An Introduction to 802.11

Bhaskaran Raman

Department of CSE, IIT Kanpur

Reference: IEEE specifications on 802.11
http://grouper.ieee.org/groups/802/11/

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005
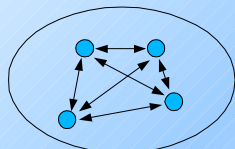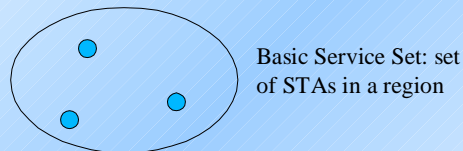
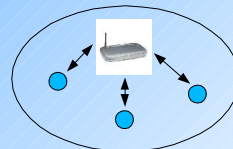# 802.11: What does it Specify?

- PHY sub-layer
  - 802.11a, 802.11b, 802.11g
- MAC sub-layer
  - Independent of the PHY
  - DCF (Distributed Coodrination Function)
    - CSMA/CA
  - PCF (Point Coordination Function)
- MAC management

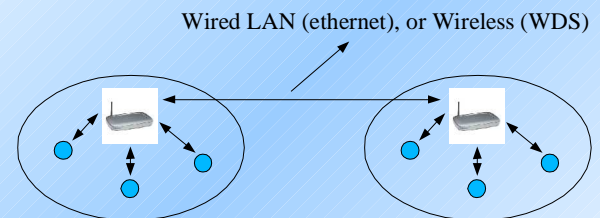Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

802.11 Service Sets

Basic Service Set: set of STAs in a region

IBSS: Independent Basic Service Set

Infrastructure Basic Service Set

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

802.11 Extended Service Set (ESS)

Wired LAN (ethernet), or Wireless (WDS)

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005
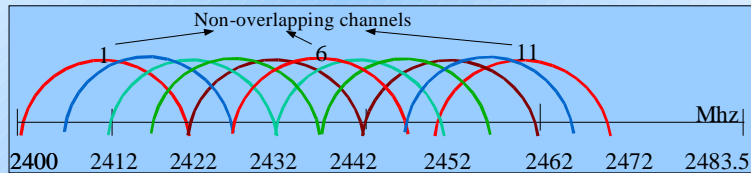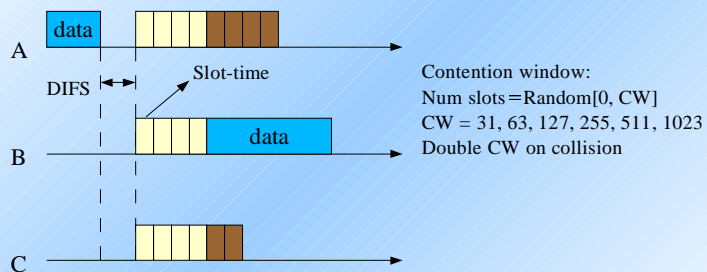
802.11 PHY

- DSSS (Direct Sequence Spread Spectrum)
  - Use 11-bit Barker code to spread the signal over a wide-band (22MHz)
  - Avoid narrow-band interference
- 802.11b uses DSSS, in 2400-2483.5MHz

Non-overlapping channels

1   6   11

Mhz

2400   2412   2422   2432   2442   2452   2462   2472   2483.5

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005
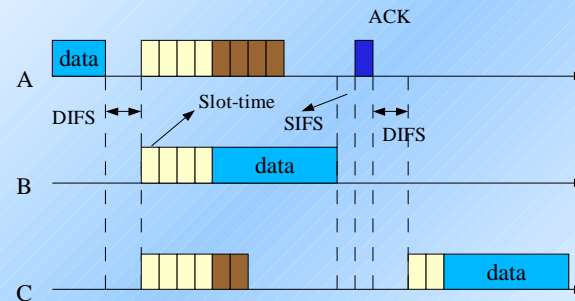
The MAC Protocol: CSMA/CA

- CSMA/CD:
  - Listen before transmit
  - Backoff on collision detection
- Wireless:
  - Cannot listen while transmitting
  - Collision detection is impossible
- CSMA/CA:
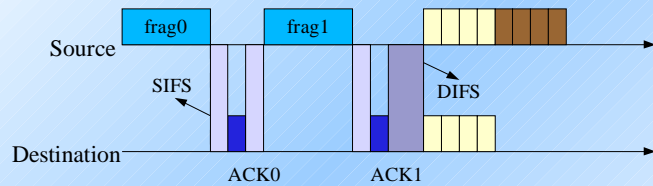 - Collision avoidance: backoff + priority-ACK

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

The Backoff Procedure

A
data

DIFS   Slot-time

B
data

C

Contention window:
Num slots = Random[0, CW]
CW = 31, 63, 127, 255, 511, 1023
Double CW on collision

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

CSMA/CA + ACK

ACK

A
data

DIFS   Slot-time   SIFS   DIFS

B
data

C
data

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

Transmission of Fragments

Source

frag0   frag1

SIFS   DIFS

Destination

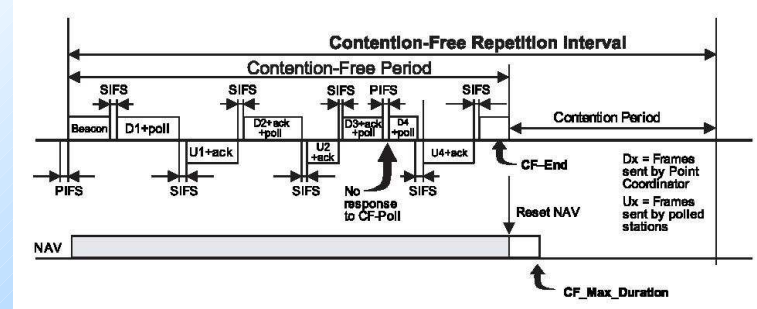ACK0   ACK1

SIFS, PIFS, and DIFS

Source: IEEE 802.11 Specification

IFS Relations

aSIFSTime and aSlotTime are fixed per PHY.

aSIFSTime is: aRxRFDelay + aRxPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime.

aSlotTime is: aCCATime + aRxTxTurnaroundTime + aAirPropagationTime
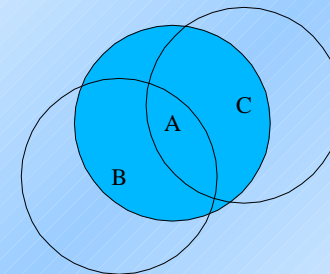   + aMACProcessingDelay.

The PIFS and DIFS are derived by the following equations, as illustrated in Figure 58.

PIFS = aSIFSTime + aSlotTime

DIFS = aSIFSTime + 2 × aSlotTime

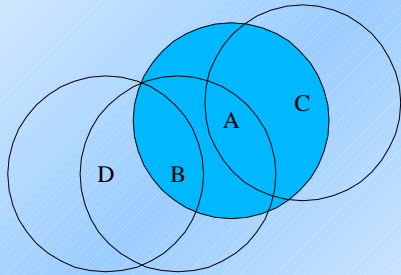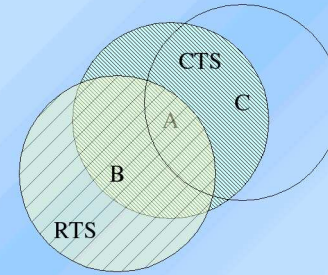Source: IEEE 802.11 Specification

The Hidden Node Problem

Medium is free DOES NOT IMPLY ok-to-transmit
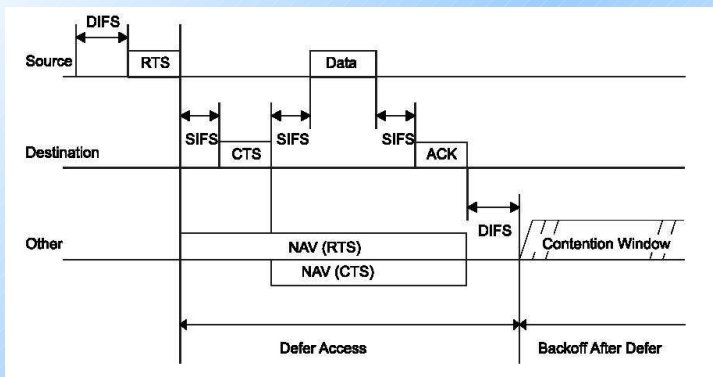
The Exposed Node Problem

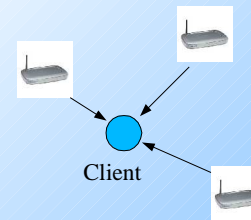Medium is busy DOES NOT IMPLY not-ok-to-transmit

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

Hidden Node Solution: RTS/CTS

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

RTS/CTS Exchange Example

Source: IEEE 802.11 Specification

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

Beacons and Probes

Client

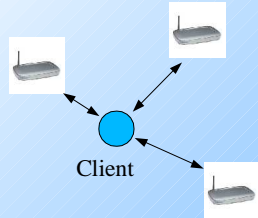Beacon has: AP capabilities, beacon period, SSID, Traffic Indication Map (TIM)

- A client may be in the coverage area of many APs
- APs send periodic beacons
- Client may passively scan these
- Or, probe-response for active scanning

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005
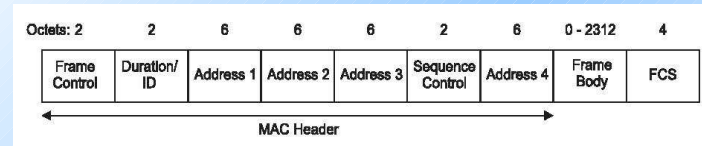
Authentication and Association

Client
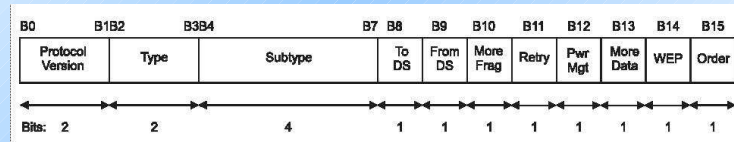
- A client has to
  - Authenticate itself to an AP
  - Then Associate itself
- A client may authenticate itself to many APs to speed-up roaming

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

802.11 Frame Format

Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Source: IEEE 802.11 Specification

B0	B1B2	B3B4		B7 B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

| Bits: 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Source: IEEE 802.11 Specification

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

Throughput estimation in 802.11

- PLCP preamble + header: 24 bytes
- RTS: 20 bytes, CTS: 14 bytes
- MAC header: 28 or 34 bytes
- IP header: 20 bytes
- TCP header: 20 bytes
- UDP header: 8 bytes
- Bottomline: too much per-packet overhead!

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005

802.11 WEP

- 40 bit or 128 bit shared encryption mechanism
- Has been broken
- 802.11i is the new security standard

Fundamentals of Wired and Wireless Networks, Kameswari Chebrolu and Bhaskaran Raman, 09-13 May 2005