18-452/18-750
Wireless Networks and Applications
Lecture 13: Wireless LAN
802.11 Standards

Peter Steenkiste

Fall Semester 2018

http://www.cs.cmu.edu/~prs/wirelessF18/

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

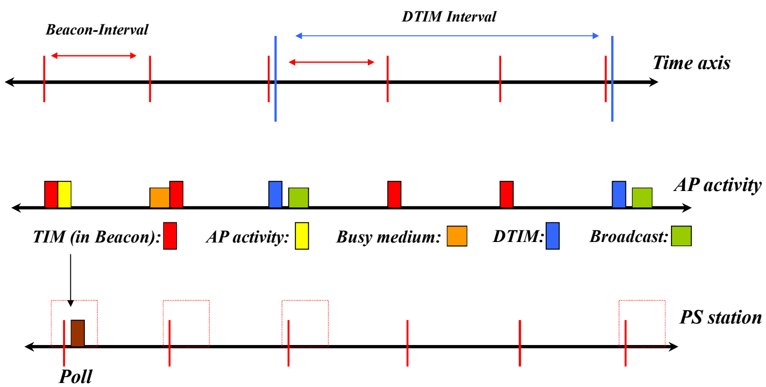
Power Management

- Goal is to enhance battery life of the stations
- Idle receive state dominates LAN adapter power consumption over time
- Allow stations to power off their NIC while still maintaining an active session
- Different protocols are used for infrastructure and independent BSS
  - » Our focus is on infrastructure mode

Power Management Approach

- Idle station to go to sleep
- AP keeps track of stations in Power Savings mode and buffers their packets
  - » Traffic Indication Map (TIM) is included in beacons to inform which power-save stations have packets waiting at the AP
- Power Saving stations wake up periodically and listen for beacons
  - » If they have data waiting, they can send a PS-Poll to request that the AP sends their packets
- TSF assures AP and stations are synchronized
  - » Synchronizes clocks of the nodes in the BSS
- Broadcast/multicast frames are also buffered at AP
  - » Sent after beacons that includes Delivery Traffic Indication Map (DTIM)
  - » AP controls DTIM interval

Infrastructure Power Management Operation



Peter A. Steenkiste, CMU

Some IEEE 802.11 Standards

- IEEE 802.11a
  - PHY Standard : 8 channels : up to 54 Mbps : some 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 : standardization expected late 2008

Peter A. Steenkiste, CMU

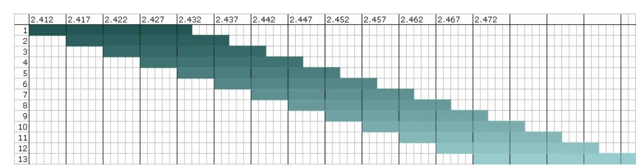
IEEE 802.11 Family

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	200 Mbps	600 Mbps	~50 m

Peter A. Steenkiste, CMU

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

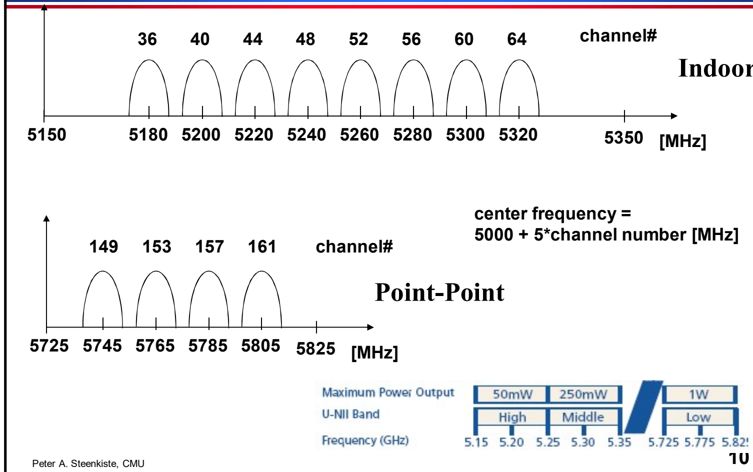


Peter A. Steenkiste, CMU

802.11b Physical Layer

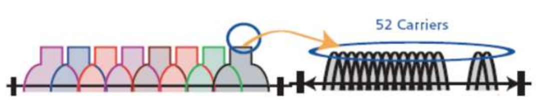
- FHSS (legacy)
  - » 2 & 4 GFSK
  - » Using one of 78 hop sequences, hop to a new 1MHz channel (out of the total of 79 channels) at least every 400milliseconds
- DSSS (802.11b)
  - » DBPSK & DQPSK
  - » Uses one of 11 overlapping channels (22 MHz)
  - » 1 and 2 Mbps: multiply the data by an 11-chip spreading code (Barker sequence)
  - » 5.5 and 11 Mbps: uses Complementary Code Keying (CKK) to generate spreading sequences that support the higher data rates
    - – Spreading code is calculated based on the data bits

802.11a Physical Channels



802.11a Modulation

- Use OFDM to divide each physical channel (20 MHz) into 52 subcarriers (20M/64=312.5 KHz each)
  - » 48 data, 4 pilot



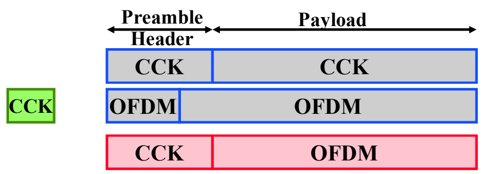
- Adaptive modulation
  - » BPSK: 6, 9 Mbps
  - » QPSK: 12, 18 Mbps
  - » 16-QAM: 24, 36 Mbps
  - » 64-QAM: 48, 54 Mbps

802.11a Discussion

- Uses OFDM in the 5 GHz band
  - » Also used by 802.11g in 2.4 GHz (next slides)
- What are the benefits of 802.11a compared with 802.11b/g?
  - » Greater bandwidth (up to 54Mb)
    - – 54, 48, 36, 24, 18, 12, 9 and 6 Mbs
    - – 802.11g (next slide) offers same benefit
  - » Less potential interference (5GHz)
  - » More non-overlapping channels
- But it does not provide interoperability with 802.11b, as 802.11g does
  - » Cannot fall back to lower rates (not an issue in practice)
  - » Cards typically support a and g

Interoperability 802.11b and 802.11g

- 802.11g is the same as 802.11a, but in 2.4GHz band
  - » Falls back to 802.11b for the lower rates (1,2, 5.5, 11 MHz)
  - » Uses 802.11a OFDM technology for new rates (6 Mbs and up)
- Creates an interoperability problem since 802.11b cards cannot interpret OFDM signals
  - » Interoperability mode: protection mechanism in hybrid environment: Send CCK CTS before OFDM packets or use(optional) hybrid packet
  - » Can also run an 802.11n only network – reduces overhead



Spectrum and Transmit Power Management Extensions (802.11h)

- Support 802.11 operation in 5 GHz band in Europe: coexistence with primary users
  - » Radar: cannot use bands if a radar is nearby
    - – Allows opening up 11 more bands in 5 GHz band
  - » Satellite: limit power to 3dB below regulatory limit
- Dynamic Frequency Selection (DFS)
  - » Detect primary users and adapt
  - » AP notifies stations to switch channel at some point in time
- Transmit Power Control (TPC)
  - » Goal is to limit interference – also controlled by AP
- DFS and TPC have broader uses such as range and interference control, reduced energy consumption, automatic frequency planning, load balancing, ..

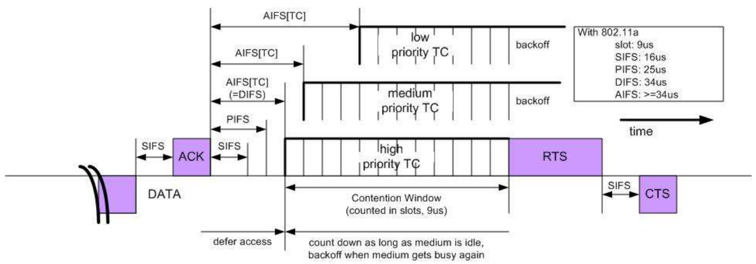
IEEE 802.11e

- Original intent was that 802.11 PCF could be used to provide QoS guarantees
  - » Scheduler in the PCF priorities urgent traffic
  - » But: overhead, “guarantees” are very soft
- 802.11e Enhanced Distributed Coordination Function (EDCF) is supposed to fix this.
  - » Provides Hybrid Coordination Function (HCF) that combines aspects of PCF and DCF
- EDCF supports 4 Access Categories
  - » *AC_BK (or AC0)* for Back-ground traffic
  - » *AC_BE (or AC1)* for Best-Effort traffic
  - » *AC_VI (or AC2)* for Video traffic
  - » *AC_VO (or AC3)* for Voice traffic

Service Differentiation Mechanisms in EDCF

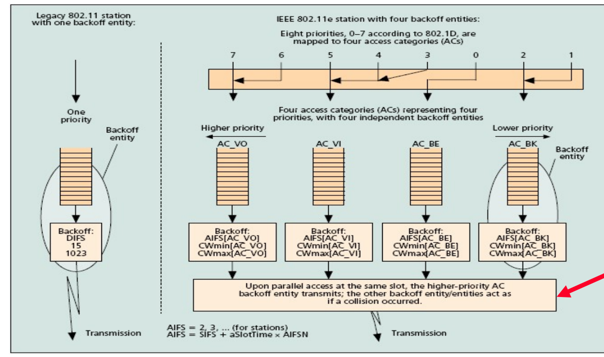
- The two types of service differentiation mechanisms proposed in EDCF are:
- *Arbitrate Inter-frame Space (AIFS) Differentiation*
  - Different AIFSs instead of the constant distributed IFS (DIFS) used in DCF.
  - Back-off counter is selected from [1, CW[AC]+1] instead of [0,CW] as in DCF.
- Contention Window (CWmin) Differentiation
  - Different values for the minimum/maximum CWs to be used for the back-off time extraction.

IEEE 802.11e: Priorities



Mapping different priority frames to different AC

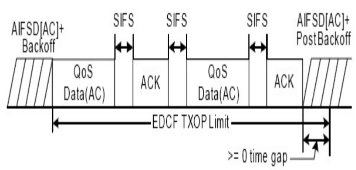
- Each frame arriving at the MAC with a priority is mapped into an AC as shown in figure below.



Resolves Virtual Collisions

Other 802.11 MAC Improvements

- *TXOP- **Transmission opportunity*** (TXOP) is an interval of time during which a back-off entity has the right to deliver multiple MSDUs.
  - » A TXOP is defined by its starting time and duration
  - » Announced using a traffic specification (length, period)
  - » Can give more transmission opportunities to a station
  - » Can also limit transmission time (e.g. for low rate stations)
- *CFB-* In a single TXOP, multiple MSDUs can be transmitted.
  - » *"Contention Free Burst" (CFB)*
  - » *Can use a block acknowledgement*



802.11p: Vehicular Networking

- Basis for Dedicated Short Range Communication (DSRC)
  - » Connecting vehicles and road side units
  - » Dedicated band at 5.9 GHz
  - » Higher layers of protocol stack defined by WAVE
  - » Primary driver is vehicular safety such as reporting accidents, ..
- Differences with 802.11a
  - » Channels are 10 MHz wide; this means that symbol times are twice as long (more robust to ISI)
  - » Communication is between stations that are not associated or authenticated (no BSS ID)

OFDM Q & A

How Do We Increase Rates?

- Two challenges related to multipath:
- Frequency selective fading starts to have a bigger impact because there is less redundancy in the signal
  - » This is major issue for wide-band channels only
- As rates increase, symbol times shrink and the effects of inter-symbol interference becomes more pronounced
  - » There is a limit on how much we can shrink symbol times
- We need an encoding/modulation solution that has long symbol times and limits the impact of frequency selective fading

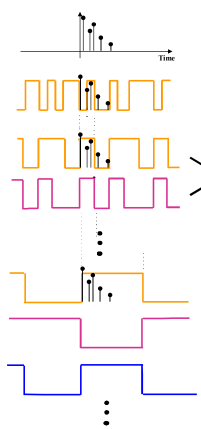
Distributing Bits over Subcarriers

Channel impulse response

Single Carrier

2 Carriers

8 Carriers



Channels are transmitted at different frequencies (sub-carriers)

Resistance to ISI improves with number of channels

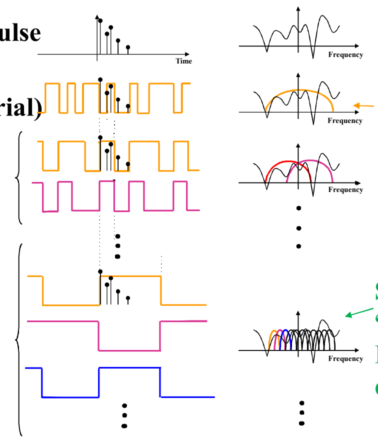
Benefits of Narrow Band Channels

Channel impulse response

1 Carrier (serial)

2 Carriers

8 Carriers

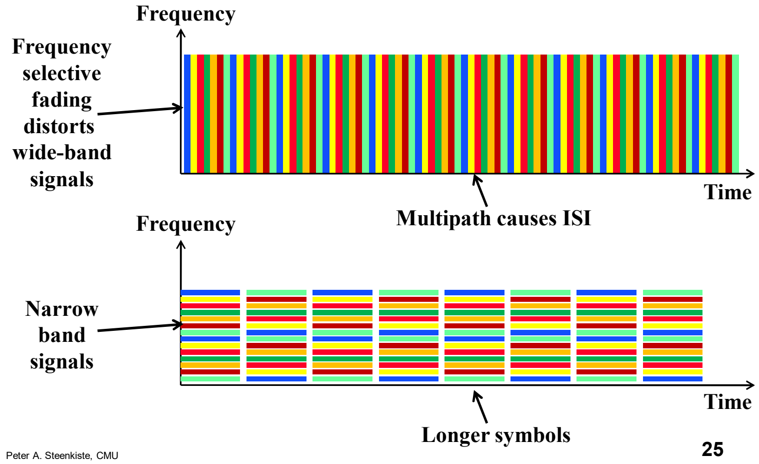


Channel transfer functi

Signal is "broadband": Frequency selective fading

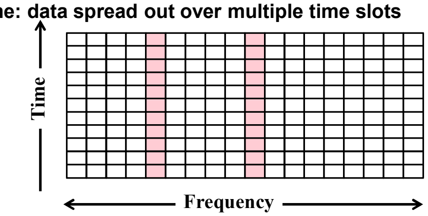
Sub-carriers ar "narrowband": Flat fading in each sub-carrie

OFDM Transmission



Use of Redundancy in OFDM

- OFDM uses error coding as described earlier
  - » Degree of error coding depends on channel conditions
- OFDM offers frequency and diversity
  - » Frequency: data is spread out over multiple subcarriers
  - » Time: data spread out over multiple time slots



- Combining OFDM with MIMO adds space diversity (discussed later in course)