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

Lectures 6 and 7: Protocols Part 2

Peter Steenkiste

Thomas Gross

Computer Science Department

ETH Zürich

Spring Semester 2007

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**

IEEE 802.11 Overview

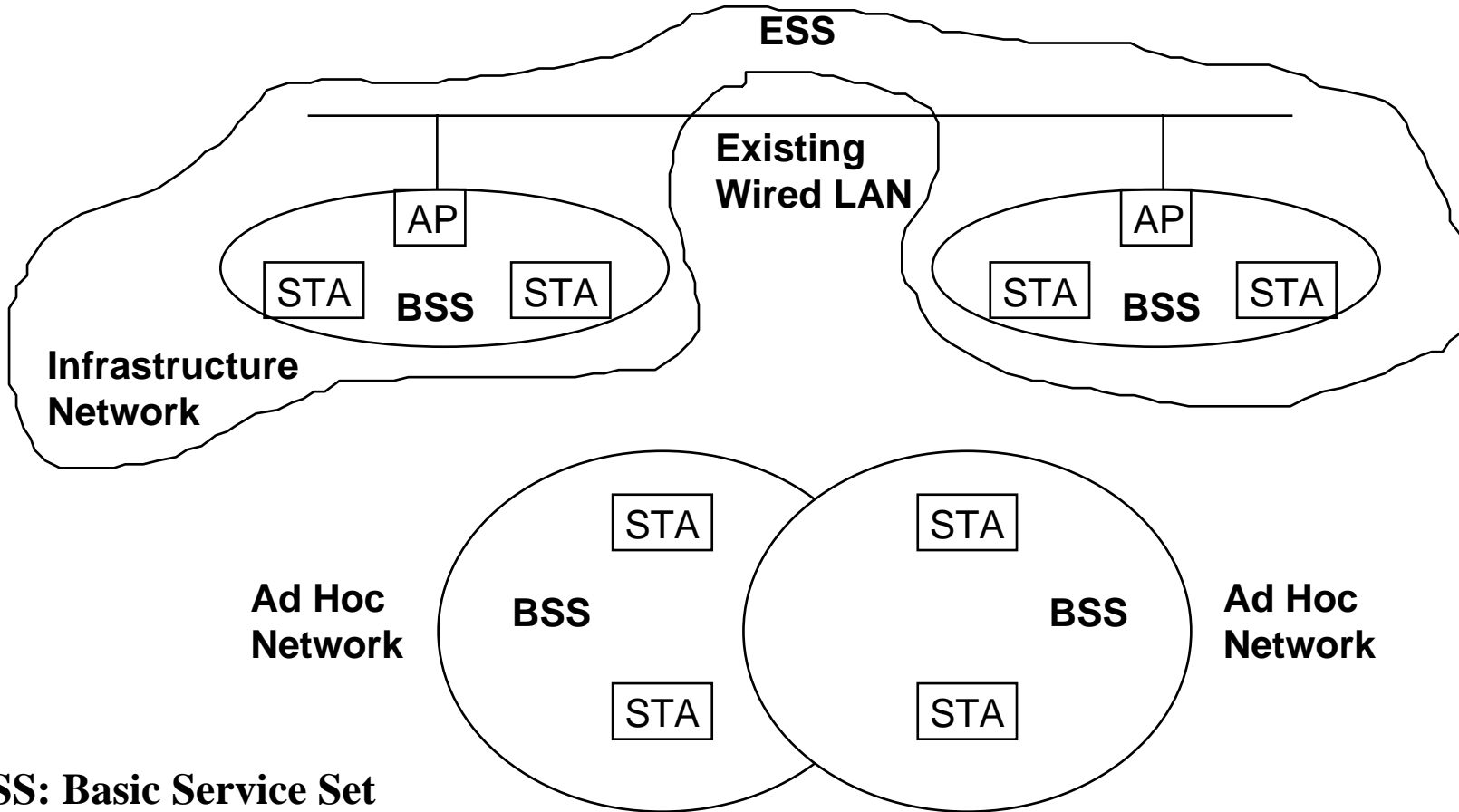
- **Adopted in 1997 with goal of providing**
 - » Access to services in wired networks
 - » High throughput
 - » Highly reliable data delivery
 - » Continuous network connection, e.g. while mobile
- **The protocol defines**
 - » MAC sublayer
 - » MAC management protocols and services
 - » Three physical (PHY) layers
 - IR
 - FHSS
 - DSSS
- **Wi-Fi Alliance is industry group that certifies interoperability of 802.11 products**

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!



802.11 Architecture



BSS: Basic Service Set

ESS: Extended Service Set

Terminology for DCF

- **Stations and access points**
- **BSS - Basic Service Set**
 - » One access point that provides access to wired infrastructure
 - » Infrastructure BSS
- **ESS - Extended Service Set**
 - » A set of infrastructure BSSs that work together
 - » APs are connected to the same infrastructure
 - » Tracking of mobility
- **DS – Distribution System**
 - » AP communicates with another
 - » Thin layer between LLC and MAC sublayers

MAC Functions

Functionality:

- **Reliable data delivery**
- **Fair control access**
- **Protection of data**

Deals with:

- **Noisy and unreliable medium**
- **Frame exchange protocol - ACK**
- **Overhead to IEEE 802.3**
- **Hidden Node Problem – RTS/CTS**
- **Participation of all stations**
- **Reaction to every frame**

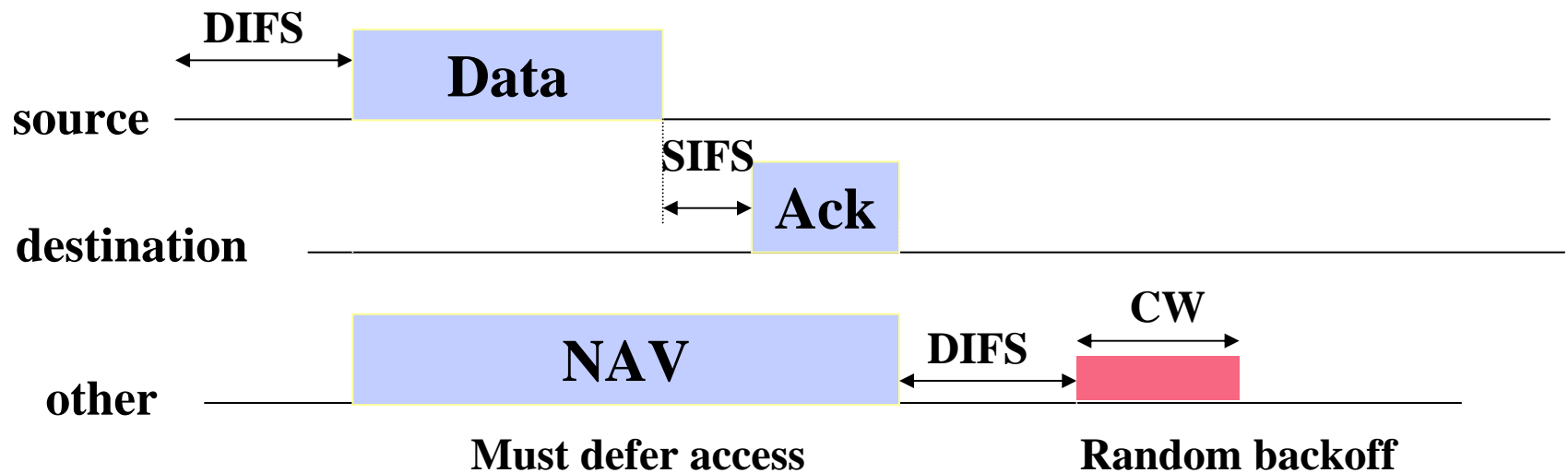
Features of 802.11 MAC protocol

- **Supports MAC functionality**
 - » Addressing
 - » CSMA/CA
- **Error detection (FCS)**
- **Error correction (ACK frame)**
- **Flow control: stop-and-wait**
- **Fragmentation (More Frag)**

Carrier Sense Multiple Access

- **Before transmitting a packet, sense carrier**
- **If it is idle, send**
 - » After waiting for one DCF inter frame spacing (DIFS)
- **If it is busy, then**
 - » Wait for medium to be idle for a DIFS (DCF IFS) period
 - » Go through exponential backoff, then send
 - » Want to avoid that several stations waiting to transmit automatically collide
- **Wait for ack**
 - » If there is one, you are done
 - » If there isn't one, assume there was a collision, retransmit using exponential backoff

DCF mode transmission without RTS/CTS

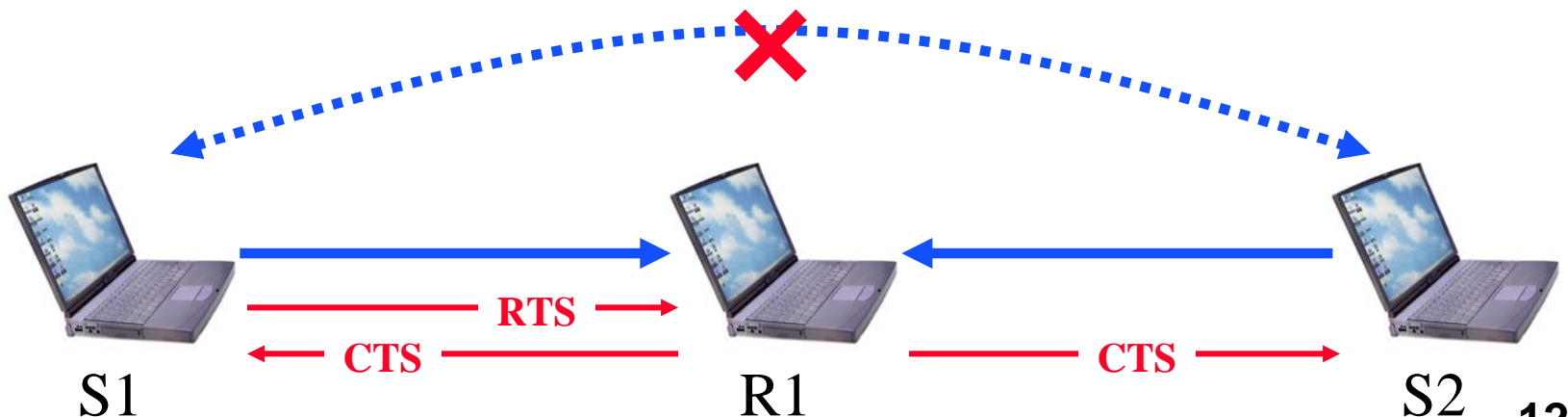


Exponential Backoff

- **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
- **If the medium is sensed it is 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; 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, ...

Collision Avoidance

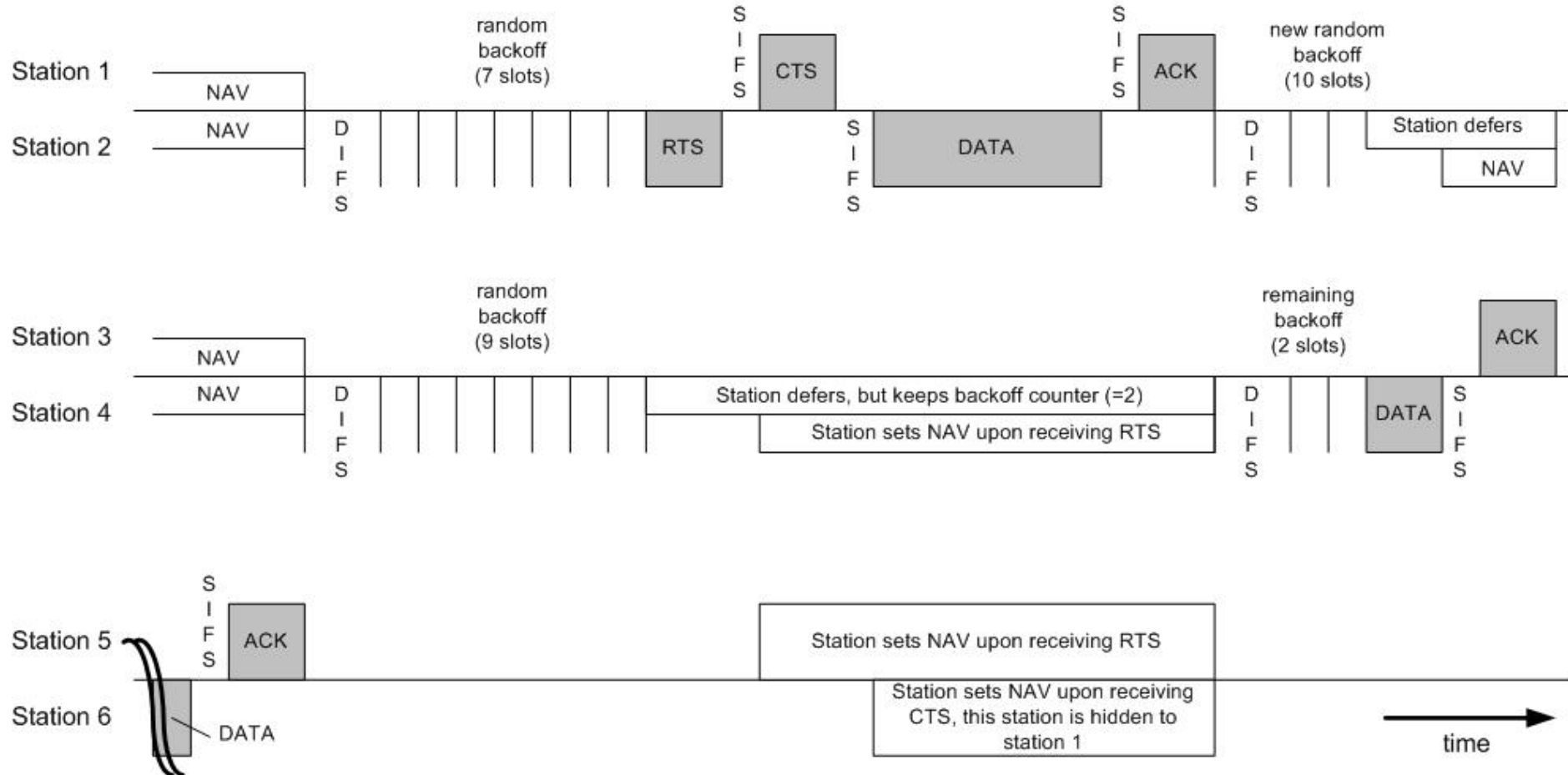
- **Difficult to detect collisions in a radio environment**
 - » While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- **Why do collisions happen?**
 - » Near simultaneous transmissions
 - Period of vulnerability: propagation delay
 - » Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver



Request-to-Send and Clear-to-Send

- **Before sending a packet, first send a station first sends a RTS.**
- **The receiving station responds with a CTS.**
 - » RTS and CTS are smaller than data packets
 - » RTS and CTS use shorter IFS to guarantee access
- **Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission**
 - » Based on a Duration ID in the RTS and CTS
- **Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)**
 - » Time that must elapse before a station can sample channel for idle status

Use of RTS/CTS

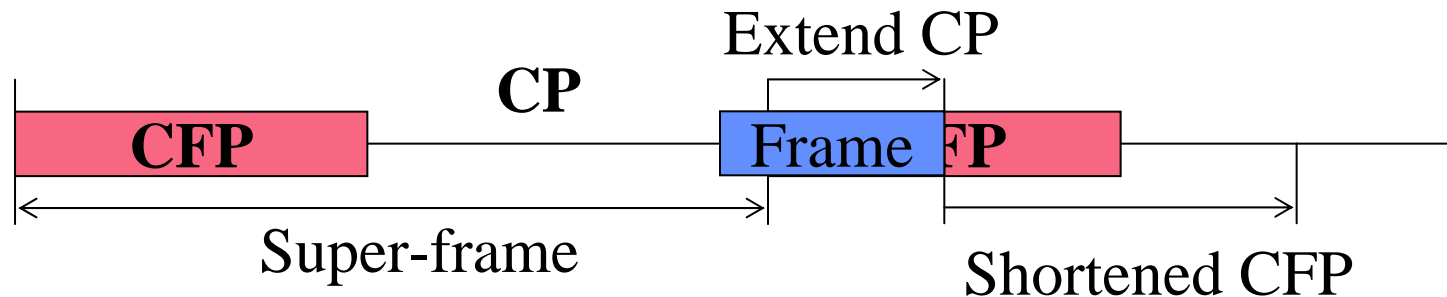


Some More MAC Features

- **Use of RTS/CTS is controlled by an RTS threshold**
 - » RTS/CTS is only used for data packets longer than the RTS threshold
 - » Pointless to use RTS/CTS for short data packets – high overhead!
- **Number of retries is limited by a Retry Counter**
 - » Short retry counter: for packets shorter than RTS threshold
 - » Long retry counter: for packets longer than RTS threshold
- **Packets can be fragmented.**
 - » Each fragment is acknowledged
 - » But all fragments are sent in one sequence
 - » Sending shorter frames can reduce impact of bit errors
 - » Lifetime timer: maximum time for all fragments of frame

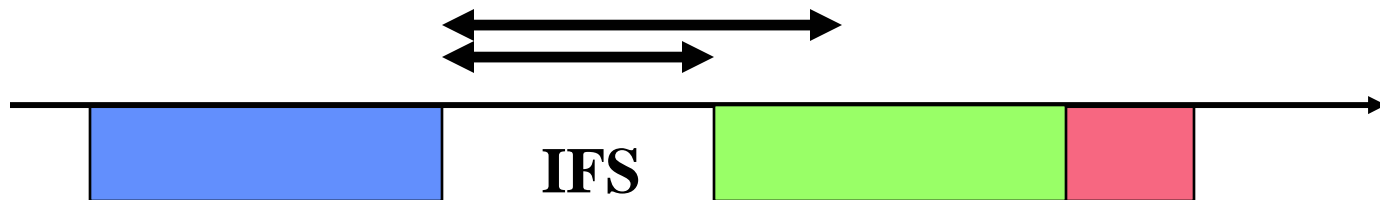
Now What about PCF?

- **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**



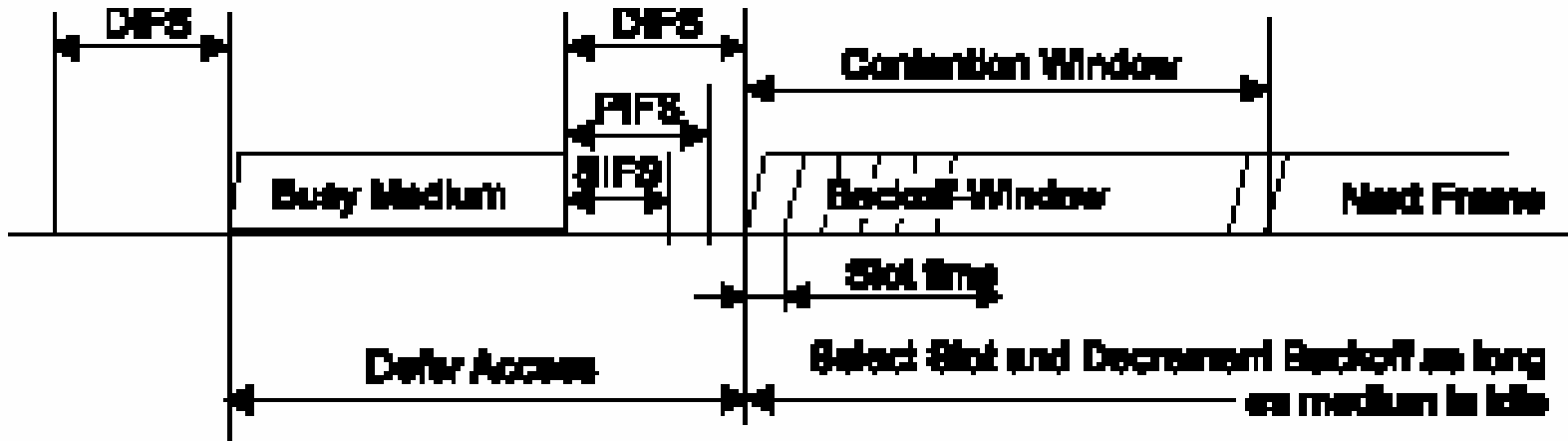
Playing Games with Inter Frame Spacing

- Assigning different IFS effectively provides a mechanism for prioritizing packets and events
- SIFS - short IFS: for high priority transmissions
- PIFS – PCF IFS: used by PCF during contention-free period
- DIFS – DCF IFS: used for contention-based services
- EIFS – extended IFS: used when there is an error



Effect of Different IFS

Immediate access when medium is free \Rightarrow DIFS



- PCF transmissions effectively get priority over DCF transmission because they use a shorter IFS

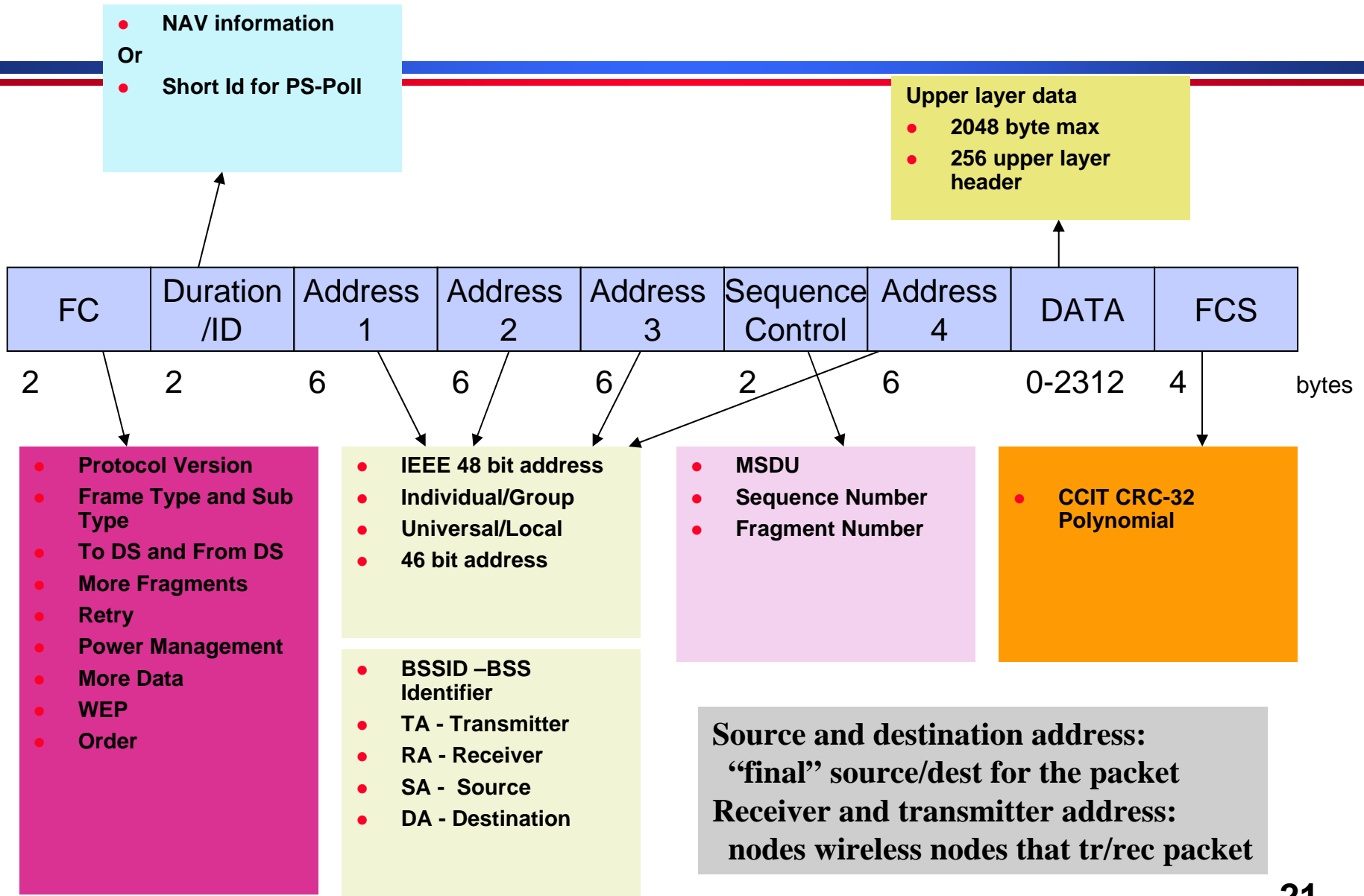
PCF Operation Overview

- **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

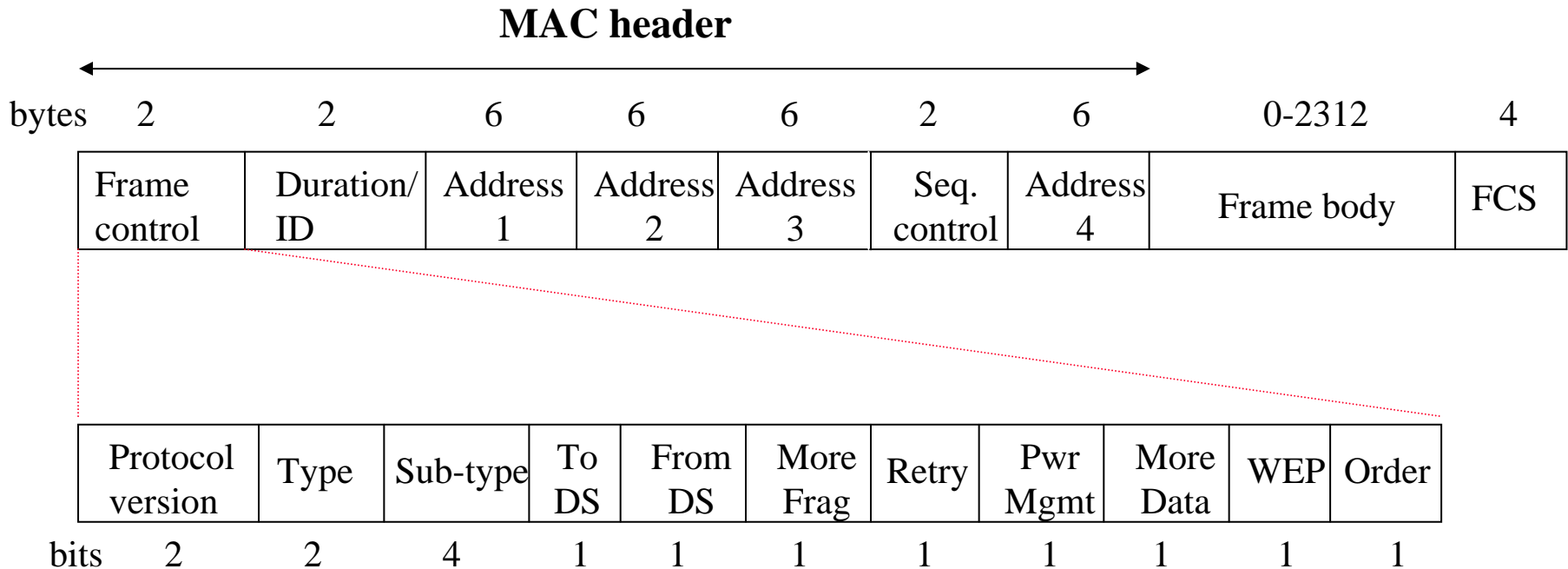
And What about Ad Hoc?

- **Infrastructure mode: access points relay packets**
 - » Based on an Infrastructure BSS
 - » APs are connected through a distribution system
- **Ad-hoc mode: no fixed network infrastructure**
 - » Based on an Independent BSS
 - » A wireless endpoint sends and all nodes within range can pick up signal
 - » Each packet carries destination and source address
 - » Effectively need to implement a “network layer”
 - How do know who is in the network?
 - Routing?
 - Security?
 - » Research area – discussed later in the course

Frame Format



Detailed 802.11 MAC Frame Format



Packet Types

- **Type/sub-type field is used to indicate the type of the frame**
- **Management:**
 - » Association/Authentication/Beacon
- **Control**
 - » RTS, CTS, CF-end, ACK
- **Data**
 - » Data only, or Data + CF-ACK, or Data + CF-Poll or Data + CF-Poll + CF-ACK

Addressing Fields

To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS; all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

RA: Receiver Address **TA: Transmitter Address**
DA: Destination Address **SA: Source Address**
BSSID: MAC address of AP in an infrastructure BSS

Some More Fields

- **Duration/ID:** Duration in DCF mode/ID is used in PCF mode
- **More Frag:** 802.11 supports fragmentation of data
- **More Data:** In polling mode, station indicates it has more data to send when replying to CF-POLL
- **RETRY** is 1 if frame is a retransmission; **WEP** (Wired Equivalent Privacy)
- **Power Mgmt** is 1 if in Power Save Mode; **Order = 1** for strictly ordered service

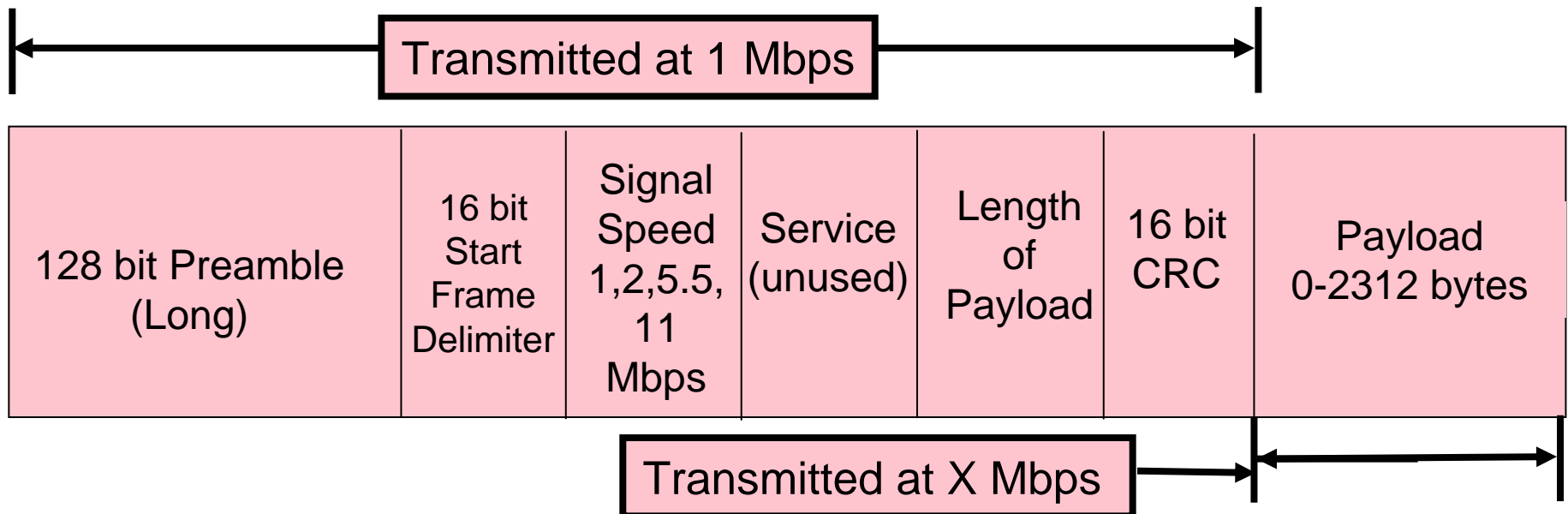
Multi-bit Rate

- **802.11 allows for multiple bit rates**
 - » Allows for adaptation to channel conditions
 - » Specific rates dependent on the version
- **Algorithm for selecting the rate is not defined by the standard – left to vendors**
- **Packets have multi-rate format**
 - » Different parts of the packet are sent at different rates

Long Preamble

Long Preamble = 144 bits

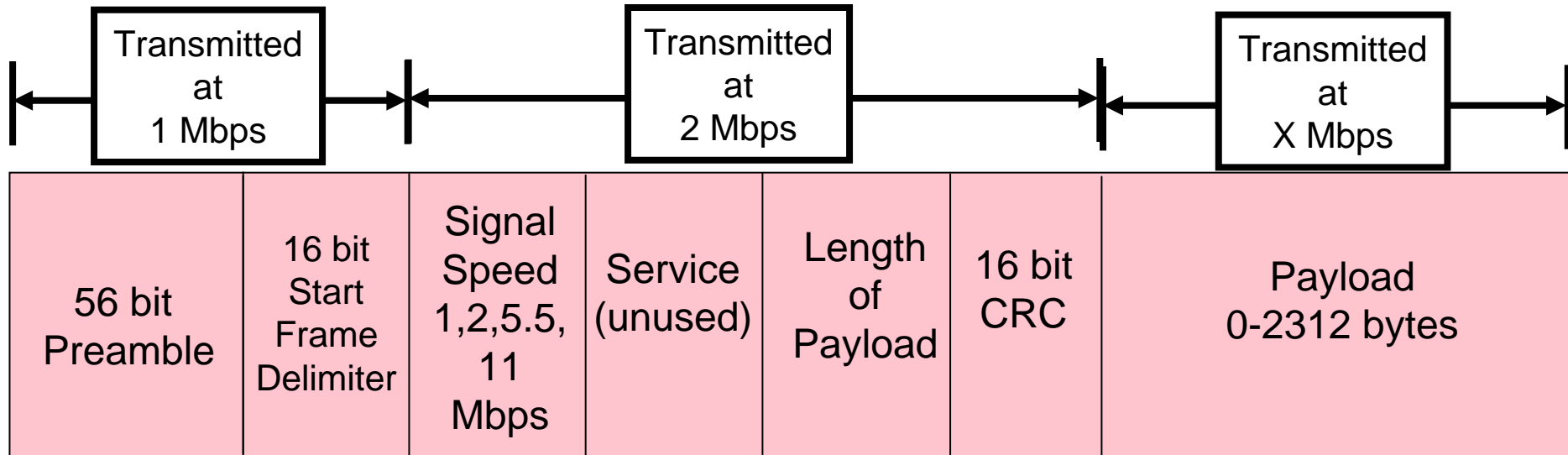
- Interoperable with older 802.11 devices
- Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*



Short Preamble

Short Preamble = 72 bits

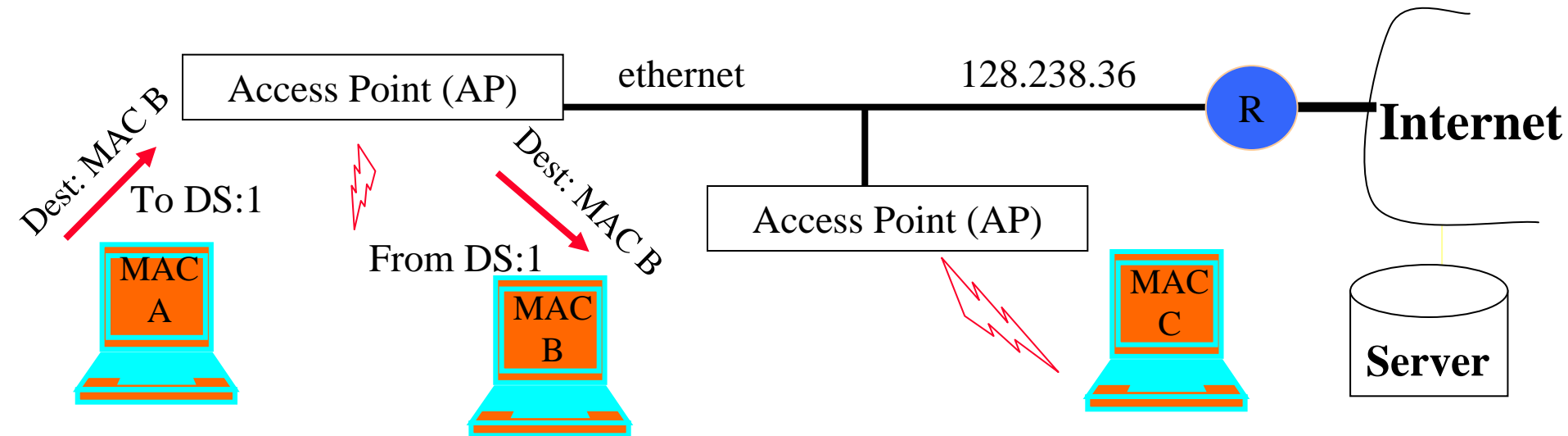
- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble



Data Flow Examples

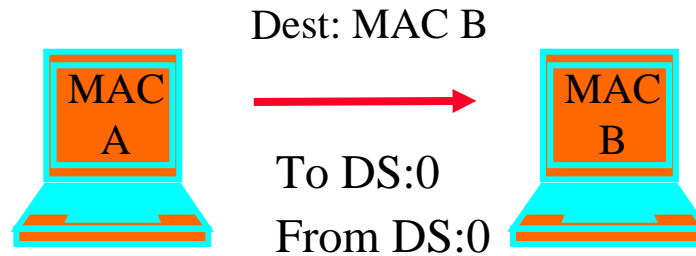
- **Case 1: Packet from a station under one AP to another in same AP's coverage area**
- **Case 2: Packet between stations in an IBSS**
- **Case 3: Packet from an 802.11 station to a wired server on the Internet**
- **Case 4: Packet from an Internet server to an 802.11 station**

Case 1: Communication Inside BSSS



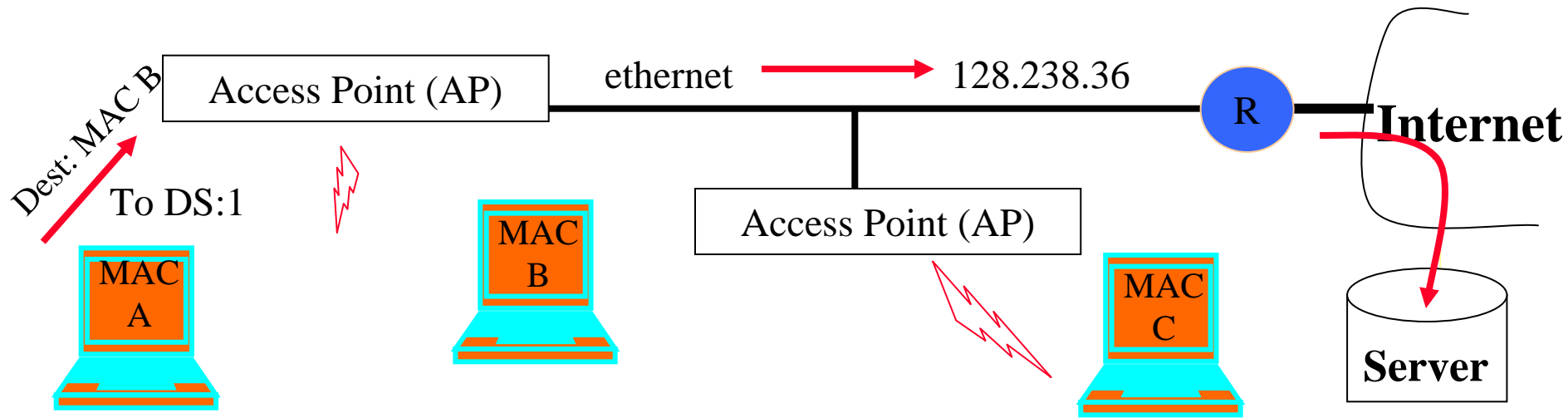
- **AP knows which stations are registered with it so it knows when it can send frame directly to the destination**

Case 2: Ad Hoc



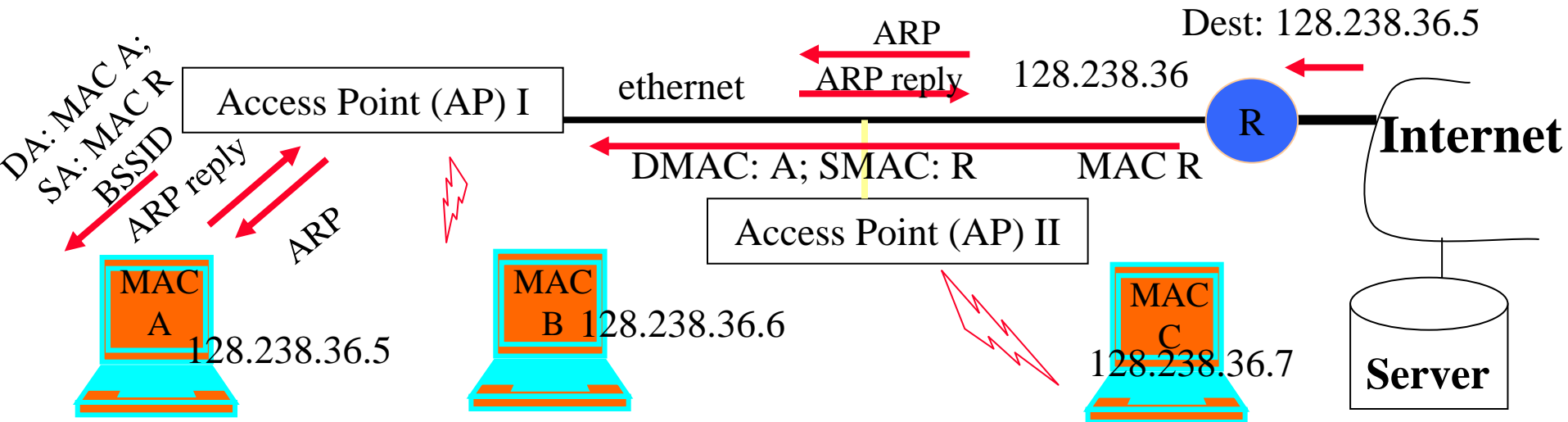
- **Direct transmit only in IBSS (Independent BSS), i.e., without AP**
- **Note: in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B**

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?**

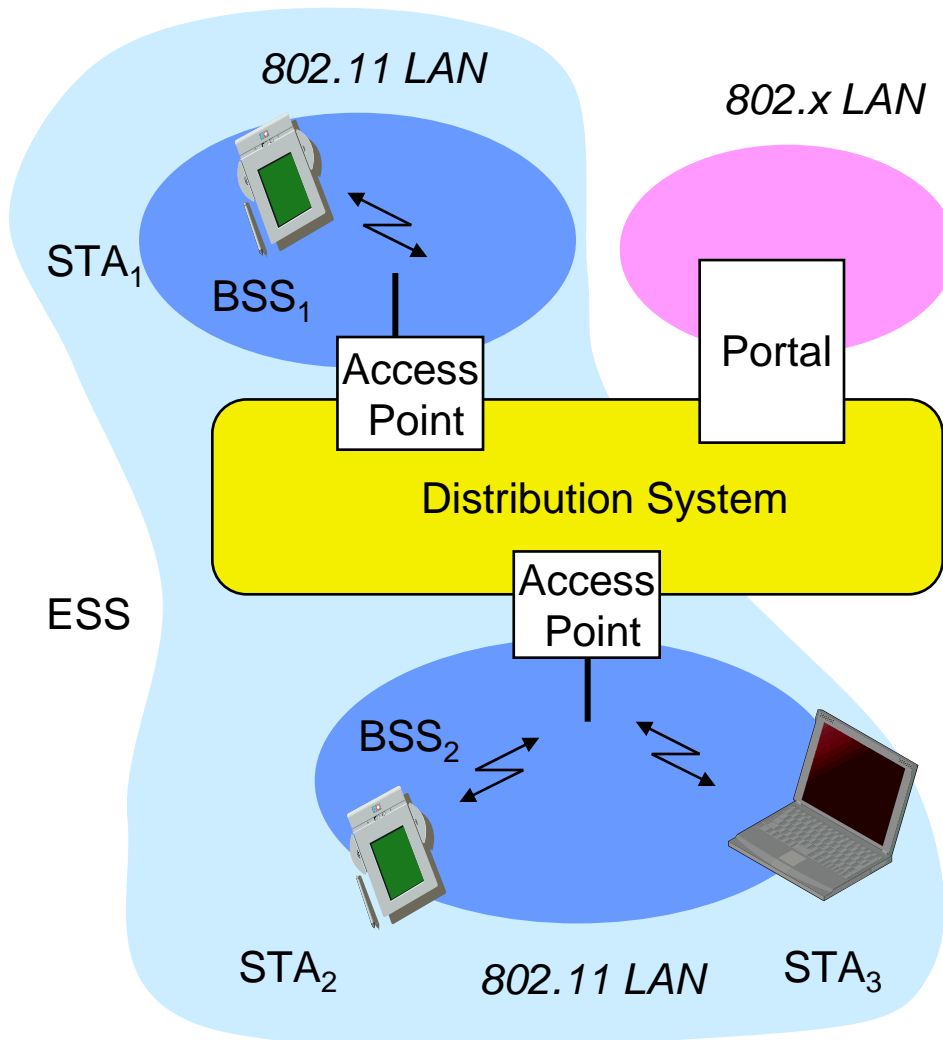
Outline

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
 - » Overview of 802.11
 - » 802.11 MAC, frame format, operations
 - » 802.11 management
 - » 802.11 a/b/g
 - » 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



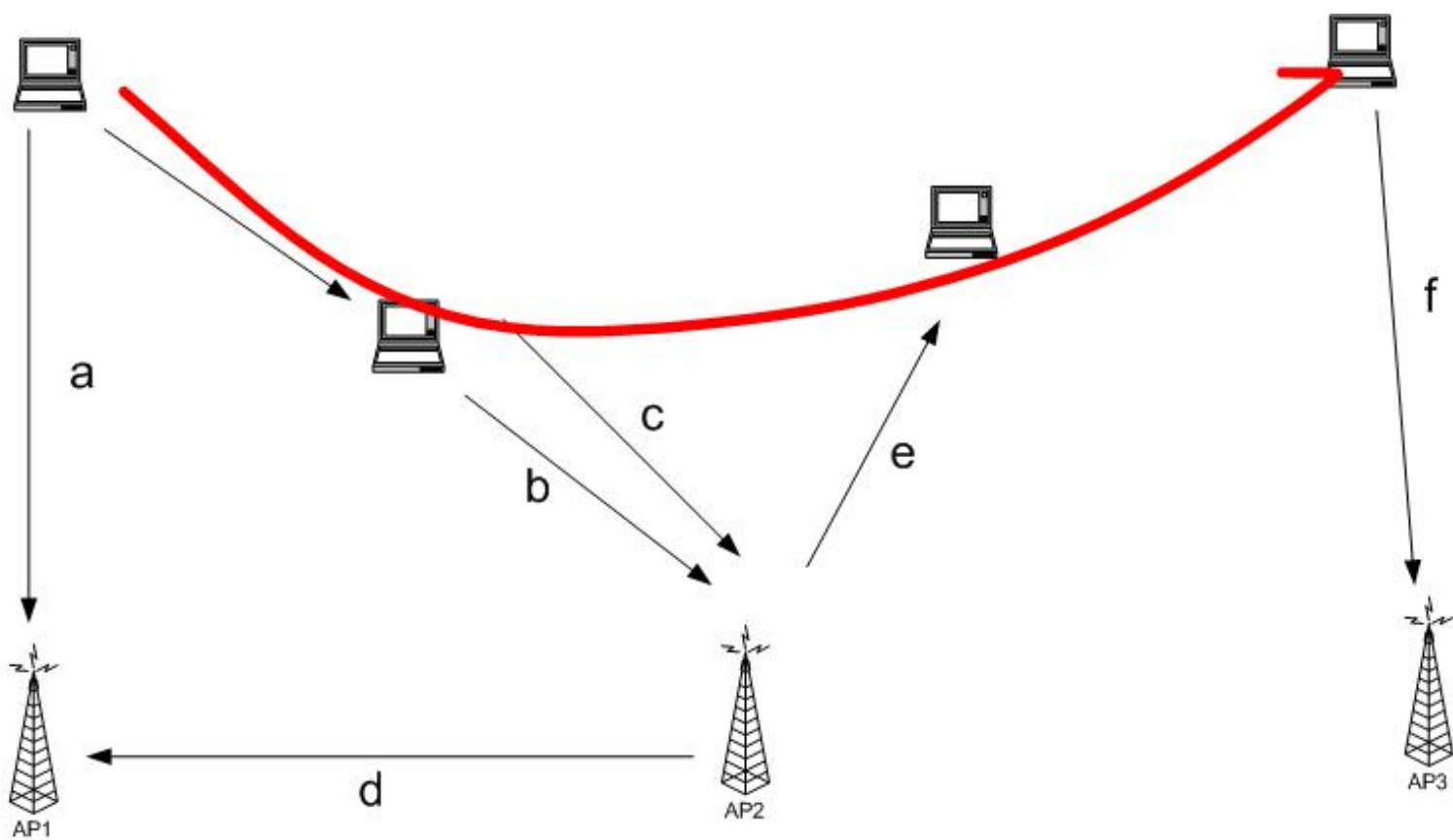
- **Station (STA)**
 - » terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Access Point**
 - » station integrated into the wireless LAN and the distribution system
- **Basic Service Set (BSS)**
 - » group of stations using the same AP
- **Portal**
 - » bridge 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.

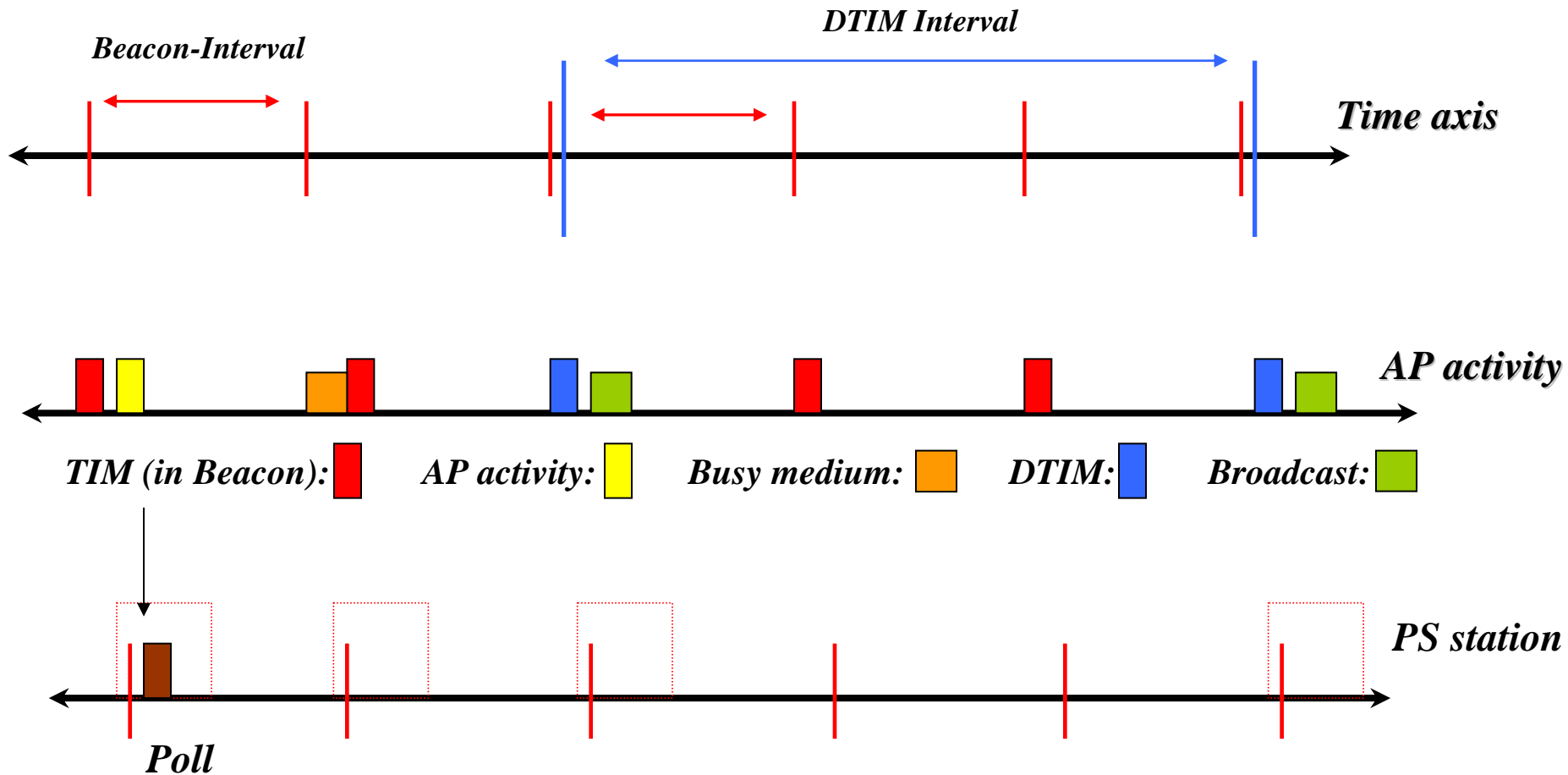
Power Management

- **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
 - » 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

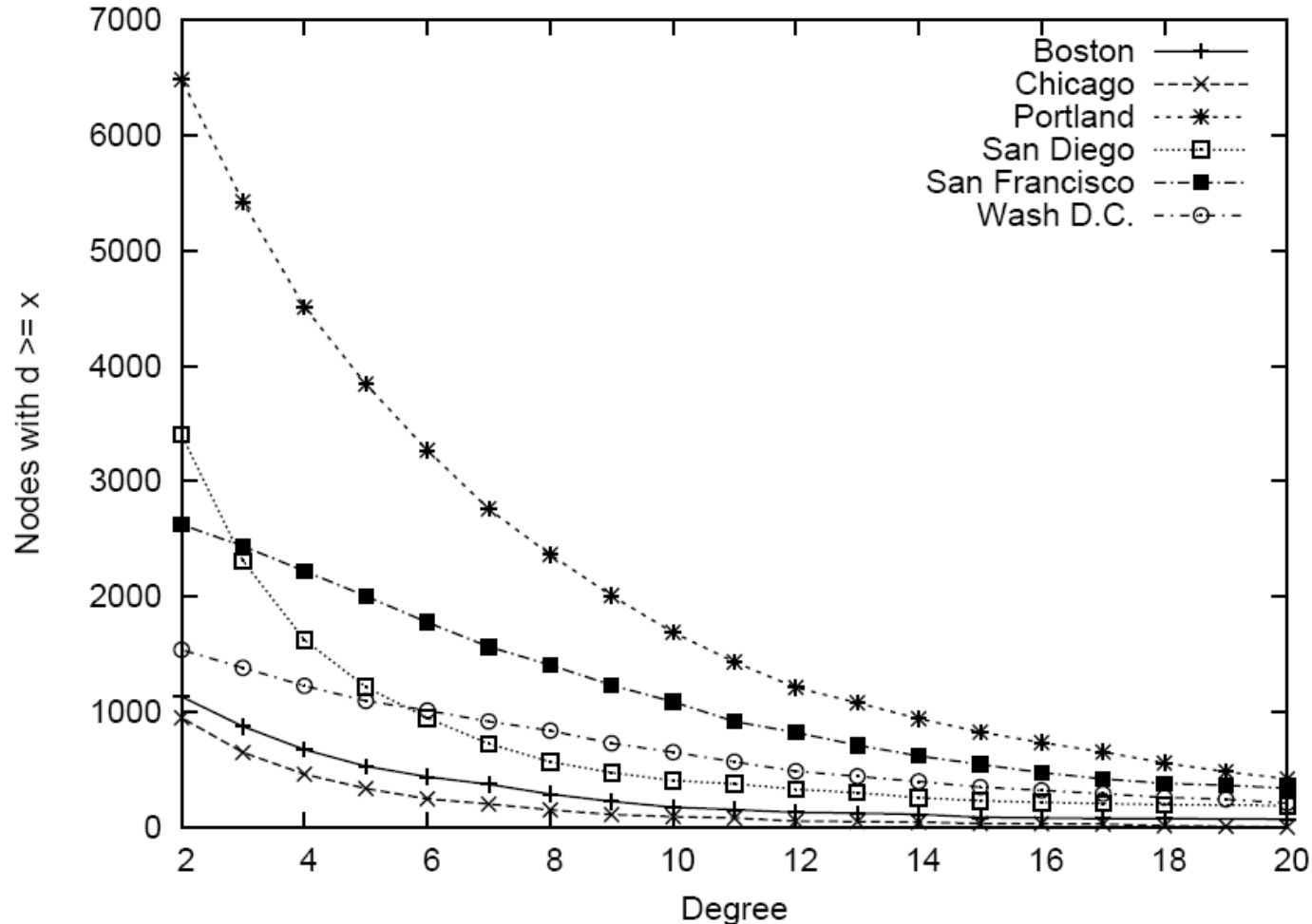
Best Practices for WiFi Security

- **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