

**CSMA / CA**

**definición y mecánica del protocolo**

Con las siglas **CSMA** se describe un proceso fundamental para regular la

comunicación de los integrantes de una red que usan **un mismo medio de transmisión estructurado de forma descentralizada**.

Comprende **tres variantes distintas** en función del medio de transmisión: CSMA/CA, [CSMA/CD](https://www.ionos.es/digitalguide/servidores/know-how/csmacd/) y CSMA/CR. Mientras la primera se usa principalmente en redes inalámbricas, CSMA/CD se creó para [Ethernet](https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/). CSMA/CR se emplea con el protocolo de comunicación Controller Area Networks (CAN), usado principalmente en máquinas y coches.

Para poder entender realmente en qué consiste el protocolo Carrier Sense Multiple Access with Collision Avoidance (acceso múltiple por detección de portadora y prevención de colisiones) es necesario analizar cada una de sus partes:

* **Carrier Sense** (CA): la idea principal es que los miembros de una red solo pueden enviar datos a través de ella cuando el medio de transmisión no esté ocupado. Para que esto sea posible en todo momento se está realizando un reconocimiento de la red para comprobar el estado del canal (detección de portadora). Solo cuando esté libre, se pueden enviar los datos.
* **Multiple Access** (MA): distintos nodos comparten el mismo medio de transmisión. Por eso es determinante que se atengan a un mismo protocolo para que la comunicación fluya.
* **Collision Avoidance** (CA): para prevenir colisiones se recurre a una compleja organización del tiempo que permite evitar que dos o más miembros de una red comiencen la transmisión a la vez. Eso sí, en el caso de que los datos se superpongan, se reconoce el problema en la transmisión y se inicia de nuevo el envío.

**Índice**

1. [¿Qué es CSMA/CA y cuál es su función?](https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/#c136060)
2. [CSMA/CA vs. CSMA/CD](https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/#c136064)
3. [CSMA/CA: mecanismos para su funcionamiento](https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/#c136065)
4. [Ventajas e inconvenientes de CSMA/CA](https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/#c136071)
5. [¿Qué es el acceso múltiple coordinado?](https://www.ionos.es/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/#c136073)

**¿Qué es CSMA/CA y cuál es su función?**

Todos los integrantes de una red de área local (LAN) comparten el mismo medio de transmisión, esto es, un cable denominado bus. En las **redes inalámbricas** (WLAN), como es lógico, no se recurre a ningún cableado, aunque no por ello se deja de recibir y enviar información a todos los dispositivos mediante un único medio de transmisión constituido por **radiofrecuencias.** En este sentido, una red WLAN (IEEE 802.11) se puede equiparar a las redes Ethernet semidúplex y, como en ellas, es necesario un protocolo que regule el uso del medio.

La regla más importante a cumplir en estos procesos de comunicación establece que **dos o más dispositivos** –también llamados a lo largo del texto nodos, estaciones o miembros– **no pueden realizar envíos al mismo tiempo**. Cierto es que esta norma es aplicable a otras situaciones comunicativas. Imaginemos una comida en familia: si todos hablan al mismo tiempo, es imposible entender una palabra y el proceso comunicativo falla. En la red, las aportaciones de cada miembro, que se materializan en forma de paquetes, también pueden superponerse unas a otras. Se produce entonces una **colisión**, es decir, los paquetes se encuentran e invalidan su contenido, por lo que la comunicación no tiene lugar.

CSMA/CA trata de reducir el riesgo de colisión y al mismo tiempo introduce un plan de actuación en caso de que se produzca. El protocolo es especialmente importante en las transmisiones realizadas en redes inalámbricas pues, debido a la misma naturaleza de la tecnología que utilizan, la circulación de los envíos es más desorganizada que la de los realizados por cable. Además, en las redes descentralizadas es esencial que todos los miembros sigan el mismo reglamento y **organicen la comunicación entre ellos**.

**El problema del nodo oculto**

El problema del terminal oculto surge cuando empiezan a emplearse redes inalámbricas. Los nodos en una red inalámbrica tienen un **alcance limitado**, por lo que puede ocurrir que los miembros de una misma red no se perciban entre sí (en lenguaje técnico, *escucharse*) al estar ambos en diferentes áreas de alcance.

De hecho, es completamente factible que dos nodos que no se escuchen quieran llegar al mismo tiempo a otro situado entre ellos, de tal modo que se realicen transmisiones que corren el riesgo de superponerse en el nodo destinatario y, dado el caso, perderse todos los datos (es decir, colisionan). Además, como ninguno de los emisores son conscientes de que se ha producido una colisión, no vuelven a intentar el envío de los datos, pues asumen que han llegado correctamente. CSMA/CA no puede por sí solo eliminar el problema del nodo oculto, para lo que debe recurrir a un protocolo complementario: RTS/CTS (Request to Send y Clear to Send).

**CSMA/CA vs. CSMA/CD**

CSMA/CA adapta los procedimientos de gestión de colisiones CSMA/CD utilizados en las redes semidúplex de Ethernet a las necesidades de las redes inalámbricas. Y es que el protocolo CSMA/CD **entiende que las colisiones son naturales** y establece un **mecanismo** para que los miembros de la red, en caso de que se produzca una colisión, puedan evitar que vuelva a producirse en un segundo intento. El mecanismo es el siguiente: se establece un periodo de tiempo aleatorio de espera (*backoff* o mecanismo de contienda) al que deben atenerse los nodos tras haberse producido una transmisión fallida. De este modo se evita que los miembros que han realizado las citadas transmisiones vuelvan a coincidir en el momento del envío.

No obstante, una red inalámbrica no es tan fácil de gestionar como una alámbrica. Las colisiones pueden estar causadas por un segundo emisor (C) que se **encuentra fuera del alcance del primero** (A) y que inicia simultáneamente el envío al mismo receptor (B). Ninguno de los dos emisores puede percibir los intentos de envío del otro al encontrarse ambos en diferentes áreas de alcance. Por eso, el objetivo principal en este tipo de redes debe concentrarse en **reducir la probabilidad de colisiones**. Para ello, el protocolo CSMA/CA recurre también al mecanismo de contienda, pero lo emplea antes del primer intento de envío con la intención de reducir la probabilidad de que los miembros de la red empiecen al mismo tiempo una transmisión que desencadene una colisión.

**CSMA/CA: mecanismos para su funcionamiento**

La idea que se esconde tras el protocolo CSMA/CA se resume en la oración **“Listen before talk”** (escucha antes de hablar), es decir, hay que comprobar primero si el canal está libre antes de que el nodo empiece con la transmisión, aunque esto es solo un primer paso. El resto de funciones de este protocolo trata de evitar las colisiones en todo lo posible.

**Función de coordinación distribuida (DCF)**

La función de coordinación distribuida (DCF) regula en CSMA/CA el periodo de espera de los nodos antes de iniciar la transmisión en un medio desocupado. DFC también adjudica a las estaciones ranuras de tiempo aleatorias (time slots) para acciones que tienen lugar posteriormente, consiguiendo **una estructuración coordinada de los tiempos de espera**. Este procedimiento es la clave en la prevención de colisiones o collision avoidance. Para su creación, DCF recurre a determinados intervalos:

* **DCF Interframe Space** (DIFS): si un nodo de la red **quiere empezar** una transmisión, en primer lugar escucha el medio. Si descubre que el medio está libre, espera un intervalo DIFS. Este indica a CSMA/CA que en el momento en el que se inicie la nueva trama ningún otro nodo dentro del alcance va a estar transmitiendo información. El DIFS resulta del SIFS y de un espacio de tiempo duplicado y tiene entre 28 y 50 µs de longitud.
* **Ventana de contienda o contención** (contentwindow): cuando las estaciones se aseguran de que el medio está libre, esperan un periodo de tiempo aleatorio antes de empezar con el envío. Este espacio de tiempo es lo que se conoce como ventana de contención y se duplica con cada colisión. Se corresponde con el Binary Exponential Backoff (BEB) del protocolo CSMA/CD.
* **Short Interframe Space** (SIFS): una vez que los paquetes de datos llegan al nodo receptor, este manda una notificación al emisor, siempre y cuando se use RTS/CTS. No obstante, este nodo receptor también espera un periodo de tiempo establecido antes de proceder al envío de la confirmación. SIFS hace referencia al tiempo que se necesita para procesar un paquete de datos. Su duración depende del estándar IEEE-802.11 utilizado y oscila entre 10 µs y 16 µs.

Hecho

Una **ranura temporal** (slot time) se corresponde con el tiempo que los datos necesitan para recorrer el largo de la red. En las redes inalámbricas depende del estándar utilizado y oscila entre los 9 µs y los 20 µs.

**Request to Send y Clear to Send (RTS/CTS)**

Las tramas Request to Send (RTS) o petición para enviar y Clear to Send (CTS) o permiso para enviar componen el protocolo complementario de CSMA/CA conocido como RTS/CTS y conforma un **procedimiento que tiene lugar antes de la transmisión de datos**. Tras comprobar que el medio está libre, el emisor envía una trama RTS al destinatario, que también escuchan todos los miembros de la red dentro de su alcance, indicándole su deseo de iniciar una transmisión. Es decir, comunica que el medio de transmisión va a estar ocupado durante cierto tiempo.

El receptor envía a modo de respuesta al emisor una trama CTS donde se transmite también a todos los miembros dentro de su alcance que el medio de transmisión va a estar ocupado. Además, indica al emisor que tiene vía libre para realizar la transmisión. Solo entonces el dispositivo inicia el envío.

Además, dado que los nodos en una red inalámbrica no pueden detectar colisiones u otro tipo de irregularidades en la transmisión, es importante que el receptor mande también una confirmación de que el paquete de datos ha llegado correctamente. Para ello recurre a la trama ACK. Si ACK no llega, el emisor deduce que ha debido surgir algún problema durante el envío y vuele a enviar los datos, pues **tiene preferencia** para usar el medio, es decir, no tiene que esperar hasta que el canal esté de nuevo libre.

Los tres tipos de tramas (RTC, CTS y ACK) están compuestos por diferentes campos:

* **Campos de control de tramas**: cada campo de control de tramas contenido en una trama 802.11 mide 2 bytes (16 bits) y se divide en los siguientes elementos:
  + Versión del protocolo: ofrece la versión del protocolo utilizado.
  + Tipo: especifica si se trata de una trama de control (RTS/CTS y ACK), una trama de datos o de gestión.
  + Subtipo: de las 25 subcategorías existentes, especifica el tipo de trama.
  + Para Distribution System: establece si el sistema se dirige a un sistema de distribución.
  + De Distribution System: establece si la trama procede de un sistema de distribución.
  + Más fragmentos: elemento importante en las tramas de gestión y de datos. Solo en caso de que sigan varias tramas.
  + Retry: especifica si ya se ha intentado mandar la trama y, en caso afirmativo, el número de intentos.
  + Power Management: muestra el modo de ahorro de energía.
  + Más datos: especifica que se deben enviar más datos.
  + WEP: informa de si los datos están cifrados con WEP.
  + Orden: comunica al destinatario si los datos se envían en el orden correcto.
* **Duración**: establece el tiempo que el emisor necesita para el envío de información. Este campo es esencial para el mecanismo Network Allocation Vector que, como se verá más adelante, inhibe un dispositivo que no está transmitiendo durante el periodo aquí estipulado. También este campo ocupa 2 bytes.
* **Dirección del receptor**: contiene la dirección [MAC del destinatario](https://www.ionos.es/digitalguide/servidores/know-how/direccion-mac/) (6 bytes).
* **Dirección del emisor**: contiene la dirección MAC del emisor (6 bytes); solo necesaria para RTS, no para CTS y ACK.
* **Control de secuencia de trama (FCS)**: la secuencia de caracteres de verificación de bloques, de 4 bytes, es una suma de verificación. Permite al nodo destinatario comprobar si la trama de datos ha llegado como había sido planeado. El emisor calcula la suma a partir de los datos de la trama, proceso que imita el destinatario una vez ha recibido los datos. La transmisión se habrá realizado con éxito si el resultado obtenido por el receptor coincide con lo que el emisor agregó como FCS a la trama.

RTS, CTS y ACK contienen todos los campos a excepción del que muestra la dirección del emisor, pues solo es útil en la primera toma de contacto para que el receptor tenga constancia del nodo con el que se está comunicando.

Si se activa el protocolo RTS/CTS complementario de CSMA/CA, se consiguen reducir las colisiones a la trama RTS inicial. Cabe la posibilidad de que dos nodos envíen al mismo tiempo la trama RTS correspondiente. En tal caso el receptor no puede responder con una trama CTS. Es así como RTS resuelve **el problema del nodo oculto** pues, aunque los dos emisores que envían la trama RTS al mismo tiempo no se pueden escuchar al no estar dentro del mismo alcance, solo ponen en riesgo las tramas RTS y no los datos reales. Entonces entra en acción CSMA/CA (backoff) y se consigue que la transmisión se lleve a cabo de una manera ordenada.

Aunque con las tramas RTS/CTS se resuelve el problema del nodo oculto, su uso también da lugar a una nueva complicación: el **problema del nodo expuesto**. En un principio la situación es igual a la de la estación oculta. Un nodo A está situado entre otros dos B y C, que no se encuentran en el mismo alcance, por tanto no se pueden escuchar. El dispositivo B quiere enviar datos a la estación A, que está en el medio. El dispositivo A mandará a todos los dispositivos a su alcance (B Y C) la trama CTS que avisará a B de que tiene vía libre y al mismo tiempo inhibirá a C hasta que finalice la transmisión.

Aunque se evita el problema de nodo oculto, surge otro nuevo, pues el nodo C permanecerá inhibido, aun cuando este quisiera enviar un paquete de datos a un nodo D, fuera del alcance de A y B y que, por tanto, no supusiera un riesgo de colisión. Como consecuencia se produce una ralentización de la red.

**Network Allocation Vector (NAV)**

Antes de que un dispositivo empiece con una transmisión, envía a todos los nodos información sobre el tiempo en el que el canal va a estar ocupado en el campo “duración” de la trama RTS. Cada dispositivo introduce esta información en **su respectivo vector de reserva de red**,conocido por sus siglas en inglés NAV, de Network Allocation Vector. El NAV, que matemáticamente hablando no se puede considerar un vector, se gestiona de forma interna y establece, mediante una cuenta atrás, el momento a partir del cual se puede volver a intentar enviar datos. Es decir, cuando una estación emisora informa a un nodo de que se va a producir una transmisión, este vuelve a poner en marcha su mecanismo interno de cuenta regresiva.

El valor máximo que un NAV puede establecer en el contador es de 33ms (32.767 µs), medida que se corresponde con el tiempo límite del que un nodo emisor puede disponer para ocupar el medio. Mientras el contador no llegue a 0, los dispositivos permanecerán inhabilitados, lo que ahorra energía; y solo cuando alcance el valor nulo se puede comprobar el estado de la red. Pero además del campo “duración” de RTS, NAV también está influido por el de CTS y ACK. Esta última trama es la señal que indica a las estaciones de una red que pueden poner el contador a 0, pues el medio vuelve a estar libre.

**¿Cuál es el procedimiento de actuación de CSMA/CA?**

Cuando los integrantes de una red inalámbrica siguen las normas del protocolo Carrier Sense Multiple Access with Collision Avoidance, tienen que cumplir una serie de pasos:

En primer lugar, las estaciones que quieren transmitir escuchan el medio de transmisión. En el caso de WLAN esto implica que el carrier sense **escucha el canal** y comprueba si algún otro nodo está usando el medio de transmisión. Como ya se ha dicho, solo se podrá escuchar a los nodos dentro de la misma área de alcance.

Si resulta que el medio de transmisión se encuentra ocupado, se inicia una **contienda aleatoria:** la estación espera un periodo de tiempo aleatorio hasta que se lleva a cabo una nueva comprobación. El resto de estaciones que quieren enviar información en ese momento llevan a cabo el mismo proceso. El tiempo de espera aleatorio trata de evitar que todos los nodos de la red empiecen al mismo tiempo a comprobar el estado de la red, impidiendo así que dos o más nodos coincidan en el momento de transmitir los datos. Aunque esto solo ocurre si la estación no tiene conocimiento que el medio está ocupado, es decir, no está aplicando el mecanismo NAV, o cuando este ha llegado a 0.

En caso de que la red esté libre, la estación inicia la DCF: durante el tiempo de DIFS se vuelve a comprobar si el canal está ocupado. Si sigue libre en este periodo, se inicia una contienda aleatoria y, solo tras esta, comienza el **intercambio RTS/CTS**, siempre y cuando el protocolo complementario esté activado. Si el destinatario recibe con éxito la trama Request to Send, y por tanto, no se ha producido una colisión, este envía a su vez al emisor a través de CTS el permiso para ocupar el medio de transmisión.

Al mismo tiempo, los campos “duración” de las tramas RTS, CTS y ACK informan al resto de miembros que el medio va a estar ocupado durante un periodo de tiempo. El mecanismo NAV se activa, deshabilitando a cada uno de los nodos que no envía ni recibe. **Solo entonces la estación comienza con la transmisión**. Cuando ha finalizado el envío de datos, el destinatario espera el periodo de duración de SIFS y envía al emisor una respuesta con la trama ACK para que tenga conocimiento de que los datos se han transmitido correctamente. El contador de NAV se pone a cero, lo que implica que la red vuelve a estar libre para otra transmisión.

**Ventajas e inconvenientes de CSMA/CA**

Con el protocolo CSMA/CA se consiguen solucionar algunos de los problemas que surgen en las redes inalámbricas y que el CSMA/CD no consigue abarcar. Aunque este tipo de protocolo no está libre de inconvenientes. Por un lado, no consigue solucionar determinados casos problemáticos y, por otro, CSMA/CA también incluye algunos obstáculos:

| **Ventajas** | **Desventajas** |
| --- | --- |
| Ayuda efectiva frente a la colisión de datos | Tiempos de espera fijos |
| Gracias a ciertas notificaciones, los datos que colisionan no pasan desapercibidos | Provoca un tráfico adicional de datos |
| Con la extensión RTS/CTS se evita el tráfico innecesario de datos | El problema del nodo oculto solo se soluciona con RTS/CTS |
|  | RTS/CTS, a su vez, provoca que aparezca el problema del terminal expuesto |

**¿Qué es el acceso múltiple coordinado?**

Como el protocolo CSMA/CA no es perfecto por sí solo, se han llevado a cabo algunas acciones con la intención de subsanar sus puntos débiles. Se han desarrollado dos procesos que persiguen un acceso múltiple coordinado, si bien, por motivos diversos, apenas se aplican. El acceso múltiple coordinado establece un **sistema de coordinación centralizado**, por lo que el derecho de acceso de las estaciones independientes al medio no se coordina entre ellas, sino que lo hace un punto de acceso (access point), como puede ser un router WLAN.

**Point Coordination Function (PCF)**

La función de coordinación centralizada (PCF) se usa de forma adicional en el protocolo CSMA/CA y sustituye o complementa a la función de coordinación distribuida (DCF). El **punto de acceso (AP)funciona como coordinador** y controla las estaciones de una misma red, por lo que se encarga de gestionar la ocupación del medio de transmisión. Para establecer el orden de las estaciones individuales, cada AP cuenta con un mecanismo de polling (sondeo).

Con este mecanismo se pregunta a cada nodo, **bien uno tras otro, bien por orden de prioridad**, si quiere llevar a cabo la transmisión. Antes de que AP inicie esta actividad, se inicia un tiempo de espera, que se conoce como PIFS. En la función de coordinación centralizada la trama PCF Interframe Space tiene una ranura menos que DIFS y, por tanto, su prioridad es mayor. Es decir, PCF se inicia antes que DCF.

La función PCF sirve de pieza adicional para solucionar el problema del nodo escondido. Si se consigue colocar el punto de acceso como corresponde, este alcanza toda la red. Y es que con PCF no es necesario que los miembros de una red puedan escucharse unos a otros, pues basta con que el punto de acceso se posicione en el medio y alcance a todas las estaciones.

No obstante, si se recurre a la función de coordinación centralizada aparece otro obstáculo: todos los nodos de la red tienen que admitir la PCF para poder usar esta función, y como se puede sospechar, no siempre es el caso. Cuando los dispositivos no pueden participar en este proceso, la PCF los ignora. Por este motivo, se ha desarrollado un sistema con el que es posible alternar las funciones PCF y DCF para ofrecer a todos los dispositivos de la red la posibilidad de realizar una transmisión. Para ello el punto de acceso ofrece dos periodos de tiempo. Por un lado, se distingue el Contention Free Period (CFP) o periodo libres de conflicto, en el que la PCF garantiza un acceso múltiple coordinado y el Contenion Period (CP) o periodo con conflictos que se aplica con la DCF y que evita las colisiones, como ya se ha descrito en apartados anteriores. Esta alternancia se produce gracias a una trama beacon que el coordinador dirige a todas las estaciones.

**Hybrid Coordination Function Controlled Channel Access (HCCA)**

Las funciones de PCF y DFC se mejoran con dos métodos que tratan de establecer prioridad en las transmisiones en función del tipo de información que se quiera enviar. Se puede distinguir entre HCF Controlled Channel Access (HCCA) y Enhanced Distributed Channel Access (EDCA).

**Hybrid Coordination Function Controlled Channel Access (HCCA)** toma como referencia el método PCF y lo amplía. HCCA establece un punto de acceso (AP) que se corresponde con el Hybrid Coordinator, que recoge información sobre las Traffic Categories (TC) que cada estación le especifica. De este modo controla quién envía los datos y cuándo puede hacerlo **en función de su prioridad**. Todo ello es posible gracias a un periodo llamado Controlled Access Phase, que permite al punto de acceso de HCCA cambiar de CP a CFP en cualquier momento.

Además, el coordinador híbrido puede dar un periodo de transmisión conocido como Transmit Opportunity (TXOP). Con este término se describe el periodo de tiempo en el que le emisor no solo envía una trama, sino tantas como se permitan en la duración de TXOP. Si una trama es muy larga para un periodo determinado, esta ha de dividirse y enviarse en diferentes partes. Con TXOP se evita el retardo de algunas estaciones.

Cuando se inicia un periodo de contención (CP) se activa el **enhanced distributed channel access** (EDCA). También en EDCA se establece un orden de prioridades, orden que no se organiza de forma centralizada, sino que son las estaciones las que se coordinan entre sí, como ocurre en la función de coordinación distribuida. Los puntos del nodo que tengan que transmitir el tráfico de datos con mayor importancia no deben esperar el DIFS completo. En su lugar estas estaciones solo esperan un tiempo denominado Arbitration Interframe Space (AIFS), que varía dependiendo de la prioridad de la información y se numera sucesivamente. Así, AIFS1 tiene la máxima prioridad y es más corta que DIFS pero más larga que SIFS. También en EDCA se puede aplicar TXOP.