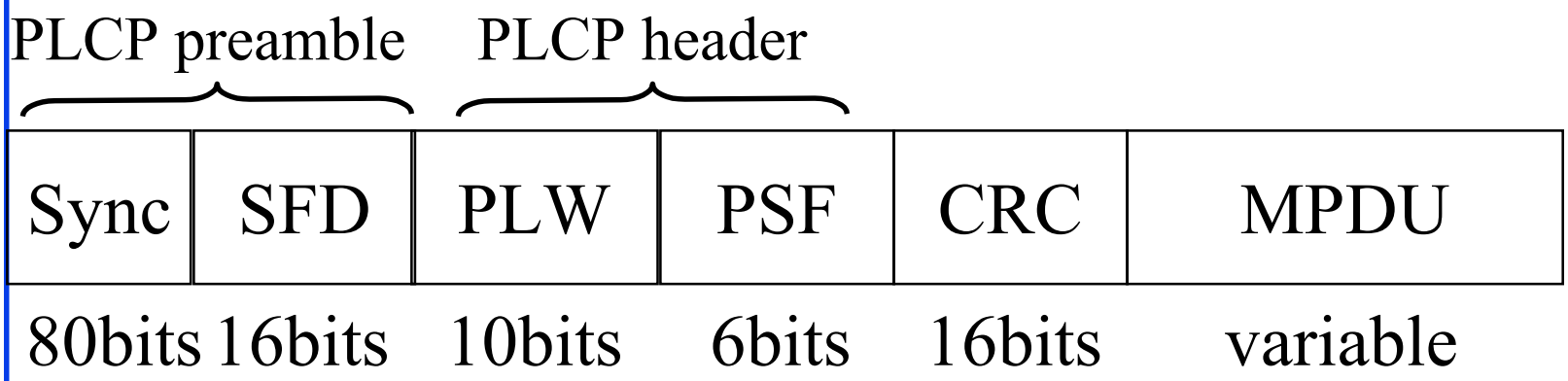
IEEE 802.11 Phy

- Three Phys specified:
  - Direct Seq. Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Diffused Infrared (DFIR): Wide angle
- DSSS and FHSS operate in 2.4-2.4835 GHz Industrial, Scientific, and Medical (ISM) band (International)
  Some early systems use 902-928 MHz band.
  Different PHY specifications for 915-MHz, 2.4-, 5.2 GHz, and Infrared (850-900 nm) bands.
- SS at 1 or 2 Mbps. DFIR at 1 Mbps.

FHSS Phy

- 2.4 GHz ISM Band.
- 1 and 2 Mbps
- 79 Frequencies in US and Europe, 23 in Japan
- Three sets of frequency hopping patterns. Each set has 22 hopping sequences (22 Channels).
  Total 66 channels. 12 in Japan.
- Consecutive frequencies in each sequence are at least 6 MHz apart to avoid a narrowband interferer.
- Modulation: 2GFSK for 1Mbps and 4GFSK for 2Mbps
- Adjacent or overlapping cells use different patterns.
- Many channels $\Rightarrow$ FH systems better than DS in dense (overlapping cells) environment.

FHSS PLCP Frame



Synch:Used by PHY circuitry
SFD: Start Frame Delimiter
PLW: PLCP Length Word, to detect the end of frame
PSF: PLCP Signaling Field including data rate
MPDU: MAC PDU

DSSS Phy

- 2.4 GHz band
- 1 and 2 Mbps
- 11 chip spreading factor
- 11 DS center frequencies (11 Channels)
- Differential Binary Phase Shift Keying (DBPSK) for 1Mbps, Differential Quadrature Phase Shift Keying (DQPSK) for 2Mbps
- 6 overlapping channels provide 3 pairs of non-overlaping channels.
- 10 mW to 100 mW transmitted power

DSSS PLCP Frame

PLCP preamble

Sync	SFD	DR	SER-VICE	Length	CRC	MPDU
128bits	16bits	8bits	8bits	16bits	16bits	variable

SFD: Start Frame Delimiter
DR: Data Rate
SERVICE: Future use
MPDU: MAC PDU

IEEE 802.11 b

- Higher-Speed Physical Layer Extension in the 2.4GHz Band
- Use High Rate Direct Sequence Spread Spectrum (HR/DSSS)
- HR/DSSS uses the same PLCP preambe and header as DSSS, so both PHYs can co-exist in the same BSS
- Multirate: 1, 2, plus 5.5 and 11 Mbps, rate switching mechanism
- Use Complementary Code Keying (CCK) modulation with 8 chip for high rates.

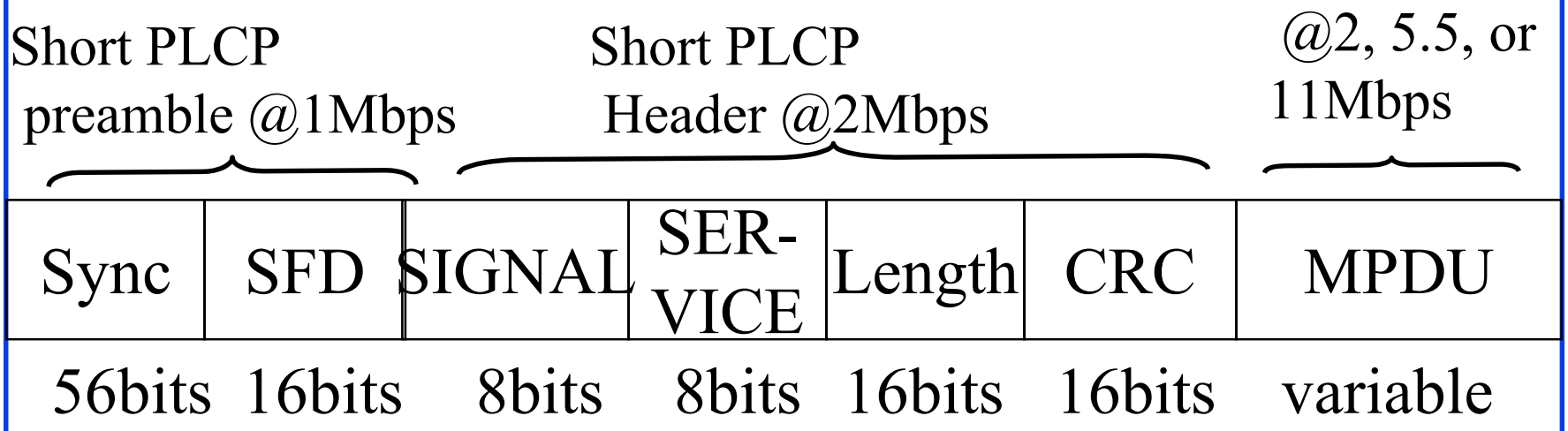
IEEE 802.11 b (cont.)

- An optional modulation scheme: packet binary convolution coding: HR/DSSS/PBCC
- Option to use a shorter PLCP preamble to increase the data rate: HR/DSSS/short, HR/DSSS/PBCC/short
  - Can co-exist with not short on different channels or with appropriate CAC mechanisms
- Optional Channel Agility: permit interpretability with both FH and DS modulations

Multirate

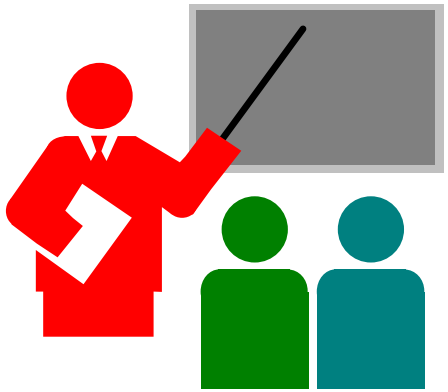
- Multirate:
  - All control frames will be transmitted at one rate so all stations can understand

Short PLCP Frame



SFD: Start Frame Delimiter
SIGNAL: Data Rate
MPDU: MAC PDU

Summary



- Wireless WANs or LANs
- IEEE 802.11
- Short Overview of IEEE 802.11b

Literature

- For a detailed list of references see: http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm
- [DAYEM97] "Mobile Data & Wireless LAN Technologies", Rifaat A. Dayem, Prentice Hall 1997
- IEEE Std 802.11-1999
- IEEE Std 802.11b-1999

Wireless: Key References

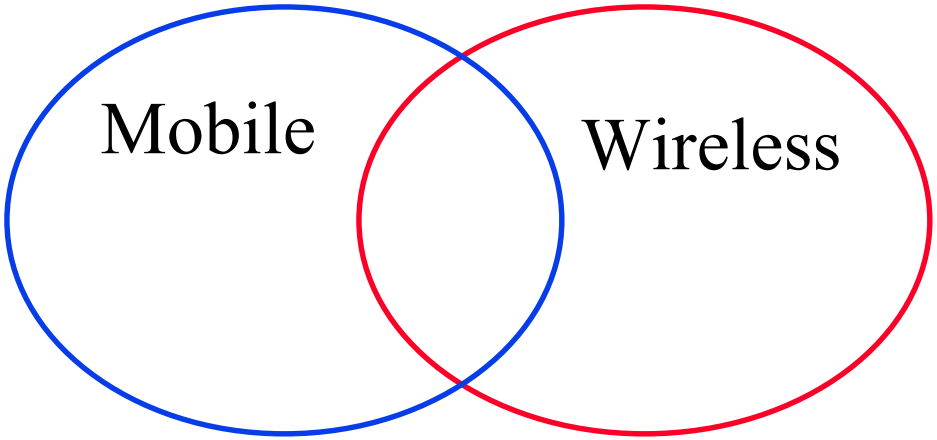
- For a detailed list of references see: http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm
- "Wireless Local Area Networks," Aug 97, http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans/index.htm
- "In-building wireless LANs," http://www.cis.ohio-state.edu/~jain/cis788-99/wireless_lans/index.html

Thank You!

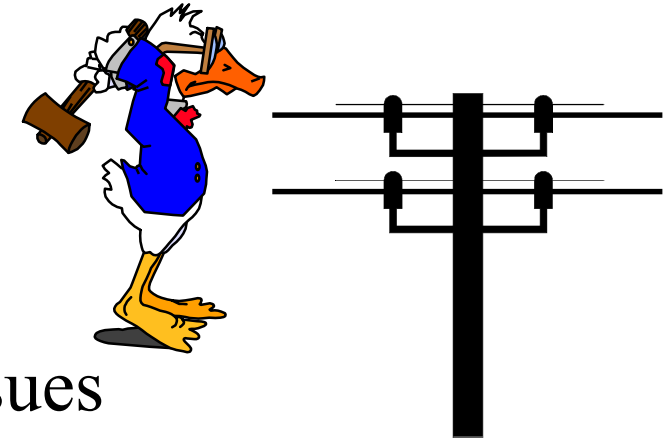
Wireless: Key References

- For a detailed list of references see: http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm
- E. Prem, "Wireless Local Area Networks," Aug 97, http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans
- X. Cong, "Wireless ATM - An Overview," Aug 97, http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_atm
- Baseline Text for Wireless ATM specifications, ATM Forum/btd-watm-01.06.txt, February 1998.

Mobile vs Wireless

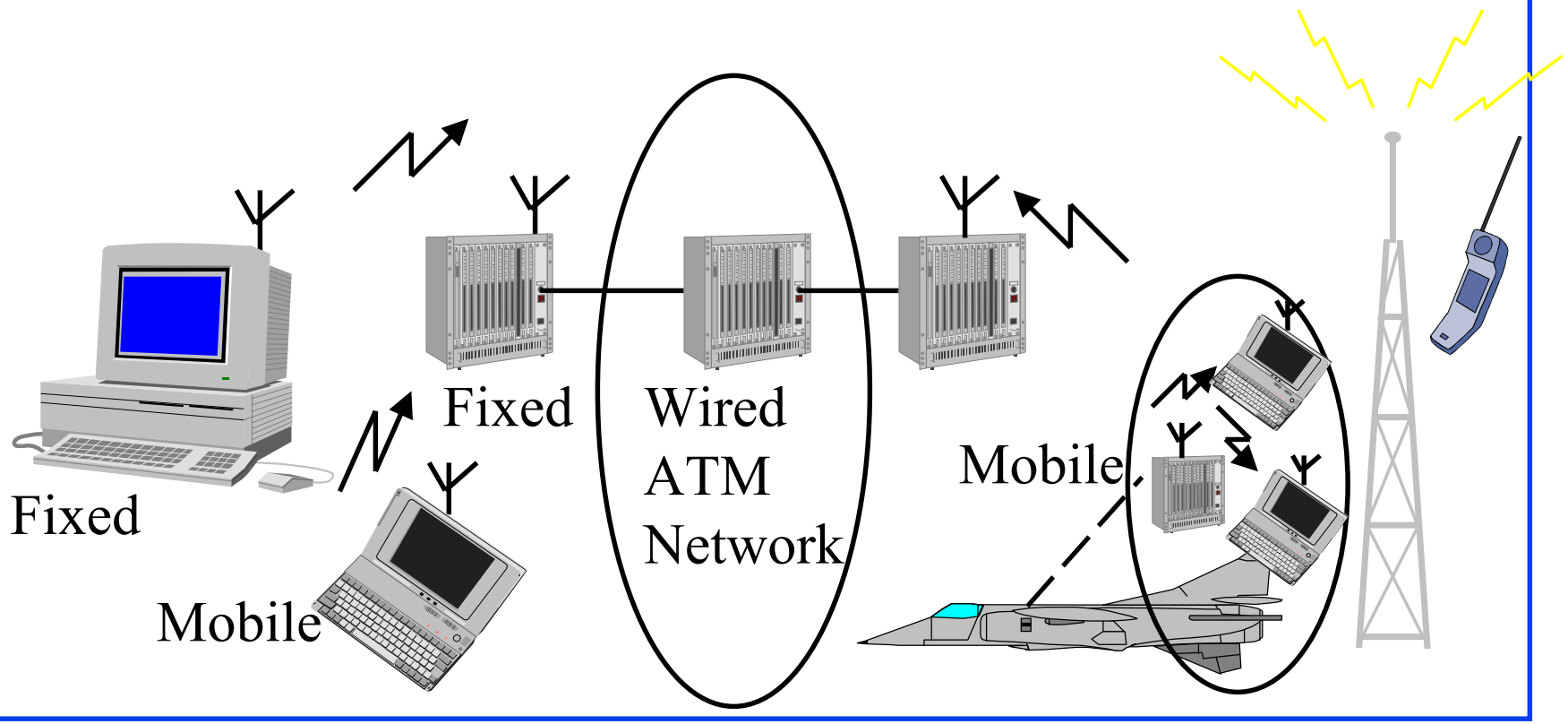


- Mobile vs Stationary
- Wireless vs Wired
- Wireless ⇒ media sharing issues
- Mobile ⇒ routing, addressing issues

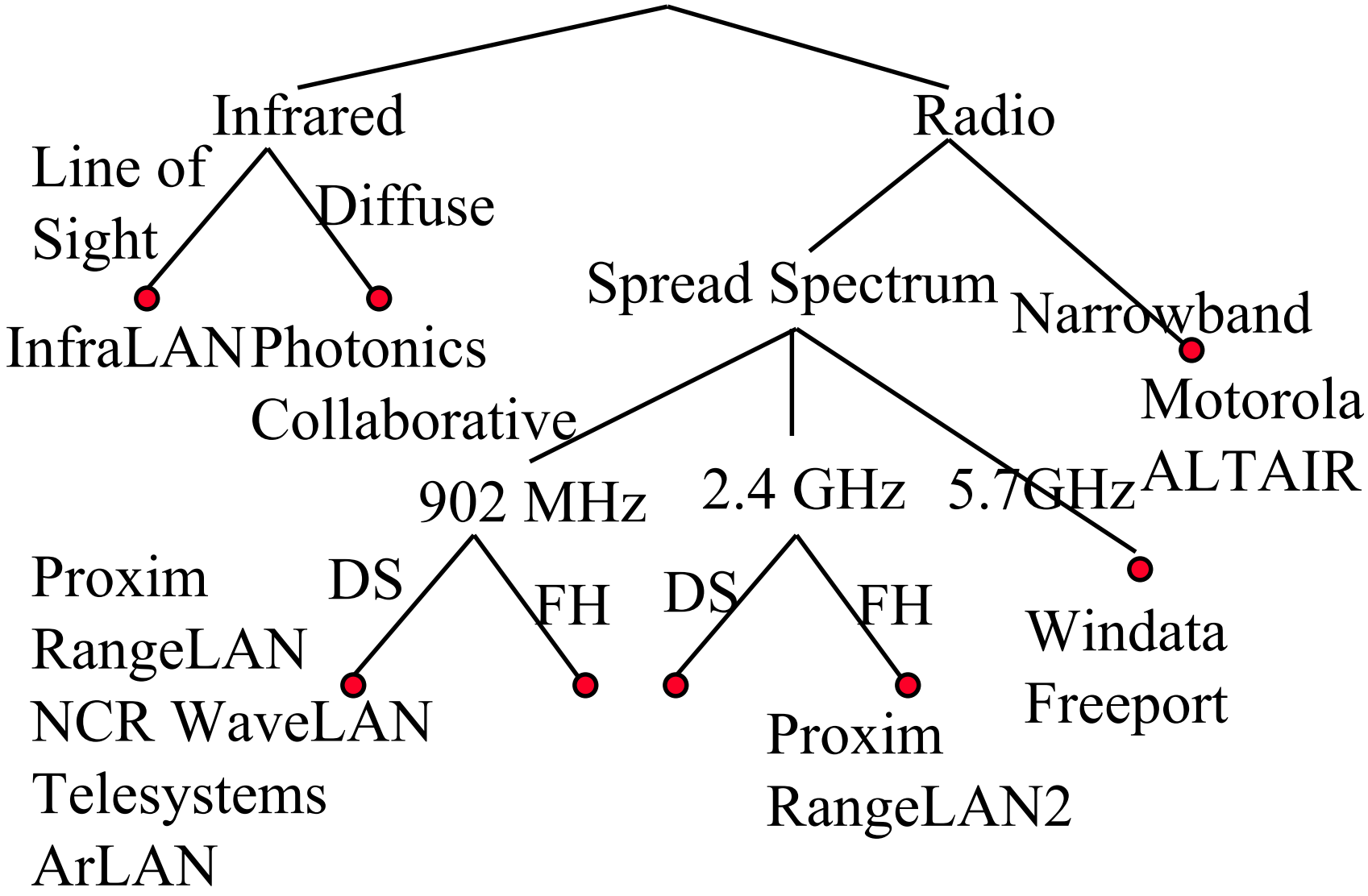


Reference Configurations

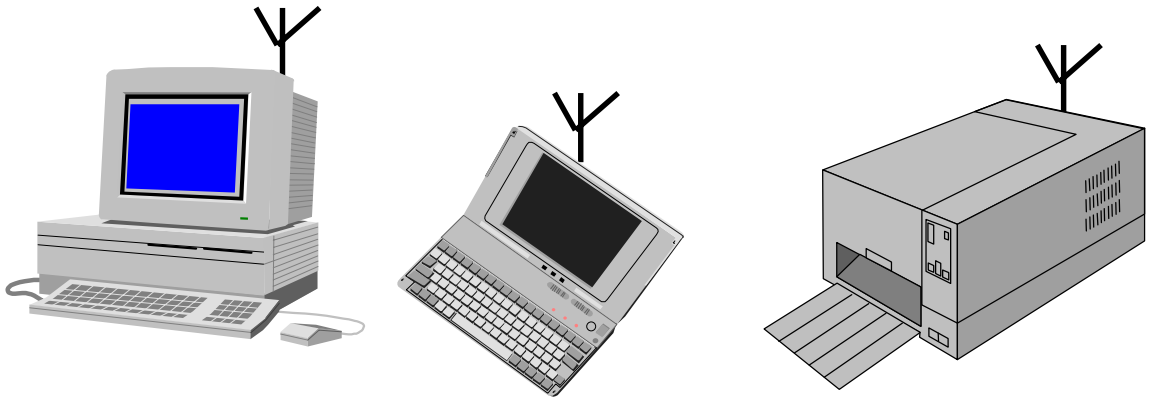
1. Fixed Wireless Access
2. Mobile End-Users,
3. Mobile Networks
4. Ad Hoc Networks
5. PCS Access
6. PCS Interworking



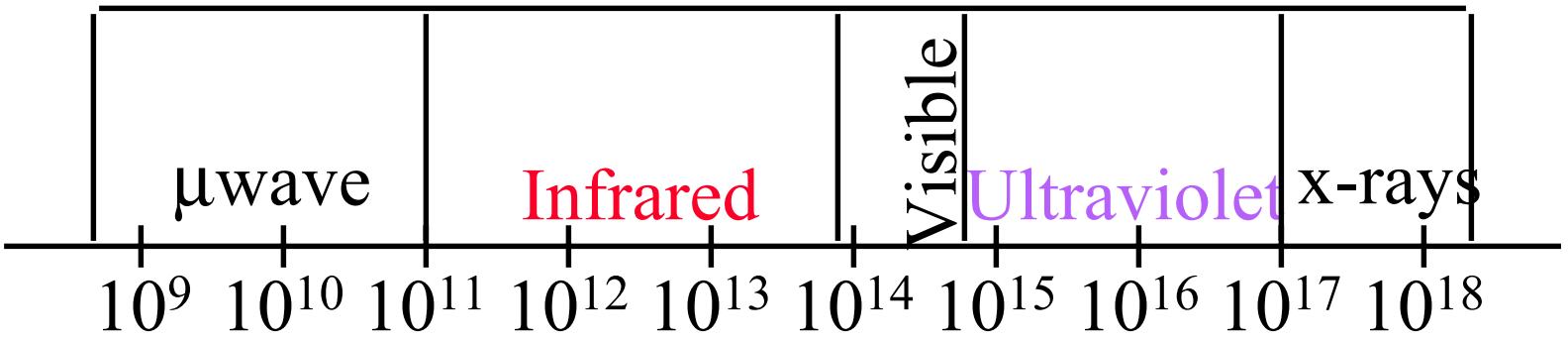
Wireless LANs



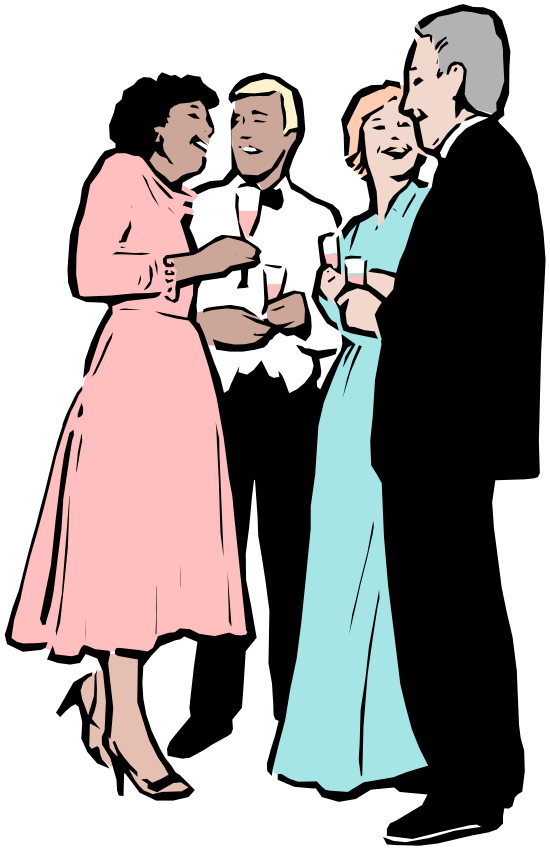
Wireless LANs



- IR ⇒ Line of sight, short range, indoors
- RF ⇒ Need license
- Spread-Spectrum: Resistance to interference



Ad-Hoc vs Infrastructure



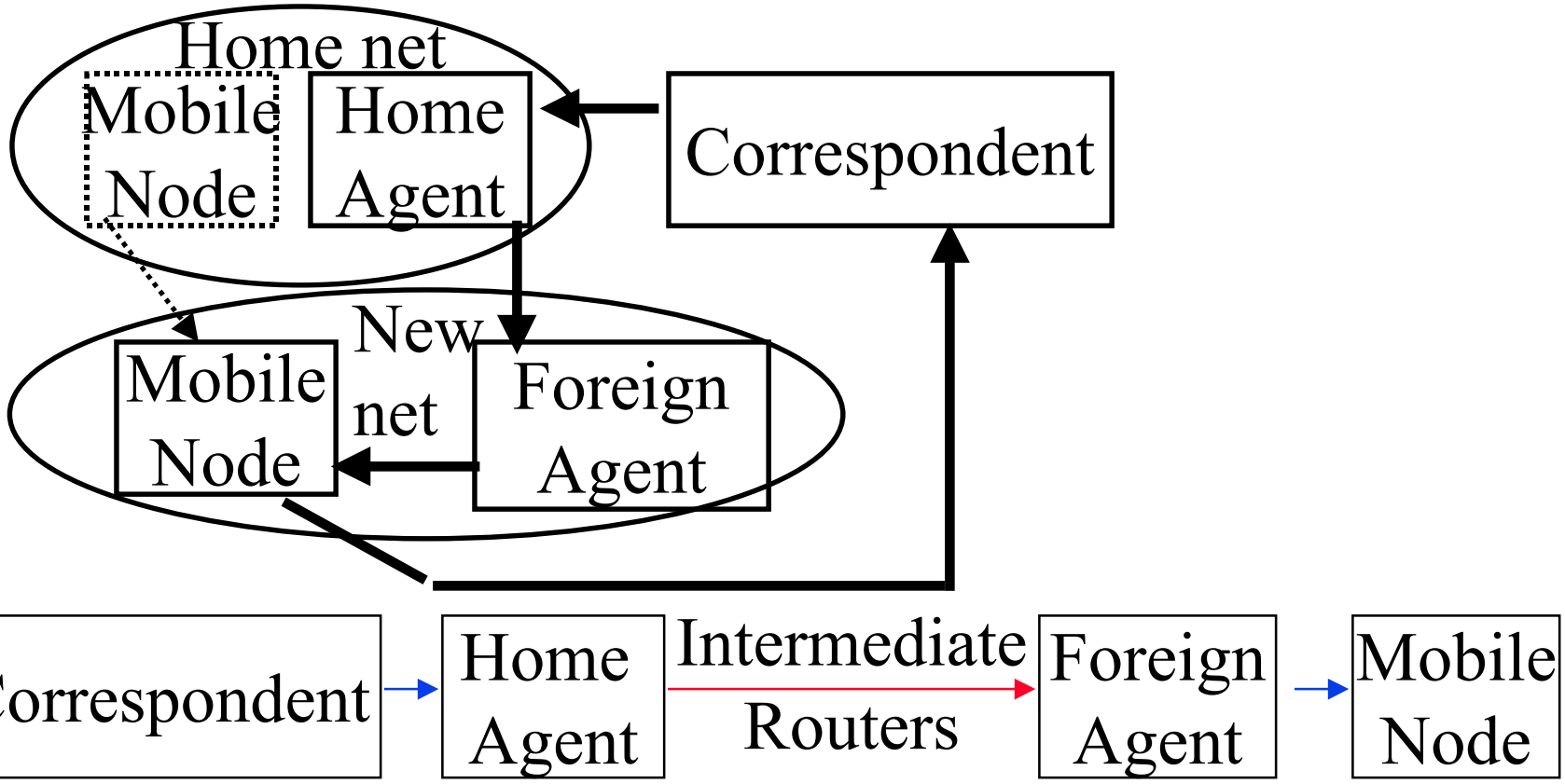
Status and Future

- 802.11 including both MAC and PHY approved June 1997.
- More bandwidth in future by:
  1. Better encoding: Multilevel modulation $\Rightarrow$ 8 Mbps
  2. Fewer channels with more bandwidth $\Rightarrow$ 4 MHz channels. Or Entire ISM band for one channel.
  3. Find another band. May get 150 MHz band in 5-GHz band. Fifteen 10-MHz channels with 15-20 Mb/s.

Mobile IP: Features

- You can take you notebook to any location
- Finds nearby IP routers and connects *automatically.* You don't even have to find a phone jack.
- Only "Mobility Aware" routers and mobile units need new s/w. Other routers and hosts can use current IP
- No new IP addresses or address formats
- Secure: Allows authentication
- Also supports mobile networks (whole airplane/car load of mobile units)

Mobile IP: Mechanisms



Mechanism (Cont)

- Mobile node finds foreign agents via solicitation or advertising
- Mobile registers with the foreign agents and informs the home agent
- Home agent intercepts mobile node's datagrams and forwards them to the care-of-address
- Care-of-address (COA): Address of the end-of-tunnel towards the mobile node. May or may not be foreign agent
- At COA, datagram is extracted and sent to mobile