11. Conexión inalámbrica

11.1. ¿Por qué las LAN inalámbricas se han vuelto tan populares?

Las redes comerciales actuales evolucionan para dar soporte a la gente que está en continuo movimiento. Empleados y empleadores, estudiantes y docentes, agentes del gobierno y aquellos a quienes sirven, aficionados a los deportes y compradores están todos en continuo movimiento y muchos de ellos están "conectados". Tal vez usted tiene un teléfono celular al que envía mensajes instantáneos cuando se encuentra lejos de su computadora. Esta es la visión de ambiente móvil donde las personas pueden llevar su conexión a la red consigo cuando se trasladan.

Hay muchas infraestructuras diferentes (LAN conectada por cable, redes del proveedor de servicios) que permiten que exista este tipo de movilidad, pero en un ambiente de negocios, lo más importante es la WLAN.

La productividad ya no está restringida a una ubicación de trabajo fija o a un período de tiempo definido. Las personas esperan ahora estar conectadas en cualquier momento y en cualquier lugar, desde la oficina hasta el aeropuerto o incluso en el hogar. Los empleados que viajan solían estar restringidos a utilizar teléfonos públicos para verificar sus mensajes y para devolver algunas llamadas telefónicas entre vuelos. Ahora pueden verificar su correo electrónico, correo de voz y estado de los productos en asistentes personales digitales (PDA) mientras están en ubicaciones temporales diferentes.

Muchas personas cambiaron su forma de vivir y aprender en el hogar. Internet es un servicio estándar en muchos hogares, junto con el servicio de TV y teléfono. Incluso el método para acceder a Internet cambió rápidamente de servicio temporal de dial-up vía módem a DSL dedicado o servicio por cable. Los usuarios domésticos buscan muchas de las mismas soluciones flexibles inalámbricas que buscan los trabajadores de oficina. Por primera vez, en 2005, se compraron más computadoras portátiles con Wi-Fi habilitado que computadoras personales fijas.

Además de la flexibilidad que ofrecen las WLAN, el costo reducido es un beneficio importante. Por ejemplo: con una infraestructura inalámbrica ya ubicada, se ahorra al moverse una persona dentro del edificio, al reorganizar un laboratorio, o al moverse a ubicaciones temporarias o sitios de proyectos. En promedio, el costo de IT de mover a un empleado a una nueva ubicación dentro del sitio es de $375 (USD).

Otro ejemplo es cuando la compañía se muda a un nuevo edificio que no tiene ninguna infraestructura de cableado. En este caso, el ahorro resultante de utilizar las WLAN puede ser incluso más notorio, dado que se evita el gran costo de pasar cables a través de paredes, techos y suelos.

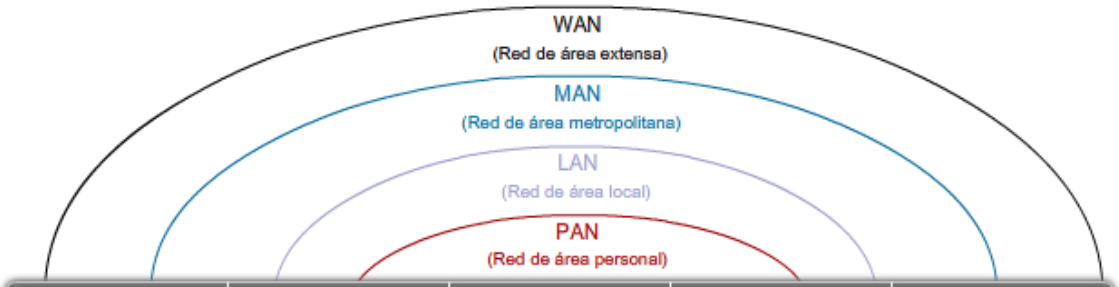
Aunque es difícil de medir, las WLAN pueden dar como resultado una mejor productividad y empleados más relajados, y así obtener mejores resultados para los clientes y mayores ingresos.

11.2. Porque utilizar conexión inalámbrica

LAN inalámbricas

En los capítulos anteriores, aprendió sobre funciones y tecnologías de switch. Muchas redes de negocios actuales dependen de las LAN basadas en switch para las operaciones diarias dentro de las oficinas. Sin embargo, los trabajadores son cada vez más móviles y desean mantener el acceso a los recursos de LAN de sus negocios desde otras ubicaciones además de sus escritorios. Los trabajadores en la oficina desean llevar sus computadoras portátiles a reuniones o a la oficina de sus colegas. Cuando se utiliza una computadora portátil en otra ubicación, no es conveniente depender de una conexión conectada por cable. En este tema, aprenderá acerca de las LAN inalámbricas y cómo benefician a su negocio. También explorará las consideraciones de seguridad asociadas con las WLAN.

Las comunicaciones portátiles se convirtieron en una expectativa en muchos países alrededor del mundo. Puede ver movilidad y portabilidad en todo, desde teclados inalámbricos y audífonos, hasta teléfonos satelitales y sistemas de posicionamiento global (GPS). La mezcla de tecnologías inalámbricas en diferentes tipos de redes permite que los trabajadores tengan movilidad.



	PAN	LAN	MAN	WAN
Estándares	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satélite
Velocidad	< 1 Mbps	de 11 a 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Intervalo	Cortocircuito	Medio	Medio-Largo	Largo
Aplicaciones	Punto a punto Dispositivo a dispositivo	Redes de empresas	Acceso de última milla	Datos móviles Dispositivos

11.3. Comparación entre una WLAN y una LAN

Las LAN inalámbricas comparten un origen similar con las LAN Ethernet. El IEEE adoptó la cartera 802 LAN/MAN de estándares de arquitectura de red de computadoras. Los dos grupos de trabajo 802 dominantes son Ethernet 802.3 y LAN inalámbrica 802.11. Sin embargo, hay diferencias importantes entre ellos.

Las WLAN utilizan radiofrecuencia (RF) en lugar de cables en la capa física y la subcapa MAC de la capa de enlace de datos. Comparada con el cable, la RF tiene las siguientes características:

- La RF no tiene límites, como los límites de un cable envuelto. La falta de dicho límite permite a las tramas de datos viajar sobre el medio RF para estar disponibles para cualquiera que pueda recibir la señal RF.
- La señal RF no está protegida de señales exteriores, como sí lo está el cable en su envoltura aislante. Las radios que funcionan independientemente en la misma área geográfica, pero que utilizan la misma RF o similar, pueden interferirse mutuamente.
- La transmisión RF está sujeta a los mismos desafíos inherentes a cualquier tecnología basada en ondas, como la radio comercial. Por ejemplo: a medida que usted se aleja del origen, puede oír estaciones superpuestas una sobre otra o escuchar estática en la transmisión. Con el tiempo, puede perder la señal por completo. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.
- Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

Las WLAN conectan a los clientes a la red a través de un punto de acceso inalámbrico (AP) en lugar de un switch Ethernet.

Las WLAN conectan los dispositivos móviles que, en general, están alimentados por batería, en lugar de los dispositivos enchufados de la LAN. Las tarjetas de interfaz de red inalámbrica (NIC) tienden a reducir la vida de la batería de un dispositivo móvil.

Las WLAN admiten hosts que se disputan el acceso a los medios RF (bandas de frecuencia). 802.11 recomienda la prevención de colisiones, en lugar de la detección de colisiones para el acceso a medios, para evitar -en forma proactiva- colisiones dentro del medio.

Las WLAN utilizan un formato de trama diferente al de las LAN Ethernet conectadas por cable. Las WLAN requieren información adicional en el encabezado de la Capa 2 de la trama.

Las WLAN tienen mayores inconvenientes de privacidad debido a que las frecuencias de radio pueden salir fuera de las instalaciones.

Comparación entre una WLAN y una LAN

Característica	LAN inalámbrica 802.11	Redes LAN Ethernet 802.3
Capa física	Radiofrecuencia (RF)	Cable
Acceso de medios	Prevención de colisión	Detección de colisiones
Disponibilidad	Cualquiera con una radio NIC en el rango de un punto de acceso	Se requiere conexión por cable
Interferencia en la señal	Sí	Irrelevante
Regulación	Regulación adicional a cargo de las autoridades locales	El estándar IEEE dictamina

11.4. Certificación Wi-Fi

La Wi-Fi Alliance (http://www.wi-fi.org), una asociación de comercio industrial global sin fines de lucro, dedicada a promover el crecimiento y aceptación de las WLAN proporciona la certificación Wi-Fi. Apreciará mejor la importancia de la certificación Wi-Fi si considera el rol de la Wi-Fi Alliance en el contexto de los estándares WLAN.

Los estándares aseguran interoperabilidad entre dispositivos hechos por diferentes fabricantes. Las tres organizaciones clave que influencian los estándares WLAN en todo el mundo son:

- ITU-R
- IEEE
- Wi-Fi Alliance

El ITU-R regula la asignación del espectro RF y órbitas satelitales. Éstos se describen como recursos naturales finitos que se encuentran en demanda por parte de clientes, como redes inalámbricas fijas, redes inalámbricas móviles y sistemas de posicionamiento global.

El IEEE desarrolló y mantiene los estándares para redes de área local y metropolitanas con la familia de estándares IEEE 802 LAN/MAN. El IEEE 802 es administrado por el comité de estándares IEEE 802 LAN/MAN (LMSC), que supervisa múltiples grupos de trabajo. Los estándares dominantes en la familia IEEE 802 son 802.3 Ethernet, 802.5 Token Ring, y 802.11 LAN inalámbrica.

A pesar de que el IEEE especificó estándares para los dispositivos de modulación RF, no especificó estándares de fabricación, de modo que las interpretaciones de los estándares 802.11 por parte de los diferentes proveedores pueden causar problemas de interoperabilidad entre sus dispositivos.

La Wi-Fi Alliance es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de productos que están basados en el estándar 802.11, y certifica proveedores en conformidad con las normas de la industria y adhesión a los estándares. La certificación incluye las tres tecnologías RF IEEE 802.11, así como la adopción temprana de los borradores pendientes de la IEEE, como el estándar 802.11n, y los estándares de seguridad WPA y WPA2 basados en IEEE 802.11i.

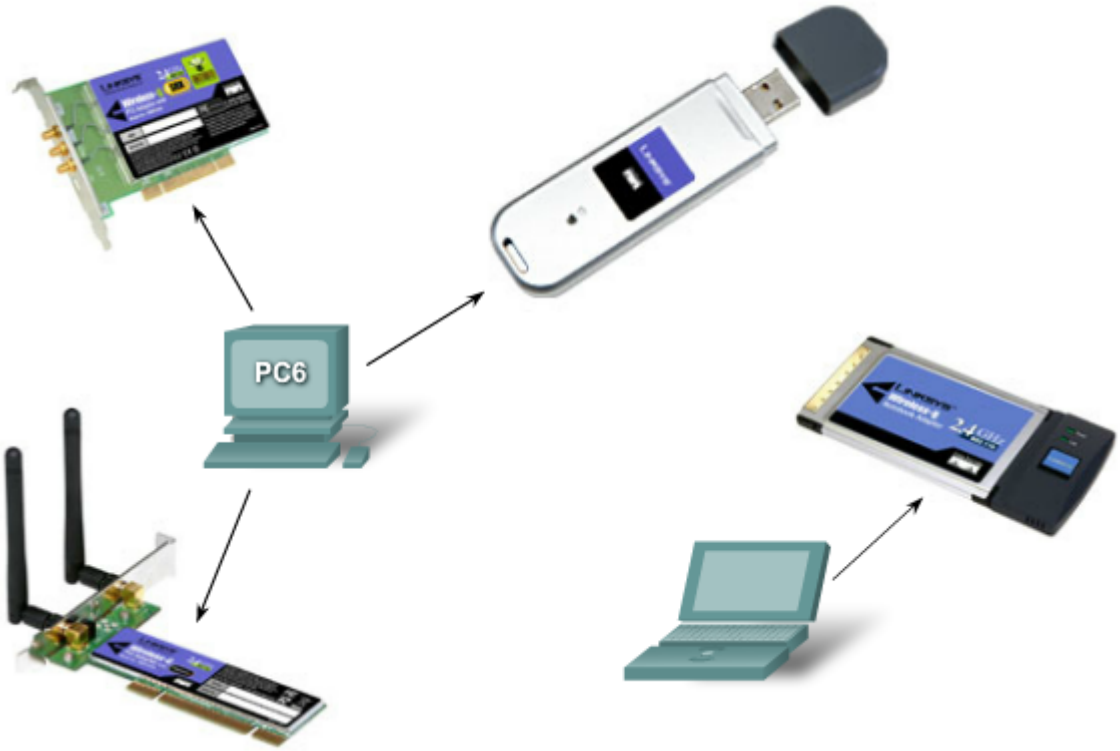
Los roles de estas tres organizaciones pueden resumirse de la siguiente manera:

- El ITU-R regula la asignación de las bandas RF.
- IEEE especifica cómo se modula RF para transportar información.
- Wi-Fi asegura que los proveedores fabriquen dispositivos que sean interoperables.

Certificación Wi-Fi

11.5. NIC inalámbricas

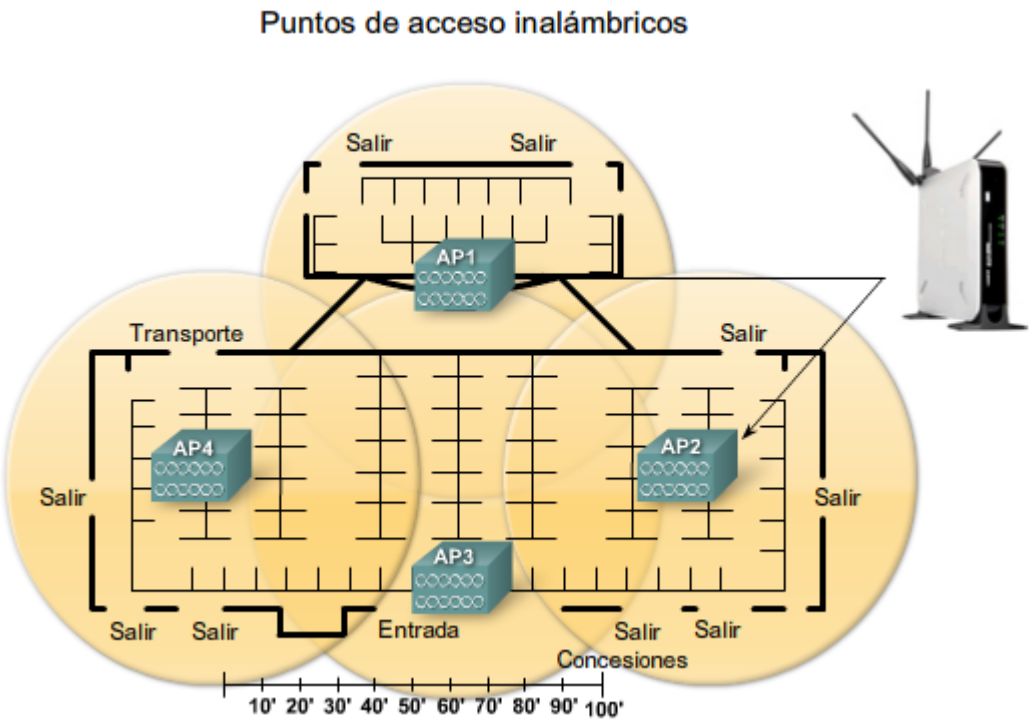
NIC inalámbricas



11.6. Puntos de acceso inalámbricos

Un punto de acceso conecta a los clientes (o estaciones) inalámbricos a la LAN cableada. Los dispositivos de los clientes, por lo general, no se comunican directamente entre ellos; se comunican con el AP. En esencia, un punto de acceso convierte los paquetes de datos TCP/IP desde su formato de encapsulación en el aire 802.11 al formato de trama de Ethernet 802.3 en la red Ethernet conectada por cable.

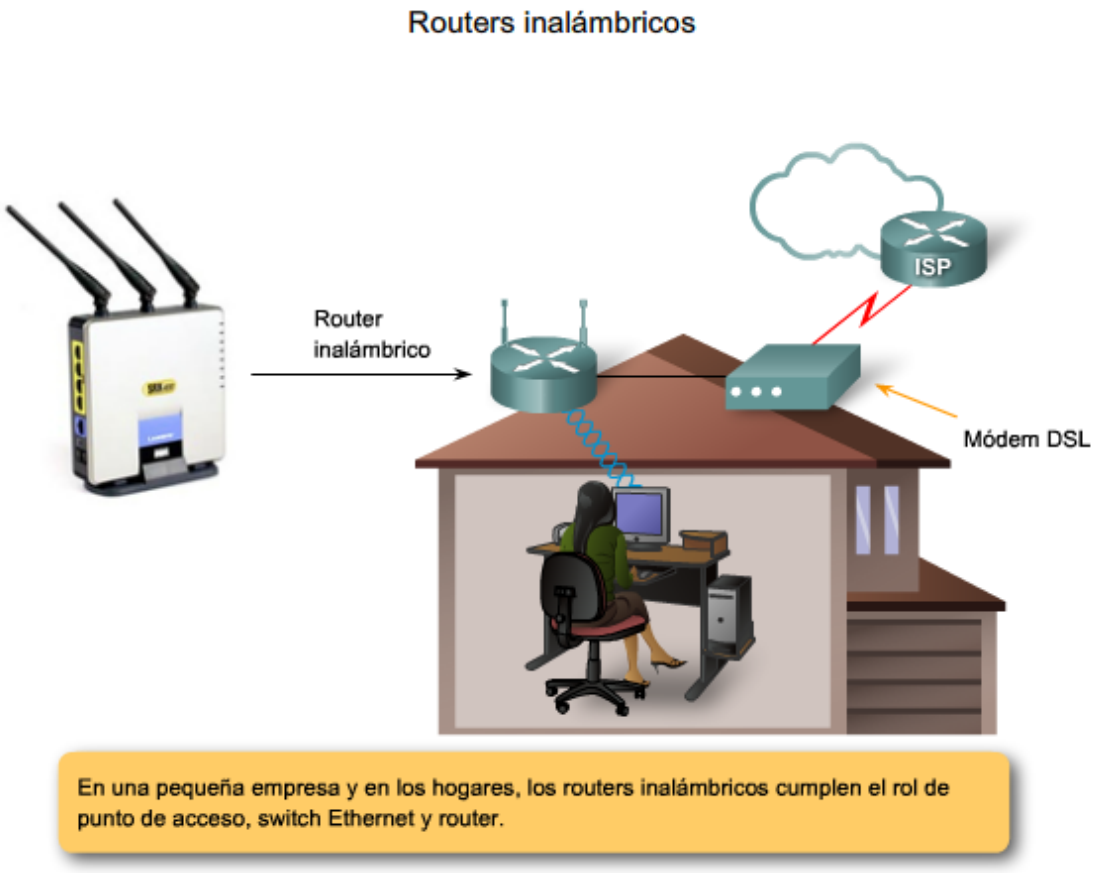
En una infraestructura de red, los clientes deben asociarse con un punto de acceso para obtener servicios de red. La asociación es el proceso por el cual un cliente se une a una red 802.11. Es similar a conectarse a una red LAN conectada por cable. La asociación se discute en temas posteriores.



11.7. Routers inalámbricos

Los routers inalámbricos cumplen la función de punto de acceso, switch Ethernet y router. Por ejemplo: los Linksys WRT300N utilizados son en realidad tres dispositivos en una caja. Primero está el punto de acceso inalámbrico, que cumple las funciones típicas de un punto de acceso. Un switch integrado de cuatro puertos full-duplex, 10/100 proporciona la conectividad a los dispositivos conectados por cable. Finalmente, la función de router provee un gateway para conectar a otras infraestructuras de red.

El WRT300N se utiliza más frecuentemente como dispositivo de acceso inalámbrico en residencias o negocios pequeños. La carga esperada en el dispositivo es lo suficientemente pequeña como para administrar la provisión de WLAN, 802.3 Ethernet, y conectar a un ISP.



11.8. Parámetros configurables para los puntos finales inalámbricos

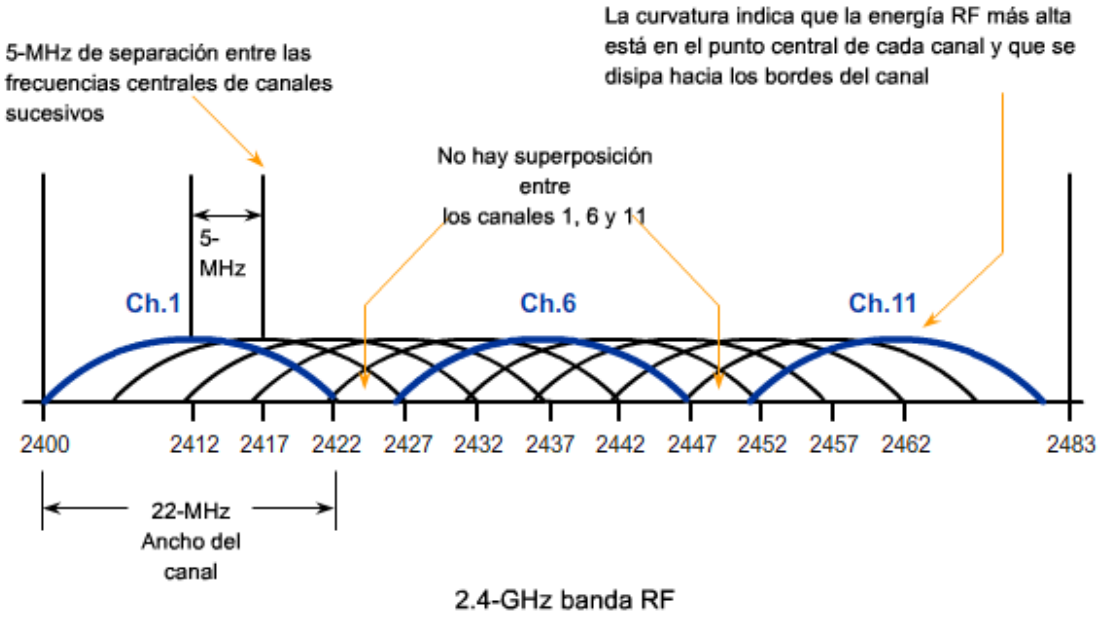
La figura muestra la pantalla inicial para la configuración inalámbrica en un router Linksys inalámbrico. Varios procesos deben tener lugar para crear una conexión entre cliente y punto de acceso. Debe configurar los parámetros en el punto de acceso y, posteriormente, en el dispositivo de su cliente, para permitir la negociación de estos procesos.

El modo de red inalámbrica se remite a los protocolos WLAN: 802.11a, b, g, o n. Dado que 802.11g es compatible con versiones anteriores de 802.11b, los puntos de acceso admiten ambos estándares. Recuerde que si todos los clientes se conectan a un punto de acceso con 802.11g, se beneficiarán con las mejores velocidades de transmisión de datos. Cuando los clientes 802.11b se asocian con el punto de acceso, todos los clientes más veloces que se disputan el canal deben esperar que los clientes en 802.11b lo despejen antes de poder transmitir. Cuando un punto de acceso Linksys se configura para permitir clientes de 802.11b y 802.11g, opera en modo mixto.

Para que un punto de acceso admita tanto el 802.11a como los 802.11b y g, deberá tener una segunda radio para operar en la banda RF diferente.

Un identificador de conjunto de servicios (SSID) es un identificador único que utiliza los dispositivos cliente para distinguir entre múltiples redes inalámbricas cercanas. Varios puntos de acceso en la red pueden compartir un SSID. La figura muestra un ejemplo de los SSID que se distinguen entre las WLAN, cada uno de los cuales puede ser alfanumérico, con entrada de 2 a 32 caracteres de longitud, con distinción entre mayúsculas y minúsculas.

El estándar IEEE 802.11 establece el esquema de canalización para el uso de las bandas ISM RF no licenciadas en las WLAN. La banda de 2.4 GHz se divide en 11 canales para Norteamérica y 13 canales para Europa. Estos canales tienen una separación de frecuencia central de sólo 5 MHz y un ancho de banda total (u ocupación de frecuencia) de 22 MHz. El ancho de banda del canal de 22 MHz combinado con la separación de 5 MHz entre las frecuencias centrales significa que existe una superposición entre los canales sucesivos. Las optimizaciones para las WLAN que requieren puntos de acceso múltiple se configuran para utilizar canales no superpuestos. Si existen tres puntos de acceso adyacentes, utilice los canales 1, 6 y 11. Si sólo hay dos, seleccione dos canales cualesquiera con al menos 5 canales de separación entre ellos, como el canal 5 y el canal 10. Muchos puntos de acceso pueden seleccionar automáticamente un canal basado en el uso de canales adyacentes. Algunos productos monitorean continuamente el espacio de radio para ajustar la configuración de canal de modo dinámico en respuesta a los cambios del ambiente.



11.9. Asociación del cliente y el punto de acceso

Una parte clave del proceso de 802.11 es descubrir una WLAN y, luego, conectarse a ella. Los componentes principales de este proceso son los siguientes:

Beacons - Tramas que utiliza la red WLAN para comunicar su presencia.
Sondas - Tramas que utilizan los clientes de la WLAN para encontrar sus redes.

Autenticación - Proceso que funciona como instrumento del estándar original 802.11, que el estándar todavía exige.
Asociación - Proceso para establecer la conexión de datos entre un punto de acceso y un cliente WLAN.

El propósito principal de la beacon es permitir a los clientes de la WLAN conocer qué redes y puntos de acceso están disponibles en un área dada, permitiéndoles, por lo tanto, elegir qué red y punto de acceso utilizar. Los puntos de acceso pueden transmitir beacons periódicamente.

Aunque las beacons pueden transmitirse regularmente por un punto de acceso, las tramas para sondeo, autenticación y asociación se utilizan sólo durante el proceso de asociación (o reasociación).

Proceso conjunto 802.11 (Asociación)

Antes de que un cliente 802.11 pueda enviar información a través de una red WLAN, debe atravesar el siguiente proceso de tres etapas:

Etapa 1: Sondeo de 802.11

Los clientes buscan una red específica mediante una solicitud de sondeo a múltiples canales. El pedido de sondeo especifica el nombre de la red (SSID) y las tasas de bit. Un cliente típico de WLAN se configura con el SSID deseado, de modo que los pedidos de sondeo del cliente WLAN contienen el SSID de la red WLAN deseada.

Si el cliente WLAN sólo quiere conocer las redes WLAN disponibles, puede enviar un pedido de sondeo sin SSID, y todos los puntos de acceso que estén configurados para responder este tipo de consulta responderán. Las WLAN con la característica de broadcast SSID deshabilitada no responderán.

Etapa 2: Autenticación 802.11

802.11 se desarrolló originalmente con dos mecanismos de autenticación. El primero, llamado autenticación abierta, es fundamentalmente una autenticación NULL donde el cliente dice "autentícame", y el punto de acceso responde con "sí". Éste es el mecanismo utilizado en casi todas las implementaciones de 802.11.

Un segundo mecanismo de autenticación se denomina clave de autenticación compartida. Esta técnica se basa en una clave de Privacidad equivalente por cable (WEP) compartida entre el cliente y el punto de acceso. En esta técnica, el cliente envía una solicitud de autenticación al punto de acceso. El punto de acceso luego envía un texto de reto al cliente, quien encripta el mensaje utilizando la clave compartida y vuelve a enviar el texto encriptado al punto de acceso. Luego, el punto de acceso decodifica el texto encriptado utilizando su clave y si el texto decodificado

coincide con el texto de reto, el cliente y el punto de acceso comparten la misma clave y el punto de acceso autentica la estación. Si los mensajes no coinciden, el cliente no se autentica.

A pesar de que la clave de autenticación compartida necesita estar incluida en las implementaciones de cliente y de punto de acceso para el cumplimiento general de los estándares, no se utiliza ni se recomienda. El problema es que la clave WEP normalmente se usa para encriptar datos durante el proceso de transmisión. Al usar la misma clave WEP en el proceso de autenticación, el atacante tiene la posibilidad de extraer la clave detectando y comparando el texto de reto sin encriptar y luego el mensaje de respuesta encriptado. Una vez extraída la clave WEP, cualquier información encriptada que se transmite a través del enlace puede decodificarse con facilidad.

Etapa 3: Asociación 802.11

Esta etapa finaliza la seguridad y las opciones de tasa de bit, y establece el enlace de datos entre el cliente WLAN y el punto de acceso. Como parte de esta etapa, el cliente aprende el BSSID, que es la dirección MAC del punto de acceso, y el punto de acceso traza un camino a un puerto lógico conocido como el identificador de asociación (AID) al cliente WLAN. El AID es equivalente a un puerto en un switch. El proceso de asociación permite al switch de infraestructura seguir la pista de las tramas destinadas para el cliente WLAN, de modo que puedan ser reenviadas.

Una vez que un cliente WLAN se ha asociado con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

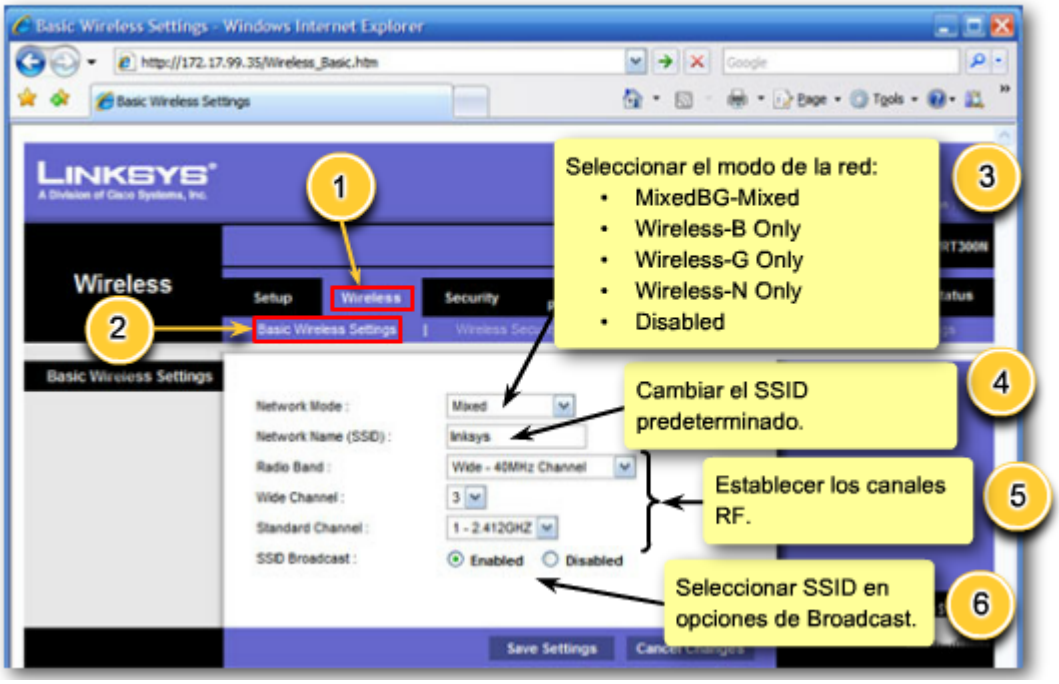
11.10.Configuración de los parámetros inalámbricos básicos

La pantalla Basic Setup es la primera pantalla que ve cuando accede a la utilidad basada en la Web. Haga clic en la etiqueta Wireless y luego seleccione la etiqueta Basic Wireless Settings.

Configuraciones inalámbricas básicas

- Network Mode - Si tiene los dispositivos Wireless-N, Wireless-G, y 802.11b en su red, mantenga Mixed, la configuración predeterminada. Si tiene los dispositivos Wireless-G y 802.11b, seleccione BG-Mixed. Si sólo tiene dispositivos Wireless-N, seleccione Wireless-N Only. Si sólo tiene dispositivos Wireless-G, seleccione Wireless-G Only. Si sólo tiene dispositivos Wireless-B, seleccione Wireless-B Only. Si quiere desactivar el networking, seleccione Disable.
- Network Name (SSID) - El SSID es el nombre de red compartido entre todos los puntos en la red inalámbrica. El SSID debe ser idéntico para todos los dispositivos en la red inalámbrica. Distingue entre mayúsculas y minúsculas, y no debe exceder los 32 caracteres (utilice cualquier caracter en el teclado). Para mayor seguridad, debe cambiar el SSID predeterminado (linksys) a un nombre único.
- SSID Broadcast - Cuando los clientes inalámbricos inspeccionan el área local para buscar redes inalámbricas para asociarse, detectan el broadcast del SSID mediante el punto de acceso. Para transmitir el SSID, mantenga Enabled, que es la configuración predeterminada. Si no quiere transmitir el SSID, seleccione Disabled. Cuando termine de realizar los cambios a esta pantalla, haga clic en el botón Save Settings, o haga clic en el botón Cancel Changes para deshacer sus cambios. Para más información, haga clic en Help.
- Radio Band - Para un mejor rendimiento en una red que utiliza dispositivos Wireless-N, Wireless-G, y Wireless-B, mantenga la opción Auto como la predeterminada. Para dispositivos Wireless-N, únicamente, seleccione Wide - 40MHz Channel. Para networking, únicamente, Wireless-G y Wireless-B, seleccione Standard - 20MHz Channel.
- Wide Channel - Si seleccionó Wide - 40MHz Channel para la configuración de Radio Band, esta configuración está disponible para su canal Wireless-N principal. Seleccione cualquier canal del menú desplegable.
- Standard Channel - Seleccione el canal para networking Wireless-N, Wireless-G y Wireless-B. Si seleccionó Wide - 40MHz Channel para la configuración de Radio Band, el canal estándar es un canal secundario para Wireless-N.

Configuración de los parámetros inalámbricos básicos



11.11.Configuración de seguridad

Esta configuración ajustará la seguridad de su red inalámbrica. Existen siete modos de seguridad inalámbrica que el WRT300N admite. Se listan aquí en el orden en que los ve en la GUI, desde el más débil al más fuerte, con excepción de la última opción, que está deshabilitada:

- WEP
- PSK-Personal o WPA-Personal en v0.93.9 firmware o posterior
- PSK2-Personal o WPA2-Personal en v0.93.9 firmware o posterior
- PSK-Enterprise o WPA-Enterprise en v0.93.9 firmware o posterior
- PSK2-Enterprise o WPA2-Enterprise en v0.93.9 firmware o posterior
- RADIUS
- Disabled

Cuando vea "Personal" en un modo de seguridad, no se está utilizando un servidor AAA. "Enterprise" en el modo seguridad significa un servidor AAA y la utilización de una autenticación EAP.

Aprendió que el WEP es un modo de seguridad con fallas. PSK2, que es lo mismo que WPA2 o IEEE 802.11i, es la opción preferida para una mejor seguridad. Si WPA2 es la mejor, se preguntará por qué hay tantas otras opciones. La respuesta es que muchas LAN inalámbricas admiten dispositivos viejos. Dado que todos los dispositivos de clientes que se asocian a un punto de acceso deben

ejecutar el mismo modo de seguridad que ejecuta el punto de acceso, éste debe estar configurado para admitir el dispositivo que ejecuta el modo de seguridad más débil. Todos los dispositivos de LAN inalámbricas fabricados luego de marzo de 2006 deben poder admitir WPA2 o, en el caso de los routers Linksys, PSK2; por lo que en el tiempo, a medida que se mejoren los dispositivos, será capaz de conmutar el modo de seguridad de su red a PSK2.

La opción RADIUS que está disponible para un router Linksys inalámbrico permite utilizar un servidor RADIUS en combinación con WEP.

Para configurar la seguridad, realice lo siguiente:

- Security Mode - Seleccione el modo que quiera utilizar: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2-Enterprise, RADIUS, o WEP.
- Mode Parameters - Cada uno de los modos PSK y PSK2 tiene parámetros que puede configurar. Si selecciona la versión de seguridad PSK2-Enterprise, debe tener un servidor RADIUS adjunto a su punto de acceso. Si tiene esta configuración, necesita configurar el punto de acceso para que apunte al servidor RADIUS.
- Dirección IP del servidor RADIUS - Ingrese la dirección IP del servidor RADIUS.
- RADIUS Server IP Address - Ingrese el número de puerto utilizado por el servidor RADIUS. De manera predeterminada, es 1812.
- Encryption - Seleccione el algoritmo que quiere utilizar, AES o TKIP. (AES es un método de encriptación más sólido que TKIP.)
- Pre-shared Key - Ingrese la clave compartida por el router y sus otros dispositivos de red. Debe tener entre 8 y 63 caracteres.
- Key Renewal - Ingrese el período de renovación de la clave, que le dirá al router con qué frecuencia debe cambiar las claves de encriptación.

Cuando termine de realizar los cambios a esta pantalla, haga clic en el botón Save Settings o haga clic en el botón Cancel Changes, para deshacer sus cambios.

Configuración de seguridad