The 802.11 Alphabet Soup

a b g e s t k r n

Sachin Ganu

WINLAB

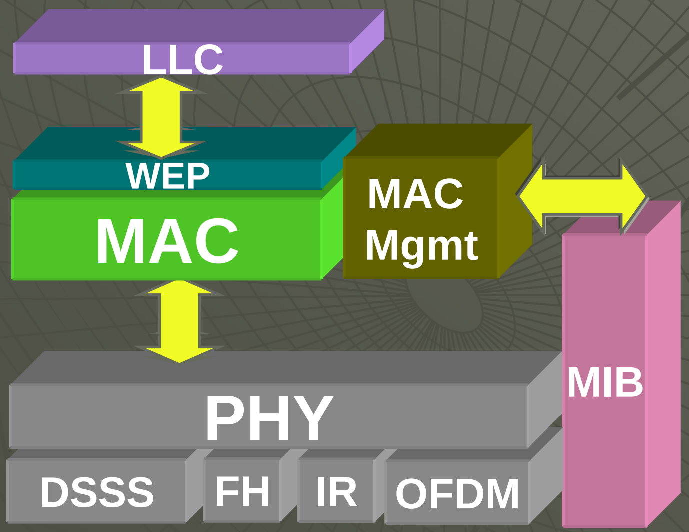
a b g e s t k r n

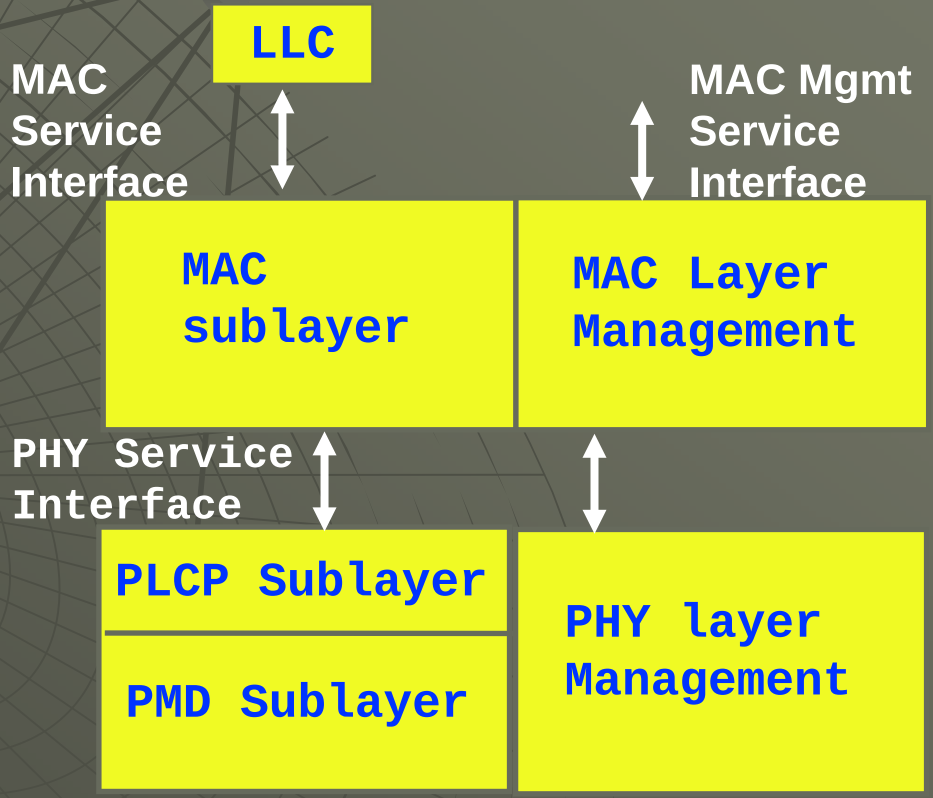
802.11 Background

- First standard was in 1997
  - Replacement for wired Ethernet
  - 2.4 GHz (Industrial Scientific and Medical Band)
  - CSMA/CA based contention
  - 1, 2 Mbps (DSSS, FHSS, IR PHY)

802.11 → 802.11b

- 802.11b (1999)
  - Higher data rates: 5.5 Mbps and 11 Mbps using CCK modulation



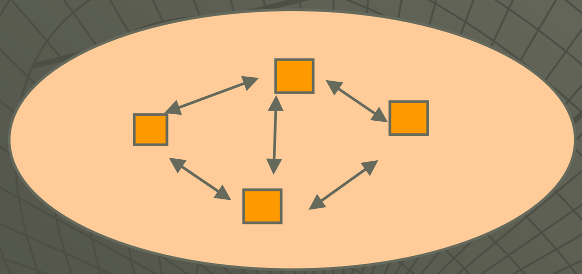


Courtesy: Dr. Pravin Bhagwat

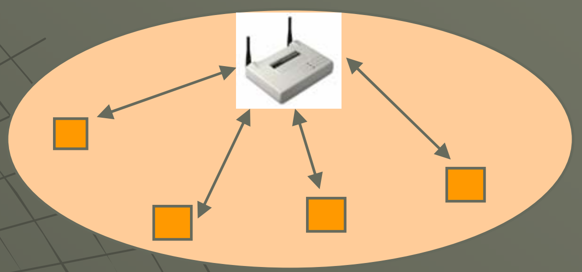
802.11 System Architecture

Basic Service Set (BSS): a set of stations which communicate with one another

Independent Basic Service Set (IBSS)



Infrastructure Basic Service Set (BSS)



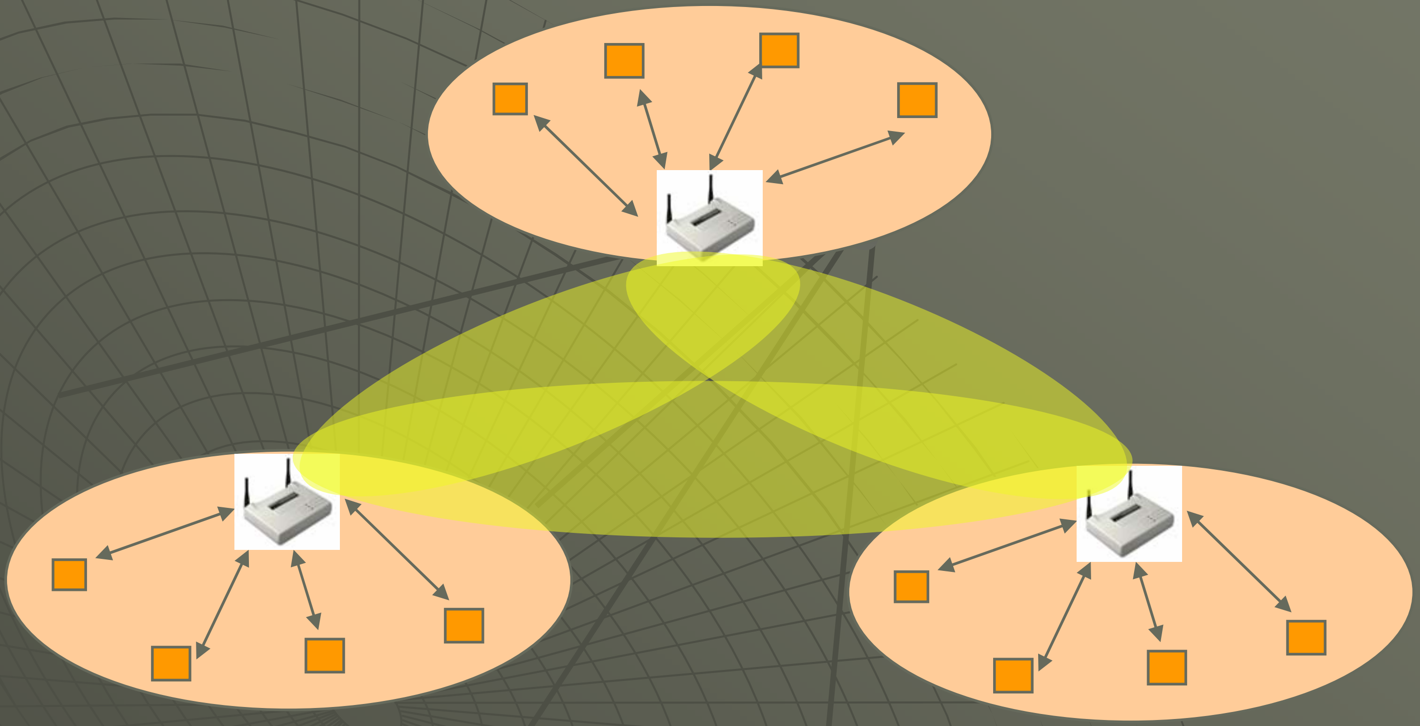
- only direct communication possible
- no relay function

- AP provides
  - connection to wired network
  - relay function
- stations not allowed to communicate directly

Courtesy: Dr. Pravin Bhagwat

Extended Service Set

ESS: a set of BSSs interconnected by a distribution system (DS)



- ESS and all of its stations appear to be a single MAC layer
- AP communicate among themselves to forward traffic
- Station mobility within an ESS is invisible to the higher layers

Courtesy: Dr. Pravin Bhagwat

802.11 PHY

Sender

MAC Protcol Data Unit (MPDU)

Receiver

MAC Protcol Data Unit (MPDU)

MAC

PHY

PLCP header | **MAC Protcol Data Unit (MPDU)**

PLCP header | **MAC Protcol Data Unit (MPDU)**

Physical Media Dependent (PMD) layer

PMD layer

Frequency Hopping Spread Spectrum (FHSS) PHY
1, 2 Mbps

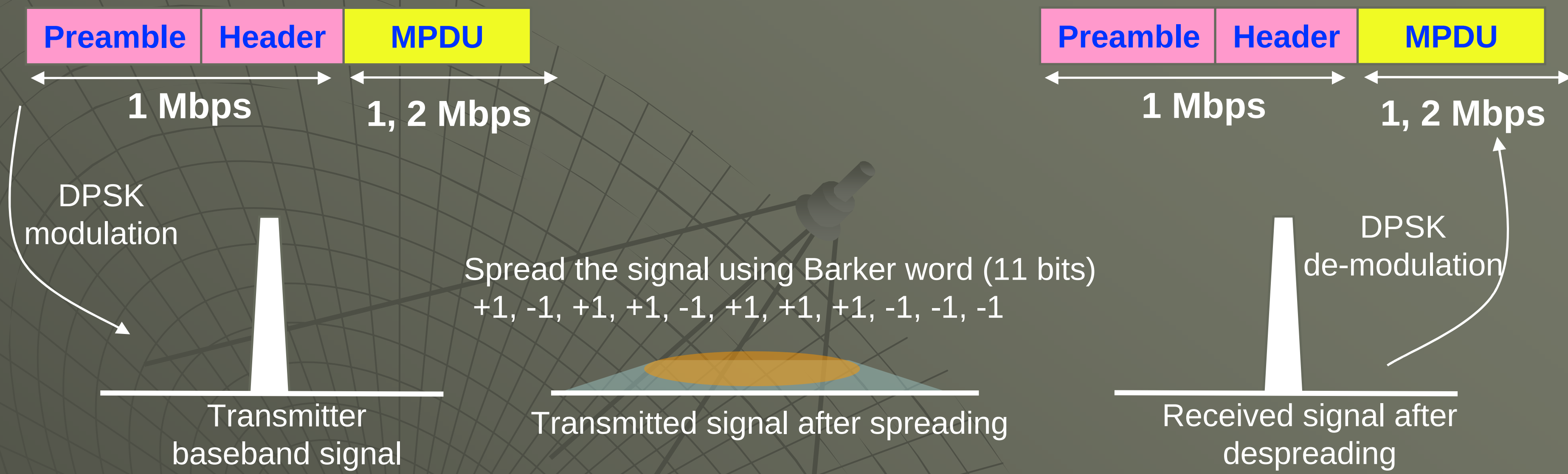
Direct Sequence Spread Spectrum (DSSS) PHY
1,2 Mbps

High rate (DSSS) PHY
11, 5.5 Mbps
802.11b

Infrared (IR) PHY
1,2 Mbps

Courtesy: Dr. Pravin Bhagwat

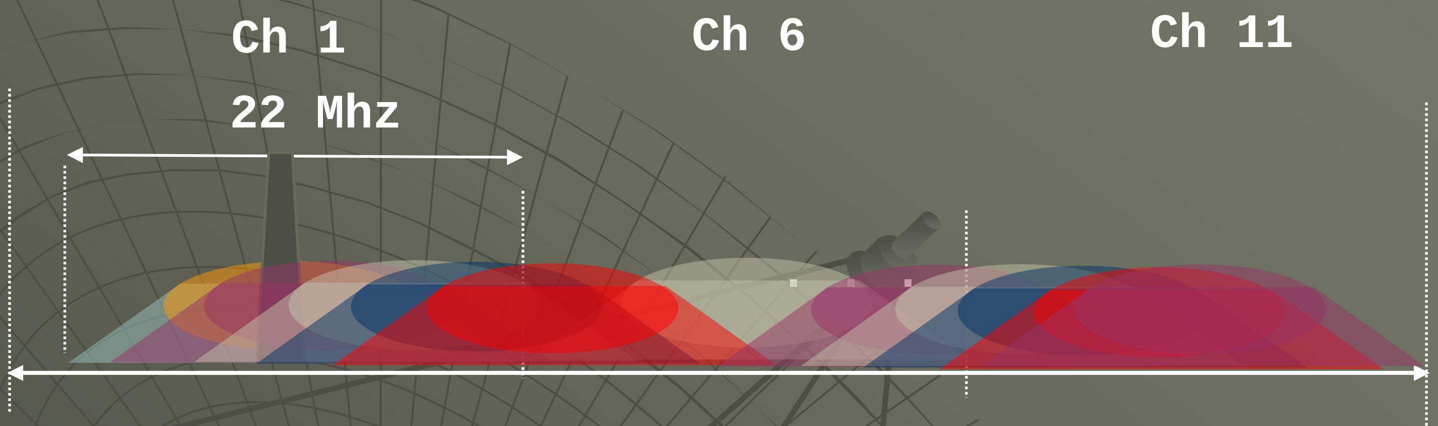
DSSS PHY



- Baseband signal is spread using Barker code
- Spread signal occupies approximately 22 Mhz bandwidth
- Receiver recovers the signal by applying the same Barker code
- DSSS provides good immunity against narrowband interferer
- CDMA (multiple access) capability is not possible

Courtesy: Dr. Pravin Bhagwat

DSSS PHY



- Direct sequence spread spectrum
  - Each channel is 22 Mhz wide
- Symbol rate
  - 1 Mb/s with DBPSK modulation
  - 2 Mbps with DQPSK modulation
  - 11, 5.5 Mb/ps with CCK modulation
- Max transmit power
  - 100 Mw (20 dBm)

Courtesy: Dr. Pravin Bhagwat

802.11 MAC

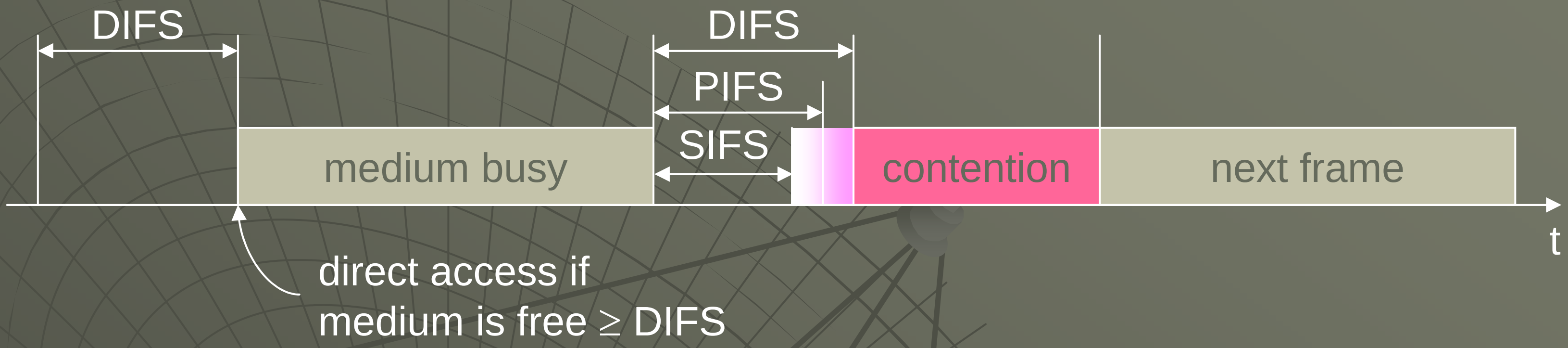
- Carrier sensing (CSMA)
  - carrier → do not transmit
  - no carrier → OK to transmit
  - Virtual carrier-sense → NAV
  - Hidden Terminals?
    - Solution: RTS/CTS
    - Problem: exposed terminals
- Collision Avoidance (CA)
  - CD does not work well (attenuation, half duplex radios)
  - Therefore, use collision avoidance (CA)
    - random backoff, priority ack protocol

Courtesy: Dr. Pravin Bhagwat

802.11 - MAC layer

- Distributed Co-ordinated Function (DCF) – random access
- Point Coordinated Function (PCF) – polling based

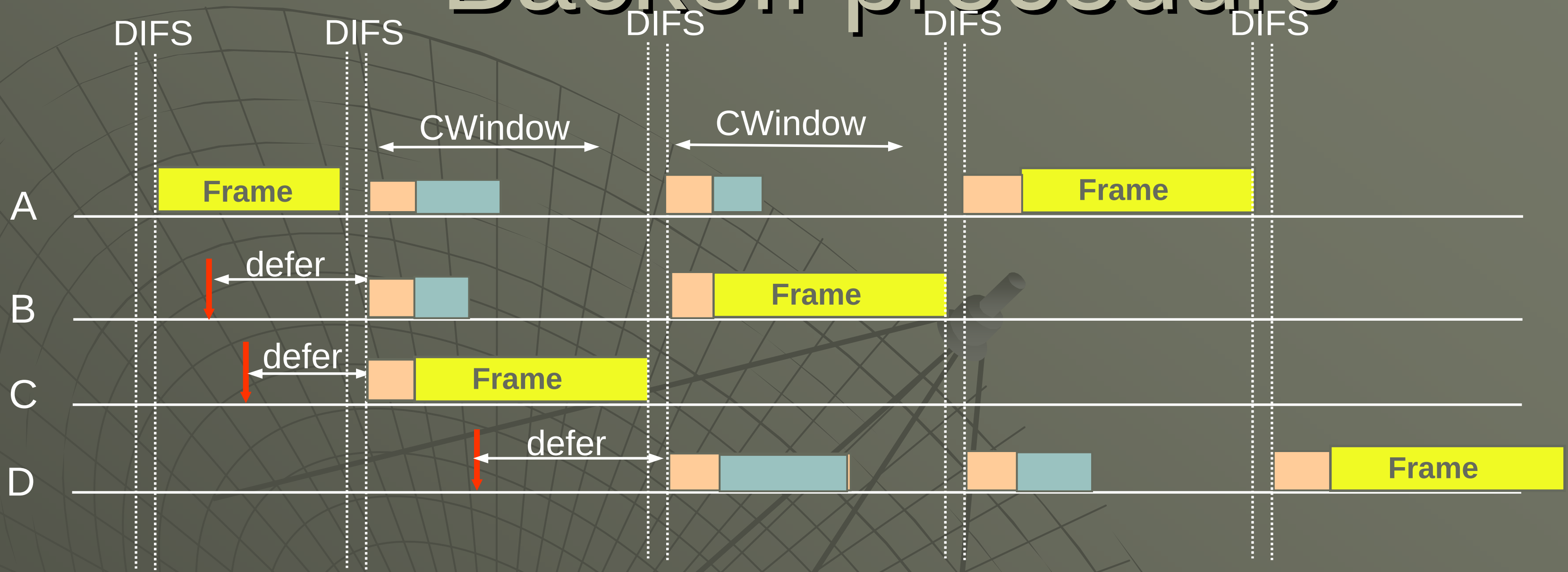
802.11 - DCF



- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF IFS)
  - lowest priority, for asynchronous data service

Courtesy: Dr. Pravin Bhagwat

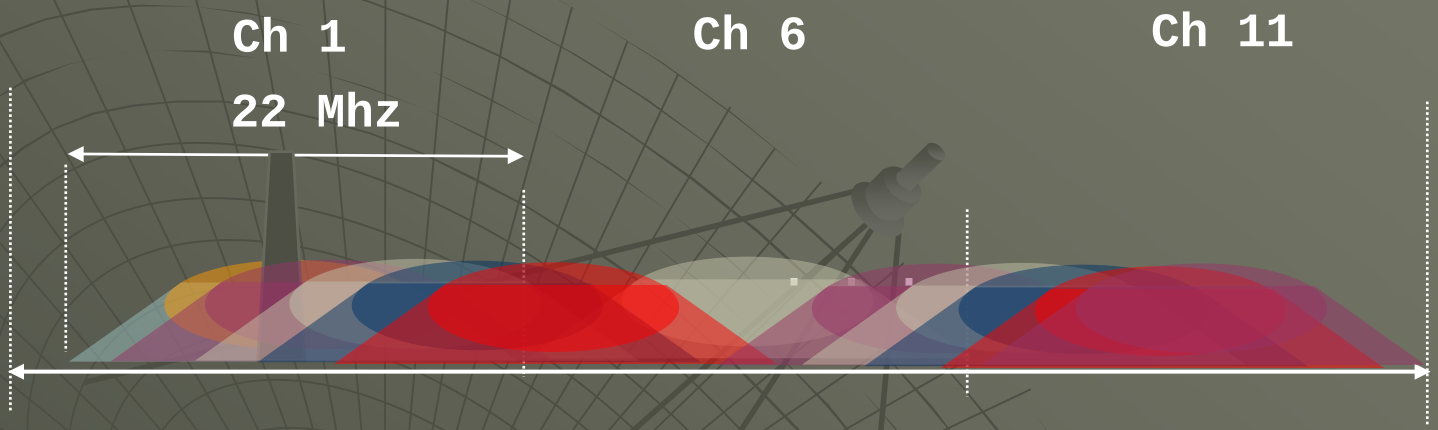
Backoff procedure



- Immediate access when medium is free >= DIFS
- When medium is not free, defer until the end of current frame transmission + DIFS period
- To begin backoff procedure
  - Choose a random number in (0, Cwindow) in terms of slots
  - Use carrier sense to determine if there is activity during each slot
  - Decrement backoff time by one slot if no activity is detected during that slot
- Suspend backoff procedure if medium is determined to be busy at anytime during a backoff slot
- Resume backoff procedure after the end of current frame transmission+DIFS

Courtesy: Dr. Pravin Bhagwat

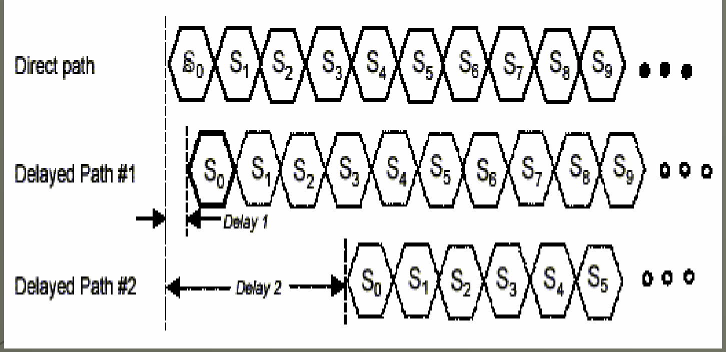
802.11b → 802.11a



- Crowding in the ISM 2.4 Ghz band
  - Microwaves
  - Cordless phones
  - Increased interference
- Move to 5 GHz UNII band
  - OFDM modulation to counteract multipath
  - Higher rates: upto 54 Mbps

802.11a PHY

- OFDM - Information signal split across 52 subcarriers- 4 pilot carriers, 48 data carriers
- Multipath problem: If (delay spread > guard time between symbols) => ISI
- Lower rate per subcarrier=> tolerance to delay spread
- Multi-carrier
- Slot times adjusted according to RTT (9 μs)



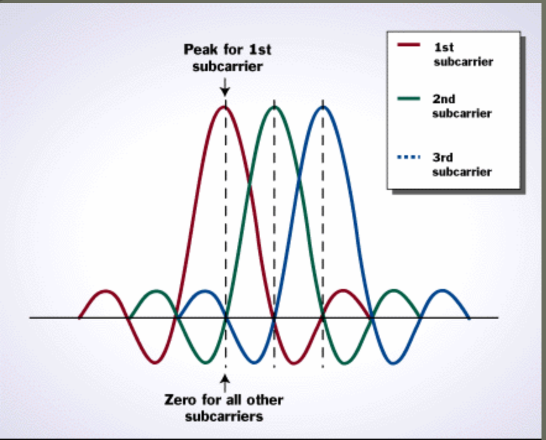


FIGURE 4: Orthogonality in an OFDM system occurs when at the peak of each subcarrier spectrum, the contribution from all other subcarriers is zero.

Ref: CommsDesign
IEEE 802.11a - Speeding Up Wireless Connectivity in the Home

802.11a MAC

- Same as ‘b’ with timers adjusted according to *aslottime*

802.11a Problems

- Reduced range
- No interoperability with legacy ‘b’

Enter 802.11g (2003)

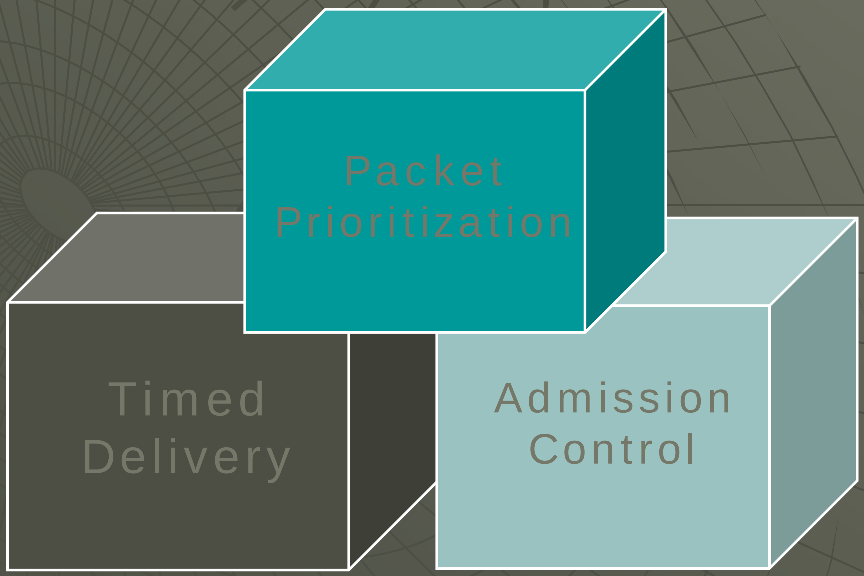
- Range of 802.11b with speed of 802.11a
  - i.e OFDM at 2.4 Ghz
  - Problem – Interoperability with b
  - For Carrier sensing and backoff to work, DSSS based ‘b’ clients must be able to hear OFDM-based ‘g’ clients

Interoperability with 802.11b

- RTS/CTS to the rescue – Protection mechanism
- CCK CTS exchange precedes each OFDM high rate packet and the subsequent OFDM ACK
- As long as there are 802.11b clients, CTS will be on

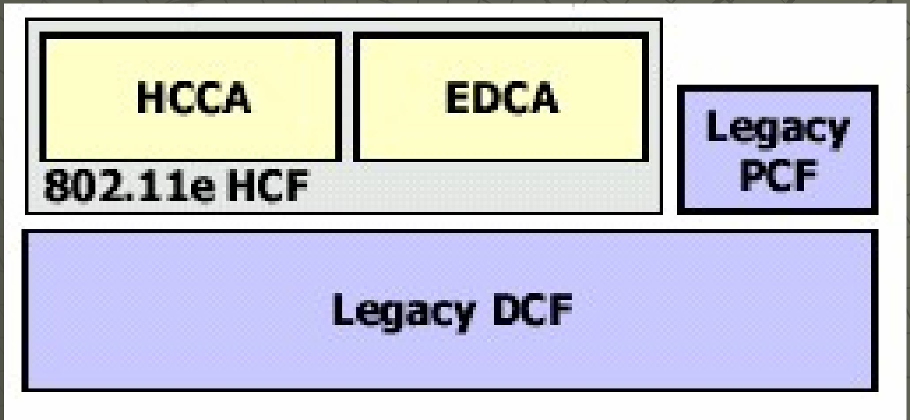
Quality of Service

- All packets were treated alike
  - e.g AP downstream traffic treated the same as upstream traffic to AP from the clients
  - VoIP packet same as FTP packet
  - How to deal with QoS sensitive applications? E.g VoIP over 802.11



Enter 802.11e

- 802.11 with QoS support
- Ratified last month



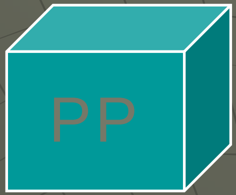
EDCA = Enhanced Distributed Channel Access

HCCA = HCF Controlled Channel Access

HCF = Hybrid Coordination Function

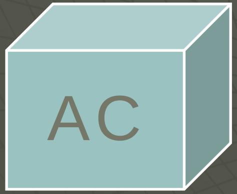
EDCA = DCF++
HCCA = PCF++

802.11e NCF



- Prioritization
  - 802.11e EDCA Access Categories

- Timed Delivery
  - 802.11e HCCA allows AP to create ‘master schedule’ to coordinate traffic delivery for all devices



- Admission Control
  - TSpecs sent by the device to the AP indicate:
    - Frequency of transmission
    - Bandwidth requirement
  - AP decides to admit the device based on current traffic load

Prioritization: EDCA

For each packet

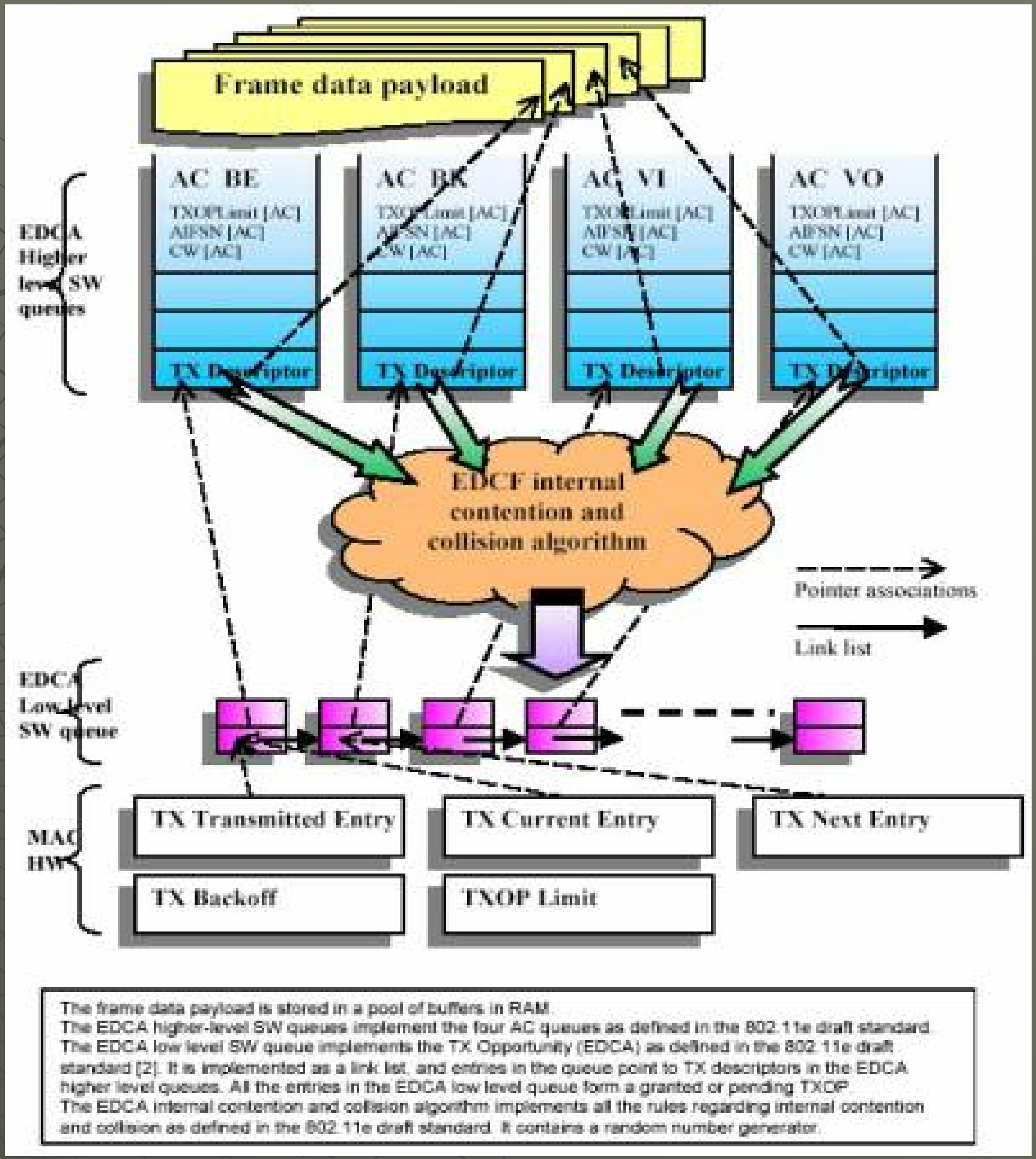
- Classify packet
- Push into appropriate queue
- MSDUs from different ACs contend for EDCA-TXOP internally within the QSTA

Internal contention resolution selects backoff based on

- TxOP Limit
- AIFSN
- CW

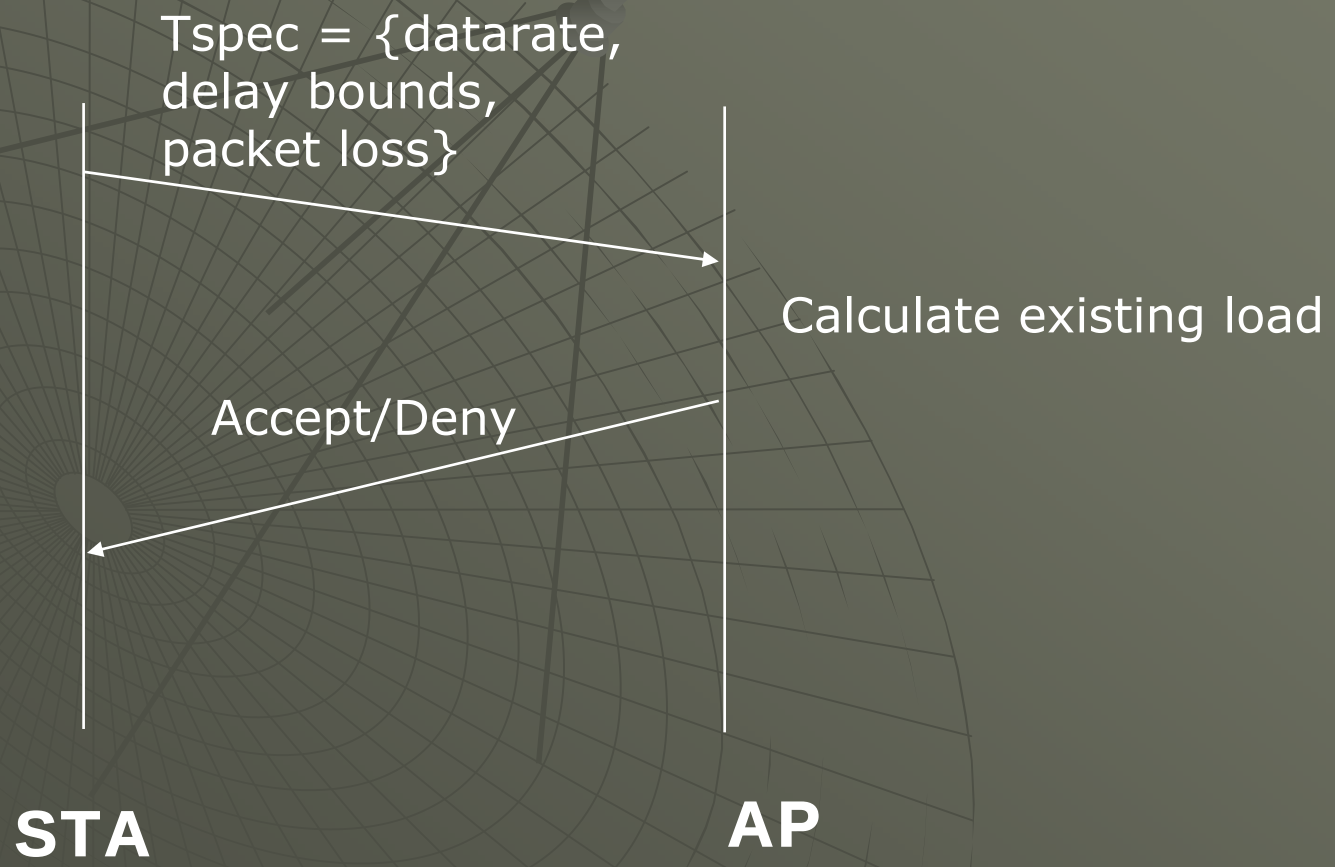
The winning MSDU then contends for the channel

Reference: **Understanding the MAC impact of 802.11e** http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=16502136



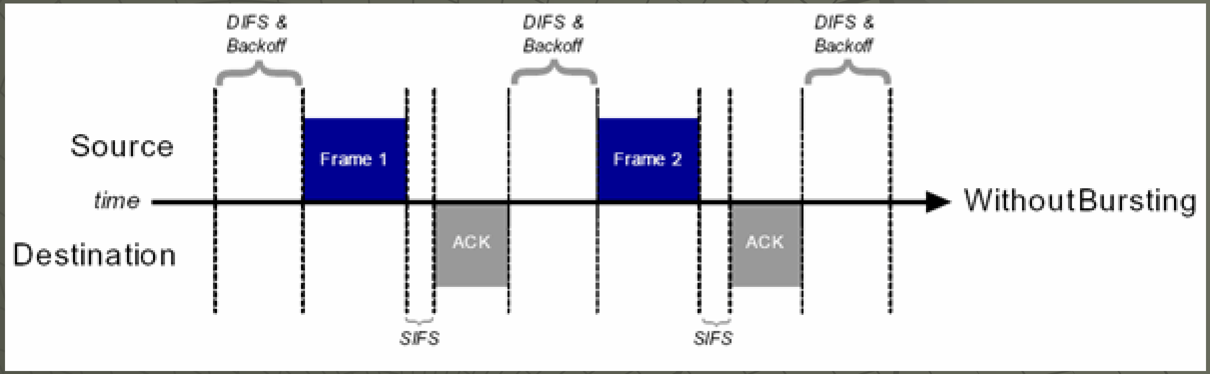
Admission Control: TSpec

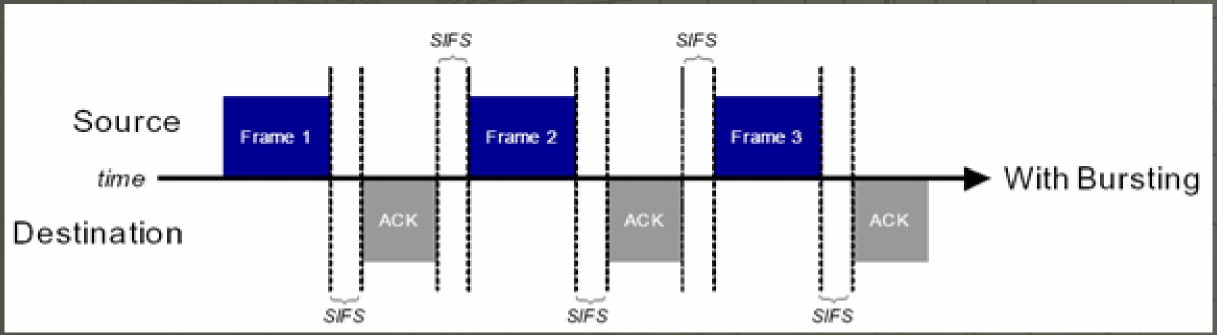
- Mandatory at AP, optional at STA



Other Features

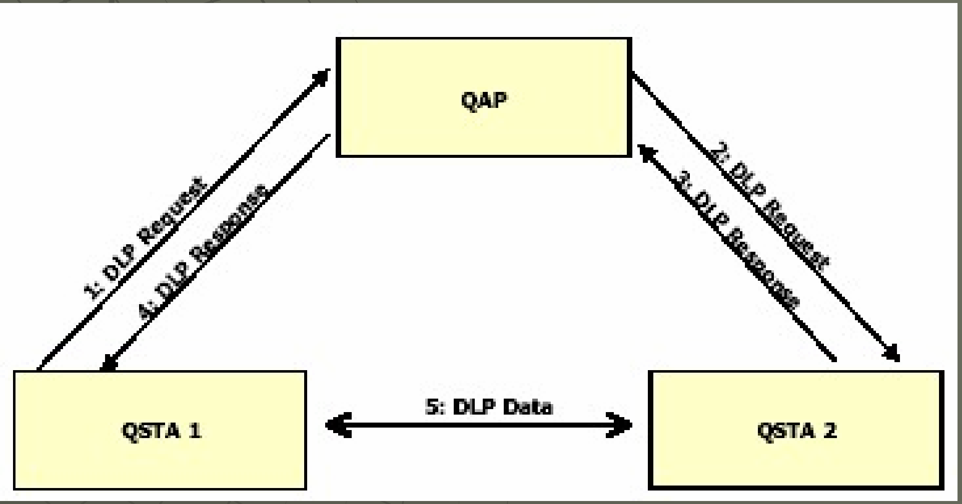
- Frame bursting





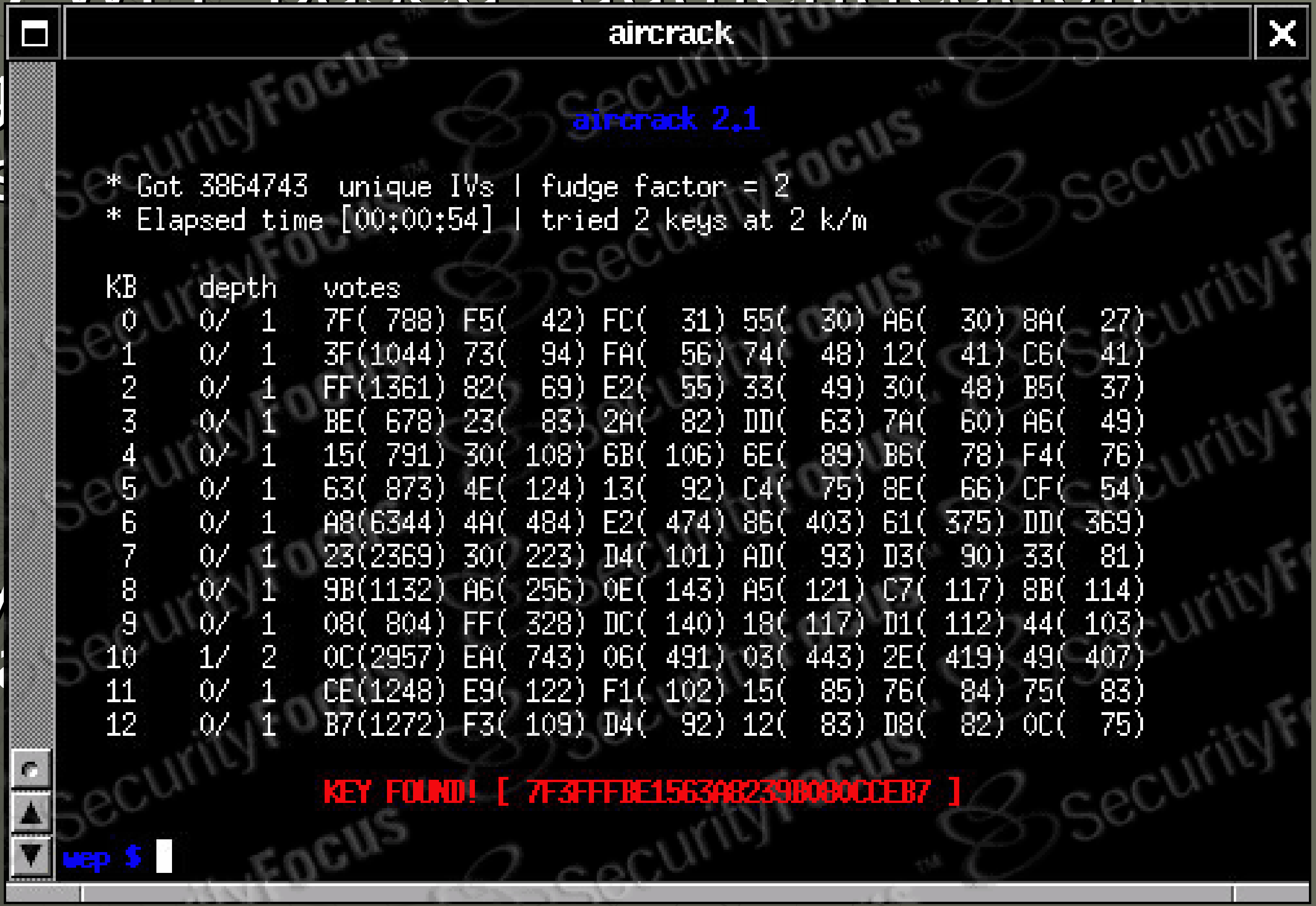
Other Features

- ACK suppression
- Fast Frames – (single header, multiple frames)
- Compression
- Direct Link setup



Mandatory slide on Security

- Earlier, WEP based "authentication"
  - Desig
    eaves
  - Simp
    key
- Issues
  - Easily
    AirCr

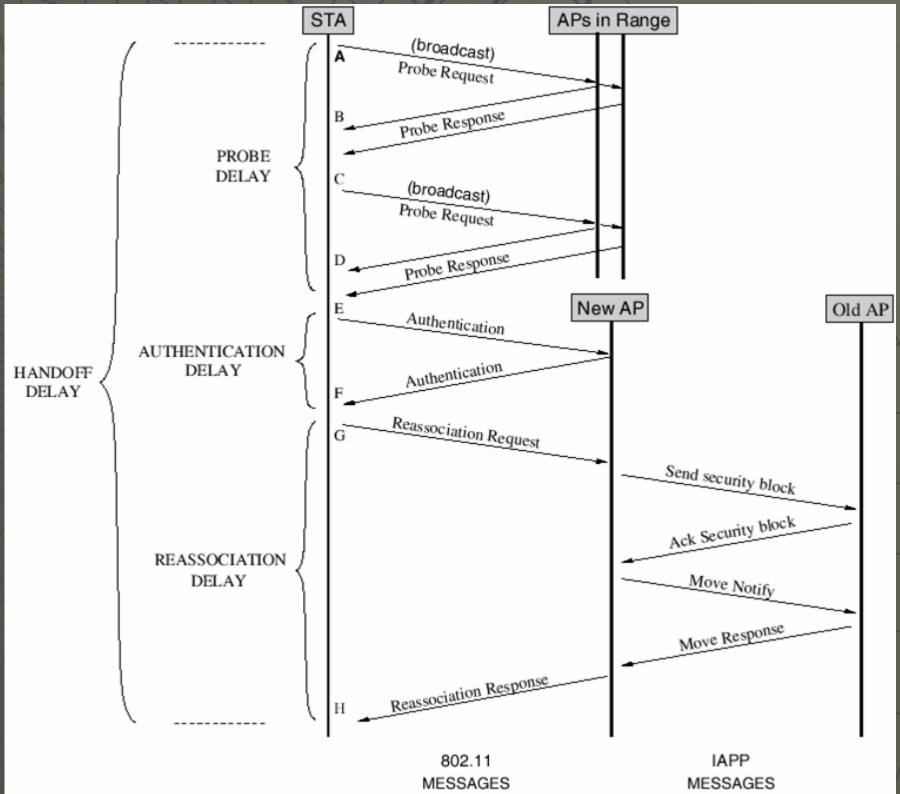


802.11i

- 802.11i – Used 802.1x based mutual authentication, Encryption and key rotation, message integrity check
- Increased message exchange between AP/Clients prior to association

Roaming

- So we have VoIP calls using *e* and security using *i*
- What if I want to roam between APs without experiencing "gaps"?



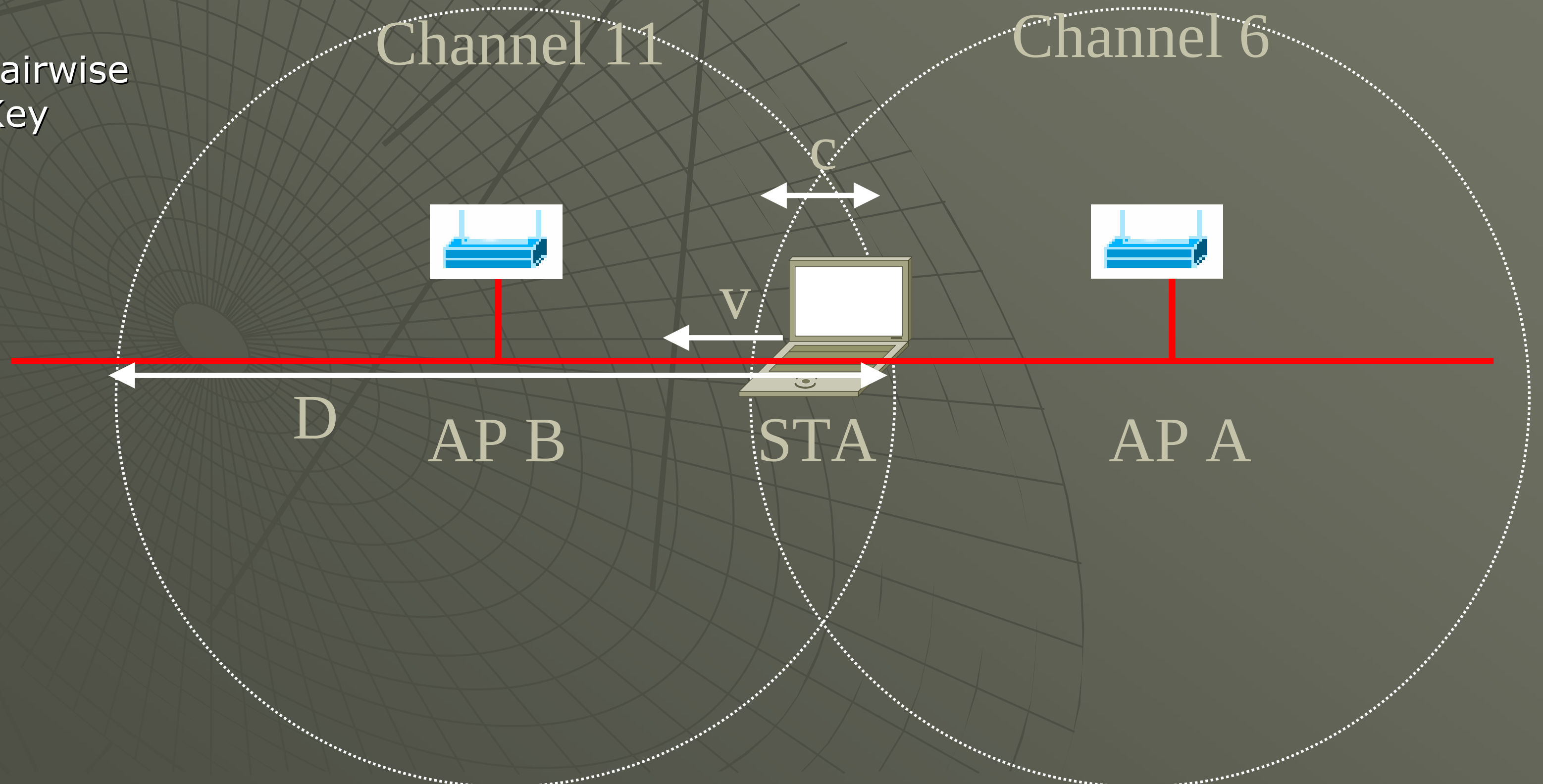
Layer	Item	Time (ms)
L2	802.11 scan (passive)	0 ms (cached), 1 second (wait for Beacon)
L2	802.11 scan (active)	40 to 300 ms
L2	802.11 assoc/reassoc (no IAPP)	2
L2	802.11 assoc/reassoc (w/ IAPP)	40
L2	802.1X authentication (full)	1000
L2	802.1X authentication (fast resume)	250
L2	Fast handoff (4-way handshake only)	60
L3	DHCPv4	1000
L3	Initial RS/RA	5
L3	Wait for subsequent RA	1500
L3	DAD (full)	1000
L3	Optimistic DAD	0
L3	MN-HA BU	1 RTT (IKE w/HA SA), 4 RTT (IKE w/CoA SA)
L3	MN-CN BU	1-1.5 RTT (CAM) to 2.5 RTT (RR)
L4	TCP parameter adjustment (status quo)	5000 (802.11/CDMA) - 20000 (802.11/GPRS)
Best case	All fixes	150 ms
Average case	6to4, RR, Active scan	1300 ms
Worst case	No TCP changes, full EAP auth, IAPP, DHCPv4	25000 ms

Source: Bernard Aboba, http://www.drizzle.com/~aboba/IEEE/

802.11r (Roaming)

- Handoff triggering mechanisms
- Pre-Authentication (authenticate before break)
- Reduced re-association message exchange (cache keys and use them again-STA recognizes that it has already derived a PMK with AP B that still has lifetime remaining

PMK = Pairwise Master Key



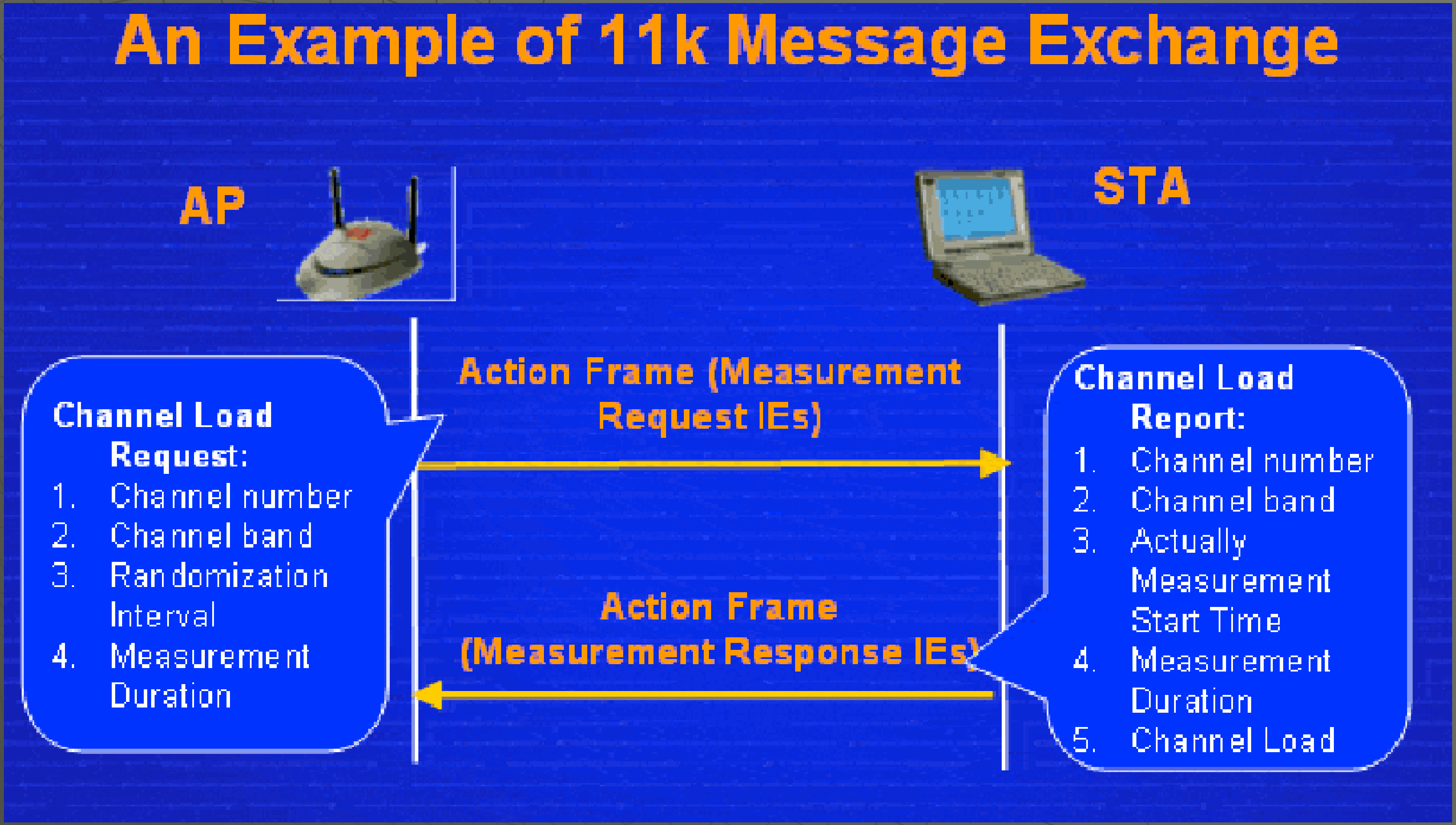
802.11k (Neighbor Report)

- How to decide which is the best AP to associate to??

- Radio Resource Measurements
  - Beacon Report : SSID, Channel and RSSI of all beacons seen
  - Frame Report
    - Channel Load : Channel busy fraction
    - Noise Histogram : sample channel when idle to estimate noise
    - Hidden node Report
    - Medium Sending Time Histogram
    - Peer STA Stats : Failed count, Retry count
    - Receiver Channel Power Indicator (RCPI) = RSSI++

- STA reports measurements to AP

802.11k


An Example of 11k Message Exchange
AP
STA
Channel Load Request:
1. Channel number
2. Channel band
3. Randomization Interval
4. Measurement Duration
Action Frame (Measurement Request IEs)
Action Frame (Measurement Response IEs)
Channel Load Report:
1. Channel number
2. Channel band
3. Actually Measurement Start Time
4. Measurement Duration
5. Channel Load

802.11k Possible Applications

Network Management
- Load Balancing
- Admission Control
- Detect Rogue AP

Network Configuration
- Coverage/Frequency Planning
- Transmit Power Adjustment
- Estimate non 802.11 interference

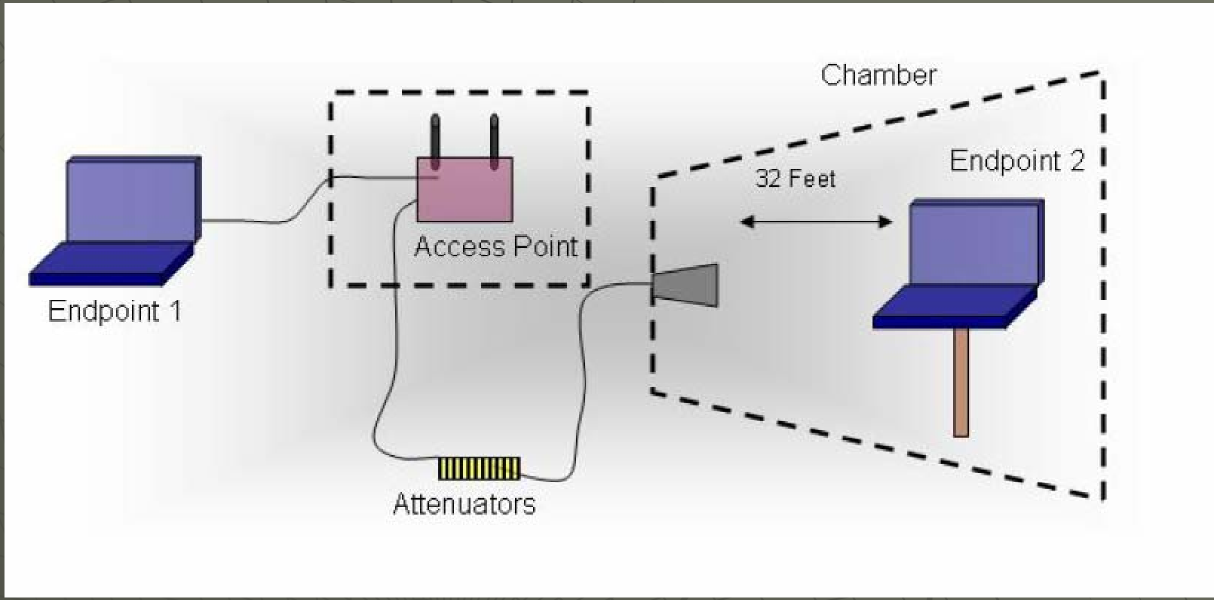
Roaming
- Find overlapping BSS
- Best AP selection
- Roaming-Handoff

Locationing

802.11t : Test Methodology

- Helps define standardized ways for measurement and prediction of WLAN systems
- Several equipment vendors
- How do you compare the performance of their products?
  - 802.11 t – Standard testing methodology

802.11t

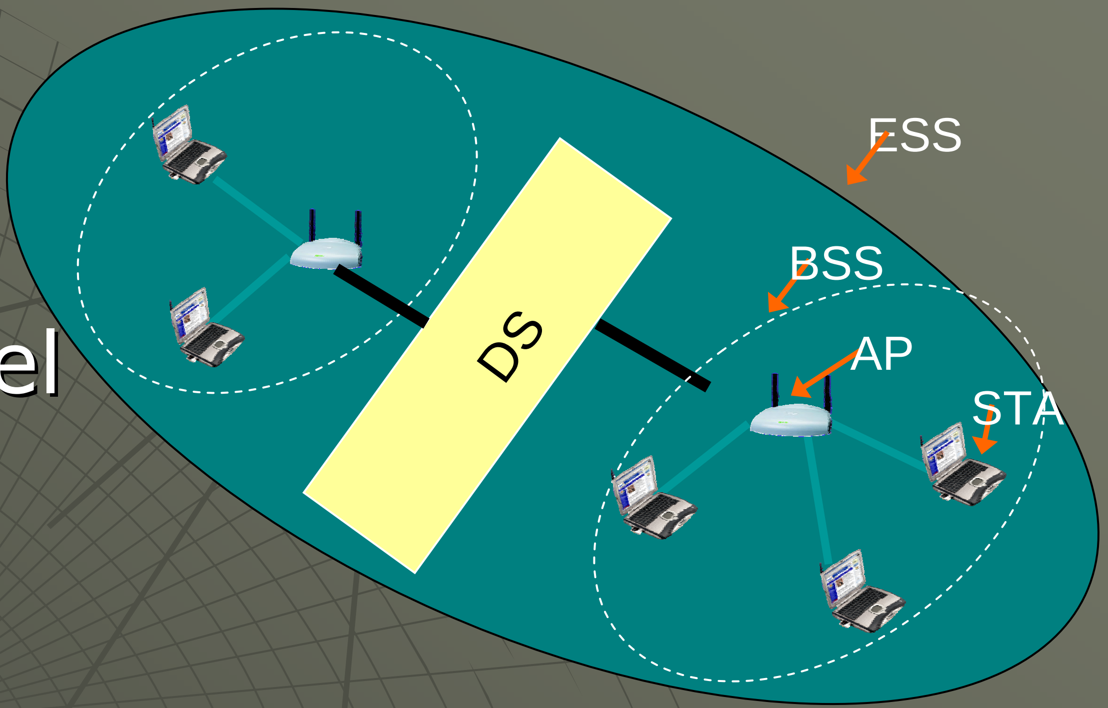


Test methodology
- Over the air
- Conducted
- Throughput vs range

Test metrics
- Throughput, delay, packet loss, handoff latency, jitter

Mesh Networking

- So far..
- Multi-hop multi-channel

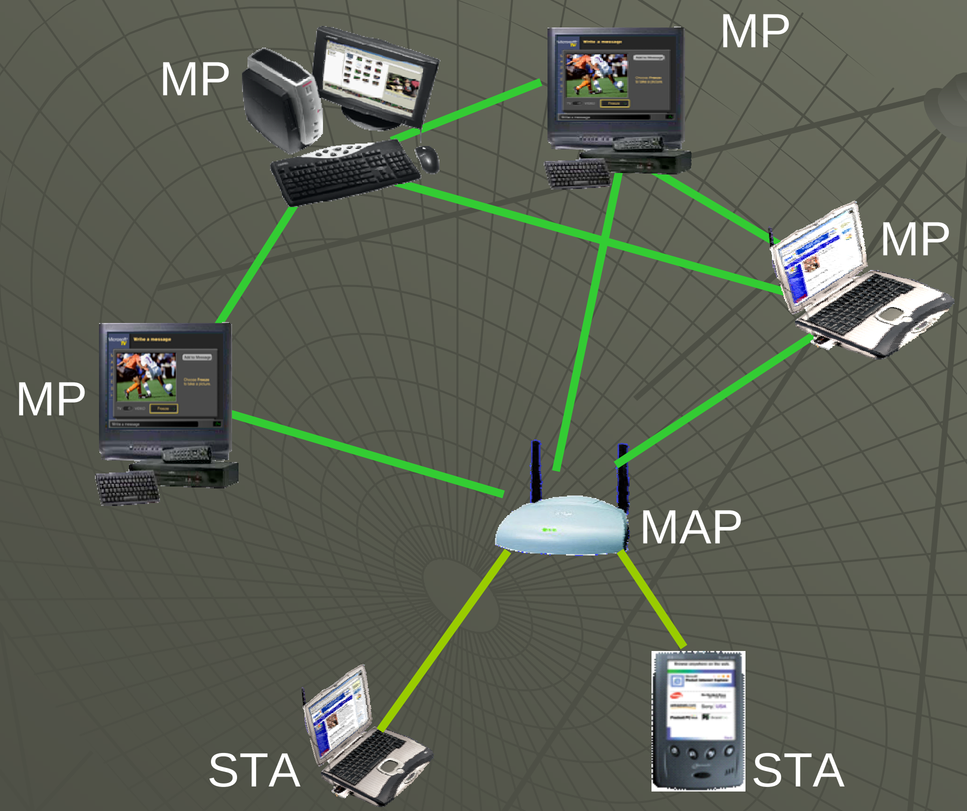


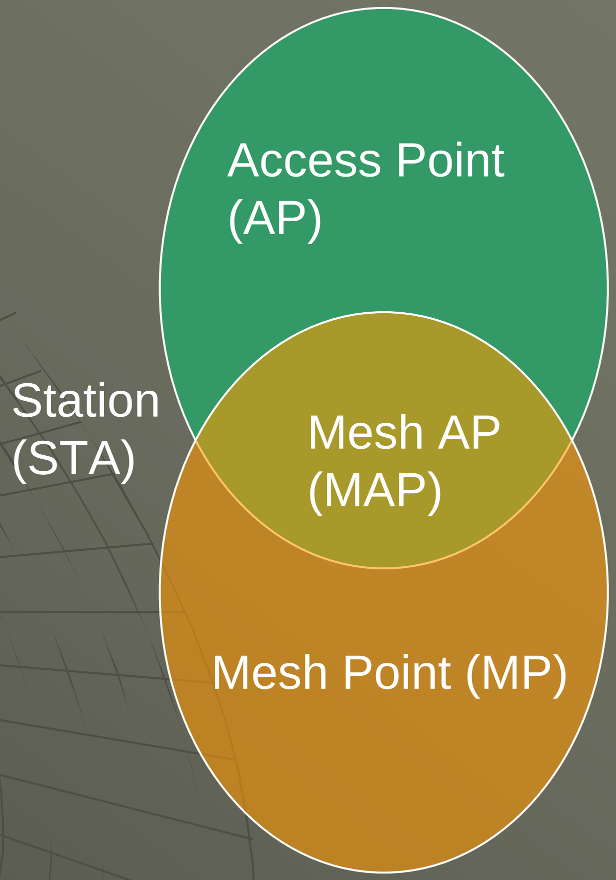
- Proprietary solutions MeshNetworks, FireTide, Tropos, MeshDynamics etc

802.11s Motivation and Objectives

- Provide a protocol for self-configuring, for unmanaged WLAN networks i.e those that are not fully configured by a SP
- Interoperability
- Increased Range/coverage
- Backward compatibility
- Multimedia transport between devices

Devices in a mesh





Functional components

- MAC enhancements (e, n)
- Routing (HopCount, ETX, ETT)
- Self-configuration (channel, power, sensitivity)
- QoS
- Security

Major players

SEE-Mesh	WI-Mesh
Intel	Nortel
Motorola	Thomson
Nokia	Interdigital
TI	MITRE
Cisco	NextHop
Firetide	Philips
Tropos	
Sony	

What next??

- 802.11n = Σ (OFDM, QoS, MIMO)
  - Currently, deadlocked at IEEE Standards meeting
- 802.11p: Vehicular wireless access
  - Looking at issues relating to using Wi-Fi radios in cars to access stationary wireless APs (Initially, 1 km at 125 mph)

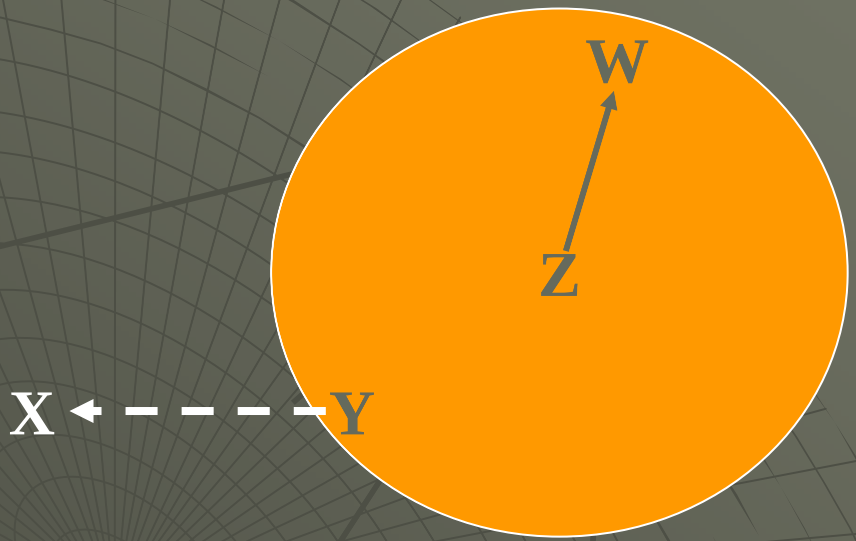
802.11aa, ab, ac??

Homework for next week

- ‘a’ for OFDM
- ‘b’ for DSSS
- ‘e’ for QoS
- ‘g’ for OFDM at 2.4
- ‘k’ for radio measurements
- ‘r’ for roaming
- ‘s’ for mesh
- ‘t’ for testing
- ‘n’ for going nowhere

Problems with carrier sensing

<u>Exposed terminal problem</u>



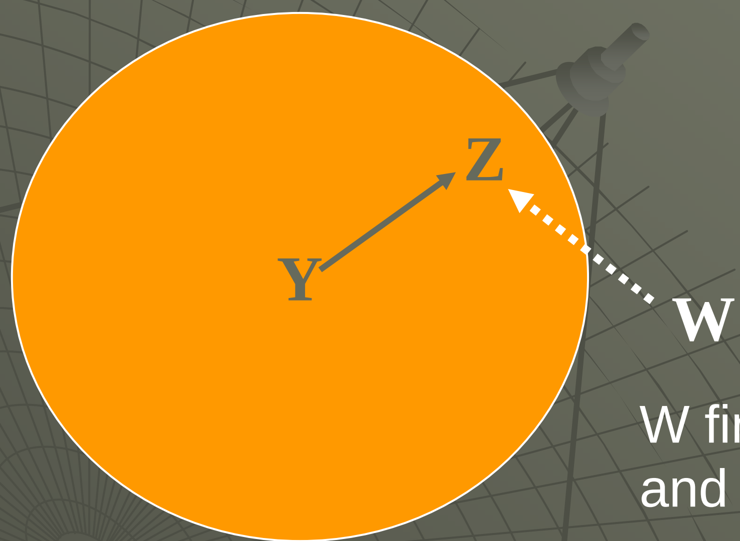
Z is transmitting to W

Y will not transmit to X
even though it cannot interfere

Presence of carrier =/=> hold off transmission

Problems with carrier sensing

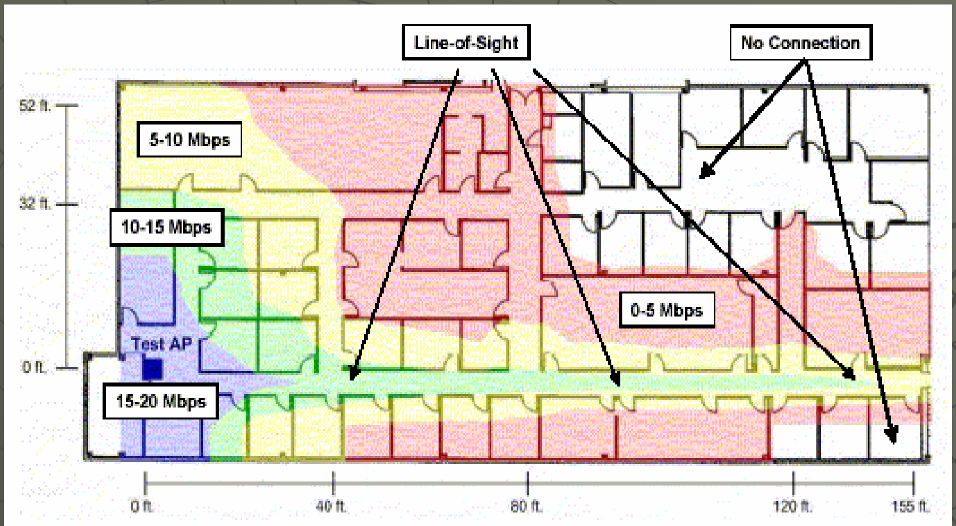
<u>Hidden terminal problem</u>



W finds that medium is free and it transmits a packet to Z

no carrier =/=> OK to transmit

Range tests: ‘a’ vs ‘g’



a

g