Redes y comunicación de Datos 2

Sesión 21

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Dinámica: Lluvia de ideas sobre los estándares de las redes Inalámbricas.
- Estándar WIFI 802.11
- Punto de acceso inalámbrico y funcionamiento de WLAN
- Canales de frecuencia
- **Actividad:**
  - **Implementación de una red Wi-Fi**

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la sesión, el estudiante utiliza los conceptos de la tecnología inalámbrica para configurar una WLAN, a través de ejemplos desarrollados en clase.

Buenas Prácticas

Con respecto a la Sesión 20

- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

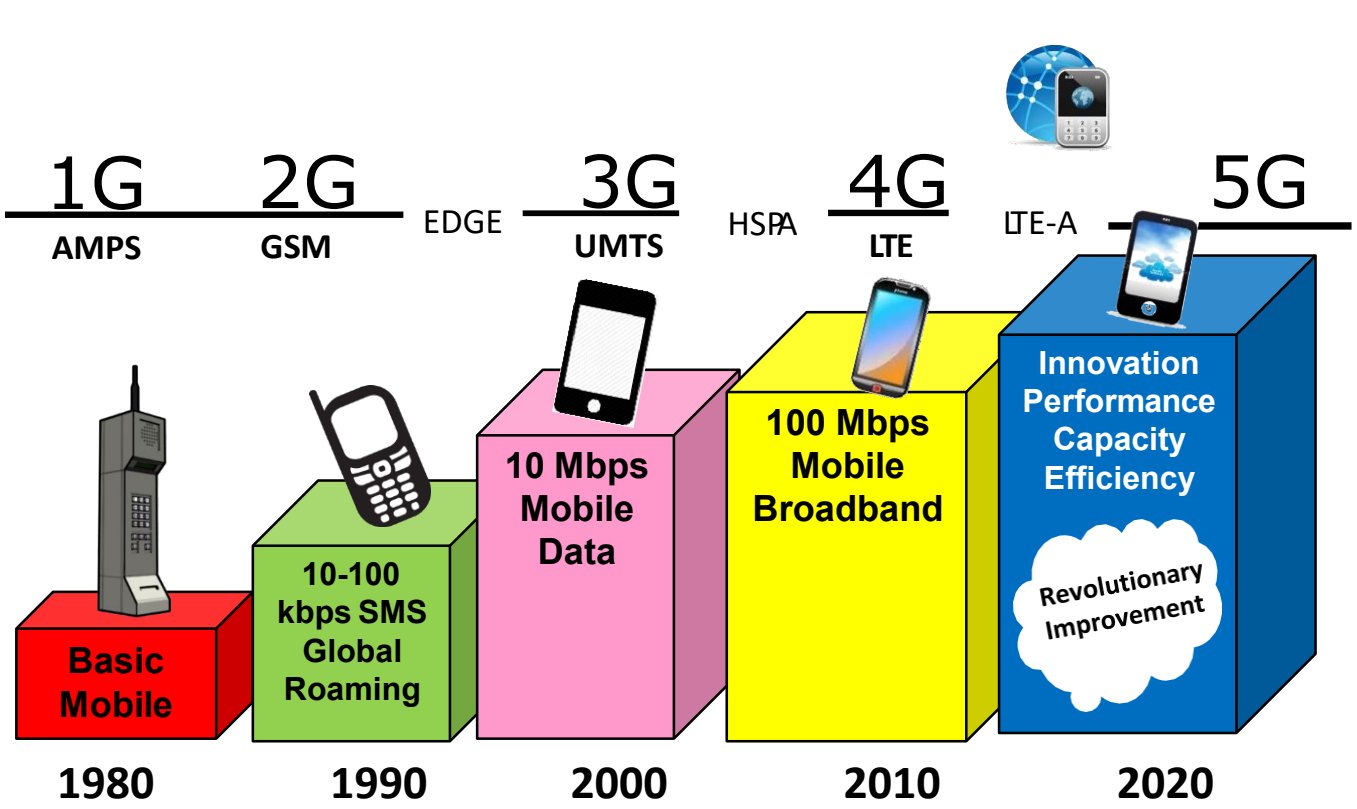
Introducción

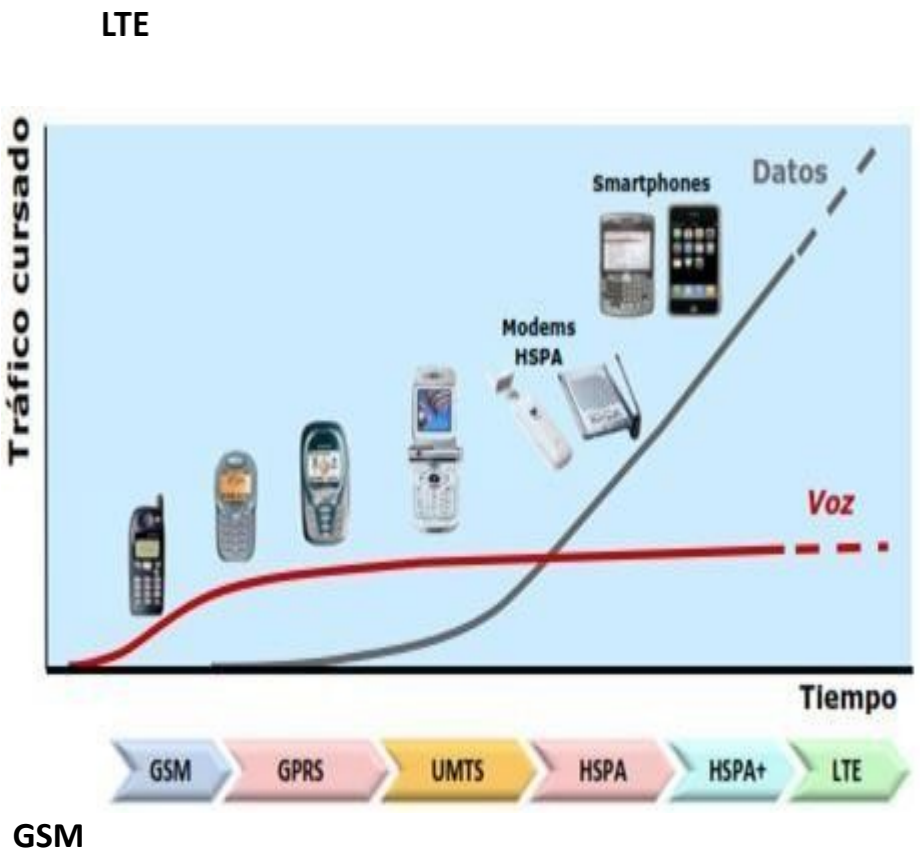
Los estándares del Instituto de ingenieros eléctricos y electrónicos (IEEE) para el Wi-Fi, según se especifican en el grupo colectivo de estándares 802,11 que especifican las frecuencias de radio, las velocidades y otras funcionalidades para las WLAN.

A través de los años, se han desarrollado varias implementaciones de los estándares IEEE 802.11

Evolución de la tecnología celulares

"Banda Ancha Móvil como el centro del universo de una Sociedad Conectada"





https://www.youtube.com/watch?v=h2oFquv96O8&t=216s

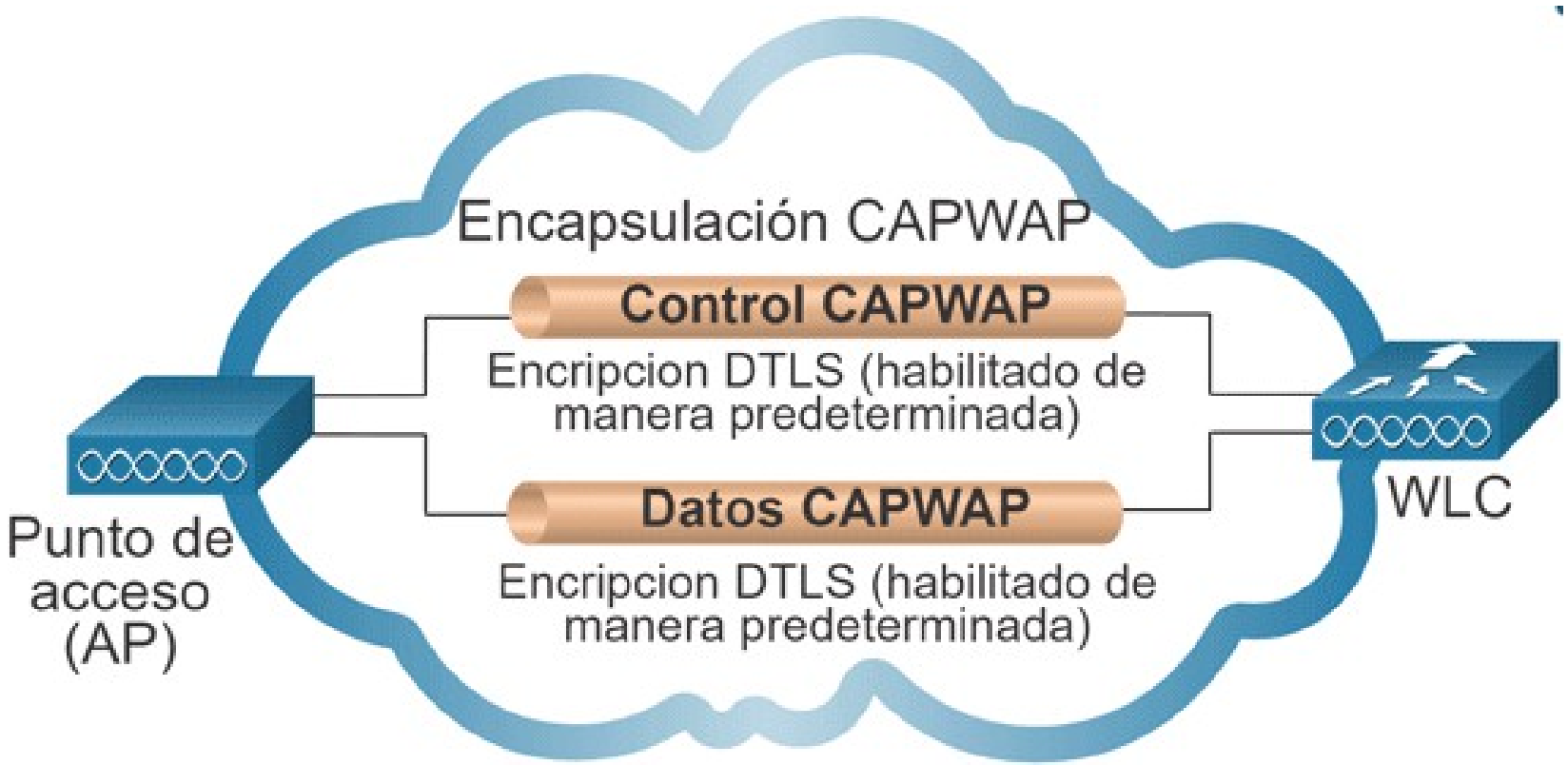
Buenas Prácticas

Sesión 21

Lluvia de ideas sobre las tecnologías inalámbricas

- ¿Qué es CAPWAP?
- ¿Para que nos sirve el FLEXCONNECT?

Funcionamiento de la CAPWAP



Operación de la CAPWAP

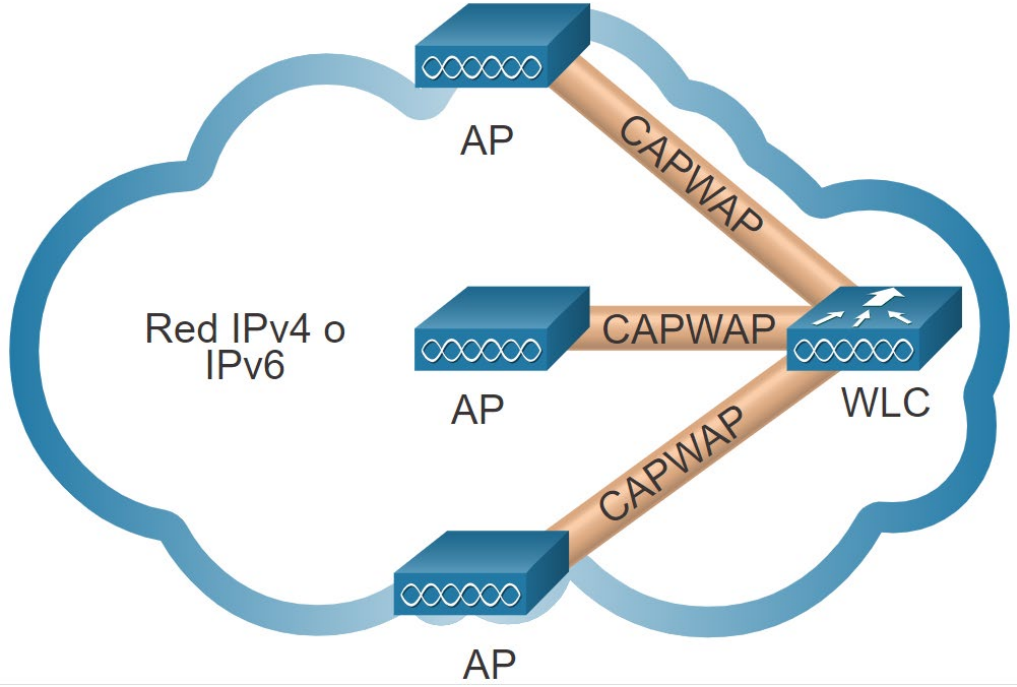
Introducción a CAPWAP

CAPWAP: Es el Control y aprovisionamiento de puntos de acceso inalámbricos. CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLANs. CAPWAP también es responsable de la encapsulación y el reenvío del tráfico del cliente WLAN entre un AP y un WLC.

Basado en El protocolo de punto de acceso ligero (LWAPP), pero agrega seguridad adicional con Datagram Transport Layer Security (DLTS).

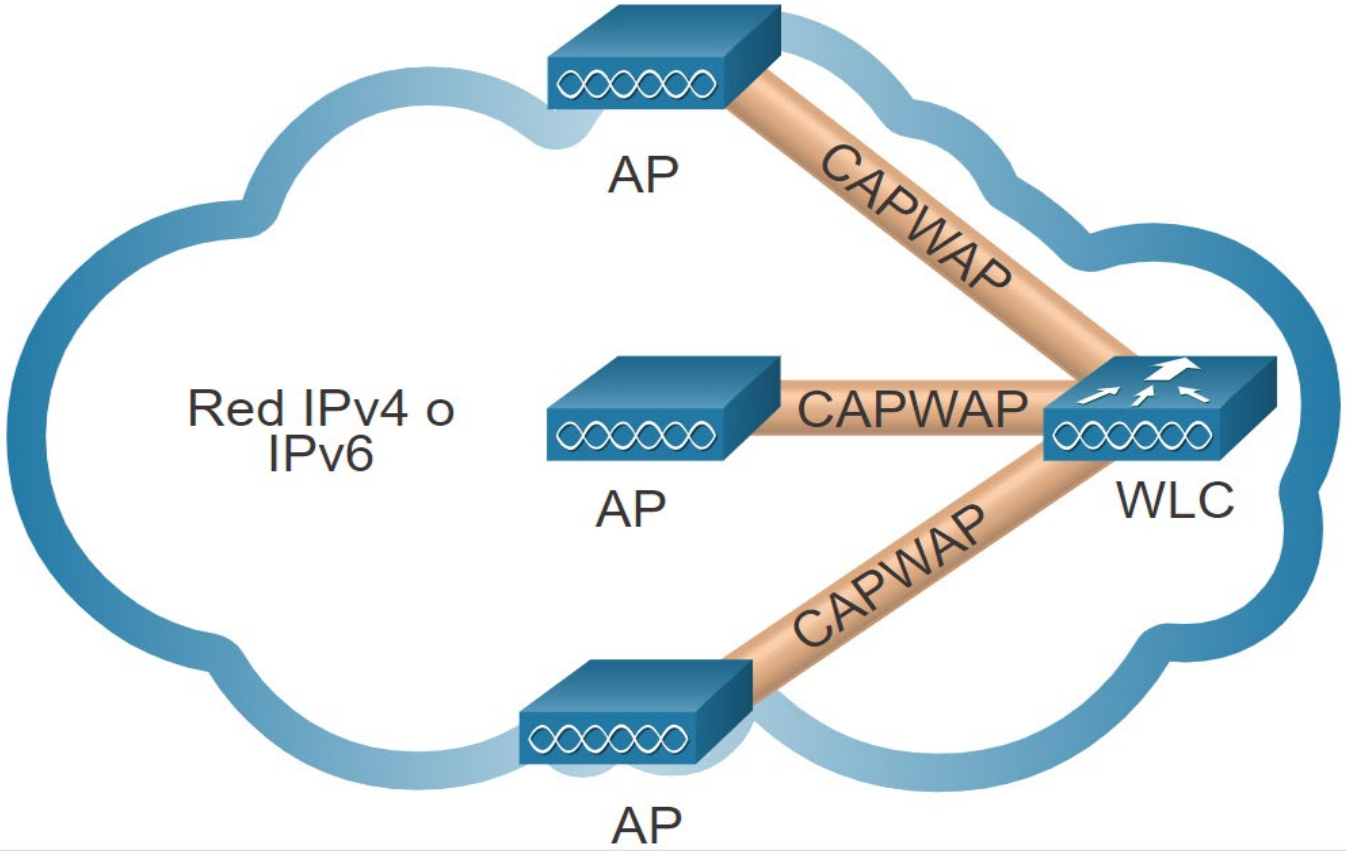
CAPWAP establece túneles en los puertos del Protocolo de datagramas de usuario (UDP).

CAPWAP puede operar sobre IPv4 o IPv6, pero usa IPv4 de manera predeterminada.



Introducción a CAPWAP

IPv4 e IPv6 pueden usar los puertos UDP 5246 y 5247. Sin embargo, los túneles CAPWAP usan diferentes protocolos IP en el encabezado de la trama. IPv4 usa el protocolo IP 17 e IPv6 usa el protocolo IP 136.



La figura muestra una pequeña red IPv4 o IPv6 en la nube. Un WLC se conecta a tres AP usando CAPWAP.

Operación de la CAPWAP

Arquitectura MAC dividida

Un componente clave de CAPWAP es el concepto de un control de acceso a medios divididos (MAC). El concepto CAPWAP split MAC realiza todas las funciones que normalmente realizan los AP individuales y las distribuye entre dos componentes funcionales:

- AP Funciones MAC
- Funciones WLC MAC

AP Funciones MAC	Funciones WLC MAC
Beacons y respuestas de sonda	Autenticación
Reconocimientos de paquetes y retransmisiones	Asociación y re-asociación de clientes itinerantes.
Cola de Frame y priorización de paquetes	Traducción de Frames a otros protocolos
Cifrado y descifrado de datos de capa MAC	Terminación del tráfico 802.11 en una interfaz cableada

Cifrado DTLS

DTLS es un protocolo que proporciona seguridad entre el AP y el WLC. Les permite comunicarse mediante encriptación y evita escuchas o alteraciones.

DTLS está habilitado de manera predeterminada para asegurar el canal de control CAPWAP pero está deshabilitado de manera predeterminada para el canal de datos.

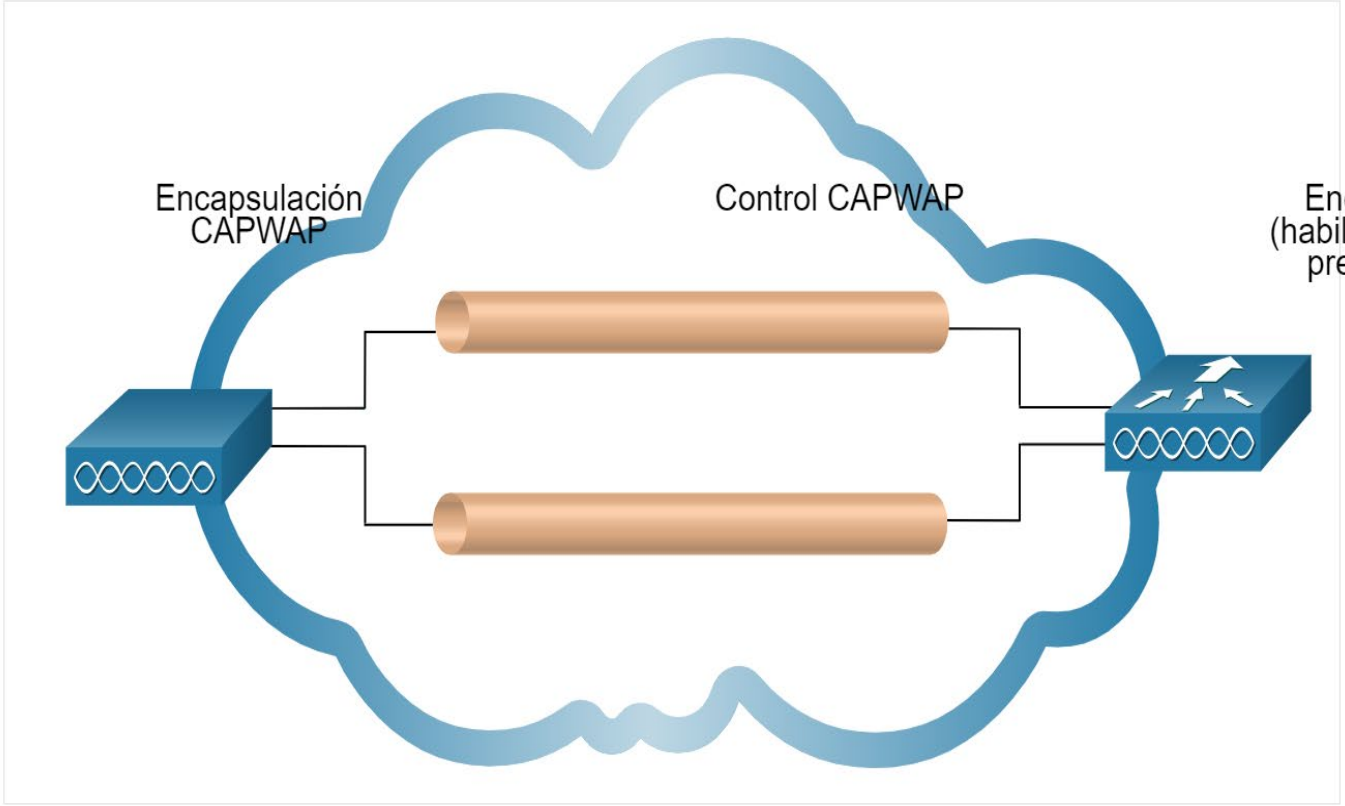
Todo el tráfico de control y gestión CAPWAP intercambiado entre un AP y WLC está encriptado y protegido de forma predeterminada para proporcionar privacidad en el plano de control y evitar ataques de Man-In-the-Middle (MITM).

Operación de CAPWAP

Cifrado DTLS

El cifrado de datos CAPWAP es opcional y se habilita para cada AP. El cifrado de datos está deshabilitado de manera predeterminada y requiere que se instale una licencia DTLS en el WLC antes de que se pueda habilitar en el AP.

Cuando está habilitado, todo el tráfico del cliente WLAN se encripta en el AP antes de reenviarse al WLC y viceversa.



Conexión flexible a AP

FlexConnect es una solución inalámbrica para las implementaciones en sucursales y oficinas remotas. Le permite configurar y controlar puntos de acceso en una sucursal desde la oficina corporativa a través de un enlace WAN, sin implementar un controlador en cada oficina.

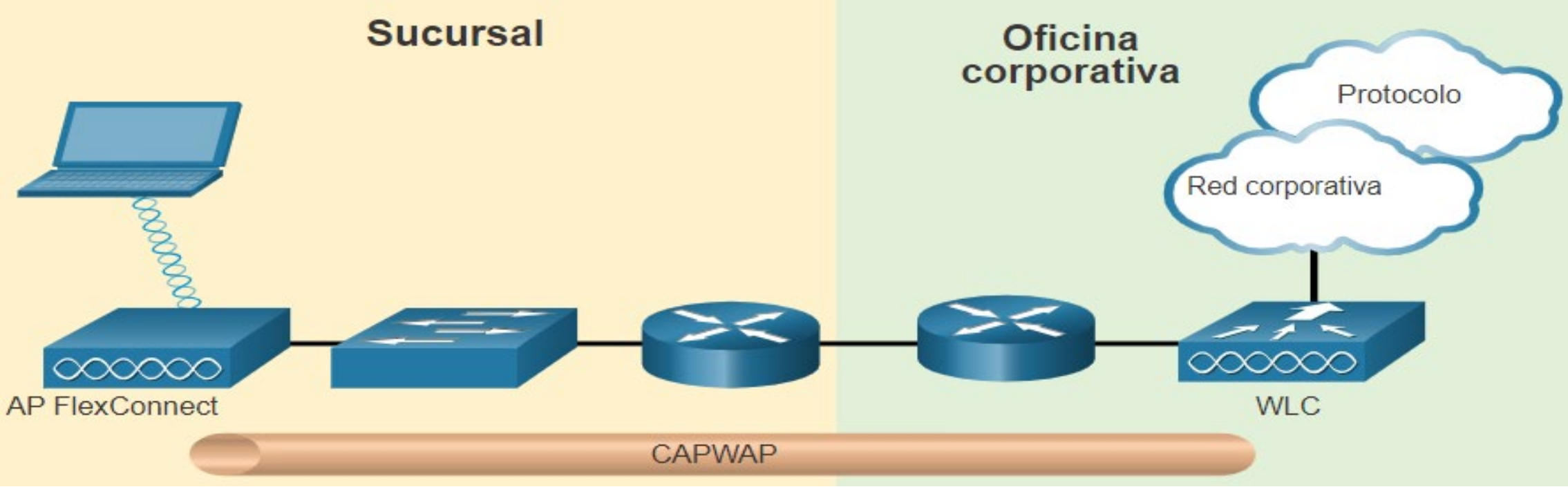
Hay dos modos de opción para FlexConnect AP:

- **Modo conectado -** El WLC es accesible. En este modo, el AP FlexConnect tiene conectividad CAPWAP con su WLC y puede enviar tráfico a través del túnel CAPWAP, como se muestra en la figura. El WLC realiza todas las funciones CAPWAP.
- **Modo independiente -** El WLC es inalcanzable. El AP FlexConnect ha perdido la conectividad CAPWAP con el WLC. El AP FlexConnect puede asumir algunas de las funciones de WLC, como cambiar el tráfico de datos del cliente localmente y realizar la autenticación del cliente localmente.

Operación de CAPWAP

Conexión flexible a AP

La figura muestra un túnel CAPWAP formado entre un AP FlexConnect en una sucursal y un WLC en una oficina corporativa. El equipo de la sucursal consiste en una computadora portátil con conexión inalámbrica a un AP FlexConnect conectado a un switch, que está conectado a un router. Luego, el router se conecta a otro router en la oficina corporativa a la que está conectado el WLC. El WLC proporciona acceso a la red corporativa e Internet.



Gestión de Canales

Canal de Frecuencia de Saturación

Los dispositivos de LAN inalámbricos tienen transmisores y receptores sintonizados a frecuencias específicas de ondas de radio para comunicarse. Una práctica común es que las frecuencias se asignen como rangos. Los rangos se dividen en rangos más pequeños llamados canales.

Si la demanda de un canal específico es demasiado alta, es probable que ese canal se sature en exceso. La saturación del medio inalámbrico degrada la calidad de la comunicación.

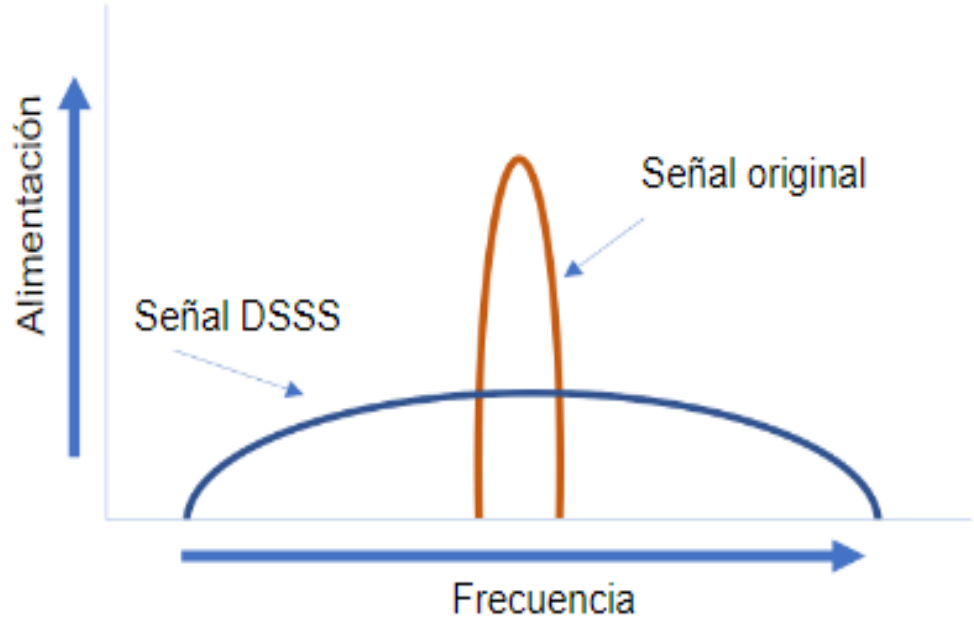
Con los años, se han creado una serie de técnicas para mejorar la comunicación inalámbrica y aliviar la saturación. Estas técnicas mitigan la saturación de canales usándolos de manera más eficiente.

Canal de Frecuencia de Saturación

Espectro de extensión de la secuencia directa (DSSS) - Una técnica de modulación diseñada para extender una señal sobre una banda de frecuencia más grande.

Las técnicas de amplio espectro se desarrollaron durante el tiempo de guerra para que sea más difícil para los enemigos interceptar o bloquear una señal de comunicación.

Lo hace al extender la señal sobre una frecuencia más amplia que efectivamente oculta el pico discernible de la señal, como se muestra en la figura. Un receptor configurado correctamente puede revertir la modulación DSSS y reconstruir la señal original. DSSS es Usado por dispositivos 802.11b para evitar interferencias de otros dispositivos que usan la misma frecuencia de 2.4 GHz.

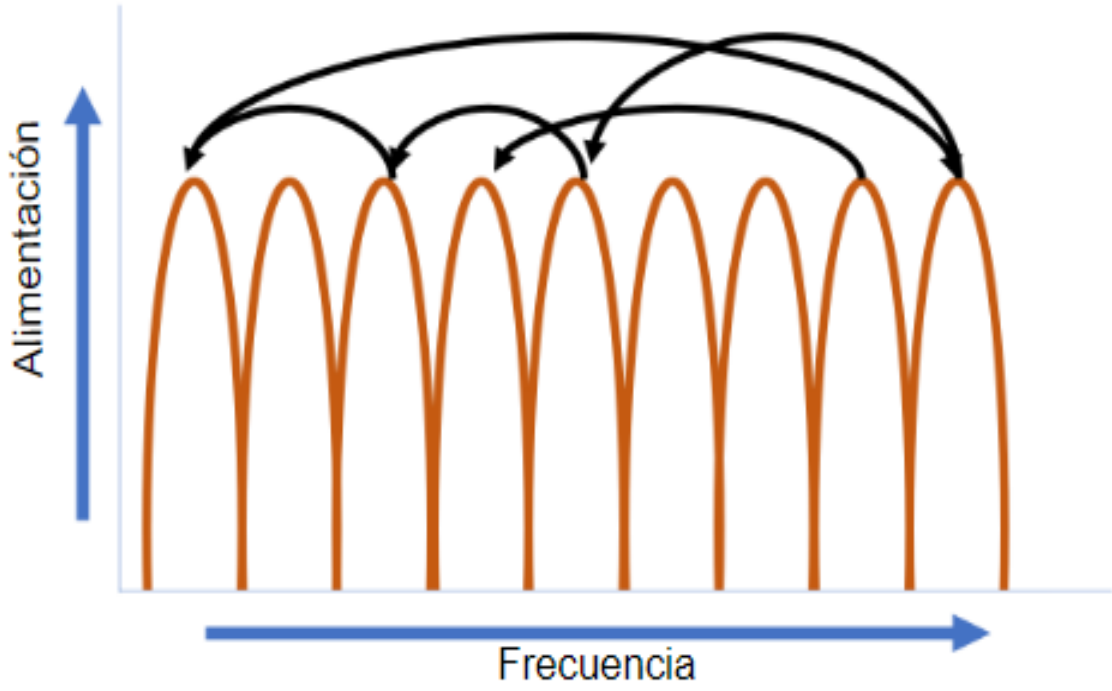


Canal de Frecuencia de Saturación

Espectro ensanchado por salto de frecuencia (FHSS)- Esto se basa en métodos de amplio espectro para comunicarse.

Transmite señales de radio cambiando rápidamente una señal portadora entre muchos canales de frecuencia. El emisor y el receptor deben estar sincronizados para "saber" a qué canal saltar.

Este proceso de salto de canal permite un uso más eficiente de los canales, disminuyendo la congestión del canal. FHSS fue Usado por el estándar 802.11 original. Los walkie-talkies y los teléfonos inalámbricos de 900 MHz también usan FHSS, y Bluetooth usa una variación de FHSS.

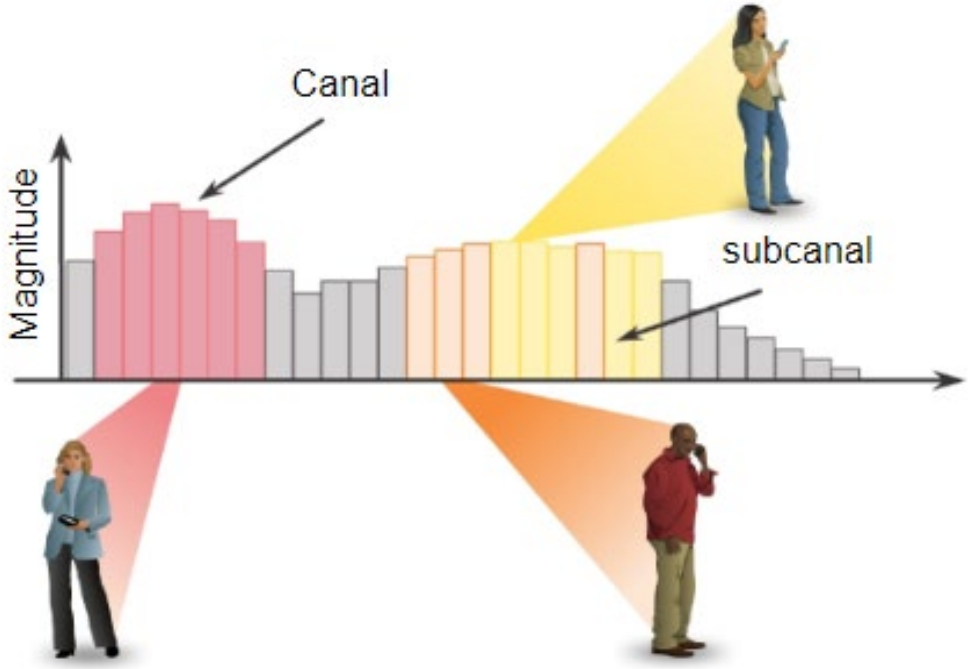


Canal de Frecuencia de Saturación

Multiplexación por división de frecuencias ortogonales (OFDM) - subconjunto de multiplexación por división de frecuencia en el que un solo canal utiliza múltiples subcanales en frecuencias adyacentes.

Los subcanales en un sistema OFDM son precisamente ortogonales entre sí, lo que permite que los subcanales se superpongan sin interferir.

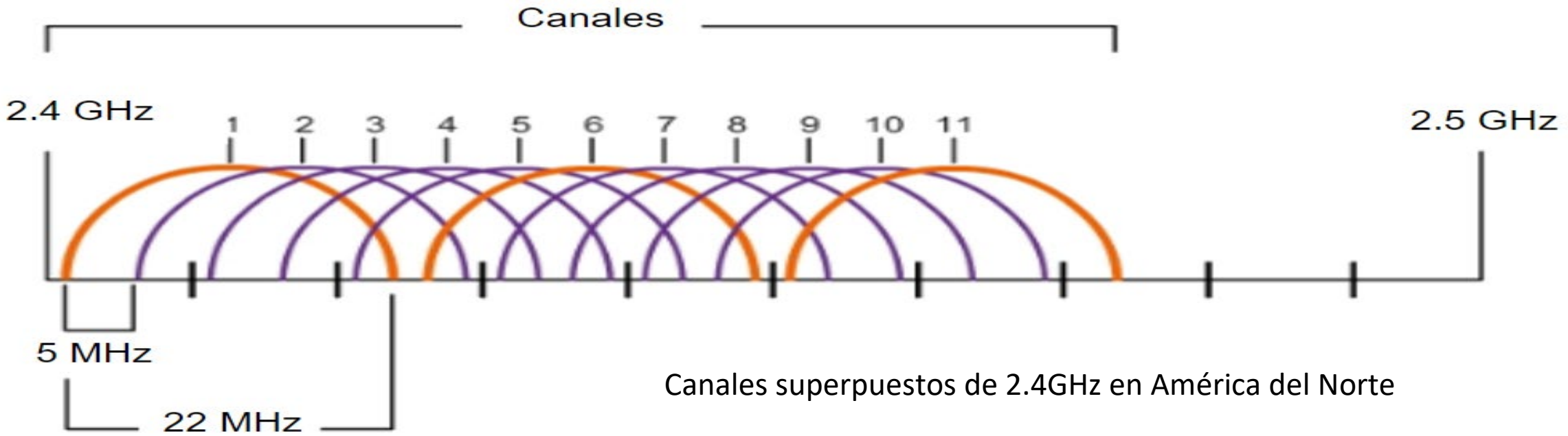
OFDM es utilizado por varios sistemas de comunicación, incluidos 802.11a/g/n/ac. El nuevo 802.11ax utiliza una variación de OFDM llamada acceso múltiple por división de frecuencia ortogonal (OFDMA).



Gestión de Canales (Channel Management)

Selección del canal

Una práctica recomendada para las WLAN que requieren múltiples AP es utilizar canales no superpuestos. Por ejemplo, los estándares 802.11b/g/n operan en el espectro de 2.4 GHz a 2.5GHz. La banda 2.4 GHz está subdividida en múltiples canales. Cada canal tiene un ancho de banda de 22 MHz y está separado del siguiente canal por 5 MHz. El estándar 802.11b identifica 11 canales para América del Norte, como se muestra en la figura (13 en Europa y 14 en Japón).



Canales superpuestos de 2.4GHz en América del Norte

Gestión de Canales (Channel Management)

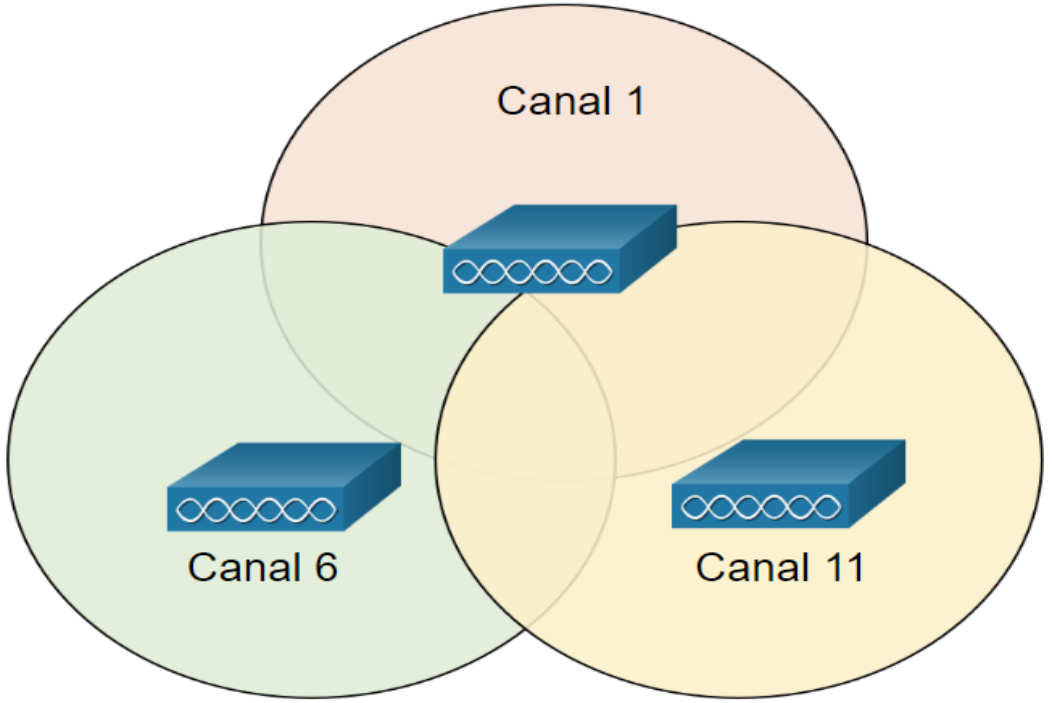
Selección del canal

La interferencia ocurre cuando una señal se superpone a un canal reservado para otra señal, causando una posible distorsión.

La mejor práctica para las WLAN de 2.4GHz que requieren múltiples AP es usar canales no superpuestos, aunque la mayoría de los AP modernos lo harán automáticamente.

Si hay tres AP adyacentes, use los canales 1, 6 y 11, como se muestra en la figura.

Canales no superpuestos de 2.4GHz para 802.11b/g/n



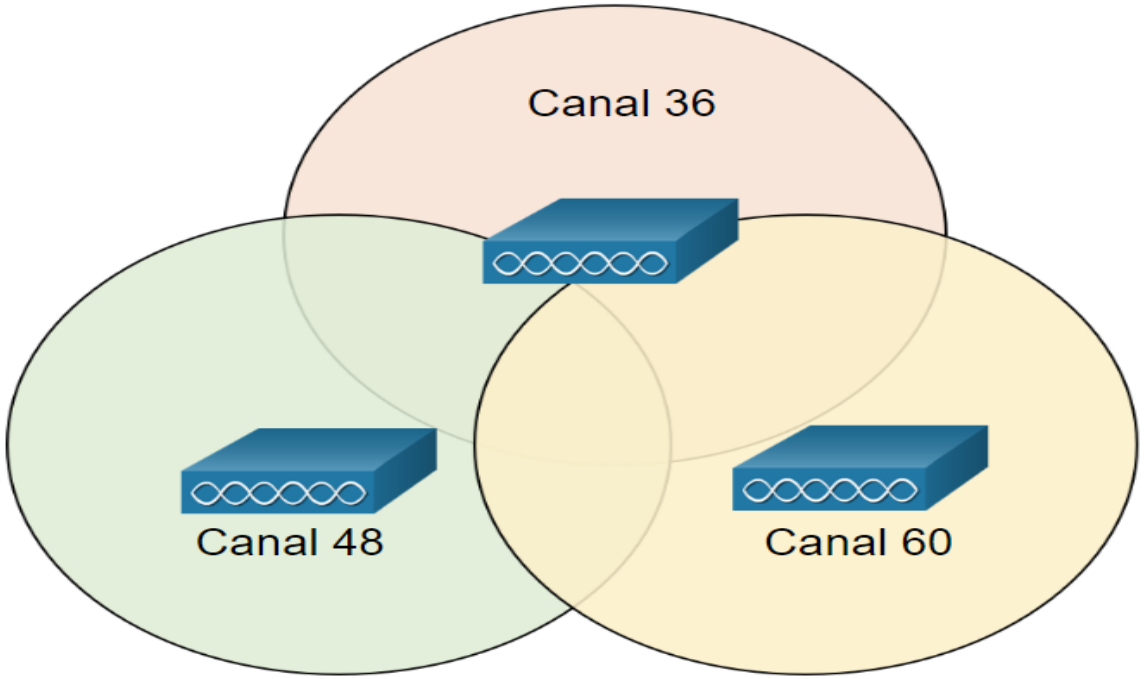
Gestión de Canales (Channel Management)

Selección del canal

La conexión inalámbrica de 5 GHz puede proporcionar una transmisión de datos más rápida para clientes inalámbricos en redes inalámbricas muy pobladas debido a la gran cantidad de canales inalámbricos no superpuestos.

Al igual que con las WLAN de 2.4GHz, elija canales que no interfieran al configurar múltiples AP de 5GHz adyacentes entre sí, como se muestra en la figura.

Canales no interferentes de 5 GHz para 802.11a/n/ac



Amenazas en la WLAN

Resumen de seguridad inalámbrica

Una WLAN está abierta a cualquier persona dentro del alcance de un AP y las credenciales apropiadas para asociarla. Con una NIC inalámbrica y conocimiento de técnicas de craqueo, un atacante puede no tener que ingresar físicamente al lugar de trabajo para obtener acceso a una WLAN. Los ataques pueden ser generados por personas externas, empleados descontentos e incluso involuntariamente por los empleados. Las redes inalámbricas son específicamente susceptibles a varias amenazas, incluidas las siguientes:

- **Intercepción de datos -** Los datos inalámbricos deben estar encriptados para evitar que los espías los lean.
- **Intrusos inalámbricos -** Los usuarios no autorizados que intentan acceder a los recursos de la red pueden ser disuadidos mediante técnicas de autenticación efectivas.
- **Ataques de denegación de servicio (DoS) -** El acceso a los servicios WLAN puede verse comprometido de forma accidental o maliciosa. Existen varias soluciones dependiendo de la fuente del ataque DoS.
- **APs Falsos -** Los AP no autorizados instalados por un usuario bien intencionado o con fines maliciosos se pueden detectar utilizando un software de administración.

Ataques DoS

Los ataques DoS inalámbricos pueden ser el resultado de:

- **Dispositivos configurados inapropiadamente -** Los errores de configuración pueden deshabilitar la WLAN. Por ejemplo, un administrador podría alterar accidentalmente una configuración y deshabilitar la red, o un intruso con privilegios de administrador podría deshabilitar intencionalmente una WLAN.

- **Un usuario malintencionado que interfiere intencionalmente con la comunicación inalámbrica. -** Su objetivo es deshabilitar la red inalámbrica por completo o hasta el punto en que ningún dispositivo legítimo pueda acceder al medio.

- **Interferencia Accidental -** La redes WLANs son propensas a interferencia de otros dispositivos inalámbricos como hornos microondas, teléfonos inalámbricos, monitores de bebé y más como se muestra en la figura. La banda 2.4 GHz es más propensa a interferencia que la banda 5 GHz.

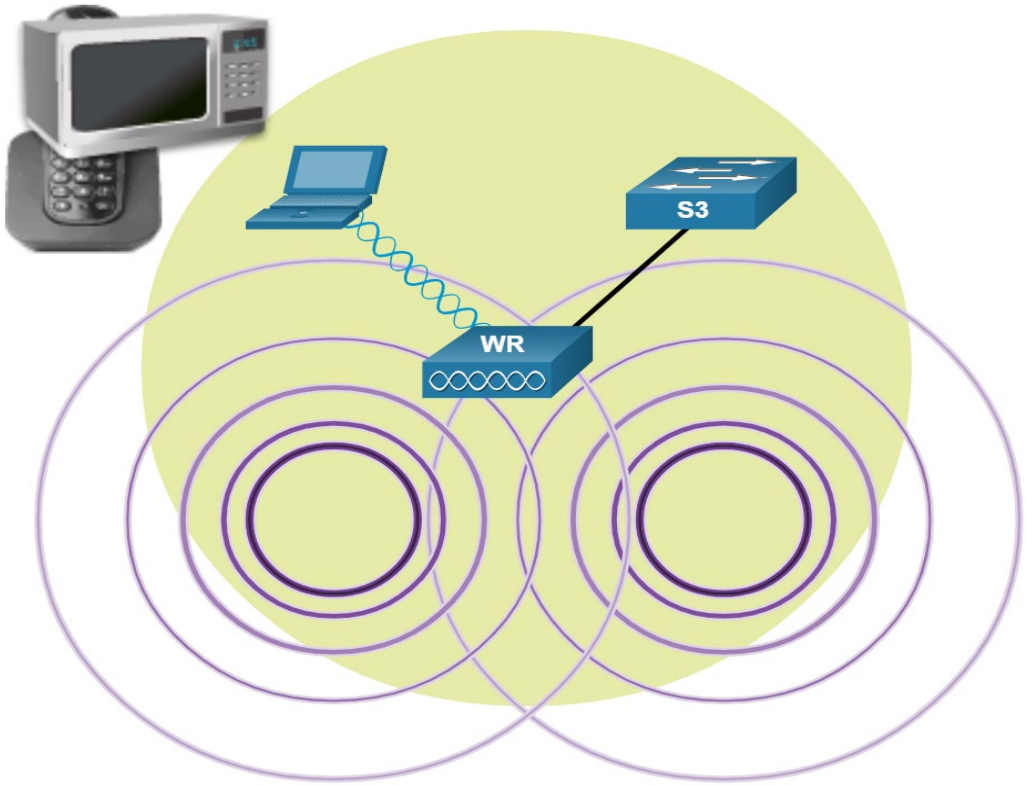
Amenazas en la WLAN

Ataques DoS

Para minimizar el riesgo de un ataque DoS debido a dispositivos mal configurados y ataques maliciosos, fortalezca todos los dispositivos, mantenga las contraseñas seguras, cree copias de seguridad y asegúrese de que todos los cambios de configuración se incorporen fuera de horario.

Monitoree la WLAN en busca de problemas de interferencia accidental y atiéndalos cuando aparezcan.

Debido a que la banda 2.4 GHz es usada por otro tipo de dispositivos, la banda 5 GHz debe ser usada en áreas propensas a interferencias.



Puntos de acceso no autorizados

Un AP falso es un AP o un router inalámbrico que se ha conectado a una red corporativa sin autorización explícita y en contra de la política corporativa. Cualquier persona con acceso a las instalaciones puede instalar (de forma maliciosa o no maliciosa) un enrutador inalámbrico de bajo costo que potencialmente puede permitir el acceso a un recurso de red seguro.

Una vez conectado, el AP falso puede ser usado por el atacante para capturar direcciones MAC, capturar paquetes de datos, obtener acceso a recursos de red o lanzar un ataque intermediario.

Un punto de acceso a la red personal también podría usarse como un AP no autorizado, por ejemplo, un usuario con acceso seguro a la red permite que su host Windows autorizado se convierta en un AP Wi-Fi. Al hacerlo, elude las medidas de seguridad y otros dispositivos no autorizados ahora pueden acceder a los recursos de la red como un dispositivo compartido.

Ataques intermediarios

En un ataque intermediario (MITM por su sigla en inglés), el pirata informático se coloca entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes. Hay muchas maneras de crear un ataque MITM.

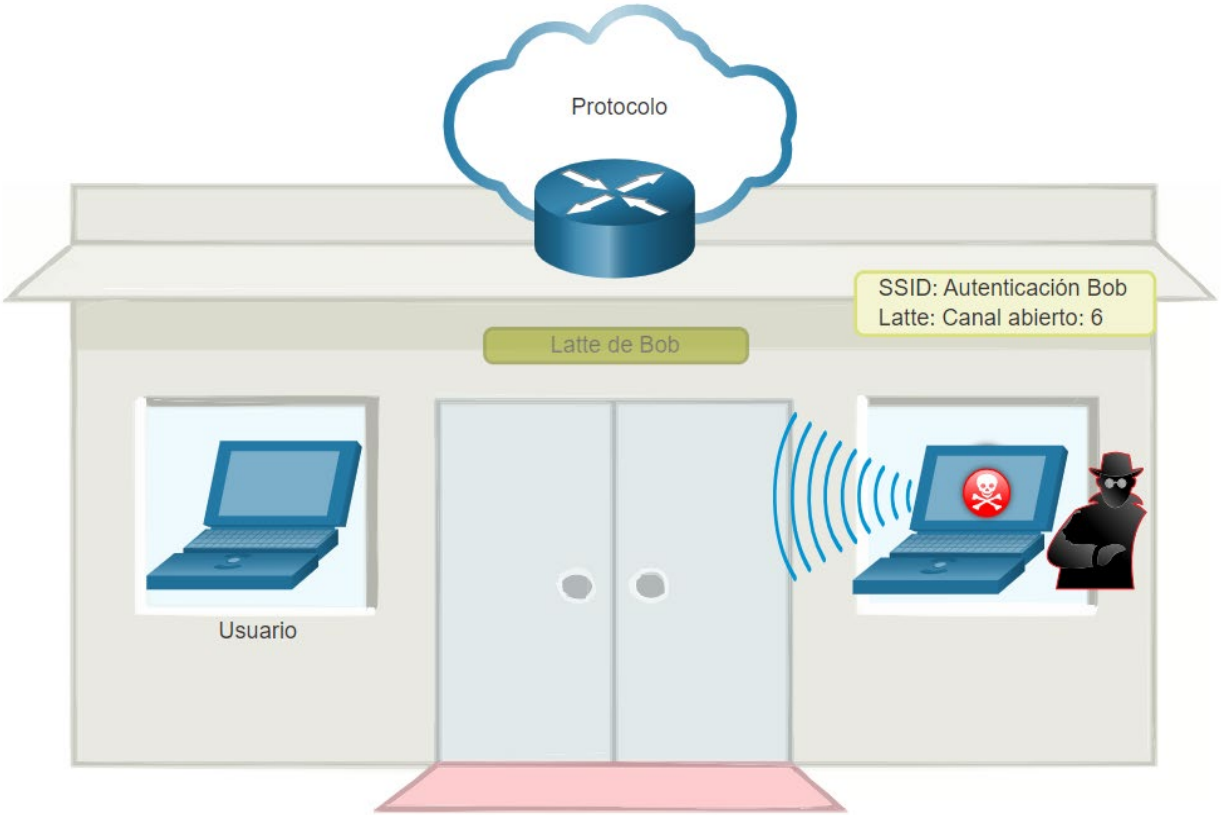
Un ataque de "AP gemelo malvado" es un ataque MITM inalámbrico popular en el que un atacante introduce un AP falso y lo configura con el mismo SSID que un AP legítimo, estas pueden ser las ubicaciones que ofrecen Wi-Fi gratis, como aeropuertos, cafeterías y restaurantes, son lugares particularmente populares para este tipo de ataque debido a la autenticación abierta.

Amenazas en la WLAN

Ataques intermediarios

Clientes inalámbrico que se tratan de conectar a una red WLAN podrían ver dos APs con el mismo SSID ofreciendo acceso inalámbrico. Los que están cerca del AP falso encuentran la señal más fuerte y probablemente se asocian con ella.

El tráfico de usuarios ahora se envía al AP falso, que a su vez captura los datos y los reenvía al AP legítimo, como se muestra en la figura. El tráfico de retorno del AP legítimo se envía al AP falso, se captura y luego se reenvía al usuario desprevenido. El atacante puede robar la contraseña del usuario, su información personal, obtener acceso a su dispositivo y comprometer el sistema

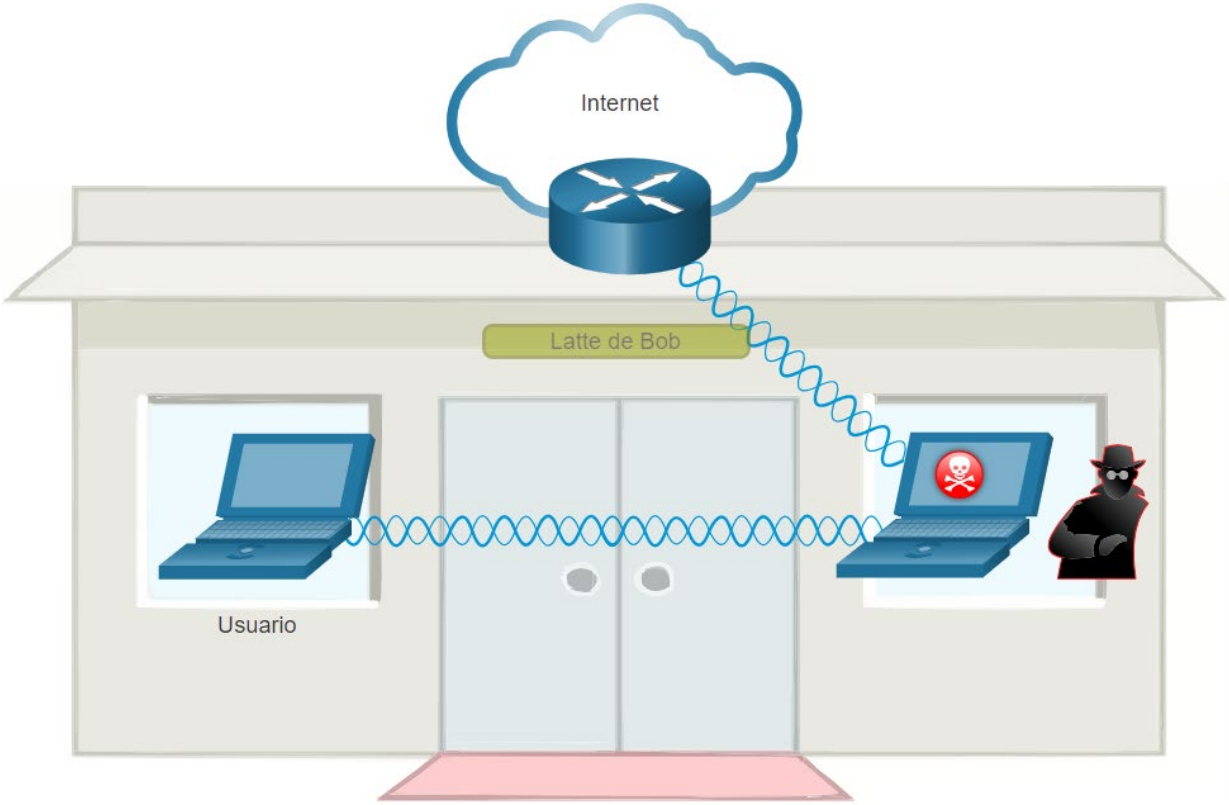


Ataques intermediarios

La derrota de un ataque como un ataque MITM depende de la sofisticación de la infraestructura WLAN y la vigilancia en el monitoreo de la actividad en la red. El proceso comienza con la identificación de dispositivos legítimos en la WLAN.

Para hacer esto los usuarios deben estar autenticados.

Una vez que todos los dispositivos legítimos son conocidos, la red puede ser monitoreada de dispositivos o tráfico anormal.

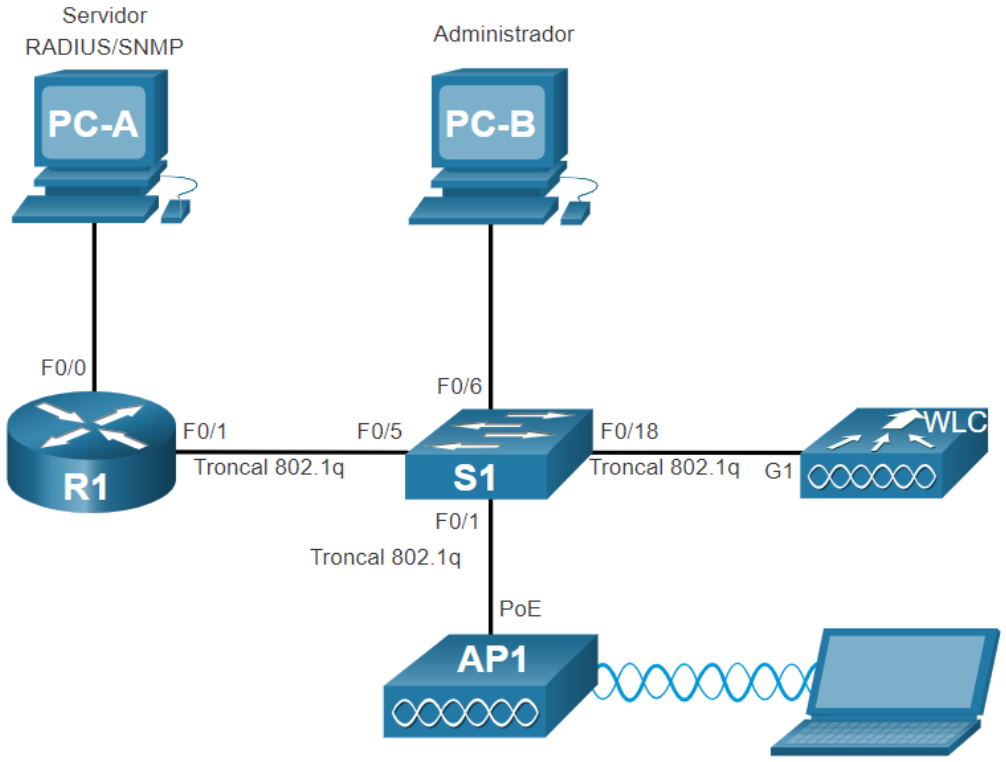


Topología WLC

Para topologia y el esquema de direccionamiento usados en los videos y este tema se muestran en la figura y en la tabla. El punto de acceso (AP) es basado en un controlador, que es diferente a un AP autónomo. Recuerde que los puntos de acceso basados en controlador no necesitan una configuración inicial y normalmente se les denomina Puntos de Acceso Lightweight (LAPs).

Los puntos de acceso LAP usan el Protocolo Lightweight Access Point Protocol (LWAPP) para comunicarse con el controlador WLAN (WLC).

Los puntos de acceso basados en controlador son útiles en situaciones en las que se necesitan varios puntos de acceso en la red. Conforme se agregan puntos de acceso, cada punto de acceso es configurado y administrado de manera automática por el WLC.

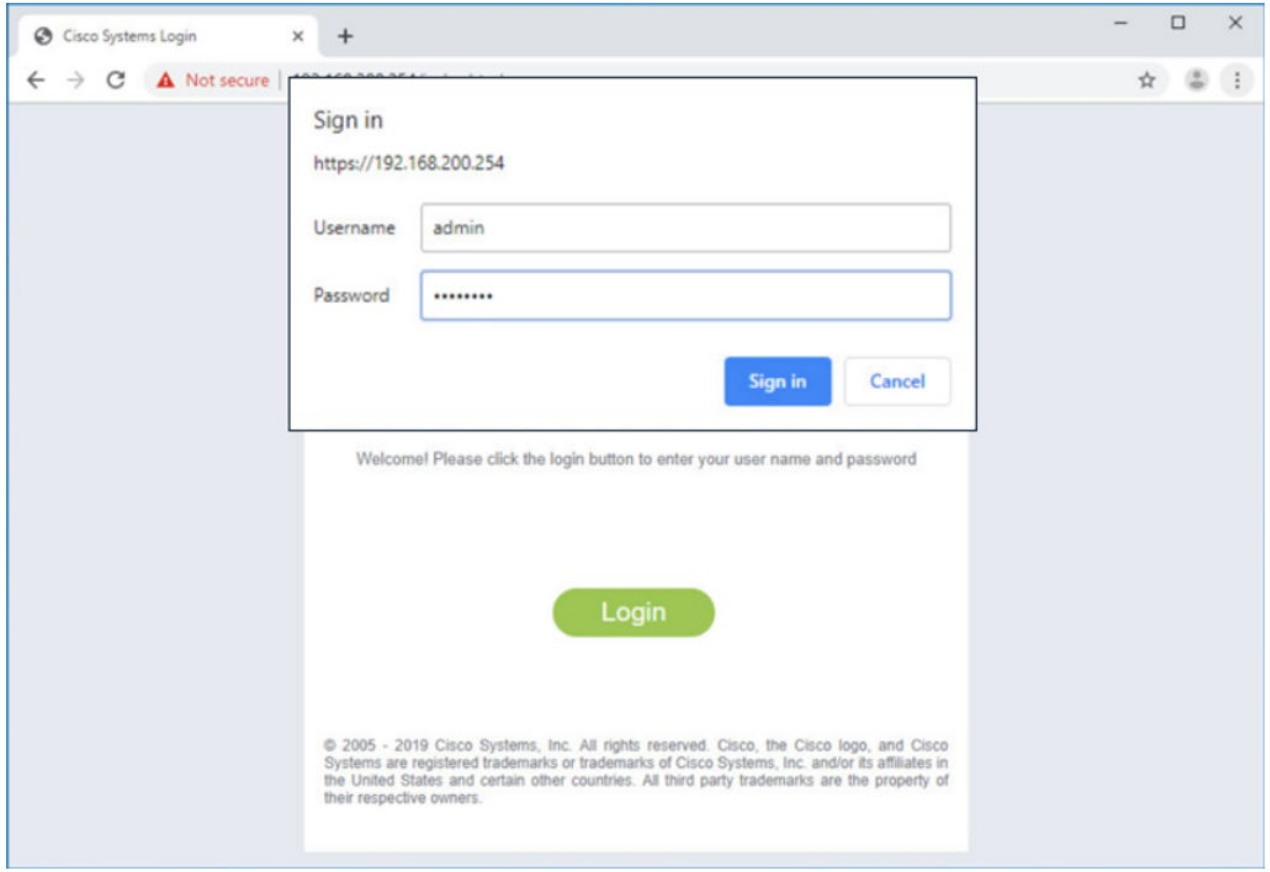


Iniciar sesión en el WLC

Configurar un controlador de red inalámbrica (WLC) no es muy diferente que configurar un router inalámbrico La diferencia mas grande es que el WLC controla los puntos de acceso y provee más servicios y capacidades de administración.

Nota: Las figuras de este tema que muestran la interfaz gráfica (GUI) y los menús, son del Controlador Inalámbrico Cisco 3504. Sin embargo, otros modelos de WLC tienen menús y características similares.

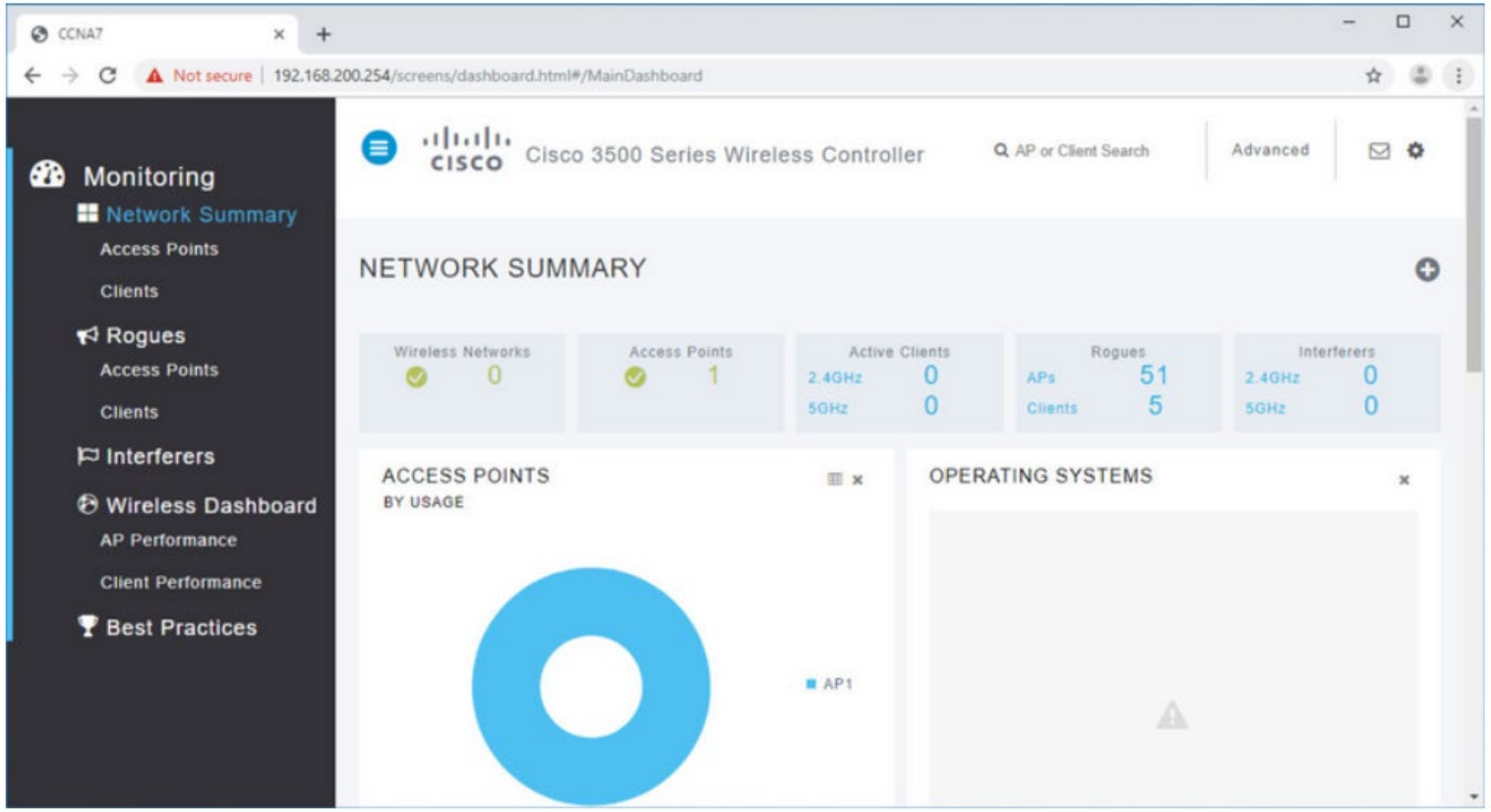
La figura muestra un usuario iniciando sesión en el WLC con los credenciales que fueron configurados en la configuración inicial.



Iniciar sesión en el WLC

La página de **Network Summary** es un panel que provee una visión rápida del número de redes inalámbricas configuradas, los puntos de acceso asociados y los clientes activos.

También se puede ver la cantidad de puntos de acceso dudosos y los clientes, como se muestra en la figura.



WLAN seguras

Encubrimiento SSID y filtrado de direcciones MAC

Para abordar las amenazas de mantener alejados a los intrusos inalámbricos y proteger los datos, se utilizaron dos características de seguridad tempranas que aún están disponibles en la mayoría de los enrutadores y puntos de acceso:

Encubrimiento SSID

- Los AP y algunos enrutadores inalámbricos permiten deshabilitar la trama de baliza SSID, (Beacon frame SSID). Los clientes inalámbricos deben configurarse manualmente con el SSID para conectarse a la red.

Filtrado de Direcciones MAC

- Un administrador puede permitir o denegar manualmente el acceso inalámbrico de los clientes en función de su dirección física de hardware MAC. En la figura, el router está configurado para permitir dos direcciones MAC. Los dispositivos con diferentes direcciones MAC no podrán unirse a la WLAN de 2.4GHz.

802.11 Métodos de Autenticación Originales

La mejor manera de proteger una red inalámbrica es utilizar sistemas de autenticación y cifrado. Se introdujeron dos tipos de autenticación con el estándar 802.11 original:

Autenticación abierta

- No se requiere contraseña. Normalmente se usa para proporcionar acceso gratuito a Internet en áreas públicas como cafeterías, aeropuertos y hoteles.
- El cliente es responsable de proporcionar seguridad, como a través de una VPN.

Autenticación de clave compartida

- Proporciona mecanismos, como WEP, WPA, WPA2 y WPA3 para autenticar y cifrar datos entre un cliente inalámbrico y AP. Sin embargo, la contraseña se debe compartir previamente entre las dos partes para que estas se conecten.

Métodos de autenticación de clave compartida

Actualmente hay cuatro técnicas de autenticación de clave compartida disponibles, como se muestra en la tabla.

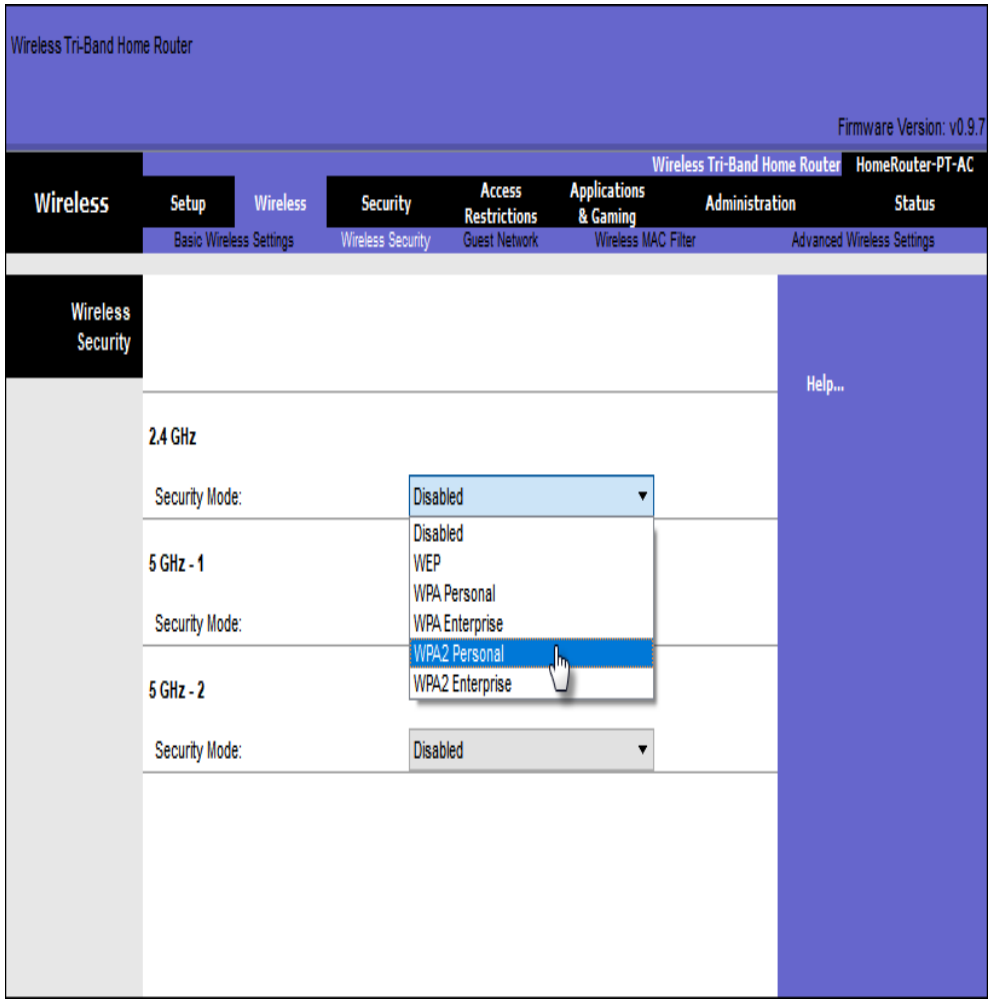
Método de Autenticación	Descripción
Privacidad Equivalente al Cableado (WEP)	La especificación original 802.11 diseñada para proteger los datos utilizando el método de cifrado Rivest Cipher 4 (RC4) con una clave estática. WEP ya no se recomienda y nunca debe usarse.
Acceso Protegido Wi-Fi (WPA)	Un estándar de Wi-Fi Alliance que usa WEP pero asegura los datos con el algoritmo de cifrado del Protocolo de integridad de clave temporal (TKIP) mucho más fuerte. El TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.
WPA2	Utiliza el Estándar de Cifrado Avanzado (AES) para el cifrado. AES actualmente se considera el protocolo de cifrado más sólido.
WPA3	Esta es la próxima generación de seguridad Wi-Fi. Todos los dispositivos habilitados para WPA3 utilizan los últimos métodos de seguridad, no permiten protocolos heredados obsoletos y requieren el uso de marcos de administración protegidos (PMF).

WLAN Seguras

Autenticando a un Usuario Doméstico

Los routers domésticos suelen tener dos opciones de autenticación: WPA y WPA2. Con WPA 2 tenemos dos métodos de autenticación.

- **Personal** – Destinados a redes domésticas o de pequeñas oficinas, los usuarios se autentican utilizando una clave precompartida (PSK). Los clientes inalámbricos se autentican con el enrutador inalámbrico utilizando una contraseña previamente compartida. No se requiere ningún servidor de autenticación especial.
- **Empresa** – Destinado a redes empresariales. Requiere un servidor de autenticación de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El servidor RADIUS debe autenticar el dispositivo y, a continuación, se deben autenticar los usuarios mediante el estándar 802.1X, que usa el protocolo de autenticación extensible (EAP).

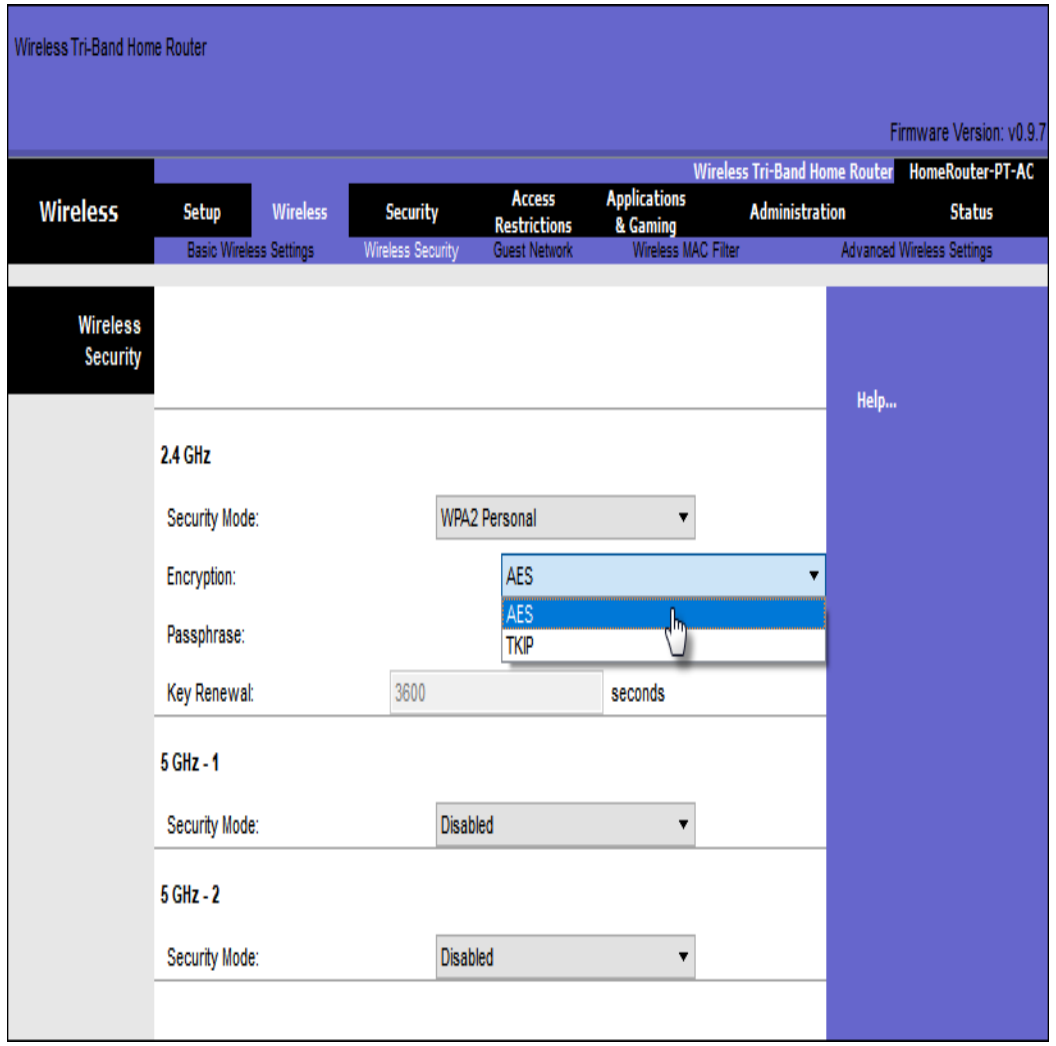


WLAN seguras

Métodos de encriptación

WPA y WPA2 incluyen dos protocolos de encriptación:

- **Protocolo de integridad de clave temporal (Temporal Key Integrity Protocol (TKIP))** – Utilizado por WPA y proporciona soporte para equipos WLAN heredados. Hace uso de WEP pero encripta la carga útil de Capa 2 usando TKIP.
- **Estándar de cifrado avanzado (Advanced Encryption Standard (AES))** – Utilizado por WPA2 y utiliza el modo de cifrado de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloque (CCMP) que permite a los hosts de destino reconocer si los bits cifrados y no cifrados han sido alterados.



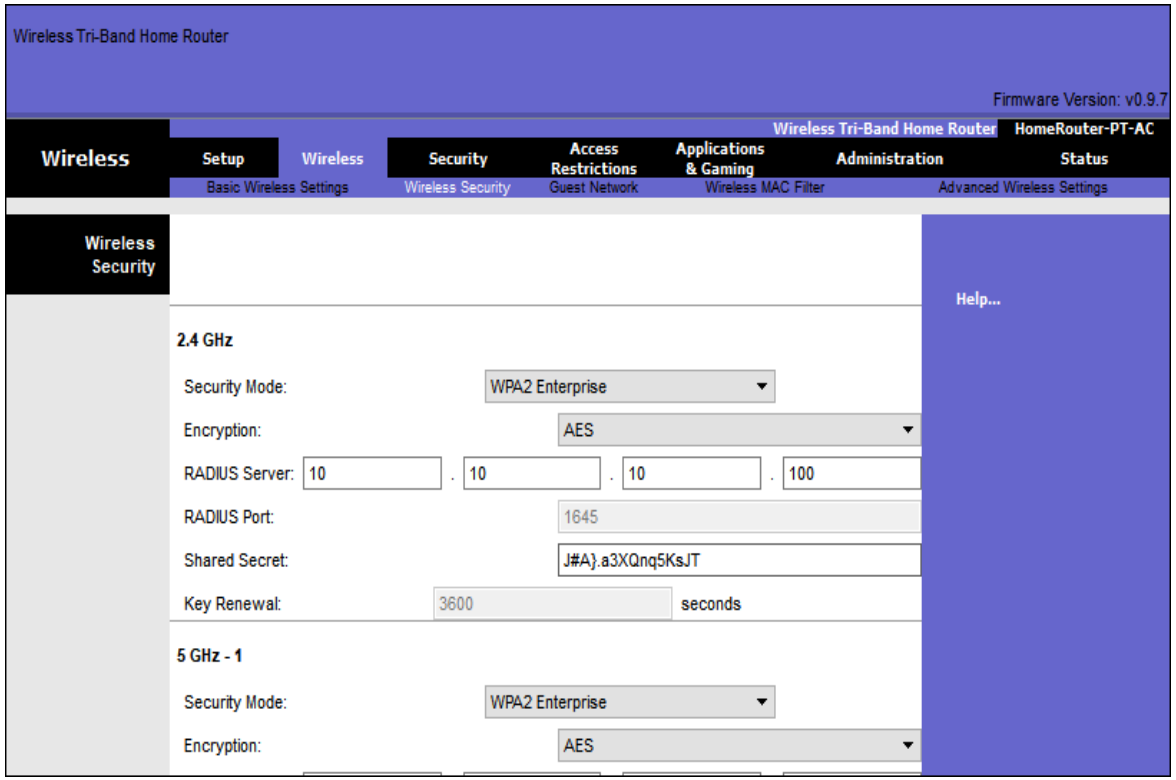
WLANs seguras

Autenticación en la empresa

La elección del modo de seguridad empresarial requiere un servidor RADIUS de autenticación, autorización y contabilidad (AAA).

Allí se requieren piezas de información:

- **Dirección IP del servidor RADIUS** – Dirección IP del servidor.
- **Números de puerto UDP**–Los puertos UDP 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar utilizando los puertos UDP 1645 y 1646.
- **Llave compartida** – Se utiliza para autenticar el AP con el servidor RADIUS.



Nota: La autenticación y autorización del usuario se maneja mediante el estándar 802.1X, que proporciona una autenticación centralizada basada en el servidor de los usuarios finales.

WLAN seguras

WPA 3

Debido a que WPA2 ya no se considera seguro, se recomienda WPA3 cuando esté disponible. WPA3 incluye cuatro características:

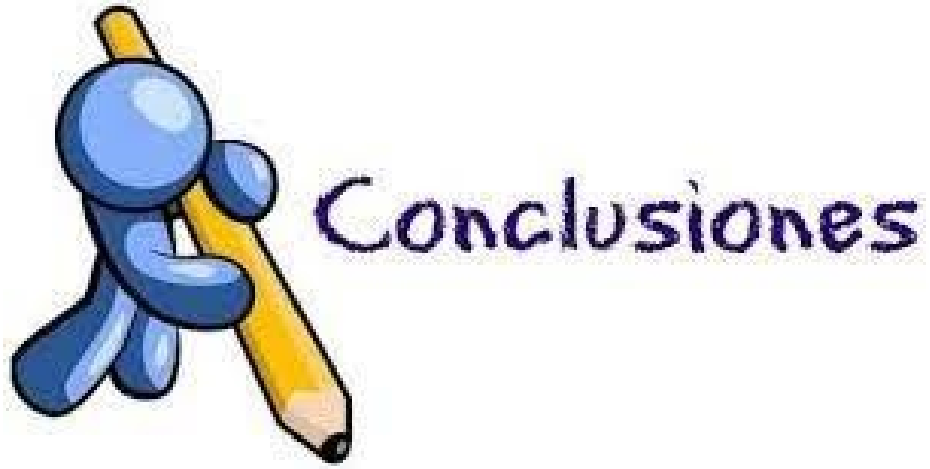
- **WPA3 - Personal:** Frustra los ataques de fuerza bruta mediante el uso de la autenticación simultánea de iguales (Simultaneous Authentication of Equals, SAE).
- **WPA3 - Empresa:** Utiliza la autenticación 802.1X / EAP. Sin embargo, requiere el uso de una suite criptográfica de 192 bits y elimina la combinación de protocolos de seguridad para los estándares 802.11 anteriores.
- **Redes Abiertas:**No usa ninguna autenticación. Sin embargo, utiliza el cifrado inalámbrico oportunista (OWE) para cifrar todo el tráfico inalámbrico.
- **Incorporación de IoT :** Utiliza el Protocolo de aprovisionamiento de dispositivos (DPP) para incorporar rápidamente dispositivos IoT.

Actividad

Resolver la siguiente actividad

Actividades

- ¿Qué es el CAPWAP?
- ¿Qué es el DTLS?
- ¿Qué es DSSS, FHSS y OFDM?
- ¿Cuáles son las cuatro técnicas de autenticación de clave compartida?
- ¿Cuáles son las amenazas en las WLAN?
- ¿Qué es el FlexConnect?
- ¿Qué es el filtrado MAC?

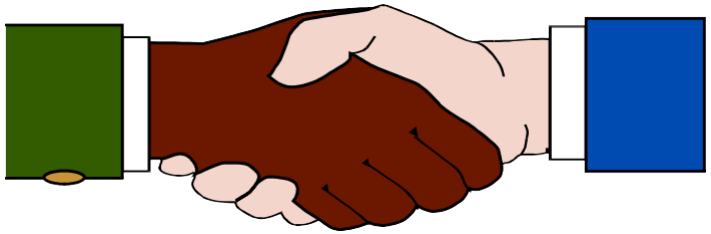


¿Qué aprendí en esta sesión?

¿Qué aprendí en está sesión?

- CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLAN.
- DTLS es un protocolo que proporciona seguridad entre el AP y el WLC.
- Los dispositivos de LAN inalámbricos tienen transmisores y receptores sintonizados a frecuencias específicas de ondas de radio para comunicarse. Los rangos se dividen en rangos más pequeños llamados canales: DSSS, FHSS y OFDM.
- Los estándares 802.11b/g/n operan en el espectro de 2.4 GHz a 2.5GHz. La banda de 2,GHz se subdivide en varios canales. Cada canal tiene un ancho de banda de 22 MHz y está separado del siguiente canal por 5 MHz.
- Las redes inalámbricas son susceptibles a amenazas, que incluyen: interceptación de datos, intrusos inalámbricos, ataques DoS y puntos de acceso no autorizados.
- Para mantener alejados a los intrusos inalámbricos y proteger los datos, dos características de seguridad tempranas todavía están disponibles en la mayoría de los enrutadores y puntos de acceso: ocultamiento de SSID y filtrado de direcciones MAC.
- Hay cuatro técnicas de autenticación de clave compartida disponibles: WEP, WPA, WPA2 y WPA3.

Gracias



Universidad
Tecnológica
del Perú