**Redes Inalámbricas**

La utilización de las WLAN (Wireless LAN) es hoy en día de uso frecuente y cada vez más veloz, eficaz y seguro.

**Normas WLAN**

**La norma IEEE 802.3 establece el estándar para las redes LAN mientras que el IEEE 802.11 lo hace para la familia de redes inalámbricas. Ambas definen, entre otras cosas, el formato de la trama que se diferencia en que las  WLAN no usan una trama estándar 802.3.**

Por lo tanto, el término “Ethernet inalámbrica” puede resultar engañoso al ser básicamente diferentes. En el caso de las direcciones MAC es de 6 Bytes (48 bits) para los dos tipos de estándares. La diferencia más grande entre los dos  métodos es la posibilidad de transmitir datos sin necesidad de cableado, aunque esto puede estar limitado al espacio aéreo si existen objetos que puedan interferir con las ondas de radiofrecuencia.

Ethernet puede transmitir de forma full-duplex simplemente si un ordenador se encuentra directamente conectado a un puerto de un switch, creando así su propio dominio de colisión. El CSMA/CD permite a los dispositivos escuchar antes de transmitir o generar un algoritmo de espera ante colisiones en el medio compartido. Debido a que la radiofrecuencia (RF) es un medio compartido, se pueden producir colisiones de la misma manera que se producen en un medio compartido cableado. La principal diferencia es que no existe un método por el que un nodo origen pueda detectar que ha ocurrido una colisión. Por eso, las WLAN utilizan Acceso Múltiple con Detección de Portadora/Carrier y Prevención de Colisiones (CSMA/CA) similar en su funcionamiento al CSMA/CD de Ethernet.

**Estándares WLAN**

**El estándar IEEE 802.11 es un protocolo de comunicaciones que define el uso de las dos capas inferiores del modelo OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento para una red inalámbrica (WLAN).**

La tecnología clave que contiene el estándar 802.11 es el Espectro de Dispersión de Secuencia Directa (DSSS). El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma.  
802.11b también recibe el nombre de Wi-Fi o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso. 802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHZ.

El uso del rango de 5 GHZ no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHZ. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como “duplicación de la velocidad” ha alcanzado los 108 Mbps. En las redes de producción, la velocidad estándar es de 20-26 Mbps.

802.11g ofrece tasa de transferencia que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b utilizando tecnología de modulación por Multiplexión por División de Frecuencia Ortogonal (OFDM). Cisco ha desarrollado un punto de acceso que permite que los dispositivos 802.11b y 802.11a coexistan en la misma WLAN. El punto de acceso brinda servicios de gateway que permiten que estos dispositivos, que de otra manera serían incompatibles, se comuniquen.

802.11n A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

**Autenticación y Asociación WLAN**

La autenticación de las WLAN se produce en la Capa 2 del modelo OSI. Es el proceso de autenticar el dispositivo no al usuario. Este es un punto fundamental a tener en cuenta con respecto a la seguridad, detección de fallos y administración general de una WLAN.

El proceso se inicia cuando el cliente envía una trama de petición de autenticación al AP y éste acepta o rechaza la trama. El cliente recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el AP para derivar la tarea de autenticación a un servidor de autenticación, que realizaría un proceso de credencial más exhaustivo.

La asociación que se realiza después de la autenticación es el estado que permite que un cliente use los servicios del AP para transferir datos.

**Métodos de Autenticación**

**WEP**WEP (Wired Equivalency Privacy) es un sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Está basado en el algoritmo de encriptación RC4, y utiliza claves de 64 bits, de 128 bits o de 256 bits. Es poco seguro debido a su arquitectura, por lo que al aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

**WPA**WPA (Wi-Fi Protected Access – Acceso Protegido Wi-Fi) es un sistema para asegurar redes inalámbricas, creado para corregir las falencias de seguridad de WEP; los investigadores han encontrado varias debilidades en WEP (tal como un ataque estadístico que permite recuperar la clave WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era preparado.

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario; sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK – Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP es dada por el Protocolo de Integridad de Clave Temporal (TKIP – Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El comparador de redundancia cíclica (CRC) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un chequeo de integridad del mensaje llamado “Michael”. Además WPA incluye protección contra ataques de “repetición”, ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es suceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 30 segundos cada vez que se detecta un intento de ataque.

**WPA-2**  
WPA-2 está basada en el nuevo estándar IEEE 802.11i. WPA, por ser una versión previa, que se podría considerar de “migración”, no soporta todas las características, mientras que WPA-2 ya implementa el estándar completo. Particularmente WPA no se puede utilizar en redes ad-hoc.