Wireless LAN Standards

802.11 and variants
HiperLAN and HiperLAN/2

IEEE 802 Group

- Develops LAN/MAN standards
- Individual working groups focus on specific areas, e.g.,
  - 802.3 also called Ethernet
  - 802.11 the wireless LAN standard
  - 802.15 the wireless PAN standard

IEEE 802.11 Wireless LAN

- Formed in 1990
- Defines the PHY and MAC layer
- Frequency bands used are in ISM or U-NII bands
- Represents the first standard for WLANs
  - Before: application specific proprietary products (may have better performance for the given application but vendor specific and expensive)
- Originally to develop standard for data rates of 1Mbps and 2Mbps - released in 1997.

IEEE 802.11 Evolution

	802.11a	802.11b	802.11
Standard Approved	September 1999	September 1999	July 1997
Available Bandwidth	300MHz	83.5MHz	83.5MHz
Unlicensed Frequencies of Operation	5.15-5.35GHz, 5.725-5.825GHz	2.4-2.4835GHz	2.4-2.4835GHz
Number of Non-Overlapping Channels	4 (Indoor) 4 (Indoor/Outdoor) 4 (Indoor/Outdoor)	3 (Indoor/Outdoor)	3 (Indoor/Outdoor)
Data Rate per Channel	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2 Mbps
Modulation Type	OFDM	DSSS	FHSS, DSSS

802.11g: not released yet, backwards compatible with 802.11b, defines symbol rates up to 54Mbps using OFDM

IEEE 802.11 Wireless LAN

- Two kinds of operation:
  - Ad hoc
    IBSS (Independent Basic Service Set)
  - Client-server
    Infrastructure mode (basic service set)
- A BSS (Basic Service Set) is a working group of at least two nodes (or stations – STA)

802.11 PHY

- Originally 3 different channel options:
  - Infra-red
  - Frequency Hopping Spread Spectrum (FHSS) 2.4GHz
  - Direct Sequence Spread Spectrum (DSS) 2.4GHz
- Radiated power is limited
  - 1W in the US (for radio) – limited more
  - ~20mW in Europe, 1mW in Japan (for radio)

1

802.11 Infrared PHY

- Not really used – IrDA is more common and cheap.
- Provides data rates of 1Mbps and 2Mbps
- Max output power is 2W
- Works in the ~900nm range (regular IR LED)

802.11 FHSS PHY

- 22 hop patterns to choose from
- 79 hopping frequencies
- 1 or 2 Mbps
- Some early products favored it because it is less prone to interference.
- Not really used anymore since it can not scale well with higher symbol rates.
- 20msec dwell time -> 50 hops/sec

802.11 DSS PHY

- 3 separate channels in the 80MHz wide band of the 2.4GHz ISM – each 20MHz wide.
- Baker sequence (PN-sequence) to modulate the data stream (to spread the spectrum).
- Not to be confused with CDMA! Here the PN sequence is fixed for all stations and published in the standard, thus DSS – originally used for encryption – is only used to spread energy.
- 1 or 2 Mbps symbol rate.

802.11 MAC layer

- Two access functions defined.
  - The default is: Distributed Coordination Function (DCF) and is CSMA/CA based.
  - The optional access method is the Point Coordination Function (PCF) . Only to be used in the infrastructure mode. Based on a TDMA polling scheme.

Distributed Coordination Function (DCF) - CSMA/CA

- All stations have to be equipped with DCF. The DCF can be used in both the IBSS and infrastructure modes.
- STAs have to monitor the channel. If the channel is busy, stations have to back-up for a random time.
- RTS – CTS message exchange for CA.
- ACK packets for fast arq after data transmission.

CSMA

- A station desiring to transmit has to sense the medium. If the medium is busy the station will defer its transmission for a later time. If the medium is free, the station can go ahead and transmit.
- Collision Avoidance is needed (Detection cannot be used)

CSMA/CA

- If the medium is free for a specific time duration (DIFS – Distributed Inter Frame Space) then the station can transmit.
  - This enables radio propagation delay
  - Also, since time is not slotted, nodes will not know the difference between a free channel or a temporary free (e.g., between an RTS and CTS or data and ACK) channel otherwise.

CSMA/CA

- Virtual Carrier Sense
  - A fancy name for RTS/CTS exchange or CA.
  - A station contending for the channel sends out an RTS message first. RTS contains the destination and the required time needed for the entire transmission process.
  - The CTS response will contain the duration of the transmission process too, thus all nodes that are susceptible for a hidden terminal interference can keep a timer for the duration of this transmission.

CSMA/CA

- The virtual carrier sense indicator is also called Network Allocation Vector.
- The physical carrier sensing and the virtual carrier sensing functions will provide the nodes the information about the channel's state.
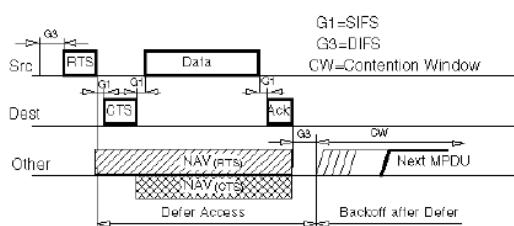- Time between RTS-CTS-data-ACK has to be smaller than DIFS, and is maximized in SIFS (Short Inter Frame Space)

CSMA/CA

- Back-off is based on BEB (Binary Exponential Back-off).
- If nodes are backed-off and the channel is empty for at least DIFS, then they start decrementing their back-off counter with a given frequency.

DCF

MAC Layer Acknowledgments

- "Collision Detection" is employed by the use of ACK packets after each transmission (and CRC check).
- Exceptions are the multicast transmissions.
- Thus the MAC layer provides with guaranteed delivery.

Fragmentation and Reassembly

- In a wireless environment it is more error-safe and efficient to transmit short packets:
  - Higher BER of wireless
  - Retransmission times should be considered
  - Shorter messages can have better FEC.
- Since Ethernet packets can be up to ~1500 bytes long it would be beneficiary if WLAN could provide the same size.

Fragmentation and Reassembly

- 802.11 uses a simple F&R:
  - Larger PDUs can be divided up into smaller fragments and sent one-by-one.
  - Fragments have to arrive ordered – a station cannot send a new segment until the previous one has been acknowledged.
  - If a fragment has been retransmitted too many times, the entire frame has to be dropped.

Joining a BSS

- If a station wants to join an existing BSS, it needs to be synchronized to the AP. This can happen in two ways:
  - Passive scanning: a station is scanning the channel for a beacon frame (a periodic frame sent by the AP for synchronization)
  - Active scanning: the station tries to find an AP by transmitting Probe Request frames, waiting for a Probe Response.
- Performance trade offs

Authentication Process

- Once a station has found an Access Point and decided to join the BSS, it will go through the optional authentication process
- Authentication is based on the knowledge of a password or encryption key

Association Process

- Once a station is authenticated, it will start the association process, which is the exchange of information about the BSS capabilities (e.g., roaming).
- Only after the association is completed can a station transmit and receive data frames.

Power Saving

- Battery power is a scarce resource in mobile equipment using WLANs.
- Stations in the infrastructure mode can go into a Power Saving Mode.
- The AP maintains a record of the stations in the power saving mode and buffers packets until the stations poll the AP for it or change their mode.

Power Saving

- APs periodically transmit beacon frames (for synchronization). This beacon frames also include information on which stations have back-logged packets waiting.
- Stations in the power saving mode monitor beacon transmissions, awake and "poll" the AP for these packets.
- Multicast messages are transmitted at an a priory known time, where all stations who wish to receive these information should wake up.

Timing

Short Inter Frame Space

- SIFS
- To separate transmission belonging to the same dialogue.
- Radio switch over times have to be calculated.
- Set to 28μs in 802.11

Point Coordination IFS

- Used to give priority access to Point Coordinator (PC).
- Only the Point Coordinator can access a channel between SIFS and DIFS.
- Set to SIFS + a virtual slot time (the time the back-off counter is working), thus its value is 78μs in 802.11.

Distributed IFS

- For stations that wait for a free channel to contend.
- Set to PIFS + a virtual slot time, thus 128μs in 802.11.

Extended IFS

- A node that receives a non-decodable (e.g., due to collision of two RTS messages) message has to wait at least EIFS time before it can access the channel again.

Frame Types

- Data Frames
- Control Frames (e.g., RTS, CTS, ACK)
- Management Frames (exchanged the same way as data frames but are not reported to the higher layer).

Frame Format for All Frames

Preamble	PLCP Header	MAC Data	CRC

- Preamble (PHY dependent)
  - Synch – An 80 bit sequence of alternating zeros and ones
  - SFD – Start frame delimiter, 16 bit pattern: 0000 1100 1011 1101 (for frame timing)

Frame Format for All Frames

Preamble	PLCP Header	MAC Data	CRC

- PLCP Header (has to be transmitted with 1Mbps)
  - Length Word – number of bytes in this packet (good for PHY)
  - Signalling Field – for data speed
  - HEC – 16 bit CRC for the header

Frame Format for All Frames

Preamble	PLCP Header	MAC Data	CRC

- General MAC Data and CRC

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration or ID	Addr. 1	Addr. 2	Addr. 3	Sequnc. Control	Addr. 4	Frame Body	CRC

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- Protocol Version:
  - To differentiate between, e.g., 802.11, 802.11a,b,e,g,h,i

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- Type and Subtype
  - Define the type of the frame (management (e.g., beacon, probe, association), control (e.g., RTS, CTS, Poll, ACK) , or Data). There are more than 30 different types of frames defined.

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- ToDS
  - 1 In case the AP is not the final destination but the Distribution System
- FromDS
  - 1 in case the frame is coming from the DS

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- More fragments
  - To signal more incoming fragments
- Retry
  - 1 if it is a retransmission fragment

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- Power Management
  - To signal that station is changing from Active to power save mode (or vice-versa)
- More Data
  - There are more frames buffered to this station (for polling or changing status)

Frame Control Field

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4		1	1	1	1	1	1	1	1

- WEP
  - Indicates that the frame body is encrypted with WEP
- Order
  - The frame is in a stream that is strictly ordered (for legacy applications – DEC's LAT)

Frame Format for All Frames

Preamble	PLCP Header	MAC Data	CRC

- General MAC Data and CRC

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration or ID	Addr. 1	Addr. 2	Addr. 3	Sequnc. Control	Addr. 4	Frame Body	CRC

MAC Data Fields

- Duration/ID
  - Duration used for NAV calculation
  - (or station ID for power save polling)
- Sequence Control
  - Frame numbering and fragment numbering
- CRC
  - 32 bits

Address Fields

- Address-1

  Recipients Address (if TODS is not set this is the AP if it is set then the address of the end station)
- Address-2
  - Transmitters Address (if FromDS then address of AP, else the address of source)

Address Fields

- Address-3

  If FromDS is set then the original source address, if ToDS is set, then the final destination
- Address-4
  - For the wireless distribution system, where a frame is transmitted from one Access point to another

Example: RTS Frame

octets: 2	2	6	6	4
Frame Control	Duration	RA	TA	CRC

MAC Header

- RA: Intended immediate recipient
- TA: The station transmitting this frame
- Duration: (in μs) the time required to transmit the next (data) frame plus a CTS frame plus an ACK frame and three SIFSs

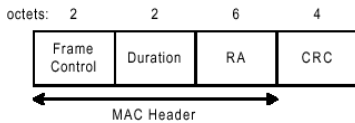## Example: CTS Frame

octets: 2	2	6	4
Frame Control	Duration	RA	CRC

MAC Header

- RA: The TA field of the RTS message
- Duration: (in μs) the duration value of the previous RTS frame minus a CTS time minus one SIFS.

Example: ACK Frame

octets: 2   2   6   4

| Frame Control | Duration | RA | CRC |

MAC Header

- RA: is copied from the Address –2 field of the previous frame
- Duration: set to 0 if More Fragment bit was 0, otherwise the duration of the previous frame minus an ACK time minus one SIFS.

802.11 Task Groups

802.11b (Task Group b)

- Standard accepted in 1999.
- Most popular WLAN standard today.
- The WECA (Wireless Ethernet Compatibility Alliance or Wi-Fi Alliance) adopted 802.11b and renamed it Wi-Fi 2.4GHz (Wireless Fidelity).
- MAC is identical to that of 802.11
- PHY is solely 2.4GHz DSS, with rates: 11, 5.5, 2, 1Mbps.

802.11a (Task Group a)

- Standard accepted in 1999. People had to wait for products for more than 2 years.
- Quickly emerging.
- WECA adopted it as Wi-Fi 5.2GHz.
- MAC is identical to that of 802.11
- PHY is (Code) Orthogonal Frequency Division Multiplexing (OFDM) at 5.2GHz.
- Symbol rates of 54, 48, 36, 24, 12, 9, 6Mbps.
- 8 independent channels.

802.11a (Task Group a)

- 20MHz channels are divided into 52 sub-channels, each about 300kHz wide. 48 are used for data while 4 for FEC. Amplitude keying and phase keying modulation – high spectral efficiency. Well suited for indoor environments.
- The first products are just announced and are already capable of 108Mbps – will IEEE adopt this? (Atheros turbo mode of 72Mbps)
- Will the higher frequency have an essential impact on the communication range?

802.11a Physical (OFDM)

- Channels are of 20MHz
- Each channel has 52 "narrow-band" 300kHz carriers, (used by one station at a time)
- 108Mbps is enabled using two channels simultaneously.

Eight channels in lower 5-GHz band   One Channel (detail) 20-MHz

52 Carriers

Each carrier is ~300kHz wide

Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

- Power consumption is similar, although it takes 4 to 9 times less energy to transmit a given length packet (due to speed) with 802.11a.
- 8 independent channels with 802.11a compared to 3 for Wi-Fi for cellular networks.
- Max data speed is 5 to 10 times higher.

Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

- Wi-Fi 5.2GHz has no other equipment interfering with it (yet), including microwave ovens. Can co-exist with Bluetooth or Wi-Fi 2.4GHz.
- Atheros claims, that during real measurements, the throughput of 802.11b never superseded that of 802.11a (in a typical office environment - despite the higher frequency band usage) – see diagrams on next pages.
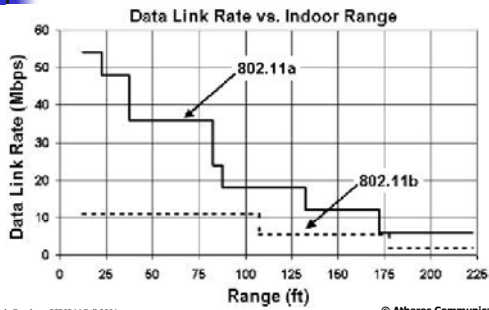
Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

Data Link Rate vs. Indoor Range

Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

Throughput Comparison
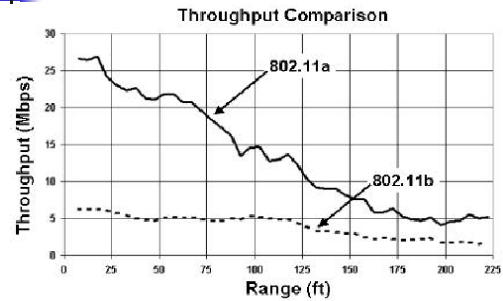
Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

Cells and Co Channel Interference
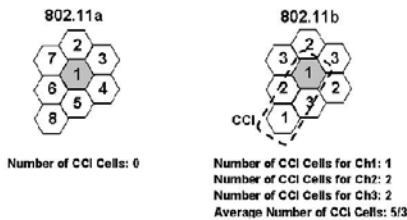
802.11a vs. Wi-Fi

8 Cell System – Average Cell Throughput
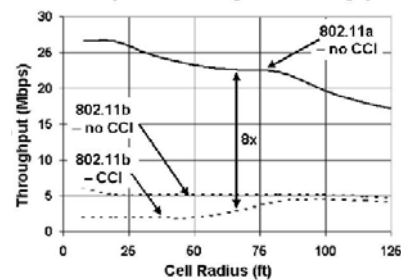
802.11a vs. Wi-Fi
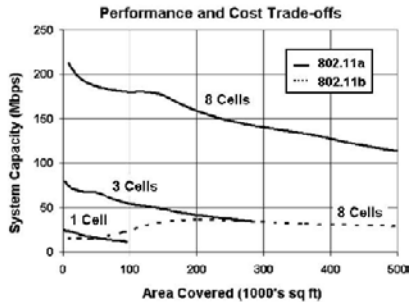
802.11g

- MAC remains the same as 802.11
- PHY to be backwards compatible with Wi-Fi 2.4GHz, thus at 2.4GHz.
- High symbol rate modes of up to 54Mbps using OFDM, lower speeds up to 11Mbps using DSS. I took long to reach a common agreement.
- Final specification expected soon.

802.11h

- There were strong European concerns that 802.11a could interfere with NATO satellites and microwave radar systems.
- To avoid such interference, two extensions to the PHY of 802.11a were added in 802.11h:
  - the capability to select the employed channel automatically based upon observations (DFS – Dynamic Frequency Selection)
  - ensuring the enforcement of strict radio power control (TPC – Transmit Power Control)

802.11e

- Goal: to define a new MAC.
- Addressing the flaw of IEEE802.11 working in a best effort mode, not being able to provide with any QoS provisioning.
- Task Group e is redefining both the centrally controlled channel access as well as redefining the contention based channel access of CSMA/CA including priorities to ensure that packets with higher priorities enjoy access benefits compared to lower priority packets in a Differentiated Services manner. This later function is called the *Enhanced Distributed Coordination Function* (*EDCF*).

Other Task Groups

- **IEEE802.11.c:** wireless extension to IEEE802.1D enabling bridging using IEEE802.11
- **IEEE802.11.d** deals with including country specific information into the beacon transmissions, so STAs are informed what part of the spectrum is available and what radio constraints they have to obey to (e.g., maximum transmission power).
- **IEEE802.11.f** is defining a standard inter access point communication protocol for users roaming between access points (irrelevant to ad hoc networks).
- **IEEE802.11.i** addresses the flaws of WEP, improving the wireless security at the MAC layer.

ETSI HiperLAN

HiperLAN

- European effort for WLAN standardization (superior to 802.11)
- European Telecommunications Standards Institute (ETSI) – Broadband Radio Access Networks (BRAN).
- HiperLAN is defined to work in the 5.2GHz U-NII.
- TDMA based access method.
- No commercial products.

HiperLAN/2

- New version of HiperLAN.
- Superior to any of the 802.11 versions.
- PHY is the same as that of 802.11h (similar to 802.11a).
- MAC layer is based on TDMA and is said to be Wireless-ATM-like.
- QoS provisioning.
- Infrastructure and ad hoc modes.
- Engineered to work with 3G and other systems.
- No products yet.