18-759: Wireless Networks
Lecture 9: 802.11 MAC

Peter Steenkiste
Departments of Computer Science and Electrical and Computer Engineering

Spring Semester 2010
http://www.cs.cmu.edu/~prs/wirelessS10/

Announcements

- Projects …
- Surveys …
- Midterm …

Outline

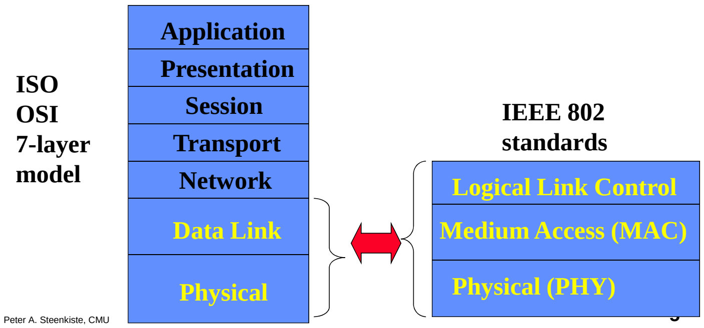
- 802 protocol overview
- Wireless LANs – 802.11
- Personal Area Networks – 802.15
- Midterm
- Cellular networks
- Wireless Access – 802.16

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

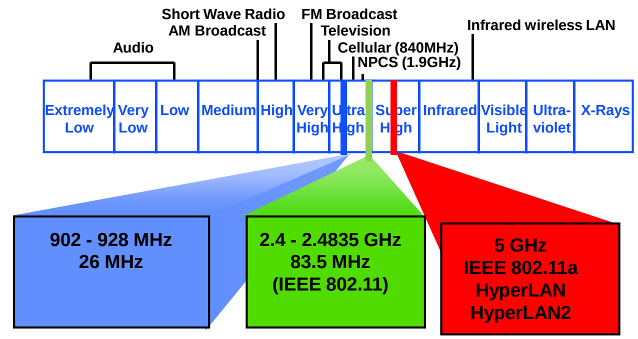
Standardization of Wireless Networks

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



Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth



The 802 Class of Standards

- List on next slide
- 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- Some standards are for technologies that are outdated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
  - » E.g. 802.6

- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
  - » 802.3a Contention Bus Standard 10base 2 (Thin Net)
  - » 802.3b Broadband Contention Bus Standard 10broad 36
  - » 802.3d Fiber-Optic InterRepeater Link (FOIRL)
  - » 802.3e Contention Bus Standard 1 base 5 (Starlan)
  - » 802.3i Twisted-Pair Standard 10base T
  - » 802.3j Contention Bus Standard for Fiber Optics 10base F
  - » 802.3u 100-Mb/s Contention Bus Standard 100base T
  - » 802.3x Full-Duplex Ethernet
  - » 802.3z Gigabit Ethernet
  - » 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
  - » 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
  - » 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard

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
- Cellular technologies
- Wireless Access – 802.16

IEEE 802.11 Overview

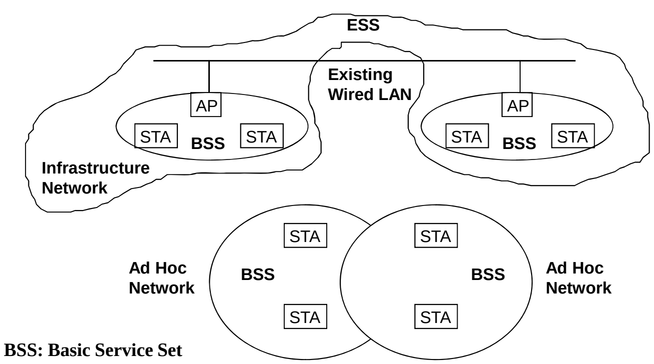
- Adopted in 1997 with goal of providing
  - » Access to services in wired networks
  - » High throughput
  - » Highly reliable data delivery
  - » Continuous network connection, e.g. while mobile
- The protocol defines
  - » MAC sublayer
  - » MAC management protocols and services
  - » Several physical (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!

Our Focus

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

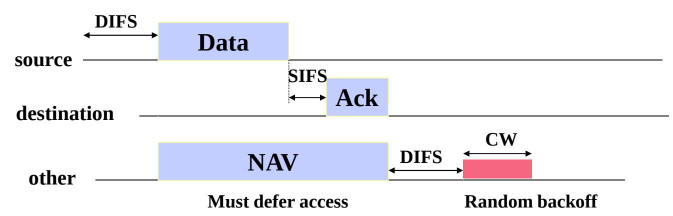
Features of 802.11 MAC protocol

- 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 back off is high and expect a lot of contention
- 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

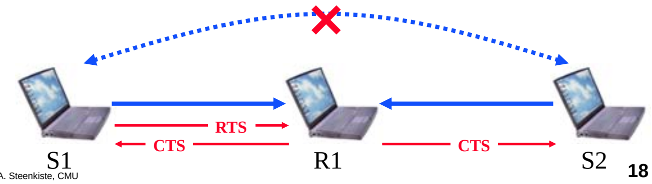


Exponential Backoff

- 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



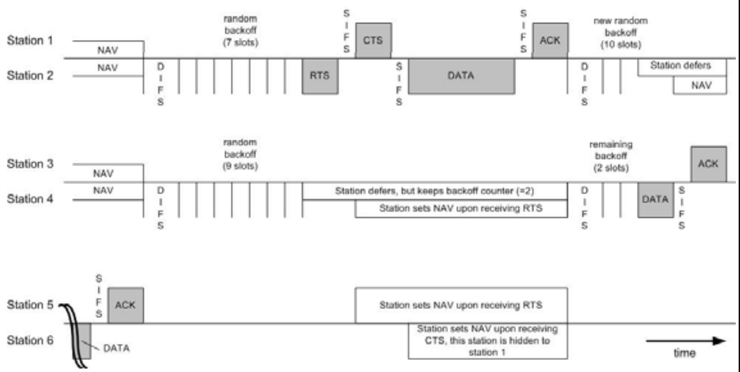
Request-to-Send and Clear-to-Send

- Before sending a packet, first send a station first sends a RTS
  - » Collisions can still occur but chance is relatively small since RTS packets are short
- 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
  - » Effectively priority over data packets
- First introduced in the Multiple Access with Collision Avoidance (MACA) protocol
  - » Fixed problems observed in Aloha

Virtual Carrier Sense

- RTS and CTS notify nodes within range of sender and receiver of upcoming transmission
- 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
  - » Note that they may not be able to hear the data packet!
- Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)
  - » Time that must elapse before a station can sample channel for idle status
  - » Consider the medium to be busy even if it cannot sense a signal

Use of RTS/CTS

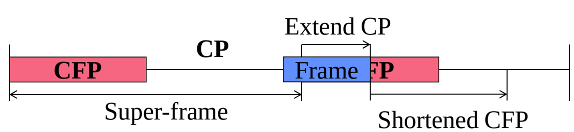


Some More MAC Features

- 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

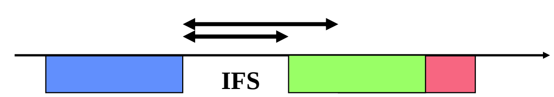
Now What about PCF?

- 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

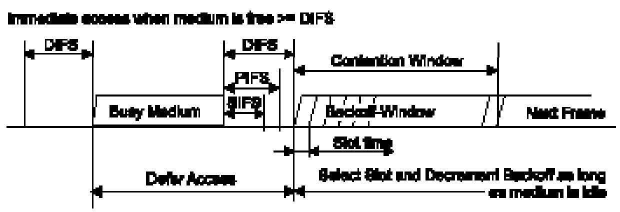


Playing Games with Inter Frame Spacing

- 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



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

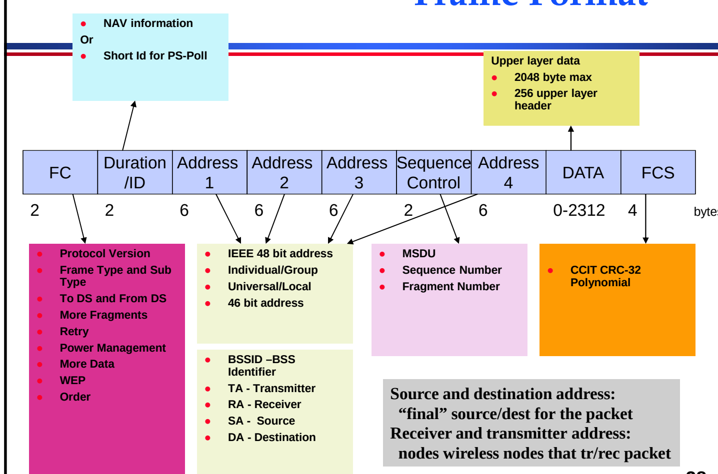
PCF Operation Overview

- 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

MAC header

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Seq. control	Address 4	Frame body	FCS

	Protocol version	Type	Sub-type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
bits	2	2	4	1	1	1	1	1	1	1	1

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

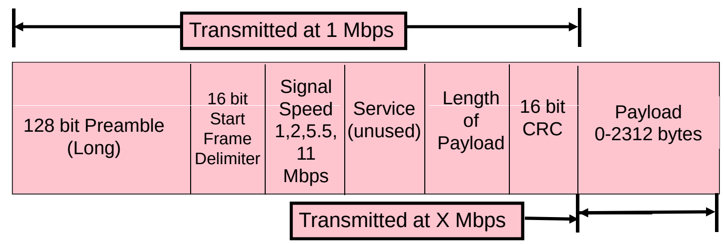
Multi-bit Rate

- 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
  - » Still a research topic!
  - » More later in the semester
- Packets have multi-rate format
  - » Different parts of the packet are sent at different rates
  - » Why?

Long Preamble

Long Preamble = 144 bits

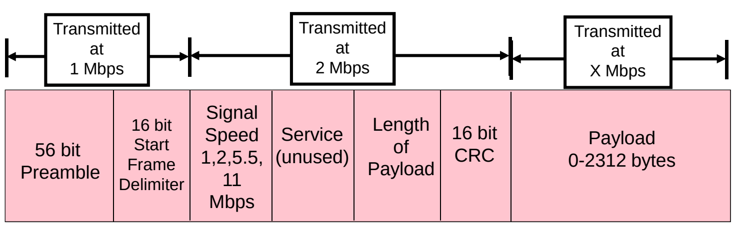
- Interoperable with older 802.11 devices
- Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*



Short Preamble

Short Preamble = 72 bits

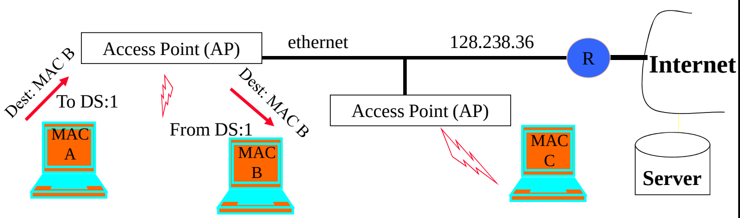
- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble



Data Flow Examples

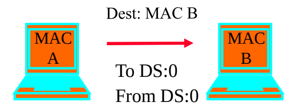
- Case 1: Packet from a station under one AP to another in same AP’s coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station

Case 1: Communication Inside BSS



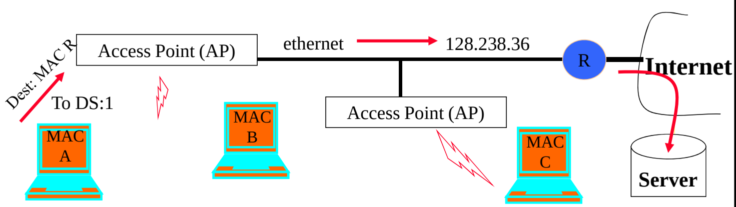
- AP knows which stations are registered with it so it knows when it can send frame directly to the destination

Case 2: Ad Hoc



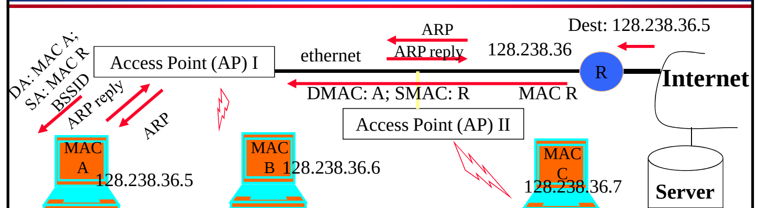
- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- Note: in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B

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?