

# UNIDAD N° 4: Redes LAN inalámbricas

Métodos inalámbricos de transmisión de datos. Modulación por pseudoruido. Espectro disperso SSS. Modulación por salto de frecuencia. Métodos de control de acceso. Protocolos de redes LAN inalámbricas. Ejemplo de redes WIRELESS.

# MECANISMOS DE CONTROL DE TRÁFICO CONEXIÓN - ACCESO AL MEDIO - FLUJO - ERRORES

## • Protocolos de Gestión del Canal

Determinan qué estación puede usar el canal en cada momento.

### ○ Protocolos Primario/Secundario (Maestro/Esclavo)

Una estación gestiona el uso del canal

■ Ej. Sondeo/Selección

### ○ Protocolos de Igual a Igual

No hay una estación que controle el canal

Con prioridad o sin prioridad

■ Ej. 1. Detección de portadora, 2. Paso de testigo

# RESUMEN DE MECANISMOS DE CONTROL DE TRÁFICO

Basado en canales <b>CAPA 1</b>	<b>FDMA</b>	MDF (OFDMA • SC-FDMA) • WDM (WDMA)	Métodos inalámbricos de transmisión de datos • <b>Modulación por pseudoruido:</b> ○ Espectro disperso SSS. • <b>Modulación por salto de frecuencia.</b>
	<b>TDMA</b>	MF-TDMA • STDMA	
	<b>CDMA</b>	W-CDMA • TD-CDMA • TD-SCDMA • DS-CDMA • FH-CDMA • MC-CDMA	
	<b>SDMA</b>	HC-SDMA	
	<b>PDMA</b>		
	<b>PAMA</b>		
Basado en paquetes <b>CAPA 2</b>	<b>Recuperación de colisión</b>	ALOHA • ALOHA ranurado • R-ALOHA • AX.25 • CSMA/CD	
	<b>Evitación de colisiones</b>	MACA • QJACAMAYO • CSMA • CSMA/CA • FCD • PCF • HCF • CSMA/CARPA	
	<b>Sin colisiones</b>	Anillo simbólico • Autobús de fichas • MS-ALOHA	
	<b>Tolerante a retrasos e interrupciones</b>	MANETA • VANET • DTN • Enrutamiento de origen dinámico	
<b>Métodos de duplexación</b>		TDD • FDD	

[https://en.wikipedia.org/wiki/Multiple\\_Access\\_with\\_Collision\\_Avoidance](https://en.wikipedia.org/wiki/Multiple_Access_with_Collision_Avoidance)

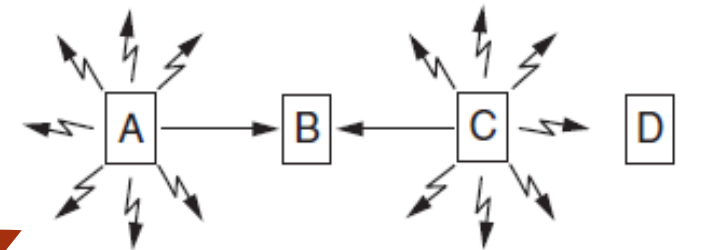
# MECANISMOS DE CONTROL DE TRÁFICO CONEXIÓN - ACCESO AL MEDIO - FLUJO - ERRORES

- **Protocolos de Igual a Igual (SIN PRIORIDAD): Escucha de Portadora p-persistente.**
  - Se divide el tiempo en intervalos de una trama
    - Si está libre → transmitir en el intervalo actual con probabilidad  $P$ , esperar al siguiente intervalo con probabilidad  $1-p$
    - Si está ocupado → espera aleatoria y escucha
    - **Colisión** → espera aleatoria y retransmisión
  - Compromiso entre la alta ocupación del canal y el bajo número de colisiones

**CSMA/CD**  
LAN cableadas

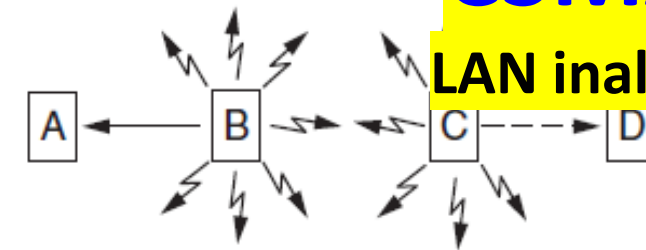
# MECANISMOS DE CONTROL DE TRÁFICO CONEXIÓN - ACCESO AL MEDIO - FLUJO - ERRORES

- Protocolos de Igual a Igual (SIN PRIORIDAD): **Escucha de Portadora p-persistente.**
  - Se divide el tiempo en intervalos de una trama
    - Si está libre → transmitir en el intervalo actual con probabilidad  $P$ , esperar al siguiente intervalo con probabilidad  $1-p$
    - Si está ocupado → espera aleatoria y escucha
    - Colisión → espera aleatoria y retransmisión
  - Compromiso en la ocupación del canal y reducción de colisiones



A y C son terminales ocultas cuando transmiten a B.

(a)



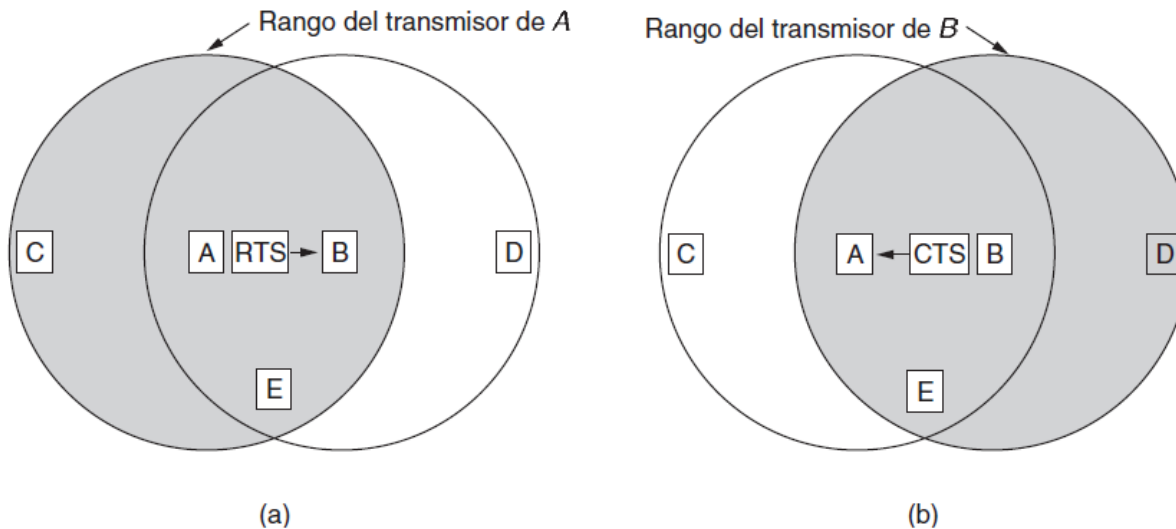
B y C son terminales expuestas cuando transmiten a A y D.

(b)

**CSMA/CA**  
**LAN inalámbricas**

**CSMA/CD**  
**LAN cableadas**

# MECANISMOS DE CONTROL DE TRÁFICO MA/CA

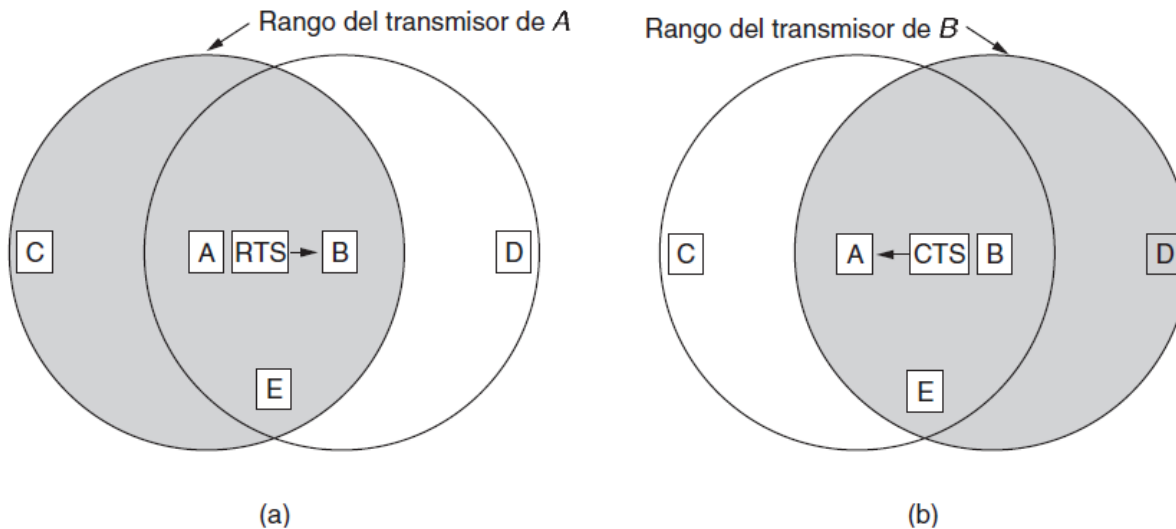


**MA/CA** (*Multiple Access with Collision Avoidance*)  
Acceso Múltiple con **Prevención de Colisiones**

- **(a) A envía un RTS a B.**
  - A comienza enviando una trama RTS (Solicitud de Envío, RTS) a B.
  - Esta trama corta (30 bytes) contiene la longitud de la trama de datos que seguirá después.
- **(b) B responde con un CTS a A.**
  - Después B contesta con una trama CTS (Libre para Envío, CTS).
  - La trama CTS contiene la longitud de los datos (que copia de la trama RTS).
- **Al recibir la trama CTS, A comienza a transmitir.**

# MECANISMOS DE CONTROL DE TRÁFICO MA/CA

## PROBLEMAS que persisten en MA/CA



**MA/CA** (*Multiple Access with Collision Avoidance*)  
**Acceso Múltiple con Prevención de Colisiones**

- (a) **Al emitir A un RTS:**
  - C está en el alcance de A, pero no en el alcance de B. Por lo tanto, escucha el RTS de A pero no el CTS de B.
  - En tanto no interfiera con el CTS, está libre para transmitir mientras se envía la trama de datos.
- (b) **Al responder B con un CTS a A.**
  - En contraste, D está en el alcance de B, pero no de A.
  - No escucha el RTS, pero sí el CTS.
  - Al escuchar el CTS sabe que está cerca de una estación que está a punto de recibir una trama, por lo que difiere el envío de cualquier cosa hasta el momento en que se espera la terminación de esa trama.
- **La estación E escucha ambos mensajes de control y, al igual que D, debe permanecer en silencio hasta que se haya completado la trama de datos.**
- **A pesar de estas precauciones, aún pueden ocurrir colisiones.**
  - Por ejemplo, B y C podrían enviar tramas RTS a A al mismo tiempo. **Éstas chocarán y se perderán.**
  - **En el caso de una colisión**, un transmisor sin éxito (es decir, uno que no escucha un CTS en el intervalo esperado) **espera un tiempo aleatorio y vuelve a intentar más tarde.**

# MECANISMOS DE CONTROL DE TRÁFICO CSMA/CA

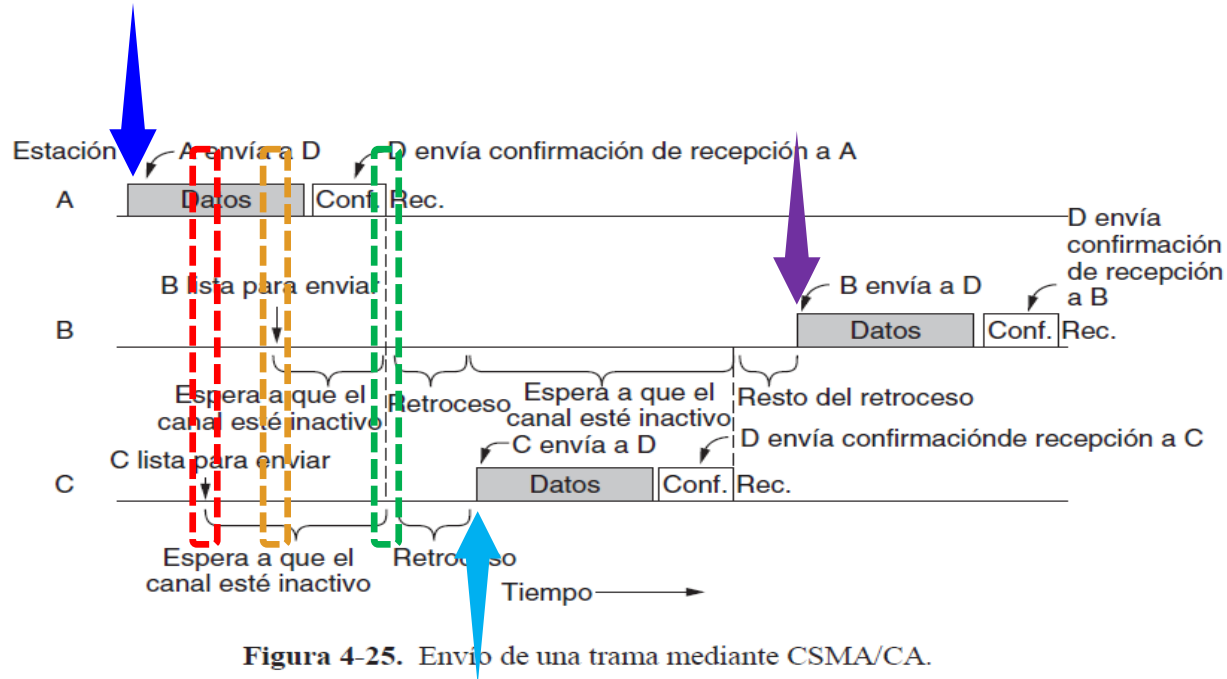


Figura 4-25. Envío de una trama mediante CSMA/CA.

**SOLUCIÓN** a los problemas en MA/CA

- La estación A es la primera en enviar una trama.
  - Mientras A envía, las estaciones B y C se preparan para enviar. Ven que el canal está ocupado y esperan a que esté inactivo.
- Poco después de que A recibe una confirmación de recepción, el canal queda inactivo.
- Sin embargo, en vez de enviar una trama de inmediato y colisionar, B y C realizan un retroceso.
  - C elige un retroceso corto, por lo que envía primero.
  - B detiene su conteo mientras detecta que C está usando el canal y lo reanuda después de que C recibe una confirmación de recepción.
- Poco después, B completa su retroceso y envía su trama.



# MECANISMOS DE CONTROL DE TRÁFICO

## CSMA/CA

- En WLAN el nodo funciona en semidúplex (no se puede usar CSMA/CD)
- **WiFi usa CSMA/CA** e incluye una capa denominada MAC que emplea 2 funciones:
  - **Distribuida** (DCF - Distributed Coordination Function), basada en el protocolo CSMA/CD.
  - **Centralizada** (PCF - Point Coordination Function), utilizada para tráfico con calidad de servicio garantizada.
- **IEEE 802.11** propone un manejo diferente de las colisiones (**evitar la colisión** - CA), acompañado de un esquema de **reconocimiento ACK positivo** cuando las tramas se reciben correctamente.

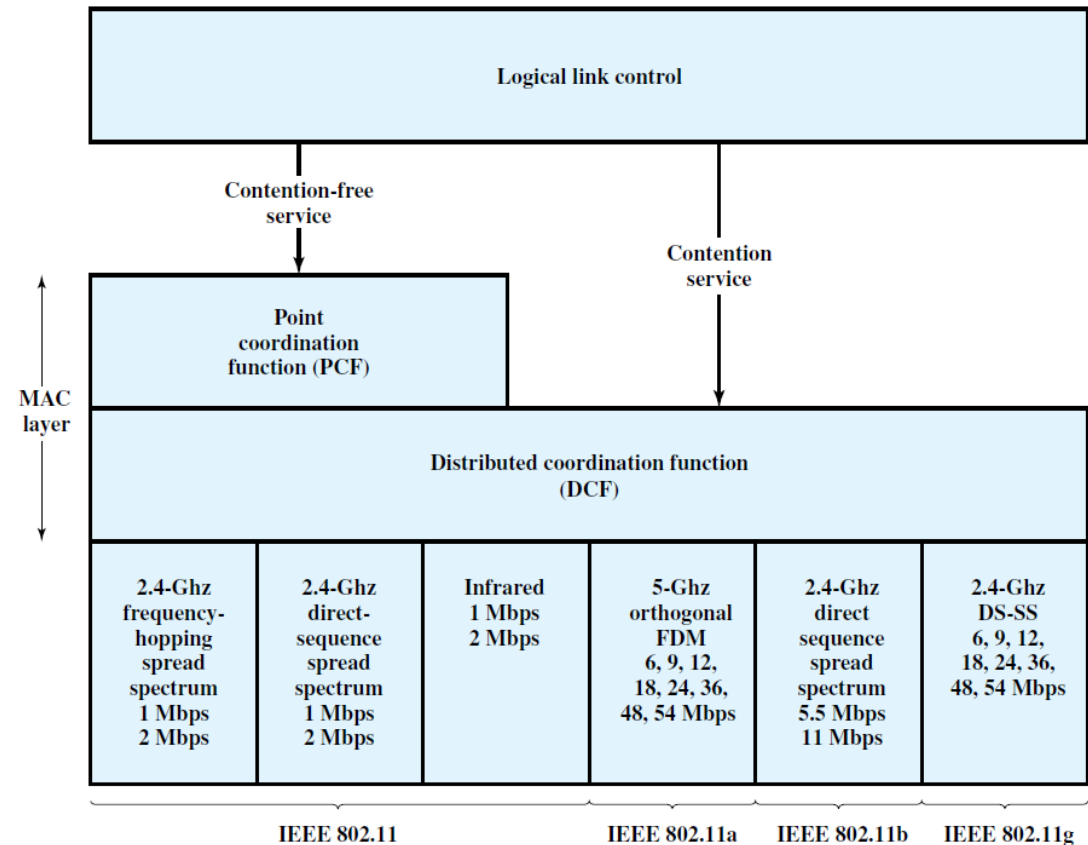


Figure 17.5 IEEE 802.11 Protocol Architecture

# MECANISMOS DE CONTROL DE TRÁFICO CSMA/CA

- **DCF** es el algoritmo básico de CSMA/CA.
  - El transmisor escucha el canal y envía el paquete cuando detecta que está libre.
  - Si detecta que está ocupado, espera un tiempo aleatorio y lo vuelve a intentar.
- **DCF** no evita el problema del nodo oculto, pero lo resuelve con una secuencia previa de mensajes de control:
  - Si un terminal quiere iniciar una transmisión, envía un mensaje RTS (Request-To-Send).
  - Al recibir el AP el mensaje RTS, si el canal está libre, envía un mensaje CTS (Clear-To-Send).
  - Recibido el mensaje CTS el terminal procede a enviar sus paquetes.
  - El nodo devuelve una señal ACK de acuse de recibo de los paquetes. Si no se recibe el ACK, se retransmiten los paquetes hasta que reciba un ACK o desiste si lo ha intentado cierto número de veces sin éxito.
- **PCF** permite establecer prioridades en el acceso al medio, gestionadas por un coordinador PC (Point Coordinator). *No todos los equipos soportan esta característica.*
- **PCF** siempre coexiste con DCF, pero la primera tiene mayor prioridad.
- En **PCF** el AP organiza el tráfico dentro del BSS.
  - **Se pregunta a los equipos si tienen paquetes pendientes y se les autoriza a transmitir si es necesario.**
  - **No puede haber solapamiento, ya que los terminales no pueden transmitir si no se les ha dado permiso.**

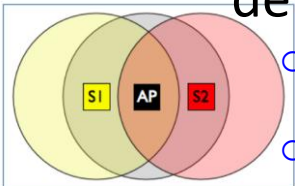


Figura 2-6 Problema del nodo oculto

# MECANISMOS DE CONTROL DE TRÁFICO CSMA/CA

- **Detección de Portadora (CS):**

- Se realiza tanto de forma física como virtual.
- Generalmente, **las estaciones esperan un período de tiempo cuando están listas para enviar** (llamado espacio intertramas distribuido o **DIFS**) para permitir que las estaciones de mayor prioridad accedan al canal.
- **Se agrega un mecanismo de detección virtual al mecanismo de detección física del medio** (útiles para reducir la probabilidad de colisión).

- La detección física de la portadora depende del medio y del esquema de modulación, tratándose de una funcionalidad más compleja que en el caso de Ethernet.

- **Uso de NAV** (Vector de Asignación de Red - *Network Allocation Vector*):

- Se consigna la duración de un intercambio, para que el resto de los dispositivos se abstenga de acceder durante ese tiempo.
- Funciona como un contador.

- **Espaciamiento entre tramas – IFS:**

**4 tipos de IFS** (Inter Frame Spacing), que se usan como un esquema de prioridades para acceso sin contienda o como una medida de lo que se debe diferir en el acceso al tratar de evitar la colisión:

- **Espaciamiento Corto entre Tramas SIFS** (Short Inter Frame Space): para manejar las transmisiones de mayor prioridad. Por ej: **tramas RTS/CTS, tramas ACK.**
- **Espaciamiento entre tramas en el modo PCF PIFS** (Point Coordination IFS): para que fuera utilizado por el AP (Punto de Coordinación), para permitirle **ganar el acceso al medio antes que a cualquier otra estación.**
- **Espaciamiento entre tramas en el modo DCF DIFS** (Distributed IFS): para usar al momento de intentar realizar una transmisión. Siempre es mayor que SIFS.
- **Espaciamiento entre tramas Extendido EIFS** (Extended IFS): **Es el mayor** y se usa si una estación ha recibido una trama que no es capaz de interpretar (errores).

# TECNOLOGÍAS IEEE 802.11

<https://grouper.ieee.org/groups/802/11/>

	IEEE 802.11n (Wi-Fi 4)	IEEE 802.11ac (Wi-Fi 5)	IEEE 802.11ax (Wi-Fi 6/6E)
Velocidad de transmisión teórica	300 MBit/s	867 MBit/s	1,200 MBit/s
Velocidad de transmisión máxima	600 Mbit/s	6,936 MBit/s	9,608 MBit/s
Alance	Hasta 100 m	Hasta 50 m	Hasta 50 m
Área de frecuencia	2.4 GHZ + 5 GHZ	5 GHZ	2.4 GHZ + 5 GHZ + 6 GHZ
Unidades de transmisión y recepción	4 x 4	8 x 8	8 x 8
Antenas	MIMO	MU-MIMO	MU-MIMO
Anchura del canal	Hasta 40 MHz	Hasta 160 MHz	Hasta 160 MHz
Método de modulación	64 QAM	256 QAM	1024 QAM

x 4

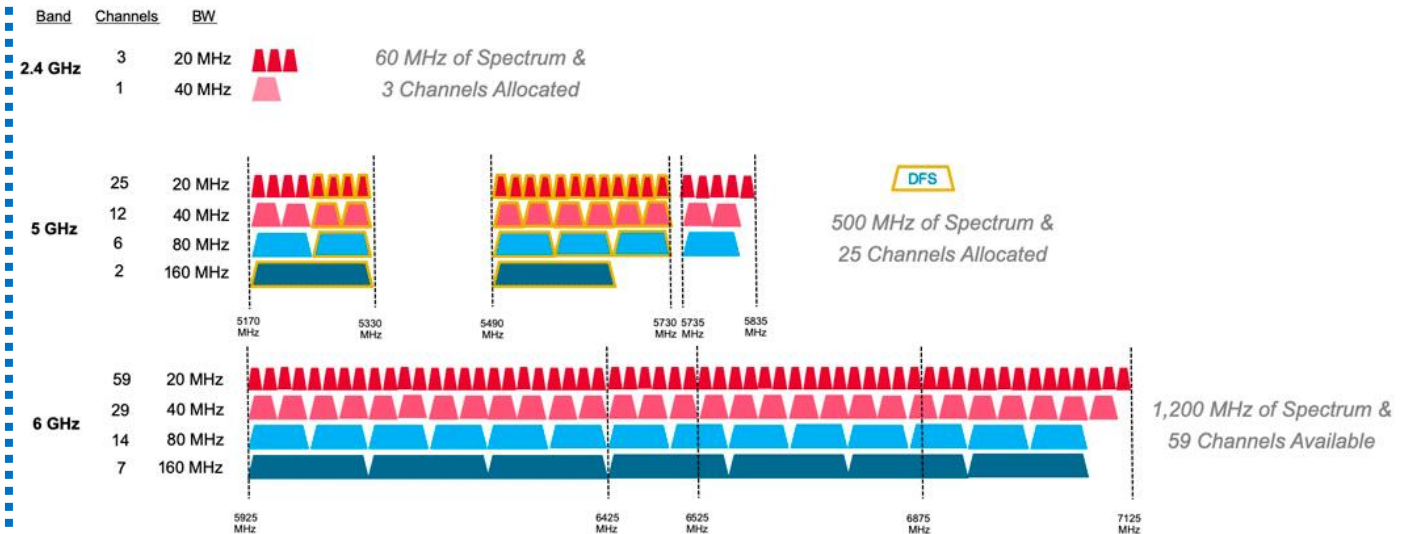
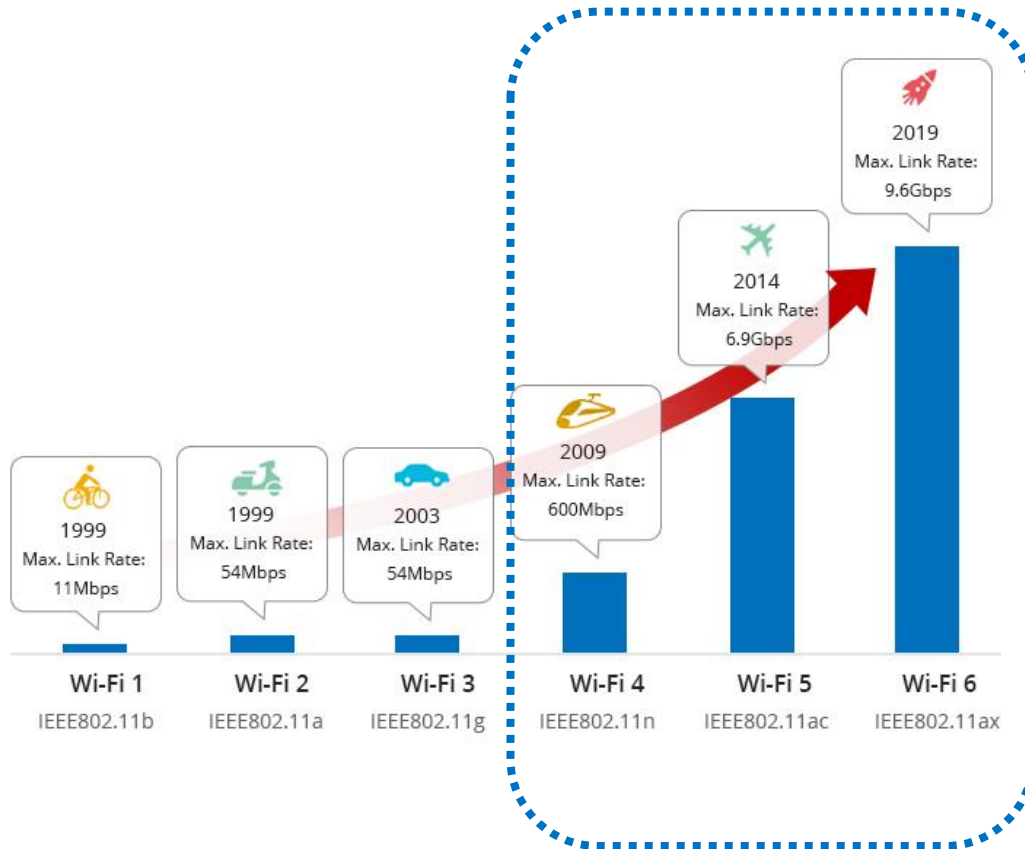
# TECNOLOGÍAS IEEE 802.11

	IEEE 802.11 (Wi-Fi 1)	IEEE 802.11n (Wi-Fi 4)	IEEE 802.11ac (Wi-Fi 5)	IEEE 802.11ax (Wi-Fi 6/6E)
Frecuencia	2.4 GHz	2.4 GHz + 5 GHz	5 GHz	2.4 GHz + 5 GHz + 6 GHz
Transmisiones	1	1, 2, 3, 4	1, 2, 3, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 6, 7, 8
A 20 MHz de ancho de canal	Hasta 2 MBit/s	Hasta 300 MBit/s	-	Hasta 574 MBit/s
A 40 MHz de ancho de canal	-	Hasta 600 MBit/s	-	Hasta 1,144 MBit/s
A 80 MHz de ancho de canal	-	-	Hasta 3,400 MBit/s	Hasta 4,804 MBit/s
A 160 MHz de ancho de canal	-	-	Hasta 6,936 MBit/s	Hasta 9,608 MBit/s

**VELOCIDAD MÁXIMA**

En 2024 se certificará la norma IEEE 802.11be, que supuestamente alcanzará los 45,1 GBps.

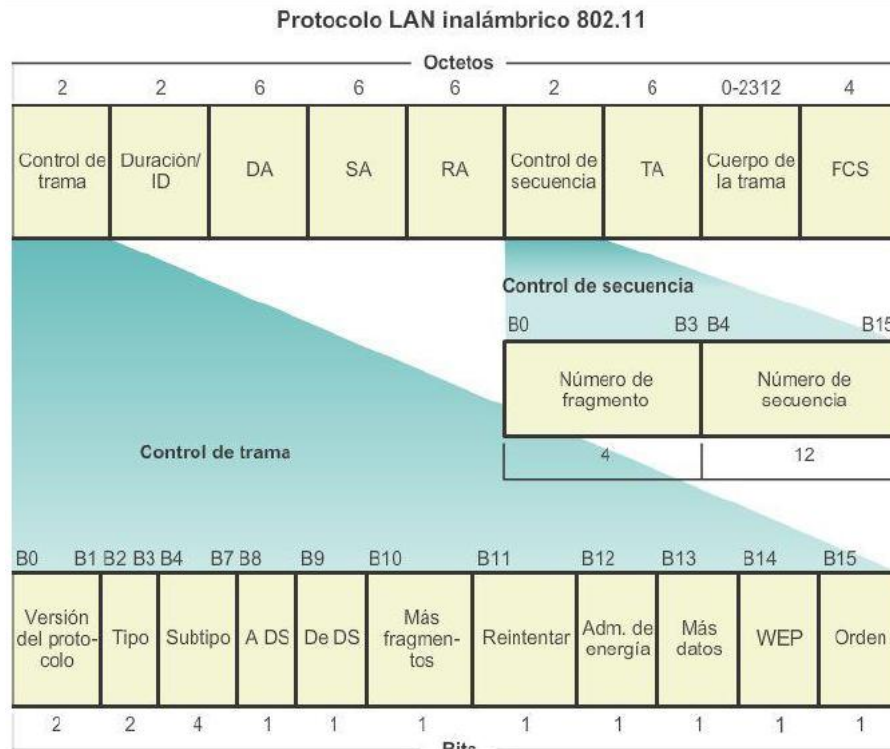
# TECNOLOGÍAS IEEE 802.11





# TRAMA IEEE 802.11 (WiFi 1)

- Existe un formato de trama general común para las redes 802.11, pero **varios tipos de tramas**.
- No todos los campos están presentes en todos los tipos de marco.

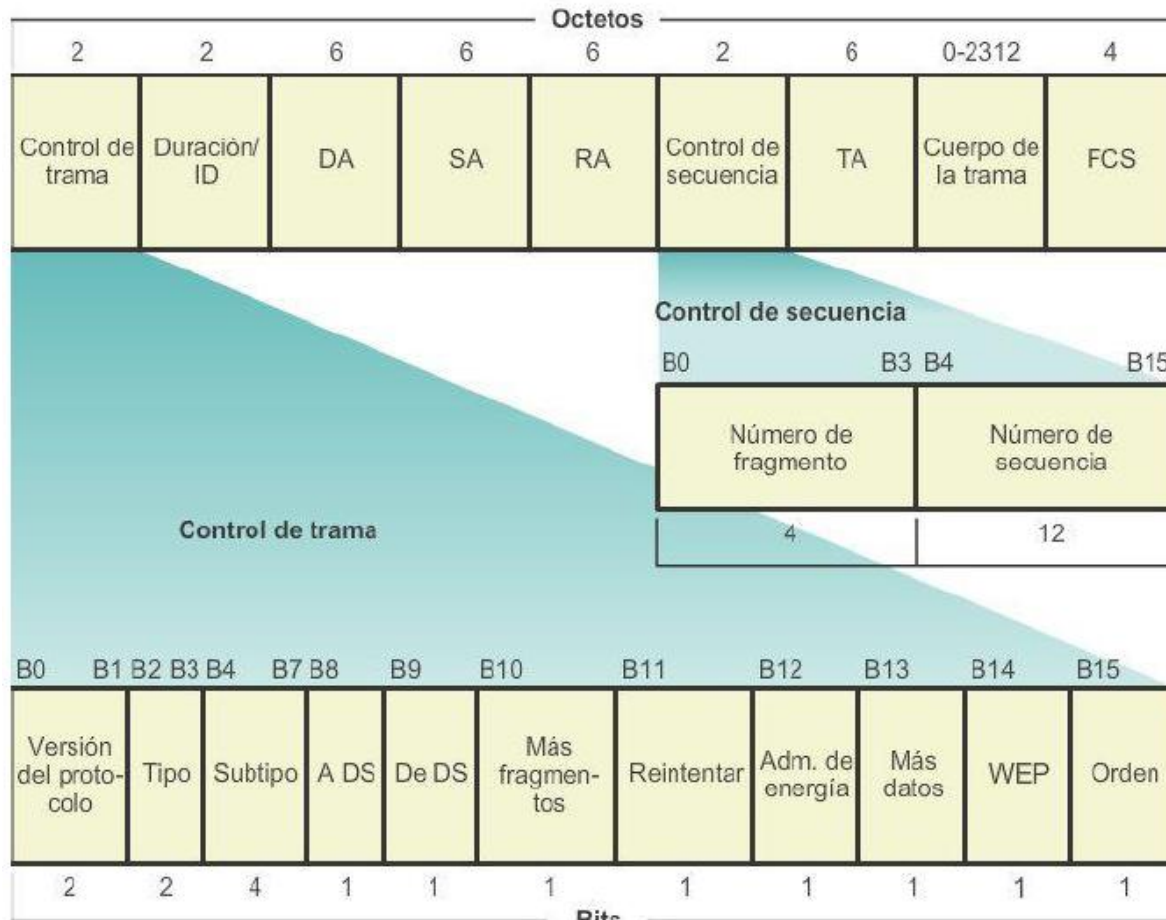


## Control de trama:

- **Versión de protocolo:** la versión de la trama 802.11 en uso.
- **Tipo y Subtipo:** identifican una de las tres funciones y subfunciones de la trama (control, datos y administración).
- **A DS:** se establece en 1 para las tramas de datos destinadas al sistema de distribución (dispositivos en la estructura inalámbrica).
- **Desde DS:** se establece en 1 para las tramas de datos que salen del sistema de distribución.
- **Más fragmentos:** se establece en 1 para las tramas que tienen otro fragmento.
- **Reintentar:** se establece en 1 si la trama es una retransmisión de una trama anterior.
- **Administración de energía:** se establece en 1 para indicar que un nodo estará en el modo de ahorro de energía.
- **Más datos:** se establece en 1 para indicarle a un nodo en el modo de ahorro de energía que se almacenan más tramas en búfer para ese nodo.
- **WEP:** se establece en 1 si la trama contiene información encriptada mediante WEP para propósitos de seguridad
- **Orden:** se establece en 1 en una trama de tipo de datos que utiliza la clase de servicio Estrictamente ordenada (no requiere reordenamiento).

# TRAMA IEEE 802.11 (WiFi 1)

Protocolo LAN inalámbrico 802.11



**Duración/ID:** según el tipo de trama, representa el tiempo que se requiere en microsegundos para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió la trama.

**Dirección de destino (DA):** contiene la dirección MAC del nodo de destino final en la red.

**Dirección de origen (SA):** contiene la dirección MAC del nodo que inició la trama.

**Dirección del receptor (RA):** contiene la dirección MAC que identifica al dispositivo inalámbrico que es el destinatario inmediato de la trama.

- **Número de fragmento:** indica el número de cada fragmento de la trama.
- **Número de secuencia:** indica el número de secuencia asignado a la trama. Las tramas retransmitidas se identifican con números de secuencia duplicados.

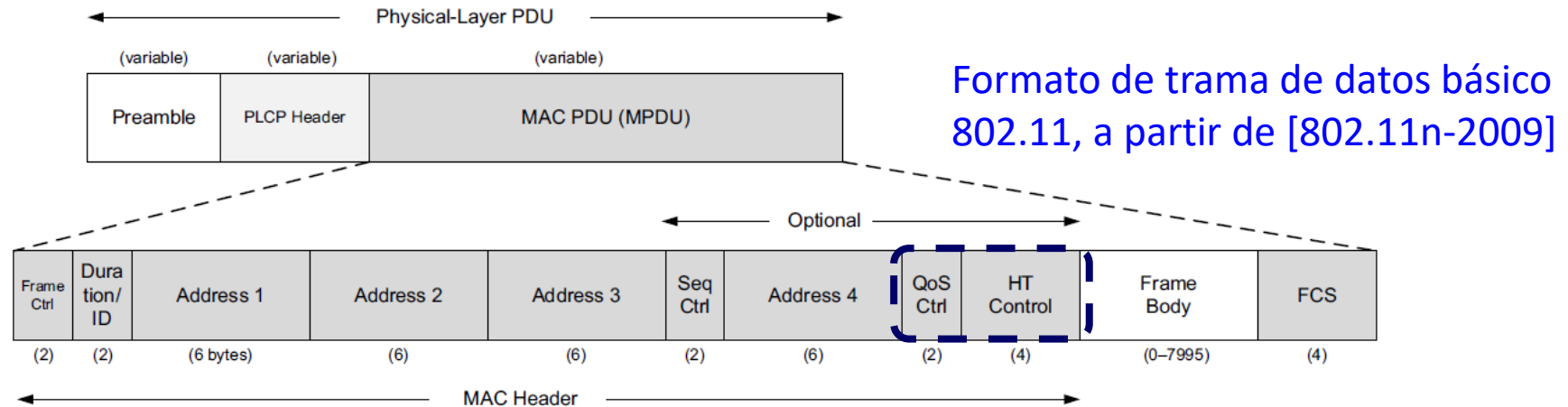
**Dirección del transmisor (TA):** contiene la dirección MAC que identifica al dispositivo inalámbrico que transmitió la trama.

**Cuerpo de la trama:** contiene la información que se transporta. En las tramas de datos; generalmente se trata de un paquete IP.

**FCS:** contiene una comprobación de redundancia cíclica (CRC) de 32 bits de la trama.



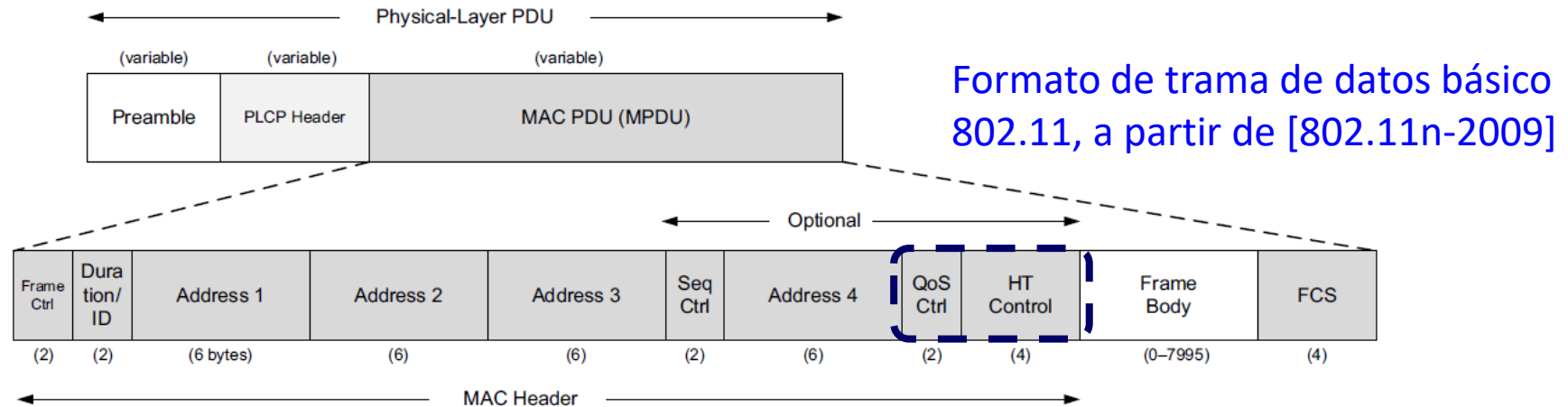
# PDU's IEEE 802.11 (WiFi 4)



- **L1 PDU:**

- **Preámbulo:** se usa para sincronismo, pero también puede ayudar en la selección de la antena apropiada.
- **PLCP** (Procedimiento de convergencia de la capa física):
  - Proporciona información sobre la capa física específica, de manera independiente del L1.
  - Generalmente, se transmite a una velocidad de datos más baja que el resto de la trama:
    - Mejorar la probabilidad de una entrega correcta (las velocidades más bajas tienden a tener una mejor resistencia a errores)
    - y brindar compatibilidad y protección contra la interferencia de equipos antiguos.

# PDU's IEEE 802.11 (WiFi 4)



- **L2 (MPDU):**

~ Ethernet, pero tiene campos adicionales según: el tipo de DS que se utiliza entre los puntos de acceso, si la trama se dirige al DS o desde él, y si las tramas se están agregando.

- **Control de trama:** 2 bits que identifica el tipo de trama (de gestión, de control y de datos). Cada uno de estos puede tener varios subtipos.
- **Control QoS:** se utiliza para funciones de rendimiento especiales.
- **Control HT:** se utiliza para controlar las funciones de "alto rendimiento" de 802.11n.

# LANs DE ALTA VELOCIDAD

**Table 16.1** Characteristics of Some High-Speed LANs

	<b>Fast Ethernet</b>	<b>Gigabit Ethernet</b>	<b>Fibre Channel</b>	<b>Wireless LAN</b>
<b>Data Rate</b>	100 Mbps	1 Gbps, 10 Gbps	100 Mbps–3.2 Gbps	1 Mbps–54 Mbps
<b>Transmission Media</b>	UTP, STP, optical Fiber	UTP, shielded cable, optical fiber	Optical fiber, coaxial cable, STP	2.4-GHz, 5-GHz microwave
<b>Access Method</b>	CSMA/CD	Switched	Switched	CSMA/Polling
<b>Supporting Standard</b>	IEEE 802.3	IEEE 802.3	Fibre Channel Association	IEEE 802.11

# VENTAJAS IEEE 802.11ax (WiFi 6)



- Optimiza la eficiencia con la tecnología **OFDMA**.
- Aumenta el rendimiento con la tecnología **MU-MIMO**.
- Minimiza los posibles conflictos con la tecnología de coloración **BSS**.
- Reduce el consumo de energía con la tecnología **TWT**.
- Ofrece un entorno de red más seguro con **WPA3**.

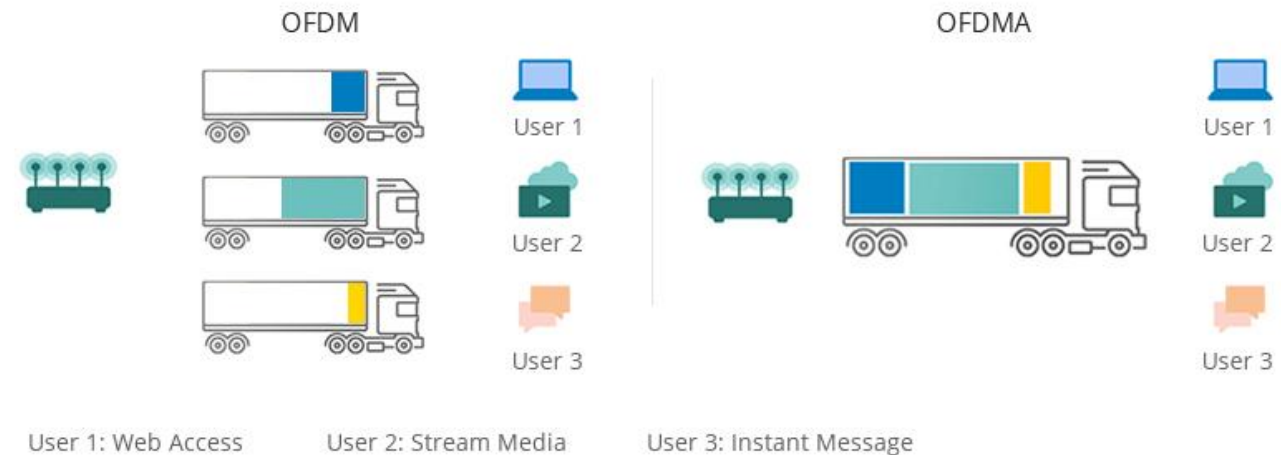
# VENTAJAS IEEE 802.11ax (WiFi 6)

## Optimiza la eficiencia con la tecnología OFDMA

- Divide el ancho de banda disponible del canal en varias subportadoras o unidades de recursos (RU) ortogonales mutuas.
  - Así, las aplicaciones que utilizan tramas pequeñas pueden transmitirse simultáneamente a varios puntos extremos
    - >> reduce la sobrecarga y la congestión en L2.
  - Cuando las conexiones múltiples transmiten cantidades limitadas de datos
    - >> se aprovecha al máximo OFDMA.
- Es flexible para asignar todo el canal a una subdivisión en función del tráfico >> mejora enormemente la eficiencia y reduce la latencia.

## (orthogonal frequency-division multiple access)

- Un AP puede:
  - elegir entre asignar todo el canal (todos los subcanales) a un único usuario en un periodo determinado, o
  - dividir el canal para servir simultáneamente a varios dispositivos.



WiFi6 pasa de un servicio basado en la contienda a otro basado en la programación (ayuda a estabilizar el rendimiento del WiFi).

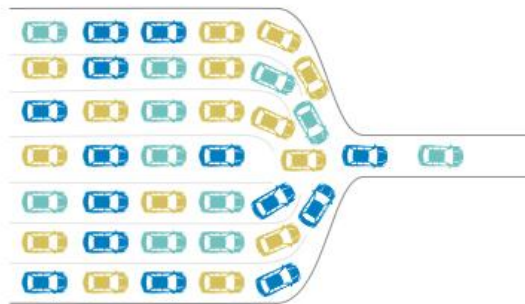
# VENTAJAS IEEE 802.11ax (WiFi 6)

(multi-user, multi-input, multi-output)

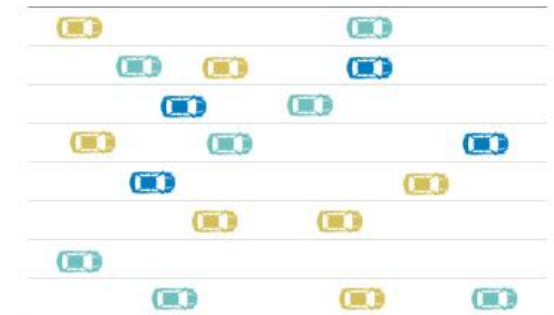
- Permite a los enrutadores comunicarse con múltiples dispositivos al mismo tiempo, en lugar de comunicarse sucesivamente.
- Funciona tanto para las subidas como para las descargas. El WiFi 5 (MU-MIMO, sólo para descargas)
- Utiliza 8x8 ascendente/descendente para proporcionar una capacidad cuádruple:
  - Aumenta la utilización del ancho de banda de la red Wi-Fi.
  - MU-MIMO ha ampliado la capacidad para una mejor eficiencia.

## Aumenta el rendimiento con la tecnología MU-MIMO

- MU-MIMO y OFDMA forman una unidad de complementación:
  - Mejorar la eficiencia de las redes WiFi
  - Reducir la latencia de las aplicaciones sensibles al tiempo.
- MU-MIMO y OFDMA tienen sus ventajas y aplicaciones respectivamente:
  - OFDMA es ideal para aplicaciones de ancho de banda bajo y de paquete pequeño (IoT).
  - MU-MIMO aumenta la capacidad y la eficiencia en aplicaciones de ancho de banda alto (llamadas de voz o video de misión crítica).



Without MU-MIMO



With MU-MIMO



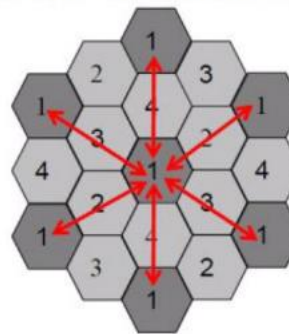
# VENTAJAS IEEE 802.11ax (WiFi 6)

## Minimiza los posibles conflictos con la tecnología de coloración BSS.

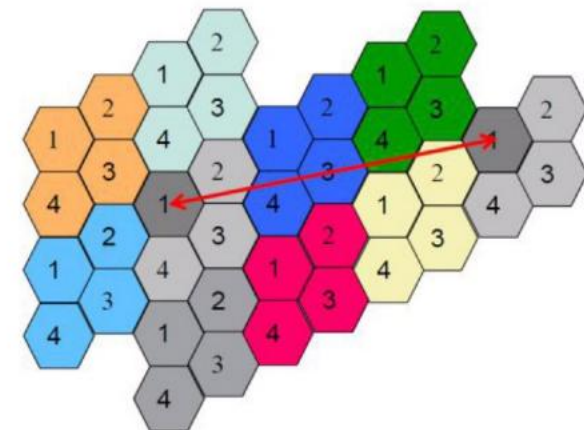
(basic service set)

- Cada BSS se marca con un color que lo identifica.
- Las tramas que llegan a la misma frecuencia, pero con otro color se las trata de otra manera.
- Ayuda a remediar reutilización de canales ineficiente:
  - Inserta una identidad en una señal Wi-Fi transmitida.
  - Cuando los dispositivos receptores detecten esta señal «coloreada»:
    - se conocerá qué BSS la está enviando y la fuerza de su señal,
    - se creará una nueva secuencia lógica para optimizar el proceso, donde se decidirá cuándo transmitirla y cuándo no.
- Se refiere a un conjunto de clientes inalámbricos asociados con el mismo AP.
- “Coloración BSS” es un mecanismo que codifica inteligentemente con colores las frecuencias compartidas con un número.

Increased Frequency Reuse (w/  
80 MHz channels) -  
All same-channel BSS blocking



Same-channel BSS only blocked on Color Match



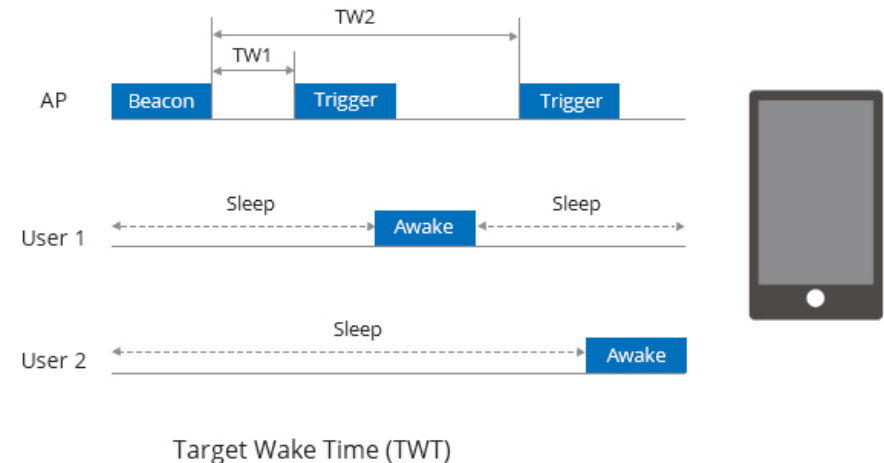
# VENTAJAS IEEE 802.11ax (WiFi 6)

## Reduce el consumo de energía con la tecnología TWT.

- El «tiempo de activación del objetivo» permite a los dispositivos negociar **cuándo y con qué frecuencia** se activarán para enviar o recibir datos:
  - Aumenta el tiempo en modo de espera y mejora sustancialmente la duración de la batería de los dispositivos.
- Se planifican las comunicaciones de los dispositivos con un AP
  - >> podrán reducir el periodo de tiempo en el que deben mantener sus antenas encendidas para transmitir y buscar señales.
  - >> los dispositivos permanecerán inactivos hasta que sea su turno de transmitir datos usando un esquema de programación negociado con los AP
- Con menos congestión y ahorro de energía ofrecerá una mejor experiencia para los usuarios.



## TWT (target wake time)





# VENTAJAS IEEE 802.11ax (WiFi 6)

	WEP	WPA	WPA2	WPA3
Año de publicación	1999	2003	2004	2018
Método de encriptación	Rivest Clipher 4 (RC4)	Protocolo de integridad de clave temporal (TKIP) con RC4	CCMP y estándar de cifrado avanzado (AES)	Estándar de cifrado avanzado (AES)
Tamaño de la clave de sesión	40-bit	128-bit	128-bit	128-bit (WPA3-Personal) 192-bit (WPA3-Enterprise)
Tipo de cifrado	Stream (cifrado de flujo)	Stream (cifrado de flujo)	Block (cifrado de bloque)	Block (cifrado de bloque)
Integridad de datos	CRC-32	Código de integridad del mensaje	CBC-MAC	Algoritmo hash de seguridad
Gestión de claves	No proporcionado	Mecanismo de handshaking de 4 vías	Mecanismo de handshaking de 4 vías	Autenticación simultánea de iguales handshake
Autenticación	WEP-Abierto WEP-Compartido	Clave precompartida (PSK) y 802.1x con variante EAP	Clave precompartida (PSK) y 802.1x con variante EAP	Autenticación simultánea de iguales (SAE) y 802.1x con variante EAP

## Ofrece un entorno de red más seguro con WPA3.

- **WPA y WPA2**, que utilizan un handshake imperfecto de 4 vías para habilitar las conexiones inalámbricas (vulnerabilidad KRACK)
- **WPA3** autentica con el handshake de Autenticación Simultánea de Iguales (protege las conexiones frente a ataques).
- **WPA3** sustituye los protocolos criptográficos susceptibles al criptoanálisis por **protocolos que requieren la interacción con la infraestructura por cada contraseña adivinada:**
  - >> la infraestructura puede poner límites temporales al número de adivinanzas.
  - >> dificulta que se descifren las contraseñas a base de probar distintas combinaciones constantemente.
  - >> hace que algunos datos sean «menos útiles» aunque los hackers logren obtenerlos.