Wireless Local Area Networks

Wireless LANs

- *Local Area*
- Ubiquitous – WiFi
- Others
  - HIPERLAN?
  - Bluetooth based WLANs
  - IR WLANs
- Started as extensions to wired LANs
  - Still extensions to wired LANs, but increasingly stand-alone LAN solutions (especially in homes)

Topologies

- Infrastructure based (most popular)
  - Connect users to a wired infrastructure network
  - Wireless access network like cellular phone system
  - IEEE 802.11, a, b, g , n, etc.
- Ad-Hoc based networks
  - Provide peer to peer communication – mobiles communicate between each other directly
  - Rapid Deployment (conference room)
  - Bluetooth, IEEE 802.11, a, b, g, n, Zigbee/802.15.4, Proprietary
- Point – to –Point (cable replacement)
- Mesh

Wireless LAN Markets

- Medical
  - Hospitals doctors and nurses have PDA's
- Education
  - Universities/colleges have campus wide network
- Manufacturing – factories, storage, etc.
- Retail/Small Business
  - Superstores, grocery stores, Walmart, etc. use it for inventory management
- Public Access (Hotels, airports, coffee shops)
  - (T-Mobile has > 2300 in U.S. coffee shops and bookstores, Wayport > 500 hotels, BT 5000 in U.K.)
- Wireless ISPs in many cities and housing developments
- Homes – mobility in and around house
- Market over $4.8 billion in 2005 *source researchmarkets

Spectrum for Wireless LANS

- Licensed Vs. Unlicensed
  - Private yard Vs. Public park
- Industrial Scientific and Medical bands
  - 902-928 MHz
  - 2.4 – 2.4835 GHz
  - 5.725 – 5.875 GHz
- (Unlicensed - National Information Infrastructure Bands) U-NII bands (5-6 GHz) region
  - Three bands of 100 MHz each
    - Band 1: 5.15 - 5.25 GHz
    - Band 2: 5.25 - 5.35 GHz
    - Band 3: 5.725 - 5.825 GHz
- 18-19 GHz licensed available in U.S.
- 17 GHz, 40 GHz and 60 GHz under study

IEEE 802.11 Standard

- The project was initiated in 1990
- The first complete standard was released in 1997
- Supports two topologies: Infrastructure and Ad hoc
- Suite of standards for MAC layer and below
- Main sub-standards IEEE 802.11, a, b, g, n
- Common MAC layer for all sub-standards
- Supports different physical layers at various data rates and frequencies
  - Diffused infrared (802.11)
  - Frequency hopping and direct sequence spread spectrum (802.11)
  - Complementary Code Keying (802.11b)
  - Orthogonal Frequency Division Multiplexing (OFDM) (802.11a, g)
  - Multiple Input Multiple Output & OFDM (802.11n)
  - Is TDD for each physical layer
- Many additional sub-standards studying various aspects

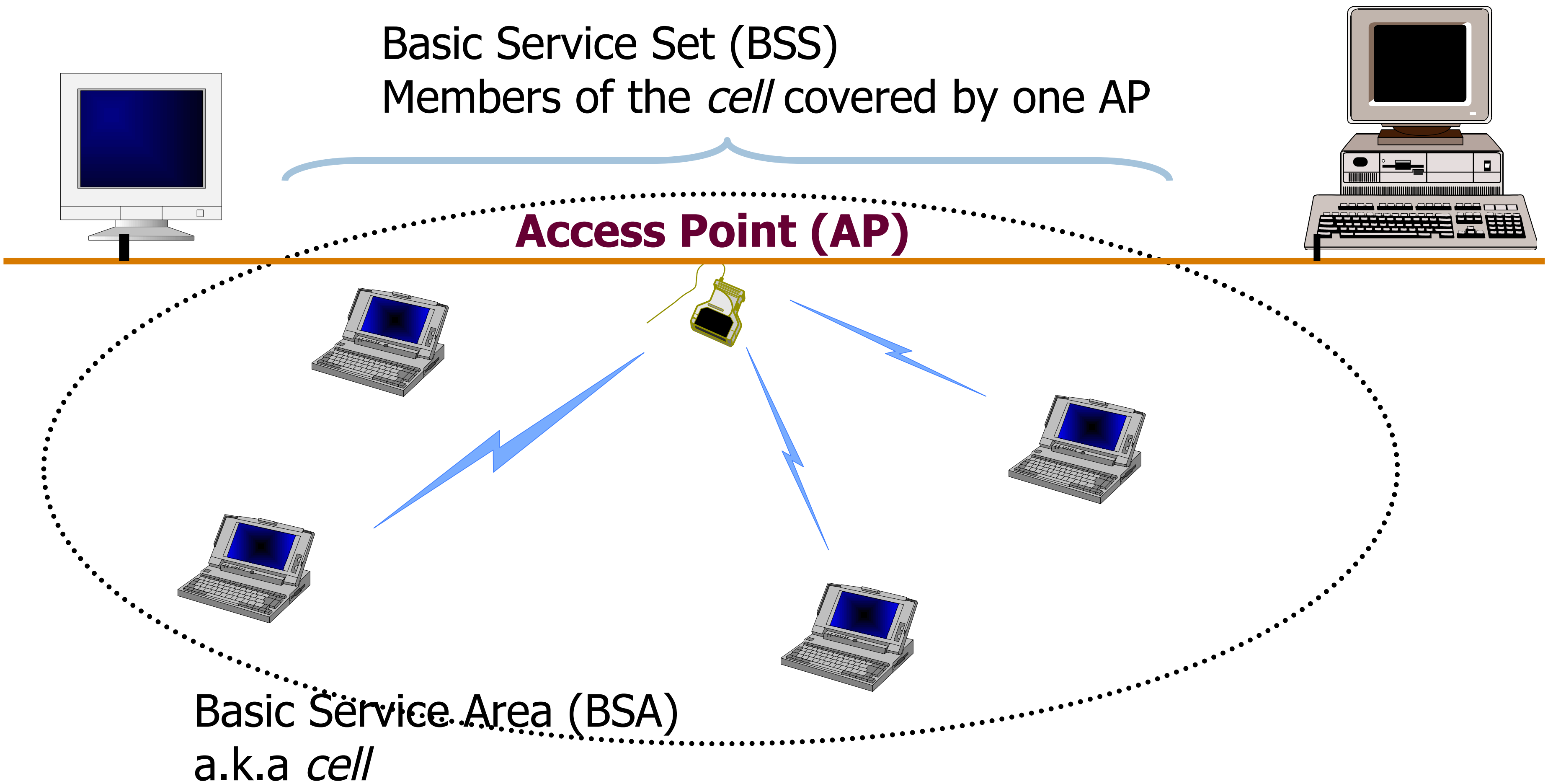
IEEE 802.11 Terminology

- Access Point (AP)
  - Acts as a base station for the wireless LAN and is a bridge between the wirless and wired network
- Basic Service Area (BSA)
  - The coverage area of one access point
- Basic Service Set (BSS)
  - A set of stations controlled by one access point
- Distribution system
  - The fixed (wired) infrastructure used to connect a set of BSS to create an extended service set (ESS)
- Portal(s)
  - The logical point(s) at which non-802.11 packets enter an ESS

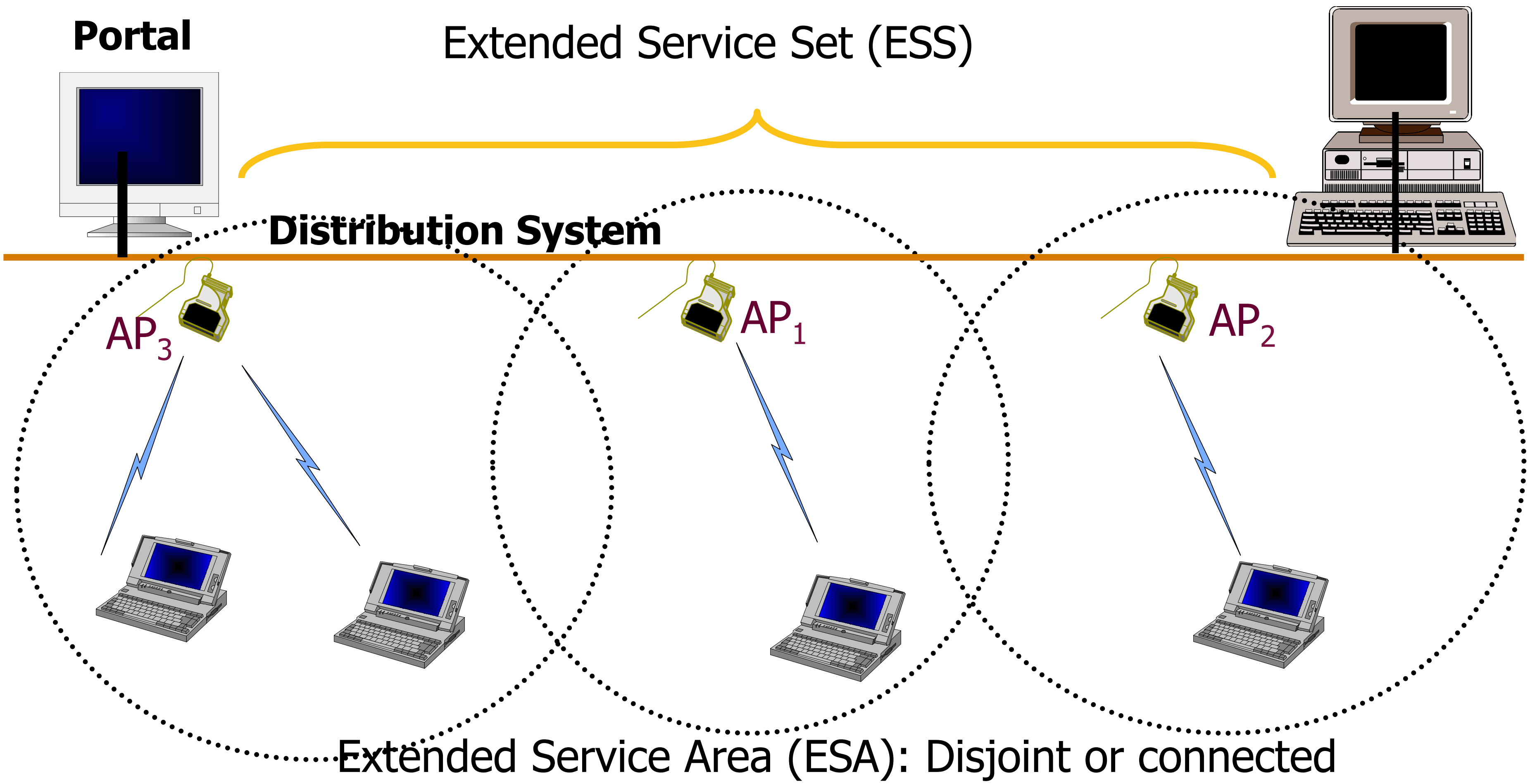
Infrastructure Network Topology

- A wired infrastructure supports communications between mobile hosts (MHs) and between MHs and fixed hosts
- Star topology
  - The BS or AP is the hub
  - Any communication from a MH to another has to be sent through the BS or AP
  - The AP manages user access to the network
  - APs typically mounted on wall or ceiling
  - AC power maybe a problem, power over Ethernet option delivers AC power over UTP (Unshielded Twisted Pair) Ethernet cable
- Designed for multiple APs interconnected to cover larger areas to form ESS

Infrastructure based Architecture

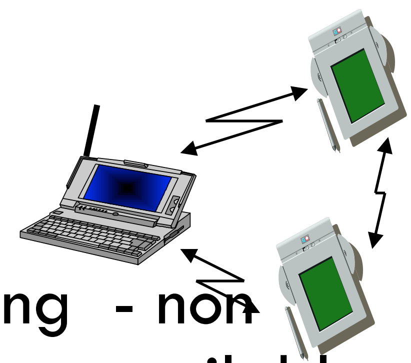


Infrastructure-based Architecture

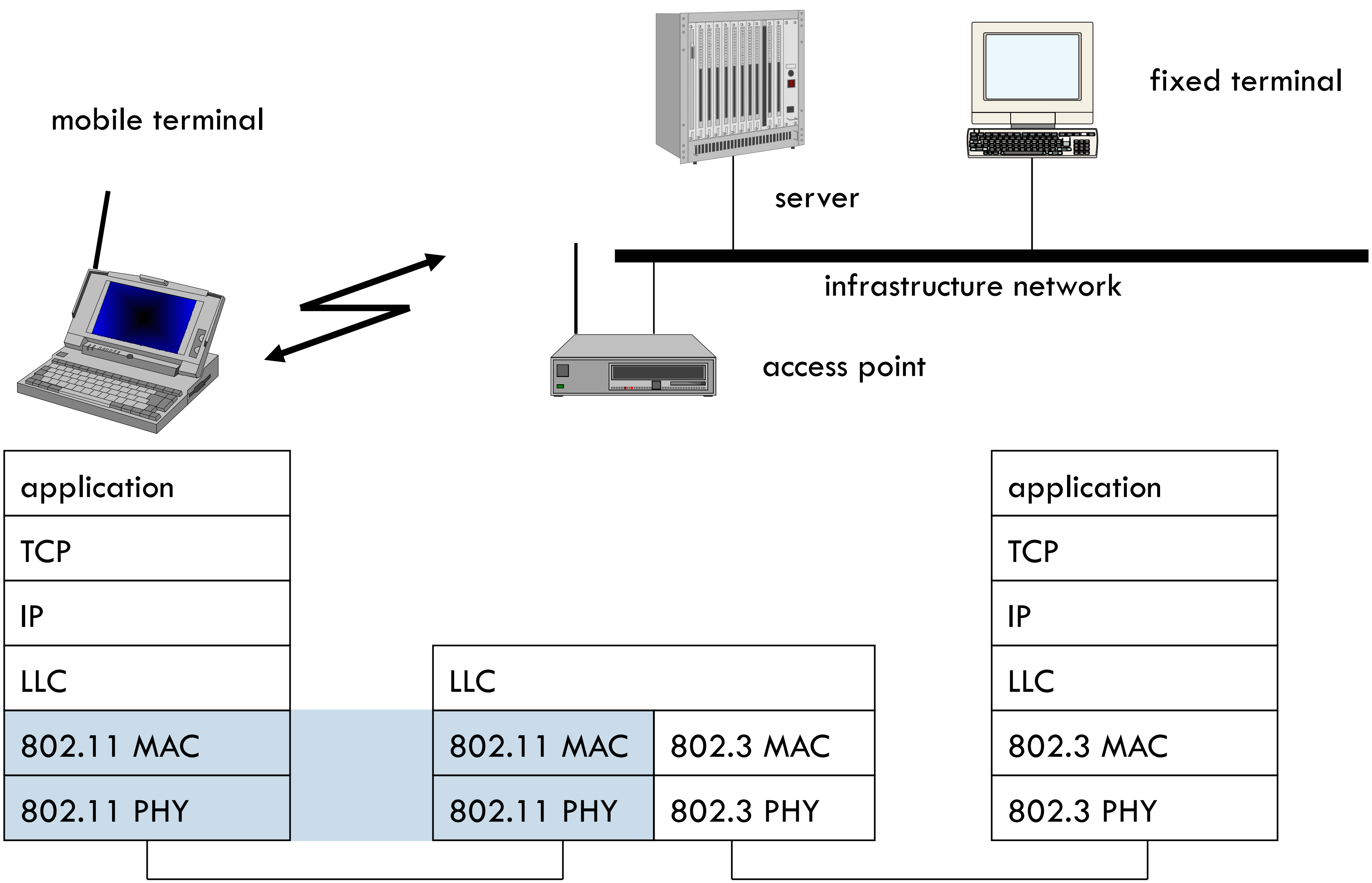


Ad hoc network topology

- Independent Basic Service Set (IBSS)
- Distributed topology
- MHs communicate between each other directly (like walkie-talkies)
- No need for a wired infrastructure
- Suitable for rapid deployment
- Use in conference rooms
- No support for multi-hop ad hoc networking - non standard freeware and proprietary systems available that support multi-hop

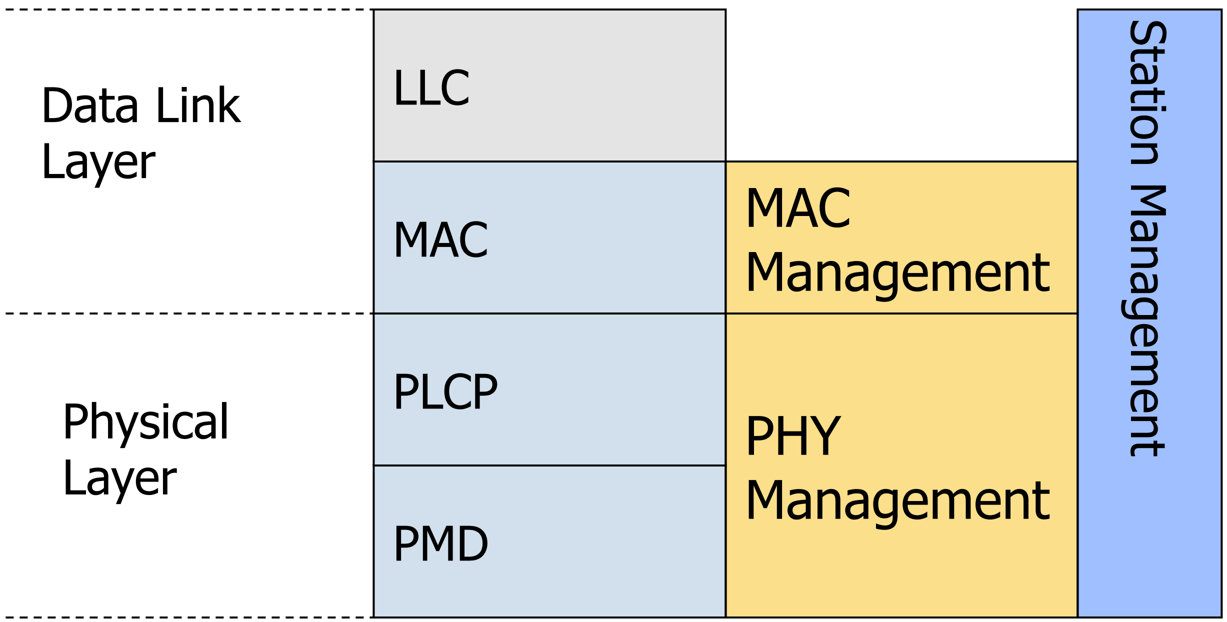


Protocol position of IEEE 802.11



IEEE 802.11 Protocol Architecture

MAC layer independent of Physical Layer
Physical varies with standard (802.11, 802.11a, etc.)
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent



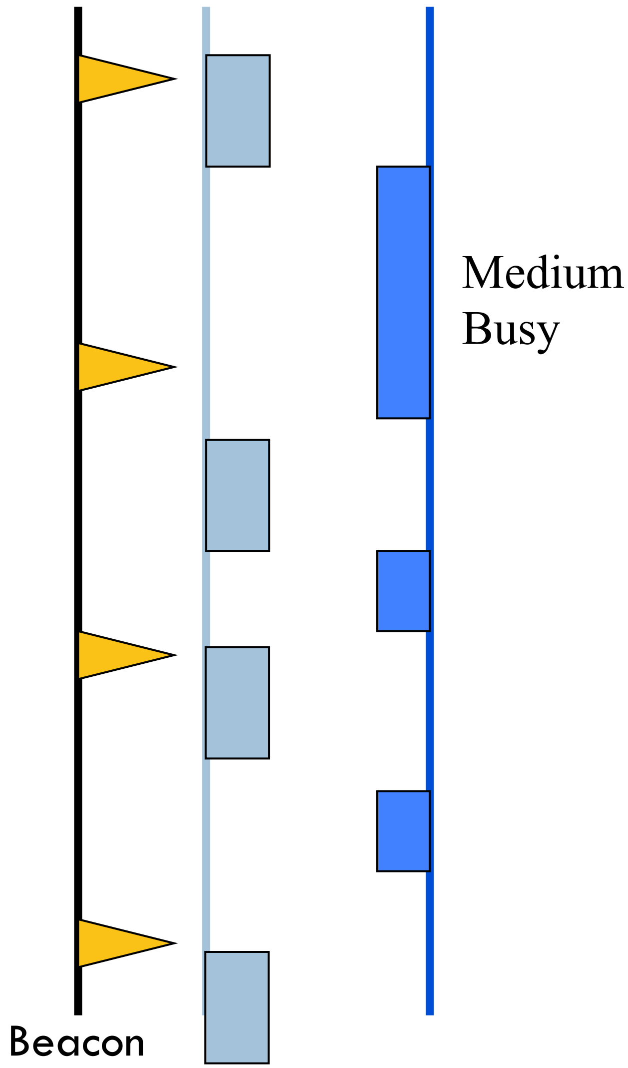
More on the Protocol Stack

- IEEE 802.11 data link layer has two sublayers
  - Logical Link Layer
    - Determined by wired network interface
  - Media Access Control (MAC) layer :
    - Security, reliable data delivery, access control
    - Provides coordination among MSs sharing radio channel

MAC Management Frames in 802.11

- Beacon
  - timestamp, beacon interval, capabilities, ESSID, traffic indication map (TIM)
- Probe
  - ESSID, Capabilities, Supported Rates
- Probe Response
  - same as beacon except for TIM
- Re-association Request
  - Capability, listen interval, ESSID, supported rates, old AP address
- Re-association Response
  - Capability, status code, station ID, supported rates

Beacon



- Beacon is a message that is transmitted quasi-periodically by the access point
- It contains information such as the BSS-ID, timestamp (for synchronization), traffic indication map (for sleep mode), power management, and roaming
- Beacons are always transmitted at the expected beacon interval unless the medium is busy
- RSS measurements are made on the beacon message

Association

- In order to deliver a frame to a MS, the distribution system must know which AP is serving the MS
- Association is a procedure by which a MS “registers” with an AP
- Only after association can a MS send packets through an AP
- How the association information is maintained in the distribution system is NOT specified by the standard

Re-association and Dissociation

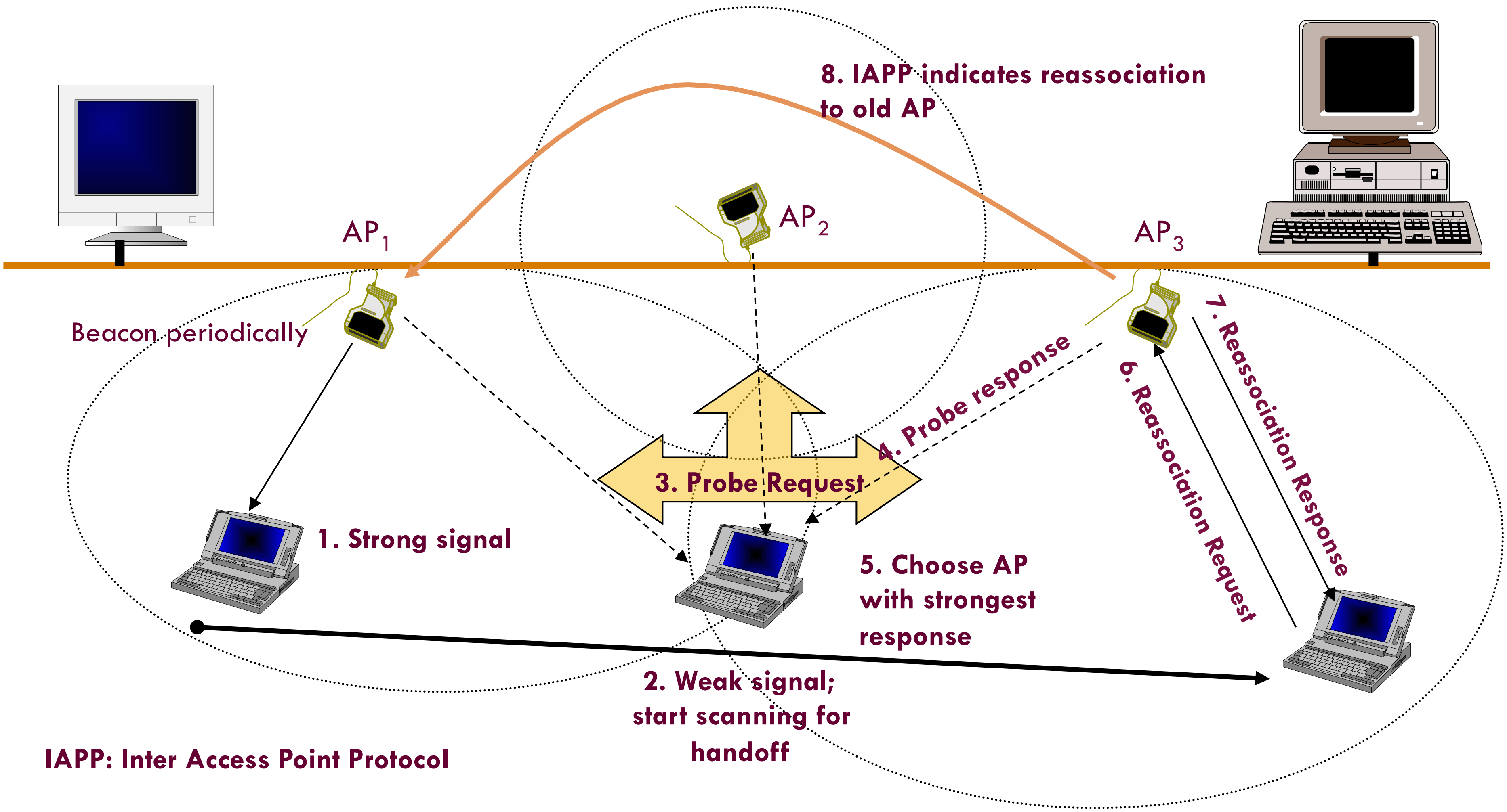
- The ***re-association*** service is used when a MS moves from one BSS to another within the same ESS
- It is always initiated by the MS
- It enables the distribution system to recognize the fact that the MS has moved its association from one AP to another

- The ***dissociation*** service is used to terminate an association
- It may be invoked by either party to an association (the AP or the MS)
- It is a notification and not a request. It cannot be refused
- MSs leaving a BSS will send a dissociation message to the AP which need not be always received

IEEE 802.11 Mobility Types

- No Transition
  - MS is static or moving within a BSA
- BSS Transition
  - The MS moves from one BSS to another within the same ESS
- ESS Transition
  - The MS moves from one BSS to another BSS that is part of a new ESS
  - Upper layer connections may break (needs Mobile IP)

Handoff in 802.11



IAPP: Inter Access Point Protocol

Inter-AP Protocol (802.11f)

- APs register with a “Registration Service” in the distribution system
  - They use the IAPP-INITIATE and IAPP-TERMINATE to register and deregister
- A MS in 802.11 can be associated with only one AP
- When the MS sends a reassociation request and obtains an association frame, the new AP sends an IAPP-MOVE-notify packet to the old AP
  - The old AP address is obtained from the registration service
  - If the registration service cannot be located, the AP will issue an IAPP-ADD-notify packet to the broadcast MAC address on the LAN
- The old AP sends an IAPP-MOVE-response packet with any context information it had for the MS

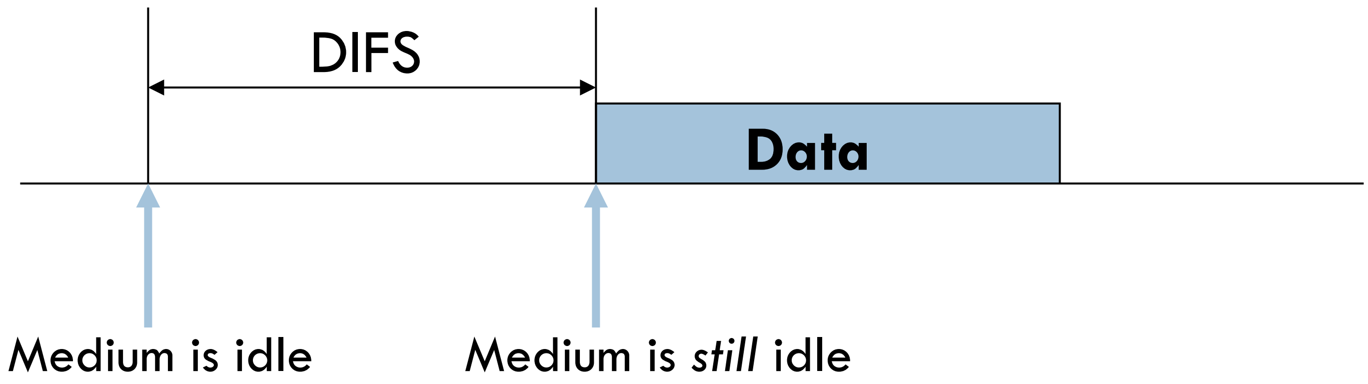
The IEEE 802.11 MAC Layer

- IEEE 802.11 is based on Carrier Sense Multiple Access with Collision Avoidance: CSMA/CA
- Mandatory access mechanism is "asynchronous" based on CSMA/CA and is provided by what is called the Distributed Coordination Function (DCF)
- Optional access mechanism for "time bounded" service is based on polling and is provided by what is called a Point Coordination Function (PCF)

Physical and Virtual Carrier Sensing

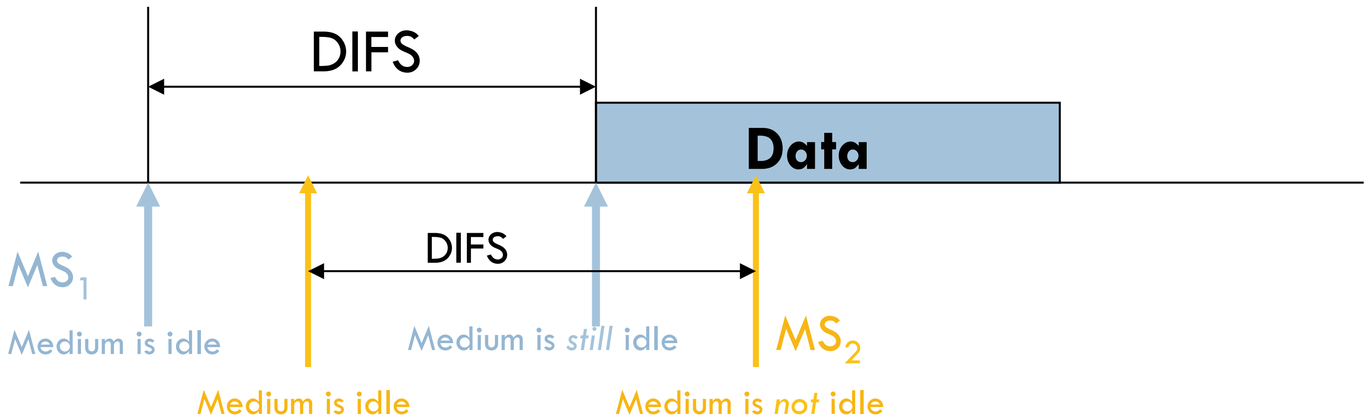
- The physical layer performs a "real" sensing of the air interface to determine if a medium is busy or idle
  - Analyzes detected packets
  - Detects carrier otherwise by RSS
- The MAC layer performs a "virtual" carrier sensing
  - The "length" field is used to set a network allocation vector (NAV)
  - The NAV indicates the amount of time that must elapse before the medium can be expected to be free again
  - The channel will be sampled only after this time elapses (why?)
- The channel is marked busy if either of the physical or virtual carrier sensing mechanisms indicate that the medium is busy

Idle Channel



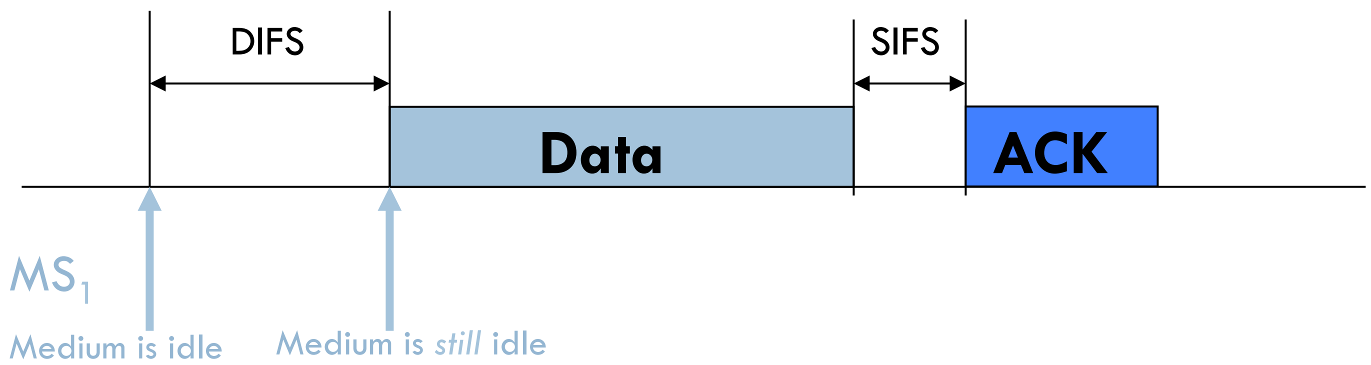
- If the medium is idle, every MS has to wait for a period DIFS (DCF inter-frame spacing) to send DATA
- After waiting for DIFS, if the medium is still idle, the MS can transmit its data frame

How does it help?



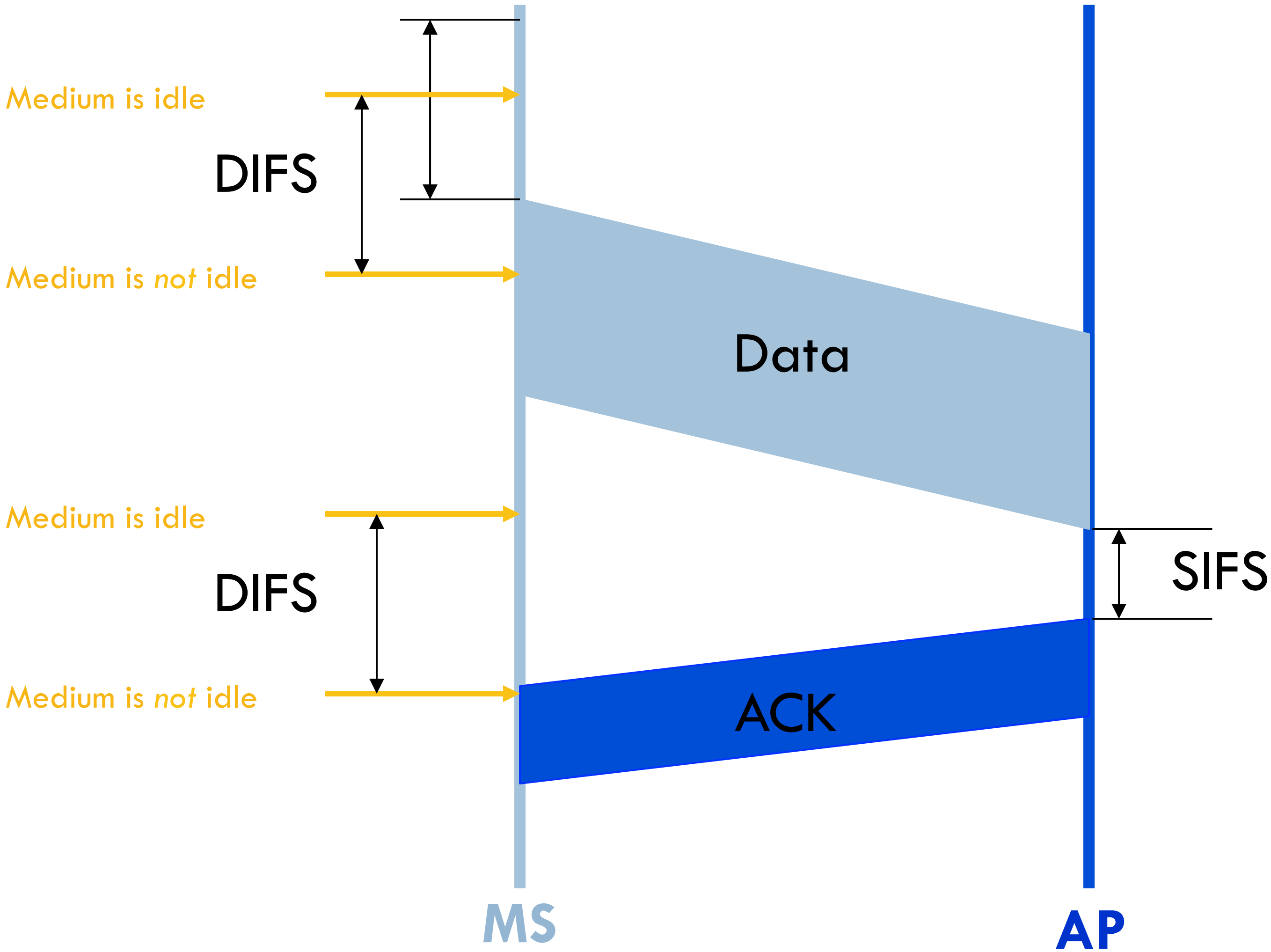
- If a second MS senses the medium to be idle after the first MS, it will find the medium to be busy after DIFS
- It will not transmit => collision is avoided

Acknowledgements

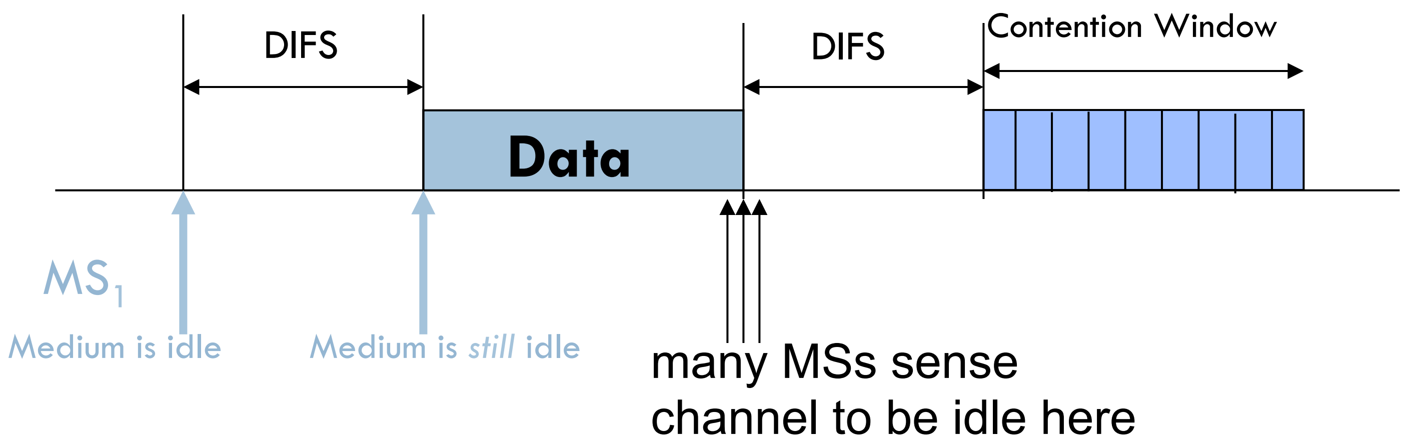


- A short inter-frame spacing (SIFS) is used
  - SIFS is the absolute minimum duration that any MS should wait before transmitting anything
- It is used ONLY for acknowledgements (which will be sent by a receiving MS or AP alone)
- ACKs receive highest priority!
- ACKs will almost always be sent on time

Data Transmission and ACKs



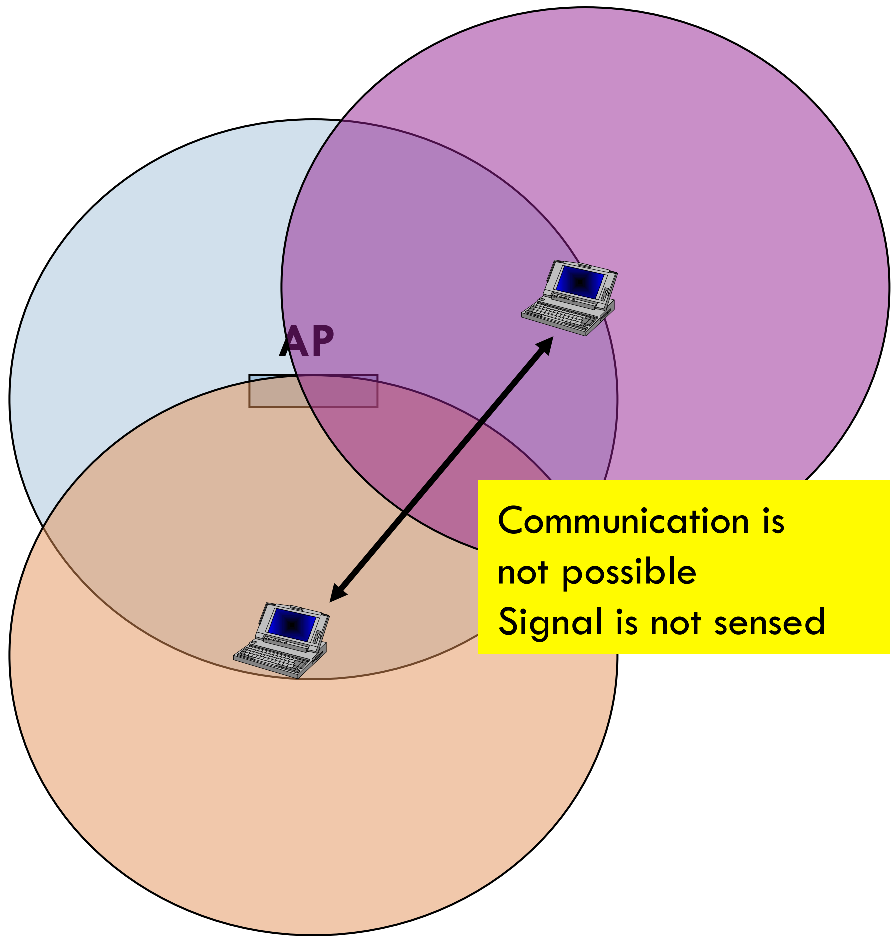
Busy Channel



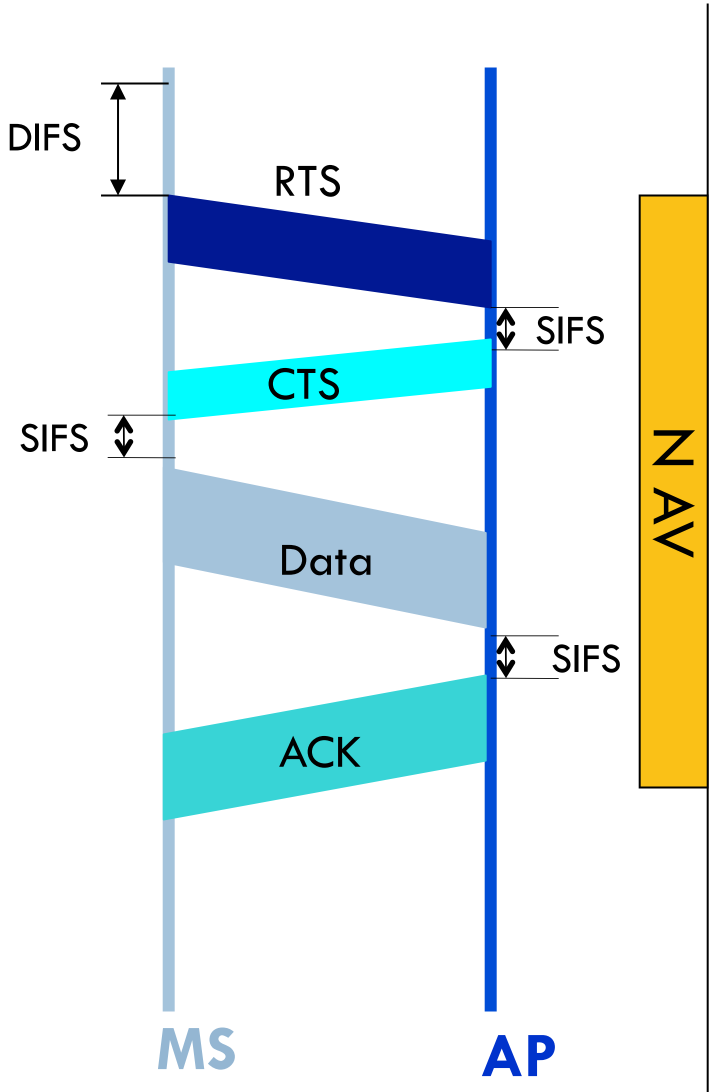
- Each MS has to still wait for a period of DIFS
- Each MS chooses a random time of back-off within a contention window
- Each MS decrements the back-off. Once the back-off value becomes zero, if the medium is idle, the MS can transmit
- The MS with the smallest back-off time will get to transmit
- All other MSs freeze their back-off timers that are "decremented" and start decrementing the timer in the next contention window from that point

When do collisions occur?

- MSs have the same value of the back-off timer
- MSs are not able to hear each other because of the "hidden terminal" effect
- MSs are not able to hear each other because of fading
- Solution: RTS/CTS
  - Also avoids excessive collision time due to long packets



RTS/CTS Mechanism



- RTS-Request to Send (20 bytes)
- CTS-Clear to Send (14 bytes)
- They can be used only prior to transmitting data
- After successful contention for the channel, a MS can send an RTS to the AP
- It gets a CTS in reply after SIFS
- CTS is received by all MSs in the BSS
- They defer to the addressed MS while it transfers data
- If there is a collision, no CTS is received and there is contention again

Large Frames

- Large frames that need fragmentation are transmitted sequentially without new contention
- The channel is automatically reserved till the entire frame is transmitted
- The sequence of events is:
  - Wait for DIFS & CW; Get access to channel OR use RTS/CTS
  - Send first fragment; include number of fragments in the field
    - All other MSs update their NAV based on the number of fragments
    - ACK is received after SIFS
    - The next fragment is transmitted after SIFS
  - If no ACK is received, a fresh contention period is started
- RTS/CTS, if used, is employed only for the first fragment

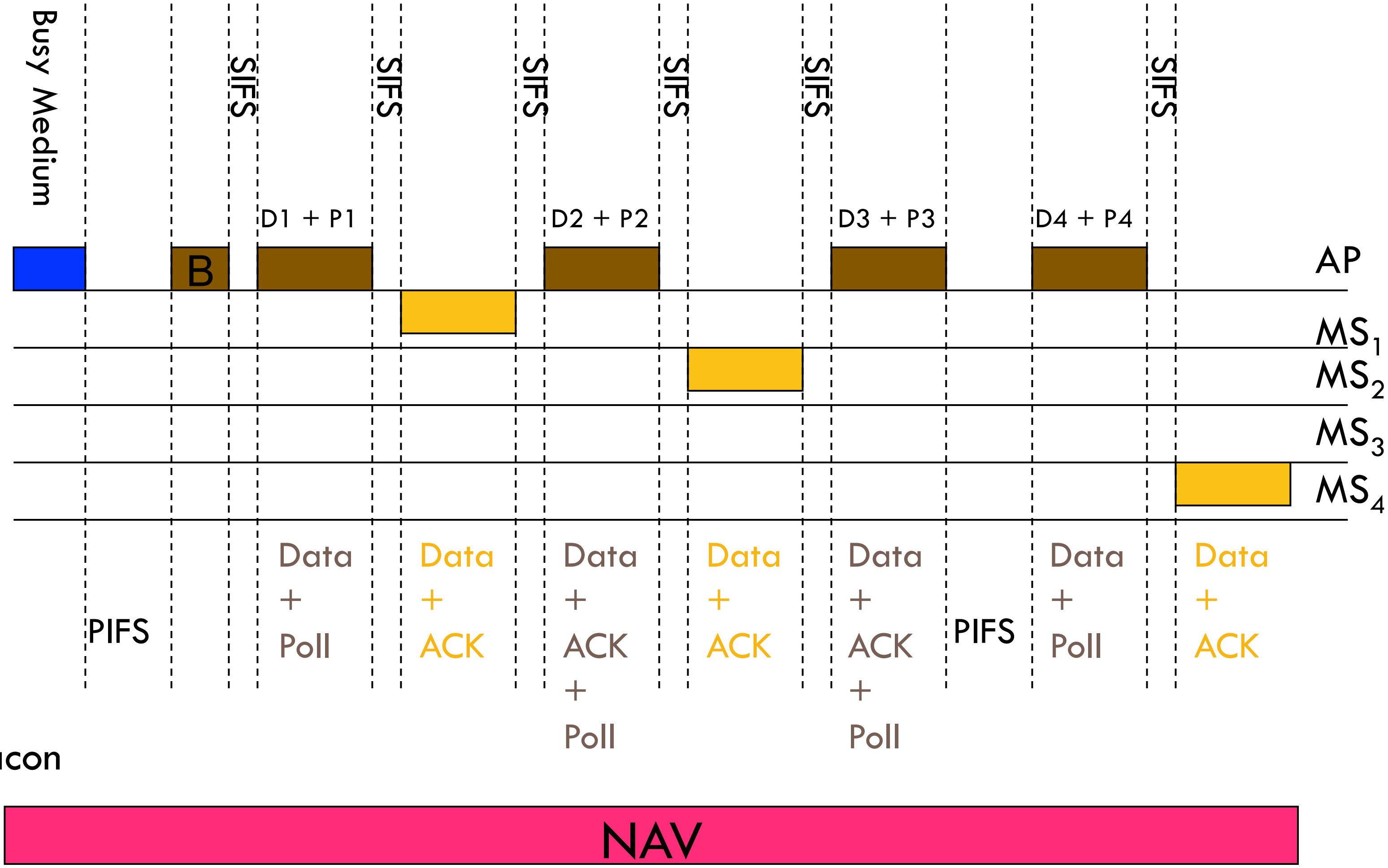
Taking turns protocols

- Token ring or bus
  - Infeasible for wireless networks
    - Errors and self configuration
  - Not widely studied except for IR systems
- Polling
  - A centralized authority polls each MS for data and the MS can respond to the poll if it has anything to transmit
  - If the MS has nothing to transmit or it is inactive, the polling scheme consumes bandwidth unnecessarily
- Can guarantee delays and throughput unlike random access schemes
- Example systems
  - PCF in IEEE 802.11
  - Bluetooth

Point Coordination Function (PCF) in IEEE 802.11

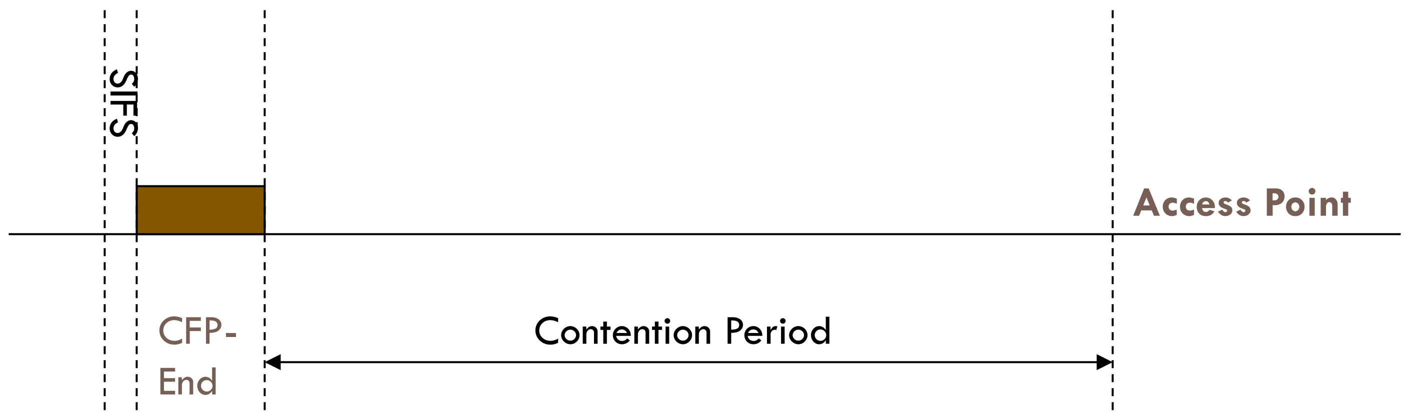
- Optional capability to provide "time-bounded" services
- It sits on top of DCF and needs DCF in order to successfully operate
- A point coordinator (the AP)
  - Maintains a list of MSs that should be polled
  - Polls each station and enables them to transmit without contention
  - Ad hoc networks cannot use this function (why?)
- Time (a superframe) is divided into two parts
  - Contention Free Period (CFP)
  - Contention Period (CP)
- A MS must be CFP-aware to access the CFP
- Replies to polling can occur after SIFS

PCF Continued



B = Beacon

PCF Continued



- The CFP is dynamically variable
- A MS can transmit to another MS within the CFP
  - In such a case, an ACK from the receiver is given priority over the next polling message
- The AP could transmit data to a non CF-aware MS
  - In such a case, once again, an ACK from the receiver is given priority

Physical Sub-Layers in 802.11

- PLCP maps the MAC frame into an appropriate PHY frame
  - Reduces MAC dependence on PMD
- PLCP frame includes information for synchronization, length of transmission, header error check, frame delimiters, etc.
- The PLCP forms the PMD frame which is different for different physical layers
- The PMD layer specifies the modulation, demodulation, and coding
- Together the two physical sub-layers provide the MAC layer a "clear channel assignment" signal to indicate the busy/idle nature of the channel
- The Physical Management layer fine tunes the channel, modulation, etc. and manages the physical layer MIBs

802.11 Physical Layer Options

- Diffused infrared (802.11)
  - PPM , 1, 2 Mbps, ARQ with CRC, 10m range, cheap
- Frequency hopping spread spectrum (802.11)
  - Random 2.5 hops per second, GMSK modulation, ARQ with CRC, 1, 2 Mbps in 915MHz band
- Direct sequence spread spectrum (802.11)
  - 11 bit spreading Barker code, DBPSK – 1Mbps, DQPSK – 2Mbps, ARQ with CRC, in 915MHz band
- Complementary Code Keying (802.11b)
  - 1,2, 5.5, 11 Mbps - spreading done in modulation channel symbols, error control ARQ with CRC in 20MHz band – 20MHz channels
  - Rate depends on RSS
- Orthogonal Frequency Division Multiplexing (OFDM) (802.11a, g)
  - Parallel sub-channels with adaptive modulation based on SNR – higher data rates up to 54Mbps - 20MHz channels
- OFDM and Multiple Input Multiple Output (802.11n)
  - Multiple antenna and receivers together with OFDM – higher data rates > 100Mbps

802.11a,g

- OFDM: Each subcarrier uses same modulation

Data rate	Modulation	FEC Coding Rate	Data bits per channel symbol
6Mbps	BPSK	1/2	24
9Mbps	BPSK	3/4	36
12Mbps	QPSK	1/2	48
18Mbps	QPSK	3/4	72
24Mbps	16QAM	1/2	96
36Mbps	16QAM	3/4	144
48Mbps	64QAM	2/3	192
54Mbps	64QAM	3/4	216

802.11n

- Approved recently - works in 2.4 and 5 GHz bands
  - 4 to 5 times the data rates of 802.11a,g → 200-300Mbps
- Main Changes
  - Physical layer uses Multiple Input Multiple Output (MIMO) OFDM
    - Has multiple antennas at each end of the channel – provides spatial diversity
    - OFDM part about the same as 802.11a,g – uses 64QAM with 5/6 FEC rate
  - Channel Bonding
    - Combines 2 of the 20MHz 802.11a,g channels to achieve higher data rates
  - Packet Aggregation
    - Reduce overhead by aggregating multiple packets from a single application/user into a common frame

Other 802.11 standards in progress

- 802.11ac
  - Extremely high throughput in frequency bands below 6 GHz
- 802.11ad
  - Extremely high throughput in frequency bands 57-66 GHz
  - Also called WiGig
- 802.11af
  - TV White Spaces Operation