



Cisco Networking Academy Program
**Fundamentals of
Wireless LANs**

The only authorized textbook for the
Cisco Networking Academy Program

Módulo 1: Introducción a las LANs wireless

Descripción general

Este módulo proporciona una introducción a la tecnología en rápida evolución de las LANs inalámbricas (WLANs). Las WLANs redefinen la forma en que la industria contempla las LANs. La conectividad ya no implica conexión física. El networking inalámbrico proporciona todas las funciones y beneficios de las tecnologías de LAN tradicionales sin alambres ni cables. La libertad de movilizarse sin perder la conectividad ha ayudado a conducir al networking inalámbrico hasta nuevos niveles.

Después de proporcionar las razones de la popularidad del networking inalámbrico, este módulo enumerará y explicará los diferentes tipos de medios de networking, identificará las características básicas de las WLANs y presentará los componentes de las WLANs y sus funciones.

Existen cuatro factores importantes a considerar antes de implementar una red inalámbrica:

- Alta disponibilidad
- Escalabilidad
- Gestionabilidad
- Arquitectura abierta

Finalmente, este módulo explicará el uso del espectro inalámbrico y su conservación en lo que se refiere al futuro del networking inalámbrico.

1.1 Introducción a las LANs Inalámbricas

1.1.1 ¿Qué es una LAN inalámbrica?

En términos sencillos, una red de área local inalámbrica (WLAN) hace exactamente lo que el nombre implica. Proporciona todas las funciones y beneficios de las tecnologías LAN tradicionales, como Ethernet y Token Ring, pero sin las limitaciones impuestas por los alambres o cables. De esta forma, las WLANs redefinen la forma en la cual la industria contempla las LANs. Conectividad ya no significa conexión física. Las áreas locales ya no se miden en pies ni en metros, sino en millas o kilómetros. Una infraestructura no necesita estar enterrada u oculta detrás de los muros, sino que puede desplazarse y cambiar según las necesidades de una organización.

Una WLAN, al igual que una LAN, requiere un medio físico a través del cual pasan las señales de transmisión. En lugar de utilizar par trenzado o cable de fibra óptica, las WLANs utilizan luz infrarroja (IR) o frecuencias de radio (RFs). El uso de la RF es mucho más popular debido a su mayor alcance, mayor ancho de banda y más amplia cobertura. Las WLANs utilizan las bandas de frecuencia de 2,4 gigahertz (GHz) y de 5 GHz. Estas porciones del espectro de RF están reservadas en la mayor parte del mundo para dispositivos sin licencia. El networking inalámbrico proporciona la libertad y la flexibilidad para operar dentro de edificios y entre edificios. A lo largo de este curso, los íconos y símbolos mostrados en las Figuras 1 a 4 se utilizarán para documentar los dispositivos y la infraestructura del networking inalámbrico.

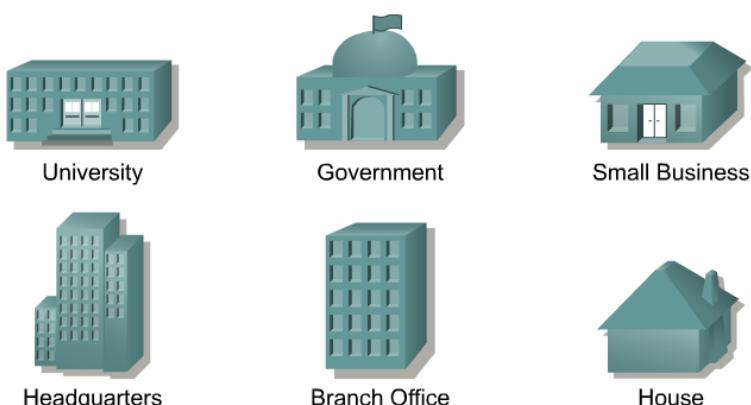
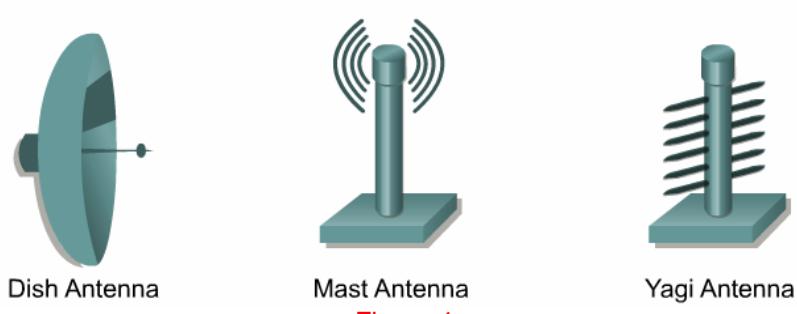
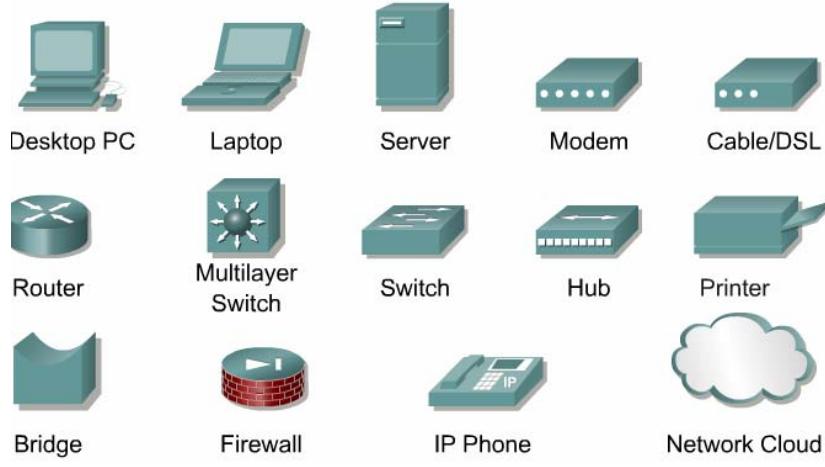
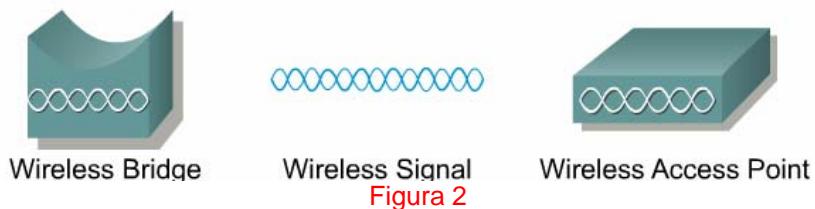


Figura 1



1.1.2 ¿Ya no más cables?

Los sistemas inalámbricos no carecen completamente de cables. Los dispositivos inalámbricos son sólo una parte de la LAN cableada tradicional. Estos sistemas inalámbricos, diseñados y construidos utilizando microprocesadores y circuitos digitales estándar, se conectan a sistemas LAN cableados tradicionales. Además, los dispositivos inalámbricos deben recibir alimentación que les proporcionen energía para codificar, decodificar, comprimir, descomprimir, transmitir y recibir señales inalámbricas.

Los dispositivos WLAN de primera generación, con sus bajas velocidades y falta de estándares, no fueron populares. Los sistemas estandarizados modernos pueden ahora transferir datos a velocidades aceptables. El comité IEEE 802.11 y la Alianza Wi-Fi han trabajado diligentemente para hacer al equipo inalámbrico estandarizado e interoperable. La Figura 1 enumera algunas de las funciones importantes de estas dos organizaciones

IEEE 802.11
<ul style="list-style-type: none"> • Design specifications for high performance WLANs • Wireless Security, Interoperability, Quality of Service (QoS)
Wi-Fi Certification by the Wi-Fi Alliance:
<ul style="list-style-type: none"> • Ensures user level interoperability: the products of all vendors should work together. • Successful testing earns a "seal of approval." • Cisco is a founding member.

Figura 1

La tecnología inalámbrica soportará ahora las tasas de datos y la interoperabilidad necesarias para la operación de la LAN. Además, el costo de los nuevos dispositivos inalámbricos ha disminuido mucho. Las WLANs son ahora una opción costeable para la conectividad LAN. En la mayoría de los países estos dispositivos no requieren licencia gubernamental.

1.1.3 ¿Por qué utilizar tecnología inalámbrica?

Las LANs Ethernet cableadas actuales operan a velocidades de alrededor de 100 Mbps en la capa de acceso, 1 Gbps en la capa de distribución, y hasta 10 Gbps a nivel de la capa principal. La mayoría de las WLANs operan a una velocidad de 11 Mbps a 54 Mbps en la capa de acceso y no tienen como objetivo operar en la capa de distribución o en la capa principal. El costo de implementar WLANs compite con el de las LANs cableadas. Por lo tanto, ¿por qué instalar un sistema que se encuentra en el extremo más bajo de las capacidades de ancho de banda actuales? Una razón es que en muchos entornos LAN pequeños, las velocidades más lentas son adecuadas para soportar las necesidades de las aplicaciones y del usuario. Con muchas oficinas conectadas ahora a la Internet por medio de servicios de banda ancha como DSL o cable, las WLANs pueden manejar las demandas de ancho de banda. Otra razón es que las WLANs permiten a los usuarios movilizarse dentro de un área definida con libertad y aún así permanecer conectados. Durante las reconfiguraciones de oficina, las WLANs no requieren un recableado ni sus costos asociados. La Figura 1 enumera muchos de los beneficios proporcionados por las WLANs.

Modern WLANs offer many benefits to networking

Benefits of WLANs

- Mobility
- Scalability
- Flexibility
- Short and long term cost savings
- Installation advantages
- Reliability in harsh environments
- Reduced installation time

Figura 1

Las WLANs presentan numerosos beneficios para las oficinas hogareñas, los negocios pequeños, los negocios medianos, las redes de campus y las corporaciones más grandes. Los entornos que es probable que se beneficien de una WLAN tienen las siguientes características:

- Requieren las velocidades de una LAN Ethernet estándar
- Se benefician de los usuarios móviles
- Reconfiguran la disposición física de la oficina a menudo
- Se expanden rápidamente
- Utilizan una conexión a Internet de banda ancha
- Enfrentan dificultades significativas al instalar LANs cableadas
- Necesitan conexiones entre dos o más LANs en un área metropolitana
- Requieren oficinas y LANs temporales

La Figura 2 proporciona ejemplos adicionales de situaciones en las cuales una WLAN sería beneficiosa.

The value-added features of modern WLANs

WLANs provide value-added features for the following:

- IT professionals or business executives who want mobility within the enterprise, perhaps in addition to a traditional wired network
- Business owners or IT directors who need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas
- Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space, or temporary sites
- Any company that needs the flexibility and cost savings offered by a line-of-sight, building-to-building bridge, that avoids expensive trenches, leased lines, and right-of-way issues

Figura 2

Las WLANs no eliminan la necesidad de la existencia de los Proveedores de Servicios de Internet (ISPs). La conectividad a Internet aún requiere de acuerdos de servicios con portadoras de intercambio locales o ISPs para un acceso a la Internet. Existe una tendencia actual para que los ISPs proporcionen un servicio de Internet inalámbrico. Estos ISPs se denominan Proveedores de Servicios de Internet Inalámbricos (WISPs). Además, las WLANs no reemplazan la necesidad de los routers, switches y servidores cableados tradicionales de una LAN típica.

Incluso aunque las WLANs han sido diseñadas principalmente como dispositivos LAN, pueden utilizarse para proporcionar una conectividad de sitio a sitio a distancias de hasta 40 km (25 millas). El uso de dispositivos de WLAN es mucho más eficaz en costos que el uso del ancho de banda WAN o la instalación o arrendamiento de largas trayectorias de fibra. Por ejemplo, para instalar una WLAN entre dos edificios se incurrirá en un costo único de varios miles de dólares estadounidenses. Un enlace T1 arrendado dedicado, que sólo proporciona una fracción del ancho de banda de una WLAN, fácilmente costará cientos de dólares estadounidenses por mes o más. Instalar fibra a través de una distancia de más de 1,6 km (1 milla) es difícil y costaría mucho más que una solución inalámbrica.

1.1.4 La evolución de las LANs inalámbricas

Las primeras tecnologías LAN inalámbricas definidas mediante el estándar 802.11 eran ofertas propietarias de baja velocidad de 1 a 2 Mbps. A pesar de estos inconvenientes, la libertad y flexibilidad de las tecnologías inalámbricas permitieron a estos primeros productos encontrar su lugar en los mercados tecnológicos. Los trabajadores móviles utilizaban dispositivos portátiles para la administración de inventarios y la recolección de datos en ventas al por menor y almacenamiento. Posteriormente, los hospitales aplicaron la tecnología inalámbrica para reunir y entregar información acerca de los pacientes. A medida que las computadoras se abrían paso hacia las aulas, las escuelas y universidades comenzaron a instalar redes inalámbricas para evitar costos de cableado, a la vez que habilitaban un acceso compartido a la Internet. Al darse cuenta de la necesidad de un estándar similar a Ethernet, los fabricantes de tecnologías inalámbricas se aliaron en 1991 y formaron la Alianza de Compatibilidad de Ethernet Inalámbrica (WECA). La WECA propuso y construyó un estándar basado en tecnologías contribuyentes. WECA cambió posteriormente su nombre a Wi-Fi. En junio de 1997 IEEE lanzó el estándar 802.11 para el networking de área local inalámbrico. La Figura 1 ilustra la evolución en las LANs inalámbricas.

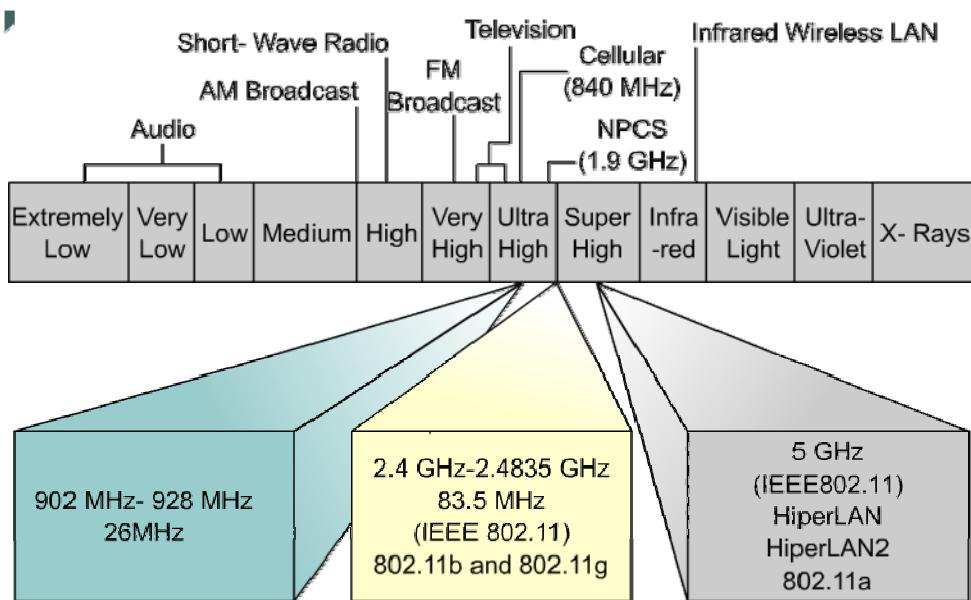
Speed	860 Kbps	1 and 2 Mbps	11 Mbps	54 Mbps
Network	Proprietary		Standards-Based	
Analog Radio	900 MHz	2.4 GHz		5 GHz
		IEEE 802.11 begins drafting	802.11 ratified	802.11a,b ratified
			802.11g drafted	
	1986	1988	1990	1992
			1994	1996
			1998	2000
			2002	

Figura 1

Así como el estándar de Ethernet 802.3 permite la transmisión de datos a través de par trenzado y cable coaxial, el estándar de WLAN 802.11 permite la transmisión a través de medios diferentes. Los medios especificados incluyen los siguientes:

- Luz infrarroja
- Tres tipos de transmisión de radio dentro de las bandas de frecuencia de 2,4 GHz no licenciadas:
 - Espectro expandido de saltos de frecuencia (FHSS)
 - Espectro expandido de secuencia directa (DSSS)
 - Multiplexado por división de frecuencia ortogonal (OFDM) 802.11g
- Un tipo de transmisión de radio dentro de las bandas de frecuencia de 5 GHz no licenciadas:
 - Multiplexado por división de frecuencia ortogonal (OFDM) 802.11a

El espectro expandido es una técnica de modulación que se desarrolló en los años cuarenta. Expande una señal de transmisión a través de un amplio rango de frecuencias de radio. Esta técnica es ideal para las comunicaciones de datos porque es menos susceptible al ruido de radio y crea menos interferencia.



El futuro del networking de área local inalámbrico

Las tecnologías WLAN actuales ofrecen velocidades de datos en rápido incremento, una mayor confiabilidad, y menores costos. Las tasas de datos se han incrementado de 1 Mbps a 54 Mbps, la interoperabilidad se ha convertido en una realidad con la introducción de la familia de estándares IEEE 802.11, y los precios han disminuido mucho. A medida que las WLANs se hacen más populares, los fabricantes pueden cada vez más hacer hincapié en la economía a gran escala.

Hay muchas mejoras por venir. Por ejemplo, se han hallado muchas debilidades en las configuraciones de seguridad básicas de las WLANs, y una seguridad más fuerte en todos los productos futuros es una prioridad. Versiones tales como 802.11g ofrecerán 54 Mbps como 802.11a, pero también serán compatibles con 802.11b.

Este curso tratará las tecnologías generales detrás de las WLANs 802.11a y 802.11b, incluyendo las tecnologías de radio, el diseño de una WLAN, la preparación del sitio y la teoría de la antena. También se presentará una cobertura detallada de los productos y accesorios Cisco Aironet. Los alumnos deberán poder aplicar su conocimiento una vez completo el curso para diseñar WLANs utilizando productos de uno o múltiples fabricantes.

1.2 Medios de Networking

1.2.1 Medios de la capa física

Para construir una LAN cableada o inalámbrica debe utilizarse una base sólida. Como lo muestra la Figura 1, esta base se denomina Capa 1 o capa física en el modelo de referencia OSI. La capa física es la capa que define las especificaciones eléctricas, mecánicas, procedimentales y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Esta sección presenta diferentes tipos de medios de networking que se utilizan en la capa física, incluyendo:

- cable de par trenzado blindado
- cable de par trenzado sin blindaje
- cable coaxial
- cable de fibra óptica
- ondas de radio propagadas

Las ondas de radio son el medio utilizado por las tecnologías inalámbricas.

Al diseñar y construir redes, es importante cumplir con todos los códigos de incendio, códigos edilicios y estándares de seguridad aplicables. Deberán seguirse los estándares de desempeño establecidos para asegurar una óptima operación en la red. A causa de la amplia variedad de opciones actualmente disponibles en medios de networking, también deberán considerarse la compatibilidad y la interoperabilidad.

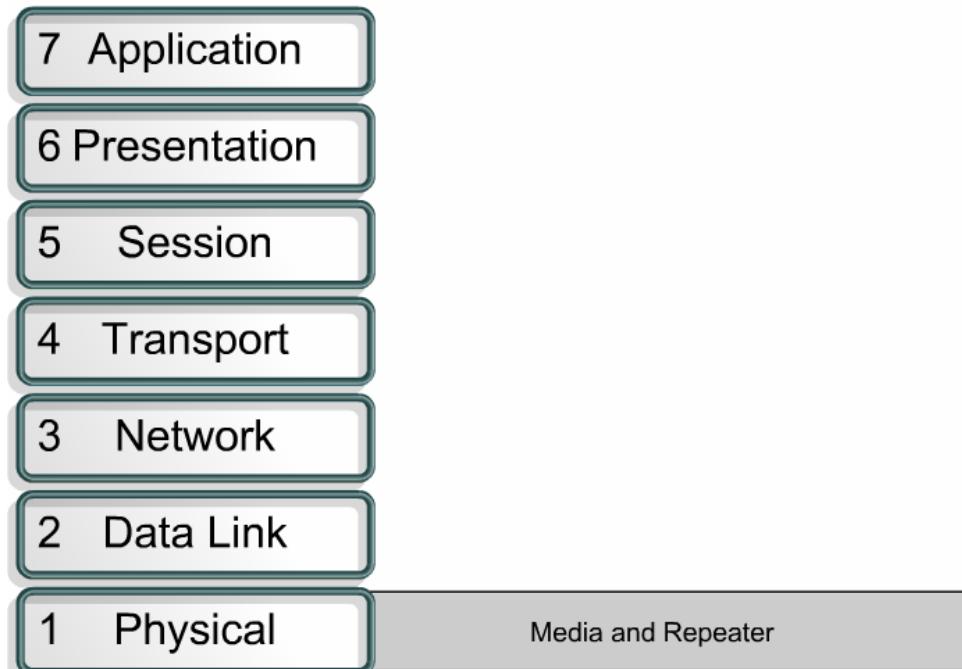


Figura 1

1.2.2 STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje y trenzado de los alambres. El cableado STP se muestra en la Figura 1. Cada par de alambres es trenzado y luego envuelto en una lámina metálica. Los cuatro pares de alambres se envuelven en una malla o lámina metálica que lo cubre todo. STP usualmente es un cable de 150 ohms. Según se lo especifica en las instalaciones de red Ethernet, STP reduce el ruido eléctrico. Éste incluye el acoplamiento de par a par, o diafonía, desde el interior del cable, y la interferencia electromagnética (EMI) y la interferencia de frecuencia de radio (RFI) desde el exterior del cable. El cable STP debe seguir especificaciones precisas respecto a la cantidad de trenzados existentes cada 30 cm (1 pie) de cable. El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado sin blindaje (UTP). Un STP instalado apropiadamente ofrece una mayor protección contra todos los tipos de interferencia externa, pero es más caro y difícil de instalar que el UTP.

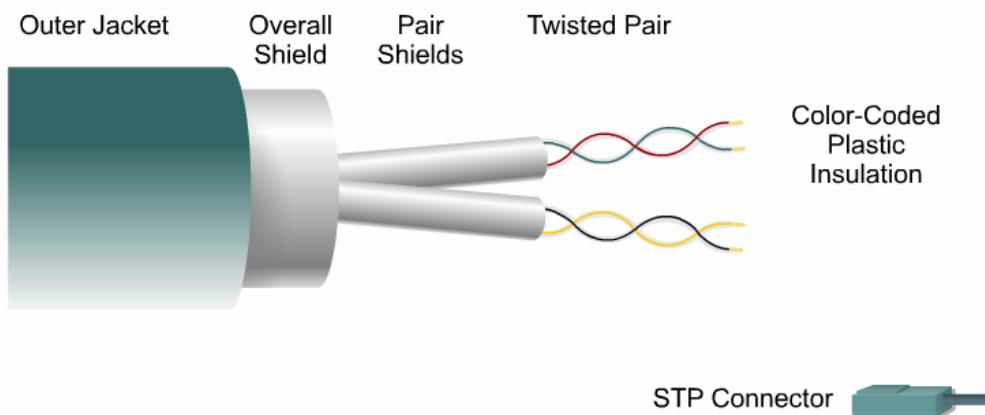


Figura 1

Un híbrido entre UTP y STP es UTP protegido (ScTP), también denominado par trenzado con lámina (FTP), o pares en lámina metálica (PiMF). Éste se muestra en la Figura 2. ScTP es esencialmente UTP envuelto en un blindaje de lámina metálica, o protección. Usualmente es un cable de 100 ohms.

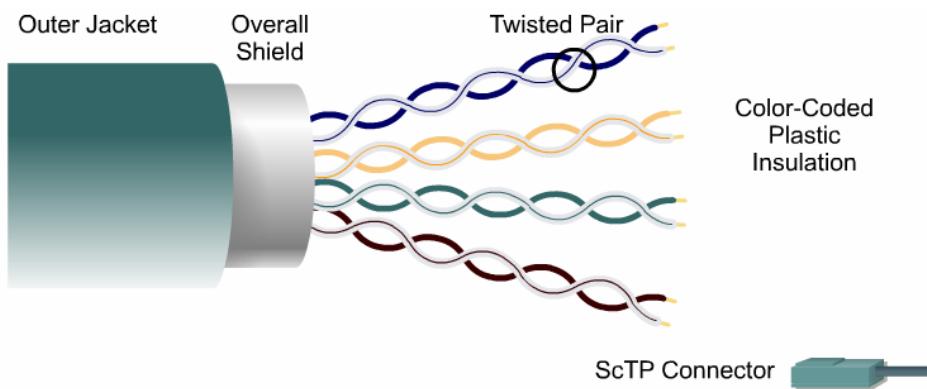


Figura 2

Si se los conecta a tierra inapropiadamente, o si existe alguna discontinuidad a lo largo de la longitud del material del blindaje, (por ejemplo, debido a una instalación pobre) STP y ScTP se vuelven susceptibles a importantes problemas de ruido. Esto se debe a que los problemas de ruido hacen que el blindaje actúe como una antena, recogiendo señales no deseadas. Este efecto funciona de dos maneras. La lámina no sólo evita que ondas electromagnéticas entrantes ocasionen ruido en los alambres de datos, sino que también minimiza las ondas electromagnéticas irradiadas, lo cual podría ocasionar ruido en otros dispositivos. Los cables STP y ScTP no pueden tenderse tan lejos como otros medios de networking, como el cable coaxial o la fibra óptica, sin que la señal se repita. Además, más aislación y blindaje se combinan para incrementar considerablemente el tamaño, el peso y el costo de los cables. Los materiales de blindaje hacen a las terminaciones más difíciles y susceptibles a una mano de obra pobre. A pesar de sus desventajas, los cables STP y ScTP aún son útiles en entornos altamente eléctricos o con ruido de RF, como cerca de la instalación de radar de un aeropuerto. Estos cables también son populares en Europa.

1.2.3 UTP

El cable de par trenzado sin blindaje (UTP) es un medio de cuatro pares de alambres utilizado en una variedad de redes. [1](#). Los ocho alambres de cobre individuales del cable UTP están recubiertos por material aislante. Dos alambres se trenzan entre sí para formar pares. Este tipo de cable se basa en el efecto de cancelación, producido por los pares de alambres trenzados, para limitar la degradación de la señal ocasionada por la diafonía y la EMI y RFI externas. Para reducir aún más la diafonía entre pares en el cable UTP, se incrementa la cantidad de trenzados de los pares de alambres. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas respecto a cuántos trenzados existen cada 30 cm (1 pie) de cable.

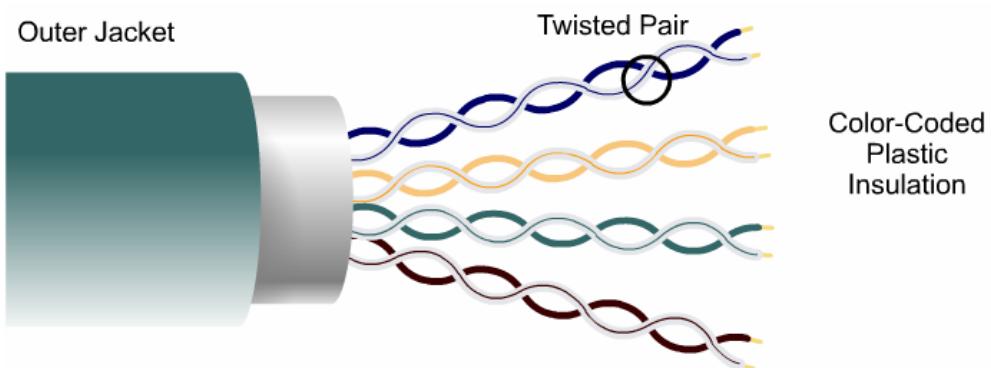


Figura 1

Los cuatro pares utilizados en el cable UTP para networking son usualmente alambres de cobre con un Calibre de Alambres Norteamericano (AWG) número 22 ó 24. Esto lo diferencia del par trenzado utilizado para el cableado telefónico, que es de usualmente 19, 22, 24, o 26 AWG. Puesto que UTP tiene un diámetro externo de aproximadamente 0,64 cm (0,25 pulgadas), su pequeño tamaño puede resultar ventajoso durante la instalación. Puesto que UTP puede utilizarse con las más importantes arquitecturas de networking, continúa creciendo en popularidad.

El cable UTP tiene muchas ventajas. Es fácil de instalar y es menos caro que otros tipos de medios de networking. Puesto que tiene un diámetro externo pequeño, UTP no llena los conductos de cableado tan rápidamente como otros tipos de cable, a excepción del cable de fibra óptica, que es el más costoso de adquirir e instalar. Éste puede ser un factor extremadamente importante a considerar, particularmente al

instalar una red en un edificio antiguo. Otra ventaja del UTP está relacionada con la topología en estrella basada en el hub o basada en el switch que se utiliza en las LANs Ethernet cableadas con UTP . Resulta mucho más fácil detectar problemas en esta topología que en la topología de bus de las LANs cableadas con coaxial.

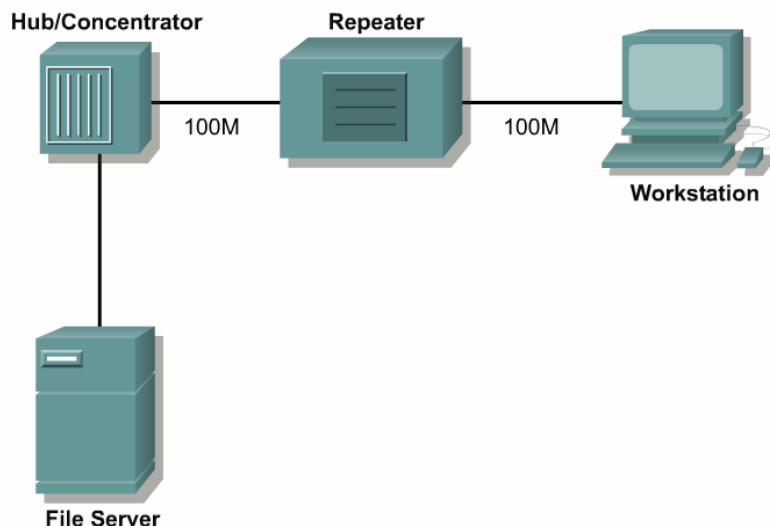


Figura 2

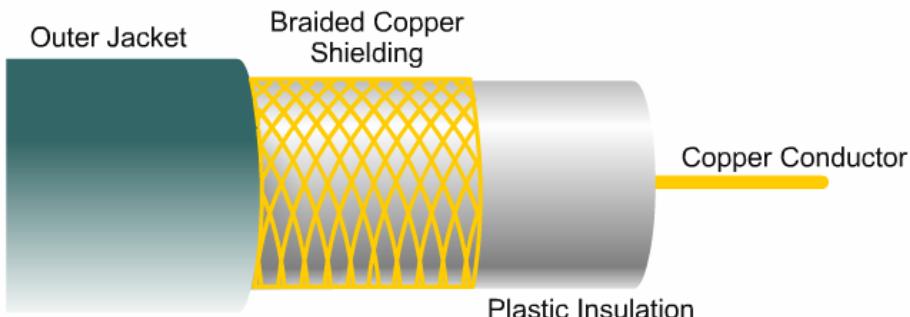
También hay desventajas en el uso de cableado UTP. El cable UTP es más proclive al ruido eléctrico y a la interferencia que otros tipos de medios de networking, y la distancia entre potenciamientos de la señal es más corta para UTP que lo que lo es para los cables coaxiales y de fibra óptica.

UTP se consideraba más lento en la transmisión de datos que otros tipos de cable. UTP puede alcanzar actualmente velocidades de transmisión de hasta 1000 Mbps (1 Gbps). Se está considerando un estándar de 10 Gbps.

1.2.4 Cable coaxial

El cable coaxial consiste en un conductor central, ya sea en hebras o sólido, que está rodeado por una capa de material aislante llamado dieléctrico. El dieléctrico está rodeado por un blindaje hecho de papel de aluminio, hebras de alambre trenzado, o ambos. Fuera de este blindaje hay una vaina de aislación protectora que forma la funda del cable.

Todos los elementos del cable coaxial rodean al conductor central, como los anillos de crecimiento de un árbol rodean al núcleo. Puesto que todos comparten el mismo eje, esta construcción se denomina coaxial, o abreviado, coax. El coax es el medio más ampliamente utilizado para transportar elevadas frecuencias de radio a través del alambre, especialmente señales de televisión por cable. Los cables que conducen a las antenas más externas son de coax. Los cables de video que conectan una VCR a una TV son de coax. En la mayoría de las instalaciones de producción de video se encuentran kilómetros de coax.



En el pasado, el cable coaxial ofrecía ventajas significativas para las LANs. Su respuesta de frecuencia le permitía transportar señales con menor degradación a través de distancias más largas que los medios de par trenzado disponibles en el momento. Técnicas de fabricación mejoradas y una mejor electrónica han hecho desde hace tiempo del par trenzado o de las fibras ópticas la opción preferida para el cableado de red.

Originalmente, las LANs Ethernet utilizaban un grueso cable coaxial que tenía 1,27 cm (0,5 pulgadas) de diámetro. La industria comenzó a referirse a este cable como Thicknet. Era difícil trabajar con el gran coax

utilizado para las redes de la era 10Base5 y requería gran cuidado para evitar dobleces y torceduras. Cuando se estandarizó Ethernet, Thicknet se convirtió en IEEE 802.3 10Base5.

Posteriormente, el comité 802.3 estandarizó 10Base2, una versión que utilizaba un cable coaxial mucho más delgado, con un diámetro exterior de sólo 0,635 cm (0,25 pulgadas). 10Base2 se denomina en ocasiones Thinnet. A causa de su bajo costo y facilidad de instalación, también se denomina en ocasiones cheapernet.

Consideraciones respecto a la conexión a tierra

Debe tenerse un especial cuidado en asegurarse de que los cables coaxiales estén siempre apropiadamente conectados a tierra. En networking, una conexión a tierra correcta significa que el cable queda sin conexión a tierra en uno de sus extremos. En la mayoría de las otras aplicaciones es importante asegurarse de que exista una sólida conexión eléctrica a ambos extremos del cable. El no observar una conexión a tierra apropiada puede resultar en que corrientes errantes fluyan por el blindaje del coax. Esto puede resultar en una interferencia electromagnética y posiblemente incluso en la corrupción de paquetes de datos hasta el punto de que la red se vuelva inutilizable. También podría crear un riesgo de choque eléctrico.

1.2.5 Fibra óptica

El cable de fibra óptica es un medio de networking que utiliza transmisiones de luz modulada. Puede ser más costoso que otros medios de networking, dependiendo de la pureza y del tamaño de la fibra utilizada. Los conectores que terminan la fibra también tienden a ser más costosos. La fibra no es susceptible a la interferencia electromagnética o de frecuencia de radio. Es capaz de velocidades de datos más elevadas que cualquiera de los otros tipos de medios de networking actuales. A medida que el diámetro de la fibra se hace más pequeño, se incrementa la velocidad de transmisión máxima.

Los datos que viajan por el cable de fibra óptica se convierten en impulsos luminosos y se permite a esta luz propagarse por la fibra.

Según lo ilustra la Figura 1, las partes que guían la luz de una fibra óptica se denominan núcleo y revestimiento. El núcleo es usualmente vidrio muy puro. Cuando una capa de revestimiento de vidrio o plástico con un índice de refracción más bajo rodea al vidrio del núcleo, la luz puede quedar atrapada en el núcleo de la fibra. Este proceso se denomina reflexión total interna, y permite a la fibra óptica actuar como un conducto luminoso que guía a la luz a través de tremendas distancias, incluso en curvas.

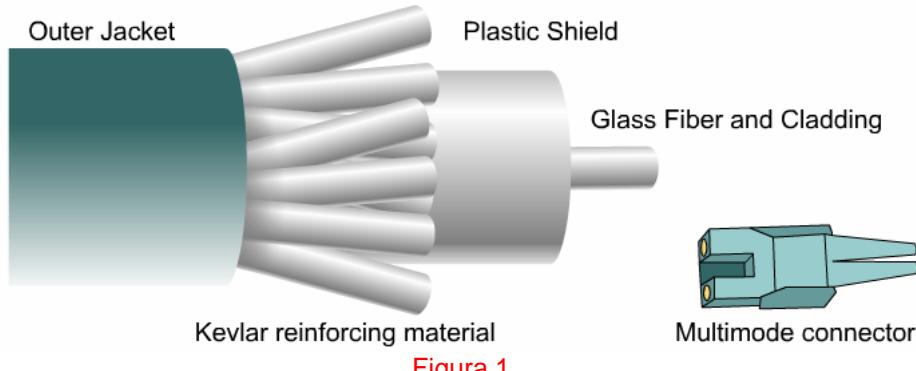


Figura 1

La comunicación de fibra óptica se basa en cierta cantidad de invenciones del siglo diecinueve. No fue hasta los '60, con la introducción de las fuentes de luz láser de estado sólido y los vidrios de alta calidad y libres de impurezas, que se pusieron en práctica las comunicaciones de fibra óptica. Las compañías telefónicas, que vieron sus beneficios para las comunicaciones a larga distancia, fueron pioneras en su uso difundido.

1.2.6 Atmósfera: los medios inalámbricos

Las señales inalámbricas son ondas electromagnéticas, que pueden viajar a través del espacio. Ningún medio físico es necesario para las señales inalámbricas, que viajan tan bien en el vacío del espacio como lo hacen a través del aire en un edificio de oficinas. La capacidad de las ondas de radio de atravesar las paredes y abarcar grandes distancias convierten a la tecnología inalámbrica en una forma versátil de construir una red. La Figura 1 muestra tecnologías y funciones inalámbricas. La Figura 2 representa una onda electromagnética.

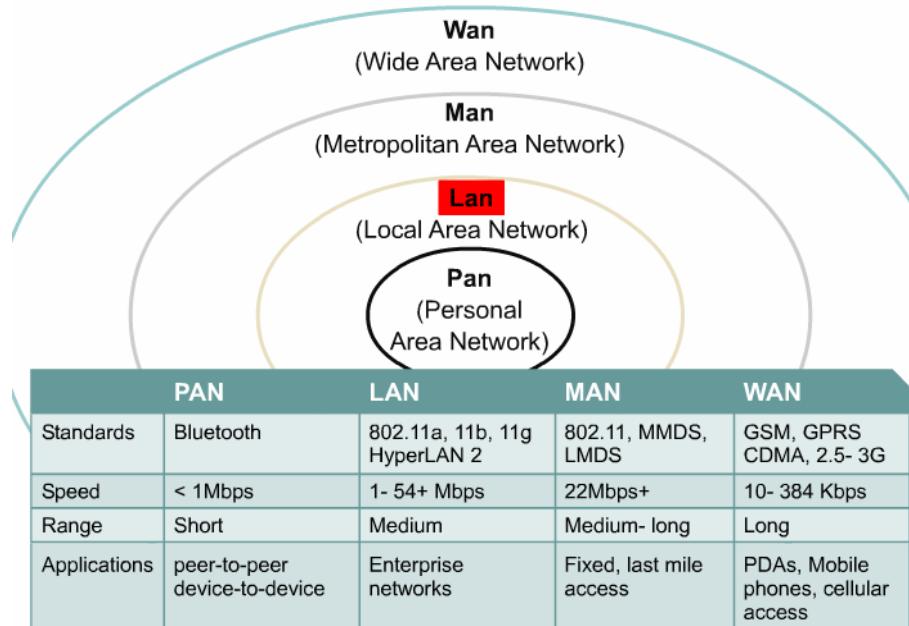


Figura 1

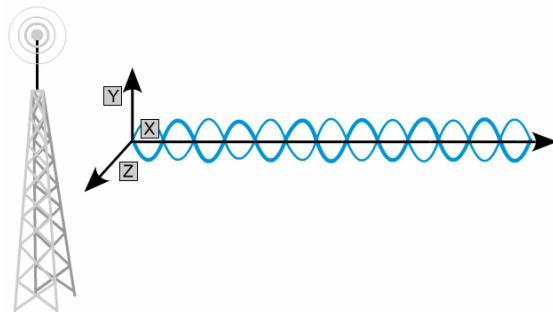


Figura 2

Las ondas difieren sólo en su frecuencia. Las ondas de energía, ondas de radio, microondas, ondas de luz infrarroja, ondas de luz visible, ondas de luz ultravioleta, rayos x, y rayos gamma proporcionan algunas características muy importantes:

- Todas estas ondas tienen un patrón de energía similar al representado en la Figura 2.
- Todas estas ondas viajan a la velocidad de la luz, $c = 299.792.458$ metros por segundo, en el vacío. Esta velocidad podría denominarse con más precisión velocidad de las ondas electromagnéticas.
- Todas estas ondas obedecen a la ecuación (frecuencia) \times (longitud de onda) = c .
- Todas estas ondas viajarán a través del vacío. No obstante, tienen interacciones muy diferentes con diversos materiales.
- La diferencia principal entre las diferentes ondas electromagnéticas es su frecuencia. Ondas electromagnéticas de baja frecuencia tienen una longitud de onda larga, mientras que las ondas electromagnéticas de alta frecuencia tienen una longitud de onda corta. La longitud de onda representa la distancia de un pico al siguiente en la onda sinusoidal.

Aplicaciones inalámbricas

Una aplicación común de comunicación de datos inalámbrica es el uso móvil. Algunos ejemplos de uso móvil incluyen los siguientes:

- Comunicaciones persona a persona desde automóviles o aviones en movimiento
- Transmisiones de comunicación satelital
- Señales de telemetría a sondas espaciales remotas
- Enlaces de comunicación a transbordadores espaciales y estaciones espaciales
- Comunicaciones sin basarse en cobre o hebras de fibra óptica
- Comunicaciones de cualquiera a cualquiera para intercambiar datos en la red

1.2.7 Instalación de los medios

Es importante calcular todos los costos involucrados al diseñar redes. El impacto del diseño y la construcción del edificio deben considerarse al instalar medios LAN. Algunos factores importantes a considerar incluyen la calefacción, ventilación y acondicionamiento de aire (HVAC), el agua, los desagües cloacales, la iluminación y los sistemas eléctricos existentes. Los materiales estructurales como el yeso, el cemento armado, la madera y el acero, así como los códigos de incendios, deben considerarse también. Muchas paredes representan un papel estructural y de contención de incendios, y no pueden perforarse sin seguir pasos especiales para restaurar su integridad.

Las LANs se convertirán rápidamente en una combinación de sistemas cableados e inalámbricos, dependiendo de las necesidades de la red y de las restricciones de diseño. En redes empresariales más grandes, las capas principal y de distribución continuarán siendo sistemas de backbone cableados, conectados en general por medio de fibra óptica y cables UTP. La capa más cercana al usuario final, la capa de acceso, será la más afectada por la implementación de la tecnología inalámbrica.

Enlaces inalámbricos de edificio a edificio

Las conexiones de edificio a edificio se llevan a cabo en general utilizando fibra óptica, a causa de las altas velocidades disponibles y para evitar medidas de protección de conexión a tierra que se requieren en los medios de cobre. Instalar cable de fibra óptica entre edificios es muy costoso y consume mucho tiempo. Incluso cortas distancias son difíciles de cubrir debido a utilidades subterráneas existentes, cemento armado y otros obstáculos estructurales. Una instalación aérea sujetada con cuerdas es una opción de instalación alternativa. Las WLANs se han convertido actualmente en una opción popular puesto que la instalación se limita a construir antenas montadas. ¿Qué sucedería si utilizáramos conexiones de edificio a edificio allí donde las distancias excedieran los límites de una propiedad o las limitaciones de cableado? La mayoría de los negocios utilizan una conectividad WAN entre sitios metropolitanos distantes. Algunos negocios utilizan microondas entre sitios distantes. En el caso de los bridges LAN inalámbricos, los edificios que se encuentran a hasta 32 km (20 millas) de distancia pueden conectarse a velocidades de hasta 11 Mbps.

En general, cuanto mayor es la distancia entre edificios, más alto es el costo de la instalación LAN inalámbrica. Las antenas estándar rubber ducky no serán adecuadas. Se requieren torres y antenas de elevada ganancia. Las torres pueden resultar costosas, dependiendo de la altura y los requisitos de la construcción. El costo inicial puede recuperarse dentro del primer año. Se generan ganancias provenientes de un incremento en la productividad utilizando más elevado ancho de banda y tarifas de líneas arrendadas mensuales discontinuas.

Los bridges inalámbricos Cisco ofrecen muchas ventajas sobre conexiones alternativas más costosas. Por ejemplo, una línea T-I cuesta en general aproximadamente 400 a 1000 dólares estadounidenses por mes. Para un sitio con cuatro edificios, eso significaría alrededor de 15.000 a 36.000 dólares estadounidenses al año. Con un sistema inalámbrico, la recuperación de los costos de hardware podría tener lugar realmente en menos de un año.

Si una línea T-I no está disponible o los edificios están ubicados en la misma propiedad, podría colocarse un cable subterráneo. No obstante, la introducción en la tierra puede costar más de 100 dólares estadounidenses por cada 0,3 m (1 pie), dependiendo de la tarea. Para conectar tres edificios ubicados a 305 m (1000 pies) separados entre sí, el costo podría exceder los 200.000 dólares estadounidenses.

Las microondas son una solución posible. En el caso de las microondas se requiere usualmente un permiso del gobierno. En Estados Unidos, éste se obtiene de la Comisión Federal de Comunicaciones (FCC). Este permiso sirve como proceso de registro que permite al dueño del permiso tomar acciones legales contra aquéllos que interfieran. El costo del equipamiento es en general de más de 10.000 dólares estadounidenses por sitio, lo cual no incluye el costo de los elementos de instalación. El desempeño puede verse severamente degradado en el caso de niebla espesa, lluvia o nieve. Las microondas también tienden a ser punto a punto. Las conexiones multipunto usualmente no son posibles.

Independientemente de si son cableadas o inalámbricas, las redes modernas deben poder manipular un ancho de banda más elevado, más aplicaciones y una mayor movilidad. Se requieren combinaciones de tecnologías cableadas e inalámbricas para proporcionar las soluciones. El diseñador de redes es responsable de proporcionar el diseño más eficaz en materia de costos y la solución que cumpla con o exceda las necesidades de la organización.

El diseño, la preparación y el sondeo del sitio se tratarán en detalle posteriormente en el curso. Debe completarse un sondeo del sitio antes de tomar las decisiones de implementación. Por ejemplo, los planes

iniciales pueden incluir una solución inalámbrica, pero el sondeo del sitio podría indicar que la tecnología inalámbrica sería ineficaz. Inversamente, una solución cableada puede planificarse inicialmente y el sondeo final puede probar que la solución inalámbrica resultaba una mejor opción.

1.3 Tecnologías Inalámbricas

1.3.1 Descripción general

Las WLANs son sólo uno de los usos del espectro de frecuencia de radio (RF). La Figura 1 ilustra las relaciones de distancia versus velocidad de datos que existen en diferentes tecnologías inalámbricas. La Figura 2 enumera las diferentes bandas de frecuencia de radio, junto con el nombre de las ondas transmitidas en cada banda y sus tipos de usos. Una multitud de tecnologías diferentes y complejas llenan el espectro de frecuencia y no pueden abarcarse completamente en este curso.

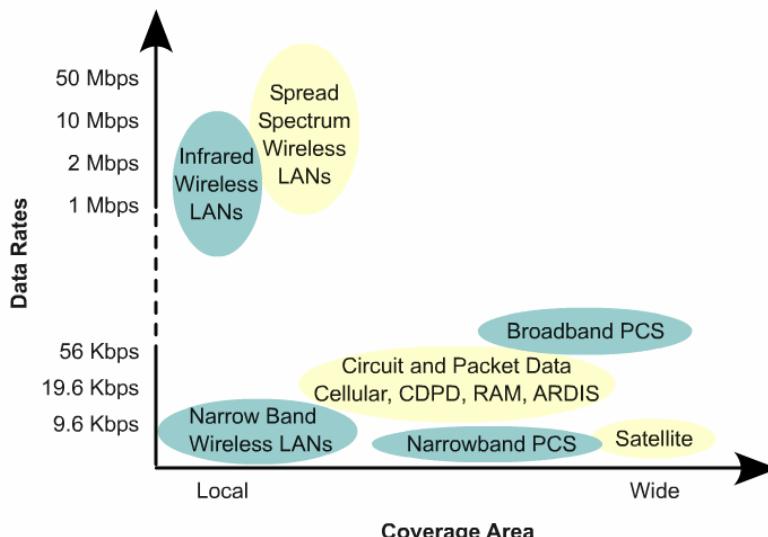


Figura 1

Frequency Band Designation, Use and Propogation	
3- 30 KHz	Very low frequency (VLF): Called surface waves, these frequencies are used worldwide for long-distance communications.
30- 300 KHz	Low frequency (LF): Called ground waves, these frequencies are used for long distance communication and long-wave broadcasting.
300- 3000 KHz	Medium frequency (MF): Also called ground waves, these frequencies are used in medium wave broadcasting.
3- 30 MHz	High frequency (HF): Called sky waves, these frequencies are used for long distance communication and short-wave broadcasting.
30- 300 MHz	Very high frequency (VHF): Called space waves, these frequencies are used for short range, mobile communications, and sound broadcasting.
300- 3000 MHz	Ultra high frequency (UHF): Also called space waves, these frequencies are used for short range, television broadcasting, and point-to-point links.
3- 30 GHz	Super high frequency (SHF): Also called space waves, these frequencies are used for point-to-point links, radar, and satellite communications.
Above 30 GHz	Extra high frequency (EHF): Also called space waves, these frequencies are used for inter-satellite and micro-cellular radio telephony.

Figura 2

La definición de radio de la Administración de Servicios Generales de EE.UU. es la siguiente:

1. Tele comunicación por medio de modulación e irradiación de ondas electromagnéticas
2. Un transmisor, receptor o transceptor utilizado para la comunicación a través de ondas electromagnéticas
3. Un término general aplicado al uso de ondas de radio

Las tecnologías inalámbricas se componen de muchos parámetros variables, como los que se enumeran en la Figura 3. Algunas tecnologías proporcionan comunicaciones en un solo sentido mientras que otras proporcionan comunicaciones simultáneas en dos sentidos. Algunas operan a niveles de baja energía, mientras que otros operan a niveles de energía altos. Algunos son digitales y otros son analógicos. Algunos operan a distancias cortas de 30,5 m (100 pies) o menos, y otros operan a mayores distancias, incluso a través de continentes. El costo de las diversas tecnologías inalámbricas puede variar de varios dólares estadounidenses a billones de dólares estadounidenses.

Frequency	Low (Hz) - High (GHz)
Power Level	Low (<1mW) - High (>100,000W)
Bandwidth	Narrowband - Wideband
Dialog	Simplex - Full duplex
Signal Range	Short (< 30.5 m or 100 ft) - Long (thousands of miles)
Signal Type	Digital or Analog
Signal Path	Direct or Reflective
Applications	Fixed or Mobile
Coverage	Local or Wide area
Data Rates	Low (Kbps) - High (>10Mbps)
Cost	Inexpensive (<\$20 U.S.) - Expensive (>\$1B U.S.)

Figura 3

Las tecnologías inalámbricas, algunas de las cuales se muestran en la Figura 4, han estado en circulación durante muchos años. La televisión, la radio AM/FM, la televisión satelital, los teléfonos celulares, los dispositivos de control remoto, el radar, los sistemas de alarmas, las radios climáticas, las CBs, y los teléfonos inalámbricos están integrados a la vida cotidiana. Las tecnologías beneficiosas que dependen de la tecnología inalámbrica incluyen sistemas de radares climáticos, rayos x, Imágenes de Resonancia Magnética (MRIs), hornos a microondas, y Satélites de Posicionamiento Global (GPSs). La tecnología inalámbrica rodea a la humanidad diariamente, en los negocios y en la vida personal.

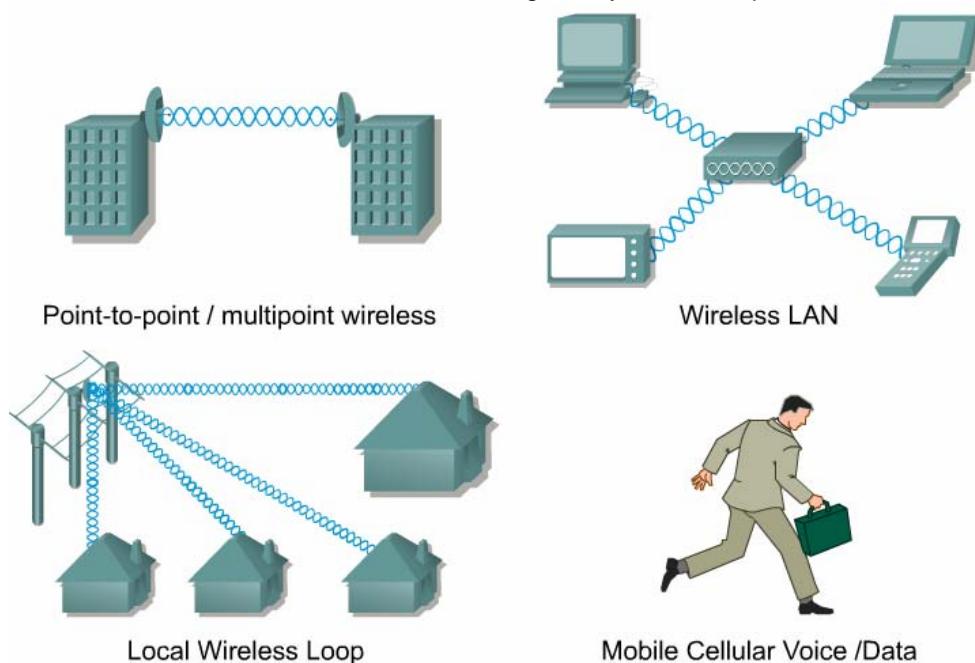


Figura 4

1.3.2 Tecnología inalámbrica digital y celular

La tecnología inalámbrica digital y celular data de los '40, cuando comenzó la telefonía móvil comercial. La revolución inalámbrica comenzó después de que los microprocesadores de bajo costo y la conmutación digital se hicieron disponibles, y el clima regulador cambió para permitir un mejor control del equipamiento de transmisión de radio.

Radio celular

La radio celular proporciona un servicio de telefonía móvil empleando una red de sitios célula distribuidos a través de un área amplia. Un sitio célula contiene un transceptor de radio y un controlador de estación de base. La estación de base administra, transmite y recibe tráfico proveniente de las radios móviles de su área geográfica. Un sitio célula también tiene una torre y antenas, así como un enlace a un switch distante, que se denomina oficina de conmutación de telecomunicaciones móviles (MTSO). La MTSO conecta llamadas de teléfonos basados en tierra a clientes inalámbricos, conmuta llamados entre células a medida que los móviles viajan a través de fronteras de células, y autentica a los clientes inalámbricos antes de que hagan llamadas.

Las redes celulares utilizan un principio llamado reutilización de la frecuencia para incrementar en gran medida la cantidad de clientes servidos. La reutilización de la frecuencia se muestra en la Figura 1. Las radios móviles de baja energía y el equipamiento de radio en cada sitio célula permite que las mismas frecuencias de radio sean reutilizadas en células diferentes, no contiguas, multiplicando así la capacidad sin crear interferencia. Este método eficiente en cuanto al espectro contrasta claramente con los sistemas móviles más antiguos que utilizaban un transmisor de alta potencia, localizado centralmente para comunicarse con móviles montados en automóviles de elevada energía en una pequeña cantidad de frecuencias. Los canales se utilizaban y no se reutilizaban a través de un área amplia.

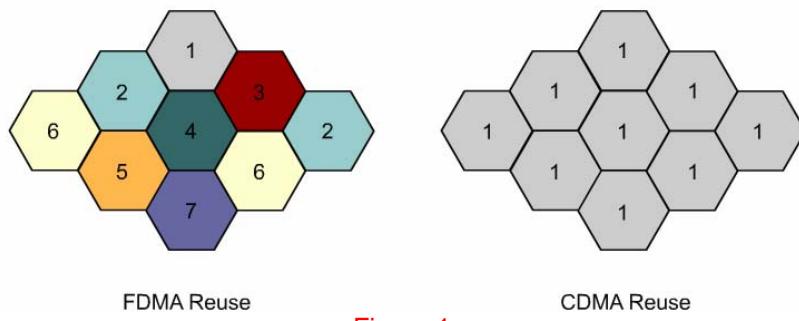


Figura 1

Rutinas de señalización complejas manejan las ubicaciones de llamadas, solicitudes de llamadas, transferencias de llamadas de una célula a otra, que se denominan transferencias, y roaming, que tiene lugar cuando un usuario se desplaza desde un área portadora a otra área portadora. Diferentes sistemas de radio celular utilizan las técnicas acceso múltiple por división de frecuencia (FDMA) analógica, acceso múltiple por división de tiempo (TDMA), y acceso múltiple por división de código (CDMA) de espectro expandido.

El diseño de una WLAN es similar al de las tecnologías celulares. En lugar de tener un access point o bridge grande, centralizado, de alta energía, las WLANs favorecen el modelo celular de utilizar múltiples estaciones base de baja energía para maximizar las capacidades de cobertura, la redundancia y las capacidades de ancho de banda.

Tercera generación (3G)

Los sistemas inalámbricos 3G proporcionan acceso a un amplio rango de servicios de telecomunicaciones soportados por las redes de telecomunicación fijas, y a otros servicios que son específicos de usuarios móviles. Se abarca un rango de tipos de terminales inalámbricas, que enlazan a los usuarios a las redes terrestres o basadas en satélites. Las terminales pueden diseñarse para un uso móvil o fijo.

Los sistemas 3G tienen varias funciones de diseño claves:

- Un alto grado de factores en común de diseño en todo el mundo
- Compatibilidad de servicios en todo el mundo
- Uso de pequeñas terminales de bolsillo con capacidad de roaming en todo el mundo
- Acceso a la Internet y a otras aplicaciones multimedia
- Un amplio rango de servicios y terminales

De acuerdo a la Unión Internacional de Telecomunicaciones (ITU), Iniciativa de Telecomunicaciones Móviles Internacional 2000 (IMT-2000), los servicios de sistemas 3G se planificaron para iniciarlos alrededor del año 2000, dependiendo de las consideraciones del mercado. Posteriormente se predijo que los servicios 3G se ofrecerían en 2001. No obstante, los servicios 3G no comenzaron a aparecer hasta 2002 y la mayoría de los observadores de la industria afirman que estos servicios no son auténticos servicios 3G porque no logran velocidades de datos 3G.

La Figura 2 describe algunos de los atributos y capacidades de servicios clave esperados de los sistemas 3G.

Frequency Reuse - The Key to Channel Capacity

Capability to support circuit and packet data at high bit rates:

- 144 Kbps or higher for high mobility, or vehicular traffic
- 384 Kbps for pedestrian traffic
- 2 Mbps or higher for indoor traffic

Interoperability and roaming

Common billing/user profiles:

- Sharing of usage and rate information between service providers
- Standardized call detail recording
- Standardized user profiles
- Capability to determine geographic position of mobiles and report it to both the network and the mobile terminal

Support of multimedia services and capabilities:

- Sharing of usage and rate information between service providers

Figura 2

1.4 Componentes y Topologías

1.4.1 Descripción general de los componentes

La familia de productos Cisco Aironet, que se muestra en las Figuras 1 y 2, está disponible en una variedad de factores de forma que encajan con casi cualquier aplicación. Proporciona una solución completa a los clientes que requieren la movilidad y flexibilidad de una WLAN para complementar o reemplazar a una LAN cableada. Los productos se integran sin fisuras a las redes Ethernet cableadas, cumplen completamente con los estándares IEEE 802.11 y entregan un desempeño de hasta 54 Mbps, dependiendo de la tecnología subyacente.

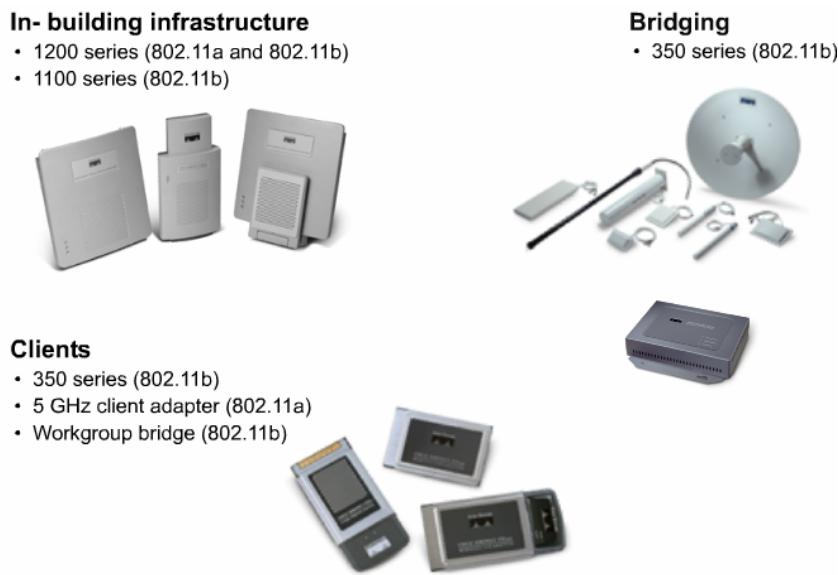


Figura 1

In Building Infrastructure			
AP 1200 Series	802.11a,b	2.4 GHz and 5 GHz	11 Mbps and 54 Mbps
AP 1200 Series	802.11a,b	2.4 GHz	11 Mbps

Bridging			
350 Series Bridges			
Dish Antenna	802.11b	2.4 GHz	11 Mbps
Mast Antenna	802.11b	2.4 GHz	11 Mbps
Panel Antenna	802.11b	2.4 GHz	11 Mbps
Patch Antenna	802.11b	2.4 GHz	11 Mbps
Yagi Antenna	802.11b	2.4 GHz	11 Mbps

Clients			
PCM350 Series	802.11b	2.4 GHz	11 Mbps
PCM1200 Series	802.11a	5 GHz	54 Mbps

Figura 2

La serie Cisco Aironet incluye adaptadores clientes y un conjunto de access points (APs) inalámbricos. También incluye antenas para conectar clientes inalámbricos a redes tanto inalámbricas como cableadas. También hay productos y antenas de bridge de línea de visión, que están diseñados para un uso de edificio a edificio con alcances de hasta 40 km (25 millas).

Los productos 802.11b utilizan la tecnología del espectro expandido de secuencia directa (DSSS) a 2,4 GHz para entregar un throughput de hasta 11 Mbps. Los productos 802.11a utilizan multiplexado por división de frecuencia ortogonal (OFDM) a 5 GHz y ofrecen hasta 54 Mbps.

1.4.2 Adaptadores clientes

Los adaptadores clientes proporcionan a los usuarios la libertad, flexibilidad y movilidad del networking inalámbrico. La Figura 1 ilustra los tres tipos de adaptadores clientes inalámbricos Cisco Aironet®, que son: basado en PCMCIA (placa de PC), LM, y placa basada en PCI. Los adaptadores de placa de PC otorgan a los usuarios de PCs laptop o notebook la capacidad de moverse libremente a través de un entorno de campus, a la vez que se mantiene la conectividad a la red. Los adaptadores PCI inalámbricos permiten a los usuarios agregar PCs de escritorio a la WLAN. Todos los adaptadores cuentan con antenas que proporcionan el rango requerido para la transmisión y recepción de datos en grandes facilidades de interiores.



Figura 1

El Adaptador Cliente Mini-PCI (MPI350) Cisco Aironet® es una solución incorporada, disponible sólo para los fabricantes, que complementa al Aironet Serie 350. Basándose en la tecnología de espectro expandido de secuencia directa (DSSS) que opera en la banda de 2,4 GHz, el adaptador cliente MPI350 cumple con el estándar IEEE 802.11b, asegurando una interoperabilidad con otros productos WLAN que

también lo hacen. El factor de forma pequeño Mini-PCI y el diseño liviano son idealmente aptos para las notebooks de PC, aparatos electrodomésticos de Internet y otros dispositivos móviles. Se soportan controladores para todos los sistemas operativos populares, incluyendo Windows 95, 98, NT 4.0, Windows 2000, Windows ME, Windows XP, Mac OS Versión 9.x, y Linux.



Figura 2

1.4.3 Access points

Un access point (AP) contiene un transceptor de radio. Puede actuar como punto central de una red inalámbrica autónoma o como punto de conexión entre redes inalámbricas y cableadas. En grandes instalaciones, la funcionalidad de roaming proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente a través de la facilidad, a la vez que se mantiene un acceso sin fisuras y sin interrupciones a la red.



Figura 1

Los APs vienen con funciones de tecnología, seguridad y administración variadas. Algunos access points son de banda dual y soportan tecnologías tanto de 2,4 GHz como de 5 GHz, mientras que otros sólo soportan una única banda. Si un access point tiene una ROM FLASH no volátil para almacenar firmware y configuraciones, es más fácil actualizar el firmware y cambiar las configuraciones. Cualquier access point puede utilizarse como repetidor, o punto de extensión, para la red inalámbrica. La Figura 1 ilustra los APs Cisco Aironet 1100 y 1200. El Aironet 1100 soporta 802.11b y el Aironet 1200 es un AP de banda dual que soporta tanto 802.11b como 802.11a. Ambos dispositivos serán actualizables a 802.11g con un reemplazo de mini-PCI.

1.4.4 Bridges

Existen 2 tipos de bridges Cisco. En primer lugar, el Bridge Inalámbrico (WB) 350 está diseñado para conectar dos o más redes (conectadas en general en edificios diferentes), los bridges inalámbricos proporcionan conexiones inalámbricas de alta velocidad, de rango extenso y de línea de vista. El WB es ideal para instalaciones sujetas a clasificación de pleno y entornos rigurosos. La Figura 1 muestra el WB. Las velocidades de datos son más rápidas que las líneas E1/T1 sin la necesidad de líneas arrendadas costosas o cable de fibra óptica, mientras pueda lograrse la frecuencia de radio (RF) de línea de vista (LOS).



Figura 1

En segundo lugar, el Bridge de Grupos de Trabajo (WGB) Cisco Aironet® Serie 350 lleva la conectividad inalámbrica de bajo costo a cualquier dispositivo habilitado para Ethernet que esté diseñado para cumplir con las necesidades de grupos de trabajo remotos, oficinas satelitales y usuarios móviles. El Bridge de Grupos de Trabajo conecta rápidamente hasta ocho laptops habilitados para Ethernet u otras computadoras portátiles a una WLAN inalámbrica, proporcionando el enlace desde estos dispositivos a cualquier AP Cisco Aironet o Bridge Inalámbrico.

Un bridge inalámbrico 802.11b, que opera en el rango de los 2,4 GHz, no requiere ningún FCC de EE.UU. ni otro permiso de agencia aplicable. Mientras no haya ningún requisito de permiso es más fácil de instalar, pero deberá tenerse cuidado de evitar ocasionar interferencia a los usuarios existentes. Recuerde también que los bridges Cisco, al igual que muchos otros bridges de fabricantes, son implementaciones propietarias del estándar 802.11 y por lo tanto no puede lograrse la interoperabilidad entre fabricantes.

1.4.5 Antenas

Una variedad de antenas opcionales de 2,4 GHz están disponibles para APs y bridges, que pueden utilizarse para reemplazar la antena estándar rubber ducky. Las antenas deberán escogerse cuidadosamente para asegurar la obtención de un rango y cobertura óptimos [1](#).



Figura 1

Cada antena tiene diferentes capacidades de ganancia y rango, amplitudes de rayo, cobertura y factores de forma. El acoplamiento de la antena correcta con el AP correcto permite una cobertura eficiente en cualquier instalación, así como una mejor confiabilidad a velocidades de datos más altas. Una cobertura detallada de las antenas se proporcionará posteriormente en el curso.

1.4.6 Cables y accesorios

La implementación de cada WLAN es diferente. Al planificar una solución en el interior del edificio, variar los tamaños de las instalaciones, materiales de construcción y divisiones interiores, surgirán consideraciones acerca del host de transmisión y multiruta. Al implementar una solución de edificio a edificio, se tomarán en cuenta la distancia, las obstrucciones físicas entre instalaciones y la cantidad de puntos de transmisión.

Cisco proporciona una solución completa para cualquier implementación WLAN incluyendo cables, montaje de hardware y accesorios. En primer lugar, un cable de baja pérdida extiende la longitud entre cualquier bridge Cisco Aironet y la antena. El cable de baja pérdida proporciona flexibilidad de instalación sin un sacrificio significativo en materia de alcance. Lo siguiente, un extensor de cielorraso, es un cable de antena

flexible que extiende el cableado desde el access point en general dentro de un espacio cerrado. Además de los cables, una montura articulada Yagi agrega capacidad de bisagra a las antenas Yagi montadas en un mástil. Finalmente, es importante evitar daños a la red utilizando un pararrayos que ayuda a evitar el daño debido a picos inducidos por rayos o electricidad estática.

1.4.7 Tecnologías LAN inalámbricas

La tecnología WLAN puede tomar el lugar de una red cableada tradicional o extender sus capacidades. De manera muy similar a sus contrapartes cableadas, el equipamiento WLAN del interior de un edificio consiste en adaptadores clientes y access points, que llevan a cabo funciones similares a las de los hubs de networking cableado.

Para instalaciones pequeñas o temporales, una WLAN puede disponerse en una topología peer-to-peer (también denominada ad hoc) utilizando únicamente adaptadores cliente. Para una mayor funcionalidad y alcance, pueden incorporarse puntos de acceso para que actúen como centro de una topología en estrella, según se muestra en la Figura 1. El AP también puede funcionar como bridge de una red Ethernet.

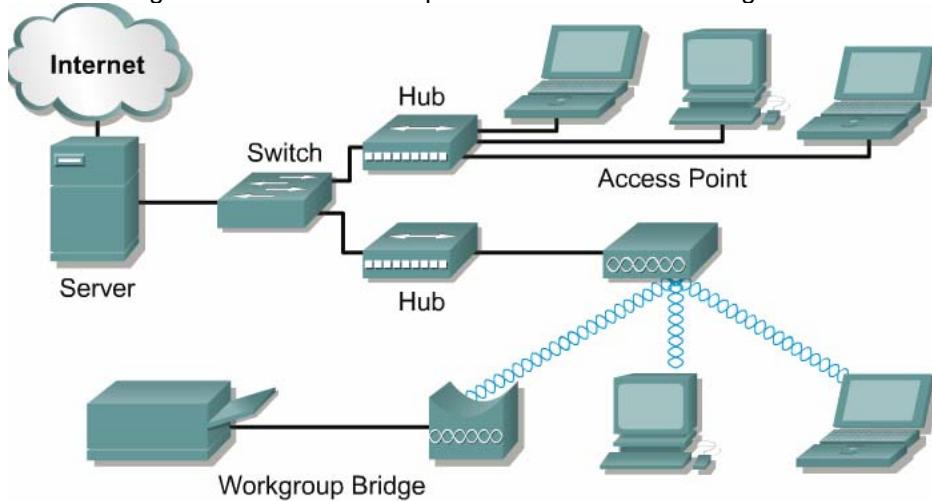


Figura 1

Adoptar la tecnología inalámbrica permite una informática tanto móvil como conectada dentro de un edificio. Los usuarios pueden desplazarse libremente dentro de una instalación, a la vez que se mantiene acceso a la red.

Aplicar tecnología WLAN a sistemas de escritorio proporciona a una organización una flexibilidad que es imposible de lograr con una LAN tradicional. Los sistemas de clientes de escritorio pueden ubicarse en lugares donde tender cables es impráctico o imposible. Las PCs de escritorio pueden re-implementarse en cualquier sitio dentro de una instalación y tan frecuentemente como sea necesario. Esto convierte a la tecnología inalámbrica en algo ideal para grupos de trabajo temporales y organizaciones en rápido crecimiento.

WLANS de edificio a edificio

De manera muy similar a como una señal de radio puede recibirse en todo tipo de clima, a kilómetros de distancia de su transmisor, la tecnología WLAN aplica la potencia de las ondas de radio para redefinir verdaderamente lo "local" de una LAN. Con un bridge inalámbrico, las redes ubicadas en edificios que se encuentran a kilómetros uno del otro pueden integrarse en una única LAN. Al efectuar bridging entre edificios utilizando cable de cobre o fibra óptica tradicional, las autopistas, lagos e incluso los gobiernos locales pueden ser obstáculos insuperables. Un bridge inalámbrico disminuye estas amenazas. Los datos transmitidos a través del aire en frecuencias no licenciadas evitan la emisión tanto de las licencias como de los derechos de paso.

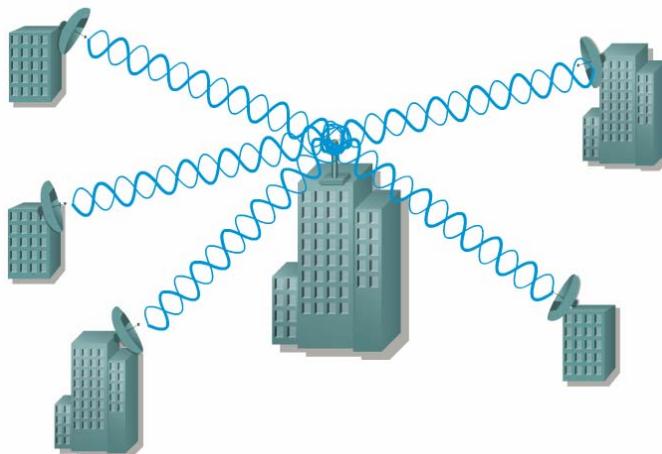


Figura 2

Sin una alternativa inalámbrica, las organizaciones recurren frecuentemente a las tecnologías de networking de área amplia (WAN) para enlazar instalaciones separadas. Contratar líneas arrendadas u otros servicios de área amplia presenta a menudo una variedad de inconvenientes:

- La instalación en general es costosa y raramente inmediata
- Las tarifas mensuales a menudo son altas para el ancho de banda

Un bridge inalámbrico puede en general adquirirse e instalarse en un día. Una vez que se hace la inversión, no hay gastos recurrentes. Los bridges inalámbricos modernos proporcionan el ancho de banda que se esperaría de una tecnología basada en comunicaciones de datos antes que en comunicaciones de voz.

1.5 El Mercado de las LANs Inalámbricas

1.5.1 Implicaciones

Durante la última década, las comunidades de networking e inalámbrica esperaban que cada año se convirtiera en el año de la WLAN. La tecnología WLAN tuvo algunos inicios fallidos en los '90, por una variedad de razones. Tecnología inmadura, problemas de seguridad y velocidades de conectividad lentas evitaron que la tecnología WLAN se convirtiera en una alternativa viable a las LANs cableadas. Cada año que pasaba proporcionaba el terreno necesario para la aceptación individual de la tecnología inalámbrica.

Las primeras aplicaciones de la tecnología WLAN se concentraban en las necesidades de los trabajadores del conocimiento móviles que requerían acceso a información en tiempo real. Soluciones inalámbricas innovadoras ayudaron a resolver los siguientes problemas específicos del mercado:

- Fabricación - La tecnología inalámbrica se utiliza para acceder al precio recomendado por el fabricante (MRP) y a sistemas de administración de inventario desde el negocio.
- Cuidado de la salud - La tecnología inalámbrica presta a los doctores y enfermeras acceso a información de cuidado de pacientes en tiempo real, desde su cama de hospital.
- Minoristas - La tecnología inalámbrica permite al personal de ventas efectuar verificaciones de inventario sin salir del local de la tienda.
- Educación - La tecnología inalámbrica permite a los alumnos y docentes conectarse a recursos de aprendizaje en entornos de campus.

Gracias a la interoperabilidad de los estándares y a las velocidades de throughput mejoradas, las soluciones WLAN se implementan ampliamente en la actualidad.

Varios desarrollos tecnológicos y estratégicos recientes han ayudado a que las tecnologías inalámbricas se desarrollen más rápidamente:

- Los estándares 802.11 han alentado la aceptación y adopción de parte del mercado.
- El desempeño inalámbrico actual no es notablemente diferente a una conexión cableada para el usuario promedio.
- Un incremento en la seguridad utilizando un cifrado de 128 bits ha reducido los temores de una privacidad y control inadecuados.
- Los access points de más largo alcance han traído soluciones más factibles.

Por primera vez la tecnología WLAN está siendo considerada seriamente como forma de completar una red existente o de crear una nueva red. La aceptación de parte del mercado alienta a que surjan nuevas aplicaciones de la tecnología WLAN a lo largo de una empresa. A medida que los usuarios comienzan a disfrutar los beneficios de conectarse en cualquier lugar, en cualquier momento, es probable que el crecimiento y la aceptación de las soluciones empresariales inalámbricas continúen.

1.5.2 Crecimiento y aplicaciones de las WLANs

Cuatro factores clave influencian la creciente aceptación de la tecnología inalámbrica:

1. Velocidad: la velocidad de datos de 11 Mbps IEEE 802.11b cumple con los estándares empresariales de desempeño. IEEE 802.11a ofrece una velocidad de datos de 54 Mbps.
2. Posicionamiento: posicionar las WLANs como forma de completar la solución de networking LAN/WAN simplifica la decisión de la adopción de la tecnología. También alienta a los clientes a incluir la tecnología inalámbrica en sus planes de networking estratégicos.
3. Valor: costos más bajos con un desempeño aceptable convierten a la tecnología inalámbrica en una alternativa atractiva a las soluciones cableadas.
4. Facilidad de implementación: las soluciones instantáneas y las alternativas implementadas fácilmente aceleran la adopción en el mercado.

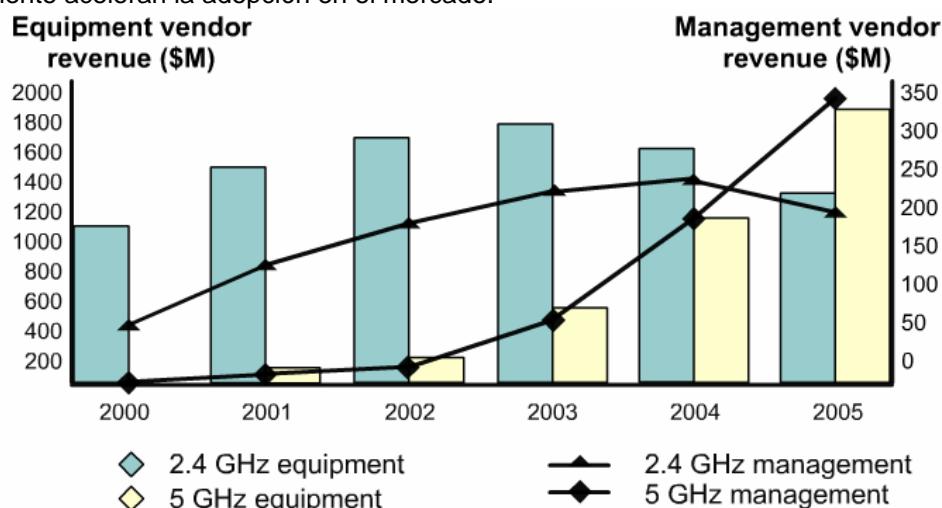


Figura 1

Se espera que las WLANs crezcan, tal como lo muestra la Figura 1. Esta tecnología tiene varias aplicaciones inmediatas, incluyendo las siguientes:

- Los profesionales IT o ejecutivos de negocios que desean movilidad dentro de la empresa, tal vez además de una red cableada tradicional
- Propietarios de negocios o directores de IT que necesitan flexibilidad para cambios frecuentes en el cableado de la LAN, ya sea en todo el sitio o en áreas seleccionadas
- Cualquier compañía cuyo sitio no conduzca a un cableado LAN a causa de limitaciones edilicias o de presupuesto, como edificios más antiguos, espacio arrendado o sitios temporales
- Cualquier compañía que necesite la flexibilidad y los ahorros en materia de costos ofrecidos por un bridge de línea de vista, de edificio a edificio para evitar excavaciones, líneas arrendadas o problemas de derecho de paso de elevado costo

El mercado de las WLANs se encuentra en sus primeras etapas de desarrollo. La innovación tecnológica y la reciente normalización están preparando el terreno para una más amplia adopción de parte del mercado. Controladores clave del mercado, como un incremento en el desempeño, costos más bajos y facilidad de implementación están acelerando el crecimiento del mismo.

Un mercado vertical es una industria o grupo de empresas en particular en el cual productos o servicios similares se desarrollan y publicitan utilizando métodos similares. Ejemplos de mercados verticales actuales se muestran en la Figura 2.

Vertical Markets which are Adopting WLAN Technology	
Wireless Application	
<ul style="list-style-type: none"> • Retail • Warehouses • Electronics and technology • Government • Healthcare • Insurance • Real estate • Transportation • Delivery by train, ground, ship, and air • Hospitality and conventions • Energy and utilities such as water, gas, and electricity • Banking and financial • Field service • Vending • Manufacturing and industrial • Education • Travel and recreation • Military 	

Figura 2

1.5.3 Requisitos del Mercado

Los cuatro requisitos principales para una solución WLAN son los siguientes:

1. Alta disponibilidad — La alta disponibilidad se logra mediante la redundancia del sistema y un diseño de área de cobertura apropiado. La redundancia del sistema incluye APs redundantes en frecuencias separadas. Un diseño de área de cobertura apropiado incluye cuentas para roaming, negociación de velocidad automática cuando se debilita la señal, una selección apropiada de la antena, y el posible uso de repetidores para extender la cobertura a áreas donde un AP no podría utilizarse de otro modo.
2. Escalabilidad — La escalabilidad se logra soportando múltiples APs por área de cobertura, que utilizan múltiples frecuencias. Los APs también pueden llevar a cabo el equilibrio de la carga, si así se lo desea.
3. Capacidad administrativa — Las herramientas de diagnóstico representan una gran porción de la administración dentro de las WLANs. Los clientes deberán poder administrar dispositivos WLAN a través de APIs estándar de la industria, incluyendo SNMP y Web, o a través de aplicaciones de administración empresarial importantes, como CiscoWorks 2000, Cisco Stack Manager, y Cisco Resource Monitor.
4. Arquitectura abierta — La apertura se logra mediante la adhesión a estándares tales como 802.11a y 802.11b, la participación en asociaciones de interoperabilidad como la Alianza Wi-Fi, y de certificación, como la certificación FCC de EE.UU.

Otros requisitos están evolucionando a medida que las tecnologías WLAN obtienen popularidad:

- Seguridad — Es esencial para encriptar los paquetes de datos transmitidos por vía aérea. Para instalaciones más grandes, se requieren también una autenticación centralizada del usuario y una administración centralizada de claves de cifrado.
- Costo — Los clientes esperan reducciones continuas en el precio de un 15 a un 30 por ciento cada año, e incrementos en desempeño y seguridad. Los clientes están preocupados no sólo por el precio de adquisición sino por el costo total propietario (TCO), incluyendo los costos de instalación.

1.6 Desafíos y Problemas

1.6.1 Interferencia y Degrado de la Señal de Radio

Un desafío importante de las WLANs es la interferencia de las señales de radio. En diseños de área metropolitana de edificio a edificio, es posible tener interferencia de terceros, otras compañías que utilizan tecnología inalámbrica. 1En esta situación, los administradores de la red deben asegurarse de utilizar diferentes canales. La interferencia no puede detectarse hasta que el enlace no se implemente realmente. Puesto que los estándares 802.11 utilizan un espectro sin licencia, la mejor forma de evitar la interferencia es cambiar de canales.

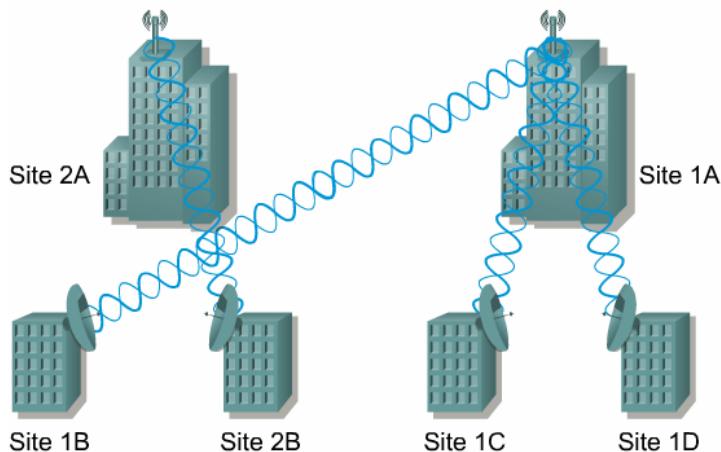


Figura 1

Muchos otros dispositivos, como los teléfonos portátiles, los hornos a microondas, los parlantes inalámbricos y los dispositivos de seguridad, utilizan también estas frecuencias. La cantidad de interferencia mutua que será experimentada por estos dispositivos de networking y otros planificados no está clara. La interferencia entre parlantes inalámbricos y otros dispositivos es común hoy en día. A medida que esta banda sin licencia se va poblando, es probable que aparezcan otros tipos de interferencia. Los objetos físicos y las estructuras de los edificios también crean diversos niveles de interferencia.

	802.11b	802.11a	802.11g
Frequency band	2.4 Ghz	5 GHz	2.4 GHz
Availability	Worldwide	US / AP	Worldwide
Maximum data rate	11 Mbps	54 Mbps	54 Mbps
Other services (interference)	Cordless phones, microwave ovens, wireless video, bluetooth devices	Hyper LAN Devices	Cordless phones, microwave ovens, wireless video, bluetooth devices

Figura 2

La operación en bandas no licenciadas lleva con ella un riesgo inherentemente más alto de interferencia, porque los controles y protecciones de las licencias no están disponibles. En Estados Unidos, por ejemplo, la Comisión Federal de Comunicaciones (FCC) no tiene ninguna regla que prohíba específicamente a un nuevo usuario instalar un nuevo enlace de radio de banda sin licencia y en una frecuencia ya ocupada. Esto puede ocasionar interferencia.

Existen dos advertencias a tener en cuenta:

Si alguien instala un enlace que interfiere con un enlace inalámbrico, la interferencia es probablemente mutua. En el caso de los enlaces punto a punto que emplean antenas direccionales, cualquier fuente de señales de un nivel de potencia comparable que podría ocasionar interferencia tendría que alinearse físicamente a través del eje de la ruta de transmisión. En las bandas sin licencia, el potencial de interferencia proveniente de otro usuario sin licencia crece en relación a lo que ocurre con bandas licenciadas. La diferencia depende del control. Los poseedores de licencias esencialmente poseen un canal permitido. Tienen un derecho legal a defenderse contra interferencias que disminuyan su desempeño. Debido a la popularidad de las WLANs, el uso de las bandas no licenciadas se está incrementando. Los administradores de red deberán tener en cuenta que hay otros usuarios con licencia que en ocasiones también operan en las bandas sin licencia. Las bandas sin licencia se adjudican de manera compartida. Aunque puede que no se requiera obtener una licencia para operar una aplicación de comunicaciones de datos de baja potencia utilizando equipamiento aprobado, puede permitirse a los usuarios con licencia operar con una potencia significativamente superior.

Es posible que se genere interferencia electromagnética (EMI) proveniente de equipamiento no relacionado con las ondas de radio que opera en proximidad al equipamiento WLAN Cisco Aironet. Aunque teóricamente es posible que esta interferencia afecte directamente la recepción y la transmisión de señales,

es más probable que afecte los componentes del transmisor. Para minimizar los posibles efectos de la EMI, el mejor curso de acción es aislar el equipamiento de radio de fuentes potenciales de EMI. El equipamiento deberá ubicarse lejos de dichas fuentes de ser posible, y deberá proporcionarse una fuente de potencia condicionada por el equipamiento WLAN para ayudar a reducir los efectos de la EMI.

1.6.2 Administración de la energía

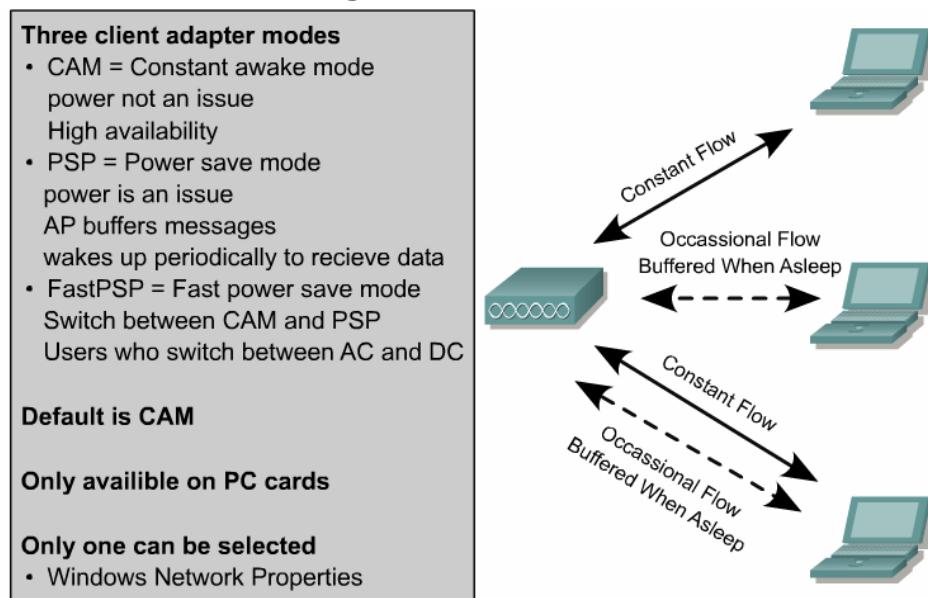


Figura 1

El consumo de energía siempre es un problema en el caso de las laptops, porque la energía y la batería tienen vidas limitadas. Como se muestra en la Figura 1, hay disponibles tres modos de energía en el caso de las placas de PC de Cisco:

1. Modo constantemente encendido (CAM): este modo es el mejor cuando la energía no es un problema, por ejemplo cuando una fuente de energía AC está disponible para el dispositivo. Este modo proporciona la mejor opción de conectividad y la infraestructura inalámbrica más disponible desde la perspectiva del cliente.
2. Modo de ahorro de energía (PSP): este modo deberá seleccionarse cuando la energía es de la mayor importancia. En esta situación, la NIC inalámbrica se apagará después de un periodo de inactividad y se encenderá periódicamente para recuperar datos almacenados en el buffer del AP.
3. Modo de ahorro de energía rápido (FastPSP): este modo es una combinación de CAM y PSP. Es bueno para los clientes que alternan entre energía AC y DC.

1.6.3 Interoperabilidad

La mayoría de los fabricantes desean que sus clientes utilicen sus APs y NICs de manera exclusiva. Ofrecen cierto grado de capacidad reducida si existe la necesidad de combinar y hacer coincidir diferentes marcas de APs y NICs.

En la mayoría de los casos los problemas son mayormente cosméticos pero pueden resultar en un incremento de llamadas al escritorio de ayuda. Hasta el lanzamiento de la siguiente generación, el administrador del sistema tiene que tomar una difícil decisión, utilizar un sistema de un único fabricante, con todos los NICs y APs provenientes de ese fabricante, o arreglárselas sin las herramientas de administración avanzadas que proporcionan las soluciones de un único fabricante.

Tal como se muestra en la Figura 1, en una red cerrada como una red corporativa, existen ventajas en una solución de un único fabricante. Hacer responsable a un único fabricante del desempeño del equipamiento elimina la posibilidad de que un fabricante culpe al otro por fallos en el equipo. En un entorno más abierto, como una red de un instituto terciario o una universidad o una terminal de aeropuerto, una solución de fabricante único puede no ser factible. Pueden ofrecerse sugerencias respecto a qué equipo deberá adquirirse, pero el administrador de red probablemente necesitará soportar lo que los usuarios compraron.

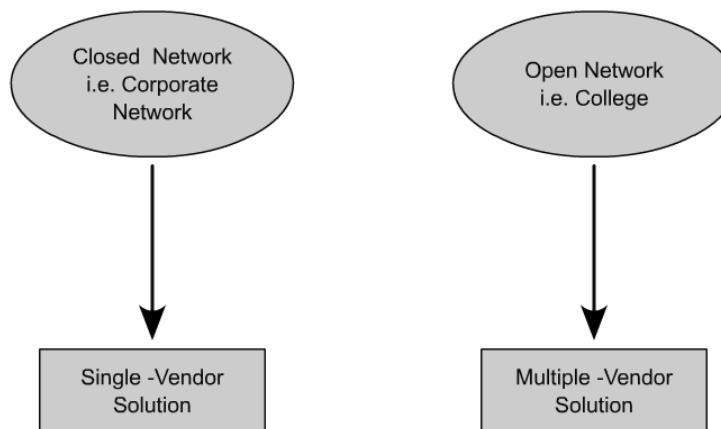


Figura 1

Recuerde también que los bridges Cisco, al igual que muchos otros bridges de fabricantes, son implementaciones propietarias del estándar 802.11 y por lo tanto no puede lograrse la interoperabilidad entre fabricantes.

1.6.4 Seguridad en la red

La seguridad en la especificación IEEE 802.11—que se aplica a 802.11b, 802.11a, y 802.11g—ha pasado por un intenso escrutinio. Los investigadores han expuesto varias vulnerabilidades en los mecanismos de autenticación, privacidad de los datos e integridad de los mensajes definidos en la especificación. A medida que crecen las redes inalámbricas, la amenaza de intrusos provenientes del interior y el exterior es grande. Los atacantes denominados “war drivers” están continuamente conduciendo sus autos en busca de WLANs inseguras que explotar.

La Privacidad Equivalente a la Cableada (WEP) mejorada por el IEEE con el Protocolo de Integridad de Claves Temporales (TKIP), proporciona opciones de autenticación robustas con 802.1X para hacer seguras las LANs inalámbricas basadas en 802.11. Al mismo tiempo, el IEEE está buscando mecanismos de cifrado más fuertes. El IEEE ha adoptado el uso del Estándar de Cifrado Avanzado (AES) a la sección de privacidad de datos del estándar 802.11i propuesto.

Además de 802.1X, Cisco soporta el uso de VPNs basadas en la Seguridad IP (IPSec) de capa 3 a través de LANs cableadas 802.3 y WLANs 802.11, utilizando los dispositivos de terminación VPN de Cisco y software del cliente VPN instalado en dispositivos inalámbricos. Esto es vital para proporcionar un acceso empresarial eficaz en materia de costos desde espacios públicos tales como hoteles y aeropuertos.

Las debilidades y técnicas de mitigación de la tecnología inalámbrica se tratarán en profundidad posteriormente en el curso. Un diseñador y especialista en soporte de tecnologías inalámbricas debe poder implementar de manera segura una red inalámbrica. La seguridad en la red siempre deberá implementarse basándose en una política de seguridad adecuada.

1.6.5 Confiabilidad y conectividad

Las LANs inalámbricas incluyen mecanismos para mejorar la confiabilidad de las transmisiones de paquetes, para que al menos tengan el mismo nivel que la Ethernet cableada. El uso de protocolos TCP/IP ayudará a proteger la red contra cualquier pérdida o corrupción de datos en el aire. La mayoría de los sistemas de WLAN utilizan una tecnología de espectro expandido o multiplexado por división de frecuencia ortogonal (OFDM).

Los dos tipos de radio de espectro expandido son secuencia directa (DSSS) y salto de frecuencia (FHSS). Ambos se muestran en la Figura 1. Se basan en la idea de que una señal que se expande ampliamente o que se mueve rápidamente de canal a canal será difícil de detectar y de interferir con ella. DSSS genera un patrón de bits redundante denominado chip o código de chipping, para cada bit a transmitir. FHSS utiliza una portadora de banda angosta que cambia la frecuencia en un patrón conocido tanto por el transmisor como por el receptor. Si todo se mantiene apropiadamente sincronizado, esto crea un único canal lógico, incluso aunque la frecuencia cambie constantemente. Las primeras implementaciones de 802.11 utilizaban FHSS, no obstante 802.11b estandarizó DSSS.

Spread-spectrum Technology Types

- **DSSS:** Direct-sequence spread spectrum generates a redundant bit pattern called a chipping sequence, for each bit to be transmitted.
- **FHSS:** Frequency-hopping spread spectrum uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.
- **OFDM:** orthogonal frequency-division multiplexing limits the crosstalk or interference of transmitting channels, thus allowing greater transmission speeds.

Figura 1

Actualmente los estándares 802.11a y 802.11g, que operan en hasta 54 Mbps, utilizan OFDM en lugar de DSSS. OFDM limita la diafonía o la interferencia de los canales de transmisión. OFDM se utiliza en servicios de emisión de audio digital europeos. En comparación con DSSS, OFDM permite más velocidad. OFDM no pierde distancia. De hecho, facilita la capacidad para lograr distancias más largas. OFDM sí requiere más potencia de procesamiento en la radio.

Además de cuidar de que coincidan las tecnologías de transmisión, los administradores de redes inalámbricas deben tener en cuenta que los problemas de conexión también pueden existir en entornos cambiantes donde hay obstáculos que pueden bloquear, reflejar o dificultar el paso de las señales. La elección y ubicación del montaje de la antena debe considerarse cuidadosamente al diseñar WLANs para evitar una futura interferencia. La conexión usualmente no se perderá incluso aunque el ancho de banda disponible caiga hasta niveles muy bajos. La falta de un ancho de banda garantizado es de particular interés para muchas compañías.

1.6.6 Problemas de instalación y diseño del sitio

No todos los sitios se crean de igual manera. Incluso sitios similares pueden ser muy diferentes aunque parezcan uniformes. Esto requiere un enfoque ligeramente diferente de la instalación en cada sitio.

La contribución de los clientes es un requisito. En algunos lugares puede aceptarse un bache en la cobertura, mientras que en otros puede resultar esencial tener una cobertura del 100 por ciento. El cliente es el único que puede determinar esto.

1.6.7 Problemas de salud

Existen muchos factores desconocidos respecto a los límites seguros de la exposición humana a la radiación de frecuencia de radio (RF). El uso de la palabra radiación no connota necesariamente ninguna relación con la fisión nuclear u otros procesos radioactivos, sino más bien una radiación no ionizante de emisiones de radio. La regla general es no someter innecesariamente a seres vivientes a energía RF irradiada. Esto significa que uno no debería pararse en frente de, o en estrecha proximidad a, cualquier antena que esté irradiando una señal transmitida. Las antenas que sólo se utilizan para recibir no representan ningún peligro ni problema. En el caso de las antenas parabólicas, es seguro estar cerca de una antena transmisora en operación si uno se encuentra en la parte posterior o lateral de la antena. Estas antenas son direccionales, y niveles de emisión potencialmente peligrosos sólo estarán presentes en la parte frontal de la misma.

Siempre deberá suponerse que cualquier antena está energizada en ese momento, en especial porque la mayoría de las antenas se utilizan en sistemas dúplex. Parabólicas de pequeño tamaño, de 30 cm (1 pie) o menos a menudo irradian energía RF en el rango de frecuencia de decenas de gigahertz. Como regla general, cuanto más alta es la frecuencia, más potencialmente peligrosa es la radiación. Deberá tenerse cuidado de asegurarse de que el transmisor no está operando antes de quitar o reubicar cualquier conexión de antena.

Es importante no pararse frente a, o caminar alrededor de, antenas de microondas que están instaladas sobre los techos. Si es necesario caminar frente a tales antenas, en general existe un peligro de seguridad muy bajo si uno se desplaza rápidamente a través del eje de la ruta de la antena. Para cumplir con los límites de exposición a RF establecidos en los estándares ANSI C95.1, se recomienda que al utilizar una laptop con un adaptador cliente de placa de PC, la antena integrada del adaptador debe posicionarse a más de 5 cm (2 pulgadas) del cuerpo del operador o de otras personas cercanas. Esto es especialmente cierto durante extensos períodos de transmisión o tiempo de operación. Se recomienda limitar el tiempo de exposición si la antena está colocada a menos de 5 cm (2 pulgadas) del usuario. Recuerde que la

computadora puede estar transportando comunicaciones de red de respaldo, incluso si la red no está siendo utilizada activamente.

1.6.8 Futuras direcciones

En la comunidad WLAN continúa el desarrollo. Un estándar emergente es el 802.11g. Este estándar en borrador opera en el rango de los 2,4 GHz, como 802.11b, pero a velocidades más altas. 802.11g se ejecuta a la misma velocidad de 54 Mbps que 802.11a, y utiliza el mismo sistema de modulación OFDM. Está diseñado para ser compatible con clientes 802.11b. Algunos APs 802.11b soportarán la velocidad más alta de 802.11g. Si se necesita en la actualidad una velocidad adicional, o si la frecuencia de 2,4 GHz es ruidosa en una instalación determinada, la tecnología 802.11a de 5 GHz puede ser la mejor opción.

El desempeño continuará mejorando incuestionablemente y los clientes continuarán requiriendo un socio confiable para integrar estas tecnologías dinámicas sin fisuras a la red existente.

Resumen

Este módulo presentó la tecnología en rápida evolución de las WLANs. Las WLANs proporcionan la flexibilidad, movilidad y escalabilidad que desean los usuarios. Tecnologías WLAN actuales operan en los rangos de 2,4 GHz y 5 GHz.

Este módulo trató el efecto que el networking inalámbrico ha tenido en la comunidad del networking. Presentó diferentes tipos de medios de networking que pueden utilizarse con networking inalámbrico. También trató los componentes básicos de una WLAN, que son el punto de acceso, los adaptadores de clientes y las antenas. Los adaptadores de clientes vienen en una variedad de formas para una fácil instalación en computadoras de escritorio, notebooks o PDAs.

Los cuatro factores principales que los administradores de red necesitan considerar al decidir respecto a las tecnologías inalámbricas son la alta disponibilidad, escalabilidad, capacidad de administración y el hecho de que sea una arquitectura abierta. También se trataron otros factores importantes, como el costo y la seguridad.

Módulo 2: IEEE 802.11 y Network Interface Card (NIC)

Descripción general

Este módulo tratará en detalle los estándares IEEE 802.11 WLAN (WLAN), incluyendo el enlace de datos y las especificaciones de la capa física. La normalización de las funciones del networking ha hecho mucho por el avance en el desarrollo de productos de networking costeables e interoperables. A lo largo de este módulo y de este curso, los términos IEEE y 802 se utilizan a menudo. Este módulo proporciona una breve descripción general de IEEE y el comité 802.

Se tratarán los servicios MAC y de capa física que han sido normalizados. Tres servicios son proporcionados por la subcapa MAC en IEEE 802.11. Estos servicios incluyen el servicio de datos asíncronos MAC, los servicios de seguridad y el ordenamiento de las Unidades de Servicios MAC (MSDU). Además, se presentarán servicios de capa física, como el Procedimiento de Convergencia de la Capa Física (PLCP) y el Sistema Dependiente del Medio Físico (PMD), que se normalizan a través de 802.11 a, b, y g. Finalmente, se tratarán los adaptadores clientes, los tipos de controladores y el soporte a los clientes. La función principal de los adaptadores clientes es transferir paquetes de datos a través de la infraestructura inalámbrica. También se tratarán la instalación, configuración y monitoreo de placas de interfaz de red (NICs) inalámbricas.

2.1 Estándares 802.11

2.1.1 Descripción general

Descripción general de la normalización

La normalización de las funciones de networking ha hecho mucho por adelantar el desarrollo de productos de networking costeables e interoperables. Esto es así también en el caso de los productos inalámbricos. Antes de que existieran los estándares inalámbricos, los sistemas inalámbricos estaban plagados de bajas velocidades de datos, incompatibilidad y elevados costos.

La normalización proporciona todos los siguientes beneficios:

- Interoperabilidad entre los productos de múltiples fabricantes
- Desarrollo más rápido de productos
- Estabilidad
- Capacidad para actualizar
- Reducciones de costos

Es importante comprender los dos tipos principales de estándares. Un estándar público no ha sido aprobado por una organización oficial de normalización, sino que es reconocido como estándar a causa de la difusión de su uso. También se denomina estándar de facto. A menudo, un grupo de estándares oficiales adoptarán posteriormente estándares de facto.

Un estándar oficial es publicado y controlado por una organización de normalización oficial como el IEEE. La mayoría de los grupos de normalización oficiales son financiados por el gobierno y la industria, que incrementa la cooperación y la implementación a nivel nacional e internacional. Por esta razón la mayoría de las compañías deberán implementar productos inalámbricos que sigan normas oficiales. Los estándares oficialmente aprobados se denominan estándares de jure. Algunas organizaciones de normalización importantes se muestran en la Figura 1.



Figura 1

Al implementar dispositivos de múltiples fabricantes, es importante que todos los dispositivos se conformen al mismo estándar para asegurar la interoperabilidad. Por ejemplo, el cumplimiento con el estándar 802.11b actual puede crear una WLAN funcional, independientemente del fabricante del producto. El desempeño, la configuración y la capacidad de administración no son siempre los mismos, o iguales, entre fabricantes. La Figura 2 demuestra la interoperabilidad en un entorno de Conjunto de Servicios Básico (BSS).

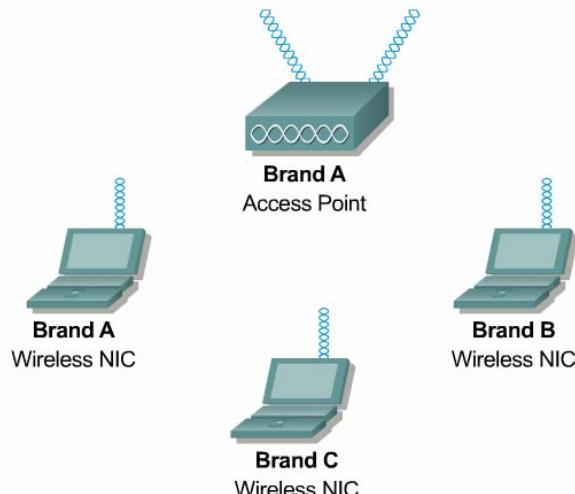


Figura 2

Un problema común en entornos móviles será que las NICs multi-fabricante intenten acceder a una marca diferente de punto de acceso. Por ejemplo, una compañía utiliza productos marca A en el departamento de cuentas, mientras que los usuarios roaming del departamento de IS utilizan las marcas B y C. Utilizar productos que adhieran al estándar 802.11b ayudará a eliminar la mayoría de los problemas de interoperabilidad. Los problemas de roaming, seguridad y capacidad de administración aún pueden presentar desafíos.

2.1.2 IEEE y 802.11

Descripción de IEEE y del Comité 802

El IEEE, fundado en 1884, es una organización profesional sin fines de lucro con más de 377.000 miembros en todo el mundo. El IEEE consiste en muchas sociedades y grupos de trabajo individuales. Desempeña un papel crítico en el desarrollo de estándares, la publicación de obras técnicas, conferencias de patrocinamiento y otorgamiento de acreditación en el área de tecnología eléctrica y electrónica. En el área de networking, el IEEE ha producido muchos estándares ampliamente utilizados como el grupo 802.x de estándares de red de área local (LAN) y los estándares de red de área metropolitana (MAN), que se enumeran en la Figura 1.

IEEE LAN/MAN Standards
<ul style="list-style-type: none"> • 802.0 Sponsor Executive Committee (SEC) • 802.1 High Level Interface (HILI) • 802.2 Logical Link Control (LLC) • 802.3 CSMA/CD (Ethernet) • 802.4 Token Bus • 802.5 Token Ring • 802.6 Metropolitan Area Network (MAN) • 802.7 BroadBand Technical Advisory Group (BBTAG) • 802.8 Fiber Optics Technical Advisory Group (FOTAG) • 802.9 Integrated Services LAN (ISLAN) • 802.10 Standard for Interoperable LAN Security (SILS) • 802.11 Wireless LAN (WLAN) <ul style="list-style-type: none"> • 802.11a, 802.11b, 802.11e, 802.11g, 802.11i • 802.12 Demand Priority • 802.14 Cable-TV Based Broadband Communication Network • 802.15 Wireless Personal Area Network (WPAN) • 802.16 Broadband Wireless Access (BBWA) • 802.17 RPRSG Resilient Packet Ring Group (RPRSG)

Figura 1

El Comité de Normalización LAN/MAN (LMSC) de IEEE 802 desarrolla estándares de red de área local (LAN) y de red de área metropolitana (MAN), principalmente para las dos capas inferiores del modelo de referencia de Interconexión de Sistemas Abiertos (OSI). LMSC, o IEEE Project 802, se coordina con otros estándares nacionales e internacionales. Algunos estándares que comenzaron aquí están publicados por el ISO como estándares internacionales.

La Figura 2 muestra la arquitectura definida por el comité 802 y cómo muchos métodos de acceso al medio diferentes son soportados por este modelo. El control de acceso al medio (MAC) y las capas físicas (PHY) están organizados en un conjunto separado de estándares desde el control de enlace lógico (LLC). Esto se debe a la interdependencia entre el control de acceso al medio, el medio y la topología de cada estándar. Al mismo tiempo, un único proceso LLC puede soportar las funciones lógicas para todos los protocolos MAC y PHY subyacentes.

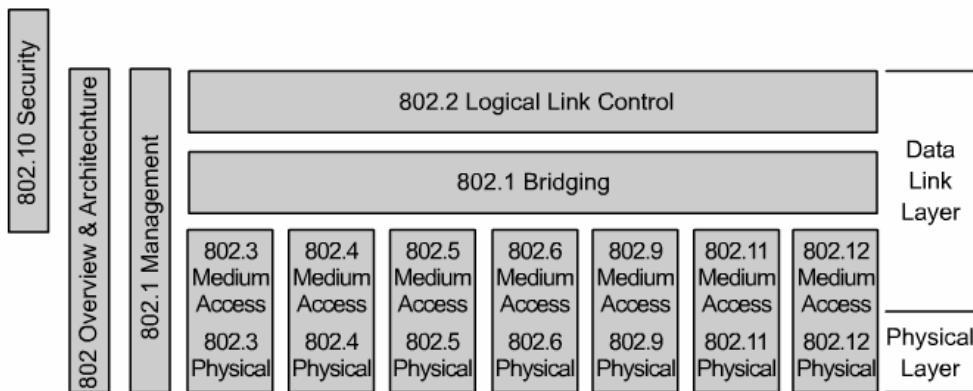


Figura 2

Como se muestra en la Figura 3, la combinación del estándar LLC 802.2 y cualquier protocolo MAC dado es funcionalmente equivalente a la capa de enlace de datos OSI. Los procesos MAC y LLC se denominan en general subcapas de la capa de enlace de datos, aunque en ocasiones se los denomina capas.

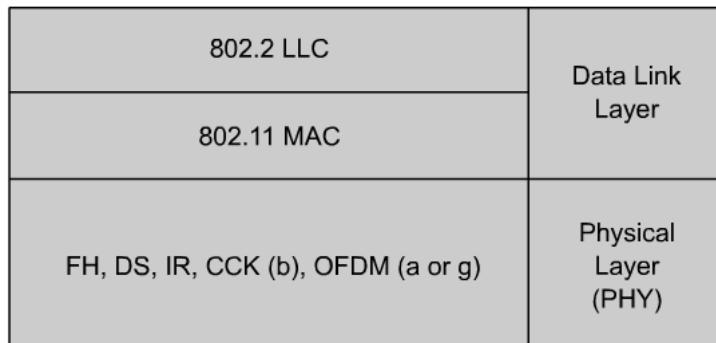


Figura 3

IEEE 802.11

El término 802.11 se refiere realmente a una familia de protocolos, incluyendo la especificación original, 802.11, 802.11b, 802.11a, 802.11g y otros. El 802.11 es un estándar inalámbrico que especifica conectividad para estaciones fijas, portátiles y móviles dentro de un área local. El propósito del estándar es proporcionar una conectividad inalámbrica para automatizar la maquinaria y el equipamiento o las estaciones que requieren una rápida implementación. Éstos pueden ser portátiles, handheld o montados en vehículos en movimiento dentro de un área local.

El estándar 802.11 se denomina oficialmente Estándar IEEE para especificaciones MAC y PHY de WLAN. Define los protocolos por aire necesarios para soportar un networking inalámbrico en un área local. El servicio principal del estándar 802.11 es entregar Unidades MAC de Servicio de Datos (MSDUs) entre dispositivos peer LLC en la capa de enlace de datos. En general, una placa de radio, o NIC, y uno o más access points proporcionan las funciones del estándar 802.11.

Las características de MAC y PHY para las redes de área local inalámbricas (WLANs) están especificadas en 802.11, 802.11b, 802.11a, y 802.11g, entre otros estándares. La capa MAC de este estándar está diseñada para soportar unidades de capa física adicionales a medida que se adoptan, dependiendo de la capacidad del espectro y de las nuevas técnicas de modulación.

2.1.3 Repaso del LLC IEEE 802.2

El LLC es la capa más alta del Modelo de Referencia IEEE 802. El propósito del LLC es intercambiar datos entre usuarios finales a través de una LAN que utiliza protocolos MAC basados en 802. El LLC proporciona una identificación del protocolo de capa superior (ULP), funciones de control de enlace de datos y servicios de conexión. Es independiente de la topología, el medio de transmisión y las técnicas de control de acceso al medio utilizados en las capas MAC y PHY. Las capas superiores, como la capa de red, pasan los datos del usuario al LLC, esperando transmisiones libres de errores a través de la red.

El LLC proporciona los siguientes tres servicios de conexión para ULP:

- Servicios sin conexión no confirmados — Éste es el servicio usual de mejor esfuerzo de una LAN. Las entidades de la red pueden intercambiar unidades de datos de servicio del enlace (LSDUs) sin el establecimiento de una conexión de nivel de enlace de datos. La transferencia de datos puede ser punto a punto, multicast o broadcast.
- Servicios orientados a la conexión confirmados — Este conjunto de servicios proporciona el medio para establecer, utilizar, reconfigurar y terminar conexiones de la capa de enlace de datos. Este servicio proporciona también un secuenciamiento de capa de enlace de datos, un control de flujo y recuperación de errores, para intercambiar LSDUs de manera confiable en la conexión establecida. Las conexiones son punto a punto.
- Servicios sin conexión confirmados — Los servicios sin conexión confirmados proporcionan el medio mediante el cual las entidades de la capa de red pueden intercambiar LSDUs de manera confiable, pero sin el establecimiento de una conexión de enlace de datos. La transferencia de la unidad de datos es punto a punto.

Estos servicios se aplican a la comunicación entre capas peer LLC.

La Figura 1 muestra el formato del encabezado LLC 802.2. Los access points del servicio de destino y origen (DSAP y SSAP) identifican al ULP utilizado, en general un protocolo de capa de red. El campo Control indica si el LSDU contiene información de control o datos del usuario. Para los datos del usuario, los números de secuencia también se mantienen aquí. Cuando se los confirma, se utilizan los servicios orientados a conexión.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

Figura 1

2.1.4 Descripción general de una WLAN

WLANs

Las redes inalámbricas tienen características fundamentales que las hacen significativamente diferentes a las LANs cableadas tradicionales. Algunos países imponen requisitos específicos para el equipamiento de radio además de aquéllos especificados en el estándar 802.11.

En las LANs inalámbricas, una dirección MAC equivale a una ubicación física. Esto se da por supuesto implícitamente en el diseño de LANs cableadas. En IEEE 802.11, la unidad direccionable es una estación (STA). La STA es el destino de un mensaje, pero no es, en general, una ubicación física fija.

Las capas físicas utilizadas en IEEE 802.11 son fundamentalmente diferentes de aquéllas utilizadas en medios alámbricos. Lo siguiente es cierto respecto a los protocolos PHY IEEE 802.11:

- Utilizan un medio que no tiene fronteras absolutas ni fácilmente observables, fuera de las cuales las estaciones no podrán enviar ni recibir frames de red.
- No están protegidos de señales externas.
- Se comunican a través de un medio que es significativamente menos confiable que los medios cableados.
- Tienen topologías dinámicas.
- Les falta una conectividad completa. Normalmente, se supone que cada STA puede escuchar a cada una de las otras STAs. Esta suposición es inválida en el caso de las WLANs. Las STAs pueden estar "ocultas" entre sí.

- Tienen propiedades de propagación variables en el tiempo y asimétricas.

A causa de las limitaciones de los rangos PHY inalámbricos, las WLANs que necesitan cubrir distancias geográficas razonables deben construirse a partir de bloques de construcción de una cobertura básica.

Uno de los requisitos de IEEE 802.11 es manipular estaciones tanto móviles como portátiles. Una estación portátil se desplaza de ubicación a ubicación, pero sólo se utiliza mientras se encuentra en una ubicación fija. Las estaciones móviles en realidad acceden a la LAN mientras se encuentran en movimiento. No es suficiente para manipular sólo estaciones portátiles, puesto que los efectos de propagación desdibujan la distinción entre estaciones portátiles y móviles. Las estaciones fijas a menudo parecen ser móviles, debido a estos efectos de propagación.

Wireless LAN General Description

IEEE 802.11 PHY protocols

- Use a medium without absolute or observable boundaries
- Are unprotected from outside signals
- Have dynamic topologies
- Lack full connectivity
- Communicate over a medium less reliable than wired media
- Have time-varying and asymmetric propagation properties

Otro aspecto de las estaciones móviles es que a menudo reciben alimentación proveniente de baterías. De ahí que la administración de energía sea una consideración importante. Por ejemplo, no puede presuponerse que el receptor de una estación siempre estará encendido.

Se requiere IEEE 802.11 para aparecer en capas superiores, como LLC, como LAN IEEE 802. La red IEEE 802.11 debe manipular la movilidad de la estación dentro de la subcapa MAC.

2.1.5 Arquitectura lógica

La arquitectura IEEE 802.11 consiste en varios componentes que interactúan para proporcionar conectividad inalámbrica. Estos componentes pueden soportar movilidad entre estaciones transparentes para las capas superiores.

Conjunto de servicios básicos (BSS)

El conjunto de servicios básicos (BSS) es el bloque constructor básico de una LAN IEEE 802.11. La Figura 1 muestra un BSS con tres estaciones que son miembros del BSS, además del access point (AP). El BSS abarca una única área RF, o celda, según lo indica el círculo. A medida que una estación se aleja del AP, su velocidad de datos disminuirá. Cuando sale de su BSS, ya no puede comunicarse con otros miembros del mismo. Un BSS utiliza el modo de infraestructura, un modo que necesita un AP. Todas las estaciones se comunican por medio del AP, y no directamente. Un BSS tiene una única ID de conjunto de servicios (SSID).

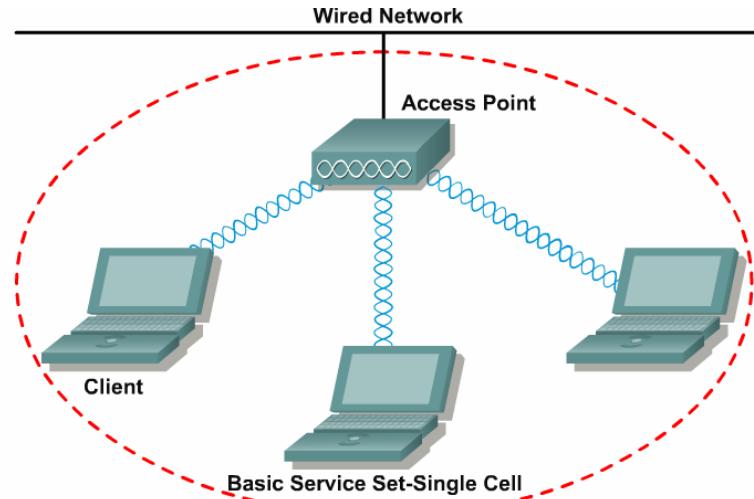


Figura 1

BSS independiente (IBSS)

El conjunto de servicios básicos independiente (IBSS) es el tipo más básico de LAN IEEE 802.11. Una LAN IEEE 802.11 mínima consiste sólo en dos estaciones. En este modo de operación, las estaciones IEEE 802.11 se comunican directamente. Puesto que este tipo de LAN IEEE 802.11 se forma a menudo sin pre-planificar solamente mientras es necesaria una WLAN, a menudo se denomina red ad hoc.

Puesto que un IBSS consiste en STAs conectadas directamente, también se denomina red peer-to-peer. Existe, por definición, sólo un BSS y no hay un Sistema de Distribución (DS). Un IBSS con cuatro estaciones se muestra en la Figura 2. Un IBSS puede tener una cantidad arbitraria de miembros. Para comunicarse fuera del IBSS, una de las STAs debe actuar como gateway o router.

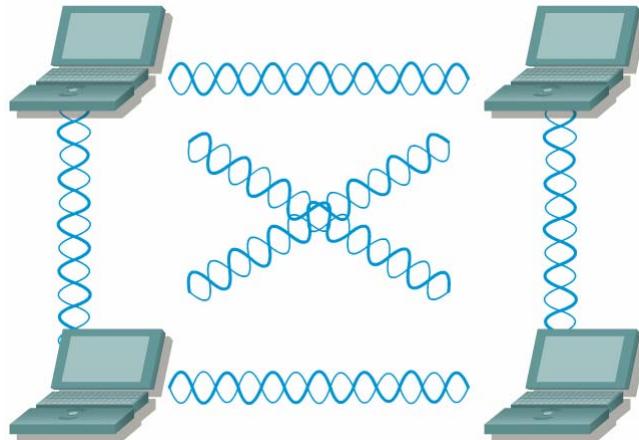


Figura 2

Sistema de distribución (DS)

Las limitaciones de PHY determinan las distancias de estación a estación que pueden soportarse. En el caso de algunas redes esta distancia es suficiente. En el caso de otras, se requiere un incremento en la cobertura. En lugar de existir independientemente, un BSS también puede formar un componente de un conjunto de servicios extendido (ESS). Un ESS se construye a partir de múltiples BSSs, que se conectan a través de APs. Los APs se conectan a un DS común, como lo muestra la Figura 3. El DS puede ser cableado o inalámbrico, LAN o WAN. La arquitectura WLAN IEEE 802.11 se especifica independientemente de las características físicas del DS.

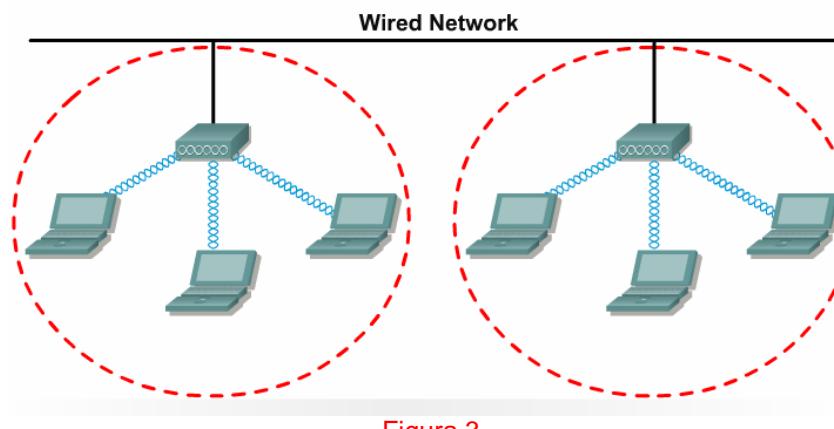


Figura 3

El DS habilita el soporte a dispositivos móviles proporcionando los servicios necesarios para manipular el mapeo de dirección a destino y la integración sin fisuras de múltiples BSSs. Los datos se desplazan entre un BSS y el DS a través de un AP. Nótese que todos los APs son también STAs, lo cual los convierte en entidades direccionables.

Conjunto de servicios extendido (ESS)

Un conjunto de servicios extendido (ESS) se define como dos o más BSSs conectados por medio de un DS común, como lo ilustra la Figura 3. Esto permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios. Al igual que sucede con un BSS, todos los paquetes de un ESS deben atravesar uno de los APs.

Un concepto clave es que la red ESS parece la misma para la capa LLC que una red IBSS o que una única red BSS. Las estaciones que se encuentran dentro de un ESS pueden comunicarse y las estaciones móviles pueden desplazarse de un BSS a otro (dentro del mismo ESS), de manera transparente a LLC.

Roaming

Roaming es el proceso o capacidad de un cliente inalámbrico de desplazarse de una celda, o BSS, a otra, sin perder conectividad con la red. Los access points se entregan el cliente entre sí y son invisibles al mismo. El estándar IEEE 802.11 no define cómo debería llevarse a cabo el roaming, pero sí define los bloques de construcción básicos, que incluyen la búsqueda activa y pasiva y un proceso de re-asociación. La re-asociación con el AP debe tener lugar cuando una STA hace roaming de un AP a otro.

2.2 Capa MAC 802.11

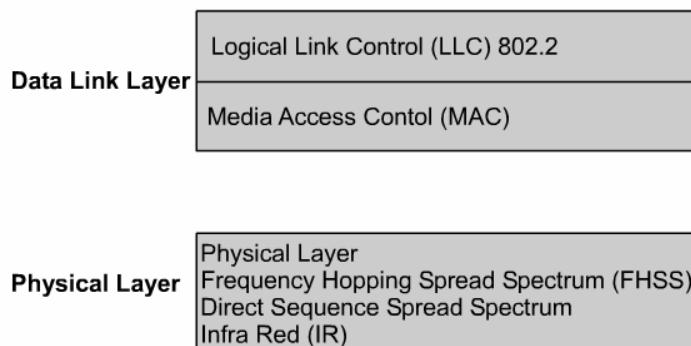
2.2.1 Servicios MAC

Un aspecto de la definición de estándares para una red inalámbrica interoperable es proporcionar estándares para servicios en las capas MAC y física (PHY). Esta sección tratará los estándares de la capa MAC, mientras que la siguiente sección tratará los servicios de la capa física. Tres servicios son proporcionados por la subcapa MAC en IEEE 802.11. Estos servicios son los siguientes:

1. Servicio de datos asíncronos
2. Servicios de seguridad
3. Ordenamiento de MSDUs

Servicio de datos asíncronos

Este servicio proporciona a las entidades peer LLC la capacidad para intercambiar unidades de datos de servicios MAC (MSDUs). Para soportar este servicio la MAC local utiliza los servicios de nivel PHY subyacentes para transportar una MSDU a una entidad MAC peer, donde se la entregará a la LLC peer. Ese transporte MSDU asíncrono se lleva a cabo sobre una base de mayor esfuerzo y sin conexión. No existen garantías de que la MSDU se entregará exitosamente. El transporte broadcast y multicast es parte del servicio de datos asíncrono proporcionado por la MAC. Debido a las características del medio inalámbrico, las MSDUs broadcast y multicast pueden experimentar una más baja calidad de servicio, en comparación a la de las MSDUs unicast. Todas las STAs soportan el servicio de datos asíncrono.



Servicios de seguridad

Los servicios de seguridad de IEEE 802.11 son proporcionados por el servicio de autenticación y el mecanismo de Privacidad Equivalente a la Cableada (WEP). El alcance de los servicios de seguridad proporcionados se limita a un intercambio de datos de estación a estación. El servicio de privacidad ofrecido por la implementación WEP IEEE 802.11 es el cifrado de la MSDU. Para los propósitos de este estándar, WEP se visualiza como servicio de capa lógica ubicado dentro de la subcapa MAC. La implementación real del servicio WEP es transparente para la LLC y para las otras capas que se encuentran por encima de la subcapa MAC. Los servicios de seguridad proporcionados por la WEP en IEEE 802.11 fueron diseñados para soportar los siguientes objetivos de seguridad:

- Confidencialidad
- Integridad de los datos
- Control de acceso

WEP y otros servicios de seguridad se tratan en detalle en próximos módulos.

Ordenamiento de MSDUs

Los servicios proporcionados por la subcapa MAC permiten, y pueden requerir, el reordenamiento de las MSDUs. La MAC reordenará intencionalmente las MSDUs, sólo si es necesario para aumentar la

probabilidad de una entrega exitosa basada en el modo operativo actual ("administración de energía") de la(s) estación o estaciones receptora(s). El único efecto de este reordenamiento es un cambio en el orden de la entrega de MSDUs broadcast y multicast. Este cambio es relativo a MSDUs dirigidas, o unicast, que se originan desde una única dirección de estación de origen. A las MSDUs unicast se les otorga prioridad sobre las multicast y broadcast.

2.2.2 Estructura, arquitectura y operación de frames MAC

Todas las estaciones deben construir frames para la transmisión y decodificación de los frames al recibirlos, basándose en un formato de frames estándar. Las unidades de datos del protocolo MAC (MPDUs), o frames, se describen como una secuencia de campos en un orden específico, como lo muestra la actividad que aparece más abajo.

Cada frame consiste en los siguientes componentes básicos:

- Un encabezado MAC, que consiste en información acerca del control de frames, la duración, la dirección y el control de las secuencias
- Un cuerpo de frames de longitud variable, que contiene información específica del tipo de frame. Por ejemplo, en los frames de datos, esto contendría datos de la capa superior
- Una secuencia de verificación de frames (FCS), que contiene una verificación de redundancia cíclica (CRC) IEEE de 32 bits

Tipos de frames

Los tres tipos principales de frames utilizados en la capa MAC son los siguientes:

1. Frames de datos
2. Frames de control
3. Frames de administración

Los frames de datos se utilizan para la transmisión de datos. Los frames de control, como la Solicitud para Enviar (RTS), Despejado para Enviar (CTS) y Confirmación (ACK), controlan el acceso al medio utilizando frames RTS, CTS y ACK. Los frames de administración, como los frames baliza, se transmiten de la misma manera en que los frames de datos intercambian la información de administración, pero no se envían a las capas superiores.

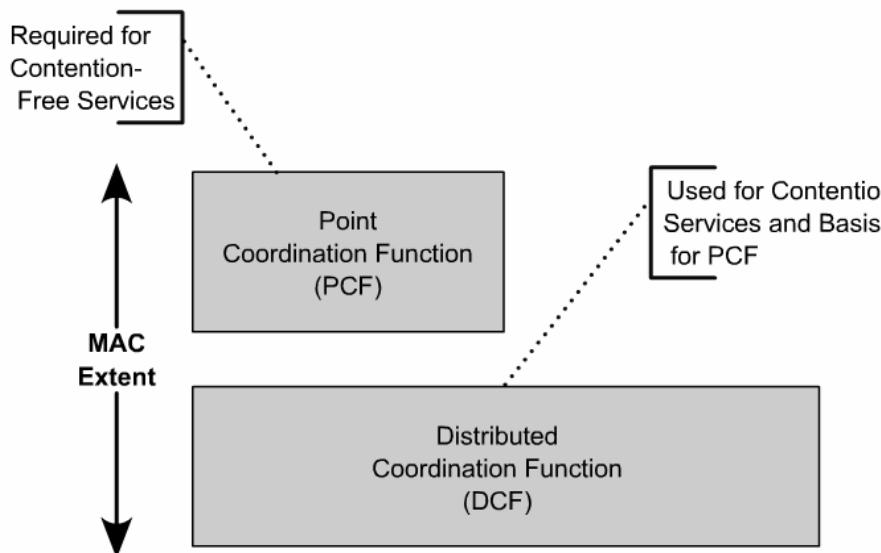


Figura 1

Arquitectura MAC

Antes de transmitir un frame, una STA debe obtener acceso al medio utilizando uno de dos métodos, que se muestran en la Figura 1:

1. El método de acceso fundamental del MAC IEEE 802.11, acceso múltiple con detección de portadora y colisión evitable (CSMA/CA), se denomina Función de Coordinación Distribuida (DCF). La DCF se implementa en todas las STAs, para su uso tanto en configuraciones de red ad hoc como de infraestructura.
2. El MAC IEEE 802.11 MAC también puede incorporar un método de acceso opcional, denominado Función de Coordinación de Punto (PCF), que crea un acceso libre de contención (CF). La PCF sólo puede utilizarse en configuraciones de red de infraestructura.

Coexistencia de DCF y PCF

La DCF y la PCF pueden operar ambas concurrentemente dentro del mismo BSS. Cuando éste es el caso, los dos métodos de acceso se alternan, con un periodo de CF seguido por un periodo de contención. Además, todas las transmisiones bajo la PCF pueden utilizar el Espacio Interframe (IFS), que es más pequeño que el utilizado para los frames transmitidos por medio de la DCF. El uso de IFSs más pequeños implica que el tráfico coordinado por punto tendrá un acceso de prioridad al medio a través de STAs que operan en modo DCF.

2.2.3 Mecanismos de detección de portadora, confirmaciones del nivel de la MAC, y espacios interframe

Mecanismo de detección de portadora

Las funciones de detección de portadora físicas y virtuales se utilizan para determinar el estado del medio. Cuando alguna de estas funciones indica un medio ocupado, el medio se considera ocupado. Si el medio no está ocupado, se considerará inactivo. Un mecanismo de detección de portadora físico es proporcionado por la PHY. Los detalles de la detección de portadora física se proporcionan en las especificaciones individuales de la PHY.

El MAC proporciona un mecanismo de detección de portadora virtual. Este mecanismo se denomina vector de adjudicación de la red (NAV). El NAV mantiene una predicción del tráfico futuro en el medio, basado en la información del campo de duración de los frames unicast. La información respecto a la duración también está disponible en los encabezados MAC de todos los frames enviados durante el CP.

Confirmaciones del nivel de la MAC

La recepción de algunos frames requiere que la estación receptora responda con una confirmación, en general un frame ACK, si la Secuencia de Verificación de Frames (FCS) del frame recibido es correcta. Esta técnica se conoce como confirmación positiva y se muestra en la Figura 1.

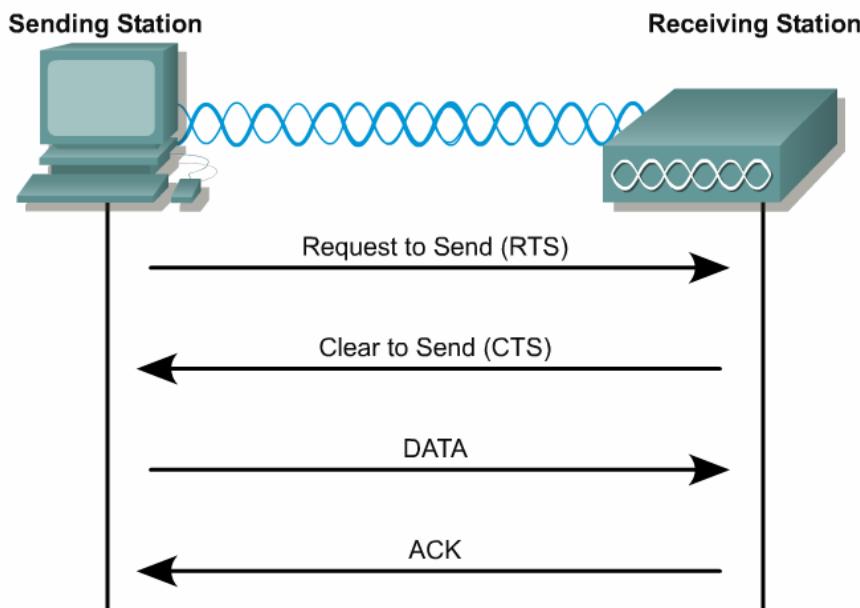


Figura 1

La falta de recepción de un frame ACK esperado indica a la estación de origen que ha ocurrido un error. Puede ser posible que la estación de destino haya recibido el frame correctamente y que el error haya ocurrido en la entrega del frame ACK. Para el iniciador del intercambio de frames, estas dos condiciones son indistinguibles entre sí.

Espacio interframe (IFS)

El intervalo entre frames se denomina espacio interframe (IFS). Cada intervalo IFS se define como el tiempo desde el último bit del frame anterior al primer bit del preámbulo del frame subsiguiente, como se aprecia en la interfaz aérea. Como se muestra en la Figura 2, cuatro IFSs diferentes se definen para proporcionar niveles de prioridad para un acceso al medio inalámbrico. Los IFSs se enumeran en orden, desde el más corto al más largo:

1. SIFS es el espacio interframe corto

2. PIFS es el espacio interframe PCF
3. DIFS es el espacio interframe DCF
4. EIFS es el espacio interframe extendido

Los diferentes IFSs son independientes de la velocidad de bits de la STA. Las temporizaciones del IFS se definen como aberturas temporales en el medio y son fijas para cada PHY.

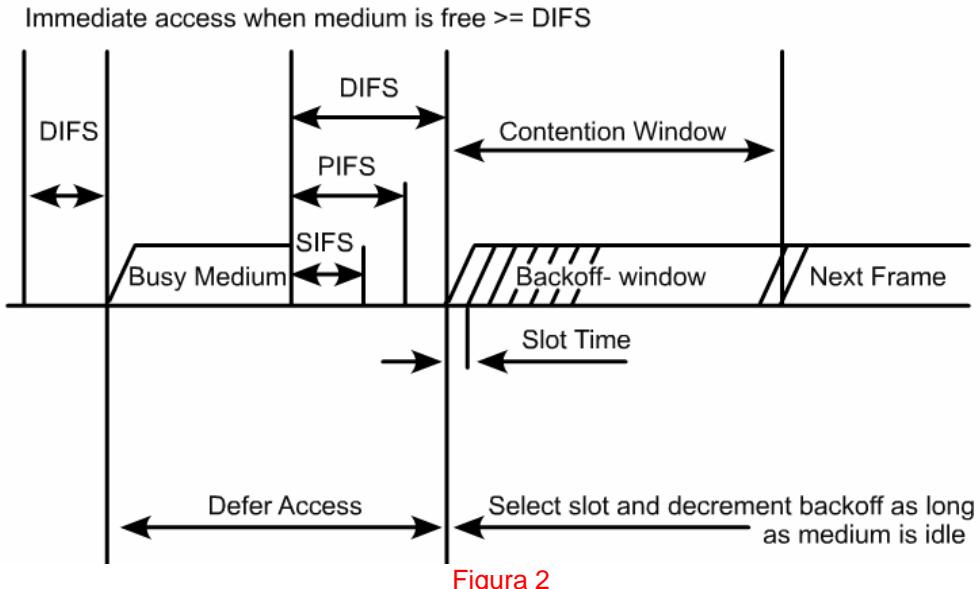


Figura 2

2.3 Capa Física (PHY)

2.3.1 Alcance y funciones

La capa MAC es sólo la mitad de la operación total de 802.11. El estándar de capa física (PHY) es la otra mitad. La mayoría de las definiciones de PHY contienen tres entidades funcionales, como lo muestra la Figura 1. Diferentes PHYs se definen como parte del estándar IEEE 802.11.

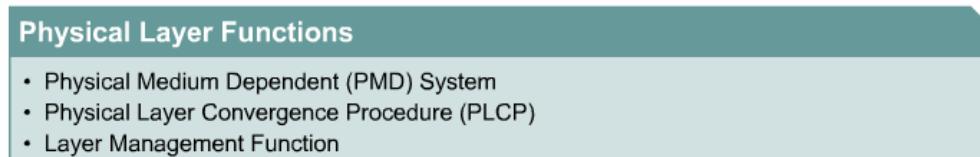


Figura 1

Procedimiento de convergencia de la capa física (PLCP)

La función de convergencia de PHY adapta las capacidades del sistema dependiente del medio físico (PMD) para el servicio MAC. PLCP define un método para mapear las unidades de datos de protocolo de subcapa MAC (MPDUs) en un formato de framing apto para su envío y recepción entre dos o más STAs utilizando el sistema PMD asociado. El PHY intercambia unidades de datos de protocolo PHY (PPDUs) que contienen una MPDU, más información adicional acerca de encabezados para los transmisores y receptores de la capa física. El PLCP también entrega frames entrantes desde el medio inalámbrico a la subcapa MAC. El servicio de PHY es proporcionado a la entidad MAC de la STA a través de un access point de servicio (SAP), denominado SAP PHY, como lo muestra la Figura 2.

Sistema dependiente del medio físico (PMD)

El sistema PMD define las características y métodos de transmisión y recepción de datos a través de un medio inalámbrico entre dos o más STAs, cada una de ellas utilizando el mismo sistema PHY.

También se definen conjuntos de primitivos, para describir la interfaz entre el PLCP y la subcapa PMD. La interfaz se denomina SAP PMD y también se muestra en la Figura 2.

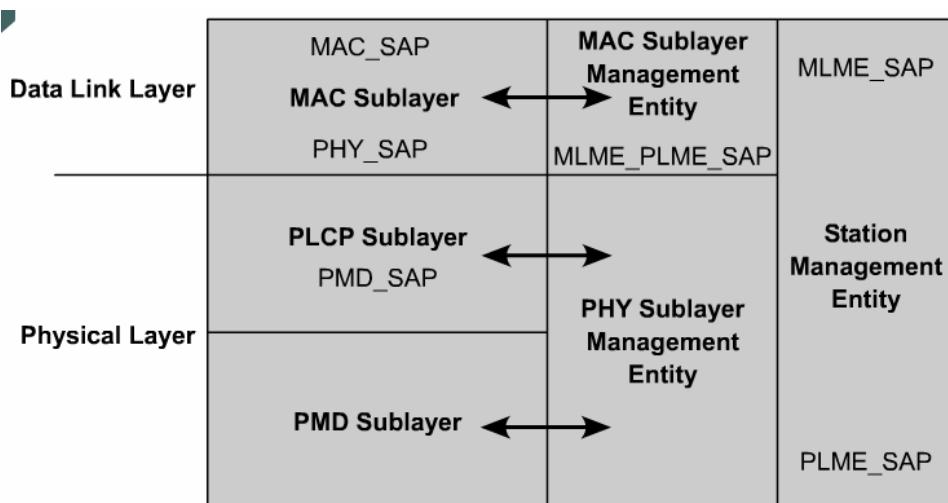


Figura 2

La subcapa PMD acepta los primitivos del servicio de la subcapa PLCP y proporciona el medio mediante el cual se transmiten o reciben realmente los datos provenientes del medio. El flujo de datos, la información de temporización y los parámetros de la señal recibidos se entregan a la subcapa PLCP. Una funcionalidad similar se proporciona para la transmisión de datos. Esto se ilustra en la Figura 3.

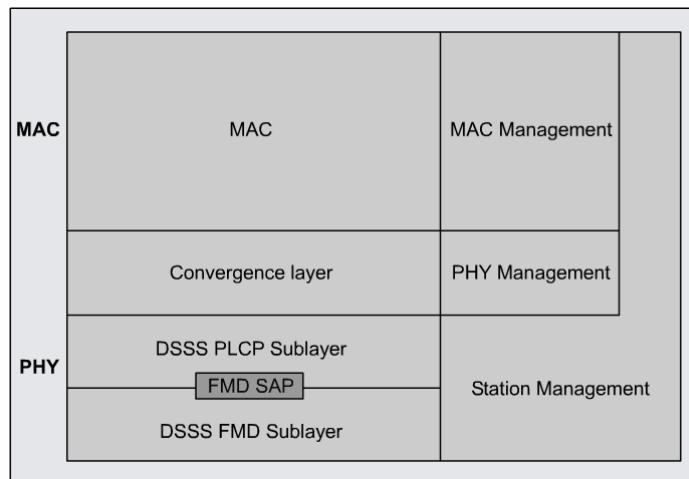


Figura 3

2.3.2 Especificación PHY DSSS IEEE 802.11b (Alta Velocidad)

Esta sección se concentra en la extensión de Alta Velocidad de 1999 de la PHY para el sistema de Espectro Expandido de Secuencia Directa (HR/DSSS). El estándar 802.11b es conocido como PHY de Alta Velocidad para la banda de 2,4 GHz diseñada para las aplicaciones ISM. También se conoce como WiFi.

Números de canales operativos

Las frecuencias centrales del canal y los números de CHNL_ID se muestran en la Figura 1. Como se muestra en la figura, no todos los cuerpos regulatorios de todos los países han adjudicado la misma cantidad de canales. Los tres canales operativos no superpuestos para Norteamérica se muestran en la Figura 2.

Modulación y velocidades de datos del canal

Se especifican cuatro formatos de modulación y velocidades de datos para la PHY de Alta Velocidad. La velocidad de acceso básico se basará en la modulación de afinación de desplazamiento de fase binaria diferencial (DBPSK) de 1 Mbps. La velocidad de acceso mejorada se basa en una afinación de desplazamiento de fase de cuadratura diferencial (DQPSK) de 2 Mbps. La especificación de secuencia directa extendida define dos velocidades de datos adicionales. Las velocidades de acceso de Alta Velocidad se basan en el sistema de modulación de la Codificación de Código Complementario (CCK) para 5,5 Mbps y 11 Mbps. La codificación de circunvolución binaria de paquetes (PBCC) opcional también se proporciona para un desempeño mejorado de hasta 22 Mbps.

Channel Frequencies for 802.11b (High Rate PHY)							
		Regulatory Domains					
CHNL_ID	Frequency MHz	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412	X	X	X	-	-	-
2	2417	X	X	X	-	-	-
3	2422	X	X	X	-	-	-
4	2427	X	X	X	-	-	-
5	2432	X	X	X	-	-	-
6	2437	X	X	X	-	-	-
7	2442	X	X	X	-	-	-
8	2447	X	X	X	-	-	-
9	2452	X	X'	X	-	-	-
10	2457	X	X	X	X	X	-
11	2462	X	X	X	X	X	-
12	2467	-	-	X	-	X	-
13	2472	-	-	X	-	X	-
14	2484	-	-	-	-	-	X

Figura 1

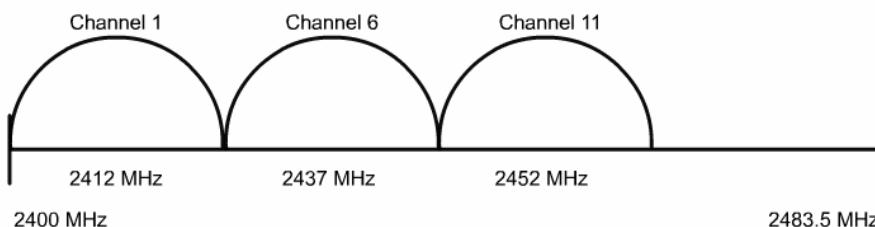


Figura 2

Spreading Code		Modulation Technology	Data Rate
2.4 GHz DSSS	Barker Code	DBPSK	1 Mbps
2.4 GHz DSSS	Barker Code	DQPSK	2 Mbps
2.4 GHz DSSS	CCK	DQPSK	5.5 Mbps
2.4 GHz DSSS	CCK	DQPSK	11 Mbps

Figura 3

La Codificación de Código Complementario (CCK) se utiliza para incrementar la velocidad de datos pico de 802.11b de 2 a 11 Mbps, a la vez que se utiliza la modulación DQPSK. Hace esto incrementando en primer lugar la velocidad de reloj de datos de 1 Mbps a 1,375 Mbps, y luego tomando los datos en bloques de 8 bits ($8 \times 1,375 = 11$). Seis de los ocho bits se utilizan para escoger 1 de 64 códigos complementarios, que tienen cada uno ocho chips de largo y se cronometran en 11 MHz. Los otros 2 bits se combinan con el código del modulador DQPSK.

2.3.3 Modulación 802.11b

Esta extensión del sistema DSSS se basa en las capacidades de velocidades de datos del estándar 802.11 original, para proporcionar tasas de datos con una carga de 5,5 Mbps y 11 Mbps. Las primeras velocidades de 1 Mbps y 2 Mbps aún se soportan. Para proporcionar las velocidades más altas, se emplea la codificación de código complementario (CCK) de 8 chips como sistema de modulación. La velocidad de chipping es de 11 MHz, que es igual a la del sistema DSSS, proporcionando así el mismo ancho de banda del canal ocupado. La PHY de Alta Velocidad básica utiliza el mismo preámbulo PLCP que la PHY DSSS, por lo cual ambas PHYs pueden co-existir en el mismo BSS.

Además de proporcionar extensiones de más alta velocidad al sistema DSSS, una cantidad de funciones opcionales permiten mejorar el desempeño del sistema LAN de frecuencia de radio.

Se han definido las siguientes funciones opcionales:

- Un modo opcional puede reemplazar la modulación CCK por la codificación de circunvolución binaria de paquetes (HR/DSSS/PBCC). Esta extensión opcional también se aplica a 802.11g, que puede operar a velocidades de hasta 54 Mbps.
 - Un modo opcional puede permitir que un throughput de datos a las velocidades más altas de 2, 5,5, y 11 Mbps se incremente significativamente utilizando un preámbulo PLCP más corto. Este modo se denomina HR/DSSS/corto, o HR/DSSS/PBCC/corto. Este modo de preámbulo corto puede coexistir con DSSS, HR/DSSS, o HR/DSSS/PBCC bajo circunstancias limitadas, como en diferentes canales. El formato estándar y más largo se muestra en la Figura 1 y el formato opcional más corto se muestra en la Figura 2. La extensión de IEEE 802.11a a 802.11 incluye una función similar, denominada secuencia de capacitación corta o larga.
 - Una capacidad opcional para la agilidad del canal permite que una implementación supere dificultades inherentes a las asignaciones de canal estáticas. Esta opción puede utilizarse para implementar sistemas que cumplen con IEEE 802.11 que sean interoperables con modulaciones tanto FH como DS.

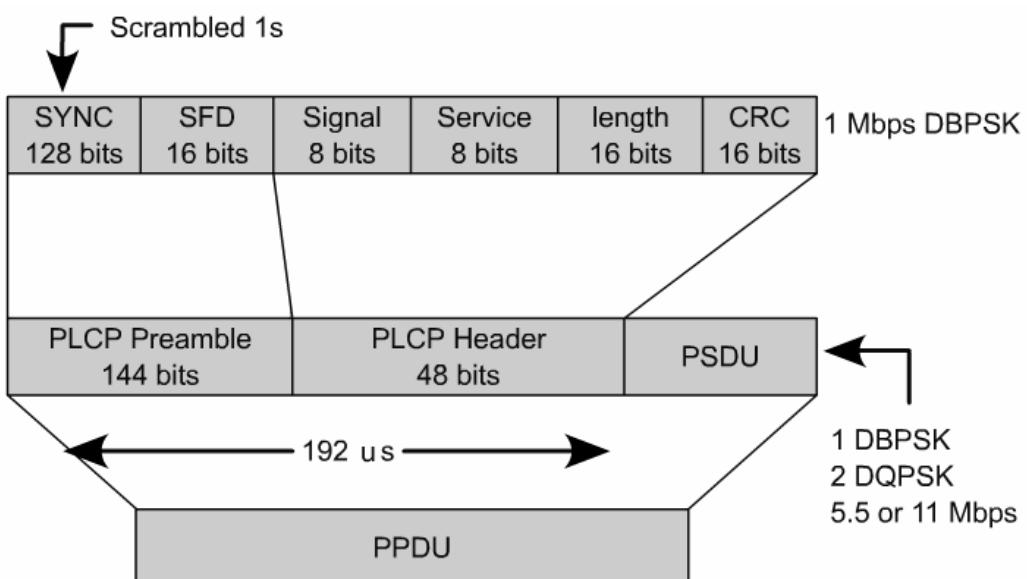


Figura 1

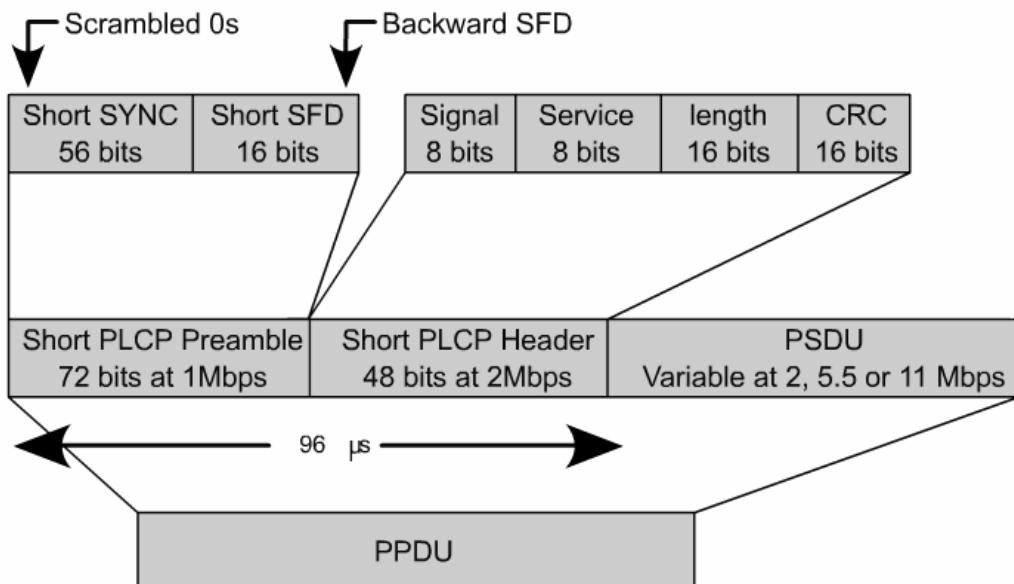


Figura 2

2.3.4 Especificación de PHY IEEE 802.11a

Los productos que cumplen con el estándar 802.11a permitirán a las WLANs lograr velocidades de datos tan altas como 54 Mbps. Los dispositivos IEEE 802.11a operan en el rango de frecuencia de 5 GHz. Es desde esta frecuencia más alta que el estándar obtiene parte de su rendimiento. El resto proviene de la combinación de las técnicas de codificación y modulación utilizadas.

802.11a se desplazó a una frecuencia más amplia (5 GHz) en parte para obtener velocidades más altas, pero también para evitar problemas de interferencia en la banda más poblada de los 2,4 GHz. Además de las WLANs 802.11b, las LANs HomeRF, los dispositivos Bluetooth, los teléfonos inalámbricos e incluso los hornos a microondas operan todos en la banda de los 2,4 GHz.

Los beneficios de utilizar el espectro de 5 GHz son contrarrestados por la falta de compatibilidad con la generación de LANs 802.11b, porque las frecuencias no coinciden. Muchos fabricantes están tratando este problema fabricando productos de modo dual que realmente contienen dos radios, una que opera en el rango de los 2,4 GHz, y una que opera en el rango de los 5 GHz.

Multiplexado por división de frecuencia ortogonal (OFDM)

El estándar IEEE 802.11a utiliza multiplexado por división de frecuencia ortogonal, una técnica que divide un canal de comunicaciones en una cierta cantidad de bandas de frecuencia que se encuentran separadas por el mismo espacio. OFDM utiliza múltiples subportadoras, que son 52, separadas por 312,5 KHz. Los datos se envían por 48 portadoras simultáneamente, donde cada subportadora transporta una porción de los datos del usuario. Cuatro subportadoras se utilizan como pilotos. Las subportadoras son ortogonales (independientes) entre sí.

El tiempo para transmitir cada bit se incrementa en proporción a la cantidad de portadoras. Esto hace al sistema menos sensible a la interferencia multiruta, una fuente importante de distorsión. La Figura 1 muestra los diferentes sistemas de codificación y modulación utilizados por 802.11a, junto con las velocidades de datos correspondientes.

Coding Technique	Modulation technology	Data Rate
OFDM	BPSK	6 Mbps
OFDM	BPSK	9 Mbps
OFDM	QPSK	12 Mbps
OFDM	QPSK	18 Mbps
OFDM	16QAM	24 Mbps
OFDM	16QAM	36 Mbps
OFDM	64QAM	48 Mbps
OFDM	64QAM	54 Mbps

Figura 1

2.3.5 Especificación de PHY IEEE 802.11g

IEEE 802.11a proporciona velocidades de hasta 54 Mbps. El problema más importante de 802.11a, que se especificó al mismo tiempo que 802.11b, es que utiliza la banda de frecuencia de 5 GHz en lugar de la de 2,4 GHz. Esto impide la compatibilidad con productos anteriores y representa un bloqueo considerable a la difusión de su implementación. El grupo de trabajo IEEE 802.11 aprobó recientemente el estándar IEEE 802.11g. No obstante, el estándar no ha sido aprobado aún como definitivo. Se espera que el estándar se publique (finalice) en julio de 2003. Proporciona la misma velocidad máxima que 802.11a, que es de 54 Mbps, pero opera en el mismo espectro de 2,4 GHz que los otros estándares de WLAN existentes. Existe una interoperabilidad entre todas las velocidades, por lo cual no es necesario actualizar toda la WLAN al desplazarse a velocidades más elevadas. Las velocidades de datos operativas para los diferentes estándares 802.11, junto con la banda de frecuencia y modulación utilizadas, se resumen en la Figura 1.

Set	Number of Channels	HR/ DSSS Channel Numbers
1	3	1, 6, 11
2	6	1, 3, 5, 7, 9, 11

Figura 1

El IEEE seleccionó a OFDM, la misma tecnología utilizada en las redes 802.11a, como base para el estándar de la red 802.11g. La forma de onda OFDM multiportadora es superior en casi cada aspecto a la forma de onda CCK de portadora única utilizada en 802.11b. Ofrece velocidades mucho más altas, un mayor alcance y una mejor tolerancia de ecos multiruta, que son comunes en las aplicaciones del interior de los edificios.

El estándar 802.11g requiere el uso de OFDM para velocidades de datos rápidas (mayores que 20 Mbps), así como compatibilidad con la codificación CCK 802.11b. Aunque la arquitectura híbrida no es tan eficiente como OFDM pura, es atractiva. Incluso aunque los dispositivos 802.11b de legado no podrán decodificar la carga de paquetes de estos frames, pueden "detectarlos" en la red. Los nuevos frames pueden coexistir con 802.11b, de manera similar a la forma en la cual 802.11b puede coexistir con sistemas 802.11 más antiguos de 2 Mbps.

La especificación OFDM pura, que utiliza un preámbulo/encabezado basado en OFDM más eficiente, no tiene las mismas características. Los dispositivos 802.11b no detectarán los frames 802.11g, y viceversa. Aprovechando los elementos RTS/CTS de IEEE 802.11, en el cual los access points que hablan ambos lenguajes pueden regular las transmisiones, los dos pueden coexistir pacíficamente.

2.3.6 Especificaciones de PHY de FHSS e Infrarrojo (IR)

El Espectro Expandido de Salto de Frecuencia (FHSS) y el Infrarrojo (IR) son dos de las diversas especificaciones de PHY disponibles. IR y FHSS no se utilizan ampliamente hoy en día. DSSS y OFDM son las tecnologías más comunes actualmente en uso.

FHSS

El estándar 802.11 define un conjunto de canales FH espaciados de manera pareja a lo largo de la banda de 2,4 GHz. La cantidad de canales, como ocurre con DSSS, depende de la geografía. Puede haber hasta 79 canales en Norteamérica y en la mayor parte de Europa, y 23 canales en Japón. El rango de frecuencia exacta varía levemente según la ubicación.

El PMD FHSS transmite PPDUs saltando de canal a canal, de acuerdo a una secuencia de salto pseudo-aleatoria particular que distribuye uniformemente la señal a través de la banda de frecuencia operativa. Una vez que la secuencia de saltos se configura en un AP, las estaciones se sincronizarán automáticamente según la secuencia de salto correcta. Tres conjuntos de secuencias de salto válidas están definidas.

El PMD utiliza una modulación de codificación de desplazamiento de frecuencia de Gauss (GFSK) de dos niveles para transmitir a 1 Mbps. Un seno de modulación GFSK de cuatro niveles se utiliza para transmitir a 2 Mbps. Las estaciones que operan a 2 Mbps también deben poder operar a 1 Mbps.

PHY infrarroja (IR)

La PHY IR utiliza luz casi visible en el rango de los 850 nm a los 950 nm para la señalización. Esto es similar al uso espectral de dispositivos comunes entre los consumidores tales como controles remotos infrarrojos, así como otro equipamiento de comunicaciones de datos, como los dispositivos de la Asociación de Datos Infrarrojos (IrDA). A diferencia de muchos otros dispositivos infrarrojos, la PHY IR no está dirigida. Esto significa que el receptor y el transmisor no tienen que estar dirigidos uno al otro y no necesitan una línea de visión clara. Esto permite construir con más facilidad un sistema WLAN inalámbrico. Un par de dispositivos infrarrojos que cumplen con las normas podrían comunicarse en un entorno típico a un rango de alrededor de 10 m (33 pies). Este estándar permite receptores más sensibles, que pueden incrementar el rango hasta en 20 m (66 pies).

La PHY IR se basa tanto en energía infrarroja reflejada como en energía infrarroja de línea de visión para las comunicaciones. La mayoría de los diseños anticipan que toda la energía del receptor sea energía reflejada. Esta forma de transmisión basada en la energía infrarroja se denomina transmisión infrarroja difusa.

La PHY IR operará sólo en entornos de interiores. La radiación infrarroja no pasa a través de las paredes, y se ve significativamente atenuada al pasar a través de la mayoría de las ventanas que dan al exterior. Esta característica puede utilizarse para "contener" una PHY IR en una única habitación física, como un aula o una sala de conferencias. Diferentes LANs que utilizan la PHY IR pueden operar en salas adyacentes separadas sólo por una pared, sin interferencia y sin la posibilidad de que ocurra una escucha no deseada.

Actualmente no existe ninguna restricción regulatoria respecto a la adjudicación de frecuencia o a la adjudicación de ancho de banda sobre las emisiones infrarrojas. El emisor, en general, un diodo

electroluminiscente, LED, y el detector, en general, un diodo PIN, utilizados para las comunicaciones infrarrojas son de relativamente bajo costo en las longitudes de onda infrarrojas especificadas en la PHY IR y en las frecuencias operativas eléctricas requeridas por esta PHY.

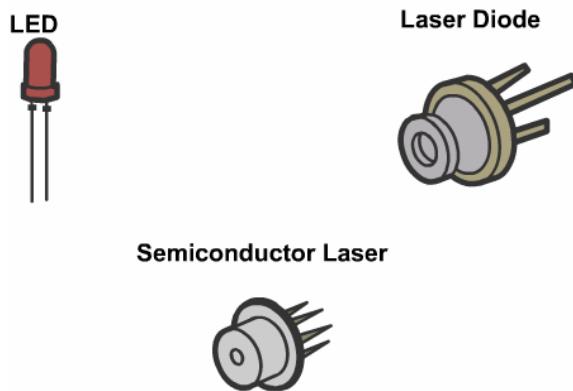


Figura 1

2.4 Adaptadores Clientes

2.4.1 Introducción

Los Adaptadores de WLAN Cisco Aironet Inalámbricos también se denominan adaptadores clientes. Son módulos de radio que proporcionan comunicaciones de datos inalámbricas entre dispositivos fijos, portátiles o móviles y otros dispositivos inalámbricos o una infraestructura de red cableada. Los adaptadores clientes son completamente compatibles cuando se los utiliza en dispositivos que soportan la tecnología Plug-and-Play (PnP).

La función principal de los adaptadores de clientes es transferir paquetes de datos a través de la infraestructura inalámbrica. Los adaptadores operan de manera similar a un producto de red estándar, excepto en que el cable se reemplaza por una conexión de radio. No se requiere ninguna función de networking especial, y todas las aplicaciones existentes que operan a través de una red operarán utilizando los adaptadores.

Los cinco adaptadores de clientes Cisco se ilustran en las Figuras 1 a 5 y se describen a continuación:



Figura 1



Figura 2



Figura 3



Figura 4



Figura 5

- El Adaptador Cliente de placa de PC Serie 350 que se muestra en la Figura 1 también se denomina placa de PC. Las placas de PC tienen una antena integrada. Un módulo de radio de placa PCMCIA puede insertarse en cualquier dispositivo equipado con un slot de placa de PC Tipo II o Tipo III. Los

dispositivos host pueden incluir laptops, computadoras notebook, asistentes digitales personales y dispositivos handheld o portátiles.

- El Adaptador Cliente de placa LM Serie 350, también denominado placa LM, es también un módulo de radio de placa PCMCIA, que puede insertarse en cualquier dispositivo equipado con un slot de placa de PC Tipo II o Tipo III. La principal diferencia entre éste y el adaptador de placa de PC es que la placa LM no incluye una antena incorporada. Los dispositivos de host incluyen a dispositivos handheld o portátiles. La placa LM se muestra en la Figura 2.
- El Adaptador Cliente PCI Serie 350 es un módulo de radio de placa adaptadora cliente, que puede insertarse en cualquier dispositivo equipado con un slot de expansión PCI vacío, como una computadora de escritorio. Estas placas se venden en general con una antena que se conecta externamente. La Figura 3 ilustra un adaptador cliente PCI.
- El Adaptador Mini-PCI Serie 350 (MPI350) es una solución incorporada que complementa al Cisco Aironet Serie 350 de 11 Mbps, líder de la industria. 4 El Mini-PCI está disponible para que los fabricantes de laptops proporcionen un soporte 802.11b integrado. El Mini-PCI también se utiliza en el AP Cisco 1100 y en el AP 1200 para proporcionar 802.11b.
- El Adaptador Cliente WLAN Cisco Aironet® de 5 GHz y 54 Mbps es un adaptador CardBus Tipo II que cumple con IEEE 802.11a. 5 El adaptador cliente complementa al Access Point Cisco Aironet Serie 1200 802.11a, proporcionando una solución que combina desempeño y movilidad con la seguridad y capacidad de administración que requieren las empresas.

2.4.2 Partes del adaptador cliente

El adaptador cliente se compone de tres partes principales, como lo muestra la Figura 1. Las tres partes de un adaptador cliente inalámbrico son una radio, una antena y un LED. Cada una de ellas se describe a continuación.

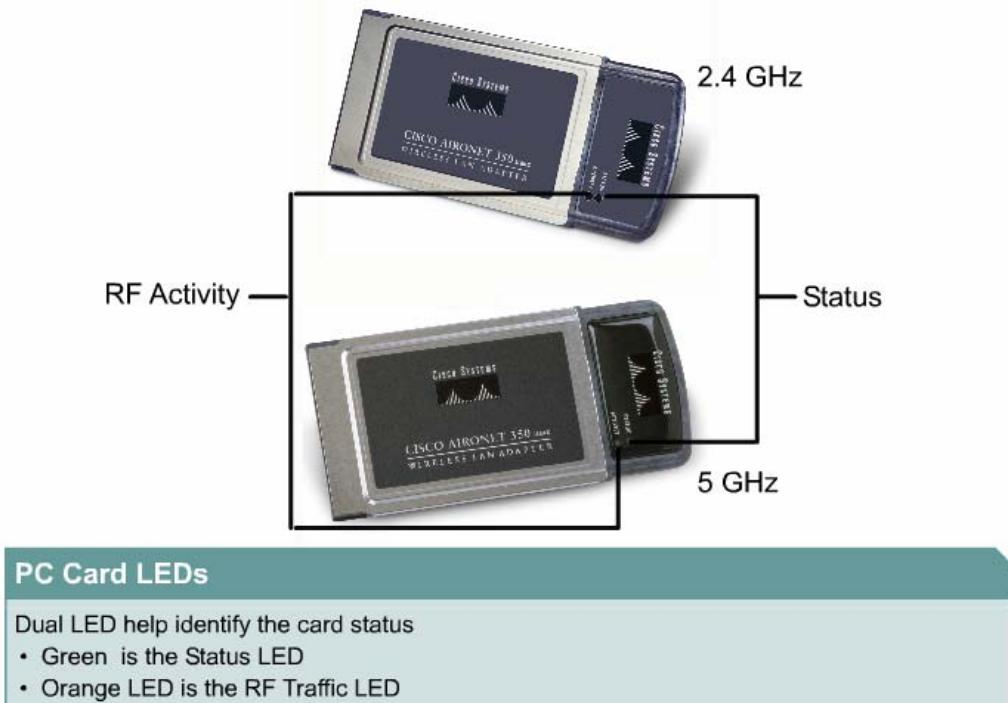


Figura 1

Radio

La radio transmite datos a través de un canal de radio semiduplex que opera a hasta 54 Mbps dependiendo de la tecnología inalámbrica.

Antena

El tipo de antena utilizada depende del adaptador cliente, de la siguiente manera:

- Las placas de PC poseen una antena integrada, conectada de manera permanente. El beneficio del sistema de antena de diversidad es un incremento en la cobertura. El sistema funciona permitiendo que la placa commute y muestre entre sus dos puertos de antena para seleccionar el puerto óptimo para recibir paquetes de datos. Como resultado de ello, la placa tiene mejores posibilidades de mantener la conexión de frecuencia de radio (RF) en áreas de interferencia. La antena está albergada dentro de la sección de la placa que sobresale del slot de la placa de PC cuando ésta se instala.

- Las placas LM se venden sin antena, aunque una antena puede conectarse a través de un conector externo de la placa. Si se utiliza una antena a presión, deberá operarse en modo de diversidad. De otro modo, el modo de antena utilizado deberá corresponderse con el puerto de la antena al cual está conectada la misma.
- Los adaptadores cliente PCI se venden con una antena dipolo de 2 dBi que se conecta al conector de antena del adaptador. No obstante, pueden utilizarse otros tipos de antenas. Los adaptadores cliente PCI pueden operarse únicamente a través del puerto de la antena correcta.

Diodos electroluminiscentes (LEDs)

El adaptador cliente tiene dos diodos electroluminiscentes (LEDs) que brillan o parpadean para indicar el estado del adaptador o para transportar indicaciones de errores. [1](#)Se describen los LEDs y su interpretación para la placa de PC de la Figura [2](#). El photozoom muestra usos del adaptador cliente PCI.

Green LED	Amber LED	Condition
Off	Off	Client adapter is not receiving power or an error has occurred
Blinking quickly	Blinking quickly	Power is on, self-test is OK, and client adapter is scanning for a network.
Blinking slowly	Blinking quickly	Client adapter is associated to an Access Point.
Continuously on or blinking slowly	Blinking	Client adapter is transmitting or receiving data while associated to an Access Point.
Off	Blinking quickly	Client adapter is in power save mode.
On	Blinking quickly	Client adapter is in ad hoc mode.
Off	On	Driver installed incorrectly.
Off	Blinking in a pattern	Indicates an error condition.

Figura 2

El LED verde de la placa de PC es el LED de estado. Tiene varios modos de operación:

- Si parpadea una vez cada medio segundo indica que la placa se encuentra operando en modo de infraestructura y está buscando un access point al cual asociarse.
- Si parpadea una vez cada dos segundos significa que la placa se encuentra en modo de infraestructura y está asociada a un access point.
- Una luz verde sin parpadeo significa que la placa está operando en modo ad hoc y no se comunicará con un AP.

El LED color ámbar es el LED de Tráfico RF. Tiene dos modos de operación principales:

- Una luz de LED color ámbar parpadeante indica tráfico RF
- Un LED color ámbar indica que la placa se está reinicializando y no se encuentra en modo operativo. En general esto significa que el controlador no se ha instalado o cargado apropiadamente.

Todas las combinaciones de ON/OFF posibles de los dos LEDs se muestran en la tabla de la Figura [2](#).

2.4.3 Tipos de controladores y soporte al cliente

Sistemas operativos Windows

La Figura [1](#)muestra los diversos entornos de SO Windows que pueden soportar controladores Aironet. El disco de controladores Aironet para Windows incluye controladores para todas las versiones de Windows 95 y 98, así como Windows ME, Windows NT, Windows 2000, Windows XP, y Windows CE 2.x, 3.x, y 4.x. Además, el controlador se incluye en el CD de Instalación de Windows para Windows Me, Windows 2000, y Windows XP.

Puesto que no todos los procesadores de Conjunto de Instrucciones Computacionales Reducidas (RISC) son similares, es necesario desarrollar una versión compilada separada del controlador según el procesador. Además, a causa de la naturaleza de Windows CE, es necesario desarrollar un controlador separado para cada versión. Finalmente, no todos los dispositivos CE adhieren a los estándares PCMCIA a causa de su tamaño limitado y una construcción que reduce costos. Esto significa que incluso con el controlador correcto para el procesador y la versión de CE, aún puede no funcionar. Una máquina no

funcionará si la placa del sistema muestra el mensaje "unknown card inserted" ["placa insertada desconocida"]. Deberá mostrarse el mensaje "network card inserted" ["placa de red insertada"]. En general, esto ocurre porque el fabricante no sigue completamente las especificaciones PC CARD 2.1, lo que resulta en problemas de incompatibilidad.

Supported Microsoft Operating Systems

Windows 95, 98, ME

Windows NT 4.x

Windows 2000

Windows XP

Binds to all protocol stacks within Windows

Windows CE

- Version 2.11
- Version 3.0

Figura 1

Sistemas operativos no Windows

Cisco Aironet ofrece soporte para Linux y Macintosh, según se muestra en la Figura 2. El controlador para Linux de Cisco Aironet se utiliza con cualquier versión de Linux que utilice las versiones de kernel 2.2.x o 2.4.x. El controlador para Macintosh de Cisco Aironet se utiliza con las PowerBooks Macintosh y PowerMacs que utilizan Mac OS 9.x o Mac OS X 10.1. El controlador no tiene como objetivo su uso en notebooks Macintosh que tengan una placa inalámbrica incorporada.

Other Supported Operating Systems

LINUX

- Version 2.2.x
- Version 2.4.x

Macintosh

- OS 9.x
- OS 10.x

Figura 2

Descarga de software inalámbrico desde Cisco Connection Online (CCO)

Todos los controladores, utilidades y firmware disponibles pueden descargarse desde Cisco Connection Online (CCO). Para obtener acceso a estos materiales necesitará un nombre de usuario y contraseña CCO. Obtener un nombre de usuario y contraseña CCO válidos requiere una cuenta de mantenimiento smartnet.

Desde la página principal de Cisco (www.cisco.com), seleccione Products and Services [Productos y Servicios] desde el menú desplegable. Haga clic en WLAN Products [Productos WLAN], y luego en Aironet WLAN Client Adapters [Adaptadores de Clientes WLAN Aironet]. A continuación, haga clic en Software Center [Centro de Software], a la izquierda, y en Software Center, nuevamente. Seleccione Wireless Software [Software para Sistemas Inalámbricos] y luego en Option 2: Aironet Wireless Software Display Tables [Opción 2: Tablas de Muestra de Software para Sistemas Inalámbricos Aironet]. La Opción 1 permite la descarga de controladores agrupados, por ejemplo, todos los controladores para Windows.

Las últimas actualizaciones a todo el firmware y software Cisco Aironet están disponibles a través de este enlace.

2.4.4 Configuraciones de red utilizando los adaptadores clientes

El adaptador cliente puede utilizarse en una variedad de configuraciones de red. En algunas configuraciones, los access points (APs) proporcionan conexiones a la red cableada o actúan como repetidores para incrementar el rango de comunicación inalámbrica. El rango de comunicación máximo se basa en cómo está configurada la red inalámbrica.

WLAN ad hoc

Una WLAN ad hoc, o peer-to-peer, es la configuración WLAN más simple. Se muestra en la Figura 1. En una WLAN que utiliza una configuración de red ad hoc, todos los dispositivos equipados con un adaptador cliente pueden comunicarse directamente entre sí. También se denomina conjunto de servicios básicos independientes (IBSS) o microcelda.

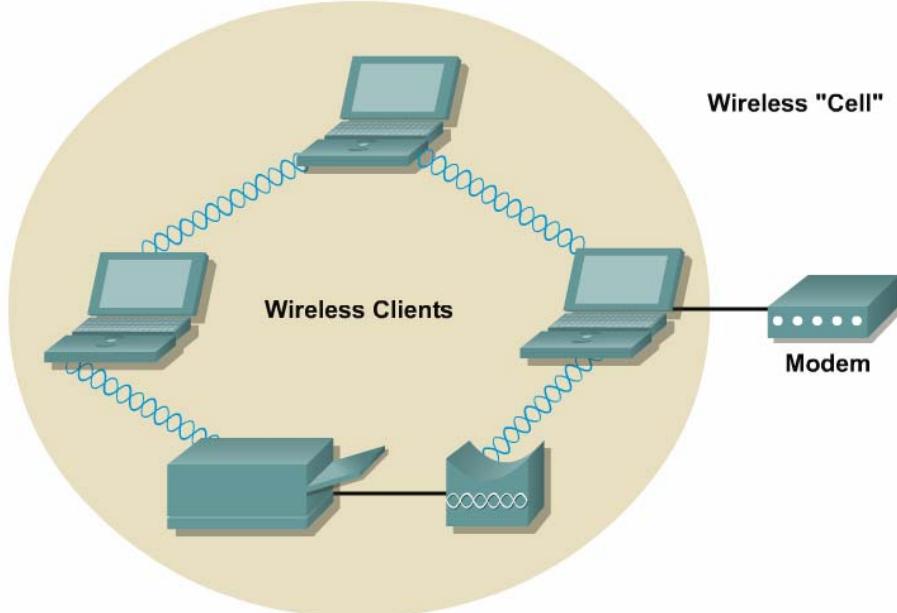


Figura 1

Los sistemas operativos como Windows 98 y Windows 2000 han hecho de este tipo de red algo fácil de configurar. Esta topología puede utilizarse para permitir que una pequeña oficina u oficina en el hogar se conecte a la PC principal, o que varias personas simplemente comparten archivos.

La desventaja principal de este tipo de red es la limitación de la cobertura. Todos deben poder escuchar a cada uno de los demás.

Infraestructura inalámbrica con estaciones de trabajo que acceden a una LAN Inalámbrica

Una WLAN que está conectada a una infraestructura cableada consiste en un conjunto de servicios básicos (BSS). Colocar dos o más access points en una LAN puede extender el BSS. La Figura 2 muestra una red microcelular del conjunto de servicios extendido (ESS), con estaciones de trabajo que acceden a una LAN cableada a través de access points.

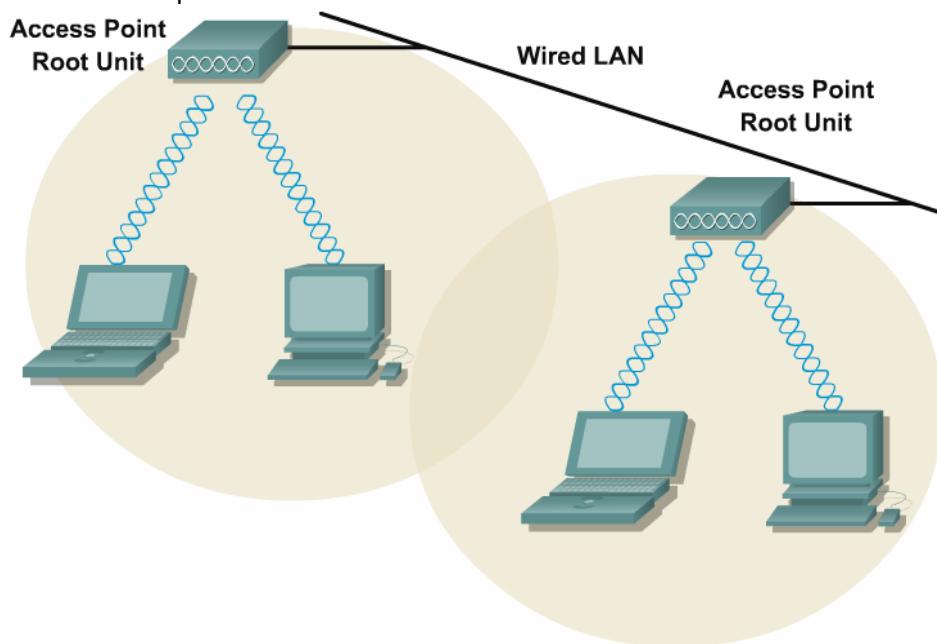


Figura 2

Esta configuración es útil en el caso de estaciones portátiles o móviles porque les permite conectarse directamente a la red cableada incluso al desplazarse de un dominio de microcelda a otro. Este proceso es transparente y la conexión al servidor de archivos se mantiene sin interrupciones. La estación móvil permanece conectada a un access point tanto tiempo como le resulte posible. Una vez que la STA sale fuera de alcance, la estación busca automáticamente y se asocia a otro AP. Este proceso se denomina roaming.

2.4.5 Ubicación de los productos inalámbricos

La determinación de la ubicación de la red de productos inalámbricos puede verse influenciada por una cantidad de factores. Las herramientas de estudio del sitio y de prueba del enlace proporcionadas por la utilidad del cliente Aironet (ACU) pueden ayudar a determinar la mejor ubicación para los access points y estaciones de trabajo dentro de la red inalámbrica. Las herramientas de prueba del enlace y estudio del sitio no son soportadas por el sistema operativo Linux.

Herramienta de estudio del sitio

A causa de las diferencias en la configuración, ubicación y entorno físico de los componentes, cada aplicación de la red es una instalación única. Antes de instalar el sistema, deberá llevarse a cabo un estudio del sitio para determinar la ubicación óptima de los componentes de networking. Esto se lleva a cabo para maximizar el alcance, la cobertura y el desempeño de la red. La Herramienta de Estudio del Sitio se muestra en la Figura 1.



Figura 1

Consideré las siguientes condiciones operativas y ambientales al llevar a cabo una encuesta del sitio:

- La sensibilidad y el alcance son inversamente proporcionales a las velocidades de bits de datos. El alcance máximo de la radio se logra a la velocidad de datos más baja con la que se puede trabajar. Tiene lugar una disminución en la sensibilidad umbral del receptor a medida que los datos de radio se incrementan.
- Una configuración apropiada de la antena es un factor crítico para maximizar el alcance de la radio. Como regla general, el alcance se incrementa proporcionalmente a la altura de la antena.
- El entorno físico es importante porque áreas despejadas o abiertas proporcionan un mejor alcance de la radio que las áreas cerradas o congestionadas. Cuanto menos atestado se encuentre el entorno de trabajo, mayor será el alcance.
- Una obstrucción física, como una estantería metálica o una columna de acero, pueden impedir el desempeño del adaptador cliente. Deberá evitarse la colocación de la estación de trabajo en un sitio donde exista una barrera metálica entre las antenas emisora y receptora.
- La penetración de las ondas de radio se ve muy influenciada por el material utilizado en la construcción. La construcción de muros de yeso permite un mayor alcance que los bloques de cemento armado. La construcción metálica o de acero es una barrera para las señales de radio.
- Puesto que el adaptador cliente es un dispositivo de radio, es susceptible a las obstrucciones RF y a fuentes comunes de interferencia que pueden reducir el throughput y el alcance. El adaptador cliente deberá instalarse lejos de los hornos a microondas. Los hornos a microondas operan en la misma frecuencia que el adaptador cliente y pueden ocasionar interferencia en la señal.

Herramienta de prueba del enlace

La herramienta de prueba del enlace se utiliza para determinar la cobertura RF. Los resultados de las pruebas pueden ayudar al instalador a eliminar áreas de bajos niveles de la señal RF que pueden resultar en una pérdida de conexión entre el adaptador cliente y el AP.

La Figura 2 ilustra la Herramienta de Prueba del Enlace ACU y la pantalla de Estadísticas. La pantalla de Estadísticas puede visualizarse haciendo clic en el botón de Estadísticas de la página principal.

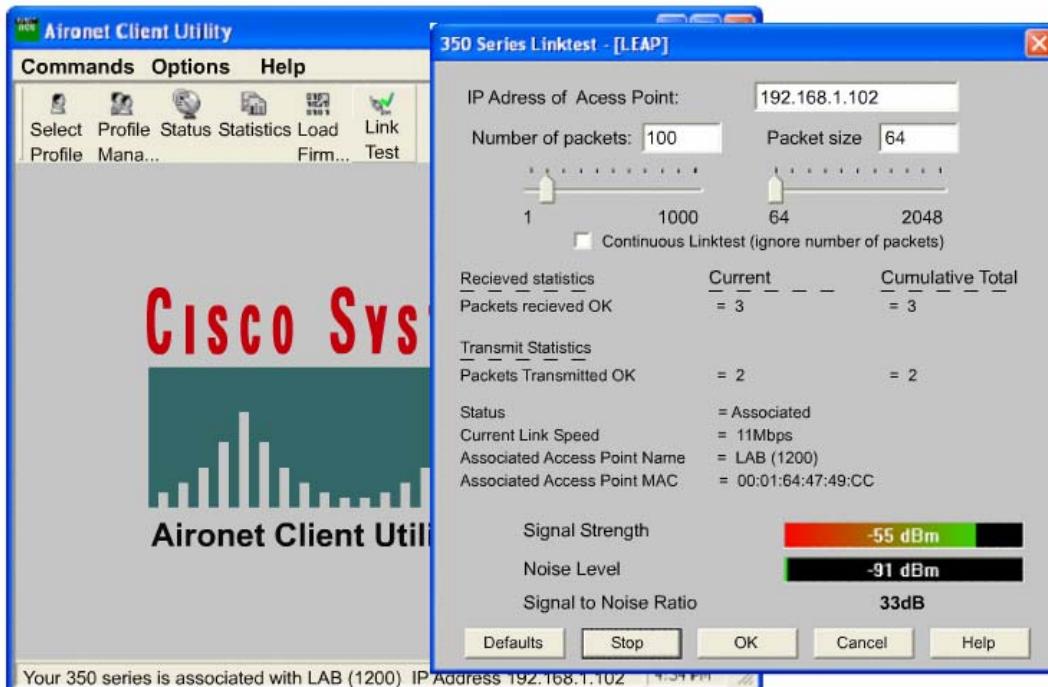


Figura 2

La pantalla de estadísticas es un recurso valioso para propósitos de diagnósticos según el cliente. La pantalla muestra la cantidad de paquetes que la placa del cliente ha transmitido y recibido, tanto multicast como unicast. También entrega un registro de errores que han tenido lugar desde la última vez que se efectuó una reconfiguración. Éstas son herramientas invaluables para determinar si la placa está experimentando cualquier dificultad o si la red está ralentizando la placa con el tráfico multicast.

Para una explicación de las diferentes estadísticas haga clic en el botón de Ayuda y en las definiciones que se mostrarán.

2.4.6 Medidor de estado del enlace

Si el sistema operativo de la computadora es Windows 95, Windows 98, Windows NT, Windows 2000, Windows Millennium Edition (Me), Windows XP, o Linux, se dispone de las siguientes utilidades para su uso:

- La Utilidad de Clientes Aironet (ACU) carga nuevo firmware, habilita funciones de seguridad, configura el adaptador cliente y lleva a cabo diagnósticos a nivel del usuario.
- El Medidor de Estado del Enlace (LSM) monitorea gráficamente la calidad de la señal y su potencia entre el adaptador cliente y un access point asociado a él.

La utilidad LSM se utiliza para determinar el desempeño del enlace RF entre el adaptador de clientes y su access point asociado.

La pantalla del Medidor de Estado del Enlace proporciona una pantalla gráfica de lo siguiente:

- Potencia de la señal — la potencia de la señal de radio del adaptador cliente en el momento en que se reciben los paquetes. Se muestra en forma de porcentaje a lo largo de un eje vertical.
- Calidad de la señal — la calidad de la señal de radio del adaptador cliente en el momento en el cual se reciben los paquetes. Se muestra en forma de porcentaje a lo largo de un eje horizontal.

Para abrir LSM en Windows, haga doble clic en el ícono LSM del escritorio.

Una línea diagonal representa el resultado combinado de potencia y calidad de la señal. Allí donde la ubicación de la línea recae en la pantalla gráfica se determina si el enlace RF entre el adaptador del cliente y su AP asociado es pobre, adecuado, bueno o excelente.

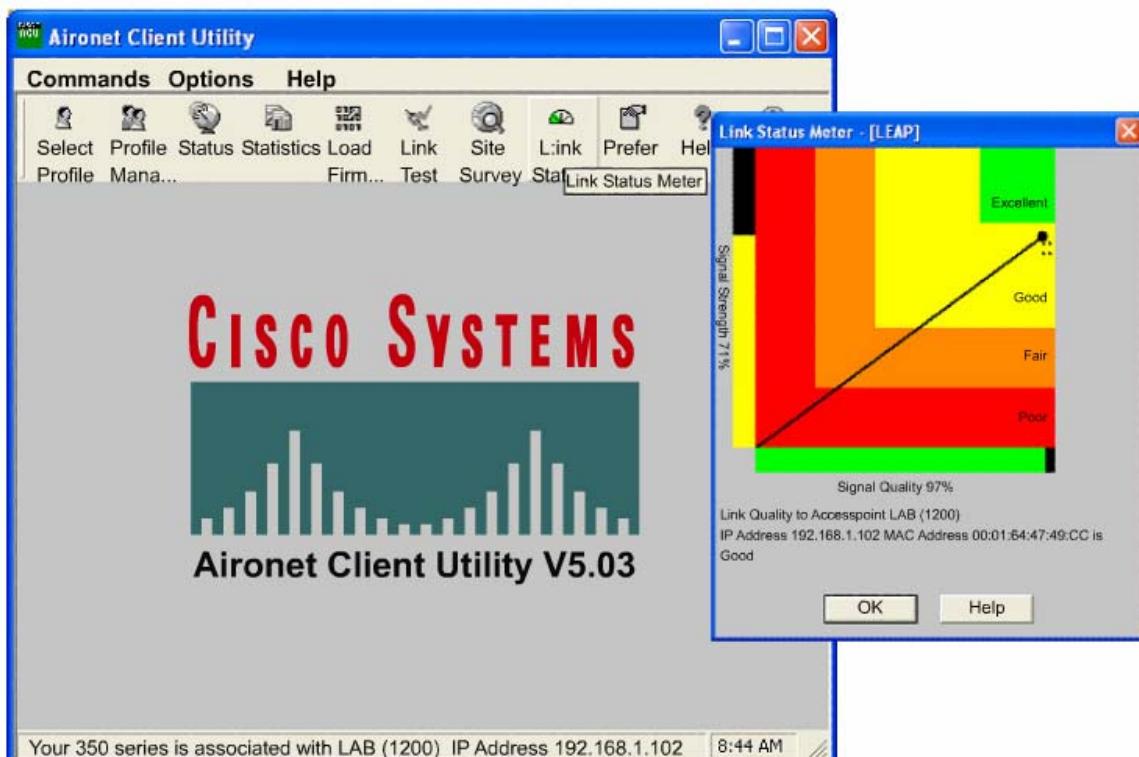


Figura 1

Esta información puede utilizarse para ayudar a determinar la cantidad óptima y la ubicación de APs en la red RF. Utilizando LSM para evaluar el enlace RF en diversas ubicaciones, es posible evitar áreas donde el desempeño es débil y eliminar el riesgo de perder la conexión entre el adaptador de clientes y el AP.

El punto de acceso asociado al adaptador cliente y su dirección MAC se indican en la parte inferior de la pantalla.

La Utilidad del Cliente Aironet (ACU) es una utilidad de diagnóstico y configuración de la interfaz gráfica del usuario (GUI) de Windows que puede utilizarse para llevar a cabo una variedad de funciones. La Actividad 2.4.6.1 demostrará las funciones de la ACU. La Actividad 2.4.6.2 simula el Medidor de Estado del Enlace. La actividad demostrará cómo llevar a cabo diagnósticos ACU.

Resumen

IEEE 802.11 especifica estándares para las WLANs. MAC y capa física (PHY) son servicios que han sido normalizados, utilizando los estándares 802.11 a, b, y g.

La función principal de los adaptadores de clientes es transferir los paquetes de datos a través de la infraestructura inalámbrica. La instalación, la configuración y el monitoreo de las placas de interfaz de red (NICs) inalámbricas son siempre importantes.

Módulo 3: Tecnología de radio wireless

Descripción general

En este módulo, el alumno aprenderá acerca de la tecnología inalámbrica y las ondas de radio. Las ondas de radio transmiten los datos de manera invisible a través del aire, a menudo a través de una distancia de millones de kilómetros o millas. Incluso aunque las ondas de radio son invisibles y completamente indetectables por los humanos, han cambiado totalmente a la sociedad. Ya sea que hablemos de un teléfono celular, un monitor para bebés, o miles de otros productos, todos los dispositivos inalámbricos utilizan ondas de radio para comunicarse. La siguiente lista muestra algunos de los usos importantes de la comunicación de radio:

- Emisiones de radio AM y FM
- Teléfonos inalámbricos
- Puertas de garage automáticas
- Redes inalámbricas
- Juegos controlados por radio
- Emisiones de televisión
- Comunicaciones satelitales en un solo sentido y en dos sentidos
- Unidades de control remoto de televisión
- Teléfonos celulares

En lo esencial, la radio es una tecnología increíblemente simple. Con sólo un par de componentes electrónicos que cuestan muy poco, alguien puede construir un simple transmisor o receptor de radio.

Este módulo explorará la tecnología y los aspectos matemáticos de la radio, para que el lector pueda comprender cómo funcionan las invisibles ondas de radio para hacer posibles tantas cosas, incluyendo las WLANs.

3.1 Ondas

3.1.1 Descripción general de las ondas

El diccionario Webster define una onda como se muestra en la Figura 1.

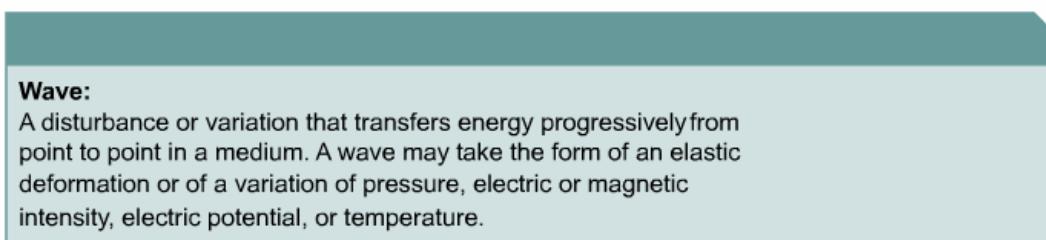


Figura 1

La parte más importante de esta definición es que una onda es una "perturbación o variación" que pasa a través de un medio. El medio a través del cual viaja la onda puede experimentar algunas oscilaciones de índole local a medida que la onda pasa, pero las partículas del medio no viajan con la onda. La perturbación puede asumir cualquier cantidad de formas, desde un impulso de amplitud finito hasta una onda sinusoidal infinitamente larga.

En muchos eventos deportivos, los entusiastas llevan a cabo una actividad denominada "la ola". "La ola" está formada por un grupo de personas que saltan y vuelven a sentarse. Algunas personas que se encuentran cerca las ven y saltan, otras que se encuentran más lejos hacen lo mismo y muy pronto hay una onda ("la ola") viajando por el estadio. La ola, o la acción de saltar y volver a sentarse, es la perturbación, y viaja por el estadio. No obstante, ninguna de las personas individuales del estadio es arrastrada por la ola a medida que viaja. Todos permanecen en sus asientos.

Las ondas de sonido longitudinales en el aire se comportan de manera muy similar. A medida que el sonido pasa, las partículas en el aire oscilan hacia atrás y adelante desde sus posiciones de equilibrio pero es la perturbación la que viaja, no las partículas individuales del medio. La Actividad 3.1.1a ilustra este concepto.

Las ondas transversales que viajan a través de una cuerda son otro ejemplo. La cuerda se desplaza hacia arriba y abajo, a medida que la onda viaja de izquierda a derecha, pero la cuerda en sí no experimenta ningún movimiento neto. Esto se muestra en la Actividad 3.1.1b.

3.1.2 Ondas sinusoidales

Una forma de onda es una representación de cómo la corriente alterna (AC) varía con el tiempo. La forma de onda AC familiar es la onda sinusoidal, que deriva su nombre del hecho de que la corriente o voltaje varía según la función sinusoidal matemática del tiempo transcurrido. La onda sinusoidal es única por el hecho de que representa energía enteramente concentrada en una única frecuencia. Una señal inalámbrica ideal asume una forma de onda sinusoidal, con una frecuencia usualmente medida en ciclos por segundo o Hertz (Hz). Un millón de ciclos por segundo está representado por un megahertz (MHz). Un billón de ciclos por segundo está representado por un gigahertz (GHz). Una onda sinusoidal tiene varias propiedades básicas, que se ilustran en la Figura 1:

- Amplitud — La distancia de cero al valor máximo de cada ciclo se denomina amplitud. La amplitud positiva del ciclo y la amplitud negativa del ciclo son las mismas.
- Periodo — El tiempo que le lleva a una onda sinusoidal completar un ciclo se define como periodo de la forma de onda. La distancia que viaja el seno durante este periodo se denomina longitud de onda.
- Longitud de onda — La longitud de onda, indicada por el símbolo griego lambda λ , es la distancia a través de la forma de onda desde un punto al mismo punto del siguiente ciclo.
- Frecuencia — La cantidad de repeticiones o ciclos por unidad de tiempo es la frecuencia, expresada en general en ciclos por segundo, o Hz.

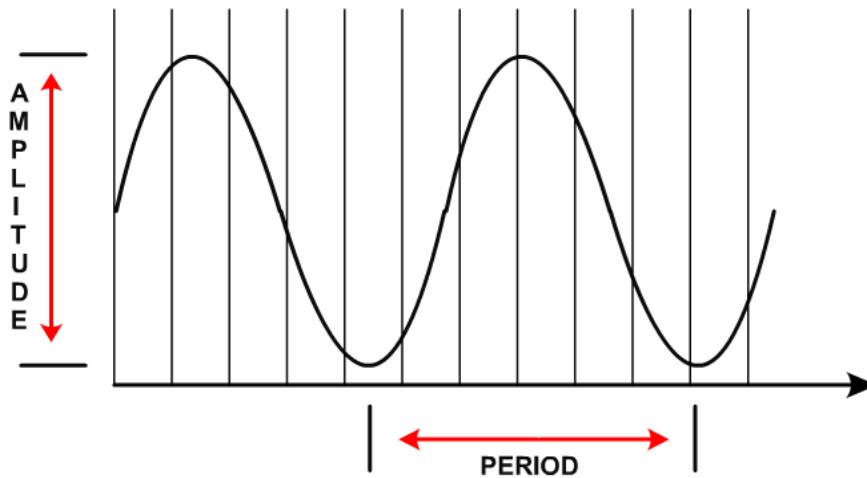


Figura 1

La relación inversa entre tiempo (t), el periodo en segundos, y frecuencia (f), en Hz, está indicada por las siguientes fórmulas:

$$t = 1/f$$

$$f = 1/t$$

Se dice que un periodo o ciclo completo de una onda sinusoidal abarca 360 grados (360°). Es posible que una onda sinusoidal se adelante o sea adelantada por otra onda sinusoidal en cualquier cantidad de grados, excepto cero o 360° . Cuando dos ondas sinusoidales difieren en exactamente 0° o 360° , se dice que las dos ondas están en fase. Dos ondas sinusoidales que difieren en fase en cualquier otro valor están fuera de fase, una respecto de la otra.

La transmisión en un medio puede cambiarse o modularse, para imprimir la información sobre ella. De igual forma, puede utilizarse desmodulación para recuperar la información. En lo que se refiere a las comunicaciones de frecuencia de radio (RF), la modulación involucra imprimir las características de una forma de onda en una segunda forma de onda variando la amplitud, frecuencia, fase u otra característica de la segunda forma de onda, o portadora.

Utilice las siguientes actividades para ver las relaciones entre amplitud, frecuencia y fase de una onda sinusoidal.

3.1.3 Conversión analógica a digital

La sección anterior habló sobre cuán complejas pueden llegar a ser las ondas analógicas y digitales que asumen la forma de ondas sinusoidales. Otra forma de contemplar la conexión entre analógico y digital es ver cómo una onda analógica puede convertirse en dígitos discretos que representan la onda analógica.

En la actividad interactiva, haga clic en Draw Wave [Dibujar Onda], y se dibujará una onda sinusoidal. El objetivo es representar completamente esta onda, y sus voltajes en constante variación, por medio de un conjunto de valores discretos. Este proceso se denomina conversión analógica a digital (A a D). De manera inversa, un proceso similar opera en dirección contraria, convirtiendo de D a A.

El proceso A a D se completa a través de los siguientes pasos:

1. Las amplitudes de onda analógicas se muestrean a instancias específicas a tiempo.
2. A cada muestra se le asigna un valor discreto.
3. Cada valor discreto se convierte en un flujo de bits.

Antes de que pueda muestrearse una onda analógica, debe determinarse en qué puntos debe medirse. El proceso de medir la onda analógica sólo en determinados intervalos se denomina muestreo. Una decisión relacionada es cuántas muestras deberán tomarse. Haga clic en Take Samples [Tomar Muestras] de la actividad y anote el resultado. Luego, desplace la barra Set # of Samples [Establecer # de Muestras] a la derecha y haga clic nuevamente en Take Samples. Ahora, deslice la barra hasta el extremo derecho y haga clic nuevamente en Take Samples. Es fácil ver que cuantas más muestras se toman, mejor se representa la onda.

Nótese que los valores mostrados no consisten en valores positivos y negativos equilibrados, como es lo usual en el caso de una onda sinusoidal. Esto se debe a que los valores se han normalizado, lo cual significa que existe un rango continuo de números positivos desde cero hasta el máximo. La normalización de los valores se lleva a cabo frecuentemente en matemática, para facilitar el trabajo con los valores, y comprender lo que representan. Aunque los voltajes reales no han cambiado, la escala que representa los voltajes ha oscilado.

Parecería que tomar más muestras es la forma de lograr una representación precisa de la señal. No obstante, cuantas más muestras se tomen, más bits será necesario enviar. Desafortunadamente, existe un punto más allá del cual muestras adicionales no serán de utilidad. Basándose en una fórmula denominada teorema de muestreo, muestrear a cualquier tasa igual o mayor que dos veces la frecuencia de la onda permitirá la reconstrucción de la onda sin error. Por lo tanto, una tasa de muestreo de más de dos veces la frecuencia de la onda no incrementará la precisión.

Utilice la actividad para configurar diferentes valores para la cantidad de muestras. Haga clic en Read Sampled Values [Leer Valores Muestreados] cada vez, para ver el flujo de bits que se transmitirían para cada muestra.

Tal como se enunció anteriormente, este proceso puede invertirse. El flujo de bits puede decodificarse, utilizando los valores analógicos aproximados. Este proceso tiene lugar cada vez que alguien reproduce un disco compacto (CD) musical. La música está codificada en bits en el plástico del CD. Estos bits pasan por una conversión digital a analógica (D a A), son procesados por más medios electrónicos y se convierten en la música que la gente escucha.

3.2 Matemática para el Estudio de la Radio

3.2.1 Watts

Para comprender qué es un watt, se debe considerar primero la energía. Una definición de energía es la capacidad para producir trabajo. Existen muchas formas de energía, incluyendo energía eléctrica, energía química, energía térmica, energía potencial gravitatoria, energía cinética y energía acústica. La unidad métrica de la energía es el Joule. La energía puede considerarse una cantidad.

Un watt es la unidad básica de potencia, y la potencia está relacionada con la energía. No obstante, potencia es un índice, y energía una cantidad. La fórmula para la potencia es $P = DE / Dt$

- DE es la cantidad de energía transferida.
- Dt es el intervalo temporal durante el cual se transfiere la energía.

Si un Joule de energía se transfiere en un segundo, esto representa un watt (W) de potencia. La Figura 1 muestra la cantidad de potencia asociada con algunas funciones comunes. Un watt se define como un ampère (A) de corriente por un volt (V).

El FCC de EE.UU. permite que se emita un máximo de cuatro watts de energía en las transmisiones WLAN en la banda no licenciada de 2,4 GHz. En las WLANs, los niveles de energía son tan bajos como un miliwatt (mW), o una milésima (1/1000) de watt, que pueden utilizarse en un área pequeña. Los niveles de energía en un único segmento de WLAN son raramente más elevados que 100 mW, lo suficiente para comunicarse a una distancia de hasta tres cuartos de un kilómetro o media milla bajo condiciones óptimas. Los access points en general tienen la capacidad para radiar desde 30 a 100 mW, dependiendo del fabricante. Las aplicaciones para exteriores de edificio a edificio son las únicas que utilizan niveles de potencia por encima de los 100 mW. Diversos ejemplos de potencia se muestran en la Figura 1.

Work Performed	Type of Energy	Power Created or Used
Laser pen operation	optical	5 mW
WLAN Access point operation	microwave	30 to 100 mW
Lifting a book one meter above a table	kinetic and gravitational	5 W
Night-light operation	electrical	7 W
Light-bulb operation	electrical	60 W
Loud Noise	acoustic	100 W
Power Plant operation	electrical	100 W

Figura 1

3.2.2 Decibeles

El decibel (dB) es una unidad que se utiliza para medir la potencia eléctrica. Un dB es un décimo de un Bel, que es una unidad de sonido más grande así denominada en homenaje a Alexander Graham Bell. El dB se mide en una escala logarítmica base 10 [1]. La base se incrementa en diez veces diez por cada diez dB medidos. Esta escala permite a las personas trabajar más fácilmente con grandes números. Una escala similar (la escala de Richter) se utiliza para medir terremotos. Por ejemplo, un terremoto de magnitud 6.3 es diez veces más fuerte que un terremoto de 5.3.

Type of Sound	Units or Individual Decibels	Decibel Scale Value
Rustle of leaves	10	10
Whisper	100	20
Soft conversation	1,000	30
Average residence	10,000	40
Average office	100,000	50
Telephone conversation	10,000,000	70
Heavy traffic	1,000,000,000	90
Subway traffic	10,000,000,000	100
Airplane engine	1,000,000,000,000	120

Figura 1

Cálculo de dB

La fórmula para calcular dB es la siguiente:

$$dB = 10 \log_{10} (P_{final}/P_{ref})$$

- dB = la cantidad de decibeles. Esto usualmente representa una pérdida de potencia, a medida que la onda viaja o interactúa con la materia, pero también puede representar una ganancia, como al atravesar un amplificador.
- P_{final} = la potencia final. Ésta es la potencia entregada después de que algún proceso haya ocurrido.
- P_{ref} = la potencia de referencia. Ésta es la potencia original.

Utilice la Actividad 3.2.3a para obtener una comprensión adicional de esta fórmula. En esta actividad, los alumnos calcularán los decibeles para los valores introducidos de Pref y Pfinal. En la Actividad 3.2.3b, los alumnos calcularán la Pfinal basándose en los valores introducidos para dB y Pref.

También hay algunas reglas generales para aproximarse a la relación entre dB y potencia:

- Un incremento de 3 dB = duplica la potencia
- Una disminución de 3 dB = la mitad de la potencia
- Un incremento de 10 dB = diez veces la potencia
- Una disminución de 10 dB = un décimo de la potencia

3.2.3 Referencias a los decibeles

Puesto que dB no tiene ninguna referencia definida en particular, el dBx, donde la x representa un valor específico, se utiliza a menudo en lugar del dB. Por ejemplo, el dBm hace referencia al miliwatt. Puesto que el dBm tiene una referencia definida, también puede convertirse a watts, si se lo desea. La ganancia o pérdida de potencia en una señal se determina comparándola con este punto de referencia fijo, el miliwatt. Existen varios términos relacionados con los que uno debería familiarizarse, para diseñar e instalar WLANs apropiadamente: [1](#)

Decibel References	
dBm	= dB milliWatt
dBd	= dB dipole
dBi	= dB isotropic
EIRP	= Effective Isotropic Radiated Power
Gain	= RF signal increase

Figura 1

- dB miliWatt (dBm) — Ésta es la unidad de medida del nivel de potencia de una señal. Si una persona recibe una señal de un miliwatt, esto representa una pérdida de cero dBm. No obstante, si una persona recibe una señal de 0,001 miliwatts, entonces tiene lugar una pérdida de 30 dBm. Esta pérdida se representa de la forma -30 dBm. Para reducir la interferencia con otras, los niveles de potencia de una WLAN 802.11b están limitados por los siguientes organismos:
 - 36 dBm de EIRP según el FCC
 - 20 dBm de EIRP según el ETSI
- dB dipolo (dBd) — Esto se refiere a la ganancia que tiene una antena, en comparación con la antena dipolo de la misma frecuencia. Una antena dipolo es la antena más pequeña y menos práctica en cuanto a la ganancia que puede obtenerse.
- dB isotrópico (dBi) — Esto se refiere a la ganancia que tiene una determinada antena, en comparación con una antena isotrópica, o de origen puntual, teórica. Desafortunadamente, una antena isotrópica no puede existir en el mundo real, pero es útil para calcular áreas de cobertura y debilitamiento teóricas.
 - Una antena dipolo tiene una ganancia de 2,14 dB por encima de la ganancia de una antena isotrópica de 0 dBi. Por ejemplo, una simple antena dipolo tiene una ganancia de 2,14 dBi o 0 dBd.
- Potencia Irradiada Isotrópica Efectiva (EIRP) — La EIRP se define como la potencia efectiva que se halla en el lóbulo principal de la antena transmisora. Es igual a la suma de la ganancia de la antena, en dBi, más el nivel de potencia, en dBm, que entra a la antena.
- Ganancia — Esto se refiere al incremento en la energía que parece agregar una antena a una señal RF. Existen diferentes métodos para medir esto, dependiendo del punto de referencia elegido. Cisco Aironet inalámbrico se estandariza en dBi para especificar mediciones de ganancia. Algunas

antenas se clasifican en dBd. Para convertir cualquier número de dBd a dBi, simplemente agregue 2,14 al número de dBd.

3.3 Ondas Electromagnéticas (EM)

3.3.1 Conceptos básicos acerca de las ondas EM

Espectro EM es simplemente un nombre que los científicos han otorgado al conjunto de todos los tipos de radiación, cuando se los trata como grupo. La radiación es energía que viaja en ondas y se dispersa a lo largo de la distancia. La luz visible que proviene de una lámpara que se encuentra en una casa y las ondas de radio que provienen de una estación de radio son dos tipos de ondas electromagnéticas. Otros ejemplos son las microondas, la luz infrarroja, la luz ultravioleta, los rayos X y los rayos gamma.

Todas las ondas EM viajan a la velocidad de la luz en el vacío y tienen una longitud de onda (λ) y frecuencia (f), que pueden determinarse utilizando la siguiente ecuación:

$$c = \lambda f, \text{ donde } c = \text{velocidad de la luz} (3 \times 10^8 \text{ m/s})$$

Esta fórmula enuncia que la longitud de onda de cualquier onda EM viajando en el vacío, en metros, multiplicada por la frecuencia de la misma onda EM, en Hz, siempre es igual a la velocidad de la luz o 3×10^8 m/s o 186.000 millas por segundo (aproximadamente 300.000 km/s).

Utilice la Actividad 3.3.1c para practicar cómo hallar la frecuencia o la longitud de onda de una onda EM, cuando el otro valor es conocido. Cuando la onda EM no viaja en el vacío, el material afecta su velocidad. Esto se ilustra en la Actividad 3.3.1a.

Las ondas EM gozan de las siguientes propiedades:

- reflexión, o rebote
- refracción, o quiebre en ángulo
- difracción, o dispersión en torno a los obstáculos
- dispersión, o redireccionamiento de parte de las partículas

Esto se tratará en mayor detalle posteriormente en este módulo. Además, la frecuencia y la longitud de onda de una onda EM son inversamente proporcionales entre sí, como lo muestra la Figura 1.

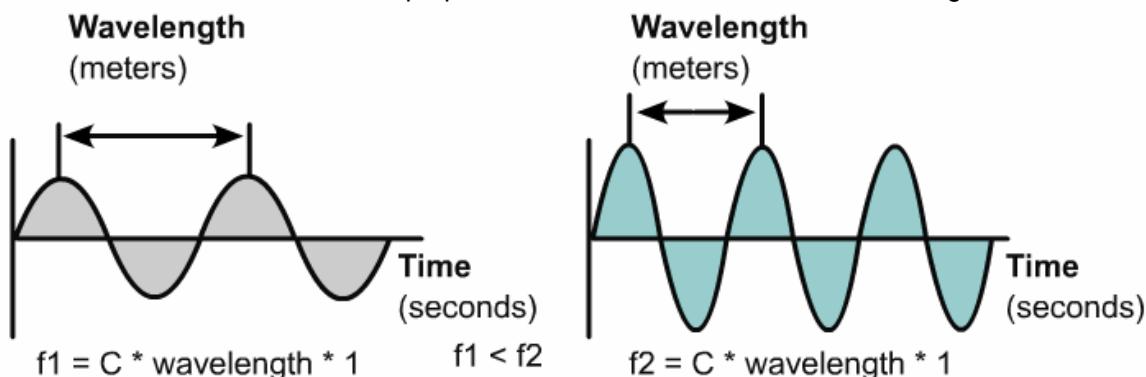


Figura 1

Existe una cierta cantidad de propiedades que se aplican a todas las ondas EM, incluyendo la dirección, la frecuencia, la longitud de onda, la potencia, la polarización y la fase. Las propiedades no definidas previamente se muestran en la Figura 2.

Este curso se concentrará en estas propiedades en cuanto se aplican a una porción del espectro EM total, que incluye las ondas de radio y las microondas. Estas bandas se denominan colectivamente Espectro RF. Las ondas EM son energía que asume la forma de campos eléctricos y magnéticos alternos y transversales. Aprenda más acerca de los campos EM y la polarización en las Actividades Interactivas que figuran más abajo.

Properties of Electromagnetic Waves

- **Direction in degrees:** While the actual pattern that radio waves form upon leaving an antenna is complex, one can approximate the wave pattern with a ray showing the primary direction of travel.
- **Horizontal or vertical polarization:** Radio waves are often emitted and reflected preferentially. For example, more waves are emitted horizontally or vertically. The transmission and detection of radio waves can be strongly influenced by the polarization and the relative orientations of the transmit and receive antennas.
- **Phase in degrees:** Assume, for simplicity, that radio waves lead to a sine wave like change in voltage in an antenna, with time. Also, the relative timing of different sine waves can be very important. If, for example, two waves of the same frequency arrive at the same point in time, or the waves are in-phase, they can form a more powerful wave together. If these two waves arrive at slightly different times, they may join together to form a complex wave. If they arrive exactly out of synchronization, or out of phase, they can cancel each other out.

Figura 2

3.3.2 Gráfica del espectro EM

Uno de los diagramas más importantes tanto en ciencia como en ingeniería es la gráfica del espectro EM, que se ilustra en la Figura 1. El diagrama del espectro EM típico resume los alcances de las frecuencias, o bandas que son importantes para comprender muchas cosas en la naturaleza y la tecnología. Las ondas EM pueden clasificarse de acuerdo a su frecuencia en Hz o a su longitud de onda en metros. El espectro EM tiene ocho secciones principales, que se presentan en orden de incremento de la frecuencia y la energía, y disminución de la longitud de onda:

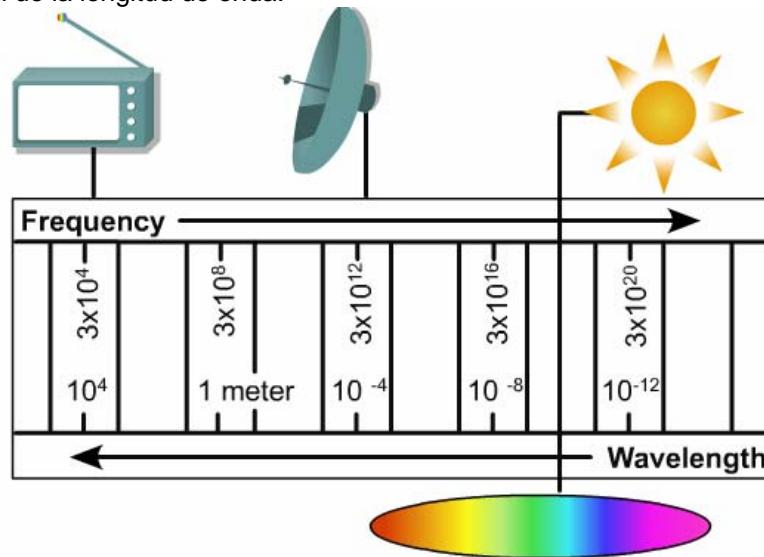


Figura 1

1. Ondas de potencia — Ésta es la radiación EM más lenta y por lo tanto también tiene la menor energía y la mayor longitud de onda.
2. Ondas de radio — Ésta es la misma clase de energía que emiten las estaciones de radio al aire para que un aparato de radio la capture y la reproduzca. No obstante, otras cosas, como las estrellas y los gases del espacio también emiten ondas de radio. Muchas funciones de comunicación utilizan ondas de radio.
3. Microondas — Las microondas cocinan maíz inflado en pocos minutos. En el espacio, los astrónomos utilizan las microondas para aprender acerca de la estructura de las galaxias cercanas.
4. Luz infrarroja (IR) — El infrarrojo a menudo se considera igual que el calor, porque hace que sintamos tibia nuestra piel. En el espacio, la luz IR sirve para rastrear el polvo interestelar.
5. Luz visible — Éste es el rango visible para el ojo humano. La radiación visible es emitida por todo, desde luciérnagas hasta lámparas y estrellas. También es emitida por partículas en rápido movimiento que golpean a otras partículas.

6. Luz ultravioleta (UV) — Es bien conocido que el sol es una fuente de radiación ultravioleta (UV). Son los rayos UV los que hacen que la piel se queme. Las estrellas y otros objetos calientes del espacio emiten radiación UV.
7. Rayos X — Un doctor utiliza rayos X para observar los huesos y un dentista los utiliza para observar los dientes. Los gases calientes del universo también emiten rayos X.
8. Rayos gamma — Los materiales radioactivos naturales y fabricados por el hombre pueden emitir rayos gamma. Los grandes aceleradores de partículas que los científicos utilizan para ayudarlos a comprender de qué está hecha la materia pueden irradiar en ocasiones rayos gamma. No obstante, el mayor generador de rayos gamma de todos es el universo, que crea radiación gamma de muchas formas.

El rango más importante que trataremos en este curso es el espectro RF. El espectro RF incluye varias bandas de frecuencia incluyendo las microondas y las Frecuencias Ultra Altas (UHF) y Frecuencias Muy Altas (VHF) de emisión de radio terrestre y televisión. Aquí es también donde operan las WLANs. El espectro RF tiene un rango que va desde los nueve kHz a miles de GHz. Realmente consiste en dos secciones importantes del espectro EM, ondas de radio y microondas. Por razones históricas, mucha gente se refiere a ambas secciones juntas como espectro RF. Las frecuencias RF, que abarcan una porción significativa del espectro de radiación EM, se utilizan mucho para las comunicaciones.

La mayoría de los rangos RF son licenciados, aunque unos pocos rangos se utilizan sin licencia.

3.3.3 Síntesis de Fourier

Cuando dos ondas EM ocupan el mismo espacio, sus efectos se combinan para formar una nueva onda de diferente forma. Por ejemplo, los cambios en la presión del aire ocasionados por dos ondas de sonido se suman. Las fuerzas eléctricas y magnéticas ocasionadas por dos ondas luminosas o dos ondas de radio también se suman.

Jean Baptiste Fourier es responsable de un importante descubrimiento matemático. Descubrió que una suma especial de ondas sinusoidales, de frecuencias relacionadas armónicamente, podían sumarse para crear cualquier patrón de ondas. Las frecuencias relacionadas armónicamente son frecuencias simples que son múltiplos de cierta frecuencia básica. Ondas complejas pueden construirse en base a ondas simples. Otra forma de enunciar esto es que cualquier onda reiterativa es matemática y físicamente equivalente al resultado de tan sólo sumar el conjunto correcto de ondas sinusoidales. Esta suma se denomina serie de Fourier.

Utilice la actividad interactiva para crear múltiples ondas sinusoidales y una onda compleja que se forma a partir de los efectos aditivos de las ondas individuales.

Finalmente, una onda cuadrada, o impulso cuadrado, puede construirse utilizando la combinación correcta de ondas sinusoidales. La importancia de esto se aclarará cuando se trate la modulación.

3.3.4 Usos del espectro

Es cierto que existe una cantidad infinita de diferentes frecuencias de ondas EM. No obstante, hablando en términos prácticos, cualquier creación de ondas EM realmente ocupa más que una cantidad infinitesimal de espacio de frecuencia. Por lo tanto, las bandas de frecuencia tienen una cantidad limitada de frecuencias, o canales de comunicaciones utilizables diferentes. Muchas partes del espectro EM no son utilizables para las comunicaciones y muchas partes del espectro ya son utilizadas extensamente con este propósito. El espectro electromagnético es un recurso finito.

Una forma de adjudicar este recurso limitado y compartido es disponer de instituciones internacionales y nacionales que configuren estándares y leyes respecto a cómo puede utilizarse el espectro. En EE.UU., es el FCC el que regula el uso del espectro. En Europa, el Instituto Europeo de Normalización de las Telecomunicaciones (ETSI) regula el uso del espectro.

Las bandas de frecuencia reguladas se denominan espectro licenciado. Ejemplos de éste incluyen la radio de Amplitud Modulada (AM) y Frecuencia Modulada (FM), la radio de radioaficionados o de onda corta, los teléfonos celulares, la televisión por aire, las bandas de aviación y muchos otros. Para poder operar un dispositivo en una banda licenciada, el usuario debe solicitar primero y luego otorgársele la licencia apropiada.

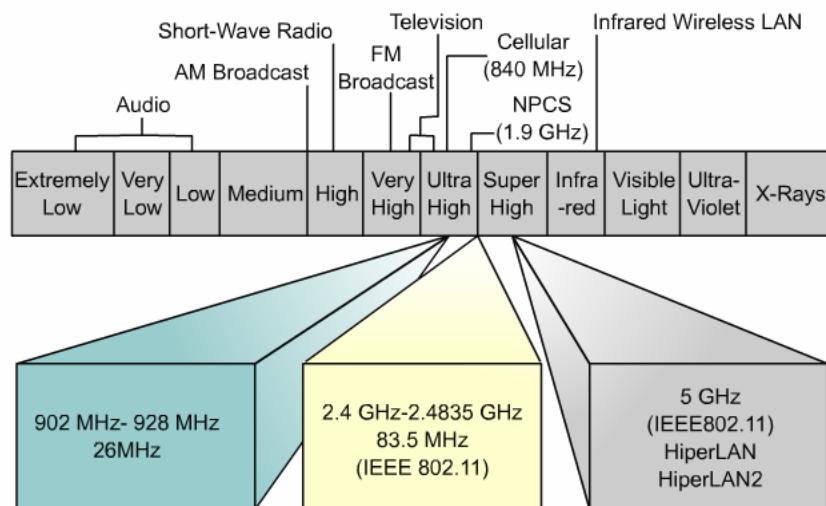


Figura 1

Algunas áreas del espectro han quedado sin licenciar. Esto es favorable para determinadas aplicaciones, como las WLANs. Un área importante del espectro no licenciado se conoce como banda industrial, científica y médica (ISM), que se muestra en la Figura 1. Estas bandas son sin licencia en la mayoría de los países del mundo. Los siguientes son algunos ejemplos de los elementos regulados que están relacionados con las WLANs:

- El FCC ha definido once canales DSSS 802.11b y sus correspondientes frecuencias centrales. ETSI ha definido 13.
- El FCC requiere que todas las antenas vendidas por un fabricante de espectro expandido estén certificadas junto con la radio con la cual se las vende.

3.4 Señales

3.4.1 Visualización de las señales en el tiempo

Un osciloscopio es un dispositivo electrónico importante y sofisticado que se utiliza para estudiar las señales eléctricas. Un osciloscopio puede graficar ondas, impulsos y patrones eléctricos. Consta de un eje x que representa el tiempo y de un eje y que representa el voltaje. Usualmente existen dos entradas de voltaje al eje y, por lo cual dos ondas pueden observarse y medirse al mismo tiempo. Una onda sinusoidal, tal como aparecería en un osciloscopio, se muestra en la Figura 1. La imagen tradicional de un seno u onda cuadrada expresa el voltaje como una función del tiempo. Ésta es la representación de la onda en el dominio de tiempo.

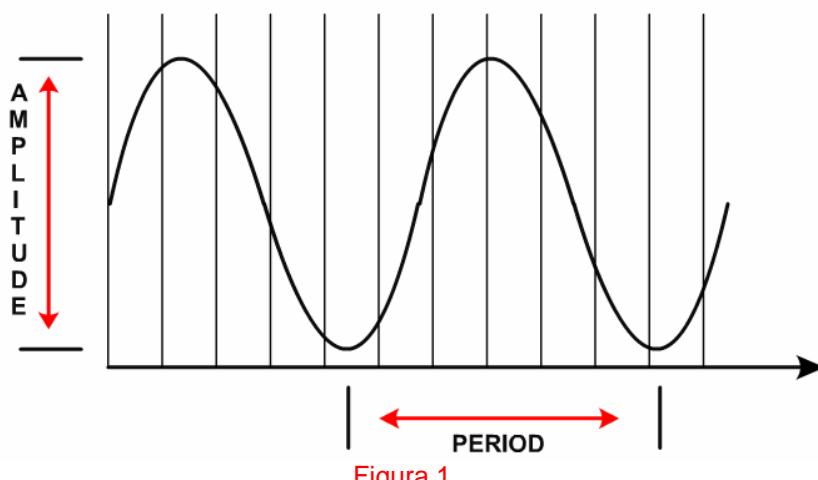


Figura 1

La Figura 2 muestra la energía permanente, en verde, alrededor de una antena bipolar eléctrica alineada verticalmente con la pantalla de la computadora. La energía permanente varía con el tiempo. La grilla púrpura muestra la porción radial, que representa la potencia de salida. La gente puede utilizar análisis del dominio de tiempo, para ver la energía permanente y la energía saliente en cuanto se relacionan entre sí.

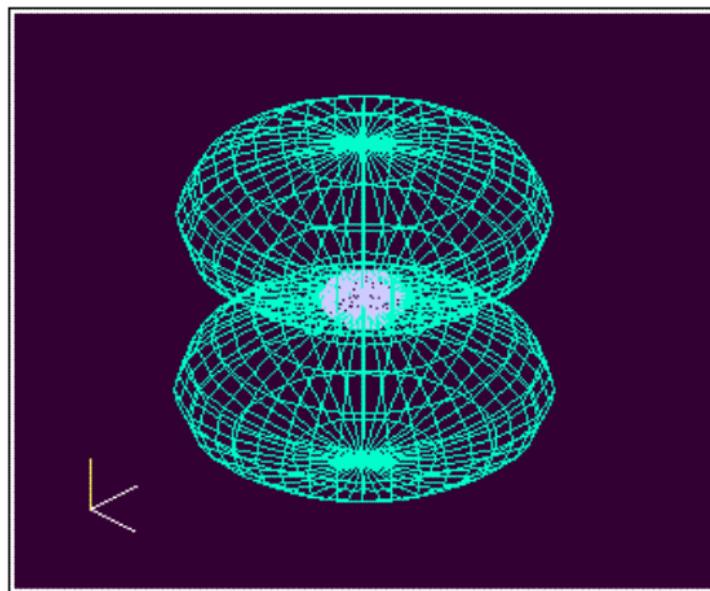


Figura 2

3.4.2 Visualización de las señales en la frecuencia

El estudio de cómo las señales varían con el tiempo se denomina análisis del dominio de tiempo. Otra forma de aprender acerca de las señales es analizar las frecuencias que utilizan. Los ingenieros se refieren a este proceso como análisis del dominio de frecuencia. Un dispositivo electrónico denominado analizador de espectro crea gráficas de potencia versus frecuencia, como la mostrada en la Figura 1.

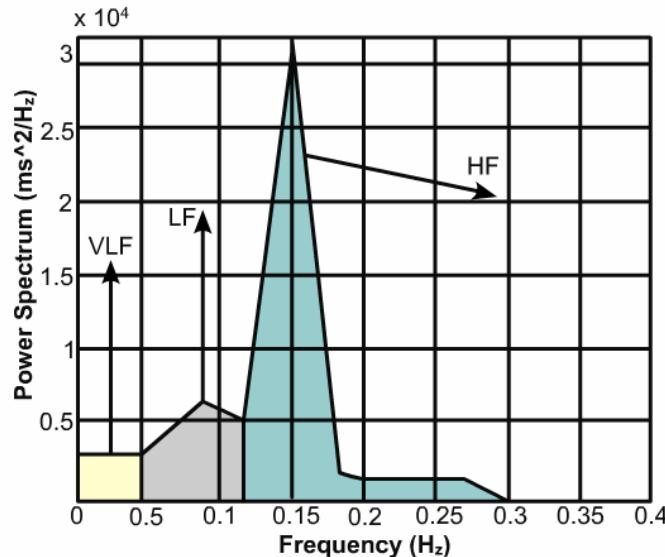


Figura 1

Para comprender el análisis del dominio de frecuencia en lo que tiene que ver con las WLANs, es útil examinar primero un sistema de radio más familiar, para ser más precisos, las emisoras de radio FM comerciales. En este caso, el término radio se refiere a un dispositivo receptor, que podría estar ubicado en una casa o automóvil.

Cuando se sintoniza una radio FM, se cambia la configuración de la misma, de modo tal que ésta responda a la frecuencia seleccionada. Las diferentes estaciones tienen cada una un centro o frecuencia portadora diferente. Esto es así porque no interfieren entre sí, transmitiendo en las mismas frecuencias. Además, dependiendo de factores tales como la potencia transmisora y la ubicación de una estación, así como cualquier obstáculo potencial, la fortaleza de la señal en el receptor de radio FM puede ser débil o fuerte.

Estos mismos factores existen en una WLAN. Por ejemplo, para obtener el mayor beneficio de múltiples APs en la misma ubicación, es importante que no se superpongan sus frecuencias. De otro modo, los APs interferirán entre sí en lugar de multiplicar la cantidad de ancho de banda utilizable por la cantidad de APs.

3.4.3 Las señales en tiempo y frecuencia

Para comprender mejor las complejidades de las ondas de radio, es útil examinar cómo las señales analógicas varían con el tiempo y la frecuencia. Considere en primer lugar una onda sinusoidal pura de una única frecuencia. Si una onda eléctrica sinusoidal con una frecuencia audible se aplica a un parlante, se escuchará un tono. Una gráfica de este tono puro en un analizador espectroscópico sería una única línea recta [1](#). La actividad interactiva ilustra una gráfica semejante. Haga clic en Play [Reproducir] en la actividad, para escuchar un ejemplo del tono.

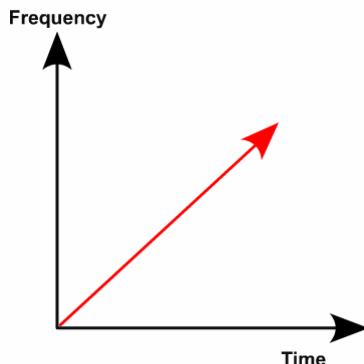


Figura 1

Ahora imagine varias ondas sinusoidales sumadas todas al mismo tiempo. La onda resultante es más compleja que una onda sinusoidal pura. Hay varios tonos y la gráfica de estos tonos mostrará varias líneas individuales, correspondiendo cada una a la frecuencia de cada tono.

Como ejemplo final, imagine una señal extremadamente compleja, como una voz o un instrumento musical. Con una cantidad suficiente de tonos diferentes, la gráfica de un analizador espectroscópico parecería un espectro continuo de tonos cerrados, espaciados e individuales. Haga clic en Sweep [Barrer] en la actividad, para escuchar un ejemplo de los tonos asociados a muchas frecuencias poco espaciadas. Se dibuja una gráfica a medida que las frecuencias cambian con el tiempo.

Señales digitales

El patrón de cambios en el voltaje versus tiempo se denomina onda cuadrada. Existen muchas formas de representar datos mediante señales digitales. La Figura [2](#) ilustra un ejemplo muy simple, en el cual existen sólo dos niveles de voltaje, que se interpretarán como uno o cero.

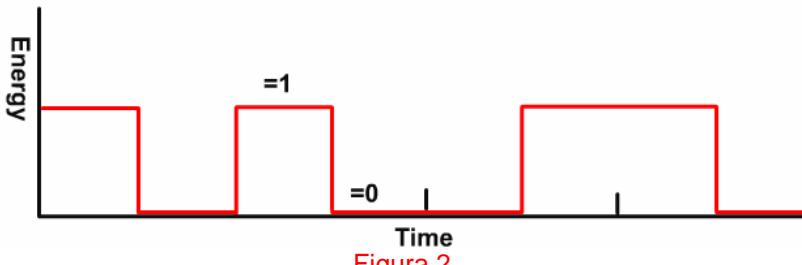


Figura 2

En principio, puede resultar difícil imaginar que la gráfica de voltaje versus tiempo de una señal digital pueda construirse en base a ondas sinusoidales. No obstante, recuerde la Síntesis de Fourier y que una onda cuadrada puede construirse utilizando la combinación adecuada de ondas sinusoidales.

El proceso matemático utilizado para calcular esto se encuentra más allá del alcance de este curso, pero una descripción simplificada respecto a cómo funciona puede ayudar a aclarar este concepto. El proceso se inicia con la fórmula fundamental frecuencia (f) con amplitud (A). Se agregan los armónicos impares, como $3f$, $5f$, $7f$, $9f$, etcétera. No obstante, estos armónicos impares no se agregan con amplitudes iguales, sino más bien con amplitudes de una tercera, una quinta, una séptima, una novena, etcétera.

En general, formas de onda complejas tendrán gráficas espectroscópicas complejas.

3.4.4 Ruido en tiempo y frecuencia

Un concepto muy importante en los sistemas de comunicaciones, incluyendo las WLANs, es el ruido. La palabra ruido tiene el significado general de sonidos indeseables. No obstante, en el contexto de las telecomunicaciones, el ruido puede definirse mejor como voltajes indeseables provenientes de fuentes

naturales y tecnológicas. Puesto que el ruido es sólo otra señal que produce ondas, puede agregarse a otras señales, como se trató anteriormente. Si la señal afectada representa información en un sistema de comunicaciones, el ruido puede cambiar la información. Es claro que esto no es aceptable.

En lo que respecta a una WLAN, las fuentes de ruido incluyen la electrónica del sistema de la WLAN, más la interferencia de frecuencia de radio (RFI), y la interferencia electromagnética (EMI) que se encuentra en el entorno WLAN. Estudiando el ruido, la gente puede reducir sus efectos en el sistema WLAN.

Una forma de ruido se denomina de Gauss, o ruido blanco. El analizador espectroscópico de ruido blanco es una línea recta a través de todas las frecuencias. En teoría, el ruido de Gauss afecta a todas las diferentes frecuencias de igual forma. En realidad, el ruido blanco no sigue un patrón tan simple. No obstante, éste es aún un concepto muy útil, al estudiar sistemas de comunicaciones. Puesto que el ruido blanco afectaría de igual forma a todas las frecuencias de una señal de radio, existen implicaciones para los circuitos tanto del transmisor como del receptor.

Otra forma de ruido se denomina interferencia de banda angosta. El término banda se refiere a una agrupación de frecuencias. Una banda angosta tiene un rango de frecuencias relativamente más pequeño. La radio FM es un ejemplo de interferencia de banda angosta. Aunque el ruido blanco perturbaría de igual forma a todas las estaciones de radio, la interferencia de banda angosta sólo interferiría con algunas estaciones de radio.

Ambas formas de ruido son importantes para comprender las WLANs. Puesto que el ruido blanco degradaría los diversos canales de igual forma, los diversos componentes de FHSS y DSSS se verían igualmente afectados. La interferencia de banda angosta podría perturbar sólo a ciertos canales o a extensos componentes del espectro. Incluso podría ser posible utilizar un canal diferente para evitar la interferencia por completo.

3.5 Técnicas de Modulación

3.5.1 Frecuencia portadora

Una frecuencia portadora es una onda electrónica que se combina con la señal de información y la transporta a través del canal de comunicaciones.

Utilizar una onda portadora también resuelve muchos otros problemas de circuitos, antenas, propagación y ruido. Por ejemplo, una antena práctica debe tener un tamaño de alrededor de una longitud de onda, de la onda EM a ser transmitida. Si las ondas sonoras se emitieran en frecuencias audibles, la antena tendría que tener más de un kilómetro de altura. Utilizando frecuencias mucho más altas para la portadora, el tamaño de la antena también se ve significativamente reducido debido al hecho de que frecuencias más altas tienen longitudes de onda más cortas.

Una estación de radio FM posee en general letras de llamado asociadas a ellas, como KPBS. No obstante, una forma más práctica de pensar acerca de una estación de radio es su frecuencia portadora, como 101.1 MHz, según la cual el alumno sintoniza su radio. En el caso de las WLANs, la frecuencia portadora es de 2,4 GHz o 5 GHz. Utilizar frecuencias portadoras en las WLANs tiene una complejidad extra, por el hecho de que la frecuencia portadora se cambia a salto de frecuencia o chipping de secuencia directo, para hacer la señal más inmune a la interferencia y al ruido.

El proceso de recuperar la información de la portadora se denomina desmodulación. Esencialmente es una inversión de los pasos utilizados para modular los datos. En general, a medida que los sistemas de transmisión o modulación (compresión) se hacen más complejos y las velocidades de los datos se incrementan, la inmunidad al ruido disminuye, y la cobertura baja.

3.5.2 Técnicas básicas de modulación

Tal como se trató anteriormente, un objetivo de las comunicaciones es utilizar una frecuencia portadora como frecuencia básica de comunicación, pero modificándola utilizando un proceso denominado modulación para codificar la información en la onda de la portadora. [1](#)

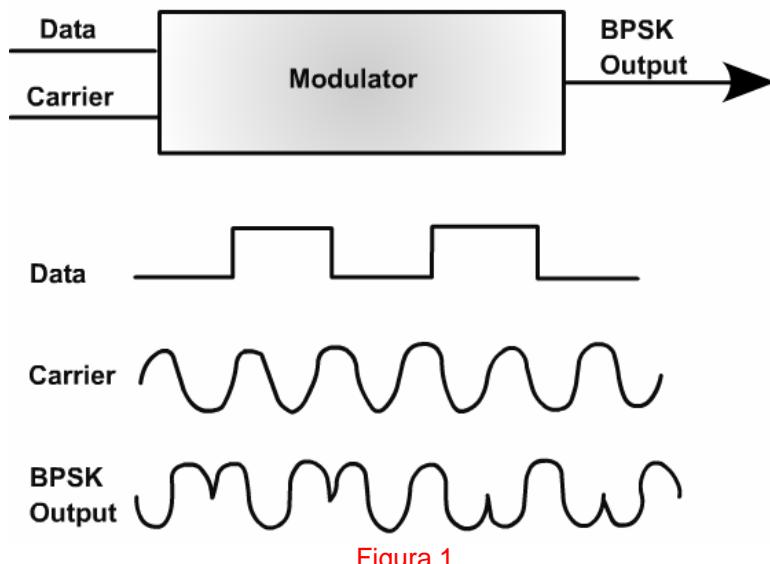


Figura 1

Existen tres aspectos básicos de la portadora que pueden modularse:

1. Amplitud
2. Frecuencia
3. Fase o ángulo

Las tres técnicas correspondientes son las siguientes:

1. Amplitud modulada (AM)
2. Frecuencia modulada (FM)
3. Modulación de fase (PM)

La mayoría de los sistemas de comunicaciones utilizan alguna forma o combinación de estas tres técnicas de modulación básicas.

Casos extremos de estas técnicas incluyen los siguientes:

- Codificación por desplazamiento de amplitud (ASK) — Eliminar por completo la amplitud
- Codificación por desplazamiento de frecuencia (FSK) — Saltar a una frecuencia extrema
- Codificación por desplazamiento de fase (PSK) — Desplazar la fase 180 grados

Utilice la actividad interactiva para ver cómo un cero o un uno pueden modular una señal portadora analógica, en cada una de estas técnicas.

3.5.3 FHSS

FHSS es una técnica de espectro expandido que utiliza la agilidad de la frecuencia para distribuir los datos a través de más de 83 MHz de espectro. La agilidad de la frecuencia es la capacidad de una radio para cambiar la frecuencia de la transmisión rápidamente, dentro de la banda de frecuencia RF utilizable. En EE.UU., basándose en los estándares establecidos por el FCC, las WLANs FHSS utilizan los 83 MHz que rodean a la banda ISM de 2,4 GHz. La Figura 1 muestra un diagrama de bloque FHSS.

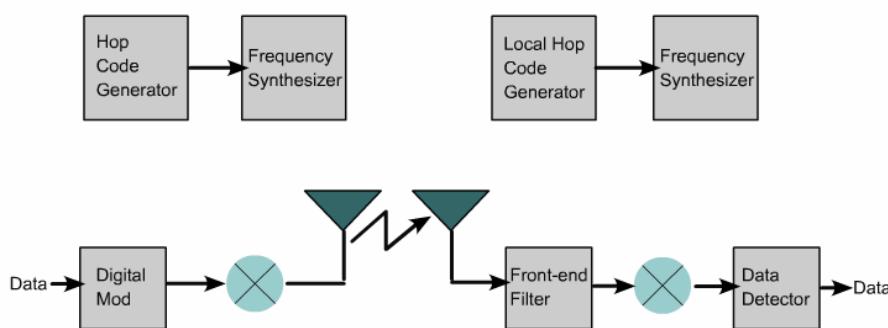


Figura 1

En los sistemas FHSS, la portadora cambia de frecuencia, o salta, de acuerdo a una secuencia pseudo-aleatoria, esto en ocasiones se denomina código de salto. Esta secuencia define al canal FHSS. Se trata de una lista de frecuencias, a las cuales saltará la portadora durante intervalos específicos. El transmisor utiliza esta secuencia de saltos para seleccionar su frecuencia de transmisión. La portadora permanecerá en una determinada frecuencia durante un periodo especificado, que se denomina tiempo de permanencia. El transmisor utilizará entonces una pequeña cantidad de tiempo, denominado tiempo de salto, para desplazarse a la siguiente frecuencia. Cuando la lista de frecuencias se ha atravesado completamente, el transmisor comenzará nuevamente y repetirá la secuencia.

La radio receptora se sincroniza según la secuencia de salto de la radio transmisora para permitir al receptor estar en la frecuencia correcta en el momento correcto.

3.5.4 DSSS

La tempranamente desarrollada tecnología Espectro Expandido de Secuencia Directa (DSSS) se encontraba en el rango de frecuencia de los 900 MHz. ¹En ese momento no se había implementado un sistema de modulación estándar. El concepto básico de este sistema era el uso de todo el canal para producir un único canal rápido de 860 Kbps. De otro modo, el canal se dividía en secciones más pequeñas para producir más canales, pero esos canales se desempeñaban a velocidades más lentas (por ejemplo, tres canales a 215 Kbps o dos canales a 344 Kbps).

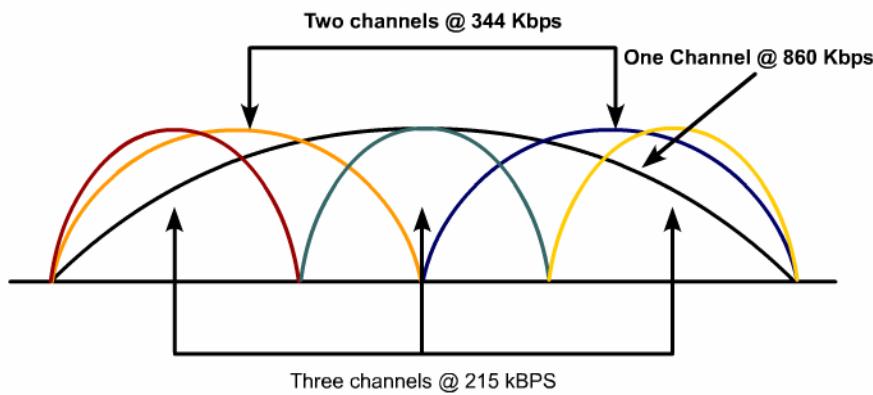


Figura 1

Ahora que se han implementado los estándares 802.11, un ingeniero RF tiene que seguir las reglas para hacer que el hardware cumpla con 802.11. La práctica de utilizar una mayor parte del canal ya no podría utilizarse para lograr velocidades de datos más altas. El nuevo sistema para 802.11 es utilizar técnicas de modulación muy avanzadas para lograr velocidades de datos más altas.

La Figura ²muestra un diagrama de bloque de DSSS 802.11b. DSSS define un canal como banda contigua de frecuencias, de 22 MHz de amplitud. En EE.UU., cada canal opera de una a 11 frecuencias centrales definidas y extiende los 11 MHz en cada dirección. ³Por ejemplo, el Canal 1 opera desde los 2,401 GHz a los 2,423 GHz, que es 2,412 GHz más o menos 11 MHz. El Canal 2 utiliza 2,417 más o menos 11 MHz, etcétera.

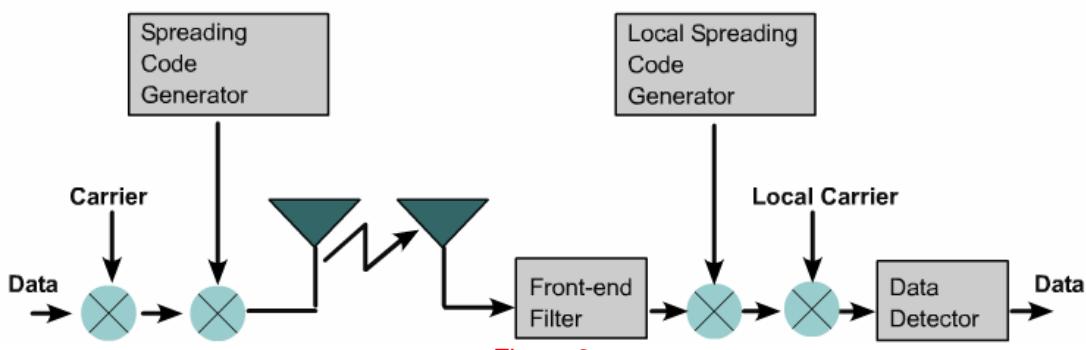


Figura 2

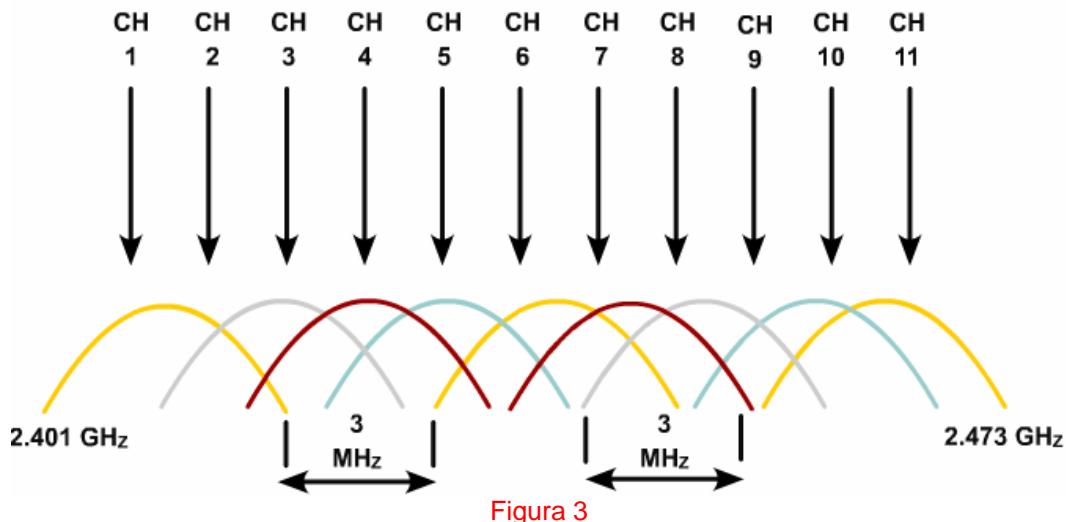


Figura 3

Existe una superposición significativa entre canales adyacentes. Las frecuencias centrales están separadas sólo por 5 MHz, sin embargo cada canal utiliza 22 MHz de ancho de banda analógico. De hecho, los canales deberán compartir su ubicación sólo si los números de canal se encuentran al menos a cinco de diferencia. Los Canales 1 y 6 no se superponen, los Canales 2 y 7 no se superponen, etcétera. Existe un máximo posible de tres sistemas DSSS con ubicación compartida. Los Canales 1, 6 y 11 son canales no superpuestos, como los muestra la Figura 3. Nótense las bandas de guardia de 3 MHz entre cada uno de estos canales. En Europa, ETSI ha definido un total de 14 canales, lo cual permite cuatro conjuntos diferentes de tres canales no superpuestos.

Mientras que FHSS utiliza cada frecuencia durante un breve periodo en un patrón repetitivo, DSSS utiliza un rango de frecuencia amplio de 22 MHz todo el tiempo. La señal se expande a través de diferentes frecuencias. Cada bit de datos se convierte en una secuencia de chipping, o una cadena de chips que se transmiten en paralelo, a través del rango de frecuencia. Esto se denomina en ocasiones código de chipping. Las agencias reguladoras configuran una tasa de chipping mínima para las diferentes velocidades soportadas. IEEE 802.11 utiliza 11 chips. Por ejemplo, la velocidad de chip mínima para DSSS 802.11, según el FCC, es de diez chips para 1 y 2 Mbps (BPSK/QPSK) y ocho chips para 11 Mbps (CCK). La Figura 4 muestra un ejemplo de secuencia o código de chipping. Si los bits del código de chipping para cero y para uno se examinan de cerca, puede determinarse que más de cinco bits de datos de 11 tendrían que invertirse en error, antes de que el valor cambiara de un cero a un uno, o de un uno a un cero. Esto significa que más de la mitad de la señal puede perderse, y aún así el mensaje original será recuperable.

If the data bit was: 1001

Chipping code is: 1=00110011011 0=11001100100

Transmitted data would be:

00110011011	11001100100	11001100100	00110011011
1	0	0	1

Figura 4

802.11b utiliza tres tipos diferentes de modulación, dependiendo de la velocidad de datos utilizada:

- Codificación de desplazamiento de fase binario (BPSK) — BPSK utiliza una fase para representar un 1 binario y otra para representar un 0 binario, para un total de un bit de datos binarios. Esto se utiliza para transmitir datos a 1 Mbps.
- Codificación de desplazamiento de fase de cuadratura (QPSK) — Con QPSK, la portadora pasa por cuatro cambios de fase y puede así representar dos bits binarios de datos. Esto se utiliza para transmitir datos a 2 Mbps.
- Codificación de código complementario (CCK) — CCK utiliza un conjunto complejo de funciones como códigos complementarios para enviar más datos. Una de las ventajas de CCK sobre técnicas

de modulación similares es que sufre menos la distorsión multiruta. La distorsión multiruta se tratará posteriormente. CCK se utiliza para transmitir datos a 5,5 Mbps y 11 Mbps.

3.5.5 OFDM

El estándar 802.11a y el de próxima aparición 802.11g utilizan ambos multiplexado por división de frecuencia ortogonal (OFDM), para lograr velocidades de datos de hasta 54 Mbps. OFDM funciona dividiendo una portadora de datos de alta velocidad en varias subportadoras de más baja velocidad, que luego se transmiten en paralelo. Cada portadora de alta velocidad tiene 20 MHz de amplitud y se divide en 52 subcanales, cada uno de aproximadamente 300 KHz de amplitud. 1 OFDM utiliza 48 de estos subcanales para datos, mientras que los cuatro restantes se utilizan para la corrección de errores. El multiplexado por división de frecuencia ortogonal codificada (COFDM) proporciona velocidades de datos más elevadas y un alto grado de recuperación de la reflexión multirruta, gracias a su sistema de codificación y corrección de errores. OFDM utiliza el espectro de manera mucho más eficiente, espaciando los canales a una distancia mucho menor. El espectro es más eficiente porque todas las portadoras son ortogonales entre sí, evitando de esa forma la interferencia entre portadoras muy cercanas.

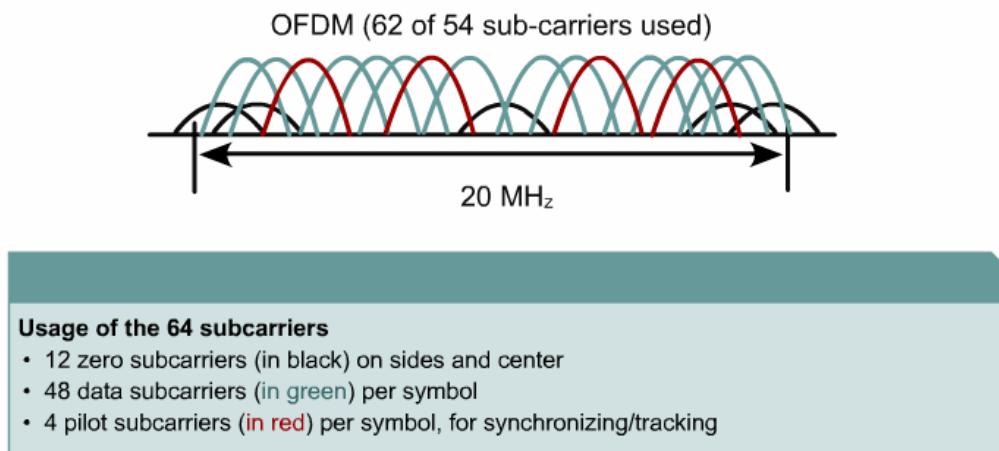


Figura 1

Cada subcanal de la implementación de OFDM tiene alrededor de 300 KHz de amplitud. 802.11a utiliza diferentes tipos de modulación, dependiendo de la velocidad de datos utilizada. El estándar 802.11a especifica que todos los productos que cumplen con 802.11a deben soportar tres velocidades de datos básicas que incluyen las siguientes 2:

Modulation with Sub Channels	Data Rate Per Sub Channel (Kbps)	Total Data Rate (Mbps)
BPSK	125	6
BPSK	187.5	9
QPSK	250	12
QPSK	375	18
16QAM	500	24
16QAM	750	36
64QAM	1000	48
64QAM	1125	54

Figura 2

- Codificación de Desplazamiento de Fase Binaria (BPSK) — codifica 125 Kbps de datos por canal, lo cual resulta en una velocidad de datos de 6.000 Kbps, o 6 Mbps.
- Codificación de Desplazamiento de Fase de Cuadratura (QPSK) — codifica a 250 Kbps por canal, dando como resultado una velocidad de datos de 12 Mbps.
- Modulación de Amplitud de Cuadratura de 16 Niveles — codifica 4 bits por hertz, logrando una velocidad de datos de 24 Mbps.

El estándar también permite al fabricante extender el sistema de modulación más allá de los 24 Mbps. Se logran velocidades de datos de 54 Mbps utilizando la Modulación de Amplitud de Cuadratura de 64 Niveles (64-QAM), que da como resultado 8 bits por ciclo o 10 bits por ciclo, para un total de hasta 1,125 Mbps por

canal de 300-KHz. Con 48 canales, esto resulta en una velocidad de datos de 54 Mbps. Recuerde que cuantos más bits por ciclo (hertz) son codificados, más susceptible será la señal a la interferencia y al debilitamiento, y en última instancia, más corto es el alcance, a menos que se incremente la potencia de salida.

Ortogonal es un término matemático derivado de la palabra griega *orthos*, que significa recto, correcto o cierto. En matemática, la palabra ortogonal se utiliza para describir elementos independientes. La ortogonalidad se aprecia mejor en el dominio de frecuencia, observando un análisis espectroscópico de una señal. OFDM funciona porque las frecuencias de las subportadoras se seleccionan de tal manera que, por cada frecuencia de subportadora, todas las otras subportadoras no contribuyen a la forma de onda total.

3.6 Acceso Múltiple y Ancho de Banda

3.6.1 Acceso múltiple al medio compartido

Un problema fundamental de las comunicaciones inalámbricas es que la atmósfera es un medio compartido. ¿Cómo hacen dos o más usuarios para acceder al mismo medio sin que surjan colisiones?

Una forma de tratar el acceso compartido es hacer que una autoridad oficial como el FCC o el ETSI establezcan el uso de frecuencias fijas. De esta forma, las diversas estaciones que buscan transmitir pueden hacerlo simultáneamente, sin colisiones, mientras utilicen sus frecuencias de portadora asignadas y sigan las reglas de potencia e interferencia. Los receptores deben sintonizar la frecuencia portadora, para obtener broadcasts de una estación específica.

Las redes de telefonía celular han utilizado, en diversos momentos, varios métodos diferentes para compartir su medio. Existen tres técnicas principales que se han utilizado para compartir las ondas por aire:

1. Acceso Múltiple por División de Tiempo (TDMA) — Cada dispositivo puede utilizar todo el espectro disponible en la célula, pero sólo durante un periodo breve.
2. Acceso Múltiple por División de Frecuencia (FDMA) — Cada dispositivo puede utilizar una porción del espectro disponible, durante tanto tiempo como lo necesite el dispositivo, mientras se encuentra en la célula.
3. Acceso Múltiple por División de Código (CDMA) — Esta técnica es realmente una combinación de las dos anteriores. Se trata del sistema más avanzado y el que está conduciendo a las tecnologías inalámbricas móviles de Tercera Generación (3G).

3.6.2 DSSS WLAN y CSMA/CA

Como se mencionó anteriormente, las WLANs operan en el espectro sin licencia. 802.11b y 802.11g operan en la banda de 2,4 GHz. 802.11a opera en la banda de 5 GHz. Dentro de las bandas de 2,4 GHz y 5 GHz, las frecuencias no tienen licencia. No obstante, estas bandas tienen un tamaño limitado, establecido por una regulación. Esto significa que el medio compartido es propenso a colisiones y necesita, por lo tanto, un método para tratar con esta posibilidad.

La técnica utilizada actualmente se denomina acceso múltiple con detección de portadora y colisión evitable (CSMA/CA). Es similar en muchos aspectos a CSMA/CD en Ethernet. El protocolo CSMA/CA está diseñado para reducir la probabilidad de colisiones entre múltiples dispositivos que acceden a un medio, en el punto donde es más probable que ocurran las colisiones. Una vez que el medio se convierte en inactivo, al seguir un medio ocupado es el momento en el que existe la probabilidad de una colisión. Esto se debe a que múltiples dispositivos podrían haber estado esperando a que el medio se vuelva disponible nuevamente. Aquí es cuando un procedimiento de retardo de envío aleatorio se utiliza para resolver conflictos de contención del medio.

El método de acceso CSMA/CA utiliza un mecanismo de detección de portadora tanto físico como virtual. El mecanismo de detección de portadora física funciona tal como ocurre en CSMA/CD. El mecanismo de detección de portadora virtual se logra distribuyendo la información de reserva que anuncia el uso inminente del medio. El intercambio de frames RTS y CTS anterior al frame de datos real es una forma de distribuir esta información de reserva del medio. Los frames RTS y CTS contienen un campo de duración que define el periodo durante el cual es necesario el medio, para transmitir el frame de datos real, el frame ACK que regresa, y todos los espacios entre frames (IFSs). Todos los dispositivos que se encuentran dentro del rango de recepción del origen, que transmite el RTS, o el destino, que transmite el CTS, aprenderán la reserva del medio. El intercambio RTS/CTS también lleva a cabo un tipo de inferencia de colisión rápida y una verificación de la ruta de transmisión. La Figura 1 ilustra el intercambio de RTS/CTS. Este método de acceso se denomina función de coordinación distribuida (DCF).

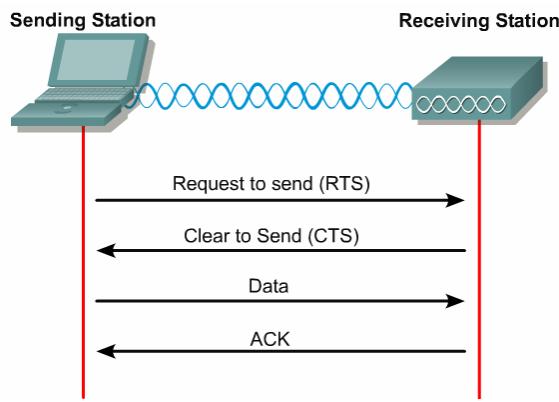


Figura 1

El MAC IEEE 802.11 también puede incorporar un método de acceso opcional, denominado función de coordinación de punto (PCF), que crea un acceso al medio libre de contención, utilizando un tipo de estudio, en el cual el AP es quien dirige el estudio.

3.6.3 Ancho de banda

El ancho de banda es un concepto extremadamente importante en los sistemas de comunicaciones. Existen dos formas comunes de considerar el ancho de banda, que se denominan ancho de banda analógico y ancho de banda digital. Estos dos conceptos relacionados son importantes para el estudio de las WLANs. Esta sección explorará estos tipos de ancho de banda en más profundidad.

Ancho de banda analógico

El ancho de banda analógico se refiere en general al rango de frecuencia de un sistema electrónico analógico. Por ejemplo, el ancho de banda analógico podría utilizarse para describir el rango de frecuencias irradiado por una estación de radio FM. El ancho de banda analógico también podría referirse al rango de frecuencias que pueden propagarse por un cable de cobre. Se describe en unidades de frecuencia, o ciclos por segundo, que se miden en Hz. Existe una correlación directa entre el ancho de banda analógico de cualquier medio y la velocidad de datos en bits por segundo que el medio puede soportar.

Ancho de banda digital

El ancho de banda digital es una medida de cuánta información puede fluir de un lugar a otro, en un tiempo determinado. El ancho de banda digital se mide en bits por segundo. Al tratar las comunicaciones de datos, el término ancho de banda significa más a menudo ancho de banda digital.

El throughput se refiere al ancho de banda real medido. En algunos casos, se lo restringe más para incluir sólo los datos reales, descartando cualquier sobrecarga del protocolo, como encabezados, trailers y mensajes del protocolo, de los totales calculados. Independientemente del método exacto de cálculo, el throughput real a menudo es mucho menos que el ancho de banda digital máximo posible del medio que está siendo utilizado. Muchos factores afectan al throughput, incluyendo el medio, la distancia, el ruido y los protocolos utilizados.

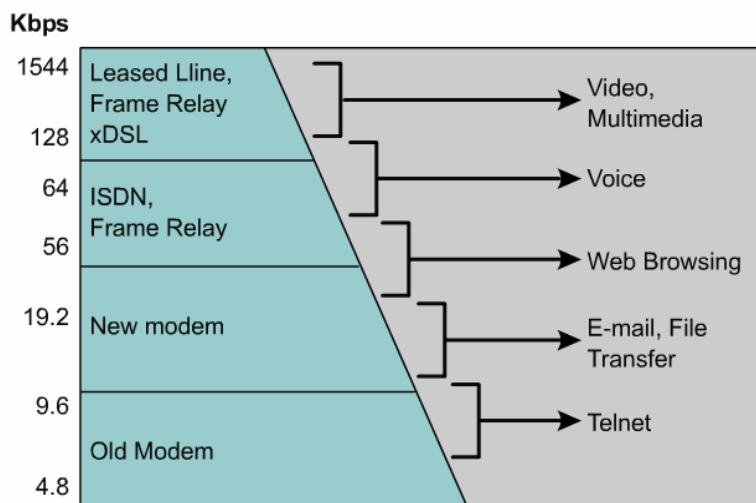


Figura 1

Al diseñar una red, es importante considerar el ancho de banda teórico. La red nunca será más rápida que lo que el medio permita. Una consideración relacionada es la cantidad de ancho de banda que requieren las aplicaciones del usuario. La Figura 1 ilustra diferentes métodos de conectarse a la Internet y sus correspondientes anchos de banda, en Kbps. En la Figura 1 también se muestran algunas aplicaciones de Internet típicas y sus necesidades de ancho de banda correspondientes.

3.7 Propagación de las Ondas de Radio

3.7.1 Propagación de RF

El estudio de cómo las ondas EM viajan e interactúan con la materia puede volverse extremadamente complejo. No obstante, existen varias simplificaciones importantes que pueden llevarse a cabo, para estudiar más fácilmente las propiedades de las ondas EM. Históricamente, estas simplificaciones se desarrollaron para las ondas luminosas, pero también se aplican a las ondas de radio, las microondas y todo el espectro EM.

En el vacío, las microondas de 2,4 GHz viajan a la velocidad de la luz. Una vez que se originan, estas microondas continuarán en la dirección en la cual fueron emitidas para siempre, a menos que interactúen con alguna forma de materia. El rayo geométrico se utiliza para significar que las microondas están viajando en espacio libre. Puesto que las WLANs se encuentran usualmente en tierra, dentro de la atmósfera, las microondas viajan por el aire, no en el vacío. No obstante, en la siguiente sección el alumno verá que esto no cambia significativamente su velocidad.

De manera similar a la luz, cuando la RF viaja a través de materia transparente, algunas de las ondas se ven alteradas. Por lo tanto, la velocidad de las microondas de 2,4 GHz y 5 GHz también cambia, a medida que las ondas viajan a través de la materia. No obstante, la cantidad de la alteración depende mucho de la frecuencia de las ondas y de la materia. En las siguientes dos secciones, se estudiarán algunos de los fenómenos que pueden afectar las ondas de radio de una WLAN a medida que viajan a través de la materia.

3.7.2 Refracción

Una superficie se considera lisa si el tamaño de las irregularidades es pequeño, en relación a la longitud de onda. De otro modo, se la considera irregular. Las ondas electromagnéticas se difractan alrededor de objetos interpuestos. Si el objeto es pequeño en relación a la longitud de onda, tiene muy poco efecto. La onda pasará alrededor del objeto sin perturbaciones. No obstante, si el objeto es grande, aparecerá una sombra detrás del mismo y una cantidad de energía significativa se refleja nuevamente hacia el origen. Si el objeto tiene alrededor del mismo tamaño que la longitud de onda, las cosas se complican, y aparecen patrones de difracción interesantes.

Utilice la actividad interactiva para calcular y mostrar gráficamente el ángulo de refracción para diferentes ángulos de incidencia y diferentes materiales.

Las ondas de radio también cambian de dirección al entrar en materiales diferentes. Esto puede ser muy importante al analizar la propagación en la atmósfera. No sólo es muy significativo para las WLANs, sino que se incluye aquí, como parte del trasfondo general para el comportamiento de las ondas electromagnéticas.

3.7.3 Reflexión

La reflexión tiene lugar cuando la luz rebota en la dirección general de la cual provino. Consideremos una superficie metálica lisa como interfaz. A medida que las ondas golpean la superficie, gran parte de su energía rebotará o se reflejará. Pensemos en experiencias comunes, como mirarse al espejo u observar la luz del sol reflejándose desde una superficie metálica o agua. Cuando las ondas viajan de un medio a otro, un determinado porcentaje de la luz se refleja. Esto se denomina reflexión de Fresnel.

Las ondas de radio también se reflejan al entrar en diferentes medios. La ley de reflexión puede describir estas reflexiones. Las ondas de radio pueden rebotar desde diferentes capas de la atmósfera. Las propiedades reflexivas del área donde ha de instalarse la WLAN son extremadamente importantes y pueden determinar si una WLAN funciona o falla. Además, los conectores a ambos extremos de la línea de transmisión que se dirigen a la antena deberán estar apropiadamente diseñados e instalados, para que no tenga lugar ninguna reflexión de las ondas de radio. Si la línea y los conectores no coinciden

apropiadamente, parte de la energía puede rebotar como eco y constituir una pérdida de potencia del sistema.

Utilice la actividad para calcular y mostrar gráficamente el ángulo de reflexión para diferentes ángulos de incidencia y diferentes materiales.

3.7.4 Difracción y dispersión

La dispersión de una onda en torno a un obstáculo se denomina difracción. [1](#) Esta dispersión se denomina en ocasiones rodear un obstáculo. No obstante, para evitar una posible confusión con la refracción, que es un proceso enteramente diferente, aquí utilizaremos el término difracción. Las ondas de radio pasan por una difracción a pequeña escala y a gran escala. Un ejemplo de difracción a pequeña escala son las ondas de radio de una WLAN que se dispersa en un ambiente interior. Un ejemplo de difracción a gran escala son las ondas de radio que se dispersan en torno a una montaña, hacia un área inaccesible.

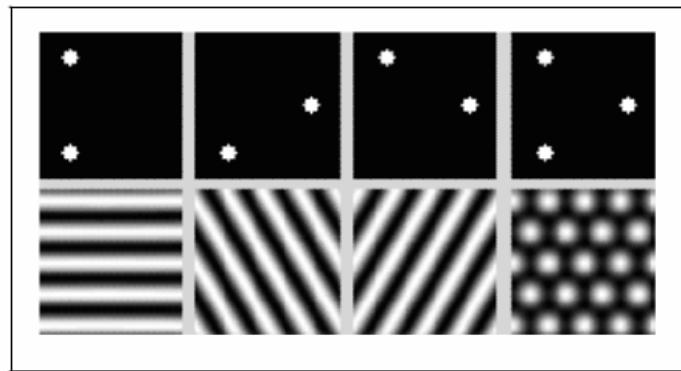


Figura 1

Un efecto diferente tiene lugar cuando la luz golpea pequeñas partículas. Dependiendo de la frecuencia de la luz y del tamaño y la composición de las partículas, es posible un fenómeno denominado dispersión. La dispersión en general resulta en el redireccionamiento de la energía de onda entrante hacia direcciones que no son la dirección deseada.

El sol irradia ondas visibles y otras ondas EM. Si no hubiera atmósfera, la luz llegaría directamente desde el sol y el resto del cielo estaría oscuro, excepto por las otras estrellas. Esta es exactamente la visión que se obtiene desde la luna. Sin embargo, en la tierra el cielo es azul. Eso se debe a que las moléculas de la atmósfera dispersan la luz azul, mucho más que los otros colores. El resultado es que aunque la luz del sol de la mayoría de los colores llega directamente hacia un observador en la tierra, la luz azul se dispersa a través de una porción tan grande de la atmósfera que ésta aparece esencialmente azul brillante. Esto se ilustra en la Figura [2](#).

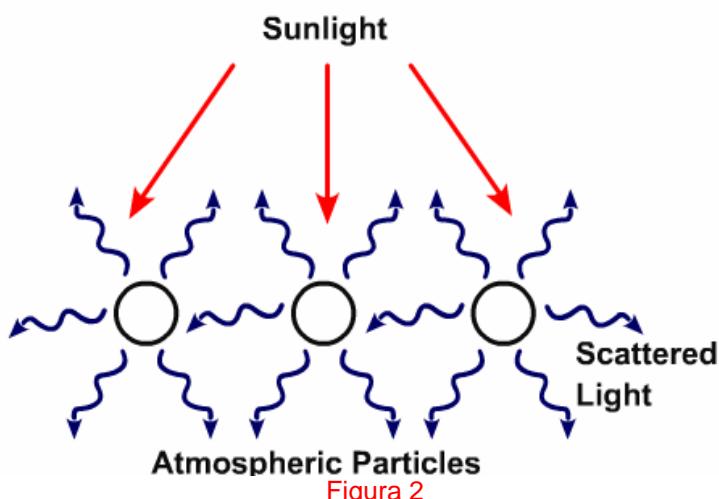


Figura 2

La luz se dispersa desde todos los tipos de materiales. La Figura [3](#) muestra por qué una nube tiene color blanco, lo cual es otro efecto de la dispersión.

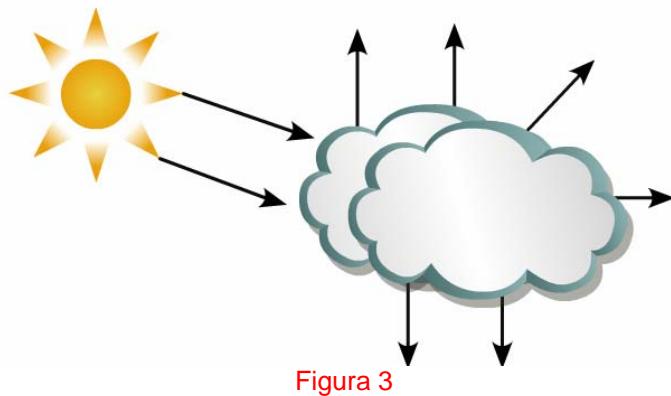


Figura 3

3.7.5 Multirruta

Imaginemos un sándwich de varias capas de materiales transparentes. Imaginemos que la capa central, el núcleo, tiene un índice de refracción más alto que el de las dos capas exteriores. Los rayos de luz que viajan en determinados ángulos a través del medio del núcleo se reflejarán desde las interfaces, de acuerdo a la ley de reflexión interna total. Ahora imaginemos una fuente de luz que emita en varios ángulos, y que todos ellos se reflejarían. Esto se denomina distorsión multirruta o interferencia [1](#).

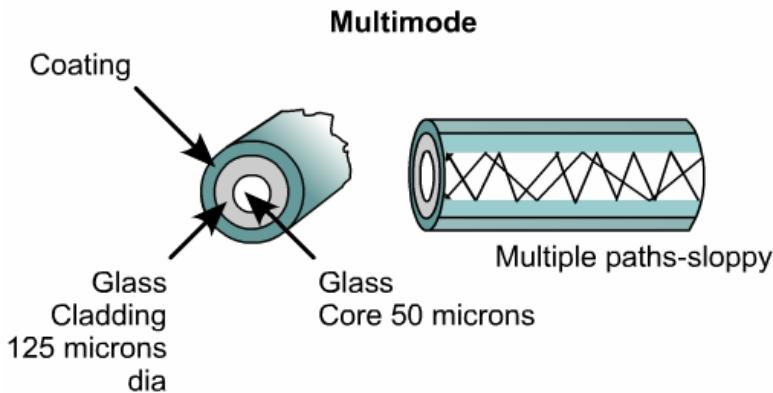


Figura 1

En muchas instalaciones comunes de WLAN, las ondas de radio emitidas desde un transmisor viajan a diferentes ángulos. Pueden reflejarse desde diferentes superficies y terminan llegando al receptor en momentos levemente diferentes. Todas las ondas viajan a aproximadamente la velocidad de la luz. No obstante, sólo una pequeña cantidad de diferencia temporal es necesaria, para resultar en una señal de microondas distorsionada. La interferencia multirruta puede dar fuerza a la señal RF, pero ocasionando niveles de calidad de la señal pobres. Éste es un tema importante a considerar al instalar WLANs.

Utilice la actividad interactiva para aprender más acerca de la distorsión multirruta. Se mostrará la ruta de dos rayos reflejados, desde una laptop a un AP. Nótese que los rayos toman rutas diferentes. Cuanto más larga es la ruta, más tiempo se requerirá para llegar al destino. En el destino, los dos rayos de luz pueden interferir entre sí, a través de una interferencia constructiva y destructiva. Si esta interferencia es lo suficientemente destructiva, los mensajes no llegarán. Esto es lo que puede ocurrir con las fibras ópticas multimodo.

3.7.6 Pérdida de la ruta

Un factor crucial en el éxito o fracaso de un sistema de comunicaciones es cuánta potencia procedente del transmisor llega al receptor. Se tratarán muchas formas diferentes en las cuales las ondas EM pueden verse afectadas, incluyendo reflexión, difracción y dispersión. Estos efectos diferentes pueden combinarse y describirse por medio de lo que se conoce como cálculos de pérdida de ruta. Los cálculos de pérdida de ruta determinan cuánta potencia se pierde a lo largo de la ruta de comunicaciones.

La pérdida del espacio libre (FSL) es la atenuación de la señal que resultaría si todas las influencias de absorción, difracción, obstrucción, refracción, dispersión y reflexión se eliminaran lo suficiente como para que no tuvieran ningún efecto en la propagación. La fórmula es la siguiente: [1](#)

$$\text{Free Space Loss} = 20\log_{10}(\text{Frequency in MHz}) + 20\log_{10}(\text{Distance in Miles}) + 36.6$$

Figura 1

$$\text{FSL (in dB)} = 20 \log_{10}(f) + 20 \log_{10}(d) + 36.6$$

Cada vez que la distancia desde el transmisor al receptor se duplica, el nivel de la señal baja (o se incrementa) en 6 dB. Además, para cada frecuencia, hay una serie de longitudes de onda, donde la energía escapará de la línea de transmisión y entrará al espacio que la rodea. Esto se denomina efecto de lanzamiento. El efecto de lanzamiento tiene lugar en general en múltiplos de media longitud de onda de la señal. Esto se ilustra en la Figura 2.

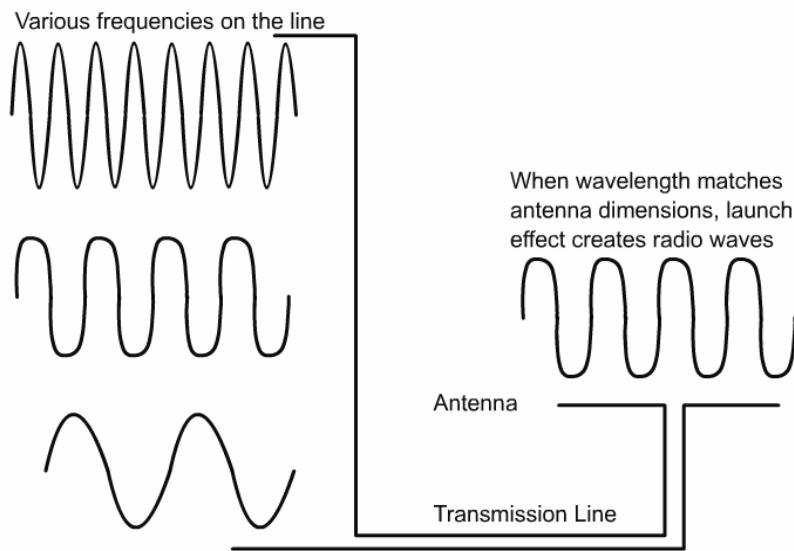


Figura 2

Utilice la calculadora de pérdida de ruta de la actividad interactiva para familiarizarse con este cálculo. Introduzca dos valores cualesquiera y el tercero se calculará. Luego, utilice el simulador de la segunda actividad interactiva para ver cómo esto puede afectar las comunicaciones entre WLANs.

Resumen

Este módulo trató la matemática y la física necesarias para comprender cómo operan las WLANs. Aunque usualmente no es necesario llevar a cabo cálculos complejos para instalar una WLAN, una comprensión de los principios subyacentes hace más fácil el darse cuenta de los muchos factores que pueden interferir con la operación apropiada de la WLAN.

Al llevar a cabo un sondeo de un sitio en busca de una WLAN nueva o existente, asegúrese de tener en cuenta factores tales como la refracción, la reflexión y la distorsión multirruta, que se trataron en este módulo.

Módulo 4: Topologías wireless

Descripción general

Los módulos anteriores trataban la teoría y operación básica de la tecnología inalámbrica, así como de los NICs y clientes inalámbricos. El Módulo 4 comenzará a tratar el diseño, la integración y la implementación práctica de las WLANs. Proporciona una transición de la teoría a los casos de WLAN del mundo real de LANs nuevas o existentes.

En primer lugar se presentarán las topologías y los componentes de las WLANs. Esto proporcionará un conocimiento previo, antes de presentar las fases de diseño e implementación. Se tratan los adaptadores cliente o NICs inalámbricas. La función principal de los adaptadores cliente es transferir los paquetes de datos de manera transparente, a través de la infraestructura inalámbrica. Estas NICs inalámbricas proporcionan comunicaciones de datos transparentes entre dispositivos inalámbricos fijos, portátiles o móviles, y entre otros dispositivos, tanto inalámbricos como cableados. Los access points y bridges también se presentan antes de que el alumno obtenga experiencia en el diseño y la implementación de redes inalámbricas.

Después de examinar los diferentes tipos de topologías inalámbricas, se tratan el establecimiento y el uso de los canales. Al igual que con cualquier buena configuración de networking, es necesario un diseño apropiado. Existen dos pasos críticos para una buena implementación de la WLAN. En primer lugar, debe determinarse la ubicación de los access points o bridges. En segundo lugar, deberán mapearse las asignaciones de canales.

Finalmente, se presenta una cantidad de configuraciones de muestra. El alumno tendrá la oportunidad de trabajar con el Diseñador de Redes Cisco para configurar y diseñar diferentes topologías de red. Esta actividad permitirá al alumno determinar la factibilidad de diversas topologías de red.

4.1 Componentes

4.1.1 Laptops y estaciones de trabajo

Los dispositivos más comunes utilizados en las WLANs son las estaciones de trabajo, que incluyen tanto a los modelos laptop como de escritorio. Fotos de computadoras laptop y de escritorio aparecen en las Figuras 1 y 2. Muchas corporaciones proporcionan laptops a su fuerza de trabajo en lugar de modelos de escritorio. Mientras se encuentra en la oficina, la laptop se conecta en general a una estación de acoplamiento con un gran monitor, un teclado completo y un mouse, para un uso más ergonómico. La laptop se transporta fácilmente para su uso en los negocios o personal, en el hogar o en el camino. Esto ha eliminado la necesidad de dos sistemas para cada empleado y la necesidad de transferir archivos constantemente entre dos PCs. Las laptops y las estaciones de acoplamiento eliminan las preocupaciones acerca de dejar un archivo necesario en el escritorio mientras se está lejos de la oficina. Lo que es más, las corporaciones pueden reducir los gastos asociados con la adquisición y el mantenimiento de dos dispositivos por cada empleado.



Figura 1



Figura 2

Las computadoras laptop y las computadoras notebook se están volviendo cada vez más populares, como las computadoras palm top, los asistentes personales digitales (PDAs), y otros dispositivos de computación

pequeños. La principal diferencia entre computadoras de escritorio y laptops es que los componentes de una laptop son más pequeños. En lugar de slots de expansión, hay slots PCMCIA, donde pueden insertarse las NICs, las NICs inalámbricas, los módems, las unidades de disco duro y otros dispositivos útiles. La placa tiene usualmente el tamaño de una tarjeta de crédito gruesa. Se inserta en los slots PCMCIA, a lo largo del perímetro. El uso de las NICs inalámbricas elimina la necesidad de adaptadores, conectores y cables engorrosos.

Un resultado de la movilidad del usuario es el incremento en la productividad. Por ejemplo, las reuniones y conferencias se han convertido en menos desafiantes. El acceso a los recursos en general era más limitado o requería tiempo valioso para prepararse, como copiar todos los archivos necesarios a la laptop antes de la reunión. Con las laptops habilitadas para la WLAN, los usuarios pueden simplemente recoger sus cosas y marcharse, con todos sus recursos disponibles. Además, los usuarios se conectan a los recursos corporativos durante la reunión, lo cual significa que la mensajería instantánea, el email, la impresión, los archivos y el acceso a Internet son fácilmente accesibles.

Si las computadoras de escritorio se encuentran actualmente en uso, pueden convertirse fácilmente de sistemas cableados a inalámbricos, cambiando la NIC e implementando access points. Las NICs inalámbricas también están disponibles como adaptadoras PCI. Esto puede parecer un retroceso, si Ethernet 10/100 ya está instalada. No obstante, cuando tenga lugar la siguiente reorganización de la oficina, no se requerirá un costoso recableado. Mientras las aplicaciones no requieran un ancho de banda mayor que 54 Mbps, las WLANs son una opción viable.

Una gran ventaja del uso del estándar 802.11 es que muchas laptops ahora se venden con NICs inalámbricas compatibles pre-instaladas. Sin ninguna modificación, estos dispositivos pueden interesar con cualquier producto Aironet, así como con otros dispositivos que cumplan con IEEE. El estándar IEEE 802.11b se trata en detalle en el Módulo 2.

La prueba de productos en diferentes configuraciones de hardware y software incluye ahora los dispositivos WLAN, como las NICs, los clientes de software y los access points (APs). Es importante completar esta fase, para asegurarse de que la red cumple con los requisitos del negocio. Incluso con las grandes ventajas de las WLANs, éstas pueden no ser viables en algunas situaciones.

La Figura 3 muestra que los dispositivos tales como las PCs y laptops operan en la totalidad de las siete capas del Modelo de Referencia OSI. Estos dispositivos llevan a cabo funciones que pueden asociarse a cada capa del modelo OSI.

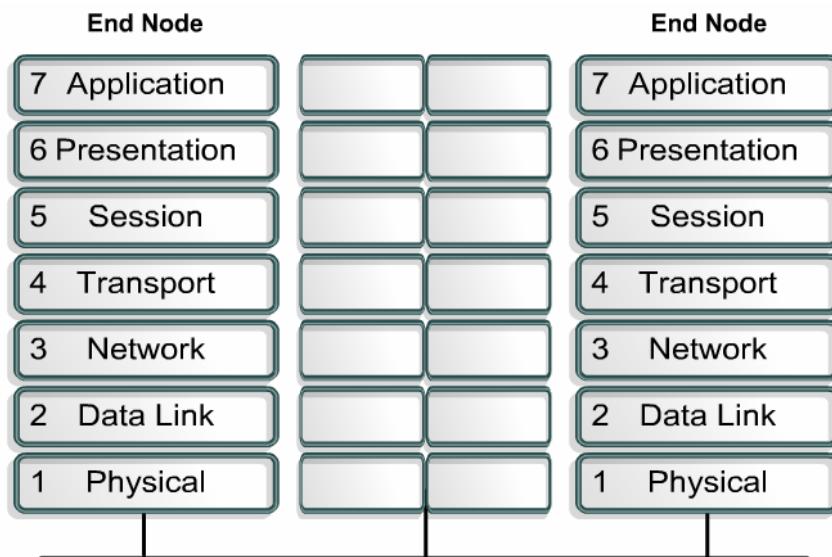


Figura 3

4.1.2 Computadoras móviles, PDAs, y lectores de código de barras

Las computadoras móviles vienen en diferentes tamaños y formas, y utilizan diferentes sistemas operativos. El objetivo es proporcionar soluciones para una variedad de entornos. Algunas de estas opciones se resumen en la Figura 1.

Mobile Computers

Designs

- Key-based computers
- Pen/touch computers
- Stationary and vehicle-mount
- Wearable (scanning) computers

Communication Types

- Batch processing
- Real-time communications

Operating Systems

- MS DOS
- Palm OS
- Symbian OS
- Windows CE
- Windows XP Embedded (x86 CPU only)

Figura 1

Algunos dispositivos utilizan una NIC inalámbrica integrada, mientras que otros utilizan una que se basa en la placa PCMCIA o CompactFlash. Existen tres tipos básicos de dispositivos handheld. Se basan en teclas, punteros y montaje en vehículos. Los dispositivos handheld permiten a los usuarios navegar en la web, acceder a recursos de la LAN, capturar datos en tiempo real, escanear e imprimir. Estos dispositivos se construyen en general para soportar ambientes hostiles, a diferencia de la mayoría de las computadoras laptop y PCs. La computación móvil es muy buena para la recolección, el procesamiento y la información de comunicaciones y datos cuándo y dónde sea necesario. Estos dispositivos también operan en la totalidad de las siete capas del modelo OSI como las laptops y PCs de escritorio.

Los dispositivos basados en teclas se utilizan para aplicaciones que requieren una entrada manual de datos de caracteres. Tales dispositivos tienen un teclado alfanumérico completo, así como una pantalla LCD. Las computadoras basadas en teclas se encuentran en muchos negocios incluyendo minoristas, mayoristas y quienes envían pedidos.

Los dispositivos basados en punteros utilizan un puntero similar a una lapicera y en general no poseen teclado ni teclado numérico. Un ejemplo de ellos se muestra en la Figura 2. Estos dispositivos están diseñados específicamente para aplicaciones intensivas en cuanto a la información. Son muy resistentes y pueden llevarse prácticamente a cualquier lado. Estos dispositivos no requieren tipar en un teclado pequeño.



Figura 2

Los dispositivos móviles montados en vehículos, tienen como objetivo su uso en autoelevadores o carritos móviles. Muchos de estos dispositivos pueden conectarse mediante un puerto a un escáner de código de

barras. Esto permite a los operadores transmitir y recibir datos hacia y desde un servidor remoto. Vienen en diversas variedades, incluyendo algunas con teclados, manipuladas por menú y pantallas táctiles.

Sistemas Operativos (OS) de computación móvil

Varios sistemas operativos se utilizan en computadoras móviles. Los principales, enumerados en la Figura 1, incluyen MS DOS, Palm OS, Symbian OS, Windows Compact Edition (CE), y Windows XP Embedded. DOS es un SO muy básico y eficiente que ejecutará un programa a la vez. Los otros SOs ejecutarán múltiples programas a la vez. El Palm OS es un SO que fue desarrollado especialmente para las PDAs. Symbian OS es un SO de estándares abiertos, licenciado para su uso en muchos dispositivos de computación móviles y fácilmente personalizables con software de terceros. Windows CE y Windows XP embedded son versiones simplificadas de Windows. Windows XP Embedded es sólo para su uso en CPUs x86. El aspecto es muy similar al de las versiones de escritorio de Windows. Una versión temprana de Windows CE se denominaba Pocket PC. Recuerde que la computadora móvil debe ser interoperable con los protocolos de PC de escritorio, o de lo contrario puede ser necesario software adicional.

Otros dispositivos de computación móviles

La primera fase de dispositivos de voz que cumplen con 802.11 ya está disponible. Incluyen dispositivos handheld de Cisco y Symbol. La segunda fase soportará tanto datos como voz en un único dispositivo handheld, como Compaq iPaq. Los productos de voz IEEE 802.11 deben integrarse a una plataforma de administración de voz basada en servidores como Cisco Call Manager. Cisco Call Manager se presentará en la última sección. La última sección también trata la Arquitectura de Cisco para Voz, Video y Datos Integrados (AVVID).

Los dispositivos móviles pueden basarse en diferentes estándares de tecnología inalámbrica. Es importante utilizar sólo dispositivos que cumplan con 802.11. Las grandes ventajas de hacer esto incluyen la interoperabilidad, velocidad, confiabilidad y comunicaciones de datos en tiempo real. Igualmente importante es elegir un paquete de aplicación de software que sea compatible con los dispositivos utilizados en un entorno dado. Otras consideraciones incluyen la vida y duración de la batería. Algunos usos de dispositivos móviles con aplicaciones de terceros se tratarán posteriormente en el curso.

4.1.3 Clientes y adaptadores

Los Adaptadores de WLAN Cisco Aironet, también denominados adaptadores cliente o NICs, son módulos de radio. Se los ilustra en la Figura 1. La función principal de estas NICs inalámbricas es proporcionar comunicaciones de datos transparentes entre otros dispositivos, tanto inalámbricos como cableados. Los adaptadores clientes son completamente compatibles con dispositivos que soportan la tecnología Plug-and-Play (PnP).



Figura 1

Las NICs operan tanto en la Capa 1 como en la 2 del Modelo de Referencia OSI, como lo muestra la Figura 2. Los adaptadores operan de manera similar a un adaptador de red estándar, excepto en que el cable ha sido reemplazado por una conexión de radio. No se requiere ninguna función de networking inalámbrico especial. Podrán operar todas las aplicaciones existentes que operan a través de una red cableada, utilizando adaptadores inalámbricos.

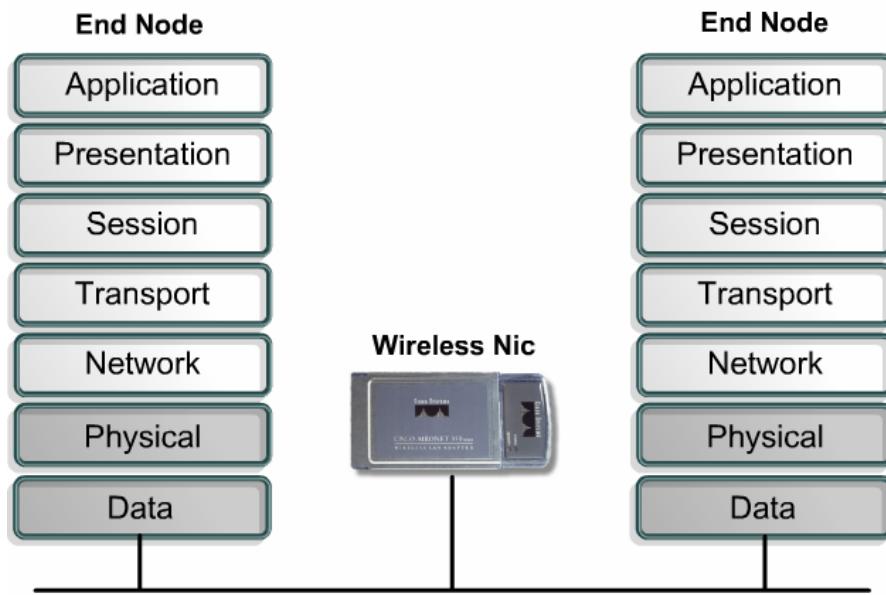


Figura 2

Al igual que con Ethernet, es necesario un controlador para comunicarse con el SO de la computadora. Existen tres tipos de controladores disponibles para los adaptadores cliente inalámbricos. Éstos son NDIS, ODI, y Paquete. El disco de controladores para Windows de Aironet incluye controladores para Windows 95, 98, ME, NT, 2000, y XP. Además, el controlador se incluye en el CD de los sistemas operativos Windows Me, Windows 2000, y Windows XP.

Los diferentes tipos de controladores y sus plataformas son los siguientes:

- Especificación de Interfaz de Controlador de Red (NDIS) — El propósito principal de NDIS es definir un API estándar para las NICs. NDIS también proporciona una biblioteca de funciones que pueden ser utilizadas por los controladores MAC, así como controladores de protocolo de más alto nivel, como TCP/IP. Las versiones actuales de NDIS utilizadas por Windows son especificaciones propietarias de Microsoft. Los controladores son soportados bajo 95/98, ME, NT, 2000, y XP. También se soporta Novell NetWare Client32.
- Interfaz abierta de enlace de datos (ODI) — ODI es análoga a NDIS, pero es específica de NetWare. Se la utiliza en los entornos Novell NetWare 3.x y 4.x y funciona con NETX o VIMs. Los controladores ODI funcionarán también bajo DOS.
- Paquete — Esta interfaz sirve para su uso con pilas IP basadas en DOS. Algunas de las pilas IP basadas en DOS que funcionan con los productos Cisco Aironet incluyen el Software FTP y NetManage.
- Windows CE — Windows CE es necesario para desarrollar una versión compilada separadamente del controlador, basándose en cada procesador y versión. Se soportan los controladores Cisco Aironet para las versiones 2.11 y 3.0 de Windows CE.

4.1.4 Access points y bridges

El access point (AP) opera en las Capas 1 y 2 del Modelo de Referencia OSI. Aquí es también donde operan el bridge inalámbrico y el bridge de grupos de trabajo, como lo muestra la Figura 1.

Access points

Un access point (AP) es un dispositivo WLAN que puede actuar como punto central de una red inalámbrica autónoma. Un AP también puede utilizarse como punto de conexión entre redes inalámbricas y cableadas. En grandes instalaciones, la funcionalidad de roaming proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente a través de la instalación, a la vez que se mantiene un acceso sin fisuras e ininterrumpido a la red.

Los APs Cisco vienen en varios modelos. La Serie 1100 soporta IEEE 802.11b. La Serie 1200, que se muestra en la Figura 2, soporta a 802.11a y 802.11b en la misma unidad. También soporta inyección de potencia por línea entrante, para ahorrar costos de cableado AC, y conectores Ethernet tanto RJ45 como 10/100.

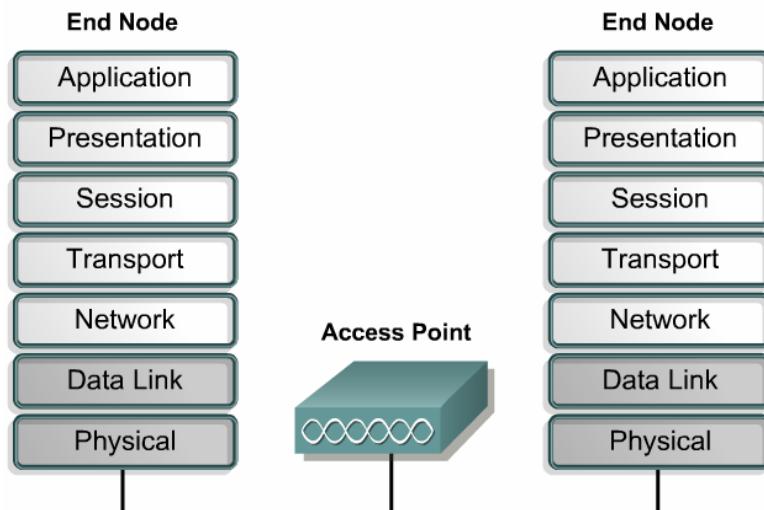


Figura 1



Figura 2

Bridges inalámbricos

El Bridge Inalámbrico Cisco Aironet Serie 350 está diseñado para conectar dos o más redes ubicadas en general en diferentes edificios. Proporciona elevadas velocidades de datos y un throughput superior para aplicaciones intensivas en cuanto a los datos, de línea de visión. Los bridges conectan sitios difíciles de cablear, pisos no contiguos, oficinas satelitales, instalaciones de campus de escuelas o corporaciones, redes temporales y depósitos. Pueden configurarse para aplicaciones punto a punto o punto a multipunto. Los bridges inalámbricos y bridges de grupo de trabajo Cisco, junto con sus iconos gráficos estándar, se muestran en la Figura 3.



Figura 3

Bridges de grupo de trabajo

El producto bridge de grupo de trabajo (WGB) Cisco Aironet 350 se conecta al puerto Ethernet de un dispositivo que no tiene un slot PCI o PCMCIA disponible. Proporciona una única conexión de dirección MAC a un AP, y al backbone de la LAN. El bridge de grupo de trabajo Aironet no puede utilizarse en una conexión de modo peer-to-peer. Debe comunicarse con un AP.

Una configuración del bridge de grupo de trabajo se conectaría hasta con ocho máquinas cableadas a un AP. Es ideal para conectar grupos de trabajo remotos a una LAN inalámbrica, según se muestra en la Figura 4.

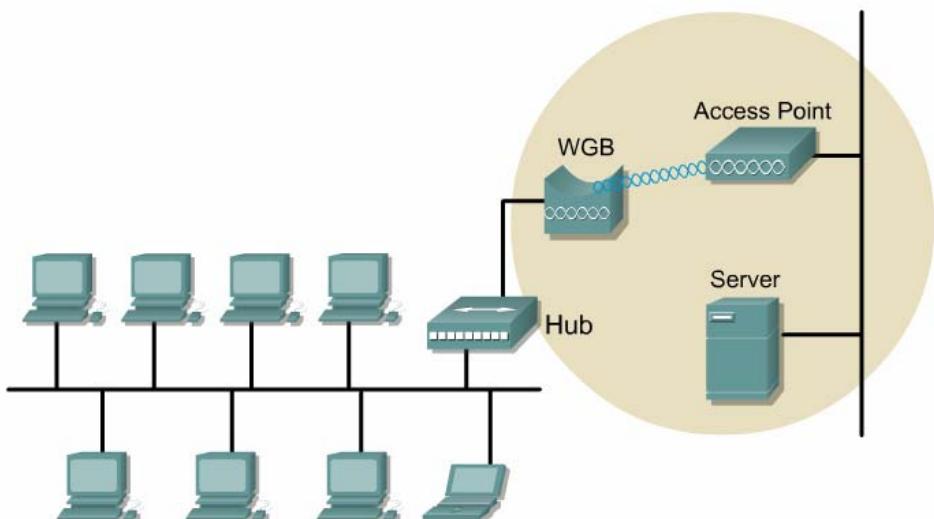


Figura 4

Para utilizar un WGB con múltiples direcciones MAC, el WGB y todos los usuarios deben conectarse a un hub. La unidad seleccionará automáticamente las primeras ocho direcciones MAC que escucha en la Ethernet. Como alternativa, las direcciones pueden introducirse manualmente en una tabla. Las ocho direcciones MAC son estáticas.

4.1.5 Antenas

Los access points Cisco Aironet de 2,4 GHz están disponibles con antenas integradas bipolares o con conectores tipo Conector Naval A Rosca (TNC), que le permiten a un cliente conectar diferentes tipos de antenas. Los usuarios pueden escoger la antena correcta para su aplicación a partir de una amplia selección de productos Cisco, que se ilustra en la Figura 1.

Type	Omni	Directional	Omni	Directional	Omni	Omni
Gain	2.15 dBi	5.2 dBi	5.2 dBi	8.5 dBi	2.2 dBi	5.2 dBi
Beamwidth	360° H 75° V	360° H 75° V	360° H 75° V	60° H 55° V	360° H 75° V	360° H 75° V
Indoor Range at 1Mbps	300' 91.4 m	497' 151.4 m	497' 151.4 m	700' 213.3 m	350' 106.6 m	497' 154.4 m
Indoor Range at 11Mbps	100' 30.4 m	142' 43.2 m	142' 43.2 m	200' 60.9 m	100' 30.4 m	142' 43.2 m
Cable Length	N/A	3' .91 m	3' .91 m	3' .91 m	9' 2.7 m	3' .91 m

Figura 1

Las antenas del AP Cisco Aironet de 2,4 GHz son compatibles con todos los APs equipados con Cisco RP-TNC. Las antenas están disponibles en diferentes capacidades de ganancia y rango, amplitudes del rayo y factores de forma. El acoplar la antena correcta en el AP correcto permite una cobertura eficiente en cualquier instalación, así como una mayor confiabilidad a velocidades de datos más altas. Una cobertura detallada de las antenas se proporcionará posteriormente en el curso.

Las antenas del bridge Cisco Aironet de 2,4 GHz proporcionan transmisión entre dos o más edificios. Cisco tiene una antena de bridge para cada aplicación. Estas antenas están disponibles en configuraciones direccionales para la transmisión punto a punto y en configuración omnidireccional para implementaciones punto a multipunto. Para distancias de hasta 1,6 km (1 milla), Cisco ofrece un mástil omnidireccional. Para distancias intermedias, Cisco ofrece un mástil Yagi y un mástil omnidireccional. La antena parabólica sólida proporciona conexiones de hasta 40 km (25 millas). Las antenas de bridge Cisco Aironet se muestran en la Figura 2.

					
Type	Directional	Omni	Omni	Directional	Directional
Gain	8 dBi	5.2 dBi	12 dBi	13.5 dBi	21 dBi
Beamwidth	60° H 55° V	360° H 75° V	360° H 75° V	30° H 25° V	12.4° H 12.4° V
Approximate Range at 2 Mbps	2.0 miles 3.21 k	5000' 1,524 m	4.6 miles 7.4 k	6.5 miles 10.46 k	25 miles 40.23 k
Approximate Range at 11 Mbps	3390' 1,033.2 m	1580' 481.5 m	1.4 miles 2.25 k	2 miles 3.21 k	11.5 miles 18.50 k
Cable Length	3' .91 m	3' .91 m	1' .305 m	1.5' .457 m	2' .609 m

Figura 2

Las antenas operan en la Capa 1 del Modelo OSI, según se muestra en la Figura 3. Recuerde que la capa física define las especificaciones eléctricas, mecánicas, procedimentales y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Características tales como los niveles de voltaje, la temporización de los cambios de voltaje, las velocidades de datos físicas, las distancias máximas de transmisión, los conectores físicos, y otros atributos similares están definidos por especificaciones de la capa física.

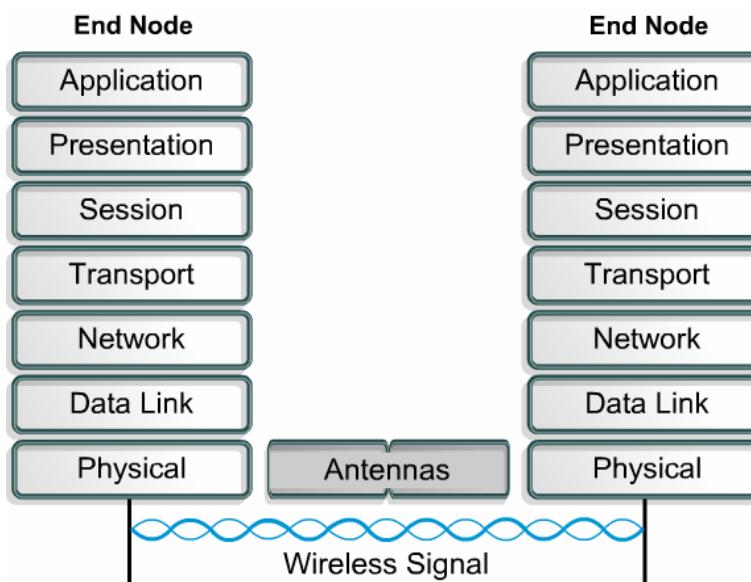


Figura 3

4.1.6 Ethernet y LANs cableadas

Una topología WLAN puede ser una extensión de una LAN escalable existente. Las internetworks mejor construidas y administradas se diseñan en general en capas, siguiendo un modelo jerárquico. Utilizando capas jerárquicas, el usuario puede dividir una red grande en trozos más pequeños, que pueden tratarse cada uno por separado. Para comprender la importancia de la división en capas, consideremos el Modelo de Referencia OSI. El Modelo de Referencia OSI es un modelo en capas para comprender e implementar comunicaciones en las computadoras. Dividiendo la funcionalidad de la red total en trozos más pequeños, o capas, el modelo OSI simplifica las tareas requeridas para que dos computadoras se comuniquen. La Actividad 4.1.6a muestra muchos de los dispositivos que existen en un entorno corporativo típico. Los dispositivos se muestran en la capa más alta del Modelo OSI, en la cual operan.

Los modelos jerárquicos para el diseño de internetworks también utilizan capas, para simplificar la tarea requerida para el internetworking. Cada capa puede concentrarse en funciones específicas, permitiendo así al usuario elegir los sistemas y las funciones apropiadas para la capa. Como resultado de ello, un modelo jerárquico simplifica la administración de la internetwork y permite al usuario controlar el crecimiento, sin pasar por alto los requisitos de la red. El modelo jerárquico de tres capas de Cisco se muestra en la Figura 1.

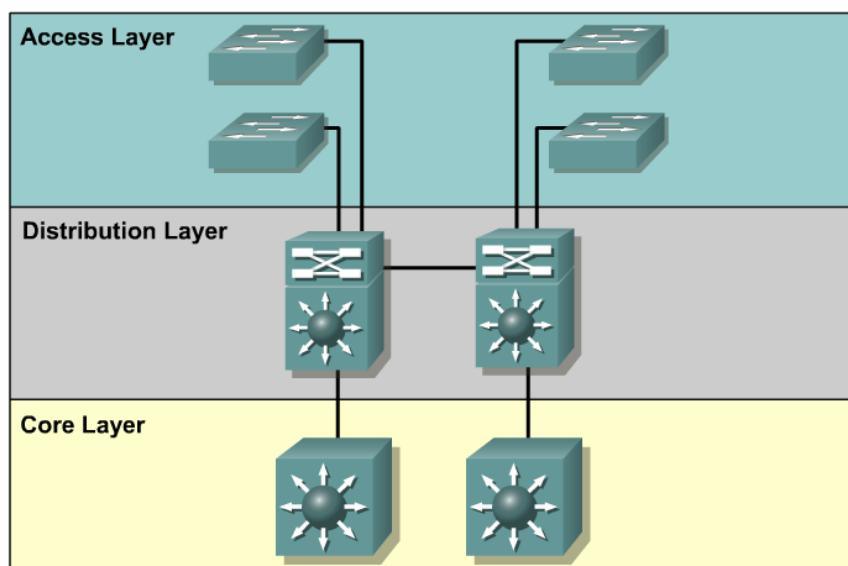


Figura 1

Los dispositivos cableados tradicionales que se utilizan incluyen routers, switches, servidores e impresoras. Estos dispositivos se muestran en las Figuras 2 a 5, junto con sus íconos gráficos. Tecnologías en desarrollo, como voz sobre IP (VoIP), pueden agregar capacidades adicionales para LANs tanto cableadas como Inalámbricas. Los teléfonos IP y el ícono gráfico se muestran en la Figura 6. Finalmente, los dispositivos de seguridad como firewalls, dispositivos VPN y sistemas de detección de intrusiones se convierten en requisitos para una LAN/WAN segura. Un firewall Cisco PIX y su ícono se ilustran en la Figura 7.

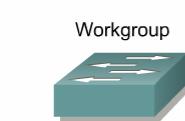
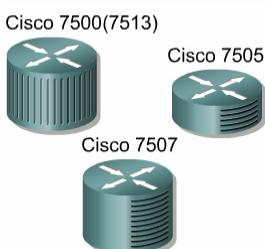


Figura 2

Figura 3



Figura 4



Figura 5



Figura 6



Figura 7

Al implementar una solución WLAN deben considerarse todos los dispositivos. Esto se debe a que la WLAN debe interoperar sin fisuras con la red cableada existente. La configuración de seguridad WLAN se tratará posteriormente en el curso. La LAN cableada continuará como porción predominante del sistema de red completo y moderno.

4.2 Topologías WLAN

4.2.1 Modularidad

La capa principal es la internetwork central de toda la empresa y puede incluir backbones de LAN y WAN. La función principal de esta capa es proporcionar una estructura de transporte optimizada y confiable y enviar tráfico a altas velocidades. Además, la capa principal es un backbone de conmutación de alta velocidad. Puesto que el trabajo primordial de un dispositivo de la capa principal de la red es conmutar paquetes, el alumno deberá diseñar la capa principal para que commute los paquetes tan rápido como sea posible. Por lo tanto, la capa principal de la red no deberá llevar a cabo ninguna manipulación de paquetes. La manipulación de paquetes, como el verificar las listas de acceso o el filtrado, ralentizaría la conmutación.

La modularidad es otro beneficio de utilizar un diseño jerárquico, porque se ven facilitados los cambios en la internetwork. La Figura 1 muestra las tres capas principales de un diseño de red jerárquico. Además, la modularidad en el diseño de redes permite al usuario crear elementos de diseño que pueden replicarse a medida que la red crece. Cuando un elemento del diseño de la red requiere un cambio, el costo y la complejidad de efectuar la actualización se ve restringida a un pequeño subconjunto de la red total. En grandes arquitecturas de red planas o de malla, los cambios tienden a tener un impacto en una gran cantidad de sistemas.

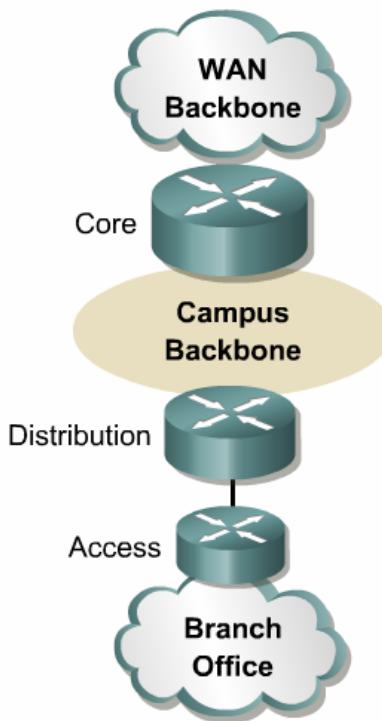


Figura 1

La estructura modular de la red en elementos pequeños y fáciles de comprender también simplifica el aislamiento de fallos. El usuario puede comprender fácilmente los puntos de transición de la red, e identificar así puntos de fallo.

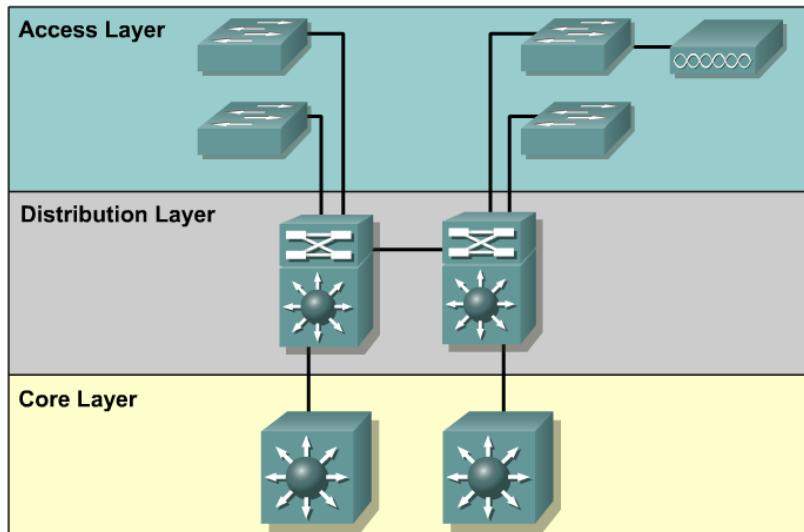


Figura 2

El modelo de internetworking jerárquico de tres capas de Cisco se ilustra en la Figura 2. En ocasiones se considera equivocadamente que las capas principal, de distribución y de acceso deben existir cada una como entidad física clara y diferenciada. No obstante, éste no tiene por qué ser el caso. Las capas se definen para ayudar a un diseño exitoso de la red y para representar la funcionalidad que debe existir en una red. Cada capa puede encontrarse en routers o switches diferenciados, puede combinarse en un único dispositivo o puede omitirse totalmente. La forma en la cual se implementan las capas depende de las necesidades de la red que se está diseñando. Nótese que debe mantenerse una jerarquía para que la red funcione de manera óptima.

4.2.2 Categorías de WLAN

Las WLANs son elementos o productos de la capa de acceso. Los productos WLAN se dividen en dos categorías principales:

1. LANs inalámbricas en el interior de un edificio

2. Bridging inalámbrico de edificio a edificio

Las WLANs reemplazan al medio de transmisión de la Capa 1 de una red cableada tradicional, que es usualmente un cable de Categoría 5, por transmisión de radio por el aire. Las WLANs también reemplazan la funcionalidad MAC de Capa 2, con controladores MAC inalámbricos. Los productos MAC pueden enchufarse a una red cableada y funcionar como aditamento de las LANs tradicionales o cableadas. Las WLANs también pueden implementarse como LAN autónoma, cuando un networking cableado no es factible. Las WLANs permiten el uso de computadoras de escritorio, portátiles y dispositivos especiales de un entorno donde la conexión a la red es esencial. Las WLANs se encuentran en general dentro de un edificio, y se las utiliza para distancias de hasta 305 m (1000 pies). Las WLANs utilizadas apropiadamente pueden proporcionar un acceso instantáneo desde cualquier lugar de una instalación. Los usuarios podrán hacer roaming sin perder sus conexiones de red. La WLAN Cisco proporciona una completa flexibilidad.

Los bridges inalámbricos permiten a dos o más redes que están físicamente separadas conectarse en una LAN, sin el tiempo ni los gastos ocasionados por los cables dedicados o por las líneas T1. Ejemplos de aplicaciones de bridge inalámbricas se muestran en las Figuras 1 y 2.

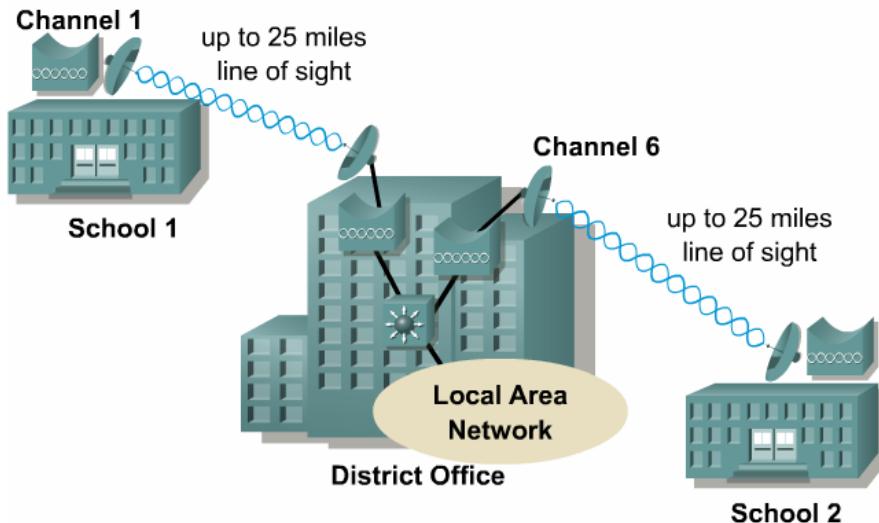


Figura 1

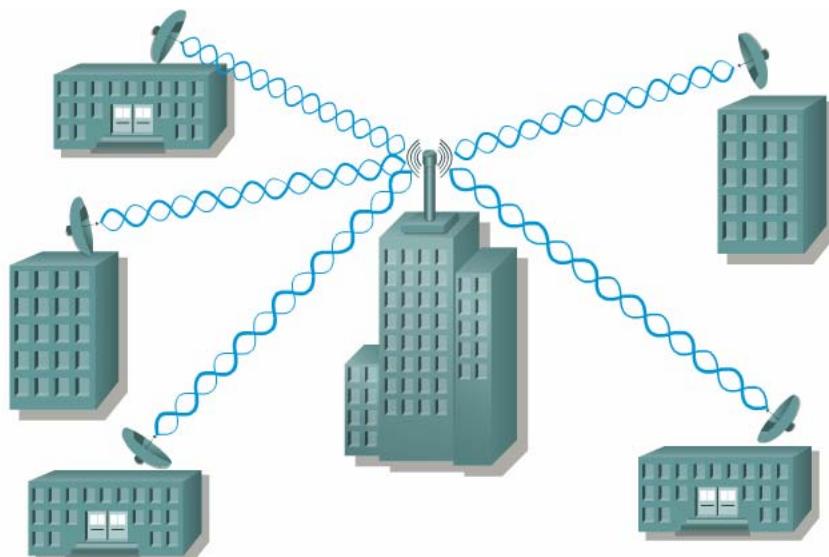


Figura 2

4.2.3 Redes de área local (LANs)

Las LANs cableadas requieren que los usuarios permanezcan en una única ubicación. Las WLANs son una extensión de la red LAN cableada. Las WLANs también pueden ser un sustituto completo de las redes LAN cableadas tradicionales. En el caso de las WLANs Cisco, los usuarios móviles pueden hacer lo siguiente:

- Desplazarse libremente por una instalación
- Disfrutar de un acceso en tiempo real a la LAN cableada, a velocidades de Ethernet cableada
- Acceder a todos los recursos de las LANs cableadas

El conjunto básico de servicios (BSS) es el área de cobertura de RF proporcionada por un único access point. También se denomina microcélula. Como se muestra en la Figura 1, un BSS puede extenderse agregando otro AP. Cuando más de un BSS se conecta a una LAN inalámbrica, esto se denomina conjunto extendido de servicios (ESS). Agregar un AP también es una forma de agregar dispositivos inalámbricos y de extender el alcance de un sistema cableado existente.

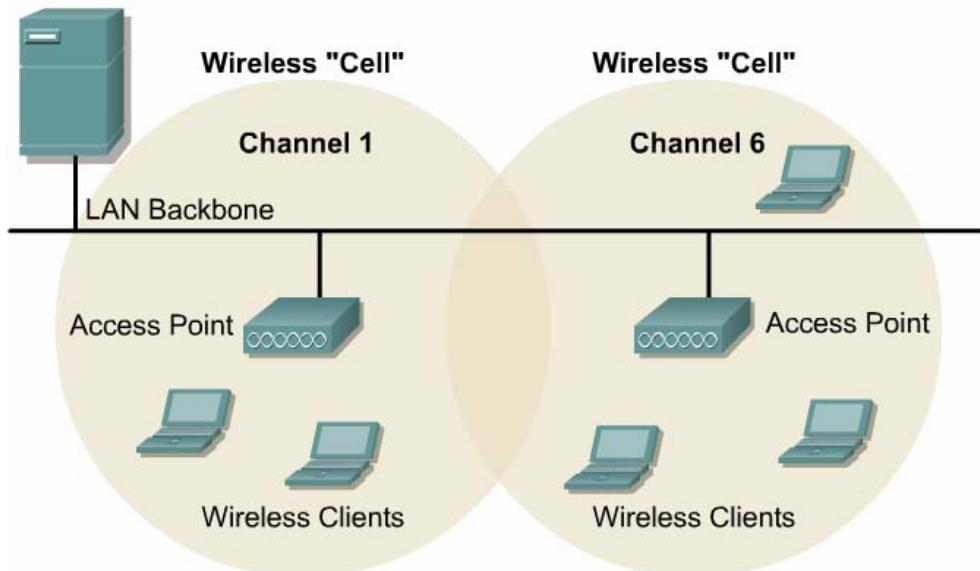


Figura 1

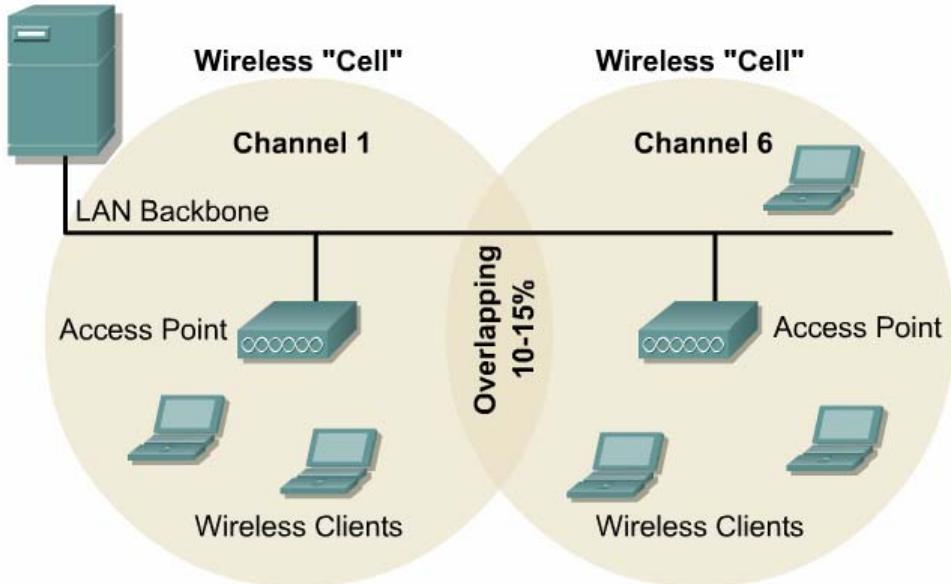


Figura 2

El AP se conecta al backbone de Ethernet y también se comunica con todos los dispositivos inalámbricos del área de la célula. El AP es el master de la célula. Controla el flujo de tráfico hacia y desde la red. Los dispositivos remotos no se comunican directamente entre sí. En cambio, los dispositivos se comunican a través del AP.

Si una única célula no proporciona la suficiente cobertura, se puede agregar cualquier cantidad de células para extender el alcance. Se recomienda que las células BSS adyacentes tengan de un 10 a un 15 por ciento de superposición, como se muestra en la Figura 2. Esto permite a los usuarios remotos hacer roaming sin perder conectividad RF. Las células fronterizas deberán configurarse a canales, o frecuencias, no superpuestas y diferentes para un mejor desempeño.

4.2.4 Repetidor inalámbrico

En un entorno donde es necesaria una cobertura extendida, pero el acceso al backbone no es práctico o no está disponible, puede utilizarse un repetidor inalámbrico. Un repetidor inalámbrico es simplemente un access point que no está conectado al backbone cableado. Esta configuración requiere una superposición del 50% del AP en el backbone y en el repetidor inalámbrico, como lo muestra la Figura 1.

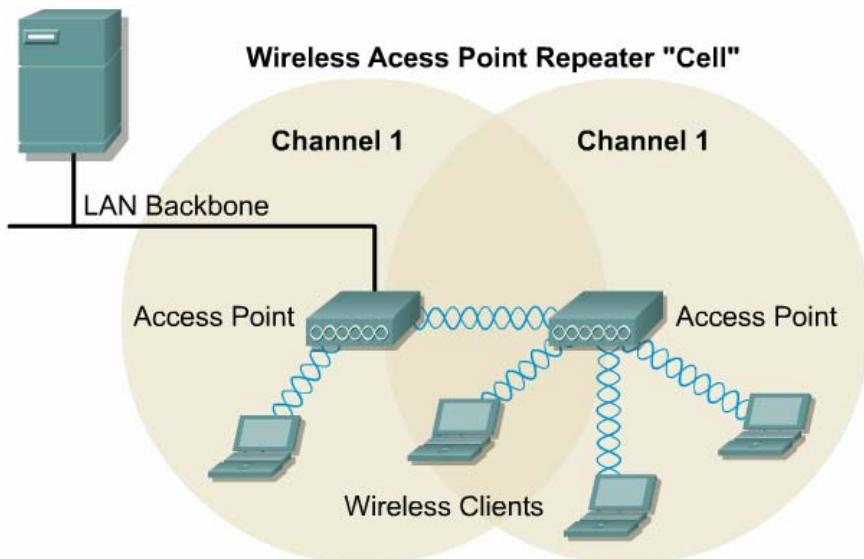


Figura 1

El usuario puede configurar una cadena de varios access points repetidores. No obstante, el throughput de los dispositivos clientes que se encuentran en el extremo de la cadena de repetidores puede ser muy bajo. Esto se debe a que cada repetidor debe recibir y luego retransmitir cada paquete por el mismo canal. Por cada repetidor agregado a la cadena, el throughput se reduce a la mitad. Se recomienda el uso de no más de dos saltos.

Al configurar los access points repetidores utilice las siguientes directrices:

- Utilice repetidores para servir a dispositivos clientes que no requieren un throughput elevado. Los repetidores extienden el área de cobertura de la WLAN, pero reducen drásticamente el throughput.
- Utilice repetidores cuando los dispositivos clientes que se asocian a los repetidores son clientes Cisco Aironet. Los dispositivos cliente que no son Cisco en ocasiones tienen problemas para comunicarse con los access points repetidores.
- Utilice antenas omnidireccionales, como las que se venden con el access point, para los access points repetidores.

En general, dentro de los edificios la disponibilidad de las conexiones Ethernet está muy generalizada. Los repetidores pueden utilizarse para extender los APs del borde del edificio a las porciones exteriores que rodean al edificio, para un uso temporal. Por ejemplo, un cliente podría utilizar APs en modo repetidor para extender la cobertura en la playa de estacionamiento durante una época pico de ventas de un supermercado.

La asociación de clientes se asigna al AP cableado/raíz y no al AP que actúa como repetidor.

4.2.5 Redundancia del sistema y equilibrio de la carga

En una LAN donde es esencial tener comunicaciones, algunos clientes requerirán redundancia. Con los productos de espectro expandido de secuencia directa (DSSS) de un fabricante diferente, ambas unidades AP se configurarían según la misma frecuencia y velocidad de datos, según se ilustra en la Figura 1. Puesto que estas unidades comparten el tiempo de la frecuencia, sólo una unidad puede hablar a la vez. Si dicha unidad pasa a inactividad por alguna razón, los clientes remotos transferirán la comunicación a la otra unidad activa. Aunque esto sí proporciona redundancia, no proporciona más throughput que el que proporcionaría un único AP.

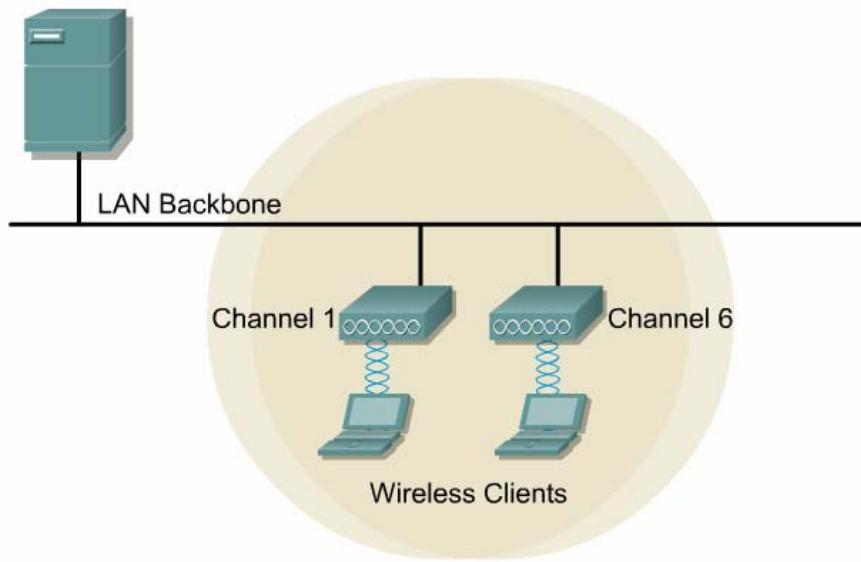


Figura 1

En el caso de los sistemas Cisco DS, las unidades se instalan en canales diferentes. Los clientes remotos equilibrarán la carga, cuando ambas unidades estén activas, según lo muestra la Figura 2. Si una unidad pasa a inactividad, los clientes remotos transferirán la comunicación a la unidad restante y continuarán trabajando. El equilibrio de la carga puede configurarse basándose en la cantidad de usuarios, la tasa de errores de bit o la fuerza de la señal.

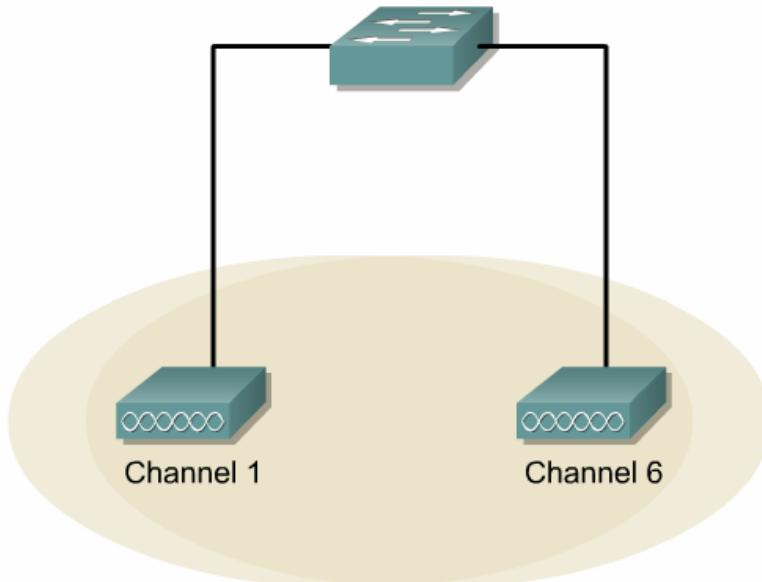


Figura 2

Otra opción, cuando la tolerancia a fallos y la disponibilidad son críticas, es un AP hot-standby. En este caso, no existe un equilibrio de la carga. Para implementaciones críticas para los negocios, un AP Cisco Aironet puede configurarse como hot-standby redundante de otro AP en la misma área de cobertura. El AP hot-standby monitorea continuamente al AP principal del mismo canal, y asume su papel en el raro caso de un fallo del AP principal. El standby estará listo para tomar su lugar, si el AP principal ya no está disponible. Nótese que ambos APs de la Figura 3 utilizan el mismo canal, o Canal X.

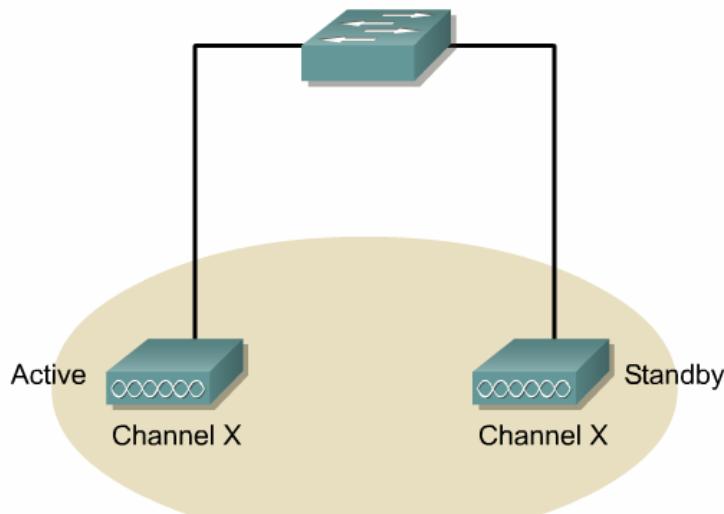


Figura 3

4.2.6 Roaming

Al diseñar WLANs, determine si los clientes requerirán o no roaming sin fisuras, de access point a access point, según se indica en la Figura 1.

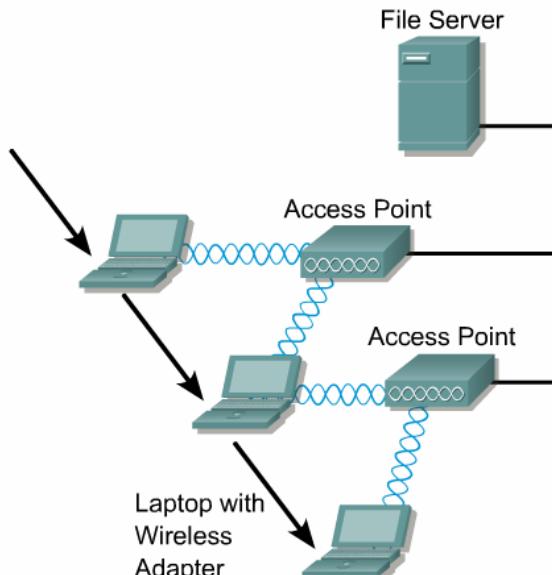


Figura 1

A medida que un cliente hace roaming a través de la red inalámbrica, debe establecer y mantener una asociación con un access point Aironet.

Los siguientes pasos se toman para asegurar un roaming sin fisuras:

- El cliente envía una solicitud de asociación e inmediatamente recibe una respuesta proveniente de todos los puntos de acceso dentro de su área de cobertura.
- El cliente decide a qué access point asociarse basándose en la calidad y en la fuerza de la señal y en la cantidad de usuarios asociados, y en la cantidad de saltos requeridos para llegar al backbone.
- Una vez establecida una asociación, la dirección de Control de Acceso al Medio (MAC) del cliente recae en la tabla del punto de acceso seleccionado. Si el cliente encuentra dificultades, hará roaming para otro access point. Si no se dispone de otro punto de acceso, el cliente bajará su velocidad de transmisión de datos e intentará mantener la conexión.
- Una vez que un cliente hace roaming a otro punto de acceso, su dirección MAC recae en la tabla del nuevo access point, que envía un mensaje broadcast que básicamente enuncia que recibió la "dirección MAC X".
- El access point original envía cualquier dato que tuviera para el cliente al otro punto de acceso, que responde enviándolo al cliente.

Es necesario considerar los siguientes dos factores al diseñar una WLAN con capacidades de roaming sin fisuras que se activa al desplazarse de un punto a otro:

- La cobertura debe ser suficiente para toda la ruta.
- Una dirección IP consistente deberá estar disponible a lo largo de toda la ruta. La subred IP para cada punto de acceso podría encontrarse en diferentes switches y estar separada por dispositivos de Capa 3. De ser así, considere la utilización de tecnologías de commutación de Capa 2 como ATM-LANE, ISL, o 802.1q, para cruzar las VLANs. Esto ayudará a asegurar que exista un único dominio de broadcast para todos los access points. La Figura 2 ilustra un caso semejante.

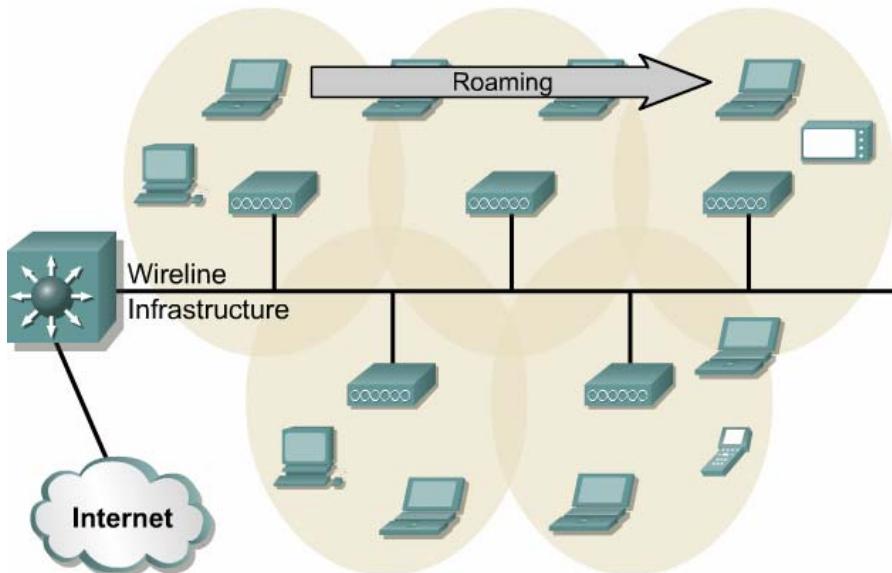


Figura 2

Proceso de asociación

Cuando un cliente pasa a estar online, emitirá como broadcast una Solicitud de Sondeo. Un AP que escucha esto responderá con información acerca del AP como saltos RF al backbone, carga, etcétera. Si más de un AP responde, entonces el cliente decidirá a qué AP asociarse, basándose en la información que devuelve el AP. Los APs emiten 'balizas' a intervalos periódicos. Una baliza contiene detalles similares a la información en la Respuesta de Sondeo. El cliente escucha todos los APs que puede y construye una tabla de información acerca de los APs. El proceso de asociación se ilustra en la Figura 3.

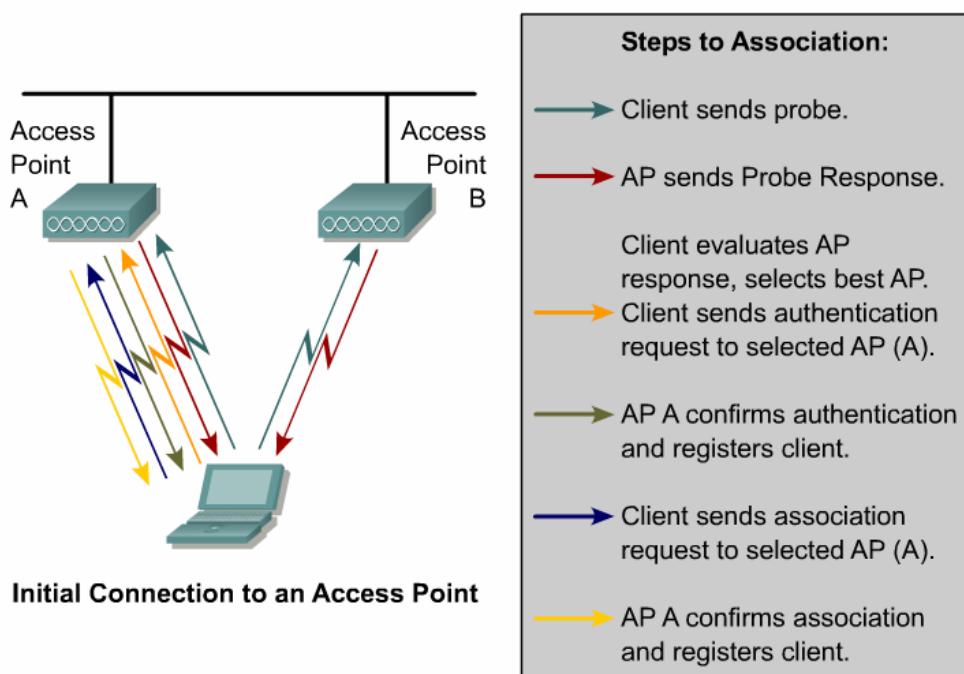


Figura 3

Proceso de reasociación

A medida que el cliente se desplaza fuera del rango de su AP asociado, la fortaleza de la señal comenzará a debilitarse. Al mismo tiempo, la fortaleza de otro AP comenzará a incrementarse. El proceso de reasociación que tiene lugar se muestra en la Figura 4. El mismo tipo de transferencia puede ocurrir, si la carga de un AP se vuelve demasiado grande, mientras el cliente se pueda comunicar con otro AP.

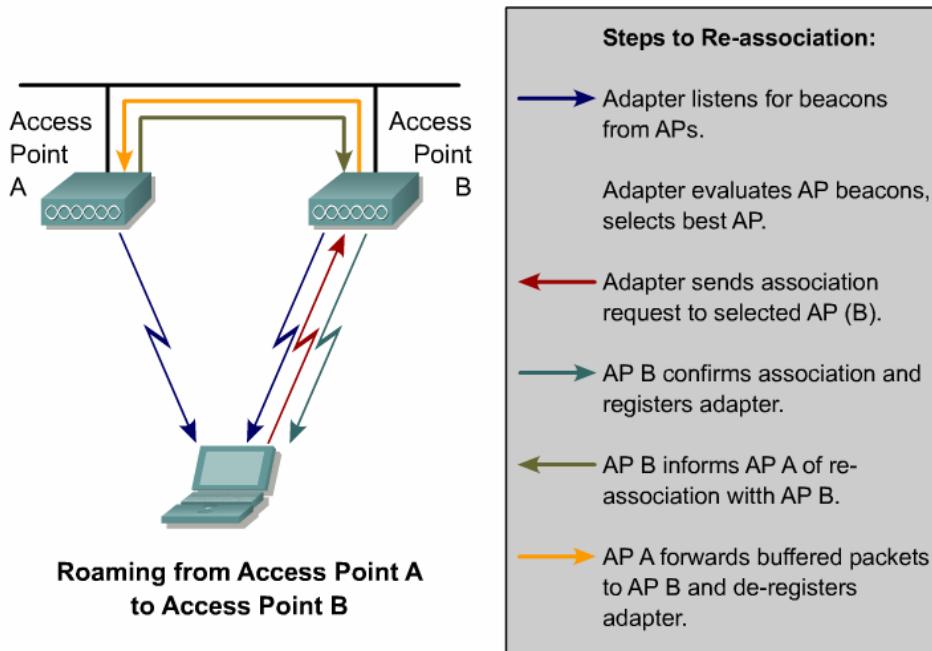


Figura 4

4.2.7 Escalabilidad

La escalabilidad es la capacidad de localizar más de un access point en la misma área. Esto incrementará el ancho de banda disponible de esa área para todos los usuarios locales respecto a ese access point. En el pasado, esta escalabilidad se limitaba sólo a los productos del espectro expandido de salto de frecuencia (FHSS). Los productos DSSS no podían cambiar de canal sin cierta reconfiguración. Los productos Cisco Aironet actuales son ágiles en cuanto a la frecuencia. Esto significa que pueden buscar y utilizar el mejor canal. Existen tres canales de 11 Mbps separados disponibles. Estos canales no están superpuestos en absoluto y no interfieren entre sí. Pueden lograrse hasta 33 Mbps por célula con dispositivos 802.11b. No obstante, los usuarios aún operan únicamente a un valor teórico máximo de 11 Mbps, puesto que sólo pueden conectarse a un AP en un momento determinado. [\[1\]](#)

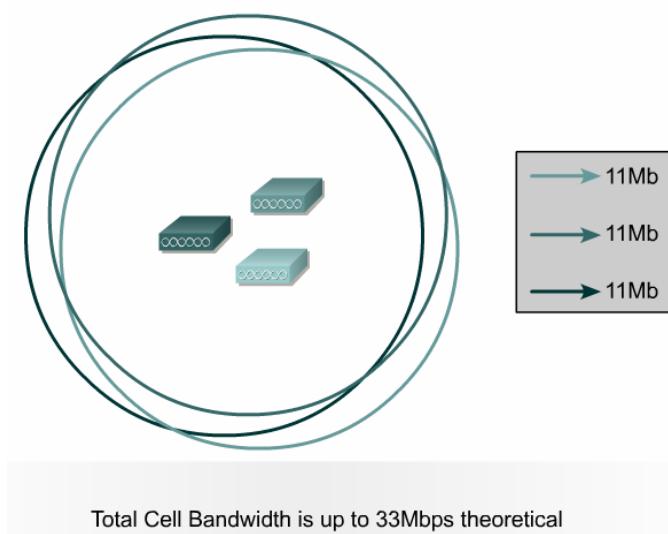


Figura 1

En el caso de 802.11a, existen ocho canales no superpuestos, cada uno con un ancho de banda teórico de 54 Mbps. Esto significa que un máximo de ocho sistemas discretos pueden residir en la misma área, sin interferencia. Por lo tanto, la velocidad de datos total agregada más alta para un sistema 802.11a es en teoría de 432 Mbps, para un área de célula determinada. Recuerde que cualquier usuario conectado sólo

recibirá hasta 54 Mbps. Con más APs, los usuarios tendrán una mayor posibilidad de obtener velocidades de datos más altas. [2](#)

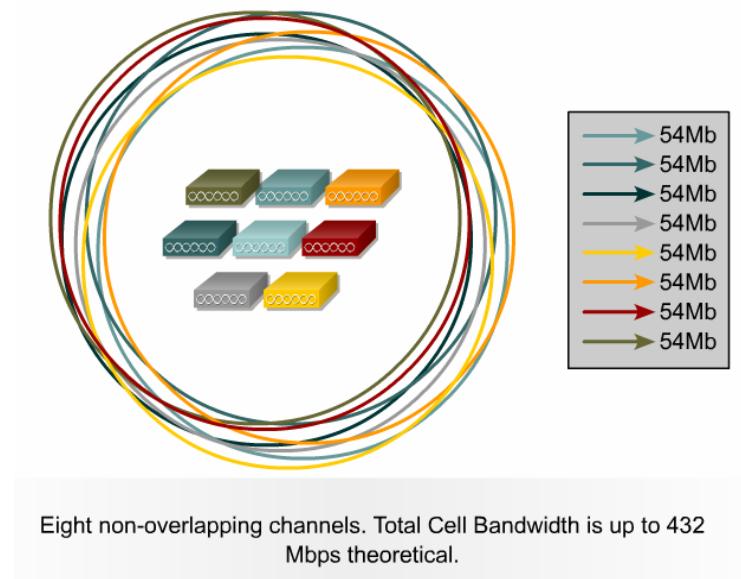


Figura 2

4.3 Configuración del Canal

4.3.1 Descripción general

Existen dos pasos críticos para la buena implementación de una WLAN:

1. Determinar la ubicación de los access points o los bridges — Esto incluye determinar dónde deberán ubicarse, y decidir cuántos se requieren, para la cobertura deseada. Se dejarán muy pocos huecos en la cobertura. Estos huecos son esencialmente aire "muerto" y al cliente le faltará conectividad en estas ubicaciones. Tal como se trató anteriormente, los requisitos de ancho de banda tienen un impacto en las áreas de cobertura.
2. Mapear las asignaciones al canal — Habrá una pequeña superposición, según sea posible, entre canales que utilizan la misma frecuencia.

IEEE 802.11b

En el ejemplo que se muestra en la Figura [1](#), el objetivo era cubrir toda el área de la oficina con una cobertura inalámbrica. En todos lados se proporciona un total de 11 Mbps, debido a la densidad de los usuarios.

54 Cubes - 4 Conference Rooms

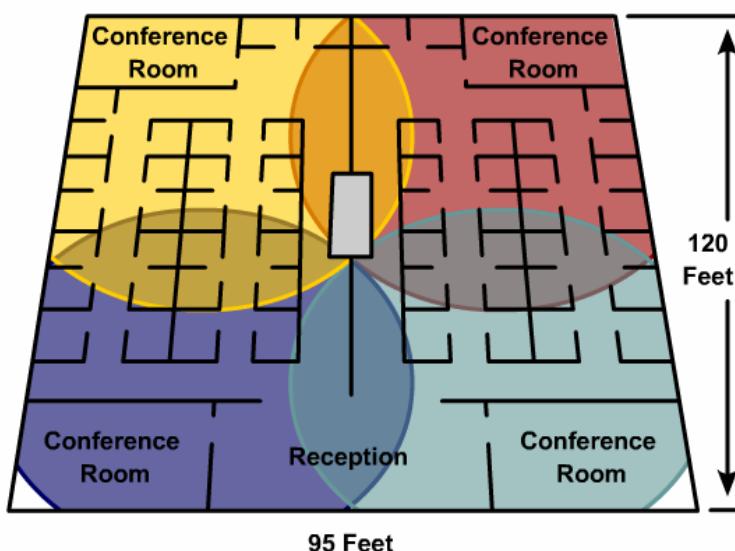


Figura 1

La Figura 2 muestra un diseño que utiliza sólo tres canales 802.11b no superpuestos disponibles en EE.UU. Como puede apreciarse en la Figura 3, los Canales 1, 6, y 11 no tienen frecuencias superpuestas. Este concepto puede correlacionarse con la ubicación de las estaciones de radio FM en todo el país. Nunca habrá dos estaciones de radio, en la misma área geográfica, en el mismo canal o frecuencia exactos.

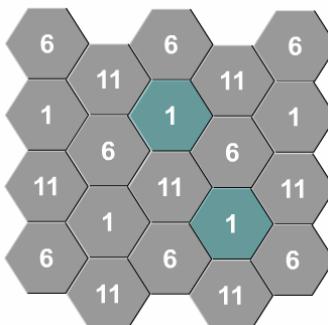


Figura 2

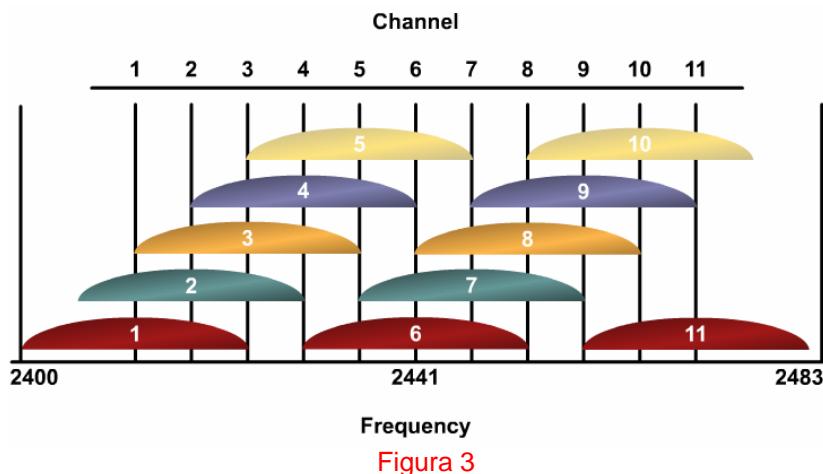


Figura 3

IEEE 802.11a

Utilizando el mismo diagrama que en el ejemplo de 802.11b, la Figura 4 muestra cómo, utilizando productos 802.11a, puede incrementarse el throughput de cualquier usuario individual. Esto se debe al incremento en la velocidad de datos de cada célula. 54 Mbps completos están disponibles en cualquier célula.

54 Cubes - 4 Conference Rooms

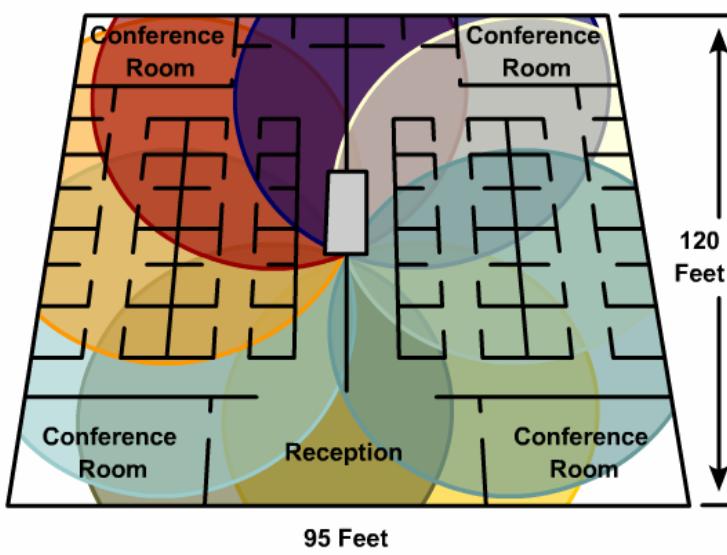


Figura 4

Con los productos 802.11a el usuario tiene ocho canales no superpuestos. Esto significa que puede haber más células, según el área. También significa que será más fácil implementar múltiples APs. Puesto que hay ocho canales con los cuales trabajar, no es tan importante preocuparse respecto a la interferencia co-canal. Esto se muestra en la Figura 5.

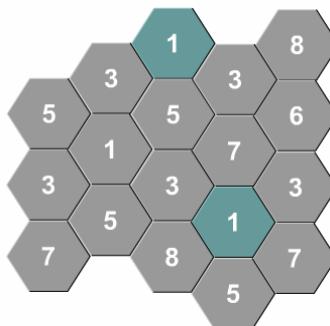


Figura 5

El proceso para lograr una óptima ubicación y mapeo de canales se trata en módulos posteriores. Estos módulos posteriores también tratarán el estudio y el diseño del sitio en más detalle.

4.3.2 Cobertura y comparación de access points

La Figura 1 ilustra que, a medida que un cliente hace roaming alejándose del access point, las señales de transmisión entre ambos se atenúan (debilitan). En lugar de disminuir la confiabilidad, el AP se desplaza a una velocidad de datos más lenta, lo cual proporciona una transferencia de datos más precisa. Esto se denomina velocidad de datos o desplazamiento multi-velocidad. A medida que un cliente se aleja de un access point 802.11b, la velocidad de datos pasará de los 11 Mbps, a los 5,5 Mbps, a los 2 Mbps, y, finalmente, a 1 Mbps. Esto ocurre sin perder la conexión, y sin ninguna interacción de parte del usuario. Lo mismo ocurre con 802.11a. No obstante, como lo muestra la Figura 2, las velocidades de datos bajan de 54 Mbps. La Figura 2 también muestra las distancias aproximadas desde el AP, para cada velocidad de datos.

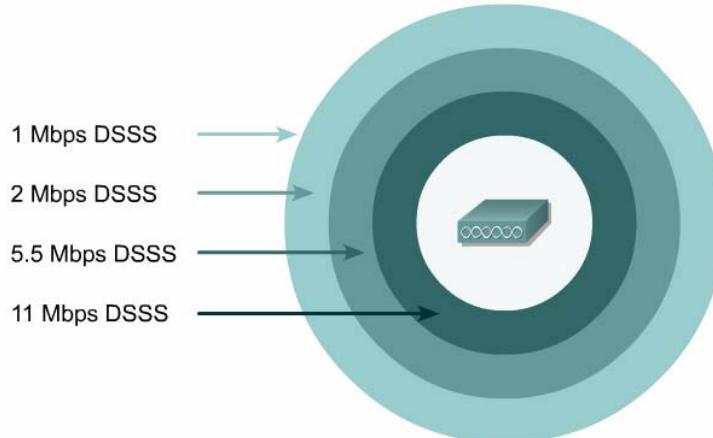
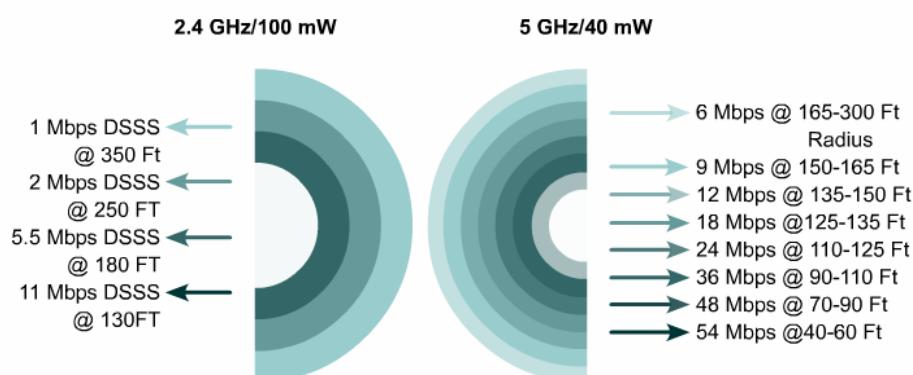


Figura 1



Omni 2.2 dBi 2.4 GHz and Omni 5 dBi 5 GHz AP antennas
 Omni 0 dBi 2.4 GHz client and Patch 5 dBi 5 GHz client
 Distances vary greatly because of building layouts

Figura 2

La radio de 2,4 GHz Cisco Aironet proporciona 100 mW de salida y ofrece un alto grado de sensibilidad de parte del receptor. La radio cliente de 5 GHz tiene una potencia de transmisión de 20 mW y el access point de 5 GHz tiene una potencia de transmisión de 40 mW. Es posible ajustar hacia abajo el nivel de potencia, para crear células pico, o células de cobertura más pequeña. Esto se llevará a cabo, por ejemplo, para evitar que el área de cobertura de un AP se extienda demasiado lejos hacia el área de cobertura de otro AP.

4.3.3 Implementación multivelocidad

Los requisitos de ancho de banda son un factor en los mapeos de cobertura, puesto que la distancia desde un access point tiene efecto sobre el ancho de banda disponible. El ejemplo de la Figura 1 proporciona un roaming sin fisuras, pero no a velocidad constante. En este ejemplo se aprovecha la tecnología multivelocidad, para bajar el ancho de banda y obtener mayores distancias de cobertura, con un único access point.

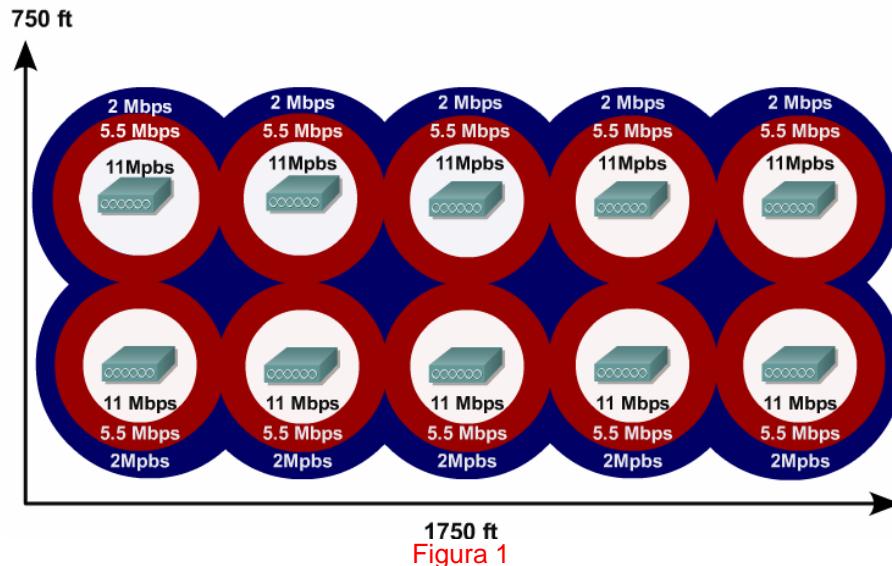


Figura 1

Si se requieren 11 Mbps en todas partes, sería necesario readjudicar los access points de modo tal que sólo los círculos de 11 Mbps se toquen entre sí, con alguna superposición. Esto requeriría una mayor cantidad de APs, pero se lograría un ancho de banda consistente. 2

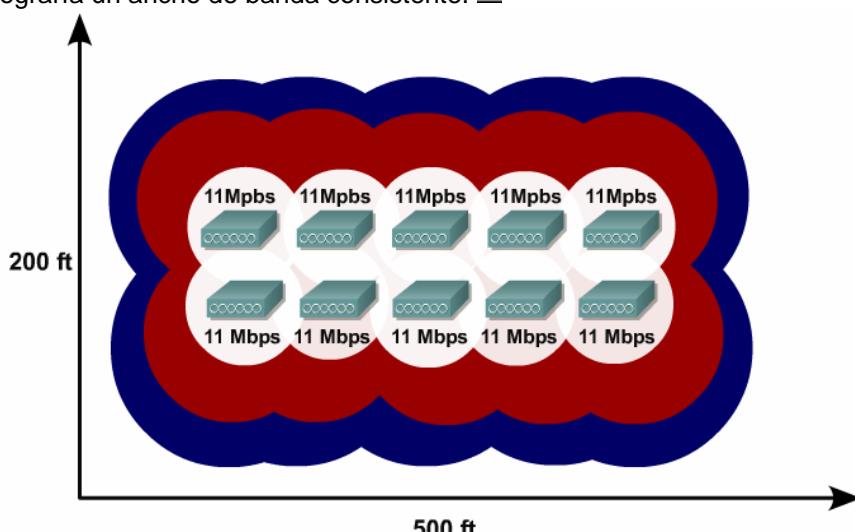
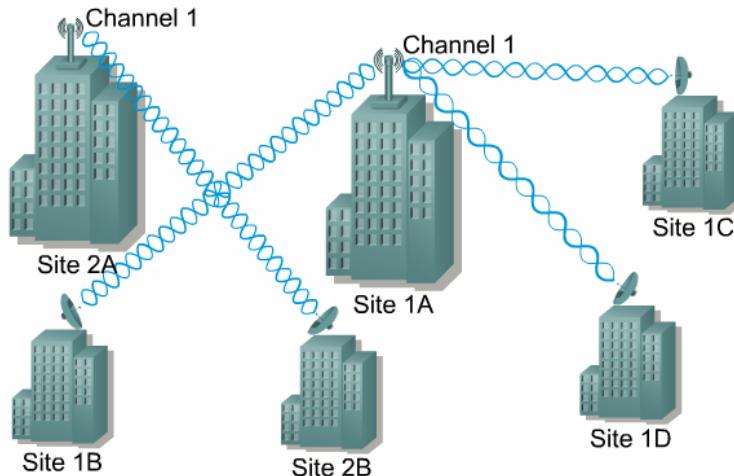


Figura 2

4.3.4 Uso e interferencia del canal

En áreas metropolitanas, es posible recibir una interferencia de parte de terceros, otras compañías que utilizan dispositivos inalámbricos. Esto se muestra en la Figura 1. En esta situación, es importante asegurarse de que se utilicen diferentes canales. No obstante, esta situación no será conocida hasta que el usuario realmente no implemente el enlace inalámbrico. Cambiar de canal es la mejor forma de evitar la

interferencia. Recuerde que el estándar 802.11 utiliza el espectro sin licencia y, por lo tanto, cualquiera puede utilizar estas frecuencias.



Third-party interference from same channel usage

- Potential problem in congested areas

Figura 1

4.4 Topologías de Bridge

4.4.1 Modos raíz

Los access points y bridges Cisco Aironet tienen dos modos raíz diferentes, en los cuales se opera lo siguiente:

1. Root = ON — El bridge o AP es raíz. Si se trata de un bridge, se denomina bridge master.
2. Root = OFF — El bridge o AP no es raíz.

Esta configuración controla cuándo se permitirán las asociaciones y la comunicación entre diferentes dispositivos de infraestructura. El significado de estas configuraciones para bridges inalámbricos y access points se muestra en las Figuras 1 y 2.

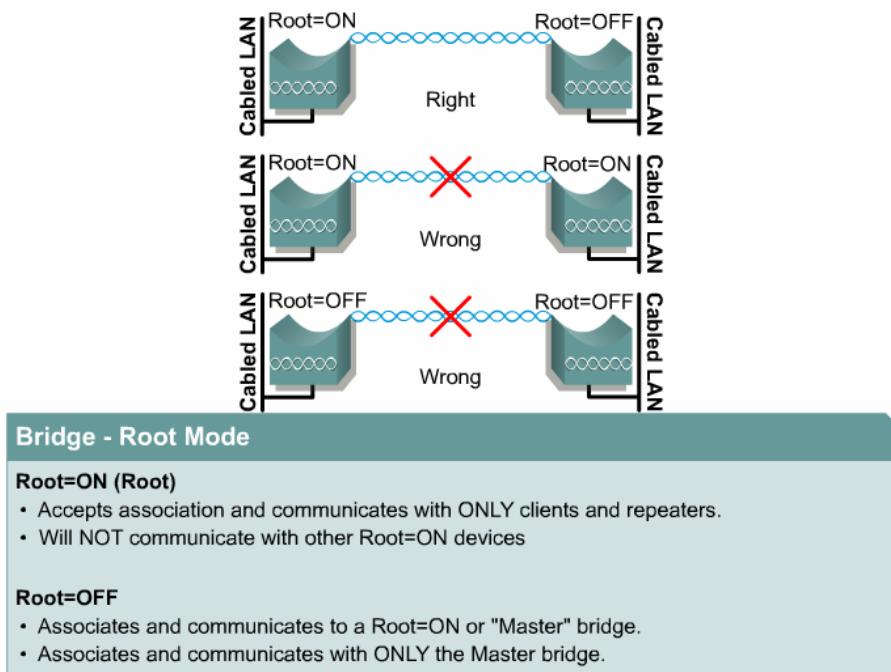


Figura 1

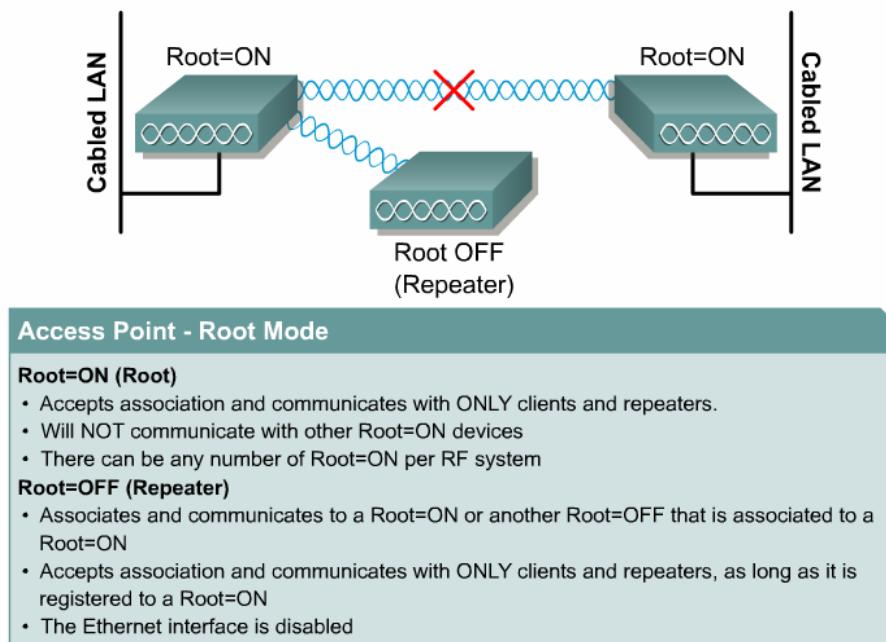


Figura 2

4.4.2 Configuración punto a punto

Al utilizar bridges inalámbricos punto a punto, dos LANs pueden ubicarse hasta a 40 km (25 millas) de distancia, como se muestra en la Figura 1. No obstante, las antenas deben encontrarse en línea de visión entre sí. Obstáculos tales como edificios, árboles y montañas ocasionarán problemas de comunicación. La actividad demostrará la necesidad de la línea de visión entre bridges.

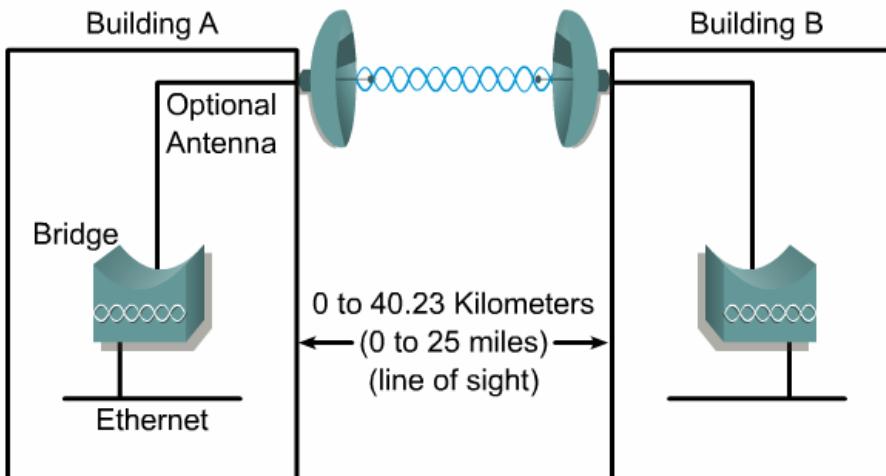


Figura 1

En esta configuración, los segmentos Ethernet de ambos edificios actúan como si fueran un único segmento. El bridge no se suma al conteo de repetidores Ethernet porque este segmento es considerado como un cable por la red.

Configure un bridge como Root = ON y el otro como Root = OFF, para permitir que los bridges se conecten entre sí.

A muchas corporaciones les agradaría tener más ancho de banda entre dos ubicaciones que los 11 Mbps proporcionados por el estándar 802.11b. Actualmente, con el Cisco IOS, es posible utilizar Fast Etherchannel o trunking multienlace para unir o crear una agregación de hasta tres bridges. Esto proporciona al cliente el potencial para 33 Mbps. Esto se ilustra en la Figura 2.

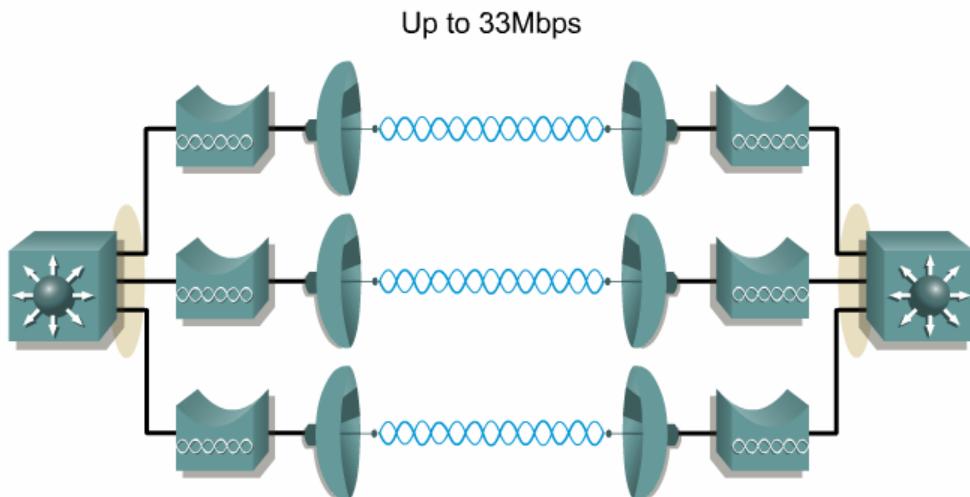


Figura 2

4.4.3 Configuración de punto a multipunto

Para el bridging multipunto, se utiliza en general una antena omnidireccional en el sitio principal. Las antenas direccionales se utilizan en los sitios remotos. Esta distinción se muestra en la Figura 1. Mediante estas antenas los sitios remotos pueden comunicarse entonces con el sitio principal. En esta configuración, nuevamente, todas las LANs aparecen como un único segmento. El tráfico desde un sitio remoto a otro se enviará al sitio principal y luego al otro sitio remoto. Los sitios remotos no pueden comunicarse directamente entre sí.

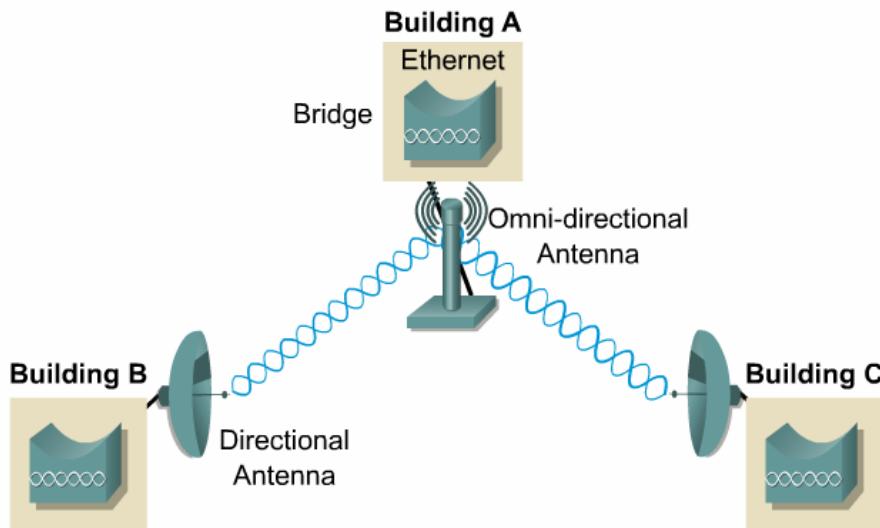


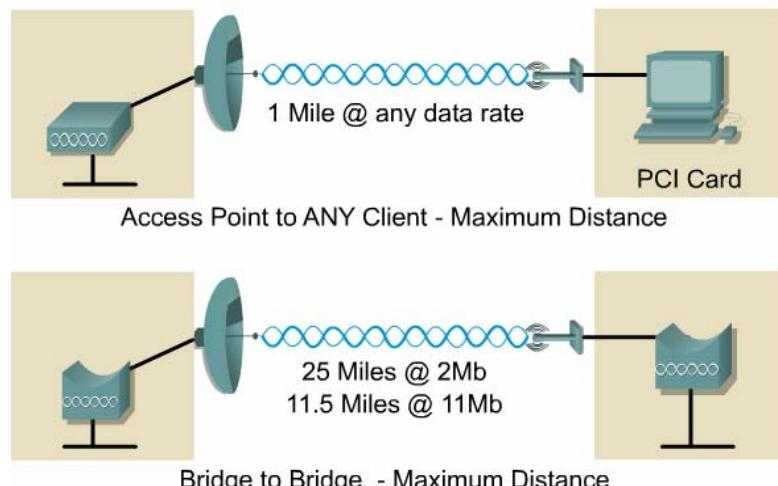
Figura 1

Debe mantenerse la línea de visión entre cada sitio remoto y el sitio principal.

Configure el bridge principal a Root = ON y todos los otros bridges a Root = OFF, para permitir que los bridges se conecten entre sí.

4.4.4 Limitaciones de distancia

Si la distancia a través de la cual se utiliza el bridging es menor que 1,6 km (1 milla), en ocasiones puede utilizarse el Bridge de Grupo de Trabajo y AP Cisco Aironet 350, para ahorrar dinero. No obstante, si la distancia es mayor que 1,6 km (1 milla), se recomienda la utilización de un producto bridge, por razones de confiabilidad. Utilizar un AP a más de una milla no proporcionará comunicaciones confiables, a causa de las restricciones de temporización. El estándar 802.11 establece un límite de tiempo para la confirmación de los paquetes. Recuerde que 802.11 también define una Red de Área Local, lo cual implica un alcance inalámbrico típico de hasta 305 m (1000 pies), no de varios kilómetros o millas.



Los productos bridge tienen un parámetro que incrementa esta temporización, mientras que el bridge de grupo de trabajo y AP no. La temporización se incrementa, violando el estándar 802.11. Esto permite a los dispositivos Cisco operar a mayores distancias. Cualquier bridge inalámbrico que soporte distancias de más de una milla deben violar 802.11. Esto significa que radios de otros fabricantes de 802.11 pueden no funcionar con los bridges Cisco cuando las distancias son mayores que 1,6 km (1 milla).

4.4.5 Ancho de banda

Mucha gente piensa que los productos de 11 Mbps soportarán muchas radios de 2 Mbps. También se considera que proporcionarán una velocidad de datos total, o sumanda, de 11 Mbps, y que cada unidad remota obtendrá 2 Mbps completos. El problema es que las unidades de 2 Mbps transmiten a 2 Mbps. Esto requerirá cinco veces más tiempo para transmitir la misma cantidad de datos, que lo que haría un producto de 11 Mbps. Esto significa que la velocidad de datos es de sólo 2 Mbps, para cualquier sitio remoto determinado. El total que la unidad de 11 Mbps verá es de sólo 2 Mbps, como lo muestra la Figura 1.

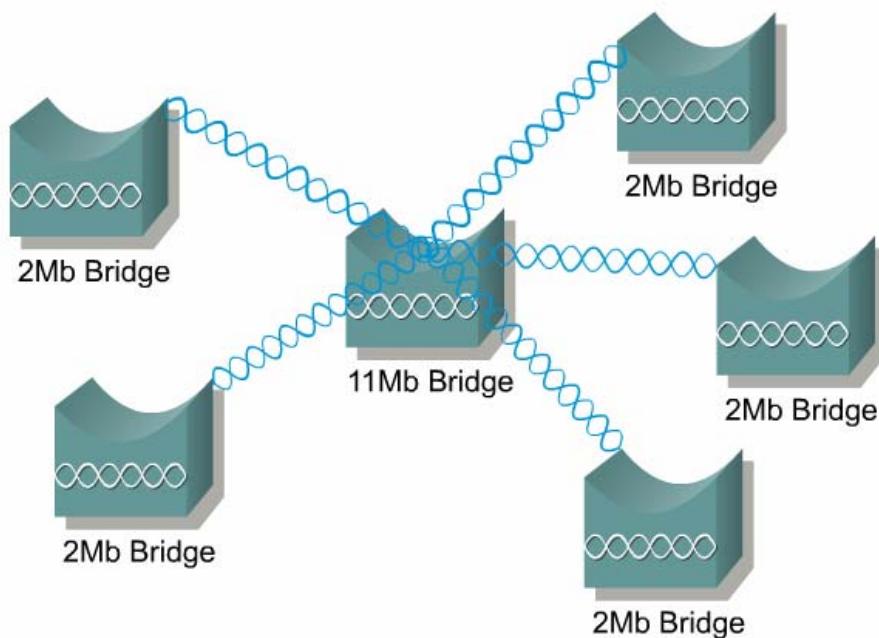


Figura 1

Para lograr una velocidad de datos sumanda de 11 Mbps, todas las unidades remotas deberán utilizar una velocidad de 11 Mbps. Si una única unidad es menor que 11 Mbps, todas las unidades remotas tienen que estar utilizando una velocidad de 11 Mbps. Si una única unidad es menor que 11 Mbps, la velocidad total será bastante menor que los 11 Mbps. La unidad base o central tiene que servir también a los sitios remotos más lentos.

Si todos los dispositivos están operando a la misma velocidad de datos, a todos les llevará la misma cantidad de tiempo enviar paquetes del mismo tamaño. Si algunos dispositivos están operando a velocidades más altas, transmitirán el paquete más rápido. Esto permitirá que la RF esté disponible más rápidamente, para el siguiente dispositivo que está esperando para enviar datos.

Nótese, en la Figura 2, las diferencias entre los valores para la velocidad de datos y aquéllos para throughput. Por ejemplo, una velocidad de datos de 1,6 Mbps sólo puede entregar 500 Kbps de throughput. Esto representaría sólo una eficiencia del 31 por ciento. Esta diferencia se debe a que la velocidad de datos del término no toma ninguna sobrecarga en cuenta. La sobrecarga incluye los encabezados y trailers del protocolo, las confirmaciones, las retransmisiones y más. En el caso de las WLANs, el intercambio RTS/CTS también puede agregarse a esta sobrecarga.

Algunos fabricantes de 802.11b afirman ofrecer 1 Mbps completo, pero la cobertura puede verse limitada a alrededor de 9 m (30 pies). A la distancia máxima alcanzada, algunos de estos sistemas sólo pueden ver alrededor de 300 Kbps de throughput.

Según se muestra en la Figura 2, los alcances del equipamiento Cisco Aironet se encuentran en la distancia máxima, a menos que se lo enuncie específicamente de otra forma.

Questions	Aironet 350 Series	Aironet 1100 Series ¹	Aironet 1200 Series ^{1,2}
Maximum data rate?	11 Mbps	11 Mbps	11 Mbps, 54 Mbps
Typical throughput?	5.5 Mbps	5.5 Mbps	5.5 Mbps, 32 Mbps
Distance for max - outdoors	244 m (800 ft)	244 m (800 ft)	244 m (800 ft) 30.5-36.5 m (100 to 120 ft)
Distance for max - indoors	46 m (150 ft)	46 m (150 ft)	40 m (130 ft) 18 to 21 m (60 to 70 ft)
Maximum clients per AP	2007	2007	
Typical clients per AP	Same as 10BaseT	Same as 10BaseT	Same as 10 BaseT - 11b Same as 100 BaseT - 11a
Maximum co-located APs	3	3, 8	

1 = Although the focus is on bridging, the numbers for the Cisco Aironet 1100 and 1200 APS are also included.
2 = The first number in each box applies to 802.11b. The second number applies to 802.11a.

Figura 2

Aunque los APs Cisco Aironet permitirán 2007 asociaciones, con cada AP del sistema, el factor limitante es la necesidad de ancho de banda de las aplicaciones. Los APs Cisco Aironet 802.11b actúan como hubs Ethernet de 10 Mbps. Si el sistema se utiliza para aplicaciones con un uso mínimo del ancho de banda, como el e-mail, entonces pueden soportarse fácilmente 50 usuarios por AP. Para las aplicaciones de elevada velocidad de datos, pueden soportarse menos usuarios.

Aunque esta sección se ha concentrado en 802.11b y su velocidad de datos máxima de 11 Mbps, los conceptos también se aplican a las velocidades de datos más elevadas de 802.11a. La velocidad de datos máxima sumada sólo puede lograrse en una célula, si todas las unidades remotas están operando a la velocidad más alta. La cantidad de usuarios que pueden ser soportados por un solo AP depende del ancho de banda que la aplicación necesite.

4.5 Topologías de Muestra

4.5.1 Topologías básicas

Existen varias configuraciones físicas básicas que pueden utilizarse en una implementación de WLAN. Esta sección tratará las siguientes topologías principales de WLAN:

- Topología Peer-to-Peer (Ad Hoc) (IBSS) — Como lo muestra la Figura 1, un conjunto de servicios inalámbricos puede consistir tan sólo en dos o más PCs, cada una con una placa de red inalámbrica. Esta configuración, que no incluye un AP, se denomina BSS Independiente (IBSS). Sistemas operativos tales como Windows 98 o Windows XP han hecho que este tipo de red peer-to-peer sea muy fácil de configurar. Esta topología puede utilizarse para una oficina pequeña u oficina en el hogar, para permitir la conexión de una laptop a la PC principal, o para varios individuos, simplemente para compartir archivos. No obstante, las limitaciones de cobertura son una desventaja en este tipo de red, ya que todo el mundo debe poder escuchar a todo el resto.

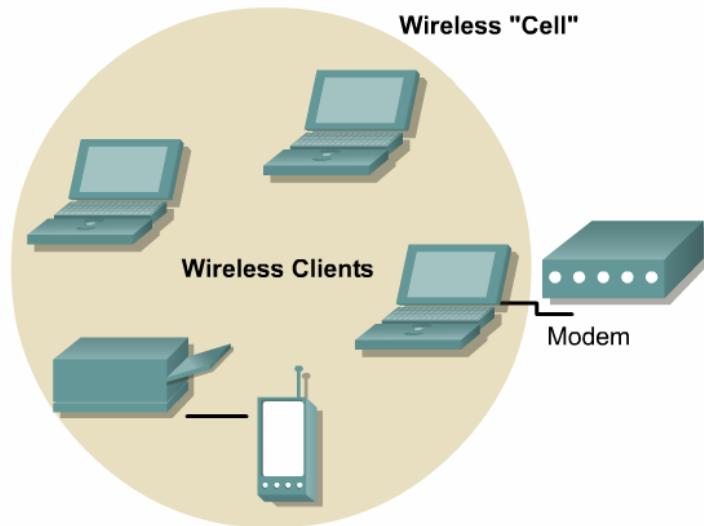


Figura 1

- Topología de Infraestructura Básica (BSS) — El conjunto de servicios básicos (BSS) es el bloque constructor de una LAN 802.11. La Figura 2 muestra una BSS con tres estaciones que son miembros de la BSS, además del AP. La BSS abarca una única célula, tal como lo indica el círculo. Cuando un dispositivo se desplaza fuera de su BSS, ya no puede comunicarse con otros miembros de la BSS. Una BSS utiliza el modo de infraestructura, un modo que necesita un access point (AP). Todas las estaciones se comunican a través del AP. Las estaciones no se comunican directamente. Una BSS tiene una ID de conjunto de servicios (SSID).

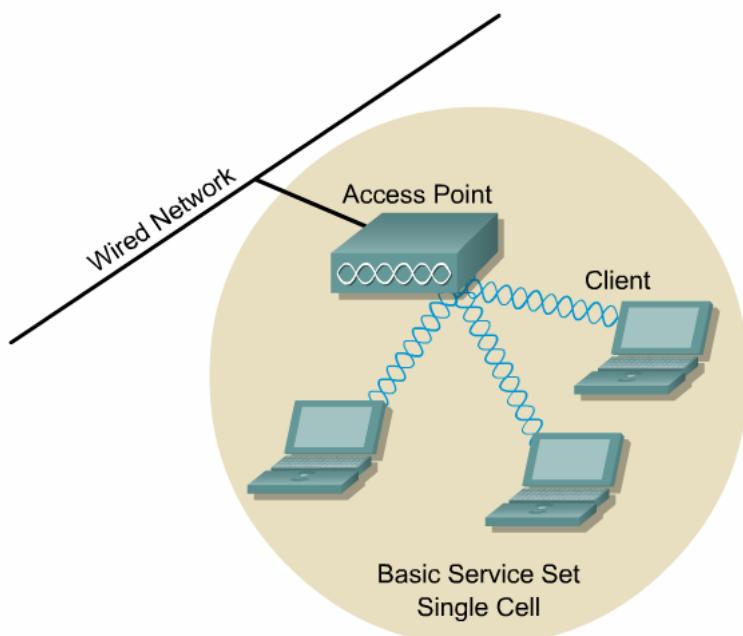
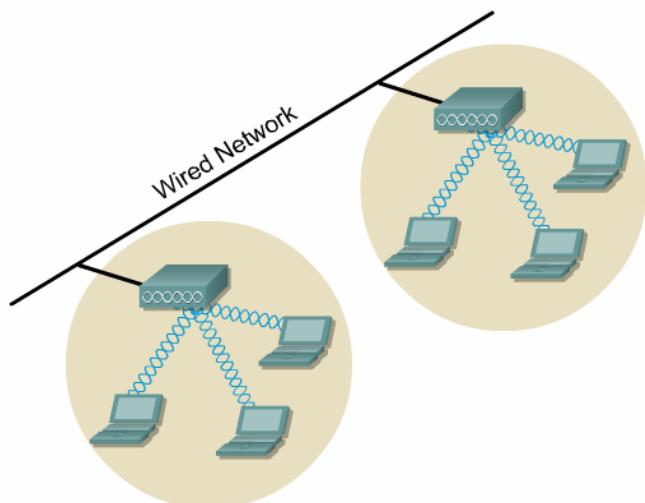


Figura 2

- Topología de Infraestructura Extendida (ESS) — Un conjunto de servicios extendido (ESS) se define como dos o más BSSs que están conectados por medio de un sistema de distribución común, como lo ilustra la Figura 3. Esto permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios. Al igual que sucede con BSS, todos los paquetes de un ESS deben atravesar uno de los APs.



Coverage may overlap to provide roaming capabilities.

Figura 3

- Conexión Telefónica de Estación Base — La estación base está diseñada para el mercado de oficina pequeña/oficina en el hogar (SOHO). Le brinda a los telecommutadores, SOHOs y usuarios hogareños la conveniencia de una conectividad inalámbrica, como lo muestra la Figura 4. La conectividad telefónica permite a los dispositivos tanto cableados como inalámbricos acceder al módem y a la Internet. La estación base también funcionará como servidor DHCP, para hasta 100 clientes cableados o inalámbricos.

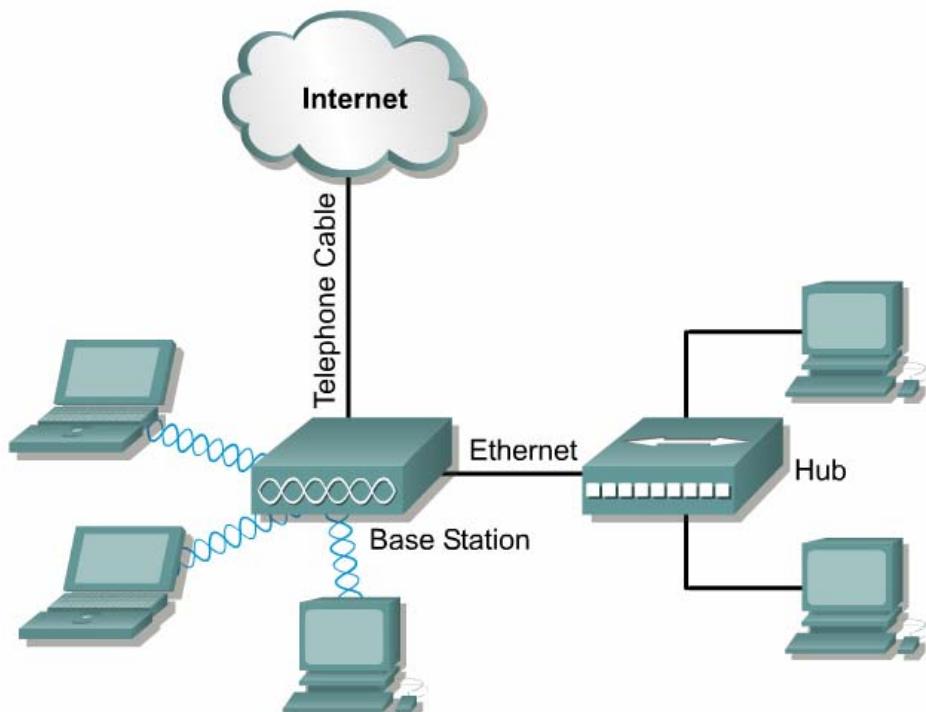


Figura 4

- DSL de Estación Base — La estación base ofrece soporte para un Cable Módem o módem DSL, como lo muestra la Figura 5. En este modo, la estación base sólo soportará clientes inalámbricos. Aunque se soporta la funcionalidad DHCP, no se proporciona el acceso a la red cableada, porque el puerto Ethernet debe utilizarse para conectarse al Cable Módem/módem DSL. En esta configuración, la estación base también tiene soporte para PPP sobre Ethernet, porque algunos ISPs lo requieren.

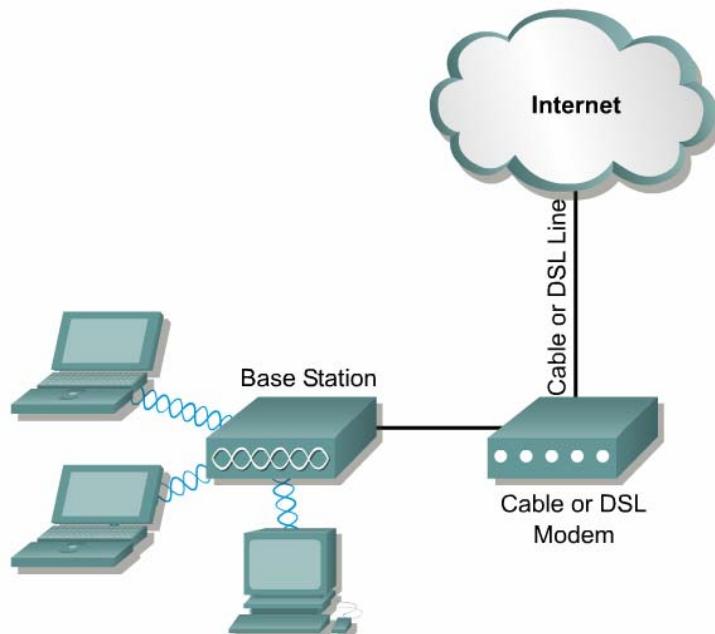


Figura 5

4.5.2 Topologías de campus

El propósito de una WLAN de campus es servir como sistema de acceso que incorpore una movilidad completa. Las WLANs permiten a los usuarios acceder a la información desde lugares no cableados en el exterior, en comedores o espacios informales para el estudio, los bancos del aula e incluso campos de atletismo. No obstante, las WLANs de campus no deberán considerarse como reemplazo de un entorno inalámbrico, sino más bien como forma de agregar más funcionalidad a la red existente.

Una superposición inalámbrica de todo el campus proporciona networking en ubicaciones difíciles de alcanzar o temporales. Éstos son lugares que podrían haber sido ignorados completamente. Los access points Cisco Aironet 1100 y 1200 y los bridges Aironet 350 se integran bien con los switches Cisco Ethernet, que se utilizan en general en un entorno de campus. Muchos de los elementos de tal implementación de todo el campus se ilustran en la Figura 1. Varios switches, incluyendo el Catalyst series 3500 y 6500, proporcionan energía de entrada de línea. Esto elimina la necesidad de fuentes de alimentación adicionales para los APs conectados.

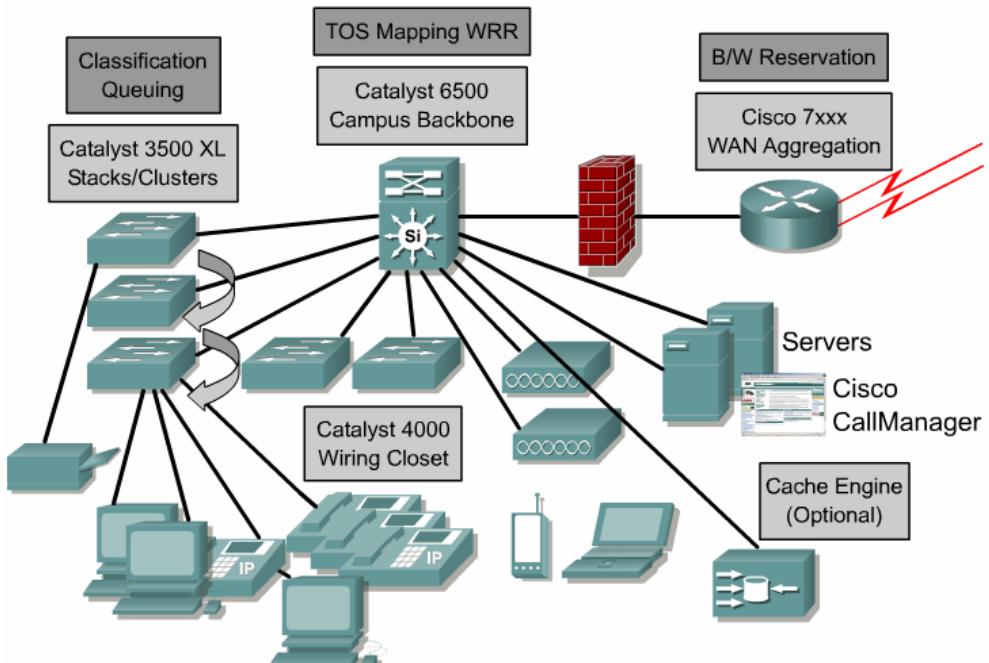


Figura 1

Uno de los mayores beneficios de una WLAN de campus es su capacidad para que la gente se siente en áreas comunes y trabaje en conjunto, a la vez que obtiene fácilmente un acceso a la red. En el caso de muchas instituciones educativas, donde los recursos son limitados, esto podría significar que existen menos usuarios que compiten por un puñado de computadoras integradas. La tecnología inalámbrica se está convirtiendo rápidamente en una herramienta viable e importante, en una variedad de entornos de negocios y educativos.

4.5.3 Adición de las WLANs a AVVID

Las WLANs son parte de la Arquitectura Integrada de Cisco para Voz, Video y Datos (AVVID). Una descripción general de AVVID se muestra en la Figura 1. Como arquitectura principal de red empresarial, basada en estándares e integrada de la industria, AVVID proporciona el mapa de rutas para combinar las estrategias de negocios y tecnología en un único modelo cohesivo.

La infraestructura de red inteligente de AVVID incluye una variedad de clientes, plataformas de red y servicios de red, como lo muestra la Figura 2. Otro componente importante es el control de servicios, que permite a las tecnologías ayudar a proporcionar las soluciones. La Figura 3 enumera los controles de servicios optimizados por Cisco.

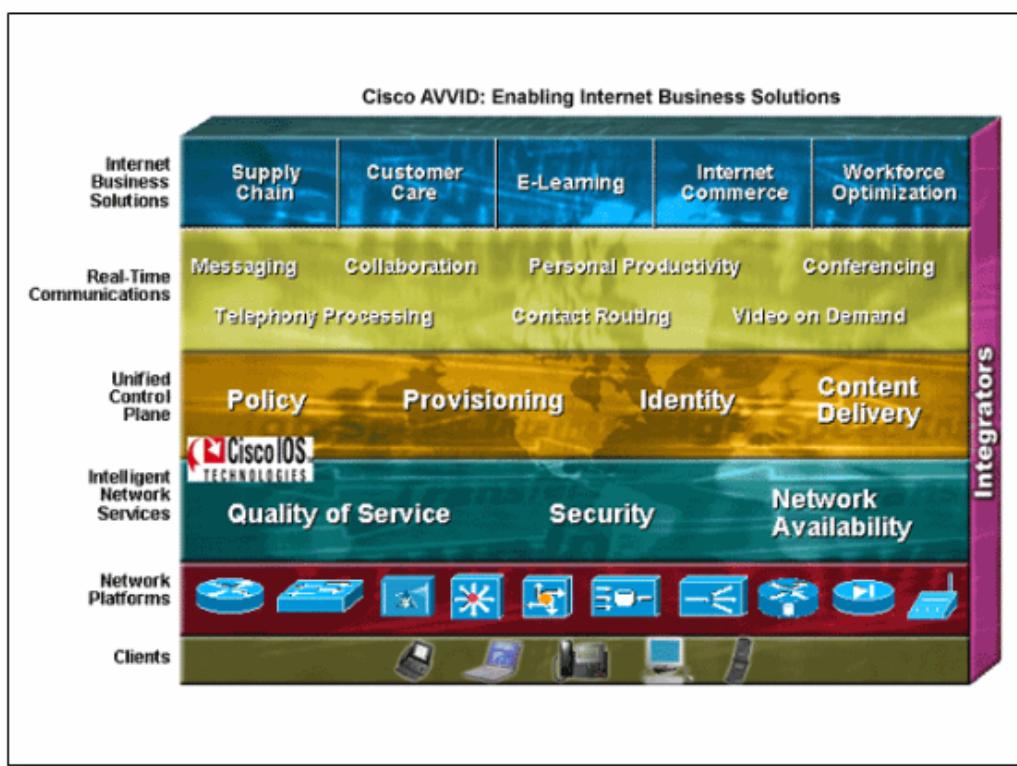


Figura 1

Cisco AVVID Intelligent Network Infrastructure

Clients

- Network clients include Cisco IP Phones and wire and wireless devices, including PCs and Laptops. These standards-based devices can be interconnected, and functionality can be added through intelligent network services.

Network Platforms

- The network platforms are comprised of routers, gateways, switches, servers, firewalls, and other devices. This layer of the architecture provides the basis for a complete networking solution.

Intelligent Network Services

- These are the platforms, network services, appliances, and management systems that allow business rules and policies to be reflected in network performance.

Figura 2

AVVID Service Control

Service control helps the Internet technologies work with the Internet business solutions. Service control software performs network fine-tuning and optimization. Functions include the following:

- VPN/Security Control
- Perimeter Control
- Call Control
- QoS/Policy Control
- Video Media Control
- Content Distribution Control
- Wireless Access Control
- Directory Control

Figura 3

Combinando la infraestructura y los servicios de red con aplicaciones actuales y emergentes, AVVID acelera la integración de la estrategia tecnológica para la visión de los negocios. Cisco AVVID permite soluciones de negocios de Internet para clientes a través de la infraestructura de red y asociaciones clave con desarrolladores e integradores.

Una arquitectura de red es un mapa de rutas y una guía para una planificación, diseño e implementación continua de la red. Proporciona un marco que unifica soluciones dispares en una única base. Cisco AVVID proporciona lo siguiente:

- Velocidad — La velocidad en la implementación de aplicaciones se ve facilitada por productos totalmente integrados y probados. La velocidad, en términos de ancho de banda, está disponible en incrementos escalables, desde velocidades de transmisión modestas hasta de 1 Gigabit.
- Confiabilidad — El tiempo de actividad de la red se incrementa por medio de hardware y software completamente integrado y probado, así como por medio de funciones tolerantes a los fallos.
- Interoperabilidad — Las APIs basadas en estándares permiten una integración abierta con desarrollos de terceros, proporcionando a los clientes opciones y flexibilidad. La prueba de interoperabilidad garantiza que múltiples soluciones funcionen juntas.
- Ritmo del cambio — Los clientes tienen la capacidad para adaptarse rápidamente, en entornos de negocios competitivo y cambiante. Esto se debe a que las nuevas tecnologías están continuamente integrándose a la solución AVVID de extremo a extremo.
- Reducción de costos — Los requisitos de recursos y tiempo se minimizan, lo cual ayuda a reducir los costos de implementación.
- Movilidad — El recableado y la reconfiguración se ven minimizados. Los usuarios siempre están conectados y pueden hacer roaming libremente, incrementando así sus niveles de productividad.

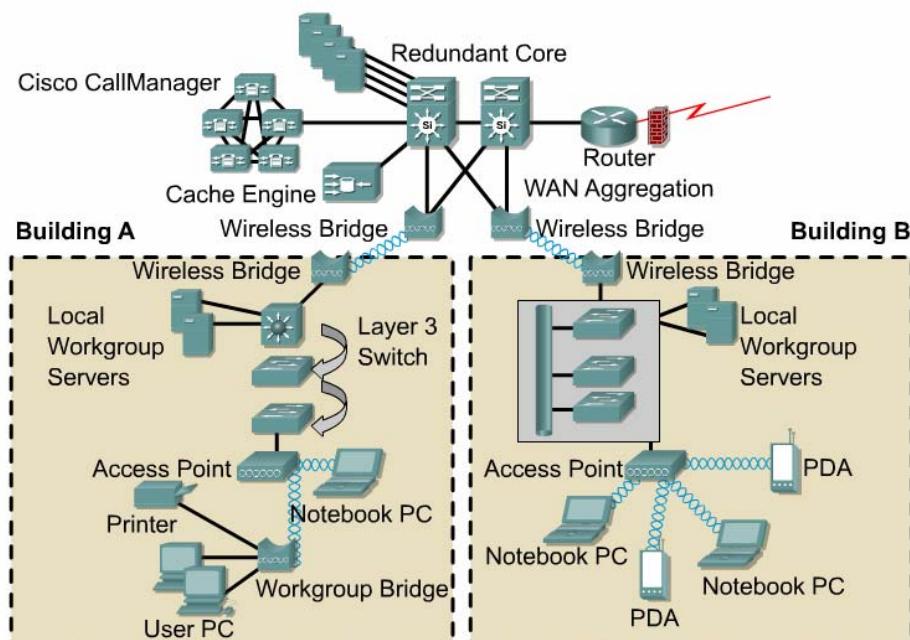


Figura 4

Una vez que una arquitectura de red se ha desarrollado, una organización tendrá un marco en su lugar. El marco permitirá una toma de decisiones más informada, incluyendo inversiones especialmente apropiadas en tecnologías, productos y servicios de red. Una topología AVVID de muestra, incluyendo el acceso a la WLAN, se muestra en la Figura 4.

4.6 VLAN, QoS, e IP Móvil Proxy

4.6.1 Características de una VLAN

Las redes LAN se dividen cada vez más en grupos de trabajo conectados a través de backbones comunes para formar topologías de LAN virtuales (VLAN). Las VLANs permiten una eficiente separación del tráfico, proporcionan una mejor utilización del ancho de banda y alivian los problemas de escalamiento segmentando lógicamente la infraestructura de la red de área local (LAN) física en diferentes subredes para que los paquetes se comunten únicamente entre puertos dentro de la misma VLAN. Cuando se las combina con un soporte de administración de configuración central, las VLANs facilitan las adiciones de grupos de trabajo y las adiciones y cambios de cliente/servidor. Algunas razones comunes por las cuales una compañía podría tener VLANs son:

- Seguridad — Los sistemas separados que tienen datos sensibles provenientes del resto de la red disminuyen las posibilidades de que la gente obtenga acceso a la información que no están autorizados para ver.
- Tipos de trabajo por departamento/específicos — Las compañías pueden desear que las VLANs configuren departamentos que tienen usuarios de red intensivos (como multimedia o ingeniería), o una VLAN a través de departamentos que esté dedicada a tipos específicos de empleados (como administradores o personal de ventas).
- Flujo de broadcasts/tráfico — Puesto que el elemento principal de una VLAN es el hecho de que no pasa tráfico de broadcast a nodos que no son parte de la VLAN, reduce automáticamente los broadcasts. Las listas de acceso (ACL) proporcionan al administrador de red una forma de controlar quién ve qué tráfico de la red.

Los Access Points Cisco Aironet sólo soportan el estándar del protocolo Trunking 802.1Q. Los Switches y Routers Cisco pueden soportar el protocolo pre-estándar Enlace Inter-Switch (ISL) y 802.1Q, o ambos, dependiendo del modelo y la imagen del IOS. Los switches no permitirán que diferentes VLANs hablen entre sí. Será necesario un Router para permitir que diferentes VLANs se comuniquen entre sí. Los Access Points Cisco Aironet pueden configurarse con 16 VLANs diferentes para una flexibilidad en el diseño del sistema.

Las WLANs ahora pueden encajar bien en la red mayor porque las VLANs han sido habilitadas en los Access Points. Esto permite a los usuarios de la WLAN hacer roaming de access point a access point manteniendo la conectividad con la VLAN apropiada. Las Figuras 1- 5 muestran una topología de muestra que utiliza las funciones de la VLAN.

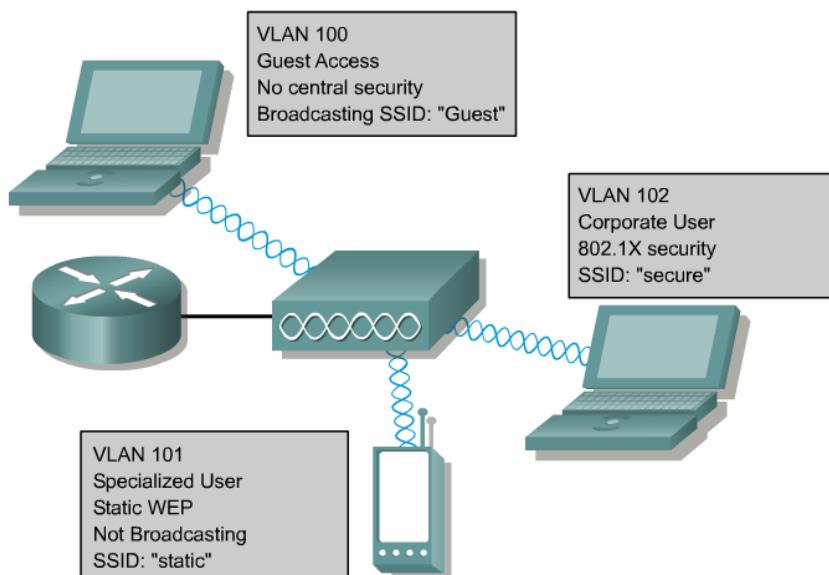
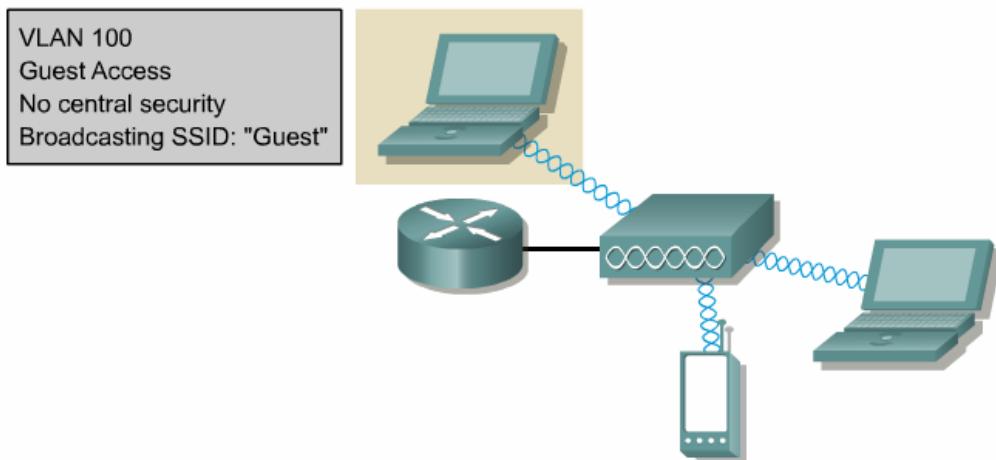
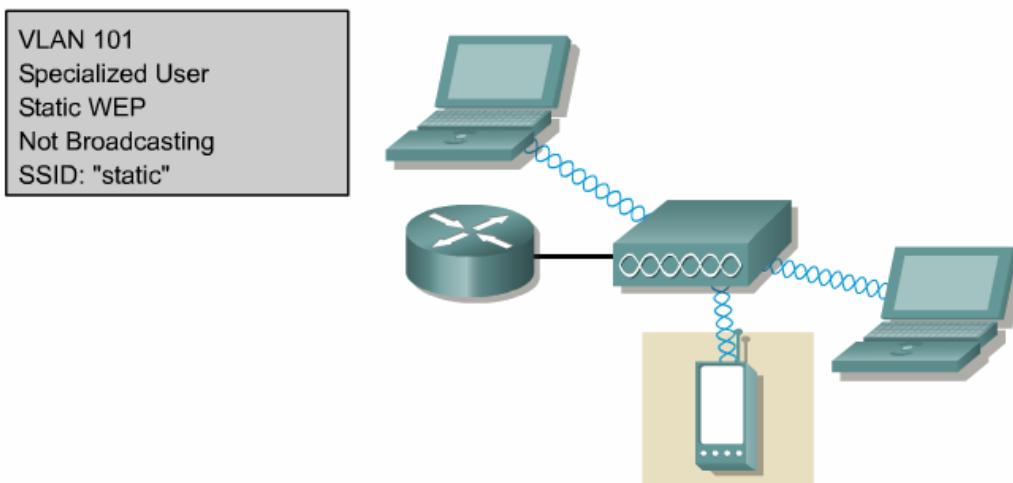


Figura 1



VLAN 100 allows guests who come into the Enterprise environment to connect directly to the internet, without having access to the Enterprise Servers. Without the function of VLANs, it would require two access points to provide isolated connectivity for the Guest users and Enterprise users. VLAN 100 would be configured with no security and it would broadcast its SSID. An Access Control List on the Router could also be configured to ensure that traffic with VLAN 100 tags go straight out the firewall.

Figura 2



VLAN 101 allows specialized users (shipping/receiving clerk) to use a barcode scanner with static WEP security since the barcode scanner cannot support dynamic security. VLAN 101 would be configured with static WEP security and not to broadcast its SSID.

Figura 3

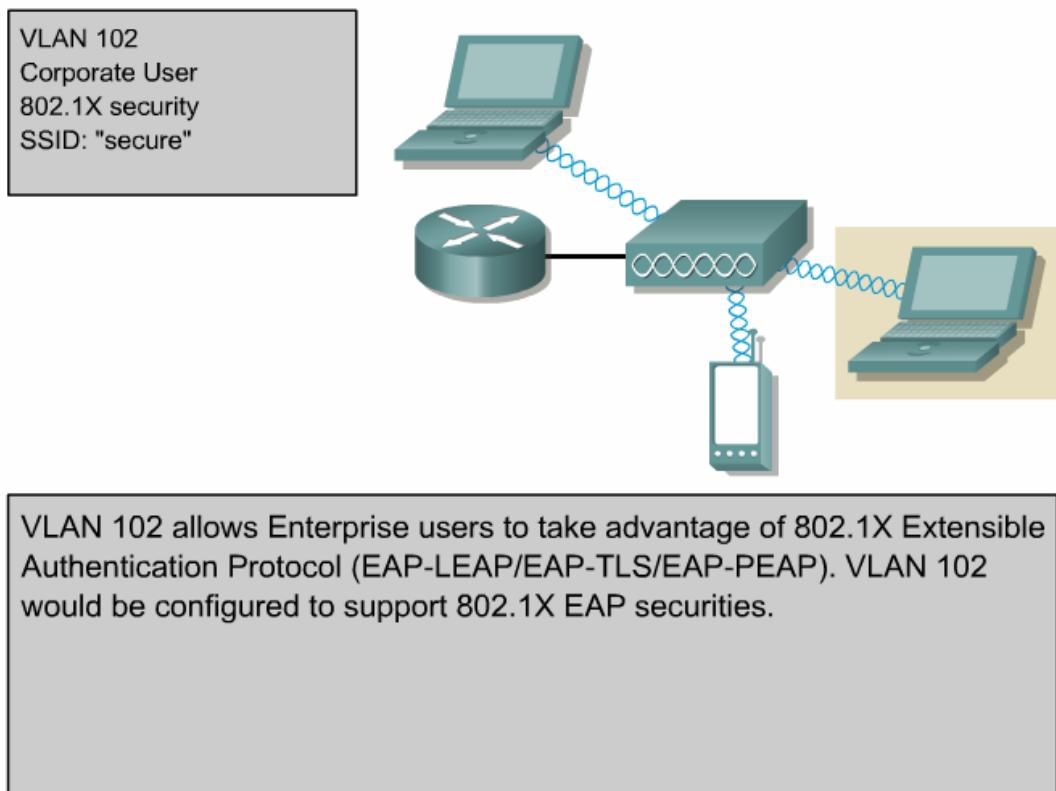


Figura 4

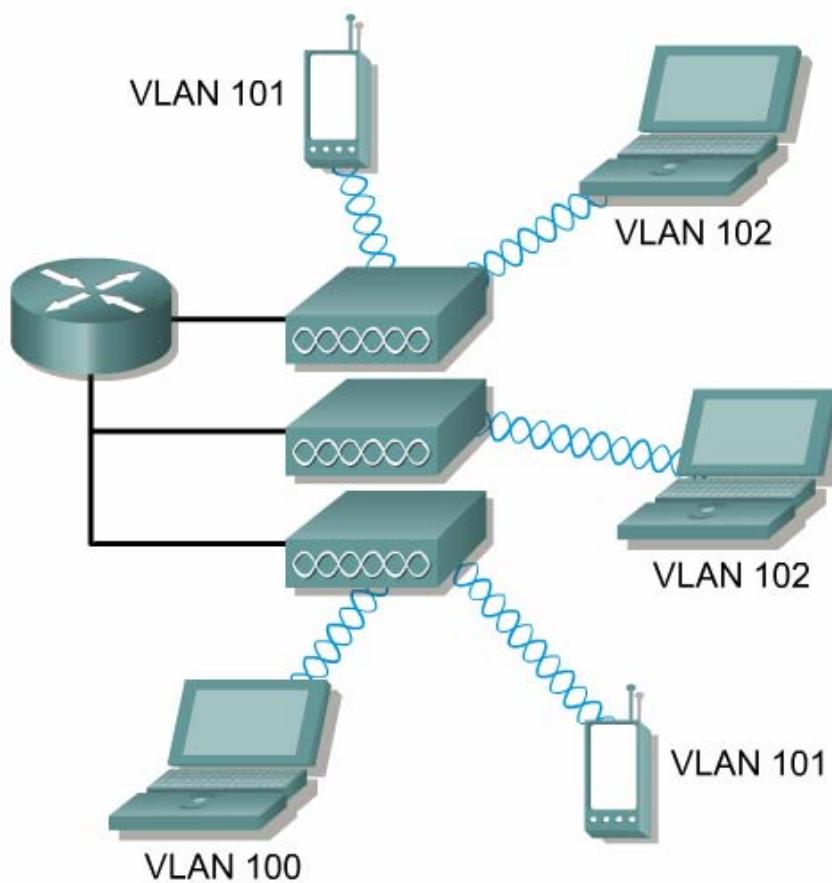


Figura 5

4.6.2 Función Calidad del Servicio (QoS)

El tráfico de datos crítico para el tiempo como voz y video se beneficia de la Calidad del Servicio (QoS), que puede configurarse para dar a la voz y al video una más alta prioridad. Esto permite una comunicación de voz fluida, video libre de jitter y una entrega confiable de e-mail configurado con una prioridad más baja. [1](#)

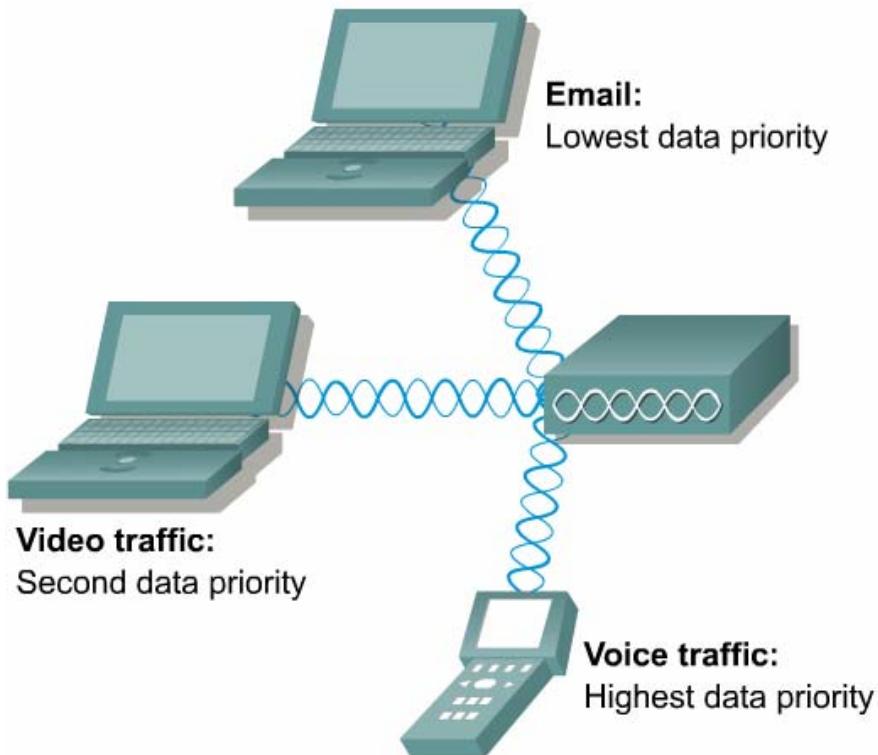


Figura 1

Cisco utiliza la misma Clase de Servicio (CoS) utilizada en los Routers Cisco. En este momento Cisco sólo puede soportar QoS downstream (Access Point a Cliente). Cuando se ratifique la QoS 802.11e, Cisco también soportará QoS upstream (Cliente a Access Point) simplemente actualizando el firmware.

La Clase de Servicio (CoS) utiliza el estándar 802.1P para configurar el campo de prioridad a tráfico de red. Existen ocho tipos diferentes de valores de tráfico CoS a los que se les puede asignar diferentes tráficos de red. [2](#)

CoS	Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Video Conferencing
3	Call Signaling
2	High Priority Data
1	Medium Priority Date
0	Best Effort Data

Figura 2

802.11e es suplementario de la capa MAC para proporcionar soporte de QoS para las aplicaciones LAN. Se aplicará a los estándares físicos 802.11 a, b, y g. El propósito es proporcionar clases de servicio con niveles administrados de QoS para aplicaciones de datos, voz y video.

802.11e tiene dos componentes:

1. Función de Coordinación Distribuida Mejorada (eDCF), que es responsable de la priorización.
2. Oportunidad de Transmisión (TXOP), que es responsable del control de la transmisión.

4.6.3 eDCF

Es un hecho que hay colisiones en la red al compartir la WLAN. Los clientes que se comunican en la WLAN en el mismo momento exacto ocasionan estas colisiones. Esto hace que ambos paquetes retrocedan durante un periodo aleatorio antes de ser enviados nuevamente. Las colisiones no pueden eliminarse enteramente pero mantenerlas en un mínimo ayudará a preservar el ancho de banda de su WLAN.

Para ayudar a mantener el ancho de banda, QoS utiliza eDCF para permitir que el tráfico de prioridad más alta acceda en primer lugar al medio WLAN. En el caso de QoS, en lugar de retroceder durante un periodo aleatorio, retroceden durante una cantidad de tiempo reducida, dependiendo de la prioridad de los paquetes. eDCF permite que el tráfico de más alta prioridad pase a través de las interfaces del Access Point más rápido que el tráfico de más baja prioridad.

En la Figura 1, un IFS (Espacio Interframe) (0) tiene un tiempo de retroceso más breve, por ejemplo, que un paquete de voz. Un IFS (n) tiene un tiempo de retroceso más largo (por ejemplo, paquete de email).

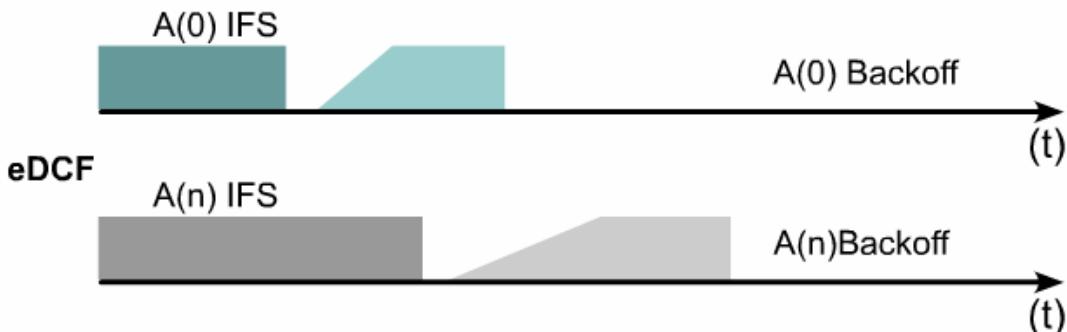


Figura 1

La oportunidad de transmisión (TXOP) es para entornos que tienen una gran cantidad de tráfico WLAN dirigiéndose a través del access point. Los paquetes de prioridad elevada sólo esperarán unos pocos segundos para retransmitir. Si el volumen del tráfico aún es alto, el paquete de alta prioridad continuará reenviándose una y otra vez. TXOP siempre reservará un lugar en la línea para los paquetes de alta prioridad utilizando para ellos los primeros pocos segundos. Esto garantizará una manipulación de este tipo de paquetes. Si no hay un paquete de prioridad alta en la cola, ese access point trata al siguiente paquete en la línea. eDCF también se utiliza para ayudar en el proceso de la manipulación de paquetes de alta prioridad.

4.6.4 IP móvil proxy

Roaming de Capa 2/IAPP

Los diseñadores de red que trabajan con usuarios móviles en un área grande a menudo encuentran que es necesario implementar más de un access point. El estándar 802.11 no define de qué manera los access points rastrean a los usuarios móviles ni cómo negociar una transferencia de un access point al siguiente, proceso denominado roaming. Varias compañías han introducido Protocolos de Punto de Inter-Acceso (IAPP) propietarios para soportar el roaming. IAPP logra el roaming dentro de una subred. No obstante, no se ocupa de cómo el sistema inalámbrico rastrea a los usuarios que se desplazan de una subred a otra cuando debe mantenerse la misma sesión, como es el caso de las llamadas de voz. 1

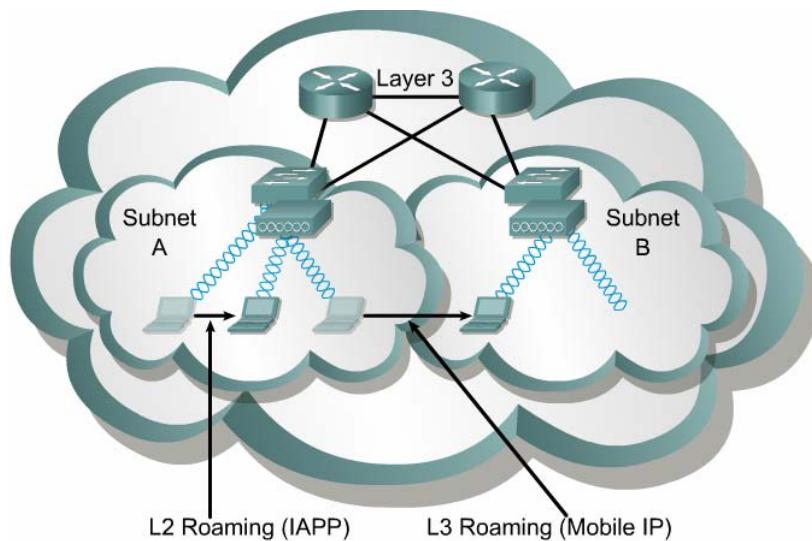


Figura 1

Roaming de Capa 3/IP Móvil

Allí donde la tecnología inalámbrica se implementa a través de múltiples subredes, existen opciones para lograr un roaming sin fisuras. Los adaptadores clientes inalámbricos pueden contener pilas IP clientes propietarias que comprenden la movilidad y permiten el roaming entre subredes. Todos los usuarios móviles de la red deben tener instalado este software. [1](#)

Roaming de Capa 3/IP Móvil Proxy

Otra opción es hacer que la infraestructura inalámbrica contenga la inteligencia necesaria para llevar a cabo la tarea. IP Móvil Proxy de Cisco proporciona esta funcionalidad. IP Móvil está diseñado para su uso incluso en los entornos de red más complejos. A medida que la estación inalámbrica abandona un área y entra en la siguiente, el nuevo access point consulta a una estación en busca de su agente home. Una vez que ha sido ubicado, el envío de paquetes se establece automáticamente entre el access point nuevo y el antiguo para asegurar que el usuario pueda intercambiar datos de manera transparente.

IP Móvil Estándar

IP Móvil Estándar requiere personal de IT para instalar software cliente IP Móvil en todos los clientes.

IP Móvil Proxy

IP Móvil Proxy no requiere que personal de IT instale el software cliente en cada cliente. No obstante, requiere la instalación y configuración de firmware en los Routers para soportar la función Agente Home/Agente de Envío. También será necesario configurar los access points para que soporten IP Móvil Proxy. [2](#)

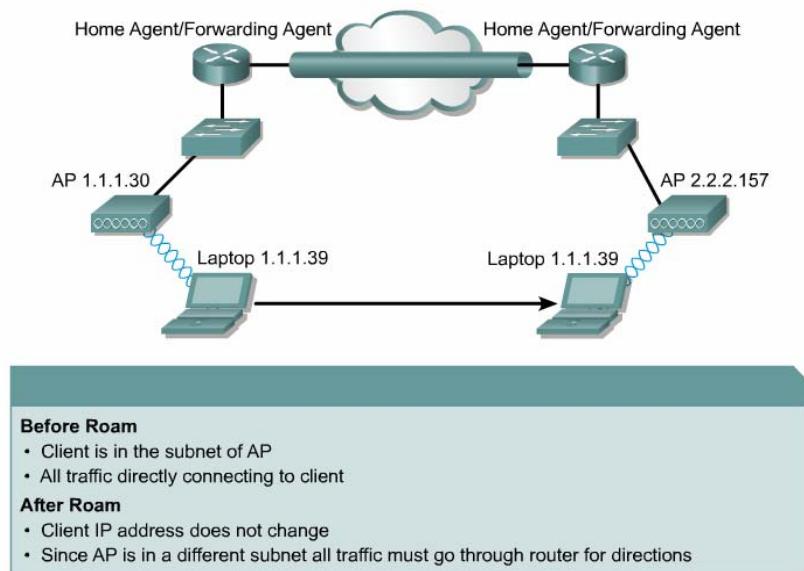


Figura 2

Resumen

Este módulo trató las topologías inalámbricas. En primer lugar, se describieron los componentes de las WLANs, como los dispositivos móviles y los adaptadores cliente, access points y bridges, y antenas. Una WLAN se definió como extensión de un entorno de red cableado.

Las dos topologías importantes tratadas fueron las WLANs y los bridges inalámbricos. También se trataron algunas variantes, que incluyen el repetidor inalámbrico y el bridge de grupo de trabajo. También se mencionaron funciones adicionales, como tolerancia a fallos, equilibrio de la carga y roaming.

Además se trató la configuración del canal junto con la importancia de la planificación del uso del canal, con tan poca superposición como sea posible entre canales que utilizan la misma frecuencia.

Finalmente, se abarcaron algunos ejemplos de diferentes topologías, concluyendo con una descripción general de Cisco AVVID.

Módulo 5: Puntos de acceso (APs)

Descripción general

Este módulo comenzará con información acerca de la instalación y configuración básicas de un access point (AP). Un access point actúa como hub de comunicaciones para los usuarios de redes inalámbricas. Un access point puede enlazar redes cableadas e inalámbricas. El objetivo de este módulo es hacer que el AP se configure y comunique. Es importante mantener la configuración simple hasta lograr la conectividad. Posteriormente en este módulo, se tratarán configuraciones y servicios de puerto más detallados.

En primer lugar, se trata la configuración básica utilizando una interfaz de línea de comandos (CLI), un navegador Web, y SNMP. El módulo examinará los pasos y tareas apropiados que deben seguirse para configurar apropiadamente un AP.

A continuación, se examina la configuración de los puertos AP. En general, existen dos puertos que pueden configurarse con access points. Se tratan tanto la configuración del puerto Ethernet como la configuración del puerto de radio. El módulo llevará al alumno paso a paso a través del proceso de configurar los puertos para su uso.

Finalmente, se tratan los diferentes servicios disponibles para los access points. El módulo tratará los servidores de tiempo, Web, nombre e inicio disponibles y cómo deberá configurarse cada uno de ellos.

5.1 Conexión del Access Point

5.1.1 Introducción

Un access point (AP) actúa como hub de comunicaciones para los usuarios de redes inalámbricas. Un AP puede enlazar redes cableadas e inalámbricas. En grandes instalaciones, múltiples APs pueden configurarse para permitir a los usuarios inalámbricos hacer roaming entre APs sin interrupción. Los access points también proporcionan seguridad. Finalmente, un AP puede actuar como repetidor inalámbrico, o punto de extensión para la red inalámbrica.

La Figura 1 ilustra el access point Cisco Aironet 1100 con una placa PCM 350. La Figura 2 enumera las funciones importantes de un AP.



Figura 1

Un access point puede controlarse y configurarse a través de la línea de comandos e interfaces de la Web. La administración también puede llevarse a cabo a través de protocolos tradicionales como SNMP y syslog. Una variedad de opciones de antena puede proporcionar un alcance o velocidad adicional, dependiendo de la instalación. Un access point puede ser de banda única, como el access point 802.11a de 5 GHz. También puede ser de banda dual, como el access point 802.11a de 5 GHz o el 802.11b de 2,4 GHz.

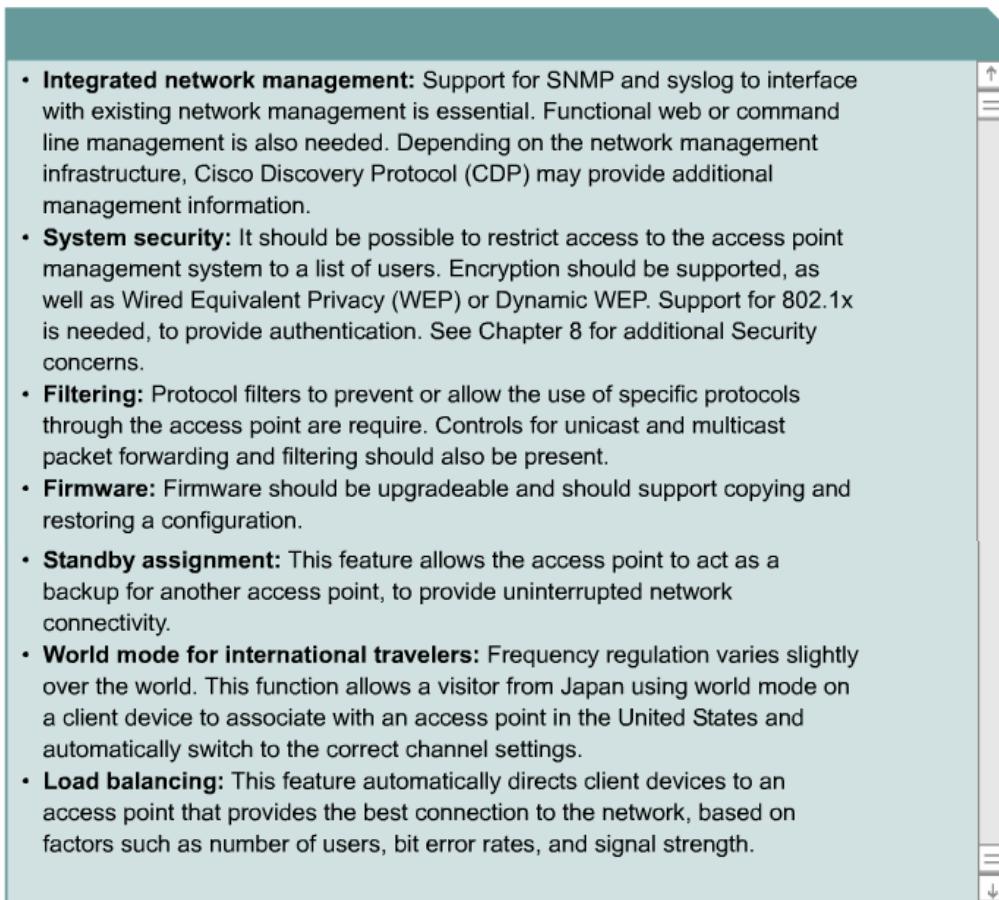


Figura 2

5.1.2 Conexión del 1100/1200

Con la radio 802.11a, o tanto la 802.11a como la 802.11b instaladas, el Cisco Aironet Serie 1200 puede alimentarse a través de Ethernet mediante el inyector de energía por línea entrante opcional, mediante un switch con energía de línea entrante, por medio de un patch panel con alimentación de línea entrante, o mediante una fuente de alimentación universal. **1**El 1100 puede también alimentarse a través de las mismas cuatro opciones. **2**Nunca conecte la alimentación DC al puerto de energía del AP y a la energía de la línea entrante de manera simultánea. **3**

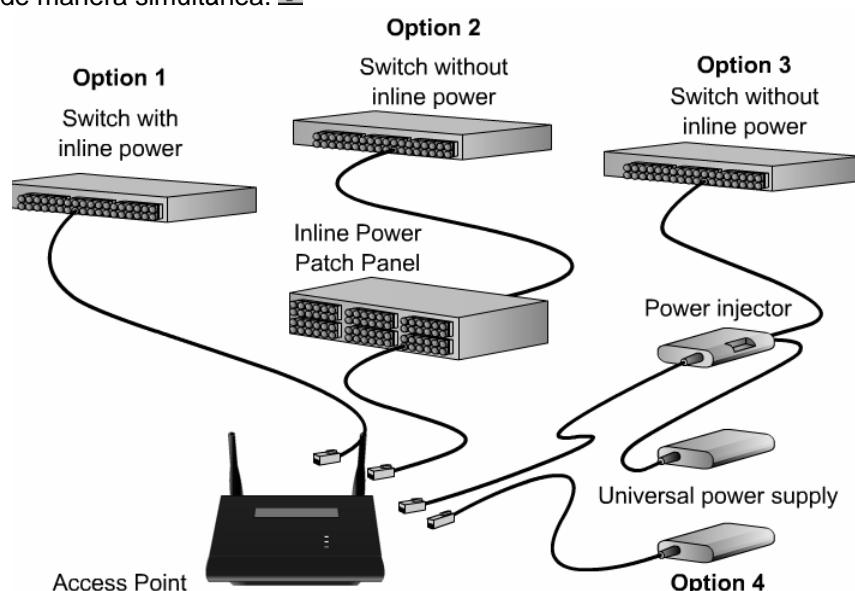


Figura 1

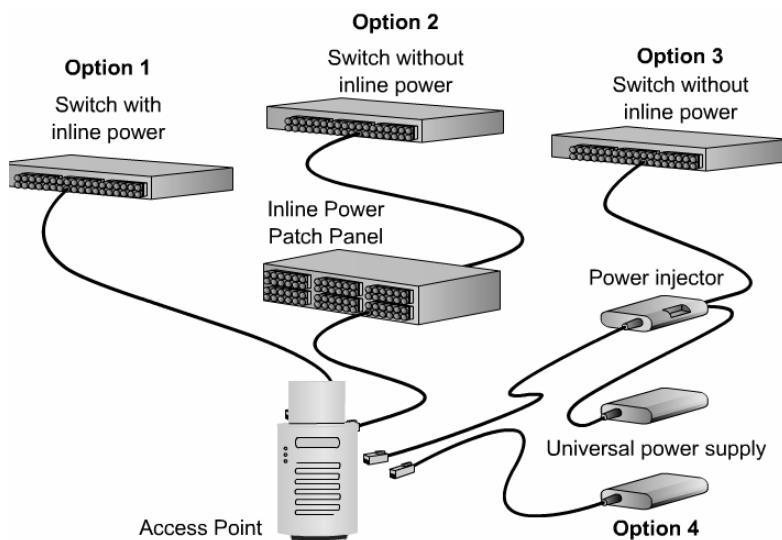


Figura 2

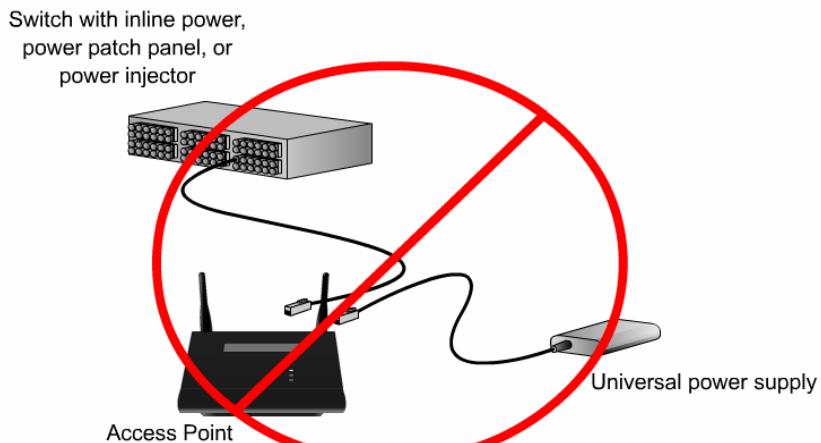


Figura 3

Las tecnologías de 2,4 GHz y 5 GHz utilizan 48 volts. Esto permite enviar energía a través del cable Cat 5 sin interrumpir la señal de datos. Se requiere menos hardware para la instalación.

La energía proveniente de una línea entrante reduce los costos de instalación, ya que no se requiere un electricista. Cualquier persona que esté calificada para tender cables Cat 5 puede instalar el cableado requerido para alimentar el Access Point Cisco Aironet. Los requisitos de cableado Cat 5 estándar aún se aplican (un máximo de 328 pies o 100 metros).

La tecnología de 2,4 GHz es compatible con toda la línea de dispositivos con alimentación habilitada de Cisco. La tecnología de 5 GHz también es compatible si se utiliza sólo una radio. Muchos de estos dispositivos ya existen para alimentar elementos tales como los teléfonos Cisco VoIP.

Junto con cada Access Point Serie 350 se vende un módulo de Inyección de Energía. El Access Point Serie 350 puede recibir energía ÚNICAMENTE a través del puerto RJ-45. No existe otro medio de alimentar al access point. Junto con el Access Point Serie 1200 se vende una batería tipo brick. Si es necesaria una fuente de energía de línea entrante, está disponible un inyector de energía de línea entrante que puede adquirirse por separado.

Hay cinco pasos que es necesario seguir al conectar el access point:

1. Enchufar el cable RJ-45 al puerto Ethernet que se encuentra en la parte posterior del access point.
2. Conectar el otro extremo del cable Ethernet a la LAN Ethernet 10/100.
3. Enchufar el adaptador de energía a un receptáculo de energía apropiado.
4. Enchufar el conector de energía a la parte posterior del access point. Durante el inicio, los tres LEDs del access point parpadean lentamente con los colores ámbar, rojo y verde en secuencia. Se requieren pocos minutos para completar la secuencia. Durante la operación normal, los LEDs parpadean con una luz verde.

5. Seguir los pasos de configuración para asignar configuraciones básicas al access point. El access point no tiene un interruptor de encendido/apagado. La energía se aplica a la unidad apenas se la enchufa. No conecte el cable Ethernet cuando el access point se activa. Siempre conecte el cable Ethernet antes de aplicar energía al access point.

5.1.3 Indicadores LED de los 1100/1200

LED Light	AP 1100 Ethernet LED	AP 1100 Status LED	AP 1100 Radio LED	1200 AP Ethernet LED	1200 AP Status LED	1200 AP Radio LED
Black/unlit	Link is down or port is shutdown	No client devices are associated. Check the units SSID and WEP settings	Default	No special meaning. Does not indicate link on 350 or 1200.	No power	No special meaning. Does not indicate link on 350 or 1200.
Blinking Green	Transmitting or receiving packets		Transmitting or receiving radio packets.	Receiving Ethernet packets	No client devices are associated. Check the SSID and WEP settings of the unit.	Transmitting or receiving radio packet
Steady Green	Link is up	At least one wireless device is associate. Everything is all right. Check the Ethernet or radio LED for more information.			Normal operation. At least one wireless client device is associated to the unit.	
Blinking Amber	Transmitting or receiving Ethernet errors	General warning	Maximum retries or buffer full occurred on one of the radios.	Transmitting or receiving Ethernet errors	General warning	Maximum retries or buffer full occurred on one of the radios.
Steady Red	Firmware failure. Disconnect power from the unit and reapply power.	If the other LEDs are not red, the unit is loading new firmware. If the other LEDs are red this is firmware failure. Disconnect power from the unit and reapply power.	Firmware failure. Disconnect power from the unit and reapply power.	Firmware failure. Disconnect power from the unit and reapply power.	If no other LEDs are lit, firmware is loading. If all lights are lit, it means a firmware failure has occurred. Disconnect power from the unit and reapply power.	Firmware failure. Disconnect power from the unit and reapply power.

Figura 1

Las luces LED de un access point transmiten información de estado. Cuando el access point se está encendiendo, los tres LEDs normalmente parpadean. Después del inicio, los colores de los LEDs representan lo siguiente:

- LEDs verdes indican una actividad normal.
- LEDs ámbar indican errores o advertencias.
- LEDs rojos significan que la unidad no está operando correctamente o está siendo actualizada.

La Figura 1 explica el significado de cada LED para los access points 1100 y 1200.

5.1.4 Conexión al AP

Un access point puede configurarse de varias formas. Un navegador Web es la forma más fácil de configurar el AP, pero también pueden utilizarse un cliente Telnet o una conexión de consola. El AP obtendrá una dirección IP utilizando DHCP, de ser posible. Si no se dispone de ningún servidor DHCP, un AP Cisco utilizará la dirección IP estática 10.0.0.1, por defecto. La sección 5.2 explicará cómo hallar la dirección IP del AP.

Configuración utilizando un navegador Web

Abra un navegador Web, e introduzca la dirección IP del AP en la línea de dirección del navegador. Se mostrará la pantalla de la página Web del AP.

Configuración utilizando Telnet

Desde un Shell DOS, tipee telnet <dirección-ip>. Utilice la dirección IP actualmente asignada al access point para <dirección-ip>.

Configuración utilizando la consola

Conecte un cable serie desde la PC al access point y abra HyperTerminal. Utilice los siguientes datos para configurar HyperTerminal:

- Bits por segundo (velocidad en baudios): 9600
- Bits de datos: 8
- Paridad: No parity
- Bits de parada: 1
- Control de flujo: Xon/Xoff o None

5.2 Configuración Básica

5.2.1 Resumen sobre configuración

Before setting up the access point, determine or gather the following information:

- A system name
- The case-sensitive wireless service set identifier (SSID) for the radio network
- If not connected to a DHCP server, use a unique IP address for the access point
- If the access point is not on the same subnet as the PC, use a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute, if SNMP is in use
- The MAC address from the label on the bottom of the access point, if IPSU is in use

Figura 1

Antes de comenzar la configuración, es importante reunir la información necesaria, que se muestra en la Figura 1.

Una vez reunida la información, utilice un navegador Web para asignar configuraciones básicas al access point. Siga los siguientes pasos para introducir las configuraciones básicas para el access point:

1. Conecte el access point tal como se describió en la sección anterior.
2. Utilice un navegador Web para abrir el sistema de administración para el access point, navegando hasta su dirección IP. Si una red utiliza un servidor DHCP, utilice la Utilidad de Configuración IP (IPSU) para hallar la dirección IP para el AP asignada por DHCP. El uso de la Utilidad de Configuración IP se tratará posteriormente en esta sección.

Introduzca las configuraciones básicas en la página Configuración Rápida [Express Setup].

5.2.2 Configuración de la dirección IP y la SSID de los APs

Pueden utilizarse cuatro métodos para configurar inicialmente el AP:

1. Una configuración remota utilizando una computadora que se comunique con el AP a través de un AP Cisco. La computadora utilizada para la configuración debe hallarse en la misma subred que el bridge.

2. Utilizar una computadora de la LAN cableada para comunicarse con el AP a través de un hub en la LAN cableada. La Utilidad de Configuración IP (IPSU) debe instalarse en la computadora, así como en la misma subred que el AP. IPSU utiliza IP multicast a través de la LAN cableada para comunicarse con el AP.
3. Utilizar una computadora no conectada en red para comunicarse directamente con el AP a través del cable cruzado. IPSU debe estar instalada en la computadora, así como en la misma subred que el AP.
4. Utilizar un cable consola y configurar el AP a través de la CLI (sólo para el AP 1200).

Si el access point no recibe una dirección IP desde un servidor DHCP, utilice IPSU para asignar la dirección IP y la SSID de un AP al mismo tiempo, como lo muestra la Figura 1. La computadora que se utiliza para asignar una dirección IP al access point debe tener una dirección IP propia. IPSU sólo puede cambiar la dirección IP y la SSID del access point a partir de su configuración por defecto. Una vez que la dirección IP y la SSID se han cambiado, IPSU no puede cambiarlas nuevamente a menos que el botón de modo se mantenga presionado. Esto reiniciará la configuración según los valores por defecto de fábrica.

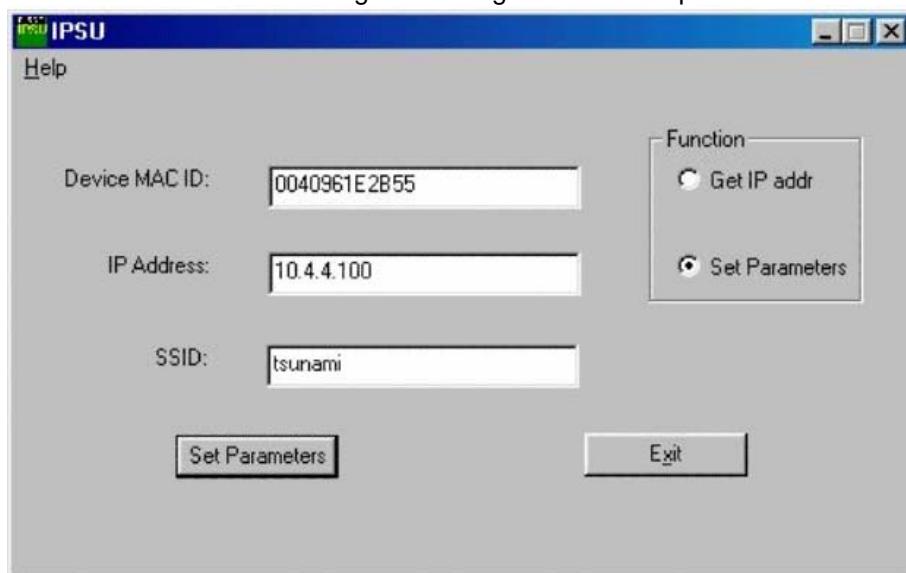


Figura 1

Siga los pasos de la Figura 2 para asignar una dirección IP y una SSID al access point.

- **Step 1** Double-click the IPSU icon on the desktop to start the utility.
- **Step 2** Click the Set Parameters radio button in the Function box.
- **Step 3** Enter the MAC address for the access point in the Device MAC ID field. The MAC address is printed on a label on the bottom of the unit. It should contain six pairs of hexadecimal digits. The MAC address field is not case-sensitive.
- **Step 4** In the IP Address field, enter the appropriate IP address to be assigned.
- **Step 5** Enter the SSID to be assigned in the SSID field.
- **Step 6** Click Set Parameters to change the IP address and SSID settings.
- **Step 7** Click Exit to exit IPSU.

Figura 2

5.2.3 Uso del navegador web: configuración rápida para introducir la configuración básica

Siga los pasos de la Figura 1 para introducir la configuración básica mediante un navegador Web de Internet. Si utiliza Netscape Communicator, el campo en el cual se introduce la dirección IP para el AP lleva el nombre Netsite o Location. Si se utiliza Microsoft Explorer, el campo lleva el nombre Dirección. Si el access point es nuevo y su configuración de fábrica no se ha cambiado, aparecerá la página Configuración Rápida [Express Setup] en lugar de la página Resumen de Estado [Summary Status] al navegar hacia el access point.

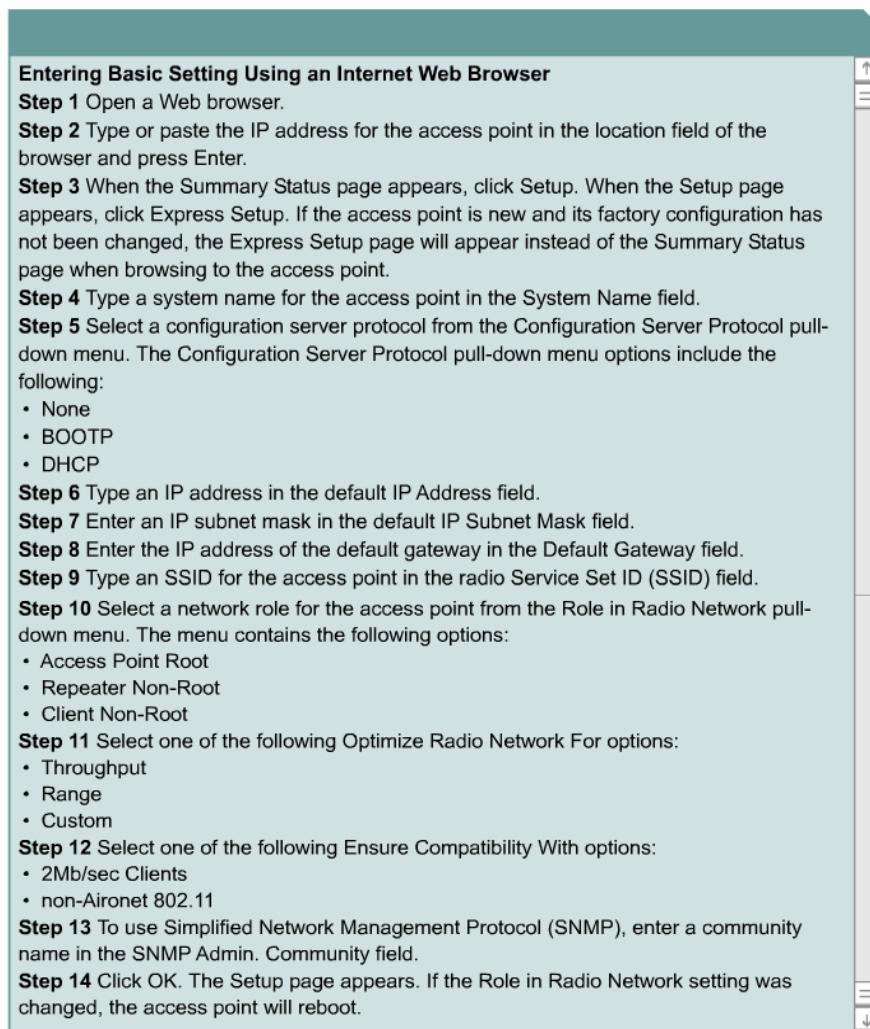


Figura 1

Las páginas del menú Configuración Rápida [Express Setup], para el Cisco Aironet series 1100 y 1200, se muestran en las Figuras 2 y 3. Éste es el menú de la página Web para el AP cuando se lo enciende por primera vez. Seguirá siendo la página por defecto hasta que no se haya introducido una configuración y el usuario haya hecho clic en Aplicar o Aceptar. Algunos nombres de campo varían ligeramente entre el Aironet 1100 y el 1200.

Hostname gui-ap
gui-ap uptime is 14 minutes

Express Set-Up

System Name:

MAC Address: 0005.9a39.2108

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SSID:

Broadcast SSID in Beacon: Yes No

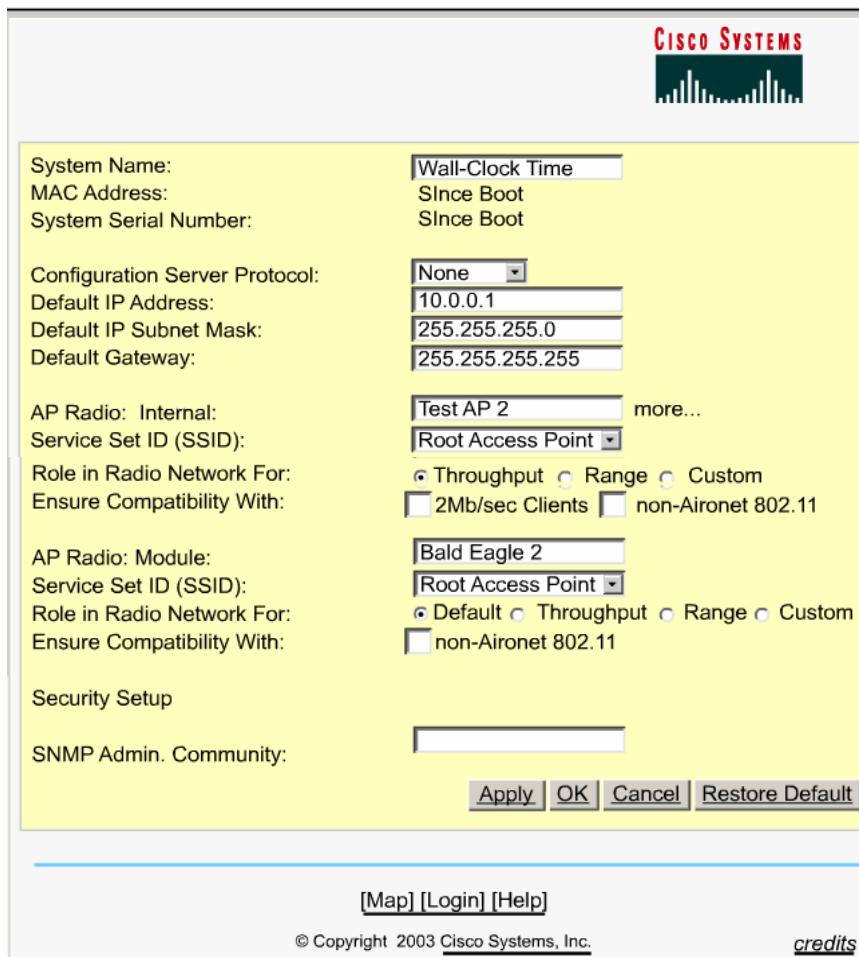
Role in Radio Network: Access Point Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Custom

Aironet Extensions: Enable Disable

SNMP Community:

Figura 2

[\[Map\]](#) [\[Login\]](#) [\[Help\]](#)

© Copyright 2003 Cisco Systems, Inc.

[credits](#)

Figura 3

Las configuraciones AP por defecto se muestran en la Figura 4.

Setting Name	Default Value
System Name	AP1100-CA62
Config Server Protocol	DHCP
IP address	This is assigned by DHCP. If DHCP is disabled, the default setting is 10.0.0.1.
IP Subnet Mask	This is assigned by DHCP. If DHCP is disabled, the default setting is 255.0.0.0.
Default Gateway	This is assigned by DHCP. If DHCP is disabled, the default setting is 0.0.0.0.
SSID	tsunami
Broadcast SSID in Beacon	Yes
Role in Radio Network	Access point (root)
Optimize Radio Network for	Throughput
Aironet Extensions	Enabled
SNMP Admin. Community	default Community

Figura 4

5.2.4 Interfaz de Línea de Comandos (CLI) y Configuración de SNMP

Otro método para configurar access points es mediante el uso de la interfaz de línea de comandos, menú, GUI o SNMP. En general, los usuarios pueden utilizar diferentes métodos para configurar los access points dependiendo del modelo y la versión de la imagen. Otros usuarios pueden preferir configurar un access

point con SNMP. En general, SNMP se utiliza para configurar access points cuando un servidor de administración SNMP existente se utiliza para configurar y administrar otros dispositivos de red. Las actividades de demostración de esta sección documentan los pasos requeridos para configurar un access point utilizando CLI y SNMP [1](#).

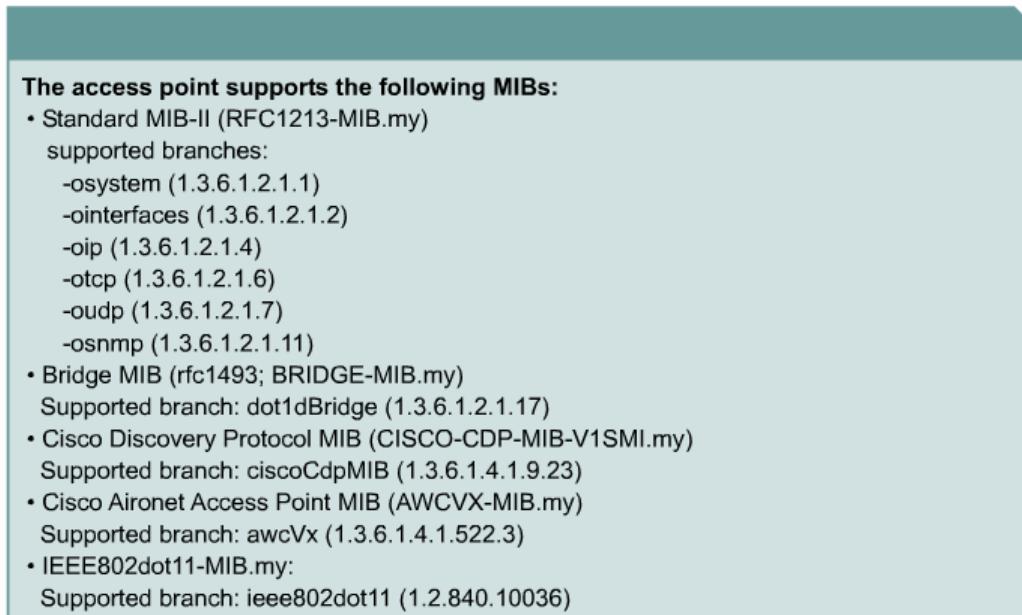


Figura 1

5.2.5 Navegación por la administración

Esta sección presentará información acerca de la interfaz de Web para las funciones de administración de los access points Cisco Aironet. Dependiendo del modelo y la versión de la imagen, la interfaz del navegador Web tendrá un aspecto diferente [1](#).

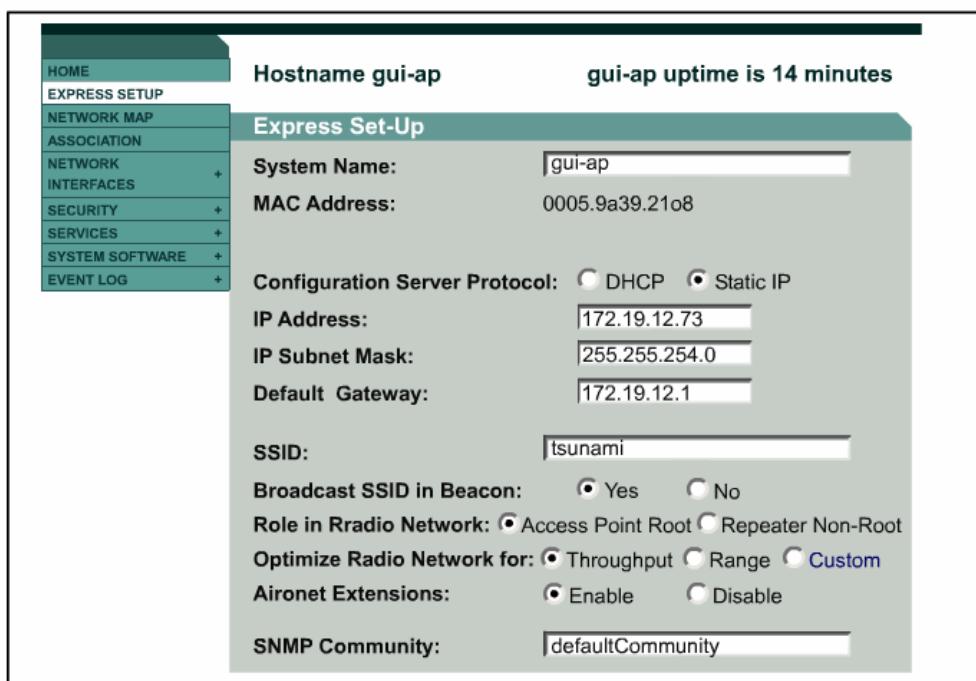


Figura 1

La interfaz del navegador Web contiene páginas de administración que pueden utilizarse para cambiar las configuraciones de los access points, actualizar el firmware y monitorear y configurar otros dispositivos inalámbricos de la red. La interfaz del navegador Web del access point es completamente compatible con Microsoft Internet Explorer versión 5.x o posterior, o Netscape Navigator versión 4.x.

Utilice los pasos que se muestran en la Figura 2 para comenzar a utilizar la interfaz del navegador de la Web.

- Step 1: Start the browser.
 - Step 2: Enter the IP address of the AP in the browser Location field or Address field and press Enter.
 - Step 3: The Summary Status page will appear.
- Some of the key areas of the Web browser interface include the following:**
- Buttons and Navigation Links
 - Main Web Pages Overview
 - Summary Status Home Page
 - Map Window
 - Network Page
 - Setup Page
 - Event Log Page
 - Online Help Page

Figura 2

5.3 Configuración del Puerto Ethernet

5.3.1 Descripción general

Esta sección describe cómo configurar el puerto Ethernet en un access point. Utilice las páginas de Ethernet que están vinculadas a la página de Configuración del sistema de administración, para establecer la configuración del puerto Ethernet. Las páginas Ethernet incluyen los elementos que se muestran en la Figura 1:

- Ethernet Port
- Ethernet Identification
- Ethernet Hardware
- Ethernet Filters
- Ethernet Advanced

Figura 1

- Puerto Ethernet — Enumera la información clave de configuración y estadística para el puerto Ethernet del access point
- Identificación de Ethernet — Contiene la información básica acerca de la identidad para el puerto Ethernet
- Hardware Ethernet — Contiene la configuración para la velocidad de conexión del puerto Ethernet en el access point
- Filtros Ethernet — Contiene las configuraciones para los filtros de protocolo
- Ethernet Avanzada — Contiene información acerca del estado operativo del puerto Ethernet en el access point. Esta página también puede utilizarse para efectuar cambios temporales en el estado del puerto, para ayudar a resolver problemas de la red.

5.3.2 Página de identificación de Ethernet

La página de identificación de Ethernet contiene información detallada acerca de la ubicación e identificación del puerto Ethernet. La página de identificación de Ethernet difiere levemente de otros puertos. En general documenta la conexión principal con la red cableada.

La página de identificación de Ethernet contiene la configuración del puerto principal, la dirección IP por defecto y la máscara de subred. La página también muestra la dirección MAC del access point, su dirección IP actual y su máscara de subred IP actual.

Configuración del puerto principal

La primera opción determina si este puerto es el puerto principal o no. La segunda opción sólo es significativa si el puerto actual no es el puerto principal. En este caso, un sí indica que deberán utilizarse los parámetros para el puerto principal, en lugar de cualquier parámetro configurado en este puerto. Las dos opciones disponibles para las configuraciones del puerto son las siguientes:

- Puerto principal — El puerto principal determina las direcciones MAC e IP del access point. Lo común es que el puerto principal del AP sea el puerto Ethernet. Seleccione sí para configurar el puerto Ethernet como puerto principal. Seleccione no para configurar el puerto Ethernet como puerto principal. Seleccione no para configurar el puerto de la radio como puerto principal.
- Adoptar la identidad del puerto principal — Seleccione sí para adoptar la configuración de puerto principal para las direcciones MAC e IP del puerto Ethernet. Seleccione no para utilizar direcciones MAC e IP para el puerto Ethernet.

Algunas configuraciones de bridge avanzadas requieren configuraciones diferentes para los puertos Ethernet y de radio.

Direcciones IP por defecto y actuales

Utilice esta configuración para asignar o cambiar la dirección IP por defecto para el access point. Si DHCP o BOOTP no están habilitados para la red, la dirección IP introducida en este campo se utilizará como dirección IP del AP. Si DHCP o BOOTP están habilitados, la dirección IP será proporcionada por este campo, pero sólo si no responde ningún servidor.

La dirección IP actual mostrada bajo la configuración de Dirección IP por Defecto muestra la dirección IP actualmente asignada al access point. Ésta es la misma dirección que la dirección IP por defecto a menos que DHCP o BOOTP estén habilitados. Si DHCP o BOOTP están habilitados, este campo mostrará la dirección IP que ha sido asignada dinámicamente al dispositivo. Esta dirección se mostrará mientras dure la sesión de la red.

Esta configuración también puede introducirse en las páginas Configuración Rápida [Express Setup] e Identificación de la radio del AP [AP Radio Identification].

Máscara de subred IP por defecto y actual

Introduzca una máscara de subred IP para identificar a la subred. Esto permitirá a la dirección IP ser reconocida en la LAN. Si DHCP o BOOTP no están habilitados, este campo se utiliza como máscara de subred. Si DHCP o BOOTP están habilitados, este campo proporcionará la máscara de subred, pero sólo si ningún servidor responde a la solicitud efectuada por el AP.

La máscara de subred IP actual muestra la máscara de subred IP que está actualmente asignada al access point. Ésta es la misma máscara de subred que la máscara de subred por defecto, a menos que DHCP o BOOTP estén habilitados. Si DHCP o BOOTP están habilitados, ésta es la máscara de subred asignada por el servidor.

Esta configuración también puede introducirse en las páginas Express Setup y AP Radio Identification.

5.3.3 Página hardware de Ethernet

Utilice la página Hardware de Ethernet [Ethernet Hardware] para seleccionar el tipo de conector, la velocidad de la conexión y la configuración dúplex utilizada por el puerto Ethernet del access point. La Figura 1 muestra la página Ethernet Hardware.

La página Ethernet Hardware contiene la configuración de Velocidad [Speed]. El menú desplegable Speed enumera cinco opciones para el tipo de conector, la velocidad de conexión y la configuración dúplex utilizados por el puerto. La opción seleccionada debe coincidir con el tipo, velocidad y configuración dúplex del conector real utilizados para enlazar el puerto con la red cableada.

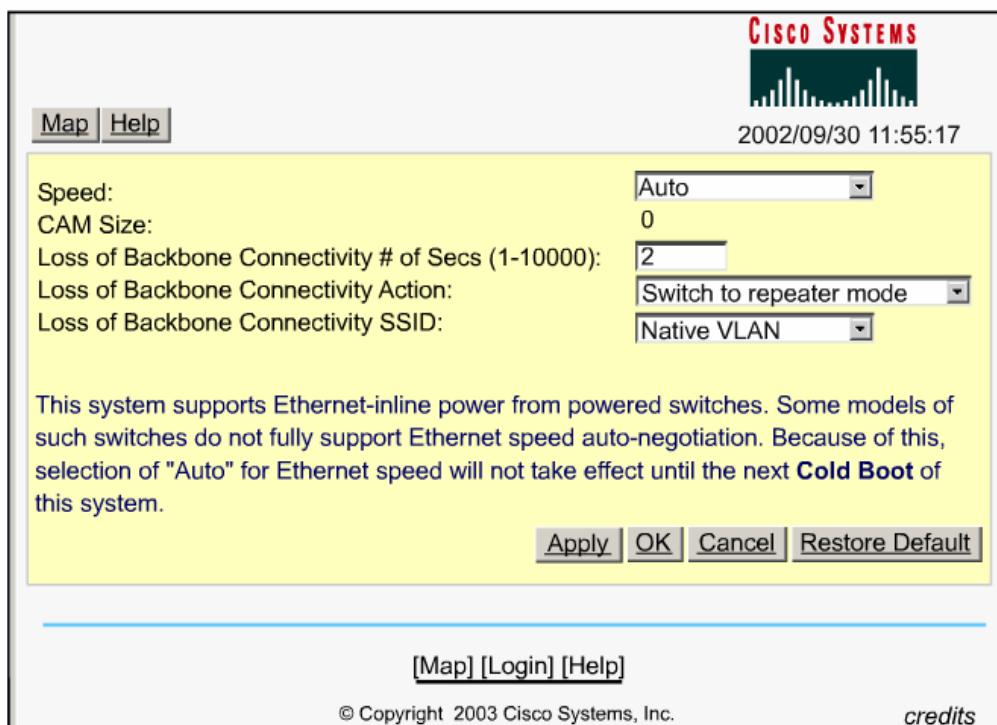


Figura 1

La configuración por defecto, Auto, es la mejor para la mayoría de las redes. Esto se debe a que las mejores velocidades de conexión y configuración dúplex se negocian automáticamente entre la LAN cableada y el access point. Si se utiliza otra configuración que no sea Auto, asegúrese de que el hub, switch o router al cual se conecta el access point soporte la selección. Existen las siguientes cinco opciones:

- Auto — Ésta es la configuración por defecto y recomendada. La velocidad de conexión y la configuración dúplex se negocian automáticamente, así como el hub, switch o router al cual está conectado el access point.
- 10BaseT / Half Duplex — Esto configura el conector de red Ethernet para una velocidad de transmisión de 10 Mbps a través de cable de par trenzado y operar en modo semidúplex.
- 10BaseT / Full Duplex — Esto configura el conector de red Ethernet para una velocidad de transmisión de 10 Mbps a través de cable de par trenzado y operar en modo full-dúplex.
- 100BaseT / Half Duplex — Esto configura el conector de red Ethernet para una velocidad de transmisión de 100 Mbps a través de cable de par trenzado y operar en modo semidúplex.
- 100BaseT / Full Duplex— Esto configura el conector de red Ethernet para una velocidad de transmisión de 100 Mbps a través de cable de par trenzado y operar en modo full-dúplex.

Algunos switches con energía de línea entrante no soportan por completo la auto-negociación de la velocidad de Ethernet. Si un interruptor enciende el access point con energía de línea entrante, la configuración de velocidad Auto se aplica sólo después de reiniciar el access point.

5.3.4 Página del filtro de protocolo de Ethernet

Los filtros de protocolo evitarán o permitirán el uso de protocolos específicos a través del access point. Los usuarios pueden configurar filtros de protocolo individuales o conjuntos de filtros. Pueden filtrarse los protocolos para dispositivos clientes inalámbricos, los usuarios de una LAN cableada o ambos. Por ejemplo, un filtro SNMP del puerto de radio del AP evitaría que los dispositivos clientes inalámbricos utilicen SNMP. No obstante, el filtro SNMP no bloquearía el acceso a SNMP desde la LAN cableada.

Utilice la página de Filtros de Protocolo de Ethernet para crear y habilitar filtros de protocolo para el puerto Ethernet del AP. Esta página proporciona a los administradores un control muy granular del flujo de tráfico a cada lado del access point, para mejorar la seguridad o el desempeño. Pueden configurarse tres clases de filtros en el puerto Ethernet, de la siguiente manera:

- EtherType — Ejemplos incluyen IP, ARP, y RARP
- Protocolo IP— Ejemplos incluyen TCP, UDP, RIP, y OSPF
- Puerto TCP o UDP — Ejemplos incluyen HTTP = 80 y SMTP = 25

La configuración y definiciones de filtros específicas se tratan en el Módulo 8.

5.3.5 Página avanzada de Ethernet

Utilice la página Avanzada de Ethernet para asignar configuraciones especiales para el puerto Ethernet del AP. La Figura 1 muestra la página Avanzada de Ethernet.

La página Avanzada de Ethernet contiene las siguientes configuraciones:

- Estado Solicitado
- Envío de Paquetes
- Filtros de Direcciones Unicast y Multicast por Defecto

La configuración del Estado Solicitado es útil para detectar problemas en la red. Activo [Up] es la configuración por defecto. Esta configuración por defecto permite al puerto Ethernet llevar a cabo operaciones normales. Inactivo [Down] inhabilita el puerto Ethernet del access point.

The screenshot shows the 'Advanced Ethernet' configuration page for port 0. At the top right is the Cisco Systems logo and the uptime information 'Uptime: 3 days, 19:30:22'. Below the header are two tabs: 'Map' and 'Help'. The main configuration area has several sections with dropdown menus and radio buttons:

- Requested Status:** Up
- Current Status:** Up
- Packet Forwarding:** Enabled
- Forwarding State:** Forwarding
- Default Multicast Address Filter:** Allowed
- Maximum Multicast Packets/Second:** 0
- Default Unicast Address Filter:** Allowed
- Always unblock Ethernet when STP is disabled:** No (radio button selected)
- Optimize Ethernet for:** Performance

At the bottom of the configuration area are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Default'. Below this is a horizontal line followed by three links: '[Map]', '[Login]', and '[Help]'. The entire window has a light gray border.

Figura 1

La línea Estado Actual [Current Status] bajo la configuración muestra el estado actual del puerto Ethernet. Este campo también puede mostrar Error, que indica que el puerto se encuentra en condición de error.

Durante las operaciones normales, la configuración Envío de Paquetes siempre es Habilitado [Enabled]. Para la detección de problemas, configure el envío de paquetes como Inhabilitado [Disabled]. Esto evita que los datos se desplacen entre los puertos Ethernet y de radio.

La línea Estado de Envío [Forwarding State] bajo la configuración muestra el estado del envío actual. El estado de la operación normal es Envío [Forwarding]. Los siguientes cinco estados son posibles:

- Enabled (Habilitado) — Éste es el estado operativo normal
- Unknown (Desconocido) — El estado no puede determinarse
- Disabled (Inhabilitado) — Las capacidades de envío están inhabilitadas
- Blocking (En bloqueo) — El puerto está bloqueando la transmisión
- Broken (Roto) — Este estado informa respecto a un fallo en el puerto Ethernet

Filtros de direcciones unicast y multicast por defecto

Los filtros de direcciones MAC permiten o no el envío de paquetes unicast y multicast enviados a direcciones MAC específicas. Pueden establecerse filtros que permitirán el paso del tráfico hacia todas las direcciones MAC excepto a aquéllas especificadas, o no permitirán que el tráfico pase si no se lo especifica. Los paquetes unicast se dirigen a un solo dispositivo de la red. Los paquetes multicast y broadcast se dirigen a múltiples dispositivos de la red.

Los menús desplegables para los filtros de direcciones unicast y multicast contienen las siguientes dos opciones:

- Permitido [Allowed] — El access point envía todo el tráfico excepto los paquetes enviados a las direcciones MAC enumeradas como no permitidas, en la página Filtros de Dirección.
- No permitido [Disallowed] — El access point descarta todo el tráfico excepto los paquetes enviados a las direcciones MAC enumeradas como permitidas, en la página Filtros de Dirección.

Para la mayoría de las configuraciones, el filtro de direcciones multicast por defecto deberá configurarse como Allowed. Si se pretende configurarlo como Disallowed, agregue la dirección MAC broadcast ff ff ff ff ff ff a la lista de direcciones permitidas de la página Filtros de Direcciones, antes de cambiar la configuración.

Si se planifica descartar el tráfico de todas las direcciones MAC excepto aquéllas especificadas utilizando la configuración Disallowed, asegúrese de permitir la dirección MAC utilizada en la página Filtros de Dirección.

5.4 Configuración del Puerto de la Radio AP

5.4.1 Descripción general

Esta sección describe cómo configurar la radio AP. Utilice las páginas de la Radio AP en la página de configuración del sistema de administración, para establecer la configuración de la radio. Las páginas de la radio incluyen las siguientes:

- AP Radio Port Link
- AP Radio Identification
- AP Radio Hardware
- AP Radio Filters
- AP Radio Advanced

- Enlace del Puerto de la Radio AP — Enumera la información de configuración del puerto de la radio y estadísticas claves para el access point
- Identificación de la Radio AP — Contiene la información básica sobre la ubicación e identidad para el puerto de radio del access point
- Hardware de la Radio AP — Contiene las configuraciones de SSID para las velocidades de datos, potencia de transmisión, antenas, canal de radio y umbrales operativos del access point
- Filtros de la Radio AP — Contiene configuraciones para los filtros de protocolo
- Radio AP Avanzada — Contiene información acerca del estado operativo del puerto de la radio del access point. Esta página también puede utilizarse para efectuar cambios temporales en el estado del puerto para ayudar a detectar problemas de red.

5.4.2 Identificación del puerto de radio

La página de Identificación de la Radio Raíz [Root Radio Identification] contiene la información básica acerca de la ubicación e identificación del puerto de radio del AP. La página de Identificación de la Radio del AP difiere levemente de la del puerto Ethernet, por el hecho de que administra la conexión con la red inalámbrica.

Dos opciones permiten a los usuarios diseñar el puerto de la radio como puerto principal y seleccionar si el puerto de la radio adopta o asume la identidad del puerto principal.

1. Puerto principal — El puerto principal determina las direcciones MAC e IP para el access point. Comúnmente, el puerto principal del AP es el puerto Ethernet, que está conectado a la LAN inalámbrica. Seleccione no para configurar el puerto Ethernet como puerto principal. Seleccione sí para configurar el puerto de la radio como puerto principal.
2. Adopción de una identidad de puerto principal — Seleccione sí para adoptar la configuración del puerto principal para las direcciones MAC e IP de este puerto. Seleccione no para utilizar diferentes direcciones MAC e IP para el puerto de la radio.

Cuando los access points actúan como unidades raíz, asumen la configuración del puerto principal para el puerto de la radio.

Dirección IP por defecto y actual

Utilice esta configuración para asignar una dirección IP por defecto para el puerto de la radio que sea diferente a la dirección IP Ethernet del access point. Durante la operación normal, el puerto de la radio adopta la identidad del puerto Ethernet. No obstante, cuando un access point se encuentra en modo standby, se asigna una dirección IP diferente al puerto de radio. Algunas configuraciones de bridge avanzadas también requieren una dirección IP única para el puerto de radio.

Máscara de subred IP por defecto y actual

Introduzca una máscara de subred IP para identificar la subred de modo tal que la dirección IP pueda reconocerse en la LAN. Si DHCP o BOOTP no están habilitados, este campo es la máscara de subred. Si DHCP o BOOTP están habilitados, este campo proporciona la máscara de subred sólo si ningún servidor responde a la solicitud efectuada por el access point. La máscara de subred IP actual mostrada bajo la configuración muestra la máscara de subred IP actualmente asignada al access point. Ésta es la misma máscara de subred que la máscara de subred por defecto a menos que DHCP o BOOTP estén habilitados. Si DHCP o BOOTP están habilitados, ésta es la máscara de subred asignada por el servidor DHCP o BOOTP. Esta configuración también puede introducirse en la página Express Setup.

ID del conjunto de servicios (SSID)

La SSID es un identificador único que utilizan los dispositivos clientes para asociarse con el access point. La SSID ayuda a los dispositivos clientes a distinguir entre múltiples redes inalámbricas del mismo "vecindario". La SSID puede ser cualquier valor alfanumérico de uno a 32 caracteres de longitud. Esta configuración también puede introducirse en la página Express Setup.

5.4.3 Hardware del puerto de radio

Utilice la página Hardware de Radio del AP, que se muestra en la Figura 1, para asignar configuraciones relativas al hardware de radio del access point.

Las siguientes son descripciones de los diversos campos:

- ID del conjunto de servicios (SSID) — La SSID es un identificador único que los dispositivos cliente utilizan para asociarse al access point. La SSID ayuda a los dispositivos clientes a distinguir entre múltiples redes inalámbricas vecinas. La SSID puede ser cualquier valor alfanumérico de 1 a 32 caracteres de longitud. Cisco recomienda asignar o cambiar la SSID en la página Express Setup. Los caracteres no ASCII pueden introducirse en la SSID tipeando una barra invertida (\), una x minúscula, y los caracteres hexadecimales que representan el carácter no ASCII. Por ejemplo, \xbd inserta el símbolo ½.
- ¿Permitir la asociación de la SSID de broadcast? [Allow Broadcast SSID to Associate?] — Utilice esta configuración para elegir si se permite a los dispositivos que no especifican una SSID asociarse al access point. Estos dispositivos enviarán un mensaje broadcast que busca un access point al cual asociarse. Las siguientes son las opciones que pueden llevarse a cabo:
 - Yes (Sí) — Ésta es la configuración por defecto. Permite a los dispositivos que no especifican una SSID asociarse al access point.
 - No — No se permite a los dispositivos sin una SSID especificada asociarse al access point. Si se selecciona no, la SSID utilizada por el dispositivo cliente debe coincidir exactamente con la SSID del access point.
- Habilitar el modo mundial [Enable World Mode] — Cuando se selecciona sí desde el menú desplegable del modo mundial, el access point agrega información del conjunto de la portadora del canal a su baliza. Los dispositivos clientes con el modo mundial habilitado recibirán la información del conjunto de la portadora y ajustarán su configuración automáticamente.
- Velocidades de datos [Data Rates] — Utilice la configuración de velocidad de datos para elegir las velocidades de datos que utiliza el access point para la transmisión de datos. Las velocidades se expresan en megabits por segundo (Mbps). El access point siempre intenta transmitir a la velocidad más alta seleccionada. Si hay obstáculos o interferencia, el access point baja a la velocidad más alta que permite la transmisión de datos. Para cada una de las cuatro velocidades, 1, 2, 5.4, y 11 Mbps, un menú desplegable enumerará las siguientes tres opciones:
 - Básica [Basic] (por defecto) — Permite la transmisión a esta velocidad para todos los paquetes, tanto unicast como multicast. Al menos una velocidad de datos debe configurarse a Básica.
 - Yes (Sí) — Permite la transmisión a esta velocidad sólo para paquetes unicast.
 - No — No permite la transmisión a esta velocidad.

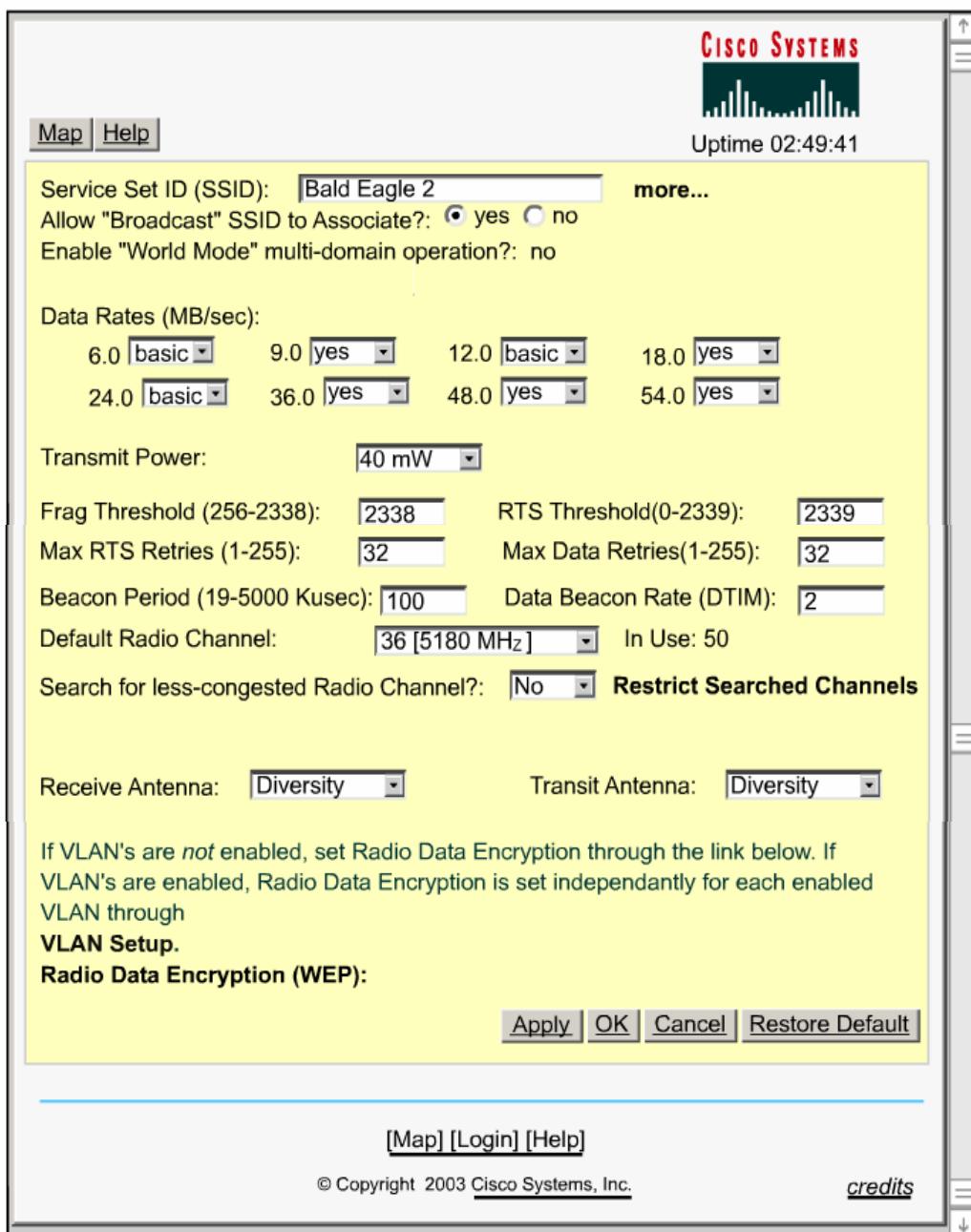


Figura 1

La configuración Optimizar la Red de Radio para [Optimize Radio Network for] en la página Configuración Rápida selecciona la configuración de velocidad de datos automáticamente. Al seleccionar Optimize Radio Network for Throughput (para Throughput) en la página Configuración Rápida, las cuatro velocidades de datos se configuran como Básicas. Al seleccionar Optimize Radio Network for Range (para Alcance) en la página Configuración Rápida, la velocidad de datos de 1,0 se configura a Básica, y las otras velocidades de datos se configuran a Sí.

- **Potencia de transmisión [Transmit Power]** — Esta configuración determina el nivel de potencia de la transmisión de radio. Las regulaciones del gobierno definen el nivel de potencia más alto disponible para los dispositivos de radio. Esta configuración debe conformarse a los estándares establecidos para el país en el cual se está utilizando el access point. Para reducir la interferencia o conservar la potencia, seleccione una configuración de potencia más baja. Las configuraciones del menú desplegable en los access points serie 350 incluyen 1, 5, 20, 50, y 100 miliwatts.
- **Umbral de fragmentación [Frag. Threshold]** — Esta configuración determina el tamaño según el cual se fragmentan los paquetes y se los envía como varios trozos, en lugar de un único bloque. Introduzca un valor de 256 a 2338 bytes. Utilice una configuración baja en áreas donde la comunicación es pobre o donde hay gran cantidad de interferencia de radio.
- **Umbral RTS [RTS Threshold]** — Esta configuración determina el tamaño del paquete según el cual el access point emite una solicitud de envío (RTS) antes de enviar un paquete. Un Umbral RTS bajo

puede ser útil en áreas donde hay muchos dispositivos cliente asociados con el access point. También puede ser útil en áreas donde los clientes están lejos y pueden detectar sólo el access point y no detectarse entre sí. Introduzca un valor de 0 a 2339 bytes.

- Máxima cantidad de reintentos de RTS [Max. RTS Retries] — Ésta es la cantidad máxima de veces que el access point emitirá una RTS, antes de que deje de intentar enviar el paquete a través de la radio. Introduzca un valor de uno a 128.
- Máxima cantidad de reintentos de datos [Max. Data Retries] — Ésta es la cantidad máxima de intentos que hará el access point para enviar un paquete, antes de dejar de intentar y descartarlo.
- Periodo de Baliza [Beacon Period] — Ésta es la cantidad de tiempo entre balizas en unidades de milisegundos donde 1 ms es 1024 μ s.
- Velocidad de balizas de datos (DTIM) — Esta configuración, siempre un múltiplo del periodo de baliza, determina cuán a menudo la baliza contiene un mensaje de indicación de tráfico de entrega (DTIM). El DTIM le indica a los dispositivos clientes con ahorro de energía que un paquete los está esperando. Por ejemplo, si el periodo de baliza está configurado a su valor por defecto de 100, y la velocidad de balizas de datos está configurada a su configuración por defecto de dos, entonces el access point envía una baliza que contiene un DTIM cada 200 ms.
- Canal de radio por defecto [Default Radio Channel] — La configuración de fábrica para los sistemas Cisco WLAN es el Canal de Radio 6, que transmite a 2437 MHz. Para superar un problema de interferencia, otras configuraciones de canal están disponibles desde el menú desplegable de 11 canales, que van de los 2412 a los 2462 MHz. Cada canal abarca 22 MHz. El ancho de banda de los Canales 1, 6, y 11 no se superpone. Por lo tanto, múltiples access points cercanos crean una congestión de radio que puede reducir el throughput. Un estudio cuidadoso del sitio puede determinar la mejor ubicación de los access points para una máxima cobertura de radio y un máximo throughput.
- Búsqueda del canal de radio menos congestionado [Search for Less-Congested Radio Channel] — Cuando se selecciona sí desde el menú desplegable Search for Less-Congested Radio Channel, el access point busca el canal de radio menos ocupado y selecciona dicho canal para su uso. El access point busca durante el inicio y cuando las configuraciones de radio cambian. De ser necesario, mantenga el access point asignado a un canal específico para evitar que interfiera con otros access points. Esta configuración deberá dejarse en no.
- Antena de recepción y antena de transmisión [Receive Antenna and Transmit Antenna] — Los menús desplegables para las antenas de recepción y transmisión ofrecen las siguientes tres opciones:
 - Diversidad [Diversity] — Esta configuración por defecto le indica al access point que utilice la antena que reciba la mejor señal. Si el access point tiene dos antenas fijas, utilice esta configuración tanto para recibir como para transmitir.
 - Derecha [Right] — Si el access point tiene antenas removibles y se instala una antena de alta ganancia en el conector derecho, deberá utilizarse la configuración tanto para recibir como para transmitir. Al observar el panel trasero del access point, la antena derecha se encuentra a la derecha.
 - Izquierda [Left] — Si el access point tiene antenas removibles y se instala una antena de alta ganancia en el conector izquierdo, deberá utilizarse la configuración tanto para recibir como para transmitir. Al observar el panel trasero del access point, la antena izquierda se encuentra a la izquierda.

El access point recibe y transmite utilizando una única antena a la vez. Por lo tanto, instalar antenas de alta ganancia en ambos conectores, con una apuntando hacia el norte y otra apuntando hacia el sur, no incrementará el alcance. Cuando el access point utiliza la antena que apunta al norte, los dispositivos cliente del sur se ignorarían.

5.4.4 Filtros del puerto de radio

Los filtros de protocolo evitan o permiten el uso de protocolos específicos a través del access point. Pueden configurarse filtros de protocolo individuales o conjuntos de filtros. Pueden configurarse protocolos para dispositivos clientes inalámbricos, usuarios en la LAN cableada, o ambos. Por ejemplo, un access point con un filtro SNMP en el puerto de la radio evitaría que los dispositivos clientes utilicen SNMP. No obstante, el filtro no bloquearía el acceso SNMP desde la LAN cableada.

Utilice la página Filtros de Protocolo de Radio AP [AP Radio Protocol Filters] para crear y habilitar filtros de protocolo para el puerto de radio del access point. Esta página otorga a los administradores un control granular del flujo de tráfico de cada lado del access point, para mejorar la seguridad y el desempeño. Pueden configurarse tres clases de filtros en el puerto de radio del AP:

- EtherType

- Protocolo IP
- Puerto IP

La configuración y las definiciones específicas de los filtros se tratan en el Módulo 8.

5.4.5 Radio AP avanzada

La página Radio del AP avanzada [AP Radio Advanced] se utiliza para asignar configuraciones especiales para el estado operativo del puerto Inalámbrico. Esta página puede utilizarse para efectuar cambios temporales en el estado del puerto para ayudar a detectar problemas en la red.

5.5 Configuración de Servicios

5.5.1 Servidor de tiempo

Los diez servicios que pueden configurarse desde la página de configuración se enumeran en la Figura 1. SNMP, los Servicios Cisco y la Seguridad se tratarán en el Módulo 8.



Figura 1

La página Configuración del servidor de tiempo [Time Server Setup] se utiliza para introducir configuraciones propias del servidor de tiempo. La página Configuración del servidor de tiempo contiene las siguientes configuraciones:

- Protocolo de Tiempo de Red Simple [Simple Network Time Protocol]: seleccione Enabled o Disabled para activar o desactivar el Protocolo de Tiempo de Red Simple (SNTP). Si la red utiliza SNTP, seleccione Enabled.
- Servidor de Tiempo por Defecto [Default Time Server]: si la red tiene un servidor de tiempo por defecto, introduzca la dirección IP para el servidor en el campo de entrada del Servidor de Tiempo por Defecto.
- La línea Servidor de Tiempo Actual [Current Time Server] informa la dirección IP del servidor de tiempo que está utilizando actualmente el access point. El servidor DHCP o BOOTP puede anular el servidor de tiempo por defecto.
- Compensación GMT (hora) [GMT Offset (hr)]: el menú desplegable Compensación GMT enumera las zonas horarias mundiales, en relación a la Hora del Meridiano de Greenwich (GMT). Seleccione la zona horaria en la cual opera el access point.
- Utilizar horario de verano [Use Daylight Savings Time]: seleccione Sí o No para que el access point se ajuste automáticamente al horario de verano o no.
- Configurar manualmente la fecha y la hora [Manually Set Date and Time]: introduzca la fecha y la hora actual en los campos de entrada para anular el servidor de tiempo o para configurar la fecha y la hora si no hay un servidor disponible. Al introducir la fecha y la hora, utilice barras para separar el año, mes y día. Utilice dos puntos para separar las horas, minutos y segundos. Por ejemplo: introduzca 2001/02/17 para el 17 de febrero de 2001; y 18:25:00 para las 6:25 pm.

5.5.2 Servidor de inicio

Utilice la página Configuración del servidor de inicio [Boot Server Setup] para configurar el access point para que utilice los servidores BOOTP o DHCP de la red, para una asignación automática de direcciones IP. La página Boot Server Setup contiene las siguientes configuraciones, también enumeradas en la Figura 1:

- Configuration Server Protocol
- Use Previous Configuration Server Settings
- Read .ini File from File Server:
- BOOTP Server Timeout (sec):
- DHCP Multiple-Offer Timeout (sec)
- DHCP Requested Lease Duration (min)
- DHCP Minimum Lease Duration (min)
- DHCP Class Identifier

Figura 1

- Protocolo del servidor de configuración [Configuration Server Protocol]: utilice el menú desplegable del protocolo del servidor de configuración para seleccionar el método o la asignación de direcciones IP que utilizará la red. El menú contiene las siguientes opciones:
 - None (Ninguno): la red no tiene un sistema automático para la asignación de direcciones IP.
 - BOOTP: la red utiliza el Protocolo de Inicio, en el cual las direcciones IP se asignan de forma permanente, basándose en las direcciones MAC.
 - DHCP: con el Protocolo de Configuración Dinámica del Host, las direcciones IP se alquilan durante un tiempo. Establezca la duración del alquiler mediante las configuraciones de esta página.
- Utilizar las configuraciones anteriores del servidor de configuración [Use Previous Configuration Server Settings]: seleccione Sí para hacer que el access point guarde la respuesta más reciente desde el servidor de inicio. El access point utiliza las configuraciones más recientes, si el servidor de inicio no está disponible.
- Leer el archivo .ini desde el servidor de archivos [Read .ini File from File Server]: utilice esta configuración para hacer que el access point utilice las configuraciones de un archivo .ini del servidor BOOTP o DHCP o el servidor de archivos por defecto. Los archivos con extensiones .ini usualmente contienen información de configuración que se utiliza durante el inicio del sistema. El menú desplegable contiene las siguientes opciones:
 - Always (Siempre): el access point siempre carga las configuraciones desde un archivo .ini que se encuentra en el servidor.
 - Never (Nunca): el access point nunca carga las configuraciones desde un archivo .ini que se encuentra en el servidor.
 - If specified by server (Si lo especifica el servidor): el access point carga las configuraciones desde un archivo .ini que se encuentra en el servidor, si la respuesta del servidor DHCP o BOOTP especifica que un archivo .ini está disponible. Ésta es la configuración por defecto.
 - Load Now (Cargar ahora): este botón instruye al access point para que lea un archivo .ini inmediatamente.
 - Current Boot Server (Servidor de inicio actual): esta línea enumera el servidor que respondió a la solicitud de inicio del AP. Si aparecen todos ceros, significa que el access point no está utilizando BOOTP/DHCP o que ningún servidor respondió a la solicitud BOOTP/DHCP. La línea Servidor de Archivos ".ini" Especificado [Specified ".ini" File Server] enumera la dirección IP del servidor donde está almacenado el archivo .ini. Si aparecen todos ceros, significa que ningún servidor de archivos está configurado para proporcionar un archivo .ini.
- Tiempo vencido del servidor BOOTP (s) [BOOTP Server Timeout (sec)]: esta configuración especifica el tiempo que espera el access point para recibir una respuesta de un único servidor BOOTP. Introduzca la cantidad de segundos que deberá esperar el access point.
- Tiempo vencido de oferta múltiple DHCP (s) [Multiple-Offer Timeout (sec)]: esta configuración especifica el tiempo que espera el access point para recibir una respuesta, cuando existen múltiples servidores DHCP. Introduzca la cantidad de segundos que deberá esperar el access point.
- Duración del alquiler solicitado por el DHCP (m) [DHCP Requested Lease Duration (min)]: esta configuración especifica el tiempo que el access point solicita para el alquiler de la dirección IP del servidor DHCP. Introduzca la cantidad de minutos que deberá solicitar el access point.
- Duración mínima del alquiler de DHCP (m) [DHCP Minimum Lease Duration (min)]: esta configuración especifica el tiempo más breve que el access point acepta un alquiler de dirección IP. El access point ignora alquileres más breves que este periodo. Introduzca la cantidad mínima de minutos que el access point deberá aceptar por un periodo de alquiler.

- Identificador de clase de DHCP [DHCP Class Identifier]: el servidor DHCP puede configurarse para enviar respuestas de acuerdo al grupo al cual pertenece un dispositivo. Utilice este campo para introducir el nombre del grupo del access point. El servidor DHCP utiliza el nombre del grupo para determinar la respuesta a enviar al access point. El identificador de clase de DHCP del access point es un identificador de clase del fabricante.

5.5.3 Servidor Web

Utilice la página Configuración del servidor Web [Web Server Setup] para llevar a cabo las siguientes tres funciones:

- Habilitar la navegación hacia el sistema de administración basado en la Web.
- Especificar la ubicación de los archivos de Ayuda del access point.
- Introducir configuraciones para un sistema personalizado para la administración del access point.

La página Configuración del servidor Web contiene las siguientes configuraciones:

- Permitir la navegación fuera de la consola [Allow Non-Console Browsing] – Seleccione Sí para permitir la navegación en el sistema de administración. Si se selecciona No, el sistema de administración es accesible únicamente a través de las interfaces de consola y Telnet.
- Puerto HTTP [HTTP Port] – Esta configuración determina el puerto a través del cual el access point otorga acceso a la Web. El Administrador del Sistema deberá poder recomendar una configuración de puerto.
- URL Raíz de Ayuda por Defecto [Default Help Root URL] – Esta entrada indica al access point dónde buscar archivos de ayuda. El botón Help de cada página del sistema de administración abre una nueva ventana del navegador que muestra la ayuda para dicha página. Los archivos de ayuda online son proporcionados en el CD del access point y del bridge, en el directorio Help. Los archivos de ayuda pueden encontrarse en cuatro ubicaciones posibles:
 - Internet – Cisco mantiene ayuda actualizada para los access points en el sitio Web de Cisco. Aunque esta ubicación requiere acceso online, ofrece la información más actualizada. Si se utiliza esta ubicación de la ayuda, no es necesario copiar los archivos desde el CD del access point y del bridge. La Internet es la ubicación por defecto de la ayuda.
 - Servidor de archivos – En redes multi-usuario, los archivos de ayuda pueden ubicarse en el servidor de archivos de la red. Para esta ubicación, introduzca el URL completo del directorio en el campo de entrada de URL raíz de ayuda por defecto [Default Help Root URL]. La entrada podría tener el siguiente aspecto:
[nombre sistema]\[directorio]\wireless\help
 - Unidad de CD-ROM – Para un acceso ocasional, el CD del access point puede dejarse en la unidad de CD-ROM, en la computadora que se utiliza para administrar la WLAN. Para esta ubicación, introduzca la letra de la unidad y la ruta en el campo de entrada Default Help Root URL. La entrada deberá tener el siguiente aspecto:
file:///[letra de la unidad de CD-ROM]:\Cisco\Help
 - Unidad de Disco Rígido – Los archivos de ayuda pueden copiarse en el disco rígido de la computadora utilizada para administrar la WLAN. Si se utiliza esta ubicación, introduzca todo el URL del directorio. La entrada podría tener el siguiente aspecto:
file:///[letra de la unidad]:\[carpeta o subdirectorio]\wireless\help
- Archivo de página Web extra [Extra Web Page File] – Para crear una alternativa al sistema de administración del AP, cree páginas HTML y cárguelas en el access point. Utilice este campo de entrada para especificar el nombre de archivo para la página HTML almacenada en el servidor de archivos. Haga clic en Cargar ahora [Load Now] para cargar la página HTML.
- URL Raíces de la Web por Defecto [Default Web Roots URL] – Esta configuración conduce a las páginas HTML del sistema de administración. Si se crean páginas HTML alternativas, cambie esta configuración para que conduzca a las páginas alternativas. La configuración por defecto es mfs0:/StdUI/.

5.5.4 Servidor de nombres

Utilice la página Configuración del servidor de nombres [Name Server Setup] para configurar el access point para que funcione junto con el servidor del Sistema de Nombres de Dominio (DNS) de la red.

Si la red utiliza un Sistema de Nombres de Dominio (DNS), seleccione Enabled (Habilitado) para indicarle al access point que utilice el sistema. Si la red no utiliza DNS, seleccione Disabled (Inhabilitado).

Introduzca el nombre del dominio IP por defecto para la red, en el campo de entrada. La entrada podría tener el siguiente aspecto:
mycompany.com

La línea Dominio actual [Current Domain] bajo el campo de entrada enumera el dominio que está sirviendo al access point. El dominio actual podría ser diferente al dominio del campo de entrada. Por ejemplo, un usuario puede configurar DHCP o BOOTP como Protocolo del servidor de configuración [Configuration Server Protocol] en la página Configuración del servidor de inicio [Boot Server Setup], pero seleccione No para la configuración "Use previous Configuration Server settings when no server responds?" ("¿Utilizar la configuración anterior del Servidor de Configuración cuando no responde ningún servidor?").

Servidores de nombre de dominio — Introduzca las direcciones IP de hasta tres servidores de nombre de dominio de la red. Las líneas actuales a la derecha de los campos de entrada enumeran los servidores que está utilizando actualmente el access point, que pueden ser especificados por el servidor DHCP o BOOTP.

Sufijo de dominio — En este campo de entrada, introduzca la porción del nombre de dominio completo que ha de omitirse desde las pantallas del access point. Por ejemplo, en el dominio mycompany.com, el nombre completo de una computadora podría ser mycomputer.mycompany.com. Con el sufijo de dominio configurado como mycompany.com, el nombre de la computadora se mostraría en las páginas del sistema de administración como mycomputer.

5.5.5 FTP

Utilice la página Configuración de FTP [FTP Setup] para asignar las configuraciones del Protocolo de Transferencia de Archivos (FTP) para el access point. Todas las transferencias de archivos que no se efectúan mediante el navegador son regidas por las configuraciones de esta página.

- File Transfer Protocol
- Default File Server
- FTP Directory
- FTP User Name
- FTP User Password

Figura 1

La página FTP Setup contiene las siguientes configuraciones 1:

- Protocolo de Transferencia de Archivos [File Transfer Protocol]: utilice el menú desplegable para seleccionar FTP o TFTP. El Protocolo de Transferencia de Archivos Trivial (TFTP) es un protocolo relativamente lento, de baja seguridad que no requiere ningún nombre de usuario ni password.
- Servidor de archivos por defecto [Default File Server]: introduzca la dirección IP o nombre DNS del servidor de archivos. Introduzca la dirección IP o nombre DNS del servidor de archivos. Aquí es donde el access point buscará archivos FTP.
- Directorio FTP [FTP Directory]: introduzca el directorio del servidor que contiene los archivos de imágenes del firmware.
- Nombre de usuario FTP [FTP User Name]: introduzca el nombre de usuario del servidor FTP. No es necesario introducir un nombre en este campo si TFTP es seleccionado como Protocolo de Transferencia de Archivos.
- Password de usuario FTP [FTP User Password]: introduzca la password asociada al nombre de usuario del servidor de archivos. No es necesario introducir una password en este campo, si se seleccionó TFTP como Protocolo de Transferencia de Archivos.

5.5.6 Enrutamiento

Utilice la página Configuración de Enrutamiento [Routing Setup] para configurar el access point para que se comunique con el sistema de enrutamiento de la red IP. Utilice las configuraciones de la página para especificar el gateway por defecto y para construir una lista de configuraciones de las rutas de red instaladas.

La página Routing Setup contiene las siguientes configuraciones:

- Gateway por defecto [Default Gateway] — Introduzca la dirección IP del gateway por defecto de la red en este campo de entrada. La entrada 255.255.255.255 indica que no hay ningún gateway.

- Configuraciones de las nuevas rutas de la red [New Network Route Settings] — Pueden definirse rutas de red adicionales para el access point. Para agregar una ruta a la lista de rutas instaladas, complete los tres campos de entrada y haga clic en Agregar [Add]. Para eliminar una ruta de la lista, resáltela y haga clic en Eliminar [Remove]. Los tres campos de entrada son los siguientes:
 - Red de destino [Dest Network] — Introduzca la dirección IP de la red de destino.
 - Gateway — Introduzca la dirección IP del gateway utilizado para llegar a la red de destino.
 - Máscara de subred [Subnet Mask] — Introduzca la máscara de subred asociada a la red de destino.
- Lista de rutas de red instaladas [Installed Network Routes list] — La lista de rutas instaladas proporciona la dirección IP de la red de destino, la dirección IP del gateway, y la máscara de subred para cada ruta instalada.

5.5.7 Configuración de consola y telnet

Utilice la página Configuración de consola/telnet [Console/Telnet Setup] para configurar el access point para que funcione con un emulador de terminal o Telnet.



Figura 1

La página Console/Telnet Setup contiene las siguientes configuraciones (Figura 1):

- Velocidad en baudios [Baud Rate]: la velocidad de la transmisión de datos expresada en bits por segundo (bps). Seleccione una velocidad de 110 a 115200 baudios, dependiendo de la capacidad de la computadora utilizada para abrir el sistema de administración del access point. La velocidad por defecto es 9600.
- Paridad [Parity]: éste es un proceso de detección de errores basado en la adición de un bit de paridad, para componer la cantidad total de bits pares o impares. La configuración por defecto, None (Ninguno), no utiliza ningún bit de paridad.
- Bits de datos [Data Bits]: la configuración por defecto para los bits de datos es 8.
- Bits de parada [Stop Bits]: la configuración por defecto para los bits de parada es 1.
- Control de flujo [Flow Control]: esto define la forma en la cual la información se envía entre dispositivos, para evitar la pérdida de datos, cuando llega demasiada información al mismo tiempo. La configuración por defecto es SW Xon/Xoff.
- Tipo de terminal [Terminal Type]: la configuración preferida es ANSI, que ofrece funciones gráficas tales como botones de retroceso de video y enlaces subrayados. No todos los emuladores de terminal soportan ANSI, por lo cual la configuración por defecto es Teletype.
- Columnas [Columns]: define el ancho de la pantalla del emulador de terminal, dentro del rango de 64 a 132 caracteres. Ajuste el valor para obtener la pantalla óptima para el emulador de terminal.
- Líneas [Lines]: define la altura de la pantalla del emulador de terminal, dentro del rango de 16 a 50 caracteres. Ajuste el valor para obtener la pantalla óptima para el emulador de terminal.
- Habilitar Telnet [Enable Telnet]: la configuración por defecto es Sí. Seleccione No para evitar el acceso por Telnet al sistema de administración.

Resumen

Se dispone de una variedad de herramientas para configurar un access point (AP). El navegador Web usualmente es la forma más fácil de configurar un AP. Algunas instalaciones utilizarán extensamente SNMP. El AP 1100 utiliza el Cisco IOS para la configuración. Futuros APs también soportarán al Cisco IOS. Tal como las actividades y laboratorios lo han demostrado, es importante mantener simple la configuración, hasta no haber logrado la conectividad. Cada función puede sumarse a la complejidad total y hacer que la detección de problemas consuma más tiempo.

Módulo 6: Puentes

Descripción general

Este módulo trata los bridges inalámbricos como medio de conectar LANs. Los bridges se utilizan para conectar dos o más LANs cableadas para crear una única LAN grande. Se tratarán los seis roles que desempeñan los bridges en las redes inalámbricas. Además, se examinarán las consideraciones acerca de la instalación, incluyendo la pérdida de la ruta, la distancia y la velocidad de datos deseada. Puesto que el bridge es un dispositivo de radio, es susceptible a causas comunes de interferencia que pueden reducir el throughput y el alcance. Al configurar un bridge deben tenerse en cuenta ciertas precauciones.

Este módulo proporcionará a los alumnos la oportunidad de configurar un bridge y experiencia en la configuración de Ethernet y de los puertos de radio de un bridge. A continuación, el módulo tratará cómo se configuran y administran los servicios de tiempo, nombre, inicio y enrutamiento.

Mediante el uso de las actividades prácticas que acompañan este módulo, el alumno desarrollará una comprensión de la configuración inicial del bridge, la configuración de servicios y cómo deberán administrarse los archivos de configuración.

6.1 Bridges Inalámbricos

6.1.1 Definición del bridging inalámbrico

Los bridges se utilizan para conectar dos o más LANs cableadas, para crear una única LAN grande. Las LANs se encuentran usualmente dentro de edificios separados, como lo ilustra la Figura 1. Un bridge puede actuar como access point en algunas aplicaciones, comunicándose con los clientes de los sitios remotos. Esto se logra mediante el Bridge de Grupos de Trabajo (WGB) de Cisco.

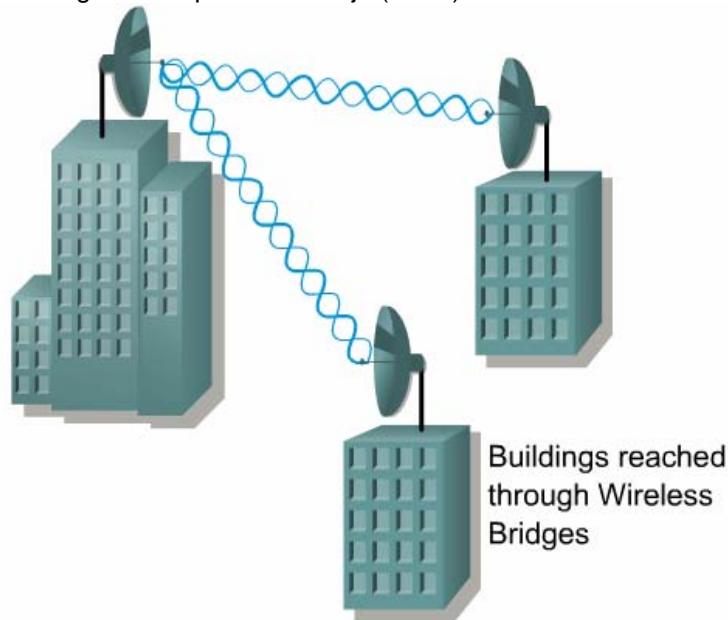


Figura 1

Los bridges Cisco Aironet operan en la capa de enlace de datos OSI, que en ocasiones se denomina capa de dirección MAC. Esto significa que los bridges no tienen capacidad de enrutamiento. Si se requiere división en subredes IP, debe colocarse un router dentro de la red.

El bridging se ha convertido rápidamente en uno de los usos más populares de las redes inalámbricas. Esto se debe parcialmente a su facilidad de instalación y configuración. También se debe a la variedad de mercados emergentes, a los cuales puede aplicarse el bridging WLAN. Tal como lo muestra la Figura 2, algunos de estos mercados incluyen los siguientes:

- Entornos de campus, como hospitales, escuelas, universidades y corporaciones
- Áreas donde la geografía puede excluir otras soluciones
- Instalaciones de red temporales
- Proveedores de servicios de Internet (ISPs)

- Conexiones de respaldo o alternativas
- Países en vías de desarrollo, donde soluciones alternativas pueden no estar disponibles
- Mercados internacionales

Wireless building-to-building bridges connect separate LANs at high speed
 No tariff, no recurring fee
 E1, T1 alternative
 High-speed internet access (ISP)
 Educational campuses
 International markets
 Developing countries
 Alternative to wired data infrastructure
 Rapid deployment with lower cost

Figura 2

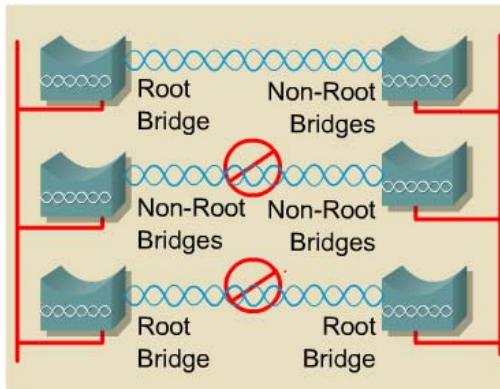
6.1.2 Roles que desempeña un bridge en una red

Los bridges multi-función Cisco Aironet pueden configurarse para operar en muchos modos diferentes. Ésta es la función del parámetro Raíz [Root].

Los access points y bridges Cisco Aironet utilizan la misma radio. El bridge multi-función Cisco Aironet tiene la misma sensibilidad receptora, niveles de energía y capacidades que el access point Cisco Aironet. Esto significa que mientras está operando en modo AP, el bridge multi-función Cisco Aironet puede configurarse como access point completamente compatible con IEEE 802.11, que soportará a los clientes inalámbricos Cisco Aironet.

Un único bridge padre puede soportar a numerosos bridges hijos. En teoría, la cantidad máxima de bridges hijos que podrían soportarse es 2007. La cantidad de bridges hijos que deberán conectarse realmente a un bridge padre está determinada por las necesidades de uso y throughput.

Las Figuras 1- 2 ilustran y describen las opciones de comunicación entre bridges raíz y no raíz.



Root Bridge (Parent):

- Accepts associations and communicates with Non-Root Bridge (child) devices
- Will not communicate with other Root Bridge devices
- Communicates with multiple Non-Root bridges

Non Root (Child):

- Can associate and communicate with Root devices or Clients
- Will not communicate with other Non-Root devices
 - Unless other Non-Root device is communicating with a parent

Figura 1

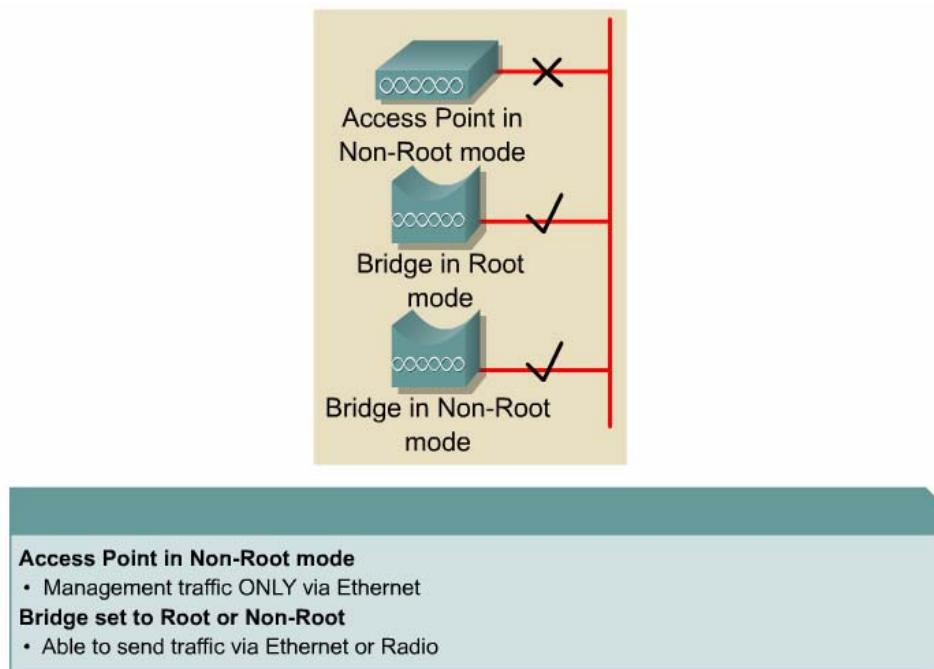
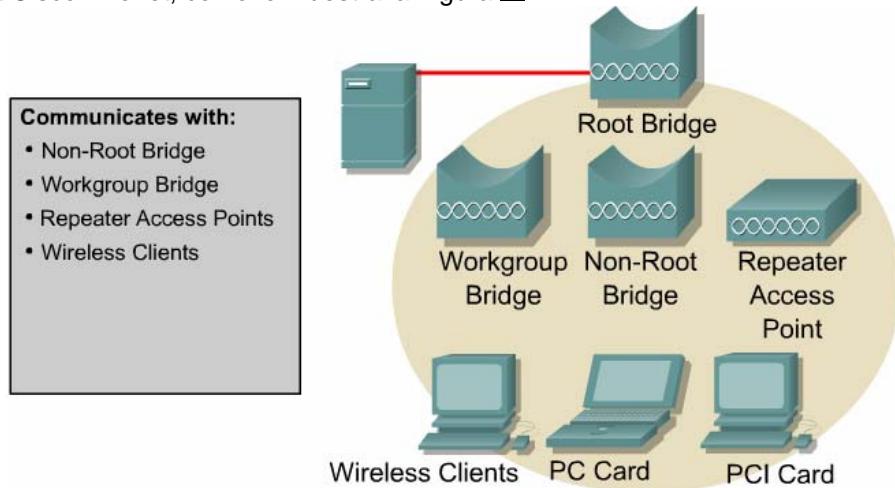


Figura 2

Ya sea que esté configurado como dispositivo raíz o no raíz, un bridge siempre puede comunicarse con otros bridges a través de la RF. El bridge se comunica con la red cableada a través del puerto Ethernet. Incluso cuando se lo configura para operar en modo access point, el bridge aún puede pasar tráfico de la red a través de RF y de puertos Ethernet. Ésta es una de las diferencias principales entre un bridge y un access point Cisco Aironet, como lo muestra la Figura 3.



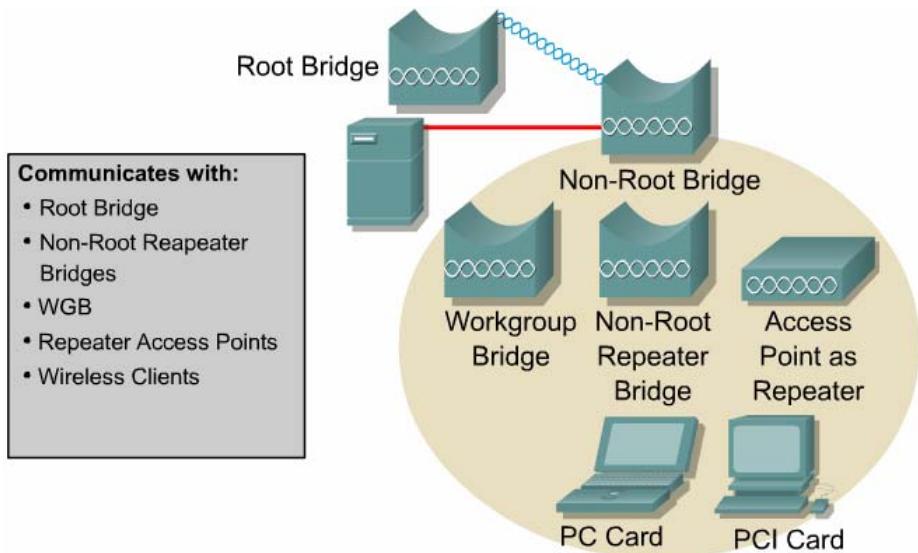
This is the bridge that is connected to the main network. This bridge would be used to provide connectivity to the main LAN, for other wireless clients. Only one bridge in a WLAN can be set as the root bridge. This is the default setting for Cisco Aironet bridges.

Figura 3

Existen seis opciones para configurar el estado de raíz y parámetros relacionados. Estas opciones corresponden a los siguientes seis roles, que un bridge puede asumir en una LAN:

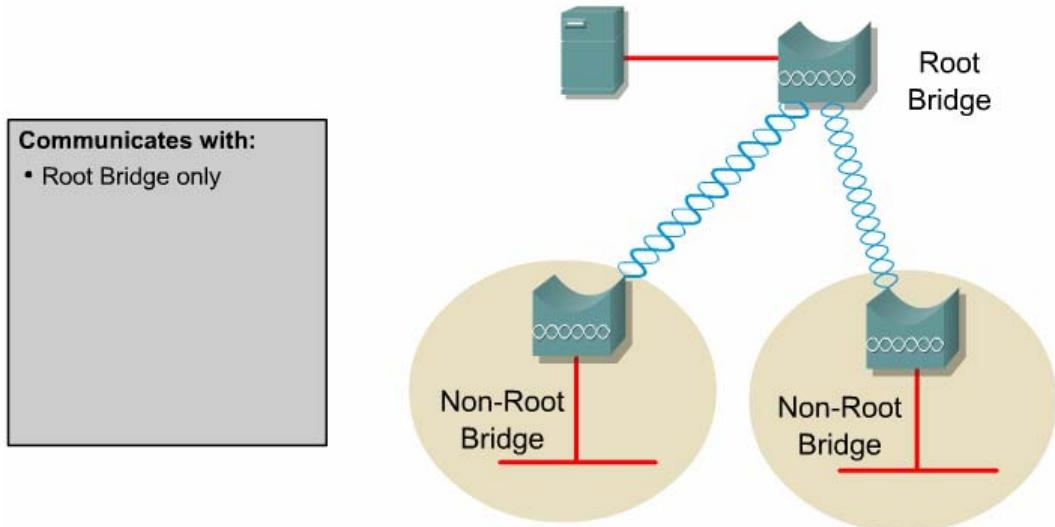
- Bridge raíz
- Bridge no raíz con clientes
- Bridge no raíz sin clientes
- Access point raíz
- Access point repetidor
- Cliente de estudio del sitio

Estos seis roles del bridge se describen brevemente en las Figuras 4 a 9.



This setting is used for any wireless bridges that will be connecting to a root bridge, either directly or through a repeater bridge or access point. When used as a repeater bridge, traffic is passed from associated wireless clients, to another non-root or root bridge. In order for wireless clients to attach to a non-root bridge, the bridge must be associated with a root bridge, or with another non-root bridge that is associated with a root bridge.

Figura 4



This mode would be used for a bridge that is used to connect a remote wired LAN. It will only communicate with a root bridge. In this mode, the bridge will refuse associations from wireless clients.

Figura 5

Rugged AP



Aironet 350

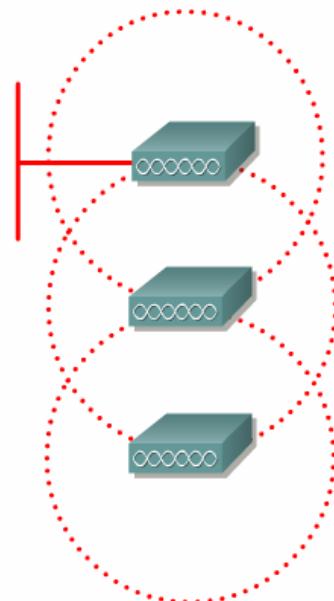
- Same functionality as Cisco Aironet Access Point
- Supports all wireless clients

When configured as a root access point, the Cisco Aironet 350 Bridge offers the exact same functionality as the Cisco Aironet Rugged AP. In this mode, the bridge will pass traffic between the wired LAN and wireless clients.

Figura 6

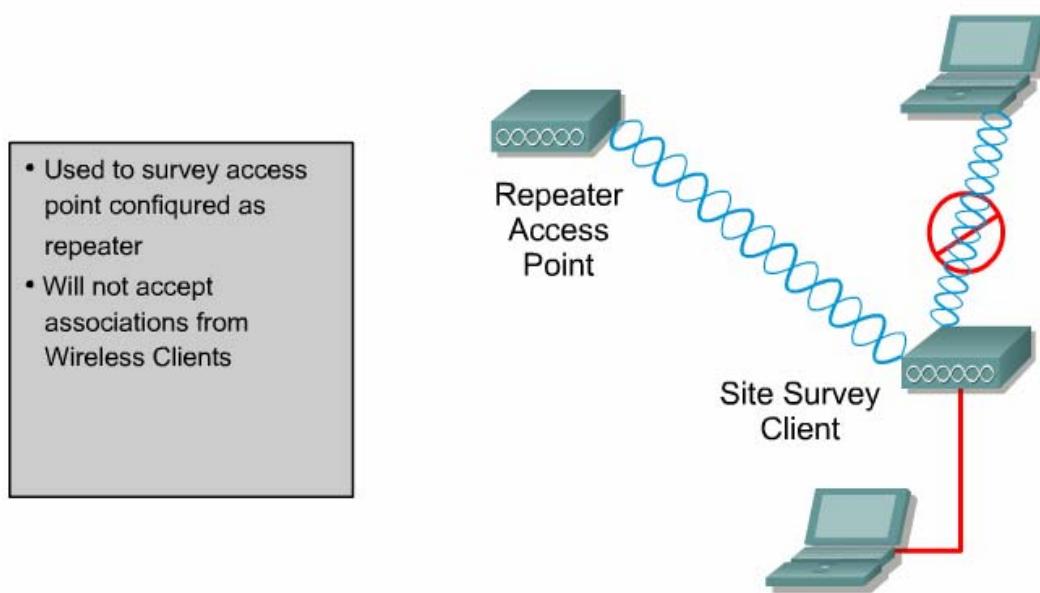
Connects to:

- Root Bridges
- Non-Root bridges
- Root access points
- Other repeater access points
- Repeaters are not covered by 802.11 standards



In this mode, the bridge will operate with the same functionality as a Cisco Aironet AP in repeater mode. The bridge will only pass management traffic, and will not pass WLAN client traffic, through the Ethernet port.

Figura 7



The bridge can be configured as a site survey client for surveying a repeater access point. While in this mode, the bridge can connect to another bridge or access point, but will not accept associations from wireless clients.

Figura 8

6.1.3 Consideraciones respecto a la instalación

Al planificar la implementación de un bridge inalámbrico, debe tenerse cuidado de seleccionar los mejores productos. Las cuestiones a considerar incluyen las siguientes:

- Las funciones de un bridge, como el protocolo spanning-tree o el soporte para VLAN
- Distancia y velocidad de datos necesarias
- Antenas opcionales, para incrementar la distancia
- Consideraciones sobre el exterior, como disipador de rayos
- Sellado de las conexiones coax

Consideraciones típicas para los bridges incluyen la distancia que cubrirán, la velocidad a la cual operarán y la cantidad de usuarios que pueden soportar. Un factor muy engañoso es la velocidad de datos. Como sucede con los sistemas LAN, la velocidad de datos indica cuán rápidamente pasa datos la RF. Estos datos sobre la RF incluyen la sobrecarga del sistema de radio y los datos de la red. El elemento real que deberá tratarse es el throughput. Ésta es la cantidad real de datos de la red que pasa de una LAN a otra. Recordemos que una velocidad de datos elevada no significa un throughput más alto.

Cisco Aironet Bridge		How Fast?	
		11 Mbps	2 Mbps
Max data rate		11 Mbps	2 Mbps
Typical throughput		5.5 Mbps	1.4 Mbps
How Far?			
Yagi antenna		3.63 Miles 5.8 Km	7.26 miles 11.7 Km
Dish antenna		20.52 Miles 33 Km	25+ miles 40+ Km

Figura 1

La velocidad de datos de los bridges inalámbricos puede configurarse a velocidades de 1, 2, 5,5, y 11 Mbps. Reducir la velocidad incrementa la distancia máxima que puede obtenerse, a la vez que el incremento de la velocidad baja la distancia máxima ¹. El filtrado puede incrementar el desempeño real a través de la RF eliminando el tráfico innecesario. Esto tiene el mismo efecto que incrementar el throughput. La cantidad de

usuarios que puede soportar el bridge depende del tipo de tráfico que se está manipulando. El throughput es el factor limitante real.

Otra consideración que puede afectar la distancia y las velocidades de datos es la elección de la antena. Cisco ofrece varias antenas direccionales de largo alcance. La Yagi es una antena pequeña, de 46 x 8 cm (18 x 3 pulgadas), y liviana, de 0,68 kg (1,5 libras), que puede utilizarse para un alcance de hasta 11,7 km (7,62 millas) a 2 Mbps, y de hasta 5,8 km (3,63 millas) a 11 Mbps. La parabólica sólida es la mejor antena parabólica estructural del mercado. Soportará congelamiento y vientos de más de 117 kilómetros por hora (110 millas por hora). Permitirá una operación de 2 Mbps para hasta 40 km (25 millas) y una operación de 11 Mbps para hasta 33 km (20,52 millas) [2](#), [3](#).

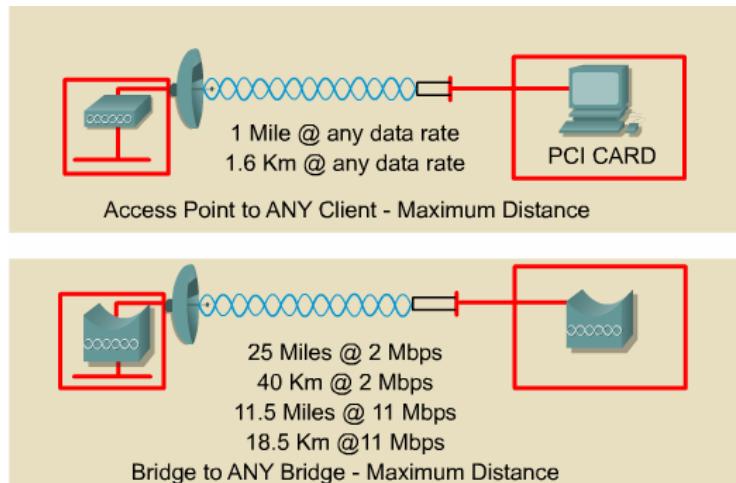


Figura 2

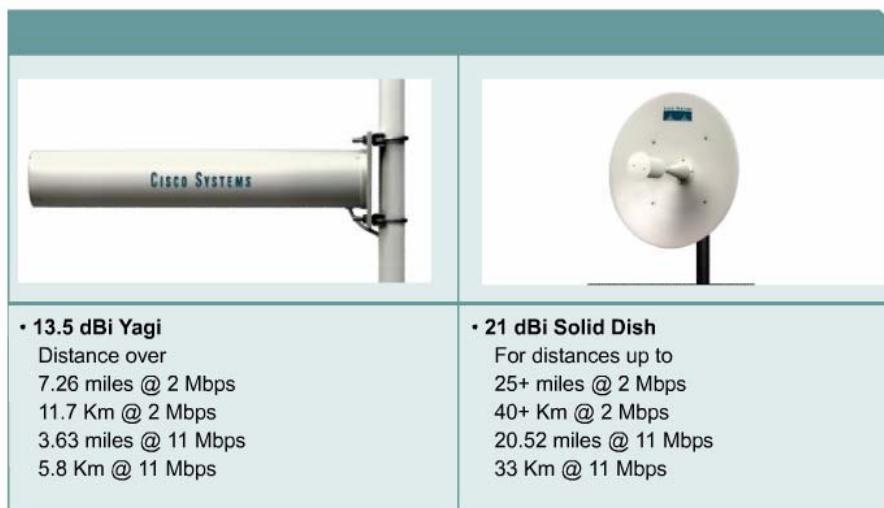
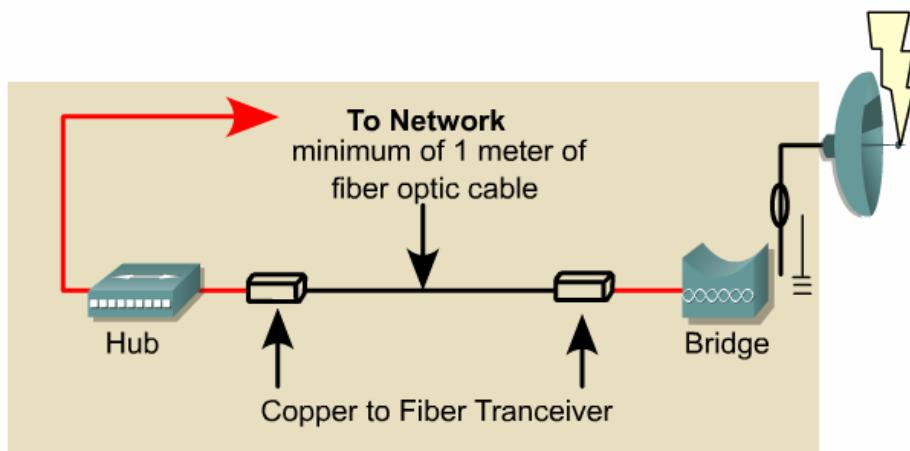


Figura 3

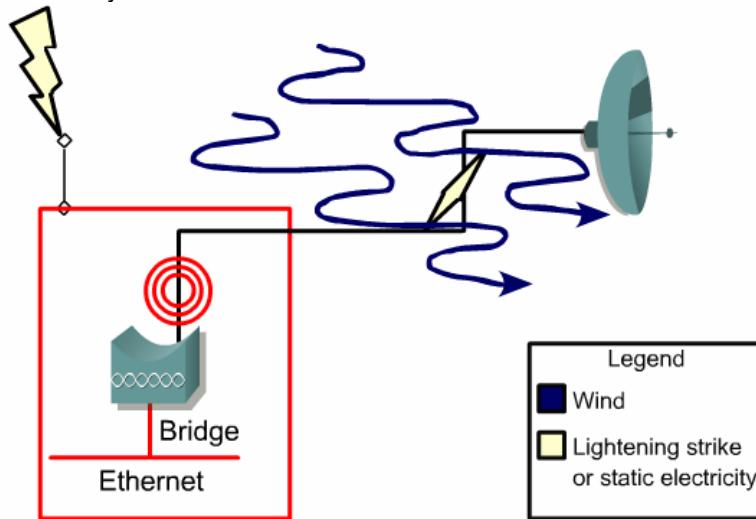
Cuando una antena se instala fuera del edificio, existe la posibilidad de que pudiera ser golpeada por un rayo. A causa del extremo voltaje asociado a la caída de un rayo, la corriente podría viajar hacia la red, utilizando la antena, el cable de extensión y el cable Cat 5 como ruta. Una vez que la corriente se encuentra en el cable Cat 5, podría viajar a través de toda la red y dañar cualquier equipamiento conectado al cable. La mejor protección contra la caída directa de un rayo es el cableado de fibra óptica. El disipador de rayos Cisco Aironet no detendrá la caída directa de un rayo. Puesto que el conductor del cableado de fibra óptica es el vidrio, la corriente no puede viajar a través de la fibra. La energía se disipa en forma de calor y derrite el cableado de fibra óptica [4](#).

**Protection from a direct strike**

- 1 meter fiber optic cabling
- Electricity will not travel over fiber
- Transceivers require power

Figura 4

El rayo no necesita caer directamente encima para ocasionar problemas. Una caída indirecta puede inducir la suficiente energía en el cable y las antenas como para ocasionar daños al bridge y a otros dispositivos de la red. Un disipador de rayos puede ser de ayuda en estos casos. Éste tiene dos propósitos principales. Uno de ellos es eliminar cualquier carga de estática elevada que sea recolectada por la antena. Esto evitará que la antena atraiga la caída de un rayo. El segundo propósito es disipar cualquier energía inducida hacia la antena o coax desde la caída de un rayo en las cercanías ⁵.

**Static Electricity**

- Wind
- Nearby Strikes

Figura 5

También es necesario sellar los conectores de coax. Esto tiene como objeto evitar que el agua entre a los conectores. Si el agua entra a los conectores, se abrirá camino hacia el coax, contaminándolo y volviéndolo inutilizable.

6.1.4 Consideraciones acerca de la distancia y la pérdida de las rutas

Al planificar la implementación de un bridge inalámbrico, es importante lograr el equilibrio óptimo entre costo, disponibilidad, distancia y velocidad de datos. Esto se ilustra en la Figura 1. Pueden efectuarse cálculos para proporcionar una información precisa acerca de estos factores.

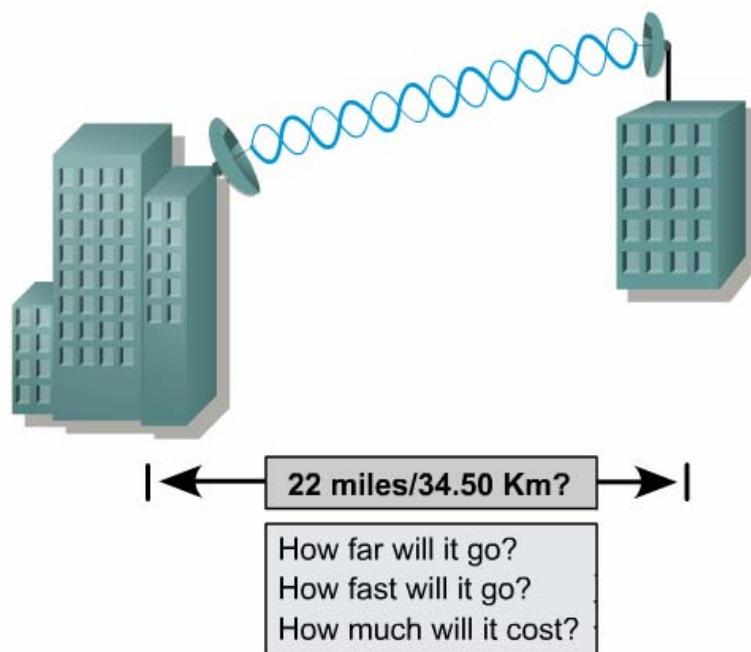


Figura 1

La pérdida de la ruta determina cuán lejos viajará una señal sin dejar de proporcionar comunicaciones confiables. Los cálculos se miden en dB. Los valores pueden derivarse del modelo teórico.

El margen determina cuánta interferencia en la ruta puede insertarse manteniéndose aún las comunicaciones. Un margen de debilitamiento de 10 dB se requiere para que existan comunicaciones confiables en todas las condiciones climáticas.

Si el caso de bridging ilustrado en la Figura 2 se estuviera planificando, ¿funcionaría el sistema según se indica? Utilizando cálculos de pérdida de ruta, ganancias de la antena y la longitud de los cables, las distancias pueden, teóricamente, verificarse. Esto permite cambios en el diseño antes de la instalación, basándose en estos cálculos.

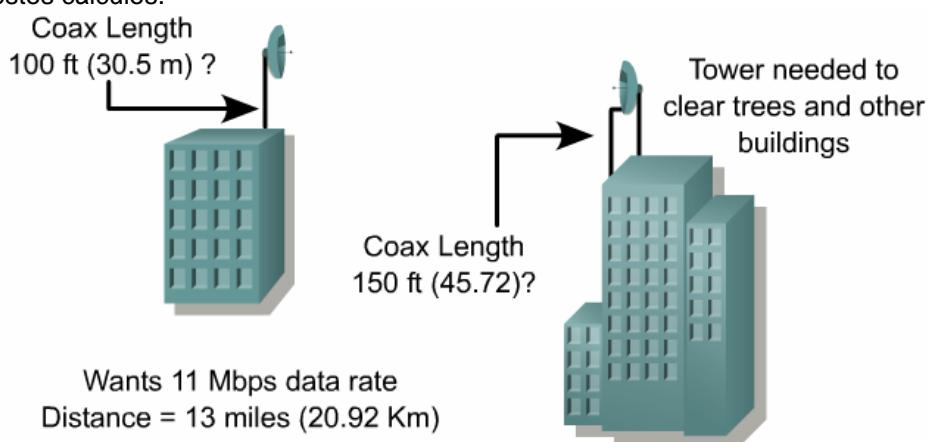


Figura 2

Cisco ofrece el utilitario para el Cálculo del Alcance del Bridge en Exteriores Cisco Aironet [Cisco Aironet Outdoor Bridge Range Calculation]. Este utilitario es una planilla de cálculos que contiene las fórmulas necesarias para calcular cuán lejos puede llegar un enlace de bridge propuesto. Puede descargarse desde Cisco Connection Online (CCO).

6.2 Configuración Básica

6.2.1 Precauciones

Puesto que el bridge es un dispositivo de radio, es susceptible a causas comunes de interferencia que pueden reducir el throughput y el alcance. Las siguientes precauciones pueden ayudar a asegurar el mejor desempeño posible:

- Instale la antena del bridge en un área donde los árboles, edificios o grandes estructuras de acero como estanterías, bibliotecas, y gabinetes archivadores no obstruyan las señales de radio hacia y desde la antena. Las antenas deben ubicarse de modo tal que se permita una operación de línea de visión directa.
- Minimice la distancia entre el bridge y la antena para reducir la pérdida de la señal.
- Instale el bridge lejos de hornos a microondas u otros dispositivos que operen en el rango de frecuencia de los 2,4 GHz. Los hornos a microondas operan en la misma frecuencia que el bridge y pueden ocasionar una interferencia en la señal.
- Repase todas las precauciones y advertencias de los materiales de instalación.

El bridge proporciona dos conectores de antena TNC inversos en la parte posterior de la unidad. Estos conectores tienen como objeto configuraciones de diversidad con dos antenas. Cuando se utiliza una única antena, conecte la antena al conector principal, que está ubicado a la derecha. Refiérase a la actividad Photozoom que figura más abajo para obtener información adicional.

El bridge serie 350 recibe energía a través del cable Ethernet. Las opciones de alimentación del bridge serie 350 incluyen:

1. Un switch con energía de línea entrante, como un Cisco Catalyst 3524-PWR-XL
2. Un patch panel con energía de línea entrante, como un Patch Panel Cisco Catalyst Inline Power
3. Un inyector de energía Cisco Aironet

La Figura 1 muestra las tres opciones de energía para el bridge.

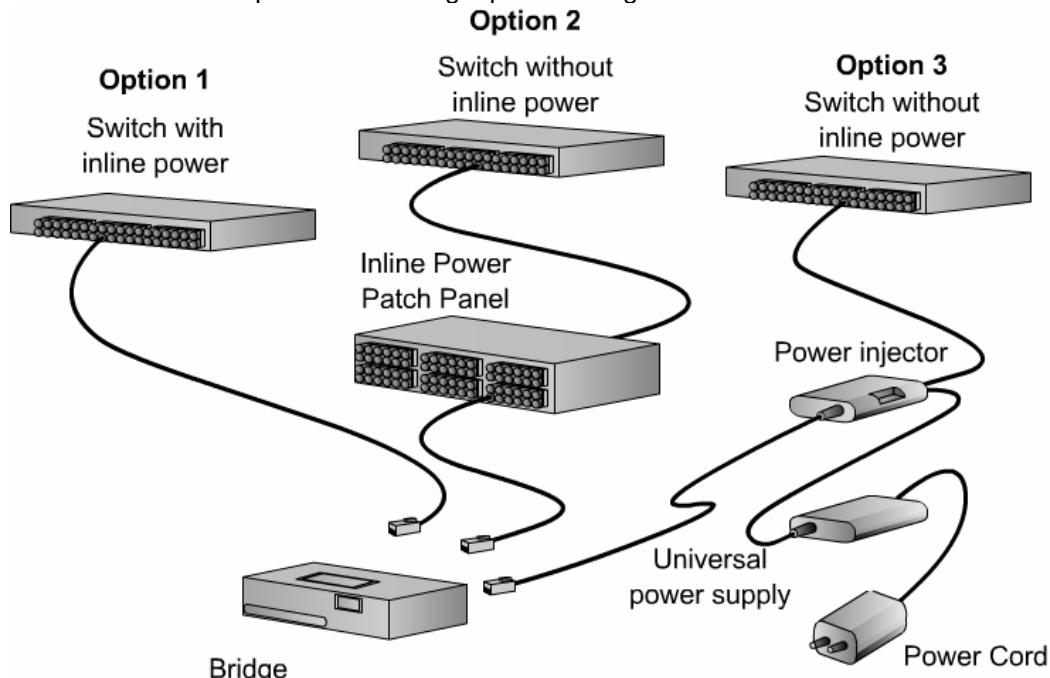


Figura 1

6.2.2 Conexión al bridge

Antes de configurar el bridge, el administrador de la red debe facilitar la siguiente información:

- El identificador del conjunto de servicios (SSID) que se utilizará para identificar la WLAN
- Un nombre de sistema para el bridge que describa la ubicación o usuarios principales del bridge
- Una dirección IP para el bridge si la red no utiliza DHCP para asignar direcciones IP
- Un gateway por defecto y una máscara de subred IP para el bridge si la red utiliza subredes
- La dirección MAC para el bridge, que está impresa en la etiqueta de la parte inferior del bridge y que identifica exclusivamente al bridge de la WLAN

Interfaces de administración

Una vez registrada esta información, existen tres opciones básicas para la configuración:

1. La interfaz del navegador de la Web
2. La interfaz de la línea de comandos (CLI), que utiliza un emulador de terminal o una sesión de Telnet
3. Una aplicación del Protocolo de Administración de Red Simple (SNMP)

Las páginas Web del sistema de administración del bridge están organizadas de la misma manera para el navegador de la Web que para la interfaz de la línea de comandos. Este módulo se concentrará en la interfaz del navegador de la Web.

Siga estos pasos para utilizar la interfaz del navegador de la Web:

1. Inicie el navegador. Introduzca la dirección IP del bridge en el campo Location del navegador si utiliza Netscape Communicator, o en el campo Dirección si utiliza Internet Explorer, y presione Enter.
2. Si el bridge no ha sido configurado todavía, la página Configuración Rápida [Express Setup] aparece según se muestra en la Figura 1. Si el bridge ha sido configurado, aparece la página Resumen de Estado. La página Resumen de Estado también se conoce como página Home o de Inicio.

Un ejemplo de página de la configuración en la CLI se muestra en la Figura 2.

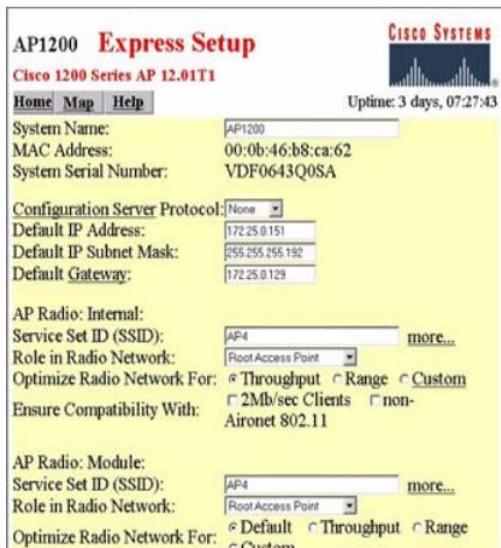


Figura 1

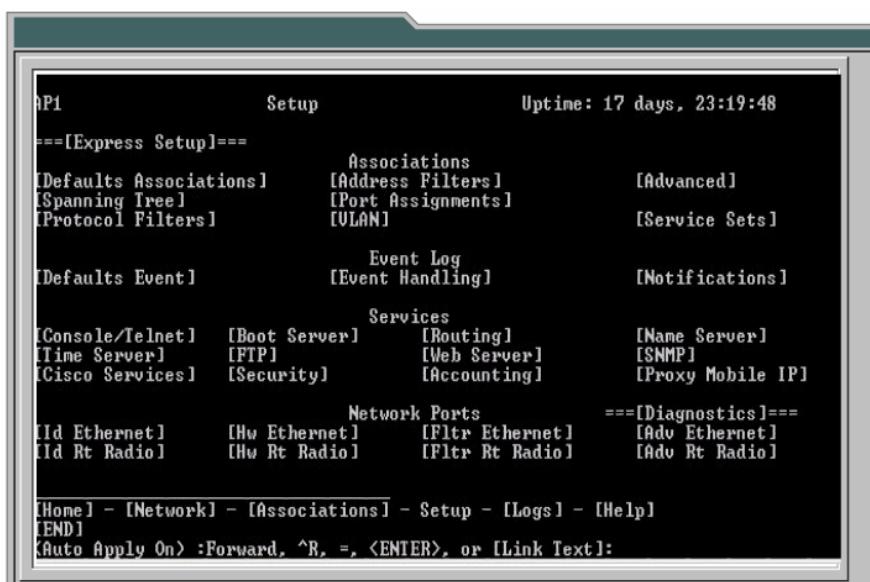


Figura 2

6.2.3 Configuración de la dirección IP y el SSID para el bridge

Para configurar inicialmente el bridge pueden utilizarse cuatro métodos:

1. Configuración remota utilizando una computadora que se comunique con el bridge mediante un AP Cisco. La computadora utilizada para la configuración debe encontrarse en la misma subred que el bridge.
2. Utilizar una computadora de la LAN cableada para comunicarse con el bridge a través de un hub de la LAN cableada. IPSU debe estar instalado en una computadora que se encuentre en la misma subred que el bridge.
3. Utilizar una computadora no conectada a una red para comunicarse directamente con el bridge a través de un cable cruzado. IPSU debe estar instalado en la computadora, así como en la misma subred que el bridge.
4. Utilizar un cable consola y configurar el bridge a través de la línea de comandos.

Si el bridge no recibe una dirección IP de un servidor DHCP, o la dirección IP por defecto ha de ser cambiada, utilice IPSU para asignar una dirección IP. El SSID para el bridge puede configurarse al mismo tiempo, como se muestra en la Figura 1.

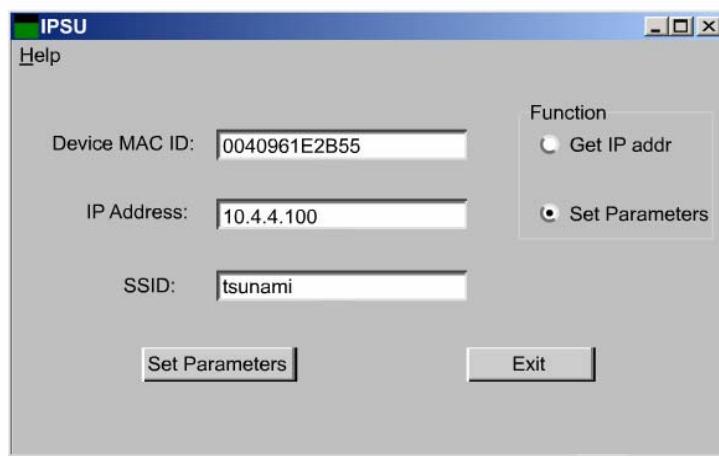


Figura 1

La computadora utilizada para asignar una dirección IP al bridge debe tener una dirección IP propia. IPSU sólo puede cambiar la dirección IP y el SSID en el bridge a partir de sus configuraciones por defecto. Una vez que la dirección IP y el SSID se han cambiado, IPSU no puede cambiarlos nuevamente hasta no haber mantenido presionado el botón Mode (Modo). Esto reiniciará la configuración según los valores por defecto de fábrica.

Siga los pasos de la Figura 2 para asignar una dirección IP y un SSID al bridge.

Assigning an IP Address and SSID

Step 1 Double-click the **IPSU** icon on the computer desktop to start the utility.
Step 2 Click the **Set Parameters** radio button in the **Function** box, as shown in Figure [1].
Step 3 Enter the MAC address for the bridge in the **Device MAC ID** field. The MAC address for the bridge is printed on a label, on the bottom of the unit. It should contain six pairs of hexadecimal digits. The **Device MAC ID** field is not case-sensitive.
Step 4 Enter the IP address that is to be assigned to the bridge in the **IP Address** field.
Step 5 Enter the SSID that is to be assigned to the bridge in the **SSID** field. The SSID cannot be set without also setting the IP address. However, the IP address can be set without setting the SSID.

Figura 2

6.2.4 Introducción de la configuración básica mediante configuración rápida

La página Configuración Rápida [Express Setup] se utiliza para asignar configuraciones básicas al bridge. La configuración de los puertos y servicios de radio y Ethernet se tratarán posteriormente en este módulo. Información acerca de la configuración de la seguridad, el filtrado y otras funciones del bridge se tratarán en módulos posteriores. Refiérase a la Guía de Configuración del Software del Bridge [Bridge Software Configuration Guide] del Cisco Aironet Serie 350 que se encuentra en el CD del bridge para obtener información detallada acerca de la configuración.

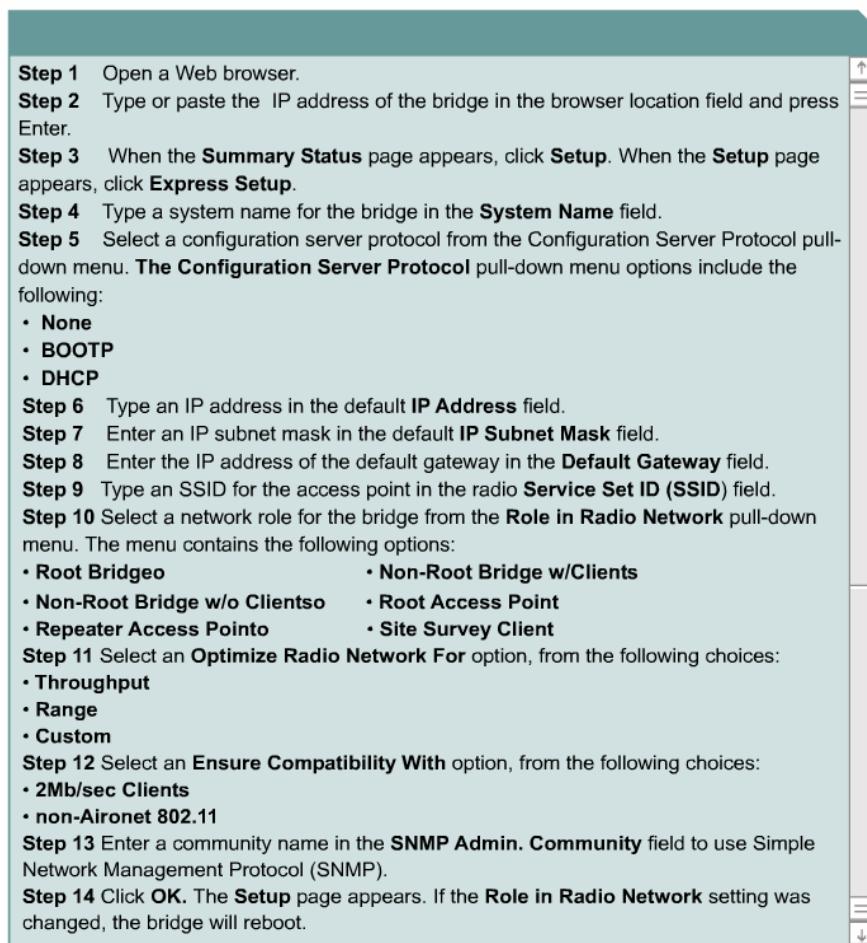


Figura 1

Siga los pasos de la Figura 1 para introducir la configuración básica del bridge utilizando un navegador Web. Si utiliza Netscape Communicator, introduzca la dirección IP en el campo Netsite o Location. Si utiliza Microsoft Internet Explorer, introduzca la dirección IP en el campo Dirección.

La página Express Setup para el Bridge Cisco Aironet 350 se muestra en la Figura 2. Éste es el menú de la página Web por defecto para el bridge cuando se lo enciende por primera vez. Seguirá siendo la página por defecto hasta que no se haya introducido con éxito una configuración y el usuario haya hecho clic en Aplicar o Aceptar.

La configuración del bridge por defecto se muestra en la Figura 3.

BR350 Express Setup	
Cisco 350 Series Bridge	
Home Map Help	
System Name: <input type="text" value="BR360"/> MAC Address: <input type="text" value="00:40:96:31:55:c1"/>	
Configuration Server Protocol: <input type="button" value="None"/> <input type="button" value="10.84.137.48"/> <input type="button" value="256.255.256.192"/> <input type="button" value="10.84.137.1"/>	
Default IP Adress: <input type="text" value="10.84.137.48"/> Default IP Subnet Mask: <input type="text" value="256.255.256.192"/> Default Gateway: <input type="text" value="10.84.137.1"/>	
Radio Service Set ID (SSID): <input type="text" value="tsunami"/> Roll in Radio Network: <input type="button" value="Root Bridge"/> Optimize Radio Network For: <input checked="" type="radio" value="Throughput"/> <input type="radio" value="Range"/> <input type="radio" value="Custom"/> Ensure Compatibility With: <input type="checkbox" value="2Mb/sec Clients"/> <input type="checkbox" value="non-Aironet 802.11"/>	
SNMP Admin. Community: <input type="text"/> <input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Restore Default"/>	

Figura 2

Setting Name	Default Value
System Name	AIR-BR350_xxxxxx, x = the last six characters of the MAC address
Terminal Type (Console interface only)	Teletype
Config Server Protocol	DHCP
IP Subnet Mask	10.0.0.1
IP address	255.255.255.0
Default Gateway	255.255.255.255
SSID	Tsunami
Role in Radio Network	Root Bridge
Optimize Radio Network For	Throughput
Ensure Compatibility With	(not configured)
SNMP Admin. Community	(not configured)

Figura 3

6.3 Configuración de los Puertos de Radio y Ethernet

6.3.1 Configuración básica del puerto de radio

Esta sección describe cómo configurar la radio del bridge. Utilice las páginas Radio Raíz [Root Radio] del sistema de administración para establecer la configuración de radio. Las páginas Root Radio incluyen las siguientes:

- Identificación de Radio Raíz [Root Radio Identification]: contiene la información básica acerca de la ubicación y la identidad para el puerto de radio del bridge.
- Hardware de Radio Raíz [Root Radio Hardware]: contiene configuraciones para el SSID, velocidades de datos, potencia de transmisión, antenas, canal de radio y umbrales operativos del bridge.
- Radio Raíz Avanzada [Root Radio Advanced]: contiene configuraciones para el estado operativo del puerto de radio. Esta página también puede utilizarse para efectuar cambios temporales en el estado del puerto, para ayudar a detectar problemas en la red.

Siga estos pasos para llegar a la página Identificación de Radio Raíz:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Configuración [Setup], haga clic en Identificación [Identification] en la fila Radio Raíz [Root Radio], bajo Puertos de la Red [Network Ports].

La página Identificación de Radio Raíz se utiliza para introducir información de ubicación e identidad para la radio del bridge. La Figura 1 muestra la página de Identificación de Radio Raíz.

The screenshot shows the 'Identification' configuration page for a Cisco Root Radio. At the top right, it displays 'Uptime: 3 days, 17:03:45'. The main area contains the following fields:

Primary Port?	<input type="radio"/> yes <input checked="" type="radio"/> no <input type="radio"/> Adopt Primary Port Identity?	<input checked="" type="radio"/> yes <input type="radio"/> no
MAC Address:	0040:96:40:16:B1	
Default IP Address:	10.0.0.2	
Default IP Subnet Mask:	255.255.255.0	
Current IP Address:	192.168.147.47	
Current IP Subnet Mask:	256.255.255.0	
Maximum Packet Data Length:	2304	
Service Set ID (SSID):	GJOLEAP	
LEAP User Name:	<input type="text"/>	
LEAP Password:	<input type="password"/> more...	
Firmware Version:	4.99.68	
Boot Block Version:	1.50	

At the bottom are four buttons: Apply, OK, Cancel, and Restore Default.

Figura 1

Configuraciones de la Página de Identificación de Radio Raíz

Las siguientes configuraciones pueden cambiarse en la página de Identificación de Radio Raíz:

- Configuraciones de Puerto Principal [Primary Port Configurations]: dos opciones permiten la designación del puerto de radio como puerto principal del bridge:
 1. ¿Puerto Principal? [Primary Port?] El puerto principal determina las direcciones MAC e IP del bridge. El puerto principal por defecto del bridge es el puerto Ethernet. El puerto Ethernet se conecta a la LAN cableada, por lo cual esta configuración se configura usualmente como no. Seleccione no para configurar el puerto Ethernet como puerto principal. Seleccione sí [yes] para configurar el puerto de radio como puerto principal.
 2. ¿Adoptar Identidad de Puerto Principal? [Adopt Primary Port Identity?] Seleccione sí para adoptar las direcciones MAC e IP del puerto principal para el puerto de radio. Seleccione no para utilizar direcciones MAC e IP diferentes para el puerto de radio. Los bridges que actúan como unidades de raíz adoptan las configuraciones de puerto principal para el puerto de radio. Cuando se coloca un bridge en modo de espera, seleccione no para esta configuración. Algunas configuraciones de bridge inalámbricos avanzadas también requieren diferentes configuraciones de identidad para el puerto de radio.
- Dirección IP por Defecto [Default IP Address]: utilice esta configuración para asignar una dirección IP para el puerto de radio que sea diferente de la dirección IP Ethernet del bridge. Por ejemplo, cuando el bridge se encuentra en modo de espera. Durante la operación normal, el puerto de radio adopta la identidad del puerto Ethernet.
- Máscara de Subred IP por Defecto [Default IP Subnet Mask]: introduzca una máscara de subred IP para identificar la subred para que la dirección IP pueda ser reconocida en la LAN. Si ni DHCP ni BOOTP están habilitados, este campo es la máscara de subred utilizada. Si DHCP o BOOTP están habilitados, este campo proporciona la máscara de subred, pero sólo si ningún servidor responde a la solicitud efectuada por el bridge.
- ID de Configuración del Servicio [Service Set ID] (SSID): un SSID es un identificador único que los dispositivos clientes utilizan para asociarse con el bridge. Los SSIDs ayudan a los dispositivos clientes a distinguir entre múltiples redes inalámbricas cercanas y proporcionan acceso a las VLANs a través de dispositivos clientes inalámbricos. Varios bridges de una red o subred pueden compartir un SSID. Pueden configurarse hasta 16 SSIDs en un bridge. Un SSID puede ser cualquier entrada alfanumérica, sensible al uso de mayúsculas de dos a 32 caracteres de longitud. Haga clic en Más... [More...] para dirigirse a la página de Configuraciones de Servicios de Radio Raíz [Root Radio Service Sets], donde pueden crearse SSIDs adicionales. Desde esta página, puede editarse un SSID existente o eliminarlo del sistema. Esta configuración también puede introducirse en la página Express Setup.
- Nombre de Usuario LEAP [LEAP User Name]: utilice este campo si la radio se configura como repetidora y se autentica para entrar a la red utilizando LEAP. Cuando la radio se autentica utilizando LEAP, el bridge envía este nombre de usuario al servidor de autenticación. Información acerca de cómo configurar un access point repetidor como cliente LEAP se trata en el Módulo 8.
- Password LEAP [LEAP Password]: utilice este campo si la radio se configura como repetidora y se autentica para entrar a la red utilizando LEAP. Cuando la radio se autentica utilizando LEAP, el bridge utiliza esta password para la autenticación.

6.3.2 Configuración de radio extendida - página de hardware

Esta sección describe cómo configurar la página Hardware de Radio Raíz [Root Radio Hardware] de la radio del bridge. La página Hardware de Radio Raíz contiene configuraciones para el SSID, velocidades de datos, potencia de transmisión, antenas, canal de radio y umbrales operativos del bridge.

Siga estos pasos para llegar a la página Hardware de Radio Raíz:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Hardware de la fila Radio Raíz, bajo Puertos de Red [Network Ports].

6.3.3 Configuración de radio extendida - página avanzada

Esta sección describe cómo configurar la página Radio Raíz Avanzada para asignar configuraciones especiales para el radio de bridge.

Siga estos pasos para llegar a la página Radio Raíz Avanzada:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Avanzado en la fila Radio Raíz, bajo Puertos Raíz [Network Ports].

6.3.4 Configuración del puerto Ethernet - página de identificación

Esta sección describe cómo configurar el puerto Ethernet del bridge, utilizando las páginas del sistema de administración. Las páginas de Ethernet incluyen las siguientes:

- Identificación de Ethernet [Ethernet Identification]: contiene información acerca de ubicación e identidad del puerto Ethernet.
- Hardware Ethernet [Ethernet Hardware]: contiene la configuración de la velocidad de conexión al puerto Ethernet del bridge.
- Ethernet Avanzada [Ethernet Advanced]: contiene configuraciones para el estado operativo del puerto Ethernet del bridge.

Siga estos pasos para llegar a la página Identificación de Ethernet:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Identificación [Identification] en la fila Ethernet, bajo Puertos de la Red [Network Ports].

6.3.5 Configuración del puerto Ethernet - página de hardware

Esta sección describe cómo configurar el puerto Ethernet del bridge, utilizando la página de Hardware Ethernet. Esta página se utiliza para seleccionar el tipo de conector, la velocidad de conexión y la configuración de dúplex utilizados por el puerto Ethernet del bridge.

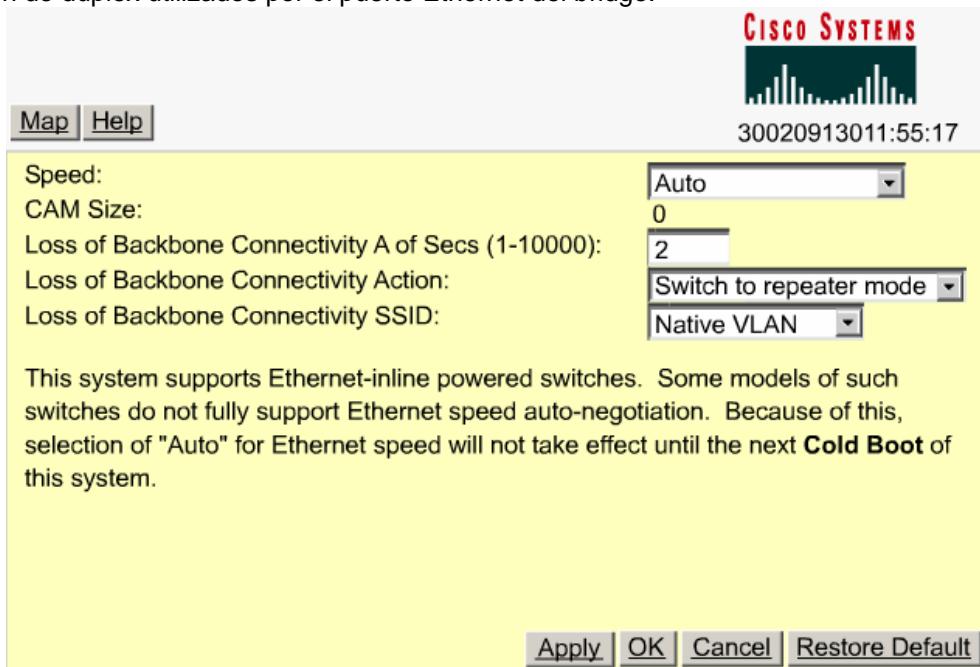


Figura 1

Siga estos pasos para llegar a la página Hardware Ethernet [Ethernet Hardware], como se muestra en la Figura 1:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Hardware en la fila Ethernet, bajo Puertos de la Red [Network Ports].

6.3.6 Configuración del puerto Ethernet - página avanzada

Esta sección describe cómo configurar el puerto Ethernet del bridge, utilizando la página Ethernet Avanzada [Ethernet Advanced] del sistema de administración. La página Ethernet Avanzada contiene configuraciones para el estado operativo del puerto Ethernet del bridge.

Siga estos pasos para llegar a la página Ethernet Avanzada:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Avanzada [Advanced] en la fila Ethernet, bajo Puertos de la Red [Network Ports].

6.4 Configuración de Servicios

6.4.1 Configuración de servicios de tiempo

Siga estos pasos para llegar a la página de Configuración del Servidor de Tiempo [Time Server Setup], como se muestra en la Figura 1:

The screenshot shows the 'Time Server Setup' configuration page. At the top right is the Cisco Systems logo and the uptime information 'Uptime: 3 days, 19:30:22'. Below this, there's a section for 'Simple Network Time Protocol (SNTP)' with an 'Enabled' radio button selected. The 'Default Time Server' field is empty. Under 'Current Time Server', there's a dropdown menu showing '(GMT-05:00) Eastern Time (US & Canada)'. The 'GMT offset (hr):' dropdown also shows '(GMT-05:00) Eastern Time (US & Canada)'. The 'Use Daylight Savings Time:' section has a 'yes' radio button selected. There are two empty input fields for 'Manually set date (YYYY/MM/DD):' and 'Manually set time (HH:MM:SS):'. At the bottom are four buttons: 'Apply', 'OK', 'Cancel', and 'Restore Default'.

Figura 1

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Servidor de Tiempo [Time Server], bajo Servicios [Services].

La página Configuración del Servidor de Tiempo [Time Server Setup] contiene las siguientes configuraciones:

- Protocolo de Tiempo de Red Simple [Simple Network Time Protocol]: seleccione Habilitado o Inhabilitado [Enabled o Disabled] para activar o desactivar el Protocolo de Tiempo de Red Simple (SNTP). Si la red utiliza SNTP, seleccione Habilitado.
- Servidor de Tiempo por Defecto [Default Time Server]: si la red tiene un servidor de tiempo por defecto, introduzca la dirección IP en el campo de entrada Servidor de Tiempo por Defecto. La línea Servidor de Tiempo Actual [Current Time Server] bajo el campo de entrada muestra el servidor de tiempo que está utilizando actualmente el bridge.
- Compensación GMT (h) [GMT Offset (hr)]: el menú desplegable Compensación GMT enumera zonas horarias internacionales, en relación a la Hora del Meridiano de Greenwich (GMT). Seleccione la zona horaria en la cual opera el bridge.
- Utilizar Horario de Verano [Use Daylight Savings Time]: seleccione sí [yes] o no, para que el bridge se ajuste automáticamente al Horario de Verano.
- Configurar manualmente la fecha y la hora [Manually Set Date and Time]: introduzca la fecha y la hora actuales en los campos de entrada, para anular el servidor de tiempo o para ajustar la fecha y la hora si no se dispone de un servidor.

6.4.2 Configuración de los servicios de inicio

Siga estos pasos para llegar a la página Configuración del Servidor de Inicio [Boot Server Setup]:

Paso 1 En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].

Paso 2 En la página Setup, haga clic en Servidor de Inicio [Boot Server], bajo Servicios [Services].

La página Configuración del Servidor de Inicio [Boot Server Setup], que se muestra en la Figura 1, contiene las siguientes configuraciones:

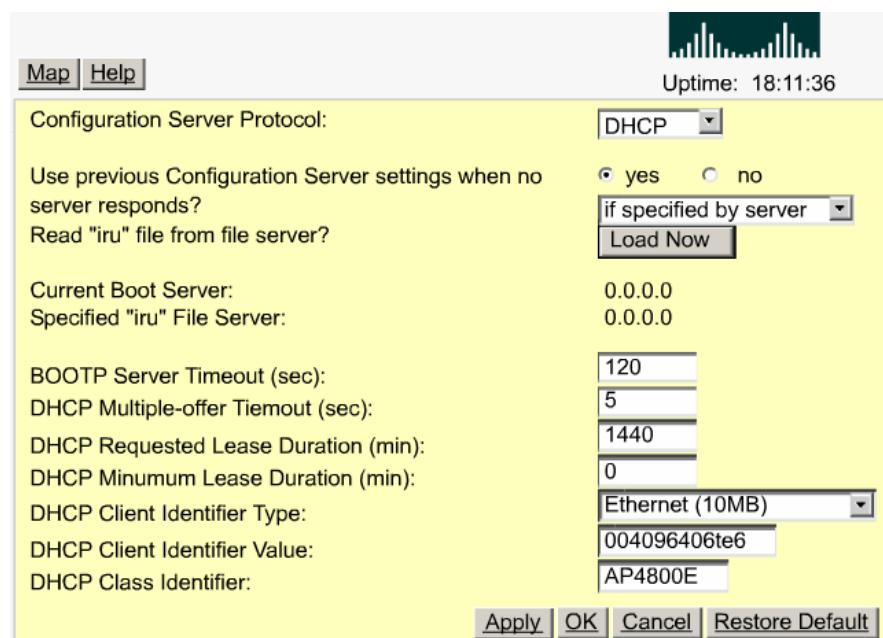


Figura 1

- Protocolo del Servidor de Configuración [Configuration Server Protocol] – Utilice el menú desplegable del Protocolo del Servidor de Configuración para seleccionar el método que utiliza la red para la asignación de direcciones IP. El menú contiene las siguientes opciones:
 - Ninguno [None] – La red no cuenta con un sistema automático para la asignación de direcciones IP.
 - BOOTP – La red utiliza el Protocolo de Inicio [Boot Protocol], en el cual las direcciones IP se preprograman, según las direcciones MAC.
 - DHCP – En el caso del Protocolo de Configuración Dinámica del Host (DHCP), las direcciones IP se alquilan durante un tiempo. La duración del alquiler puede configurarse desde esta página.
- Utilizar las Configuraciones Anteriores del Servidor [Use Previous Configuration Server Settings] – Seleccione sí [yes] para que el bridge guarde la respuesta más reciente del servidor de inicio. El bridge utiliza las configuraciones más recientes si el servidor de inicio no está disponible.
- Leer el Archivo .iru desde el Servidor de Archivo [Read ".iru" File from File Server] – Utilice esta configuración para que el bridge utilice configuraciones en un archivo .iru en el servidor BOOTP o DHCP, o en el servidor de archivos por defecto. Los archivos con extensiones .iru usualmente contienen información de configuración utilizada durante el inicio del sistema. El menú desplegable contiene las siguientes opciones:
 - Siempre [Always] – El bridge siempre carga las configuraciones desde un archivo .iru del servidor.
 - Nunca [Never] – El bridge nunca carga configuraciones desde un archivo .iru del servidor.
 - Si lo especifica el servidor [If specified by server] – El bridge cargará las configuraciones desde un archivo .iru en el servidor, si la respuesta DHCP o BOOTP del servidor especifica que se dispone de un archivo .iru. Ésta es la configuración por defecto. El botón Cargar Ahora [Load Now], bajo el menú desplegable, instruye al bridge para que lea un archivo .iru inmediatamente.
- Servidor de Inicio Actual [Current Boot Server] – La línea Servidor de Inicio Actual, bajo el menú desplegable, enumera los servidores que respondieron a la solicitud de inicio del bridge. Si aparecen todos ceros, significa que el bridge no está utilizando BOOTP ni DHCP, o que ningún servidor respondió a la solicitud BOOTP ni DHCP.
- Servidor de Archivos Especificados por ".iru" [Specified ".iru" File Server] – La línea Servidor de Archivos Especificados por ".iru" enumera la dirección IP del servidor donde está almacenado el archivo .iru. Si aparecen todos ceros, significa que ningún servidor de archivos está configurado para proporcionar un archivo .iru.
- Tiempo Vencido del Servidor BOOTP [BOOTP Server Timeout] – Esta configuración especifica el tiempo, en segundos, que el bridge espera para recibir una respuesta de un único servidor BOOTP. Esta configuración se aplica sólo cuando se selecciona BOOTP desde el menú desplegable Protocolo del Servidor de Configuración.

- Tiempo Vencido de Oferta Múltiple DHCP [DHCP Multiple-Offer Timeout] – Esta configuración especifica el tiempo, en segundos, que el bridge espera para recibir una respuesta cuando hay múltiples servidores DHCP.
- Duración del Alquiler Solicitado por DHCP [DHCP Requested Lease Duration] – Esta configuración especifica el tiempo, en minutos, durante el cual el bridge solicita el alquiler de una dirección IP desde el servidor DHCP.
- Duración Mínima del Alquiler DHCP [DHCP Minimum Lease Duration] – Esta configuración especifica el tiempo más breve, en minutos, que el bridge aceptará por el alquiler de una dirección IP. El bridge ignora alquileres más breves que este periodo.
- Tipo de Identificador del Cliente DHCP [DHCP Client Identifier Type] – Esta configuración opcional se utiliza para incluir un tipo de identificador de clase en los paquetes de solicitud DHCP que el bridge envía al servidor DHCP. El servidor DHCP puede configurarse para enviar respuestas de acuerdo al tipo de identificador de clase.

6.4.3 Configuración de servicios de nombre

Siga estos pasos para llegar a la página Configuración del Servidor de Nombres, que se muestra en la Figura 1:

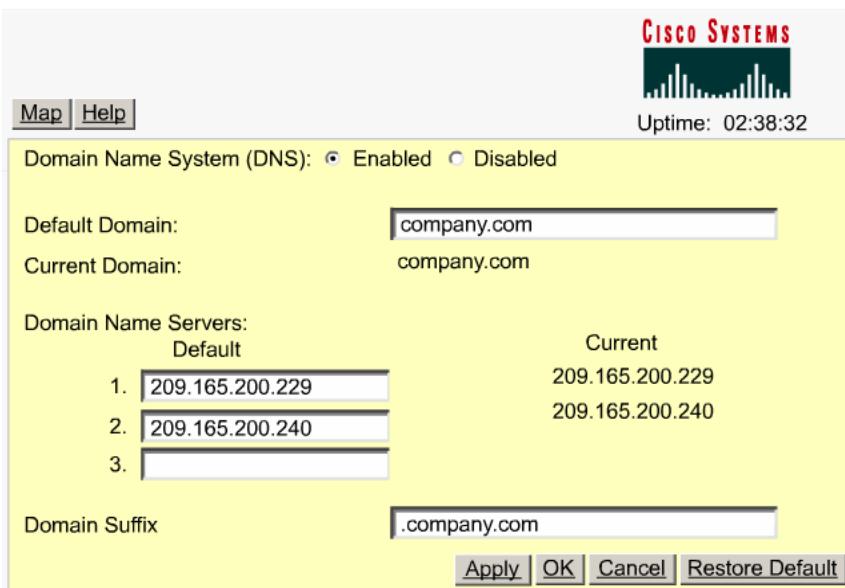


Figura 1

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Servidor de Nombres [Name Server], bajo Servicios [Services].

La página Configuración del Servidor de Nombres [Name Server Setup] contiene las siguientes configuraciones:

- Sistema de Nombres de Dominio [Domain Name System]: si la red utiliza un Sistema de Nombres de Dominio (DNS), seleccione Habilitado [Enabled] para indicar al bridge que utilice el sistema. Si la red no utiliza DNS, seleccione Inhabilitado [Disabled].
- Dominio por Defecto [Default Domain]: introduzca el nombre del dominio IP de la red en el campo Entrada [Entry]. La entrada podría tener el siguiente aspecto: mycompany.com

La línea Dominio Actual [Current Domain] bajo el campo de entrada enumera el dominio que sirve al bridge.

- Servidores de Nombre de Dominio [Domain Name Servers]: introduzca las direcciones IP de los tres servidores de nombre de dominio de la red. Las líneas Actual [Current] a la derecha de los campos de entrada enumeran los servidores que el bridge está utilizando actualmente. El servidor DHCP o BOOTP puede especificarlos.
- Sufijo del Dominio [Domain Suffix]: en este campo de entrada, introduzca la porción del nombre de dominio completo que ha de omitirse de la pantalla del bridge. Por ejemplo, en el dominio "mycompany.com", el nombre completo de una computadora podría ser "mycomputer.mycompany.com". Con el sufijo de dominio configurado como "mycompany.com", el nombre se mostraría en las páginas del sistema de administración como "mycomputer."

6.4.4 Configuración del enrutamiento

Siga estos pasos para llegar a la página Configuración del Enrutamiento [Routing Setup]:

1. En la página Resumen de Estado [Summary Status], haga clic en Configuración [Setup].
2. En la página Setup, haga clic en Enrutamiento [Routing], bajo Servicios [Services].

Utilice la página de configuración del enrutamiento para configurar el bridge para que se comunique con el sistema de enrutamiento de la red IP. Utilice las configuraciones de la página para especificar el gateway por defecto y para construir una lista de configuraciones de rutas de red instaladas. La Figura 1 muestra la página de configuración de enrutamiento.

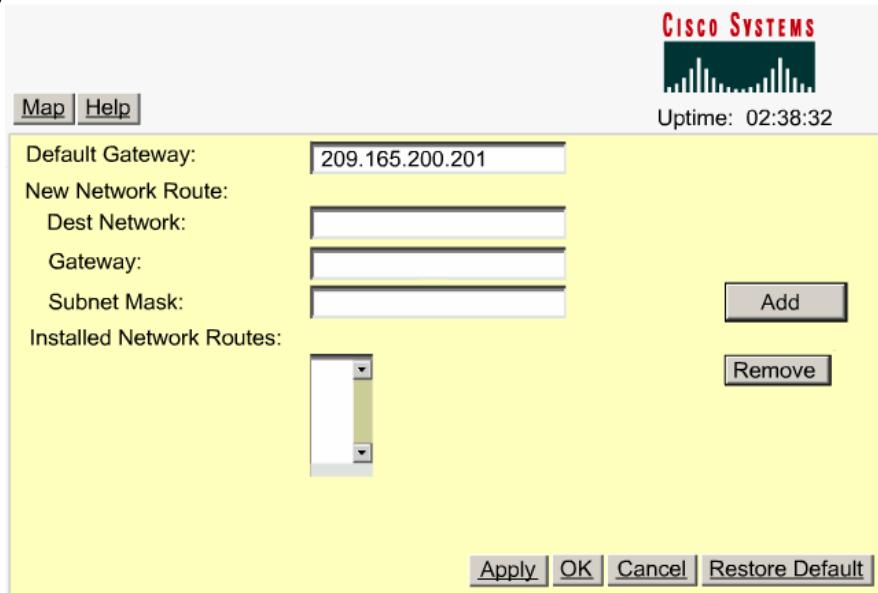


Figura 1

- **Gateway por Defecto [Default Gateway]:** introduzca la dirección IP del gateway por defecto para la red, en este campo de entrada. La entrada 255.255.255.255 indica que no hay ningún gateway.
- **Nueva Ruta de Red [New Network Route]:** pueden definirse rutas de red adicionales para el bridge. Para agregar una ruta a la lista instalada, complete los tres campos de entrada y haga clic en Agregar [Add]. Para eliminar una ruta de la lista, resalte la ruta y haga clic en Eliminar [Remove]. Los tres campos de entrada son los siguientes:
 - **Red de Destino [Dest Network]:** introduzca la dirección IP de la red de destino.
 - **Gateway:** introduzca la dirección IP del gateway utilizado para llegar a la red de destino.
 - **Máscara de Subred [Subnet Mask]:** introduzca la máscara de subred asociada a la red de destino.
- **Rutas Instaladas de la Red [Installed Network Routes]:** la lista de rutas instaladas proporciona la dirección IP de la red de destino, el gateway y la máscara de subred para cada ruta instalada.

6.5 Servicios de Cisco

6.5.1 Descripción general de los servicios

La página de la Figura 1 se utiliza para configurar servicios de Cisco y actualizar el firmware navegando hasta una unidad local o utilizando FTP para actualizar el firmware desde un servidor de archivos.

Puede accederse a las siguientes configuraciones desde esta página:

- **Administrar Claves de Instalación [Manage Installation Keys]** se utiliza para leer especificaciones de la licencia de software y para instalar una nueva licencia.
- **Administrar la Configuración del Sistema [Manage System Configuration]** se utiliza para reiniciar el dispositivo, descargar un archivo de configuración o reiniciar las configuraciones según los valores por defecto de fábrica.
- **Distribuir la Configuración a otros Dispositivos Cisco [Distribute Configuration to other Cisco Devices]** se utiliza para enviar la configuración del dispositivo a otros dispositivos Cisco Aironet de su red.
- **Distribuir el Firmware a otros Dispositivos Cisco [Distribute Firmware to other Cisco Devices]** se utiliza para enviar una nueva versión del firmware a otros dispositivos Cisco Aironet de su red.

- Administración Hot Standby [Hot Standby Management] se utiliza para configurar el dispositivo en espera.
- Cisco Discovery Protocol (CDP) se utiliza para ajustar las configuraciones CDP del dispositivo.



Figura 1

Actualización Completa del Firmware

Estos son enlaces a formas alternativas para leer y actualizar el firmware del sistema, el firmware de radio y las páginas web, todo en un solo paso.

- Mediante el Navegador -- Con este método, pueden utilizarse la unidad de disco rígido o las unidades de red mapeadas para hallar el firmware y los archivos de la página web deseados, y actualizar todos los componentes de firmware al mismo tiempo.
- Desde el Servidor de Archivos -- Con este método, la información del archivo se utiliza para actualizar todos los componentes del firmware al mismo tiempo.

Actualización Selectiva del Firmware

Estos son enlaces utilizados como formas alternativas para leer y actualizar el firmware del sistema, el firmware de radio y las páginas web.

- Mediante el Navegador -- Con este método, pueden utilizarse la unidad de disco rígido o las unidades de red mapeadas para hallar el firmware y los archivos de la página web deseados, y actualizar los componentes del firmware de manera individual.
- Desde el Servidor de Archivos -- Con este método, la información de los archivos se utiliza para actualizar todos los componentes de firmware de manera individual.

Ubicar la Unidad por medio de LEDs Parpadeantes

Seleccione Habilitado [Enabled] y haga clic en Aplicar [Apply]. Los indicadores del panel superior del bridge parpadean al unísono. Seleccionar Inhabilitado [Disabled] y hacer clic en Aplicar [Apply] hace que los indicadores dejen de parpadear y regresen a la operación normal.

6.5.2 CDP

CDP es un protocolo de descubrimiento de dispositivos que se ejecuta en todo el equipamiento de red de Cisco. La información de los paquetes CDP se utiliza en el software de administración de redes como CiscoWorks2000.

Utilice la página de Configuración de CDP [CDP Setup] para ajustar las configuraciones de CDP del access point. CDP se habilita por defecto.

Cisco Discovery Protocol (CDP): seleccione Inhabilitado [Disabled] para inhabilitar CDP en el access point. Seleccione Habilitado [Enabled] para habilitar CDP en el access point. CDP se habilita por defecto.

Tiempo de Espera del Paquete [Packet Hold Time]: la cantidad de segundos durante la cual otros dispositivos habilitados para CDP deberán considerar válida la información del CDP del access point. Si otros dispositivos no reciben otro paquete CDP del access point antes de que transcurra este tiempo, deberán suponer que el access point ha pasado a estado offline. El valor por defecto es 180. El tiempo de espera del paquete siempre deberá ser mayor que el valor del campo "Paquetes enviados cada" ["Packets sent every"]. Paquetes Enviados Cada [Packets Sent Every]: la cantidad de segundos entre cada paquete CDP que envía el access point. El valor por defecto es 60. Este valor deberá ser menor que el tiempo de espera del paquete.

Habilitación del Puerto Individual [Individual Port Enable]: Ethernet: cuando se lo selecciona, el access point envía paquetes CDP a través de su puerto Ethernet y monitorea Ethernet en busca de paquetes CDP provenientes de otros dispositivos.

Habilitación del Puerto Individual [Individual Port Enable]: Radio del AP: este recuadro de verificación aparece cuando la radio del access point está vinculada a otro dispositivo de infraestructura de radio, como un access point, bridge o repetidor. Cuando se lo selecciona, el access point envía paquetes CDP a través del puerto de radio y monitorea la radio en busca de paquetes CDP provenientes de otros dispositivos.

6.5.3 Actualización y distribución del firmware

Desde el menú Servicios Cisco [Cisco Services], haga clic en el vínculo Distribuir el firmware a otros Dispositivos [Distribute firmware to other Devices]. La Figura 1 muestra que esta página permite la distribución del firmware de Cisco de un access point a otros dispositivos Cisco. El access point de distribución envía el firmware a todos los access points de su red que:

- Ejecuten firmware que soporta la función Distribuir Firmware [Distribute Firmware]
- Puedan escuchar la "consulta" IP multicast emitida por el access point de distribución (dispositivos de red como los routers que bloquean los mensajes multicast)
- Que sus servidores web se habiliten para una navegación externa
- Que el Administrador de Usuarios esté habilitado, contenga en sus Listas de Usuarios un usuario con el mismo nombre de usuario, password y capacidades que el usuario que lleva a cabo la distribución (la persona que inició sesión en el access point de distribución)

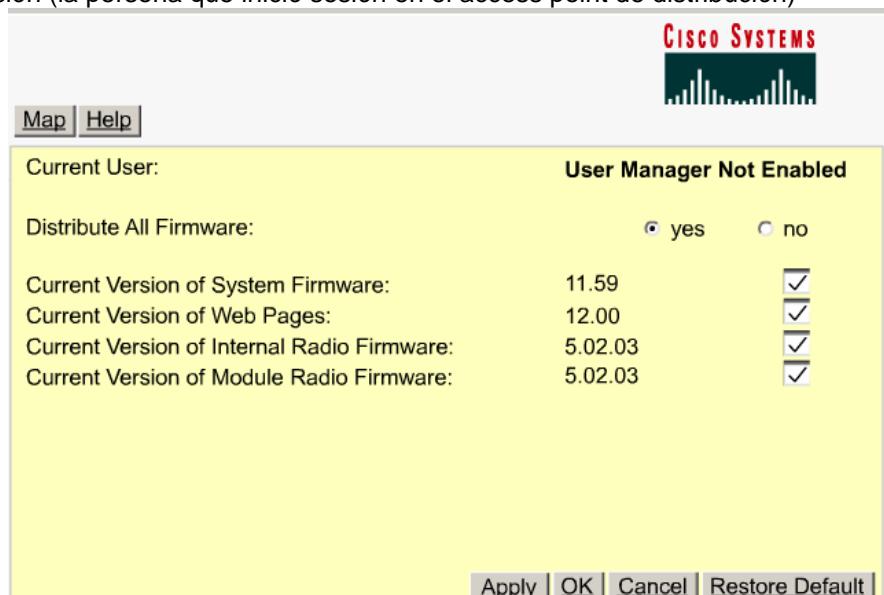


Figura 1

Usuario Actual [Current User]: éste es el usuario que ha iniciado sesión para distribuir el firmware. Si el administrador de usuarios está habilitado en los access points de su red, las Listas de Usuarios de esos access points deben contener un usuario con el mismo nombre de usuario, password y capacidades que el usuario que lleva a cabo la distribución (la persona que inició sesión en el access point de distribución).

Distribuir Todo el Firmware [Distribute All Firmware]: esta característica funciona como un botón "Seleccionar todo" ["Select all"] para distribuir el firmware. Seleccione Sí [Yes] para distribuir la versión actual del firmware del sistema, las páginas web, y, de aplicarse, el firmware de radio.

Versión Actual del Firmware del Sistema [Current Version of System Firmware]: ésta es la versión del firmware del sistema en el access point de distribución. Haga clic en el recuadro de verificación para marcar esta versión para su distribución.

Versión Actual de las Páginas Web [Current Version of Web Pages]: ésta es la versión de las páginas web del sistema de administración en el access point de distribución. Haga clic en el recuadro de verificación para marcar esta versión para su distribución.

Versión Actual del Firmware de Radio [Current Version of Radio Firmware]: ésta es la versión del firmware de radio para cada una de las radios (módulo interno de 2,4 GHz y externo de 5 GHz) en el access point de distribución. Haga clic en el recuadro de verificación para marcar esta versión para su distribución.

Botones de Acción

Los dos botones de acción controlan la distribución del firmware.

1. Iniciar [Start]: una vez que se selecciona el firmware que desea distribuir, haga clic en Iniciar para comenzar la distribución.
2. Abortar [Abort]: haga clic en Abortar para cancelar la distribución.

Desde la página de Configuración [Setup], haga clic en Servicios Cisco [Cisco Services], y luego haga clic en el vínculo Actualizar el Firmware Completamente: Mediante el Navegador [Fully Update Firmware: Through Browser].

Esta sección muestra tres niveles de versión del firmware actuales:

1. Firmware del Sistema, Páginas Web, y Firmware de Radio
2. Recuperar Todos los Archivos de Firmware [Retrieve All Firmware Files]: haga clic en el vínculo Recuperar todo el Firmware [Retrieve All Firmware] para guardar el Firmware del Sistema y las Páginas Web actuales en una unidad de disco rígido local.
3. Nuevo Archivo para Todo el Firmware [New File for All Firmware]: utilice esta sección para navegar por su unidad de disco rígido o unidades de red mapeadas para hallar el nuevo archivo firmware. Hacer clic en el botón Actualizar por Navegador Ahora [Browser Update Now] comenzará el proceso de actualización de firmware en el access point.

6.5.4 Administración hot standby

El modo Hot Standby designa un access point como respaldo para otro access point. El access point standby se coloca cerca del access point al cual monitorea, configurado de manera exactamente igual que el access point monitoreado. El access point standby se asocia al access point monitoreado como cliente y consulta el access point monitoreado regularmente a través tanto de Ethernet como de los puertos de radio. Si el access point monitoreado no responde, el access point standby pasa al estado online y asume el lugar del access point monitoreado en la red.

Excepto por la dirección IP, las configuraciones del access point standby deberán ser idénticas a las configuraciones del access point monitoreado. Si el access point monitoreado pasa a estado offline y el access point standby toma su lugar en la red, hacer coincidir las configuraciones asegura que los dispositivos cliente puedan alternar fácilmente al access point standby.

El modo hot standby está inhabilitado por defecto.

Para utilizar hot standby, configure los siguientes parámetros:

ID del Conjunto de Servicios [Service Set ID] (SSID): el SSID es un identificador único que utilizan los dispositivos clientes para asociarse al access point. El SSID permite a los dispositivos clientes distinguir entre múltiples redes inalámbricas cercanas. El SSID puede ser una entrada alfanumérica de 2 a 32 caracteres de longitud.

Dirección MAC para el Access Point Monitoreado [MAC Address for the Monitored Access Point]: introduzca la dirección MAC del access point monitoreado.

Frecuencia de Sondeo [Polling Frequency]: introduzca la cantidad de segundos entre cada consulta que el access point envía al access point monitoreado.

Tiempo Vencido para Cada Sondeo [Timeout for Each Polling]: introduzca la cantidad de segundos que deberá esperar el access point standby desde el access point monitoreado antes de que el access point monitoreado haya funcionado mal.

Estado Actual [Current Status]: informa respecto al estado del access point standby.

6.5.5 Administración de la configuración del sistema

Administración del Sistema

Desde la página de servicios Cisco haga clic en el vínculo Administración de la Configuración del Sistema [Manage System Configuration]. Desde esta página, pueden llevarse a cabo las siguientes tareas:

- REINICIO "EN CALIENTE" DEL SISTEMA AHORA ["WARM" RESTART SYSTEM NOW] – Haga clic en este botón para llevar a cabo un reinicio en caliente del access point. Un reinicio en caliente reinicia el access point.
- REINICIO "EN FRÍO" DEL SISTEMA AHORA ["COLD" RESTART SYSTEM NOW] – Haga clic en este botón para llevar a cabo un reinicio en frío del access point. Un reinicio en frío es el equivalente de eliminar y luego volver a aplicar la energía al access point.
- Descargar la Configuración del Sistema No por Defecto Excepto la Identidad IP [Download Non-Default System Configuration Except IP Identity] – Haga clic en este botón para guardar el archivo de configuración del sistema no por defecto del access point, menos la información de Identidad IP (Protocolo Internet) del access point, en su computadora, o en cualquier unidad accesible.
- Reiniciar los Valores por Defecto del Sistema Excepto la Identidad IP [Reset System Factory Defaults Except IP Identity] – Haga clic en este botón para reiniciar todas las configuraciones del access point, excepto la información de identidad IP del access point, según sus valores por defecto de fábrica. Al no reiniciar la información de la identidad IP según los valores por defecto de fábrica, asegúrese de que mantendrá una conectividad Ethernet al access point.
- Descargar las Configuraciones del Sistema No por Defecto [Download Non-Default System Configurations] – Haga clic en este botón para guardar el archivo de configuración no por defecto del access point en su computadora, o en cualquier unidad accesible.
- Descargar Todas las Configuraciones del Sistema [Download All System Configurations] – Haga clic en este botón para guardar el archivo de configuración del access point en su computadora, o en cualquier unidad accesible.
- Reiniciar Todos los Valores por Defecto de Fábrica [Reset All System Factory Defaults] – Haga clic en este botón para reiniciar todas las configuraciones del access point, incluyendo la información de identidad IP del access point, según los valores por defecto de fábrica.
- Leer el Archivo de Configuración del Servidor [Read Config File from Server] – Haga clic en este botón para recuperar un archivo de configuración desde el servidor al access point.
- Actualizar desde el Navegador Ahora [Browser Update Now] – Haga clic en este botón para enviar el archivo de configuración que nombró en el campo de entrada del archivo de configuración del sistema adicional del access point.

Resumen

Este módulo trató los bridges inalámbricos como medio para conectar dos o más LANs para crear una LAN grande. Puesto que el bridge es un dispositivo de radio, se tratan las causas comunes de interferencia que pueden reducir el throughput y el alcance, junto a las precauciones que deben considerarse al configurar un bridge.

Este módulo brindó la oportunidad de configurar un bridge y proporcionó experiencia al configurar puertos Ethernet y de radio en un bridge. Finalmente, el módulo trató cómo se configuran y administran los servicios de tiempo, nombre, inicio y enrutamiento.

Mediante el uso de las actividades de práctica de laboratorio que acompañaron este módulo, el alumno obtuvo una comprensión de la configuración inicial del bridge, la configuración de servicios y cómo deberán administrarse los archivos de configuración.

Módulo 7: Antenas

Descripción General

Este módulo cubrirá la teoría básica de las antenas, incluyendo la selección de antena direccional y onmidireccional. En general, las antenas de alta ganancia dirigen la energía en forma restringida y precisa. Las antenas de baja ganancia dirigen la energía en un patrón más amplio y ancho. Todo acerca de la elección de la antena involucra un equilibrio. Si se desea un rango máximo, se debe sacrificar cobertura. Con una antena direccional, la misma cantidad de energía llega a la antena, pero el diseño de la antena puede reflejar y dirigir la energía RF en ondas más estrechas y fuertes, o en ondas más amplias y menos intensas, al igual que con una linterna.

Después de tratar la teoría y los tipos de las antenas, se hablará sobre los cables, conectores y accesorios. Con los cables, cuanto menor sea la longitud, mayor es la calidad de la cobertura. Además se tratarán consideraciones importantes sobre el diseño de la antena, como la ingeniería del enlace, el planeamiento de la ruta y la instalación.

7.1 Antenas

7.1.1 Introducción

Las antenas generalmente se dividen en dos tipos. La Figura 1 muestra los dos tipos. La Figura 2 muestra ejemplos de cada uno de estos tipos. Una buena antena transfiere la potencia en forma eficiente. La transferencia eficiente de la potencia depende de la correcta alineación de la antena (polarización) y de la concordancia apropiada de la impedancia. Para lograr una concordancia de la impedancia se debe hacer concordar en forma eléctrica la línea de transmisión hacia la antena. Esto significa que la línea de transmisión transfiere toda la potencia hacia la antena y no irradia la energía misma.

Types of Antennas

Directional antennas radiate RF energy predominantly in one direction. Common types of directional antennas include the following:

- Yagi
- Solid parabolic
- Semi parabolic
- Patch or panel

Omni-directional antennas radiate RF energy equally in all horizontal directions. This horizontal radiation covers 360 degrees. Common types of omni-directional antennas include the following:

- Mast mount
- Rubber dipole

Figura 1

Todas las antenas tienen un patrón de radiación. Muy relacionada con el patrón de radiación está la polarización de la antena. Las antenas pueden ser agrupadas en sistemas para lograr el patrón deseado. Estos sistemas pueden entonces ser dirigidos electrónicamente. Debido al diseño de baja potencia de las WLANs, todas las antenas usadas son pasivas. Una antena pasiva no tiene amplificadores conectados, y por lo tanto tendrá las mismas características sea que esté transmitiendo o recibiendo. La Figura 3 muestra la cobertura general de las antenas direccionales versus las omnidireccionales y algunas de las aplicaciones típicas.

Las antenas usadas para las WLANs tienen dos funciones:

- Receptor: Este es el terminador de una señal sobre un medio de transmisión. En comunicaciones, es un dispositivo que recibe información, control, u otras señales desde un origen.
- Transmisor: Este es el origen o generador de una señal sobre un medio de transmisión.

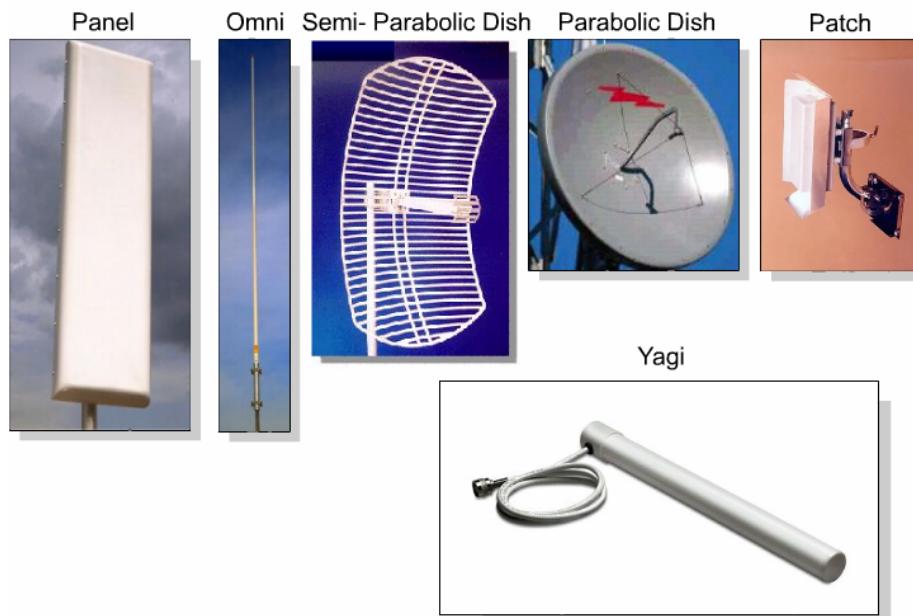
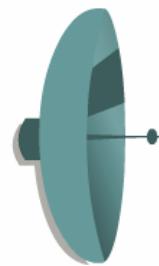


Figura 2



Omnidirectional



Directional

OMNI		DIRECTIONAL	
Type	Application	Type	Application
DiPole	Indoor	Patch	Indoor
Mast mount	Indoor/outdoor	Yagi	outdoor P2P/P2MP
Ceiling mount	indoor	Dish	outdoor P2P/P2MP
Ground Plane	indoor	Mast mount	indoor/outdoor P2MP

Figura 3

Para comprender a las redes inalámbricas, además de la forma de configurarlas y optimizarlas para un rendimiento óptimo, es esencial tener conocimiento sobre las antenas.

Este módulo cubrirá algunos de los temas básicos sobre las antenas y el funcionamiento de las antenas. Estos fundamentos son necesarios cuando se debe elegir antenas para una instalación WLAN.

Muchos access points vienen con antenas omnidireccionales que proporcionan una cobertura básica. Para extender el alcance de la transmisión, se debería usar una antena con mayor ganancia. La elección dependerá del alcance y de la cobertura deseada.

Debido a las leyes de la Comisión Federal de Comunicaciones [Federal Communication Commission (FCC)] de los EE.UU., todos los fabricantes de WLANs deben usar diferentes conectores para sus antenas. Esto ayuda a asegurar que las antenas estén diseñadas para trabajar con el equipo de WLAN. Cisco Systems, Inc. utiliza el conector RP-TNC, como se describe en la Figura 4.

U.S. FCC Antenna Regulations

- In 1994, the U.S. Federal Communications Commission (FCC) established some new rules for spread spectrum products. The antenna that is sold with a product must be tested by an FCC lab and approved with that product.
- In order to keep the average user from installing any type of antenna, the FCC also implemented a rule stating that any removable antenna had to use a unique, non-standard connector, which is not available through general distribution channels.
- Cisco antennas and all Cisco cables use a Reverse Polarity TNC (RP-TNC). This connector looks like a TNC, but the center contacts have been reversed. This prohibits a standard off-the-shelf antenna from being attached to a Cisco RF product.
- The FCC does permit a professional installer to use a different antenna or connector. A professional installer is defined as someone who has been trained in the applicable rules and regulations. A professional installer must also be able to verify that a site, which deviates from the standard product set requirements, meets the limitations of the FCC rules.

Figura 4

Las antenas están disponibles con diferentes capacidades de ganancia y alcance, anchos del rayo, y factores de formato. El acoplar la antena correcta con el access point (AP) o bridge correcto permite una cobertura eficiente en cualquier instalación, además de una mejor confiabilidad, a velocidades de datos muy altas. Las antenas Cisco para APs se muestran en la Figura 5.

						
Type	Rubber DiPole	Pillar Mount	Ground Plane	Patch Wall	Ceiling Mount	Ceiling Mount High Gain
Gain	2.15 dBi	5.2 dBi	5.2 dBi	8.5 dBi	2.2 dBi	5.2 dBi
Bandwidth	360° H 75° V	360° H 75° V	360° H 75° V	60° H 55° V	360° H 75° V	360° H 75° V
Indoor Range at 1Mbps	300' 91.4 m	497' 151.5 m	497' 151.5 m	700' 213.4 m	350' 106.7 m	497' 151.5 m
Indoor Range at 11Mbps	100' 30.5 m	142' 43.3 m	142' 43.3 m	200' 61 m	100' 30.5 m	142' 43.3 m
Cable Length	N/A	3' 0.9 m	3' 0.9 m	3' 0.9 m	9' 2.7 m	3' 0.9 m

Figura 5

Está disponible una variedad de antenas para bridges, dependiendo de la distancia requerida y de las posibilidades de montaje. Las antenas omnidireccionales son usadas generalmente para implementaciones punto a multipunto. La Figura 6 muestra las antenas Cisco para bridges inalámbricos.

					
Type	Patch Wall	Mast Mount	High Mount High Gain	Yagi Mast	Solid Dish
Gain	8 dBi	5.2 dBi	12 dBi	13.5 dBi	21 dBi
Bandwidth	60° H 55° V	360° H 75° V	360° H 7° V	30° H 25° V	12.4° H 12.4° V
Approximate Range at 1Mbps	2.0 Miles 3.2 km	5000' 1.5 km	4.6 Miles 7.4 km	6.5 Miles 10.5 km	25 Miles 40.2 km
Approximate Range at 11Mbps	3390' 1 km	1580' 0.5 km	1.4 Miles 2.3 km	2.0 Miles 3.2 km	11.5 Miles 18.5 km
Cable Length	3' 0.9 m	3' 0.9 m	1' 0.3 m	1.5' 0.5 m	2' 0.6 m

Figura 6

Cuando se utilizan equipos 802.11a de 5 GHz, las opciones de antenas externas están limitadas. La FCC de EE.UU. restringe el uso de esta banda U-NII no licenciada, que incluye un total de 300 MHz de espectro; desde 5.15 hasta 5.825 GHz. U-NII-1 incluye las frecuencias entre 5.15 y 5.25 GHz. Sólo es para acceso en interiores, usando una antena fija. U-NII-2 va de 5.25 a 5.35 GHz y es para uso en interiores o exteriores, con una antena flexible. U-NII-3 va de 5.725 a 5.825 y es sólo para aplicaciones externas de bridging. Diferentes restricciones se aplican en Europa para HiperLAN.

7.1.2 Variables

La distancia máxima de la antena se expresa normalmente en kilómetros o metros. La determinación de la distancia máxima entre las antenas a cada lado de un enlace no es un problema sencillo. La distancia máxima del enlace está determinada por lo siguiente:

- Potencia máxima de transmisión disponible
- Sensibilidad del receptor
- Disponibilidad de una ruta no obstruida para la señal de radio
- Máxima ganancia disponible, para la(s) antena(s)
- Pérdidas del sistema (como una pérdida a través del cable coaxial, conectores, etc.)
- Nivel de confiabilidad deseada (disponibilidad) del enlace

Antenna Variables

- Bandwidth
- Beamwidth
- Gain
- Polarization
- Diversity
- Power

Figura 1

Alguna literatura o tablas de aplicación del producto indicarán una distancia. En general, este valor es el óptimo, con todas las variables mostradas en la Figura 1 optimizadas. Además, el requerimiento de disponibilidad tendrá un efecto drástico en el alcance máximo. Una distancia de enlace puede exceder las distancias estándares si se pueden aceptar tasas de error constantemente altas.

La mejor forma de saber la distancia funcional entre dispositivos WLAN, es hacer un buen estudio del sitio. Un estudio del sitio comprende el examen de cada ubicación propuesta del enlace. Un examen del terreno y de las obstrucciones hechas por el hombre ayudará a determinar la factibilidad del sitio. Para estudios del sitio de bridging externo, también ayudará el determinar posibles necesidades de una torre. El resultado de tal examen arrojará la siguiente información:

- La pérdida de la ruta de la radio

- Cualquier problema que pueda comprometer el rendimiento del enlace, como la interferencia potencial

Una vez que el examen del sitio está hecho, se necesita hacer cálculos y elecciones de equipamiento. Variables como ganancia y tipo de antena, como lo muestra la Figura 2, conducirán a una respuesta definitiva para el alcance máximo.

Important Antenna Concepts

Directionality

- Omnidirectional (360 degree coverage)
- Directional (limited angle of coverage)

Gain

- Measured in dBi and dBd. (0 dBd is equal to 2.14 dBi)
- More gain mean more coverage in certain directions

Polarization

- Cisco Aironet antennas use vertical polarization.

Figura 2

7.1.3 Ancho de banda

El ancho de banda de una antena es la banda de frecuencias sobre la cual se considera que funciona en forma aceptable. Cuanto más amplio es el rango de frecuencias que abarca una banda, más amplio es el ancho de banda de la antena. La fórmula para el ancho de banda se muestra en la figura.

Percent Bandwidth is Defined as:

- $BW = 100 \frac{F_H - F_L}{F_C}$ where:
- F_H is the highest frequency in the band
- F_L is the lowest frequency in the band
- F_C is center frequency in the band $F_C = \frac{F_H + F_L}{2}$

Las antenas se adquieren pre-sintonizadas por el fabricante, para utilizarlas en un segmento de banda específico. El sacrificio en el diseño de una antena para un ancho de banda más amplio es que por lo general no tendrá un rendimiento tan bueno en comparación con una antena similar que está optimizada para un ancho de banda más angosto.

7.1.4 Ancho del rayo

El ancho del rayo es una medida usada para describir a las antenas direccionalles. El ancho del rayo a veces es llamado ancho de banda de la potencia media. Es el ancho total en grados del lóbulo de radiación principal, en el ángulo donde la potencia de radiación ha caído por debajo de la línea central del lóbulo, por 3 dB (potencia media). Esto está ilustrado en la Figura 1.

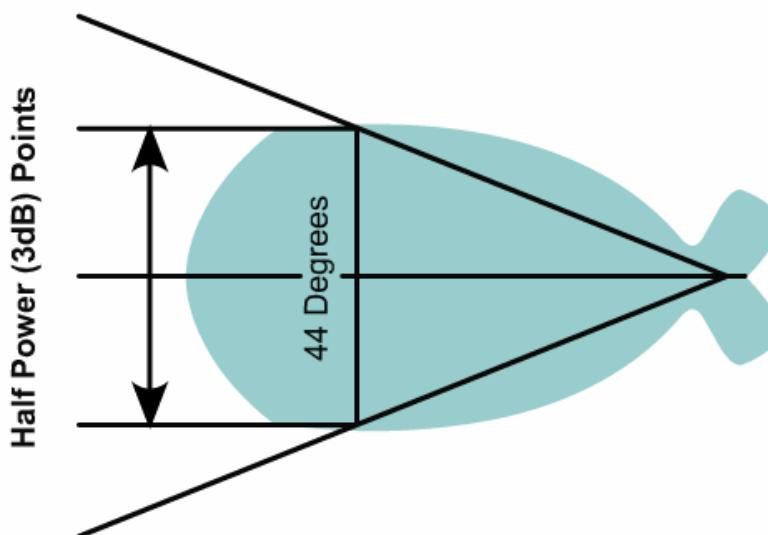


Figura 1

7.1.5 Ganancia

La ganancia de cualquier antena es en esencia una medida de cuán bien la antena enfoca la energía RF irradiada en una dirección en particular. Existen diferentes métodos para medir esto, dependiendo del punto de referencia elegido. Para asegurar una comprensión común, Cisco se está estandarizando en dBi para especificar las medidas de ganancia. Este método de medición de ganancia utiliza una antena isotrópica teórica como punto de referencia. Algunas antenas están medidas en dBd, que utiliza una antena de tipo bipolar en lugar de una antena isotrópica como el punto de referencia. Recuerde, para convertir cualquier número de dBd a dBi, simplemente sume 2,14 al número de dBd. La Figura 1 resume los fundamentos de la ganancia de la antena.

Overview of Gain

- Antenna gain is a fundamental parameter in radio link engineering.
- Gain is an indication of the antenna concentration of radiated power in a given direction.
- Antenna gain is most often expressed in dBi, which is gain over an isotropic antenna.
- Some antennas are specified in dBd. This number can be converted to dBi, by adding 2.14 to the dBd value.
 - For example, 18 dBd = 20.14 dBi
- An isotropic antenna is an ideal antenna, which radiates in all directions and has a gain of one (0 dB). This equates to zero gain and zero loss.

Figura 1

Las antenas de alta ganancia dirigen la energía en forma más restringida y precisa. Las antenas de baja ganancia dirigen la energía en una forma más amplia. Con las antenas del tipo plato, por ejemplo, la operación es similar a la operación del reflector en una linterna. En este ejemplo, el reflector concentra la salida de la lámpara de la linterna en una dirección predominante para maximizar el brillo de la salida de la luz en esa dirección. Muy poca luz va en otras direcciones. Este principio también se aplica a cualquier antena de ganancia, ya que siempre hay un equilibrio entre la ganancia, que es comparable al brillo en una dirección en particular, y el ancho del rayo, que es comparable a la angostura del rayo. Por lo tanto, la ganancia de una antena y su patrón de radiación están profundamente relacionados. Las antenas de mayor ganancia siempre tienen anchos de rayos o patrones más angostos. Las antenas de menor ganancia siempre tienen anchos de rayo más amplios. La Figura 2 ilustra esta relación. Las Figuras 3 y 4 muestran las relaciones entre la ganancia de la antena y el tamaño o frecuencia.

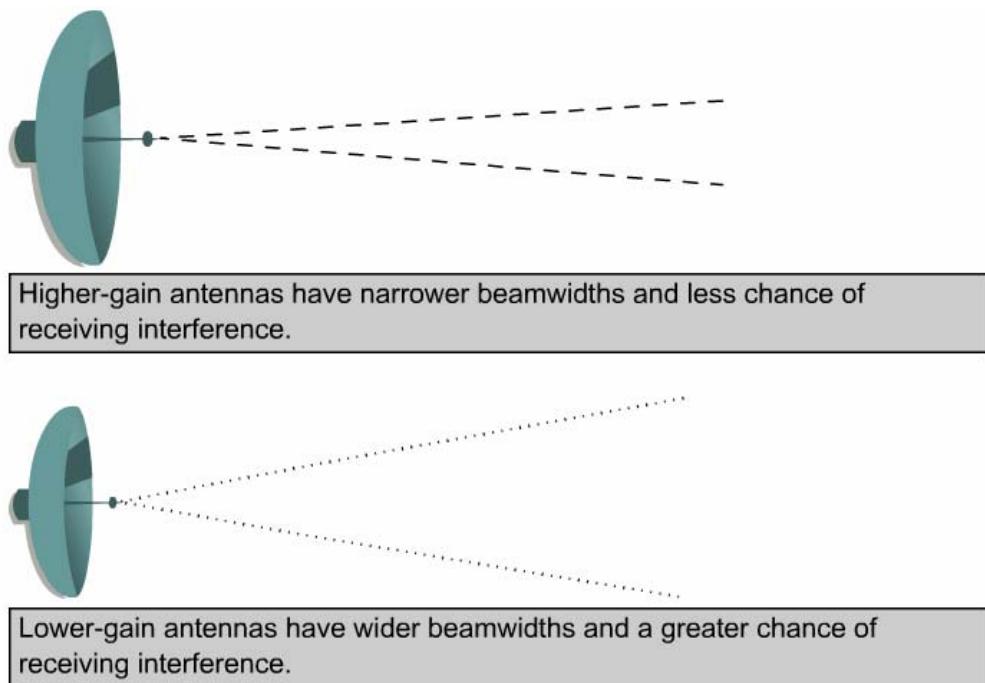


Figura 2

Frequency (GHz)	Size (Ft.)	Approx. Gain (dBi)
2.5	1	14.5
2.5	2	21
2.5	4	27
5.8	1	22.5
5.8	2	28.5
5.8	4	34.5

Figura 3

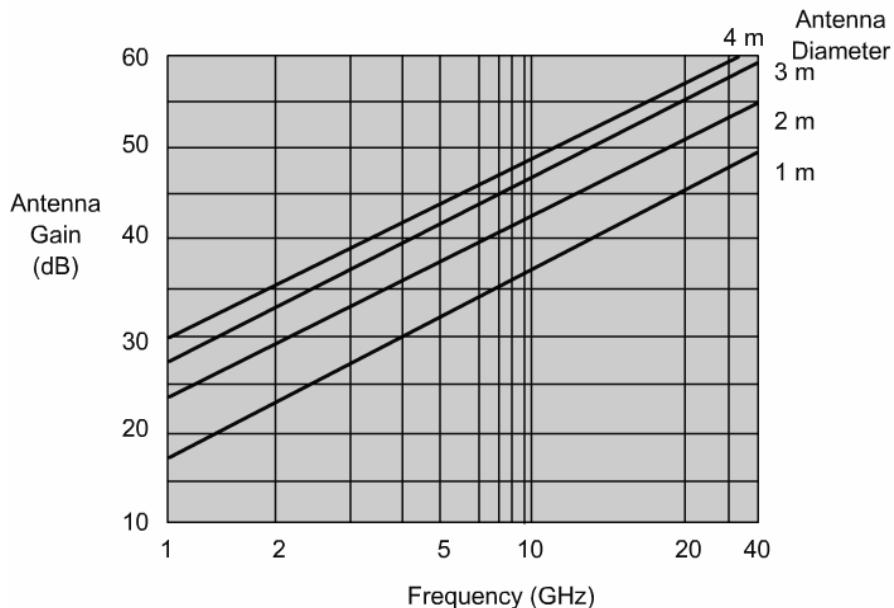


Figura 4

7.1.6 Polarización

La polarización es la orientación física del elemento en la antena que emite realmente la energía de RF. La polarización es un fenómeno físico de propagación de la señal de radio. Normalmente, dos antenas

cualesquiera que forman un enlace entre sí deben ser configuradas con la misma polarización. La polarización es normalmente ajustable durante o después del momento de la instalación de la antena. En la Figura 1 se muestra información básica sobre la polarización de la antena.

Basics of Antenna Polarization

Polarization refers to the orientation of the electric field that is created as the electromagnetic wave moves through space. The basic rules of polarization are as follows:

- For a horizontally polarized antenna, the electric field will be in the horizontal plane. For a vertically polarized antenna, the electric field will be in the vertical plane.
- For any given link between two units, it is necessary that both antennas have the same polarization. If they do not, additional unwanted signal loss will result.

Figura 1

Existen dos categorías, o tipos, de polarización. Ellas son lineal y circular, como lo muestra la Figura 2. Cada tipo tiene dos subcategorías. Las subcategorías para la polarización lineal son vertical u horizontal, como lo ilustra la Figura 3. Las subcategorías para la polarización circular son a mano derecha o a mano izquierda.

Polarization Category	Polarization Sub-Category	Notes
Linear	Vertical or Horizontal	The vast majority of microwave or dish-type antennas are linearly polarized.
Circular	Right Handed or Left Handed	This is not encountered much in commercial data communications.

Figura 2

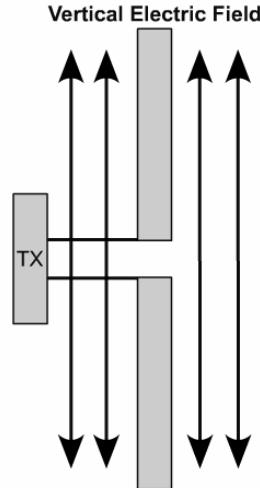
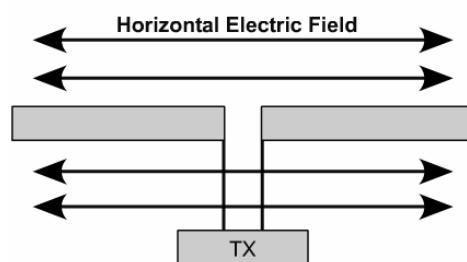


Figura 3

Una antena omnidireccional normalmente es una antena polarizada verticalmente. Todas las antenas de Cisco están configuradas para la polarización vertical.

Las antenas en ambos extremos de un enlace no necesitan ser del mismo tipo o tamaño. En algunos casos, las monturas de la antena en un extremo de un enlace sólo pueden soportar físicamente a una antena relativamente pequeña. El enlace puede necesitar una antena más grande en el otro extremo para proporcionar la ganancia de antena necesaria para la longitud de la ruta. Por otra parte, una antena de alta ganancia y patrón angosto puede ser necesaria en un extremo para evitar un problema de interferencia, que puede no ser un problema en el otro extremo.

Si dos antenas tienen diferentes ganancias, no importa cuál antena está en cada extremo, excepto si se consideran problemas de monturas o de interferencias. Recuerde que aunque las dos antenas para un

enlace puedan parecer muy diferentes entre sí, deben tener la misma polarización para que el enlace funcione correctamente.

Polarización Cruzada

Cuando dos antenas no tienen la misma polarización, la condición se llama polarización cruzada. Por ejemplo, si dos antenas tienen ambas polarización lineal, pero una tiene polarización vertical y la otra tiene polarización horizontal, estarían polarizadas en forma cruzada. El término polarización cruzada también se utiliza para describir dos antenas cualesquiera con polarización opuesta.

La polarización cruzada a veces es beneficiosa. Por ejemplo, suponga que las antenas del enlace A están polarizadas en forma cruzada con respecto a las antenas del enlace B. En este ejemplo, los enlaces A y B son dos enlaces diferentes, que están ubicados cercanos el uno del otro, pero no se pretende que se comuniquen entre sí. En este caso, el hecho de que los enlaces A y B tienen polaridad cruzada es beneficioso porque la polaridad cruzada evitará o reducirá cualquier posible interferencia entre los enlaces. La Figura 4 resume esta relación.

Cross Polarization

- Cross polarization discrimination defines how effectively an antenna discriminates between a signal with the correct polarization and one with the opposite polarization.
- Isolation of 20 to 40 dB is typical.
- Cross polarization can be used to great advantage when the two antennas belong to different links, such as at a hub. It can help minimize any potential interference that one link might cause to the other.

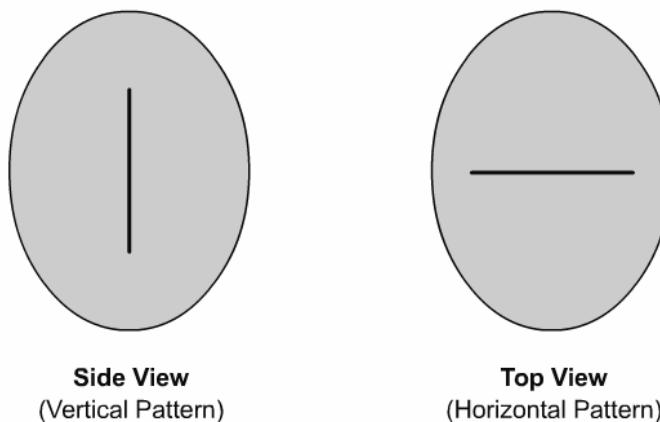
Figura 4

7.1.7 Patrones de emisión

El patrón de emisión es la variación de la intensidad del campo de una antena, como una función angular, con respecto al eje.

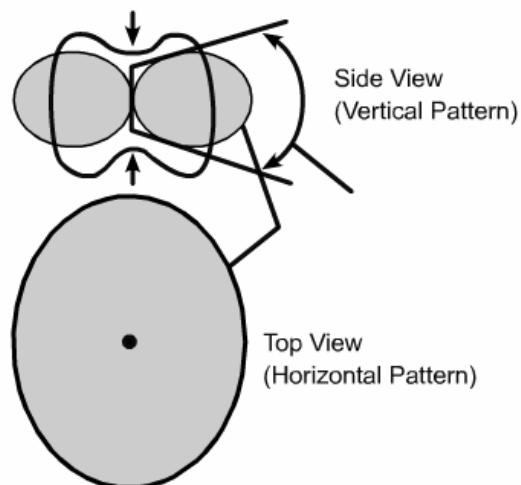
Todas las antenas son medidas contra lo que se conoce como una antena isotrópica, que es una antena teórica. Esta es la base para todas las otras antenas, como se muestra en la Figura 1. La cobertura de la antena isotrópica puede ser pensada como un globo que se extiende en todas direcciones por igual. Cuando una antena omnidireccional está diseñada para tener ganancia, la cobertura se pierde en ciertas áreas.

Imagine la presión en la parte superior e inferior de un globo. Esto causa que el globo se expanda en dirección hacia afuera, por lo que cubre más área en el patrón horizontal. También se reduce el área de cobertura por encima y por debajo del globo. Esto produce una ganancia más alta, ya que el globo, que representa a la antena, parece extenderse hacia un área de cobertura horizontal más grande. Esto puede verse en la Figura 2.



- A theoretical isotropic antenna has a perfect 360° vertical and horizontal beamwidth
- This is a reference for all antennas

Figura 1



- To obtain omni-directional gain from an isotropic antenna, the energy lobes are 'pushed in' from the top and bottom, and forced out in a doughnut type pattern.
- The higher the gain, the smaller the vertical beamwidth, and the larger the horizontal lobe area.
- This is a typical dipole pattern. Gain of a dipole is 2.14 dBi (0 dBd).

Figura 2

Recuerde que cuanto más alta es la ganancia, menor es el ancho del rayo vertical.

Algunos tipos importantes de antenas son los siguientes:

- Antena isotrópica - Esta es una antena hipotética que emite o recibe energía en forma igual en todas direcciones. Las antenas isotrópicas no existen físicamente, pero representan a antenas de referencia convenientes para expresar propiedades direccionales de las antenas físicas.
- Antena bipolar - Esta es normalmente una antena recta, de pie central y longitud de onda media, que está ilustrada en la Figura 3.
- Sistema de antenas - Este es un montaje de elementos de antena con dimensiones, espaciado y secuencia de iluminación dispuestos de tal forma que los campos de los elementos individuales se combinan. Esta combinación produce una intensidad máxima en una dirección en particular e intensidades de campo mínimas en otras direcciones.

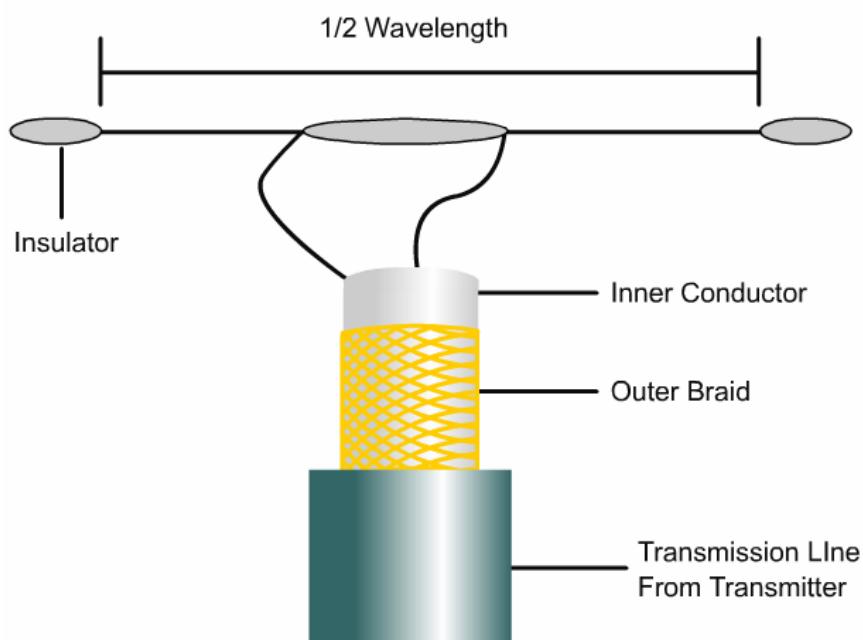


Figura 3

7.1.8 Diversidad

La diversidad es la operación simultánea de dos o más sistemas o partes de un sistema. La diversidad se utiliza para mejorar la confiabilidad del sistema. La desaparición de la multiruta puede causar fallas temporales en incluso las rutas mejor diseñadas. La diversidad es una solución posible para este problema. Existen dos tipos de diversidad como sigue:

1. Diversidad espacial
2. Diversidad de frecuencia

Con la diversidad espacial, el receptor de una radio de microonda acepta señales desde dos o más antenas que están separadas por muchas longitudes de onda. Esto está ilustrado en la Figura 1. La señal de cada antena es recibida y luego conectada en forma simultánea con las demás a un combinador de diversidad. Dependiendo del diseño, la función del combinador es seleccionar la mejor señal de sus entradas o sumar las señales entre ellas. La diversidad espacial es normalmente la primera elección para la protección del sistema, porque no requiere ancho de banda extra.

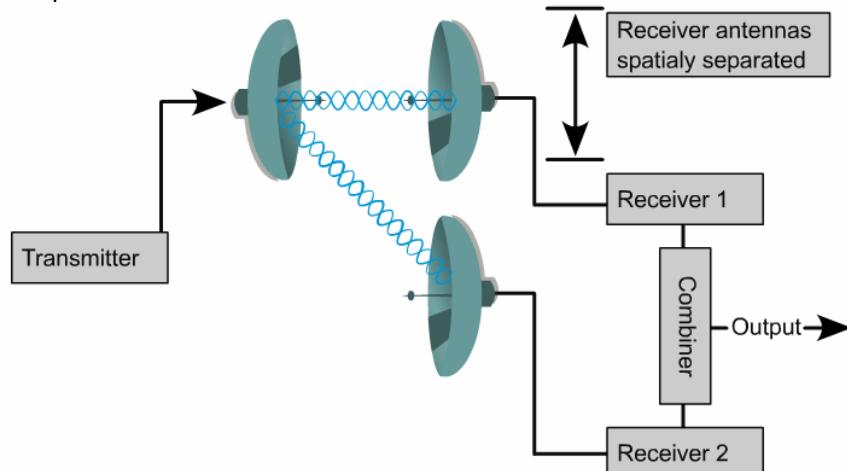


Figura 1

Con la diversidad de frecuencias, la señal de la información es transmitida en simultáneo por dos transmisores que operan en dos frecuencias diferentes, como lo muestra la Figura 2. Si la separación en frecuencias de los dos transmisores es grande, el desvanecimiento selectivo de frecuencias tendrá pocas probabilidades de afectar ambas rutas de la misma forma. Esto mejorará el rendimiento del sistema.

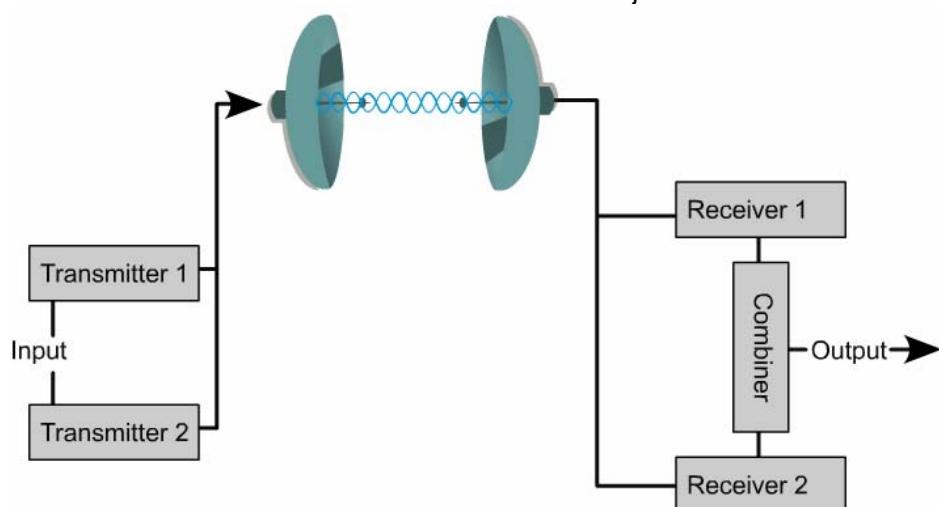


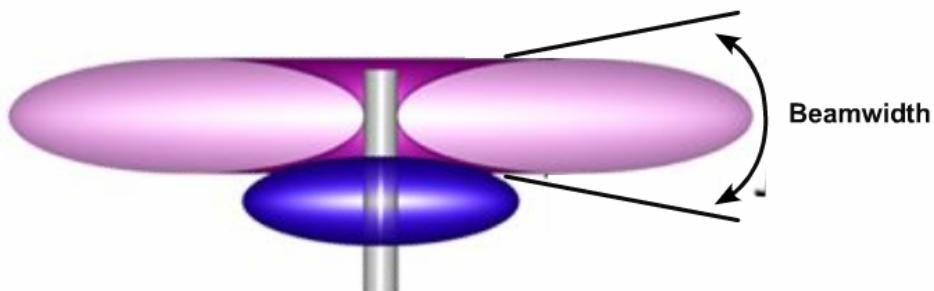
Figura 2

Los access points pueden tener dos antenas conectadas a ellos. Estas dos antenas son para diversidad en la recepción de la señal, no para aumentar la cobertura. Ellas ayudan a eliminar la ruta nula y a impedir que la RF sea recibida fuera de fase. Sólo una antena por vez está activa. Para una señal óptima, la antena activa es seleccionada en base al cliente. La selección sólo se aplica a ese cliente específico. El access point puede pasar de una a otra antena entre las dos cuando habla con diferentes clientes. Las tarjetas PCMCIA también tienen diversidad de antena incorporada en la tarjeta. Es posible desactivar la diversidad por medio de la configuración de los dispositivos, usando un access point o una tarjeta PCMCIA.

7.2 Antenas Omnidireccionales

7.2.1 Teoría

Toda elección de una antena involucra un equilibrio. Si se desea el alcance máximo, se debe resignar cobertura. No olvide que la cobertura es más que sólo horizontal. También hay un aspecto vertical. La mayoría de las antenas omnidireccionales resignan cobertura vertical para aumentar el alcance.



Area of poor coverage directly beneath the antenna.

- More Coverage area in a circular pattern
- Energy level directly above or below the antenna will become lower

Figura 1

La cobertura de la antena puede compararse con un globo. Si se presiona la parte superior e inferior del globo se obtiene un panqueque. Esto daría un ancho de rayo vertical muy angosto, pero una cobertura horizontal muy grande. Este tipo de diseño de antena puede atravesar distancias de comunicación muy largas. El diseño tiene una desventaja, que es una cobertura pobre abajo de la antena, como lo muestra la Figura 1. Con las antenas omnidireccionales de alta ganancia, este problema puede ser resuelto parcialmente diseñando algo llamado inclinación hacia abajo. Una antena que utiliza la inclinación hacia abajo está diseñada para emitir en un ángulo pequeño en lugar de en 90 grados desde el elemento vertical. Esto ayuda en la cobertura local, pero reduce la efectividad de la capacidad de largo alcance. Las antenas de celulares usan la inclinación hacia abajo. La Figura 2 muestra las diferentes antenas omnidireccionales de Cisco. La antena omnidireccional Cisco 12dBi tiene una inclinación hacia abajo de cero grados.

Cisco Omni-directional Antennas

- 2.2 dBi Dipole Antenna (standard rubber ducky)
- 2.2 dBi Ceiling Mount Antenna
- 5.14 dBi Mast Mount Vertical Antenna
- 5.14 dBi Ceiling Mount Antenna
- 5.14 dBi Pillar Mount Diversity Antenna
- 5.14 dBi Ground Plane Antenna
- 12 dBi High Gain Omnidirectional Antenna

Figura 2

7.2.2 Bipolar de 2.2 dBi "rubber ducky" estándar"

La antena bipolar rubber ducky es una antena bipolar estándar. Las antenas bipolares están ilustradas en las Figuras 1 y 2. También se la llama antena doblete. Es una antena omnidireccional adecuada para muchas aplicaciones. La antena es un conductor eléctrico recto. Las antenas bipolares pueden ser orientadas en forma horizontal, vertical o con una inclinación. Las antenas bipolares se suministran con algunos access points Cisco Aironet y dispositivos clientes.



Figura 1



Figura 2

7.2.3 2.2dBi de montura en cielo raso

La antena Cisco 2.2 dBi Omnidireccional de Montura en Cielo Raso está ilustrada en la Figura 1. Está diseñada para ser montada en la grilla de metal de un cielo raso suspendido. Esta antena es más agradable estéticamente que la rubber ducky.

La antena de montura en cielo raso es sólo para aplicaciones interiores y debería ser montada con el extremo del orificio del tornillo apuntando hacia el cielo raso. No es una buena elección para escuelas, hospitales u otras instalaciones de gran tráfico con cielos rasos bajos. Esto es porque la antena tiende a ser golpeada y posiblemente dañada. Esta antena está polarizada verticalmente, pero tiene un rayo ligeramente inclinado hacia abajo. Esto permite que su patrón de cobertura cubra las áreas por debajo del cielo raso.



Figura 1

Esta antena es muy similar en apariencia a la 5.14 dBi Omni de Montura en Cielo Raso, sólo que es más corta y tiene menos ganancia.

7.2.4 5.14 dBi vertical de montura en mástil

La antena 5.14 dBi Omnidireccional Vertical de Montura en Mástil está diseñada para ser sujetada a un mástil o poste. La base de la antena tiene una sección de aluminio que le da suficiente fuerza como para resistir ser sujetada. Esta antena se entrega con una abrazadera y una banda de fricción de aluminio para la montura. Se debe proporcionar un mástil separado en el cual sujetar la antena.



La antena de montura en mástil está diseñada para aplicaciones industriales. En aplicaciones exteriores, el extremo del cable de la antena debe ir hacia abajo. En aplicaciones interiores, el extremo del cable deberá mirar hacia el cielo raso.

7.2.5 5.14 dBi montura en cielo raso

La antena Cisco 5.14 dBi Omnidireccional de Montura en Cielo Raso, mostrada en la Figura 1, está diseñada para ser montada en la grilla de metal de un cielo raso suspendido.

Más agradable estéticamente que la versión de montura en mástil, esta antena es sólo para aplicaciones interiores. Debería ser montada con el orificio del tornillo apuntando hacia el cielo raso. Esta antena no es una buena elección para escuelas u hospitales que tienen cielos rasos bajos. Esto es porque la antena tiende a ser golpeada y posiblemente dañada. Esta antena está polarizada verticalmente, pero tiene un rayo ligeramente inclinado hacia abajo. Esto permite que su patrón de cobertura cubra las áreas por debajo del cielo raso. El patrón de emisión se muestra en la Figura 2.



Figura 1

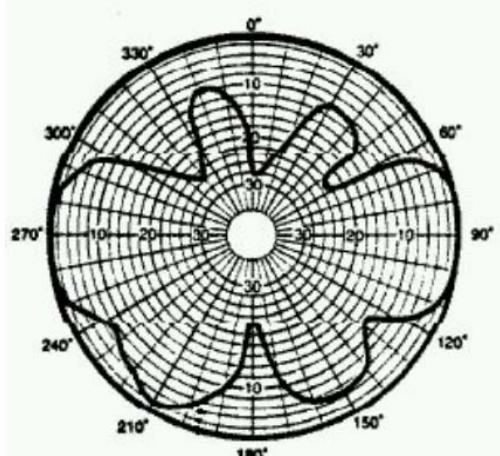


Figura 2

7.2.6 5.14 dBi diversidad de montura en pilar

La Cisco 5.14 dBi Omni de Diversidad de Montura en Pilar está diseñada para ser montada en el costado de un pilar. La Figura 1 muestra un paquete con dos antenas en él. Están envueltas con tela para que se vea más como un parlante que como una antena. Esta antena tiene dos coletas con dos conectores RP-TNC. No es necesario comprar dos de éstas para un AP. Simplemente se conectan a los dos puertos RP-TNC del access point los dos conectores de la antena de montura en pilar. Esta antena es usada sólo para aplicaciones interiores. Viene con dos abrazaderas que facilitan montarla en un pilar.



Figura 1

7.2.7 5.14 dBi plano del piso

La antena omnidireccional 5.14 ddBi Plano del Piso se muestra en la Figura 1. Está diseñada para ser instalada en un cielo raso y que apunte directamente hacia abajo. Tiene un plato de refuerzo de aluminio incorporado para enfocar la energía de la transmisión hacia abajo. Esta antena es una muy buena elección para los cielos rasos suspendidos. Cuando se instala la antena, se realiza un orificio del tamaño suficiente como para que el mástil de la antena sea pasado a través de la placa del cielo raso. El plato de refuerzo se extenderá encima de la placa del cielo raso con sólo una pequeña porción del mástil de la antena sobresaliendo por debajo de la placa del cielo raso. Esto crea una instalación plana y limpia, mientras que proporciona una cobertura total. Esta antena se utiliza sólo en aplicaciones interiores. Hay un orificio de 6.35 mm (0.25 pulgadas) en el plato de refuerzo, lo que permite que la antena sea atornillada para diferentes necesidades de monturas.



Figura 1

7.2.8 12 dBi omnidireccional (sólo largo alcance)

La antena de 12 dBi, mostrada en la Figura 1, es sólo para aplicaciones exteriores de largo alcance. Esta antena podría ser usada en el centro de una configuración de bridging punto a multipunto. También podría ser usada en un área central, ya que proporciona conexiones de alcance mayor a un access point. La antena, como todas las antenas sólo para exterior, tiene una coleta corta de coaxial de 30.48 cm (12 pulgadas), lo que hace necesario el usar cables de extensión de antena.



Figura 1

Esta antena se entrega con un conjunto de tornillos U y abrazaderas de fricción. La antena debe ser montada en un mástil sólido. La base de la antena tiene una sección de metal, lo que le da suficiente fuerza

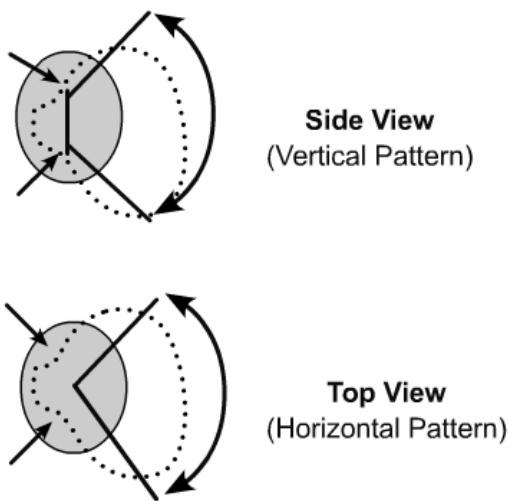
como para soportar ser sujetada. Esta antena está polarizada verticalmente y debe ser montada perpendicular al suelo con la coleta en la parte inferior. Tiene una extensión del rayo de más o menos 3,5 grados desde la perpendicular.

7.3 Antenas Direccionales

7.3.1 Teoría

Para una antena direccional, la energía es dirigida en una dirección común, como muestra la Figura 1. Las antenas direccionales son llamadas también no isotrópicas.

Para visualizar la forma en que una antena direccional funciona, imagine una linterna de rayo ajustable. Es posible cambiar la intensidad y el ancho del rayo de luz moviendo el reflector trasero y dirigiendo la luz, en ángulos más angostos o más anchos. A medida que el rayo se hace más ancho, su intensidad en el centro decrece, y viaja una distancia más corta.



- For directional antennas the lobes are pushed in a certain direction, causing the energy to be condensed in a particular area.
- Very little energy is in the backside of a directional antenna.

Figura 1

Lo mismo es cierto para una antena direccional. La misma cantidad de potencia llega a la antena. Sin embargo, el diseño de la antena puede reflejar y dirigir la energía RF en ondas más estrechas y fuertes o en ondas más amplias y menos intensas, igual que con la linterna.

Las diferentes antenas direccionales de Cisco están ilustradas en la Figura 2.

Directional Antennas

- 6dBi Patch Antenna - 65 degree
- 8.5dBi Patch Antenna - 60 degree
- 13.5dBi Yagi Antenna - 25 degree
- 21dBi Parabolic Dish Antenna - 12 degree

Figura 2

7.3.2 Antenas patch

Una antena patch, mostrada en la Figura 1, proporciona una cobertura excelente con un patrón amplio de radiación. La antena patch Cisco 6 dBi es común para aplicaciones no europeas que necesitan un área amplia de cobertura. Si es aceptable un área de cobertura ligeramente más limitada, la antena Cisco 8.5 dBi proporciona ganancia y distancia adicionales.



Figura 1

La antena patch es excelente para aplicaciones interiores y exteriores, cuando está correctamente montada. Es posible montarla en una variedad de superficies, usando orificios en el perímetro de la antena.

7.3.3 Antena yagi de 13.5 dBi – 25 grados

Una antena yagi, mostrada en la Figura 1, es una antena direccional de alta ganancia. La Yagi está construida con al menos tres elementos, que son barras de metal que suplementan la energía de onda transmitida. En una antena Yagi, hay al menos un elemento conducido, un elemento reflector y normalmente uno o más elementos directores. La antena Yagi también es conocida como una antena lineal de radiación longitudinal o un sistema Yagi-Uda. Los elementos pueden verse en la Yagi descubierta de la Figura 2.



Figura 1

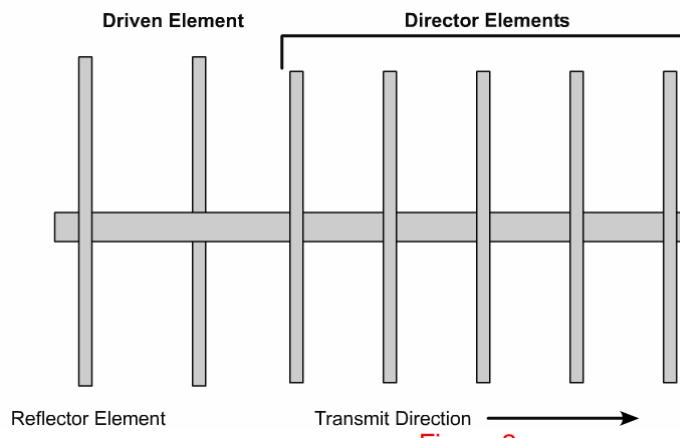


Figura 2

Las antenas Yagi son direccionales y están diseñadas para comunicaciones de larga distancia. Una Yagi es normalmente más pequeña, liviana y barata que una antena de plato. Una yagi es excelente para aplicaciones exteriores y para algunas aplicaciones interiores. La Yagi de Cisco proporciona 13.5 dBi de ganancia y ofrece un rango de hasta 10 km (6.5 millas) a 2 Mbps, y 3.2 km (2 millas) a 11 Mbps. La mayoría de las antenas Yagi son montadas con tornillos U a un mástil macizo.

7.3.4 Antena de plato parabólico de 21 dBi – 12 grados

Un plato parabólico sólido, mostrado en la Figura 1, puede permitir a las WLANs trabajar sobre grandes distancias. Tiene un ancho de rayo angosto, y dependiendo de la velocidad y de la ganancia de la antena usada, pueden ser posibles distancias de hasta 40 km (25 millas). Es importante evaluar cuán bien soportará el plato las condiciones de mucho frío y los grandes vientos. Igualmente importante es la solidez del mástil y de la torre donde la antena será montada.



Figura 1

Una antena de plato puede exceder las limitaciones de potencia del FCC de EE.UU., como se muestra en la Figura 2.

FCC Part 15 Antenna Requirements

802.11b Antenna

- Must use a unique or proprietary connector
- Cisco Aironet products use RP-TNC connector

Part 15 Standards

- Approved antenna may exceed
- Exceeding may lead to interference problems
- Penalties could result in fines
- FCC standards apply to part 15 users in the United States

Different countries will have similar standards

Figura 2

7.3.5 Antenas de 5 GHz integradas

Con soporte simultáneo para radios de 2.4 GHz y de 5 GHz, la Serie Cisco Aironet 1200 preserva las inversiones existentes de IEEE 802.11b y proporciona una ruta de migración hacia las tecnologías futuras IEEE 802.11a e IEEE 802.11g. Su diseño modular soporta configuraciones de banda única y dual, más la capacidad de actualización de campo para cambiar estas configuraciones a medida que las necesidades cambian y las tecnologías evolucionan. La protección de la inversión se proporciona además gracias a una gran capacidad de almacenamiento y soporte para las herramientas de administración de Cisco, brindando la capacidad y los medios para actualizar el firmware y para ofrecer nuevas características a medida que se hacen disponibles. El módulo tiene 2 pares de antenas de diversidad. El primer par es para utilizar como patch de diversidad y el segundo par es para usar como omni de diversidad. Como se muestra en la Figura 1, cuando el módulo está horizontal contra el armazón del Access Point Serie 1200, las antenas patch están activadas. Cuando el módulo está vertical desde el armazón del Access Point Serie 1200, las antenas omni están activadas.

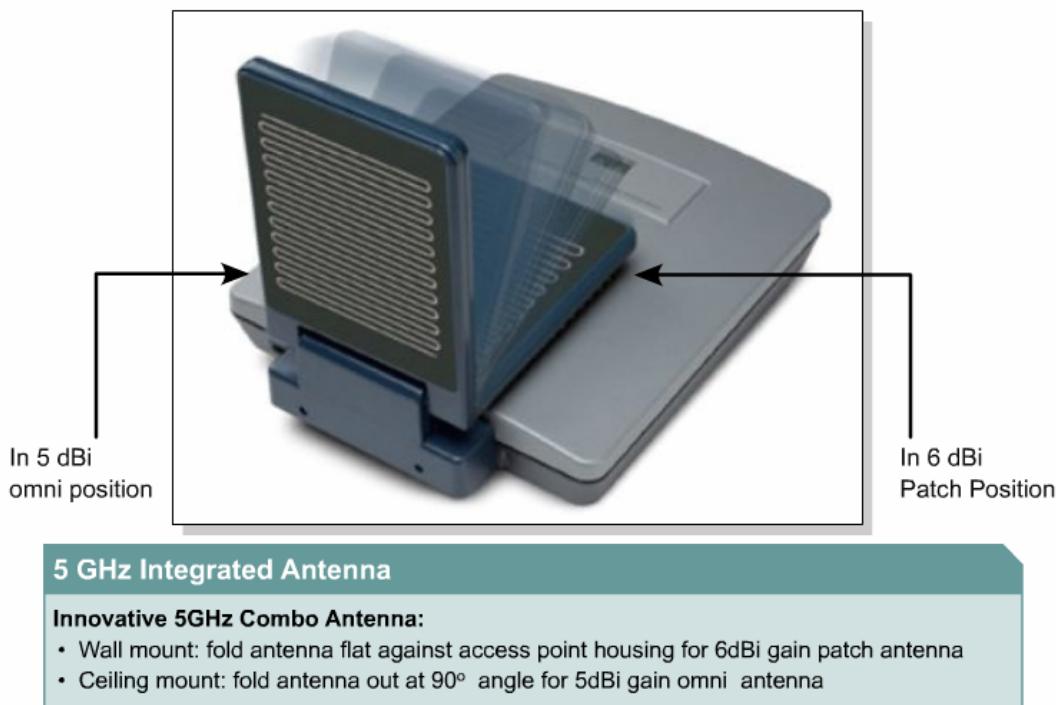


Figura 1

La omni tiene una ganancia de 5 dBi y un patrón de 360 grados. La patch tiene una ganancia de 6 dBi y un patrón de 180 grados. No hay conexión desde la radio de 5 GHz a los puertos de antena RP-TNC de 2.4 GHz.

7.3.6 Antenas integradas de 2.4 GHz

El bastidor del Access Point Cisco Aironet Serie 1100 permite que el usuario final actualice la radio Mini-PCI de 802.11b a 802.11g en el futuro. Simplemente debe quitar un tornillo de la parte trasera del Cisco Aironet Serie 1100 para acceder a la Radio Mini-PCI. Luego debe sacar la radio 802.11b y reemplazarla por una radio 802.11g. El procedimiento es similar al proceso de sacar e instalar módulos de memoria de una computadora.

Los usuarios finales no podrán actualizar las antenas del Cisco Aironet Serie 1100 porque utiliza una antena cautiva. Una antena cautiva es una antena que está integrada al access point para proporcionar facilidad de instalación y diseño de WLAN. La antena omnidireccional de 2.2 dBi está diseñada para proporcionar diversidad de antena para ayudar a combatir la distorsión multiruta. Las antenas del Access Point Cisco Aironet Serie 1100 proporcionan un rendimiento de cobertura comparable a un par de antenas rubber ducky de 2.2 dBi.

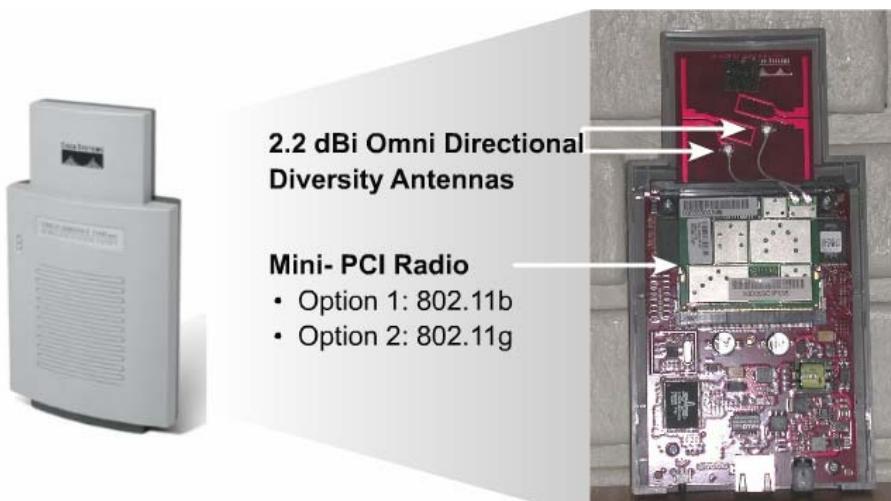


Figura 1

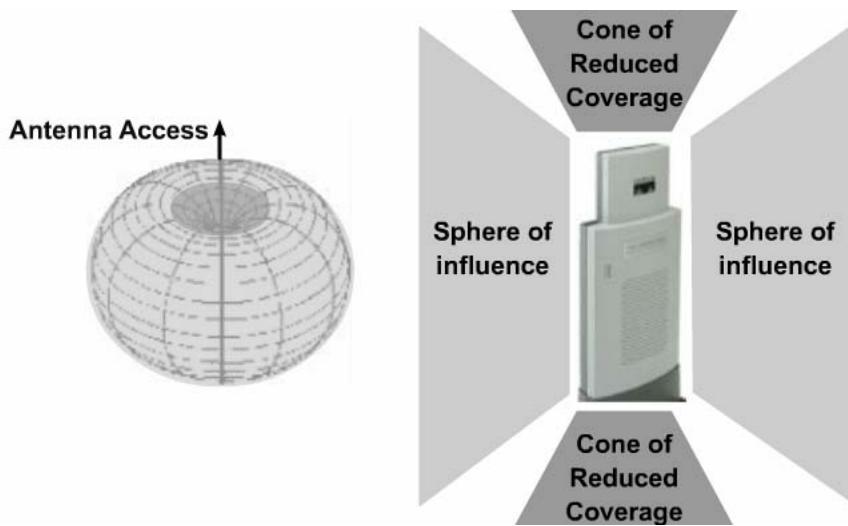


Figura 2

Se debe considerar la propagación de RF de la antena cuando se selecciona un sistema de antenas para cualquier dispositivo WLAN. Como el Access Point Cisco Aironet Serie 1100 utiliza una antena omnidireccional de 2.2 dBi cautiva, el instalador necesita estar consciente de que el cono de cobertura reducida está directamente por encima y por debajo del Access Point (zona roja). Un usuario final ubicado en el cono de cobertura reducida experimentará una conectividad pobre con el access point. Como lo muestra la Figura 2 los usuarios finales ubicados en la esfera de influencia (zona verde) experimentarán una mejor conectividad con el access point.

El Access Point Cisco Aironet Serie 1100 ha sido diseñado para diferentes opciones de montura de uso (p.e.) escritorio, pared, cubículo y cielo raso. Para que la antena del Cisco Aironet Serie 1100 funcione en forma confiable en todas las orientaciones de la montura, fue diseñada para producir una esfera de influencia más fuerte que la de un par de antenas rubber ducky de 2.2 dBi.

Los patrones de propagación de RF son útiles para ayudar a los diseñadores de WLAN a "ver" cómo la energía de RF se propaga desde la antena. Los patrones del Cisco Aironet Serie 1100 mostrado en la Figura 3 señalan el Plano Horizontal (H-Plane) y el Plano de Elevación (E-Plane) de la antena. El H-Plane muestra cómo se propaga la energía RF mirando hacia abajo desde la parte superior de la antena. En el ejemplo de H-Plane mostrado en la Figura 3 la antena tiene un patrón de cobertura horizontal de 360 grados.

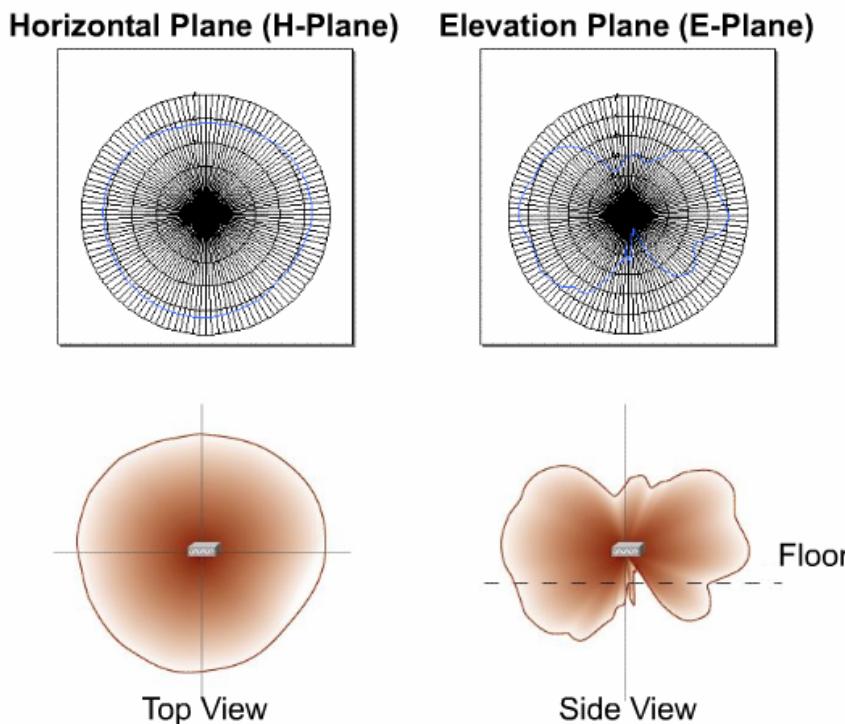


Figura 3

El E-Plane muestra cómo la energía RF se propaga mirando a la antena de costado. Este ejemplo de E-Plane muestra la esfera de influencia y el cono de cobertura reducida para la antena. Con respecto al E-Plane, como una rosquilla cortada por la mitad muestra la forma de rosquilla, el E-Plane muestra la forma de la propagación de RF producida por la antena.

7.4 Cables y Accesorios

7.4.1 Selección de cables

Los tipos de cables de antena son mostrados en la Figura 1. Es importante mantener el cable de la antena corto para maximizar el alcance. Esto es cierto, sea que se instale un access point interior o sea que se instalen bridges para comunicarse sobre una gran distancia. Esto es así porque un cable largo atenuará la señal y reducirá el alcance confiable del equipo. La distancia máxima sobre la que dos bridges pueden comunicarse depende de las combinaciones de antena y cable que se utilicen. Una herramienta que ayuda en los cálculos de distancia está en la lista de recursos Web de abajo.

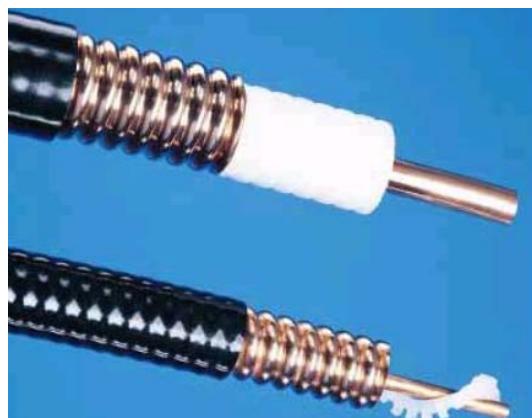


Figura 1

Puede ser posible utilizar el cable coaxial existente. Esta determinación dependerá de la calidad del cable y si cumple con las tres especificaciones siguientes:

1. La impedancia debe ser de 50 ohms.
2. La pérdida total a 400 MHz, para la longitud total del cable, debe ser de 12 dB o menos.
3. El tamaño del conductor central del cable debe ser #14 AWG, o mayor.

Si las especificaciones no concuerdan, no utilice el cable. En muchos casos, un cable sin usar fue un cable problemático que perteneció a alguien. Si existe cualquier duda acerca del cable, instale un cable coaxial nuevo.

7.4.2 Pérdida del cable

La cantidad de energía perdida en el cable se llama pérdida del cable. El uso de cable coaxial para transportar energía RF siempre produce alguna pérdida de fuerza de la señal. La dimensión de la pérdida depende de los cuatro factores siguientes:

1. Longitud: Los cables largos pierden más potencia que los cables cortos.
2. Grosor: Los cables delgados pierden más potencia que los cables gruesos.
3. Frecuencia: Las frecuencias más bajas de 2.4 GHz pierde menos potencia que las frecuencias superiores a 5 GHz, como se muestra en la Figura 1.
4. Materiales del cable: Los cables flexibles pierden más potencia que los cables rígidos.

Cable Type	400 MHz Loss (dB/100 ft.)	2.5 GHz Loss (dB/100 ft.)	5.8 GHz Loss (dB/100 ft.)
LMR 400	2.6	6.8	10.8
LMR 600	1.62	4.45	7.25
1/2" Heliax	2.25	5.7	10.5

Figura 1

La pérdida del cable no depende de la dirección en que viaja la señal. Las señales transmitidas pierden el mismo porcentaje de fuerza que las señales recibidas. La energía perdida se libera como calor.

Curiosamente, los bajos niveles de potencia de las WLANs hacen que el calor del cable sea casi indetectable.

7.4.3 Conectores y divisores de cables

Conectores

Las antenas Cisco utilizan el conector TNC de Polaridad Reversa [Reverse-polarity TNC (RP-TNC)], como lo muestra la Figura 1. Las Figuras 2 y 3 muestran vistas de cortes laterales de la ficha y el conector RP-TNC. La Figura 4 muestra las especificaciones para ambos.



Figura 1

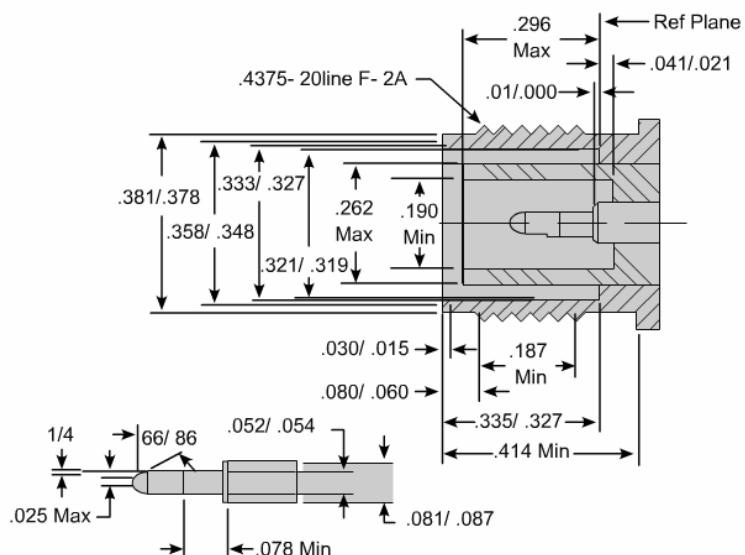


Figura 2

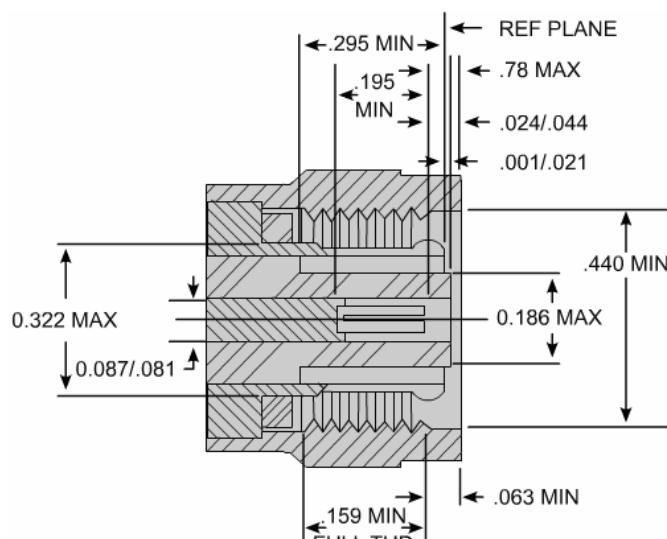


Figura 3

Specifications for the RP-TNC Connectors	
Connector - TNC Plug	
• Part Number: 31-5677	
• Description: Reverse Polarity TNC RG58 Plug	
• Product Line: RP-TNC	
• Plating/Insulator Codes: P15/D1	
Base Connector - TNC Jack	
• Part Number: 31-5678	
• Description: Reverse Polarity TNC RG58 Jack	
• Product Line: RP-TNC	
• Plating/Insulator Codes: P15/D1	

Figura 4

Divisores

Un divisor permite que una señal sea usada con dos antenas al mismo tiempo. El usar dos antenas con un divisor puede proporcionar más cobertura. El uso de un divisor agrega aproximadamente 4 dB de pérdida. Un divisor de 5 GHz normalmente es incompatible con un divisor de 2.4 GHz. Revise las especificaciones técnicas de un divisor específico para las mediciones exactas.

7.4.4 Amplificadores

La FCC de EE.UU. tiene leyes que limitan el uso de amplificadores con una WLAN. Un amplificador sólo puede ser usado si es vendido como parte de un sistema. Esto significa que el AP, el amplificador, el cable de extensión y la antena son todos vendidos como un sistema. Estas leyes ayudan a asegurar que los amplificadores estén probados con ciertos productos y legalmente comercializados y vendidos.

Exteriores

La resolución de la FCC de EE.UU. está diseñada para evitar que los instaladores agreguen un amplificador e interfieran con otros usuarios del espectro inalámbrico. La interferencia desde equipos configurados en forma incorrecta es un gran problema en un área metropolitana. Tenga presente las leyes locales y los otros sistemas en el área, que pueden ser afectados por un amplificador.

La Figura 1 ilustra un ejemplo de un amplificador montado polar bidireccional exterior a prueba de agua para usar con radios de 2.4 GHz de Amplio Espectro y equipo WLAN. El dispositivo tiene un pre-amplificador receptor de bajo ruido y un amplificador de potencia de transmisión.



Figura 1



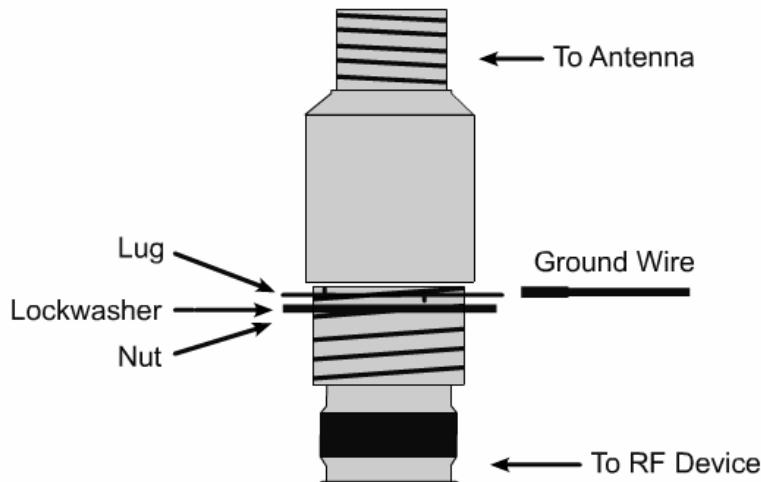
Figura 2

Interiores

Cuando se instalan equipos en interiores, es preferible instalar un access point adicional en lugar de instalar un amplificador. En raras circunstancias un amplificador puede ser necesario en interiores. Se debe tener cuidado para evitar interferir con usuarios del espectro inalámbrico cercanos. Algunos amplificadores que se venden hoy están certificados con líneas de productos enteras, que incluyen a todos los APs, cables y antenas. La Figura 2 muestra un amplificador bidireccional de interior para usar con un modem de radio de 2.4 GHz de Amplio Espectro y equipo WLAN. Como el amplificador de exterior, tiene un pre-amplificador receptor de bajo ruido y un amplificador de potencia de transmisión.

7.4.5 Pararrayos

Un pararrayos está diseñado para proteger a los dispositivos WLAN de la electricidad estática y de los rayos. Es similar en su función a una válvula de seguridad en una caldera de vapor. Un pararrayos evita que picos de energía lleguen al equipo derivando la corriente hacia la tierra. Un pararrayos es mostrado en la Figura 1.



- Designed to protect LAN devices from static electricity and lightning that travel on coax transmission lines.
- Good for both 900 MHz and 2.4 GHz systems.
- RP-TNC connectors used on all Cisco antennas

Figura 1

Un pararrayos tiene dos propósitos principales:

1. Desagotar cualquier carga alta de estática que se acumule en la antena, lo que ayuda a evitar que la antena atraiga el golpe de un rayo.
2. Disminuir o disipar cualquier energía que se haya introducido en la antena o el coaxial, que viene desde un rayo caído en las cercanías.

La parte más importante de la instalación de un pararrayos es instalar una descarga a tierra apropiada, que disipará el exceso de energía. Esto se realiza normalmente usando una varilla de tierra. Una varilla de tierra es un asta de metal clavada en la tierra, normalmente a una profundidad de al menos 2.44 m (8 pies). Las varillas de tierra pueden estar hechas de materiales que sean o no de hierro. Cuando una varilla de tierra está hecha de hierro o acero, que son metales ferrosos, necesita tener un grosor al menos de 15.9 mm (0.63 pulgadas). Las varillas no ferrosas deben estar libres de materiales no conductores incluyendo pintura. Debe tener un grosor mayor a 12.7 mm (0.5 pulgadas).

La electricidad seguirá el camino con la menor resistencia para llegar a tierra. La mayoría de los códigos piden un sistema de tierra de 25 ohms o menos. Se puede utilizar un medidor de tipo pinzas para medir la resistencia de las varillas de tierra. Si un único electrodo no cumple con los requisitos de tierra, se pueden agregar electrodos adicionales. Si se instalaron múltiples electrodos para cumplir con estos requisitos, deberían estar separados entre sí al menos 1.83 m (6 pies).

7.5 Ingeniería del Enlace y Planificación de la Ruta de RF

7.5.1 Descripción General

La instalación de redes inalámbricas requiere el mismo planeamiento básico que para cualquier red cableada. La principal diferencia es que debido a la naturaleza de la señal inalámbrica, se necesita algún planeamiento adicional. Este planeamiento incluye la elección del sitio y el análisis de la ruta de RF. También puede ser necesario investigar las leyes zonales locales, además de las regulaciones gubernamentales, cuando se deben levantar torres. El planeamiento de un enlace inalámbrico comprende la

recolección de información haciendo un estudio del sitio físico y la toma de decisiones. Estas tareas de ingeniería del enlace están descriptas en la Figura 1.

- Raise the antenna mounting point
- Build a new structure i.e. a radio tower, tall enough to mount the antenna
- Increase the height of an existing tower
- Locate a different mounting point, for the antenna
- Cut down problem trees

Figura 1

Cuando diseña una conexión edificio a edificio, no olvide la zona Fresnel. La Figura 2 muestra algunos detalles importantes acerca de la línea de visión y la zona Fresnel. La zona Fresnel es un área elíptica que rodea directamente la ruta visual, como se ilustra en la Figura 3. Varía dependiendo de la longitud de la ruta de la señal y de la frecuencia de la señal. La zona Fresnel puede ser calculada, y debe ser tomada en cuenta cuando se diseña un enlace inalámbrico. La Figura 4 muestra algunas formas de mejorar el efecto Fresnel.

Line of Sight and the Fresnel Zone

- Microwave signals travel in a straight line, but they spread as they travel.
- The required beam clearance is called the Fresnel Zone.
- The Fresnel Zone is an imaginary ellipsoid, which surrounds the linear path between the antennas.
- The required Fresnel Zone clearance is greatest at mid-path and diminishes near each antenna site.
- The Fresnel zone thickness, or girth, is a function of path length. The longer the path, the broader the Fresnel zone.
- The antennas must be high enough, to allow for the first Fresnel zone to clear the hills, earth bulge, buildings or trees.

Figura 2

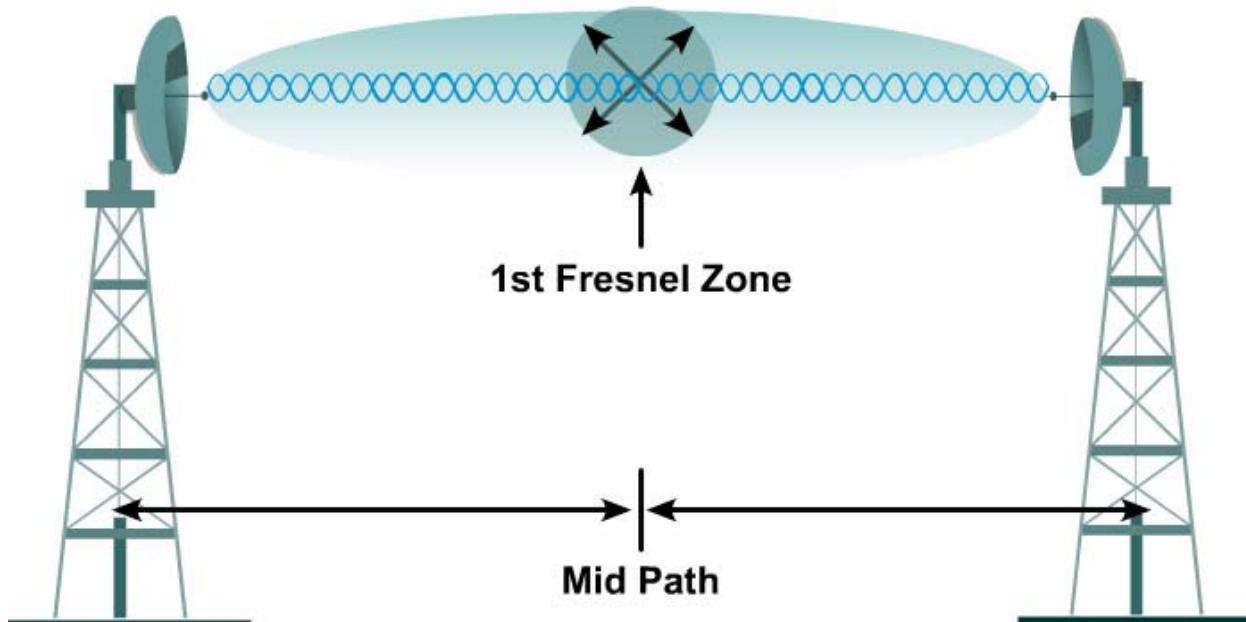


Figura 3

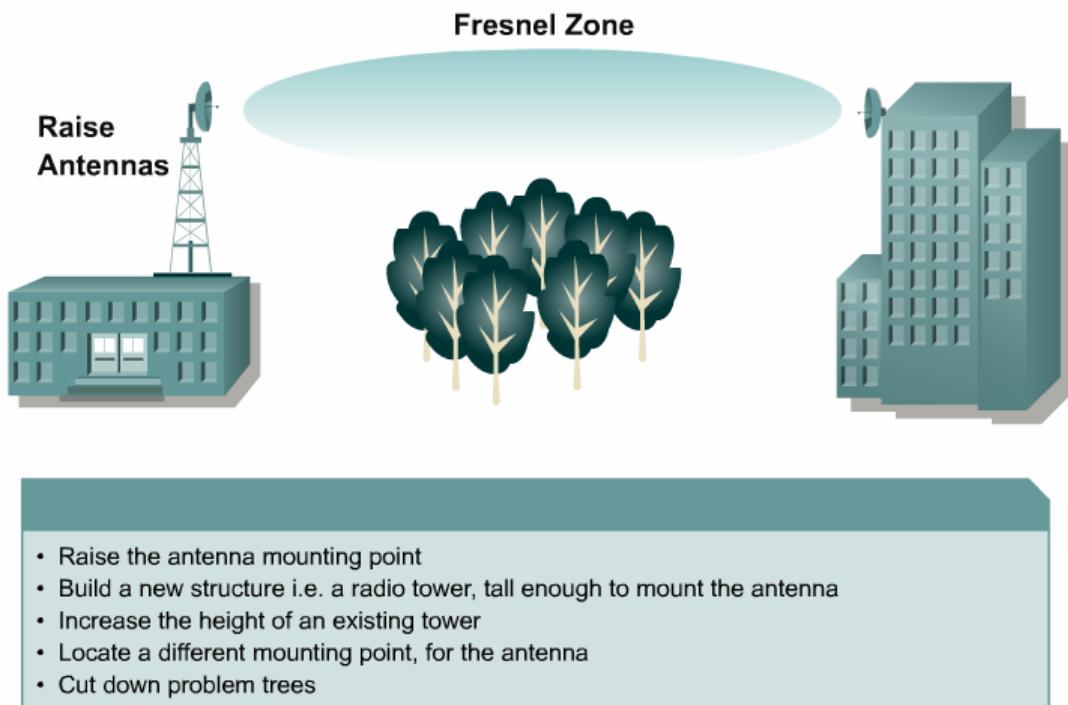


Figura 4

Las siguientes herramientas pueden ser útiles para realizar una alineación precisa:

- Globo: La soga deberá estar marcada a intervalos de tres metros (diez pies), para que se pueda establecer una altura. Este valor ayudará a determinar la altura general de la torre o mástil necesario, como se muestra en la Figura 5.
- Binoculares o un telescopio: Estos son necesarios para los enlaces más distantes. Recuerde que el globo debe ser visible desde el sitio remoto.
- GPS: Para enlaces de radio muy distantes, esta herramienta permite al instalador apuntar las antenas en la dirección correcta.
- Luz estroboscópica: Esta puede ser usada en lugar del globo. Use esto de noche para determinar dónde alinear la antena y a qué altura.

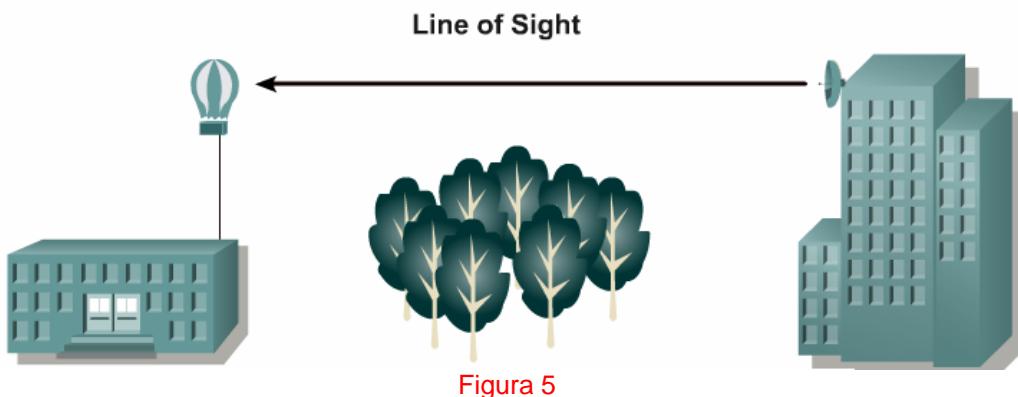


Figura 5

Una consideración importante en un diseño edificio a edificio es la zona Fresnel, que podemos imaginar como la línea de visión. Para las WLANs, la línea de visión es más que una línea directa entre las dos antenas. La línea de visión es más una elipse que está libre de obstáculos, y debería tener en cuenta el crecimiento futuro de los árboles.

A causa de la elipse de la zona Fresnel, las antenas deben ser montadas lo suficientemente altas como para asegurar que haya un espacio libre en el punto medio de la zona Fresnel.

7.5.2 Elevación de la Tierra

La curvatura de la Tierra se convierte en un problema para los enlaces mayores a 11 km (7 millas). La línea de visión desaparece a los 25 km (16 millas). Por lo tanto, la curvatura de la Tierra debe ser considerada

cuando se determina la altura de la montura de la antena, como se indica en la Figura 1. Para evitar la obstrucción de la curvatura de la Tierra, las antenas deben ser erigidas más alto sobre el suelo que si la Tierra fuera plana. La Figura 2 ilustra esto.

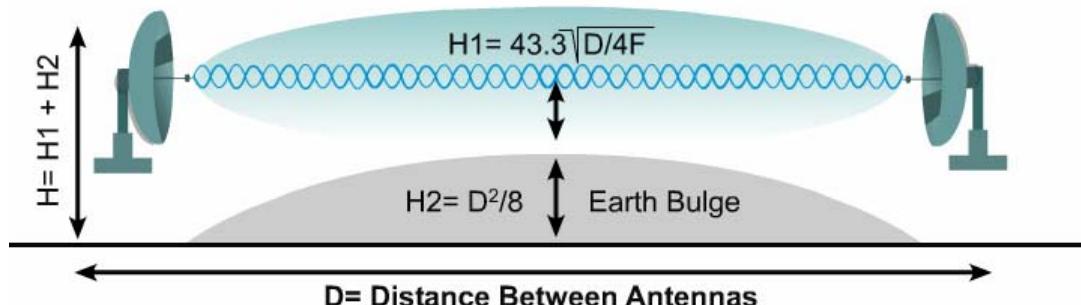
Additional Antenna Height for Earth Bulge

- The longer the path, the greater the additional antenna height needed.
- Calculate the additional height using the following formula:

$$\text{Added Height} = D^2 / 8$$

Where D is the Path Distance, in miles, and Added Height is in feet.

Figura 1



- H_1 = added antenna height for fresnel zone clearance
- H_2 = added antenna height for earth bulge clearance
- Where D is the path length in miles

Figura 2

7.5.3 Estudio del sitio y perfil de la ruta

El estudio del sitio de la antena es una operación detallada, como lo indica la Figura 1. Una vez que el estudio del sitio de la antena está hecho y la ruta propuesta tiene una adecuada línea de visión, el paso siguiente es el perfil de la ruta. La Figura 2 muestra los objetivos importantes del perfil de la ruta. Después de que el perfil de la ruta está hecho, se debería hacer un análisis de la ruta. Un análisis de la ruta prevé las peores obstrucciones potenciales para hacer una instalación confiable, como lo muestra la Figura 3. Se necesita información precisa acerca del equipo inalámbrico y de las antenas para calcular la fuerza realista de la señal. Una vez que la fuerza de la señal es calculada, se pondera los efectos dañinos de la distancia, el terreno, el clima y las condiciones climáticas de la ruta. Cuando los efectos perjudiciales causen que la señal se atenúe o se desvanezca demasiado, el receptor de microondas se volverá poco confiable.

Antenna Site Survey Planning Tasks

- Topography of the path
- Possible obstructions
- Proximity of site to airports
- Building or tower heights
- General site layout
- Site access
- Antenna location and mounting antenna height
- Lightning grounding
- Cable path to equipment
- Distance between antenna and indoor equipment
- Equipment room layout
- Power availability
- GPS coordinates of the sites

Figura 1

Path Profiling to Find Possible Obstructions

- Plot the coordinates on a topographical map or enter them in path profiling software with terrain database for the region.
- Check for any possible obstructions in the path.
- Calculate the distance between the sites.
- Possibly ride along the path to look for obstructions.
- Get the coordinates of the obstruction.

Figura 2

Ensure Reliable Operation with Path Analysis

- Determine the theoretical system performance along the proposed path.
- Consider wind, rain, fog, and atmospheric absorption.
- Select proper antenna and coaxial cable for required fade margin and availability.

Figura 3

El uso de una antena de más alta ganancia y un cable de menor pérdida puede aumentar el nivel de la señal y mejorar el rendimiento general del sistema. Sin embargo, las regulaciones locales acerca de la máxima Potencia Efectiva Isotrópica Radiada [Effective Isotropic Radiated Power (EIRP)] deberían ser seguidas al seleccionar un tipo de antena y de cable coaxial. EIRP es la suma de la potencia de transmisión y la ganancia de la antena menos las pérdidas del cable.

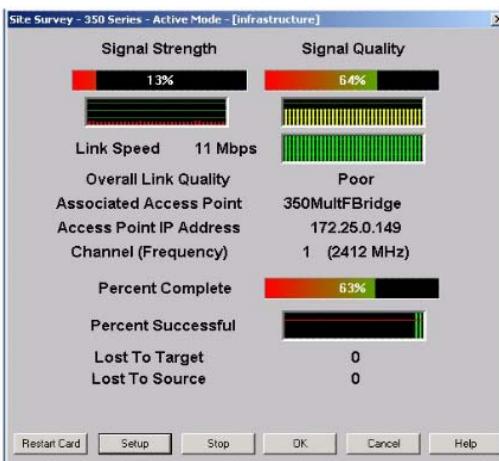
7.5.4 Alineación e interferencia

Cuando alinee las antenas, asegúrese de que las dos antenas del enlace no tengan polaridad cruzada. Luego, asegúrese de que cada antena esté alineada para maximizar el nivel de la señal recibida. Como lo muestra la Figura 1, se proporciona una herramienta de fuerza de la señal recibida, que da una lectura del nivel de la señal recibida. En un extremo del enlace por vez, la dirección donde apunta la antena es cuidadosamente ajustada para maximizar o hacer que llegue a su punto más alto la lectura en la herramienta indicadora de señal.

Después de que esto esté hecho en ambos extremos, es muy importante obtener el nivel de la señal real recibida, en dBm. Esto es para verificar que esté entre 0 y 4 dB del valor obtenido en el cálculo del presupuesto del enlace. Si los valores medidos y calculados difieren en más de 8 dB, controle la alineación de la antena, y luego busque un defecto en el sistema de la línea de transmisión de la antena. Una ruta de enlace inalámbrico que atraviesa la ruta de otro enlace no causará interferencia. Esto es porque cualquier tipo de señal de radio o de otra señal electromagnética que se propaga a través del espacio o del aire no será afectada por ninguna otra señal que cruce el mismo punto en el espacio. Esto puede ser demostrado usando dos linternas. Ilumine una pared con una linterna. Sostenga la otra linterna a cierta distancia de la primera, pero apúntela como para que los dos rayos se crucen. Observe que el rayo de la segunda linterna no tiene efecto sobre el punto en la pared de la primera linterna. Lo mismo es cierto para las señales de radio de cualquier frecuencia. Si la segunda linterna se apunta hacia el mismo punto en la pared, el punto parecerá más brillante. De la misma manera, si los rayos fueran señales de radio de la misma frecuencia, y si el punto en la pared fuera una antena receptora para uno de los enlaces, el segundo rayo probablemente causaría interferencia. Sin embargo, observe que esta es una situación diferente que cuando los rayos se cruzan en el espacio.

Una ruta de enlace inalámbrico normalmente no es afectada por las líneas de servicios públicos que corren perpendicularmente a través de ella. Esto es porque los cables parecen ser conductores infinitamente largos. Esto causa un ligero efecto de difracción en la señal que se propaga a través de ellos. Esta ligera difracción normalmente es inmensurable.

Para sistemas de RF, la lluvia y otras atenuaciones de precipitaciones no son significativas por debajo de los 10 GHz. La Figura 2 grafica la forma en que la lluvia afecta más a las frecuencias más altas que a las frecuencias más bajas.



Client signal strength and link quality indicators help determine whether interference may be a problem.

Figura 1

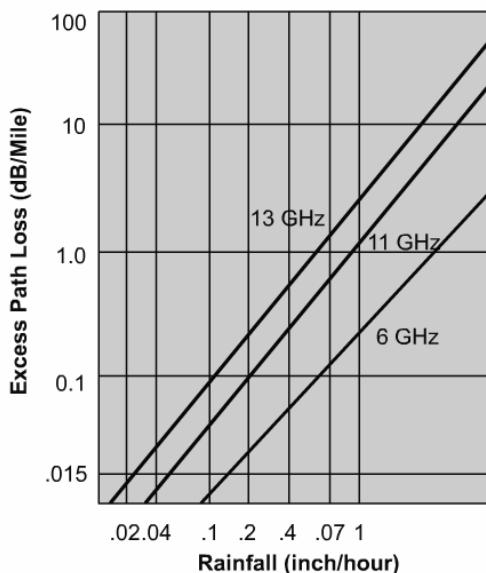


Figura 2

7.6 Instalación de la Antena

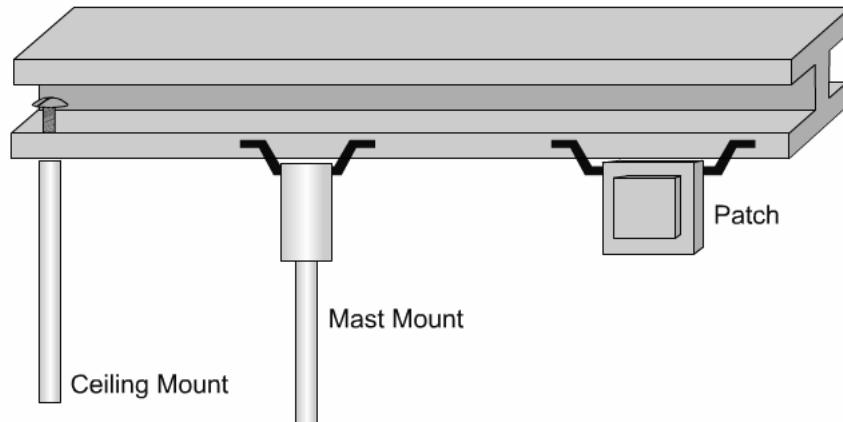
7.6.1 Descripción general

Una antena debería ser montada como para que utilice completamente sus características de propagación. Una forma de hacer esto es orientar la antena en forma horizontal, tan alta como sea posible, en o cerca del centro de su área de cobertura. La Figura 1 muestra las monturas de antenas más comunes.



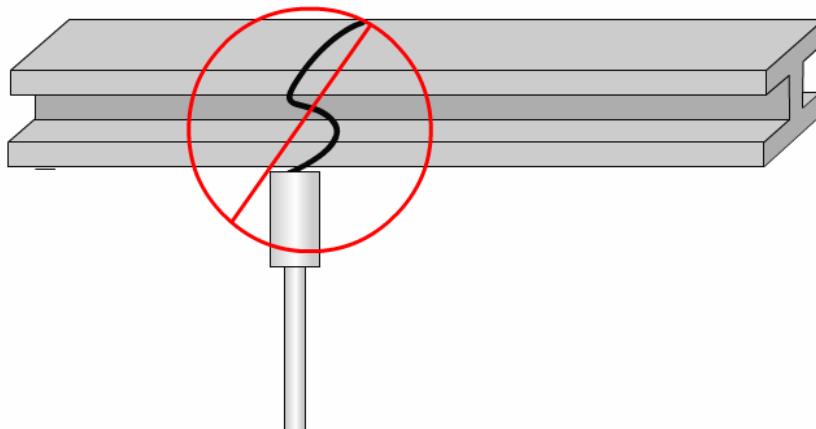
Figura 1

Mantenga a la antena lejos de las obstrucciones de metal, como conductos de calefacción y de aire acondicionado, grandes armazones de cielo raso, superestructuras de edificios y cableados de energía importantes. Si es necesario, utilice un conducto rígido para alejar a la antena de estas obstrucciones.



- Some antennas are not shipped with mounting brackets
- Modify brackets to fit your needs
- Modified brackets can be used with a variety of antennas
- Be creative

Figura 2



- Make sure the antennas mount is solid and secure
- Do not hang antenna by its cable
- Cable can break or become damaged
- Antenna can sway and provide a "moving cell"

Figura 3

La densidad de los materiales usados en la construcción de un edificio determina la cantidad de paredes que la señal puede atravesar y aun mantener una cobertura adecuada. Considere lo siguiente antes de elegir el lugar donde instalar una antena:

- Las paredes de papel y de vinilo tienen muy poco efecto sobre la penetración de la señal.
- Las paredes sólidas y de concreto pre-moldeado limitan la penetración de la señal a una o dos paredes sin degradar la cobertura.
- Las paredes de concreto y de bloques de madera limitan la penetración de la señal a tres o cuatro paredes.
- Una señal puede penetrar cinco o seis paredes construidas de yeso o madera.
- Una pared de metal grueso causa que la señal se refleje, lo que produce una penetración pobre.
- Un alambrado o un tejido metálico espaciado entre 2.5 y 3.8 cm (1 y 1.5 pulgadas) actúa como un reflector armónico, por lo que bloquea una señal de radio de 2,4 Ghz.

- Instale la antena lejos de hornos a microonda y de teléfonos inalámbricos de 2,4 GHz. Estos productos pueden causar interferencia en la señal, porque funcionan en el mismo rango de frecuencias.
- Instale la antena horizontalmente para maximizar la propagación de la señal.

Todos los APs tienen una antena conectada a ellos. La mayoría de las antenas son vendidas con un soporte para montarla, o éste está disponible como una opción. El desafío es que la mayoría de las antenas están diseñadas para ser montadas en una cierta forma.

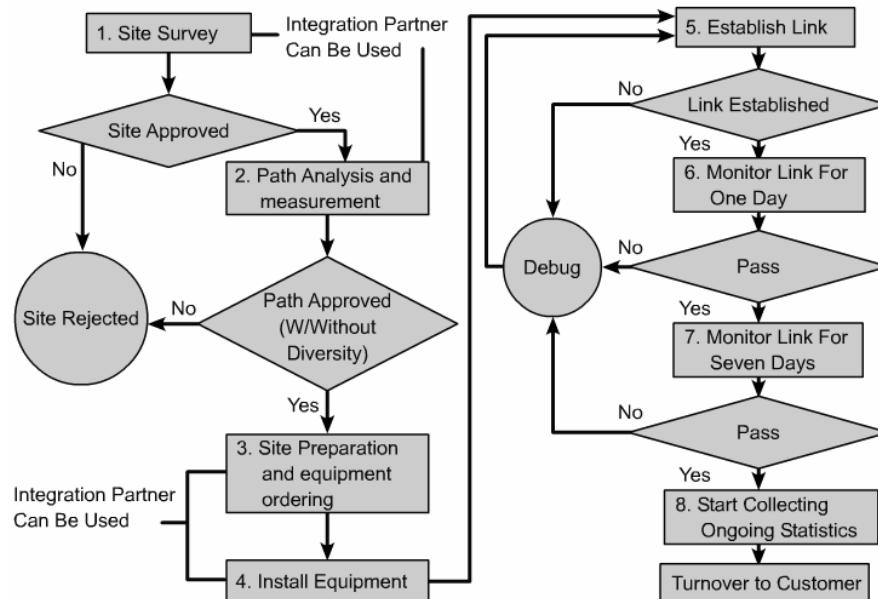


Figura 4



Figura 5

Una Antena Montada en Mástil de 5.2 dBi está diseñada para ser montada sobre un mástil y se vende con el hardware necesario para montarla. Para montar la antena en una viga doble T se necesita creatividad. Hay disponibles abrazaderas separadoras, pero no están diseñadas para montarlas en vigas doble T. Algunos instaladores usan abrazaderas plásticas, abrazaderas de viga o tornillos para ajustar los soportes separadores a las vigas doble T. La antena es luego montada al soporte. Cuando se utiliza una antena montada en un mástil en interiores, asegúrese de que esté montada como se muestra en las Figuras 2 y 3. La antena que es para usar en exteriores está diseñada para ser montada con la funda de metal en la parte inferior. Para usarla en interiores, invierta la antena. Sea creativo. Los soportes modificados pueden ser usados para una variedad de antenas.

Restricciones

Cuando se trabaja con estructuras altas e instalaciones de torres, los códigos y las leyes de cada ciudad o municipio pueden variar. Se puede necesitar un permiso de construcción para instalar torres o mástiles, dependiendo de la altura. Los mejores planes pueden derrumbarse si no se consiguen los permisos del construcción. La Figura 4 proporciona un diagrama de flujo paso a paso para la instalación de una antena. La Figura 5 ilustra las monturas de torres de antena.

7.6.2 Seguridad de las escaleras

Las escaleras vienen en muchos tamaños y formas para muchos propósitos específicos, como lo muestra la Figura 1. Pueden estar hechas de madera, aluminio o fibra de vidrio y están diseñadas para uso ligero o industrial. Los dos tipos más comunes son escaleras rectas y de tijera. Sin importar el tipo o construcción, asegúrese de que la escalera tenga una etiqueta que certifique que cumpla con las especificaciones del Instituto de Estándares Nacional Norteamericano [American National Standards Institute (ANSI)] y de los Laboratorios de Seguros [Underwriters Laboratories (UL)].

Más de 30.000 personas en los Estados Unidos resultan heridas cada año por caídas de escaleras. La mayoría de estos accidentes ocurren porque la gente no sigue las reglas básicas de seguridad de las escaleras:

- Seleccione la escalera correcta para el trabajo.
- Inspeccione la escalera.
- Fije la escalera en forma correcta y segura. En la Figura 2 se muestran ejemplos de valores para diferentes alturas.
- Suba y baje en forma segura. El subir demasiado alto también puede llevar a tener accidentes.
- Trabaje sobre la escalera en forma segura.
- Asegure el área alrededor de la escalera. Acordone el área de trabajo con indicadores apropiados como los conos de tráfico mostrados en la Figura 3 o cinta de precaución, como se muestra en la Figura 4. Cierre o bloquee cualquier puerta cercana que se abra hacia adentro.



Choose a ladder of the appropriate size. If the ladder is too high, the range of movement is restricted. If the ladder is too low, there is a risk of stepping off.

Figura 1

Height of ladder (m)	Distance from wall (m)
4	1
8	2
12	3
16	4
20	5
24	6
28	7

A straight ladder should extend away from the wall at the base, 0.25 m (9.84 inches) for each meter (3.28 ft) of vertical difference. Some are equipped with a gauge to help achieve the proper alignment.

Figura 2



Figura 3



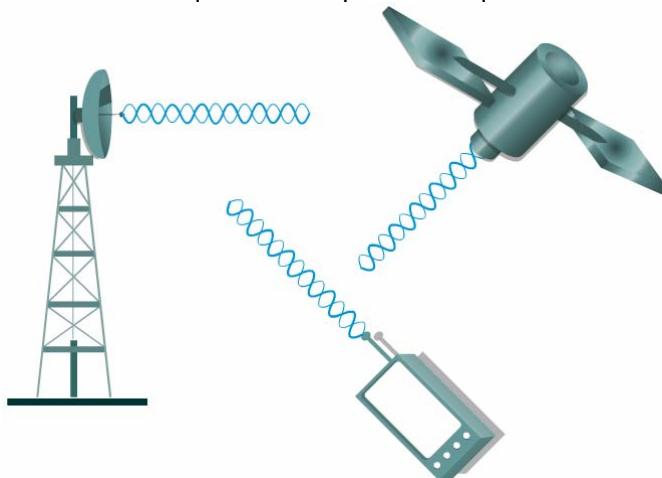
Figura 4

7.6.3 Seguridad en la instalación

Siga estas instrucciones de seguridad cuando instale una antena:

- Planifique el procedimiento de la instalación con cuidado y por completo antes de comenzar.
- Busque ayuda profesional si no está familiarizado con la instalación de antenas. Consulte a un vendedor que pueda explicarle el método de montura a usar en la ubicación donde la antena va a ser instalada.
- Seleccione el sitio de la instalación. Además considere la seguridad y el rendimiento. Como los cables de energía eléctrica y las líneas telefónicas son parecidos, suponga que cualquier línea es de energía eléctrica hasta que se determine lo contrario.
- Llame a la compañía de servicio público o a la organización de mantenimiento del edificio si los cables están cerca del sitio del montaje.
- Cuando instale la antena, no utilice una escalera de metal.
- Vístase en forma apropiada. Esto incluye usar zapatos con suela de goma y tacones, guantes de goma y una camisa o chaqueta de mangas largas.
- Si ocurre un accidente o una emergencia con las líneas de energía, llame a una ayuda de emergencia calificada inmediatamente.

Siempre suponga que alguna antena está transmitiendo energía RF. Sea particularmente cuidadoso con los platos pequeños, que tienen 30,48 cm (1 pie) o menos. Ellos a menudo emiten energía RF en el rango de frecuencias de gigahertz. Como una regla general, cuanto más alta es la frecuencia, más potencialmente peligrosa podría ser la radiación. Esto es así incluso si la exposición dura sólo décimas de segundo y el nivel de la potencia de transmisión es de sólo unos pocos watts. No hay un peligro conocido asociado con mirar el extremo sin terminador de los cables coaxiales que transportan tal energía. Asegúrese de que el transmisor no esté funcionando antes de quitar o reemplazar cualquier conexión de antena.

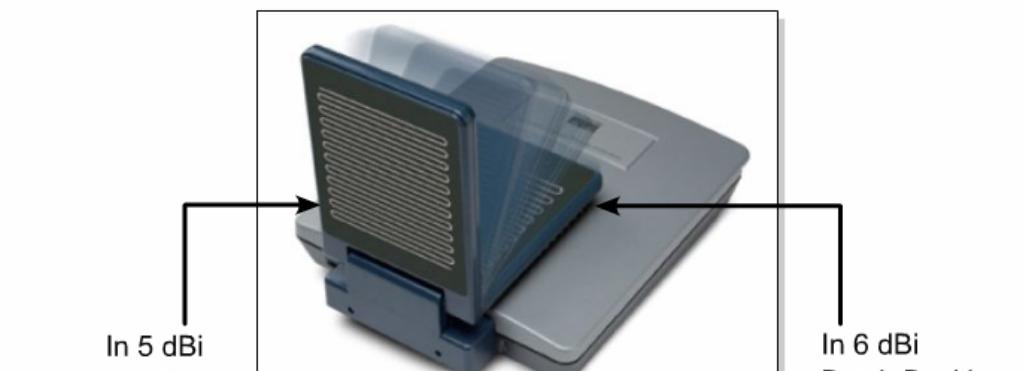


Cuando esté subido a un techo durante la instalación de antenas de microondas, evite caminar, y en especial no se quede parado en frente de ellas. Si es necesario caminar frente a alguna, normalmente no hay un mayor peligro si se mueve con rapidez a través del eje de la ruta de la antena.

7.6.4 Problemas legales

Las reglas de las frecuencias de radio varían en todo el mundo. Es importante cumplir con todas las leyes locales, regionales y nacionales que se aplican a la instalación. En los Estados Unidos tiene jurisdicción la FCC. En la mayor parte de Europa, el ETSI fija las leyes que afectan a los equipos inalámbricos. Algunas de estas reglas se muestran en las Figuras 2 y 3.

Como un ejemplo de cómo las reglas afectan a la configuración de las antenas, las reglas de la FCC de EE.UU. indican que cualquier dispositivo que soporte de uno a cuatro canales UNII-1 está limitado a una antena fija. Por lo tanto, el access point Cisco Aironet 1200 802.11a, mostrado en la Figura 1, tiene una antena plegable. Incluso aunque no es legal reemplazar la antena, puede servir a una variedad de aplicaciones.



Innovative 5GHz Combo Antenna:

- Wall mount: fold antenna flat against access point housing for 6dBi gain patch antenna
- Ceiling mount: fold antenna out at 90° angle for 5dBi gain omni antenna

Due to U.S. laws, most 802.11a access points do not support external antennas.

Figura 1

802.11b EIRP Rules for ETSI Governed Countries

Currently ETSI stipulates a maximum of 20dBm EIRP on Point-to-Multipoint and Point-to-Point installations – 17 dBm maximum transmitter power with 3 dBi in gain attributed to antenna and cable combination.

Professional installers are allowed to increase the gain of an antenna/cable system if the transmitter power is reduced below 17dBm in a 1:1 ratio.

- Reduce Transmit Power below maximum of 17 dBm by 1 dBm and increase antenna/cable system gain by 1 dBi

Figura 2

Cisco Aironet 802.11a Antennas

FCC requires that all radios utilizing the UNII-1 Band (5.15 GHz – 5.25 GHz) must have non-removable or integrated antennas.

FCC allows radios utilizing the UNII-2 Band (5.25 GHz – 5.35 GHz) to have external or removable antennas.

FCC Requires radios operating in both UNII-1 and UNII-2 bands must comply with antenna rules regulating UNII-1 band (including indoor use only).

- The Cisco Aironet 802.11a radios utilize both UNII-1 and UNII-2 bands, therefore cannot have external or removable antennas and must be used indoors only.
- Cisco 802.11a antennas are integrated into the radio module.

Figura 3

7.6.5 Reglas de la EIRP

La Potencia Efectiva Isotrópica Radiada [Effective Isotropic Radiated Power (EIRP)] de un transmisor es la potencia que el transmisor parece tener si fuera un radiador isotrópico (si la antena emite en forma igual en todas direcciones). En virtud de la ganancia de una antena de radio (o plato), se forma un rayo que transmite preferentemente la energía en una dirección. El EIRP se estima sumando la ganancia (de la antena) y la potencia de transmisión (de la radio).

EIRP = potencia de transmisión + ganancia de la antena – pérdida del cable

Cuando se utiliza un equipo de radio, hay límites en la salida del sistema. Estos límites son dados como EIRP, y no deben ser excedidos. Diferentes países tendrán diferentes estándares. Consulte con las autoridades del país de la instalación cuál es la EIRP máxima.

La salida de la radio será medida en dBm (decibeles por miliwatt). La Figura 1 muestra una tabla que indica la clasificación en dBm de los distintos niveles de salida disponibles con el equipo Inalámbrico Cisco Aironet y la EIRP resultante cuando se usa con una antena patch de 6 dBi.

Point to Multipoint				
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
FCC Maximum	1 Watt	30 dBm	6 dBi	36 dBm
Cisco Maximum	100 mW	20 dBm	16 dBi	36 dBm
The Above values represent the 1 : 1 rule.				

Point To Point				
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
FCC Maximum	1 Watt	30 dBm	6 dBi	36 dBm
Cisco Maximum	100 mW	20 dBm	36 dBi	56 dBm
The Above values represent the 3 : 1 rule.				

Figura 1

Point To Multipoint and Point to Point				
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
Gov. Body Maximum	50 mW	17 dBm	3 dBi	20 dBm
Cisco integrated Antennas	50 mW	17 dBm	2.2 dBi	19.2 dBm
Reduced TX Power	30 mW	15 dBm	5 dBi	20 dBm
Reduced TX Power	20 mW	13 dBm	7 dBi	20 dBm
Reduced TX Power	5 mW	7 dBm	13 dBi	20 dBm
Reduced TX Power	1 mW	0 dBm	20 dBi	20 dBm
The above values reflect the 3 : 1 rule.				

Governing bodies with 20 dBm ceiling on EIRP:
ETSI, France/ Singapore, Israel, Mexico

Figura 2

La EIRP máxima permitida por la FCC para un dispositivo 802.11b Parte 15 en los Estados Unidos es 36 dBm. Los estándares son diferentes para sistemas punto a puntos específicos. Sin embargo, este curso está enfocado en las WLANs que serían consideradas soluciones punto a multipunto, por lo que la EIRP máxima permitida no debe exceder los 36 dBm y la ganancia máxima en una antena no debe exceder los 16 dBi (para los Estados Unidos) a menos que sea instalada por un instalador profesional. [\[2\]](#)

La EIRP máxima permitida para un dispositivo de 2.4 GHz en Francia, Singapur, Israel, México y ETSI es de 20 dBm. Los estándares son diferentes para sistemas punto a punto específicos. Sin embargo, esta clase está enfocada en WLANs que serían consideradas soluciones punto a multipunto, por lo que la EIRP máxima permitida no debe exceder los 20 dBm y la ganancia máxima en una antena no debe exceder los 20 dBi.

Resumen

La elección y la instalación de antenas es una parte integral de una instalación de WLAN exitosa. Es importante comprender la diferencia entre antenas direccionales y omnidireccionales. Las especificaciones de las antenas pueden variar, pero la teoría subyacente es la misma.

Este módulo también habló de algunos requisitos básicos del estudio del sitio junto con algunos problemas de seguridad a tener en cuenta. Cuando se trabaja con WLANs, la línea de visión no es sólo una línea recta entre antenas. La línea de visión inalámbrica debe tener en cuenta la zona Fresnel y podría tener que ajustarse a la curvatura de la Tierra.

Módulo 8: Seguridad

Descripción General

La seguridad de la red es el proceso por el cual se protegen los recursos de información digital. Los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y asegurar la disponibilidad. El crecimiento de la computación ha generado enormes avances en la forma en que las personas viven y trabajan. Por lo tanto, todas las redes deben estar protegidas para alcanzar su máximo potencial. Las WLANs presentan desafíos de seguridad únicos.

Este módulo hablará sobre los fundamentos de la seguridad de WLANs. El crecimiento exponencial del networking, incluyendo las tecnologías inalámbricas, ha conducido a aumentar los riesgos de seguridad. Muchos de estos riesgos se deben al hacking, además del uso incorrecto de los recursos de la red. Se tratarán las debilidades y vulnerabilidades específicas de las WLANs. Se mostrará y explicará la configuración de seguridad para APs, bridges y clientes. Finalmente, se presentará la seguridad de WLAN a nivel empresarial.

8.1 Fundamentos de Seguridad

8.1.1 ¿Qué es la seguridad?

Un propósito principal de la seguridad es mantener afuera a los intrusos. En la mayoría de los casos, esto significa construir paredes fuertes y establecer puertas pequeñas bien protegidas para proporcionar acceso seguro a un grupo selecto de personas. Esta estrategia funciona mejor para las LANs cableadas que para las WLANs. El crecimiento del comercio móvil y de las redes inalámbricas hace que los modelos viejos sean inadecuados. Las soluciones de seguridad deben estar integradas sin fisuras y ser muy transparentes, flexibles y administrables.

Cuando la mayoría de la gente habla sobre seguridad, hacen referencia a asegurar que los usuarios puedan realizar sólo las tareas que tienen autorizado hacer y que puedan obtener sólo la información que tienen autorizado tener. La seguridad también significa asegurar que los usuarios no puedan causar daño a los datos, a las aplicaciones o al entorno operativo de un sistema. La palabra seguridad comprende la protección contra ataques maliciosos. La seguridad también comprende el control de los efectos de los errores y de las fallas del equipo. Todo lo que pueda proteger contra un ataque inalámbrico probablemente evitará también otros tipos de problemas. El balance entre permitir el acceso autorizado y evitar el acceso no autorizado está ilustrado en la Figura 1.



Figura 1

8.1.2 Vulnerabilidades de las WLANs

Las WLANs son vulnerables a ataques especializados. Muchos de estos ataques explotan las debilidades de la tecnología, ya que la seguridad de WLAN 802.11 es relativamente nueva. También hay muchas debilidades de configuración, ya que algunas compañías no están usando las características de seguridad

de las WLANs en todos sus equipos. En realidad, muchos dispositivos son entregados con passwords de administrador predeterminadas. Finalmente, hay debilidades de políticas. Cuando una compañía no tiene una política inalámbrica clara sobre el uso de la tecnología inalámbrica, los empleados pueden configurar sus propios APs. Un AP configurado por un empleado se conoce como un AP furtivo, que raramente es seguro.

Hay personas entusiastas, dispuestas y calificadas para tomar ventaja de cada vulnerabilidad de WLAN. Ellas están constantemente tratando de descubrir y explotar nuevas vulnerabilidades. Se han escrito numerosos documentos sobre el tema de la seguridad del 802.11. Lo que sigue es un resumen de las principales vulnerabilidades:

- Autenticación débil únicamente de dispositivo - Se autentican los dispositivos clientes. Los usuarios no se autentican.
- Encriptación de datos débil - Se ha probado que la Privacidad Equivalente a la Cableada (WEP) es ineficiente como medio para encriptar datos.
- No hay integridad de mensajes - Se ha probado que el Valor de Control de Integridad (ICV) no es efectivo como medio para asegurar la integridad de los mensajes.

Las vulnerabilidades de seguridad del 802.11 pueden ser una barrera para el desarrollo de WLANs empresariales. Para tratar estas vulnerabilidades, Cisco ha desarrollado la Suite de Seguridad Inalámbrica para proveer mejoras sólidas a la encriptación WEP y autenticación centralizada basada en usuarios.

En esta sección, numerosas actividades demostrarán los múltiples métodos utilizados en la configuración de la seguridad inalámbrica de Cisco.

8.1.3 Amenazas a la WLAN

Existen cuatro clases principales de amenazas a la seguridad inalámbrica:

1. Amenazas no estructuradas
2. Amenazas estructuradas
3. Amenazas externas
4. Amenazas internas

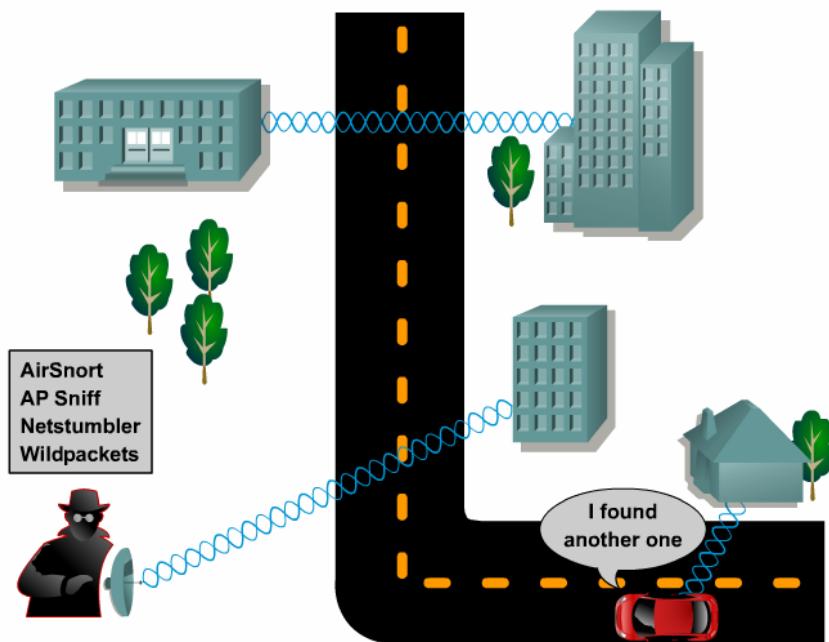


Figura 1

Las amenazas no estructuradas consisten principalmente en individuos inexpertos que están usando herramientas de hacking disponibles fácilmente como scripts de shell y crackers de passwords. Las amenazas estructuradas vienen de hackers que están mucho más motivados y son técnicamente competentes. Estas personas conocen las vulnerabilidades de los sistemas inalámbricos y pueden comprender y desarrollar explotación de códigos, scripts y programas. Las amenazas externas son individuos u organizaciones que trabajan desde el exterior de la compañía. Ellos no tienen acceso autorizado a la red inalámbrica. Ingresan a la red principalmente desde el exterior del edificio como estacionamientos, edificios adyacentes o áreas comunes.¹ Estos son los tipos de amenazas por los que la gente gasta la mayor parte del tiempo y dinero en protegerse. Las amenazas internas ocurren cuando

alguien tiene acceso autorizado a la red con una cuenta en un servidor o con acceso físico al cableado. De acuerdo con el FBI, el acceso interno y el mal uso forman el 60 al 80 por ciento de los incidentes reportados. El acceso inalámbrico puede ser una gran amenaza a la seguridad de la red. La mayoría de las WLANs tienen pocas o ninguna restricción. Una vez asociado a un access point, un atacante puede recorrer libremente la red interna.

8.1.4 Reconocimiento

Los métodos de ataques inalámbricos pueden ser divididos en tres categorías:

1. Reconocimiento
2. Ataque de acceso
3. Negación del Servicio [Denial of Service (DoS)]

Reconocimiento

El reconocimiento es el descubrimiento y mapeo no autorizado de sistemas, servicios o vulnerabilidades. También es conocido como reunión de información y normalmente precede a un acceso real o ataque DoS. El reconocimiento es similar a un ladrón que revisa un vecindario buscando casas fáciles donde entrar. En muchos casos, los intrusos llegan tan lejos como a probar el picaporte de la puerta para descubrir áreas vulnerables, a las que pueden explotar en un momento posterior. La realización del reconocimiento comprende el uso de comandos o utilitarios comunes para conocer tanto como sea posible el sitio de la víctima.

The screenshot shows the Kismet Network List interface. The main window displays a table of wireless networks with columns: Name, T, W, CH, Packts, Flags, Data, Clnt. The table includes rows for p@thfInd3r, <no ssid>, KrullNet1, linksys, marley, <no ssid>, FARMAS, <no ssid>, GRXWirelessNetwork, SECHMAS, <no ssid>, and <Lucent Outdoor Router>. To the right of the table is an 'Info' panel showing metrics like Ntwrks (105), Pckets (1258), Cryptd (104), Weak (0), Noise (289), Discrd (289), and Pkts/s (50). Below the table is a 'Status' panel listing network discovery events. At the bottom is a 'Battery' status bar indicating AC Charging 100% 0h0m0s.

Name	T	W	CH	Packts	Flags	Data	Clnt
p@thfInd3r	A	Y	06	171		70	35
<no ssid>	A	N	05	1		0	0
KrullNet1	A	Y	06	27		0	0
linksys	A	N	06	81	FU4	8	2
marley	A	N	06	312		17	1
<no ssid>	D	N	--	20	A2	20	18
FARMAS	A	Y	07	30		0	0
<no ssid>	A	Y	06	1		0	0
GRXWirelessNetwork	A	N	06	2		0	0
SECHMAS	A	N	07	13		0	0
<no ssid>	D	N	--	1	A4	1	66
<Lucent Outdoor Router>	D	N	--	267		267	1

Figura 1

El snooping (simulación) inalámbrico y el sniffing (rastreo) de paquetes son términos comunes para las escuchas. La información reunida por las escuchas puede luego ser usada en futuros accesos o ataques DoS a la red. El usar encriptación y evitar protocolos que son fácilmente escuchados puede combatir las escuchas. Los analizadores de protocolos inalámbricos comerciales como AiroPeek, AirMagnet, o Sniffer Wireless se pueden usar para escuchar las WLANs. Los analizadores de protocolos gratuitos como Ethereal o tcpdump soportan por completo las escuchas inalámbricas bajo Linux. Las escuchas inalámbricas se pueden usar para ver el tráfico de la red y descubrir los SSIDs en uso, las direcciones MAC válidas o para determinar si la encriptación está siendo usada.

El reconocimiento inalámbrico a menudo es llamado wardriving. Los utilitarios usados para explorar las redes inalámbricas pueden ser activos o pasivos. Las herramientas pasivas, como Kismet, no transmiten información mientras están detectando redes inalámbricas. Una pantalla del Kismet se muestra en la Figura 1. Los utilitarios activos, como el NetStumbler, transmiten pedidos de información adicional sobre una red inalámbrica, una vez que es descubierta. El sistema operativo Windows XP es sensible a la tecnología inalámbrica. Windows XP realiza una búsqueda activa. Intentará conectarse automáticamente a una WLAN descubierta. Algunas personas que usan herramientas WLAN están interesadas en recolectar información acerca del uso de la seguridad inalámbrica. Otros están interesados en encontrar WLANs que ofrezcan acceso libre a Internet o una puerta trasera fácil hacia una puerta corporativa.

8.1.5 Acceso

El acceso al sistema, en este contexto, es la capacidad para que un intruso no autorizado logre acceder a un dispositivo para el cual no tiene una cuenta o password. Para ingresar o acceder a los sistemas donde uno no tiene acceso autorizado normalmente se debe ejecutar un hack script o una herramienta que explote una vulnerabilidad conocida del sistema o aplicación a ser atacada. Acceso es un término demasiado abarcativo que hace referencia a la manipulación de datos, acceso a sistemas o escaladas privilegiadas no autorizados. Algunos ejemplos de acceso son los siguientes:

- Explotación de passwords débiles o no existentes
- Explotación de servicios como HTTP, FTP, SNMP, CDP y Telnet.

El hack más fácil se llama Ingeniería Social. No comprende ninguna habilidad informática. Si un intruso puede engañar a un miembro de una organización para que le de información valiosa como ubicaciones de archivos y servidores o passwords, entonces el proceso de hacking resulta mucho más sencillo.

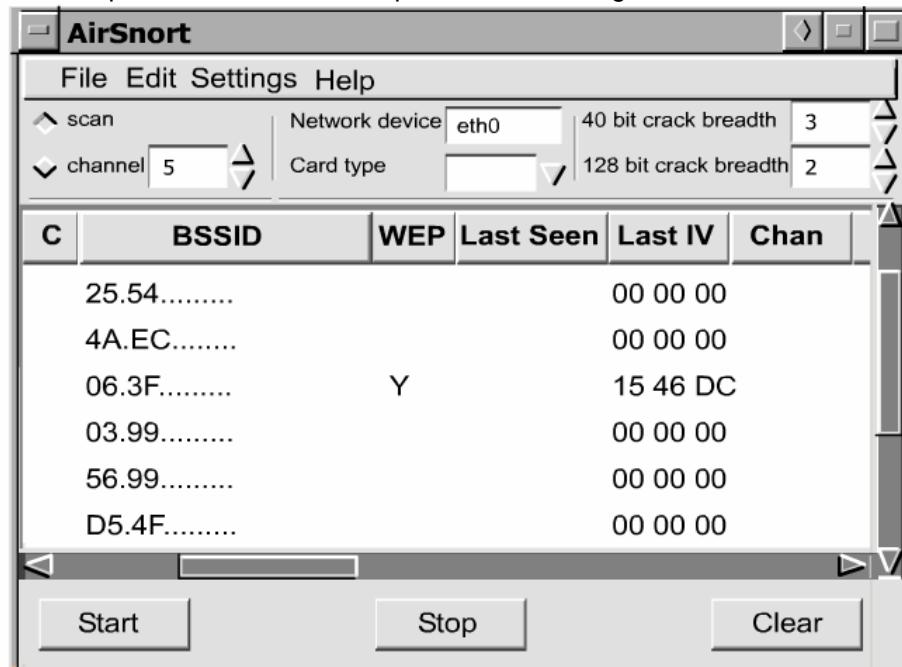


Figura 1

Ataque de un AP furtivo

La mayoría de los clientes se asociarán al access point con la señal más fuerte. Si un AP no autorizado, que por lo general es un AP furtivo, tiene una señal fuerte, los clientes se asociarán al él. El AP furtivo tendrá acceso al tráfico de red de todos los clientes asociados. Por lo tanto, el AP furtivo puede ser usado para realizar ataques por desconocidos [man-in-the-middle attacks] contra tráfico encriptado como SSL o SSH. El AP furtivo también puede usar spoofing de ARP e IP para engañar a los clientes para que envíen passwords e información confidencial. El AP furtivo puede también pedir sesiones no protegidas con la Privacidad Equivalente a la Cableada (WEP) con clientes durante la asociación.

Ataques de Privacidad Equivalente a la Cableada (WEP)

Los ataques contra la WEP incluyen Bit Flipping, Replay Attacks, y la colección Weak IV. Muchos ataques WEP no han salido del laboratorio, pero están bien documentados. Un utilitario, llamado AirSnort, captura Vectores de Inicialización débiles para determinar la clave WEP que se está usando. La Figura 1 muestra una pantalla del AirSnort.

8.1.6 Negación del servicio

La DoS ocurre cuando un atacante desactiva o corrompe las redes, sistemas o servicios inalámbricos, con la intención de negar el servicio a usuarios autorizados. Los ataques DoS toman muchas formas. En la mayoría de los casos, la realización del ataque comprende simplemente ejecutar un hack, una script o una herramienta. El atacante no necesita acceder previamente al objetivo, porque todo lo que se necesita normalmente es una forma de acceder a él. Por estas razones y a causa del gran daño potencial, los ataques DoS son los más temidos, ya que son los más difíciles de evitar.

Muchos ataques DoS contra las redes inalámbricas 802.11 han sido teorizados. Un utilitario, llamado Wlan Jack, envía paquetes de disociación falsos que desconectan a los clientes 802.11 del access point. Siempre que se ejecute el utilitario de ataque, los clientes no pueden usar la WLAN. De hecho, cualquier dispositivo que opere a 2.4 GHz o a 5 GHz puede ser usado como una herramienta DoS.¹

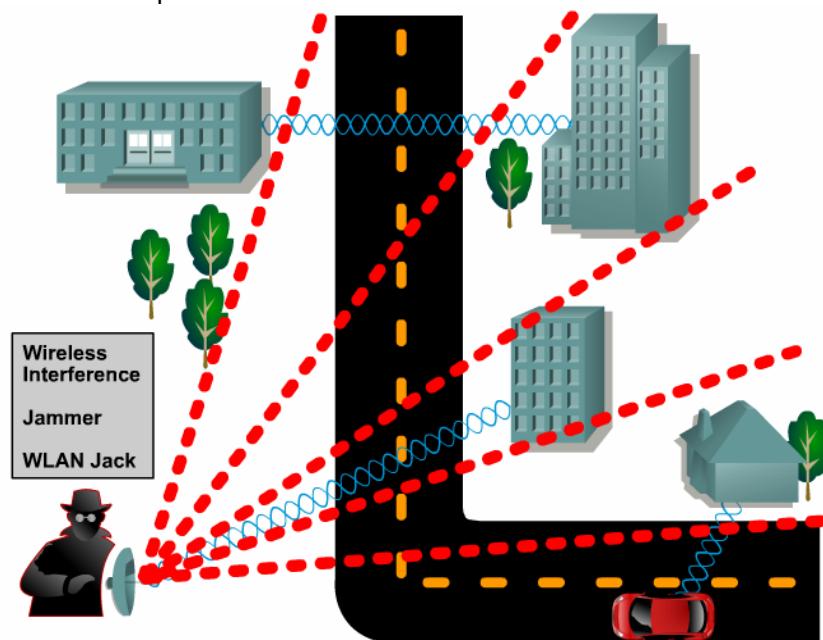


Figura 1

8.2 Tecnologías de Seguridad WLAN Básica

8.2.1 La rueda de la seguridad WLAN

La mayoría de los incidentes de seguridad inalámbrica ocurren porque los administradores de sistemas no implementan contramedidas. Por lo tanto, la cuestión no es sólo confirmar que existe una vulnerabilidad técnica y encontrar una contramedida que funcione. También es crítico verificar que la contramedida está en su lugar y que funciona correctamente.

Aquí es donde la Rueda de la Seguridad WLAN, que es un proceso de seguridad continuo, es efectiva. La Rueda de la Seguridad WLAN no sólo promueve la aplicación de medidas de seguridad a la red, sino que lo más importante es que promueve el control y la aplicación de medidas de seguridad actualizadas en forma continua. La Rueda de la Seguridad WLAN está ilustrada en las Figuras 1–4.

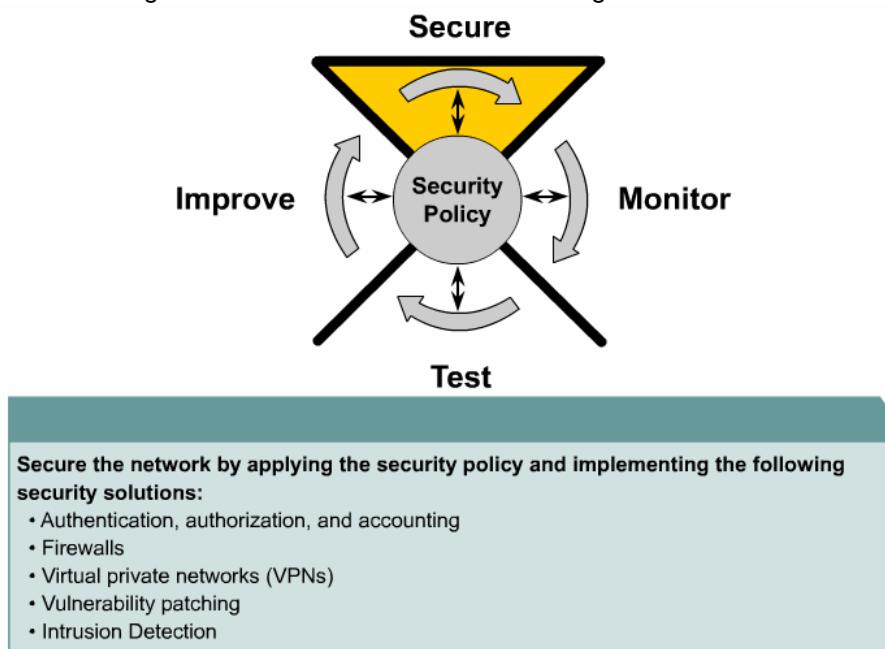


Figura 1

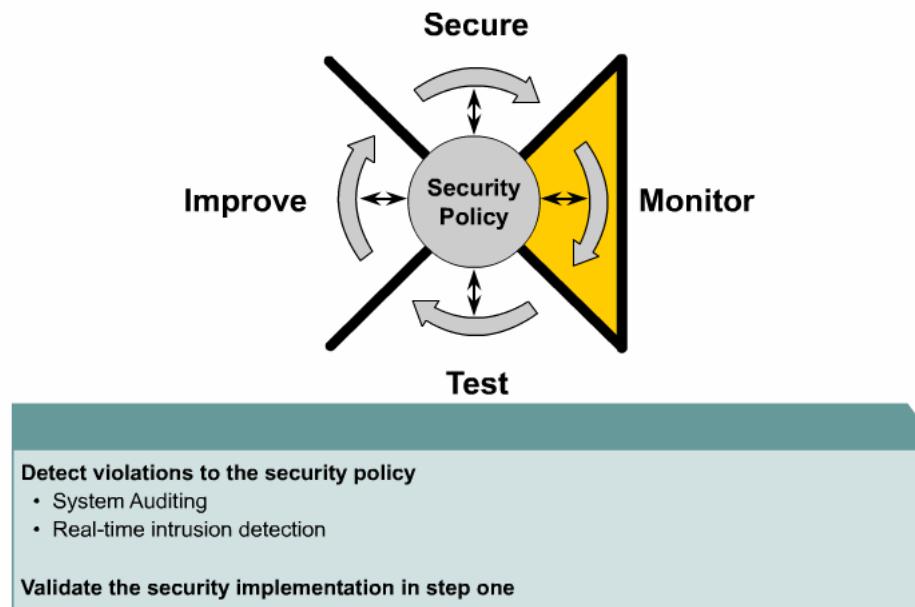


Figura 2

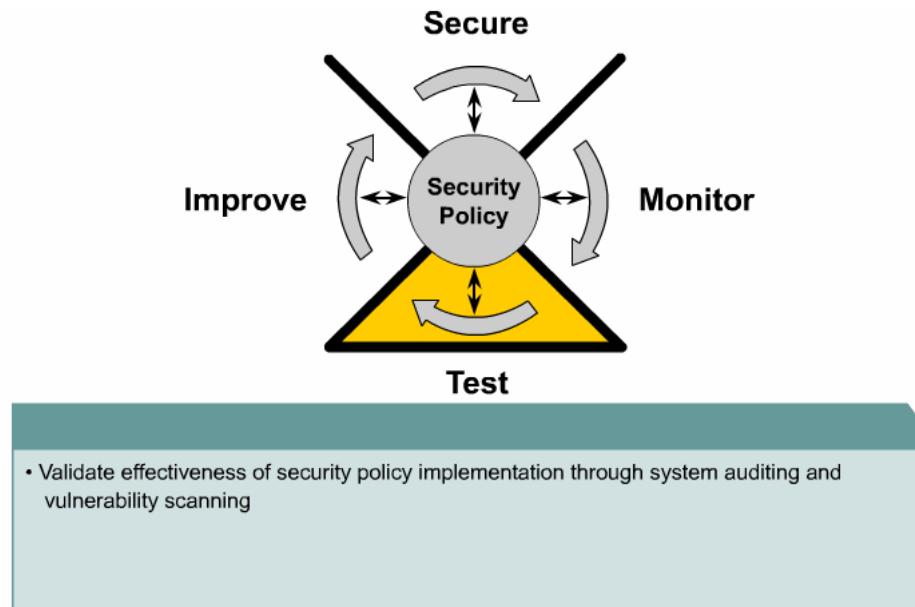


Figura 3

Para comenzar el proceso de la Rueda de la Seguridad, primero desarrolle una política de seguridad de WLAN que permita la aplicación de medidas de seguridad. Una política de seguridad debe realizar las siguientes tareas:

- Identificar los objetivos de seguridad inalámbrica de la organización
- Documentar los recursos a ser protegidos
- Identificar la infraestructura de la red con los mapas e inventarios actuales

Las políticas de seguridad proporcionan muchos beneficios. Ellas valen el tiempo y el esfuerzo necesarios para desarrollarlas. El desarrollo de una buena política de seguridad logra lo siguiente:

- Proporciona un proceso para auditar la seguridad inalámbrica existente.
- Proporciona un marco de trabajo general para implementar la seguridad
- Define los comportamientos que están o no permitidos
- Ayuda a determinar cuáles herramientas y procedimientos son necesarios para la organización
- Ayuda a comunicar un consenso entre un grupo de directivos clave y define las responsabilidades de los usuarios y de los administradores
- Define un proceso para manipular violaciones inalámbricas
- Crea una base para la acción lógica, si fuera necesario

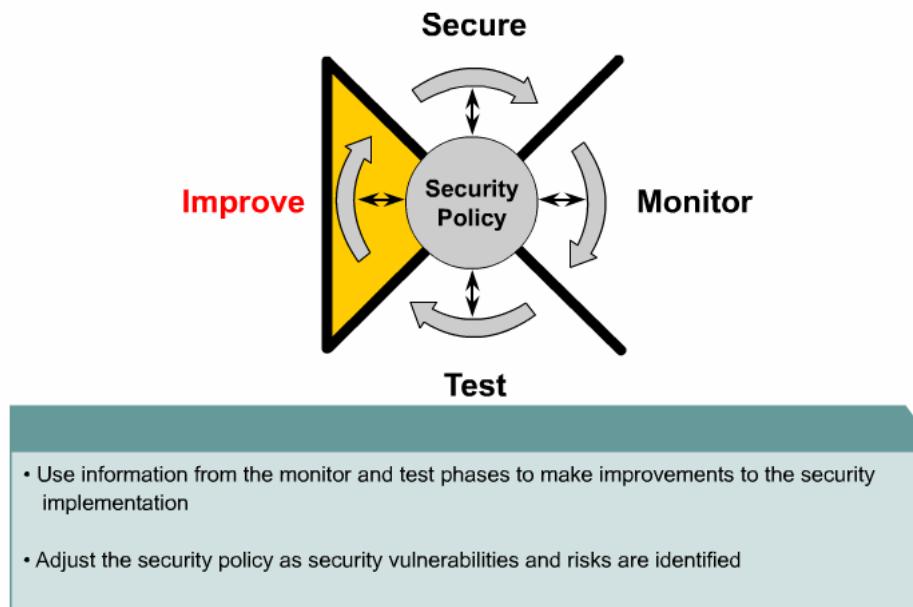


Figura 4

Una política de seguridad inalámbrica efectiva trabaja para asegurar que los recursos de la red de la organización estén protegidos contra el sabotaje y el acceso inapropiado, que incluye tanto el acceso intencional como el accidental. Todas las características de la seguridad inalámbrica deberían ser configuradas en conformidad con la política de seguridad de la organización. Si no está presente una política de seguridad, o si está desactualizada, se debería crear o actualizar antes de decidir cómo configurar o hacer uso de los dispositivos inalámbricos.

8.2.2 Seguridad inalámbrica de primera generación

La seguridad no era una gran preocupación para las primeras WLANs. El equipo era propietario, costoso y difícil de conseguir. Muchas WLANs usaban el Identificador del Conjunto de Servicio [Service Set Identifier (SSID)] como una forma básica de seguridad¹. Algunas WLANs controlaban el acceso ingresando la dirección de control de acceso al medio (MAC) de cada cliente en los access points inalámbricos. Ninguna opción era segura, ya que el sniffing inalámbrico podía revelar las direcciones MAC válidas y el SSID.

Older forms of security on WLANs

- SSID
- Authentication controlled by MAC

Figura 1

El SSID es una cadena de 1 a 32 caracteres del Código Estándar Norteamericano para el Intercambio de Información [American Standard Code for Information Interchange (ASCII)] que puede ser ingresada en los clientes y en los access points, como muestra la Figura 2. La mayoría de los access points tienen opciones como 'SSID broadcast' ['broadcast de SSID'] y 'allow any SSID' ['permitir cualquier SSID']. Estas características están normalmente activas por defecto y facilitan la configuración de una red inalámbrica. El usar la opción 'allow any SSID' permite que un cliente con un SSID en blanco acceda a un access point. El 'SSID broadcast' envía paquetes baliza que publican el SSID. El desactivar estas dos opciones no asegura a la red, ya que un sniffer inalámbrico puede fácilmente capturar un SSID válido del tráfico normal de la WLAN. Los SSIDs no deberían ser considerados una característica segura.

SSID (Service Set Identifier)

- 32 ASCII character string
- Under 802.11, any client with a 'NULL' string will associate to any access point regardless of SSID setting on access point

This should not be considered a security feature.

Figura 2

La autenticación basada en MAC no está incluida en las especificaciones del 802.11. Sin embargo, muchos fabricantes han implementado una autenticación basada en MAC. La mayoría de los fabricantes simplemente requieren que cada access point tenga una lista de direcciones MAC válidas. Algunos fabricantes también permiten que el access point consulte una lista de direcciones MAC en un servidor centralizado.

Controlar el acceso a una red inalámbrica usando direcciones MAC es tedioso. Se debe mantener un inventario preciso y los usuarios deben reportar rápidamente la pérdida o el robo de equipo. Las direcciones MAC no son un verdadero mecanismo de seguridad, ya que todas las direcciones MAC no están encriptadas cuando se transmiten. Un atacante sólo necesitaría capturar una dirección MAC válida para poder acceder a la red. En ciertos casos, la autenticación de direcciones MAC puede suplementar las características de seguridad, pero no debería ser nunca el método principal de seguridad inalámbrica.

8.2.3 Privacidad equivalente a la cableada [Wired equivalent privacy (WEP)]

El estándar IEEE 802.11 incluye a WEP para proteger a los usuarios autorizados de una WLAN de las escuchas ocasionales. El estándar WEP de IEEE 802.11 especificaba una clave de 40 bits, por lo que WEP podía ser exportado y usado en todo el mundo, como lo indica la Figura 1. La mayoría de los fabricantes han extendido el WEP a 128 bits o más. Cuando se usa el WEP, tanto el cliente inalámbrico como el access point deben tener una clave WEP idéntica. WEP está basado en un tipo de encriptación existente y familiar, la Rivest Cipher 4 (RC4).

- Wired Equivalent Privacy
- Based on RC4 symmetric stream cipher
- Static, pre-shared, 40-bit or 104-bit keys on client access point

Figura 1

El estándar IEEE 802.11 proporciona dos esquemas para definir las claves WEP a ser usadas en una WLAN. En el primer esquema, un conjunto de hasta cuatro claves predeterminadas son compartidas por todas las estaciones, incluyendo clientes y access points, en un subsistema inalámbrico. Cuando un cliente obtiene las claves predeterminadas, ese cliente puede comunicarse en forma segura con todas las otras estaciones en el subsistema. El problema con las claves predeterminadas es que cuando llegan a estar distribuidas extensamente, es más probable que estén en peligro. El equipo WLAN de Cisco utiliza este primer esquema.

En el segundo esquema, cada cliente establece una relación de mapeo de clave con otra estación. Esta es una forma más segura de operación, porque menos estaciones tienen las claves. Sin embargo, la distribución de tales claves unicast se vuelve más difícil a medida que la cantidad de estaciones aumenta. La forma en que 802.11 utiliza la encriptación WEP es débil en varias formas. Estas debilidades están siendo tratadas por el estándar 802.11i, que será explicado en las secciones siguientes.

8.2.4 Autenticación y asociación

La Autenticación Abierta y la Autenticación de Clave Compartida son los dos métodos que define el estándar 802.11 para que los clientes se conecten a un access point.¹ El proceso de asociación puede ser dividido en tres elementos, que son investigación, autenticación y asociación. Esta sección explicará ambos métodos de autenticación y las etapas que atraviesa el cliente durante el proceso. El EAP de red será tratado en la sección de seguridad WLAN empresarial.

Autenticación Abierta

El método de Autenticación Abierta realiza el proceso de autenticación completo en texto abierto. Esto se muestra en la Figura 2. La Autenticación Abierta es básicamente una autenticación nula, lo que significa que no hay una verificación del usuario o de la máquina. La Autenticación Abierta está normalmente ligada a una clave WEP. Un cliente puede asociarse al access point con una clave WEP incorrecta o incluso sin una clave WEP. Un cliente con la clave WEP incorrecta no podrá enviar o recibir datos, ya que la carga de paquetes estará encriptada. Tenga presente que el encabezado no está encriptado por el WEP. Sólo la carga o los datos están encriptados.

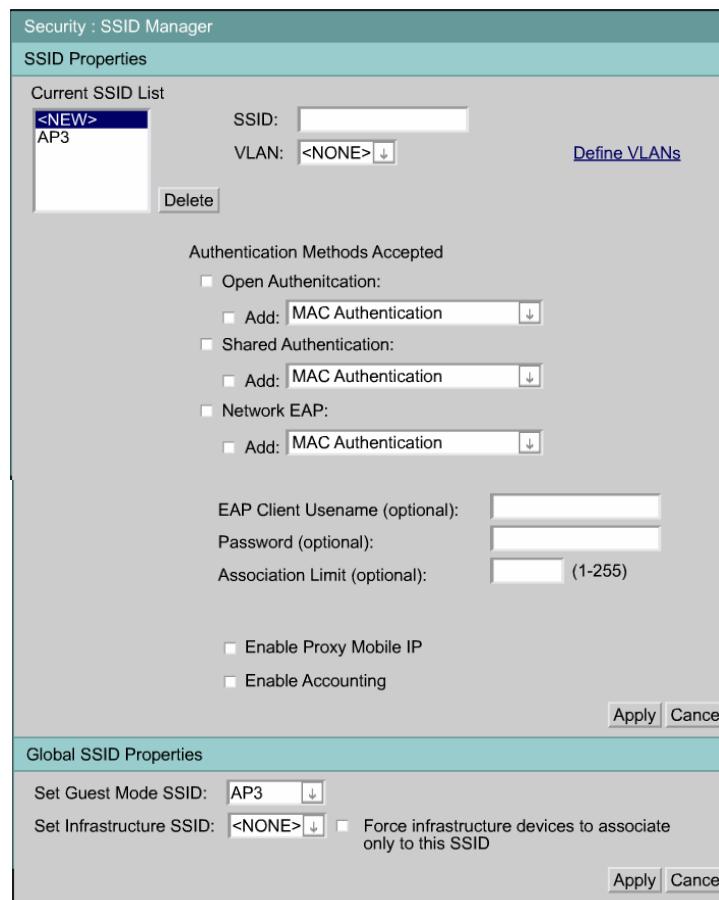
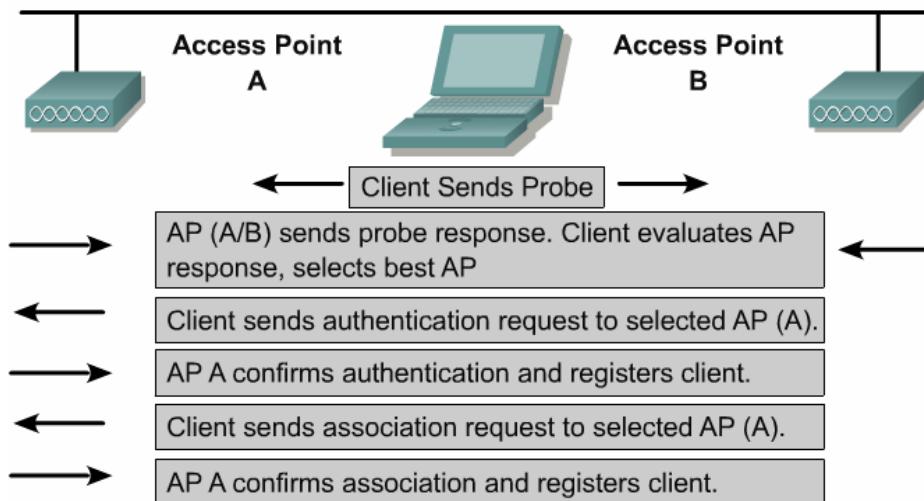


Figura 1



Open authentication uses clear text transmission to allow a client to associate to an access point.

Figura 2

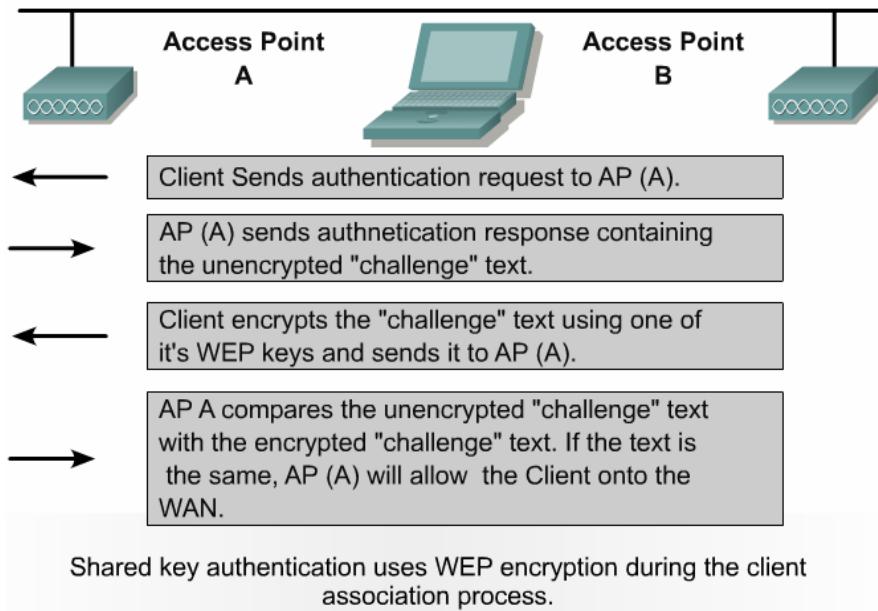


Figura 3

Autenticación de Clave Compartida

La Autenticación de Clave Compartida funciona en forma similar a la Autenticación Abierta, excepto que utiliza la encriptación WEP para un paso. La clave compartida requiere que el cliente y el access point tengan la misma clave WEP. Un access point que usa la Autenticación de Clave Compartida envía un paquete de texto de desafío al cliente, como muestra la Figura 3. Si el cliente tiene la clave equivocada o no tiene clave, fallará en esta parte del proceso de autenticación. El cliente no tendrá permitido asociarse al AP. La clave compartida es vulnerable a un ataque por desconocidos, por lo que no es recomendada.

Interoperabilidad

En la mayoría de los access points, incluyendo los de Cisco, es posible usar la Autenticación Abierta con o sin una clave WEP. Para una interoperabilidad básica que requiera WEP, se configurará un access point Cisco usando Autenticación Abierta. La Encriptación de Datos es fijada en Required [Necesaria], y TKIP, MIC, y BKR están todos desactivados.

8.3 Configuración de Seguridad WLAN Básica

8.3.1 Seguridad WLAN Básica

Los access points y bridges inalámbricos deben estar asegurados. A menudo, la administración se realiza usando protocolos estándares, que no son seguros. Esta sección explicará los pasos básicos que se deben tomar para asegurar un equipo de infraestructura inalámbrica. La Figura 1 proporciona algunas recomendaciones de seguridad básicas para el tráfico de administración de red.

Basic Security Recommendations

- Enable user authentication for the management interface.
- Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often.
- Consider using SNMP Read Only if the management infrastructure allows it.
- Disable any insecure and nonessential management protocol provided by the manufacturer.
- Limit management traffic to a dedicated wired subnet.
- Encrypt all management traffic where possible.
- Enable wireless frame encryption where available.

Figura 1

El equipo de red ofrece muchos protocolos adicionales, lo que simplifica la administración de la red y el acceso de los usuarios. Dependiendo de la configuración de la red, sólo algunos de estos protocolos pueden ser necesario. Esta sección hablará de protocolos que podrían no ser necesarios. Si un protocolo es necesario, es importante comprender sus debilidades y cómo puede ser asegurado.

Acceso Físico

La mayoría de los access points son fácilmente accesibles. Normalmente están ubicados cerca de los usuarios y fuera de habitaciones cerradas. Esto pone a los access points en peligro de ser robados y al alcance de usuarios malintencionados. Se puede usar la supervisión de la red para determinar cuándo un access point se desactiva. Se necesitará seguir procedimientos apropiados para determinar lo que le sucedió al equipo. Casi todos los fabricantes de tecnología inalámbrica publican los métodos para reconfigurar un access point usando botones de reset o el puerto consola.

Firmware

El último firmware normalmente será el más seguro. El firmware nuevo deberá ser probado y usado. Se deberán aplicar parches de seguridad o actualizaciones cuando se justifique.

Acceso por Consola

Las cuentas y los privilegios del administrador deberán estar configurados correctamente.² El puerto consola debería estar protegido por una password. Elija una password segura.³

Telnet/SSH

Telnet es un protocolo no encriptado e inseguro. Si es posible, se deberá usar un shell seguro [secure shell (SSH)] para todas las funciones de la Interfaz de Línea de Comando (CLI).⁴ Telnet y SSH deberán estar protegidos con passwords. Para máxima seguridad, desactive Telnet y use sólo SSH.

Se necesita un cliente SSH en la PC de administración o en la estación de trabajo para conectarse a un AP que corre SSH. Hay varios programas freeware que están disponibles como PuTTY, Teraterm SSH y SecureNetTerm.

Security Summary		
Administrators		
Username	Read-Only	Read-Write
user1		✓
user2		✓
user3		✓
ppatrick		✓
tonorwoo		✓
SSIDs		
SSID	VLAN	Open
AP3	none	✓
Server-Based Security		
Server Name/IP Address	EAP	MAC
	Proxy Mobile IP	Admin
	Accounting	

Figura 2

Security: Admin Access	
Administrator Authenticated by: <input checked="" type="radio"/> Default Authentication (Global Password) <input type="radio"/> Local User List Only (Individual Passwords) <input type="radio"/> Authentication Server Only <input type="radio"/> Authentication Server if not found in Local List	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Default Authentication (Global Password)	
Default Authentication Password: <input type="password" value="*****"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Local User List (Individual Passwords)	
User List:	Username: <input type="text"/> Password: <input type="password"/> Confirm Password: <input type="password"/>
<input type="button" value="Delete"/>	Capability Settings: <input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figura 3

TFTP/FTP

El Protocolo de Transferencia Trivial de Archivos (TFTP) y el Protocolo de Transferencia de Archivos (FTP) son usados para enviar y recibir archivos a través de una red. TFTP no permite que se utilicen passwords, y está limitado a archivos menores a 16 Mb. FTP permite nombres de usuario y passwords, pero aun es un protocolo no encriptado.

SSID

Como se mencionó antes, el SSID no debería ser considerado como una característica de seguridad. Los SSIDs pueden ser usados en conjunto con las VLANs para permitir el acceso limitado a invitados.

Services: Telnet/SSH				
Telnet:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
Terminal Type:	<input checked="" type="radio"/> Teletype <input type="radio"/> ANSI			
Columns:	80 (64-132)			
Lines:	24 (16-50)			
Secure Shell Configuration				
Secure Shell:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
System Name:	AccessPoint			
Domain Name:	cisco.com			
RSA Key Size (optional): (360-2048 bits)			
Authentication Timeout (optional):	120 (1-120 sec)			
Authentication Retries (optional):	3 (0-5)			
Secure Shell Server Connections				
Connection	Version	Encryption	State	Username

Figura 4

8.3.2 Activación de filtros de protocolo y de MAC en APs

El filtrado puede proporcionar una capa adicional de seguridad inalámbrica. Los filtros pueden ser creados para filtrar un Protocolo o un puerto IP. Los filtros de protocolos evitan o permiten el uso de protocolos específicos a través del access point. Los filtros de protocolos individuales pueden ser creados y activados para una o más VLANs. Los filtros MAC, Ethertype e IP pueden ser usados para filtrar dispositivos clientes inalámbricos, usuarios en la LAN cableada, o ambos.¹

APPLY FILTERS MAC ADDRESS FILTERS IP FILTERS ETHERTYPE FILTERS				
Hostname AccessPoint		AccessPoint uptime is 2 weeks, 2days, 22 hours, 50 minutes		
Services: Filters - Apply Filters				
	Ethernet		802.11b Radio	
Incoming	MAC	<NONE> <input type="button" value="▼"/>	MAC	<NONE> <input type="button" value="▼"/>
	Ethertype	<NONE> <input type="button" value="▼"/>	Ethertype	<NONE> <input type="button" value="▼"/>
	IP	<NONE> <input type="button" value="▼"/>	IP	<NONE> <input type="button" value="▼"/>
Outgoing	MAC	<NONE> <input type="button" value="▼"/>	MAC	<NONE> <input type="button" value="▼"/>
	Ethertype	<NONE> <input type="button" value="▼"/>	Ethertype	<NONE> <input type="button" value="▼"/>
	IP	<NONE> <input type="button" value="▼"/>	IP	<NONE> <input type="button" value="▼"/>

Figura 1

Por ejemplo, un filtro SNMP en el puerto de radio del access point evita que los dispositivos clientes inalámbricos usen SNMP con el access point pero no bloquea el acceso de SNMP desde la LAN cableada.

8.3.3 Seguridad en clientes y APs

La seguridad del cliente es importante, porque asegurando simplemente a los access points no se protege a una red inalámbrica. Después de que estén protegidas las debilidades de los access points, el ataque a los clientes se convierte en la forma más fácil de obtener acceso a la red. La seguridad apropiada para los clientes debería ser especificada en la política de seguridad inalámbrica. Esto incluye medidas de seguridad como búsqueda de virus, firewalls personales y mantener a los programas clientes y a los sistemas operativos actualizados.

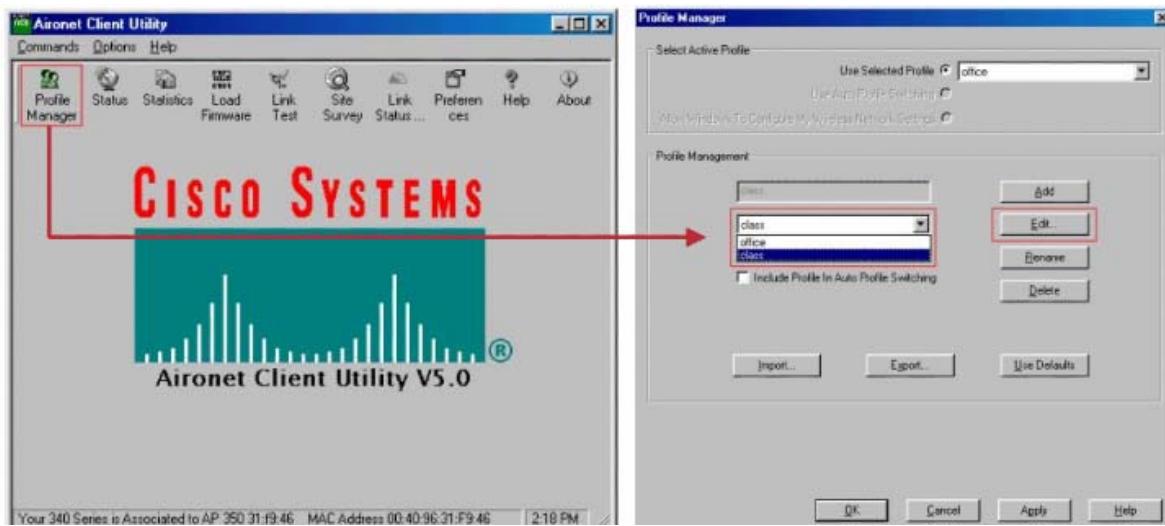


Figura 1

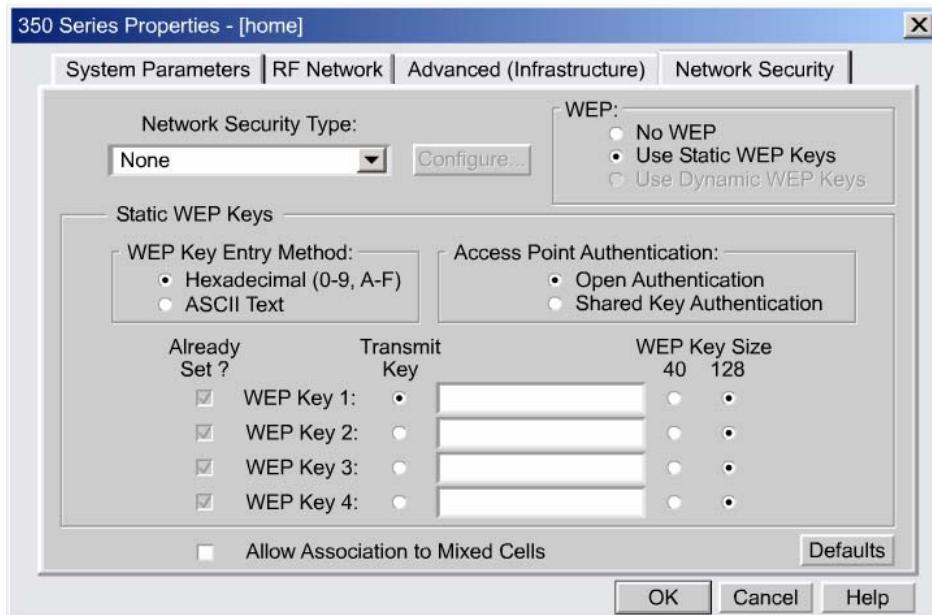


Figura 2

Puede ser deseable el tener seguridad adicional para clientes inalámbricos. Por ejemplo, WEP debería ser activado cuando sea posible. Como se dijo antes, la WEP estática tiene debilidades. Características de seguridad adicionales, como la clave por paquete de protocolo de integridad de clave temporal (TKIP) y el Control de Integridad de Mensajes (MIC), necesitan estar activas para la seguridad adicional. Esto será tratado en la sección de encriptación empresarial.

Las Figuras 1 y 2 muestran la pantalla del Utilitario del Cliente Aironet (ACU) para configurar claves WEP. Además de los clientes, los APs y los bridges deben ser asegurados usando WEP.³

No importa el tipo de autenticación que se esté usando, las claves WEP ingresadas en el cliente y en el access point deben coincidir. Las claves mismas deben coincidir, y el orden de las claves debe coincidir. Por ejemplo, una clave de 40 bits ingresada como Clave 1 en el cliente debe coincidir con la clave de 40 bits ingresada como Clave 1 en el access point.

Security : WEP Key Manager

Set encryption Mode and Keys for VLAN: <NONE> [Define VLANs](#)

Encryption Modes

- None
- WEP Encryption [Mandatory](#)

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

WEP Keys

Encryption Keys

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	128 bit
Encryption Key 2:	128 bit
Encryption Key 3:	128 bit
Encryption Key 4:	128 bit

Broadcast Key Rotation Interval: Disable Rotation
 Enable Rotation with Interval: [DISABLED \(1-10000000 SEC\)](#)

Figura 3

8.3.4 Supervisión del equipo WLAN

El registro de eventos a través de SNMP o Syslog es muy importante en el proceso de seguridad general. Como se muestra en la Figura 1, los niveles de notificación de eventos pueden ser definidos para SNMP y Syslog. Debe estar definido un servidor Syslog para que se puedan enviar mensajes Syslog a un servidor de supervisión central.² La configuración de Syslog y de SNMP será tratada en detalle en el Módulo 11.

Event Log : Configuration Options

Disposition of Events (by Severity Level):

	Display on Event Log	Notify via SNMP/Syslog Trap	Record for SNMP/Syslog History Table	Display on Telnet/SSH Monitor
◆ Emergency	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Alert	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Critical	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Error	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Warning	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Notification	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Information	<input checked="" type="checkbox"/> Display	<input checked="" type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor
◆ Debugging	<input checked="" type="checkbox"/> Display	<input type="checkbox"/> Notify	<input checked="" type="checkbox"/> Record	<input checked="" type="checkbox"/> Monitor

Time Stamp Format for Future Events: System Uptime Global Standard Time Local Time

Event Log Size: (4-2147483) kilobytes

History Table Size: (0-500) Messages

Figura 1

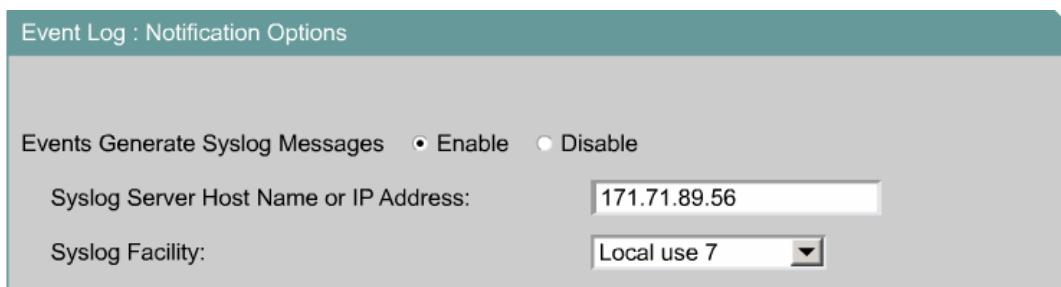


Figura 2

Protocolo Simple de Administración de Red (SNMP)

SNMP permite que los programas de administración de red vean y cambien configuraciones de equipos. SNMP puede ser usado para ver configuraciones usando un pedido Get. SNMP también puede ser usado para cambiar las configuraciones usando un pedido Set. Finalmente, los dispositivos SNMP pueden enviar alertas a las estaciones de administración usando la función Trap. SNMP utiliza un secreto no encriptado llamado cadena o nombre de comunidad. Los nombres de comunidad de sólo lectura sólo permiten pedidos Get, mientras que los nombres de comunidad de lectura y escritura permiten pedidos Get y Set. Las versiones 1 y 2 de SNMP son inseguras, porque el nombre de comunidad puede ser visto en los pedidos. La versión 3 de SNMP agrega seguridad adecuada, pero aun no está ampliamente usada o soportada. Nunca utilice public o private como nombres de comunidad porque son los predeterminados. Utilice un nombre de comunidad que cumpla con las pautas de passwords seguras.³

Services: SNMP - Simple Network Management Protocol

SNMP Properties

Simple Network Management Protocol (SNMP): • Enabled • Disabled

System Description: Cisco 110 Access Point 12.2

System Name (optional): FOC064206UD

System Location (optional): bldg 8 first floor

System Contact (optional): tonorwoo #72250

SNMP Request Communities

Current Community Strings Edit Community Strings

<NEW>
private
public

Delete SNMP Community: []
Object Identifier (optional): []
• Read-Only • Read-Write

SNMP Trap Community

SNMP Trap Destination: 171.71.89.56 (Hostname or IP Address)
SNMP Trap Community: private

• Enable All Trap Notifications
• Enable Specific Traps

802.11 Event Traps Encryption Key Trap
QOS Change Trap Standby Switchover Trap
Syslog Trap Rogue AP Trap

Figura 3

Recuerde que parte de la seguridad es la supervisión continua. La mayor parte de la supervisión de la red se realiza con una combinación de protocolo de mensaje de control de internet (ICMP) y SNMP. La registración de SNMP y de eventos está tratada con más detalle en el Módulo 11.

8.3.5 Desactivación de servicios no necesarios

Es importante desactivar o asegurar todos los servicios no necesarios. Por ejemplo, si el protocolo de descubrimiento de Cisco (CDP) **1**, el servicio de nombre de dominio (DNS), el protocolo de tiempo de la red (NTP) **2**, el protocolo de transferencia de hipertexto (HTTP) **3**, TFTP, SNMP y Telnet no son usados en la red, deberían ser desactivados

Services: CDP-Cisco Discovery Protocol

CDP Properties

Cisco Discovery Protocol (CDP): Enabled Disabled

Packet Hold Time (optional): (10-255 sec)

Packets Sent every (optional): (5-254 sec)

Individual Port Enable:

Ethernet
 AP Radio

CDP Neighbors Table

Device ID	Interface	Hold Time	Capability	Platform	Port ID
cat3524	FastEthernet 0	174	T S	WS-C3524-P	0/9

Figura 1

Services: NTP-Network Time Protocol

NTP Server

Network Time Protocol (NTP): Enabled Disabled

Time Server (optional): (Hostname or IP Address)

Time Settings

GMT Offest: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London (hrs)

Use Daylight Savings Time: Yes No

Manually Set Date: (yyy/mmm/dd)

Manually Set Time: (hh:mm:ss)

Figura 2

Services: HTTP-Web Server

Allow Web-based Configuration Management: Enabled Disabled

HTTP Port: (0-65535)

Default Help Root URL:

Figura 3

HTTP/Administración Web

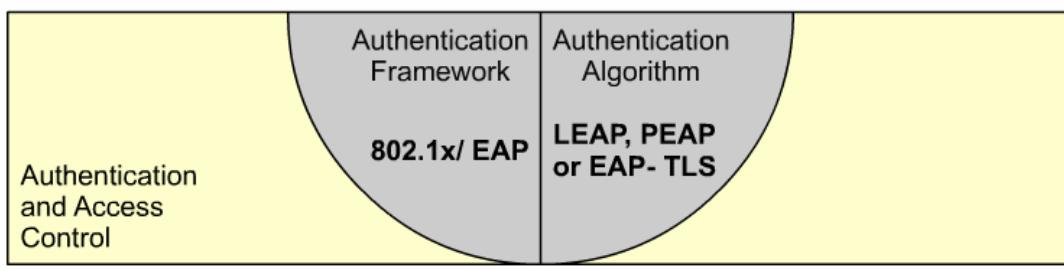
El uso de HTTP/Administración Web es útil, pero si se usa sobre el equipo de la red puede debilitar la seguridad de la red. Muchos fabricantes tienen serios problemas en su software de servidor Web. Para una máxima seguridad, HTTP deberá estar desactivado en una red de producción. Si se utiliza HTTP, deberá estar protegido con una password. Si la vulnerabilidad está publicada, deberá consultarse a asesores de seguridad del fabricante y se deberá aplicar nuevo firmware.

A menos que sean necesarios, TFTP y FTP no deberían estar activados. Algunos fabricantes usan esquemas TFTP muy débiles, lo que permite que el archivo de configuración sea bajado por cualquier usuario. Como el archivo de configuración contiene passwords y claves WEP, la seguridad puede estar comprometida.

8.4 Autenticación WLAN Empresarial

8.4.1 Autenticación de segunda generación

Los diseñadores de red y los expertos en seguridad saben que no es suficiente arreglar las debilidades de WEP. La Figura 1 muestra algunos de los requisitos y soluciones para asegurar las WLANs. La verdadera seguridad inalámbrica requiere más que sólo hacer dinámicas las claves WEP o mejorar el WEP. La verdadera seguridad inalámbrica debe poder autenticar a los usuarios, no sólo a los dispositivos, como lo ilustra la Figura 2.



LEAP = Lightweight EAP, also called EAP-Cisco,

PEAP = Protected EAP

EAP-TLS = EAP-Transport Layer Security

Figura 1

Security Requirements for WLANs

First generation security

- SSID
- Static 40 or 128-bit WEP

Second generation security

- Centralized user-based authentication (ACS 2000 v2.60 integrated with network logon)
- Dynamic 128-bit WEP
- VPN
- Access control lists

Leading edge security

- TKIP
- MIC
- AES
- Rogue AP detection

Figura 2

Las organizaciones deben decidir cuánta seguridad necesitan e incluirla en la política de seguridad inalámbrica. Algunas redes dependerán de soluciones VNP existentes para proporcionar seguridad adicional. Otras redes implementarán el control de acceso y los arreglos para WEP, que están incluidos en el Acceso Protegido Wi-Fi (WPA). WPA utiliza elementos de 802.11i, una solución de seguridad estandarizada de más largo plazo, para asegurar las WLANs. WPA también es llamado Networking de Seguridad Simple (SSN). Algunos administradores de red pueden decidir esperar al 802.11i antes de desarrollar las WLANs. Las secciones siguientes hablarán sobre lo que está mal en la seguridad WEP y qué está faltando.

8.4.2 Autenticación de usuarios inalámbricos

Algunas limitaciones WEP están en la Figura 1. Una severa limitación de una WLAN con sólo WEP es que los usuarios no se autentican. WPA permite la autenticación de usuarios a través del protocolo IEEE 802.1x. 802.1x es un estándar terminado recientemente para controlar la entrada a las LANs cableadas e inalámbricas. 802.1x proporciona autenticación mutua. La autenticación mutua significa que la red y el usuario se intercambian las identidades, como lo indica la Figura 2.

Limitations of IEEE 802.11 Security

- Authentication**
 - Authentication is device based, not user based
 - Client does not authenticate network
 - Existing authentication databases are not leveraged
- Key management**
 - Keys are static
 - Keys are shared among devices and APs
 - If adapter or device is stolen all devices and APs must be re-keyed
- RC4- based WEP keys**
 - Encryption algorithm is vulnerable to attack
 - Message integrity is not ensured

Figura 1

IEEE 802.1x for 802.11

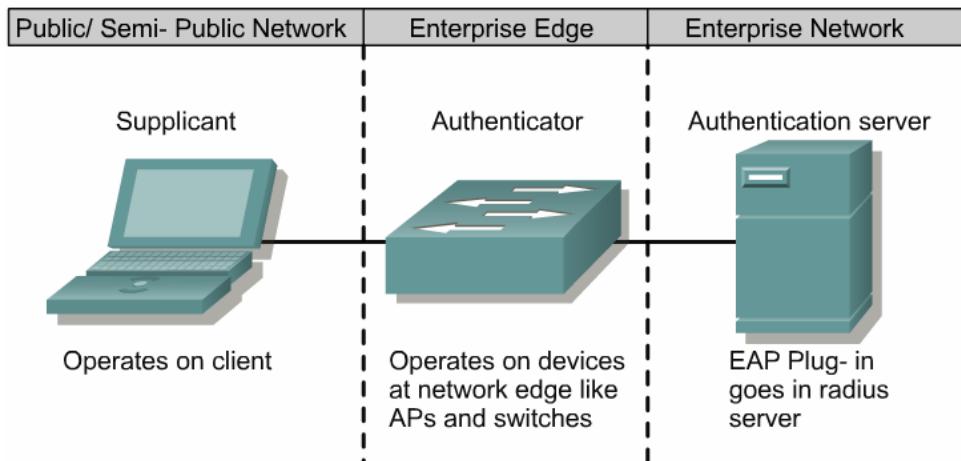
- Part of 802.11i standard
- Supported by Cisco since 2000
- Extensible and interoperable
 - Support: Different authentication methods or types.
 - New encryption algorithms, including Advanced Encryption Standard(AES) as a replacement for RC4
- Key management**
 - Keys are static
 - Keys are shared among devices and APs
 - If adapter or device is stolen all devices and APs must be re-keyed
- RC4- based WEP keys**
 - Encryption algorithm is vulnerable to attack
 - Message integrity is not ensured

Figura 2

El estándar 802.11i también utiliza 802.1x y las mejoras TKIP para WEP. Una ventaja del estándar 802.1x es que puede soportar una variedad de tipos de autenticación. Un access point que soporta 802.1x y a su protocolo, el Protocolo de Autenticación Extensible (EAP), actúa como la interfaz entre un cliente inalámbrico y un servidor de autenticación como el servidor de Servicio al Usuario de Acceso Telefónico Remoto [Remote Access Dial-In User Service (RADIUS)]. El access point se comunica con el servidor RADIUS a través de la red cableada.

8.4.3 Fundamentos de 802.1x

802.1x requiere soporte en el cliente, en el access point y en el servidor de autenticación, como lo ilustra la Figura 1. 802.1X utiliza un proxy RADIUS para autenticar a los clientes en la red. Este dispositivo proxy podría ser un switch o un access point. Este dispositivo trabaja en la capa de acceso.

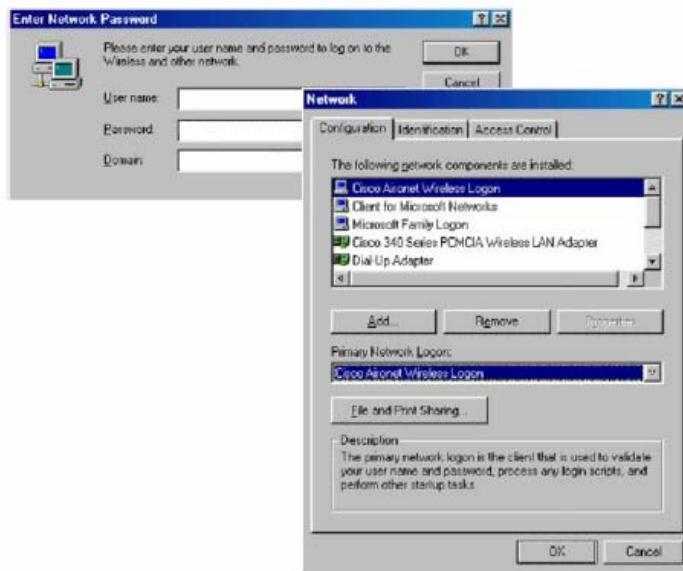


802.1x requires support on the client, the access point, and the authentication server.

Figura 1

El cliente o solicitante EAP envía las credenciales de autenticación al autenticador el que a su vez envía la información al servidor de autenticación, donde el pedido de ingreso es comparado con una base de datos de usuarios para determinar si el usuario puede obtener acceso a los recursos de la red, y a qué nivel. El access point recibe el nombre de autenticador. El servidor de autenticación es normalmente un RADIUS o un servidor de autenticación, autorización y contabilidad (AAA). El servidor de autenticación necesita ejecutar un software extra para comprender el tipo de autenticación que está usando el cliente.

Cualquier cliente que no tiene incorporado el 802.1x debe usar un software llamado solicitante [supplicant]. La Figura 2 muestra al cliente Microsoft Windows 2000. Microsoft XP tiene incorporado el EAP que proporciona soporte a 802.1x. La Figura 3 muestra al cliente Cisco LEAP. El cliente debe tener alguna prueba de su identidad. Las formas de identidad incluyen un nombre de usuario y password, certificación digital, o password ocasional [one-time password (OTP)].



- Use with EAP requires a client
- Referred to as a supplicant

Figura 2

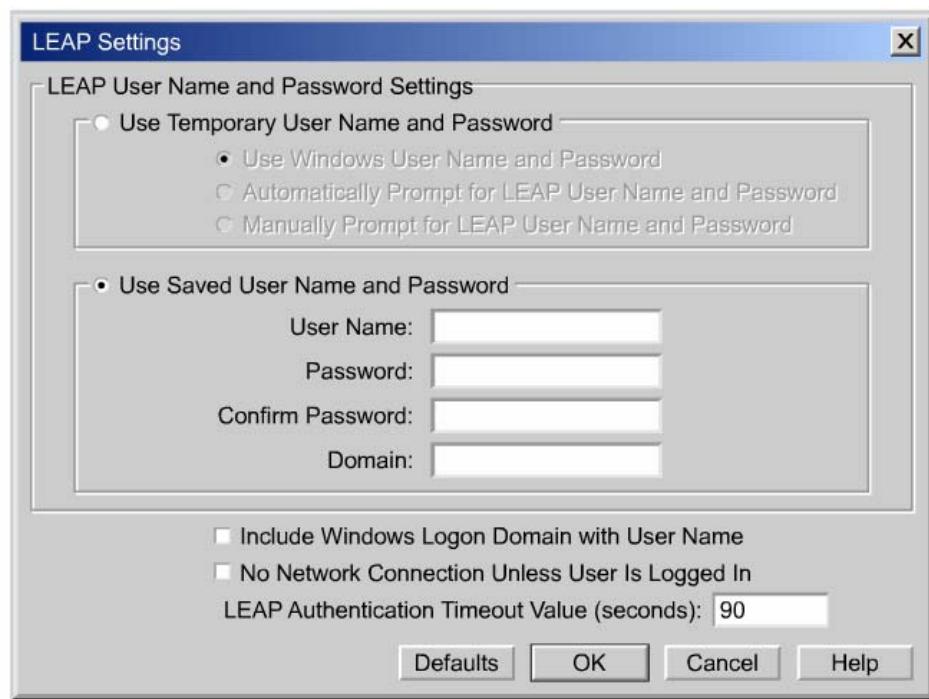
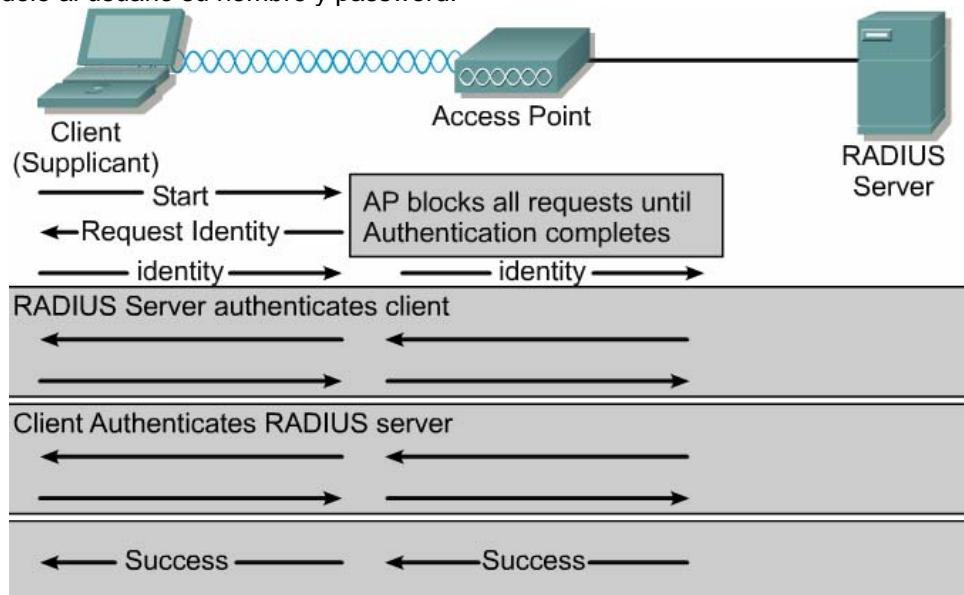


Figura 3

8.4.4 Cómo funciona 802.1x

La Figura 1 proporciona una descripción general de la forma en que trabaja el 802.1x. Después de que el cliente se ha asociado al access point, el solicitante comienza el proceso para usar EAPOL (EAP sobre LAN) pidiéndole al usuario su nombre y password.



802.1x requires support on the client, the access point, and the authentication server.

Figura 1

El cliente responde con su nombre de usuario y password. Usando 802.1X y EAP el solicitante luego envía el nombre de usuario y un hash de un sentido de la password al access point. El access point luego encapsula el pedido y lo envía al servidor RADIUS.

El servidor RADIUS luego compara el nombre de usuario y la password con la base de datos para determinar si el cliente debería ser autenticado en la red. Si el cliente debe ser autenticado, el servidor RADIUS emite luego un desafío de acceso, que es pasado al access point y después enviado al cliente.

El cliente envía la respuesta EAP para el desafío de acceso al servidor RADIUS a través del access point. Si el cliente envía la respuesta correcta entonces el servidor RADIUS envía un mensaje de acceso exitoso y una clave WEP (EAP sobre Inalámbrico) al cliente a través del access point. La misma clave WEP de sesión también es enviada al access point en un paquete exitoso.

El cliente y el access point luego comienzan a usar las claves WEP de sesión. La clave WEP usada para multicast es luego enviada desde el access point hacia el cliente. Es encriptada usando la clave WEP de sesión.

Ante la desconexión del cliente, el access point vuelve al estado inicial, permitiendo que sólo pase tráfico 802.1X.

8.4.5 Tipos de autenticación de 802.1x

	LEAP	EAP- TLS	EAP- PEAP
Server Authentication	Password	Certificates/public Key Infrastructure (Certs/ PKI)	Certs/ PKI
Client Authentication	Password	Certs/ PKI	Password ¹
Single Sign On	Yes	Yes	No ²
Vulnerable to Password Attack	No ³	No	No
OTP/ LDAP Support	No	N/A	Yes
Additional Infrastructure	No	Yes/ Certificate Authority (CA)	Yes/ CA

¹ Not limited to password schemes, but that is what is currently available
² MS native supplicant supports SSo w/ EAP -MS- CHAP v2
³ Requires strong passwords

Figura 1

Cuando se utiliza 802.1x sobre una WLAN están soportados diferentes tipos de autenticaciones. [1](#)

- LEAP - EAP Liviano [Lightweight EAP (LEAP)] es también llamado EAP-Cisco. LEAP es la versión de Cisco de EAP. Es para usar sobre redes que actualmente no soportan EAP. Las versiones actuales de EAP pueden no proporcionar la funcionalidad que se necesita y pueden ser demasiado exigentes. Esto podría comprometer el rendimiento del equipo WLAN. LEAP es una buena opción cuando se utiliza equipo Cisco junto con sistemas operativos como Windows 95, Windows 98, Windows Me, Windows CE, Windows NT/2000/XP y Linux.
- EAP-TLS - La EAP-Seguridad de Capa de Transporte [EAP-Transport Layer Security (EAP-TLS)] es una opción de seguridad de trabajo intensivo. EAP-TLS requiere que haya un certificado digital configurado en todos los Clientes WLAN y en el Servidor. EAP-TLS está basado en certificados X.509. Normalmente es más fácil de usar que PEAP, que está basado en EAP-TLS.
- PEAP - EAP Protegido [Protected EAP (PEAP)] es un tipo de autenticación EAP borrador que está diseñado para permitir la autenticación híbrida. PEAP emplea la autenticación PKI del lado del servidor. Para la autenticación del lado del cliente, PEAP puede usar cualquier otro tipo de autenticación EAP. Como PEAP establece un túnel seguro por medio de la autenticación del lado del servidor, se pueden usar tipos de EAP no mutuamente autenticables para la autenticación del lado del cliente. Las opciones de autenticación del lado del cliente incluyen EAP-GTC para passwords ocasionales y EAP-MD5 para autenticación basada en password. PEAP está basado en EAP-TLS del lado del servidor y soluciona los defectos de administrabilidad y escalabilidad de EAP-TLS. Las organizaciones pueden evitar los problemas relacionados con la instalación de certificados digitales en cada máquina cliente como lo requiere EAP-TLS. Ellas pueden luego seleccionar el método de autenticación del cliente que mejor les convenga.
- EAP-MD5 - El Protocolo de Autenticación Extendible MD5 [Extensible Authentication Protocol MD5 (EAP-MD5)] no debería ser usado, porque no proporciona autenticación mutua. EAP-MD5 es una autenticación de un sentido que esencialmente duplica la protección de password CHAP en una WLAN. EAP-MD5 se utiliza como un bloque de construcción en EAP-TTLS.
- EAP-OTP - EAP-Passwords Ocasionales [EAP-One Time Passwords (EAP-OTP)] también recibe el nombre de EAP-Tarjeta Token Genérica [EAP- Generic Token Card (EAP-GTC)]. No es recomendable, ya que las OTPs no son una forma de autenticación mutua.
- EAP-SIM - EAP-SIM utiliza la misma tarjeta inteligente o SIM que se utiliza en los teléfonos móviles GSM para proporcionar autenticación. EAP-SIM puede fácilmente montarse sobre EAP-TLS.

- EAP-TTLS - EAP-Seguridad de Capa de Transporte en Túnel [EAP-Tunneled Transport Layer Security (EAP-TTLS)] es un borrador IETF creado por Funk software y Certicom. EAP-TTLS provee una funcionalidad similar a PEAP. EAP-TTLS protege las passwords usando TLS, que es una forma avanzada de Capa de Socket Seguro [Secure Socket Layer (SSL)]. EAP-TTLS actualmente requiere un servidor RADIUS de Funk software.
- Kerberos - Kerberos no es parte del estándar 802.1x, sino que está siendo promocionado por algunos fabricantes. Kerberos es un sistema de autenticación que permite la comunicación protegida sobre una red abierta, que utiliza una clave única llamada ticket. Requiere configuración del servicio. PEAP puede soportar Kerberos a través del EAP-Servicio de Seguridad Genérico [EAP-Generic Security Service (EAP-GSS)].

8.4.6 Elección de un tipo de 802.1x

Es importante elegir un tipo de 802.1x que sea lo más compatible con la red existente. Los métodos disponibles son LEAP, EAP y PEAP. 802.1x no especifica el tipo de autenticación a usar. Las consideraciones principales a tener en cuenta cuando se elige un tipo de autenticación son la integración sencilla y la seguridad adecuada.

Extensible Authentication Protocol (EAP) Type Criteria	
Must support mutual authentication	
• Network authenticates client	
• Client authenticates network	

Figura 1

La Figura 1 proporciona una lista de los principales elementos a considerar antes de utilizar una seguridad basada en 802.1x:

- Elija un método que se integre bien con la red existente.
- Elija un método que soporte la autenticación mutua.
- Revise la política de seguridad y averigüe cuáles tipos de 802.1x son compatibles.
- Finalmente, vea que los clientes estén protegidos y elija la mejor forma de asegurar al equipo existente.

LEAP

LEAP proporciona una solución WLAN completa. LEAP debería utilizarse cuando se necesita un inicio de sesión único al dominio de Windows NT o cuando se necesita un Active Directory. El Active Directory es un componente esencial de la arquitectura del Windows 2000 y presenta organizaciones con un servicio de directorio diseñado para entornos de computación distribuidos. El Active Directory permite que las organizaciones administren y compartan información sobre los recursos y usuarios de la red en forma centralizada mientras que actúa como la autoridad central para la seguridad de la red. Además de proporcionar servicios de directorio extensos a un entorno Windows, Active Directory está diseñado para ser un punto de consolidación para aislar, migrar, administrar en forma centralizada y reducir la cantidad de directorios que requiere la compañía.

LEAP también puede ser usado cuando se necesita una clave WEP dinámica y autenticación mutua. Recuerde que se debería usar TKIP para asegurar el LEAP.

EAP-TLS

EAP debería ser usado cuando se necesita utilizar certificados digitales para la identificación de los usuarios. EAP es la mejor solución cuando hay una Infraestructura de Clave Pública (PKI) existente en el lugar. PKI asegura que las comunicaciones electrónicas sensibles sean privadas y estén protegidas contra la manipulación. Proporciona garantías en las identidades de los participantes en esas transacciones, y evita su rechazo posterior en la participación en la transacción.

EAP-TLS también puede ser usado para vincular el ingreso con el NT/2000 y el Protocolo Liviano de Acceso a Directories [Lightweight Directory Access Protocol (LDAP)]. LDAP le permite usar servicios de directorio para integrar un cliente de Registro de Red [Network Registrar] e información de arrendamiento. Al construir el esquema de estándares existentes para objetos almacenados en directorios LDAP, puede manipular la información sobre entradas de clientes del protocolo de configuración dinámica de hosts (DHCP). Así, en lugar de mantener la información de los clientes en la base de datos del servidor DHCP, puede pedir que el servidor DHCP de Registro de Red envíe consultas a uno o más servidores LDAP para obtener información en respuesta a las peticiones del cliente DHCP.

PEAP

PEAP puede ser usado cuando la clave WEP y la autenticación mutua son necesarios. Recuerde que debería utilizarse el TKIP para asegurar el LEAP

EAP-TLS también puede ser usado para vincular el ingreso con NT/2000, LDAP, Servicios de Directorio de Novell (NDS), servidores de Passwords Ocasionales (OTP) y servidores de base de datos de lenguaje de consulta estructurado (SQL). Cuando se utiliza PEAP, los certificados digitales son necesarios sólo en el lado del servidor.

8.5 Encriptación Inalámbrica Empresarial

8.5.1 Fortalecimiento WEP

WPA incluye mecanismos del estándar emergente 802.11i para mejorar la encriptación de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Estas tecnologías son fácilmente implementadas usando la interfaz gráfica de usuario (GUI) del AP de Cisco.

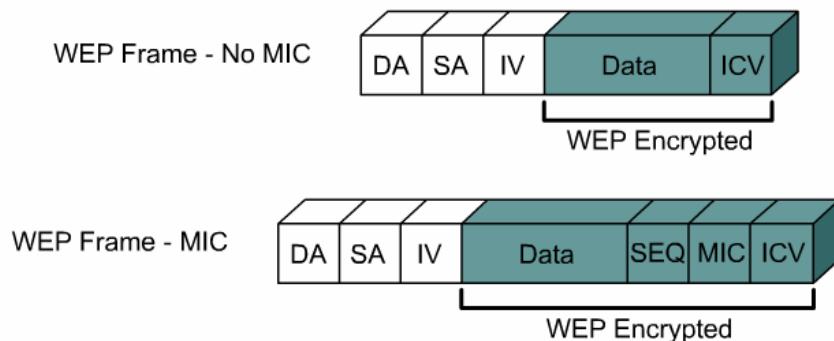
TKIP es también llamado hashing de Clave WEP y recibió inicialmente el nombre WEP2. TKIP es una solución temporal que soluciona el problema de reutilización de clave de WEP. WEP utiliza periódicamente la misma clave para encriptar los datos. El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los access points. TKIP combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que encriptará a los datos. Este procedimiento asegura que cada estación utilice diferentes streams claves para encriptar los datos. El hashing de clave WEP protege a los Vectores de Inicialización (IVs) débiles para que no sean expuestos haciendo hashing del IV por cada paquete.

TKIP utiliza el RC4 para realizar la encriptación, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que el TKIP cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red.

Una ventaja de usar TKIP es que las compañías que tienen access points basados en WEP y NICs de radio pueden actualizarse a TKIP a través de patches de firmware relativamente simples. Además, el equipo sólo WEP aún interoperará con los dispositivos con TKIP activado usando WEP. TKIP es sólo una solución temporal. La mayoría de los expertos creen que aun es necesaria una encriptación más fuerte.

8.5.2 Control de la integridad de los mensajes

Las mejoras de TKIP, como MIC, proveen claves WEP más fuertes. MIC evita los ataques de bit-flip en paquetes encriptados. Se muestra en la Figura 1. Durante un ataque bit-flip, un intruso intercepta un mensaje encriptado, lo altera levemente y lo retransmite. El receptor acepta el mensaje retransmitido como legítimo. El controlador y el firmware del adaptador cliente deben soportar la funcionalidad del MIC, y MIC debe estar activo en el access point. Las mejoras de TKIP, como MIC y hashing de Clave WEP pueden ser activados usando claves WEP estáticas. No necesitan un servidor RADIUS para funcionar.



- MIC uses a hashing algorithm to stamp frame
- The MIC is still pre-standards, awaiting 802.11i ratification

Figura 1

8.5.3 Rotación de clave de broadcast [Broadcast key rotation (BKR)]

La característica Rotación de Clave de Broadcast (BKR), descripta en la Figura 1, es también una mejora de TKIP. BKR protege al tráfico multicast del access point para que no sea explotado cambiando dinámicamente la clave de encriptación. El access point genera claves WEP de broadcast usando un generador de números pseudo aleatorios [pseudorandom number generator (PRNG)] sembrados. El access point rota la clave de broadcast después de que se agota un temporizador configurado de clave WEP de broadcast. Este proceso por lo general debería estar en sincronía con los tiempos vencidos configurados en los servidores RADIUS para la re-autenticación de los usuarios. La rotación de clave de broadcast es una excelente alternativa al hashing de clave WEP. Esto es cierto si la WLAN soporta dispositivos clientes inalámbricos que no son dispositivos Cisco o que no pueden ser actualizados con el último firmware para dispositivos clientes de Cisco. Se recomienda que la rotación de clave de broadcast esté activa cuando el access point sirve a una LAN inalámbrica exclusiva de 802.1x. No es necesario activar la rotación de clave de broadcast si el hashing de clave WEP está activado. El uso de la rotación de clave y de hashing de clave provee de protección innecesaria. Cuando la rotación de clave de broadcast está activada, sólo pueden usar el access point los dispositivos clientes inalámbricos que usan autenticación LEAP o EAP-TLS. Los dispositivos clientes que usan WEP estática con clave abierta compartida o autenticación EAP-MD5 no pueden usar el access point cuando la rotación de clave de broadcast está activada.

- Broadcast key is required in 802.1X environments
- Re-keying of broadcast key is necessary, just as with unicast key
- Key is delivered to client encrypted with client's dynamic key

Figura 1

8.5.4 Encriptación de segunda generación

Además de la solución TKIP, el estándar 802.11i es muy probable que incluya al protocolo Estándar Avanzado de Encriptación [Advanced Encryption Standard (AES)], como muestra la Figura 1. AES ofrece una encriptación mucho más fuerte. En efecto, el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los EE.UU. eligió al AES para reemplazar el DES obsoleto. El AES es ahora un Estándar de Procesamiento de Información Federal (FIPS) de los EE. UU., Publicación 197. Define un algoritmo criptográfico para ser usado por las organizaciones gubernamentales de los EE.UU. para proteger la información delicada no clasificada. La Secretaría de Comercio aprobó la adopción del AES como un estándar oficial del Gobierno en Mayo del 2002.

Sin embargo, está el problema de que AES requiere un coprocesador o un hardware adicional para funcionar. Esto significa que las compañías necesitan reemplazar los access points y las NICs clientes existentes para implementar AES. Basado en reportes de marketing, la base instalada actualmente es relativamente pequeña comparada con el desarrollo futuro predicho. Como resultado, habrá un porcentaje muy alto de nuevas implementaciones de WLAN que tomarán ventaja del AES cuando sea parte del 802.11. Por otra parte, las compañías que ya han instalado las WLANs necesitarán determinar si vale la pena los costos de actualizar para una mejor seguridad.

Advanced Encryption Standard (AES) - Successor to Triple-DES

Mandatory for 802.11i compliance

Rijndael Algorithm

- Block Cipher
- 128, 192, and 256 bit key support

3DES Successor Sponsored by National Institute of Standards in Technology (NIST)

Figura 1

Advanced Encryption Standard (AES) - Successor to Triple-DES

- Provides stronger encryption algorithm than RC4
- Includes MIC
- Supports key lengths of up to 256 bits
- Works with static and dynamic (802.1x) keys
- Is accepted by U.S. federal government for FIPS compliance
- For best performance, requires hardware (radio) implementation

Figura 2

AES especifica tres tamaños de claves, que son 128, 192 y 256 bits. Utiliza el Algoritmo Rijndael, como lo indica la Figura 2. Si alguien fuera a construir una máquina que pudiera recuperar una clave DES en un segundo, entonces el penetrar una clave AES de 128 bits le tomaría a esa máquina aproximadamente 149 billones de años. Para ponerlo en perspectiva, se cree que el universo tiene menos de 20 mil millones de años de edad.

8.5.5 Uso de VPNs

La Seguridad IP (IPSec) es un marco de trabajo de estándares abiertos para asegurar la comunicación privada segura sobre redes IPs. Las Redes Privadas Virtuales (VPNs) IPSec utilizan los servicios definidos dentro de IPSec para asegurar la confidencialidad, la integridad y la autenticidad de las comunicaciones de datos a través de redes como la Internet. La implementación del VPN está ilustrada en la Figura 1. IPSec también tiene una aplicación práctica para asegurar las WLANs. Logra esto superponiendo IPSec por sobre el tráfico inalámbrico de 802.11.

Cuando se implementa IPSec en un entorno WLAN, se coloca un cliente IPSec en cada PC conectada a la red inalámbrica. Se necesita que el usuario establezca un túnel IPSec y que enrute todo el tráfico hacia la red cableada, como lo muestra la Figura 1. Se colocan filtros para evitar que el tráfico inalámbrico llegue a cualquier destino que no sea el concentrador VPN y el servidor DHCP/DNS. Los clientes VPN también pueden ser terminados sobre un router IOS Firewall o un Aparato de Seguridad PIX.

IPSec proporciona confidencialidad al tráfico IP. También tiene capacidades de autenticación y anti-respuesta usando el Resumen de Mensajes 5 [Message Digest 5 (MD5)] o el Algoritmo Hash Seguro [Secure Hash Algorithm (SHA)]. La confidencialidad se logra a través de la encriptación, que utiliza el Estándar de Encriptación de Datos [Data Encryption Standard (DES)], el Triple DES (3DES) o el AES. El proceso se muestra en la Figura 3.

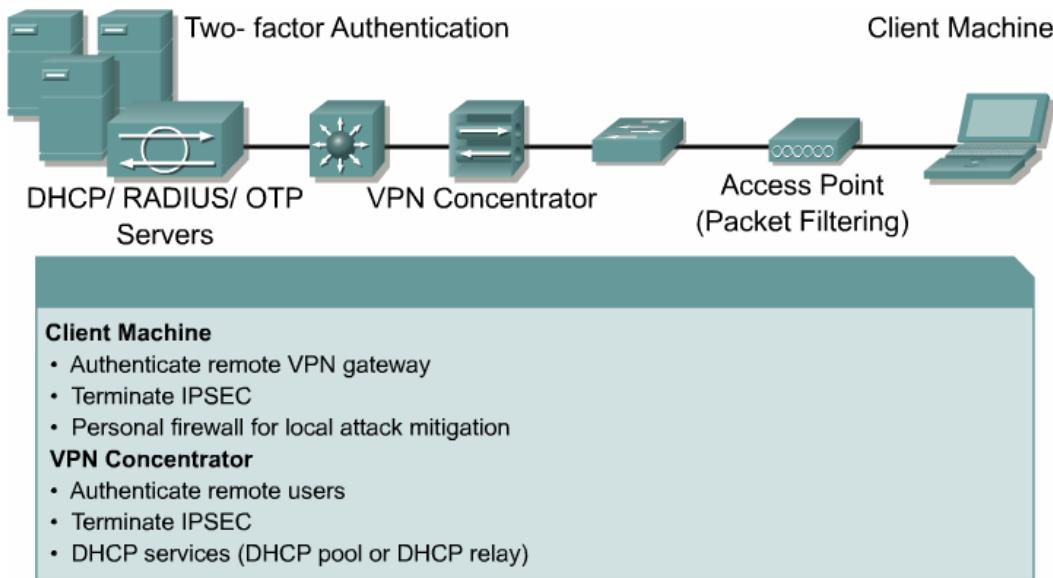


Figura 1



Figura 2

El filtrado puede proporcionar una capa adicional de seguridad inalámbrica. Los filtros pueden ser creados para filtrar un Protocolo o un puerto IP. Cuando un access point está diseñado para utilizarse sólo en VPN, se pueden usar filtros como el de la Figura 4. Estos filtros se utilizan para permitir sólo tráfico específico como la Carga de Seguridad Encapsulada [Encapsulated Security Payload (ESP)] y el Intercambio de Clave de Internet [Internet Key Exchange (IKE)], que son necesarios para asegurar la comunicación VPN.

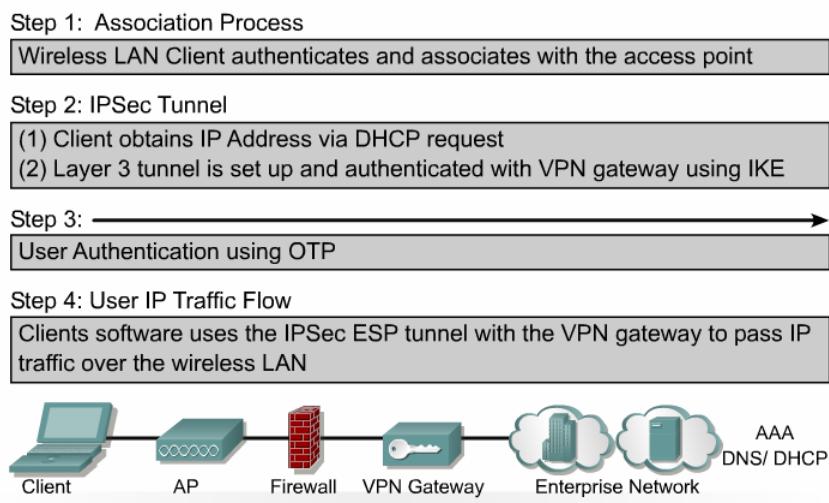


Figura 3

Filter Type	Protocol	Value	Disposition
Ethertype	ARP	0x0806	Forward
Ethertype	IP	0x0800	Forward
IP Protocol	UDP	17	17
IIP Protocol	ESP	50	50
IP Port	BootPC	68	Forward
IP Port	DNS	53	Forward
IP Port	IKE	500	Forward

Figura 4

8.6 Otros Servicios de Seguridad Empresariales

8.6.1 VLANs

Una red de área local virtual (VLAN) es una red comutada que está segmentada en forma lógica por funciones, equipos de proyectos o aplicaciones en lugar de estarlo en forma física o geográfica. Por ejemplo, todas las estaciones de trabajo y los servidores usados por un grupo de trabajo en particular puede estar conectado a la misma VLAN, sin importar sus conexiones físicas a la red o el hecho de que puedan estar entremezclados con otros equipos. Usted utiliza VLANs para reconfigurar la red a través de software en lugar de hacerlo físicamente desconectando y moviendo dispositivos o cables.

Una VLAN puede imaginarse como un dominio de broadcast que existe dentro de un conjunto definido de switches. Una VLAN consiste en una cantidad de sistemas terminales, hosts o equipos de red (como bridges y routers), conectados por un único dominio de bridging. El dominio de bridging está soportado en varios equipos de red como switches LAN que ejecutan protocolos de bridging entre ellos con un grupo separado para cada VLAN.

Las VLANs proporcionan los servicios de segmentación tradicionalmente proporcionados por los routers en las configuraciones LAN. Las VLANs dirigen la escalabilidad, la seguridad y la administración de la red. Considere varios problemas claves cuando diseñe y construya redes LAN comutadas:

- Segmentación de la LAN
- Seguridad
- Control de broadcast
- Rendimiento
- Administración de la red
- Comunicación entre VLANs

Las LANs se pueden utilizar en algunos equipos inalámbricos para separar el tráfico, como lo muestran las Figuras 1 y 2. Esto puede ser útil para separar clientes WEP básicos en una VLAN de los usuarios que no están usando ninguna encriptación. 3 Cuando están correctamente configuradas, las VLANs son seguras. El tráfico de una VLAN no puede atravesar otra VLAN. Los SSIDs pueden utilizarse junto con las VLANs para permitir un acceso limitado a los invitados. Las VLANs pueden ser creadas usando la página de configuración de Servicios VLAN. 4

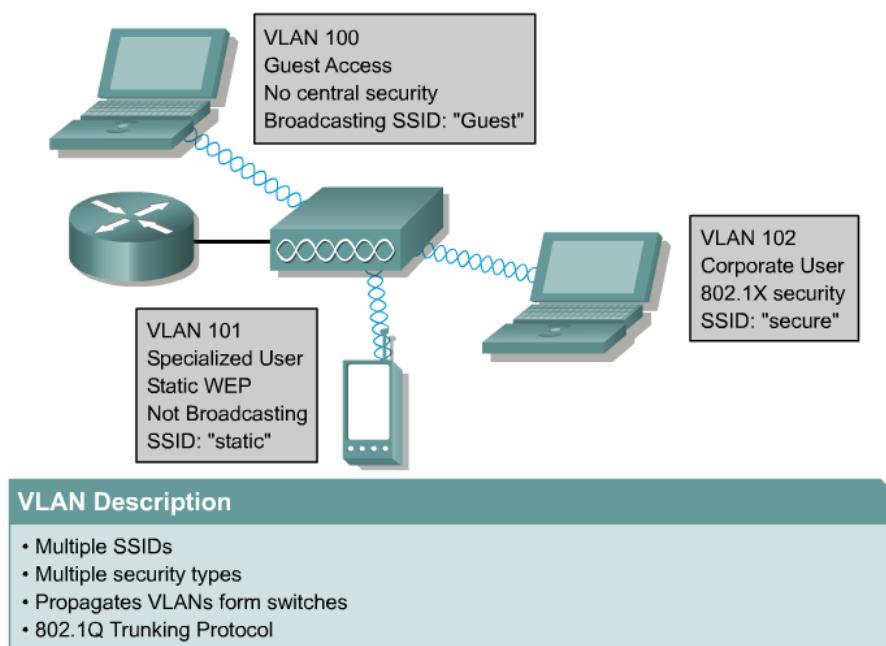


Figura 1

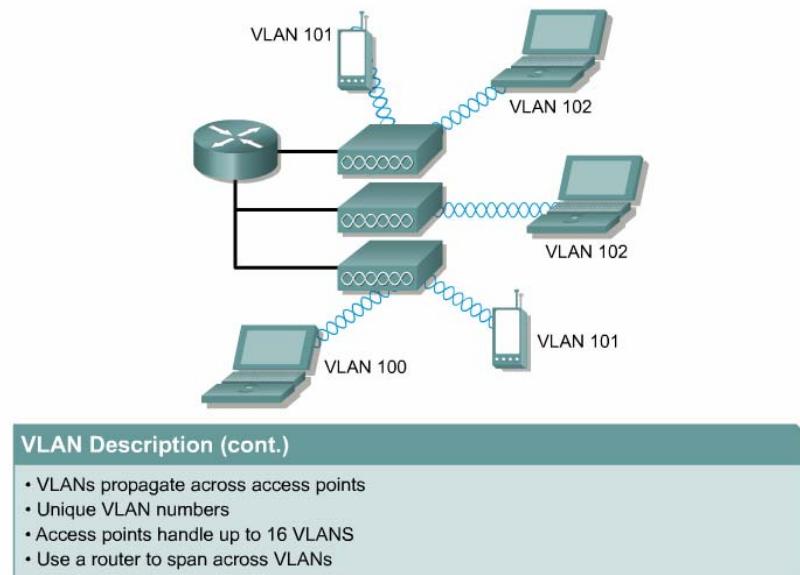


Figura 2

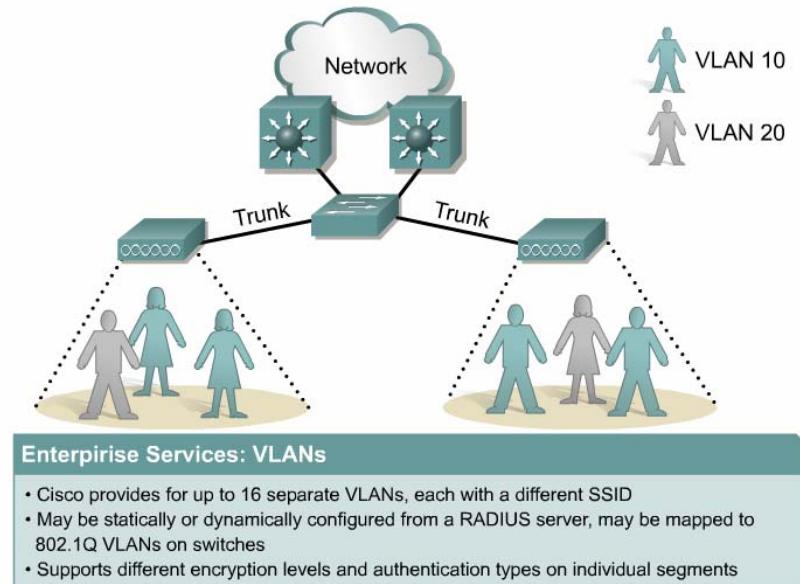


Figura 3

Services: VLAN	
Global VLAN Properties	
Set Default VLAN: <input type="button" value="▼"/>	
Assigned VLANs	
Current VLAN List	Create VLAN
<input type="button" value="Delete"/>	VLAN ID: <input type="text"/> (1-4095)
	SSID: <NONE> <input type="button" value="▼"/> <input type="button" value="Add"/> Define SSID
VLAN Information	
View Information for: <input type="button" value="▼"/>	

Figura 4

8.6.2 Spanning tree

El Spanning tree es sólo necesario cuando se utilizan bridges inalámbricos. Debería permanecer desactivado para los access points y los repetidores, a menos que existan circunstancias especiales en la red. El algoritmo de Spanning Tree se utiliza para evitar bucles de bridging. El algoritmo computa las rutas de red disponibles y cierra las rutas redundantes, para que sólo haya una ruta entre cualquier par de LANs en la red.

Una configuración de spanning tree incorrecta puede desactivar conexiones necesarias. Desde una perspectiva de seguridad, un atacante podría desactivar puertos en una red configurada pobremente. Por favor revise y comprenda la información de spanning tree cuando tome decisiones de configuración.

Resumen

En foco principal de este módulo fue la seguridad de WLAN. Para asegurar una WLAN, son necesarias la encriptación y la autenticación. El corregir simplemente los problemas descubiertos en WEP no es suficiente. Las redes inalámbricas deben autenticar tanto los usuarios como los dispositivos. 802.1x y TKIP proporcionan los mecanismos de seguridad necesarios para proteger las WLANs. Las VPNs fueron tratadas como otra forma de asegurar las WLANs con éxito.

A través del uso de actividades prácticas de laboratorio y de actividades de demostración, los alumnos comprenden mejor los ataques inalámbricos y las contramedidas. Los alumnos obtienen experiencia en la configuración de claves WEP, activación de filtros MAC y activación del LEAP en un AP.

Módulo 9: Aplicaciones, diseño y prep. del estudio del sitio

Descripción General

Este módulo proveerá el background y el conocimiento necesarios para realizar un estudio del sitio. Un buen estudio del sitio ayudará a determinar la factibilidad de la cobertura deseada, la interferencia de la frecuencia de radio y las limitaciones de conectividad cableada. Al preparar un estudio del sitio, el ingeniero tiene múltiples factores que considerar. Algunos de ellos son las aplicaciones y la infraestructura que una institución desea implementar. Una instalación de asistencia médica tiene diferentes necesidades que un comercio minorista, y un comercio minorista tiene diferentes necesidades que un depósito. El ingeniero del sitio debe tener muy presente la forma en que un sitio desea implementar la WLAN.

Después de hablar sobre la forma en que un ingeniero del sitio debe prepararse para un estudio del sitio, el módulo trata los cuatro requisitos principales de diseño para cualquier solución de WLAN:

1. Disponibilidad
2. Escalabilidad
3. Administrabilidad
4. Interoperabilidad

Después de dar una consideración cuidadosa respecto a las necesidades de la institución que desea implementar una WLAN, el ingeniero del sitio debe llegar preparado con el equipo apropiado. Un ingeniero del sitio debería tener múltiples access points listos para probar. Además, el ingeniero del sitio debería llevar consigo los dispositivos de prueba apropiados para asegurarse de que el plan sea factible.

Luego, el módulo introducirá los diferentes utilitarios de documentación que están disponibles para el ingeniero del sitio. Como con cualquier tipo de diseño de LAN o WLAN, la documentación es de vital importancia.

Finalmente, el alumno participará en actividades prácticas de laboratorio que cubren el diseño de la WLAN, utilitarios de cálculo y medidores del estado del enlace.

9.1 Estudio del Sitio

9.1.1 Descripción General

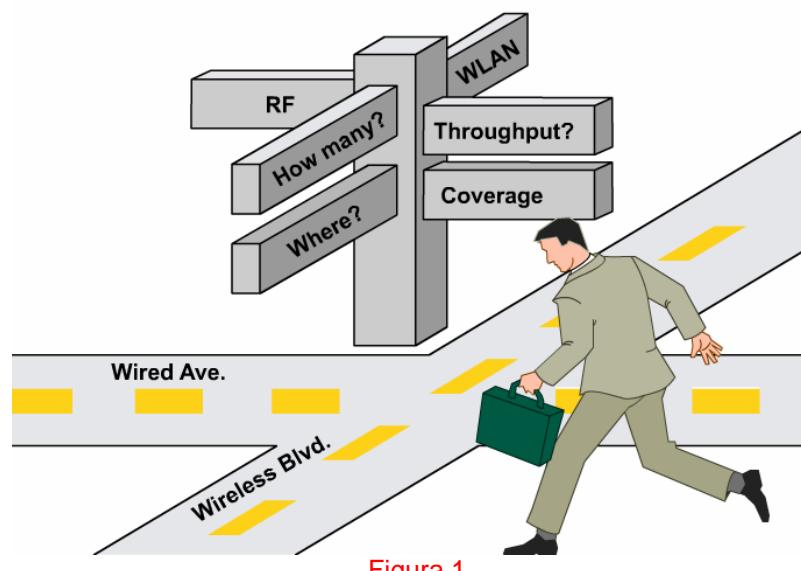


Figura 1

Un estudio del sitio es importante. Antes de instalar los access points de la WLAN, la Figura 1 ilustra algunas cosas que deberían ser investigadas acerca de las instalaciones del cliente. Un buen estudio del sitio ayudará a determinar lo siguiente:

- Factibilidad de la cobertura deseada.
- Interferencia de la frecuencia de radio
- Limitaciones de la conectividad cableada

Un estudio del sitio permitirá que el cliente instale correctamente la WLAN y que tenga un acceso inalámbrico consistente y confiable. Un ingeniero de estudio del sitio de WLAN debería conocer el equipo inalámbrico y cableado.

Un estudio del sitio ayudará al cliente a determinar cuántos APs serán necesarios en todas las instalaciones para proporcionar la cobertura deseada. También determinará la ubicación de esos APs y detallará la información necesaria para la instalación. Un estudio del sitio también determinará la factibilidad de la cobertura deseada ante obstáculos como limitaciones de la conectividad cableada, peligros de la radio y requisitos de las aplicaciones. Esto permitirá que la WLAN sea instalada correctamente y que el cliente tenga un acceso inalámbrico consistente y confiable.

El proceso de realizar estudio del sitio incluye los siguientes pasos:

1. Reunir las herramientas y la configuración
2. Estudiar e investigar las inquietudes específicas de la industria
3. Realizar una lista de los equipos recomendados, o la caja de herramientas del estudio del sitio
4. Implementar el estudio del sitio
5. Documentar el estudio del sitio

9.1.2 Consideraciones del estudio del sitio

A causa de las diferencias en la configuración de los componentes, la ubicación y el entorno físico, cada aplicación de infraestructura es una instalación única. Antes de instalar el sistema se debería realizar un estudio del sitio para determinar la utilización óptima de los componentes de networking y para maximizar el alcance, la cobertura y el rendimiento de la infraestructura. La Figura 1 muestra algunas condiciones operativas y ambientales que se necesitan considerar:

- Data Rates
- Antenna Type and Placement
- Physical Environments
- Obstructions
- Building Materials
- Line of Sight

Figura 1

- Velocidad de Datos - La sensibilidad y el alcance son inversamente proporcionales a la velocidad de los bits de datos. El alcance máximo de la radio se consigue a la velocidad de datos más baja viable. Habrá una disminución en el umbral de recepción a medida que la velocidad de datos de la radio aumenta.
- Tipo y Ubicación de la Antena - La configuración correcta de la antena es un factor crítico en la maximización del alcance de la radio. Como una guía general, el alcance aumenta en proporción a la altura de la antena.
- Entornos Físicos - Las áreas limpias o despejadas proporcionan un alcance de radio mejor que las áreas cerradas o llenas.
- Obstrucciones - Una obstrucción física como una estantería o un pilar puede dificultar el rendimiento del bridge. Evite colocar el dispositivo de computación y la antena en una ubicación donde haya una barrera entre las antenas emisora y receptora.
- Materiales de Construcción - La penetración de la radio es influenciada enormemente por el material de construcción usado en la construcción. Por ejemplo, la construcción de mampostería permite un alcance mayor que los bloques de concreto.
- Línea de Visión - Se debe mantener una línea de visión despejada entre las antenas del bridge inalámbrico. Cualquier obstrucción puede dificultar el rendimiento o prohibir la capacidad del bridge inalámbrico para transmitir y recibir datos. Las antenas direccionales deberían colocarse en ambos extremos a la altura apropiada con un espacio libre máximo para la ruta.

9.1.3 Estándares y topologías

Un diseñador de WLANs debe conocer los diferentes estándares 802.11. Un diseñador también debe conocer las limitaciones del 802.11 mientras diseña una WLAN. Como el estándar no cubre la comunicación entre APs a través del backbone cableado, se recomienda que el backbone de WLAN conste de un único

producto de un fabricante. Muchas aplicaciones requieren características no definidas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) como roaming, balance de carga y repetidores inalámbricos.

Al igual que con las redes cableadas, la topología de las WLANs pueden tomar muchas formas. **1** Pero con respecto a una WLAN, el término ‘topología’ no hace referencia a las arquitecturas como bus o anillo. En realidad hace referencia al Área de Servicio Básico [Basic Service Area (BSA)], que está compuesta por microcélulas. Cada AP tiene un área de cobertura llamada microcélula o célula. En una instalación que consiste en un único AP este es un concepto muy simple. Cuando están instalados múltiples APs, las células deben superponerse para que la conexión inalámbrica nunca se interrumpa mientras se hace roaming de AP en AP. El propósito principal de un estudio del sitio es localizar la ubicación apropiada para los APs de la conexión inalámbrica para el cliente.

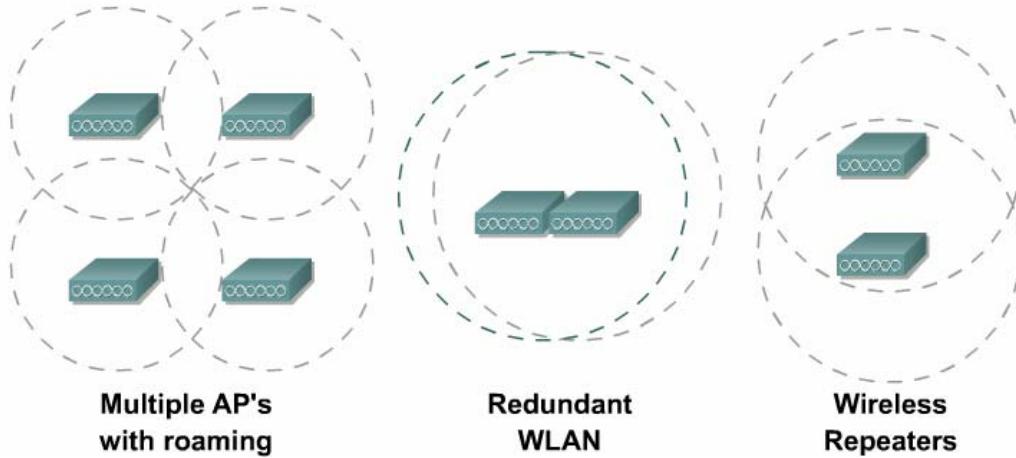
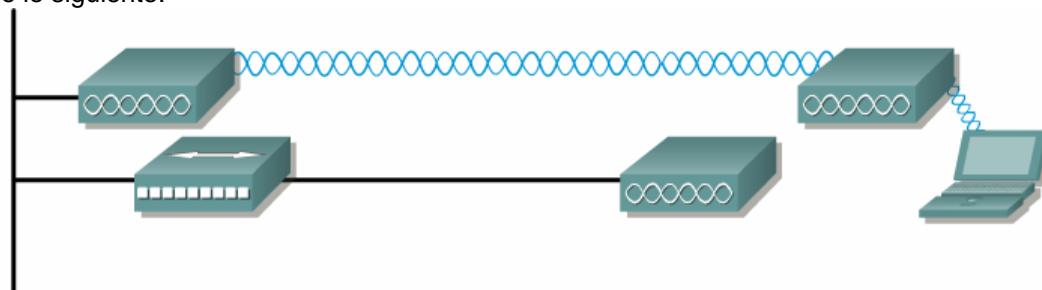


Figura 1

A veces la topología de la WLAN será dictada por el formato de la LAN cableada a la que está conectada la WLAN. **2** Si la conectividad cableada sólo está disponible a lo largo de un lado de un depósito de 9.290 m cuadrados (100.000 pies cuadrados), por ejemplo, las limitaciones de distancia de un cable Cat 5 de 100 m (328 pies) de largo pueden no ser suficientes para llegar a la ubicación recomendada para el AP. Aquí es donde el ingeniero para el estudio del sitio tendrá que ser creativo. Hay muchas soluciones posibles, incluyendo lo siguiente:



Sometimes the limitations of the wired network may decide how you design your WLAN

- Knowledge of wired LANs allows you to be creative in your WLAN design. This means a superior design for your customer
- Know your wired and wireless alternatives

Figura 2

- Un salto inalámbrico que use un repetidor para responder a un AP cableado
- Un repetidor o un hub para extender el alcance del cable Cat 5
- Instalar un enlace de fibra para proporcionar conectividad del otro lado del depósito

Un ingeniero de estudio del sitio es responsable no sólo de encontrar las mejores ubicaciones para los APs, sino también de encontrar formas para conectar los APs a la red cableada. Por lo tanto, es crucial que el

ingeniero conozca las redes cableadas. Este conocimiento debería cubrir las topologías, estándares y componentes de las LANs cableadas.

9.1.4 Consideraciones importantes

Es importante que un ingeniero de estudio del sitio realice lo siguiente:

- Esté preparado para responder preguntas
- Se vista en forma apropiada
- Infunda un sentido de confianza en el cliente
- Use credenciales de la compañía
- Tenga tarjetas profesionales disponibles
- Lleve el equipo apropiado

Asegúrese de presentarse ante el personal apropiado al ingresar a cualquier organización. Muchas compañías tienen sus propios guardias de seguridad uniformados que necesitan estar informados acerca de cualquier visitante. Las escuelas normalmente requieren que un visitante se presente en la oficina principal antes de acceder a otras áreas del campus. En áreas de alta seguridad como emplazamientos del gobierno, la aviación y militares, es extremadamente importante obtener una autorización de seguridad y ser escoltado si fuera necesario.

Un ingeniero de estudio del sitio debería seguir las pautas de seguridad mostradas en la Figura 1 para asegurar el funcionamiento apropiado y el uso seguro de los dispositivos inalámbricos.

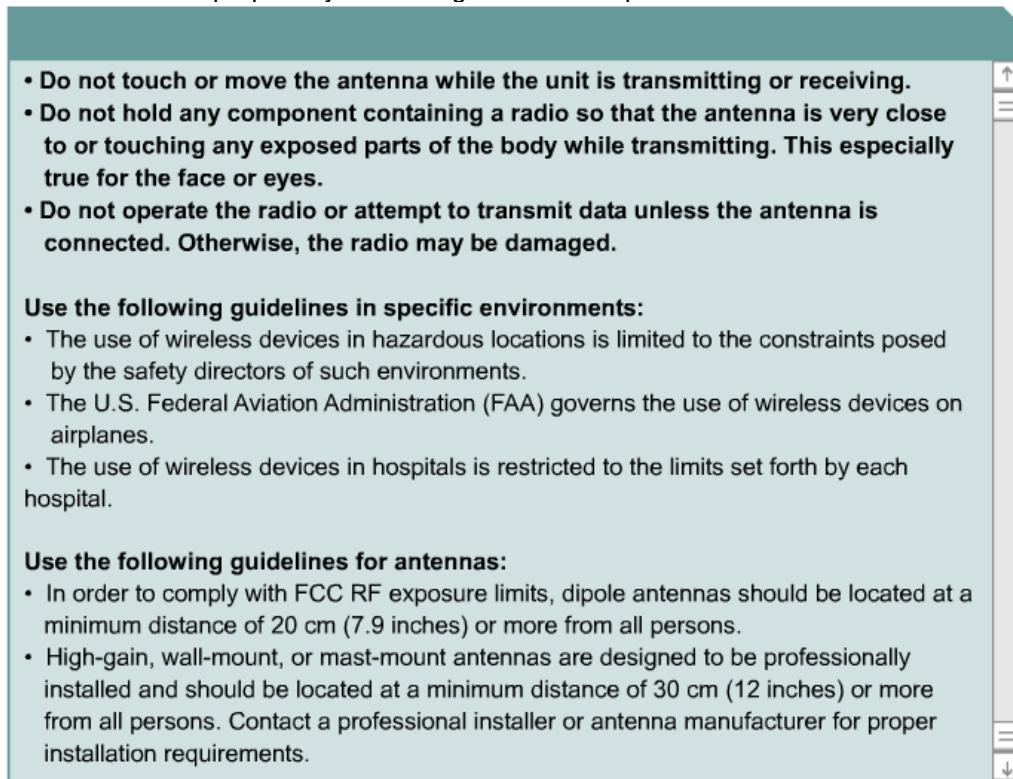


Figura 1

9.2 Aplicaciones

9.2.1 Cambio de tecnología y de aplicaciones

Los primeros en adoptar la tecnología inalámbrica estaban en mercados verticales. Estos usuarios estaban más preocupados por la movilidad que por los estándares o el throughput. Los usuarios hoy se están moviendo más hacia los mercados horizontales donde la movilidad puede ser menos preocupante que la interoperabilidad y el throughput. Con los productos WLAN 802.11a y 802.11b, la movilidad y el roaming no tienen que ser sacrificados para ganar throughput e interoperabilidad. Sin embargo, el elegir la tecnología WLAN correcta es muy importante y depende de la aplicación y de la infraestructura 1.

	2.4 GHz/802.11b Uses	5 GHz/802.11a Uses
Hospitality	X	
Manufacturing	X	
Healthcare	X	X
Higher Education	X	X
Enterprise Office	X	X
Financial Institutions	X	
Retail	X	
Transportation	X	
Warehouse	X	

Figura 1

Las aplicaciones principales para el networking inalámbrico son las siguientes:

- La primera es el uso en la pequeña oficina, oficina hogareña (SOHO). Por lo general, dentro de esta aplicación, múltiples PCs se comunican por medio del AP o directamente tarjeta a tarjeta sin el uso de un hub.
- Segundo, los trabajadores móviles dentro de una empresa normalmente no tienen un escritorio fijo dentro de su oficina corporativa. Los trabajadores móviles también podrían necesitar conectividad dentro de un entorno de espacio abierto como una sala de conferencias. Los trabajadores móviles por lo general están en ocupaciones como la educación, la venta minorista, mayorista y la asistencia médica.
- Finalmente, la conectividad exterior puede ser la conexión de dos o más edificios para formar conexiones sitio a sitio que unan todas sus redes. También podrían ser trabajadores móviles que necesiten acceso a su red corporativa desde el exterior de sus edificios, como desde un estacionamiento.

La infraestructura consiste en una variedad de hardware. En algunos casos se necesitan múltiples productos para completar la infraestructura total. Los distintos componentes incluyen a los siguientes: [2](#)

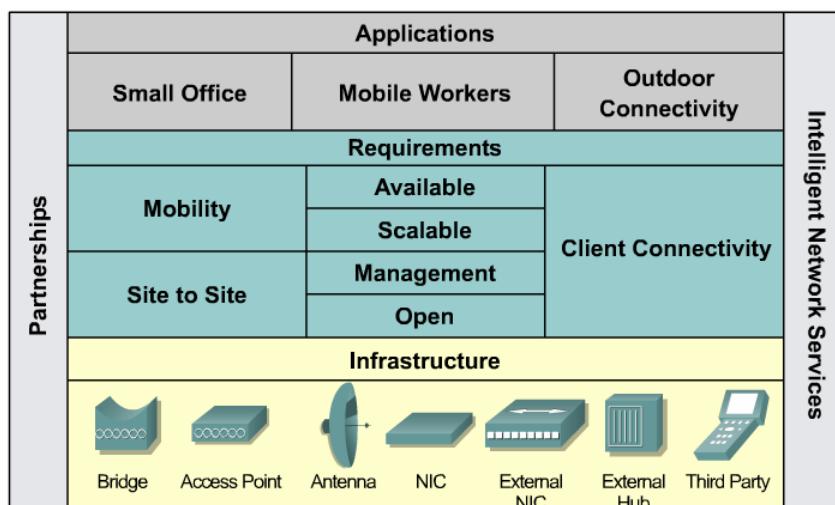


Figura 2

- Bridges: Usados para conectar LANs entre sí en una aplicación sitio a sitio
- AP: Sirve como un punto de conexión entre una red cableada y una inalámbrica
- Antena: Transmite señales entre el cliente inalámbrico y el bridge o AP
- Tarjeta de Interfaz de Red (NIC): Reside con el cliente y proporciona un punto de conexión con el AP
- NIC Externa: Proporciona una conexión Ethernet con un transmisor inalámbrico para un dispositivo que ya tiene una NIC Ethernet instalada
- Hub Externo: Proporciona múltiples conexiones Ethernet en la forma de un hub con un transmisor inalámbrico para dispositivos que ya tienen NICs Ethernet instaladas.
- Terceros: Dispositivos como lectores de código de barras, teléfonos y asistentes personales digitales (PDAs), que se pueden conectar a la infraestructura inalámbrica 802.11.

9.3 Diseño de WLAN

9.3.1 Descripción general

Los cuatro requisitos principales del diseño para una solución WLAN son los siguientes:

1. Una alta disponibilidad se consigue a través de la redundancia del sistema y del diseño apropiado de un área de cobertura. La redundancia del sistema incluye APs redundantes en frecuencias separadas. El diseño apropiado del área de cobertura incluye cálculos para el roaming, negociación automática de la velocidad cuando la fuerza de la señal se debilita, selección de la antena apropiada y posiblemente el uso de un repetidor para extender la cobertura hacia áreas donde no se puede usar un AP.
2. La escalabilidad se consigue soportando múltiples APs por área de cobertura que utilizan múltiples frecuencias o patrones de salto. Los APs también pueden realizar balance de carga si fuera necesario.
3. Las herramientas de diagnóstico representan a una gran parte de la administración dentro de las WLANs.
4. La interoperabilidad se consigue a través de la adhesión a estándares como 802.11a, b y g, de la participación en asociaciones de interoperabilidad como la Alianza de Compatibilidad Ethernet Inalámbrica [Wireless Ethernet Compatibility Alliance (WECA)], y de certificaciones tales como la de FCC.

Los factores en el diseño apropiado de WLAN serán tratados aquí y en las secciones siguientes..

Un factor adicional que afecta el diseño de las WLANs es el tipo particular de cliente que el usuario estará usando. Algunos usuarios pueden optar por usar tarjetas de la Asociación Internacional de Fabricantes de Tarjetas de Memoria de Computadora Personal [Personal Computer Memory Card International Association (PCMCIA)] en laptops para proporcionar movilidad a su personal interno y conectividad sencilla a los usuarios remotos cuando están en las instalaciones. Algunos pueden desear utilizar tarjetas de interfaz de componente periférico [peripheral component interface (PCI)], que les da a los usuarios la libertad para mover ocasionalmente las computadoras personales (PCs) de escritorio sin tener que preocuparse por el cable de la instalación. Algunos pueden usar un repetidor o un bridge de grupo de trabajo para proporcionar conectividad a usuarios remotos sin usar líneas arrendadas estándares o sin tener que preocuparse por intentar instalar fibra. Otros pueden querer usar terminales de recolección de datos. Algunos usuarios pueden usar una combinación de estas opciones.

En un entorno donde las PCs permanecerán estacionarias la mayor parte del tiempo, el proveer conectividad inalámbrica es una tarea bastante fácil. Para las instalaciones de este tipo, los usuarios normalmente necesitan células de 54 Mbps u 11 Mbps de cobertura y no estarán demasiado preocupados por la velocidad de su enlace mientras se están moviendo. Muchos usuarios no comprenden en su totalidad al equipo que será instalado ni saben qué esperar. Algunos cuestionarán la confiabilidad del enlace de radiofrecuencia (RF) e intentarán usar el enlace inalámbrico en forma limitada.

Recuerde que el throughput real es menor que el throughput teórico. Hay muchos factores que limitan la velocidad del enlace, incluyendo la sobrecarga, el sistema operativo y la cantidad de usuarios. Hay más sobrecarga asociada con el enlace RF que la que hay con el enlace cableado. Para ser realistas, la velocidad máxima del enlace para 802.11b será cercana a los 7 Mbps. Las velocidades de transferencia de archivos varían según los diferentes sistemas operativos. Las velocidades para un sistema operativo de Microsoft son de alrededor de 5.5 Mbps. Las velocidades de Linux están cercanas a los 7 Mbps. El enlace inalámbrico de 11 Mbps puede ser considerado como un segmento Ethernet cableado de 10 Mbps cuando se decide cuántos usuarios lo pueden manipular.

9.3.2 Aplicaciones y recolección de datos

Tenga presente las aplicaciones que los usuarios puedan estar utilizando . Un usuario que realiza la transferencia ocasional de archivos y revisa los e-mails tiene necesidades muy diferentes de las de alguien que utiliza una aplicación de diseño asistido por computadora (CAD) a través de la red. La mayoría de las oficinas de hoy utilizan un modelo cliente/servidor donde las aplicaciones usadas frecuentemente están cargadas en cada terminal. Algunas compañías se están pasando a clientes ligeros y pueden tener necesidades de ancho de banda mucho mayores. Este tipo de configuración requiere una conexión confiable con la red, ya que una interrupción del servicio de red deja a los usuarios desamparados.

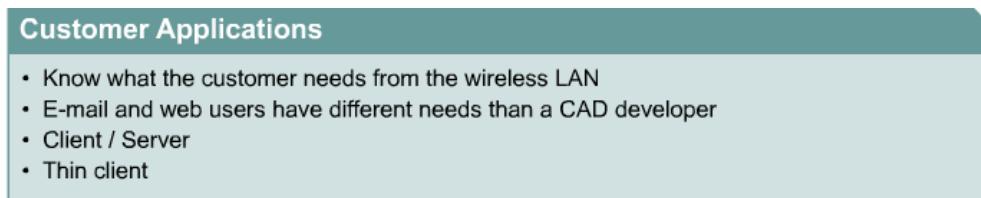


Figura 1

Si el usuario intenta usar dispositivos de recolección de datos exclusivamente, esto cambiará la forma en que se realiza el estudio del sitio²¹. La mayoría de los dispositivos de recolección de datos de hoy trabajan a 2 Mbps y no necesitan 11 Mbps. Si el usuario está usando un dispositivo de recolección de datos de 2 Mbps sin intenciones de agregar otros clientes inalámbricos que puedan trabajar a 11 Mbps, entonces realice el estudio del sitio a 2 Mbps.



Figura 2

Asegúrese de que todas las áreas donde se utilizarán los dispositivos de recolección de datos tengan un enlace de 2 Mbps. Algunos dispositivos de recolección de datos tienen la capacidad de cambiar de velocidad. Hable con los usuarios acerca de los dispositivos que estarán usando, qué capacidades tendrán estos dispositivos, y cómo intentarán usarlos.

Como se dijo antes, los sitios de venta mayorista o minorista pueden tener áreas donde se ubicarán grandes cantidades de usuarios. Un área de recepción puede ser este tipo de área. A medida que la mercadería es descargada de los camiones, se saca de las cajas y se leen los códigos de barras en rápida sucesión. Las necesidades de ancho de banda van a ser determinadas por la aplicación. Por ejemplo, una emulación de adaptación de pantallas envía grandes paquetes conteniendo muchos datos. Si hay 20 a 30 usuarios leyendo códigos de barras y pulsando teclas en rápida sucesión, un único AP puede no ser suficiente.

Por ejemplo, si todos los dispositivos de recolección de datos están funcionando a 11 Mbps, el AP sólo está funcionando a 2 Mbps. Esto no significa que el AP está limitado a 2 Mbps, sino que todos los clientes se están comunicando con el AP a 2 Mbps. Mientras que una conexión de 55 Mbps u 11 Mbps puede ser suficiente para manejar 20 o 30 usuarios, la conexión de 2 Mbps puede no serlo. El tamaño de paquete de la aplicación y la cantidad de usuarios deben ser considerados para determinar si se necesitan APs extras en esta área.

Cobre versus WLAN

Las instalaciones de cobre aun pueden proporcionar altas velocidades de datos, pero el precio ya no es un factor. Una WLAN puede ser instalada por casi el mismo precio que una red basada en cobre, y proporciona muchos beneficios más que una red cableada. A medida que los precios continúen bajando en los productos inalámbricos y las velocidades de throughput continúen aumentando, la popularidad de la tecnología inalámbrica continuará creciendo. Esto también puede ser un factor en el diseño. Si el usuario desea comenzar usando unos pocos clientes inalámbricos y luego aumentar la cantidad después de asegurarse de la confiabilidad, la WLAN deberá estar diseñada para recibir una expansión futura.

9.3.3 Carga y cobertura

Habrá rangos de cobertura en cada velocidad de datos. Si el usuario desea proporcionar cobertura a una cierta área con una velocidad de datos específica, pueden ser necesarios múltiples estudios del sitio. Cada velocidad de datos debe ser estudiada para averiguar dónde está el rango de cobertura de cada una.

Para determinar dónde colocar los APs, es importante averiguar cuánto throughput necesitarán los usuarios. Los requisitos de ancho de banda para la conectividad inalámbrica determinarán potencialmente la cantidad de APs que se necesita utilizar. Si se requiere una velocidad constante y esa velocidad es bastante alta, como 11 Mbps, entonces la cobertura será bastante baja y se necesitará una gran cantidad de APs.

En muchas situaciones, la cobertura de un AP será el factor conductor por sobre el ancho de banda y se podrá usar una negociación automática de ancho de banda. Con la negociación automática, el cliente elige la mejor velocidad según su distancia actual, así mientras el cliente se mueve desde una proximidad cercana al AP, utiliza un ancho de banda alto como 11 Mbps. Mientras el cliente se aleja del AP y la distancia aumenta, el ancho de banda es reducido para permitir la mejor calidad de señal posible.

La carga en un access point o la cantidad total de clientes potenciales debería ser considerada en cualquier diseño. Un problema con las WLANs es que la cantidad de clientes potenciales puede ser desconocida, ya que la libertad de la tecnología inalámbrica permite que cualquier cantidad de personas converjan dentro de un área. La cantidad máxima de clientes como lo dicta la tabla de direccionamiento en el access point es 2.048. Este máximo no es práctico, porque las WLANs son una infraestructura compartida, lo cual es similar a los hubs en una red cableada.

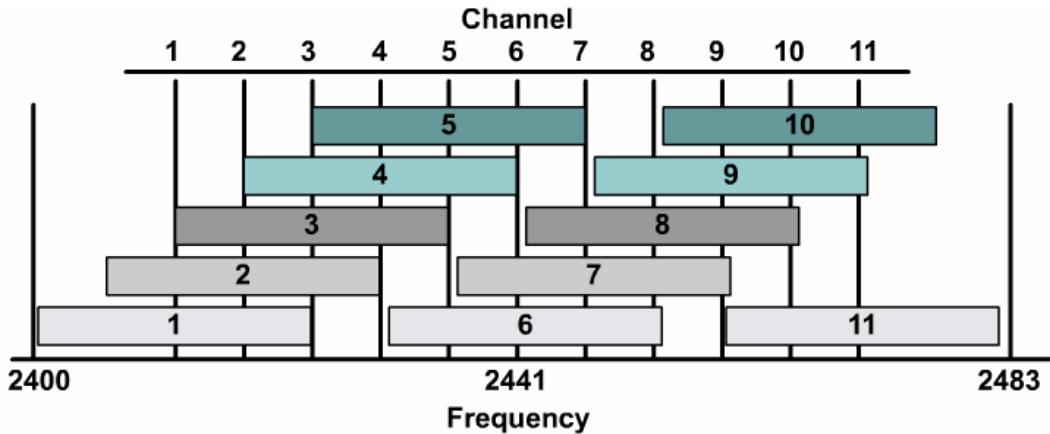


Figura 1

Cada usuario individual tiene menos ancho de banda general disponible a medida que más clientes se suman al AP. Esto puede ser aceptable para aplicaciones de ancho de banda variable. Sin embargo, para muchas aplicaciones, en especial con entornos gráficos modernos intensivos en datos, esto puede no ser adecuado. La distribución de los clientes entre más access points, particularmente en áreas congestionadas, resuelve con facilidad este problema. Esto sirve para distribuir la carga, por medio de la cobertura superpuesta entre APs. Asegúrese de que cada AP se esté comunicando sobre su propio canal único para evitar la interferencia entre ellos. Si sólo dos APs van a tener una cobertura superpuesta, entonces se puede utilizar dos canales diferentes cualesquiera de entre uno y 11. La cantidad máxima de APs que se puede utilizar en forma simultánea es tres. Esto es porque sólo tres canales no se superponen entre sí, que son los canales uno, seis y 11 como se muestra en la Figura 1.

En algunos entornos, el ancho de banda y la carga del AP son factores de diseño fuertes para la implementación de WLANs. Una forma de asegurarse de que un área pequeña de usuarios está usando un AP seleccionado es manipular las configuraciones de potencia en el AP para ajustar el tamaño de la célula. Este ajuste creará células que cubren áreas específicas.

9.3.4 Ancho de banda y throughput

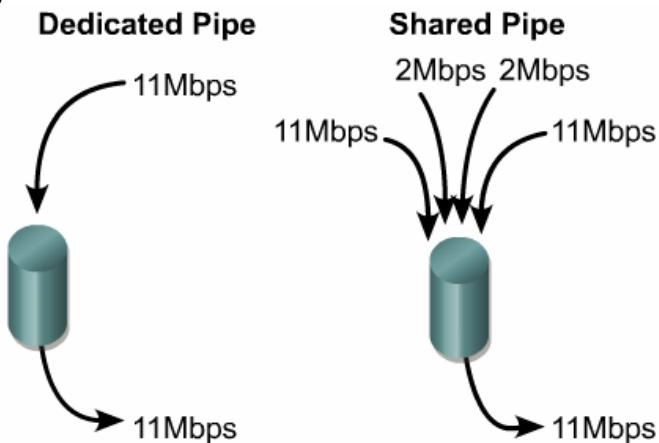
Mucha gente piensa que un producto con una velocidad de datos en conjunto de 11 Mbps puede soportar completamente muchas radios de 2 Mbps a su velocidad de datos total. El problema es que las unidades de 2 Mbps transmiten a 2 Mbps, lo que lleva cinco veces más tiempo el transmitir los mismos datos que un producto de 11 Mbps. Esto significa que la velocidad de datos es sólo 2 Mbps para cualquier remoto dado, y el total que podría ver la unidad de 11 Mb es 2 Mbps.

Para lograr una velocidad de datos de 11 Mbps en total, todos los dispositivos tendrán que estar fijados en 11 Mbps. Este es también el caso con 802.11a y g trabajando a 54 Mbps. Si una única unidad es menor que

el máximo, la velocidad general será un poco menor que la máxima. Esto es porque la unidad base o central tiene que servir a la unidad remota más lenta.

Recuerde lo siguiente:

- Si todos los dispositivos trabajan a la misma velocidad de datos, a todos les llevará la misma cantidad de tiempo enviar paquetes del mismo tamaño.
- Si algunos dispositivos están funcionando a velocidades mayores, entonces el paquete se transferirá más rápido. Esto permitirá que la RF esté disponible más rápidamente para el siguiente dispositivo que espera enviar datos.
- Si se intenta reducir el throughput hacia un sitio dado bajando la velocidad del bridge, esto también afectará a los bridges de alta velocidad.



- If Data rate=11 -Mbps why do I only see 5.5 -Mbps of data?
- Through = data+overhead
- 10Mbps Ethernet has approximately 6 or 7 -Mbps of throughput

Figura 1

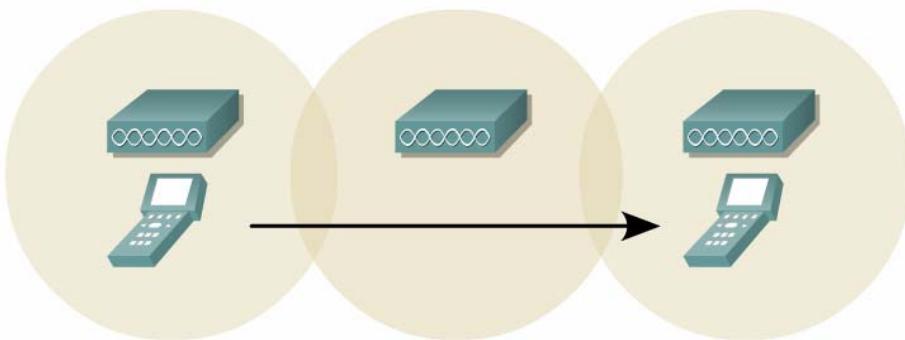
La cantidad de datos del usuario que pasa por el medio es el throughput . Cuando se compara el throughput verdadero con la capacidad de un caño, la velocidad de datos es la cantidad de datos que puede pasar por el medio. Esto incluye paquetes con sobrecarga como ACKs, paquetes de asociación y reintentos. El throughput normalmente es el 50 o 60 por ciento de la velocidad de datos para un sistema inalámbrico.

Cuando se compara a los caños dedicados con un caño compartido, una configuración de bridge punto a punto es un ejemplo de un caño dedicado. Si el enlace RF está fijado en 11 Mbps, entonces el throughput de datos entre esos sitios es 11 Mbps. Un caño compartido consiste en una red de RF punto a multipunto. Si el enlace RF está fijado en 11 Mbps, todos los sitios remotos comparten ese caño de 11 Mbps. Esta forma de compartir puede ser comparada con la de un segmento Ethernet. Cuando hay múltiples dispositivos Ethernet en un segmento cableado, ellos comparten el caño donde residen. Cuantos más dispositivos se agreguen al caño, más lento será el throughput general.

9.3.5 Usuarios móviles

Usuarios Móviles

Los usuarios de recolección de datos también son usuarios altamente móviles . Esa es la ventaja del dispositivo de recolección de datos inalámbrico. Permite que el usuario final se traslade libremente por todas las instalaciones y lea los ítems en lugar de tener que llevarlos hasta un lector que esté conectado a una terminal fija. La cobertura no debe tener orificios y debe tener suficiente superposición entre APs para ofrecer un roaming verdaderamente transparente.



- Wireless data collection means mobility!
- Coverage must be seamless

Figura 1

Usuarios Altamente Móviles

Algunos dispositivos de recolección de datos están montados en horquillas elevadoras, que se pueden mover por todas las instalaciones muy rápidamente. Un chofer puede leer un código de barra y luego ingresar la cantidad mientras está conduciendo. Tenga en cuenta que el chofer de la horquilla elevadora no conoce la tecnología y normalmente tampoco desea hacerlo. El chofer simplemente desea un sistema que funcione. Al proveer una cobertura con las menores fisuras posibles, un diseñador de WLAN se asegurará que la aplicación tenga la menor cantidad de problemas posible y que funcione con éxito.

Cuando se realiza un roaming sin fisuras [2](#), se debería evitar el uso de IP móvil, y es necesaria una subred IP constante para el cliente. Sin embargo, es posible extender la cobertura para un cliente sin implementar un AP conectado al mismo dominio de broadcast. Se puede hacer esto usando un segundo AP en modo repetidor. Esta configuración puede extender la cobertura del primer AP si no hay un cableado disponible para el segundo AP. Cuando los APs son implementados como repetidores, la asociación del cliente se hace realmente con el AP cableado o el raíz. La asociación del cliente no se hace con el AP que actúa como un repetidor. Dentro de los edificios, las conexiones Ethernet por lo general están fácilmente disponibles. Sin embargo, un uso de la configuración de repetidor es extender los APs desde el límite del edificio hacia las partes externas de los alrededores del edificio para un uso temporal. Por ejemplo, un usuario puede usar los APs en modo repetidor para extender la cobertura dentro del estacionamiento durante las ventas de primavera de un comercio.



Seamless Roaming

- All AP's on same Subnet
- Use VLAN Tagging to span switches
- LAN Emulation (LANE), InterSwitch Link (ISL), IEEE 802.1q (802.1Q is a major spec so upper case/802.1p is an addendum to 802.1D therefore lower case)
- Repeater Mode
- AP used to extend distance of another AP
- Wired AP is the associated connection point

Figura 2

9.3.6 Consumo de energía

Como la energía de la batería es limitada, el consumo de energía al usar una tarjeta PCMCIA mientras se hace roaming siempre va a ser un problema. Hay tres modos de energía disponibles y que se pueden seleccionar para las laptops de los usuarios [1](#). La configuración de estos diferentes modos de energía se realiza usando Administrador de Perfiles [Profile Manager] > Editar [Edit] para el perfil deseado [2](#).

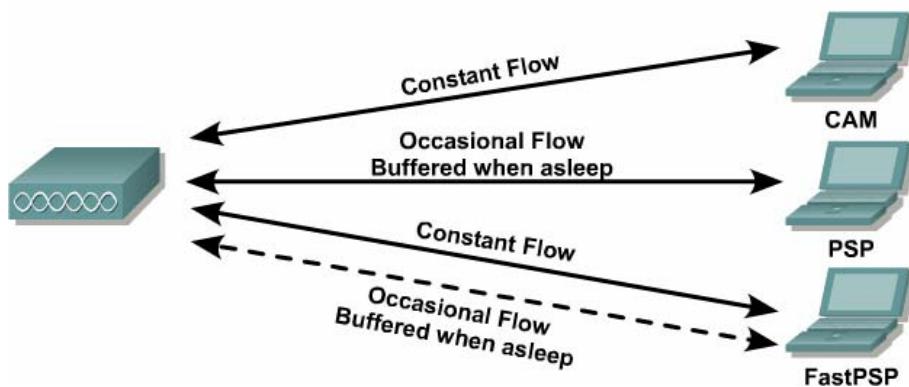


Figura 1

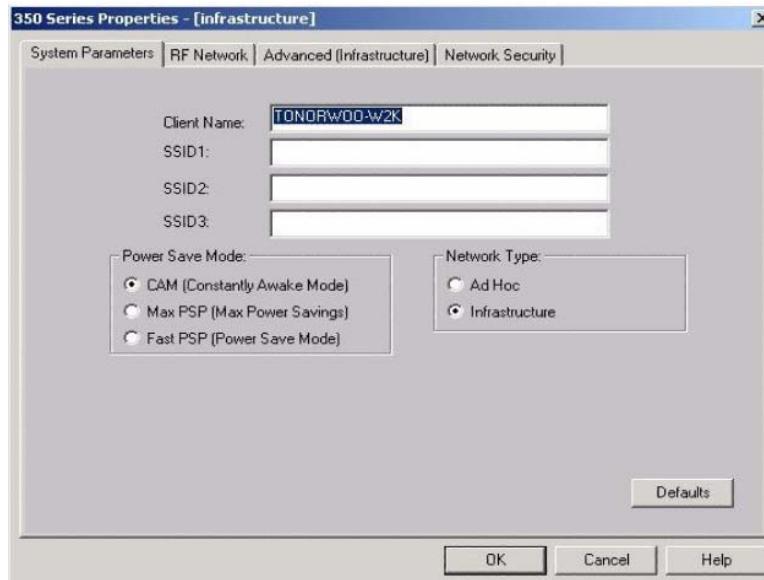


Figura 2

El primer modo es Modo Constantemente Despierto [Constantly Awake Mode (CAM)]. Es el mejor para usar con dispositivos cuando la energía no es un problema, como cuando la energía AC está disponible para el dispositivo. CAM proporciona la mejor opción de conectividad y, por lo tanto, la infraestructura inalámbrica con mayor disponibilidad desde la perspectiva del cliente.

El segundo modo es Ahorro Máximo de Energía [Max Power Savings (Max PSP)]. Debería seleccionarse cuando la conservación de la energía es de máxima importancia. En esta situación, la NIC inalámbrica se dormirá después de un período de inactividad y se despertará periódicamente para recuperar datos almacenados en el AP.

El último modo es el Modo de Ahorro de Energía Rápido [Fast Power Save Mode (Fast PSP)]. Es una combinación de CAM y PSP. Esto es bueno para los clientes que pasan de energía AC a DC y viceversa.

9.3.7 Interferencia

Las WLANs utilizan un espectro sin licencia, que permite a los usuarios administrar sus propios productos e implementaciones. Esto hace a las WLANs escalables además de fáciles de implementar y administrar. La desventaja de usar un espectro sin licencia es que otros dispositivos pueden también usar las mismas frecuencias y, por lo tanto, impactar entre sí. Otros dispositivos que usan 2.4 GHz o 5 GHz, como los teléfonos inalámbricos, pueden tener un impacto sin importar las implementaciones de SSID y WEP. Mientras que SSID y WEP proporcionan seguridad para los datos de la WLAN, la señal de RF misma es aun objeto de interferencia. Esto es porque es una transmisión de Capa 1. La interferencia puede ser evitada en la mayoría de los casos seleccionando productos que funcionan fuera de estos rangos.

El impacto sólo va a suceder si los dispositivos de terceros usan más que una mínima cantidad de RF. Si una persona fuera a encender otro dispositivo de 2.4 GHz, no sucederá mucho y no ocurrirá un verdadero impacto. Pero si ese dispositivo de terceros comienza a usar el espectro de 2.4 GHz, entonces ambos

sistemas sufrirán una degradación del rendimiento. Esto proviene del hecho de que los productos WLAN están basados en Acceso Múltiple con Detección de Portadora y Colisión Evitable (CSMA/CA). Antes de que se envíe una transmisión, el transmisor controla las ondas de radio para ver si el canal está disponible para ser usado. Si un tercero está usando el espectro, entonces las ondas de radio no estarán disponibles. El dispositivo esperará hasta que la RF vuelva a estar disponible. En una red Ethernet cableada, esto sería lo mismo que enviar un frame de broadcast constante por el cable, y tendrá el mismo efecto.

9.3.8 Encriptación



Figura 1

Hay tres tipos de opciones de encriptación disponibles para las WLANs. Las WLANs pueden ser instaladas sin encriptación, con encriptación WEP de 40 bits o con encriptación WEP de 128 bits. Cisco tiene un proceso de encriptación basado en hardware, por lo que sólo tiene un muy pequeño efecto sobre el rendimiento cuando la encriptación está activada en el producto. Otros fabricantes de WLAN tienen encriptación basada en software, lo que significa que disminuye significativamente el throughput de la LAN.

La encriptación WEP se conoce por ser débil. El IEEE está mejorando a WEP con TKIP y proporcionando opciones de autenticación robustas con 802.1X para hacer que las WLANs basadas en 802.11 sean seguras. Al mismo tiempo, el IEEE está investigando mecanismos de encriptación más fuertes. El IEEE ha adoptado el uso del Estándar de Encriptación Avanzado (AES) en la sección de privacidad de datos del estándar 802.11i propuesto.

9.3.9 Código contra incendios y problemas de seguridad

Es importante usar los códigos locales de edificación, incendios y eléctricos cuando se diseñan WLAN. La serie de productos Cisco Aironet no están hechos para el pleno. Los dispositivos hechos para el pleno aseguran que no despedirán gases venenosos. Siempre debe quedarse dentro de las pautas del código cuando diseñe WLANs. Esto eliminará virtualmente la necesidad de rehacer las instalaciones que no cumplan con el código. Especifique el equipo y los suministros apropiados en el planeamiento para evitar costosos excesos del presupuesto.

Recuerde que el costo de reemplazar o arreglar el problema normalmente será responsabilidad del instalador. Cualquier daño o herida personal debido a una WLAN instalada de forma incorrecta también será responsabilidad del instalador. Asegúrese de consultar o tener profesionales con licencia para realizar tareas de instalación como erección de torres, sistemas de puesta a tierra y servicios eléctricos. No baje los estándares cuando diseñe o instale WLANs para ahorrar dinero. Esto podría dar por resultado una mala reputación, pérdida de trabajos o incluso litigios.

Por ejemplo, a un cliente corporativo le gustaría ocultar los APs por encima del cielo raso y proveer el máximo ancho de banda a los usuarios. En este caso, es mejor reducir la potencia de la antena para obtener la mayor cantidad de APs sobre el piso, y usar un cerramiento del pleno de una compañía como LXE para obtener la categoría del pleno.

La Agencia Nacional de Protección contra Incendios (NFPA) desarrolla, publica y difunde códigos y estándares con la intención de minimizar la posibilidad y los efectos del fuego y otros riesgos. Estos están reunidos en el NEC. Todos los edificios, procesos, servicios, diseños e instalaciones están afectados por los documentos de la NFPA. Más de 300 códigos y estándares NFPA son usados alrededor del mundo. Más de 225 Comités Técnicos de la NFPA, cada uno de los cuales representando un balance de intereses afectados, desarrollan documentos NFPA.

9.4 Diseño de Edificio a Edificio

9.4.1 Descripción General

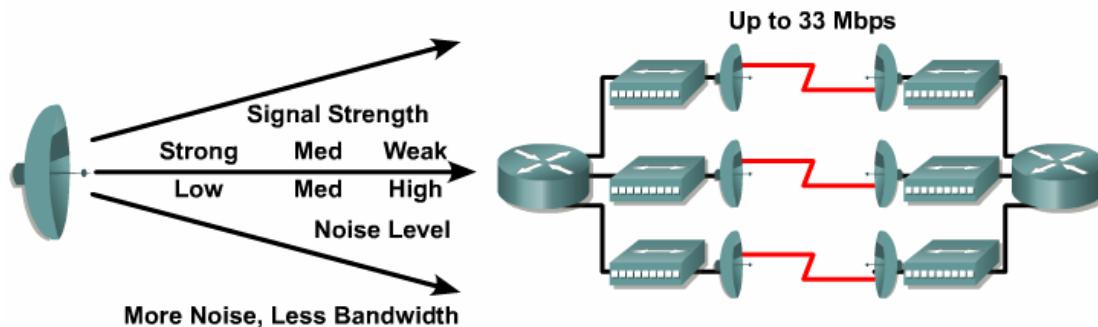
Las WLANs de edificio a edificio presentan algunos desafíos. A medida que la distancia entre los sitios aumenta, se vuelve más difícil crear enlaces de calidad. Además, las antenas deben estar colocadas dependiendo de la distancia entre los sitios. El costo de instalar una torre puede convertirse en el ítem más costoso del proyecto.

Además del problema del costo, las regulaciones locales, estatales o federales pueden presentar obstáculos cuando que erigen torres. Incluso el colocar antenas montadas puede ir en contra de algunas regulaciones de edificación locales. Asegúrese de investigar estos temas y de obtener permisos antes de finalizar el plan del diseño. Incluso un permiso negado puede seriamente poner en peligro un proyecto. Es mejor tratar con esto durante la fase de diseño.

Cuando se consideran los diseños de edificio a edificio, la distancia y el ancho de banda tienen un gran impacto en el diseño general. Las grandes distancias son posibles usando velocidades más bajas. Esto es porque la señal se debilita a medida que se extiende y así lo hace también el nivel de ruido. Los anchos de banda más altos requieren un nivel de ruido menor a causa de las técnicas de compresión y modulación usadas.

A muchas corporaciones les gustaría tener mucho ancho de banda entre las nuevas ubicaciones para una variedad de aplicaciones, incluso aunque el estándar 802.11 esté limitado a 11 Mbps. Para las WLANs, es posible usar un canal fast ether o un troncal multienlace para vincular o sumar tres bridges juntos y dar al usuario un potencial de 33 Mbps ¹.

Una opción para dar mayor ancho de banda es usar 802.11a o 802.11g. Una solución de bridging 802.11a proporcionará hasta 54 Mbps en cada enlace. Sin embargo, 802.11a no puede alcanzar las distancias que logra 802.11b. 802.11g pronto proveerá la misma distancia que 802.11b pero también funcionará a 54 Mbps.

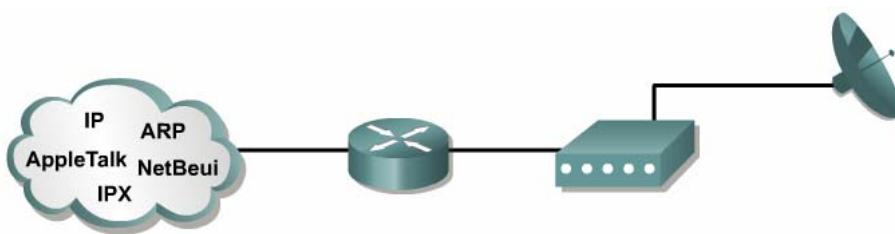


Distance or Bandwidth

- Greater distances possible at slower speed
- Aggregation using FEC or multilink bond up to three bridge links

Figura 1

Finalmente, las WLANs deben estar integradas correctamente para maximizar el ancho de banda entre los sitios ². Esto puede lograrse de varias formas, incluyendo el filtrado en el bridge, el filtrado de la Capa 2 usando un switch, o el filtrado de la Capa 3 usando un router. La solución del router es por lejos la mejor solución, lo que permite un control muy preciso del tráfico. Un router puede controlar lo siguiente:



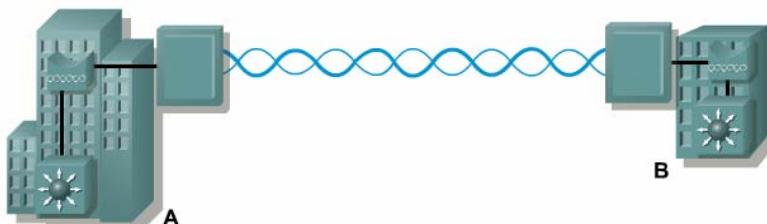
- Improve performance by sending only necessary data
- Bridges include filtering options to reduce unnecessary RF traffic
- Run a router in front of the bridge to selectively send desired traffic

Figura 2

- Protocolos de enrutamiento como el Protocolo de Información de Enrutamiento (RIP), Primero la Ruta Abierta Más Corta (OSPF) y el Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP) - Minimizan la cantidad de ancho de banda necesarios para los protocolos de enrutamiento. Las rutas estáticas no requieren ancho de banda y son recomendadas cuando se crea una red de conexión única.
- Protocolo enrutados como el Protocolo de Internet (IP), Intercambio de Paquetes de Internetwork (IPX) y AppleTalk - Minimizan los protocolos enrutados a través del enlace. Debido a las publicaciones frecuentes, IPX puede consumir ancho de banda necesario. Si es posible, limite el tráfico a IP puro.
- Origen y Destino - Minimice las direcciones que son permitidas a través del enlace.
- Seguridad - Maximice la seguridad a través del enlace usando IPSec para crear una red privada virtual (VPN).
- Broadcast de LAN - Elimine el tráfico de broadcast de Capa 2 y Capa 3 como ARP, NetBeui, Protocolo de Descubrimiento Cisco (CDP), IPX e IP creado por dispositivos LAN como estaciones de trabajo, servidores e impresoras.

9.4.2 Ejemplos de diseño

El ejemplo de diseño sitio a sitio de la Figura 1 es para una conexión punto a punto que requiere un enlace de bridge a través de una autopista. La distancia requerida es de sólo 0.8 km (0.5 millas). Por lo tanto, las antenas necesitan estar montadas a 3.9 m (13 pies). Suponiendo que las antenas están montadas en las azoteas de los edificios, esto no es un problema porque los edificios exceden la altura mínima. El cableado desde el bridge hasta las antenas es de 6.09 m (20 pies) en el Edificio A y 15.24 m (50 pies) en el Edificio B. Esto no tiene impacto, porque la distancia es muy corta. En este caso, utilice antenas patch para que el rayo pueda mantenerse enfocado y no le preocupe la interferencia de otras compañías.



Building A

- Antenna 8.5 dBi Patch

Building B

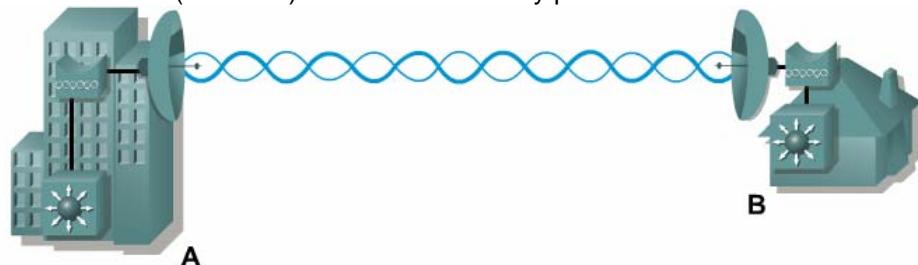
- Antenna 8.5 dBi Patch

Possible Distance

- 11 Mbps 0.6 Miles
- 1 Mbps 2.0 Miles

Figura 1

El ejemplo de diseño en la Figura 2 es un área rural que requiere una distancia de 40 km (25 millas). A causa de la gran distancia fueron elegidos platos parabólicos y las longitudes de los cables se mantuvieron mínimas. Una velocidad de 11 Mbps será imposible a causa de la distancia, por lo que se utilizará una velocidad de 2 Mbps. Esta configuración está bien dentro de las especificaciones necesarias. Incluso aunque sea posible alcanzar una distancia de 81.6 km (58 millas) a 2 Mbps, por favor observe que la línea de visión por sobre los 40 km (25 millas) es difícil de alinear y por lo tanto no es recomendable.



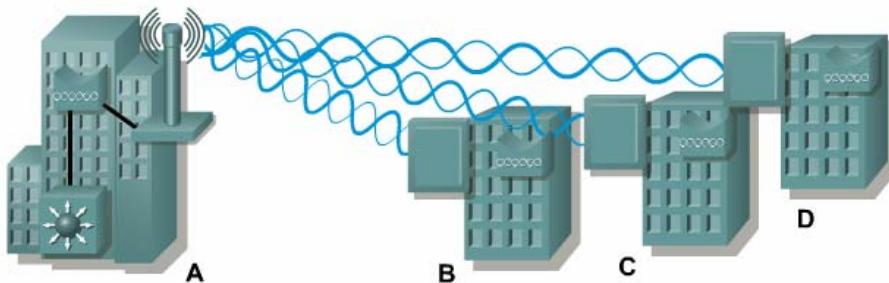
- Building A**
- Antenna 21 dBi Dish

- Building B**
- Antenna 21 dBi Dish

- Possible Distance**
- 11 Mbps N/A- Too Far
 - 1 Mbps 25 Miles

Figura 2

El ejemplo de diseño en la Figura 3 muestra la misma área metropolitana que saca provecho de la implementación punto a multipunto. La antena Omni posee un problema potencial de interferencia con otros usuarios de WLAN que utilicen los mismos canales, pero es razonable pensar que no existen interferencias.



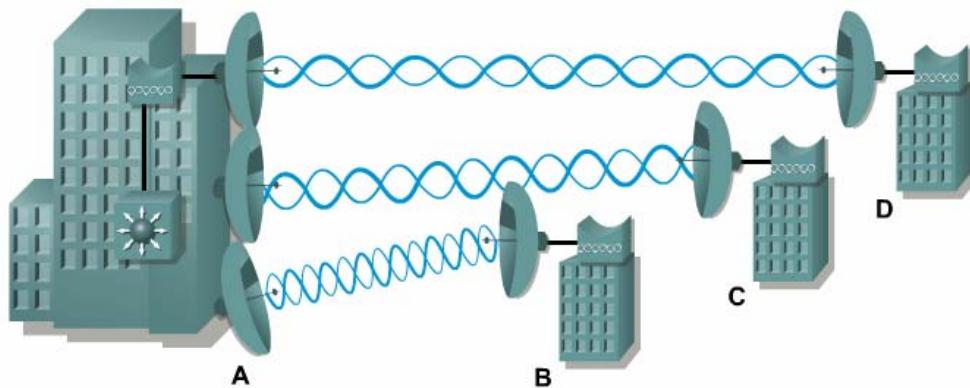
- Building A**
- Antenna 12 dBi High Gain Mast

- Building B ,C and D**
- Antenna 8.5 dBi Patch

- Possible Distance**
- 11 Mbps 0.6 Miles
 - 1 Mbps 2.0 Miles

Figura 3

El ejemplo de diseño de la Figura 4 muestra un edificio central dentro de un área metropolitana donde han sido implementados tres enlaces punto a punto separados. Tal configuración podría ser necesaria a causa de la interferencia de otras compañías que utilizan WLANs. Esto reemplaza a usar simplemente un diseño punto a multipunto. Además, los edificios recibirán un ancho de banda mayor en esta configuración que si estarían usando punto a multipunto. Esto es porque no hay ancho de banda compartido en este diseño. La montura de la antena no es una preocupación a causa de la corta distancia y los edificios altos.

**Buildings A, B, C, and D**

- Antenna 21 dBi Dish

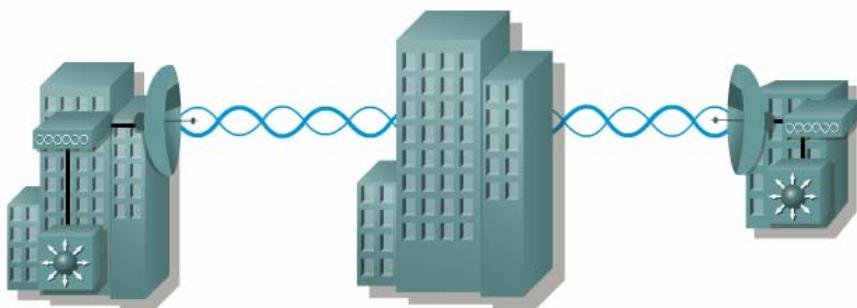
Possible Distance

- 11 Mbps 11 Miles
- 1 Mbps 25 Miles

Figura 4

9.4.3 Consideraciones de rutas

El principal factor que necesita ser considerado cuando se diseñan WLANs de edificio a edificio es la línea de visión de la radio. La antena de la ubicación remota debería ser visible desde el sitio principal. No debería haber obstrucciones entre las antenas 1. Otra consideración es un diseño edificio a edificio es la zona Fresnel, que se relaciona con la línea de visión. Es más parecida a una elipse, debido a la forma en que las ondas de radio se propagan realmente. Esta elipse debe estar libre de obstáculos durante todo el año. La primera consideración clave es asegurarse de que las antenas estén montadas lo bastante alto como para proveer un espacio libre en el punto medio de la zona Fresnel 2. A medida que la distancia aumenta, la curvatura de la tierra se convierte en otro problema. Esto también se debe considerar cuando se determine la altura de la montura de la antena.

**The following obstructions might obscure a visual link:**

- Topographic features, such as mountains
- The curvature of the earth.
- Buildings and other man-made objects
- Trees

Figura 1

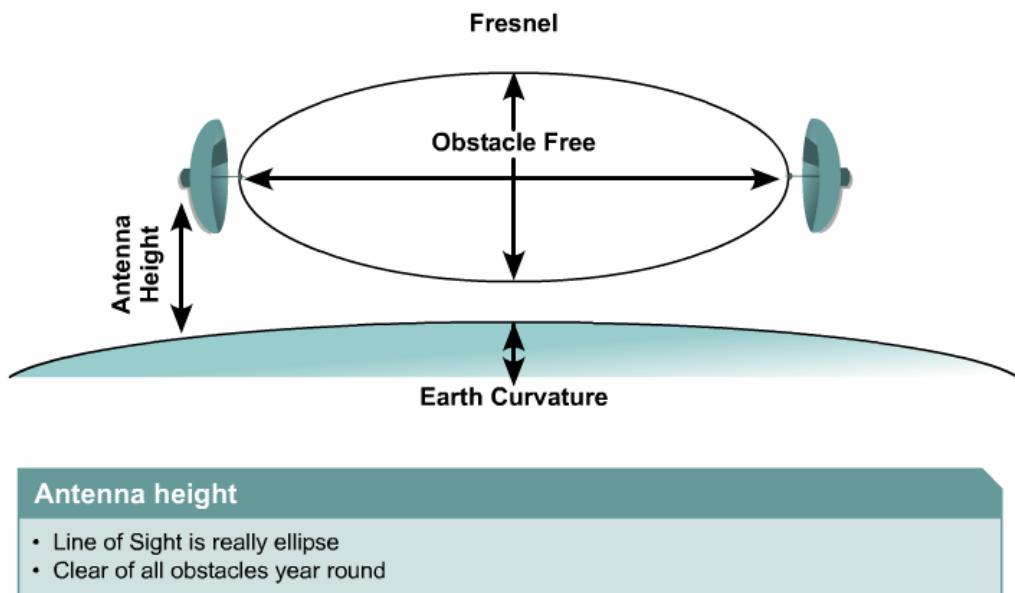
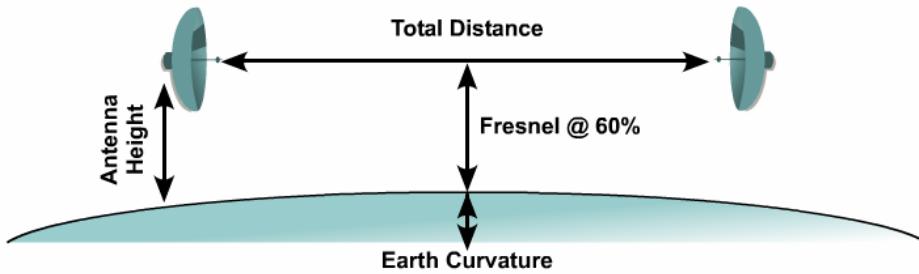


Figura 2

Para determinar la altura de la montura de la antena, tome el ancho de la ruta media de la zona Fresnel, al 60 por ciento para 2.4 GHz, y súmelo a la curvatura de la tierra. Para obtener estas medidas, vea la Figura 3. Los enlaces superiores a 40 km (25 millas) de distancia son muy difíciles de instalar y alinear, por lo que se debe tener cuidado cuando se recomiendan estos tipos de configuraciones.



Wireless Link-Distance in Miles	Approximate Value "F" in Feet (60% Fresnal Zone at 2.4GHz)	Approximate Value "C" Earth Curvature in Feet	Value "H" Antenna mounting Height in Feet with no obstructions
1	10	3	13
5	30	5	35
10	44	13	57
15	55	26	83
20	65	50	115
25	72	78	150

Figura 3

9.5 Equipo para el Estudio del Sitio

9.5.1 Equipo

Antes de instalar una WLAN, asegúrese de que habrá una cobertura de onda de radio adecuada en toda la instalación y una interferencia RF mínima.

El equipo para el estudio debería incluir lo siguiente:

- Access point: Este es necesario para el área base del estudio. Siempre es recomendable uno de repuesto.
- Dispositivo cliente: Utilice el dispositivo cliente que el usuario desea utilizar. Siempre lleve uno de repuesto.

- PC laptop: Use la PC laptop con la tarjeta de PC elegida. Se recomienda usar una batería de gran potencia y llevar una batería de repuesto.
- Batería del AP: La energía CA no está disponible en ciertas áreas. Un dispositivo sencillo que se puede utilizar para duraciones cortas es una batería de respaldo APC [2](#). Otra opción es una batería CD TerraWave, que proporciona hasta 8 horas de energía. Incluye adaptadores para los APs y bridges de Cisco. Se puede comprar un adaptador de energía especial de línea entrante.
- Antenas: Lleve todas las variedades de antenas que pueda necesitar. Todas las áreas de cobertura pueden ser diferentes.
- Cámara digital: Tome fotos para comparar el sitio estudiado con las ubicaciones reales de los equipos en el momento de la instalación.
- Cables: Pueden ser necesarios cables patch Categoría 5. Tenga una caja de cables y una bolsa de conectores a mano. De esa forma podrá hacer el cable con la longitud que necesite.

Los siguientes ítems varios también deberían estar incluidos:

- Banda de sujeción: Puede ser necesario sujetar el AP o la antena cuando se realiza el estudio.
- Cinta aisladora: Este ítem siempre es necesario.
- Linterna pequeña: El área del cielo raso puede no tener luces.
- Equipo - Siempre utilice el equipo que el usuario final usará. No realice el estudio con una rubber ducky a menos que sea lo que el usuario utilizará.
- Dispositivo de etiquetado: Puede ser útil para etiquetar cables, ubicaciones y dispositivos [1](#), [2](#). Puede utilizarse también cinta de color, marcadores indelebles o autoadhesivos.
- Escalera: Muchas veces se necesitará una escalera para acceder a los cielos rasos y a espacios abiertos por sobre la cabeza. Diferentes proyectos y tareas requieren el uso de escaleras de diferentes estilos, tamaños, resistencias y materiales. Tenga presente la seguridad y elija la escalera correcta para el trabajo.
- Alargadores y luz colgante: Si se necesita hacer una prueba extensa, una batería puede no durar lo suficiente como para completarla. Además, una luz colgante puede ser una mejor opción que una linterna y no requiere una mano extra.
- Medidores: Estos son necesarios para determinar las distancias de los cables y las áreas de cobertura. Una rueda de medición se muestra en la Figura [3](#). Un metro es útil, y una soga marcada puede ser necesaria para medir distancias verticales.
- Herramientas de seguridad: Se debería usar dispositivos de protección ocular y cascos mientras se trabaja en cielos rasos o en otras áreas peligrosas. Un chaleco naranja fluorescente ayuda a aumentar su visibilidad.
- Binoculares o Telescopios: Son necesarios en el estudio de sitio a sitio para controlar la línea de visión en distancias de hasta 40 km (25 millas). También se puede usar un láser o un telémetro.
- Dispositivos de comunicación: Los walkie-talkies son muy útiles cuando se trabaja con un compañero o grupo de estudio. Se pueden usar los teléfonos celulares pero usted necesita estar seguro de que tendrá una buena fuerza de señal..



Figura 1

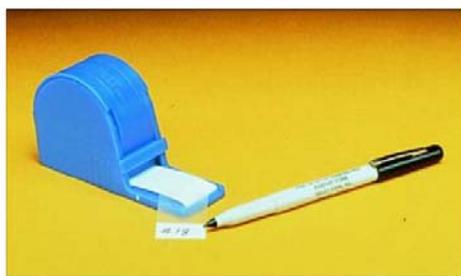


Figura 2



Figura 3

Se debería utilizar la siguiente maquinaria pesada:

- Grúa: Cuando se realiza un estudio para la implementación de una WLAN de sitio a sitio, puede ser necesario alquilar una grúa o un dispositivo elevador que alcance una altura de hasta 45.72 m (150 pies) para determinar cualquier obstrucción de la línea de visión. Se podría contratar a un tercero para que realice esta tarea.
- Elevador de tijera: Cuando se trabaja en áreas con cielos rasos altos o techos por encima de los 6 m (20 pies), puede ser necesario alquilar un elevador del tipo de tijera para acceder al área.

Con la cantidad y costo del equipo necesario para un estudio del sitio, puede ser necesario utilizar una valija con ruedas de alta resistencia. El tener el equipo adecuado es profesional y simplifica el trabajo. Tenga presente que las herramientas costosas atraen a los ladrones. Siempre asegure o guarde el equipo y las herramientas.

9.5.2 APs y tarjetas

Access Points

También es una buena idea llevar más de un access point. Muchos ingenieros han tenido un contratiempo con un AP que les produjo una pérdida de tiempo durante el estudio. Un AP extra permite que el estudio continúe sin tener que esperar a recibir un repuesto.

Los APs pueden tener una variedad de configuraciones, como se ve en la Figura 1. Los access points que tienen Conectores de la Marina a Rosa de Polaridad Invertida (RP-TNC) dan al ingeniero del estudio la opción de usar una variedad de antenas para solucionar problemas de cobertura. Diferentes antenas pueden tener diferentes tipos de conectores, como se muestra en la Figura 2. Los puertos de antena de 2,4 GHz de los APs Serie 1200 tienen conectores RP-TNC. Los APs Serie 1100 no tienen conectores RP-TNC, lo que limita al ingeniero del estudio a una antena de diversidad de 2,2 dBi. Los APs serie 1200 tienen un módulo de 5 GHz que sirve como la radio y la antena CardBus de 5 GHz. Debido a los requisitos de FCC el módulo de la antena de 5 GHz ofrece dos opciones, que son modo patch de 6 dBi y modo omni direccional de 5 dBi.

Access Points	
802.11b	
• With RP-TNC	<ul style="list-style-type: none"> - Reverse Polarity Threaded Naval Connector (RP-TNC) - 1200 Series Access Point (2.4 GHz)
• Without RP-TNC	<ul style="list-style-type: none"> - 1100 Series Access Point
802.11a	<ul style="list-style-type: none"> • 1200 Series with 5 GHz Module
Survey with correct access point	<ul style="list-style-type: none"> • Customer purchases an 1200 Series Access Point - survey with a 1200 Series Access Point

Figura 1



Client Cards

Client Cards

- PC Cards

MicroMate Connector (MMCX)

Figura 2

Tarjetas Clientes

Hay múltiples tipos de tarjetas PCMCIA, como lo muestra la Figura 2. Una caja de herramientas para el estudio debería contener al menos una tarjeta PCMCIA de cada tipo. Estudie el sitio con el tipo de tarjeta que con más probabilidad se utilizará.

9.5.3 Antenas y atenuadores

Antenas

No hay una única antena que sea perfecta para todas las aplicaciones. Por lo tanto se ofrece una variedad de antenas, como lo muestra la Figura 1. El usuario normalmente indicará la elección y la ubicación de la antena. Un usuario puede no querer que la antena esté visible, o que pueda estar ubicada en un área de gran tráfico. La colección mínima de antenas debería ser la siguiente:



Antennas

- Two of every antenna you may have to use
- Diversity
- Availability of antennas

Figura 1

- Antena "rubber ducky" Bipolar de 2.2 dBi
- Antena de Montura en Cielo Raso Omni de Diversidad de 2.0 dBi
- Antena de Montura en Mástil de 5.2 dBi
- Antena Omni de Diversidad Montada en Pilar de 5.2 dBi
- Antena Montada en Pared Parch de Diversidad 6.0 dBi
- Antena Patch Hemisférica de 8.5 dBi
- Antena de Montura en Mástil Yagi de 13.5 dBi

También pueden utilizarse otras antenas.

Siempre realice el estudio con la antena pretendida. Si está planeado usar diversidad, entonces serán necesarias dos antenas de cada tipo. No utilice una antena diferente e intente adivinar la cobertura que se necesita. El estudio del sitio se realiza para evitar las conjeturas en la instalación.

Atenuador de antena

Los estudios siempre deberían realizarse usando el equipo que finalmente será instalado. Esto a veces puede ser difícil en el caso de divisores, pararrayos y cables alargadores.

En lugar de llevar muchas longitudes de cables, pararrayos, divisores y otros accesorios, algunos ingenieros equipan a la caja de herramientas para el estudio del sitio con un atenuador de antena. El atenuador de antena permite injectar pérdida sin necesidad de otros accesorios. Por ejemplo, si hay un cable de 250 m que se extiende con divisores en la instalación real, la pérdida de la señal puede simularse por medio del atenuador. Esto puede ahorrarle al ingeniero del sitio un valioso tiempo y dinero.

9.5.4 Baterías, cables, monturas y marcadores

Baterías y Cables

Los access points necesitan energía para funcionar. No siempre habrá electricidad disponible en los alrededores mientras se realiza un estudio del sitio. Una buena batería durará por al menos 8 horas, lo que le permite al ingeniero estudiar todo el día sin tener que recargarla.

También se recomienda tener un cargador rápido para la herramienta del estudio del sitio. Si se utiliza una laptop, siempre se recomiendan baterías que puedan ser cargadas en forma separada de la laptop. Las tarjetas PC inalámbricas necesitan una fuente de energía continua mientras se realiza el estudio y pueden reducir la vida de la batería a menos de dos horas. Las baterías de ión de litio alimentan a la unidad por más tiempo, se cargan con más eficiencia, y son livianas [1](#)

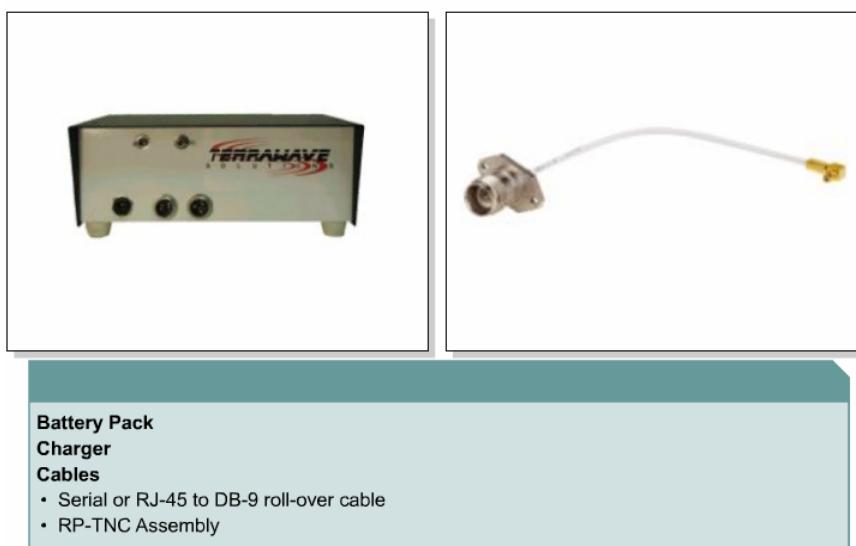


Figura 1

Hardware de Montura

Siempre se debería llevar un soporte para montar el AP. La caja de herramienta debería también contener varias soluciones de montura para el soporte. Esto incluye abrazaderas de viga, abrazaderas "C" y soportes de montura para cada antena cuando estén disponibles. Abrazaderas plásticas, cinta adhesiva, alambre bobina, cinta aisladora, cinta adhesiva por los dos lados, Velcro y clips de papel con componentes comunes en la caja de herramientas de un ingeniero.

Durante un estudio no hay soluciones de monturas malas excepto la solución que no asegure correctamente al access point, a la batería y a la antena. No sólo se podría dañar al equipo, sino que hay riesgo de daños debido a la caída del equipo. [2](#)

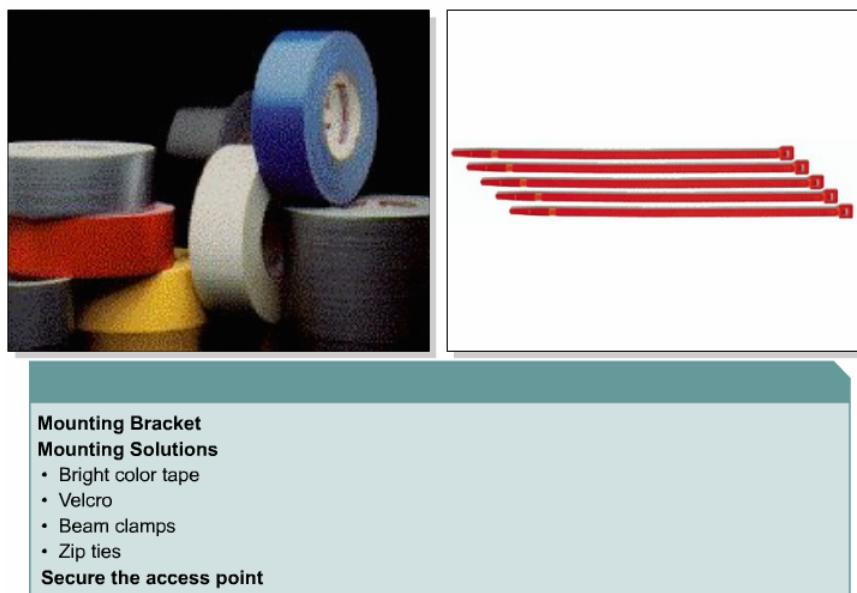


Figura 2

Marcadores

Una vez que la ubicación del access point está determinada, será necesario marcarla. Como se muestra en la Figura 3, los marcadores de ubicación deberían ser muy brillantes y resistentes al polvo, la grasa y el agua. Las cintas de agrimensor son muy buenas y vienen en una variedad de colores brillantes. Los marcadores deberían ser resistentes pero temporales.

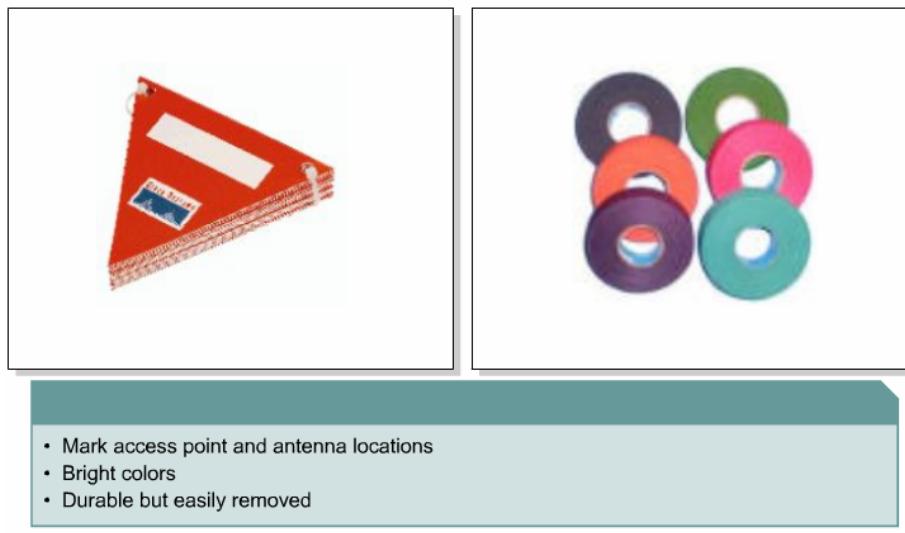


Figura 3

9.5.5 Dispositivos de medición y cámaras digitales

Dispositivos de medición

Para proporcionar al usuario los detalles necesarios para conseguir la instalación, se deben proporcionar muchas mediciones en el reporte del estudio del sitio. Estas mediciones deben ser tan exactas como sea posible.

La caja de herramientas incluye una rueda de medición para medir distancias de cables. Muchas personas incluyen equipos más avanzados como dispositivos de medición por láser y telémetros. Para medir distancias verticales, una soga marcada en incrementos de 3 m (10 pies) permitirá medir distancias en forma precisa desde el piso hasta el cielo raso. 1



- Measuring wheel (horizontal distances)
- Height measurement
- Rope marked in 10' or 3 meters increments (vertical distances)

Figura 1

La cantidad de baldosas en el piso o de losas en el cielo raso no es siempre un buen método para medir distancias.

Cámara digital

Siempre es mejor fotografiar cualquier situación inusual encontrada mientras se está realizando el estudio del sitio. ~~2~~ Éstas incluyen paredes móviles o retráctiles, ubicaciones actuales de estanterías y puentes grúas.



- Easiest way to document unusual situations
- Need to photograph antenna mounting locations & methods

Figura 2

Todos los métodos y ubicaciones de montura de antenas deberían ser fotografiados e incorporados en la documentación del estudio del sitio. Recuerde, el que realiza el estudio puede no hacer el trabajo de instalación.

9.5.6 Valija de viaje

La parte más importante de un estudio del sitio es la caja de herramientas del estudio del sitio. No importa cuán talentoso pueda ser el ingeniero, es imposible realizar un estudio del sitio sin las herramientas apropiadas. Se recomienda que la caja de herramientas del estudio del sitio sea una unidad portátil. Para facilidad de uso, una caja de plástico duro con ruedas y que pueda ser registrada como equipaje es el mejor y más común embalaje.

Los estudios del sitio a menudo son pedidos con muy poca anticipación. El ingeniero debería poder llevar la valija en el baúl o en el asiento de atrás de un auto o registrado como equipaje para viajar con el equipo.

Este resuelve el problema de la pérdida de la caja o de la retención cuando se envía. También permite la instalación rápida del ingeniero.

9.5.7 Dispositivo de prueba de RF

Está disponible una variedad de herramientas de prueba de RF para el diseñador de WLANs, incluyendo los ítems listados en la Figura 1.

- A Spectrum Analyzer is sometimes used to locate sources of Radio Frequency Interference (RFI) [1]
- A handheld Frequency Counter can provide a quick reference to specific emissions in a close area
- An Electromagnetic Field Probe can detect local sources of Electro-Magnetic Interference (EMI)

Figura 1

Las herramientas de prueba listadas en esta sección no son dispositivos comunes para los que estudian el sitio. Cuando se determina la factibilidad de colocar equipos en entornos celulares o áreas de corriente eléctrica alta como maquinaria industrial, estos dispositivos podrían utilizarse para rastrear el entorno en busca de problemas potenciales antes de colocar el equipo de estudio. Estos dispositivos también son usados para solucionar problemas en cualquier entorno aislando las fuentes de RFI o de EMI.

9.6 Documentación y Utilitarios del Estudio del Sitio

9.6.1 Dibujo y recorrido del sitio

Dibujo del sitio

Como se indicó en la Figura 1, asegúrese de tener una buena cantidad de papel para la recorrida y el estudio del sitio para realizar notas y marcar áreas de cobertura. Si debe pedir un conjunto de planos/dibujos al usuario, recuerde que deberá esperar de dos a tres semanas para obtener las copias. Los dibujos digitales son mejores para transferir la información a un reporte en un momento posterior.

- A set of drawings or prints are needed to annotate:**
- AP locations
 - Coverage areas
 - Cable and electrical requirements
 - Sources of interference
- A set of colored pens, ruler, and something to mark the locations in the facility such as flagging tape are also needed.**

Figura 1

Recorrido del sitio

Este paso crítico ayudará a definir las áreas de cobertura y los puntos ciegos en las instalaciones. El usuario debería dirigir el recorrido y responder a cualquier necesidad o preocupación. Un recorrido del sitio es también útil para localizar cualquier fuente posible de interferencia de frecuencia de radio (RFI), interferencia electromagnética (EMI), problemas ambientales o de construcción buscando otras antenas o motores eléctricos de alto voltaje. Algunos elementos del entorno que definen la posible cobertura para el área son los siguientes:

- Otras WLANs
- Motores eléctricos de alto voltaje
- Paredes o cielos rasos de acero corrugado
- Cantidad de varillas de refuerzo en el concreto
- Polarización de ventanas de óxido de metal
- Inventario como de materiales y suministros

Construya un diagrama del sitio basado en los dibujos que identifican la cobertura deseada y los problemas encontrados en el recorrido.

9.6.2 Utilitario para el cálculo del alcance del bridge

Cisco hace más fácil el cálculo de las distancias del bridge con el uso de la planilla de cálculo de distancias de Cisco que está disponible en el sitio Web de Cisco. Todo lo que tienen que hacer los usuarios es seguir varios pasos básicos.

- Seleccione la línea de productos que está utilizando.
- Luego seleccione la antena apropiada para ambos sitios. Para antenas que no son Cisco, ingrese la ganancia en dBi. El concepto de unidad dBd era capturar la ganancia de una antena en relación con una antena bipolar. Una bipolar se considera la antena horizontal estándar básica, y las comparaciones con ella parecían tener más sentido que las comparaciones con el radiador isotrópico. Si la ganancia de la antena se da en dBd, simplemente sume 2,15 al número para convertirlo en dBi.
- Luego seleccione el cable usado en ambos sitios. Si no está usando antenas Cisco estándares, ingrese la longitud y la pérdida del cable por cada 30 metros (100 pies) en el lugar apropiado. Para los cables Cisco esto es 6,7dB / 100 pies a 2,4GHz. Si se utiliza un cable diferente, contáctese con el fabricante para obtener esta información.
- Agregue cualquier otra pérdida debida a divisores, conectores, etc. en la columna de misceláneas.

Recuerde que éstos son valores teóricos, pero deberían proporcionar un buen nivel de comodidad para un funcionamiento apropiado. Estos valores son para la línea de visión y proporcionan un margen de debilitamiento de 10dB que asegura que los cálculos funcionarán.

Para determinar la distancia de bridging se consideran los siguientes ítems:

- La ganancia de las antenas se da en dBi, en base a una antena isotrópica teórica, no en dBd que está basado en una antena bipolar.
- Para convertir dBd en dBi sume 2,15 a los dBd. Como resultado, $0\text{dBd} = 2.15\text{dBi}$.
- Las longitudes de los cables son una pérdida y se restan.

Los parámetros de las antenas y de la radio incluyen pérdidas del cable en los sitios de recepción y transmisión, las antenas usadas en ambos sitios y el rendimiento del receptor y el transmisor. La ganancia del receptor cambia con la velocidad de los datos. Siempre utilice los valores de velocidad de datos máximos necesitados por el usuario.

Las distancias para estas fórmulas están calculadas en millas. Para cualquier frecuencia dada, la atmósfera ofrece pérdidas. Esta pérdida es un estándar para cualquier radio en esa frecuencia. En este caso, utilice la frecuencia media de 2442Mhz.

Un ejemplo de parámetros de radio y de antena está calculado en la Figura 1. Este cálculo utiliza un valor de 20 dBm para la potencia de transmisión, antenas yagi de 2 dBi a 13.5 dBi y dos cables de 6 m (20 pies) cada uno. Los valores se ingresan en la fórmula para calcular la distancia máxima.

Models Supported- Cisco Aironet BR350, BR340, BR500, WGB350, WGB340, PCI350 and PCI340			
Regulatory Domain----->	N. America FC	Select this from Power Regulatory Domain page	
Site 1		Site 2	
Select Product #1 ----->	AIR- BR350	Select Product #2 ----->	AIR- BR350
Select Power level----->	100	Select Power level----->	100
Select Datarate----->	1Mbps		
Select Antenna 1 here----->	13.5dBi Yagi	Select Antenna 2 Here---->	13.5dBi Yagi
For other Antenna- Enter Gain Here-->	6	For other Antenna- Enter Gain Here---->	6
Select Cable 1----->	100ft Ultra Low	Select Cable 2----->	100ft Ultra Low
For 'OTHER' Cable		For 'OTHER' Cable	
Enter Cable Loss/100 ft here----->	4.4	Enter Cable Loss/100 ft here----->	4.4
Enter in Length Here----->	100	Enter in Length Here----->	100
Effective Isotropic Radiated Power-->	29.1	Effective Isotropic Radiated Power-->	29.1
Max Distance (w/ 10dB Fade Margin)----->		2.8 Miles	4.6 Kilometers
Earth Bulge at above distance----->		5 feet	1.5 Meters
Fresnel Zone clearance for above distance-->		23 feet	7.1 Meters
Required antenna height above obstructions-->		28 feet	8.6 Meters

Figura 1

9.6.3 Estudio del sitio con ACU

La herramienta de Estudio del Sitio Utilitario del Cliente Aironet (ACU) funciona en el nivel de RF y se utiliza para determinar la mejor ubicación y la cobertura o superposición para las Aplicaciones de red 1. Durante el estudio del sitio, el estado actual de la red se lee en el adaptador cliente y es mostrado cuatro veces por segundo para el rendimiento de la red pueda ser medido con exactitud. La retroalimentación que se recibe puede ayudar a eliminar áreas de niveles bajos de señal RF que pueden dar por resultado una pérdida de conexión entre el adaptador cliente y su AP asociado.

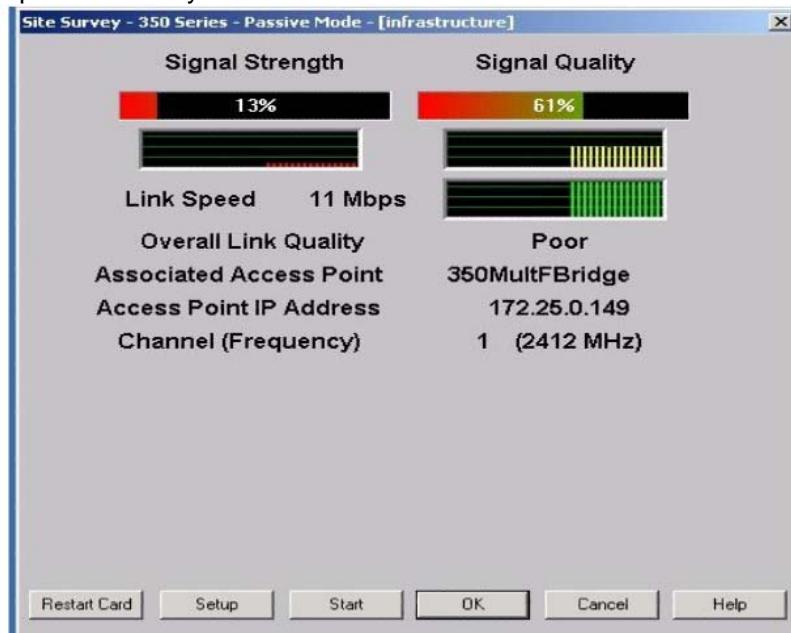


Figura 1

La herramienta de Estudio del Sitio puede ser usada en dos modos:

1. Modo Pasivo - Este es el modo de estudio predeterminado. No inicia ningún tráfico de red RF. Simplemente escucha el tráfico que el adaptador cliente oye y muestra los resultados.
2. Modo Activo - Este modo, mostrado en la Figura 2, causa que el adaptador cliente envíe en forma activa paquetes de RF de bajo nivel hacia o desde su AP asociado y proporciona información sobre el índice de éxito. También activa parámetros como la velocidad de los datos a ser enviados para controlar la forma en que se realiza el estudio del sitio.

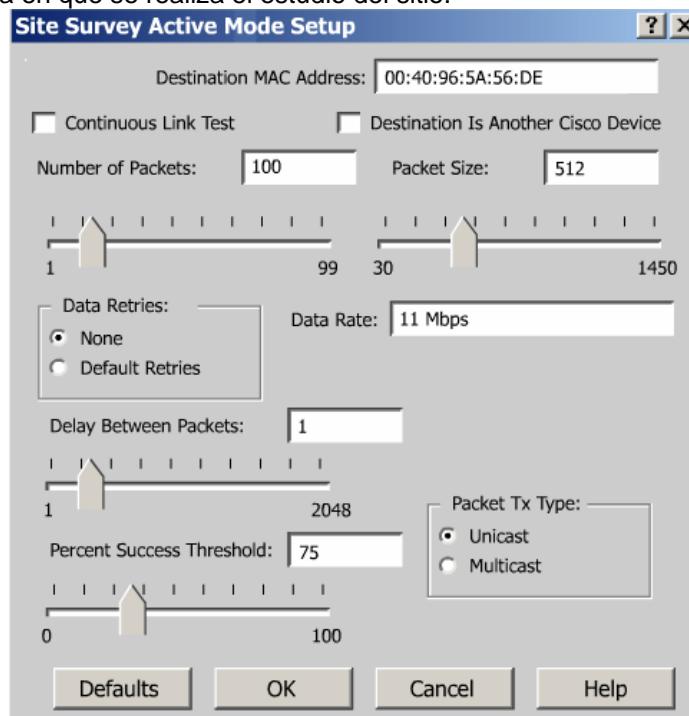


Figura 2

Se debería mantener en mente las siguientes pautas cuando se prepare la realización de un estudio del sitio:

- Realice el estudio del sitio cuando el enlace RF esté funcionando y todos los otros sistemas y fuentes de ruido estén activos.
- Ejecute el estudio del sitio totalmente desde la estación móvil.
- Dirija el estudio del sitio con todas las variables fijadas con valores operativos cuando se utilice el modo activo.

9.6.4 Medidor del estado del enlace (LSM)

Uso del medidor del estado del enlace

Esta sección explica cómo usar el utilitario LSM para determinar el rendimiento del enlace RF entre el adaptador cliente y su access point asociado.

Para abrir el LSM en Windows 95, 98, NT, 2000, XP o Me, haga doble clic sobre el ícono ACU en el escritorio **1**. Luego, haga clic sobre el ícono Link Status Meter[Medidor del Estado del Enlace]. Aparece la pantalla Link Status Meter **2**. La pantalla Link Status Meter proporciona una visualización gráfica de lo siguiente:

- Fuerza de la señal - La fuerza de la señal de radio del adaptador cliente en el momento en que los paquetes están siendo recibidos. Se muestra como un porcentaje a lo largo del eje vertical.
- Calidad de la señal - La calidad de la señal del adaptador cliente en el momento en que los paquetes están siendo recibidos. Se muestra como un porcentaje a lo largo del eje horizontal.



Figura 1

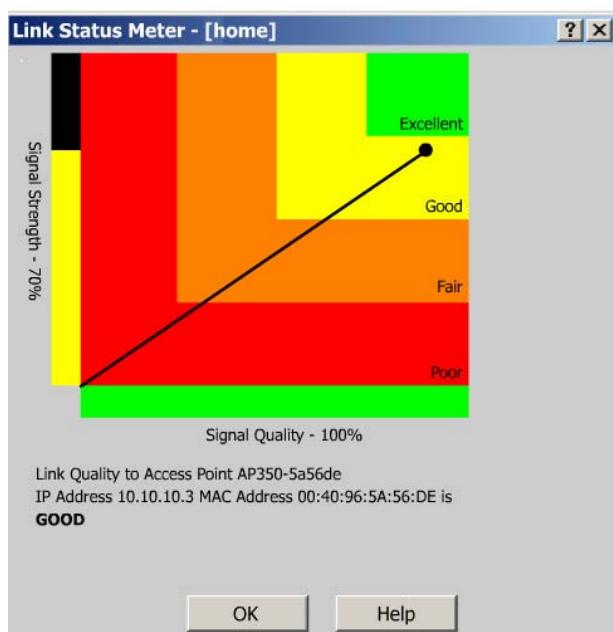


Figura 2

La línea diagonal representa el resultado combinado de la fuerza de la señal y la calidad de la señal **2**. La ubicación de la línea sobre la visualización gráfica determina si el enlace RF entre el adaptador cliente y su AP asociado es pobre, regular, bueno o excelente.

Esta información puede ser utilizada para determinar la cantidad óptima y ubicación de APs en la red de RF. Al usar el LSM para evaluar el enlace RF en varias ubicaciones, se pueden evitar las áreas de rendimiento débil para eliminar el riesgo de perder la conexión entre el adaptador cliente y el AP.

El AP que está asociado al adaptador cliente y su dirección MAC están indicados en la parte inferior de la visualización.

Los parámetros que controlan el funcionamiento del LSM pueden ser fijados por el usuario. Para hacer esto, seleccione Preferences [Preferencias] en el menú desplegable Options [Opciones] **3**. Los parámetros y descripciones del LSM se muestran en la Figura **4**.

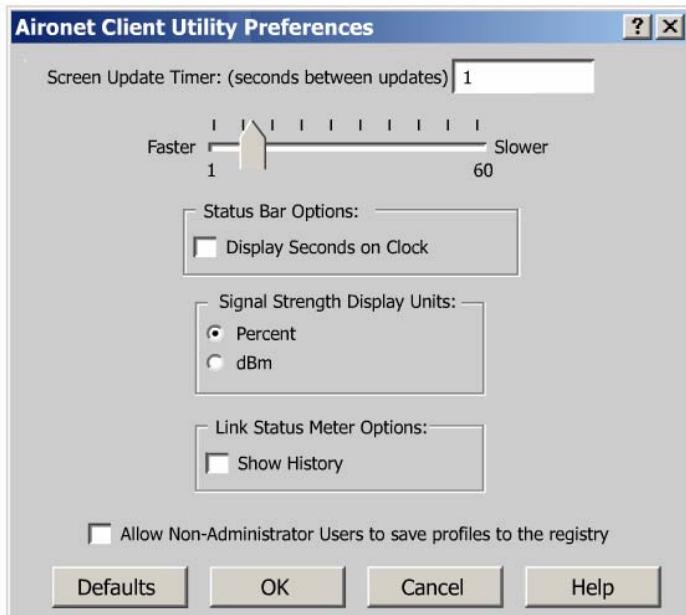


Figura 3

Parameters	Description	
Screen Updates Per Minute	Specifies how often the LSM graphical display is updatedRange: 1 to 120 updates per minute, or once a minute to twice a secondDefault: 60 updates per minute, which is once per second	
Display Icon in Systray when minimized	Selecting this checkbox causes an LSM icon to be displayed in the bottom right corner of the desktop when LSM is minimized.Default: Selected; Display Link Status icon tool tipSelect the information that displays when the cursor is positioned over the icon. The following table lists and describes the options:	
	Systray Icon Tool Tips	Description
	Display Link Status	Indicates the client adapter ability to communicate with the access point Range: Not Associated, Poor, Fair, Good, Excellent
	Display Signal Strength	Indicates the signal strength for received packets Range: 0 to 100 percent
	Display Signal Quality	Indicates the signal quality for received packets Range: 0 to 100 percent
Display History	Selecting this checkbox causes the LSM graphical display to show a recent history of the RF performance between the client adapter and its associated access point. Black dots on the graphical display show the performance of the last 50 signals.Default: Selected	

Figura 4

Haga clic sobre OK [Aceptar] en la parte inferior de la pantalla Preferences del LSM para guardar todos los cambios.

Resumen

Este módulo proporcionó las herramientas necesarias y el conocimiento necesario antes de realizar un estudio del sitio. Un buen estudio del sitio permite que el ingeniero determine la cantidad de APs de cobertura que proporcionará, los tipos de APs que serán utilizados, la interferencia de frecuencias de radio y cualquier otra limitación.

Después de hablar sobre la forma en que un ingeniero debe prepararse para un estudio del sitio, el módulo trata los cuatro requisitos principales de diseño para cualquier solución WLAN:

1. Disponibilidad
2. Escalabilidad
3. Administrabilidad
4. Interoperabilidad

Después de dar cuidadosas consideraciones acerca de las necesidades de la institución que desea implementar una WLAN, el ingeniero del sitio debe ir preparado con el equipo apropiado. Un ingeniero del sitio debería tener múltiples APs listos para probar. El ingeniero del sitio debería también llevar los dispositivos de prueba apropiados para asegurar que el plan sea factible.

Finalmente, el alumno obtendrá una valiosa experiencia práctica a través del uso de laboratorios y actividades demostrativas que cubren el diseño de WLAN, utilitarios de cálculo, documentación y el utilitario Medidor del Estado del Enlace.

Módulo 10: Estudio del sitio e instalación

Descripción General

El Módulo 9 habló sobre los pasos necesarios para preparar un estudio del sitio. Este módulo hablará sobre el estudio del sitio y la instalación real de la WLAN. Los temas tratados en este módulo incluyen la importancia del conocimiento de la infraestructura y la creación de un mapa de red preciso como paso inicial en la conducción de un estudio del sitio. Este es un paso importante en el diseño de la red porque el examinador del sitio puede juzgar mejor la forma de satisfacer las expectativas para la escalabilidad, el rendimiento y la disponibilidad de la red. El examen de la red existente incluye conocer la topología y la estructura física, y evaluar el rendimiento de la red.

Después de examinar la forma en que los mapas de red iniciales son creados, se tratará el proceso de realizar un estudio del sitio. También se hablará sobre los problemas de montaje e instalación. Aunque la determinación del área de cobertura apropiada involucra prueba y error, la experiencia y los mapas de red apropiados pueden ser de mucha ayuda para el ingeniero del estudio. Recuerde, si se necesita una cobertura sin fisuras, las células de cobertura se deben superponer.

Finalmente, el alumno aprenderá a documentar el proceso completo creando un reporte del estudio del sitio o respondiendo en forma apropiada a las Peticiones de Propuestas (RFPs).

10.1 Conocimiento de la Infraestructura

10.1.1 Trabajo con el personal

Al darle al usuario un reporte detallado del estudio del sitio, un administrador de IT puede entregar las partes necesarias a un contratista local. El contratista puede instalar el cableado necesario para proporcionar conectividad a los dispositivos WLAN con la red. Los contratistas necesitan un estudio del sitio que les provea información detallada acerca de dónde se van a ubicar los APs, cómo estarán conectados a la red, y dónde se necesita instalar cableado o energía. Al mismo tiempo, se pueden hacer preparativos en la red del usuario para la instalación próxima.

Trate de identificar los problemas potenciales por adelantado y hable sobre cómo serán manejados. Este descubrimiento puede ahorrar mucho tiempo y preocupaciones durante la instalación. Al tratar con problemas potenciales y ser proactivo en lugar de reactivo, el ingeniero del estudio del sitio es visto como una fuente de fortaleza y confianza durante la instalación. Un buen estudio comienza con una lista de control previa, como lo muestra la Figura 1.

- Step 1** Make a detailed layout of the building.
- Step 2** Decide on the method of powering the AP, AC accessible or 18 volts at 4-Amp hour battery pack
- Step 3** Prepare a description of the desired coverage areas.
- Step 4** Prepare a description of the desired usage of e-mail, Internet, applications, and so forth. This will determine the potential load of each AP.
- Step 5** Select the same model of RF equipment that the customer will use.

Figura 1

Después de que el usuario ha decidido tener un estudio del sitio, se debe completar un formulario previo al estudio del sitio. Éste determinará el tipo de estudio que será conducido, cuántos días llevará, el equipo que será necesario y qué preguntas será necesario hacer durante el recorrido. Un formulario previo al estudio del sitio es una introducción a las instalaciones del usuario. Es muy importante reunir toda la información necesaria.

10.1.2 Infraestructura de la LAN

Un paso importante en el diseño de la red es examinar una red existente del usuario para determinar cómo satisfacer las expectativas de escalabilidad, rendimiento y disponibilidad de la red. El examen de la red existente incluye conocer la topología y la estructura física, y evaluar el rendimiento de la red.

El conocimiento de la estructura, el uso y el comportamiento de la red existente se pueden usar para determinar si los objetivos de diseño del usuario son realistas. Los problemas potenciales pueden ser documentados. Los problemas incluyen la identificación de los dispositivos y de los enlaces de internetworking que deben ser reemplazados porque la cantidad de puertos o la capacidad es insuficiente para el nuevo diseño de la WLAN. La identificación de los problemas de rendimiento puede ser útil al seleccionar soluciones para resolver problemas y para desarrollar una referencia para futuras mediciones de rendimiento.

La mayoría de los diseñadores de redes no las diseñan desde cero, sino que diseñan mejoras para las redes existentes. Un diseño de red exitoso requiere que la red existente interactúe con la inclusión inalámbrica anticipada.

Algunas de las áreas de la red a investigar incluyen la infraestructura y la topología de la LAN. El usuario desea tener confianza en que el ingeniero en sistemas (SE) o el ingeniero del estudio sea capaz de realizar esta tarea.

El SE necesitará trabajar con alguien del departamento de IT del usuario para descubrir el formato de la red existente. Por lo general, es una buena idea comenzar identificando la topología de la LAN. Será de ayuda si el cliente puede proporcionar un dibujo lógico de la red.

Existen muchas topologías diferentes. La mayor parte de las compañías utilizan una topología del tipo estrella para su red, como una estrella agrupada o distribuida. El SE debería identificar dónde están ubicados los componentes de la red. El representante de IT debería identificar dónde están ubicados los servidores, dónde están los puntos de conectividad y por dónde está corriendo el cableado sobre un mapa de la red, que puede ser fácilmente impreso o duplicado. Si no existe un mapa de red, o si está desactualizado, se debe crear uno.

10.1.3 Mapa de la red

Hay varios aspectos involucrados en la caracterización de la infraestructura de una red:

- Desarrollo de un mapa de red [1](#)
- Aprendizaje de la ubicación de los principales dispositivos de internetworking y segmentos de red
- Documentación de los nombres y direcciones de los principales dispositivos y segmentos
- Identificación de cualquier método estándar para direccionar y colocar nombres
- Documentación de los tipos y longitudes del cableado físico
- Investigación de la arquitectura y limitaciones ambientales

Para desarrollar una comprensión del flujo de tráfico, conozca la ubicación de los principales hosts, dispositivos de interconexión y segmentos de red. Una combinación de la información sobre las características del rendimiento de los segmentos de la red y sus ubicaciones proporciona una idea sobre el lugar donde se concentran los usuarios y el nivel de tráfico que debe soportar un diseño de red.

En este punto del proceso de diseño de la red, el objetivo es obtener un mapa de la red existente. Algunos usuarios del diseño pueden tener también mapas para el nuevo diseño de red. Sin embargo, evite usar suposiciones que no estén basadas en un análisis detallado de la empresa y en los requisitos técnicos.

No todos los usuarios pueden proporcionar un mapa detallado y actualizado de la red existente. Las compañías que están constantemente reaccionando a situaciones no tienen tiempo de completar la documentación de la red existente.

Mientras esté estudiando una instalación y decidiendo la ubicación de los APs, busque formas de conectar los APs a la red. En este punto, el formato y los componentes de la red deberían ser bien conocidos y el SE debería tener una buena idea de dónde y cómo colocar interfaces con la red. La mayoría de los SEs no son expertos en cableado. La tarea del SE es realizar el estudio y hacer recomendaciones. Estas recomendaciones deben incluir al cableado asociado con los APs. A causa de esto se necesita algo de conocimiento sobre cableado. Algunos de los problemas con respecto al cableado serán tratados para una percepción general de los ítems con los que se trabajará durante el estudio.

What Should a Network Map Include?

Regardless of the tools used to develop a network map, the goal should be to develop, or obtain, a map that includes the following:

- Geographical information, such as countries, states or provinces, cities, and campuses
- WAN connections between countries, states, and cities
- Buildings and floors, and possibly rooms or cubicles
- WAN and LAN connections between buildings and between campuses
- An indication of the data-link layer technology for WANs and LANs such as Frame Relay, ISDN, 10-Mbps or 100-Mbps Ethernet, and Token Ring
- The name of the service provider for WANs
- The location of routers and switches, though not necessarily hubs
- The location and reach of any Virtual Private Networks (VPNs) that connect corporate sites via a service provider's WAN
- The location of major servers or server farms
- The location of mainframes
- The location of major network-management stations
- The location and reach of any virtual LANs (VLANs). If the drawing is in color, all devices and segments within a particular VLAN can be shown in a specific color.
- The topology of any firewall security systems
- The location of any dial-in and dial-out systems
- Some indication of where workstations reside, though not necessarily the explicit location of each workstation
- A depiction of the logical topology or architecture of the network

Figura 1

La regla número uno del diseño de la parte del cableado de las WLANs es evitar la creación de un peligro de incendio. Esto requiere diseñar que el cable se extienda correctamente. El usuario puede elegir ignorar las recomendaciones de cableado. Es por esto que es necesario una documentación precisa. En el futuro podría ser necesario tener pruebas para demostrar que el cableado instalado no es el mismo que el cableado recomendado. Sin la documentación apropiada, esto será muy difícil de probar. Sin embargo, si se diseña un sistema con fallas y se instala de acuerdo a las recomendaciones del SE, éste sería el responsable.

Elements that must be sufficient to support the design:

- Air conditioning
- Heating
- Ventilation
- Power
- Protection from electromagnetic interference
- Clear paths for wireless transmission and an absence of confusing reflecting surfaces
- Space for the following:
 - Cabling, or conduits
 - Patch panels
 - Equipment racks
 - Work areas for technicians installing and troubleshooting equipment

Figura 2

Cuando investigue el cableado, preste atención a los problemas ambientales como el cableado que correrá cerca de arroyos que podrían anegarse, vías de tren y autopistas donde el tráfico podría empujar los cables, o áreas de construcción e industriales donde equipo pesado o excavadoras podrían romper los cables. Dentro de edificios, preste atención a los problemas de arquitectura que podrían afectar la factibilidad de implementar el diseño de la red. Asegúrese de que los elementos arquitectónicos detallados en la Figura 2 son suficientes para soportar el diseño.

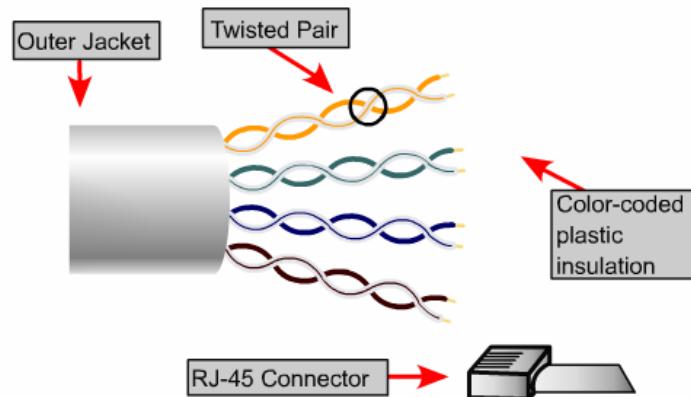
10.1.4 Medios de la LAN

Examine los tipos de medios que forman la red. Es muy probable que el usuario utilice algún tipo de cableado UTP de cobre para la mayoría de los casos. El cobre puede ser extendido hasta una distancia máxima de 100 m (328 pies) sin un repetidor o hub. La fibra puede ser extendida por kilómetros si fuera necesario.

Algunas instalaciones utilizan cableado de fibra. La mayoría de estos sitios utilizan una combinación de fibra y cobre. La fibra actúa como el backbone principal de la red y el cobre se extiende hasta el escritorio. Si las instalaciones utilizan cableado de fibra en toda su extensión, asegúrese de avisar al usuario que los APs sólo proporcionan conexiones RJ-45 y que será necesario un transceptor de medios para cada uno de los APs. Los transceptores de medios necesarios pueden representar un costo significativo.

El cable usado con más frecuencia para las redes modernas es el de Categoría 5 (Cat 5), mostrado en la Figura 1, par trenzado sin blindaje (UTP). El cable Categoría 5 consiste en ocho alambres de cobre, agrupados en pares. El cable UTP Categoría 5 puede ser extendido hasta una distancia máxima de 100 m (328 pies). El cable Categoría 5 está disponible en pleno y no pleno. La construcción del edificio, además de los códigos de construcción locales y estatales, determinarán el tipo de cableado que se debe utilizar. El pleno es el espacio entre el cielo raso de placas flotantes y el verdadero techo. En un entorno de pleno, este espacio es usado para la renovación del aire. En el caso de un incendio, la cubierta de PVC puede derretirse y producir humo tóxico.

Unsheilded Twisted Pair (UTP)



- Speed and throughput: 10-100 Mbps
- Average \$ per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m (short)

Figura 1

Ya que algunos cables de red son extendidos tradicionalmente en el pleno, los humos tóxicos estarán circulando entonces por todo el edificio. Por lo tanto, el cable de pleno debe ser usado en estas instalaciones. Todos los otros equipos instalados, incluyendo APs, también deben tener categoría de pleno. Los cables de pleno tienen una cobertura diferente que no se derretirá tan fácilmente y no producirá humo tóxico. Los cables de pleno se identifican fácilmente. La cubierta del cable de pleno es mucho más dura y rígida para trabajar que el cable Categoría 5 estándar. El cable también estará marcado con un código. CMP, por ejemplo, indica que es un cable sin blindaje clasificado como pleno.

Una forma fácil de identificar un entorno de pleno son placas suspendidas de cielo raso, una falta de aislamiento por encima de las placas del cielo raso y firewalls [cortafuegos]. Algunos códigos de edificación locales y estatales requieren cables de pleno sin importar el entorno. Un entorno de no pleno es donde el retorno del aire es conducido por tuberías. Cuando el retorno del aire es conducido por tubos hay muy pocas posibilidades de que los humos tóxicos puedan propagarse en el caso de un incendio.

En este tipo de entornos puede ser conveniente usar un cableado tipo PVC de propósito general. Algunas características de los entornos de no pleno son abundancia de tuberías por encima de las placas del cielo

raso, falta de firewall y un aislamiento por encima de las placas del cielo raso. Estos cables también tendrán códigos de identificación. CM, por ejemplo, indica que es un cable sin blindaje de no pleno.

10.1.5 Firewalls, conductores verticales, rutas de los cables y bucles de servicio

Firewalls

Como se muestra en la Figura 1, los firewalls son fáciles de identificar, ya que por lo general son de concreto, de hormigón ligero o estructuras de ladrillos que se extienden por todo el ancho de una habitación o corredor, desde el piso hasta el techo. No hay fisuras en los firewalls. Los firewalls están diseñados para contener un incendio en un área específica actuando como una barrera. Si es necesario atravesar un firewall, hay procedimientos para penetrar la pared. Estos procedimientos deben cumplir con el Código Eléctrico Nacional (NEC). Se puede obtener una copia del NEC con los proveedores de suministros eléctricos locales.

- Easily identified
- Act as barriers to contain fires
- Standards for penetrating firewalls

Figura 1

Por esta razón es importante hacer una nota en el reporte del estudio acerca de cualquier área donde un diseño tendrá que penetrar un firewall. Otra razón para hacer una nota sobre firewalls es que ellos afectarán a la señal RF. Muchas instalaciones tienen firewalls con entradas. Las puertas están construidas especialmente y selladas para resistir un incendio durante un tiempo específico. Estas puertas no son fáciles de identificar, salvo por su construcción pesada. Incluso pueden parecer estar hechas de madera. Si se cree que un conjunto de puertas es parte de un firewall, reviselas para estar seguro. Si las puertas son parte de un firewall, realice el estudio con las puertas cerradas. Las puertas cerradas tendrán un efecto en la cobertura. No suponga que las puertas siempre estarán abiertas sólo porque están abiertas durante el estudio.

Conductores verticales

Los conductores verticales a menudo reciben el nombre de armarios de cableado. Los conductores verticales son las áreas del edificio donde el cableado, la tubería y la plomería pueden correr de un piso al otro. A menudo se apilan uno sobre otro, facilitando la instalación de cables hasta la altura del edificio. Las cuatro paredes de un conductor vertical, además del piso y el techo, actúan como firewalls. Es importante anotar la ubicación de los conductores verticales. Al igual que con los firewalls, los conductores verticales requieren penetraciones que cumplan con los estándares NEC y necesitarán equipo de clasificación pleno.

Rutas de los cables

Siempre diseñe y mida los cables en rutas rectas. Si un cable que corre de norte a sur necesita ser extendido en una dirección diferente, siempre realice un giro de 90 grados. No extienda el cable en ángulo. Nunca mida la distancia desde un punto de conectividad de la red hasta el AP con una línea recta. Si la distancia se mide en forma incorrecta y el usuario le da el reporte a un contratista local para un presupuesto, éste puede resultar erróneo. Además, la extensión del cable puede ser mayor que la anticipada y puede necesitar un tipo diferente de cableado.

Bucle de servicio

Calcule un bucle de servicio en cada extremo de la extensión del cable. Los bucles de servicio son normalmente de 3 m (10 pies) de largo. Este bucle le da al contratista un poco de cable extra en caso de que deba ser terminado numerosas veces.

Cable extra

Un 15 por ciento de cable extra normalmente es suficiente para asegurar que habrá bastante cable para extender alrededor de objetos no previstos. Anote el porcentaje de cable extra estimado en el reporte. De lo contrario, el contratista puede determinar cuánto cable agregar y decidir que la extensión se saldrá de la especificación.

10.1.6 Infraestructura de LAN

Sistemas operativos y protocolos

Consulte con el representante de IT acerca del sistema operativo para los clientes y los servidores. Pregunte cuáles protocolos están siendo usados en la red.  Además, pregunte cuáles protocolos serán enviados por la WLAN. Los protocolos que no serán usados en la WLAN pueden necesitar ser filtrados para reducir el tráfico inalámbrico innecesario. Asegúrese de que el usuario sepa que no se soportarán todos los sistemas operativos.

- Find out what operating systems are used on servers and clients
- Find out what protocols need to go over the WLAN
- Not all O/S have supporting drivers yet

Figura 1

Switches y hubs

Mientras investiga la topología y los medios de la red, examine sus componentes. Los hubs pueden ser de 10 Mbps, 100 Mbps o 10/100. Los APs Cisco Aironet tienen puertos auto sensitivos de 10/100, y funcionarán en cualquiera de los dos modos. Siempre que sea posible, trate de conectarse usando un puerto de 100 Mbps de capacidad. Muchas personas no conocen estas capacidades y por lo tanto tratarán de usar switches de la misma forma en que se usaría un hub. La creencia es que todos los dispositivos conectados al switch podrán comunicarse. Este puede no ser el caso, dependiendo de la configuración predeterminada del switch. Si el usuario utiliza switches, averigüe cómo están configurados. Los switches tienen la capacidad de hacer que cada puerto represente una LAN virtual (VLAN). Las VLANs pueden agruparse entre sí para formar VLANs más grandes. Los switches pueden detener a los paquetes de broadcast. Sin embargo, no pueden detener a los frames de broadcast. Los switches no están diseñados para manipular usuarios móviles. Los APs Cisco Aironet están configurados para trabajar con switches. Cuando un cliente pasa del AP1 al AP2, el AP2 envía un paquete multicast con la dirección origen del cliente móvil. El AP luego envía este paquete para el cliente, que actualiza la Memoria Direccional de Contenidos (CAM) en el switch. El AP1 puede luego enviar cualquier paquete que tenga desde el cliente hacia el AP2.

La aplicación del usuario puede no estar configurada para manipular una red conmutada. La aplicación puede enviar paquetes de broadcast. Si el cliente está conectando a un AP que no está en la misma VLAN que el servidor, los paquetes de broadcast nunca podrán llegar a su destino. Esto puede variar dependiendo de la configuración del switch y de la configuración de la red.

Una solución potencial a este problema es formar una VLAN agrupando los puertos con APs conectados a ellos y el puerto que el host está usando. Sin embargo, esta solución puede no funcionar para todos los usuarios. Otra solución potencial es poner en red a todos los APs con el mismo hub que utiliza el host. Las limitaciones de distancia de los cables pueden dificultar esto. Una solución posible más es poner en red a todos los APs por medio de hubs y tenerlos conectados al mismo hub que utiliza el host. Sin embargo, esta no es una opción viable si el host es remoto.

Algunos hubs pueden parecer switches. Recuerde que un hub es un repetidor multipuerto. Todo el tráfico de Capa 1 y Capa 2 será propagado hacia y desde un AP. El AP, el hub y cualquier dispositivo que esté conectado directamente verá todo el tráfico. Sin embargo, es mejor conectar un AP o un bridge inalámbrico a un switch. Si se necesita control de broadcast de Capa 3, entonces se debería usar un router para conectar la WLAN con la LAN cableada.

Algunos switches Cisco pueden proporcionar energía al AP o al bridge por medio de Ethernet. Las redes que utilizan teléfonos IP Cisco es muy probable que tengan switches alimentados en su lugar. Los switches alimentados o los Módulos Inyectores de Energía Cisco Aironet ayudan a eliminar la necesidad de colocar una fuente de energía AC separada para el AP o el bridge.

Routers

Los routers presentan muchos de los desafíos de los switches. Al igual que los switches, los routers no pasan paquetes de broadcast. Como antes, esto puede presentar un problema para la aplicación o para los clientes que tratan de usar el Protocolo de Configuración Dinámica de Host (DHCP). Los routers también

pueden indicar que intentan usar un host remoto. Si este es el caso, puede ser necesario ingresar una ruta estática en el router.

10.1.7 Control de la salud de la red existente

The network health checklist is generic in nature and documents a best-case scenario. The thresholds might not apply to all networks.

The network health checklist includes:

- The network topology and physical infrastructure are well documented.
- Network addresses and names are assigned in a structured manner and are well documented.
- Network wiring is installed in a structured manner and is well labeled.
- Network wiring between telecommunications closets and end stations is generally no more than 100 meters.
- Network availability meets current customer goals.
- Network security meets current customer goals.
- No shared Ethernet segments are becoming saturated, 50 percent average network utilization in a 10-minute window.
- No shared Token Ring segments are becoming saturated, 70 percent average network utilization in a 10-minute window.
- No shared FDDI segments are becoming saturated, 70 percent average network utilization in a 10-minute window.
- No WAN links are becoming saturated, 70 percent average network utilization in a 10-minute window.
- No segments have more than one CRC error per million bytes of data
- On Ethernet segments, fewer than 0.1 percent of packets are collisions. There are no late collisions.
- On Token Ring segments, fewer than 0.1 percent of packets are soft errors not related to ring insertion. There are no beacon frames.
- Broadcast traffic is less than 20 percent of all traffic on each network segment, some networks are more sensitive to broadcast traffic and should use a 10 percent threshold.
- Wherever possible, frame sizes have been optimized to be as large as possible for the data-link layer in use.
- No routers are overutilized, five minute CPU utilization is under 75 percent
- On an average, routers are not dropping more than 1 percent of packets, for networks that are intentionally oversubscribed to keep costs low, a higher threshold can be used.

Figura 1

El estudio del rendimiento de la red existente proporciona una medición de referencia con la cual comparar el rendimiento de la nueva red. Las mediciones de la red actual pueden ser usadas para mostrar al usuario cuánto mejor trabaja la nueva red después de que el diseño ha sido implementado. Cualquier problema existente también debería ser documentado. Si el usuario intenta culpar por estos problemas a la nueva instalación, la documentación será de ayuda.

Como el rendimiento de los segmentos de la red existente afectará al rendimiento general, es importante estudiar sus rendimientos para determinar cómo cumplir los objetivos de rendimiento general de la red. Si una red es demasiado grande como para estudiar todos los segmentos, entonces analice los segmentos que interoperarán más con el nuevo diseño de red. Preste particular atención a las redes backbone y a las redes que conectan áreas viejas y nuevas.

En algunos casos, los objetivos de un usuario pueden tener conflicto con el rendimiento mejorado de la red. Por ejemplo, el usuario puede desear reducir los costos y no se preocupa por el rendimiento de la red. En este caso, la documentación del rendimiento original probará que la red no fue optimizada por razones de costo, y que el nuevo diseño no ha empeorado el rendimiento.

El análisis de una red existente puede ser usado para identificar sistemas heredados que deben ser incorporados a un nuevo diseño. A veces los usuarios no conocen el hecho de que protocolos antiguos aun corren en sus redes. Al capturar tráfico de red con un analizador de protocolos como parte del análisis de

referencia, los protocolos que corren en la red pueden ser identificados sin tener que depender del conocimiento del usuario.

10.1.8 Referencia de rendimiento de la red

Los desafíos de desarrollar una referencia del rendimiento de la red

El desarrollo de una referencia precisa del rendimiento de la red no es una tarea fácil. Un aspecto desafiante es determinar cuánto tiempo se necesita para realizar el análisis. Es importante asignar varios días para asegurar una referencia precisa. Si las mediciones se realizan durante un período corto, los errores temporales pueden parecer más significativos de lo que son en realidad.

Además de asignar suficiente tiempo para un análisis de referencia, también es importante establecer un período durante el cual realizar el análisis. Una referencia de rendimiento normal no debería incluir problemas no típicos causados por cargas de tráfico excepcionalmente grandes. Por ejemplo, el procesamiento de las ventas de final de temporada puede colocar una carga anormal en la red de una compañía. En un entorno de venta minorista, el tráfico de la red puede aumentar cinco veces cerca de ciertas fechas. El tráfico de red hacia un servidor web puede aumentar inesperadamente tanto como diez veces si el sitio web se enlaza con otros sitios populares o si aparece listado en motores de búsqueda.

En general los errores, la pérdida de paquetes, la pérdida de células y la latencia aumentan junto con la carga de la red. Para obtener una medición significativa de la precisión y retardo típicos, realice el análisis de referencia durante períodos de carga normal del tráfico. Sin embargo, si el objetivo principal del usuario es mejorar el rendimiento durante la carga pico, entonces asegúrese de estudiar el rendimiento durante la carga pico. La decisión de medir el rendimiento normal, el rendimiento durante la carga pico o ambos, depende de los objetivos del diseño de la red.

Algunos usuarios no reconocen el valor del estudio de la red existente antes de diseñar e implementar las mejoras. Las expectativas del usuario por una propuesta de diseño rápida puede dificultar el tomar tiempo para desarrollar una referencia de rendimiento sobre la red existente. Además, las otras tareas y objetivos de un SE podrían hacer que sea impráctico pasar días desarrollando una referencia precisa.

Un buen conocimiento de los objetivos técnicos y de negocios del usuario puede ser útil para determinar cuán minucioso debería ser el estudio. Las charlas con el usuario sobre los objetivos del negocio pueden ayudar a identificar segmentos importantes a estudiar, que transportan tráfico crítico y de backbone. Pídale al usuario que lo ayude a identificar los segmentos típicos desde los cuales podrá sacar conclusiones acerca de otros segmentos.

10.2 Estudio

10.2.1 Preparativos

Después de realizar todo el trabajo de preparación necesario para realizar un estudio del sitio, es tiempo de comenzar realmente con el estudio. Antes de llegar al sitio, asegúrese de que todo el equipo esté configurado, en funcionamiento y listo para el estudio. La Figura 1 ilustra los pasos básicos a realizar en la preparación de un estudio del sitio.

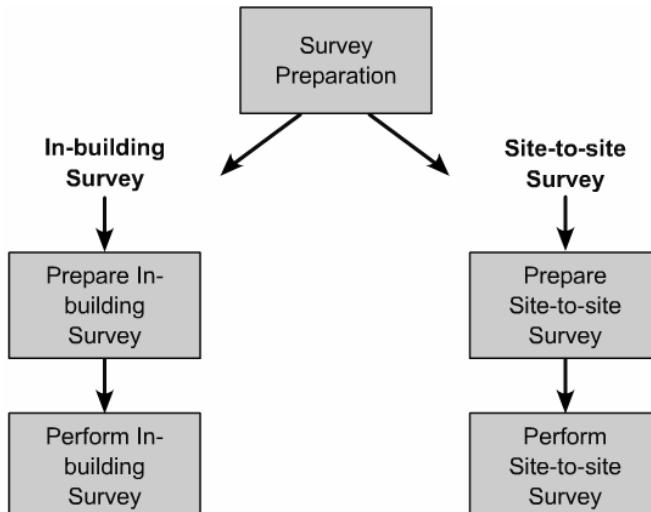


Figura 1

Estudio dentro del edificio

Llame antes para averiguar si se necesitará un elevador de tijera para llegar al cielo raso. Si es así, averigüe si el usuario proveerá el elevador o no. Si fuera necesario, asegúrese de que el equipo apropiado y el operador autorizado han sido obtenidos.

Estudio sitio a sitio

Si el estudio es para una WLAN sitio a sitio con una distancia de varios kilómetros, o millas, probablemente será necesario acceder al techo. Además, asegúrese de que esté disponible un analizador de espectro. Las antenas montadas en edificios son mucho más costosas que las instalaciones de interiores. Las monturas de edificio o de techo, la energía, el hardware, los pararrayos, el cable coaxial, los accesorios y los sistemas de varillas de pararrayos son caros. La instalación eléctrica y de tierra debería ser hecha sólo por un profesional autorizado, lo que se sumará al costo. En muchas áreas también se necesitará un permiso de construcción para instalar la antena. La protección legal y la cobertura proporcionadas por un contratista respetable son aun más importantes que seguir los códigos de construcción, las regulaciones y los requisitos de autorizaciones. Cualquier intento por reducir costos durante este proceso puede dar por resultado la pérdida eventual de mucho dinero y credibilidad en un juicio.

Al probar la ruta de línea de visión [line-of-sight (LOS)], tanto visualmente como con un analizador de espectro RF, se evita al inicio el error costoso de tener que reubicar la antena. Recuerde que las WLANs utilizan la banda no licenciada de 2,4 GHz y no hay garantías de que la interferencia no se convierta en un problema en el futuro. Asegúrese de explicar y documentar esto como una protección legal y para conocimiento del usuario. Si es posible, realice esta prueba durante varios días a diferentes horas en el día. Si el usuario depende de un enlace confiable durante la mitad de la noche, entonces se debería realizar un estudio a esa hora, si es posible.

Si los sitios están separados por unos pocos kilómetros, o millas, entonces puede ser necesaria una torre en uno o en ambos extremos de la ruta. Puede ser necesaria una grúa equipada con una canasta para simular una torre y controlar que la LOS no tenga obstáculos ni interferencias RF. Esto puede volverse bastante costoso y llevar mucho tiempo, aun si el equipo es alquilado. Recuerde alquilar una grúa que alcance la altura deseada y siempre planifique de antemano reservar el equipo. En este punto probablemente será necesario un grupo de personas para que a varios kilómetros, o millas, puedan trabajar juntos para establecer y probar la calidad del enlace. También es importante tener teléfonos celulares o dispositivos de comunicación disponibles para los esfuerzos de coordinación.

Pocos errores podrían ser más costosos que erigir una torre de 45,7 m (150 pies) para descubrir más tarde que la interferencia RF ha destruido parcialmente o por completo la calidad del enlace. La torre podría fácilmente haber sido reubicada a varios metros, o pies, para evitar el problema.

Cambie todas las pilas y baterías la noche anterior al estudio planeado. Esto incluye al elevador tijera si es operado con batería. Asegúrese de que todo el equipo esté listo para ser usado.

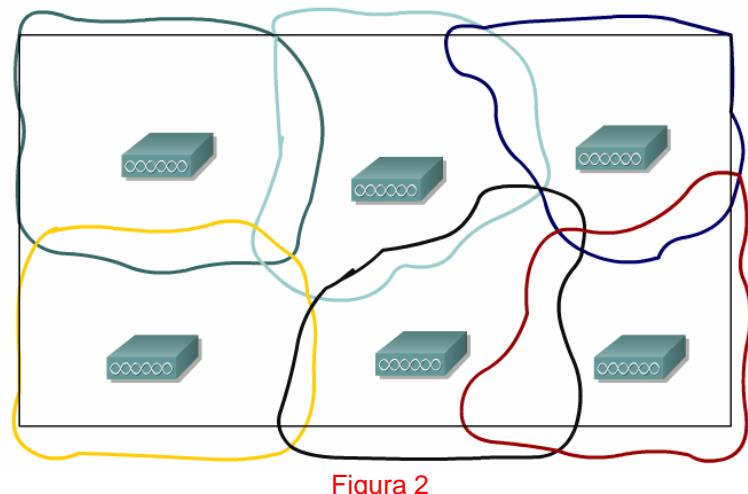
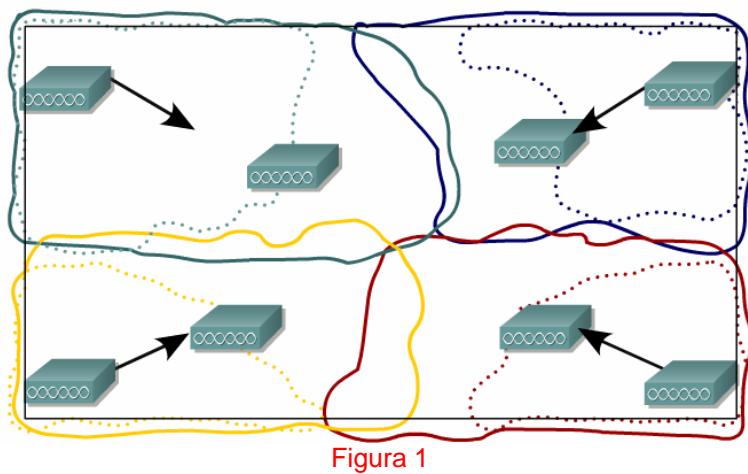
10.2.2 Primeros pasos

La forma más fácil de comenzar un estudio del sitio es tomar un área de las instalaciones que necesite cobertura. Elija un rincón y coloque el AP allí  1. Estudie la cobertura de ese AP y tome nota de dónde está el punto de cobertura más lejano al AP. Luego mueva el AP a ese punto. Si el AP fue colocado en una esquina, se perderá tanto como el 75 por ciento de la célula de cobertura al cubrir un área fuera del edificio que no necesita cobertura.

Después de que el AP ha sido movido, estudie la cobertura del AP. Puede ser necesario mover el AP varias veces para encontrar la mejor ubicación. Después de determinar la mejor ubicación para el AP, muévase hacia una esquina diferente de las instalaciones y repita el proceso. En un depósito simple como el mostrado en la Figura, el proceso se repetiría cuatro veces. El estudio de la cobertura RF estaría entonces completo.

En un estudio más avanzado, el repetir el proceso cuatro veces sólo proveerá cobertura alrededor del perímetro de las instalaciones. Después se deberían llenar todos los huecos. Este proceso requiere experiencia y criterio. Algunos SEs pueden elegir estudiar el perímetro y luego llenar el centro. Recuerde que si se necesita una cobertura sin fisuras, las células de cobertura se deben superponer  2.

En un estudio estándar, 15 por ciento de superposición es normalmente suficiente para proporcionar una transferencia suave y transparente. Si pretende usar repetidores, entonces éstos necesitarán tener un 50 por ciento de superposición con un AP cableado.



Otro enfoque es estudiar los primeros dos APs y determinar sus áreas de cobertura 3. Luego coloque un AP en el borde de la primera célula del AP, y estudie la cobertura. Aleje el AP más aún para utilizar la célula completa. Esto permite tener un conocimiento aproximado del tamaño de la célula. Estudie la nueva ubicación para determinar la factibilidad y ajuste si fuera necesario. Después de que la ubicación del AP ha sido decidida, el SE continúa este proceso hasta que las instalaciones completas estén cubiertas.

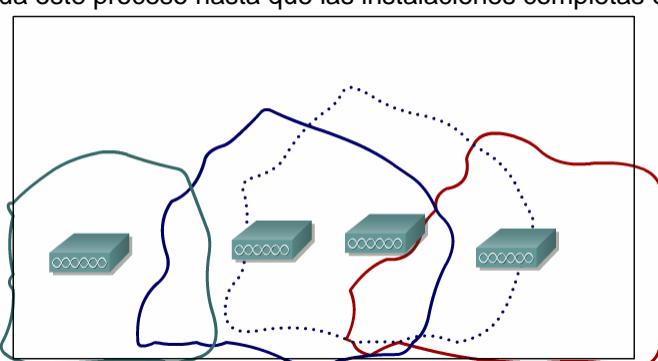


Figura 3

10.2.3 Selección del canal, velocidades de datos y superposición

Cuando esté realizando el estudio, recuerde que sólo hay tres canales que no se superponen para 802.11b 1. Para maximizar la velocidad de datos, utilice estos canales. El uso de canales que no se superponen asegura que los APs no interferirán entre sí.

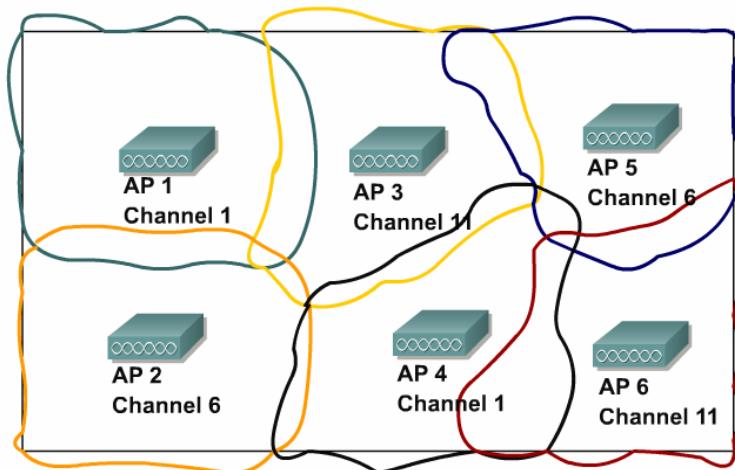


Figura 1

Cuando diseñe la WLAN, realice el estudio usando el canal sobre el cual el AP trabajará. Una prueba de interferencia es necesaria como parte del estudio. Si cada AP es estudiado usando el mismo canal, y no el canal real que el AP estará usando, no hay certeza que de no exista interferencia en el canal que el AP realmente estará usando. Después de determinar la velocidad de datos mínima que el usuario utilizará, realice el estudio en esa velocidad de datos [2](#).

La velocidad de datos elegida afectará drásticamente a los resultados del estudio del sitio. En el ejemplo de la Figura [2](#), el mismo depósito es estudiado a dos velocidades de datos diferentes. Si seis APs son necesarios para cubrir las instalaciones a 2 Mbps, se necesitarán doce APs para que lo hagan a 5,5 Mbps.

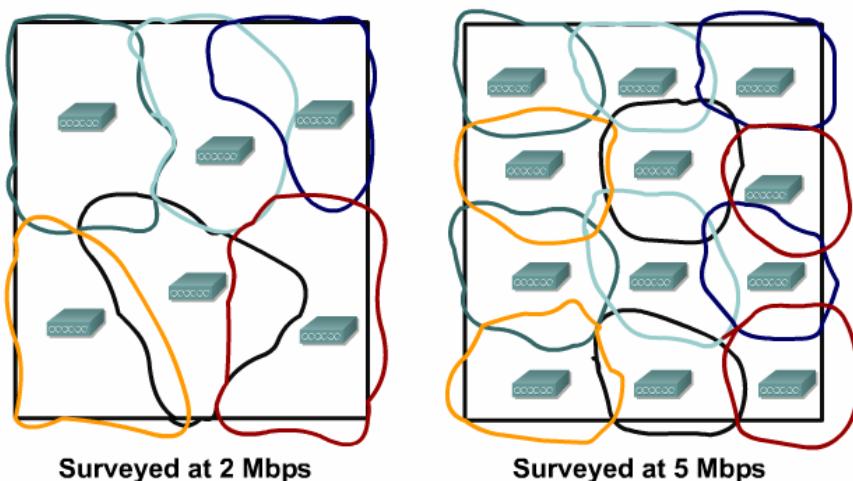


Figura 2

Es importante conocer las necesidades del usuario. Si un estudio es terminado con la velocidad de datos incorrecta y el usuario instala la WLAN, la conexión puede que sólo funcione en ciertas áreas, o puede no funcionar en absoluto.

Si hay demasiada superposición, el ingeniero inalámbrico puede encontrar una situación donde un AP adicional puede proporcionar demasiada cobertura, pero la cantidad actual de APs proporciona muy poca cobertura [3](#). El ingeniero puede resolver esto de diversas formas. La primera opción es usar una antena diferente para obtener más cobertura de los APs. La segunda opción es usar antenas más pequeñas y agregar más APs. Otra posibilidad es cambiar los niveles de potencia en uno o más de los APs para cambiar el tamaño de las células de cobertura. La opción final es usar una combinación de estas opciones para obtener la cobertura necesaria.

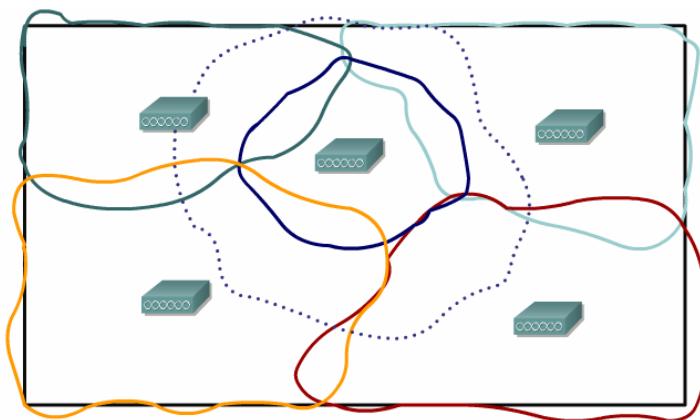


Figura 3

Este proceso es de prueba y error. Por lo tanto, la experiencia juega un rol vital. Los estudios del sitio a menudo son como rompecabezas. A veces los individuos están tan seguros de que han descubierto la mejor solución que no ven las otras soluciones posibles. Siempre que sea posible, pregunte a otros ingenieros inalámbricos por sus estudios. Se pueden encontrar soluciones creativas que pueden ser implementadas en diseños futuros.

A veces un ingeniero estudiará unos pocos APs, sólo para descubrir que el plan propuesto no funcionará. En lugar de comenzar el proceso desde el principio, un ingeniero puede intentar una serie de opciones para encontrar la última pieza del rompecabezas.

A veces los problemas del estudio del sitio se deben a frustración o pereza. Un ingeniero podría enfocarse en una solución para evitar tener que comenzar el estudio de nuevo. En esta situación, es mejor tomar un descanso del trabajo. Este es un buen momento para ir por una taza de café, revisar el correo o ir a comer. La mejor solución a menudo se presenta sola después de este tipo de descanso. Si no sucede así, puede ser necesario comenzar de nuevo. Puede haber puntos problemáticos que fueron pasados por alto la primera vez. Cuando termine el estudio por segunda vez, estos puntos problemáticos serán evidentes y podrán ser tenidos en cuenta cuando se planifique el nuevo diseño de los APs. Siempre es mejor comenzar el estudio de nuevo y diseñar la WLAN correctamente que tratar de forzar una solución o usar una solución que puede no proporcionar la mejor cobertura.

10.2.4 Trabajo en las condiciones existentes

Cuando sea posible, trabaje con las condiciones y el diseño existentes. Puede haber veces en que la ubicación de los APs sea dictada por la conectividad de red disponible. Por ejemplo, el cobre tiene un límite de longitud de 100 m (328 pies). Cualquiera sea el problema, casi siempre hay una forma de corregirlo. En la Figura 1, la conectividad de red en el depósito sólo está disponible a lo largo de una pared. El depósito está lleno de estanterías que crean pasillos largos y angostos.

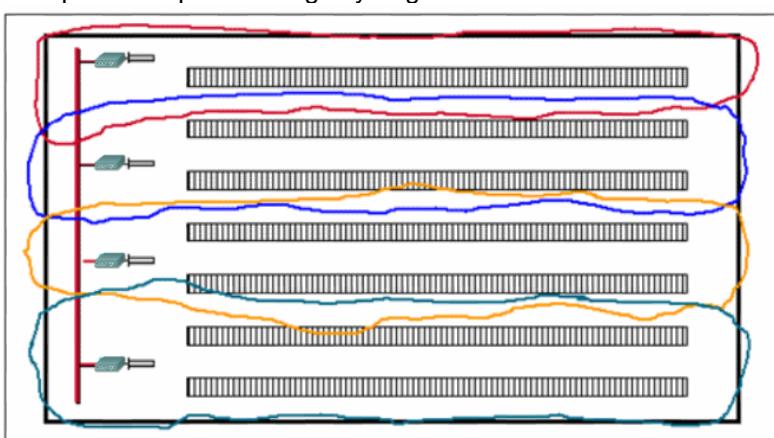


Figura 1

Una buena solución para este depósito puede ser ubicar los APs a lo largo de la pared donde pueden ser conectados a la red. Las antenas Yagi podrían ser colocadas en los pasillos, cubriendo un pasillo y parte de otros dos pasillos. La cobertura podría estar superpuesta para cubrir el depósito completo. La señal puede

rebocar contra las paredes de metal en el extremo lejano del depósito y llenar los puntos muertos creados por las estanterías.

A veces habrá áreas dentro de un sitio que no pueden ser cubiertas. La Figura 2 muestra una habitación de radiología en un hospital. La Sala de Emergencias [Emergency Room (ER)] que lo rodea está cubierta. La ER tiene cielos rasos de placas colgantes, paredes de yeso, un piso de placas de linóleo y presenta muy poco desafío.

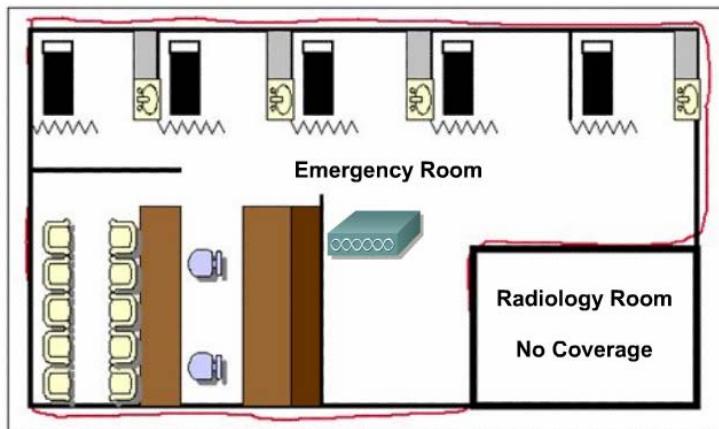


Figura 2

Un paciente puede ser traído a la sala de radiología y recibir rayos x allí. Sin embargo, la sala de radiología tiene pesadas puertas de madera, un cielo raso de placas duras, paredes de concreto y un piso de concreto vertido que están revestidos de plomo para proteger a la ER.

En el ejemplo de la Figura 2, no hay cobertura en la habitación de radiología. La habitación de radiología está diseñada para ser extremadamente estéril y la administración del hospital no quería cables y APs expuestos en la sala de traumatismos. A causa de esto, la aplicación del hospital fue rediseñada para cubrir la desconexión ocasional. La aplicación fue cambiada para que durante los períodos de desconexión el nodo almacene todos los datos como una unidad de trabajo por lotes, y luego envíe los datos una vez que la conectividad esté re establecida.

10.2.5 Congeladores

La Figura 1 muestra un ejemplo de un centro de distribución (CD). El CD almacena ítems perecederos. Diferentes áreas del CD se mantienen a diferentes temperaturas. Algunas de las áreas son congeladores con temperaturas tan bajas como -29 grados C (-20 grados F). La instalación de APs en áreas con temperaturas así de bajas puede requerir coberturas climatizadas costosas para proteger los APs. Una alternativa puede ser usar un divisor de antena. Al usar un divisor, el AP puede ser montado fuera del congelador con una antena que provea un área de cobertura afuera y otra antena que provea cobertura adentro del congelador. Más allá del ahorro de no tener que pagar la costosa cobertura climatizada, el usuario no tiene que pagar el costoso tiempo que llevaría instalar el cableado y la energía dentro del congelador. Instalar este tipo de equipo usando un traje para bajo cero y guantes pesados puede llevar bastante tiempo y ser muy costoso.

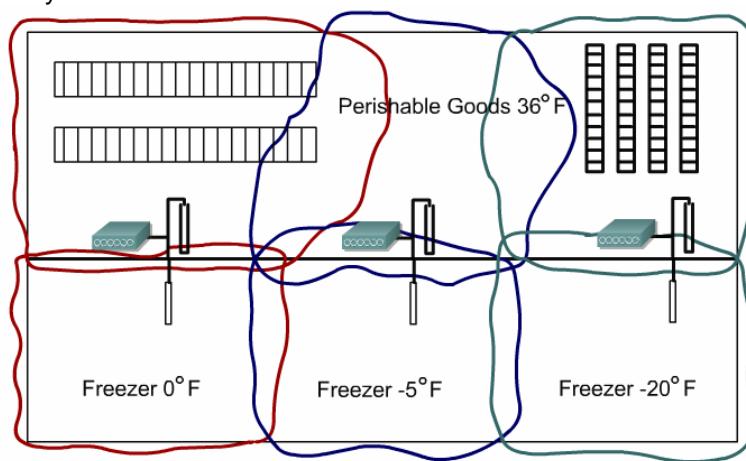


Figura 1

Diversidad de Antena

Cuando se utiliza diversidad de antena el AP usa una antena o la otra, pero nunca ambas. No intente conectar una antena a cada conector y colocar una adentro del congelador y la otra afuera. Esta no sería una solución efectiva. En los ejemplos de uso de divisores de antenas mostrados en la Figura 2, la característica de diversidad de antena debe estar desactivada. De lo contrario, serían necesarios dos divisores y cuatro antenas.

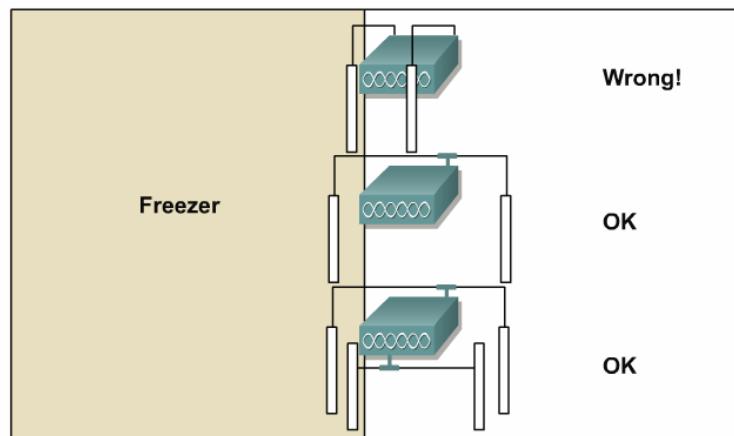


Figura 2

10.2.6 Estudio de múltiples pisos

Se necesita tener un cuidado especial cuando se estudian instalaciones con múltiples pisos. Los APs en los diferentes pisos pueden interferir entre sí tan fácilmente como los APs ubicados en el mismo piso. Es posible tomar ventaja de esto durante un estudio. Al usar antenas más grandes, puede ser posible penetrar pisos y techos y proporcionar una cobertura a los pisos por encima y por debajo del piso donde está montado el AP.

En la Figura 1, un complejo de oficinas de cuatro pisos necesita ser cubierto. Montar dos APs en cada piso sería costoso y podría presentar un problema con APs en el mismo canal superpuesto. El usar antenas patch en los APs resolvió el problema. Como la antena patch es semidireccional, hubo suficiente cobertura desde cada AP como para cubrir la mayor parte de un piso y una parte de los pisos por encima y por debajo de él. Al montar APs en pisos alternativos y en extremos opuestos del edificio, el SE pudo lograr la cobertura deseada con sólo cuatro APs.

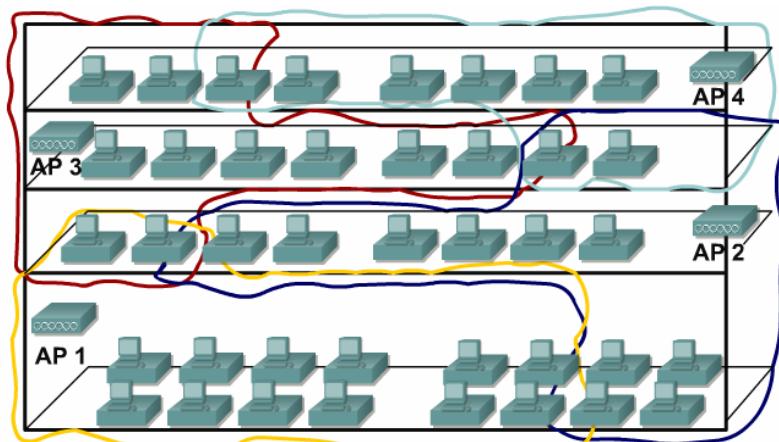


Figura 1

10.2.7 Interferencia y propagación de RF

Interferencia

Siempre monte las antenas en un área abierta para la mejor propagación de la señal. Evite objetos que puedan afectar la señal RF. Hay una cantidad de objetos que pueden causar interferencia. Algunos de los objetos que pueden tener un efecto negativo sobre una señal se muestran en la Figura 1.

Common sources of interference include the following:

- Cardboard
- Wood
- Paper
- Firewalls
- Electrical Transformers
- Microwave Ovens
- Fluorescent Lighting

Figura 1

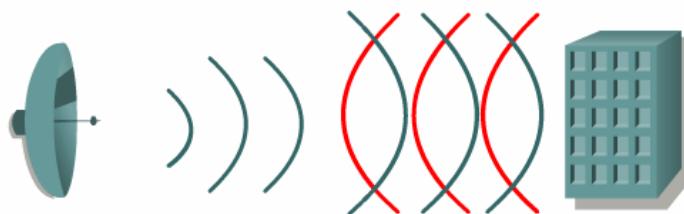
Evite las siguientes fuentes de Interferencia Electromagnética (EMI):

- Luces fluorescentes y sistemas de iluminación Fusion de 2,4 GHz
- Hornos de microondas
- Conductos de aire acondicionado
- Otros equipos de radio

Siempre intente montar el AP y las antenas tan lejos de estos ítems como sea posible.

Propagación de RF

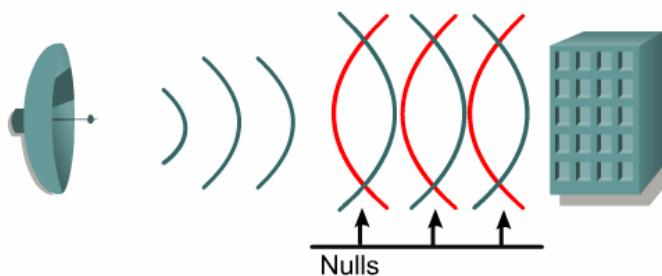
La propagación de RF se trató en el Módulo 3. Recuerde las características nombradas en las Figuras 2, 3 y 4 cuando realice un estudio del sitio.



Propagation has the following characteristics:

- Radio waves are reflected just like light waves
- Can reduce the reflected waves by using directional antennae

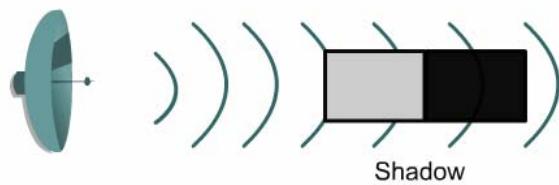
Figura 2



Nulls have the following characteristics:

- Waves 180 degrees out of phase will create a "null" or dead spot:
- Use diversity antennae to help overcome nulls:
- When using a single antennae, change the antennae location to overcome the null:

Figura 3



Diffraction and shadows can impact RF:

- If the RF wave is unable to pass through an object, it may suffer from diffraction
- Diffraction creates RF "shadows"

Figura 4

10.3 Montaje e Instalación

10.3.1 Montaje del AP

Después de decidir dónde serán montados los APs, el SE tendrá que decidir cómo serán montados. Al igual que con la montura del AP para un estudio del sitio, hay muchas formas de colgar el AP, y se pueden utilizar una variedad de recursos. Esta sección cubrirá la mayoría de los métodos comunes para montar APs y algunas de las preocupaciones asociadas con el montaje de un AP y de las antenas.

Algunos APs tienen dos orificios deslizables para el montaje **1**. Estos orificios pueden ser usados para cualquier superficie donde sea posible montar dos tornillos. Los tornillos en perforaciones del concreto serán bastante estables y deberán proveer una montura segura para el AP cuando estén colocados correctamente. Los muros de mampostería o la madera pueden ser menos seguros. Todos los APs deberían ser montados con un cuidado extra para garantizar la seguridad y el funcionamiento continuo del AP. Un montaje apropiado para el AP disminuye las posibilidades de tiempo caído. La pérdida de conectividad produce pérdida de tiempo para los trabajadores.



Considerations in Column Mounting

- Use heavy-duty zip ties to secure AP to column
- Do not cover AP lights with zip ties
- Mount "upside-down" so Ethernet indicator lights can be seen from the floor
- Label APs

Figura 1

Montaje en Columnas

Los soportes de montaje están disponibles de terceros **2**. Una solución más simple, pero menos segura es crear algún tipo de montura. Esto se puede realizar usando muchos de los mismos ítems llevados en una caja de herramienta para el estudio del sitio.

Cuando está montado en un poste o columna, el AP puede ser atado al poste o columna con abrazaderas plásticas de alta resistencia. Las abrazaderas plásticas de alta resistencia pueden ser tan anchas como 1,3 cm (0,5 pulgadas). Si utiliza estas abrazaderas, asegúrese de que las luces indicadoras en el AP no estén tapadas.

En el diagrama de la Figura 2, el AP está montado en lo que parece ser una posición invertida. Esta posición permite que las luces indicadoras para el puerto Ethernet se vean desde el piso.

Siempre que sea posible, los APs deberían ser etiquetados con el nombre, la dirección IP, el canal y el SSID. Las letras deben ser fácilmente legibles desde el piso en caso de que se necesite solucionar problemas del AP.

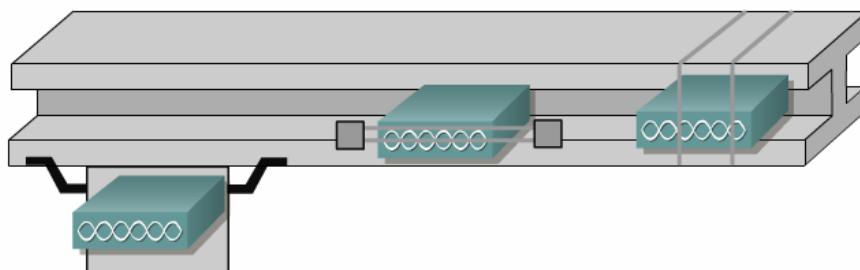
Si la columna es demasiado grande para las abrazaderas, otra opción es montar un pedazo pequeño de madera a la columna 3. Se puede hacer esto usando tornillos o pernos para asegurar la madera a la columna. Otra opción es usar silicona o pegamento para montar el tablero a la columna, como Liquid Nails.



Considerations in Using a Backing Board

- Mount 2x4 to column
- Use 2x4 as mounting base for AP
- Secure AP to 2x4 with zip ties

Figura 2



Considerations in Beam Mounting

- Zip ties
- 2x4 secured with beam clamps
- Mounting bracket secured with beam clamps
- Mount antenna in same position they were surveyed

Figura 3

Nota: No utilice el Liquid Nails para montar el AP directamente a la columna. En el caso de que el AP necesite ser quitado o reemplazado, normalmente será destruido.

Luego se monta el AP sobre la madera usando tornillos y se asegura usando abrazaderas. Si la madera se extiende más allá del ancho de la columna, las abrazaderas pueden ser colocadas alrededor de los extremos de la madera y a través de la cara del AP. De lo contrario puede ser necesario asegurar una base de montura para la abrazadera sobre el tablero. Si se utilizan bases de montura, asegúrese de sujetarlas al tablero usando un tornillo. No dependa de la cinta adhesiva en la parte inferior de la montura. El AP probablemente vivirá más que la cinta adhesiva. El uso de un pedazo de madera terciada es también bueno para cielos rasos y paredes de concreto.

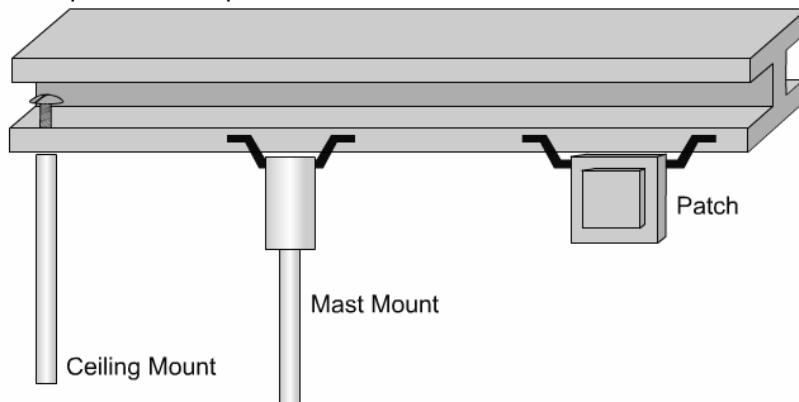
Cuando se monta sobre un tirante o viga, el AP puede ser asegurado al tirante o viga. En algunos casos, no es posible rodear con la abrazadera al tirante o viga. Si este es el caso, asegure la pieza de madera a la viga con abrazaderas de vigas. Otra opción es usar una abrazadera de vigas para asegurar una lámina de montura al tirante y luego se sujetan el AP a la lámina de montura.

Siempre asegúrese de que la madera esté montada con firmeza sobre la estructura antes de montar el AP. Si se realiza el estudio con antenas rubber ducky, asegúrese de estudiar con ellas en la misma posición en que serán montadas. En los ejemplos mostrados en esta sección, las antenas estarían apuntando hacia abajo. Hay diferentes patrones de cobertura por encima y por debajo de la antena. Si el estudio se realizó con la antena en una posición y luego se montan en otra posición, la cobertura puede ser diferente a lo esperado.

No Monte equipos sobre conductos eléctricos, de plomería o soportes de cielo raso. Esto es normalmente una violación al código. También podría haber una pérdida en la plomería, o temperaturas extremas en el caño. Los conductos podrían volverse electrificados en el caso de un cortocircuito, y el cableado eléctrico en el conducto es una buena fuente de EMI. Por lo tanto, el equipo debería ser montado tan lejos como sea posible de ellos.

10.3.2 Montaje de la antena

Cada AP tendrá una antena conectada a él. La mayoría de las antenas vienen con un soporte de montaje o está disponible como un opcional 1. El desafío es que la mayoría de las antenas están diseñadas para ser montadas en una determinada forma. Por ejemplo, una antena montada en mástil de 5,2 dBi está diseñada para ser montada sobre un mástil y es vendida con el hardware necesario. Para montar la antena sobre una viga doble T puede ser necesario un poco de ingenio. Están disponibles soportes separadores, pero no están diseñados para ser montados sobre una viga doble T. Algunos instaladores usan abrazaderas plásticas, abrazaderas de vigas o pernos para asegurar los soportes separadores a las vigas doble T y luego montar la antena en el soporte. La antena está pensada para uso externo y está diseñada para ser montada con la funda metálica en la parte inferior. Para uso interno, invierta la antena. Sea creativo. Los soportes modificados se pueden usar para una variedad de antenas.



Antenna Mounting

- Some antennas are not shipped with mounting brackets
- Modify brackets to meet installation requirements
- Modified brackets can be used with a variety of antennas
- Be creative

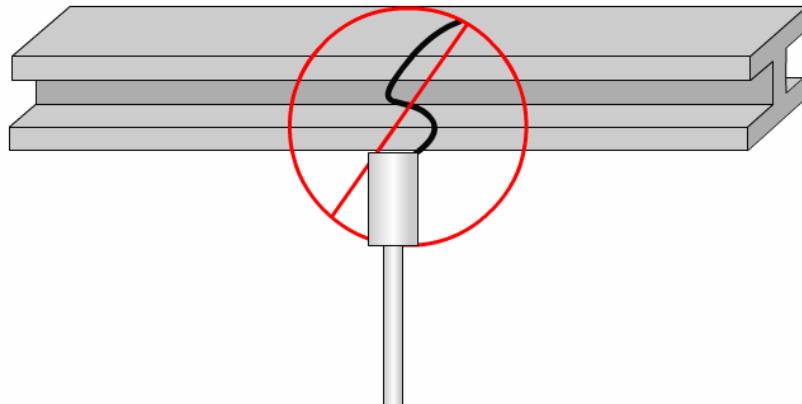
Figura 1

Al igual que con los APs, siempre asegúrese de que la antena tenga una montura segura y sólida 2. Asegúrese de que la antena colgará correctamente cuando sea montada a la base. Si el estudio fue realizado con la antena en posición vertical y está montada sobre una base insegura, puede colgar en un ángulo de 45 grados, lo que cambiaría el patrón de cobertura. No cuelgue las antenas por sus cables. El cable no está diseñado para esto y puede eventualmente cortarse o sufrir daño interno. El colgar las antenas por sus cables también cambiaría la célula de cobertura. Las antenas pueden balancearse cuando el aire acondicionado se enciende, lo que crearía una célula de cobertura móvil.

A veces las antenas pueden ser usadas o montadas en una forma inusual 3. En ciertas circunstancias, una antena Yagi o Patch montada muy alta y apuntada directamente al piso es la mejor solución. Si la antena necesita ser montada en una forma inusual, anótelo en el reporte. De lo contrario, puede ser que el

instalador no comprenda el intento y que monte la antena según sus especificaciones, lo que cambiaría el patrón de cobertura.

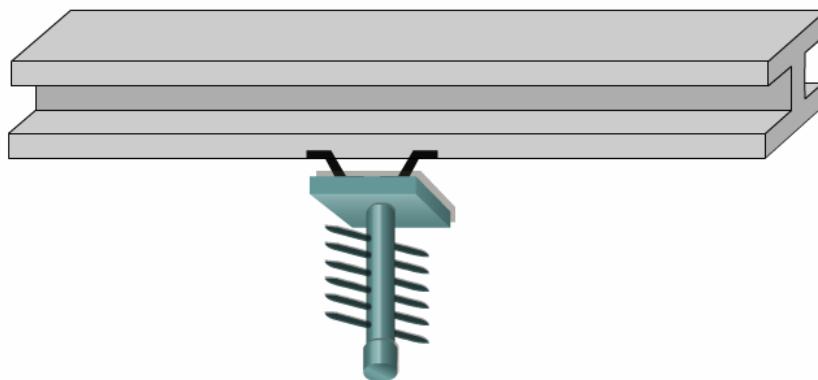
Cuando se monte una antena que se extienda a una sala, pasillo o área de trabajo, asegúrese de que no interferirá físicamente con los peatones o el tráfico vehicular.



Antenna Mounting

- Make sure that the antenna mount is solid and secure
- Do not hang antennas by their cable
- Cable can break or become damaged
- Antenna can sway and provide a "moving cell"

Figura 2



Antenna Mounting

- Sometimes antennas are mounted in unusual ways
- Specify in the report exactly how the antenna is mounted

Figura 3

10.3.3 Energía

Todos los APs requieren energía para funcionar. Coloque detalles en el reporte acerca de cómo y dónde se conectarán los APs al sistema eléctrico. Los APs deberían ser alimentados con un disyuntor de fuente de energía entrante las 24 horas. Esta fuente de energía puede ser compartida, pero se prefiere una fuente dedicada.

Hay diferentes tipos y marcas de equipos eléctricos. Un SE no necesita ser un experto en esto, pero debería poder identificarlos. Esto permitirá realizar referencias específicas en el reporte cuando detalle la fuente de energía para el AP. Por ejemplo, el reporte puede especificar que el AP 4 recibirá energía de una caja Square D en la pared norte del área de transporte, y que la distancia desde la caja eléctrica hasta el AP fue estimada en 44 m (145 pies).

Al definir la ubicación y la marca de la caja del disyuntor, el electricista podrá fácilmente identificar la caja e instalar el cableado asociado. El SE también debería estar familiarizado con los paneles de disyuntores para determinar si hay suficientes o si está lleno. Si una caja en particular es especificada para ser usada y no hay disyuntores disponibles, esto podría presentar un problema, en especial si el reporte se utiliza para generar un presupuesto para el trabajo eléctrico.

Las cajas eléctricas deberían ser montadas boca arriba para que el peso del transformador del AP pueda descansar sobre el frente. El transformador debería luego ser asegurado al frente o a la caja usando abrazaderas plásticas.

10.3.4 Gabinetes NEMA

A veces los APs están ubicados en áreas donde están sujetos a humedad y temperatura extremas, polvo y partículas. Estos APs pueden necesitar ser montados dentro de un gabinete sellado. La Asociación Nacional de Fabricantes de Electrónica [National Electronics Manufacturers Association (NEMA)] tiene un sistema de clasificación para estos gabinetes, que por lo general reciben el nombre de gabinetes NEMA [1](#). La clasificación se muestra en la Figura [2](#).

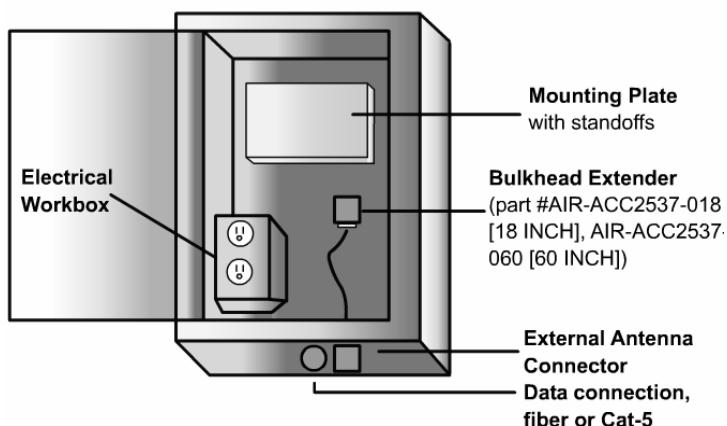


Figura 1

NEMA Rating System

- **Type 1** - Intended for indoor use primarily to provide a degree of protection against hand contact with enclosed equipment. This is usually a low cost enclosure and suitable for clean and dry environments.
- **Type 2** - Intended for indoor use primarily to provide a degree of protection against limited amounts of falling dirt and water.
- **Type 3** - Intended for outdoor use primarily to provide a degree of protection against windblown dust, rain, and sleet. This type is undamaged by ice that forms on the enclosure.
- **Type 3R** - Intended for outdoor use primarily to provide a degree of protection against falling rain and sleet. This type is undamaged by ice that forms on the enclosure.
- **Type 4** - Intended for indoor use primarily to provide a degree of protection against windblown dust and rain, splashing water, and hose directed water. This type is undamaged by ice that forms on the enclosure.
- **Type 4X** - Intended for indoor or outdoor use primarily to provide a degree of protection against corrosion, windblown dust and rain, splashing water, and hose directed water. This type is undamaged by ice that forms on the enclosure.
- **Type 6** - Intended for indoor or outdoor use, when occasional temporary submersion is needed.
- **Type 6P** - Intended for indoor or outdoor use, during which occasional prolonged submersion is encountered. This type includes corrosion protection
- **Type 12** - Intended for indoor use to provide a degree of protection against dust, falling dirt, and dripping non-corrosive liquids.
- **Type 13** - Intended for indoor use primarily to provide a degree of protection against dust, spraying of water, oil, and non-corrosive coolant.

Figura 2

Los gabinetes NEMA usados más a menudo para los productos de networking inalámbrico son Tipo 2, Tipo 4 y Tipo 4X. Algunas situaciones pueden requerir el Tipo 12 o 13. Estos tipos de gabinetes pueden ser adquiridos a través de almacenes de suministros eléctricos y ferreterías locales. Desafortunadamente, cuando se compran a través de estos tipos de negocios, los gabinetes NEMA no son más que una caja sellada. No hay conectores externos de antena, ni conectores externos de red, ni separadores de monturas internos, ni fuentes de energía internas.

Muy pocos gabinetes NEMA están disponibles en los negocios con una fuente de energía interna. Se puede montar un AP dentro del gabinete de la misma forma en que se monta un AP sin un gabinete. La energía tendrá que llegar al gabinete y se deberá instalar una caja eléctrica dentro de él. Una antena montada dentro de la caja no es muy efectiva, por lo que se deberá usar una antena externa. Para conectar una antena externa se necesitará una extensión de la mampara. Esto es simplemente un conector que se enchufa al AP dentro del gabinete y proporciona una conexión de antena en el exterior del gabinete. Asegúrese de que todos los orificios perforados en la caja estén sellados. Si queda aunque sea un orificio abierto, entonces la integridad del gabinete estará comprometida. Los conectores de antena deberían estar montados en la parte inferior del gabinete para proporcionar tanta protección como sea posible contra la condensación de humedad. También es una buena idea sellar la conexión de la antena con un producto como Coax Seal.

Los gabinetes NEMA prefabricados con conectores de antenas, soportes separadores y protectores contra picos están disponibles de terceros. Son más costosos que un gabinete NEMA estándar, pero proporciona una mejor protección al AP y puede ahorrar al SE, al usuario y al instalador una gran cantidad de tiempo y problemas. También están disponibles gabinetes NEMA especiales que tienen temperatura controlada y usan paneles solares para alimentar al equipo. Asegúrese de que el gabinete NEMA esté montado en forma segura. Un gabinete NEMA que mide 0,2 metros cúbicos (2 pies cúbicos) puede pesar tanto como 13,6 kg (30 libras). Si el gabinete no está correctamente asegurado se podría caer, dañar a alguien o destruir el conducto conectado para la energía. El cableado expuesto crea un peligro potencial de incendio.

10.4 Documentación

10.4.1 Documentación del diseño de la WLAN

Esta sección proporciona consejos sobre cómo responder a un pedido de propuesta [request for proposal (RFP)] de un usuario, e incluye información sobre cómo debería ser escrito un documento de diseño cuando no existe un RFP.

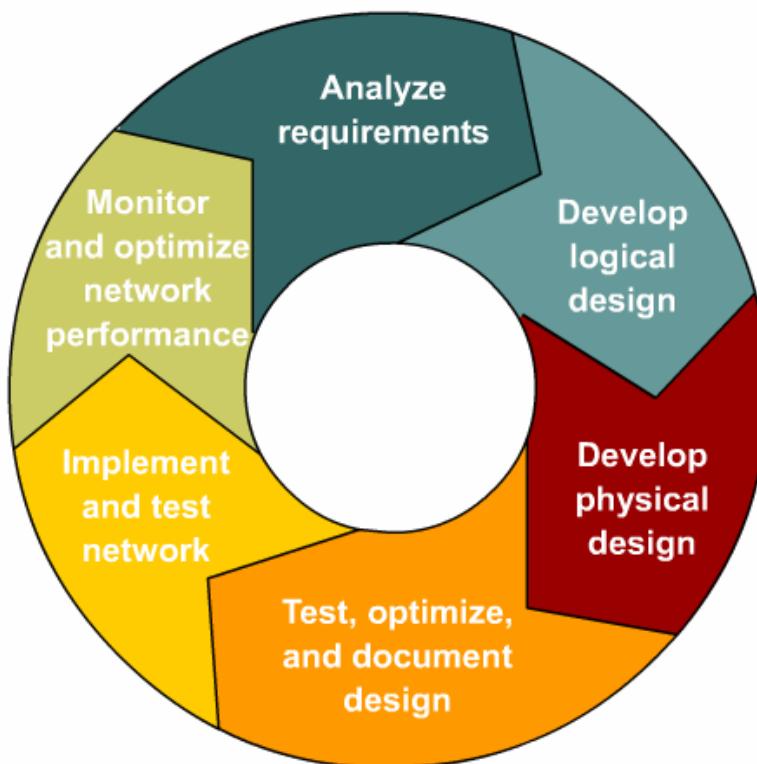


Figura 1

En este punto del proceso de diseño de la red debería existir un diseño integral, que esté basado en un análisis del negocio y en los objetivos técnicos del usuario, y que incluya componentes tanto lógicos como físicos que hayan sido probados y optimizados. El paso siguiente en el proceso es escribir un documento de diseño.

Un documento de diseño describe los requisitos de un usuario y explica cómo cumple el nuevo diseño con esos requisitos. También documenta la red existente, el diseño lógico y físico, y el presupuesto y los gastos asociados con el proyecto.

También es importante que un documento de diseño incluya planes para implementar el diseño de la red, para medir el éxito de la implementación y para desarrollar el diseño cuando aparezca un nuevo requisito de aplicación. La tarea del diseñador de red nunca está completa. El proceso de análisis de requisitos y de desarrollo de soluciones de diseño continúa aun después de que se ha implementado un diseño. La Figura 1 muestra la naturaleza cíclica del proceso de diseño de la red.

Además de ser cíclico, el diseño de la red también es iterativo. Se realizan pasos específicos durante múltiples fases de un diseño. Las pruebas se realizan durante la fase de validación del diseño y también durante la implementación. La optimización ocurre mientras finaliza el diseño y también durante la fase de supervisión de la red después de la implementación. La documentación es un esfuerzo continuo. La documentación puede facilitar el proceso de aprobación para un diseño.

10.4.2 Pedido de propuesta

Un RFP enumera los requisitos de diseño de un usuario y los tipos de soluciones que un diseño de red debe incluir. Las organizaciones envían RFPs a los fabricantes y consultores de diseño y utilizan las respuestas que reciben para identificar a los proveedores que pueden cumplir con sus requisitos. Las respuestas al RFP ayudan a las organizaciones a comparar diseños competidores, capacidades de los productos, precios y alternativas de servicios y soporte.

Algunas organizaciones especifican el formato requerido para la respuesta RFP. Si este es el caso, el documento del diseño inicial debería seguir el formato prescripto y la estructura proporcionada por el usuario. Las organizaciones que especifican un formato pueden negarse a leer respuestas que no cumplen con el formato solicitado. En algunos casos, el usuario puede pedir un documento complementario que proporcione información más detallada sobre el diseño lógico y físico de la red.

Algunos RFPs tienen la forma de un cuestionario. En este caso, las preguntas deberían determinar la forma en que está organizada la propuesta. Se pueden agregar ornamentos del diseño que se enfoquen en requisitos claves y puntos de venta, a menos que el RFP establezca específicamente que no deben ser agregados.

Aunque cada organización maneja los RFPs de manera ligeramente diferente, la mayoría de los RFPs requieren que las respuestas incluyan algunos o todos los puntos mostrados en la Figura 1.

Request for Proposal (RFP)

An RFP may include the following topics:

- A network topology for the new design
- Information on the protocols, technologies, and products that form the design
- An implementation plan
- A training plan
- Support and service information
- Prices and payment options
- Qualifications of the responding vendor or supplier
- Recommendations from other customers for whom the supplier has provided a solution
- Legal contractual terms and conditions

Figura 1

A pesar del hecho de que una respuesta a un RFP debe permanecer dentro de las pautas especificadas por el usuario, se debería usar el ingenio para asegurarse de que la respuesta resalte los beneficios del diseño. En base a un análisis del negocio y de los objetivos técnicos del usuario, y al flujo y características del

tráfico de la red, escriba la respuesta para que el lector pueda fácilmente reconocer que el diseño satisface los criterios de selección críticos.

Cuando escriba la respuesta, asegúrese de considerar a la competencia. Trate de predecir lo que los otros fabricantes o consultores de diseño podrían proponer para que la respuesta pueda enfatizar los aspectos de la solución que probablemente sean superiores a los diseños de la competencia. También es importante prestar atención al estilo del negocio del usuario. Recuerde la importancia de comprender las tendencias del usuario y cualquier política oficial o historia del proyecto que podría afectar a la percepción del diseño propuesto.

10.4.3 Especificaciones del estudio del sitio de la WLAN

Un estudio in situ es esencial para el desarrollo exitoso de la mayoría de las redes inalámbricas Aironet consistentes de tres o más access points inalámbricos y una cantidad de bridges inalámbricos. El diseño de red inalámbrica debería incluir los ítems mostrados en la Figura 1. La Figura 2 enumera los servicios de implementación necesaria.

Wireless Network Design Specifics

- The logical network design functional and performance requirements
- The physical network topology
- A map of coverage areas and signal strengths
- A design that provides the physical layout for wireless equipment

Figura 1

Implementation Services

- Design Review
- Equipment unpack and installation
- Configuration
- Verification testing

Figura 2

Beneficios de la planificación, diseño e implementación de servicios de la WLAN

La funcionalidad y rendimiento de una WLAN pueden variar dependiendo del entorno en el cual se despliega. El usuario puede no tener la habilidad o experiencia para estudiar y evaluar correctamente el sitio y para diseñar la ubicación de los access points y bridges para la cobertura y rendimiento que cumplirán con las necesidades únicas de uso de un usuario. Además, estos dispositivos y sus antenas deben ser correctamente orientados, instalados y configurados para lograr la cobertura y rendimiento deseados. De nuevo, dependiendo de los requisitos únicos del sitio, el usuario puede carecer de las habilidades y experiencia para hacer esto correctamente.

10.4.4 Reporte del estudio del sitio

El reporte final que será producido es el reporte del estudio del sitio. Todo el trabajo de estudio no significa nada sin el reporte del estudio del sitio. Esto es por lo que el usuario está pagando. El reporte proporciona toda la información que el usuario necesita para comenzar la instalación de la WLAN.

Sea tan específico como pueda en el reporte

La persona que escribe el reporte del sitio probablemente no realizará la instalación. Por lo tanto, el reporte deberá ser claro, conciso y fácil de entender. El reporte debería proteger tanto al escritor como al usuario. En el caso de un desacuerdo o problema, un buen reporte del estudio del sitio puede probar que el estudio fue realizado de acuerdo a los requisitos del usuario en el momento del estudio. Cuando se describan ubicaciones de APs, sea tan específico como pueda. Utilice objetos e identificadores para explicar exactamente dónde debería ser colocado el AP. Si el AP está ubicado en un pasillo, especifique cuál pasillo y la ubicación de esa área en las instalaciones. Especifique exactamente cómo debería ser montado el AP.

La ubicación de la antena es aun más importante que la ubicación del AP. Por lo tanto, es importante ser tan específico como sea posible cuando describa el lugar donde se ubicarán la antena. Por ejemplo, en lugar de especificar un área como "en la pared encima de la puerta", es mejor decir "en la pared encima de la puerta, 0,6 m (2 pies) a la izquierda del cartel SALIDA".

Descripciones precisas

El estudio del sitio describe la forma en que la antena va a ser orientada. Si la antena es omnidireccional, mencione que la antena va a ser montada en forma vertical, con el cable en la parte superior. No todos los instaladores estarán familiarizados con el equipo y con la forma de montarlo. Si la antena es direccional, describa la dirección en la cual debería ser orientada. Por ejemplo, una antena patch podría ser descripta como "mirando al norte" o "dirigida hacia la enfermería al final del pasillo".

Describa las instalaciones, su construcción, sus medidas y su contenido. Hable de las herramientas que fueron usadas en el estudio y de la forma en que el estudio fue realizado. Describa las configuraciones que fueron usadas en el estudio para determinar las velocidades de datos, los canales, el tamaño de los paquetes y los umbrales. Describa la cobertura para cada access point e incluya un diagrama de la cobertura.

Marque las áreas donde el usuario no desea cobertura. Si el usuario más tarde reclama haber pedido cobertura en una de estas áreas, esta documentación puede probar que el SE recibió instrucciones para no estudiar esas áreas. El usuario debería firmar y devolver una copia del reporte.

Agregue secciones que hablen sobre el montaje correcto de los APs y de las antenas. Detalle las especificaciones para proporcionar energía a los APs y para montar las cajas de electricidad. Hable sobre las extensiones del cableado de red y de energía propuestas, incluyendo dónde y cómo las extensiones de conectarán a cada sistema.

Enumere los componentes del sistema

El estudio del sitio debería enumerar los tipos de medios de red sugeridos y los componentes de conexión. Enumere los componentes de la WLAN que son propuestos para la instalación. Hable sobre la topología de la red y sobre la implementación planeada de la topología de la WLAN.

Incluya una lista de las partes que serán necesarias. Incluya la cantidad total de APs para la instalación y recomiende que haya uno de repuesto a mano en caso de una emergencia. Enumere la cantidad total de antenas necesarias.

Incluya diagramas que muestren las instalaciones, las ubicaciones de los APs y las extensiones de cables propuestas. Siempre que sea posible, incluya fotos. Una foto de la ubicación del AP o de la instalación de la antena propuesta clarifica la forma y el lugar donde el equipo debería ser instalado.

Enumere los contactos para cada una de las compañías involucradas. Estas pueden incluir los fabricantes, revendedores, compañías de servicios e información. Enumere nombre, direcciones, números telefónicos, números de fax y direcciones de e-mail. La lista de control en la actividad se puede utilizar para llevar la cuenta de los problemas de la administración del proyecto y de las responsabilidades del instalador y del usuario durante el proceso de instalación.

Resumen

Este módulo cubrió el estudio del sitio y la instalación de una WLAN. Se trató la importancia del conocimiento de la infraestructura y de los mapas de red precisos como paso inicial en la creación del estudio del sitio. A través del uso de actividades de laboratorio prácticas y actividades de demostración, el alumno deberá comprender mejor la creación de estudios del sitio y de documentación. Aunque se utilice la prueba y error, el alumno aprendió que un buen diseño ayuda al estudio del sitio.

Luego, el alumno aprendió a realizar un estudio del sitio, y conoció los problemas de las diferentes monturas e instalaciones. Finalmente, el alumno aprendió a documentar el proceso completo creando un reporte del estudio del sitio, respondiendo apropiadamente a un RFP y enviando el reporte final.

Módulo 11: Localización, supervisión, manejo y diagnóstico de averías

Descripción General

Este módulo hablará sobre los fundamentos de la solución de problemas. Comienza examinando una metodología que divide el proceso de solución de problemas en pasos manejables. Este enfoque sistemático puede ser usado para minimizar la confusión y reducir el tiempo requerido para la solución de problemas por prueba y error. La solución de problemas es un proceso paso a paso que todos los ingenieros de networking deben realizar. Este proceso por lo general requiere un enfoque de razonamiento inductivo o deductivo.

Luego se presentará una variedad de herramientas que son usadas para solucionar problemas en una WAN. Estas herramientas incluyen probadores de cables, que están diseñados para verificar la conectividad de todos los tipos de cables de LAN, y analizadores de espectro, que son usados para determinar si hay actividad en una frecuencia. Después de hablar sobre las herramientas, se presentará una explicación sobre la solución de problemas relacionados con el ingreso al sistema y a un único punto de falla.

Finalmente, se detallará una herramienta de administración propietaria de Cisco. Esta herramienta se llama Motor de Soluciones de LAN Inalámbrica [Wireless LAN Solution Engine (WLSE)], y está diseñada para la administración empresarial de la WLAN. El WLSE utiliza una interfaz gráfica de usuario (GUI) basada en web para una gran cantidad de access points (APs) y bridges para supervisar cambios de configuración, seguridad, cuentas, fallas y rendimiento.

11.1 Enfoque General de la Solución de Problemas

11.1.1 Descripción General

Las claves para mantener un entorno de red libre de problemas son la documentación, planificación y comunicación. Estos tres factores también determinan la capacidad para aislar y arreglar una falla de red rápidamente. Esto requiere un marco de trabajo de procedimientos y de personal que esté establecido mucho antes de que se realice cualquier cambio en la red. El objetivo de este módulo es ayudar a aislar y resolver los problemas más comunes de conectividad y rendimiento en un entorno de red.

Las redes continúan sumando servicios a medida que pasa el tiempo, y cada servicio adicional introduce más variables en la implementación de la red. Esto también agrega complejidad a la solución de problemas de la red. Por lo tanto, las organizaciones dependen cada vez más de los administradores de red y de los ingenieros de red con fuertes habilidades en la solución de errores.

Los ingenieros pasan una gran parte de su tiempo solucionando problemas. Por lo tanto, todas las herramientas procedimentales que puedan simplificar el proceso son importantes. El tiempo que tome el familiarizarse con cada una de las herramientas procedimentales puede reducir el tiempo pasado solucionando problemas en el campo. La decisión de invertir tiempo en aprender un nuevo procedimiento no es algo fácil de hacer. El objetivo principal es optimizar el tiempo de aprendizaje de nuevos procedimientos para ayudar a acortar el tiempo de trabajo en el campo.

Definition List

Deductive reasoning- reasoning from the general to the particular, or from cause to effect [syn: deduction, synthesis]

Inductive reasoning- reasoning from detailed facts to general principles [syn: generalization, induction]

Source: WordNet ® 1.6, © 1997 Princeton University

Figura 1

Después de que hayan sido considerados los protocolos y las líneas de productos, la solución de problemas es esencialmente un ejercicio de lógica. 1Cuando se enfrente a un problema de la red, debería usar algún

tipo de modelo de solución de problema. Este modelo deberá proporcionar un método lógico de trabajo paso a paso hacia una solución. Es importante comprender que los ingenieros de redes no consultan de un manual de metodología de solución de problemas cuando encuentran un problema. En realidad ellos trabajan en base a sus propias habilidades personales y con la metodología de solución de problemas que han desarrollado con el tiempo. Una metodología lógica puede ayudar a minimizar el tiempo perdido asociado con la solución de problemas no estructurada.

El razonamiento deductivo trabaja de lo más general a lo más específico. **2** Esto recibe el nombre informal de enfoque descendente. El razonamiento deductivo comienza con el desarrollo de una teoría sobre el problema. Esa teoría es luego reducida a una hipótesis específica que puede ser probada. Las observaciones luego se reúnen en base a la hipótesis. Esto permite que la hipótesis sean probadas con datos específicos. Esto dará por resultado una confirmación o rechazo de la teoría original.

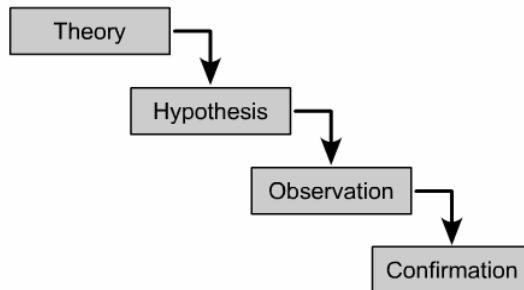


Figura 2

El razonamiento inductivo funciona en forma opuesta, yendo desde las observaciones específicas hasta las generalizaciones y teorías más amplias. **3** Esto a veces recibe el nombre de un enfoque ascendente. El razonamiento inductivo comienza con observaciones y mediciones específicas. Los patrones y regularidades luego conducen a la formulación de hipótesis tentativas que pueden ser exploradas. Finalmente se pueden desarrollar algunas conclusiones o teorías generales.

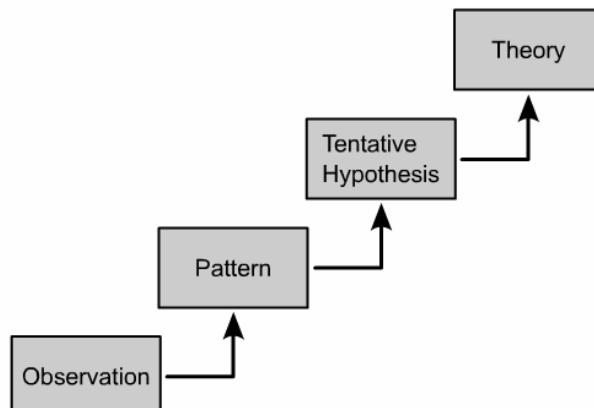


Figura 3

11.1.2 Síntoma - diagnóstico - solución

Síntomas, Problemas y Soluciones

Las fallas en las redes se caracterizan por ciertos síntomas. Estos síntomas pueden ser generales, como la incapacidad para acceder a Internet. Los síntomas también pueden ser más específicos, como la incapacidad para acceder a servidores específicos. Usando herramientas y técnicas específicas de solución de problemas se puede identificar a los problemas o causas de cada síntoma. Una vez identificados, cada problema puede ser resuelto implementando una solución consistente en una serie de acciones.

Modelo General de Solución de Problemas

Cuando se solucionan problemas en un entorno de red, funciona mejor un enfoque sistemático:

1. Defina el problema y reúna los síntomas.
2. Identifique todas las causas potenciales que pudieran estar causando los síntomas observados.
3. Elimine cada problema potencial, desde el más probable hasta el menos probable, hasta que los síntomas desaparezcan.

La Figura 1 ilustra el flujo del proceso para el modelo general de solución de problemas. Este flujo del proceso no es una pauta rígida para solucionar problemas en una red. Es una base sobre la cual se puede construir un proceso de solución de problemas que se acomode a un entorno en particular. El diagrama de flujo en esta sección proporciona los pasos específicos necesarios para completar el proceso.

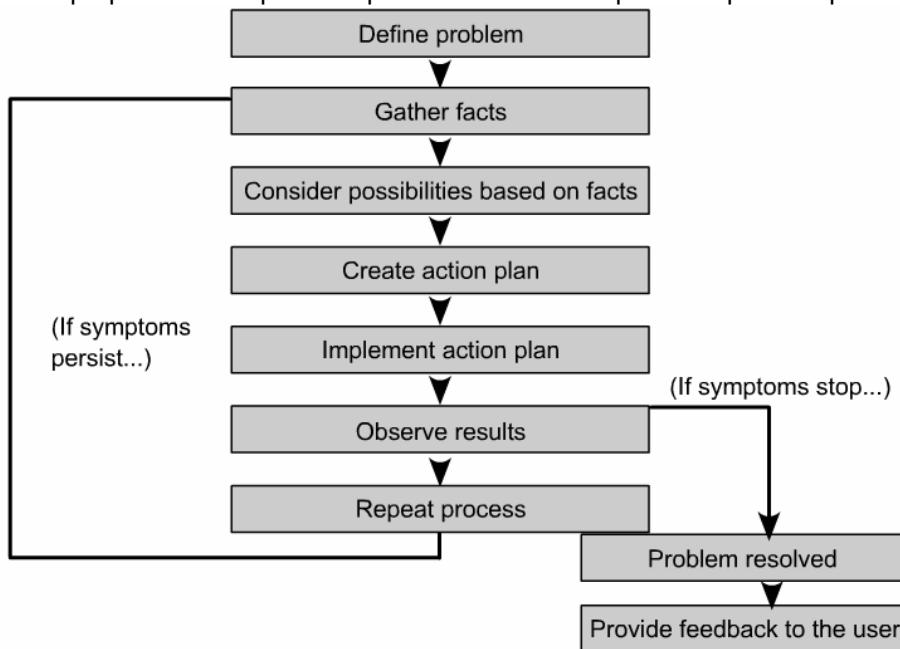


Figura 1

Cuando una red está caída, se necesita un enfoque sistemático para levantarla. En la mayoría de los escenarios de solución de problemas, es mejor ir de lo general a lo específico y eliminar las variables no relacionadas para enfocarse en el subconjunto de variables que contiene la solución. Este es un principio fundamental de la ciencia y no es sólo aplicable a la ingeniería de redes. El dividir problemas complejos en pasos más pequeños y el determinar las relaciones entre ellos puede ayudar a simplificar la formación de una solución total después de haber resuelto los problemas más pequeños.

En algunas situaciones, la parte más difícil de solucionar problemas es la documentación después de que el problema está resuelto. Un diagrama de red sencillo sirve como punto focal para la documentación compilada. La documentación cuidadosa es un proceso necesario que simplificará la vida del ingeniero y de otros en la organización. La documentación deberá realizarse una vez durante el estudio del sitio de la WAN y otra vez después de la finalización de la instalación y de la fase de prueba. La falta de documentación puede ser un factor que afecte a muchos problemas. Esto es especialmente cierto cuando el personal no tiene una vista detallada del estado actual de la red o del rendimiento anterior de la red. La documentación deberá proporcionar información fácilmente accesible a aquellos que la necesiten. Esta información también deberá ser fácil de actualizar. Es importante recordar que la documentación simplifica la administración de la red y reduce en gran medida el tiempo necesario para solucionar problemas.

11.1.3 Preparación para una falla de la red

Siempre es más fácil recuperar una falla de la red cuando los preparativos se realizaron antes de que ocurra. Posiblemente el requisito más importante en cualquier entorno de red es tener información actualizada y detallada sobre la red disponible para el personal de soporte en todo momento. La información completa es necesaria para permitir tomar decisiones inteligentes relacionadas con cambios en la red. La información completa también permite que la solución de problemas se realice tan rápida y fácilmente como sea posible. Durante el proceso de solución de problemas de la red, es muy importante asegurarse de que esta documentación se mantenga actualizada.

Como ayuda para prepararse para una falla de la red, responda las siguientes preguntas:

- ¿Hay un mapa físico y lógico detallado de la red?
 - ¿La organización o el departamento tienen un mapa de la red actualizado que explica la ubicación física de todos los dispositivos de la red y cómo están conectados?
 - ¿Tienen un mapa lógico de las direcciones de red, números de red, subredes, etc.?
- ¿Hay una referencia establecida para la red?
 - ¿La organización ha documentado el comportamiento y el rendimiento normal de la red en diferentes horas del día?

- ¿Hay una lista de todos los protocolos de red implementados en la red?
 - Para cada uno de los protocolos implementados, ¿hay una lista de números de red, subredes, zonas, áreas, etc. que están asociados con ellos?
- ¿Qué protocolos están siendo enrutados? **1**
 - >Para cada protocolo enrutado, ¿hay una configuración correcta y actualizada del router?
 - ¿A qué protocolos se les está aplicando bridging?
 - ¿Hay filtros configurados en los bridges? Si es así, ¿hay una copia de estas configuraciones?
- ¿Cuáles son los puntos de contacto de las redes externas, incluyendo cualquier conexión con la Internet?
 - Para cada conexión de red externa ¿qué protocolo de enrutamiento está siendo usado? **2**

Routed Protocols

- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)
- AppleTalk (AT)
- DECnet

Figura 1

Routing Protocols

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Enhanced IGRP (EIGRP)
- Border Gateway Protocol (BGP)
- AppleTalk Update-Based Routing Protocol (AURP)

Figura 2

11.1.4 Administración de la red y de las fallas

Administración de la red significa diferentes cosas para diferentes personas. En algunas situaciones, comprende a un asesor de redes solitario supervisando la actividad con un analizador de protocolos obsoleto. En otras situaciones, la administración de la red puede involucrar una base de datos distribuida, auto-sondeo de los dispositivos de la red y estaciones de trabajo avanzadas que generan visualizaciones gráficas en tiempo real de los cambios de topología y del tráfico de la red. En general, la administración de la red es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de red a supervisarlas y mantenerlas.

Modelo de Administración de Red ISO

La ISO ha contribuido en mucho a la estandarización de la red. **1** El modelo de administración de red ISO es el recurso principal para comprender las funciones más importantes de los sistemas de administración de red. Este modelo consiste en cinco áreas conceptuales, mostradas en la Figura **1**, que están definidas en las Figuras **2-6**.

Conceptual Areas Overview of the Network Management Model

1. Performance management
2. Configuration management
3. Accounting management
4. Fault management
5. Security management

Figura 1

Performance Management

The goal of performance management is to measure network performance and provide the necessary tools to maintain it at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Figura 2

Configuration Management

The goal of configuration management is to monitor network operation and system configuration information so that the effects of various hardware and software elements can be tracked and managed.

Figura 3

Accounting Management

The goal of accounting management is to measure network-utilization parameters so that individual or group use of the network can be regulated appropriately. Such regulation minimizes network problems because network resources can be distributed based on resource capacities. Regulation maximizes the fairness of network access for all users.

Figura 4

Fault Management

The goal of fault management is to detect, log, notify users of, and automatically fix network problems, whenever possible, to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements. The five steps are as follows:

1. Detecting the problem symptoms
2. Isolating the problem
3. Fixing the problem automatically if possible, or manually if necessary
4. Testing the solution on all the important subsystems
5. Logging the detection and resolution of the problem

Figura 5

Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network cannot be intentionally or unintentionally sabotaged. This prevents users without appropriate authorization from accessing sensitive information. For example, a security management subsystem can monitor users logging on to a network resource, and refuse access to those who enter inappropriate access codes.

Figura 6

11.2 Solución de Problemas según OSI

11.2.1 Descripción general del modelo

Protocolos de Internet

Los Protocolos de Internet (IPs) pueden ser usados para comunicarse a través de cualquier conjunto de redes interconectadas. Son igualmente aplicables a las comunicaciones de redes de área local (LAN) como a las de redes de área amplia (WAN). La suite de Internet incluye especificaciones de capa inferior como TCP e IP, y también especificaciones para aplicaciones comunes como e-mail, emulación de terminal y transferencia de archivos. La Figura 1 muestra a las capas de la suite TCP/IP y sus relaciones con el modelo de referencia OSI.

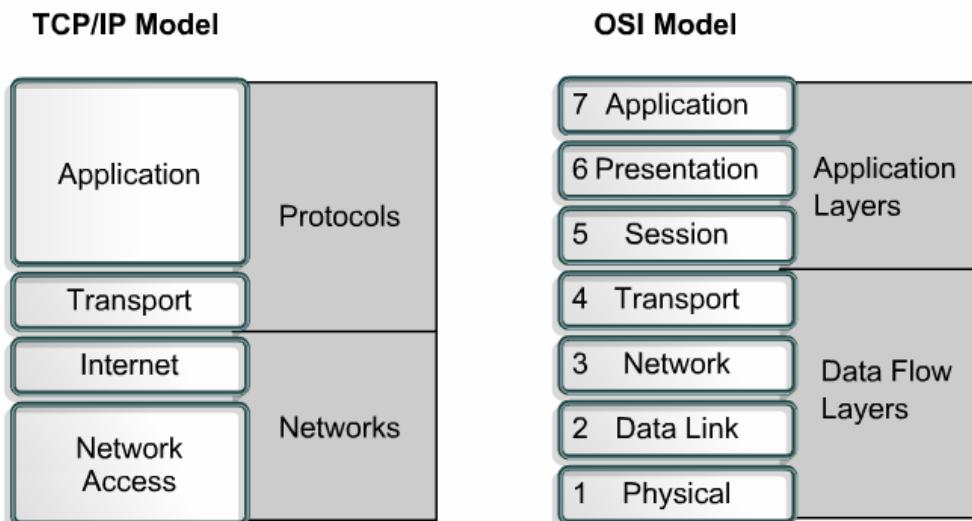


Figura 1

El modelo de referencia OSI proporciona un lenguaje común para los ingenieros de redes. Cuando se utiliza un enfoque sistemático en la documentación y en las arquitecturas de red, el modelo OSI es dominante en la solución de problemas de la red. El modelo permite que la solución de problemas se realice en una forma estructurada. Los problemas son normalmente descriptos en base a la capa del modelo OSI relacionada. Una revisión rápida del modelo OSI puede ayudar a clarificar su rol en la metodología de la solución de problemas.

Cada capa está razonablemente autocontenido, por lo que las tareas asignadas a cada una de ellas pueden ser implementadas en forma independiente. Esto permite que se puedan aplicar las soluciones ofrecidas por una capa sin afectar en forma adversa a las otras. El modelo OSI proporciona un marco de trabajo lógico y un lenguaje común usado por los ingenieros de redes para describir los escenarios de la red. La terminología de la Capa 1 a la Capa 7 es tan común que la mayoría de los ingenieros no tienen que pensar dos veces al respecto.

11.2.2 Solución de problemas según las capas

La Figura 1 muestra un enfoque para solucionar problemas en las diferentes capas OSI. Deberá haber un proceso ordenado basado en los estándares de networking que son usados.

La siguiente lista contiene alguno de los errores más comunes 2:

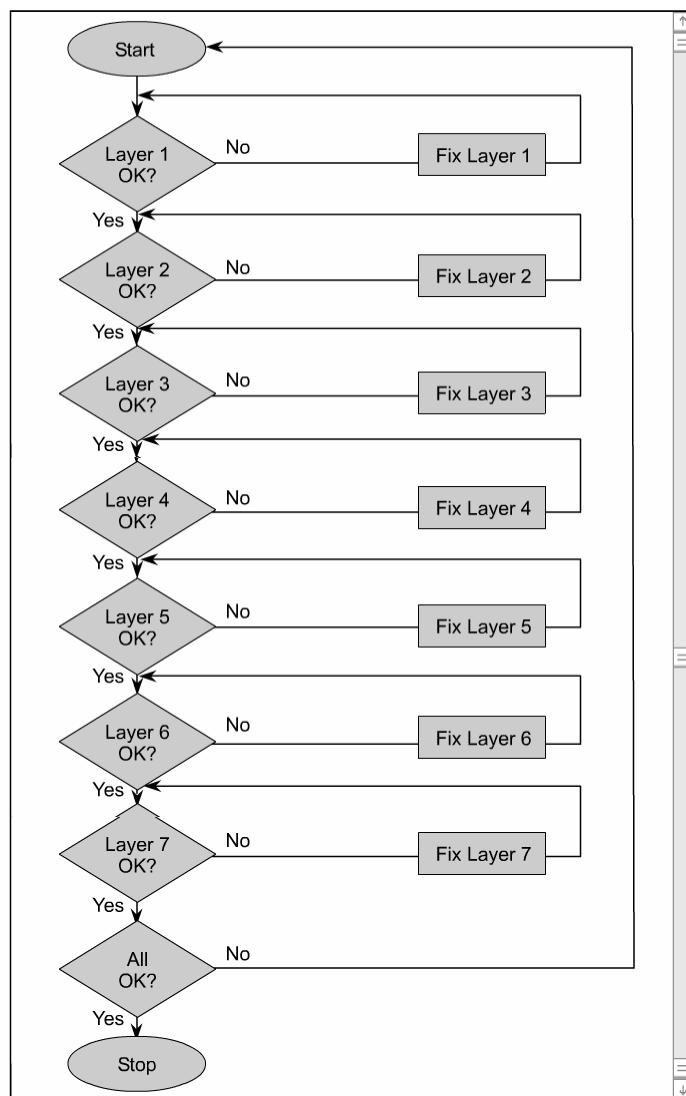


Figura 1

Problemas a Solucionar en la Capa Física

- Problemas de energía
- Cableado de la antena
- Frecuencia de 2,4 Ghz
- Control de la configuración de Ethernet
- 802.11a,b,g
- Interferencia
- Amplificadores
- Conexión a tierra
- Concordancia del número de canal
- Distancia versus velocidad
- Seguridad eléctrica
- Energía de transporte
- Modo de la antena
- Rol de la radio
- Arranque contra repetidor
- Durante la configuración inicial
- Interfaz Ethernet
- Que esté activa
- Asegurarse de que la radio esté activada

Problemas a Solucionar en la Capa de Datos

- Controladores NDIS
- SSIDs

- Adhoc versus infraestructura
- Claves WEP activadas
- Autenticación OPEN/compartida/EAP
- Filtros
- Modo encabezado/mundial de onda corta
- VLANs
- LEAP nombre de usuario/password
- STP
- ¿Está activada la espera en caliente [hotstandby]?
- Que los LEDs del Access Point titilen
- Reinicio/restauración

Problemas a Solucionar en la Capa de Red

- Predeterminados
- Filtros
- Dirección IP y máscara de subred
- Problemas de la VPN
- NAT

Physical Layer	Data Layer	Network Layer	Transport Layer
Power issues	NDIS drivers	Default	Filters ↑
Antenna cabling	SSIDs	Filters	=
Frequency 2.4Ghz	Adhoc versus Infrastructure	IP Address and subnet mask	
Check ethernet settings	WEP keys enabled	VPN issues	
802.11a,b,g	OPEN/shared/EAP authentication	NAT	
Interference	Filters		
Amplifiers	Short radio header/world mode		
Grounding	VLANs		
Channel number matching	LEAP username/password		
Distance versus speed	STP		
Power safe	Is hotstandby enabled?		
Transport power	Blink Access Point LEDs		
Antenna mode	Do a reset/restore		
Radio role			
Boot versus repeater			
During initial setup			
Ethernet interface			
Be active			
Make sure radio is enabled			↓

Figura 2

11.2.3 Capa 1: medios, conectores y dispositivos

Los problemas más comunes de la red pueden ser atribuidos a problemas de cableado que comprenden medios, conectores y paneles de conexión. Estos son los problemas de la Capa 1 que no pueden ser pasados por alto. Por ejemplo, los cables de fibra multimodo y de modo simple son usados a menudo para ATM, FDDI, Fast Ethernet y Gigabit Ethernet ①. Cuando se solucionan problemas con cables de fibra óptica, una consideración importante a hacer es a los problemas de conectividad asimétrica. Un problema de conectividad asimétrica ocurre cuando falla un extremo de un par de cables transmisor/receptor, pero el cable restante continúa enviando datos. La conectividad asimétrica puede afectar la habilidad de eludir bucles del spanning-tree. Muchas cosas también pueden funcionar mal con los cables de cobre UTP ②. Por ejemplo, el cable que está expuesto a áreas de alto tráfico puede ser roto, doblado o desconectado causando problemas de conectividad.



Figura 1

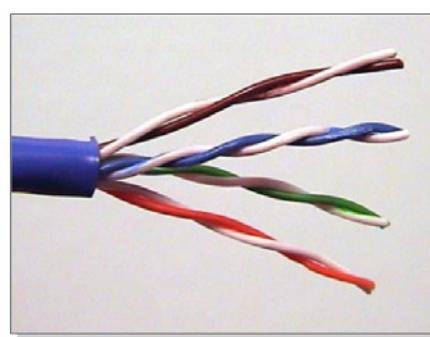


Figura 2

Cuando se solucionan problemas de cableado de un dispositivo o entre dispositivos, realice las siguientes preguntas:

- ¿Los cables son del tipo correcto para la instalación? La Categoría 3 es sólo para 10BaseT. ¿Está instalado un cable de Categoría 3 en lugar de un cable de Categoría 5?
- ¿El cable de Categoría 5 está instalado correctamente?
- ¿El cable es cruzado o derecho? ¿De cuál tipo debería ser? Compare los conectores RJ-45 de ambos extremos del cable si no está seguro.
- ¿Hay un alambre cortado en alguno de los extremos del cable? Los cables que están instalados demasiado ajustados o agrupados demasiado apretados con una banda de sujeción pueden tener alambres cortados en el conector. Los cables que se extienden por un pleno pueden tener alambres cortados y exhibir condiciones intermitentes de circuitos abiertos.
- ¿El cable es más largo que la especificación de 100 m (328 pies)? Un reflectómetro de dominio de tiempo [time domain reflectometer (TDR)] puede mostrar la longitud del cable, incluyendo a todas las conexiones del gabinete de cableado.
- ¿El cableado del punchdown es correcto? ¿Hay cables faltantes, flojos o cortados en el bloque punchdown ?
- ¿Está funcionando bien la tarjeta del adaptador de red/puerto de interfaz en el extremo del usuario?
- ¿El dispositivo está conectado al puerto correcto? ¿El puerto está activo?
- ¿Se está usando un transceptor para convertir el medio? ¿Funciona correctamente?



Figura 3

Un método que puede utilizarse para probar el cableado instalado es reemplazar el cable completo por un cable externo. Si hay un cable Categoría 5 probado, extienda el cable entre los dos dispositivos para probar la conectividad. Esta prueba eliminará cualquier duda sobre los cables de los equipos o sobre las conexiones punchdown. Esto también puede ser verificado con un probador de cables.

Los hubs aun son usados en muchos entornos LAN. Asegúrese de que estén funcionando correctamente controlando la luz del enlace/estado del puerto además de los LEDs de estado de la unidad.

11.2.4 Capa 2: bridges y switches

Bridges

Los bridges y APs inalámbricos son dispositivos de comunicación de datos que funcionan principalmente en la Capa 2. Varios tipos de bridges son usados como importantes dispositivos de internetworking. El bridging transparente se encuentra principalmente en los entornos Ethernet, mientras que el bridging de ruta origin ocurre principalmente en los entornos Token Ring. El bridging de traducción trabaja sobre los principios de formatos y de transporte de diferentes tipos de medios, normalmente Ethernet y Token Ring.

Los bridges analizan los frames entrantes, toman decisiones de envío basadas en la información contenida en los frames, y envían a los frames hacia sus destinos. La transparencia en el protocolo de capa superior es una ventaja principal del bridging. Como el dispositivo funciona en la capa de enlace de datos, no se necesita examinar la información de capa superior. Esto le permite enviar rápidamente al tráfico que representa a cualquier protocolo de capa de red. No es raro que un bridge mueva tráfico de AppleTalk, DECnet, TCP/IP, XNS y otros entre dos o más redes.

Los bridges son capaces de filtrar frames en base a cualquier campo de la Capa 2. Un bridge inalámbrico, por ejemplo, puede ser programado para que rechace a todos los frames de una red en particular. Como la información de la capa de enlace de datos a menudo incluye una referencia a un protocolo de capa superior, los bridges pueden normalmente filtrar sobre este parámetro. Además, los filtros pueden ser útiles al tratar con broadcast innecesario y paquetes multicast.

Al dividir a las redes grandes en unidades auto contenidas, los bridges inalámbricos proporcionan varias ventajas. El bridge puede actuar como un firewall contra algunos errores de red potencialmente dañinos, y puede soportar comunicaciones entre una cantidad de dispositivos mayor que la que una sola LAN conectada al bridge podría soportar. Los bridges extienden el alcance efectivo de una LAN, permitiendo la conexión de estaciones distantes que no estaban permitidas anteriormente.

Switches

La conmutación es una tecnología que alivia la congestión en las LANs Ethernet reduciendo el tráfico y el ancho de banda creciente. Las características comunes del switch incluyen puertos Ethernet o de Fibra para proporcionar conectividad entre dispositivos de red como estaciones de trabajo, impresoras, servidores y dispositivos de internetworking como routers, switches y hubs.

En las comunicaciones de datos, todo el equipo de conmutación y enrutamiento realizan dos operaciones básicas:

- Comutación de frames de datos – El proceso por el cual un frame es recibido sobre un medio de entrada y luego es transmitido hacia un medio de salida
- Mantenimiento de las operaciones de conmutación – Los switches arman y mantienen tablas de enrutamiento y buscan bucles. Los routers arman y mantienen tablas de enrutamiento y tablas de servicios.

Al igual que los bridges, los switches conectan segmentos de LAN, usan una tabla de direcciones MAC para determinar el segmento sobre el cual un datagrama necesita ser transmitido, y reducen el tráfico. Los switches funcionan a velocidades mucho mayores que los bridges, y pueden soportar nueva funcionalidad, como LANs virtuales (VLANs). Si las VLANs han sido configuradas sobre un switch, esto puede afectar la conectividad con otros dispositivos sobre la LAN, dependiendo de la configuración del router.

Los switches determinan la segmentación de una red construyendo tablas de direcciones que contienen la dirección de cada dispositivo de red e identifican cuál segmento debe ser usado para llegar a ese dispositivo. Mientras ocurre el aprendizaje, el tráfico no será enviado.

Si el tráfico no pasa después de la fase de aprendizaje y si las VLANs están configuradas correctamente, otro problema común puede ser las configuraciones de seguridad de los puertos que bloquean el tráfico desde dispositivos host no autorizados. Revise la configuración del switch para verificar las configuraciones de seguridad.

11.2.5 Capa 3: routers

Los routers son dispositivos de internetworking que trabajan en la Capa 3 de OSI, la capa de red. Los routers enlazan, o interconectan, segmentos de red o redes completas. Pasan los paquetes de datos entre las redes basándose en información de Capa 3.

Los routers toman decisiones lógicas con respecto a la mejor ruta para enviar los datos en una Internetwork basándose en información de Capa 3. Luego los routers dirigen los paquetes hacia el puerto y segmento de salida apropiados. Por lo tanto, el enrutamiento a veces es llamado conmutación de Capa 3. Los routers vienen en una gran variedad de tamaños y factores de formato, pero tienen características físicas comunes, como interfaces LAN/WAN que proporcionan conectividad entre redes.

Si IP u otros servicios pueden ser accedidos sobre la LAN, pero el acceso a Internet no está disponible, el router puede ser el punto de falla. Otros problemas de conectividad, como acceder a otras VLANs, pueden

ser atribuidos a un router. En muchos casos, el router está configurado con listas de control de acceso (ACLs) para evitar el acceso no autorizado. En una red muy segura, el agregar nuevos dispositivos requiere planificación y coordinación. Siempre consulte al administrador de LAN/WAN cuando conecte nuevos dispositivos a la LAN.

The **show** commands help monitor installation behavior and normal network behavior, as well as isolate problem areas.

The **debug** commands assist in the isolation of protocol and configuration problems.

The **ping** commands help determine connectivity between devices on the network.

The **trace** commands provide a method of determining the route by which packets reach their destination from one device to another.

Figura 1

Los routers proporcionan numerosos comandos integrados para ayudar en la supervisión y solución de problemas de la internetwork, como muestra la Figura 1. Si no existen problemas de configuración en el router, otros posibles podrían ser problemas de cableado en el router o cortes del proveedor del servicio.

Uso de Comandos show

Los comandos show, mostrados en la Figura 2, son poderosas herramientas de supervisión y solución de problemas. Utilice los comandos show para realizar una variedad de funciones, incluyendo:

- Supervisión del comportamiento del router durante la instalación inicial.
- Supervisión del funcionamiento normal de la red.
- Aislamiento de interfaces, nodos, medios o aplicaciones con problemas.
- Determinación del congestionamiento de la red.
- Determinación del estado de los servidores, clientes u otros vecinos.

show version - Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot image.

show processes - Displays information about the active processes.

show protocols - Displays the configured protocols and shows the status of all configured Layer 3 protocols.

show memory - Shows statistics about the router memory, including memory free pool statistics.

show stacks - Monitors the stack use of processes and interrupt routines and displays the reason for the last system reboot.

show buffers - Provides statistics for the buffer pools on the router.
show flash-Shows information about the Flash memory device.

show running-config - Displays the active configuration file. The command is write term for Cisco IOS Release 10.3 or earlier.

show startup-config - Displays the backup configuration file. The command is show config for Cisco IOS Release 10.3 or earlier.

show interfaces - Displays statistics for all interfaces configured on the router.

show users - Displays information about users that are connected to the router.

Figura 2

11.2.6 Solución de problemas de TCP/IP

La solución de problemas básicos de TCP/IP en máquinas con Windows combina los datos reunidos desde la perspectiva del router, switch, bridge y AP con datos reunidos desde la perspectiva del cliente o servidor Windows. Algunos de los problemas comunes de conectividad TCP/IP se muestran en la Figura 1.

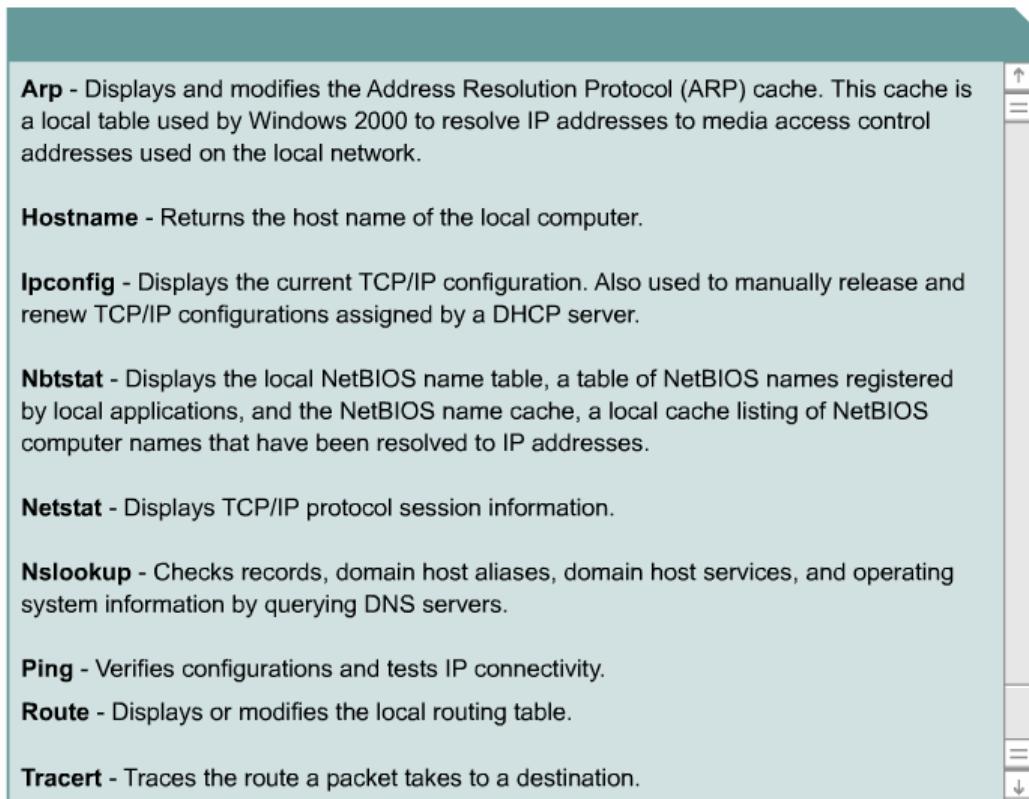


Figura 1

Ping

Uno de los usos más comunes del ICMP es como herramienta de diagnóstico. Un simple ping utiliza ICMP para determinar si un host está recibiendo o no paquetes. Para más detalles sobre ICMP, vea el RFC 792. Un ping al loopback es una de las primeras pruebas de ping que debería realizarse cuando está cuestionada la conectividad. Un ping al loopback está dirigido a 127.0.0.1, la dirección de loopback, para revisar la integridad de la pila TCP/IP y de la NIC.

ARP

ARP mostrará el mapeo de dirección IP a MAC. Para ver el caché ARP, en el prompt de comando escriba arp –a.

Ipconfig o Winipcfg

Se puede usar ipconfig en Windows NT, 2000 o XP, o winipcfg en Windows 95 o 98 para revisar la configuración de host local. Ingrese a una ventana de Prompt de Comando en el host y escriba el comando ipconfig /all. El resultado de este comando muestra la configuración de dirección TCP/IP, incluyendo la dirección del servidor del Sistema de Nombres de Dominio (DNS). Si alguna dirección IP es incorrecta o si no muestra ninguna dirección IP, determine la dirección IP correcta y editela o ingrésela para el host local. El comando ipconfig /release seguido por ipconfig /renew forzará un pedido para el servidor DHCP de una dirección IP.

Tracert

La herramienta tracert en un host Windows NT, 2000, o XP reporta cada nodo que cruza un paquete TCP/IP en su camino hacia un destino. Hace esencialmente lo mismo que el comando trace en el Software Cisco IOS.

11.3 Herramientas de Diagnóstico

11.3.1 Probadores de cables, multímetros y monitores de red

Las que siguen son herramientas de terceros que se utilizan normalmente en la solución de problemas de la internetwork:

- Volt-ohmímetros, multímetros digitales y probadores de cables son útiles para probar la conectividad física de una red de cables.
- Los reflectores con indicación temporal [time domain reflectors (TDRs)] y los reflectores con indicación temporal ópticos (OTDRs) son dispositivos que ayudan a localizar roturas de cables, desigualdades de impedancias y otros problemas físicos de la red de cables.
- Las cajas de conmutación y las fox boxes son útiles para solucionar problemas en las interfaces periféricas.
- Los analizadores de red decodifican problemas en las siete capas OSI y pueden identificarlos automáticamente en tiempo real, proporcionando así una visión clara de la actividad de la red y clasificando los problemas por su importancia crítica.



Figura 1

Los volt-ohmímetros y los multímetros digitales están en el extremo inferior del espectro de las herramientas para probar cables 1. Estos dispositivos miden parámetros como el voltaje AC y DC, la corriente, la resistencia, la capacitancia y la continuidad. Un probador de cable podría realizar las siguientes funciones:

- Probar y reportar las condiciones del cable, incluyendo NEXT, atenuación y ruido
- Realizar reflectometría con indicación temporal, supervisión del tráfico y funciones de mapeo de cables
- Visualizar información de capa MAC sobre el tráfico de la LAN, proporcionar estadísticas como el uso de la red y proporciones de errores de paquetes, y realizar una prueba de protocolo limitada, como pruebas de ping TCP/IP

Un equipo de pruebas similar está disponible para el cable de fibra óptica. A causa del costo relativamente alto del cable de fibra óptica, éste debería ser probado antes de la instalación, lo que también recibe el nombre de prueba en el carrete, y después de la instalación. La prueba de continuidad de la fibra requiere una fuente de luz visible, o un Reflectómetro, y se utiliza con medidores de energía que miden las mismas longitudes de ondas de la luz, prueban la atenuación y devuelven la pérdida en la fibra.

El probador de cables mostrado en la Figura 2 es el Fluke 620 LAN CableMeter. Este probador de cable se utiliza en muchas Academias Cisco para verificar la conectividad de todos los tipos de cables de LAN. Puede medir la longitud del cable o la distancia hasta un defecto. También se utiliza para probar las fallas como: pares abiertos, en corto, invertidos, cruzados o separados.



Figura 2

En el extremo superior del espectro de probadores de cables están los TDRs. Estos dispositivos pueden localizar rápidamente circuitos abiertos y en corto, dobleces aplastados, enrulados, agudos, discrepancias de impedancias y otros defectos en los cables de cobre. Algunos TDRs también pueden calcular la velocidad de propagación basada en la longitud de un cable configurado.

Los supervisores de red llevan la cuenta continuamente de los paquetes que atraviesan una red. Esto proporciona una imagen precisa de la actividad de la red en cualquier momento, o un registro histórico de la actividad de la red durante un período de tiempo. Los supervisores de red no decodifican el contenido de los frames. Son útiles para encontrar la referencia de una red. La toma de muestras de la actividad de una red durante un período de tiempo para establecer un perfil normal del rendimiento proporciona la referencia. El

Fluke OptiView es un ejemplo de supervisor de red. El OptiView detecta dispositivos en la red, lista posibles problemas y también descubre segmentos de la red y dominios de Net BIOS.

11.3.2 Sniffers

Analizadores de Red

Un analizador de red decodifica las diferentes capas de protocolos en un frame grabado y las presenta como abreviaturas o resúmenes legibles. Un analizador de red detalla cuál capa está involucrada y qué función proporciona cada byte o contenido de byte. Los analizadores de redes también reciben el nombre de analizadores de protocolos o sniffers de paquetes. Están disponibles diferentes paquetes de software inalámbrico, como WildPackets Airopeek, Network Stumbler y Sniffer Wireless 1. Fluke proporciona dos dispositivos dedicados diferentes, el OptiView y el WaveRunner, los que proporcionan análisis inalámbrico.



Figura 1

La mayoría de los analizadores de red pueden realizar las siguientes funciones:

- Filtra el tráfico que cumple con cierto criterio, por ejemplo, puede capturar todo el tráfico hacia y desde un dispositivo en particular
- Le coloca la hora a los datos capturados
- Presenta a las capas de protocolos en una forma fácilmente legible
- General frames y los transmite por la red
- Incorpora un sistema experto en el cual el analizador utiliza un conjunto de reglas, combinadas con información sobre la configuración y funcionamiento de la red, para diagnosticar y resolver problemas de red

11.3.3 Analizadores de Espectro

Impedimentos de RF

Muchos factores impiden la transmisión o recepción exitosa de una señal de radio. Los problemas más comunes son:

- interferencias de radio
- interferencias electromagnéticas
- problemas de cables
- problemas de antena

Un analizador de espectro es la mejor herramienta para determinar si existe actividad sobre una frecuencia 1. Si se sospecha que hay interferencia de radio en la transmisión o recepción de la WLAN, apague el equipo que funciona sobre la misma frecuencia y ejecute la prueba. La prueba muestra cualquier actividad sobre esa frecuencia y sobre otras frecuencias donde el equipo puede trabajar. Esto ayuda a determinar los cambios de frecuencias.

RF Impairments Radio Interference Electromagnetic Interference Cordless Phones or other 2.4-GHz wireless devices

Figura 1

Las fuentes de interferencia y de degradación de la señal pueden ser las siguientes:

- Interferencias de Radio – Como no se necesita licencia para trabajar con equipos de radio en la banda de los 2,4 GHz, donde trabajan los equipos de la WLAN, es posible que otros transmisores emitan sobre la misma frecuencia.
- Interferencias Electromagnéticas – Es posible que las EMI sean generadas por un equipo que no es de radio que funciona en las proximidades del equipo de la WLAN. Es más probable que las EMI afecten a los componentes del transmisor en lugar que a la transmisión. Para minimizar los efectos posibles de las EMI, es mejor ubicar el equipo de radio tan lejos como sea posible de las fuentes potenciales de EMI. Trate de suministrar energía condicionada al equipo WLAN para disminuir los efectos de la EMI generados también sobre los circuitos de energía.
- Teléfonos Inalámbricos u otros dispositivos inalámbricos de 2,4 GHz – Si el teléfono es un dispositivo DS que utiliza el mismo canal que el equipo WLAN, y si el teléfono está ubicado cerca del equipo, pueden ocurrir problemas cuando ambos se utilicen simultáneamente. Las siguientes sugerencias pueden ayudar a resolver el problema:
 - Cambie la ubicación del AP o de la base del teléfono inalámbrico.
 - Trate de comutar al canal 1 o al canal 11 en el AP.
 - Utilice una antena remota en la tarjeta del cliente si eso es una opción.
 - Utilice el teléfono con la antena bajada, si es posible.
 - Utilice un teléfono de 900 MHz en lugar de un teléfono de 2,4 GHz.

11.3.4 Medidores de gauss y tesla

Un medidor de gauss mide campos eléctricos y magnéticos (EMFs), que son producidos por las líneas eléctricas, el cableado eléctrico y el equipo eléctrico.¹ A veces éstos pueden causar problemas con los dispositivos y operaciones de red. Los EMFs son líneas de fuerza invisibles que rodean a todos los dispositivos eléctricos. Los campos eléctricos son producidos por el voltaje y aumentan en fuerza a medida que el voltaje aumenta. La fuerza del campo eléctrico se mide en unidades de voltios por metro (V/m). Los campos magnéticos resultan del flujo de la corriente a través de cables o dispositivos eléctricos y aumentan en fuerza a medida que la corriente aumenta.

Electric fields - Electric field strength is measured in volts per meter (V/m) or in kilovolts per meter (kV/m). One kilovolt equals 1000 volts.

$$1 \text{ kV} = 1000 \text{ V}$$

Magnetic fields - Magnetic field intensity is measured in units of gauss (G) or tesla (T). Gauss is the unit most commonly used in the United States. Tesla is the internationally accepted scientific term. One tesla equals 10,000 gauss.

$$1 \text{ T} = 10,000 \text{ G}$$

Since most environmental EMF exposures involve magnetic field intensities, which are only a fraction of a tesla or a gauss, these are commonly measured in units of microteslas (μT) or milligauss (mG). A milligauss is 1/1000 of a gauss. A microtesla is 1/1,000,000 of a tesla.

$$1 \text{ G} = 1000 \text{ mG}$$

$$1 \text{ T} = 1,000,000 \text{ } \mu\text{T}$$

To convert a measurement from microteslas (μT) to milligauss (mG), multiply by ten.

$$1 \text{ } \mu\text{T} = 10 \text{ mG}$$

$$0.1 \text{ } \mu\text{T} = 1 \text{ mG}$$

Wavelength and frequency

Electric and magnetic fields can be characterized by their wavelength, frequency, and amplitude. Wavelength describes the distance between one peak on the wave and the next peak. The frequency, measured in hertz (Hz), describes how many wave peaks pass by in one second. Electricity in North America alternates 60 times each second and thus has a frequency of 60 cycles per second, or 60 Hz. In many other parts of the world, the frequency for electric power is 50 Hz. Amplitude is also referred to as field intensity.

Figura 1

Los campos magnéticos se miden en unidades gauss (G) o tesla (T). La mayoría de los equipos eléctricos tienen que estar encendidos para que se produzca un campo magnético, ya que la corriente debe estar

fluyendo. Los campos eléctricos están presentes incluso cuando el equipo está apagado, mientras permanece conectado a la fuente de la energía eléctrica.

Los campos eléctricos son blindados o debilitados por materiales que conducen electricidad incluyendo árboles, edificios y la piel humana. Los campos magnéticos atraviesan la mayoría de los materiales y por lo tanto son más difíciles de blindar. Tanto los campos eléctricos como los magnéticos disminuyen a medida que la distancia desde el origen aumenta.

11.4 Puntos Simples de Falla

11.4.1 Firmware y controladores

Puede haber muchos puntos de fallo cuando se instala y solucionan problemas en una WLAN. Si es posible el acceso a un AP o bridge a través del puerto Ethernet, entonces hay muy poca necesidad de solucionar problemas con la LAN cableada. El problema está principalmente con el AP, el bridge o el cliente.

Comience controlando el firmware. En ocasiones se puede rastrear un problema con la señal de radio hasta un problema con el firmware, y las actualizaciones de la versión del software del controlador se utilizan principalmente para solucionar el problema y mejorar la estabilidad. Por lo tanto, es aconsejable usar la versión más reciente del controlador o firmware con los productos WLAN. Si se encuentra un problema de comunicación de radio en la WLAN, asegúrese de que cada componente esté ejecutando la versión más actualizada de su firmware o controlador.

El administrador de dispositivos [1](#) en una estación de trabajo de Windows puede ser usado para controlar la versión del controlador y determinar si el hardware está funcionando correctamente.

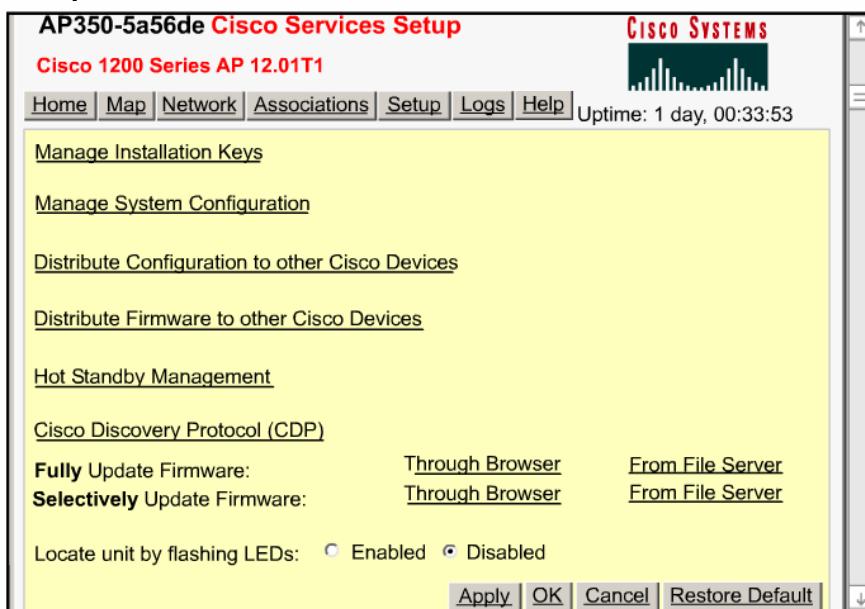


Figura 1

Desde la Página de Servicios de Cisco, es posible controlar el sistema actual y el firmware de la radio además de actualizar el firmware a través del browser o el servidor FTP.

11.4.2 Configuración del software

Problemas de Configuración del Software

Cuando se encuentran problemas de configuración, la configuración de los dispositivos WAN, incluyendo clientes, APs y bridges, puede ser la causa de la falla de la radio. Ciertos parámetros, que se muestran en la Figura [1](#), deben estar correctamente configurados para que los dispositivos se comuniquen exitosamente. Si están mal configurados, el problema resultante puede parecer un problema del dispositivo de radio. Estos parámetros incluyen al Identificador del Conjunto de Servicios, la frecuencia, la velocidad de los datos y la distancia.

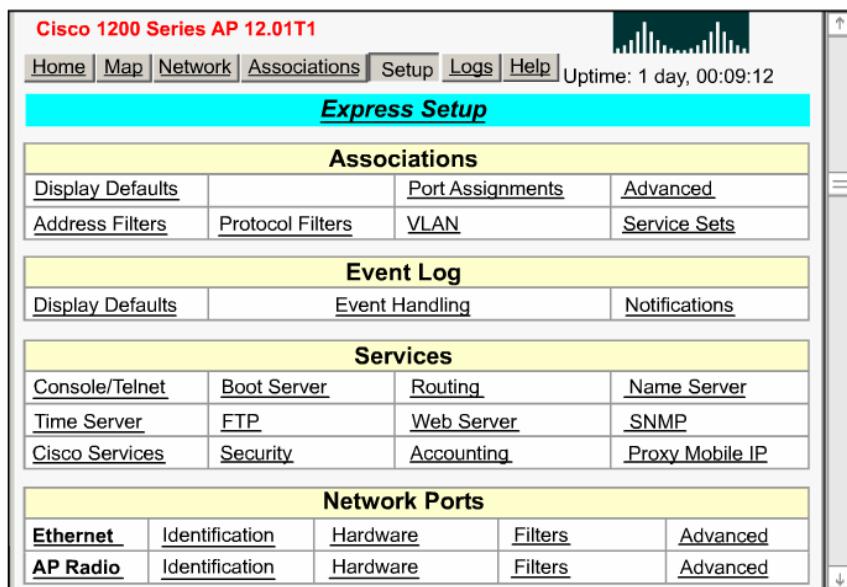


Figura 1

Identificador del Conjunto de Servicios

Los dispositivos WLAN deben tener el mismo Identificador del Conjunto de Servicios (SSID) que todos los otros dispositivos en la infraestructura inalámbrica. Las unidades con diferentes SSIDs no pueden comunicarse directamente entre ellas.

Frecuencia

Los dispositivos de radio son configurados para que encuentren automáticamente la frecuencia correcta. El dispositivo recorre el espectro de frecuencias, buscando una frecuencia no usada o buscando paquetes transmitidos que tengan el mismo SSID que el dispositivo. Si la frecuencia no está configurada como Automática, asegúrese de que todos los dispositivos en la infraestructura WLAN estén configurados con la misma frecuencia.

Velocidad de Datos

Si los dispositivos WLAN están configurados para diferentes velocidades de datos no podrán comunicarse. Las velocidades de datos se expresan en megabits por segundo (Mbps). Algunos escenarios comunes incluyen lo siguiente:

- Los bridges son usados para comunicarse entre dos edificios. Si un bridge está configurado en una velocidad de datos de 11 Mbps y el otro está configurado para una velocidad de datos de 1 Mbps, la comunicación fallará.
- Si ambos dispositivos están configurados para usar la misma velocidad de datos, otros factores podrían evitar que alcancen esa velocidad, en cuyo caso la comunicación falla.
- Si un bridge tiene una velocidad de datos de 11 Mbps, y el otro está configurado para usar cualquier velocidad, entonces las unidades se comunican a 11 Mbps. Sin embargo, si hay algún impedimento en la comunicación que requiere que las unidades bajen a una velocidad de datos inferior, la unidad configurada para 11 Mbps no puede bajar, y las comunicaciones fallan.

Para reducir el potencial de fallas, los dispositivos WLAN deberían estar configurados para comunicarse a más de una velocidad de datos.

Distancia

Como el enlace de radio entre bridges puede ser bastante largo, el tiempo que tarda la señal de radio en viajar entre las radios puede volverse significativo. El parámetro de distancia se utiliza para ajustar los diversos temporizadores utilizados en el protocolo para contar el retardo. El parámetro sólo es ingresado en el bridge raíz, el que a su vez lo informa a los repetidores. La distancia del enlace de radio más largo en el conjunto de bridges se ingresa en kilómetros, no en millas.

11.4.3 Cables de antena

El tipo de cable mostrado en la Figura 1 que conecta las antenas a los dispositivos WLAN es una posible fuente de dificultades en la comunicación de radio.

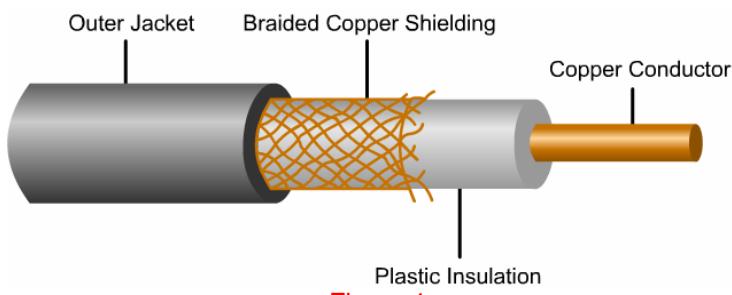


Figura 1

La selección del cable también es importante. Cuando se configuran bridges para comunicarse sobre una larga distancia, los cables de la antena no deberían ser más largos de lo necesario. Esto es importante porque cuanto más largo es el cable, más se atenuará su señal, dando por resultado una fuerza de señal inferior y en consecuencia un alcance menor. Se puede utilizar un utilitario de cálculo del alcance del bridge Cisco para calcular la distancia máxima en la que se pueden comunicar dos bridges en base a las combinaciones de antena y cable en uso.

Al igual que con cualquier otro cable de red, los cables de la antena deben estar correctamente instalados para asegurar que las señales que transportan estén limpias y libres de interferencias. Para asegurarse de que los cables rinden de acuerdo a sus especificaciones, es importante evitar lo siguiente:

- **Conexiones flojas** — Los conectores flojos en cualquiera de los extremos del cable producen un contacto eléctrico pobre y degradan la calidad de la señal.
- **Cables dañados** — Los cables de la antena con un daño físico obvio no tienen un rendimiento acorde a las especificaciones. Por ejemplo, el daño puede producir un reflejo inducido de la señal dentro del cable.
- **El cable se extiende junto a los cables eléctricos** — Es posible que la EMI producida por los cables eléctricos afecten la señal en el cable de la antena.
- **Agua en las conexiones del cable** — Es posible que el agua penetre en los conectores que no estén correctamente sellados. Esto causará una degradación severa en la señal RF.

11.4.4 Antena

Línea de Visión y Ubicación de la Antena

En muchas situaciones, la línea de visión [line of sight (LOS)] no es considerada como un problema, en particular para los dispositivos WLAN que se comunican a cortas distancias. Debido a la naturaleza de la propagación de las ondas de radio, los dispositivos con antenas omnidireccionales a menudo se comunican exitosamente de habitación a habitación. La densidad de los materiales usados en la construcción de un edificio determina la cantidad de paredes que la señal RF puede atravesar mientras aun mantiene una cobertura adecuada. El impacto de varios materiales en la penetración de la señal es el siguiente:

- Las paredes de papel y de vinilo tiene poco efecto sobre la penetración de la señal.
- Las paredes de concreto sólido y prefundido limitan la penetración de la señal a una o dos paredes sin degradar la cobertura..
- Las paredes de concreto y de bloques de concreto limitan la penetración de la señal a tres o cuatro paredes.
- La madera o la mampostería permiten una adecuada penetración de la señal para cinco o seis paredes.
- Una pared de metal grueso causa que la señal se refleje, dando por resultado una penetración pobre.
- Un tejido metálico de alambrado con espacios de 2,5 cm a 3,8 cm (1 a 1,5 pulgadas) actúa como una onda de 1,3 cm (0,5 pulgadas) que bloqueará a una señal de 2,4 GHz.

Cuando se conectan dos puntos se debe considerar la distancia entre ellos, las obstrucciones y la ubicación de la antena. Si las antenas pueden ser montadas en interiores y la distancia es corta, se puede usar la antena bipolar estándar o la omnidireccional de 5,2 dBi de montura magnética o la antena Yagi.

Para distancias grandes de 0,8 km (0,5 millas) o más se deben usar las antenas direccionales de alta ganancia como una Yagi o un Plato Parabólico. Estas antenas deben estar tan altas como sea posible, y por sobre las obstrucciones como árboles y edificios. Si se utilizan antenas direccionales, deben estar alineadas para que sus lóbulos principales de potencia irradiada estén dirigidos entre ellas.

La FCC de los EE.UU. requiere una instalación profesional de las antenas direccionales de alta ganancia para sistemas que funcionarán sólo como punto a punto y que tengan una potencia total que excedan los 36

dBm de EIRP. La EIRP es la potencia aparente transmitida hacia el receptor. El instalador y el usuario final son los responsables de asegurar que los sistemas de alta potencia estén funcionando sólo como sistemas punto a punto.

Cuando se diseña un sistema, es importante comprender que si la antena de sitio a sitio fue instalada y probada durante el invierno, pueden ocurrir problemas en la primavera. Durante la primavera, las hojas vuelven a formar un follaje completo y las microondas de baja potencia rebotarán en las hojas como en un espejo cuando estén húmedas. Por lo tanto, una señal fuerte en el invierno puede convertirse en una señal débil en la primavera.

11.5 Registro de Eventos

11.5.1 Configuración de eventos en el AP

Para supervisar los APs y los bridges tan efectivamente como sea posible, es importante configurar los registros. Esta característica puede ser usada para activar y configurar la notificación de eventos fatales, de alerta, de advertencia y de información a destinos externos al AP, como un servidor SNMP o un sistema syslog. Primero se debe configurar la visualización de eventos y la manipulación de eventos. Luego se puede configurar la tecnología o solución de supervisión que mejor convenga a las necesidades de administración.

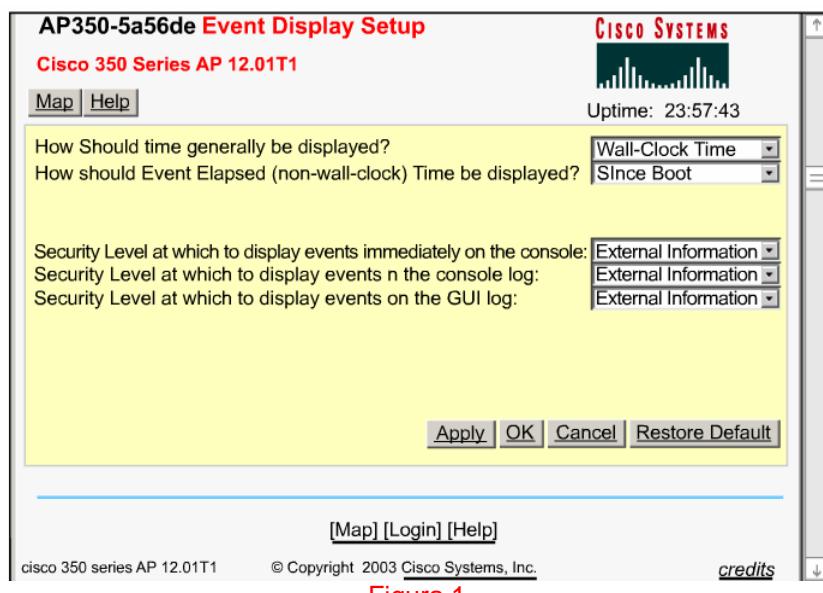


Figura 1

La página de Event Display Setup [Configuración de Visualización de Eventos] mostrada en la Figura 1 puede ser usada para determinar la forma en que se puede mostrar el tiempo en el registro de eventos. También puede ser usada para determinar el nivel de seguridad que es lo suficientemente significativo como para visualizar un evento. Esta página también incluye las siguientes configuraciones:

- ¿Cómo se mostrará en general la hora? Decida si los eventos en el Registro de Eventos son mostrados como tiempo de actividad del sistema u hora del reloj de pared. Si se selecciona el tiempo de actividad del sistema, las horas de los eventos serán mostradas desde el arranque o desde la última vez que el Registro de Eventos fue mostrado. Si se selecciona la hora del reloj de pared, los eventos son mostrados en un formato YY:MM:DD:HH:MM:SS. Si no se ha fijado la hora en el dispositivo, manualmente o por medio de un servidor de tiempo, la visualización de la hora aparece como tiempo de actividad sin importar esta selección.
- ¿Cómo se mostrará el tiempo transcurrido del evento? Elija mostrar el tiempo del evento desde el último arranque o desde el evento ocurrido.
- ¿A qué nivel de severidad se deben visualizar los eventos? Cuando ocurre un evento, puede ser mostrado inmediatamente en la consola, en el registro de la consola, o en el registro de la GUI sólo para ser leído. El evento también puede ser guardado.

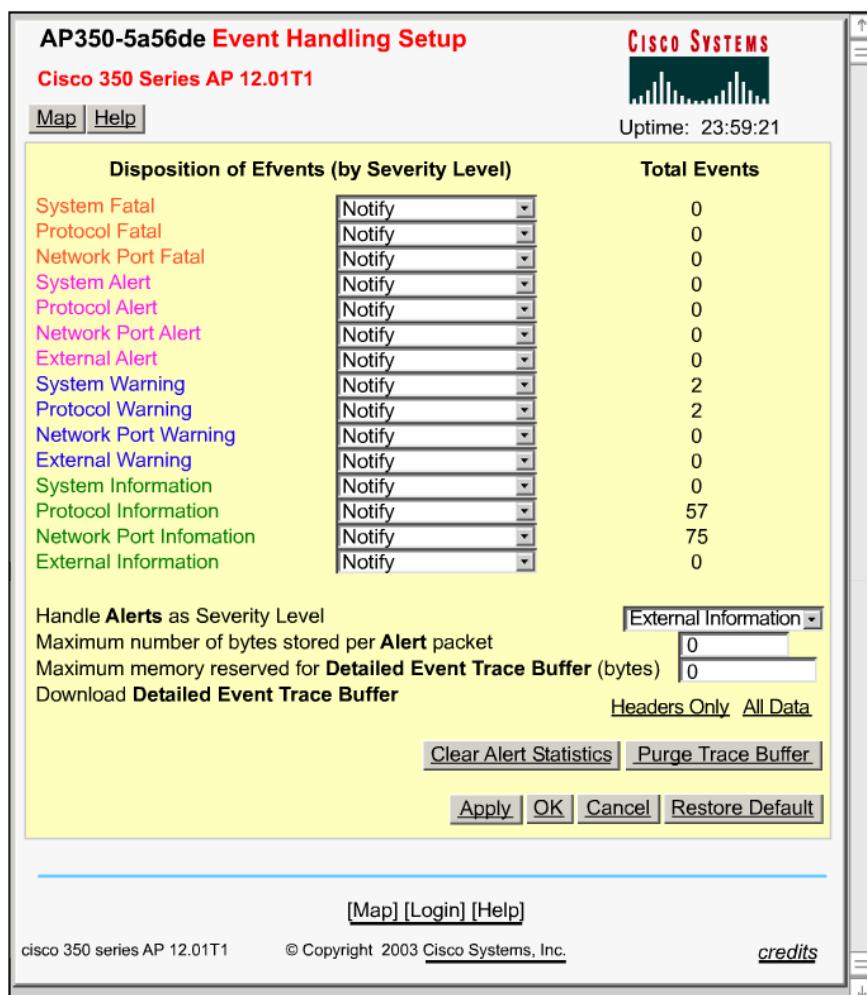


Figura 2

La página Event Handling [Manipulación de Eventos] mostrada en la Figura 2 puede utilizarse para determinar cómo deberá ocurrir la notificación de los diferentes eventos fatales, de alerta, de advertencia y de información. La configuración de los eventos controla cómo el AP manipula los eventos y si son contados, mostrados en el registro, guardado o anunciado en una notificación. Las diferentes configuraciones de eventos son las siguientes:

- Count [Contar] – Contar simplemente cuenta los eventos totales ocurridos en esta categoría sin ninguna forma de notificación o visualización.
- Display console [Consola de visualización] – Esta configuración de eventos proporciona una visualización de sólo lectura del evento pero no lo guarda.
- Record [Guardar] – Esta configuración de evento guarda el evento en el registro y proporciona una visualización de sólo lectura del evento.
- Notify [Notificar] – Esta configuración de evento guarda el evento en el registro, visualiza el evento y ordena al usuario que notifique a alguien dentro de la organización acerca de la ocurrencia.
- Handle Station Alerts as Severity Level [Manipular las Alertas de Estación según el Nivel de Severidad] – Esta configuración de eventos puede ser usada para fijar un nivel de severidad a las alertas del sistema. Utilice los menús desplegables para elegir uno de los once niveles de seguridad. Las alertas indican qué acción se debe tomar para corregir la condición. Las advertencias indican una condición potencial de error. La información es simplemente una notificación de rutina de algún tipo de acción cuando no ha ocurrido ningún error.
- Maximum memory reserved for Detailed Event Trace Buffer [Memoria máxima reservada para el Buffer de Seguimiento Detallado de Eventos] – Esta configuración de eventos puede ser usada para ingresar la cantidad de bytes reservados para el Buffer de Seguimiento Detallado de Eventos. Éste es una herramienta de alto rendimiento para seguir los contenidos de los paquetes entre estaciones específicas en la red.
- Download Detailed Event Trace Buffer [Bajar el Buffer de Seguimiento Detallado de Eventos] – Esta configuración de eventos proporciona un enlace para ver sólo los encabezados o todos los datos en el buffer de seguimiento detallado de eventos. La cantidad de bytes guardados por paquete es

controlada en la página Association Table Advanced Setup [Configuración Avanzada de la Tabla de Asociaciones].

11.5.2 Configuración de la notificación de eventos

Después de que los eventos han sido configurados en el AP o bridge, pueden ser enviados a un servidor de syslog. El syslog es un método usado para recolectar mensajes desde dispositivos en un servidor que corre un daemon syslog. El registro en un servidor syslog central ayuda a administrar los registros y las alertas. Los dispositivos Cisco pueden enviar mensajes de registro a un servicio syslog de UNIX.

The screenshot shows the 'Cisco 350 Series AP 12.01T' configuration interface. At the top, there are 'Map' and 'Help' buttons, and a status bar indicating 'Uptime: 1 day, 00:01:12'. The main area is titled 'Event Notifications Setup'. It includes sections for 'Should Notify-Disposition Events generate SNMP Traps?' (radio buttons for 'yes' or 'no'), 'SNMP Trap Destination' (text input 'test'), 'SNMP Trap Community' (text input 'test'), 'Should Notify-Disposition Events generate Syslog Messages?' (radio buttons for 'yes' or 'no'), 'Should Syslog Messages use the Cisco EMBLEM Format?' (radio buttons for 'yes' or 'no'), 'Syslog Destination Address' (text input '192.168.1.51'), 'Network Default Syslog Destination' (text input '0.0.0.0'), 'Syslog Facility Number' (text input '16'), and 'IEEE SNMP Traps should generate the following notifications:' for three event types, each with dropdown menus for 'Both IEEE Trap and Event Log'. At the bottom are 'Apply', 'OK', 'Cancel', and 'Restore Default' buttons.

Figura 1

Utilice la página Event Notifications Setup [Configuración de Notificaciones de Eventos] mostrada en la Figura 1 para activar y configurar la notificación de eventos fatales, de alerta, de advertencia y de información en destinos externos al AP, como un servidor SNMP o un sistema syslog. Para que las notificaciones de eventos sean enviadas a un destino externo, los eventos deben ser configurados como Notify en la página Event Handling Setup.

11.5.3 Servidor syslog

Un servicio de syslog simplemente acepta mensajes y los almacena en archivos o los imprime de acuerdo a un simple archivo de configuración. Esta es la mejor forma de que los registros estén disponibles para los dispositivos de red porque puede proporcionar un almacenamiento protegido de largo plazo para los registros. Esto es útil tanto para solucionar problemas como para manipular incidentes. Los mensajes son enviados sobre el puerto UDP 514 por defecto.

Las aplicaciones syslog incluyen las siguientes:

- Windows
 - Kiwi
 - Daemon syslog Mikrotik
 - WinSyslog
- Macintosh
 - Netlogger
 - Syslogd
- UNIX
 - Syslogd

11.5.4 SNMP

El SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la suite de protocolos TCP/IP. SNMP permite que los administradores de red administren el rendimiento de la red, encuentren y resuelvan problemas de red y planifiquen el crecimiento de la red.

Una red administrada con SNMP consiste en tres componentes básicos:

- Dispositivos administrados
- Agentes
- Sistemas de administración de la red [Network-management systems (NMSs)]

Un dispositivo administrado es un nodo de la red que está ubicado en una red administrada y que contiene un agente SNMP. Los dispositivos administrados recolectan y almacenan información de administración y hacen que esta información esté disponible para los NMSs usando SNMP. Los dispositivos administrados, que a veces son llamados elementos de red, pueden ser routers y servidores de acceso, switches y bridges, APs, hubs, hosts de computadora o impresoras.

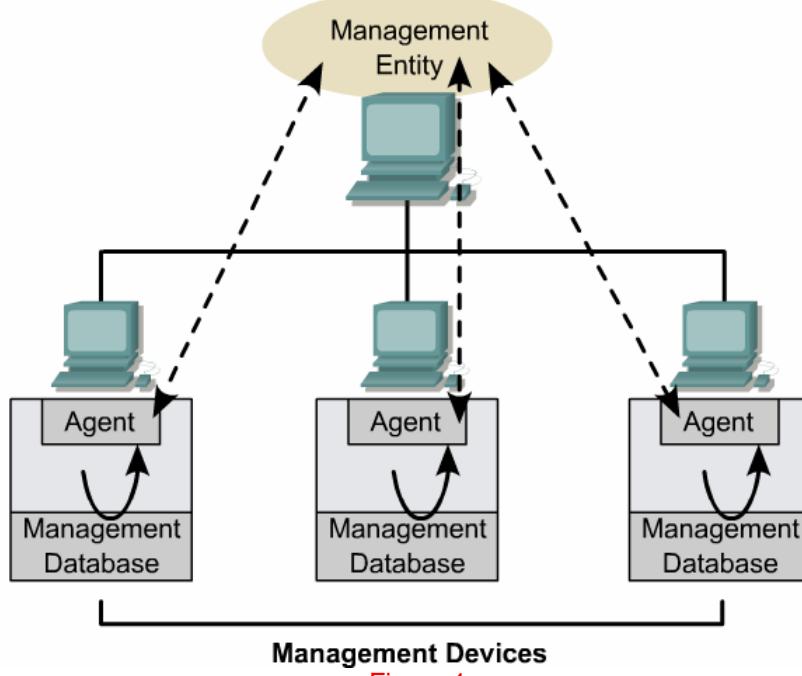


Figura 1

Un agente es un módulo de software de administrador de red que está ubicado en un dispositivo administrado. Un agente tiene conocimiento local de la información de administración y traduce esa información en una forma compatible con SNMP.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. NMSs proporciona la mayor parte de los recursos de procesamiento y memoria requeridos para la administración de la red. Deben existir uno o más NMSs en cualquier red administrada. La Figura 1 ilustra la relación entre estos tres componentes.

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos:

- trap
- read
- write
- traversal operations

El comando trap puede ser configurado en el AP o bridge para que reporte en forma asincrónica los eventos al NMS. Cuando ocurren ciertos tipos de eventos, un dispositivo administrado envía un trap al NMS. Los comandos básicos restantes aun no están integrados a los productos Cisco Aironet.

11.5.5 Configuración del SNMP

Configuración de los Destinos del Trap de SNMP

Utilice la página Event Notifications Setup [Configuración de las Notificaciones de Evento] mostrada en la Figura 1 y la página SNMP Setup [Configuración de SNMP] mostrada en la Figura 2 para configurar el dispositivo para que trabaje con la estación de administración de SNMP de la red.

Figura 1

La página SNMP Setup contiene las siguientes configuraciones:

- Protocolo Simpre de Administración de la Red (SNMP) – Seleccione Enabled para usar el SNMP con el AP.
- System Description [Descripción del Sistema] – El tipo de dispositivo del sistema y la versión actual del firmware.
- System Name [Nombre del Sistema] – El nombre del AP. El nombre en este campo es reportado a la estación de administración del SNMP como el nombre del dispositivo cuando se utiliza SNMP para comunicarse con el AP.
- System Location [Ubicación del Sistema] – Utilice este campo para describir la ubicación física del AP, como el edificio o la habitación en la que está instalado.
- System Contact [Contacto del Sistema] – Utilice este campo para nombrar al administrador del sistema responsable del AP.
- SNMP Trap Destination [Destino del Trap de SNMP] – La dirección IP de la estación de administración del SNMP. Si la red utiliza DNS, ingrese un nombre de host que se traduzca a una dirección IP.
- SNMP Trap Community [Comunidad del Trap de SNMP] – El nombre de la comunidad SNMP requerido por el destino del trap antes de que registre traps enviados por el AP.

Figura 2

Después de que la configuración del SNMP del dispositivo está terminada, se debe instalar una aplicación SNMP. Hay diferentes aplicaciones freeware, demo y software comercial.

11.6 Administración Empresarial

11.6.1 Descripción General

El Motor de Soluciones WLAN [WLAN Solution Engine (WLSE)] está diseñado para la administración empresarial de la WLAN . El WLSE utiliza una GUI basada en web para realizar la supervisión de cambios de configuración, seguridad, cuentas, fallos y rendimiento en una gran cantidad de APs y bridges . WLSE proporciona una configuración centralizada basada en plantillas con grupos de dispositivos definidos por el usuario para configurar en forma efectiva una gran cantidad de APs y bridges. El WLSE puede administrar cientos de dispositivos inalámbricos sobre una LAN o a través de múltiples LANs.

El WLSE supervisa al servidor de autenticación del Protocolo de Autenticación Extensible Ligero [Lightweight Extensible Authentication Protocol (LEAP)] y mejora aun más la administración de seguridad detectando configuraciones erróneas en APs y bridges. El WLSE también supervisa la infraestructura de la WLAN y genera notificaciones para la no disponibilidad y la degradación del rendimiento. El WLSE CiscoWorks ayuda en el planeamiento de la capacidad identificando los APs más utilizados y acelerando la solución de problemas del cliente al generar reportes de asociación de clientes. El WLSE es una solución especializada que corre en el hardware Cisco 1105.

El conjunto de características del WLSE proporciona una solución de administración de red para las redes empresariales como las de servicios financieros, asistencia médica, instituciones gubernamentales, venta minorista, educación y manufactura. Las actividades de demostración en esta sección mostrarán las características principales del WLSE y cómo administrar con el WLSE.

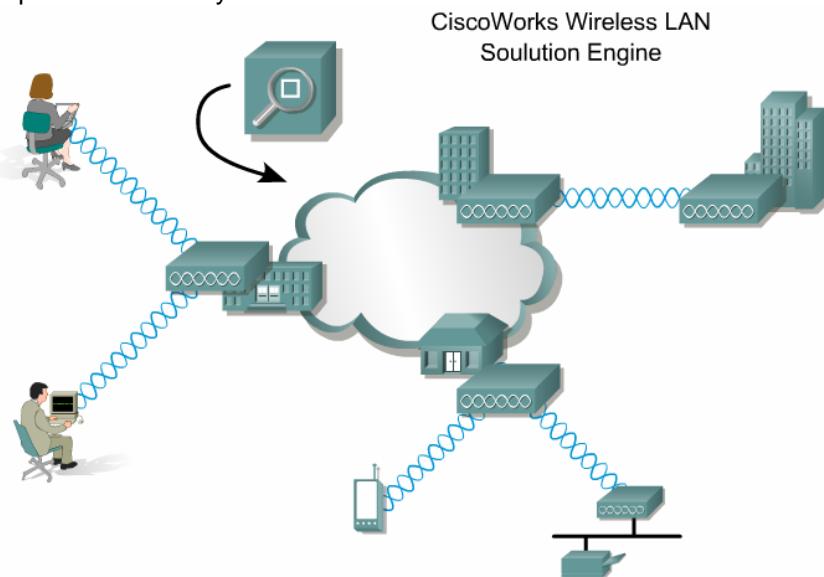


Figura 1



Figura 2

11.6.2 Mobile Manager de Wavelink

Wavelink es un desarrollador de soluciones inalámbricas para desplegar y administrar aplicaciones e infraestructuras inalámbricas empresariales. Las empresas con múltiples sitios no desean poner a un experto en redes en cada uno de ellos. La administración centralizada elimina la necesidad de hacer esto. El detectar y resolver los problemas de la WLAN automáticamente aumenta el rendimiento y la eficiencia

general. Es difícil mantener la consistencia del firmware mientras se expande la WLAN. Si se despliega una WLAN sobre el tiempo, la versión del firmware de los APs es probable que cambie.

Mobile Manager™ es el producto de Wavelink usado para desplegar y administrar los APs de la WLAN. 1 El Mobile Manager de Wavelink puede ser usado para fijar el firmware de la WLAN de la empresa y supervisar su consistencia. Las WLANs pueden incluir APs y clientes móviles de diferentes fabricantes. Wavelink puede administrar una red WLAN de múltiples fabricantes.

En un entorno Cisco, el Mobile Manager toma ventaja del broadcast de CDP que los APs Cisco Aironet transmiten tan pronto como entran en línea. Después de tomar este broadcast, un agente Mobile Manager auto-descubrirá el AP y asignará configuraciones predefinidas. Muchos APs Cisco Aironet son instalados en entornos comunitados de Cisco. El Mobile Manager está diseñado para detectar APs y switches y routers Cisco para crear un mapa topográfico de la red completa. Este mapa incluye switches, routers, APs y una tabla de las direcciones MAC de los clientes móviles asociados a cada AP.

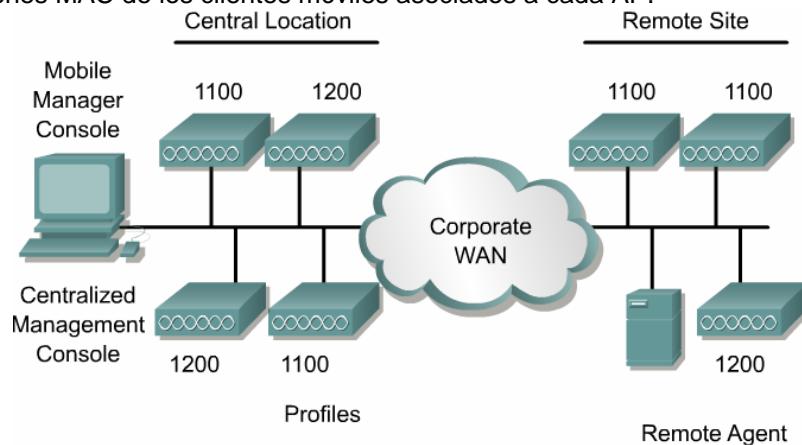


Figura 1

Mobile Manager es una solución de software. La consola y el agente del Mobile Manager correrán sobre cualquier máquina con Windows. Los perfiles contienen parámetros de configuración del AP y pueden ser asignados en forma automática a medida que nuevos APs son puestos en línea. Los perfiles del Mobile Manager facilitarán el despliegue de nuevos APs. El Mobile Manager tiene cuatro componentes 2:

- Consola de Administración
- Servicio de Alerta
- Agente Remoto
- Servicios Remotos

Management Console
Shows the entire wireless network topology
Organizes the network into regions
Displays alerts real time
Gives the exact status of any wireless device
Alert Service
Generates alerts in real-time
Fowards alerts to e-mail, pager, and alternative console
Divines fault, performance, and security thresholds
Remote Agent
Provides continuous real-time monitoring of wireless components
Deploys settings defined by the administrator
Proactively responds to error conditions with rules-based reasoning
Remote Services
Automatically upgrades or rolls back firmware
Logs statistical records
Optional DHCP server

Figura 2

Resumen

Este módulo habló sobre los fundamentos básicos de la solución de problemas. Después de una explicación y de actividades de laboratorio para documentar el proceso de solución de problemas, el alumno debería estar familiarizado con el enfoque sistemático para la solución de problemas. Este enfoque minimiza la confusión y acorta el tiempo que de otra forma se perdería con la solución de problemas a prueba y error.

Luego, se presentaron una variedad de herramientas que son usadas para solucionar problemas en una WLAN. Los alumnos conocieron cosas como probadores de cables, que están diseñados para verificar la conectividad de todos los tipos de cables de LAN. También aprendieron acerca de los analizadores del espectro, otra herramienta común usada por los profesionales de redes. El analizador del espectro es la mejor herramienta para determinar si hay actividad en la frecuencia.

Finalmente se presentó el WLSE. Este software permite una administración efectiva de la WLAN empresarial. El WLSE utiliza una GUI basada en la Web para supervisar los cambios de configuración, seguridad, cuentas, fallos y rendimiento de una gran cantidad de APs.

Módulo 12: Tecnologías que emergen

Descripción General

Los módulos anteriores hablaron sobre los estándares y tecnologías inalámbricas actuales, incluyendo los productos inalámbricos Cisco Aironet y cómo configurarlos. En este módulo, el lector aprenderá sobre las tecnologías inalámbricas emergentes, tanto fijas como móviles. Por ejemplo, las tecnologías de banda ultra ancha permitirán que los usuarios disfruten un amplio rango de aplicaciones, las que utilizan altas velocidades de transferencia de datos. Luego, el módulo hablará sobre la historia de la Voz sobre IP (VoIP) y los avances que ofrece a los usuarios.

Finalmente, el módulo hablará sobre las diferentes organizaciones y certificaciones de la industria inalámbrica y proporcionará diversos casos de estudio de implementaciones inalámbricas.

12.1 Tecnología Inalámbrica de Banda Ultra Ancha

12.1.1 Descripción general de la tecnología inalámbrica de banda ultra ancha [ultra-wideband (UWB)]

Imagine la libertad de usar un reproductor de DVD en una habitación para mirar una película en otra habitación diferente. Imagine usar un controlador para mirar diferentes programas en diferentes televisores. Imagine conectar una cámara digital a un televisor sin cables y sin línea de visión (LOS). Gracias a la tecnología inalámbrica emergente de banda ultra ancha (UWB), los consumidores pronto podrán disfrutar una amplia variedad de aplicaciones, las que pueden utilizar velocidades muy altas de transferencia de datos, como se muestra en la Figura 1.

Ultra-wideband Wireless Definition

Any wireless transmission scheme that occupies a bandwidth of more than 25 percent of a center frequency, or more than 1.5 GHz.

Figura 1

Marconi usó transmisores de separación de contactos para enviar corrientes de pulsos de código Morse a través de la habitación del laboratorio sin cables. En 1901, después de elevar la potencia y construir antenas mucho más grandes, el pionero de la radio usó el dispositivo para transmitir señales inalámbricas codificadas a través del Océano Atlántico. Un siglo después, los investigadores una vez más proyectaron pequeños pulsos electromagnéticos a través de sus laboratorios. Con el paso de los años, la tecnología ha cambiado. Las bobinas y capacitores voluminosos han sido reemplazados por pequeños circuitos integrados y diodos de túnel. En lugar de corrientes irregulares y erráticas, ahora hay secuencias cronometradas con precisión de pulsos de formas especiales que duran sólo unos pocos cientos de trillónésimas de segundo. Y mientras que los dispositivos de Marconi podían cubrir el equivalente a casi 10 bits de datos por segundo, la UWB puede enviar más de 100 millones de bits de información digital en la misma cantidad de tiempo.

La tecnología UWB se define en términos generales como cualquier esquema de transmisión inalámbrico que ocupa un ancho de banda de más del 25 por ciento de una frecuencia central, o más de 1,5 GHz. Los primeros productos para consumidores que usan chips UWB se esperan para fines del 2003.

Los primeros sistemas UWB deberían poder proporcionar un ancho de banda en el rango de 40 a 60 Mbps, con expectativas de velocidades muy altas de transmisión de datos, de 100 a 500 Mbps, a través de distancias de 5 a 10 m (16,4 a 32,8 pies). Eventualmente, la UWB incluso podría llegar a velocidades de datos en el rango de 1 Gbps, y alcanzar distancias de hasta 2 km (1,2 millas). Esta tecnología conducirá a aplicaciones inalámbricas que actualmente son imposibles. Los ingenieros también esperan que las unidades UWB sean más baratas, más pequeñas y menos dependientes de la energía que los dispositivos de radio actuales.

12.1.2 Aplicaciones UWB

Con raíces en aplicaciones militares, como imágenes de radar de avión a través de árboles, es más probable que la UWB sea usada para comunicaciones inalámbricas a distancias cortas.

Los dispositivos UWB envían y reciben transmisiones de alta velocidad a distancias relativamente cortas. Los dispositivos UWB pueden ser usados para proporcionar conectividad en WLANs hogareñas y de oficina, y puede proporcionar conexiones de corta distancia entre dispositivos móviles como teléfonos celulares, pagers y computadoras de mano.

Además de las comunicaciones, la tecnología UWB tiene otras aplicaciones significativas. Depende de pulsos delgadísimos cronometrados con precisión, similares a los usados en las aplicaciones de radar. Estos pulsos le dan a la tecnología inalámbrica UWB la capacidad de detectar objetos enterrados o movimiento detrás de las paredes. Estas capacidades podrían ser importantes para misiones de rescate y de imposición de la ley.

Los pulsos de precisión de la UWB también pueden ser usados para determinar la posición de emisores de interiores. Al funcionar como una versión local del Sistema de Posicionamiento Global (GPS), un sistema inalámbrico UWB puede triangular la ubicación de objetos marcados con transmisores, usando múltiples receptores ubicados en la vecindad. Esta capacidad podría ser muy útil para el personal de tiendas departamentales, para vigilar productos de gran valor en las estanterías o en el depósito. Esta característica de búsqueda de ubicación también podría ser usada para mejorar la seguridad. Por ejemplo, los receptores de UWB instalados en cerraduras inteligentes o máquinas ATM podrían permitirles funcionar sólo cuando un usuario autorizado esté dentro del radio de un metro (3,3 pies) del dispositivo. Los usuarios autorizados podrían llevar un transmisor UWB como identificación.

La tecnología UWB utiliza pulsos de corta duración que se lanzan como dardos alrededor de otro tráfico, atravesando las mismas ondas del aire. Como resultado, UWB puede trabajar a través del espectro que ya está ocupado por otros servicios de radio. Esta tecnología funciona bien en edificios y en otros ambientes densos porque utiliza los reflejos de la señal desde las paredes y otros objetos sólidos para enviar datos.

12.1.3 Aceptación de la UWB

En Febrero de 2002, la Comisión Federal de Comunicaciones (FCC) de los EE.UU. autorizó el uso comercial limitado de los dispositivos de comunicaciones inalámbricas UWB. Los tipos de operaciones que están actualmente aprobadas están enumeradas en la Figura 1. La aprobación en Europa y Asia se espera pronto.

- Per the U.S. FCC regulations, UWB devices can be used for the following:**
- Precise measurement of distances or locations
 - Obtaining the images of objects buried under ground or behind surfaces
 - Wireless communications, particularly for short-range, high-speed data transmissions

Figura 1

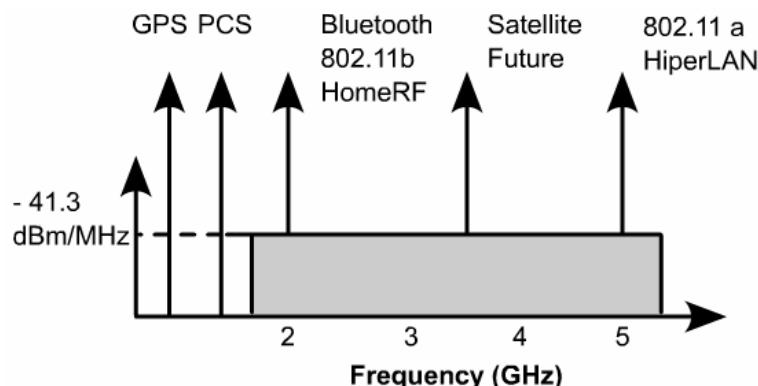


Figura 2

La FCC de los EE.UU. actualmente está trabajando en fijar límites de emisión que permitiría a los sistemas de comunicaciones UWB ser utilizados sin licencias, siguiendo las reglas para las emisiones emitidas por radiadores intencionales. ²Estas son las mismas reglas que gobiernan las emisiones emitidas por las computadoras hogareñas. Este cambio de reglas permitiría a los dispositivos con UWB activado cubrir a los sistemas existentes de banda angosta, que actualmente no están permitidos. Esto podría dar por resultado un uso mucho más eficiente del espectro disponible. Los dispositivos podrían llenar las porciones no usadas del espectro de frecuencias en cualquier lugar en particular.

Tomando un enfoque conservador, la FCC de los EE.UU. eligió restringir el uso del espectro de radio UWB de 3,1 a 10,6 GHz. Esto se aplica a las aplicaciones de comunicaciones UWB con una potencia de radiación incidental completa. La FCC de los EE.UU. espera que esto esté bastante alejado de la banda de 1 6 GHz que es usada para las comunicaciones GPS. Afuera de la banda de 3,1 a 10,6 GHz, las señales deben ser atenuadas a 12 decibeles (dB), necesitándose una atenuación de 34 dB en áreas cercanas a las bandas de frecuencia GPS.

Restricciones más liberales fueron creadas para el personal policial y de seguridad pública que usan unidades UWB para buscar víctimas de terremotos u otras personas perdidas.

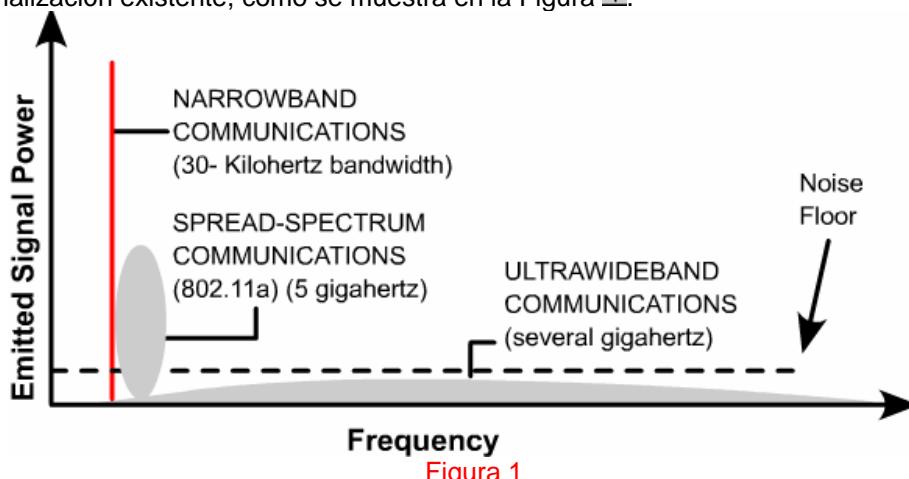
12.1.4 Interferencia

Existen algunas preocupaciones con respecto a que los dispositivos UWB interferirán con los servicios de radio y con el funcionamiento del GPS. A causa de esto, la regulación de la FCC de los EE.UU. del uso comercial de la tecnología UWB está acompañada por una lista de estándares estrictos para el uso y conformidad del dispositivo.

Grupos tan diversos como la Asociación de Transporte Aéreo de Norteamérica, Nortel, Nokia y Qualcomm se han unido contra la propuesta de ampliar el uso de la UWB. Estos grupos dicen que la UWB interferirá con las frecuencias GPS y con las redes inalámbricas de seguridad pública y seguridad aérea. En este momento, las pruebas al respecto no han sido concluyentes.

Como los pulsos UWB emplean las mismas frecuencias que los servicios de radio convencionales, potencialmente pueden interferir con ellos. Las estaciones de separación de contactos de Marconi usaban una gran cantidad de potencia porque necesitaban cubrir grandes distancias. En el entorno regulatorio actual, los sistemas como el de Marconi deberían ser intolerables, porque interferirían con casi todas las otras tecnologías de radio. Los sistemas de comunicación UWB funcionan a niveles de potencia tan bajos que emiten menos energía de radio como subproducto que una computadora laptop. Por ejemplo, un transmisor UWB de 200 microwatts irradia sólo 1/3000 de la energía promedio emitida por un teléfono celular convencional de 600 milliwatts.

A diferencia de los sistemas de comunicaciones tradicionales, la tecnología inalámbrica UWB ocupa un amplio rango de frecuencias a niveles muy bajos de energía, a menudo por debajo del piso de ruido del entorno de señalización existente, como se muestra en la Figura 1.



Esta salida de baja potencia también significa que el alcance de la UWB está nítidamente restringido a distancias de 100 m (328 pies) o menos, y a veces a menos de 10 m (32,8 pies).

12.1.5 Evitar la interferencia de otros dispositivos

El problema técnico más desafiante asociado con el uso de la UWB, es encontrar formas de evitar que otros emisores interfieran con los dispositivos UWB. Otros sistemas de radio tienen una fuerte ventaja en esta área. Todos los otros sistemas tienen un filtro frontal que evita la interferencia de transmisores que trabajan fuera de sus bandas de recepción. Desafortunadamente, un receptor UWB necesita tener un filtro frontal abierto para permitir un amplio espectro de frecuencias, incluyendo señales de fuentes potenciales de interferencia. La habilidad para vencer este impedimento, que a veces recibe el nombre de resistencia al atascamiento, es un atributo clave de un receptor de UWB bien diseñado. Un enfoque para mejorar la

resistencia al atascamiento es instalar filtros de ranura, que buscan y disminuyen las señales de fuentes particularmente fuertes de interferencia de banda angosta.

Interferencia Multiruta

La interferencia multiruta, como se habló en el Módulo 4, también es un problema. Sin embargo, un diseño inteligente puede permitir a los sistemas UWB tomar ventaja de este fenómeno. Los pulsos angostos de las streams UWB hacen posible que algunos receptores resuelvan las streams multiruta separadas y simultáneamente que se acoplen a las distintas señales reflejadas. Luego una comparación en tiempo casi real determina si un bit recibido es un cero o un uno. Esta función de control de bit en realidad mejora el rendimiento del receptor.

12.1.6 Especificaciones de la UWB

UWB permite que un sistema trabaje a través de un rango de bandas de frecuencias sin interferir con los sistemas de comunicaciones existentes. Esto es porque UWB utiliza una potencia de transmisión muy baja. Los pulsos UWB a menudo se miden en picosegundos. Un picosegundo representa a una trillonésima de segundo. UWB aun puede mantener una velocidad de datos alta porque trabaja en el dominio temporal en lugar de en el dominio de las frecuencias. Las señales UWB consisten en pulsos electromagnéticos de alta velocidad, en lugar de ondas sinusoidales. Esto permite que las ondas atravesen muchas frecuencias sin impedimentos y sin ser notadas.

A causa de su duración extremadamente corta, estos pulsos UWB trabajan en una banda continua de frecuencias, la que puede extenderse a varios gigahertz. Como se muestra en la Figura 1, cuanto más corto es el pulso en el tiempo, más amplia es la frecuencia central, y más amplia la extensión de su espectro de frecuencias.

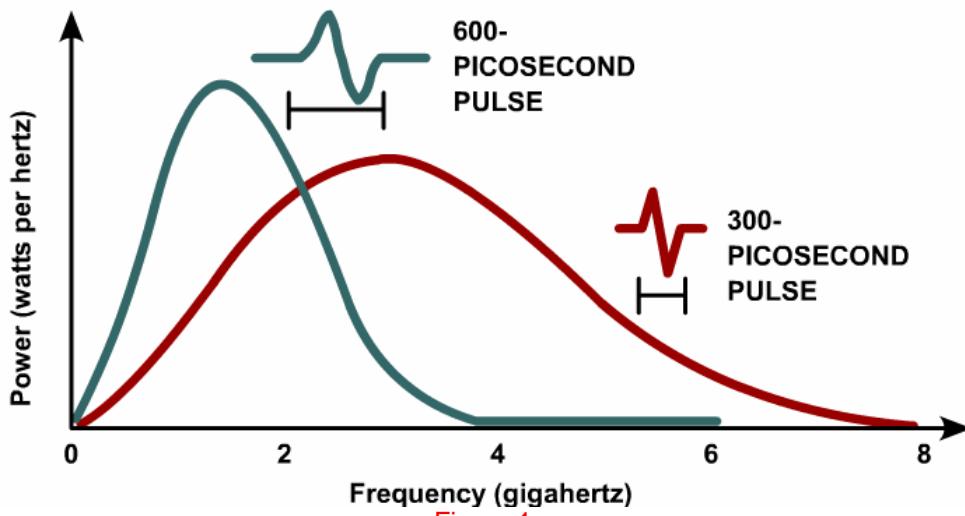
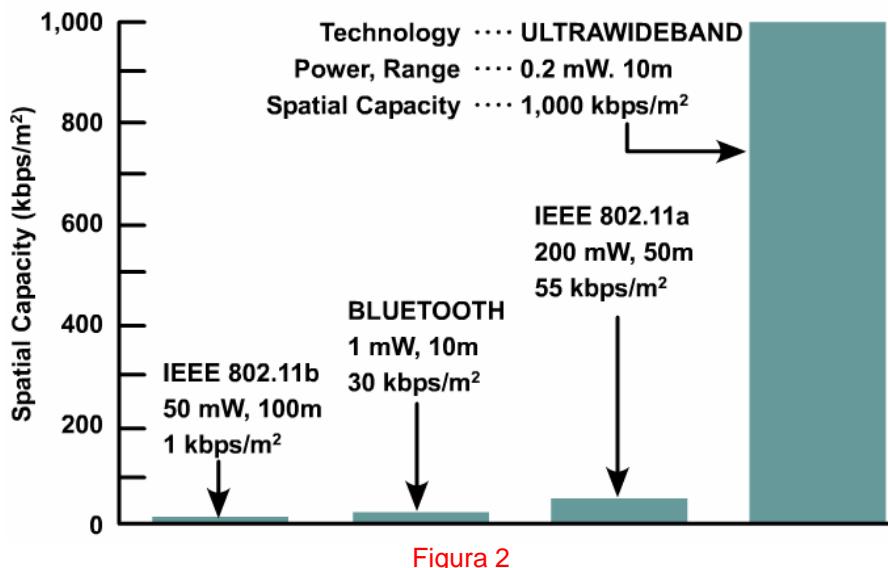


Figura 1

Capacidad Espacial

UWB es superior en otros aspectos a otros esquemas inalámbricos de corto alcance. La demanda creciente de mayores capacidades de datos inalámbricos y la población del espectro RF favorecen a los sistemas que ofrecen velocidades altas de bits concentradas en áreas físicas pequeñas. Esta métrica recibe el nombre de capacidad espacial. Medida en kilobits por segundo por metro cuadrado (Kbps/m^2), la capacidad espacial es un cálculo de la intensidad de los datos, casi de la misma forma en que los lumens por metro cuadrado pueden ser usados para determinar la intensidad de la iluminación de una fuente luminosa. A medida que aumente la cantidad de usuarios de banda ancha reunidos en espacios llenos de gente como aeropuertos, hoteles, centros de convenciones y lugares de trabajo, el parámetro más crítico de un sistema inalámbrico será su capacidad espacial. La tecnología UWB sobresale en capacidad espacial, como lo ilustra la Figura 2.



Modulación UWB – Radio sin Portadora

La tecnología inalámbrica UWB es diferente a las formas familiares de comunicaciones de radio, como la AM/FM, la radio de la policía/bomberos y la televisión. Estos servicios de banda angosta, que evitan interferir entre sí permaneciendo en los confines de sus bandas de frecuencias asignadas, usan todos una onda portadora. La información es estampada sobre la señal portadora subyacente por algún tipo de modulación de su amplitud, frecuencia o fase. La información es extraída, o demodulada, al ser recibida. Esto se muestra en la Figura 3.

Narrowband Transmissions

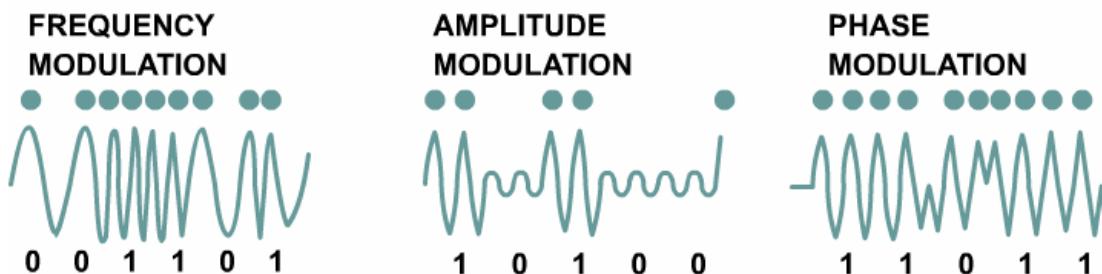


Figura 3

La tecnología UWB es única. En lugar de emplear una señal portadora, las emisiones UWB están compuestas por una serie de pulsos intermitentes. Al variar la amplitud, polaridad, cronometraje u otras características de los pulsos individuales, la información es codificada en una corriente de datos. En un esquema de modulación bipolar, un dígito uno representa un positivo, o pulso ascendente, mientras que un cero representa un pulso invertido o descendente. En la modulación por amplitud, los pulsos con amplitud completa representan los unos y los pulsos con media amplitud representan los ceros. La modulación por posición del pulso envía pulsos idénticos pero altera el cronometraje de la transmisión. Los pulsos retardados indican ceros. Estas técnicas de modulación se muestran en la Figura 4.

Wideband Transmissions

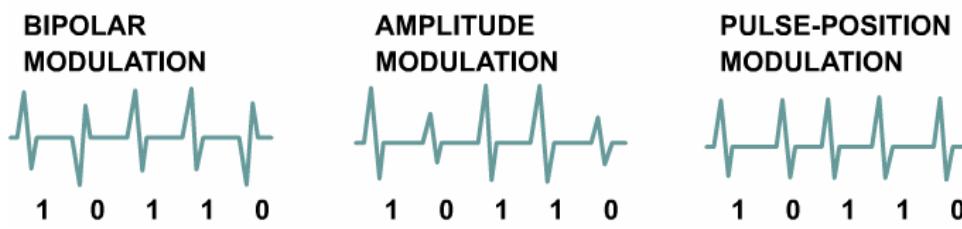


Figura 4

Se han usado otros términos distintos para denominar al modo de transmisión UWB en el pasado, incluyendo sin portadora, banda base y basado en impulso.

Va Bajo y Corto

Hay una tendencia creciente a enviar señales de baja potencia sobre alcances cortos. Antes de 1980, durante los primeros días de la radiotelefonía, una única torre con un transmisor de alta potencia podía cubrir una ciudad entera. Sin embargo, a causa de la disponibilidad limitada del espectro, esa única torre no podía dar servicio a muchos usuarios. En 1976, los proveedores de radiotelefonía de la Ciudad de Nueva York podían administrar sólo 545 usuarios de teléfonos móviles al mismo tiempo. Este es un número extremadamente pequeño para los estándares actuales. La telefonía celular podía alojar a una gran cantidad de usuarios reduciendo drásticamente la potencia y la distancia. Esto permite que el mismo espectro sea reutilizado muchas veces dentro de un área geográfica. Ahora se espera que la UWB haga lo mismo para las WLANs.

12.2 VoIP y Voz sobre WLANs

12.2.1 Descripción general de la voz sobre IP (VoIP)

En la década pasada, la industria de las telecomunicaciones ha sido testigo de los rápidos cambios en la forma en que la gente y las organizaciones se comunican. Muchos de estos cambios vienen del crecimiento explosivo de la Internet y de aplicaciones basadas en el IP. La Internet se ha convertido en un medio popular de comunicación, y la cantidad total de tráfico de red basado en paquetes ha superado rápidamente al tradicional tráfico de red de voz, o de circuitos commutados.

Se espera que el tráfico de voz se convierta en una de las próximas mayores áreas de aplicación que aproveche la ventaja del IP. Esta expectativa se basa en el impacto de las tecnologías VoIP, que a veces se las conoce como telefonía IP. La Figura 1 ilustra algunas de las formas en que se puede usar VoIP.



Figura 1

VoIP ofrece muchos beneficios, que incluyen los siguientes:

- Ahorro de costos – Al pasar el tráfico de voz a las redes IP, las compañías pueden reducir o eliminar los costos asociados al transporte de llamadas sobre la Red Pública de Telefonía Comutada (PSTN). Los proveedores de servicios y los usuarios finales también pueden conservar el ancho de banda invirtiendo en capacidad adicional sólo cuando sea necesario. Esto es posible gracias a la naturaleza distribuida de la VoIP y a los costos reducidos de las operaciones cuando las compañías combinan el tráfico de voz y de datos en una sola red.
- Estándares abiertos – Al adoptar estándares abiertos, se asegura la interoperabilidad de múltiples fabricantes. Tanto los proveedores de servicios como los empresarios pueden comprar equipos de distintos fabricantes y eliminar su dependencia a soluciones propietarias.
- Redes integradas de voz y datos – Cuando la voz se convierte en otra aplicación IP, las compañías pueden construir redes verdaderamente integradas para voz y datos. Estas redes integradas proporcionan la misma calidad y confiabilidad que la PSTN, mientras que permiten que las compañías tomen ventaja rápida y flexiblemente de nuevas oportunidades dentro del mundo cambiante de las comunicaciones.

En 1995, los primeros productos comerciales de VoIP comenzaron a aparecer en el mercado. Estos productos apuntaban a compañías que deseaban reducir sus costos de telecomunicaciones pasando el tráfico de voz a la red de paquetes. Los primeros en adoptar redes VoIP construyeron soluciones para evitar

costos y tomar ventaja del tratamiento regulatorio favorable del tráfico IP. Sin estándares establecidos, la mayor parte de las primeras implementaciones estaban basadas en tecnología propietaria.

A medida que las redes telefónicas de paquetes crecían y aparecían dependencias de interconexión, se hacía claro que la industria necesitaba protocolos VoIP estándares. Existen cuatro protocolos estandarizados diferentes de señalización y control de llamadas que se usan para VoIP:

- H.323
- Protocolo de Control de Gateway de Medios [Media Gateway Control Protocol (MGCP)]
- Protocolo de Inicio de Sesión [Session Initiation Protocol (SIP)]
- H.248/Megaco

Otros protocolos que funcionan con estos protocolos de señalización y control son el Protocolo de Transporte en Tiempo Real [Real-time Transport Protocol (RTP)], el Protocolo de Control de Transporte en Tiempo Real [Real-time Transport Control Protocol (RTCP)], y el Protocolo de Reserva de Recursos [Resource Reservation Protocol (RSVP)].

Cada uno de estos protocolos será tratado en las siguientes secciones.

12.2.2 Componentes de la VoIP

VoIP permite que un dispositivo de red transporte tráfico de voz sobre una red IP. En VoIP, un procesador de señales digitales (DSP) segmenta la señal de voz y la almacena en paquetes de voz. Estos paquetes de voz son transportados usando IP. Como las aplicaciones multimedia son sensibles a los retardos, se necesita una red bien planificada de extremo a extremo para poder usar con éxito VoIP, como lo muestra la Figura 1. La adecuación de una red para que soporte VoIP comprende una serie de protocolos y características para mejorar la calidad del servicio (QoS). También debe tenerse en cuenta el formateo del tráfico para asegurar la confiabilidad de la conexión de voz.

Los componentes principales de una red VoIP son similares a los de una red de circuitos commutados. Además de conectar a los usuarios a la PSTN, las redes VoIP deben realizar todas las tareas de la PSTN. Hay tres componentes principales en una red VoIP:

- Gateways de medios
- Controladoras de gateways de medios
- La red IP

Es importante comprender que la terminología no siempre se utiliza en forma consistente, en especial en el caso de las tecnologías emergentes. Esta sección presenta los términos más usados, pero también se podrían usar otros términos.

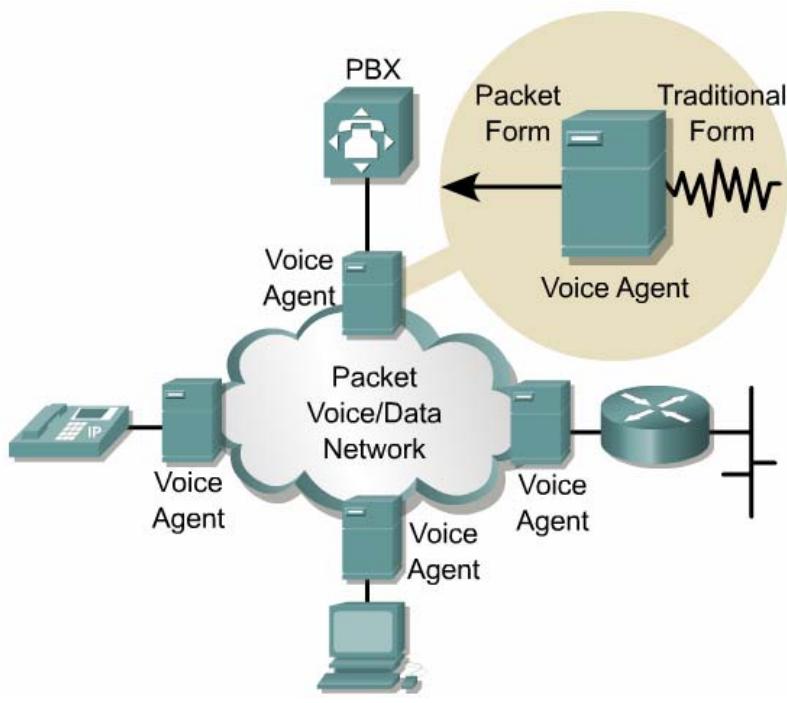


Figura 1

Gateway de Medios

Los gateways de medios tienen la responsabilidad de originar la llamada, detectar la llamada, convertir la voz de analógica a digital y crear paquetes de voz, o realizar las funciones de compresión-descompresión (codec). Los gateways de medios también tienen características opcionales, como compresión de voz, cancelación del eco, supresión del silencio y recolección de estadísticas. El gateway de medios forma la interfaz para voz en la red IP. Cada llamada es normalmente una sesión IP única que es transportada por un RTP sobre el Protocolo de Datagrama del Usuario (UDP).

Los gateways de medios pueden ser equipos de telecomunicaciones dedicados o una PC genérica que esté ejecutando un software de VoIP. Algunas características y servicios adicionales soportados incluyen funciones como hacer trunking al PSTN, proveer una interfaz analógica a digital de Central Telefónica Privada (PBX), o integrar una PBX sencilla. El gateway de medios también puede ser usado como una unidad telefónica IP, y puede recibir el nombre de Agente de Voz.

Controladora de Gateway de Medios

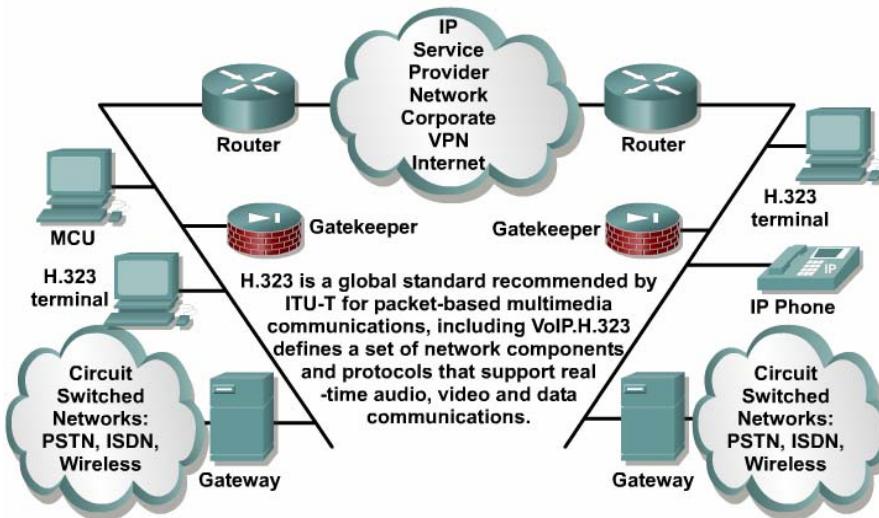


Figura 2

Las controladoras de gateway de medios contienen los servicios de señalización y de control que coordinan las funciones del gateway de medios, como lo muestra la Figura 2. La controladora de gateway de medios es la responsable de algunos o todos los servicios de coordinación de señalización, traducción del número telefónico, búsqueda de hosts, administración de recursos e interfaz con el Sistema de Señalización 7 (SS7) del PSTN.

En una red VoIP escalable, dos dispositivos pueden realizar las funciones de la controladora. El primero es una controladora de gateway de señalización y el segundo es una controladora de gateway de medios. Si una llamada se origina y termina dentro de la misma red VoIP, una controladora de gateway de medios puede ser el único dispositivo necesario para completar la llamada. Sin embargo, una red VoIP está conectada con frecuencia al PSTN. La controladora de señalización estaría dedicada a la traducción del mensaje y a la señalización necesaria para conectarse al PSTN.

La controladora de señalización también recibe el nombre de agente de llamada en una arquitectura centralizada. Es conocida como un gatekeeper en una red H.323 y como un servidor proxy o de redirección en una red SIP.

La definición de softswitch ha causado alguna confusión. El Consorcio Internacional de Softswitch limita el término softswitch a la controladora de gateway de medios. Algunos fabricantes incluyen al gateway de medios o al gateway de señalización como parte del softswitch. En el nivel más básico, un softswitch es un software de controladora de gateway de medios que proporciona el control de llamada y la administración de recursos para un gateway de medios. Los softswitches realizarán una función significativa en los servicios de convergencia.

Red IP

Es posible ver a la red VoIP como un switch lógico. Sin embargo, este switch lógico es un sistema distribuido más que un switch único. El backbone de IP proporciona conectividad entre los elementos distribuidos. Este sistema completo es a veces llamado en forma colectiva arquitectura de softswitch.

El diagrama de flujo en esta sección muestra los eventos que ocurren cuando se realiza una llamada usando VoIP y H.323 o SIP.

12.2.3 Arquitecturas VoIP centralizadas y distribuidas

Uno de los beneficios de la tecnología VoIP es que permite que las redes sean construidas usando una arquitectura centralizada o distribuida. En general, las arquitecturas centralizadas están asociadas con los protocolos MGCP y H.248/Megaco. Estos protocolos fueron diseñados para un dispositivo centralizado conocido como controladora de gateway de medios, o un agente de llamada que manipula la lógica de la conmutación y el control de llamadas. El dispositivo centralizado se comunica con los gateways de medios, los que enrutan y transmiten el audio y la parte de medios de las llamadas. En las arquitecturas centralizadas, la inteligencia de la red está centralizada y los puntos finales tienen relativamente poca inteligencia.

Las arquitecturas distribuidas están asociadas con los protocolos H.323 y SIP. Estos protocolos permiten que la inteligencia de la red esté distribuida entre los puntos finales y los dispositivos de control de llamadas. En las arquitecturas distribuidas, se llama inteligencia al estado de llamada, las características de llamada, el enrutamiento de llamada, abastecimiento, facturación, o cualquier otro aspecto de la manipulación de llamada.

Los puntos finales pueden ser gateways VoIP, teléfonos IP, servidores de medios o cualquier dispositivo que pueda iniciar y terminar una llamada VoIP. Los dispositivos de control de llamada son llamados gatekeepers en una red H.323, y servidores proxy o redirectores en una red SIP.

Existen muchos protocolos que son usados para VoIP. Las siguientes secciones describirán lo más importante de estos protocolos, algunos de los cuales se muestran en la Figura 1.

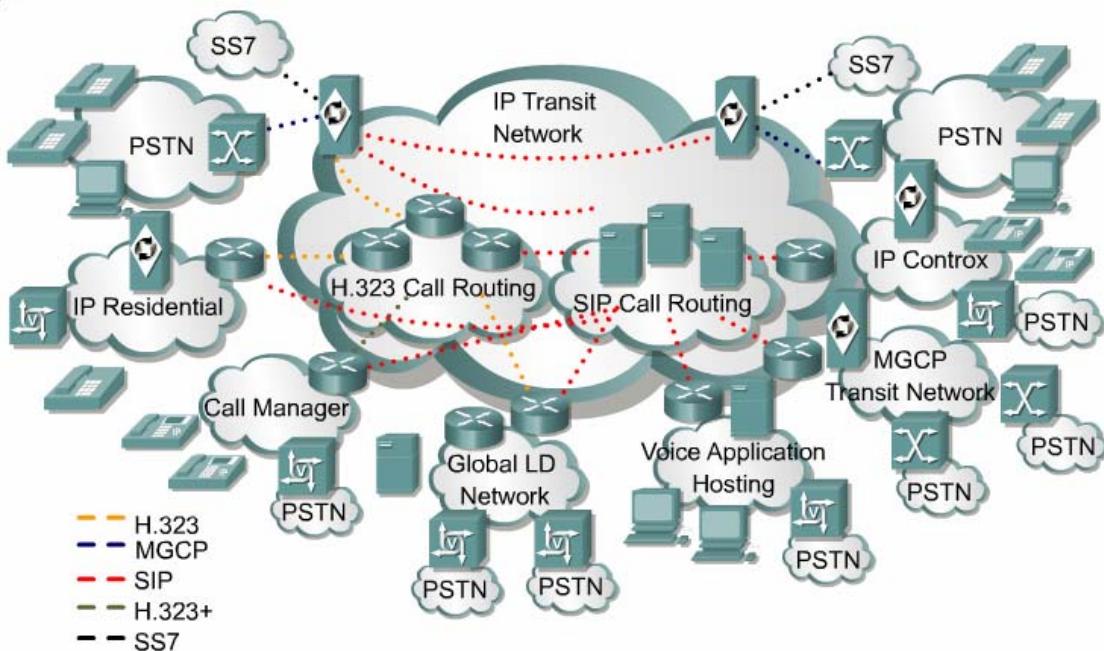


Figura 1

12.2.4 El protocolo marco de ITU-T: H.323

H.323 es un estándar de la Unión Internacional de Telecomunicaciones-Telecomunicaciones (ITU-T) que define a un sistema de comunicaciones multimedia basado en paquetes. H.323 define a una arquitectura distribuida para transportar aplicaciones multimedia sobre LANs. A causa de su temprana disponibilidad y su evolución para satisfacer las necesidades de VoIP, H.323 es actualmente el protocolo de señalización de VoIP y de control de llamada más ampliamente usado. Las portadoras internacionales y domésticas se basan en el H.323 para manipular miles de millones de minutos de uso cada año.

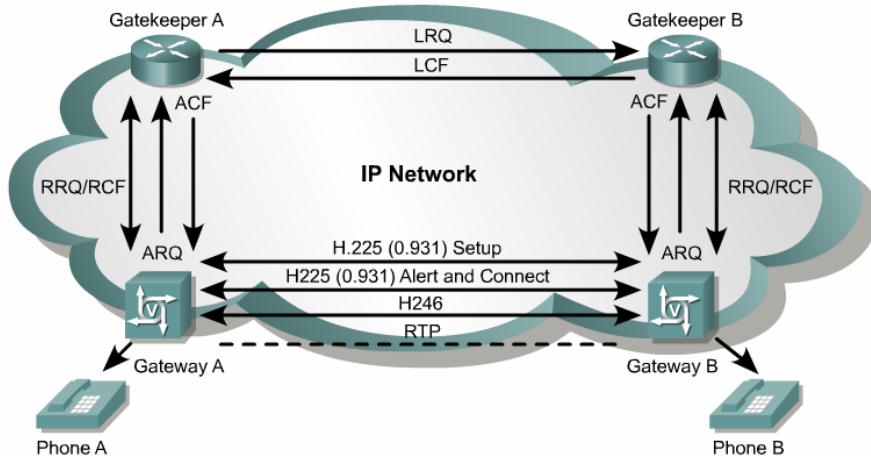


Figura 1

H.323 es considerado un protocolo marco porque define todos los aspectos de la transmisión de llamadas. H.323 define al protocolo de Registro, Admisión y Estado [Registration, Admission, and Status (RAS)] para el enrutamiento de llamadas, a los protocolos H.225 para establecimiento de llamada y a los protocolos H.245 para intercambio de capacidades. H.323 está basado en el protocolo Q.931 de Red Digital de Servicios Integrados (ISDN), que permite interoperar fácilmente con redes de voz heredadas como el PSTN y SS7. La Figura muestra un ejemplo de una red H.323. H.323 utiliza los siguientes tipos de mensajes para facilitar la comunicación, como muestra la Figura 1:

- Mensaje de Pedido de Ubicación [Location Request Message (LRQ)]
- Mensaje de Confirmación de Ubicación [Location Confirm Message (LCF)]
- Mensaje de Confirmación de Admisión [Admission Confirmation Message (ACF)]
- Mensaje de Pedido de Admisión [Admission Request Message (ARQ)]
- Mensaje de Pedido de Registración [Registration Request Message (RRQ)]

12.2.5 Protocolo de Inicio de Sesión [Session Initiation Protocol (SIP)]

El Protocolo de Inicio de Sesión (SIP), mostrado en la Figura 1, es un protocolo desarrollado por la Fuerza de Tareas de Investigación de Internet (IETF) como una alternativa simple para el H.323. Como H.323, SIP define a una arquitectura distribuida. A diferencia de H.323, SIP sólo define la forma en que se establecen y se cortan las sesiones. Utiliza otros protocolos IETF para definir otros aspectos las sesiones de VoIP y de multimedia. Ejemplos de esto son el Protocolo de Descripción de Sesión [Session Description Protocol (SDP)] para intercambio de capacidades, los Localizadores de Recursos Universales [Universal Resource Locators (URLs)] para direccionar, los Sistemas de Nombres de Dominios [Domain Name Systems (DNSs)] para localizar servicios, y el Enrutamiento Telefónico sobre IP [Telephony Routing over IP (TRIP)] para el enrutamiento de llamadas.

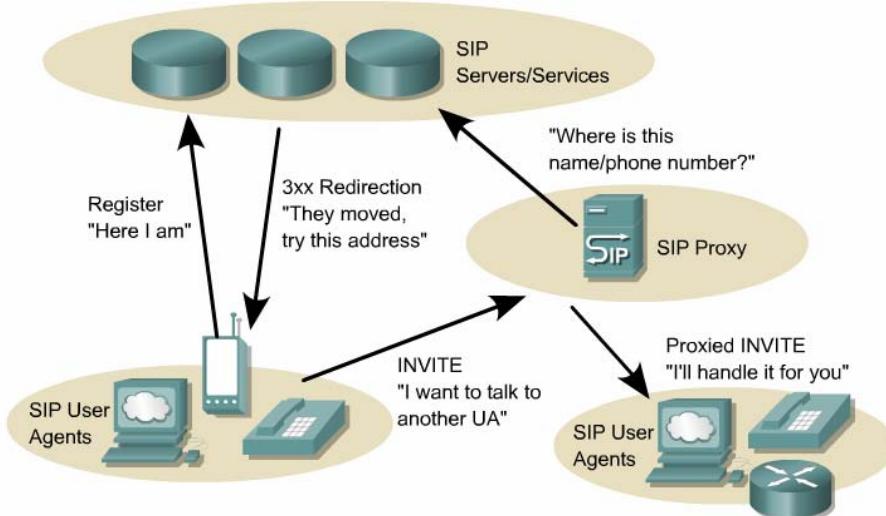


Figura 1

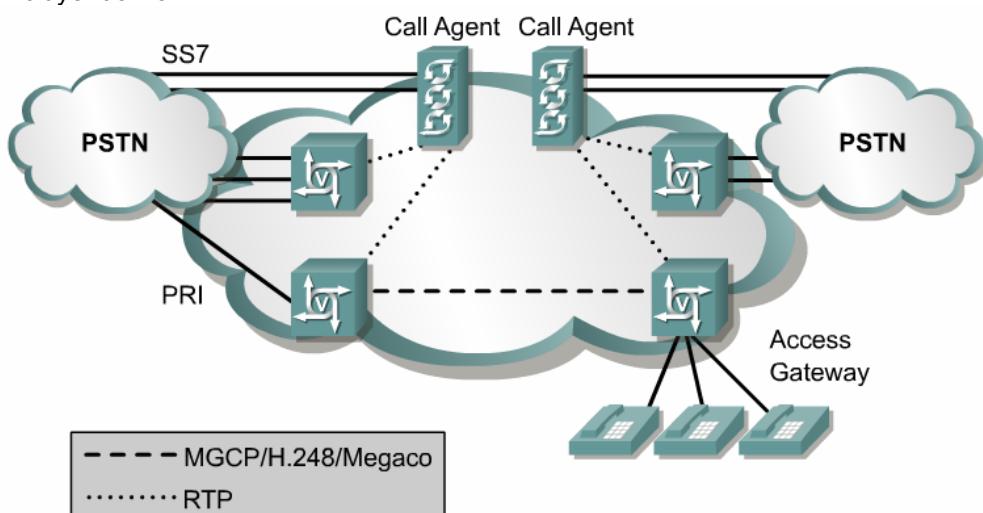
SIP fue diseñado como un protocolo multimedia que podía tomar ventaja de la arquitectura y de los mensajes que ya se encontraban en las aplicaciones de Internet populares. Al usar una arquitectura distribuida que utiliza URLs para los nombres y mensajes basados en texto, SIP intenta tomar ventaja del modelo de Internet para construir redes y aplicaciones VoIP. Además de en VoIP, SIP se utiliza en videoconferencias y en mensajería instantánea.

Aunque la IETF ha hecho un gran progreso en la definición de extensiones que permite que SIP funcione con redes de voz heredadas, el motivo principal detrás del protocolo es soportar los modelos de comunicación de próxima generación. Estos modelos utilizan Internet y aplicaciones de Internet.

Como un protocolo usado en una arquitectura distribuida, SIP permite que las compañías construyan redes a gran escala que sean escalables, elásticas y redundantes. Proporciona mecanismos para interconectarse con otras redes VoIP. Se puede agregar inteligencia y nuevas características a los puntos finales o al proxy SIP, o pueden ser usadas para redirigir servidores.

12.2.6 MGCP y H.248/Megaco

El Protocolo de Control de Gateway de Medios [Media Gateway Control Protocol (MGCP)], también conocido como IETF RFC 2705, define a una arquitectura centralizada para crear aplicaciones de red multimedia, incluyendo VoIP.



H.248 es el resultado de un trabajo en conjunto entre el ITU-T y la Fuerza de Tareas de Investigación de Internet (IETF). H.248 también se conoce como IETF RFC 2885 y como el Protocolo de Control de Gateway Multimedia [Multimedia Gateway Control Protocol (Megaco)]. H.248 también define a una arquitectura centralizada para crear aplicaciones multimedia. En muchas formas, H.248 construye sobre y extiende a MGCP.

MGCP y H.248/Megaco fueron diseñados para proporcionar una arquitectura en la cual se podría agregar en forma centralizada control de llamada y servicios a una red VoIP. Una arquitectura que utiliza estos protocolos se parece mucho a la arquitectura PSTN y a los servicios existentes.

MGCP y H.248/Megaco definen la mayor parte de los aspectos de señalización usando un modelo llamado paquetes. Estos paquetes definen la funcionalidad usada comúnmente, como la señalización PSTN, la conectividad de dispositivo del lado de la línea, y características tales como transferencia y contención. SDP también es usado para intercambio de capacidades.

En una arquitectura centralizada, MGCP y H.248/Megaco permite que las compañías construyan redes a gran escala que son escalables, elásticas y redundantes. Proporciona mecanismos para interconectarse con otras redes VoIP y para agregar inteligencia y características al agente de llamada.

12.2.7 Otros protocolos VoIP

SIP trabaja en conjunto con el Protocolo de Reserva de Recursos[Reservation Protocol (RSVP)], Protocolo de Transporte en Tiempo real [Real-time Transport Protocol (RTP)], Protocolo de Control en Tiempo real [Real-time Control Protocol (RTCP)], Protocolo de Streaming de Tiempo real [Real-time Streaming Protocol (RTSP)], Protocolo de Anuncio de Sesión [Session Announcement Protocol (SAP)], y Protocolo de Descripción de Sesión [Session Description Protocol (SDP)].

H.323 también trabaja en conjunto con RTP y RTCP. Los gateways de voz modernos normalmente tienen dos partes. La primera parte es el gateway de señalización y la segunda es el gateway de medios. El gateway de señalización se comunica con el gateway de medios usando MGCP. MGCP puede interoperar con SIP y con H.323.

Sistema de Señalización 7 [Signaling System 7 (SS7)]

Otro protocolo que debería mencionarse es el Sistema de Señalización 7 (SS7). SS7 es el sistema de Señalización de Canal Común [Common Channel Signaling (CCS)] que es usado con las redes de circuitos conmutados, como la Red Digital de Servicios Integrados (ISDN) y el PSTN. Bellcore desarrolló el SS7. Éste separa la información de señalización de los datos del usuario. Un canal específico, llamado canal D, se utiliza exclusivamente para transportar información de señalización para todos los otros canales en el sistema. Este tipo de señalización se llama fuera de banda porque no utiliza el ancho de banda del usuario. Para que VoIP pueda enrutar llamadas hacia el PSTN, debe poder hacer interfaz con el SS7, que es utilizado por el PSTN.

ENUM

El grupo de trabajo de IETF de Resolución de Número Telefónico, conocido como ENUM, está ideando un esquema para mapear los números telefónicos de E.164 con direcciones IP usando el DNS de Internet. El objetivo es permitir que cualquier aplicación, incluyendo una aplicación SIP, descubra recursos asociados con un único número telefónico. Un teléfono SIP o un servidor proxy usarían la traducción del dominio de números y la resolución DNS para descubrir un recurso DNS. Estos recursos DNS proporcionan una dirección SIP en la cual se puede encontrar el número marcado.

12.2.8 VoIP y Calidad del Servicio (QoS)

En términos simples, QoS significa proporcionar datos con el tipo de servicio de transporte que necesitan. Por ejemplo, en las transacciones bancarias, lo que más importa es el 100 por ciento de confiabilidad. Para las transferencias de archivos, un ancho de banda suficiente es más importante que una demora baja. Y para la voz, la demora y la variación en la demora son lo más importante. Hay cuatro factores que contribuyen a la QoS:

- Demora de extremo a extremo
- Confiability
- Variación en la demora de paquete a paquete, o jitter
- Ancho de banda

QoS se implementa clasificando datos, a menudo fijando bits en el encabezado IP llamados Tipo de Servicio [Type of Service (TOS)] o Punto de Código de Servicios Diferenciados [Differentiated Services Code Point (DSCP)]. Luego las diferentes clases de datos son tratadas de forma diferente. Ciertas clases pueden recibir prioridad sobre otras clases. La demora puede ser minimizada a través de diferentes técnicas de gestión de colas. Se puede garantizar a algunas clases un ancho de banda mínimo durante la congestión.

12.2.9 VoIP y WLANs

802.11e es un estándar emergente que brindará capacidades QoS a las WLANs 802.11 para permitir conversaciones de voz confiables. El estándar IEEE 802.11e es una mejora a nivel MAC que trabaja con las capas físicas 802.11b y 802.11a, además de la capa física 802.11g de próxima aparición. Además del soporte multimedia y de QoS, 802.11e también agrega mejoras en la seguridad. Está programado que el estándar esté listo durante 2003.

El estándar 802.11e traerá repercusiones sobre las redes empresariales, y también sobre los entornos de pequeñas empresas y hogareños. Aparte de la VoIP, se espera que el estándar soporte video bajo demanda y audio bajo demanda.

Un dispositivo que es probable que emerja de este estándar es la NIC multimodo. La NIC multimodo podrá manejar llamadas de voz sobre IP inalámbrico o WAN móvil. Los productos Cisco SoftPhone soportarán 802.11e.

Una cantidad de fabricantes de APs inalámbricos, incluyendo Cisco, han adoptado una solución temporal para mejorar la calidad de las llamadas de voz sobre IP inalámbrica. Conocido como Prioridad de Voz Spectralink [SpectraLink Voice Priority (SVP)], este protocolo propietario manipula los conflictos de voz y

datos permitiendo que los administradores de red y los usuarios finales prioricen la voz en el entorno de datos inalámbrico.

SVP mejora el filtrado de paquetes, que es un mecanismo ya presente en la mayoría de los APs, para poder identificar a los paquetes de voz y de datos. Al fijar que el AP soporte no más de cuatro llamadas simultáneas, al menos la mitad del ancho de banda inalámbrico estará disponible para datos. Esto se considera una solución temporal, hasta que los productos 802.11e sean lanzados.

SpectraLink ha hecho al SVP públicamente disponible para las compañías 802.11 sin costo alguno. Cisco ha implementado SVP en los APs Cisco Aironet APs.

La Figura 1 ilustra la integración de la voz y los datos inalámbricos, que sólo es parte de la Arquitectura para Voz, Video y Datos Integrados [Architecture for Voice, Video, and Integrated Data (AVVID)] de Cisco.

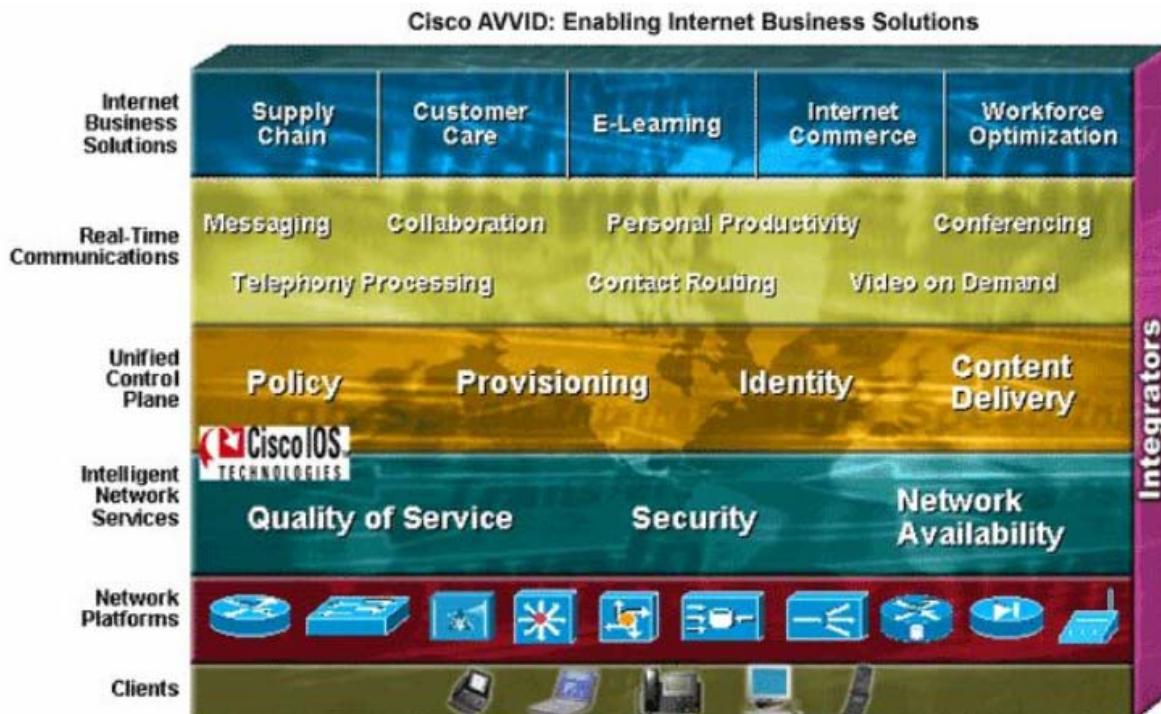


Figura 1

12.3 Tecnología Inalámbrica Móvil

12.3.1 Breve historia de la tecnología inalámbrica móvil

Las principales tecnologías inalámbricas móviles pueden ser clasificadas de acuerdo al método por el cual el compartido el medio. Las opciones de tecnología inalámbrica móvil son variadas y a menudo confusas, en parte porque hay muchas y en parte porque las mismas tecnologías son conocidas con nombres diferentes en diferentes partes del mundo.

FDMA

En los '70, los Bell Telephone Labs desarrollaron el primer sistema práctico de teléfono móvil inalámbrico. Era un sistema analógico conocido como Sistema Telefónico Móvil Avanzado [Advanced Mobile Phone System (AMPS)]. El espectro era compartido entre los usuarios a través del acceso múltiple por división de frecuencias (FDMA). Con FDMA, una célula se subdivide por frecuencias en distintos canales, que permiten a múltiples usuarios acceder a las células.

TDMA

La tecnología inalámbrica móvil de segunda generación (2G) usaba el acceso múltiple por división de tiempo (TDMA) para compartir las bandas con más eficiencia. TDMA divide a los canales de radio en ranuras de tiempo. Cada ranura de tiempo consiste en una fracción de segundo. TDMA proporciona de tres a seis canales en el mismo ancho de banda como un único canal AMPS.

CDMA

El Acceso Múltiple por División de Código [Code Division Multiple Access (CDMA)] es una forma de multiplexación que permite que numerosas señales ocupen un único canal de transmisión, optimizando el uso del ancho de banda disponible. Es una tecnología de espectro de difusión que permite que múltiples usuarios comparten las frecuencias de radio al mismo tiempo sin interferir entre sí. Los nuevos servicios 3G están casi todos basados en CDMA.

GSM

GSM es un sistema abierto, no propietario, que es la tecnología celular dominante en casi todo el mundo actual. GSM utiliza una variación del protocolo de Acceso Múltiple por División de Tiempo (TDMA). Los datos son digitalizados y comprimidos y luego enviados a través de un canal con otras dos streams de datos del usuario, las que están cada una en su propia ranura de tiempo.

GPRS

El servicio general de radiocomunicaciones por paquetes [general packet radio services (GPRS)], basado en tecnologías GSM, ya es extremadamente popular en Europa y está comenzando a surgir en los Estados Unidos. Con GPRS, las streams de datos son divididas en paquetes de datos en lugar de ser la stream continua de las redes de conmutación por paquetes de GSM. El GPRS por paquetes ofrece una conectividad siempre presente en oposición al GSM.

EDGE

La próxima etapa en la evolución del GSM es Velocidades de Datos Ampliadas para la Evolución del GSM [Enhanced Data rates for Global Evolution (EDGE)], con velocidades potenciales de datos de hasta 384 Kbps. Desarrollado específicamente para satisfacer las necesidades de ancho de banda de la 3G, EDGE es un nuevo esquema de modulación para la interfaz aérea que retiene la estructura básica del frame de GSM y utiliza protocolos de datos por paquetes GPRS.

WCDMA

El equivalente 3G de GSM, el Acceso Múltiple por División de Código de Banda Ancha [Wideband Code Division Multiple Access (WCDMA)], puede soportar comunicaciones móviles de voz, imágenes, datos y video a velocidades mucho más altas. Las señales entrantes son digitalizadas y transmitidas en un modo codificado de espectro de difusión sobre un rango de frecuencias.

CDMA2000

El acceso múltiple por división de código 2000 optimizado para la evolución de datos 1x [Code division multiple access 2000, 1x Evolution-Data Optimized (CDMA2000 1xEV-DO)] es una tecnología inalámbrica de 3G que permite a los proveedores del servicio transmitir streaming de video y audio, además de otros servicios multimedia. A diferencia de WCDMA, está completamente separado de la red inalámbrica de voz de circuitos conmutados heredada.

La Figura 1 muestra las diferentes tecnologías de acuerdo a si son consideradas de primera, segunda o tercera generación.

Generation	Services	Description
1G	FDMA	Initial successful cellular system, analog, voice traffic only, circuit-switched
2G	TDMA, CDMA, GSM	Digital services, voice and limited data such as text messages, circuit-switched, data rates of 9.6 to 19.2 Kbps, depending on technology
2.5G	GPRS	Voice and data via overlay network, data rates up to 115 Kbps, always-on data connections
3G	EDGE, CDMA2000, WCDMA	Converged voice and data network, capable of data transmission speeds of 144 Kbps inside a moving vehicle and 2 Mbps in a fixed location, packet-based rather than circuit-switched technology, permits global roaming, always-on data connections

Figura 1

12.3.2 Descripción general de los sistemas inalámbricos móviles

El AMPS analógico original consistía en tres componentes principales, que siguen siendo los componentes básicos de un sistema celular de hoy:

- Oficina de conmutación telefónica móvil [mobile telephone switching office (MTSO)]
- Estaciones base
- Teléfonos celulares u otros dispositivos

En algunos sistemas celulares, las funciones pueden residir en la estación base en lugar de en el MTSO. La terminología puede diferir ligeramente, pero la mayoría de los sistemas celulares incluyen estos tres componentes, como se muestra en la Figura 1. Las nuevas tecnologías de 3G tienen componentes adicionales para hacer interfaz con la Internet o una intranet, usando IP.

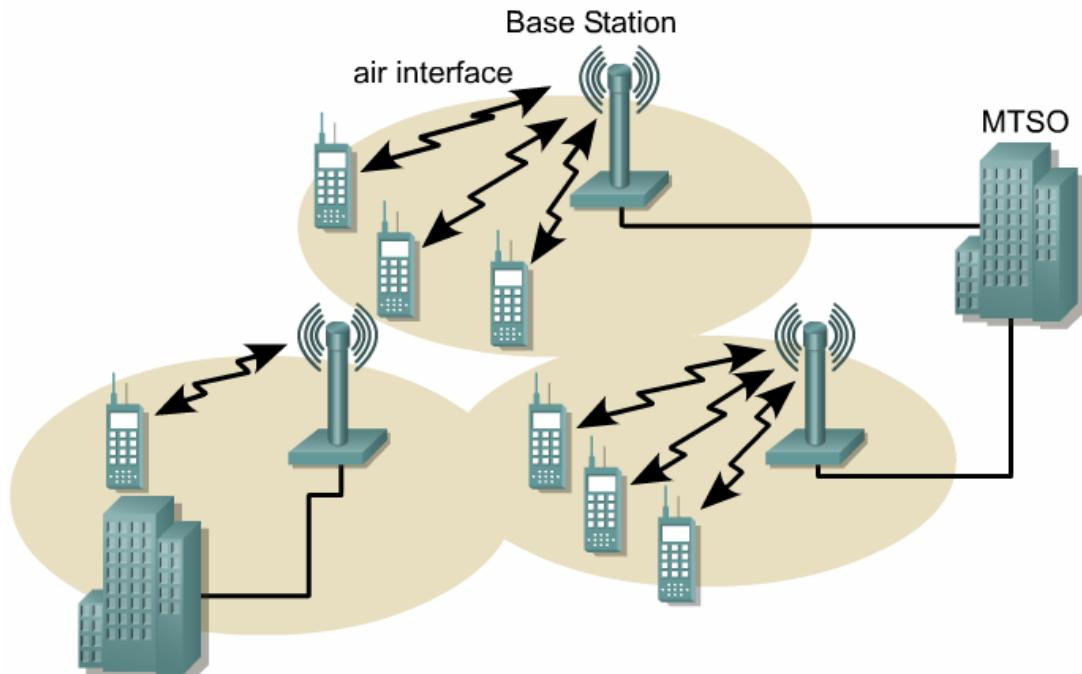


Figura 1

La idea básica detrás de las comunicaciones celulares es dividir un área de servicio en zonas geográficas, llamadas células. El ancho de banda dentro de una célula es compartido entre los usuarios de acuerdo a un método de control de acceso al medio. Cada célula tiene una estación base en el centro. Todos los dispositivos celulares se comunican a través de esta estación base. Esto es similar a una célula WLAN con un AP. Habrá al menos un MTSO por sistema celular. El MTSO se comunica con las estaciones base y con el PSTN.

Las células son normalmente bastante circulares. Por lo general, un tamaño de célula menor significa que se necesita menos potencia, lo que lleva a dispositivos más pequeños y baratos. Sin embargo, también significa que se necesitan más sitios de célula para la cobertura completa de un área. Cuando una célula está demasiado poblada, la célula sobrecargada es dividida en células más pequeñas sectorizando la cobertura en segmentos en forma de torta usando antenas direccionalles en el sitio de célula. Los sitios de célula son muchas veces diseñados desde el principio para que tengan múltiples sectores debido a la carga de tráfico y a la cobertura proyectadas. Esto permite una reutilización más frecuente y por lo tanto, mayor capacidad.

12.3.3 Roaming en un sistema inalámbrico móvil

En las comunicaciones analógicas y celulares TDMA, al igual que en las WLANs, hay un esquema para transferir un usuario móvil de una célula a otra célula adyacente, cuando la señal en la célula actual se vuelve demasiado débil. Este proceso es conocido como un handoff. El procedimiento real usado para un handoff varía, pero es similar entre las diferentes tecnologías celulares. En cualquier momento, cada dispositivo móvil está ubicado en una célula específica o sectores de célula y bajo el control de la estación base de esa célula, como se muestra en la Figura 1. Cuando un dispositivo deja una célula, la estación base nota que la señal se debilita y pregunta a todas las estaciones base de alrededor cuánta potencia están obteniendo de la señal. Luego la estación base transfiere la propiedad a la célula que recibe la señal

más fuerte. El dispositivo es informado de la nueva estación base, y si una llamada está en progreso, es instruido para que cambie a un nuevo canal o frecuencia. Este proceso de handoff lleva alrededor de 300 msec. La asignación real del canal la realiza el MTSO, ya que las estaciones base en realidad son sólo relevos de radio. Los dispositivos involucrados en este handoff se dice que están haciendo roaming.

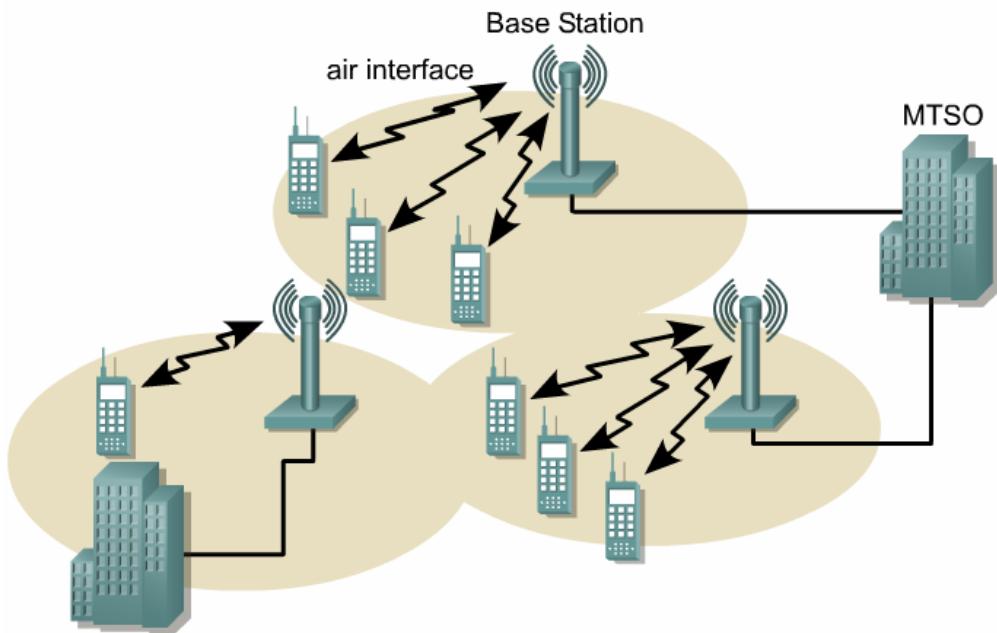


Figura 1

El handoff a una célula adyacente ocurre sobre un canal de una frecuencia diferente para reducir la posibilidad de interferencias. Este tipo de handoff es llamado handoff duro y puede realizarse entre diferentes sitios de células o diferentes sectores de un sitio de célula.

En las comunicaciones celulares CDMA móviles, el usuario en movimiento puede estar conectado a múltiples células al mismo tiempo, agregando y sacando conexiones como sea necesario mientras el móvil se traslada por el área de cobertura del sistema. Cada célula está funcionando normalmente en el mismo canal pero usando diferentes códigos de espectro de difusión, y los handoffs entre células sobre el mismo canal son llamados handoffs blandos. Si un handoff de CDMA involucra diferentes canales o bandas, es un handoff duro. En un proceso de handoff blando o muy blando, no hay demora cuando la nueva conexión es agregada antes de que la vieja se pierda.

El handoff a una célula adyacente ocurre sobre un canal de una frecuencia diferente para reducir la posibilidad de interferencia.

12.3.4 Software intermedio [middleware] de tecnología inalámbrica móvil

El rol principal del middleware inalámbrico es hacer bridging entre las aplicaciones empresariales que se están ejecutando sobre redes cableadas y los transportes de WLAN y WAN móvil. El middleware puede tomar la forma de un gateway o de una herramienta de desarrollo de software, o puede estar incluido en las ofertas de un proveedor de servicios de aplicación inalámbrica. La Figura 1 muestra un ejemplo de middleware de Protocolo de Aplicación Inalámbrica [Wireless Application Protocol (WAP)]. El Lenguaje de Etiquetado Inalámbrico [Wireless Markup Language (WML)] es un lenguaje similar a HTML, que ha sido optimizado para la tecnología inalámbrica. Está basado en el Lenguaje de Etiquetado Extensible [Extensible Markup Language (XML)]. WAP es tratado en la siguiente sección.

Existen diferentes enfoques para realizar este rol de bridging, y diferentes funciones que pueden ser proporcionadas por las distintas soluciones. No todos los productos de fabricantes realizarán todas las funciones. Algunas de estas funciones son las siguientes:

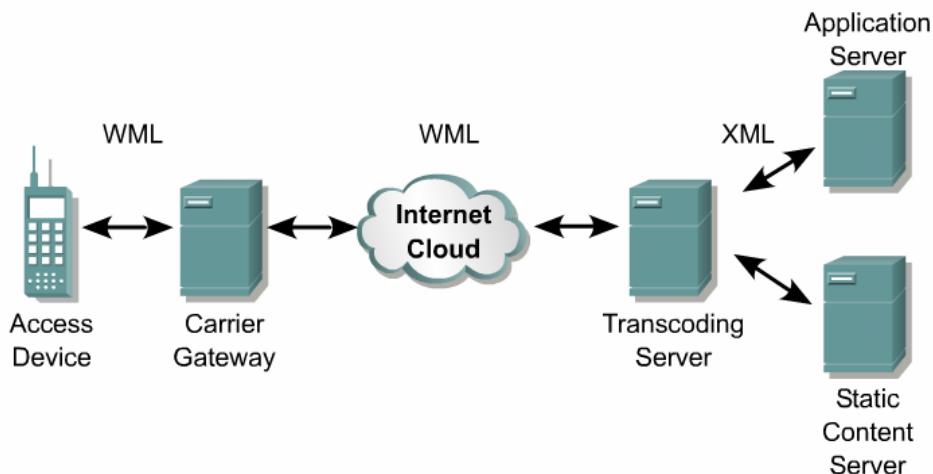


Figura 1

- Compresión de datos y de encabezado — La compresión de datos minimiza la carga enviada sobre los enlaces inalámbricos, lo que aumenta la eficiencia del ancho de banda. Esto puede ser particularmente importante para los tiempos de respuesta del usuario.
- Recuperación de cortes en las transmisiones — Las interrupciones de las transmisiones son causadas por una cobertura pobre o por interferencias. Algunos middleware pueden detectar cuándo una transmisión ha sido interrumpida. El middleware permitirá que la sesión continúe desde el punto de corte cuando sea reestablecida. Algunos middleware podrán a los mensajes en colas, para proteger a los usuarios que pueden quedar desconectados de la red. Luego, cuando los usuarios se vuelvan a conectar, los mensajes serán enviados al dispositivo móvil de ese usuario.
- Consolidación de paquetes — Algun middleware combinará los paquetes de datos pequeños en un único paquete más grande para transmitirlo sobre la red inalámbrica. Esto puede ayudar a bajar los costos del servicio de transmisión de los servicios WAN móviles basados en el uso que le cobra a los usuarios en base a la cantidad de paquetes.

El Motor de Transformación de Contenido del Cisco CTE Serie 1400 es otra solución middleware. El CTE 1400 transforma el contenido existente en la empresa para su visualización e interacción sobre dispositivos móviles de pantalla pequeña y teléfonos IP. Cuando un dispositivo realiza un pedido de conexión, el CTE transforma el contenido para que se adapte al dispositivo, usando una regla de transformación como se ve en la Figura 2. Los datos originales quedan sin cambios.

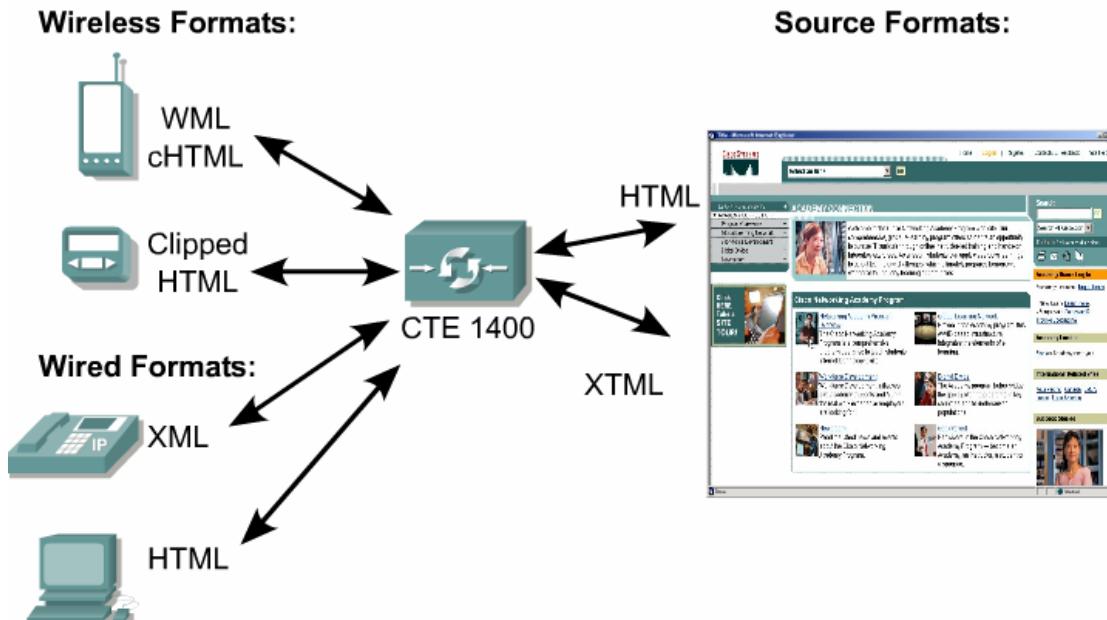


Figura 2

12.3.5 Protocolo de Aplicación Inalámbrica [Wireless Application Protocol (WAP)]

El Protocolo de Aplicación Inalámbrica (WAP) es un entorno de aplicación y un conjunto de protocolos de comunicación para dispositivos inalámbricos. Está diseñado para activar el acceso a Internet y a servicios de telefonía avanzados. Este acceso es independiente del fabricante, el vendedor y la tecnología.

WAP llena el espacio entre el mundo móvil y la Internet o las intranets corporativas. Les da a los usuarios de dispositivos móviles de tamaño bolsillo, acceso a la misma información que pueden obtener desde sus escritorios.

WAP es un estándar global que no está controlado por una sola compañía. Ericsson, Nokia, Motorola y Unwired Planet fundaron el Foro WAP en 1997. Ahora hay más de cien miembros. Las especificaciones WAP definen un conjunto de protocolos para las capas de aplicación, sesión, transacción, seguridad, y transporte.

WAP también define a un entorno de aplicación inalámbrica [wireless application environment (WAE)], que permite a operadores, fabricantes y desarrolladores de contenidos crear servicios y aplicaciones diferenciados avanzados. Los tipos de aplicaciones incluyen micro-navegadores, facilidades de scripting, e-mail, mensajería de WWW a móvil y acceso de móvil a telefax.

WAP utiliza estándares de Internet como XML, UDP e IP. Muchos de los protocolos WAP están basados en estándares de Internet, como HTTP. Los protocolos WAP han sido optimizados para las limitaciones únicas del entorno inalámbrico, las que incluyen ancho de banda angosto, alta latencia y menor estabilidad de conexión. El contenido estándar HTML no puede ser visualizado de forma efectiva en las pequeñas pantallas de los dispositivos móviles de tamaño bolsillo.

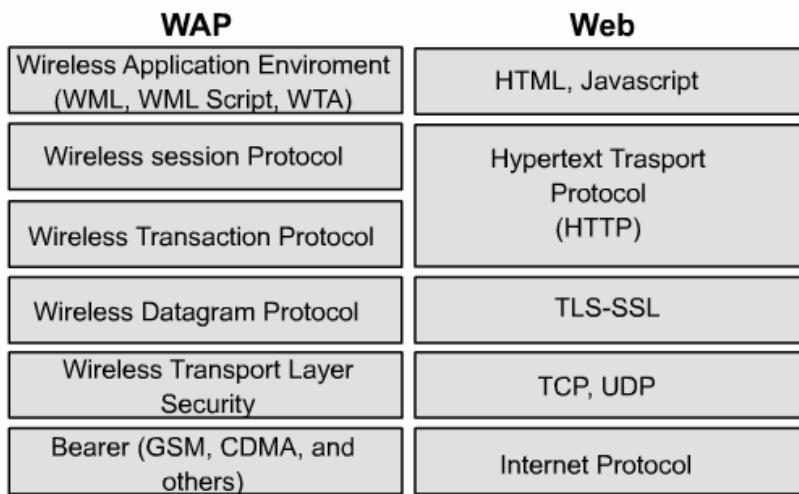


Figura 1

La pila de protocolos WAP livianos mostrada en la Figura 1 está diseñada para minimizar el ancho de banda requerido y para maximizar la cantidad de tipos de redes inalámbricas que pueden enviar contenido WAP. El objetivo serán múltiples redes, incluyendo GSM, TDMA, PCS y CDMA. Todas las tecnologías y portadores de red también serán soportados, incluyendo el servicio de mensajes breves [short message service (SMS), Datos del celular de circuitos commutados [circuit-switched cellular data (CSD)], datos digitales en modo paquete celulares [cellular digital packet data (CDPD)] y GPRS.

El contenido WAP es convertido en un formato binario compacto conocido como código byte para transmitirlo por el aire. El software del micro-navegador WAP interpreta el código byte y muestra el contenido WAP interactivo.

El navegador WAP puede hacer para la Internet móvil, lo que hace el navegador Web para la Internet. Más de 75 por ciento de los principales fabricantes de dispositivos móviles del mundo están involucrados en el Foro WAP y han anunciado dispositivos compatibles con WAP. Los navegadores Web no se espera que sean el principal factor de venta para WAP. Se espera que las aplicaciones y los servicios en tiempo real que suministran información importante sean los que promuevan el éxito de WAP. Son ejemplos precios de acciones, el clima y direcciones de restaurantes.

12.3.6 La Alianza Móvil Abierta [Open Mobile Alliance (OMA)]

Los operadores móviles están transformando rápidamente su infraestructura existente de redes de circuitos conmutados propietarias a las redes basadas en IP de estándares abiertos basados en 3G. Los operadores móviles reconocen la necesidad de optimizar sus redes para el tráfico de datos.

Existe una arquitectura que hace referencia a 3G, promovida por Cisco y sus socios, que está basada en interfaces abiertas. La arquitectura fue soportada previamente a través del Foro de Internet Inalámbrica Móvil [Mobile Wireless Internet Forum (MWIF)], que cesó sus operaciones a finales del 2002. La Alianza Móvil Abierta (OMA) está ahora continuando el trabajo técnico del foro.

Existen cuatro principios básicos de la OMA:

- Los productos y servicios están basados en protocolos abiertos, estándares globales e interfaces y no están restringidos a tecnologías propietarias.
- La capa de aplicaciones es agnóstica de portadora, como GSM, GPRS, EDGE, CDMA o UMTS.
- El marco de trabajo de la arquitectura y los activadores de servicios son independientes del SO.
- Las aplicaciones y las plataformas son interoperables, dando un roaming sin fisuras geográfico e inter-generacional.

Al promover un núcleo IP común, una arquitectura basada en IP peer-to-peer distribuida para escalabilidad e interfaces IP estándares para la facturación y la atención del usuario, las eficiencias operativas de los nuevos servicios móviles de voz y datos beneficiarán a los operadores y a los clientes móviles.

12.3.7 El futuro de la tecnología inalámbrica móvil

Otra tendencia importante para el futuro de los productos inalámbricos son los hot spots [puntos calientes]. Un hot spot es un lugar donde una WLAN es públicamente accesible. El salón de un aeropuerto o una cafetería, como se muestra en la Figura 1, son dos ejemplos de hot spots. Esta tendencia facilitará la integración de las WLANs con la WAN móvil.



Figura 1

T-Mobile y AT&T son dos portadoras inalámbricas que han comenzado a ofrecer servicios Wi-Fi como complementos de mayor velocidad para sus servicios móviles en aeropuertos, hoteles y cafeterías. Estos servicios se volverán más generalizados a medida que las portadoras móviles compren o colaboren con las compañías enfocadas en Wi-Fi.

Además de ofrecer mayores velocidades, los productos futuros pueden incluir una unidad que actúa como un teléfono inalámbrico cuando el usuario está cerca de la oficina, comuta a una WLAN en algún lado en el campus corporativo y pasa sin fisuras hacia una red celular de banda ancha cuando el usuario sale al exterior. Tales productos de doble banda y triple banda están comenzando a surgir como NICs y chips. Éstos permitirán que los usuarios se conecten a la mejor conexión inalámbrica disponible. Un software especial controlará la transferencia entre las redes Wi-Fi y los servicios de red WAN móviles. Los usuarios de roaming no tendrán que cambiar las configuraciones, los inicios de sesión, las IDs o las passwords para mantener las conexiones y las sesiones de aplicación.

¿Teléfono celular o Billetera?

Otra posibilidad es una aplicación que convierte un microteléfono en una especie de billetera. Al menos una compañía está trabajando en unos lentes que permitirán al rayo infrarrojo encontrado en algunos dispositivos de mano transmitir a través de distancias mayores sin apuntar en forma precisa. Esto permitirá

a los usuarios apuntar su teléfono celular y pagar compras hechas en varios lugares, como en una ventana de atención rápida en un comercio de comidas rápidas, en un supermercado o en una máquina expendedora.

12.4 Organizaciones y Certificaciones Inalámbricas

12.4.1 La Alianza Fidelidad Inalámbrica [Wireless Fidelity (Wi-Fi)]

La Alianza Fidelidad Inalámbrica (Wi-Fi) es una asociación internacional sin fines de lucro formada en 1999. Wi-Fi fue formada para certificar la interoperabilidad de productos WLAN en base a la especificación IEEE 802.11. La Alianza Wi-Fi actualmente tiene 202 compañías miembros de todo el mundo. Cerca de 580 productos han recibido la certificación Wi-Fi desde que la certificación comenzó en Marzo del 2000. El objetivo de la Alianza Wi-Fi es mejorar la experiencia del usuario a través de la interoperabilidad de los productos. Para asegurar la interoperabilidad entre las marcas, la Alianza Wi-Fi trabaja con grupos de estándares técnicos como el IEEE y con compañías que están desarrollando futuras generaciones de herramientas de networking inalámbrico.

La Alianza Wi-Fi se llamaba originalmente Alianza de Compatibilidad con Ethernet Inalámbrica [Wireless Ethernet Compatibility Alliance (WECA)]. Sin embargo, el término Ethernet inalámbrica nunca se hizo tan popular como los términos WLANs y Wi-Fi. Por lo tanto, la organización cambió su nombre.

Wi-Fi CERTIFIED es el logo dado al equipo de networking inalámbrico que pasa las rigurosas pruebas de funcionalidad e interoperabilidad administradas por la Alianza Wi-Fi. El equipo Wi-Fi CERTIFIED funcionará con cualquier otro equipo de networking inalámbrico que también tenga el logo Wi-Fi CERTIFIED.

Existen también Wi-Fi ZONEs. Wi-Fi ZONEs son redes de hot spots inalámbricas a las que los usuarios pueden acceder cuando están lejos de sus hogares u oficinas. Al igual que con los productos Wi-Fi, sólo los proveedores de servicios que cumplen con los estándares de desarrollo y servicios Wi-Fi ZONE pueden exhibir el logo, que se muestra en la Figura 1. Los usuarios pueden buscar el logo para asegurarse de que un hot spot es una Wi-Fi ZONE.



Figura 1

Existe una base de datos en línea de ubicaciones Wi-Fi ZONE en todo el mundo en el sitio web de la Alianza Wi-Fi. Esto ayuda a los usuarios a localizar la Wi-Fi ZONE más conveniente, esté ésta en una cafetería, un hotel, un aeropuerto, un centro de convenciones u otro lugar público.

12.4.2 Asociación WLAN [WLAN Association (WLNA)]

La Asociación WLAN (WLNA) es una asociación sin fines de lucro de capacitación educativa. Los miembros de WLNA incluyen a los líderes y a los innovadores en tecnología de la industria de tecnología inalámbrica de área local. A través del vasto conocimiento y experiencia de los miembros, WLNA proporciona información sobre aplicaciones, problemas, tendencias y próximos eventos de la industria de las WLANs. El logo WLNA se muestra en la figura.

WLNA promociona el uso de tecnología inalámbrica de networking e intenta elevar la conciencia del consumidor con respecto al uso y disponibilidad de las WLANs. Sirve como un recurso para los usuarios y posibles clientes de productos WLAN y de productos de área personal inalámbricos. También proporciona información sobre los medios y los analistas de la industria.

WLNA mantiene un directorio en línea de los miembros de la industria en todas las áreas del desarrollo de productos WLAN. Este directorio incluye fabricantes de WLAN, proveedores de servicio, fabricantes de semiconductores y organizaciones de capacitación. WLNA también ofrece foros de discusión inalámbrica en su sitio web.

Recientemente WLNA presentó su Programa de Aval Educativo y ha avalado oficialmente el programa de certificación Administrador de Redes Inalámbricas Certificado [Certified Wireless Network Administrator™]

(CWNA™)] de Planet3 Wireless bajo este programa. La certificación CWNA será tratada más tarde en este módulo.

12.4.3 Comisión Federal de Comunicaciones [Federal Communications Commission (FCC)]

La FCC es una agencia gubernamental independiente de los EE.UU. bajo el Congreso de los EE.UU. La FCC de EE.UU. fue establecida por el Acta de Comunicaciones de 1934 y es responsable de regular las comunicaciones interestatales e internacionales por radio, televisión, teletipo, satélite y cable.

Cada nodo en una red inalámbrica basada en radio es necesario que tenga un transmisor y un receptor de radio. Hay un tremendo potencial de que los diversos transmisores y receptores se interfieran entre sí. Por lo tanto, casi todas las naciones del mundo tienen alguna agencia regulatoria que supervisa el uso del espectro de radio en el país. En los Estados Unidos, la FCC es la agencia controladora. En muchos otros países es un ministerio de correos y telecomunicaciones [posts and telecommunications (PTT)] o una agencia con un nombre similar.

El control gubernamental evita el caos en las ondas del aire, pero crea una carga extra sobre cualquier planificación para operar un transmisor. Ésta debe cumplir con las restricciones burocráticas y con los posibles gastos para obtener una licencia.

Afortunadamente existen exclusiones al requisito de licencia. Las regulaciones de la Parte 15 de PTT permiten el funcionamiento sin licencia de dispositivos de espectro de difusión en las bandas de frecuencias de 902 a 928MHz, 2,4 a 2,5 GHz, y 5,8 a 5,9 GHz. Estas tres bandas de frecuencias han sido asignadas para varias aplicaciones industriales, científicas y médicas. Por lo tanto, a menudo se las llama bandas ISM. Mucho del equipo de espectro de difusión anterior al 802.11 usaba la banda ISM de 900 MHz. El estándar 802.11 para FHSS y DSSS, 802.11b para DSSS y 802.11g para OFDM especifican todos que se debería usar la banda ISM de 2,4 GHz. El estándar 802.11a especifica la banda de 5 GHz. Una de las razones para elegir estas bandas es que están disponibles en todo el mundo para su uso sin licencia, aunque los límites precisos de la banda varían según el país. En los Estados Unidos, la FCC ha fijado los límites de la banda en 2,4 GHz y 2,4835 GHz.

Además de las asignaciones del espectro, la FCC de los EE.UU. también regula otros detalles de los estándares. Por ejemplo, esta banda ha sido dividida en canales de 1 MHz para radios de salto de frecuencias. La FCC requiere que el transmisor visite al menos 79 de los canales al menos una vez cada 30 segundos. La secuencia de saltos es un patrón pseudoaleatorio, por lo que la transmisión de salto de frecuencias parece ser nada más que un ruido de fondo de bajo nivel para las radios convencionales.

Resumen

Este módulo observó a algunas de las tecnologías emergentes actuales. Primero se habló de la recientemente aprobada tecnología inalámbrica de banda ultra ancha. Luego se habló de la voz sobre IP (VoIP) y de algunos de sus importantes protocolos.

Luego se presentó una breve historia de la tecnología inalámbrica móvil, seguida por una mirada a su estado actual, y futuras direcciones posibles.

Se describieron algunas de las importantes organizaciones involucradas con el networking inalámbrico, además de las certificaciones de la industria que están relacionadas con las redes inalámbricas. Finalmente, el módulo proveyó varios estudios de casos que involucran despliegues de WLAN.