Wireless Technology

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Wireless Network

- Introduction to WLAN
- 802.11 IEEE & NIC
- Radio Transmission
- WLAN Topologies
- Access Points
- Bridges
- Security
- Site Survey
- Troubleshooting
- Emerging Technologies

Introduction to Wireless LANs

Cisco | Networking Academy®
Mind Wide Open™

1 - ¿Qué significa para WLAN?

Es la unión de dos o más ordenadores sin necesidad de utilizar cables. Inalámbrico utiliza la tecnología de espectro ensanchado o de OFDM (802.11a) de modulación basado en ondas de radio para permitir la comunicación entre dispositivos en un área limitada.

Una WLAN, al igual que una LAN, requiere un medio físico a través del cual pasan las señales de transmisión. las WLANs utilizan luz infrarroja (IR) o frecuencias de radio (FR). El uso de la RF es mucho más popular por su mayor alcance, mayor ancho de banda, y una cobertura más amplia.

2 - ¿Por qué necesitamos WLAN y cuáles son sus beneficios?

WLAN se está volviendo más y más popular debido a su conveniencia, la conectividad de alta velocidad, la eficiencia de costes, y la facilidad de integración con otras redes y componentes de red.

Algunos de los beneficios de WLAN son:

Conveniencia: permite a los usuarios acceder a los recursos de red desde casi cualquier lugar.

movilidad

confiabilidad

Capacidad de ampliación

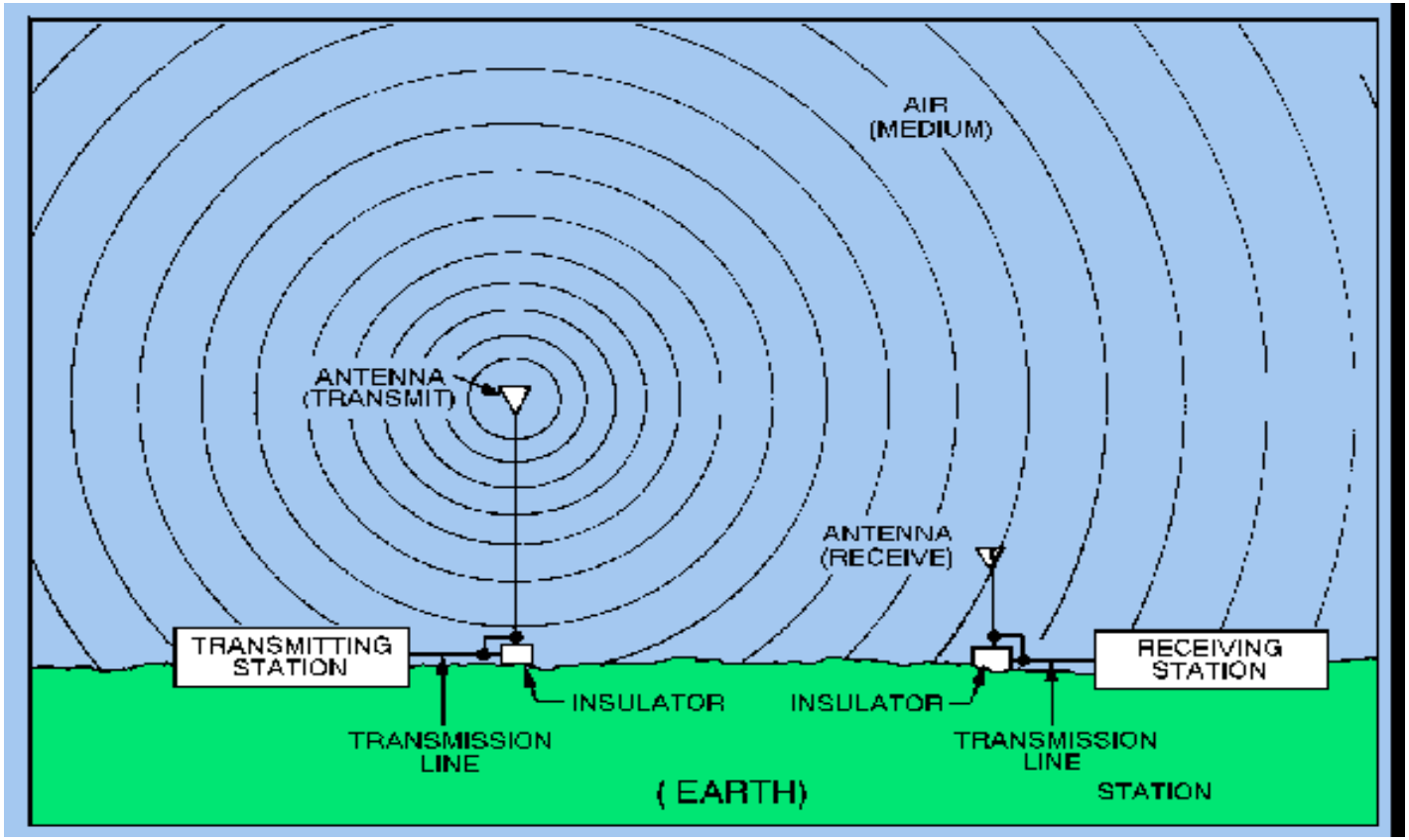
ahorro de costes

ventajas de montaje

3 - ¿Cuál es el medio de una red para la WLAN?

La conectividad inalámbrica utiliza la atmósfera como un medio de red. Las señales inalámbricas son ondas electromagnéticas que pueden viajar a través del espacio. Así hay medios físicos son necesarios para transmitir y recibir señales.

La capacidad de las ondas de radio de viajar a grandes distancias y extenderse en espacios cubiertos se comunica sin hilos una manera versátil para construir una red.



4 - Componentes y topologías WLAN:

Los diversos componentes de una LAN inalámbrica que debe dar pleno cumplimiento a los estándares IEEE 802.11 y entregar un rendimiento hasta 54 Mbps son:

Receptor Wireless Client: se necesita para conectar un dispositivo de computación (por ejemplo, de escritorio, portátil, PDA ...) para el cableado en red a través de un punto de acceso. Incluye PCMCIA, LM, tarjeta PCI ....

- ***Los puntos de acceso (APs):*** se necesitan sólo en el modo de infraestructura de redes WLAN. Ellos proporcionan al cliente inalámbrico con un punto de acceso en una red. Son como los conmutadores Ethernet en una red cableada y operan en modo half-duplex (por ejemplo O bien recibir o transmitir en un momento dado).

- ***Puentes:*** se utilizan para conectar dos o más redes. En este momento hay 3 series de Cisco Puentes: El 350 Wireless Bridge (BR350), Cisco 350 Series Puente de grupo de trabajo (WGB350), y Cisco Aironet 1400.

- ***WLAN Antenas:*** la adición de una antena no aumenta la potencia de transmisión pero se centra la señal en una dirección particular para aumentar la recepción.

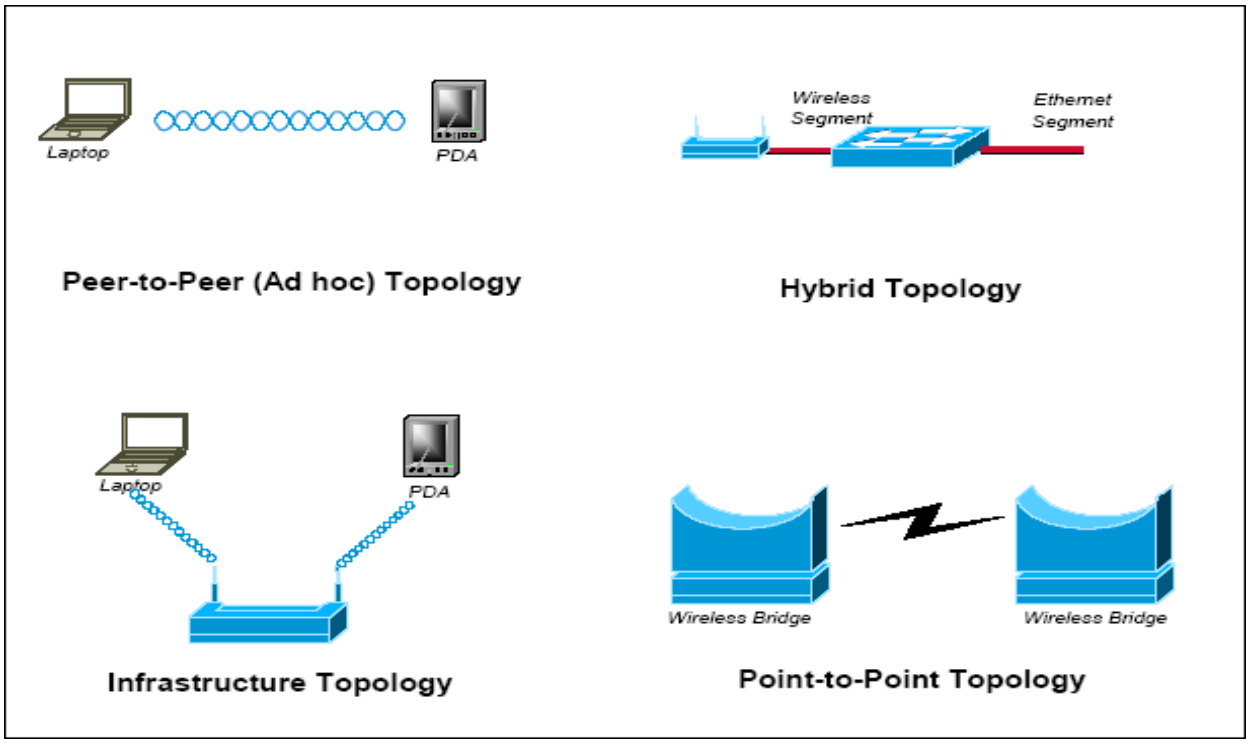
La WLAN es compatible con cuatro topologías de red:

Topología Peer-to-Peer (Ad hoc)

Topología híbrido

Topología Infraestructura

Topología de punto a punto



IEEE 802.11

Cisco | Networking Academy®
Mind Wide Open™

Public and Vendor Standards

Official Standards

El comité 802 soporta en su modelo lógico de LLC (control de enlace lógico), MAC (control de acceso a medios) y PHY (capa física).

La LLC: es la subcapa superior de la capa de enlace de datos de OSI. Es lo mismo para los diversos medios físicos (por ejemplo, Ethernet, Token Ring ...).

Principalmente para:

Multiplexación y demultiplexación protocolos transmitidos a través de la MAC al transmitir y recibir.

Asegurando el control del flujo y la detección y la retransmisión de paquetes perdidos, si así lo solicita.

MAC: es una parte de la capa de enlace de datos del modelo OSI. Proporciona el direccionamiento y los mecanismos de control de acceso de canal que hace varios nodos de la red se comunican dentro de una red multipunto (LAN o WAN).

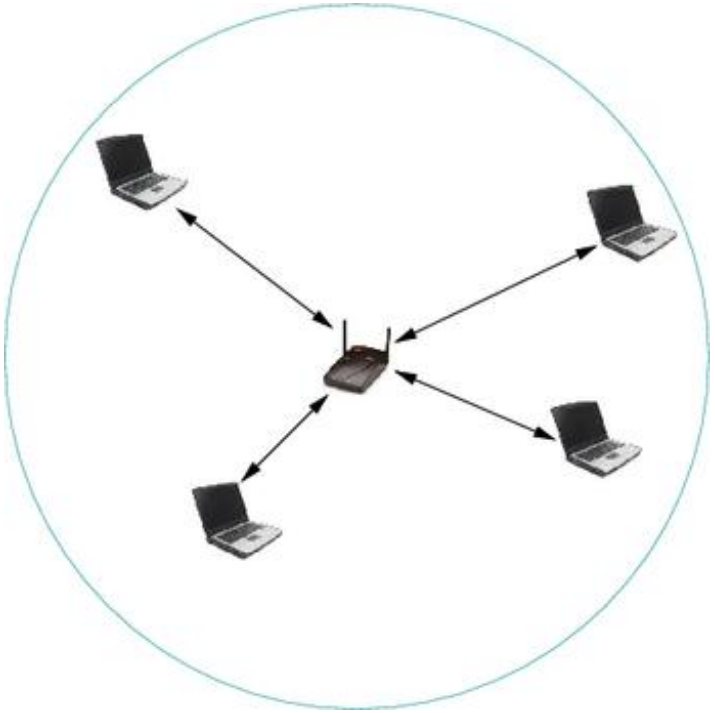
Capa física: es el nivel uno en el modelo OSI. Se lleva a cabo los servicios solicitados por la capa de enlace de datos.

La capa física es la capa de red más básica, proporcionando únicamente los medios de transmisión de bits de primas en lugar de paquetes a través de un enlace de datos físico que conecta los nodos de la red.

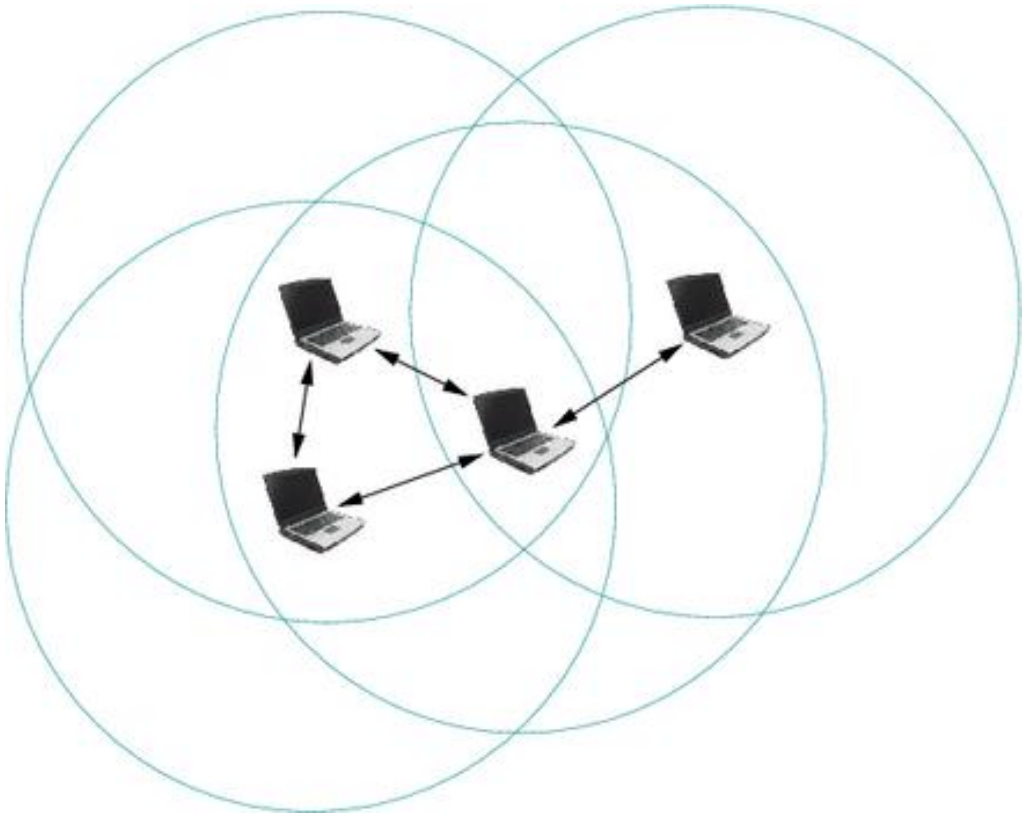
2- Arquitectura lógica 802,11

La arquitectura IEEE 802.11 tiene 5 componentes:

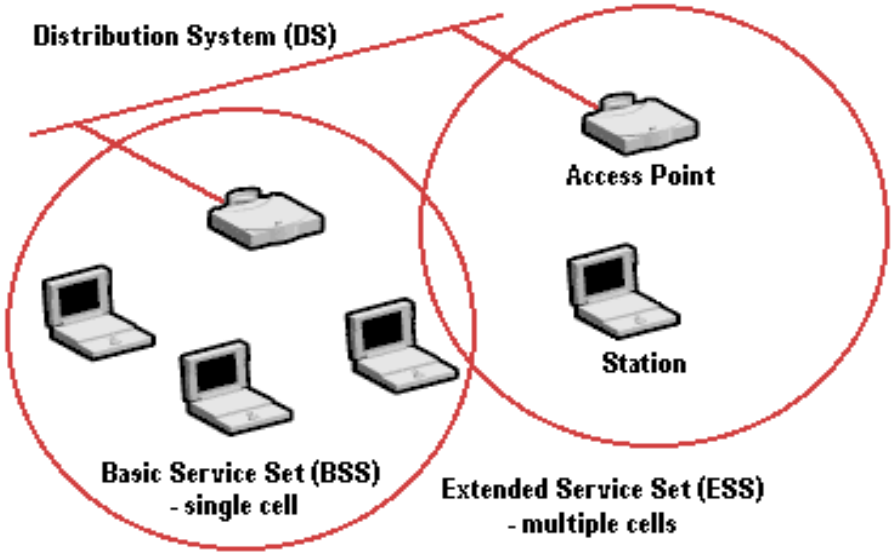
BSS: conjunto de servicios básicos (BSS) es el bloque básico de una LAN IEEE 802.11. Cubre una sola área de RF, o célula



- **IBSS (Independent Service Set Básico):** En este modo de operación, IEEE 802.11 las estaciones se comunican directamente. también se le llama una red peer-to-peer

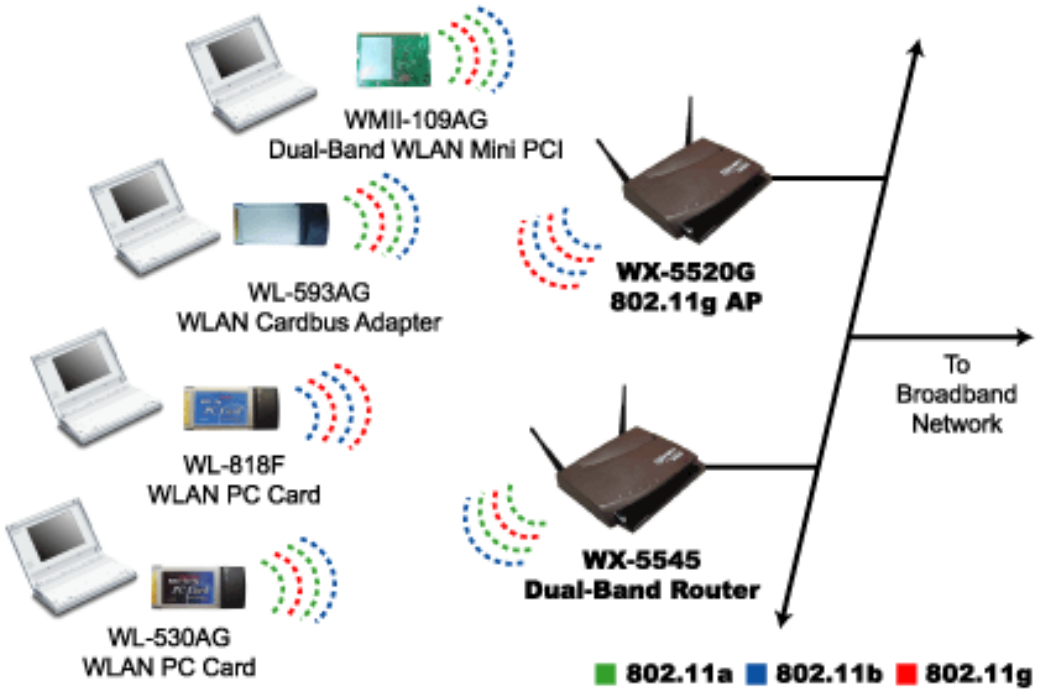


- **DS (Distribution System):** Este modo se trata de conectar dos estaciones WLAN físicamente.



- **ESS (conjunto de servicio extendido):** Se define como dos o más BSS conectados por un DS comunes.

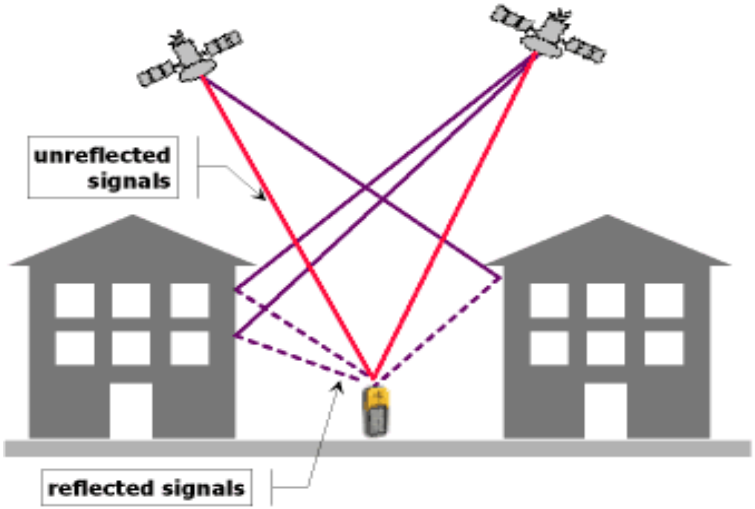
- **Roaming:** da el cliente inalámbrico la capacidad de moverse de una célula a otra sin perder la conexión a la red.



Propagación de las ondas de radio

En el vacío, a 2,4 GHz las microondas viajan a la velocidad de la luz. Una vez iniciado, estas microondas continuarán en la dirección en que se emitieron para siempre, a menos que interactúan con alguna forma de materia.

Dado que las WLAN son por lo general en la tierra, dentro de la atmósfera, las microondas viajan en el aire, no en el vacío. La señal deberá enfrentarse a angulos de refracción y reflexión causada por obstáculos como montañas, edificios ...



WLAN Topologies

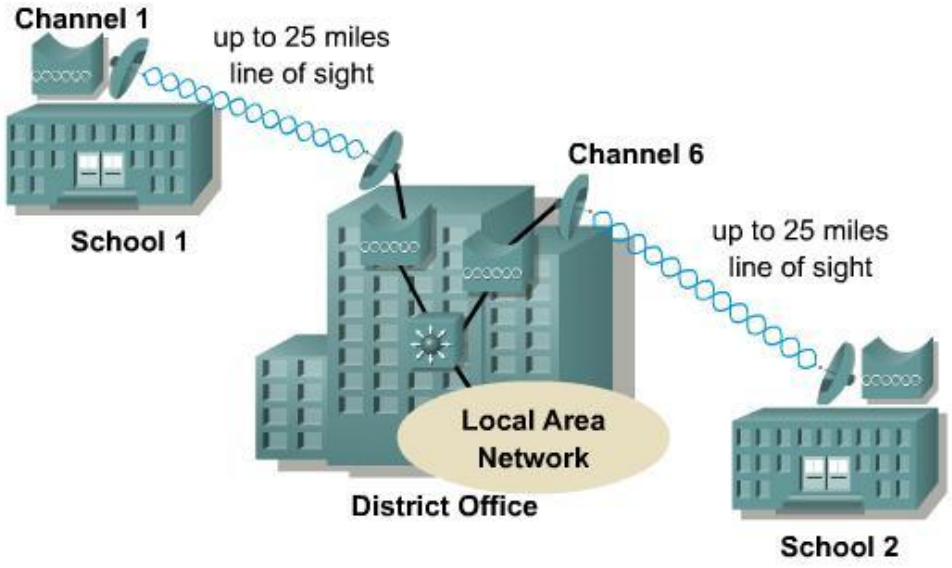
Cisco | Networking Academy®
Mind Wide Open™

categorías WLAN

Los productos WLAN encajan en dos categorías principales:

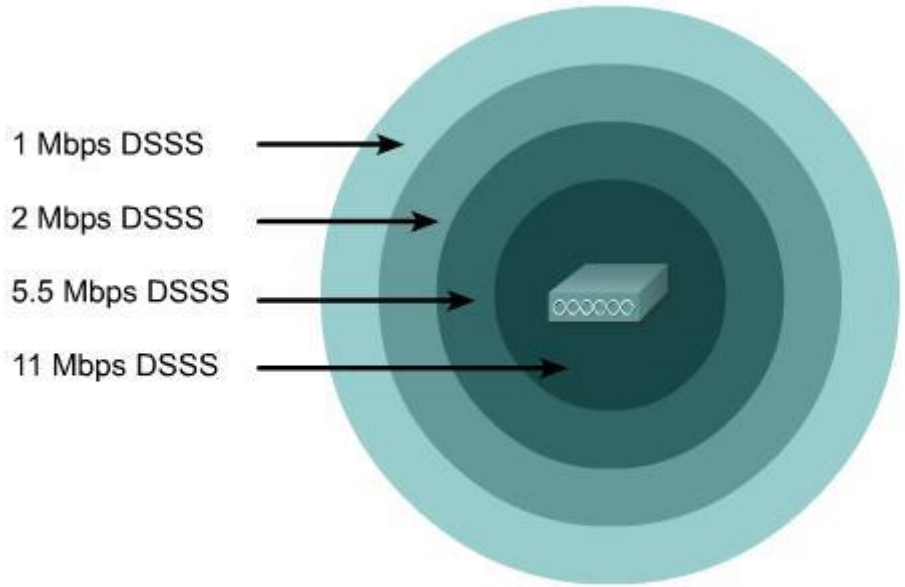
LAN inalámbricas de edificios

puente Wireless de edificio a edificio



La cobertura del punto de acceso

A medida que el cliente se desplaza de un punto de acceso a otro, cuando se aleja de un punto de acceso, la velocidad de datos disminuirá sin perder la conexión.



VLAN

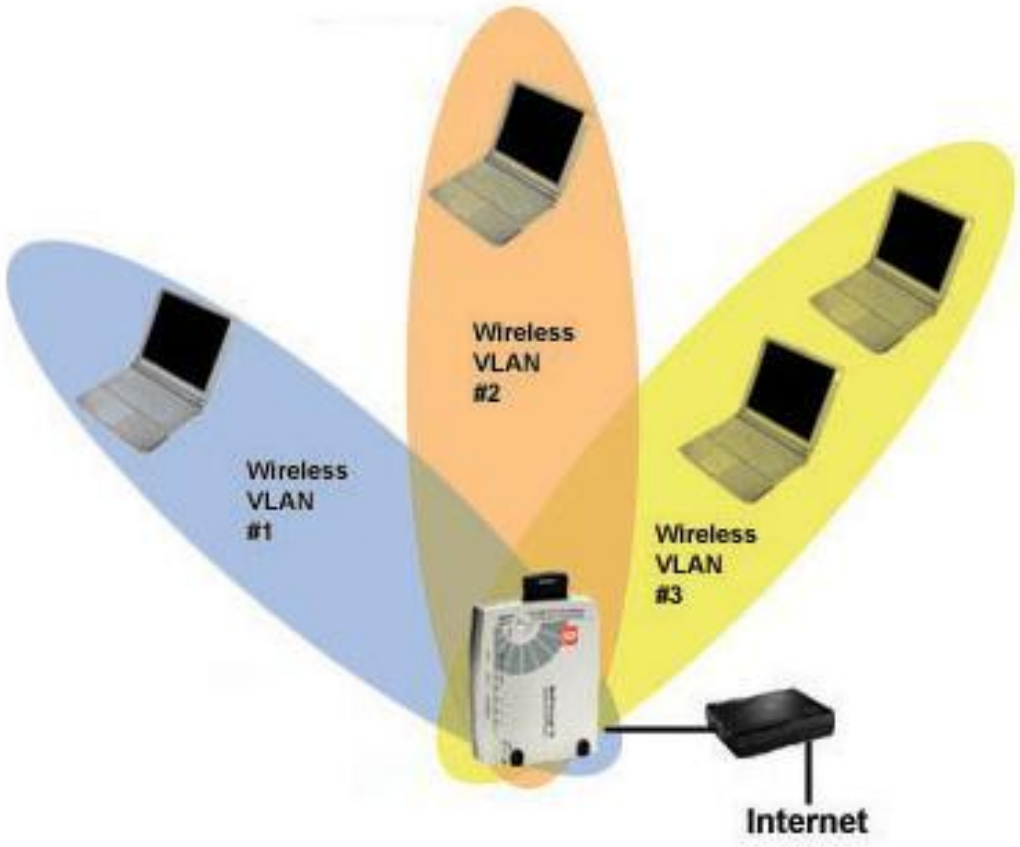
VLAN (red de área local virtual) es un método de creación de redes lógicas independientes dentro de una red física.

Algunos de los beneficios y las razones que una empresa podría tener VLAN son:

seguridad

Aumentar el control sobre múltiples tipos de tráfico.

No pasa el tráfico a los nodos y automáticamente reduce emisiones.


Wireless
VLAN
#2
Wireless
VLAN
#1
Wireless
VLAN
#3
Internet

¿Por qué asegurar la WLAN?

Si sólo se navega por la Web y envia correos electrónicos ocasionales, el riesgo de ser hackeado bajo. Sin embargo, no es tan simple como eso. En primer lugar, si alguien se las arregla para interceptar su WLAN y su conexión a Internet, incluso si es sólo un enlace de módem lenta, están robando su ancho de banda.

Peor aún, cualquier persona en su WLAN va a utilizar la misma dirección de protocolo Internet (IP) como tú. Para otras personas en Internet parecen ser usted. Así que la seguridad de su WLAN parece una idea brillante

¿Cuánta seguridad es suficiente?

Cuando se piensa en la seguridad de su conexión inalámbrica, usted debe responder a estas preguntas primero:

¿Qué valor tiene la información que usted está enviando?

¿Cuántos inconvenientes están dispuestos a tolerar?

¿Cuánto estás dispuesto a pagar?

¿Qué seguridad se puede obtener ahora?

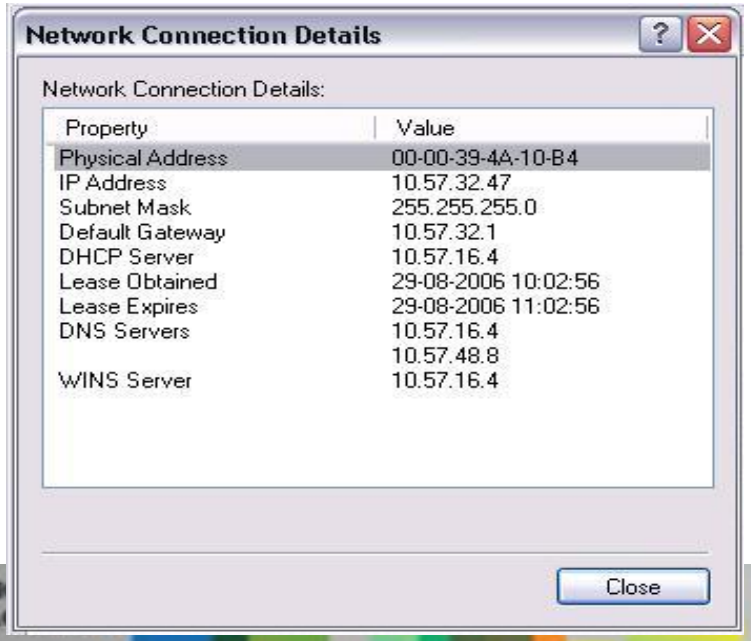
Hay una serie de pasos que puede tomar para minimizar el riesgo de un robo WLAN, la primera es cambiar la configuración predeterminada de su punto de acceso.

ESSID: El principal de ellos es el ESSID (Extended Service Set ID), o el nombre de la WLAN. **configure el punto de acceso para que no transmite el ESSID.** De esta manera, sólo los clientes autorizados pueden conectarse a su AP.

Filtros de direcciones MAC

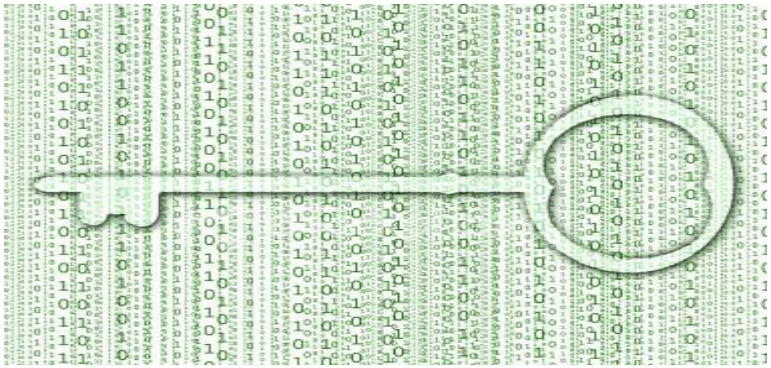
Hay una segunda capa de seguridad que puede adoptar, el filtro de direcciones MAC (Media Access Control). Una dirección MAC es una identidad única a fuego en cada adaptador de red durante la fabricación, y no hay forma de cambiarlo.

AP tiene una lista de direcciones MAC y sólo permite a los de la lista para conectarse.



Encryption

- Incluso si los hackers pueden ir más allá de su punto de acceso, pueden todavía ser capaz de acceder a los datos que está atravesando su WLAN.
- La manera de proteger los datos en tránsito es el cifrado, el estándar de cifrado WLAN siendo WEP (Wired Equivalencia de Privacidad).
- WEP funciona mediante la encriptación del tráfico para cifrar el trafico al punto de acceso o el PC cliente y descifrar a su llegada.



Locking down (OBSERVANDO)

- El siguiente paso consiste en bloquear el AP. Se dará cuenta de que se puede cambiar la configuración de la AP sobre la WLAN. Esto no es una buena idea. Asegúrese de sólo configurar el punto de acceso a través de una conexión por cable. Y no se olvide de cambiar la contraseña siempre que sea posible defecto.

Authentication

- La capa final de protección es la autenticación individual. El método estándar de autenticación de WLAN utiliza el protocolo 802.1X. Si el protocolo está activado, los usuarios no autenticados no pueden pasar de la AP para acceder al resto de la red.

Las normas de seguridad del futuro

La próxima generación de estándares de seguridad, conocido como el WPA (Wi-Fi Protected Access), mejora lo que tenemos ahora. A diferencia de las claves de cifrado estáticas de hoy en día, se utiliza una contraseña maestra de la cual el sistema genera claves que cambian continuamente usando un protocolo conocido como TKIP.

Las claves nunca se reutilizan, reducir el riesgo de que un hacker las descubra. WPA también incluye 802.1X, se discutió anteriormente, lo que permite el sistema para comprobar que está accediendo contra una base de datos central de usuarios conocidos.

Site Survey

Cisco | Networking Academy®
Mind Wide Open™

¿Qué es una inspección del lugar?

Un estudio del sitio de radio frecuencia (RF) es el primer paso en el despliegue de una red inalámbrica y el paso más importante para garantizar el funcionamiento deseado. descubre las áreas de cobertura de RF, comprueba la interferencia de RF y determina la colocación adecuada de los dispositivos inalámbricos.

¿Cuál es la necesidad Wireless de la inspección del lugar?

Un estudio del lugar ayuda a definir los contornos de cobertura de RF en una instalación particular. Nos ayuda a descubrir las regiones donde puede ocurrir mulitpath distorsión, áreas en las que la interferencia de RF es elevada y encontrar soluciones para eliminar esas cuestiones.

Un estudio del sitio que determina el área de cobertura de RF en una instalación que también ayuda a elegir el número de dispositivos inalámbricos que una empresa necesita para satisfacer sus necesidades de negocio.

¿Cuáles son las limitaciones de diseño en una inspección del lugar adecuado?

Los cuatro principales requisitos de diseño que deben ser atendidos, mientras se lleva a cabo una inspección del lugar son:

alta disponibilidad

Escalabilidad

Manejabilidad

Interoperabilidad

¿Cuáles son los resultados de una visita sobre el sitio Wireless?

Una visita sobre el sitio adecuado proporciona información detallada que aborda la cobertura, fuentes de interferencias, la colocación del equipo, las consideraciones de energia y los requisitos de cableado. La documentación de la visita al sitio sirve como una guía para el diseño de la red y para la instalación y verificación de la infraestructura de comunicación inalámbrica.

¿Qué equipo básico es necesario para la realización de una visita sobre el sitio?

Algunos de los equipos básicos y utilidades que se requiere para la realización de un estudio del sitio incluyen:

Punto de acceso inalámbrico

Tarjeta de cliente inalámbrico

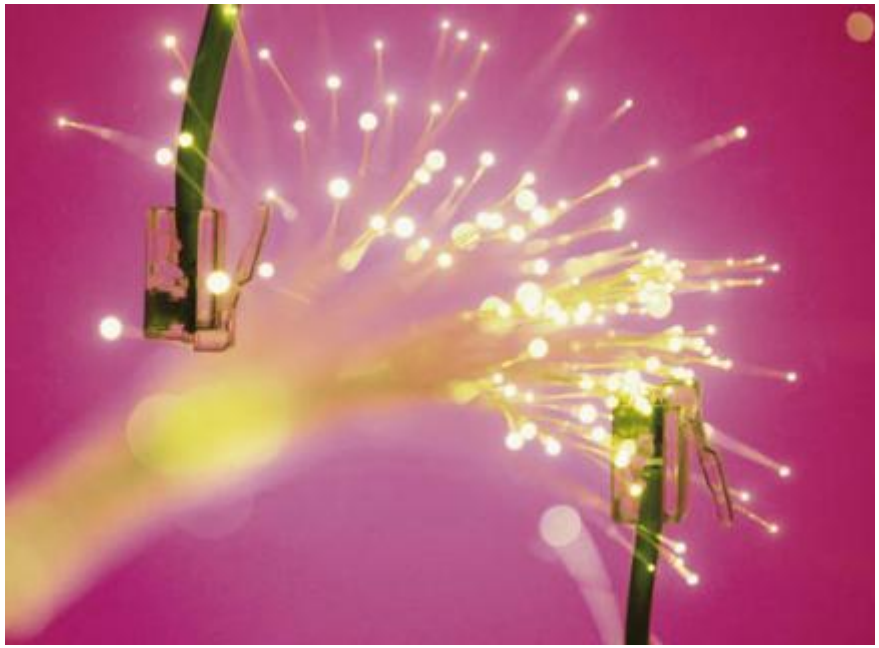
Portátil o PDA

Variedad de antenas (esto depende de la exigencia de la firma)

Software de utilidad de la encuesta del sitio

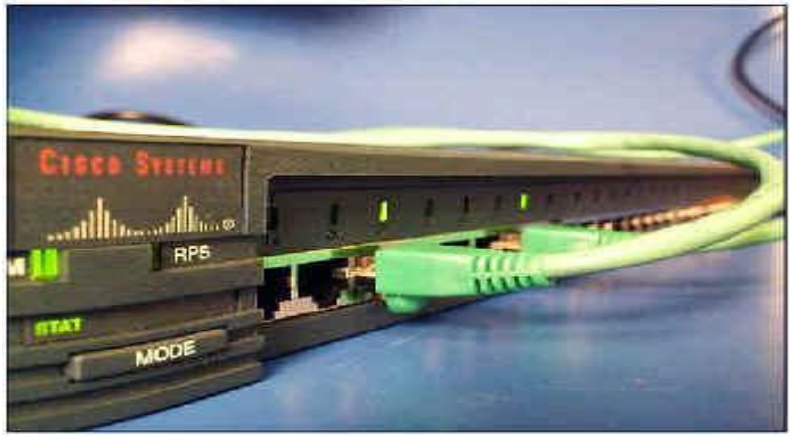
OSI Solución de problemas

Capa 1: los medios de conexión, conectores y dispositivos. La mayoría de los problemas comunes que se producen son a causa de los cables, conectores y panel de conexión.



Capa 2: puentes y switches

Analizan las tramas de entrada, toman decisiones de envío basadas en la información contenida en los tramas y reenviar las tramas hacia sus destinos. Debido a que el dispositivo opera en la capa de enlace de datos, no se requiere para examinar la información de capa superior.



Emerging Technologies

Cisco | Networking Academy®
Mind Wide Open™

Una gran cantidad de tecnologías emergentes están listos para estar en el lado de los clientes.

Algunas de estas tecnologías son:

Voz sobre LAN

VoIP

Wireless Mobile

Voice over IP

Existen cuatro diferentes estandares de señalización y protocolos de control de llamada que utilizan para VoIP:

H.323

Media Gateway Control Protocol (MGCP)

Protocolo de Iniciación de Sesión (SIP)

H.248/Megaco

VoIP ofrece muchos beneficios:

ahorro de costes

Los estándares abiertos

Redes de voz y datos integrados

Mobile Wireless

Las principales tecnologías inalámbricas móviles se pueden clasificar de acuerdo con el método por el que se comparte el medio. Las opciones inalámbricas móviles son variadas y a menudo confusa, en parte porque hay tantos y en parte debido a que las mismas tecnologías son conocidas por diferentes nombres en diferentes partes del mundo.

- FDMA
- TDMA
- CDMA
- GSM
- GPRS
- EDGE
- WCDMA; CDMA2000
  - 3G, 4G, LTE

Cisco | Networking Academy®

Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO