Wireless Local Area Networks

Ref Book:

Ad Hoc Wireless Networks, Architectures and Protocols, C. Siva Ram Murthy B. S. Manoj

Chapter 2

Difference between Wireless and Wired Transmission

In wireless communication,

- Address in not equivalent to physical location
- Dynamic topology and restricted connectivity
- Medium boundaries are not well-defined.
- Error-prone medium

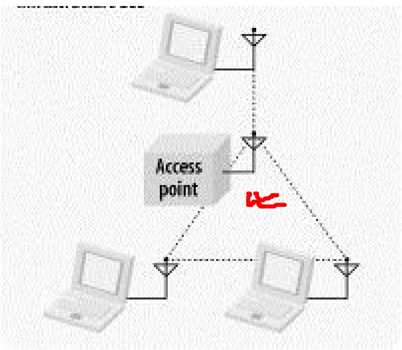
wireless channel

The above four factors imply that we need to build a reliable network on top of an inherently unreliable channel.

This is realized in practice by having reliable protocols at the MAC layer, which hide the unreliability that is present in the physical layer.

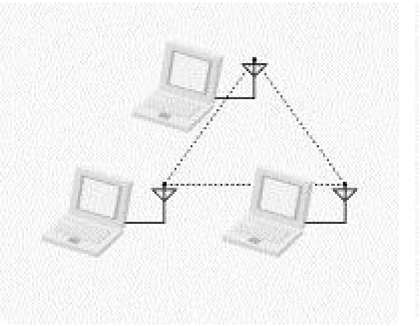
Types of WLANs

- WLANs can be broadly classified into two based on underlying architecture:
  - Infrastructure networks
  - Adhoc LANs



Infrastructure networks:

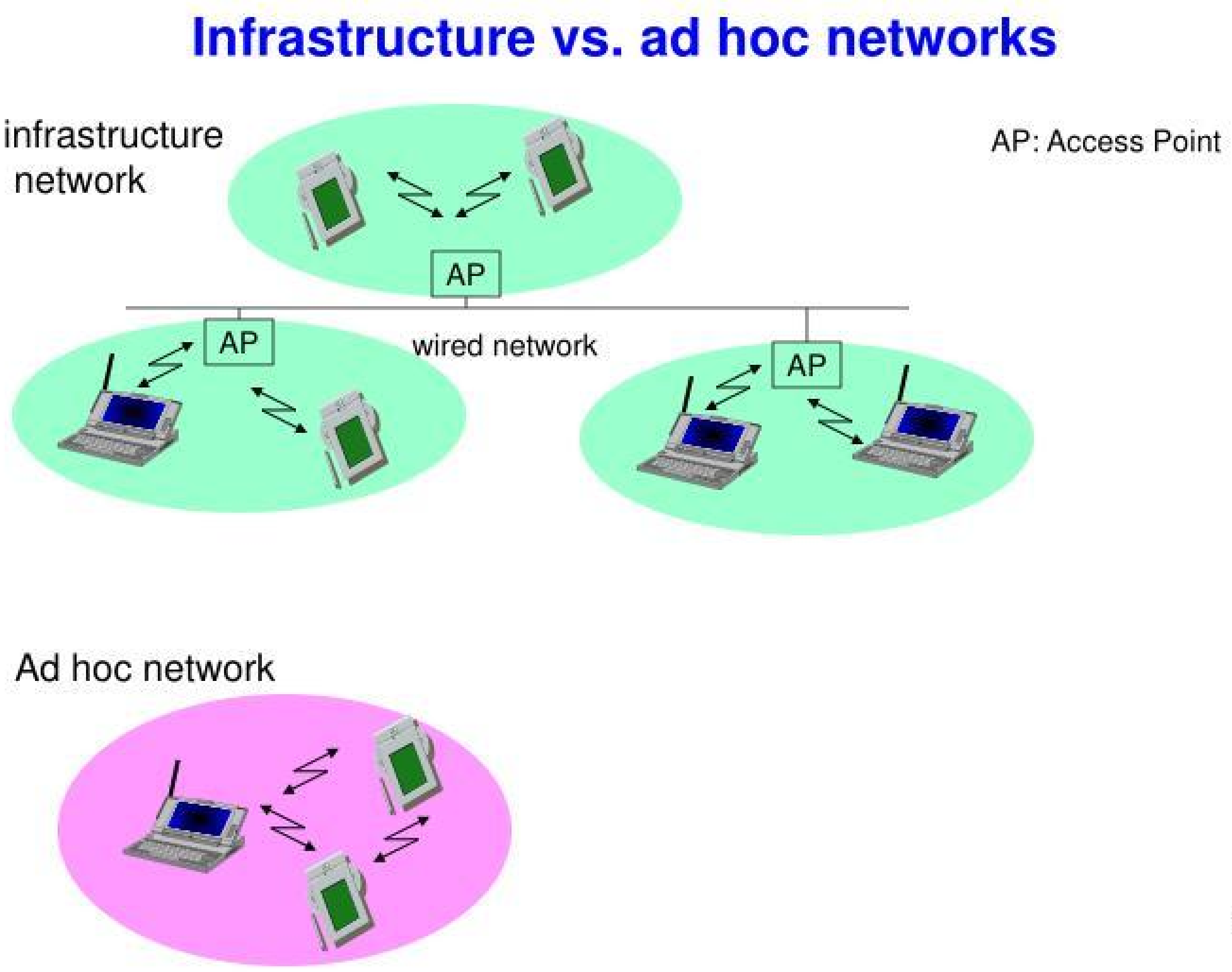
- Infrastructure networks are distinguished by the use of an access point.
- Access points are used for all communications in infrastructure networks, including communication between mobile nodes in the same service area.
- The other wireless nodes, also known as mobile stations (STAs) communicate via AP



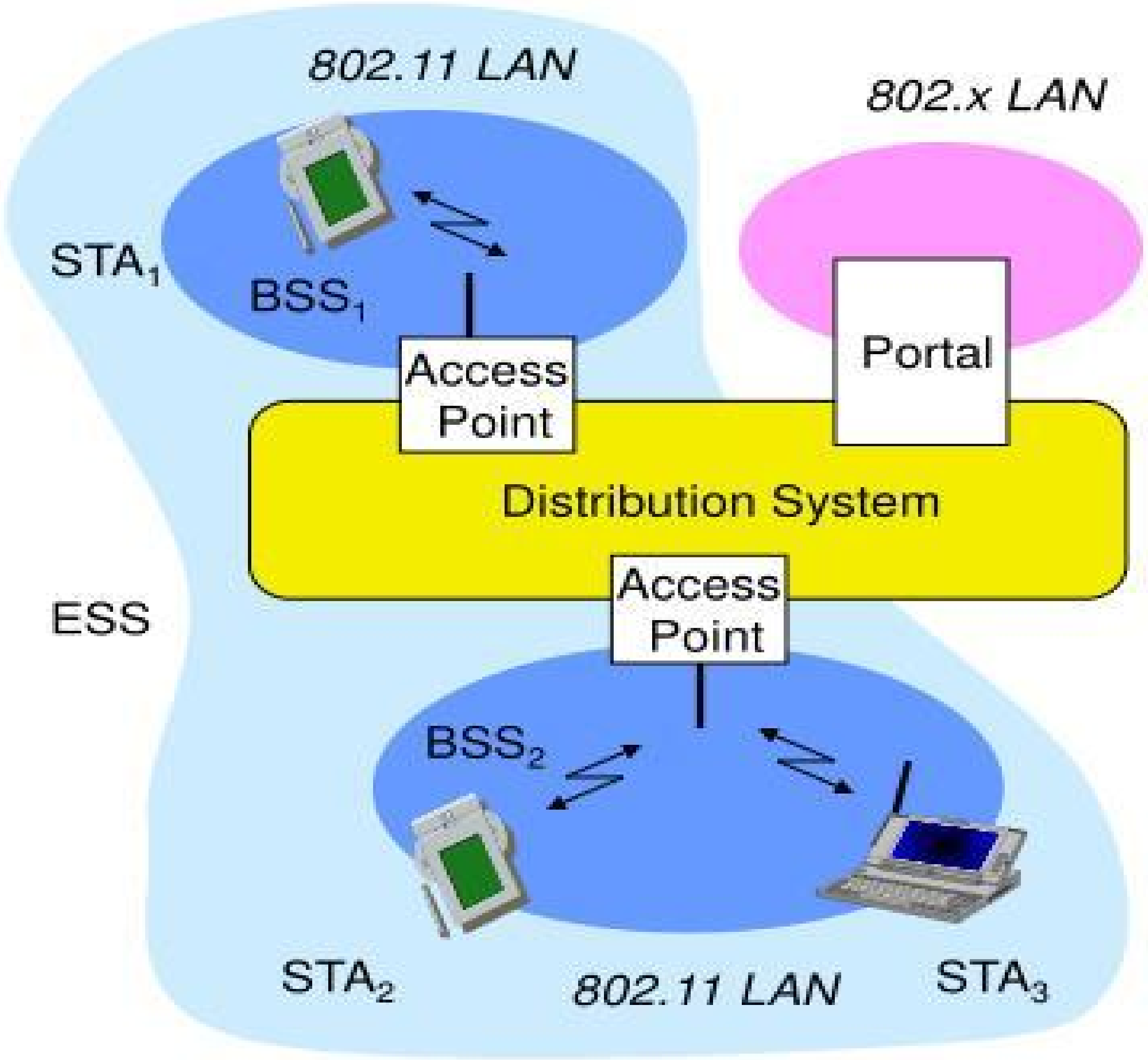
Independent networks/ Ad-hoc LANs:

- Adhoc LANs do not need any fixed infrastructure.
- These n/ws can be set up on the fly at any place.
- Nodes communicate directly with each other or forward messages through other nodes that are directly accessible

Types of WLANs



IEEE 802.11 - Architecture of an infrastructure network



Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point

- station integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

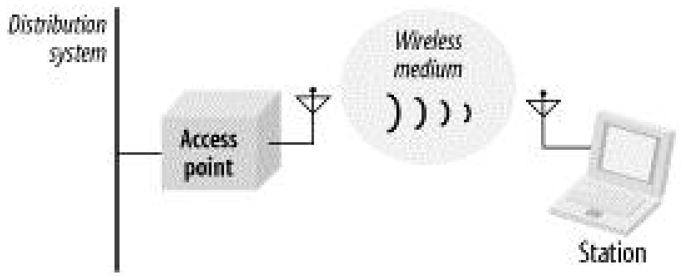
Distribution System

- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

802.11 Architecture ,Nomenclature and Design

Wireless medium:

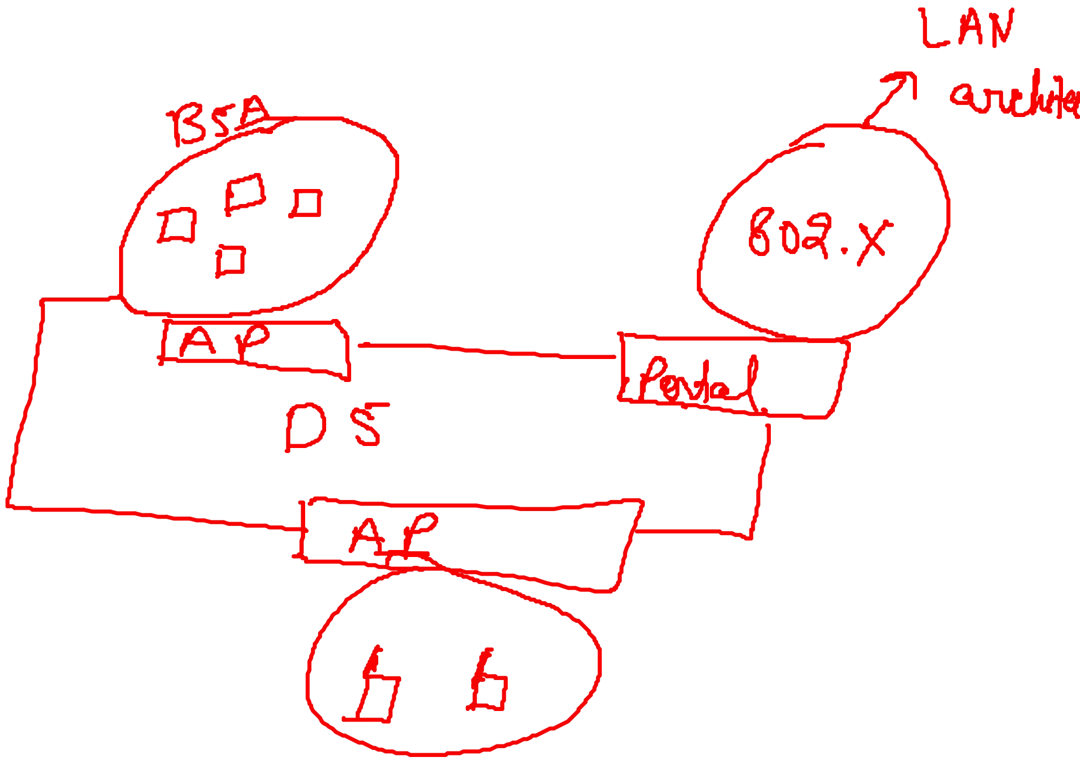
- To move frames from station to station, the standard uses a wireless medium. Several different physical layers are defined;
- Initially, two radio frequency (RF) physical layers and one infrared physical layer were standardized, though the RF layers have proven far more popular.



Components of 802.11 LANs

Portals

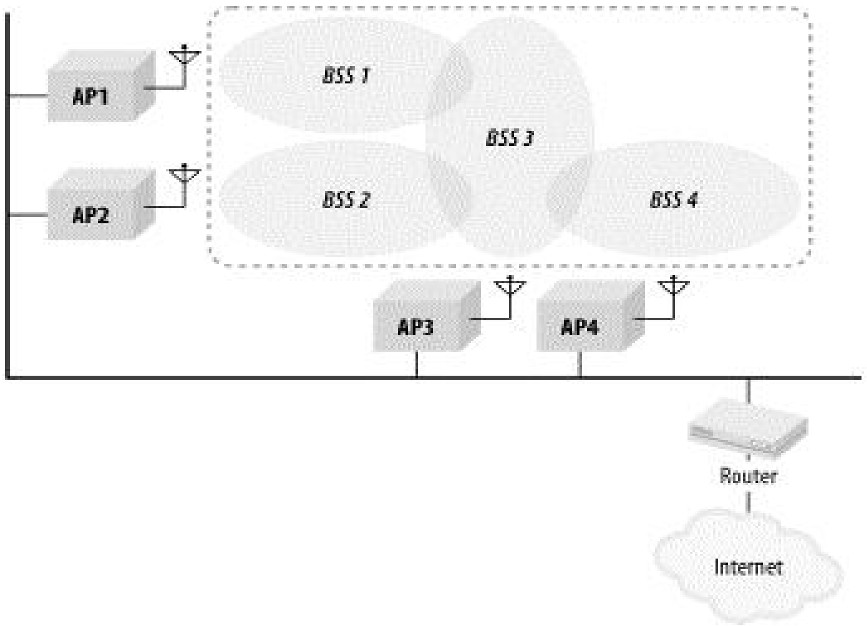
- Logical points through which non-wireless packets enters the system.
- They are necessary for integrating wireless n/w with existing wired n/ws.
- Just as an AP interects with the DS as well as the wireless nodes, the portal interacts with the wired network as well as with the DS.



Extended Service Set (ESS)

- An ESS is created by chaining BSSs together with a backbone network.
- 802.11 allows wireless networks of arbitrarily large size to be created by linking BSSs into an *extended service set (ESS)*.
- In Figure , the ESS is the union of the four BSSs (provided that all the access points are configured to be part of the same ESS).
- In real-world deployments, the degree of overlap between the BSSs would probably be much greater than the overlap in Figure.
- Stations within the same ESS may communicate with each other, even though these stations may be in different basic service areas and may even be moving between basic service areas.

- Access points act as bridges, so direct communication between stations in an ESS requires that the backbone network also be a layer 2 connection

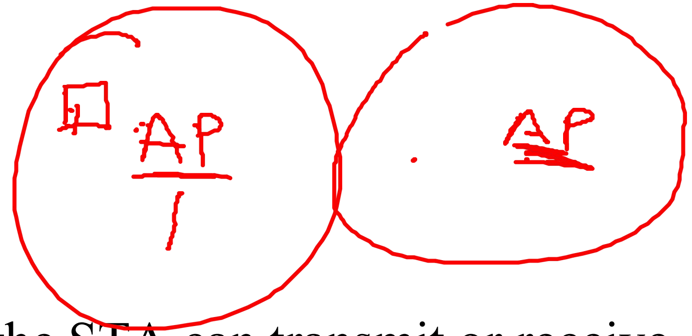


Services offered by IEEE 802.11 networks

- **Services offered can be broadly divided into two categories:**

(1) AP Services

(2) STA Services



Following are AP services:

Association:

- identity of an STA and its address should be known to the AP before the STA can transmit or receive frames on the WLAN.
- done during association and the info is used by AP to faciliatate routing of frames.

Reassociation

- established association is transferred from one AP to another using reassociation
- allows STAs to move from one BSS to another

Disassociation

- When an existing association is terminated, a notification is issued by the STA to the AP.
- Done when node leaves the BSS or when node shut down

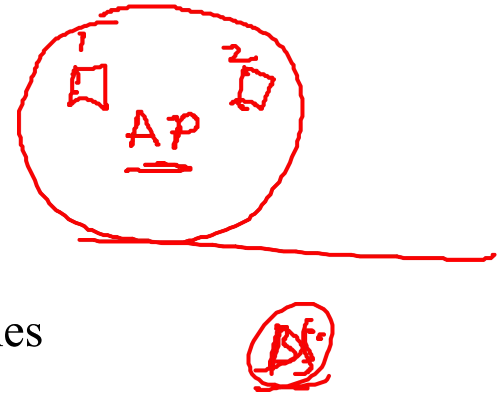
Services offered by IEEE 802.11 networks

Distribution:

- takes care of routing frames.
- If destination is in same BSS, frame is transmitted directly, otherwise, frame is sent via DS.

Integration

- To send frames through networks which have diffrent addressing schemes or frame formats



Following are STA services

Authentication:

- done in order to establish the identity of stations to each other.
- authentication scheme range from relatively insecure handshaking to public-key encrpytion schemes

Deauthentication:

- used to terminate existing authentication

Privacy:

- contents of the messages may be encrypted to prevent eavesdroppers from reading the messages

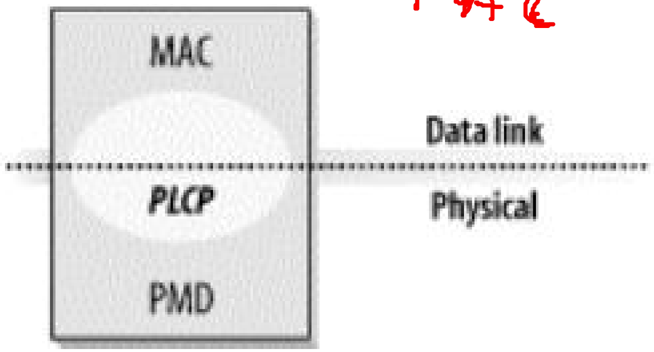
Data Delivery:

- IEEE 802.11 naturally provides a way to transmit and receive data.
- However, like ethernet, the transmission is not guarnteed to be completly reliable.

IEEE 802.11 Physical layer

IEEE 802.11
↳ Physical
MAC

- Supports three options for the medium to be used at the physical level.
  - one is based on infra-red
  - other two are based on radio transmission.



- Physical layer is subdivided conceptually into two parts:
  - Physical medium dependent sublayer (PMD)
  - Physical layer convergence protocol (PLCP)

- PMD handles encoding, decoding and modulation of signals
- PLCP abstracts the functionality the the physical layer has to offer the MAC layer

- PLCP offers service access points (SAP) that is independent of the transmission technology and a clear channel assessment (CCA) carrier sense signal to the MAC layer.
- The SAP abstracts the channle which can offer up to 1 or 2 Mbps data transmission bandwidth.
- The CCA is used by the MAC layer to implement the CSMA/CA mechanism.

CSMA/CD → wired n/w

IEEE 802.11 Physical layer

Three choices for physical layer in the original 802.11 standards are as follows:

1. FHSS operating in the license free 2.4 GHz at data rate of 1 Mbps
2. DSSS operating in the 2.4 Ghz band at data rate of 1 Mbps

radio

3. infra-red operating at wavelemgth in 850-950nm, at data rate of 1 Mbps and 2 Mbps

Carrier Sense Mechanisms

- In IEEE 802.3, sensing the channel is very simple.
  - receiver reads the peak voltage on the cable and compares it against the threshold.
- In contrast, the mechansim employed in IEEE 802.11 is relatively more complex.
- It is performed either physically or virtually.
- The physical layer sensing is through CCA channel provided by PLCP.
- The CCA is generated based on 1 sensing of the air interface by sensing the detected bits in the air or by 2 checking the received signal strenght (RSS) of the carrier against a threshold.
- Decisions based on the detected bits are somewhat more slow but more reliable.
- Decisions based on the RSS can potentially create a false alarm caused by measuring the level of interference.

IEEE 802.11 Protocol Architecture

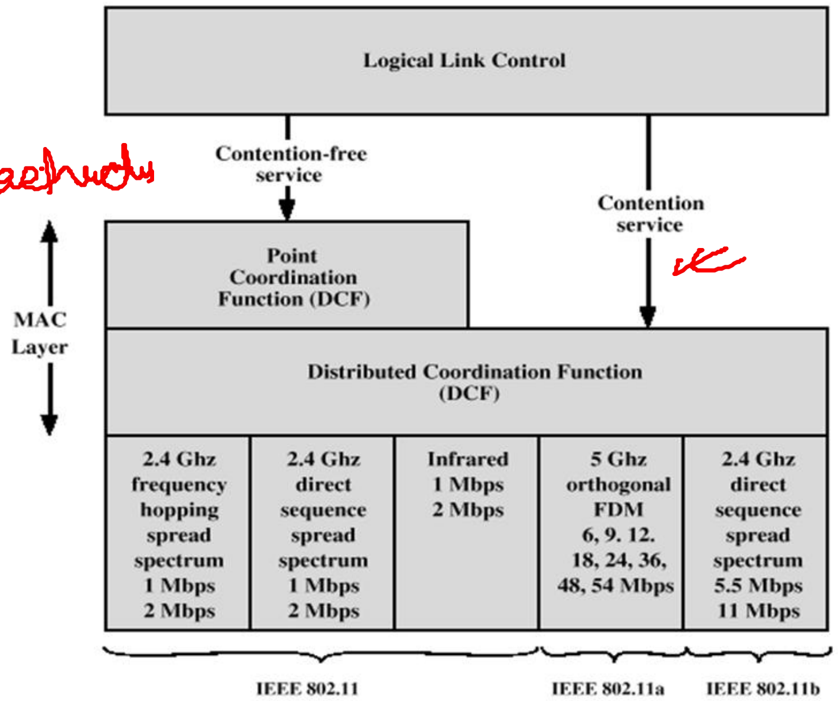
MAC layer divided into two sublayers: the distributed coordination function (DCF) and Point coordination function. PCF build on the top of DCF

① DCF → Adhoc LANs

② PCF → infrastructure N/w

DCF (distributed coordination function):

- The lowest sublayer of the MAC layer is the distributed coordination function (DCF).
- DCF uses a contentation algorithm to provides access to all traffic.
- The DCF is the basis of the standard CSMA/CA access mechanism.
- Like Ethernet, it first checks to see that the radio link is clear before transmitting.
- To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the CTS/RTS clearing technique to further reduce the possibility of collisions.



(i) CSMA/CA technique

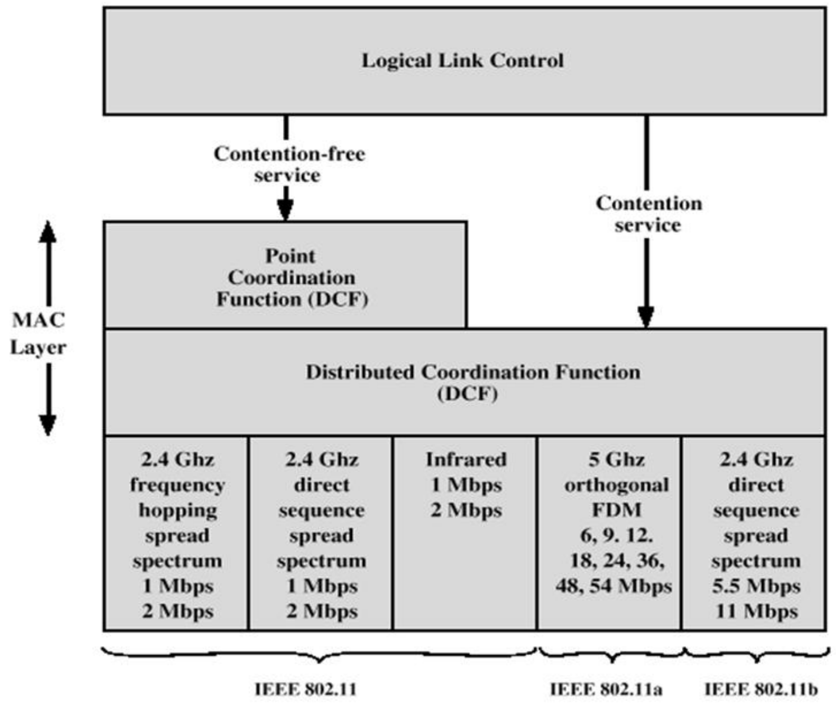
(ii) RTS/CTS (avoid hidden terminal

IEEE 802.11 Protocol Architecture

MAC layer divided into two sublayers: the distributed coordination function (DCF) and Point coordination function. PCF build on the top of DCF

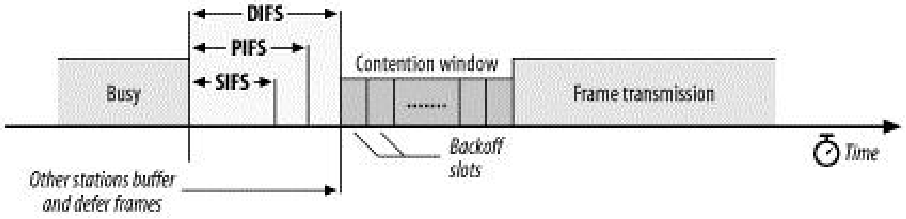
PCF (point coordination function):

- Point coordination function provides contention-free services.
- Special stations called point coordinators are used to ensure that the medium is provided without contention. Point coordinators reside in access points, so the PCF is restricted to infrastructure networks.



Interframe Spacing : time interval b/w the transmission of two successive frames by any station

- 802.11 uses four different interframe spaces (Set of delays). Three are used to determine medium access;
- Varying interframe spacings create different priority levels for different types of traffic. The logic behind this is simple: high-priority traffic doesn't have to wait as long after the medium has become idle.



Short interframe space (SIFS):

- The SIFS is used for the highest-priority transmissions, such as RTS/CTS frames and positive acknowledgments.
- High-priority transmissions can begin once the SIFS has elapsed.
- Once these high-priority transmissions begin, the medium becomes busy, so frames transmitted after the SIFS has elapsed have priority over frames that can be transmitted only after longer intervals.

PCF interframe space (PIFS):

- used by the PCF during contention-free operation.
- Stations with data to transmit in the contention-free period can transmit after the PIFS has elapsed and preempt any contention-based traffic.

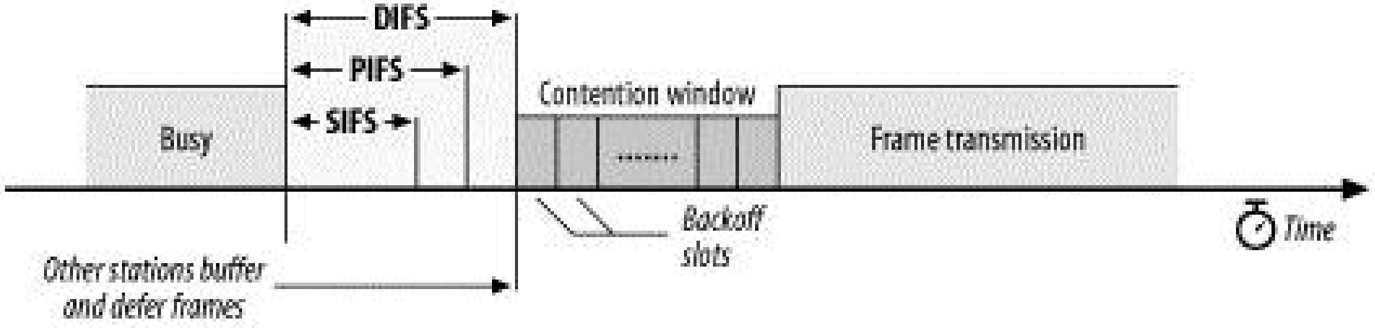
Interframe Spacing

DCF interframe space (DIFS):

- minimum medium idle time for contention-based services.
- Stations may have immediate access to the medium if it has been free for a period longer than the DIFS.

Extended interframe space (EIFS):

- largest of all the IFSs
- denotes the least priority to access the medium.
- used for resynchronization whenever physical layer detects incorrect MAC frame reception.
- The EIFS is not illustrated in Figure because it is not a fixed interval. It is used only when there is an error in frame transmission.



CSMA/CA vs CSMA/CD

- -Media Access Control (MAC) describes how the media (wired or wireless) is used.
  - Polling, token passing, contention based
- CSMA/CD is for ethernet wired based
- CSMA/CA for wireless 802.11
- Stations using either access metod must first listen to see whether any other device is transmitting. If another device is transmitting, the stations must wait untill the medium is available.

CSMA/CA vs CSMA/CD

- The difference is when the transmission medium is clear.
- CSMA/CD node can immediatly begin transmitting.
- If a collision occurs while a CSMA/CD node is transmitting, the collisin will be detected and the node will temporarly stop transmitting.
- *02.11 nodes use CSMA/CA transmissions.
- If CSMA/CA station sees no transmissions, it will wait a random interval
- - keep watching the medium
- if still clear after interval, transmit
- if not, start over

CSMA/CA Mechanism

Carrier sense multiple access with collision avoidance (CSMA/CA)

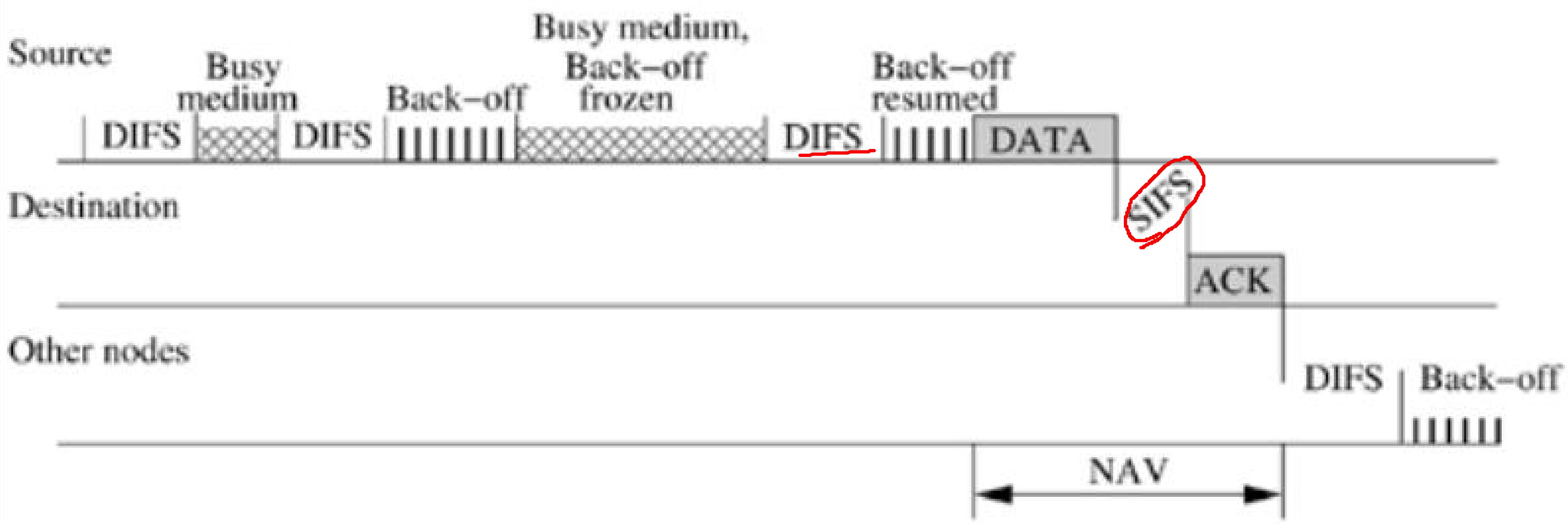
- a MAC layer mechanism used by IEEE 802.11 WLANs

Why CSMA/CA not CSMA/CD? → Why not wireless

Reasons:

- error rate in WLAN is much higher and allowing collision leads to drastic reduction in throughput.
- detecting collisions in the wireless medium is not always possible.

CSMA/CA Mechanism



basic channel access mechanism of IEEE 802.11

CSMA/CA Mechanism

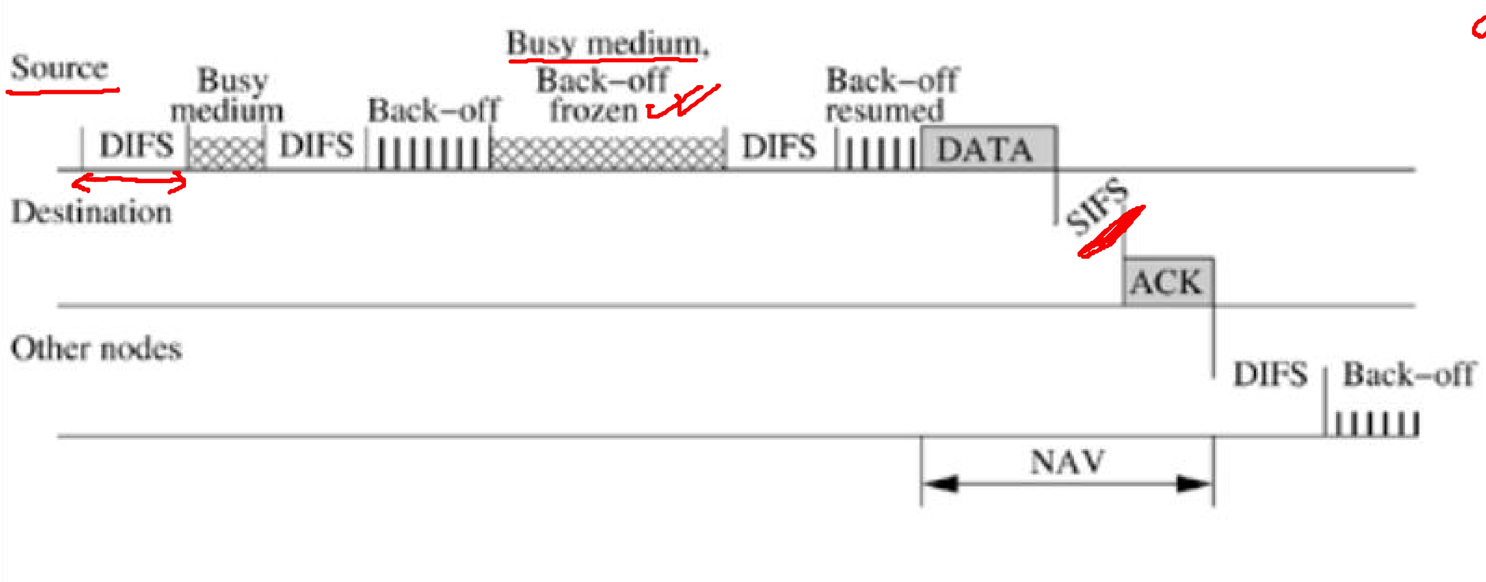
Suppose a source node wants to sends a message to destination:

DCF

1st Possiblity: medium is idle

1. if the medium is sensed to be idle for a duration of DIFS, node accesses the medium for transmission. Channel access delay at very light load is equal to DIFS.

channel access delay = DIFS



CSMA/CA Mechanism

CWmin

2nd Possiblity: medium is busy

- If the medium is busy, the node back off - stations defer channel access by a random amount of time-chosen within contention window.
  - value of CW can varry between CWmin and CWmax.
  - Time intervals are all integral multiples of slot times (Def: Slot Time: basic unit of time measure)
  - chosen judiously using propgation delay, transmission delay and any other physical layer dependent parameters.

- When backoff counter expires, station can access the medium.

Note:

- During the backoff process, if a node detects a busy channel, it freezes the backoff counter.
  - **benefit:** Longer waiting stations instead of choosing another random interval from the contention window, wait only for a residual amount of time. mechanism is fair.
- Process is resumed once the channel becomes idle for period of DIFS.

Contention Window Size

- imp. parameter
- CW is small- random values will be close together- there is high probablity of packet collisions.
- CW is large - unnecessary delay because of back-off values
- Therefore, system should adept to the current number of stations that are contending for channel access.
- Hence, binary exponential backoff technique is used. (BEB)
- With every unsuccessful attempt, the maximum backoff interval is doubled (

  (Ref: https://devopedia.org/binary-exponential-backoff)

CWmin CWmax

- initial contention window size= random value between (0, CWmin)
- CW doubles its size to a maximum of CWmax -each time collision occurs.

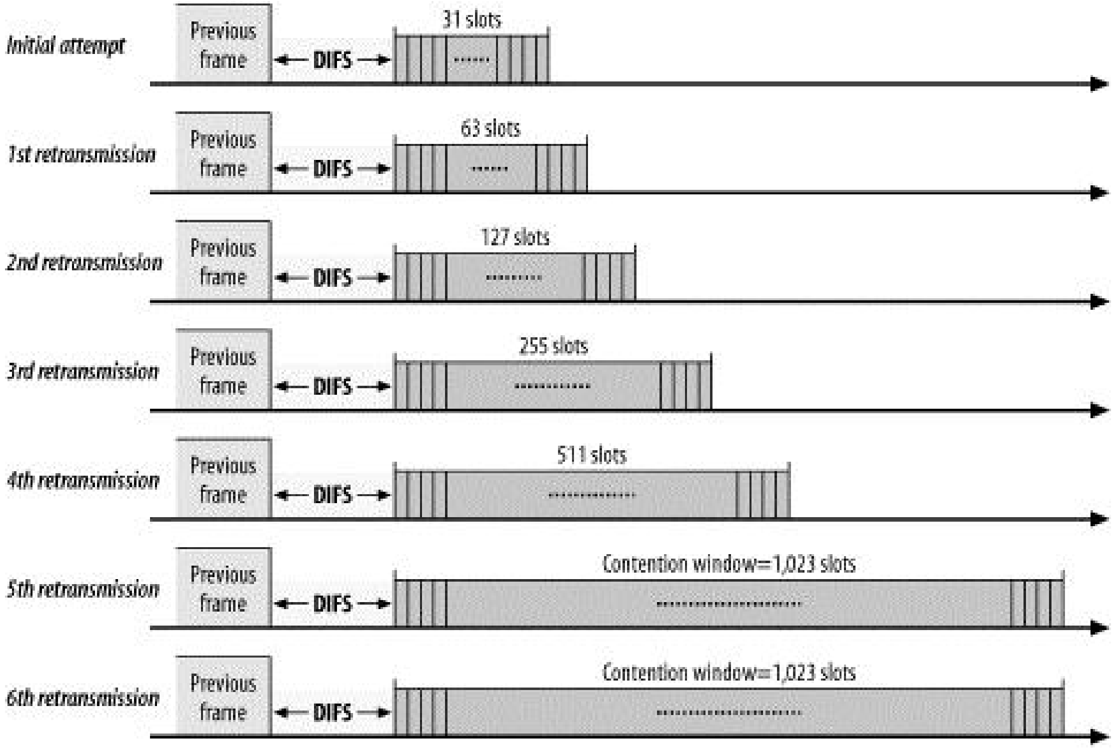
- So, CW size is high at high load
- and low loads, small CW ensures low access delay

Backoff with the DCF

- After frame transmission has completed and the DIFS has elapsed, Many stations may attempt to transmit frames.
- A period called the contention window or backoff window follows the DIFS.
- This window is divided into slots. Slot length is medium-dependent; higher-speed physical layers use shorter slot times.
- Stations pick a random slot and wait for that slot before attempting to access the medium; all slots are equally likely selections.
- When several stations are attempting to transmit, the station that picks the first slot (the station with the lowest random number) wins.
- Contention window sizes are always 1 less than a power of 2 (e.g., 31, 63, 127, 255).
- Each time the retry counter increases, the contention window moves to the next greatest power of two.
- The size of the contention window is limited by the physical layer. For example, the DS physical layer limits the contention window to 1023 transmission slots.

Backoff with the DCF

- When the contention window reaches its maximum size, it remains there until it can be reset.
- Allowing
- long contention windows when several competing stations are attempting to gain access to the medium keeps the MAC algorithms stable even under maximum load.
- The contention window is reset to its
- minimum size when frames are transmitted successfully, or the associated retry counter is reached, and the frame is discarded.



In Figure illustrates the growth of the contention window as the number of transmissions increases, using the numbers from the direct-sequence spread-spectrum (DSSS) physical layer.

Acknowledgements

- ACK must be sent - to ensure their data packets correct delivery

For Unicast Packets,

- receiver accesses the medium after waiting for a SIFS and send an ACK.
- Other stations have to wait for DIFS plus their backoff time
- This mechanism reduces- probablity of collision
- Note: Higher priority is given for sending an ACK for the previously received data packet then for starting a new data packet transmission
- ACK ensures the correct reception of the MAC layer frame by using cyclic redundancy checksum (CRC)
- technique.
- If no ACK is received by the sender, then a retransmission takes place.
- The number of retransmissions is limited, and failure is reported to the higher layer after the retransmission count exceeds this limit

Acknowledgements

Wifi

Parameter	802.11 (FHSS)	802.11 (DSSS)	802.11 (IR)	802.11b	802.11a
t_{slot}	50 μsec	20 μsec	8 μsec	20 μsec	9 μsec
SIFS	28 μsec	10 μsec	10 μsec	10 μsec	16 μsec
PIFS	SIFS $+t_{slot}$				
DIFS	SIFS+$(2 \times t_{slot})$				
Operating Frequency	2.4 GHz	2.4 GHz	850-950 nm	2.4 GHz	5 GHz
Maximum Data Rate	2 Mbps	2 Mbps	2 Mbps	11 Mbps	54 Mbps
CWmin	15	31	63	31	15
CWmax	1,023	1,023	1,023	1,023	1,023

Hidden Station Problem

One of the major problem- observed in wireless networks.

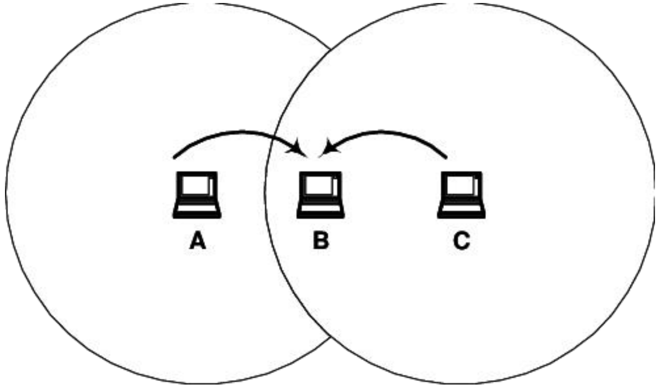
Considered as a classsic example of problems arising due to incomplete topology information in wireless n/ws.

The problem of a station not being able to detect a potential competitor for the medium because the competitor is too far away.

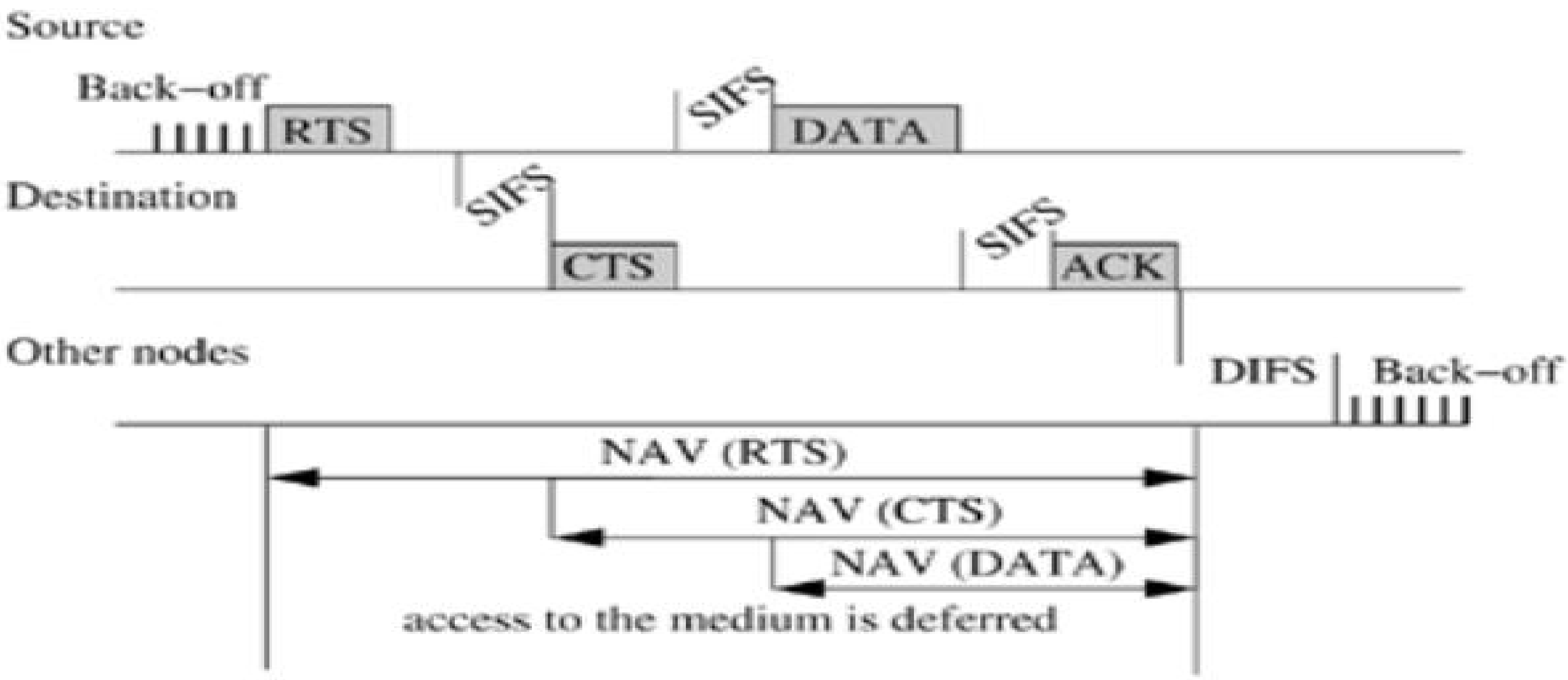
Example of the problem:

- A and C send a signal to B.
- But A and C aren't aware of each other's signals.
- Signals collide at B.
- But A and C don't know they collided so don't go into collision avoidance.

A and C are "hidden nodes"



RTS-CTS Mechanism



(b)

RTS-CTS Mechanism

Sender sends a RTS packet to the receiver.

RTS packet Content: Receiver of the next data packet and expected duration of the whole data transmission

RTS packet is received by all stations that can hear the sender.

Every station that receives this packet will set its network allocation vector (NAV) accordingly

NAV: specifies the earliest time when the station is permitted to attempt transmission.

After Waiting for SIFS, the intended receiver of the data packet answers with a clear to send (CTS) if it is ready to accept the data packet

CTS packet contains the duration fiels and all stations receiving the CTS packet also set their NAVs.

Note: The set of stations receiving the CTS packet may be different from the set of stations that received the RTS packet (indicates presence of hidden terminal).

RTS-CTS Mechanism

- Once the RTS packet has been sent and CTS packet has been received successfully, all nodes are informed of the medium reservation.
- The sender then starts transmission after waiting for SIFS.
- receiver, after receiving the data packet, waits for another SIFS and sends the ACK.
- As the transmissin is over, the NAV in each node marks the medium as free (unless the node has heard some other RTS/CTS) and the process can repeat again.

- The usage of RTS-CTS before data packet transmission is a form of virtual carrier sensing.

Overhead involved in RTS-CTS

- RTS-CTS Mechanism is used to reserve the medium prior to a particular data transfer sequence in order to avoid collisions during the transfer.
- However, transmission of RTS-CTS can result in non-negligible overhead.
- Therfore, RTS-CTS mechanism should be used judiously.
- An RTS Threshold is used to determine whether to start the RTS-CTS mechanism or not.
- Typically, if the frame size is more than the RTS threshold, the RTS-CTS mechanism is activated and a four-way handshake (i.e. RTS-CTS-DATA-ACK) follows.
- If the frame size is below RTS threshold, the nodes resort to a two-way handshake(DATA-ACK)

Contention-Free Access Using the PCF

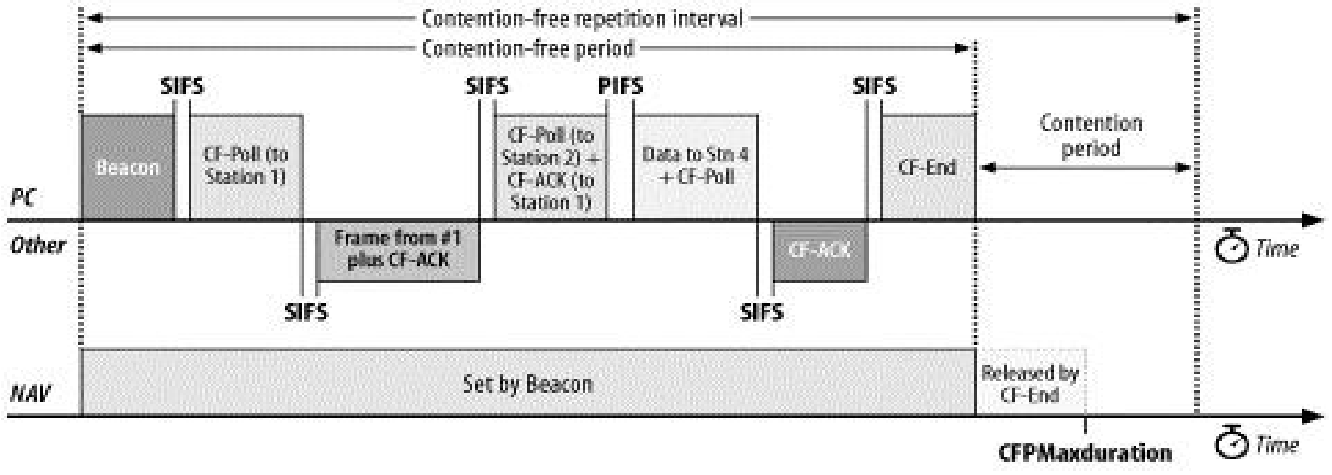
- **objective:** to provide guarantees on the maximum access delay, minimum transmission bandwidth, and other QoS parameters.
- Unlike the DCF, where the medium contention is resolved in a distributed manner, the PCF works by effecting a centralized contention resolution scheme, and is applicable only in networks where an AP polls the nodes in its BSS.
- A point coordinator (PC) at the AP splits the access time into super frame periods.
- The super frame period consists of **alternating contention free periods (CFPs) and contention periods (CPs).**
- The PC will determine which station has the right to transmit at any point of time.
- The PCF is essentially a polled service with the PC playing the role of the polling master.
- The operation of the PCF may require additional coordination to perform efficient operation in cases where multiple PCs are operating simultaneously such that their transmission ranges overlap.
- The IFS used by the PCF is smaller than the IFS of the frames transmitted by the DCF.
- This means that point-coordinated traffic will have higher priority access to the medium if DCF and PCF are concurrently in action.
- The PC controls frame transmissions so that contentions are eliminated over a limited period of time, that is, the CFP.

Contention-Free Access Using the PCF

- The point coordination function (PCF) allows an 802.11 network to provide an enforced *"fair" access to the medium.*
- In some ways, access to the medium under the *PCF resembles token-based medium access control schemes, with the access point holding the token.*
- Contention-free service uses a centralized access control method. Access to the medium is restricted by the point coordinator, a specialized function implemented in access points.
- Associated stations can transmit data only when they are allowed to do so by the point coordinator.
- Access is under the control of a central entity, all transmissions must be acknowledged.

PCF Operation

- When the PCF is used, time on the medium is divided into the contention-free period (CFP) and the contention period.
- The contention period must be long enough for the transfer of at least one maximum-size frame and its associated acknowledgment.
- Alternating periods of contention-free service and contention-based service repeat at regular intervals, which are called the contention-free repetition interval.



Reserving the medium during the contention-free period:

- At the beginning of the contention-free period, the access point transmits a Beacon frame. One component of the beacon announcement is the maximum duration of the contention-free period, *CFPMaxDuration.*
- *All stations receiving the Beacon set the NAV to the maximum duration to lock out* DCF-based access to the wireless medium.
- As an additional safeguard to prevent interference, all contention-free transmissions are separated only by the short interframe space and the PCF interframe space. Both are shorter than the DCF interframe space, so no DCF-based stations can gain access to the medium using the DCF.