UTN
FACULTAD REGIONAL MENDOZA
UNIVERSIDAD TECNOLÓGICA NACIONAL

WLAN

GRUPO N° 4

Integrantes

Hernandez, Edgardo Humberto
Bacin Rauber, Janaina - 47726
Condori, Facundo
Hidalgo Molina, Jesús Exequiel
Pereyra Gamez, Alvaro
Rodriguez Guzman, Sara
Hofer, Luis Sebastian

ÍNDICE

1. Introducción a las Redes Inalámbricas WLAN

Una red inalámbrica de área local (WLAN, por sus siglas en inglés "Wireless Local Area Network") es una red que permite la conexión de dispositivos móviles o fijos utilizando ondas de radio en lugar de cables físicos. Las WLANs son esenciales en entornos donde la movilidad y la flexibilidad son prioritarias, permitiendo a los usuarios conectarse a internet y compartir recursos sin necesidad de conexiones físicas.

2. Tecnología de WLAN

La tecnología detrás de las redes inalámbricas WLAN se basa en estándares de la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), principalmente los de la familia **IEEE 802.11**. Estos estándares definen los aspectos técnicos de las redes inalámbricas, como el tipo de modulación, las frecuencias de operación, las tasas de transmisión y los mecanismos de acceso al medio.

- **IEEE 802.11**: Base general para WLAN.
- **IEEE 802.11a/b/g/n/ac/ax**: Extensiones y versiones mejoradas de la tecnología inicial.

Frecuencias de Operación

Las WLAN operan en dos bandas de frecuencia principales:

- **2.4 GHz**: Esta es la banda más antigua y tiene un mayor alcance, pero está más congestionada debido a que muchos dispositivos la utilizan (teléfonos, microondas, etc.).
- **5 GHz**: Ofrece más canales y menos interferencias, pero con un rango más corto que la banda de 2.4 GHz.

3. Tipos de WLAN

3.1. Según la tecnología y los estándares

3.1.1. IEEE 802.11b

- **Frecuencia**: 2.4 GHz
- **Velocidad Máxima**: Hasta 11 Mbps

- **Características**: Primera versión ampliamente adoptada. Utiliza modulación DSSS (Direct Sequence Spread Spectrum). Tiene menos canales no superpuestos, lo que genera interferencias con otros dispositivos en la misma frecuencia.
- **Uso**: Popular en los años 90, actualmente obsoleto debido a sus bajas velocidades.

3.1.2. IEEE 802.11a

- **Frecuencia**: 5 GHz
- **Velocidad Máxima**: Hasta 54 Mbps
- **Características**: Utiliza OFDM (Orthogonal Frequency Division Multiplexing), lo que permite mayores velocidades y menos interferencias. Sin embargo, su alcance es menor debido a la banda de 5 GHz.
- **Uso**: Implementado en redes que requieren mayor velocidad y menos interferencias, como las empresariales.

3.1.3. IEEE 802.11g

- **Frecuencia**: 2.4 GHz
- **Velocidad Máxima**: Hasta 54 Mbps
- **Características**: Combinó lo mejor de 802.11b (mayor rango) y 802.11a (mayor velocidad). Utiliza OFDM y DSSS, permitiendo compatibilidad con dispositivos 802.11b.
- **Uso**: Dominante en redes domésticas y comerciales hasta la llegada de 802.11n.

3.1.4. IEEE 802.11n

- **Frecuencia**: 2.4 GHz y 5 GHz (dual band)
- **Velocidad Máxima**: Hasta 600 Mbps
- **Características**: Introduce el uso de múltiples antenas (MIMO: Multiple Input, Multiple Output) para mejorar la velocidad y la cobertura. Utiliza canales de 20 MHz o 40 MHz para aumentar las tasas de transmisión.
- **Uso**: Compatible con versiones anteriores, ideal para redes mixtas.

3.1.5. IEEE 802.11ac

- **Frecuencia**: 5 GHz
- **Velocidad Máxima**: Hasta 1.3 Gbps (1300 Mbps)
- **Características**: Aumenta el ancho de banda del canal hasta 160 MHz, utiliza MIMO con múltiples flujos espaciales y modulación 256-QAM. Exclusivo para la banda de 5 GHz, reduciendo interferencias.
- **Uso**: Presente en redes Wi-Fi modernas, con altas velocidades y buena cobertura.

3.1.6. IEEE 802.11ax (Wi-Fi 6)

- **Frecuencia**: 2.4 GHz y 5 GHz

- **Velocidad Máxima**: Hasta 9.6 Gbps
- **Características**: Optimiza la eficiencia en redes con alta densidad de usuarios. Utiliza OFDMA (Orthogonal Frequency Division Multiple Access) y MU-MIMO (Multi-User MIMO), permitiendo comunicación simultánea con múltiples dispositivos.
- **Uso**: Ideal para entornos con muchos dispositivos, como hogares inteligentes y oficinas.

3.2. Según la topología

3.2.1. Infraestructura WLAN

- **Descripción**: Todos los dispositivos se conectan a través de un punto de acceso (AP), que actúa como puente entre la red inalámbrica y la red cableada o internet.
- **Ventajas**:
    - Centraliza el control y la administración.
    - Escalable y fácil de gestionar.
- **Desventajas**:
    - Requiere inversión en puntos de acceso.
    - Si el AP falla, se pierde conectividad.

3.2.2. Ad-hoc WLAN

- **Descripción**: Red punto a punto o Peer-to-Peer (P2P), donde los dispositivos se conectan directamente entre sí sin necesidad de un AP.
- **Ventajas**:
    - No requiere infraestructura adicional.
    - Ideal para comunicaciones temporales y redes pequeñas.
- **Desventajas**:
    - Alcance limitado y menor eficiencia.
    - Menor control sobre la seguridad.

3.2.3. Red de Malla (Mesh WLAN)

- **Descripción**: Los puntos de acceso están interconectados de manera distribuida, permitiendo autorreparación y enrutamiento dinámico.
- **Ventajas**:
    - Alta confiabilidad: los datos se enrutan a través de otros nodos si uno falla.
    - Cobertura ampliada sin necesidad de conexiones físicas entre nodos.
- **Desventajas**:
    - Costosa y compleja de implementar.
    - Requiere administración eficiente de recursos.

3.3. Según el entorno de implementación

3.3.1. WLAN para el hogar

- **Descripción**: Redes domésticas para conectar dispositivos como computadoras, smartphones, tablets y IoT.
- **Características**:
    - Generalmente utilizan 802.11ac o 802.11ax.
    - Enfocadas en facilidad de uso y compatibilidad con diversos dispositivos.

3.3.2. WLAN empresarial

- **Descripción**: Diseñadas para soportar una mayor cantidad de dispositivos en entornos con alta densidad de usuarios.
- **Características**:
    - Implementan roaming y seguridad avanzada.
    - Usan VLAN para separar el tráfico de empleados y visitantes.

3.3.3. WLAN pública

- **Descripción**: Redes en lugares de acceso público, como cafeterías y aeropuertos, proporcionando acceso a internet.
- **Características**:
    - Manejan un alto volumen de conexiones simultáneas.
    - Seguridad básica, priorizando la facilidad de acceso.

3.4. Según el uso o aplicación específica

3.4.1. WLAN para VoIP

- **Descripción**: Optimizada para la transmisión de voz, con baja latencia y alta calidad de servicio (QoS).
- **Características**:
    - Prioriza el tráfico de voz sobre otros tipos de datos.

3.4.2. WLAN para IoT

- **Descripción**: Conecta dispositivos inteligentes que requieren baja velocidad de transmisión y alta capacidad de conexión.
- **Características**:
    - Enfocada en eficiencia energética y conexiones de largo alcance con bajo consumo.

3.4.3. WLAN para redes industriales

- **Descripción**: Diseñadas para conectar dispositivos de automatización en ambientes industriales.
- **Características**:
    - Resilientes a interferencias y entornos adversos.
    - Alta disponibilidad y redundancia.

3.5. Evolución hacia Wi-Fi 7 (802.11be)

- **Descripción**: Wi-Fi 7, también conocido como Extremely High Throughput (EHT), promete velocidades superiores a 30 Gbps.
- **Características**:
    - Ancho de banda de canal de hasta 320 MHz.
    - Mejora en la eficiencia de MU-MIMO y OFDMA.

4. Protocolos en WLAN

4.1. Protocolos de Seguridad

Dado que las WLAN utilizan ondas de radio, son más susceptibles a ataques de interceptación y accesos no autorizados, por lo que la seguridad es una parte fundamental. Los principales protocolos de seguridad son:

- **WEP (Wired Equivalent Privacy)**: Fue el primer estándar de seguridad para redes Wi-Fi, pero es vulnerable a varios tipos de ataques. Actualmente se considera inseguro.
- **WPA (Wi-Fi Protected Access)**: Introducido como solución temporal tras los problemas de WEP. Utiliza TKIP (Temporal Key Integrity Protocol) para mejorar la seguridad.
- **WPA2**: Utiliza un cifrado más robusto basado en AES (Advanced Encryption Standard). Es el estándar de seguridad más utilizado en redes modernas.
- **WPA3**: La última versión introduce mejoras en la autenticación y en la encriptación, haciendo que las redes sean más seguras contra ataques de fuerza bruta y otros métodos de cracking.

4.2. Protocolo de Control de Acceso

Las WLAN utilizan el protocolo **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**, que se encarga de controlar cómo los dispositivos acceden al canal compartido.

- **CSMA/CA**: Cada dispositivo verifica si el canal está libre antes de transmitir. Si detecta que otro dispositivo está utilizando el canal, espera un tiempo aleatorio antes de intentar de nuevo. Esto reduce las colisiones, que son más comunes en entornos inalámbricos.

4.3. Protocolos de Gestión y Control

Estos protocolos están diseñados para gestionar la conexión y operación de los dispositivos dentro de una red inalámbrica. Se encargan de aspectos como la asociación, autenticación y roaming entre puntos de acceso.

- **Protocolo de Asociación (Association):** El proceso de asociación es clave en WLAN, ya que permite a un dispositivo (cliente) conectarse a un punto de acceso (AP - Access Point). Este protocolo asegura que el dispositivo pueda enviar y recibir datos a través de la red.
- **Protocolo de Autenticación (Authentication):**Antes de que un dispositivo se asocie a un AP, debe ser autenticado. Existen dos métodos principales de autenticación en WLAN:
    - **Autenticación abierta**: Básicamente, no requiere seguridad. Cualquier dispositivo puede conectarse, pero se suele combinar con WEP o WPA para mayor seguridad.
    - **Autenticación compartida**: Utiliza una clave compartida previamente para autenticarse. Este método, sin embargo, es considerado inseguro con WEP, por lo que generalmente se usa con WPA o WPA2.
- **Protocolo de Roaming:** En las redes WLAN, los usuarios pueden moverse entre áreas cubiertas por diferentes puntos de acceso. El **roaming** permite que los dispositivos cambien de un punto de acceso a otro sin perder la conexión. Para que esto sea posible, se utilizan varios protocolos como:
    - **802.11r (Fast Roaming)**: Optimiza el tiempo que tarda un dispositivo en cambiar de un punto de acceso a otro, reduciendo la latencia durante el proceso.
    - **802.11k y 802.11v**: Permiten que los dispositivos seleccionen el mejor punto de acceso disponible y gestionen mejor los recursos de la red.

4.4. Protocolos de Calidad de Servicio (QoS - Quality of Service)

En las redes WLAN, especialmente en aplicaciones que requieren transmisión de video, voz o datos en tiempo real, es fundamental priorizar el tráfico de red para garantizar la calidad de la conexión. Los protocolos QoS permiten controlar cómo se distribuye el ancho de banda entre diferentes tipos de tráfico.

- **IEEE 802.11e:** Este estándar define mecanismos para mejorar la calidad de servicio en redes inalámbricas. Introduce un esquema llamado **EDCA (Enhanced Distributed Channel Access)**, que permite la priorización de ciertos tipos de tráfico. Por ejemplo, el tráfico de voz o video puede tener prioridad sobre el tráfico de datos normales, garantizando así una mejor experiencia para aplicaciones en tiempo real.
- **WMM (Wi-Fi Multimedia):** WMM es un subconjunto del estándar 802.11e y permite priorizar ciertos tipos de tráfico en la red. Clasifica el tráfico en cuatro categorías: voz, video, mejor esfuerzo y fondo. Esto asegura que el tráfico más importante tenga prioridad en la red.

4.5. Protocolos de Movilidad

Además del roaming, existen otros protocolos que permiten gestionar la movilidad de los usuarios de manera eficiente dentro de una WLAN.

- **Mobile IP:** Este protocolo permite que los dispositivos mantengan la misma dirección IP mientras se mueven entre diferentes redes. Esto es esencial en escenarios de movilidad, como cuando un usuario se desplaza entre redes inalámbricas de diferentes áreas sin perder la conexión a la red.
- **CAPWAP (Control and Provisioning of Wireless Access Points):**Es un protocolo que facilita la administración y control de múltiples puntos de acceso desde un controlador centralizado. Esto es importante en redes empresariales grandes, donde los puntos de acceso deben coordinarse y gestionarse de forma central para optimizar el rendimiento de la red.

4.6. Protocolos de Gestión de Energía

Los dispositivos móviles, como teléfonos y laptops, necesitan ahorrar energía mientras están conectados a la red. Los protocolos de gestión de energía ayudan a minimizar el consumo de batería mientras mantienen la conectividad.

- **802.11 Power Save Mode (PSM):** Este protocolo permite que los dispositivos entren en modo de suspensión cuando no están transmitiendo o recibiendo datos, lo que ahorra energía. Los dispositivos se despiertan periódicamente para verificar si hay datos nuevos que se les han dirigido.
- **Wi-Fi Power Save Mode (WMM-PS):** Es una extensión de WMM y permite la gestión eficiente de la energía en dispositivos que utilizan QoS. Este protocolo está optimizado para aplicaciones en tiempo real, como la transmisión de voz y video, y asegura que el ahorro de energía no afecte la calidad de servicio.

4.7. Protocolos de Gestión de Redes

En redes empresariales, donde hay muchos dispositivos conectados, es esencial contar con herramientas que permitan administrar y supervisar el estado de la red.

- **SNMP (Simple Network Management Protocol):** Es un protocolo que permite monitorear y gestionar dispositivos en una red. En WLAN, SNMP se utiliza para supervisar el estado de los puntos de acceso, el rendimiento de la red y las conexiones de los clientes.
- **LWAPP (Lightweight Access Point Protocol):** Este protocolo facilita la comunicación entre un punto de acceso inalámbrico y un controlador de red. Permite gestionar y configurar los puntos de acceso de manera centralizada, haciendo más fácil la administración de grandes despliegues de redes inalámbricas.

4.8. Protocolos de Seguridad de la Red

Además de los protocolos WPA y WPA2, hay otros protocolos relacionados con la autenticación y la protección de la red.

- **IEEE 802.1X:** Es un estándar para el control de acceso basado en puertos, utilizado principalmente en redes inalámbricas empresariales. Este protocolo permite la autenticación mutua entre un cliente y un servidor de autenticación mediante EAP (Extensible Authentication Protocol), proporcionando un nivel adicional de seguridad.
- **EAP (Extensible Authentication Protocol):** Es un marco que soporta múltiples métodos de autenticación, como contraseñas, certificados digitales, tarjetas inteligentes, etc. En redes WLAN, es utilizado junto con 802.1X para proporcionar autenticación segura.

5. Comparativa entre redes inalámbricas y redes por cable.

5.1 Redes Wlan

Redes que utilizan señales de radio para conectar dispositivos de forma inalámbrica.

Ventajas:

1. Movilidad, los usuarios pueden tener conexión dentro del área sin perder cobertura.
2. Facilidad de instalación, menos requerimiento de cables, especialmente en lugares difíciles de cablear.
3. Escalabilidad, podemos agregar más dispositivos sin necesidad de cableado extra.

Desventajas:

1. Interferencia, las señales pueden ser afectadas por interferencias de otros dispositivos electrónicos y redes.
2. Seguridad, Mayor riesgo de ataques si no se implementan medidas de seguridad.
3. Rango y Velocidad limitados, la cobertura puede verse afectada por paredes, muebles, etc, y la velocidad puede disminuir con muchos usuarios conectados simultáneamente.

5.2 Redes por Cable (Ethernet)

Utilizan cables físicos, par trenzado o fibra óptica, para transmitir datos entre dispositivos
Ventajas:

1. Estabilidad y velocidad, generalmente altas y con una conexión más estable con menor latencia.

2. Seguridad, son menos vulnerables a ataques externos, ya que requieren acceso físico a la red.
3. Menos interferencias, no se ven afectadas por señales de radio, permite un rendimiento más confiable.

Desventajas:

1. Inmovilidad: Los dispositivos deben estar físicamente conectados a la red, limitando la movilidad.
2. Instalación Costosa: Requiere la instalación de cableado, lo que puede ser costoso y complicado, especialmente en edificios existentes.
3. Dificultad de Expansión: Ampliar la red puede ser más complicado y costoso debido a la necesidad de instalar más cables.

Característica	**WLAN (Inalámbrica)**	**Redes por Cable (Ethernet)**
Movilidad	Alta	Baja
Instalación	Fácil, menos cableado	Difícil, requiere cableado físico
Velocidad	Generalmente menor (dependiendo de la señal)	Mayor, con velocidades de hasta 10 Gbps
Estabilidad	Afectada por interferencias	Muy estable
Seguridad	Vulnerable si no se asegura adecuadamente	Más seguro, acceso físico requerido
Escalabilidad	Alta, fácil de agregar dispositivos	Moderada, requiere más cableado
Costo de Implementación	Menor en términos de infraestructura física	Mayor debido a la instalación de cableado

6. Aplicaciones de las redes WLAN.

Las redes inalámbricas WLAN han revolucionado la forma en que las personas y las empresas se conectan. Sus aplicaciones abarcan distintos sectores y escenarios:

1. Hogares Inteligentes: Las redes WLAN son esenciales para conectar dispositivos IoT (Internet de las cosas), como termostatos, luces, cámaras de seguridad y asistentes de voz. Esto permite la automatización y el control remoto de diversas funciones del hogar.
2. Empresas: En el ámbito empresarial, las WLAN facilitan el acceso móvil a los recursos corporativos y permiten a los empleados trabajar de manera más flexible. Además,

ofrecen soluciones de seguridad avanzadas y alta disponibilidad para soportar entornos de trabajo exigentes.

3. Espacios Públicos: Aeropuertos, cafeterías y centros comerciales utilizan redes WLAN públicas para ofrecer a los clientes acceso a internet. A menudo se configuran para gestionar un gran volumen de conexiones simultáneas y priorizar la facilidad de uso.
4. Educación: En universidades y escuelas, las redes WLAN permiten a los estudiantes y profesores acceder a recursos educativos, realizar investigaciones y colaborar en tiempo real desde cualquier lugar del campus.
5. Salud: Los hospitales utilizan redes WLAN para conectar equipos médicos, registrar información del paciente en tiempo real y mejorar la coordinación entre el personal sanitario. Estas redes también permiten la movilidad de los profesionales sin comprometer la conexión a sistemas críticos.
6. Industria: Las redes WLAN industriales conectan dispositivos de automatización y maquinaria. Esto asegura una comunicación continua y confiable, incluso en entornos con interferencias o condiciones adversas.

7. Conclusiones.

Las redes inalámbricas WLAN han transformado el acceso a la conectividad, permitiendo movilidad, flexibilidad y escalabilidad en múltiples sectores. Más allá de los retos como la seguridad y las posibles interferencias, sus ventajas en términos de facilidad de implementación, expansión y acceso remoto son indiscutibles. La evolución hacia nuevos estándares, Wi-Fi 7, va a mejorar aún más su eficiencia, velocidad y capacidad, lo que le permite tener su lugar como una tecnología indispensable tanto actualmente como el día de mañana.