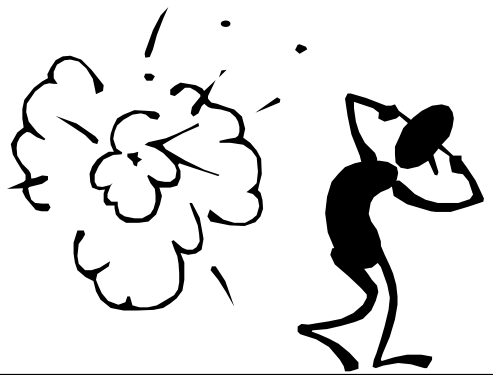
IEEE802.11 Wireless LAN

The broadband wireless Internet

Maximilian Riegel

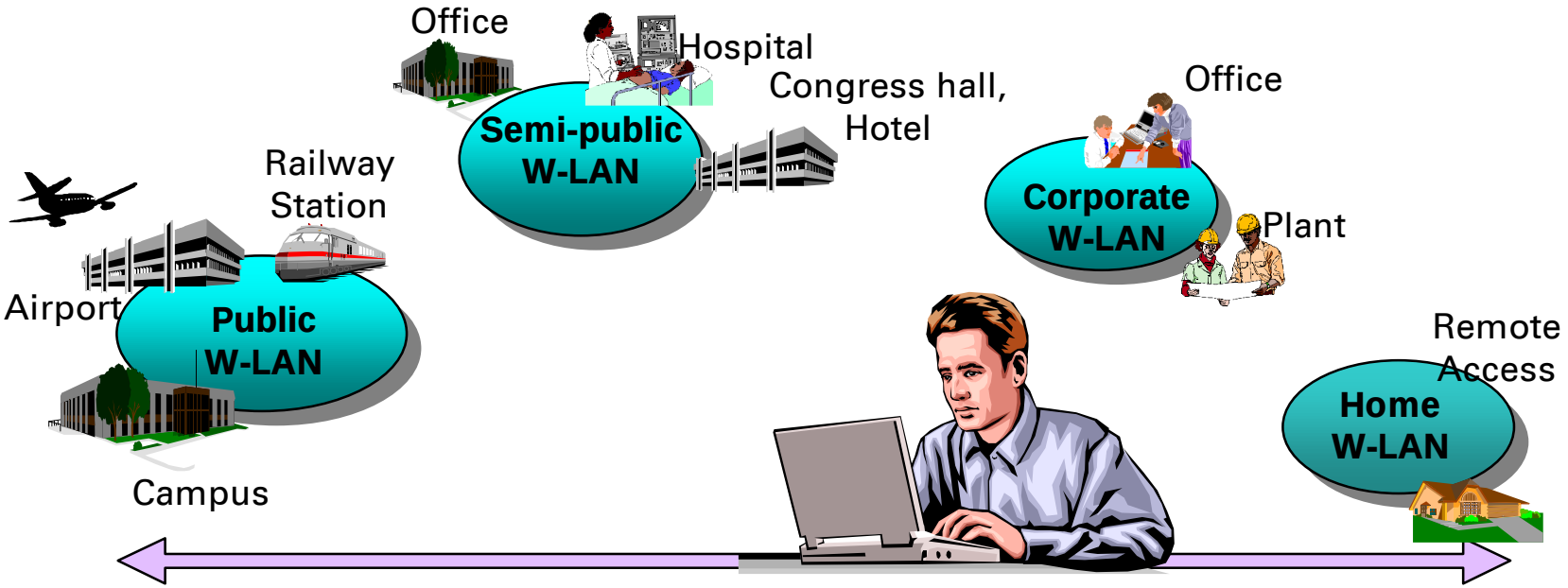
WLAN Dream Finally Seems to Happen...

- Recently lots of serious WLAN activities have been announced
  - Big players have invested in WLAN (Cisco, Intel, Nokia)
  - Integrated WLAN solutions appearing (Apple, IBM, Dell, ...)
- Wireless IP solutions have lots of momentum!
  - People desire wireless IP terminals and access devices
- WLAN offers a good mobile solution for indoor IP access
  - Added value for the user - Flexibility, user mobility
  - Added value for ISP - solution for public high speed IP access
- WLAN standards are converging - IEEE 802.11b rules
  - Interoperability has been the main obstacle

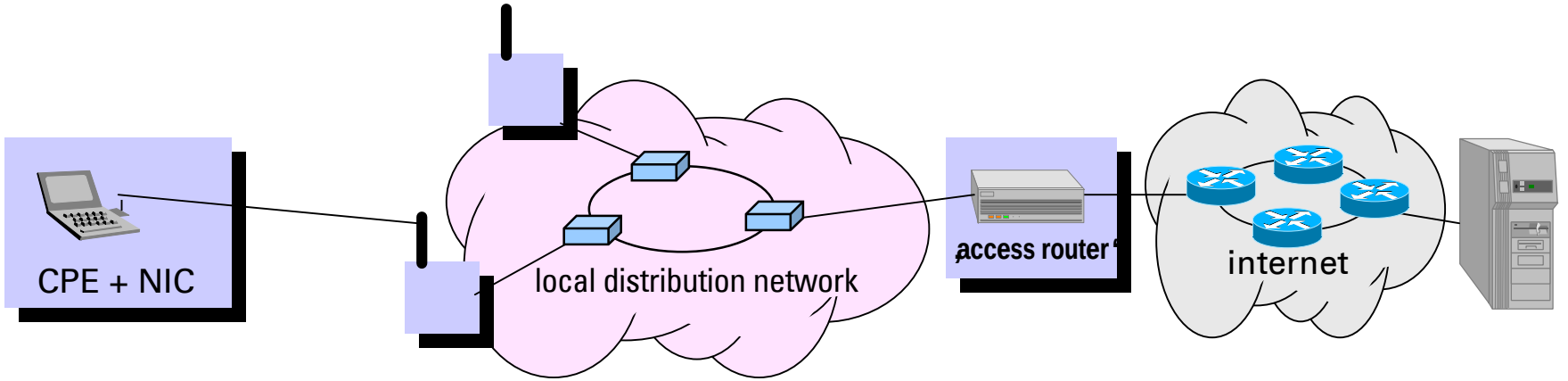


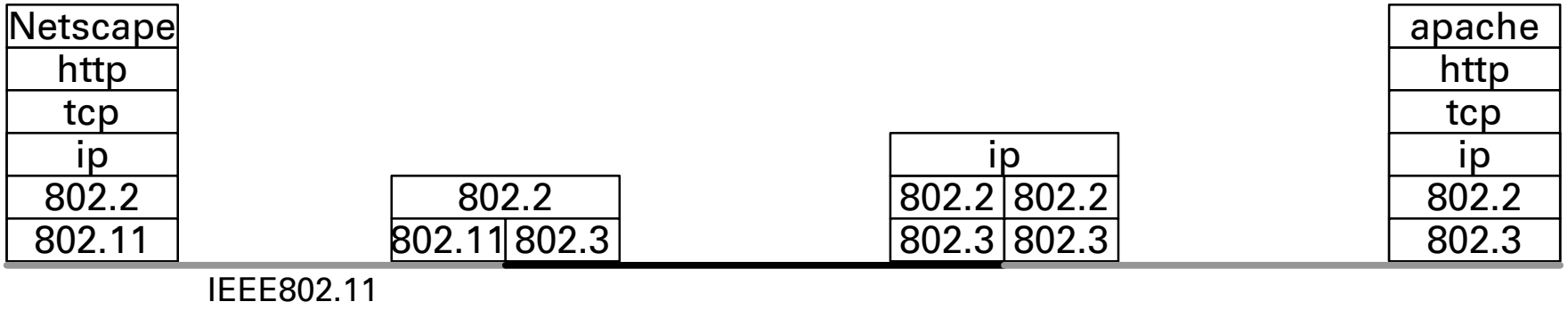
The Wireless LAN market has taken off...

- In the past:
  Deployment of WLAN for vertical markets - *moderate growth*
- Now:
  Ubiquitous broadband wireless Internet access - *the killer app*
  - ⇨ IEEE802.11b 11 Mbps Wireless LAN everywhere



Wireless LAN IEEE802.11 Basic Architecture

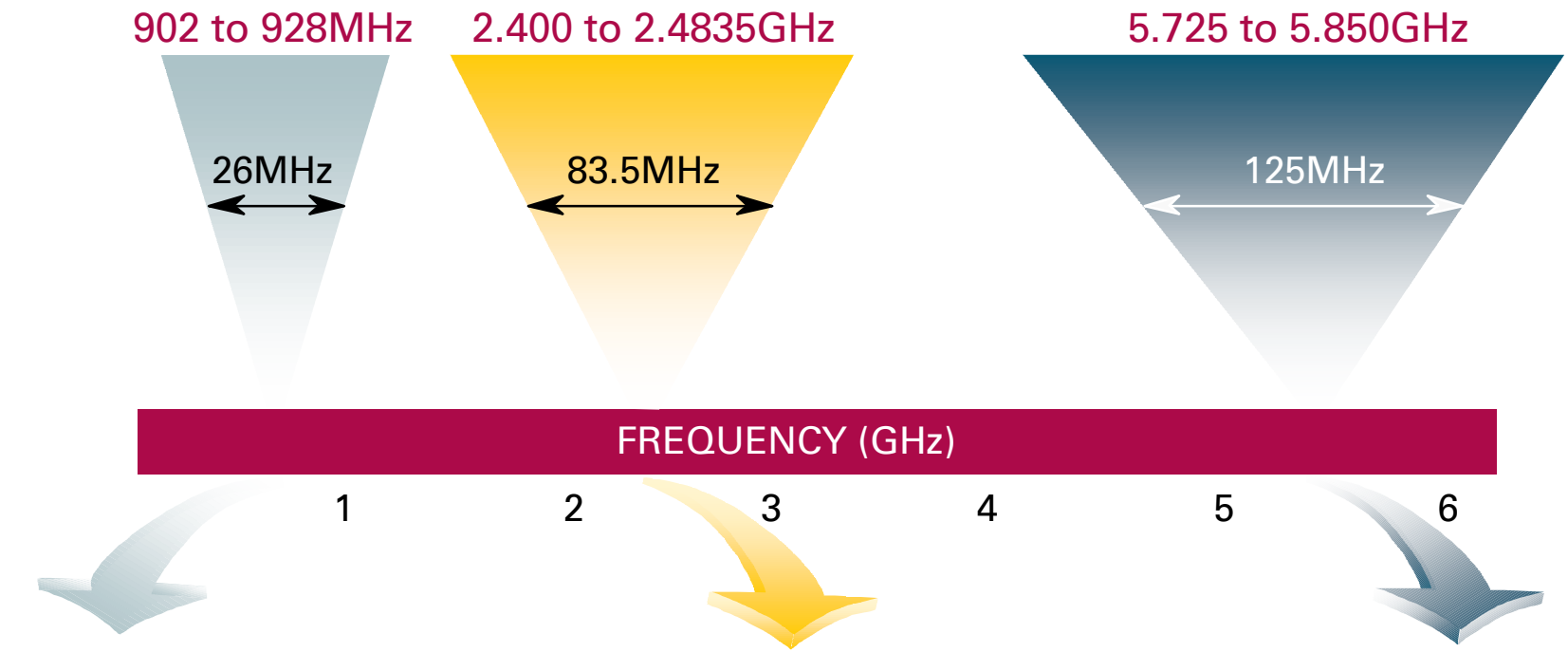




What is unique about wireless?

- Difficult media
  - interference and noise
  - quality varies over space and time
  - shared with “unwanted” 802.11 devices
  - shared with non-802 devices (unlicensed spectrum, microwave ovens)
- Full connectivity cannot be assumed
  - “hidden node” problem
- Mobility
  - variation in link reliability
  - battery usage: requires power management
  - want “seamless” connections
- Security
  - no physical boundaries
  - overlapping LANs
- Multiple international regulatory requirements

Industrial, Scientific and Medical (ISM) Bands



- Low bandwidth
- Polluted by cellular and cordless

- Relatively clean spectrum
- DS radios good at rejecting microwave interference
- Can fit several (11) WLAN Channels

- A band for the future
- No cost effective technology yet

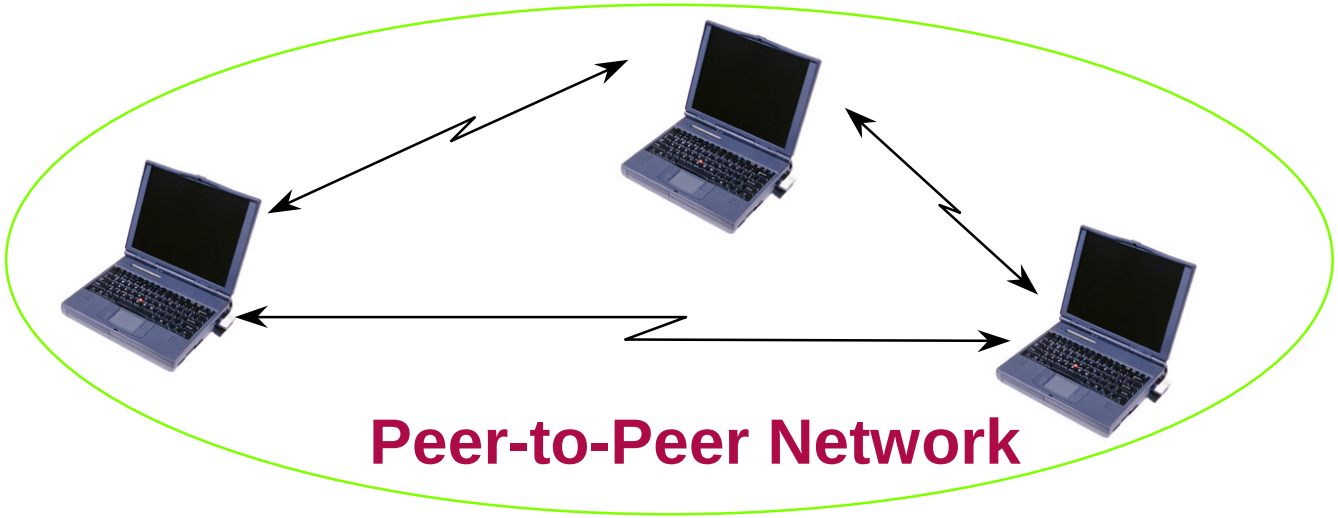
Wireless IEEE802.11 Standard

802.11 Standard supports 3 Physical Layers

- Frequency hopping
  - Limited to 2Mbps data rate
  - Requires more network overhead
  - Has higher power density that can generate interference
- Direct sequence
  - Only PHY to support the 11Mbps data rate
  - Low power density to minimize interference
- Infrared
  - Range limited

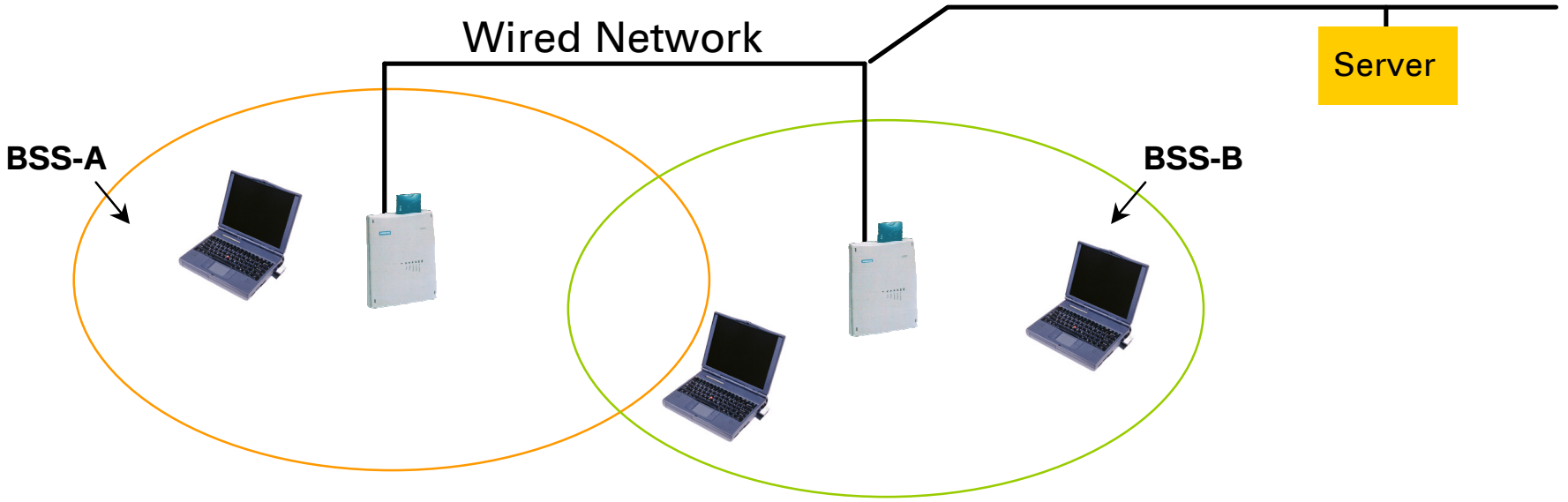
Approved June 1997
802.11b approved September 1999

IEEE802.11 Ad Hoc Mode



- Independent networking
  - Use Distributed Coordination Function (DCF)
  - Forms a Basic Service Set (BSS)
  - Direct communication between stations
  - Coverage area limited by the range of individual stations

IEEE802.11 Infrastructure Mode



- Access Points (AP) and stations (STA)
- BSS (Basic Service Set): a set of stations controlled by a single coordination function
- Distribution system interconnects multiple cells via access points to form a single network
- Extends wireless coverage area and enables roaming

IEEE 802.11 Network elements

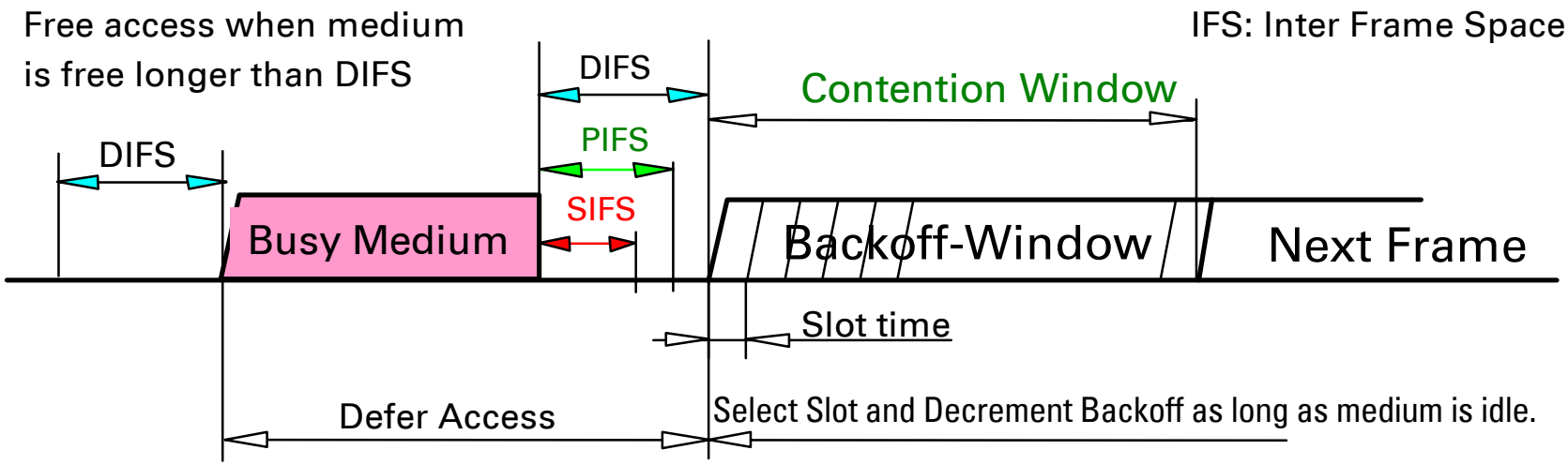
- Distribution system
  - Used to interconnect wireless cells
    - *multiple BSS connected together form an ESS, Extended Service Set*
    - *Allows mobile stations to access fixed resources*
  - Not part of 802.11 standard
    - *could be bridged IEEE LANs, wireless, other networks …*
    - *Distribution System Services are defined*

- Access Points
  - Stations select an AP and “associate” with it
  - Support roaming
  - Provide other functions
    - *time synchronization (beaconing)*
    - *power management support*
    - *point coordination function*
  - Traffic typically (but not always) flows through AP
    - *direct communication possible*

MAC Functionality

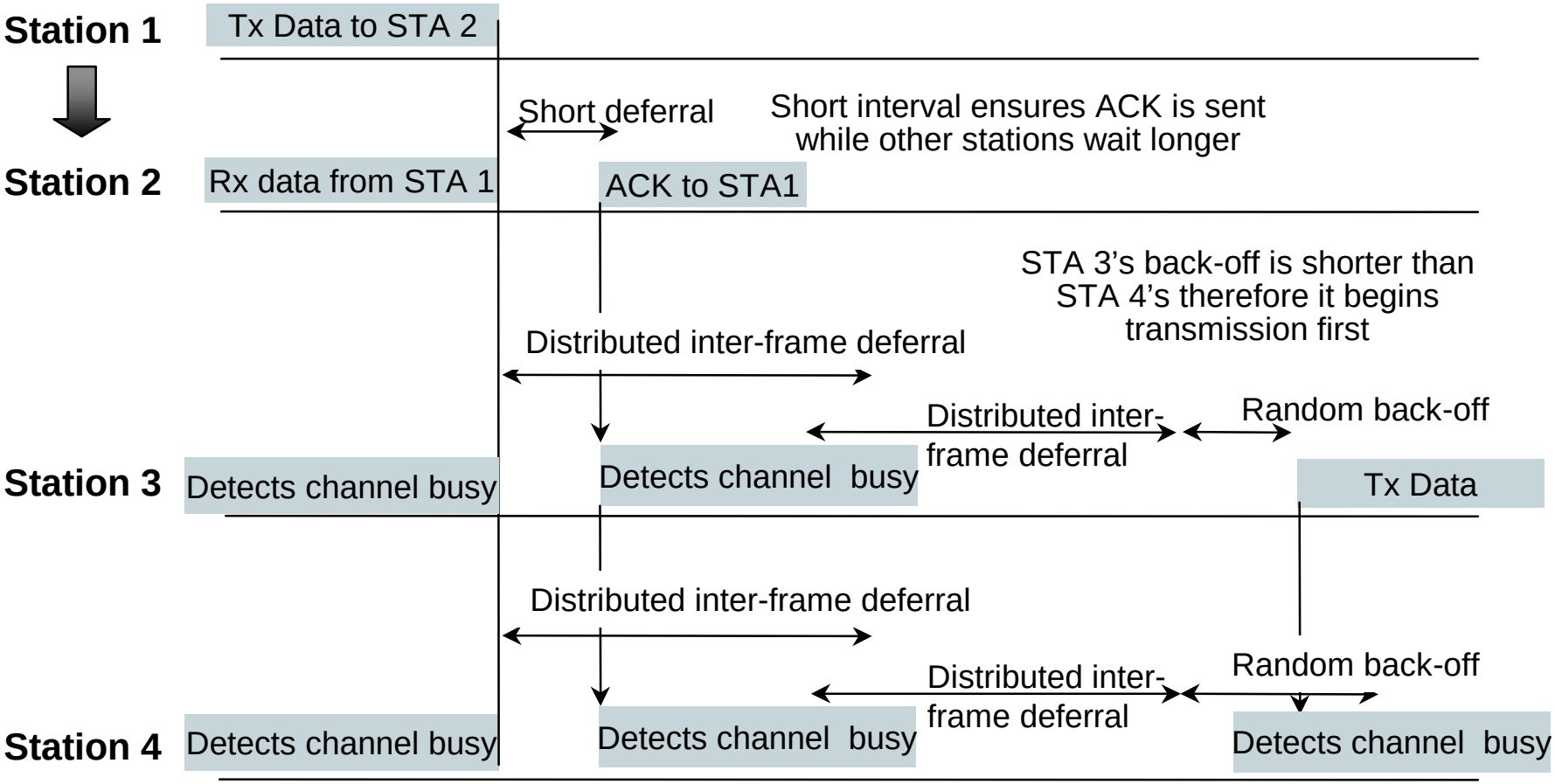
- Independent and Infrastructure configuration support
  - Each BSS has a unique 48 bit address
  - Each ESS has a variable length address
- CSMA with collision avoidance
  - MAC-level acknowledgment
  - allows for RTS/CTS exchanges (hidden node protection)
  - MSDU fragmentation
  - “Point Coordination” option (AP polling)
- Association and Reassociation
  - station scans for APs, association handshakes
  - Roaming support within an ESS
- Power management support
  - stations may power themselves down
  - AP buffering, distributed approach for IBSS
- Authentication and privacy
  - Optional support of “Wired Equivalent Privacy” (WEP)
  - Authentication handshakes defined

CSMA/CA Explained

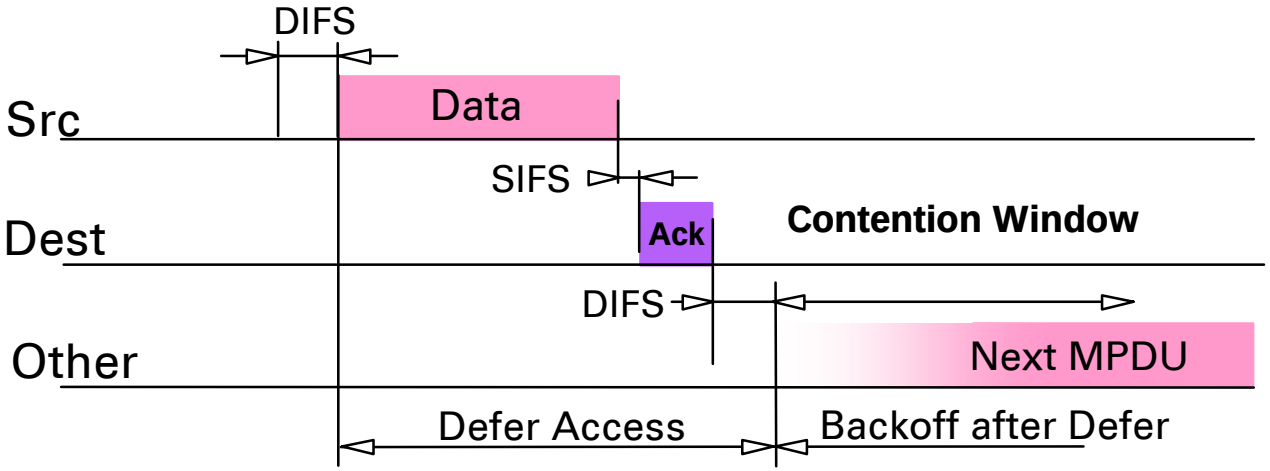


- Reduce collision probability where mostly needed.
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- Efficient Backoff algorithm stable at high loads.
  - Exponential Backoff window increases for retransmissions.
  - Backoff timer elapses only when medium is idle.
- Implement different fixed priority levels

Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)

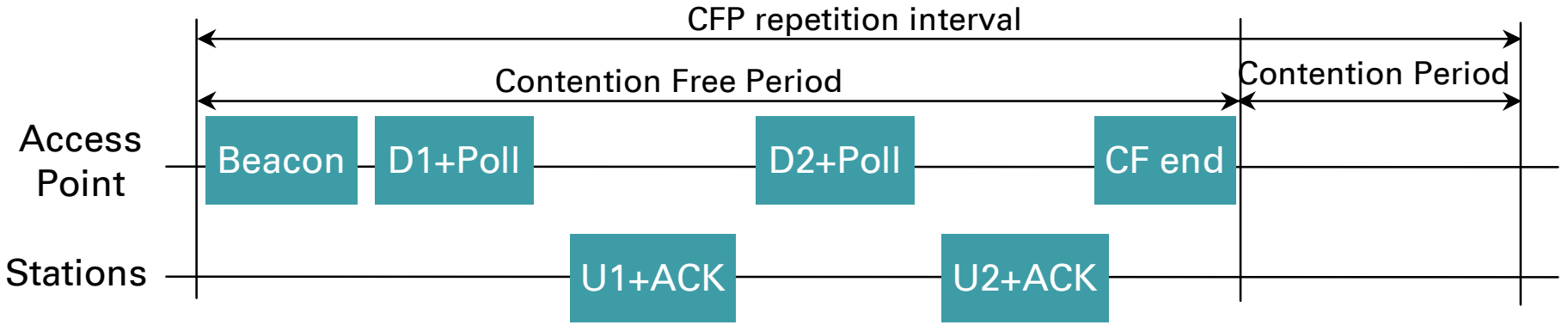


CSMA/CA + ACK protocol



- Defer access based on Carrier Sense.
  - CCA from PHY and Virtual Carrier Sense state.
- Direct access when medium is sensed free longer then DIFS, otherwise defer and backoff.
- Receiver of directed frames to return an ACK immediately when CRC correct.
  - When no ACK received then retransmit frame after a random backoff (up to maximum limit).

IEEE802.11 Point Coordination Function (PCF)

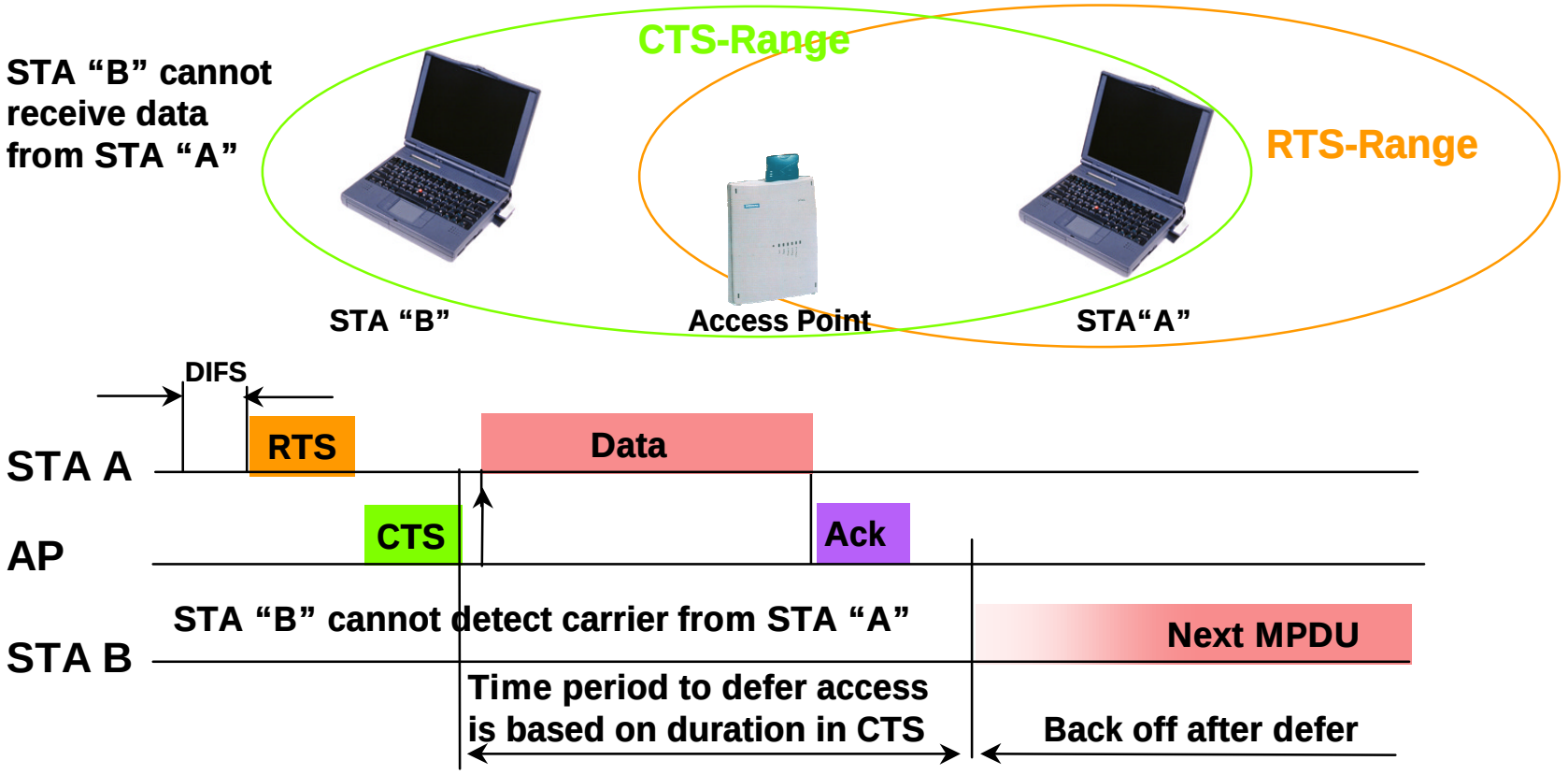


- Optional PCF mode provides alternating contention free and contention operation under the control of the access point
- The access point polls stations for data during contention free period
- Network Allocation Vector (NAV) defers the contention traffic until reset by the last PCF transfer
- PCF and DCF networks will defer to each other
- PCF improves the quality of service for time bounded data

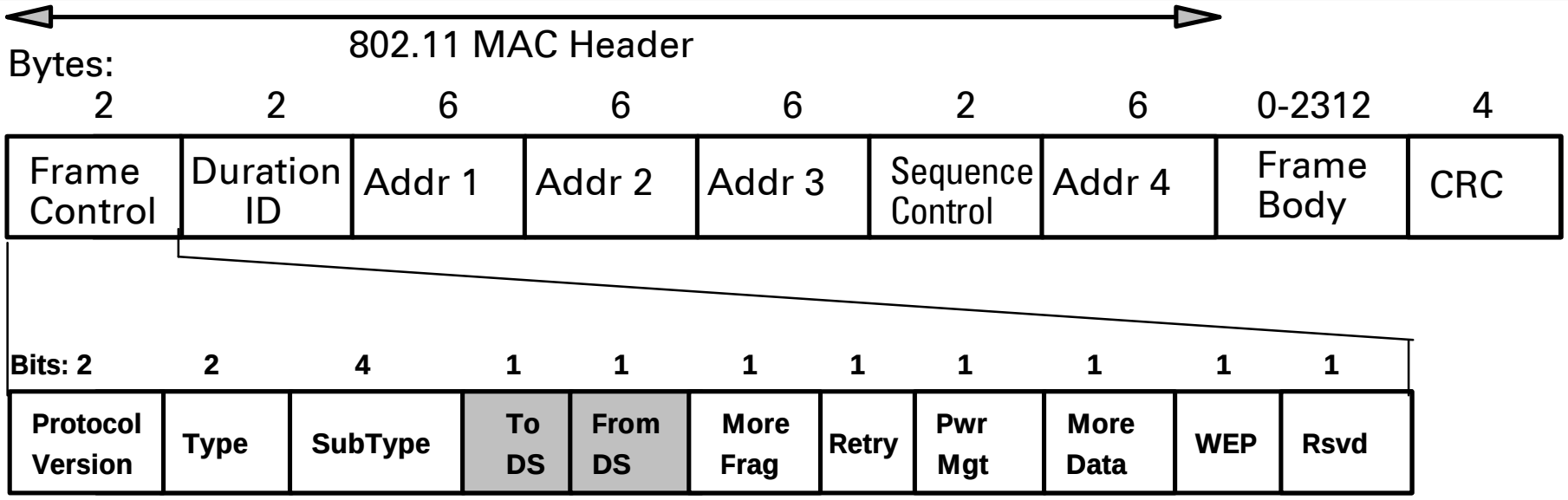
“Hidden Node” Provisions

Problem – Stations contending for the medium do not *Hear* each other

Solution – Optional use of the *Duration* field in RTS and CTS frames with AP

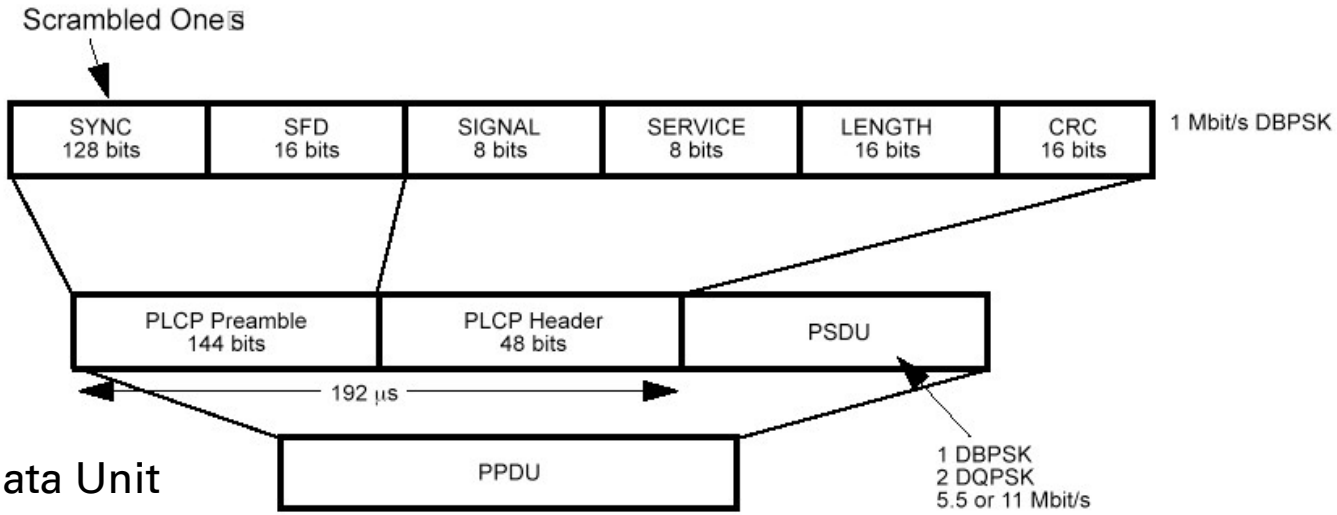


Frame Formats



- MAC Header format differs per Type:
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames
- Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.

Physical Layer Convergence Protocol (PLCP)



PLCP Protocol Data Unit

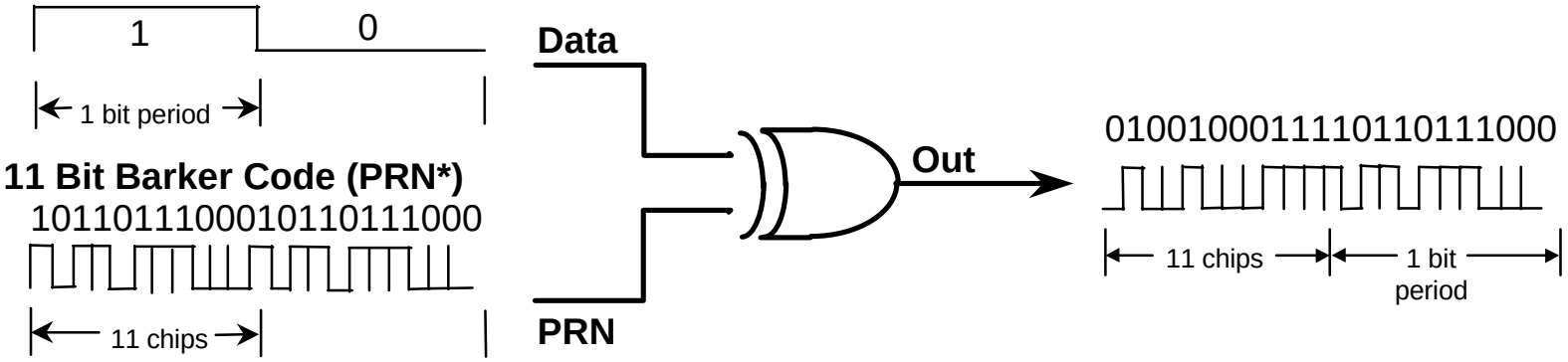
- SYNC (gain setting, energy detection, antenna selection, frequency offset compensation)
- SFD (Start Frame Delimiter; bit synchronization)
- SIGNAL (rate indication; 1, 2, 5.5, 11 Mbit/s)
- SERVICE (reserved for future use)
- LENGTH (number of octets in PSDU)
- CRC (CCITT CRC-16, protects signal, service, length field)

Three PHYs

- Frequency Hop Spread Spectrum
  - 2.4GHz band, 1 and optional 2Mbps
    - *2GFSK, 4GFSK (Gaussian Frequency Shift Keying)*
  - 2.5 hops/sec over 79 1MHz BW channels (North America)
- Direct Sequence Spread Spectrum
  - 2.4GHz band, 1 and 2Mbps
    - *DBPSK, DQPSK (Differential Binary/Quadrature Phase Shift Keying)*
    - *11 chip Barker sequence*
  - 2.4GHZ band, 5.5 and 11Mbps
    - *CCK*
    - *Complex spread functions*
- Baseband IR
  - Diffused infrared, 1 and 2Mbps, 16-PPM and 4-PPM (Pulse Position Modulation)

Direct Sequence Spread Spectrum

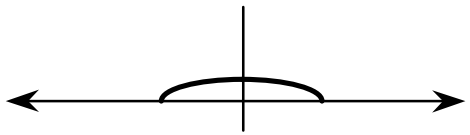
RF Energy is Spread by XOR of Data with PRN Sequence



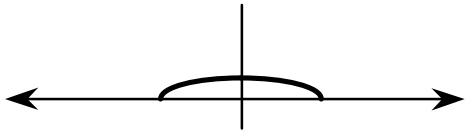
*** PRN: Pseudorandom Number**

Signal Spectrum

Transmitter baseband signal before spreading



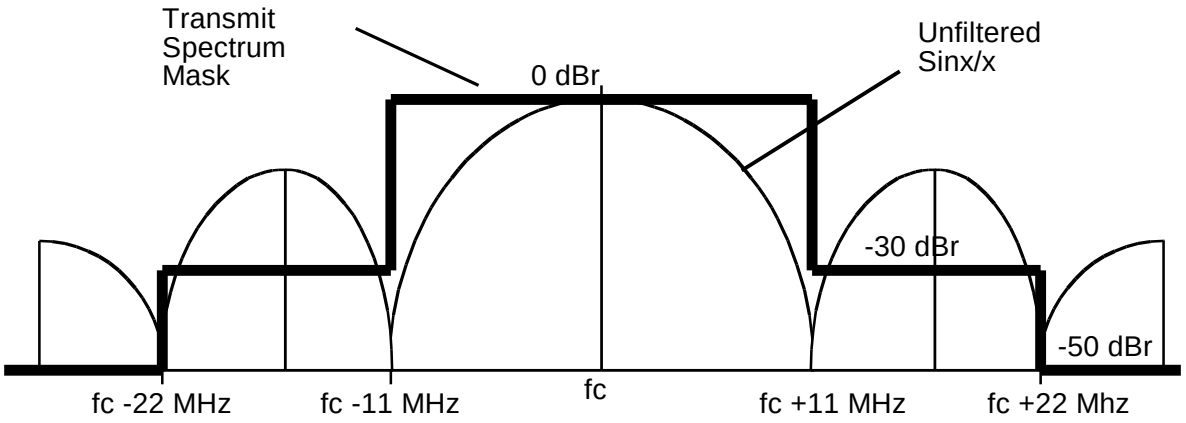
Transmitter baseband signal after spreading



Receiver baseband signal before matched filter (Correlator)

Receiver baseband signal after matched filter (De-spread)

DSSS Transmit Spectrum and Channels



Cannel	USA	ETSI	Japan
1	2412 MHz	2412 MHz	N/A
2	2417 MHz	2417 MHz	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	2467 MHz	N/A
13	N/A	2472 MHz	N/A
14	N/A	N/A	2484 MHz

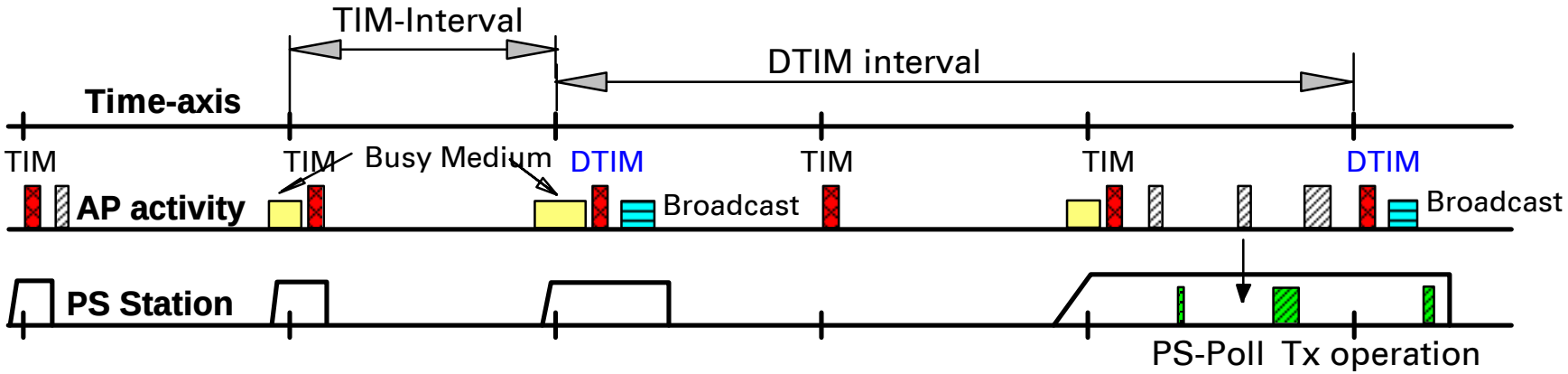
Power Management

- Mobile devices are battery powered.
  - Power Management is important for mobility.
- Current LAN protocols assume stations are always ready to receive.
  - Idle receive state dominates LAN adapter power consumption over time.
- How can we power off during idle periods, yet maintain an active session?
- 802.11 Power Management Protocol:
  - allows transceiver to be off as much as possible
  - is transparent to existing protocols
  - is flexible to support different applications
    - *possible to trade off throughput for battery life*

Power Management Approach

- Allow idle stations to go to sleep
  - station's power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF assures AP and Power Save stations are synchronized
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- Independent BSS also have Power Management
  - similar in concept, distributed approach

Infrastructure Power Management

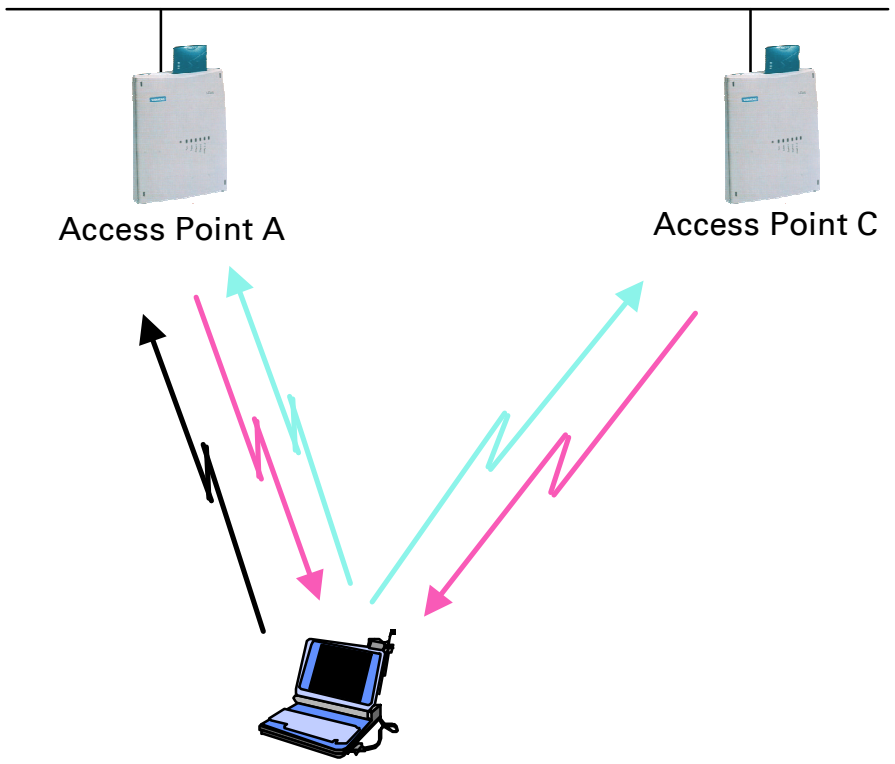


- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after Delivery Traffic Indication Message (DTIM)
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected DTIM.
- If TIM indicates frame buffered
  - station sends PS-Poll and stays awake to receive data
  - else station sleeps again

Scanning

- Scanning required for many functions.
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- 802.11 MAC uses a common mechanism for all PHY.
  - single or multi channel
  - passive or active scanning
- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel
    - *Send a Probe, Wait for a Probe Response*
- Beacon or Probe Response contains information necessary to join new network.

Active Scanning Example

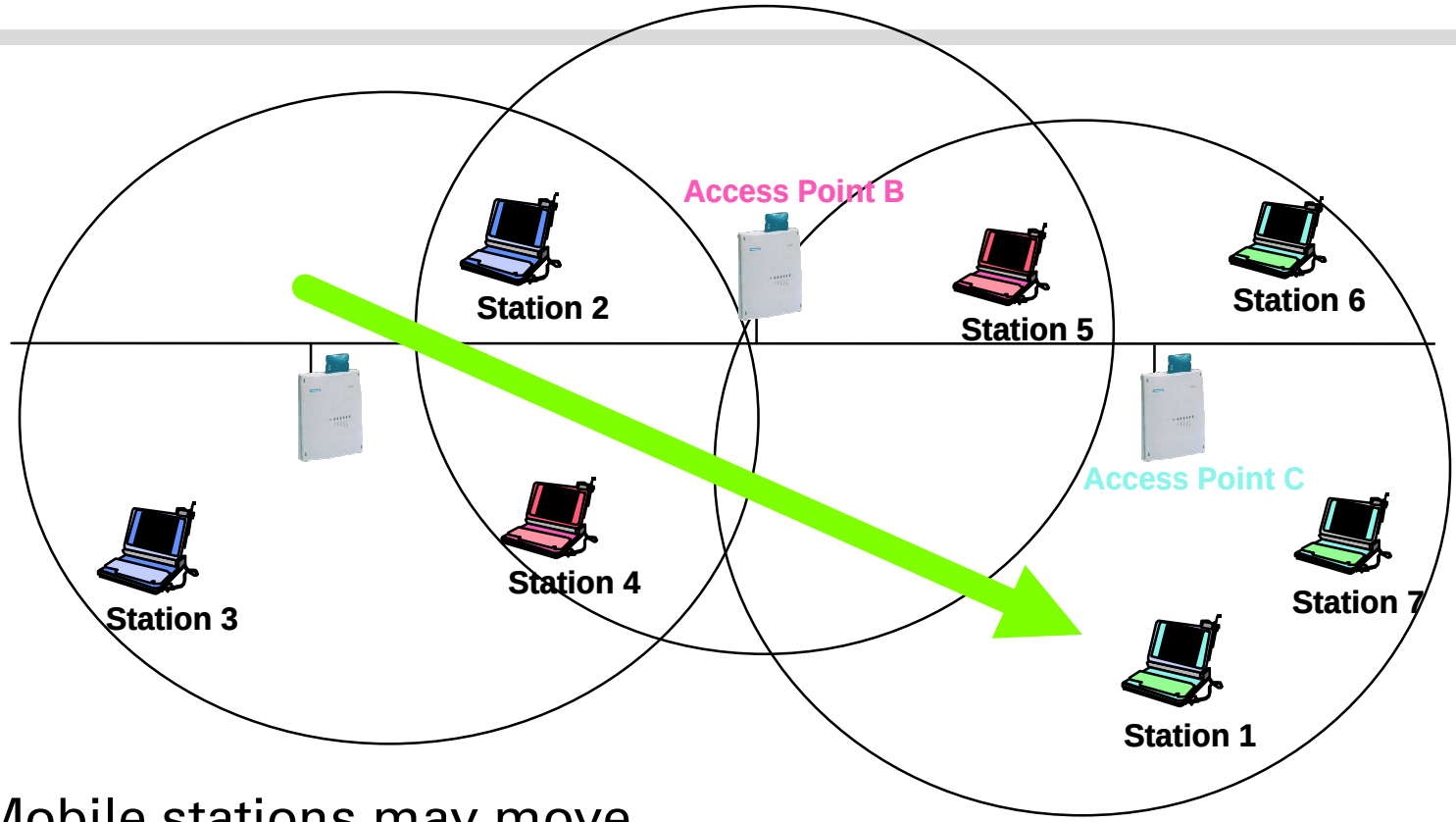


Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point
- ReAssociation follows a similar process

Roaming



- Mobile stations may move…
  - beyond the coverage area of their Access Point
  - but within range of another Access Point
- Reassociation allows station to continue operation

Roaming Approach

- Station decides that link to its current AP is poor
- Station uses scanning function to find another AP
  - or uses information from previous scans
- Station sends Reassociation Request to new AP
- If Reassociation Response is successful
  - then station has roamed to the new AP
  - else station scans for another AP
- If AP accepts Reassociation Request
  - AP indicates Reassociation to the Distribution System
  - Distribution System information is updated
  - normally old AP is notified through Distribution System

Privacy and Access Control

- Goal of 802.11 is to provide “Wired Equivalent Privacy” (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control.
  - Has provisions for “OPEN”, “Shared Key” or proprietary authentication extensions.
- Optional (WEP) Privacy mechanism defined by 802.11.
  - Limited for Station-to-Station traffic, so not “end to end”.
  - Only implements “Confidentiality” function.
  - Uses RC4 algorithm based on:
    - *a 40 bit secret key (No Key distribution standardized)*
    - *and a 24 bit IV that is send with the data.*
    - *includes an ICV to allow integrity check.*
  - Only payload of Data frames are encrypted.
    - *Encryption on per MPDU basis.*

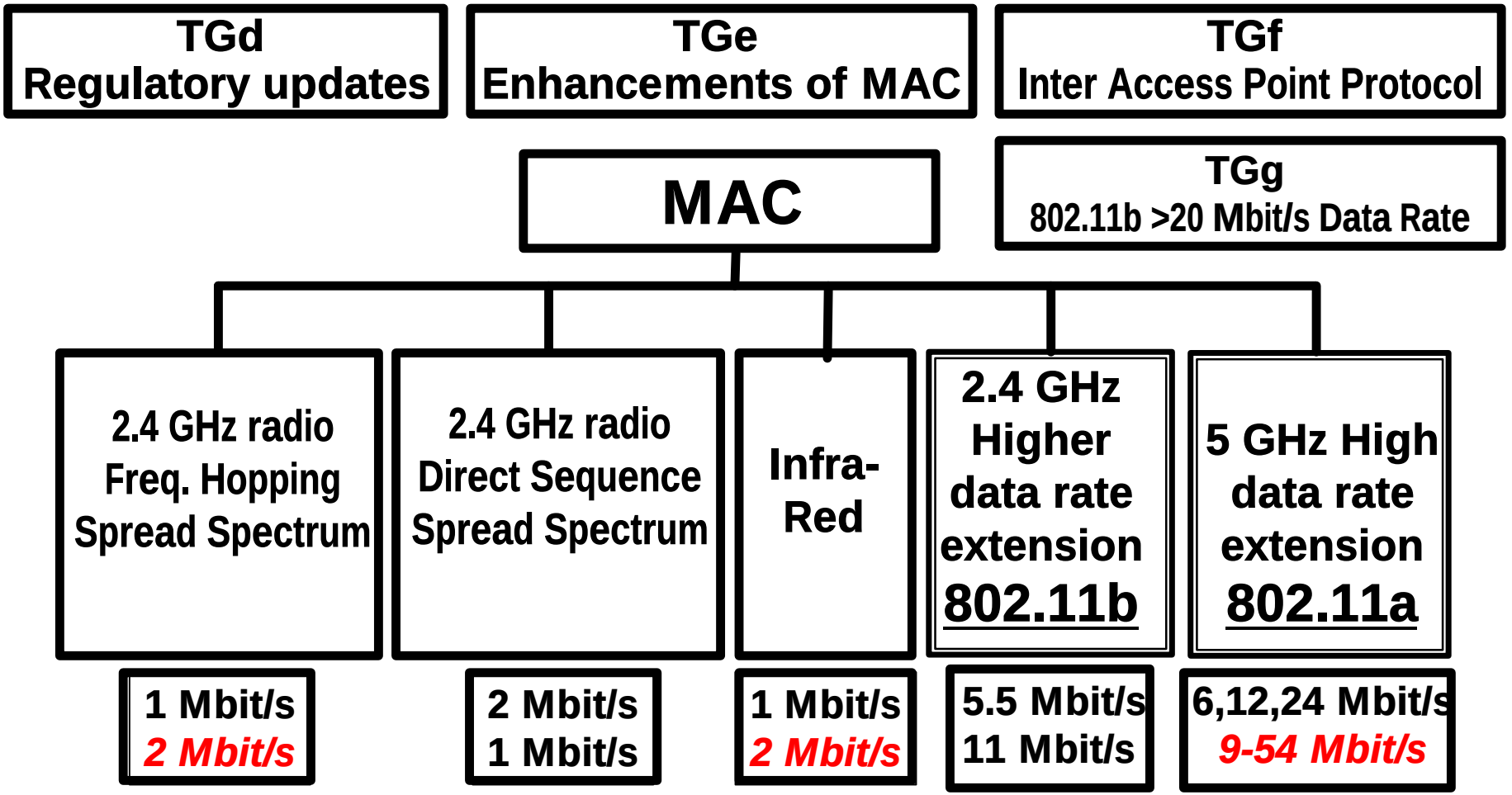
IEEE802.11 Architecture Overview

- One MAC supporting multiple PHYs
  - currently Frequency Hopping, Direct Sequence and Infrared PHYs
- Two configurations
  - “Independent” (ad hoc) and “Infrastructure”
- CSMA/CA (collision avoidance) with optional “point coordination”

  Connectionless Service
  - Transfer data on a shared medium without reservation
  - data comes in bursts
  - user waits for response, so transmit at highest speed possible
  - is the same service as used by Internet

  Isochronous Service
  - reserve the medium for a single connection and provide a continues stream of bits, even when not used
  - works only when cells (using the same frequencies) are not overlapping.
- Robust against noise and interference (ACK)
- Hidden Node Problem (RTS/CTS)
- Mobility (Hand-over mechanism)
- Security (WEP)
- Power savings (Sleep intervals)

IEEE802.11 - Current and future work



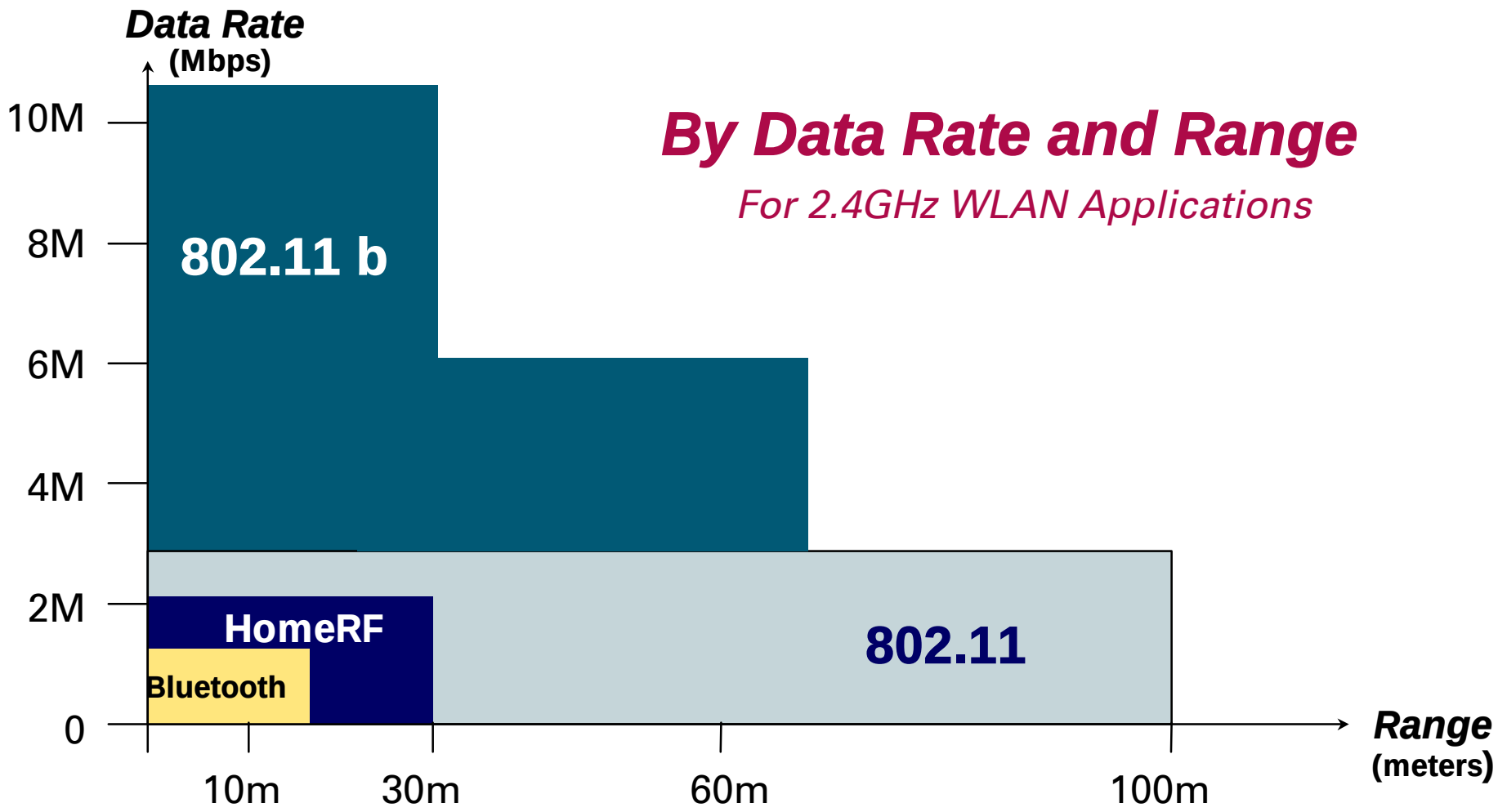
Legend: italic (and red) = optional

- **Mission Statement**

  WECA's mission is to certify interoperability of Wi-Fi (IEEE 802.11b High Rate) products and to promote Wi-Fi as the global wireless LAN standard across all market segments.

- Current Activities:
  - Promote IEEE 802.11b HR technology in enterprise, home, and education spaces
  - One standard ---- everywhere
- Consortium of Over 40 companies
  - Leading vendors
    - *WLAN equipment, PC companies, chip companies, service*
  - Published compliance matrix
  - Independent test lab (SVNL)
  - Wi-Fi seal of certified interoperability

2.4 GHz Wireless LAN Standards Efforts



Bluetooth

- Backed by cellular industry
  - Ericsson, Nokia, Intel, IBM, Toshiba
- Not a network solution
  - Simple point-to-point link
  - Low data rate (sub 1Mbps)
  - 10cm to 10m range
  - Low power and low cost
  - Under 802.15 standard
- Applications
  - Wireless desktop (replaces infrared)
  - Cell phone, cordless phone, pager
  - Internet bridge
- For more data: http:// www.bluetooth.com