18-452/18-750
Wireless Networks and Applications
Lecture 11: WiFi
Management and Deployments

Peter Steenkiste

Spring Semester 2024

http://www.cs.cmu.edu/~prs/wirelessS24/

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 power control and other features
- 802.11 management
- 802.11 security
- 802.11 deployments
- 802.11 versions

Early 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, ac, ad, ay, ay

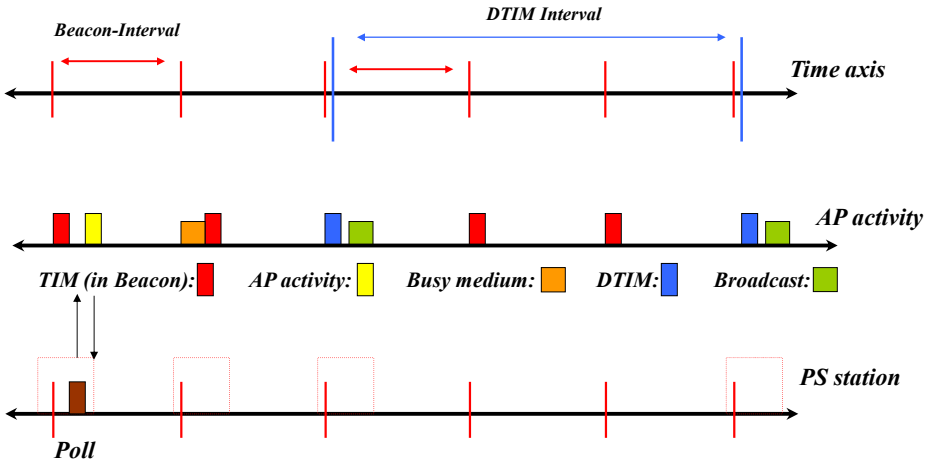
Power Management

- 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

- Allow idle station to put radio in a low power mode
- AP keeps track of stations in Power Savings (PS) 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
- PS 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
  - » Poll is needed since stations can skip beacons with a TIM
- TSF assures AP and stations are synchronized
  - » Time Synchronization Function: Synchronizes clocks in a BSS
- Broadcast/multicast frames are also buffered at AP
  - » Sent after beacon with a Delivery Traffic Indication Map (DTIM)
  - » Stations must wake up for beacons with a DTIM
  - » AP controls DTIM interval

Infrastructure Power Management Operation



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, ..

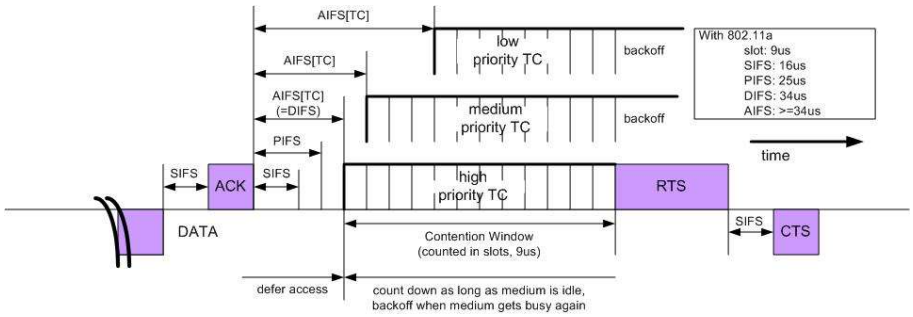
IEEE 802.11e

- 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

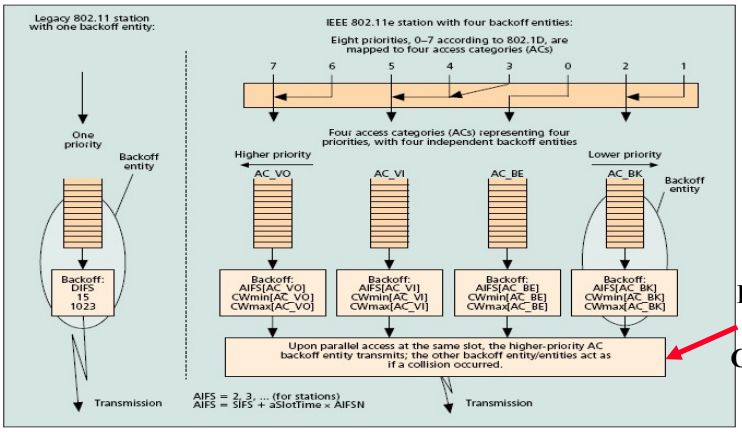
- The two types of service differentiation mechanisms proposed in EDCF are:
- *Arbitrate Inter-frame Space (AIFS) Differentiation*
  - Different AIFSs instead of the constant distributed IFS (DIFS) used in DCF.
  - Back-off counter is selected from [1, CW[AC]+1] instead of [0,CW] as in DCF.
- Contention 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

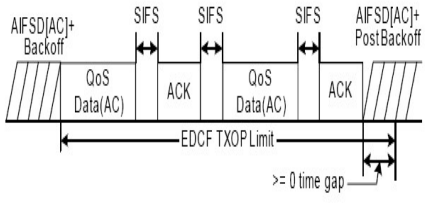
- Each frame arriving at the MAC with a priority is mapped into an AC as shown in figure below.



Resolves Virtual Collisions

Other 802.11 MAC Improvements

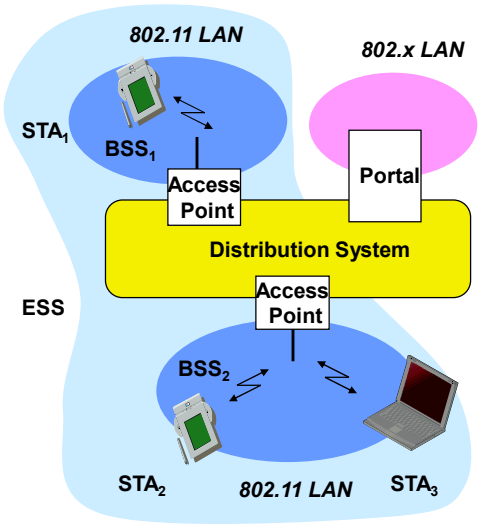
- *TXOP*- ***Transmission opportunity*** **(TXOP) is an interval of time during which a back-off entity has the right to deliver multiple MSDUs.**
  - » **A TXOP is defined by its starting time and duration**
  - » **Announced using a traffic specification (length, period)**
  - » **Can give more transmission 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 also use a block acknowledgement – reduces overhead***



Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 power control and other features
- 802.11 management
- 802.11 security
- 802.11 deployments
- 802.11 versions

802.11: Infrastructure Reminder



- 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

Service Set Identifier - SSID

- Mechanism used to segment wireless networks
  - » Multiple independent wireless networks can coexist in the same location
- Each independent WiFi network has a user-readable name – "SSID"
  - » It is advertised by the APs so users can pick correct network
- A network can have one or more APs
  - » Home network: SSID corresponds to one AP
  - » Campus networks: SSID corresponds to multiple APs
- Security considerations
  - » AP are typically configured to "broadcast" its SSID
    - – Broadcasting can be disabled to improve security
  - » Network can use misleading SSID

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
  - » Devices often also have to authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: finding out what access points are available
  2. Selection: user decides what SSID to use
  3. Association: devices picks best "AP" and "signs up" with the AP – this involves an exchange of parameters
  4. Authentication: needed to gain access to secure APs – many options possible
- Disassociation: station or AP can terminate association

Association Management: Scanning

- Stations can detect AP using scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
  - » Beacons are sent roughly 10 times per second
  - » Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
  - » Saves time + is more thorough
  - » Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
  - » Especially with passive scanning
  - » Cannot transmit and receive frames during most of that time – not a big problem during initial association

Association Management: Selecting an AP and Joining

- Selecting a network (SSID) typically involves the user
  - » What networks do you trust? Are you willing to pay?
  - » Can be done automatically based on stated user preferences (e.g., the "automatic" list in Windows)
- The wireless host selects an AP in the network based on vendor-specific algorithm
  - » Uses the information from the scan
  - » Typically simply joins the AP with the strongest signal
- Associating with an AP
  - » Synchronization in Timestamp Field and frequency
  - » Adopt PHY parameters
  - » Other parameters: BSSID, WEP, Beacon Period, etc.

What about Mobile Users?

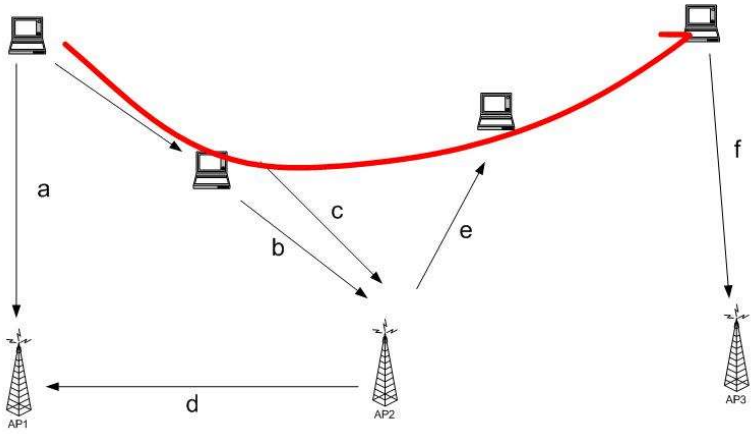
- Example: WiFi VoIP call while walking
  - » Device needs to swich between APs
  - » Challenging: picking AP, associating, security, …
  - » Goals: minimize how long the device is disconnected and avoid packet loss
- Moving around in campus network: devices needs two switch between APs that are part of the same wireless network
  - » Supported by standards – next slide
- Moving in area with many single AP networks
  - » Very challenging! Handover will be time consuming

Association Management: Reassociation Algorithms

- Failure driven: only try to reassociate after connection to current AP is lost
  - » Typically efficient for stationary clients since it not common that the best AP changes during a session
  - » Mostly useful for nomadic clients
  - » Can be very disruptive for mobile devices
- Proactive reassociation: periodically try to find an AP with a stronger signal
  - » Tricky part: cannot communicate while scanning other channels
  - » Trick: user power save mode to “hold” messages
  - » Throughput during scanning is still affected though
    - – Mostly affects latency sensitive applications

Association Management: Roaming inside a Wireless Network

- **Reassociation: association is transferred from active AP to a new target AP**
  - **Supports mobility in the same ESS – layer 2 roaming**
- **Reassociation is initiated by the wireless host based on vendor specific algorithms**
  - **Implemented using an Association Request Frame that is sent to the new AP**
  - **New AP accepts or rejects the request using an Association Response Frame**
- **Coordination between APs is defined in 802.11f**
  - **Allows forwarding of frames in multi-vendor networks**
  - **Inter-AP authentication and discovery typically coordinated using a RADIUS server**
  - **"Fast roaming" support (802.11r) also streamlines authentication and QoS, e.g. for VoIP**



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 power control and other features
- 802.11 management
- 802.11 security
- 802.11 deployments
- 802.11 versions

WLAN Security Requirements

- Confidentiality: hide the contents of traffic from unauthorized parties
  - » Important for wireless links!
- Authentication: only allow authorized stations to associate with and use the AP
- Integrity: make sure traffic contents is not modified while in transit

WLAN Security Exploits

- Insertion attacks: unauthorized Clients or AP
  - » Client: reuse MAC or IP address –free service on "secured" APs
  - » AP: impersonate an AP, e.g., use well known name
- Interception and unauthorized monitoring
  - » Packet Analysis by "sniffing" – listening to all traffic
- Brute Force Attacks Against AP Passwords
  - » Dictionary Attacks Against SSID
- Encryption Attacks
  - » Exploit known weaknesses of WEP
- Misconfigurations, e.g., use default password
- Jamming – denial of service
  - » Cordless phones, baby monitors, leaky microwave oven, etc.

Security in WiFi

- Focus is on authentication, confidentiality, and integrity
- Encryption is very widely used today
  - » Pretty much pervasive
  - » Encryption at the datalink layer only provides privacy on the Wifi link only – not end-to-end!
  - » Integrity is typically provided by the same protocol
- Authentication is more complicated and three classes of solutions are used:
  - » MAC based pre-access control based on IEEE address
  - » Authentication using pre-shared keys
  - » Authentication based on an authentication server

Confidentiality in 802.11

- WEP: Wired Equivalent Privacy
  - » Achieve privacy similar to that on LAN through encryption
  - » Provides privacy using the RC4 stream cypher
  - » Provides integrity using a CRC32
  - » Had known vulnerabilities was replaced very quickly
- WPA: Wi-Fi Protected Access
  - » Larger, dynamically changed keys
- 802.11i (WPA2)
  - » Builds on WPA but fixes various vulnerability
  - » Uses Advanced Encryption Standard (AES) for encryption
  - » Authentication has two options: pre-shared keys (PSK) and Enterprise
- WPA3: similar to WPA2 but with stronger crypto algorithms (2018)

Primitive Access Control - MAC Filtering

- Each client is identified by its IEEE MAC address
- The AP has a list of MAC addresses that are allowed to use the network ("white list")
  - » Alternatively, it can have a "black list"
- Combine this filtering with the AP's SSID
  - » Only traffic associated with the AP is forwarded
- Very simple solution
  - » Minimal overhead to maintain list of MAC addresses
- But it is possible to forge MAC addresses …
  - » Unauthorized client can "borrow" the MAC address of an authenticated client
- Not a particularly secure solution

Authentication in WLAN based on 802.1x

- IEEE 802.1x supports authenticated and encrypted access to IEEE 802 networks
  - » Supports secure exchange of cryptographic keys
- Involves a client device, an authentication server, and a network device that filters out unauthenticated traffic
- Based on the Extensible Authentication Protocol (EAP - RFC3748)
  - » Supports a variety of authentication protocols

Wi-Fi Protected Access WPA

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
  - » Uses a different Message Integrity Check
  - » Encryption still based on RC4, but uses larger keys that change periodically
  - » Also frame counter in MIC to prevent replay attacks.
- Uses the 802.1x protocol for establishing session
- 802.11i is a "permanent" security fix (WPA2)
  - » Builds on the interim WPA protocol
  - » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
  - » Better key management and data integrity
- Two versions:
  - » WPA2-PSK uses pre-shared keys
  - » WPA2-professional uses an authentication server

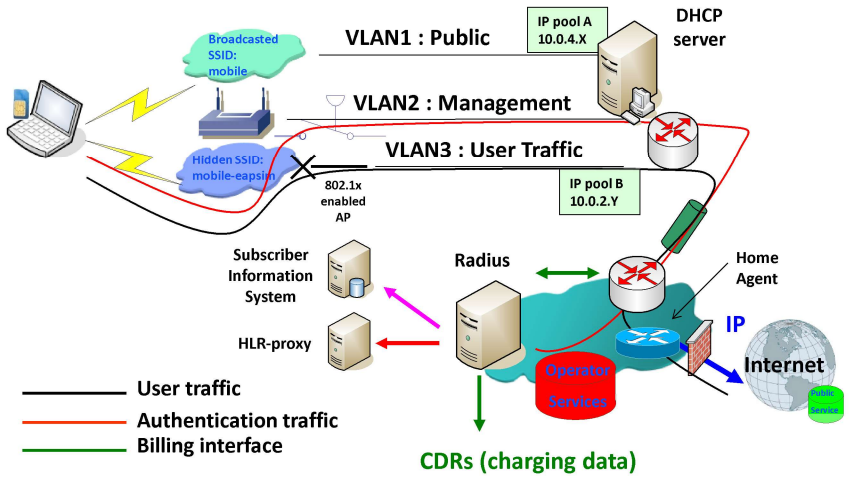
Access Control using Pre-Shared Keys

- The client device and AP share a key that is used to bootstrap security
- The AP has the key which can be distributed to authorized users who enter it on their device
  - » E.g., it is on a label on the AP, printed in a menu, ..
- AP can only verify that the user is authorized – it does not authenticate users
- Widely used in residential WiFi deployments and hot spots
- Easy to implement and intuitive for users!
- But is it is not secure in large deployments
  - » It is very likely that the key will be leaked

Using an Authentication Server

- Large deployments use an authentication server
  - » RADIUS: Remote Authentication Dial-in User Server
  - » Knows and can verify the identity of all authorized users
  - » E.g., based on password, two factor authentication, ..
  - » Also supports authorization: what services can the user access on the network
- Example: a corporation can offer different access privileges for employees and guests
  - » Example: the user of CMU secure versus CMU guest
- Question: how does a device communicate with the RADIUS server without network access?

Dual SSID Approach

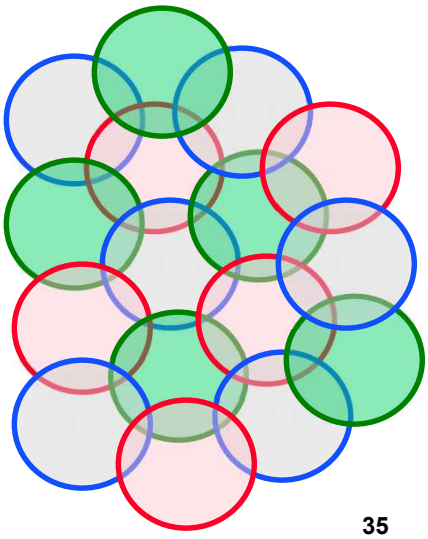


Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 power control and other features
- 802.11 management
- 802.11 security
- 802.11 deployments
- 802.11 versions

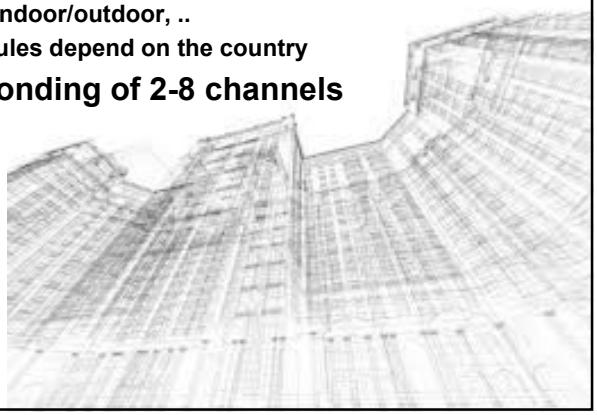
Infrastructure Deployments: Frequency Reuse in Space

- Set of cooperating cells with base stations that cover a large area
  - » E.g., campus network
- This is typically a managed deployment
  - » Professional staff
- Cells that reuse frequencies should be as distant as possible to minimize interference and maximize capacity
  - » Hidden and exposed terminals are also a concern



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!

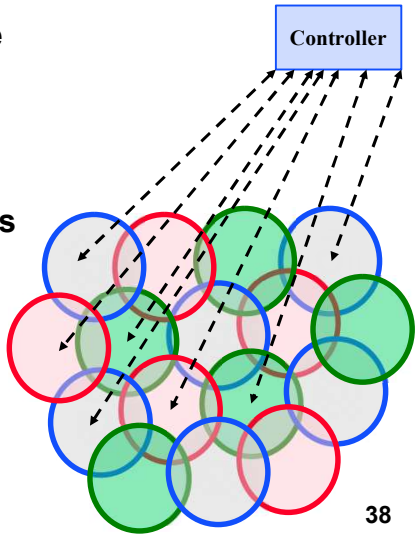


Frequency Planning

- Campus-style WiFi deployments are very carefully planned:
- A lot of measurements to determine where to place the AP
  - » What is the coverage area?
  - » What set of APs has good coverage with few "dead spots"
  - » What level of interference can we expect between cells
  - » What traffic loads can we expect, e.g., auditorium vs office
- Frequencies are carefully assigned
  - » Can use the above measurements
- Must periodically re-evaluate infrastructure
  - » Furniture is moved, remodeling, …

Centralized Control

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



Monitoring the Spectrum

- FCC (in the US) controls spectrum use
  - » Rules for unlicensed spectrum, licenses for other spectrum, what technologies can be used, …
- … but there is an special clause for campuses
  - » They have significant control over unlicensed spectrum use on the campus
  - » They can even use some "licensed" spectrum if it does not interfere with the license holder
- Network management involves carefully monitoring for performance and security
  - » Shut down rogue APs – interference, security
  - » Non-approved equipment - interference
  - » Discourages outdated standards - inefficient

How about Small Networks?

- Most WiFi networks are small and (largely) unmanaged
  - » Home networks, hotspots, …
- Traditional solution: user-chosen frequency of their AP or use a factory set default
  - » How well does that work?
- Today, APs pick a channel automatically the best channel
  - » This is done by measuring the ``channel busy time'' on all channels
  - » Can also consider signal strength from nearby APs/clients
  - » Can periodically check for better channels