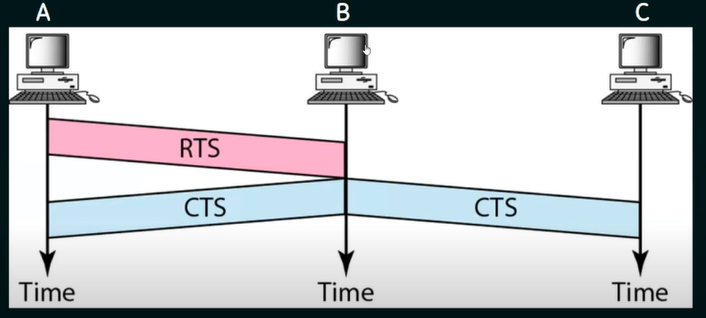
Multiple Access with Collision Avoidance (MACA)

1. 802.11 addresses these two problems (hidden and exposed terminal problems) with an algorithm called Multiple Access with Collision Avoidance (MACA)
2. Sender and receiver exchange control frames with each other before the sender actually transmits any data.
3. This exchange informs all nearby nodes that a transmission is about to begin
4. Sender transmits a Requets to Send (RTS) frame to the receiver
   1. The RTS frame includes a field that indicates how long the sender wants to hold the medium Length of the data frame to be transmitted
5. Receiver replies with a Clear to Send (CTS) frame
   1. This frame echoes this length field back to the sender.

Collision Avoidance

1. Any node that sees the CTS frame knows that
   1. It is close to the receiver, therefore
   2. Cannot transmit for the period of time it takes to send a frame of the specified length
2. Any node that sees the RTS frame but not the CTS frame
   1. Is not close enough to the receiver to interfere with it, and
   2. So is free to transmit
3. The idea of using ACK in MACA is proposed in **MACAW: MACA for Wireless LANs**
4. Receiver sends an ACK to the sender after successfully receiving a frame
5. All modes must wait for this ACK before trying to transmit
6. If two or more nodes detect on idle and try to transmit an RTS frame at the same time
   1. Their RTS frame will collide with each other
7. 802.11 does not support collision detection
   1. So the senders realize the collision has happened when they do no receive the CTS frame after a period of time
   2. In this case, they each wait a random amount of time before trying again
   3. The amount of time a given node delays is defined by the same exponential backoff algorithm used on the Ethernet.

Demonstration



Station C doesn't hear RTS from A, but it does hear CTS from B, so it knows something is up.