Tema 12-Tecnologías a nivel de enlace

El WiFi es una tecnología de comunicación inalámbrica que permite la transmisión de datos a través del aire mediante ondas de radio. Una de las principales ventajas del WiFi es la movilidad que proporciona, ya que no es necesario estar conectado mediante cables, lo que permite la conexión a Internet o a una red local en cualquier lugar donde haya señal.

Es importante destacar que el WiFi no es un sustituto de las redes tradicionales, sino que se utiliza principalmente para proporcionar conectividad a dispositivos móviles o portátiles que no pueden estar conectados mediante cables.

Los estándares WiFi son definidos por la organización WiFi Alliance, y se pueden consultar en su página web. Estos estándares definen las especificaciones técnicas de la tecnología, como la velocidad de transmisión, el rango de frecuencias utilizadas y las medidas de seguridad.

En una red WiFi, se utiliza la tecnología 802.11 para enviar las tramas de datos a su destino. Estas tramas se transmiten mediante ondas de radio a través de un medio inalámbrico. Para gestionar la comunicación entre los dispositivos inalámbricos y la red, se utiliza un punto de acceso, que es el encargado de enviar y recibir las tramas de datos.

Los dispositivos inalámbricos, como portátiles, tabletas o móviles, tienen una interfaz de red inalámbrica que les permite conectarse a la red WiFi. Estos dispositivos utilizan una tarjeta inalámbrica para comunicarse con el punto de acceso y acceder a la red.

BSS y ESS

El Basic Service Set (BSS) es un grupo de estaciones que se comunican entre sí en una red inalámbrica. Hay dos tipos de BSS: BSS independiente (ad-hoc) y BSS infraestructura. En el primer tipo, las estaciones se comunican directamente entre sí y se utiliza para grupos reducidos y con carácter temporal, como una reunión. En cambio, en el BSS infraestructura, se utiliza un punto de acceso como intermediario para la comunicación entre estaciones móviles. Cada estación se asocia a un punto de acceso, y los puntos de acceso envían periódicamente una señal baliza. La distancia de las estaciones se mide desde la estación al punto de acceso, no entre estaciones.

Por otro lado, el Extended Service Set (ESS) es una asociación de BSSs, donde varias BSSs se encadenan usando un backbone. La transición BSS permite que los usuarios se muevan de una área de cobertura a otra, sin perder la conectividad. En resumen, el BSS y ESS son dos conceptos importantes en la configuración de redes inalámbricas, ya que permiten establecer la comunicación entre diferentes estaciones y la movilidad de los usuarios.

Asociación

La asociación en redes WiFi se refiere al proceso mediante el cual un equipo móvil (como un portátil, un teléfono móvil, una tableta, etc.) se conecta a un punto de acceso (PA) para tener acceso a la red inalámbrica. El proceso de asociación comienza con la identificación del PA y la red inalámbrica a la que está asociado, que se realiza mediante el SSID (Service Set Identifier).

Existen dos métodos principales para identificar el SSID: la exploración pasiva y la exploración activa. En la exploración pasiva, el equipo móvil espera a recibir tramas baliza del PA que contienen el SSID. En la exploración activa, el equipo solicita a los PA cercanos que se identifiquen y les envíen sus tramas baliza.

Una vez identificado el PA y el SSID, el equipo móvil determina a cuál PA asociarse, por ejemplo, mediante la señal más potente. Después de la asociación, se lleva a cabo el proceso de autenticación y se establece la configuración de red, que suele incluir la asignación de una dirección IP mediante DHCP.

La seguridad en las redes WiFi puede incluir el filtrado de direcciones MAC, así como el uso de un servidor de autenticación (como RADIUS) para la autenticación de usuarios mediante login y password.

CSMA/CA

El acceso múltiple en las redes WiFi se gestiona a través del protocolo de acceso al medio CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). A diferencia de Ethernet, que utiliza el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection), en las redes WiFi no es posible detectar colisiones porque el nodo emisor no puede recibir mientras está transmitiendo. Por lo tanto, en lugar de detectar colisiones, se trata de evitarlas.

Cuando una estación WiFi desea transmitir, primero escucha el canal para detectar si está siendo utilizado por otra estación. Si el canal está libre, la estación comienza a transmitir su trama de datos. Si el canal está ocupado, la estación espera un tiempo aleatorio antes de volver a intentar la transmisión. Si la estación recibe una trama de un punto de acceso, envía un mensaje de confirmación ACK al punto de acceso para indicar que ha recibido la trama correctamente.

La solución al problema de los nodos ocultos en WiFi se llama RTS/CTS (Request To Send/Clear To Send). Cuando un emisor quiere transmitir, primero envía un RTS indicando el tiempo total que necesita. Luego, cuando el punto de acceso recibe el RTS, responde con un CTS indicando el tiempo restante que tiene reservado el canal. De esta manera, el emisor sabe que tiene el canal disponible y el resto de los dispositivos saben que el canal estará ocupado.

Esta solución tiene varios beneficios, entre ellos, que una trama solo se enviará después de reservar el canal, lo que evita colisiones de nodos ocultos. Además, las colisiones solo se producen sobre las tramas RTS o CTS, que son tramas cortas.

Sin embargo, también tiene algunas desventajas. Por ejemplo, introduce un retardo en la transmisión debido a la necesidad de enviar las tramas RTS y CTS antes de enviar la trama real. Además, consume recursos del canal y, por lo tanto, se establece un umbral de tamaño de trama a partir del cual se utiliza esta técnica.

Seguridad

El hecho de que el medio de transmisión en redes inalámbricas sea el aire lo hace más susceptible a escuchas y, por lo tanto, más vulnerable a ataques. Para asegurar la privacidad y la seguridad de las comunicaciones inalámbricas, se utilizan mecanismos adicionales de seguridad.

Inicialmente se utilizó WEP (Wired Equivalent Privacy), que es un método de cifrado de clave estática. Sin embargo, se descubrió que WEP era muy fácil de romper y no proporcionaba suficiente seguridad. Actualmente se utilizan las familias WPA (WiFi Protected Access), WPA2 y WPA3.

WPA implementa TKIP (Temporal Key Integrity Protocol) para cifrado, lo que cambia dinámicamente las claves según se utiliza el sistema. También utiliza MIC para asegurar la integridad de los datos transmitidos.

WPA2, por su parte, utiliza AES para cifrado y CCMP para integridad, lo que lo hace más seguro que WPA. También utiliza una clave de 128 bits para una mayor protección.

Finalmente, WPA3 es el método más seguro disponible en la actualidad, utilizando una clave de 192 bits y proporcionando una mejor protección incluso si se utilizan contraseñas simples. Además, la contraseña inicial no se utiliza para derivar las claves de sesión, lo que proporciona una mayor protección en caso de que la contraseña sea descubierta