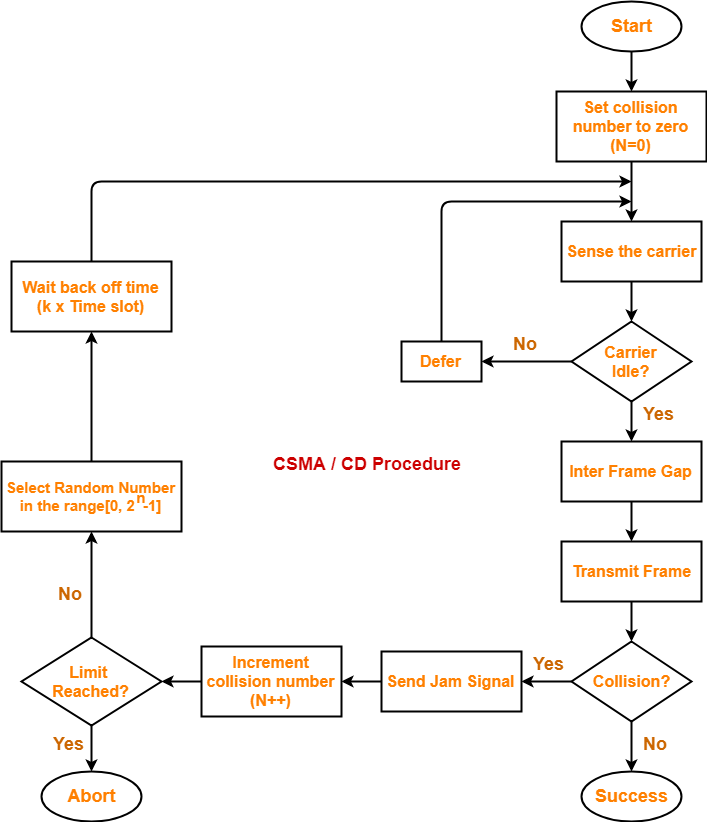
**oooooCSMA/CD, CSMA/CA, IFS, HIDDEN NODE PROBLEM**

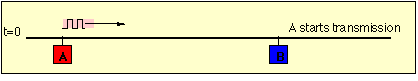
|  |  |
| --- | --- |
| Prepared by | Ayushi Pradhan |
| Reviewed by | V.Mamatha |

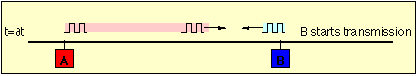
**CSMA/CD**

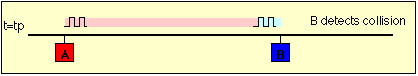
CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs when there used to be shared Bus Topology and each node ( Computers) were connected By Coaxial Cables.

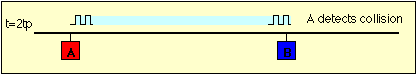
**FLOWCHART:**











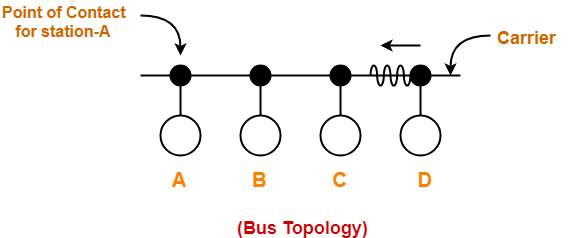
**ALGORITHM**

**Step-01: Sensing the Carrier**

* Any station willing to transmit the data senses the carrier.
* If it finds the carrier free, it starts transmitting its data packet otherwise not.
* Each station can sense the carrier only at its point of contact with the carrier.
* It is not possible for any station to sense the entire carrier.
* Thus, there is a huge possibility that a station might sense the carrier free even when it is not.

Example-

Consider the following scenario-



At the current instance,

* If station A senses the carrier at its point of contact, then it will find the carrier free.
* But the carrier is not free because station D is already transmitting its data.
* If station A starts transmitting its data now, then it might lead to a collision with the data transmitted by station D.

**Step-02: Detecting the Collision**

* It is the responsibility of the transmitting station to detect the collision.
* For detecting the collision, CSMA / CD implements the following condition.
* This condition is followed by each station-

Transmission delay >= 2 x Propagation delay

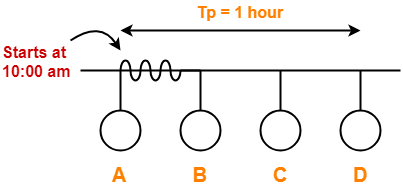
According to this condition,

* Each station must transmit the data packet of size whose transmission delay is at least twice its propagation delay.
* If the size of data packet is smaller, then collision detection would not be possible.

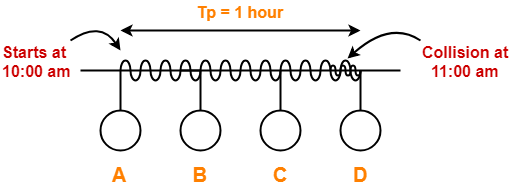
**Length Of Data Packet-**

Length of data packet (L) >= 2 x Bandwidth (B) x Distance between the two stations (D) / Propagation speed (V)

Understanding the Condition to Detect Collision with Example



* Consider at time 10:00 am, station A senses the carrier.
* It finds the carrier free and starts transmitting its data packet to station D.
* Let the propagation delay be 1 hour.



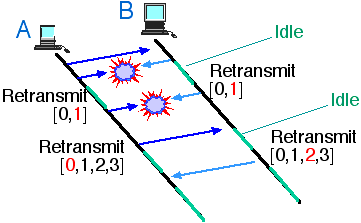
* Let us consider the scenario at time 10:59:59:59 when the packet is about to reach the station D.
* Currently, station D senses the carrier.
* It finds the carrier free and starts transmitting its data packet.
* Now, as soon as station D starts transmitting its data packet, a collision occurs with the data packet of station A at time 11:00 am.
* After collision occurs, the collided signal starts travelling in the backward direction.
* The collided signal takes 1 hour to reach the station A after the collision has occurred.
* For station A to detect the collided signal, it must be still transmitting the data.
* So, transmission delay of station A must be >= 1 hour + 1 hour >= 2 hours to detect the collision.
* That is why, for detecting the collision, condition is Tt >= 2Tp.
* Two cases are possible-
  + Case-01:
    - If no collided signal comes back during the transmission,
    - It indicates that no collision has occurred.
    - The data packet is transmitted successfully.
  + Case-02:
    - If the collided signal comes back during the transmission,
    - It indicates that the collision has occurred.
    - The data packet is not transmitted successfully.
    - Step-03 is followed.

**Step-03: Releasing Jam Signal**

* Jam signal is a 48-bit signal.
* It is released by the transmitting stations as soon as they detect a collision.
* It alerts the other stations not to transmit their data immediately after the collision.
* Otherwise, there is a possibility of collision again with the same data packet.
* Ethernet sends the jam signal at a frequency other than the frequency of data signals.
* This ensures that jam signal does not collide with the data signals undergone collision.

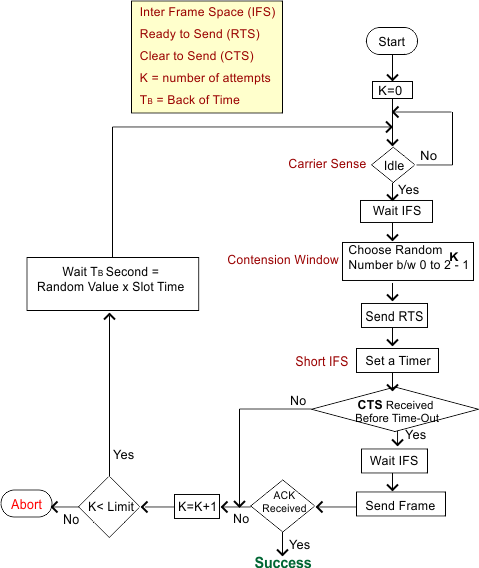
**Step-04: Waiting for Back Off Time-**

* After the collision, the transmitting station waits for some random amount of time called as back off time.
* After back off time, it tries transmitting the data packet again.
* If again the collision occurs, then station again waits for some random back off time and then tries again.
* The station keeps trying until the back off time reaches its limit.
* After the limit is reached, station aborts the transmission.
* Back off time is calculated using Back Off Algorithm.



**CSMA/CA**

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station first check the state of the medium before sending.

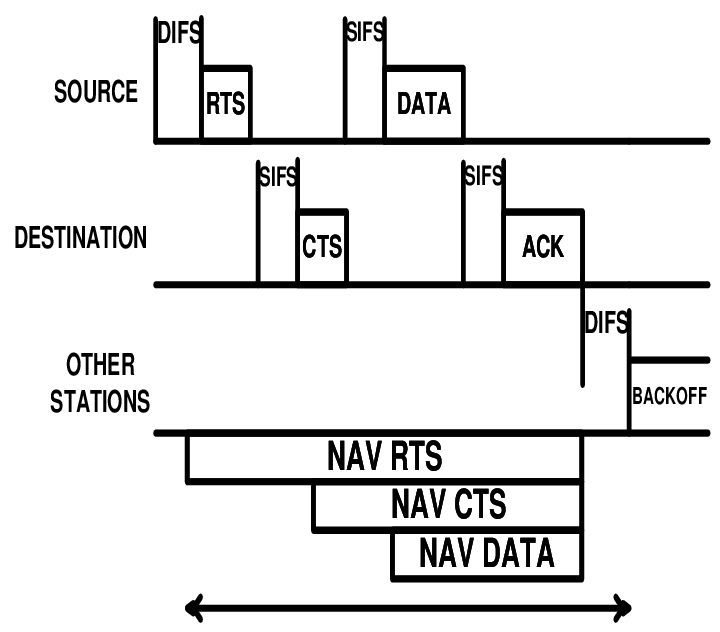


**PHYSICAL CARRIER SENSE**

* Physical carrier sensing is performed constantly by all stations that are not transmitting
* or receiving.
* When a station performs a physical carrier sense, it is actually listening to the
* channel to see whether any other transmitters are taking up the channel.
* Physical carrier sense has two purposes:
  + The first purpose is to determine whether a frame transmission is inbounded for a station to receive. If the medium is busy, the radio will attempt to synchronize with the transmission.
  + The second purpose is to determine whether the medium is busy before transmitting. This is known as the *clear channel assessment (CCA)*.
* The CCA involves listening for 802.11 RF transmissions at the Physical layer. The medium must be clear before a station can transmit. Physical carrier sensing is performed constantly by all stations that are not transmitting or receiving.
* If the channel is considered occupied, then the CCA indicates a state of busy.
* If the channel is considered clear, then the CCA indicates a state of idle.
* CCA is set to busy if a high level of energy is detected coming from valid modulated 802.11 bits.
* If the modulated bits are detected at those energy levels, the CCA will go busy for
  + - * + 15 microseconds in DSSS
        + 4 microseconds in OFDM
* If at the end of the period, modulated bits are getting detected then the CCA will continue to stay busy.
* If an AP or STA sees the CCA as an idle while the channel is still occupied, it could lead to collisions. That is why WLANs have NAV which acts as virtual carrier sense.

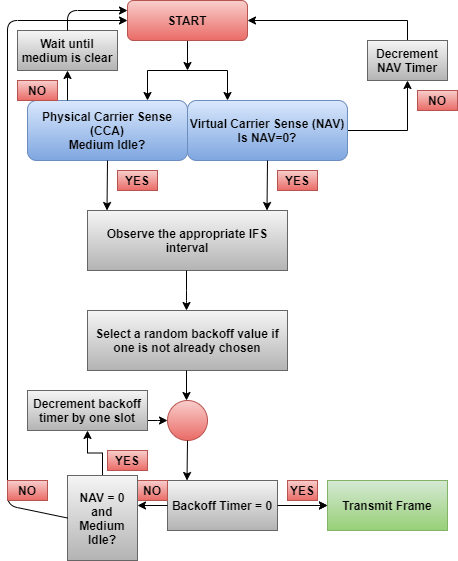
**VIRTUAL CARRIER SENSE**

* The network allocation vector (NAV) is the virtual carrier sense mechanism for 802.11 APs and stations.
* The NAV is a timer that counts down toward zero. When a device has a NAV value greater than zero, the device stays quiet.
* Once the NAV value reaches zero, the wireless medium is considered clear.
* APs and stations set their NAV values according to the Duration value inside the 802.11 header.
* The Duration value is contained within the Duration/ID field of all 802.11 frames except the power save poll.
* The Duration value will set the NAV only if the AP or station viewing the header is not the receiver of the frame.



**DISTRIBUTED COORDINATION FUNCTION (DCF)**

* Distributed coordination function (DCF) is a mandatory technique used to prevent collisions in IEEE 802.11-based WLAN standard (Wi-Fi).
* It is a medium access control (MAC) sublayer technique used in areas where carrier-sense multiple access with collision avoidance (CSMA/CA) is used.
* Basic concept of DCF is that all WLANs must complete an arbitration process before transmitting a frame.
* Arbitration is mandatory for all APs and STAs staying quiet for variable amount of time before attempting to transmit whichever STA finishes first gains access to the channel.

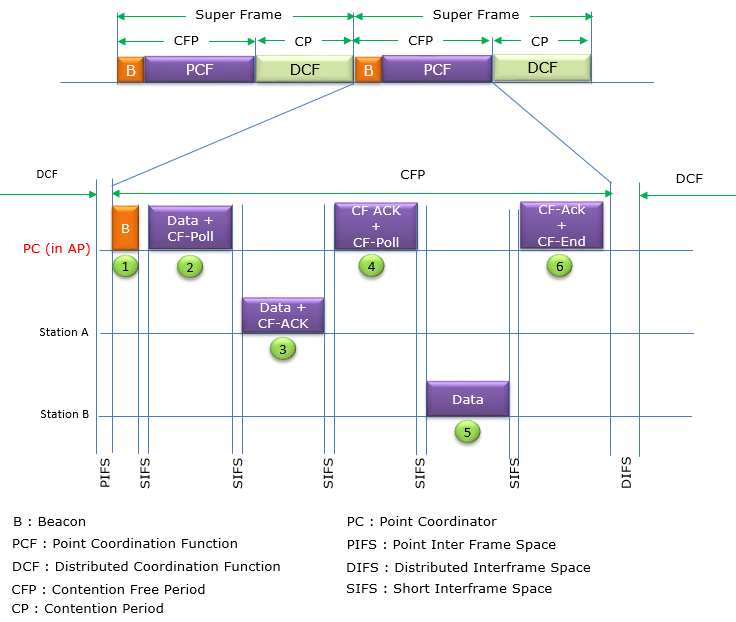


**POINT CORDINATION FUNCTION (PCF)**

* It is an optional function that resides on the top of the mandatory DCF. Both PCF and DCF operate simultaneously.
* It provides channel access to the stations using poll and response method thus eliminating the need of contention.
* The polling is done by the point coordinator (PC) that resides in central access point (AP).
* The station waits for Point Inter–Frame Space (PIFS) before transmission. PIFS is typically smaller than DIFS (Distributed Inter-Frame Space) as used in DCF.
* PC polls in a round – robin method to provide access to the stations in the wireless network.
* AP issues a special control frame called beacon frame to initiate and repeat polling.

**Algorithm**

1. PC sends a beacon frame after waiting for PIFS. The beacon frame reaches every station in the wireless network.
2. If AP has data for a particular station, say station X, it sends the data and a grant to station X.
3. When station X gets the grant from the AP, if it has a data frame for AP, it transmits data and acknowledgement (ACK) to the AP.
4. On receiving data from station X, the AP sends an ACK to it.
5. The AP then sends goes to the next station, say station Y. If AP has data for Y, it sends data and grant to Y, otherwise it sends only grant to Y.
6. On receiving grant from AP, station Y transmits its data (if any) to AP.
7. This process continues for all the stations in the poll.
8. At the end of granting access to all the stations, the AP sends an ACK to the last station. It then notifies all stations that this is the end of polling.



**CONTENTION PERIOD**

The period of time when a station starts transmitting before other stations know that the line is busy.

**CONTENTION FREE PERIOD**

It defines a period of time during which access to the Wireless Medium is free of contention.

**INTER FRAME SPACES (IFS)**

* After each frame transmission 802.11 protocol require an idle period on the medium called Inter Frame Space (IFS).
* The length of the IFS is dependent on previous frame type, following frame type, access category, coordination function in use & PHY type as well.
* The purpose of an IFS is both to provide a buffer between frames to avoid interference as well as to add control and to prioritize frame transmissions.

**SIFS (Shortest Inter Frame Space)**

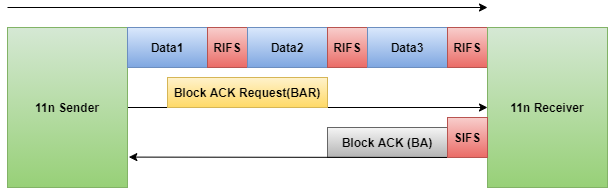
* SIFS are used within all the different coordination functions.
* For 802.11-2007, SIFS is the shortest of the IFSs and is used prior to ACK and CTS frames as well as the second or subsequent MPDUs of a fragment burst.
* However, with 802.11n, a shorter IFS (RIFS) was introduced.
  + SIFS for 802.11b/g/n (2.4 GHz) = 10μS
  + SIFS for 802.11a/n/ac (5 GHz) = 16μS

**RIFS (Reduced Inter Frame Space)**

* RIFS were introduced with 802.11n to improve efficiency for transmissions to the same receiver in which a SIFS-separated response is not required, such as a transmission burst (CFB-Contention Free Burst).

RIFS = 2μS

* 802.11n standard use RIFS & Block Acknowledgement (mandatory in 802.11n).
* RIFS is used only when Block ACK is enabled.
* When Block ACK are used, data frames of a of Contention Free Burst(CFB) may send consecutively without interruption by ACK.
* At the end of Contention Free Burst(CFB), Transmitting station will simply send BAR (BlockACKRequest) & receiving a single Block Acknowledgement (BA).



**DIFS (Distributed Inter Frame Space)**

When a STA desires to transmit a data frame (MPDU) or management frame (MMPDU) for the first time within a DCF network, the duration of a DIFS must be observed after the previous frame’s completion. The duration of a DIFS is longer than both the SIFS and PIFS.

DIFS = SIFS + 2x Slot Time

* Slot Time for 802.11a/n/ac (5 GHz) = 9μS
* Slot Time for 802.11g/n (2.4 GHz – HT or ERP) = 9μS with short preamble
* Slot Time for 802.11g/n (2.4 GHz – HT or ERP) = 20μS with long preamble
* Slot Time for 802.11b/g/n (2.4 GHz – DSS ) = 20μS

**EIFS (Extended Inter Frame Space)**

* The EIFS value is used by STAs that have received a frame that contained errors.
* By using this longer IFS, the transmitting station will have enough time to recognize that the frame was not received properly before the receiving station commences transmission.
* If, during the EIFS duration, the STA receives a frame correctly (regardless of intended recipient), it will resume using DIFS or AIFS, as appropriate

EIFS (in DCF) = SIFS + DIFS + ACK\_Tx\_Time

* EIFS 802.11b/g/n devices using DSS = 364μS
* EIFS 802.11g/n devices using OFDM = 160μS
* EIFS 802.11a/n devices (5GHz) = 160μS

**PIFS (PCF Inter Frame Spaces)**

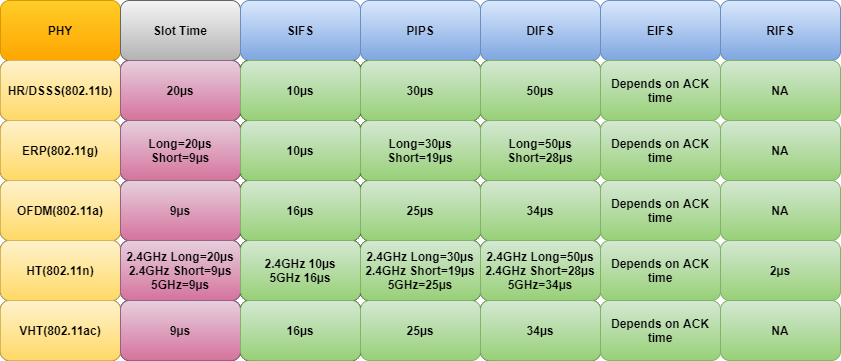
* PIFS are used by STAs during the contention-free period (CFP) in PCF mode.
* Because PCF has not been implemented in 802.11 devices, we cannot see PIFS used for this purpose.
* To gain priority over other STAs during contention, the AP can transmit a Channel Switch Announcement (802.11h) frame after observing a PIFS.

PIFS = SIFS + Slot Time

**AIFS (Arbitration Inter Frame Space)**

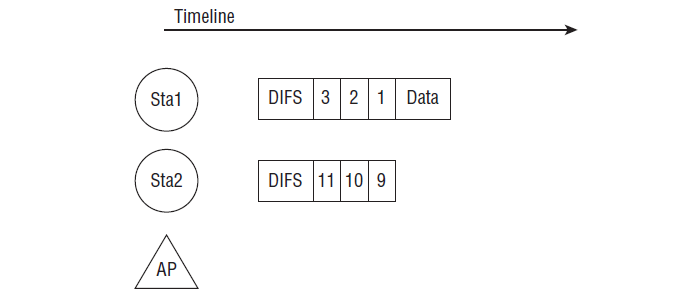
* The AIFS shall be used by QoS STAs to transmit all data frames (MPDUs), all management frames (MMPDUs), and some control frames: PS-Poll, RTS, CTS (when not transmitted as a response to the RTS), BlockAckReq, and BlockAck (when not transmitted as a response to the BlockAckReq).
* The number of slot times used in the AIFS is called the Arbitration Inter Frame Space Number (AIFSN).
* 802.11e specifies 4 access categories (AV\_VO : Voice, AC\_VI : Video, AC\_BE : Best Effort & AC\_BK : Background).
* Voice & Video category use 2 slot times by default.
* Best Effort category use 3 slot times
* Background traffic use 7 slot times by default.

AIFS[AC] = AIFSN[AC] × Slot Time + SIFSTime



**RANDOM BACKOFF TIMER**

* Consider two stations having data to send, the IFS is not enough to determine which device will have access to the channel is busy and then both the devices stay quiet for the length of a DIFS once the channel becomes idle. The problem then becomes making sure that both devices do not start transmitting data simultaneously thereby causing a collision.
* The mechanism that prevents collisions by differentiating 802.11 channel access is the random backoff.
* Random backoff is the quiet period before the frame transmission.
* APs and STAs count for a random chosen number of slot times and counting down up to zero. Once the number of slot hits zero, AP or STA is allowed to transmit the frame.
* The lower limit of timer is 0.
* The upper limit of timer is contention window (CW).



**Contention window (CW)**

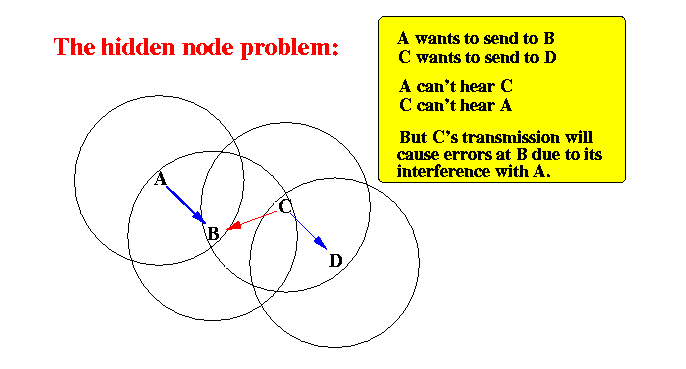
* Contention window is an amount of time divided into slots.
* A station that is ready to send chooses a random number of slots as its wait time.
* In contention window the station needs to sense the channel after each time slot.
* If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.
* CW is derived by 2x – 1. x is the retransmission counter. x increments after each failed frame.

|  |  |  |
| --- | --- | --- |
| Modulation technique | x | Contention window |
| DSSS | 5 | 31 |
| OFDM | 4 | 15 |
| DSSS/OFDM | 10 | 1023 |

|  |  |  |
| --- | --- | --- |
| Standards | CWmin | CWmax |
| 802.11b | 31 | 1023 |
| 802.11a | 15 | 1023 |
| 802.11g | 31/15 | 1023 |
| 802.11n | 15 | 1023 |

**HIDDEN NODE PROBLEM**

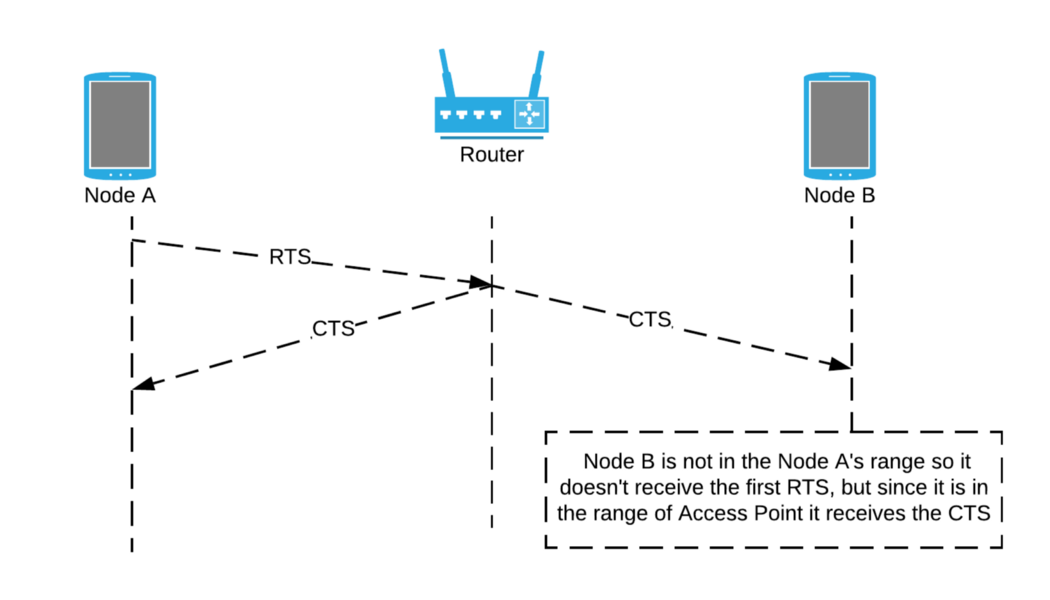
The hidden node problem or hidden terminal problem occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP.



When nodes A and C start to send packets simultaneously to the access point B. Because the nodes A and C cannot receive each other's signals, so they cannot detect the collision before or while transmitting, carrier-sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point.

**SOLUTIONS**

* RTS/CTS frame exchange
* Increase transmitting power from the nodes
* Use omnidirectional antennas
* Remove obstacles
* Move the node
* Use protocol enhancement software
* Use antenna diversity
* **RTS/CTS frame exchange**



When a node wants to send data, it will first send the RTS signal. If the Access Point is ready to receive the data (if it is not communicating with any other node) it will send back the CTS signal. It is a little bit confusing to understand, but you will get a clear understanding from the following diagram.

Node B is not in the Node A’s range, so it does not receive the first RTS, but since it is in the range of Access Point, it receives the CTS.

When a node receives a CTS signal from an Access Point without a RTS signal, it will understand that CTS signal is for a hidden terminal, so it will not transfer the data.

* **Increasing transmitting power**

Increasing the transmission power of the nodes can solve the hidden node problem by allowing the cell around each node to increase in size, encompassing all the other nodes. This configuration enables the non-hidden nodes to detect, or hear, the hidden node. If the non-hidden nodes can hear the hidden node, the hidden node is no longer hidden. Because wireless LANs use the CSMA/CA protocol, nodes will wait their turn before communicating with the access point.

* **Omnidirectional antennas**

Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks (e.g., dedicated point-to-point connections). Use omnidirectional antennas for widespread networks consisting of more than two nodes.

* **Removing obstacles**

Increasing the power on mobile nodes may not work if, for example, the reason one node is hidden is that there is a concrete or steel wall preventing communication with other nodes. It is doubtful that one would be able to remove such an obstacle, but removal of the obstacle is another method of remedy for the hidden node problem.

* **Moving the node**

Another method of solving the hidden node problem is moving the nodes so that they can all hear each other. If it is found that the hidden node problem is the result of a user moving his computer to an area that is hidden from the other wireless nodes, it may be necessary to have that user move again. The alternative to forcing users to move is extending the wireless LAN to add proper coverage to the hidden area, perhaps using additional access points.

* **Protocol enhancement**

There are several software implementations of additional protocols that implement a polling or token passing strategy. Then, a master (typically the access point) dynamically polls clients for data. Clients are not allowed to send data without the master's invitation. This eliminates the hidden node problem at the cost of increased latency and less maximum throughput.

* **Cell network**

With cellular networks the hidden node problem has practical solutions by time domain multiplexing for each given client for a mast, and using spatially diverse transmitters, so that each node is potentially served by any of three masts to greatly minimize issues with obstacles interfering with radio propagation.