This lecture is being recorded

18-452/18-750
Wireless Networks and Applications
Lecture 8: Wireless LANs
802.11 Wireless

Peter Steenkiste

Spring Semester 2022

http://www.cs.cmu.edu/~prs/wirelessS22/

Outline

- Data link fundamentals
  - And what changes in wireless
- Aloha
- Ethernet
- Wireless-specific challenges
- 802.11 and 802.15 wireless standards

So What about Wireless?

- Wireless datalink protocols similar to those used in wired networks
- Wireless is inherently multiple access
- The specifics depend on many factors, but ..
- Random access solutions are a good fit for data in the unlicensed spectrum
  - » Low control complexity, especially for contention-based protocols (e.g., Ethernet)
  - » No control over the shared spectrum band

Next

- Cellular uses scheduled access
  - » Need to be able to guarantee performance
  - » Have control over spectrum – simplifies scheduled access
  - » There is always a central controller

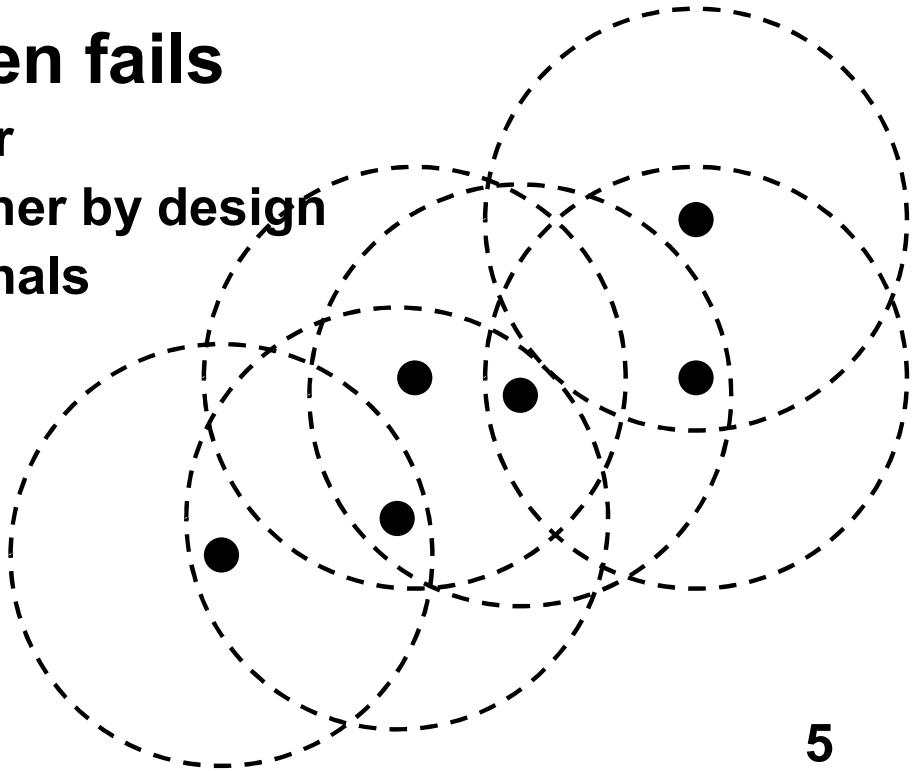
Later

Wireless Ethernet is a Good Idea, but …

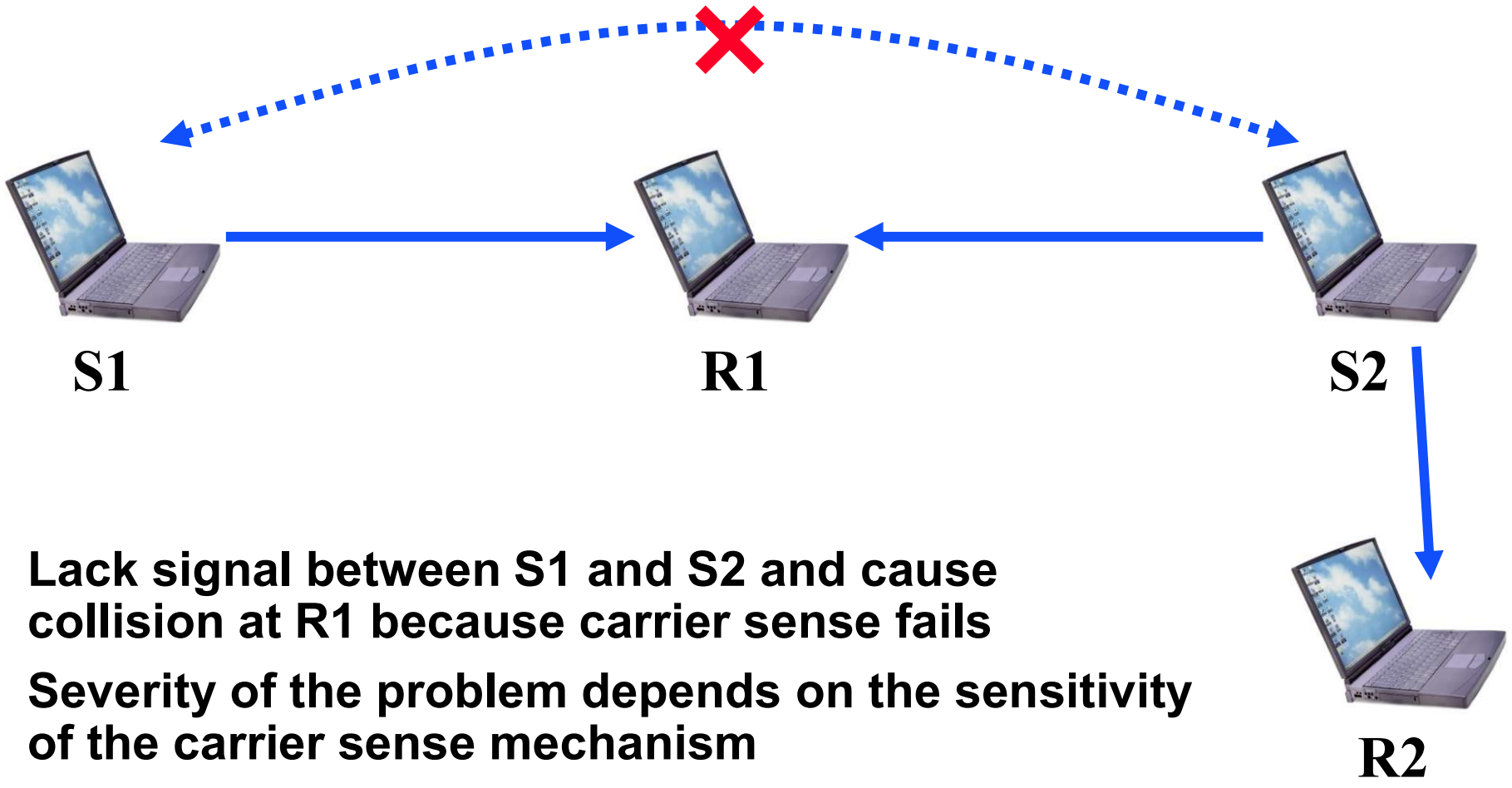
- **Attenuation is very different from that of a wire**
  - » **Depends strongly on distance, frequency**
- **Wired media have exponential attenuation**
  - » **Received power at d meters proportional to 10^{-kd}**
  - » **Attenuation in dB = *k d*, where *k* is dB/meter**
- **Wireless attenuation is quadratic in d**
  - » **Received power at d meters proportional to d^{-n}**
  - » **Attenuation in dB = *n log d*, where *n* is path loss exponent; *n=2* in free space**
  - » **So signal level more slowly with distance?**
- **No! We cannot igenore the constants!**
  - » **Wireless attenuation at 2.4 GHz: 60-100 dB**
  - » **In practice numbers are much lower for wired**

Implications for Wireless Ethernet

- **Collision detection is not practical**
  - » Ratio of transmitted signal power to received power is too high at the transmitter
  - » Transmitter cannot detect competing transmitters (is deaf while transmitting)
  - » So how do you detect collisions?
- **"Listen before you talk" often fails**
  - » Not all nodes can hear each other
  - » Ethernet nodes can hear each other by design
  - » Hidden terminals, exposed terminals
  - » Capture effects
- **Made worse by fading**
  - » Changes over time!

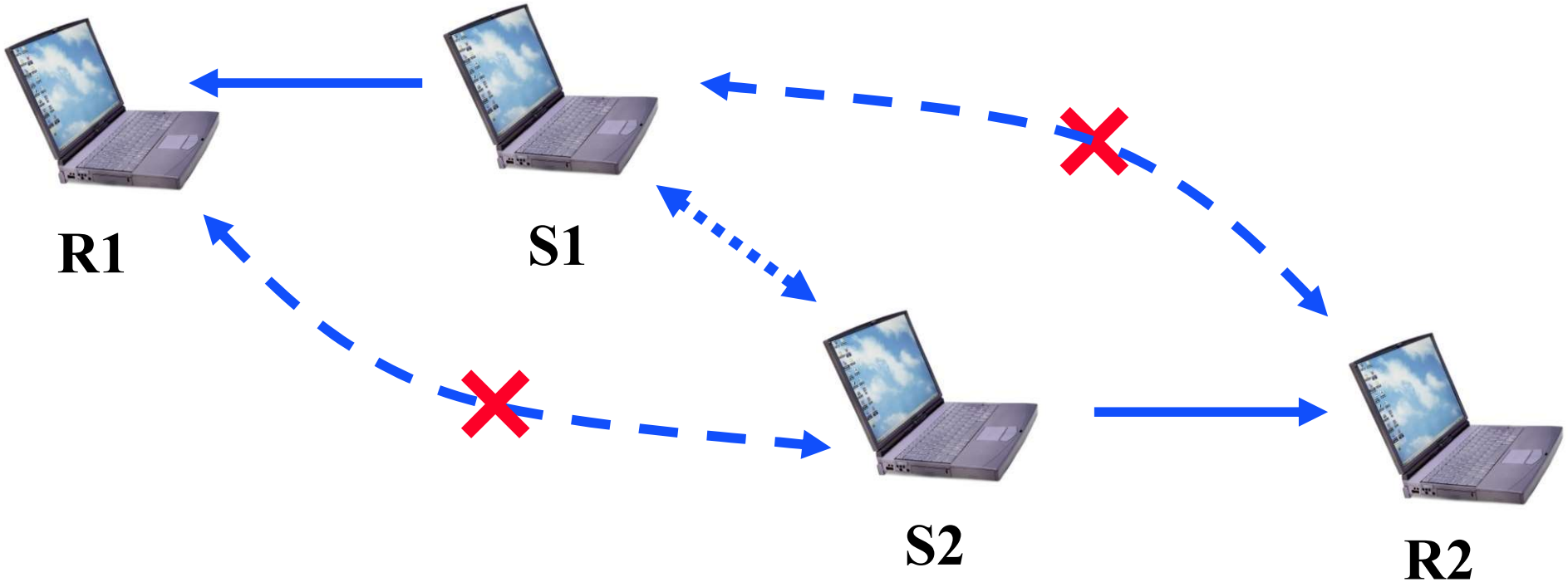


Hidden Terminal Problem



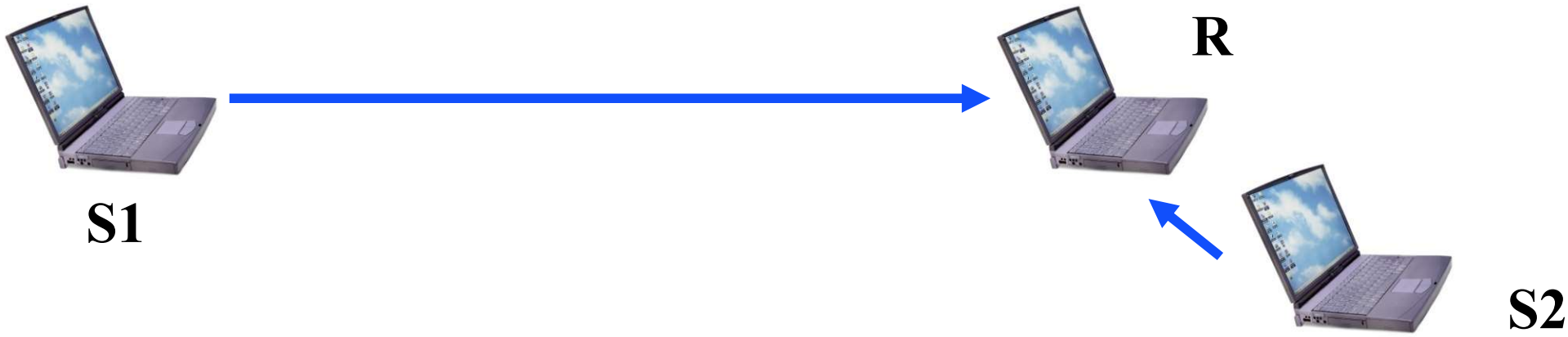
- Lack signal between S1 and S2 and cause collision at R1 because carrier sense fails
- Severity of the problem depends on the sensitivity of the carrier sense mechanism
  - » Clear Channel Assessment (CCA) threshold

Exposed Terminal Problem



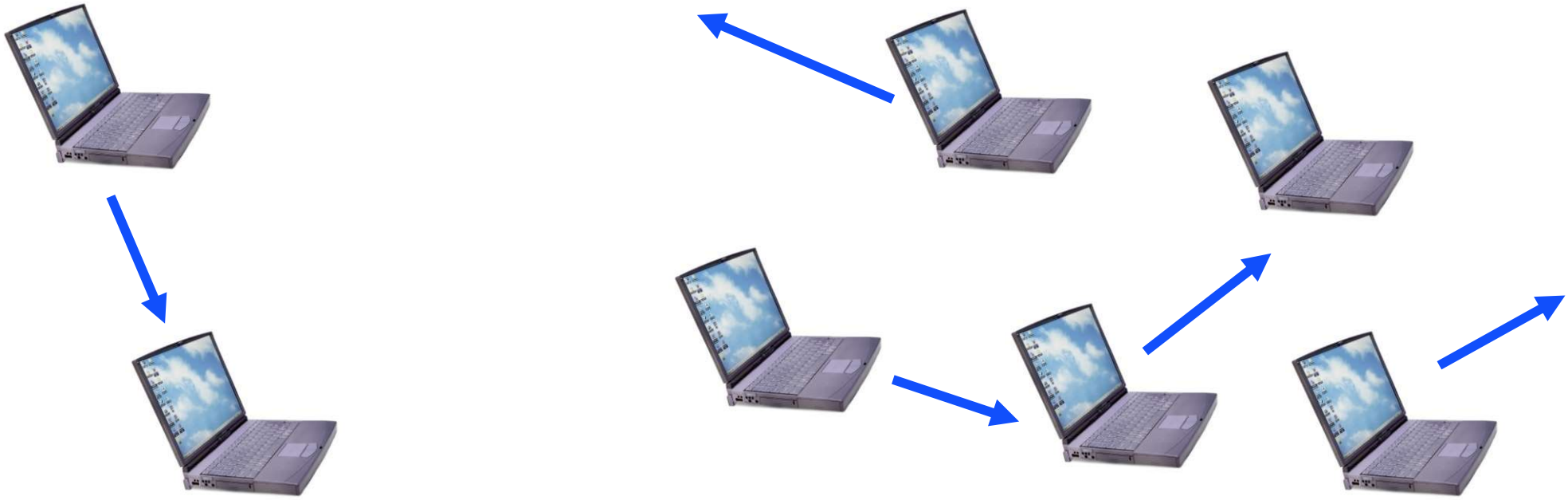
- Carrier sense prevents two senders from sending at the same time even when they cannot reach each other's receiver
- Severity again depends on CCA threshold
  - » Higher CCA reduces occurrence of exposed terminals, but can create hidden terminal scenarios

Capture Effect



- Sender S2 will almost always "win" if there is a collision at receiver R.
- Can lead to extreme unfairness and even starvation.
- Solution is power control
  - » Very difficult to manage in a non-provisioned environment!

Wireless Packet Networking Problems



- Some nodes suffer from more interference than others
  - » Node density
  - » Traffic volume sent by neighboring nodes
- Leads to unequal throughput
- Similar to wired network: some flows traverse tight bottleneck while others do not

Summary
Wireless Challenges

- **Wireless signal propagation creates problems for "wireless Ethernet"**
  - » **Collision Detection is not possible**
  - » **Hidden and exposed terminals**
  - » **Capture effect**
- **Aloha uses a very simple protocol: offers low latency but has terrible capacity**
- **Ethernet has much better performance but its key features do not work for wireless**
- **How can we do better for wireless?**

Outline

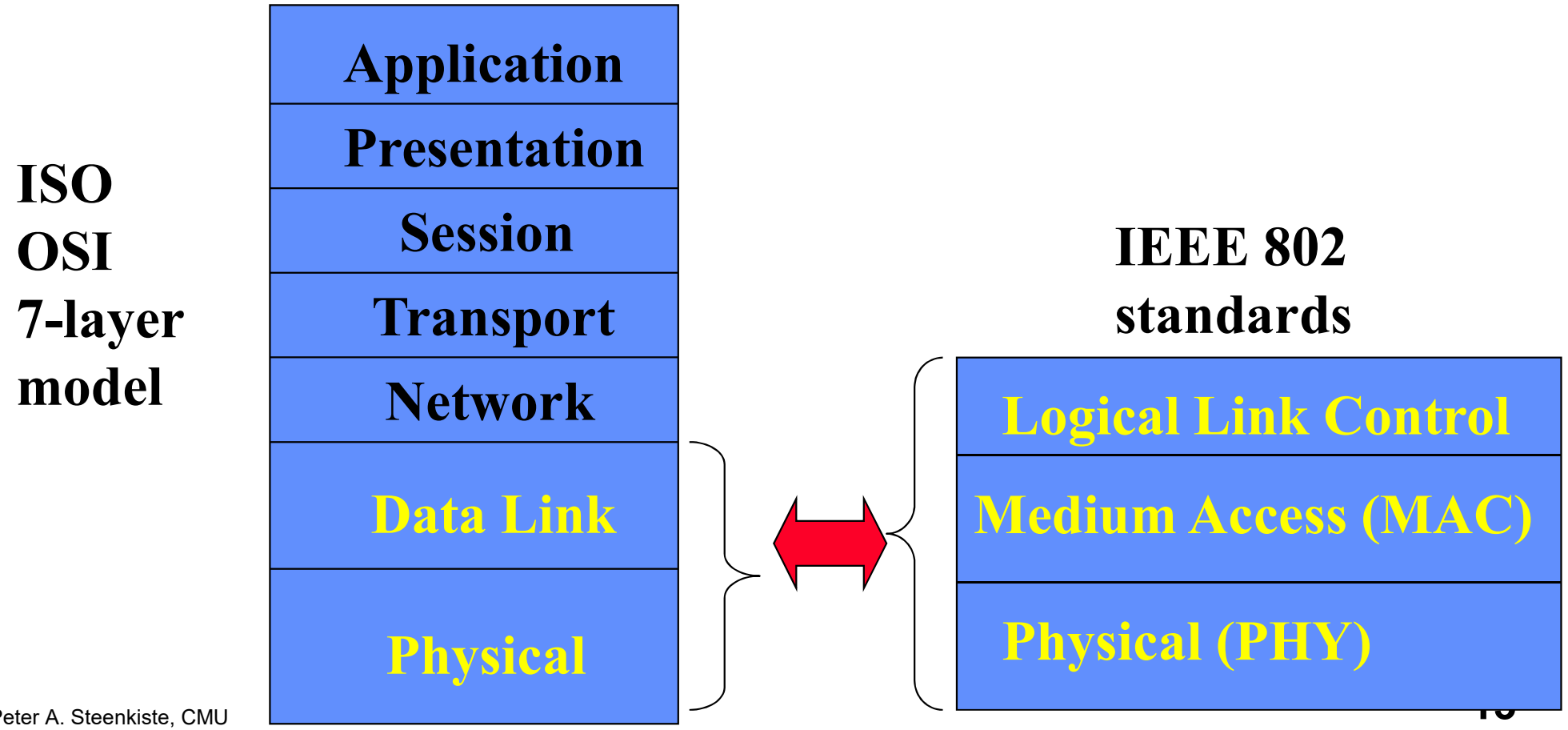
- Data link fundamentals
  - And what changes in wireless
- Ethernet
- Aloha
- Wireless-specific challenges
- 802.11 and 802.15 wireless standards
  - 802 protocol overview
  - Wireless LANs – 802.11
  - Personal Area Networks – 802.15

History

- Aloha wireless data network
- Car phones
  - Big and heavy “portable” phones
  - Limited battery life time
  - But introduced people to “mobile networking”
  - Later turned into truly portable cell phones
- Wireless LANs
  - Originally in the 900 MHz band
  - Later evolved into the 802.11 standard
  - Later joined by the 802.15 and 802.16 standards
- Cellular data networking
  - Data networking over the cell phone
  - Many standards – throughput is the challenge

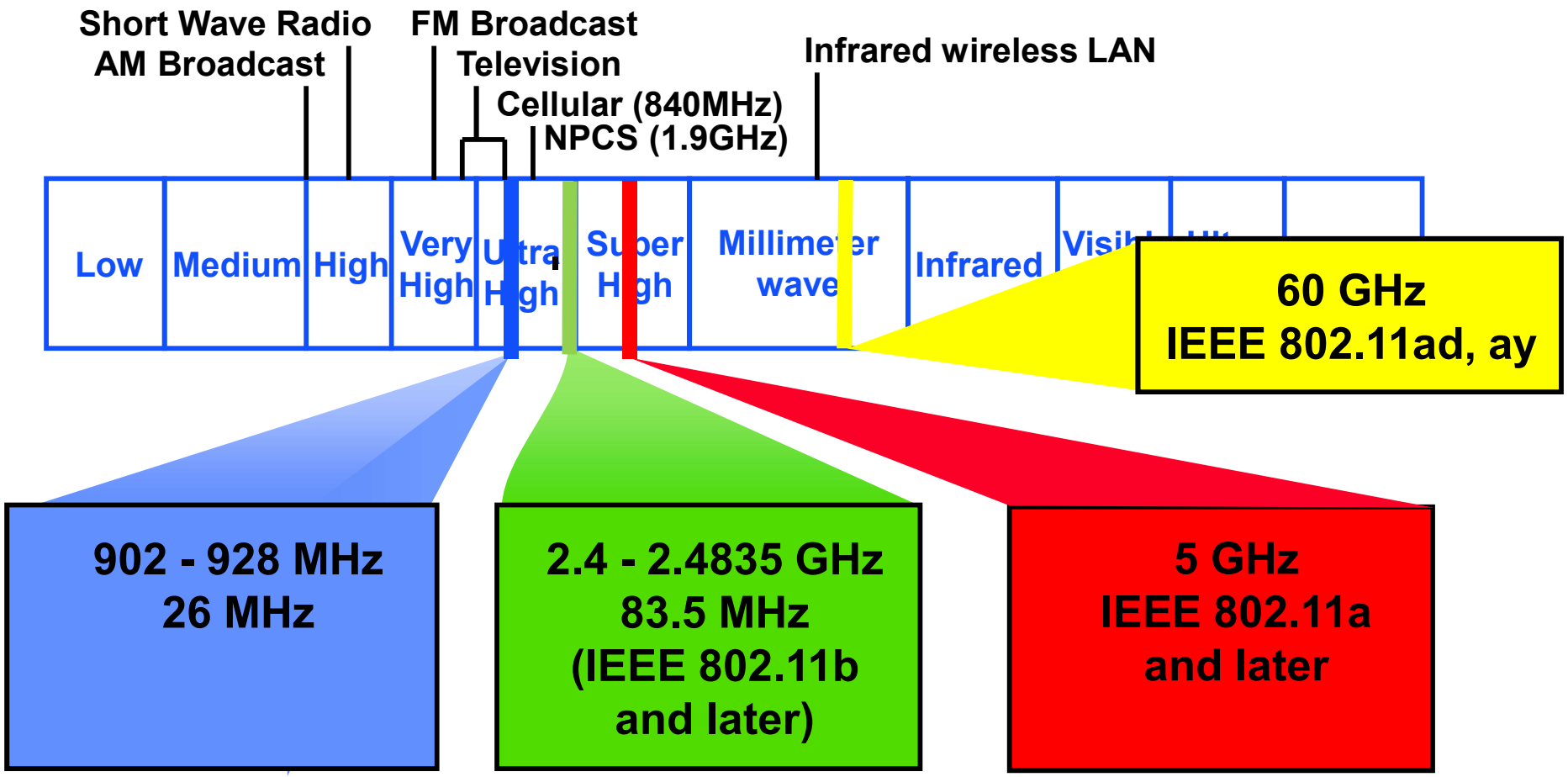
Standardization of Wireless Networks

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



Frequency Bands

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



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	

Outline

- 802 protocol overview
- Wireless LANs – 802.11
  - Overview of 802.11
  - 802.11 MAC, frame format, operations
  - 802.11 management
  - 802.11*
  - Deployment example
- Personal Area Networks – 802.15

IEEE 802.11 Overview

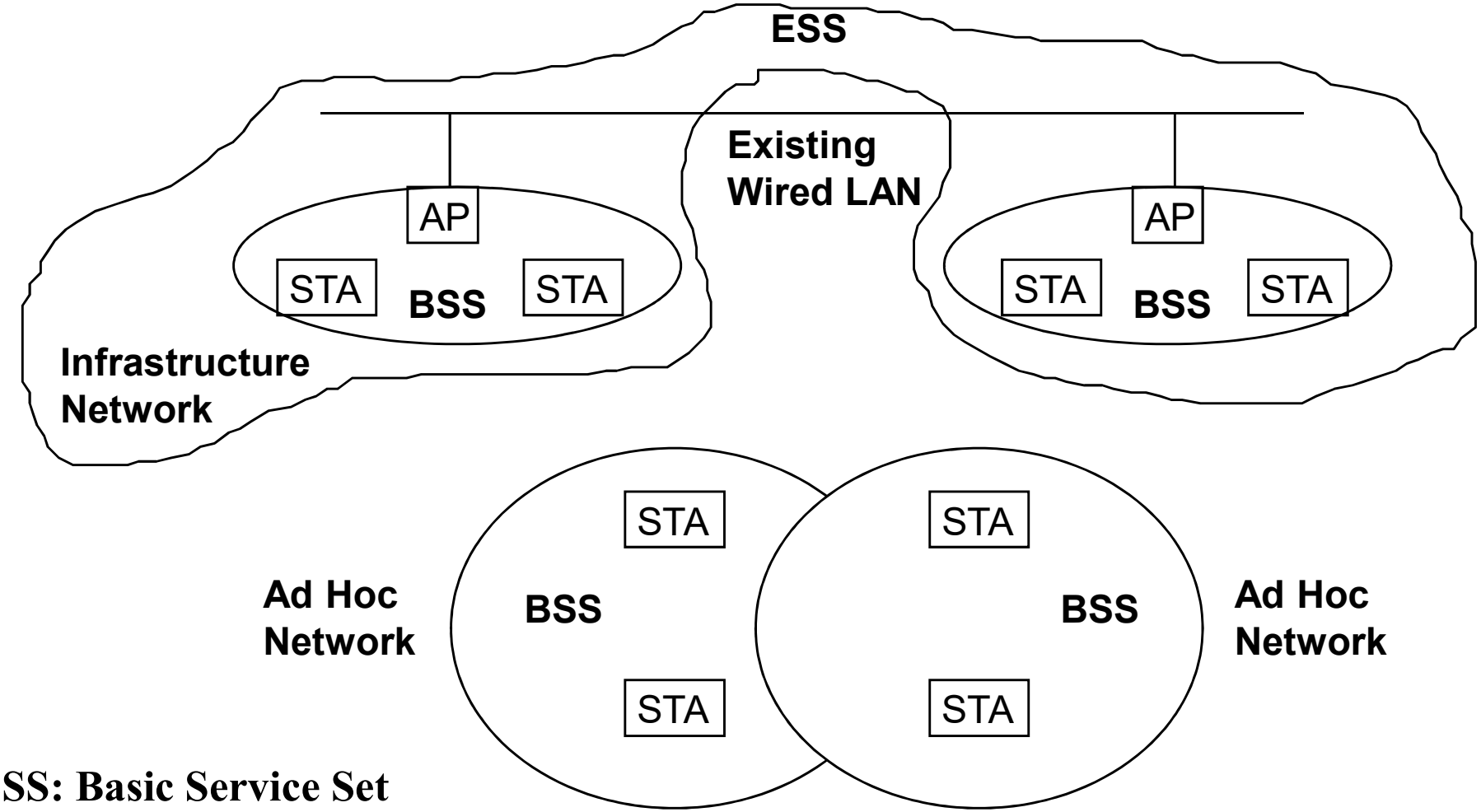
- **Adopted in 1997 with the following goal of providing**
  - » **Access to services in wired networks**
  - » **High throughput**
  - » **Highly reliable data delivery**
  - » **Continuous network connection, e.g. while mobile**
- **The protocol defines**
  - » **MAC sublayer**
  - » **MAC management protocols and services**
  - » **Several physical (PHY) layers: IR, FHSS, DSSS, OFDM**
- **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 each other
  - Thin layer between LLC and MAC sublayers

Outline

- 802 protocol overview
- Wireless LANs – 802.11
  - Overview of 802.11
  - 802.11 MAC, frame format, operations
  - 802.11 management
  - 802.11*
  - Deployment example
- Personal Area Networks – 802.15

How Does WiFi Differ from Wired Ethernet?

- **Signal strength drops off quickly with distance**
  - » **Path loss exponent is highly dependent on context**
- **Should expect higher error rates**
  - » **Solutions?**
- **Makes it impossible to detect collisions**
  - » **Difference between signal strength at sender and receiver is too big**
  - » **Solutions?**
- **Senders cannot reliably detect competing senders resulting in hidden terminal problems**
  - » **Solutions?**

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)
- Collision Avoidance (RTS-CTS)

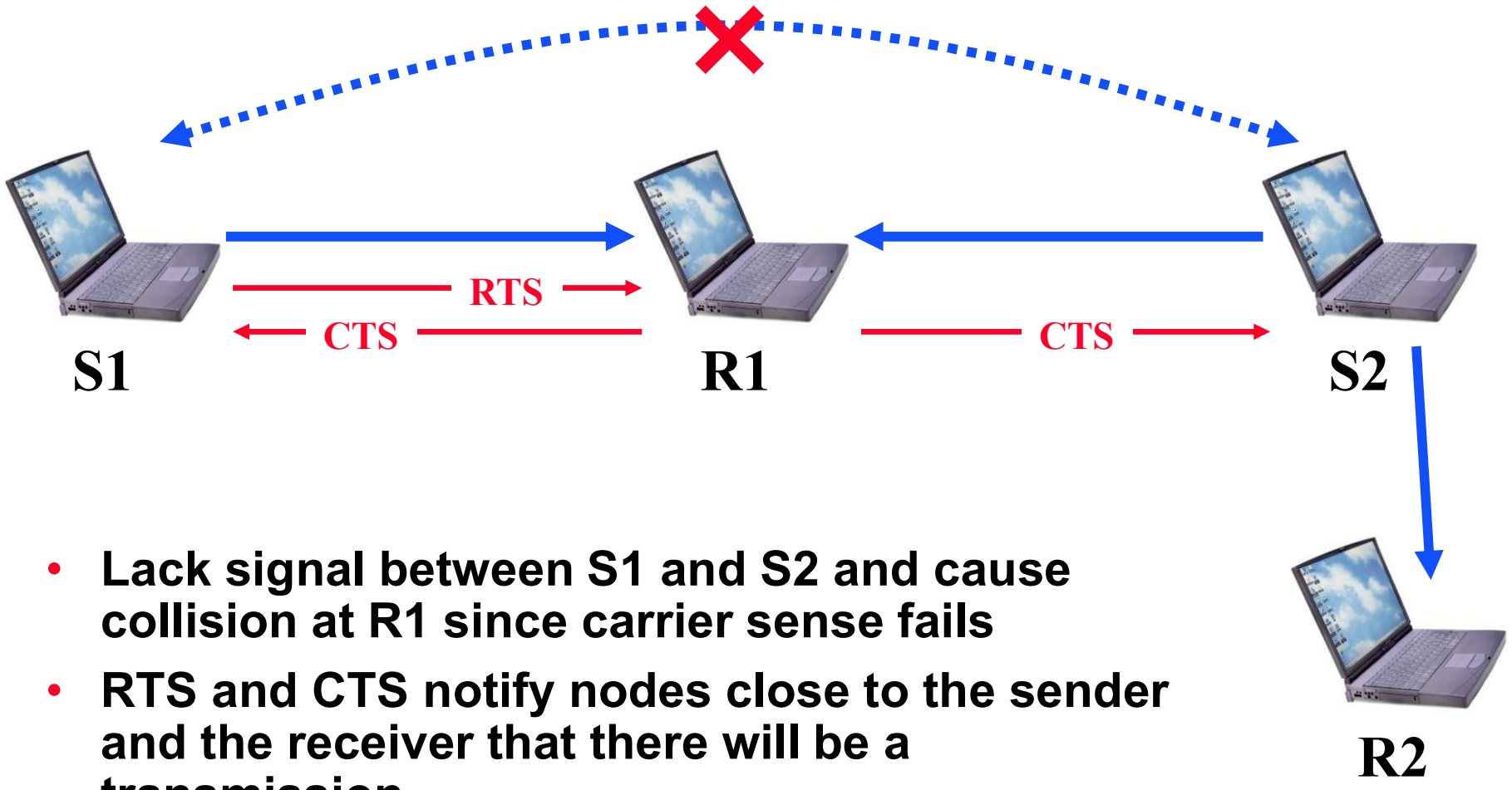
Carrier Sense Multiple Access

- 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 (non-persistent solution)
  - » Want to avoid that several stations waiting to transmit automatically collide
  - » Cost of a collision is high and medium is expected to be busy
- Wait for ack
  - » If there is one, you are done
  - » If there isn't one, assume there was a collision, retransmit using exponential backoff

Why Do Collisions Happen?

- **Near simultaneous transmissions**
  - » **Period of vulnerability: propagation delay**
  - » **Similar to ethernet**
- **Difficult to detect collisions in a radio environment**
  - » **Fading can cause signals from neighboring nodes to be weak, so carrier sense fails**
- **Hidden node situation: two transmitters cannot hear each other causing collisions**
- **Solution has two parts:**
  - » **Collision Avoidance – CSMA/CA**
  - » **Virtual carrier sense**

Collision Avoidance RTS/CTS Protocol



- Lack signal between S1 and S2 and cause collision at R1 since carrier sense fails
- RTS and CTS notify nodes close to the sender and the receiver that there will be a transmission

Request-to-Send and Clear-to-Send

- **Before sending a packet, first send a station first sends a RTS**
  - » **Collisions can still occur but chance is relatively small since RTS packets are short**
  - » **Headers contain information on transmission length**
- **The receiving station responds with a CTS**
  - » **Tells the sender that it is ok to proceed**
- **RTS and CTS use shorter IFS to guarantee access (more later)**
  - » **Effectively priority over data packets**
- **First introduced in the Multiple Access with Collision Avoidance (MACA) protocol**
  - » **Fixed problems observed in Aloha**

Virtual Carrier Sense

- The header of RTS and CTS header contains a Duration ID that indicates the duration of the entire transmission (data + control packets)
  - » The same information is also stored in all data packet headers – redundant to increase chances of receiving it
- Stations that hear the header of any packet "remember" how long the medium will be busy
  - » Based on a Duration ID in the packet headers
  - » Note that they may not be able to hear the entire packet!
- Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)
  - » Time that must elapse before a station can use channel
  - » The medium is busy even if node cannot sense a signal

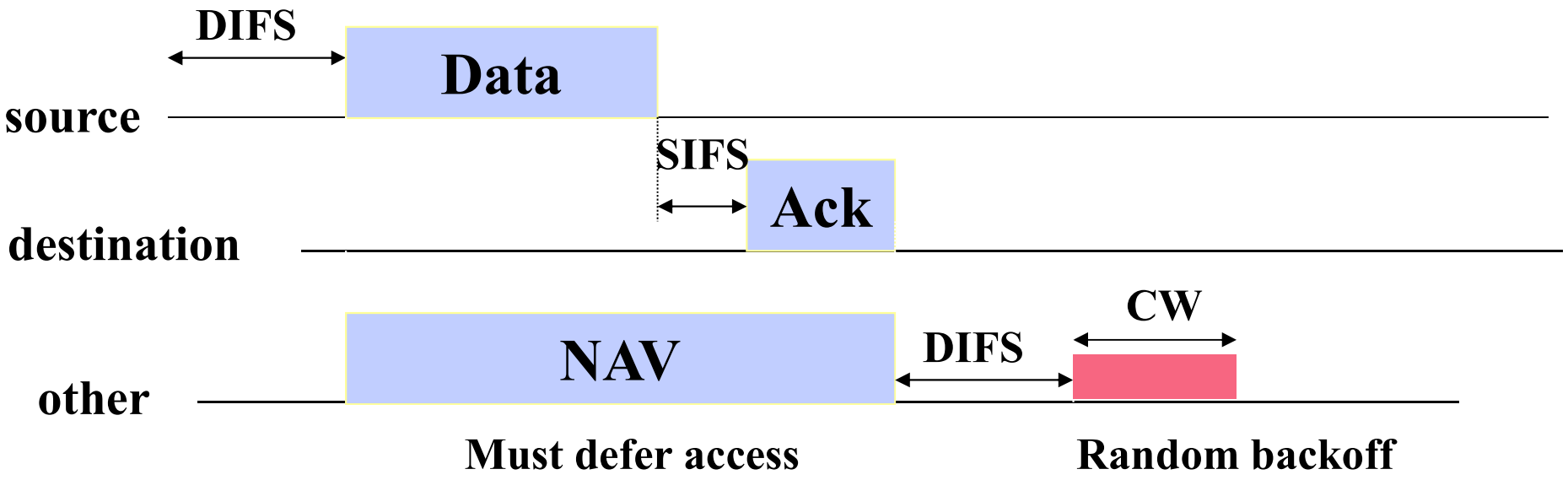
No Collision Detection

- Any received signal is effectively noise during a transmission so it cannot be detected
  - » Received signals are very weak
- In Ethernet all nodes can detect a collision and they abort the transmission right away
  - » Cost of a collision (in lost transmission time) is low
- In wireless all transmission are completed – even transmissions corrupted by a collision
  - » Lack of an ACK signals that the packet was lost
- The cost of collision is high!

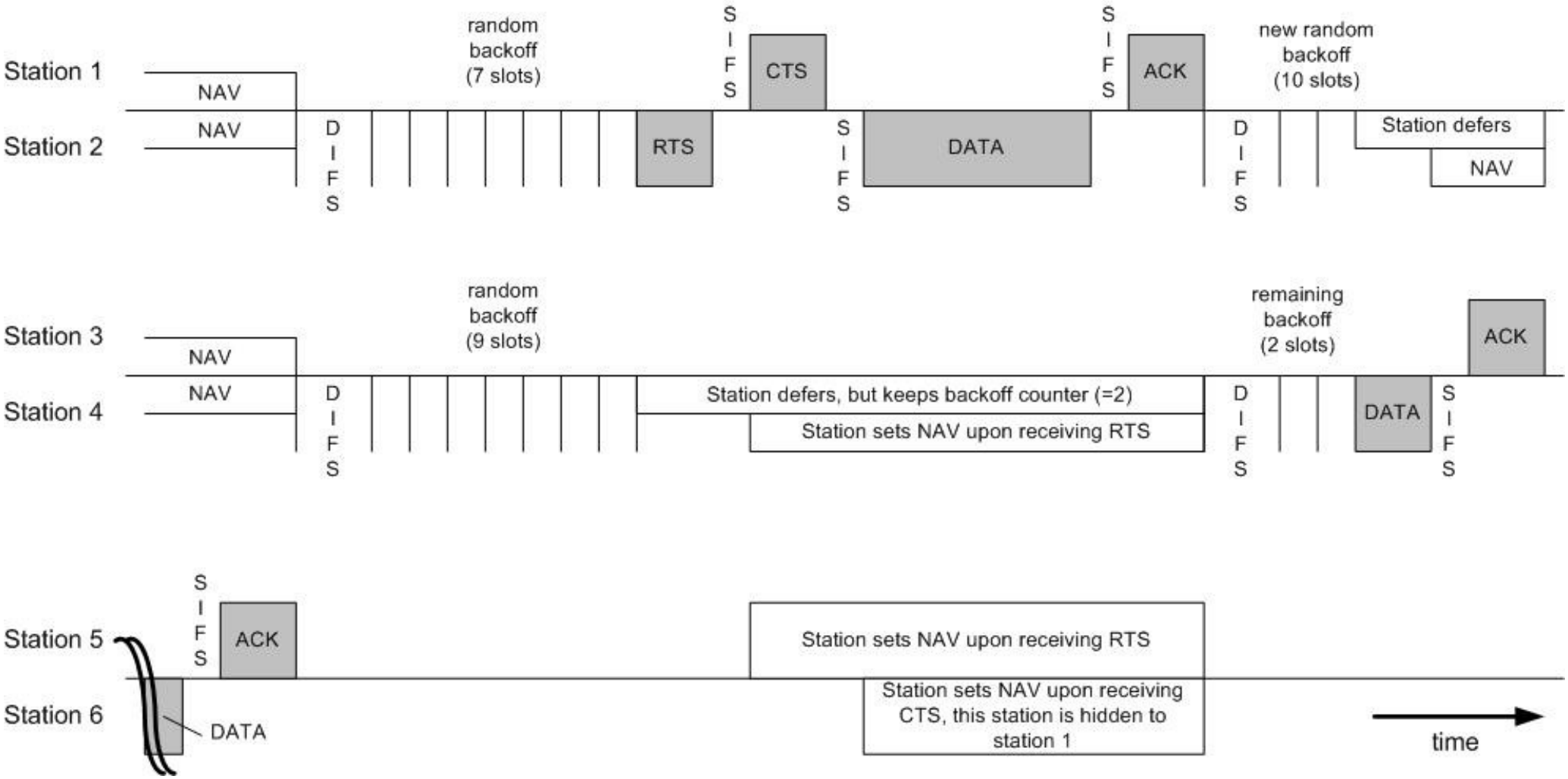
Exponential Backoff

- **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, ...**

DCF mode transmission without RTS/CTS



Use of RTS/CTS



Some More MAC Features

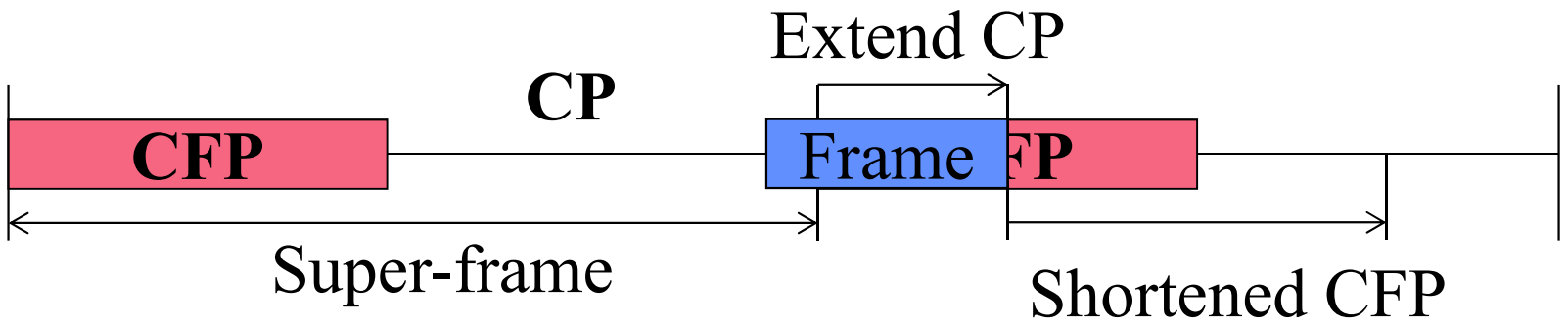
- **Use of RTS/CTS is controlled by an RTS threshold**
  - » RTS/CTS is only used for data packets longer than the RTS threshold
  - » Pointless to use RTS/CTS for short data packets – high overhead!
- **Number of retries is limited by a Retry Counter**
  - » Short retry counter: for packets shorter 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

Summary 802.11 MAC Protocol Features

- Supports MAC functionality
  - » IEEE addressing
  - » CSMA/CA
- Error detection (checksum)
- Error correction (ACK frame)
- Flow control: stop-and-wait
- Fragmentation (More Frag)
- Collision Avoidance (RTS-CTS)

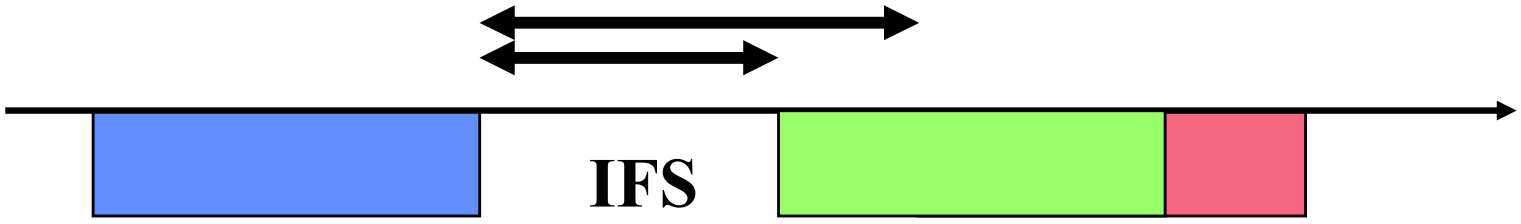
Now What about PCF?

- **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**

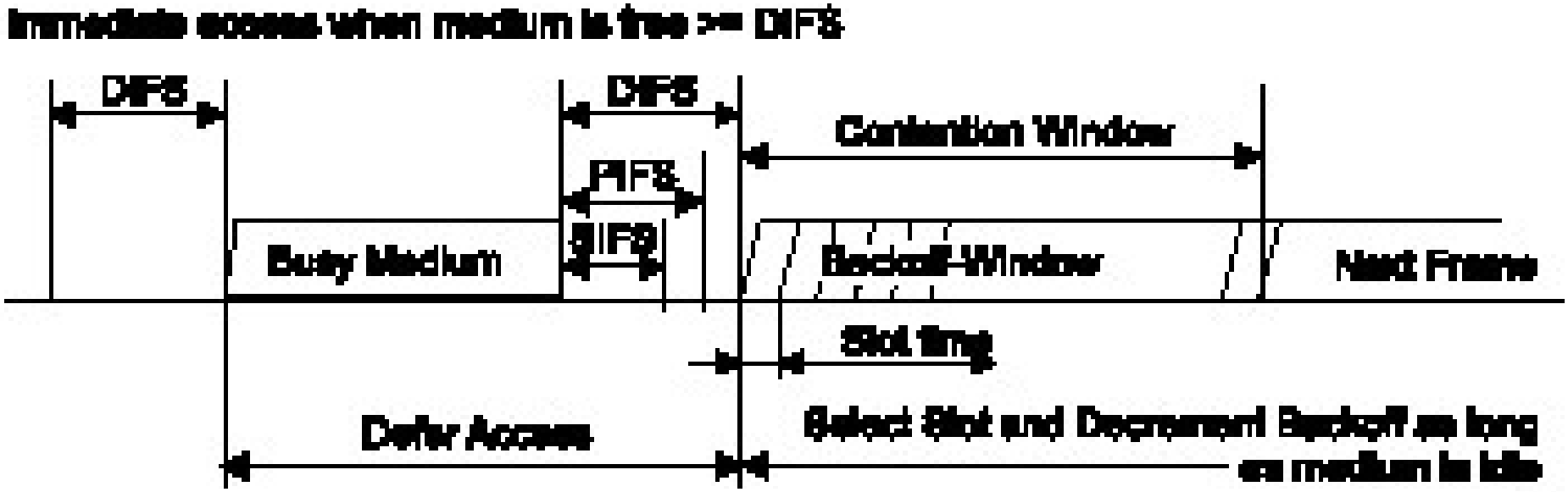


Playing Games with Inter Frame Spacing

- 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



- 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

Summary WiFi

- Supports infrastructure and ad hoc mode
- Uses ACKs to detect collisions
- Uses RTS-CTS to avoid hidden terminals
  - » Adds virtual carrier sense to physical carrier sense
  - » Almost never used because of overhead
- Supports a point control function in addition to distributed control
  - » Supports scheduled access in addition to random access
  - » Almost never used because of overhead