Ethernet & Wireless

Terms	Definitions
Station	Device capable of using 802.11 protocol.
IEEE 802.11	Also known as WiFi, specifies the set of MAC and PHY protocols to implement a WLAN.
Channel	Specific frequency (in radio spectrum) used by WiFi to transmit and receive data.
Medium	PHY used to transmit data between devices.
Collisions	Overlap of transmitted signals caused by simultaneous transmission of data by devices.
Round-trip delay	Time taken for a packet to reach a receiver from the sender, back and forth.
Access Point	Device that allows wireless devices to connect to a Wired Network, using Wi-Fi.
Basic Service Set	Unit of a WLAN that consists of a single Access Point and the stations connected to it.
Extended Service Set	Unit of a WLAN that consists of several Basic Service Sets connected together.
MAC Protocol Reliability	Ability of the Media Access Control (MAC) to deliver data packets from a node to another.
Service Set Identifier	Unique name that identifies a specific wireless connection.
Wireless Network Interface Card	Type of hardware installed on devices that enables it to connect to a wireless connection.

CSMA

What is CSMA?

CSMA (Carrier-Sense Multiple Access) is a common MAC protocol in many types of Networks.

Where is it used?

In Networks with a small number of devices that need to communicate with each other.

Why is it used?

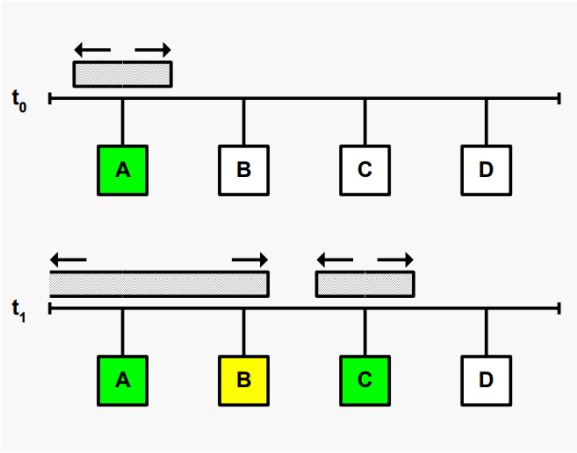
Because it removes the need to use a central controller (device used to manage and coordinate other devices' activities) or other coordination mechanisms.

What are their particularities?

Is primarily designed to transmit and receive data in the same channel.

The sending station checks the availability of a medium (Carrier-Sense), only transmitting data if it's not being occupied. This reduces but does not nullify collisions, since, due to the distance of stations, it's possible for devices to transmit data before detecting the medium is being used.

Example of Collision



On time t_0, station A starts transmitting data.

On time t_1, station B tries to transmit data, detects the medium is being used, so it stops.

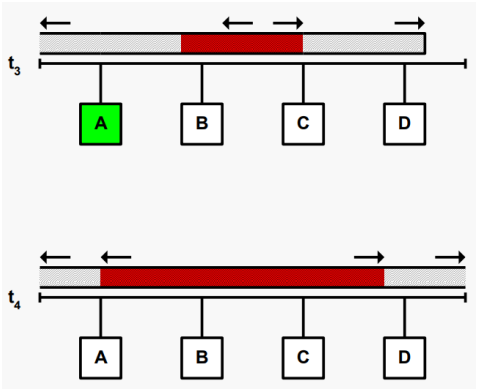
Simultaneously, station C tries to transmit, doesn't sense the medium is being used, so continues.

What happens after a collision?

On time t_3, station C detects the collision and stops transmitting data.

The same event does not occur in station A, since it has not yet detected the collision.

On time t_4, station A, finally, stops transmitting after detecting the collision.



What can increase collisions?

High traffic levels. A large number of devices increases the chances of stations transmitting data simultaneously.

Long distances. Two stations separated by long distances increase the chances of the device not detecting that the channel is being used.

Poor signal quality. If the signal is poor, a device may not be able to detect that a channel is being used.

Incorrect configuration of the Network.

CSMA/CD

What is the difference between CSMA and CSMA/CD?

Basically, CSMA/CD (Carrier-Sense Multiple Access with Collision Detector) is a variant of CSMA with an extra step for handling collisions.

What is this extra step?

First, before transmitting a frame, a station checks if the medium is free for an IFS (Inter-Frame Spacing) time period. If busy, it waits for another IFS time period, and so on.

Again, this does not nullify collisions. If stations send data almost at the same instant, they can cause a collision. In this case, instead of stopping definitively, they will send a JAM signal and wait a random period of time before attempting transmission again (this is called backoff).

What is a JAM signal? (Unimportant)

It's a special signal used to disrupt the normal operation of a communication network. Normally it's used to reset the network, forcing devices to re-synchronize with each other.

In some cases it can be transmitted intentionally, to identify troubleshooting or test resilience of the network, in others it can be transmitted unintentionally, due to interference in the network.

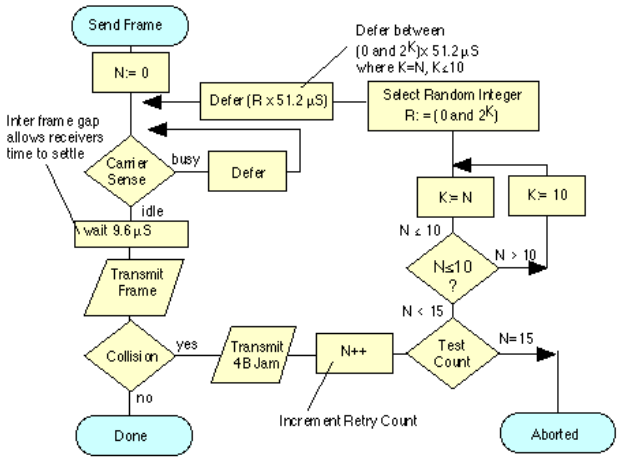
Where is it used?

In Networks shared by multiple devices where there is a possibility of occurrence of collisions.

Why is it used?

To ensure that collisions are resolved quickly and efficiently, ensuring that the network continues functioning normally.

Process of CSMA/CD Illustrated



First the station attempts to send data, being the number of retries (N) equal to 0.

Checks if the medium is idle (Carrier Sense). If not it awaits an IFS time period before attempting to send a frame again.

If so, it checks transmission for an IFS time period and transmits if the medium is idle.

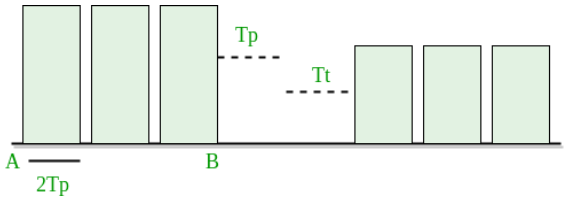
If collision doesn't happen the process is done. Else, it transmits a JAM signal, increments the retry count by 1.

If count equals 15, the process is aborted.

Else, taking in account the count of the retries, it assigns a random value to be used as time delay, continuing the loop.

How to calculate useful time of CSMA/CD? (Unimportant)

$$a = Tt / (C \times Tp + Tt + Tp)$$



a - useful time.
Tt - Transmission time
Tp- Propagation time
C - Number of collisions

Wireless Networks

How do WLAN standards increase over time?

The data rate increases and the frequency band switches according to the needs of the time.

Comparison

Frequency Bands	2.4 GHz	5 GHz
Speed	Generally, slower.	Generally, faster.
Range	Longer range.	Shorter range.
Preferred for	Covering larger areas. Penetrating solid objects. Better compatibility with devices.	Covering smaller areas. Faster connection. Less crowded with devices.

What are the components of a WLAN?

A station. An access point. A Basic Service Set (Can cover a home). An extended service set (Can cover a Campus). All described in page 1.

What are the differences between Wireless and Wired?

Wired is faster, more secure (since it's harder for outsiders to intercept data) and can detect collisions (typically used CSMA/CD). Wireless has more range, easier mobility and cannot detect collisions (CSMA has problems).

If Wireless cannot detect collisions how does it work?

Stations work in Half-Duplex, where transmission and reception take turns, or in Full-Duplex, where transmission and reception can happen simultaneously.

Nodes

What are hidden nodes?

Wireless devices that are unable to directly communicate with each other due to physical obstructions or the limited range of their wireless radios.

How do hidden nodes communicate?

Through intermediate nodes, such as access points or routers.

What problems can hidden nodes cause?

Since devices are unable to communicate, they put themselves at risk of collisions, without even noticing it happened.

What workarounds exist for hidden nodes?

Detect collisions in the receiver instead of the sender.

“Virtual Carrier sense”. Sender asks the receiver if it’s receiving traffic, and in case of absence of answer (possible hidden node), he assumes the channel is busy (MACA).

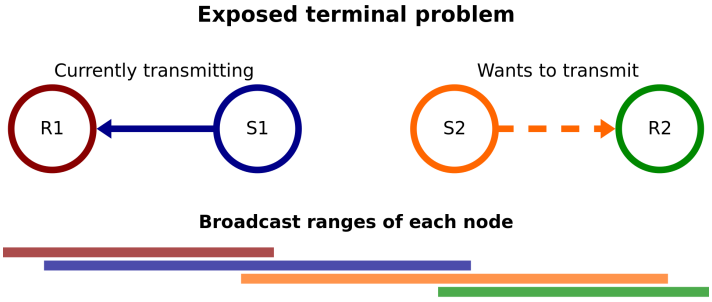
What are exposed nodes?

Opposite of hidden nodes. Wireless devices that are able to directly communicate with each other without the need for intermediate nodes.

What is the exposed nodes problem?

The transmission is capable of occurring without collision, but since S2 detects S1 in transmitting data, it stops unnecessarily.

R1 and R2 are considered exposed nodes.



MACA

What is MACA?

MACA (Multiple Access with Collision Avoidance) is a protocol used to allow multiple devices to transmit and receive data in a shared medium.

How does MACA avoid collisions?

Through the use of signaling packets. Firstly, sends a RTS (Request before send), which is a small packet sent before transmitting, and secondly, waits for an CTS (Clear to send) from the receiver, signaling the right to transmit.

What do signaling packets contain?

Sender address. Receiver address. Packet Length.

When is MACA used?

In Network scenarios with a large amount of traffic and collisions.

Does MACA avoid all Collisions?

No. MACA cannot avoid collisions of RTS and CTS packets.

MAC Reliability

Why are Wireless connections so prone to errors?

Because transport is not reliable if transmission success is not verified.

How do we correct this problem?

When a station receives data it responds with an ACK (Acknowledgment). If the sending station does not receive this ACK, it will retransmit the data. Other devices will also wait for the ACK to transmit data, this way avoiding collisions.

Practical Part

How do we start a Wireless Connection?

1. The Station scans/probes for an AP.

2. The Station performs authentication.

3. The Station performs association.

What are the three types of frames?

1. Control: RTS, CTS and ACK.

2. Management: Association, Authentication, Beacon (Frame used to advertise presence of AP and provide information of the Network, including the SSID (Service Set Identifier)).

3. Data.

How do we notice the difference?

Through the header.

How can the Scanning be performed?

1. Passive Scanning. A station scans the channel for a Beacon Frame, with information for WNICs (Wireless Network Information Card) within range.

2. Active Scanning. Through probe requests from a station to another, where all AP within reach will respond, asserting this way that station finds an AP.

How can Authentication BE performed?

1. Station sends an authentication frame with MAC address (identity), and AP responds with an ACK or NACK (Negative Acknowledgement).

2. Shared Key Authentication. Stations receive a shared key through a secure channel. When the WNIC sends the authentication request it will receive an authentication frame from the AP with a text. The WNIC sends an authentication frame with the text encrypted with the key. The AP verifies it and sends an ACK or NACK.