UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

DISEÑO DE UNA RED INALÁMBRICA EN UNA SALA DE CÓMPUTO EDUCATIVA

T E S I S

PARA OBTENER EL TITULO

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

NANCY ACALCO RIOS

DIRECTORA DE TESIS:

M.C. CINTIA QUEZADA REYES

CIUDAD UNIVERSITARIA, CIUDAD DE MÉXICO, 2017

AGRADECIMIENTOS

AGRADECIMIENTOS

Este trabajo de tesis realizado en la Universidad Nacional Autónoma de México es un esfuerzo de personas que estuvieron participando de diferentes formas, ya sea dando apoyo moral, revisando y corrigiendo lo que se escribía en la misma, lo que me ha permito de alguna manera aprovechar lo investigado en varios lugares y así tener la oportunidad de adquirir mayor conocimiento.

Quiero agradecerle a mi mamá que es la primera persona que me ha apoyado en los momentos en lo que he estado a punto de desfallecer, ella me da la fuerza que necesito para seguir adelante y poder cumplir la metas que me estoy proponiendo. En este escrito le doy las gracias por su cariño y comprensión.

También le quiero agradecer a mi directora de Tesis la maestra Cintia Quezada Reyes por haber confiado en que podía desarrollar un buen tema, por su paciencia cuando revisaba mi escrito, así como por su valioso dirección y su apoyo para seguir con el tema hasta llegar al final del mismo.

Así mismo quiero darles las gracias a los profesores que me enseñaron en el transcurso de la carrera, sobre todo por los conocimientos que me proporcionaron.

No puedo dejar de mencionar a algunos amigos que en su momento me brindaron el apoyo para que esta Tesis se llevara a cabo.

Gracias

CONTENIDO

INTRODUCCIÓN

INTRODUCCIÓN

En la actualidad la comunicación inalámbrica está en el mercado de consumo, ya que los precios son accesibles o incluso en algunos lugares públicos la comunicación es gratis.

Hay diferentes aplicaciones a las que todos los usuarios tienen acceso, las cuales pueden ser visualizadas desde un teléfono celular hasta una computadora portátil (laptop), todo esto en tiempo real.

Conforme va pasando el tiempo, ya no es necesario que se cuente forzosamente con un cable para que se logre la comunicación, con los medios inalámbricos la productividad de las actividades cotidianas se realiza con mayor una facilidad que en años anteriores.

En la actualidad en algunos lugares ya se cuenta con dos tecnologías que en años pasados no se imaginaba que pudieran estar juntas, esto es, la red alámbrica y la inalámbrica, logrando una red híbrida, la cual está conformada por un sistema de cableado como una parte principal y como una parte secundaria se encuentra la red inalámbrica que da solución a las personas que necesitan trabajar fuera del perímetro cableado, lo que permite que el usuario no retrase sus labores y pueda llevarlas a cabo con toda la seguridad que la misma requiere.

Tales es el caso de la tecnología WiMAX que en algunos dispositivos de comunicación ya se está implementando como en los teléfonos móviles pero en nuestro país aún no cuenta con el equipo adecuado para que se implemente la misma en los móviles.

La combinación de las redes inalámbricas, es decir, WiFi y WiMAX y la de telefonía por IP permitirá el despliegue de las telecomunicaciones en las zonas apartadas en donde no es fácil la comunicación. Por lo que es necesario que se cuente con un ancho de banda suficiente para que se puedan integrar todos los servicios de multimedia los cuales son de voz, imagen y de datos ya que de alguna manera sin estos servicios la comunicación en estos tiempos es muy escasa.

En la primera generación de WiMAX solo se contaba con una velocidad de 10 GHz a 66 GHz, pero esto es con una línea de vista. Lo único que se trató con esta generación era la entrega de licencias para que se utilizara el servicio, lo que dio relevancia a que la tecnología se diera a conocer con los usuarios.

Hace unos meses el Instituto de Ingenieros Electricistas y Electrónicos (IEEE) liberó la última generación de WiMAX la cual es 802.16m la cual a inicios prometía que iba a tener una velocidad de 1Gbps pero tiene una velocidad mayor a las demás tecnologías inalámbricas la cual es a 300 Mbps, la cual también es conocida con WiMAX 2.

La nueva liberación permite que los aparatos móviles adopten la nueva velocidad, como ya lo está haciendo la telefonía celular y algunas compañías que venden computadoras portátiles como DELL.

Esta es la razón por la en algunas empresas tienen a sus empleados trabajando desde sus hogares, ya que las redes están siendo más seguras y más eficientes en la comunicación.

OBJETIVO

OBJETIVO

Poner las bases para el diseño de una red inalámbrica utilizando los protocolos y estándares establecidos para la implementación de la misma.

Satisfacer las necesidades de la institución con una nueva red inalámbrica.

Mejorar la seguridad de dicha red para obtener un mejor servicio y más beneficios para la organización y sus empleados.

Mejorar la comunicación para que los empleados tengan movilidad en la empresa con la información y la seguridad en la transferencia de información.

CAPÍTULO I

CONCEPTOS GENERALES

DEFINICIÓN DE REDES

Una **red de computadoras** es un sistema de comunicación de datos, definida como una interconexión de computadoras y otros dispositivos periféricos conectados entre sí para compartir información, los recursos y servicios, para que potencialmente se pueda aumentar la disponibilidad de los sistemas, obtener la posibilidad de poseer fuentes alternativas de recursos en una red y tener acceso remoto a la información.

Una red cuenta con tres niveles de componentes:

a) Software de aplicaciones

Está formado por programas informáticos que se comunican con los usuarios de la red, permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).

Un tipo de *software* de aplicaciones se denomina cliente-servidor. “El modelo cliente-servidor ofrece un conveniente método para colocar funciones en ordenadores distribuidos en una o múltiples redes. El servidor no utiliza ningún recurso hasta que reciba una solicitud para que así ocurra.”[1]

[1] Vanesa Casanova Fernández, U. B. (2009). *Sams Teach Yourself Networking in 24 Hours.* España: Ediciones Anaya Multimedia.

Otro tipo de *software* de aplicación se conoce como 'de igual a igual' (*peer to peer*). En una red de este tipo los ordenadores se envían entre sí mensajes y peticiones directamente sin utilizar un servidor como intermediario.

b) Software de red

"Se hace referencia a los medios de transmisión de datos, el protocolo de control de transmisión de datos y el de internet. Ambos son una parte del gran conjunto de protocolos que se encuentran dentro del paquete.

Con la combinación de ambos protocolos, se pueden transportar datos a través del internet. En otras palabras, dichos protocolos son los proveedores de todos los servicios que utiliza el usuario." [2] Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

[2] Alvarez, C. A. (1998). *Máxima Seguridad en Internet.* España: Anaya Multimedia.

c) **H*ardware* de red**

Está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red que permite acceder al medio, material que conecta a los ordenadores, recibir paquetes desde el *software* de red, transmitir instrucciones y peticiones a otras computadoras.

Por lo que podemos llamar que es un servidor de datos, “En realidad, que algo sea más grande no siempre significa que sea lo mejor. El objetivo de generar una red de datos, ha sido lograr piezas interiores sean cada vez más pequeñas y sean rápidas y baratas porque requiere menor energía para trabajar” [3]

Una red de computadoras debe cumplir con algunos aspectos de seguridad para que se lleve a cabo con una mayor fiabilidad; algunos que se pueden mencionar:

a) Confiabilidad

Estar disponible y con una velocidad de respuesta adecuada.

b) Confidencialidad

Poder tener un sistema de protección para los datos e información de los usuarios.

[3] Solórzano, C. a. (1995). *¡Redes Facil!* Edo.de México: Prentice-Hall Hispanoamericana, S.A.

c) Integridad

Éste es referente a la corrección y completitud de la información

1.1 TOPOLOGÍAS DE RED

La topología de red es un arreglo físico o lógico en el cual los dispositivos o los nodos de una red (computadoras, impresoras, servidores, hubs, switches, enrutadores, etcétera) se interconectan entre sí con un medio de comunicación (transmisión) adecuado.

Una topología de red es una forma de colocar un cable a estaciones de trabajo individual; esto puede ser desde los muros, suelos, etcétera. Hay factores que se deben considerar para determinar cuál sería la topología adecuada.

En la configuración de las redes existen tres aspectos diferentes que se deben de tomar en cuenta:

1. Topología lógica

Se refiere a la trayectoria lógica que una señal sigue a su paso por los nodos de la red.

Los dos tipos más comunes de topologías lógicas son:

a) Broadcast

“Se basa en un único proceso de envío, independientemente del número de potenciales máquinas receptoras, de una misma información en una o más unidades de datos (datagramas IP) desde un origen a

todas las máquinas de una red de área local. Todo ello, sin necesidad de transmitir desde el origen una copia de la misma información, por separado, a cada una de dichas máquinas.

Se resalta el hecho de que desde la máquina origen sólo se envía una vez la pertinente información y no se transmiten “n” copias de la misma aunque haya “n” destinatarios.

El problema de este tipo de difusión es que aparte de aumentar el tráfico por la red, la información transmitida llegará posiblemente a ciertas máquinas que no tienen el más mínimo interés por la información en cuestión. Este tipo de transmisión es muy frecuente en enlaces basados en redes de área local del tipo Ethernet IEEE 802.” [4]

Es por orden de llegada, es así como funciona Ethernet, como se muestra en la 1.1 en donde el codificador vendría siendo el broadcast.

[4] Leyva/09, J. L. (2003). *Cisco Networking Academy Program*. Obtenido de Cisco Networking Academy Program: www.innacap.cl

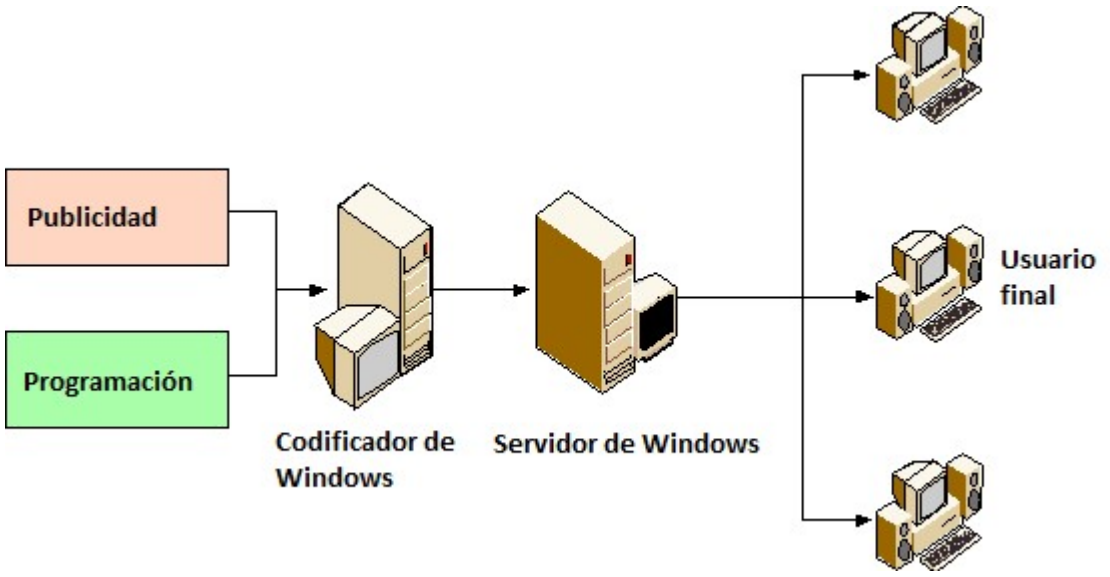


Figura 1.1 Broadcast [5]

b) Transmisión de tokens

"Es un sistema de red de banda base, con paso de un testigo (token), de forma secuencial. La velocidad de transmisión de un token de 2.5 [Mbits/seg]." [6]

Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de estrella.

[5] Leyva/09, J. L. (2003). *Cisco Networking Academy Program*. Obtenido de Cisco Networking Academy Program: www.innacap.cl

[6] Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING)*. México: McGRAW-HILL/INTERAMERICANA DE ESPAÑA.

Hay varias topologías para una red básica, pero no se puede dejar de lado la existencia de las redes híbridas que es la combinación de una o más topologías en una misma red.

2. Topología matemática

Esta topología es la que está basada en los mapas de los nodos y de los enlaces que están formando los patrones de una red.

Es una sucesión de nodos que no necesariamente tiene que ser una cantidad grandes de dichos, para que se realice una cantidad, es decir es como un filtro para que se estudie la convergencia en un espacio.

3. Topología física

Puede definirse como la forma en la que se adopta un plano esquemático del cableado o de la estructura física de la red, también se habla de métodos de control que se utilizan de acuerdo con la necesidad planteada.

a) TOPOLOGÍA DE BUS O LINEAL

"Un único cable de conexión conecta una estación en una topología serie. Las señales se emiten a todas las estaciones, pero sólo recibe los paquetes la estación a la cual se dirige. Ethernet 802.3 IEEE es la principal norma de bus." [7]

Las computadoras escuchan al emisor, cuando ya están listas para transmitir, ellas se aseguran de que no haya nadie más transmitiendo en él mismo canal, para que entonces puedan enviar sus paquetes de información. Las redes de bus basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión) típicamente emplean la arquitectura de red Ethernet.

Las redes de bus comúnmente utilizan cable coaxial como medio de comunicación (transmisión), las computadoras se conectaban al ducto mediante un conector BNC en forma de T. En el extremo de la red se coloca un terminador (si se utilizaba un cable de 50 ohm, se ponía un terminador de 50 ohms) (Figura 1.2).

[7] Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING).* México: McGRAW-HILL/INTERAMERICANA DE ESPAÑA.

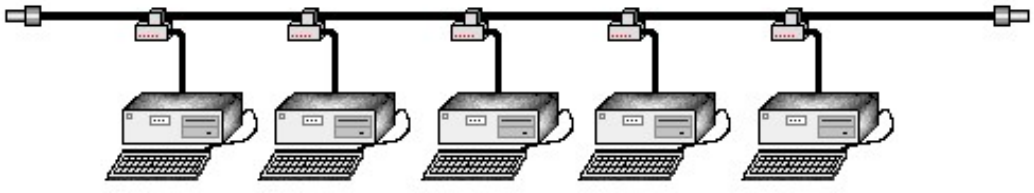


Figura 1.2 Topología de bus [8]

La topología de bus como tiene una fácil instalación es la que se podía adaptar con mayor facilidad a un lugar en donde se obtuvieran bastantes equipos de cómputo, sin embargo si por alguna razón se rompiera el cable coaxial se inhabilitaría la comunicación por completo de la red. Es por tal motivo que esta topología dejó de ser útil para transmitir comunicación.

b) TOPOLOGÍA DE ESTRELLA

"Las redes con topología en estrella son bien activas o bien pasivas. En la topología de estrella pasiva, se configura con una caja que sencillamente sirve para la organización del cable, como un bloque de conexión de telefónica. En la topología de estrella activa, un conector (hub) es un dispositivo que regenera y repite las señales. El concentrador activo puede contener características de diagnóstico que indica las puertas defectuosas o que rinde cuentas de la información con fallos a la estación gestora. Un fallo en un nodo o la ruptura de un cable de un nodo no incapacita al resto de la red." [9]

[8 y 9] Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING).* México: McGRAW-HILL/INTERAMERICANA DE ESPAÑA.

Debido a que la topología estrella de tipo activa utiliza un cable de conexión para cada computadora aunque alguna no tenga comunicación, la misma no se pierde puesto que los demás equipos seguirán con la transmisión de información, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch (aunque se pueden conectar hubs o switches en cadena para así incrementar el número de puertos) (Figura 1.3).

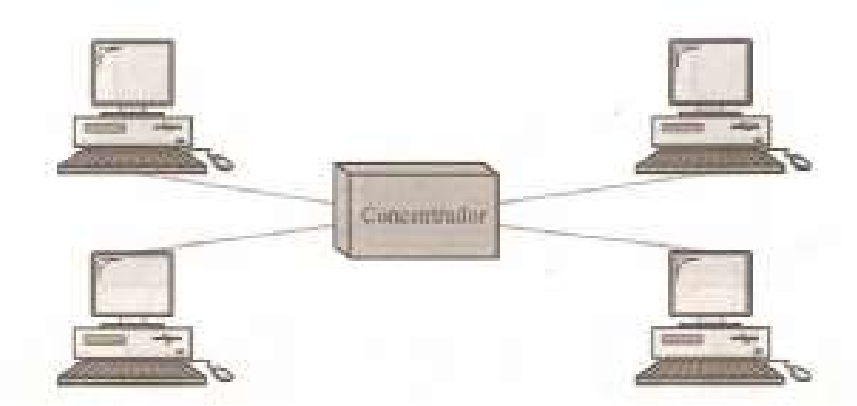


Figura 1.3 Topología de estrella

c) TOPOLOGÌA DE ESTRELLA EXTENDIDA

Se utiliza con el fin de facilitar la administración de la red. Físicamente la red es una estrella centralizada en un concentrador o hub, mientras que a nivel lógico la red es un anillo.

d) TOPOLOGÍA BUS EN ESTRELLA

En este caso la red es un bus que se cablea físicamente como una estrella mediante el uso de concentradores.

e) TOPOLOGÍA ESTRELLA JERÁRQUICA

Esta estructura se utiliza en la mayor parte de las redes locales actuales. Por medio de concentradores dispuestos en cascadas para formar una red jerárquica.

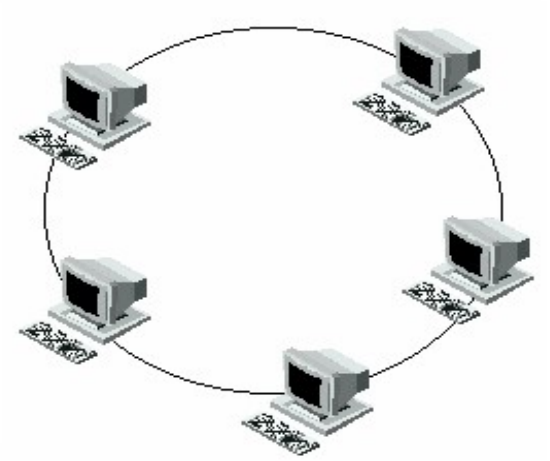
f) TOPOLOGÍA DE ANILLO

"La topología de red de anillo es una topología en ciclos cerrados que no precisa terminadores. La topología de anillo con el testigo forma un anillo lógico pero el cable se dispone como si fuese una estrella con un concentrador central. El anillo se mantiene gracias al concentrador. Cuando se conecta al concentrador una nueva estación de trabajo, el anillo se extiende a la estación a través del cable, para luego regresar al concentrador." [10]

[10] Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING).* México: McGRAW-HILL/INTERAMERICANA DE ESPAÑA.

Esta topología conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa (retransmite los paquetes que recibe y los envía a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un token). Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red.

El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y se posiciona de él (Figura 1.4).



1.4 Topología de anillo

g) TOPOLOGÍA DE ANILLO DOBLE

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo con la diferencia de que para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos.

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

h) TOPOLOGÍA DE MALLA

La topología de malla utiliza conexiones redundantes entre los dispositivos de la red que tiene como estrategia la tolerancia de fallas. Cada dispositivo en la red está conectado a todos los demás.

Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe (Figura 1.5).

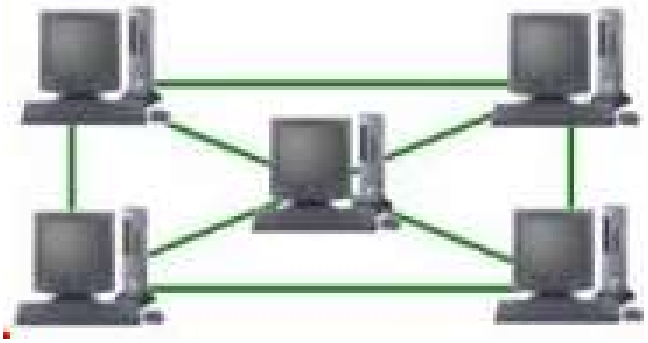


Figura 1.5 Topología de malla [11]

[11] Leyva/09, J. L. (2003). *Cisco Networking Academy Program*. Obtenido de Cisco Networking Academy Program: www.innacap.cl

i) TOPOLOGÍA DE ÁRBOL

"Está formado por segmentos de red o subredes, las cuales dependen de un concentrador específico. Cada estación de trabajo compite por el acceso a la red con otras estaciones dentro de un segmento y después con otros segmentos." [12]

En esta topología que es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia afuera utilizando ramas en donde se conectan las demás terminales.

Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más existe una ruta de datos entre dos terminales cualesquiera (Figura 1.6)

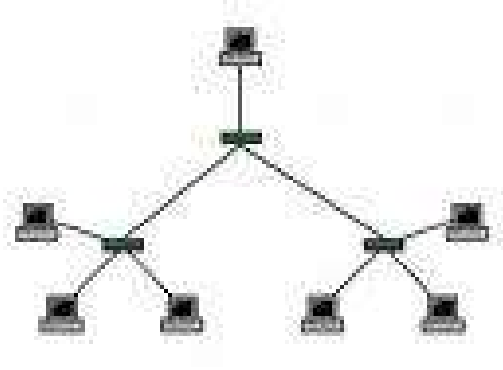


Figura 1.6 Topología de árbol [13]

[12 y 13] M., A. G. (1997). Telecomunicaciones: Redes de datos. México: McGRAW-HILL

j) TOPOLOGÍA DE RED CELULAR

"Se utiliza en las redes inalámbricas, se utilizan protocolos de difusión; todos los nodos son capaces de recibir transmisiones en un canal de control desde una ubicación central. Un nodo inalámbrico central, conocido con el nombre de estación base, utiliza este canal común para ordenar a un nodo que bloquee el canal específico de usuario para la conexión. Durante la conexión en curso, el teléfono móvil se comunica simultáneamente con la estación base, con el enlace de control y con el enlace de usuarios." [14]

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

En una topología celular (inalámbrica) no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites) (Figura 1.7).

[14] Black, U. (2009). *Redes.* Madrid: Gráficas Hermanos Goméz, S.L.L.

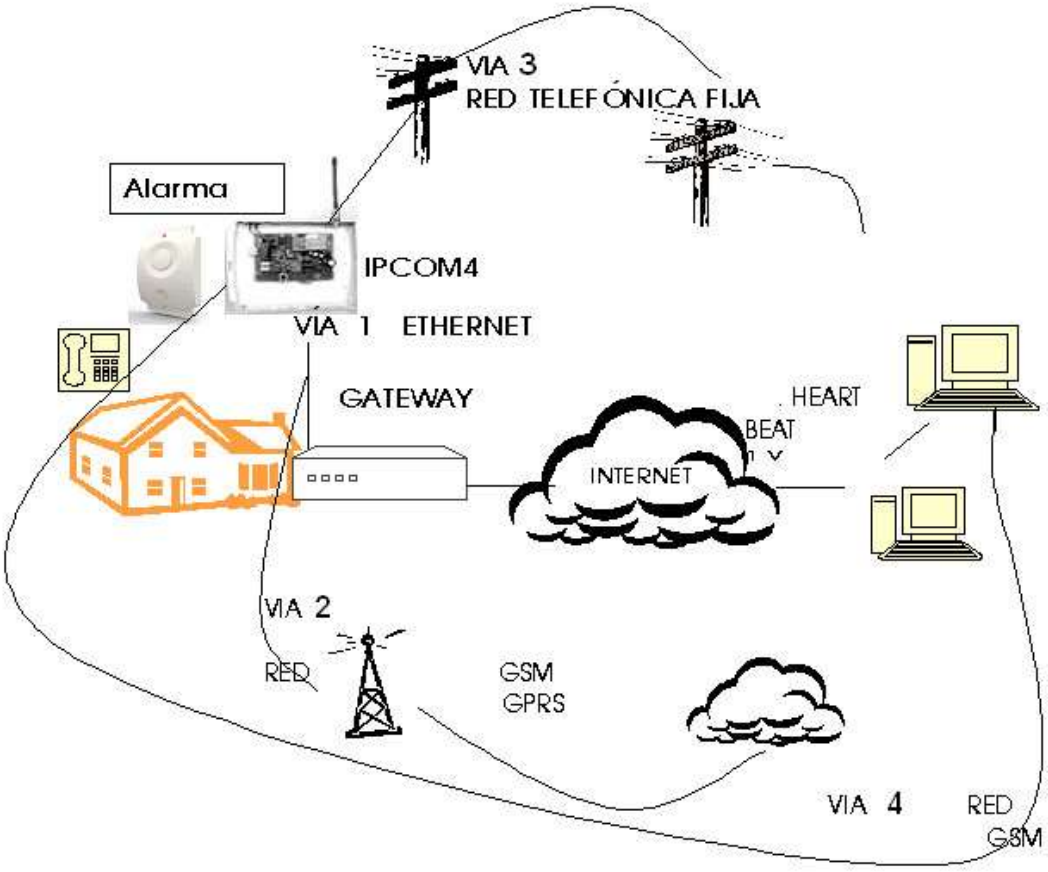


Figura 1.7 Topología de red celular [15]

k) TOPOLOGÍA HÍBRIDA

La palabra híbrida se utiliza de diferentes maneras en referencia a topologías de redes. Se usa el término híbrido para describir redes que corren con múltiples protocolos, sistemas operativos, y plataformas. En este caso la palabra híbrida hace referencia a las topologías que combinan elementos de dos o más de las topologías básicas. (*Estrella, Bus, Malla).* (Figura 1.8).

[15] Black, U. (2009). *Redes.* Madrid: Gráficas Hermanos Goméz, S.L.L.

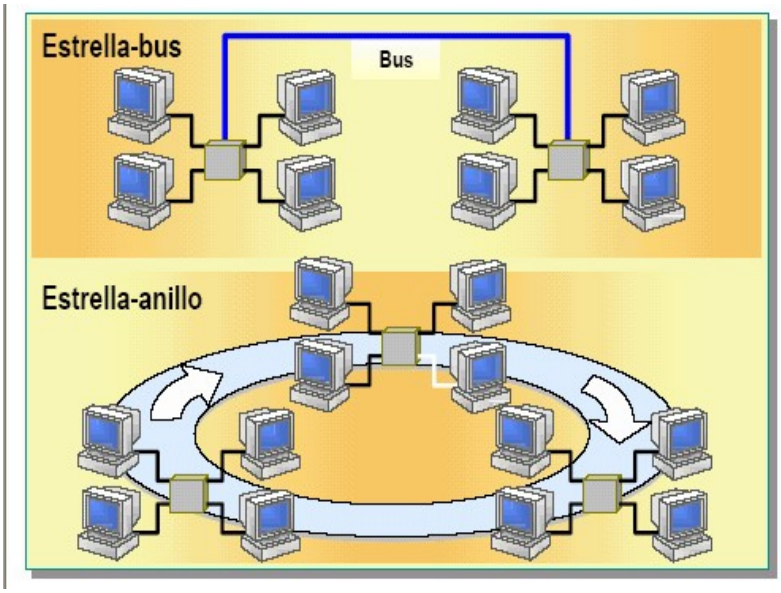


Figura 1.8 Topología híbrida

1.3 TIPOS DE REDES SEGÚN SU EXTENSIÓN

Un criterio para clasificar redes de computadoras es el que se basa en su extensión geográfica, es en este sentido en el que se habla de redes LAN, MAN y WAN.

1. Redes de Área Local (LAN *Local Área Network*)

"Una red de área local (LAN, Local Área Network) conecta las computadoras de un grupo de trabajo, departamento u oficina. En contraste, una inter-red es una colección de LAN's dentro de un edificio, grupo de edificios o áreas de campus y una red de área extensa." [16]

Es una red simple. La cual tiene una velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps y 1 Gbps. Una red de área local puede contener 100 o incluso 1000 usuarios (Figura 1.9).

Al extender la definición de una LAN con los servicios que proporciona, se pueden definir dos modos operativos diferentes:

En una red "de igual a igual" (P2P), la comunicación se lleva a cabo de un equipo a otro sin un equipo central y cada equipo tiene la misma función.

[16] Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING).* México: McGRAW-HILL/INTERAMERICANA DE ESPAÑA.

En un entorno "cliente/servidor", un equipo central les brindan servicios de red a los usuarios

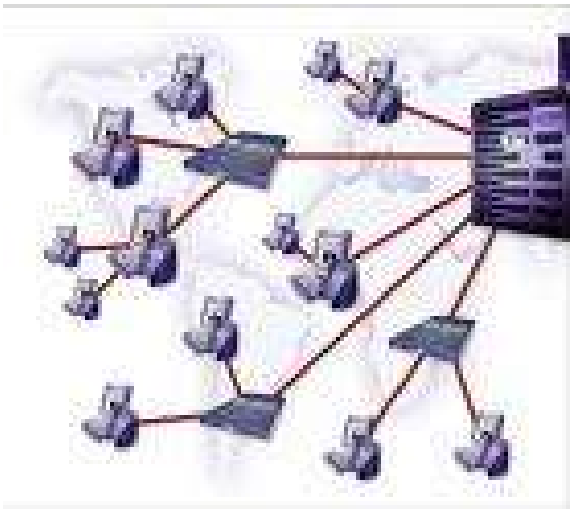


Figura 1.9 LAN

2. REDES DE ÁREA METROPOLITANA (MAN)

"Esta es una red que cubre una ciudad completa, pero utiliza la tecnología desarrollada para la LAN. Tiene el propósito de interconectar ordenadores entre sí.[17]

Este tipo de redes se utiliza normalmente para interconectar redes de área local (Figura 1.10).

[17] Tanenbaum, A. S. (1991). *Redes de Ordenadores.* México: Prentice- Hall Hispanoamericana, S.A.

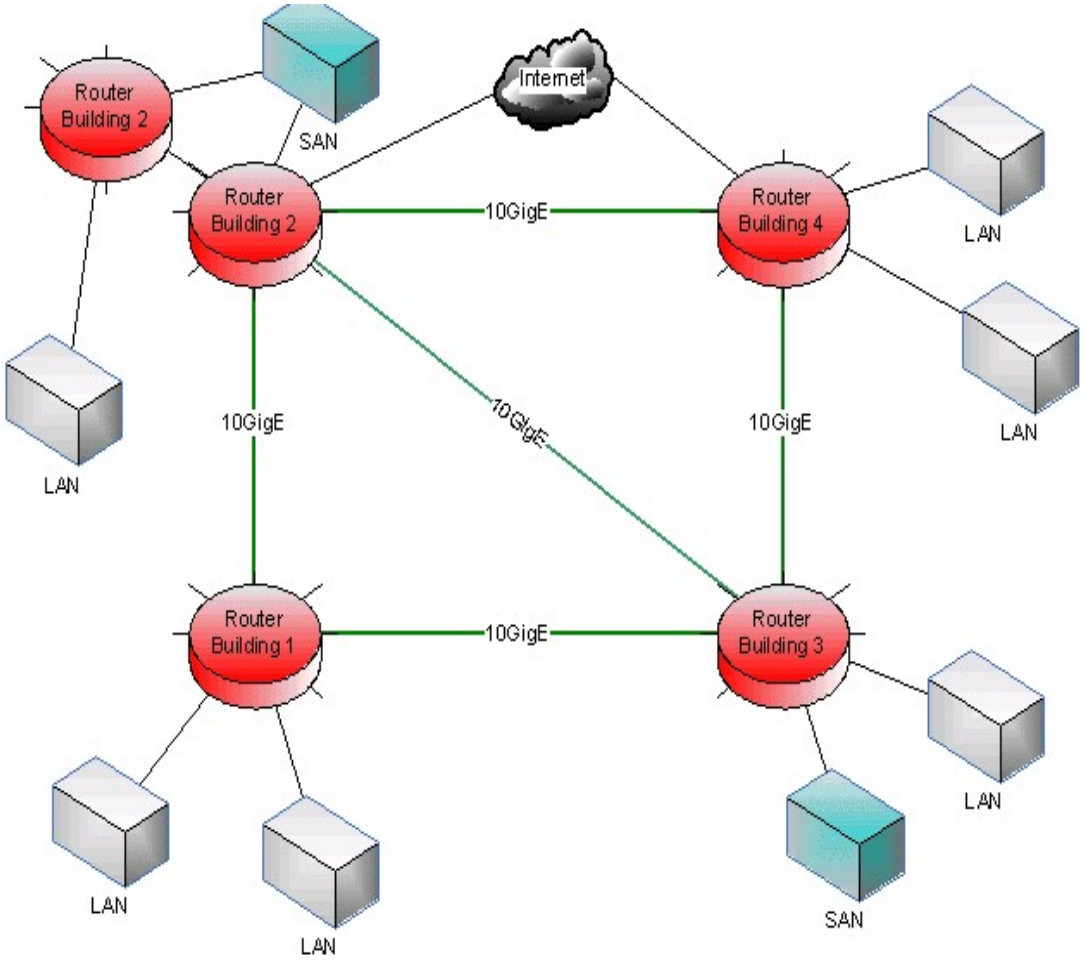


Figura 1.10 MAN

3. REDES DE ÁREA AMPLIA (WAN)

Una WAN (Wide Área Network) se extiende sobre un área geográfica amplia, a veces un país o un continente; el cual contiene una colección de máquinas dedicadas a ejecutar programas de usuario u aplicaciones, estas máquinas son comúnmente conocidas como hosts.

Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un host a otro. La separación entre los aspectos exclusivamente de comunicación de la red o la subred y los aspectos de aplicación, simplifica enormemente el diseño total de una red (Figura 1.11).

En muchas redes de área amplia, la subred tiene dos componentes distintos:

a) Las líneas de transmisión

Mueven los bits de una máquina a otra.

b) Los elementos de conmutación

Son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. A las computadoras de conmutación, se les conoce mejor como enrutadores.

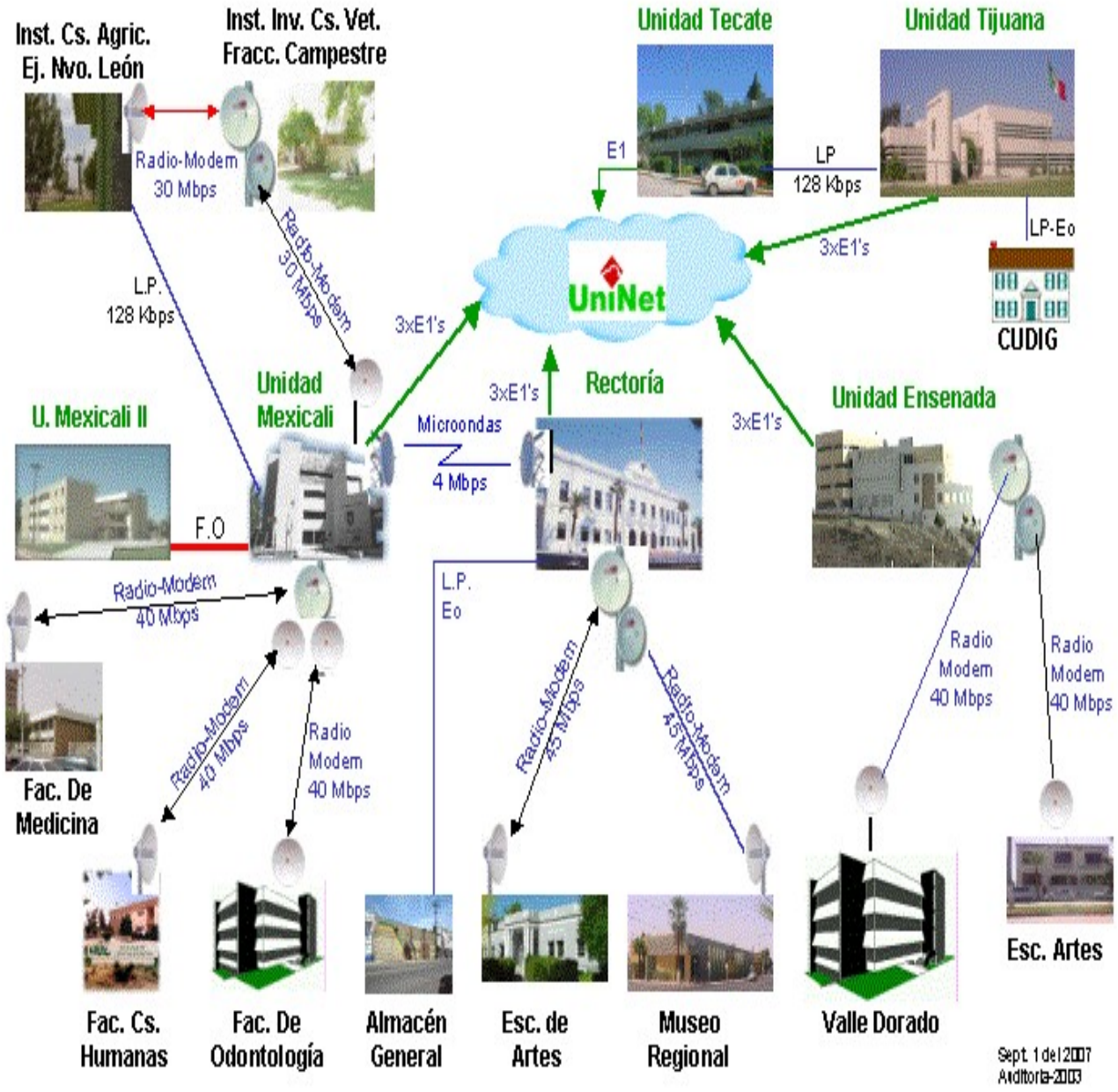


Figura 1.11 WAN

4. INTERREDES

La Interred es un sistema de comunicación compuesto por varias redes que se han enlazado juntas para proporcionar posibilidades de comunicación ocultando las tecnologías y los protocolos y métodos de interconexión de las redes individuales que la componen.

Éstas son necesarias para el desarrollo de sistemas distribuidos que son abiertos extensibles. En ellas se puede integrar una gran variedad de tecnología de redes de área local y amplia para proporcionar la capacidad de trabajo en red necesaria para cada grupo de usuario.

Así que las interredes aportan gran parte de los beneficios de los sistemas abiertos a las comunicaciones de los sistemas distribuidos.

Las interredes se construyen a partir de varias redes. Éstas están interconectadas por computadoras dedicadas llamadas routers y computadoras de propósito general llamadas gateways y por un subsistema integrado de comunicaciones producidos por una capa de software que soporta el direccionamiento y la transmisión de datos a las computadoras a través de la interred. Los resultados pueden contemplarse como una red virtual construida a partir de solapar una capa de interred sobre un medio de comunicación que consiste en varias redes, routers y gateways.

En la tabla 1.1 se muestra cómo se distribuyen los diferentes tipos de red y la extensión que abarca.

Tabla 1.1 Redes según su extensión

	Rango	Ancho de Banda (bps)	Latencia (ms)
LAN	1 – 2 Km	10 – 1,000	1 – 10
WAN	Mundial	0.010 – 600	100 - 500
MAN	250 Km	1 - 150	10
LAN inalámbrica	1.15 – 1.5 Km	1 - 150	5 - 20
WAN inalámbrica	Mundial	0.010 - 2	100 – 500
Internet	Mundial	0.010 - 2	100 - 500

1.4 CLASIFICACIÓN DE UNA RED SEGÚN SU ACCESIBILIDAD

Se pueden tener dos tipos de redes de acuerdo con la accesibilidad y a la facilidad de conexión ya que con esto se puede obtener una mejor disponibilidad de servicio.

1.4.1 REDES ALÁMBRICAS

Este tipo de red proporciona a los usuarios una buena seguridad y la capacidad de mover muchos datos de manera rápida y efectiva. Además son más rápidas que las redes inalámbricas y son más económicas de implementar.

Sin embargo, el costo de las redes alámbricas puede crecer entre más computadoras sean y más retiradas se encuentren entre ellas. Además, a menos que se esté construyendo una casa o edificios nuevos y se planee con anticipación la instalación del cableada (Figura 1.11).

Si tan sólo se planea conectar dos computadoras, lo único que se necesita es una tarjeta de red (NIC) en cada computadora y el cable para conectarlas.

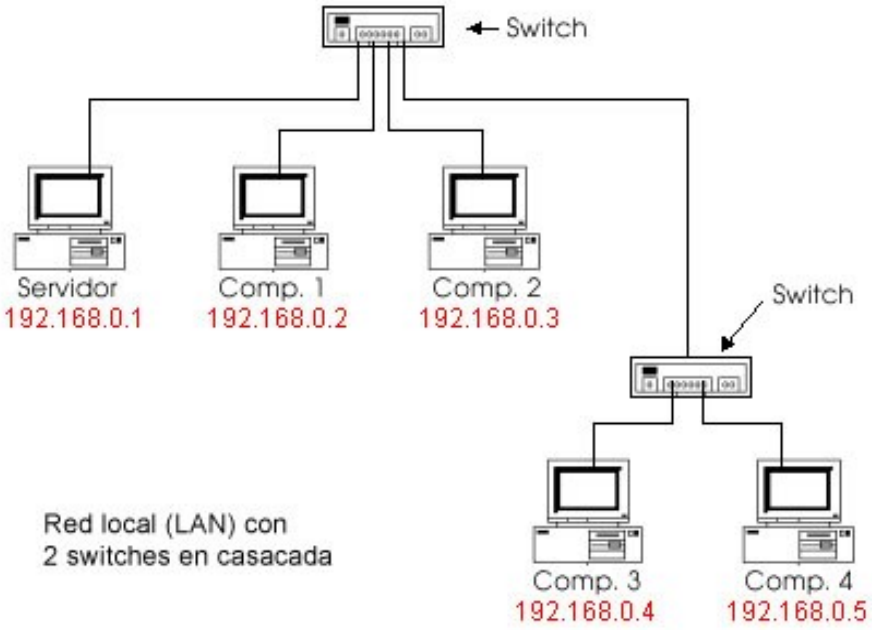


Figura 1.12 Red alámbrica

1.4.2 REDES INALÁMBRICAS

La conexión de los dispositivos portátiles y de mano necesita redes de comunicación inalámbrica. Algunos de ellos son los que se encuentran dentro del estándar IEEE 802.11 (este estándar está basado en dos capas inferiores que son la capa física y la de enlace de datos) y forman parte de verdaderas redes LAN inalámbricas que se diseñaron para que se utilizaran en vez de las redes LAN (Figura 1.13).

También se encuentran las redes de área personal inalámbricas, incluida la red europea mediante el Sistema Global para Comunicaciones Móviles, GSM (global system for mobile communication).

En las redes inalámbricas se restringe el ancho de banda disponible y existen limitaciones de los conjuntos de protocolos llamados Protocolos de Aplicación Inalámbrica WAP (Wireless Aplication Protocol)

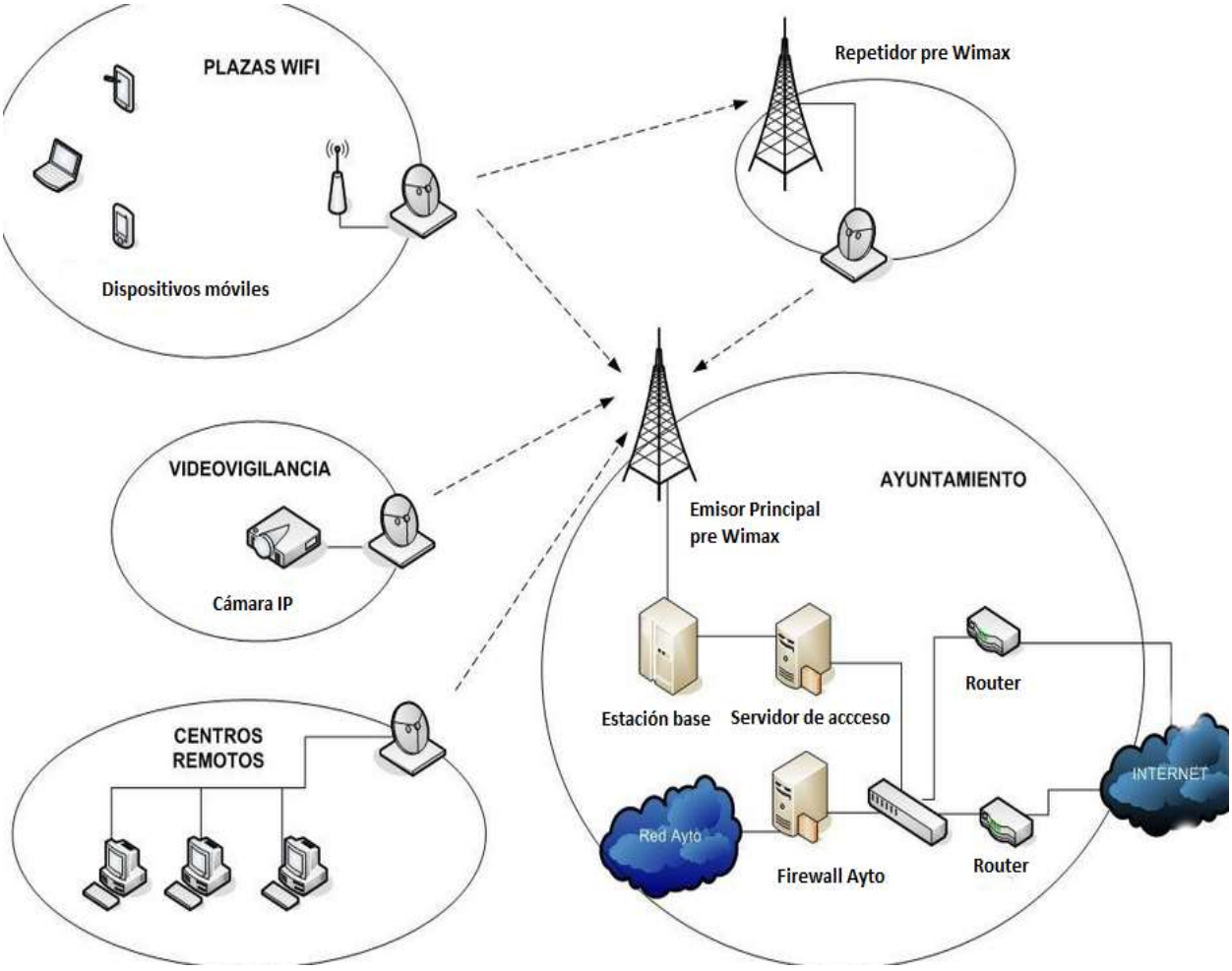


Figura 1.13 Red inalámbrica

1.4.2.1 WI-FI

Wi-Fi, son las sigla para Wireless Fidelity (Wi-Fi), que literalmente significa Fidelidad inalámbrica.

Es un conjunto de redes que no requieren de cables y que funcionan con base en ciertos protocolos previamente establecidos. Si bien fue creado para acceder a redes locales inalámbricas, hoy es muy frecuente que sea utilizado para establecer conexiones a Internet.

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuera compatible entre los distintos aparatos.

En concreto, esta tecnología permite a los usuarios establecer conexiones a Internet sin ningún tipo de cables y puede encontrarse en cualquier lugar que se haya establecido un punto caliente o hotspot Wi-Fi.

En la actualidad se emplea el estándar 802.1X en la comunicación Wi-Fi

En los siguientes puntos se explica la historia de cómo fue evolucionando Wi-Fi

1) (Stallings, 2000)El primero es el estándar IEEE 802.11b que opera en la banda de 2.4 GHz a una velocidad de hasta 11 Mbps.

2) El segundo es el IEEE 802.11g que también opera en la banda de 2.4 GHz, pero a una velocidad mayor, alcanzando hasta los 54 Mbps.
3) El tercero que está en uso es el estándar IEEE 802.11a que se le conoce como Wi-Fi 5, ya que opera en la banda de 5 GHz, a una velocidad de 54 Mbps. Una de las principales ventajas de esta conexión es que cuenta con menos interferencias que los que operan en las bandas de 2.4 GHz ya que no comparte la banda de operaciones con otras tecnologías como bluetooth.
4) El cuarto, y que aún se encuentra en estudio, es el IEEE 802.11n que operaría en la banda de 2.4 GHz a una velocidad de 108 Mbps.
5) Los estándares actuales son 802.11h y 802.11j y permiten la interoperabilidad entre los productos de diferentes continentes. Finalmente, 802.1X soporta la autenticación de usuarios.

Los estándares que se emplean en la actualidad con la tecnología inalámbrica de Wi-Fi se muestran en la tabla 1.2

Tabla 1.2 Estándares actuales de Wi-Fi

Estándar	Funcionalidad Principal
802.11e: MAC Enhancements (QoS)	Mejoras en capa MAC
802.11k: Radio Resource Measurement	Mediciones y registros de rendimiento
802.11n: High Throughput	Alta velocidad de transmisión
802.11p: Wireless Access for the Vehicular Environment	Wi-Fi en vehículos
802.11r: Fast Roaming	Transiciones entre puntos de acceso
802.11s: ESS Mesh Networking	Redes Malla 802.11
802.11u: InterWorking with External Networks	Interoperabilidad con otras redes

Para contar con este tipo de tecnología es necesario disponer de un punto de acceso que se conecte al módem y un dispositivo Wi-Fi conectado al equipo. Aunque el sistema de conexión es bastante sencillo, trae aparejado riesgos ya que no es difícil interceptar la información que circula por medio del aire. Para evitar este problema se recomienda el cifrado de la información.

Actualmente, en muchas ciudades se han instalados nodos Wi-Fi que permiten la conexión a los usuarios. Cada vez es más común ver

personas que pueden conectarse a Internet desde cafés, estaciones de metro y bibliotecas, entre muchos otros lugares (Figura 1.14).

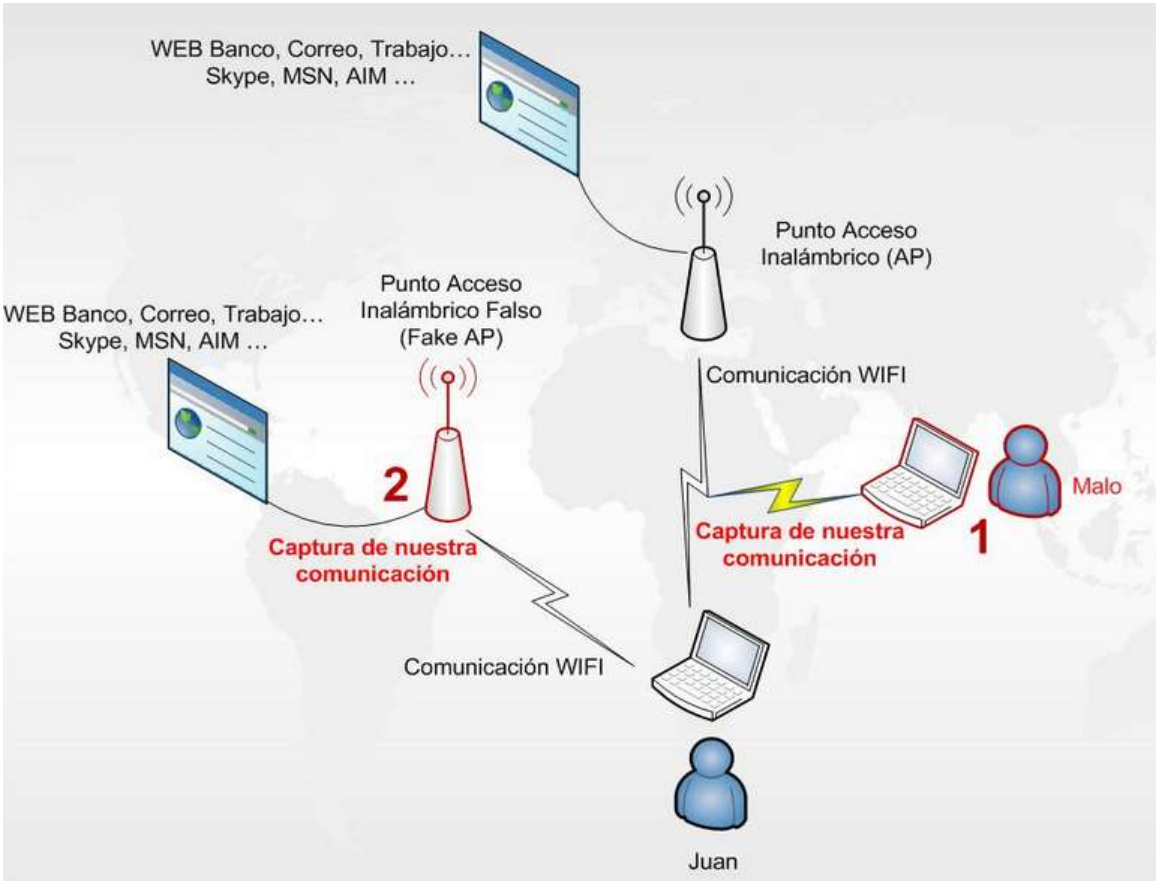


Figura 1.14 Wi-Fi

1.4.2.2 WIMAX

WiMAX Interoperabilidad mundial de acceso por microondas (*Worldwide Interoperability for Microwave Access*) es una tecnología inalámbrica que está basada en estándares, que ofrece conectividad en banda ancha de alta velocidad en hogares y empresas para las redes inalámbricas móviles.

El objetivo de WiMAX es optimizar la infraestructura de acceso y se puede usar para enlaces de larga distancia, destacando por su capacidad como tecnología portadora, sobre la que se puede transportar cualquier tipo de protocolo de comunicaciones, lo que la hace perfectamente adecuada para entornos de grandes redes de voz y datos, así como para el establecimiento de enlaces troncales en redes inalámbricas.

El estándar WiMAX 802.16 define diferentes niveles de calidad de servicio así como el uso de distintos canales de comunicación en un mismo radio enlace físico, posibilitando conexiones de 70 Mbps a una distancia de hasta 50 km a campo abierto.

La tecnología WiMAX ha sido diseñada para complementar a la tecnología Wi-Fi con aquellos aspectos que son relacionados con la transmisión de la señal hasta las proximidades de las ubicaciones de los usuarios (interconexión de Estaciones Base, Radioenlaces, Enlaces punto a punto, etcétera) (Figura 1.15).

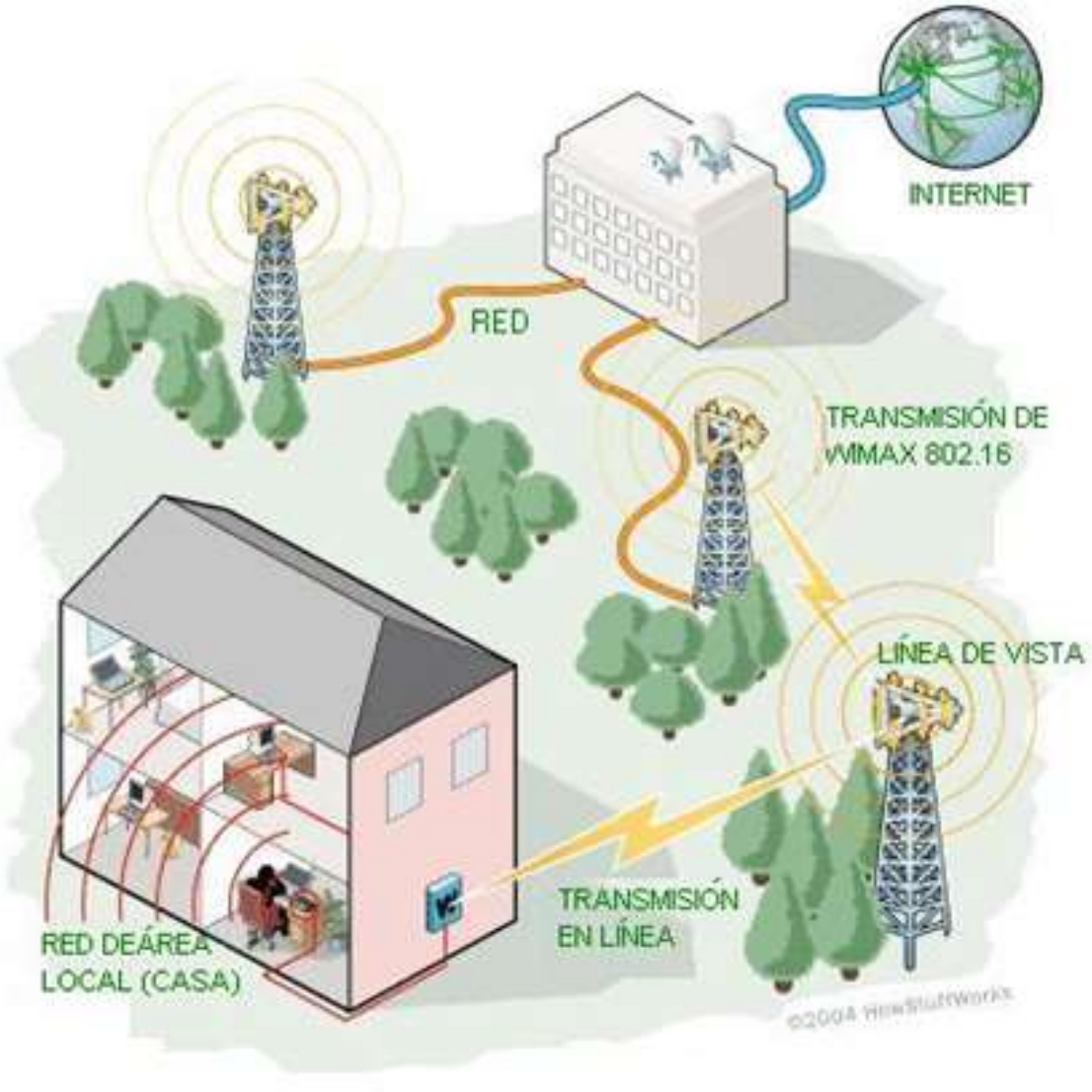


Figura 1.15 WiMAX

1.4.2.3 DIFERENCIAS ENTRE WI-FI Y WIMAX

Después de varios años de hablar de las conexiones Wi-Fi, en miles de sitios públicos y privados ya es una realidad la conexión inalámbrica a internet a través de Wi-Fi.

Sin embargo, estos puntos Wi-Fi tienen aún varias limitaciones, incluyendo un radio de cobertura limitado a unos pocos cientos de metros y sin demasiadas barreras físicas. Ahora estas limitaciones para los usuarios de computadoras portátiles y agendas electrónicas pueden llegar a su fin con WiMAX.

WiMAX o Interoperabilidad mundial de acceso de microondas (Worldwide Interoperability for Microwave Access) es el nombre con el que se conoce la norma 802.16a, un estándar inalámbrico aprobado hace poco en el WiMAX Forum formado por un grupo de 67 compañías, que ofrece un mayor ancho de banda y alcance que la familia de estándares Wi-Fi (compuesta por el 802.11a, 802.11b y 802.11g).

Las diferencias más notables entre estas dos tecnologías inalámbricas (Wi-Fi y WiMAX) son su alcance y ancho de banda.

WiMAX ofrece tasas de transferencia de 124Mbit/s y una cobertura a distancias de entre 40-70 km de una estación base. Por otro lado Wi-Fi ofrece una tasa de transferencia de 11-54 Mbit/s y una cobertura a distancias de 300 metros.

Con WiMAX los usuarios podrán desplazarse mientras tengan acceso de datos de banda ancha o a una sesión de transmisión en tiempo real de multimedia.

Por otro lado WiMAX puede resultar muy adecuado para unir hot spots Wi-Fi a las redes de los operadores sin necesidad de establecer un enlace fijo. De momento no se habla de WiMAX para el acceso residencial, pero en un futuro podría ser una realidad, sustituyendo con enorme ventaja a las conexiones ADSL o de cable y haciendo que la verdadera revolución de la banda ancha llegue a zonas rurales de difícil acceso a las que no llegan las redes cableadas.

CAPÍTULO II

ASPECTOS GENERALES DE WIMAX

2.1 EVOLUCIÓN DE WIMAX

Gracias a su estandarización por IEEE en enero de 2003 en la norma IEEE 802.16, WiMAX ha sentado las bases para la interoperabilidad en el mercado de acceso inalámbrico de banda ancha. WiMAX se impone poco a poco como una tecnología de comunicación inalámbrica de banda ancha capaz de superar las carencias de Wi-Fi.

Con el soporte de movilidad en la próxima especificación IEEE 802.11e, se abre todo un mundo de nuevas posibilidades. Gracias a su estandarización, WiMAX ha sentado las bases para la interoperabilidad en el mercado de acceso inalámbrico de banda ancha. Se trata de una tecnología gestada por la evolución de la familia de estándares Wi-Fi, pero que supera con creces a todos sus predecesores en lo que a ancho de banda, prestaciones y cobertura se refiere. Mientras que Wi-Fi ha sido pensado para proporcionar cobertura sobre áreas relativamente pequeñas, como oficinas o hotspots, WiMAX ofrece alrededor de 70 Mbps a distancias de hasta 48 kilómetros a miles de usuarios desde una única estación base. Además, puede funcionar tanto en bandas licenciadas como no licenciadas, lo que abre enormemente el abanico de sus posibles aplicaciones y al introducir importantes mejoras en prestaciones Non line-of-sight (Fuera de la línea de visión) resulta una tecnología apta para entornos donde existan obstáculos, como árboles o edificios.

Todas estas prestaciones y ventajas convierten a WiMAX en una alternativa atractiva tanto por su rendimiento como por su bajo costo, no sólo en la empresa, sino también en el segmento de operadores. Con un ancho de banda máximo teórico de 75 Mbps en la versión fija

(802.16d), aprobada en septiembre de 2004, la tecnología permite distribuir servicios de banda ancha con la calidad habitualmente requerida para soportar las aplicaciones empresariales más exigentes y sensibles a la latencia, como voz sobre IP o videoconferencia. En el hogar representa un medio idóneo para integrar en un único enlace el suministro de servicios triple play (voz, vídeo, datos e incluso televisión).

La creación de backhaul (conexión entre estaciones base y estaciones controladoras) de datos de alta velocidad en redes móviles GSM o UMTS es una de las aplicaciones de WiMAX móvil (802.16e), que será aprobado este año por IEEE. Una red WiMAX resulta mucho más barata de desplegar que una red UMTS. Cuando lo que se pretende es crear un backhaul el costo se puede ver reducido hasta en un 90%. Estos tramos de las infraestructuras móviles tienden a saturarse por el incremento de tráfico de datos derivado de los servicios 2.5G y 3G. Los operadores necesitan un backhaul nuevo, de bajo costo y eficiente y que aporte elevados anchos de banda. Para resolver la necesidad del backhaul inalámbrico, WiMAX es la tecnología adecuada para tal solución.

Otra aplicación especialmente interesante de WiMAX móvil en la infraestructura de los operadores consiste en la superposición de celdas en despliegues UMTS. De esta forma, el soporte de tráfico IP se ve reforzado en zonas donde la cobertura es deficiente o el ancho de banda insuficiente. Representa, una alternativa válida al ADSL, permitiendo llevar la banda ancha a zonas rurales o de difícil acceso e incluso facilitando la entrada en el mercado de nuevos proveedores de

servicios en competencia con los propietarios de licencias GSM o 3G. La evolución de WiMAX se puede ver desde dos puntos de vista:

1) Empresa

En la empresa, el abanico de aplicaciones es igualmente amplio. Al tratarse de una tecnología de IP es susceptible a convertirse en el soporte de la integración de todos los servicios corporativos, incluida la voz sobre IP inalámbrica. Aquí se encuentra precisamente otra de sus aplicaciones más interesantes, dado que resuelve los dos principales inconvenientes que han disuadido a muchas empresas de adoptar la telefonía IP sobre Wi-Fi: la seguridad y la calidad. Una de las diferencias más importantes entre Wi-Fi y WiMAX radica precisamente en que la primera no soporta calidades de servicio (QoS), no fue ideada para la transmisión de voz. WiMAX, por el contrario, contempla esta posibilidad desde su origen. Es una tecnología pensada desde cero para entornos `todo IP´. Incorpora QoS y además, al implementar una modulación mucho más compleja que Wi-Fi (Scalable OFDMA- Orthogonal Frequency Division Multiplexing- Multiplexación de División de Frecuencia Ortogonal), hace virtualmente impracticables las temidas escuchas. Puede decirse que ofrece niveles de seguridad equivalentes a GSM y a UMTS.

En cuanto a su lugar en los entornos corporativos, WiMAX es tan flexible como lo es en posibles aplicaciones. El usuario utiliza WiMAX para el transporte a nivel WAN, combinado con Wi-Fi o cualquier tecnología cableada para distribuir internamente en la red de área local. Pero también puede optar por desplegar WiMAX tanto en el acceso WAN

como a nivel LAN, en aquellos casos en que las necesidades de movilidad, ancho de banda, soporte QoS y seguridad compensen su mayor costo.

2) Principios confusos

Probablemente, una de las claves para explicar por qué, pese a todos los beneficios de esta nueva tecnología, aún no existen en el mercado productos certificados para el estándar, se encuentre en la bifurcación de la norma original, dando lugar a dos especificaciones diferentes y, por el momento, incompatibles entre sí. La aparición de IEEE 802.16e, la iniciativa de estandarización más reciente y aún no aprobada como especificación, coincidió prácticamente en el tiempo con la ratificación de IEEE 802.16d o WiMAX fijo, alternativa que ofrece, acceso inalámbrico fijo. No soporta, sin embargo, el mantenimiento de la sesión de usuario mientras éste se mueve de un área de cobertura a otra. La segunda variante, IEEE 802.16e, añade soporte de movilidad, una característica especialmente interesante en un entorno inalámbrico, facilitando comunicación entre celdas sin interrupción de la sesión y de forma transparente para el usuario, siempre que su movimiento no supere la velocidad de vehículo (entre 120 y 140 Km/h). Sin embargo, la iniciativa para el desarrollo de esta nueva versión ha generado confusión en un mercado todavía incipiente, haciendo que muchos fabricantes y potenciales usuarios retrasen sus decisiones al respecto hasta la aparición de la nueva alternativa y comprobar la evolución y aceptación de ambas versiones.

Algunos fabricantes, sin embargo, han tenido clara desde un principio su estrategia respecto a WiMAX.

"El WiMAX Forum afirma que el número de usuarios conectados a las **redes WiMAX** es de 430 millones de personas y se espera que se duplique a 800 millones de personas a finales de 2010. Las redes WiMAX se están acercando a 460 en más de 135 países para fijos, portátiles y redes móviles."[1] (Figura 2.1)

Figura 2.1 Evolución de WiMax [1]

[1] *wimax*. (2010). Obtenido de wimax: http://www.islabit.com/2912/wimax-forum-espera-duplicar-el-numero-de-usuarios-wimax-a-finales-de-2010.html

2.2 ESTANDARIZACIÓN

El estándar WiMAX está diseñado teniendo en cuenta las cuestiones relacionadas con la seguridad y ofrece una protección más sólida mediante el cifrado basado en certificados.

No es una tecnología demasiado nueva, sino que es la estandarización de la última y más reciente tecnología de acceso radio OFDM (Orthogonal Frequency Division Multiplexing) de banda ancha. Así, se trata de un sistema pensado para proporcionar servicios triple play, de voz, vídeo y datos, con calidad de servicio independientemente de si se opera en banda regulada o banda libre.

En este sentido, WiMAX es la solución más efectiva y económica para suministrar banda ancha a escala universal. La estandarización cambia la situación del mercado BWA (Broadband Wireless Access- Acceso Inalámbrico De banda ancha), convirtiéndose en un mercado masivo, aportando todos los beneficios económicos que acompañan a un producto dirigido al mercado de masas. De igual modo, a largo plazo, WiMAX permitirá eliminar la barrera permanente para ofrecer acceso de banda ancha a millones de usuarios potenciales de mercados a los que es difícil llegar o que cuentan con un servicio pobre en todo el mundo.

WiMAX ofrece equipamiento de banda ancha inalámbrica lo que significa:

a) Menor precio en el equipamiento para proveedores de servicio y operadores, lo que permite a los operadores poner en marcha redes inalámbricas ya sea en banda libre o licenciada, para suministrar servicios en áreas en las que el despliegue con anterioridad ha sido inviable por cuestiones económicas.
b) Interoperabilidad, lo que derivará en su momento en productos plug-and-play. Los proveedores de servicios serán capaces de combinar equipamiento de otros muchos proveedores de soluciones, asegurándose la compatibilidad.

En su evolución, WiMAX da el mayor salto sobre Wi-Fi, proporcionando conectividad de banda ancha en la última milla sobre un área geográfica significativamente más extensa, abarcando un radio de más de diez kilómetros y ofreciendo características estables, cumpliendo de forma rigurosa los requerimientos de los operadores en una amplia variedad de escenarios de despliegue.

Es importa saber cómo está la estructura de una red WiMAX para verificar cuál es el alcance de ésta.

Las Redes de Área Metropolitana WiMAX (Wimax MAN) se configuran de modo celular y generalmente constan de una celda o de un grupo de celdas, cada una de las cuales contiene varias terminales inalámbricas (también conocidas como unidades de abonado o CPE). A su vez, cada celda consta de uno o más dispositivos de Unidad de Acceso (estaciones base) que normalmente están conectadas al backbone y las cuales gestionan todo el tráfico dentro del área cubierta y entre dicha área y el backbone de la red.

Las terminales dentro del área de alcance de una unidad de acceso se conectan al backbone de la red a través de la unidad de acceso. Todas las terminales asociadas con una estación base están sincronizadas, tanto por frecuencia y tiempo, y utilizan un protocolo riguroso para comunicarse con la unidad de acceso. La misma regla se aplica para un dispositivo de intercepción, para que los datos sean interceptados, un dispositivo inalámbrico (wireless) debe ser empleado y sincronizado dentro del área cubierta por la unidad de acceso.

Como cualquier otra red de comunicación al servicio de empresas y usuarios individuales que desean mantener su información segura, los sistemas WiMAX necesitan aplicar medidas para asegurar la privacidad de sus usuarios finales y prevenir del acceso a información confidencial o sensible a personas que no están autorizadas.

Desde que los sistemas WiMAX utilizan la interfaz de radio como medio de transmisión, la pregunta que conviene hacerse es ¿cómo prevenir que los intrusos no intercepten información sensible y confidencial transmitida por ondas hertzianas ya sea en banda libre o banda licenciada? Tanto los clientes como los operadores deberían sentirse protegidos y confiar en que su sistema es privado y seguro, y que las medidas apropiadas están disponibles para minimizar los riesgos de seguridad, incluyendo (Figura 2.2):

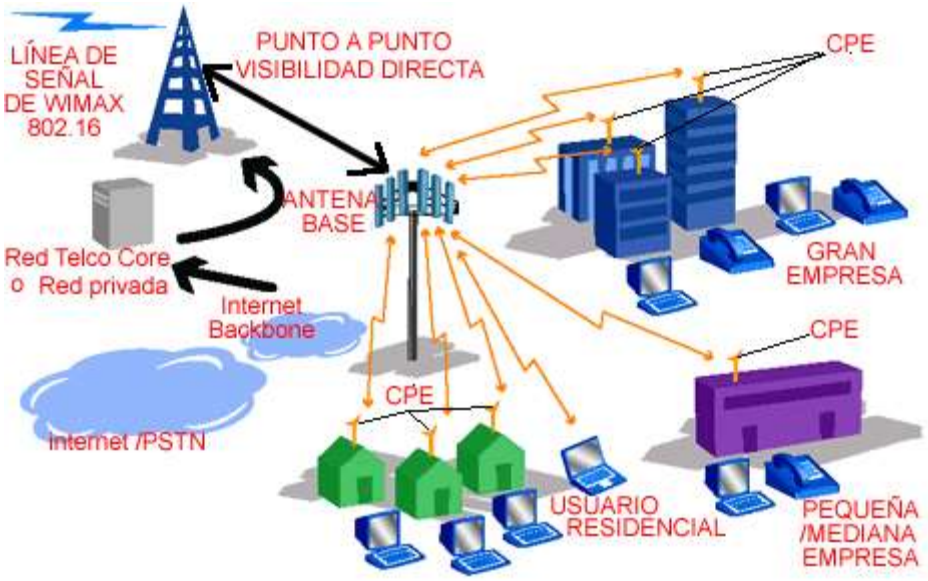


Figura 2.2 Estructura de una red WiMax [2]

a) Escuchas/espionaje: interceptar información de forma intencional cuando se está transmitiendo.
b) Privacidad: Asegurarse de que la información transmitida es solamente leída por los destinatarios a los que va dirigida.
c) MAC Spoofing: evitar que un atacante copie las direcciones MAC de CPE legítimas con el fin de conseguir el acceso a la red.
d) Robo del Servicio: prevenir que los agresores puedan acceder a Internet u otros servicios utilizando CPE robadas y advirtiendo a los usuarios legítimos de obtener los servicios de forma gratuita.

[2] Sánchez, O. A. (Noviembre de 2011). *Comparación de la eficiencia volumétrica entre redes inalámbricas Wi-Fi y WiMax*. Obtenido de http://132.248.9.195/ptb2011/noviembre/0674882/0674882_A1.pdf

El estándar WiMAX requiere de las mejores características de seguridad en su clase, esto se ha logrado gracias a la adopción de las mejores tecnologías disponibles actualmente. Las características de seguridad son independientes al tipo de operador (ILEC -Incumbent Local Exchange Carrier - Portador encargado local de cambio o CLEC - Competitive Local Exchange Carrier - Portador competitivo local de cambio) y a la topología de la red de acceso. En este sentido, el estándar aborda las cuatro áreas principales a tener en cuenta: cómo prevenir el uso clandestino de la conexión inalámbrica; denegación de servicios para unidades robadas o utilizadas de forma fraudulenta; suministrar servicios sólo a los usuarios finales específicos; y cumplir con la gestión de acceso seguro.

Respecto a cómo prevenir la utilización clandestina de la conexión inalámbrica, la clave está en el cifrado.

La seguridad WiMAX soporta dos estándares de cifrado de calidad, DES3 y AES, que es considerado tecnología de vanguardia. Básicamente, todo el tráfico en redes WiMAX debe ser cifrado empleando el protocolo modo contador con código de autenticación de mensaje del bloque cifrado encadenado(Counter Mode con Cipher Block Chaining Message Authentication Code Protocol CCMP) que utilizan AES para transmisiones seguras y autenticación de la integración de datos.

La autenticación end-to-end de la metodología PKM-EAP (Protocolo de Autenticación Extensible) es utilizada de acuerdo con el estándar TLS de encriptación de clave pública.

El estándar define un proceso de seguridad dedicada en la estación base para los principiantes. Del mismo modo, también hay unos requerimientos de cifrado mínimos para el tráfico, así como para la autenticación end-to-end.

En relación al suministro de servicios sólo a los usuarios finales específicos, la autenticación -basada en certificados digitales X.509- es incluida en la capa de control de acceso a los medios y da a cada usuario 802.16 receptor su propio certificado incorporado, más otro para el fabricante, permitiendo a la estación base autorizar al usuario final. La privacidad de la conexión es implementada como parte de otro subnivel MAC, la capa de privacidad. Ésta se basa en el protocolo Privacy Key Management (clave privada de administrador) que es parte de la especificación DOCSIS BPI.

El estándar WiMAX tiene muchas más funcionalidades de seguridad incorporadas que un sistema Wi-Fi.

Como en otros estándares, los fabricantes se ven beneficiados por las múltiples ventajas, si bien las mejoras que diferencian un producto determinado o el trabajo, deben retroalimentarse en los procesos de estándares (Figura 2.3).

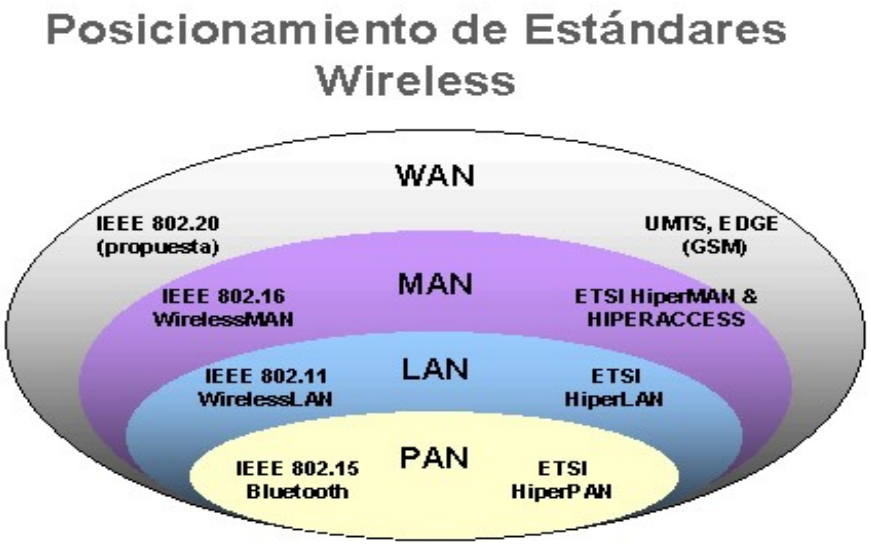


Figura 2.3 Estandarización [3]

[3] Sánchez, O. A. (Noviembre de 2011). *Comparación de la eficiencia volumétrica entre redes inalámbricas Wi-Fi y WiMax*. Obtenido de http://132.248.9.195/ptb2011/noviembre/0674882/0674882_A1.pdf

2.3 CARACTERÍSTICAS DE WIMAX

Las características principales de esta red inalámbrica WiMAX son las siguientes:

a) Esta red inalámbrica define una capa MAC que soporta múltiples especificaciones físicas (capa física).

b) Tiene una mayor productividad en rangos más distantes (hasta 50 Km.)

c) Mejor tasa de bits/segundo/HZ en distancias largas, de hasta 70 Mbps

d) Cuenta con un sistema escalable

e) Cuenta con una fácil adición de canales: puede maximizar las capacidades de las células.

f) Tiene ancho de banda flexible que permite usar espectros licenciados y exentos de licencia.

g) Tiene una cobertura más amplia

h) Puede soportar mallas basadas en estándares y antenas inteligentes.

i) Cuenta con un soporte nativo para la calidad de servicio de QoS

j) Tiene un servicio de niveles diferenciados: E1/T1 para negocios, que tenga una mejor capacidad para el uso doméstico.

k) Tiene un costo y riesgo de investigación.

WiMAX cuenta con diferentes tipos que se pueden utilizar de acuerdo con las necesidades:

i. Fijo

Utiliza una antena que se coloca en un lugar estratégico del suscriptor. También se ocupa en instalaciones de interiores, en cuyo caso no necesita ser tan robusto como al aire libre.

Es una solución inalámbrica para acceso a Internet de banda ancha que provee una solución de clase ínter operable de transportador para la última milla. WiMAX cuenta con un acceso fijo que funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y las líneas digitales de suscriptor de cualquier tipo (xDSL).

ii. Móvil

Para obtener esta modalidad se usa un Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), lo cual es similar a OFDM en que divide las subportadoras múltiples. OFDMA, sin embargo, va un paso más allá agrupando subportadoras múltiples 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.

En la tabla 2.1 se observa la comparación que hay entre las diferentes redes inalámbricas

2.1 Comparativa de WiMAX frente a otras tecnologías

	WI-MAX 802.16	WI-FI 802.11	MOBILE-FI 802.20	UMTS Y CDMA 2000
Velocidad	124 Mbit/s	11 – 54 Mbit/s	16 Mbit/s	2 Mbit/s
Cobertura	40 – 70 km	300 m	20 km	10 km
Licencia	Sí/No	No	Sí	Sí
Ventajas	Velocidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Mobilidad
Desventajas	Interferencias	Bajo alcance	Precio alto	Lento y caro

2.4 COBERTURA DE TRANSMISIÓN

WiMAX tiene una cobertura de transmisión con radio de acción de hasta 50 kilómetros. Esta tecnología funciona de forma muy parecida a Wi-Fi pero con tres diferencias básicas: mayor distancia, más usuarios y más ancho de banda, facilitando la creación de redes de área metropolitana (MAN).

La tecnología 802.16, o WiMAX funciona de manera muy similar a la telefonía celular. El principal componente es una antena colocada en una torre con una cobertura de hasta 7500 kilómetros cuadrados. El segundo elemento es el receptor WiMAX, que puede ir desde una caja colocada en el techo de la casa, hasta algo tan pequeño como una tarjeta PCMCIA en una computadora portátil.

Una antena WiMAX estará conectada al proveedor de Internet (ISP) por medio de fibra óptica o cable con un alto ancho de banda (30 Mbps o más) y esa misma antena, en el modelo de la telefonía celular, podrá ser el punto de acceso a la red tanto de usuarios móviles como de otras antenas funcionando como repetidoras, sin conexión por cable alguno. De esta forma, la tecnología WiMAX permite enlazar zonas rurales o de difícil acceso, donde las compañías de telecomunicaciones no han colocado cables por el costo de instalación o mantenimiento.

Parte fundamental de la cobertura, estabilidad e impacto de WiMAX radica en la frecuencia de transmisión. Existen dos alternativas:

1. Cuando el equipo del usuario se encuentre en una zona con varios obstáculos (edificios, árboles, cerros, etcétera) se podrá usar una

baja frecuencia, en el orden de los dos a 11 GHz. Estas frecuencias son menos susceptibles a la pérdida del enlace por algún objeto que se interponga entre la antena WiMAX y el dispositivo del usuario. El precio por pagar para mantener la conectividad, es que el ancho de banda también será inferior a los 54 Mbps.

2. Si existe línea de vista, es decir, cero obstáculos entre la antena WiMAX y el equipo del usuario, se opta por una mayor frecuencia, hasta 66 GHz, con el considerable incremento en el ancho de banda. La norma 802.16 establece un tope de 70 Mbps.

A partir de las variaciones en el uso de frecuencias, es claro determinar que equipos de mayor capacidad, como es el caso de los ruteadores, preferentemente están asociados a una conexión de alta frecuencia con las antenas WiMAX; y los equipos de mayor movilidad, como las computadoras portátiles, seguirán asociándose a redes Wi-Fi o WiMAX en menores frecuencias y anchos de banda.

WiMAX es una estupenda oportunidad para ampliar los servicios de telecomunicaciones a nivel gubernamental, empresarial e institucional. Una universidad puede proporcionar acceso a la red en todo su campus con una sola antena, a la suficiente altura y ubicación. Los gobiernos pueden respaldar los actuales esquemas de comunicación de datos por medios alámbricos, usando celdas WiMAX ubicadas de manera estratégica en zonas de acceso controlado. En el ámbito social, la combinación de Wi-Fi, WiMAX y la telefonía por IP (VoIP) permite el despliegue de más líneas de telecomunicaciones hacia zonas

apartadas, con ancho de banda suficiente para la integración de servicios multimedia: voz, imagen y datos. (Figura 2.4)

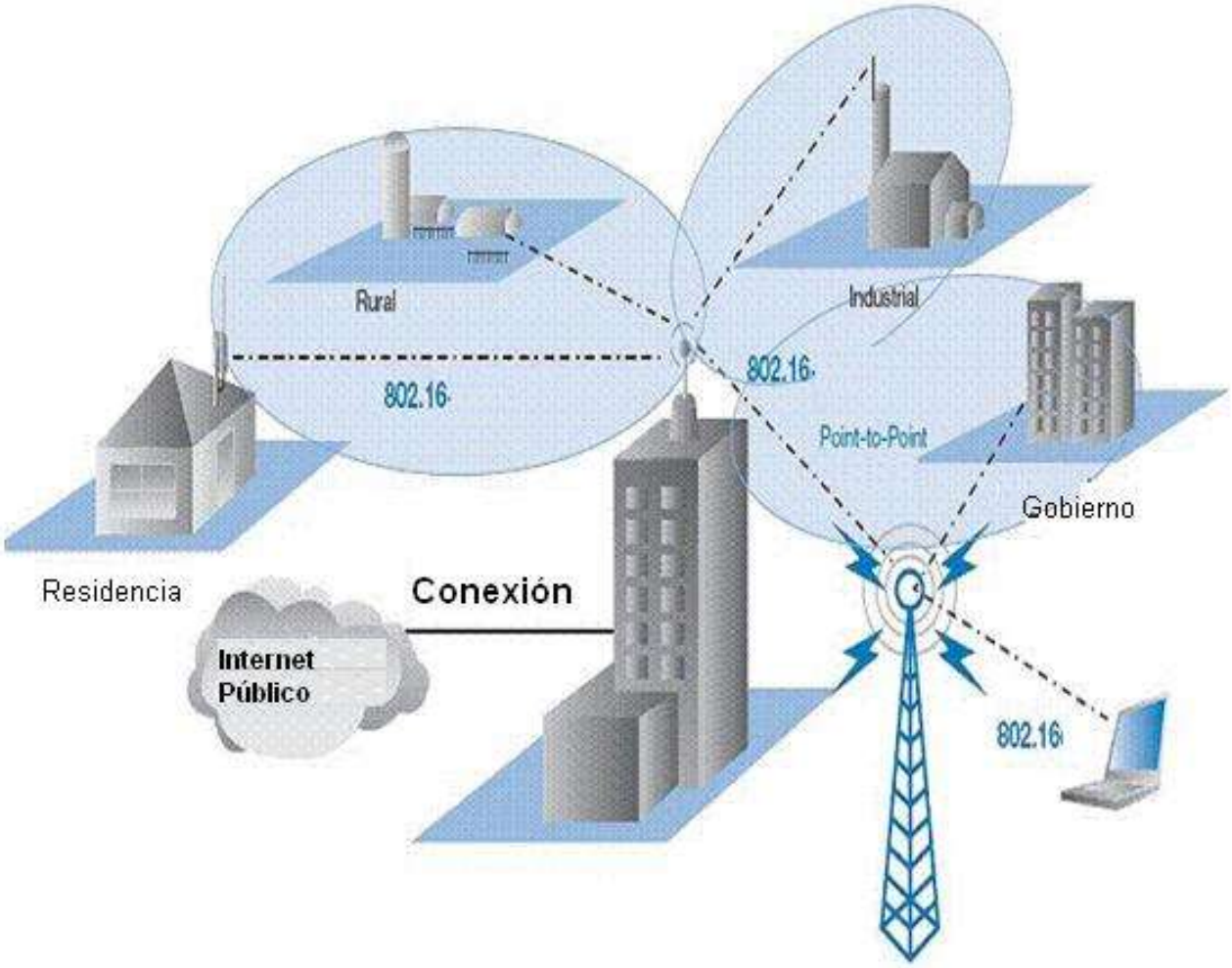


Figura 2.4 Cobertura de Transmisión [4]

[4] *Cobertura de transmisión*. (s.f.). Obtenido de https://www.google.com.mx/search?q=Estructura+de+una+red+WiMAX/BWA.&espv=2&biw=1309&bih=705&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiR1Onyz5bNAhVpxoMKHfvIAD4Q_AUIBigB#imgrc=_XLZvqkwkt0eIM%3A

2.5 TIPO DE TRANSMISIÓN

Con todas estas revisiones y mejoras adoptadas por el estándar se pueden determinar beneficios que este tipo de red provee a sus usuarios:

1) Gran cobertura

En ambientes LOS hasta 50 Km; para ambientes NLOS hasta 8 Km

2) Alta capacidad de transferencia de bits

Idealmente la red es capaz de transferir datos a 70 Mbps

3) Soporte para ambientes NLOS

En las frecuencias indicadas es posible implantar una red bajo el estándar sin tener línea de vista.

4) Tamaño flexible de canales

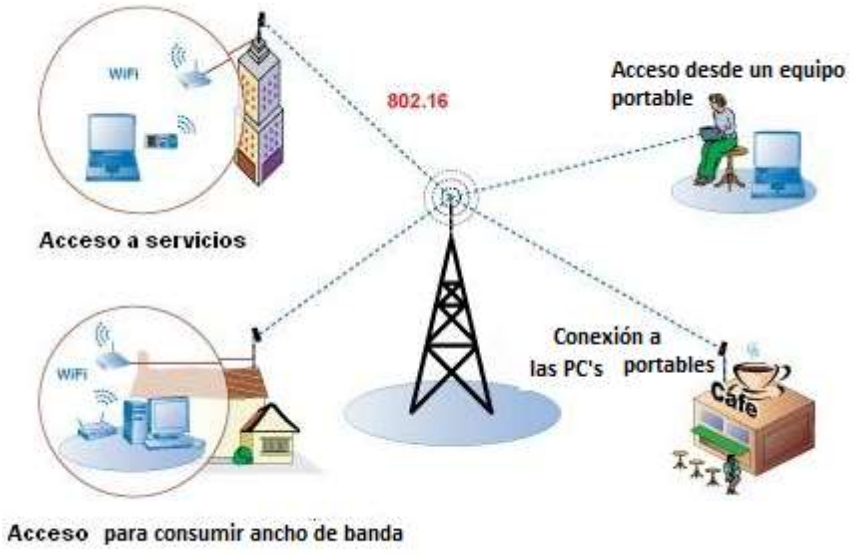
Ésta es una prestación muy importante ya que se puede configurar el ancho de los canales de comunicación optimizando así su uso y evitando el desperdicio de recursos de red.

5) Soporte para redes en malla

Esta opción permite a las ES (estación del suscriptor) hacer enrutamiento entre unas y otras sin pasar por la EB (estación base) haciendo esta función transparente a ella.

Soporte para usuarios móviles.

Una ES puede tener acceso a la red moviéndose a una velocidad vehicular. Esto da a la ES la posibilidad de tener servicio usando dispositivos móviles. (Figura 2.5)



2.5 Tipo de Transmisión [5]

[5] Sánchez, O. A. (Noviembre de 2011). *Comparación de la eficiencia volumétrica entre redes inalámbricas Wi-Fi y WiMax*. Obtenido de http://132.248.9.195/ptb2011/noviembre/0674882/0674882_A1.pdf

2.6) MARCO REGULATORIO Y BANDAS DE FRECUENCIA

WiMAX abarca un rango de espectro debajo de 11GHz. Asimismo, existe la posibilidad de desplegar WiMAX en las bandas del servicio celular y en las bandas de 700MHz. A pesar de la supuesta abundancia de espectros, algunos de estos espectros disponibles presentan sus propios problemas.

Además, una amplia variedad de opciones de espectros también tiene como resultado la incompatibilidad o la necesidad de dispositivos multibanda.

Dentro de este rango de frecuencias, el espectro más probable está disponible en 2.3GHz, 2.4GHz, 2.5GHz, 3.5GHz, 5.8GHz y, potencialmente, en 700MHz. Por consiguiente, para asegurar la interoperabilidad mundial, los CPE, tarjetas de datos o soluciones con chips incorporados de WiMAX deberían soportar hasta 5 bandas de frecuencia.

El espectro disponible se divide en dos categorías distintivas:

A) Sin licencia
B) Con licencia

2.6.1) CON LICENCIA

El espectro que requiere licencia tiene un potencialmente alto, en especial cuando la oferta del servicio requiere una alta calidad de servicio. La mayor ventaja de tener el espectro que requiere licencia es que el licenciatario tiene uso exclusivo del espectro.

Está protegido de la interferencia externa, el espectro que requiere licencia se encuentra en 700MHz, 2.3GHz, 2.5GHz y 3.5GHz; de éstas, las últimas dos bandas de frecuencia son las que en la actualidad reciben mayor atención.

2.6.2) SIN LICENCIA

El espectro que no requiere licencia y que podría emplearse para WiMAX es 2.4 GHz y 5.8 GHz.

Debido a que el espectro no requiere licencia, la barrera para ingresar es baja, por lo que hace más fácil que un posible operador comience a ofrecer servicios empleando el espectro, esto puede tener beneficios.

En Europa rige el concepto de espectro con licencia, lo que significa que el usuario tiene que presentar su intención de usar el espectro que no requiere licencia. De esta forma, los entes reguladores tienen una mejor noción de quién está empleando el espectro, y controlan la cantidad de licenciatarios y minimizan potencialmente el impacto de interferencias.

Hay cuatro desventajas principales relacionadas con el uso del espectro que no requiere licencia.

a. Interferencias

Debido a que el espectro que no requiere licencia, puede ser utilizado por varios sistemas diferentes de RF (Sistema de radio frecuencia con el control de inventarios), hay altas probabilidades de que ocurran interferencias.

Los sistemas de RF que no requieren licencia pueden incluir desde las redes rivales de WiMAX o los puntos de acceso de Wi-Fi. Los teléfonos inalámbricos y Bluetooth (sólo 2.4GHz) también usan este espectro. Tanto WiMAX como Wi-Fi soportan la Selección Dinámica de Frecuencia (DFS - Dynamic Frequency Selection) que permite que se utilice un nuevo canal si fuera necesario (por ejemplo, cuando se detectan interferencias). No obstante, DFS también puede introducir una mayor latencia que a su vez afecta las aplicaciones en tiempo real como VoIP.

a. Mayor competencia

Los operadores que utilizan el espectro que no requiere licencia tienen que asumir que otro operador fácilmente podría ingresar en el mercado empleando el mismo espectro. En gran medida, el número relativamente alto de puntos de acceso públicos Wi-Fi se debe a este hecho. No obstante, los gastos de capital relacionados con la instalación de un punto de acceso Wi-Fi de carácter comercial son relativamente triviales (cientos de dólares) en comparación con el costo relacionado con desplegar una red WiMAX, que podría ser equivalente al costo de desplegar una red celular.

b. Potencia limitada

Otra desventaja del espectro que no requiere licencia es que los entes reguladores del gobierno por lo general limitan la cantidad de potencia que puede transmitirse. Esta limitación es especialmente importante en 5.8GHz, donde la mayor potencia podría compensar la pérdida de propagación relacionada con el espectro en frecuencias más altas.

c. Disponibilidad

Mientras el espectro de 2.4 GHz está disponible universalmente, en la actualidad el espectro 5.8 GHz no se encuentra disponible en varios países.

Dadas estas desventajas, el espectro no requiere licencia, en particular 2.4 GHz, antes de instalar una red. Hay excepciones, entre las que se incluyen las regiones rurales o remotas, donde hay menos probabilidades de interferencia y competencia.

En México el Instituto Federal de Telecomunicaciones (IFT), que es el órgano encargado de regular el sector de las telecomunicaciones, tiene establecido ciertas características para la operación de los equipos de radiocomunicación que empleen las bandas de uso libre (esto es, sin licencia) de los 2450 MHz (2400 a 2483.5), 5800 MHz (5725 a 5850) y 915 MHz (902 a 928). Algunas de las principales características, que se indican en tablas, son las que se mencionan a continuación:

A.- En relación a la Potencia Isótropa Radiada Equivalente (PIRE) máxima que se debe manejar en la transmisión de acuerdo a la banda de operación, ésta se muestra en la tabla 2.2

Tabla 2.2 PIRE Máximo

Banda de Frecuencias (MHz)		PIRE Máxima (watt)
902-928		4
2 400-2 483.5	Sistemas fijos punto a punto	2
	Sistemas punto a multipunto	1
5 725-5 850		4

B.- Para equipos de comunicación que emplean técnicas de espectro disperso de salto de frecuencia, de tal manera que puedan operar en las anchuras de banda a 20 [dB] en el canal del sistema, se tienen algunas condiciones adicionales que deben cumplir como se indica la tabla 2.3

Tabla 2.3 Especificaciones para los equipos del tipo salto de frecuencia

Banda (MHz)	Anchura de banda del canal de salto a 20 dB ($AB20_{dB}$)	Número de canales de salto (N)	Tiempo promedio de ocupación (t) de canal de salto por periodo [s]	Periodo de ocupación del conjunto de saltos (T) [s]	Potencia pico máxima de salida [W]
902-928	< 250 kHz	≥ 50	≤ 0.4	20	1
	≥ 250 kHz (máximo permitido: 500 kHz)	25 ≤ N < 50	≤ 0.4	10	0.25
		≥ 50	≤ 0.4	10	1.0
2 400-2483.5	Sin especificación	≥ 75, no traslapados	≤ 0.4	(0.4 s) (N)	1.0
	Sin especificación	≥ 15	≤ 0.4	(0.4 s) (N)	0.125
5 725-5 850	≤ 1 MHz	≥ 75	≤ 0.4	30	

C.- En las tablas que a continuación se muestran, se mencionan las especificaciones generales para el uso de las bandas de frecuencias de uso libre (o sin licencia) en cuestión:

Tabla 2.4 Frecuencia de 2,400 a 2,483.5 [MHz] [6]

UHF (Ultra High Frequency, 'frecuencia ultra alta')

Segmento de frecuencias	**2400.0000 - 2483.5000 MHz**
Atribución internacional	• 2300-2450 MHz FIJO, MOVIL, RADIOLOCALIZACIÓN, Aficionados • 2450-2483 MHz FIJO, MÓVIL, RADIOLOCALIZACIÓN Notas RR 5.150 5.282 5.393 5.396
Atribución nacional	• 2360-2450 MHz FIJO, MÓVIL, RADIOLOCALIZACIÓN, Aficionados • 2450-2483.5 MHz FIJO, MÓVIL Nota CNAF MEX102
Resumen técnico	• La potencia máxima de transmisión entregada a las antenas de sistemas de radiocomunicación fijos en enlaces punto a punto no deberá exceder los 500 mW ○ La ganancia direccional máxima de la antena se recomienda que sea de 6 dBi de manera que la Potencia Isotrópica Radiada Equivalente (PIRE) máxima no exceda los 2 W • La potencia máxima de transmisión entregada a las antenas por los sistemas de radiocomunicación en enlaces punto a multipunto no deberá exceder los 250 mW ○ Se puede utilizar cualquier tipo de antena de transmisión con ganancia direccional máxima recomendada de 6 dBi de manera que la a Potencia Isotrópica Radiada Equivalente máxima no sea mayor de 1 W • En ambos casos, si se utilizan antenas con ganancia direccional mayor a 6 dBi, la potencia máxima de transmisión de entrada de las mismas deberá ser modificada reduciéndola en la misma proporción que la ganancia direccional exceda los 6 dBi • En caso de ser un dispositivo de radiocomunicación de corto alcance, la intensidad de campo eléctrico no deberá exceder de 200 µV/m, medida a una distancia de 3 metros
Referencia normativa	Acuerdo SCT 130306, DOF 13/03/2006

[6] (28 de 12 de 2016). Obtenido de Inventario de Bandas de Frecuancia de uso libre: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjDkrTJ9JnRAhUr94MKHYrUCdgQFgggMAE&url=http%3A%2F%2Fwww.ift.org.mx%2Fsites%2Fdefault%2Ffiles%2Fcontenidogeneral%2Fespectro-radioelectrico%2Fespectro-de-uso-libre-vf.doc&usg=AFQjC

Tabla 2.5 Frecuencia 5,725 a 5,850 [MHz] [7]

SHF (Super High Frequency, frecuencia super alta)

Segmento de frecuencias	**5725.0000 - 5850.0000 MHz**
Atribución internacional	• 5725-5830 MHz RADIOLOCALIZACIÓN, Aficionados • 5830-5850 MHz RADIOLOCALIZACIÓN, Aficionados, Aficionados por satélite (espacio-Tierra) Nota RR 5.150
Atribución nacional	• 5725-5830 MHz RADIOLOCALIZACIÓN, Aficionados • 5830-5850 MHz RADIOLOCALIZACIÓN, Aficionados, Aficionados por satélite (espacio-Tierra) Nota CNAF MEX102
Resumen técnico	• La potencia máxima de transmisión entregada a las antenas no deberá de exceder de 1W • La ganancia directiva de las antenas se recomienda que sea de 6 dBi de tal manera que la Potencia Isotrópica Radiada Equivalente (PIRE) máxima no exceda los 4 W • Densidad PIRE: 200 mW/MHz (23 dBm/MHz) en cualquier banda de 1 MHz • Si se utilizan antenas de ganancia direccional mayor a 6 dBi, la potencia máxima de entrada a las mismas y la correspondiente densidad de PIRE deberán ser reducidas en la misma proporción que la ganancia direccional exceda los 6 dBi • Todas las emisiones dentro de un rango de 10 MHz fuera de los extremos inferior y superior de la banda, no deberá exceder una densidad de PIRE de -17dBm/MHz; para frecuencias a partir de 10 MHz fuera de esos rangos, las emisiones no deberán de exceder una densidad de PIRE de -27dBm/MHz
Referencia normativa	Acuerdo SCT 150306, DOF 14/04/2006

[7] (28 de 12 de 2016). Obtenido de Inventario de Bandas de Frecuancia de uso libre: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjDkrTJ9JnRAhUr94MKHYrUCdgQFgggMAE&url=http%3A%2F%2Fwww.ift.org.mx%2Fsites%2Fdefault%2Ffiles%2Fcontenidogeneral%2Fespectro-radioelectrico%2Fespectro-de-uso-libre-vf.doc&usg=AFQjC

Tabla 2.6 Frecuencia 902 a 928 [MHz] [8]

UHF

Segmento de frecuencias	**902.00000-928.00000 MHz**
Atribución internacional	FIJO, Aficionados, Móvil salvo móvil aeronáutico y Radiolocalización Nota RR 5.150
Atribución nacional	FIJO, MÓVIL, Aficionados Nota CNAF MEX102
Resumen técnico	• La potencia máxima de transmisión entregada a las antenas: no mayor a 1 W • La máxima ganancia direccional de antenas de transmisión se recomienda que sea de 6 dBi, de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 4 W • Si la ganancia direccional de la antena es mayor a 6 dBi, la potencia máxima de transmisión a la entrada de la mismas deberá ser reducida en la misma proporción que la ganancia direccional exceda los 6 dBi • En caso de ser un dispositivo de radiocomunicación de corto alcance, la intensidad de campo eléctrico no deberá exceder de 200 µV/m, medida a una distancia de 3 metros
Referencia normativa	Acuerdo SCT 130306, DOF 13/03/2006

[8] (28 de 12 de 2016). Obtenido de Inventario de Bandas de Frecuancia de uso libre: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjDkrTJ9JnRAhUr94MKHYrUCdgQFgggMAE&url=http%3A%2F%2Fwww.ift.org.mx%2Fsites%2Fdefault%2Ffiles%2Fcontenidogeneral%2Fespectro-radioelectrico%2Fespectro-de-uso-libre-vf.doc&usg=AFQjC

2.6.3) COMPARACIÓN CON LA TECNOLOGÍA WI-MAX CON LICENCIA Y SIN LICENCIA

En todo el mundo se reconoce el valor de las innovaciones que están asociadas a los estándares abiertos y las soluciones que pertenecen a las de sin licencia ya han establecido las bandas de frecuencia disponibles para el uso de las tecnologías de WiMAX.

En cambio, para que se imponga algún tipo de control sobre dichas soluciones se debe disminuir el potencial de la interferencia, se tienen que estipular algunos requisitos para la potencia de las operaciones tanto de alta como de baja potencia.

Para cada región geográfica se regulan sus propias bandas tanto de con como de sin licencias, que permiten a los proveedores usar todos los espectros disponibles dentro de estas banda.

En la tabla 2.7 se describen cómo son usadas las bandas en las diferentes regiones geográficas

Tabla 2.7 Asignación de las bandas en diferentes áreas geográficas

PAÍS/ÁREA GEOGRÁFICA	BANDAS USUADAS
México	2.5 Y 5.8 GHz
América Central y del Sur	2.5, 3.5 Y 5.8 GHz
Europa Occidental	3.5 Y 5.8 GHz
África Asia-Pacífico	3.5 Y 5.8 GHz

CAPÍTULO III

SEGURIDAD EN WIMAX

3.1 SEGURIDAD INFORMÁTICA

Se describe a continuación cada una de las palabras por separado y después se da un concepto con el término compuesto.

A) Informática: es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora.

El término informática proviene de la conjunción de las palabras francesas “information” y “automatique” que derivaron en la palabra “informatique”, creada por el ingeniero Dreyfus.

La informática es la que se encarga de estudiar todo lo relacionado con las computadoras que incluye desde los aspectos de su arquitectura y fabricación hasta los aspectos referidos a la organización y almacenamiento de la información. Incluso contiene las cuestiones relacionadas con la robótica y la inteligencia artificial.

B) Seguridad: proviene de la palabra *securitas* del latín. Se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

Esto se puede ver reflejado en la pirámide de Maslow (Figura 3.1), puesto que en ella se muestra la seguridad dependiendo del ámbito en el se encuentre la situación, persona, etcétera.

Figura 3.1 Pirámide de Maslow

C) Seguridad Informática: se puede entender como una característica de cualquier sistema que indica que está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de *seguridad informática* y se habla de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de *seguridad*; por tanto, se habla de *sistemas fiables* en lugar de hacerlo de *sistemas seguros*.

A grandes rasgos se entiende que mantener un sistema *seguro* (o fiable) consiste básicamente en garantizar tres aspectos:

1) Confidencialidad

   La confidencialidad se refiere a que la información sólo puede ser conocida por individuos autorizados, no debe ser revelada a ninguno por ningún motivo.

2) Integridad

   La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etcétera, durante el proceso de transmisión o en su propio equipo de origen.

3) Disponibilidad

   La disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

En la figura 3.2 se observa una forma de emplear la seguridad informática, claro que ésta no es la única forma de proteger los activos. Ya que para esto se necesitan realizar tres preguntas necesarias para que de alguna manera éstos se encuentren más protegidos, las preguntas son las siguientes:

a) ¿Qué se quiere proteger?

   En esta sección se tienen que identificar todos los recursos que se necesitan o los que se quieren proteger.

   Para que se logre este objetivo es necesario que se tenga una visión completa del valor de los activos y las consecuencias de qué tanto se vea comprometida la confidencialidad, la integridad y la disponibilidad del activo.

   Para esto es necesario que se identifiquen algunas preguntas importantes:

   - ¿Qué podría pasar?
   - ¿Qué tan malo sería si pasara?
   - ¿Qué tan frecuente sería? (relacionado con la pregunta anterior)
   - ¿Qué tan verdaderas son las respuestas anteriores?

b) ¿De qué se quiere proteger?

   Esta pregunta va relacionada a qué es lo que permite identificar las amenazas, los riesgos y por supuesto las vulnerabilidades a

los que se encuentran expuestos los activos que se quieren proteger.

Para que se tenga una protección de todos los bienes y principalmente de aquellos que son de interés, es responsabilidad de la persona que se encuentre a cargo de ellos, se tiene que estimar un valor aproximado de los mismos.

c) ¿Cómo se quiere proteger?

Esta pregunta está basada en las repuestas anteriores; para esto es necesario determinar:

- Objetivos de seguridad
- Requerimientos de seguridad

Figura 3.2 Seguridad informática

3.1.1 AMENAZAS

Una amenaza se puede representar por medio de una persona, circunstancia, de un fenómeno, los cuales pueden causar un daño al momento de realizar alguna violación de la seguridad.

No se debe olvidar que también puede ser un evento que posiblemente desencadenee un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Las amenazas provienen de cinco diferentes tipos de fuentes, que a continuación se van a mencionar.

1) De humanos

Esta amenaza surge por ignorancia, por descuido, por negligencia, de la información.

Para esto existen diferentes formas de que se presente una amenaza por medio de los humanos, sólo sé mencionarán algunos de ellos.

a) Ingeniería social
b) Ingeniería social inversa
c) Personal
d) Sabotaje

En la figura 3.3 se observa una caricatura de cómo se puede realizar una de las amenazas de tipo humana.

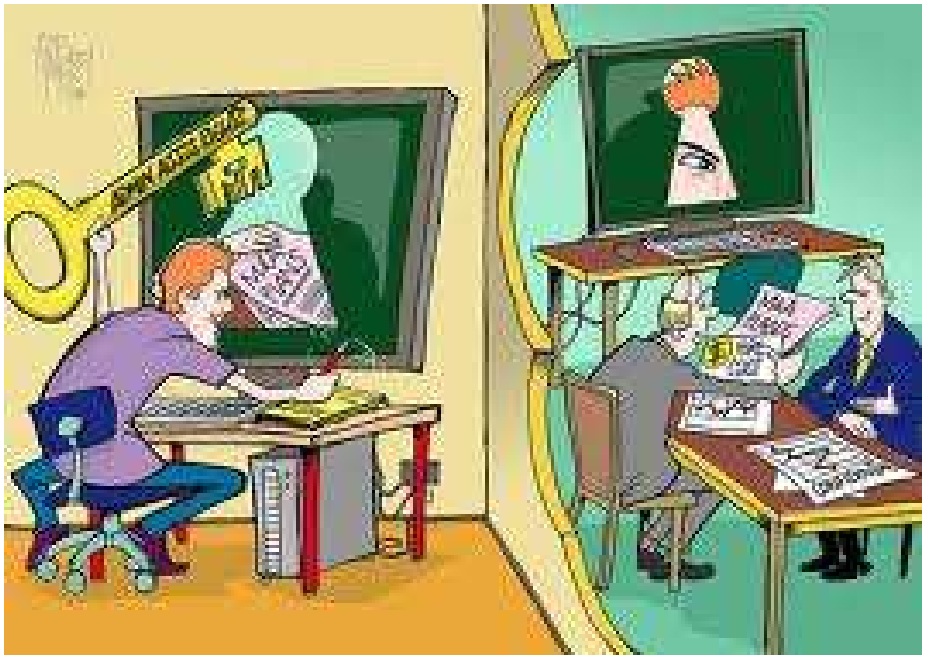


Figura 3.3 Amenaza tipo humana

2) Errores de Hardware

Se da por medio de fallas físicas que se estén presentando en un equipo.

Uno de los problemas más frecuentes son los de suministro de energía, que éstá falle, es decir, los voltajes bajos, ruidos electromagnéticos, alto voltaje, variación en él la frecuencia, etcétera.

3) Errores de red

Esta amenaza se presenta cuando no se calcula bien el flujo de la información que va a circular por medio del canal de la comunicación, esto se podría dar cuando un atacante satura la comunicación lo cual provoca que no exista la disponibilidad de la red.

En este factor también influyen los humanos, puesto que esto es cuando hay dos personas que están conectadas a la red, y si el canal se llega

a desconectar por cualquier razón, el sistema operativo debe dar de baja a los usuarios o en todo caso almacenar los datos.

Esto también abarca el aspecto lógico, se observan las amenazas por medio del monitoreo, ataques de identificación, la obtención de la contraseña, etcétera.

4) Problemas de tipo lógico

Esta amenaza se presenta cuando el mecanismo de seguridad se implementa mal, es decir, cuando no se cumplen las especificaciones del diseño. La comunicación entre procesos puede resaltar una amenaza cuando un intruso utiliza una aplicación que permite enviar o recibir información.

La amenaza de tipo lógico puede detener la información por medio de un código malicioso esto es, cuando un software entra en el sistema de cómputo sin ser invitado e intenta que se rompan las reglas.

Éstos son ejemplos de amenazas de tipo lógico que se encuentran:

a) Jamming o Flooding
b) Syn Flood
c) Connection Flood
d) Net Flood
e) Land Attack
f) Smurf o Broadcast Storm

En la figura 3.4 se ve cómo se puede representar una amenaza de alguno de los ejemplos antes mencionados.

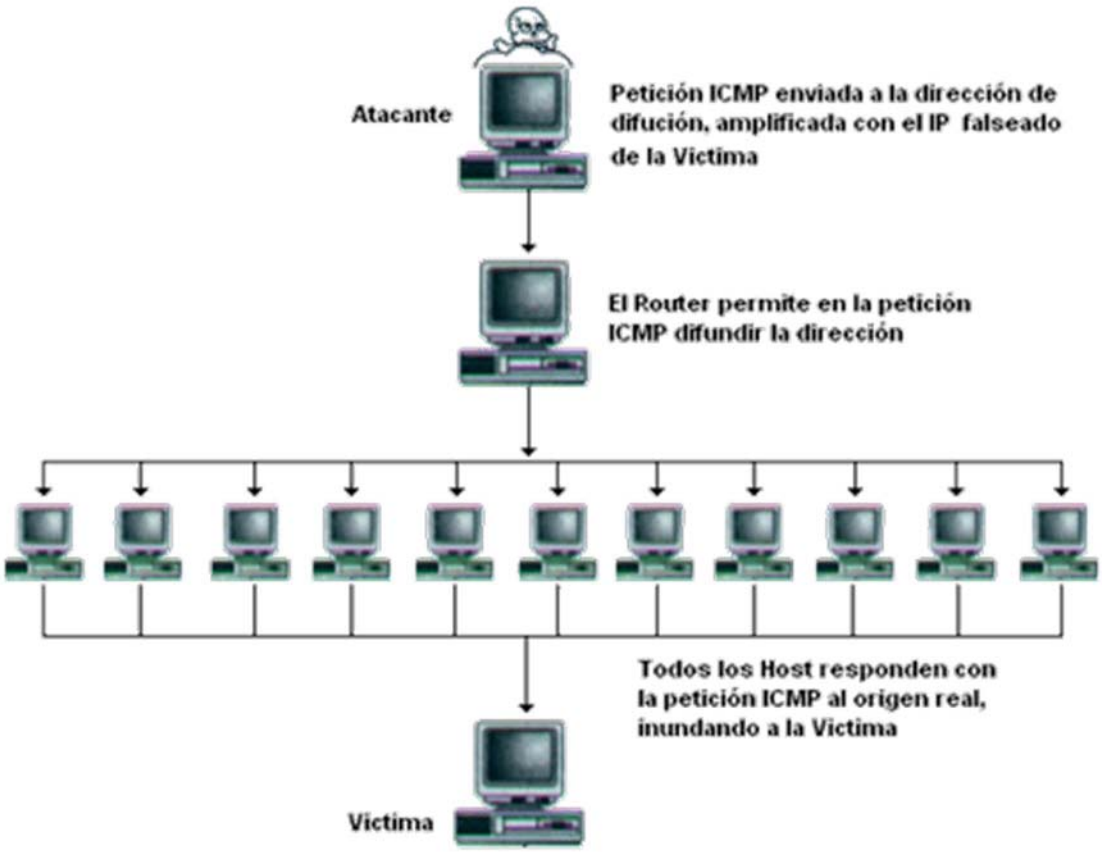


Figura 3.4 Amenaza tipo lógico

5) Desastres naturales

Esta amenaza como su nombre lo dice es de la naturaleza, esto es, que no se puede decir o predecir cuándo va a pasar, porque son amenazas directas.

Estos desastres pueden ser de diferentes tipos, sólo sé mencionarán algunos de ellos, éstos podrían ser los rayos, las fallas eléctricas, picos de potencias, etcétera.

Una de las principales amenaza contra la seguridad es el fuego ya que es considerado como uno de los enemigos número uno de las computadoras ya que destruye con mucha facilidad los archivos de información y programas que hay en ellas.

Así se encuentra un número inmenso de desastres naturales que pueden traer grandes problemas a las computadoras. En la figura 3.5 se observa cómo se puede llevar a cabo un desastre natural sin que el humano pueda hacer algo para detenerlo.

Figura 3.5 Desastre natural

3.1.2 VULNERABILIDADES

Las vulnerabilidades son los aspectos que influyen de manera negativa en un activo que se encuentra latente a un riesgo, esto no necesariamente sucede.

Esto representa una debilidad o aspectos que pueden ser atacables en un sistema informático, esto también es explotado para que se viole la seguridad. Estas vulnerabilidades son extremadamente variables.

Las vulnerabilidades en un sistema se pueden presentar porque al momento de realizar el diseño del mismo no se toma en cuenta la seguridad necesaria para que no se encuentre expuesto y existan muchos agujeros de seguridad que podrían ser explotados por los perpetradores para acceder a los archivos y tener los privilegios necesarios para realizar algún sabotaje.

Con base en lo anterior se encuentran seis diferentes tipos de vulnerabilidades:

1) Física

Esta vulnerabilidad se refiere al acceso o al control físico de un sistema.

Para un servidor se pueden plantear algunos mecanismos estrictos de la seguridad, pero en cambio en una computadora portátil pueden tener acceso todo tipo de personas y se puede obtener el control total de ella, para esto se pueden implementar medidas vía software para que se impida el robo de la información, en el acceso a los periféricos, pero aun así no se cubren todas las vulnerabilidades que hay en un equipo.

2) Natural

Esta vulnerabilidad no depende del humano ya que por más seguro que se encuentre y se haya realizado el estudio necesario en el lugar se pueden presentar diferentes desastres naturales los cuales no se pueden evitar debido a que no se tiene control sobre ellos.

Por lo que no se sabe que tan afectado va a ser el sistema que se esté protegiendo.

Algunas de las vulnerabilidades que pueden ser atacadas son:

a) No tener un espejo del sistema en otro sitio
b) No disponer de reguladores
c) No contar con no-breaks
d) Falta de plantas de energía eléctricas

Se tiene que contemplar todas las posibles vulnerabilidades para que se puedan evitar.

3) De hardware

Esta vulnerabilidad se da por no revisar las características técnicas de los dispositivos junto con sus respectivas especificaciones, sin dejar de lado la falta del mantenimiento del equipo.

Sin embargo, no todos los dispositivos requieren el mismo cuidado ya que en algunos se debe ser más cuidadoso que en otros, para que así se tenga un funcionamiento adecuado.

4) De software

Las fallas o debilidades de los programas en un sistema hacen que se pueda obtener acceso al mismo con mayor facilidad, lo cual lo hace menos confiable.

En esta vulnerabilidad influyen todos los errores de los programas en el sistema operativo u otras aplicaciones que darán oportunidad de que los perpetradores ataquen, no sólo hay que tomar en cuenta los errores de programación.

5) De red

Esta vulnerabilidad se da en la conexión de las computadoras a la red, lo cual ocasiona que las vulnerabilidades del sistema sean aprovechadas, por lo tanto se aumenta el riesgo al que se está sometiendo.

Por lo tanto también aumenta el riesgo de intercepción de las comunicaciones:

- Se puede penetrar a través de la red
- Interceptar la información que es transmitida.

Esto se presenta cuando la conexión tiene debilidades, debido a una mala estructura y que el diseño del cableado no cuenta con ningún estándar para la implementación del mismo.

6) Humana

Éste es el eslabón más débil, puesto que es el ser más vulnerable a la ingeniería social, ya que contiene información y por varias circunstancias puede que lo revele o que por algún descuido no proteja adecuadamente la información.

3.1.3 SERVICIOS DE SEGURIDAD

Hay aspectos importantes en WiMAX dentro de la seguridad que deben considerarse en el diseño de la red. Éstos van desde técnicas de reducción en la capa física hasta la mejora de la autenticación inalámbrica de intrusos y el cifrado de datos y la protección de la seguridad del transporte.

Los servicios de seguridad que se implementan en WiMAX son:

1) Capa física
2) Autenticación de las Transmisiones Inalámbricas
3) Cifrado
4) Participación de Terceros en la Protección Contra Intrusiones
5) Participación de Terceros en el Transporte de Datos de Seguridad

También WiMAX tiene una seguridad muy importante ya que ésta cuenta con DOCSIS + protocolo de seguridad, es decir, el DOCSIS en la interfaz en el servicio de cable con un protocolo se seguridad (SSL/TSL -- Secure Sockets Layer/Transport Layer Security - Seguridad de la Capa de Transporte) extra para brindar una mayor confiabilidad en la transmisión de los datos.

Con esto se puede hacer más robusta la seguridad en las redes, al igual que intercambio de información.

A continuación se mencionan algunas características del DOCSIS

La especificación de datos mediante una interfaz de servicio de cable (DOCSIS- Data Over Cable Service Interface Specification – Datos sobre la especificación de interfaz del servicio de cable), define los estándares de interfaz para los módems de cable y equipo de apoyo que participan en alta velocidad de transferencia y distribución de datos a través de redes de sistemas de cable de televisión. Permite datos adicionales de alta velocidad de transferencia de más de un sistema de televisión por cable existentes y es ampliamente utilizado por los operadores de televisión para ofrecer acceso a Internet a través de una fibra híbrida coaxial.

Otros dispositivos ya están incluyendo el método para que sea compatible con la Web, específicamente con las redes WiMAX ya que aún en México no se cuenta con la tecnología necesaria para que exista el auge que la tecnología requiere, es decir, se necesita un cable o un dispositivo diferente para que se pueda tener acceso al ancho de banda que está requiriendo la tecnología.

En la figura 3.6 se observa cómo se llevan a cabo los servicios de la seguridad en WiMAX.

Figura 3.6 Servicios de Seguridad de WIMAX

WiMAX también está basado en la autenticación PKM-EAP (Extensible Authentication Protocol) y TLS (Transport Layer Security).

WiMAX también utiliza CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Modo contador con Protocolo del código para la autenticación del mensaje del encadenamiento del cifrado en bloque), que utiliza el algoritmo AES de cifrado de datos.

WiMAX también está apoyado por la norma del algoritmo del Triple DES.

3.1.4 ATAQUES DE SEGURIDAD

Los principales ataques en las redes inalámbricas WiMAX son en la autenticación y confidencialidad.

Puesto que se centran en la autenticación y autorización de WiMAX, ya que son componentes clave de cualquier solución de seguridad.

Por lo que a continuación se mencionan los diferentes ataques que se presentan en los diferentes niveles de la seguridad.

1) Capa física de Seguridad

Hay dos tipos básicos de ataques que pueden afectar a la capa física de WiMAX.

a) Atascos de información

Los atascos de la información se pueden dar por medio de Jamming que consta de una señal más fuerte de la red WiMAX, que ocasiona que los datos se saturen, es decir, que no fluya el tráfico en la red o con intermitentes ráfagas sostenidas.

Dado que la mayoría de los servicios de red WiMAX son provistos a través de las bandas con licencia (en la actualidad, 3.5 GHz y 2.5 GHz internacionalmente), ofrece este espectro la interferencia accidental. Las interferencias en el espectro con licencia no siempre pueden ser totalmente eliminadas ya que hay una posibilidad de presencia de lo que se llama segunda y tercera interferencia armónica, por ejemplo, con un frecuencia de 2.3 GHz que es la mínima que utiliza

la tecnología de WiMAX, esto es con una distancia corta entre antenas lo que ocasionaría que la señal fuera deficiente.

b) Paquetes de codificación.

Paquete de codificación es un ataque que se produce cuando los paquetes de control en los respectivos enlaces ascendente y descendente son codificados y luego son regresados a la red. “Las redes WiMAX pueden ser por división de tiempo de uso de la doble cara (TDD), en donde las señales son rodajas de tiempo a través de las cuales un atacante puede analizar este momento y la secuencia de captura de datos de control, en el preámbulo y de ruta, y enviar de vuelta con el momento correcto para interrumpir legítimamente la Señal, lo que resulta en demoras y reduce el ancho de banda de manera efectiva "[1].

2) Autenticación de las Transmisiones

En el control de acceso a medios (MAC) WiMAX la capa de control o cabecera MAC parte de las transmisiones no está cifrada, puede generar fácilmente un ataque en la red inalámbrica (WiMAX), por lo que es necesario que se autentique la información.

Useckas, A. (s.f.). De tecnología de NetSieben Technologies.

3) Cifrado

Se puede tener un ataque en la autenticación de los usuarios así mismo como en el viaje de la información por medio de la red de WiMAX.

4) Participación de Terceros en la Protección Contra Intrusiones

Si la base de clientes es muy sensible a la integridad de los datos (sector financiero hospital o clientes) de terceros los sistemas de prevención de intrusos pueden ayudar a los usuarios del segmento, así como garantizar que no exista un ataque desde el exterior.

5) Participación de Terceros en el Transporte de Datos de Seguridad

Se puede tener un ataque cuando se utiliza la participación de terceros y esto se da principalmente en la capa de transporte por lo que se está comprometiendo la integridad, la confiabilidad del viaje de la información, as mismo como la información confidencial del usuario.

3.1.5 MECANISMOS DE SEGURIDAD

WiMAX es una tecnología adecuada para dar un servicio de acceso fijo; es decir, puede utilizarse como competidor o sustituto de la red de acceso fija (DSL y cable) en determinados entornos, especialmente en entornos rurales donde el despliegue de soluciones de cable es muy costoso y los radioenlaces punto-multipunto se presentan como una alternativa flexible y más barata. Lógicamente, si las aplicaciones están orientadas a operadores de telecomunicaciones, no tiene sentido utilizar bandas de frecuencias no reguladas y por lo tanto susceptibles de interferencias. Es también por eso que el estándar incluye mecanismos de seguridad y QoS.

Otra característica destacada del WiMAX es que incorpora en el mismo estándar los mecanismos de seguridad que son necesarios para que se brinde un mejor servicio de red inalámbrico; ya que, como se ha explicado, es una tecnología destinada al uso de operadores de telecomunicaciones que requieren esta funcionalidad.

Wi-Fi incorporó muchos de los mecanismos que WiMAX implementa para que la seguridad sea más robusta y utiliza prácticamente los mismos algoritmos. Así pues, el WiMAX incorpora:

• Cifrado de los datos utilizando el algoritmo AES, igual que WPA2 del 802.11.

• Autenticación entre la estación base y el usuario basada en certificados digitales X.509 para evitar suplantaciones de personalidad por parte tanto de la estación base como del usuario.

• Autenticación de cada mensaje donde se intercambia una nueva clave mediante una firma digital para evitar que estos mensajes puedan ser interceptados y modificados.

• Claves de encriptación y autenticación que se renuevan periódicamente para evitar ataques basados en almacenar y repetir mensajes válidos y para evitar que se puedan romper estas claves.

Así pues, la seguridad en WiMAX es comparable a la conseguida por el Wi-Fi con las mejoras introducidas con el estándar 802.11i, los cuales son mencionados a continuación:

1) TKIP (Temporary Key Integrity Protocol) es un protocolo de gestión de claves dinámicas admitido por cualquier adaptador que permite utilizar una clave distinta para cada paquete transmitido. La clave se construye a partir de la clave base, la dirección MAC de la estación emisora y del número de serie del paquete como vector de inicialización.

2) CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) es un nuevo protocolo que utiliza AES como algoritmo criptográfico y proporciona integridad y confidencialidad.

3) WRAP

Existe un sistema de cifrado opcional denominado WRAP (Wireless Robust Authentication Protocol – Protocolo de autenticación inalámbrica robusta) que puede sustituir a CCMP.

Hay que prestar atención, ya que algunos fabricantes sacaron en el mercado productos llamados "pre- WiMAX". Estos productos seguían las directrices generales de lo que se esperaba que fuera el estándar WiMAX, pero no necesariamente son compatibles, ni proporcionan la misma funcionalidad o rendimiento. Entonces hay que evaluar esmeradamente la conveniencia de atarse a una línea de productos y a un fabricante que probablemente sean incompatibles con los futuros desarrollos del estándar WiMAX. Dicho esto, hay un gran número de productos y despliegues en el mercado basados en tecnología pre-WiMAX, especialmente como sustituto de LMDS.

Para finalizar, se tiene que decir que todavía no han salido al mercado tarjetas PCMCIA para ordenadores portátiles, y menos portátiles con dispositivos Wi- MAX integrados, como sí sucede en el caso de Wi-Fi. Aunque hay una evidente reducción en dimensión y precio de los receptores WiMAX, todavía son más caros y más aparatosos que en el caso de Wi-Fi, lo cual los hace poco adecuados como tecnología móvil o incluso para soluciones que lleguen a utilizar una tarjeta inteligente. WiMAX tiene una tecnología de respaldo (Backup), para que el usuario final tenga la confiabilidad y la seguridad de que la comunicación en red es adecuada para sus necesidades y exista un respaldo en caso de emergencia.

3.1.6 POLÍTICAS DE SEGURIDAD

Una **política de seguridad** en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero.

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad.

Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos. Debe ser fácilmente accesible de tal forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

3.2 SEGURIDAD DE WIMAX

Las redes WiMAX se consideran seguras, esto debido al uso de protocolos de cifrado de datos, el filtrado de MAC (de manera que sólo se le permite el acceso a la red a aquellos dispositivos autorizados), ocultar el nombre de la red o la autentificación de los usuarios, son técnicas que implementa para asegurar que solamente podrán acceder a la red WiMAX los aparatos o personas que estén autorizados.

3.2.1 AUTENTICACIÓN

Como se ha comentado previamente, la autenticación sirve para garantizar el acceso seguro, evitando que usuarios no autorizados hagan uso de la conexión inalámbrica. El estándar *IEEE 802.16-2009* define dos filosofías de autenticación:

a) **OSA (*Open System Authentication – Sistema Abierto de Autenticacion*):** el cliente realiza una solicitud de autenticación asociada a su dirección MAC, a lo que sigue una respuesta de la Estación Base (en adelante, BS) con la aceptación o denegación. La BS realiza únicamente y de forma opcional un filtrado por dirección MAC.

b) **SKA (*Shared Key Authentication* - Autenticación dominante compartida):** se utilizan en el proceso claves compartidas que ambos extremos deberán conocer para garantizar una autenticación más segura.

c) Para la autenticación mediante claves compartidas, WiMAX define el protocolo **PKM** (*Privacy Key Management – Clave Maestra Privada*) para que una Estación de Usuario (en adelante, **SS**) pueda intercambiar claves y obtener autorización de la **BS**).

PKM también se encarga de otras cuestiones relacionadas como el refresco de las claves, la re-autorización periódica. El proceso de autenticación entre BS y SS se puede describir de forma simple de la siguiente forma:

1) Una SS envía un mensaje **PKM** (*Privacy Key Management*) solicitando autenticación a la BS e incluyendo su **certificado digital X.509**. Este certificado es único por equipo e infalsificable, con lo que le define de forma unívoca y evita los ataques por suplantación de MAC.

2) La BS procede a autenticar y a verificar el certificado comprobando la **firma digital** del fabricante incluida en el certificado.

3) Si el certificado X.509 es aceptado, la BS genera la **clave de autenticación** (AK) y **la cifra** mediante la **clave pública de 1024 bits** contenida en el propio certificado X.509.

3.2.2 ALGORITMOS DE CIFRADO

Después de que la BS autorice a la SS, son necesarios también mecanismos de cifrado para velar por la confidencialidad y la integridad de los datos. Para ello, la SS envía a la BS una **solicitud de claves** de cifrado llamada TEKs (*Traffic Encryption Keys –C*laves =para el cifrado del tráfico), que es enviada por la BS en un mensaje de respuesta. Estos mensajes a su vez están cifrados con una clave conocida por ambas partes. El algoritmo empleado para el cifrado de las TEKs puede ser de tipo **3DES** (*Triple Data Encryption Standard* **–** Estándar triple para el cifrado de datos), **AES** (*Advanced Encryption Standard* **–** Estándar avanzado de cifrado), o **RSA** (Son las siglas de los nombres de quienes lo realizaron Ron Rivest, Adi Shamir, y Leonard Adleman**)**

Una vez conocidas las TEKs, diversas técnicas pueden ser utilizadas para cifrar los datos: CBC (DES), CBC (AES), CTR (AES), CCM (AES).

Algunas de las ventajas de los mecanismos de cifrado que implementa WiMAX respecto a los de otras tecnologías son:

1. Los algoritmos empleados son muy robustos
2. Soportan generación de claves dinámicas con tiempos de vida variables
3. Permiten realizar un cifrado independiente para cada flujo de datos
4. Todo esto se realiza con el objetivo de garantizar la confidencialidad en las redes WiMAX.

WiMAX utiliza también un certificado que es el siguiente: **Certificado digital X 509.**

Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Existen varios formatos para certificados digitales, pero uno de los estándares más populares es el **UIT-T X.509** (usado también en el DNI electrónico). El certificado contiene habitualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado, de forma que el receptor pueda verificar que ésta última ha establecido realmente la asociación.

Los formatos de certificación pueden emplear:

a) **Claves ESTÁTICAS:** No se actualizan, son muy vulnerables y fáciles de adivinar.

b) **Claves DINÁMICAS (WiMAX):** tienen un tiempo de vida limitado, cambian y se renuevan automáticamente. Máxima seguridad.

CAPÍTULO IV
DISEÑO DE LA RED INALÁMBRICA

4.1 INTRODUCCIÓN

Para que se diseñe una red inalámbrica se tienen que tomar en cuenta los siguientes puntos, puesto que es importante para realizar un diseño adecuado para el lugar en el que se va a diseñar, y así tener un buen servicio de internet:

a) Cobertura

En este punto se debe tener claro para qué área se va a realizar el diseño, ya que la estación de la red debe colocarse en un punto estratégico para que el funcionamiento sea adecuado.

b) Capacidad

Trata de la capacidad que tiene el canal para el traslado de la información, es decir, cuál es, cuántos bits y bytes se van a ir trasladando por el canal de información.

En este punto también se debe tener claro para que la información viaje completa, rápida y segura.

c) Costo

Es indispensable tomar en cuenta el costo inicial de todo el equipo que se necesita para la realización de la misma; de todo el equipamiento que se requiere para aplicar la tecnología WiMAX, también las instalaciones en la que se va a diseñar la red.

Se debe tomar en cuenta el costo que va a generar el mantenimiento de la misma y de las actualizaciones que se vayan requiriendo para que la red tenga un funcionamiento adecuado.

d) Complejidad

En la complejidad que la red va a tener se puede definir de acuerdo con el tamaño de la red, pero para esto se toma en cuenta el cómo se va a administrar, los componentes físicos y por supuesto los componentes lógicos, ya que todos son indispensables para que la red tenga un funcionamiento adecuado y así brindar un mejor servicio.

e) Interferencia

La interferencia puede ser tolerada puesto que es generada por diferentes fuentes, a continuación se van a mencionar algunas de ellas.

- Los equipos que ya se encuentran en el sitio, es decir, los canales que se van a reutilizar en un canal del sistema
- Por los sistemas que no se tiene control de ellos, es decir, que no están al alcance.
- Las paredes que muestran dificultad para transmitir la información con facilidad.

Los puntos anteriores son importantes y se encuentran íntimamente ligados para que se tenga un diseño adecuado a las necesidades para las cuales se está diseñando la red.

Por lo que es importante tener en cuenta que no existe ninguna red que sea de bajo costo y que tenga una buena calidad en la cobertura y un capacidad para el envío de la información, por lo que se tiene que tener presente cuales son las condiciones del lugar en donde se va a realizar el diseño de la red.

Para esto es necesario que se tenga un equilibrio entre los puntos anteriores para que se realice una red inalámbrica adecuada y que brinde un servicio eficiente y por supuesto seguro.

Y así mismo brindarles una mejor solución a las necesidades de los usuarios y por supuesto cubriendo las expectativas que se tienen del lugar como un centro de cómputo de la Facultad de Ingeniería (Universidad Nacional Autónoma de México).

4.2 ANÁLISIS DE LA RED INALÁMBRICA WIMAX

Para realizar adecuadamente el diseño de una red inalámbrica de la tecnología WiMAX es necesario que se lleve a cabo un estudio de todas las redes que existen en el lugar, las necesidades que se tienen en la sala uno de cómputo de UNICA, la estimación aproximada de las instalaciones necesarias y de la configuración.

Para que se realice un análisis adecuado es necesario que se base en los siguientes puntos para que el diseño de la red sea el más adecuado y cubra con las necesidades que se tienen en la sala 1 de cómputo.

a) **Antecedentes del lugar:** es una descripción detallada de todas las condiciones del lugar y por supuesto de lo que se desee de dicha red; se tiene deben satisfacer todas las necesidades que se establecieron como objetivo, así mismo como prever un crecimiento a futuro

b) **Identificación de redes:** este punto es para verificar que las redes que se encuentran en el sitio no se encuentran adyacentes al lugar, es lograr un análisis adecuado con el radio de frecuencia y así mismo brindar un mejor servicio y con esto cubrir todas las necesidades que se están requiriendo en el momento y a futuro.

c) **Demanda del servicio (usuarios):** verificar cómo es la demanda de los servicios y así mismo identificar las características de éstas, sin olvidar el comportamiento de todos los usuarios que están requiriendo del servicio; esto es de los alumnos, profesores y personal administrativo. Esto puede

resultar de un alto interés ya que facilita el diseño de la red, sin olvidar los diferentes factores que pueden resultar conforme vayan creciendo los servicios de esta red.

d) **Dimensión de la red:** se necesita un número aproximado de las instalaciones y de la configuración de la red para que se cubran las necesidades de los usuarios pero así mismo con los requisitos que se están proponiendo en los objetivos del diseño de la red, es decir, la cobertura de la zona de interés, la capacidad que se tiene que cubrir, el número de los elementos que se necesitan, los enlaces que deben existir entre ellos.

e) **Necesidades (usuarios):** identificar las características, las necesidades y el comportamiento de todos los usuarios que van a utilizar la red ya sean estudiantes, profesores o personal administrativo, esto es de interés para ayudar a facilitar el diseño de la red.

Desde el punto de vista de los usuarios, se puede definir con los requerimientos responsables para indicar las aplicaciones y las tareas aplicadas en la red y se pueda catalogar como que el servicio es efectivo.

Después de que se describieron los antecedentes del lugar es necesario conocer un poco de la historia del sitio en donde se va a colocar la red inalámbrica, es decir, qué servicios se van a brindar y si son los que los usuarios necesitan, ya que con esto se podrá tener más claro por qué se debe diseñar y al mismo tiempo ver que las necesidades de todos los usuarios van cambiando y que se debe hacer un cambio para crecer con la tecnología.

El lugar en donde se va a realizar el diseño de la red es en la Unidad de Servicios de Cómputo Académico de la Facultad de Ingeniería (UNICA), por lo que es necesario que se conozca un poco de su historia de cómo es que existe este centro de cómputo en la Facultad de Ingeniería.

"UNICA es el resultado de la división del antiguo Centro de Cálculo (**CECAFI**), en 1994. **CECAFI** tiene sus orígenes a partir del 16 de junio 1972, contando con una sola terminal "Remote Job Entry" modelo 2780 de OBM, que se encontraba conectada vía telefónica a una computadora IBM 370/155 de la Secretaría de Obras Públicas, el tiempo de respuesta que se tenía en este tipo de equipo generó problemas y gracias a éstos se decidió cambiar este equipo por una computadora, el equipo que se instaló fue una computadora IMB 1130 con tan solo 8 KB de memoria principal, una lectora de tarjetas de 120 tarjetas por minuto y una impresora lenta de 80 líneas por minuto"[1]

Conforme fueron pasando los años, CECAFI fue siendo independiente de todos los procesos que se llevaban a cabo con IBM, por lo que se crea otra dependencia totalmente diferente de lo que inicialmente se tenía y así cubrir con las necesidades de los usuarios tanto alumnos, profesores y personal administrativo.

[1] *UNICA*. (s.f.). Obtenido de http://132.248.54.13/UNICA/index.jsp

“Surge en el año de 1994 cuando se decide seccionar el Centro de Cálculo de acuerdo con sus objetivos y funciones, con la finalidad de proporcionar una mayor eficiencia en el desempeño del personal. Con base en esto se crean dos Unidades para desempeñar el trabajo que realizaba el Centro de Cálculo. La Unidad de Servicios de Cómputo Académico (UNICA) y la Unidad de Servicios de Cálculo Académico (USECAD) son las dos unidades creadas para llevar a cabo las tareas académicas y administrativas de la Facultad de Ingeniería.” [2]

Las funciones que desempeña la Unidad de Servicios de Cómputo Académico son:

- Mantener el liderazgo en cuanto a tópicos en cómputo.
- Continuar proporcionando recursos de cómputo de calidad a la comunidad de la Facultad.
- Impulsar a nivel de la Facultad la creación de una política de cómputo definida.
- Lograr la capacitación cada vez más completa y actualizada para la formación de recursos humanos.
- Aplicar todos los conocimientos y las herramientas de cómputo con los que cuenta la Unidad para realizar las actividades de forma más eficiente y segura.

[2] *UNICA*. (s.f.). Obtenido de http://132.248.54.13/UNICA/index.jsp

Después de conocer un poco de la historia del lugar en donde se va a diseñar la red es necesario que se especifiquen algunas características del lugar para que así se puede llevar a cabo el diseño de ésta y cubrir con todas los objetivos.

- **Características del lugar:** la sala uno de UNICA tiene un área específica que se encuentra en la figura 4.1, la cual está ubicado en la planta baja del edificio principal a un costado del estacionamiento de profesores y de la librería.

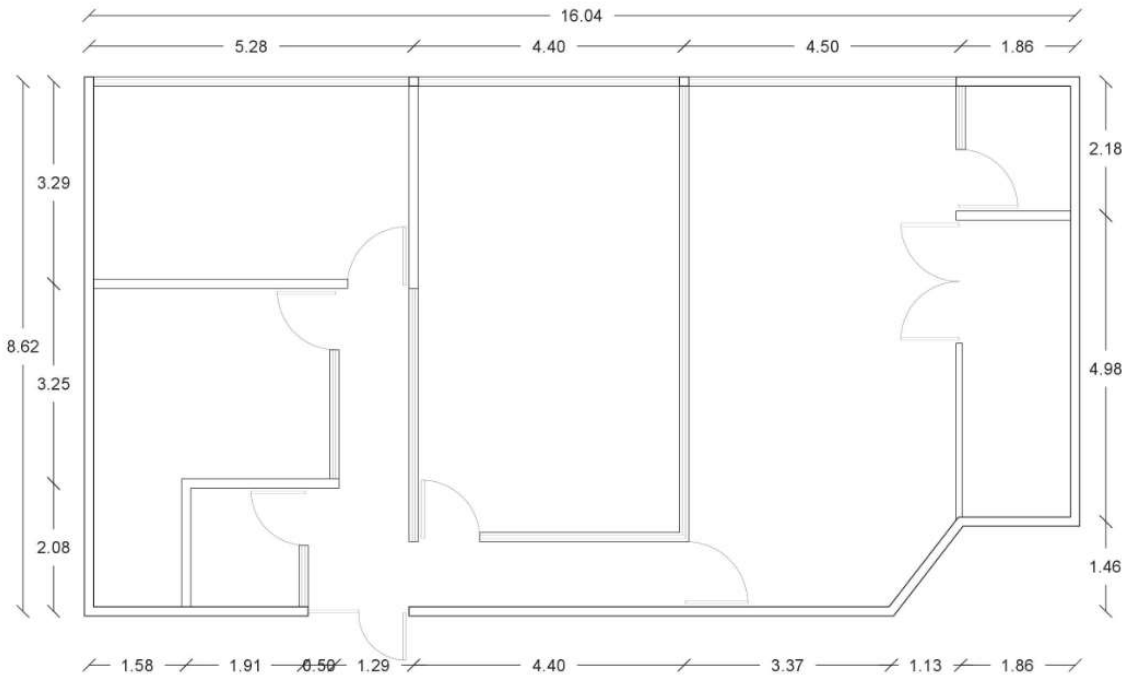


Figura 4.1 Plano de sala 1 UNICA

Una de las características del sitio en general es que se encuentra rodeado por muros que hacen que la transmisión de las señales de propagación de una red inalámbrica presente dificultad.

Se considera que se tiene identificado que existen otras redes como son:

a) Redes de WiFi: de ésta no se tiene una propagación de la señal adecuada, ya que en las aulas de cómputo no se tiene señal continúa por lo que no se puede utilizar cómputo móvil, y es indispensable contar con la transmisión de la red alámbrica.
b) Red alámbrica: se cuenta con un Switch para la propagación de la misma.

Los equipos que se encuentran funcionando actualmente en la sala 1 (UNICA) son los siguientes:

a) 28 equipos son del modelo Optiplex 620, en la tabla 4.1 se muestran todas las características de los equipos mencionados.

Tabla 4.1 Especificación de los Equipos

Tipo del microprocesador	Microprocesadores Intel® Pentium® 4 y Celeron™. El diseño proporciona actualizaciones futuras compatibles con Dell. Es posible fijar una velocidad de compatibilidad más lenta por medio de la configuración del sistema, 1.84 GB
Memoria	SDRAM (synchronous dynamic random-access memory - memoria dinámica sincrónica de acceso aleatorio), con 512 Mb de memoria mínima y 1 GB máxima.
Disco Duro	Una unidad de disco duro IDE de 1 pulgada de altura, 160 Gb

b) 6 equipos son del modelo Optiplex 260 y tienen las especificaciones que se muestran en la tabla 4.2.

Tabla 4.2 Especificaciones del Equipo

Tipo del microprocesador	Microprocesadores Intel® Pentium® 4 y Celeron™. El diseño proporciona actualizaciones futuras compatibles con Dell. Es posible fijar una velocidad de compatibilidad más lenta por medio de la configuración del sistema.
Memoria	SDRAM (synchronous dynamic random-access memory - memoria dinámica sincrónica de acceso aleatorio) de velocidad de datos doble de 200 y 266 megahertz (MHz)
Disco Duro	Una unidad de disco duro IDE de 1 pulgada de altura, 80 MB.
Memoria Caché	Procesadores de 1,5– 2,0* GHz: SRAM con política de actualización exclusiva de la memoria caché, juego asociativo de ocho vías, transmisión en bloques por conducto, 256 KB Procesadores 2.2–2.6 GHz: 512 KB de SRAM *Algunos sistemas de 2.0 G se pueden actualizar a una caché de 512 K.

En la figura 4.2 se muestra la ubicación de todo el equipo que actualmente se encuentra en función en la sala para el servicio de los usuarios y por su puesto cubriendo algunas necesidades de los alumnos, profesores y personal administrativo.

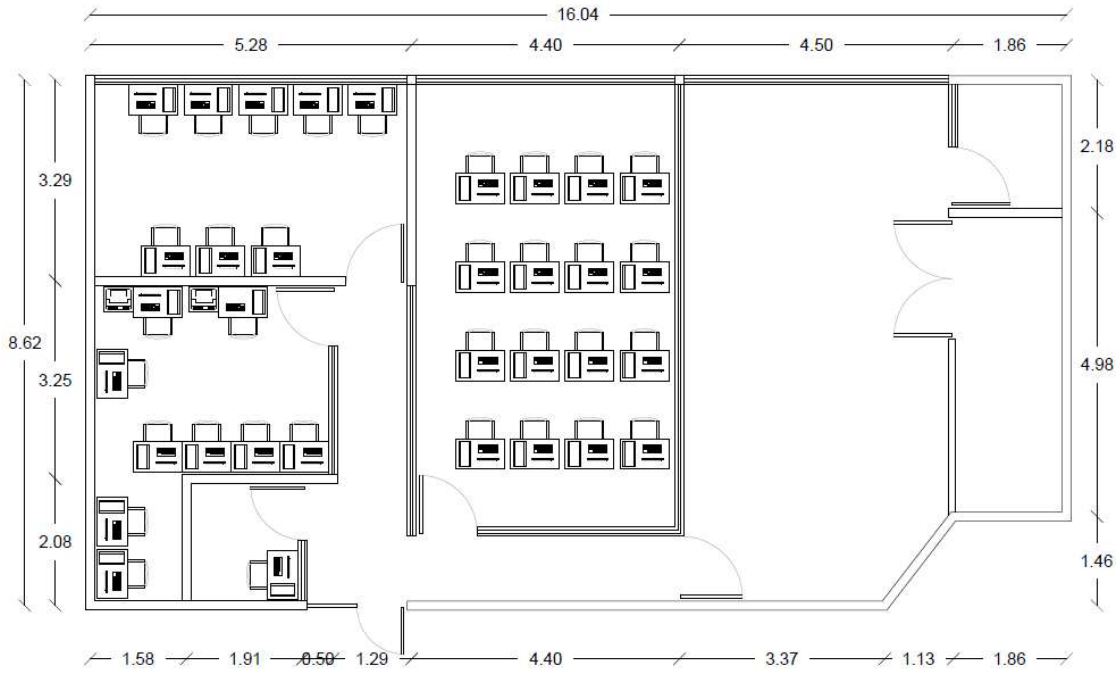


Figura 4.2 Ubicación de los equipos

Por otro lado, se tiene los switches que proporcionan red a los equipos que se encuentran en funcionamiento en la sala 1.

Estos son 3 switches 3COM, en la tabla 4.3 se muestran las especificaciones con la que cuentan.

Tabla 4.3 Especificación de Switch 3COM

Puertos	Velocidad	Protocolos
48 x Ethernet	100 Mbps	TCP/IP

Se está realizando el diseño de esta red inalámbrica porque la sala de cómputo con la que cuenta el edificio principal de la Facultad de Ingeniería, no cuenta con los equipos necesarios para satisfacer a

todos los alumnos, trabajadores de la misma, las cuales son ocupadas para que los mismos puedan realizar trabajos que se les pide.

Además hay asignaturas en las cuales es necesario que se ocupe equipo portátil para realizar pruebas de conexión y no se tiene una red inalámbrica que cuente con una cobertura amplia como es la red WI-MAX.

La misma será ocupada por todos los compañeros que se encuentran alrededor, es decir, la cobertura que tiene la red podría alcanzar a los compañeros de la Facultad de Arquitectura.

4.3 MATERIALES A UTILIZAR

Los componentes que se necesitan para poder llevar a cabo el diseño de la red son tanto elementos físicos como lógicos para que tenga un funcionamiento adecuado a las necesidades que se necesitan cubrir.

1. ELEMENTOS FÍSICOS

Se mencionan los elementos más importantes para que se lleve a cabo el diseño de la red.

No basaremos en la familia de los equipos de RedMAX que proporciona una conectividad de WiMAX con certificación para todo tipo de zona, es decir, ya sea en zonas urbanas o rurales. Una de las características que se tiene es la velocidad de transmisión puede ser configurable en las implementaciones de punto a punto y punto a multipunto que se encuentran totalmente destinadas a que se cumpla la fiabilidad, se cuenta con 10/100 puertos de datos de Ethernet, las cuales pueden ser tanto de voz como de datos.

Se mencionan algunas características del equipo que se necesita para realizar el diseño de la misma.

a) Estación Base (BS)

Este equipo fue fabricado por RedLine, con un modelo AN-100U o AN-100UX, este es un dispositivo que cumple con todas las certificaciones que están operando en el estándar IEEE 802.16-2004 para una implementación.

Con la BS se tiene dos diferentes terminales en las que se puede operar, las cuales son:

1) SU-O (outdoor terminal—Terminal exterior)

2) SU-I (SU-I indoor terminal—Terminal interior)

La estación tiene dos tipos de conexión las cuales son:

1) **IDU (Indoor Unit—Unidad del interior):** es una plataforma integrada en RIU sin módulos extraíbles. Es un equipo de 10/100 de Ethernet y gestión de datos, como se muestra en la figura 4.3

Figura 4.3 IDU [3]

[3] IDU. (s.f.). System description RedMAX rev 3.

2) **ODU (Outdor Unit—Unidad del exterior):** esta contiene un Hardware de RF que está unido a una torre con un soporte de montaje que acepta una elección de antenas sectoriales, que sirve para satisfacer las necesidades de transmisión, frecuentemente el nodo consta de 4 sectores de 90° o 60° grados (Figura 4.4).

Figura 4.4 ODU [4]

Una de las características que se debe mencionar es que tienen un rango de 3.4 a 3.6 GHz., el cual se encuentra dentro de la banda que maneja WiMAX y así mismo esta licencia en México.

b) CPE (Equipo Local del Cliente)

El CPE es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

[4] (s.f.). System description RedMAX rev 3.

Son unidades terminales asociadas a equipamientos de telecomunicaciones, localizadas en el lado del suscriptor y que se encuentran conectadas con el canal de comunicaciones del proveedor o portador de información.

c) **Tarjeta de RED**

Las tarjetas de red (adaptadores de red, tarjetas de interfaz de red) actúan como la interfaz de un ordenador ya sea de cable o inalámbrico.

La función de las tarjetas de red es la de preparar, enviar y controlar los datos en la red.

Algunas de las características de las tarjetas inalámbricas se mencionan a continuación:

* Están diseñadas para ciertos tipos de estándares de redes inalámbricas, por lo que tienen una velocidad máxima de transmisión de datos en bits por segundo (bps) acorde al estándar.
* Tienen una antena que permite la buena recepción de datos de la red, así como para su envío
* Permiten la comunicación entre sí mismas, independientemente del punto de acceso, es decir, que no se mandan los paquetes directamente al punto de acceso sino que pueden pasarlos a otras tarjetas de red y así llegar a su destino.

Las WLAN (Wireless Local Area Network- redes de área local inalámbricas) permiten a sus usuarios acceder a información y

recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante, incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s o superiores.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (hot spots) en las próximas redes de tercera generación (3G) se ven como las aplicaciones de más interés durante los próximos años.

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como son los PDAs (Personal Digital Assistants – Asistentes Personales Digitales), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de

la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

RedMAX cuenta con una tarjeta compacta que está diseñada para dar los servicios de banda ancha, la cual daría un rendimiento excepcional, y cumple con los estándares de IEEE 802.16 (Figura 4.5)

Figura 4.5 Tarjeta de red [5]

[5] (s.f.). System description RedMAX rev 3.

La cual tiene las siguientes características como se muestra en la siguiente tabla 4.4:

Tabla 4.4 Características de una tarjeta de RED

Descripción del sistema	Tarjeta para PC WiMAX (basada en WiMAX® Forum system profile)
Capa física	FDMA (256 Mbs)
Atributos de la tarjeta madre	QoS (Quality of Service - Calidad de Servicio)
Técnica doble cara	TTD (Time Division Duplex—Tiempo de división de doble cara)
Banda de frecuencia	3.5 – 7 Hz
La media de potencia de salida	+20 dBm
Modulación	16 QAM a 64 QAM
Cifrado	DES o 3DES
Antena	Omnidireccional

d) Línea de vista: es un camino que se encuentra sin obstrucciones (path), es decir, que se encuentren las antenas de transmisión y recepción de manera directa.

Para lo cual existen dos diferentes tipos de vista que se pueden encontrar al momento de querer realizar una conexión de comunicación entre diferentes equipos y así poder brindar el servicio, las cuales son:

1) **NLOS (Sin línea de visión directa)**: no se cuenta con una línea de visión directa entre la base y en donde se encuentra el CPE, es decir, esta característica es la más común porque en la mayoría de los casos en donde se desea lograr la comunicación la mayoría de las veces está rodeada del ambiente, edificios de gran altura, etcétera.

La señal entregada del receptor depende de una reflexión o refracción como se muestra en la figura 4.6.

Figura 4.6 Línea de vista NLOS [6]

[6] (s.f.). System description RedMAX rev 3.

2) **LOS (Línea de visión):** es la visión ideal para una comunicación de redes inalámbricas, ya que no existe ningún obstáculo entre ellos. Lo que permite una visibilidad directa que permite que las ondas sean propagadas después de que salen de la antena, las cuales llegaran con una gran intensidad a su destino (Figura 4.6).

3) **OLOS (Óptica de línea de visión):** con esta característica se puede obtener una visión clara para transmitir y lograr la comunicación, pero hay obstrucción dentro de toda la zona (Figura 4.7).

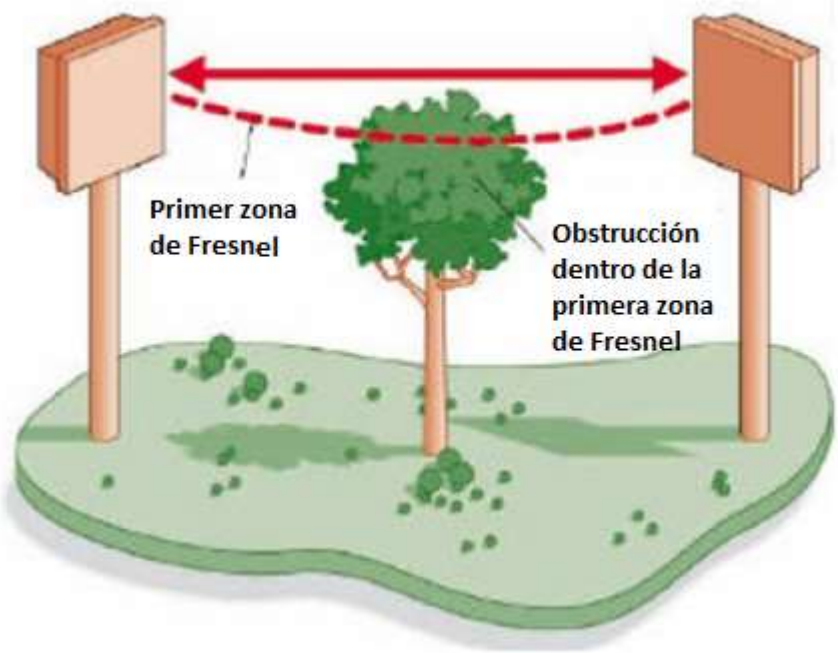


Figura 4.7 Línea de vista NLOS [7]

[7] IDU. (s.f.). System description RedMAX rev 3.

d) Estación suscriptora (SS)

Son equipos que identifican el funcionamiento de las redes Broadband Wireless Acces (BWA—Banda ancha inalámbrica de acceso). Este equipo proporciona la conectividad vía radio con la estación base (BS).

Los equipos suscriptores de la marca RedLine están certificados por el WiMAX Forum los cuales soportan perfiles que tienen comunicación con BS.

4.4 DISEÑO DE LA RED

Para realizar el diseño de la red es necesario que se tomen en cuenta las siguientes características ya que de esto depende que el funcionamiento sea totalmente adecuado y que se cubra la mayoría de las necesidades si no es que todas.

1. Usuarios: Para todos los usuarios que hacen uso de la sala de cómputo y así se pueda implementar un espacio específico para que los usuarios que tengan PC móvil puedan estar dentro de ésta utilizando la red y cubrir sus necesidades.
   Uno de los requerimientos importantes de los usuarios es que la información viaje con toda la seguridad posible, es decir, que se tenga una confidencialidad, integridad de los servicios, etcétera.
   La adaptabilidad es otro de los requerimientos que toma en cuenta ya que se debe tener la facilidad de adaptarse a nuevos requerimientos, esto es, que si la red cambia debe ser fácil la adaptación de la misma.
2. Aplicaciones: Como estas son para todos los usuarios que requieran de una red, es necesario que se cubran las mismas necesidades ya que por el momento sólo se utilizan algunas aplicaciones, como las que se mencionan a continuación:
   a) WEB: ésta involucra el acceso al equipo remoto, esperando que el tiempo de respuesta sea más rápido y seguro.
   b) Correo electrónico: no es necesario que el tiempo de respuesta sea rápido pero lo ideal es que la respuesta sea lo más eficiente posible.

2. Arquitectura: es uno de los principales requerimientos que se debe cumplir, ya que si no se cuenta con una buena arquitectura en el diseño de la red inalámbrica; no se va a poder brindar un servicio eficiente, también porque de acuerdo con la cobertura que la tecnología de WiMAX brinda, es más amplia de la que ya se cuenta en la sala de cómputo.

   Para que se tenga una gestión de la red más apropiada a las necesidades que se quieren cubrir deberá cumplir con varios elementos como los que a continuación se mencionan:

   a) Software de gestión que tiene que ser compatible con el sistema operativo de Windows XP en adelante, y Fedora 7 o posteriores.

      Esta herramienta debe permitir realizar las funciones como operar, mantener, y por supuesto administrar los recursos que se deben soportar.

   b) Los lineamientos del marco regulatorio en la implementación y operación para realizar la modulación de la banda ancha de la red.

   c) La interoperabilidad, ya que éste debe facilitar la conexión de una red LAN que ya existe, que con las necesidades que se tienen que cubrir se necesita una interconexión con los equipos de cómputo para que este servicio sea más eficiente.

- Demanda de la red: la demanda principal que se tiene en la sala es por parte de los estudiantes ya que durante el día ellos son los que solicitan el préstamo de los equipos, el cual debe ser capaz de cubrir todas las necesidades que se van presentando.

Al mismo tiempo debe tener una interactividad con los switches que están bridando el servicio que ya se está satisfaciendo.

Ya que se tienen cubiertos estos puntos, es necesario que se conozca la ubicación aproximada del área de cobertura para así cubrir el diseño de la red en la sala 1 de cómputo de UNICA.

ÁREA DE COBERTURA Y ESTRUCTURA DE LA RED

La red está conformada con una estación base, una suscriptora fija CPE y de diversos equipos de cómputo móviles, ya que éstas cuentan con su propia tarjeta de red inalámbrica con los requerimientos necesarios, es decir, la tarjeta de red está configurada para que pueda tener acceso al punto de acceso y con la velocidad de bits que requiere.

En la sala 1 de cómputo de UNICA se va a contar con la estación base y la suscriptora para que de acuerdo con la dimensión de la cobertura se brinde un servicio en todas las aulas de la misma sin que exista intermitencia en la comunicación. Si la Facultad de Ingeniería desea ampliar la red a las demás salas de cómputo o a otras áreas de la misma, es necesario que se integren más estaciones suscriptoras en las áreas deseadas.

El AP es para transmitir y recibir información para las estaciones de CPE que están dentro de la zona de cobertura, pues se encarga de asignar y controlar el ancho de banda para los usuarios. El AP está integrado por varias entenas, las cuales son las encargadas de transmitir por diferentes caminos y así mejorar la recepción y transmisión de la información.

Con el CPE se puede originar una comunicación adecuada con los usuarios finales, los cuales se encuentran conectados al canal de comunicación ya sea de voz, de datos; esto es para tratar de evitar cualquier vulnerabilidad, ataque, etcétera, que se pueda generar. También es para que se cuente con la seguridad adecuada en la transmisión de los datos.

Las tarjetas estarán integradas por los usuarios finales que deseen contar con el servicio en las PC móviles ya que en la sala 1 de cómputo ya se tendrán integradas dichas tarjetas en algunos equipos para así disminuir las necesidades de los usuarios, mientras se encuentran dentro del radio de cobertura.

La red que saldrá del CPE se va a configurar para que sea el punto en específico y vaya a la estación base que va fungir como un multipunto, esto es para que se mantenga una adecuada seguridad en la transmisión de la información, una comunicación adecuada y se puedan cubrir todas las aulas de la sala.

La estación base se encontrará en el exterior de la sala 1 de cómputo de UNICA, para que se disperse mejor la comunicación y el CPE se encontrará dentro de la misma para que se cubra con las expectativas de los servicios.

El AP que se solicita para el diseño de la red es configurable para la tecnología de WiMAX con el objetivo de lograr una mejor comunicación y con la seguridad necesaria para que la información llegue al destino final sin ningún tipo de daño.

Con esto se mejorará y se actualizará la red cableada que se encuentra dentro de la sala 1 de cómputo, brindando servicio a todos los alumnos de la facultad.

La ubicación de los puntos es sencilla ya que solo se necesita una antena de AP al exterior de la sala y el CPE debe estar en el interior de la misma (sala 1 de cómputo), en la figura 6.4 se muestra cómo deben estar colocados ambos puntos para que se logre una cobertura adecuada tanto al exterior como al interior y así mejorar el servicio que se está brindando.

Para este diseño de la red inalámbrica y por las características de donde se encuentra el BS y en donde se encontraría el CPE es necesario que se ocupe la característica de línea de vista LOS.

Dentro de las condiciones y en el medio ambiente que se quiere realizar el diseño es necesario que se realicen los cálculos de cómo es que va a llegar la comunicación a la estación receptora que se encuentra en la sala 1 de UNICA que está ubicada en el edificio principal de la Facultad de Ingeniería.

Esto es por la ubicación ya que se encuentra la antena a 580 metros del edificio principal de la Facultad de ingeniería.

El edificio en donde se va a encontrar el CPE va a estar a una altura de 15 metros.

Se realiza el modelo en donde se encontrará la BS, la cual está ubicada en DGTIC (Dirección General de Cómputo y de Tecnologías de Información y Comunicación) y el CPE se encontrará en el edificio donde está la sala 1 de UNICA, la primera parte es de un punto a un

multipunto entre la BS y la estación suscriptora (SS), solo va a llegar a un equipo de cómputo que es el servidor (Figura 4.8)

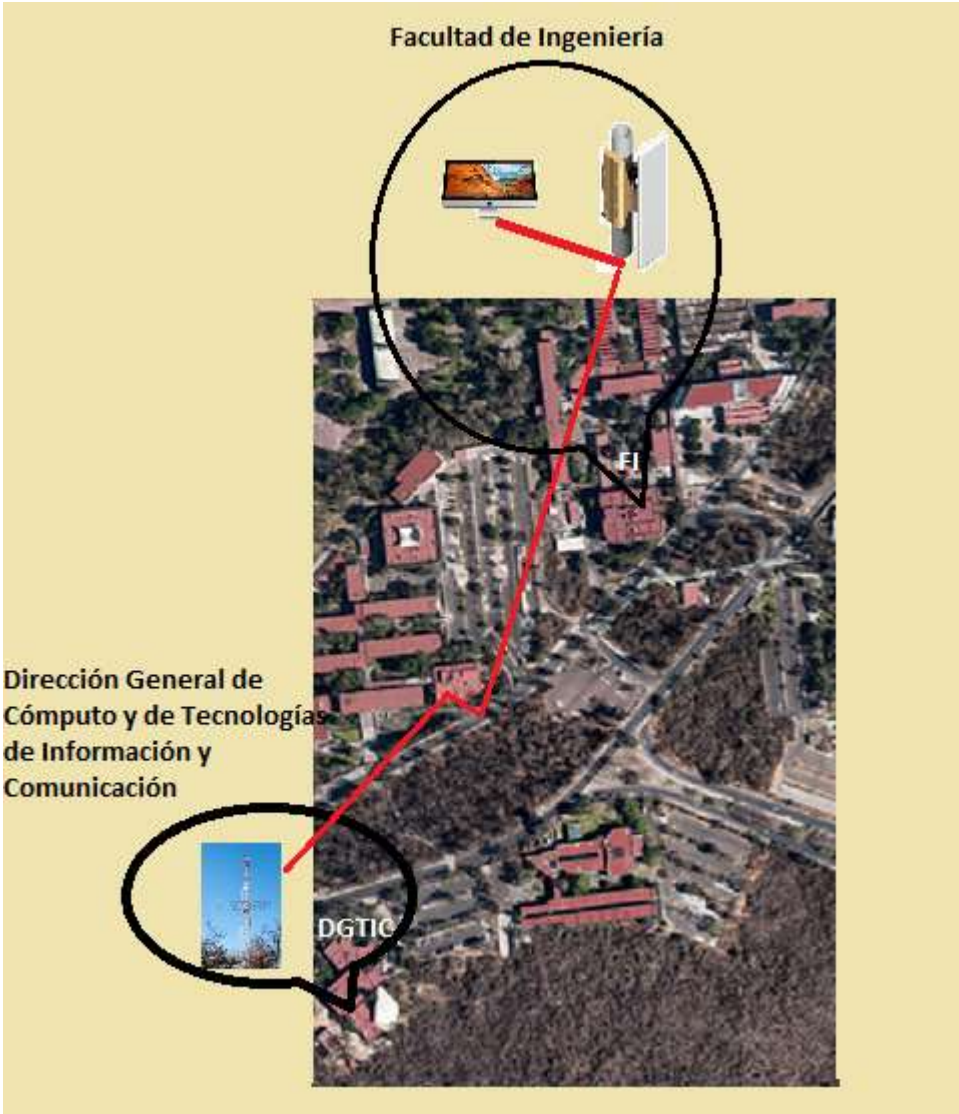


Figura 4.8 Mapa de conexión de la Red

Después de que se realice la conexión al servidor este es el encargado de mandar la información al switch para que sea el que proporcione los servicios a los usuarios (Figura 4.9).

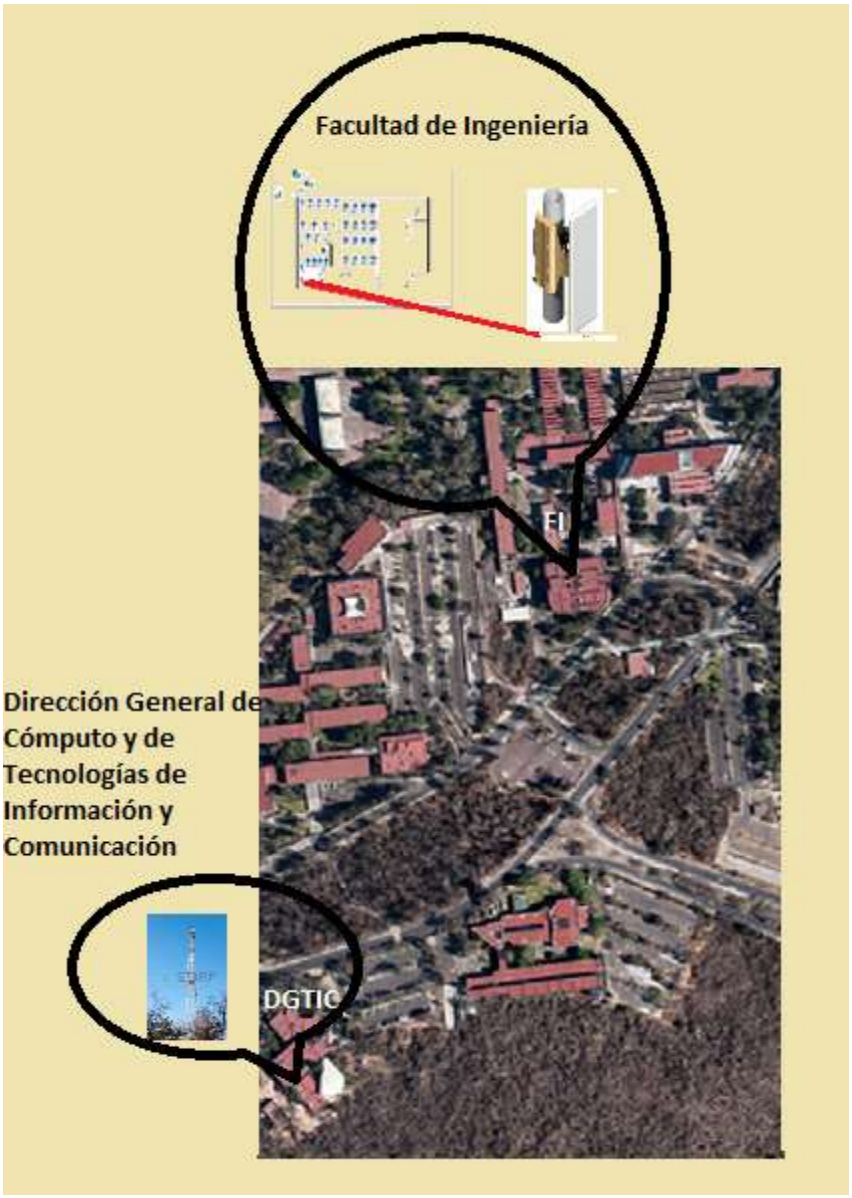


Figura 4.9 Detalle de la conexión

Ya con estas características del escenario que se va a ocupar, es necesario que se realicen las condiciones técnicas de comunicación, para saber qué tipo de línea de vista es más adecuada con base en cómo se encuentra la zona del diseño, por lo que se muestran tres tipos de modelos de línea de vista para que se observe la diferencia entre cada uno de ellos.

Se utiliza el software linkBudget, que con ayuda del mismo se realizarán tres modelos diferentes para poder decidir cuál sería el adecuado por el tipo de terreno en donde se desarrolla el diseño y la transmisión de los datos por medio de un espacio abierto.

Se toma en cuenta la pérdida de propagación que no se encuentre a más 3 dB, esto es porque de lo contrario la información que llegue al receptor será la mínima y no se tendría una comunicación adecuada.

Los datos que se ingresaron en linkBudget son:

- Distancia: 0.58 [Km]
- Altura de la antena: 30 [m]
- Altura del receptor: 10 [m]
- Según fuera el caso qué tipo de línea de vista se iba a utilizar.

En las figuras 4.10, 4.11 y 4.12 se encuentra la pérdida de propagación en un rango de 3 [dB] la cual se encuentra encerrada en color rojo

En la tabla 4.5 se describe cada parámetro de las figuras 4.10, 4.11 y 4.12

4.5 Descripción de parámetros

PARÁMETRO	DESCRIPCIÓN
Transmisión	
Frequency (Frecuencia)	Está sujeta una banda que necesita licencia.
ODU Tx Power	Potencia de transmisión de la Unidad Exterior de Radio
Tx Antenna Gain	La ganancia de la transmisión de

	la antena
Tx Implementarion Loss	Es la pérdida de transmisión en la implementación
EIRP	Es un canal que limita en cualquier momento transmisión.
Propagación	
Range	Es la distancia que se va a transmitir.
Path Loss	Son los datos que se pierden en el camino en decibeles
Perfil de enlace	
Modulation/Coding Rate	Selección automática de BPSK , QPSK , 16 QAM , 64 QAM , Forward Error Corrección y velocidades de codificación : convolucional Turbo Codificador / decodificador con una tasa de 1/2 , 3/4 y 2/3
Minimum Requiered CINR	Son los requerimientos mínimos de la medida de la estación base, basándose en la señal que se pierde en el camino.
Expected Channel Throughput	Canal de espera de transmisión

Max Unidirectional Throughput	Es el máximo rendimiento unidireccional que se tiene del perfil de enlace.
Receptor	
Receiver Antenna Gain	Receptor de la ganancia que se tiene de la antena.
Rx Implementation Loss	Es la pérdida de recepción en la implementación
RSSI	Es el valor del indicador de la intensidad de la señal recibida medida basada en la señal recibida de este abonado.
Threshold at BER = 10^{-6}	Es el umbral
Fade Margin	Es el margen de desvanecimiento que debe ser incluido para anticipar las fluctuaciones.
Ajustes	
Antenna Height (m)	Altura de la antena
Antenna Gain (dB)	Ganancia de la antena
Fade Margin	Margen de desvanecimiento
Disable Automatic Tx Power Adjustment	Desactivar el ajuste automático de potencia de Transmisión.
Disable Automatic Antenna	Desactivar las alturas

Heights	automáticas de la antena
Measures Units	Unidades de medida
Pathloss Model	Modelo de pérdida de propagación
SS Type	Es el tipo de instalación que se puede realizar.

1) Tipo de vista NLOS tipo A: este tipo se utiliza para zonas montañosas o pobladas, es decir, para zonas urbanas. (Figura 4.10)

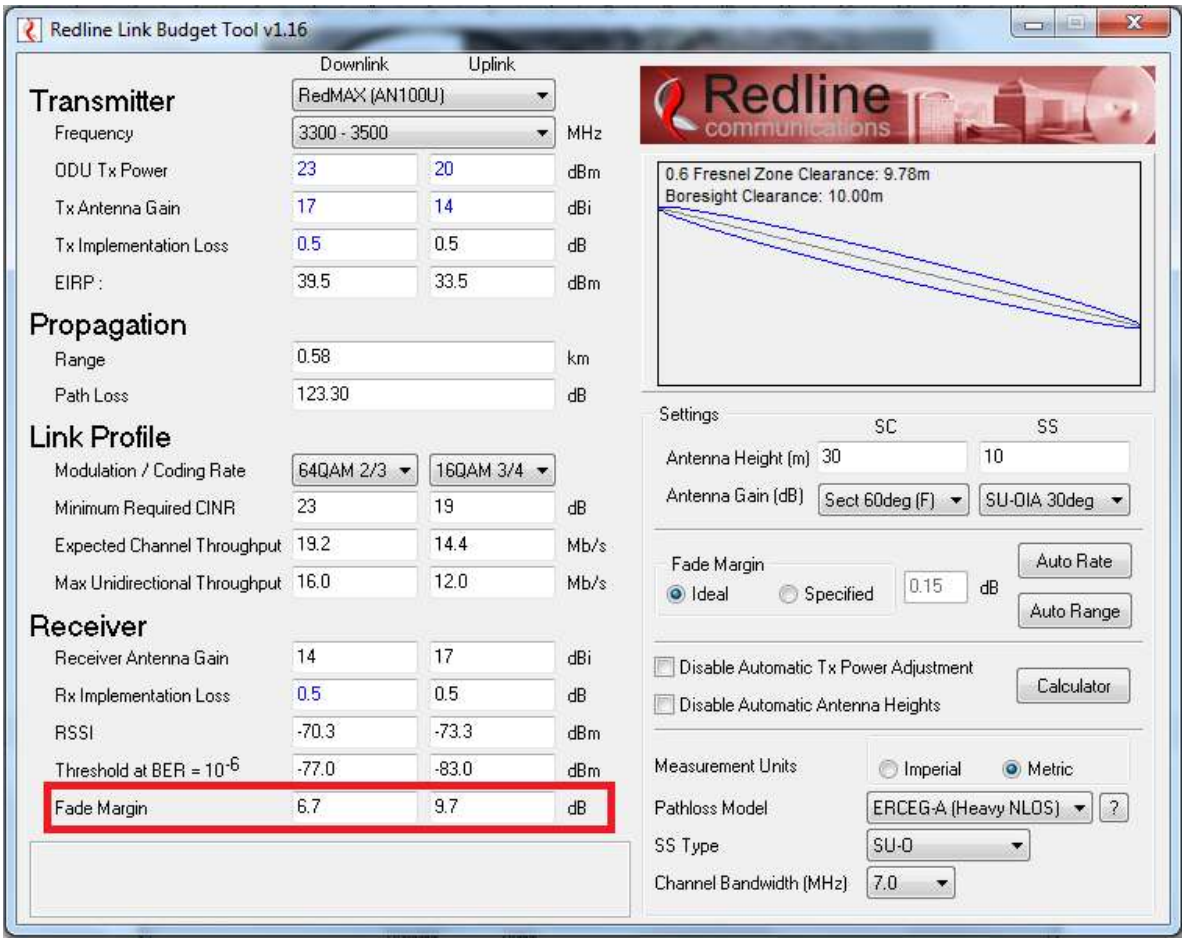


Figura 4.10 Línea de vista NLOS tipo A

2) Línea de vista NLOS tipo B: es para los casos en donde no existe tanta población, es decir, para zonas semi – urbanas (Figura 4.11).

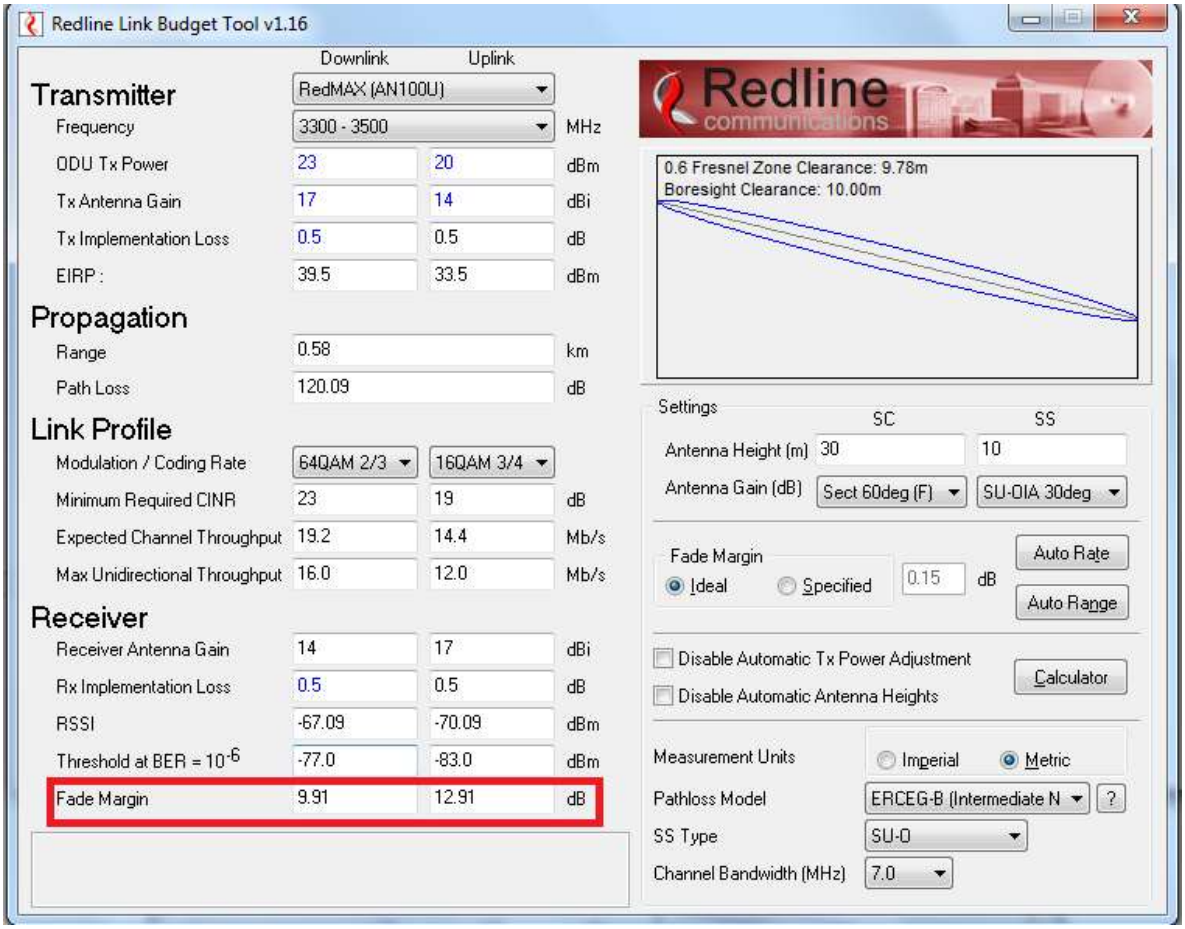


Figura 4.11 Línea de vista NLOS tipo B

3) Línea de vista NLOS tipo C: es para un terreno que se encuentra totalmente despejado, como se muestra en la (Figura 4.12)

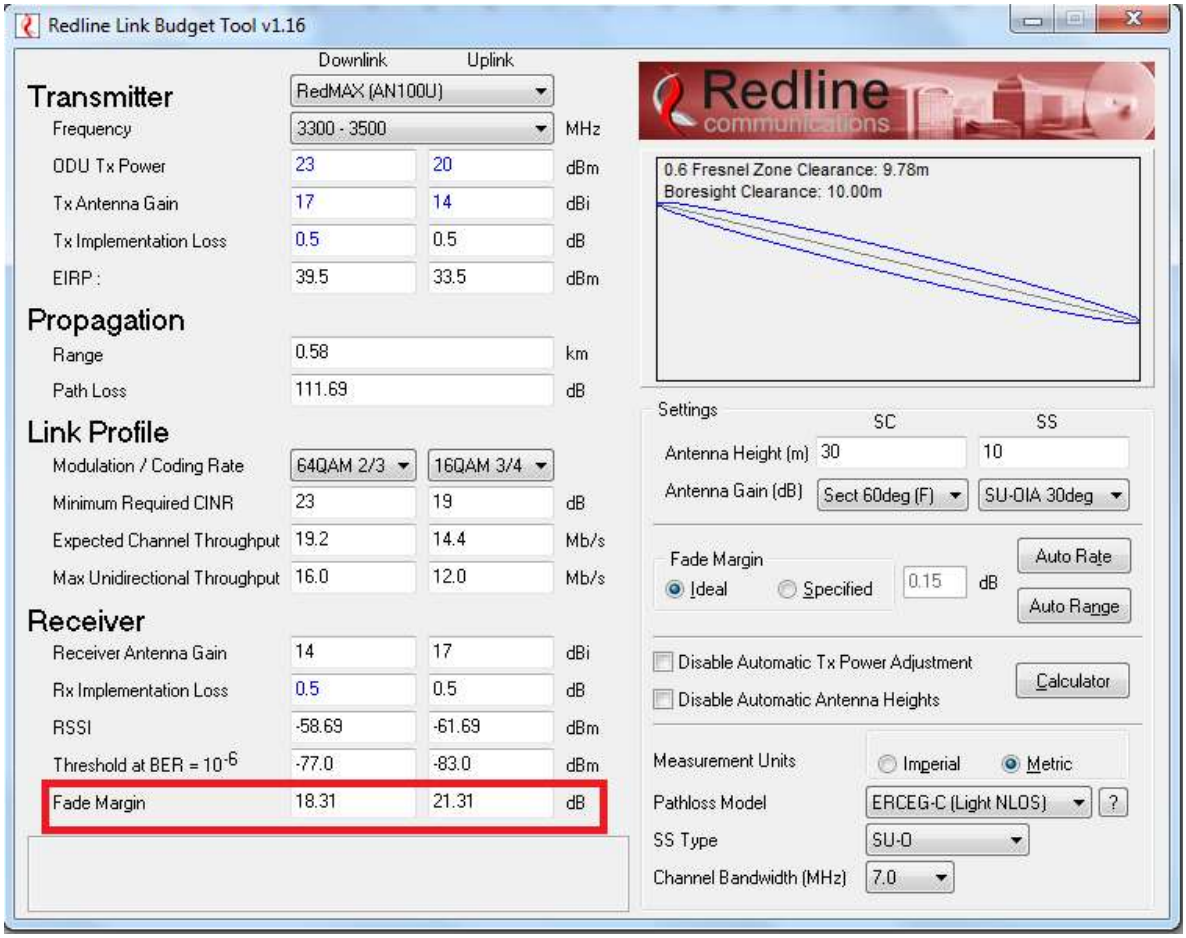
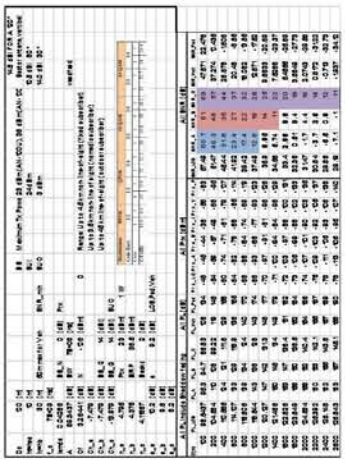


Figura 4.12 Línea de vista NLOS tipo C

Ya que se tiene el resultado de la línea de vista NLOS, para este diseño es necesario que se tome el tipo A ya que el área en la que se realiza el diseño es una zona con una gran cantidad de edificios, así como de vegetación.

Se hace una comparación en la tabla 4.6 de la potencia de propagación que se tiene entre los tres tipos para saber cuál es la que tiene menos pérdida de potencia en la transmisión de los datos, que son los que se encuentran de color, es decir, la que se encuentra de color morado tipo C, color rojo es el tipo B y finalmente la color azul es tipo A, ésta última se empleará para este diseño, se observa que existe menos pérdida en un terreno urbano, ya que la distancia en metros es de 1200 [m].

Tabla 4.6 Modelo de propagación



En la tabla 4.6 que es el modelo de propagación se pueden observar tres tipos de colores en donde se muestra un rango de ruido que puede existir en la transmisión de los datos de acuerdo a la distancia.

En las 4.13 y 4.14 se muestran los diferentes comportamientos de la pérdida que se tendrá en el camino de transmisión, es decir, como la transmisión es abierta, proporciona cuánta información se puede perder de acuerdo a como vaya creciendo la distancia

En las figuras 4.13 y 4.14 se muestra cómo es la pérdida de los paquetes en los tres tipos de línea de vista de NLOS así como en la línea de vista de LOS.

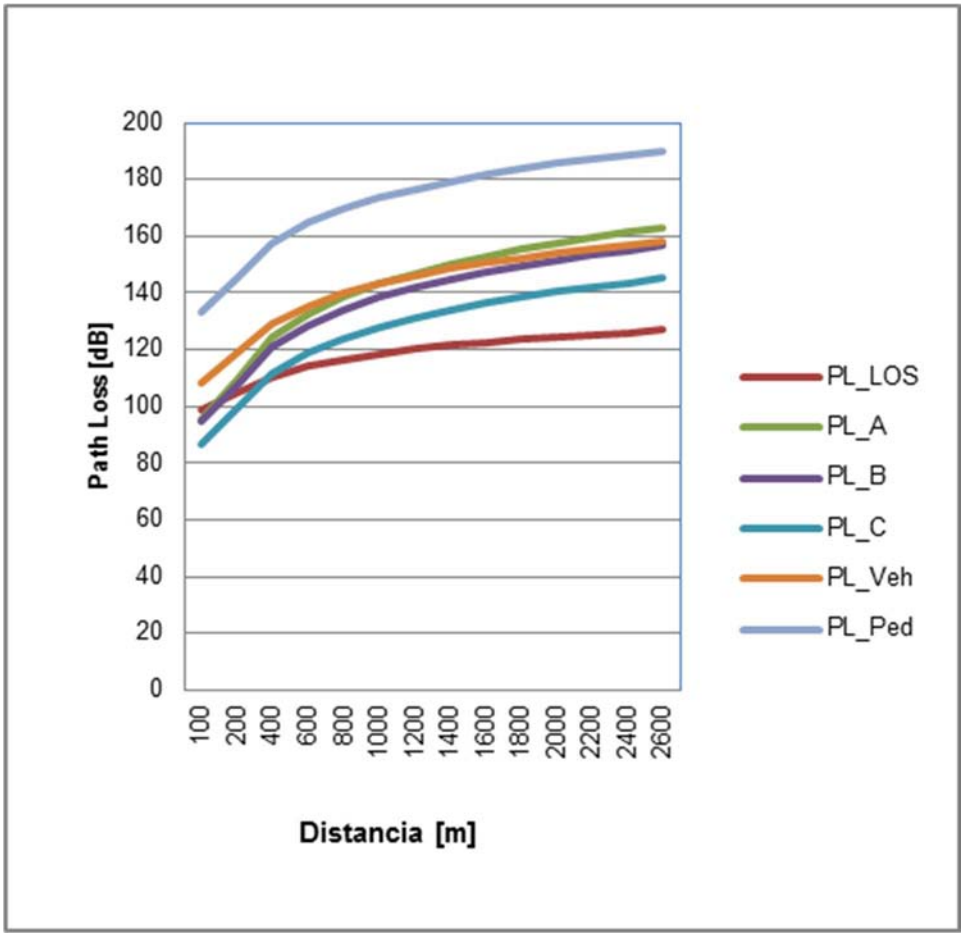


Figura 4.13 Camino perdido

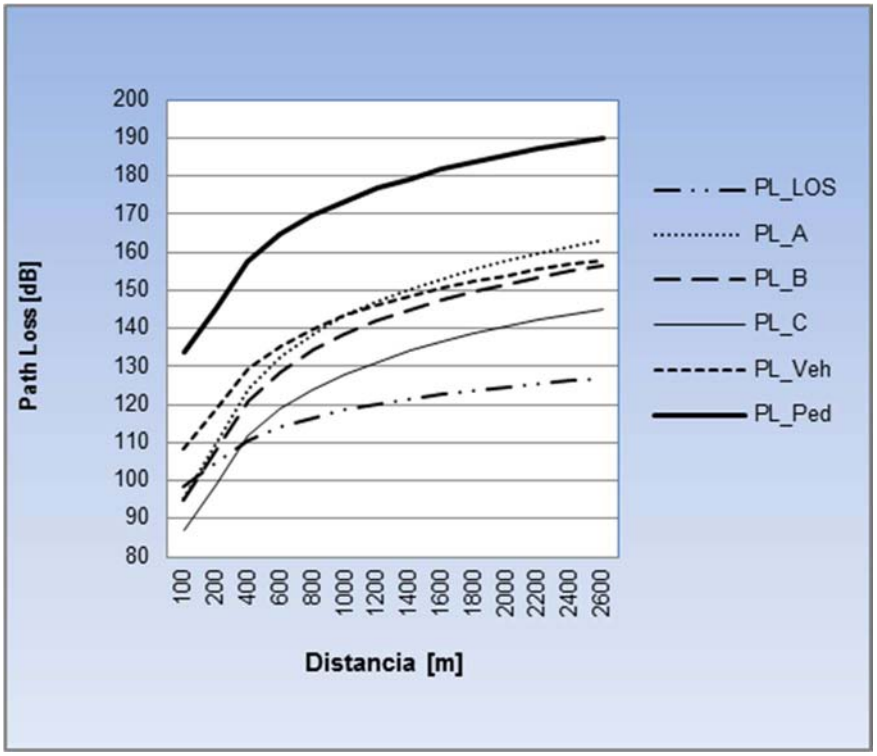


Figura 4.14 Camino perdido

Las figuras 4.15 y 4.16 representan a la información que va a llegar a la SS desde la BS

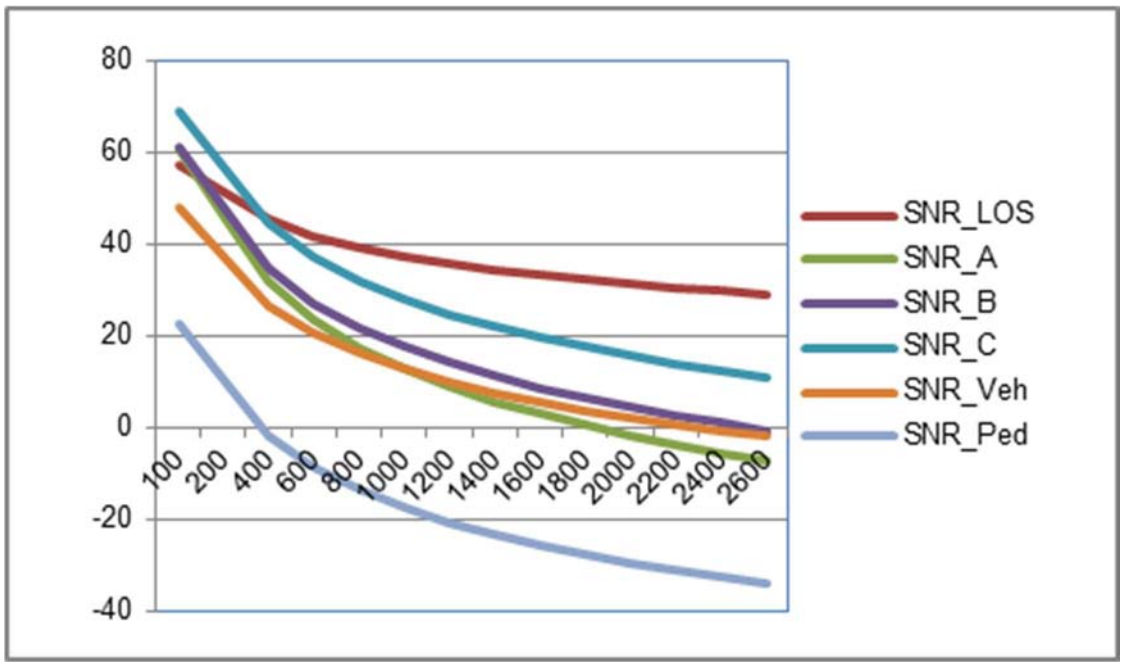


Figura 4.15 Llegada de información

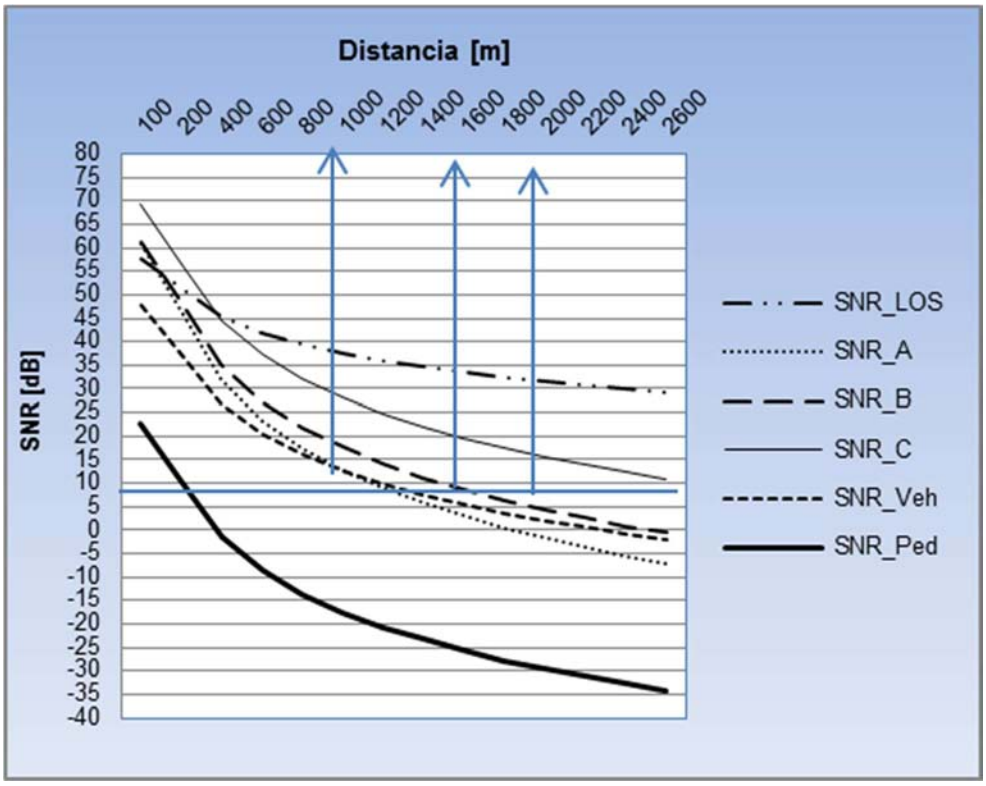


Figura 4.16 Llegada de información

Con base en los resultados, la línea de vista que se utilizará será NLOS tipo A, ya que es conveniente por el tipo de zona en la que se diseña la red. También es la que cuenta con mejor comunicación y mayor envío de información.

CONFIGURACIÓN DE PC

Después de que se realiza la conectividad será necesario ejecutar las pruebas de conectividad para saber si existe comunicación entre los diferentes dispositivos de la red que se está diseñando, por lo que se revisan los siguientes puntos:

1) Firewalls: en los equipos tendrá que estar desactivado para que no bloquee la comunicación de forma local.
2) Software: el software que se ocupa para la seguridad, como los antivirus, malware, anti-spywares, etc., debe estar desactivado ya que puede impedir la conexión remota hacia otros equipos.
3) Segmento: es necesario que todos los equipos se encuentren en el mismo segmento de red, es decir que la SS, BS y los equipos que van a tener comunicación formen parte de la misma subred.
4) Verificar conectividad: es necesario que se verifique la comunicación ya sea con una tracer o un ping entre los equipos.

CALCULO TEÓRICO DE TASA DE TRANSMISIÓN

Para realizar este cálculo es necesario que se cuente con el Orthogonal Frequency Division Multiplexing--Multiplexación por División de Frecuencias Ortogonales (OFDM), el cual es un mecanismo de modulación que está ideado para evitar la interferencia entre los símbolos consecuencia de una propagación de multitrayectos que es característico de los medios inalámbricos.

Es como una matriz en donde se muestra el tiempo y los símbolos que se alojan, esto es el eje horizontal y en el eje vertical se muestra la frecuencia, donde se alojan las subportadoras, como se muestra en la figura 4.17.

Para poder encontrar el enlace de transmisión es necesario que se encuentre el número de símbolos que se transmiten por el canal.

Figura 4.17 OFDM [8]

[8] (26 de 04 de 2016). Obtenido de OFDM: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-40/112-WiMAX.html

En la figura 4.18 se muestra la estructura de la frecuencia de un símbolo OFDM.

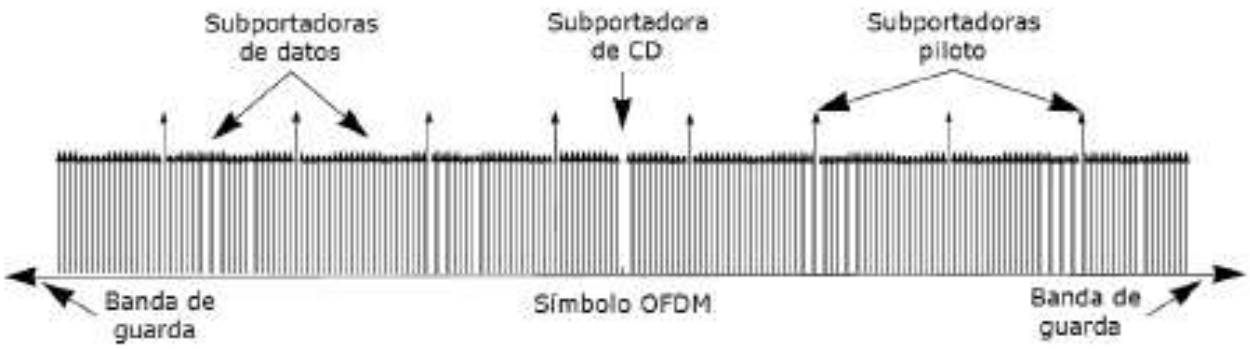


Figura 4.18 Frecuencia de un símbolo de OFDM [9]

En la tabla 4.7 se muestran el tamaño de los campos que se toman en cuenta para realizar los cálculos teóricos de la transmisión

Tabla 4.7 Tamaño de los campos de control

Tipo	Cantidad	Función
Piloto	8	La sincronización de la capa física (PHY)
Banda de guarda	55 (17 inferior y 28 superior)	Para prevenir la inferencia entre los canales de transmisión adyacentes
Nula (D)	1	Indica la frecuencia de referencia para el canal central (frecuencia central)
Datos	192	Cuántos datos se van a transmitir
Total	256	

[9] Frecuencia de un símbolo OFDM. (s.f.). Obtenido de Frecuencia de un símbolo OFDM: http://132.248.9.195/ptd2009/junio/0644574/Index.html

En la tabla 4.7 se tiene 256 portadoras en total en una transmisión de datos de 192 que estarán disponibles.

Para las nuevas redes inalámbricas se utiliza división de tiempo (TDD) o división de frecuencia (FDD) en ambos casos es dúplex asignación de recursos de una interfaz de aire como es el caso de este diseño de red.

"En TDD, las transmisiones de enlace ascendente y descendente se realizan sobre las mismas frecuencias portadoras y la separación entre las direcciones de transmisión se realiza mediante la asignación de intervalos de tiempo, en el que está prevista la transmisión de una dirección a la vez. En FDD, las transmisiones de enlace ascendente y descendente se realizan simultáneamente en diferentes frecuencias portadoras." [10]

Es común que en las redes inalámbricas WiMAX se utilice el TDD que permite que se compartan de manera más flexible el ancho de banda que se encuentre disponible.

Una trama TDD se divide en dos subtramas:

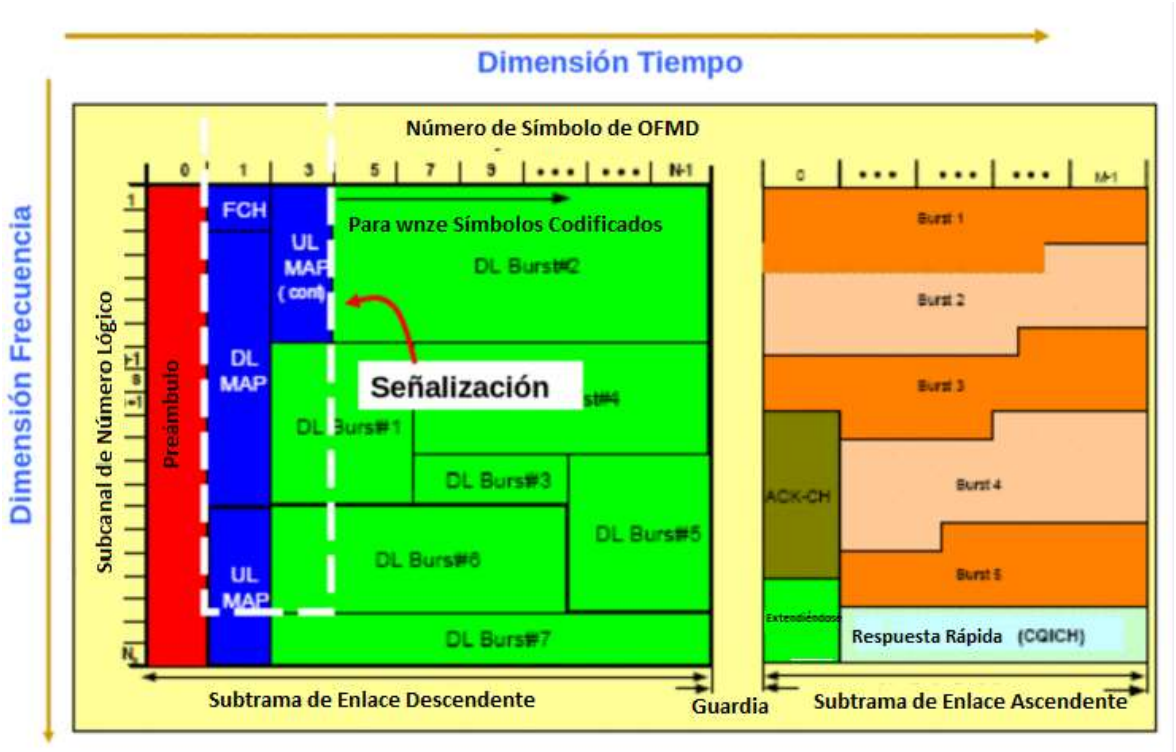
1) Enlace descendente: es un intervalo corto llamado transmisión/recepción de transición (TTG).

   Inicia con un preámbulo, que sirve para la sincronización y la estimación del canal, así mismo sirve para mejorar la tolerancia frente a las degradaciones de transmisión de datos por el canal de movilidad-infligida.

[10] (26 de 04 de 2016). Obtenido de OFDM: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-40/112-WiMAX.html

2) Enlace ascendente: se encuentra en la misma banda de frecuencia.

"WiMAX permite el soporte opcional para una repetición de preámbulo más frecuente durante la transmisión. En el enlace ascendente, preámbulos cortos, también llamados partes intermedias, se pueden utilizar después de 8 símbolos, 16 o 32 de OFDM y en el enlace descendente, preámbulos cortos en frente de cada ráfaga de datos se pueden utilizar. Después del preámbulo viene un marco de encabezado de control (FCH), que consiste en mensajes de enlace ascendente y de enlace descendente Protocolo de Acceso al Medio (MAP), que informa a los usuarios acerca de sus parámetros de transmisión. (Figura 4.19)" [11]



4.19 Diagrama de frame OFDM [12]

[11 y 12] (26 de 04 de 2016). Obtenido de OFDM: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-40/112-WiMAX.html

Para el caso de DL Map se tiene un promedio de 4 bytes lo que es correspondiente a las diferentes ráfagas de datos dentro de una trama de 8 bytes. Así mismo para el UL Map son 40 bytes por cada 8 bytes, los 7 bytes que restan tienen información que corresponde al canal del ID, tiempo del mensaje, etc.

A continuación se realizan los cálculos teóricos para ver la transmisión de los datos.

Tabla 4.8 Cálculos teóricos

Campo de control	Tamaño
Preámbulo	1 simb
FCH (Frame Control Header—Marco de encabezado de control: es la duración de un símbolo OFDM)	1 simb
Ranging (envía cuando la SS se quiere registrar en la BS)	2 simb
Contención	5 simb [UL frame]
DL Map	24 bytes (QPSK ½, DL frame)
UL Map	47 bytes (QPSK ½, DL frame)
TTG	4 símbolos + 35 [us] + t_p[4]
RTG	4 símbolos + 35 [us] + t_p

Cálculos para ver cuánta tasa de transferencia hay.

Datos generales:

- Distancia: 100 [m]
- Altura de la antena: 30 [m]
- Altura del edifico: 15 [m]
- Frame OFDM (subportadoras): 256
- Frecuencia central: 3.3 [GHz] o 3300 [MHz]

- Ancho de banda del canal (BW): 7 [MHz]

1) Se calcula el espacio entre las portadoras para cada uno de los símbolos

   Δf: Frecuencias sub-portadoras

   $\Delta f = \frac{\text{BW}}{\text{subportadoras (OFDM)}}$

   $\Delta f = \frac{7000\ [\text{KHz}]}{256} = 27.34\ [\text{KHz}]$…… (1)

   Si se considera un factor de muestreo, es decir, n=8/7 por el ando de banda que se va a utilizar

   $f_s = n \cdot \Delta f$

   $f_s = (8/7)(27.34\ [\text{KHz}]) = 26.67\ [\text{KHz}]$……..…..(2)

2) Se tiene que calcular el duración del símbolo OFDM, con lo que se obtuvo en la ecuación 2

   $T_d = \frac{1}{\text{fs}}$

   $T_d = \frac{1}{26.67\ [KHz]} = 37.495\ [\frac{\text{us}}{\text{simb}}]$…… (3)

   Tomando en cuenta que la eficiencia del canal es de ¼, se calcula el tiempo total del símbolo OFDM.

   $T_s = T_d + ¼ \cdot T_d$

   $T_s = 37.495\ [\text{us}] + ¼(37.495[\text{us}]) = 46.868\ [\frac{\text{us}}{\text{simb}}]$……. (4)

3) Con la duración de uno de los símbolos se podrá obtener cuántos símbolos viajan por el frame

   Frame = 10 [ms]

   $\#\text{simb} = \frac{frame}{Ts}$

   $\#\text{simb} = \frac{10\ [ms/frame]}{46.868\ [us/simb]} = 213.36\ [\frac{simb}{frame}]$…… (5)

4) Se toma como referencia la siguiente tabla, para poder calcular el número de símbolos consumidos en cada frame

   TTG = 4 [simb] + $\frac{35\ [us]}{46.868[us/simb]}$ = 4.746 [simb] …… (6)

   RTG = 4 [simb] + $\frac{35\ [us]}{46.868[us/simb]}$ = 4.746 [simb] …… (7)

   Para obtener los símbolos consumidos

   Total = TTG + RTG

   Total = 4.746 + 4.746 = 9.49 [simb]

   Total ≈ 10 [simb] …… (8)

5) Para el frame DL se toman los campos de DL Map y UL Map, los cuales transmiten QPSK ½ el número de bits que se envían, así como las subportadoras

   UL Map = 47 [bytes] · 8 [$\frac{bits}{Bytes}$] = 376 [subportadoras]… (9)

   Dl Map = 24 [bytes] · 8 [$\frac{bits}{Bytes}$] = 192 [subportadoras]…. (10)

   Una Bs no utiliza una subcanalización, es decir, que todas las portadoras se van por un solo canal, tomando en cuenta que UL Map utiliza 2 símbolos mientras que DL Map solo uno.

6) Se calculan los símbolos útiles con los resultados obtenidos en las ecuaciones (5) y (8)

   $simb_{utiles}$ = # simb – Total

   $simb_{utiles}$ = 213.36 – 10 = 203.36 [simb]

   $simb_{utiles}$ ≈ 203 [simb] …… (11)

7) Con la ecuación (11) y tomando en cuenta la misma distribución de símbolos que se ocupan en la BS que es del 56% en DL y 44% UL

$simb_{ÚtilesUL} = simb_{utiles} * 0.44$

$simb_{ÚtilesUL} = 203 * 0.44 = 89.32$

$simb_{ÚtilesUL} \approx 89$ [simb]…….. (12)

$simb_{ÚtilesDL} = simb_{utiles} * 0.56$

$simb_{ÚtilesDL} = 203 * 0.56 = 113.68$

$simb_{ÚtilesDL} \approx 114$ [simb]…….. (13)

8) Podremos obtener los símbolos que se utilizaran para transmitir en el canal, asi como la tasa de transmisión que encuentra en PHY

$simb_{DatosUL} = simb_{ÚtilesUL} - RG - CT$

$simb_{DatosUL} = 89 - 2 - 5 = 82$ [simb] …….. (14)

$simb_{DatosDL} = simb_{ÚtilesDL} - PB - FCH - UL_{MAP} - DL_{MAP}$

$simb_{DatosDL} = 114 - 5 = 109$ [simb] …….. (15)

Donde:

RG: es el símbolo de ranging

CT: símbolo de contención

PB: símbolos de preámbulo

9) Con las ecuaciones (14) y (15) se calcular~~a~~ la tasa de transmisión

$R_{UL} = SD * M * CC * simb_{DatosUL} * \#frames$

$R_{UL} = 192(6)\ (3/4)\ (44)\ (100) = 3.8$ [Mbps]…….. (16)

$R_{UL} = 192(6)\ (3/4)\ (60)\ (100) = 5.18$ [Mbps]…… (17)

Donde:

SD: número de subportadoras

M: número de bits de la subportadora

CC: la tasa de codificación total

#frames: son los frames por segundo para una duración de 10 [ms], por cada frame

10) La tasa de transmisión en las ecuaciones (14) y (15) está localizada en la capa física, para poder calcular la tasa en las capas de nivel de enlace (2), red (3) y transporte (capa 4), es necesario que se cuente con un analizador de protocolo que sirve para medir el tráfico en la red, es decir, 20 TCP, 20 IP, 18 MAC Ethernet y 6 MAC WiMAX, la suma total de los encabezados es de 64.

En el iPERF se tiene un tamaño de 1460 bytes en la capa de transporte de acuerdo con el encapsulamiento, está dado como:

$RE = \frac{1460}{1524} = 0.95$…… (18)

11) Para finalizar la tasa de transmisión teórica sería, la multiplicación de las ecuaciones (16), (17) y (18)

$R4_{UL} = 3.8\ [Mbps] \cdot 0.95 = 3.61\ [Mbps]$…….. (19)

$R4_{DL} = 5.18\ [Mbps] \cdot 0.95 = 4.92\ [Mbps]$…….. (20)

$R_{total} = R4_{UL} + R4_{DL}$

$R_{total} = 3.61 + 4.92 = 8.53\ [Mbps]$……. (21)

CONCLUSIÓN

CONCLUSIÓN

El objetivo de este trabajo es colocar las bases de una nueva tecnología de red inalámbrica con mayor velocidad para los estudiantes en un centro de cómputo que ya cuenta con una red alámbrica.

Por lo que fue necesario ver las necesidades de los estudiantes de la Facultad de Ingeniería en específico de la zona del edificio principal, la biblioteca ya que es esta área en donde se llevó a cabo el estudio de las necesidades para que los estudiantes cuenten con una tecnología actual.

Esta decisión de que el diseño de la red fuera en una sala de cómputo de UNICA se debe a que es una de las salas más pequeñas y con una demanda mayor a la de su capacidad, tanto en red inalámbrica como en la alámbrica. Aunado a que se encuentra en una zona en la que los estudiantes se encuentran con más frecuencia, lo cual lleva a que utilicen más las redes inalámbricas, tanto por el uso de sus teléfonos celulares como por computadoras portátiles, así que con la nueva tecnología no va a estar tan saturada la banda ancha como en la actualidad.

También se tomó esta decisión porque en algunas aulas ya se imparten clases por medio de computadoras y es necesario que las mismas tengan acceso a la red.

Con la investigación que se llevó a ~~a~~cabo de la red inalámbrica con la tecnología WiMAX se tiene el respaldo de que va a hacer una excelente inversión de comunicación.

Cabe mencionar que tomando en cuenta la demanda que existe en la actualidad de personal que se encuentra en la Facultad de Ingeniería y los equipos que tiene la sala de cómputo que se encuentra en el edificio principal no cubren la demanda solicitada por los alumnos, por lo que se realizó un diseño de red inalámbrica para el uso de los equipos móviles, y así todo el personal que cuenta con un equipo de este tipo pueda tener comunicación y pueda realizar sus actividades sin problemas.

Este escrito es sólo un diseño para la creación de una red inalámbrica WiMax la cual está orientada para el edificio principal de la Facultad de Ingeniería, y que podría servir como base para la creación de la misma. Se tomó la decisión de realizar el diseño en este edificio ya que se cuenta con una mayor demanda de personas y es posible que porten un equipo móvil y tengan la necesidad de conectarse a la red, aunado a que existen menos equipos disponibles para el uso de los alumnos.

APÉNDICE A

FIREWALL

APÉNDICE A FIREWALL

Un Firewall es un dispositivo que funciona como cortafuegos entre las redes, permitiendo o denegando las transmisiones de una red a la otra.

Es necesario que se encuentre entre una red local y la red de Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial, para que sea un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que permite o deniega para el paso de información. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo, etc. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación son entrante o saliente y dependiendo de su dirección puede que lo permita o no.

De este modo un firewall permite desde una red local hacia Internet servicios de web, correo y ftp.

Se configuran los accesos que se hagan desde Internet hacia la red local y se deniega todos o se permitir algunos servicios como el de la web, (si se posee un servidor web y se necesita acceso a Internet). Dependiendo del firewall que se tenga se puede permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparato que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso se pueden encontrar ordenadores de

cómputo muy potentes y con el software específico que lo único que hace es monitorear las comunicaciones entre redes.

Para lo cual existen dos tipos de firewall los cuales son:

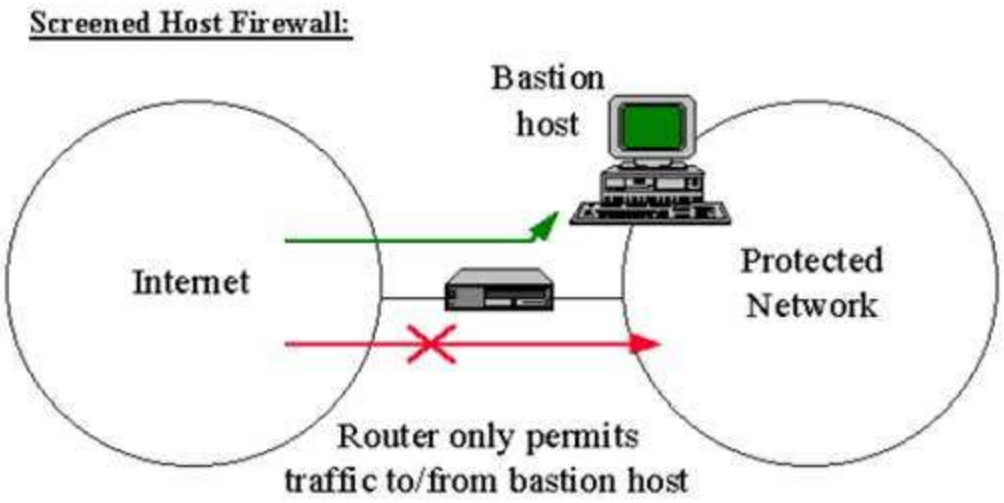
a) Firewall a nivel de aplicación:

Por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una elaborada auditoria y verifican el tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT, debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original. Este tipo tiende a proveer una auditoría más detallada.

b) Firewall a nivel de red:

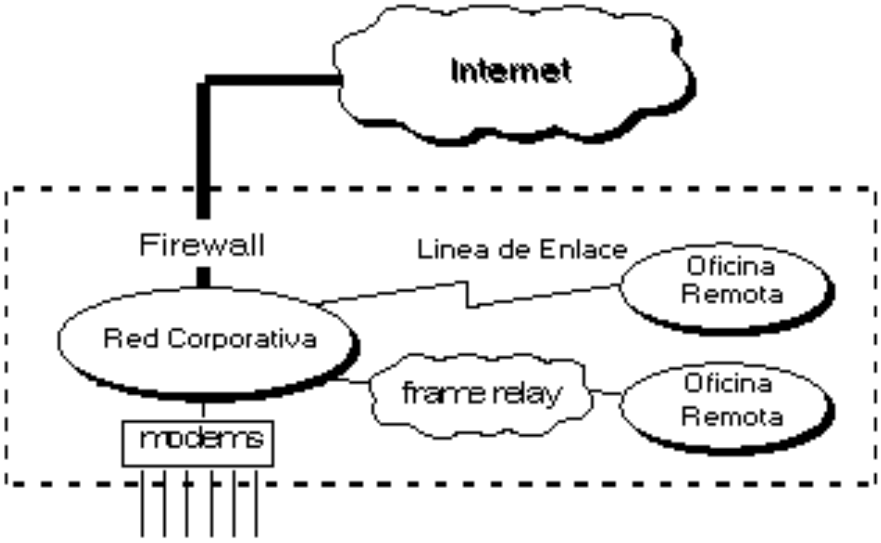
Este firewall toma decisiones según la dirección de procedencia, la de destino y puerto de cada uno de los paquetes IP. Un simple router es un ejemplo de firewall de nivel de red, con la deficiencia de que no pueden tomar decisiones sofisticadas. Los actuales firewall o como se le conoce también corta fuegos de nivel de red permiten mayor complejidad a la hora de decidir; mantienen información interna acerca del estado de las conexiones que pasas por él, los contenidos de algunos datos. Estos sistemas, como es lógico han de tener una dirección IP valida. Los firewalls tienden a ser muy rápidos, y sobre todo, transparentes al usuario. Como se muestra en la figura 1.1

Figura 1.1



Después de que se tiene elegido que tipo de firewall es que se va configurar es necesario que se creen políticas de seguridad esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda, como se muestra en la figura 1.2.

Figura 1.2



Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados como hackers, crakers, vándalos, y espías, fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Para lo que es necesario que se tengan las siguientes características:

1) Concentra la seguridad Centraliza los accesos
2) Genera alarmas de seguridad Traduce direcciones (NAT)
3) Monitorea y registra el uso de Servicios de WWW y FTP.
4) Internet.

GLOSARIO

GLOSARIO

3DES:

Data Encryption Standard - Estándar de cifrado de datos: En criptografía, tipo de algoritmo que realiza un triple cifrado tipo DES, esto lo hace muchísimo más seguro que el cifrado DES simple. Fue desarrollado por IBM en el año 1978.

ADSL:

Asymmetric Digital Subscriber Line - Línea de Abonado Digital Asimétrica. Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado.

AES:

Advanced Encryption Standard - Estándar Avanzado de cifrado es el nuevo estándar de criptografía simétrica adoptado en el FIPS.

AP:

Access Points - Puntos de Acceso: son dispositivos que se interconectan con otros dispositivos de comunicación inalámbrica para formar una red inalámbrica, también puede conectarse una red cableada y puede transmitir datos entre los dispositivos inalámbricos, a su vez pueden conectarse entre sí para formar una red aun mayor, permitiendo realizar "roaming" (movimiento de una zona de cobertura a otra). Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para que se puedan configurar.

ARCNET:

Arquitectura de red de área local que utiliza una técnica de acceso de paso de testigo como el Token Ring. Tiene una topología física en forma de estrella, utilizando cable coaxial y hubs pasivos o activos. Fue desarrollada por Datapoint Corporation en el año 1977.

Transmite a 2 megabits por segundo y soporta longitudes de hasta 600 metros. Actualmente se encuentran en desuso en favor de las Ethernet.

Arquitectura de red de área local desarrollado por Datapoint Corporation que utiliza una técnica de acceso de paso de testigo como el Token Ring. La topología física es en forma de estrella mientras que la topología lógica es en forma de anillo, utilizando cable coaxial y hubs pasivos (hasta 4 conexiones) o activos.

BLUETOOTH:

Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.

- Eliminar cables y conectores entre éstos.

- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

BPS:

Bits per Seconds o Bits por Segundos. Unidad de medida para la cantidad de bits que se transfieren (entrada, salida o ambos) por segundo.

BS:

Servicio de radiodifusión

CBC (AES):

Es un método para implementar un algoritmo de cifrado por bloques, cuando se necesita descomponer el texto de entrada en bloques de longitud fija, por medio del Estándar de Cifrado Avanzado

CBC (DES):

Es un método para implementar un algoritmo de cifrado por bloques, cuando se necesita descomponer el texto de entrada en bloques de longitud fija, por medio del estándar de cifrado de datos

CCM (AES):

Acrónimo de Communication Control Module - Módulo de control de la comunicación

CCMP:

Es un protocolo de cifrado de IEEE 802.11i. CCMP significa Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Modo de contador con cifrado de bloque de protocolo de código de autenticación de mensajes en cadena

CDMA:

Code divison Multiple Access - Acceso Múltiple de División de Código. Norma de transferencia de información empleado por teléfonos inalámbricos.

CECAFI:

La Unidad de Servicios de Cómputo Académico de la Facultad de Ingeniería (UNICA) es resultado de la división del antiguo Centro de Cálculo (CECAFI), en 1994.

CONFIDENCIALIDAD:

Es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas.

CPE:

Customer Premises equipmet - Equipo Local del Cliente

DHCP:

Dynamic Host Confíguration Protocol - Protocolo de configuración dinámica de host. Protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.

DISPONIBILIDAD:

Es la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

DNI:

Documento nacional de identidad.

DOF:

Diario Oficial de la Federación

DS:

Data Synchronization - Sincronización de Datos

DSL:

Digital Subscriber Line - Línea de Abonado Digital. Tecnología que permite una conexión a una red con más velocidad a través de las líneas telefónicas

ESSID:

Extended Service Set ID - Conjunto de Servicio extendido de identificación es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

ETHERNET:

Define las características de cableado y señalización de nivel físico así como también los formatos de tramas del nivel de enlace de datos del modelo OSI. Ethernet es la red de área local (LAN) más ampliamente instalada tecnológicamente. Según lo especificado en un estándar, IEEE 802.3.

FDDI:

Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra: Topología de red local en doble anillo y con soporte físico de fibra óptica. Alcanza velocidades de hasta 100 Mbps

FDMA:

Frequency Division Multiple Access – Acceso múltiple por división de frecuencia es una técnica de multiplexación usada en múltiples protocolos de comunicaciones, tanto digitales como analógicas, principalmente de radiofrecuencia, y entre ellos en los teléfonos móviles de redes GSM

FIABILIDAD:

Característica de los sistemas informáticos por la que se mide el tiempo de funcionamiento sin fallos.

GATEWAYS:

Es una puerta de enlace, acceso, pasarela. Es un nodo en una red informática que sirve de punto de acceso a otra red

GBPS:

Giga bit por segundo es la unidad que se utiliza para cuantificar un flujo de datos y es un múltiplo de bit por segundo y se suele notar por la

abreviatura Gbps, de esta forma 1 Gbps equivale a 1,073,741,824 bit por segundo

GHz:

Giga Hertz. Mil millones de ciclos por segundo

GSM:
Global System for Mobile communications – Sistema Global para las comunicaciones Móviles, es el sistema de teléfono móvil digital más utilizado y el estándar de facto para teléfonos móviles

HACKERS:

Es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

HUBS:

Es un dispositivo que se utiliza como punto de conexión entre los componentes de una red de área local.

IEEE:

Instituto de Ingenieros Eléctricos, Electrónicos, una asociación técnico-profesional mundial dedicada al avance de las tecnologías relacionadas con la electricidad, electrónica, ciencias de la computación y carreras afines

IFT:

Instituto Federal de Telecomunicaciones

INTEGRIDAD:

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

JAMMING:

Este tipo de ataques desactivan o saturan los recursos del sistema

LAN:

Local Area Network – Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada

MAC:

Media Access Control - Control de Acceso al Medio. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits)

MAN:

Metropolitan Area Network - Red de Área Metropolitana: Red de alta velocidad que cubre un área geográfica extensa.

MBPS:

Megabits por segundo

MIMO:

Multiple-in, Multiple-out - Múltiple entrada, múltiple salida. MIMO sirve para tomar ventaja del multiplexado para incrementar el ancho de banda y el alcance de las conexiones inalámbricas.

NIC:

Network Information Center – Centro de Información sobre la Red. Institución que se encarga de asignar los dominios de internet que les compete.

P2P:

Peer-To-Peer, red de pares, red entre iguales, red entre pares o red punto a punto: es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

PC:

Personal Computer – Computadora Personal

PKI:

Public Key Infrastructure - Infraestructura de clave Pública: En criptografía, es una disposición que ata las claves públicas con su respectiva identidad de usuario por medio de una autoridad de certificación

PKM:

Private Key Management - Administración de claves privadas en este método los datos del transmisor se transforman por medio de un algoritmo público de criptografía con una clave binaria numérica privada sólo conocida por el transmisor y por el receptor. El algoritmo más conocido de este tipo es el DES (Data Encription Standard).

PKM-EAP:

Private Key Management - Administración de claves privadas --- Electronic Authentication Partnership – Sociedad Electrónica de Autenticación

POTS:

Plain Old Telephone Services - Servicios Telefónicos Antiguos o Tradicionales: se refiere al servicio telefónico estándar de voz analógico (no digital) que utiliza hilos de cobre. Contrasta con las líneas digitales.

PROTOCOLOS:

Es el lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí. Al encontrar un lenguaje común no existen problemas de compatibilidad entre ellas.

QoS:

Quality of Service – Calidad de servicio: es la posibilidad de saber la calidad o rendimiento de una red como internet con un determinado servicio.

RED DE COMPUTADORAS:

Es un conjunto de estas máquinas donde cada uno de los integrantes comparte información, servicios y recursos con el otro.

RF:

Radiofrecuencia: puede definirse como una red local que utiliza tecnología de radio frecuencia para enlazar los equipos conectados a la red en lugar de los medios utilizados en las LAN convencionales cableadas.

RIESGO:

Es aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de posibilidades de incumplimiento o exceso del objetivo planeado. El riesgo solo se planea como una amenaza, esto es determinando el grado de exposición a la ocurrencia de una pérdida.

ROUTERS:

Es un enrutador, es el dispositivo conectado a la computadora que permite que los mensajes a través de la red se envíen de un punto (emisor) a otro (destinatario), de manera tal que entre el alto volumen de tráfico que hay en Internet, nos va a asegurar que el mensaje llegue a su destinatario y no a otro lado.

RP-SMA:

Es para conectar una antena externa con un conector hembra RP-SMA a cualquier dispositivo inalámbrico 802.11b/g de 2.4GHz y 802.11a de 5.8 GHz. Es fácil de instalar y no requiere de configuración ni de software.

RSA:

Son las siglas de sus creadores los cuales fueron Rivest, Shamir, Adelman. Algoritmo de cifrado de clave pública desarrollado por las tres personas mencionadas.

SS:

Es un acrónimo de Style Sheet y pertenece a la categoría Bases de Datos.

SWITCHES:

Es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI

T1:

Servicio de portadora de WAN digital. T1 transmite datos formateados DS-1 a 1.544 Mbps a través de la red de conmutación telefónica

TDMA:

Time Division Multiple Access -Acceso Múltiple de División de Tiempo: A la transmisión digital inalámbrica que permite a un gran número de usuarios para acceder a una frecuencia de radio sin interrupción del servicio. Se utiliza un "Slot Time", es decir, es como un centro de llamadas ("Un representante tomará su llamada en el orden en que se recibió").

TEKs:

Transmission Encryption Key - Clave de Cifrado de Transmisión

TKIP

Temporal Key Integrity Protocol - Protocolo de Integridad con una clave temporal es un método de codificación. TKIP suministra una clave por paquete mezclando la integridad de un mensaje y un mecanismo de reescritura

TLS:

Transport Layer Security Protocol – Protocolo de seguridad de nivel de transporte

TOKEN:

También llamado componente léxico es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación.

TOKENS:

Pequeños grupos de datos que representan un conjunto de información mayor previamente establecida.

TOKEN RING:

Es una información del estándar IEEE 802.5 el cual se distingue más por su forma de transmitir la información que por la forma en que se conectan las computadoras.

UNICA:

Unidad de Servicios de Cómputo de la Facultad de Ingeniería

USECAD:

Unidad de Servicios de Cómputo Administrativos

WAN:

Wide Area Network - Red de Área Amplia. El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial.

WEP:

Protocolo de equivalencia con red cableada .WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos.

WIFI:

Wireless Fidelity –Tecnología de comunicación inalámbrica mediante ondas que permite conectar diferentes equipos informáticos a través de una red de banda ancha.

WI-MAX:

Worldwide Interoperability for Microwave Access - Interoperabilidad mundial para acceso por microondas, es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 50 km.

WPA:

Wireless Application Protocol – Protocolo de aplicaciones inalámbricas, un estándar seguro que permite que los usuarios accedan a información de forma instantánea a través de dispositivos inalámbricos

WPA2:

Wireless Application Protocol - Protocolo de aplicaciones inalámbricas está creado para corregir las deficiencias del WPA ya que está basado en el estándar 802.11i

WRAP:

Wireless Router Application Platform - Plataforma de Aplicación de Router Inalámbrico

REFERENCIAS

REFERENCIAS

(29 de Diciembre de 2016). Obtenido de WiMAX Forum espera duplicar el número de usuarios WiMAX a finales de 2010: http://www.islabit.com/2912/wimax-forum-espera-duplicar-el-numero-de-usuarios-wimax-a-finales-de-2010.html

(Septiembre de 2016). Obtenido de UNICA: http://132.248.54.13/UNICA/index.jsp

(29 de Diciembre de 2016). Obtenido de Comparación de la Eficacia Volumétrica entre Redes WIFI y WIMAX: http://132.248.9.195/ptb2011/noviembre/0674882/0674882_A1.pdf

(20 de Septiembre de 2016). Obtenido de Antenas y Líneas de Transmisión: http://www.eslared.org.ve/walc2012/material/track1/03-Antenas_y_Lineas_de_Transmision-es-v3.0-notes.pdf

(5 de Octubre de 2016). Obtenido de Cobertura de transmisión: https://www.google.com.mx/search?q=Estructura+de+una+red+WiMAX/BWA.&espv=2&biw=1309&bih=705&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiR1Onyz5bNAhVpxoMKHfvIAD4Q_AUIBigB#imgrc=_XLZvqkwkt0eIM%3A

(30 de Mayo de 2016). Obtenido de Frecuencia de un símbolo OFDM: http://132.248.9.195/ptd2009/junio/0644574/Index.html

(20 de Septiembre de 2016). Obtenido de Introducción a OFDM: http://bibing.us.es/proyectos/abreproy/11254/fichero/5_CAPITULO+1.pdf

(29 de Diciembre de 2016). Obtenido de Mobile WiMax-The Protocol Journal Volume 11, No. 2: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-40/112-wimax.html

(25 de Marzo de 2016). Obtenido de Sistema OFDM de alta eficiencia espectral: http://e-archivo.uc3m.es/bitstream/handle/10016/16948/TFG_Olaia_Nehme_Rivas.pdf?sequence=1

(15 de Marzo de 2016). Obtenido de Técnicas de estimación de canal en la capa física Wirelessman-OFDM de la norma IEEE 802.16E: http://bibing.us.es/proyectos/abreproy/11764/fichero/Carpeta5%252FCap%EDtulo4.pdf

(29 de Diciembre de 2016). Obtenido de Diario Oficial de Federación: http://www.dof.gob.mx/nota_detalle.php?codigo=5411997&fecha=19/10/2015

(29 de Diciembre de 2016). Obtenido de Inventario de bandas de Frecuencia de uso libre: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjDkrTJ9JnRAhUr94MKHYrUCdgQFgggMAE&url=http%3A%2F%2Fwww.ift.org.mx%2Fsites%2Fdefault%2Ffiles%2Fcontenidogeneral%2Fespectro-radioelectrico%2Fespectro-de-uso-libre-vf.doc&usg=AFQjC

ACISSI. (2015). *Seguridad Informática: Ethical Hacking, conocer el ataque para una mejor defensa.* Barcelona: España.

Anaya, C. A. (1998). *Máxima Seguridad en Internet .* España: Anaya Multimedia.

Black, U. (2009). *Redes.* Madrid: Gráficas Hermanos Goméz.

Black, U. (2009). *Redes Edición 2010.* España: Graficas Hermanos Gomez S.L.L.

Caldarelli, G. (2014). *Redes: una breve introducción.* Madrid: Alianza.

Casanova, V. F. (2009). *Sams Teach Yourself Networking in 24 hours.* España: Anaya Multimedia.

H., A. G. (2007). *Fundamentals of Wimax: Understanding Broadband Wireless Networking.* Estados Unidos: Prentice Hall.

Huidobro, J. M. (1992). *Todo sobre comunicaciones.* México: Paraninfo.

Katz, M. (2013). *Redes y Seguridad .* México: Alfaomega.

Leyva, J. (3 de Febrero de 2016). Obtenido de Cisco Networking Academy Program: www.innacap.cl

M., A. G. (1997). *Telecomunicaciones redes de datos.* México: Mc-GRAW HILL.

Madron, T. W. (1992). *Redes de Área .* México: Megabyte Noriega Editores.

Manuel, L. (20 de Mayo de 2016). Patente No. Modelo_Propagación_Equipo_RedMax_REDLINE. México, D.F.

Moya, J. H. (2014). *Telecomunicaciones: Tecnologías, redes y servicios.* España: Paracuellos de Jarama.

Sheldon, T. (1994). *Enciclopedia LAN TIMES de redes (NETWORKING).* México: McGRAW-HILL.

Solórzano, C. (1995). *¡Redes Fácil!* Edo. de México: Prentice-Hall Hispanoamericana, S.A.

Tanenbaum, C. (1991). *Redes de Ordenadores.* México: Prentice-Hall Hispanoamericana S.A.