LAN inalámbricas

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Objetivos

- Describir la tecnología y los estándares de la LAN inalámbrica.
- Describir los componentes de una infraestructura LAN inalámbrica.
- Describir las topologías y la estructura de la trama 802.11
- Describir la administración de canales en una WLAN.
- Describir las amenazas a las redes LAN inalámbricas.
- Describir los mecanismos de seguridad de las LAN inalámbricas.
- Configurar los clientes inalámbricos para conectarse a un router inalámbrico.
- Solucionar problemas de configuración inalámbrica comunes.

Apoyando la Movilidad

- La Productividad ya no se limita a un lugar de trabajo fijo o un periodo de tiempo definido.
- Ahora la gente espera estar conectado en cualquier momento y lugar, desde la oficina hasta el aeropuerto o el hogar.
- Los usuarios esperan poder navegar de forma inalámbrica.
- El Roaming permite a un dispositivo inalámbrico mantener el acceso a Internet sin perder la conexión.

Beneficios de Wireless

- Mayor flexibilidad
- Aumento de la productividad
- Reducción de costes
- Capacidad para crecer y adaptarse a las necesidades cambiantes

Tecnologías inalámbricas

Pueden clasificarse en:

- **Red de área personal inalámbrica (WPAN)**: **pocos pies (Bluetooth).**

- **LAN inalámbrica (WLAN)**: **Cientos de pies**.

- **Red de área amplia inalámbrica (WWAN)** rango de **millas**.

- **Bluetooth**: IEEE 802.15, utiliza un proceso de emparejamiento de dispositivos para comunicarse a distancias de hasta 0,05 millas **(100 metros).**

Tecnologías inalámbricas

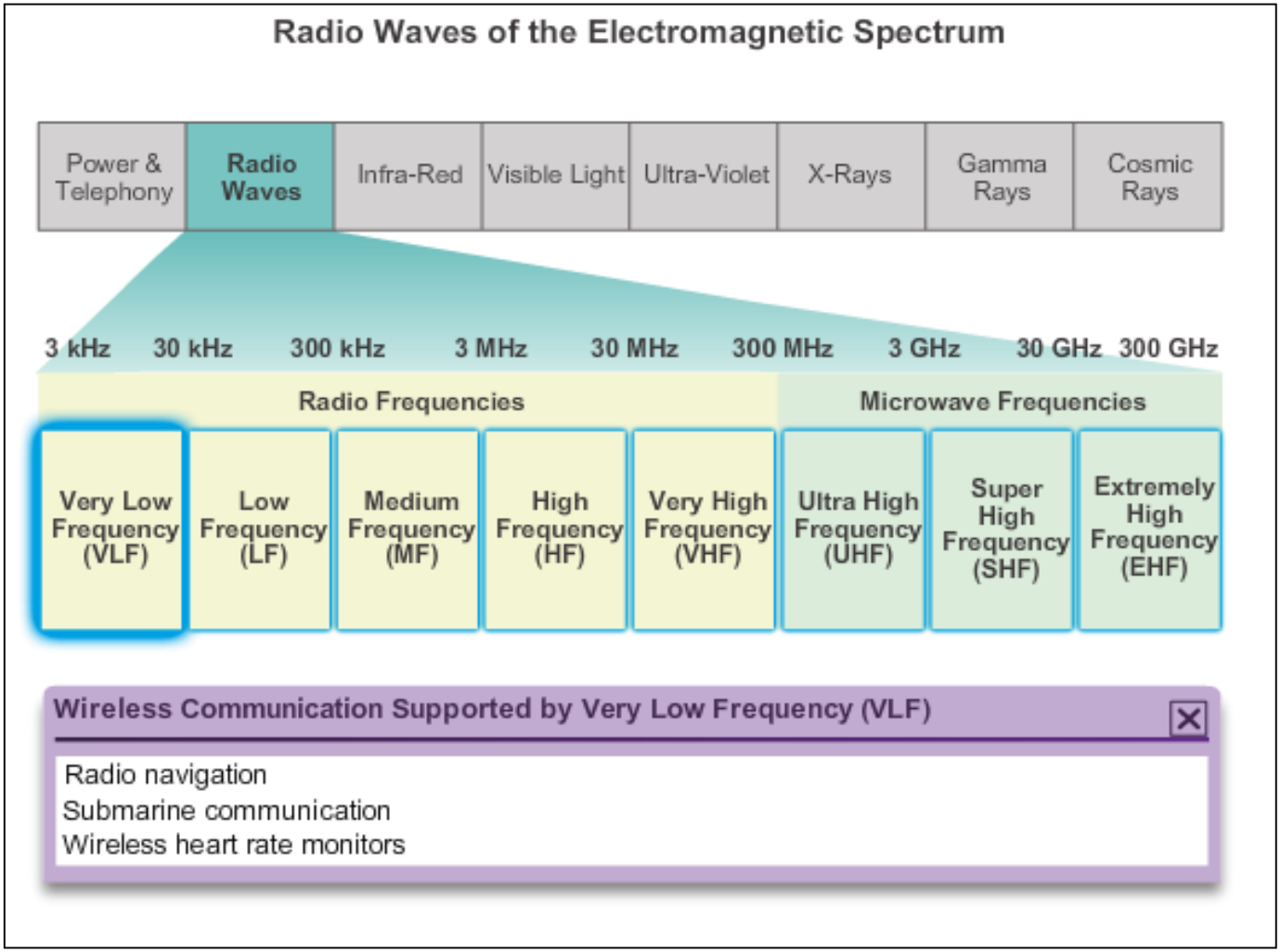
- **Wi-Fi (fidelidad inalámbrica)** IEEE 802.11, ofrece acceso a la red a los usuarios domésticos y corporativos, hasta **0,18 millas (300 metros).**

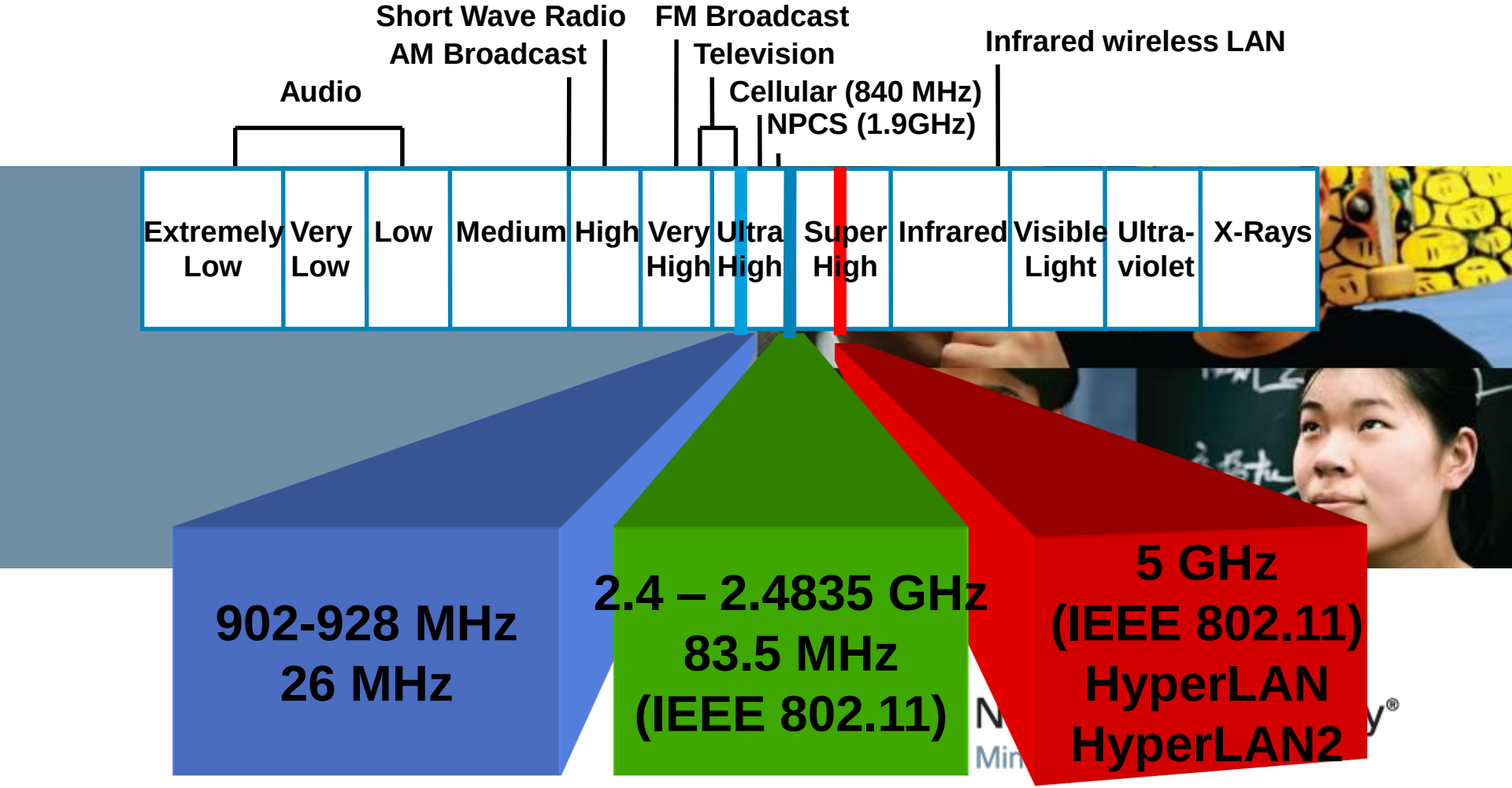
- **Interoperabilidad mundial para acceso por microondas (WiMAX)** IEEE 802.16, hasta **30 millas (50 km)**.

- **Banda ancha móvil** utilizan el ISP de **acceso celular para proporcionar conectividad de red móvil de banda ancha.**

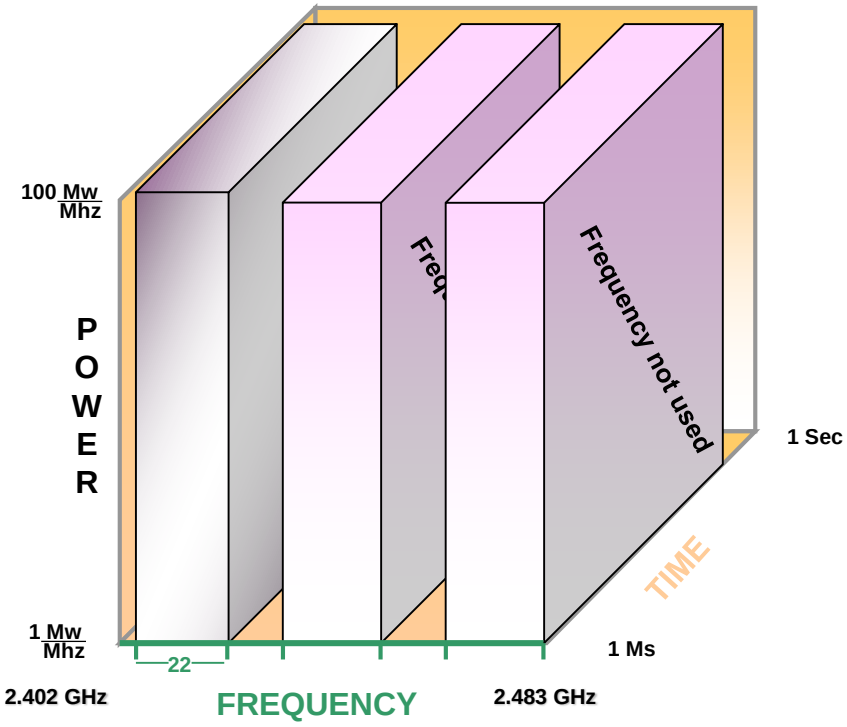
- **Banda ancha por satélite** acceso a la red a sitios remotos mediante el uso de una antena parabólica direccional.

Las frecuencias de radio

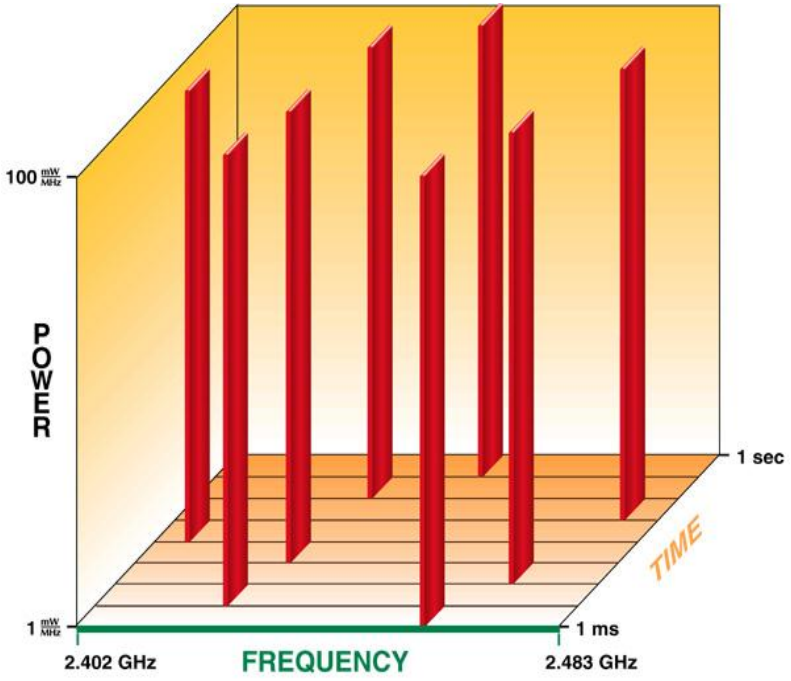



Short Wave Radio
AM Broadcast
FM Broadcast
Television
Infrared wireless LAN
Audio
Cellular (840 MHz)
NPCS (1.9GHz)
Extremely Low
Very Low
Low
Medium
High
Very High
Ultra High
Super High
Infrared
Visible Light
Ultra-violet
X-Rays
902-928 MHz
26 MHz
2.4 – 2.4835 GHz
83.5 MHz
(IEEE 802.11)
5 GHz
(IEEE 802.11)
HyperLAN
HyperLAN2

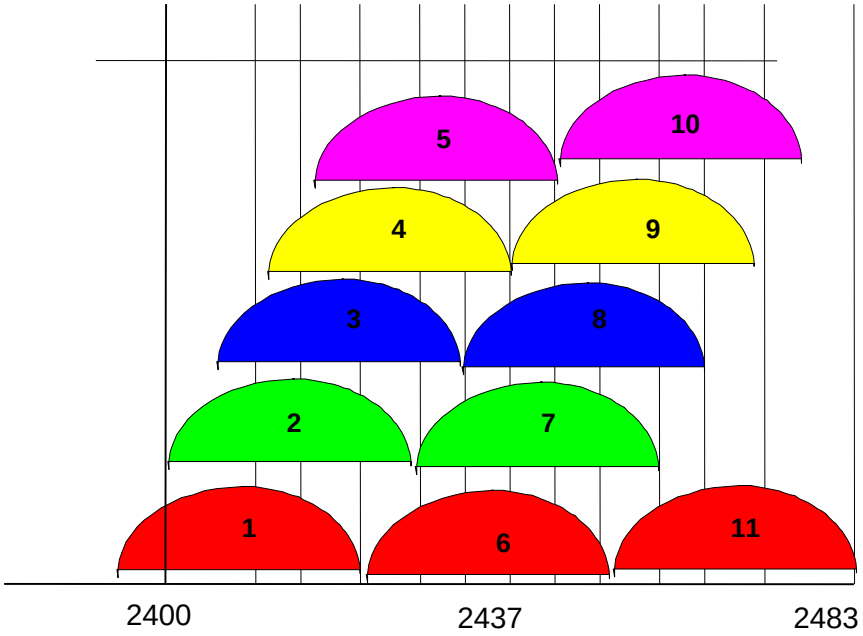
Direct Sequence



Frequency Hopping



Direct Sequence



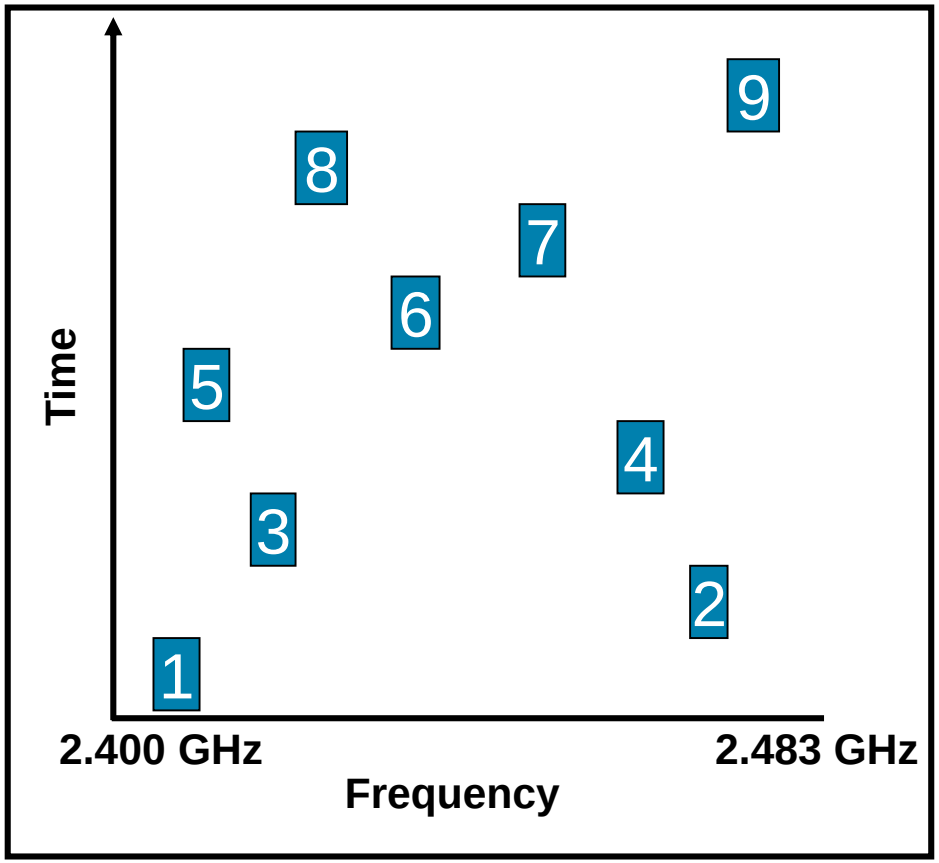
EEUU Y CANADA: CHANNEL 1, 6 Y 11

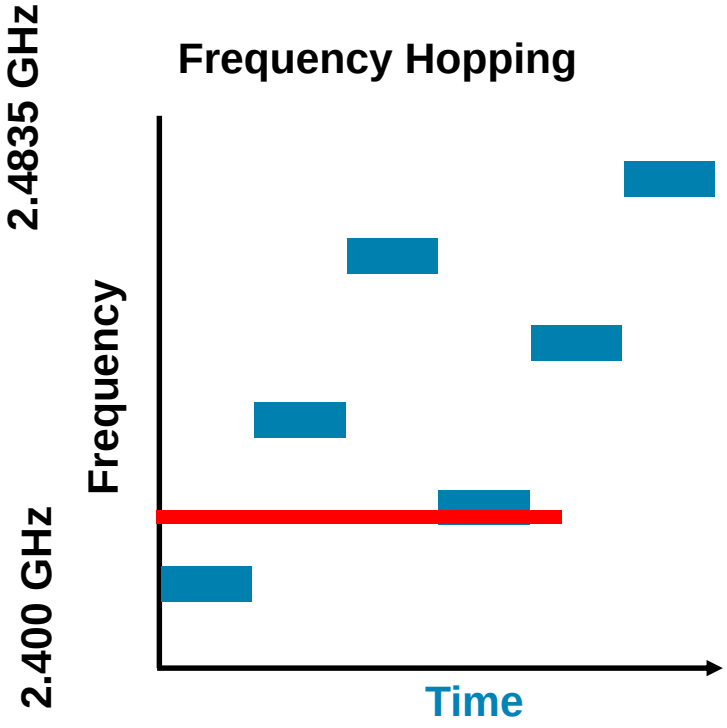
EUROPA: 1, 7, Y 13.

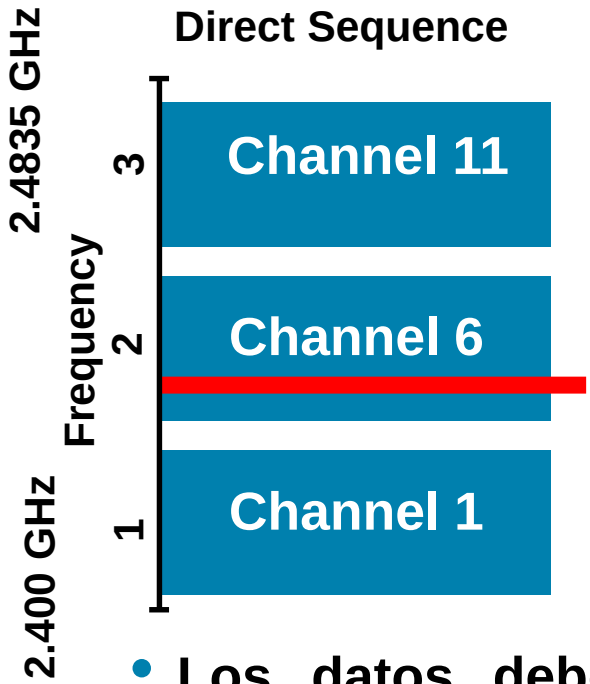
JAPON: SÓLO EL 14.

Frequency Hopping

- Un total de 79 canales disponibles.
- Cambios de frecuencia (hops) al menos cada 0.4 segundos.
- Se requieren sincronización de saltos.







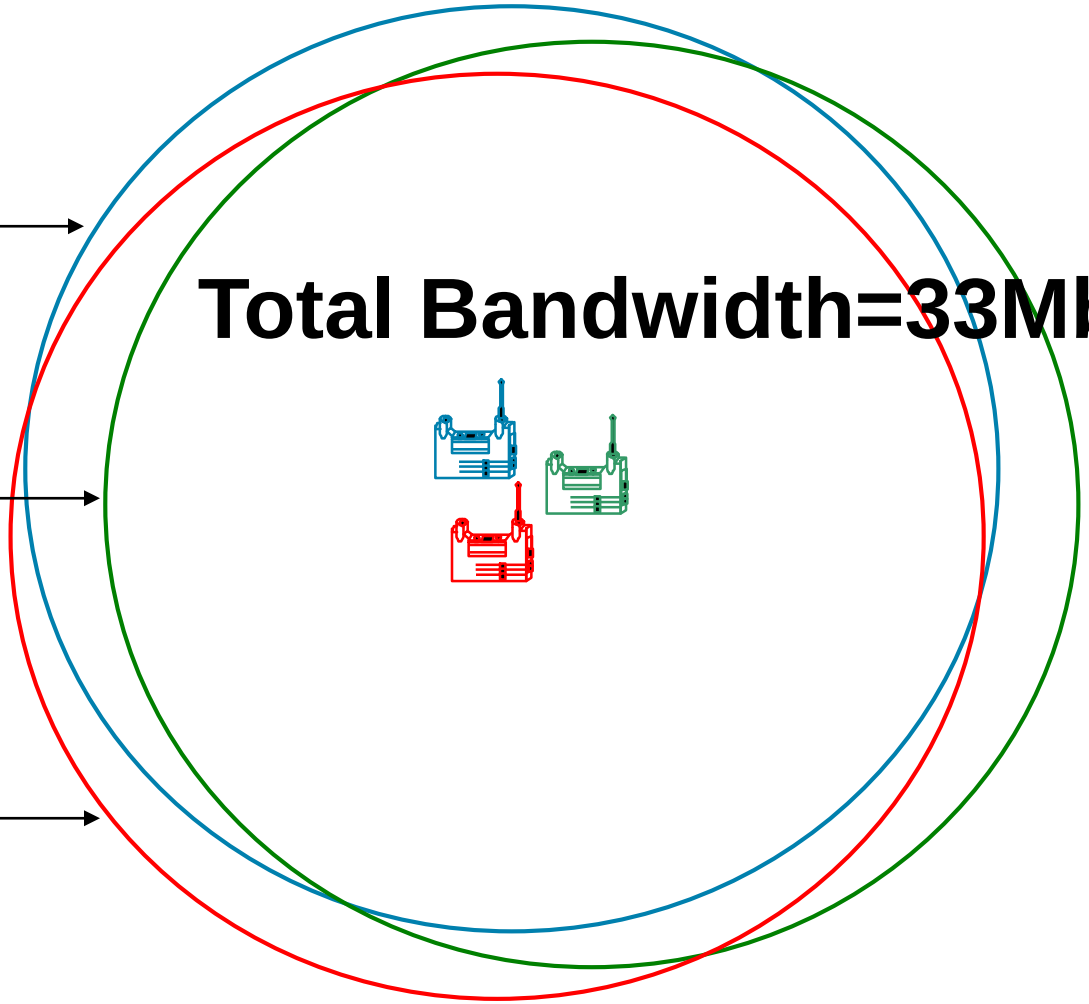
- FH rodea la interferencia
- Los paquetes perdidos se retransmiten en el siguiente salto.
- Los datos deben ser decodificados de bits redundantes.
- Pueden moverse a otro canal para evitar la interferencia.

ESCALABILIDAD CON DS

Blue = 11Mb

Green = 11Mb

Red = 11Mb



Estandares 802.11

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

Certificación Wi-Fi

La Wi-Fi Alliance certifica Wi-Fi y compatibilidad del producto:

- IEEE 802.11a/b/g/n/ac/ad-compatible.
-
- IEEE 802.11i segura utilizando WPA2 ™ y el protocolo de autenticación extensible (EAP)

- Wi-Fi Protected Setup (WPS) simplificar conexiones del dispositivo.

- Wi-Fi Direct compartir archivos multimedia entre dispositivos
- Wi-Fi PassPoint simplificar la conexión segura a redes con AP Wi-Fi

- Wi-Fi Miracast mostrar la perfección de vídeo entre dispositivos.

Comparativo de WLAN y LAN

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

NICs inalámbricas

La Implementación inalámbrica requiere:

Los dispositivos finales con NICs inalámbricas

Dispositivo de infraestructura, como un enrutador inalámbrico o punto de acceso inalámbrico

Router inalambricos de hogar

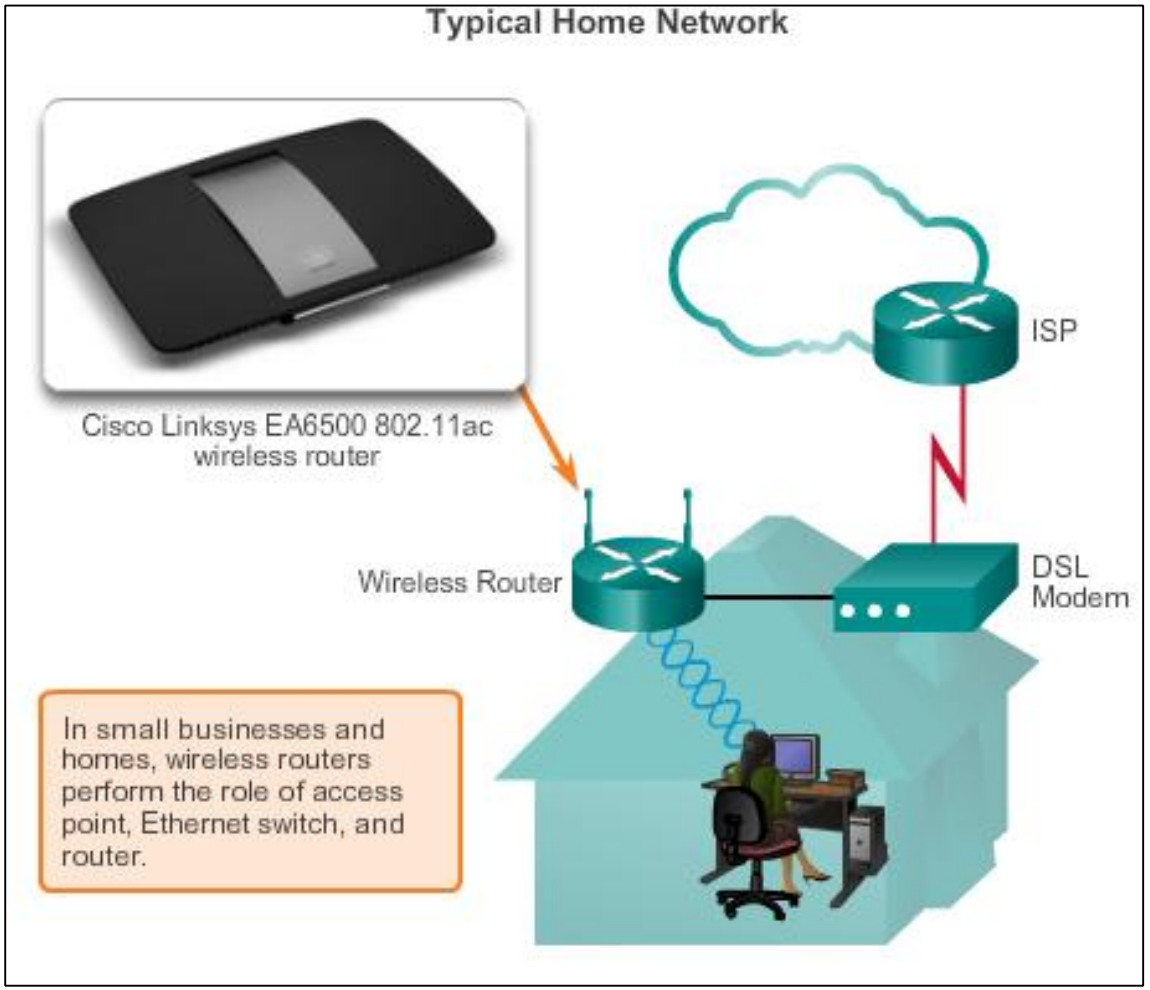
Un usuario doméstico se interconecta a dispositivos inalámbricos que utilicen un pequeño router inalámbrico integrado.

Estos sirven como:

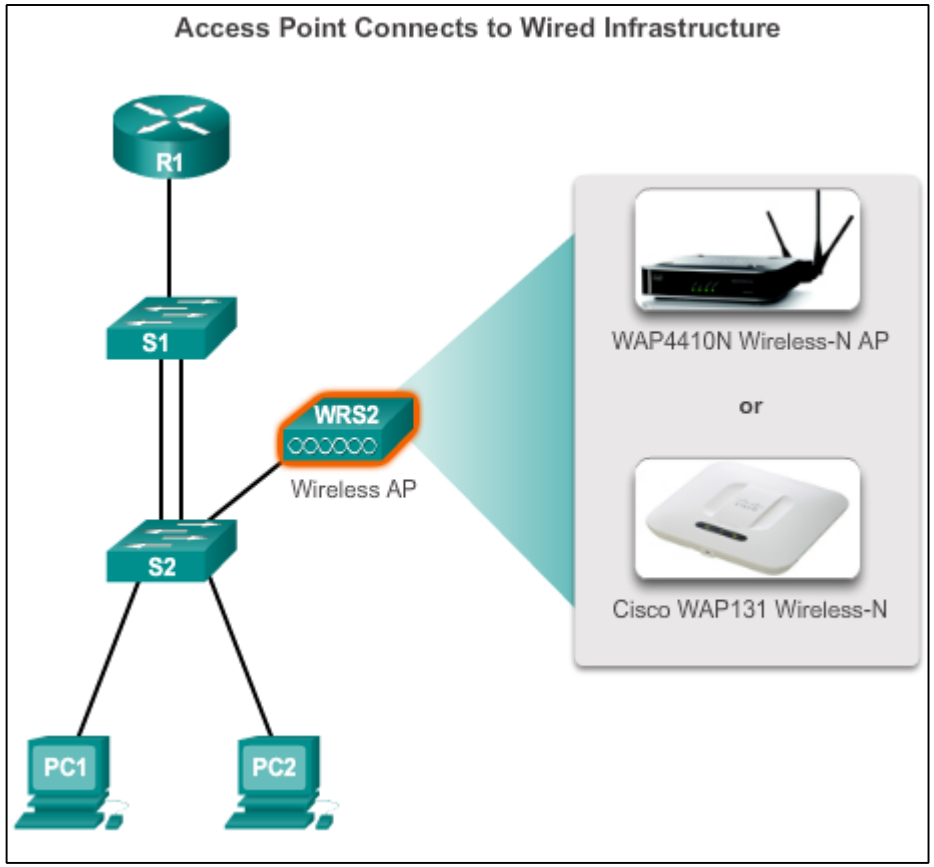
Punto de acceso

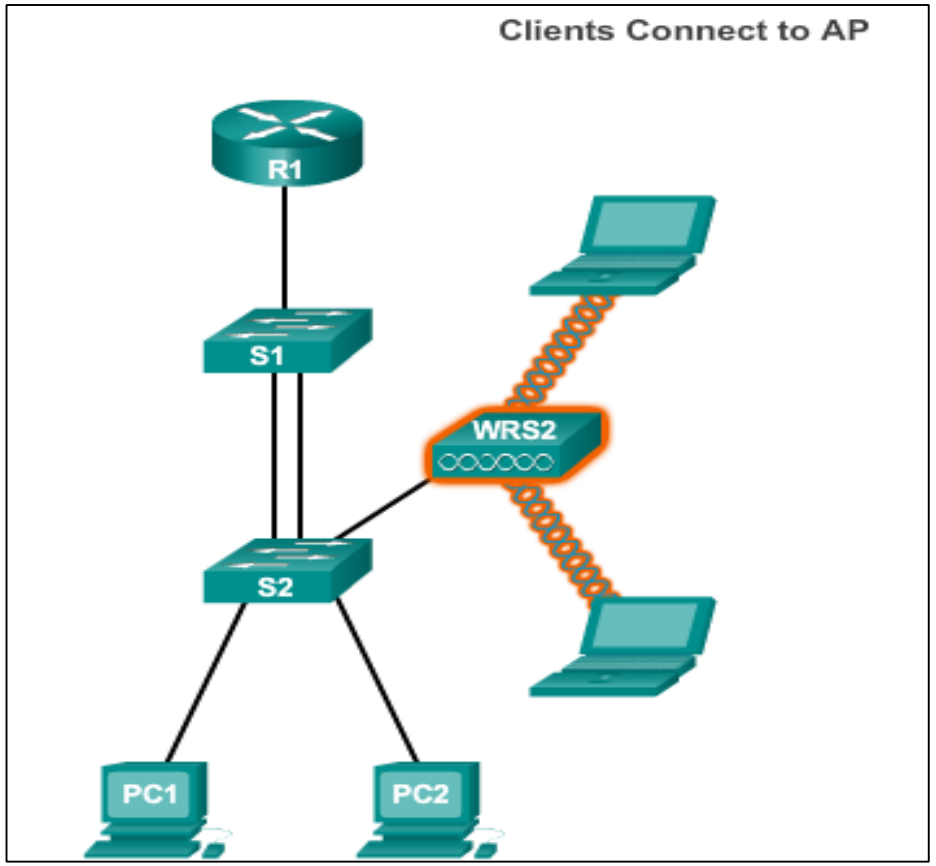
Conmutador Ethernet

enrutador

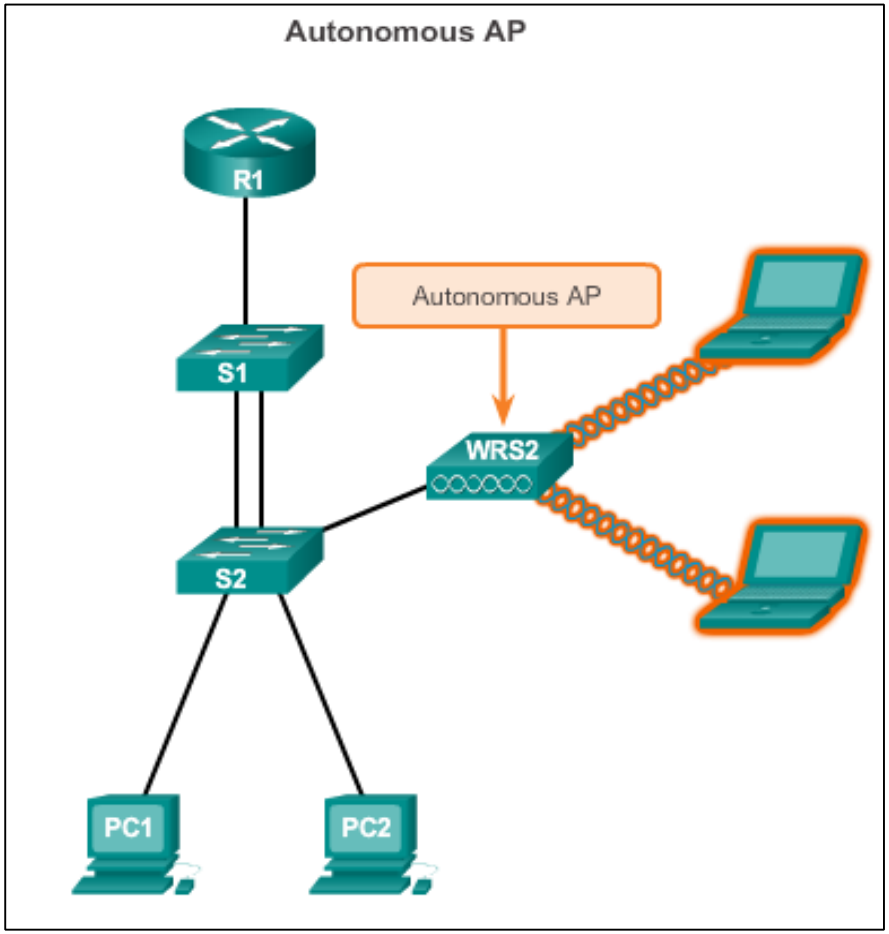


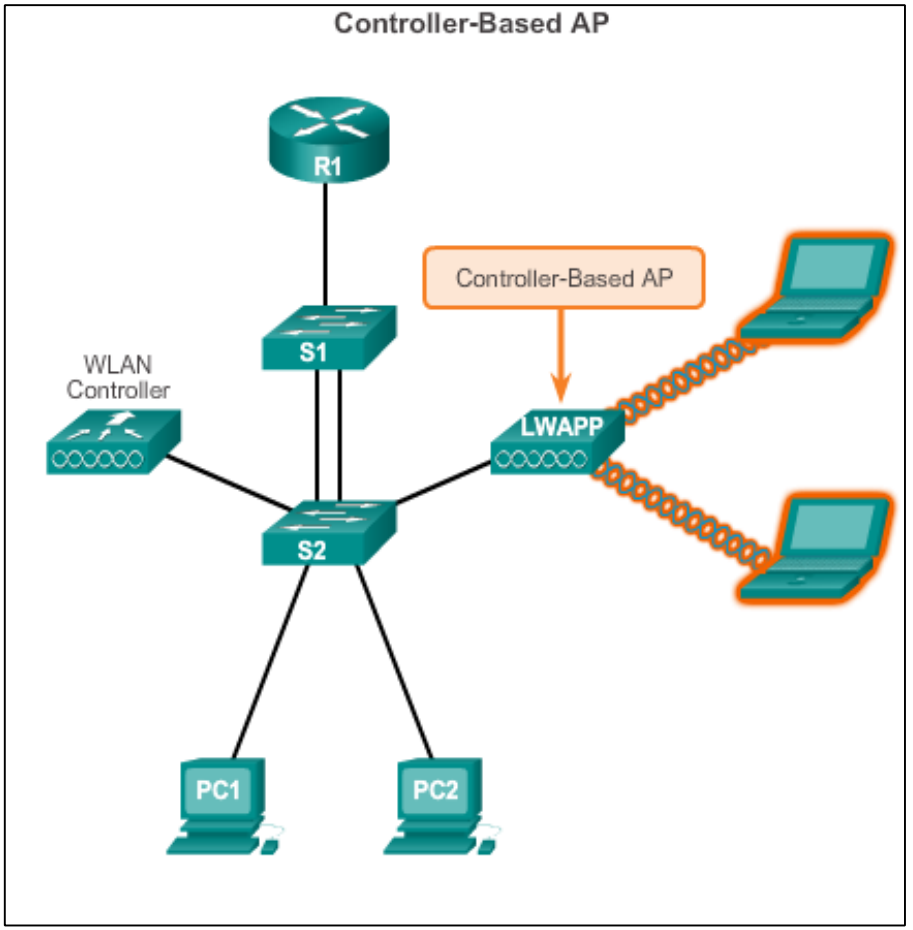
Soluciones empresariales Inalámbricos





Puntos de acceso inalámbrico





Soluciones Pequeñas para implementación inalámbrica

Cisco Small Business Autonomous APs

Cisco WAP4410N

- Intro-level small business AP
- Configured using a GUI
- Powered using AC or PoE

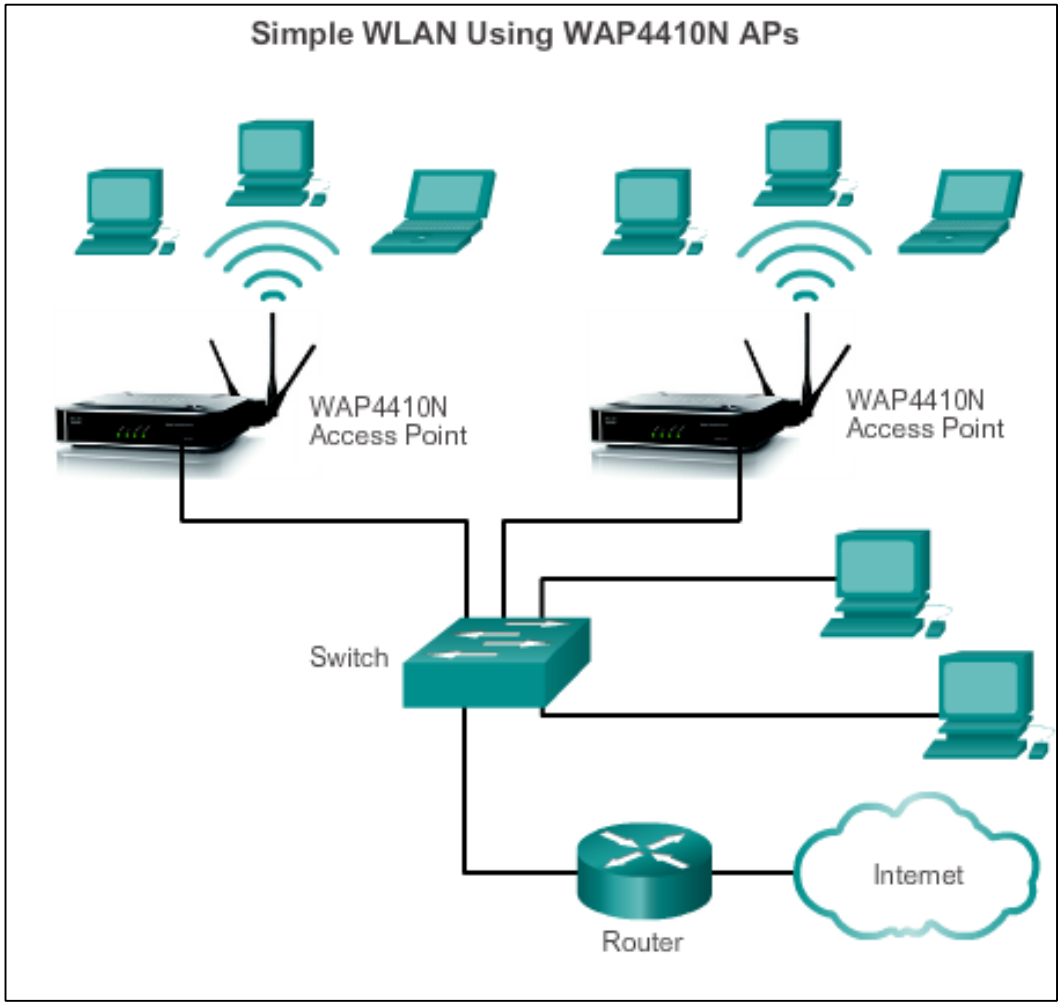
Cisco WAP121 and WAP321

- Mid-level small business APs
- Configured and managed using a GUI or CLI
- Supports clustering with Single PointSetup
- Powered using AC or PoE

Cisco AP541N

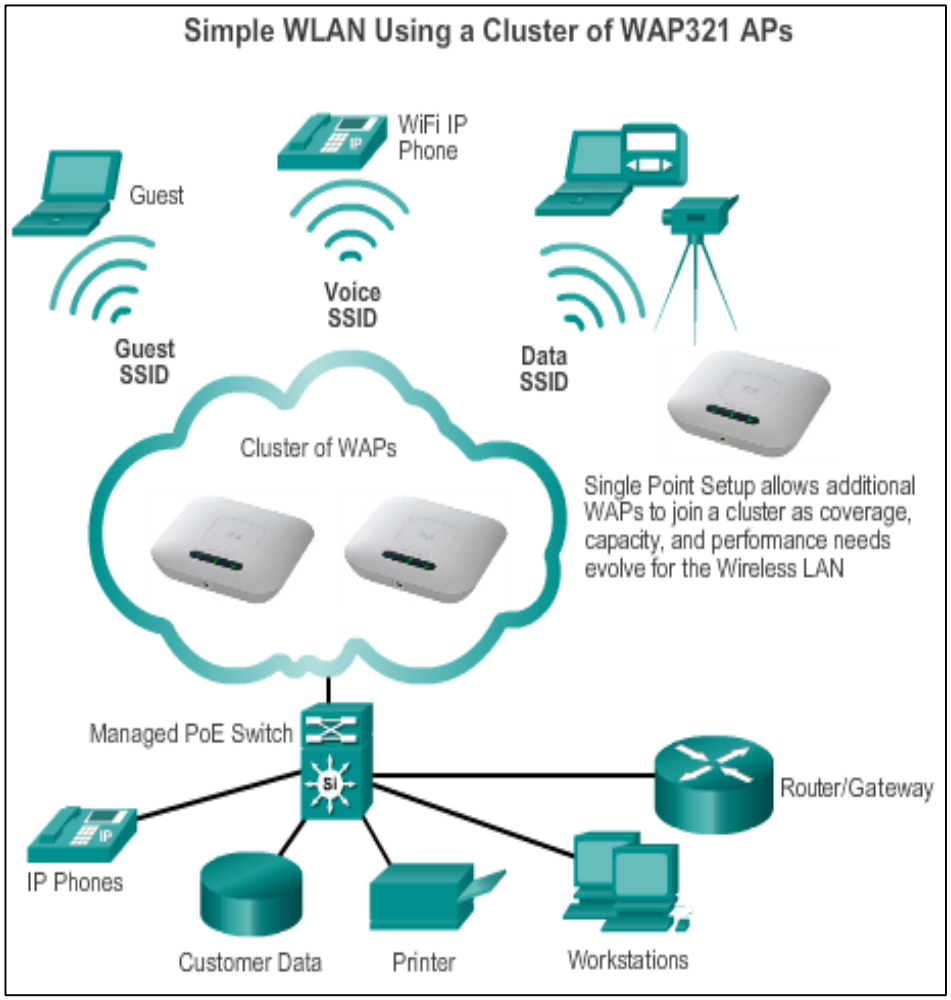
- Mid-level small business APs
- Configured using a GUI
- Supports controller-less clustering technology
- Powered using AC or PoE

Soluciones Pequeñas para implementación inalámbrica



- Cada AP es configurado y gestionado de forma individual.
- Esto puede convertirse en un problema cuando se necesitan varios puntos de acceso.

Soluciones empresariales para implementación inalámbrica



- Apoyar la agrupación de los AP sin el uso de un controlador.
- Múltiples AP se pueden implementar en una sola configuración de todos los dispositivos dentro del grupo(cluster)
- La gestión de la red inalámbrica como un solo sistema, sin tener que preocuparse por la interferencia entre los AP y sin tener que configurar cada AP como un dispositivo independiente.

Grandes Soluciones de implementación inalámbrica

- Para grandes organizaciones con muchos AP, proporciona soluciones gestionadas basadas en controladores, incluyendo la arquitectura de Managed Meraki Cloud y la arquitectura de red inalámbrica unificada.

- **Cisco Meraki** arquitectura de nube es una solución de gestión que se utiliza para simplificar el despliegue inalámbrico. Utilizando esta arquitectura, los AP se gestionan de forma centralizada desde un controlador en la nube.

Meraki Cloud Controller (MCC)

Grandes Soluciones de implementación inalámbrica

Controller-Based Wireless APs

Cisco Aironet 1600, 2600, and 3600 Series
Robust controller-based APs

Cisco Aironet 600 Series OfficeExtend
Used to extend 802.11n wireless coverage to the home teleworking environment

Cisco 1552 Series Outdoor Rugged APs
Robust outdoor controller-based AP

Grandes Soluciones de implementación inalámbrica

Controllers for Small and Medium-Sized Businesses

Cisco Virtual Controller

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Antenas inalámbricas

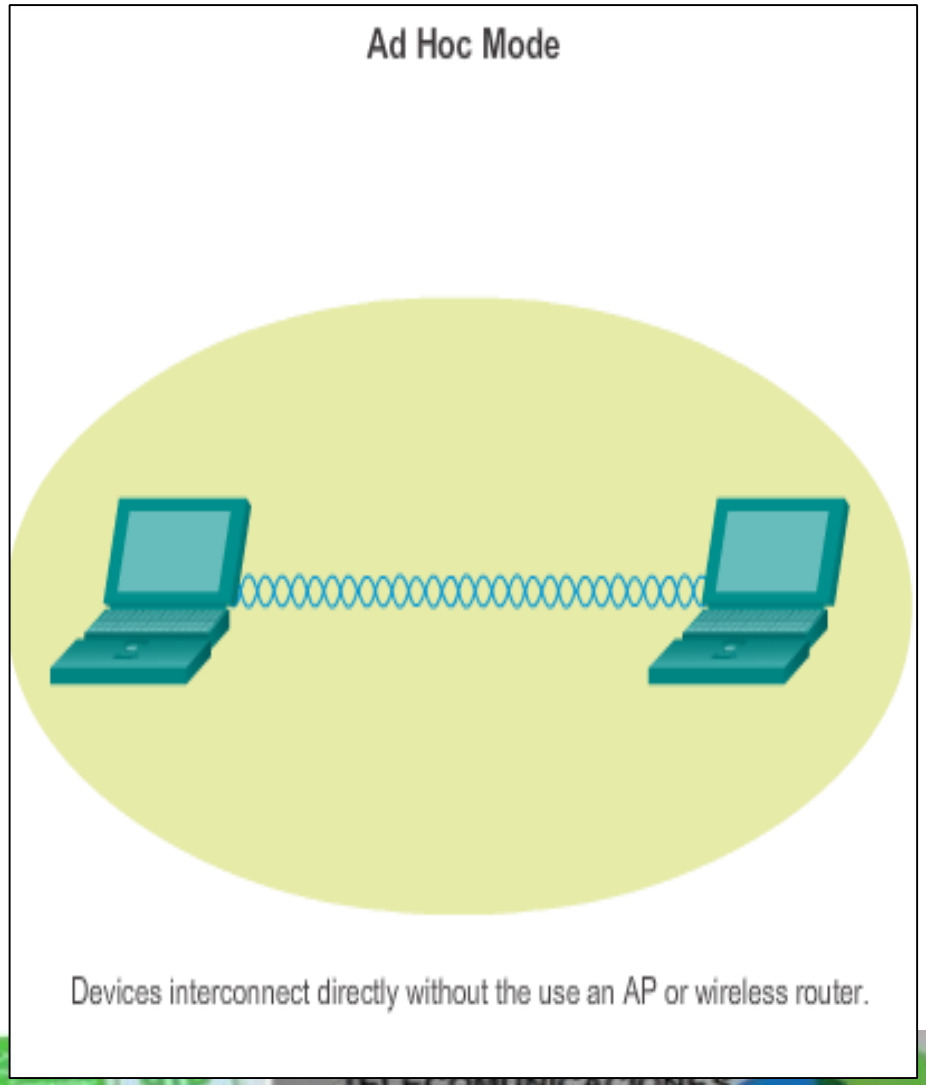
Cisco Aironet AP puede usar:

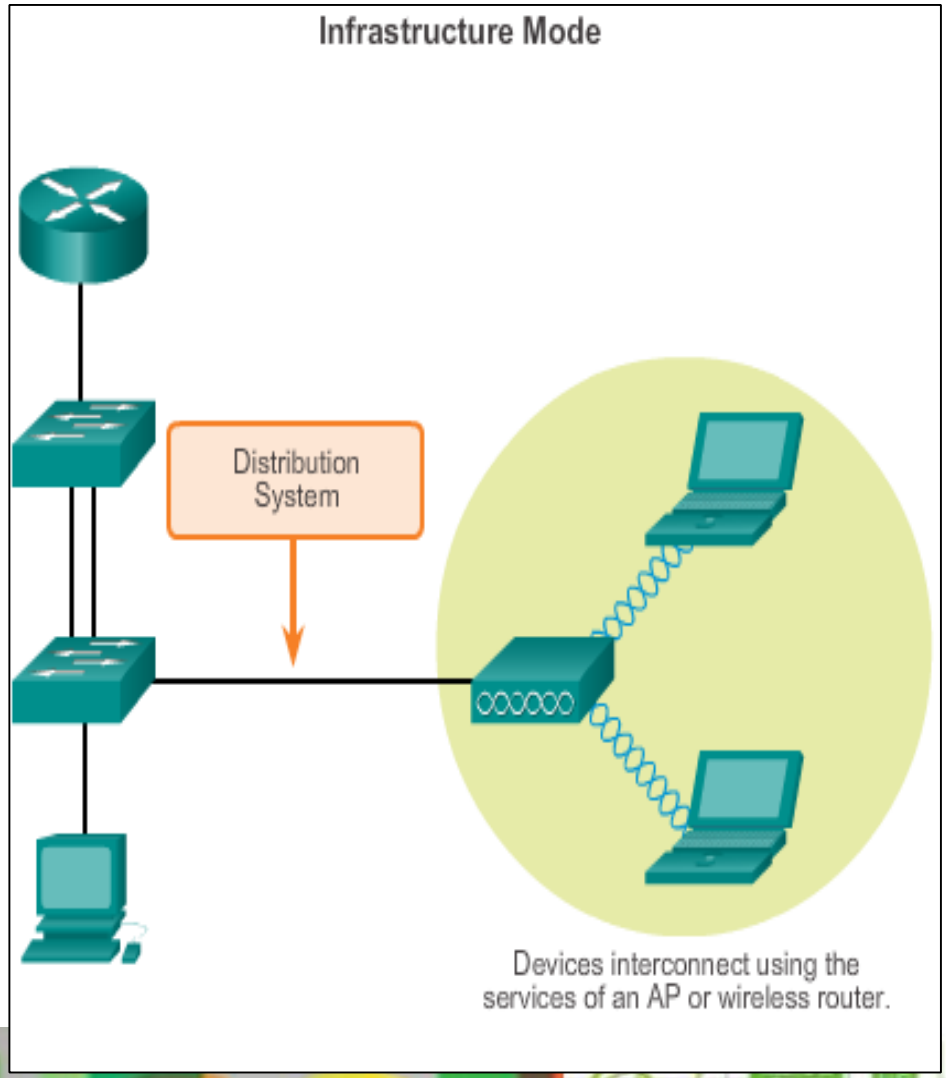
Antenas Omnidireccional Wi-Fi son a menudo antenas dipolo básicas, conocidas como "pato de goma". Ofrecen cobertura de 360 grados.

Antenas Direccionales Wi-Fi concentran la señal de radio en una dirección dada, mejora la señal hacia y desde el AP en la dirección que la antena está apuntando.

Antenas Yagi de radio direccional que se puede utilizar para la creación de redes de larga distancia Wi-Fi.

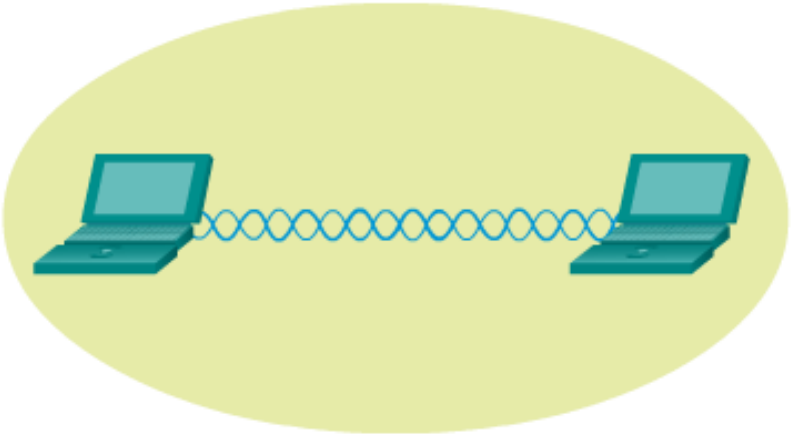
Modos de topología 802.11





Modo Ad Hoc

Tethering (hotspot personal) Variación de la topología Ad Hoc cuando un teléfono inteligente o una tableta con acceso a datos de telefonía móvil está habilitado para crear un punto de acceso personal.



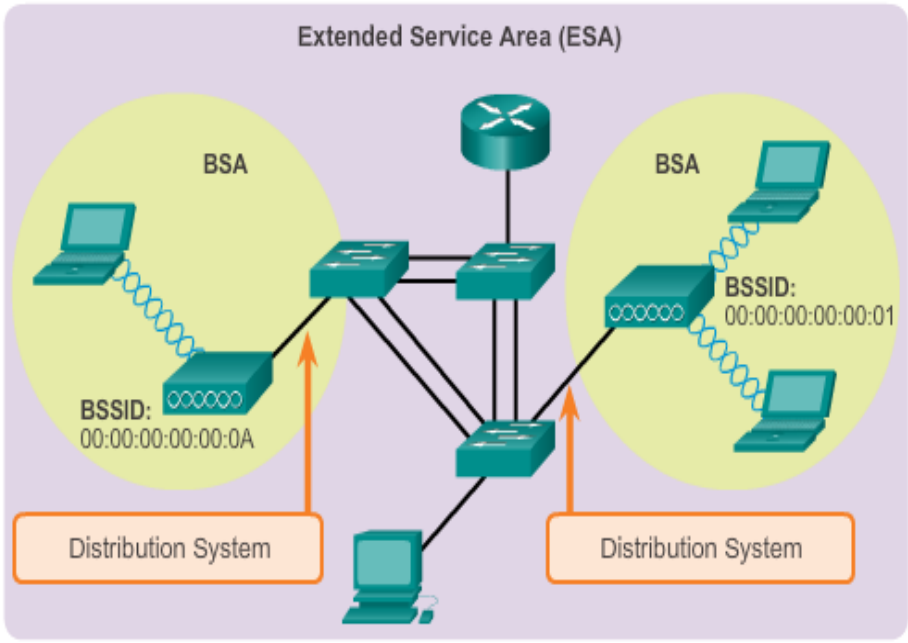
IBSS Summary	
WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)

Modo infraestructura

Basic Service Set Summary

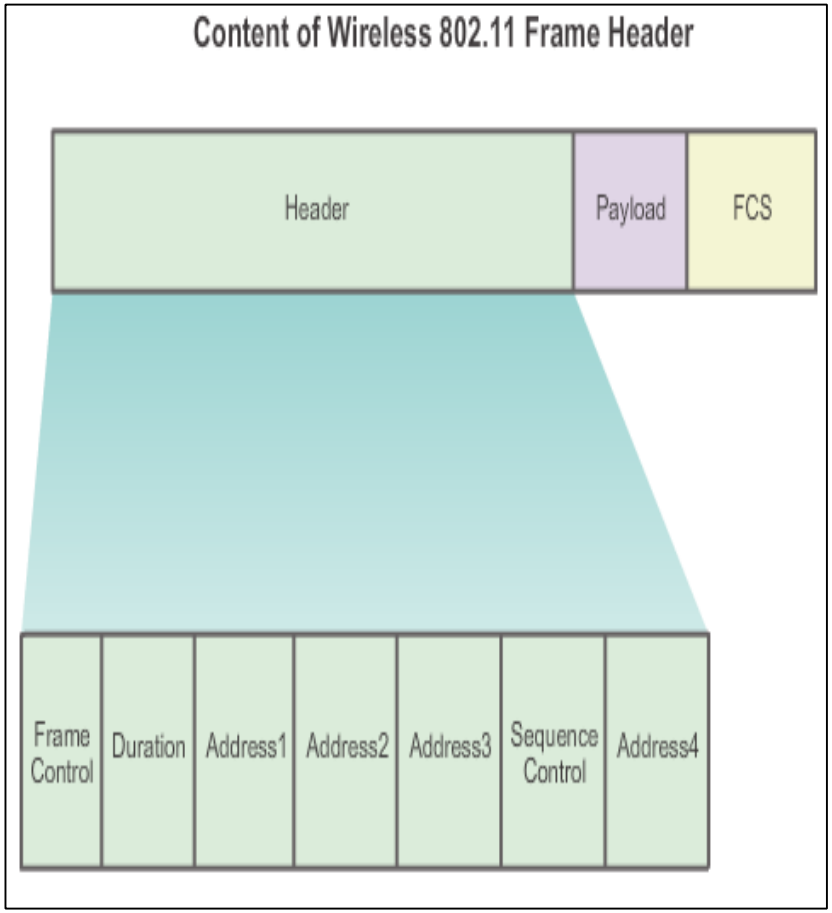
BSS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Basic Service Set (BSS)
Number of APs	1
802.11 Coverage Area	Basic Service Area (BSA)

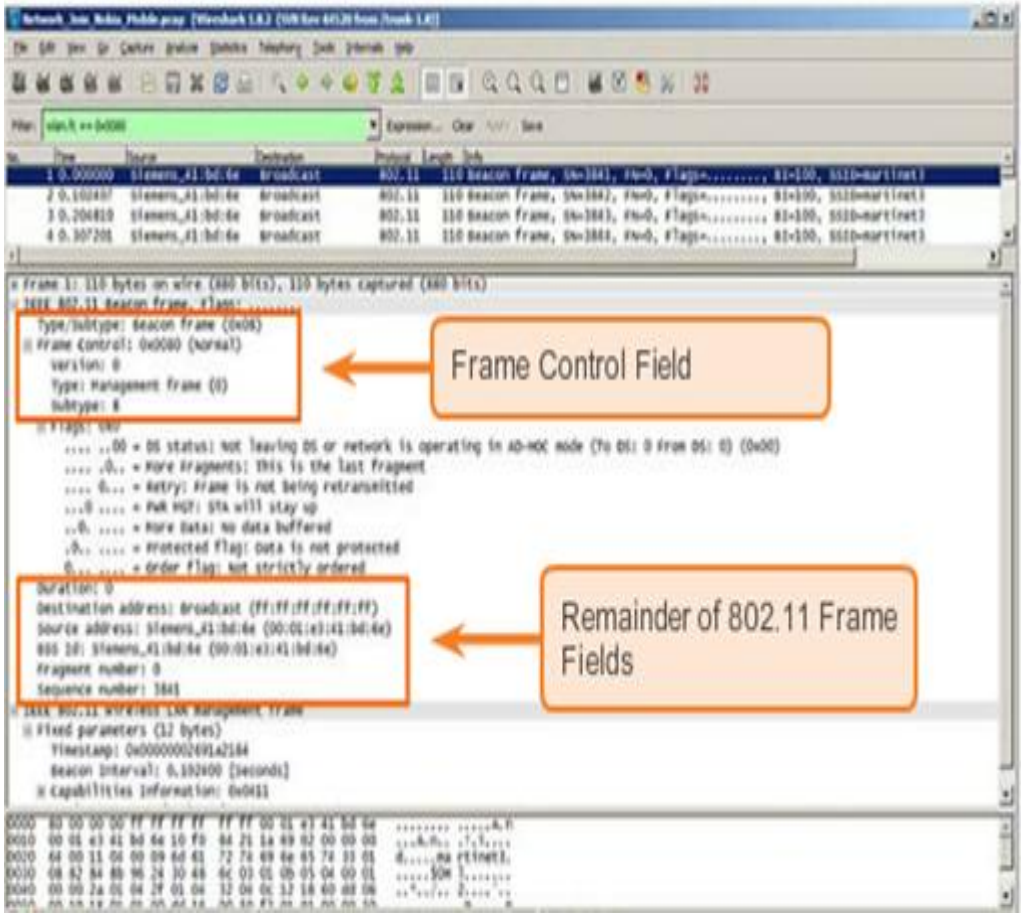
Extended Service Set Summary



ESS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Extended Service Set (ESS)
Number of APs	2 or more
802.11 Coverage Area	Extended Service Area (ESA)

Trama inalambrica 802.11

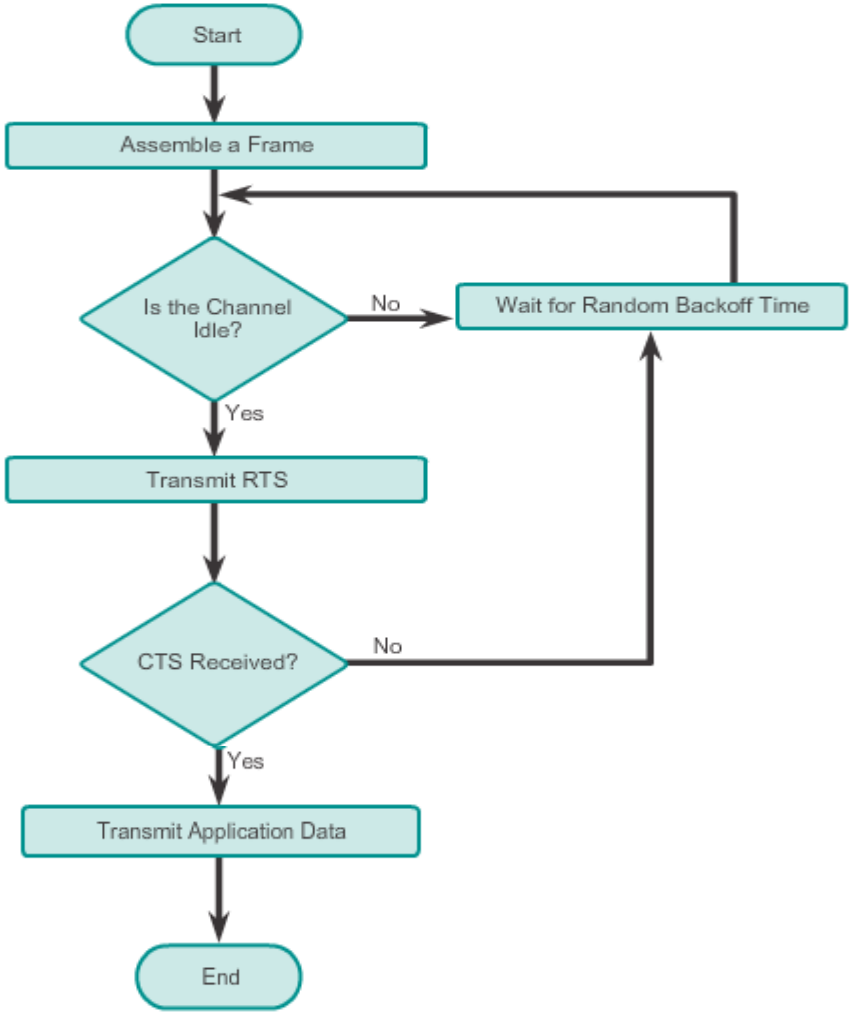




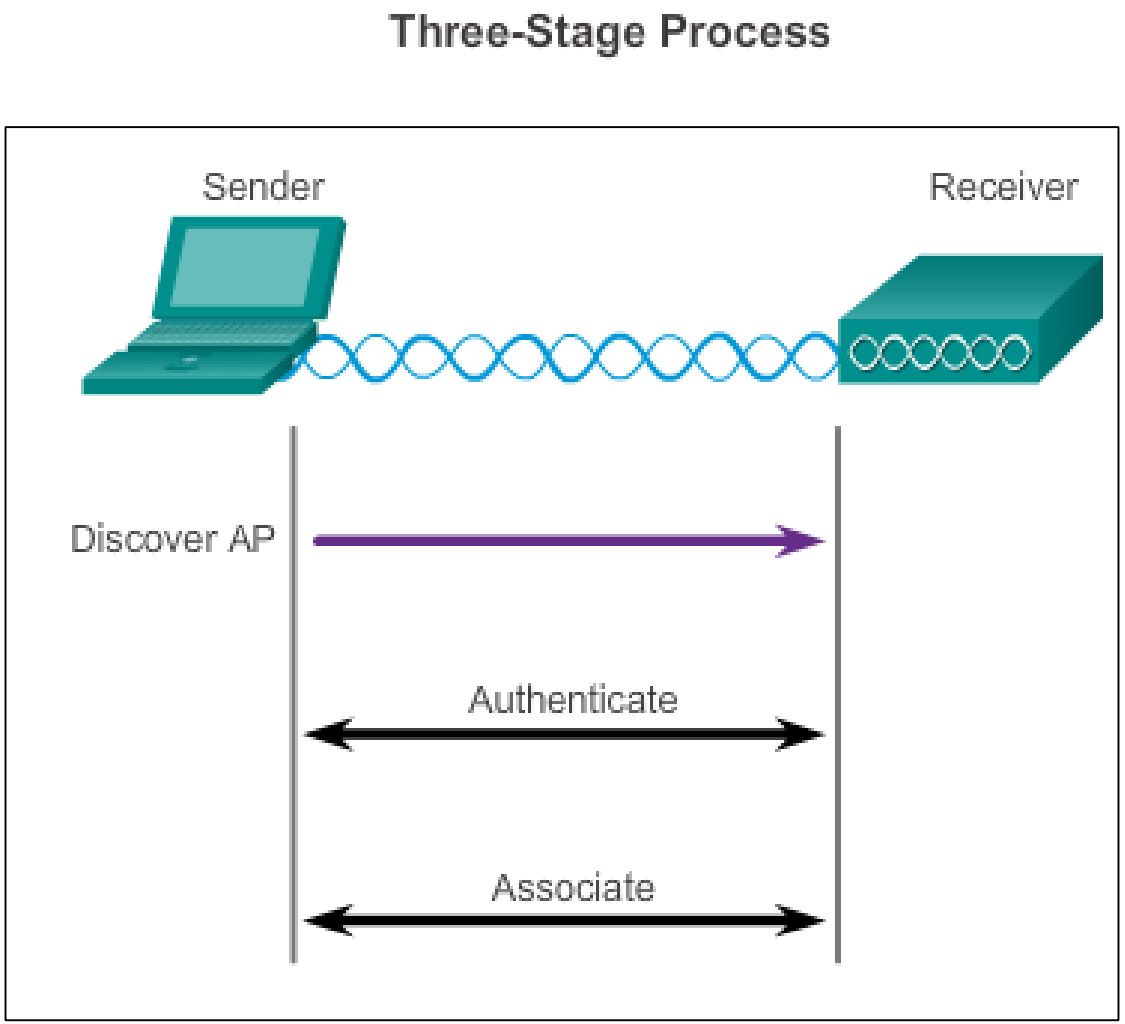
Operación de CSMA/CA

CSMA / CA

Diagrama de flujo



Los clientes inalámbricos y la Asociación al AP



Parámetros de la Asociación

- **SSID** Identificador único que los clientes inalámbricos distinguir entre varias redes inalámbricas en la misma radio.
- **Contraseña** Requerido por el cliente inalámbrico para autenticarse con el AP.
- **Modo de red** son los estándares WLAN 802.11a/b/g/n/ac/ad. AP y routers inalámbricos pueden operar en modo mixto.
- **Modo de seguridad** parámetros WEP, WPA o WPA2.
- **Ajustes de canal** bandas de frecuencia utilizadas para transmitir datos inalámbricos. Se puede elegir el ajuste de canal o configurar manualmente.

El descubrimiento de los AP

Modo pasivo: el AP anuncia su servicio enviando trama en broadcast contienen el SSID, los estándares y parámetros de seguridad.

El propósito de los **beacons** es permitir a los clientes aprendan la disponibidad de la red y los AP en un área determinada.

Modo activo: Los clientes deben conocer el SSID.

El Cliente inicia el proceso mediante la difusión de trama de petición de **sondas** en múltiples canales. incluyen el SSID y los estándares soportados.

Puede ser requerido si un AP o router inalámbrico está configurado para no difundir tramas beacons.

PROCESO DE ASOCIACION

Pasos de la asociación:

El cliente envia una sonda.

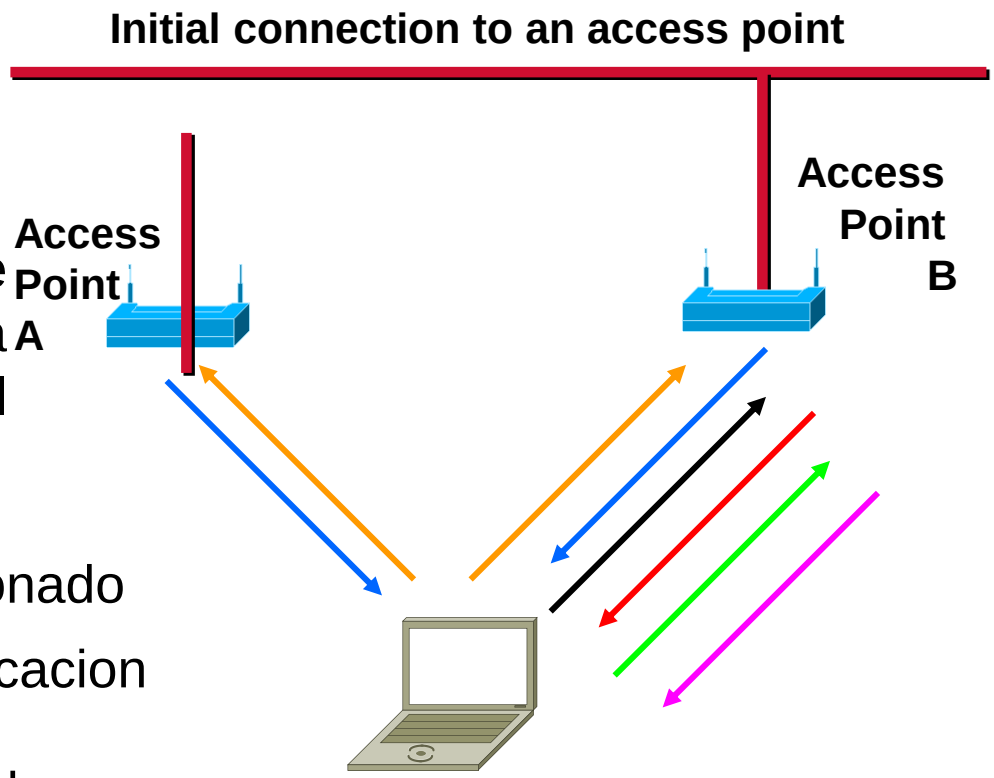
AP envia un beacons de respuesta. El Cliente la evalua, selecionando el mejor AP

EL cliente envia solicitud de Autenticación al AP seleccionado

AP B le confirma la autenticacion .

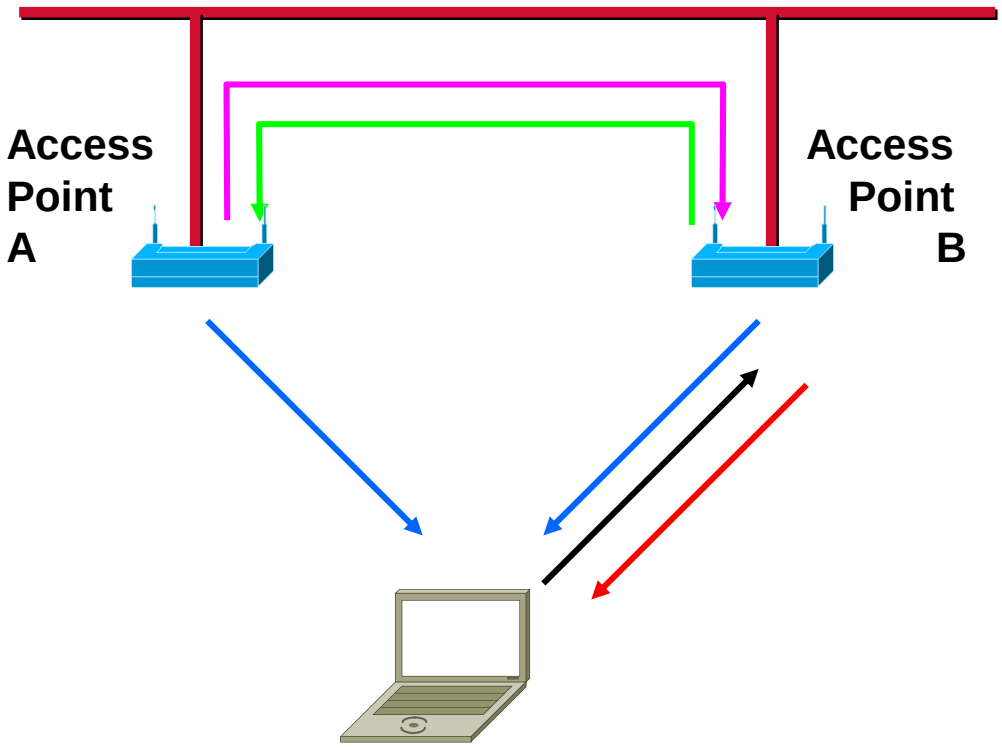
El Cliente envia la solicitud de Asociación al AP B

AP B le confirma la asociación Y le registra como cliente.



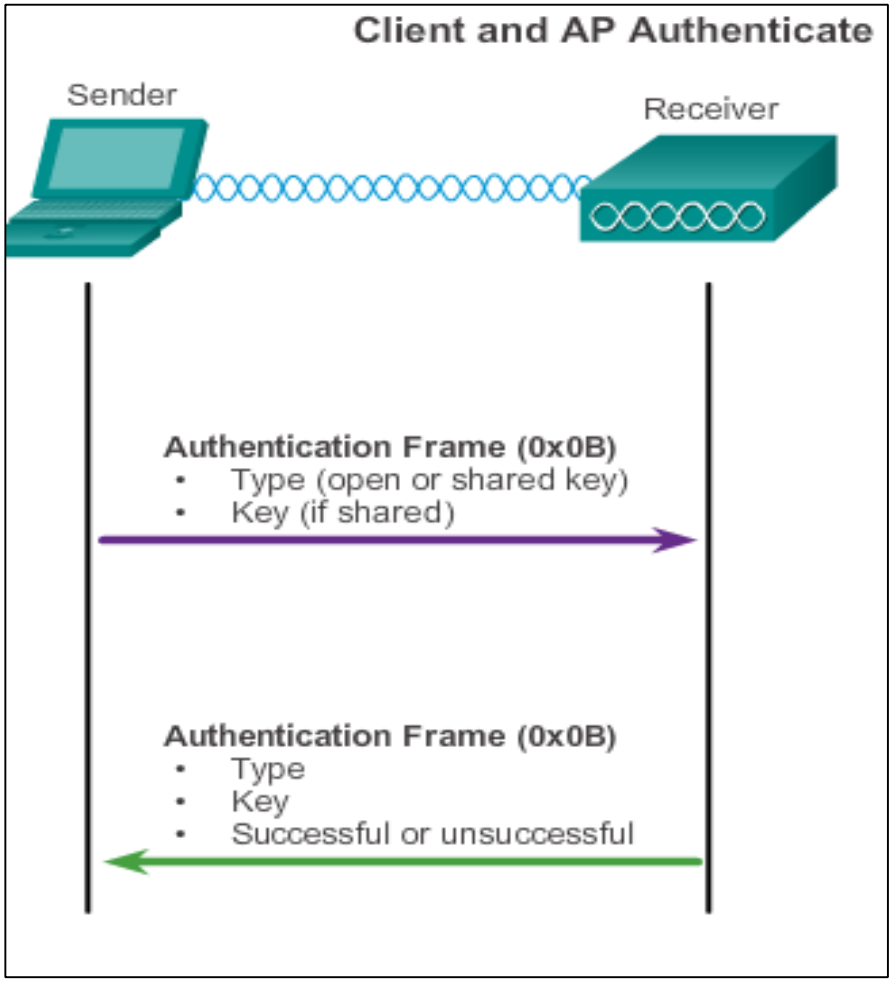
PROCESO DE RE-ASOCIACION

- El adaptador escucha los destellos de los APs, los evalua y elige el mejor AP.
- El adaptador envia la solicitud de asociación al AP que ha elegido (B).
- AP B le confima la asociación y le registra.
- AP B informa a AP A la re-association con AP B.
- AP A envia los paquetes del buffer a B y desregistra el adaptador.



Roaming from Access Point A to Access Point B

Autenticación



- **Abierta:** autenticación NULL donde el cliente dice " autentiqueme" y el AP responde con un "sí." Se utiliza cuando la seguridad no es una preocupación.

- **De clave compartida - s**e basa en una clave que es pre-compartida entre el cliente y el AP.

Saturación de la frecuencia de canal

- **Espectro ensanchado de secuencia directa (DSSS):** modulación de espectro ensanchado; difunde una señal sobre una banda de frecuencia más grande por lo que es más resistente a la interferencia. Utilizado por 802.11b.

- **Espectro ensanchado por salto de frecuencia (FHSS):** espectro ensanchado para comunicarse.

Transmite señales de radio cambiando rápidamente una señal portadora entre muchos canales de frecuencia.

Este proceso de salto de canal permite un uso más eficiente de los canales, la disminución de la congestión del canal. Utilizado por el estándar 802.11 original.

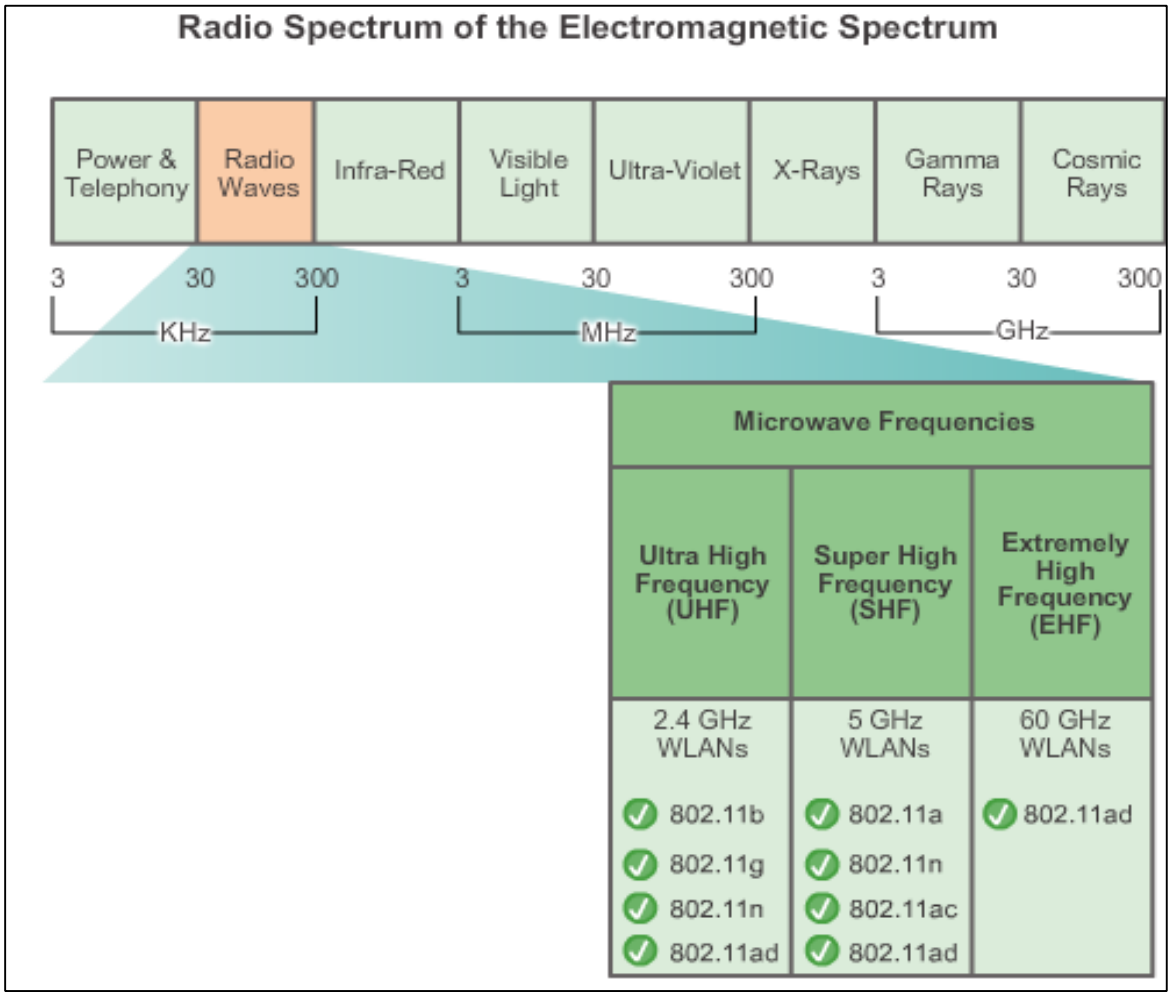
Saturación de la frecuencia de canal

Por división de frecuencia ortogonal multiplexación (OFDM): multiplexación por división de frecuencia de canales un único canal utiliza múltiples subcanales en frecuencias adyacentes.

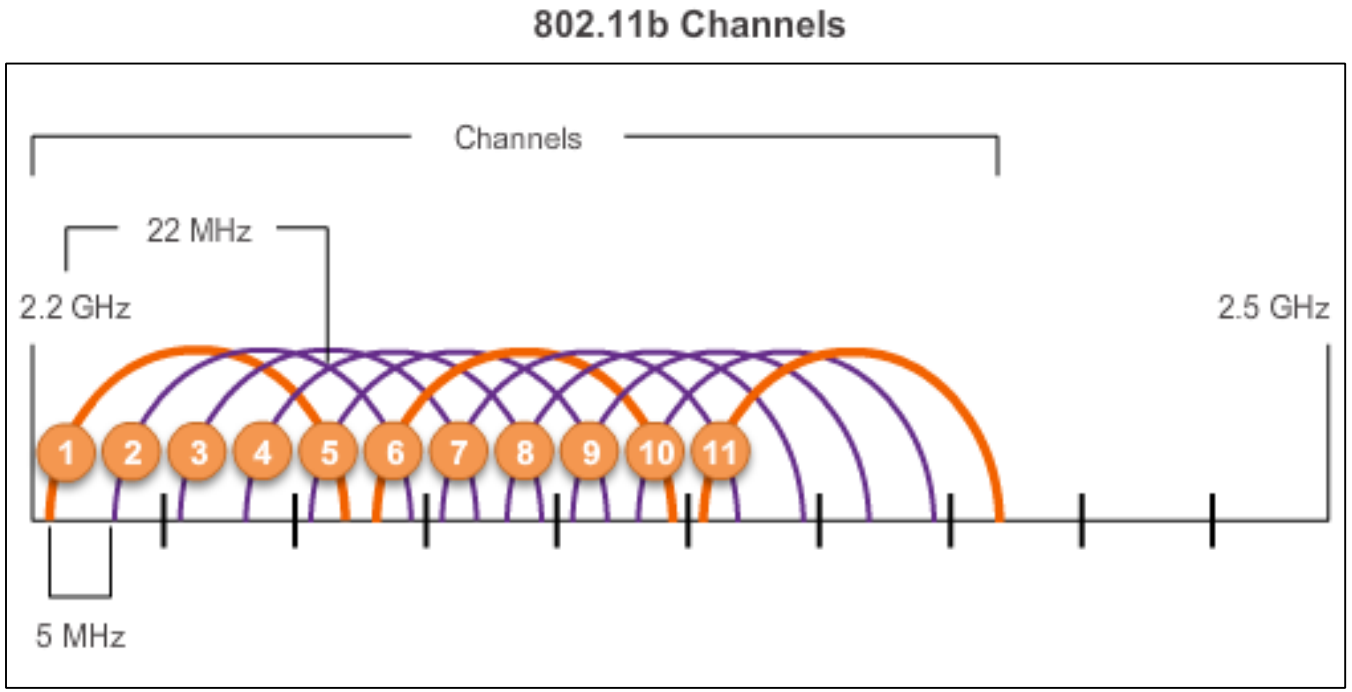
OFDM utiliza subcanales, el uso del canal es muy eficiente.

Utilizado varios sistemas de comunicación, incluidos 802.11a/g/n/ac.

Selección de canales

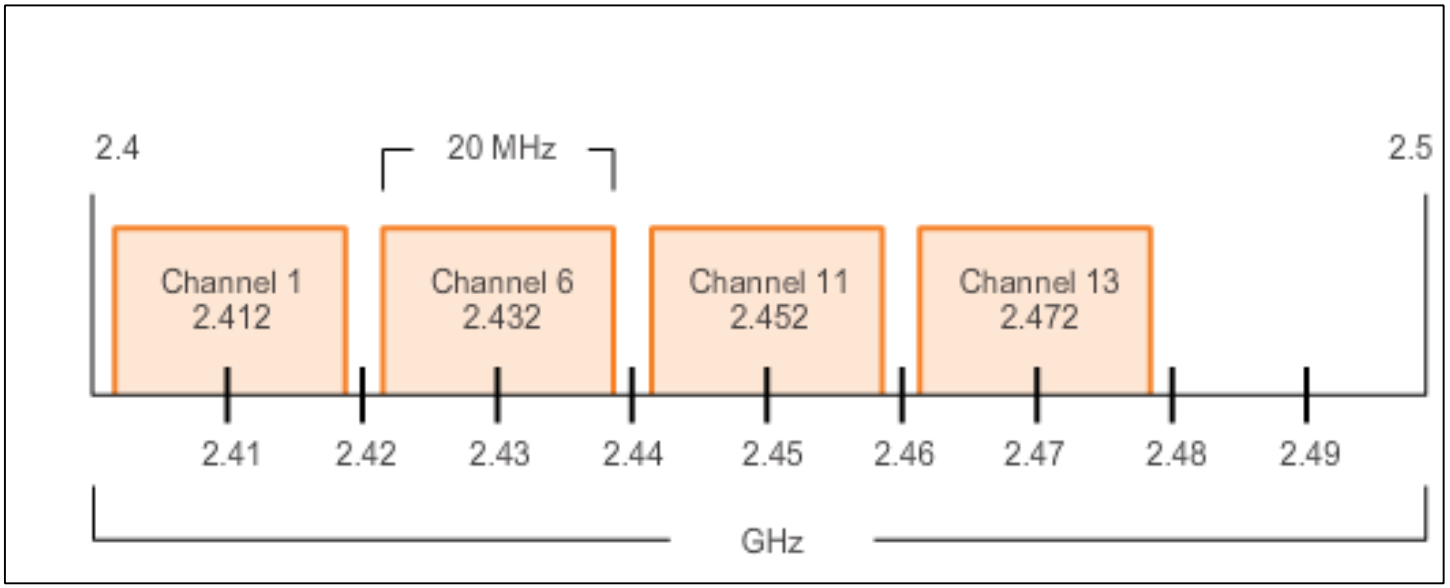


Selección de canales



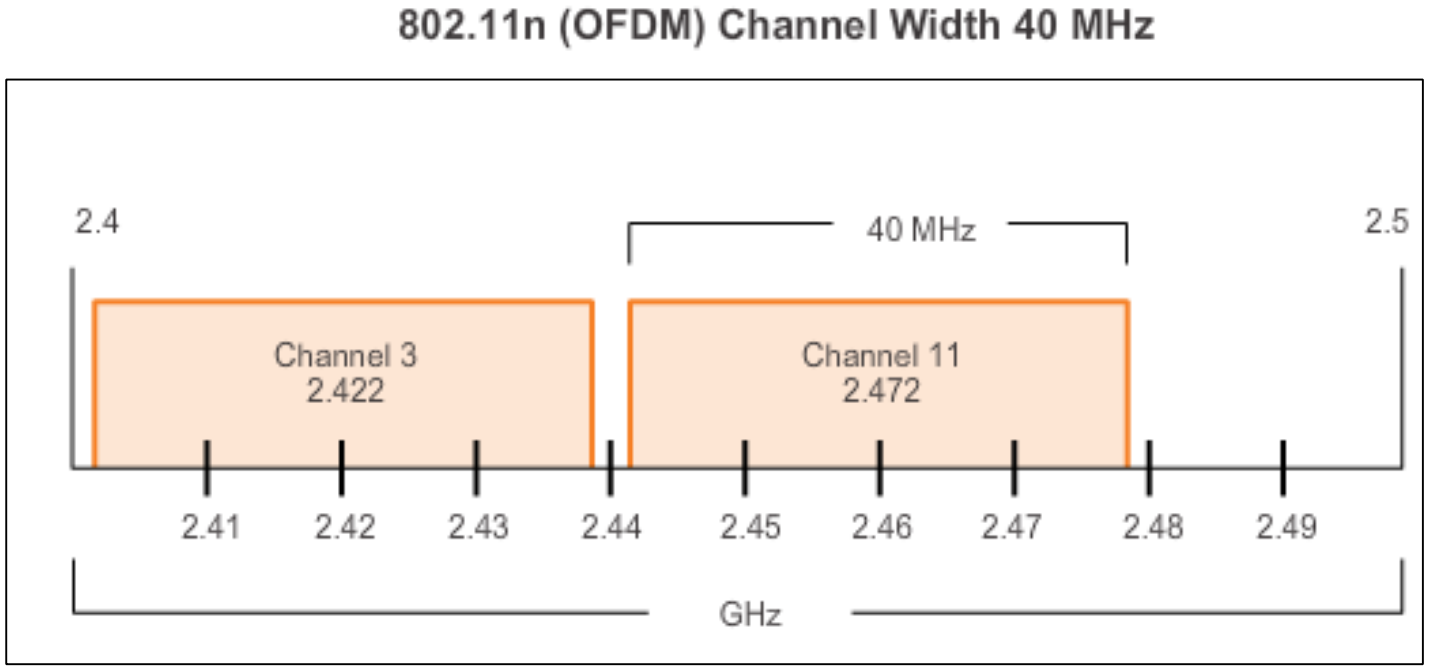
La solución a la interferencia 802.11b es el uso de los canales que no se superponen 1, 6 y 11.

Selección de canales



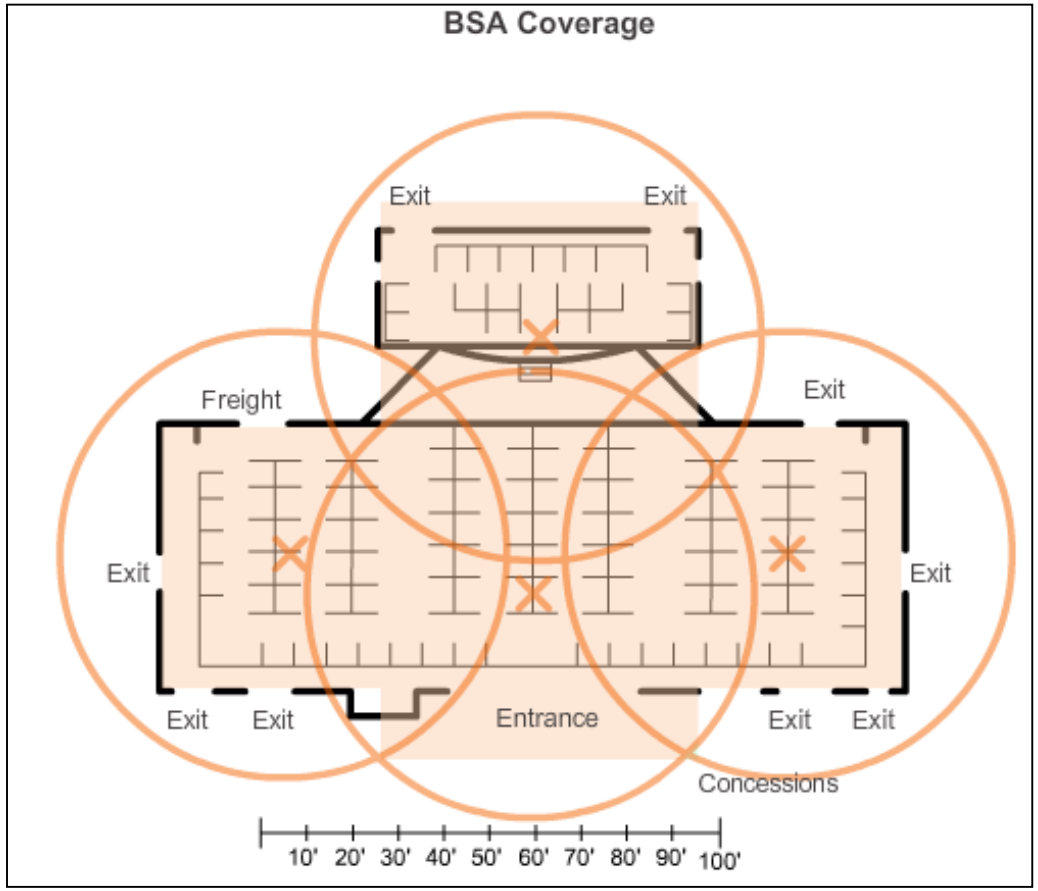
Utilizar canales de los mas grandes a los menos concurridos en la banda de los 5 GHz, reduce la "negación accidental del servicio (DoS)," esta banda puede soportar cuatro canales que no se superponen.

Selección de canales



La unión de canales combina dos canales de 20 MHz en un canal de 40 MHz.

Planear una implementación de WLAN



- La Posición de los APs no cerca de obstrucciones.
- La Posición AP verticalmente cerca del techo en el centro de cada área de cobertura.
- La posición AP en lugares donde se espera usuarios.

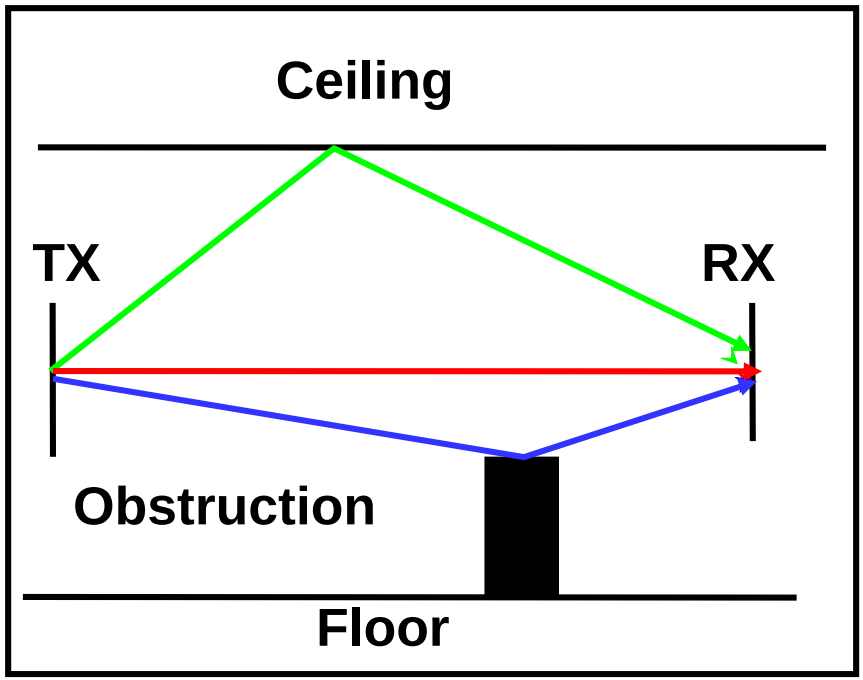
INTERFERENCIAS

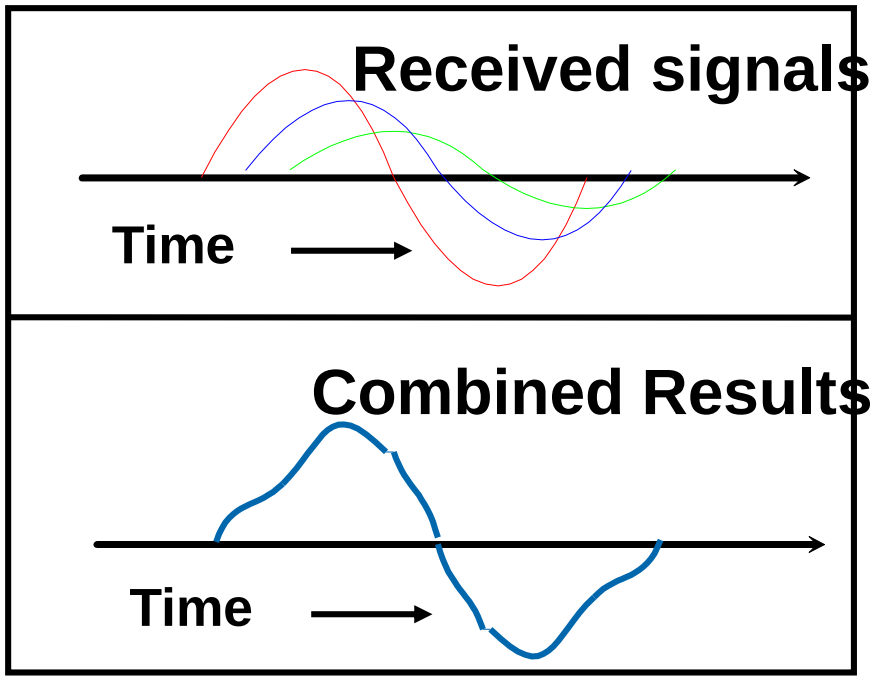
EXTERNAS: interfiere con FHSS (usan la misma banda) menos con DSSS. hornos microondas (funcionan a 2,4 GHz) interfieren con FHSS, a DSSS no le afectan.

Otros dispositivos: teléfonos inalámbricos, mandos a distancia de puertas de garage, etc.) potencia demasiado baja para interferir con las WLANs

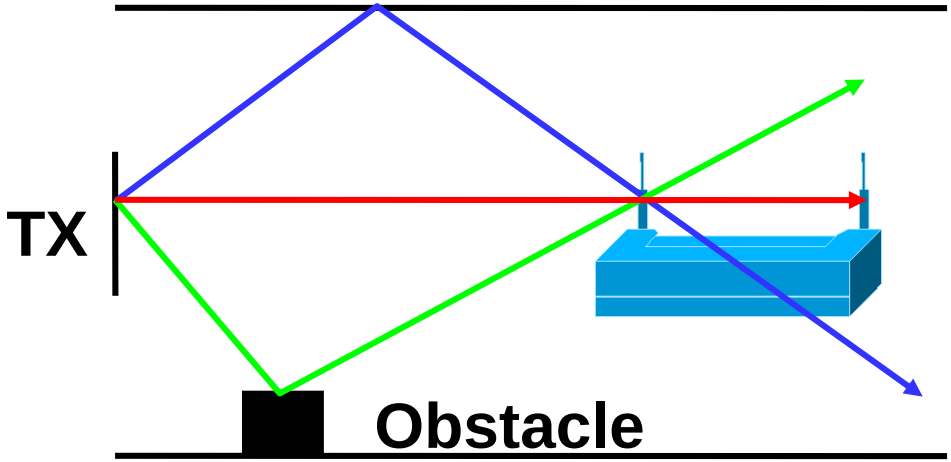
INTERNAS: Rebotes de la propia señal

DISTORSIÓN MULTITRAYECTORIA



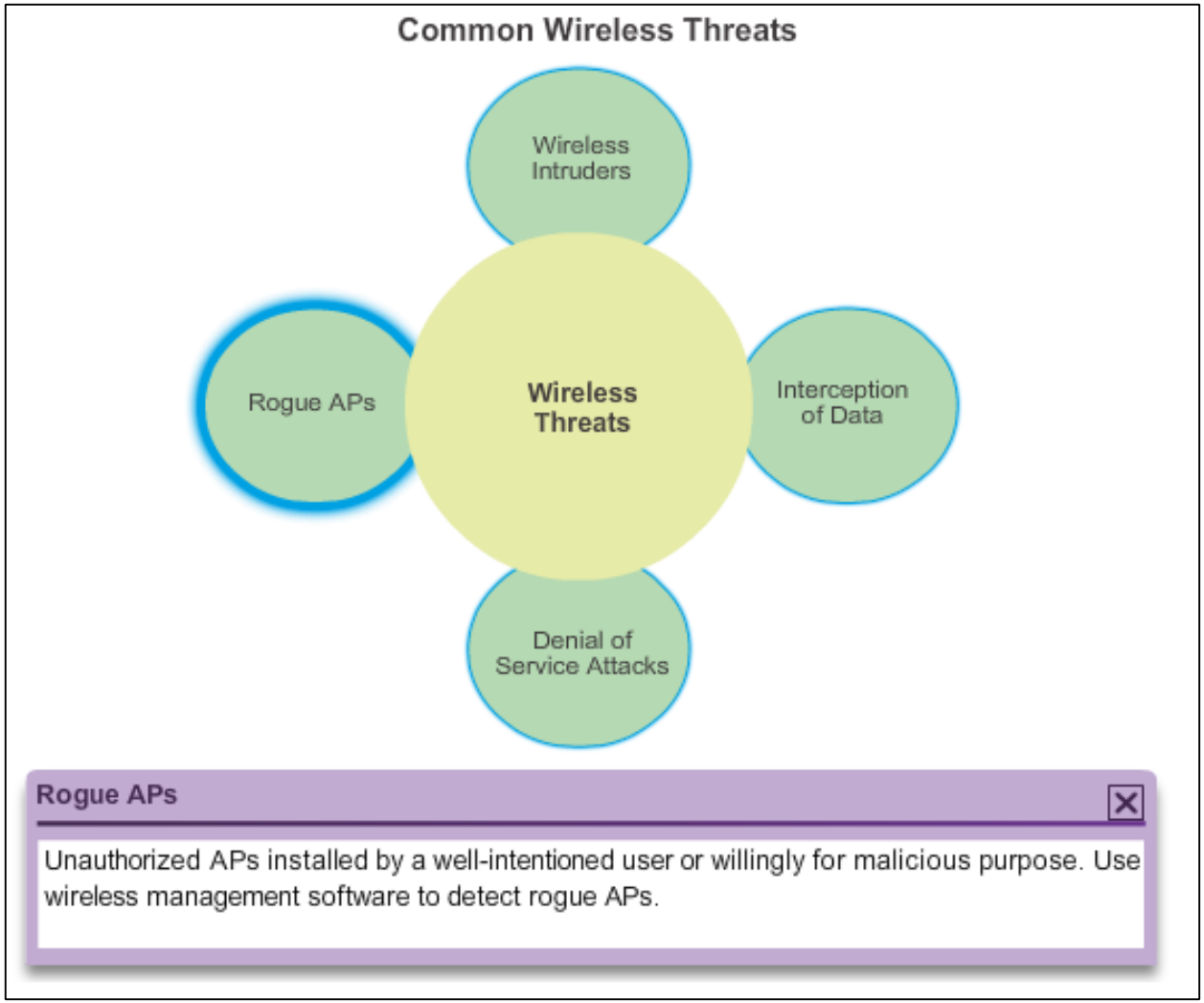


SOLUCIÓN: cambiar el tipo de antenas(antenas diversidad) y/o la Localización.



Las antenas duales basicamente lo que hacen es que si una antena no puede captar la señal, la otra si, consiguiento grandes ventajas en medios con obstaculos.

Ataques a la Seguridad inalambrica



Ataque DoS

Pueden ser el resultado de:

Dispositivos incorrectamente configurados.

Los errores de configuración pueden desactivar la WLAN.

Interferencia accidental

Las WLANs operan en las bandas de frecuencia sin licencia y son propensos a la interferencia de otros dispositivos inalámbricos.

Con dispositivos hornos microondas, teléfonos inalámbricos, y más.

2,4 GHz es más propenso a las interferencias que la banda de 5 GHz.

Administración de la trama de los ataques de DoS

Un ataque de desconexión falsa: cuando un atacante envía una serie de comandos de "desasociar“ para todos los clientes.

Los clientes tratan inmediatamente de volver a asociar, lo que crea una explosión de tráfico.

Una inundación CTS : atacante aprovecha el método de contención CSMA / CA para monopolizar el ancho de banda.

Inunda repetidamente tramas Clear to Send (CTS) con un PC falso.

Todos los clientes inalámbricos que comparten el medio de RF reciben el CTS y retienen las transmisiones hasta que el atacante deja de transmitir las tramas CTS.

Puntos de acceso ilegales (rogue)

Un AP ilícito es un AP o router inalámbrico que ha sido:

Conectado a una red corporativa sin autorización explícita y en contra de la política corporativa.

Conectado o activado por un atacante para capturar datos de los clientes, como las direcciones MAC (tanto alámbricas e inalámbricas), o para capturar paquetes y para obtener acceso a recursos de red, o lanzar ataques man-in-the-middle (MITM).

Para impedir la instalación de AP maliciosos, las organizaciones deben utilizar el software de monitoreo para vigilar activamente el espectro radioeléctrico para los AP no autorizados.

Ataque de Man-in-the-Middle

Ataque de “AP gemelo malvado (Evil twin AP)”:

Un ataque de MITM inalámbrica muy popular un atacante introduce un AP ilícito y lo configura con el mismo SSID que un AP legítimo.

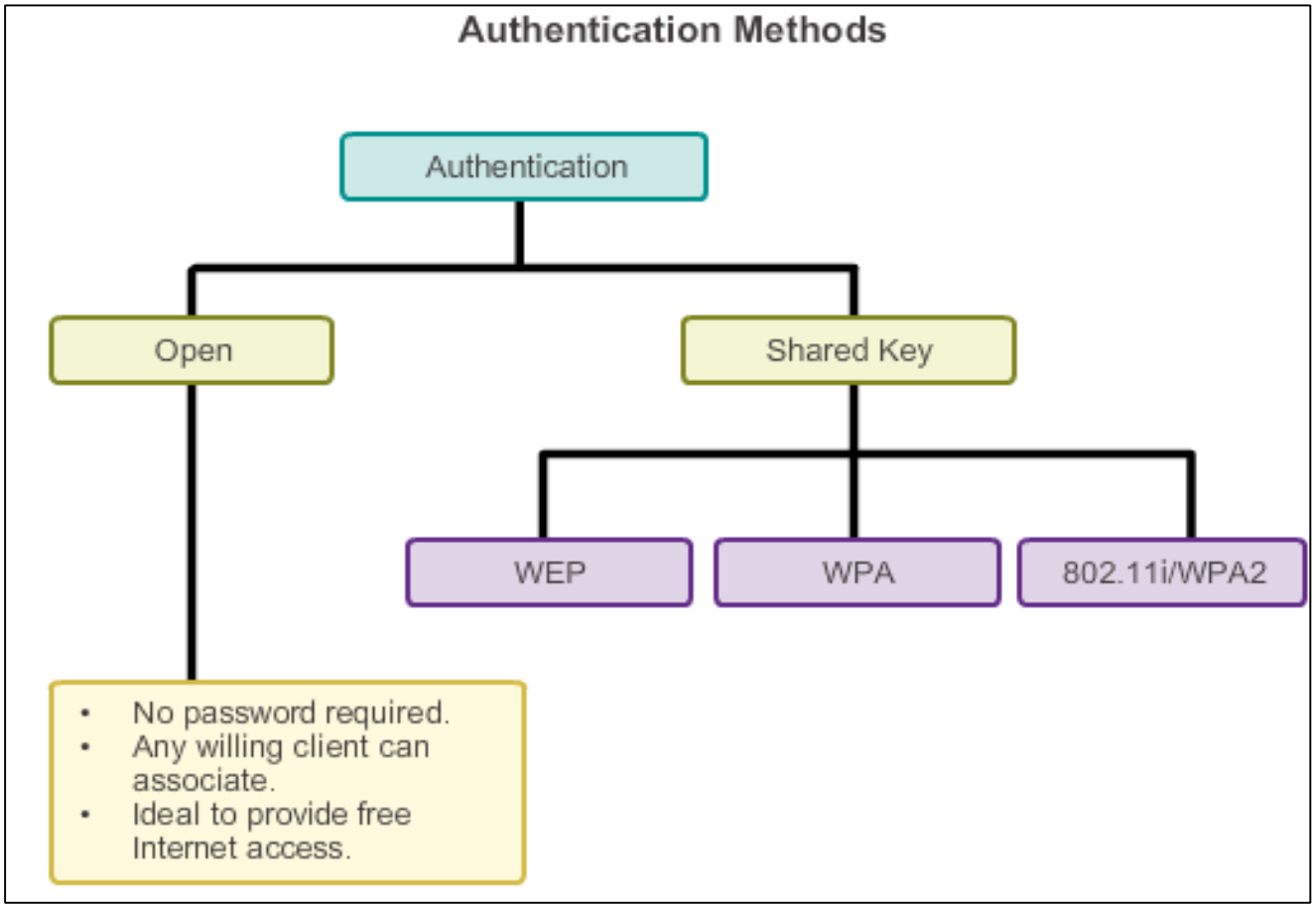
Se da en lugares que ofrecen Wi-Fi, aeropuertos, cafés y restaurantes, debido a la autenticación abierta.

La Conexión de clientes vería dos AP que ofrecen acceso inalámbrico. Aquellos cerca del AP ilegal encuentran la señal y lo más probable el asociado más fuerte con el gemelo AP pero ilegal. El tráfico de usuarios ahora se envía al AP ilegal, que a su vez recoge los datos y los envía al AP legítimo

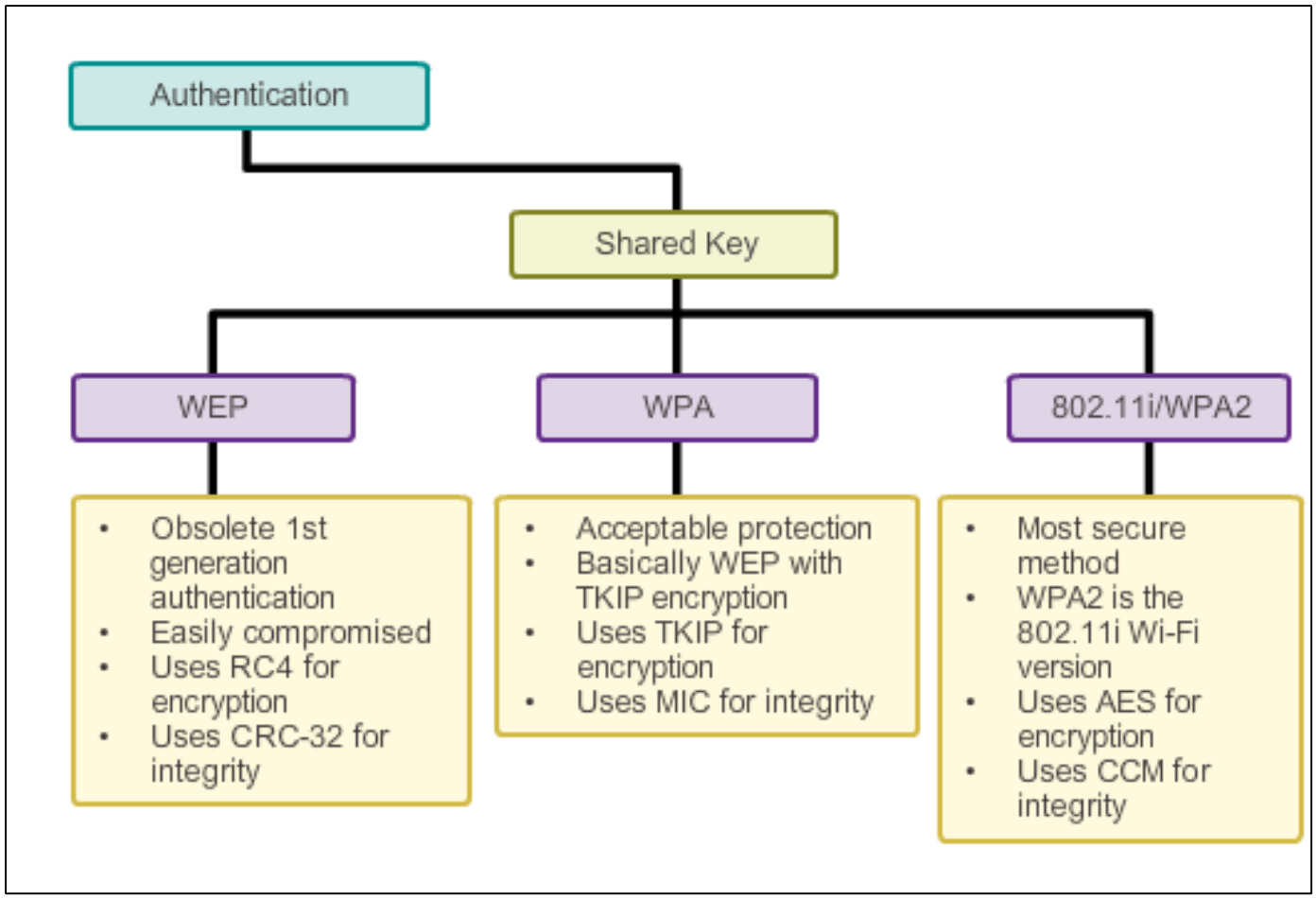
El tráfico de retorno del AP legítimo se envía al AP ilegal, capturando, y reenviando a los usuarios incautos .

Información general sobre seguridad Wireless

Utilice la autenticación y el cifrado para asegurar una red inalámbrica.



Metodos de autenticación de clave compartida



Metodos de encriptamiento

El estandar IEEE 802.11i y el Wi-Fi Alliance WPA y WPA2 utilizan:

Protocolo de Integridad de Clave Temporal (TKIP) : utiliza WPA.

- Hace uso de WEP, y de TKIP y lleva a cabo una comprobación de integridad de mensajes de Cisco (MIC).

- **Advanced Encryption Standard (AES) :** utiliza WPA2.
- Método preferido, se alinea con el estándar IEEE 802.11iA.
- Método de cifrado más fuerte.
- Utiliza el modo Cifrado de contador con encadenamiento de Mensaje Protocolo de Autenticación de código de bloque (CCMP).

- **Elija siempre WPA2 con AES cuando sea posible.**

WPA y WPA2 dos tipos de autenticación

Personal : para el hogar o pequeñas redes de oficina los usuarios utilizan una clave pre-compartida (PSK).

No se requiere servidor de autenticación especial.

Empresa: Requiere autenticación remota Dial-In User Service (RADIUS) servidor de autenticación. seguridad adicional.

Los usuarios deben autenticarse utilizando el estándar 802.1X, que utiliza el protocolo de autenticación extensible (EAP)

Autenticación en la Empresa

Opciones de seguridad de la empresa requieren una autenticación, autorización y contabilidad (AAA) del servidor RADIUS.

Configuración de un router inalámbrico

Antes de instalar un router inalámbrico, tenga en cuenta:

Management Parameters	Settings
Network Name (SSID)	Home-Net
Network Password	cisco123
Router Password	class123
Guest Network Name	Home-Net-Guest
Guest Network Password	cisco
Linksys Smart Wi-Fi Username	My-Name
Linksys Smart Wi-Fi Password	class12345

Configuración de un router inalámbrico

Paso 1. Iniciar el proceso de implementación de la WLAN con un único AP y un solo cliente, sin habilitar la seguridad inalámbrica.

Paso 2. Compruebe que el cliente ha recibido una dirección IP DHCP y puede hacer ping al router por defecto conectado por cable local y, a continuación, vaya a Internet .

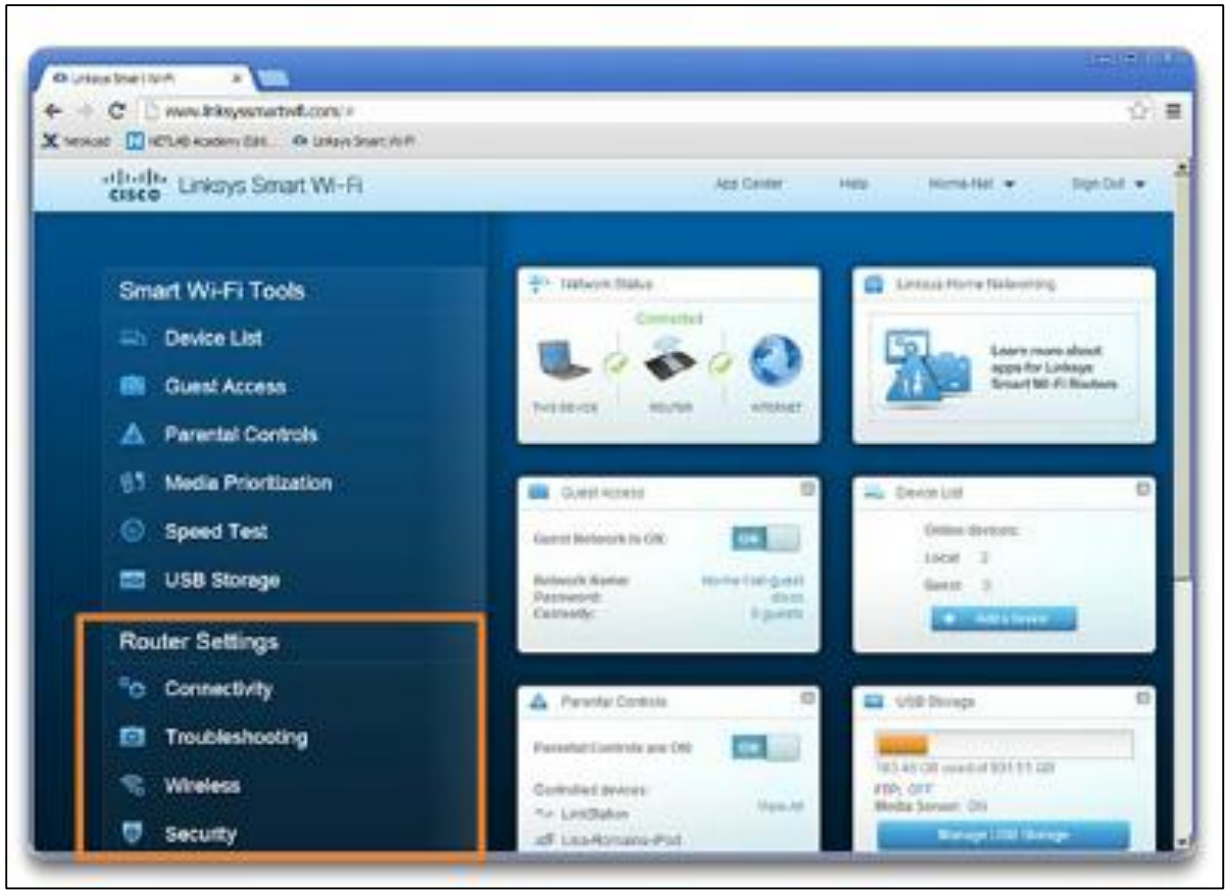
Paso 3. Configurar la seguridad inalámbrica utilizando WPA2/WPA Mixta Personal. Nunca use WEP a menos que no existan otras opciones.

Paso 4. haga una Copia de seguridad de la configuración.

Configurar e instalar el Linksys EAS6500

Configuración de la Página de inicio Linksys Smart Wi-Fi

Smart Wi-Fi Router Settings



Configuración inteligente del Wi-Fi

Realizar la configuración básica del router para la red local.

Diagnosticar y solucionar problemas de conectividad de la red.

Asegurar y personalizar la red inalámbrica.

Configurar la función DMZ, ver los equipos y dispositivos de la red conectados y configurar el redireccionamiento de puertos.

Herramientas inteligentes de Wi-Fi

- **Lista dispositivos** - Lista quién está conectado a la WLAN. Personalice los nombres de dispositivos e iconos.
- **Acceso de invitados** - Crea una red independiente para 50 invitados en el hogar, manteniendo la red principal a salvo.
- **Controles parentales** - Protege los niños y miembros de la familia al restringir el acceso a sitios web
- **Medios Priorización** - Prioriza el ancho de banda de los dispositivos y aplicaciones específicas.
- **Testeo de la velocidad** - Prueba la velocidad y descarga de la conexión a Internet. Útil para la línea de base.
- **Almacenamiento USB** - Controla el acceso a los archivos compartidos.

Copia de seguridad de una configuración

Para realizar copias de seguridad de la configuración con el router inalámbrico, realice los siguientes pasos:

Paso 1. Inicie sesión en la página de Smart Wi-Fi Home. Haga clic en el icono de solución de problemas para mostrar la ventana Estado de solución de problemas.

Paso 2. Haga clic en la ficha Diagnóstico para abrir la ventana de diagnóstico para solucionar problemas.

Paso 3. Bajo el título de configuración del router, haga clic en Copia de seguridad y guardar el archivo en una carpeta adecuada.

Conexión de clientes inalámbricos

- Después que el AP o router inalámbrico se ha configurado, la NIC inalámbrica en el cliente debe ser modificado para permitir que se conecte a la WLAN.

- El usuario debe verificar que el cliente se ha conectado correctamente a la red inalámbrica correcta, porque puede haber muchas redes WLAN disponibles con los que conectarse.

Enfoques de solución de problemas

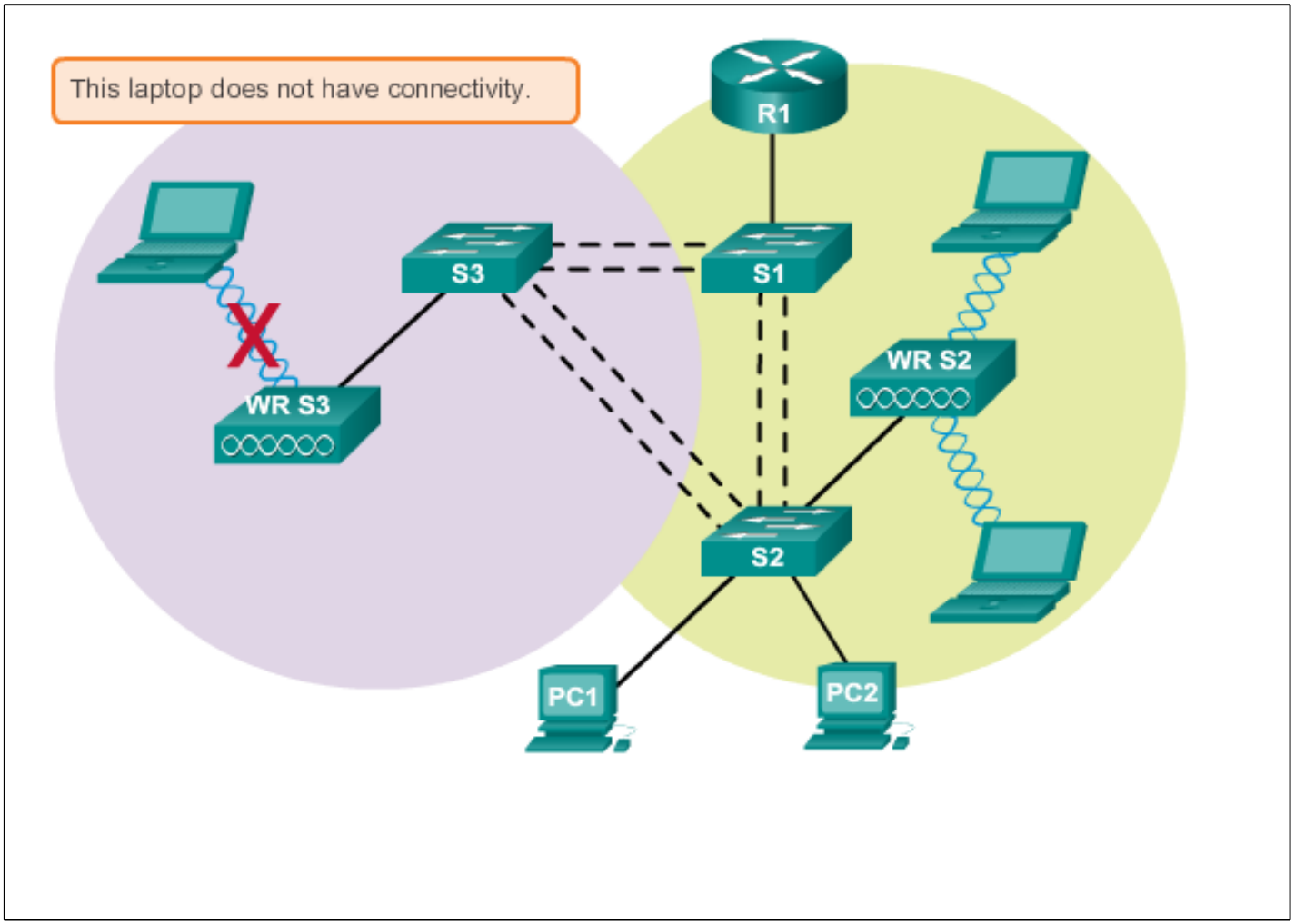
Tres enfoques principales de solución de problemas:

De abajo hacia arriba Comience en la capa 1 y vaya subiendo.

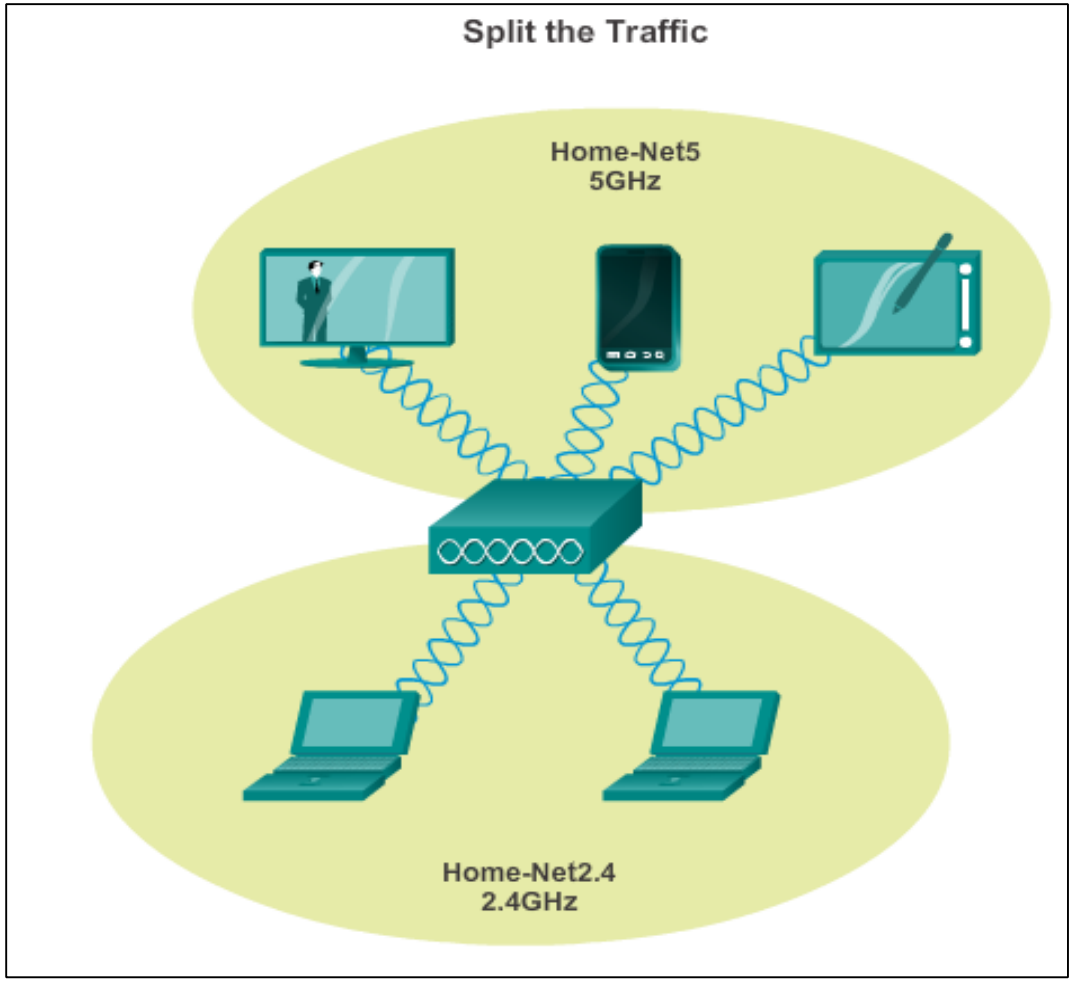
De arriba hacia abajo Comience en la capa superior y trabaje hacia abajo.

Divide y vencerás Ping al destino. Si los pings fallan, compruebe las capas inferiores. Si los pings son exitosos, verificar las capas superiores.

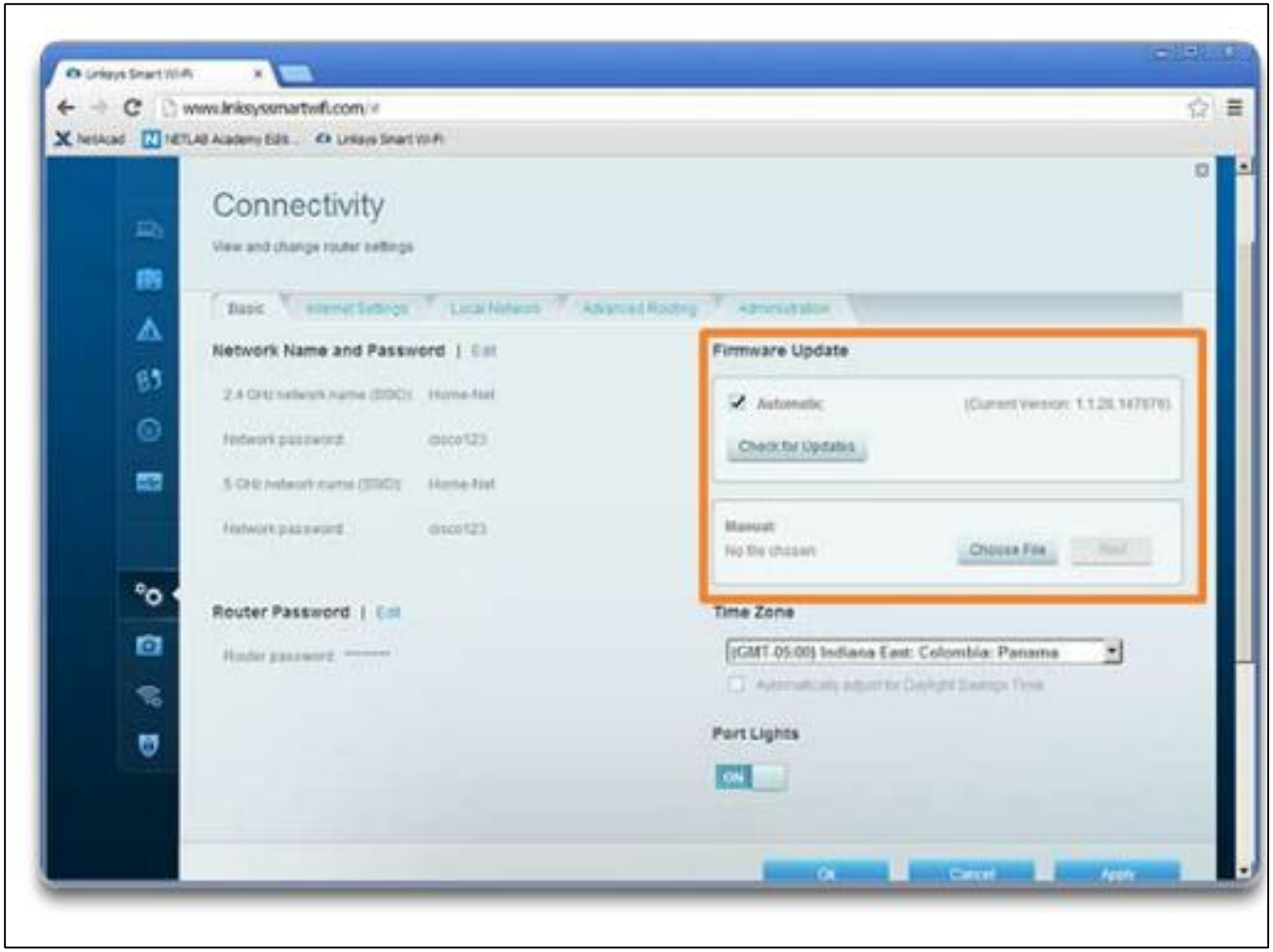
Cliente inalámbrico no se conecta



Solución de problemas cuando la red es lenta



Actualización del firmware



Resumen

- WLANs a menudo en los hogares, oficinas y entornos de campus.
- Frecuencias 2,4, 5,0 y 6,0 GHz se utilizan para redes WLAN 802.11.
- El UIT-R regula el espectro de RF, los estándares IEEE 802.11 para definir cómo se utilizan estas frecuencias para la sub-capa física y MAC de las redes inalámbricas.
- La Wi-Fi Alliance certifica que los productos de los proveedores se ajustan a normas de la industria.
- El STA (estación o PC) utiliza una tarjeta de red inalámbrica para conectarse a un AP, o enrutador inalámbrico o AP.
- STA se conecta utilizando un SSID.
- Los AP pueden ser implementados como dispositivos independientes, en pequeños grupos, o en una red basada en el controlador más grande.

Resumen

- Un AP Cisco puede usar una antena omnidireccional, direccional o Yagi de señales directas.
- IEEE 802.11n/ac/ad utilizan la tecnología MIMO para mejorar el rendimiento y soporte para hasta cuatro antenas, simultáneamente.
- En modo ad-hoc o IBSS, dos dispositivos inalámbricos se conectan entre sí de una manera P2P.
- En modo infraestructura, AP se conectan a la infraestructura de red utilizando la red de cable.
- Cada AP define un BSS y se identifica por su BSSID.
- Múltiples BSS se pueden unir en un ESS.
- El uso de un SSID particular en un ESS proporciona capacidades de itinerancia sin fallas entre el BSS en el SEE.

Resumen

- SSID adicionales se pueden utilizar para separar el nivel de acceso a la red definida por cual es el SSID que está en uso.
- Una STA se autentica primero con un AP, y luego se asocia al AP.
- La autenticación 802.11i/WPA2 se debe utilizar. Utilice el método de cifrado AES con WPA2.

- En la planificación de la red inalámbrica, los canales no se superponen deben utilizarse en la implementación de varios AP para cubrir un área en particular. Debe haber una superposición de 10-15 por ciento entre BSA en un ESS.
- Las redes inalámbricas son susceptibles a amenazas como intrusos inalámbricos, AP ilegales, interceptación de datos y ataques de DoS. Cisco ha desarrollado soluciones para mitigar este tipo de amenazas.

Cisco | Networking Academy®

Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO