# CSCD 433
# Network Programming
## Winter 2017

## Lecture 7
Ethernet and Wireless 802.11

# Topics

- 802 Standard
  - MAC and LLC Sublayers
  - Review of MAC in Ethernet
  - Ethernet vs. Wireless - CSMA
  - MAC  in 802.11 Wireless

# IEEE Standards


- In 1985, Computer Society of IEEE started a project, called Project 802,
- Set standards to enable intercommunication among equipment from a variety of manufacturers … wonderful!!!
- Project 802
  - Specifies functions of  physical layer and the data link layer of major LAN protocols

# IEEE 802 Series of LAN Standards

802 standards free to download from http://standards.ieee.org/getieee802

**IEEE 802®: Overview & Architecture**

**IEEE 802.1 ™ Bridging & Management**

**IEEE 802.2 ™: Logical Link Control**

**IEEE 802.3 ™: CSMA/CD Access Method**

**IEEE 802.4 ™: Token-Passing Bus Access Method**

**IEEE 802.5 ™: Token Ring Access Method**

**IEEE 802.6 ™: DQDB Access Method**

**IEEE 802.7 ™: Broadband LAN**

**IEEE 802.10 ™: Security**

**IEEE 802.11 ™: Wireless**

**IEEE 802.12 ™: Demand Priority Access**

**IEEE 802.16™: Broadband Wireless Metropolitan Area Networks**

# 802.11 Physical Layer

- Issued in four stages

- **1997, First part**
  - IEEE 802.11
  - Includes MAC layer and three physical layer specifications
  - Two in 2.4-GHz band and one infrared, Operate 1 and 2 Mbps

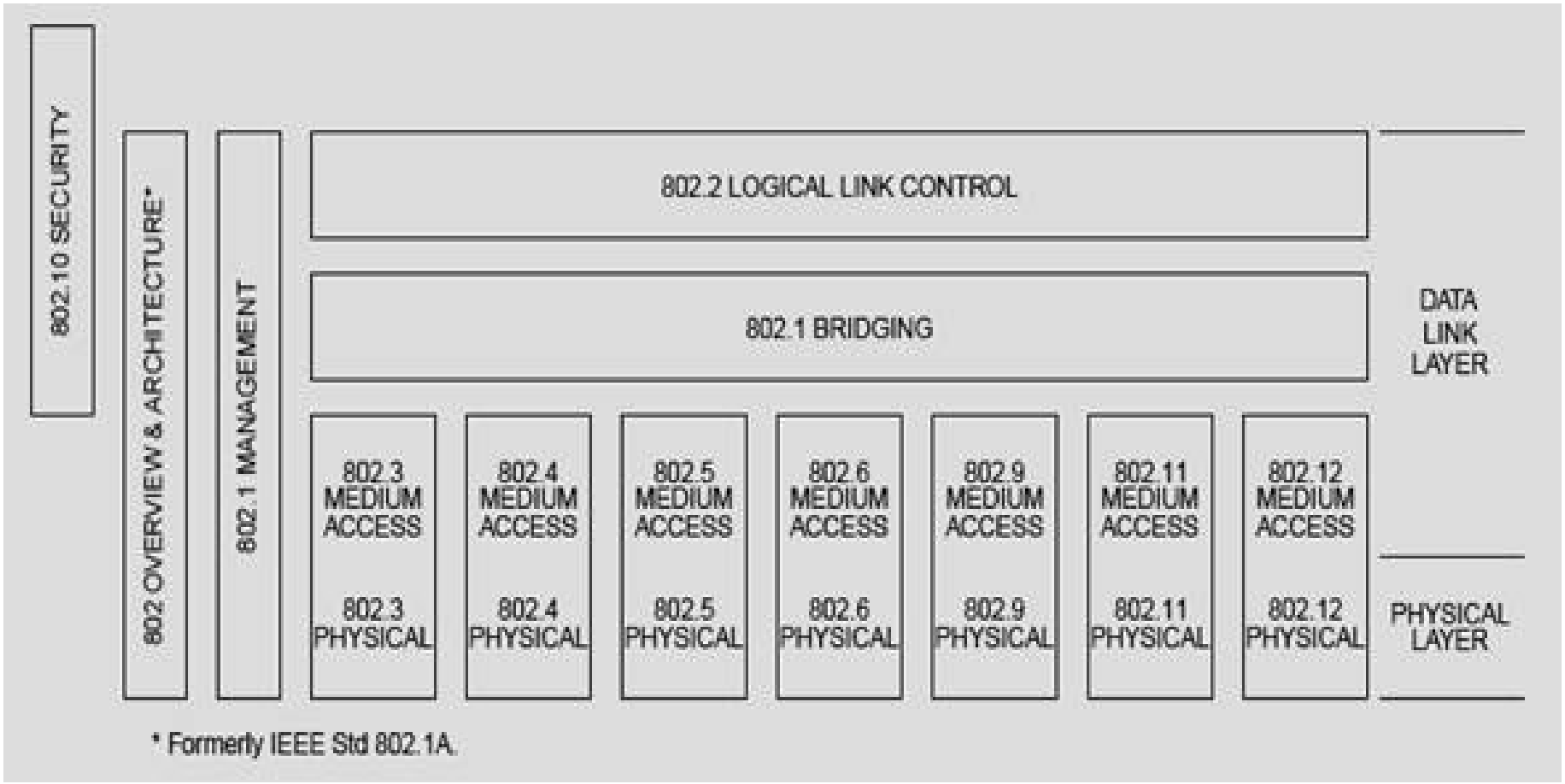
- **1999, Two more parts**
  - IEEE 802.11a
    - 5-GHz band, data rate up to 54 Mbps
  - IEEE 802.11b
    - 2.4-GHz band, data rate at 5.5 and 11 Mbps

- **2002, Most recent**
  - IEEE 802.11g extended IEEE 802.11b to higher data rates, up to 54 Mbps

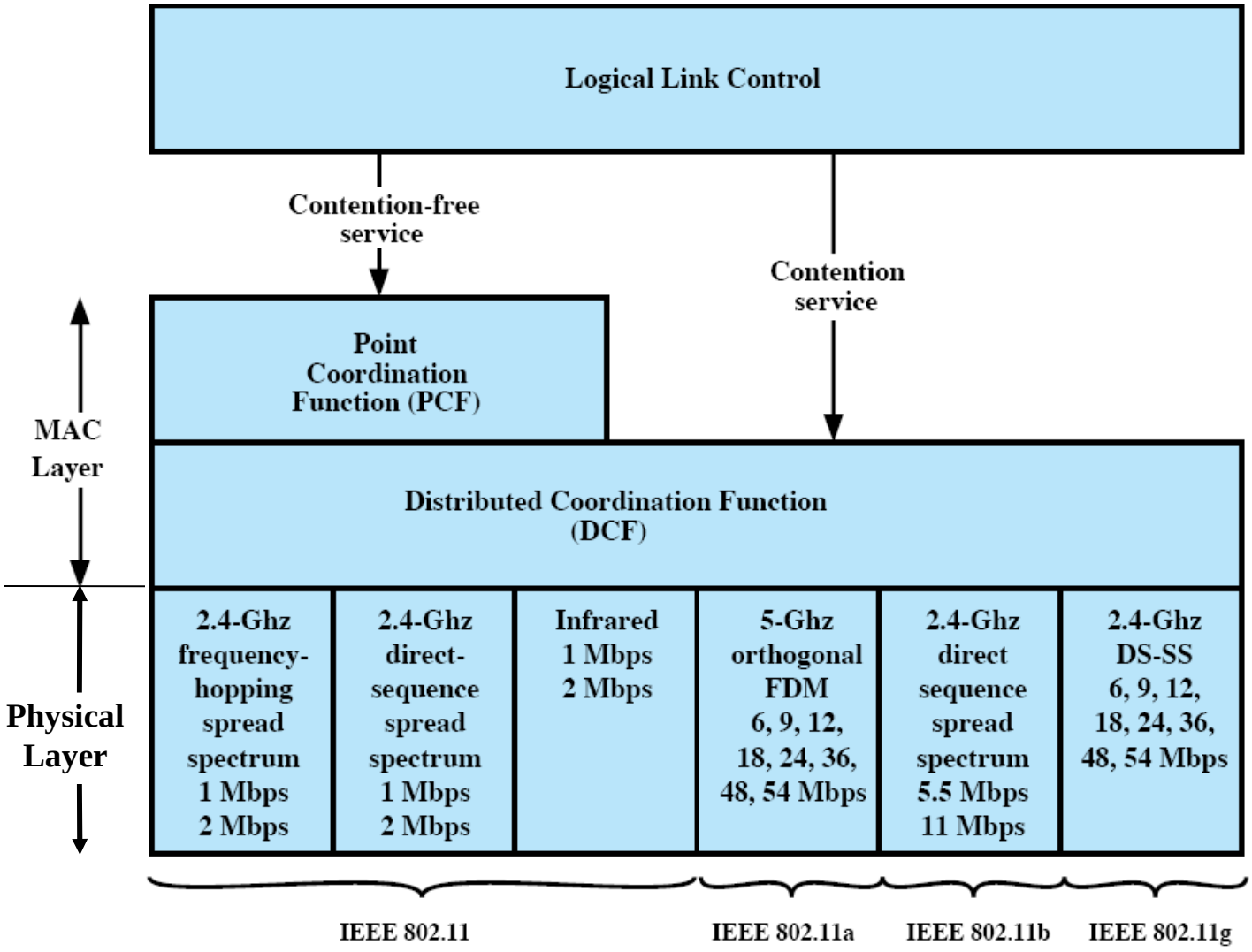
- **At present**
  - IEEE 802.11n and 802.11ac data rate up to hundreds of Mbps

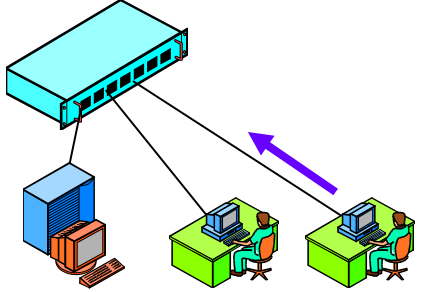
# IEEE 802 Standard

Complete specification of 802 standard



# IEEE 802.11 Protocol Architecture





# 802 Layering

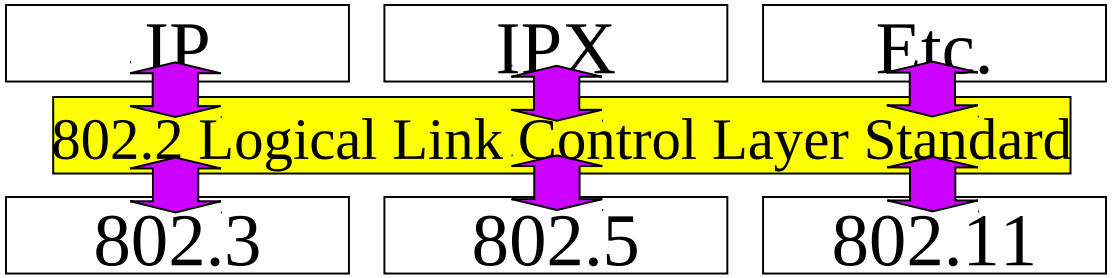
## Media Access Control (MAC) Layer

- 802.11 standard specifies common medium access control (MAC) Layer
- In general, MAC Layer manages and maintains communications between 802.11 stations by coordinating access to shared radio channel, has most of functionality

## Logical Link Control (LLC) Layer

Adds optional error correction (rarely used)

Connects to next-higher-layer (internet), multiplexes higher level protocols



# Medium Access Control

- Two sublayers

**Lower sublayer**

**Distributed Coordination Function** (DCF)

- Uses a contention algorithm to provide access to all traffic
- Uses CSMA/CA – Carrier Sense Multiple Access/Collison Avoidance

**Higher sublayer**

**Point Coordination Function** (PCF)

- Uses a centralized algorithm
- "Contention free"
- Implemented on top of DCF

- **Note:** PCF has not been popularly implemented in today's 802.11 products, DCF is widely used

# MAC Sublayer Functions

- MAC is set of rules to determine how to access medium and data link components.

  It provides core framing operations, sets the frame header fields

- MAC purpose in General
  - Coordinates and shares use of radio bandwidth
  - Synchronization between stations
  - Datagram transfer function
  - **MAC layer management functions**

    Authentication and De-Authentication

    Association, Re-Association, and Disassociation

    Beacon and Probe frames

# MAC Sublayer Functions

- 802.11 uses CSMA/CA mechanism

  **Carrier Sense Multiple Access with Collision Avoidance**

  - It is considered to be ‘fair’ for all users because treats them equally

Recall that Ethernet uses CSMA/CD ….

# Brief Review of
# Classical or Standard Ethernet

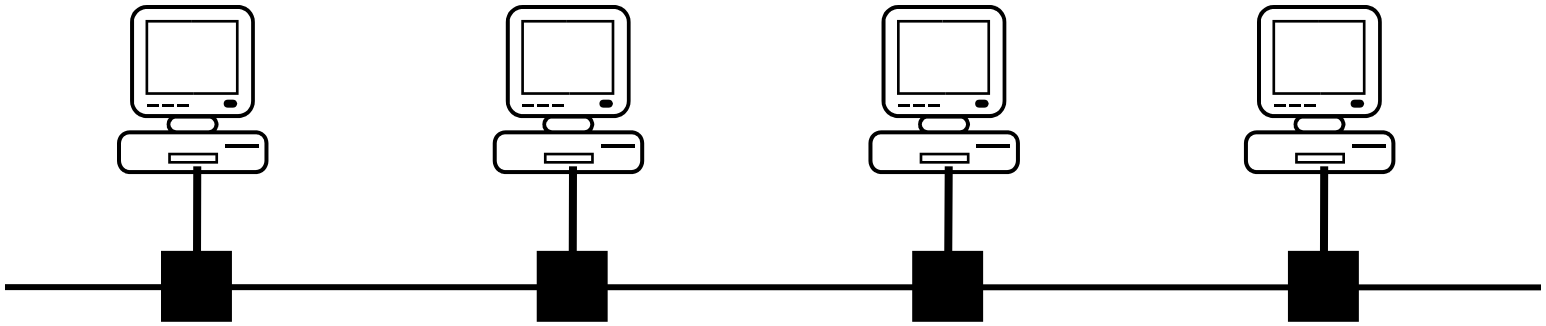
# Review of Classical Ethernet

- Recall that classical Ethernet is shared technology
- Everyone has access to wires
- Users contend with collisions and MAC layer protocol dealt with these collisions
  - Note – This is with traditional cable and Hubs
- Review characteristics of Ethernet

# Ethernet Recap

- Classic Ethernet
  - One long cable, 500 meter max segment
  - Snaked around building as single, long cable
  - All computers attached
- Thick Ethernet and Thin
  - Began as thick yellow cable, marked every 2.5 meters to show computer attachments
  - Thinner, bent more easily connections with BNC connectors
  - Cheaper to install, 185 meter max segment

# CSMA/CD Protocol



All hosts transmit & receive on one channel

When a host has a packet to transmit

1. Carrier Sense: Check that the line is quiet before transmitting
2. Collision Detection: Detect collision as soon as Possible.
   Collision is detected, stop transmitting; wait a random time, then return to step 1.

# Ethernet CSMA/CD algorithm

## Algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission

   If NIC senses channel busy, waits until channel idle, then transmits
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !

# Ethernet CSMA/CD Algorithm

4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. **After aborting**

   NIC enters **exponential backoff**

   after **mth** collision, NIC chooses a *K,* small integer, at random from {0,1,2,…,$2^m$-1}

   NIC then waits K·512 bit time,

- Returns to Step 2

# Ethernet's CSMA/CD (more)

## Exponential Backoff

- Goal Adapt retransmission attempts to estimated current load
  - **Heavy load -> random wait will be longer and more varied**

- First collision: Choose K from {0,1};
  Delay is K· 512 bit transmission times
- After second collision: Choose K from {0,1,2,3}…
- After ten collisions, Choose K from {0,1,2,3,4,…,1023}
- Set size grows Exponentially

# Wireless Communication Systems

- In terms of packet or frame delivery ….
- What complicates wireless networking vs. wired networking?

# Wireless Link Characteristics


## Differences from wired link ….

- Decreased signal strength: Radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: Standardized wireless network frequencies shared by other devices that can interfere
- Multipath propagation: Radio signal reflects off objects and ground, arriving at destination at slightly different times

…. make communication across link much more "difficult"

# CSMA/CD vs. CSMA/CA

- **CSMA/CD – CSMA/Collision detection**
  - For wired communication
  - No control BEFORE transmission
  - Generates collisions
  - Collision Detection- Monitors signal strength, can detect
- **CSMA/CA – CSMA/Collision Avoidance**
  - For wireless communication
  - Collision avoidance BEFORE transmission
  - Difference in energy/power for transmit & receive
  - Difficult to distinguish between incoming weak signals, noise, and effects of own transmission

# 802.11 Medium Access Control

- Shares the medium through coordination with other stations
  1. Sends control packets for coordination
     Including Acks
  2. Sets and sends individual frame timers for all to see, each frame has its own timer

- Note: There is the 802.11 standard and then there is reality of did it actually get implemented!
  - Create a lot of details for a standard but not all of it is implemented

# Wireless Collision Avoidance

STEPS

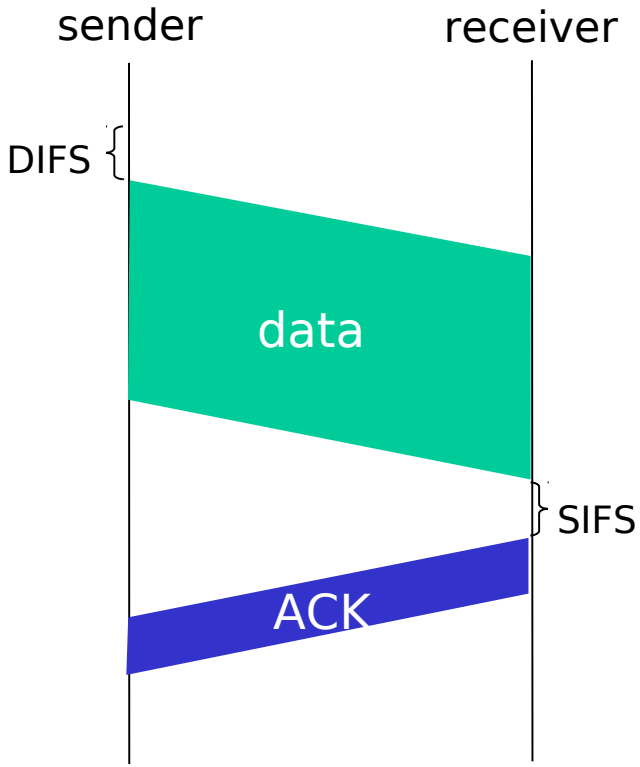
1. Have a frame to send
2. Wait a random time, until channel is idle
3. Sense it is idle for short time, called **DIFS** period
4. Sends frame, if gets through, destination waits a **SIFS** time and sends an **ACK**
5. Lack of an ACK back means frame failed
6. Sender then doubles backoff time, tries again
7. Continues until frame succeeds

Distributed Inter-frame Spacing (DIFS)
Short Inter-frame Spacing (SIFS)

# IEEE 802.11 MAC Protocol: CSMA/CA

## 802.11 sender

1. If sense channel idle for **DIFS** then
   transmit entire frame
2. If sense channel busy then
   a) start random backoff time
   b) timer counts down
   c) transmit when timer expires
   d) if no ACK, increase random backoff interval, repeat 2 (frame failed)




## 802.11 receiver

- if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)

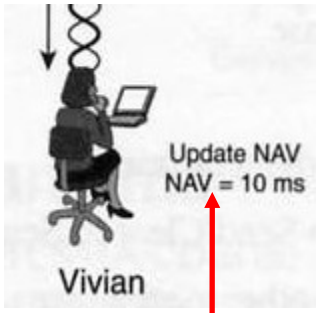
Distributed Inter-frame Spacing (DIFS)
Short Inter-frame Spacing (SIFS)

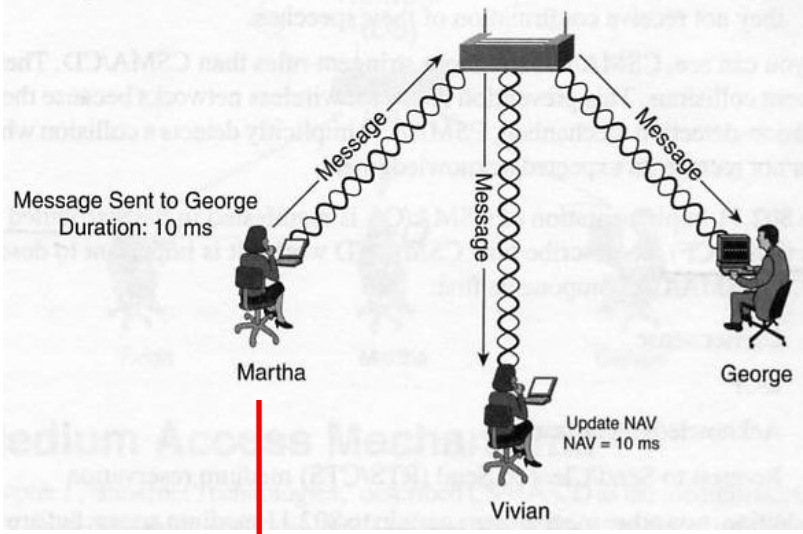
# 802.11 Frames have Timers

- Network Allocation Vector (NAV) timer
  - NAV is set when a frame sequence is sent
  - Says how long a sequence will take so other stations have an idea when the medium will be available
  - For example, a NAV for a data frame will also include the ACK back

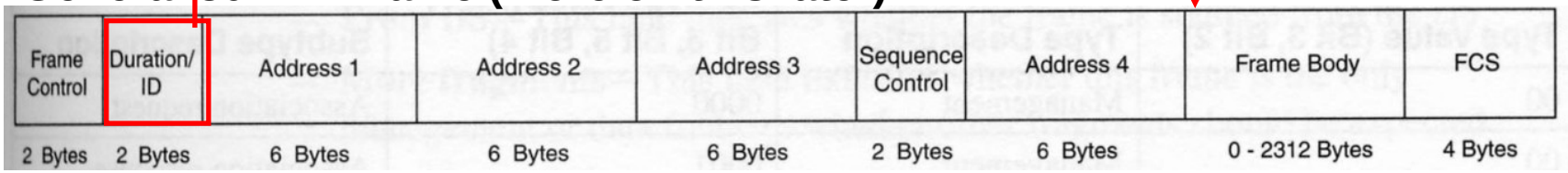
Next Slides Demo this with Example ...

# NAV Timer



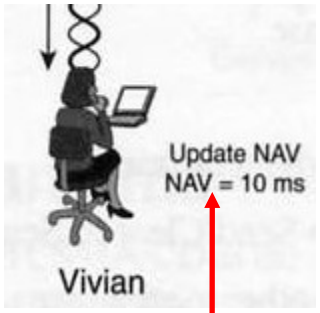



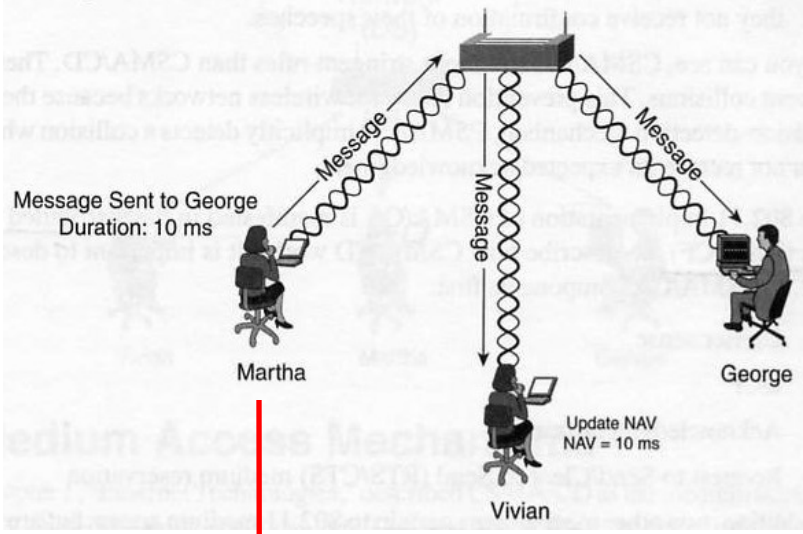

**General 802.11 Frame (more on this later)**




- All stations have a **NAV (Network Allocation Vector) timer**
  Protects frames from interruption
- Example: **Martha sends a frame to George**
- Since wireless medium is “broadcast-based” shared medium, all stations including Vivian receive frame
- Vivian updates her NAV timer with duration value
- Vivian will not attempt to transmit until her NAV is decremented to 0.
- Stations will only update their NAV when duration field value received is greater than their current NAV

# Duration Field



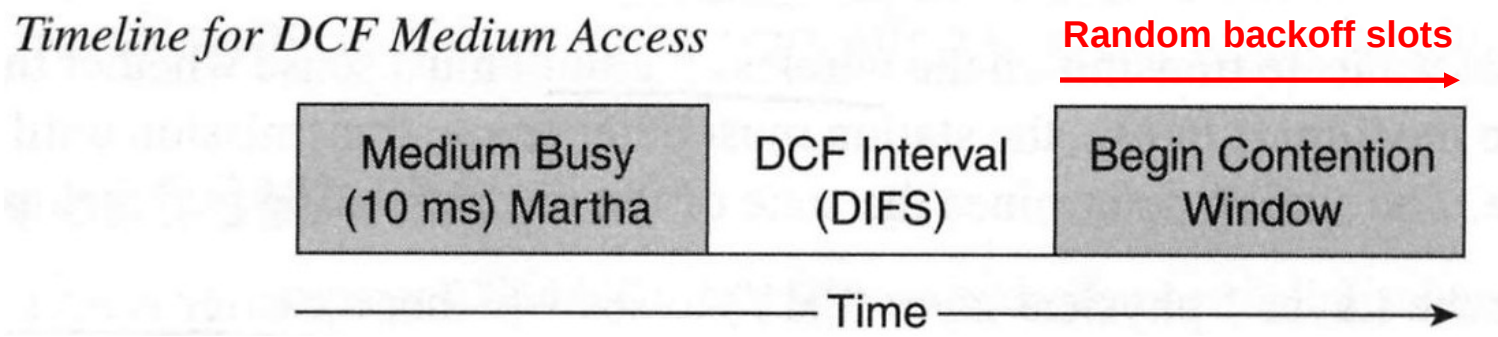

**General 802.11 Frame (more on this later)**

| Frame Control | Duration/ ID | Address 1 | Address 2 | Address 3 | Sequence Control | Address 4 | Frame Body | FCS |
|---|---|---|---|---|---|---|---|---|
| 2 Bytes | 2 Bytes | 6 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 6 Bytes | 0 - 2312 Bytes | 4 Bytes |

- **Duration/ID field** – Number of microseconds medium is expected to remain busy for transmission currently in progress
  - **Transmitting device sets Duration time in microseconds**
  - **Includes time to:**
    - **Transmit this frame to AP (or to the client if an AP)**
    - **Includes returning ACK**

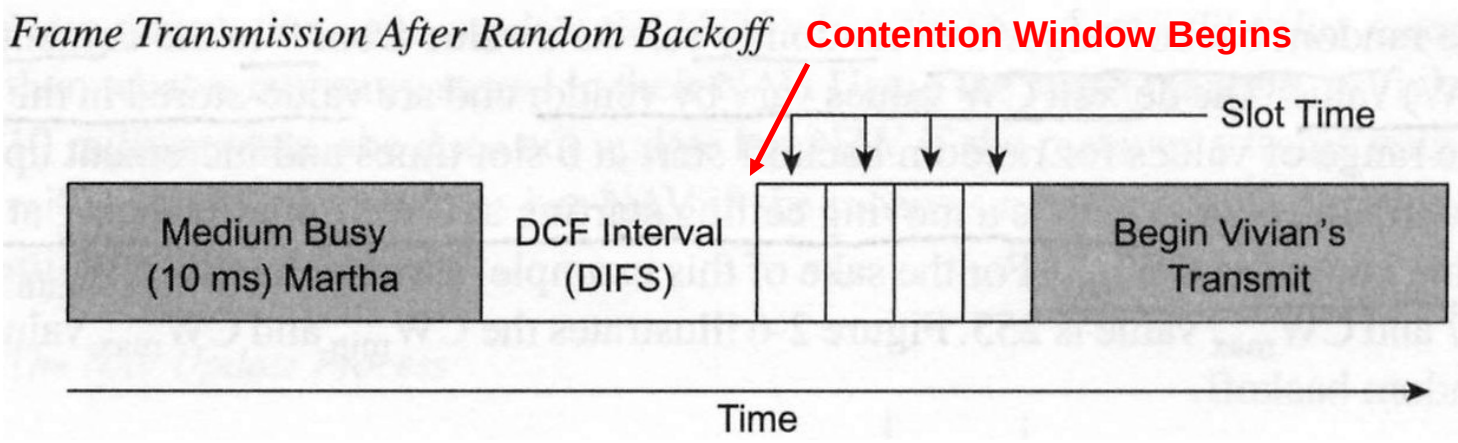
- All stations monitor this field!
- All stations update their **NAV** (Network Allocation Vector) timer

# Wanting to transmit (1/3)



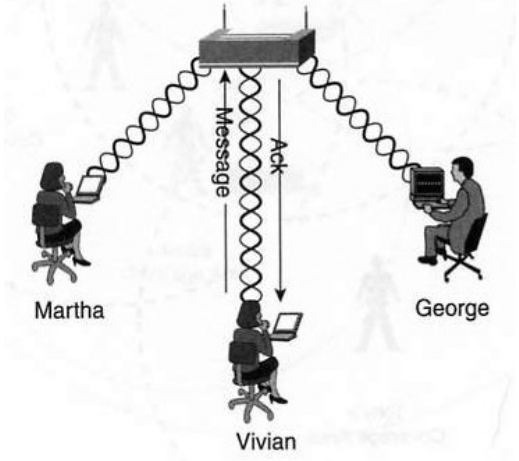

- Station wanting to transmit.
- **Carrier Sensing**
  - **Physical: Physically senses medium is idle**
  - **Virtual: NAV timer is 0**
- Waits **DIFS** (Distributed or DCF Interframe Space)
  - **Minimum amount of medium idle time until contention-based services begin.**
  - **Once DIFS is over, stations can contend for access.**
- **Contention window** begins.
  - **Uses random backoff algorithm to determine when it can attempt to access the medium. (next)**

# Wanting to transmit (2/3)




- The **random backoff algorithm** randomly selects a value from **0 to 255**
  Maximum value varies by vendor
- The random value is number of **802.11 slot times** the station must wait after the DIFS, during the contention window before it may transmit.
- **Stations pick a random slot** and wait for that slot before attempting to access the medium.
- With several stations attempting to transmit, the station that picks the **lowest slot, lowest random number, wins**.

# Wanting to transmit (3/3)





**Others update NAV**

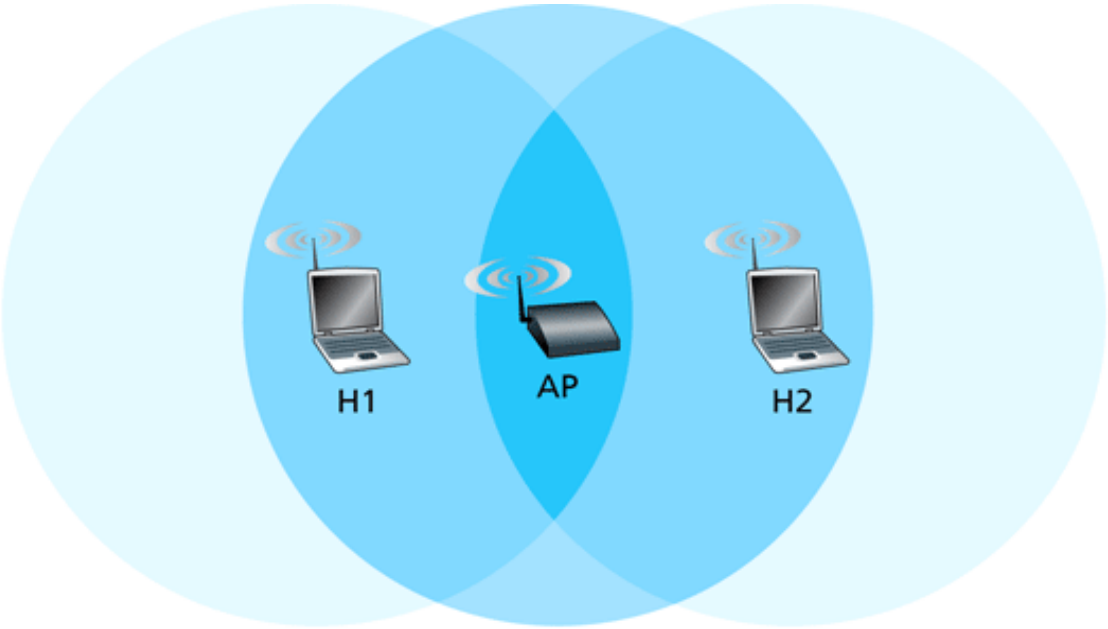
**General 802.11 Frame (more on this later)**

| Frame Control | Duration/ ID | Address 1 | Address 2 | Address 3 | Sequence Control | Address 4 | Frame Body | FCS |
|---|---|---|---|---|---|---|---|---|
| 2 Bytes | 2 Bytes | 6 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 6 Bytes | 0 - 2312 Bytes | 4 Bytes |

- **Station transmits**, setting the **Duration ID** to the time needed to transmit data, ACK and IFSs.
- **Other stations** with higher slots will see the new transmission and wait to transmit.
- If **frame arrives at AP** (assuming the transmitter is a station), then an **ACK will be returned**
- If there is **not an ACK received**, the sending station assumes there has been a collision
  - **If two stations have the same lowest slot time and both transmit, then a collision occurs**
- Stations will **update its retry counter** (double) to determine a **new randomly selected slot time** and **process starts all over again**

# Hidden Terminal Problem in WLANs

- Both H1 and H2 transmit at same time
- Signals collide at AP, H1 can't detect H2




Collison is the darker blue

**Figure 6.11** ♦ Hidden terminal example: H1 is hidden from H2, and vice versa.

# Avoiding collisions: RTS/CTS

*Another Idea:* Allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

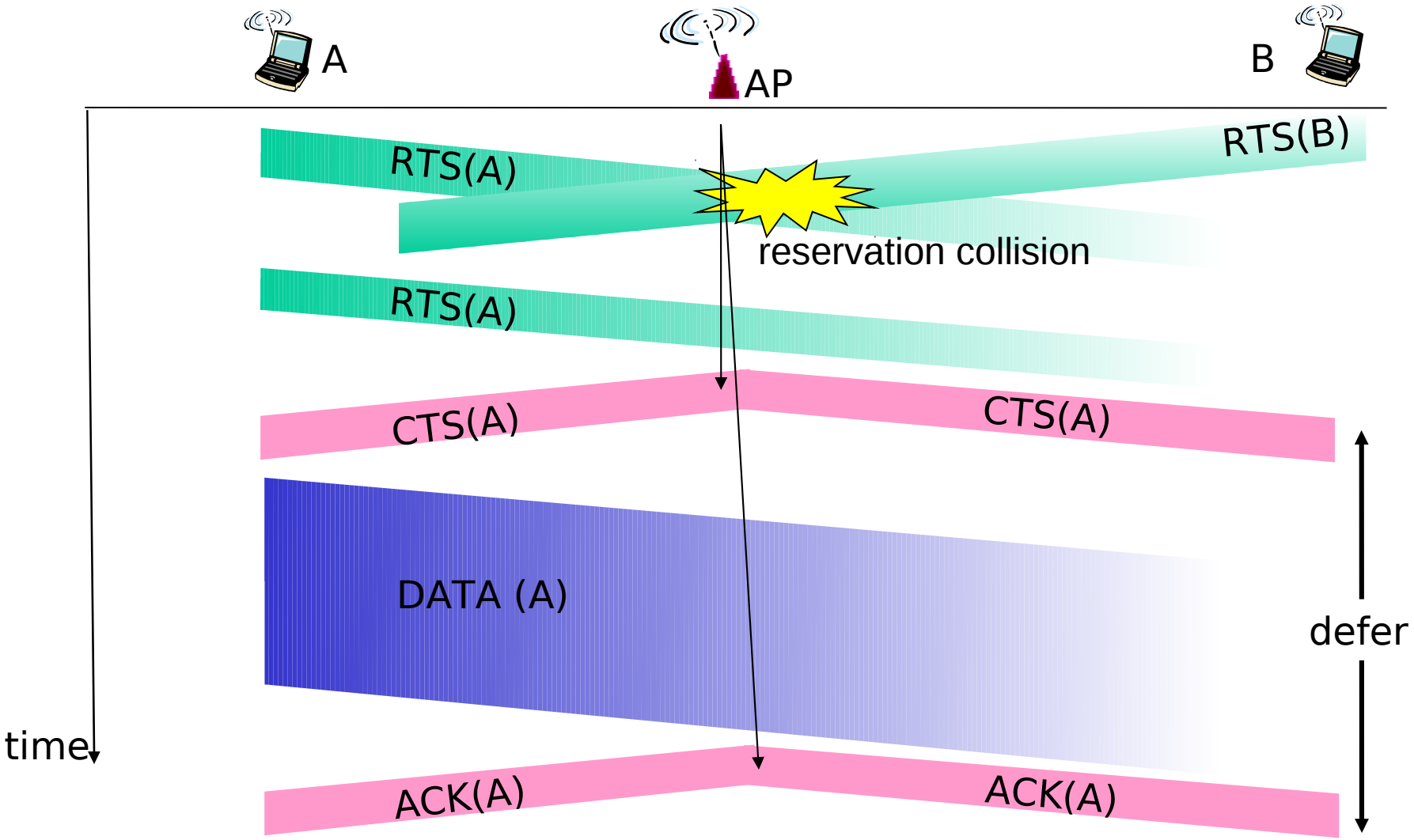
Sender first transmits *small* request-to-send (RTS) packets using CSMA, say want to transmit to AP

- RTSs may still collide with each other (but they're short)

- AP broadcasts clear-to-send (CTS) in response to RTS
- RTS heard by all nodes
  - Sender transmits data frame
  - Other stations defer transmissions

Avoids data frame collisions completely using small reservation packets!

# Collision Avoidance: RTS-CTS exchange



# RTS/CTS in practice

- 802.11 standardized both CSMA/CA and RTS/CTS
- In practice, most operators disable RTS/CTS
  - Very high overhead!
    - RTS/CTS packets sent at “base rate” (often 1Mbit)
  - Neighboring AP's are often configured to use non-overlapping channels, so hidden terminals on downlink are rare


# MAC Addresses

# Review

# MAC Addresses

## Network Layer

32-bit IP address

Network-layer address, dotted decimal

Ex.: 146.187.130.76

To route datagram to destination machine, router uses

## MAC (or LAN or physical or Ethernet) Address

MAC stands for Media Access Control

48 bit MAC address (for most LANs)

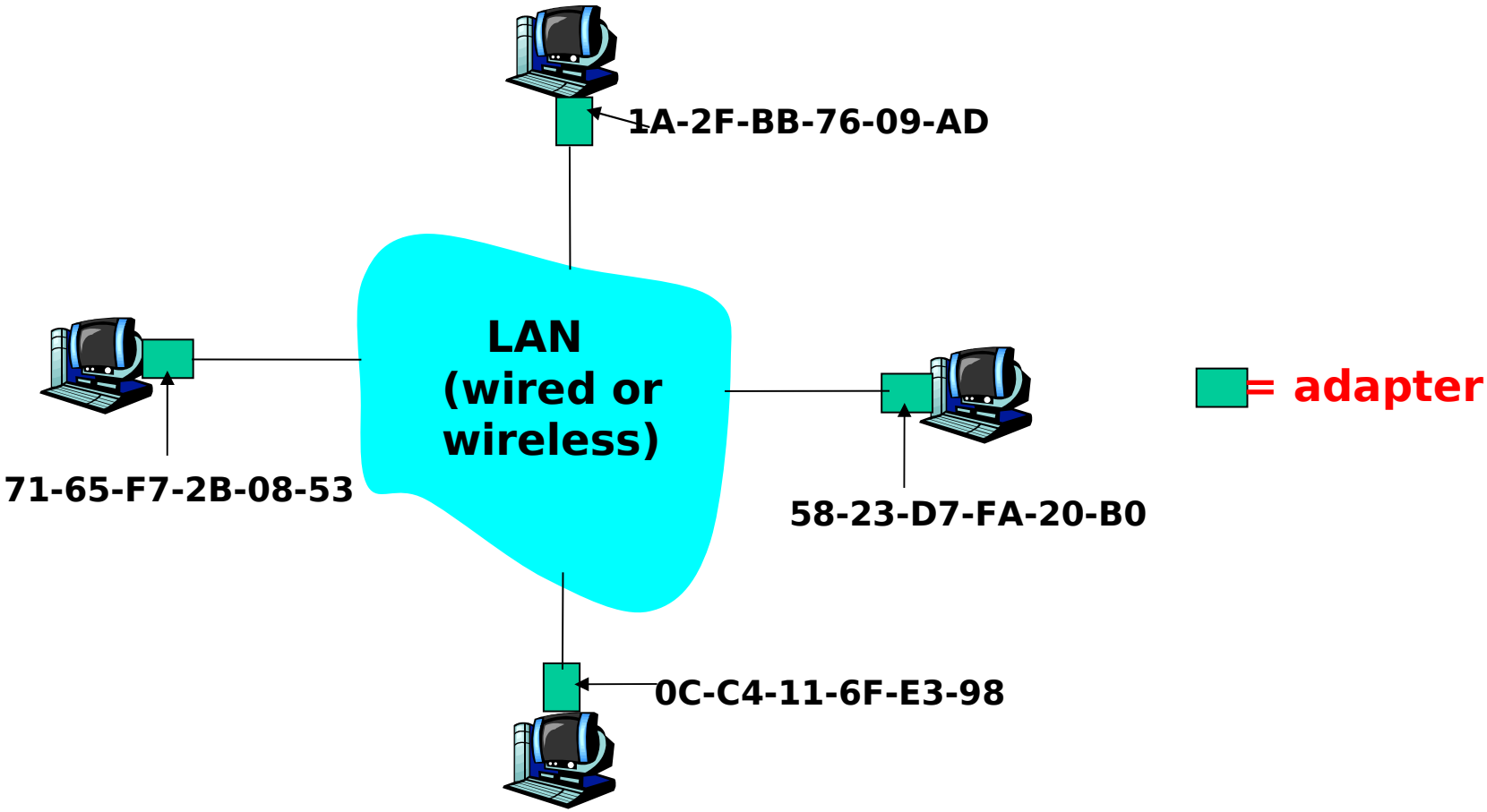
Burned in NIC ROM, also sometimes software settable

24 bits set for manufacturer, 24 bits for NIC adapter

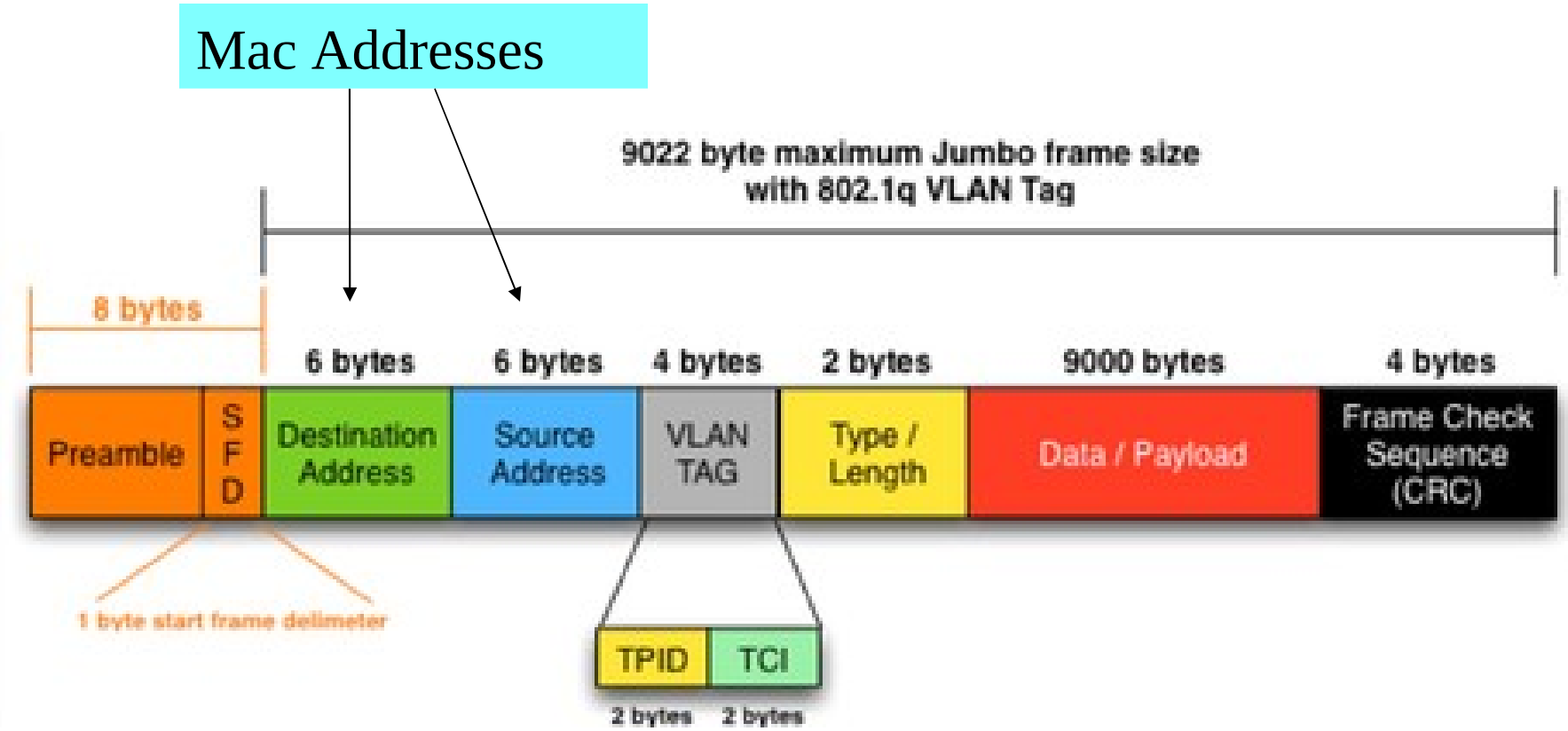
Ex.: 00:E0:B8:9C:A6:60

# MAC Addresses

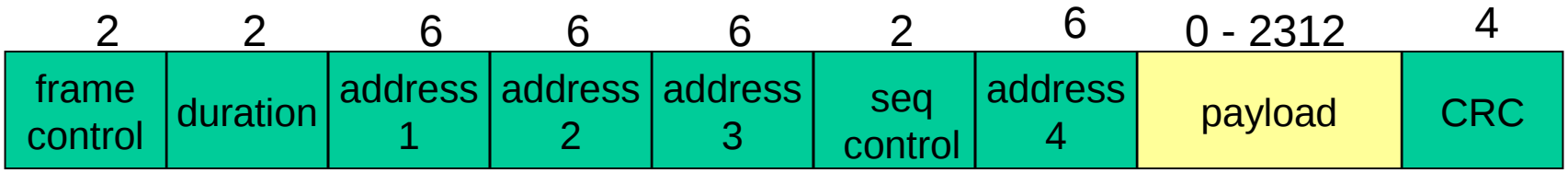
**Each adapter on LAN has unique MAC address except for Broadcast address which is FF-FF-FF-FF-FF-FF**



# Ethernet Frame



# 802.11 Frame: Addressing



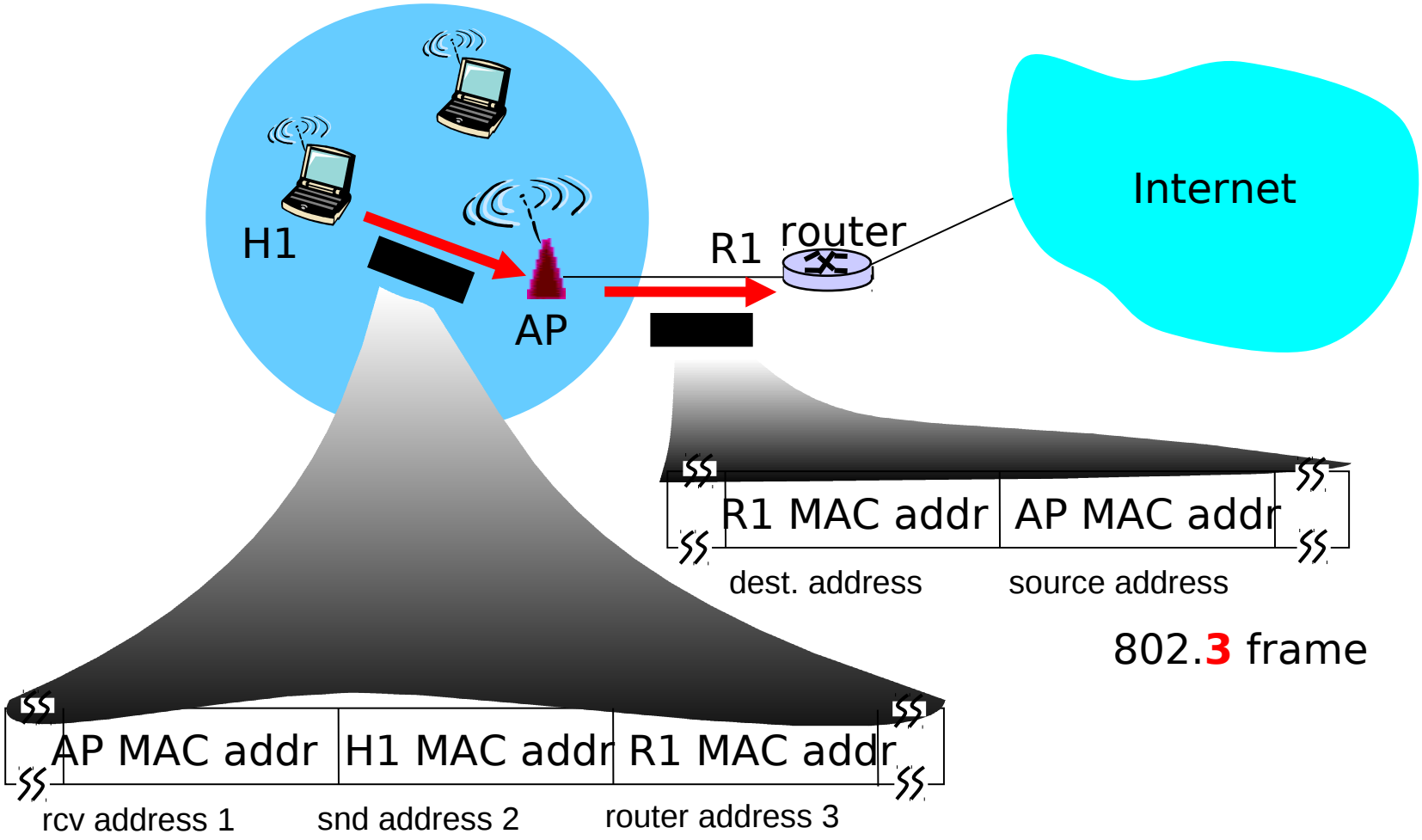

Address 1: MAC address of wireless host or AP to receive this frame

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

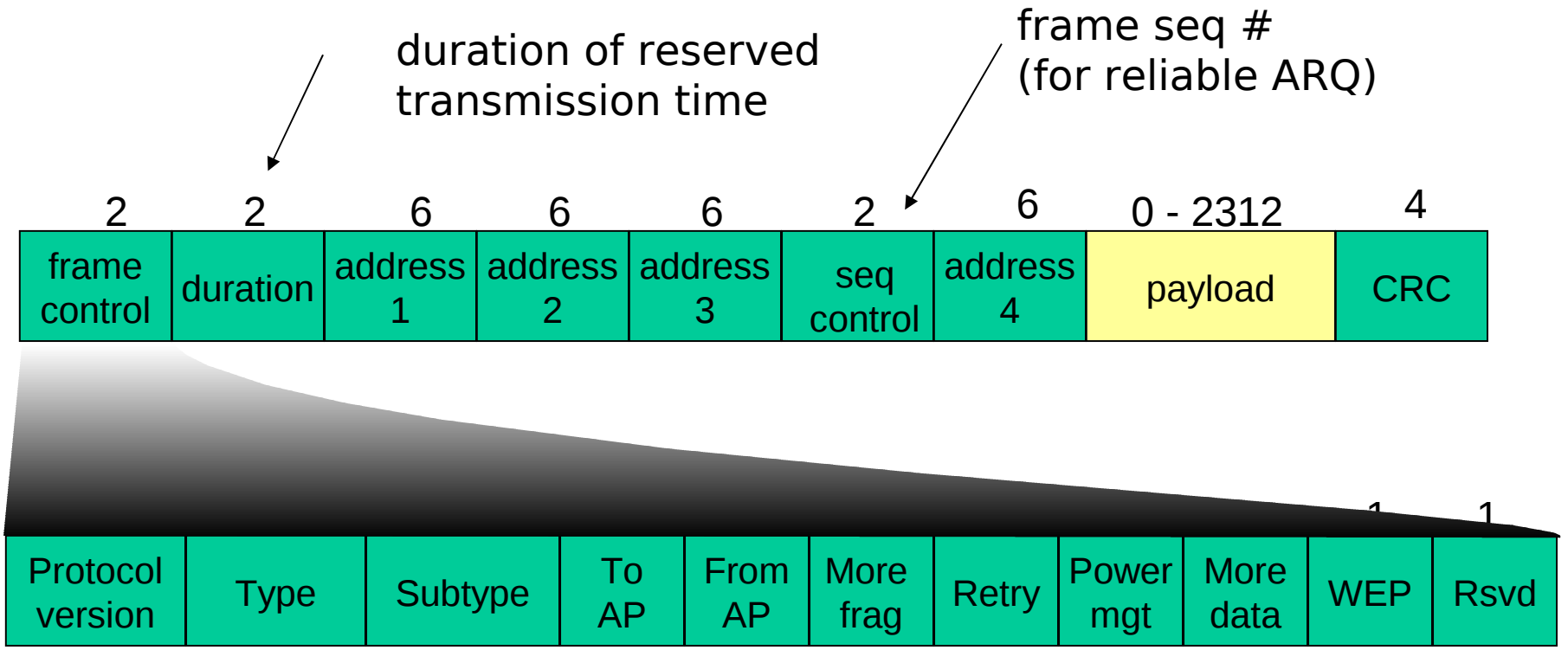
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

# 802.11 frame: addressing



# 802.11 frame: more



| 2 bits | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Protocol Version | Type | Subtype | To DS | From DS | More Fragments | Retry | Power Mgt. | More data | WEP | Order |

# Protocol Version provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.

# Type and Subtype determines the function of the frame.
There are three different frame type fields:
**control, data, and management.**

# **To DS and From DS** indicates whether the frame is going to or exiting from the DS
This affects the order of the address fields see below ….

**To DS field is 1 and From DS field is 0**

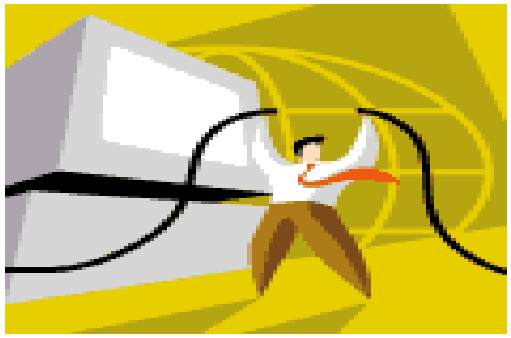
Address 1 = BSSID
Address 2 = Source
Address 3 = Destination

**To DS field is 0 and From DS field is 1**

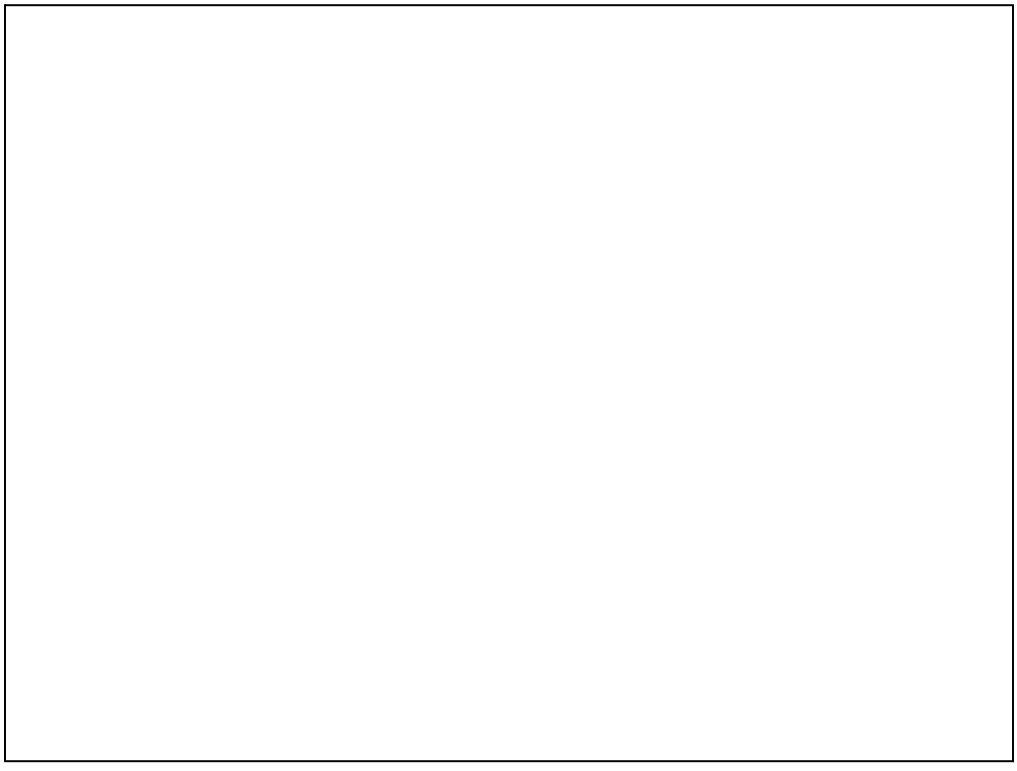
Address 1 = Destination
Address 2 = BSSID
Address 3 = Source

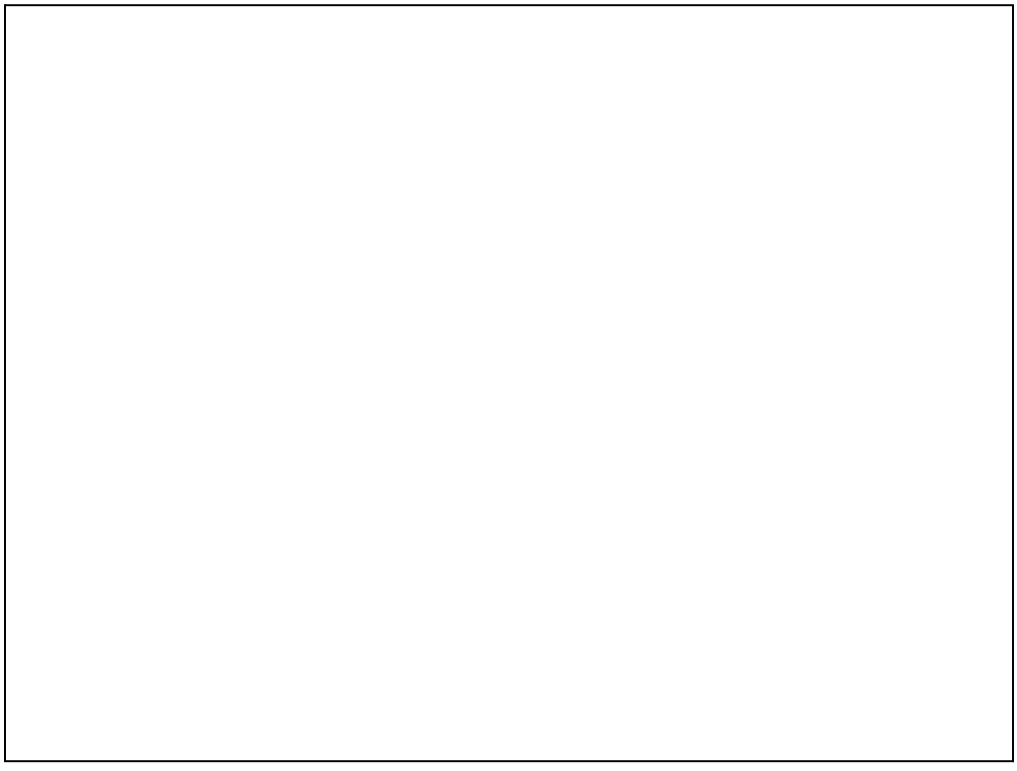
# Summary

- 802.11 wireless more challenging because of disruptions to signal vs. wired
- However, mobility far outweighs the downside of interference and security
- No going back to wired when we can plug in during flights and have access to Facebook!
- Will see how wireless works in Wireshark lab



The End





# IEEE Standards


- In 1985, Computer Society of IEEE started a project, called Project 802,
- Set standards to enable intercommunication among equipment from a variety of manufacturers … wonderful!!!
- Project 802
  - Specifies functions of physical layer and the data link layer of major LAN protocols

# IEEE 802 Series of LAN Standards

802 standards free to download from http://standards.ieee.org/getieee802

IEEE 802®: Overview & Architecture

IEEE 802.1 ™ Bridging & Management

IEEE 802.2 ™: Logical Link Control

IEEE 802.3 ™: CSMA/CD Access Method

IEEE 802.4 ™: Token-Passing Bus Access Method

IEEE 802.5 ™: Token Ring Access Method

IEEE 802.6 ™: DQDB Access Method

IEEE 802.7 ™: Broadband LAN

IEEE 802.10 ™: Security

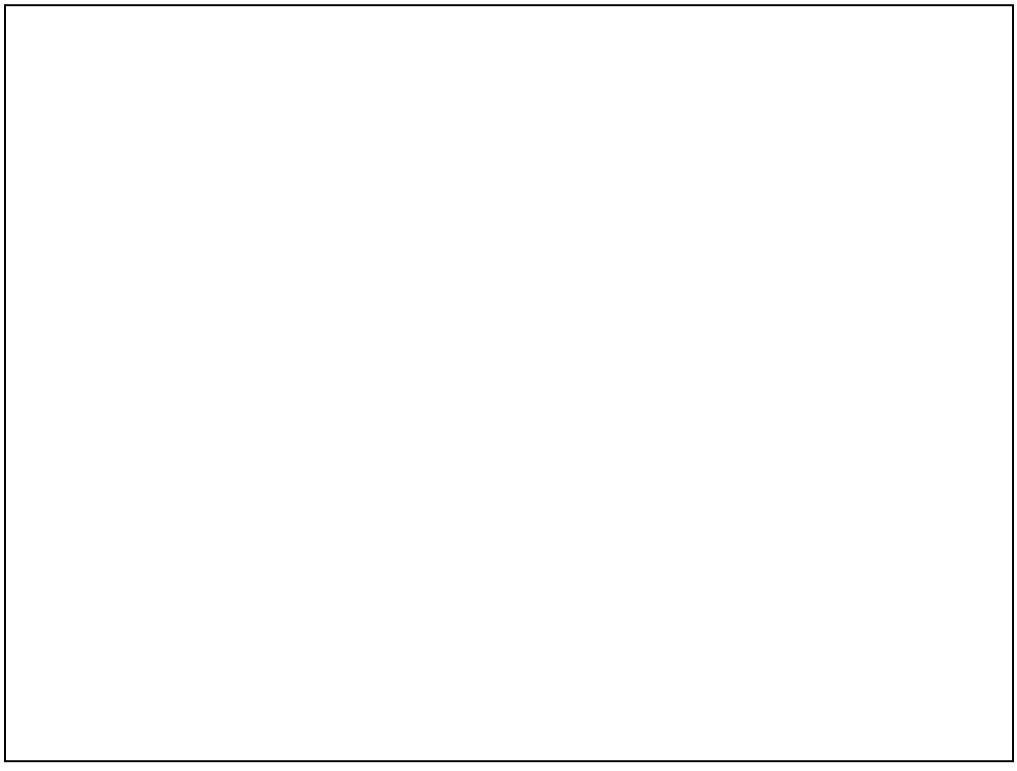
IEEE 802.11 ™: Wireless

IEEE 802.12 ™: Demand Priority Access

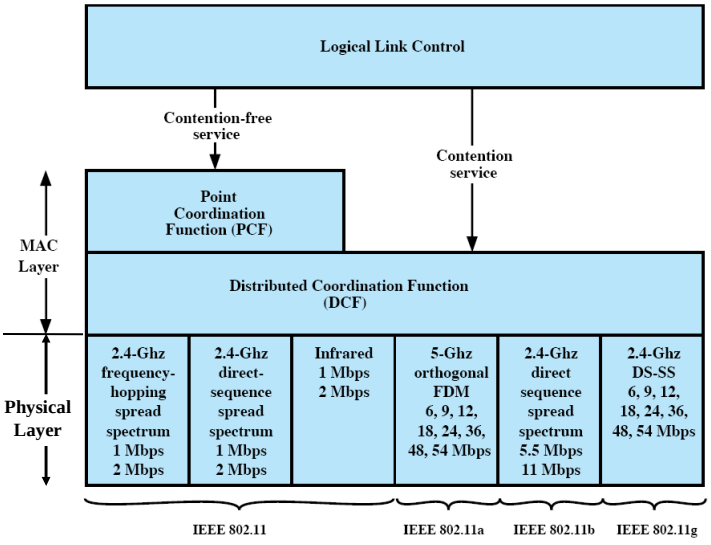
WiMAX IEEE 802.16™: Broadband Wireless Metropolitan Area Networks

# 802.11 Physical Layer

- Issued in four stages
- **1997, First part**
  - IEEE 802.11
  - Includes MAC layer and three physical layer specifications
  - Two in 2.4-GHz band and one infrared, Operate 1 and 2 Mbps
- **1999, Two more parts**
  - IEEE 802.11a
    - 5-GHz band, data rate up to 54 Mbps
  - IEEE 802.11b
    - 2.4-GHz band, data rate at 5.5 and 11 Mbps
- **2002, Most recent**
  - IEEE 802.11g extended IEEE 802.11b to higher data rates, up to 54 Mbps
- **At present**
  - IEEE 802.11n and 802.11ac data rate up to hundreds of Mbps

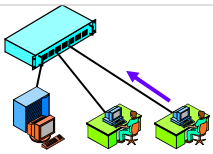


# IEEE 802.11 Protocol Architecture




7

# 802 Layering

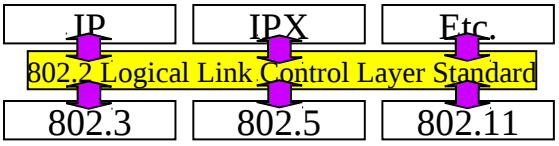


## Media Access Control (MAC) Layer

- 802.11 standard specifies common medium access control (MAC) Layer
- In general, MAC Layer manages and maintains communications between 802.11 stations by coordinating access to shared radio channel, has most of functionality

## Logical Link Control (LLC) Layer

Adds optional error correction (rarely used)
Connects to next-higher-layer (internet), multiplexes higher level protocols



# Medium Access Control

- Two sublayers

**Lower sublayer**

**Distributed Coordination Function** (DCF)

- Uses a contention algorithm to provide access to all traffic
- Uses CSMA/CA – Carrier Sense Multiple Access/Collison Avoidance

**Higher sublayer**

**Point Coordination Function** (PCF)

- Uses a centralized algorithm
- "Contention free"
- Implemented on top of DCF

- **Note:** PCF has not been popularly implemented in today's 802.11 products, DCF is widely used

# MAC Sublayer Functions

- MAC is set of rules to determine how to access medium and data link components.

  It provides core framing operations, sets the frame header fields

- MAC purpose in General
  - Coordinates and shares use of radio bandwidth
  - Synchronization between stations
  - Datagram transfer function
  - **MAC layer management functions**

    Authentication and De-Authentication
    Association, Re-Association, and Disassociation
    Beacon and Probe frames

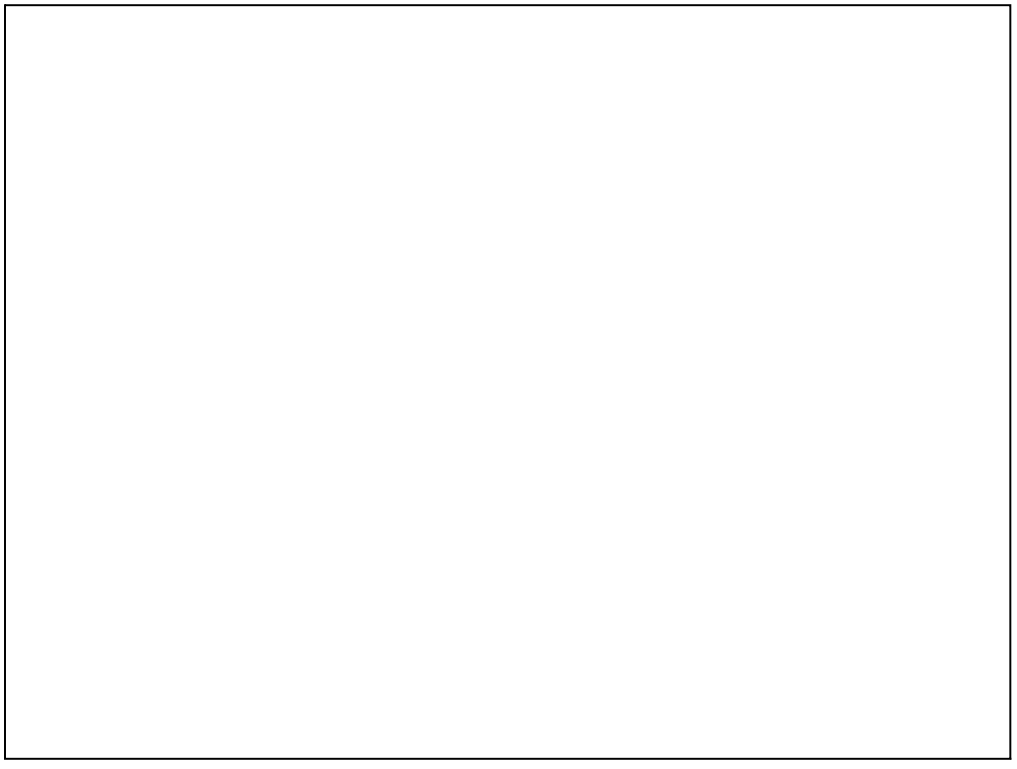
# MAC Sublayer Functions

- 802.11 uses CSMA/CA mechanism

  **Carrier Sense Multiple Access with Collision Avoidance**

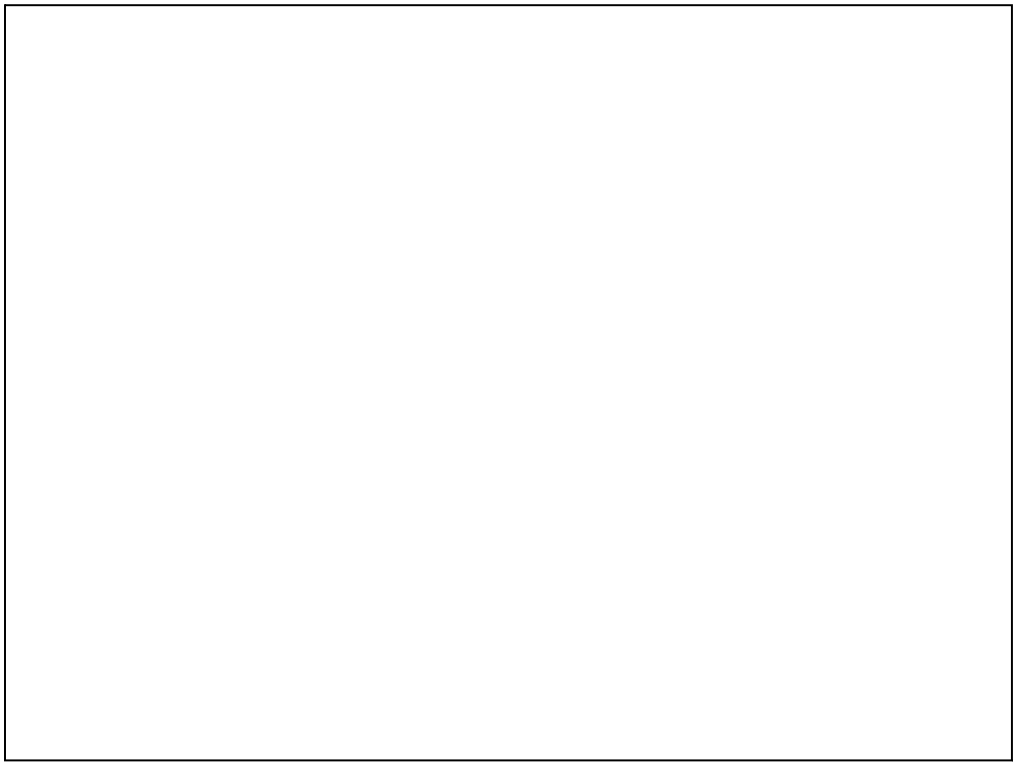
  - It is considered to be ‘fair’ for all users because treats them equally

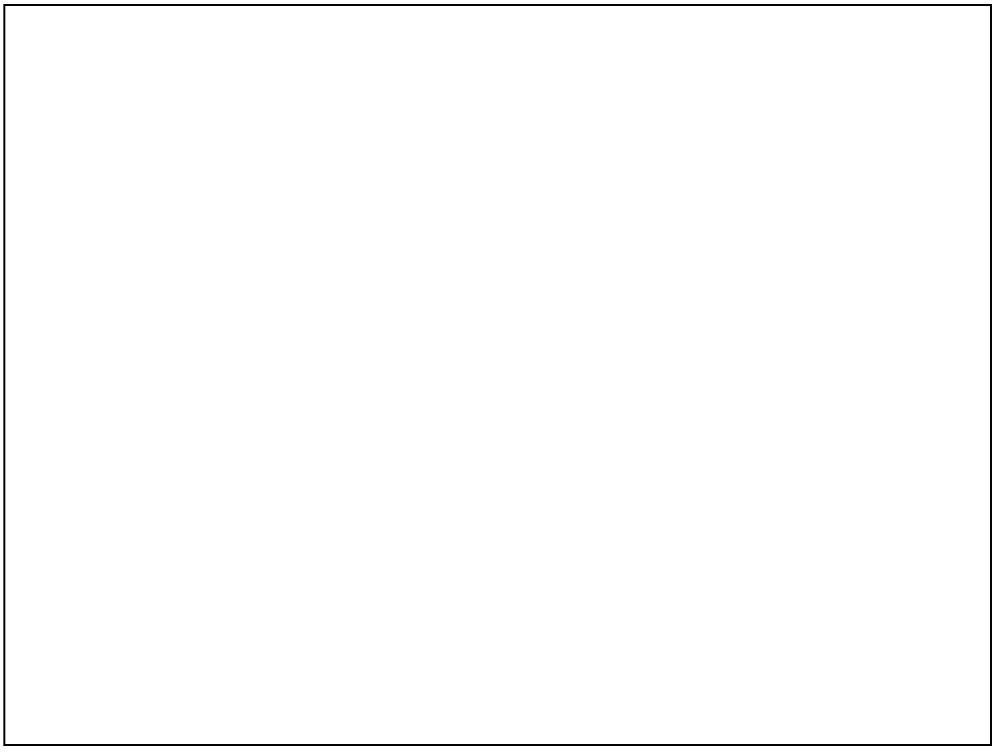
Recall that Ethernet uses CSMA/CD ….

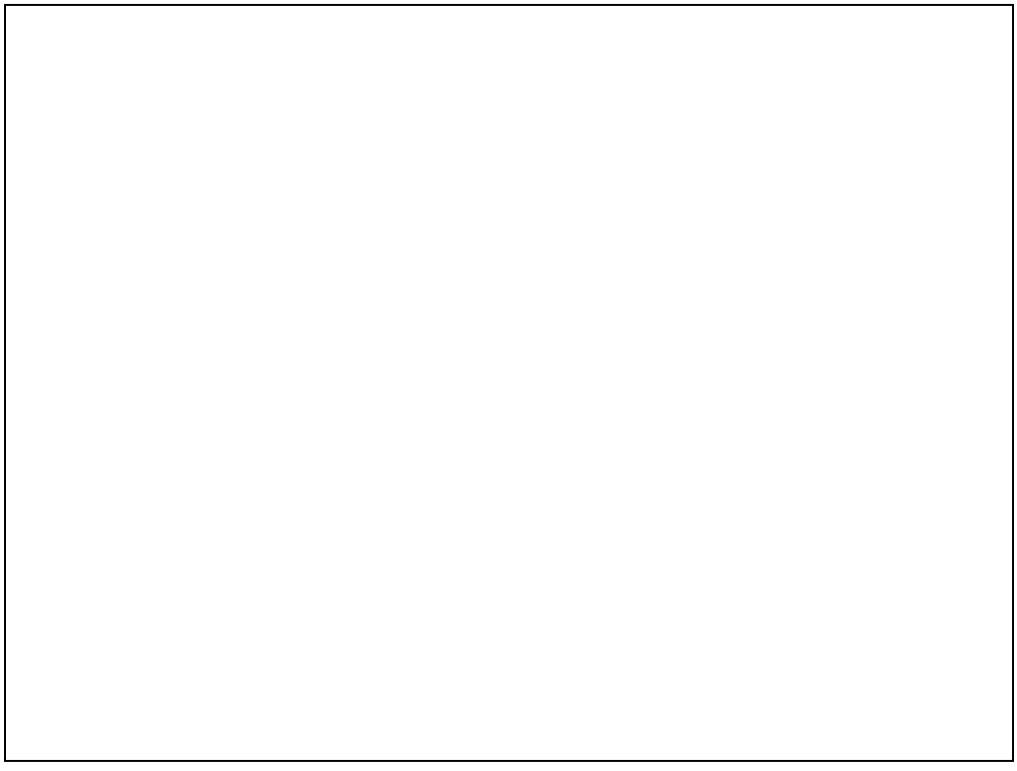


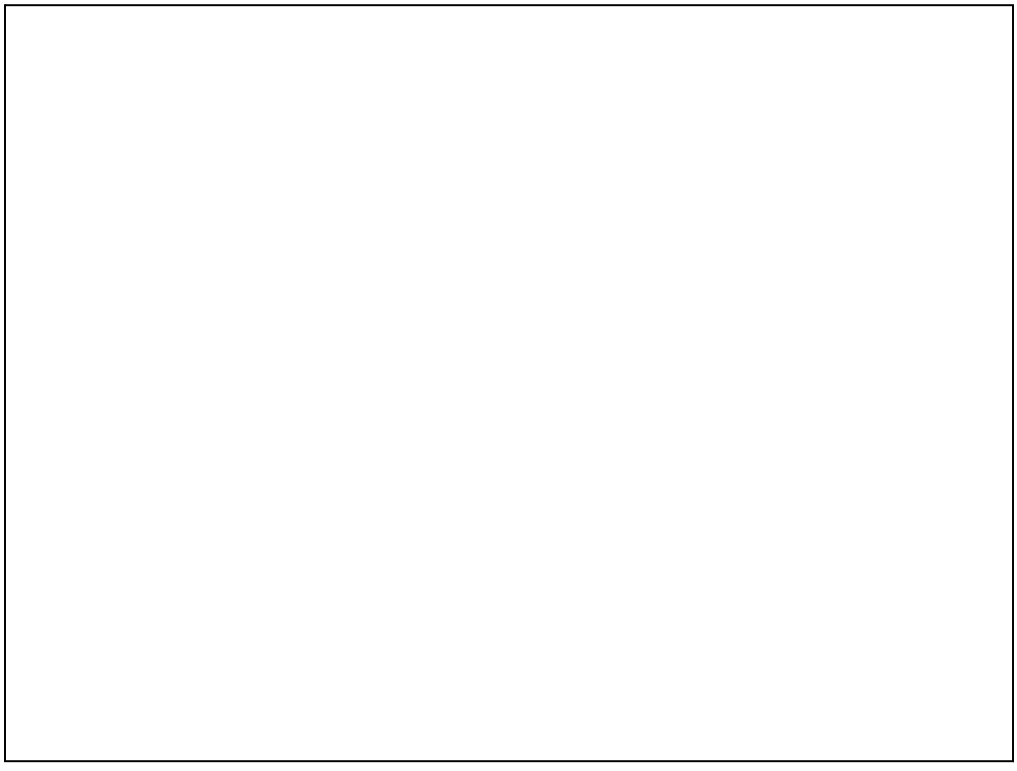
# Review of Classical Ethernet

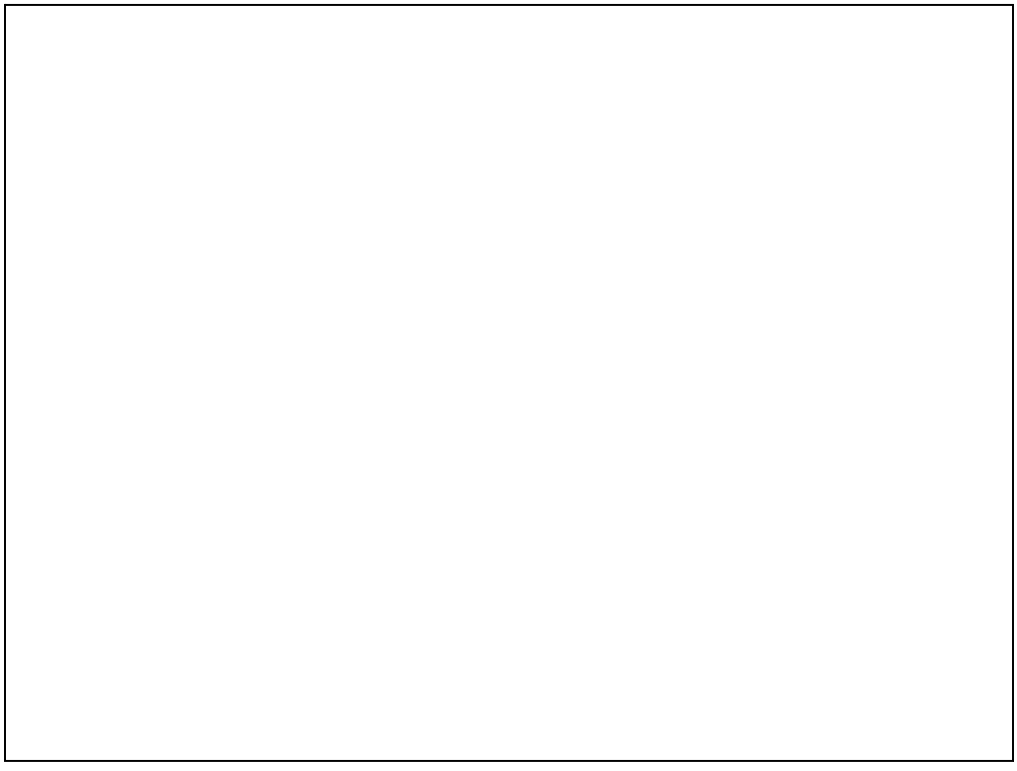
- Recall that classical Ethernet is shared technology
- Everyone has access to wires
- Users contend with collisions and MAC layer protocol dealt with these collisions
  - Note – This is with traditional cable and Hubs
- Review characteristics of Ethernet











## Wireless Communication Systems

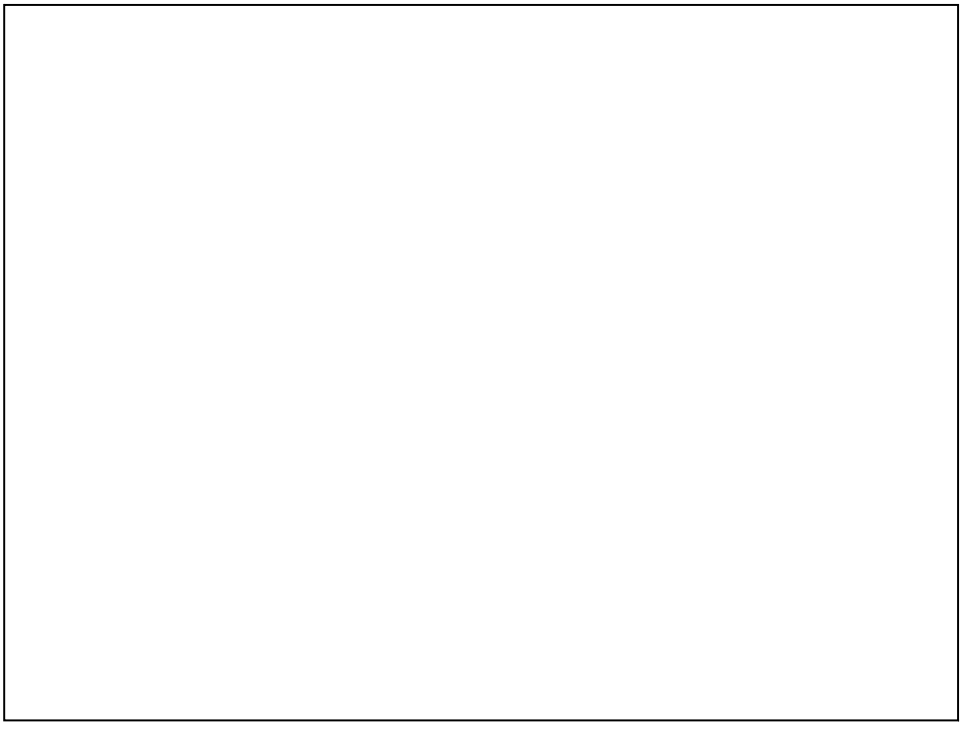
- In terms of packet or frame delivery ….
- What complicates wireless networking vs. wired networking?

# Wireless Link Characteristics


## Differences from wired link ….

- Decreased signal strength: Radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: Standardized wireless network frequencies shared by other devices that can interfere
- Multipath propagation: Radio signal reflects off objects and ground, arriving at destination at slightly different times

…. make communication across link much more "difficult"



DIFS= Distributed interframe Space

PIFS=Point Coordination Interframe Space

SIFS=Short Coordination Interframe Space

# 802.11 Medium Access Control

- Shares the medium through coordination with other stations
  1. Sends control packets for coordination
     Including Acks
  2. Sets and sends individual frame timers for all to see, each frame has its own timer

- Note: There is the 802.11 standard and then there is reality of did it actually get implemented!
  - Create a lot of details for a standard but not all of it is implemented

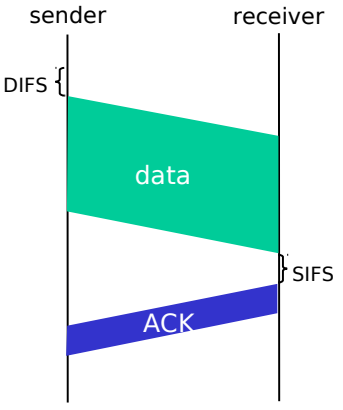
# Wireless Collision Avoidance

STEPS

1. Have a frame to send
2. Wait a random time, until channel is idle
3. Sense it is idle for short time, called **DIFS** period
4. Sends frame, if gets through, destination waits a **SIFS** time and sends an **ACK**
5. Lack of an ACK back means frame failed
6. Sender then doubles backoff time, tries again
7. Continues until frame succeeds

Distributed Inter-frame Spacing (DIFS)
Short Inter-frame Spacing (SIFS)

# IEEE 802.11 MAC Protocol: CSMA/CA




Distributed Inter-frame Spacing (DIFS)
Short Inter-frame Spacing (SIFS)

802.11 sender

1. If sense channel idle for **DIFS** then
   transmit entire frame
2. If sense channel busy then
   a) start random backoff time
   b) timer counts down
   c) transmit when timer expires
   d) if no ACK, increase random backoff interval, repeat 2 (frame failed)

802.11 receiver

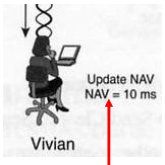
- if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)

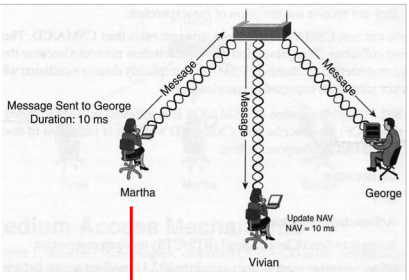
# 802.11 Frames have Timers

- Network Allocation Vector (NAV) timer
  - NAV is set when a frame sequence is sent
  - Says how long a sequence will take so other stations have an idea when the medium will be available
  - For example, a NAV for a data frame will also include the ACK back

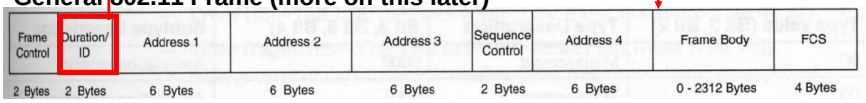
Next Slides Demo this with Example ...

# NAV Timer



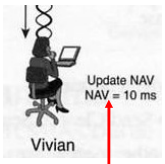



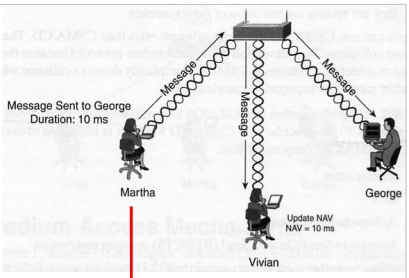

**General 802.11 Frame (more on this later)**



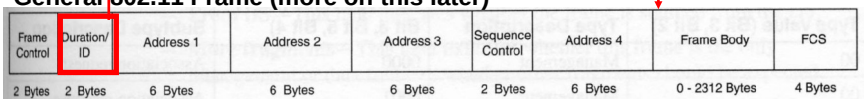

- All stations have a **NAV (Network Allocation Vector) timer**
  Protects frames from interruption
- Example: **Martha sends a frame to George**
- Since wireless medium is “broadcast-based” shared medium, all stations including Vivian receive frame
- Vivian updates her NAV timer with duration value
- Vivian will not attempt to transmit until her NAV is decremented to 0.
- Stations will only update their NAV when duration field value received is greater than their current NAV

# Duration Field



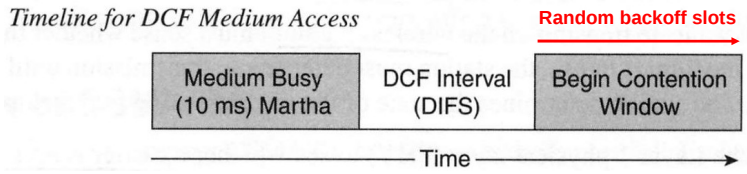

**General 802.11 Frame (more on this later)**




- **Duration/ID field** – Number of microseconds medium is expected to remain busy for transmission currently in progress
  - **Transmitting device sets Duration time in microseconds**
  - **Includes time to:**
    - **Transmit this frame to AP (or to the client if an AP)**
    - **Includes returning ACK**

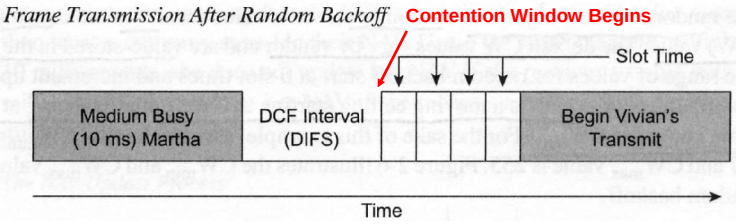
- All stations monitor this field!
- All stations update their **NAV** (Network Allocation Vector) timer

# Wanting to transmit (1/3)



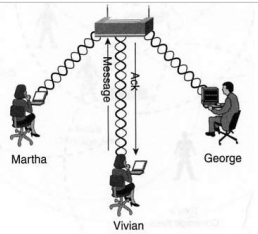

- Station wanting to transmit.
- **Carrier Sensing**
  - **Physical: Physically senses medium is idle**
  - **Virtual: NAV timer is 0**
- Waits **DIFS** (Distributed or DCF Interframe Space)
  - **Minimum amount of medium idle time until contention-based services begin.**
  - **Once DIFS is over, stations can contend for access.**
- **Contention window** begins.
  - **Uses random backoff algorithm to determine when it can attempt to access the medium. (next)**

# Wanting to transmit (2/3)




- The **random backoff algorithm** randomly selects a value from **0 to 255** Maximum value varies by vendor
- The random value is number of **802.11 slot times** the station must wait after the DIFS, during the contention window before it may transmit.
- **Stations pick a random slot** and wait for that slot before attempting to access the medium.
- With several stations attempting to transmit, the station that picks the **lowest slot, lowest random number, wins**.

# Wanting to transmit (3/3)

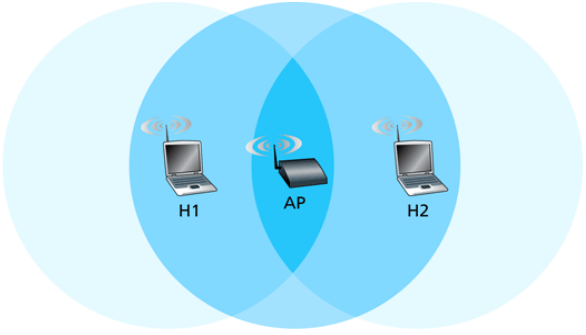

**General 802.11 Frame (more on this later)**

| Frame Control | Duration/ ID | Address 1 | Address 2 | Address 3 | Sequence Control | Address 4 | Frame Body | FCS |
|---|---|---|---|---|---|---|---|---|
| 2 Bytes | 2 Bytes | 6 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 6 Bytes | 0 - 2312 Bytes | 4 Bytes |

- **Station transmits**, setting the **Duration ID** to the time needed to transmit data, ACK and IFSs.
- **Other stations** with higher slots will see the new transmission and wait to transmit.
- If **frame arrives at AP** (assuming the transmitter is a station), then an **ACK will be returned**
- If there is **not an ACK received**, the sending station assumes there has been a collision
  - **If two stations have the same lowest slot time and both transmit, then a collision occurs**
- Stations will **update its retry counter** (double) to determine a **new randomly selected slot time** and **process starts all over again**

# Hidden Terminal Problem in WLANs

- Both H1 and H2 transmit at same time
- Signals collide at AP, H1 can't detect H2




Collison is the darker blue

**Figure 6.11** ♦ Hidden terminal example: H1 is hidden from H2, and vice versa.

# Avoiding collisions: RTS/CTS

*Another Idea:* Allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

Sender first transmits *small* request-to-send (RTS) packets using CSMA, say want to transmit to AP
- RTSs may still collide with each other (but they're short)

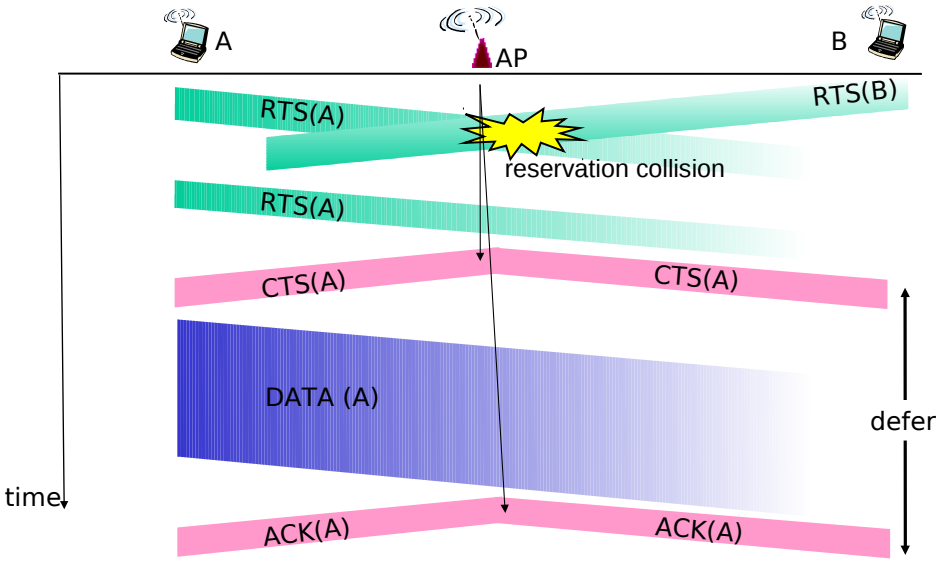
- AP broadcasts clear-to-send (CTS) in response to RTS
- RTS heard by all nodes
  - Sender transmits data frame
  - Other stations defer transmissions

Avoids data frame collisions completely using small reservation packets!



32

# Collision Avoidance: RTS-CTS exchange



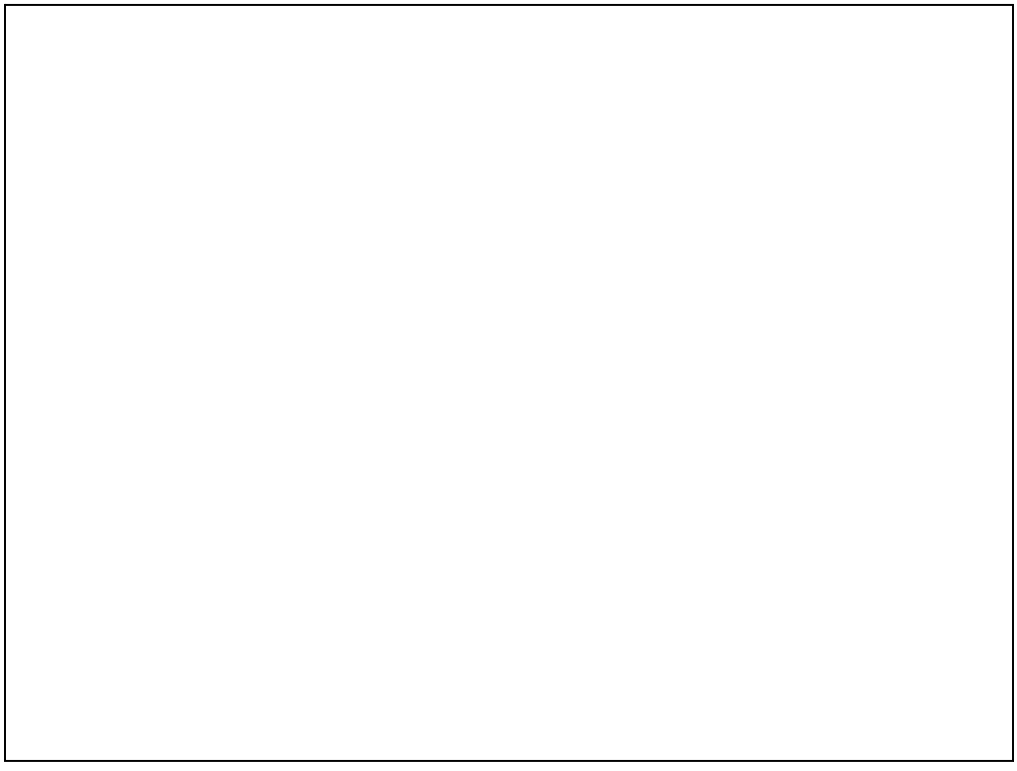

33

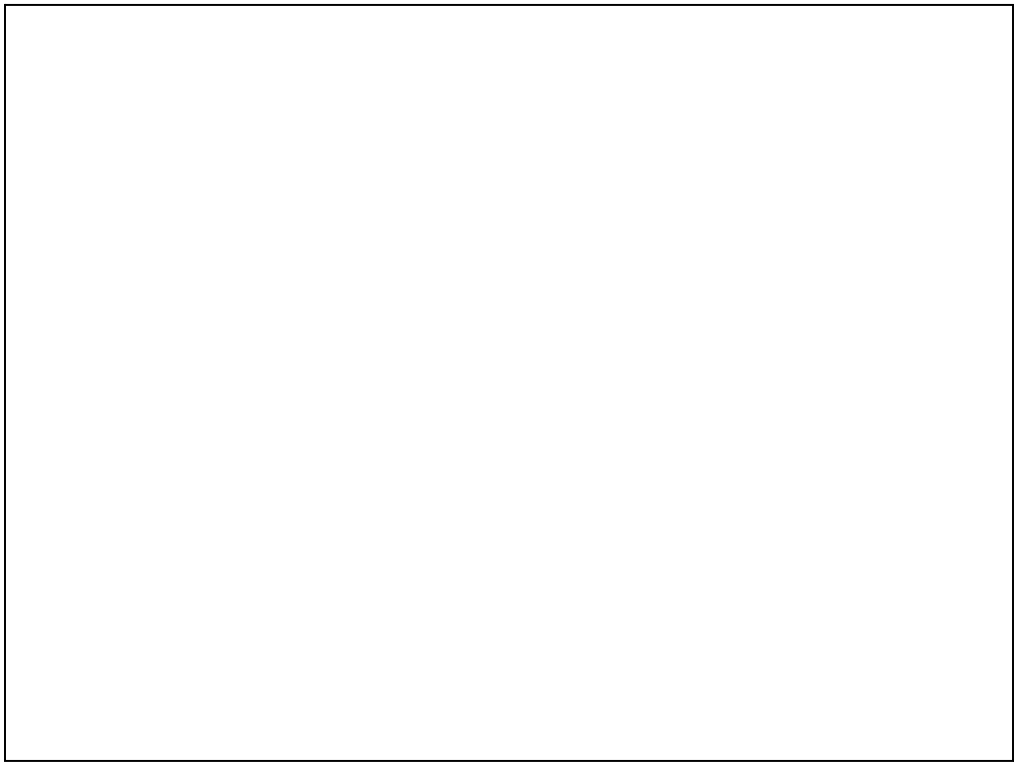
# RTS/CTS in practice

- 802.11 standardized both CSMA/CA and RTS/CTS
- In practice, most operators disable RTS/CTS
  - Very high overhead!
    - RTS/CTS packets sent at “base rate” (often 1Mbit)
  - Neighboring AP's are often configured to use non-overlapping channels, so hidden terminals on downlink are rare

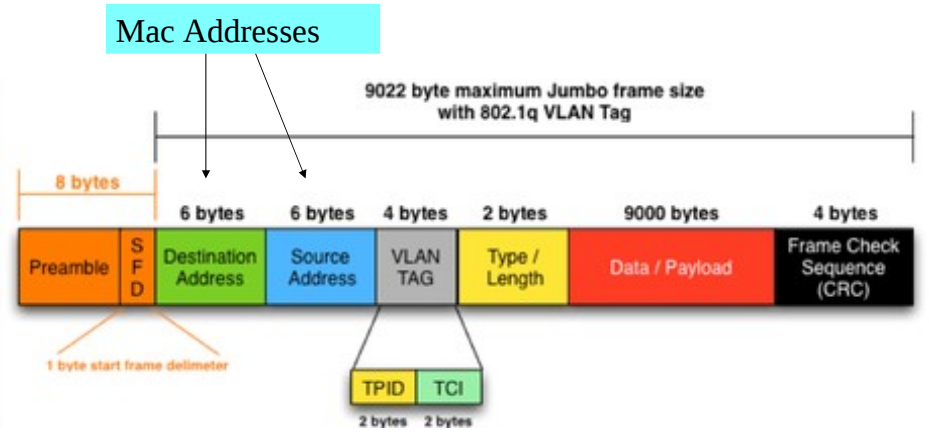

MAC Addresses

Review

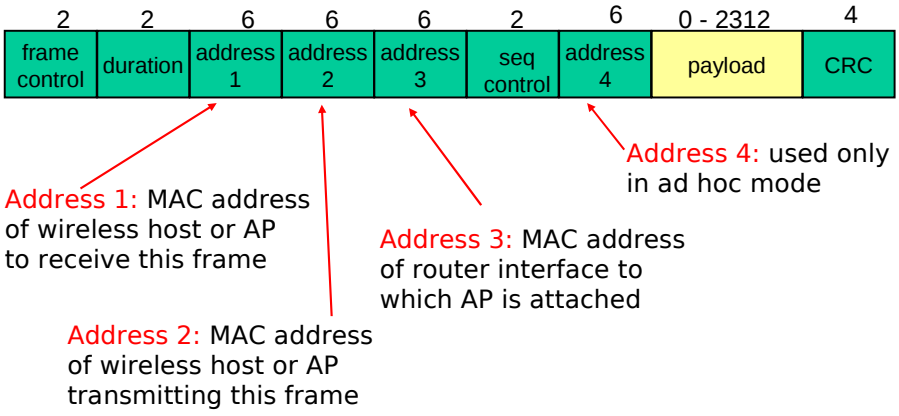




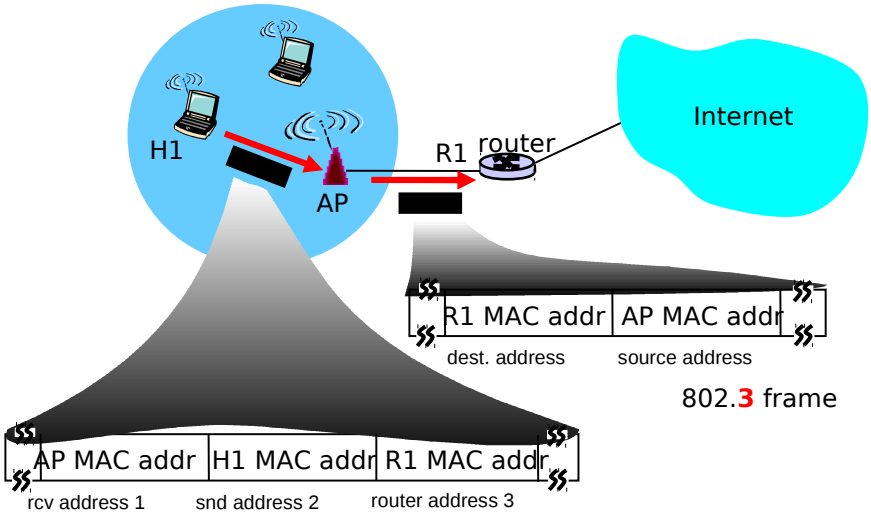
# Ethernet Frame



# 802.11 Frame: Addressing



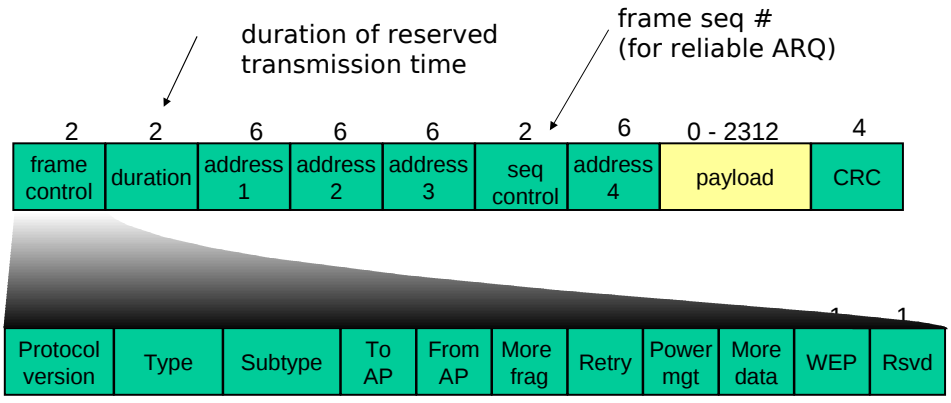
# 802.11 frame: addressing





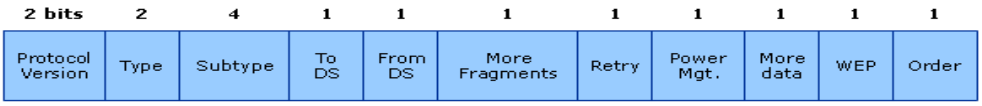

40

# 802.11 frame: more






41




# Protocol Version provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.

# Type and Subtype determines the function of the frame.
There are three different frame type fields:
**control, data, and management.**

# **To DS and From DS** indicates whether the frame is going to or exiting from the DS
This affects the order of the address fields see below ….

**To DS field is 1 and From DS field is 0**

Address 1 = BSSID
Address 2 = Source
Address 3 = Destination

**To DS field is 0 and From DS field is 1**

Address 1 = Destination
Address 2 = BSSID
Address 3 = Source