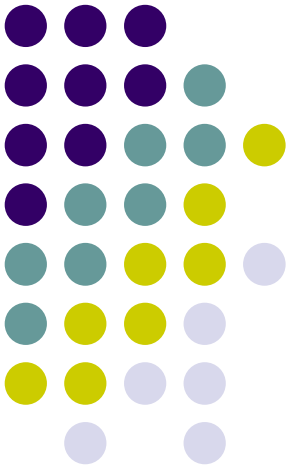
WiFi

Is for “Wireless Fidelity”

Or

IEEE 802.11 Standard

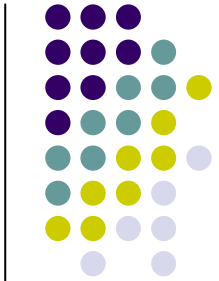
By Greg Goldman



What is the goal of 802.11 standard ?

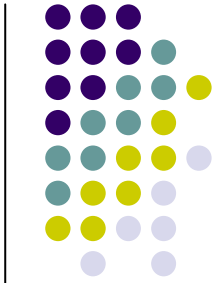
- To develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable and moving stations within a **local area**.

802.11 sub-standards(amendments) ….



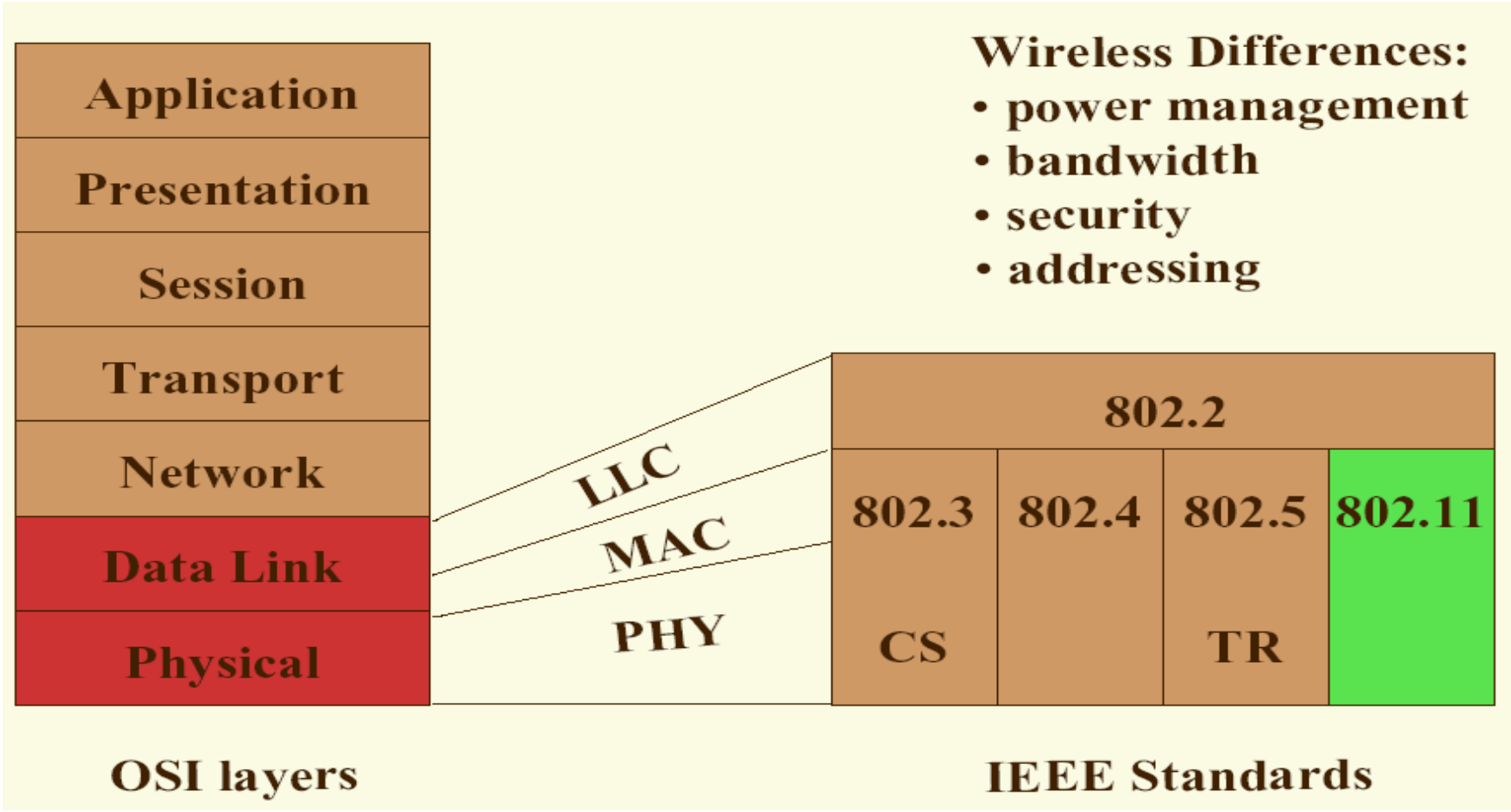
- 802.11 MAC (Media Access Control) ratified 1999
- 802.11b PHY 2.4 GHz (max 11 Mbps) ratified 1999
- 802.11a PHY 5.0 GHz (max 54 Mbps) ratified 1999
- 802.11g PHY 2.0 GHz (max 54 Mbps) ratified 2003
- 802.11i Security draft number XXX
- 802.11e QoS, Multimedia draft number XXX
- 802.11h European regulations for 5GHz draft number XXX
- 802.11h Japan regulations for 5GHz draft number XXX

Do I need any license to use 802.11 device ?

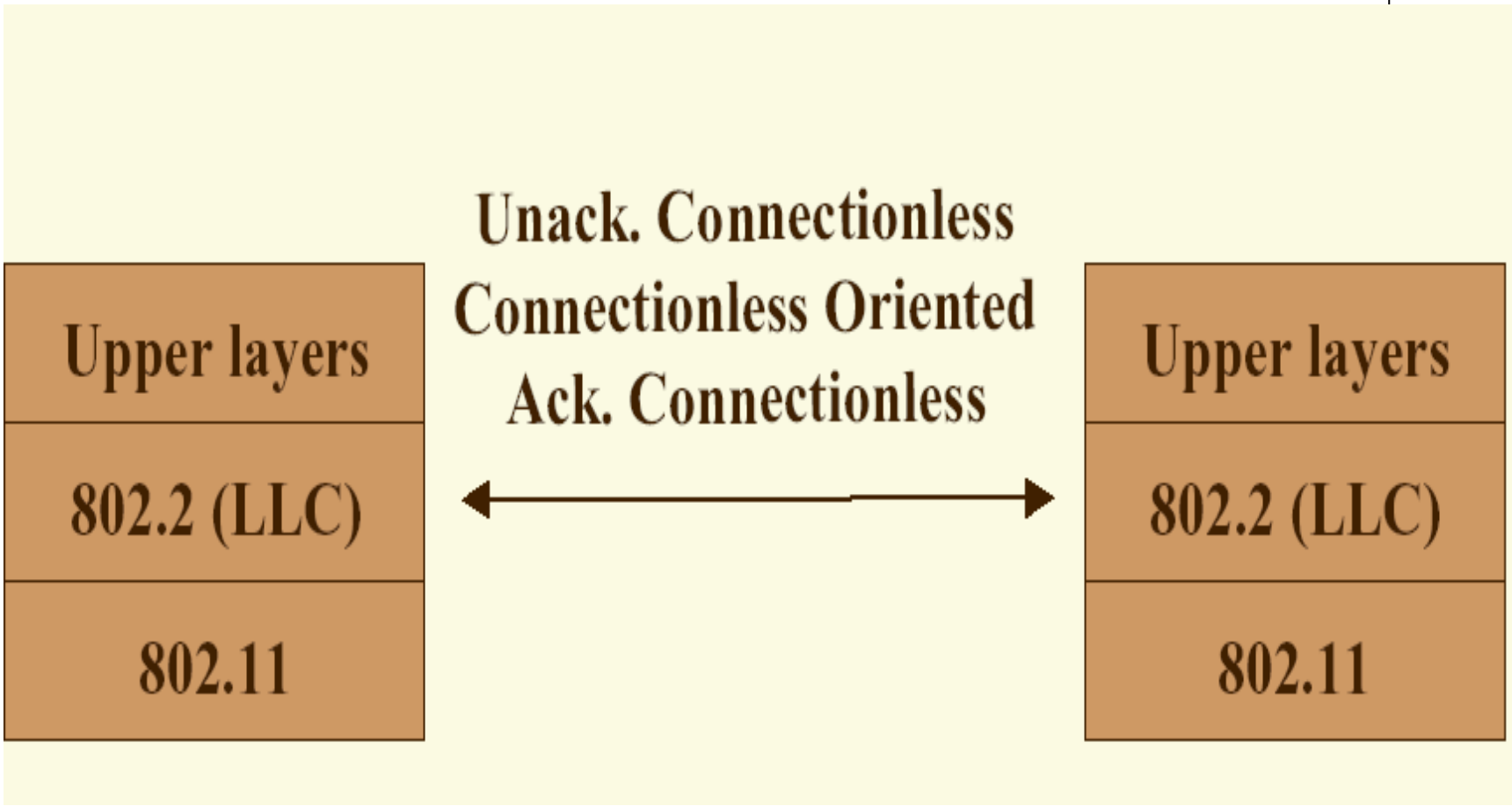


- No , 2.4 GHz and 5.0 GHz are public available frequency !!!

Context with OSI layers



Logical Link Control Services



Standard 802.11 frame format

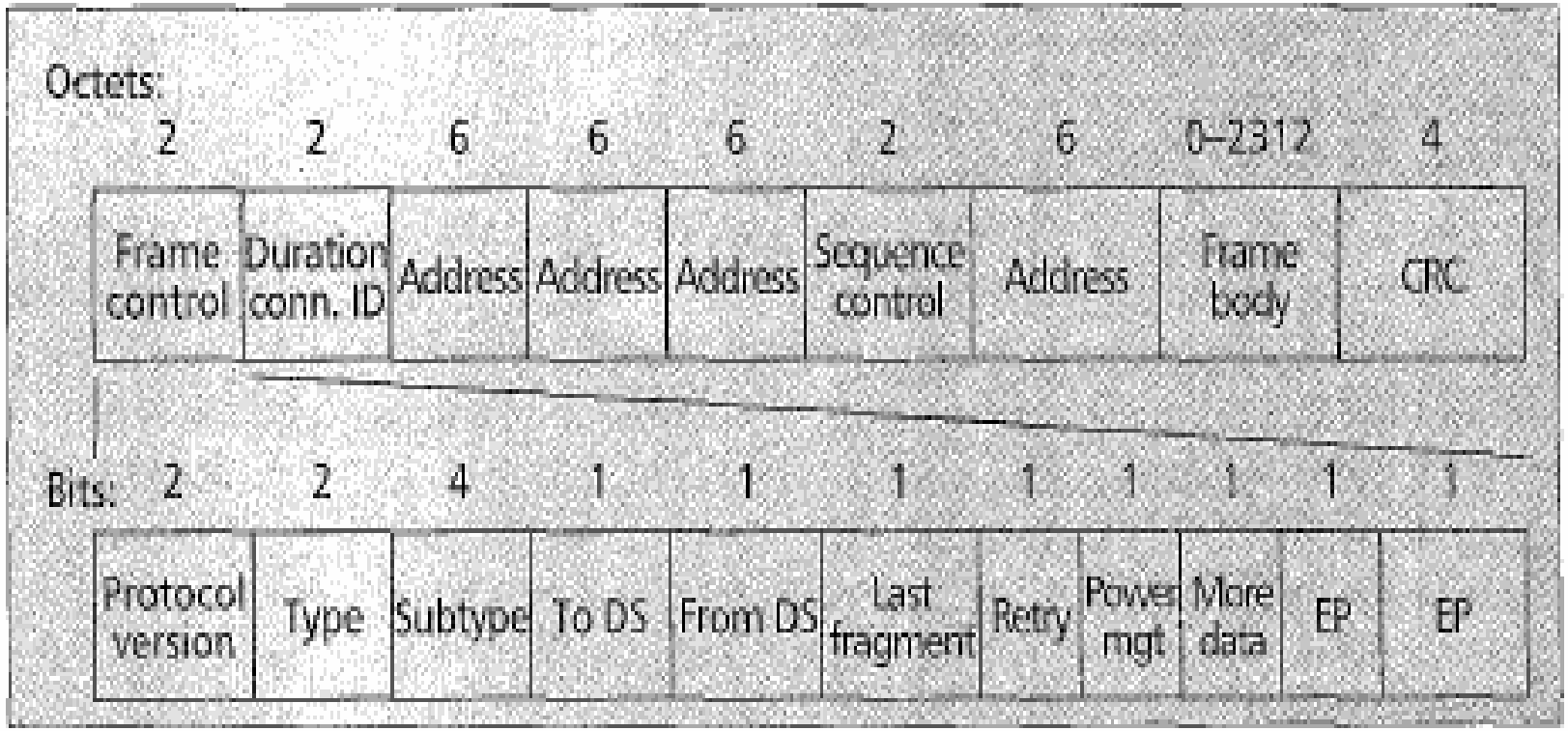
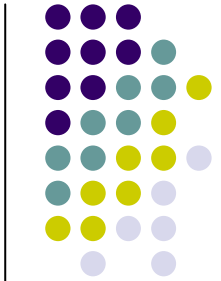


Figure 3. *Standard IEEE 802.11 frame format.*

Frames types and subtypes



- Three types of frames:
  - Control

    (ACK,RTS,CTS ,Power Save …)
  - Management

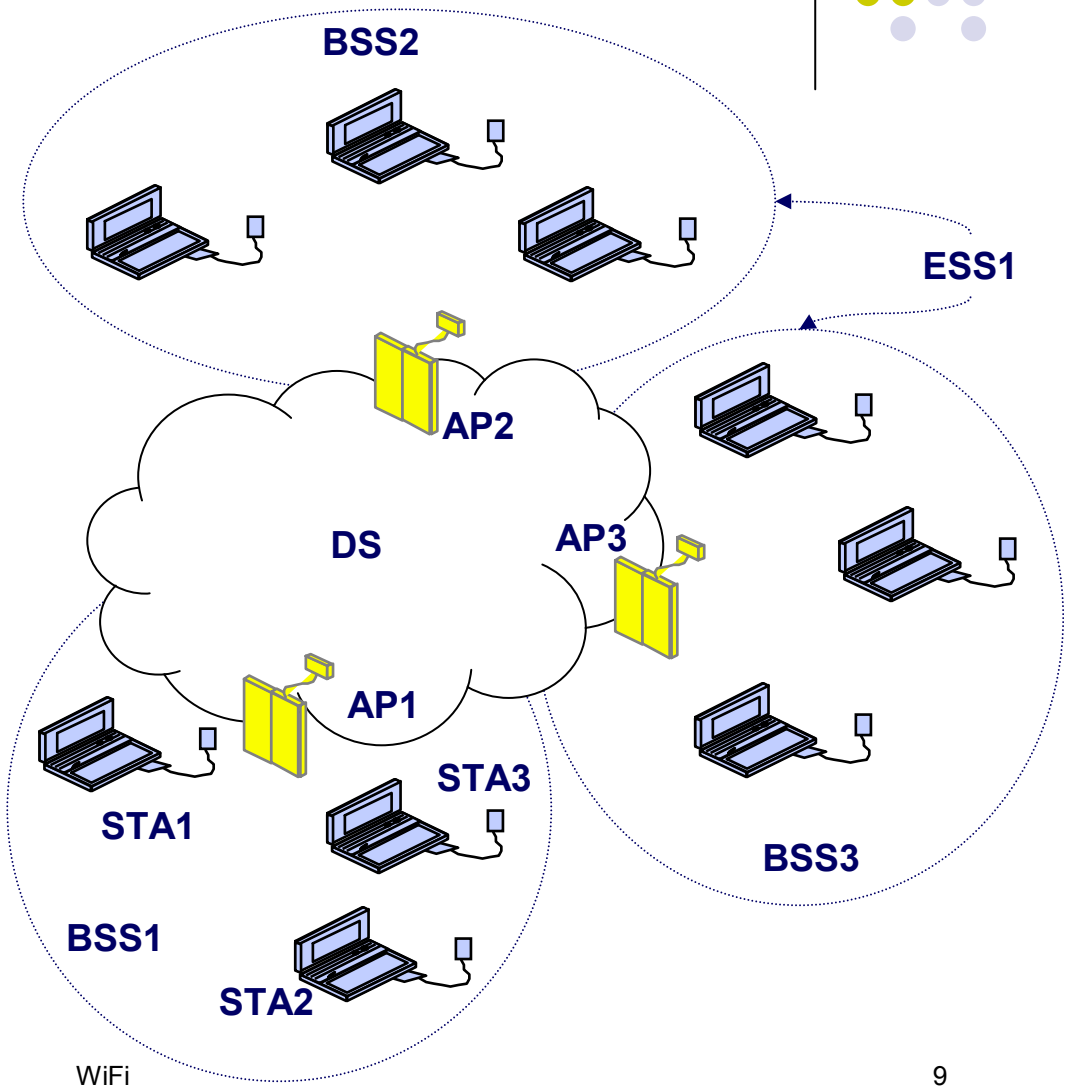
    (Beacon,Probe Request ,Probe Response,

    Association request , Association response …)
  - Data

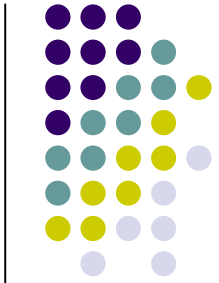
    (Data, Null Data, Data_CF_Ack , ….)

Infrastructure Model includes: (most common)

- Stations (STA)
  - any wireless device
- Access Point (AP)
  - connects BSS to DS
  - controls access by STA's
- Basic Service Set (BSS)
  - a region controlled by an AP
  - mobility is supported within a single BSS
- Extended Service Set (ESS)
  - a set of BSS's forming a virtual BSS
  - mobility is supported between BSS's in an ESS
- Distribution Service (DS)
  - connection between BSS's

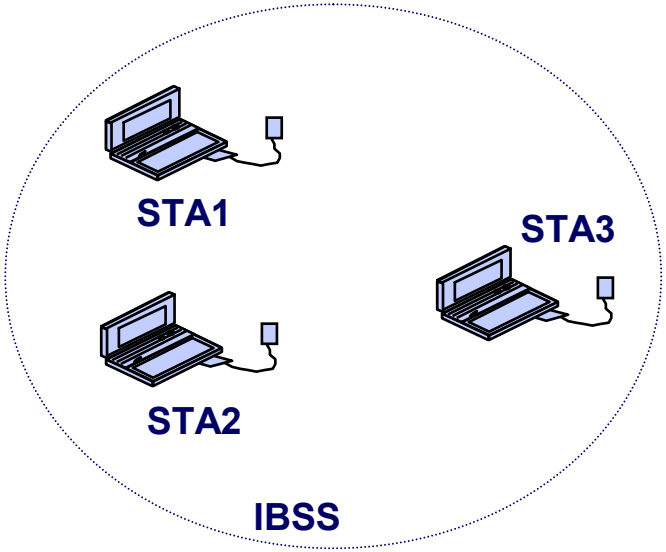


The 802.11 MAC supports infrastructure and ad hoc network models

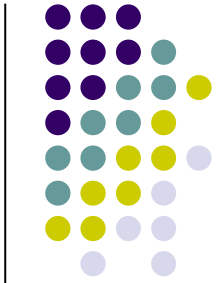


Ad Hoc Model includes:

- Stations (STA)
  - any wireless device
  - act as distributed AP
- Independent Basic Service Set (IBSS)
  - BSS forming a self contained network
  - no AP and no connection to the DS



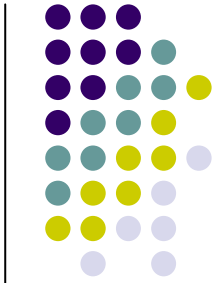
Two types of access to air



- **DCF** (distributed coordination function)
  means everybody can speak and try
  to get air : 100% on the market

- **PCF** (point coordination function)
  means ONE point coordinator (BOSS)
  who will allowed you to speak
  (like in bluetooth)

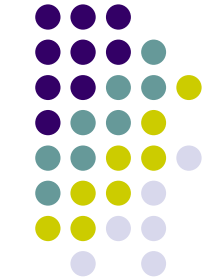
Summary of required features and difficulties vs 802.11 features



- **Features**
  - High speed operation (PHY only)
  - Fair access (DCF, PCF)
  - Time-bounded access (PCF)
  - Flexible configuration (BSS, IBSS)
  - Security (WEP)
  - Mobility support (ESS)
  - Low power (PS)

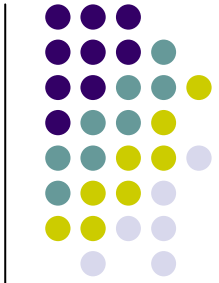
  - **Difficulties**
    - Hidden terminals (RTS/CTS)
    - Capture (CSMA/CA, ACK)
    - Noise and interference (ACK, frag)
    - Limited spectrum (licencing, PHYs)

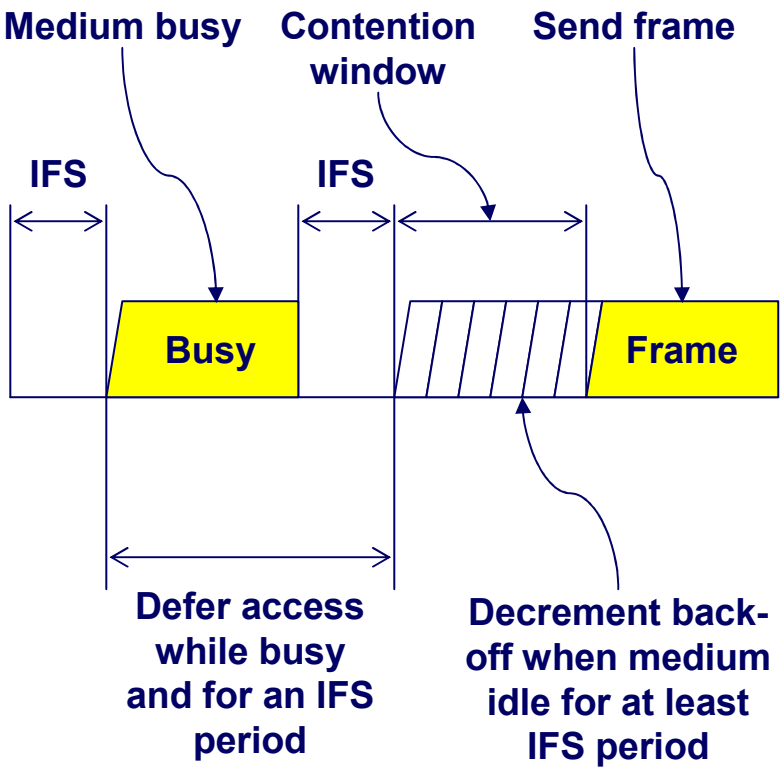
The 802.11 MAC basic Distributed Co-ordination Function (DCF) access scheme uses a CSMA/CA based protocol



- If the STA detects the medium is busy when attempting to send a packet then:
  - the STA starts a random back-off timer
  - the randomisation parameters depend on previous transmission successes/failures
  - the back-off timer runs once the medium has been idle for an IFS period
- An STA may transmit a packet after sensing the medium is idle for an Inter Frame Space (IFS) period
  - the back-off timer suspends when the medium is busy and does not restart until medium is idle for an IFS period
  - The STA may transmit when the back-off timer expires
- The state (busy or idle) of the medium is determined using:
  - physical carrier sense
  - virtual carrier sense, based on reservations in received packets. These reservations set the NAV timer. The medium is considered busy until the NAV timer expires

The 802.11 MAC basic Distributed Co-ordination Function (DCF) access scheme uses a CSMA/CA based protocol

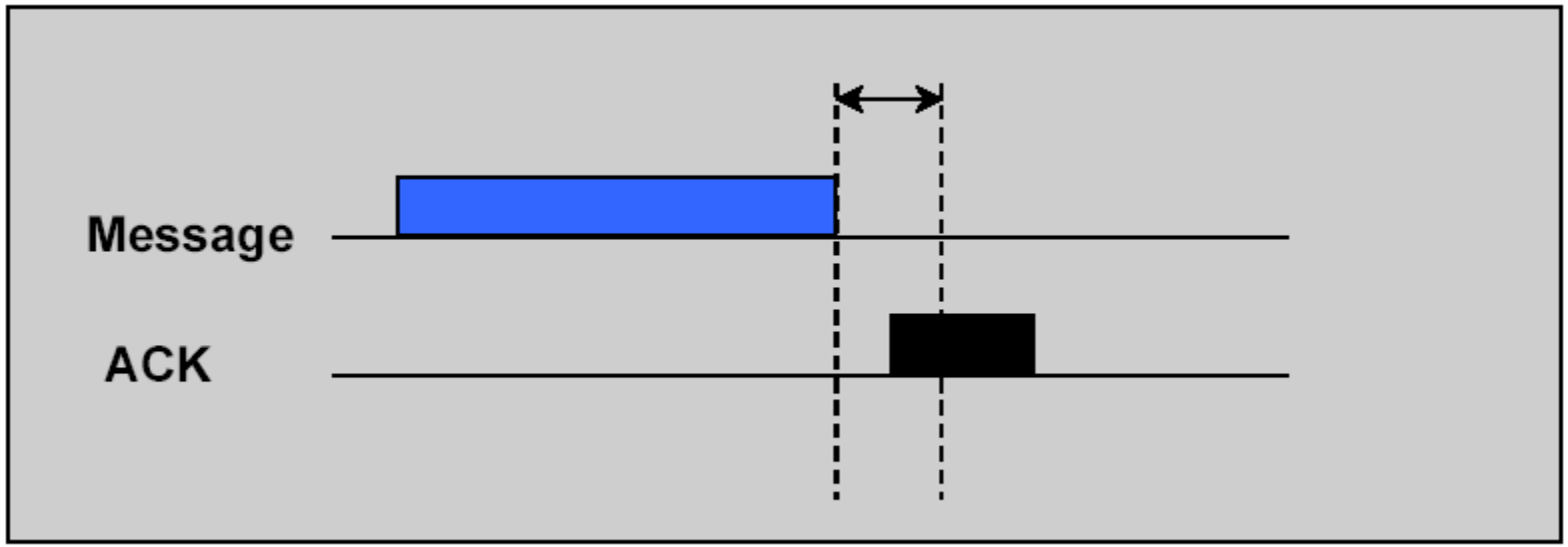




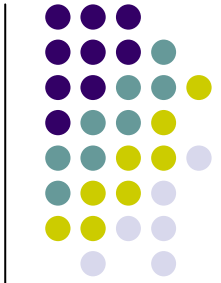
Acknowledgment

Collisions still can occur (interference; incapability of sensing other carrier)

- ★ IEEE 802.11 defines “low-level” ACK protocol
- ★ Provides faster error recovery
- ★ Makes presence of high level error recovery less critical



Security



- **WEP** (wired equivalent privacy) 64/128 bits

  Using RC4 algorithm, almost permanent key, very week

  security, able to crack by collecting statistic

  Current security level for 99.9% products on the market.

- **TKIP** (temporal key integrity protocol)

  Used RC4 algorithm with with a 128-bit "temporal key"

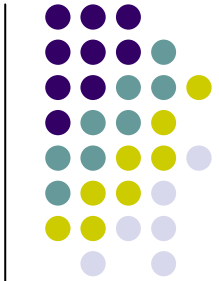
  but changes temporal keys every 10,000 packets and key dependes on address and sequence number.

  Will be required to obtain WiFi certification from 09/01/03

- **AES** (Advanced Encryption Standard)

  New, much more stronger encryption, protect against hacker frames in insertion. Need hardware accelerator. Optional feature.

Why do we need 11A/11B/11G ?



- 11B: 2.4 GHz , CCK modulation
  Rates from 1 to 11Mbps , on market from 1999
- 11A: 5.0 GHz , OFDM modulation
  Rates from 6 to 56 Mbps , on market from 2002
- 11G: 2.4 GHz, CCK+OFDM modulation
  Rates from 6 to 56 Mbps, on market from 2003 and …
  most popular today !!!

Advantages of 2.4 GHz PHY:

Low frequency, better wall penetration, less sensitive to multipath

3 not-overlapped channels

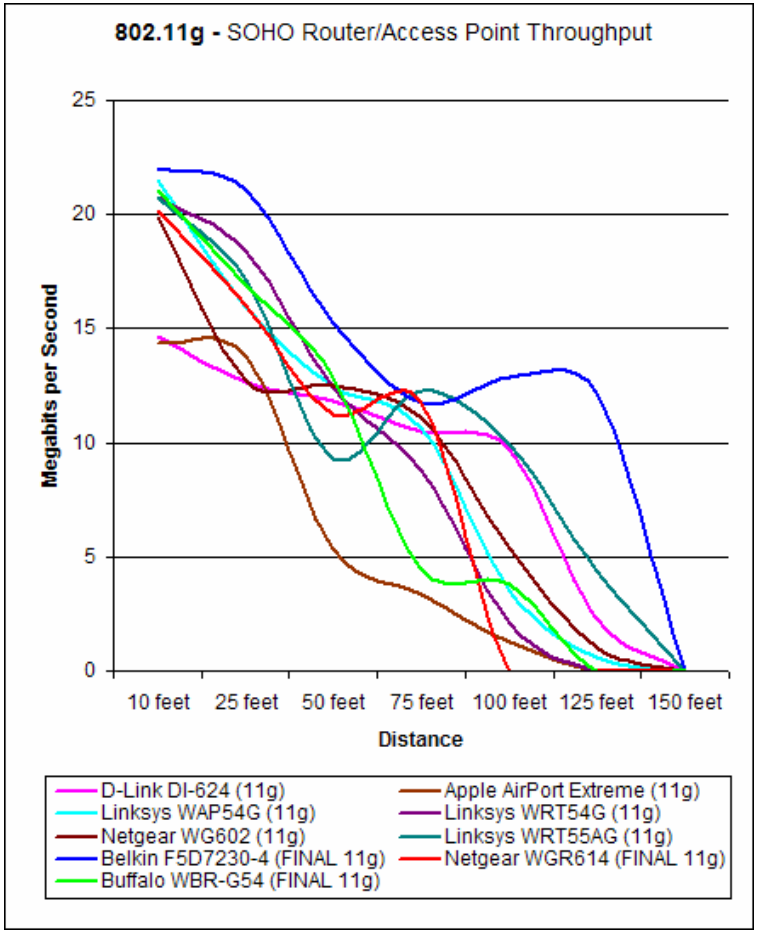
Advantages of 5.0 GHz PHY:

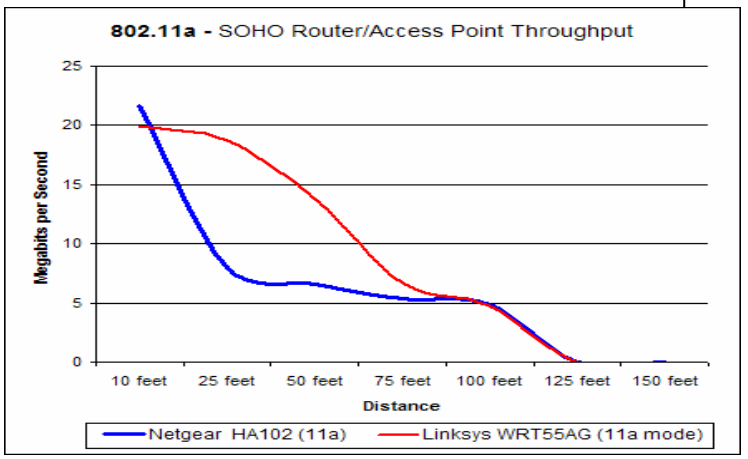
Less devices on the market (no microwave, no blue tooth …)

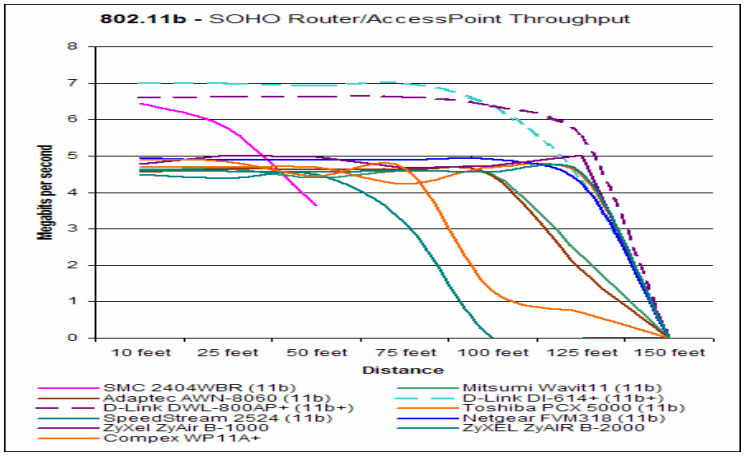
8 not-overlapped channels

Range: almost the same …

802.11 a/b/g performance
11A/G max throughput ~22 Mbps , not 54 Mbps (!!!)
11B max throughput ~6 Mbps



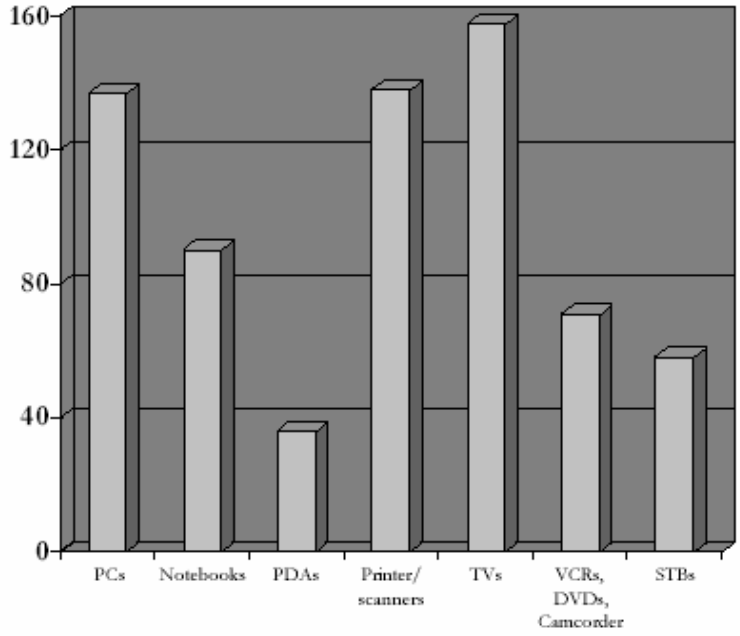




Wlan market Scenarios

WLAN Market Scenarios

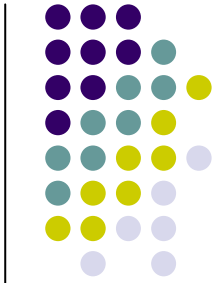
Appliances in mio. 2005



WLAN Penetration Levels 2005

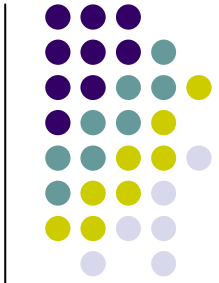
	Worst case	Best Case
PC	12%	50%
Notebooks	24%	100%
PDAs	12%	50%
Printer/ scanners	12%	20%
TVs	8%	15%
VCRs, DVDs, Camcorder	8%	15%
STBs	8%	15%

IEEE 802.16 for MAN==Metropolitan Area Network New alternative to DSL/Cable modems



- **IEEE 802.16 Progress**
- Work on 802.16 started in July 1999. Four years into its mission, the IEEE 802.16 Working Group on Broadband Wireless Access has delivered a base and three follow-on standards.
- IEEE 802.16 (“Air Interface for Fixed Broadband Wireless Access Systems”) was approved in December 2001. This standard is for wireless MANs operating at frequencies between 10 and 66 GHz.
- IEEE 802.16.2, published in 2001, specifies a “recommended practice” to address the operation of multiple, different broadband systems in the 10-66 GHz frequency range.
- In January of this year, the IEEE approved an amendment to 802.16, called 802.16a, which adds to the original standard operation in licensed and unlicensed frequency bands from 2-11 GHz.
- 802.16c, which was approved in December 2002, is aimed at improving interoperability by specifying system profiles in the 10-66 GHz range.

802.11/802.16



Summary

	IEEE 802.11	IEEE 802.16a
Max Speed	54 Mbps (11a & g)	70 Mbps
Range	100 m	40 km
QoS	None	Yes
Coverage	Indoor Opt.	Outdoor Opt.
Users	Hundreds	Thousands
Service Levels	None	Yes

Comparisons: 3G vs. WiFi

	3G	WiFi
Standard	WCDMA,CDMA2000	IEEE 802.11
Max Speed	2 Mbps	54 Mbps
Operations	Cell phone companies	Individuals, WISP
License	Yes	No
Coverage Area	Several km	About 100m
Advantages	Range, mobility	Speed, cheap
Disadvantages	Relatively slow Expensive	Short range

It's all about the money

Comparisons: 3G vs. Wi-Max

	3G	Wi-Max (Wider-Fi)
Standard	WCDMA,CDMA2000	IEEE 802.16
Max Speed	2 Mbps	10 to 100 Mbps
Operations	Cell phone companies	Individuals, WISP
License	Yes	Yes/No
Coverage Area	Several km	Several km
Advantages	Range, mobility	Speed, long range
Disadvantages	Relatively slow Expensive	Interference issues?