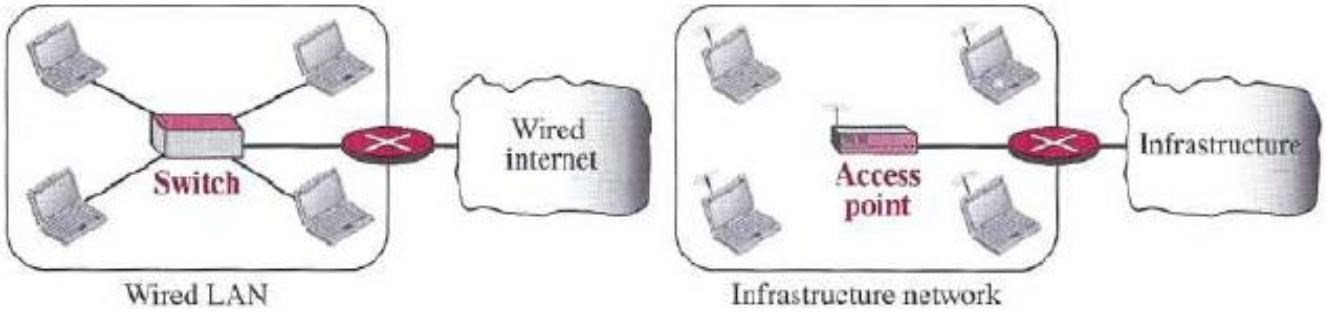
CS343: Data Communication

Wireless LAN

by
Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Guwahati
E-mail: manaskhatua@iitg.ac.in

Wireless LAN



- Wireless LAN satisfies requirements for
  - mobility,
  - relocation,
  - ad hoc networking,
  - coverage of locations difficult to wire.

- Influential Characteristics
  - Attenuation
  - Error
  - Interference
  - Multipath Propagation

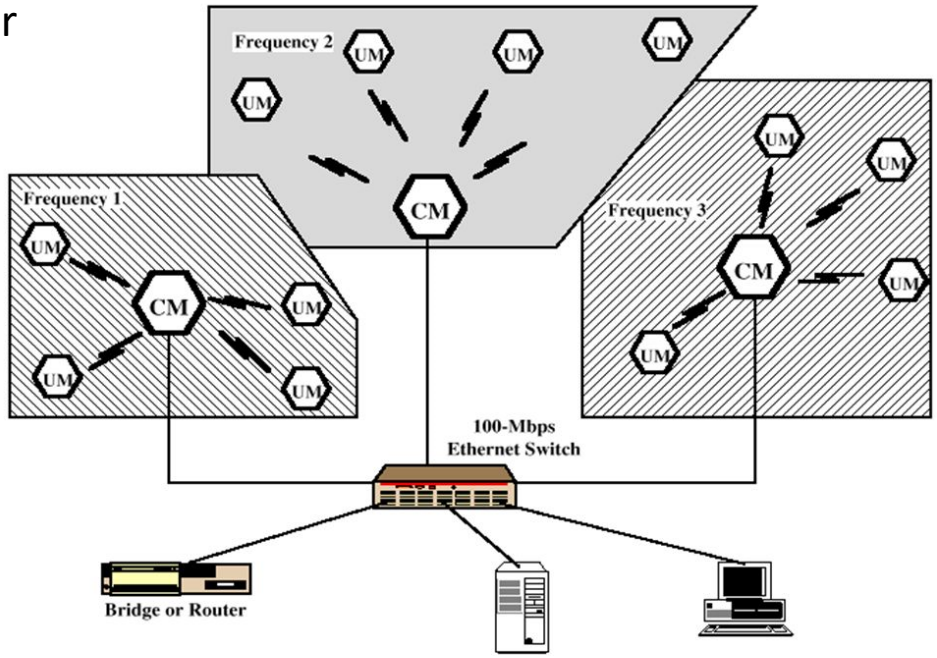
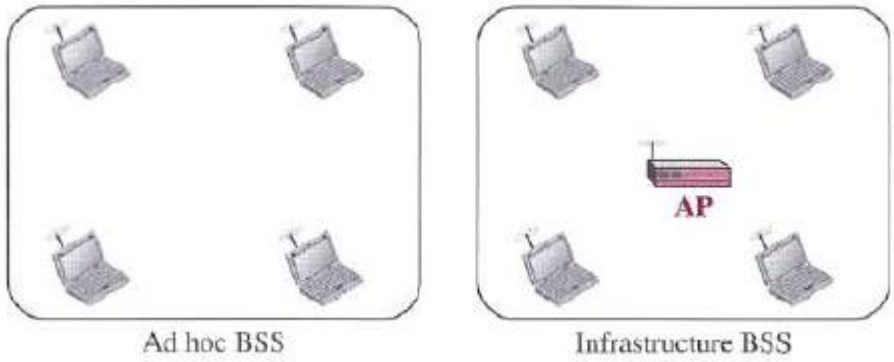


Figure 13.2 Example Multiple-Cell Wireless LAN Configuration

WLAN Configuration

- Configuration:
  - Ad hoc mode
  - Infrastructure mode
- Basic Architecture:
  - BSS (Basic Service Set)
  - ESS (Extended Service Set)



- Important requirements for WLANs:
  - Throughput
  - Number of nodes
  - Connection to backbone LAN
  - Service area
  - Battery power consumption
  - Transmission robustness and security
  - Collocated network operation
  - License-free operation
  - Handoff/roaming
  - Dynamic configuration

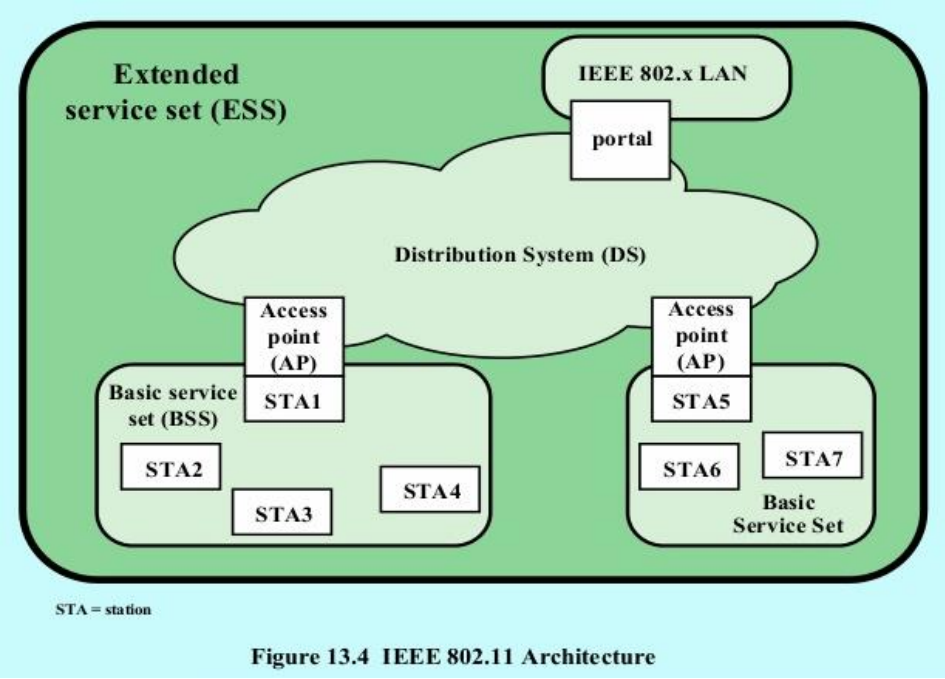


Figure 13.4 IEEE 802.11 Architecture

IEEE 802.11 Services

- Institute of Electrical and Electronics Engineers (IEEE) defines standard for Wireless LANs (802.11)
- IEEE 802.11 defines a number of services that need to be provided by the WLAN

- Three of the services are used to control IEEE 802.11 LAN access and confidentiality.
- Six of the services are used to support delivery of MAC service data units (MSDUs) between stations.

- The MSDU is a block of data passed down from the MAC user to the MAC layer; typically this is a LLC PDU.

Service	Provider	Used to Support
Association	Distribution system	MSDU delivery
Disassociation	Distribution system	MSDU delivery
Reassociation	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Integration	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security

IEEE 802.11 Medium Access Control

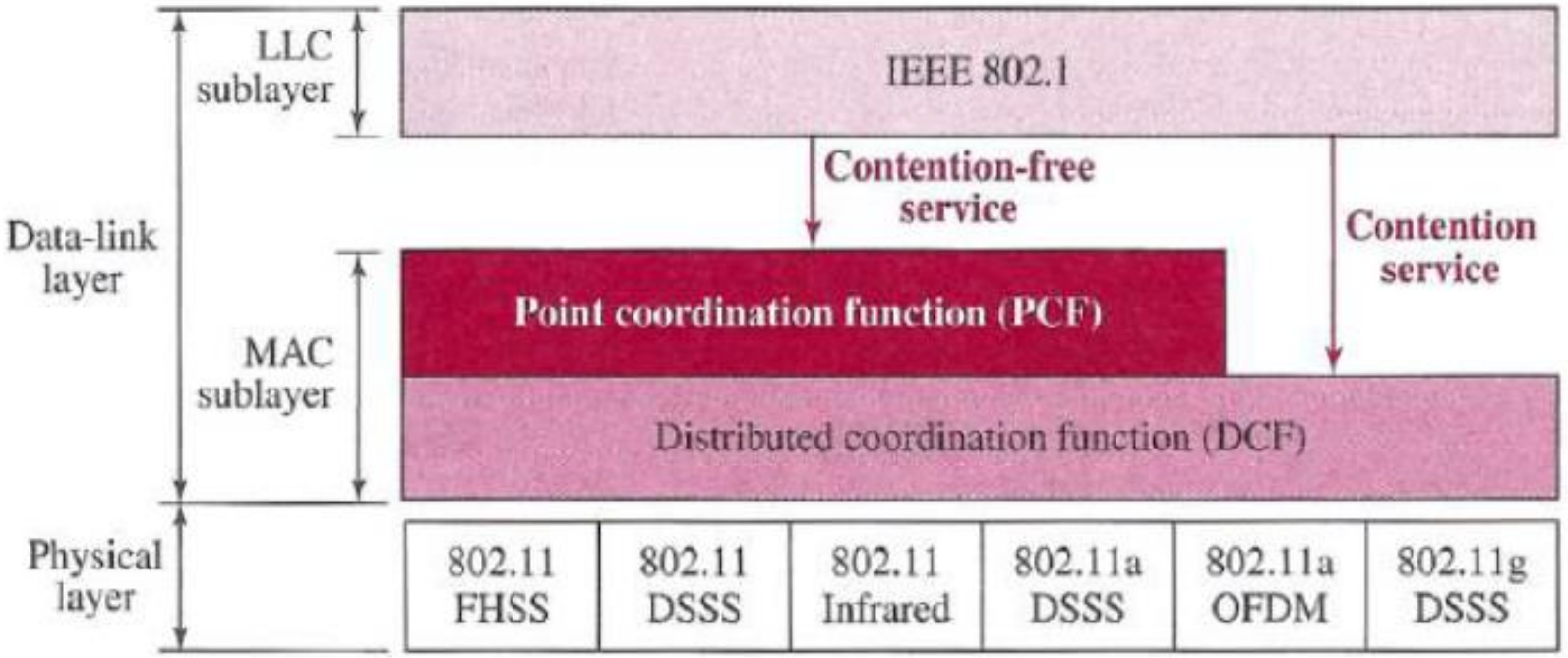
- The IEEE 802.11 MAC layer covers three functional areas
  - reliable data delivery,
  - access control,
  - security.

- Reliable Data Delivery:
  - This situation can be dealt with by reliability mechanisms at a higher layer, such as TCP.
  - However, wireless medium is subject to considerable unreliability.
  - It is therefore more efficient to deal with errors at the MAC level
  - Solution: ACK and re-transmission after timeout

- Security:
  - User authentication
  - Data Privacy
  - Solution: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)

Cont…

- Access Control:



- The DCF sublayer makes use of a simple CSMA/CA (carrier sense multiple access with collision avoidance) algorithm

CSMA/CA (Collision Avoidance)

- CSMA/CD is not useful in wireless networks
- So, CSMA/CA was invented

- Why??
  - In wireless, send power (generally around 100mw) and receive sensitivity (commonly around 0.01 to 0.0001mw)
  - The sending would cover up any possible chance of receiving a foreign signal, no chance of "Collision Detection“
  - So, wireless transceivers can't send and receive on the same channel at the same time

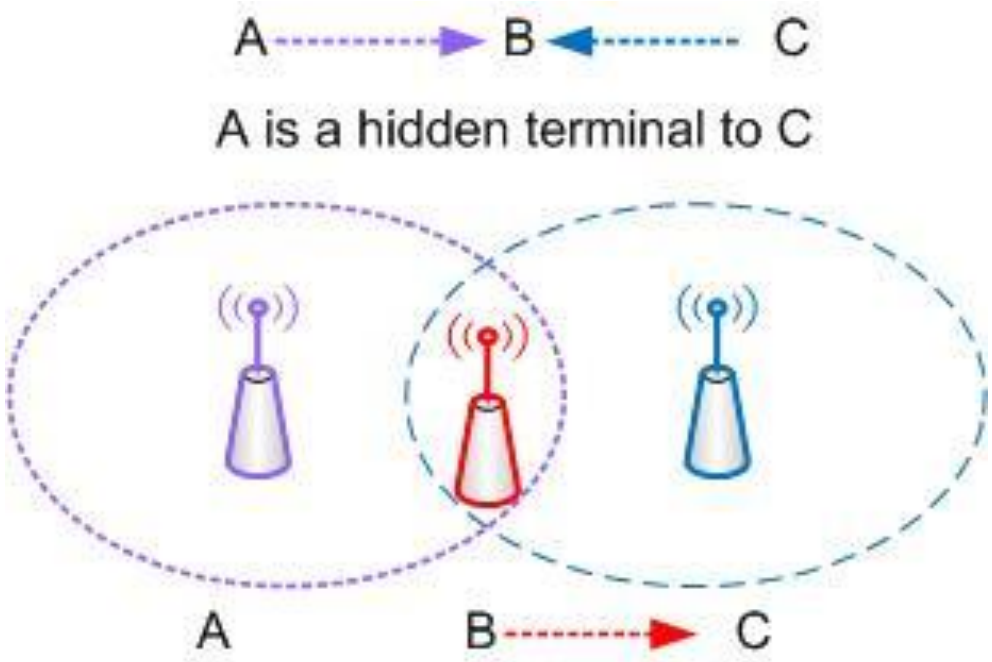
  - But, in wired networks (like Ethernet) the voltage is around 1 to 2.5v; sending and receiving are roughly same voltage
  - Let, sending a 2.5v signal, and someone else collides with a 2.5v signal;
  - So, receive signal would be around 5v.

Cont…

- Common features:
  - Channel sensing
  - Retransmission
  - Backoff

- Important modifications / inclusions in DCF:
  - Inter-Frame Space (IFS): it is used instead of persistent methods
  - Contention window (CW) and Binary exponential backoff (BEB) : time is treated in slots; randomness is itroduced
  - Acknowledgement (ACK) / Timeout : no collision detection; achieve reliability
  - Basic / RTS-CTS mode of transmission: to avoid hidden terminal problem
  - Use of Network Allocation Vector (NAV): to defer transmission instead of one slot or backoff slot

HT/ET Problem



Inter-frame Space

- Slot time: basic unit of MAC algorithm
  = Time required for station to sense end of frame, start transmitting, and beginning of frame to propagate to others

- SIFS (Short Inter-Frame Space)
  = Time required for station to sense end of frame and start transmitting
  = By that time the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet

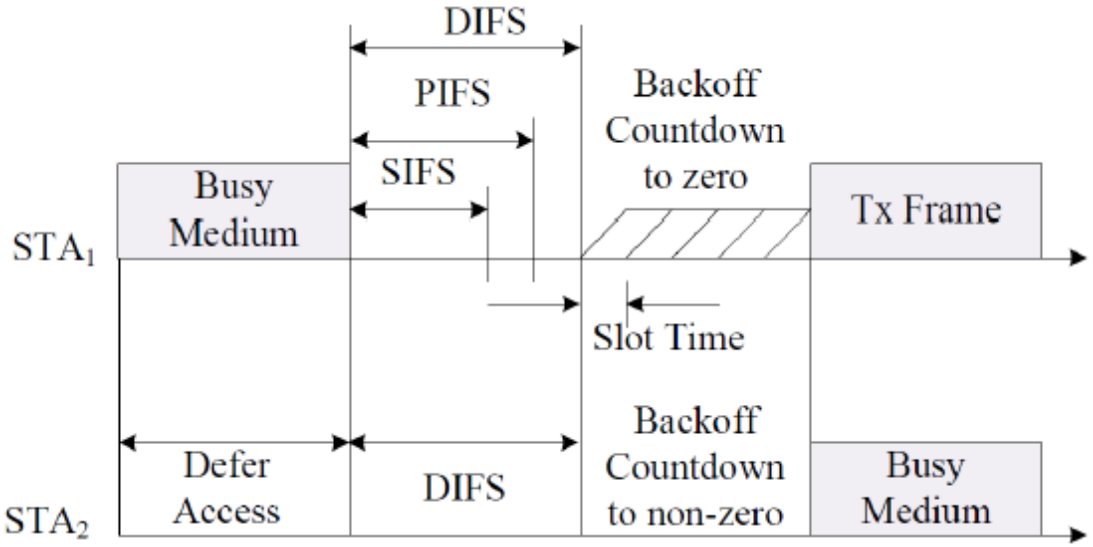
- DIFS (DCF Inter-Frame Space)
  = SIFS + 2 *Slot time

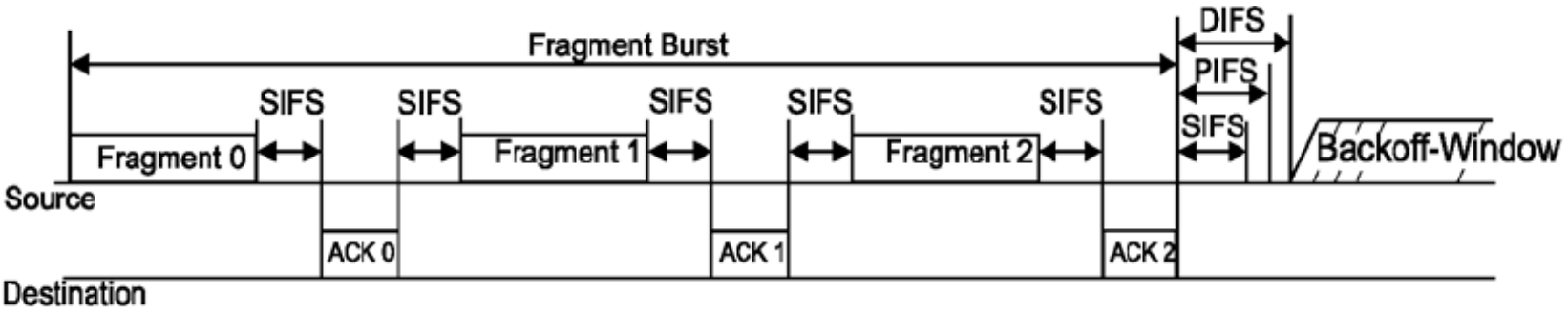
- PIFS (PCF Inter-Frame Space)
  = SIFS + Slot time

- AIFS (Arbitration Inter-Frame Space)

Standard	Slot time (µs)	DIFS (µs)
IEEE 802.11-1997 (FHSS)	50	128
IEEE 802.11-1997 (DSSS)	20	50
IEEE 802.11b	20	50
IEEE 802.11a	9	34
IEEE 802.11g	9 or 20	28 or 50
IEEE 802.11n (2.4 GHz)	9 or 20	28 or 50
IEEE 802.11n (5 GHz)	9	34
IEEE 802.11ac (5 GHz)	9	34

DCF (in basic access mode)





Cont…

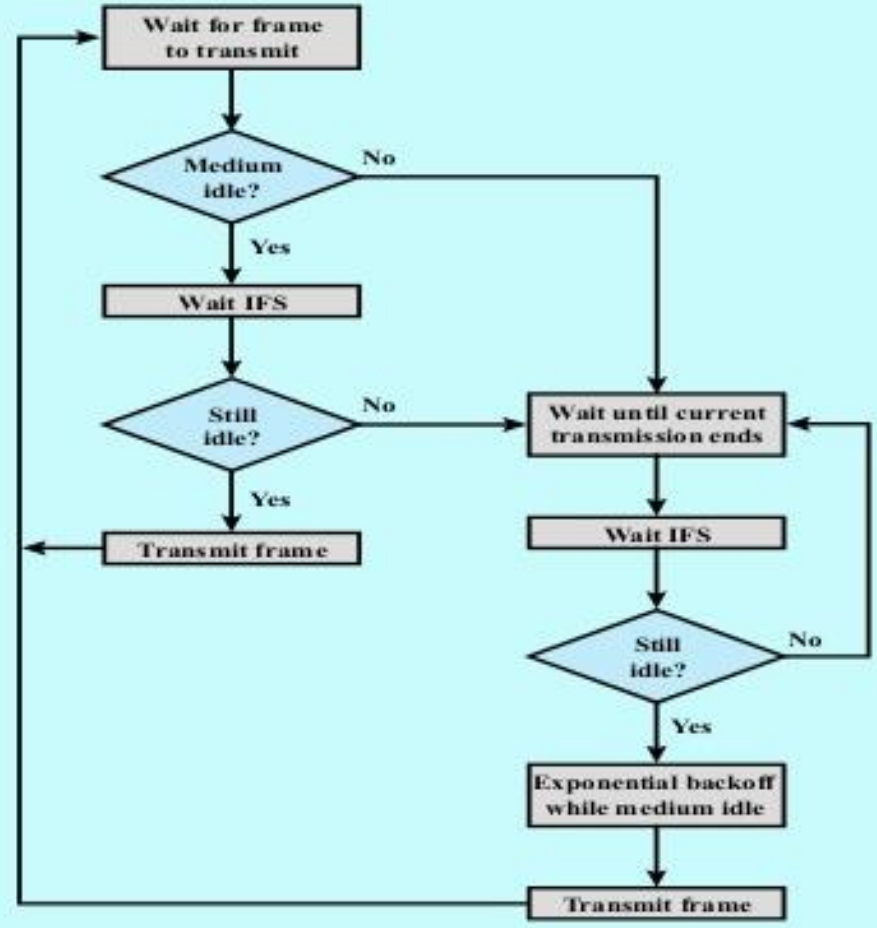
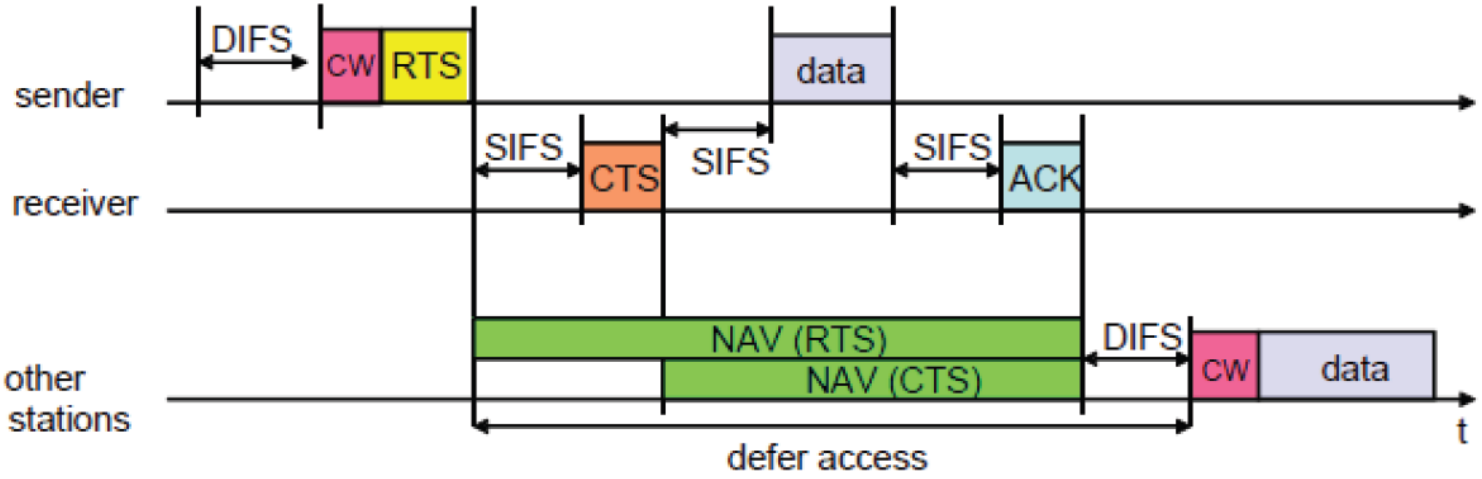
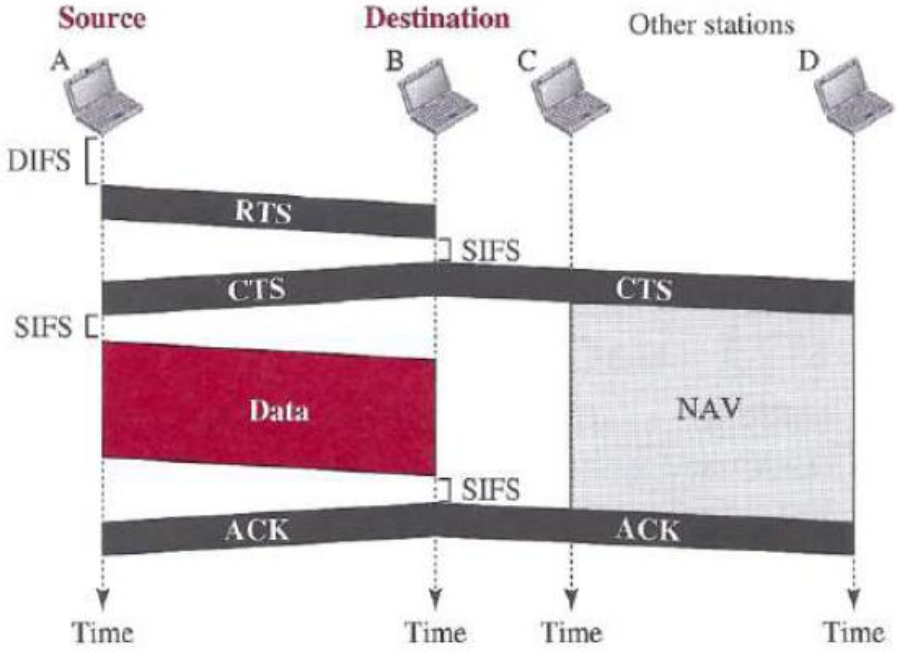


Figure 13.6 IEEE 802.11 Medium Access Control Logic

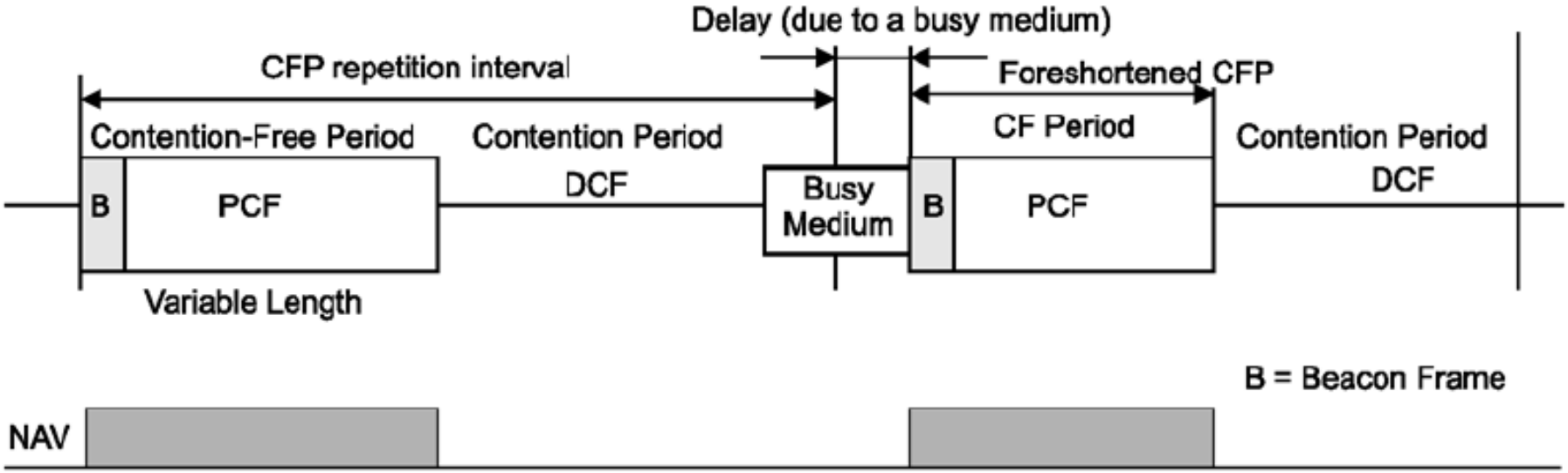
With RTS/CTS


DIFS
CW
RTS
data
sender
SIFS
CTS
SIFS
SIFS
ACK
receiver
NAV (RTS)
DIFS
NAV (CTS)
CW
data
other
stations
t
defer access

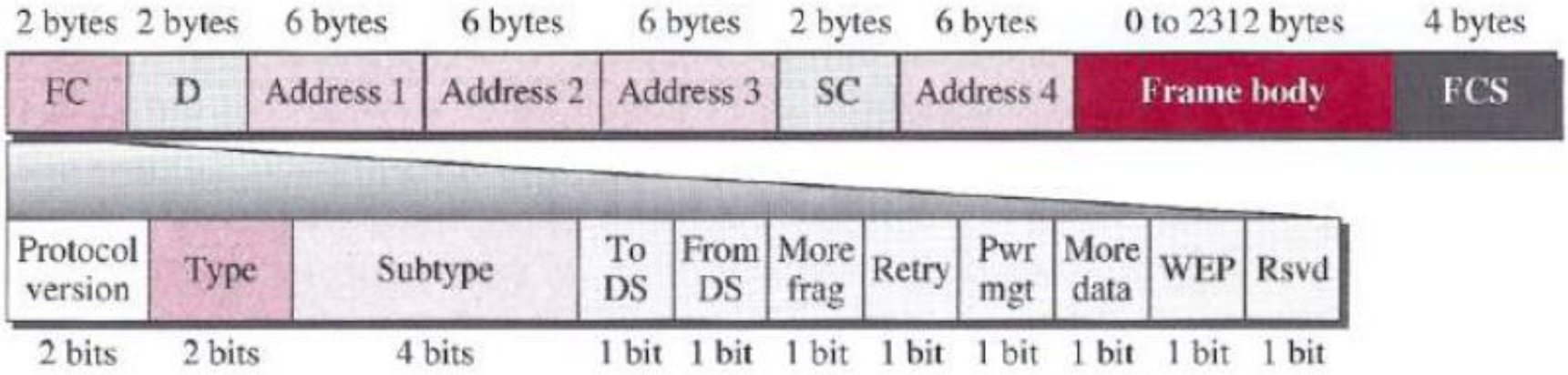

Source
Destination
Other stations
A
B
C
D
DIFS
RTS
SIFS
CTS
CTS
SIFS
Data
NAV
SIFS
ACK
ACK
Time
Time
Time
Time

PCF (Point Coordination Function)

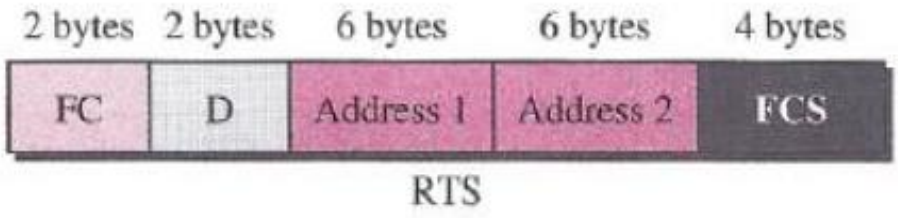
- PCF is an alternative access method implemented on top of the DCF.
- The operation consists of polling by the centralized polling master (point coordinator).
- The point coordinator makes use of PIFS when issuing polls.

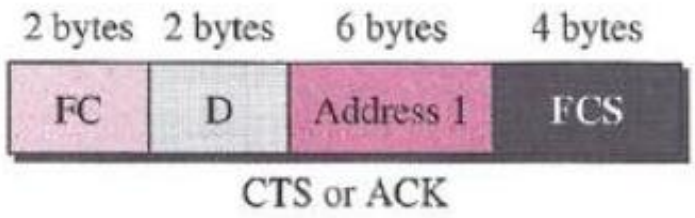


MAC Frame Format



- FC: Frame Control
- D: Duration / ID
- SC: Fragment number & Sequence counter
- FCS: Frame Check Sequence (CRC-32)





Frame Control (FC)

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Pathway to Gigabit WiFi

- IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s (1999)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)

- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- IEEE 802.11n: Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas) (September 2009)

- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z (March 2012)
- IEEE 802.11ac: Very High Throughput < 6 GHz; potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multiuser MIMO;(December 2013)
- IEEE 802.11ad: Very High Throughput 60 GHz (December 2012) — see WiGig

Performance of DCF

Thanks!

Figure and slide materials are taken from the following sources:

1. W. Stallings, (2017), Data and Computer Communications, 10th Ed.
2. B. A. Forouzan, (2012), Data Communication and Networking, 5th Ed.
3. Kurose and Ross, (2013), Computer Networking – A Top Down Approach, 6th Ed.