Introducción a las redes WiFi

La tecnología WiFi nació de la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos. En esta nota, explicamos de qué se trata la transmisión por aire, qué seguridad brinda esa transferencia de datos y los estándares de comunicación más utilizados.

Ing. Rodrigo Hernández
ingrjhernandez@gmail.com

En las comunicaciones inalámbricas, el medio de transmisión siempre es compartido. Esta es una diferencia fundamental con las tecnologías cableadas (ya sean transportadas por cobre o fibra óptica), donde los enlaces son dedicados. Es por esto que la utilización del espacio debe regularse de forma estricta, para que las bandas de frecuencia no se solapen y se eviten las interferencias. Los protocolos de comunicación utilizados por cada uno de los dispositivos que participan de la red son los encargados de coordinar el acceso al medio.

La efectividad de una red inalámbrica depende de varios factores, entre ellos la cantidad de equipos que estén compartiendo la red, las condiciones ambientales, las interferencias electromagnéticas, los obstáculos y la latencia. También hay que destacar que las tasas máximas de transmisión de datos nunca representan la máxima tasa de transmisión de datos "útiles" (throughput), ya que parte de la trama es ocupada por información de control de acceso al medio, control de flujo, encriptación, etc. Podemos decir, entonces, que la tasa de transferencia de datos real siempre está por debajo de lo definido en los estándares. Sin embargo, al ser transmisión por aire y teniendo en cuenta que cualquiera puede acceder al medio (espacio), la seguridad se vuelve un factor crítico y es necesario utilizar autenticación y encriptación de datos para evitar el acceso no autorizado a la red.

ACCESO AL MEDIO

Los estándares inalámbricos IEEE 802.11 utilizan un protocolo de acceso al medio llamado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Su nombre es, de hecho, similar al utilizado en las redes Ethernet cableadas (CSMA/CD: Carrier Sense Multiple Access with Collision Detection), pero su funcionamiento es diferente. En el caso inalámbrico, CA se refiere a evitar la colisión, mientras que en Ethernet se trata de detectar la colisión.

Las redes Wi-Fi son half-duplex, es decir, los dispositivos no pueden transmitir y recibir al mismo tiempo en el mismo canal de radio. Un dispositivo no puede "escuchar" al mismo tiempo que está transmitiendo, por lo que no puede detectar colisiones. Debido a esto, los expertos de la IEEE utilizaron un mecanismo para evitar la colisión que llamaron DCF (Distributed Control Function).

Entonces, de acuerdo con el DCF, un dispositivo WiFi iniciará una transmisión sólo si percibe que el canal no está en uso. Para lograr esto, primero debe reconocer todas las transmisiones, por lo que si un dispositivo no recibe una trama de reconocimiento, supone que hubo colisión y reintenta la comunicación tras un intervalo de tiempo aleatorio. Las colisiones pueden aumentar por varios motivos: a medida que crece el tráfico en la red, los dispositivos móviles no se pueden percibir unos a otros o debido a interferencias.

SEGURIDAD EN REDES WIFI

Dado que el medio de transmisión es el aire, el cual es naturalmente accesible por cualquier dispositivo, es fundamental asegurar que el acceso a la red será restringido a aquellos dispositivos autorizados. Para esto, el estándar 802.11i define distintos sistemas, como WEP, WPA y WPA2, en los cuales los dispositivos utilizan claves para autenticarse. Los AP emiten en forma periódica un aviso que contiene el SSID (Service Set IDentifier), lo cual permite a los usuarios identificar al AP correcto y conectarse a él. El proceso de conexión comienza con un procedimiento de autenticación, para lo cual se genera una clave (key).

Existen tres tipos de autenticación en las redes WiFi.

1. WEP (Wired-Equivalent Privacy key): como su nombre lo indica, el objetivo de este método es intentar hacer que las redes inalámbricas sean tan seguras como las cableadas. Lamentablemente fue rápidamente vulnerado y en la actualidad no se recomienda su uso. Al inicio del proceso de autenticación, el dispositivo cliente envía un mensaje de texto sin encriptar, el cual es encriptado por el AP usando una clave compartida y devuelto al cliente. Las claves son usualmente de 128 o 256 bits.

El principal problema de WEP es la administración de la llave. Generalmente, las llaves son distribuidas en forma manual o a través de otra vía segura. WEP usa llaves compartidas, es decir, el AP utiliza la misma llave para todos los clientes por lo que si la llave es descubierta, todos los usuarios son puestos en riesgo. Para obtener la llave solamente es necesario escuchar hasta obtener la devolución de las tramas de autenticación.

Utilizar WEP es mejor que nada; cuando no haya nada mejor es recomendable usarlo. Después de todo, no todo el mundo quiere vulnerar redes inalámbricas. Una buena recomendación es utilizar seguridad en las capas superiores, por ejemplo mediante encriptación SSL, TSL, etc.

2. WPA (Wi-Fi Protected Access): para salvar las fallas de seguridad de WEP se desarrolló WPA. Este sistema fue diseñado con el auspicio de WiFi Alliance y se utilizó una parte del estándar 802.11i, que luego se actualizó para reemplazar el protocolo WEP. Uno de los elementos clave de WPA es TKIP (Temporal Key Integrity Protocol), que forma parte del estándar 802.11i y opera generando claves dinámicas.

WPA puede utilizar en forma opcional AES-CCMP (Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) como reemplazo de TKIP.

3. WPA2 / WPAv2: es, actualmente, la mejor técnica disponible para asegurar una red WiFi. Utiliza en forma obligatoria AES-CCMP y es empleada en todos los dispositivos que se fabrican en la actualidad.

ESTÁNDARES

En la actualidad accedemos a redes inalámbricas de todo tipo, las cuales nos ofrecen conectividad a los múltiples dispositivos que utilizamos en nuestra vida diaria.

Bajo la denominación "WiFi" se ubican distintos estándares de comunicación que son comúnmente utilizados.

Estos son:

- 802.11a: red inalámbrica con portadora en la banda ISM de 5 GHz y una tasa de transferencia de datos de hasta 54 Mbps.
- 802.11b: red inalámbrica con portadora en la banda ISM de 2,4 GHz y una tasa de transferencia de datos de hasta 11 Mbps.
- 802.11g: red inalámbrica con portadora en la banda ISM de 2,4 GHz y una tasa de transferencia de datos de hasta 54 Mbps.
- 802.11i: autenticación y encriptación.
- 802.11n: red inalámbrica con portadora en la banda ISM de 2,4 GHz y 5 GHz, con tasas de transferencia de datos de hasta 600 Mbps.
- 802.11ac: red inalámbrica con portadora debajo de 6 GHz, con tasas de transferencia de datos de al menos 1 Gbps en operación multiestación y 500 Mbps en un solo enlace. ■

+ datos: **video-ip.net**