IEEE 802.11 Wireless LAN Standard

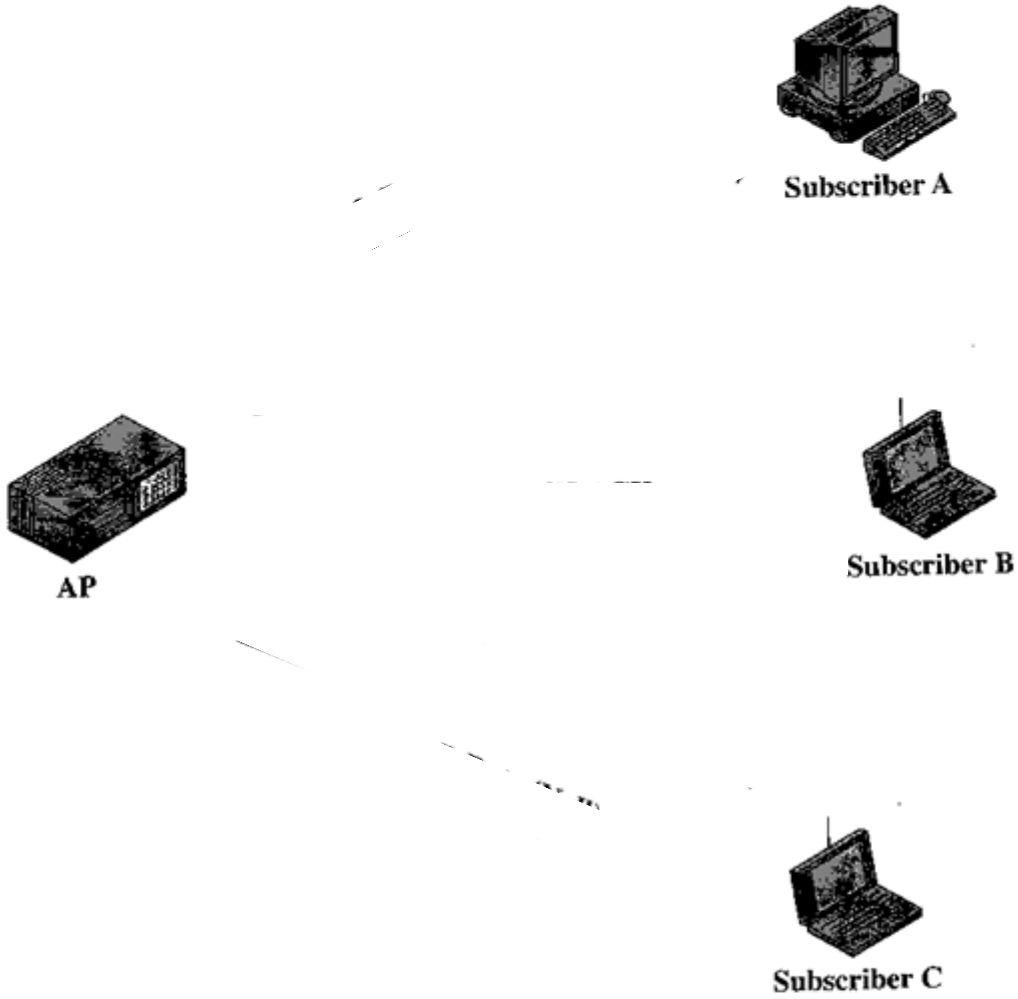
Physical Layers and Security

Updated: 5/6/2011

Reading Assignments:

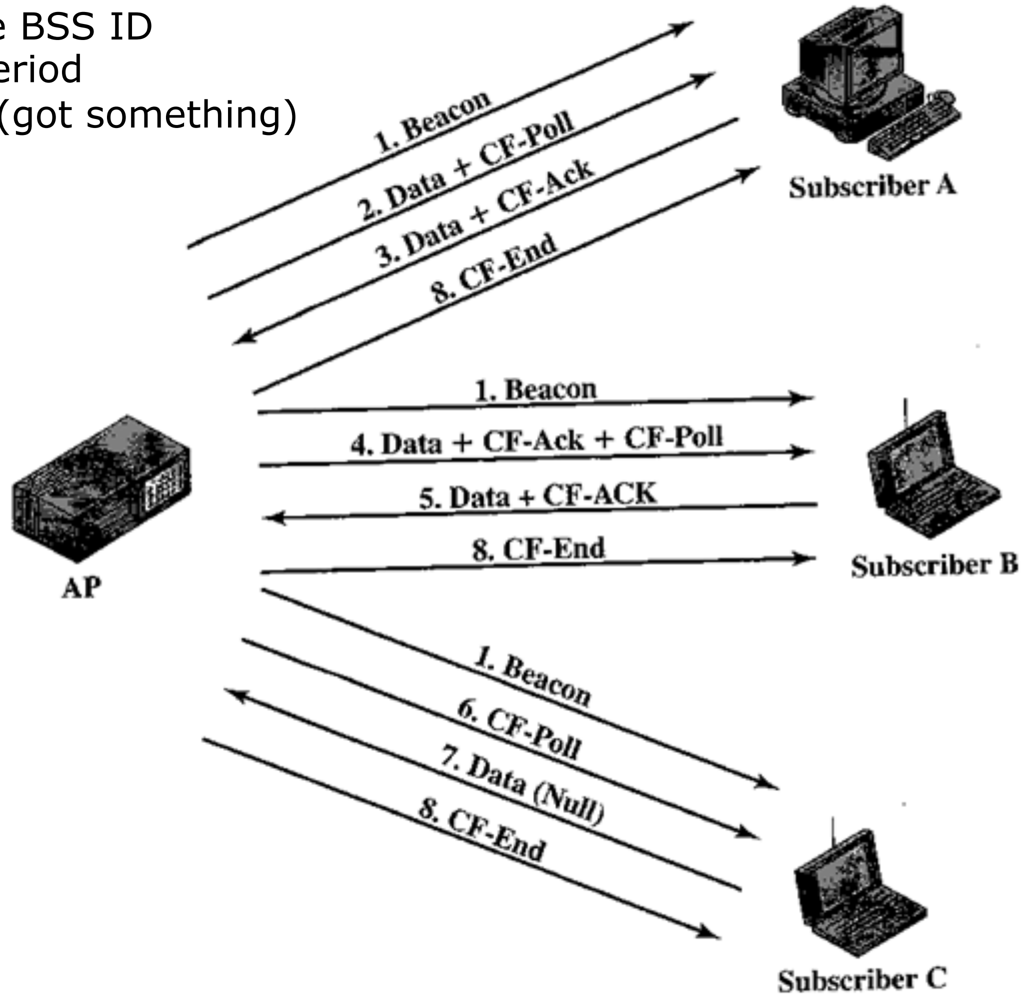
Chapter 14, Walsh Codes pp.184, OFDM pp.337,

Example



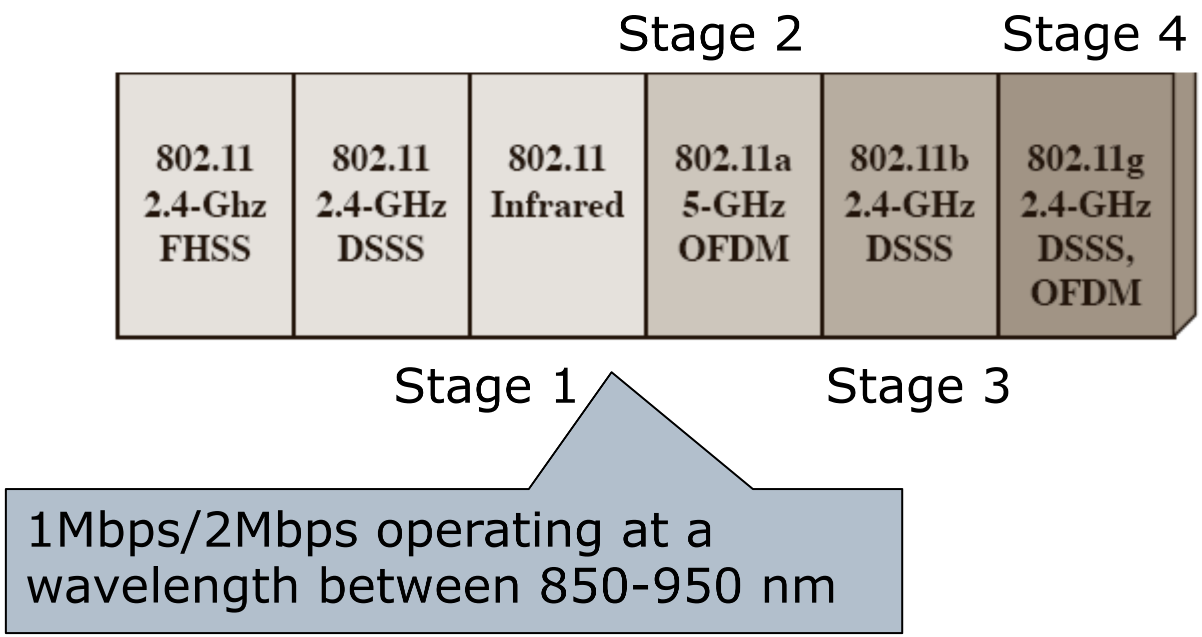
Example

Beacon: locate the BSS ID
Contention Free Period
CF-Poll: AP->STA (got something)



802.11 Physical Layer

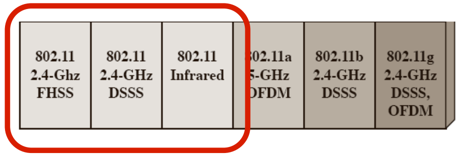
- Issued in four stages



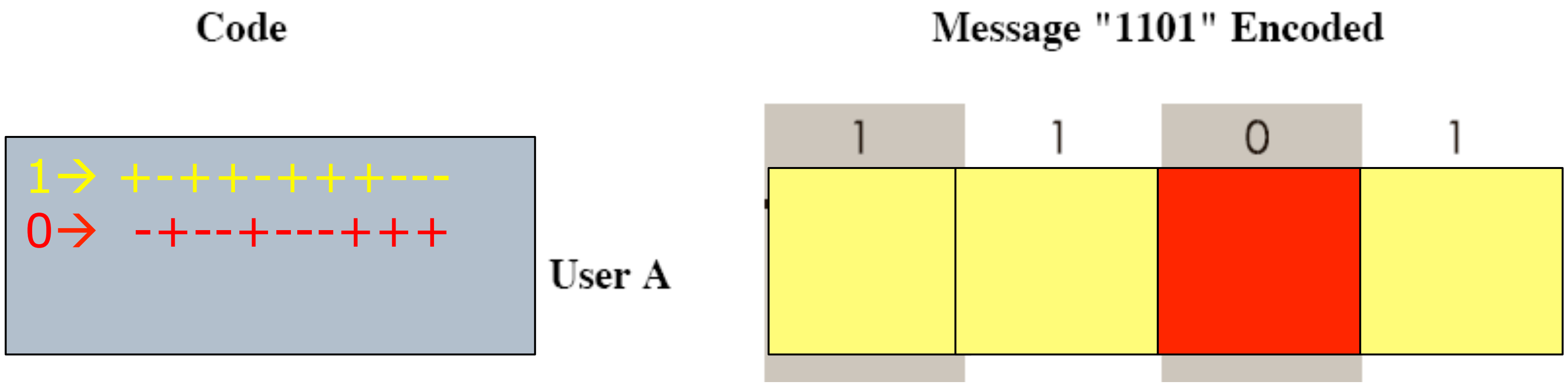
802.11 Physical Layer

	802.11	802.11a	802.11b	802.11g
Available bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed frequency of operation	2.4–2.4835 GHz DSSS, FHSS	5.15–5.35 GHz OFDM 5.725–5.825 GHz OFDM	2.4–2.4835 GHz DSSS	2.4–2.4835 GHz DSSS, OFDM
Number of nonoverlapping channels	3 (indoor/outdoor)	4 indoor 4 (indoor/outdoor) 4 outdoor	3 (indoor/outdoor)	3 (indoor/outdoor)
Data rate per channel	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11 Mbps and below

Physical Media Defined by Original 802.11 Standard



- Direct-sequence spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates of 1 and 2 Mbps
  - Uses Barker Sequence (11-bit chip)



Autocorrelation of Barker Sequence (11-bit chip)

- For N=11
- For R(τ =0)=11/11=1

Autocorrelation of the code sequence

$$R(\tau) = \frac{1}{N}\sum_{k=1}^{N} B_k B_{k-\tau}$$

+	–	+	+	–	+	+	+	–	–	–
+	–	+	+	–	+	+	+	–	–	–
+	+	+	+	+	+	+	+	+	+	+

- For R(3)=-1/11

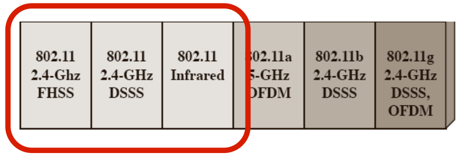
+	–	+	+	–	+	+	+	–	–	–
–	–	–	+	–	+	+	–	+	+	+
–	+	–	+	+	+	+	–	–	–	–

- Same for R(1) = R(N-1 =10)=-1/11

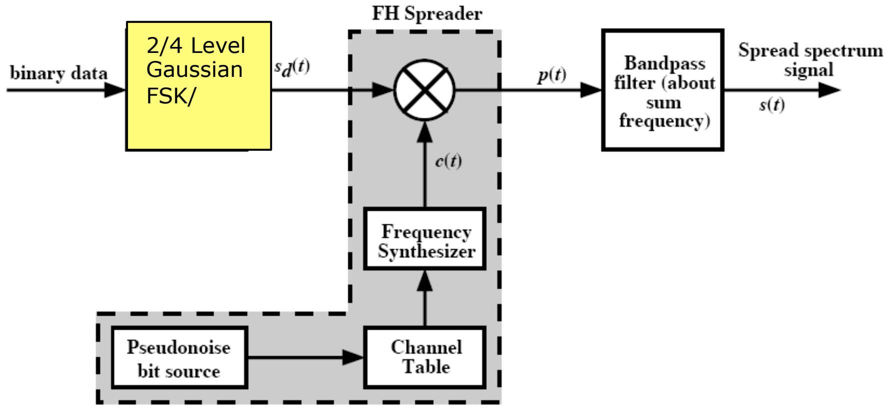
We want |R(τ)|<=1 for all |τ|<=N-1;
N is the number of chips in the code

Note(τ) represents shift from correct value!
(τ) = 0 indicates the received value is correct

Physical Media Defined by Original 802.11 Standard



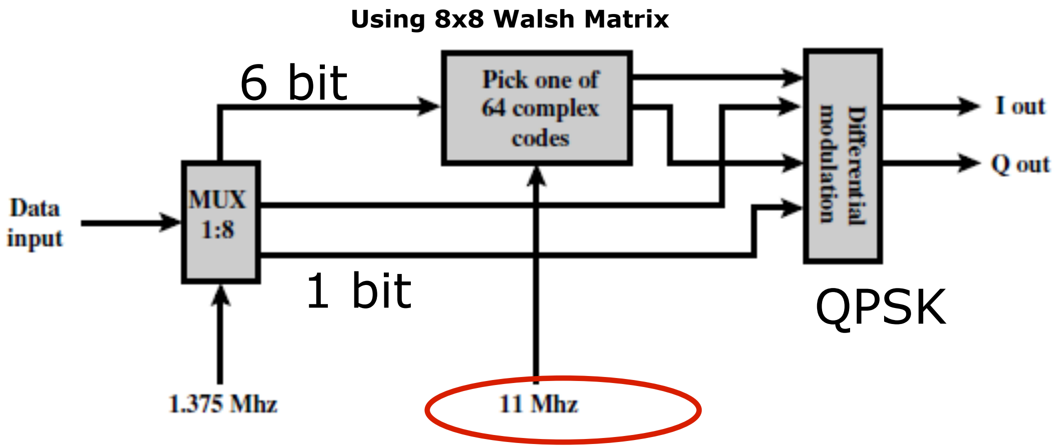
- Frequency-hopping spread spectrum
  - Based on signal hopping concept
    - 2.5 hop / sec with hop distance of 6 MHz
  - Operating in 2.4 GHz ISM band (unlicensed)
  - Data rates of 1 and 2 Mbps
- Infrared
  - Omni directional with 20 meter of range
  - 1 and 2 Mbps
  - Wavelength between 850 and 950 nm

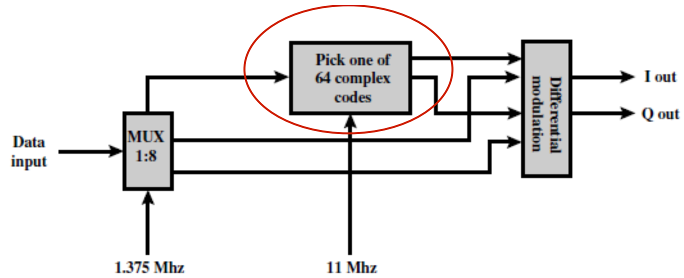


802.11b

- Extension of 802.11 DSSS
- Provides data rate at 5.5 and 11 MHz
- Same chipping rate but higher data rate using Complementary Code Keying (CCK) modulation.

	802.11b
Available bandwidth	83.5 MHz
Unlicensed frequency of operation	2.4–2.4835 GHz DSSS
Number of nonoverlapping channels	3 (indoor/outdoor)
Data rate per channel	1, 2, 5.5, 11 Mbps
Compatibility	Wi-Fi





Walsh Matrix

- Orthogonal Codes used in CDMA applications
- Walsh codes of length n consists of *n* rows of an nxn Walsh Matrix
- Properties
  - Every row is orthogonal to every other row
  - Every row is orthogonal to the logical NOT of every other row

$$H(2^0) = [1],$$

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

8x8 Walsh Code

W(8,2) →

−1	−1	−1	−1	−1	−1	−1	−1
−1	1	−1	1	−1	1	−1	1
−1	−1	1	1	−1	−1	1	1
−1	1	1	−1	−1	1	1	−1
−1	−1	−1	−1	1	1	1	1
−1	1	−1	1	1	−1	1	−1
−1	−1	1	1	1	1	−1	−1
−1	1	1	−1	1	−1	−1	1

A single Walsh code

Walsh code orthogonality

- Code is given as a row in WC matrix
- To generate a code
  - "0" -> "1"
  - "1" -> "-1"
- Example: Codes $W_{4,2}$ and $W_{4,3}$
  - $W_{8,2}$: (0,0,1,1,0,0,1,1) -> (1,1,-1,-1,1,1,-1,-1)
  - $W_{8,3}$: (0,1,1,0,0,1,1,0) -> (1,-1,-1,1,1,-1,-1,1)

$$W_8 = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0 \\ 0&1&1&0&1&0&0&1 \end{bmatrix}$$

When synchronized – codes are orthogonal

$$W_{8,2} \cdot W_{8,3} = (1,1,-1,-1,1,1,-1,-1) \cdot (1,-1,-1,1,1,-1,-1,1) = 0$$

When out of sync – codes are not orthogonal

$$W_{8,2} \cdot \text{shift}(W_{8,3},1) = (1,1,-1,-1,1,1,-1,-1) \cdot (1,1,-1,-1,1,1,-1,-1) = 8$$

Walsh Matrix - Example

- A and B use the following Walsh Code

  W(8,3) = -1,1,-1, 1, -1,1,-1, 1
  W(8,2) = -1, -1,1,1, -1, -1,1,1

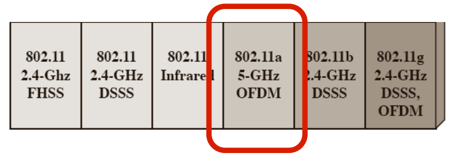
- Assuming A transmits 1 and B does not transmit, what will be the output at the receiver? (+8)
- Assuming A transmits 0 and B does not transmit, what will be the output at the receiver? (-8)
- Assuming A and B transmit 1 with equal power, what will the receiver get?

A output (data = 1)	–1	1	–1	1	–1	1	–1	1	
B output (data = 1)	–1	–1	1	1	–1	–1	1	1	
Received	–2	0	0	2	–2	0	0	2	
Receiver codeword	–1	1	–1	1	–1	1	–1	1	
Multiplication	2	0	0	2	2	0	0	2	=8

Added: (Received row)

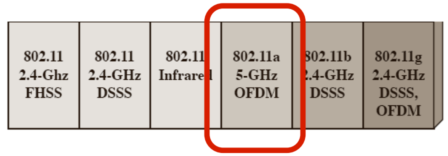
Code For A (Receiver codeword row)

A sent a 1



IEEE 802.11a

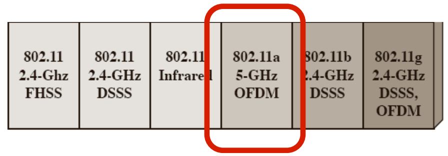
- Based on IEEE 802.11a standard, rating 54 megabytes per second (Mbps)
  - Alternatively called: WiFi5
  - 5-GHz radio spectrum
- Range of about 150+ feet (bandwidth decreases with the range – similar to 802.11b)
  - 802.11a: This is called Data Rate Selection (DRS)
    - As the distance changes BW changes from 54,24,9,etc.
  - 802.11b: DRS will be 11,5.5,2, and finally 1 Mbps as the distance changes and power reduces
- Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps



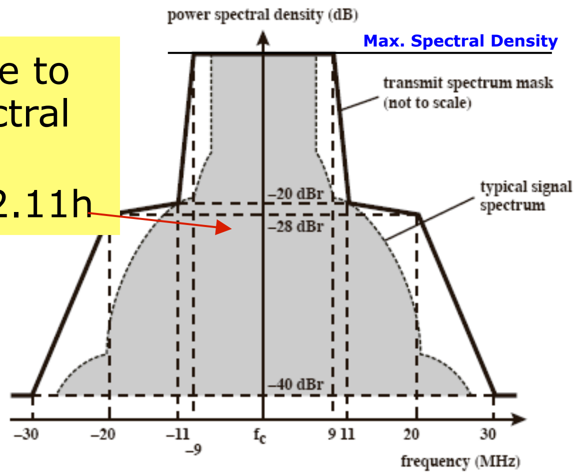
IEEE 802.11a

- Uses orthogonal frequency division multiplexing (OFDM) as the modulation technique
- Major issues due to operating at higher frequencies
  - Higher path loss
  - Travels shorter distance (more APs are required)
    - Better for indoor applications

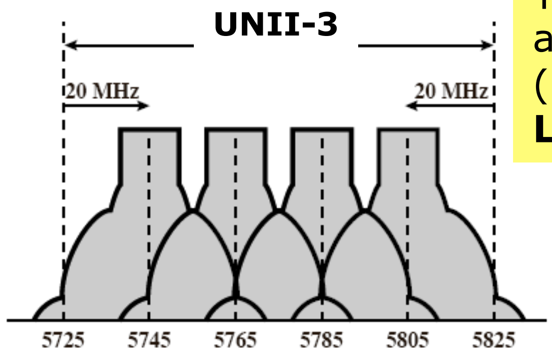
IEEE 802.11a – Channel Structure (OFDM)



dBr: dB relative to maximum spectral Density
Defined by 802.11h



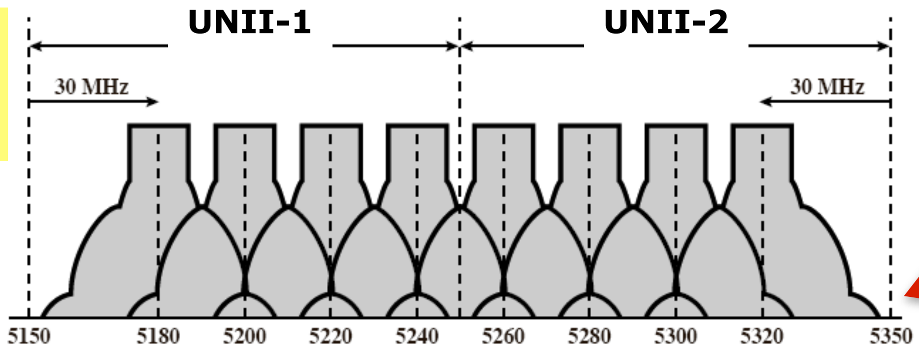
(a) Transmit spectrum mask



(b) Upper U-NII bands: 4 carriers in 100 Mhz/20 MHz spacing

Total of 12 channels across the spectrum (between **all UNIIs: Low, Med, High)**

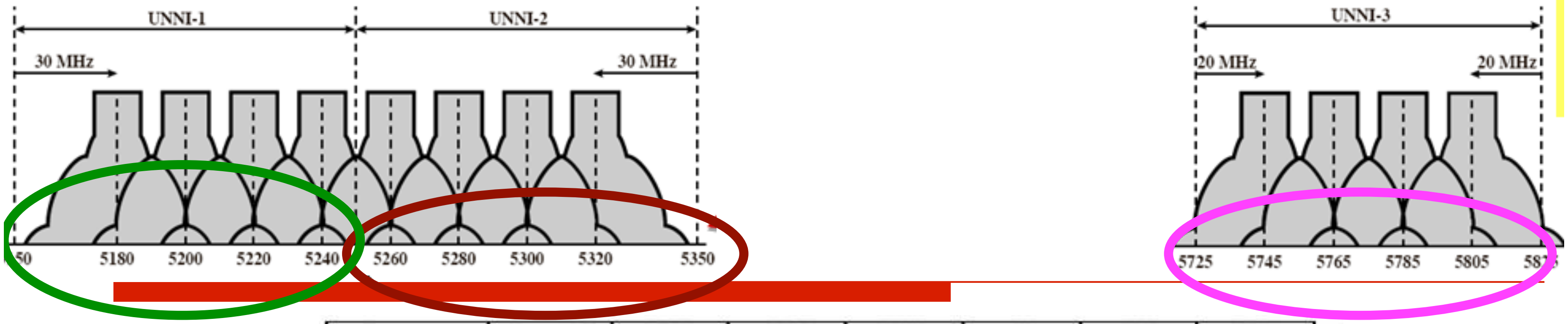
Each UNII has four non-overlapping channels



UNII=Universal Networking Information Infrastructure

UNII-1 band → 5.15 to 5.25 GHz

UNII-2 band → 5.25 to 5.35 GHz

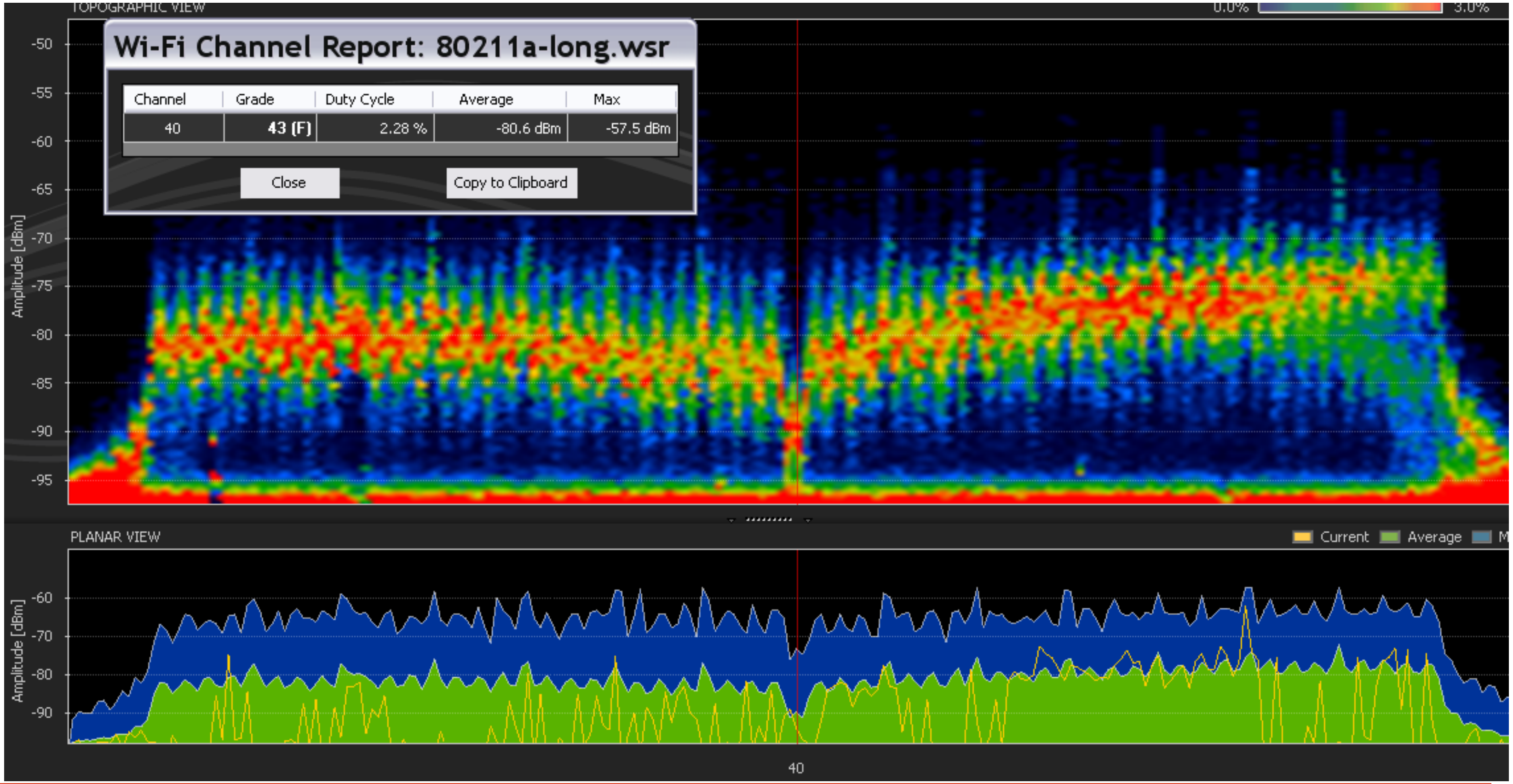


Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	SG (GHz)	ASIA (GHz)	TW (GHz)
Lower Band (36 = default)	34	—	—	5.170 [1]	—	—	—
	36	5.180	5.180	—	5.180	—	—
	38	—	—	5.190	—	—	—
	40	5.200	5.200	—	5.200	—	—
	42	—	—	5.210	—	—	—
	44	5.220	5.220	—	5.220	—	—
	46	—	—	5.230	—	—	—
	48	5.240	5.240	—	5.240	—	—
Middle Band (52 = default)	52	5.260	5.260	—	—	—	5.260
	56	5.280	5.280	—	—	—	5.280
	58	5.300	5.300	—	—	—	5.300
	60	5.320	5.320	—	—	—	5.320
H Band	100		5.500	—	—	—	—
	104	—	5.520	—	—	—	—
	108	—	5.540	—	—	—	—
	112	—	5.560	—	—	—	—
	116	—	5.580	—	—	—	—
	120	—	5.600	—	—	—	—
	124	—	5.620	—	—	—	—
	128	—	5.640	—	—	—	—
	132	—	5.660	—	—	—	—
	136	—	5.680	—	—	—	—
	140	—	5.700	—	—	—	—
Upper Band (149 = default)	149	5.745	—	—	5.745	5.745	5.745
	153	5.675	—	—	5.675	5.675	5.675
	157	5.785	—	—	5.785	5.785	5.785
	161	5.805	—	—	5.805	5.805	5.805
ISM Band	165	5.825	—	—	5.825	—	5.825

Note 1: Channel 34 is the default channel for Japan

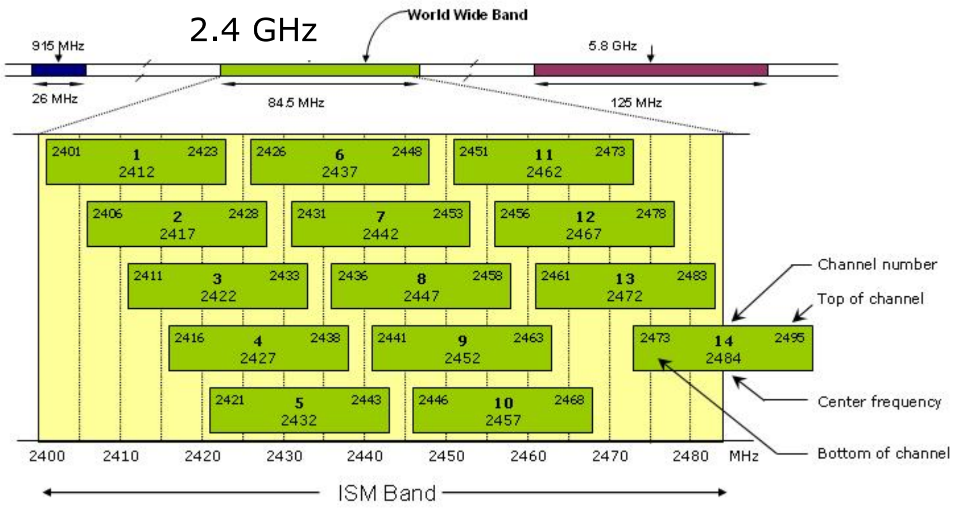
802.11a @ Channel 40 (5190MHz-5210 – 20MHz spacing)

Carrier 2 @ UNII-1 in 200 MHz/200 MHz spacing

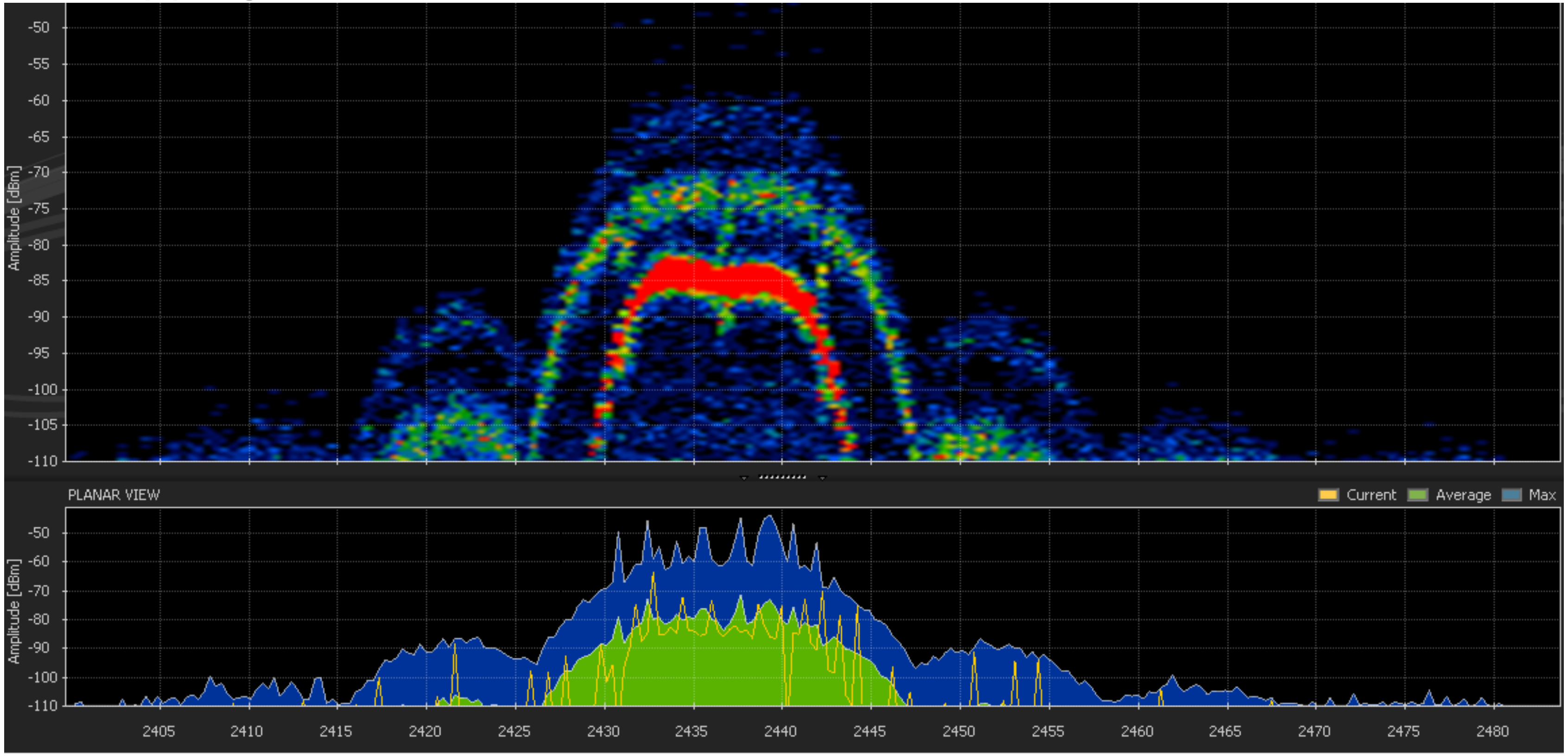


Compare:

802.11b Spectrum Using Analyzer 3.4

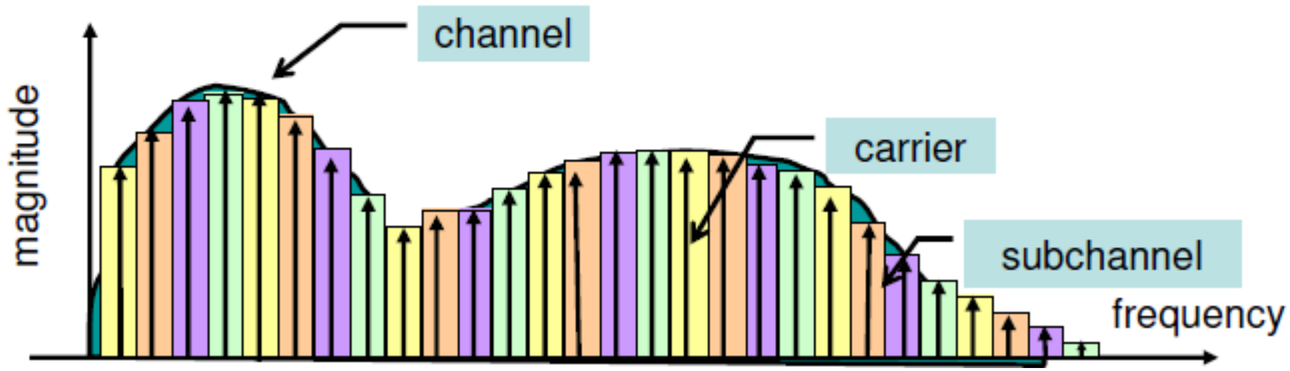


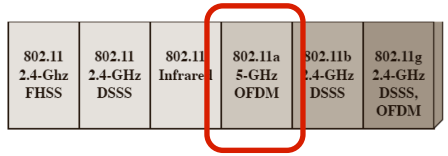
Channel 6 @ 2436;
Note there are only 3 overlapping channels



OFDM - Basics

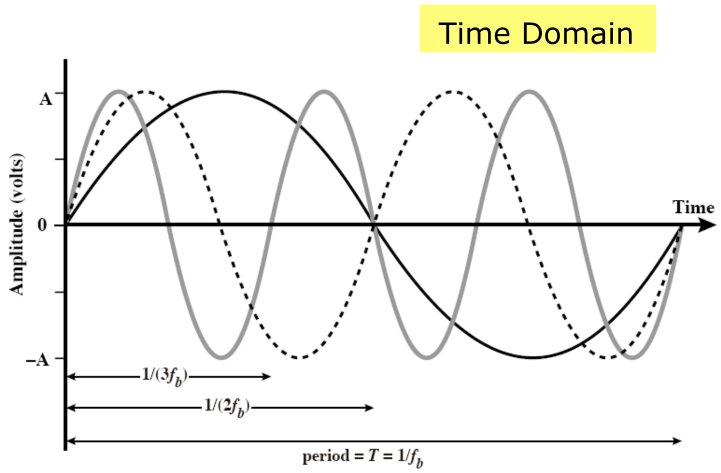
- Frequency-selective channel is divided into flat fading subchannels
- Fast serial data stream is transformed into slow parallel data streams
  - Longer symbol durations



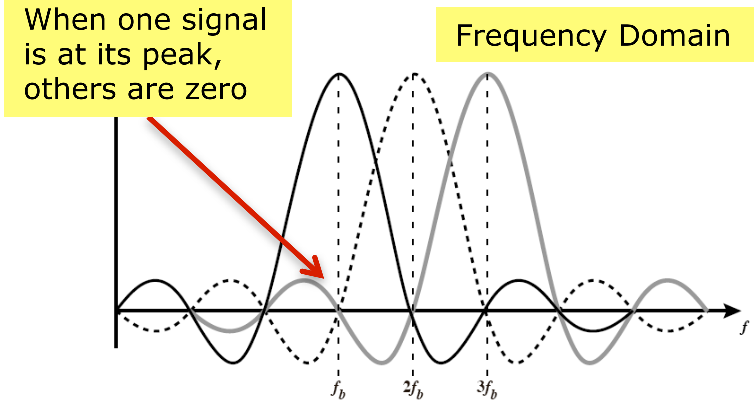


OFDM Advantages

- Used in 802.11a
- Frequency selective fading affects some subchannels not the entire signal
- Overcomes intersymbol interference (ISI) in a multipath environment
  - Each subchannel has much larger period
  - Thus, time shift results in less ISI
- One major issue with OFDM is ICI
  - Inter-carrier interference (ICI) – due to frequency shift
  - Caused by Doppler effect OR lack of synchronization
- One approach to reduce ICI or ISI is to use Guard time (Ref: GAST)



(a) Three subcarriers in time domain

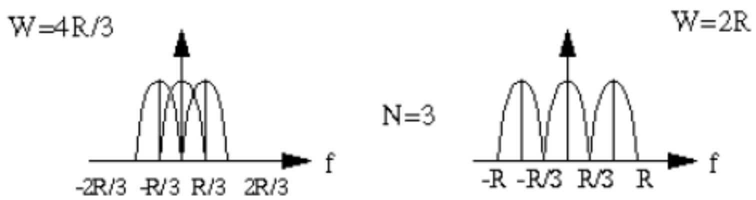


(b) Three subcarriers in frequency domain

http://www.dsptutor.freeuk.com/analyser/SA102.html

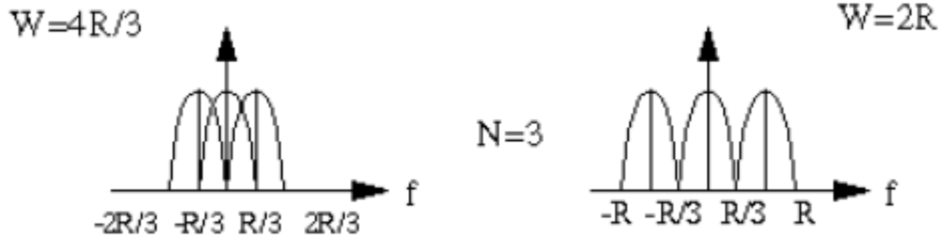
OFDM - Basics

- Orthogonal frequency division multiplexing (OFDM)
  - Also called multicarrier modulation
  - Encoding single transmission into multiple subcarriers
  - Converting fast transmission into smaller transmission
  - **Note:** different from CDMA: multiple transmissions into a single subcarrier!
  - Also used in 1G mobile phones
  - FDM has high overhead
- Advantage
  - Spectral efficiency
  - Simple implementation
  - Tolerant to ISI
- Disadvantages
  - BW loss due guard time
  - Prone to frequency and phase offset errors
  - Peak to average power - problem



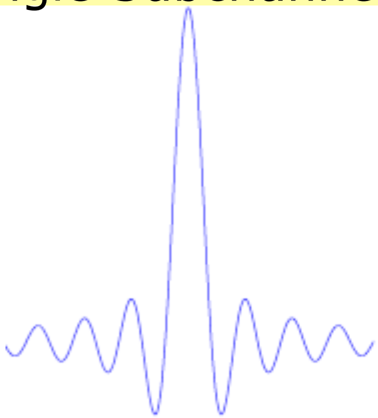
Spectrum Representation with 3 Channels

OFDM - Basics

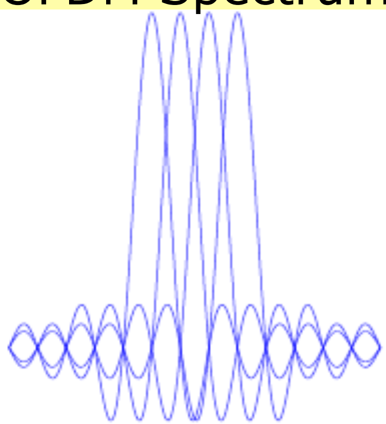


- Similar to FDM but all frequency channels are dedicated to a single data source
  - OFDM uses parallel data and FDM with overlapping subchannels
- Subchannels overlap on each other
  - Sinc -shaped spectra
- In OFDM the carriers are arranged so that the sidebands of the individual carriers overlap and the signals are still received without adjacent carrier interference.

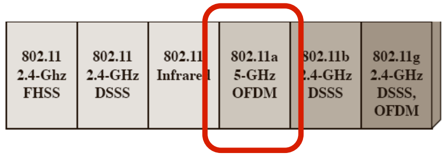
Single Subchannel



OFDM Spectrum



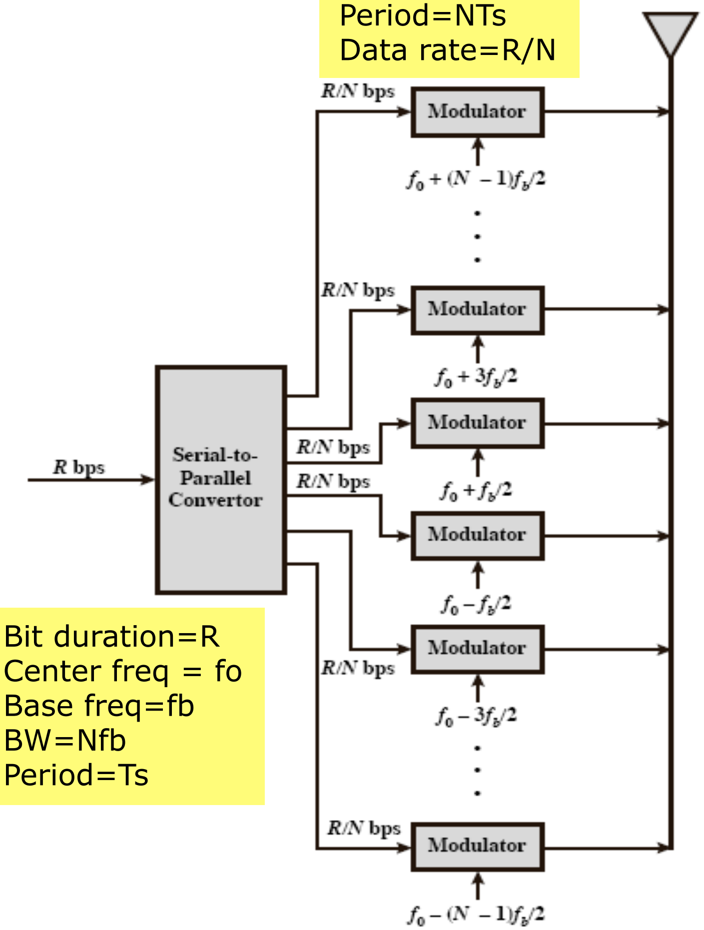
Sinc shape – sidebands overlap



IEEE 802.11a - OFDM

- A modulating technique
  - Chopping large frequency into subcarrieres
  - Some of the bits are transmitted on each subcarrier
- 802.11a
  - Consists of multiple subcarriers and base frequency of 0.3125 MHz
  - Total of 48 channels
  - Spacing between channels cannot be less than 15 MHz (48 x 0.3125)
  - Center frequency will be about 5MHz
- The new slower frequencies are all orthogonal to each other
  - Independent frequencies

Subcarriers
Period=NTs
Data rate=R/N



Bit duration=R
Center freq = fo
Base freq=fb
BW=Nfb
Period=Ts

Read: http://www.comlab.hut.fi/opetus/333/2004_2005_slides/ofdm.pdf

OFDM Variations

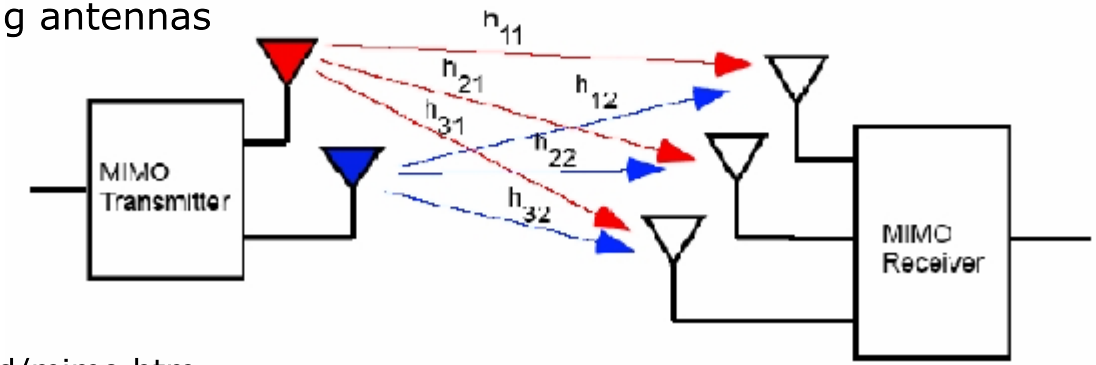
- ERP-OFDM (extended rate physical layer)
- Flash OFDM - also called fast-hopped OFDM, which uses multiple tones and fast hopping to spread signals over a given spectrum band.
- WOFDM - Wideband OFDM
- MIMO-OFDM

Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 Meters	~140 Meters
802.11n	June 2009[4] (est.)	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	MIMO	~70 Meters	~250 Meters
802.11y	June 2008[4] (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters

IEEE 802.11n – MIMO-OFDM

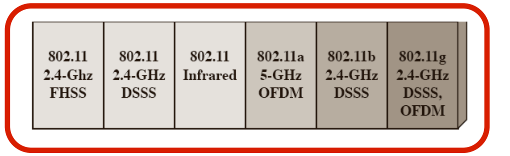
Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 Meters	~140 Meters
802.11n	June 2009[4] (est.)	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	MIMO	~70 Meters	~250 Meters
802.11y	June 2008[4] (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters

- Multiple Input, Multiple Output Orthogonal Frequency Division Multiplexing
- MIMO-OFDM is used for WiFi, WiMax and 4G communication systems
  - Based on the draft IEEE 802.11n standard
- The basic idea is using multiple antennas to transmit and receive radio signals
- The MIMO system uses multiple antennas to simultaneously transmit data, in small pieces to the receiver, which can process the data flows and put them back together.
  - This process, called spatial multiplexing
  - It boosts the data-transmission speed by a factor equal to the number of transmitting antennas



http://www.xcad.com/xcad/mimo.htm

Comparing IEEE 802.11a and b/g



- 11a utilizes more available BW
- 11a provides higher data rate than 11b and the same as 11g
- 11a uses 5GHz which is less cluttered frequency band
- Important: 802.11b and 802.11a are not interoperable or compatible

	802.11	802.11a	802.11b	802.11g
Available bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed frequency of operation	2.4–2.4835 GHz DSSS, FHSS	5.15–5.35 GHz OFDM 5.725–5.825 GHz OFDM	2.4–2.4835 GHz DSSS	2.4–2.4835 GHz DSSS, OFDM
Number of nonoverlapping channels	3 (indoor/outdoor)	4 indoor 4 (indoor/outdoor) 4 outdoor	3 (indoor/outdoor)	3 (indoor/outdoor)
Data rate per channel	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11 Mbps and below

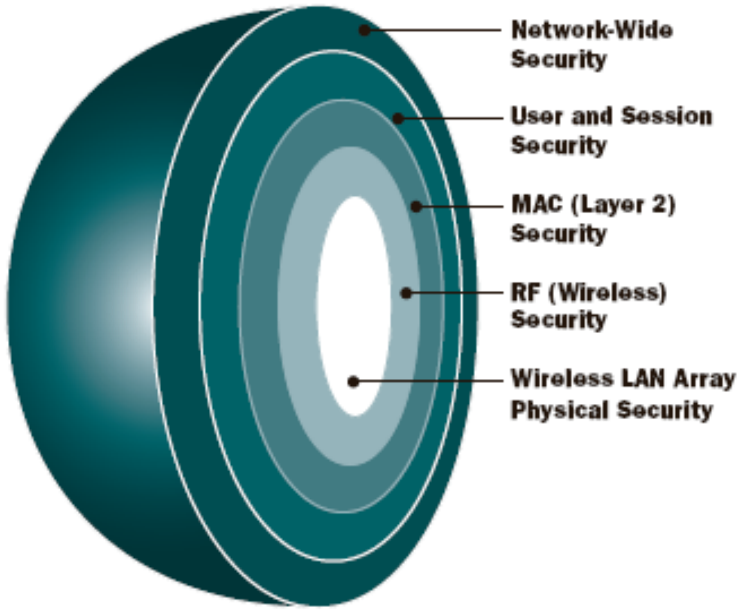
References

- Read about OFDM: http://www.create.ucsb.edu/ATON/01.01/OFDM.pdf

Security and Authentication

802.11 Security Features

- Wireless security can be implemented at various levels
- Privacy
  - Defined by Wired Equivalent Privacy (WEP) algorithm
    - Using RC4 Encrypted algorithm (40-bit key or 104-bit key)
- Authentication
  - The end users share a secret key
- General weaknesses
  - Heavy reuse of shared-key
  - No key management within the protocol



WEP Privacy

- Contains major weaknesses
- Initially 40-bit key - very inadequate
- Later 104-bit key – still vulnerable

BASIC PROBLEM:
To determine a 104 bit WEP key, we capture between 2000 and 4000 interesting packets…in just a few days!

RC4

- The most widely-used software stream cipher
  - Secure Sockets Layer (SSL)
    - Protecting Internet traffic
  - WEP
    - Securing wireless networks

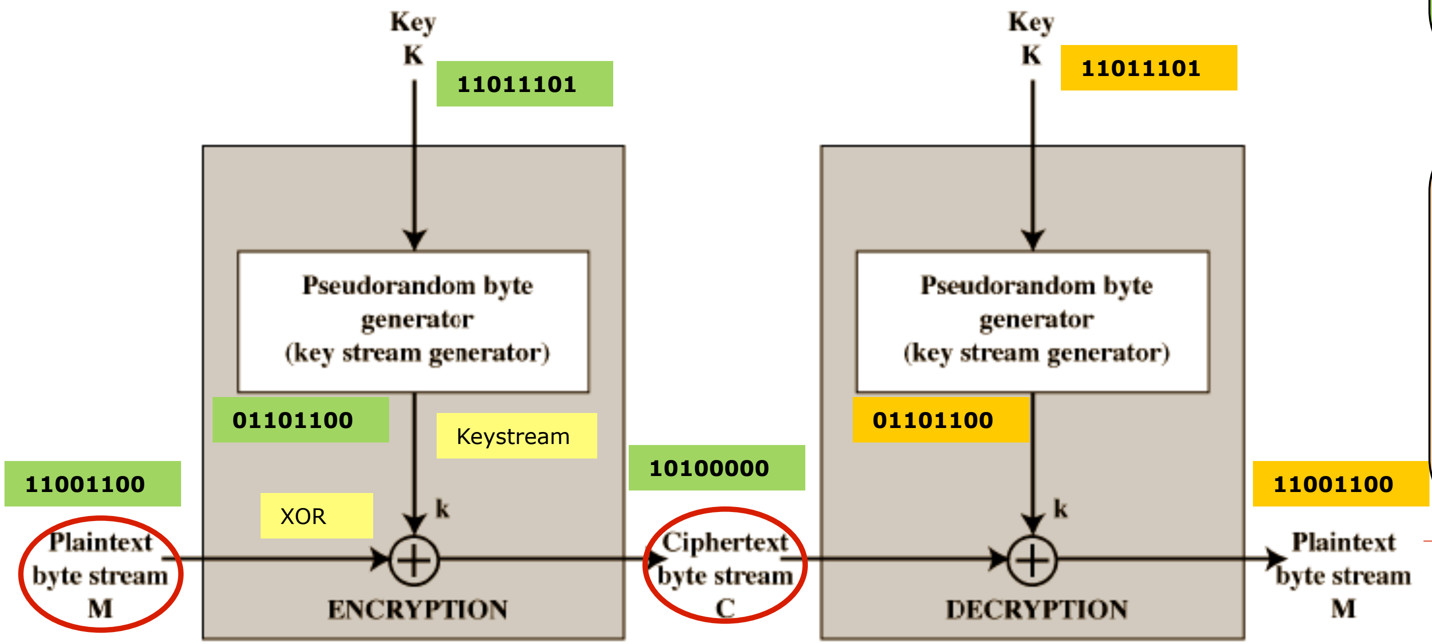
Breaking WEP:
http://eprint.iacr.org/2007/120.pdf
http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

Basic Stream Cipher

- A variable key-size stream cipher, typically, with byte orientation
- The algorithm was actually revealed in 1994
- Very effective and simple
- Basic idea stream cipher
  - Bit-by-bit or byte-by-byte
  - A key is an input to a pseudorandom stream
  - The output of the generator is called keystream

```
11001100
01101100 XOR
-------------
10100000
```

```
10100000
01101100 XOR
-------------
11001100
```



802.11i Security Features

- 802.11i was developed to address security standards in WLAN
- WiFi Alliance Promulgated WiFi-Protected Access (WPA)
  - Accepting basic security measures in 11i before converting to 11i

802.11i Architecture

- Data transfer privacy
  - MAC layer encryption
  - Makes sure the data is not altered
- Authentication
  - Developing a **protocol** to ensure exchange between STA and AP using a temporary key over the wireless link
  - Examples
    - EAP: Extensive Authentication Protocol
    - RADIUS: Remote Authentication Dial-In Service
- Access control (key management)
  - Makes sure the key exchange is done properly
  - Regardless of what the actual authentication technique is

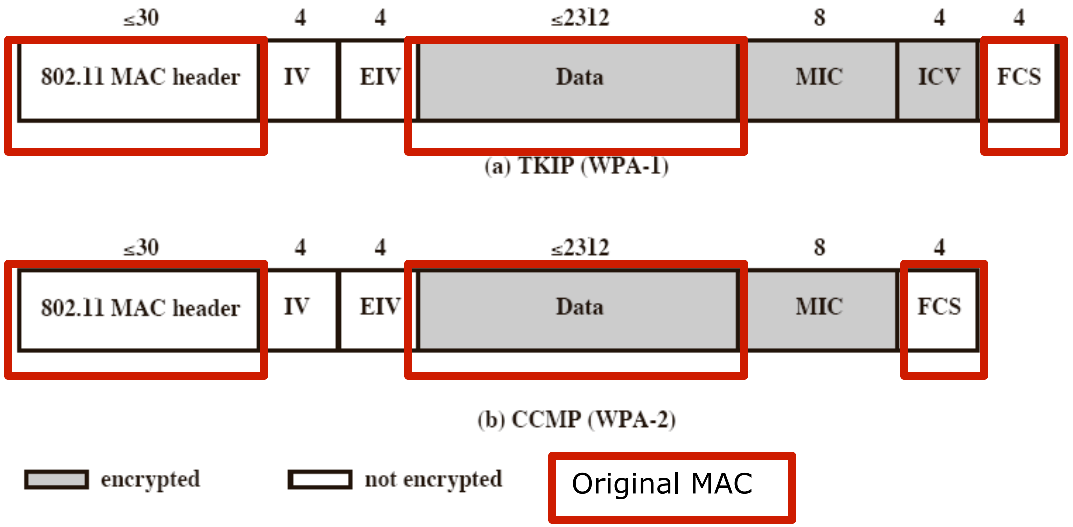
802.11i Basic Architecture

- Authentication
  - Requires Authentication Server (AS)
    - AS passes the secret key to the AP
    - Eventually the key is passed to stations
    - Station used the key to encrypt the data between the AP and STA
  - Offers several encryption techniques
    - Uses Advanced Encryption Standard (AES) – 128-bit keys (expensive!)
    - 104-bit RC4; compatible with many existing equipments

802.11i Security Features – Data transfer privacy

- MAC level encryption algorithm
- Two schemes
  - Temporal Key Integrity Protocol (TKIP or WPA-1)
- Requires only software changes to devices with WEP
    - Uses RC4 104-bit (similar to WEP) encryption algorithm
  - Counter-mode CBC MAC Protocol (CCMP or WPA-2)
    - Uses Advanced Encryption Standard (ASE)

FCS: Frame Check Sequence



802.11i Security Features – Data transfer privacy

A CRC calculated on all the fields and then encrypted using RC4 key

Used to ensure the message is not modified

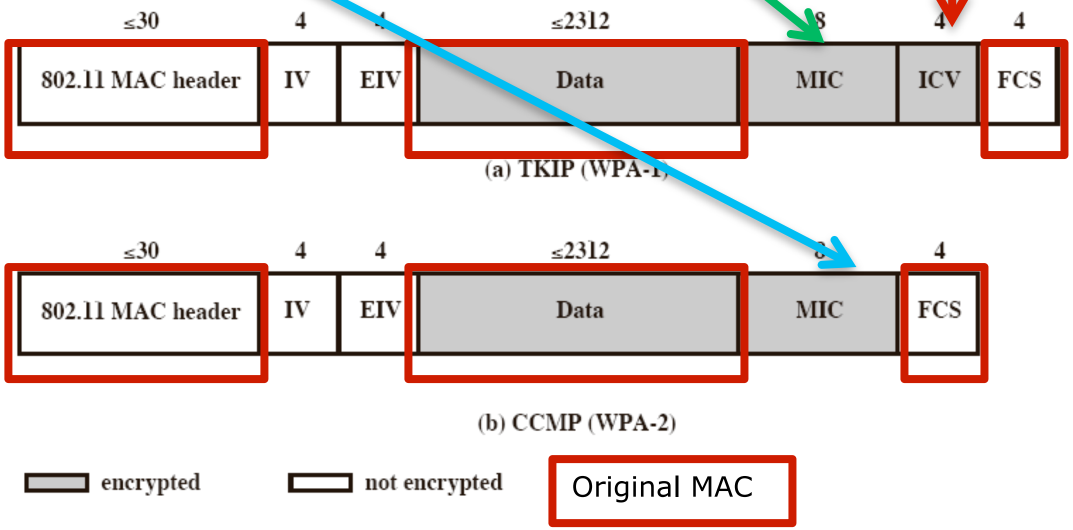
No ICV; Uses Advanced Encryption Standard (ASE)

64-bit value calculated using MAC src/des and data fields – uses a separate RC4-based key

24-bit Initialization Vector (IV)- is combined with the 104-bit RC4 key

Extended IV (EIV) provides 48-bit IV; thus IV+EIV+RC4 key → 128-bit Encryption key

IV and EIV also act as sequence counter → out-f-seq. frames are ignored



Calculating CRC

- **Cyclic Redundancy Check**
- **Basic error checking technique**
  - Parity check
  - Checksum
  - CRC
- Basic Operation:
  - convert binary message to a polynomial
  - divide it by another predefined polynomial called the *key*
  - The remainder from this division is the CRC
  - Transmit CRC and Message together

CRC Example (Read page 197)

- Assume the message is 11010011101100
- Polynomial is 110101(six bits)
- Then, divide Message+00000 by the Polynomial →
  - Remainder will be 01110
- Append: 11010011101100 & 01110
  - Transmit the message
- The receiver takes 11010011101100
  - Divides it by the Polynomial 110101(six bits)
  - If the message is not altered → there will be no remainder

Message Authentication Using 1-Way Hashing (P. 402)

- We use a hash function to transmit the message
  - Message + hashed code is transmitted
- Hashing
  - mathematical function that converts a large amount of data into a small datum, usually a single integer
- Basic Idea
  - Compute H(Sab||M)
  - Transmit M|| H(Sab||M)
- Hash function properties
  - Weak hash function
  - Strong hash function
- A Widely used Hash function is MD5

Example: http://www.fileformat.info/tool/hash.htm?hex=1010101000011100000

Questions

- How does 802.11i handles authentication for an IBSS?