COEN-4720 Embedded Systems

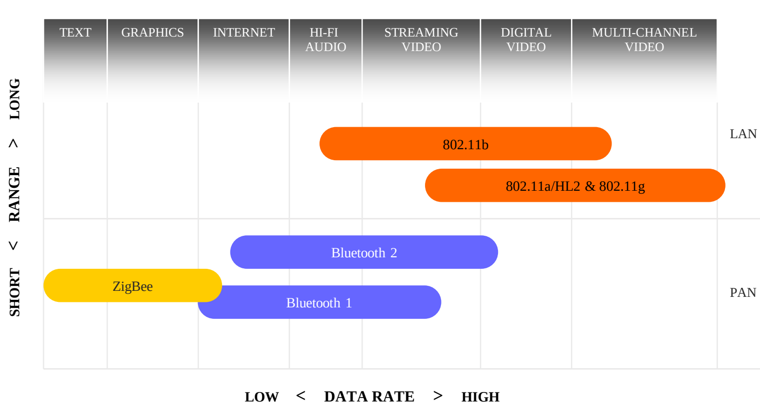
Lecture 9
WiFi

Cris Ababei
Dept. of Electrical and Computer Engineering
MARQUETTE UNIVERSITY

BE THE DIFFERENCE.

Wireless Technologies: WiFi

- Bluetooth
- WiFi
- Cellular
- 3G (3rd Generation)
- UWB (Ultra Wide Band)
- FSO (Free Space Optics)
- WiMAX
- ZigBee
- …



Outline

- WiFi
  - Introduction
  - History
  - Standards
  - Security
  - Network architectures
  - Requirements
  - Antennas
- ESP8266 module and example

3

3

What is a Wireless LAN?

- **Wireless LAN (WLAN)** - provides all the features and benefits of traditional LAN technologies such as Ethernet, but without the limitations of wires or cables.

4

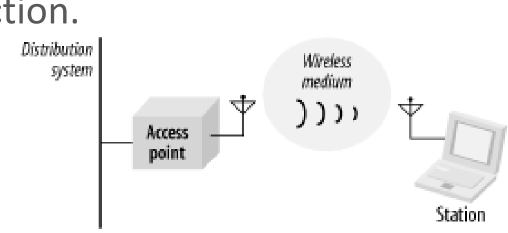
What is WiFi?

- Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices to connect to the network.
- The **standard** for wireless local area networks (WLANs).
- It is like a common "language" that all the devices use to communicate to each other. If you have a standard, people can make all sorts of devices that can work with each other.
- The governing body that owns the term Wi-Fi, **the Wi-Fi Alliance**, defines it as any WLAN products that are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards.

5

What is WiFi?

- The way Wi-Fi works is through the use of radio frequency (RF) signals.
- The wireless adapter card that is found inside of computers then uses the data that is being sent to change it into a radio signal to be transmitted by the antenna.
- A router then receives these signals and decodes them in order to send the information contained within to the Internet via a Local Area Network or a wired Ethernet connection like a cable network connection.



6

Figure 1.

Select the Best Wireless Standard for Your Application

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM 1XRTT/CDMA
System resource	4-32 KB	250 KB+	1 MB ±	16 MB+
Battery life (days)	100-1,000+	1-7	0.1-5	1-7
Nodes per network	255/65,000+	7	30	1-1000
Bandwidth (KBps)	20-250	720	11,000+	64-128
Range (meters)	1-75+	1-10+	1-100	1000+

Figure 2.

Which Wireless Standard?

	Application Focus	Success Metrics
ZigBee	Monitoring and control	Reliable, secure networking Protocol simplicity Low power consumption
Bluetooth	Cable replacement	Low incremental cost Ease of use/convenience Moderate data rate
Wi-Fi	Web, email, and video	High data throughput Flexibility (work and home) Hot Spot connectivity
GPRS / GSM	Wireless voice and data	Broad geographic coverage Datacentric pricing plans Network build-out

7

Advantages

- Freedom – You can work from any location that you can get a signal.
- Setup Cost – No cabling required.
- Flexibility – Quick and easy to setup in temp or permanent space.
- Scalable – Can be expanded with growth.
- Mobile Access – Can access the network on the move.

8

Disadvantages

- Speed – Slower than cable.
- Range – Affected by various medium.
  - Travels best through open space.
  - Reduced by walls, glass, water, etc.
- Security – Greater exposure to risks.
  - Unauthorized access.
  - Compromising data.
  - Denial of service.

9

History of Wi-Fi

- **In 1985, FCC allowed the opening of several bands of the wireless spectrum, allowing those bands to be used without government license.**
- The bands were taken from the scientific, medical, and industrial bands of the wireless spectrum.
- FCC made these bands available for communication purposes.
- Using *spread spectrum technology*, which spreads a radio signal over wide range of frequencies, they were able to steer around interference from other equipment.
- When Ethernet became popular vendors came to the realization that a wireless standard was best.

10

History of Wi-Fi (Continued)

- In 1988, the NCR Corporation wanted to use the unlicensed spectrum to hook up wireless cash register, they looked into getting a standard started.
- Victor Hayes and Bruce Tuch were hired and they went to the IEEE and created the committee known as 802.3.
- Vendors took a while to agree on an acceptable standard due to the fragmented market.
- In 1997, the committee agreed on a basic specification that allowed for a data-transfer rate of two megabits per second.
- Two technologies, known as frequency hopping and direct-sequence transmission, allowed for this data-transfer rate.

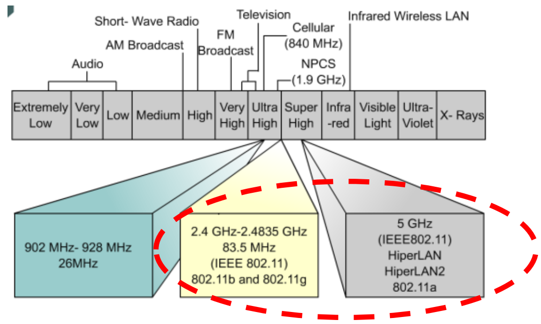
11

History of Wi-Fi (Continued)

- The new standard was finally published in 1997, and engineers immediately began working on prototype equipment that was compliant.
- **Two variants 802.11b (operates in 2.4GHz band), and 802.11a (operates in 5.8GHz band) were ratified in December 1999 and January 2000 respectively.**
- In August 1999, the Wireless Ethernet Compatibility Alliance (WECA) was created with the intention to assure compatibility between products from various vendors.
- A consumer-friendly name was need for this new technology and the term “Wi-Fi” came to be.
- Apple was the first to supply their computers with Wi-Fi slots on all their laptops, thus sparking the mainstream penetration of Wi-Fi.

12

US Frequency Bands



Band	**Frequency range**
UHF ISM	902-928 MHz
S-Band	2-4 GHz
S-Band ISM	2.4-2.5 GHz
C-Band	4-8 GHz
C-Band satellite downlink	3.7-4.2 GHz
C-Band Radar (weather)	5.25-5.925 GHz
C-Band ISM	5.725-5.875 GHz
C-Band satellite uplink	5.925-6.425 GHz
X-Band	8-12 GHz
X-Band Radar (police/weather)	8.5-10.55 GHz

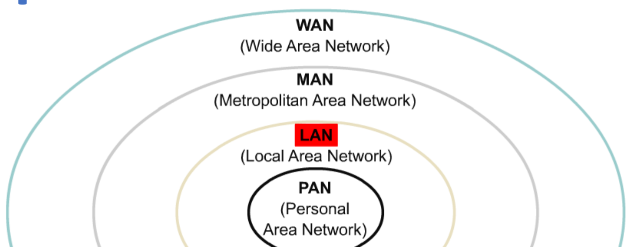
13

Wi-Fi Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

14

Atmosphere: the Wireless Medium



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HyperLAN 2	802.11, MMDS, LMDS	GSM, GPRS CDMA, 2.5- 3G
Speed	< 1Mbps	1- 54+ Mbps	22Mbps+	10- 384 Kbps
Range	Short	Medium	Medium- long	Long
Applications	peer-to-peer device-to-device	Enterprise networks	Fixed, last mile access	PDAs, Mobile phones, cellular access

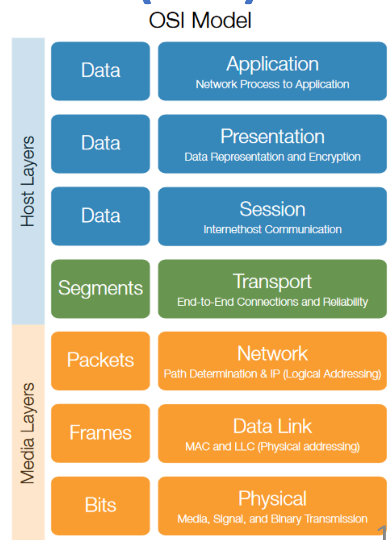
- The ability of radio waves to pass through walls and cover great distances makes wireless a versatile way to build a network.

IEEE 802.11 Standards Activities

- 802.11a: 5GHz, 54Mbps
- **802.11b: 2.4GHz, 11Mbps**
- 802.11d: Multiple regulatory domains
- 802.11e: Quality of Service (QoS)
- 802.11f: Inter-Access Point Protocol (IAPP)
- **802.11g: 2.4GHz, 54Mbps**
- 802.11h: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
- 802.11i: Robust Security Network
- 802.11j: Japan 5GHz Channels (4.9-5.1 GHz)
- 802.11k: Measurement
- 802.11n: High throughput standard > 100Mbps. Backwards compatible with a,b,g

Open Systems Interconnection (OSI) Model

- OSI model describes how information moves from an application program running on one networked computer to an application program running on another networked computer.

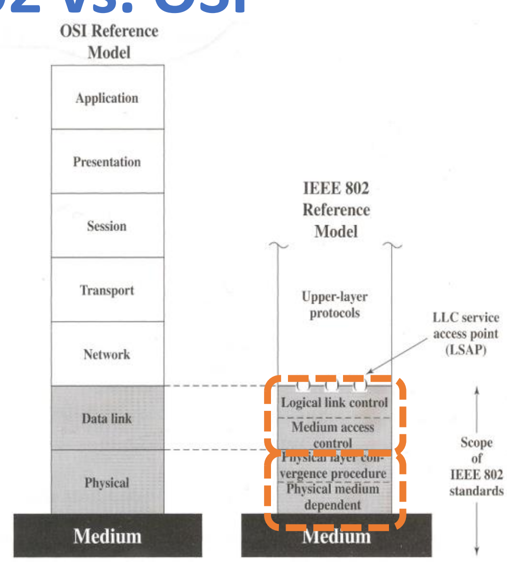


17

17

IEEE 802 vs. OSI

- **Data Link Layer**
  - Logical Link Control (LLC)
  - Medium Access Control (MAC)
- **Physical Layer**
  - Physical Layer Convergence Procedure (PLCP)
  - Physical Medium Dependent (PMD)

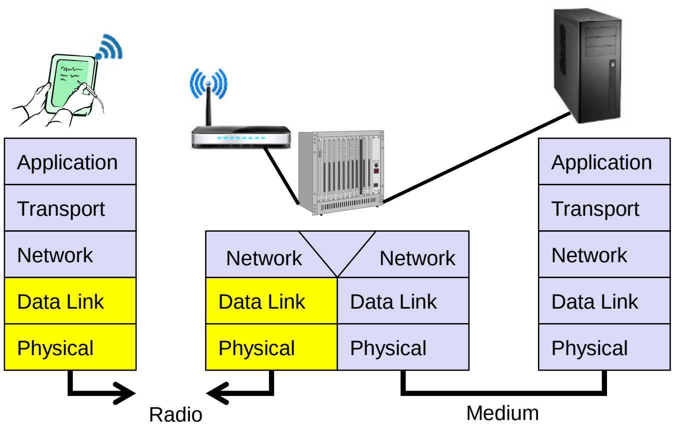


IEEE 802 Protocol Layers Compared to OSI Model

18

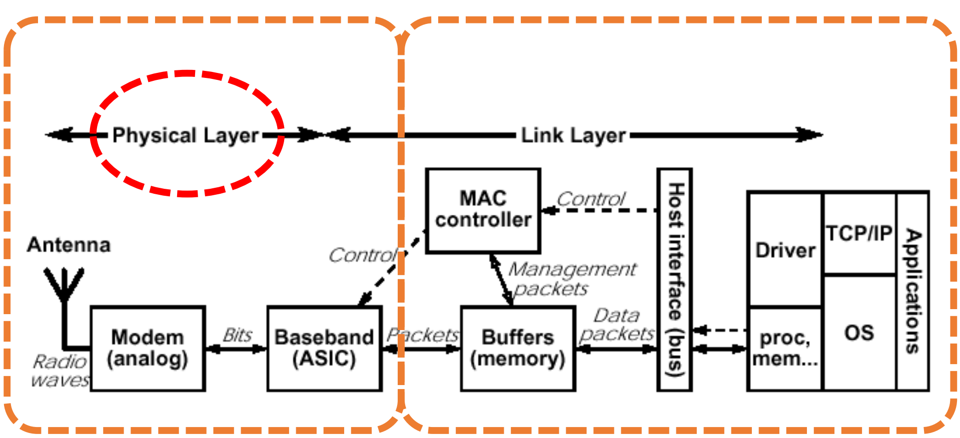
802.11 Standard

- Standard 802.11 is primarily concerned with the lower layers of the OSI model



19

Functional Diagram



20

802.11 PHY (Physical Layer) Technologies

- Three types of radio transmission within the unlicensed 2.4GHz frequency bands:
  1) Frequency hopping spread spectrum (FHSS) 802.11b (not used)
  2) Direct sequence spread spectrum (DSSS) and Complementary Code Keying (CCK) **802.11b**
  3) Orthogonal frequency-division multiplexing (OFDM) **802.11g**
- One type of radio transmission within the unlicensed 5GHz frequency bands:
  1) **Orthogonal frequency-division multiplexing (OFDM) 802.11a**

21

Orthogonal Frequency-Division Multiplexing (OFDM)

- A method of encoding digital data on multiple carrier frequencies
- Keeps the modulated carriers orthogonal
- Each carrier is modulated using BPSK/QPSK/M-ary QAM, etc.
- Do not interfere with each other
- Overlap of frequency response is possible as opposed to FDM where inter-carrier spacing is a must
- Frequency responses of the carriers overlap at zero crossings avoiding Inter Carrier Interference (ICI)
- Effectively squeezes multiple modulated carriers tightly together, reducing required bandwidth
- Popular scheme for wideband digital communication (digital television, DSL Internet access, wireless networks, 4G,…)

22

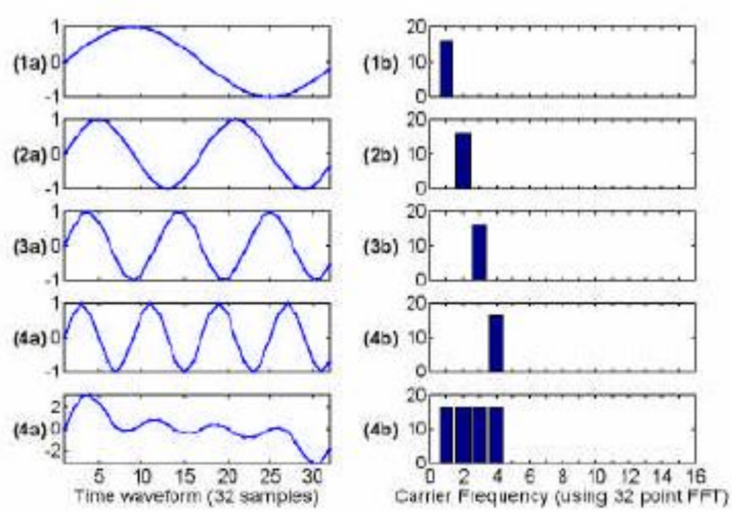
OFDM Advantages

- Allows carriers to overlap (no guard band), resulting in lesser wasted bandwidth without any Inter Carrier Interference (ICI)
- High data rate distributed over multiple carriers resulting in lower error rate
- Permits higher data rate as compared to FDM
- Increased security and bandwidth efficiency possible using CDMA-OFDM (MC-CDMA)
- Simple guard intervals make the system more robust to multipath effects

23

What is OFDM?

Orthogonality in Time domain…



24

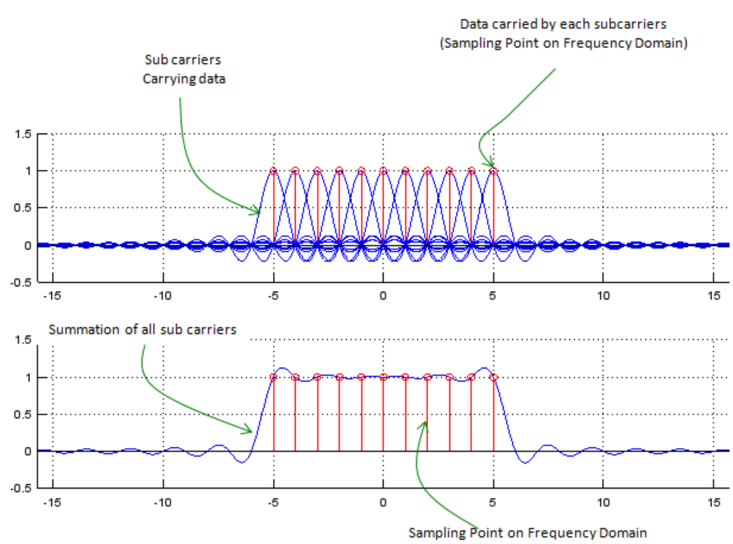
What is OFDM?

- OFDM:
  - **Orthogonal**
  - **Frequency Division**
  - **Multiplexing**
- Technology that splits a wide frequency band into many small frequencies (we call these split-frequencies as **subcarriers**) and carry data onto each of these subcarriers (see illustration on next slide).
- We "divide a wide frequency band" into multiple small/narrow frequencies - this is the meaning of "**Frequency Division**".
- Because all data on each of these subcarriers are transmitted simultaneously, we can say this is a kind of "**Multiplexing**".

25

25

What is OFDM?



26

What is OFDM?

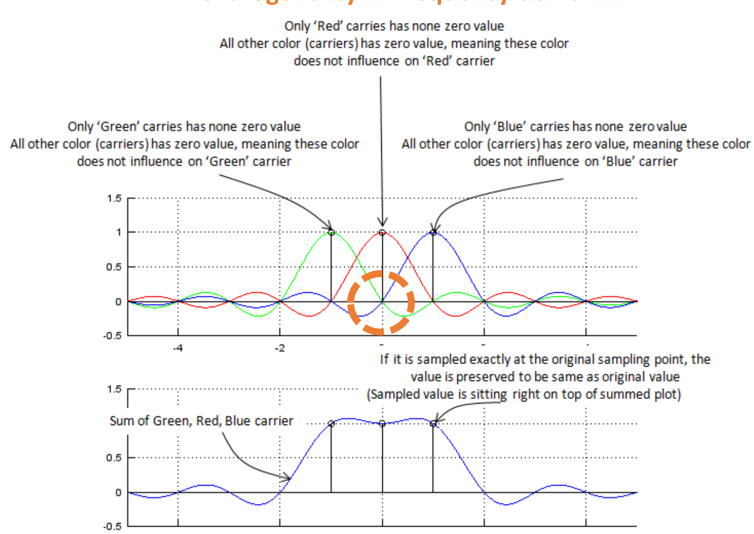
- There is a tradeoff involving **Number of Subcarriers**:
  - Cannot be too large because high possibility of interference between adjacent subcarriers
  - We would like it as large as possible to increase **Data Rate**
- OFDM splits the band into multiple subcarriers as follows (and illustrated on next slide):
  - At each sampling point in frequency domain there is **only one carrier which has non-zero value** and all other sub carriers has zero value at the sampling point.
  - It means that even though multiple subcarriers coexist, they are all independent and do not influence each other.
  - This characteristic is referred to as "**Orthogonal**".

27

27

What is OFDM?

Orthogonality in Frequency domain...



28

28

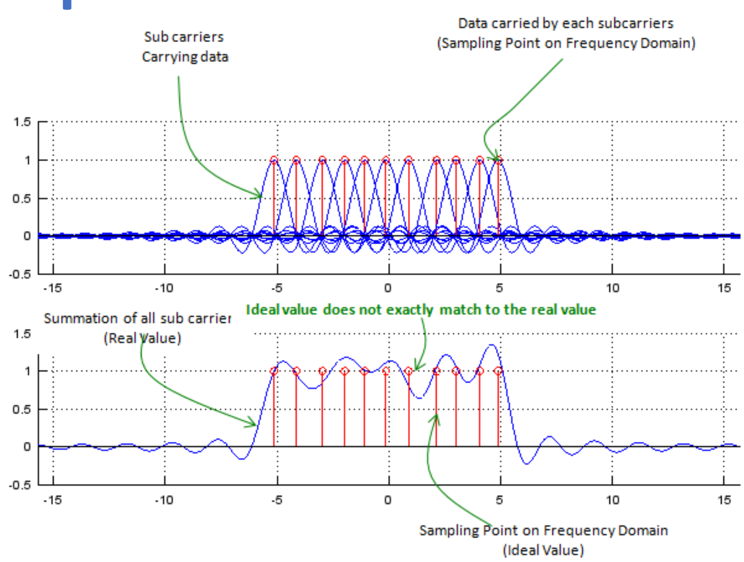
What is OFDM?

- OFDM is a very good method of utilizing the given frequency band wisely. But, it has a drawback:
  - For this method to work efficiently, the space between subcarriers must be maintained exactly at the specified position to satisfy the condition of orthogonality.
- Unfortunately, in reality:
  - Frequency drift of subcarriers– common causes for frequency drift include “Fading” and “Doppler effect”.
  - That dictates how we determine the frequency space for which the system can tolerate the signal distortion due to frequency drift.
- Example when the space between subcarriers is not maintained accurately and subcarriers are drifting around – see next slide.

29

29

Impact of Subcarriers Drift



30

30

Designing OFDM Transmitter

- Assume we need to send the following data bits using OFDM:
  - D = {d0, d1, d2, …}
- **First design parameter** that is considered in designing the OFDM transmitter:
  - Number of subcarriers required.
  - Assume that we have n subcarriers (named from 0 to n-1).
- Subcarriers are centered at frequencies that are orthogonal to each other (usually multiples of frequencies).
- **Second design parameter** is the modulation format to be used.
- An OFDM signal can be constructed using any of several digital modulation techniques: BPSK, QPSK, QAM, etc.

31

31

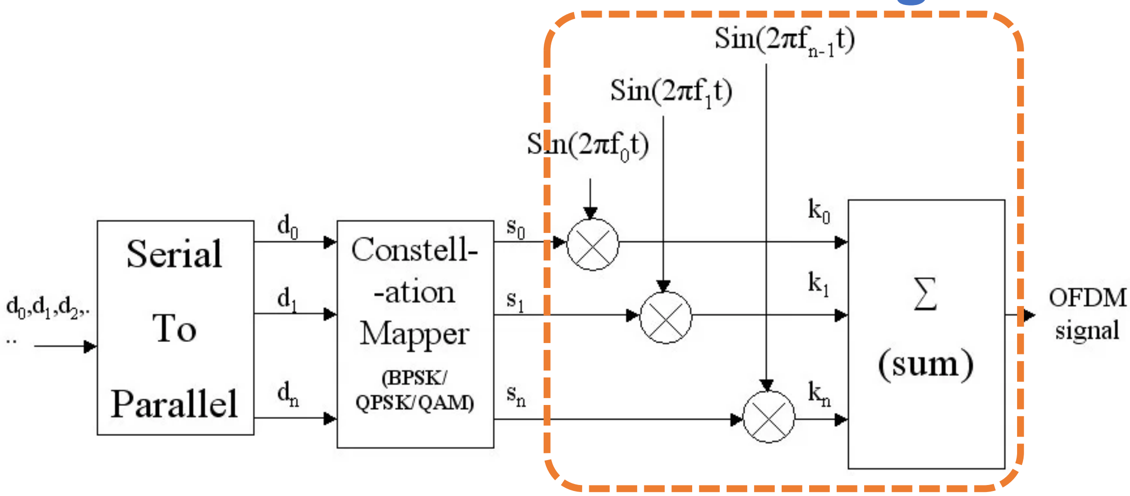
Designing OFDM Transmitter

- Data (D) must be first converted from serial into parallel
  - Serial to Parallel converter takes serial stream of input bits and outputs N parallel streams (indexed from 0 to n-1)
  - These parallel streams are individually converted into the required digital modulation format (BPSK, QPSK, QAM, etc.)
  - Call this output S0, S1, …, Sn-1
- Conversion of parallel data (D) into digitally modulated data (S)
  - Usually achieved by a constellation mapper
  - Essentially a look up table (LUT)
- Output S0, S1, …, Sn-1 must then be superimposed on the required orthogonal subcarriers for transmission.
  - Achieved by a series of N parallel sinusoidal oscillators tuned to n orthogonal frequencies (f0, f1, …, fn-1).
- Finally, resultant output from the n parallel arms are summed-up together to produce the OFDM signal.

32

32

OFDM Transmitter Block Diagram



NOTE: For simplicity of explanation, the usual IFFT block that is used in actual OFDM systems, is not shown in this block diagram

33

33

Example

- **OFDM transmission with BPSK modulation**
- **5 orthogonal subcarriers are assumed**

Data = 1,0,1,0,1,1,1,1,0,1,0,0,0,1,0,1,0,0,1,1

Time	d0	d1	d2	d3	d4
t1	1	0	1	0	1
t2	1	1	1	0	1
t3	0	0	0	1	0
t4	1	0	0	1	1

Serial to Parallel Converter

Time	S0	S1	S2	S3	S4
t1	1	-1	1	-1	1
t2	1	1	1	-1	1
t3	-1	-1	-1	1	-1
t4	1	-1	-1	1	1

BPSK mapping

Multiplying by orthogonal frequency subcarriers

Time	k0	k1	k2	k3	k4	
$t1+\Delta$	$1x \sin(2\pi F_0 t)$	$-1x \sin(2\pi F_1 t)$	$1x \sin(2\pi F_2 t)$	$-1x \sin(2\pi F_3 t)$	$1x \sin(2\pi F_4 t)$	$\Sigma \rightarrow OFDM_0$
$t2+\Delta$	$1x \sin(2\pi F_0 t)$	$1 x \sin(2\pi F_1 t)$	$1 x \sin(2\pi F_2 t)$	$-1 x \sin(2\pi F_3 t)$	$1 x \sin(2\pi F_4 t)$	$\Sigma \rightarrow OFDM_1$
$t3+\Delta$	$-1 x \sin(2\pi F_0 t)$	$-1 x \sin(2\pi F_1 t)$	$-1 x \sin(2\pi F_2 t)$	$1 x \sin(2\pi F_3 t)$	$-1 x \sin(2\pi F_4 t)$	$\Sigma \rightarrow OFDM_2$
$t4+\Delta$	$1x \sin(2\pi F_0 t)$	$-1 x \sin(2\pi F_1 t)$	$-1 x \sin(2\pi F_2 t)$	$1 x \sin(2\pi F_3 t)$	$1 x \sin(2\pi F_4 t)$	$\Sigma \rightarrow OFDM_3$

34

Example

- **OFDM transmission with pi/4 shifted QPSK modulation**
- **5 orthogonal subcarriers are assumed**

Data = 1,0,1,0,1,1,1,1,0,1,0,0,0,1,0,1,0,0,1,1

Time	d0	d1	d2	d3	d4
t1	1	0	1	0	1
t2	1	1	1	0	1
t3	0	0	0	1	0
t4	1	0	0	1	1

Serial to Parallel Converter

Time	S0	S1	S2	S3	S4
t2+Δ	-1-j	-1+j	-1-j	1+j	-1-j
t4+Δ	-1+j	1+j	1+j	-1-j	-1+j

Pi/4 shifted QPSK mapping (with gray coding)

Multiplying by orthogonal frequency subcarriers

Time	k0	k1	k2	k3	k4	
t2+Δ	(-1-j) x $\sin(2\pi F_0 t)$	(-1+j) x $\sin(2\pi F_1 t)$	(-1-j) x $\sin(2\pi F_2 t)$	(1+j) x $\sin(2\pi F_3 t)$	(-1-j) x $\sin(2\pi F_4 t)$	Σ → $OFDM_0$
t4+Δ	(-1+j) x $\sin(2\pi F_0 t)$	(1+j) x $\sin(2\pi F_1 t)$	(1+j) x $\sin(2\pi F_2 t)$	(-1-j) x $\sin(2\pi F_3 t)$	(-1+j) x $\sin(2\pi F_4 t)$	Σ → $OFDM_1$

35

Inverse Fast Fourier Transform (IFFT)

- Generally, an OFDM signal can be represented as:

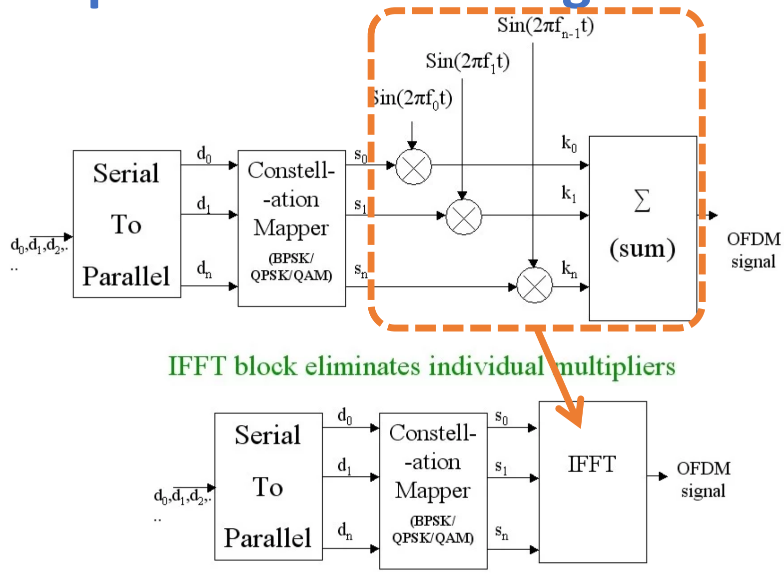
$$OFDM\ signal = c(t) = \sum_{n=0}^{N-1} s_n(t) sin(2\pi f_n t)$$

- s(t) = symbols mapped to chosen constellation (BPSK/QPSK/QAM, ...)
- fn = orthogonal frequency
- This equation can be thought of as an IFFT process

36

36

OFDM Implementation Using FFT and IFFT

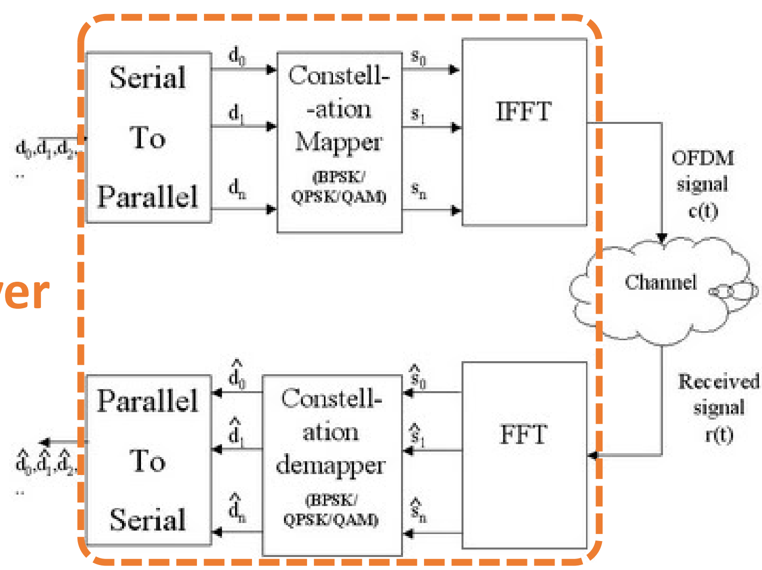


37

37

Complete OFDM Communication System

Transceiver



38

802.11b Standard

- Well-supported, stable, and cost effective, but runs in the 2.4 GHz range that makes it prone to interference from other devices (microwave ovens, cordless phones, etc.) and also has security disadvantages.
- Limits the number of access points in range of each other to three.
- Has **11 channels**, with 3 non-overlapping, and supports rates from 1 to 11 Mbps, but realistically about 4-5 Mbps max.
- Uses direct-sequence spread-spectrum (DSSS) technology.

39

802.11g Standard

- Extension of 802.11b, with the same disadvantages (security and interference).
- Has a shorter range than 802.11b.
- Is backwards compatible with 802.11b; so, it allows for a smooth transition from 11b to 11g.
- Flexible because multiple channels can be combined for faster throughput; but, limited to one access point.
- Runs at 54 Mbps, but realistically about 20-25 Mbps and about 14 Mbps when b associated.
- Uses orthogonal frequency division multiplexing (OFDM).

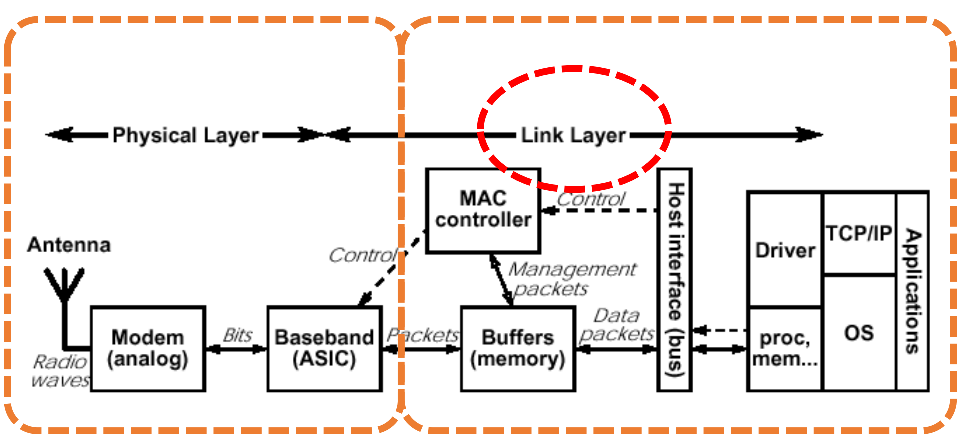
40

802.11a Standard

- Completely different from 11b and 11g.
- Flexible because multiple channels can be combined for faster throughput and more access points can be co-located.
- Shorter range than 11b and 11g.
- Runs in the 5 GHz range; so, less interference from other devices.
- Has **12 channels**, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about 27 Mbps max.
- Uses orthogonal frequency division multiplexing (OFDM).

41

Functional Diagram



42

802.11 – Medium Access Control (MAC) Sub-Layer

- Is responsible for coordinating access to the shared physical air interface so that Access Point (AP) and WiFi stations in range can communicate effectively.
- Takes data from a higher sub-layer called LLC, adds header and tail bytes, and sends them to lower physical layer for transmission. The reverse happens when receiving data from the physical layer. If a frame is received in error, MAC can retransmit it.
- Multiple access is based on carrier sensing, channel contention and random backoff. Due to contention, a WiFi network with many active stations can suffer from low throughput and high latency.

43

43

What is the purpose of MAC layer in 802.11?

- Main function is to control access to a shared medium: the air interface.
- MAC implements the control mechanisms that allow multiple devices to reliably communicate by sharing the medium as specified in the standard.
- Formally, MAC functions include: scanning, authentication, association, power saving and fragmentation.
- MAC sits as a sub-layer within Data Link Layer.
  - It takes a packet of data called MAC Service Data Unit (MSDU) from Logical Link Control (LLC) sub-layer.
  - MAC adds necessary header and tail bytes to form MAC Protocol Data Unit (MPDU).
  - MPDU is then sent to the physical layer for transmission.
  - The reverse flow happens when MAC receives a packet from physical layer.

44

44

How does a WiFi station discover and associate with an AP?

- Two modes of discovery (the station is at liberty to use either or both):

1) Passive scanning:
   - The station looks for beacon frames that are regularly sent by an AP. These frames contain essential information about the network. If there are multiple APs within range, it selects the strongest one. Station then attempts to connect to the AP. Communication happens on the channel in which the AP is operating.

2) Active scanning:
   - The station sends a probe request either to a specific AP or to any AP within range. Either way, it expects a probe response from one or more APs, selects the strongest and attempts to connect to that AP. Since no prior beacon is decoded, station will send its probe on all channels.

45

45

What multiple access scheme (method) is used in 802.11?

- MAC uses what is called:
  - Distributed Coordination Function (DCF) - more prevalent in industry and employs Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
  - Point Coordination Function (PCF)
- There are two parts to CSMA/CA:
  - **Carrier Sensing**:
    - WiFi stations must first sense the air interface.
    - Only if the channel is idle for a specified amount of time (of duration DIFS), they can transmit.
    - DIFS stands for DCF Inter Frame Spacing.
  - **Collision Avoidance**:
    - If channel is sensed busy, station waits till it is free for DIFS duration, then waits for a **random interval** before transmitting.
    - This **randomness** reduces the chances that two waiting stations end up transmitting at the same time. "Collisions" can still occur and they are inferred when no acknowledgement is received by the sender.
    - If ACK is not received, station backs off for a random duration and repeats the process again.

46

46

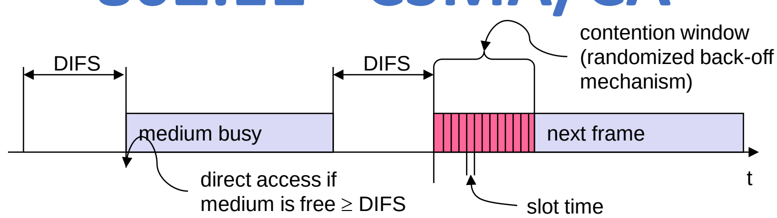
802.11 - MAC Sub-Layer

- **Traffic services**
  - **Asynchronous Data Service (mandatory) - DCF**
  - Time-Bounded Service (**optional**) - PCF
- **Access methods**
  - **DCF (distributed coordination function) CSMA/CA (carrier sense multiple access with collision avoidance): mandatory**
    - Collision Avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF with Request to Send/Clear to Send (RTS/CTS): **optional**
    - Avoids hidden terminal problem
  - PCF (Point Coordination Function): **optional**
    - Access point polls terminals according to a list

47

47

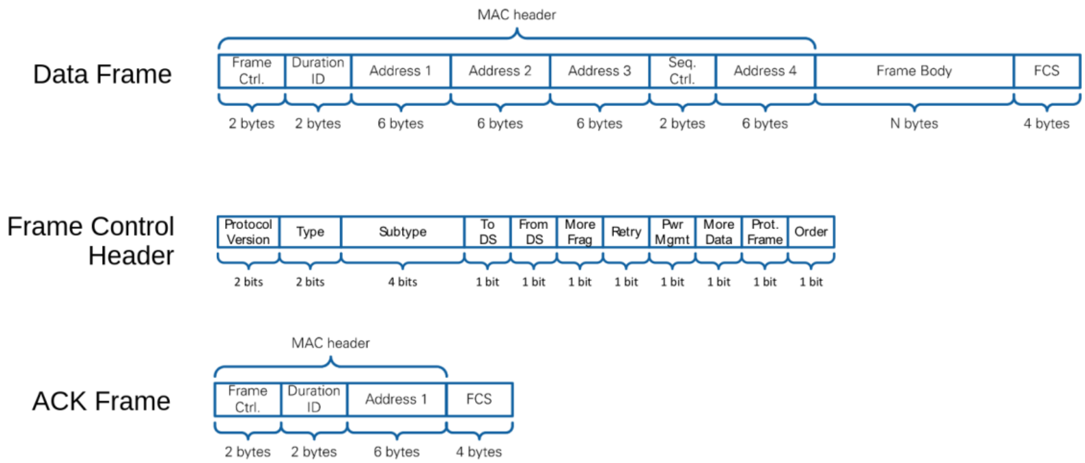
802.11 - CSMA/CA



- Station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- If the medium is free for the duration of a DCF Inter Frame Space (DIFS), the station can start sending (IFS depends on service type)
- If the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- If another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

48

What is the structure of 802.11 MAC frames?



49

49

Techniques in MAC to improve the reliability of communication?

- **Error Detection**: Every MAC frame contains 4-byte Frame Check Sequence (FCS) that is used to detect errors.
- **Retransmission**: For a corrupted frame, receiver will not send an acknowledgment frame. Sender will therefore retransmit the frame.
- **Fragmentation & Reassembly**: When frames are larger, there is a higher chance of collision. MAC can therefore fragment data/management frames and transmit them as individual MAC frames. Any errors, only fragments need to be retransmitted.
- **RTS/CTS (**optional feature**)**: Request-to-Send and Clear-to-Send are used to solve the hidden-node problem. When stations are widely spread around an AP, some may be hidden from others on the wireless channel. RTS/CTS handshaking alleviates this problem and reduces collision.

50

50

Outline

- WiFi
  - Introduction
  - History
  - Standards
  - Security
  - Network architectures
  - Requirements
  - Antennas
- ESP8266 module and example

51

51

Wired Equivalency Protocol (WEP)

- Basic encryption technology.
  - Uses an RC4 stream cipher.
    - Pseudo-random bytes.
  - Two versions: 64-bit and 128-bit versions.
- Built into Wi-Fi certified equipment.
  - Implemented at the MAC level.
- Protects radio signal between device and access point.
  - Does not protect data beyond the access point.
- Uses static encryption keys.
  - Easy to crack.
    - Still better then nothing.

52

Wi-Fi Protected Access (WPA)

- Designed to replace WEP.
  - Firmware update.
  - 128-bit Temporal Key Integrity Protocol (TKIP) encryption.
    - Uses a master key that is regularly changed.
  - User authentication.
  - Data Integrity.
- Protects radio signal between device and access point.
- Built into Wi-Fi certified equipment.
  - Implemented at the MAC level.
- Available in two versions:
  - WPA2 Personal.
  - WPA2 Enterprise.

53

Wi-Fi Protected Access 2 (WPA2)

- Designed to replace WEP.
  - 128-bit Advanced Encryption Standard (AES).
- Based on the IEEE 802.11i standard.
- Provides government level security.
- Also available in two versions:
  - WPA2 Personal.
  - WPA2 Enterprise.

54

Extended EAP

- EAP - Extensible Authentication Protocol.
- Addition to the Wi-Fi Protected Access.
  - Used in internal network.
- Extra security for enterprise and government Wi-Fi LANs.
- Several versions available.

55

Virtual Private Network (VPN)

- Creates a secure virtual “tunnel” from remote device to VPN server.
  - Creates an encryption scheme.
  - Requires authentication.
- Works across the internet.
- Many types and levels of VPN technology.
  - May include hardware and software components.
  - Some very expensive.
  - Windows provides a basic implementation in its server software.

56

Firewall

- Can make the network or computer invisible to the internet.
- Block unauthorized users.
- Monitor and control flow of data to/from a network or computer.
- Many types and levels of firewall technology.
  - Hardware and software combinations
  - Software only versions.
- Many devices provide basic firewall capability.
  - Gateways and access points.
    - Network address translation.
  - Windows XP operating system.

57

Bringing it all together

- Any combination of these security techniques can be used.
- The more security the more of a hassle.
  - Important when supporting users.

58

Four Main Requirements for a WLAN Solution

1. **High availability** — High availability is achieved through system redundancy and proper coverage-area design.
2. **Scalability** — Scalability is accomplished by supporting multiple APs per coverage area, which use multiple frequencies. APs can also perform load balancing, if desired.
3. **Manageability —** Diagnostic tools represent a large portion of management within WLANs. Customers should be able to manage WLAN devices through industry standard APIs, including SNMP and Web, or through major enterprise management applications like CiscoWorks 2000, Cisco Wireless Control System or AirMagnet
4. **Open architecture** — Openness is achieved through adherence to standards such as 802.11a and 802.11b, participation in interoperability associations such as the Wi-Fi Alliance, and certification such as U.S. FCC certification.

59

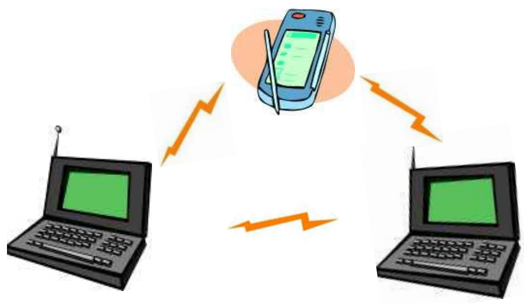
Other requirements

- **Security —** It is essential to encrypt data packets transmitted through the air. For larger installations, centralized user authentication and centralized management of encryption keys are also required.
- **Cost —** Customers expect continued reductions in price of 15 to 30 percent each year, and increases in performance and security. Customers are concerned not only with purchase price but also with total cost of ownership (TCO), including costs for installation.

60

WLAN Architecture - Ad Hoc Mode

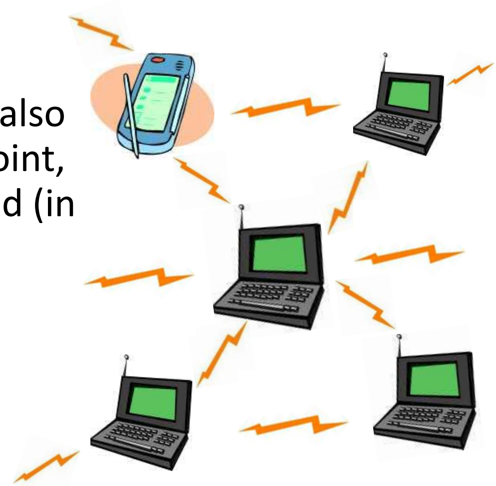
- Peer-to-peer setup where clients can connect to each other directly
- Generally, not used for business networks
- Set up for a special purpose and for a short period of time



61

WLAN Architecture - Mesh

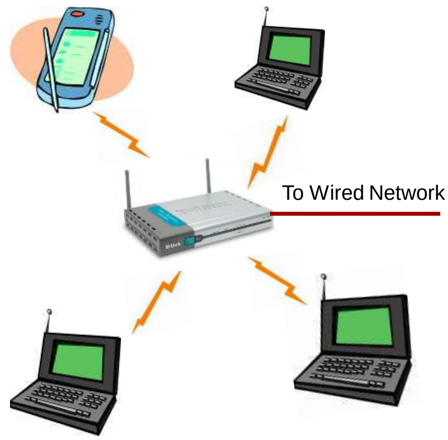
- Every client in the network also acts as an access or relay point, creating a "self-healing" and (in theory) infinitely extensible network.



62

WLAN Architecture - Infrastructure Mode

- Access Point (AP) becomes the hub of a "star topology"
- Any communication has to go through AP
- Multiple APs can be connected together to handle a large number of clients
- Majority of WLANs in homes and businesses



63

Antennas

- All WLAN equipment comes with a built-in omni-directional antenna, but some select products will let you attach secondary antennas that will significantly boost range
- Antenna
  - 2.4 GHz Antennas
  - 5 GHz Antennas

64

Antennas

- Antennas come in all shapes and styles:
  - Omni-directional:
    - Vertical Whip
    - Ceiling mount
  - Directional:
    - Yagi (“Pringles can”)
    - Wall mounted panel
    - Parabolic dish

65

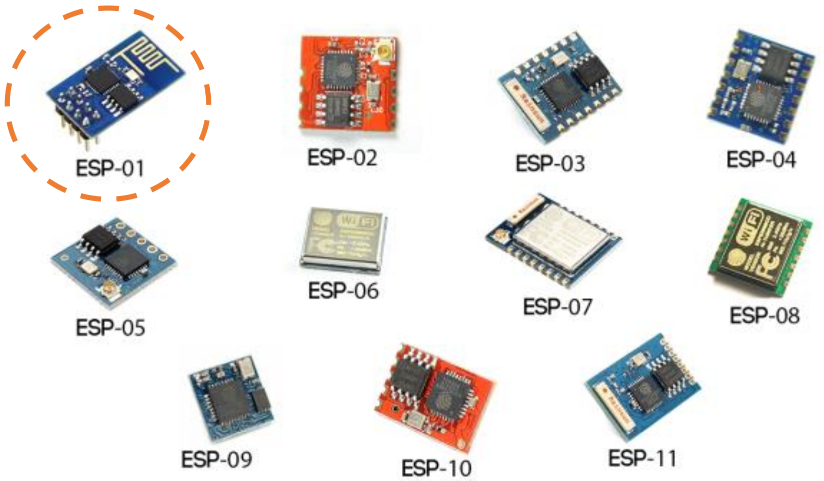
Outline

- WiFi
  - Introduction
  - History
  - Standards
  - Security
  - Network architectures
  - Requirements
  - Antennas
- ESP8266 module and example

66

66

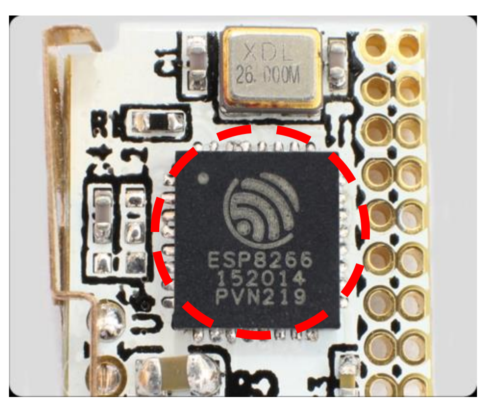
ESP-01 (ESP8266 Circuit) Module



67

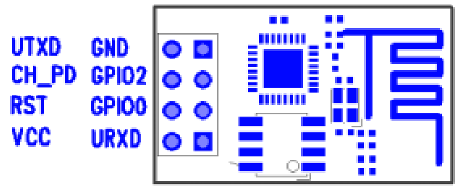
ESP8266 Circuit

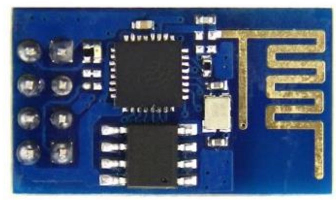
- CPU
  - 32 bit
  - 26MHz-52MHz
  - 64KB instruction RAM, 64KB boot ROM
  - 96KB data RAM
- Wi-Fi
  - 802.11b/g/n
  - Access Point or Station
  - WEP
- GPIO, UART, ADC, I2C, SPI, PWM
- Made by Expressif (China)



68

ESP-01 Module





- $US 2..3 on Ebay
- 3.3V - an inconvenience when working with boards like Arduino (5V)
- 115200 baudrate - but can be changed (to be able to use with “software” serial on Arduinos)
- AT Commands set
- Firmware can be updated - somewhat painful

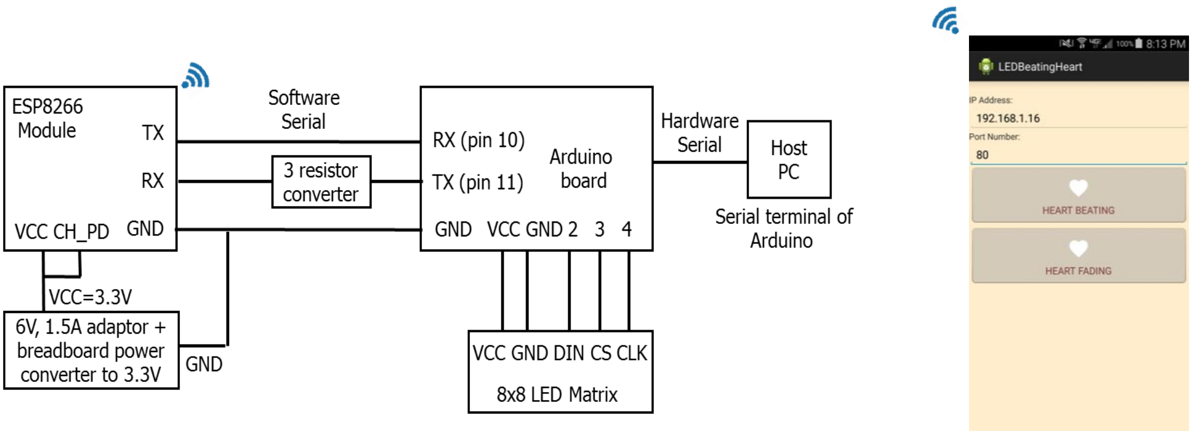
69

ESP8266 AT Commands

- AT+RST
- AT+CWMODE=1
- AT+CWJAP=ssid,password
- AT+CIPMUX=1
- AT+CIPSERVER=1,8888
- AT+CIPSEND=0,13
- ...

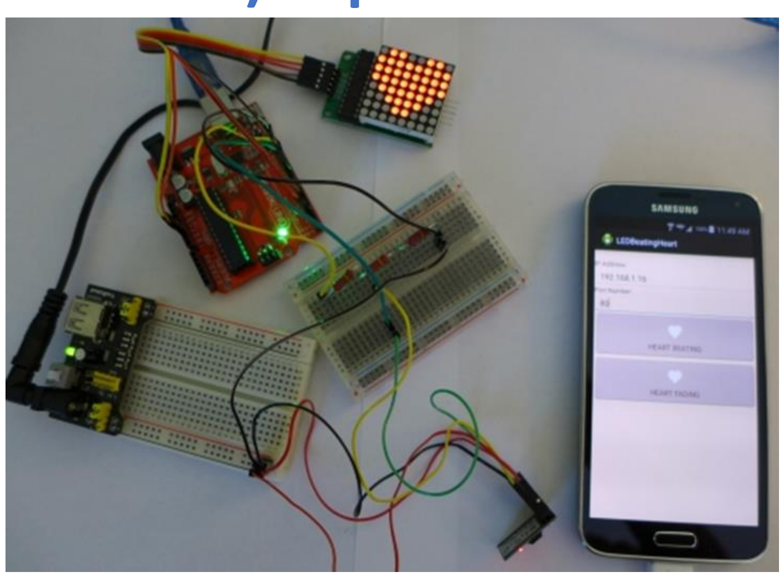
70

Example: ESP8266 Arduino + 8x8 LED matrix controled from Android app



71

(Not so neat) Experimental Set-up



72

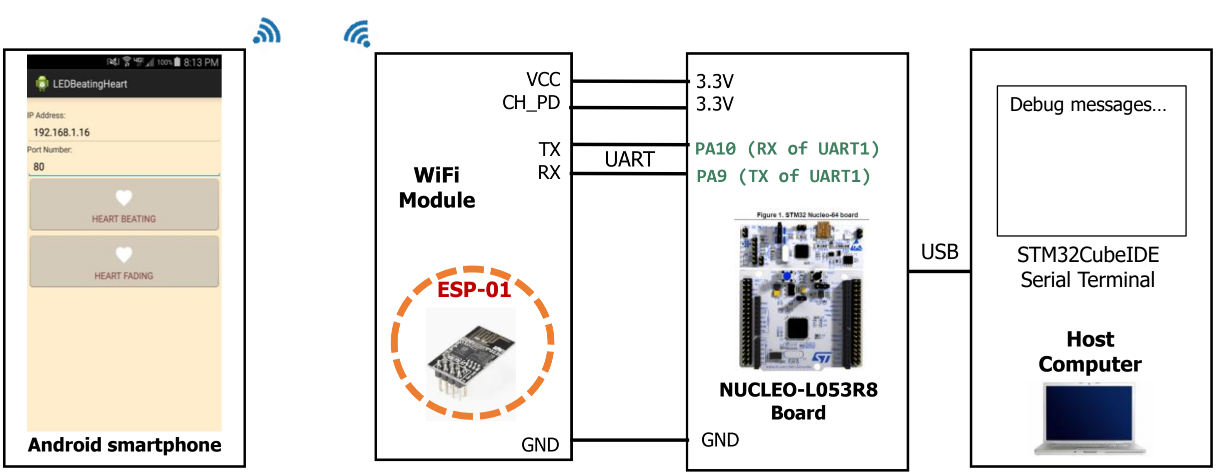
Example Implementation

- This project is described in detail and its source codes are publicly available at the link below (including the complete source code of the Android smartphone app)
- http://www.dejazzer.com/eece4920/index.html

73

73

Same Example Ported to Nucleo Board



74

74

Credits and References

- https://en.wikipedia.org/wiki/Wi-Fi
- https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements
- https://devopedia.org/wi-fi-mac-layer
- http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/Content/ofdm_basicprinciplesoverview.htm
- http://www.sharetechnote.com/html/Communication_OFDM.html
- http://www.gaussianwaves.com/2011/05/introduction-to-ofdm-orthogonal-frequency-division-multiplexing-2/

75

Potential Wi-Fi Scenarios

Technology	Wi-Fi	WiMAX	UWB	Bluetooth	3GPP/2	RFID	Zigbee
LAN for Enterprise	✓	-	-	-	-	-	-
LAN for Home	✓	-	-	-	-	-	-
Home multiple A/V distribution	✓	-	✓	(audio streaming)	-	-	-
Backhauling and last mile	Propriet ary sol'n	✓	-	-	-	-	-
Wide Area Mobility	-	✓	-	-	✓	-	-
Cable/device Replacement	✓	-	✓	✓	-	-	-
Mesh Networking	Enterp/ Home/N	Neighbor-hood Mesh	Home Mesh	-	-	-	-
Sensor Networking	-	-	-	-	-	-	✓
Inventory Control	✓	-	✓	-	-	✓	-
Auto PC	✓	✓	-	✓	✓	-	✓

76