15-441/641: WiFi Networks

15-441 Fall 2019

Profs **Peter Steenkiste** & Justine Sherry

Fall 2019

https://computer-networks.github.io/fa19/

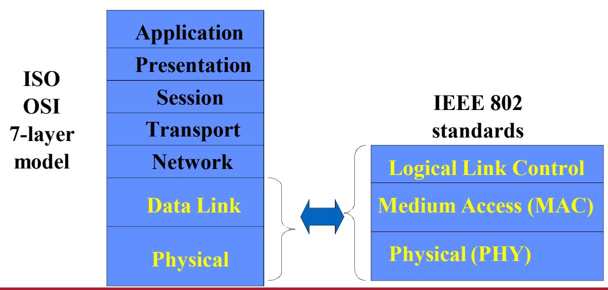
Carnegie Mellon University

Overview

- Basic WiFi concepts
- Some deployment issues
- WiFi versions

Standardization Local Area Networks

- Wireless networks are standardized by IEEE
- Under 802 LAN MAN standards committee



The 802 Class of Standards

- List on next two slides
- Some standards apply to all 802 technologies
  - E.g. 802.2 is LLC
  - Important for inter operability
- Some standards are for technologies that are outdated
  - Not actively deployed anymore
  - Many of the early standards are obsolete

802 Standards – Part 1

Name	Description	Note
IEEE 802.1	Higher Layer LAN Protocols (Bridging)	active
IEEE 802.2	LLC	disbanded
IEEE 802.3	Ethernet	active
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Token ring MAC layer	disbanded
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	active
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	active
IEEE 802.15.1	Bluetooth certification	active
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	active
IEEE 802.15.5	Mesh networking for WPAN	

802 Standards – Part 2

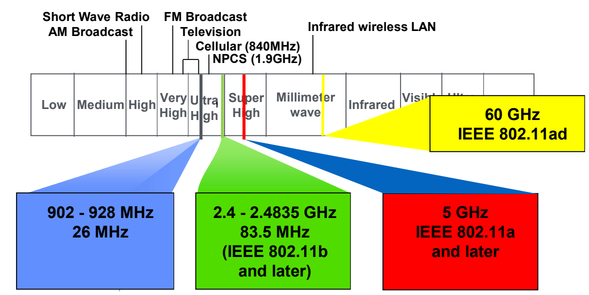
IEEE 802.15.6	Body area network	active
IEEE 802.15.7	Visible light communications	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.16.2	Coexistence wireless access	
IEEE 802.17	Resilient packet ring	hibernating
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	hibernating
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	

Some IEEE 802.11 Standards

- IEEE 802.11a
  - PHY Standard : 8 channels : up to 54 Mbps : widely deployment
- IEEE 802.11b
  - PHY Standard : 3 channels : up to 11 Mbps : widely deployed.
- IEEE 802.11d
  - MAC Standard : support for multiple regulatory domains (countries)
- IEEE 802.11e
  - MAC Standard : QoS support : supported by many vendors
- IEEE 802.11f
  - Inter-Access Point Protocol : deployed
- IEEE 802.11g
  - PHY Standard: 3 channels : OFDM and PBCC : widely deployed (as b/g)
- IEEE 802.11h
  - Suppl. MAC Standard: spectrum managed 802.11a (TPC, DFS): standard
- IEEE 802.11i
  - Suppl. MAC Standard: Alternative WEP : standard
- IEEE 802.11n
  - MAC Standard: MIMO : significant improvements in throughput
- IEEE 802.11ac
  - Support for multi-user MIMO
- IEEE 802.11ad
  - WiFi in the 60 GHz band
- IEEE 802.11ax
  - Improved version of 802.11ac
- IEEE 802.11ay
  - Improved version of 802.11ad

Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Generally called “unlicensed” bands



IEEE 802.11 Overview

- Adopted in 1997 with goal of providing
  - Giving wireless users access to services in wired networks
  - High throughput and reliability
  - Continuous network connection, e.g. while mobile
- The protocol defines
  - MAC sublayer
  - MAC management protocols and services
  - Several physical layers: IR, FHSS, DSSS, OFDM
- Wi-Fi Alliance is industry group that certifies interoperability of 802.11 products

Features of 802.11 MAC protocol

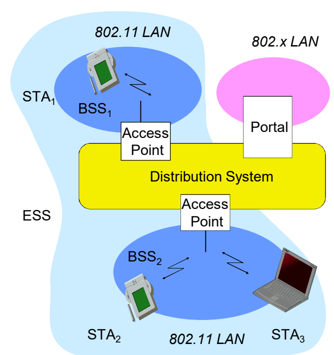
- Supports MAC functionality
  - Addressing – based on 48-bit IEEE addresses
  - CSMA/CA
- Error detection (checksum)
- Error correction (ACK frame)
- Flow control: stop-and-wait
- Fragmentation (More Frag)
- Collision Avoidance (RTS-CTS)

Infrastructure and Ad Hoc Mode

- Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure
  - What is deployed in practice
- Two modes of operation:
  - Distributed Control Functions - DCF
  - Point Control Functions – PCF
  - PCF is rarely used - inefficient
- Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure
  - Rarely used, e.g. military
  - Hot research topic!

Our Focus

802.11: Infrastructure Mode



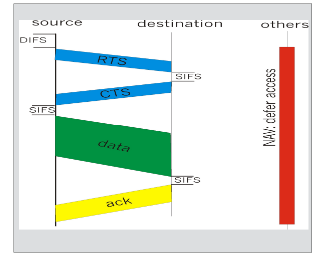
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - group of stations using the same AP
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

Wireless Collision Avoidance

- Problem: two nodes, hidden from each other, transmit complete frames to base station
- Collision detection not reliable: “listen before talking” canfail
  - Solution: rely on ACKs instead to detect packet loss
- Collisions waste bandwidth for long duration !
  - Plus also exponential back off before retransmissions – collisions are expensive!
- Solution: “CA” using small reservation packets
  - Nodes track reservation interval with internal “network allocation vector” (NAV)
  - This is called “virtual carrier sense”
- Note that nodes still do “physical” carrier sense
  - “Listen before you talk” often works and is cheap

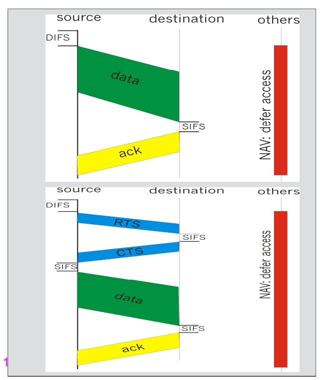
Collision Avoidance: RTS-CTS Exchange

- Explicit channel reservation
  - Sender: send short RTS: request to send
  - Receiver: reply with short CTS: clear to send
  - CTS reserves channel for sender, notifying (possibly hidden) stations
- RTS and CTS are short:
  - collisions are less likely, of shorter duration
  - end result is similar to collision detection
- Avoid hidden station collisions
- Not widely used (not used really)
  - Overhead is too high!
  - Not a serious problem in typical deployments

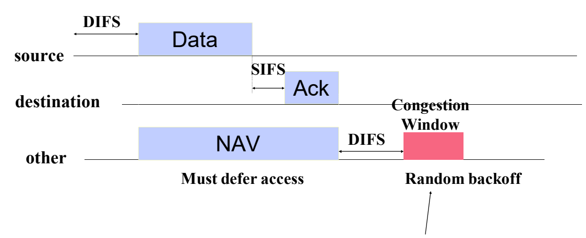


IEEE 802.11 MAC Protocol

- RTS/CTS implemented using **NAV**: Network Allocation Vector
- NAV is also used with data packets
  - 802.11 data frame has transmission time field
  - Others (hearing data header) defer access for NAV time units
- But why do you need NAV if you can hear the header?
  - Fading?
  - Header is sent at lower bit rate – more likely to be correctly received



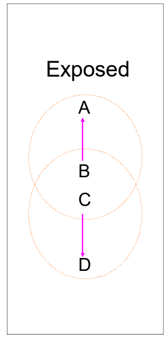
DCF mode transmission without RTS/CTS



Not used in Ethernet
WiFi is more concerned about collisions

How About Exposed Terminal?

- Exposed terminals result in a lost transmission opportunity
  - Reduces capacity – no collisions
- Exposed terminals are difficult to deal with
  - Even hard to detect them!
- Good news – they are very rare!
  - So we live with them

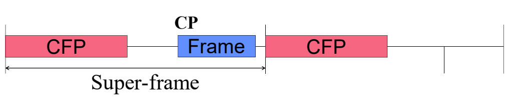


Exponential Backoff

- Force stations to wait for random amount of time to reduce the chance of collision
  - Backoff period increases exponential after each collision
  - Similar to Ethernet
- *Also used when the medium is sensed as busy*:
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Pick random number in contention window (CW) = backoff counter
  - Decrement backoff timer until it reaches 0
    - *But freeze counter whenever medium becomes busy*
  - When counter reaches 0, transmit frame
  - If two stations have their timers reach 0 at same time; collision will occur;
- After every failed retransmission attempt:
  - increase the contention window exponentially
  - $2^i - 1$ starting with CW_{min} up to CW_{max} e.g., 7, 15, 31, ...

What about PCF?

- IEEE 802.11 combines random access with a “taking turns” protocol
  - DCF (Distributed Coordination Mode) – Random access
    - CP (Contention Period): CSMA/CA is used
  - PCF (Point Coordination Mode) – Polling
    - CFP (Contention-Free Period): AP polls hosts
- Basestation can control who access to medium
  - Can offer bandwidth guarantees
- Rarely used in practice



PCF Operation Overview

- PC – Point Coordinator
  - Uses polling – eliminates contention
  - Polling list ensures access to all registered stations
  - Over DCF but uses a PIFS instead of a DIFS – gets priority
- CFP – Contention Free Period
  - Alternate with DCF
- Periodic Beacon – contains length of CFP
  - NAV prevents transmission during CFP
  - CF-End – resets NAV
- CF-Poll – Contention Free Poll by PC
  - Stations can return data and indicate whether they have more data
  - CF-ACK and CF-POLL can be piggybacked on data

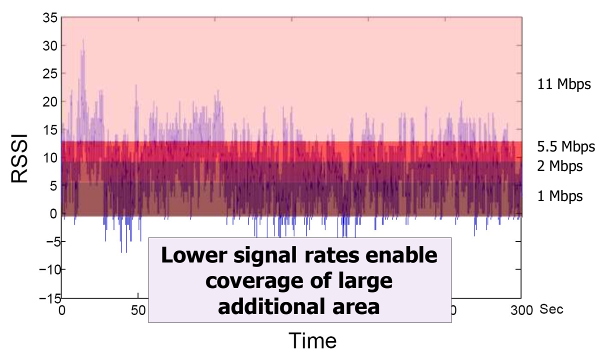
Overview

- Basic WiFi concepts
- Some deployment issues
- WiFi versions

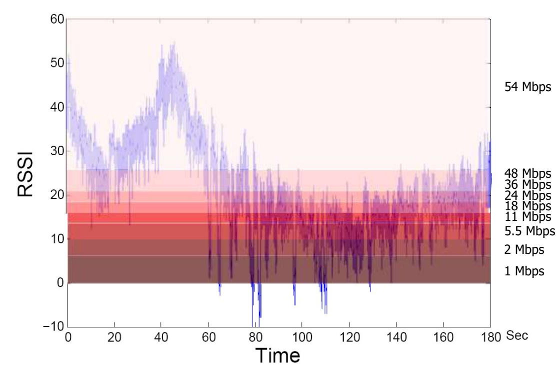
Association Management

- Stations must associate with an AP before they can use the wireless network
  - AP must know about them so it can forward packets
  - Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: discover available access points based on periodic beacons
  2. Selection: deciding what AP (or ESS) to use
  3. Association: protocol to “sign up” with AP – share configuration info
  4. Authentication: needed to gain access to secure APs – many options
- Disassociation: station or AP can terminate association

“Static” Channel – Bitrate Adaptation

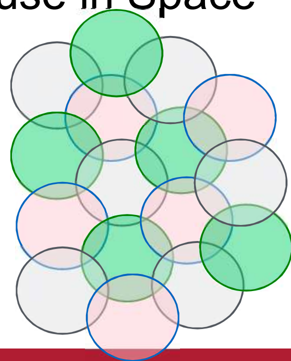


Mobile Channel – Pedestrian



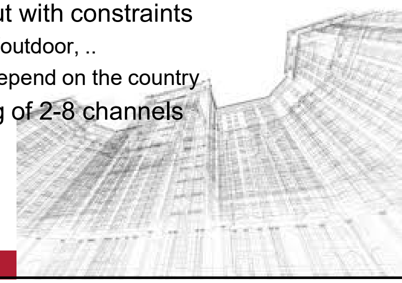
Infrastructure Deployments Frequency Reuse in Space

- Set of cooperating cells with a base stations must cover a large area
- Cells that reuse frequencies should be as distant as possible to minimize interference and maximize capacity
  - Minimizes hidden and exposed terminals
  - 3D problem!
  - Lots of measurements



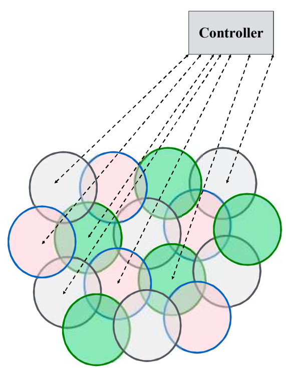
Frequencies are Precious

- 2.4 Ghz: 3 non-overlapping channels
  - Plus lots of competition: microwaves and other devices
- 5 GHz: 20+ channels, but with constraints
  - Power constraints, indoor/outdoor, ..
  - Exact number and rules depend on the country
- 802.11n and ac: bonding of 2-8 channels
- And the world is not flat!



Centralized Control

- Many WiFi deployments have centralized control
- APs report measurements
  - Signal strengths, interference from other cells, load, …
- Controller makes adjustments
  - Changes frequency bands
  - Adjusts power
  - Redistributes load
  - Can switch APs on/off
  - Very sophisticated!



Overview

- Basic WiFi concepts
- Some deployment issues
- WiFi versions
  - Very high level

IEEE 802.11 Family

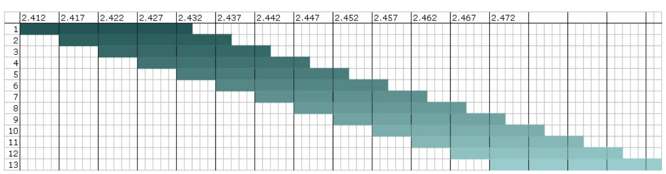
Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz 20/40 MHz	200 Mbps	600 Mbps	~50 m
802.11ac	2013	5 GHz 20→160 MHz	100s Mbps per user	1.3 Gbps	~50 m
802.11ad	2016	60 GHz	Gbps	7 Gbps	Short - room

A Factor of 1000+ Speedup?

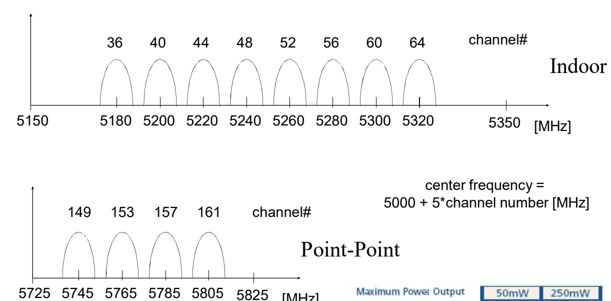
- 802.11b: first WiFi to be standardized and widely deployed
  - Used 20MHz channels, 2.4 GHz only, inefficient modulation
- 802.11a and g: increases rates from 11 to 54Mbit/sec
  - Key factor is better modulation ("OFDM")
  - They are the same standard, but 802.11a runs in 5GHz band
    - 5GHz band is wider and has lower utilization – more capacity!
- 802.11n: runs in both 5 and 2.4GHz bands – significant speed up
  - How? Better modulation, channel bonding, and MIMO

802.11b Channels

- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22MHz
- Significant overlap
- Non-overlapping channels are 1, 6 and 11
- 1, 2, 5.5 and 11 Mbps rates using DSSS technology



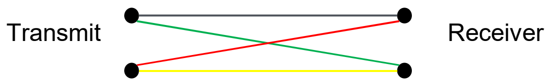
802.11a Physical Channels*



* *example; not all channels are shown*

Aside: Why Multiple Antennas?

- Access points almost always have multiple antennas
  - The number has increased with successive generations
  - Some devices also have multiple antennas (e.g., 2-3)
- Original motivation: spatial diversity

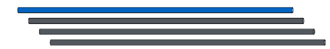


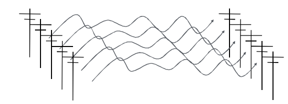
- Quality of the links can be very different and what link is best
  - Transmitter picks the antennas with the best channel to receiver
  - Receiver picks the best signal it receives, or it combines them

How do we Go Faster?

- Wired world:

Pull more wires!



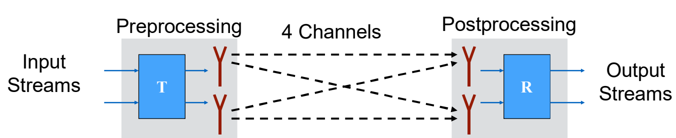


- Wireless world:

How about if we could do the same thing and simply use more antennas?

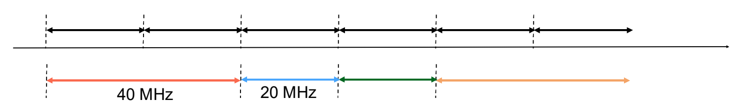
MIMO: Multiple In – Multiple Out

- Key idea: use multiple antenna pairs to send parallel data streams
  - Should give us linear capacity increase (just like the wired world)
- Problem: the different transmissions interfere!
  - Each receiving antenna receives (weighted) sum of all transmissions
  - Could be viewed as noise – low S/N ration in Shannon
- Solution: interference is not random but can be subtracted



Channel Bonding

- Why only use 20Mhz channels per user?
  - Remember Shannon?



- What changes are needed?
  - Radios need to use a wider channel: adds complexity, cost
  - Interoperability between 20 and 40 MHz devices – messy
- Mostly useful in 5 GHz band – more spectrum

How Do We Go Even Faster?

- 802.11ac: faster, mostly by more aggressive modulation and MIMO
  - Also uses multi-user MIMO: AP can send packets to multiple stations simultaneously (don't worry about the details)
- 802.11ad: first WiFi to use the 60 GHz band
  - \+ Lots of bandwidth available, mostly unused
  - – Transmission only over short distances
  - – Signal does not penetrate objects, i.e., mostly LOS
  - In practice, need to use beam forming
  - While standardized, lots of open questions remain

802.11ad – Beamforming

- 802.11ad does very aggressive beam forming
- Some background:
  - Antenna arrays can be used to concentrate transmit power into beams to specific receivers
  - Higher frequencies -> smaller antennas and narrower beams
  - Also: larger arrays -> fine grain control over narrow beams
  - Extends range and increases throughput
- How do we find the right beams?
  - Iterative search process