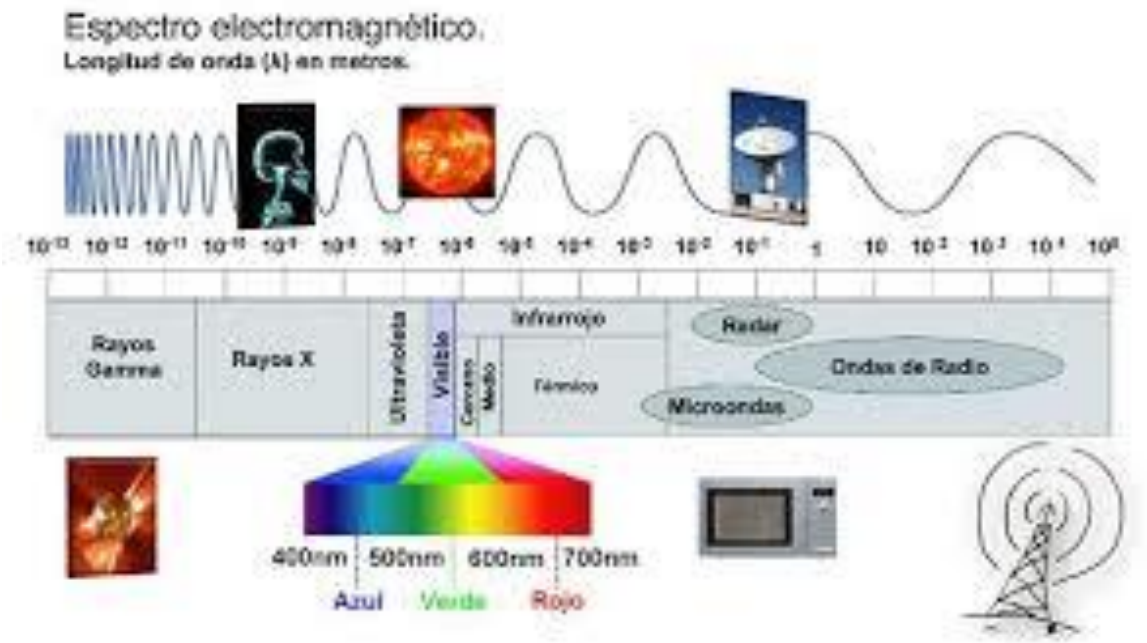
Redes inalámbricas

Temario

- Redes inalámbricas
- Estándares inalámbricos IEEE 802.11
  - IEEE 802.11 Legacy
  - IEEE 802.11 a
  - IEEE 802.11 b
  - IEEE 802.11 g
  - IEEE 802.11 n
  - Canales no superpuestos
- Estructura, características y componentes de una WLAN
  - SSID
  - Modo AD HOC
  - Modo Infraestructura
  - Tipos de antenas
- Conjuntos de servicios
  - IBSS
  - BSS
  - ESS
- Seguridad en redes inalámbricas
  - Broadcast del SSID
  - Filtrado de MAC
  - Autenticación (Abierta, WEP, WPA, WPA2)
  - Encriptación (TKIP, AES)

Wireless

- El término **WIRELESS** (inalámbrico o sin cables) es usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas (en vez de cables) llevan la señal sobre parte o toda la trayectoria de la comunicación
- Los primeros transmisores sin cables vieron la luz a principios del siglo XX usando la radiotelegrafía (código Morse). Más adelante, como la ***modulación*** permitió transmitir voces y música a través de la radio, el medio se llamó ***radio***. Con la aparición de la televisión, el fax, la comunicación de datos, y el uso más eficaz de una porción más grande del ***espectro electromagnético*** se ha resucitado el término ***wireless***.



Wireless (cont.)

- Algunos ejemplos comunes de equipos inalámbricos en uso hoy en día incluyen:
  - Teléfonos móviles, que permiten conectividad entre personas.
  - El sistema de posicionamiento global (GPS), que permite que comprobar nuestra localización en cualquier parte de la tierra.
  - Periféricos inalámbricos, como el mouse, los teclados y las impresoras.
  - Teléfonos inalámbricos, de más corto alcance que los teléfonos móviles.
  - Televisión vía satélite, permiten que los espectadores, desde casi cualquier parte, seleccionen entre centenares de canales.
  - LANs inalámbricas (WLAN), proporcionan flexibilidad y fiabilidad para usuarios de una red LAN.
- En este curso nos vamos a enfocar exclusivamente en las LANs inalámbricas o WLANs.

Wireless (cont.)

- Lo primero que tenemos que conocer es para lograr la interconectividad de los diferentes dispositivos inalámbricos, los mismos deben estar sujetos a estándares.
- Las principales entidades que se encargan de esta interoperabilidad son:
  - **Wi-Fi Alliance**: es una asociación comercial que promueve la tecnología Wi-Fi y certifica los productos Wi-Fi, si se ajustan a ciertas normas de interoperabilidad.
  - **IEEE**: el **Instituto de Ingeniería Eléctrica y Electrónica** especifica cómo se modula la radiofrecuencia (RF) para transportar información.
  - **ITU-R** (Sector de **Radiocomunicaciones** de la **Unión Internacional de Telecomunicaciones**): Su función es la gestión internacional del espectro de frecuencias radioeléctricas y de la órbita de satélites, y los recursos para desarrollar normas para sistemas de radiocomunicaciones con el objetivo de garantizar el uso eficaz del espectro.

Estándares inalámbricos IEEE 802.11

Estándares inalámbricos

ESTÁNDAR IEEE	AÑO	FRECUENCIA		VELOCIDAD		CANALES NO SUPERPUESTOS	COBERTURA (INTERIOR)	COMPATIBILIDAD
				TEÓRICA	REAL			
802.11a	1999	5.7 GHz		54 Mbps	25Mbps	14	30 m	-
802.11b	1999	2.4 GHz		11 Mbps	6 Mbps	3	45 m	-
802.11g	2003	2.4 GHz		54 Mbps	25 Mbps	3	50 m	802.11b
802.11n	2009	BW canal 20 MHz	2.4 GHz 5.7 GHz	>300 Mbps	>100 Mbps	3 7	70 m	802.11a/b/g
		BW canal 40 MHz	2.4 GHz 5.7 GHz	144 Mbps	74 Mbps	3 14		
802.11ac	2013	2.4 y 5.5 GHz		1.3 Gbps	-	-	-	802.11n/ac
802.11ad	2014	2.4, 5 y 60 GHz		7 Gbps	-	-	-	802.11a/b/g/n/ac

Estándares IEEE 802.11

- IEEE 802.11 Legacy

  La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y Mbps que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles.

  El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

Estándares IEEE 802.11 (cont.)

- IEEE 802.11 a

  La revisión 802.11a fue aprobada en 1999. Utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz, con una velocidad máxima de 54 Mbps. 802.11a tiene 14 canales no superpuestos. No puede interoperar con equipos del estándar 802.11b. Maneja modulación OFDM.

- IEEE 802.11 b

  La revisión 802.11b del estándar original fue ratificada en 1999. Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. Funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 6 Mbps sobre TCP y 7,1 Mbps sobre UDP. Utiliza modulación DSSS.

Estándares IEEE 802.11 (cont.)

- IEEE 802.11 g

  En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps, que en promedio es de 25 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar IEEE 802.11b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del nuevo estándar lo tomó el hacer compatibles ambos modelos. Sin embargo, en redes bajo el estándar IEEE 802.11g, la presencia de nodos bajo el estándar IEEE 802.11b reduce significativamente la velocidad de transmisión.

  Utiliza modulación DSSS y OFDM

  Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

Estándares IEEE 802.11 (cont.)

- IEEE 802.11 n

  IEEE 802.11n está construido basándose en estándares previos de la familia 802.11, agregando Multiple-Input Multiple-Output (MIMO) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

  MIMO es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información (cuidando la coherencia) que al utilizar una sola antena. Dos beneficios importantes que provee a 802.11n, son la diversidad de antenas y el multiplexado espacial.

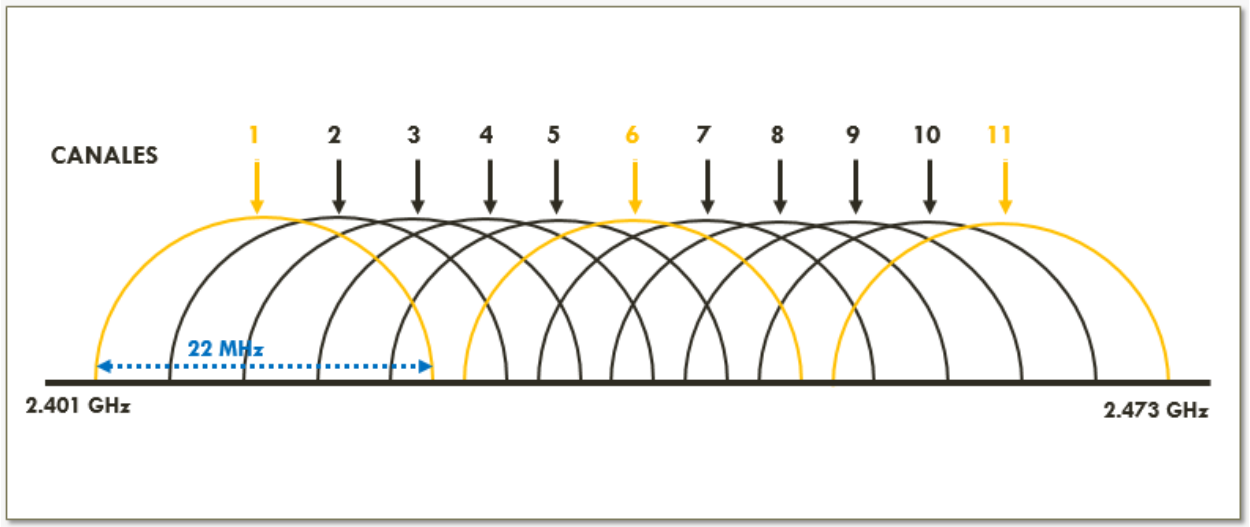
  La tecnología MIMO depende de señales multirruta. Las señales multirruta son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión (line of sight, LOS) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multiruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multirutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

  Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente múltiples flujos de datos independientes, transferidos simultáneamente con un canal espectral de ancho de banda.

  Channel Bonding, también conocido como 40 MHz o unión de interfaces de red, es la segunda tecnología incorporada al estándar 802.11n la cual puede utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente.

Canales no superpuestos

En las tecnologías que trabajan principalmente en los 2,4 GHz, la mayoría de los canales comparten la frecuencia en la que trabajan. Están superpuestos o solapados como se muestra en el gráfico inferior.



Dos dispositivos que estén trabajando en canales superpuestos y estén dentro del rango de cobertura del otro, generarán interferencias entre sus señales. Es por ellos se recomienda que utilicen canales no superpuestos. En el ejemplo vemos, que los canales 1, 6 y 11, no sufren solapamientos.

Estructura, características y componentes de una WLAN

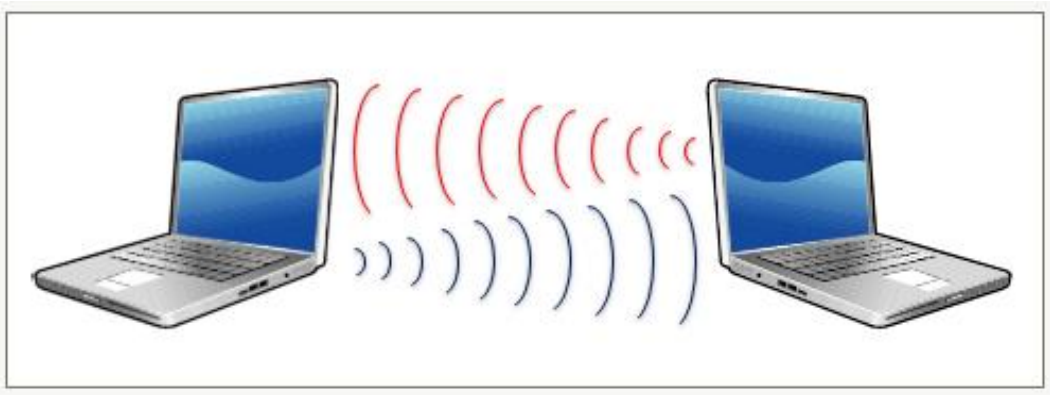
SSID

Service Set IDentification – Identificación del conjunto de servicios.

Es un identificador único que consta de hasta 32 caracteres alfanuméricos y que se utiliza para denominar redes inalámbricas. Cuando varias redes inalámbricas se superponen en un lugar determinado, el SSID asegura de que los datos se envían al destino correcto, ya que cada paquete enviado a través de una red inalámbrica incluye el SSID.

Modo AD HOC

- Es un tipo de red descentralizada e independiente, en la que cada nodo se conecta con otro nodo, sin ningún tipo de dispositivo intermedio.
- Estos nodos o clientes cuentan con placas de red inalámbrica, ya sea incorporada, PCI, USB o PCMCIA

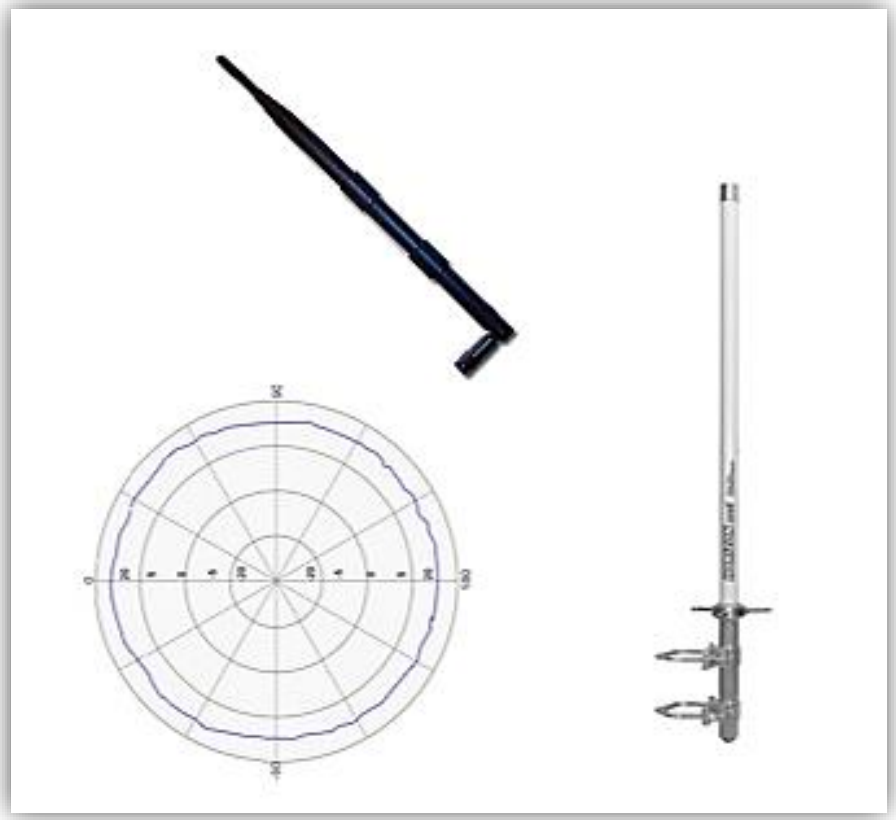


Modo Infraestructura

- En este tipo de red, los nodos se conectan a un dispositivo intermedio, un punto de acceso inalámbrico (Access Point).
- El AP no solamente brinda mayor organización en las comunicaciones, sino que además permite la conexión de la red inalámbrica a una red cableada.

Tipos de antena

Omnidireccionales



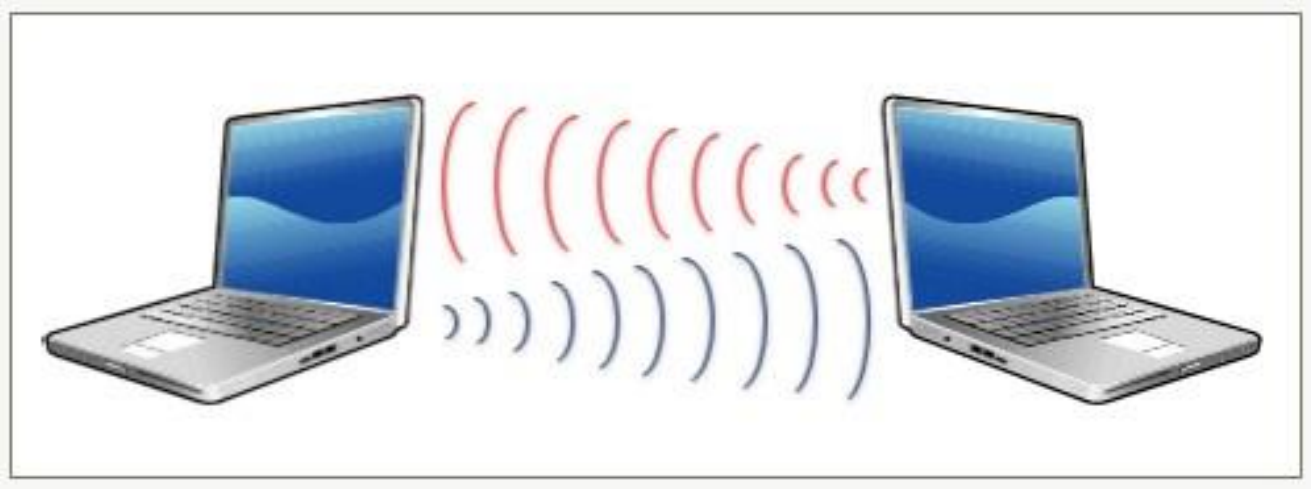
Direccionales

Conjuntos de servicios

IBSS

Independent Basic Service Set - Conjunto de Servicios Básico Independiente.

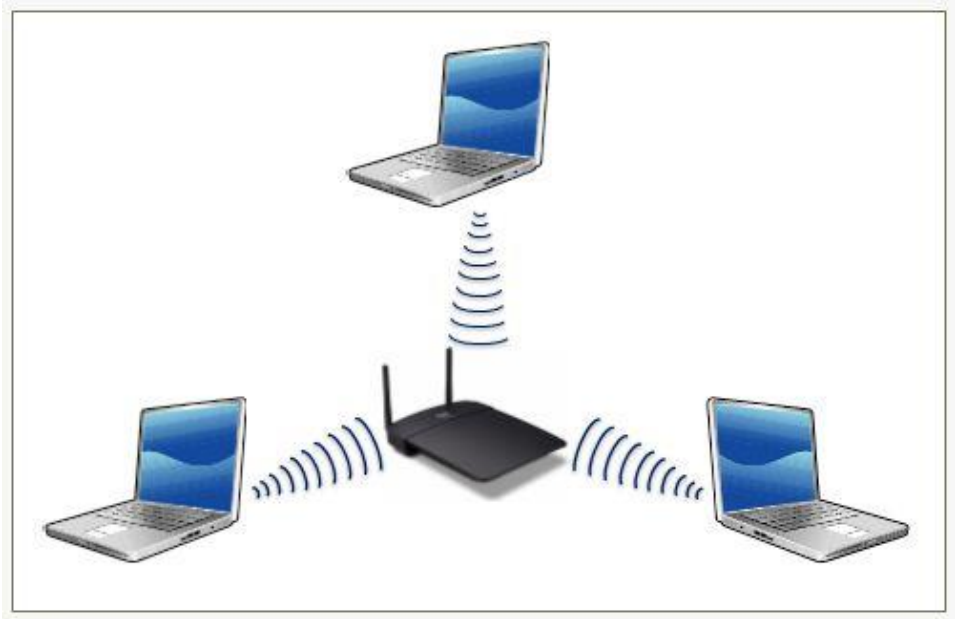
El modo de este conjunto de servicios es Ad Hoc y el IBSS está formado por los equipos que se interconectan entre ellos. Es ***independiente*** debido a que no participa un AP en este tipo de conexión.



BSS

Basic Service Set - Conjunto de Servicios Básico.

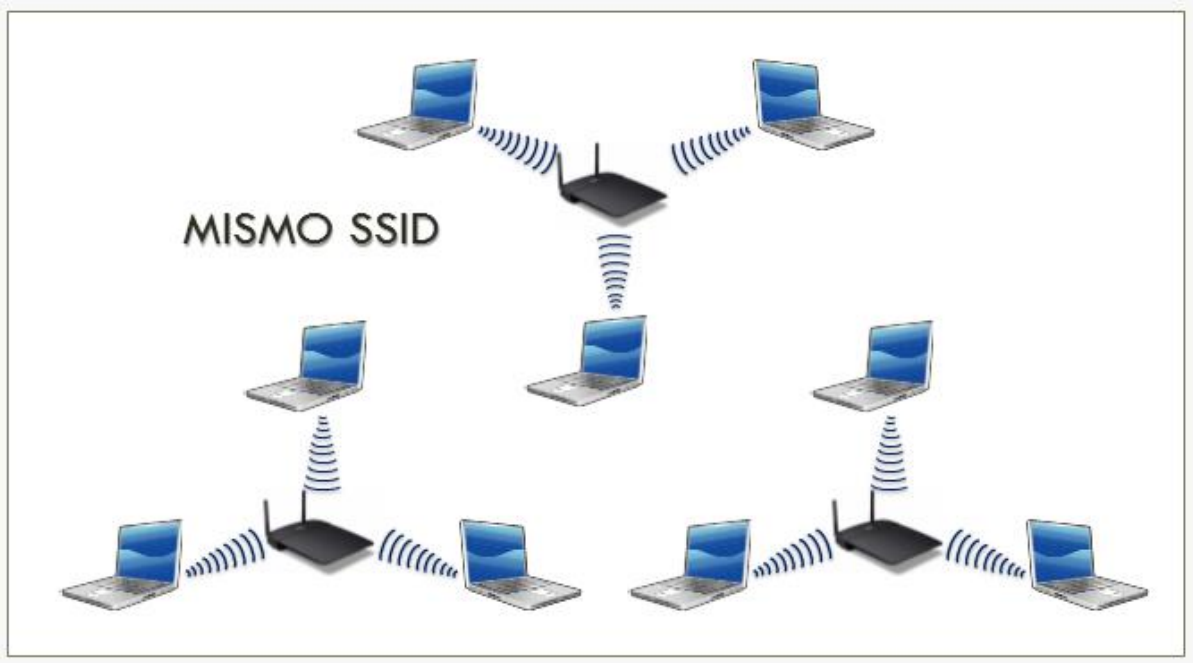
El modo de este conjunto de servicios es Infraestructura y el BSS está formado por el conjunto de equipos de que se interconectan entre ellos a través de un ***único*** punto de acceso.



ESS

Extended Service Set - Conjunto de Servicios Extendido.

El modo de este conjunto de servicios es Infraestructura y el ESS está formado por el conjunto de dispositivos que se interconectan a través de ***varios*** puntos de acceso. Los puntos de acceso ***comparten el mismo SSID***.



Seguridad en redes inalámbricas

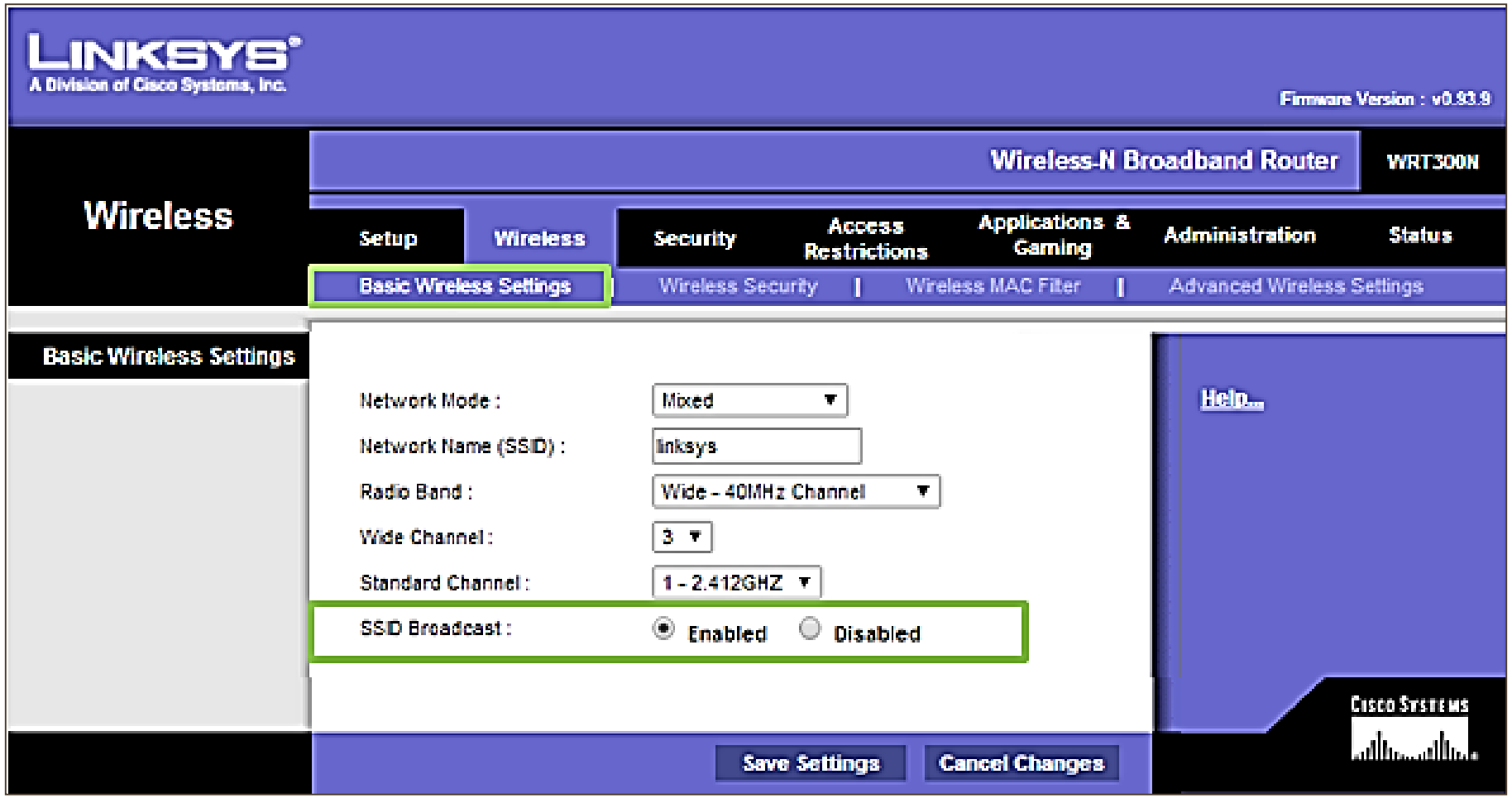
Seguridad de los datos

- Las redes LAN cableadas utilizan como medio físico de propagación, medios "contenidos" como el cable de cobre y fibra óptica principalmente. Son contenidos ya que la señal circula exclusivamente por ese medio sin propagarse fuera de él. Este tipo de medio es más seguro, ya que si alguien quisiera conectarse a nuestra red, debería tener acceso a alguna boca de trabajo o a algún dispositivo intermedio, como un switch.
- Las redes inalámbricas utilizan como medio físico de propagación el medio ambiente. Cualquier individuo con un dispositivo con placa de red inalámbrica y dentro del rango de propagación de la señal podría conectarse a nuestra red o capturar información que se propagara por el medio ambiente.
- En su diseño original, la seguridad en las redes inalámbricas no era una necesidad o preocupación. Con el correr de los tiempos, fue necesaria la implementación de diferentes soluciones para brindar seguridad a las instalaciones inalámbricas.

Broadcast del SSID

- El AP transmite periódicamente un BEACON, presentándose a los clientes inalámbricos a su alcance. El beacon es una trama con información como: SSID, velocidades soportadas e implementación de seguridad.
- Los AP pueden configurarse para que no transmitan esa trama, aunque ***no es una medida de seguridad eficiente por si sola***. Esto es debido a que, aunque el AP no difunda el beacon, las tramas de datos que se propagan entre el AP y un cliente conectado legítimamente, incluye el SSID de la red, el cual puede ser averiguado por un individuo, capturando las tramas que viajan entre esos dos dispositivos.
- Los clientes inalámbricos a su vez pueden emitir una SONDA, trama que utilizan para encontrar sus redes. Con el SSID capturado, un individuo podría enviar una sonda incluyendo ese SSID e iniciar el proceso de asociación.

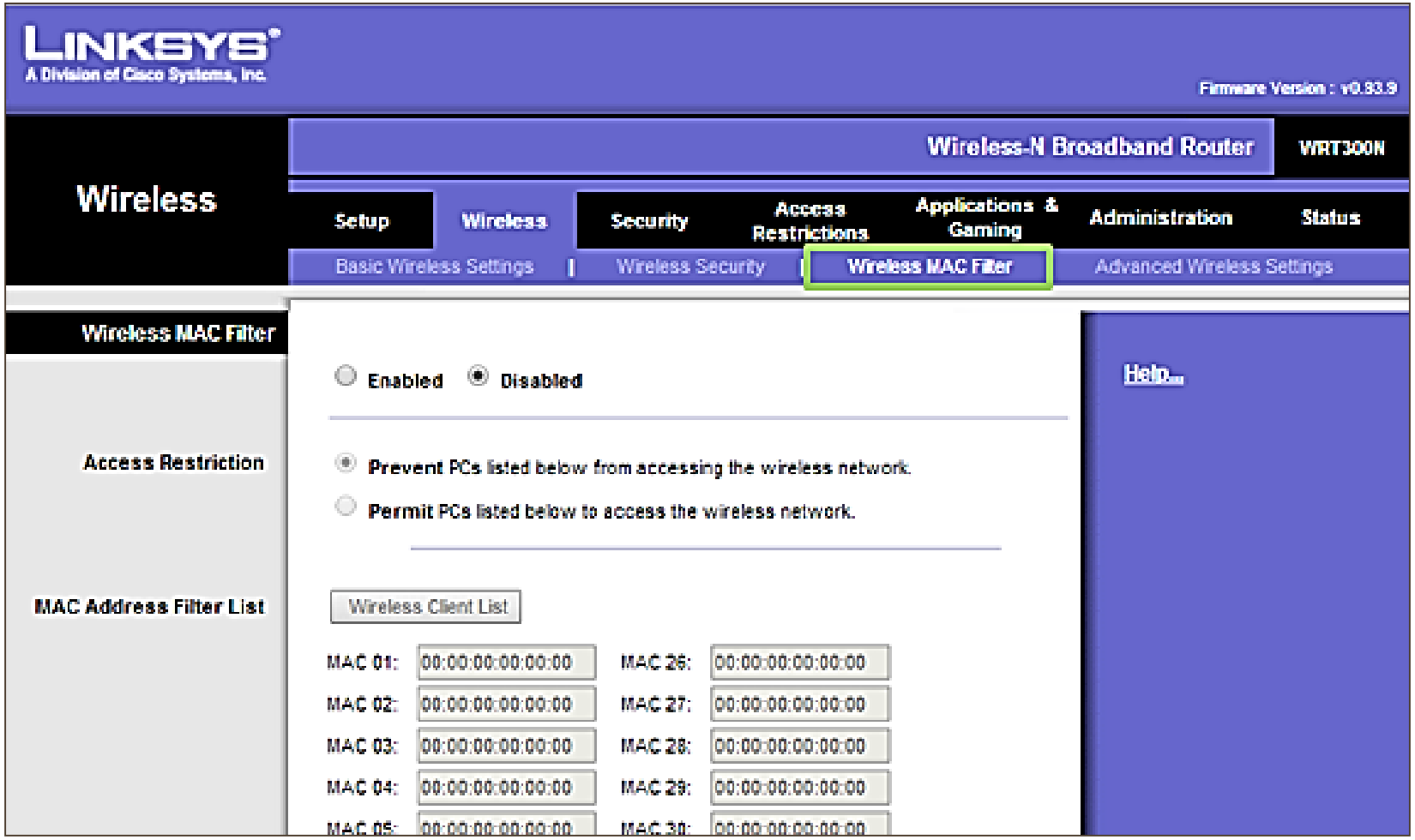
Broadcast del SSID (cont.)



Filtrado de MAC

- Otra medida de seguridad es el filtrado de la direcciones MAC de los clientes inalámbricos.
- Como cualquier placa de red para una red cableada, una placa de red inalámbrica también posee una dirección MAC única, grabada en su memoria ROM.
- En el AP se puede configurar para identificar las direcciones MAC de los clientes permitidos a conectarse.
- Esta medida de seguridad ***no es efectiva por sí sola***, ya que un individuo puede averiguar la dirección MAC de un cliente legítimo, mediante la captura de tráfico entre el AP y el cliente. Mediante algún software específico, puede "falsear" su dirección MAC y utilizar la capturada para poder conectarse a la red inalámbrica.

Filtrado de MAC (cont.)



Autenticación

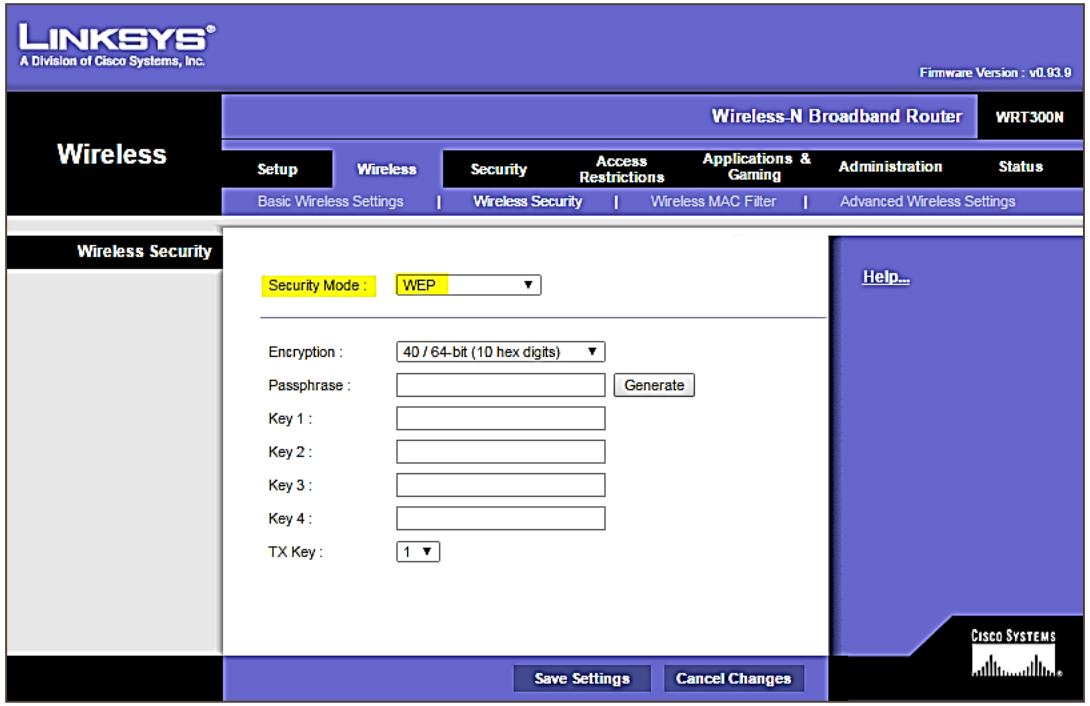
Existen varios modos de autenticación:

- Abierta (Autenticación Nula)
- WEP
- WPA
- WPA2

WEP

Wired Equivalent Privacy – Privacidad Equivalente al Cableado.

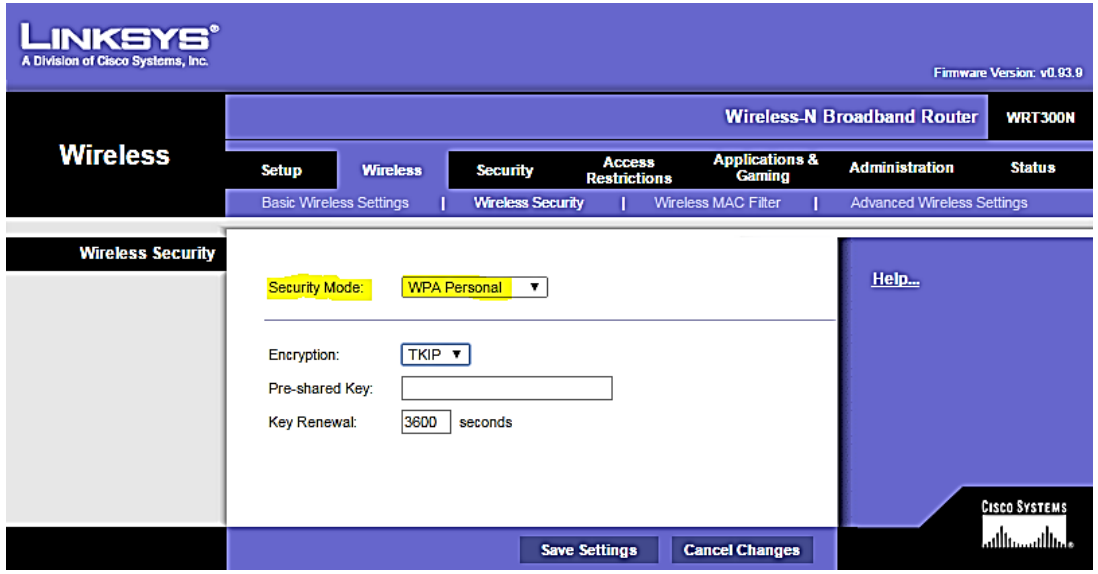
- Primer mecanismo para tratar de asegurar la información.
- Funciona con una clave secreta compartida, que se utiliza tanto para autenticar como también para encriptar los datos.
- Con tiempo y software especializado un individuo puede averiguar la clave y desencriptar los datos y/o asociarse al AP.
- Hoy en día ***no recomendada***, debido a que este tipo de autenticación puede vulnerarse.



WPA

WIFI PROTECTED ACCESS – Acceso WIFI Protegido.

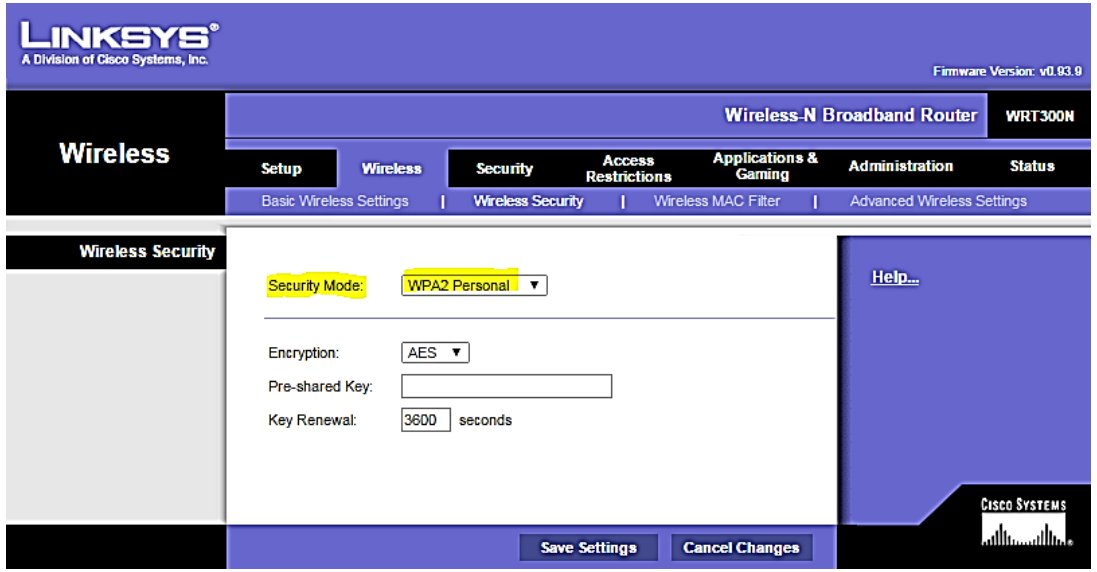
- Modo de seguridad que reemplazó a WEP. Creado por Wi-Fi Alliance
- Utiliza una clave secreta compartida (PSK - Pre Shared Key) para la autenticación y la encriptación de los datos, pero a diferencia de WEP, esta clave se renueva periódicamente dificultando la tarea de los intrusos
- Autenticación fuerte y encriptación mejorada.
- Soporta que el proceso de autenticación lo realice un servidor de seguridad.



WPA2

WIFI PROTECTED ACCESS 2 – Acceso WIFI Protegido 2.

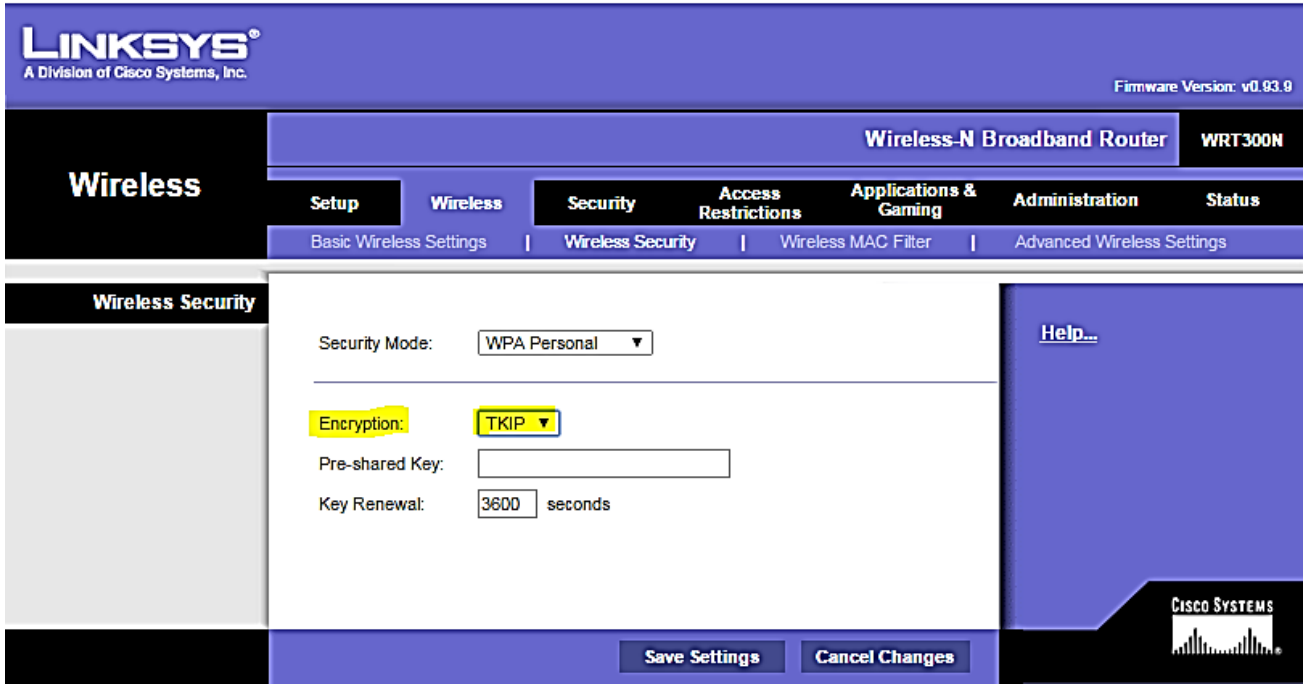
- Método definido por el estándar IEEE 802.11i
- Utiliza una clave secreta compartida (PSK) para la autenticación y la encriptación de los datos, que se renueva periódicamente dificultando la tarea de los intrusos.
- Autenticación más fuerte que WPA y encriptación mejorada.
- Soporta que el proceso de autenticación lo realice un servidor de seguridad.
- **Método de seguridad recomendado.**



Encriptación - TKIP

Temporal Key Integrity Protocol - Protocolo de Integridad de Clave Temporal

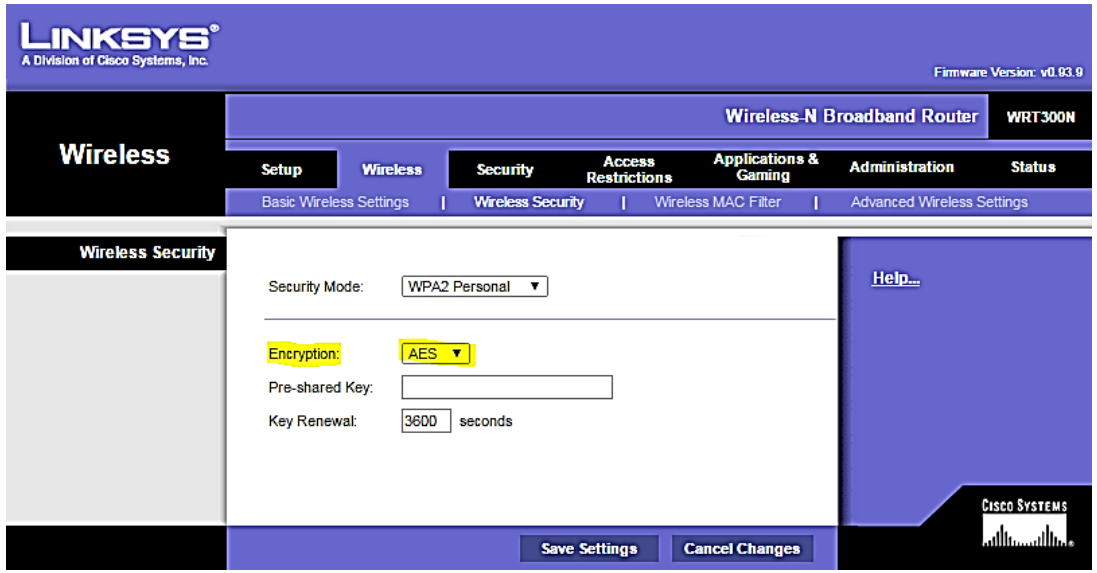
- Encripta el contenido de la Capa 2
- Lleva a cabo un control de la integridad del mensaje en el paquete encriptado
- Es el método de encriptación certificado como WPA



Encriptación - AES

Advanced Encryption Standard - Estándar de Encriptación Avanzada

- Cumple las mismas funciones que TKIP.
- Mejora las características de seguridad de TKIP.
- Alineado al estándar IEEE 802.11i
- **Método de encriptación recomendado**



Preguntas