**UNIVERSIDAD NACIONAL DE TRUJILLO**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE INGENIERÍA DE SISTEMAS**



“Redes inalámbricas”

**TRABAJO MONOGRÁFICO**

**Autores**

Alvarado Echavarria, Joseph Smith

Azañedo Gamez, Wilson David

Briones Rojas, Brandon Jhonatan

Escorza Cholan, Brayan David

Huaman Villanueva, Cristian Andres

**Docente**

Arellano Salazar, Cesar

**Trujillo-Perú**

**2021**

# DEDICATORIA

Dedicamos esta monografía a nuestro querido profesor Cesar Arellano Salazar cuya dedicación y paciencia sirvieron como pilares de apoyo para la realización de este trabajo. Agradecido por todo.

**WiMax, redes inalámbricas de banda angosta y banda ancha**

**y seguridad en redes inalámbricas**

# INTRODUCCIÓN

Hemos sido testigos de un enorme progreso en la industria de las telecomunicaciones, que nos ha llevado de una nueva tecnología a una tecnología más innovadora en un corto período de tiempo. La idea utópica de tener una red global surgió hace un tiempo, para algunas personas su desventaja es que está cableada, pero esto ya no es un obstáculo. En este momento, gracias a WiMAX, pronto podremos acceder a comunicaciones inalámbricas que antes no esperábamos, y ahora es como una nueva puerta abierta. WiMAX incluye: Internet, teléfono y TV, y algunos otros servicios.

La innovación propuesta por WIMAX, por la proximidad global que brinda Internet, nos permite implementarla en nuestro país mientras realizamos investigaciones sobre productos y mercados, lo que nos permite comprender la viabilidad de proyectos en esta gama; y comprender algunas de las ventajas y desventajas del diseño organizacional.

La innovación de un nuevo tipo de tecnología hace necesario que lo entendamos y lo hagamos más fácil de entender en nuestro entorno. Por tanto, este documento utiliza un lenguaje fácil de entender para los lectores y cuenta con información clara para que puedan formarse sus propios juicios de valor sobre WiMAX, entenderlo, saber aplicarlo y ver juntos a dónde nos llevará, su adquisición e implementación.

Además, veremos que las redes y los sistemas de telecomunicaciones se ven afectados actualmente por innovaciones tecnológicas muy cambiantes, seguidos de los sistemas basados ​​en comunicaciones inalámbricas no son una excepción, por lo que se están desarrollando rápidamente.

La red inalámbrica se crea debido a la necesidad de brindar acceso a la red a través de un dispositivo informático portátil, lo que obviamente trae problemas al medio de transmisión, ya que los intrusos pueden ingresar a la red libremente, brindando así una posibilidad virtual de no ser detectados. Por eso es importante para la comunicación segura en redes inalámbricas establecer un enlace para intercambiar información confidencial.

Las redes inalámbricas han experimentado un auge muy importante en los últimos años, por lo que los mecanismos de seguridad desarrollados inicialmente pronto comenzaron a ser superados por usuarios malintencionados que buscaban un lugar para infiltrarse en el sistema desde sus vulnerabilidades de seguridad existentes.

**Índice**

[DEDICATORIA 2](#_Toc81292825)

[INTRODUCCIÓN 4](#_Toc81292826)

[1. WIMAX 8](#_Toc81292827)

[1.1. Descripción técnica 8](#_Toc81292828)

[1.2. Estándares 8](#_Toc81292829)

[1.3. Características 10](#_Toc81292830)

[1.3.1. Capa física basada en OFDM 10](#_Toc81292831)

[1.3.2. Grandes picos de tasas de datos 10](#_Toc81292832)

[1.3.3. Escalabilidad en el ancho de banda y la tasa de datos soportada 10](#_Toc81292833)

[1.3.4. Modulación y codificación adaptativa (AMC – Adaptative Modulation and Coding) 11](#_Toc81292834)

[1.3.5. Retransmisiones en la capa de enlace 11](#_Toc81292835)

[1.3.6. Soporta multiplexaciones en tiempo (TDD) y en frecuencia (FDD) 11](#_Toc81292836)

[1.3.7. Acceso Múltiple por División de Frecuencia Ortogonal (OFDMA) 11](#_Toc81292837)

[1.3.8. Soporta técnicas avanzadas de antenas 11](#_Toc81292838)

[1.3.9. Soporta calidad de servicio (QoS) 12](#_Toc81292839)

[1.3.10. Seguridad robusta 12](#_Toc81292840)

[1.3.11. Soporta movilidad 12](#_Toc81292841)

[1.3.12. Arquitectura basada en IP 12](#_Toc81292842)

[1.4. Ventajas vs desventajas 12](#_Toc81292843)

[1.4.1. Ventajas 12](#_Toc81292844)

[1.4.2. Desventajas 13](#_Toc81292845)

[1.5. WiMax vs Wifi 13](#_Toc81292846)

[1.6. Topologías 13](#_Toc81292847)

[1.6.1. Topología punto a punto 13](#_Toc81292848)

[1.6.2. Topología punto multipunto 13](#_Toc81292849)

[1.7. Arquitectura de red WiMax 14](#_Toc81292850)

[1.7.1. Estación Base (BS) 15](#_Toc81292851)

[1.7.2. Pasarela de Acceso al Servicio (ASN-GW) 15](#_Toc81292852)

[1.7.3. Servicio de Conexión a la red (CSN) 15](#_Toc81292853)

[1.8. Capa de Control de Acceso al Medio en WiMAX 17](#_Toc81292854)

[1.8.1. Subcapa MAC de convergencia (CS) 17](#_Toc81292855)

[1.8.2. Subcapa MAC común (MAC CPS) 17](#_Toc81292856)

[1.8.3. Subcapa MAC de seguridad 18](#_Toc81292857)

[2. REDES INALÁMBRICAS DE BANDA ANGOSTA Y BANDA ANCHA 18](#_Toc81292858)

[2.1. Definición 18](#_Toc81292859)

[2.2. Estándares de redes inalámbricas 18](#_Toc81292860)

[2.2.1. WIFI 18](#_Toc81292861)

[2.2.2. 802. - Red ethernet inalámbrica 18](#_Toc81292862)

[2.2.3. 802.11 b – Red ethernet inalámbrica de alta velocidad 19](#_Toc81292863)

[2.2.4. 802.11 b+ 19](#_Toc81292864)

[2.2.5. 802.11g 19](#_Toc81292865)

[2.2.6. 802. 11ª 19](#_Toc81292866)

[2.2.7. 802.11n 19](#_Toc81292867)

[2.2.8. HiperLAN2 19](#_Toc81292868)

[2.2.9. Bluetooth 19](#_Toc81292869)

[2.2.10. Home RF – Redes inalámbricas domésticas 19](#_Toc81292870)

[2.2.11. 802.16 – WIMAX 20](#_Toc81292871)

[2.2.12. Red móvil 2G 20](#_Toc81292872)

[2.2.13. Red móvil 2.5G 20](#_Toc81292873)

[2.2.14. Red móvil 3G 20](#_Toc81292874)

[2.2.15. Red móvil 4G 21](#_Toc81292875)

[2.3. Banda angosta 21](#_Toc81292876)

[2.3.1. Definición 21](#_Toc81292877)

[2.3.2. Características 21](#_Toc81292878)

[2.4. Banda ancha 21](#_Toc81292879)

[2.4.1. Definición 21](#_Toc81292880)

[2.4.2. Tipos de redes inalámbricas de banda ancha 22](#_Toc81292881)

[2.5. Diferencias entre banda ancha y banda angosta 22](#_Toc81292882)

[3. SEGURIDAD EN REDES INALÁMBRICAS 23](#_Toc81292883)

[3.1. Requisitos de seguridad y ataques 23](#_Toc81292884)

[3.1.1. Ataques Pasivos 23](#_Toc81292885)

[3.1.2. Ataques Activos 24](#_Toc81292886)

[3.2. Privacidad con cifrado simétrico 25](#_Toc81292887)

[3.2.1. Cifrado simétrico 25](#_Toc81292888)

[3.2.2. Algoritmo de cifrado 25](#_Toc81292889)

[3.2.3. Localización de los dispositivos de cifrado 26](#_Toc81292890)

[3.2.4. Distribución de claves. 28](#_Toc81292891)

[3.3. Autenticación de mensajes y función de dispersión. 29](#_Toc81292892)

[3.3.1. Alternativas para la autenticación de mensajes 29](#_Toc81292893)

[3.4. Cifrado de clave publica y firmas digitales. 31](#_Toc81292894)

[3.4.1. Cifrado de clave publica 31](#_Toc81292895)

[3.4.2. Firma Digital 32](#_Toc81292896)

[3.4.3. Gestión de Claves 32](#_Toc81292897)

[CONCLUSIONES 34](#_Toc81292898)

[REFERENCIAS BIBLIOGRÁFICAS 35](#_Toc81292899)

# WIMAX

## Descripción técnica

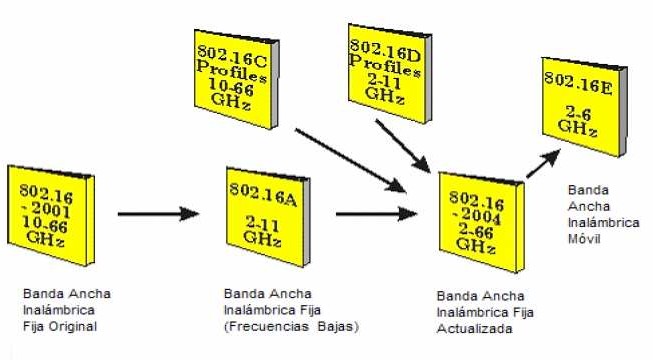
En los últimos meses en los que apenas empezábamos a sopesar todas las bondades del Wi-Fi, en el mundo tecnológico se empieza a escuchar sobre un nuevo protocolo inalámbrico de banda ancha: WiMAX, pero, ¿De qué se trata? Como lo dice el vicepresidente de Intel Communications Group, James A. Johnson y Gerente General de Wireless Networking Group: “Nuestro papel es asegurarnos que tú puedas llevar tu Laptop a cualquier lugar, y en cualquier lugar haya una red a la que puedas acceder inalámbricamente. Nuestra estrategia es asegurarnos que la tecnología fundamental y los productos tengan un costo-efectivo suficiente para que la gente puede desplegar redes inalámbricas alrededor del mundo."

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM (Ortogonal Frecuency Division Multuplexing, División de Frecuencia por Multiplexación Ortogonal, Técnica de modulación que permite transmitir grandes cantidades de datos sobre una onda de radio), y con 256 subportadoras puede cubrir un área de 48 kilómetros permitiendo la conexión sin línea de vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con un índice de modulación de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs, Service Level Agreeements, Acuerdos de Calidad de Servicio, protocolo plasmado en un documento de carácter legal en el que una compañía se compromete con otra para prestar un servicio en unas condiciones mínimas) y calidad de servicio (QoS, Quality of Service, se garantiza que se transmitirá una cantidad de datos en un tiempo determinado).

WiMAX se sitúa en el rango más alto de amplitud de cobertura con respecto a las demás tecnologías de acceso de corto alcance ofreciendo velocidades de banda ancha para un área metropolitana o rural.

## Estándares

WiMAX es una tecnología basada en estándares que permite al abonado la conectividad de banda ancha inalámbrica en uso fijo, nómada, portátil y móvil sin necesidad de visión directa de la estación base. A pesar de que el proyecto para la creación de este nuevo estándar se lleva gestionando desde julio de 1999 con el Grupo de Trabajo de Acceso Inalámbrico de Banda Ancha IEEE 802.16 o “IEEE 802.16 Working Group on Broadband Access” no fue hasta abril de 2002 que se publicó la primera versión:



|  |  |
| --- | --- |
| Estándar | Descripción |
| 802.16 | WiMAX, rango de frecuencia de 10 a 66 GHz |
| 802.16a | WiMAX para estaciones de usuarios fijas, frecuencias inferiores a 11 GHz |
| 802.16b | Frecuencias exentas de licencia; rango de frecuencia de 5 a 6GHz |
| 802.16c | Detalles del sistema para la banda de 10 a 66 GHz |
| 802.16d | Estándar |
| 802.16-2004 | Reemplaza a los estándares 802.16a y 802.16d (e incluye OFDMA) |
| 802.16e | WiMAX para estaciones de usuario en movimiento (velocidad limitada a 120 km/h; tamaño FFT 128, 512,  1024 y 2048) |
| 802.16f | Gestión MIB (Base de Información de Gestión) |
| 802.16g | Gestión de niveles |
| 802.16-1 | Interfaz aérea; rango de frecuencia de 10 a 66 GHz |
| 802.16-2 | Coexistencia de sistemas de acceso inalámbricos de banda ancha. Reemplazado por la 802.16.2-2004 |
| 802.16.2-2004 | Coexistencia de sistemas de acceso inalámbricos de banda ancha. Reemplazado por la 802.16.2-2004 |
| 802.16.2a | Recomendaciones para la coexistencia de los sistemas de acceso fijo inalámbricos de banda ancha. |
| 802.16.3 | Interfaz aérea para sistemas de acceso fijo inalámbricos de banda ancha operando por debajo de los 11 GHz |

## Características

WiMAX es una solución de banda ancha inalámbrica que ofrece una gran cantidad de características con bastante flexibilidad:

### Capa física basada en OFDM

La modulación OFDM (Orthogonal Frecuency – Division Multiplexing) presenta muchos beneficios que no presentan otras modulaciones previas a ésta, y permite que las redes inalámbricas transmitan eficientemente en pequeños anchos de banda. Esta modulación se caracteriza por dividir la señal de banda ancha en un número de señales de banda reducida. La modulación OFDM es un caso especial de modulación multiportadora, en donde múltiples datos son transmitidos de forma paralela utilizando diferentes subportadoras con banda de frecuencias solapadas ortogonalmente.

### Grandes picos de tasas de datos

WiMAX es capaz de soportar elevados picos de tasa de datos. De hecho, las velocidades que puede alcanzar la capa física (PHY) llegan a ser de 74 Mbps cuando opera con un espectro de frecuencia de 20 MHz de ancho de canal. Comúnmente, cuando se usa un espectro de 10 MHz de ancho de canal con un esquema a razón de tres a uno en el canal de bajada y el de subida respectivamente, las velocidades que se alcanzan son de 25 Mbps para el enlace de bajada y de 6.7 Mbps para el enlace de subida. Estas velocidades de pico de datos son alcanzadas cuando se usa una codificación 64QAM con un índice de corrección de error de 5/6. Bajo condiciones buenas para la señal se podrían alcanzar velocidades mayores, así como usando múltiples antenas y multiplexación espacial.

### Escalabilidad en el ancho de banda y la tasa de datos soportada

WiMAX tiene una arquitectura de capa física escalable, lo que permite que la tasa de datos sea escalable con la disponibilidad de ancho de banda en los canales. Esta escalabilidad se soporta en el modo OFDMA, donde el tamaño de la transformada rápida de Fourier (FFt) debe estar basado en el ancho de banda disponible en el canal. Por ejemplo, un sistema WiMAX debería usar una FFT de 128, 512 o 1024 subportadoras según el ancho de banda del canal sea de 1.25 MHz, 5 MHz o 10 MHz respectivamente. Esta escalabilidad debe hacerse dinámicamente para soportar el roaming de usuarios a través de las diferentes redes que podrían tener anchos de banda diferentes.

### Modulación y codificación adaptativa (AMC – Adaptative Modulation and Coding)

WiMAX soporta un número de esquemas de modulación y de mecanismos de corrección de errores (FEC) y permite que el esquema sea cambiado por usuario y por estructura básica, basada en las condiciones del canal (SNR). AMC es un mecanismo efectivo para maximizar el caudal en un canal variable en el tiempo.

### Retransmisiones en la capa de enlace

Para las conexiones que requieren una alta fiabilidad, WiMAX soporta ARQ (Automatic Retransmission Request) protocolo utilizado para el control de errores en la transmisión de datos, garantizando la integridad de los mismos en la capa de enlace. Este protocolo requiere que los paquetes transmitidos sean asentidos por el receptor mediante un acuse de recibo (ACK); los paquetes que no son asentidos se consideran perdidos y se retransmiten.

### Soporta multiplexaciones en tiempo (TDD) y en frecuencia (FDD)

En los estándares IEEE 802.16d y 802.16e se soporta tanto Time Division Duplex (TDD) como Frequency Division Duplex (FDD), y permite un modo Half Duplex FDD (HD-FDD), lo que permite una implementación de bajo coste del sistema. En la mayoría de las implementaciones se usa TDD debido a sus ventajas:

* Flexibilidad al elegir la razón entre las velocidades del enlace de subida y el de bajada.
* Habilidad para explotar la reciprocidad del canal.
* Habilidad para implementarse en un espectro no pareado.
* Diseño del transductor menos complejo.
* Todos los perfiles WiMAX están basados en TDD, excepto los dos fijados en 3.5 GHz.

### Acceso Múltiple por División de Frecuencia Ortogonal (OFDMA)

El estándar del 802.16e (WiMAX móvil) usa OFDMA, el cual es similar a OFDM puesto que divide la señal en múltiples subportadoras. OFDMA, sin embargo, va un paso más allá, agrupando subportadoras en subcanales. Una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión, o los múltiples clientes podrían transmitir simultáneamente usando cada uno una porción del número total de subcanales.

### Soporta técnicas avanzadas de antenas

WiMAX permite el uso de técnicas basadas en múltiples antenas como Beamforming, codificación espacio-tiempo, y multiplexación. Estos esquemas pueden ser usados para mejorar la capacidad total del sistema y su eficiencia espectral mediante el uso de múltiples antenas en el transmisor y/o receptor.

### Soporta calidad de servicio (QoS)

La capa MAC de WiMAX es orientada a conexión, diseñada para admitir una variedad de aplicaciones, incluyendo servicios multimedia y de voz. El sistema soporta tasas de bit constantes y tasas de bit variables, soporta flujos de tráfico en tiempo real, así como los que no lo son. WiMAX está diseñado para soportar un gran número de usuarios, con múltiples conexiones por terminal, cada uno con sus propios requisitos de calidad del servicio.

### Seguridad robusta

WiMAX admite una fuerte encriptación usando AES (Advanced Encryption standard) que es un esquema de cifrado por bloques, y tiene un protocolo robusto de privacidad y de gestión de claves. Además, el sistema ofrece una arquitectura muy flexible de autentificación basado en el protocolo EAP (Extensible Authentification Protocol), el cual permite una variedad de credenciales de usuarios, incluyendo esquemas de usuarios/password, certificados digitales y tarjetas inteligentes.

### Soporta movilidad

La variante móvil de WiMAX tiene un mecanismo para soportar traspasos seguros y ahorro de energía para alargar la duración de las baterías de los dispositivos portátiles. También se añaden mejoras en el nivel físico como una estimación más frecuente del canal, sub canalización del enlace de subida, y control de energía.

### Arquitectura basada en IP

El WiMAX Forum ha definido una arquitectura de red basada en plataformas IP.

## Ventajas vs desventajas

### Ventajas

Entre las principales ventajas que nos ofrece WiMax, se destaca:

* Presente en zonas remotas donde no llegan otras conexiones, se puede establecer la conexión a internet inalámbrica en aquellos sitios.
* No necesita instalación exterior con cableado.
* La instalación suele ser gratuita.
* Permite realizar llamadas mediante VOIP.
* No es necesario tener una línea fija.
* Gran escalabilidad.
* Tiene un alcance superior, puesto que las antenas de las radio-bases, emiten una señal que alcanza los 30 Kilómetros de distancia.
* En seguridad existe un nivel de encriptación para proteger toda la información que es propiedad de los usuarios.

### Desventajas

Entre las desventajas que se identificaron de WiMax, se obtuvo que:

* Se necesita un contacto directo con el repetidor.
* Solo puede haber cobertura con WiMax cuando existe un operador que la proporcione y posea las antenas necesarias para ello.
* Las interferencias, ya que la señal se puede ver afectada mediante interferencia u ondas.
* En la salud de la población debido a las altas frecuencias.

## WiMax vs Wifi

Con el éxito que vieron las operadoras de internet con wifi, rápidamente los fabricantes empezaron a pensar en una tecnología bastante más avanzada y ahí surgió la certificación WiMax en el año 2001. La gran diferencia con el wifi es la enorme distancia de cobertura y que es mucho más rápida, pero no solo eso ya que WiMax posee una cobertura incluso en movimiento, viajando a velocidades de hasta 250Km/h tendremos cobertura.  
Además Wi-Fi está diseñado para entornos de interior, mientras que WiMax lo está para entornos exteriores, pudiendo dar acceso a más de 1000 usuarios de forma simultánea.



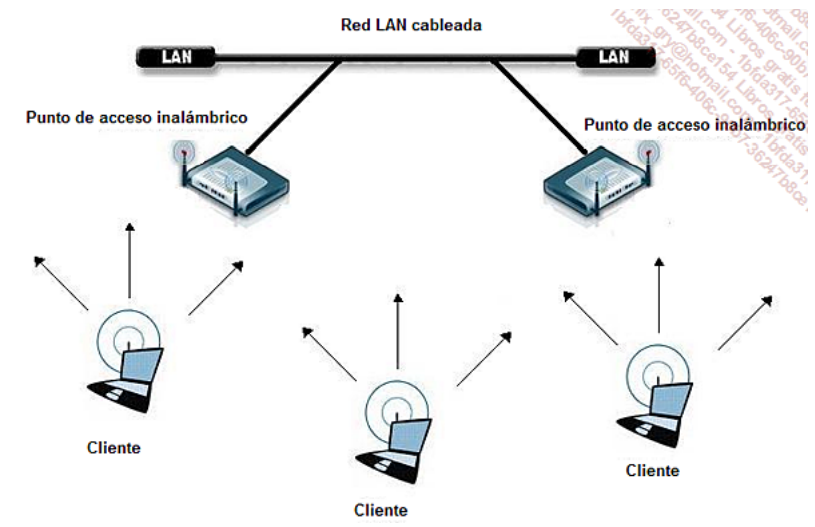
## Topologías

### Topología punto a punto

A través de una interfaz de red inalámbrica se pueden comunicar directamente dos nodos. También se le llama conexión de tipo punto a punto (peer to peer) o ad hoc. Una configuración como esta es posible con las tecnologías Bluetooth o Wi-Fi.

### Topología punto multipunto

Un componente centralizador, como el punto de acceso (AP - Access Point) y Wi-Fi centralizan las comunicaciones. También permiten la interconexión con la red cableada local.

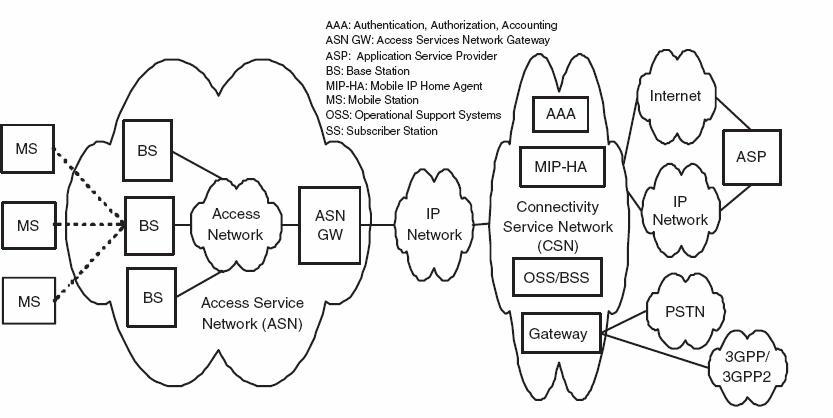


## Arquitectura de red WiMax

El estándar IEEE 802.16e-2005 nos proporciona la interfaz aérea para WiMAX, pero no nos define la estructura de la red de un extremo a otro. El grupo de trabajo del foro WiMAX es el responsable de desarrollar los requisitos de la estructura de la red, su arquitectura, y los protocolos para WiMAX, usando el estándar 802.16e-2005 como interfaz aérea.

El modelo de referencia de una red WiMAX está compuesto principalmente por tres componentes interconectadas mediante interfaces estandarizadas o puntos de referencia del R1 a R5. Los tres componentes son:

* **MS**: Mobile Station, usado en el extremo de la red del usuario para acceder a la red.
* **ASN:** Access Service Network, comprende una o más estaciones base y una o más pasarelas ASN para formar la red de acceso radio.
* **CSN:** Connectivity Service Network, que provee conectividad IP con las funciones IP del núcleo de la red.



### Estación Base (BS)

Implementa la capa física y MAC tal como se define en el estándar IEEE 802.16. En una red de acceso WiMAX, una BS está definida por un sector y una frecuencia asignada. En el caso de la asignación multifrecuencia de un sector, dicho sector incluye tantas BS como frecuencias asignadas haya. La conectividad a múltiples ASN-GW debe ser requerida en el caso de carga balanceada o propósitos de redundancia.

### Pasarela de Acceso al Servicio (ASN-GW)

Una pasarela ASN es una entidad lógica que actúa típicamente como un punto de agregación de tráfico de la capa de enlace dentro del ASN e incluye: Funciones de control entre entidades pares y Encaminamiento plano de portadora o funciones de puente.

Una entrada completamente redundante de la red del servicio del acceso (ASN- GW) conecta las estaciones bajas de WiMAX con la red de la base. Con una capacidad de hasta 256 BS por unidad. Las funciones principales del ASN-GW son: gestión y paginación de la localización dentro del ASN, gestión de los recursos de radio, claves de encriptación, funcionalidad de cliente de AAA, establecimiento y gestión de la movilidad con las estaciones base, aplicaciones de QoS, funcionalidad de agente externo para Mobile IP y envío a los CSN seleccionados.

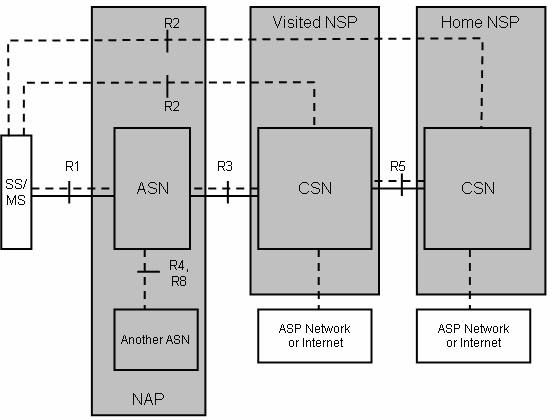
### Servicio de Conexión a la red (CSN)

El CSN consiste en unas funciones y equipos que permiten la conectividad IP a los suscriptores WiMAX. Por ello, el CSN incluye las siguientes funciones:

* Autorización de conexión de usuario en la capa de acceso 3.
* Administración de la QoS.
* Soporte de movilidad basado en Mobile IP.
* Tunelado (basado en protocolos IP) con otros equipos o redes.
* Facturación de los suscriptores WiMAX.
* Servicios WiMAX (acceso a Internet, servicios de localización, conexión de servicios Peer-To-Peer, aprovisionamiento, autorización y/o conexión a gestores de bases de datos o IMS).

Además de las entidades anteriores, el grupo de trabajo del WiMAX Forum define varios puntos de referencia entre las distintas entidades que componen la arquitectura de esta red. Esos puntos de referencia logran puntos de interoperabilidad entre equipos de diferentes fabricantes. Hay seis puntos de referencias obligatorios (del R1 al R6) y dos opcionales (R7 y R8).

* R1: Punto de referencia de la interfaz radio entre el MS y el ASN. Incluye todas las características físicas y MAC de los perfiles de WiMAX. Lleva tráfico de usuario y mensajes de control de usuario.
* R2: Es la interfaz lógica entre el MS y el CSN. Contiene los protocolos y otros procedimientos implicados en la autenticación, servicios de autorización y administración de la configuración IP.
* R3: Es la interfaz lógica entre el ASN y el CSN. Transporta mensajes del plano de control e información del plano de datos a través de un tunelado entre el ASN y CSN.
* R4: Punto de referencia que interconecta dos ASNs (ASN perfil B) o dos ASN-GW (ASN perfiles A o C). Transporta mensajes del plano de control y de datos, especialmente durante el traspaso de un usuario WiMAX entre ASNs/ASN-GWs. Presenta interoperabilidad entre ASNs de diferentes fabricantes.
* R5: Punto de referencia que interconecta dos CSNs. Consiste en el juego de métodos del plano de control y de datos para la comunicación entre el CSN del NSP visitante y el NSP.
* R6: Es específico de algunos de los perfiles de ASN. En aquel os en los que el ASN se subdivide en BS y ASN-GW que corresponden con los perfiles A y C. Por tanto, este punto de referencia no es aplicable al perfil B. R6 se encarga de unir el BS y el ASN-GW. Transporta mensajes del plano de control y de datos.
* R7 y R8: R7 es una interfaz lógica opcional entre funciones de decisión y aplicación en el ASN-GW. R8 es una interfaz lógica entre estaciones base y transporta flujo de intercambio del plano de control que sirve para permitir un rápido y eficiente traspaso entre estaciones base.



## Capa de Control de Acceso al Medio en WiMAX

La principal tarea de la capa MAC de WiMAX es la de proporcionar una interfaz entre la capa de transporte y la capa física. La capa MAC toma los paquetes de la capa inmediatamente superior, estos paquetes se llaman MAC Service Data Units (MSDUs), y los organiza dentro de los paquetes denominados MAC Protocol Data Units (MPDUs) para transmitirlos por el aire. Para la recepción la capa MAC hace lo mismo, pero en orden inverso.

Esta es la otra capa característica del protocolo IEEE 802.16, fue diseñado para accesos a las aplicaciones PMP (Punto a MultiPunto) de banda ancha de muy alta tasa de datos y con una variedad de requisitos de calidad de servicios (QoS), por lo que está orientado a conexión.

Permite que el mismo terminal sea compartido por múltiples usuarios. Lo que hace flexible a este sistema es que maneja algoritmos que permiten que cientos de usuarios finales puedan tener distintos requisitos de ancho de banda y de retardo. La capa MAC que es la encargada de coordinar el acceso al medio está compuesta de 3 subcapas:

### Subcapa MAC de convergencia (CS)

Es la encargada de adaptar las unidades de datos de protocolos de alto nivel al formato MAC SDU y viceversa. Es decir, se encarga de transformar los datos de las redes externas y pasarlos a la subcapa MAC común convertidos en unidades de datos del servicio o SDU (Service Data Units), que son las unidades de datos que se transfieren entre capas adyacentes. Se encuentra sobre la subcapa MAC común y utiliza los servicios proveídos por ésta. También se encarga de clasificar las SDUs de la MAC entrantes a las conexiones a las que pertenecen.

### Subcapa MAC común (MAC CPS)

Es el núcleo de la toda la capa MAC, provee los servicios de acceso al sistema, asignación de ancho de banda, establecimiento y mantenimiento de la conexión y se establecen las unidades de datos de protocolo o PDU (Protocol Data Units). También se encarga de hacer el intercambio de la unidad de servicios de datos de la capa MAC (SDU) con la capa de convergencia. Esta subcapa se encuentra fuertemente ligada con la capa de seguridad. En esta subcapa se prestan los servicios de planificación que representan los mecanismos de manipulación de datos soportados por el planificador de la MAC para el transporte de datos en una conexión, cada una de las cuales está asociada a un solo servicio de datos el cual, a su vez, está asociado a unos parámetros de QoS que son quienes determinan su comportamiento. Existen cuatro tipos de servicios:

* Concesión no Solicitada (UGS)
* Polling en tiempo real (rtPS)
* Polling no en tiempo real (nrtPS)
* Mejor Esfuerzo (BE)

### Subcapa MAC de seguridad

Presta los servicios de autenticación, intercambio seguro de claves y cifrado. Permite proveer a los usuarios un servicio de banda ancha seguro a través de su conexión fija mediante el cifrado de las conexiones, y al operador protegerse contra las conexiones no autorizadas forzando el cifrado. La subcapa de seguridad es la encargada de la autentificación, establecimiento de claves y encriptación. Es en el a donde se realiza el intercambio de los PDUs de la MAC con la capa física.

# REDES INALÁMBRICAS DE BANDA ANGOSTA Y BANDA ANCHA

## Definición

Examinando esta definición esta se usan repetidamente en informática con el objetivo de distinguir una conexión de nodos a través de las señales electromagnéticas, sin tener que recurrir a un cableado realizando está a través de puertos teniendo una muy buena recepción.

Una red inalámbrica permite la interconexión de dispositivos informáticos mediante ondas electromagnéticas sin necesidad de tener algún tipo de conexión física. El intercambio de datos se hace usando el espectro radioeléctrico. Una de sus ventajas más importantes es el ahorro en costos, ya que no es necesario realizar la inversión en la conexión física entre nodos; es decir, no se necesita algún tipo de cableado. 18 mediante la red inalámbrica, es posible que el usuario se mantenga conectado siempre y cuando esté internamente en la señal de la red inalámbrica y de esta forma brinda movilidad

## Estándares de redes inalámbricas

Se consignan a los fabricantes en garantizar que los productos tengan cierta mesura, vigencia e de interoperabilidad con otros productos, siempre y cuando el estándar sea abierto. Entre los estándares de redes inalámbricas tenemos:

### WIFI

Es un grupo de patrones para redes inalámbricas, fundado en los detalles técnicas 802.11 Wifi Alliance es la empresa comercial que prueba y certificas los productos que funcionan bajo este estándar. Este estándar es utilizado en redes WLAN (Wireless local Area Network) y operan en los 2.4 GHz.

### 802. - Red ethernet inalámbrica

Fue definida en 1997, opera en los 2.4 GHz y tiene una velocidad de transmisión -2 Mbps, las mejoras aceptadas para este estándar con 802.11b, 802.11 g y 802.11n y usa tres tecnologías:

* FHSS: Frecuency Hoping Spread Spectrum
* DSSS: Direct Secuence Spread Spectrum

### 802.11 b – Red ethernet inalámbrica de alta velocidad

Fue definida en 1999, puede lograr velocidades de transmisión de hasta 5.5 y 11 Mbps en el espectro de 2,4 GHz, además siendo este similar con el estándar 802.11, únicamente en sistemas DSSS y usa una técnica de modulación llamada CCK Complementary Code Keying el cual le permite llegar a la velocidad de transmisión ya antes nombrada. 28 Sin duda gracias a la adopción de CCK se logró poner en énfasis el uso de las redes Wi-Fi, ya que la velocidad que ofrece es muy buena si la necesidad de tener una red creando un uso más continuo y común. Debido a esta popularización disminuyeron los costos de fabricación y por ende se hizo más asequibles los equipos para las empresas grandes y pequeñas.

### 802.11 b+

Es una versión mejorada del estándar 802.11b y soporta velocidad de transmisión de 22 Mbps en el espectro de 2,4 GHz. El problema radica en que no es un estándar, por lo que hay problemas de compatibilidad. Dlink adoptó esta tecnología.

### 802.11g

Soporta una velocidad de transmisión de incluso 54 Mbps dentro del espectro de 2,4 GHz; es compatible con los equipos WIFI y fue creado en 2001. Usa como tecnología de acceso al medio OFDM (Multiplicación por división de frecuencias), además de CCK (Complementary Code Keying) para así asegurar la compatibilidad con 802.11b.

### 802. 11ª

Usa la banda de 5Ghz y usa OFDM para la transmisión de datos. No es compatible con los estándares que usan la banda de 2,4 GHz.

### 802.11n

Usa la banda de 2,4Ghz y podría llegar a alcanzar hasta una tasa teórica de 540 Mbps. Usa tecnología MIMO (múltiples entradas, múltiples salidas), que consta en usar múltiples transmisores y múltiples receptores.

### HiperLAN2

Usa la banda de 5Ghz y llega a una tasa de transmisión de 54 Mbps; usa también OFDM, este es un estándar desarrollado en Europa.

### Bluetooth

Usa la banda de 2,4Ghz y llega a tener una tasa de transmisión de hasta 721 Kbps; no compite directamente con el estándar 802.11, ya que está diseñado para redes de área personal y poder transmitir en un rango de distancia corto, de tan solo 0 metros; puede provocar interferencia, ya que operan en la misma banda, aunque en la versión 1.2 se han realizado mejoras técnicas y así no sufran interferencias con el estándar 802.11.

### Home RF – Redes inalámbricas domésticas

Este estándar fue creado con el propósito de brindar conectividad entre los dispositivos electrónicos domésticos; puede llegar a tener una tasa de ,6 Mbps y usa la banda de 2,4 Ghz, es incompatible con el estándar 802.11.

### 802.16 – WIMAX

Usado para la difusión de datos en redes inalámbricas dentro del espacio metropolitana; puede llegar a tener una tasa de 124 Mbps en el espectro de 2,4 Ghz y 5,8 Ghz además de tener un alcance de hasta 70 Km. La diferencia principal contra WIFI es la distancia de cobertura, mientras que WIFI fue diseñado para redes inalámbricas de área local, y WIMAx fue creado para brindar cobertura a áreas metropolitanas.

### Red móvil 2G

Fue la primera red en brindar voz y datos digitales, además de roaming internacional. Algunas características:

* Usa tecnología GSM y CDMA donde la tasa es de 14 a 64 kbps
* La banda de frecuencia usada por GSM es 850- 1900 Mhz y CDMA es de 825 a 849 MHz.
* Usa conmutación de circuitos.
* Se puede brindar servicio de voz, SMS, roaming.

### Red móvil 2.5G

Tiene como característica principal la conmutación por paquetes para poder brindar Internet de alta velocidad.

* Usa tecnología GPRS y EDGE.
* La velocidad de transmisión es de 115kbps (GPRS) y 384kbps (EDGE).
* Trabaja en la banda de 1850- 1900 MHz.
* Usa transferencia de paquetes para datos.
* Además de brindar los servicios de 2G, se puede hacer SMS multimedia, presionar para hablar (PTT), soporte WAP, MMS, acceso correo electrónico, acceso Internet.

### Red móvil 3G

El propósito principal fue aumentar la tasa de transferencia de datos; para transferir datos se usa la tecnología packetswitching, y las llamadas de voz usan conmutación de circuitos.

* Usa tecnología UMTS.
* La velocidad de transmisión es de 384kbps a 2 Mbps.
* Además de brindar servicios de 2.5G, aumenta la tasa de trasmisión de datos, acceso a Internet de alta velocidad, llamadas de video, servicios basados en localización, juegos.

### Red móvil 4G

Está establecido completamente en IP y el objetivo principal es brindar acceso de banda ancha. Usa tecnología LTE

* Velocidad de transmisión de hasta Gbps
* Además de los servicios de 3G, puede brindar telefonía IP, TV móvil de alta definición, servicios de juegos, videoconferencia.

## Banda angosta

### Definición

Las conexiones de banda angosta en el mundo de las conexiones a [Internet](http://es.wikipedia.org/wiki/Internet) hacen referencia a un tipo de conexión que utiliza un [ancho de banda](http://es.wikipedia.org/wiki/Ancho_de_banda) muy reducido. La conexión más típica de banda angosta  que existe es la conexión por [módem](http://es.wikipedia.org/wiki/M%C3%B3dem) telefónico ([Dial-up](http://es.wikipedia.org/wiki/Dial-up)). Un módem adapta las señales informáticas producidas por la [computadora](http://es.wikipedia.org/wiki/Computadora) a otro tipo de señal que se puede introducir por la [línea telefónica](http://es.wikipedia.org/wiki/L%C3%ADnea_telef%C3%B3nica); así mismo, convierte la señal que llega a través de la línea telefónica en información comprensible para el ordenador. En [telefonía](http://www.worldlingo.com/ma/enwiki/es/Telephony), la banda angosta  se considera generalmente cubrir frecuencias 300-3400 hertzios.

Los módems telefónicos realizan la [comunicación](http://es.wikipedia.org/wiki/Comunicaci%C3%B3n) en el espacio de frecuencias disponible para una llamada telefónica. Ese espacio es muy reducido, lo que provoca que la [velocidad](http://es.wikipedia.org/wiki/Velocidad) de conexión no supere los 56 kbps (kilobits por segundo). Debido a la baja velocidad que desarrollan, este tipo de conexión recibe el nombre de banda angosta.

Actualmente, las conexiones por banda angosta  están siendo sustituidas por modernas conexiones de mayor ancho de banda (llamadas conexiones de [banda ancha](http://es.wikipedia.org/wiki/Banda_ancha)). El hecho de no tener que utilizar el espacio de frecuencias de [voz](http://es.wikipedia.org/wiki/Voz_(fonolog%C3%ADa)) hace que la capacidad pueda ser de 128 kbps o superior.

### Características

* La banda estrecha se utiliza principalmente para la transmisión de voz sin hilos, y el desplazamiento de frecuencia es generalmente 3 a 5KHZ. Conveniente para las señales de audio de gama media de 800 a 3KHZ. Banda estrecha es ampliamente utilizado en radio de dos vías.
* No había ninguna banda de banda estrecha en la tecnología temprana de la radio, y más tarde hubo una tecnología más estrecha y más amplia que el ancho de banda de canal de radio, así que había una banda estrecha y banda ancha.

## Banda ancha

### Definición

La banda ancha o acceso a Internet de alta velocidad permite a los usuarios acceder a Internet y a los servicios relacionados a velocidades significativamente más rápidas que las disponibles mediante los servicios de discado (*dial-up*, en inglés). Las velocidades de banda ancha varían significativamente, dependiendo de la tecnología y del nivel de servicio contratado. Los servicios de banda ancha para consumidores residenciales proveen típicamente velocidades más rápidas de descarga de datos (de Internet a su computadora) que las velocidades de carga de datos (de su computadora a Internet).

### Tipos de redes inalámbricas de banda ancha

* **Red inalámbrica de área local (WLAN)** Las redes de área local inalámbricas (WLANs) constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado. Originalmente, las WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno de grandes redes corporativas, zonas industriales, campus universitarios, entornos hospitalarios, cyber cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet. Básicamente, una red WLAN permite reemplazar por conexiones inalámbricas los cables que conectan a la red los PCs, portátiles u otro tipo de dispositivos, dotando a los usuarios de movilidad en las zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada.
* **Wibro (Wireless Broadband Technology)** Wibro es una tecnología de banda ancha inalámbrica de Internet desarrollada por la industria de telecomunicaciones coreana. Adapta TDD para duplexarse (separar transmisión y recepción), OFDMA para el acceso múltiple y 8.75MHz como ancho de banda del canal. Esta tecnología fue ideada para superar la limitación de la velocidad del teléfono móvil y para agregar movilidad a Internet de banda ancha (por ejemplo, ADSL o LAN inalámbrica). Las estaciones de la base WiBro ofrecerán un rendimiento de procesamiento de datos agregado de 30 a 50 Mbps/s y cubrirán un radio de 1,5 km. Detalladamente, proporcionará la movilidad para los dispositivos móviles hasta 120 km/h, comparado al LAN inalámbrico cuya movilidad es la velocidad de una persona en movimiento y la del teléfono móvil que tiene movilidad de hasta 250 km/h.

## Diferencias entre banda ancha y banda angosta

* Las comunicaciones de banda estrecha utilizan un rango de frecuencia más pequeño (ancho de banda) en comparación con las comunicaciones de banda ancha.
* En el acceso a Internet, las tecnologías de banda ancha proporcionan una mayor velocidad de datos en términos de Mbps, mientras que las conexiones de banda estrecha proporcionan una velocidad de datos más lenta, como 56 kbps.
* En las comunicaciones de radio, el ancho de banda es más pequeño que el ancho de banda de coherencia del canal para banda estrecha y más ancho para banda ancha.

# SEGURIDAD EN REDES INALÁMBRICAS

## Requisitos de seguridad y ataques

La seguridad en redes implica 4 requisitos:

* **Privacidad:** Se requiere que sólo entidades autorizadas puedan tener un acceso a la información. Este tipo de acceso incluye la impresión, la visualización y otras formas de revelado, incluyendo el simple hecho de dar a conocer la existencia de un objeto
* **Integridad:** Se requiere que los datos sean modificados solamente por partes autorizadas. La modificación incluye la escritura, la modificación, la modificación del estado, la supresión y la creación.
* **Disponibilidad:** Se requiere que los datos estén disponibles para las partes autorizadas.
* **Autenticidad:** Se requiere que un computador o servicio sea capaz de verificar la identidad de un usuario.

### Ataques Pasivos

Es el ataque que intenta averiguar o hacer uso de información del sistema sin afectar a los recursos del mismo.

Los ataques pasivos consisten en escuchas o monitorizaciones de las transmisiones. La meta del oponente es la de obtener la información que está siendo transmitida. La divulgación del contenido de un mensaje y el análisis de tráfico constituyen dos tipos de ataques pasivos.

La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico o un fichero transferido pueden contener información sensible o confidencial. Por ello, desearíamos impedir que un oponente averigüe el contenido de estas transmisiones.

Un segundo tipo de ataque pasivo, el análisis de tráfico, es más sutil. Suponga que disponemos de un medio para enmascarar el contenido de los mensajes u otro tipo de tráfico de información, de forma que, aunque los oponentes capturasen el mensaje, no podrían extraer la información del mismo. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección por cifrado, el oponente podría todavía observar el patrón de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información podría serle útil para averiguar la naturaleza de la comunicación que se está realizando.

Los ataques pasivos son muy difíciles de detectar, ya que no suponen la alteración de los datos. Normalmente, el tráfico de mensajes es enviado y recibido de forma aparentemente normal y ni el emisor ni el receptor son conscientes de que un tercero haya leído los mensajes u observado el patrón de tráfico. Sin embargo, es factible impedir el éxito de estos ataques, usualmente mediante cifrado. De esta manera, el énfasis en la defensa contra estos ataques se centra en la prevención en lugar de en la detección.

### Ataques Activos

Es el tipo de ataque que intenta alterar los recursos del sistema o influir en su funcionamiento.

Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos. Los podemos clasificar en 4 categorías:

Un **enmascaramiento** tiene lugar cuando una entidad pretende ser otra entidad diferente. Un ataque por enmascaramiento normalmente incluye una de las otras formas de ataques activos. Por ejemplo, se pueden capturar secuencias de autenticación y retransmitirlas después de que tenga lugar una secuencia válida, permitiendo así obtener privilegios adicionales a otra entidad autorizada con escasos privilegios mediante la suplantación de la entidad que los posee.

La **retransmisión** supone la captura pasiva de unidades de datos y su retransmisión posterior para producir un efecto no autorizado.

La **modificación de mensajes** significa sencillamente que algún fragmento de un mensaje legítimo se modifica o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje con un significado «Permitir a Juan García leer el fichero confidencial de cuentas» se modifica para tener el significado «Permitir a Alfredo Castaño leer el fichero confidencial de cuentas»

La **denegación de servicio** impide o inhibe el normal uso o gestión de servicios de comunicación. Este ataque puede tener un objetivo específico. Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino concreto (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la interrupción de un servidor o de toda una red, bien deshabilitando el servidor o sobrecargándolo con mensajes con objeto de degradar su rendimiento.

Los ataques activos presentan características opuestas a las de los ataques pasivos. Mientras que un ataque pasivo es difícil de detectar, existen medidas para impedir que tengan éxito. Por otro lado, es bastante difícil impedir ataques activos de forma absoluta, ya que para hacerlo se requeriría protección física permanente de todos los recursos y de todas las rutas de comunicación. En su lugar, el objetivo consiste en detectarlos y recuperarse de cualquier interrupción o retardo causados por prevención.

## Privacidad con cifrado simétrico

La técnica universal para proporcionar privacidad en los datos transmitidos es el cifrado simétrico.

### Cifrado simétrico

Un esquema de cifrado simétrico tiene cinco ingredientes:

**Texto nativo (plaintext)**: es el mensaje original o datos que se proporcionan como entrada del algoritmo.

**Algoritmo de cifrado:** el algoritmo de cifrado lleva a cabo varias sustituciones y transformaciones sobre el texto nativo.

**Clave secreta:** la clave secreta es también una entrada del algoritmo de cifrado. Las sustituciones y transformaciones concretas realizadas por el algoritmo dependen de la clave.

**Texto cifrado (ciphertext):** es el mensaje alterado que se produce como salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.

**Algoritmo de descifrado:** es esencialmente el algoritmo de cifrado ejecutado a la inversa. Toma como entradas el texto cifrado y la clave secreta y produce como salida el texto nativo original.

Existen dos requisitos para la utilización segura del cifrado simétrico:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear que el algoritmo cumpla que, aunque un oponente conozca el algoritmo y tenga acceso a uno o más textos cifrados, sea incapaz de descifrar el texto o averiguar la clave. Este requisito se suele enunciar de una forma más estricta: el oponente debería ser incapaz de descifrar el texto o descubrir la clave incluso si él o ella poseyera varios textos cifrados junto a sus correspondientes textos nativos.
2. El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, toda comunicación que utilice esta clave puede ser leída.

### Algoritmo de cifrado

Los algoritmos de cifrado simétrico más comúnmente empleados son los cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño por cada bloque de texto nativo. Los dos algoritmos simétricos más importantes, ambos cifradores de bloque, son el estándar de cifrado de datos (DES) y el estándar avanzado de cifrado (AES).

#### El estándar de cifrado de datos (DES)

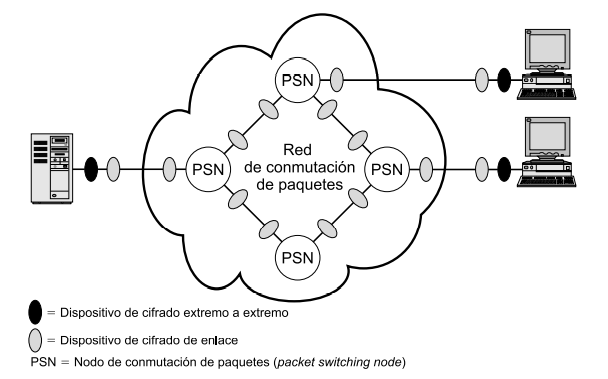
ES ha constituido el algoritmo de cifrada dominante desde su introducción en 1977. Sin embargo, dado que DES emplea sólo una clave de 56 bits, fue sólo una cuestión de tiempo que la velocidad de procesamiento computacional dejara a DES obsoleto. En 1998, la Fundación de la Frontera Electrónica (EFF, Electronic Frontier Foundation) anunció que había roto un reto de DES empleando una máquina de propósito específico para forzar DES, construida por menos de 250.000 dólares. El ataque duró menos de tres días. La EFF ha publicado una descripción detallada de la máquina, permitiendo que otros construyan su propio saboteador [EFF98]. Por supuesto, los precios del hardware continuarán cayendo al mismo tiempo que la velocidad de procesamiento irá aumentando, haciendo de DES un algoritmo inútil. La vida de DES fue prolongada gracias al uso de triple DES (3DES), que supone la repetición del algoritmo básico DES tres veces, utilizando dos o tres claves únicas, para una longitud de clave de 112 o 168 bits. El principal inconveniente de 3DES consiste en que el algoritmo por software es relativamente lento. Un inconveniente secundario es que tanto DES como 3DES utilizan un tamaño de bloque de 64 bits. Por razones de eficiencia y de seguridad, es deseable emplear bloques de mayor longitud.

#### Estándar de cifrado avanzando (AES)

A causa de las mencionadas deficiencias, 3DES no constituye un candidato razonable para su empleo a largo plazo. Como sustituto, el Instituto Nacional de Estándares y Tecnología (NIST, National Institute of Standards and Technology) publicó en 1997 una convocatoria de propuestas para un nuevo estándar de cifrado avanzado (AES, Advanced Encryption Standard), que debería poseer una robustez de seguridad igual o superior a la de 3DES y mejorar significativamente su eficiencia. Además de esos requisitos generales, NIST especificó que AES tenía que ser un cifrador de bloque simétrico con una longitud de bloque de 128 bits y admitir longitudes de claves de 128, 192 y 256 bits. Los criterios de evaluación incluían seguridad, eficiencia computacional, requerimientos de memoria, disponibilidad de software y hardware y flexibilidad. En 2001 se publicó AES como un estándar federal de procesamiento de información (FIPS 197, Federal Information Processing Standard).

### Localización de los dispositivos de cifrado

La aproximación más efectiva y común para enfrentarse a los ataques a la seguridad de la red es el cifrado. Si se utiliza, entonces necesitamos decidir qué vamos a cifrar y dónde se va a situar el equipo de cifrado.



En el cifrado de enlace, cada enlace de comunicaciones vulnerable se equipa con un dispositivo de cifrado en ambos extremos. Así se protege todo el tráfico que atraviese los enlaces de comunicaciones. Aunque esto requiere gran número de dispositivos de cifrado en redes amplias, este esquema proporciona un alto nivel de seguridad. Una desventaja de esta aproximación consiste en que el mensaje debe ser descifrado cada vez que entra en un conmutador de paquetes. Esto se debe a que el conmutador debe leer la dirección (número de circuito virtual) de la cabecera del paquete para encaminarlo. Así, el mensaje es vulnerable en cada conmutador. Si se trata de una red de conmutación de paquetes pública, el usuario no tiene control sobre la seguridad de los nodos.

Con un cifrado extremo a extremo, el proceso de cifrado se efectúa en los dos sistemas finales. La estación o terminal origen cifra los datos, que en forma cifrada se transmiten sin modificación a través de la red hasta la estación o terminal destino. El destino comparte una clave con el origen y es así capaz de descifrar los datos. Esta técnica parece proteger la transmisión contra ataques en los enlaces o conmutadores de la red. Sin embargo, existe aún un punto débil.

Considere la siguiente situación: un computador se conecta a una red de conmutación de paquetes X.25, establece un circuito virtual a otro computador y se prepara para transferir los datos al otro computador utilizando un cifrado extremo a extremo. Los datos se transmiten sobre esa red en forma de paquetes que constan de una cabecera y algunos datos de usuario. ¿Qué parte de cada paquete cifrará el computador? Supongamos que el computador cifra el paquete entero, incluyendo la cabecera. Esto no funcionará ya que, recuerde, sólo el otro computador puede realizar el descifrado. El nodo de conmutación de paquetes recibirá un paquete cifrado y no será capaz de leer la cabecera. Por tanto, no será capaz de encaminar el paquete. De esto se deduce que el computador sólo puede cifrar la parte de datos de usuario del paquete y debe dejar la parte de la cabecera intacta, para que la red pueda leerla

De esta manera, con el cifrado extremo a extremo, los datos de usuario están seguros. Sin embargo, el patrón de tráfico no lo está, ya que las cabeceras de los paquetes se transmiten sin cifrar. Para lograr un mayor grado de seguridad, se necesitan el cifrado del enlace y el extremo a extremo.

Para resumir, cuando se emplean ambas alternativas, el computador cifra la parte de datos de usuario usando una clave de cifrado extremo a extremo. Después se cifra el paquete completo usando una clave de cifrado de enlace. Conforme el paquete recorre la red, cada conmutador descifra el paquete utilizando una clave de cifrado de enlace para leer la cabecera y luego cifrar de nuevo el paquete entero para enviarlo por el siguiente enlace. Ahora el paquete entero está seguro, excepto durante el tiempo en el que el paquete está realmente en la memoria de un conmutador de paquetes, ya que la cabecera está desprotegida durante dicho intervalo.

### Distribución de claves.

Para que funcione el cifrado simétrico, las dos partes que realizarán un intercambio seguro de datos deben tener la misma clave y ésta debe protegerse para que no sea accesible por otros. Es más, es normalmente deseable realizar cambios frecuentes de la clave para limitar la cantidad de datos comprometidos si un atacante averiguara la clave. Por tanto, la fortaleza de cualquier sistema de cifrado reside en la técnica de distribución de claves empleada, un término que se refiere a los medios para distribuir una clave a las dos partes que deseen intercambiar datos, impidiendo que otros la vean. La distribución de claves se puede lograr de varias formas. Para dos partes A y B:

1. A podría seleccionar una clave y entregársela físicamente a B.
2. Una tercera parte podría seleccionar la clave y entregársela físicamente a B y A.
3. Si A y B han utilizado previa y recientemente una clave, una de las partes podría transmitir a la otra la nueva clave cifrada con la antigua clave.
4. Si A y B tienen cada uno una conexión cifrada con una tercera parte C, C podría entregar a B y A una clave a través de los enlaces cifrados

Las opciones 1 y 2 exigen una entrega manual de la clave. Éste es un requisito razonable para el cifrado de enlace, ya que cada dispositivo de cifrado de enlace va sólo a intercambiar datos con su pareja del otro extremo de enlace. Sin embargo, para el cifrado extremo a extremo, la entrega manual es complicada. En un sistema distribuido, cualquier terminal o computador dado puede necesitar efectuar intercambios con muchos otros terminales o computadores a lo largo del tiempo. Así, dispositivo necesita varias claves proporcionadas dinámicamente. El problema es especialmente difícil en sistemas distribuidos de área extensa.

La opción 3 constituye una posibilidad válida tanto para el cifrado de enlace como para el cifrado extremo a extremo, pero si un atacante tiene éxito consiguiendo una clave, entonces todas las claves posteriores son reveladas. Incluso si se cambian frecuentemente las claves de cifrado de enlace, dichos cambios deben realizarse manualmente. Por tanto, se prefiere la opción 4 para el cifrado extremo a extremo.

Se muestra una implementación de la opción 4 para el cifrado extremo a extremo. En la figura se ha ignorado el cifrado de enlace, que se puede incorporar o no según se requiera. En este esquema se identifican dos clases de claves:

**Clave de sesión:** cuando dos sistemas finales (computadores, terminales, etc.) desean comunicarse, establecen una conexión lógica (por ejemplo: circuitos virtuales). Durante la duración de la conexión lógica, todos los datos de usuario se cifran con una clave de sesión de un solo uso. Al terminar la sesión o la conexión, la clave de sesión se destruye.

**Clave permanente**: es una clave que se emplea entre entidades para la distribución de claves de sesión.

## Autenticación de mensajes y función de dispersión.

El cifrado protege contra los ataques pasivos (escuchas). Proteger contra ataques activos (falsificación de datos y transacciones) constituye un requisito diferente. La protección contra tales ataques se conoce como autenticación de mensajes.

### Alternativas para la autenticación de mensajes

Un mensaje, fichero, documento u otro conjunto de datos se dice estar autenticado cuando es genuino y proviene del origen pretendido. La autenticación de mensajes es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos son auténticos. Los dos aspectos importantes son verificar que el contenido del mensaje no se ha alterado y que el origen es auténtico. También podemos desear verificar la temporización de un mensaje (que no haya sido artificialmente retrasado y retransmitido) y verificar su secuencia relativa a los otros mensajes que se transmitan entre las dos partes.

#### Autenticación mediante cifrado simétrico

Es posible llevar a cabo la autenticación simplemente mediante el uso del cifrado simétrico. Si suponemos que solamente el emisor y el receptor comparten una clave (que es lo que debe ocurrir), entonces solamente el emisor genuino sería capaz de cifrar un mensaje satisfactoriamente para el otro participante. Es más, si el mensaje incluye un código de detección de errores y un número de secuencia, se le asegura al receptor que no se han efectuado modificaciones y que la secuencia es la adecuada. Si el mensaje incluye también una marca de tiempo, el receptor tiene la seguridad de que el mensaje no se ha retrasado más de lo normalmente esperado en el tránsito por la red.

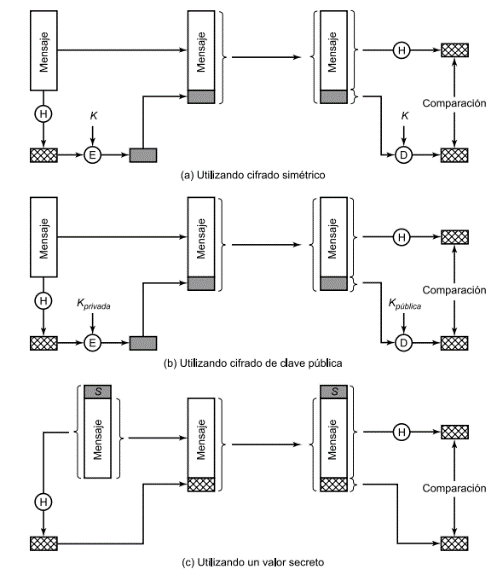
#### Autenticación de mensajes sin cifrado de mensajes.

En todas estas aproximaciones se genera una etiqueta de autenticación que se incorpora al mensaje para su transmisión. El mensaje mismo no está cifrado y se puede leer en el destino independientemente de la función de autenticación del mismo.

Ya que las técnicas descritas en esta sección no cifran el mensaje, al mensaje no se le proporciona privacidad. Dado que el cifrado simétrico proporciona autenticación y, dado que se utiliza ampliamente en productos existentes, ¿por qué no utilizar esta aproximación, que proporciona tanto privacidad como autenticación? En [DAVI89] se sugieren tres situaciones en las que es preferible la autenticación sin privacidad:

* Existen varias aplicaciones en las que el mismo mensaje se difunde a diferentes destinos. Por ejemplo, una notificación a los usuarios de que la red no está disponible en ese momento o una señal de alarma en un centro de control. Es más barato y más fiable tener solamente un destino para monitorizar la autenticación. De este modo, el mensaje debe difundirse en texto nativo con una etiqueta de autenticación del mensaje asociada. El sistema responsable lleva a cabo la autenticación. Si se detecta una violación de la autenticidad, se alerta a los otros sistemas destino mediante una alarma general.
* Otro posible escenario consiste en un intercambio en el que una de las partes soporta una carga muy elevada y no tiene tiempo de descifrar todos los mensajes que recibe. La autenticación se efectúa de forma selectiva, eligiendo mensajes de forma aleatoria para realizar las comprobaciones.
* La autenticación de un programa de computador en texto nativo es un servicio interesante. El programa se puede ejecutar sin tener que descifrarlo cada vez, lo que supondría un derroche de recursos de procesamiento. Sin embargo, si una etiqueta de autenticación de mensaje fuera incorporada al programa, se podría comprobar ésta siempre que se necesitara tener certeza de la integridad del programa

#### Función de dispersión de un solo sentido

Una variación del código de autenticación de mensajes al que se le ha prestado mucha atención recientemente es la función de dispersión de un solo sentido (one-way hash function). Como ocurre con el código de autenticación de mensajes, una función de dispersión acepta un mensaje M de longitud variable como entrada y produce un resumen del mensaje de longitud fija H(M) como salida. A diferencia del MAC, la función de dispersión no toma como entrada una clave secreta. Para autenticar un mensaje se envía junto a él el resumen del mensaje de forma que el resumen sea auténtico.

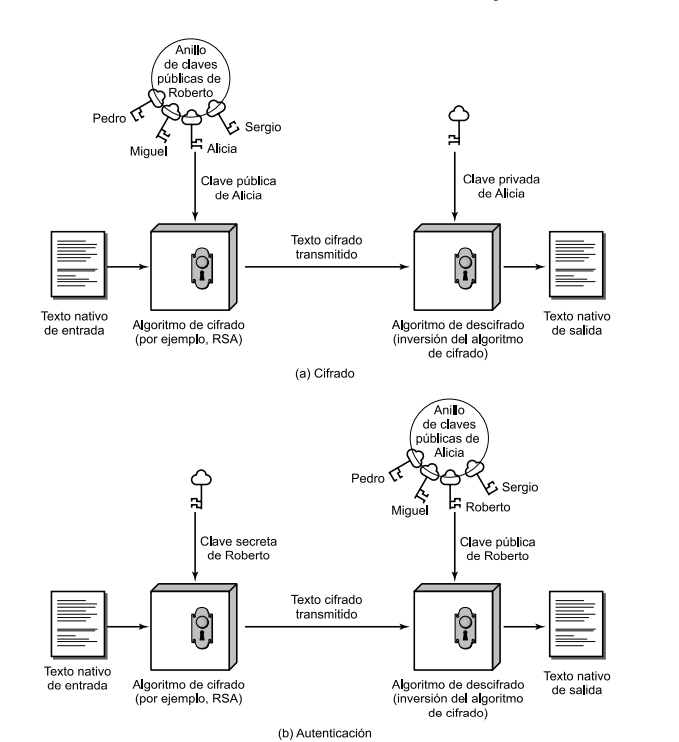
Se muestra tres formas en las que se puede autenticar un mensaje.

El resumen del mensaje se puede cifrar mediante cifrado simétrico (parte a). Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje también se puede cifrar utilizando cifrado de clave pública (parte b). La estrategia de clave pública tiene dos ventajas: proporciona una firma digital, así como la autenticación de los mensajes, y no requiere distribuir claves a las partes que se comuniquen.

## Cifrado de clave publica y firmas digitales.

### Cifrado de clave publica

El cifrado de clave pública, propuesto públicamente por primera vez por Diffie y Hellman en 1976 [DIFF76], es el primer avance realmente revolucionario en cuanto algoritmos de cifrado en, literalmente, miles de años. Y esto es debido a que el algoritmo de clave pública se basa en funciones matemáticas en lugar de en operaciones simples sobre patrones de bits. Pero más importante aún, la criptografía de clave pública es asimétrica, suponiendo el uso de dos claves diferentes, en contraste con el cifrado simétrico convencional, que sólo utiliza una. El uso de dos claves tiene profundas consecuencias en las áreas de privacidad, distribución de claves y autenticación.



Un esquema de cifrado de clave pública se compone de seis ingredientes

**Texto nativo:** es el mensaje legible o los datos que se suministran como entrada al algoritmo.

**Algoritmo de cifrado**: el algoritmo de cifrado lleva a cabo varias transformaciones sobre el texto nativo.

**Claves pública y privada:** este es un par de claves que han sido seleccionadas para que, si una se utiliza para el cifrado, la otra se use para el descifrado. Las transformaciones concretas que realiza el algoritmo de cifrado dependen de la clave pública o privada que se suministre como entrada.

**Texto cifrado:** es el mensaje desordenado producido como salida. Depende del texto nativo y de la clave. Para un mensaje dado, dos claves diferentes producirán dos textos cifrados diferentes.

**Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la clave correspondiente, produciendo el texto nativo original.

### Firma Digital

El cifrado de clave pública se puede utilizar de otra forma.

Suponga que Roberto quiere enviar un mensaje a Alicia y, aunque no es importante que el mensaje se mantenga secreto, quiere que Alicia tenga la certeza de que el mensaje proviene efectivamente de él. En este caso, Roberto utiliza su propia clave privada para cifrar el mensaje. Cuando Alicia recibe el texto cifrado, comprueba que puede descifrarlo con la clave pública de Roberto, demostrando así que el mensaje ha tenido que ser cifrado por Roberto. Nadie más tiene la clave privada de Roberto y, por tanto, nadie más ha podido crear el texto cifrado que pudo ser descifrado con su clave pública. De esta forma, todo el mensaje cifrado sirve como firma digital. Además, es imposible alterar el mensaje sin acceder a la clave privada de Roberto, por lo que el mensaje está autenticado en términos de origen e integridad de los datos.

En el esquema anterior, se cifra el mensaje entero, lo que, aunque valida al autor y al contenido, requiere una gran cantidad de almacenamiento. Cada documento debe guardarse en texto nativo para su utilización, por motivos prácticos. Se debe guardar también una copia del texto cifrado para que se pueda verificar el origen y el contenido en caso de disputa. Una forma más eficiente de lograr el mismo resultado consiste en cifrar un pequeño bloque de bits que sea una función del documento. Este bloque, llamado código de autenticación, debe poseer la propiedad de que no sea factible modificar el documento sin cambiar el código de autenticación. Si el código de autenticación se cifra con la clave privada del emisor, éste sirve como una firma que verifica al origen, al contenido y a la secuencia. Un código seguro de dispersión como SHA-1 puede realizar esta función.

Es importante enfatizar que la firma digital no ofrece privacidad. Es decir, el mensaje que se envía está seguro frente a alteraciones, pero no lo está de ser leído por otros. Esto es obvio en el caso de una firma basada en un fragmento del mensaje, ya que el resto se transmite sin cifrar. Incluso en el caso de cifrar el mensaje completo, no hay protección de privacidad, ya que cualquier observador puede descifrar el mensaje mediante la clave pública del emisor.

### Gestión de Claves

En el cifrado simétrico, un requisito fundamental para que dos partes se comuniquen de una forma segura es que compartan una clave secreta. Supongamos que Roberto quiera crear una aplicación para enviar mensajes que le permita intercambiar correo electrónico de forma segura con cualquiera que tenga acceso a Internet o a alguna otra red que ambos compartan. Supongamos que Roberto quiere utilizar sólo cifrado simétrico. Con el cifrado simétrico, Roberto y su corresponsal, digamos, Alicia, deben plantearse una manera para compartir una clave secreta única que nadie más conozca. ¿Cómo van a hacer esto? Si Alicia está en la habitación contigua, Roberto puede generar la clave y escribirla en un papel o almacenarla en un disquete y entregársela a Alicia. Pero si Alicia está en la otra parte del continente o del mundo, ¿qué puede hacer Roberto? Bien, podría cifrar la clave utilizando cifrado simétrico y enviarla por correo electrónico a Alicia, pero esto significa que Roberto y Alicia deben compartir una clave secreta para poder cifrar esta nueva clave secreta. Más aún, Roberto y cualquiera que utilice este nuevo paquete de correo electrónico se debe enfrentar al mismo problema con cualquier potencial corresponsal: cada pareja de corresponsales debe compartir una clave secreta única.

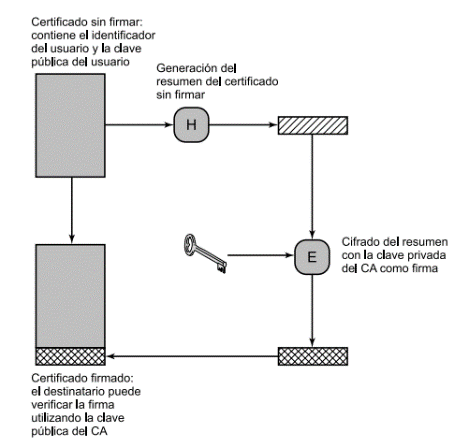
El problema más difícil para utilizar cifrado simétrico consiste en cómo distribuir las claves secretas de forma segura. Este problema desaparece en el cifrado de clave pública por el simple hecho de que nunca se distribuye la clave privada. Si Roberto quiere establecer correspondencia con Alicia y otras personas, genera un único par de claves, una privada y otra pública. Entonces guarda la clave privada de forma segura y difunde la clave pública a todos sin excepción. Si Alicia hace lo mismo, entonces Roberto tiene la clave pública de Alicia, Alicia tiene la clave pública de Roberto y ya pueden comunicarse con seguridad. Cuando Roberto desee comunicarse con Alicia, puede hacer lo siguiente:

1. Preparar un mensaje.
2. Cifrar el mensaje utilizando cifrado simétrico con una clave simétrica de sesión de un solo uso.
3. Cifrar la clave de sesión utilizando cifrado de clave pública con la clave pública de Alicia.
4. Adjuntar la clave de sesión cifrada al mensaje y enviarlo a Alicia

Solamente Alicia es capaz de descifrar la clave de sesión y, por tanto, de recuperar el mensaje original.

Para ser justos cabe señalar, sin embargo, que hemos sustituido un problema por otro. La clave privada de Alicia es segura ya que no necesita revelarla nunca. Sin embargo, Roberto ha de estar seguro de que la clave pública con el nombre de Alicia escrita en ella es de hecho la clave pública de Alicia. Alguien podría haber difundido una clave pública y haber dicho que era la de Alicia.

La solución a este problema es el certificado de clave pública. En esencia, un certificado consta de una clave pública más un identificador de usuario del propietario de la clave, todo ello firmado por una tercera parte de confianza. Normalmente la tercera parte es una autoridad de certificación (CA, Certificate Authority) en la que confía la comunidad de usuarios, como una agencia del gobierno o una institución financiera. Un usuario puede presentar su clave pública a la autoridad de un modo seguro y obtener un certificado. El usuario puede entonces publicar el certificado. Cualquiera que necesite la clave pública de este usuario puede obtener el certificado y verificar que es válido mediante la firma adjunta en que se confía.



# CONCLUSIONES

* La tecnología WIMAX ofrece grandes posibilidades de conexión para áreas suburbanas y rurales, lugares en donde podría solventar la carencia de acceso de banda ancha; debido a los costos elevados que la conexión tradicional representa. Además, gracias a su gran capacidad portadora se transforma en excelente plataforma para otras tecnologías como lo es, por ejemplo, videollamada.
* En cuanto a la relación entre WIMAX y WIFI podemos expresar que ambas tecnologías juegan un papel complementario, pues la primera está diseñada para operar en áreas metropolitanas, mientras que WIFI está diseñado para operar en rangos de pocos metros cuadrados; por lo tanto, WIMAX se proyecta como un medio idóneo para la interconexión de redes inalámbricas de área local ofreciendo mecanismos para garantizar niveles de transferencia óptimos.
* En esta monografía se pueden comprender mejor los fundamentos de las redes de banda ancha, el desarrollo de las tecnologías y aplicaciones. Se hacen notar las diferencias en cuanto a los equipos y normas de cada una de las redes y su contribución a la banda ancha.

# REFERENCIAS BIBLIOGRÁFICAS

Banda Angosta o Estrecha. (2011, enero 20). *Communications-1*. https://comunicationsone.wordpress.com/2011/01/19/banda-angosta-o-estrecha/

Escobar, D. H., Alberto, W., Hurtado, D. H., Carlos, J., Tumaya, D. V., & Luz, J. (s. f.). *Red Inalámbrica, instalación de una red Inalámbrica, configuración de Red Inalámbrica, software para redes inalámbricas, aplicaciones.* 65.

Gutiérrez, M. S. (s. f.). MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS. 22.

Ojeda, S. M. C. (s. f.). *WiM AX Descripción, Características, Escenarios de Uso y Estructura Organizacional para su Posible Implementación en Pasto (Nariño)*. 86.

*Volumen+1%2F3.-WiMAX.pdf*. (s. f.). Recuperado 29 de agosto de 2021, de http://bibing.us.es/proyectos/abreproy/11677/fichero/Volumen+1%252F3.-WiMAX.pdf

STALLINGS, William. Comunicación y Redes de Computadores. 7a. ed. España

https://www.academia.edu/5011511/Comunicaciones\_y\_Redes\_de\_Computadores\_7ma\_Edici%C3%B3n\_-\_William\_Stallings.pdf

Tanenbaum*, A. (2003). Redes de computadoras. In Paper Knowledge . Toward a Media History of Documents.*