# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

**FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**

## "PROYECTO DE UNA RED INALÁMBRICA DE COMUNICACIONES PARA UN EDIFICIO HISTÓRICO"

# T E S I S

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO MECÁNICO ELECTRICISTA**

**(ÁREA ELÉCTRICA ELECTRÓNICA)**

**P R E S E N T A N:**


**GILBERTO CARREÓN GÓMEZ**

**CELESTINO VÁZQUEZ CABRERA**


**ASESOR: ING. RAÚL BARRÓN VERA**

FES Aragón

**MÉXICO** **2008**

# *Agradecimientos*


***A mis padres:***

Que siempre me apoyaron y creyeron en mi, cualquier cosa es poco para agradecerles su confianza. Cada jalón de orejas, su infinita paciencia, todas sus enseñanzas, consejos y toda una vida llena de amor me han hecho un hombre de bien, un título profesional es solo una pequeña forma de agradecer lo mucho que me han dado, los amo.

***A Laura:***

Hermana, no tengo suficientes palabras para agradecer por todos y cada uno de los momentos que compartimos, gracias por haberme cuidado y guiado todos estos años, por todas y cada una de las noches que pasaste en vela ayudándome con mis tareas, gracias por ser mi mejor amiga, mi confidente, por tus consejos, porque siempre fuiste y sigues siendo un ejemplo de perseverancia, te admiro. Mil gracias porque a pesar de no siempre estar de acuerdo me das tu apoyo y comprensión, y lo prometido es deuda, el titulo también es tuyo.

***A mi sobrino Edgarín:***

Gracias por tu amor, por tu alegría, por tu comprensión, por compartir y apoyar mis sueños, y ahora que se cumple uno de ellos te agradezco por que eres una parte muy importante que me alienta para seguir adelante,
Te adoro.

***A Ismael:***

Cuñado, por todas las veces que me ayudaste con un libro, un apunte, algún material didáctico o simplemente tus conocimientos que compartiste conmigo fueron siempre de suma importancia para cumplir con mis tareas, muchísimas gracias.

*Gilberto*

***A Karina:***

Que eres como mi hermanita, quiero agradecerte la confianza que me has brindado, tu cariño, tu apoyo y cada palabra de aliento. Estoy muy orgulloso de que hoy seas parte del espíritu de la UNAM.

***A toda mi familia:***

Les agradezco enormemente que con una palabra de aliento, un consejo, un abrazo o cualquier estimulo, siempre estuvieran presentes apoyándome.

***A Dios:***

Gracias por guiar mis pasos, por que cuando me desviaba del camino, siempre me ayudaste a regresar, gracias infinitas por que tu amor y tu fe en mi lo veo reflejado en los que me rodean, gracias por permitirme vivir en esta era con la familia que tengo, con los amigos y maestros que pusiste en mi camino de quienes he aprendido mucho, gracias por darme tu bendición para llegar a esta meta.

***A Celestino:***

Durante toda la carrera siempre pude contar con tu ayuda cuando no entendía algo o cuando no encontraba una solución a algún problema, en los trabajos de equipo tus aportaciones siempre fueron muy valiosas, incluso fuera del campus; siempre mostraste responsabilidad y madurez sin dejar de divertirte, sabes lo mucho que te admiro y respeto. No caben palabras para agradecerte por tenerme tanta paciencia en este proyecto y por tu perseverancia para que saliera adelante. Quiero agradecerte el haberme dado tu amistad incondicionalmente, es un gran orgullo el conocer a alguien como tu y un gran honor el ser tu amigo, gracias.

*Gilberto*

***A mis maestros:***

Gracias por compartirme sus conocimientos y experiencias, por todas sus enseñanzas, por su paciencia y por todo su esfuerzo para ayudarme
a salir adelante, gracias por que me dieron las herramientas esenciales para enfrentar la vida profesional.

***A todos mis amigos:***

Gracias por su amistad, por tantos momentos que vivimos, por su apoyo y compañía en toda la carrera, nunca voy a olvidarlos.

***Gracias especiales a Karla Díazleal:***

Por ser inspiración para no dejar de luchar por mis sueños, fue por ti mi compromiso de terminar una carrera profesional, lo hemos logrado, y ahora vamos por más. No importan las piedras en el camino, eres la fuerza que necesito para levantarme y seguir adelante, mil gracias por existir, mil gracias por hacerme tan feliz, aunque no estés a mi lado, siempre estas en mi corazón.

*Gilberto*

***A mis padres:***
Porque no tengo forma de pagarles por todo su amor y el apoyo que siempre me han dado y han hecho de mí un hombre honesto, trabajador y responsable.
Gracias por creer siempre en mí.

***A mi abuelito Celestino:***
Porque desde niño siempre me cuidaste y me enseñaste a superarme. Gracias por todo el cariño que me diste y por motivarme para salir adelante. Tu recuerdo será mi guía.

***A mi hermana Haydeé:***
Porque siempre que necesite de tu ayuda estuviste conmigo. Gracias por todo tu apoyo y cariño por estar siempre conmigo y por el gran ejemplo que me has dado día con día.

***A Mamá Tere:***
Por enseñarme a nunca rendirme y a siempre luchar por mis ideales. Gracias por tus consejos, por todo tu cariño y por estar conmigo en cada momento.

***A mi abuelita Esperanza:***
Porque tu cariño y amabilidad son pilares de mi vida y me animan a luchar día tras día. Gracias por todo el amor que me diste el cual siempre llevaré conmigo.

***A mi abuelito Rafael:***
Porque siempre estás dispuesto a ayudarme y a compartir tu experiencia conmigo. Gracias por el cariño que siempre me has brindado.

*Celestino*

***A mis tíos y primos:***

Porque siempre me he sentido orgulloso De ser parte de una familia tan unida y llena de amor. Gracias por hacerme sentir tan querido

***A todos mis Profesores:***

Por todas sus enseñanzas, su dedicación y disposición para ayudarme sin importar lo difícil o complicado dela situación.

***A mis compañeros y amigos:***

Por haberme brindado su amistad, su alegría y compartir conmigo esta etapa de mi vida. Especialmente a Gilberto por su amistad, confianza y por ayudarme a terminar este logro.

***A Dios:***

Por haberme dado la oportunidad de haber conocido a personas tan maravillosas que me enseñaron lo que es el verdadero amor y me han hecho lo que soy ahora.

*Celestino*

# Contenido

# INTRODUCCION

El palacio postal es el edificio más representativo del servicio postal mexicano. Su construcción comenzó en el año de 1902 por orden del General Porfirio Díaz y fue inaugurado el 17 de febrero de 1907. De estilo ecléctico, por su combinación incomparable de formas y estructuras, el Palacio Postal es considerado como una obra Sui generis, única en su tipo, pues integra elementos de los estilos gótico veneciano, plateresco isabelino y art nouveau; su creación, se debe íntegramente al arquitecto italiano Adamo Boari. Ostenta una espléndida fachada en cantera, con decoraciones de tipo renacentista. Su puerta principal es ochavada sobre la esquina y está cubierta por una marquesina de hierro forjado, la cual es sostenida, desde el muro superior, por dos grandes cadenas, lo que la hace parecer un gran puente levadizo, que a su vez, es coronado por dos balcones que le otorgan un toque verdaderamente señorial.

En las fachadas, las gárgolas y los detalles de los pórticos son de herrería de bronce, que fueron elaboradas en la Fondería Pignone de Florencia, Italia.

Las columnas que recubren la estructura de hierro que sostiene al edificio, aparentan ser de mármol, están realizadas a base de una técnica de yeso llamado escayola.

A pesar de que el envío de correos es cada día menos requerido, el palacio postal ofrece aún en la actualidad servicios de mensajería y paquetería para todo el público, así como actividades administrativas del servicio postal mexicano.

En el año 2007 se celebró el centenario del palacio postal y con este se le entregó el reconocimiento de patrimonio cultural de la humanidad, por lo que ahora está prohibida la perforación de los muros para la instalación de cables de comunicación de datos para instalar nuevos nodos de red para computadoras de escritorio y portátiles.

Aún cuando en el interior del palacio postal ya existe una red de comunicaciones para gran parte de las oficinas que ahí se encuentran, existen otras donde no existen equipos de cómputo y ahora se requieren, así como otras oficinas donde existen nodos pero se requiere la conexión de nuevas computadoras además de las ya existentes. El propósito de esta tesis es planear la forma de dar servicio a estos nuevos usuarios sin tener que dañar la estructura interna del palacio postal. Las nuevas computadoras se encuentran distribuidas entre oficinas del segundo y tercer piso siendo que las del segundo piso no tienen nodos de red instalados mientras que en las del tercer piso hay un nodo de red en cada una de las oficinas. Es por eso que se diseñará una red inalámbrica.

El primer capítulo de esta tesis está dirigido a la descripción de los conceptos básicos y necesarios para entender la forma en la que funcionan las redes alámbricas e inalámbricas así como la forma en que se realiza la comunicación entre los equipos de computo que la integran.

El segundo capítulo nos ayuda a conocer todos los dispositivos físicos que son necesarios para realizar la tarea de comunicación de una red alámbrica o inalámbrica de acuerdo con sus características, aplicaciones y consideraciones de uso.

En el tercer capítulo mostramos la aplicación de los estándares más comunes utilizados en las redes alámbricas e inalámbricas; también se muestran los protocolos de seguridad y sus principales características de manera en que se evite el robo de información y acceso a personas no autorizadas dentro de las redes. Finalmente se muestra la descripción del protocolo de internet actual y las características del protocolo de internet v6 utilizado en los diferentes tipos de redes existentes de acuerdo a su tamaño.

El cuarto capítulo muestra los pasos que se deben realizar para la instalación práctica de una red alámbrica, inalámbrica o híbrida, las consideraciones que deben tenerse, las herramientas necesarias, los materiales a utilizar y los pasos para realizar la configuración de los equipos que conformarán la red.

Para una red inalámbrica se muestran las ecuaciones para determinar la eficacia de la transmisión y recepción de los dispositivos así como la forma de configurarlos. Finalmente se realiza la propuesta del proyecto de tesis poniendo en práctica todos los conocimientos anteriores.

# OBJETIVO

- Hacer uso de los conocimientos adquiridos en la carrera en el área de telecomunicaciones y obtener información de las tecnologías actuales para realizar una propuesta de red inalámbrica que proporcione servicio eficiente a oficinas que se encuentran distribuidas entre el segundo y el tercer piso del palacio postal del servicio postal mexicano así como una expansión de la red actual.
- Proporcionar a los estudiantes de ingeniería las herramientas necesarias para conocer y aplicar los protocolos, normas, estándares y necesidades que pueden presentarse en la proyección e instalación de una red inalámbrica.

# Capitulo I
# GENERALIDADES

# I.1 TOPOLOGÍAS DE RED

Una topología de red es una forma geométrica en que se encuentran distribuidos los equipos y los cables que los conectan. Los equipos de una red se comunican entre sí mediante una conexión física, y el objeto de las topologías es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de datos, conseguir un mejor control de la red y permitir de forma eficiente el aumento del número de ordenadores en la red.

## I.1.1 Topología Jerárquica.

La topología Jerárquica (también conocida como topología en árbol) es una de las más comúnmente utilizadas hoy en día. El software para controlar la red es relativamente simple y la propia topología proporciona un punto de concentración para control y resolución de errores. Su principal característica es que en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que se encarga de controlar el tráfico en la red. En la mayor parte de los casos, el equipo que se encuentre en la jerarquía mayor (raíz) es el que controla la red. En algunos diseños, el concepto de control jerárquico se distribuye, ya que se proponen métodos para que algunos equipos subordinados controlen a los que se encuentran por debajo de ellos en cuestión de jerarquía.

Aunque la topología jerárquica es atractiva desde el punto de vista de la simplicidad de control, presenta problemas serios de “cuellos de botella”; el equipo situado en la raíz de la jerarquía (típicamente una computadora de altas prestaciones) es el que controla todo el tráfico entre los equipos que conforman la red. Además de esto la red depende en gran parte del equipo que la controle, ya que en caso de un fallo de esta, la red quedará completamente fuera de servicio a no ser que otro equipo asuma las funciones del que se encuentre averiado. No obstante, la topología jerárquica se ha utilizado en el pasado y continúa utilizándose actualmente ya que permite una evolución simple hacia redes más complejas debido a que es muy sencillo añadir nuevos elementos.

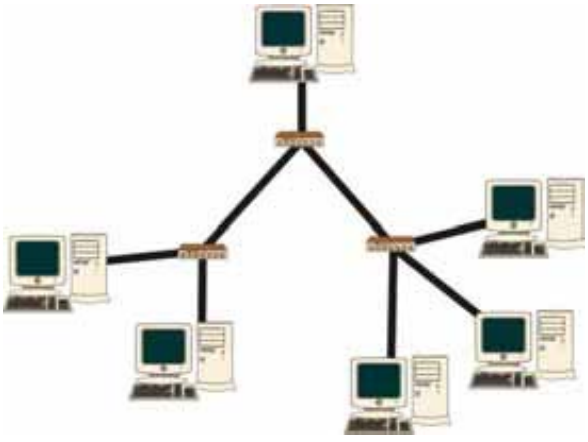


*Fig. 1.1 Topología Jerárquica*

## I.1.2 Topología en Bus

También llamada topología horizontal, es muy utilizada en redes de área local. Consiste en que todos los equipos que conforman la red se conectan a un mismo bus por medio de unidades interfaz y derivadores de manera que cada equipo pueda enviar información a todas las demás y para poder identificar hacia cual de las computadoras de toda la red se está dirigiendo, se añade un sufijo al paquete de información, este contiene la dirección del equipo que debe recibir la información en particular.

Su principal inconveniente es que al solo existir un solo canal de comunicaciones, con un fallo en alguna parte del cableado se detendría el sistema total o parcialmente dependiendo de la ubicación del mismo, además debido a que la información recorre todo el bus bidireccionalmente hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en otros tipos de red.

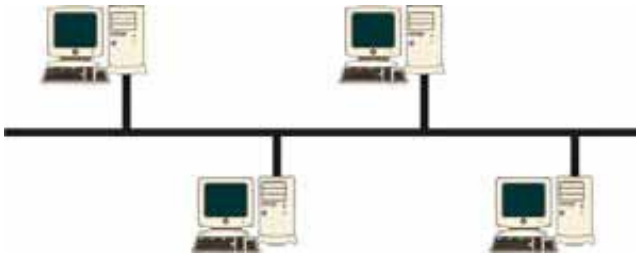


*Fig. 1.2 Topología en bus*

## I.1.3 Topología en Estrella

La topología en estrella es otra estructura ampliamente utilizada en sistemas de comunicación de datos. En este tipo de red todos los equipos se conectarán a un nodo central el cual se encargará de controlar la información de toda la red.

Generalmente se utiliza un hub o concentrador como nodo central en una topología de estrella. En este caso se dice que la red funciona con una topología de bus lógico, ya que el hub enviará la información a través de todos sus puertos haciendo que todos los equipos conectados reciban la información (incluso cuando no este destinada a ellos). Actualmente se han sustituido los hubs por switches o conmutadores, creando así una topología en estrella tanto física como lógica debido a las propiedades de segmentación y acceso al medio que nos ofrecen estos dispositivos capa 2.

La ventaja de este tipo de red consiste en una mayor facilidad de supervisión y control de la información, además de que un fallo a alguno de los equipos no afecta a la red entera, sin embargo si falla el nodo central, todo el sistema se detendrá.

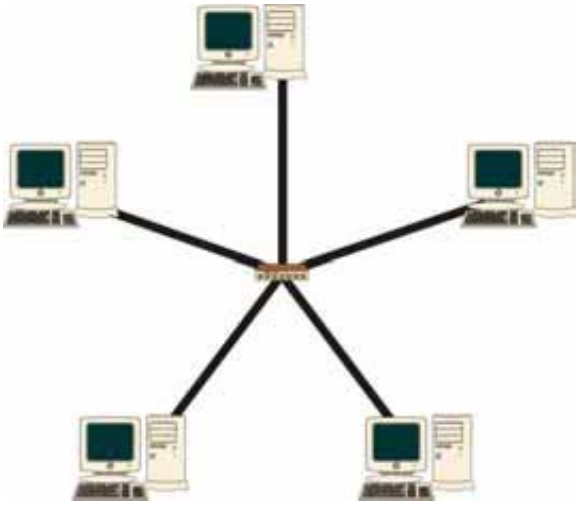


*Fig. 1.3 Topología en Estrella*

## I.1.4 Topología Estrella Extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella, generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central, además de que la topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico y de la mayoría de las LAN actuales.

## I.1.5 Topología en Anillo

Esta topología recibe su nombre debido a que los equipos que la conforman están conectados unos con otros formando un círculo por medio de un cable común. La información describe una trayectoria circular en una única dirección y cada equipo hace la función de repetidor regenerando la señal y pasándola al siguiente equipo del anillo.

En este tipo de redes la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

Esta topología es muy atractiva debido a que los cuellos de botella son mucho más raros, además la lógica necesaria para redes de este tipo es relativamente simple, sin embargo el principal de sus problemas es que al haber un único canal que une a todos los componentes, un fallo en cualquiera de los nodos provocará una falla en toda la red.

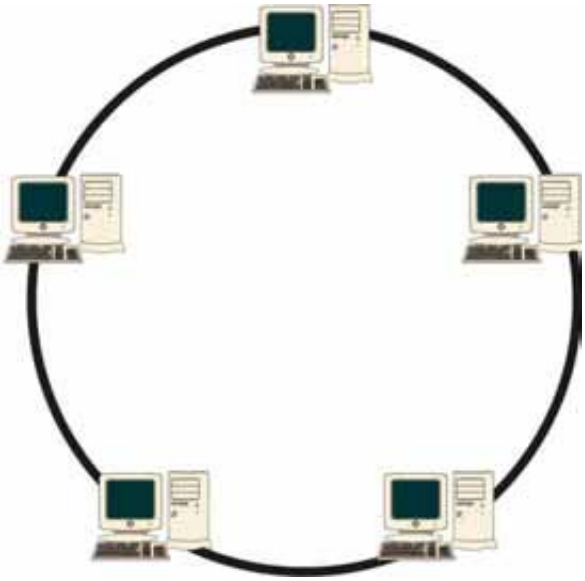


*Fig. 1.4 Topología en Anillo*

## I.1.6 Topología de Anillo Doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí, de esta manera se incrementa la confiabilidad y flexibilidad de la red, ya que en caso de falla en un canal existe otro para mantener el enlace de los mismos dispositivos. Cabe mencionar que la topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno.

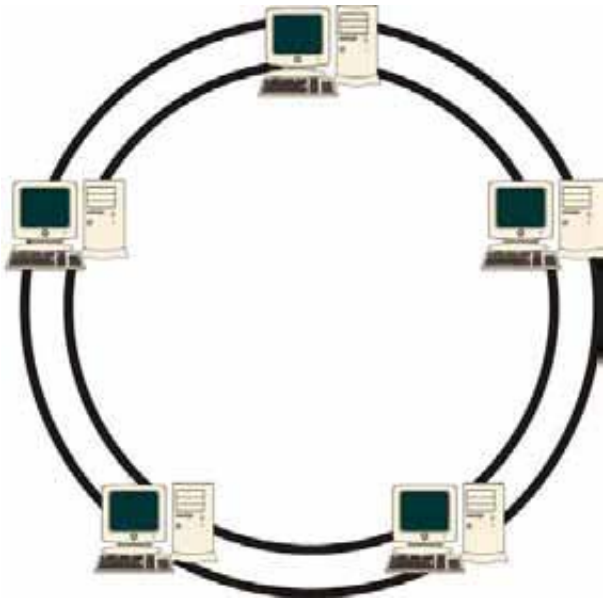


*Fig. 1.5 Topología en Anillo Doble*

### I.1.7 Topología en Malla

En este tipo de topología de red cada equipo está conectado a uno o más nodos, de modo que es posible llevar los mensajes de un punto a otro por múltiples caminos. Este tipo de conexión es utilizado frecuentemente en redes de tipo WAN en las que se necesita alcanzar diversos nodos situados en lugares muy dispersos.

Su principal ventaja es su relativa inmunidad a problemas de fallos y cuellos de botella. Dada la multiplicidad de caminos entre los equipos, es posible encaminar el tráfico evitando componentes que fallan o nodos ocupados. Entre sus desventajas se encuentran que es muy costosa de instalar en caso de utilizar cable y es difícil de hacer por lo que se combina con otras topologías para formar una topología híbrida.

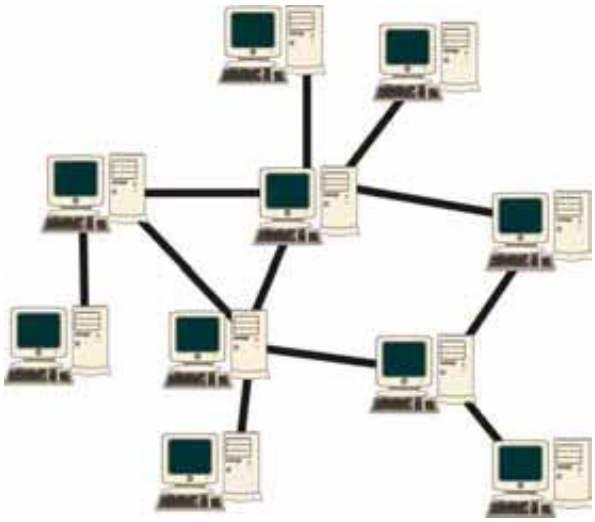


*Fig. 1.6 Topología en Malla*

## I.2 TOPOLOGÍAS DE RED INALÁMBRICAS

Las topologías de red también son importantes en el desarrollo de redes inalámbricas igualmente que las redes cableadas. Existen 4 estructuras jerárquicas que hacen posible la interconexión de los equipos inalámbricos, estas son:

IBSS (Independent Basic Service Set, Conjunto de Servicios Básicos Independientes)

BSS (Basic Service Set, Conjunto de Servicios Básicos)

ESS (Extended Service Set, Conjunto de Servicios Extendidos)

WDS (Wireless Distribution System, Sistema de Distribución Inalámbrico)

## I.2.1 IBSS

Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre las distintas terminales que forman la red. En este caso no existe ninguna terminal principal que coordine al grupo y no existe un punto de acceso. Todas las comunicaciones son directas entre dos o más terminales del grupo. A este tipo de conexión también se le conoce como *ad hoc*, independiente o de igual a igual (peer-to-peer)

*Fig. 1.7 Topología IBSS*

## I.2.2 BSS

En esta modalidad se añade un equipo llamado punto de acceso (AP o Access Point) que realiza las sunciones de coordinación centralizada de la comunicación entre los distintos equipos de la red. Los puntos de acceso tienen funciones de *buffer* (memoria de almacenamiento intermedio) y de pasarela (*Gateway*) con otras redes. A los equipos que hacen de pasarelas con otras redes externas se les conoce como *portales*. A la modalidad BSS también se le conoce como modo infraestructura.

*Fig. 1.8 Topología BSS*

## I.2.3 ESS

Esta modalidad permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS. Los puntos de acceso que conforman la red deben tener el mismo nombre (SSID) y pueden trabajar en el mismo canal o en diferentes canales.

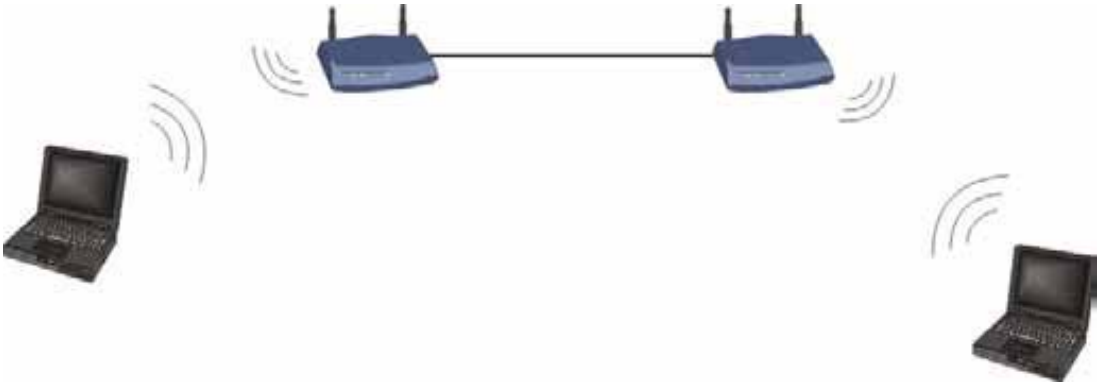


*Fig. 1.9 Topología ESS*

## I.2.4 WDS

Este sistema permite la interconexión entre los puntos de acceso de manera inalámbrica.

Con WDS un punto de acceso puede funcionar sólo como punto de acceso, como puente con otro punto de acceso o en ambas funciones.

De esta manera es posible crear una gran red inalámbrica extendiendo su cobertura hacia lugares en los que no es posible poner nuevos cables de red. A pesar de esto no es posible utilizar esta topología a menos que todos los puntos de acceso o repetidores inalámbricos sean compatibles con esta tecnología, esto hace que el costo sea mayor.

También se requiere que todos los equipos usen el mismo canal de radio frecuencia y compartan la clave de seguridad si se utiliza.

Sus nombres de red inalámbrica (SSID) pueden ser diferentes para diferenciar uno de otro.

*Fig. 1.10 Topología WDS*

Además de las topologías descritas, existe un caso especial de topología de redes inalámbricas, este es el caso de las redes Mesh.

## I.2.5 Redes Mesh

Las redes Mesh, o redes acopladas, son aquellas redes en las que se mezclan dos topologías de las redes inalámbricas. Básicamente son redes con topología BSS, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de algún adaptador de red que directamente o indirectamente está dentro del rango de cobertura del punto de acceso.

También permiten que los adaptadores de red se comuniquen independientemente del punto de acceso entre sí. Esto quiere decir que los dispositivos que actúan como adaptador pueden no mandar directamente sus paquetes al AP sino que pueden pasárselos directamente a otras tarjetas de red para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (Hops) o con un número que aún no siendo el mínimo sea suficientemente bueno.

Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Antiguamente no se usaba porque el cableado necesario para establecer la conexión entre todos los nodos era imposible de instalar y de mantener. Hoy en día con la aparición de las redes wireless este problema desaparece y nos permite disfrutar de sus grandes posibilidades y beneficios.

*Fig. 1.11 Topología Mesh*

## I.3 MODELO OSI

El modelo OSI (Open Systems Interconnection) de telecomunicaciones esta basado en una propuesta desarrollada por la organización internacional de normalización ISO (International Organization for Standardization). Su función es la de definir la forma en que se comunican los sistemas *abiertos* de telecomunicaciones, es decir, los sistemas que se comunican con otros sistemas.

El objetivo perseguido por el modelo OSI es establecer una estructura que presente las siguientes particularidades:

**Estructura multicapa:** Se diseñó una estructura multicapa con la idea de que cada una se dedique a resolver una parte del problema de comunicación; de esta manera cada capa ejecuta funciones específicas.

La capa superior utiliza los servicios de las capas inferiores: Cada capa se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de las capas inferiores en la misma computadora. La comunicación intercapa está bien definida. La capa N utiliza los servicios de la capa N-1 y proporciona servicios a la capa N+1.

**Dependencias de Capas**: Cada capa es dependiente de la capa inferior y también de la superior.

**Encabezados**: En cada capa, se incorpora al mensaje un formato de control. Este elemento de control permite que una capa en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier capa dada, puede incorporar un

encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

**Unidades de información:** En cada capa, la unidad de información tiene diferente nombre y estructura.

El modelo OSI consiste en 7 capas, las cuales se muestran a continuación:


*Fig. 1.12 Capas del Modelo OSI*

### I.3.1 Capa Física

Es la primera capa del modelo OSI y en ella se controlan todas las características físicas, mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es la capa más baja, es la que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación.

Para realizar la tarea de comunicarse, se necesita una cierta cooperación entre dos entidades pares; una a cada lado de la comunicación. Esta cooperación supone:

Un *mantenimiento de tablas*, es decir, contar el número de paquetes enviados desde el último reconocimiento recibido por una estación, para llevar un control de los datos que llegan y asegurar una comunicación fiable.

Un *mantenimiento de relojes sincronizados* para realizar la gestión del timeout o tiempo de espera máximo en las transmisiones. Este tiempo es importante y definible.

En esta capa se ubican también todos los medios de transmisión como los sistemas de telecomunicaciones para redes WAN , tales como sistemas satelitales, microondas, radio-enlaces, canales digitales y líneas privadas, así como los medios de transmisión para redes de área locales (LAN), cables de cobre (UTP,STP) y fibra óptica. Además, en esta capa se ubican todos aquellos dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como repetidores de redes LAN, repetidores de microondas y fibra óptica, concentradores (Hubs), conmutadores de circuitos físicos de telefonía o datos y equipos de modulación y demodulación (módems).

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

## I.3.2 Capa de Enlace de Datos

El objetivo de esta capa es proporcionar un "enlace lógico" entre dos equipos enviando en la trama la dirección MAC del equipo destino, de esa manera el equipo destino reconocerá la información y la interpretará como suya aún cuando el medio de transmisión en la red sea compartido para los demás equipos.

Es debido a esto que esta capa debe ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores y validar la integridad física de la trama, pero esta no será corregida sino que se le notificará al transmisor para su retransmisión.

Finalmente la capa de enlace de datos se subdivide en control lógico de enlace (LLC) y control de acceso al medio (MAC)


*Fig. 1.13 Subcapas de la Capa de Enlace de Datos*

### *I.3.2.1 Subcapa de Control Lógico de Enlace (Logical Link Control, LLC)*

Esta subcapa maneja la comunicación de enlace de datos y define el uso de puntos de interfaz lógica, llamados SAPs (Service Access Points) o puntos de acceso al servicio.

Las funciones que debe realizar esta subcapa son:

Proporcionar servicios a la capa de red: Debe realizar la transferencia de datos entre la capa de red de la máquina origen y la capa de red de la máquina destino; los datos se traspasan de la capa de red a la capa de enlace de datos de la 1ª máquina y en la 2ª máquina se realiza el proceso inverso.

Entramar la información: Toda la información que recibe de la capa de red la debe encapsular en tramas de datos, las cuales deben tener un principio y un final. Para marcar el inicio y el final se pueden utilizar varios métodos: conteo de caracteres, utilización de bytes específicos al principio y al final de la trama, etc.

Control de errores: Para detectar posibles errores, se divide todo el flujo de información en tramas y se realiza una suma de comprobación de tramas introduciendo códigos de paridad o códigos de redundancia cíclica (CRC) y el total se incluye en el campo reservado para ello en la trama enviada; de esta manera la máquina destino realiza de nuevo la suma de comprobación y la compara con la recibida en la trama, si coinciden los datos son correctos.

Recuperación de fallos: Además de asegurarse de que no existan errores de información en las tramas transmitidas, debe detectar que todas las tramas sean entregadas en el orden correcto a la

capa de red de la máquina destino. Para esto cada trama es numerada y cuando llega a la máquina destino esta envía una trama de confirmación informando a la máquina emisora el estado en que ha llegado la trama de información. Si ha llegado en mal estado se retransmite la trama.

También se puede utilizar un temporizador en el equipo emisor, así una vez vencido el tiempo de espera (timeout) se retransmite la trama debido a que se entiende que la trama se perdió al no haber respuesta de confirmación del receptor.

Control de flujo: Es otra característica que debe resolver la capa de enlace de datos para evitar que un emisor rápido sature a un receptor lento. Utilizando técnicas de realimentación el emisor no envía nuevas tramas de información hasta que el emisor le informe que lo haga.

### I.3.2.2 Subcapa de Control de Acceso al Medio (Medium Access Control, MAC)

La subcapa de control de acceso al medio es la más baja de las dos y proporciona acceso compartido y regula la compartición para todos los equipos y tarjetas conectadas a la red. Este subnivel solo aparece en redes de medio compartido como las LANs y no en enlaces punto a punto como las WANs y sus estándares están definidos en las categorías 802.3, 802.4, 802.5 y 802.12.

Los métodos de acceso utilizados por esta subcapa pueden ser estáticos o dinámicos. A continuación se mencionan los tipos de acceso que se pueden emplear:

Métodos de acceso estáticos

**FDM** (Multiplexación por División de Frecuencia)

Se caracteriza en que para un número de usuarios “N” el ancho de banda se dividirá en “N” partes iguales asignándole cada parte a un usuario. De esta manera no existe la posibilidad de interferencia entre ellos ya que cada uno de los usuarios tiene una frecuencia distinta. Su desventaja consiste en que si hay menos de los “N” usuarios a la vez usando el canal, una parte del espectro se desperdicia, y si hay más de “N” usuarios intentando acceder al medio, a una parte de ellos se le denegará el acceso aunque no esté siendo aprovechada la totalidad del ancho de banda.

**TDM** (Multiplexación por División de Tiempo)

En este método cada usuario tiene asignado un *slot* o intervalo temporal para utilizar el canal, sin embargo si el tiempo del Slot no es utilizado se desperdiciará al igual que en el caso anterior el ancho de banda.

Métodos de acceso dinámicos

En este tipo de métodos el aprovechamiento del canal es mucho mayor que los anteriores, por lo que son más adecuados para las redes con ordenadores ya que estos no transmiten ni están activos todo el tiempo.

Método de enviar tramas

Se encarga de controlar a los equipos para que ninguno pueda enviar una trama si el anterior no ha podido transmitir con éxito.

Medio Compartido

Controla que el envío y recepción de los equipos sean iguales en función y rango debido a que se transmiten por un único canal. En caso de existir prioridades serán determinadas por los protocolos.

Colisión

Sirve en caso de que dos equipos transmitan simultáneamente sus tramas dando como resultado una señal inservible. Esto ocasionará que sea necesaria una retransmisión ordenada de las tramas.

Tiempo

Puede ser de dos tipos: continuo o ranurado. Con el tiempo continuo la transmisión de la trama puede iniciar en cualquier momento y si el tiempo es ranurado, el tiempo se divide en intervalos discretos, ranuras o slot y la transmisión de las tramas empezará en el comienzo de una de estas ranuras.

Portadora

En este caso se pueden seguir dos opciones: detección o no detección de portadora. Si se utiliza detección de portadora, los equipos podrán ver si el canal está siendo usado antes de utilizarlo. En caso de no utilizar la detección de portadora los equipos transmitirán según el protocolo sin probar el estado del canal y una vez que hayan terminado de transmitir podrán determinar si la trama fue enviada exitosamente o no.

### I.3.3 Capa de Red

La capa de red, es la capa que debe asegurarse que los datos lleguen desde el equipo origen al equipo destino determinando la ruta de conexión aunque se encuentren ubicados en redes geográficamente distintas y no exista una conexión directa.

Para cumplir con su objetivo tiene que realizar ciertas tareas:

- Asignación de direcciones de red únicas
- Interconexión de subredes distintas
- Encaminamiento de paquetes
- Control de congestión

Existen varias posibilidades que pueden surgir en el momento en que se realiza la comunicación de los equipos. El más fácil es realizando un enlace punto a punto directo entre los equipos, en el cual no es necesaria esta capa ya que la capa de enlace de datos puede proporcionar las funciones necesarias para ello. En el extremo opuesto se encuentran las conexiones de dos equipos que no se encuentran conectados directamente en la red, aún cuando lo estén indirectamente; en este caso se debe establecer la ruta más sencilla para interconectarlos.

El problema del enrutamiento consiste en encontrar un camino óptimo entre un origen y un destino. La bondad de este camino puede tener diferentes criterios: velocidad, retardo, seguridad, regularidad, distancia, costos de comunicación, etc.

Los equipos encargados de esta labor se denominan enrutadores (*routers*), también realizan labores de encaminamiento los conmutadores (*switches*) "multicapa" o "de capa 3", aunque estos últimos realizan igualmente labores de capa de enlace.

### I.3.4 Capa de Transporte

La función básica de esta capa es proporcionar un mecanismo para intercambiar datos entre sistemas finales, aceptando los datos que recibe de la capa superior (sesión) y pasarlas a la capa de red, asegurándose que todos los paquetes lleguen libres de errores, en orden y sin pérdidas ni duplicaciones al otro extremo de la comunicación.

Para conseguir estas características, existen protocolos que definen la cooperación entre entidades pares de transporte de los sistemas finales En esta capa la unidad de intercambio entre ambos equipos se conoce como TPDU (Transport Protocol Data Unit) o Unidad de Datos de Protocolo del nivel de Transporte. También se le conoce como *paquetes de transporte* o *segmentos de transporte.*

Para generarla, se procede a tomar la PDU de la capa superior (sesión), conocida como SPDU (Session Protocol Data Unit) y se añade la información de control de protocolo del nivel de transporte.

Algunos ejemplos de protocolos más utilizados para esta capa son:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- XTP (Xpress Transport Protocol)
- Protocolos TP0 al Tp4 de OSI

## I.3.5 Capa de Sesión

Es la encargada de proporcionar los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles. No obstante en algunas aplicaciones su utilización es ineludible.

La capa de sesión proporciona los siguientes servicios:

**Control del Diálogo**: Controla la manera en que los equipos envían la información, la cual puede ser realizada en tres formas:

- **Simplex.** Un equipo transmite de manera exclusiva mientras otro recibe de manera exclusiva.
- **Half-duplex.** Los equipos se turnan para transmitir, un equipo no puede transmitir hasta que el otro termine.
- **Full-duplex.** Los equipos pueden transmitir y recibir simultáneamente. La comunicación full-duplex suele requerir un control de flujo que asegure que ninguno de los dispositivos envía datos a mayor velocidad de la que el otro dispositivo puede recibir.

**Agrupamiento**: El flujo de datos se puede marcar para definir grupos de datos.

**Recuperación**: La capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación y no desde el principio.

Todas estas capacidades se podrían incorporar en las aplicaciones de la capa 7. Sin embargo ya que todas estas herramientas para el control del diálogo son ampliamente aplicables, parece lógico organizarlas en una capa separada, denominada capa de sesión.

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

La unidad de intercambio entre entidades del nivel de sesión se denomina SPDU. La entidad de sesión, la cual es un usuario de los servicios de transporte, formará la TDPU a partir de la PDU en la capa de sesión. Esta PDU recibe nombres relacionados con el tipo de aplicación a las que dan servicio y se suelen llamar *mensajes* o *transacciones*. Las llamadas a procedimiento remoto RPC (Remote Procedure Calls) y NetBIOS son ejemplos de la funcionalidad de la capa de sesión

## I.3.6 Capa de Presentación

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas (como por ejemplo una comunicación entre una PC y una Macintosh).

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

## I.3.7 Capa de Aplicación

La función principal de la capa de aplicación es permitir la interacción con el usuario final, proporcionando una interfaz de usuario formada por una amplia variedad de servicios y aplicaciones de red, algunas de estas aplicaciones y sus protocolos son:

Correo electrónico (POP y SMTP)

Transferencia de ficheros (FTP)

Acceso remoto (SSH y Telnet)

Transacción en la web (HTTP)

Supervisión de la red (SNMP)

Estos son algunos ejemplos debido a que existen tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

A continuación se muestra como se realiza la comunicación con las capas del modelo OSI. Las tres primeras capas dependen del tipo de red en el que funcione por lo que los equipos intermedios en la conexión solo utilizarán estas capas. Debido a que su arquitectura está organizada en capas, la información que proporciona el usuario a la capa de aplicación, va pasando de una capa a otra

hasta alcanzar la capa física donde pasa por el medio de transmisión hasta la capa física en el extremo opuesto.

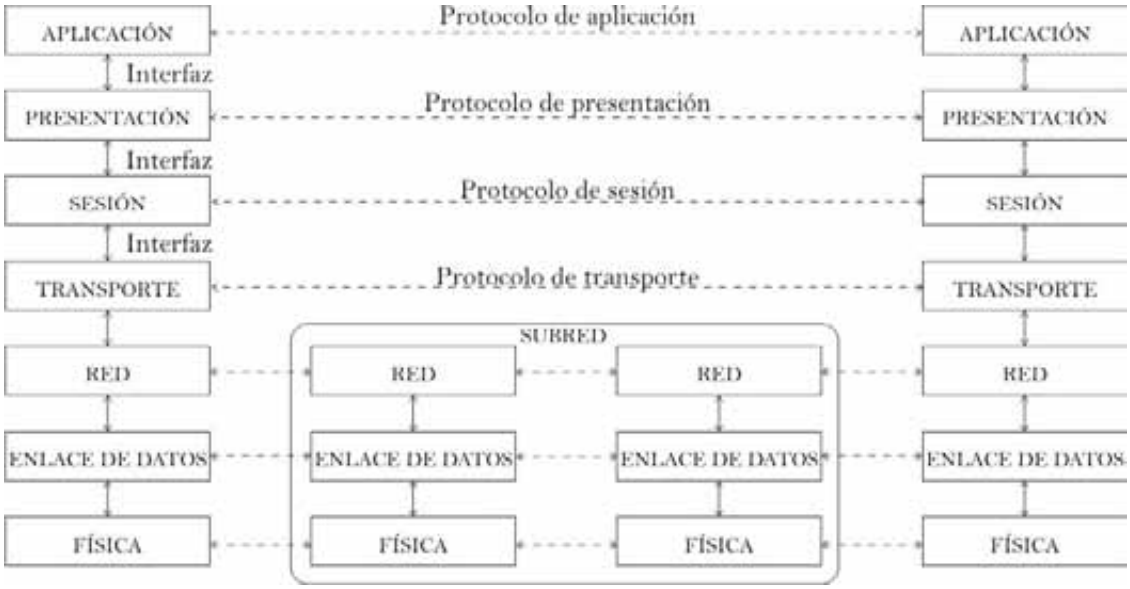



*Fig. 1.14 Proceso de comunicación de las capas del Modelo OSI*

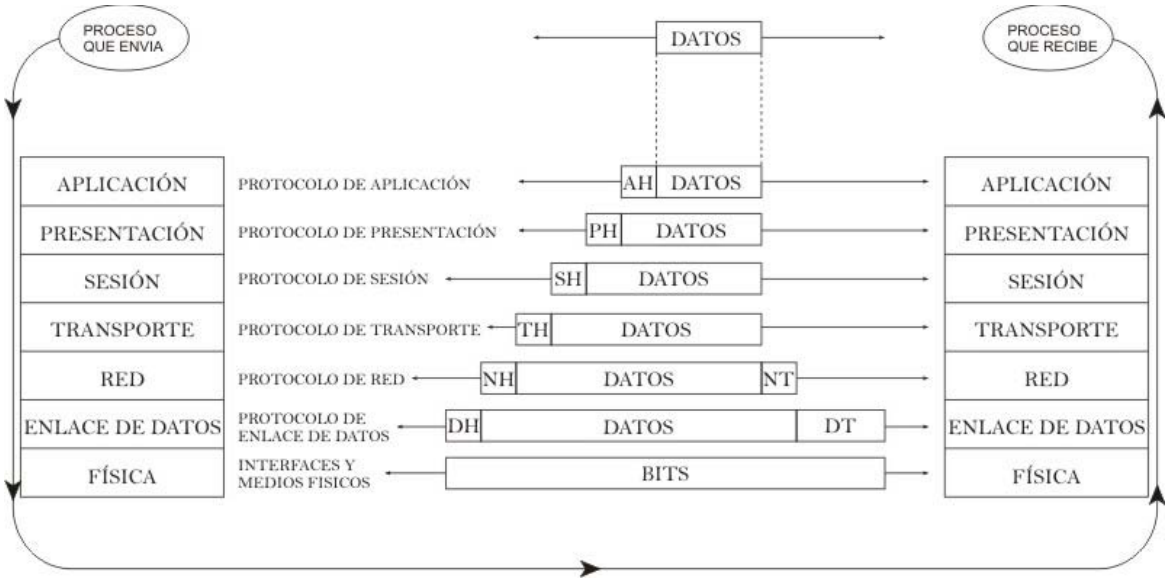



*Fig. 1.15 Proceso de envío de tramas del Modelo OSI*

A continuación se muestran los significados de los acrónimos utilizados en la imagen anterior:

| ACRÓNIMO | ELEMENTO | SIGNIFICADO |
|---|---|---|
| AH | Application Header | Cabecera de la capa de aplicación |
| PH | Presentation Header | Cabecera de la capa de presentación |
| SH | Session Header | Cabecera de la capa de sesión |
| TH | Transport Header | Cabecera de la capa de transporte |
| NH | Network Header | Cabecera de la capa de red |
| NT | Network Trailer | Cola de la capa de red |
| DH | Data-link Header | Cabecera de la capa de enlace de datos |
| DT | Data-link Trailer | Cola de la capa de enlace de datos |

*Tabla 1.1 Acrónimos de las cabeceras del Modelo OSI*

## I.4 EL MODELO TCP/IP

Las siglas TCP/IP significan Transmission Control Protocol/Internet Protocol. Originalmente era un estándar de UNIX, pero hoy en día está soportado por casi todas las plataformas y conforma el conjunto de protocolos de internet.

El IP representa el esquema mediante el cual dos dispositivos se comunican entre sí, mientras que TCP gestiona el flujo de paquetes IP y garantiza que los paquetes lleguen correctamente a su destino.

A diferencia del modelo OSI no hay un modelo oficial de referencia TCP/IP. No obstante, todas las tareas involucradas en la comunicación se pueden organizar en cinco capas relativamente independientes:

- Capa de aplicación
- Capa de origen-destino o de transporte
- Capa de internet
- Capa de acceso a la red
- Capa física

La capa física define la interfaz física y las características físicas de la comunicación entre el dispositivo de transmisión de datos y el medio de transmisión o red. Estas características pueden ser: las convenciones sobre la naturaleza del medio de comunicación (como las comunicaciones por cable, fibra óptica o radio), la velocidad de los datos y todo lo relativo a los detalles como los conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas.

La capa de acceso a la red es responsable de aceptar los datagramas IP y transmitirlos hacia una red específica de manera que el intercambio de datos entre el sistema final y la red a la que está conectado pueda realizarse correctamente, además de esto el emisor puede requerir ciertos servicios adicionales, como por ejemplo solicitar una determinada prioridad. El software en

particular que se use en esta capa dependerá del tipo de red que se disponga (ejemplo: X.25, Ethernet).

La función de la capa internet está en proporcionar una serie de procedimientos que permitan que la capa de acceso a la red pueda interconectar dos dispositivos que estén conectados a redes diferentes (enrutamiento). Durante el proceso de enrutamiento se hace uso de un servicio de conexión no orientado para el envío y recepción de paquetes. Esta capa está compuesta por los protocolos: IP, ARP, ICMP. El protocolo IP (Internet Protocol) ofrece el servicio de direccionamiento lógico de la red TCP-IP y el de enrutamiento de paquetes. El protocolo ARP "Address Resolution Protocol" ofrece el servicio de resolución de direcciones IP con su respectiva dirección física. Y el protocolo ICMP "Internet Control Message Protocol" ofrece el servicio de reporte de errores que pueden ocurrir durante el enrutamiento de paquetes. La unidad de datos que envía o recibe el protocolo IP se conoce con el nombre de datagrama IP.

La capa de transporte se encarga de proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. Debe regular el flujo de información, además de proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando avisos de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la capa de red. Los protocolos utilizados en la capa de transporte son el protocolo TCP (Transmition Control Protocol), que es un servicio orientado a conexión y el UDP (User Datagram Protocol) de la capa de transporte es un servicio no orientado a conexión. La unidad de datos que envía o recibe el protocolo TCP es conocido con el nombre de segmento TCP y la que envía o recibe el protocolo UDP es conocido con el nombre de datagrama UDP.

Finalmente la capa de aplicación contiene la lógica necesaria para posibilitar que los distintos programas puedan comunicarse a través de una red con otros programas. Los procesos que acontecen en esta capa son aplicaciones específicas que pasan los datos a la capa de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar.

Los programas específicos que se consideran se ejecutan en esta capa, proporcionan servicios que directamente trabajan con las aplicaciones de usuario. Estos programas y sus correspondientes protocolos incluyen a HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), SSH (*Secure Shell*), DNS (*Domain Name System*), SNMP (Protocolo de administración de la red) entre muchos otros.

Una vez que los datos de la aplicación han sido codificados en un protocolo estándar de la capa de aplicación son enviados a la siguiente capa de la pila de protocolos TCP/IP.

En la capa de transporte, las aplicaciones normalmente hacen uso de TCP y UDP, y son habitualmente asociados a un número de puerto bien conocido (*well-known port*). Estos puertos fueron asignados originalmente por la IANA (*Internet Assigned Numbers Authority*).

# Capitulo II
# TECNOLOGIAS EMPLEADAS EN LAS REDES

## II.1 MEDIOS DE TRANSMISION

Los medios de transmisión, utilizados para transportar información, se pueden clasificar como guiados y no guiados. Los medios guiados proporcionan un camino físico a través del cual la señal se propaga; entre los que cabe citar al par trenzado, al cable coaxial y la fibra óptica. Los medios no guiados utilizan una antena para transmitir a través del aire, vacío o el agua.

En los sistemas de transmisión de datos, el medio de transmisión es el camino físico entre el transmisor y el receptor. En cualquier caso, la comunicación se lleva a cabo con ondas electromagnéticas. En los medios guiados las ondas se confinan en un medio sólido, como, por ejemplo, el par trenzado de cobre, el cable de cobre coaxial o la fibra óptica. La atmósfera o el espacio exterior son ejemplos de medios no guiados, que proporcionan un medio de transmisión de las señales pero sin confinarlas; esto se denomina *transmisión inalámbrica.*

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio en sí mismo es lo más importante en la determinación de las limitaciones de transmisión.

En medios no guiados, el ancho de banda de la señal emitida por la antena es más importante que el propio medio a la hora de determinar las características de la transmisión. Una propiedad fundamental de las señales transmitidas mediante antenas es la directividad. En general, a frecuencias bajas las señales son omnidireccionales; es decir, la señal desde la antena se emite y propaga en todas las direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional.

En el diseño de sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grande posibles. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión

**El ancho de banda**: si todos los otros factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión puede incrementarse.

**Dificultades en la transmisión**: las dificultades, como, por ejemplo, la atenuación, limitan la distancia. En los medios guiados, el par trenzado sufre de mayores adversidades que el cable coaxial, que a su vez, es más vulnerable que la fibra óptica.

**Interferencias**: las interferencias resultantes de la presencia de señales en bandas de frecuencias próximas pueden distorsionar o destruir completamente la señal. Las interferencias son especialmente relevantes en los medios no guiados, pero a la vez son un problema a considerar en los medios guiados. Por ejemplo, frecuentemente múltiples cables de pares trenzados se embuten dentro de la misma cubierta, provocando posibles interferencias, no obstante, este problema se puede reducir utilizando un apantallamiento adecuado.

**Número de receptores**: un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido, mediante el uso de múltiples conectores. En este último caso, cada uno de los conectores utilizados puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirá.

## II.1.1 Medios de Transmisión Guiados

En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia y de si el medio se usa para un enlace punto a punto o multipunto, como redes LAN.

### II.1.1.1 Par trenzado

El par trenzado es el medio guiado más económico y a la vez el más usado. Está formado por un par de conductores de cobre aislados y trenzados entre sí, esto se hace para minimizar las interferencias provenientes de otros cables, es decir, hace al par trenzado más inmune frente a interferencias electromagnéticas. Cada par de cables constituye sólo un enlace de comunicación, normalmente se utilizan cables en los que se encapsulan varios pares mediante una envoltura protectora. En aplicaciones de larga distancia, la envoltura puede contener cientos de pares.

Tanto para señales analógicas como para señales digitales, el par trenzado es con diferencia el medio de transmisión más usado.

En telefonía, el terminal de abonado se conecta a la central local mediante cable de par trenzado. Igualmente, dentro de los edificios de oficinas, cada teléfono se conecta a la central privada (PBX, Private Branch eXchange) mediante un par trenzado.

En señalización digital, el par trenzado es igualmente el más utilizado. Generalmente, los pares trenzados se utilizan para las conexiones al conmutador digital o a la PBX digital, con velocidades de 64 Kbps. El par trenzado se utiliza también en redes de área local dentro de edificios para la conexión de computadores personales. La velocidad típica en esta configuración está en torno a los 10 Mbps. No obstante, recientemente se han desarrollado redes de área local con velocidades entre 100 Mbps y 1 Gbps mediante pares trenzados, aunque estas configuraciones están bastante limitadas por el número de posibles dispositivos conectados y la extensión geográfica de la red. Para aplicaciones de larga distancia, el par trenzado se puede utilizar a velocidades de 4 Mbps o incluso mayores.

Existen dos variantes de pares trenzados: apantallado y sin apantallar. El par trenzado no apantallado (UTP, Unshielded Twisted Pair) es el medio habitual en telefonía.

El par trenzado sin apantallar se puede ver afectado por interferencias electromagnéticas externas incluyendo interferencias con pares cercanos y fuentes de ruido. Una manera de mejorar las características de transmisión de este medio es embutiéndolo dentro de una malla metálica, reduciéndole así las interferencias. El par trenzado apantallado (STP, Shielded Twisted Pair) proporciona mejores resultados a velocidades de transmisión bajas, además que es más costoso y difícil de manipular que el anterior.

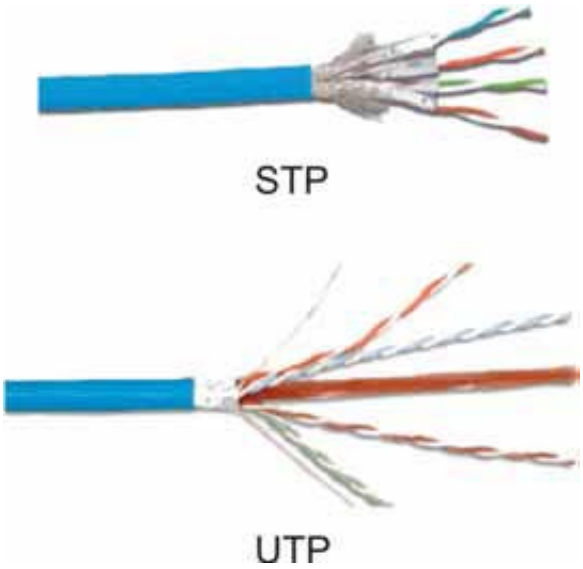



*Fig. 2.1 Tipos de Pares Trenzados*

Son tres tipos de cables UTP los que se utilizan en redes LAN, dependiendo de ancho de banda y el tipo de red utilizado:

**Tipo 3**: consiste en cables y su hardware asociado, diseñado para un ancho de banda de hasta 16 MHz Se utiliza en Ethernet

**Tipo 4**: consiste en cables y su hardware asociado, diseñado para un ancho de banda de hasta 20 MHz Se utiliza en Token Ring

**Tipo 5**: consiste en cables y su hardware asociado, diseñado para un ancho de banda de hasta 100 MHz Se utiliza en Fast Ethernet

De estos el tipo 5 es un cable de mejores características para la transmisión de datos y puede alcanzar velocidades de transmisión de hasta 100 Mbps.

En la siguiente tabla se presenta una comparación de las prestaciones de los cables tipo 3 y tipo 5 así como el STP especificado por EIA (Electronic Industries Association) en la norma 568-A. El primer parámetro para comparar es la atenuación que presenta el cable debido a la distancia y el otro es la diafonía debido a la inducción que provoca un conductor cercano.

| | Atenuación (dB por 100 m) | | | Diafonía en el extremo final (dB) | | |
|---|---|---|---|---|---|---|
| Frecuencia (MHz) | UTP tipo 3 | UTP tipo 5 | STP 150 Ω | UTP tipo 3 | UTP tipo 5 | STP 150 Ω |
| 1 | 2.6 | 2.0 | 1.1 | 41 | 62 | 58 |
| 4 | 5.6 | 4.1 | 2.2 | 32 | 53 | 58 |
| 16 | 13.1 | 8.2 | 4.4 | 23 | 44 | 50.4 |
| 25 | - | 10.4 | 6.2 | - | 41 | 47.5 |
| 100 | - | 22.0 | 12.3 | - | 32 | 38.5 |
| 300 | - | - | 21.4 | - | - | 31.5 |

*Tabla 2.1 Atenuación de diferentes tipos de pares trenzados*

### II.1.1.2 Cable coaxial

El cable coaxial es un cable de red de alta capacidad. Este cable tiene mejor blindaje que el par trenzado, así que puede abarcar tramos más largos a velocidades mayores. Consiste en una funda hueca blindada formada por cobre trenzado o por una lámina conductora (malla). Ésta rodea a un único conductor interno (vivo) aislado mediante un dieléctrico situado entre los dos elementos conductores.

La construcción y el blindaje del cable coaxial le confieren una buena combinación de elevado ancho de banda y excelente inmunidad al ruido. El ancho de banda posible depende de la longitud del cable. En cables de 1 km es factible una velocidad de datos de 1 a 2 Gbps. También se pueden usar cables más largos, pero a velocidades de datos más bajas o con amplificadores periódicos.


*Fig. 2.2 Cable coaxial*

Existen distintas clases de cable coaxial, sin embargo son 2 las más utilizadas. Una clase, el cable de 50 Ω, y el otro es el cable de 75Ω. El primero se utiliza comúnmente para transmisiones de banda base y el otro, se utiliza para transmisiones de banda ancha. El término *banda base*, hace referencia al abanico de frecuencias empleado en la transmisión de la señal. En este caso, se utiliza el mismo formato de información proporcionado por la fuente, sin realizarse en general ningún proceso de modulación o cambio de características en la información original. Ejemplos de esta aplicación son las versiones de Ethernet 10Base2 y 10Base5, pero han caído en desuso desde finales de la década de 1990.

El cable coaxial de banda ancha, se refiere a cualquier red que utilice transmisiones analógicas, aunque es posible transmitir señales digitales utilizando en cada interfaz circuitos electrónicos para convertir la corriente de bits saliente en una señal analógica y la señal analógica entrante en una corriente de bits.

Una diferencia clave entre la banda base y la banda ancha es que los sistemas de banda ancha normalmente cubre un área mayor, por lo tanto, necesitan amplificadores analógicos para reforzar la señal en forma periódica. Estos amplificadores solamente pueden transmitir señales en una dirección, de modo que mientras una computadora pueda enviarle información a otra, está última no podrá hacerlo si existe un amplificador de por medio.

La solución consiste en duplicar el medio físico, es decir, utilizar dos cables, uno de ida y otro de vuelta, de manera que cada sentido de la comunicación utilice uno de estos cables.

Otra posible solución consiste en multiplexar en frecuencias las señales. Esta comunicación se consigue separando el ancho de banda disponible, utilizando para ello las frecuencias más bajas para un sentido y las frecuencias más altas para el otro.

### II.1.1.3 Fibra óptica

El cable de fibra óptica es un cable que contiene una o varias fibras ópticas y que se utiliza para transmitir datos en forma de luz. El cable de fibra óptica es más caro y costoso de fabricar que el de cobre. Otro aspecto importante es la menor atenuación de las señales por este medio, lo que permite alcanzar mayores distancias.

El núcleo suele ser de fibra de vidrio aunque también puede ser de plástico. En realidad es el núcleo quien canaliza la luz en el camino de la comunicación. Debido a que es muy fino y de grosor similar al de un cabello, es muy delicado. El revestimiento y la cubierta proporcionan consistencia al cable.

La señal luminosa modulada en forma de pulsos, se transmite a través del núcleo, reflejándose sucesivamente en el revestimiento de la fibra, de tal forma que no hay pérdida de potencia apreciable. La refracción de este rayo luminoso se controla con un adecuado diseño del cable, así como de los equipos conectados a la fibra.

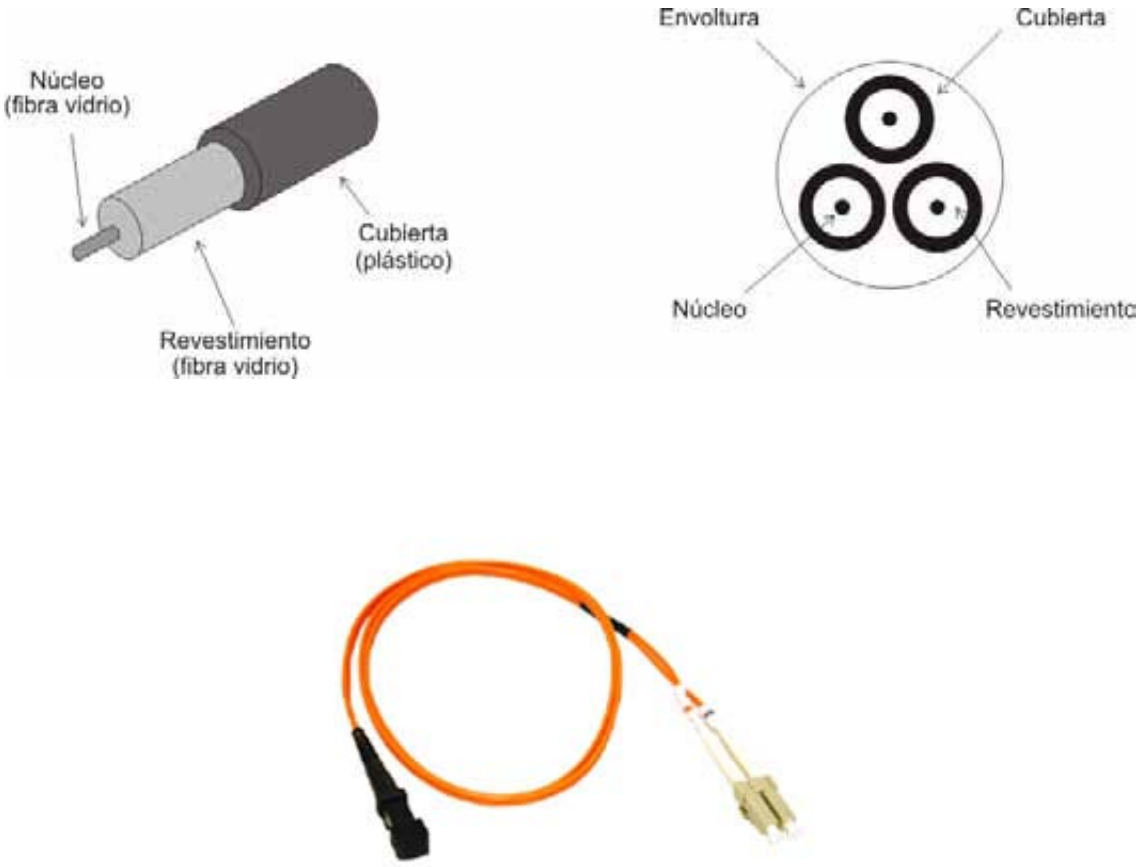



*Fig. 2.3 Cables de Fibra Óptica*

Existen dos tipos de fibras utilizadas en la transmisión de señales de datos, la *fibra monomodo* y la *fibra multimodo.*

*Fibra Monomodo:*

Potencialmente, esta es la fibra que ofrece la mayor capacidad de transporte de información. Tiene una banda de paso del orden de los 100 GHz/km. Los mayores flujos se consiguen con esta fibra, pero también es la más compleja de implantar, sin embargo se llama monomodo debido a que solamente un haz luminoso puede viajar a través de la fibra. Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten, es decir, entre 1 y 10 µm. Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Los elevados flujos que se pueden alcanzar constituyen la principal ventaja de las

fibras monomodo, ya que sus pequeñas dimensiones implican un manejo delicado y entrañan dificultades de conexión que aún se dominan mal.

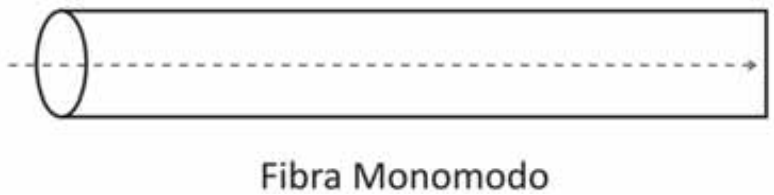



*Fig. 2.4 Ejemplo de fibra óptica monomodo*

*Fibra Multimodo:*

Una fibra multimodo es aquella que puede propagar más de un haz de luz, de manera que se pueden tener más de mil haces de propagación de luz por una sola fibra. Se usan comúnmente en aplicaciones de corta distancia, menores a 1 km, son simples de diseñar y económicas.

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Este diámetro suele estar comprendido entre los 50 y 60 µm y el del revestimiento en torno a los 125µm. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo:

Índice escalonado: en este tipo de fibra, el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal.

Índice gradual: mientras en este tipo, el índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales.

Las fibras multimodo tienen una banda de paso que llega hasta los 500MHz por kilómetro. Su principio se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra. Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra.


*Fig. 2.5 Ejemplo de fibra óptica multimodo*

## II.1.2 Medios de Transmisión no Guiados.

En medios no guiados, tanto la transmisión como la recepción se llevan a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), y en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

Las redes LAN inalámbricas se clasifican generalmente de acuerdo con la técnica de transmisión usada. Todas las redes LAN actuales se encuentran dentro de una de las siguientes categorías:

**LAN de infrarrojos (IR)**: una celda individual en una LAN IR está limitada a una sola habitación dado que la luz infrarroja no es capaz de atravesar muros opacos.

**LAN de espectro ensanchado**: este tipo de LAN hace uso de tecnologías de transmisión de espectro ensanchado. En la mayoría de los casos estas LAN operan en las bandas ISM (industria, ciencia y medicina), de modo que no se necesita licencia FCC para su utilización en los Estados Unidos.

**Microondas de banda estrecha**: estás LAN operan en el rango de las microondas pero no hacen uso de espectro ensanchado. Algunos de estos productos operan a frecuencias para las que es necesario licencia FCC, mientras que otras lo hacen en alguna e las bandas ISM.

| | **Infrarrojos** | | **Espectro ensanchado** | | **Radio** |
|---|---|---|---|---|---|
| | **Infrarrojos difusos** | **Infrarrojos de haz directo** | **Salto de frecuencia** | **Secuencia directa** | **Microondas de banda estrecha** |
| **Velocidad (Mbps)** | 1-4 | 1-10 | 1-3 | 2-20 | 10-20 |
| **Movilidad** | Estacionario/ Móvil | Estacionario con LOS | Móvil | Estacionario/Móvil | |
| **Rango (m)** | 20-70 | 30 | 35-100 | 35-300 | 15-40 |
| **Detectabilidad** | Despreciable | | Pequeña | | Alguna |
| **Longitud de onda/frecuencia** | λ: 800-900 nm | | 902-928 MHz<br>2.4-2.4835 GHz<br>5.725-5.85 GHz | | 902-928 MHz<br>5.2-5.775 GHz<br>18.825-19.205 GHz |
| **Técnica de modulación** | ASK | | FSK | QPSK | FS-QPSK |
| **Potencia radiada** | - | | <1W | | 25mW |
| **Método de acceso** | CSMA | Anillo con paso de testigo, CSMA | CSMA | | Reserva, ALOHA, CSMA |
| **Necesidad de licencia** | No | | No | | Sí a menos que sea ISM |

*Tabla 2.2 Cuadro comparativo de tipos de transmisión no guiados*

### II.1.2.1 Transmisión por radio

La transmisión por radio se refiere a cualquier técnica inalámbrica que use frecuencias de radio (RF) para transmitir información. Las transmisiones RF son actualmente muy populares para los servicios inalámbricos de datos. Las frecuencias de radio típicamente usadas para comunicaciones están en el rango de 800 MHz a 900 MHz del espectro electromagnético. En los Estados Unidos, la Comisión Federal de Comunicaciones (FCC) ha aprobado frecuencias adicionales para que los servicios de datos inalámbricos operen en el rango de 1.85 GHz a 2.20 GHz Esta porción del espectro de RF se usa, entre otras cosas, en radiolocalizadores, asistentes personales digitales (PDA), laptops con tarjetas PC y teléfonos celulares. Las WLAN sin licencia pueden utilizar las frecuencias comprendidas en el rango 2.4-2.5 GHz o 5.8-5.9 GHz, sin embargo estas bandas son usados para aplicaciones industriales, científicas y médicas y, por consiguiente, son comúnmente conocidas como bandas ISM (Industrial, Scientific, Medical). Como estas bandas no son reguladas por la FCC en los Estados Unidos, los dispositivos de espectro de difusión sin licencia generalmente operan dentro de esas bandas lo que provoca que estas se encuentren saturadas. Las frecuencias superiores en el rango GHz están menos llenas, pero el acceso es controlado por la FCC.

#### *Microonda*

Un tipo de transmisión RF es por microonda, que usa ondas de alta frecuencia y opera a una frecuencia alta del espectro radioeléctrico. El espectro de microondas abarca frecuencias entre 2 y 40 GHz El acceso a estas frecuencias es controlado estrictamente por la FCC; por lo tanto, los usuarios de transmisores por microondas deben ser autorizados. Las transmisiones por microondas son consideradas un medio de línea de vista. Como las señales de microondas viajan en línea recta, el transmisor y receptor deben estar en la línea de vista de cada uno de ellos, si no, debido a su longitud de onda muy corta, las señales de microondas se degradan una vez que encuentran una obstrucción. Aún el agua en gotas en la atmósfera atenúan las señales con microondas. En consecuencia, es necesario especificar el ambiente para garantizar que un transmisor y receptor de microondas tendrán una línea de vista clara, suficiente potencia para eliminar la atenuación y una distancia entre estaciones suficientemente pequeña, antes de instalarlas. Un medio para microondas usa antenas parabólicas montadas sobre torres hasta a 30 millas una de otra. Debido a la influencia de la curvatura de la Tierra sobre la línea de vista, entre más alta sea la torre mayor será el alcance.

Los medios de línea de vista como el de microondas son menos caros de instalar que el cable para distancias moderadas. Las microondas también ofrecen una relativamente alta velocidad de datos (45Mbps). Ellas también requieren poco o ningún mantenimiento, son bastante fáciles de implementar, y no tienen costos recurrentes mensuales o anuales, como sucede con los circuitos alquilados. Por otra parte, las transmisiones de línea de vista están sometidas a condiciones ambientales y atmosféricas (lluvia, niebla, alta humedad), así como a interferencia electromagnética de muchas fuentes, incluidas las tormentas y manchas solares. Además, si las unidades son colocadas muy cerca una de otra, pueden generar sobrecargas e interferencia en las señales. Debido a estos inconvenientes ambientales y atmosféricos, no debe confiarse completamente en comunicaciones con microondas en operaciones críticas.

### *Espectro ensanchado*

Otra tecnología de radio es el espectro ensanchado, que implica variar la frecuencia de una señal transmitida. Esto resulta en un ancho de banda mayor que con una señal no variada. El espectro ensanchado se conoce desde la Segunda Guerra Mundial y se usó para camuflar señales de radio. Sin él, la frecuencia de una señal permanece constante, lo que hace que la señal sea más susceptible a la interferencia o a la intercepción. La transmisión con espectro ensanchado enmascara los datos mezclando las señales con un patrón de pseudorruido (PN, por sus iníciales en ingles) y transmitiendo la señal real con el patrón PN. La señal transmitida es difundida sobre un rango de frecuencias en el espectro de radio. Así, para interceptar una señal, el receptor interceptor debe tener dos piezas de información específica: la función matemática que el transmisor está usando para generar el patrón PN y el momento exacto en que la función es generada.

### II.1.2.2 Transmisión infrarroja

La transmisión infrarroja (IR) es otro medio de línea de vista. Ella usa radiación electromagnética de longitud de onda entre las ondas de radio y de la luz visible, operando entre 100 GHz y 100 THz. La IR directa requiere una conexión de línea de vista no obstruida entre el transmisor y el receptor. Se trata, básicamente de un medio de “punto y haz”. En un ambiente de “IR difusa”, un transmisor “inunda” un área específica con una fuerte señal infrarroja. La luz emitida desde el transmisor es difundida sobre un ángulo amplio. La señal IR es transmitida por reflexión en cielos rasos, paredes y otras superficies. Así, la IR difusa puede considerarse como un medio de difusión, mientras que la IR directa es punto a punto. Así como las microondas, la IR es susceptible a algunos de sus mismos problemas, aunque es más resistente a la interferencia electromagnética.

## II.2 DISPOSITIVOS DE INTERCONEXION DE REDES

Estos equipos son los que permiten la comunicación entre un equipo y otro de una red o de diferentes redes dependiendo su aplicación. Estos equipos se describen a continuación:

### II.2.1 Repetidores

Los repetidores son dispositivos que trabajan al nivel físico, capaces de interconectar dos o más segmentos idénticos en una red de área local. Simplemente amplifican o regeneran las señales débiles a su entrada, retransmitiéndolas bit a bit hacia todos los segmentos de salida.

El repetidor en la norma 802.3 es el primer equipo clave para aumentar el tamaño o extensión física de la red, pues los segmentos de red están limitados a una longitud máxima de 100 metros en la implementación 10BaseT. Si necesitamos una extensión de red mayor, deberemos interconectar varios segmentos mediante repetidores.

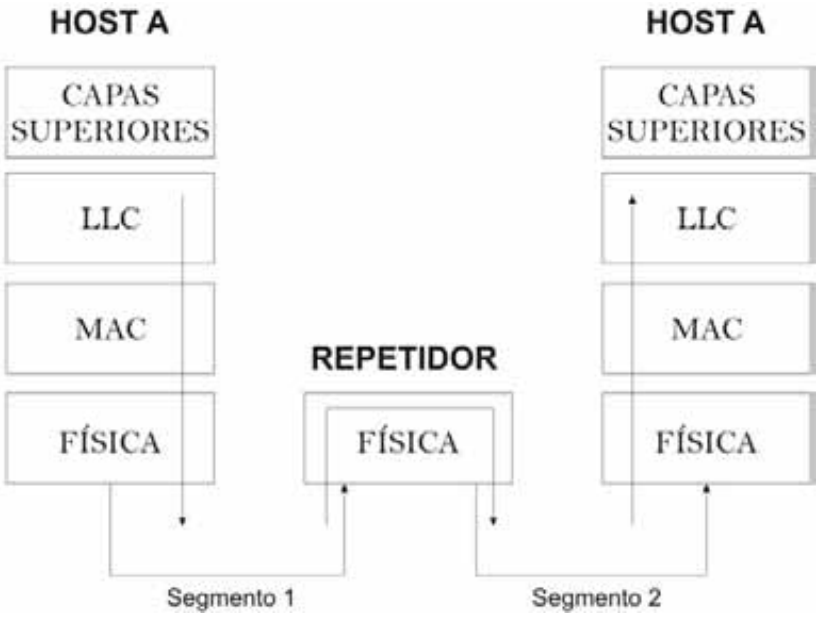



*Fig. 2.6 Funcionamiento de un repetidor en función del modelo OSI*

No obstante, el uso de repetidores presenta algunas limitaciones. En primer lugar, no pueden instalarse más de cuatro repetidores en serie, es decir; entre dos estaciones cualesquiera. En segundo lugar, esta nueva red no puede formar lazos cerrados, puesto que la información transmitida estaría continuamente circulando.

La principal ventaja de los repetidores es su simplicidad y rapidez, pues regeneran y retransmiten la información sin necesidad de almacenar tramas de información. La principal desventaja de los repetidores es la gran cantidad de tráfico que generan, puesto que no son capaces de filtrar el tráfico en función de su destino. De esta forma, cuando u repetidor recibe una trama de datos la retransmite por su salida o salidas, independientemente del destino específico de la trama.

## II.2.2 Concentradores (Hubs)

Un hub, no es más que un repetidor multipuerto con mayores prestaciones; básicamente es un dispositivo que concentra, esto es, reparte el ancho de banda disponible entre sus salidas o puertos.

El funcionamiento del hub es el siguiente:

- Cuando un hub recibe una señal de datos válida por alguna de sus entradas, la retransmite al resto de las salidas.
- Cuando el hub recibe dos o más señales de datos simultáneamente por varias entradas, se produce una situación de colisión, puesto que hay varias estaciones intentando acceder al canal de forma simultánea. En este caso el hub envía una señal de invalidación (jam) por todas las salidas.

- Cuando un hub recibe una señal de invalidación por una de sus entradas, la retransmite a todas sus salidas. Los hubs de este tipo suelen tener un piloto luminoso que indica la situación de colisión.

Es posible conectar en cascada varios hub Ethernet para ampliar el tamaño de la red. La conexión entre dos hub se realiza de forma similar a la conexión entre el hub y una estación. Se emplea igualmente un cable de conexión directo, utilizando en el hub a ampliar el puerto marcado como "uplink" o puerto cruzado.

El número máximo de hubs que pueden existir en el camino que une a dos estaciones cualesquiera no puede ser superior a cuatro. En el caso de una red Fast Ethernet 100BASETX, el máximo es de dos hub, por lo que la distancia máxima entre dos estaciones no podrá superar los 200metros. Si deseamos ampliar nuestra red requeriremos otros elementos de conexión adicionales como puentes, conmutadores o routers.

En la actualidad existen hubs que poseen una entrada BNC para conectar un segmento de cable coaxial, de esta forma es posible combinar implementaciones Ethernet 10BASE2 y 10BASET en la misma red.

Finalmente, existen otro tipo de hubs que son denominados *hubs inteligentes*. Un hub inteligente es un concentrador que dispone de la capacidad de proceso para realizar determinadas funciones adicionales como:

- Gestión de red mediante SNMP, RMON, etc.
- Capacidad de conectar tipos de LANs diferentes: Ethernet, Token Ring, FDDI
- Incorporación opcional de funciones de puente y/o router para permitir la interconexión entre las redes anteriormente mencionadas
- Mecanismos de seguridad, redundancia y tolerancia a fallos.

### II.2.3 Conmutadores (Switches)

Un conmutador o switch es un dispositivo de interconexión de redes, capaz de proporcionar un camino de comunicación dedicado entre un puerto origen y otro destino. Este dispositivo trabaja en la capa 2 según el modelo OSI. El conmutador presenta dos grandes ventajas respecto a un hub o repetidor multipuerto. En primer lugar se reduce notablemente el tráfico en la red, ya que el switch filtra la información en función de la dirección física de la estación destinataria, reenviando los datos por la salida o salidas apropiadas. En segundo lugar, el conmutador permite establecer varios canales de datos simultáneos entre distintos equipos o redes. No obstante, a cada puerto se le puede conectar un segmento de red mediante algún hub.

Para poder reenviar la información al puerto de salida adecuado, el conmutador debe acceder a la trama MAC de la capa de enlace de datos para leer la dirección de la estación destinataria. Para realizar esto, el conmutador implementa una tabla que asocia direcciones físicas a puertos,

además de incorporar un mecanismo de aprendizaje, de manera que cuando una estación se activa, el switch inserta esta dirección en la tabla y la asocia a su correspondiente puerto.

Aunque son destacables estas ventajas, el conmutador es un dispositivo menos rápido que un concentrador, pues debe interpretar al menos parcialmente las tramas de datos para conocer la dirección destino. No obstante, la red resultante en su conjunto posee un mayor rendimiento, ya que no existirán colisiones y, por tanto, no se formarán cuellos de botella.

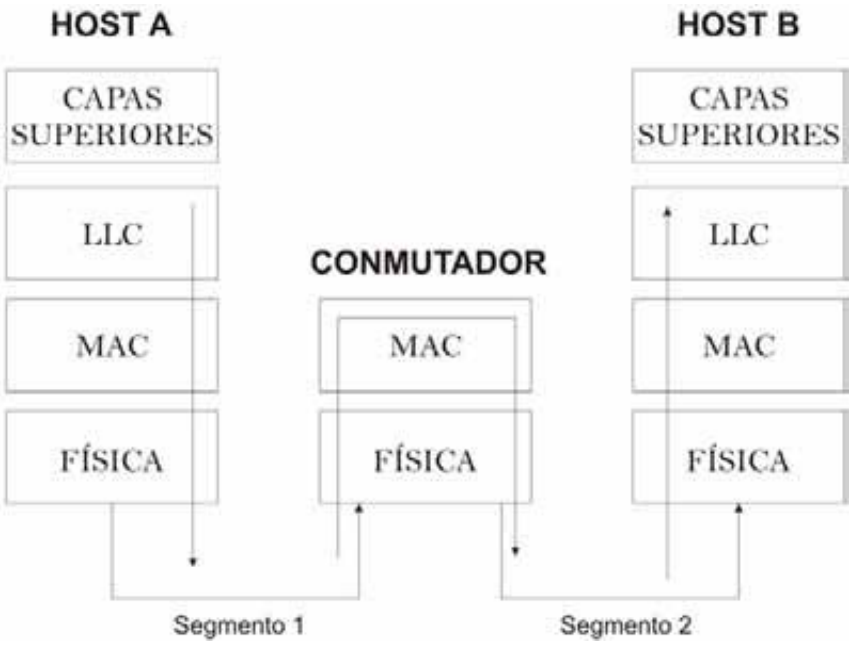



*Fig. 2.7 Funcionamiento de un conmutador en función del modelo OSI*

En función del tipo de puertos soportados por el conmutador, podemos distinguir entre *switches simétricos*, en los que todos los puertos trabajan a la misma velocidad, y *switches asimétricos.* Estos últimos funcionan indistintivamente con puertos trabajando a distintas velocidades, por ejemplo, a 10 Mbps y a 100 Mbps, e incluso a 1000 Mbps, de manera que es posible mezclar redes Ethernet, Fast Ethernet y Gigabit Ethernet.

Este tipo de conmutadores implementa un *mecanismo de autonegociación* que permite trabajar con adaptadores de red o segmentos de diferentes velocidades. Cuando se establece una comunicación entre una estación o segmento de red, previamente se establece un protocolo de autonegociación en el que se negocia, tanto la velocidad de transmisión, como el modo de transmisión.

En la práctica, dado que el coste de un switch es más elevado que el de un hub, se suele conectar al conmutador equipos que soportan gran cantidad de tráfico, tales como servidores. Lo ideal es que toda la red estuviese conmutada, aunque si no es posible, se podrán utilizar hubs para conectar estaciones de trabajo que no requieran tanto ancho de banda.

## II.2.4 Puentes (Bridges)

A diferencia de los repetidores, que retransmiten los bits a medida que llegan, los puentes son dispositivos que copian las tramas completas, observan sus direcciones de destino y las redirigen hacia la salida o puerto adecuado. Los puentes aceptan tramas enteras y las pasan a la capa de enlace de datos, donde se realizarán ciertas funciones como la verificación del *checksum* o suma de verificación.

Los puentes pueden realizar ciertos cambios en la trama de origen antes de reenviarla, como agregar o quitar algunos campos de la cabecera de la trama. Puesto que los puentes son dispositivos que trabajan en la capa de enlace de datos, no tienen relación con las cabeceras de las capas superiores, y no pueden hacer cambios ni tomar decisiones que dependan de ellas.

En cierto modo, un puente es un dispositivo similar a un switch de almacenamiento y reexpedición, aunque presenta dos diferencias fundamentales. En primer lugar, el puente puede interconectar varias redes de área local con diferentes capas de acceso al medio MAC y, por tanto, debe ser capaz de convertir el formato de las tramas de red origen al formato propio de la red destino. En segundo lugar, los puentes pueden tomar decisiones de encaminamiento más complejas que los switches, en el caso de que exista más de una ruta posible entre las estaciones origen y destino, delimitando el tráfico que viaja por la red.

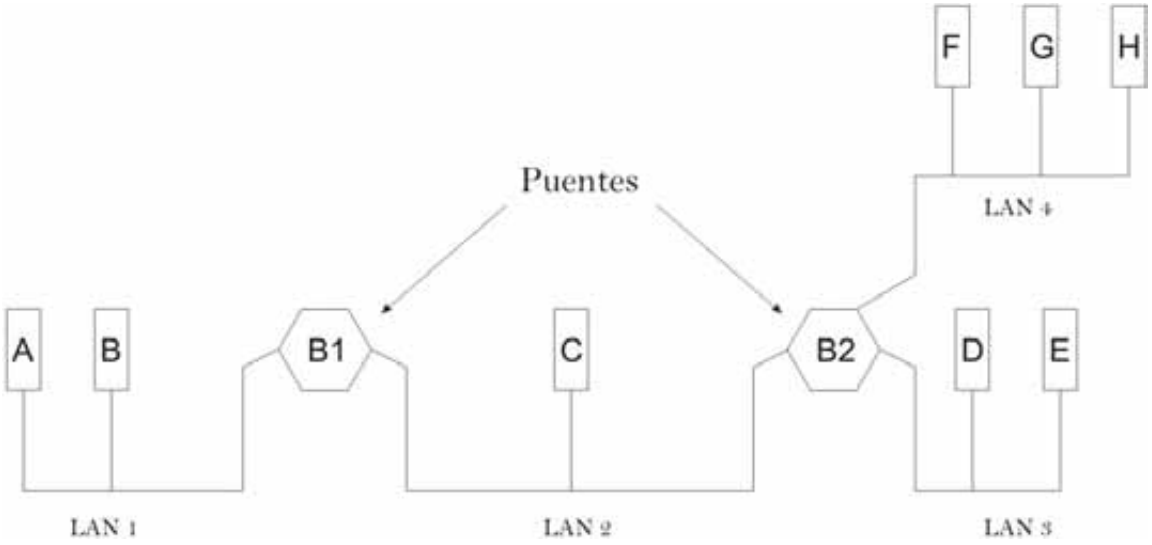



*Fig. 2.8 Interconexión de LANs mediante dos puentes*

Para interconectar redes de área local de distinta clase, los puentes deben realizar las siguientes funciones:

*Control de la longitud de las tramas:* Esto se utiliza en caso de que las redes interconectadas tengan distintas longitudes en sus tramas.

*Adaptación de las velocidades entre redes:* Se utiliza en caso de que las LANs conectadas funcionen a distintas velocidades de transmisión. En este caso el puente debe disponer de cierta capacidad de almacenamiento para adaptar las velocidades entre redes.

*Conversión de formatos de la trama MAC entre la red origen y la red destino:* Para esta situación se deben adaptar determinados campos existentes en unos formatos de trama y ausentes o diferentes en otros, tales como los campos de prioridad y los campos reservados al código de redundancia.

Como en el caso de los repetidores, existen diversos tipos de puentes, pudiendo ser apilables o modulares e incorporando funciones inteligentes. Un dispositivo especial es el BRouter o Puente-Enrutador. Este es un dispositivo que funciona como un router para un determinado protocolo o grupo de éstos, y como un puente puede tener un router en redes multiprotocolo, ya que permite la interconexión de sus segmentos y, sin embargo, los deja aislados en aquellos protocolos para los que no ha sido diseñado.

## II.2.5 Encaminadores (Routers)

La utilización de puentes está limitada a la interconexión de redes de área local, pero cuando deseamos conectar una red de área local a otras redes (WAN, redes IP, redes públicas, etc.) es necesario utilizar un dispositivo de interconexión denominado *router* o encaminador.

Conceptualmente los routers son parecidos a los puentes, excepto que su funcionamiento es definido por la capa de red. Para interconectar redes a través de routers, es necesario que se encuentren entre estas. En la actualidad el protocolo IP es el más extendido. Este es el protocolo de red utilizado en internet y forma parte de la familia de protocolos TCP/IP. No obstante, existen routers específicos que implementan determinados protocolos de nivel de red. Los routers que pueden implementar varios de estos protocolos se denominan *routers multiprotocolo.*

Un router de la red Internet es un dispositivo de interconexión que trabaja a nivel IP y que realiza básicamente dos funciones:

Efectúa la traducción de protocolos de los niveles inferiores entre la red origen y la red destino.

Proporciona los mecanismos de encaminamiento necesarios para poder alcanzar cualquier estación destino desde cualquier estación origen, ambas conectadas a internet con independencia del número de routers y redes intermedios.

La importancia de los routers radica, entre otras cosas, en la posibilidad de configurar éstos para poder encaminar los paquetes por determinadas rutas, intentando evitar situaciones en las que alguno de los routers o subredes intermedios falle, pudiéndose desviar el tráfico por rutas alternativas, e incluso en casos de congestión de la red, evitar saturarla, disminuyendo la transmisión de paquetes.

En la siguiente tabla podemos ver resumidas las funciones de los distintos equipos de interconexión y a que niveles trabajan:

| NOMBRE | CAPA | FUNCION |
|---|---|---|
| Repetidor | Física | Salvaguarda las limitaciones en las distancias físicas |
| Conmutador | MAC | Aísla los segmentos de la red de área local |
| Puente | LLC | Conversión de formatos de trama<br>Aislamiento de tráfico en función de las direcciones MAC |
| Router | Red | Encamina los paquetes basándose en las direcciones de nivel de red. |

*Tabla 2.3 Dispositivos de interconexión de redes*

Los routers también pueden instalarse para delimitar tráficos de red entre redes de área local existentes.

### II.2.6 Punto de acceso (Access Point)

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas. No solo es el medio de intercomunicación de todas las terminales inalámbricas, sino que también puede ser de interconexión con la red fija e Internet.

Existen dos categorías de puntos de acceso:

Puntos de acceso profesionales. Están diseñados para crear redes corporativas de tamaño medio o grande. Estos suelen ser los más caros, pero incluyen mejores características (aunque sean particulares del fabricante), como son mejoras en la seguridad y una más perfecta integración con el redo de los equipos.

Puntos de acceso económicos. Son dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados.

Aparte de lo anterior, cada equipo tiene sus propias características externas. Por ejemplo, algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos exteriores que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora (con su servidor de impresión), mientras que otros se limitan a ofrecer una conexión para red cableada o internet.

El objetivo principal de los puntos de acceso es comunicarse con las terminales vía radio. Por lo tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de *chips* electrónicos conocidos como *chipsets*. Aunque en el mercado existen muchos fabricantes de puntos de acceso, son muchos menos los que fabrican chipsets.

Desde el punto de vista del usuario, el funcionamiento de los distintos chipsets es idéntico. Además, entre ellos deben ser compatibles. No obstante, la teoría de la compatibilidad a veces trae sorpresas, por lo que resulta recomendable comprar equipos que utilicen chipsets del mismo fabricante. La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante.

*Fig. 2.9 Punto de acceso*

## II.3 ADAPTADORES INALAMBRICOS DE RED

Los adaptadores de red son las tarjetas o dispositivos que se conectan a las computadoras para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red.

Los adaptadores de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores o con un punto de acceso para mantener a la computadora a la que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Ésta suele venir integrada dentro del propio adaptador sin que externamente se note. Algunos adaptadores, sin embargo, permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer de una antena externa. Este tipo de antenas aumentan considerablemente el alcance del adaptador.

### II.3.1 Tipos de adaptadores de red

Al igual que desde hace tiempo viene siendo normal encontrar computadoras que incluyen de fábrica un puerto Ethernet RJ45, recientemente están apareciendo en el mercado computadoras portátiles que ya tienen integrado un adaptador de red Wi-Fi.

Actualmente, existen los siguientes tipos de adaptadores de red:

- Tarjetas PCMCIA
- Tarjetas PCI o ISA
- Unidades USB

### II.3.1.1 Tarjetas PCMCIA

Uno de los problemas que tenían antiguamente las computadoras portátiles era que difícilmente podían ampliarse en sus prestaciones. Normalmente el interior de los portátiles estuvo completamente cerrado hasta que aparecieron unos puertos especiales conocidos como PCMCIA (Personal Computer Memory Card International Association, Asociación Internacional de Tarjetas de Memoria para Computadoras Portátiles).

Los puertos PCMCIA son una especie de ranura en la que se pueden insertar las tarjetas correspondientes. Estas tarjetas quedan insertadas en el interior de la ranura, por lo que la computadora portátil no pierde su integridad y fácil portabilidad.

Todas las tarjetas PCMCIA tienen un ancho de 54 milímetros, siendo su largo variable, pero con un máximo de 85.6 milímetros. El hecho de ser variable se debe a que algunas tarjetas necesitan sobresalir hacia el exterior para mostrar algún tipo de conector, una antena o porque necesitan más espacio.

En cuanto al grosor de las tarjetas existen tres tipos: las tarjetas tipo I con un grosor de 3.3 milímetros (utilizadas, por ejemplo, para ampliaciones de memoria), las de tipo II con un grosor de 5 milímetros (son las habituales de los adaptadores de red inalámbricos) y las de tipo III con un grosor de 10.5 milímetros (utilizadas, por ejemplo, por los discos duros)

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en la computadora. Esto quiere decir que una ranura de tipo III admite cualquier tipo de tarjeta, mientras que una ranura de tipo I sólo admite tarjetas de este tipo. El tamaño más habitual de las tarjetas es del tipo II.


*Fig. 2.10 Tarjeta de red PCMCIA*

### II.3.1.2 Adaptadores PCI e ISA

Debido a que una computadora de escritorio tiene suficiente espacio interior, permiten la instalación de otro tipo de periféricos a base de tarjetas denominados PCI (Peripheral Components Interconnect, Interconexión de Componentes Periféricos) o ISA (Industry Standard Architecture, Arquitectura Normalizada de la Industria). Este tipo de tarjetas son más baratas que las tarjetas PCMCIA, aunque también son mayores en Tamaño y de instalación un poco más compleja. Lo curioso en este caso es que difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI o ISA. El motivo quizás sea que las mayores prestaciones de las redes inalámbricas se consiguen con una computadora portátil. Sin embargo una solución a este problema consiste en utilizar un adaptador USB en la computadora.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior de la computadora. Por tanto, hay que abrir la computadora. Adicionalmente, incluso los que anuncian ser *Plug & Play* (conectar y funcionar) requieren que se les instale el software con los controladores.

Por otra parte, si se tiene una computadora que dispone tanto de ranuras PCI como ISA, siempre es más aconsejable utilizar las de tipo PCI. Estas suelen dar menos problemas de instalación y requieren menos recursos del sistema.

*Fig. 2.11 Tarjeta de red PCI*

### II.3.1.3 Adaptadores USB

USB (Universal Serial Bus, Bus de Serie Universal) es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en como los periféricos se conectaban a las computadoras.

USB vino a traer las siguientes ventajas:

- ✓ No hace falta apagar la computadora para conectar o desconectar un periférico USB.
- ✓ La computadora reconoce automáticamente los periféricos que se conectan mediante USB. Si es preciso, instala automáticamente los controladores necesarios para hacerlo funcionar adecuadamente.
- ✓ Ofrecen una alta velocidad de transferencia de datos: hasta 12 Mbps
- ✓ Permite conectar hasta 127 dispositivos USB. Incluso, aunque el ordenador disponga de un solo puerto, basta con instalar un multiplicador de puertos (hub) para disponer de más puertos USB.
- ✓ Ofrece alimentación eléctrica a los periféricos a través del propio conector USB (hasta 500 mA).
- ✓ Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.
- ✓ Los periféricos USB se instalan automáticamente.

Estas ventajas han hecho que los periféricos USB hayan ido desplazando poco a poco al resto de periféricos del mercado, hasta el punto de que ya existen computadoras que no disponen de puertos serie ni paralelo, sino solo de puertos USB.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes ordenadores según se necesite. Como instalar el adaptador es tan fácil como conectarlo al puerto USB, si un ordenador necesita conectarse a la red, bastará con enchufar el adaptador. Cuando no lo necesite, con desenchufarlo del puerto USB se tiene bastante.

Otras de las ventajas es que el adaptador puede reorientarse con respecto al punto de acceso para buscar una mejor cobertura, sin tener que mover el ordenador.

El único inconveniente de los adaptadores USB es que son dispositivos externos a la computadora. No quedan integrados dentro de él como lo hacen los adaptadores PCMCIA, PCI o ISA.

*Fig. 2.12 Adaptadores USB*

Todos los dispositivos, independientemente de que sean adaptadores de red o puntos de acceso tienen dos modos de funcionamiento.

- **Modo Managed**. es el modo en el que un adaptador se conecta al punto de acceso para que éste último le sirva de "concentrador". En este caso el adaptador se comunica únicamente con el punto de acceso
- **Modo Master**. Este modo es el modo en el que trabaja el punto de acceso, pero también lo pueden utilizar los adaptadores si disponen del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Con estos modos de funcionamiento observamos que básicamente todos los dispositivos Wi-Fi son iguales, siendo los puntos de acceso realmente adaptadores de red a los que se les ha añadido cierta funcionalidad extra vía firmware.

Esta afirmación se ve confirmada al descubrir que muchos puntos de acceso en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como adaptadores de red.

## II.4 ANTENAS

Una antena es un dispositivo que permite la emisión y recepción de ondas electromagnéticas (ondas de radio) de una determinada frecuencia. Esto quiere decir que las antenas convierten las señales eléctricas en ondas electromagnéticas y viceversa.

Todos los equipos Wi-Fi incorporan sus propias antenas, sin embargo, cuando se desea disponer de una red de mayor alcance o cobertura, a veces, resulta conveniente sustituir la antena incorporada por otra exterior con mayor ganancia. El obtener un buen resultado en la colocación de antenas exteriores depende no sólo del conocimiento técnico que se tenga de los distintos tipos de antenas, sino también de la experiencia que se tenga instalándolas.

La razón de que no existan reglas absolutas para el diseño y localización de las antenas es que son muchas las variables que afectan a la propagación de la señal electromagnética. Además, con las redes inalámbricas nos enfrentamos a usuarios móviles y condiciones ambientales variables. Esto significa que la colocación de una antena exterior requiere de cierta experimentación hasta encontrar la mejor solución.

Una característica importante en las antenas es su ganancia. Para una antena la ganancia representa la relación entre la intensidad de campo que produce en un punto determinado y la intensidad de campo que produce una antena omnidireccional en el mismo punto y en las mismas condiciones. Una antena es mejor cuanto mayor es su ganancia.

El valor de la ganancia de una antena se mide en decibelios (dB). El decibelio es una unidad que se calcula como el logaritmo de una relación de valores. Una escala logarítmica permite que simples números representen grandes variaciones en los niveles de una señal. Los niveles de ganancia en decibeles en relación con los niveles de potencia se describen en la siguiente tabla:

| Watts | Decibeles |
|---|---|
| 1/1000 | 0 dB |
| 1/100 | 10 dB |
| 1/10 | 20 dB |
| 1/4 | 24 dB |
| 1/2 | 27 dB |
| 1 | 30 dB |
| 2 | 33 dB |
| 5 | 37 dB |

*Tabla 2.4 Ejemplos de ganancia de señal en relación con la potencia de salida*

Los términos utilizados para trabajar con decibeles son los siguientes:

- **dB**: Es la unidad básica que representa la proporción dos niveles de señales
- **dBm / dBW** Decibel miliWatt. Esta medida es usada para representar la potencia tomando como referencia que 0 dBm son equivalentes a 1 miliWatt. Para señales más potentes,

existe el dBW que equivale a 1W. Usualmente cuando nos referimos a dispositivos Wi-Fi, la potencia de salida está dada en dBm. La mayoría de las tarjetas WLAN PCMCIA y algunos puntos de acceso tienen una potencia de salida de +17dBm (50mW).

- **dBd.** Decibel de dipolo. Es la ganancia que una antena tiene sobre una antena de tipo dipolo funcionando en la misma frecuencia. Esta unidad de medida es usualmente utilizada en antenas por debajo de 1 GHz

- **dBi.** Decibel isotrópico. Es una medida utilizada en antenas por encima de 1 GHz, y es utilizada para calcular la ganancia de una antena teniendo como referencia una antena omnidireccional, también llamada antena isotrópica.

Una regla básica que hay que considerar al momento de trabajar con los decibeles es "la regla de 3 dB". Esta regla estipula que por cada 3 dB de incremento de la señal, la potencia es duplicada. Por cada 3 dB de atenuación, la potencia se corta a la mitad. De la misma manera, cada 10 dB de incremento multiplicará la potencia x 10, mientras que 10 dB de atenuación resultara en 1/10 de potencia.

Las antenas de los puntos de acceso suelen ser antenas verticales omnidireccionales. Estas antenas tienen una ganancia mayor que las antenas que vienen incluidas en los adaptadores de red, pero menor que una antena externa direccional. Las antenas direccionales concentran la energía radiada en una sola dirección, por lo que consiguen que la energía radioeléctrica llegue mucho más lejos (mayor alcance, aunque en una sola dirección).

### II.4.1 Patrón de radiación

El patrón de radiación (*radiation pattern*) es un diagrama polar sobre el que se representa la fuerza de los campos electromagnéticos radiados por una antena. Las antenas omnidireccionales emiten en todas direcciones y tienen menor alcance que las antenas direccionales. El patrón de radiación suele ser representado en dos planos: horizontal y vertical.

Otro valor que está relacionado con el modelo de radiación es la apertura del haz. Este valor se expresa en grados y representa la separación angular entre los dos puntos del lóbulo principal del patrón de radiación donde el valor de la energía electromagnética es la mitad de la original (-3dB). La apertura del haz se suele representar, aunque no siempre, sobre el plano horizontal.

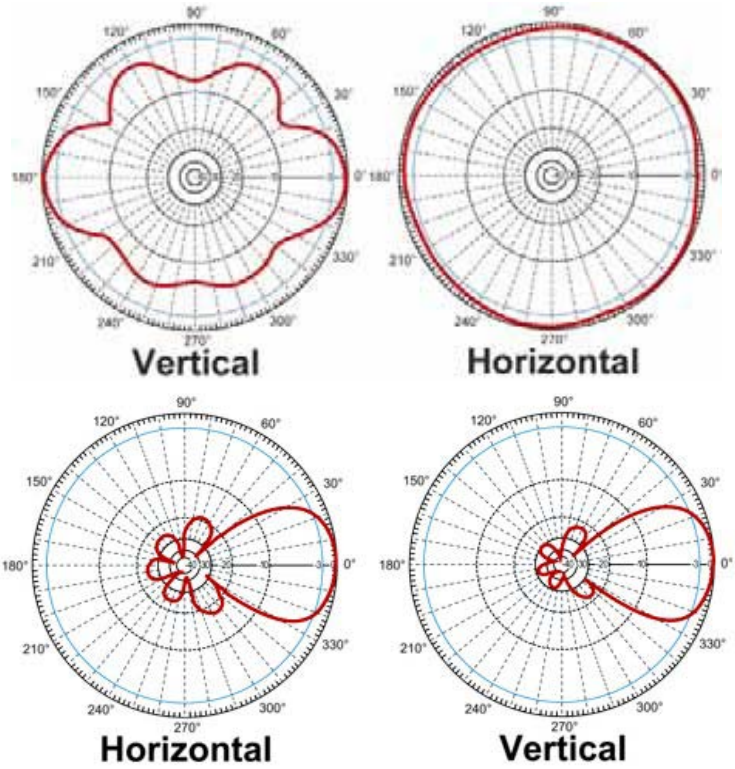



*Fig. 2.13 Ejemplos de patrones de radiación: arriba el de una antena omnidireccional y abajo el de una antena yagui*

## II.4.2 Polarización

La polarización de una antena describe la orientación de los campos electromagnéticos que irradia o recibe la antena. Las formas de polarización más comunes son las siguientes:

- **Vertical**. Cuando el campo eléctrico generado por la antena es vertical con respecto al horizonte terrestre (de arriba abajo).
- **Horizontal**. Cuando el campo eléctrico generado por la antena es paralelo al horizonte terrestre.
- **Circular.** Cuando el campo eléctrico generado por la antena va rotando de vertical a horizontal y viceversa, creando movimientos circulares en todas direcciones. La polarización circular puede girar en sentido de las manecillas del reloj o en sentido contrario.
- **Elíptica**. Cuando el campo eléctrico se mueve como en la polarización circular pero con desigual fuerza en las distintas direcciones. Generalmente, este tipo de polarización no suele ser intencionado.

## II.4.3 Tipos de Antenas

En la actualidad existen tantos tipos de antenas como ha permitido la imaginación: yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, patch, dipolo, planas, compactas, móviles, etc. No obstante, todos estos tipos de antenas pueden agruparse en tres tipos primarios: *omnidireccional, direccional* y *sectorial*.

**ANTENAS DIRECCIONALES:** Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

**ANTENA OMNIDIRECCIONALES:** Orientan la señal en todas direcciones con un haz amplio pero de corto alcance.

Las antenas Omnidireccionales transmiten la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

**ANTENAS SECTORIALES:** Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

*Fig. 2.14 Antena Omnidireccional*

Existen distintos modelos de antenas direccionales entre los cuales destacan los siguientes:

*Antena yagui***:** Es una antena direccional con una apertura de haz de entre 15 y 60 grados. Su ganancia varía entre los 6 y los 21 dBi. Estas antenas suelen venir montadas en el interior de una cobertura cilíndrica.


*Fig. 2.15 Antena Yagui*

*Antena de panel:* Es una antena plana para ser montada en la pared. Esta antena emite energía siguiendo un modelo semiesférico. Tienen ganancias de entre 12 y 22 dBi. Su mayor inconveniente es que, al ser plana, puede sufrir por la fuerza del viento si se sitúa en el exterior.

*Fig. 2.16 Antena de Panel*

*Antena Parabólica:* Es una antena que tiene forma de disco cóncavo con la que se consiguen unos haces muy direccionales. Es muy útil para comunicaciones punto a punto y se pueden conseguir ganancias de hasta 27 dBi. En el mercado existen distintas configuraciones de antenas parabólicas: redondas, malladas, cuadradas, etc.

*Fig. 2.17 Antenas parabólicas*

Además de las anteriores, existen otros tipos de antenas (dipolos, reflectores, etc.) que pueden ser utilizadas en las instalaciones Wi-Fi. En cualquier caso, siempre es conveniente asegurarse que la antena está construida para funcionar en la banda de 2.4 GHz.

La mayoría de los puntos de acceso vienen equipados con una doble antena. Esta doble antena se utiliza para obtener diversidad en la recepción. Cada antena, aunque solo estén separadas unos centímetros, pueden recibir la señal en muy distintas condiciones en cada momento. El sistema elige la mejor de las señales en cada momento evitando muchos de los posibles problemas de mala recepción.

## II.5 CONECTORES Y CABLES DE ANTENA

Las antenas externas se conectan a los equipos Wi-Fi mediante un cable, el cual normalmente es del tipo coaxial, al cual se le colocan los conectores en ambos lados los cuales deben corresponder al tipo que incluyen la antena y el dispositivo inalámbrico.

Tanto el cable como cada conector, añaden pérdidas a la señal de radio. Para evitar estas pérdidas, se deben utilizar calves y conectores de calidad y procurar utilizar un cable lo más corto posible y únicamente el número de conectores imprescindibles (como evitar utilizar conectores para extender la longitud del cable o para adaptar tipos de cables o conectores).

### II.5.1 Conectores

Aún cuando la utilización de los conectores parece sencilla no lo es debido a que no existe una regulación que especifique como deben ser. Es por esto que existen muchos modelos distintos de conectores, algunos muy específicos y otros específicos de un fabricante. Este hecho se complica cuando utilizamos una antena que posee un conector distinto al del equipo inalámbrico.


*Fig. 2.18 Ejemplos de conectores*

Los tipos de conectores más comunes son:

- **N** *Navy* (marina). Es el conector más habitual en las antenas de 2.4 GHz Trabaja bien con frecuencias de hasta 10 GHz. Es un conector de tipo rosca, tienen un tamaño apreciable y suelen confundirse con los conectores de UHF.

- **BNC** *Bayonet Navy Connector* (conector tipo bayoneta de la marina). Es un conector utilizado en las redes Ethernet del tipo 10Base2. A pesar de ser muy común es poco apto para frecuencias de 2.4 GHz.

- **TNC** *Threaded BNC* (conector BNC roscado). Es una versión roscada del conector BNC. Este tipo de conector es apto para frecuencias de hasta 12 GHz.

- **SMA** *Sub-Miniature Connect* (conector subminiatura). Son unos conectores muy pequeños, son roscados y trabajan adecuadamente con frecuencias de hasta 18 GHz.

- **SMC** Son una versión todavía más pequeña de los conectores SMA. Son aptos para frecuencias de hasta 10 GHz, sin embargo solo pueden ser utilizados en cables muy finos (con alta pérdida).

- **APC-7** *Amphenol Precision Connector* (conector Amphenol de precisión). Se trata de un conector con muy poca pérdida y muy caro. Es fabricado por la empresa Amphenol.

## II.5.2 Cables

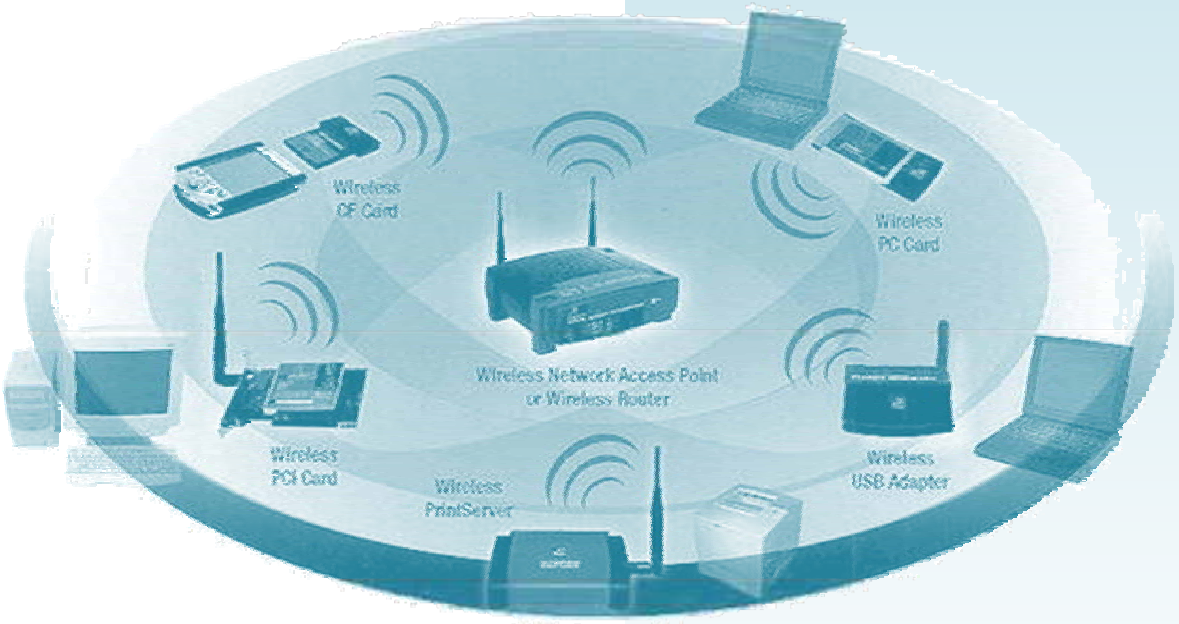
El cable es el elemento que se encarga de unir la antena al dispositivo inalámbrico, pero su función no es la de alejar a la antena del equipo ya que el cable introduce pérdidas en la señal que van desde los 0.05 a 1 dB por metro y su precio varía dependiendo de la calidad de este.

Por otro lado, el cable tiene soldado un conector en cada extremo. Como los conectores pueden encontrarse en cualquier tienda de electrónica, es posible soldarlos al cable, sin embargo es recomendable comprar el cable completo con los conectores puestos ya que si la soldadura no es aplicada correctamente, los resultados no serán favorables.

Al momento de adquirir el cable hay que asegurarse que esté fabricado para la frecuencia de 2.4 GHz, ya que un cable de televisión no es apropiado para Wi-Fi. Los cables más frecuentemente utilizados son los de tipo LMR y los de tipo Heliax. Estos cables introducen muy poca pérdida de señal pero a cambio su costo es mayor pudiendo costar hasta 100 pesos por metro.


*Fig. 2.19 Ejemplos de tipos de cable*

# Capitulo III
# ESTANDARES Y PROTECCION



## III.1 ETHERNET

Ethernet es el nombre de la tecnología de redes de computadoras de área local (LANs) más utilizada en la actualidad. Está basada en tramas de datos y su nombre proviene del concepto físico de éter. Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente en 1983, fue formalizada por el IEEE como el estándar Ethernet 802.3.

Ethernet define las características de cableado y señalización de la capa física y los formatos de trama de la capa de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque no se utilice éste.

A continuación se muestra el esquema de la trama utilizada por Ethernet, pudiendo observar los campos principales que la forman.

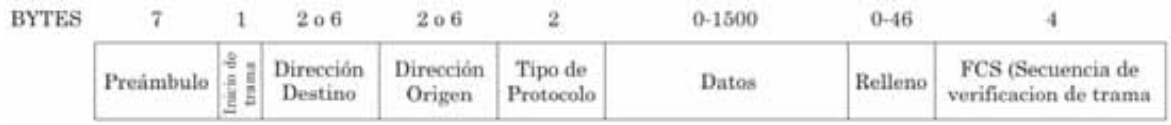



*Fig. 3.1 Trama Ethernet*

Las funciones de cada uno de los campos que componen la trama de Ethernet son las siguientes:

***Preámbulo***

Está formado por 7 bytes, con una secuencia de datos que permite estabilizar el medio físico y que el receptor pueda sincronizarse con el emisor de forma que pueda localizarse el principio de la trama. El patrón de preámbulo es:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

***Inicio de trama***

Es un byte que utiliza el patrón 10101011 para indicar al receptor el inicio de una trama. La trama se iniciará con el patrón de la dirección de destino.

***Dirección de destino***

Este campo contiene la dirección física, también conocida como dirección MAC del equipo destinatario de la trama. Estas direcciones son de 2 o 6 bytes (16 o 48 bits). De los 48 bits que forman la dirección MAC, los 24 últimos los asigna libremente el fabricante y sirven para identificar de forma univoca a las tarjetas, de esta manera nunca existirán dos tarjetas con la misma dirección física MAC. La dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.

***Dirección de origen***
Este campo de 2 o 6 bytes (16 o 48 bits) contiene la dirección MAC de la estación emisora de la trama y tiene un formato similar al de la dirección de destino. La estación que deba aceptar el paquete conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

***Tipo de protocolo***
Este campo está formado por 2 bytes que identifica el protocolo de red de alto nivel asociado con el paquete o, en su defecto, la longitud del campo de datos siendo la capa de enlace de datos la que interpreta este campo.

***Datos***
Contiene los datos que son transmitidos por la capa de enlace de datos. El tamaño máximo de este campo es de 1500 bytes de longitud. En caso de que el tamaño de este campo sea menor de 46 bytes se utilizará el siguiente campo (Relleno) para completar la trama.

***Relleno***
Este campo se utiliza para distinguir las tramas válidas de las inválidas. El tamaño mínimo que debe tener una trama para ser válida es de 64 bytes (incluye todos los campos). En caso de que se transmitan menos de 46 bytes en los datos, se utilizará el campo de relleno para que la trama tenga el tamaño necesario y no sea considerada una trama inválida.

***FCS (Frame Check Sequence – Secuencia de Verificación de Trama)***
Contiene un código de redundancia cíclica (CRC) de 32 bits (4 bytes) para detectar errores en la transmisión. El emisor calcula este CRC usando todo el contenido de la trama y el receptor lo recalcula y lo compara con el recibido a fin de verificar la integridad de la trama.

### III.1.1 Protocolo de acceso múltiple CSMA (Acceso Múltiple con Detección de Portadora - Carrier Sense Multiple Access)

Como su nombre lo indica se caracteriza por la detección de portadora. Consiste en que una máquina de la red, antes de transmitir, escucha el canal para saber si existe una portadora presente, si éste está libre la estación transmite, en caso contrario espera a que quede libre. Aún así puede suceder que dos o más estaciones intenten transmitir aproximadamente al mismo tiempo, en este caso se producirá una colisión: los datos de ambas transmisiones se interferirán y no se recibirán con éxito. Para solucionar esto, las estaciones aguardan una cantidad de tiempo razonable después de transmitir en espera de una confirmación, teniendo en consideración el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión y retransmite.

El método que utiliza CSMA es efectivo para redes en las que el tiempo de transmisión de trama es mucho mayor que el de propagación, ya que las colisiones solo se producirán en el caso de que más de un usuario comience a transmitir dentro del mismo intervalo de tiempo. Si una estación comienza a transmitir y no existen colisiones durante el tiempo de propagación, no se producirán colisiones para esta trama ya que todas las estaciones estarán enteradas de la transmisión.

## III.2 IEEE 802.11

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos.


*Fig. 3.2 Capas del modelo OSI que define el estándar IEEE 802.11*

### III.2.1 802.11

La versión original del estándar IEEE 802.11 fue publicada en 1997 y especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

Este estándar también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

## III.2.2 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. En algunos casos puede llegar a una velocidad de 22 Mbit/s cuando los fabricantes utilizan desdoblamiento de velocidad aún cuando no haya estandarización de IEEE. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

Aunque también utiliza una técnica de espectro ensanchado basada en DSSS, en realidad la extensión 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit). El estándar también admite el uso de PBCC (Packet Binary Convolutional Coding) como opcional. Los dispositivos 802.11b deben mantener la compatibilidad con el anterior equipamiento DSSS especificado a la norma original IEEE 802.11 con velocidades de bit de 1 y 2 Mbps.

Los identificadores de canales, frecuencias centrales, y dominios reguladores para cada canal usado por IEEE 802.11b se muestran en la tabla 3.1.

Tradicionalmente se utilizan los canales 1, 6 y 11, aunque se ha documentado que el uso de los canales 1, 5, 9 y 13 (en dominios europeos) no es perjudicial para el rendimiento de la red.

México está incluido en el dominio regulador de América, sin embargo los canales del 1 al 8 están reservados para uso de interiores mientras que de los canales 9 al 11 pueden ser utilizados tanto para interiores como para exteriores.

| Identificador de Canal | Frecuencia en MHz | Dominios Reguladores | | | | |
|---|---|---|---|---|---|---|
| | | América (-A) | EMEA (-E) | Israel (-I) | China (-C) | Japón (-J) |
| 1 | 2412 | × | × | — | × | × |
| 2 | 2417 | × | × | — | × | × |
| 3 | 2422 | × | × | × | × | × |
| 4 | 2427 | × | × | × | × | × |
| 5 | 2432 | × | × | × | × | × |
| 6 | 2437 | × | × | × | × | × |
| 7 | 2442 | × | × | × | × | × |
| 8 | 2447 | × | × | × | × | × |
| 9 | 2452 | × | × | × | × | × |
| 10 | 2457 | × | × | — | × | × |
| 11 | 2462 | × | × | — | × | × |
| 12 | 2467 | — | × | — | — | × |
| 13 | 2472 | — | × | — | — | × |
| 14 | 2484 | — | — | — | — | × |

*Tabla 3.1 Principales características de IEEE 802.11b*

## III.2.3 802.11a

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps.

En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b.

En 2001 hizo su aparición en el mercado los productos del estándar 802.11a.

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM (orthogonal frequency-division multiplexing) con una velocidad máxima de 54 Mbit/s (y en algunos casos hasta de 74 o 108 Mbps), lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de

aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto y puede soportar hasta 64 usuarios por punto de acceso. Su principal desventaja consiste en que no puede operar directamente con equipos del estándar 802.11b, a menos que se disponga de equipos que implementen ambos estándares.

Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso. Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

Los identificadores de canales, frecuencias centrales, y dominios reguladores para cada canal usado por IEEE 802.11a son:

| Identificador de Canal | Frecuencia en MHz | Dominios Reguladores | | | |
|---|---|---|---|---|---|
| | | América (-A) | EMEA (-E) | Israel (-I) | Japón (-J) |
| 34 | 5170 | — | × | — | — |
| 36 | 5180 | × | — | × | — |
| 38 | 5190 | — | × | — | — |
| 40 | 5200 | × | — | × | — |
| 42 | 5210 | — | × | — | — |
| 44 | 5220 | × | — | × | — |
| 46 | 5230 | — | × | — | — |
| 48 | 5240 | × | — | × | — |
| 52 | 5260 | × | — | — | × |
| 56 | 5280 | × | — | — | × |
| 60 | 5300 | × | — | — | × |
| 64 | 5320 | × | — | — | × |

*Tabla 3.2 Principales características de IEEE 802.11a*

## III.2.4 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélite

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ERC/DEC/(99)23).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

### Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

## III.2.5 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

## III.2.6 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input –

Multiple Output), el cual que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

| Estándar | Velocidad máxima | Interface de aire | Ancho de banda del canal | Frecuencia |
|---|---|---|---|---|
| 802.11b | 11 Mbps | DSSS | 25 MHz | 2.4 GHz |
| 802.11a | 54 Mbps | OFDM | 25 MHz | 5.0 GHz |
| 801.11g | 54 Mbps | OFDM/DSSS | 25 MHz | 2.4 GHz |
| HomeRF2 | 10 Mbps | FHSS | 5 MHz | 2.4 GHz |

*Tabla 3.3 Cuadro comparativo de estándares para redes inalámbricas*

DSSS: Direct Sequence Spread Spectrum
OFDM: Orthogonal Frequency Division Multiplexing
FHSS: Frequency Hopping Spread Spectrum

## III.3 TECNICAS DE MODULACIÓN

Las técnicas utilizadas para modular las señales inalámbricas se conocen como de “espectro ensanchado” y fueron desarrolladas para que los militares transmitan datos. Estas técnicas, consisten en utilizar una banda de frecuencia ancha para transmitir datos de baja potencia.

Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

1. Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.
2. Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.
3. Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

Existen 3 tipos de modulaciones de espectro ensanchado las cuales son:

1. Salto de Frecuencia (FHSS, Frecuency-Hopping Spread Spectrum)
2. Secuencia Directa (DSSS, Direct Sequence Spread Spectrum)
3. Multiplexación por División de Frecuencias Ortogonales (OFDM, Orthogonal Frequency Division Multiplexing)

### III.3.1 Salto de Frecuencia

Con esta técnica los dispositivos receptores y emisores se mueven sincrónicamente manteniendo un patrón predeterminado de forma que saltan de una frecuencia a otra al mismo tiempo y en intervalos de tiempo fijos. Las frecuencias utilizadas para los saltos y el orden de utilización se denominan **patrón de salto (hopping pattern)**. El tiempo de permanencia en cada frecuencia **(dwell time)** debe ser muy corto (menor que milisegundos) para evitar interferencias (tanto el *dwell time* como el *hopping pattern* están sujetos a restricciones por parte de los organismos de regulación). Este mecanismo, convenientemente sincronizado, actúa como si hubiera un único canal lógico: únicamente aquel receptor sincronizado con el transmisor y que tenga exactamente el mismo código de salto, podrá acceder a las frecuencias correspondientes y extraer la información. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits.

Esta técnica la utilizan los estándares Bluetooth y HomeRF.

### III.3.2 Secuencia Directa

En esta técnica, utilizada en el estándar IEEE 802.11b, la información a transmitir se mezcla con un patrón pseudoaleatorio de bits (a cada bit de código se le denomina chip) para extender los datos antes de que se transmitan (el funcionamiento consiste en desplazar la fase de una portadora mediante una secuencia de bits muy rápida), diseñada de forma que aparezcan aproximadamente el mismo número de ceros que de unos. Cuanto mayor sea la cantidad de chips en la señal, mayor será la resistencia de la esta a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En la 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 y puede ser de dos tipos, según sustituya al cero o al uno lógico; es decir, cada bit transmitido se modula por medio de la secuencia de bits de código patrón pseudoaleatorio de referencia. De esta manera, se extiende la energía de radiofrecuencia por un ancho de banda mayor que el necesario si se transmitiesen únicamente los datos originales. Al igual que con la otra técnica de modulación, únicamente aquel receptor al que se le haya enviado previamente la secuencia será capaz de regenerar la información original (aquellos que no posean el código, creerán que se trata de ruido). 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.

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, y para el estándar 802.11b 11Mbps, además de otras mejoras de seguridad.

Como vimos anteriormente, el estándar 802.11b tiene 14 canales separados por un rango de 25 MHz cada uno en frecuencias que van entre 2.412 y 2.484 GHz.

Estos canales son

Canal 01: 2.412 GHz Canal 02: 2.417 GHz Canal 03: 2.422 GHz Canal 04: 2.427 GHz Canal 05: 2.432 GHz Canal 06: 2.437 GHz Canal 07: 2.442 GHz Canal 08: 2.447 GHz Canal 09: 2.452 GHz Canal 10: 2.457 GHz Canal 11: 2.462 GHz Canal 12: 2.467 GHz Canal 13: 2.472 GHz Canal 14: 2.484 GHz

Para cada canal es necesario un ancho de banda de unos 22 MHz para poder transmitir la información, por lo que se produce un inevitable solapamiento de los canales próximos. Si tenemos que poner algunos puntos de acceso cercanos inevitablemente, debemos separarlos lo suficiente siendo recomendable usar canales que no se solapen. En el caso de América los canales recomendados son 1, 6 y 11.

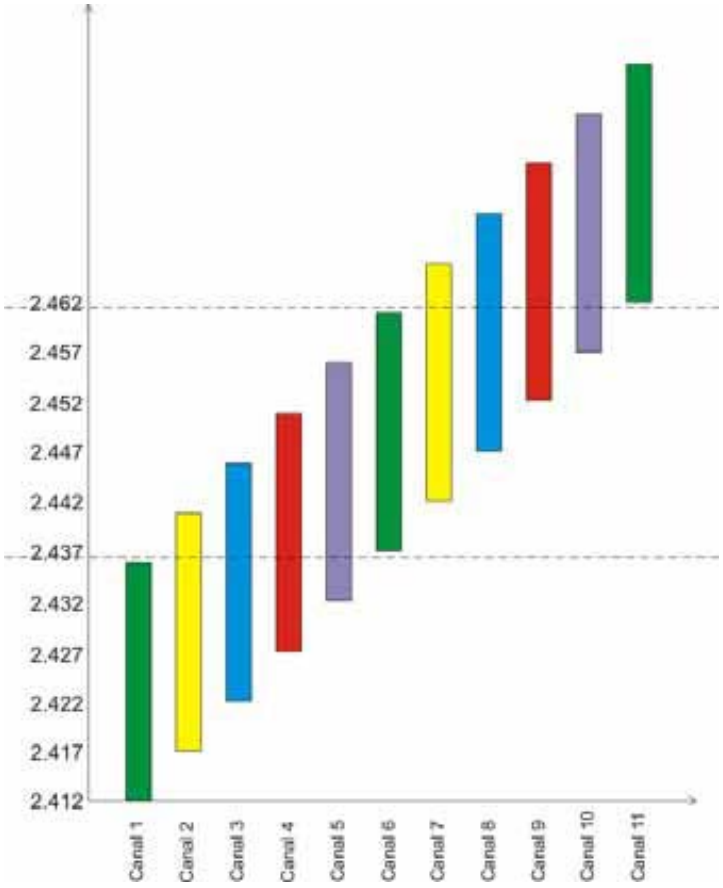



*Fig. 3.3 Ancho de banda en los canales del estándar 802.11b*

## III.3.3Multiplexación por División de Frecuencias Ortogonales

La Multiplexación por División de Frecuencias Ortogonales es una tecnología de modulación digital que trabaja en la banda libre del espectro radioeléctrico. Fue patentada por Bell Labs en 1970 y surge como alternativa para su uso en la red de tipo XDSL tanto de naturaleza alámbrica como inalámbrica, para poder cumplir con los nuevos requerimientos de ancho de banda, confiabilidad y seguridad de la próxima generación de productos y servicios principalmente en la radiofrecuencia de alta velocidad. Actualmente es utilizada en las redes inalámbricas 802.11a, 802.11g, en comunicaciones de alta velocidad por vía telefónica ADSL y en difusión de TV digital terrestre en Europa, Japón y Australia.

Consiste en enviar la información en un conjunto de portadoras de diferentes frecuencias moduladas en QAM o PSK. Ocupa un ancho de banda por canal de 20 MHz, en dicho canal existen 52 sub-portadoras ortogonales las cuales están separadas 312,5 KHz entre ellas y son moduladas digitalmente. Además, en el momento de enviar los símbolos se le agrega un intervalo de guarda el cual permite disminuir la interferencia por multitrayectoria (multi-path).

### *Características de la modulación OFDM*

La modulación OFDM es muy robusta frente al multitrayecto, que es muy habitual en los canales de radiodifusión, frente a las atenuaciones selectivas en frecuencia y frente a las interferencias de RF.

Debido a las características de esta modulación, es capaz de recuperar la información de entre las distintas señales con distintos retardos y amplitudes (fadding) que llegan al receptor, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFDM son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

### *Sistemas que utilizan la modulación OFDM*

Entre los sistemas que usan la modulación OFDM destacan:

La televisión digital terrestre DVB-T, también conocida como TDT

La radio digital DAB

La radio digital de baja frecuencia DRM

El protocolo de enlace ADSL

El protocolo de red de área local IEEE 802.11a/g, también conocido como Wireless LAN

El sistema de transmisión inalámbrica de datos WiMAX

## III.4 PROTOCOLOS DE SEGURIDAD WI-FI

La tecnología Wi-Fi es una de las tecnologías líder en la comunicación inalámbrica, y el soporte para Wi-Fi se está incorporando en cada vez más aparatos. Sin embargo, uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. En caso de instalar una red inalámbrica sin tener en consideración la seguridad, dicha red se convertirá en una red abierta y no existirá protección de la información que se envía y no podrá evitarse que usuarios no autorizados ingresen a la red.

En la actualidad existen tres protocolos de cifrado de datos para los estándares Wi-Fi. Estos protocolos son:

- WEP (Wired Equivalent Privacy, Privacidad Equivalente a Cableado)
- WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi)
- WPA2 (Wi-Fi Protected Access 2).

### III.4.1 WEP

La encriptación WEP es un tipo de cifrado, implementado en el protocolo de conexión IEEE 802.11, que se encarga de cifrar la información que se va a transmitir utilizando el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC de forma que un router Wi-Fi o un Access Point permitirá el acceso únicamente a aquellas terminales que tengan la misma clave de encriptación WEP.

Esta clave puede ser de tres tipos:

*Clave WEP de 64 bits*.-, 5 Caracteres o 10 dígitos hexadecimales (''0 a 9'' ''A a F'', precedidos por la cadena ''0x'').

*Clave WEP de 128 bits*.-, 13 Caracteres o 26 dígitos hexadecimales (''0 a 9'' ''A a F'', precedidos por la cadena ''0x'').

*Clave WEP de 256 bits*.-, 29 Caracteres o 58 dígitos hexadecimales (''0 a 9'' ''A a F'', precedidos por la cadena ''0x'').

La que más se suele usar es la de 128 bits, que ofrece un buen nivel de protección sin ser excesivamente larga y complicada, además de que la encriptación WEP de 256 bits no es soportada por muchos dispositivos.

#### III.4.1.1 Cifrado

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica el algoritmo CRC al texto en claro, lo que genera un *valor de comprobación de integridad* (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

### III.4.1.2 Algoritmo

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el tipo de clave utilizada, para ejemplificar esto utilizaremos el estándar de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Por lo tanto, ambos extremos deben conocer tanto la clave secreta como el IV.

#### *El algoritmo de encriptación de WEP*

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).

2. Se concatena la clave secreta a continuación del IV formado el *seed*.

3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed,* de la misma longitud que los bits obtenidos en el punto 1.

4. Se realiza una operación XOR con los caracteres del punto 1 y los del punto 3. El resultado es el mensaje cifrado.

5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

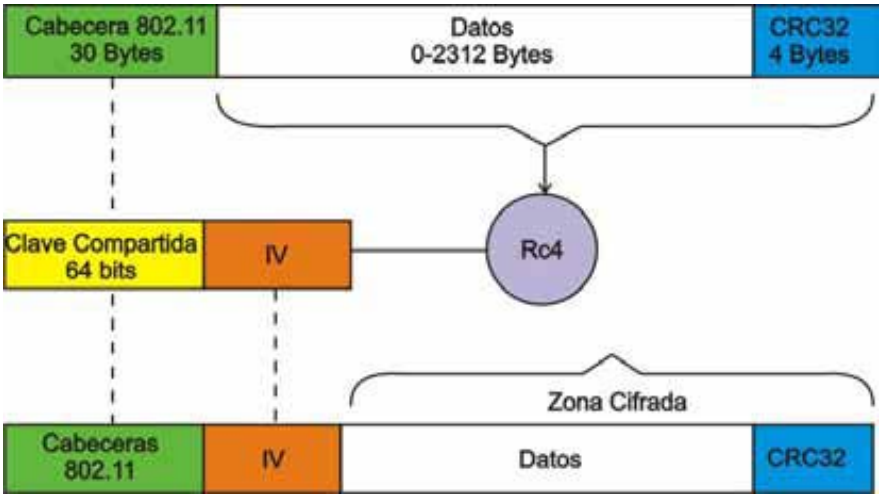



*Fig. 3.4 Algoritmo de Encriptación WEP*

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta tendrá el *seed* y con ello podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32), luego se comprueba que el CRC-32 es correcto.

### *Algoritmo de encriptación RC4*

Funciona a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

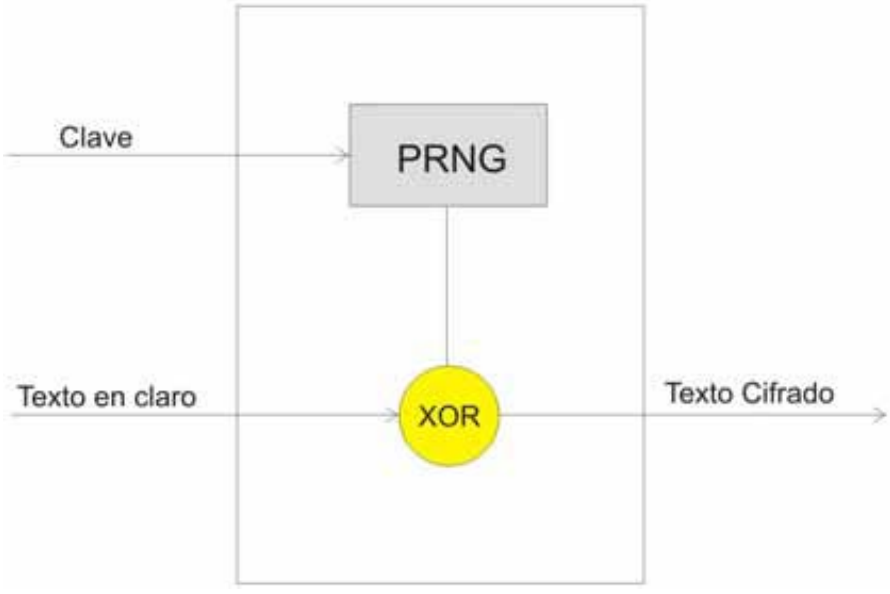



*Fig. 3.5 Cifrado del Algoritmo RC4*

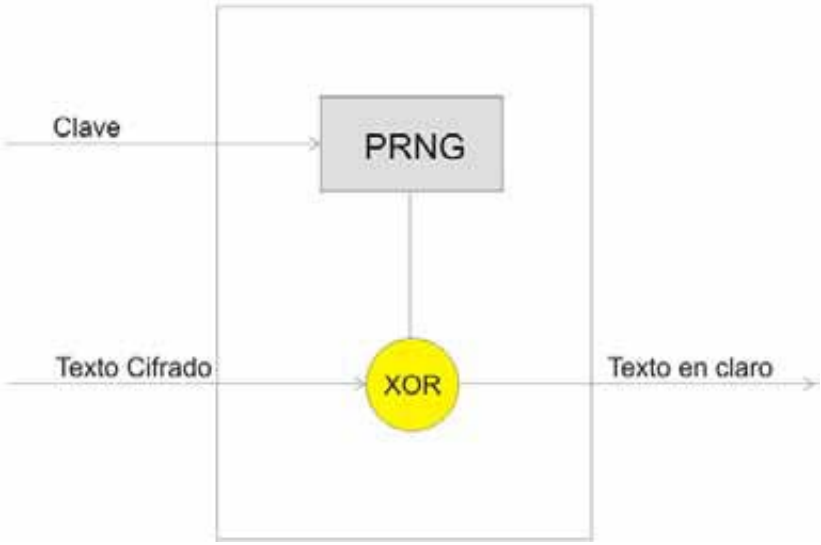



*Fig. 3.6 Descifrado del Algoritmo RC4*

Una clave de encriptación WEP se puede descifrar, pero para esto es necesario un tráfico ininterrumpido de datos durante un tiempo determinado (bastantes datos y bastante tiempo).

Evidentemente, cuanto mayor sea el nivel de encriptación y más complicada sea la clave más difícil será descifrarla.

A pesar de que es posible descifrar estas claves de encriptación, no es una tarea fácil ni rápida. Una buena clave de encriptación WEP de 128 bits (por no decir una de 256 bits) puede llegar a ser prácticamente indescifrable en caso de que sea lo suficientemente complicada.

### III.4.2 WPA

WPA es una clase de sistemas para el aseguramiento de redes inalámbricas, el cual fue creado en respuesta a las serias debilidades de otros protocolos como WEP. Implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todos los dispositivos para redes inalámbricas, excepto los puntos de acceso de primera generación.

WPA fue creado por el grupo industrial y comercial Alianza Wi-Fi, dueños de la marca registrada Wi-Fi y certificadores de los dispositivos que ostenten dicho nombre.

En la protección WPA los datos son cifrados utilizando el algoritmo RC4 con una clave dinámica TKIP (que se explicará más adelante) de 128 bits y un vector de inicialización de 48 bits, lo que significa que la clave está cambiando constantemente y esto hace que las incursiones en la red inalámbrica sean más difíciles que con una clave WEP.

Además de proporcionar autenticación y ciframiento, WPA proporciona mejor integridad de la carga útil. La verificación de redundancia cíclica (CRC o Cyclic Redundancy Check) utilizada en WEP es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de

redundancia cíclica sin necesidad de conocer la clave WEP. En cambio, en WPA se utiliza un Código de Integridad de Mensaje (MIC o Message Integrity Code) que es en realidad un algoritmo denominado "*Michael*", que fue el más fuerte que se pudo utilizar con los dispositivos antiguos para redes inalámbricas para no dejarlos obsoletos. El código MIC de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales.

WPA tiene dos modos de funcionamiento, uno de ellos está diseñado para uso empresarial o de negocios el cual es EAP. Su principal característica consiste en utilizar un servidor de autentificación 802.1X externo con protocolos EAP. Un ejemplo de esto es un servidor Radius.

Algunos de los protocolos utilizados son:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-LEAP

El otro modo de funcionamiento se refiere para uso doméstico y es conocido como PSK (Pre-Shared Key). En este caso no es necesario contar con el servidor de autentificación y solo se utilizará una contraseña para proporcionar la autentificación de un dispositivo que se quiera conectar a la red.

Para proteger la información, WPA utiliza dos tipos de protocolos que son conocidos como TKIP y AES de los cuales se hablará a continuación:

### III.4.2.1 TKIP

Como se mencionó anteriormente, el protocolo TKIP sustituye a WEP con un algoritmo de cifrado nuevo más seguro, sin embargo, maneja las utilidades de cálculo de los dispositivos inalámbricos existentes para realizar las operaciones de cifrado. TKIP también proporciona:

- La comprobación de la configuración de seguridad después de determinar las claves de cifrado.
- El cambio sincronizado de la clave de cifrado de unidifusión para cada marco.
- La determinación de una clave de inicio de cifrado de unidifusión exclusiva para cada autenticación de clave previamente compartida.

### *Michael*

Con 802.11 y WEP, se proporciona la integridad de datos con un valor de comprobación de integridad (ICV) de 32 bits que se anexa a la carga 802.11 y se cifra con WEP. Aunque el valor ICV se cifra, puede utilizar el análisis de cifrado para cambiar los bits en la carga útil cifrada y actualizar el valor ICV cifrado sin ser detectado por el receptor.

Con WPA, un método conocido como Michael especifica un nuevo algoritmo que calcula un código de integridad de mensaje (MIC) de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos existentes. El código MIC se coloca entre la parte de datos del marco IEEE 802.11 y el valor ICV de 4 bytes. El campo MIC se cifra junto con los datos del marco y los de ICV.

Michael también ayuda a proporcionar protección de reproducción, además de utilizar un nuevo contador de marco para evitar los ataques a este.

### III.4.2.2 AES

Es el otro tipo de encriptación utilizada en WPA, también es conocido como Rijndael.

AES opera en una matriz de 4×4 de bytes, llamada *state*. Para el cifrado, cada ronda de la aplicación del algoritmo AES (excepto la última) consiste en cuatro pasos:

SubBytes. - En esta etapa, cada byte en la matriz es actualizado usando la caja-S de Rijndael de 8 bits. Esta operación provee la no linealidad en el cifrado. Para evitar ataques basados en simples propiedades algebraicas, la caja-S se construye por la combinación de la función inversa con una transformación afín inversible. La caja-S también se elige para evitar puntos estables y también cualesquiera puntos estables opuestos.

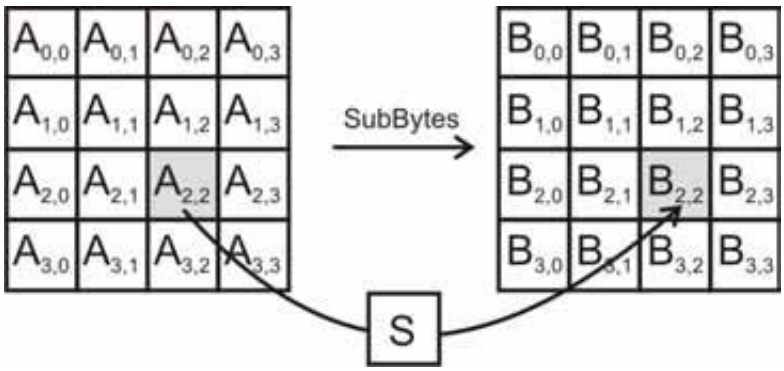



*Fig. 3.7 Etapa SubBytes*

ShiftRows. - Esta etapa rota de manera cíclica los bytes en cada fila por un determinado offset. En AES, la primera fila queda en la misma posición. Cada byte de la segunda fila es rotado una posición a la izquierda. De manera similar, la tercera y cuarta filas son rotadas por los offsets de dos y tres respectivamente. De esta manera, cada columna del state resultante del paso ShiftRows está compuesta por bytes de cada columna del state inicial.

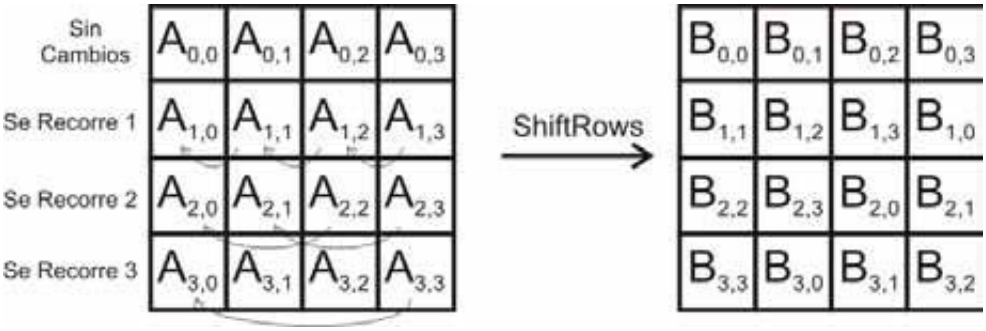



*Fig. 3.8 Etapa ShiftRows*

MixColumns —En este paso los cuatro bytes de cada columna de estado se combinan usando una transformación lineal invertible. De este modo, la función toma cuatro bytes como entrada y devuelve cuatro bytes, donde cada byte de entrada influye todas las salidas de cuatro bytes. Junto con ShiftRows, MixColumns implica difusión en el cifrado.

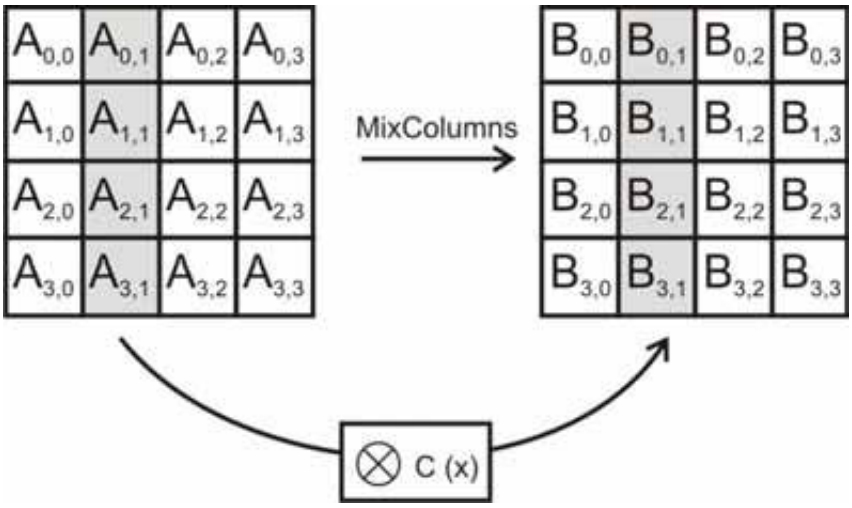



*Fig. 3.9 Etapa MixColumns*

AddRoundKey.- En el paso AddRoundKey, la subclave se combina con el state. En cada ronda se obtiene una subclave de la clave principal, usando la iteración de la clave; cada subclave es del mismo tamaño del state. La subclave se agrega combinando cada byte del state con el correspondiente byte de la subclave usando XOR.

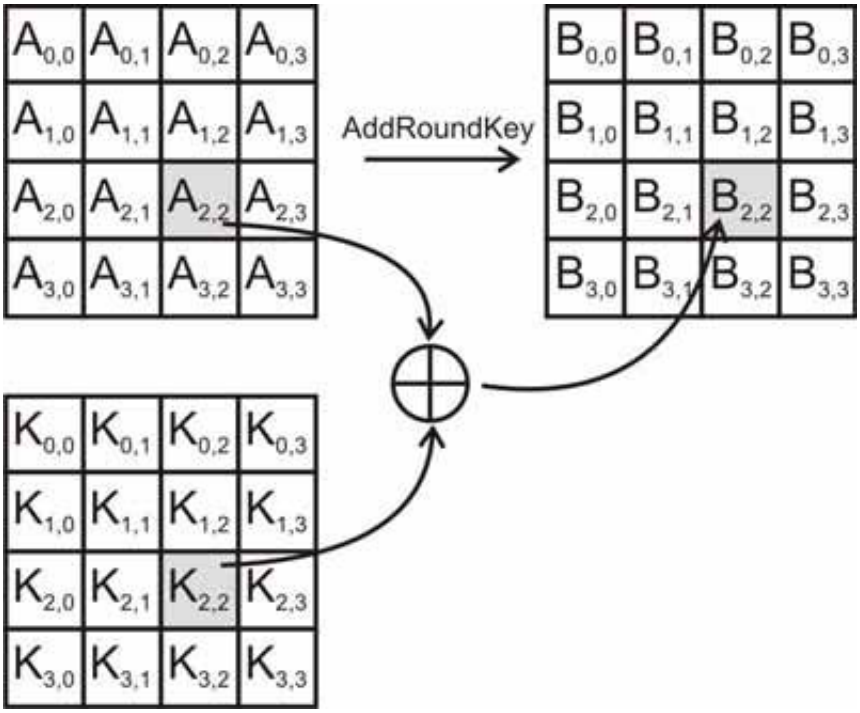



*Fig. 3.10 Etapa AddRoundKey*

En sistemas de 32 bits o de mayor tamaño de palabra, es posible acelerar la ejecución de este algoritmo mediante la conversión de las transformaciones SubBytes, ShiftRows y MixColumn en tablas. Se tienen cuatro tablas de 256 entradas de 32 bits que utilizan un total de 4 kilobytes (4096 bytes) de memoria, un Kb cada tabla. De esta manera, una ronda del algoritmo consiste en 16 búsquedas en una tabla seguida de 16 operaciones XOR de 32 bits en el paso AddRoundKey. Si el tamaño de 4 kilobytes de la tabla es demasiado grande para una plataforma determinada, la operación de búsqueda en la tabla se puede realizar mediante una sola tabla de 256 entradas de 32 bits mediante el uso de rotaciones circulares.

Es por esto que WPA está considerado como uno de los más altos niveles de seguridad para una red inalámbrica, sin embargo es recomendable que en las claves se inserten dígitos alfanuméricos, caracteres especiales, números, letras mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas y evitar claves con información personal para brindar una protección mayor a la red.

### III.4.3 WPA2

WPA2 es la segunda generación de WPA y está actualmente disponible en los dispositivos inalámbricos más modernos del mercado. Mientras que WPA fue definido por Wi-Fi Alliance, WPA2 está estandarizado por IEEE en la norma 802.11i.

La principal diferencia de WPA2 consiste en que se reemplazó el código de autenticación (Michael) por el código CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) y RC4 es sustituido por AES como algoritmo de cifrado. Al igual que WPA, WPA2 se divide en uso doméstico y uso empresarial.

## III.5 VPN

Una red VPN (Virtual Private Network, Red Privada Virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública y sirve para transmitir datos de manera segura por una red que es de naturaleza no segura, como por ejemplo Internet.

Una vez establecida la conexión de la red privada virtual los datos viajan encriptados de forma que sólo el emisor y el receptor son capaces de leerlos.

Para poder realizar una VPN se necesita un servidor (o host) que espera conexiones entrantes, y uno o varios clientes, que se conectan al servidor para formar la red privada.

Una VPN sirve para transmitir datos de manera segura por una red que, de por sí, es de naturaleza no segura. Sin embargo esta práctica ha adquirido popularidad debido a que en lugar de alquilar líneas de datos privadas para conectar los equipos, se puede utilizar Internet para realizar las comunicaciones privadas. Significa también que los usuarios corporativos que estén de viaje, o en sus domicilios, pueden conectarse con un Proveedor de Servicios de Internet y comunicarse de manera segura con la red corporativa sin necesidad de conectarse mediante una línea específica.

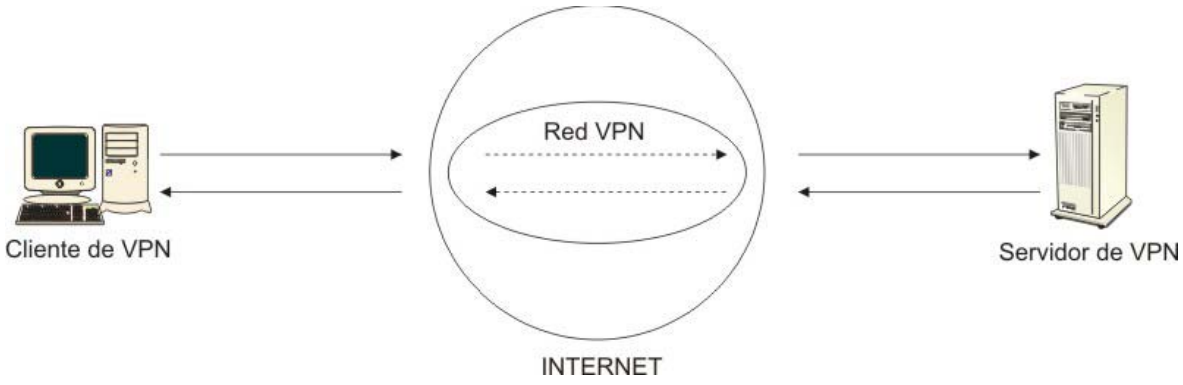



*Fig. 3.11 Ejemplo de una red VPN*

La principal ventaja de las redes privadas virtuales es la reducción del coste y la mejora de la privacidad. Las compañías pueden reducir sus costes de conexión manteniendo un único acceso WAN para cada oficina remota, mediante una única conexión a un ISP y éste reenviará el tráfico por la Internet pública.

Obviamente deben existir mecanismos que aseguren la confidencialidad de las comunicaciones. Las nuevas tecnologías utilizadas en estas redes, y que han sido desarrolladas recientemente, aseguran que los datos no se pueden leer ni modificar en su trayecto hacia la red de destino. Aunque las distintas tecnologías de VPN poseen algunas características diferentes, comparten muchos elementos comunes. Todas las VPN transportan datos a través de un *túnel*. Este túnel se crea entre dos extremos, entre dos servidores VPN o desde un cliente y un servidor VPN. Este proceso se muestra en la siguiente figura:

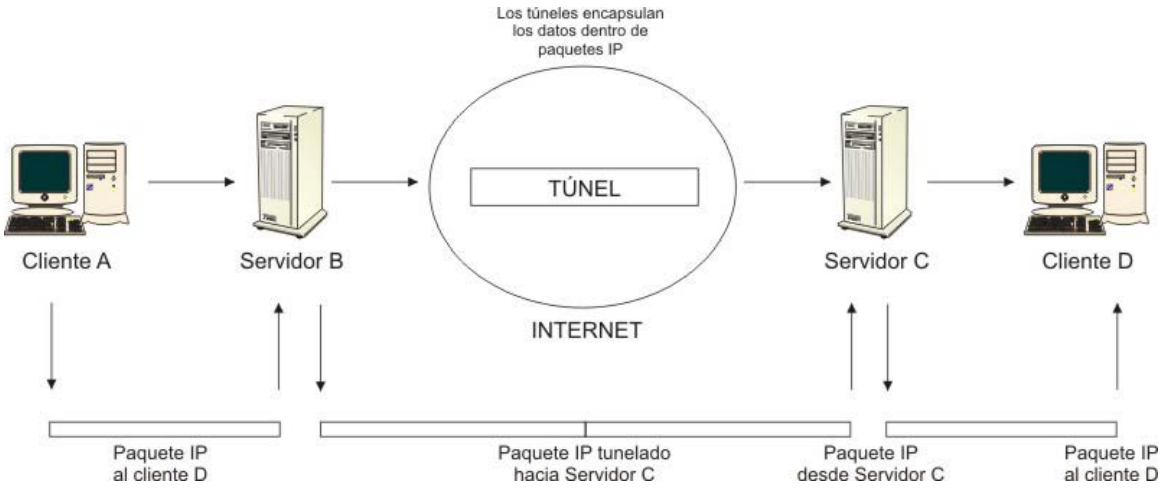



*Fig. 3.12 Proceso de envío de paquetes de una red VPN*

El túnel se crea entre dos extremos, entre dos servidores VPN o entre un cliente y un servidor VPN, los cuales se ponen de acuerdo en los protocolos de túnel a utilizar antes de empezar a transmitir datos. Cuando se envían los datos por el túnel, la trama o paquete se encapsula dentro de otro paquete que ofrece funciones de seguridad e integridad del contenido. Una vez que los datos llegan al extremo opuesto, se extraen los datos útiles de estos paquetes y se procesan como si se hubiesen recibido directamente desde la misma red de área local.

Las tres tecnologías que debemos considerar para crear redes privadas virtuales están basadas en la utilización de los siguientes protocolos:

***PPTP (Point-to-Point Tunneling Protocol)***: Este protocolo diseñado por Microsoft de creación de túnel Punto a Punto, es una tecnología que permite crear un enlace virtual entre redes públicas y privadas y recoge los mecanismos de autentificación y negociación de enlace.

PPTP encapsula los paquetes PPP usando una versión modificada del encapsulado genérico de ruteo (Generic Routing Encapsulation GRE), lo que le da la flexibilidad de manejo de otros protocolos como: intercambio de paquetes de Internet (IPX) y la interfaz gráfica de sistema básico de entrada / salida de red NetBEUI. PPTP está diseñado para correr en la capa 2 del modelo OSI o en la capa de enlace de datos. Al soportar comunicaciones en la capa 2, se permite transmitir protocolos distintos a los IP sobre los túneles. Una desventaja de este protocolo es que no provee una fuerte encriptación para proteger la información.

***L2TP: (Layer 2 Tunneling Protocol)***. El Protocolo de Túnel de la Capa 2, al igual que el protocolo de túnel punto a punto (PPTP), este protocolo se puede utilizar para proporcionar seguridad a conexiones Internet de extremo a extremo del túnel, mediante otras tecnologías de acceso remoto, como el acceso a Internet que proporciona DSL.

Al contrario que PPTP, L2TP no depende de las tecnologías de cifrado específicas del fabricante para ofrecer una implementación completamente segura y correcta. Por ello, es probable que se convierta en el estándar de las conexiones de redes privadas virtuales seguras a través de Internet.

***IPSec (Internet Protocol Security)***. Es el futuro de la tecnología de túnel. Aunque IPSec todavía está en fase de desarrollo, los nuevos sistemas operativos de Windows proporcionan gran parte de las funcionalidades requeridas y/o publicadas.

IPSec se encarga de autentificar los equipos y cifrar los datos para su transmisión entre hosts, ya sea entre estaciones de trabajo y servidores o entre servidores. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

Además de estas tecnologías, existen otras alternativas para mejorar la seguridad de las redes inalámbricas. Las más comunes son:

Utilizar un filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.

Ocultar el punto de acceso, de manera que sea invisible a otros usuarios.

## III.6 PROTOCOLO INTERNET

El protocolo Internet (IP) es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión entre redes más utilizado. Como son cualquier protocolo estándar, IP se especifica en dos partes:

- La interfaz con la capa superior (por ejemplo, TCP), especificando los servicios que proporciona IP.
- El formato real del protocolo y mecanismos asociados.

La principal función del protocolo es encaminar los paquetes de datos desde un punto de la red hasta otro a través de las conexiones de red disponibles. Estas unidades de información se denominan paquetes IP o datagramas.

Las funciones básicas que implementa el protocolo IP son:

- *Direccionamiento*

Se encarga de proporcionar un conjunto global de direcciones que permitan identificar de forma unívoca a cada una de las máquinas conectadas a Internet.

Estas direcciones se conocen con el nombre de *direcciones IP* y no deben ser confundidas con las direcciones físicas o MAC empleadas en la subcapa de control de acceso al medio en las redes de área local.

- *Encaminamiento*

El protocolo IP debe proporcionar mecanismos que permitan a las estaciones y routers de Internet encaminar los datagramas en función del destino a alcanzar. Para poder realizar esta función los datagramas que se transmiten por la red incluyen las direcciones IP de las estaciones origen y destino.

- *Fragmentación*

Cuando un datagrama se envía por la red, el protocolo IP debe encargarse, en caso de ser necesario, de dividir el paquete en fragmentos de un tamaño aceptable para cada una de las redes que atraviesa. En el destino, el protocolo IP debe ser capaz de reensamblar los distintos fragmentos recibidos que conforman el datagrama original.

Una parte sustancial del protocolo IP es, sin duda alguna, el formato del datagrama del protocolo. Un datagrama IP está formado por una cabecera IP y un campo de datos. La cabecera tiene un tamaño mínimo de 20 bytes y está formada por palabras de 32 bits (4 bytes). La cabecera tendrá, por tanto, un tamaño mínimo de 5 palabras de 32 bits (20 bytes)

El formato de un datagrama IP y las características de los campos se muestra a continuación:

<table>
<tr><td>Versión</td><td>IHL</td><td>Tipo de servicio</td><td colspan="2">Longitud total del datagrama</td></tr>
<tr><td colspan="3">Identificación</td><td>Indicadores</td><td>Desplazamiento del fragmento</td></tr>
<tr><td colspan="2">Tiempo de vida</td><td>Protocolo</td><td colspan="2">Código de redundancia de cabecera</td></tr>
<tr><td colspan="5">Dirección IP origen</td></tr>
<tr><td colspan="5">Dirección IP destino</td></tr>
<tr><td colspan="5">Opciones (0 ó más palabras)</td></tr>
<tr><td colspan="5">DATOS</td></tr>
</table>

*Fig. 3.13 Datagrama IP*

**Versión (4 bits)**: Codifica la versión del protocolo al que pertenece el datagrama. En la actualidad se utiliza ampliamente la versión 4, aunque la versión 6 con sus variantes empieza a utilizarse.

**Longitud de la cabecera Internet (IHL - Internet Header Length) (4 bits)**: Indica la longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de 5 bytes; en este caso no se utilizará el campo opciones. Su valor máximo es de 15 bytes, cosa que limita la cabecera de 60 bytes y, por tanto, el campo de opciones a 40 bytes.

**Tipo de servicio (8 bits):** Permite especificar determinados parámetros de calidad de servicio, como son la prioridad del datagrama, la rapidez de la entrega, el rendimiento, la seguridad de la entrega, etc. La mayoría de los routers comerciales no son capaces de procesar esta información. Por este motivo, en la práctica los routers disponibles ignoran por completo estos parámetros.

**Longitud total del datagrama (16 bits):** Representa la longitud total del datagrama en número de bytes incluyendo la cabecera y el campo de datos.

**Identificación (16 bits):** Este campo se emplea en el caso de que se utilice la fragmentación de los datagramas. Todos los fragmentos procedentes de un datagrama contendrán el mismo valor de identificación.

**Indicadores (3 bits):** Está formado por 3 bits de los cuales el primero es un bit no utilizado:

*DF (Don't Fragment) (segundo bit)*

Se emplea para indicar a los routers que no fragmenten el datagrama, puesto que en el destino no existe la posibilidad de volverlos a juntar

*MF (More Fragments) (tercer bit)*

Todos los fragmentos generados excepto el último tienen establecido este bit, siendo necesario para saber cuando han llegado todos los fragmentos del datagrama.

**Desplazamiento del fragmento (13 bits):** Indica la posición que ocupa el fragmento dentro del datagrama original. Este campo contiene la distancia, medida en bloques de 8 bytes, desde el inicio del fragmento hasta el inicio del datagrama original. Todos los fragmentos, excepto el último del datagrama, deben tener un número entero de bloques. El número máximo de fragmentos es de 8192 por datagrama.

**Tiempo de vida (8 bits):** Este campo contiene un contador que sirve para restringir la vida de un paquete en la red. Normalmente representa el número máximo de saltos que puede llevar a cabo el datagrama circulando en la red. Cada vez que el datagrama pasa por un router, éste le presta una unidad al tiempo de vida contenido en este campo. Si el campo llegara a ser cero, el router descartaría el datagrama.

**Protocolo (8bits):** Identifica al protocolo de la capa superior al que pertenecen los datos. La capa IP se comunica básicamente con dos tipos de protocolos: el protocolo TCP (campo de protocolo = 6) y el protocolo UDP (campo de protocolo = 17).

**Código de redundancia de cabecera (16 bits):** Este campo de *checksum* o *suma de comprobación* se emplea para verificar únicamente la integridad de la cabecera. Es importante que la cabecera sea interpretada correctamente por los routers de la red, para evitar errores en el encaminamiento de los datagramas. Este campo se calcula realizando la operación lógica O-Exclusiva (XOR) de todas las palabras de 16 bits que forman la cabecera.

**Direcciones de origen y destino (32 bits $^{c}/_{u}$):** Estas direcciones identifican a la estación emisora y receptora del datagrama. Como decíamos, cada máquina conectada a Internet debe poseer una dirección IP única en la red. Cada campo de la cabecera correspondiente a estas direcciones ocupa una palabra de 32 bits.

**Opciones (variable):** El campo opciones incluye información adicional y opcional del datagrama. No todos los routers están configurados para permitir estas funcionalidades. Suele contener los siguientes tipos de información:

- *Encaminamiento de origen*. En este caso se puede indicar en el campo la ruta que debe seguir un datagrama.
- *Registro de ruta*. Se puede registrar en este campo la ruta que ha seguido el datagrama, es decir, las direcciones de los routers por los que ha pasado el datagrama.
- *Marca de tiempo*. En este campo se pueden registrar los instantes temporales en los que el datagrama ha atravesado los routers de la red y, adicionalmente, las direcciones IP de estos routers.

Este campo también se emplea para completar palabras de cuatro bytes, puesto que la cabecera debe tener un número entero de palabras múltiplo de 32 bits. Conformarían lo que denominamos *bytes de relleno.*

**Datos (variable):** el campo de datos debe tener una longitud múltiplo de 8 bits. La máxima longitud de un datagrama (campo de datos más cabecera) es de 65.535 bytes.

## III.7 PROTOCOLO INTERNET VERSION 6

IPv6 es la siguiente generación de protocolos diseñado por el IETF (Internet Engineering Task Force) grupo de trabajo de ingeniería de Internet para reemplazar a la versión actual del protocolo de internet, IPv4.

El IETF comenzó a trabajar en 1990 en una nueva versión del protocolo IP. Esta versión debía resolver las limitaciones en el direccionamiento y ser más flexible y eficiente.

Los objetivos del IPv6 son los siguientes:

- Posibilidad de disponer miles de millones de direcciones para hosts
- Reducción del tamaño de las tablas de encaminamiento
- Simplificar el protocolo, para permitir a los routers el procesamiento más rápido de los paquetes.
- Proporcionar mayor seguridad que en el protocolo IP actual (verificación de autenticidad y confidencialidad)
- Permite el transporte de cualquier tipo de tráfico, especialmente aquellos correspondientes a servicios de tiempo real.
- Introducción de mecanismos de multitransmisión más flexibles.
- Posibilitar que un host cambie su ubicación física sin cambiar su dirección de red (*IP móvil)*
- Permitir que el protocolo evolucione
- Coexistencia de los protocolos IPv4 e IPv6

El IPv6 cumple perfectamente todos los objetivos planteados: mantiene las características del IP, descartando aquellas que son ineficientes y agregando nuevas funciones allí donde es necesario. En general IPv6 no es compatible con IPv4 pero sí lo es con todos los demás protocolos Internet, incluidos TCP, UDP, ICMP, IGMP, OSPF, DNS, etc., en ocasiones requiriendo pequeñas modificaciones.

Las Características principales del protocolo IP versión 6 son:

- El campo de direcciones en IPv6 es de 128 bits (16 bytes) de longitud, permitiendo diferenciar teóricamente hasta $3.40x10^{38}$ hosts ($2^{128}$), proporcionando una cantidad prácticamente ilimitada de direcciones de Internet.
- Simplificación de la cabecera, puesto que contiene solo 8 campos, en lugar de los 13 del IPv4. Esto permite a los routers procesar con mayor rapidez los paquetes y mejorar, por tanto, el rendimiento.
- Mayor eficiencia en el uso de los campos en la cabecera del paquete. Este cambio fue esencial, pues algunos campos que antes eran obligatorios ahora son opcionales. Además, la representación de las opciones es diferente, haciendo más sencillo que los routers hagan caso omiso de opciones no dirigidas a ellos. Esta característica mejora el tiempo de procesamiento de los paquetes.

- El protocolo IPv6 representa un gran avance en cuanto a la seguridad. Las verificaciones de autenticidad y la confidencialidad son características básicas de este nuevo protocolo IP, para disuadir a intrusos.
- El IPv6 permite canalizar de forma más eficiente el tráfico de datos multimedia.

<table>
<tr><td>Versión</td><td>Prioridad</td><td colspan="3">Etiqueta de flujo</td></tr>
<tr><td colspan="3">Longitud de carga útil</td><td>Siguiente cabecera</td><td>Límite de saltos</td></tr>
<tr><td colspan="5">Dirección origen<br>(16 bytes, 128 bits)</td></tr>
<tr><td colspan="5">Dirección destino<br>(16 bytes, 128 bits)</td></tr>
<tr><td colspan="5">DATOS</td></tr>
</table>

*Fig. 3.14 Datagrama IP versión 6*

El campo *versión* (4bits) identifica el número del protocolo. Este protocolo permite definir prioridades en los datagramas mediante el campo *prioridad* (4bits), para poder descartar aquellos paquetes con menor prioridad, en el caso de que haya congestión en la red. Mediante la *etiqueta de flujo* (16 bits) es posible definir varios flujos sobre una corriente de paquetes IP, de manera que pueden ser diferenciados paquetes con distintos requerimientos procedentes de una misma fuente. El campo *longitud de carga útil* (16 bits) identifica el número de bytes en el *campo de datos*. El campo *siguiente cabecera* (8 bits) permite introducir un campo adicional de *opciones*. Se han definido seis tipos de cabeceras de extensión de IPv6. En este campo se codificará el tipo de cabecera de extensión opcional a utilizar. El campo *límite de saltos* (8 bits) limita la vida de un paquete en la red; desempeña el mismo papel que el campo tiempo de vida del paquete IP versión 4.

## III.8 DIRECCIONES IP

Una dirección IP se utiliza para identificar de manera única e inequívoca a un equipo en la red, mediante la utilización de un formato simple de direcciones de 32 bits. Este formato de direcciones, emplea cuatro octetos, es decir 4 bytes de ocho bits separados por puntos, por lo que podemos encontrar direcciones entre 0.0.0.0 y 255.255.255.255. Una parte de la dirección identifica a la red y la otra parte identifica a la máquina dentro de dicha red. La parte de la dirección IP que identifica a la red en Internet siempre es fija, siendo necesario contratarla a la organización ICANN (Internet Corporation of Assigned Names and Numbers). Este organismo gestiona a escala mundial la asignación de direcciones IP en internet. La parte que identifica a cada estación dentro de la red, puede asignarla libremente el administrador de red para cada una de estas estaciones. En entornos de redes de área local se debe disponer de un ámbito de direcciones suficiente para diferenciar a los host en la red.

Cada host y cada router de Internet poseen al menos una dirección IP, que identifica su número de red y su número de host. La combinación es única, por tanto, no existirán dos máquinas que tengan la misma dirección IP. Todas las direcciones IP son de 32 bits de longitud y se usan en los campos de dirección origen y dirección destino de los datagramas IP. Aquellas máquinas conectadas a varias redes tienen direcciones IP diferentes en cada red, como el caso de los routers.

Se han definido cinco clases de direcciones IP que se diferencian entre sí por identificar con más o menos bits tanto a la red como a los host de la misma. En la práctica las direcciones A, B y C son las que más se utilizan. Podemos hablar igualmente de redes A, B o C en función de la clase de direcciones que se empleen. En la actualidad, las direcciones de clase A se reservan para los gobiernos de todo el mundo, aunque en el pasado se le hayan otorgado a empresas de gran magnitud y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de red permite una cantidad fija de equipos (hosts).

| Clase | Dirección IP (R=Red H=Host) | Rango de direcciones para Host | N° de Redes | N° de Host | Máscara de Red |
|---|---|---|---|---|---|
| A | 0RRRRRRR.HHHHHHHH. HHHHHHHH.HHHHHHHH | 1.0.0.0 - 127.255.255.255 | 126 | 16.777.214 | 255.0.0.0 |
| B | 10RRRRRR.RRRRRRRR. HHHHHHHH.HHHHHHHH | 128.0.0.0 - 191.255.255.255 | 16.384 | 65.534 | 255.255.0.0 |
| C | 110RRRRR.RRRRRRRR. RRRRRRRR.HHHHHHHH | 192.0.0.0 - 223.255.255.255 | 2.097.152 | 254 | 255.255.255.0 |
| D | 1110[ Dirección de multicast ] | 224.0.0.0 - 239.255.255.255 | | | |
| E | 1111[Reservado para uso futuro] | 240.0.0.0 - 255.255.255.255 | | | |

*Tabla 3.4 Formato y clases de direcciones IP*

**Direcciones Clase A**

En una red de clase A, se asigna el primer octeto para identificar la red, el primer bit es “0” y los otros 7 son asignados por la ICANN. Los tres octetos restantes están reservados para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es de 16’777,214 hosts.

**Direcciones Clase B**

En una red de clase B, se asignan los dos primeros bytes para identificar la red, los 2 primeros bits siempre son “10” y los 14 restantes son asignados por la ICANN. Los octetos restantes se utilizarán para asignarlos a los host. Puesto que son 14 bits para codificar la red, se pueden diferenciar hasta 16,384 redes con 65,534 hosts en cada una.

Muchas direcciones del espacio de direcciones de clase B se han dividido y reasignado en grupos más pequeños de direcciones. Los Proveedores de Servicios de Internet o ISP (Internet Service Providers), utilizan esta técnica para utilizar de forma más eficiente el espacio de direcciones disponible.

**Direcciones Clase C**

Con las direcciones clase C es posible identificar hasta 2'097,152 redes con 254 estaciones cada una, esto debido a que las direcciones que acaban en 0 o 255 están reservadas para otros usos. En una red clase C, se asignan los tres primeros octetos para identificar la red, los tres primeros bytes son "110" y el resto es nuevamente asignado por la ICANN, reservando el octeto final (8 bits) para que sea asignado a los hosts.

Estas redes son las que se suelen emplear en las PYME (Pequeñas Y Medianas Empresas) o en pequeñas organizaciones, puesto que en la mayoría de los casos no se requieren más de 254 direcciones IP.

**Direcciones clase D y E**

Las direcciones clase D también son denominadas *multicast*, multitransmisión o direcciones de grupo. Estas permiten realizar transmisiones a un grupo de usuarios distribuidos por internet. Cuando se envía un paquete IP a una dirección multicast, éste será recibido por todas las estaciones que conforman dicho grupo. El primer byte de estas direcciones puede tomar un valor comprendido entre 224 y 239.

Las direcciones clase E están reservadas para uso futuro o experimental. El primer byte de estas direcciones puede tomar un valor comprendido entre 240 y 247.

A pesar de esto es posible para varios equipos acceder a los servicios de internet a través de una única conexión, utilizando únicamente una dirección de Internet válida. El equipo de acceso actuará como ***servidor proxy***, pudiendo ser un router, un servidor o un equipo específico.

Los distintos equipos que conforman la red se configurarán con unas direcciones especiales. Estas direcciones reservadas pueden asignarse dentro de la red privada, porque son convertidas en el equipo proxy (router de acceso). Estas direcciones especiales, definidas en la RFC 1918, son mostradas en la siguiente tabla:

| TIPO DE RED | NUMERO DE REDES | DIRECCIONES CONTENIDAS |
|---|---|---|
| A | 1 | 10.0.0.0 a 10.255.255.255 |
| B | 16 | 172.16.0.0 a 172.31.255.255 |
| C | 256 | 192.168.0.0 a 192.168.255.255 |

*Tabla 3.5 Direcciones privadas IP*

Desde Internet solo será visible la dirección IP real del equipo que se conecte, ya sea un router o una PC con el software adecuado. Dentro de la subred a la que está conectada ese equipo, las máquinas tendrán direcciones "ficticias", "privadas" o "falsas". Por ejemplo, una empresa puede conectarse a Internet mediante un router ADSL que permita acceder a los recursos de Internet a un número reducido de ordenadores. En una pequeña subred con seis equipos, se podrá emplear el ámbito de direcciones comprendido entre la dirección 192.168.9.5 y 192.168.9.10.

## III.8.1 Direcciones IP especiales.

Existen un conjunto de direcciones especiales que no se asignan a ninguna máquina de Internet en concreto. Estas direcciones son:

*Direcciones de loopback o bucle cerrado*

Son direcciones del tipo 127.x.x.x y no están asignadas a ninguna red en particular. Estas direcciones se utilizan para permitir a una máquina aislada, ejecutar aplicaciones de red y hacer pruebas de retroalimentación.

*Direcciones de broadcast o difusión*

Estas direcciones se emplean para enviar paquetes de red a todas las máquinas que conforman dicha subred. Puesto que existen redes de clase A, B y C, encontraremos varios formatos de direcciones de broadcast. Las redes de clase A tienen el formato x.255.255.255. Las de clase B poseen un formato x.x.255.255. Por último, el formato de las direcciones de la clase C es x.x.x.255.

Si deseamos enviar un paquete a todas las máquinas de nuestra red, podemos utilizar la dirección broadcast correspondiente al tipo de red en cuestión o emplear la *dirección broadcast universal* que tiene el formato 255.255.255.255

*Dirección desconocida*

La dirección 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección. Esta dirección no se asigna a ninguna red. Se utiliza en el protocolo RARP (Reverse Address Resolution Protocol), o variantes del mismo, cuando una estación tiene que averiguar su propia dirección IP, partiendo de su dirección MAC.

*Direcciones de red*

Para referirnos a una red o subred completa, se utiliza la dirección de red terminada en cero o ceros, conocida como *dirección oficial de la* red. Las direcciones oficiales en redes clase A serán de la forma x.0.0.0, las de clase B tendrán la forma x.x.0.0 y las de clase C x.x.x.0. Las direcciones oficiales de red se emplean para decidir la ruta de los paquetes en función de la red destinataria.

## III.8.2 Subredes y máscara de subred

Una subred es simplemente una parte o porción de la red que opera como una red separada, que no es consciente de lo que sucede fuera de ella y a la que no le afecta el resto de la red.

Dividir una red en varias subredes, tiene la ventaja de permitir aislar el tráfico entre las distintas subredes, con lo que se reduce el tráfico global. Además, permite proteger y limitar el acceso a las distintas subredes, que será realizado generalmente a través de routers. Otra ventaja es la posibilidad de organizar la red en áreas o departamentos de manera que se asigne a cada departamento un conjunto de direcciones IP; de esta forma, la gestión y administración de estas direcciones IP se puede realizar de forma descentralizada.

La máscara de red es una combinación de bits que permite delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Básicamente consiste en una dirección de 32 bits, que permite enmascarar o bloquear de la vista de dicha subred a las subredes ajenas o áreas exteriores y así saber si debe enviar los datos dentro o fuera de la red.

Ejemplo:

Supongamos que tenemos una computadora que forma parte de una subred con la dirección IP 192.16.251.11. Los dispositivos que se encuentran conectados a esta subred tienen las direcciones IP 192.16.251.5, 192.16.251.6, 192.16.251.7. Debido a que es una red de clase C la máscara de subred que se utilizará será 255.255.255.0. Esto nos indica que los tres primeros octetos de las direcciones IP en la subred serán iguales para todos los dispositivos conectados y el octeto más significativo es el último por lo tanto podemos disponer de las 254 direcciones IP de una red clase C.

Todos los equipos cuyas direcciones IP fueran, por ejemplo 192.16.250.x o 192.16.252.x no serán visibles directamente desde esta subred y estarían enmascaradas; para acceder a estos equipos, se debe llegar a ellos a través de algún router o puerta de enlace.

Las máscaras, se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo, de esta manera se permite realizar una verificación de la dirección de la Red y con un OR y la máscara negada se obtiene la dirección del broadcasting.

Como la máscara consiste en una secuencia de unos y ceros, los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255.

| | Representación binaria | Punto decimal |
|---|---|---|
| Máscara de Clase A por defecto | 11111111.00000000.00000000.00000000 | 255.0.0.0 |
| Ejemplo de máscara de clase A | 11111111.11000000.00000000.00000000 | 255.192.0.0 |
| Máscara de Clase B por defecto | 11111111.11111111.00000000.00000000 | 255.255.0.0 |
| Ejemplo de máscara de Clase B | 11111111.11111111.11111000.00000000 | 255.255.248.0 |
| Máscara de Clase C por defecto | 11111111.11111111.11111111.00000000 | 255.255.255.0 |
| Ejemplo de máscara de Clase C | 11111111.11111111.11111111.11111100 | 255.255.255.252 |

*Tabla 3.6 Máscaras de subred por defecto*

# Capitulo IV
# PROYECTO DE UNA RED INALAMBRICA

## IV.1 CABLEADO ESTRUCTURADO

El diseño e instalación de los medios de la red está asociado con las capas físicas de la red. En cualquier instalación nueva de cable o proyecto de reparación del alambrado, debe diseñarse previo a cualquier instalación un plan de cableado que especifique el tipo de cable por usar y la manera en que los cables estarán configurados. El concepto de planeación del cableado está descrito en la norma EIA/TIA 568. Esta norma representa estándares de sistemas de cableado estructurado para el alambrado en sitios que trata sobre el diseño de redes y las características de desempeño de los medios físicos. Los estándares son genéricos por su naturaleza y proveen a los administradores de red con información suficiente para diseñar una planta robusta de cable que pueda acomodar diferentes formas de transmisiones y soportar un ambiente de múltiples productos y vendedores.

Un sistema de cableado estructurado comprende seis subsistemas: entrada al edificio, cuarto de equipo (site), cableado troncal (backbone), panel de parcheo (patch panel), cableado horizontal y área de trabajo. La entrada al edificio proporciona conectividad desde el exterior del edificio. Aquí es donde una línea de red troncal principal se interconecta con la red exterior de un campus o a una red WAN de manera que todas las LAN dentro tengan conectividad con el exterior. El cuarto de equipo es el alma de la infraestructura de red del edificio. En él se encuentra el equipo que proporciona conectividad con otros edificios así como con los paneles de telecomunicaciones localizados en cada piso del edificio. Así, un cuarto de equipo de un edificio puede soportar todas las funciones de un equipo de telecomunicaciones, pero generalmente contiene equipo que es más complejo que el localizado dentro de un panel de telecomunicaciones. El cableado troncal de un edificio interconecta los paneles de telecomunicaciones del edificio, los cuartos de equipo y la entrada. Así, un cable troncal sirve como la línea troncal principal para la conectividad de la red. La topología del cableado troncal específicamente es de una estrella jerárquica.

*Fig. 4.1 Rack y panel de Parcheo utilizados en el cuarto de equipo*

Un panel de telecomunicaciones aloja un equipo de telecomunicaciones de un edificio y es donde se termina un cable o donde son hechas las conexiones transversales. La mayoría de los edificios tienen un panel de telecomunicaciones por piso y están interconectados por un cable troncal. En otros casos, la entrada de un edificio funciona como un panel de telecomunicaciones, además de proporcionar conectividad a cada piso de un edificio así como conectividad en el interior de éste. En este caso, no existe cable troncal. El cableado horizontal consiste en el cable mismo, la pared de salida (salida de telecomunicaciones), las terminaciones de los cables y las conexiones transversales. Es en este punto en donde se utiliza el par trenzado UTP, FTP o SFTP categoría 5, el cual no debe exceder la distancia máxima de 100m incluyendo las conexiones del panel de parcheo. El área de trabajo se extiende desde la salida de pared hasta la estación de red. El área de trabajo consiste en el equipo en red, los cables de empalme y los adaptadores.

Las instalaciones de cable realizadas de forma apropiada y de acuerdo con los estándares deben proporcionar una organización con la infraestructura de alambrado que disponga el crecimiento actual y futuro por lo menos 10 años.

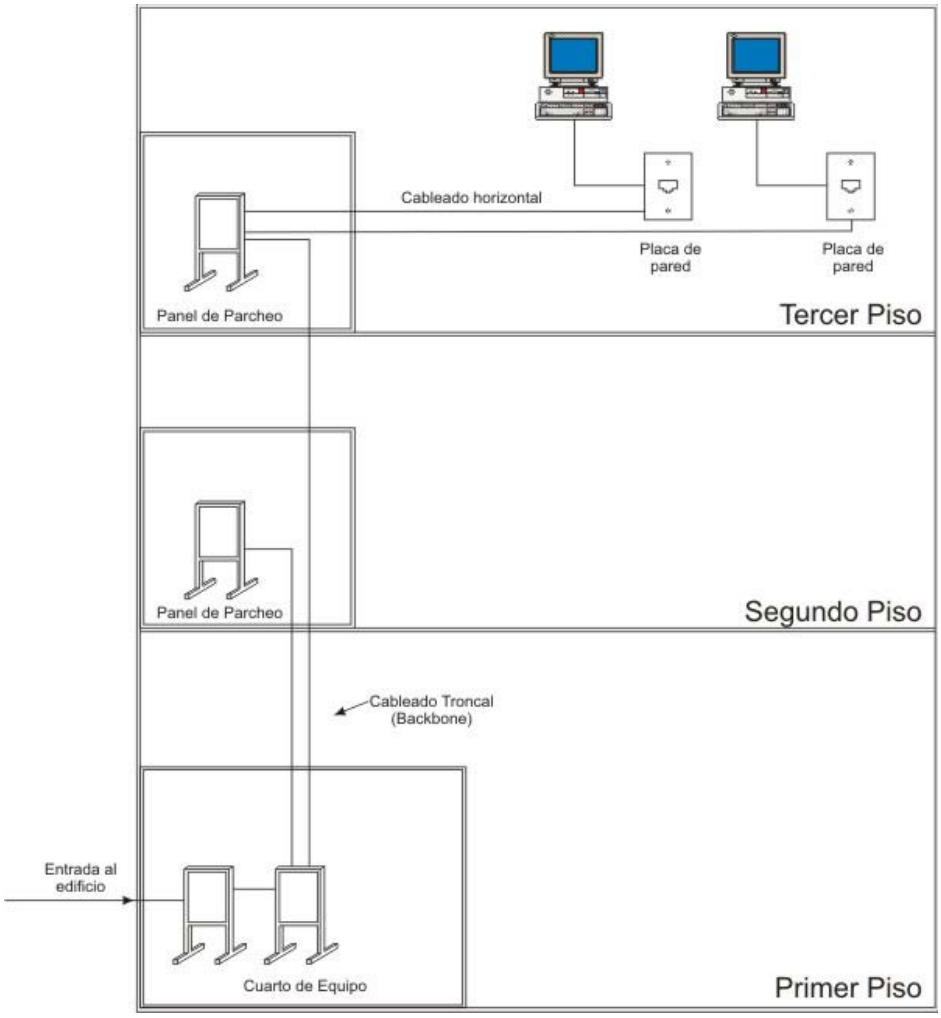



*Fig. 4.2 Componentes principales del cableado estructurado*

Además de definir la forma en que se debe colocar el cableado, la norma EIA/TIA 568 también define la manera en que se deben colocar los conectores de los cables (plugs) y las rosetas (jacks) de las placas de pared en las puntas de los cables.

## *RJ-45*

El conector RJ-45 es ampliamente utilizado en redes locales Ethernet, en redes digitales de servicios integrados (RDSI) e incluso en redes de telefonía digital, principalmente se conecta en cables de par trenzado tipo 4 y 5 de cuatro pares. Tiene 8 pines, y en función de la utilidad que le vayamos a dar, se asignará una utilidad determinada a cada pin.

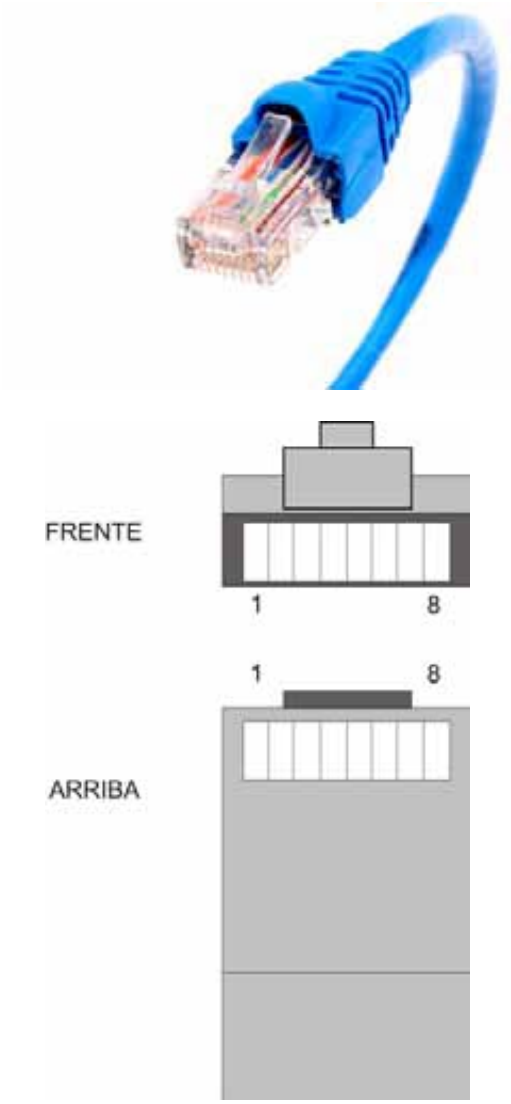



*Fig. 4.3 Conector RJ45*

Existen 2 esquemas para conectar el cable y el conector, el 568A y e 568B, sin embargo el más utilizado de los dos en la práctica es el 568B por lo que solamente se explicará este.

Los pares en el interior del cable vienen por colores para evitar una mala conexión, algunos de estos vienen con una franja blanca para identificarlo de su pareja. La forma en que deben conectarse en el conector RJ-45 así como su función esta mostrado en la siguiente tabla:

| Pin Nº | Color | Función |
|---|---|---|
| 1 | Blanco - Naranja | Transceive data + |
| 2 | Naranja | Transceive data - |
| 3 | Blanco - Verde | Receive data + |
| 4 | Azul | Bi-directional Data + |
| 5 | Blanco - Azul | Bi-directional Data - |
| 6 | Verde | Receive data - |
| 7 | Blanco - Café | Bi-directional Data + |
| 8 | Café | Bi-directional Data - |

*Tabla 4.1 Código de colores 568B*

Aunque se suelen unir todos los hilos, para las comunicaciones Ethernet sólo hacen falta los pines '1 y 2' y '3 y 6', usándose los otros para telefonía (el conector RJ-11 encaja dentro del RJ-45, coincidiendo los pines 4 y 5 con los usados para la transmisión de voz en el RJ-11) o para PoE (Power over Ethernet) lo que permite que un equipo (cámaras de seguridad, teléfonos o puntos de acceso inalámbricos) reciba la energía eléctrica a través del cable de red en lugar de un contacto de pared.

Para el caso de los jacks, también existen los esquemas 568a y 568b para conectarlas, sin embargo la forma de conectarlo con el cable viene impresa en un costado por lo que es muy fácil de instalar.


*Fig. 4.4 Jack RJ-45*

Tanto el plug como el jack requieren una herramienta especial para ser instalados, en ambos casos se llama crimpadora y ponchadora, sin embargo son muy diferentes entre ellas.

Crimpadora para Plug


Crimpadora para Jack

*Fig. 4.5 Herramientas*

## IV.2 APLICACIÓN DE LAN INALÁMBRICAS

***Ampliación de redes LAN***

La ventaja es que una red WLAN evita el coste de la instalación del cableado y facilita la tarea de traslado y otras modificaciones en la estructura de la red, sin embargo esta motivación de las WLAN fue superada por los acontecimientos. Primero, debido al aumento en la necesidad de redes LAN, los arquitectos incluyeron en el diseño de sus nuevos edificios costosos precableados para aplicaciones de datos. Segundo, con los avances en la tecnología de transmisión de datos se incrementó la seguridad en los pares trenzados para redes LAN. Así, dado que la mayor parte de los edificios viejos estaban ya cableados con par trenzado de Clase 3, y muchos de los edificios de nueva construcción lo están con par trenzado Clase 5, resulta escaso el uso de LAN inalámbricas frente a LAN cableadas.

Sin embargo, el papel de una WLAN como alternativa a las LAN cableadas es importante en un gran número de entornos. Algunos ejemplos son edificios de gran superficie, como plantas de fabricación, plantas comerciales y almacenes; edificios históricos con insuficiente cable de par trenzado donde está prohibido hacer más agujeros para nuevo cableado; y pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan económicos. En todos estos casos, una WLAN ofrece una alternativa más efectiva y atractiva. En la mayor parte de estas situaciones, un organismo dispondrá también de una LAN cableada con servidores y algunas estaciones de trabajo estacionarias. Por ejemplo, una planta de manufacturación dispone generalmente de una oficina independiente de la propia planta pero que debe estar interconectada a ella con propósitos de trabajo en red. Por tanto una WLAN está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de redes LAN.

La configuración de la primera figura se denomina LAN inalámbrica de celda única, ya que todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control. Otra configuración común es la de LAN inalámbrica de celdas múltiples. En este caso existen varios módulos de control interconectados por una LAN cableada. Cada módulo de control da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión

***Interconexión de edificios***
Otro uso de las LAN de tecnología inalámbrica es la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o inalámbricas. En este caso se usa un enlace no guiado entre dos edificios. Los dispositivos así conectados son generalmente puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de las redes LAN inalámbricas.

***Acceso nómada***
El acceso nómada permite un enlace no guiado entre un centro de LAN y una terminal de datos móvil con antena, como una computadora portátil. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de viaje la transferencia de datos desde su computadora portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio cono es un campus o un centro financiero situado lejos de un grupo de edificios. En ambos casos los usuarios se pueden desplazar con sus computadoras portátiles y pueden desear conectarse con los servidores de una LAN inalámbrica desde distintos lugares.

***Trabajo en red ad hoc***
Una red *ad hoc* es una red igual a igual (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computadora, puede reunirse para una conferencia conectando sus computadoras a una red temporal solo durante la reunión.

## IV.3 REQUISITOS DE LAS REDES LAN INALAMBRICAS

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad toral de las estaciones conectadas y capacidad de difusión. Además, existe un conjunto de necesidades específicas para entornos LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- **Rendimiento**: el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio no guiado para maximizar capacidad.

- **Número de nodos**: las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.

- **Conexión a la LAN troncal**: en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que

conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas *ad hoc*.

- **Área de servicio**: una superficie de cobertura para una red LAN inalámbrica sin obstrucciones tiene un diámetro típico de entre 100 y 300 metros.

- **Consumo de batería**: los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable. Esto sugiere que resulta inapropiado un protocolo MAC que necesita nodos móviles para supervisar constantemente los puntos de acceso o realizar comunicaciones frecuentes con una estación base.

- **Robustez en la transmisión y seguridad**: a menos que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.

- **Funcionamiento de red ordenada**: a medida que las LAN inalámbricas se están haciendo más populares, es probable que dos o más de estas redes operen en la misma o en alguna zona en que sea posible la interferencia entre ellas. Estas interferencias pueden frustrar el normal funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.

- **Funcionamiento sin licencia**: los usuarios podrían preferir adquirir y trabajar sobre LAN inalámbricas que no precisan de una licencia para la banda de frecuencia usada por la red.

- **Sin intervención/nómada**: el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.

- **Configuración dinámica**: los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

## IV.4 CONFIGURACIÓN DE UN PUNTO DE ACCESO

Las características con las que cuentan los puntos de acceso varían dependiendo de su marca y el modelo, así como la presentación del menú de cada uno, sin embargo las características principales que todos ellos incluyen y deben configurarse para instalar una red inalámbrica son las siguientes:

- **Nombre de red.** A este también se le conoce como SSID (*Service Set Identifier*), (Identificador del Conjunto de Servicios). Le permite al equipo que quiera conectarse a una red inalámbrica identificar las redes disponibles en el área. Todos los puntos de acceso incluyen un nombre de red por defecto. Sin embargo, es recomendable sustituir este nombre por cualquier otro que se considere adecuado. Los puntos de acceso también permiten deshabilitar la emisión del SSID, de manera que si un equipo busca acceso inalámbrico no podrá ver la red aún cuando se encuentre dentro del área de cobertura.

- **Canal.** En este punto se introducirá el número de canal que se considere apropiado. Por defecto, la mayoría de los puntos de acceso ya vienen configurados con un determinado canal. No obstante, en caso de que el punto de acceso se encuentre dentro del rango de cobertura de otro, es necesario configurarlo con un canal diferente para eliminar interferencias, aún así debe procurarse que el área de solapamiento sea mínima.
  En teoría, con tan solo tres frecuencias se puede cubrir cualquier área, sin dejar zonas de sombra. Los canales ideales para introducir en los puntos de acceso son el 1, 6 y 11 como vimos anteriormente. La forma de distribuir los puntos de acceso es la siguiente:

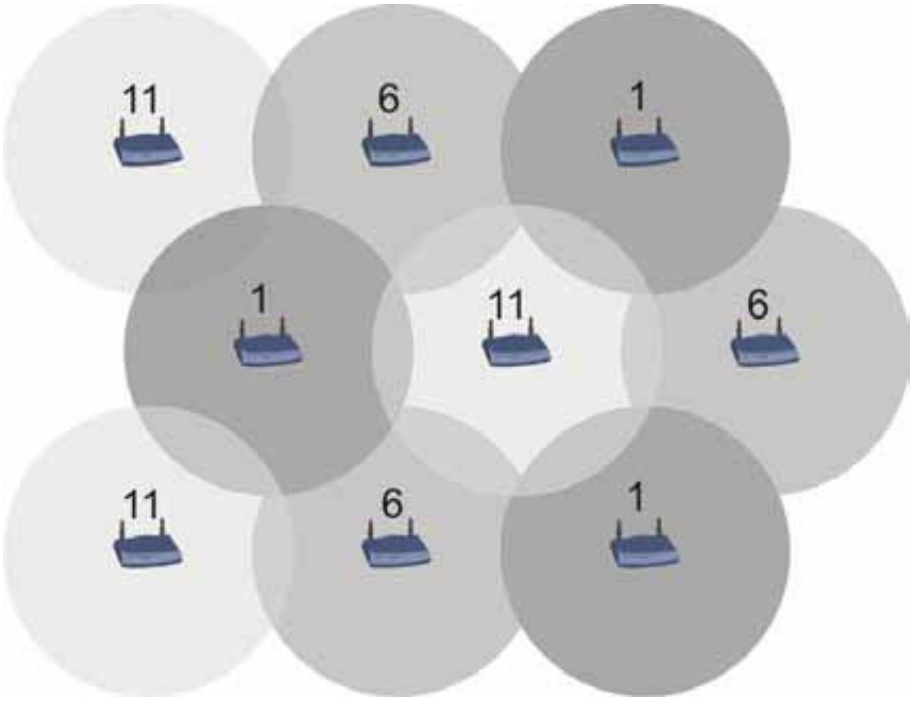



*Fig. 4.6 Distribución de canales de una red inalámbrica*

  En caso de utilizar topología WDS todos los puntos de acceso deberán estar configurados en el mismo canal. En este caso los SSID de todos los puntos de acceso deben ser iguales.
- **Seguridad.** Esta característica debe configurarse en el punto de acceso y en los adaptadores de cada ordenador que forme parte de la red. La primera vez que se configure un punto de acceso conviene deshabilitar los parámetros de seguridad. Una vez

comprobado que la red funciona adecuadamente, se puede elegir un tipo de cifrado (WEP o WPA) y seleccionar una clave de seguridad.

- **Dirección IP.** Esta opción es importante cuando se quiere conectar el punto de acceso a una red cableada (principalmente Ethernet) o a Internet. Estos parámetros son los mismos que hay que configurarle a cualquier ordenador que forme parte de la red cableada: dirección IP, máscara de subred, puerta de enlace y servidor DNS.
- **Servidor DHCP.** DHCP (*Dynamic Host Configuration Protocol,* Protocolo de Configuración Dinámica del Host) es un protocolo que permite que el punto de acceso asigne automáticamente una dirección IP al cliente que se conecte con el. Al desactivar esta opción las direcciones IP de todos los equipos que se unan a la red deberán ser introducidas manualmente, de esta manera cada cliente siempre tendrá la misma dirección IP.

  En algunos puntos de acceso es posible determinar cuantos equipos pueden tener acceso simultáneamente a la red, además de disponer de un rango determinado de direcciones IP para gestionar.

Algunas características opcionales que incluyen los puntos de acceso son:

- **Selección de ordenadores autorizados.** Algunos puntos de acceso incluyen la capacidad de realizar filtrado de direcciones MAC a través de una lista de ordenadores autorizados. Esta característica ayuda a incrementar la seguridad de la red, pero no es práctica cuando se desea disponer de una red inalámbrica abierta a nuevos usuarios. Las direcciones MAC son números únicos que cada fabricante asigna a todos sus dispositivos de red. Este número identifica al dispositivo de forma inequívoca. Las direcciones MAC están formadas por 12 caracteres hexadecimales.

  Ejemplo: 00-11-5B-CC-AD-FB
- **Reducción automática de velocidad** (*Auto rate fall back)*. Esta característica permite que, cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.
- **Habilitar la red inalámbrica.** Esta opción generalmente está incluida en puntos de acceso que disponen de las funciones de un router o switch, y es utilizada cuando se necesitan realizar estas actividades prescindiendo de sus funciones de punto de acceso.

## IV.5 CONFIGURACION DEL ADAPTADOR DE RED

Los pasos para configurar un adaptador o tarjeta de red son similares para todas las computadoras independientemente del sistema operativo que tengan.

El primer paso consiste en instalar el adaptador de red en la computadora, si el adaptador es del tipo PCI será necesario abrir el CPU para instalarla en una ranura libre de la tarjeta madre. Para los adaptadores PCMCIA o USB bastará con conectarlos en la ranura correspondiente del equipo. Una vez que nos aseguremos que está perfectamente colocada podremos cerrar el gabinete y prender la PC.

*Fig. 4.7 Ejemplo de instalación de un adaptador de red*

Una vez que hayamos conectado el adaptador de red debemos instalar los controladores. En el caso de Windows XP al encender la computadora esta reconocerá el hardware nuevo solicitando el disco de instalación. En ese momento debemos introducirlo y seguir las instrucciones.


*Fig. 4.8 Ventana para instalar equipo nuevo*

Una vez que el adaptador de red quede correctamente instalado debemos configurar la red inalámbrica. Para conectarnos a la red inalámbrica, primero hay que encontrar el icono de redes inalámbricas en la esquina inferior derecha de la pantalla y darle “clic” al botón secundario para ver las redes inalámbricas disponibles en el área.

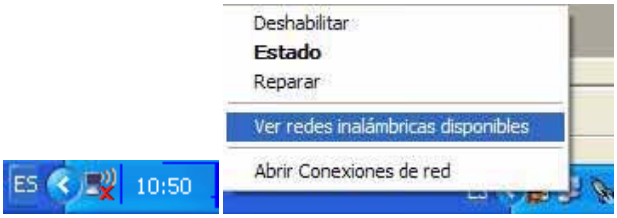



*Fig. 4.9 Icono de red inalámbrica y menú secundario*

En la ventana que se abre aparecerán las redes inalámbricas que la tarjeta detectó. Si alguna de estas redes es a la que queremos conectarnos habrá que seleccionarla y escribir la clave de red. En el caso de que nuestra red no aparezca por alguna razón como emisión SSID deshabilitada seleccionaremos opciones avanzadas.


*Fig. 4.10 Ventana con las redes disponibles para conectar*

En la ventana que se abre hay que seleccionar “Agregar…” en la parte de redes preferidas.


*Fig. 4.11 Propiedades de conexión de red inalámbrica*

Cuando seleccionamos la opción agregar aparece una ventana en la cual hay que poner el nombre de red inalámbrica además de elegir el tipo de clave de seguridad que estamos utilizando y la clave de la red. En caso de utilizar una red Ad-hoc habrá que seleccionar el recuadro del final, en cualquier otro caso deberá quedarse sin seleccionar. Cuando todos los datos estén listos pulsaremos Aceptar.


*Fig. 4.12 Ventana de Propiedades de red inalámbrica*

Al cerrar la ventana regresaremos a propiedades de conexión de red, en este momento ya se puede utilizar la red inalámbrica si nuestro punto de acceso tiene el servidor DHCP habilitado. En caso contrario tenemos que ingresar la dirección IP que utilizara nuestro equipo, para esto hay que ingresar en Inicio/Panel de control, pulsar en conexiones de red y se abrirá la ventana de conexiones de red. Seleccionaremos el ícono de la red, oprimiremos en el botón secundario y finalmente en propiedades.

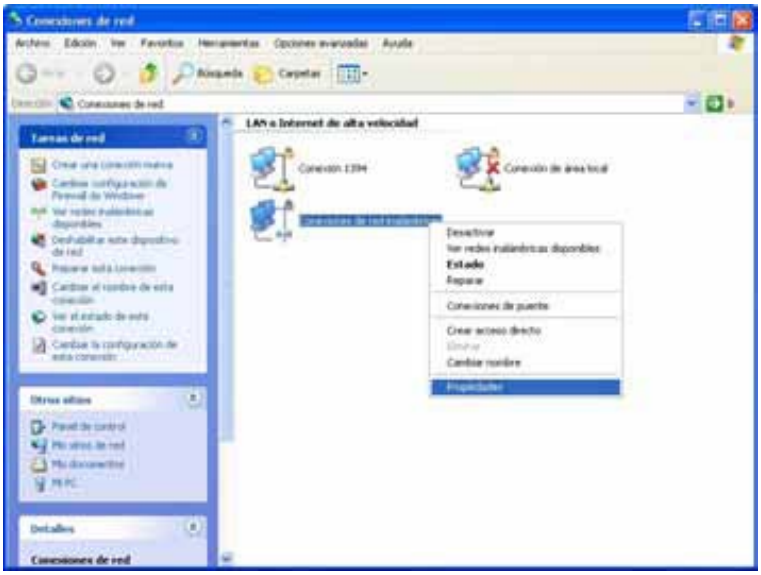


*Fig. 4.13 Ventana de conexiones de red*

Después seleccionamos “Protocolo Internet (TCP/IP) y pulsaremos en Propiedades. En la ventana que aparece debemos poner la dirección IP, máscara de subred, puerta de enlace, y si es necesario el servidor DNS correspondiente.

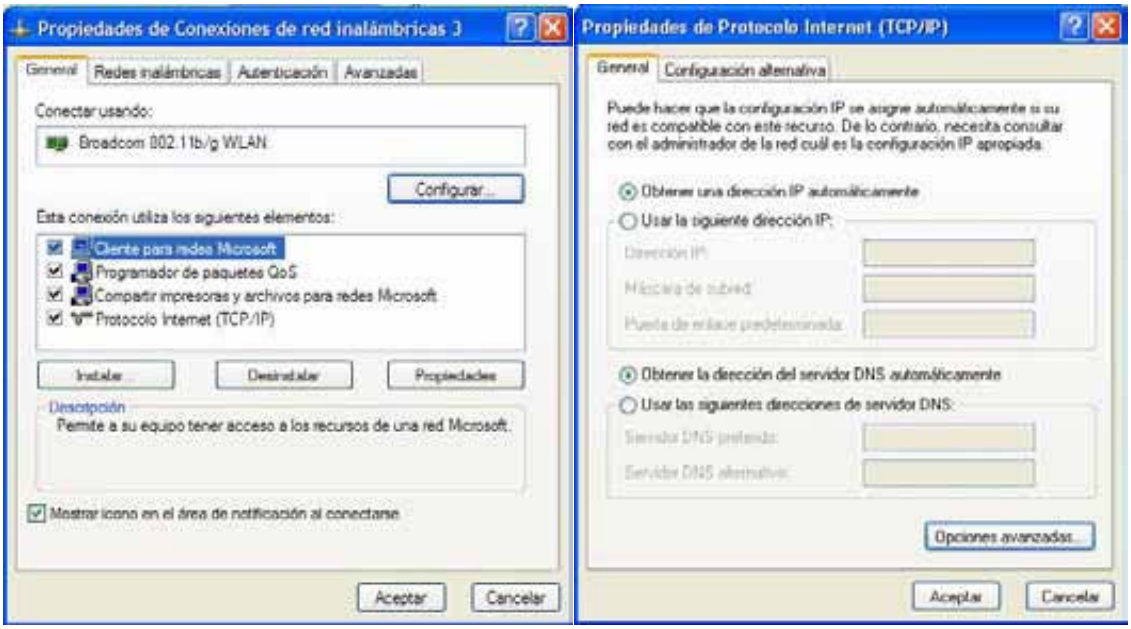



*Fig. 4.14 Ventanas de propiedades de conexión de red inalámbrica y de protocolo TCP/IP*

Una vez que el adaptador de red ha sido configurado, el icono de la red inalámbrica cambiará y se activará; si es necesario revisar el estado de la conexión de la red daremos doble clic en el icono y aparecerá la ventana de estado de conexiones de red inalámbricas.

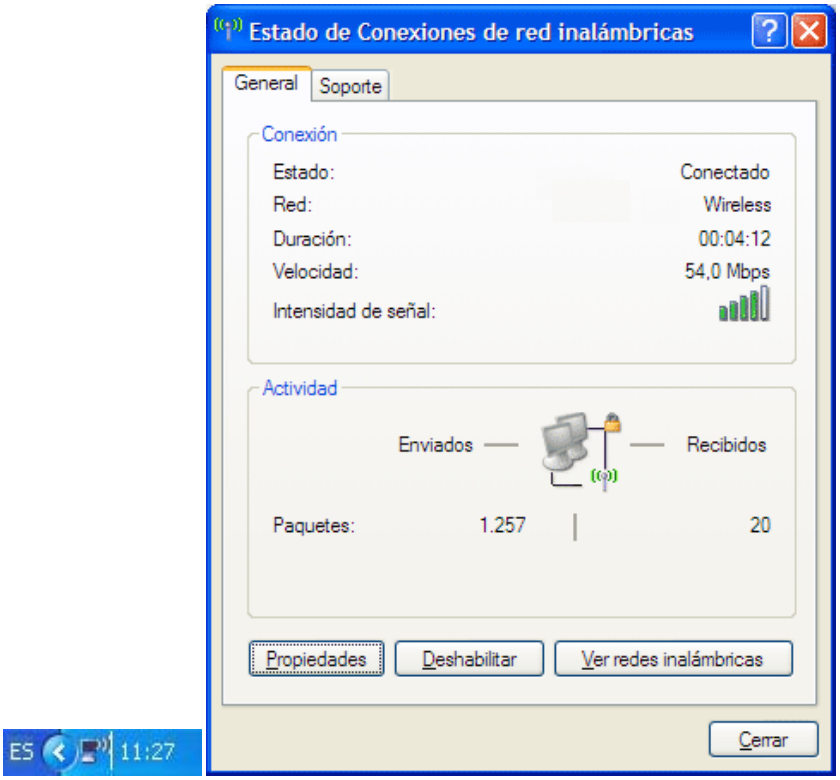



*Fig. 4.15 Estado de conexión de red inalámbrica*

Otra forma de averiguar si ha conectado a la red es haciendo un "ping" desde la computadora al punto de acceso, para ello iremos a Inicio -> Programas -> Accesorios -> Símbolo del sistema y escribimos ping y la dirección IP del punto de acceso (192.168.1.1 por ejemplo):

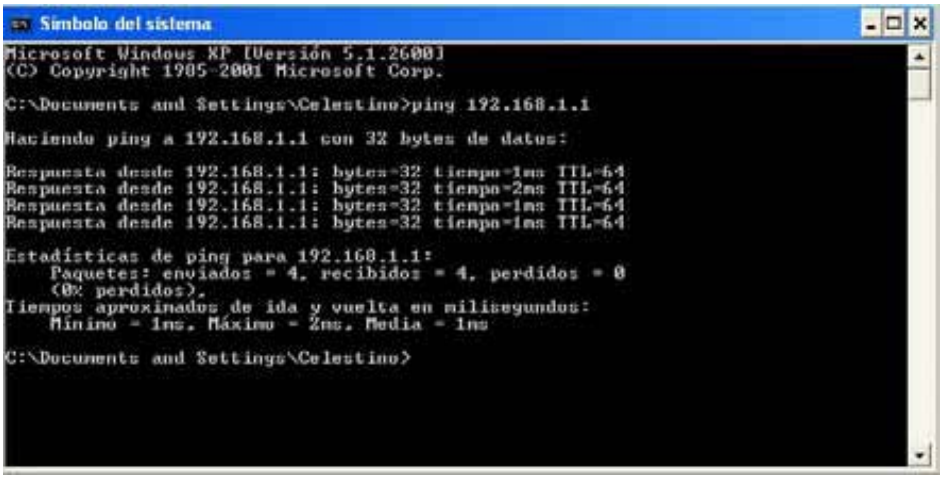



*Fig. 4.16 Ventana de un ping al PC servidor.*

Podemos ver que los paquetes perdidos son 0 lo cual es muy importante y los tiempos de ida y vuelta son muy bajos, además de que es importante que no varíen mucho entre ellos (por ejemplo: 10ms, 45ms, 80ms, 30ms), sino que sean regulares como en la imagen anterior.

## IV.6 FORMULA PARA CALCULAR EL ALCANCE DE COMUNICACION

El alcance es la distancia física y lineal entre dos puntos que permiten una conexión inalámbrica. Esta medida está determinada por las características de los equipos que utilicemos para entablar la comunicación y puede ser incrementada utilizando equipos como antenas o transmisores así como es atenuada dependiendo del tipo de cables y conectores que utilicemos, además de interferencias electromagnéticas en el aire.

La fórmula para obtener el nivel de señal que recibe un equipo receptor de un equipo transmisor es:

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par— Pa - Pm$$

Donde:

Sr = Nivel de señal que llega al receptor. El resultado siempre es negativo

Gse = Ganancia de salida del equipo transmisor.

Pce = Pérdida de los cables del equipo transmisor. Se usa en caso de utilizar una antena externa.

Pae = Pérdida de los conectores del equipo transmisor. Solo en caso de utilizar una antena externa.

Gae = Ganancia de la antena del equipo transmisor.

Pp = Pérdida de propagación

Gar = Ganancia de la antena del equipo receptor.

Pcr = Pérdida de los cables del equipo receptor. Solo se usa en caso de utilizar una antena externa.

Par = Pérdida de los conectores del equipo receptor.

Pa= Pérdidas ambientales.

Pm = Pérdidas por penetración de muros o pisos

Las pérdidas por conectores se considerarán de 0.25dB por cada conector que se utilice.

Para la atenuación por pisos y muros podemos utilizar la siguiente tabla:

| TIPO DE OBSTACULO | PERDIDA |
|---|---|
| Espacio Abierto | 0 dB |
| Ventana (tintado no metálico) | 3 dB |
| Ventana (tintado metálico) | 5 – 8 dB |
| Muros finos | 5 – 8 dB |
| Muros medios | 10 – 13 dB |
| Muros gruesos | 15 – 20 dB |
| Muros muy gruesos | 20 – 25 dB |
| Suelo / Techo grueso | 15 – 20 dB |
| Suelo / Techo muy grueso | 20 – 25 dB |

*Tabla 4.2 Pérdidas por penetración en diversos materiales*

Las pérdidas por tipo de cable dependen mucho de las características del cable que usemos. Las pérdidas típicas para los tipos de cable más comunes se muestran en la siguiente tabla:

| TIPO DE CABLE | PERDIDA EN ESTANDAR 802.11b/g |
|---|---|
| LMR-100 | 1.3 dB por metro |
| LMR-195 | 0.62 dB por metro |
| LMR-200 | 0.542 dB por metro |
| LMR-240 | 0.415 dB por metro |
| LMR-300 | 0.34 dB por metro |
| LMR-400 | 0.217 dB por metro |
| LMR-500 | 0.18 dB por metro |
| LMR-600 | 0.142 dB por metro |
| LMR-900 | 0.096 dB por metro |
| LMR-1200 | 0.073 dB por metro |
| LMR-1700 | 0.055 dB por metro |
| RG-58 | 1.056 dB por metro |
| RG-8X | 0.758 dB por metro |
| RG-213/214 | 0.499dB por metro |
| 9913 | 0.253 dB por metro |
| 3/8" LDF | 0.194 dB por metro |
| 1/2" LDF | 0.128 dB por metro |
| 7/8" LDF | 0.075 dB por metro |
| 1 1/4" LDF | 0.056 dB por metro |
| 1 5/" LDF | 0.046 dB por metro |

*Tabla 4.3 Pérdidas de los principales cables*

Las pérdidas ambientales se consideran cuando la señal va a pasar por zonas abiertas exponiéndose así a interferencias ocasionadas por lluvias o tormentas eléctricas. En este caso pueden considerarse de 20dB.

Existen ocasiones en que los fabricantes de los equipos inalámbricos no especifican la ganancia de salida (dB) sino que utilizan el valor de la potencia de emisión (mW). Para calcular el valor de la ganancia de salida se utiliza la siguiente fórmula:

$$Gse = 10\log_{10}(Pe)$$

Pe = Potencia de emisión

## IV.6.1 Pérdida de propagación

La pérdida de propagación es la cantidad de señal que se pierde al atravesar un espacio.

La pérdida de propagación se puede calcular con la siguiente fórmula:

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 20\log_{10}(f * 1000) + 32.4$$

Donde:

Pp = Pérdida de propagación (dB)

d = distancia (m)

f = frecuencia (GHz)

A pesar de que dependiendo del canal que se utilice varía la frecuencia, la diferencia entre el canal 1 (2.412 GHz) y el canal 11 (2.462 GHz) es de 0.05 GHz por lo que se puede tomar la frecuencia de 2.4 GHz para hacer el cálculo de todos los canales.

Sustituyendo el valor de la frecuencia, se puede reducir la ecuación de la siguiente manera:

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 20\log_{10}(2.4 * 1000) + 32.4$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

Una vez que tenemos el nivel de señal debemos compararlo con la sensibilidad del equipo que vamos a utilizar. Si el valor es mayor la recepción se realizará. En caso contrario el receptor no encontrará la señal. Cabe mencionar que el cálculo se debe hacer considerando la transmisión en ambos sentidos para asegurarnos que la comunicación se realice apropiadamente.

## IV.7 PASOS PARA CREAR UNA RED INALAMBRICA

Una parte muy importante antes de la creación de una red inalámbrica es la metodología que se debe seguir para lograr una planeación adecuada y así reducir al mínimo los problemas que puedan ocurrir cuando la red esté funcionando. En general los pasos que se deben seguir son los siguientes:

1. Identificar el lugar donde se va a instalar la red inalámbrica.
2. Seleccionar topología de red inalámbrica.
3. Seleccionar el estándar Wi-Fi que se va a utilizar.
4. Seleccionar marca y modelo de punto de acceso y adaptador de red a utilizar.
5. Calcular la distancia máxima entre los adaptadores y los puntos de acceso.
6. En caso de ser necesario seleccionar tipo de antena externa, así como de cable.
7. Escoger el lugar donde se va a instalar el o los puntos de acceso.
8. Configurar los puntos de acceso.
9. Instalar los adaptadores de red.
10. Configurar los adaptadores de red.
11. Probar la conexión.

1.- El primer paso es muy importante ya que se deben conocer toda la extensión del lugar o lugares en los que es necesario tener cobertura inalámbrica, si en estos lugares existe red cableada, o si es posible instalar nodos nuevos para el punto de acceso.

2.- El segundo paso es seleccionar la topología de red inalámbrica más conveniente según la zona en la que se va a instalar la red. El caso más sencillo es el de una topología BSS en la que un solo punto de acceso puede dar servicio a todos los equipos de la red; pero si la extensión es muy grande o si no hay manera de instalar nodos de red se podría considerar una topología ESS y WDS.

3.- El tercer paso consiste en seleccionar el estándar Wi-Fi para la red inalámbrica. Esto se debe seleccionar considerando el número de equipos a los que se les dará servicio, el nivel de seguridad necesario para la red y el costo de los equipos.

4.- Una vez terminados los pasos anteriores se puede elegir un modelo de punto de acceso y de adaptador de red para utilizar en la red. Antes de comprarlo es recomendable revisar sus hojas de especificaciones para asegurarnos que el equipo tenga la certificación Wi-Fi, que utilice los estándares que necesitamos y que tenga los datos técnicos del equipo como potencia y sensibilidad para realizar los cálculos necesarios.

5 y 6.- Con los datos de los equipos que queremos utilizar podemos realizar los cálculos para asegurarnos que la cobertura existirá en toda el área donde se necesita la red inalámbrica. Si el resultado está muy cercano a la distancia real en la que se pondrán los equipos se puede esperar al fin de la instalación y probar la conexión. Si la conexión no es la deseada podemos utilizar una antena externa para aumentar el alcance, también es posible considerar la antena externa al

momento de realizar los cálculos para garantizar un nivel de señal óptimo para la comunicación. En este caso se deberán considerar la ganancia de la antena y las pérdidas provocadas por el cable y los conectores utilizados.

7 y 8.- Al terminar con los cálculos, podremos decidir la manera en que los puntos de acceso serán distribuidos en los diferentes lugares, sin embargo antes de instalarlos es necesario configurarlos, principalmente porque cuando son equipos nuevos la primera configuración debe realizarse con una computadora conectada al puerto Ethernet. De esta manera podemos introducir los datos requeridos para hacer funcionar la red inalámbrica.

9.- A continuación debemos instalar un adaptador de red inalámbrico en cada equipo que vamos a incluir en la red inalámbrica y que no posea un adaptador integrado. Si el adaptador es del tipo PCI o PCMCIA habrá que abrir el CPU para instalarlo y en caso de ser USB bastará con conectarlo en un puerto USB disponible. Después tendremos que instalar los controladores necesarios.

10 y 11.- Una vez instalados los adaptadores de red debemos configurar en cada máquina los datos de la red incluyendo dirección ip, máscara de subred y puerta de enlace. Una vez hecho esto se debe probar que haya conexión primero entre la computadora y el punto de acceso y finalmente con el resto de la red. Si estas pruebas se realizan satisfactoriamente la red ha sido terminada.

## IV.8 PROYECTO

El proyecto de titulación consiste en planificar una red inalámbrica Wi-Fi para algunas oficinas del servicio postal mexicano que se encuentran en el palacio postal, en las cuales no se puede poner una red cableada debido a que el edificio se considera patrimonio cultural de la humanidad y como tal debe ser preservado en su estado actual evitando hacer perforaciones en los muros.

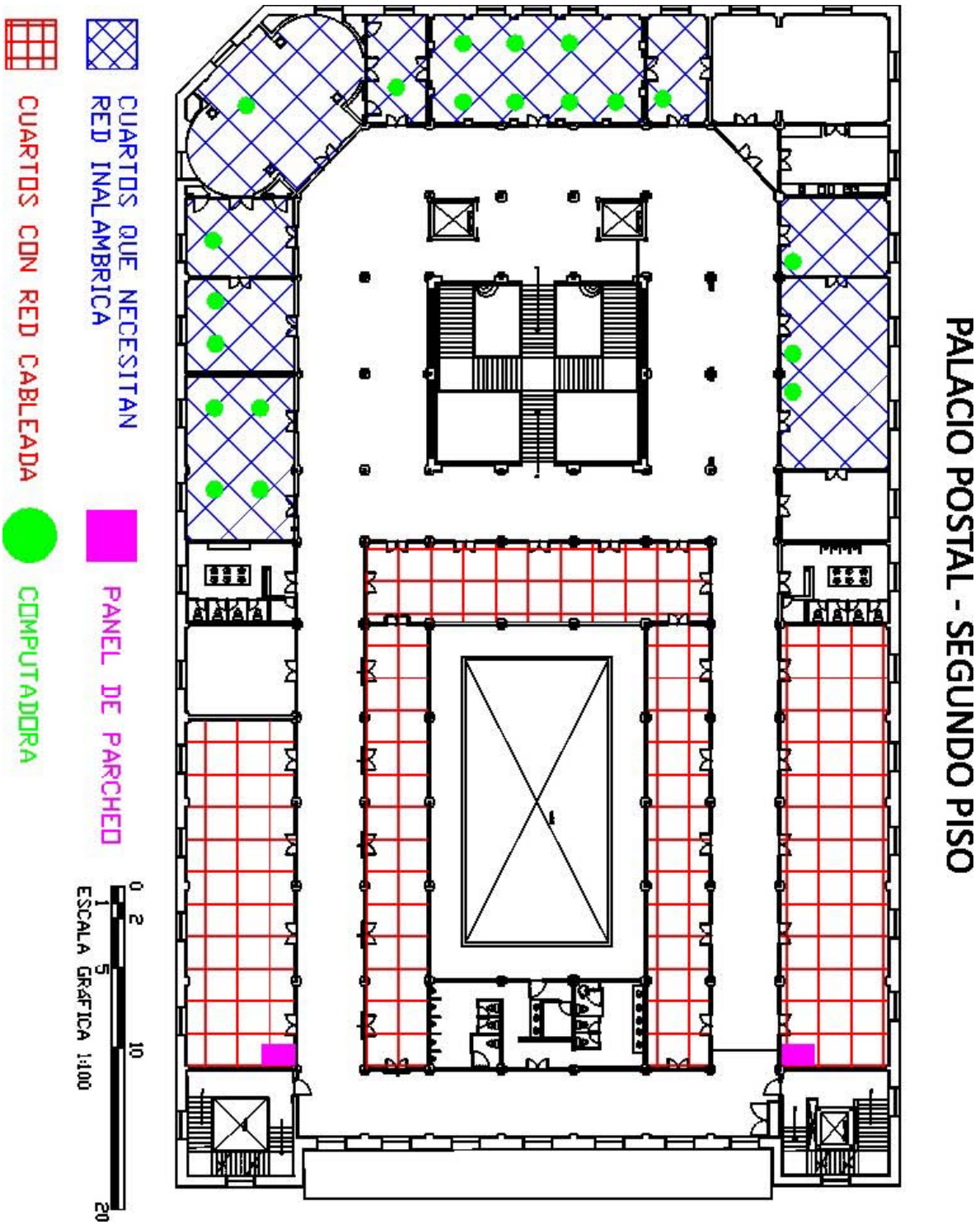
*Fig. 4.17 Palacio Postal*

El primer paso es identificar la zona donde se necesita la red inalámbrica. En este caso las oficinas se encuentran distribuidas entre el segundo y tercer piso del edificio y no cuentan con red cableada aún cuando existen otras oficinas donde si existe red cableada, en algunas de estas hay paneles de parcheo desde los que se distribuyen los nodos.

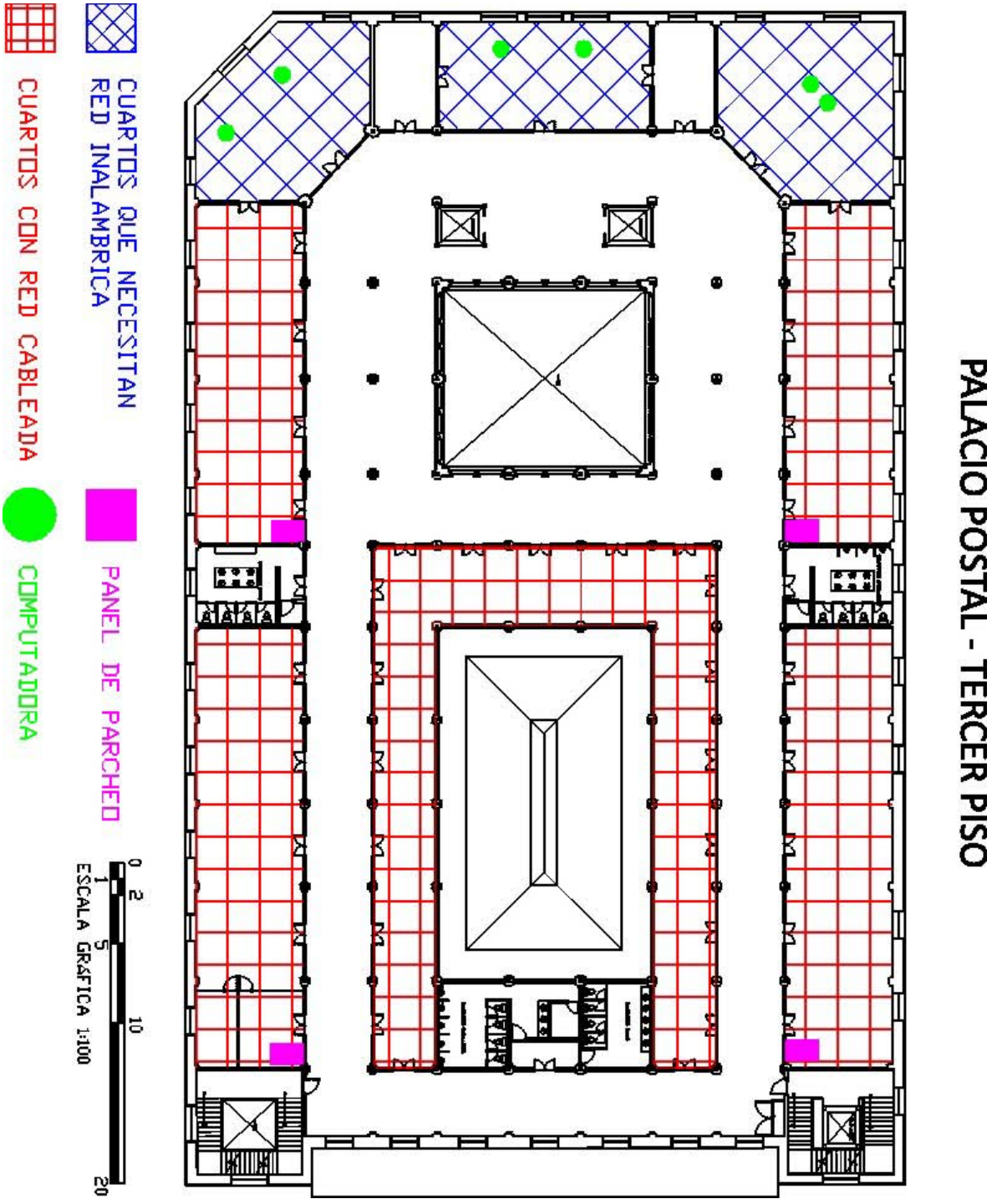
Las oficinas que necesitan la red inalámbrica así como la ubicación de los equipos se muestran en los planos 1 y 2.

Ninguna de las oficinas que se encuentran en el segundo piso tienen nodos de red instalados, por lo que la red debe iniciar desde algún nodo disponible en la red cableada, en cambio las oficinas del tercer piso cuentan con un nodo de red en cada una y es donde se encuentran los principales directores del palacio postal.

Una vez determinada la zona que necesita red, podemos definir la topología de red necesaria. Ya que en el segundo piso es necesaria una cobertura mayor que en el tercero, vamos a utilizar una topología WDS para conectar inalámbricamente varios puntos de acceso uno con otro y así incrementar la cobertura de la red. En el tercer piso se utilizará una topología BSS ya que solamente se necesitará instalar un punto de acceso en cada una de las oficinas para asegurar la comunicación apropiada. Para ambos casos se utilizará el estándar IEEE 802.11g con la velocidad máxima de 54 Mbps, con el algoritmo de seguridad WPA con AES.




*Plano 1. Oficinas que necesitan red inalámbrica y equipos en el segundo piso del palacio postal*




*Plano 2. Oficinas que necesitan red inalámbrica y equipos en el tercer piso del palacio postal*

Debido a que la gran mayoría de los dispositivos de telecomunicaciones que se utilizan en el palacio postal son de la marca 3Com, se decidió utilizar esta marca para los equipos necesarios para la red inalámbrica.

Los adaptadores de red que se utilizarán en los equipos de cómputo son adaptadores USB 3Com modelo 3CRUSB10075. Se utilizarán del tipo USB debido a que las computadoras no tienen espacio para instalar una tarjeta PCI.

*Fig. 4.18 Adaptador de red inalámbrica USB*

Las principales características del adaptador son:

| | |
|---|---|
| **Interfaces** | IEEE 802.11b/g |
| **Tasas de transferencia inalámbricas** | *802.11g*: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps<br>*802.11b*: 11, 5.5, 2 & 1 Mbps |
| **Técnicas de Modulación** | *802.11g*: DSSS/CCK, OFDM (Orthogonal Frequency<br>Division Multiplexing)<br>*802.11b*: DSSS/CCK (Direct Sequence Spread Spectrum/Complementary Code Keying) |
| **Canales** | 1-11 Norteamérica, 1-14 Japón, 1-13 Europa |
| **Potencia de transmisión** | *802.11g*: 17dBM (6, 9, 12, 18, 24, 36 Mbps), 15dBm (48, 54 Mbps)<br>*802.11b*: 19dBm |
| **Sensibilidad de recepción** | *802.11g*<br>54 Mbps: -70 dBm<br>48 Mbps: -71 dBm<br>36 Mbps: -76 dBm<br>24 Mbps: -80 dBm<br>18 Mbps: -83 dBm<br>12 Mbps: -86 dBm<br>9 Mbps: -87 dBm<br>6 Mbps: -87 dBm<br>*802.11b*<br>11 Mbps: -74 dBm<br>5.5 Mbps: -87 dBm<br>2 Mbps: -87 dBm<br>1 Mbps: -91 dBm |
| **Seguridad** | WPA con TKIP, 128-bit/192-bit/256-bit AES<br>WEP con cifrado de 64-bit/128-bit/256-bit |

*Tabla 4.4 Características de adaptador de red inalámbrica USB*

Los puntos de acceso serán 3Com modelo 7760. Sus principales características son:


*Fig. 4.19 Punto de Acceso (Access Point)*

| | |
|---|---|
| **Interfaces** | IEEE 802.11a/b/g<br>Un conector RJ-45 10BASE-T/100BASE-TX compatible con IEEE 802.3af PoE. |
| **Tasas de transferencia** | *802.11a/g* 54, 48, 36, 24, 18, 12, 9, 6 Mbps<br>*802.11b* 11, 5.5, 2, 1 Mbps |
| **Potencia de transmisión** | *802.11b/g*<br>1–11 Mbps: ≥+18 dBm<br>12 Mbps: ≥+18 dBm<br>18 Mbps: ≥+18 dBm<br>24 Mbps: ≥+18 dBm<br>36 Mbps: ≥+18 dBm<br>48 Mbps: ≥+16 dBm<br>54 Mbps: ≥+16 dBm |
| **Sensibilidad de recepción** | *802.11b/g*<br>1 Mbps: ≤-95 dBm<br>2 Mbps: ≤-92 dBm<br>5.5 Mbps: ≤-91dBm<br>6 Mbps: ≤-89 dBm<br>9 Mbps: ≤-88 dBm<br>11 Mbps: ≤-88 dBm<br>12 Mbps: ≤-86 dBm<br>18 Mbps: ≤-84 dBm<br>24 Mbps: ≤-81 dBm<br>36 Mbps: ≤-77 dBm<br>48 Mbps: ≤-73 dBm<br>54 Mbps: ≤-72 dBm |
| **Antenas** | 2 removibles con ganancia de 2dB<br>y conector R-SMA |

*Tabla 4.5 Características del Access Point*

Con los datos técnicos de los equipos que vamos a utilizar podemos hacer los cálculos para determinar la distancia máxima a la que se pueden ubicar.

Los cálculos se realizarán considerando el valor máximo de uno y dos muros medianos de obstrucción. No se considerarán pérdidas ambientales ya que no existen teléfonos inalámbricos o equipos que generen magnetismo o interferencias cerca del área de red.

## IV.8.1 Cálculos de alcance entre equipos

### IV.8.1.1 Cálculo 1

Cálculo de la distancia máxima considerando el punto de acceso como transmisor, y el adaptador de red como receptor con una obstrucción de 2 muros medianos.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del adaptador a 54 Mbps = -70 dBm
Gse = ganancia de salida del punto de acceso a 54 Mbps = 16dBm
Pce = pérdida por cable del punto de acceso =0dB
Pae = pérdida por conectores del punto de acceso = 0.25dB
Gae = ganancia de la antena del punto de acceso = 2dB
Gar = ganancia de la antena del adaptador = 0dB
Pcr = pérdida por cables del adaptador = 0dB
Par = Pérdida de los conectores del adaptador = 0dB
Pm = Pérdidas por muros = 13dBx2 = 26dB

Sustituyendo valores:

$$-70dB = 16dB - 0.25dB + 2dB - 26dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 61.75$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -38.25$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.9125$$

$$\frac{d}{1000} = 10^{-1.9125} = 0.01223$$

$$d = 12.23\ mts$$

### IV.8.1.2 Cálculo 2

Cálculo de la distancia máxima considerando el adaptador de red como transmisor, el punto de acceso como receptor y una obstrucción de 2 muros medianos.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del PA a 54 Mbps = -71 dBm
Gse = ganancia de salida del adaptador de red a 54 Mbps = 19dBm
Pce = pérdida por cable del adaptador de red =0dB
Pae = pérdida por conectores del adaptador de red = 0dB
Gae = ganancia de la antena del adaptador de red = 0dB
Gar = ganancia de la antena del punto de acceso = 2dB
Pcr = pérdida por cables del punto de acceso = 0dB
Par = Pérdida de los conectores del punto de acceso = 0.25dB
Pm = Pérdidas por muros = 13dBx2 = 26dB

Sustituyendo valores:

$$-71dB = 19dB + 2dB - 0.25dB - 26dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 65.75$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -34.25$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.7125$$

$$\frac{d}{1000} = 10^{-1.7125} = 0.01938$$

$$d = 19.38\ mts$$

Una vez hechos estos cálculos tomaremos la distancia menor y la redondearemos a un valor menor para asegurar una buena comunicación entre ambos dispositivos, por lo que tomaremos como distancia máxima 10 metros cuando existan 2 paredes obstruyendo la señal.

### IV.8.1.3 Cálculo 3

Cálculo de la distancia máxima considerando dos puntos de acceso y una obstrucción de 2 muros medianos.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del punto de acceso a 54 Mbps = -71 dBm
Gse = ganancia de salida de punto de acceso a 54 Mbps = 16dBm
Pce = Pcr = pérdida por cable del punto de acceso =0dB
Pae = Par = pérdida por conectores del punto de acceso = 0.25dB
Gae = Gar = ganancia de la antena del punto de acceso = 2dB
Pm = Pérdidas por muros = 13dBx2 = 26dB

Sustituyendo valores:

$$-71dB = 16dB - 0.5dB + 4dB - 26dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 64.5$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -35.5$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.775$$

$$\frac{d}{1000} = 10^{-1.775} = 0.01678$$

$$d = 16.78\ mts$$

### IV.8.1.4 Cálculo 4

Cálculo de la distancia máxima considerando el punto de acceso como transmisor, y el adaptador de red como receptor con una obstrucción de 1 muro mediano.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del adaptador a 54 Mbps = -70 dBm
Gse = ganancia de salida del punto de acceso a 54 Mbps = 16dBm
Pce = pérdida por cable del punto de acceso = 0dB
Pae = pérdida por conectores del punto de acceso = 0.25dB
Gae = ganancia de la antena del punto de acceso = 2dB
Gar = ganancia de la antena del adaptador = 0dB
Pcr = pérdida por cables del adaptador = 0dB
Par = Pérdida de los conectores del adaptador =0dB
Pm = Pérdidas por muro = 13dB

Sustituyendo valores:

$$-70dB = 16dB - 0.25dB + 2dB - 13dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 74.5$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -25.25$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.2625$$

$$\frac{d}{1000} = 10^{-1.2625} = 0.05463$$

$$d = 54.63\ mts$$

### IV.8.1.5 Cálculo 5

Cálculo de la distancia máxima considerando el adaptador de red como transmisor, el punto de acceso como receptor y una obstrucción de 1 muro mediano.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del punto de acceso a 54 Mbps = -71 dBm
Gse = ganancia de salida del adaptador de red a 54 Mbps = 19dBm
Pce = pérdida por cable del adaptador de red =0dB
Pae = pérdida por conectores del adaptador de red = 0dB
Gae = ganancia de la antena del adaptador de red = 0dB
Gar = ganancia de la antena del punto de acceso = 2dB
Pcr = pérdida por cables del punto de acceso = 0dB
Par = Pérdida de los conectores del punto de acceso =0.25dB
Pm = Pérdidas por muros = 13dB

Sustituyendo valores:

$$-71dB = 19dB + 2dB - 0.25dB - 13dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 78.75$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -21.25$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.0625$$

$$\frac{d}{1000} = 10^{-1.0625} = 0.8659$$

$$d = 86.59\ mts$$

Igual que en los primeros cálculos consideraremos la distancia menor y la redondearemos a su valor menor para asegurar una buena comunicación entre ambos dispositivos; así que tomaremos como distancia máxima 50 metros cuando solo exista 1 pared obstruyendo la señal.

### IV.8.1.6 Cálculo 6

Cálculo de la distancia máxima considerando dos punto de acceso y una obstrucción de 1 muro mediano.

*Fórmulas:*

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pm$$

$$Pp = 20\log_{10}\left(\frac{d}{1000}\right) + 100$$

*Datos:*

Sr = sensibilidad del punto de acceso a 54 Mbps = -71 dBm
Gse = ganancia de salida de punto de acceso a 54 Mbps = 16dBm
Pce = Pcr = pérdida por cable del punto de acceso =0dB
Pae = Par = pérdida por conectores del punto de acceso = 0.25dB
Gae = Gar = ganancia de la antena del punto de acceso = 2dB
Pm = Pérdidas por muros = 13dB

Sustituyendo valores:

$$-71dB = 16dB - 0.5dB + 4dB - 13dB - \left(20\log_{10}\left(\frac{d}{1000}\right) + 100\right)$$

$$20\log_{10}\left(\frac{d}{1000}\right) + 100 = 77.5$$

$$20\log_{10}\left(\frac{d}{1000}\right) = -22.5$$

$$\log_{10}\left(\frac{d}{1000}\right) = -1.125$$

$$\frac{d}{1000} = 10^{-1.125} = 0.07498$$

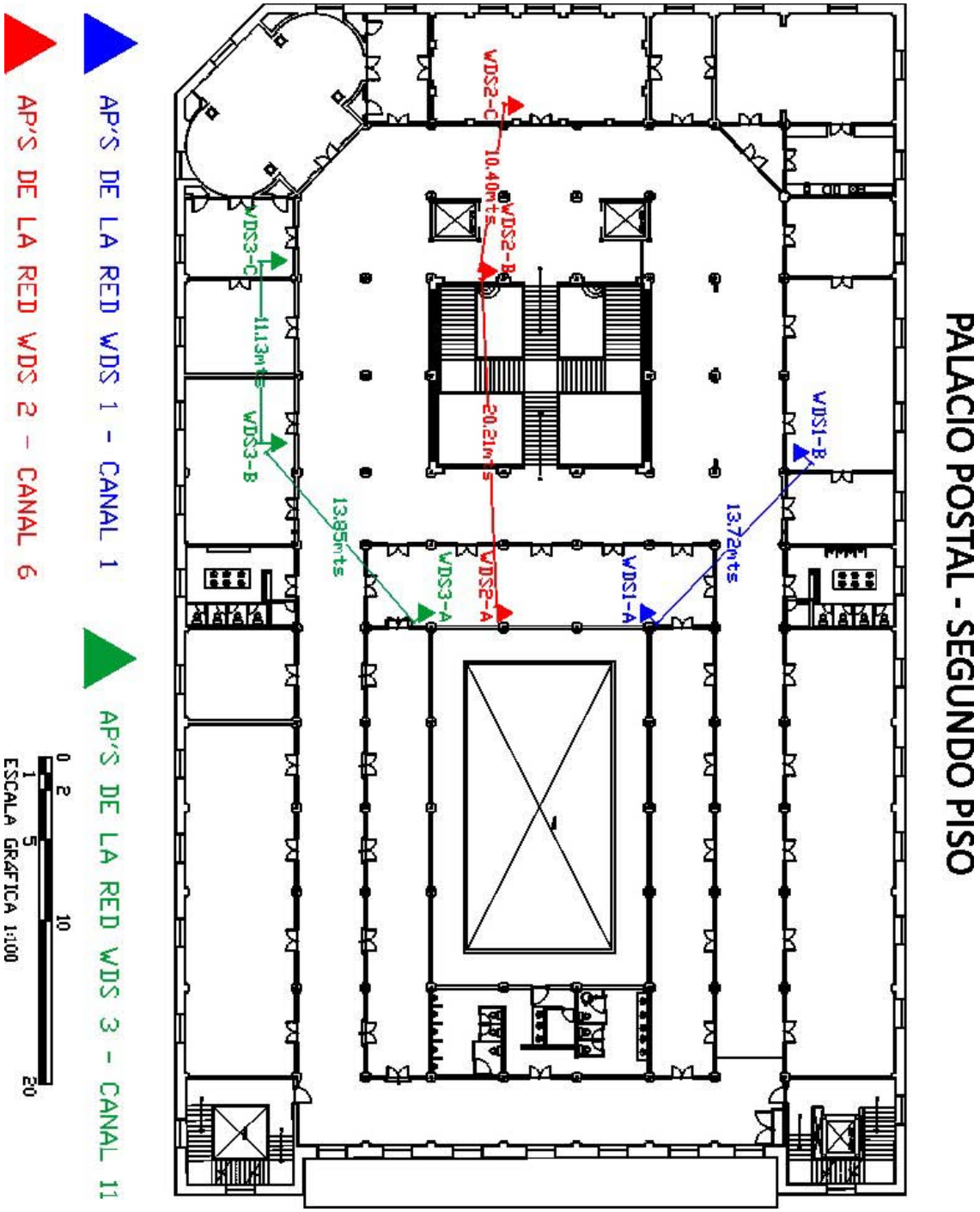
$$d = 74.98\ mts$$

Una vez realizados todos los cálculos necesarios podemos juntar los resultados en una tabla para utilizarla como referencia:

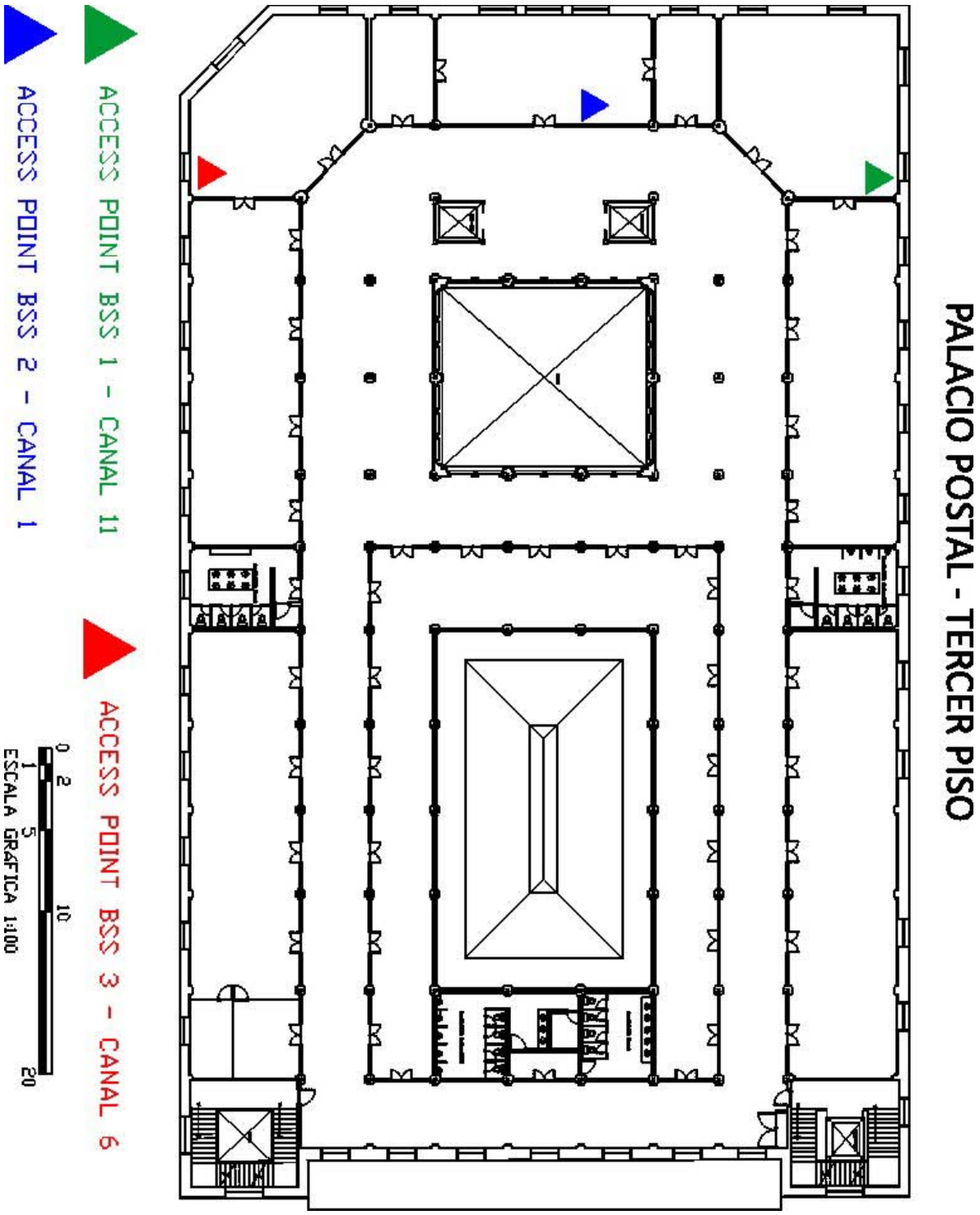
| Señal entre equipos | Obstrucción | Distancia máxima |
|---|---|---|
| punto de acceso - adaptador de red | 2 muros | 10 metros |
| punto de acceso - adaptador de red | 1 muro | 50 metros |
| punto de acceso - punto de acceso | 2 muros | 15 metros |
| punto de acceso - punto de acceso | 1 muro | 70 metros |

*Tabla 4.6 Resultados de alcance entre equipos*

Con estos datos podemos ubicar el lugar donde se instalarán los puntos de acceso. Debido a la atenuación entre 2 muros disminuye la distancia de enlace, se decidió crear 3 redes WDS para el segundo piso independientes una de otra. Cada una de estas redes tendrá canales de transmisión distintos pero entre los puntos de acceso que conformen la red el canal será el mismo. Las ubicaciones de los puntos de acceso y la distancia entre ellos pueden verse en los planos 3 y 4.




*Plano 3. Ubicación de los puntos de acceso en el segundo piso del Palacio Postal*

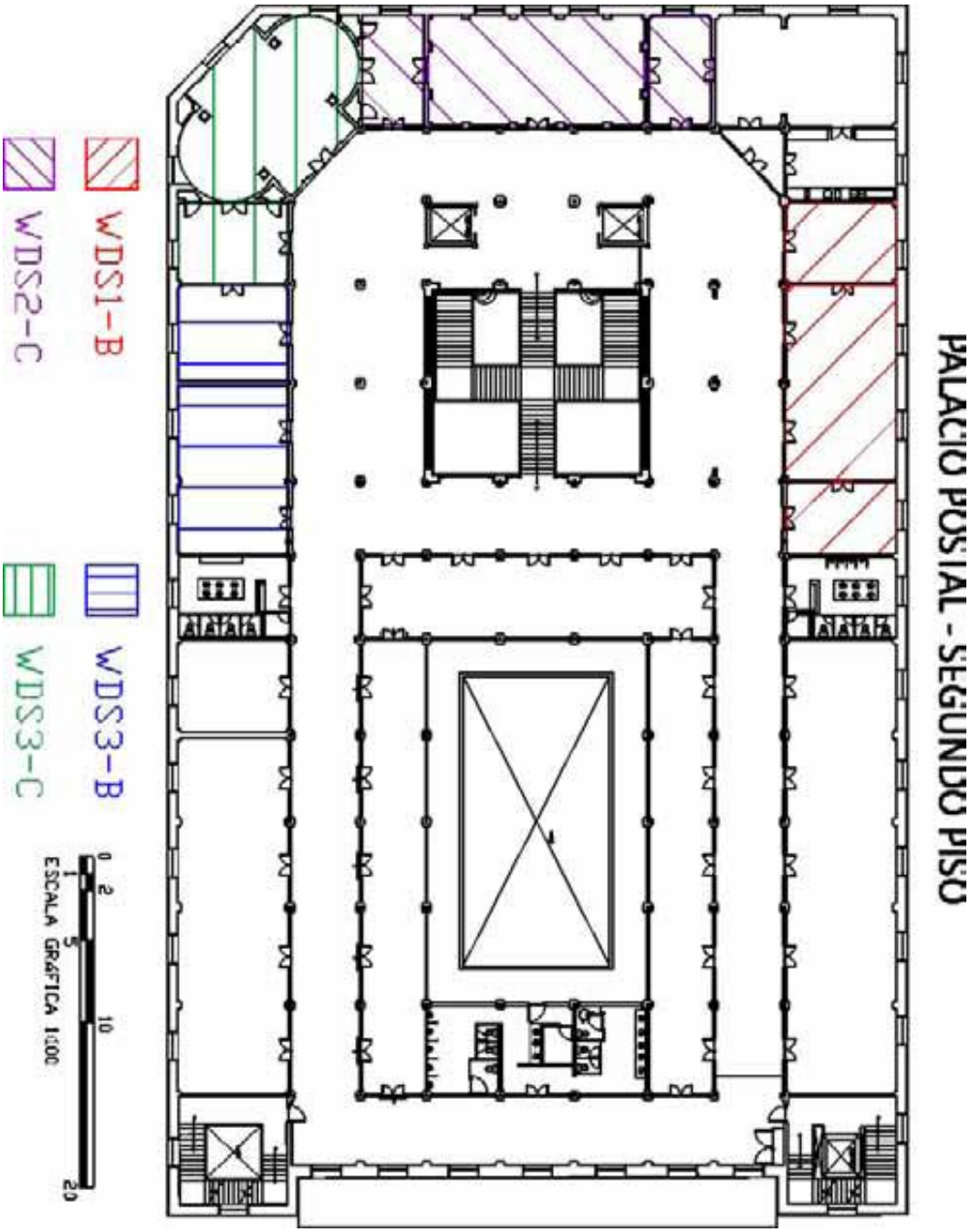



*Plano 4. Ubicación de los puntos de acceso en el tercer piso del Palacio Postal*

Los AP's "WDS1-A", "WDS2-A" Y WDS3-A" se encuentran en una sala con red cableada y únicamente se utilizarán para dar servicio a los siguientes puntos de acceso.

Todos los puntos de la red inalámbrica WDS1 tendrán el canal 1, para la red WDS2 usarán el canal 6 y la red WDS3 el canal 11.

La forma en que las oficinas tendrán cobertura de las redes en el segundo piso se muestra en el plano 5.




*Plano 5. Cobertura de los puntos de acceso en las oficinas del segundo piso*

El SSID debe ser la misma para puntos de acceso que sean parte de la misma red WDS, por lo que en la red WDS1 los puntos de acceso tendrán la SSID “2PISOWDS1”, para la red WDS2 los SSID serán “2PISOWDS2” y para la WDS3 serán “2PISOWDS3”.

Para el tercer piso el punto de acceso BSS1 utilizará el canal 11 y tendrá el SSID “3PISOBSS1”, el BSS2 tendrá el canal 1 y el SSID “3PISOBSS2” y el BSS3 el canal 6 y el SSID “3PISOBSS3”. En todos los casos se deshabilitará la emisión de SSID para evitar que la personas ajenas a la red puedan encontrarla y así aumentar la seguridad, aunque durante la etapa de instalación de los adaptadores de red permanecerá activa para facilitar la configuración de la red.

Las direcciones IP en toda la red son estáticas por lo que en los puntos de acceso se desactivará el servidor DHCP y se les asignará manualmente la dirección IP conforme a las direcciones disponibles que son dadas por los administradores de la red. La máscara de subred, puerta de enlace y servidores DNS son las mismas para todos los equipos.

| PUNTO DE ACCESO | DIRECCION IP | MASCARA DE SUBRED | PUERTA DE ENLACE | SERVIDOR DNS 1 | SERVIDOR DNS 2 |
|---|---|---|---|---|---|
| WDS1-A | 7.10.8.44 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS1-B | 7.10.8.45 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS2-A | 7.10.8.46 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS2-B | 7.10.8.47 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS2-C | 7.10.8.48 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS3-A | 7.10.8.49 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS3-B | 7.10.8.50 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| WDS3-C | 7.10.8.51 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| BSS1 | 7.10.8.112 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| BSS2 | 7.10.8.113 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |
| BSS3 | 7.10.8.114 | 255.255.0.0 | 7.10.8.100 | 7.10.8.1 | 7.10.8.10 |

*Tabla 4.7 Configuración de direcciones de los puntos de acceso*

Como se mencionó anteriormente, la clave de seguridad en los equipos será WPA con algoritmo AES; la clave será escogida por los administradores de red considerando que los puntos de acceso de cada red WDS deben tener la misma clave.

Para agregar mayor seguridad de utilizara filtrado de direcciones MAC, ingresando en cada punto de acceso las direcciones MAC de los adaptadores de red que se conectarán a ellos. Cabe recordar que cada equipo de red tiene una clave MAC única e irrepetible por lo que si es necesario cambiar algún dispositivo se tendrá que modificar la tabla de filtrado de MAC en los equipos necesarios.

Para los equipos que se encuentran en el segundo piso es necesario habilitar el uso de la red WDS, cuando se activa se debe introducir el protocolo de tipo punto a punto (PPP) en todos los puntos de acceso menos en “WDS2-B” y “WDS3-B” los cuales el protocolo será punto a multipunto (PTMP) ya que cada uno establecerá comunicación con 2 puntos de acceso. Después será necesario introducir la dirección MAC del(los) dispositivo(s) al(los) que se va a conectar cada uno

de los puntos de acceso, en la siguiente imagen se puede observar la configuración que llevará cada uno:

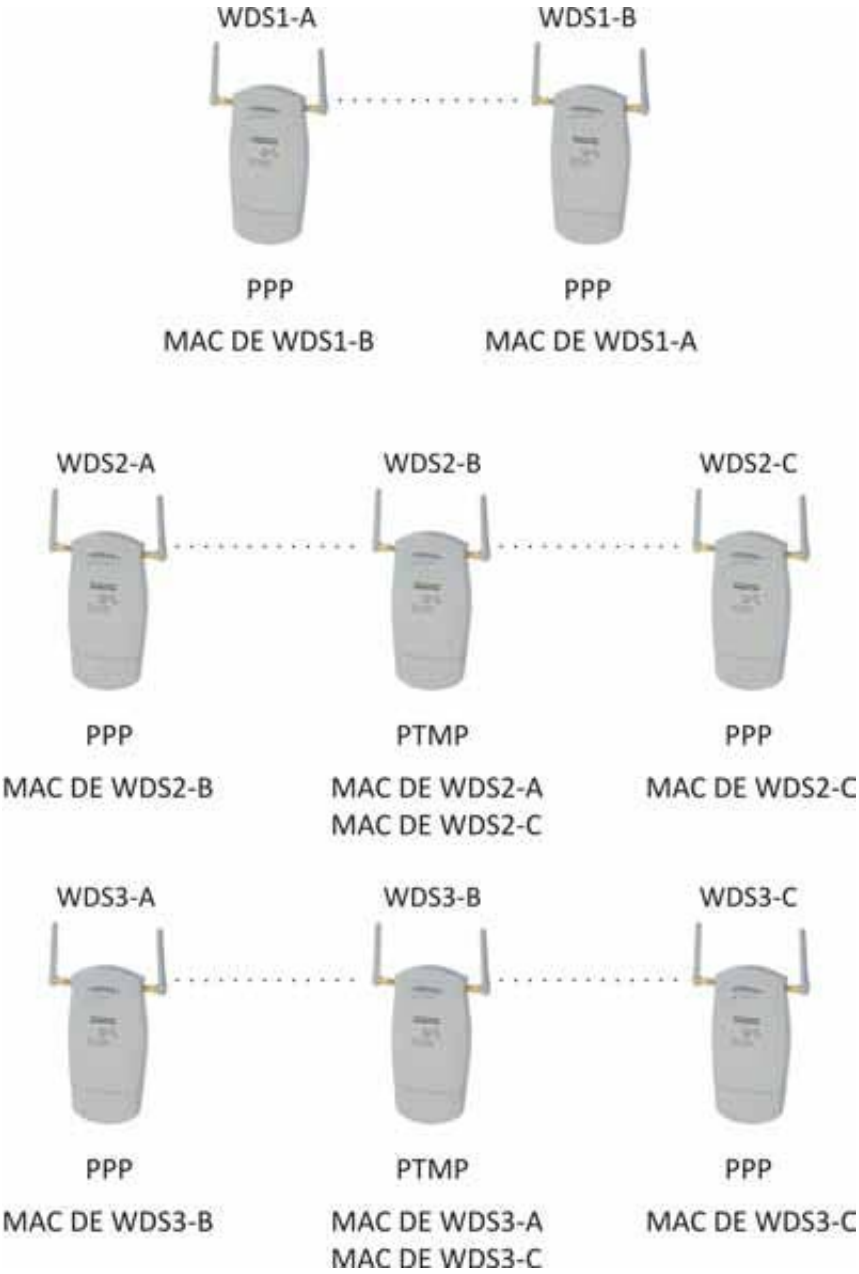



*Fig. 4.20 Protocolos y direcciones MAC de los puntos de acceso de las redes WDS*

La configuración de los adaptadores de red es muy sencilla. Después de haberlos instalado en las máquinas que utilizarán la red, debemos realizar una búsqueda de las redes inalámbricas existentes en el área aprovechando que los puntos de acceso están transmitiendo su SSID en este momento. Después de encontrar la red a la que nos vamos a conectar hay que introducir la clave de red WPA que corresponde. Una vez que la conexión se realice exitosamente, hay que ingresar la dirección IP, máscara de subred y puerta de enlace necesarias. Los equipos que se encuentran en el segundo piso pueden utilizar las direcciones IP que se encuentran entre el rango de 7.10.8.52 y 7.10.8.74, mientras que las computadoras del tercer piso podrán tener direcciones IP entre 7.10.8.115 y 7.10.8.128. La máscara de subred y la puerta de enlace y servidores DNS continuarán siendo las mismas que para los puntos de acceso.

Una vez terminada la instalación y configuración de los equipos habrá que probar las conexiones para comprobar que todo funcione correctamente.

Los costos de todos los equipos y de la instalación se muestran en las siguientes tablas:

| Marca | Modelo | Descripción | Precio Unitario | Cantidad | Total |
|---|---|---|---|---|---|
| 3Com | 7760 | Access Point compatible con WDS | $ 2,250.00 | 11 | $ 24,750.00 |
| 3Com | 3CRUSB10075 | Adaptador de red USB 802.11b/g | $700.00 | 26 | $ 18,200.00 |
| | | | | **TOTAL** | **$ 42,950.00** |

| Costo de mano de obra por nodo | Cantidad de nodos | Costo total de mano de obra |
|---|---|---|
| $800.00 | 26 | **$20,800.00** |

**Costo Total de la Red: $63,750.00**

*Tabla 4.8 Costo de instalación del Proyecto de Red Inalámbrica*

# CONCLUSIONES

Después de haber realizado la planeación del provecto hemos encontrado ventajas y desventajas de una red inalámbrica en comparación con una red cableada. Algunas de estas diferencias son:

## Ventajas de una red inalámbrica

**Movilidad:** Una de las mayores ventajas de las redes inalámbricas es la libertad de desplazamiento. Una computadora o cualquier otro dispositivo pueden situarse en cualquier punto dentro de la cobertura de la red sin tener que depender de instalar o reubicar un cable hasta ese sitio, lo que hace más fácil cualquier reubicación que se llegase a requerir en el futuro.

**Desplazamiento:** Los usuarios que posean una computadora portátil no tienen la posibilidad de acceder a internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina, sino que pueden desplazarse sin perder la comunicación dentro del rango de cobertura.

**Flexibilidad:** Esto permite que los equipos de la red puedan ser colocados en cualquier lugar sin hacer el más mínimo cambio en la configuración de la red. También permite que agregar equipos adicionales sea una tarea más sencilla evitando situaciones indeseables como la colocación de cables en el suelo para evitar tener que poner enchufes de red más cercanos. Las redes inalámbricas también permiten que los invitados que necesiten conexión a Internet puedan obtenerla de una manera muy sencilla, especialmente en zonas públicas (centros de formación, hoteles, cafés, entornos de negocio o empresariales, etc.)

**Escalabilidad:** Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Para una red inalámbrica la escalabilidad es más sencilla que para una red cableada. En la primera basta con conectar un adaptador de red y configurarlo, mientras que para el segundo caso es necesario instalar un nuevo cableado o, lo que es peor, esperar hasta que el nuevo cableado quede instalado. Al haber realizado una red inalámbrica nos aseguramos que sea más fácil la expansión de ésta si en algún momento es necesario conectar más equipos.

## Inconvenientes de una red inalámbrica

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tienen algunos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes son:

**Menor ancho de banda:** Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 54 Mbps, esto es casi la mitad de la velocidad y cuando existen muchos usuarios se puede congestionar el tráfico de la red.

**Mayor inversión inicial:** La instalación de una red inalámbrica implica la adquisición de puntos de acceso y adaptadores de red inalámbricos, los cuales son de un precio mayor en comparación con dispositivos para red cableada. También puede ser necesaria la compra de equipos de red Ethernet si la red es grande (routers y switches).

**Seguridad:** Debido a que las redes inalámbricas no necesitan un medio físico para funcionar, tienen el inconveniente de que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura para intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro del edificio o estar conectado a un cable. Es por eso que hay que ser muy cuidadosos al momento de configurar la seguridad de una red inalámbrica.

**Interferencias:** Las redes inalámbricas funcionan utilizando el medio radioeléctrico en la banda de 2.4GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencia, incluidas las redes vecinas. Este hecho hace que no se tenga la garantía de que nuestro entorno radioeléctrico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan ya que las técnicas de modulación ayudan a reducir la interferencia.

Aún con todas las desventajas con las que cuentan las redes inalámbricas, algunas de ellas pueden llegar a ser controladas mediante configuraciones y colocación de los equipos. Su implementación se está convirtiendo una práctica cada vez más común ya que sus ventajas son aún mayores y los costos de instalación se han ido reduciendo cada día más.

Por otra parte, la oportunidad que tuvimos para poder realizar de este proyectó fue de mucha utilidad ya que nos permitió poner en práctica muchos de los conocimientos que adquirimos durante nuestra carrera y nos dimos cuenta que, aunque conocemos la teoría, ponerla en práctica es muy diferente ya que pueden surgir problemas con los que no contamos o que ni siquiera conocemos, es por esto que hace falta mayor preparación práctica en los laboratorios de la escuela, especialmente con tecnologías nuevas y que cada vez tienen mayor popularidad como es el caso de las redes inalámbricas.

# BIBLIOGRAFÍA

Uyless Black, *Redes de computadores Protocolos, Normas e interfaces*, segunda edición, RA-MA Editorial. 1997. Madrid España 674 págs.

Jorge Lázaro Laporta, Marcel Miralles Aguiñiga. *Fundamentos de Telemática*. RA-MA Editorial. 2004. Valencia España. 408 págs.

Stallings William. *Comunicaciones y Redes de Computadores*. Sexta Edición. Editorial Prentice Hall. 2000. Madrid España. 747 págs.

Michael A. Gallo, William M. Hancock. *Comunicación entre computadoras y tecnología de redes*. Editorial Thompson. 2002. México. 632 págs.

Jesús García Tomás, José Luis Raya Cabrera, Víctor Rodrigo Raya. *Alta velocidad y calidad de servicio en Redes IP*. Editorial RA-MA. 2002. Madrid España. 674 págs.

Roldan Martínez David; *Comunicaciones Inalámbricas: Un enfoque aplicado*, RA-MA Editorial, Madrid España, 2005. 383 págs.

Carballar Falcón José Antonio, *WI-FI: Cómo construir una red inalámbrica 2ª Edición*, RA-MA Editorial, Madrid España 2005, 272 págs.

Molina Robles Francisco José, *Redes de Área Local*, RA-MA Editorial 2004, Madrid España, 549 págs.

Raya José Luis, Raya Cristina; *Redes locales*, RA-MA Editorial 2002, Madrid España, 347 págs.

Huidobro Moya José Manuel; *Comunicaciones en Redes WLAN, WiFi, VoiP, Multimedia, Seguridad*; Editorial Limusa, 2006 México; 356 págs.

McQuerry Steve; *Interconexión de dispositivos de red Cisco*; Ed. Pearson Educación S.A., Madrid España, 2001, 568 págs.

Held Gilbert ; *Wireless Mesh Networks*, Ed. Auerback Publications, U.S.A., 2005, 159 págs.

## Referencia Electrónica

http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202004-3/tecn_red_acceso_OFDM.doc

http://www.eveliux.com/articulos/estandareswlan.html

http://www.cisco.com/en/US/docs/wireless/access_point/1200/vxworks/configuration/guide/bkscgaxa.html

http://www.tutorial-reports.com/wireless/wlanwifi/introduction_wifi.php

http://standards.ieee.org/getieee802/802.11.html

http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm

http://www.monografias.com/trabajos13/modosi/modosi.shtml

http://elsitiodetelecomunicaciones.iespana.es/modelo_osi.htm

http://carinalusso.iespana.es/modelo_de_referencia_de_intercon.htm

http://www.mailxmail.com/curso/informatica/redes/capitulo4.htm

http://www.geocities.com/Athens/Olympus/7428/red3.html

http://www.geocities.com/Athens/Olympus/7428/red1.html

http://www.pcdoctor.com.mx/Radio%20Formula/temas/Redes.htm

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

http://www.htmlweb.net/redes/topologia/topologia_2.html

http://www.bloginformatico.com/topologia-de-red.php

http://www.geocities.com/TimesSquare/Chasm/7990/topologi.htm

http://hwagm.elhacker.net/calculo/calcularalcance.htm

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/d1e53415-9a93-4407-87d2-3967d62182dc.mspx?mfr=true

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

http://www.newdevices.com/tutoriales/modelo-tcpip/2.html

http://www.ipv6.org/

http://www.configurarequipos.com/doc527.html

http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

http://www.saulo.net/pub/inv/SegWiFi-art.htm

http://www.red.com.mx/scripts/redArticulo.php3?idNumero=70&articuloID=7483

http://documentos.shellsec.net/otros/SeguridadWireless.pdf

http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/

http://www.alcancelibre.org/article.php?story=20070404112747533

http://blog.unlugarenelmundo.es/2006/04/07/%C2%BFson-seguras-las-redes-wi-fi/

http://support.microsoft.com/kb/815485/es

http://www.mailxmail.com/curso/informatica/wifi/capitulo4.htm

http://www.monografias.com

http://www.maestrosdelweb.com/principiantes/hardware/

http://www.hyperlinktech.com/web/antennas.php

http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml

http://www.tecnowimax.com/

http://www.3com.com/

http://www.netkrom.com/es/sol_wisp.html

http://www.evcomstore.cl/vitrina/fotos/576_TG-49.jpg

http://www.ciudadwireless.com/images/DI-524UPCW.jpg

http://es.wikipedia.org/wiki/Red_inalambrica_Mesh

http://criadoindomable.wordpress.com/2008/01/24/pruebas-realizadas-sobre-la-red-mesh/

http://www.hyperlinktech.com/web/specials.php

http://www.radioptica.com/Radio/caracteristicas_estandar_wimax.asp

http://www.directorio.com.mx/wimax/#por

http://www.cipmobile.net/

http://www.wilac.net/tricalcar

http://www.jazztel.com

http://www.microsoft.com/spain/technet/recursos/articulos/wifisoho.mspx#E5B

http://www.instantbyte.com/wireless.htm

http://www.riskinformatica.com/