# CAPÍTULO II

# MARCO TEÓRICO

## 2.1. INTRODUCCIÓN

En este capítulo se describe la fundamentación teórica utilizada en el presente trabajo, como son los conocimientos de electrónica y redes inalámbricas..

## 2.2. REGISTRADORES DE ENERGÍA ELÉCTRICA

Las empresas distribuidoras del servicio eléctrico, utilizan registradores para cuantificar el consumo de energía de un abonado. Entre los más utilizados se encuentran los registradores electromecánicos y los electrónicos.

### 2.2.1. REGISTRADORES ELECTROMECÁNICOS

Los registradores electromecánicos funcionan a base de bobinados de corriente y tensión, los cuales son utilizados para generar corrientes ficticias o también denominadas parasitas en un disco, el cual mediante la influencia de campos magnéticos, gira, y a través de un sistema de engranes se transmite el movimiento del disco al registrador ciclométrico.

En la actualidad, los registradores electromecánicos están siendo reemplazados por registradores electrónicos.

### 2.2.2. REGISTRADORES ELECTRÓNICOS

Los registradores electrónicos utilizan conversores análogo-digital, la mayoría utilizan el circuito integrado ADE7756 el cual es capaz de medir potencia y energía monofásica con interfaz serial y salida de pulsos.; posee recursos

internos para el muestreo de las señales de tensión, corriente, filtrado, compensación de errores, etc.

Generalmente el consumo de kWh es realizado por conteo de impulsos, por ejemplo 1600 impulsos equivalen a 1 kWh de consumo, además poseen una salida de impulsos conocida como salida opto acoplada.

Para visualizar el consumo de energía poseen un display de cristal líquido, la *Figura 1* muestra un registrador electrónico monofásico.

**Figura 1. Registrador Electrónico Monofásico**


Fuente: http://www.imtechtron.com/im/productos/landisgyr/e22a.gif

En el *Cuadro 1* se encuentran las prestaciones de cada uno de los registradores.

**Cuadro 1. Diferencias entre registradores monofásicos electromecánicos y electrónicos**

| | **Registradores Electromagnéticos** | **Registradores Electrónicos** |
|---|---|---|
| **Método conteo de kWh** | A través del giro un disco | A través de señales ópticas |
| **Funcionamiento principal** | A base de bobinados de corriente y tensión | A base dispositivos electrónicos de alta precisión |
| **Método para medir la potencia consumida** | Utilizando corrientes ficticias | Utiliza el circuito integrado ADE7756 |
| **Visualización** | Ciclométrico numerado | Pantalla de Cristal Liquido |
| **Seguridad en caso de interrupción del servicio** | El disco deja de girar | Memoria EEPROM para almacenar la lectura |
| **Tamaño** | Grande | Reducido |

Fuente. Los autores

## 2.3. ELECTRÓNICA

La electrónica es la encargada de la utilización y el estudio de sistemas cuyo funcionamiento se encuentra basado en la conducción y el control de flujo de los electrones, o cualquier otra partícula que se encuentre eléctricamente cargada. La electrónica básicamente se clasifica en electrónica analógica y electrónica digital.

### 2.3.1. ELECTRÓNICA ANALÓGICA

La electrónica analógica se basa principalmente en una señal que adquiere valores entre un máximo y un mínimo, trabaja con señales que cambian en el tiempo.

Se puede convertir un valor analógico en un valor digital, lo cual se expresa con ceros (0) y unos (1), puesto que es más fácil tratar una señal digital que una señal analógica

### 2.3.2. ELECTRÓNICA DIGITAL

La electrónica digital se encarga de sistemas electrónicos en los cuales la información está codificada, ya que las señales tendrán dos valores: valor bajo y valor alto, o también llamados como falso y verdadero respectivamente.

### 2.3.3. MICROCONTROLADOR

Un microcontrolador es un circuito integrado que incluyen las componentes como procesador, memoria y unidades de entrada y salida los cuales permiten procesar información y ayudan a la automatización de procesos.

Un microcontrolador dispone normalmente de los siguientes componentes:

- Procesador o UCP (Unidad Central de Proceso).
- Memoria RAM para contener los datos de proceso.
- Líneas de E/S para comunicarse con el exterior.

- Diversos módulos para el control de periféricos (temporizadores, Puertas Serie y Paralelo, CAD: Conversores Analógico/Digital, CDA: Conversores Digital/Analógico, etc.)
- Generador de impulsos de reloj que sincronizan el funcionamiento de todo el sistema.

➢ **Tipos de Microcontroladores**

Los microcontroladores se clasifican básicamente de acuerdo a las prestaciones que ofrecen en gamas baja, media, y alta.

- *Gama baja*

La Gama baja está formada por dispositivos de 4, 8 y 16 bits, están dedicados fundamentalmente a tareas de control, se utilizan en electrodomésticos, cabinas telefónicas, algunos periféricos de ordenadores, etc.

**Figura 2. Microcontrolador Gama Baja**.

Fuente:http://2.bp.blogspot.com/_J16NDtdhm9g/SfEEGRWRdSI/AAAAAAAAAOg/SFKgpN8PVok/s400/PIC12F629-IP.jpg

- *Gama media*

La gama media formada por dispositivos de 16 y 32 bits, son utilizados para tareas de control con cierto grado de procesamiento como control en automóviles, teléfonos móviles, PDA.

**Figura 3. Microcontrolador Gama Media.**

Fuente: http://i37.tinypic.com/2u7m07r.jpg

- *Gama Alta*

La gama alta compuesta por dispositivos de 32, 64 y 128 bits, son utilizados fundamentalmente para procesamiento de ordenadores, videoconsolas, etc.

**Figura 4. Microcontrolador Gama Alta.**


Fuente: http://www.tme.eu/u/NewProducts1/pic32mx.jpg

- **Tipos de Memorias**

Un microcontrolador posee varios tipos de memorias las cuales son necesarias para el correcto funcionamiento del mismo.

- *Memoria RAM*

De acuerdo a lo indicado en http://es.wikipedia.org/wiki/Microcontrolador, una memoria RAM "está destinada al almacenamiento de información temporal que será utilizada por el procesador para realizar cálculos u otro tipo de operaciones lógicas. En el espacio de direcciones de memoria RAM se ubican los registros de trabajo del procesador, configuración y de trabajo de los distintos periféricos del microcontrolador."

- *Memoria ROM*

Según http://axnm.galeon.com/, una memoria ROM "es un dispositivo no volátil de sólo lectura cuyo contenido se graba durante la fabricación del chip."

- *Memoria EPROM (Erasable Programmable Read Only Memory).*

La memoria EPROM es reprogramable, pero antes debe ser borrada, mediante la exposición de la memoria a una fuente de luz ultravioleta. Actualmente han caído en desuso ya que existen tecnologías menos costosas y más flexibles.

- *Memoria EEPROM (Electrical Erasable Programmable Read Only Memory).*

Diseñadas para sustituir a las memorias EPROM, la diferencia más relevante es que pueden ser borradas eléctricamente, por lo tanto la ventanilla de cristal de cuarzo y los encapsulados cerámicos que se utilizaban en las memorias EPROM no son necesarios.

- *Memoria FLASH.*

Las memorias reprogramables para microcontroladores, se usan a gran escala, mejorando el funcionamiento de los microcontroladores con memoria EEPROM.

Para seleccionar el microcontrolador necesario, según http://www.cec.uchile.cl/~mcarter/EL54B/Informe%20SPDI%20presentaciones/pic.pdf se debe tener en cuenta factores, como la documentación y herramientas de desarrollo disponibles, características del microcontrolador, como se detallan a continuación.

- *Procesamiento de datos*

Si es necesario que el microcontrolador realice cálculos críticos en un tiempo limitado, es aconsejable seleccionar un dispositivo suficientemente rápido tomando en cuenta la precisión de los datos a manejar: si no es suficiente con un microcontrolador de 8 bits, puede ser necesario utilizar microcontroladores de 16 ó 32 bits.

- *Entrada/Salida*

Para determinar las necesidades de Entrada/Salida del sistema es aconsejable dibujar un diagrama de bloques del mismo, de tal forma que sea fácil identificar la cantidad y tipo de señales a controlar.

- *Memoria*

Se debe determinar las necesidades de memoria de una aplicación, la memoria volátil (RAM), memoria no volátil (ROM, EPROM, etc.) y memoria no volátil modificable (EEPROM) deben estar separadas.

- **Software de Programación**

Para programar un microcontrolador se han desarrollado varios tipos de software de acuerdo a http://www.sstecnica.com.ar/archivo/micros_pic.htm, se define los siguientes:

- *Ensamblador*.

La programación en lenguaje ensamblador permite desarrollar programas muy eficientes, ya que brinda al programador el dominio absoluto del sistema. Los fabricantes suelen proporcionar el programa ensamblador de forma gratuita y en cualquier caso siempre se puede encontrar una versión gratuita para los microcontroladores más utilizados.

- *Compilador*.

La programación en un lenguaje de alto nivel (como el C ó el Basic) permite disminuir el tiempo de desarrollo de un producto. No obstante, si no se programa con cuidado, el código resultante puede ser mucho más ineficiente que el programado en ensamblador. Las versiones más potentes suelen ser muy caras, aunque para los microcontroladores más populares pueden encontrarse versiones demo limitadas e incluso compiladores gratuitos.

- *Simulador.*

Permiten tener un control absoluto sobre la ejecución de un programa, siendo ideales para la depuración de los mismos. Presentan un gran inconveniente ya que es complicado simular la entrada y salida de datos del microcontrolador. Adicionalmente no cuentan con la posible interferencia en las entradas.

## 2.4. ESTÁNDARES INALÁMBRICOS

En 1978 la US-NSPAC (Comité consultivo de la política nacional de los estándares) definió “estándar” como:

> **“Un sistema de reglas prescrito, condiciones o requerimientos que atañen a las definiciones de los términos; clasificación de los componentes; especificación de materiales, prestaciones u operaciones; delimitación de procedimientos; o medidas de la cantidad y calidad en la descripción de materiales, productos, sistemas, servicios o prácticas”**

Los estándares son usados para garantizar seguridad, calidad, y consistencia en los equipos. Un equipo que sigue un estándar específico implica la posibilidad de interoperabilidad con otros productos y de no estar “atado” a un vendedor único.

### 2.4.1. ESTÁNDARES ABIERTOS Y CERRADOS

Un estándar abierto según http://eslared.org.ve/tricalcar/02_es_estandares-inalambricos_guia_v02%5B1%5D.pdf, “está disponible públicamente, mientras que uno cerrado no. Los estándares cerrados están disponibles solo bajo términos muy restrictivos establecidos en un contrato con la organización que posee el copyright de la especificación. Un ejemplo de estándar abierto es HTML mientras que el formato de un documento de Microsoft Office es cerrado.

Un estándar abierto aumenta la compatibilidad entre el hardware, software o sistemas, ya que el estándar puede ser implementado por cualquiera. Un estándar abierto no implica necesariamente que sea exento de pago de derechos o de licencias.”

### 2.4.2. IEEE 802.11 REDES DE ÁREA LOCAL INALÁMBRICAS

La primera publicación del estándar IEEE 802.11 fue presentada en 1997 en la que se especificaba que se utilizaría CSMA/CA (Acceso Múltiple por Detección de Portadora/Limitación de Colisiones) como método de acceso al medio. Todas las correcciones del IEEE 802.11 se han basado en el mismo método de acceso.

### 2.4.3. IEEE 802.11 ASPECTOS TÉCNICOS

El estándar 802.11 incluye una serie de rectificaciones, que contemplan principalmente las técnicas de modulación, gama de frecuencia. De acuerdo a lo indicado en http://eslared.org.ve/tricalcar/02_es_estandares-inalambricos_guia_v02%5B1%5D.pdf, IEEE 802.11 cubre las primeras dos capas del modelo de OSI, es decir la capa física y la capa de enlace que se detallan a continuación:

- **Capa 1 (Capa Física)**

La capa física tiene como objetivo transportar de manera confiable y eficiente la señal correspondiente a cero (0) y uno (1) lógico, que son los datos que el transmisor desea enviar al receptor, esta capa se encarga de la modulación y codificación de los datos.

- *Técnicas de Modulación*

La técnica de modulación elegida es un aspecto que influye en la transferencia de datos. A medida que los datos se codifican eficientemente, se logran tasas o flujos de bits mayores dentro del mismo ancho de banda, pero se requiere hardware más sofisticado para manejar la modulación y la demodulación de los datos.

- FHSS (FrequencyHopping Spread Spectrum – espectro esparcido por salto de frecuencia) FHSS se basa en el concepto de transmitir sobre una frecuencia por un tiempo determinado, después aleatoriamente saltar a otra. En el estándar IEEE 802.11 se utiliza la banda de frecuencia (ISM) que va de los 2,400 hasta los 2,4835 GHz,. Los saltos se hacen alrededor

de una frecuencia central que corresponde a uno de los 14 canales definidos. Este tipo de modulación no es común en los productos actuales.

- DSSS (DirectSequence Spread Spectrum - espectro esparcido por secuencia directa–). El DSSS implica que para cada bit de datos, una secuencia de bits (llamada secuencia seudoaleatoria), debe ser transmitida. Cada bit correspondiente a un uno (1) es substituido por una secuencia de bits específica y el bit igual a 0 es substituido por su complemento. El estándar de la capa física 802.11 define una secuencia de 11 bits (10110111000) para representar un “1” y su complemento (01001000111) para representar un “0”. En DSSS, en lugar de esparcir los datos en diferentes frecuencias, cada bit se codifica en una secuencia de impulsos más cortos, llamados bits, de manera que los 11 bits en que se ha dividido cada bit original ocupan el mismo intervalo de tiempo. Esta técnica de modulación ha sido común desde el año 1999 al 2005.

- OFDM (OrthogonalFrequency-DivisionMultiplexing - modulación por división de frecuenciasortogonales) OFDM, algunas veces llamada modulación multitono discreta (DMT) es una técnica de modulación basada en la idea de la multiplexación de división de frecuencia (FDM), que se utiliza en radio y TV, se basa en el concepto de enviar múltiples señales simultáneamente pero en diversas frecuencias.

  En OFDM, un sólo transmisor transmite en muchas docenas a millares de frecuencias ortogonales. El término ortogonal se refiere al establecimiento de una relación de fase específica entre las diferentes frecuencias para minimizar la interferencia entre ellas. Una señal OFDM es la suma de un número de subportadoras ortogonales, donde cada subportadora se modula independientemente usando QAM (modulación de fase y amplitud) o PSK. Esta técnica de modulación es la más común a partir del 2005.

- *Frecuencia*

Los estándares 802.11 b y la 802.11 g usan la banda no licenciadas en los 2,4 GHz ISM (Industrial, Science and Medical) definida por la UIT. Los límites exactos de esta banda dependen de las regulaciones de cada país, pero el intervalo más comúnmente aceptado es de 2.400 a 2. 483,5 MHz.

El estándar 802.11 a usa la banda de los 5 GHz UNII (Unlicensed National Information Infrastructure) cubriendo 5.15-5.35 GHz y 5.725-5.825 GHz en EEUU. En otros países la banda permitida varía, aunque la UIT ha instado a todos los países para que autoricen la utilización de todas estas gamas de frecuencias para redes inalámbricas.

- **Capa 2 (Capa de Enlace)**

La capa de transmisión de datos de 802.11, se compone de dos partes:

- Control de acceso al medio (MAC)
- Control lógico del enlace (LLC)

La subcapa LLC de 802.11 permite una compatibilidad con cualquier otra red 802, mientras que la subcapa MAC presenta cambios sustanciales para adecuarla al medio inalámbrico.
La subcapa MAC sustituye al estándar 802.3 (CSMA/CD – Ethernet) utilizado en redes cableadas.

- *Método de acceso al medio*

El protocolo de acceso al medio en redes Ethernet es el CSMA/CD, basado en la detección de colisiones y la subsiguiente retransmisión cuando éstas ocurren. En redes inalámbricas que utilizan la misma frecuencia para transmitir y recibir, es imposible detectar las colisiones en el medio, por lo que el mecanismo de compartición del medio se modifica tratando de limitar las colisiones y usando acuse de recibo (ACK) para indicar la recepción exitosa de una trama. Si el transmisor no recibe el ACK dentro de un tiempo preestablecido, supone que la transmisión no fue exitosa y la reenvía. Este protocolo se conoce como CSMA/CA, es decir, tratar de evitar las colisiones. Con este método hay que

esperar el ACK antes de poder continuar utilizando el canal, y el mismo ACK consume tiempo de transmisión.

Además, para transmisión a grandes distancias el tiempo de espera por el ACK puede ser significativo debido a que las ondas de radio tardan 2 ms en ir y volver a una distancia de 300 km. Esencialmente, CSMA/CA utiliza tiempos de espera obligatorios de longitud variable entre tramas sucesivas para evitar las colisiones. Estos tiempos se denominan espaciamiento entre tramas, Interframe Spacing, y su valor depende del estado previo del canal. Opcionalmente también se pueden utilizar mecanismos de reserva del canal, en una técnica conocida como RTS/CTS (Ready to Send/Clear to Send) que garantiza el acceso al medio a expensas de tiempos de transmisión aún más largos. El acceso al medio es controlado por el uso de diversos tipos de espacio entre tramas, que corresponde a los intervalos de tiempo que una estación necesita esperar antes de enviar datos. Los datos prioritarios como paquetes de ACKs o de RTS/CTS esperarán un período más corto (SIFS) que el tráfico normal.

### 2.4.4. ESTÁNDAR IEEE 802.11 a

De acuerdo a lo indicado en http://estared.org.ve/tricalcar/02_es_estandares-inalambricos_guia_v02%5B1%5D.pdf “El estándar IEEE 802.11 a funciona en la banda de los 5 GHz y utiliza la técnica de modulación OFDM. Usando la selección adaptativa de velocidad, la tasa de datos cae desde 54 a 48, 36, 24, 18, 12, 9 y 6 Mbit/s a medida que experimenta dificultades en la recepción”.

IEEE 802.11 a permite operar en 12 canales sin solapamiento, de los cuales 8 están dedicados para el uso en interiores y los 4 restantes son para enlaces exteriores como se muestran en el *Cuadro 2*, 802.11 a no es interoperable con 802.11 b, porque usan bandas de frecuencia distintas, pero existen equipos que trabajan con ambos estándares.

En la frecuencia de 5 GHz existe mayor atenuación en la transmisión en exteriores y es también absorbida en mayor grado por paredes y otros objetos, por lo que en general tiene menor alcance que la de 2,4 GHz; sin embargo, se puede compensar utilizando antenas exteriores de mayor ganancia.

**Cuadro 2. Canales utilizados en IEEE 802.11 a**

| Banda de Frecuencia | ID de canal | FCC (MHz) |
|---|---|---|
| Banda Menor<br>Canal predeterminado 36 | 36 | 5180 |
| | 40 | 5200 |
| | 44 | 5220 |
| | 48 | 5240 |
| Banda Media<br>Canal predeterminado 52 | 52 | 5260 |
| | 56 | 5280 |
| | 60 | 5300 |
| | 64 | 5320 |
| Banda Superior | 149 | 5745 |
| | 153 | 5765 |
| | 157 | 5785 |
| | 161 | 5805 |
| | 165 | 5865 |

Fuente:http://www.worldlingo.com/ma/enwiki/es/List_of_WLAN_channels

### 2.4.5. ESTÁNDAR IEEE 802.11 b

Como se indica en http://estared.org.ve/tricalcar/02_estandares-inalambricsos guia_v02%5B1%5D.pdf IEEE 802.11b soporta tasas de transmisión hasta de 11 Mbit/s. IEEE 802.11 b usa el DSSS.

Un dispositivo basado en IEEE 802.11 b puede transmitir hasta 11 Mbit/s, y reduce automáticamente su tasa de transmisión cuando el receptor empiece a detectar errores, debido a la interferencia o a la atenuación del canal, cayendo a 5.5, 2, hasta 1 Mbit/s, cuando el canal sea muy ruidoso, es importante recordar que los canales se encuentran espaciados 5 MHz uno de otro como se aprecia en el C*uadro 3*, pero para que no exista superposición de canales se debe utilizar únicamente los canales 1, 6, 11 indicados en el C*uadro 4.*

**Cuadro 3. Canales designados en el rango 2.4 GHz**

| ID de canal | FCC (MHz) |
|---|---|
| 1 | 2412 |
| 2 | 2417 |
| 3 | 2422 |
| 4 | 2427 |
| 5 | 2432 |
| 6 | 2437 |
| 7 | 2442 |
| 8 | 2447 |
| 9 | 2452 |
| 10 | 2457 |
| 11 | 2462 |

Fuente: http://wifiw.com/2010/03/lista-de-canales-2-4-ghz-802-11bgn/

**Cuadro 4. Canales sin solapamiento en 2.4 GHz**

| ID de canal | FCC (MHz) |
|---|---|
| 1 | 2412 |
| 6 | 2437 |
| 11 | 2462 |

Fuente: Los autores

### 2.4.6. ESTÁNDAR IEEE 802.11g

De acuerdo a lo indicado en http://eslared.org.ve/tricalcar/02_es_estandares-inalambricos_guia_v02%5B1%5D.pdf, 802.11g trabaja en la banda del estándar IEEE 802.11b. 802.11g usa la misma técnica de modulación que el 802.11a (OFDM) por lo tanto funciona con una tasa de transferencia de datos de hasta 54 Mbit/s. y asegura la interoperabilidad con el 802.11b, en las tasas de datos correspondientes a este estándar.

## 2.5. PROPAGACIÓN DE ONDAS ELECTROMAGNÉTICAS

Los efectos a los cuales están sometidas las ondas electromagnéticas se detallan a continuación.

### 2.5.1. ABSORCIÓN

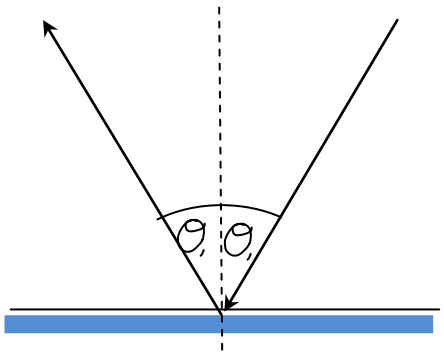
De acuerdo a lo manifestado en http://www.it46.se/courses/wireless/materials/es/03_Radio-Fisica/03_es_radio-fisica_guia_v01.pdf, Las ondas de radio, se debilitan mediante la transferencia de energía al medio en el cual viajan cuando éste no es el vacío. La potencia de la onda en el medio de transmisión decrece de manera exponencial, ya que una fuente de absorción son los materiales conductores, el agua (neblina, lluvia). Existen otros materiales que en cantidades menores absorben potencia como son, en rocas, ladrillos y concreto, dependiendo de la composición de los materiales.

### 2.5.2. REFLEXIÓN

En la radio frecuencia, los materiales que causan la reflexión son, el metal, superficies de agua, otros materiales con propiedades similares. El principio de la reflexión se basa en que una onda se refleja con el mismo ángulo con el que impacta una superficie. La *Figura 5* muestra la reflexión de una onda.

**Figura 5. Reflexión de una onda, con el mismo ángulo de incidencia**

.

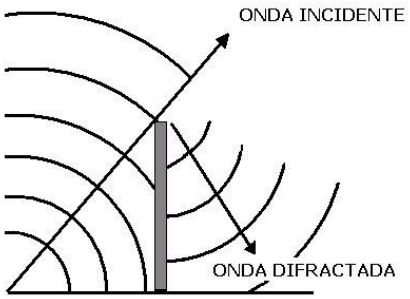



Fuente: Los autores

### 2.5.3. DIFRACCIÓN

Según http://www.it45.se/courses/wireless/materials/es/03_Radio-Fisica/03_es radio-fisica_guia_v01.pdf. Las ondas encuentran un obstáculo en su trayectoria y divergen en muchos haces, ya que las trayectorias de las ondas se apartan de la trayectoria fácilmente a medida que se incrementa la longitud de onda. Esa es la razón por la cual una estación de radio AM que opera a 1000 KHz (con una longitud de onda de 300 m) se oye fácilmente aun cuando haya considerables obstáculos en su trayecto, mientras que con redes inalámbricas (con una longitud de onda de 12 cm) se requiere una línea de vista entre transmisor y receptor.

**Figura 6. Difracción de una onda electromagnética**

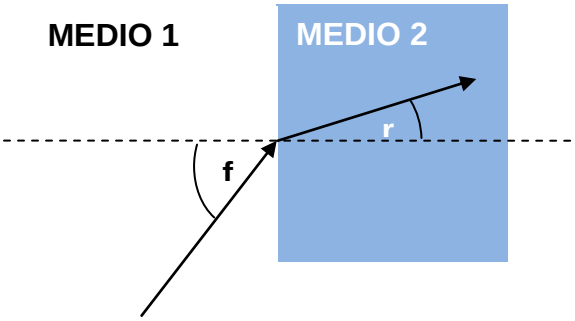



Fuente: http://data1.blog.de/blog/a/autoaudio/img/difusion.JPG

### 2.5.4. REFRACCIÓN

La refracción es la desviación de las ondas cuando encuentran un medio con composición diferente. Cuando una onda pasa de un medio a otro diferente, cambia de velocidad y en consecuencia, de dirección como se puede ver en la *Figura 7*.

**Figura 7. Refracción de una onda**




Fuente: Los autores

### 2.5.5. INTERFERENCIA

Las ondas con una misma frecuencia y una relación de fase (posición relativa de las ondas) constante pueden anularse entre sí, de manera de la suma de una onda con otra puede resultar en cero.

## 2.6. PROPAGACIÓN EN ESPACIO LIBRE

Es importante tomar en cuenta cuatro aspectos al momento de realizar un radio enlace ya que el medio de transmisión a usarse será el espacio libre.

- Pérdida en espacio libre.
- Zonas de Fresnel.
- Línea de vista.
- Efecto de trayectoria múltiple.

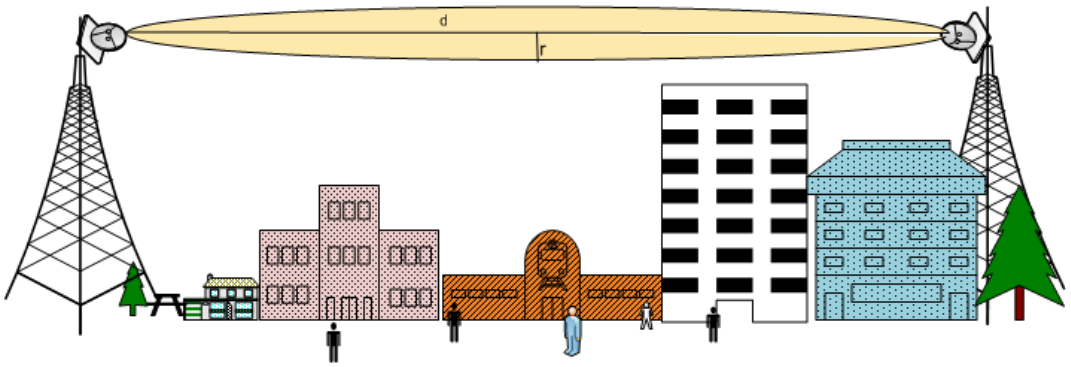
### 2.6.1. PERDIDAS EN ESPACIO LIBRE

Mide la dispersión de la potencia en el espacio libre, ya que a medida que la señal se esparce se debilita. La atenuación en el espacio libre se mide en dB (decibeles).

### 2.6.2. ZONAS DE FRESNEL

Es el área en donde se difunde una onda luego de ser emitida por una antena. Mientras menos obstáculos haya en la zona en donde se encuentra la señal la comunicación será mejor. La zona de Fresnel es muy importante, pues debe mantenerse limpia de obstáculos que detengan la señal. Los obstáculos que pueden aparecer en la zona de Fresnel son: árboles, paredes, etc., la *Figura 8* muestra la primera zona de Fresnel.

**Figura 8. Zonas de Fresnel**




d= distancia

r=radio

Fuente: Los autores

Es necesario despejar el 60% de la primera zona de Fresnel en el punto medio y a lo largo de toda la trayectoria para garantizar la funcionalidad del enlace.

### 2.6.3. LÍNEA DE VISTA

En un enlace de radio se necesita tener una línea visual (óptica) para un radio enlace. Adicionalmente, es necesario un poco de espacio alrededor, definido por las Zonas de Fresnel.

### 2.6.4. MULTITRAYECTORIA

De acuerdo a http://www.it46.se/courses/wireless/materials/es/03_Radio-Fisica/03_es_radio-fisica_guia_v01.pdf, “una onda de radio puede llegar al receptor a través de múltiples trayectorias por reflexión. Los retrasos, la interferencia y la modificación parcial de las señales pueden causar problemas en la recepción”.

## 2.7. TOPOLOGÍA E INFRAESTRUCTURA BÁSICA DE REDES INALÁMBRICAS

De acuerdo a http://eslared.org.ve/tricalcar/04_es_topologia-e-infraestructura guia_v02%5B1%5D.pdf, “la topología de una red representa la disposición de los

enlaces que conectan los nodos de una red. Las redes pueden tomar varias formas diferentes dependiendo de cómo están interconectados los nodos. Hay dos formas de describir la topología de una red: física o lógica. La topología física se refiere a la configuración de cables, antenas, computadores y otros dispositivos de red, mientras la topología lógica hace referencia a un nivel más abstracto, considerando por ejemplo el método y flujo de la información transmitida entre nodos".

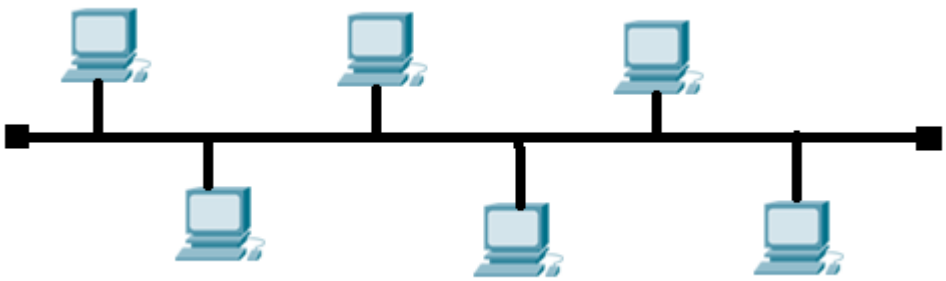
### 2.7.1. TOPOLOGÍAS RELEVANTES EN REDES INALÁMBRICAS

A continuación se detallan algunas de las topologías de red más utilizadas.

- **Bus o Barra**

Todos los nodos están conectados a un cable común o compartido. Las redes Ethernet anteriormente usaban esta topología, La *Figura 9* muestra esta topología.

**Figura 9. Topología tipo Bus**



Fuente: Los autores

- **Estrella**

Cada nodo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como en redes inalámbricas, la *Figura 10* muestra esta topología.

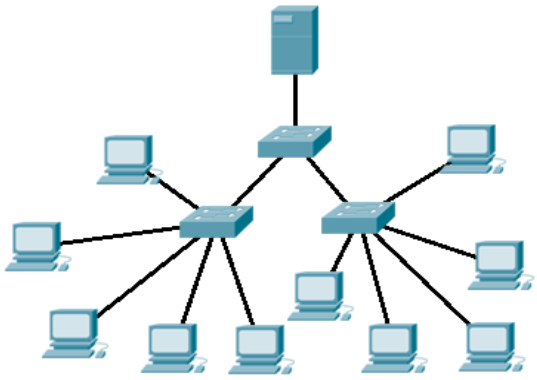
**Figura 10. Topología tipo Estrella**

Fuente: Los autores

- **Árbol**

Una combinación de las topologías de bus y estrella. Un conjunto de nodos configurados como estrella se conectan a una dorsal (backbone), en la *Figura 11* se puede observar esta topología.

**Figura 11. Topología tipo Árbol**



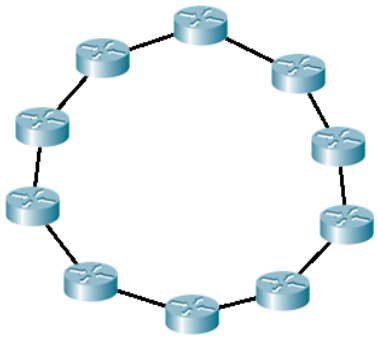
Fuente: Los autores

- **Anillo**

Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a otros dos dispositivos. Típicamente la

infraestructura es una dorsal (backbone) con fibra óptica, la *Figura 12* muestra esta topología.

**Figura 12. Topología tipo Anillo**

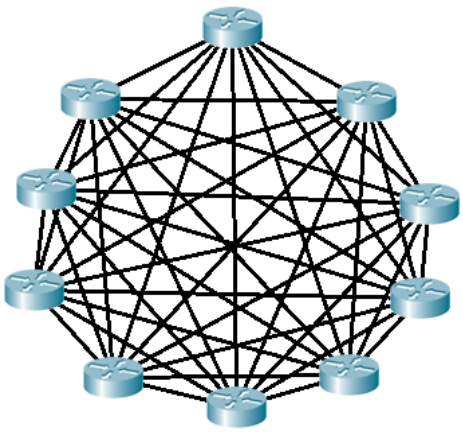


Fuente: Los autores

- **Malla completa**

Existe enlace directo entre todos los pares de nodos de la red. Una malla completa con n nodos requiere de n(n-1)/2 enlaces directos. Debido a esta característica, es una tecnología costosa pero muy confiable, la *Figura 13* muestra la topología.

**Figura 13. Topología tipo Malla**

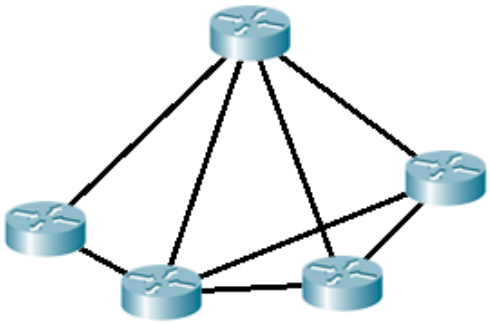


Fuente: Los autores

- **Malla Parcial**

Algunos de los nodos están organizados en una malla completa, mientras otros se conectan solamente a uno o dos nodos de la red. Esta topología es menos costosa que la malla completa ya que el número de enlaces redundantes se reduce, en la *Figura 14* se observa esta topología.

**Figura 14. Topología tipo Malla parcial**



Fuente: Los autores

## 2.8. MODOS DE OPERACIÓN DE REDES INALÁMBRICAS

El conjunto de estándares 802.11 definen dos modos fundamentales para redes inalámbricas:

- Ad hoc
- Infraestructura

### 2.8.1. MODO AD HOC (IBSS)

El modo ad hoc de acuerdo a http://eslared.org.ve/tricalcar/04_es_topologia-e-infraestructura_guia_v02%5B1%5D.pdf, se denomina a la conexión punto a punto, es un método para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo ad hoc, no es necesario involucrar un punto de acceso central. Todos los nodos de una red ad hoc se pueden comunicar directamente con otros clientes. Cada cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico en modo ad hoc y usar los mismos SSID y “número de canal” de la

red. Una red ad hoc normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros. En una red ad hoc el rendimiento es menor a medida que el número de nodos crece. Para conectar una red ad hoc a una red de área local (LAN) cableada o a Internet, se requiere instalar una Pasarela o Gateway especial. En redes IEEE 802.11 el modo ad hoc se denota como Conjunto de Servicios Básicos Independientes (IBSS - Independent Basic Service Set).

Se puede usar el modo ad hoc cuando se desea conectar directamente dos estaciones, de edificio a edificio, también se puede usar dentro de una oficina entre un conjunto de estaciones de trabajo, la *Figura 15* muestra la topología de una red Ad Hoc.

**Figura 15. Ejemplo de una red Ad hoc**

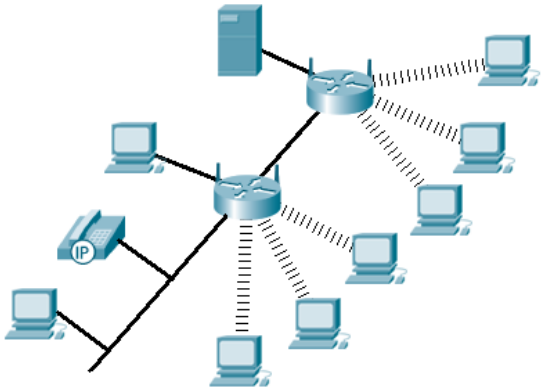
Fuente: Los autores

### 2.8.2. MODO INFRAESTRUCTURA

Según http://eslared.org.ve/tricalcar/04_es_topologia-e- infraestructura_guia_v02%5 B1 %5D.pdf en el modo de infraestructura hay un elemento de “coordinación”: un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID. Para maximizar la capacidad total de la red, se debe configurar canales diferentes en todos los puntos de acceso que se encuentran en la misma área física. En redes IEEE

802.11 el modo de infraestructura se conoce como Conjunto de Servicios Básicos (BSS – Basic Service Set). También llamado Maestro y Cliente, en la *Figura 16* se observa la topología de una red Infraestructura.

**Figura 16. Ejemplo de una red Infraestructura**



Fuente: Los autores

## 2.9. RADIOENLACES

En el proyecto de grado “Estudio y diseño de una red virtual privada móvil (VPN móvil) con tecnología WiMAX802.16e -2005 (World wide Interoperability for Microwave Access) para un carrier local con cobertura en la zona norte de la ciudad de Quito” escrito por Andrés Carrillo manifiesta:

> **“Para elaborar un radioenlace operativo se debe tomar en cuenta el cálculo de ganancias y pérdidas desde el radio transmisor (fuente de la señal de radio), a través de cables, conectores y espacio libre hacia el receptor. La estimación del valor de potencia en diferentes partes del radioenlace es necesaria para hacer el mejor diseño y elegir el equipamiento adecuado.**

**Los elementos de un radioenlace se pueden dividir en tres partes principales:**

- **El lado de Transmisión con potencia efectiva de transmisión.**
- **Pérdidas en la propagación.**
- **El lado de Recepción con efectiva sensibilidad receptiva ".**

### 2.9.1. EL LADO TRANSMISOR

Es importante diferenciar que en un radio enlace se va a tener una estación base o llamado también transmisor y estaciones adyacentes o llamadas estaciones receptoras. Según http://www.eslared.org.ve/tricalcar/06_es_calculo-de-radioenlace_guia_v01%5B1%5D.pdf, en la estación base es importante destacar los siguientes aspectos.

- **Potencia de Transmisión (Tx)**

La potencia de transmisión es la potencia de salida del radio. El límite superior depende de las regulaciones vigentes en cada país, dependiendo de la frecuencia de operación y puede cambiar al variar el marco regulatorio. En general, los radios con mayor potencia de salida son más costosos.

La potencia de transmisión del radio, normalmente se encuentra en las especificaciones técnicas del vendedor. Se debe considerar que las especificaciones técnicas le darán valores ideales, los valores reales pueden variar con factores como la temperatura y la tensión de alimentación.

La potencia de transmisión típica en los equipos IEEE 802.11 varía entre 15 – 26 dBm (30 – 400 mW).

- **Perdidas en el Cable**

La pérdida en la señal de radio se puede producir en los cables que conectan el transmisor y el receptor a las antenas. Las pérdidas dependen del tipo de cable, la frecuencia de operación y normalmente se miden en dB/m.

Independientemente de lo bueno que sea el cable, siempre tendrá pérdidas. Se debe tener en cuenta que el cable de la antena debe ser lo más corto posible. La pérdida típica en los cables está entre 0,1 dB/m y 1 dB/m. En general, mientras más grueso y más rígido sea el cable menor atenuación presentará. Como regla general, puede tener el doble de pérdida en el cable [dB] para 5 GHz comparado con 2,4 GHz, en el *Cuadro 5* se muestra la perdida de cables más comunes a 2.4 GHz.

**Cuadro 5. Perdidas de Cables más comunes a 2.4 GHz**

| Tipo de Cable | Pérdida (dB/100m) |
|---|---|
| RG 50 | 80-100 |
| RG 213 | 50 |
| LMR 200 | 50 |
| LMR 400 | 22 |
| LMR 600 | 14 |

Fuente: http://www.eslared.org.ve/tricalcar/06_es_calculo-de-radioenlace_guia_v01%5B1%5D.pdf

- **Perdidas en los Conectores**

Se debe estimar por lo menos 0,25 dB de pérdida para cada conector en el cableado. Estos valores son para conectores bien hechos mientras que los conectores mal soldados DIY (Do It Yourself) pueden implicar pérdidas mayores.
Se debe considerar un promedio de pérdidas de 0,3 a 0,5 dB por conector como regla general.
Además, los protectores contra descargas eléctricas que se usan entre las antenas y el radio deben ser presupuestados hasta con 1 dB de pérdida, dependiendo del tipo. Los protectores de buena calidad sólo introducen 0,2 dB.

- **Amplificadores**

Se pueden utilizar amplificadores para compensar la pérdida en los cables. En general, se debería utilizar amplificadores como última opción. Se debe realizar

una buena elección de las antenas y tener alta sensibilidad del receptor para evitar la intervención de amplificadores ya que añaden ruido extra a la señal, y los niveles de potencia resultantes pueden infringir las normas legales de la región.

- **Ganancia de la Antena**

La ganancia de una antena típica varía entre 2 dBi (antena integrada simple) y 8 dBi (omnidireccional estándar) hasta 21 – 30 dBi (parabólica). Se debe considerar que hay muchos factores que disminuyen la ganancia real de una antena.
Las pérdidas pueden ocurrir por muchas razones, principalmente relacionadas con una incorrecta instalación (pérdidas en la inclinación, en la polarización, objetos metálicos adyacentes). Esto significa que sólo puede esperar una ganancia completa de antena, si está instalada en forma óptima.

### 2.9.2. PERDIDAS DE PROPAGACIÓN

Según http://www.eslared.org.ve/tricalcar/06_es_calculo-de-radioenlace_guia_v01%5B1%5D.pdf, Las pérdidas de propagación están relacionadas con la atenuación que ocurre en la señal cuando esta sale de la antena de transmisión hasta que llega a la antena receptora, para lo cual es importante analizar los siguientes aspectos.

- **Perdidas en el Espacio Libre**

La mayor parte de la potencia de la señal de radio se pierde en el aire. Aún en el vacío, una onda de radio pierde energía que se irradia en direcciones diferentes a la que puede capturar la antena receptora. Esto no tiene nada que ver con el aire, la niebla, la lluvia o cualquier otra cosa que puede adicionar pérdidas.
La Pérdida en el Espacio libre (FSL, por sus siglas en inglés), mide la potencia que se pierde en el mismo sin ninguna clase de obstáculo. La señal de radio se debilita en al aire debido a la expansión dentro de una superficie esférica.

La Pérdida en el Espacio libre es proporcional al cuadrado de la distancia y también proporcional al cuadrado de la frecuencia. Aplicando decibeles, resulta la siguiente ecuación:

**Ecuación 1. Cálculo de pérdida en el espacio libre**

$$\boldsymbol{FSL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + K$$

*d = distancia.*

*f = frecuencia.*

*K= Constante, depende de unidades de f y* d.

- **Zona de Fresnel**

La primera zona de Fresnel es el espacio alrededor del eje que contribuye a la transferencia de potencia desde la fuente hacia el receptor.

Lo ideal es que la primera zona de Fresnel no esté obstruida, pero normalmente es suficiente despejar el 60% del radio de la primera zona de Fresnel para tener un enlace satisfactorio. La siguiente fórmula calcula la primera zona de Fresnel:

**Ecuación 2. Cálculo de la primera zona de Fresnel**

$$\boldsymbol{r} = 17{,}32 * \sqrt{[(d1 * d2) \div (d * f)]}$$

*d1 = distancia al obstáculo desde el transmisor [km]*

*d2 = distancia al obstáculo desde el receptor [km]*

*d = distancia entre transmisor y receptor [km]*

*f = frecuencia [GHz]*

*r = radio [m]*

Si el obstáculo está situado en el medio (d1 = d2), la fórmula se simplifica:

**Ecuación 3. Cálculo primera zona de Fresnel**

$$\boldsymbol{r} = 17{,}32 * \sqrt{(d \div 4f)}$$

### 2.9.3. LADO RECEPTOR

En el lado del receptor o estación se debe tener en cuenta los siguientes aspectos:

- **Sensibilidad del receptor**

La sensibilidad de un receptor es un parámetro que merece especial atención ya que identifica el valor mínimo de potencia que necesita para poder decodificar/extraer “bits lógicos” y alcanzar una cierta tasa de bits.
Cuanto más baja sea la sensibilidad, mejor será la recepción del radio. Un valor típico es -82 dBm en un enlace de 11 Mbps y -94 dBm para uno de 1 Mbps.
Una diferencia de 10 dB es tan importante como 10 dB de ganancia que pueden ser obtenidos con el uso de amplificadores o antenas más grandes. La sensibilidad depende de la tasa de transmisión.

- **Potencia de recepción**

La potencia de recepción es un parámetro que ayuda a verificar si la potencia recibida en el lado receptor es suficiente para lograr enlazar las estaciones, a continuación se presenta la ecuación para la potencia de recepción.

**Ecuación 4. Cálculo de Potencia de Recepción**

$$\begin{aligned}\boldsymbol{Prx(dBm)} = {} & Ptx + G.Ant\ tx - FSL + G.Ant.rx - Pérdida\ Cable\ tx \\ & - Pérdida\ Cable\ rx - Pérdida\ Conectores\ tx \\ & - Pérdida\ Conectores\ rx\end{aligned}$$

- **Margen y Relación Señal Ruido**

No es suficiente que la señal que llega al receptor sea mayor que la sensibilidad del mismo, sino que además se requiere que haya cierto margen para garantizar el funcionamiento adecuado.

La relación entre el ruido y la señal se mide por la tasa de señal a ruido (SNR en inglés). Un requerimiento típico de la SNR es 16 dB para una conexión de 11 Mbps y 4 dB para la velocidad más baja de 1 Mbps.

En situaciones donde hay muy poco ruido el enlace está limitado primeramente por la sensibilidad del receptor. En áreas urbanas donde hay muchos radioenlaces operando, es común encontrar altos niveles de ruido (tan altos como -92 dBm). En esos escenarios, se requiere un margen mayor:

**Ecuación 5. Cálculo relación señal a ruido**

$$\boldsymbol{Relación\ señal\ a\ ruido}\ [\boldsymbol{dB}] = 10 * \log 10\ (Potencia\ de\ la\ señal\ [W] \div Potencia\ de\ ruido\ [W])$$

En condiciones normales sin ninguna otra fuente en la banda de 2.4 GHz y sin ruido de industrias, el nivel de ruido es alrededor de los -100 dBm.

### 2.9.4. MARGEN DEL SISTEMA

Corresponde a la diferencia entre el valor de la señal recibida y la sensibilidad del receptor.

**Ecuación 6. Cálculo de Margen del Sistema**

$$\begin{aligned}\boldsymbol{Margen}\ (\boldsymbol{dBm}) = {} & Ptx(dBm) - Pérdida\ en\ el\ cable\ tx(dB) + G.Antena\ tx(dBi) \\ & - FSL(dB) + G.Antena\ rx(dBi) - Pérdida\ en\ el\ cable\ Rx(dB) \\ & + Sensibilidad\ rx(-dBm) - Pérdida\ Conectores\ tx\ (dB) \\ & - Pérdida\ Conectores\ rx(dB)\end{aligned}$$

### 2.9.5. MARGEN DE DESVANECIMIENTO

El margen de desvanecimiento es un parámetro que depende de las condiciones a la que está sometida cada transmisión.

Factores como el tipo de suelo, el tipo de clima, el entorno que lo rodea y el factor de confiabilidad tienen influencia directa en el cálculo del desvanecimiento, en el *Cuadro 6* se muestra los valores para el factor de rugosidad y en el *Cuadro 7* se encuentran los valores para el factor climático

**Cuadro 6. Valores de factor de rugosidad**

| Valor | Descripción |
|---|---|
| 4 | Espejos de agua, ríos muy anchos, etc. |
| 3 | Sembrados densos, pastizales, arenales |
| 2 | Bosques (la propagación es por encima) |
| 1 | Terreno normal |
| 0.25 | Terreno rocoso disparejo |

Fuente: http://sig.utpl.edu.ec/sigutpl/Staftpro/sig/radioenlace.PDF

**Cuadro 7. Valores para el factor climático**

| Valor | Descripción |
|---|---|
| 1 | Aéreas marítimas |
| 0.5 | Áreas tropicales calientes y húmedas |
| 0.25 | Áreas mediterráneas de clima normal |
| 0.125 | Áreas montañosas de clima seco y fresco |

Fuente: http://sig.utpl.edu.ec/sigutpl/Staftpro/sig/radioenlace.PDF

La ecuación para el cálculo del margen de desvanecimiento es la siguiente

**Ecuación 7. Cálculo del Margen de desvanecimiento**

$$\boldsymbol{L_D(dB)} = 30\log D + 10\log(6ABf) - 70 - 10\log(1-R)$$

*Dónde:*

*D: _Distancia*

*A: Factor de Rugosidad*

*B: Factor Climático*

*F: Frecuencia*

*R: Confiabilidad esperada en decimal*

### 2.9.6. MARGEN DE DESPEJE

Es importante considerar que en un radio enlace debe existir línea de vista directa o se debería realizar un análisis tomando en cuenta el lugar donde se encuentra el obstáculo, y ver si es factible el enlace o no.

El margen de despeje sobre un obstáculo se obtiene mediante la siguiente ecuación:

**Ecuación 8. Cálculo de Margen de despeje**

$$\boldsymbol{h_{des}} = h_1 + \frac{d_1}{d}(h_2 - h_1) - \left(H + \frac{d_1 d_2}{2Ka}\right)[m]$$

*Dónde:*

*K = Coeficiente del radio efectivo de la Tierra, este valor es igual a 4/3.*

*a = Radio de la Tierra igual a 6.37 Km.*

*h1 = altura de punto 1*

*h2 = altura del punto 2*

*d1 = distancia hacia el obstáculo*

*d2 = distancia hacia el obstáculo*

*d= distancia total del enlace*

Los cálculos del margen de despeje se los realiza en el punto más crítico; es decir, donde pueda existir obstrucción, basta con que el margen de despeje sobre

el obstáculo sea mayor al radio de la primera zona de Fresnel en el mismo punto, con lo cual se asegura que no exista obstrucción.

### 2.9.7. AZIMUT

Según http://es.wikipedia.org/wiki/Acimut, “es el ángulo de una dirección contado en el sentido de las agujas del reloj a partir del norte geográfico. El acimut de un punto hacia el este es de 90 grados y hacia el oeste de 270 grados sexagesimales. El término azimut se usa cuando se trata del norte geográfico. Cuando se empieza a contar a partir del norte magnético se suele denominar rumbo o azimut magnético”.

### 2.9.8. POTENCIA IRRADIADA

De acuerdo a http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/06_es_calculo-de-radioenlace_guia_v02.odt, La Potencia Irradiada Isotrópica Efectiva está regulada por la autoridad nacional. La misma especifica la potencia máxima legalmente permitida para ser enviada al espacio abierto en un área/país específico. La PIRE es una medida de la potencia que se está enfocando en una determinada región de espacio, determinada por las características de la antena transmisora.

La PIRE es el resultado de restar pérdidas de potencia en el cable y conectores y sumar la ganancia relativa de antena a la potencia del transmisor.

**Ecuación 9. Cálculo de Potencia irradiada**

$$\boldsymbol{PIRE} = Potencia\ del\ transmisor - Pérdidas\ en\ el\ cable\ y\ conectores + ganancia\ de\ la\ antena$$

## 2.10. SEGURIDAD DE REDES INALÁMBRICAS

La seguridad en redes inalámbricas se resume como la seguridad de la información que circula a través de la misma, definida como Seguridad

Informática y según U.S. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) es definida como:

> **"Medidas y controles que se toman para negar el acceso no autorizado de personas a información derivada de las telecomunicaciones y augurar la autenticidad de tales telecomunicaciones".**

### 2.10.1. INTEGRIDAD

La Integridad de datos es la capacidad para determinar si la información transmitida ha sido alterada por personas no autorizadas. La integridad busca mantener los datos libres de modificaciones no autorizadas

### 2.10.2. DISPONIBILIDAD

Acceso oportuno y confiable a datos y servicios de información para usuarios autorizados. La disponibilidad de la red es el porcentaje de tiempo que el servicio es ofrecido a un lugar dado con la calidad requerida. La disponibilidad depende de la fiabilidad de los equipos, retrasos.

### 2.10.3. NO REPUDIACIÓN (RENDICIÓN DE CUENTAS)

Se asegura que el remitente de información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

### 2.10.4. CONFIDENCIALIDAD EN REDES INALÁMBRICAS

Según http://wilac.net/doc/tricalcar/materiales_abril2008/PDF_es/12_es_seguriad-inalambrica_guiav02.pdf la confidencialidad en redes inalámbricas "Se define como el hecho de asegurar que la información transmitida entre los clientes no sea revelada a personas no autorizadas"

La confidencialidad debe asegurar que la comunicación entre un grupo de puntos de acceso en un sistema de distribución inalámbrico (WDS por sus siglas en inglés), o un punto de acceso (AP) y una estación o cliente, se conserva protegida contra intercepciones.

### 2.10.5. AUTENTICACIÓN EN REDES INALÁMBRICAS

De acuerdo a lo expuesto en http://wilac.net/doc/tricalcar/materiales_abril 2008/PDF_es/12_es_seguridad-inamalbrica_guia_v02.pdf La autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas En otros términos, la autenticación inalámbrica significa “el derecho a enviar hacia y mediante el punto de acceso”. Para entender “Autenticación” en redes inalámbricas es necesario entender qué sucede en el inicio de la sesión de comunicación entre un punto de acceso y una estación inalámbrica. El inicio de una comunicación comienza por un proceso llamado “asociación”.

Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de “asociación”:

- Autenticación abierta
- Autenticación con llave compartida

La autenticación abierta implica NO seguridad y cualquiera puede hablarle al punto de acceso.

En la autenticación de llave compartida, se comparte una contraseña entre el punto de acceso y la estación cliente. Un mecanismo de reto/respuesta le permite al punto de acceso verificar que el cliente conoce la llave compartida, y entonces concede el acceso.

Pasos para la autenticación con llave compartida:

1. El cliente envía una solicitud de autenticación al AP
2. El AP envía una respuesta a la autenticación que contiene el texto de desafío sin cifrar
3. El cliente cifra el texto de desafío utilizando una de sus llaves y lo envía al AP
4. El AP comparara el texto de desafío sin cifrar con el texto de desafío cifrado. Si el texto es el mismo el AP permitirá que el cliente entre a la Red.

- **WEP (Wired Equivalent Privacy)**

WEP, brinda a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambradas. La necesidad de un protocolo como WEP es imprescindible, las redes inalámbricas funcionan a base de ondas de radio y son más vulnerables a ser interceptadas.

WEP utiliza una misma clave en las estaciones y el punto de acceso. Por lo que la clave se debe escribir manualmente en cada elemento de la red, esto genera varios inconvenientes. Ya que la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea divulgada. La distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que con lleva a que la clave no se cambie nunca.

- **WPA**

En WPA las claves son generadas dinámicamente y automáticamente distribuidas, lo que evita modificarlas manualmente como ocurría en WEP, Esta mejora en WPA se la realiza mediante un protocolo de integridad temporal de llaves (TKIP -Temporal Key Integrity Protocol).

WPA puede funcionar en dos modos:

- Con servidor, RADIUS. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor Radius, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

WPA / TKIP

TKIP inicialmente se lo denomino WEP 2 porque corrige la reutilización de la clave WEP para cifrar los datos, La gran diferencia de TKIP con WEP, es que

TKIP cambia la clave temporalmente con cada paquete o cuando se presenta un proceso de autenticación o itinerancia.

- **WPA2**

WPA2 (IEEE 802.11i) proporciona seguridad en redes WLAN. Incluye el algoritmo de cifrado AES (*AdvancedEncryption Standard*). Es un algoritmo con claves generalmente de 128 bits. Requiere un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Una mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

- WPA2 / AES

Además de la solución TKIP se puede utilizar AES el cual cuenta con algoritmos con soporte para cifrar claves de 128, 192, 256 bits además funciona con claves estáticas y dinámicas. AES ofrece un cifrado mucho más sólido generalmente utilizado para grandes empresas o corporaciones ya que la utilización de AES requiere que el Hardware y Software en el que va a operar este diseñado para este propósito, como más capacidad de memoria, CPU.

### 2.10.6. PORTALES CAUTIVOS PARA REDES INALÁMBRICAS

En una red donde la Autenticación se hace mediante portales cautivos, a los clientes se les permite asociarse con un punto de acceso sin Autenticación inalámbrica y obtener una dirección IP con el protocolo DHCP, no se requiere Autenticación para obtener la dirección IP. Una vez que el cliente obtiene la dirección IP, todas las solicitudes HTTP se capturan y son enviadas al portal cautivo, y el cliente es forzado a identificarse en una página web.
Los portales cautivos son responsables de verificar la validez de la contraseña y luego modificar el estatus del cortafuego. Las reglas del cortafuego esta comúnmente basadas en la dirección MAC del cliente y las direcciones IP.

### 2.10.7. DETENER LA DIFUSIÓN DE SSID COMO MEDIDA DE SEGURIDAD

Las redes cerradas se diferencian del estándar IEEE 802.11b en que el punto de acceso no difunda periódicamente su SSID. Evitar la publicación de SSID implica que los clientes de la red inalámbrica necesitan saber de manera previa que SSID deben asociar con un punto de acceso. Esta cualidad ha sido implantada por muchos fabricantes como una mejora de seguridad. La verdad es, mientras detener la difusión de la SSID previene a los clientes enterarse de la SSID por medio de una become frame, no impedirá que otro software de intercepción detecte la asociación que provenga de otro punto de la red cuando ésta eventualmente ocurra.

La detección de la difusión de la SSID no impedirá que una persona encuentre la SSID de la red. Configurando la red como “cerrada” solo añadirá una barrera adicional a un intruso corriente. Detener la difusión de la SSID debe considerarse como una precaución adicional, más no una medida de seguridad efectiva.