

---

# **251-0292: A Hand-on Introduction to Wireless Networks**

## **Lectures 6 and 7: Protocols**

**Peter Steenkiste**

**Thomas Gross**

**Computer Science Department**

**ETH Zürich**

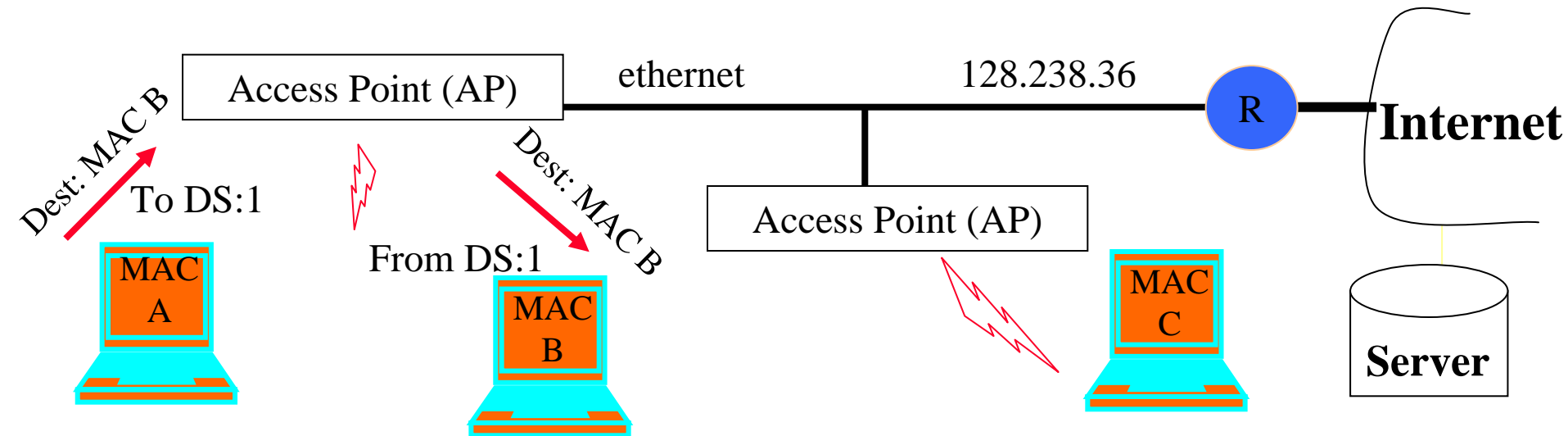
**Spring Semester 2007**

# Data Flow Examples

---

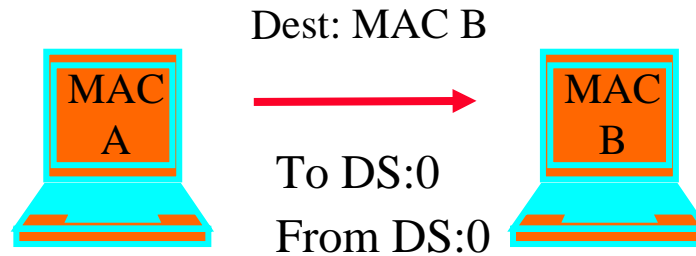
- **Case 1: Packet from a station under one AP to another in same AP's coverage area**
- **Case 2: Packet between stations in an IBSS**
- **Case 3: Packet from an 802.11 station to a wired server on the Internet**
- **Case 4: Packet from an Internet server to an 802.11 station**

# Case 1: Communication Inside BSSS



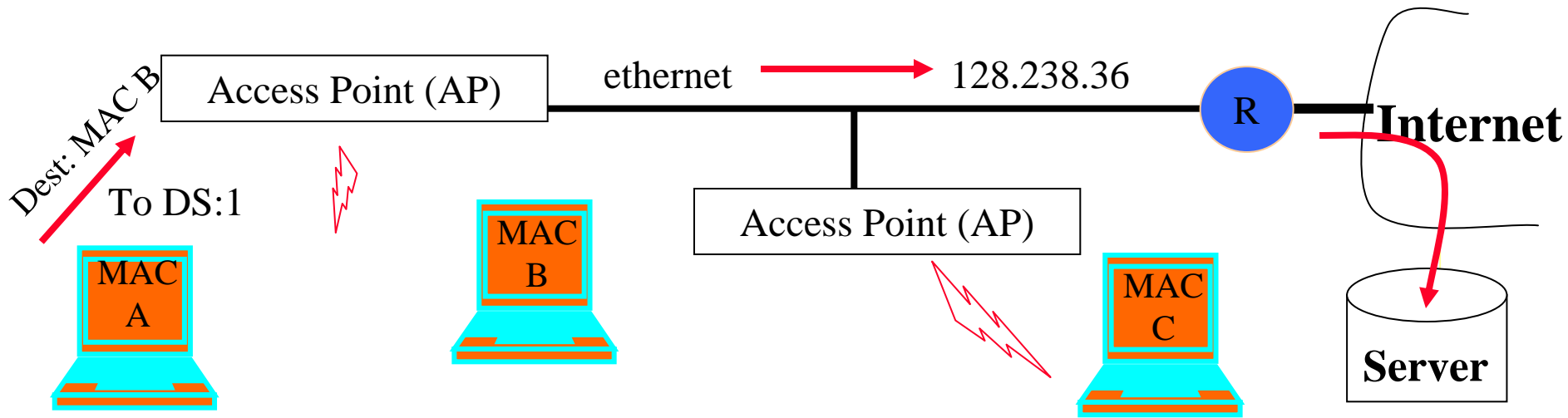
- **AP knows which stations are registered with it so it knows when it can send frame directly to the destination**

# Case 2: Ad Hoc



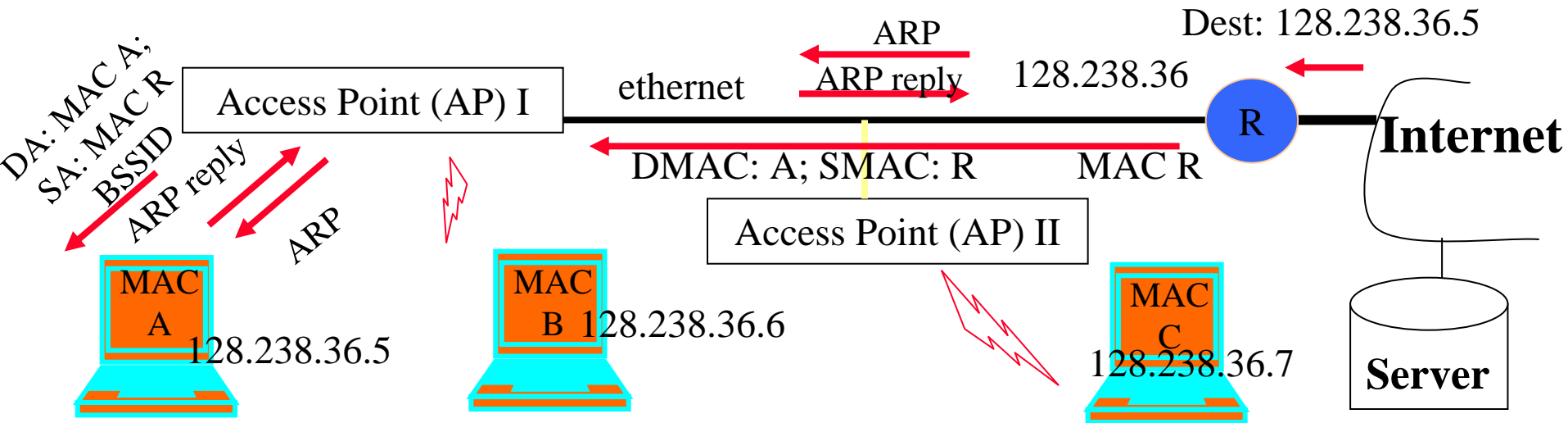
- **Direct transmit only in IBSS (Independent BSS), i.e., without AP**
- **Note: in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B**

# Case 3: To the Internet



- **MAC A determines IP address of the server (using DNS)**
- **From the IP address, it determines that server is in a different subnet**
- **Hence it sets MAC R as DA;**
  - » Address 1: BSSID, Address 2: MAC A; Address 3: DA
- **AP will look at the DA address and send it on the ethernet**
  - » AP is an 802.11 to ethernet bridge
- **Router R will relay it to server**

# Case 4: From Internet to Station



- **Packet arrives at router R – uses ARP to resolve destination IP address**
  - » AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link
  - » DA = all ones – broadcast address on the ARP
- **MAC A host replies with its MAC address (ARP reply)**
  - » AP passes on reply to router
- **Router sends data packet, which the AP simply forwards because it knows that MAC A is registered**
- **Will AP II broadcast the ARP request on the wireless medium? How about the data packet?**

# Outline

---

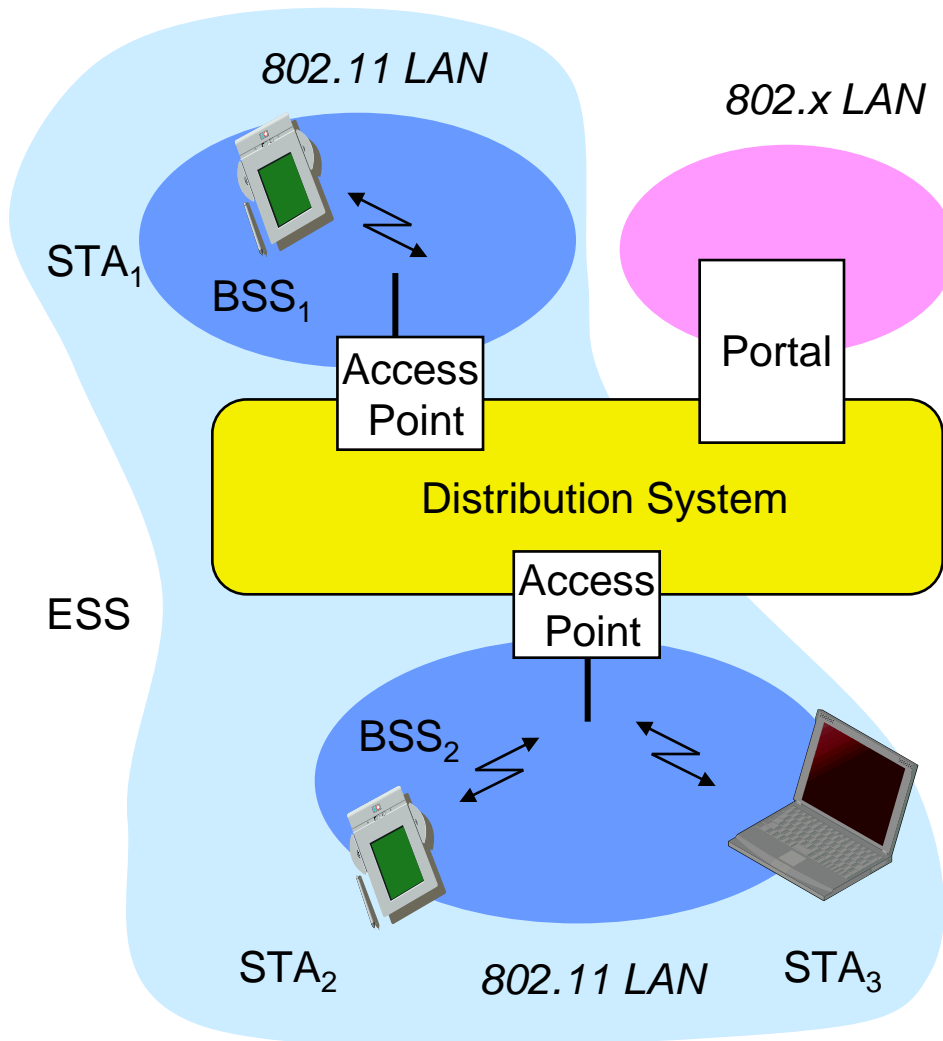
- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
  - » Overview of 802.11
  - » 802.11 MAC, frame format, operations
  - » 802.11 management
  - » 802.11\*
  - » Deployment example
- **Wireless Access – 802.16**
- **Personal Area Networks – 802.15**
- **Special topics**

# Management and Control Services

---

- **Association management**
- **Handoff**
- **Power management**
- **Security: authentication and privacy**

# 802.11: Infrastructure Reminder



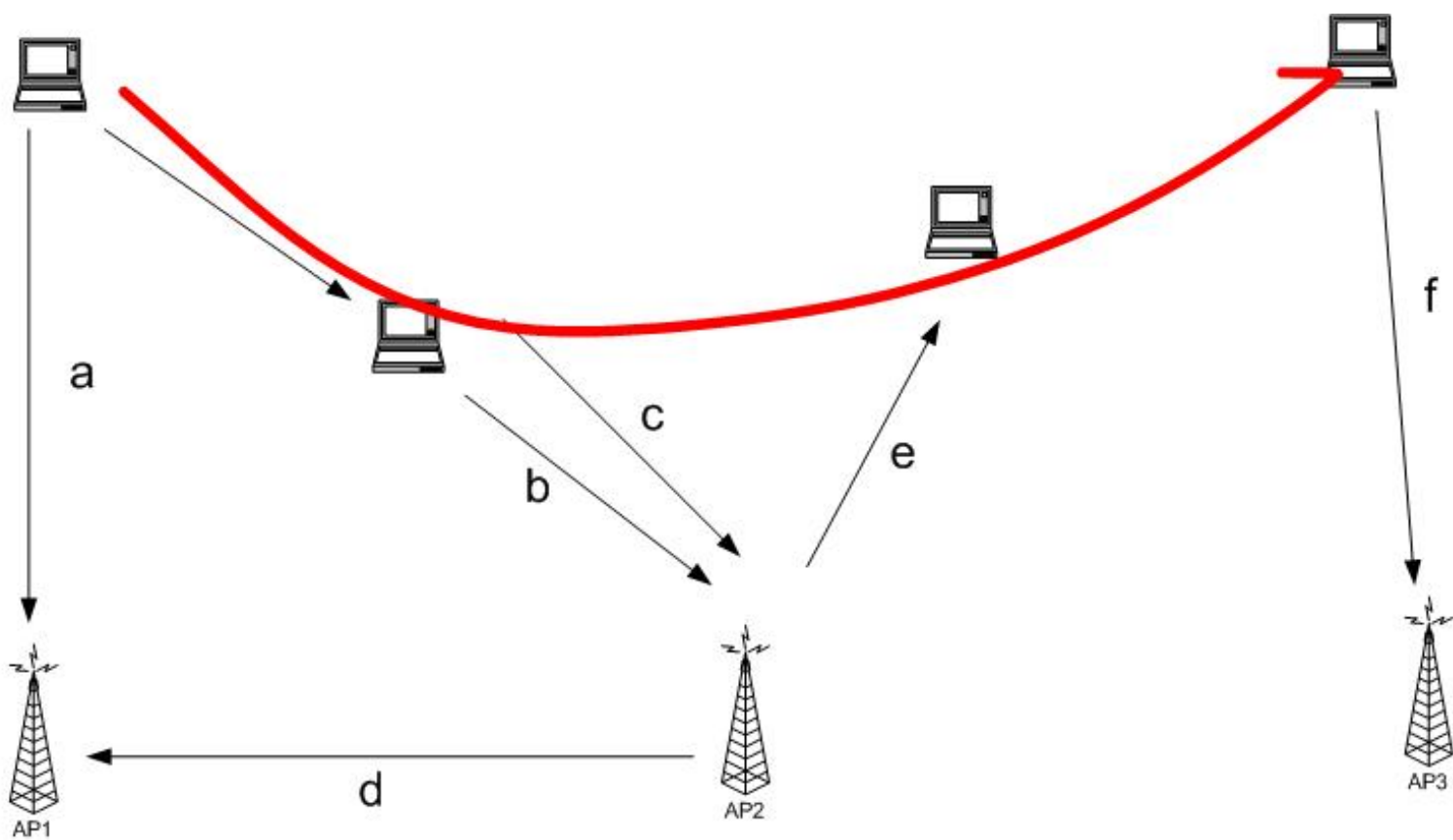
- **Station (STA)**
  - » terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Access Point**
  - » station integrated into the wireless LAN and the distribution system
- **Basic Service Set (BSS)**
  - » group of stations using the same AP
- **Portal**
  -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

# SSID

- **Mechanism used to segment wireless networks**
  - » Multiple independent wireless networks can coexist in the same location
- **Each AP is programmed with a SSID that corresponds to its network**
- **Client computer presents correct SSID to access AP**
- **Security Compromises**
  - » AP can be configured to “broadcast” its SSID
  - » Broadcasting can be disabled to improve security
  - » SSID may be shared among users of the wireless segment

# Association Management: Scanning, and Joining

- **Station must associate with an AP before they can use the network**
  - » AP must know about them so it can forward packets
- **Reassociation: association is transferred**
  - » Supports mobility in the same ESS
- **Disassociation: station or AP can terminate association**
- **Stations can detect AP based by scanning**
  - » **Passive Scanning:** station simply listens for Beacon and get info of the BSS. Power is saved.
  - » **Active Scanning:** station transmits Probe Request; elicits Probe Response from AP. Saves time.
- **Joining a BSS**
  - » Synchronization in Timestamp Field and frequency :
  - » Adopt PHY parameters
  - » Other parameters: BSSID, WEP, Beacon Period, etc.



(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.

# Power Management

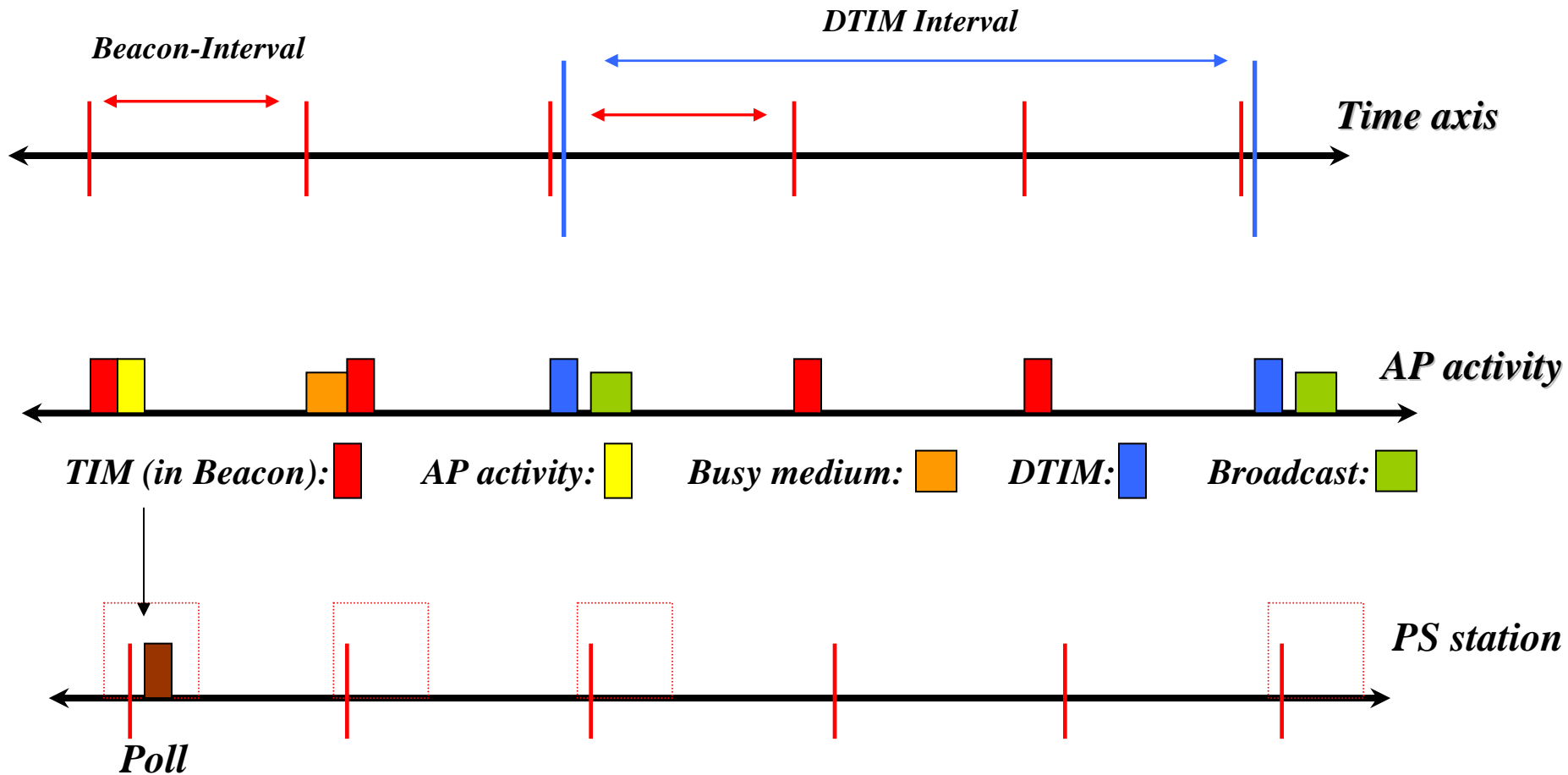
---

- **Goal is to enhance battery life of the stations**
- **Idle receive state dominates LAN adapter power consumption over time**
- **Allow stations 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 with PS stations have packets waiting at the AP
- **Power Saving stations wake up periodically and listen for beacons**
  - » If they have data waiting, they can a PS-Poll to request that AP sends the data
- **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



# WLAN Security Requirements

---

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

# Security in 802.11b

- **WEP: Wired Equivalent Privacy**
  - » Achieve privacy similar to that on LAN through encryption
  - » Intended to provide both privacy and integrity
  - » RC4 and CRC32
  - » Has known vulnerabilities
- **WPA: Wi-Fi Protected Access**
  - » Larger, dynamically changed keys
- **802.1x: port-based authentication for LANs**
  - » Port-based authentication for LANs
- **802.11i (WPA2)**
  - » Builds on WPA
  - » Uses AES for encryption

# WLAN Security Exploits

- **Insertion attacks**
  - » Unauthorized Clients or AP
- **Interception and unauthorized monitoring**
  - » Packet Analysis by “sniffing” – listening to all traffic
  - » AP Clone
- **Jamming**
  - » Denial of Service - using cordless phones, baby monitors, leaky microwave oven, etc.

# WLAN Security Exploits

- **Client-to-Client Attacks**
  - » DOS - duplicate MAC or IP addresses
  - » Can also be used to get free service on “secured” APs
- **Brute Force Attacks Against AP Passwords**
  - » Dictionary Attacks Against SSID
- **Encryption Attacks**
  - » Exploit known weaknesses of WEP
- **Misconfigurations**
  - » APs ship in an unsecured configuration
  - » Many people use APs with default configuration

# MAC Filtering

---

- **Each client identified by its 802.11 NIC Mac Address**
- **Each AP can be programmed with the set of MAC addresses it accepts**
- **Combine this filtering with the AP's SSID**
- **Overhead of maintaining list of MAC addresses**

# Wired Equivalent Privacy WEP

- **Employs RC4 to Encrypt/Decrypt data**
  - » RC4 is a stream cypher based on a symmetric algorithm
  - » 40 bit encryption key is supplied by the user
  - » 24 bit initialization vector (IV) is supplied in the header
  - » 64 bit string is seed for PRNG to generate a “key sequence”
  - » 40 and 64 bit WEP are the same thing
- **ICV (integrity check value) is computed for plaintext (CRC-32)**
- **ICV is appended to plaintext to create data string**
- **Key Sequence is XORéd to data string to create ciphertext**
- **Ciphertext and IV are sent to receiver**
- **128-bit encryption uses a 104+24 bit key**

# WEP-Based Security Discussion

- **WEP has known vulnerabilities**
- **Key can be cracked with a couple of hours of computing**
  - » IV transmitted in the clear
  - » No protocol for encryption key distribution
- **All data then becomes vulnerable to interception**
  - » WEP typically uses a single shared key for all stations
- **The CRC32 check is also vulnerable so that the data could be altered as well**
- **128-bit WEP encryption is recommended**

# WEP Authentication

---

- **Access request by client**
- **Challenge text sent to client by AP**
- **Challenge text encoded by client using shared secret then sent to AP**
- **If challenge text encoded properly, AP allows access; else access is denied**

# 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 176 bit key (48bit IV) and keys are changed periodically
  - » Also frame counter in MIC to prevent replay attacks.
- **Can be used with 802.1x authentication (optional)**
  - » It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
  - » Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- **802.11i is a “permanent” security fix**
  - » Builds on the interim WPA standard (i.e. WPA2)
  - » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
  - » Better key management and data integrity
  - » Uses 802.1x for authentication.

# Port-based Authentication

---

- **802.1x is the IEEE standard for port-based authentication**
- **Users get a username/password to access the access point**
- **Was originally defined for switches but extended to APs**
- **Can be used to bootstrap other security mechanisms**
  - » Effectively creating a session

# Best Practices for WiFi Security

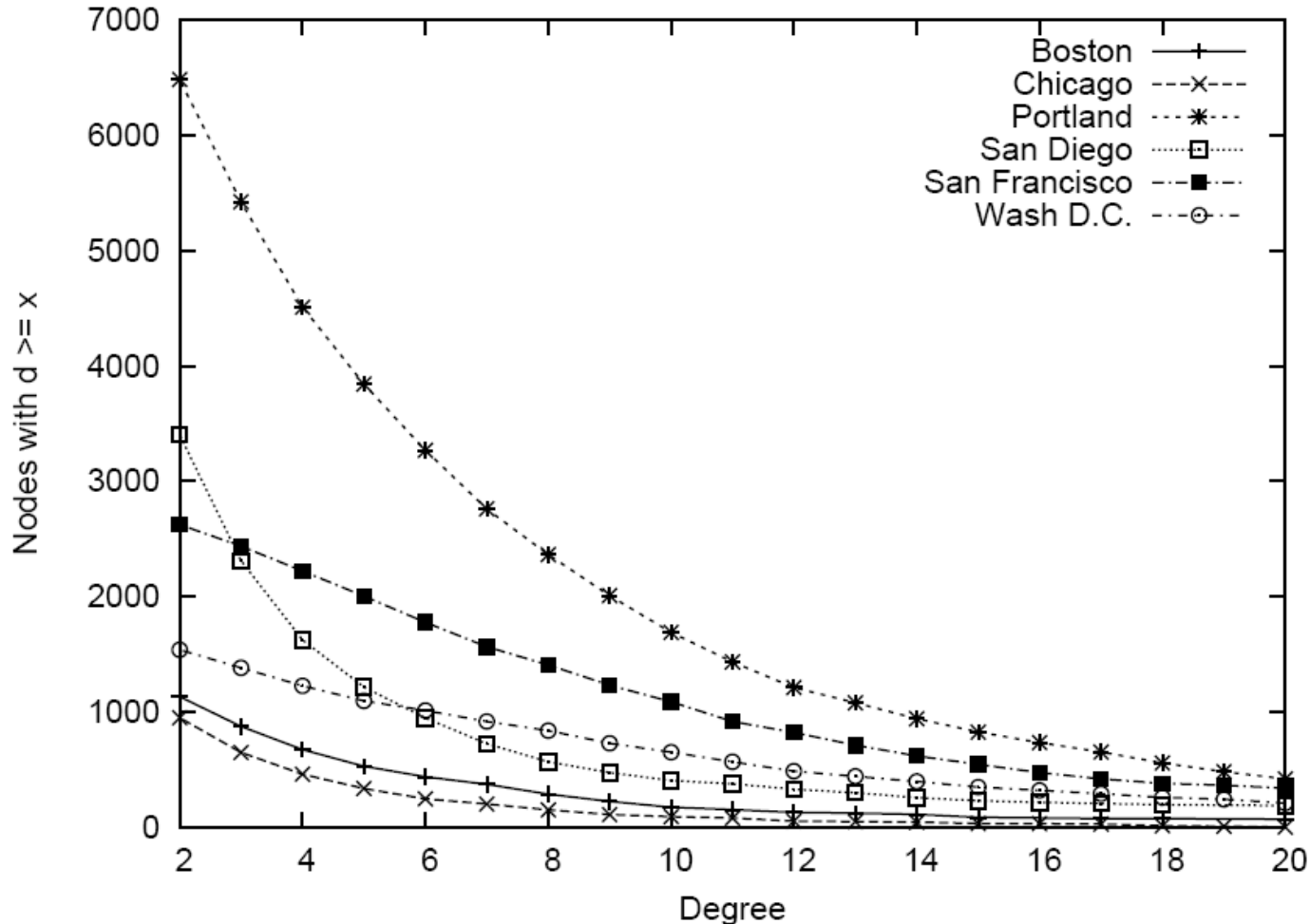
- **Use WEP**
  - » change default key
  - » change WEP key frequently
- **Change the default configuration of your AP:**
  - » Change default passwords on APs
  - » Don't name your AP by brand name
  - » Don't name your AP by model #
  - » Change default SSID
- **Use MAC filtering if available**
- **Use a VPN**
  - » Must assume that wireless segment is untrusted
  - » Provides end-to-end encryption

# Wardriving

---

- The act of locating and possibly exploiting to a wireless network while driving around a city
- You need a vehicle, a laptop, a wireless PC card and some kind of antenna
- People can intercept your wireless signal when the signal exceeds your building
- <http://www.wardriving.com>
- Is this legal??

# Example Degree Distribution



Degree of node = number of access points within range

# Netstumbler

---

- Free software that searches for unauthorized wireless access points located on your network
- Also checks coverage of your wireless LAN
- Get it at <http://www.netstumbler.com>

# Wireless “Honeypots”

- It is where you set up a wireless AP that is open (little or no security)
- These wireless AP “decoys” are not hooked up to the network; rather, you would hook it up to a wireless “honeypot” host (e.g., server with a wireless NIC) that is not wired into your network
- They act as a decoy; sniffers think they’ve stumbled onto an open AP, but you get their data instead
- Designed to log hacker activity
- Special case of honeypots

# Outline

---

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
  - » Overview of 802.11
  - » 802.11 MAC, frame format, operations
  - » 802.11 management
  - » 802.11\*
  - » Deployment example
- **Wireless Access – 802.16**
- **Personal Area Networks – 802.15**
- **Special topics**

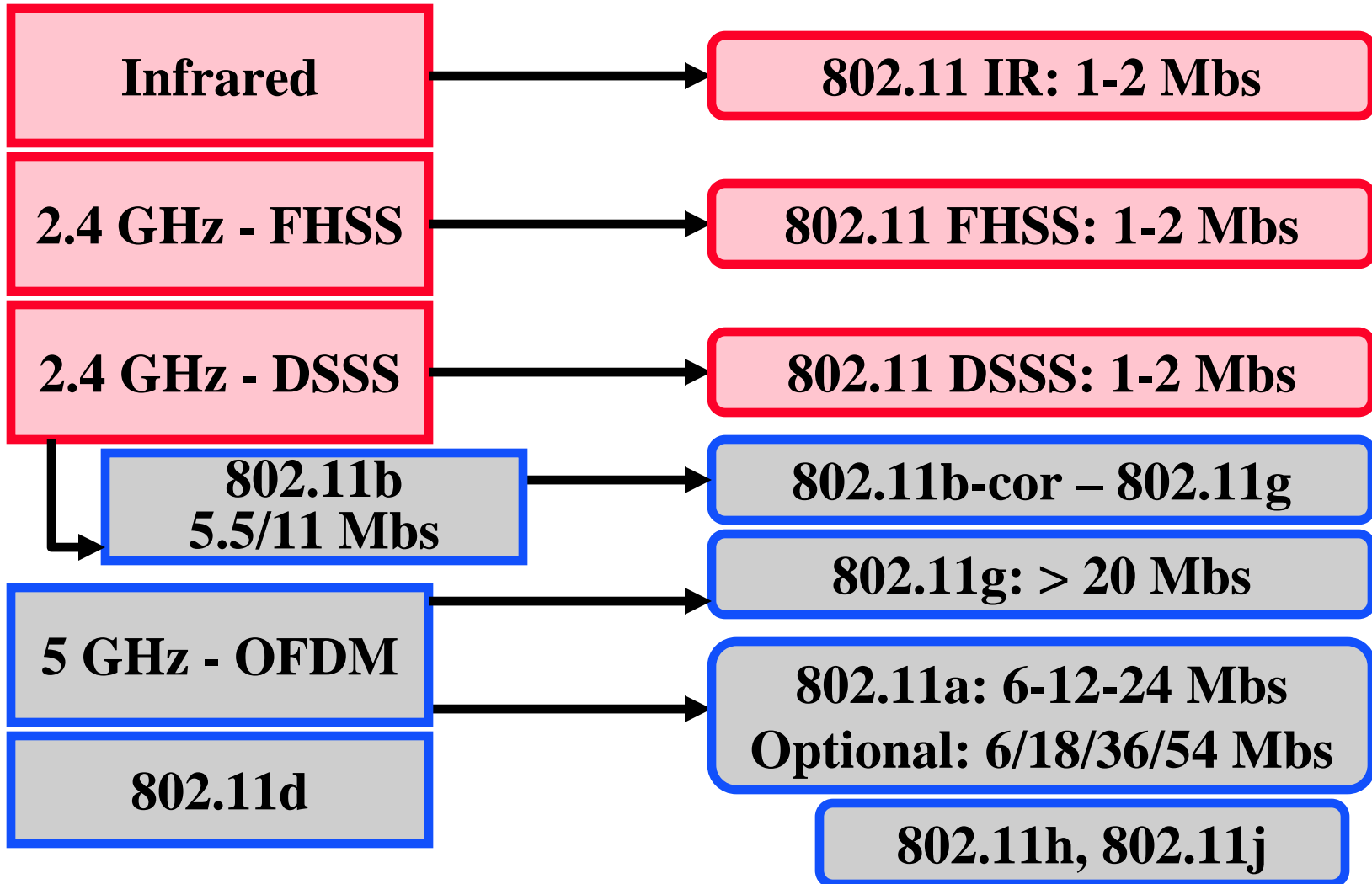
# Some IEEE 802.11 Standards

- » **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**

# IEEE 802.11 Family

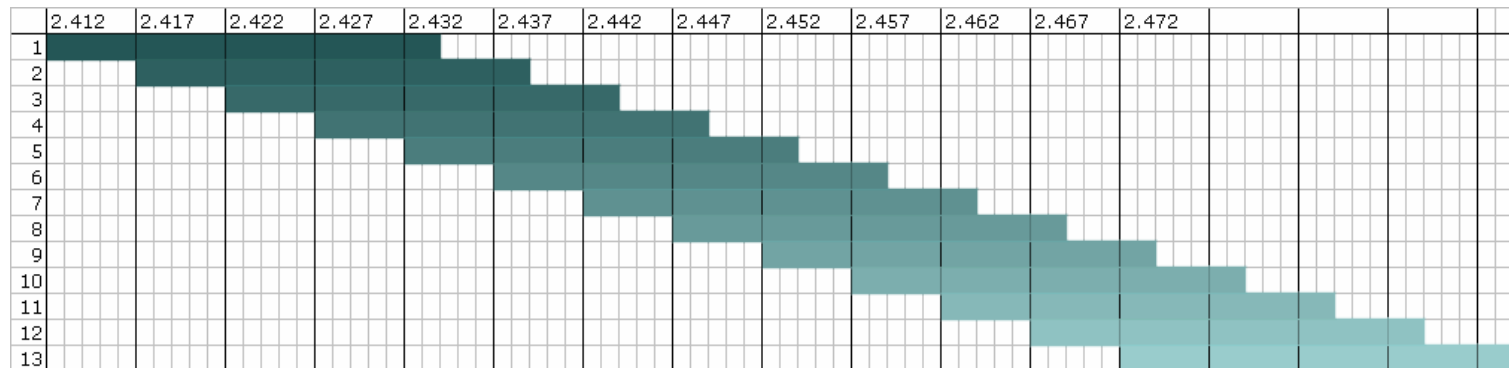
Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	540 Mbps	~50 m

# Physical Layer



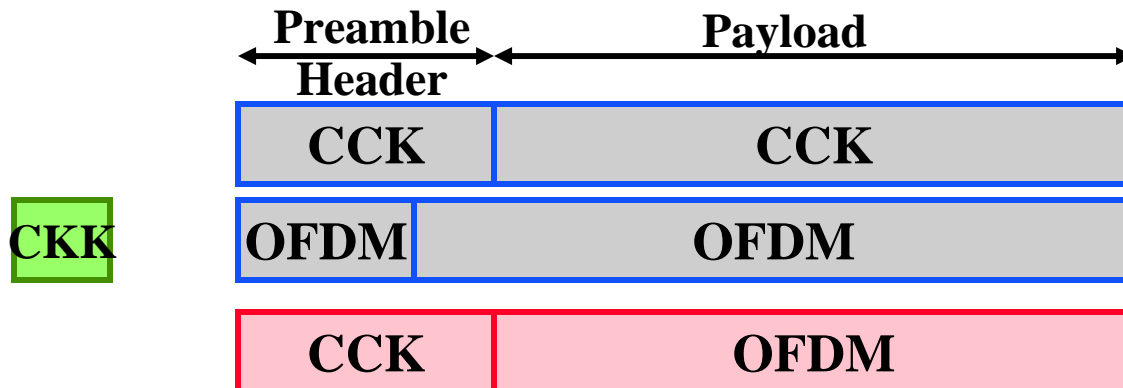
# 802.11b Channels

- 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
- Best channels are 1, 6 and 11



# Going Faster: 802.11(g)

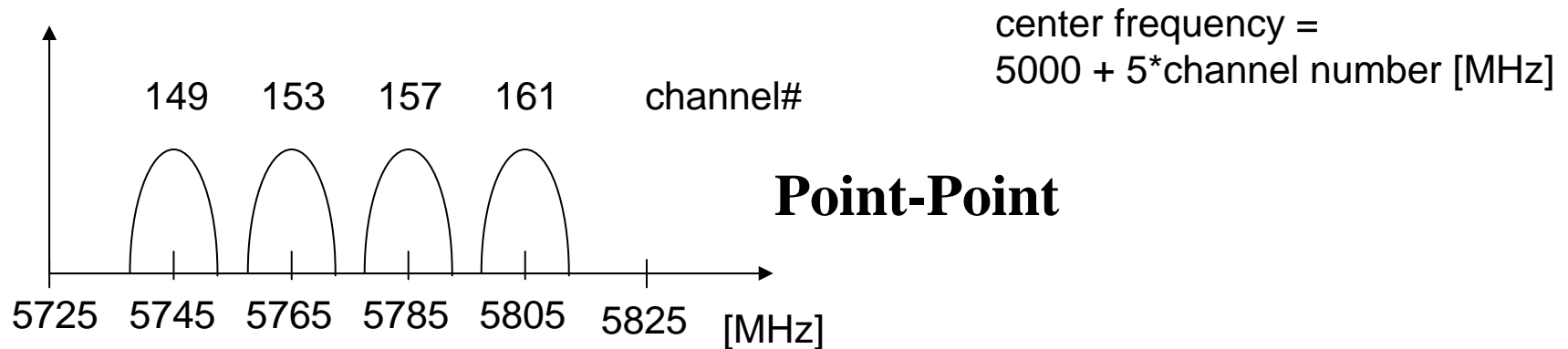
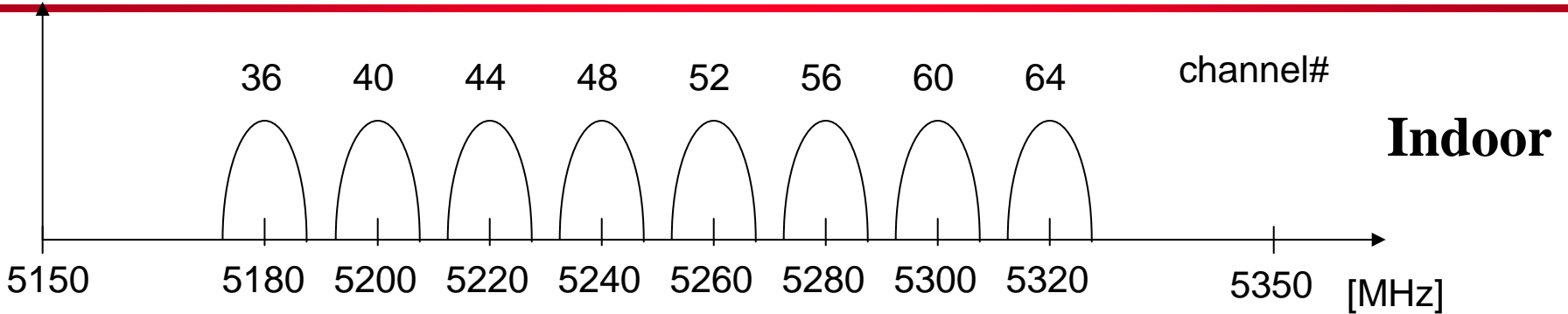
- **802.11g basically extends of 802.11b**
  - » Use the same technology DSSS/CCK for lower rates
  - » Uses OFDM technology for rates > 20 Mbps
- **Using OFDM makes it easier to build 802.11a/g cards**
  - » Since 802.11a uses OFDM
- **But it creates an interoperability problem since 802.11b cards cannot interpret OFDM signals**
  - » Solutions: send CTS using CCK before OFDM packets in hybrid environments, or use (optional) hybrid packet format



# 802.11a

- **Uses OFDM in the 5.2 and 5.7 GHz bands**
- **What are the benefits of 802.11a compared with 802.11b?**
  - » **Greater bandwidth (up to 54Mb)**
    - 54, 48, 36, 24, 18, 12, 9 and 6 Mbs
  - » **Less potential interference (5GHz)**
  - » **More non-overlapping channels**
- **But does not provide interoperability with 802.11b, as 802.11g does**

# 802.11a Physical Channels



Maximum Power Output

U-NII Band

Frequency (GHz)



# 802.11 Physical Layer Discussion

- **Antenna diversity is very common**
  - » Can significantly reduce the effect of multipath
- **RTS/CTS is almost never used**
  - » Overhead is too high compared with benefit
- **Two key parameters are the transmit power and the Clear Channel Assessment (CCA) threshold**
  - » The two parameters have impact on the hidden and exposed terminal problem
  - » With default settings, in most deployments, exposed terminals are a more common than hidden terminals
    - Transmit power is pretty high while CCA is pretty sensitive
- **Receive threshold controls what packets you will hear or ignore**

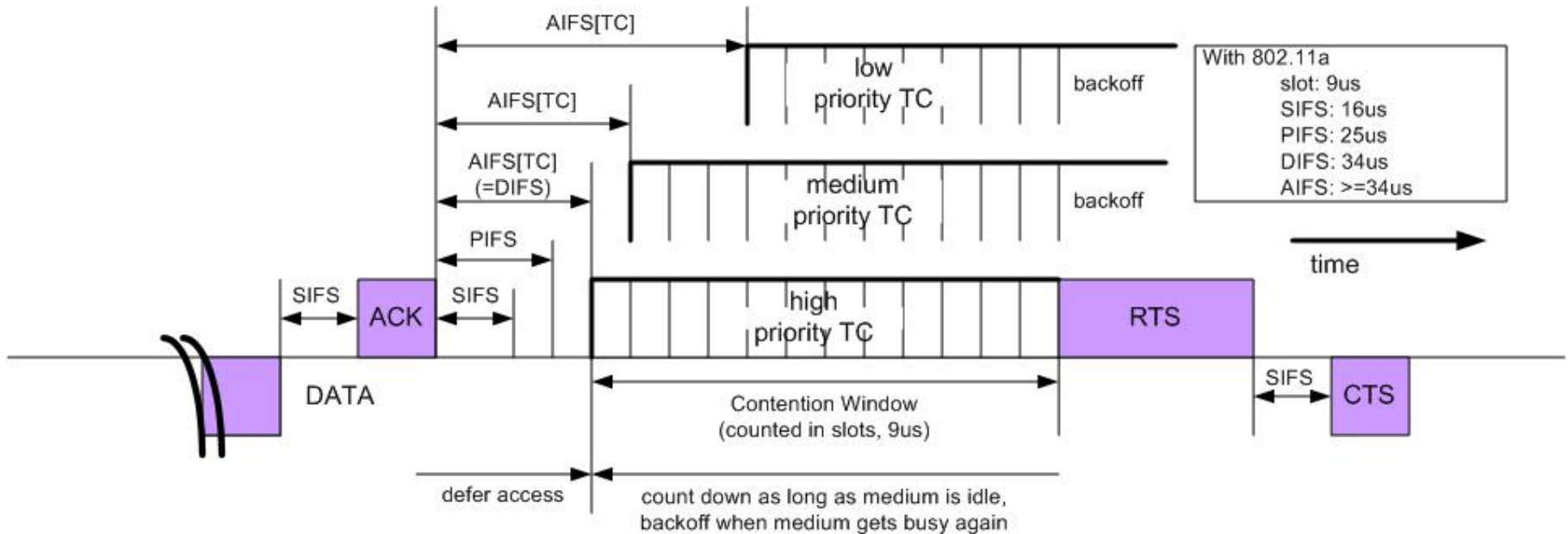
# IEEE 802.11e

- **Original intent was that 802.11 PCF could be used to provide QoS guarantees**
  - » Scheduler in the PCF prioritizes 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

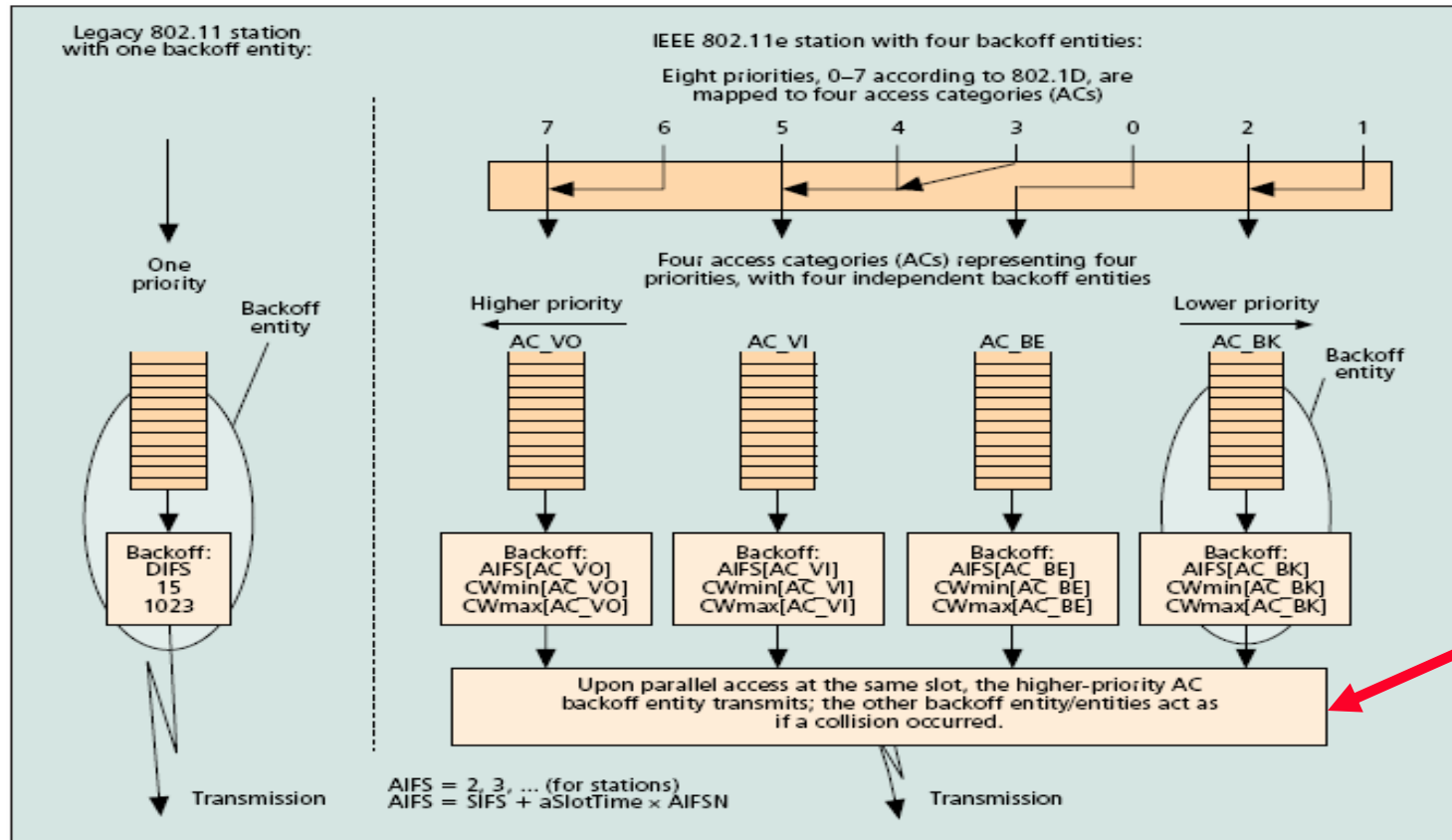
- The two types of service differentiation mechanisms proposed in EDCF are:
- ***Arbitrate Inter-frame Space (AIFS) Differentiation***
  - Different AIFSs instead of the constant distributed IFS (DIFS) used in DCF.
  - Back-off counter is selected from  $[1, CW[AC]+1]$  instead of  $[0, CW]$  as in DCF.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

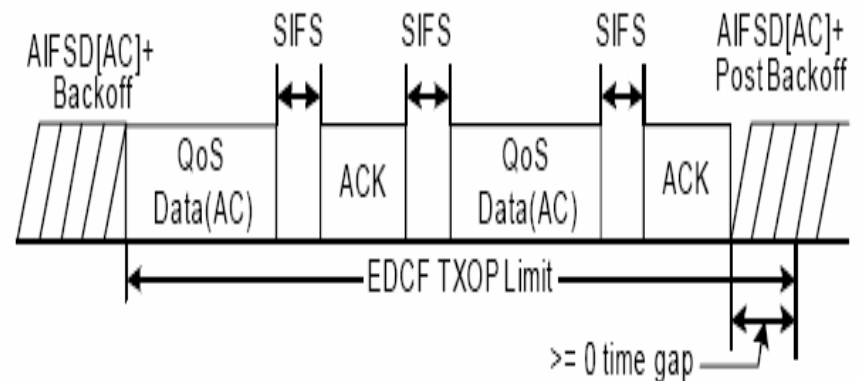
- Each frame arriving at the MAC with a priority is mapped into an AC as shown in figure below.



**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 MSDUs.**
  - » A TXOP is defined by its starting time and duration
- **CFB- In a single TXOP, multiple MSDUs can be transmitted.**
  - » “**Contention Free Burst**” (CFB)



# 802.11n

- **802.11n extends 802.11 for MIMO**
- **Standardization is still ongoing, but early products are on the market**
  - » Support in both the 2.4 and 5 GHz bands
  - » Goal: typical indoor rates of 100-200 Mbps; max 600 Mbps
- **Early products typically use either 1 or 2 non-overlapping channels**
  - » Maximum rate with 2 overlapping channels is ~300 Mbs
  - » Not clear what you get in practice
- **Tests have created interoperability problems for existing 802.11 devices**
  - » 802.11n does not sense their presence
  - » Legacy devices end up deferring and dropping in rate

# Outline

---

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
  - » Overview of 802.11
  - » 802.11 MAC, frame format, operations
  - » 802.11 management
  - » 802.11 a/b/g
  - » 802.11\*
  - » Deployment example
- **Wireless Access – 802.16**
- **Personal Area Networks – 802.15**
- **Special topics**

# What is Next?

	<b>Monday</b>	<b>Friday</b>
<b>Week 1</b>	-	<b>Lecture 1</b>
<b>Week 2</b>	<b>Lecture 2</b>	<b>Lecture 3</b>
<b>Week 3</b>	<b>Lab 1</b>	<b>Vacation</b>
<b>Week 4</b>	<b>Vacation</b>	<b>Lab 2</b>
<b>Week 5</b>	<b>Vacation</b>	<b>Lab 3/Lecture 4</b>
<b>Week 6</b>	<b>Lecture 5</b>	<b>Lab 4</b>
<b>Week 7</b>	<b>Lab 5</b>	<b>Lecture 6/Proj.</b>
<b>Week 8</b>	<b>Lecture 7</b>	<b>Lab</b>
<b>Week 9</b>	<b>Lecture 8</b>	<b>Vacation</b>
<b>Week 10</b>	-	<b>Status Pres.</b>
<b>Week 11</b>	<b>Vacation</b>	<b>Exam</b>
<b>Week 12</b>	-	<b>Lecture 9</b>
<b>Week 13</b>	<b>Lecture 10</b>	-
<b>Week 14</b>	-	<b>Final Pres.</b>