# Clase VIII

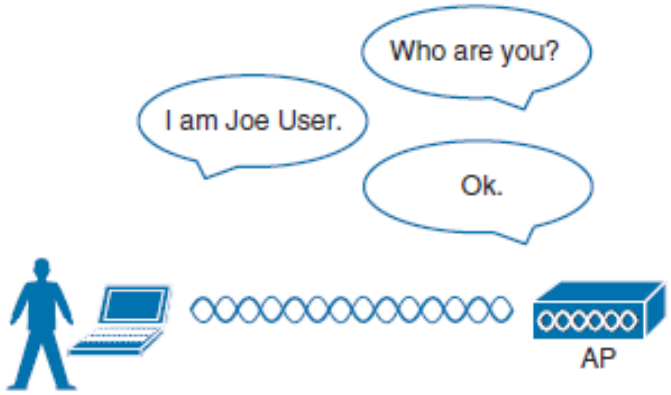
## Interconexión de redes de datos (IRD101)

# Agenda

- Fundamentos de seguridad en redes inalámbricas
- Arquitecturas inalámbricas centralizadas
- Wi-Fi 6

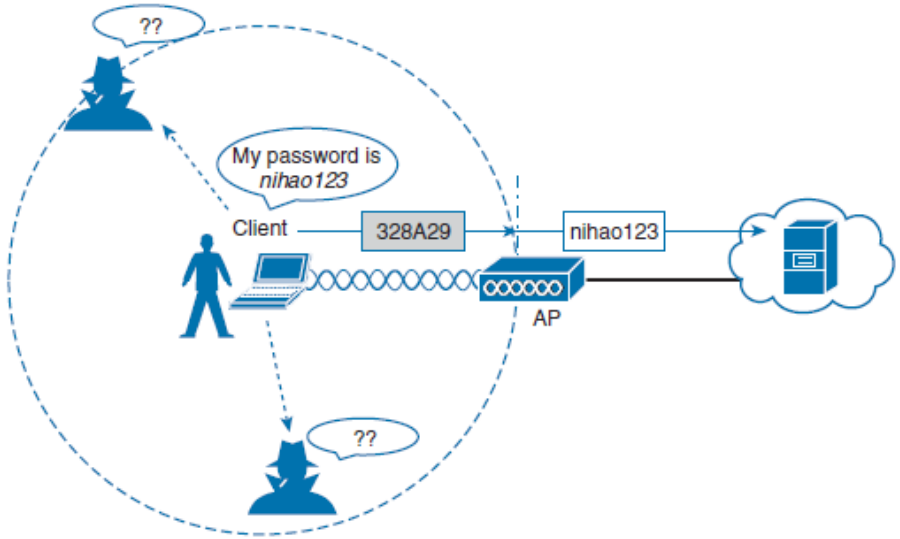
# Autenticación

Para controlar el acceso, las redes inalámbricas pueden autenticar a los dispositivos clientes antes de permitir su asociación. Los clientes potenciales deben identificarse presentando sus credenciales a los puntos de acceso (APs).



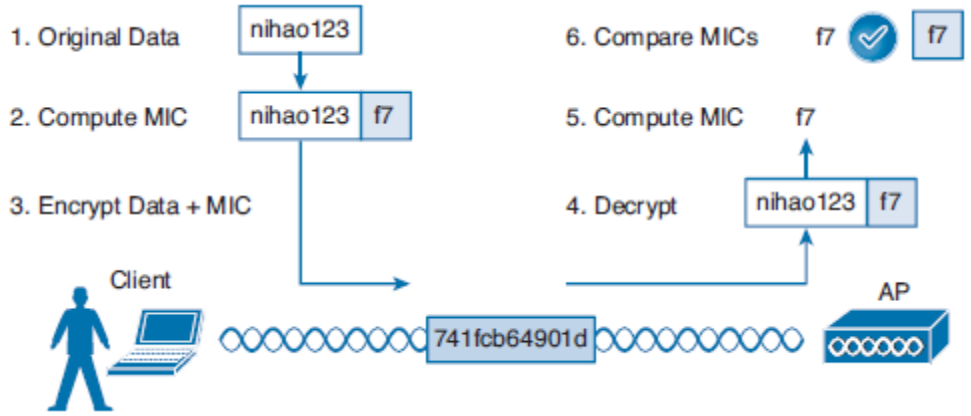
# Privacidad

Para proteger los datos en una red inalámbrica, los datos deben ser encriptados, por lo que el payload de cada trama es encriptado y es desencriptado cuando es recibido.
En redes inalámbricas, cada WLAN soporta solo un esquema de encriptación y autenticación, por lo que los clientes deben utilizar el mismo esquema cuando se asocian.



# Integridad

Después de aplicado el proceso de encriptación/desencriptación, es necesario un método que asegure que el mensaje original no ha sido modificado, por lo que se aplica la revisión de integridad de mensaje (Message Integrity Check – MIC) utilizando una secuencia de bits conocida como secret stamp, si se recibe la misma secret stamp se garantiza que el mensaje no ha sido modificado.

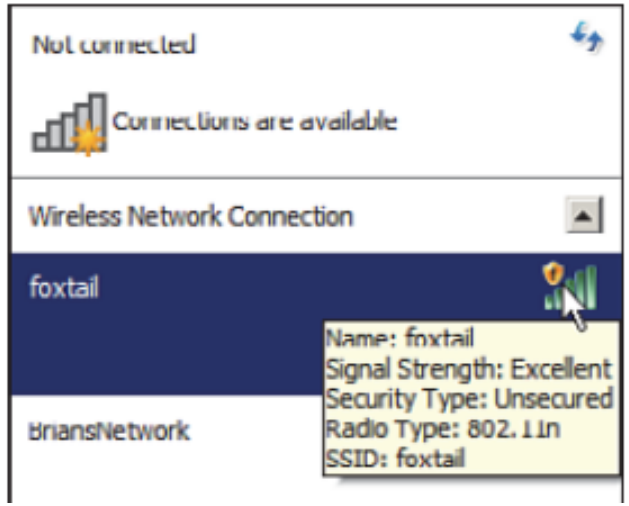


# Metodos de autenticación

## Autenticación abierta.

Ofrece un acceso abierto a una WLAN, el único requisito es que el cliente debe usar el protocolo 802.11 para asociarse con un punto de acceso, no es requerido utilizar credenciales. Este método generalmente es utilizado en espacios públicos.

Este método no ofrece opciones para encriptación de tráfico entre el cliente inalámbrico y el AP.



# Metodos de autenticación

## WEP

Wireless Equivalent Privacy (WEP), es un estándar definido en 1999, utiliza el algoritmo de cifrado RC4 en todas las tramas inalámbricas. El algoritmo encripta los datos utilizando una cadena de bits como llave, la cual es utilizada tanto como por el emisor como por el receptor, WEP es conocido como el método de seguridad de clave compartida.

Las llaves WEP pueden estar compuestas entre 40 y 104 bits de longitud, representados por una cadena de 10 a 26 caracteres en código hexadecimal.

En 2001 fueron descubiertas y reveladas una cantidad importante de vulnerabilidades que impulsaron el desarrollo de otros métodos de autenticación más robustos.

# Metodos de autenticación

## 802.1x / EAP

Extensible Authentication Protocol (EAP), es una estructura de autenticación flexible y escalable que fue desarrollada después de la identificación de las vulnerabilidades de WEP.

La característica principal de EAP es que puede ser integrada con el estándar de control de acceso basado en puertos IEEE 802.1x, lo cual permite que un cliente inalámbrico pueda ser asociado a un AP pero no pueda transmitir información a recursos de red hasta que la autenticación se complete correctamente.

# Metodos de autenticación

## Suplicante

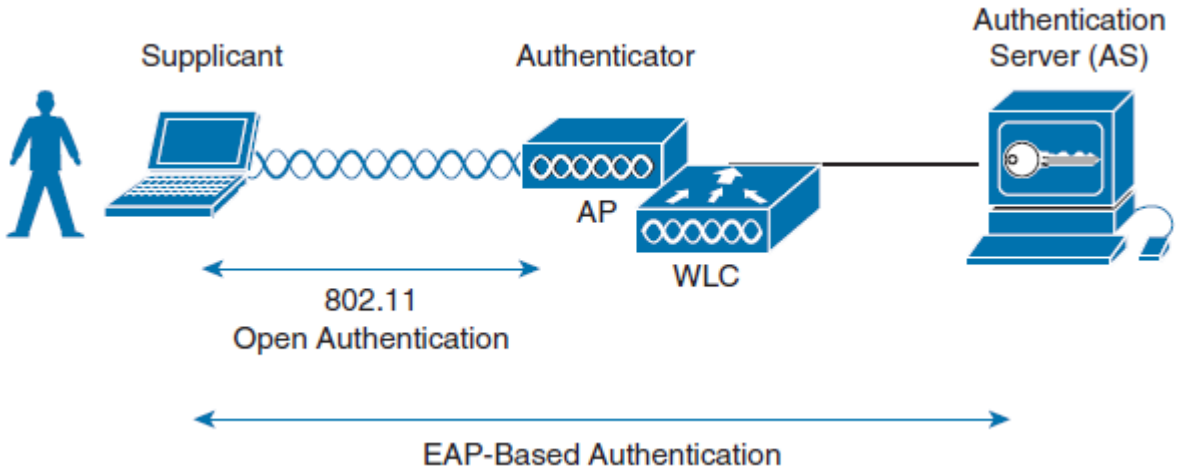
- Es el dispositivo cliente que requiere acceso a la red.

## Autenticador

- Es el dispositivo de red que provee acceso a la red (usualmente una WLC)

## Servidor de autenticación (AS)

- Es el dispositivo que evalúa las credenciales proporcionadas y permite o deniega el acceso a la red con base a políticas (usualmente un servidor RADIUS)




(LEAP / EAP-FAST / PEAP / EAP-TLS)

# Metodos de autenticación

A continuación un resumen de los métodos de autenticación basados en EAP:

| LEAP | EAP-FAST | PEAP | EAP-TLS |
|---|---|---|---|
| • Es un método de autenticación propietario de Cisco basado en intercambio de llaves dinámicas. | • Es un método de autenticacion desarrollado por Cisco que utiliza un túnel TLS. | • Es un método de autenticación que utiliza un certificado digital. | • Es un método de autenticación que utiliza un certificado digital y un tunel TLS. |

# Metodos de autenticación

## WPA y WPA2

WPA (Wi-Fi Protected Access) esta basado en parte del protocolo 802.11i incluyendo autenticación 802.1x, TKIP (Temporal Key Integrity Protocol) y un método de administración de llaves dinámicas encriptadas.

Luego que WPA fue ratificado y publicado se incluyó su versión completa denominada como WPA2.
Tanto los estándares WPA como WPA2 soportan dos métodos de autenticación:

- **Modo personal:** Utiliza una llave compartida para autentica clientes WLAN.
- **Modo empresarial:** Utiliza un modo de autenticación de clientes basado en 802.1x EAP.

# Wi-Fi Protected Setup (WPS)

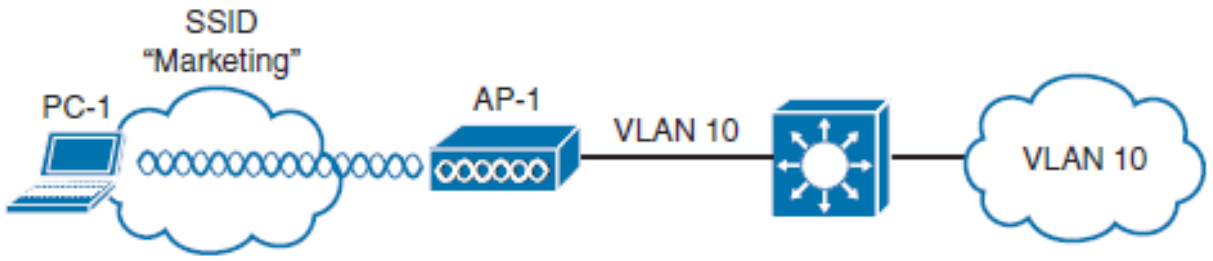
WPS define los mecanismos a través de los cuales los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK) necesarias para iniciar el proceso de autenticación.

No se requieren habilidades técnicas para conectarse a una WLAN solamente se debe presionar el botón WPS en el router inalámbrico y en el cliente.


Wi-Fi PROTECTED SETUP

# Arquitectura autónoma

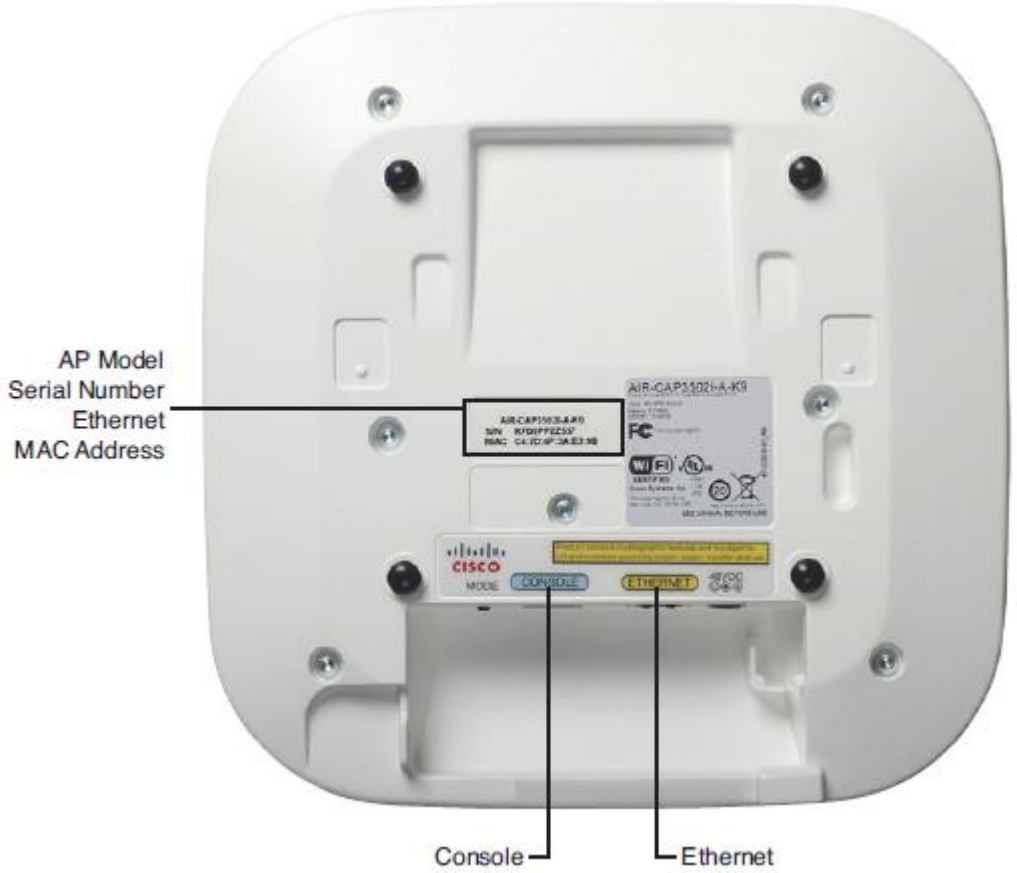
Los APs autónomos controla el acceso de clientes inalámbricos a la WLAN, se encuentra equipado con hardware para trabajar con señales cableadas e inalámbricas. Son utilizados comúnmente en redes pequeñas por su facilidad de despliegue y configuración, donde cada AP se administra de forma independiente.



# Arquitecturas inalámbricas centralizadas

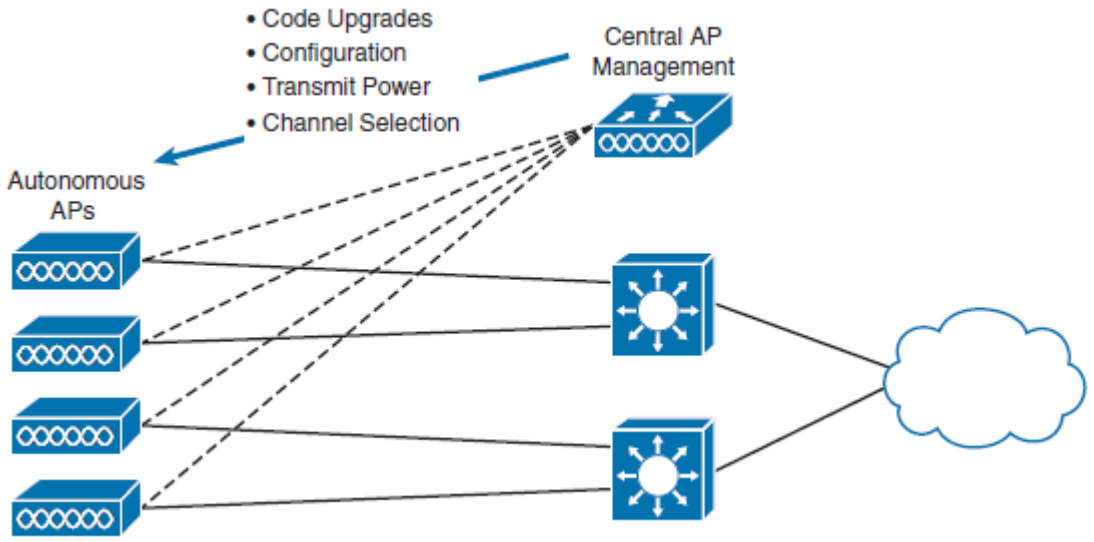
La administración de infraestructura de red inalámbrica implica la selección y configuración de cada canal que es ocupado por cada AP, revisar interferencias de señal, niveles de transmisión, áreas de cobertura, etc.

Las labores de administración se vuelven más complicadas al estar a cargo de una red desplegada con APs autónomos.

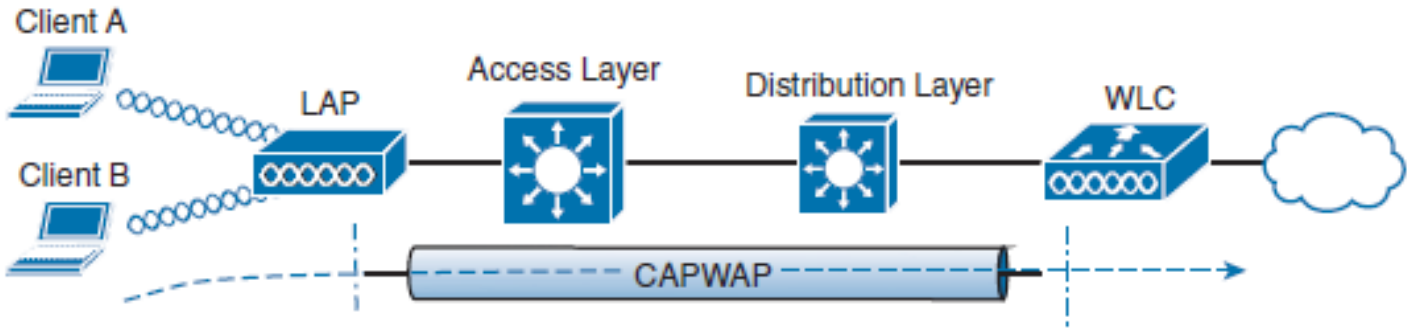


# Arquitecturas inalámbricas centralizadas

A medida las WLAN experimentaron un acelerado crecimiento, se presentó la necesidad de realizar una administración de sus componentes de una forma centralizada.



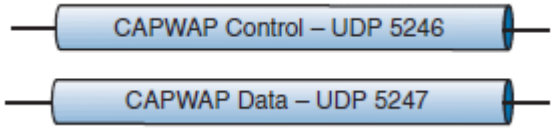
# Arquitecturas inalámbricas centralizadas




**LAP:** Lightweight Access Point

**WLC:** Wireless LAN Controller

**CAPWAP:** Control and provisioning of Wireless Access Points

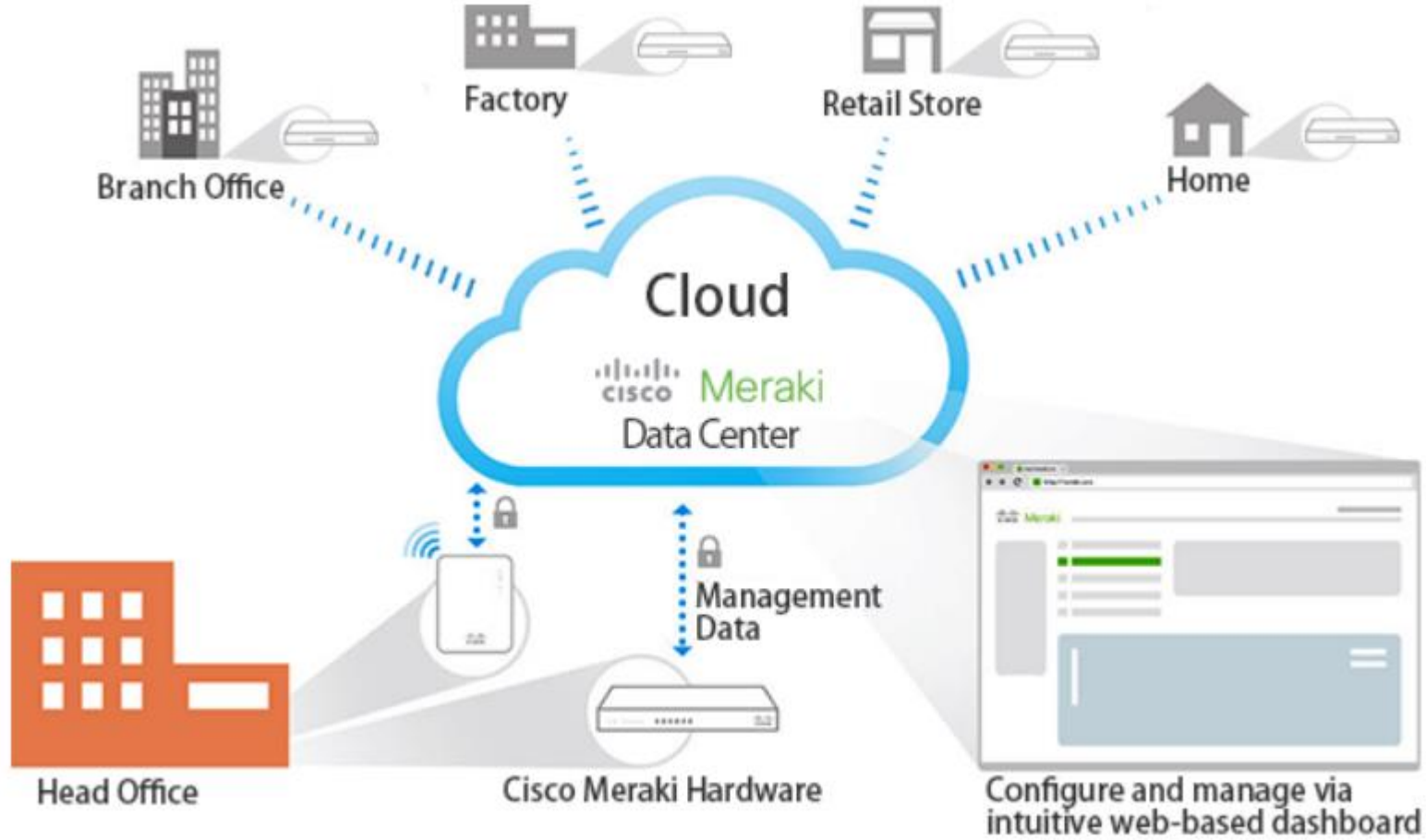


# Arquitecturas inalámbricas centralizadas

## Cisco Meraki

Es una solución de administración en la nube para pequeñas y medianas empresas.

Incluye tecnología inalámbrica, switching, seguridad (UTM) y administración de dispositivos móviles (MDM).



# Wi-Fi 6

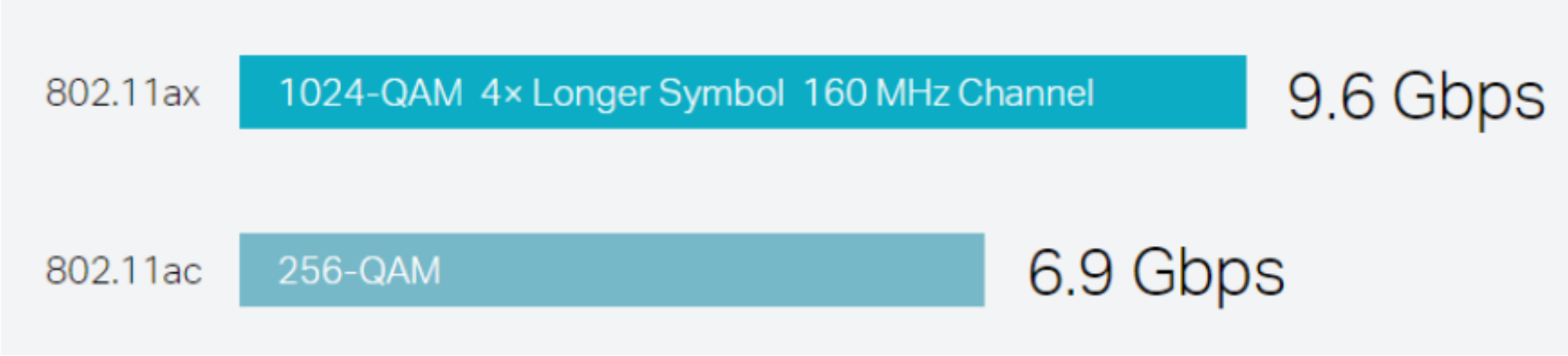
Wi-Fi 6, también conocido como 802.1ax, es el último estándar de conectividad que toma las fortalezas de los estándares anteriores y brinda soporte al constante crecimiento de los dispositivos que requieren conectividad wireless, mediante mejoras en la velocidad, estabilidad y eficiencia energética.

Es un estándar retrocompatible, lo que implica que un dispositivo con capacidad de conexión a Wi-Fi 6 puede conectarse a redes bajo una versión anterior.

# Wi-Fi 6

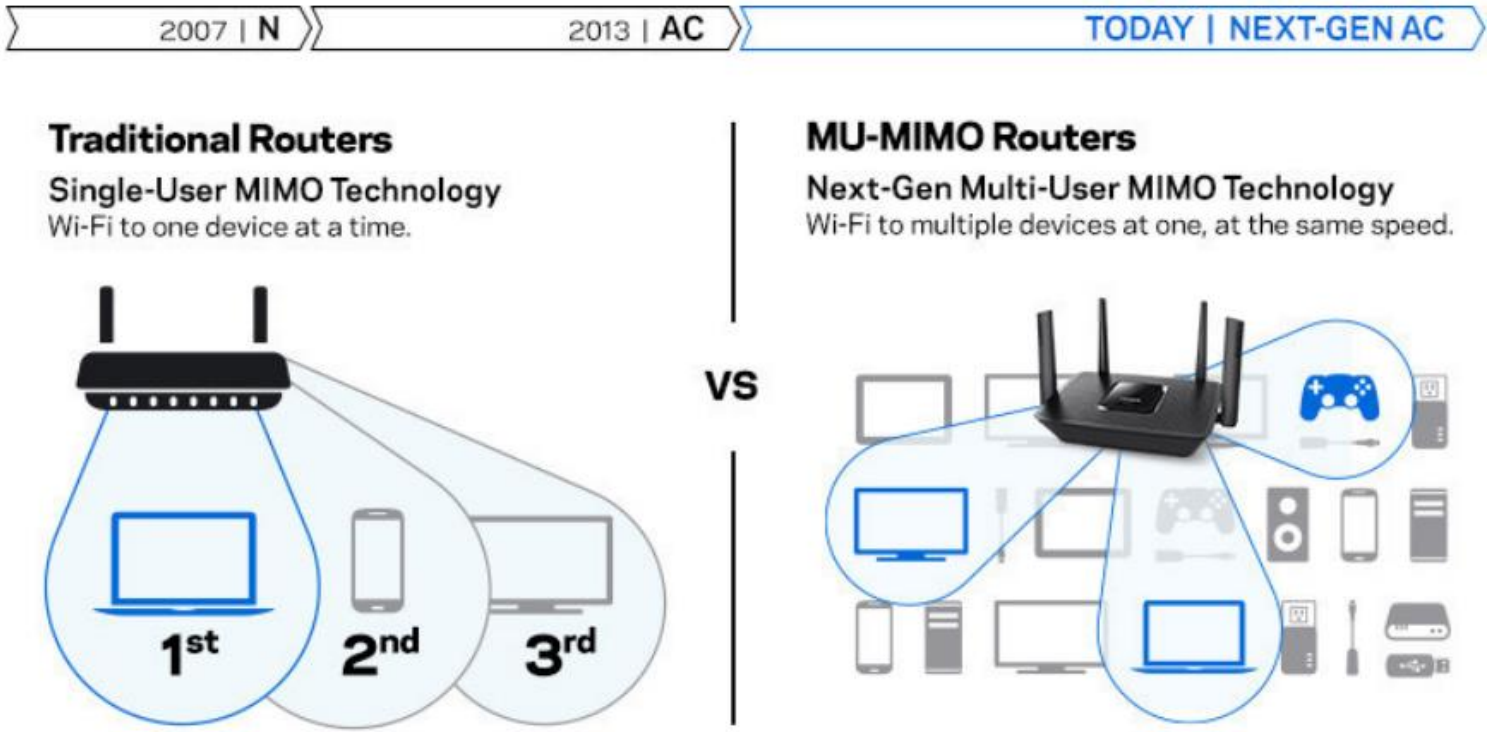
**Ventajas de Wi-Fi 6 vrs Wi-Fi 5.**

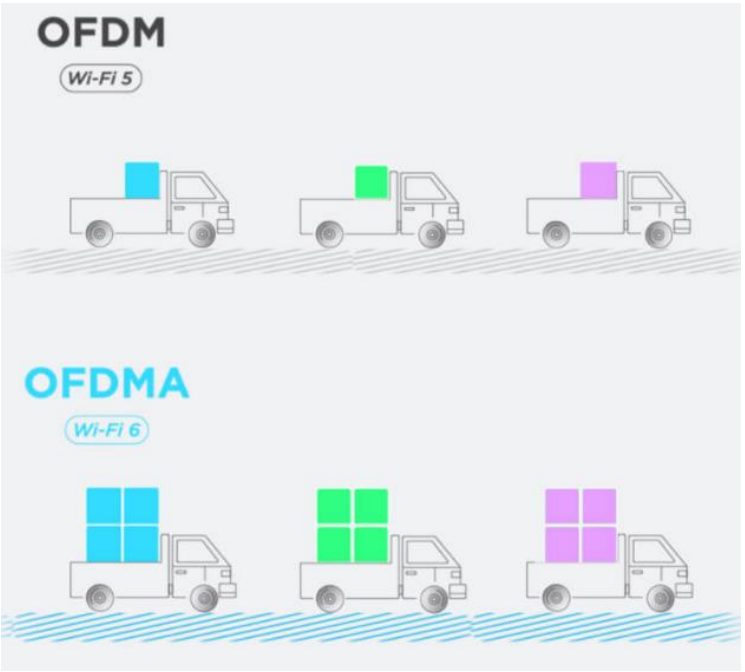
**Velocidad.**



# Wi-Fi 6

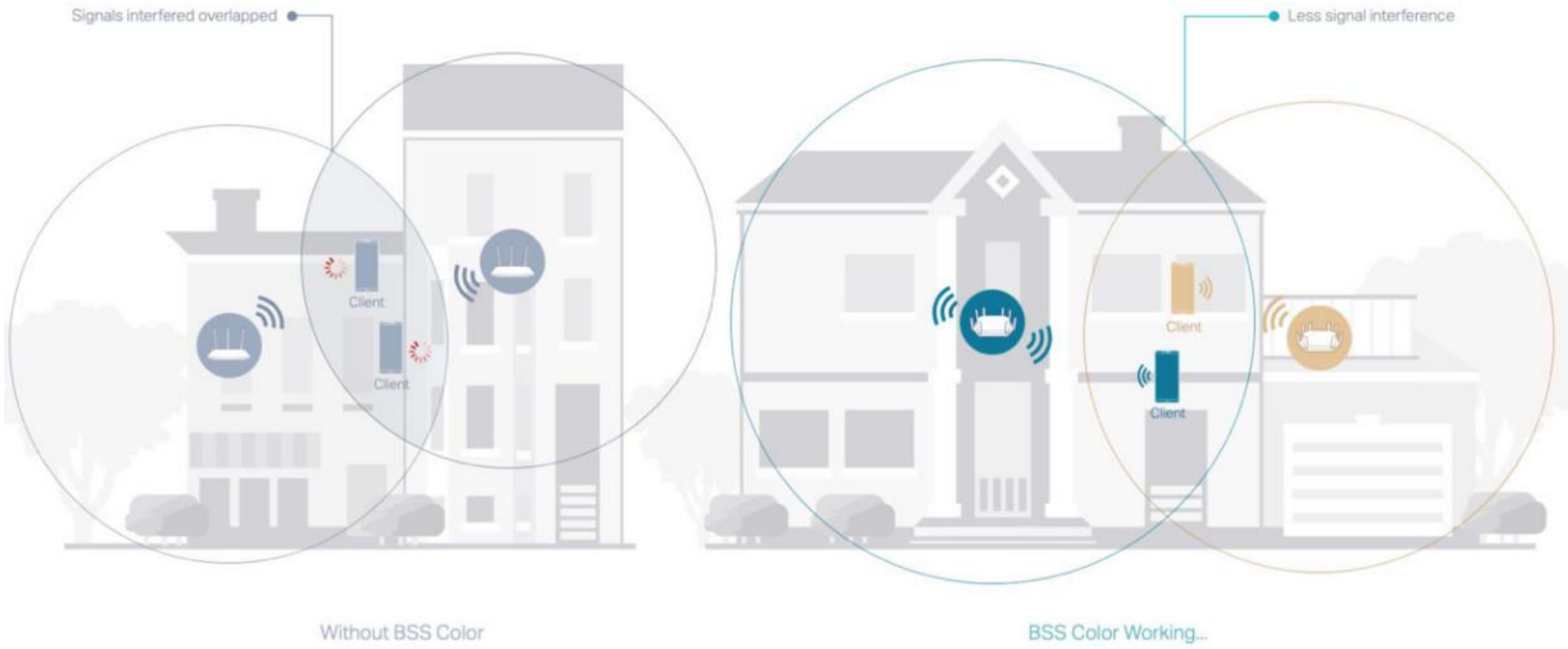
## Manejo de múltiples dispositivos.



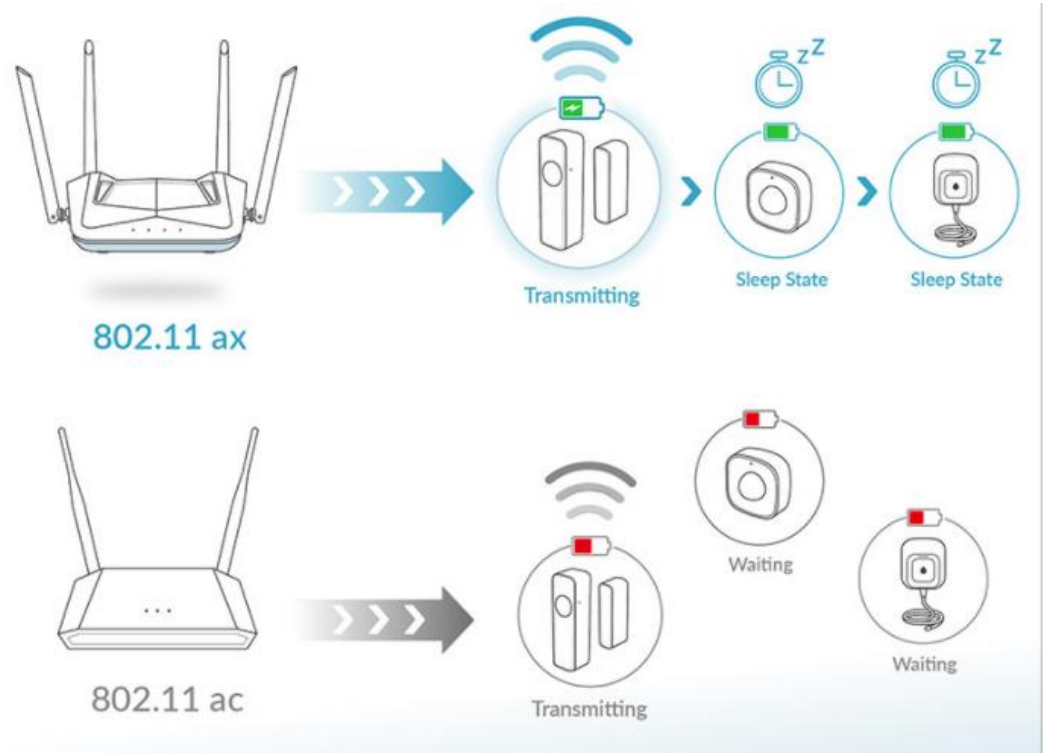
# Wi-Fi 6

## Coloración BSS.



# Wi-Fi 6

## Menor consumo energético



UNIVERSIDAD DON BOSCO

VITAM IMPENDERE VERO

# EDUCACIÓN SUPERIOR CON ESTILO SALESIANO

AUTORIDAD DE AVIACIÓN CIVIL A.A.C. EL SALVADOR
Certificación del Técnico en Mantenimiento Aeronáutico
2016-2021

ACAAI
Agencia Centroamericana de Acreditación de Programas de Arquitectura y de Ingeniería

ISPO
INTERNATIONAL SOCIETY FOR PROSTHETICS AND ORTHOTICS
Acreditación Internacional en la carrera de Técnico en Ortesis y Prótesis
Presencial 2016-2021
A distancia 2018-2020

CdA
Comisión de Acreditación Calidad de la Educación Superior
UNIVERSIDAD DON BOSCO
ACREDITADA
2017 - 2022

Instituciones Salesianas de Educación Superior