Wireless Networks

Lecture 8:
WLAN Frames Types &
WLAN Connectivity

MAC

To maintain some safety in data communications, certain rules and guidelines must be established and followed. This is especially important in wireless communications because of the nature of the medium used for the communications—air or space. The rules and guidelines are specified at different layers of the OSI model.

MAC

MAC is a sublayer of the OSI's Data Link layer. The MAC sublayer is basically responsible for providing addressing and medium access control mechanisms that make it possible for several nodes to communicate in a network.

The MAC functions are used to control and manage access to the transmission medium in a communications system.

MAC

Controlling the access of stations plugged into a wired Ethernet LAN (IEEE 802.3) is relatively simple because of the use of cables. All nodes plugged into the same network can easily sense the presence or absence of an electric current in their cables. The electric current here implies the data transmission. To coordinate access to the LAN medium, LAN stations use Carrier Sense Multiple Access with Collision Detection (CSMA/CD). The key word here is "**detection**".

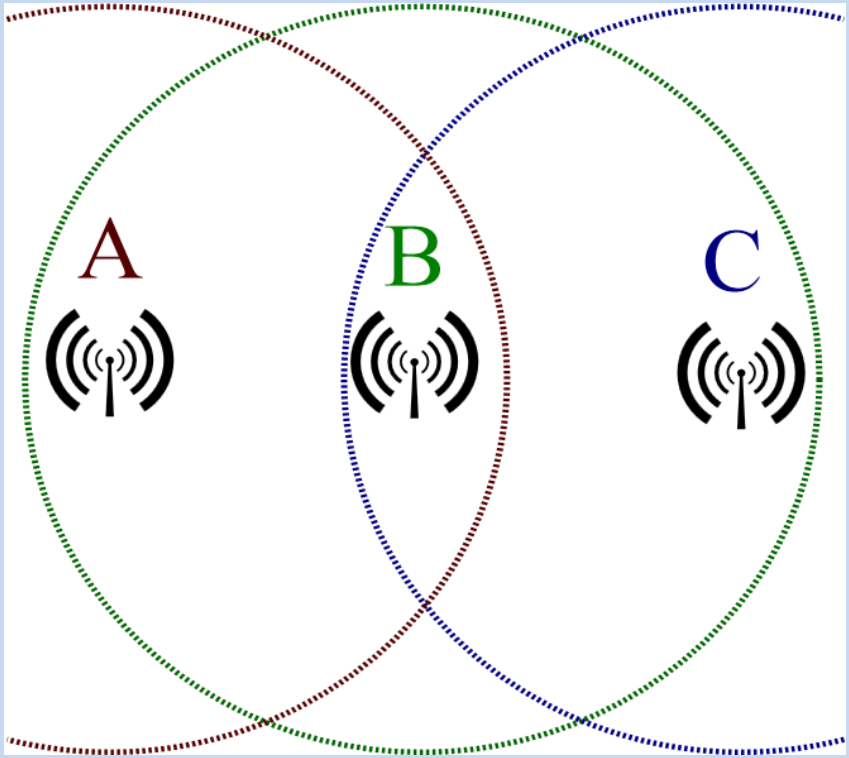
The rules that govern the IEEE 802.11 WLANs can not easily use same method for managing access to the shared medium used in wired LANs, one reason behind this is the absence of physical wires.

MAC

The Stations in a wireless network cannot always be guaranteed to be within earshot of each other so that they can hear (or detect) when the other STAs are transmitting. This phenomena is known as the “hidden node” problem in RF communications. Furthermore, the transmission may not even be destined for the hidden node, but it still needs to use the common transmission medium shared by all the nodes.

Hidden nodes in a wireless network are nodes that are out of range of other nodes or a collection of nodes

MAC



“Hidden Node Problem”

- A,C are Stations
- B is the Access point (AP)

MAC

In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as A, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, C. These nodes are known as hidden. The problem is when nodes A and C start to send packets simultaneously to the access point B. Because the nodes A and C are out of range of each other and so cannot detect a collision 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.

To overcome the hidden node problem, RTS/CTS handshaking is implemented in conjunction with the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme

MAC

The second reason is because the radio in most wireless LAN hardware is capable of operating in either a transmitting or receiving mode at one time—it can't usually do both at the same time. For the wireless hardware to be able to detect collisions (receive mode) while it is sending data (transmit mode), it needs to include a radio that offers such capabilities. And as has already been mentioned, this is not the case in wireless LAN hardware.

MAC

So instead of attempting to detect when the medium is available for use, 802.11based systems take a different way by trying to avoid any type of collision in the first place. This is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), and the key word here is "**avoidance**."

MAC

A popular method for implementing CSMA/CA in wireless LANs is known as the Distributed Coordination Function (DCF). The following steps show how three sample wireless Stations (STA-a, STA-b, and STA-c) might negotiate access to the wireless medium. Note that this is only one of the several methods by which CSMA/CA can be implemented.

MAC

1. STA-a needs to access the wireless medium, so it puts its radio in receiving mode to see if any other STAs are currently transmitting anything.

2. If STA-a sees that the medium is in use by STA-b, it waits until STA-b is done with its transmission. The amount of time that STA-a waits is determinate.

3. STA-a will attempt to transmit again by first checking to see if the medium is available. If so, STA-a will send out a special MAC frame called a **Request To Send (RTS)** frame. Also called a **control frame**, this is one of several MAC frame types.

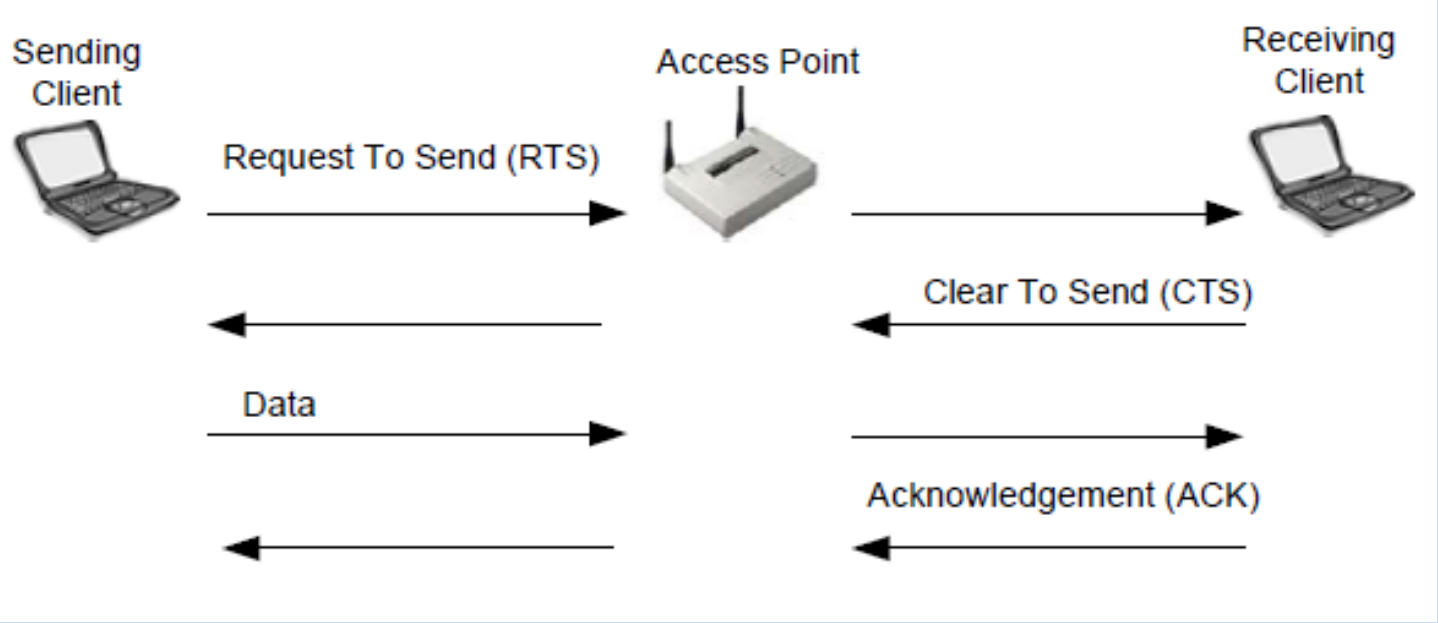
MAC

4. STA-c will see the special frame sent from STA-a and in turn send a **Clear To Send (CTS)** frame. STA-a will send its message to STA-c.

5. For the communication to be considered successful, STA-c needs to send an acknowledgement confirming that it indeed received the message sent by STA-a. This message is carried in another **control frame** type called an **Acknowledgment (ACK)** frame. This is also known as positive acknowledgement.

6. If, for whatever reason, STA-a does not receive an ACK message from STA-c, it resends the message.

MAC



RTS/CTS handshaking

MAC Frame Types

Depending on their function, IEEE 802.11 MAC frame types can be grouped into three categories:

- **Control frames.**
- **Management frames.**
- **Data frames.**

Control Frames

These most basic frame types are very important for all WLAN communications and are used to support the delivery of the other (management and data) MAC frame types. All the wireless STAs must be able to see the control frames—in other words, the information in the control frames is not secret or classified in any way.

Control frames are used, for example, when a wireless STA needs to negotiate and gain access to the WLAN using CSMA/CA. The types of control frames are the Request to Send (RTS), Clear to Send (CTS), and Acknowledgment (ACK) frames.

Management Frames

These frame types are used for management purposes on the WLAN, where they play a very important role. Management frames are used by wireless STAs whenever an STA officially wants to participate or discontinue its participation in the network and for other miscellaneous housekeeping purposes. Here are some sample management frame types:

- **Beacon frame:** A very important management MAC frame type, it performs various functions, such as time synchronization among the STAs; it also stores the value of the SSID being used, and specifies the data rates supported on the WLAN, among other things.
- **Association Request frame:** These frames are sent by the STA to request association with the AP.

Management Frames

- **Association Response frame:** These frames contains the AP's response to the STA regarding the STA's association request. It is either a yes or no.
- **Re-association Request frame:** These frames are used by STAs whenever they need to be re associated with an AP.
- **Re-association Response frame:** These frames are sent by the AP in response to the STAs request to re associate with the AP.
- **Authentication frame:** These frames are used whenever a STA needs to participate in or join a BSS. Mere association is not nearly enough— the STA needs to be authenticated to make full use of the BSS. The STA uses authentication frame types to confirm its identity.

Management Frames

- **De-authentication frame:** Authenticated STAs use these frame types to signal their intention to terminate the authenticated (secure) communications.
- **Disassociation frame:** This frame is sent by a STA that is associated with an AP to inform the AP that it wants to discontinue the association. Note that this is not a request, and as such a response or acknowledgment or confirmation is not required from the AP.
- **Probe Request frame:** STAs send probe request frames whenever they need to discover information about other STAs. Such information might include the capabilities of the other STA or information about the supported data rates.
- **Probe Response frame:** This frame carries the response to probe requests.

Data Frames

These frame types are responsible for transporting the actual data payload to and from the communication end points.

WLAN Connectivity

In order to enable the wireless station for communication with the wireless network and exchange the traffic, the station needs to pass both authentication and association processes. Briefly these processes steps are:

1. The station will send a broadcast Probe request frame to know the available APs to connect with.
2. All APs in range will reply with Probe response frame.
3. The station will send Authentication frame to the AP which the station decides to connect with.
4. The AP will send Authentication reply.
5. If the Authentication process finished successfully, the station will send Association request frame to the AP.

WLAN Connectivity

6. The AP response with Association response frame.
7. If the Association process finished successfully, the station will be able to pass the traffic to the AP, then to the destination.

As a result to the above description, there are three possible states each wireless station can be with, which is also the hierarchy in development of 802.11 network connection:

State1. The initial state: not authenticated and not associated.
State2. Authenticated but not associated.
State3. Authenticated and associated.

These three states can be found in the Infrastructure wireless network where all stations start from state 1, and the transmission of data not permitted until state 3 passed successfully, while in Ad Hoc networks, there is neither AP, nor association, so it reaches state2 only

WLAN Connectivity

- **Authentication:**

Is the process of proving the identity to determine whether the station is allowed to access the network or not, In IEEE 802.11 WLAN there are two authentication mechanisms, Open Authentication and Shared Key Authentication, both of these mechanisms make use of Authentication frame.

- **Association:**

After the Authentication process is completed successfully, the station will associate with the AP to gain full access to the network and exchange the traffic.

Thank You