# DISEÑO, IMPLEMENTACION Y CONFIGURACION DE UNA RED INALAMBRICA EN LA CORPORACION UNIVERSITARIA MINUTO DE DIOS (GIRARDOT)

**DIEGO HERNAN MENDIGAÑA CASTILLO**
**YASSED FAROUK REINA ASCENCIO**

**CORPORACION UNIVERSITARIA MINUTO DE DIOS**
**TEC. EN REDES DE COMPUTADORES Y SEG. INFORMATICA - FACULTAD DE INGENIERIA**
**GIRARDOT**
**2008**

# DISEÑO, IMPLEMENTACION Y CONFIGURACION DE UNA RED INALAMBRICA EN LA CORPORACION UNIVERSITARIA MINUTO DE DIOS (GIRARDOT)

**DIEGO HERNAN MENDIGAÑA CASTILLO**
**YASSED FAROUK REINA ASCENCIO**

**Proyecto para optar el titulo de tecnólogo en Redes de Computadores y Seguridad Informática**

**MAURICIO RODRÍGUEZ GARCÍA**
**Ingeniero de Sistema**

**CORPORACION UNIVERSITARIA MINUTO DE DIOS**
**TEC. EN REDES DE COMPUTADORES Y SEG. INFORMATICA - FACULTAD DE INGENIERIA**
**GIRARDOT**
**2008**

**NOTA DE ACEPTACIÒN**

_____

_____

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del jurado

## DEDICATORIA

Dedico este Proyecto a mi padre Álvaro Hernán Mendigaña Feria y a mi madre Janeth Consuelo Castillo Rodríguez por la gran ayuda y el apoyo que me bridaron en esta etapa de mi vida, también gracias por creer en mí.

Por último dedico esto a la Corporación Universitaria Minuto de dios por permitirme ser parte de esta gran familia, a los profesores que a lo largo de estos 6 semestres me enseñaron y me prepararon para ser lo que hoy soy, además agradezco a mis demás compañeros de estudio, los que terminaron la carrera conmigo y a los que desafortunadamente no pudieron seguir con esta gran carrera tecnológica.

Obviamente también agradezco a mi Dios por darme una gran familia, unos grandes compañeros, amigos y unos excelentes profesores a lo largo de mi vida.

**Diego Hernán Mendigaña Castillo**

## DEDICATORIA

Primero agradezco a Dios ante todo por permitirme realizar este proyecto, ya que deja aun ardua experiencia en distintos campos además de la colaboración de mi compañero por apoyarme en los momentos más culminante de este proceso y brindarme su apoyo y confianza en el proyecto que hemos realizado.

A mi mama Sandra Azucena Reina y mis abuelos que sin apoyo no hubiera podido realizar este etapa tan importante de mi vida y gracias a sus consejos hoy en día me considero una persona que le puede aportar mucho a la sociedad como una persona de bien y por último a la Corporación Universitaria minuto de Dios que sin su apoyo y su ardua experiencia no hubiera podido surgir este proyecto para el bienestar de los estudiantes y demás grupo que pertenecen a esta gran familia.

**Yassed Farouk Reina Ascencio**

## AGRADECIMIENTOS

Agradecemos a la Corporación Universitaria Minuto de Dios por apoyarnos en este gran proyecto y por colaborarnos con los implementos de trabajo.

También agradecemos a todos los profesores que fueron parte de este trabajo, al Ing. Mauricio Rodríguez que con sus grandes conocimientos y profesionalismo nos enseño a ser cada día mejores en nuestro trabajo, a los Ingenieros Efraín Másmela y Fernanda Mosquera que sin su ayuda no hubiéramos podido desarrollar correctamente este proyecto.

También agradecemos al Director de la Corporación Universitaria Minuto de Dios quien nos acepto el proyecto y nos dio un espacio para poner en práctica lo aprendido.

Por último agradecemos a todas las personas relacionadas con la Universidad.

## TABLA DE CONTENIDO

# 1. INTRODUCCION

En la actualidad la vida de las personas en cuanto a las tecnologías de información está cambiando de una manera sorprendente, en especial en el ámbito de las telecomunicaciones.
Ya podemos observar gente con dispositivos móviles como los celulares, estos ya se convierten en parte fundamentales de la sociedad al punto que se vuelven dependientes, 90 de cada 100 personas tienen teléfono móvil, para poder comunicarse desde cualquier lugar sin necesidad de cables. Pasa lo mismo con los computadores. Hemos pasado de utilizar el servicio de internet desde el computador de la casa con un cable conectado a un modem para tener acceso a la red de redes a salir a cualquier lugar de nuestra ciudad y conectarnos a la misma red pero sin ningún elemento físico, simplemente con ondas de radio, o sea inalámbricamente. Eso es lo que quiere La Corporación Universitaria Minuto de Dios, no depender solamente de las dos salas de internet cableado que hay actualmente en la sede sino que además cuente con este mismo servicio pero con la ventaja de poder estar conectado en cualquier lugar de la misma.
Tal parece que ninguna persona se habría imaginado que fuera a existir un servicio en el que con solo hacer un clic tendríamos acceso a una gran cantidad de servicios virtuales, como la educación. Es por ello que las redes de computadoras está siendo implementada en cualquier lugar, tanto en hogares como en grandes empresas, no solo para tener acceso a la internet sino también para compartir gran cantidad de datos dentro de la empresa, nos referimos a una red de área local (LAN),esta es la que utiliza la universidad para compartir datos entro de la sede, de este tipo de red pasamos a una un poco mas grande, la red de área metropolitana (MAN), la cual es la conexión de varias LAN dentro de una área limitada como la conexión de edificios un poco alejados entre si; seguida de la MAN sigue la WAN o red de área extensa que es la conexión de varias redes locales pero a un nivel mucho mas amplio como la de compartir datos entre ciudades.
Así se fue incrementando este tipo de tecnología hasta convertirse en uno de los servicios más utilizados por la sociedad, la Internet. Ya podemos ver gran cantidad de dispositivos digitales que ofrecen el servicio de WI-FI, como los computadores portátiles, los teléfonos celulares, hasta ya existen automóviles con este servicio, ademas están incrementando las conexiones satelitales para poder observar televisión digital en nuestros hogares.
Mas adelante sabremos las ventajas y desventajas que presenta la implementación de una red inalámbrica, los elementos que se deben utilizar y los diferentes tipos de redes inalámbricas que existe para saber cual es la que mejor se adapta las necesidades de la Corporación Universitaria Minuto de Dios de Girardot.

# 2. IDENTIFICACION DEL PROBLEMA

## 2.1 DESCRIPCION DEL PROBLEMA

A la hora del montaje de la red inalámbrica la cual va a hacer desarrollada en la universidad Uniminuto de Dios sede Girardot, encontramos algunos puntos los cuales pueden afectar el desarrollo del proyecto en un futuro.
Por otra parte, en la Gestión de la red se esta estudiando la posibilidad de implementar un programa para el manejo de la red inalámbrica y local, por medio **Mikrotik** el cual representa muchos puntos a favor como la implementación de usuarios inalámbricos y control de ancho de banda por parte de las redes permitiéndonos mayor utilidad en nuestro canal de Internet.

## 2.2 FORMULACION DEL PROBLEMA

En la universidad Minuto de Dios sede Girardot, cada vez mas están incrementado los usuarios con computadores portátiles que exigen el servicio de internet inalámbrico para poder estar conectados es cualquier lugar de la sede. Este servicio se necesita ya que los computadores que poseen las salas que hay actualmente en la universidad no alcanzan para la gran cantidad de estudiantes que están ingresando constantemente a la misma. Este problema lleva a que los estudiantes no posean una solución que les permitan tener accesos a varios servicios de la Red de internet como por ejemplo comunidades educativas, motores de búsqueda, educación virtual, entre otros servicios, además de una herramienta pedagógica muy útil que mantendría a la vanguardia a la Universidad ante las innovaciones tecnológicas, ya que varias empresas, instituciones educativas y universidades del país cuentan con este servicio de conexión inalámbrica.

Además de estudios realizados comprobamos que este servicio es indispensable para el desarrollo integro é intelectual de los estudiantes de la Minuto de Dios sede Girardot.

**¿Cuál sería el mejor diseño tanto físico como lógico de una red Inalámbrica que será implementada en la Corporación Universitaria Minuto de Dios de Girardot?**

## 3. JUSTIFICACION

Las nuevas tecnologías de información inalámbrica conforman las redes de datos y archivos tanto de voz como de video. Algunos de los dispositivos que utilizan la red inalámbrica son los computadores portátiles, las PALM, los celulares de última generación, entre otros.

Una red inalámbrica permite utilizar varios dispositivos para tener acceso a datos desde cualquier lugar del planeta. Las redes inalámbricas son mucho más económicas ya que no hay necesidad de instalar los caros sistemas de conexión mediante fibra y cables, además de que en cierto modo son mucho más seguras, ya que para ingresar a alguna red es necesaria una contraseña de usuario.

Muchas universidades y empresas en Colombia ya están adoptando este tipo de tecnología, así que la Corporación Universitaria Minuto de Dios no tendría por que estar atrás, al contrario debería ser una de las mejores en cuanto a comunicación y transporte de datos se refiere.

En la universidad es necesaria una red inalámbrica ya que muchos estudiantes, profesores y usuarios de la universidad están utilizando dispositivos portátiles con servicio wi-fi, esto permitirá que ellos ingresen a la red mundial en cualquier lugar de la universidad sin necesidad de conectarse físicamente a ningún servidor de Internet. Obviamente antes de conectarse deberán solicitar un nombre de usuario y contraseña a los respectivos administradores de la red, ya que el servicio tendrá seguridad para que solamente usuarios de la universidad puedan acceder a ella.

# 4. OBJETIVOS

## 4.1 Objetivo General:

Diseñar e implementar una red inalámbrica en la Corporación Universitaria Minuto de Dios de Girardot para que las personas relacionadas con la misma tengan acceso a Internet desde cualquier lugar de la sede.

## 4.2 OBJETIVOS ESPECIFICOS:

- Ofrecer una nueva solución de comunicación en la universidad por medio de una red inalámbrica.
- Compartir datos con los usuarios por medio de la red inalámbrica que se desea implementar.
- Implementar más de un punto de acceso para tener una mayor cobertura.
- Establecer unas políticas de seguridad para el control de acceso de los usuarios.
- Tener gran cantidad de usuarios inalámbricos que estén relacionados con la universidad (estudiantes, profesores y trabajadores).
- Mantener y actualizar con el paso del tiempo el laboratorio de redes inalámbricas para así tener un mejor desempeño y servicio para los usuarios de la misma.

# 5. MARCO REFERENCIAL

## 5.1. MARCO LEGAL

## PROTOCOLOS QUE UTILIZA UNA RED INALAMBRICA

Los protocolos de las redes inalámbricas son las 802.11 (802.11a, 802.11b, y 802.11g):

• **802.11b**. Ratificado por IEEE el 16 de septiembre de 1999, el protocolo de redes inalámbricas 802.11b es probablemente el más asequible hoy en día. Millones de dispositivos que lo utilizan han sido vendidos desde 1999. Utiliza una modulación llamada Espectro Expandido por Secuencia Directa

–***Direct Sequence Spread Spectrum*** (***DSSS***)– en una porción de la banda ISM desde 2400 a 2484 MHz Tiene una tasa de transmisión máxima de 11Mbps, con una velocidad real de datos utilizable mayor a 5Mbps.

• **802.11g**. Como no estuvo finalizada sino hasta junio de 2003, el protocolo 802.11g llegó relativamente tarde al mercado inalámbrico. A pesar de esto, el protocolo 802.11g es hoy por hoy el estándar de factor en la redes inalámbricas utilizado como una característica estándar en virtualmente todas las laptops y muchos de los dispositivos handheld. Utiliza el mismo rango ISM que 802.11b, pero con el esquema de modulación denominado

***Orthogonal Frequency Division Multiplexing*** (***OFDM***) –Multiplexaje por División de Frecuencias Ortogonales. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 25Mbps), y mantiene compatibilidad con el altamente popular 802.11b gracias al soporte de las velocidades inferiores.

• **802.11a**. También ratificado por la IEEE el 16 de septiembre de 1999 el protocolo 802.11a utiliza OFDM. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 27Mbps). El 802.11a opera en la banda ISM entre 5725 y 5850MHz, y en una porción de la banda UNII entre 5.15 y 5.35GHz. Esto lo hace incompatible con el 802.11b o el 802.11g, y su alta frecuencia implica un rango más bajo comparado con el 802.11b/g al mismo nivel de potencia. Si bien esta porción del espectro es relativamente inutilizada comparada con la de 2.4GHz, desafortunadamente su uso es legal sólo en unos pocos lugares del mundo. Realice una consulta a sus autoridades locales antes de utilizar equipamiento 802.11a, particularmente en aplicaciones externas. Esto mejorará en el futuro, pues hay una disposición de la unión Internacional de comunicaciones (UIT) instando a todas las administraciones a abrir el uso de esta banda. El equipo es bastante barato, pero no tanto como el 802.11b/g.

## 5.2. MARCO INSTITUCIONAL

La corporación universitaria Minuto de Dios presenta una política de calidad regida por el cumplimiento de su misión se compromete dentro de la normatividad legal existente, a ofrecer y entregar servicios de educación superior de calidad reconocida, a satisfacer las necesidades y superar las expectativas del cliente, a buscar el mejoramiento continuo, a consolidar su cultura organizacional, a usar eficientemente los recursos, con personal competente apoyándose en sistemas de información e infraestructura suficientes, adecuados y actualizados.

El Sistema Universitario UNIMINUTO tiene como Objetivos de Calidad al 2012:

- obtener del MEN la acreditación institucional de la Sede Principal;
- obtener del MEN la (re)acreditación de 12 programas dando prioridad a los tecnológicos;
- desarrollar una cultura de servicio con el fin de satisfacer las necesidades y superar las expectativas del cliente interno y externo;
- obtener la certificación ISO 9001:2000

### 5.2.1. Misión

El Sistema Universitario UNIMINUTO inspirado en el Evangelio, la espiritualidad Eudista y la Obra Minuto de Dios; agrupa Instituciones que comparten un modelo universitario innovador; para ofrecer Educación Superior de alta calidad, de fácil acceso, integral y flexible; para formar profesionales altamente competentes, éticamente responsables líderes de procesos de transformación social; para construir un país justo, reconciliado, fraternal y en paz.

### 5.2.2. Visión

El Sistema Universitario UNIMINUTO en el 2012 será reconocido en Colombia por las vivencias espirituales y la presencia de Dios en el ámbito universitario; su contribución al desarrollo del país a través de la formación en Educación para el Desarrollo; la alta calidad de sus programas académicos estructurados por ciclos y competencias; su impacto en la cobertura originado en el número de sus Sedes y la gran facilidad de acceso a sus programas; y sus amplias relaciones nacionales e internacionales.

## 5.3 MARCO CONCEPTUAL

Una red inalámbrica es un grupo de ordenadores interconectados entre si sin ningún medio físico como cables ni canaletas, están conectados por medio de

ondas electromagnéticas o infrarrojas. Existen varias clases de redes inalámbricas, pero una de las más populares es la WLAN, mas conocida como WI-FI.

Algunas computadoras vienen equipadas para el servicio inalámbrico. Los ordenadores más nuevos vienen adaptados para Wi-Fi. Los computadores anteriores necesitaban conectarle una tarjeta inalámbrica.

El comportamiento de una red inalámbrica es idéntico al de una red que se encuentra cableada con respecto a compartir diferentes tipos de datos y recursos.

## 5.4 MARCO TEORICO

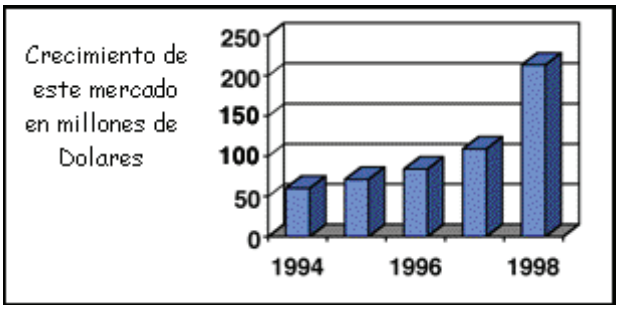
### Orígenes de las Redes Inalámbricas

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en **1979** de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 el FCC (Federal Communications Comission) asigno las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2, 400-24835 GHz, 5,725-5, 850 GHz a las redes inalámbricas basadas en spread spectrum.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.
Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y los precios elevados de una solución inalámbrica.

Crecimiento de las redes inalámbricas en el mercado:



Sin embargo, se viene produciendo estos últimos años un crecimiento explosivo en este mercado (de hasta un 100% anual). Y esto es debido a distintas razones:

• El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles.

• La conclusión de la norma IEEE 802.11 para redes de área local inalámbricas que ha establecido un punto de referencia y ha mejorado en muchos aspectos de estas redes.

**Tipo de redes inalámbricas:**

**Redes inalámbrica de área personal (WPAN)** mas que todo utilizadas por los dispositivos celulares, su cubrimiento es de aproximadamente 12 mts, en esta red su finalidad es la conexión de diferentes ordenadores los cuales pueden estar ubicados en distintos puntos del lugar de trabajo.

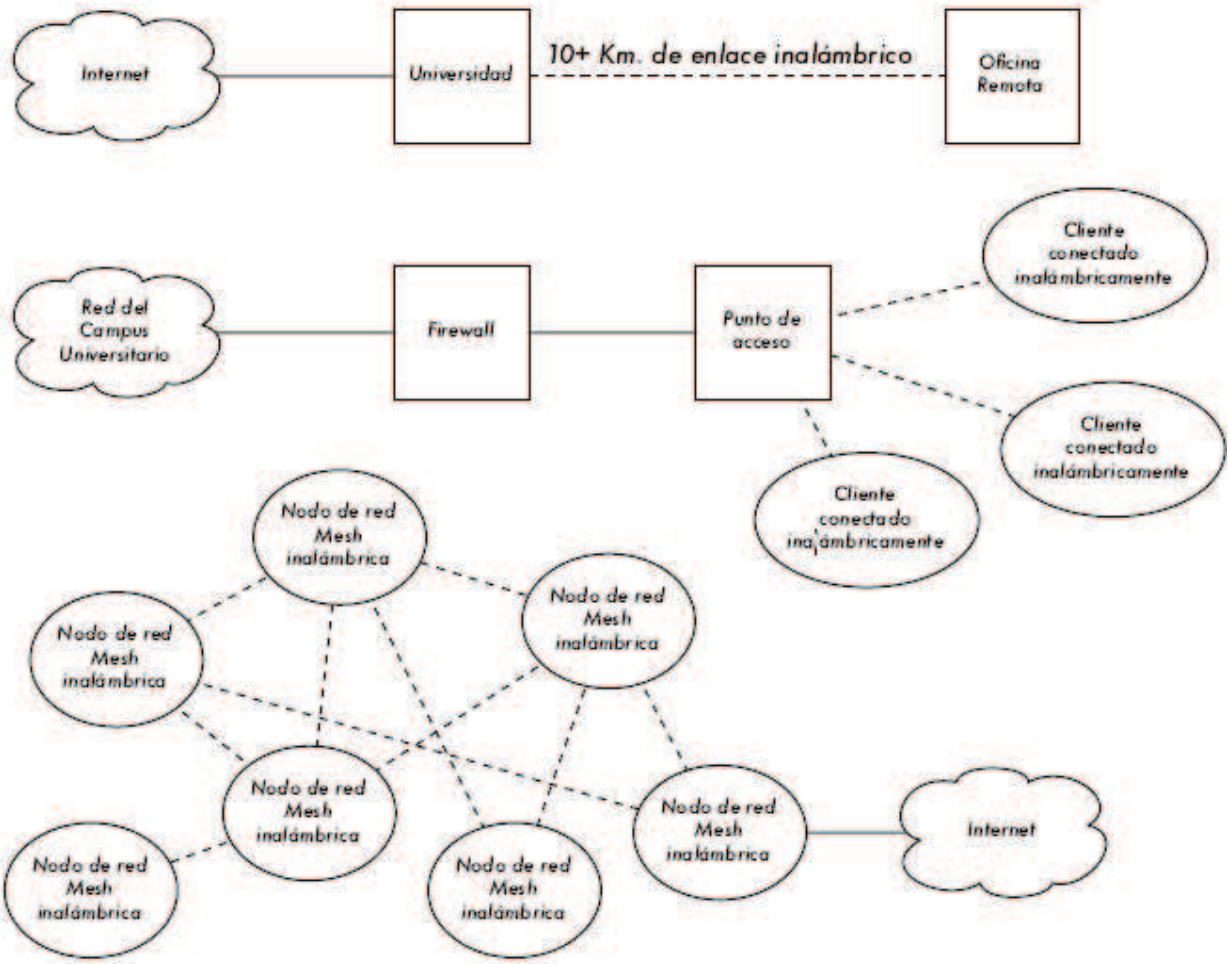
**Redes inalámbricas de área local (WLAN)** estas redes tienen una rango de señal mayor que las redes personales, son las mas utilizadas en edificios lugares donde se necesita transportar el PC libremente, mas conocidas como wi-fi (WIreles-FIdelity).

**Redes inalámbricas de área metropolitana (WMAN)** la señal es mucho mas extensa que las anteriores, su objetivo es interconectar varias sedes de una empresa u otros que estén a largas distancias como una ciudad con otra, esta clase de red es mas conocida como WI-MAX (Wireless-MAxim).

**Redes de cubrimiento global (WWAN)** son utilizadas por la tecnología celular, su objetivo es conectar varias regiones a nivel mundial, a su vez la telefonía celular se divide en varias generación van desde la 1 hasta la cuatro, cada una con mayor capacidad de señal de transmisión que la otra.

## DISEÑO DE REDES

Primero que todo vamos a ver algunos ejemplos de redes inalámbricas:

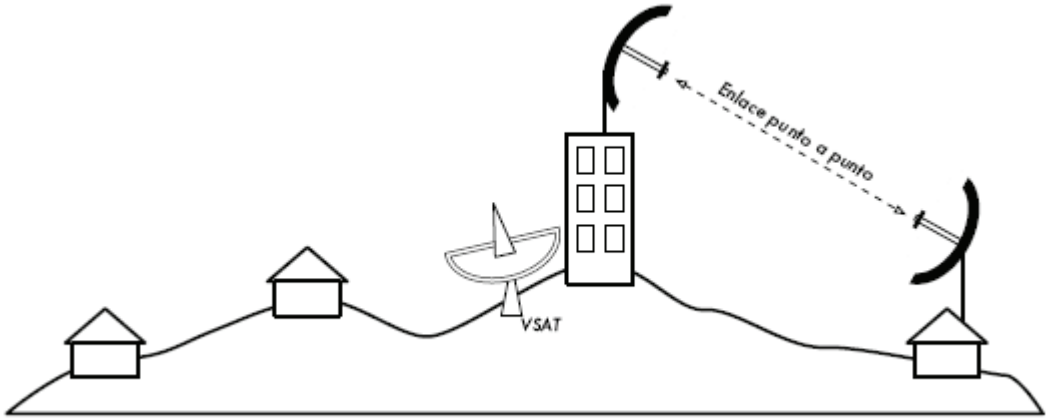


Las redes inalámbricas están organizadas en 3 configuraciones lógicas:

• Enlaces punto a punto
• Enlaces punto a multipunto
• Nubes multipunto a multipunto

**ENLACE PUNTO A PUNTO:**

Los enlaces ***punto a punto*** generalmente se usan para conectarse a Internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder al mismo. Por ejemplo, una Universidad puede tener una conexión *Frame Relay* o una conexión VSAT dentro del campus, pero difícilmente podrá justificar otra conexión de la misma índole a un edificio muy importante fuera del campus. Si el edificio principal tiene una visión libre de obstáculos hacia el lugar remoto, una conexión punto a punto puede ser utilizada para unirlos. Ésta puede complementar o incluso remplazar enlaces discados existentes. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto seguros de más de treinta kilómetros.

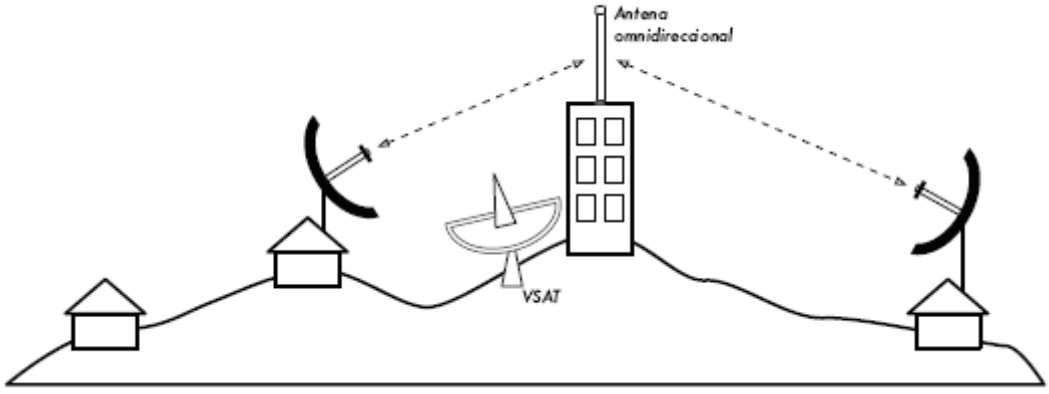



Una vez hecha una conexión punto a punto, se pueden añadir otras para extender la red aún más. Si en nuestro ejemplo, un edificio alejado se encuentra en la cima de una gran colina, puede ser posible ver otras locaciones importantes que no pueden ser vistas directamente desde el campus central. Mediante la instalación de otro enlace punto a punto hacia el lugar remoto, se puede unir a la red otro nodo y hacer uso de la conexión central a Internet. Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a Internet. Supongamos que debe desplazarse hasta una estación de monitoreo meteorológico alejada, –ubicada en lo alto de una colina–, para recolectar los

datos que ella toma. Podría conectar el lugar con un enlace punto a punto, logrando la recolección y el monitoreo de datos en tiempo real, sin tener que ir hasta el lugar. Las redes inalámbricas pueden proveer suficiente ancho de banda como para transmitir grandes cantidades de datos (incluyendo audio y video) entre dos puntos, aún en ausencia de conexión a Internet.

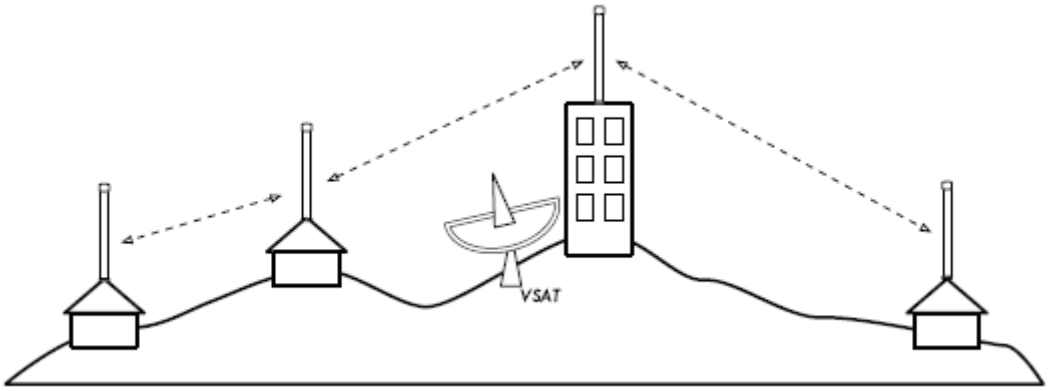
## PUNTO A MULTIPUNTO

La siguiente red más comúnmente encontrada es la ***punto a multipunto*** donde varios nodos están hablando con un punto de acceso central, esta es una aplicación punto a multipunto. El ejemplo típico de esta disposición es el uso de un punto de acceso inalámbrico que provee conexión a varias computadoras portátiles. Las computadoras portátiles no se comunican directamente unas con otras, pero deben estar en el rango del punto de acceso para poder utilizar la red.




## MULTIPUNTO A MULTIPUNTO

El tercer tipo de diseño de red es el ***multipunto a multipunto***, el cual también es denominado red ***ad hoc*** o en malla (***mesh***). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.




El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. Las buenas implementaciones de redes *mesh* son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red *mesh* es tan sencillo como agregar más nodos. Si uno de los nodos en la "nube" tiene acceso a Internet, esa conexión puede ser compartida por todos los clientes.
Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento.

Después de haber leído lo anterior, quedan claras algunas dudas acerca de las redes inalámbricas.

En el laboratorio de redes de la universidad minuto de dios, habrán entre 4 y 6 computadores de con conexión cableada, y un mínimo de dos computadores portátiles o computadores con tarjeta de red inalámbrica para su conexión sin ningún medio físico.

Contaremos con un Punto de Acceso marca 3com 7760 con tecnología inalámbrica 11a/b/g, este será el encargado de repartir y enviar correctamente el mensaje a destinatario sin ningún problema, además de dar la señal suficiente a cada uno de los PCs que están conectados a la red. Las computadoras portátiles no se comunican directamente unas con otras, pero deben estar en el rango del punto de acceso para utilizar la red.
Para la conexión a internet primero que todo debemos tener un proveedor de servicio de internet, este obviamente va a ser una empresa de telefonía. La línea telefónica va a ir conecta a el Punto de Acceso y luego este estará conectado por el puerto WAN a la tarjeta de red de un computador que en este caso será el servidor que configurará el Punto de Acceso para tener el servicio que deseamos, hay que tener en cuenta que este Punto de Acceso tendrá dos antenas inalámbricas, ya que estamos hablando de redes inalámbricas.

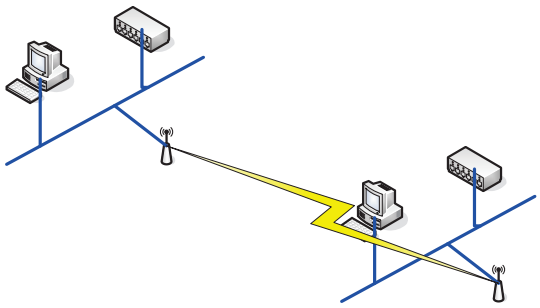
Uniremos inalámbricamente la sede de la Presentación con la sede de la García Herreros por medio de dos antenas en un enlace punto a punto para poder enviar y recibir datos sin necesidad de estar yendo y viniendo de una sede a la otra (claro, si hay los suficientes recursos para hacerlo).

**Otras configuraciones. Interconexión de redes**

Las posibilidades de las redes inalámbricas pueden verse ampliadas gracias a la interconexión con otras redes, sobre todo con redes no inalámbricas. De esta forma los recursos disponibles en ambas redes se amplían.

Mediante el uso de antenas (direccionales o omnidireccionales) es posible conectar dos redes separadas por varios cientos de metros, como por ejemplo dos redes locales situadas en dos edificios distintos. De esta forma, una LAN no inalámbrica se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serian más costosas, o simplemente imposibles

Interconexión LAN mediante antenas direccionales



**Capa física**

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos.

IEEE 802.11 define tres posibles opciones para la elección de la capa física:

• Espectro expandido por secuencia directa o **DSSS** (Direct Sequence Spread Spectrum),

• Espectro expandido por salto de frecuencias o **FHSS** (Frecuency Hopping Spread Spectrum) -ambas en la banda de frecuencia 2.4 GHz ISM-

• Y luz **infrarroja** en banda base -o sea sin modular-.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otra. No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final.

**Microondas**

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las super altas frecuencias. SHF utilizándose para las redes inalámbricas la banda de los 18-19 GHz. Estas redes tienen una propagación muy localizada y un ancho de banda que permite alcanzar los 15 Mbps.

**Laser**

La tecnología laser tiene todavía que resolver importantes cuestiones en el terreno de las redes inalámbricas antes de consolidar su gran potencia de aplicación.

Hoy en dia resulta muy útil para conexiones punto a punto con visibilidad directa, utilizándose fundamentalmente en interconectar segmentos distantes de redes locales convencionales (Ethernet y Token ring). Es de resaltar el hecho de que esta técnica se encuentre en observación debido al posible perjuicio para la salud que supone la visión directa del haz. Como circuitos punto a punto se llegan a cubrir distancias de hasta 1000 metros, operando con una longitud de onda de 820 nanómetros.

**Radiofrecuencia**

Aunque existen dos tipos de tecnologías que emplean las radiofrecuencias, la banda estrecha y la banda ancha, también conocida espectro ensanchado, ésta última es la que más se utiliza.

En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las

bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro ensanchado. Entre ellas, el IEEE 802.11 incluyo en su especificación las frecuencias en torno a 2,4 GHz que se habían convertido ya en el punto de referencia a nivel mundial, la industria se había volcado en ella y está disponible a nivel mundial.

La tecnología de espectro ensanchado, utiliza **todo el ancho de banda disponible**, en lugar de utilizar una portadora para concentrar la energía a su alrededor. Tiene muchas características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias (como la de banda estrecha, que utiliza microondas), ya que, por ejemplo, posee excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación. Esta, como muchas otras tecnologías, proviene del sector militar.

Existen dos tipos de tecnología de espectro ensanchado:

**Espectro Ensanchado por Secuencia Directa (DSSS)**

- En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o *PseudoNoise*). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente:

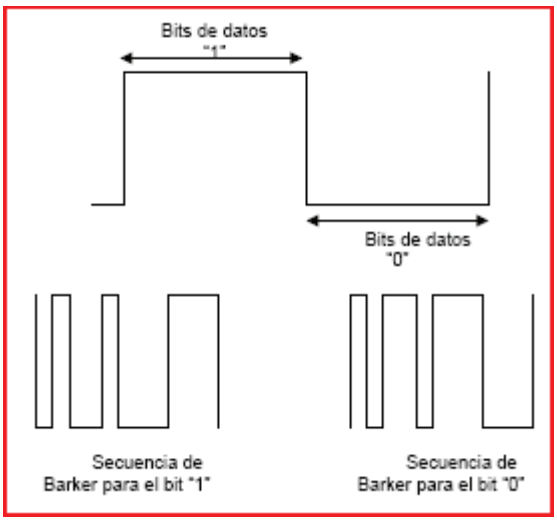
+1 –1 +1 +1 –1 +1 +1 +1 –1 –1 –1 –1

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10.4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

A continuación podemos observar cómo se utiliza la secuencia de *Barker* para codificar la señal original a transmitir:

Codificación de Barker




Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación ***DBPSK*** (Differential Binary Phase Shift Keying) y la modulación ***DQPSK*** (Differential Quadrature Phase Shift Keying), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

Recientemente el IEEE ha revisado este estándar, y en esta revisión, conocida como 802.11b, además de otras mejoras en seguridad, aumenta esta velocidad hasta los 11Mbps, lo que incrementa notablemente el rendimiento de este tipo de redes.

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país esta autorizado a utilizar un subconjunto de estos canales. En el caso de España se utilizan los canales 10 y 11, que corresponden a una frecuencia central de 2,457 GHz y 2,462 GHz.

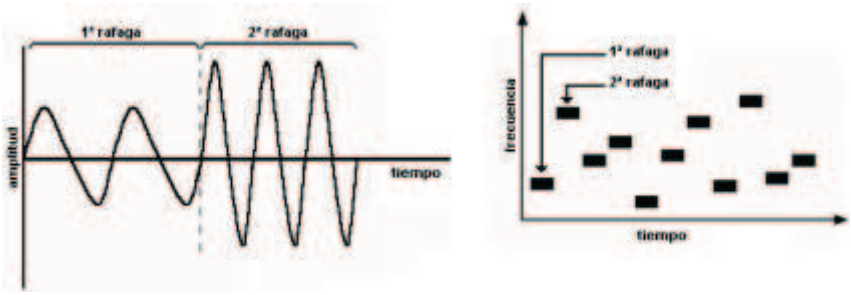
En configuraciones donde existan mas de una celda, estas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal.

La técnica de DSSS podría compararse con una multiplexacion en frecuencia:

| Canal | Frec. U.S.A | Frec. Europa | Frec. Japón |
|---|---|---|---|
| 1 | 2412 MHz | N/A | N/A |
| 2 | 2417 MHz | N/A | N/A |
| 3 | 2422 MHz | 2422 MHz | N/A |
| 4 | 2427 MHz | 2427 MHz | N/A |
| 5 | 2432 MHz | 2432 MHz | N/A |
| 6 | 2437 MHz | 2437 MHz | N/A |
| 7 | 2442 MHz | 2442 MHz | N/A |
| 8 | 2447 MHz | 2447 MHz | N/A |
| 9 | 2452 MHz | 2452 MHz | N/A |
| 10 | 2457 MHz | 2457 MHz | N/A |
| 11 | 2462 MHz | 2462 MHz | N/A |
| 12 | N/A | N/A | 2484 MHz |

**Espectro ensanchado por salto de frecuencia (FHSS)**

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una **determinada frecuencia durante un intervalo de tiempo** llamada *dwell time* e inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un **intervalo muy corto de tiempo**.




Gráfica de Codificación con Salto en Frecuencia

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer.

Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en le tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica también utiliza la zona de los 2.4GHz, la cual organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltas de 2.5 por segundo.

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia *FSK* (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps.

En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps.

La técnica FHSS sería equivalente a una multiplexación en frecuencia

| Limite inferior | Límite superior | Rango regulatorio | Area geográfica |
|---|---|---|---|
| 2.402 GHz | 2.480 GHz | 2.400-2.4835 GHz | América del Norte |
| 2.402 GHz | 2.480 GHz | 2.400-2.4835 GHz | Europa |
| 2.473 GHz | 2.495 GHz | 2.471-2.497 GHz | Japón |
| 2.447 GHz | 2.473 GHz | 2.445-2.475 GHz | España |
| 2.448 GHz | 2.482 GHz | 2.4465-2.4835 GHz | Francia |

Rango de frecuencias centrales empleadas en FHSS

| Canal | Valor | Canal | Valor | Canal | Valor |
|---|---|---|---|---|---|
| 2 | 2.402 | 28 | 2.428 | 54 | 2.454 |
| 3 | 2.403 | 29 | 2.429 | 55 | 2.455 |
| 4 | 2.404 | 30 | 2.430 | 56 | 2.456 |
| 5 | 2.405 | 31 | 2.431 | 57 | 2.457 |
| 6 | 2.406 | 32 | 2.432 | 58 | 2.458 |
| 7 | 2.407 | 33 | 2.433 | 59 | 2.459 |
| 8 | 2.408 | 34 | 2.434 | 60 | 2.460 |
| 9 | 2.409 | 35 | 2.435 | 61 | 2.461 |
| 10 | 2.410 | 36 | 2.436 | 62 | 2.462 |
| 11 | 2.411 | 37 | 2.437 | 63 | 2.463 |
| 12 | 2.412 | 38 | 2.438 | 64 | 2.464 |
| 13 | 2.413 | 39 | 2.439 | 65 | 2.465 |
| 14 | 2.414 | 40 | 2.440 | 66 | 2.466 |
| 15 | 2.415 | 41 | 2.441 | 67 | 2.467 |
| 16 | 2.416 | 42 | 2.442 | 68 | 2.468 |
| 17 | 2.417 | 43 | 2.443 | 69 | 2.469 |
| 18 | 2.418 | 44 | 2.444 | 70 | 2.470 |
| 19 | 2.419 | 45 | 2.445 | 71 | 2.471 |
| 20 | 2.420 | 46 | 2.446 | 72 | 2.472 |
| 21 | 2.421 | 47 | 2.447 | 73 | 2.473 |
| 22 | 2.422 | 48 | 2.448 | 74 | 2.474 |
| 23 | 2.423 | 49 | 2.449 | 75 | 2.475 |
| 24 | 2.424 | 50 | 2.450 | 76 | 2.476 |
| 25 | 2.425 | 51 | 2.451 | 77 | 2.477 |
| 26 | 2.426 | 52 | 2.452 | 78 | 2.478 |
| 27 | 2.427 | 53 | 2.453 | 79 | 2.479 |
| | | | | 80 | 2.480 |

Requisitos norteamericanos y europeos
( Valores especificados en GHz )

| Canal | Valor | Canal | Valor | Canal | Valor |
|---|---|---|---|---|---|
| 47 | 2.447 | 56 | 2.456 | 65 | 2.465 |
| 48 | 2.448 | 57 | 2.457 | 66 | 2.466 |
| 49 | 2.449 | 58 | 2.458 | 67 | 2.467 |
| 50 | 2.450 | 59 | 2.459 | 68 | 2.468 |
| 51 | 2.451 | 60 | 2.460 | 69 | 2.469 |
| 52 | 2.452 | 61 | 2.461 | 70 | 2.470 |
| 53 | 2.453 | 62 | 2.462 | 71 | 2.471 |
| 54 | 2.454 | 63 | 2.463 | 72 | 2.472 |
| 55 | 2.455 | 64 | 2.464 | 73 | 2.473 |

Requisitos españoles
( Valores especificados en GHz )

## TECNOLOGIA DE INFRARROJOS

La verdad es que IEEE 802.11 no ha desarrollado todavía en profundidad esta área y solo menciona las características principales de la misma:

• Entornos muy localizados, un aula concreta, un laboratorio, un edificio.

• Modulaciones de16-PPM y 4-PPM que permiten 1 y 2 Mbps de transmisión.

• Longitudes de onda de 850 a 950 manómetros de rango.

• Frecuencias de emisión entre 3,15·10e14 Hz y 3,52·10e14 Hz.

Las WLAN por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre. Los sistemas de infrarrojos se sitúan en **altas frecuencias**, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos son susceptibles de ser interrumpidos por cuerpos opacos pero se pueden reflejar en determinadas superficies.

Para describir esta capa física seguiremos las especificaciones del IrDA organismo que ha estado desarrollando estándares para conexiones basadas en infrarrojos.

Para la capa infrarroja tenemos las siguientes velocidades de transmisión:

• 1 y2 Mbps Infrarrojos de modulación directa.

• 4 Mbps mediante Infrarrojos portadora modulada.

• 10 Mbps Infrarrojos con modulación de múltiples portadoras.

### Clasificación

De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojos pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista (line of sight, LOS) y en sistemas de gran apertura, reflejados o difusos (diffused).

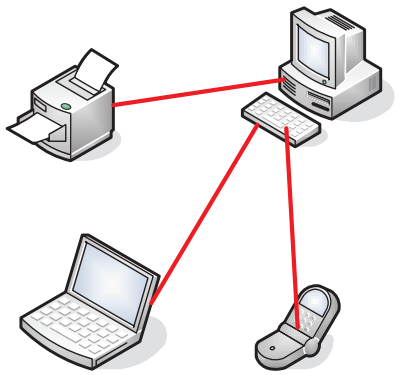
- Los sistemas infrarrojos de corta apertura, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los

controles remotos de las televisiones: el emisor debe orientarse hacia el receptor antes de empezar a transferir información, limitando por tanto su funcionalidad. Resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que esta mas orientado a la portabilidad que a la movilidad.

- Los sistemas de gran apertura permiten la información en ángulo mucho más amplio por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos.

La dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor). Esta es una de las dificultades que han retrasado el desarrollo del sistema infrarrojo en la norma 802.11.

La tecnología infrarrojo cuenta con muchas características sumamente atractivas para utilizarse en WLANs: el infrarrojo ofrece una amplio ancho de banda que transmite señales a velocidades altas; tiene una longitud de onda cercana a la de la luz y se comporta como ésta (no puede atravesar objetos sólidos como paredes, por lo que es inherentemente seguro contra receptores no deseados); debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por dispositivos hechos por el hombre (motores, luces ambientales, etc.); la transmisión infrarroja con láser o con diodos no requiere autorización especial en ningún país (excepto por los organismos de salud que limitan la potencia de la señal transmitida); utiliza un protocolo simple y componentes sumamente económicos y de bajo consumo de potencia, una característica importante en dispositivos móviles portátiles.



Transmisión por infrarrojos

Entre las **limitaciones** principales que se encuentran en esta tecnología se pueden señalar las siguientes: es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre emisor y receptor; las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unas cuantas decenas de metros; la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.

Las velocidades de transmisión de datos no son suficientemente elevadas y solo se han conseguido en enlaces punto a punto. Por ello, lejos de poder competir globalmente con las LAN de radio frecuencia, su uso está indicado más bien como apoyo y complemento a las LAN ya instaladas, cableadas o por radio, cuando en la aplicación sea suficiente un enlace de corta longitud punto a punto que, mediante la tecnología de infrarrojos, se consigue con mucho menor coste y potencia que con las tecnologías convencionales de microondas.

## Capas y protocolos

El principio de funcionamiento en la capa física es muy simple y proviene del ámbito de las comunicaciones ópticas por cable: un LED (Light Emitting Diode), que constituye el dispositivo emisor, emite luz que se propaga en el espacio libre en lugar de hacerlo en una fibra óptica, como ocurre en una red cableada. En el otro extremo, el receptor, un fotodiodo PIN recibe los pulsos de luz y los convierte en señales eléctricas que, tras su manipulación (amplificación, conversión a formato bit –mediante un comparador- y retemporización) pasan a la UART (Universal Asynchronous Receiver Transmitter) del ordenador, de forma que para la CPU todo el proceso luminoso es absolutamente transparente.

- Tras la **capa física** se encuentra la capa de enlace, conocida como IrLAP, (Infrared Link Access Protocol) que se encarga de gestionar las tareas relacionadas con el establecimiento, mantenimiento y finalización del enlace entre los dos dispositivos que se comunican. IrLAP constituye una variante del protocolo de transmisiones asíncronas HDLC (Half Duplex Line Control) adaptada para resolver los problemas que plantea el entorno radio. El enlace establece dos tipos de estaciones participantes, una actúa como maestro y otra como esclavo. El enlace puede ser punto a punto o punto a multipunto, pero en cualquier caso la responsabilidad del enlace recae en el maestro, todas las transmisiones van a o desde ella.

- La **capa de red** esta definida por el protocolo IrLMP (Infrared Link Management Protocol), la capa inmediatamente superior a IrLAP, se encarga del seguimiento de los servicios (como impresión, fax y módem), así como de los recursos disponibles por otros equipos, es decir, disponibles para el enlace.

- Finalmente, la **capa de transporte**, IrTP (Infrared Transport Protocol) se ocupa de permitir que un dispositivo pueda establecer múltiples haces de datos en un solo enlace, cada uno con su propio flujo de control. Se trata, pues, de multiplexar el flujo de datos, lo cual permite, por ejemplo, el spool de un documento a la impresora mientras se carga el correo electrónico del servidor. Este software, de carácter opcional –dado que no es necesario para la transferencia básica de ficheros- resulta útil cuando se ha de establecer un enlace, por ejemplo, entre un PDA (Personal Digital Assistant) y la LAN.

**La capa MAC**

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas. Ya que deben de tenerse en cuenta las dos topologías de una red inalámbrica:

• ad-hoc: redes peer-to-peer. Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias…

• basadas en infraestructura: La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que

controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se tiene que tener en cuenta:

• Perturbaciones ambientales (**interferencias**)

• Variaciones en la **potencia** de la señal

• **Conexiones y desconexiones** repentinas en la red

• **Roaming**. Nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas. Ayudando a la fabricación en serie de chips.

**Protocolos con arbitraje**

La **multiplexación en frecuencia** (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama **multiplexación en el tiempo** (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

**Protocolos de acceso por contienda**

Tienen similitudes al de Ethernet cableada de línea normal 802.3.

CSMA (Code-division multiple Access = Acceso múltiple por división de tiempo).

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. En este esquema se asigna una secuencia PN distinta a cada

nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

CSMA/CD (Carrier Sense, Multiple Access, Collision Detection)

Como en estos medios de difusión (radio, infrarrojos), no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseño una variación denominada detección de colisiones (peine) para redes inalámbricas. En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria seudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama. A continuación, el nodo realiza la detección de la portadora si el canal está libre transmite la secuencia del peine. Por cada 1 del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada 0 del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

Cuadro de comparación de acuerdos a las diferentes tecnologías de redes inalámbricas:

| **TECNOLOGIA** | **ESTANDAR** | **APLICACIÓN** | **AMBITO COBERTURA mts** | **FRECUENCIA GHz** |
|---|---|---|---|---|
| UWB | 802.15.3a | WPAN | 10 | 705 |
| WI-FI | 802.11a | WLAN | 100 | 5 |
| | 802.11b | WLAN | 100 | 2.4 |
| | 802.11g,n | WLAN | 100 | 4.4 |
| Wi-Max | 802.16d | WMAN | 6400 a 9600 | 11 |
| | 802.16e | Móvil/MAN | 1600 a 4800 | 2 a 6 |
| WCDMA | 3G | WWAN | 1600 a 8000 | 1.8, 1.9, 2.1 |

## SEGURIDAD EN LA RED INALÁMBRICA

En una red cableada tradicional, el control del acceso es muy sencillo: si una persona tiene acceso físico a una computadora o a un *hub* (concentrador) de la red, entonces pueden usar (o abusar) de los recursos de la red. Si bien los mecanismos a través de software son un componente importante de la seguridad de la red, el mecanismo decisivo es limitar el acceso físico a los dispositivos de la red. Es simple: si todas las terminales y los componentes de la red son accedidos sólo por personas de confianza, entonces la red puede ser considerada confiable.

En esta red inalámbrica es muy diferente. A pesar de que el alcance aparente de su punto de acceso puede ser de unos cuantos metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso de la red aunque esté a varias manzanas de distancia. Aún cuando un usuario no autorizado sea detectado, es imposible "rastrear el cable" hasta el lugar donde está esa persona. Sin transmitir ni un solo paquete, un usuario malintencionado puede registrar todos los datos de la red a un disco. Más adelante estos datos pueden utilizarse para lanzar un ataque más sofisticado contra la red. Hay que tener en cuenta que la señal de la red nunca se va detener en el límite de la universidad, esta señal ira hasta donde la potencia del punto de acceso lo permita, así que es muy fácil que cualquier persona ingrese a la red desde unos cientos de metros por fuera de la universidad.

Es por eso que ingresaremos un serie de software para administrar correctamente la red, como por ejemplo, configurar la red para que solo se pueda ingresar mediante una contraseña muy difícil o prácticamente imposible de descifrar por medio de cualquier software malicioso, para que a si cualquier persona que quiera ingresar a la red de internet tendrá que solicitar un nombre de usuario y una contraseña, obviamente el usuario que desea el servicio tiene que estar vinculado con la universidad

## ENCRIPTACION

El método de encriptación más utilizado en las redes inalámbricas es el llamado ***encriptación WEP***. WEP ***significa privacidad equivalente*** a la cableada (*del inglés Wired Equivalent Privacy*), y es soportada por casi todo el equipamiento 802.11ª/b/g. WEP utiliza una clave compartida de 40-bits para encriptar los datos entre el punto de acceso y el cliente. La clave debe ingresarse en los AP así como en cada uno de los clientes. Cuando se habilita WEP, los clientes no pueden asociarse con el AP hasta que utilicen la clave correcta. Una persona con un equipo con tarjeta inalámbrica y un software de detección de redes wifi puede estar oyendo una red con WEP, este puede ver el tráfico y las direcciones MAC, pero los mensajes de los datos de cada paquete están encriptados. Esto provee a la red de un buen mecanismo de autenticación, además de darle un poco de privacidad.

WEP definitivamente no es la mejor solución de encriptación que haya disponible. Por un lado, la clave WEP se comparte entre todos los usuarios, y si la misma está comprometida (es decir, si un usuario le dice a un amigo la contraseña, o se va un empleado) entonces cambiar la contraseña puede ser extremadamente difícil, ya que todos los AP y los dispositivos cliente deben cambiarla. Esto también significa que los usuarios legítimos de la red pueden escuchar el tráfico de los demás, ya que todos conocen la clave.

Otro protocolo de autenticación en la capa de enlace de datos es el **Acceso Protegido Wi-Fi**, o ***WPA*** (***Wi-Fi Protected Access*** *por su sigla en inglés*). WPA se creó específicamente para lidiar con los problemas de WEP que mencionamos antes. Provee un esquema de encriptación significativamente más fuerte, y puede utilizar una clave privada compartida, claves únicas asignadas a cada usuario, o inclusive un certificado SSL para autenticar el punto de acceso y el cliente. Las credenciales de autenticación se chequean usando el protocolo 802.1X, el cual puede consultar una base de datos externa como RADIUS. Mediante el uso de un Protocolo de Integridad Temporal de la Clave (*TKIP –Temporal Key Integrity Protocol*), las claves se pueden rotar rápidamente, reduciendo la posibilidad de que una sesión en particular sea descifrada. En general, WPA provee una autenticación y privacidad significativamente mejor que el estándar WEP.

El problema con WPA, es que la interoperabilidad entre los vendedores es aún muy baja. WPA requiere equipamiento de última generación para los puntos de acceso, y *firmware* actualizado en todos los clientes inalámbricos, así como una configuración laboriosa. Si uno controla la totalidad de la plataforma de equipamiento del lugar donde está realizando la instalación, WPA puede ser ideal. La autenticación de los clientes y de los AP, resuelve los problemas de puntos de acceso deshonestos y provee muchas más ventajas que WEP. Pero en la mayoría de las instalaciones de red donde el equipamiento es variado y el conocimiento de los usuarios es limitado, instalar WPA puede ser una pesadilla. Por esta razón es que la mayoría continua utilizando WEP, si es que usa algún tipo de encriptación.

Pero ahora existe un nuevo método de seguridad asociada con la WPA, llamada **WPA2:**
La norma 802.11i, nueva norma ratificada en 2004, propone una solución de seguridad avanzada para las redes inalámbricas WiFi, esta se basa en el logaritmo de cifrado TKIP, como WPA, pero por el contrario soporta AES – en lugar de RC4 – mucho más seguro en cuanto al cifrado de datos. De esta forma la WiFi Alliance ha creado una nueva certificación, llamada WPA-2, para los equipos que soportan el estándar 802.11i.

WPA-2 así como su predecesor – WPA -, garantiza el cifrado así como la

integridad de los datos pero además ofrece nuevas funciones de seguridad tal como “Key Caching” y la “Pre-Autenticación”.

***Key Caching:***

Permite al usuario conservar la clave PMK (Pairwise Master Key)- variante de PSK (Pre-Shared Key) del protocolo WPA – cuando la autenticación ha terminado con éxito y a fin de que pueda reutilizarla en sus próximas transacciones con el mismo punto de acceso. Esto quiere decir que un usuario móvil sólo necesita identificarse una sola vez con un punto de acceso específico. En efecto, éste no tiene más que conservar la clave PMK – lo que es administrado por PMKID (Pairwise Master Key Identifier) que no es más que una simplificación aleatoria de la clave PMK, la dirección MAC del punto de acceso y del cliente móvil, y una cadena de caracteres. De este modo, PMKID identifica de manera única la clave PMK.

***La Pre-Autenticación:***

Esta función permite a un usuario móvil identificarse con otro punto de acceso al que necesitará conectarse más adelante. Este proceso es realizado redirigiendo las tramas de autenticación, generadas por el cliente enviado desde el punto de acceso actual, hacia el punto futuro de acceso a través de la red cableada. Sin embargo, el hecho que una estación pueda conectarse a varios puntos de acceso al mismo tiempo incrementa de manera considerable el tiempo de carga. Para resumir, WPA-2 ofrece en relación a WPA:

- Una mayor eficacia en cuanto a la seguridad y movilidad, gracias a la autenticación del cliente independientemente del lugar donde ese encuentra.
- Fuerte integridad y confidencialidad garantizadas por un mecanismo de distribución dinámica de claves.
- Flexibilidad gracias a una re-autenticación rápida y segura.

**FILTRADO MAC:**

El filtrado por dirección MAC es una funcionalidad de seguridad que lo encontramos en ciertos puntos de acceso. Permite excluir o tolerar únicamente ciertas direcciones MAC para que accedan a la red inalámbrica.

Una dirección MAC es un identificador único para cada tarjeta de red. Este sistema, que permite controlar que tarjetas de red pueden acceder a la red,

habría permitido una gran seguridad, pero desgraciadamente, el protocolo 802.11b/g no cifra las tramas donde aparecen estas direcciones MAC.

En efecto, un simple software analizador de redes permite ver las direcciones MAC de los clientes. Por esto, ya que existen herramientas y comandos para modificar una dirección MAC y así usurpar la del cliente, la red se convierte en un verdadero "colador".

El filtrado por dirección MAC, asociado a WEP o WPA, alejará a los hacker "apurados" pero no será suficiente contra uno experimentado y motivado que disponga de tiempo.

**Portales cautivos**

Este sistema es más conocido como servidor RADIUS.

Una herramienta común que queremos utilizar en nuestra red inalámbrica es el ***portal cautivo***. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC). Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet.

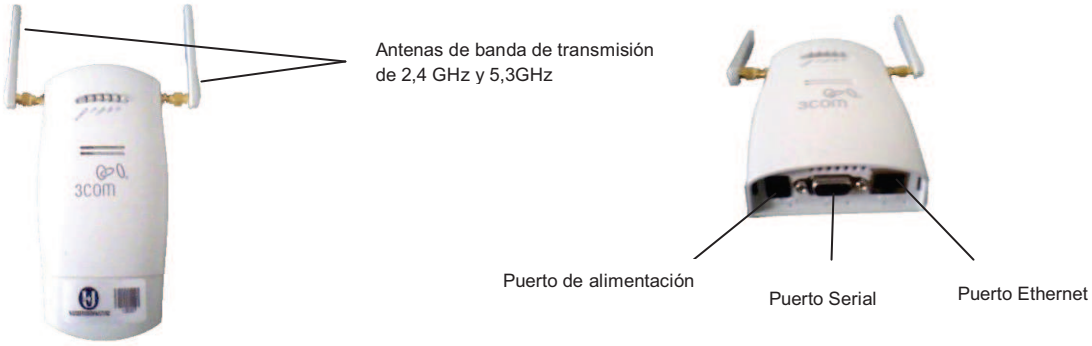
En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de "registro" (*login*), ingresa la contraseña que le haya asignado el administrador de red. El punto de acceso o el servidor en la red verifica los datos. No podrá ingresar al servicio hasta que el usuario no haya sido identificado.

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es re direccionado al sitio web que solicitó originalmente.

Con esta configuración les será muy difícil a cualquier intruso ingresar a nuestra red.

## CARACTERISITICAS DEL PUNTO DE ACCESO

Como se había dicho anteriormente, la Universidad Minuto de Dios de Girardot contara con una red inalámbrica, esta red dispondrá de un Punto de Acceso marca 3com 7760 con tecnología inalámbrica 11a/b/g.




A continuación se darán a conocer los componentes del AP con su respectiva descripción:

**Puerto Ethernet:**

Proporciona una conexión de 10/100BASE-TX a un conmutador 3com. Para hacer la conexión del Punto de Acceso al conmutador en la red, se utilizara un cable categoría 5 de acceso con señalización directa con conectores RJ45.

**Puerto de alimentación:**

El Punto de Acceso se alimenta mediante Power Over Ethernet (PoE). Eso quiere decir que su medio de alimentación será con un cable Ethernet conectado a un puerto para conmutador/concentrador en un inyector PoE 3com que viene incluido en la caja, este dispositivo tiene dos puertos para cable UTP RJ45, uno para conectar el Punto de Acceso y el otro para conectar el concentrador, además este inyector Poe ira conectado a una toma de corriente, para administrar la energía.

**Conectores de antena:**

Dos conectores de antena tipo RSMA que permiten conectar antenas que operan en las bandas de 2.4 GHz y 5.3 GHz.

**Puerto serial:**

Proporciona al Punto de Acceso una interfaz serial para su uso en diagnósticos.

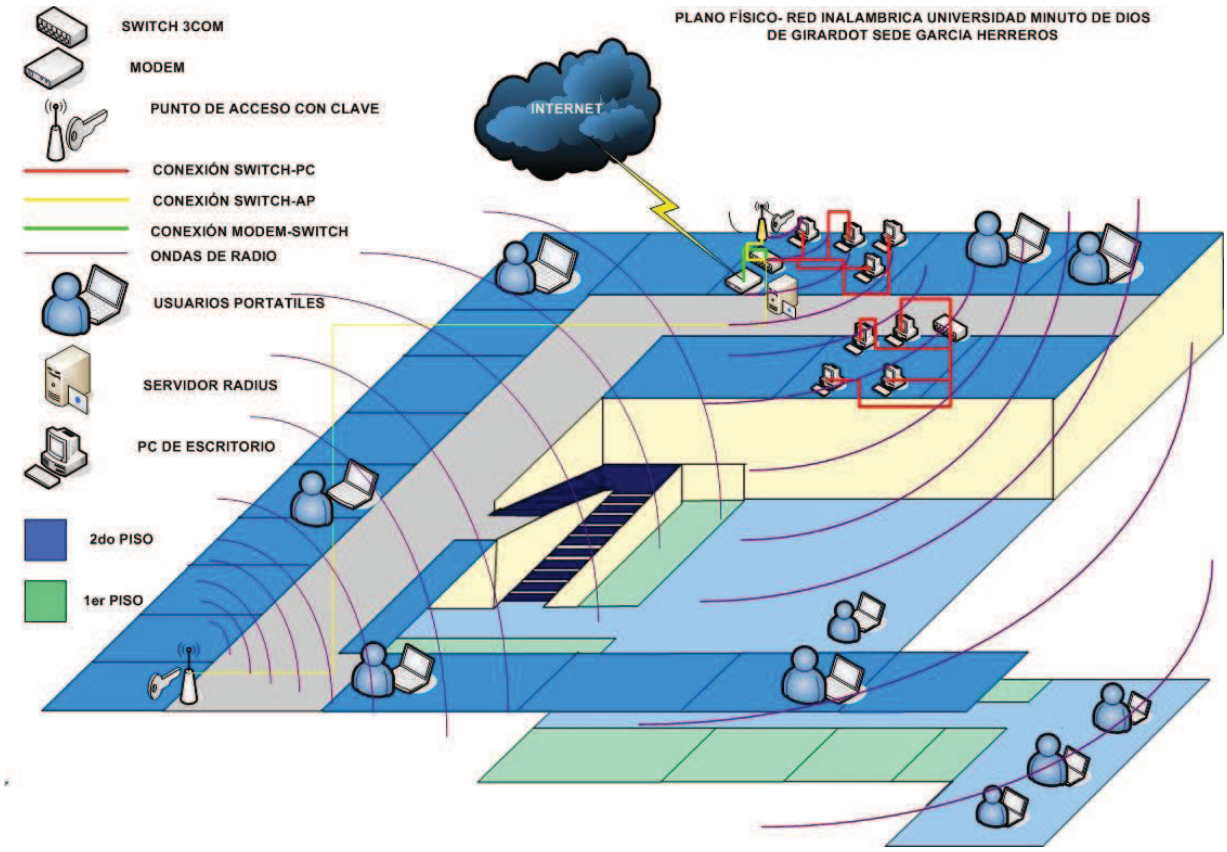
Estos son los compontes del AP además de tener algunas cosas que viene para su instalación física y lógica como un cable Ethernet, los anclajes para la pared y su respectivo CD-ROM con el software.

En la configuración del Punto de Acceso se tuvieron en cuenta as siguientes cosas:

- Nombre con el cual se identificará la red para que los usuarios se conecten a ella (SSID): **Uniminuto**
- Dirección MAC Ethernet: 00:22:57:4ª:97:40
- Dirección wireless: 00:22:57:4A:97:40
- Modo de operación: Access Point (AP)
- Modo inalámbrico: 2.4 GHz, velocidad de transmisión de 54Mbps (802.11g)
- Canal de Frecuencia: 10
- Seguridad: WPA2-PSK

## DISEÑO FÍSICO DE LA RED EN LA UNIVERSIDAD

Para la implementación de la red inalámbrica en la Universidad Minuto de Dios de Girardot fue necesario hacer un diseño físico en el que se muestra la forma en que trabajara dicha red, el lugar donde ira el Punto de Acceso y sus respectivos dispositivos que se asociaran a él.




Actualmente en la sede García Herreros hay cuatro salas de Informática, dos de ellas son para el servicio de internet de todos los estudiantes en general, otra para el laboratorio de redes y electrónica y la otra para los estudiantes de Ingeniería civil y comunicación Social. En el laboratorio de redes y electrónica actualmente se cuenta con un total de 4 computadores conectados a switch de 24 puertos marca 3com capa 3, en esta sala será conectado el Punto de Acceso con servicio de Internet, allí será desde donde se enviara la señal para que los usuarios móviles se conecten, cabe aclarar que este dispositivo también estará conectado a un

firewall para administrar la seguridad de la red, en el que se contara con un servidor RADIUS, y control de tráfico, listas negras, entre otras métodos de seguridad.

En el diseño Físico desarrollado se tenía la idea de establecer otro Punto de Acceso en un lugar de la universidad para una mayor señal y confiabilidad del transporte de datos, pero por el momento no va a ser posible.

**Implementación de tecnología QoS**

**QoS** o **Calidad de Servicio** (*Quality of Service)* son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio.

Este tipo de servicio será implementado dentro del Punto de acceso para controlar el tráfico de ancho de banda para que la información que viaje por el área de la red inalámbrica no se pierda.

**Se establecerán prioridades dentro de la red:** El tráfico de la red inalámbrica de la universidad puede ser priorizado para adecuarse necesidades de los usuarios. Por ejemplo, se tendrá que asegurar que los clientes que estén navegando en la red no estén reduciendo los recursos para aplicaciones críticas como la constante utilización de la plataforma de la universidad, aplicaciones estratégicas y servidores de información.

**La priorización de servicios es indispensable:** El acceso a las aplicaciones mas importantes puede ser interrumpido o inclusive totalmente inhabilitado por aplicaciones no tan importantes, como por ejemplo que los estudiantes estén bajando o subiendo grandes archivos vía www o ftp, utilizando paginas sociales como Facebook, Hi5, entre otras u observando aplicaciones multimedia vía Internet.

Cuando el tráfico a Internet es priorizado, los recursos limitados pueden ser utilizados en una forma que garantice los objetivos y requerimientos de la universidad. El ancho de banda de acceso a Internet, recurso costoso y limitado, puede ser gerenciado adecuadamente para garantizar una correcta jerarquización de la utilización del mismo por los servicios.

Entonces la idea es que se determine un porcentaje correcto para cada uno de los servicio de la red de internet, por ejemplo si la conexión a internet es de 2 Mbps, se tendría que organizar y gestionar este ancho de banda para que el 30% sean para navegación, 30% para FTP y un 40% para descargas. Esto es solo un ejemplo, ya que se necesita un estudio concreto para llevar a cabo esta organización correctamente.

La configuración que esta en el Punto de Acceso para la Universidad es la siguiente:

SSID de la red: Uniminutogirardot
Seguridad: WPA2 y Filtrado Mac.
Clave de Acceso para los Usuarios: uniminutoredes.

# 6. METODOLOGÍA DE DESARROLLO.

## 6.1 PARTICIPANTES

DIEGO HERNAN MENDIGAÑA CASTILLO
YASSED FAROUK REINA ASCENCIO

## 6.2 MATERIALES

El a porte institucional por parte de la Universidad Minuto de Dios de Girardot ,es el Punto de acceso 3COM 7760 y el Firewall Mikrotik donde tiene una aplicación para la configuración inalámbrica.

## 6.3 PROCEDIMIENTOS

Se está llevando a cavo la recolección de información de acuerdo a las actividades que se están desarrollando permitiéndonos tener un marco precedente y así evitar errores a futuro a nivel de infraestructura.

# 7. GLOSARIO

**AD-HOC:** Tipo de red en la que no hay un nodo central, sino que todos los ordenadores están en igualdad de condiciones.

**AES:** Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 ó 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

**CONCENTRADOR O HUB:** Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

**DHCP: D**ynamic **H**ost **C**onfiguration **P**rotocol - Protocolo Configuración Dinámica de Anfitrión) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

***DSSS**: "*Direct Sequence Spread Spectrum*",* espectro amplia de secuencia directa.

**ENCRIPTACION:** Proceso para volver ilegible información considera importante. La información una vez encriptado sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, nros. De tarjetas de crédito, conversaciones privadas, etc.

**ETHERNET:** Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

**FHS:** Filesystem Hierarchy Standard (FHS, en español *Estándar de jerarquía del sistema de archivos*).

**FIREWALL:** Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

**FIRMWARE:** Programación en firme. Programa que es grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.

**FRAME RELAY:** (*Frame-mode Bearer Service*) es una técnica de comunicación mediante retransmisión de tramas. Se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

**GHZ:** Gigahercio, En redes inalámbricas se utiliza para referirse a la frecuencia en que viaja las ondas electromagnética.

**HACKER: P**ersona especialista en redes, programación e informática capaz de violar la seguridad de casi cualquier red sea inalámbrica o cableada.

**IEEE:** ***Institute of Electrical and Electronics Engineers***, el **Instituto de Ingenieros Eléctricos y Electrónicos**, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

**IRDA: Infrared Data Association** (**IrDA**) define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojo.

**ISM: (Industrial, Scientific and Medical)** son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en areas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (*e.g.* Wi-Fi) o WPAN (*e.g.* Bluetooth).

**LOS:** Línea de Vista, conexión punto a punto entre antenas.

**MAC:** Dirección física de la tarjeta de red.

**MBPS: megabit por segundo** (**Mbps** o también **Mbit/s**) es una unidad que se usa para cuantificar un caudal de datos equivalente a 1000 kilobits por segundo o 1000000 bits por segundo.

**MHZ:** Megahertz (MHz) es equivalente (múltiplo) a 1 millón de hertzios... 1 hertz es una unidad de frecuencia que equivale a "ciclos por segundo".

**OFDM:** Multiplexación por División de Frecuencias Ortogonales.

**POE: PoE** (**P**ower **o**ver **E**thernet) es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red ethernet. PoE se rige según el estandar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad, teléfonos o puntos de acceso inalámbricos.

**PROTOCOLO:** Normas a seguir en una cierta comunicación: formato de los datos que debe enviar el emisor, cómo debe ser cada una de las respuestas del receptor, etc.

**PUNTO DE ACCESO:** (PA) Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

**RADIUS:** ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****erver*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

**SOFTWARE:** Son los ficheros, programas, aplicaciones y sistemas operativos que nos permiten trabajar con el ordenador o sistema informático. Se trata de los elementos que hacen funcionar al hardware.

**SSL:** También llamado Capa de Sockets Seguros. Este protocolo establece un canal de comunicaciones cifrado que ayuda a prevenir la interceptación de información crítica, como números de tarjeta de crédito en la Web y en otros servicios de Internet. Además de la privacidad para los datos y mensajes, brinda autenticación de los datos logrando una mayor seguridad. De acuerdo con la convención establecida, la dirección de las páginas Web que requieren una conexión SSL comienza con https: en lugar de http:.

**SWITCH:** es un dispositivo analógico de lógica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

**TOKEN RING:** arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; Actualmente no es empleada en diseños de redes.

**UIT:** La **Unión Internacional de Telecomunicaciones** (**ITU**) es el organismo especializado de las Naciones Unidas encargado de regular las

telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

**UWB:** Ultra Banda Ancha

**WCDMA: Wideband Code Division Multiple Access** (en español *Acceso múltiple por división de código de banda ancha*).

**WEP:** (Wired Equivalent Privacy) Protocolo para la transmisión de datos 'segura'. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitado. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de cifrado. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

**WI-FI:** Abreviatura de Wireless Fidelity. Es el nombre "comercial" con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

**WLAN:** Red Inalámbrica de Área Local

**WMAN:** Red Inalámbrica de Área Metropolitana

**WPA: WPA** (*Wi-Fi Protected Access* - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

**WPAN:** Red Inalámbrica de Área Personal}

**WWAN:** Red Inalámbrica de Área Extendida.

# RESULTADOS

En el tiempo que duró el desarrollo del proyecto se formularon muchas preguntas, como por ejemplo como iba a ser el diseño físico como lógico de la red Inalámbrica dentro de la Universidad, la respectiva seguridad que se iba a implementar, y si en verdad seria factible el uso de este tipo de tecnología.

Por fortuna los estudiantes aceptaron y apoyaron la idea de tener este servicio dentro de la red, gracias a una serie de encuestas realizadas dentro de la universidad a un numero de estudiantes en la que el 100% de ellas estuvieron de acuerdo en implementar esta red inalámbrica.

Gracias a el buen trabajo desarrollado por todos los estudiantes y docentes que tuvieron relación con este proyecto se pudo obtener una red inalámbrica dentro de la Corporación Universitaria Minuto de Dios de Girardot, que ya desde hace mucho se necesitaba, el buen uso de la red hasta el momento a sido satisfactorio teniendo en cuenta que ya hay una cantidad razonable de usuarios que constantemente la utilizan para tener acceso a los diferentes recursos educativos que ofrece la Internet, siendo así una base para obtener nuevos y mejores proyectos tecnológicos, ya que con la colaboración y la opinión de toda la gente que esta relacionada con la universidad (tanto estudiantes como empleados), podemos mejorar la calidad educativa a nivel tecnológico en la universidad, para que pueda competir con mucha mas fuerza con otras universidades que ya están empezando a hacer lo mismo.

## CONCLUSIONES

Obtuvimos una buena aceptación por parte de todas las personas de la Corporación Universitaria Minuto de Dios, como ya se había dicho con anterioridad.

Se logro implementar la red inalámbrica con su respectiva seguridad y se obtuvo una buena cantidad de usuarios en muy poco tiempo.

El desarrollo del proyecto no fue nada fácil ya que se tuvo que estudiar los posibles problemas que pudiera ocasionar esta red, si en verdad el diseño planteado serviría y si se podría mejorar con el paso del tiempo.

Pero gracias a esto los estudiantes desarrolladores de este proyecto obtuvimos una base fundamental para el ámbito laboral, además de aumentar nuestro nivel de aprendizaje en cuanto a redes, ya que de haber aprendido algunas cosas sobre este tema se pudo poner en practica todos los conocimientos que obtuvimos en estos 6 semestres en las que muchas veces nos sentimos frustrados por no entender algunas cosas sobre redes y otras veces emocionados y orgullosos por saber que en verdad esta carrera nos ha servido de mucho tanto en lo laboral como en lo familiar.

## BIBLIOGRAFIA


- **Redes Inalámbricas en vía de Desarrollo**
  *http://wndw.net/*

- **Normativa de uso para la conexión de redes Inalámbricas**
  http://www.ujaen.es/sci/redes/rimuja/pdf/conduso.pdf

- **Seguridad en redes inalámbricas "WIFI"**
  www.iec.csic.es/gonzalo/descargas/**Seguridad**WiFi.**pdf**

- **Manual de Configuración 3COM 7760**

- **Aportes Personales**
  Diego Hernán Mendigaña Castillo.
  Yassed Farouk Reina Ascencio.