WLAN IEEE 802.11
aka Wi-Fi

Max Riegel

Lectures overview

June 14th
– Wi-Fi deployments
– Standardization environment
– Wi-Fi system architecture
– Wi-Fi security

June 21st
– Medium access functions
– MAC layer management frame formats
– Quality of Service
– Wi-Fi roaming and Hotspot 2.0
– Wi-Fi Direct

June 28th
– Wireless channel characteristics
– Wi-Fi radio for 2.4 GHz and 5 GHz bands
– WiGig extension for 60 GHz bands
– Wi-Fi extension for below 1GHz bands
– WLAN management

Standards environments
STANDARD REFERENCE

IEEE Std 802.11™-2016 + amendment 802.11ah

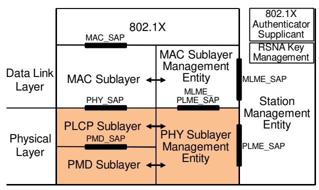
- Can be downloaded at no charge by IEEE Get Program
  – http://standards.ieee.org/getieee802/download/802.11-2016.pdf
  – http://standards.ieee.org/getieee802/download/802.11ah-2016.pdf
- No all the features specified in the standard are available in real Wi-Fi products
- Where appropriate presentation adopts behavior of real Wi-Fi products as specified by Wi-Fi Alliance in its certification programs
  – https://www.wi-fi.org/discover-wi-fi/specifications

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- Revision of IEEE Std 802.11-2012
  – Previous revisions: IEEE Std 802.11-2007 and IEEE Std 802.11-1999
  – Initial IEEE 802.11 standard release in 1997
- Comprises initial IEEE Std 802.11-1999 together with all amendments IEEE 802.11a-1999 … IEEE 802.11af-2013
  – i.e.: a, b, d, e, g, h, I, j, k, n, p, r, s, u, v, w, y, z, aa, ac, ad, ae, af

Amendment IEEE Std 802.11ah-2016
- Amendment 2: Sub 1 GHz License Exempt Operation

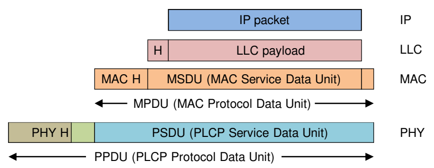
IEEE 802.11 Protocol architecture

- 802.1X
  – Port Access Entity
  – Authenticator/Supplicant
- RSNA Key Management
  – Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  – interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  – synchronization
  – power management
  – scanning
  – authentication
  – association
  – MAC configuration and monitoring
- MAC Sublayer
  – basic access mechanism
  – fragmentation
  – encryption
- PHY Sublayer Management Entity (PLME)
  – channel tuning
  – PHY configuration and monitoring
- Physical Sublayer Convergence Protocol (PLCP)
  – PHY-specific, supports common PHY SAP
  – provides Clear Channel Assessment signal (carrier sense)
- Physical Medium Dependent Sublayer (PMD)
  – modulation and encoding



IEEE 802.11 Frame structure

- Each protocol layer deploys its own header for conveying the protocol information between peers



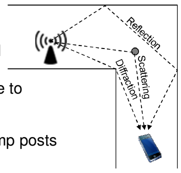
- IEEE 802.11 PHY header carries the information for setting up the reception of radio frames
- Physical Layer Convergence Protocol (PLCP) provides a PHY independent Service Access Point (SAP) for higher layers

WLAN IEEE 802.11

WIRELESS CHANNELS

Radio signal propagation issues

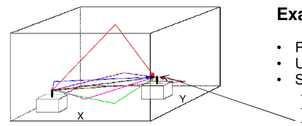
- Path loss
  - Attenuation due to distance and frequency
- Reflection
  - Surface large relative to wavelength λ of signal
- Diffraction
  - Edge of impenetrable body that is large relative to wavelength λ
- Scattering
  - Obstacle size in order of wavelength λ, e.g. lamp posts



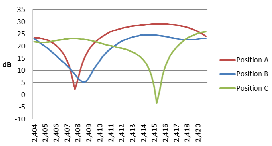
Main issues:

- Line-Of-Sight:
  - Reflected signals may cause major impact on signal
- non-Line-Of-Sight:
  - Diffraction and scattering are primary means of reception

WLAN channels with selective fading



Relative Selective Fading



Example of selective fading

- Reference doc.: IEEE 802.11-13/0416r5
- Use of ray tracing to estimate delays
- Scenario
  - Room 100 ft by 70 ft (x, y)
  - Ceiling 20 ft
  - RX position (65, 44 w/ 3ft off ground)
  - 10dB obstruction to direct and floor rays

Transmission characteristics taken for

- Position A (21, 45) (delays 23 -100 ns)
- Position B (30, 45) (delays 27 - 102 ns)
- Position C (13, 45) (delays 21 - 99 ns)

Fades up to 25 dB!

WLAN IEEE 802.11

WI-FI RADIO FOR 2.4 & 5 GHZ

Wi-Fi radio for 2.4 GHz and 5 GHz bands

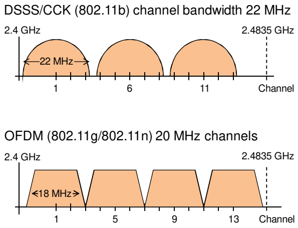
- Unlicensed Spectrum
  - 2.4 GHz
  - 5 GHz
- IEEE 802.11 Radio modes for 2.4GHz & 5 GHz
  - DSSS
    - for up to 2 Mbps
  - CCK
    - for up to 11 Mbps
  - OFDM
    - for up to 54 Mbps
  - OFDM w/ 20/40MHz & MIMO
    - for up to 600 Mbps
  - OFDM w/ 20/40/80/160MHz & MU-MIMO in 5GHz
    - for up to 6 900 Mbps
  - Outlook: 802.11ax for ultra dense deployments

WLAN IEEE 802.11

UNLICENSED SPECTRUM

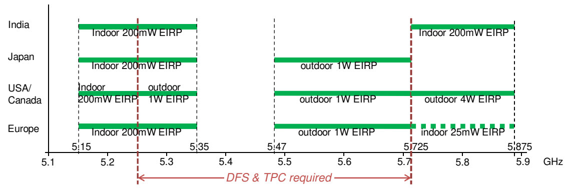
Wi-Fi in the 2.4 GHz ISM band

- Most of Wi-Fi today operate in the 2.4 GHz ISM band
  - IEEE 802.11b set the rule to deploy systems on channel 1 – 6 – 11
  - Plain IEEE 802.11 g/n (OFDM) systems would not interfere when operation on channel 1 – 5 – 9 – 13
- Avoid interference with two adjacent channels by configuration of channels in the middle.
- Regulatory requirements:
  - max TX power (EU): 100 mW EIRP
  - Use of spread spectrum coding
  - Specification: ETSI EN 300 328



5 GHz Unlicensed Spectrum

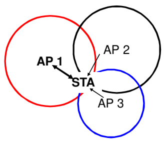
- 455 MHz of unlicensed spectrum available mostly worldwide
  - Wi-Fi is usually secondary user of that spectrum



- Dynamic Frequency Selection (DFS) and Transmission Power Control (TPC) are required for most of the 5 GHz spectrum to protect primary users (e.g. weather radars)
  - Specification: ETSI EN 301 893 (EN 300 440 for 5725-5875 MHz)

Spectrum management for the 5 GHz band

- DFS (Dynamic Frequency Selection)
  - APs dynamically select their operating channel after scanning for other users (e.g. weather radars)
  - STAs provide to APs detailed reports about spectrum usage at their locations.

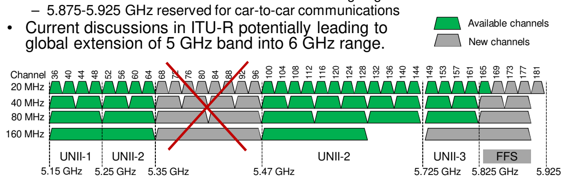


- TPC (Transmission Power Control)
  - Supports interference minimization, power consumption reduction, range control and link robustness.
  - APs define and communicate regulatory and local transmit power constraints.
  - Stations select transmit powers for each frame according to local and regulatory constraints.

5 GHz spectrum evolution

Wide bandwidth channels desired to support high throughput requirements

- Non-overlapping channels to avoid co-channel interference desired for good QoS
- Current UNII spectrum allows only
  - **Six** (Europe: **five**) 80 MHz channels or **Two** 160 MHz channels
- Discussions regarding extension into 5.35-5.47 GHz did not materialize.
  - Worldwide harmonization of 5.725-5.875 GHz ongoing
  - 5.875-5.925 GHz reserved for car-to-car communications
- Current discussions in ITU-R potentially leading to global extension of 5 GHz band into 6 GHz range.



WLAN IEEE 802.11

2.4 & 5 GHZ RADIO STANDARDS OVERVIEW

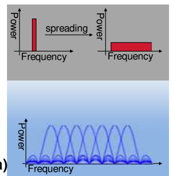
IEEE 802.11 radio standards evolution

Std	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
	Jun 1997	2.4	20	1, 2	1	DSSS	40	150
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	40	150
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	40	150
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM (DSSS)	40	150
n	Oct 2009	2.4 5	20/40	up to 72.2/150	4	OFDM	60 40	200 150
y	Nov 2008	3.7	5/10/20	up to 13.5/27/54	1	OFDM	-	5 000
ac	Dec 2013	5	20/40/ 80/160	up to 87/200/433/867	8	OFDM	40	150
ad	Oct 2012	60	2000	up to 6 700	1	SC/OFDM	line of sight	-
af	Dec 2013	TV WS	1,2,4x 6/7/8	up to 1,2,4x 26.7/26.7/35.5	4	OFDM	100	1000
ah	Dec 2016	< 1	1/2/4/8/16	0.15 … up to 4.4/9/20/43/87	4	OFDM	100	1000
ax	~ 2020*	1…6	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2020*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	line of sight	

* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

IEEE802.11 PHY layer solutions for 2.4 GHz & 5 GHz

- 2.4 GHz Direct Sequence Spread Spectrum
  - DBPSK/DQPSK providing 1/2 Mbps
  - Channel bandwidth: 22 MHz
- 2.4 GHz High Rate DSSS **(802.11b)**
  - CCK/DQPSK providing 5.5/11 Mbps
  - Channel bandwidth: 22 MHz
- 2.4 GHz Extended Rate **(802.11g)**
  - DSSS providing 1/2/5.5/11 Mbps
  - OFDM providing 6/9/12/18/24/36/48/54 Mbps
  - Channel bandwidth: 22/20 MHz
- 5 GHz Orthogonal Frequency Division Multiplex **(802.11a)**
  - OFDM providing 6/9/12/18/24/36/48/54 Mbps
  - Channel bandwidth: 20 MHz
- 2.4 GHz & 5 GHz High Throughput **(802.11n)**
  - OFDM with up to 4x4 MIMO providing up to 600 Mbps
  - Channel bandwidth: 20 MHz & 40 MHz
- 5 GHz Very High Throughput **(802.11ac)**
  - OFDM with up to 8x8 MU-MIMO providing up to 6900 Mbps
  - Channel bandwidth: 20 MHz, 40 MHz, 80 MHz, 160 MHz

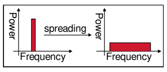


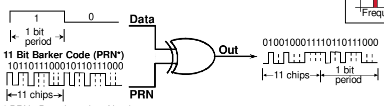
WLAN IEEE 802.11

DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

Direct Sequence Spread Spectrum

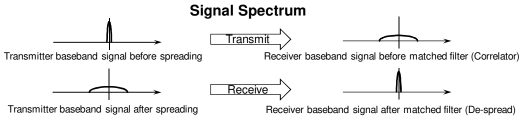
RF Energy is Spread by XOR of Data with PRN Sequence





* PRN: Pseudorandom Number

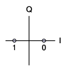
Signal Spectrum

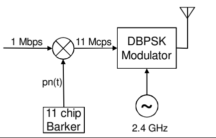


DSSS - Modulation

1 Mbps by DBPSK

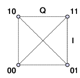
- Differential Binary Phase Shift Keying
  - 0 = 0
  - 1 = π

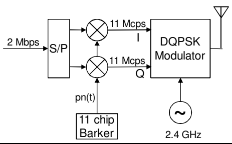




2 Mbps by DQPSK

- Differential Quadrature Phase Shift Keying
  - 00 = 0
  - 01 = π/2
  - 10 = -π/2
  - 11 = π





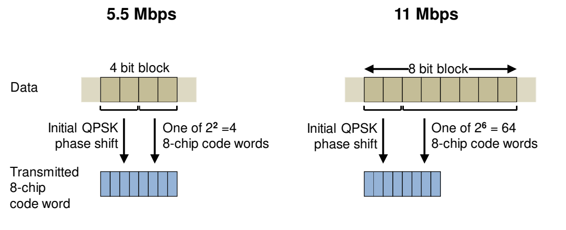
WLAN IEEE 802.11

HIGH RATE DIRECT SEQUENCE SPREAD SPECTRUM (HR/DSSS)

High Rate DSSS (802.11b) overview

- Efficient coding scheme using the same spectrum allocation of a 802.11 DSSS system
  - Introduced by IEEE 802.11b
- Basic idea:
  - Instead of transmitting a spreaded signal with a particular code sequence, different complex code sequences are used for spreading the transmitted signal
  - Each 8-bit word of the original signal is encoded with a complex chip word consisting of 8 symbols; the chip rate is 11 Mchip/s.
    - Complementary Code Keying (CCK)
  - Leads to practically the same spectrum allocation as a DSSS system

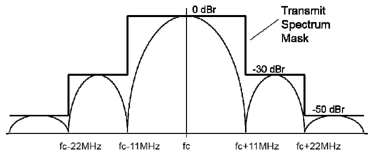
Complementary Code Keying (CCK)



Code word repetition rate = 1.375 Mwords/s

HR/DSSS Summary and Spectrum

- Maximum data rate: 11 Mbps
  - intermediate steps: 1, 2, 5.5, 11 Mbps
- Modulation: BPSK, DQPSK, CCK
  - CCK = Complementary Code Keying
    - High data rate DSSS coding with inherent spreading
- Channel bandwidth: 22 MHz
- HR/DSSS Spectrum Mask:

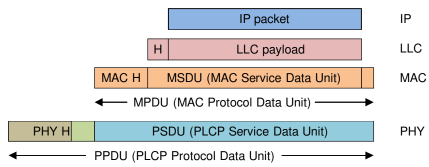


WLAN IEEE 802.11

HR/DSS PHY FRAMING

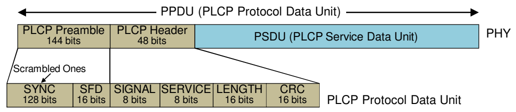
IEEE 802.11 Frame structure

- Each protocol layer deploys its own header for conveying the protocol information between peers



- IEEE 802.11 PHY header carries the information for setting up the reception of radio frames
- Physical Layer Convergence Protocol (PLCP) provides a PHY independent Service Access Point (SAP) for higher layers

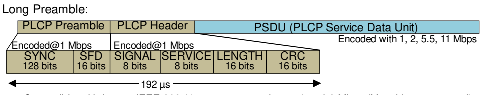
DSSS Physical Layer Convergence Protocol (PLCP)



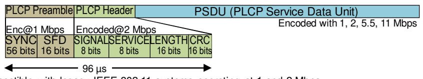
- SYNC - gain setting, energy detection, antenna selection, frequency offset compensation
- SFD - Start Frame Delimiter "0000 1100 1011 1101", bit synchronization
- SIGNAL - rate indication; (1, 2, 5.5, 11 Mbps)
- SERVICE – used to distinguish the coding schemes
- LENGTH - length of the PSDU part in µs
- CRC - CCITT CRC-16, protects signal, service, and length field
- Coding:
  - PLCP preamble is sent with minimum data rate (1 Mbps)
  - PLCP header is either send with 1 Mbps (long preample) or with 2 Mbps (short preample)

IEEE 802.11 DSSS Preambles

- The Preamble allows the receiver to acquire the wireless signal and synchronize itself with the transmitter.
- Long Preamble:



  - Compatible with legacy IEEE 802.11 systems operating at 1 and 2 Mbps (Megabits per second)
  - PLCP with long preamble is transmitted at 1 Mbps regardless of transmit rate of data frames
  - Total Long Preamble transfer time is a constant at 192 µs
- Short Preamble:



  - Not compatible with legacy IEEE 802.11 systems operating at 1 and 2 Mbps
  - PLCP with short preamble: Preamble is transmitted at 1 Mbps and header at 2 Mbps
  - Total Long Preamble transfer time is a constant at 96 µs

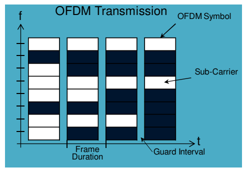
WLAN IEEE 802.11

ORTHOGONAL FREQUENCY DIVISION MULTIPLEX (OFDM)

Transformation of transmission symbols

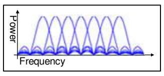
- More robust transmission by transformation of high speed bit sequences into a slower sequence of complex symbols

	D	e	m	o
ASCII	68	101	109	111
128	0	0	0	0
64	1	1	1	1
32	0	1	1	1
16	0	0	0	0
8	0	0	1	1
4	1	1	1	1
2	0	0	0	1
1	0	1	1	1



Orthogonal Frequency Division Multiplex (802.11a)

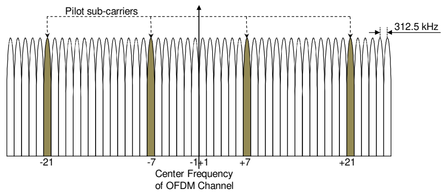
- Abbreviation: OFDM
- Introduced by 802.11a-1999
  - Cooperation with ETSI
  - Initially 5 GHz only
    - No need for backward compatibility



- Robust against reflections and multipath propagation
- Transforms data into a set of orthogonal signals
  - Each signal is build by a combination of 'tones'
- Generation/separation by FFT-64
  - FFT/IFFT required for coding/decoding
  - 52 sub-carriers out of the 64 samples used
- Guard periods between symbols enable orthogonality of subsequent symbols despite delay spread

OFDM – Time and frequency

- OFDM channel comprises 52 sub-carriers
  - 312.5 kHz sub-carrier spacing,
  - 48 data sub-carriers and 4 pilot sub-carriers
  - Total bandwidth: 16.25 MHz
- One OFDM symbol of a duration of 3.2 µs is sent every 4 µs
  - 250 kSymbols/s

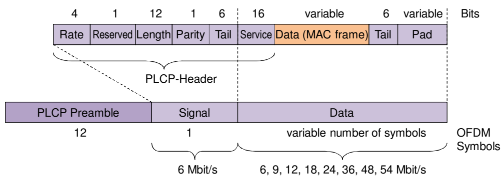


OFDM - Coding and Modulation

- 48 Data sub-carriers
- Sub-carrier modulation:
  - BPSK, QPSK, 16QAM, 64QAM
- Bit interleaved convolutional FEC coding
  - R=1/2, 2/3, 3/4
- Data rates:
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Data Rate (Mbps)	Modulation	Coding Rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	16-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

OFDM - PHY Frame Format



- OFDM PHY Preamble with 12 symbols takes 16 µs
  - 10 short training symbols without guard periods
    - Timing synchonization, antenna selection and locking to the signal
  - 2 long training symbols with guard periods for fine tuning
- Signal is one OFDM symbol with 24 data bits which takes 4 µs

WLAN IEEE 802.11

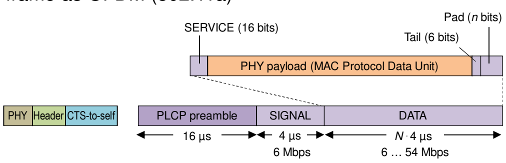
EXTENDED RATE

Extended Rate PHY (802.11g)

- Introduced by 802.11g
  - Uses OFDM according to 802.11a in the 2.4 GHz band
    - Backward compatibility with HR/DSSS added
- Support of data rates above 11 Mbps
  - Data rates like 802.11a: 6 Mbps up to 54 Mbps
- Advantages of OFDM in the 2.4 GHz band:
  - worldwide harmonized license-free frequency band
  - lower attenuation than in the 5GHz band
    - less transmission power required
- MAC layer extensions with backward compatibility to HR/DSSS
- Can use same transmission channels as HR/DSSS
  - 18 MHz OFDM fits easily in 22 MHz HR/DSSS channel

ERP PHY frame (OFDM native)

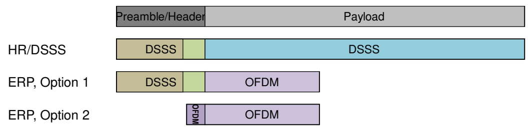
- Without backward compatibility, ERP deploys the same PHY frame as OFDM (802.11a)



- HR/DSSS systems are not able to decode OFDM PHY frames
  - For coexistence an additional protection methods like CTS-to-self or RTS/CTS may be required

ERP – HR/DSSS Interworking

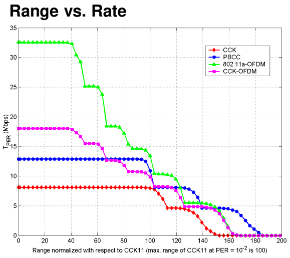
- ERP (802.11g) and HR/DSSS (802.11b) interworking is based on two alternatives regarding the ERP PHY frame structure:



- Option 1 enables HR/DSSS stations to decode the PHY header and keep off the medium according to the Length information
- Option 2 requires additional methods like CTS-to-self or RTS/CTS to provide information to HR/DSSS about other transmissions blocking the medium.

IEEE802.11 a/b/g – performance and efficiency

Range vs. Rate



Batra, Shoemake; Texas Instruments;
(Doc: IEEE 802.11-01-286r2)

Efficiency

Mode	Mod.	Coding	Mbps	Mbps	%
OFDM	64-QAM	3/4	54	26.12	48%
OFDM	64-QAM	1/2	48	23.25	48%
OFDM	16-QAM	3/4	36	18.31	51%
OFDM	16-QAM	1/2	24	14.18	59%
OFDM	QPSK	3/4	18	11.50	64%
OFDM	QPSK	1/2	12	8.31	69%
OFDM	BPSK	3/4	9	6.55	73%
OFDM	BPSK	1/2	6	4.64	77%
HR	CCK		11	7.18	65%
HR	CCK		5.5	4.07	74%
DSSS	QPSK		2	1.58	79%
DSSS	BPSK		1	0.81	81%

Huawei Quidway WA1006E Wireless Access Point
(http://www.sersat.com/descarga/quidway_wa1006e.pdf)

WLAN IEEE 802.11

HIGH THROUGHPUT (HT)

High Throughput (802.11n)

- Enhancement to OFDM (5GHz) and ERP (2.4GHz)
  - Up to 600 Mbps in either band
- Main techniques deployed for increase of bitrate:
  - Enhancements to OFDM modulation scheme and timing
  - Channel bonding of two adjacent channels to 40 MHz
  - Up to 4 parallel streams using MIMO (Multiple Input Multiple Output) technique
  - MAC frame aggregation
    - A-MPDU as well as A-MSDU
  - Block acknowledgements

HT PHY layer improvements

- OFDM (54 -> 58.5 Mbps)
  - 52 data sub-carriers instead of 48
- Forward Error Correction (58.5 -> 65 Mbps)
  - 5/6 coding rate in addition to 3/4
- Short Guard Interval (65 -> 72.2 Mbps)
  - 0.4 µs down from 0.8 µs
- Channel Bonding (72.2 -> 150 Mbps)
  - 40 MHz by combining two 20 MHz (108 data sub-carrier)
- MIMO (150 -> 600 Mbps)
  - Up to 4 parallel streams

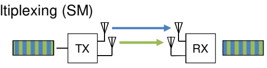
HT MCS Options for single stream

MCS Index	Spatial Streams	Modulation type	Coding rate	Data Rate [Mbps]			
				20MHz		40 MHz	
				0.8 µs GI	0.4 µs GI	0.8 µs GI	0.4 µs GI
0	1	BPSK	1/2	6.5	7.2	13.5	15.0
1	1	QPSK	1/2	13.0	14.4	27.0	30.0
2	1	QPSK	3/4	19.5	21.7	40.5	45.0
3	1	16-QAM	1/2	26.0	28.9	54.0	60.0
4	1	16-QAM	3/4	39.0	43.3	81.0	90.0
5	1	64-QAM	2/3	52.0	57.8	108.0	120.0
6	1	64-QAM	3/4	58.5	65.0	121.5	135.0
7	1	64-QAM	5/6	65.0	72.2	135.0	150.0

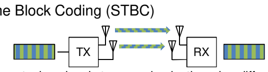
- For multiple streams multiply numbers in table by number of streams.

HT MIMO (Multiple Input Multiple Output)

- Spatial Multiplexing (SM)



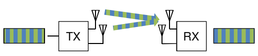
  - Subdivides an outgoing signal stream into multiple pieces, transmitted through different antennas.
  - When individual streams are received with sufficiently distinct spatial signatures, an SM enabled receiver can reassemble the multiple pieces back into one stream
  - Maximizes data rate.
- Space-Time Block Coding (STBC)



  - Sends an outgoing signal stream redundantly, using different coding for each of the transmit antennas
  - Receiver has a better chance of accurately decoding the original signal stream in the presence of RF interference and distortion.
  - STBC improves reliability by reducing the error rate and may be combined with SM.

HT MIMO

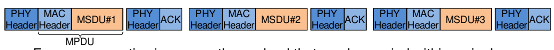
- Transmit Beamforming (TxBF)



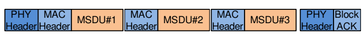
  - Steers signal stream towards the intended receiver by concentrating transmitted RF energy in a given direction.
  - Leverages signal reflection and multipath to improve received signal strength and sustain higher data rates.
  - Required channel knowledge can be obtained implicitly or explicitly by obtaining feedback from the receiver
- Availability in HT products:
  - Only Spatial Multiplexing is part of Wi-Fi certification for HT out of the three different MIMO techniques specified in the standard IEEE 802.11n.

HT MAC Protocol Data Unit Aggregation

- MAC efficiency suffers when transferring sequence of smaller frames



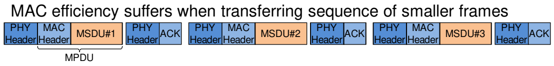
  - Frame aggregation increases the payload that can be carried within a single 802.11 physical layer frame
- MAC Protocol Data Unit Aggregation (A-MPDU) groups multiple MPDU sub-frames each with its own MAC header into one PSDU with up to 65535 bytes.



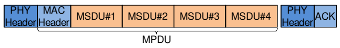
  - Reduced Interframe Space (RIFS) of 2µs used as delimiter between MPDUs
  - Block Acknowledgement for reduction of ACKs to one per multiple MPDU transmission
  - Selective retransmission of a single MPDU possible in the case that one of the aggregated MPDUs gets impacted.

HT MAC Service Data Unit Aggregation

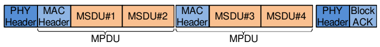
- MAC efficiency suffers when transferring sequence of smaller frames



- MAC Service Data Unit Aggregation (A-MSDU) groups multiple MSDUs into a single PSDU with a MAC header and up to 7935 data bytes.
  - All MSDUs with the same SA, DA and 802.11e QoS profile
  - High sensitivity against transmission errors; in the case of a single bit error the whole A-MSDU hast to be re-transmitted



- Higher resilience against transmission errors by a combination of MAC Service Data Unit aggregation and MAC Protocol Data Unit aggregation



  - Only erroneous MPDU has to be retransmitted.

WLAN IEEE 802.11

VERY HIGH THROUGHPUT (VHT)

Very High Throughput (802.11ac)

Extension to High Throughput in 5GHz with:

- Wider channel bandwidths
  - 80 MHz and 160 MHz channels in addition to 40 MHz and 20 MHz
- More MIMO spatial streams
  - Support for up to 8 spatial streams
- Multi-user MIMO (MU-MIMO)
  - Multiple STAs, each with one or more antennas, transmit or receive independent data streams simultaneously
  - Max. 4 streams to a single STA
- New MCS 8, 9
  - 256-QAM, rate 3/4 and 5/6, added as optional modes in addition to modes available in HT
- Single sounding and feedback format for beamforming
  - Instead of multiple methods in HT – to make certification happen.
- Coexistence mechanisms for 20/40/80/160 MHz channels
  - Dynamic spectrum allocation among 11ac and 11a/n devices
- Minor MAC modifications (mostly to support above changes)

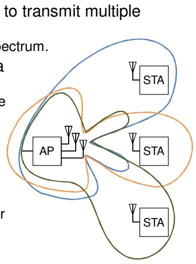
VHT MCS Options for single stream

MCS index	Spatial Streams	Modulation type	Coding rate	Data rate [Mbps]							
				20 MHz		40 MHz		80 MHz		160 MHz	
				0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI
0	1	BPSK	1/2	6.5	7.2	13.5	15.0	29.3	32.5	58.5	65.0
1	1	QPSK	1/2	13.0	14.4	27.0	30.0	58.5	65.0	117.0	130.0
2	1	QPSK	3/4	19.5	21.7	40.5	45.0	87.8	97.5	175.5	195.0
3	1	16-QAM	1/2	26.0	28.9	54.0	60.0	117.0	130.0	234.0	260.0
4	1	16-QAM	3/4	39.0	43.3	81.0	90.0	175.5	195.0	351.0	390.0
5	1	64-QAM	2/3	52.0	57.8	108.0	120.0	234	260.0	468.0	520.0
6	1	64-QAM	3/4	58.5	65.0	121.5	135.0	263.3	292.5	526.5	585.0
7	1	64-QAM	5/6	65.0	72.2	135.0	150.0	292.5	325.0	585.0	650.0
8	1	256-QAM	3/4	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0
9	1	256-QAM	5/6	N/A	N/A	180.0	200.0	390.0	433.3	780.0	866.7

- For multiple streams multiply numbers in table by number of streams.

Multi-User MIMO and Beamforming

- An VHT AP is able to use its antenna resources to transmit multiple frames to different clients.
  - all at the same time and over the same frequency spectrum.
- To send data to a particular user, the AP forms a strong beam toward that user
  - Minimizing at the same time the signal strength in the direction of the other users ("null steering")
  - Each of the users receives a strong signal of the desired data that is only slightly degraded by interference from data for the other users.
- AP has to know about the channel conditions to all connected terminals, detected
  - either detected implicitly out of the received signal, or
  - explicitly by the 802.11ac sounding protocol.
- By serving clients in parallel MU-MIMO allows to deliver more data in sum to clients being limited to a single or dual antenna.



MU- MIMO with combination of Beamforming and Null Steering

VHT (802.11ac) example configurations

Scenario	Typical Client Form Factor	PHY Link Rate	Aggregate Capacity
1-antenna AP, 1-antenna STA, 80 MHz	Handheld	433 Mbps	433 Mbps
2-antenna AP, 2-antenna STA, 80 MHz	Tablet, Laptop	867 Mbps	867 Mbps
1-antenna AP, 1-antenna STA, 160 MHz	Handheld	867 Mbps	867 Mbps
2-antenna AP, 2-antenna STA, 160 MHz	Tablet, Laptop	1.69 Gbps	1.69 Gbps
4-antenna AP, four 1-antenna STAs, 160 MHz (MU-MIMO)	Handheld	867 Mbps to each STA	3.39 Gbps
8-antenna AP, 160 MHz (MU-MIMO) -- one 4-antenna STA -- one 2-antenna STA -- two 1-antenna STAs	Set-top Box, Tablet, Laptop, PC, Handheld	3.39 Gbps to 4x STA 1.69 Gbps to 2x STA 867 Mbps to each 1x STA	6.77 Gbps
8-antenna AP, four 2-antenna STAs, 160 MHz (MU-MIMO)	Digital TV, PC, Tablet, Laptop,	1.69 Gbps to each STA	6.77 Gbps

'ac Wave 2' certification supports MU-MIMO, up to 4x4 MIMO and 160 MHz channel

WLAN IEEE 802.11

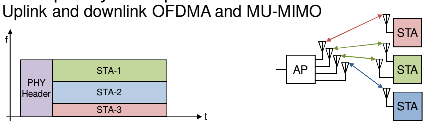
P802.11AX: NEXT GENERATION WI-FI

IEEE P802.11ax High Efficiency Wireless LAN

- The amendment defines standardized modifications to both the IEEE 802.11 physical layers (PHY) and the IEEE 802.11 Medium Access Control layer (MAC) that enable at least one mode of operation capable of supporting at least four times improvement in the average throughput per station (measured at the MAC data service access point) in a dense deployment scenario, while maintaining or improving the power efficiency per station.
  This amendment defines operations in frequency bands between 1 GHz and 6 GHz. The new amendment shall enable backward compatibility and coexistence with legacy IEEE 802.11 devices operating in the same band.
- No drive to increase peak data rates beyond what is already available by VHT
- Focus is on increasing usage of 802.11 in uncoordinated high density scenarios
- Three key focus points:
  - (1) To improve efficiency in dense networks with large number of STAs
  - (2) To improve efficiency in dense heterogeneous networks with large number of APs
  - (3) To improve efficiency in outdoor deployments
- The aim is to achieve a substantial increase in the real-world throughput
  - Creating an instantly recognizable improvement in QoE (cell edge behavior)
  - Generating spatial capacity increase (area throughput)

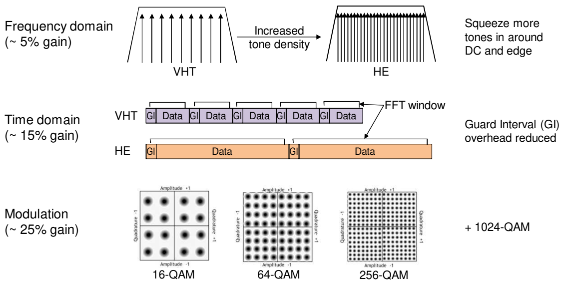
High Efficiency technical highlights

- Increase network efficiency through multiplexing users in both frequency and space
  - Uplink and downlink OFDMA and MU-MIMO



- Increase link efficiency with longer OFDM symbol (256-FFT) and high order modulation (1024-QAM)
- Increase spatial reuse through dynamic clear channel assessment (CCA)
- Improved support for outdoor operation (optional longer guard interval)

High Efficiency increased link efficiency



Further improvements

- Improved outdoor operation
  - Operates in higher delay spread channels than 11ac:
    - 11ac GI options: 0.4 µs and 0.8 µs
    - 11ax GI options: 0.8 µs, 1.6 µs and 3.2 µs
    - GI overhead mitigated with longer OFDM symbol
  - Some preamble fields repeated for higher reliability
  - Dual carrier modulation improves robustness in Data field
- Increased spatial reuse
  - Adjust CCA threshold based on transmit power of device
    - A device with low transmit power causes less interference than a device with high transmit power
      - o CCA threshold adjustment mitigates overlapping BSS traffic
  - BSS Color in the PHY header allows the identification of intra-BSS and inter-BSS PPDUs

P802.11ax timeline

- First chipsets already announced in spring 2017
- Wi-Fi Alliance certification will start based on P802.11ax-D2.0
  - Expected for November 2018
- Ratification expected for middle 2020
  - Well after first WFA certified products?

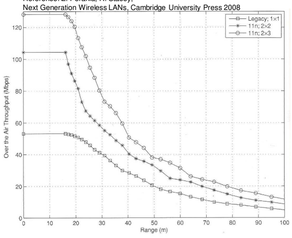
WLAN IEEE 802.11

WI-FI RADIO DEPLOYMENT HINTS

Wi-Fi Radio coverage and data throughput

- Wi-Fi basic parameters:
  - TX power usual 30..50 mW
  - Coverage range:
    - indoor: 30m, outdoor: 300m
    - strongly depending on environment
  - Max. stations per AP: ~ 35;
    - caused by particularities of CSMA/CD
    - newer deployments: ~ 10
  - Actual throughput:
    - up to ~ 120 Mbps (HT (802.11n), 2x2MIMO)
    - ~ 27 Mbps (ERP (802.11g))
    - ~ 5 Mbps (HR/DSSS(802.11b))
- Extending the coverage range:
  - APs more exposed, better antennas, more antennas, more MIMO, Wi-Fi mesh
- Extending the capacity limits:
  - smaller cells, more APs, sector antennas
    - decrease TX power to limit neighbor cell interference
- Unwanted interference
  - risky usage of unlicensed spectrum, heavily loaded, many potential interferer
  - denial of service attacks (intentionally or unintentionally)
    - usually limited to single APs/cells

Reference: E. Perahia, R. Stacey, Next Generation Wireless LANs, Cambridge University Press 2008



WLAN IEEE 802.11

WIGIG EXTENSION FOR 60 GHZ BANDS

WiGig Extension for 60 GHz bands

- 60 GHz license-exempt bands
- WiGig (802.11ad)@60 GHz
- Next generation 60 GHz system

IEEE802.11 (Wi-Fi) radio standards evolution

Std	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
	Jun 1997	2.4	20	1, 2	1	DSSS	40	150
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	40	150
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	40	150
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM (DSSS)	40	150
n	Oct 2009	2.4 5	20/40	up to 72.2/150	4	OFDM	60 40	200 150
y	Nov 2008	3.7	5/10/20	up to 13.5/27/54	1	OFDM	-	5 000
ac	Dec 2013	5	20/40/ 80/160	up to 87/200/433/867	8	OFDM	40	150
ad	Oct 2012	60	2000	up to 6 700	1	SC/OFDM	line of sight	-
af	Dec 2013	TV WS	1,2,4x 6/7/8	up to 1,2,4x 26.7/26.7/35.5	4	OFDM	100	1000
ah	Dec 2016	< 1	1/2/4/8/16	0.15 … up to 4.4/9/20/43/87	4	OFDM	100	1000
ax	~ 2020*	1…6	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2020*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	line of sight	

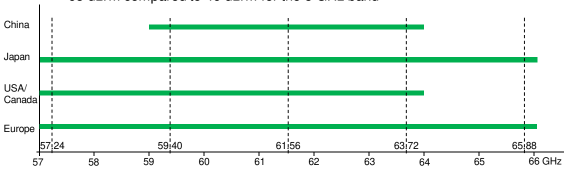
* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

WLAN IEEE 802.11

60 GHZ SPECTRUM

60 GHz unlicensed band

- 57 – 66 GHz is reserved worldwide for unlicensed operation
  - Only suited for communication over very short distances
  - Spectrum has extreme high attenuation
    - 68 dB/m compared to 46 dB/m for the 5 GHz band



- Provides up to 4 channels w/ 2.16 GHz each
- Maximum transmission power in the range of 10mW

WLAN IEEE 802.11

WIGIG IN 60 GHZ

WiGig Overview

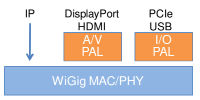
- Operates in the unlicensed 60 GHz frequency band
- Support for data transmission rates up to 7 Gbps
- Point-to-point operation over up to 10m
- Initially specified in IEEE 802.11ad, now contained in IEEE 802.16-2016
  - Extension of Wi-Fi to 60 GHz operation
  - Own PHY and MAC with fast transition support between 802.11 modes operating in the 2.4 GHz, 5 GHz and 60 GHz
- WiGig is brandname of Wi-Fi Alliance for 802.11ad
  - Certification program soon to be available
- Use cases:
  - P2P streaming, wireless docking, wireless kiosks

WiGig (802.11ad) Key features

- Channel bandwidth: 2.16 GHz
- Short distance < 10m over line-of-sight
  - Mainly indoor in single room
- Two different PHY modes: ~~OFDM~~ and Single Carrier
  - ~~OFDM: 693 Mbps – 6756 Mbps~~
  - SC: 27.5 Mbps – 4620 Mbps (low power: 626 – 2503 Mbps)
- Beamforming
  - Increasing signal strength to enable robust communication at distances beyond 10 meters
- Advanced security
  - Galois/Counter Mode of the AES encryption algorithm instead of CCMP
  - Allows for more effective implementations at highest speed
- Protocol adaptation for support of wireless implementations of HDMI, DisplayPort, USB and PCIe
  - Virtually instantaneous wireless backups, synchronization and file transfers

Protocol Adaptation Layers (PALs)

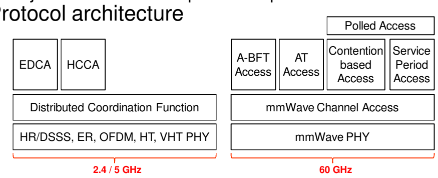
- Defined by WiGig Alliance to support specific data and display standards over 60 GHz



- PALs allow wireless implementations of these standard interfaces to run directly on the WiGig MAC and PHY
  - IP
    - Encapsulation of IP
  - Audio-visual (A/V)
    - Defines support for HDMI and DisplayPort,
  - Input-output (I/O)
    - Defines support for USB and PCIe

WiGig MAC/PHY Overview

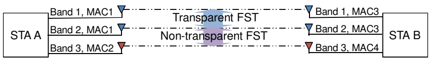
- Provides an unified and interoperable architecture across all implementations
  - Scalable across different usages, devices, and platforms
  - Adjustable to different power vs. performance trade-offs
- Protocol architecture



A-BFT: Association Beam Forming Training
AT: Announcement Time

MAC Features

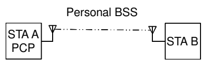
- Fast session transfer (FST) for multi-band operation
  - Enables transition of communication of STAs from any band/channel to any other band/channel in which 802.11 is allowed to operate
  - Supports both simultaneous and non-simultaneous operation
  - Supports both transparent and non-transparent FST
    - In transparent FST, a STA uses the same MAC address in both bands/channels involved in the FST
    - In non-transparent FST, the MAC addresses are different



- Several improvements to speed-up the FST switching time such as
  - Transparent FST,
  - Security key establishment prior to FST,
  - Block ACK operation over multiple bands

MAC Features, cont.

- Personal BSS (PBSS)
  - New network architecture in WiGig in addition to 802.11 infrastructure BSS and IBSS
  - In particular in support of applications like rapid sync-n-go file transfer, projection to TV/projector, etc.
  - Addresses challenges like directional channel access, power saving, etc.
  - Ad hoc network similar to the IBSS, but:
    - A STA assumes the role of the PBSS Central Point (PCP)
    - Only the PCP transmits beacon frames



- Channel Access
  - Channel access is coordinated using a schedule
    - Delivered by the PCP/AP to non-PCP/non-AP STAs
  - STAs are permitted to transmit data frames during contention-based periods (CBPs) and service periods (SPs)
    - Access during CBPs is based on EDCA fine-tuned for directional access
    - Access during SPs is reserved to specific STAs as announced in the schedule or granted by the PCP/AP

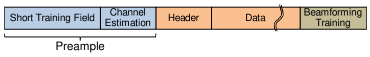
PHY Overview

- Different modulation types:
  - ~~OFDM~~
    - ~~for high performance on frequency selective channels up to 64 QAM~~
  - Single Carrier (SC)
    - for low power/low complexity transceivers
    - SC MCS 0
      - for control signaling (Channel, SNR durability)
    - SC Low Power MCS set
      - Simpler coding and shorter symbol structure to enable low power implementation
- Channelization:

Channel ID	Center Freq. (GHz)	Channel width (GHz)	OFDM Sampling Rate (MHz)	SC Chip Rate (MHz)
1	58.32	2.16	2640	1760
2	60.48	2.16	2640	1760
3	62.64	2.16	2640	1760
4	64.80	2.16	2640	1760

PHY General parameters

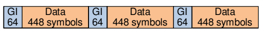
- Unified and interoperable PHY modes
  - Common preamble for all modulation types
  - Common MCS numbering scheme
  - Common frame structure



- Common LDPC Forward Error Correction
  - Four codes of common codeword length of 672
  - Excellent coding gain on realistic channels
  - Supports high throughput implementation
  - Single design supports code rates of 1/2, 5/8, 3/4, and 13/16
- Common SC PHY MCS 0
  - Very low SNR modem to allow pre-beamforming link, -78dBm sensitivity
  - Golay spreading sequence, differential encoding, and short rate 1/2 LDPC code
  - 27.5 Mbps PHY rate

Single-Carrier Data rates

- SC Modulation
  - 448 chips per symbol
  - 64 chips constant GI
    - Tracking purposes
    - Can be used for equalization
  - Pi/2 rotation applied to all modulations
- Data Rates



MCS index	Modulation type	Coding rate	Phy Rate (Mbit/s)	Sensitivity Power (dBm)
1	π/2-BPSK	1/4 (incl. repetition)	385	-68
2	π/2-BPSK	1/2	770	-66
3	π/2-BPSK	5/8	962.5	-65
4	π/2-BPSK	3/4	1155	-64
5	π/2-BPSK	13/16	1251.25	-62
6	π/2-QPSK	1/2	1540	-63
7	π/2-QPSK	5/8	1925	-62
8	π/2-QPSK	3/4	2310	-61
9	π/2-QPSK	13/16	2502.5	-59
10	π/2-16-QAM	1/2	3080	-55
11	π/2-16-QAM	5/8	3850	-54
12	π/2-16-QAM	3/4	4620	-53

OFDM Data Rates

- OFDM Modulation
  - 512 points FFT, 336 tones used for data, 16 pilot tones
  - Symbol length of 242.4ns, GI length of 48.4ns
- Data Rates:

MCS index	Modulation type	Coding rate	Phy Rate (Mbit/s)	Sensitivity (dBm)
13	SQPSK	1/2	693	-66
14	SQPSK	5/8	866.25	-64
15	QPSK	1/2	1386	-63
16	QPSK	5/8	1732.5	-62
17	QPSK	3/4	2079	-60
18	16-QAM	1/2	2772	-58
19	16-QAM	5/8	3465	-56
20	16-QAM	3/4	4158	-54
21	16-QAM	13/16	4504.5	-53
22	64-QAM	5/8	5197.5	-51
23	64-QAM	3/4	6237	-49
24	64-QAM	13/16	6756.75	-47

Low-Power Single-Carrier Data Rates

- Motivation and targets:
  - Peak power for the entire solution including PHY, MAC, Memory, RF, IOs, peripheral < 500 mW (e.g., USB 2.0)
  - Average power of PHY/MAC < 150 mW
  - Maximum delay spread for a 2 m range is in the order of 5 ns
- To meet targets low complexity low power mode with:
  - Simple FEC:
  - Simple Equalizer for very short multipath
- Data rates:

MCS index	Modulation type	Coding rate	Phy Rate (Mbit/s)	Sensitivity (dBm)
25	π/2-BPSK	13/28	626	-64
26	π/2-BPSK	1/2	834	-60
27	π/2-BPSK	5/8	1112	-57
28	π/2-QPSK	3/4	1251	-57
29	π/2-QPSK	13/16	1668	-57
30	π/2-QPSK	1/2	2224	-57
31	π/2-QPSK	5/8	2503	-57

Beamforming

- More important than in 2.4GHz or 5 GHz
  - Higher path loss
- Optional feature of WiGig
- Designed to enable reach of more than 10m
- May also be used to transmit over new path including reflection of the signal on the wall when direct path is obstructed.
- Unified protocol for simple, low power devices as well as complex devices
  - Same protocol is used for PCP/AP-to-STA beamforming and STA-to-STA beamforming
- BF comprised of two independent phases: sector level sweep (SLS) phase and beam refinement protocol (BRP) phase
  - SLS: enables communication at the control PHY rate (MCS0), and typically only provides transmit training
  - BRP: enables receiver training and iterative refinement of the AWV of both transmitter and receiver
- Support for beam tracking during data communication

WLAN IEEE 802.11

NEXT GENERATION 60 GHZ SYSTEM

Next-generation 60 GHz aka P802.11ay

- Rationale
  - Increased demand for capacity and new applications
    - Example: Backhaul, offloading, uncompressed video
  - Improve competitiveness with cable solution
    - Example: USB 3.1 (8 Gbps), Thunderbolt (20 Gbps)
- Objectives
  - Indoor and outdoor operations in license-exempt bands above 45 GHz
  - Supporting a maximum throughput of at least 20 Gbps
    - Throughput is measured at the MAC data service access point
  - Maintaining or improving the power efficiency per station
  - Enabling backward compatibility and coexistence with legacy directional multi-gigabit devices

WLAN IEEE 802.11

WI-FI EXTENSION FOR BELOW 1GHZ

IEEE802.11 (Wi-Fi) radio standards evolution

Std	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
	Jun 1997	2.4	20	1, 2	1	DSSS	40	150
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	40	150
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	40	150
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM (DSSS)	40	150
n	Oct 2009	2.4 5	20/40	up to 72.2/150	4	OFDM	60 40	200 150
y	Nov 2008	3.7	5/10/20	up to 13.5/27/54	1	OFDM	-	5 000
ac	Dec 2013	5	20/40/ 80/160	up to 87/200/433/867	8	OFDM	40	150
ad	Oct 2012	60	2000	up to 6 700	1	SC/OFDM	line of sight	-
af	Dec 2013	TV WS	1,2,4x 6/7/8	up to 1,2,4x 26.7/26.7/35.5	4	OFDM	100	1000
ah	Dec 2016	< 1	1/2/4/8/16	0.15 … up to 4.4/9/20/43/87	4	OFDM	100	1000
ax	~ 2020*	1…6	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2020*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	line of sight	

* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

WLAN IEEE 802.11

SUB 1GHZ UNLICENSED SPECTRUM

Unlicensed spectrum below 1 GHz

- Frequencies below 1 GHz provide link budget benefits of at least 10dB
  - Well suited for applications requiring longer reach and low power consumption
- Band allocation for some countries:

Country	Frequency [MHz]	max. allowed channel BW [MHz]	max. transmission power EIRP [mW]
China	775 - 779	1	5
	779 - 787	not defined	10
Europe	863 – 868.6	not defined	25
Japan	915.9 – 929.7	1	2 / 40
	920.5 – 923.5		500
South Korea	917 – 923.5	not defined	3 / 10
United States	902 - 928	not defined	1000

- Availability of spectrum and allowed operational parameters for Wi-Fi below 1 GHz strongly depends on the geographic area.

WLAN IEEE 802.11

SUB 1 GHZ WI-FI (HALOW)

Wi-Fi HaLow (IEEE 802.11ah)

Wi-Fi operating in frequency bands below 1 GHz for IoT and extended range

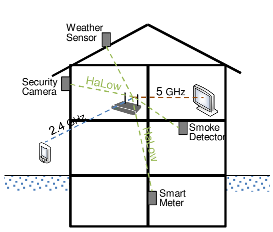
- Increased range compared to traditional Wi-Fi
  - For frequency bands below 1GHz with at least 10 dB link budget advantage
  - Reluctant to larger delay spread and Doppler spread supporting outdoor operation
  - An extra robust 1 MHz mode (MCS10) for up to 1 km range
- No need for interoperability with legacy IEEE 802.11 de
- Two types of device configurations:
  - IEEE 802.11ah-only for IoT-type connectivity
  - Multi-band devices
- Low Power Consumption
  - Multi-year battery life operation for sensors
- Rich Data Sets
  - 150Kbps ~ 87 Mbps per spatial stream
- Scalable bandwidth and MIMO support
  - 1, 2, 4, 8, 16 MHz channel; up to 4 parallel streams
- Scalable
  - Supports up to 8191 devices per AP
- IP Connectivity
  - Same as Wi-Fi

	Edge Rate (Range)	TxR
11ac/n 5 GHz 20 MHz BW 40 MHz BW	6.5 Mbps (27m)	3x2
11n/g 2.4 GHz 20 MHz BW	6.5 Mbps (54m)	3x2
11ah 900 MHz 8 MHz BW (US Only)	5.8 Mbps (88m)	2x2

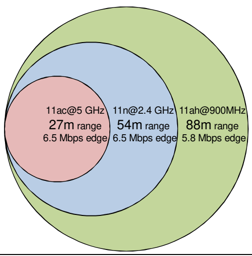
Simulation Assumptions: Minimum QoS 5Mbps, Retail AP, 21 dBm/Tx chain Tx power, Indoor to outdoor (d^4) channel model

HaLow (802.11ah) use cases

Sensors and meters



Extended range



HaLow (802.11ah) MAC Features

- Short frames to reduce active Tx/Rx time
  - 11ah Short Control frames: use an NDP (Non-Data-Packet) with MAC info in S1G field
  - Short MAC header
  - Short beacon frame (and compressed TIM) to reduce beacon decode times
  - Short probe request/response
- Support for larger number of associations
  - New TIM structure and encoding
  - Multiple TIM segments. First segment aligns with DTIM.
- Pseudo-scheduling and grouping sensor traffic
  - To support large number of devices in network and reduce contention time
  - Target wakeup times (TWT) for STAs agreed with AP
  - Periods of time where contention is restricted to group of STAs
  - Speed frame exchange, for quick UL/DL transaction
  - Improved PS-poll operation to allow sensors to sleep while AP fetches data
- Increase standby time
  - Operation without beacon; use of PS-Poll to check for data and/or re-synch
  - Expand listen and MAX BSS idle periods to allow STAs sleep for hours/days
- Coexistence and prioritization of sensor traffic
  - Ad hoc EDCA parameters to favor battery operated STAs
  - Reservation of periods of time for sensors

HaLow (802.11ah) basic PHY features

- 150 kbps – 346 Mbps data rates

Channel Bandwidth	Data rates for 1SS	Data rates for 2SS
1 MHz	150 kbps – 4.44 Mbps	600 kbps – 8.88 Mbps
2 MHz	650 kbps – 8.67 Mbps	1.3 Mbps – 17.3 Mbps
4 MHz	1.35 Mbps – 20 Mbps	2.7 Mbps – 40 Mbps
8 MHz	2.9 Mbps – 43.3 Mbps	5.8 Mbps – 87 Mbps
16 MHz	5.8 Mbps – 87 Mbps	11.7 Mbps – 173 Mbps

- 2, 4, 8, or 16 MHz channel bandwidth
  - 802.11ac OFDM design on a tenth clocking rate, i.e. 31.25 kHz spacing
  - Symbol length ten times of that in 802.11ac.
  - Up to 4x4 MIMO
- 1 MHz channel bandwidth:
  - 24 data subcarriers per OFDM symbol maintaining 31.25 KHz spacing
  - MCS 10 added for single stream long range transmission w/ 150 kbps
    - For sensing-type applications requiring extended range

S1G Data Rates

- Baseline design according 11ac/11n
  - Optimized for robust link and extended coverage in sub-GHz band
- IEEE 802.11ah MCS for 2MHz Bandwidth Channels:
  - MCS 9 is not valid for 802.11ah with a single spatial stream for a 2 MHz channel.

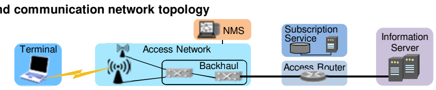
MCS Index	Modulation	Code Rate	Data Rate (Mbps) Normal GI (8µs)	Data Rate (Mbps) Short GI (4µs)
0	BPSK	1/2	0.65	0.72
1	QPSK	1/2	1.3	1.44
2	QPSK	3/4	1.95	2.17
3	16-QAM	1/2	2.6	2.89
4	16-QAM	3/4	3.9	4.33
5	64-QAM	2/3	5.2	5.78
6	64-QAM	3/4	5.85	6.5
7	64-QAM	5/6	6.5	7.22
8	256-QAM	3/4	7.8	8.67
9	256-QAM	5/6	8.67	9.63

WLAN IEEE 802.11

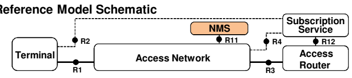
WLAN MANAGEMENT

Network Reference Model design

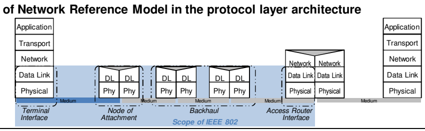
End-to-end communication network topology



Network Reference Model Schematic



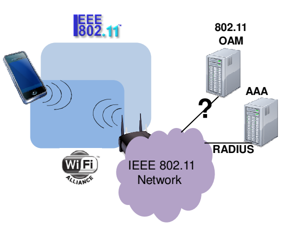
Data Path of Network Reference Model in the protocol layer architecture



WLAN IEEE 802.11

OAM FOR WI-FI

Standards for OAM of Wi-Fi



- IEEE 802.11 defines the radio interface of Wi-Fi
- Wi-Fi Alliance ensures compliance of the radio interface by certification
- OAM of the Wi-Fi radio interface is described by a comprehensive IEEE 802.11 MIB
- A couple of organizations developed special variants of OAM interfaces for Wi-Fi
- BTW: For AAA there is a single solution specified: RADIUS

RADIUS (Remote Authentication Dial-In User Service)

- RFC 2865 & RFC 2866 (RADIUS/RADIUS Accounting)
  - Common solution for the communication between Access Point and AAA server for user authentication, user authorization and user accounting.
- RFC3580 (IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines).
  - Support of EAPoLAN (IEEE 802.1X), which was introduced to IEEE 802.11 through IEEE 802.11i-2004
- RFC7268 (RADIUS Attributes for IEEE 802 Networks)
  - Further IEEE802 specific attributes for support of interworking with external networks and enhanced security modes.
- RFC5580 (Carrying Location Objects in RADIUS and Diameter)
  - Transport of location information over the AAA infrastructure.

'OAM' Interface Specifications for 802.11

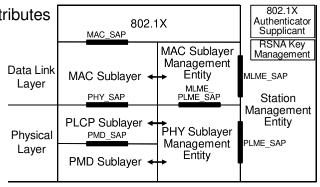
- IEEE 802.11 SNMP MIB
  - Comprehensive definition of all management information of IEEE 802.11
  - Aimed for SNMP management but rarely implemented
- BroadBandForum
  - Wi-Fi model and attributes of Device Data Model 2 (TR-181) for CPE WAN Management Protocol (TR-069)
  - CableLabs
    - Wi-Fi Provisioning Framework Specification (WR-SP-WiFi-MGMT)
- IETF CAPWAP
  - Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification (RFC5415) and Binding for IEEE 802.11 (RFC5416)
- LINUX Wireless
  - mac80211 Wi-Fi driver architecture with cfg80211 kernel configuration module and nl80211 netlink user space interface

IEEE802.11 SNMP MIB

- IEEE 802.11 MIB follows the generic protocol architecture
  - Annex C of specification and available by http://www.ieee802.org/11/802.11mib.txt

Major sections

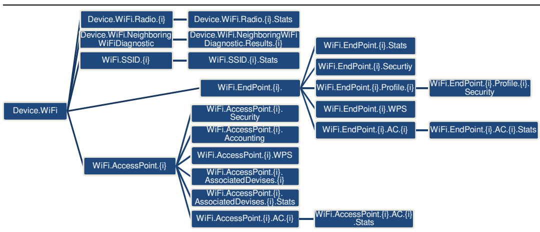
- Station Management (SMT) Attributes
  - dot11smt GROUPS
    - dot11StationConfigTable
    - ...
    - dot11RSNAConfigDLCGroupTable
- MAC Attributes
  - MAC GROUPS
    - dot11OperationTable
    - ...
    - dot11ResourceInfoTable
- PHY Attributes
  - PHY GROUPS
    - dot11PhyOperationTable
    - ...
    - dot11TransmitBeamformingConfigTable



BroadBand Forum TR-181

- TR-181 defines version 2 of the TR-069 Device data model (Device:2)
  - Applicable to all types of TR-069-enabled devices.
  - Obsoletes both Device:1 and InternetGatewayDevice:1 specifications
- Based on TR-069 / CWMP (CPE WAN Management Protocol)
  - https://www.broadband-forum.org/cwmp.php
  - TR-069 is an soap/HTTP based protocol for transmission of XMLbased descriptions of management models between CPE and ACS
- The TR-069 Management Data Model Schema is specified in TR-106.
  - TR-069 Data Models are xml documents that are "schema-like", that describe the management objects and parameters used for particular use cases.
- TR-181 provides a compact set of IEEE 802.11 specific attributes for configuration
  - Only a small subset of the attributes in IEEE 802.11
- TR-181 adds to each of the elements of the Wi-Fi model a rich set of attributes for monitoring/accounting/statistics.

TR-181 Wi-Fi Model



- TR-181 supports two kinds of devices: APs and (nonAP) STAs (Endpoints)
- A Wi-Fi device consists out of 1..n radio interfaces, 1..n SSIDs and 1..n AccessPoints or EndPoints

CableLabs amendments to TR-181

- WR-SP-WiFi-MGMT-I05-141201.pdf is CableLabs' most relevant specification for OAM of Wi-Fi interfaces.
- CableLabs builds management of Wi-Fi on top of TR-069 approaches by
  - adopting the TR-181 device model for Wi-Fi
  - amending the device model by vendor specific extensions for missing functions
    - RadiusClient
    - Interworking Service
    - Passpoint
    - ClientSessions
    - ClientState
    - ApNeighborStats
    - AccessControlFilter
  - defining a compatible SNMP MIB to enable backward-compatibility to the legacy provisioning and management systems in the cable environment

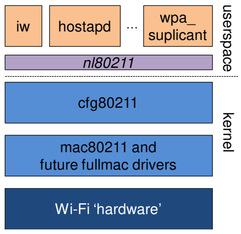
IETF CAPWAP

- CAPWAP (Control And Provisioning of Wireless Access Points) specifies interface between a wireless termination point (WTP) and an access controller (AC)
- Supports different architectural models with various possibilities to locate functions either in WTB or AC

```
+-+         wireless frames        +-+       +-+wireless frames +-+ 802.3 frames +-+
| |--------------------------------| |       | |----------------| |--------------| |
| |              +-+               | |       | |                | |              | |
| |--------------| |---------------| |       | |----------------| |--------------| |
| |wireless PHY/ | |     CAPWAP    | |       | |wireless PHY/   | |    CAPWAP    | |
| | MAC sublayer | |               | |       | | MAC sublayer   | |              | |
+-+              +-+               +-+       +-+                +-+              +-+
STA              WTP                AC       STA                WTP               AC

Split MAC CAPWAP Architecture                Local MAC CAPWAP Architecture
```

- RFC 5415 defines Control And Provisioning of Wireless Access Points (CAPWAP) Protocol
- RFC 5416 provides Binding of CAPWAP for IEEE 802.11, i.e. management model
- RFC 7494 amends RFC5416 for more recent 802.11 standards and deployment scenarios
  - RFC7494: IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP)

LINUX Wireless Wi-Fi driver architecture



- nl80211 has become defacto standard for Wi-Fi configuration in LINUX
  - Defines a comprehensive list of controls, commands and attributes for Wi-Fi
  - Communicates by netlink (RFC3549) with kernel
- cfg80211 provides unified interface into kernel drivers
- Two variants for implementation of MAC
  - softmac or fullmac

Wi-Fi OAM specification 'nl80211.h'

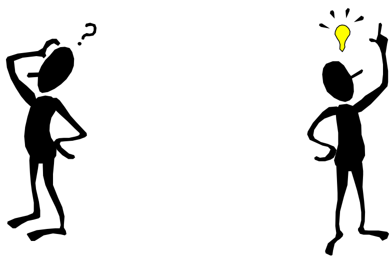
```
#ifndef __LINUX_NL80211_H
#define __LINUX_NL80211_H
/*
 * 802.11 netlink interface public header
 *
 * Copyright 2006-2010 Johannes Berg <johannes@sipsolutions.net>
 * Copyright 2008 Michael Wu <flamingice@sourmilk.net>
 * Copyright 2008 Luis Carlos Cobo <luisca@cozybit.com>
 * Copyright 2008 Michael Buesch <m@bues.ch>
 * Copyright 2008, 2009 Luis R. Rodriguez <lrodriguez@atheros.com>
 * Copyright 2008 Jouni Malinen <jouni.malinen@atheros.com>
 * Copyright 2008 Colin McCabe <colin@cozybit.com>
 *
 * Permission to use, copy, modify, and/or distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this permission notice appear in all copies.
 *
 * THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
 * WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
 * ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
 * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
 * ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
 * OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
 *
 */

#include <linux/types.h>

#define NL80211_GENL_NAME "nl80211"

/**
 * DOC: Station handling
 *
 * Stations are added per interface, but a special case exists with VLAN
 * interfaces. When a station is bound to an AP interface, it may be moved
 * into a VLAN identified by a VLAN interface index (%NL80211_ATTR_STA_VLAN).
 * The station is still assumed to belong to the AP interface it was added
 * to.
 *
```

- http://git.kernel.org/cgit/linux/kernel/git/linville/wireless.git/tree/include/uapi/linux/nl80211.h?id=HEAD
- nl80211.h defines
  - 120 commands
  - about 600 attributes and controls
- nl80211.h is allowing access to most of the PHY, MAC and SME parameters of a Wi-Fi radio interface
- Scope similar to IEEE 802.11 SNMP MIB

WLAN IEEE 802.11

END OF SON WLAN LECTURE

Questions and answers



Questions

Spectrum

1) What is the optimal channel arrangement for a 802.11g/n-only system in Europe?
2) What is the channel bandwidth of 802.11b?
3) What are the frequencies for unlicensed operation in 5 GHz in Europe?
4) What is the purpose of DFS and TPC in the 5 GHz band?
5) For which frequencies is the support of DFS and TPC mandatory in Europe?
6) How many non-overlapping 80MHz channels can be arranged in the 5 GHz range in Europe?

Radio standards for 2.4/5 GHz

1) What are the IEEE 802.11 radio standards for operation in 2.4 GHz?
2) What are the IEEE 802.11 radio standards for operation in 5 GHz?
3) What are the bit-rates provided by Complementary Code Keying in 2.4 GHz?
4) What modulation schemes are used for direct sequence spread spectrum?
5) What are the bit-rates supported by a high-rate direct sequence spread spectrum system?
6) What is the difference between a PPDU and MPDU data frame?
7) What is the purpose of the preample of the physical layer protocol data unit?
8) What is the difference between the long preample and short preample?
9) What does OFDM stand for?
10) How many sub-carriers are used by the OFDM introduced by 802.11a?
11) What is the purpose of guard intervals in OFDM?

More questions…

12) Which data rates are supported by OFDM as introduced by 802.11a?
13) How long does a OFDM PHY preample in 802.11a take?
14) What is the benefit when operating the Extended Rate PHY without backward compatibility to HR/DSSS?
15) What additional methods are needed for coexistence of Extended Rate PHY without backward compatibility with HR/DSS?
16) What bitrates are supported by the Extended Rate PHY?
17) What are the main techniques deployed by the High Throughput PHY for increased bitrates?
18) What additional modulation types are available in High Throughput PHY (802.11n) compared to OFDM (802.11a)?
19) Which MIMO methods are specified in 802.11n, and which of them is mandatory for certification?
20) What is the benefit of MAC Protocol Data Unit aggregation compared to MAC Service Data Unit aggregation?
21) What is the drawback of MAC Protocol Data Unit aggregation compared to MAC Service Data Unit aggregation?
22) By which means does Very High Throughput PHY (802.11ac) provide higher bitrates compared to High Throughput PHY (802.11n)?
23) What is the difference between explicit beam-forming and implicit beam-forming?
24) What is the maximum bitrate of Very High Throughput PHY, and what is the maximum bitrate for serving a single STA with MU-MIMO?

More questions…

WiGig (802.11ad) radio standard

1) In which frequency range operates WiGig (802.11ad)?
2) What is the purpose of the Fast Session Transfer?
3) What is the difference between transparent and non-transparent Fast Session Transfer?
4) What PHY modes are supported by WiGig (802.11ad)?
5) For what special purpose is Single Carrier MCS0 used in 802.11ad?
6) What were the motivations and targets for introducing low-power Single Carrier data rates in 802.11ad?
7) What is the highest bitrate of Single Carrier PHY mode in 802.11ad?
8) What is the purpose of Protocol Adaptation Layers in 802.11ad?

HaLow (802.11ah) radio standard

1) What are the two main use cases of 802.11ah?
2) For what frequency range is 802.11ah designed for?
3) Which channel bandwidths are supported by 802.11ah?
4) What is the maximum bitrate of MCS10 at 1 MHz bandwidth of 802.11ah?
5) What is the maximum bitrate of HaLow for a single stream?
6) How many terminals can concurrently connect to an 802.11ah AP?
7) How relates the OFDM used by 802.11ah to the OFDM used by 802.11ac?
8) What is the length of the guard interval of HaLow?

More questions…

OAM for Wi-Fi

1) What kind of OAM interface specification does IEEE 802.11 provide?
2) What is the specification of the BroadBand Forum describing the management model for Wi-Fi?
3) Which protocol is used for carrying TR-181?
4) Which specification was adopted by CableLabs to define their extensions?
5) Which organization did ‘CAPWAP’ standardize?
6) Which architectural models are supported by CAPWAP?
7) What is Wireless Linux ‘nl80211’?
8) How does nl80211 communicate with its lower layer in the kernel?

Anything left?

Thank you for your attendance!