UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

# Adecuación de la RIU: Red Inalámbrica dentro de la FES Aragón

**T E S I S**

QUE PARA OBTENER EL TÍTULO DE

I N G E N I E R A E N C O M P U T A C I Ó N

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

**LUCILA MARICELA CERVANTES LUNA**

ASESOR:

ING. ROBERTO BLANCO BAUTISTA


MÉXICO 2014

Si ante la insistente gota de agua,

la roca se perfora,

ante la tenacidad del hombre:

la palabra imposible, ¡se evapora!

José Luis Jiménez

## DEDICATORIA:

A ti Chucho, así te llamo no por falta de respeto, sino por la confianza y cercanía que siento contigo cada segundo de mi vida, por ser el hermoso vínculo que tenemos los mortales con tu padre, el creador y fuente de amor. Todos los días siento tu amor y el de él. Yo también los amo con todas mis fuerzas.

A mis padres, por ser el instrumento del Creador para darme la vida, además de otorgarme todo su amor y por estar conmigo desde el primer día de mi existencia. Son mi ejemplo de vida. Los amo.

A mi hermana, por ser mi cómplice y mi amiga, mi primer ídolo cuando fui niña (tú no lo sabías, pero fui tu fan). Sé que soy bendecida porque eres una extensión del amor que mis padres me dan todos los días. Te amo, Ame.

# AGRADECIMIENTOS:

A Dios Padre y a su hijo por dejarme concluir un pendiente que tenía en la vida, por darme todos los bellos instrumentos necesarios para poder hacerlo. Y sobre todo por cuidar tanto mi camino y ponerme en el momento justo, con las personas ideales. Mil gracias por ser el motor mi existencia.

A ti mamá, no tengo palabras para agradecerte todo lo que has hecho por mí, tu sacrificio y la devoción con la que me has cuidado desde siempre. Tú has sido mi mejor maestra, la lecciones que he aprendido de ti serán mis herramientas para esta vida; debes estar contenta porque tu obra ha sido buena. Sin ti no hubiera podido materializar mis sueños. Gracias por ser la mejor mamá del mundo.

A ti papá, gracias por todo lo que me has dado en la vida. Aún recuerdo cuando ibas por mí al kínder y en la salida me comprabas un "Mamut", el cual me sabía a gloria y ahora, en mi vida adulta, se convierte en el sabor de esos maravillosos momentos a tu lado. Desde siempre he sabido que puedo contar contigo, pues lo único que he recibido de ti es cariño; además, cuando he necesitado un aliado y cómplice te he tenido a ti. Gracias por ser mi papá.

A mi hermana. Ame, recordado un poco mi paso por la vida, has estado presente todo el tiempo; me llegan los momentos en los que me has tendido la mano, porque cuando he necesitado algo siempre estás para mí. Te debo mucho, si no fuera por ti jamás habría llegado hasta aquí. Gracias Ame y discúlpame por todo lo que te he quedado a deber. Eres una maravillosa mujer y estoy muy orgullosa de que seas mi hermana.

A Vic, de verdad que cuando te conocí jamás creí que alguien que no fuera de mi sangre representaría tanto en mi vida; muchas gracias por ser mi amigo y compañero de vida, sé que siempre que te necesito estás a mi lado. Te doy las gracias por enseñarme a valerme por mí misma, sin depender de nadie; no sabes el bien que me has hecho. Ahora tú y yo comenzaremos a caminar juntos en la gran aventura de nuestra vida. Es un placer tenerte a mi lado y caminar de la mano contigo.

A ustedes, mis hermosas princesas y mi bebé, lo único que he recibido de ustedes es el amor más puro y sincero que he encontrado, han sido mis excelentes maestros. Los amo mis pequeños guerreros. Gracias mis chaparritos bellos.

A ti Laura, por ser mi amiga y compañera de aventuras; aún recuerdo la fría mañana en la que te conocí y dije "que chava tan rara", sin saber que serías pieza importante en mi paso por la Tierra, gracias amiga porque sé que cuando he necesitado de alguien tu hombro ha sido el apoyo para levantarme. Nuestra amistad ha sido única; creo que si existe otra vida nos volveremos a encontrar y seremos amigas otra vez. Te quiero Lau.

A mi asesor Roberto Blanco Bautista. No sé cómo darle las gracias por ayudarme a terminar este pendiente que tenía en la vida. Si en el mundo existieran más personas como usted todo sería muy diferente. Mil gracias maestro.

A los Muñoz, quienes -sin saberlo- han sido parte importante en muchas etapas de mi vida y ésta no podría ser la excepción. Gracias a ustedes mi existencia ha sido como un musical.

Y a cada una de las personas que de alguna u otra forma me han ayudado en este camino, pues me han enseñado cosas valiosas que son las armas que me han ayudado para librar las batallas de esta vida, las que no son fáciles, pero sé que estoy rodeada de gente maravillosa en la que puedo confiar. Un millón de gracias a cada uno de ustedes.

# ÍNDICE

## Capítulo 3: Red Inalámbrica Universitaria (RIU)



## Capítulo 4: Mejoras estructurales de RIU



## Anexo

# INTRODUCCIÓN

Desde que el hombre pisó el mundo tuvo la necesidad de comunicarse: primero entre gente de su misma comunidad, después con personas de lugares más remotos. De esa forma el ser humano trabajó para poderse relacionar y compartir información con gente de otros países y/o continentes.

Con el fin de satisfacer y optimizar la necesidad de comunicación, el hombre puso especial interés en el desarrollo de las tecnologías para que fueran más eficaces y ágiles. Con el paso del tiempo, la sociedad no sólo se ha beneficiado de ellas, sino que se han hecho indispensables.

En la vida cotidiana muchas herramientas se han desarrollado para facilitar el trabajo a la sociedad. Parecen no muchos ayeres desde que la humanidad aprendió a escribir; posteriormente nació la imprenta, inventó la máquina de escribir hasta llegar a lo que hoy conocemos como computadora. Si hacemos una cronología nos podemos dar cuenta que en realidad la evolución de las tecnologías se ha dado a pasos agigantados.

La visión de la comunicación entre máquinas se vio transformada con el uso de las redes, éstas se han ido acrecentando junto con el uso de equipos de cómputo, los cuales son ahora una herramienta a la que la mayoría de las personas puede tener acceso.

Junto con la evolución de las tecnologías también ha crecido la necesidad de la movilidad, la solución a esto es la implementación de redes inalámbricas. Las redes inalámbricas facilitan la conectividad en lugares donde la computadora no puede permanecer en un solo lugar, como en el caso de las escuelas en donde los alumnos -debido a sus distintas materias- necesitan desplazarse dentro del plantel.

A causa del incremento de equipos móviles con tecnología inalámbrica, muchas escuelas (incluida la UNAM) se vieron en la necesidad de implementar sus propias redes inalámbricas; de ahí nació el proyecto de RIU (Red Inalámbrica Universitaria).

Y de RIU nace este trabajo, ya que me parece importante dar a conocer cómo surgió y cómo funciona esta herramienta; de hecho podría decir que se convirtió en algo indispensable para los alumnos de la comunidad. Y no únicamente para ellos, porque otros sectores de la población -como son académicos y administrativos- se ven beneficiados por RIU, siempre y cuando cuenten con dispositivos móviles adecuados para aprovechar la red.

A lo largo de este trabajo se abordarán puntos que son indispensables para comprender el funcionamiento de las redes inalámbricas y en caso particular la RIU. Como primer capítulo se manejarán conceptos básicos, tales como: ¿Qué es una red inalámbrica?, topologías, configuración y entornos de instalación.

Para poder entender cómo funcionan las redes inalámbricas, el segundo capítulo muestra los protocolos y estándares que nos garantizan la funcionabilidad y seguridad al momento de navegar en la red.

Teniendo en claro estos conceptos, el tercer capítulo da paso por completo a lo que es RIU, tanto en el ambiente en el que se implementó, como en los datos importantes para el usuario que le ayudarán a comprender la importancia de esta tecnología en nuestra Facultad.

Desde mi punto de vista no todo es perfecto, las cosas se pueden mejorar, por esto en el cuarto y último capítulo me permito dar algunas recomendaciones para poder explotar de una manera más eficaz las bondades de esta red y para que los usuarios lo aprovechen al máximo.

En el tiempo que llevo trabajando con RIU he detectado diferentes situaciones por las que pasa el usuario, cuando está en óptimas condiciones el equipo la conexión es fácil para que el mismo pueda loguearse, cuando no es así, asiste al departamento de informática a recibir asistencia técnica y es aquí en donde he podido detectar diferentes problemas que impiden el uso de la red. Al tratar de dar solución a cada caso, explorando el equipo para detectar algún detalle que impida el buen funcionamiento del equipo con respecto a su conexión inalámbrica, he considerado importante hacer mención de esto en un anexo.

Esperando que mi trabajo y experiencia sea de utilidad para los usuarios de RIU o para todo aquel que le interese saber un poco más sobre las redes inalámbricas, doy pie al contenido de esta tesis.

# CAPÍTULO 1

## REDES LOCALES INALÁMBRICAS

# CAPÍTULO 1: REDES LOCALES INALÁMBRICAS

## 1.1 ¿QUÉ SON LAS REDES LOCALES INALÁMBRICAS?

Una WLAN (Wireless Local Area **Network**) o red local inalámbrica, puede definirse como una red que funciona en un lugar específico de trabajo, ésta utiliza tecnología de radiofrecuencia para conectar a los equipos de los usuarios, sin que lo estén físicamente. De esta forma los datos (paquetes de información) se transmiten por el aire, permitiendo al usuario mayor movilidad dentro de su entorno de trabajo.

Dicho de otra manera: las redes inalámbricas utilizan **ondas electromagnéticas** como medio de transmisión, para que viaje la información a través del canal inalámbrico, enlazando equipos o terminales móviles asociados a la red.

## 1.2 EVOLUCIÓN DE LAS REDES INALÁMBRICAS

Todo lo que existe en nuestro entorno tiene un ciclo de vida, inclusive las herramientas con las que contamos en la actualidad, y las redes inalámbricas no son la excepción. El origen de las WLAN se remonta al año de 1979, cuando se publicaron los resultados de un experimento realizado por ingenieros de **IBM** en Suiza; éste consistía en usar enlaces infrarrojos para crear una red local en una fábrica. A dicho avance se le consideró como el punto de partida para la evolución de las redes inalámbricas.

Posteriormente se siguieron haciendo pruebas en laboratorios en donde utilizaron altas frecuencias. Llegó 1985 y junto con ese año la Federal Communication Comission (FCC, agencia federal de EEUU encargada de regular y administrar las telecomunicaciones) asignó una serie de bandas al uso de IMS (Industrail, Scientific and Medical). Esto dio como resultado un mayor interés por la LAN (red inalámbrica de alcance local), tanto de la industria como de la investigación. Lo cual quiere decir que sus ojos voltearon al mercado. Para 1991 se publicaron los primeros trabajos de LAN, ya que -según la norma **IEEE** 802- sólo se consideran así, las redes que transmiten al menos a 1 **Mbps**.

Las redes inalámbricas -como las conocemos actualmente- ya existían, pero su introducción en el mercado y su implementación en los hogares o a nivel laboral aún tardó años. Algunas de las circunstancias que las llevaron a tener mayor importancia, fueron: la llegada de tecnología inalámbrica como las laptops, tablets y teléfonos, lo que propicio que la sociedad exigiera conectarse a la red sin cables.

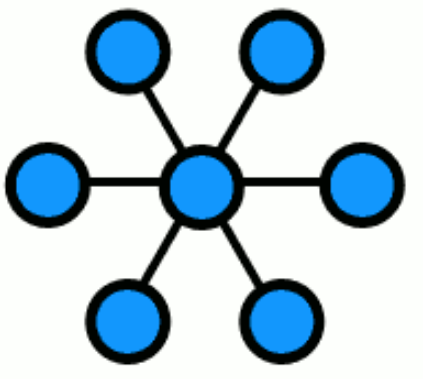
## 1.3 TOPOLOGÍAS BÁSICAS DE RED

### 1.3.1 Estrella

En una topología de *estrella*, las computadoras en la red se conectan a un dispositivo central conocido como **concentrador** (***hub*** en inglés) o a un **conmutador** de paquetes (***swith***, también en inglés).

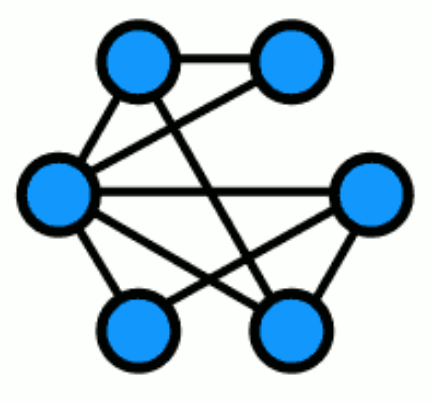
En un ambiente LAN cada computadora se conecta con su propio cable (típicamente par trenzado) a un puerto del ***hub*** o *switch*. Este tipo de red sigue siendo pasiva, utilizando un método basado en contención; las computadoras escuchan el cable y contienden por un tiempo de transmisión.

Debido a que la topología *estrella* utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el ***hub*** o *switch* (aunque, en ambos casos, se pueden conectar éstos en cadena para así incrementar el número de puertos). La desventaja de esta topología en la centralización de la comunicación, ya que si el ***hub*** falla, toda la red se cae.



### 1.3.2 Malla Parcial

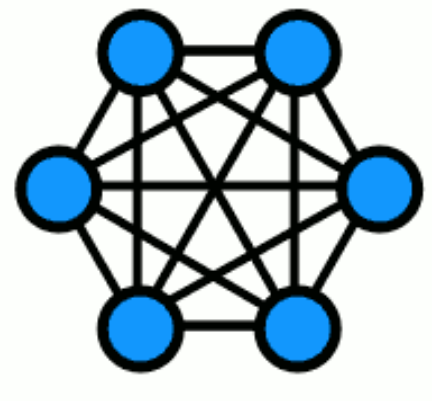
En la topología de ésta, algunos nodos están organizados en una *malla completa*, mientras otros se conectan solamente a uno o dos nodos de la red. Esta topología es menos costosa que la *malla completa*, pero no es tan confiable; ya que el número de enlaces redundantes se reduce.



### 1.3.3 Malla Completa

La topología de *malla completa (mesh)* utiliza conexiones redundantes entre los dispositivos de la red, así como una estrategia de tolerancia a fallas. Cada dispositivo en la red está enlazado a todos los demás ("todos con todos"). Este tipo de tecnología requiere mucho cable (cuando éste se utiliza como medio, pero puede ser inalámbrico también). Debido a la redundancia, la red puede seguir operando si una conexión se rompe.

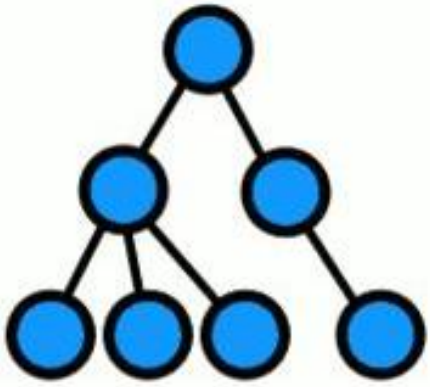
Las redes de malla son más difíciles y caras, ya que para poderlas instalar se necesita un gran número de conexiones.



### 1.3.4 Árbol

La **topología en *árbol*** es una variante de la de ***estrella***. Como en ésta, los **nodos del árbol** están conectados a un **concentrador** central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se enlazan directamente a dicho **concentrador**. La mayoría de estos dispositivos se ponen en contacto con un **concentrador** secundario que, a su vez, se conecta a uno **central (concentrador activo)**.

Un **concentrador** activo contiene un repetidor; es decir, un dispositivo **hardware** que regenera los patrones de **bits** recibidos antes de retransmitirlos. Reproducir las señales de esta forma amplifica su potencia e incrementa la distancia a la que puede viajar la señal. Los concentradores secundarios pueden ser activos o pasivos. Estos últimos proporcionan -solamente- una conexión física entre los dispositivos conectados.

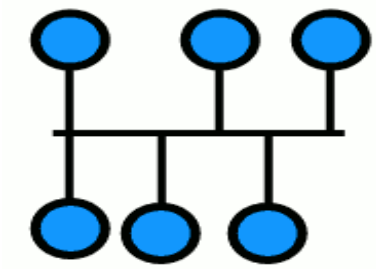


### 1.3.5 Bus

Una topología de *bus* o *ducto* está caracterizada por una dorsal principal con dispositivos de red interconectados a lo largo de esta dorsal. Las redes de este tipo son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto, cuando están listas para transmitir, ellas se aseguran que no haya nadie más haciendo lo mismo en el ducto; entonces envían sus paquetes de información. Las redes de *bus* basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión), típicamente, emplean la arquitectura de **red ETHERNET**.

Las redes de *bus* -comúnmente- usan cable coaxial como medio de comunicación; las computadoras se unen al ducto mediante un conector BNC en forma de T. En el extremo de la red se pone un terminador (si se utiliza un cable de 50 ohm, se emplea -también- un terminador de 50 ohms).

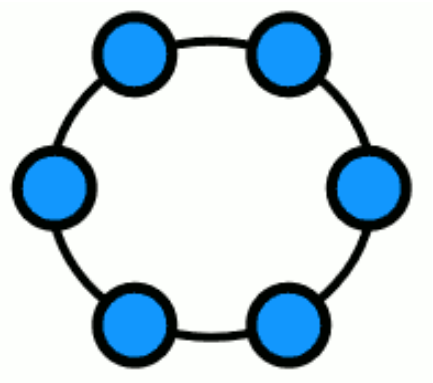
Las redes de *ducto* son fáciles de instalar y de extender. Son muy susceptibles a quebraduras de cable, conectores y cortos que son muy difíciles de encontrar. Un problema físico en la red, tal como un conector T, puede cortar todo el servicio.



### 1.3.6 Anillo

Una topología de *anillo* conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. Ésta mueve información sobre dicho cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora de la red.

El acceso al medio de la red es otorgado a una computadora en particular por un "**token**". Éste circula alrededor del anillo y cuando la máquina desea enviar datos, lo espera y se posiciona de él; entonces, manda los datos sobre el cable. El equipo destino dirige un mensaje (al que envió los datos) de que fueron recibidos correctamente. La computadora que los transmitió, crea un nuevo **token** y los envía a la siguiente máquina; empezando el ritual de paso de *estafeta* (**token passing**), nuevamente.



## 1.4 TIPOS DE REDES INALÁMBRICAS

### 1.4.1 WAN (Wide Area Network)

Es un conjunto de redes individuales unidas a través de grandes distancias, tiene la capacidad de cubrir entre 100 y 1000 km. Debido a esta característica puede dar servicio a un país o a todo un continente. En la actualidad WAN es proporcionado en altas velocidades.

Las redes WAN cuentan con una infraestructura basada en poderosos nodos de conmutación, los cuales permiten la interconexión de equipos y redes terminales que ayudan a que la información fluya de manera continua.

Las características de una red WAN son las siguientes:

- ✓ Tecnología **broadcast** (difusión) con el medio de transmisión compartido.
- ✓ Cableado específico, instalado normalmente a propósito.
- ✓ Capacidad de transmisión comprendida entre 1 **Mbps** y 1 Gbps.
- ✓ Uso de un medio de comunicación público.
- ✓ La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica, satélite o radio).
- ✓ La facilidad con que se pueden efectuar cambios en el **hardware** y **software**.
- ✓ Gran variedad y número de dispositivos conectados.
- ✓ Posibilidad de conexión con otras redes.

### 1.4.2 MAN (Metropolitan Area Network)

Una red MAN es aquella que, a través de una conexión de alta velocidad, ofrece cobertura en una zona geográfica extensa, por ejemplo una ciudad o un municipio. Con una red MAN es posible compartir e intercambiar todo tipo de datos (textos, videos, audio, etc.); la transferencia de éstos puede ser por medio de fibra óptica o cable de par trenzado. Este tipo de red supone una evolución de las LAN, ya que favorece la interconexión en una región más amplia; es decir, cubriendo un mayor radio.

Las redes MAN pueden ser públicas o privadas, éstas se desarrollan con dos **buses unidireccionales**, lo cual indica que cada uno actúa independientemente del otro, respecto a la transferencia de datos.

Este tipo de redes se pueden utilizar en las interconexiones de oficinas dispersas en una ciudad, pero pertenecientes a una misma corporación; por ejemplo, el despliegue de servicios de **VoIP** y el desarrollo de un sistema de video vigilancia municipal.

Las características de las redes MAN son las siguientes:

- ✓ Maneja ancho de banda.
- ✓ Su medio de transmisión es mediante la fibra óptica, microondas y par de cobre.
- ✓ Su conexión es de 10 **Mbps**, 20 **Mbps**, 45**Mbps**, 75**Mbps**, sobre pares de cobre y 100**Mbps**, 1Gbps y 10 Gbps mediante fibra óptica. Mayor cobertura de la red LAN, puede cubrir de una a varias ciudades.
- ✓ Esta red puede ser pública o privada.
- ✓ Maneja interconexión de operador a operador y de redes locales (LAN), utiliza algunos dispositivos para su funcionamiento: **modem**, **routers**, repetidores, etc.
- ✓ Cada equipo requiere de **hardware** para recibir y transmitir información.
- ✓ Permite transmisión de voz, video y datos.

### 1.4.3 LAN (Local Area Network)

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN), como forma de normalizar las conexiones entre las máquinas que se utilizan como **sistemas ofimáticos**. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. En su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras), junto con una serie de reglas que rigen el acceso a dicho medio.

La LAN más difundida, la **Ethernet**, utiliza un mecanismo denominado Call Sense Multiple Access-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está usando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La **Ethernet** transfiere datos a 10 M**bits**/seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

**Ethernet** y **CSMA-CD** son dos ejemplos de LAN. Hay tipologías muy diversas ( *bus*, *estrella*, *anillo*) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de **software** de gestión que cuidan la configuración de los equipos en la LAN, la administración de los

usuarios y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos; por lo general a sus computadoras personales.

Los servicios en la mayoría de las LAN son muy potentes. Muchas organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas; generalmente prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los **routers** y los **bridges** son equipos especiales que permiten conectar dos o más LAN. El *bridge* es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo, mientras el *router* es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de computadoras.

Las grandes empresas disponen de redes corporativas de datos basadas en una serie de redes LAN y **routers**. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

### 1.4.4 PAN

Las redes tipo PAN son una categoría que cubre distancias cortas y cerradas. Algunas de estas tecnologías son Bluetooth y 802.15

Bluetooth es una tecnología inalámbrica europea desarrollada por Ericsson que permite la interconectividad de dispositivos inalámbricos con otras redes e Internet. Bluetooth, al igual que 802.15 y HomeRF, trabajan en la banda de frecuencias de espectro esparcido de 2.4 GHz. Bluetooth es capaz de transferir información entre un dispositivo a otro a velocidades de hasta 1 **Mbps**, permitiendo el intercambio de video, voz y datos de manera inalámbrica.

El Estándar **IEEE** 802.15 se enfoca -básicamente- en el desarrollo de estándares para redes tipo PAN o inalámbricas de corta distancia. Al igual que Bluetooth el 802.15 permite que dispositivos portátiles como **PC**s, **PDA**s, teléfonos, pagers, entre otros, puedan comunicarse e interoperar uno con el otro. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11x, de alguna manera la **IEEE** definió este estándar para permitir la interoperabilidad de las redes WLAN con las redes tipo PAN.

## 1.5 CONFIGURACIÓN PARA REDES INALÁMBRICAS

### 1.5.1 Modo ordenador-ordenador o ad-hoc

Una red "**Ad-hoc**" consiste en un grupo de equipos que se comunican cada uno directamente con los demás, a través de las señales de radio, sin usar un punto de acceso; aunque solamente los equipos dentro de un rango de transmisión definido pueden hacerlo. Las configuraciones "**Ad-hoc**" son comunicaciones de tipo "***peer to peer***" (punto a punto). Cabe recordar, que tradicionalmente este tipo de redes son un medio que se encarga de enlazar dos puntos finales y no hay datos o paquetes de formato. El centro de computadoras en cada extremo debe asumir la responsabilidad para el formato de la información transmitida entre ellos.

Las redes "**Ad-hoc**" también son conocidas como MANET "Mobile ad hoc **networks**", el objetivo de éstas es proporcionar flexibilidad y autonomía aprovechando los principios de auto-organización. Una red móvil **ad-hoc** es una red formada sin ninguna administración central o no hay un nodo central, sino que consta de nodos móviles que usan una interface inalámbrica para enviar paquetes de datos. Los equipos están en igualdad de condiciones.

La conexión es establecida por la duración de una sección. Los equipos descubren otros que se encuentren cercanos a un rango para formar un **network**, éstos -a su vez- pueden buscar nodos que están fuera de área del alcance, conectándose con otros que estén conectados a la red y estén a su alcance. Las conexiones son posibles por múltiples nodos.

### 1.5.2 Modo infraestructura

Es una red tipo cliente-servidor, donde los clientes suelen ser los que se conectan al servidor, llamado punto de acceso, el cual es un dispositivo al que se conectan los clientes para poder comunicarse entre sí. Los puntos de acceso se identifican con su **BSSID**, que coincide con la dirección **MAC** del dispositivo y normalmente también por su **ESSID** o nombre de la red. El punto de acceso a veces también comunica con redes cableadas haciendo la función de puente entre las dos redes. A los clientes también se les suele llamar "estaciones".

Para que pueda existir comunicación entre dos estaciones, ambos tienen que estar conectados al mismo punto de acceso y no tienen por qué verse directamente entre ellos. Cuando un cliente quiere enviar un mensaje a otra estación lo envía al punto de acceso, y éste lo reenvía hasta la estación destino; es decir, es un sistema completamente centralizado. Cuando llega a caerse un punto de acceso inalámbrico provoca la desconexión total de la red, por tal motivo podemos deducir que la zona de cobertura

local es equivalente a la zona de cobertura que tenga el punto de acceso, que puede ir desde los treinta metros a cientos, en las mejores condiciones posibles. Otra problemática es que a medida que el número de estaciones crece, el rendimiento disminuye considerablemente. Recordar que las redes inalámbricas son **half-duplex**, dos elementos de la red que no pueden transmitir a la vez.

## 1.6 Entornos en donde utilizar una red inalámbrica

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- ✓ Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.
- ✓ Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- ✓ Redes locales para situaciones de emergencia o congestión de la red cableada.
- ✓ Las redes inalámbricas permiten el acceso a la información, mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.
- ✓ Generación de grupos de trabajo eventuales y reuniones **ad-hoc**. En estos casos no valdría la pena instalar una red cableada; con una red inalámbrica es suficiente, ya que se puede implementar una red local para satisfacer la necesidad de conexión por un plazo corto de tiempo.
- ✓ En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- ✓ Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableada, situadas en dos edificios distintos.
- ✓ Las salas de formación de las empresas, los alumnos de escuelas y profesores pueden recurrir a la conectividad inalámbrica para acceder e intercambiar información y aprender, sin la complejidad de cablear múltiples puestos para los alumnos.

# CAPÍTULO 2

## PROTOCOLOS Y ESTÁNDAR IEEE 802.11

# CAPÍTULO 2: PROTOCOLOS Y ESTÁNDAR IEEE 802.11

## 2.1 PROTOCOLOS DE COMUNICACIÓN

### 2.1.1 TCP/IP

TCP/**IP** es un conjunto de protocolos. Las siglas TCP/**IP** significan "Protocolo de Control de Transmisión/Protocolo de Internet" y se pronuncia "T-C-P-I-P". De tal forma, podemos darnos cuenta que proviene de los nombres de dos de los más importantes del conjunto protocolario: el TCP y el **IP**.

TCP/**IP** representa todas las reglas de comunicación para Internet y se basa en la noción de dirección **IP**, la cual se le brinda a cada equipo de la red para poder enrutar paquetes de datos.

Debido a que el conjunto de protocolos TCP/**IP** originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de funciones, que son las siguientes:

- ✓ Dividir mensajes en paquetes.
- ✓ Usar un sistema de direcciones.
- ✓ Enrutar datos por la red.
- ✓ Detectar errores en las transmisiones de datos.

Para poder aplicar el modelo TCP/**IP** en cualquier equipo; es decir, independientemente del sistema operativo, el sistema de protocolos TCP/**IP** se ha dividido en diversos módulos. Cada uno de éstos realiza una tarea específica. Además, dichos módulos realizan sus funciones uno después del otro, en un orden específico; en otras palabras, existe un sistema estratificado. Ésta es la razón por la cual se habla de "modelo de capas".

El término "*capa*" se utiliza para reflejar el hecho de que los datos que viajan por la red atraviesan distintos niveles de protocolos. Por lo tanto, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información (llamado encabezado) y los envía a la siguiente. El modelo TCP/**IP** es muy similar al **modelo OSI** (modelo de 7 capas).

Para poder comprender mejor el funcionamiento de TCP/**IP** debemos dar un vistazo a lo que es el **modelo OSI** (Interconexión de Sistemas Abiertos). Este modelo fue

establecido por **ISO** para implementar un estándar de comunicaciones entre equipos de una red; esto es, las reglas que administran la comunicación entre equipos. De hecho, cuando surgieron las redes, cada fabricante contaba con su propio sistema (hablamos de uno patentado), por lo cual coexistían con diversas redes incompatibles. Por esta razón, fue necesario establecer un estándar.

El objetivo de un sistema en capas es dividir el problema en diferentes partes (capas), de acuerdo con su nivel de abstracción. Cada una de éstas se comunica con un nivel adyacente (superior o inferior); de tal manera, utiliza los servicios de las capas inferiores y se los proporciona a la superior.

El **modelo OSI** es un modelo que comprende 7 capas, mientras que el modelo TCP/**IP** tiene sólo 4. En realidad, el modelo TCP/**IP** se desarrolló casi a la par que el **modelo OSI**; es por ello que está influenciado por éste; aunque no sigue todas sus especificaciones.

Las capas del **modelo OSI** son las siguientes:

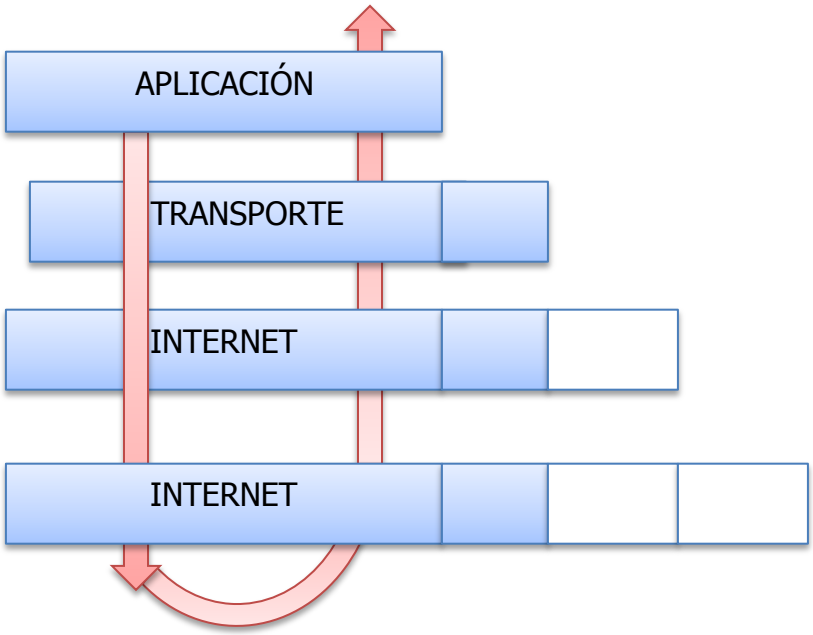
- ✓ **Capa física**: define la manera en la que los datos se convierten físicamente en señales digitales en los medios de comunicación (pulsos eléctricos, modulación de luz, etc.)
- ✓ **Capa de enlace de datos**: define la interfaz (con la tarjeta de interfaz de red) y cómo se comparte el medio de transmisión.
- ✓ **Capa de red**: permite administrar las direcciones y el enrutamiento de datos; es decir, su ruta a través de la red.
- ✓ **Capa de transporte**: se encarga del transporte de datos, su división en paquetes y la administración de potenciales errores de transmisión.
- ✓ **Capa de sesión**: define el inicio y la finalización de las sesiones de comunicación entre los equipos de la red.
- ✓ **Capa de presentación**: define el formato de los datos que maneja la capa de aplicación (su representación y, potencialmente, su comprensión y cifrado) independientemente del sistema.
- ✓ **Capa de aplicación**: le brinda aplicaciones a la interfaz. Por lo tanto, es el nivel más cercano a los usuarios, administrado directamente por el **software**.

El modelo TCP/**IP**, influenciado por el **modelo OSI**, también utiliza el enfoque modular (módulos o capas); pero sólo contiene cuatro, que se mencionan a continuación (posteriormente se detallará cada una de ellas):

- Capa de acceso a la red.
- Capa de Internet.
- Capa de transporte.
- Capa de aplicación.

Durante una transmisión, los datos cruzan cada una de las capas en el nivel del equipo remitente y –simultáneamente- se le va agregando información al paquete de datos. Esto se llama encabezado, ya que esta recopilación garantiza la transmisión.

En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original.




En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas:

- El paquete de datos se denomina **mensaje**, en el nivel de la capa de aplicación.
- El mensaje después se encapsula en forma de **segmento**, en la capa de transporte.
- Una vez que se encapsula el segmento en la capa de Internet, toma el nombre de **datagrama**.
- Finalmente, se habla de **trama** en el nivel de capas de acceso a la red.

La **capa de acceso a la red** es la primera de la pila TCP/**IP**. Ofrece la capacidad de acceder a cualquier red física, ya que brinda los recursos que se deben implementar para transmitir datos a través de la red.

Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una de área local (red en *anillo*, **Ethernet**, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red. Trata los siguientes conceptos:

- ✓ Enrutamiento de datos por la conexión.
- ✓ Coordinación de la transmisión de datos (sincronización).
- ✓ Formato de datos.
- ✓ Conversión de señal (análoga/digital).
- ✓ Detección de errores a su llegada.

Afortunadamente, todas estas especificaciones son invisibles al ojo del usuario, ya que en realidad es el sistema operativo el que realiza estas tareas, mientras los **drivers** de **hardware** permiten la conexión a la red.

La **capa de internet** es la capa "más importante", ya que es la que define los **datagramas** y administra las nociones de direcciones **IP**. Permite el enrutamiento de **datagramas** (paquete de datos) a equipos remotos junto con la administración de su división y ensamblaje, cuando se reciben.

La capa de internet contiene 5 protocolos:

- ✓ IP (Internet Protocol / Protocolo de Internet).
- ✓ ARP (Address Resolution Protocol / Protocolo de Resolución de Dirección).
- ✓ ICMP (Internet Control Message Protocol / Protocolo de Control de Mensajes de Internet).
- ✓ RARP (Reverse Address Resolution Protocol / Protocolo de Resolución de Dirección de Retorno).
- ✓ IGMP (Internet Group Management Protocol / Protocolo de Gestión de Grupos de Internet).

Los primeros tres protocolos son los más importantes para esta capa.

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse; el único problema es poderlas identificar; de hecho, éstas pueden ser un programa, una tarea, un proceso, etc. dependiendo del equipo y su sistema operativo. Por otro lado el nombre puede variar de sistema en sistema, es por ello que se ha implementado una numeración para poder asociar un tipo de aplicación con uno de datos. Estos identificadores se denominan "puertos".

La **capa de transporte** contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos, independientemente del tipo de red. Son los siguientes:

- ✓ TCP: protocolo orientado a conexión que brinda detección de errores.
- ✓ UDP: protocolo no orientado a conexión en el que la detección de errores es obsoleta.

La **capa de aplicación** se encuentra en la parte superior de las del protocolo TCP/**IP** y contiene las aplicaciones de red que permiten la comunicación mediante las inferiores.

Por lo tanto, el **software** en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la de transporte); es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo. Se pueden clasificar según los servicios que brindan:

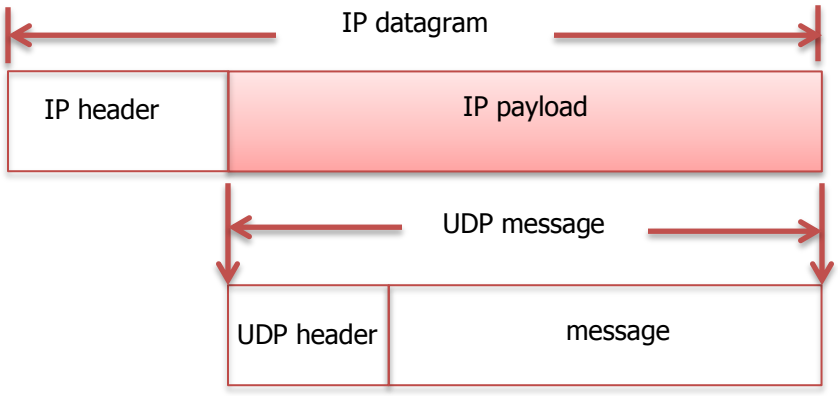
- ✓ Servicios de administración de archivos e impresión (transferencia).
- ✓ Servicios de conexión a la red.
- ✓ Servicios de conexión remota.
- ✓ Diversas utilidades de internet.

### 2.1.2 UDP

El Protocolo de **Datagramas** de Usuario (UDP / User Datagram Protocol) es un estándar TCP/**IP** que está definido en **RFC 768**. Algunos programas utilizan UDP en lugar de TCP para el transporte de datos rápido, compacto y no confiable entre **hosts** TCP/**IP**.

UDP proporciona un servicio de **datagramas** sin conexión que ofrece entrega de mejor esfuerzo, lo que significa que UDP no garantiza la entrega ni comprueba la secuencia de los **datagramas**. Un **host** de origen que necesita comunicación confiable debe utilizar TCP o un programa que proporcione sus propios servicios de secuencia y confirmación.

Los mensajes UDP están encapsulados y se envían en **datagramas IP**, como se muestra en la siguiente ilustración.




Los puertos UDP proporcionan una ubicación para enviar y recibir mensajes UDP. Dichos puertos funcionan con una única cola de mensaje que recibe todos los **datagramas** destinados al programa especificado, mediante cada número de puerto del protocolo. Lo que significa que los programas basados en UDP pueden recibir varios mensajes a la vez.

El lado de servicio de cada programa que utiliza UDP atiende los mensajes que llegan a su puerto asignado; todos los inferiores a 1.024 (y algunos superiores) están reservados y registrados por la autoridad de números asignados de internet.

Cada puerto de servicios UDP se identifica mediante un número de puerto conocido o reservado. En la siguiente tabla se muestra algunos números de puerto de servidor UDP conocidos que utilizan programas basados en UDP estándar.

| NÚMERO DE PUERTO UDP | DESCRIPCIÓN |
|---|---|
| **53** | Consulta de nombres DNS |
| **69** | Protocolo trivial de transferencia de archivos (TFTP) |
| **137** | Servicio de nombres NetBIOS |
| **138** | Servicio de **datagramas** NetBIOS |
| **161** | Protocolo simple de administración de redes (SNMP) |
| **520** | Protocolo de información de enrutamiento (RIP, **Routing** Information Protocol ) |

El protocolo UDP no está orientado a conexión de la capa de transporte del modelo TCP/**IP**. Este protocolo es muy simple, ya que no proporciona detección de errores.

Por lo tanto, el encabezado del segmento UDP –también- es muy simple:

| | |
|---|---|
| puerto de origen (16 **bits**); | puerto de destino (16 **bits**); |
| longitud total (16 **bits**); | suma de comprobación del encabezado (16 **bits**); |

datos
(longitud variable).

El significado de los diferentes cambios es el siguiente:

- ✓ Puerto de origen: es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario; por lo tanto, es opcional. Esto significa que si el puerto de origen no está especificado, los 16 **bits** de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).
- ✓ Puerto de destino: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.
- ✓ Longitud: como su nombre lo indica, este campo especifica la longitud total del segmento, con el encabezado incluido, el cual tiene una longitud de 4 x 16 **bits** (que es 8 x 8 **bits**); por lo tanto, la longitud del campo es necesariamente superior o igual a 8 bytes.
- ✓ Suma de comprobación: es la que se realiza de manera tal que permita controlar la integridad del segmento.

Las ventajas de UDP son las siguientes:

- Transferencia de datos muy rápida.
- Muy flexible, eficiente para utilizarse con sistemas ajenos.
- Con capacidad de **Routing**.
- Con capacidad de **Broadcast/Multicast**.
- Adecuado para la transferencia de cantidades de datos medianas o pequeñas (<=2048 bytes).

Por otro lado las desventajas de UDP son las siguientes:

- Los paquetes de datos perdidos no se envían de nuevo.
- Se eliminan los paquetes de datos con suma de comprobación errónea y no se solicitan de nuevo.
- Es posible la asignación múltiple de paquetes individuales.
- La secuencia de llegada de los paquetes en el receptor no se puede predecir.
- Los datos se transfieren orientados a paquetes (no orientado a flujo).
- La función de **Broadcast** sólo se puede utilizar en la dirección de envío.

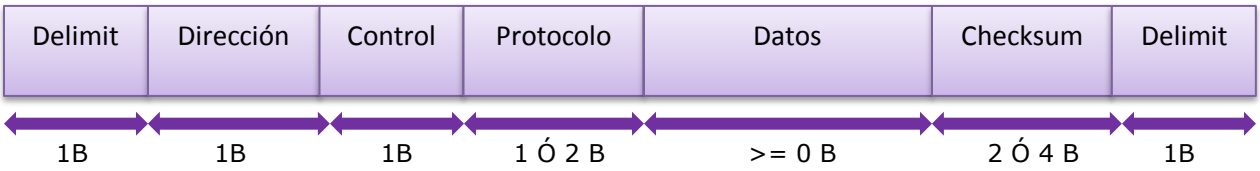
### 2.1.3 PPP

PPP son las siglas de Point to Point Protocol (Protocolo Punto a Punto). Esto significa que la conexión se realiza, obviamente, siempre entre dos **hosts** (integrantes de ésta) o puntos de conexión. Siempre, uno de estos integrantes es cliente y el otro servidor.

Este protocolo permite utilizar el **IP** a través de líneas asíncronas serie y, mediante módems, por medio de líneas telefónicas. El PPP hace posible que una computadora remota se convierta en una máquina más del Internet, de esta forma completa la conexión PPP.

El PPP fue desarrollado por el Internet Engineering Task Force (IETF) en 1990 y está especificado en los RFC 1661, 1662 y 1663. PPP fue diseñado para ser flexible, por ello incluye un protocolo especial, denominado LCP (Link Control Protocol), que se ocupaba de negociar una serie de parámetros en el momento de establecer la conexión con el sistema remoto.

La estructura de un **frame** PPP se basa en el de HDLC (High-level Data Link Control o Control de Enlace de Datos de Alto Nivel), es un estándar a nivel de enlace de datos que incluye mecanismos para la detección y corrección de errores, utilizan la técnica de relleno de **bits** y las marcas "01111110" para construir y manejar tramas; pero, a diferencia de éste, PPP es un protocolo orientado a carácter, lo que implica que la longitud del **frame** ha der ser un número entero de bytes. En función de las características del medio físico se aplica relleno de bytes (por ejemplo para transmisión por medios asíncronos). La descripción de cada uno de los campos del **frame** es la siguiente:




**Delimitador:** 1 Byte tiene siempre la secuencia 01111110 como delimitador.

**Dirección:** 1 Byte, este campo no se utiliza y siempre vale 11111111.

**Control:** 1 Byte tiene por defecto el valor 00000011, que corresponde a un servidor no confiable y no orientado a conexión. De todas formas, en el momento de establecer la conexión LCP puede negociar una transmisión fiable.

**Dirección:** 2 Bytes, por defecto, corresponde la secuencia 1111111100000011, a menos que se negocie una transmisión confiable. Para no transferir estos dos bytes de información inútil en todos los **frames.**

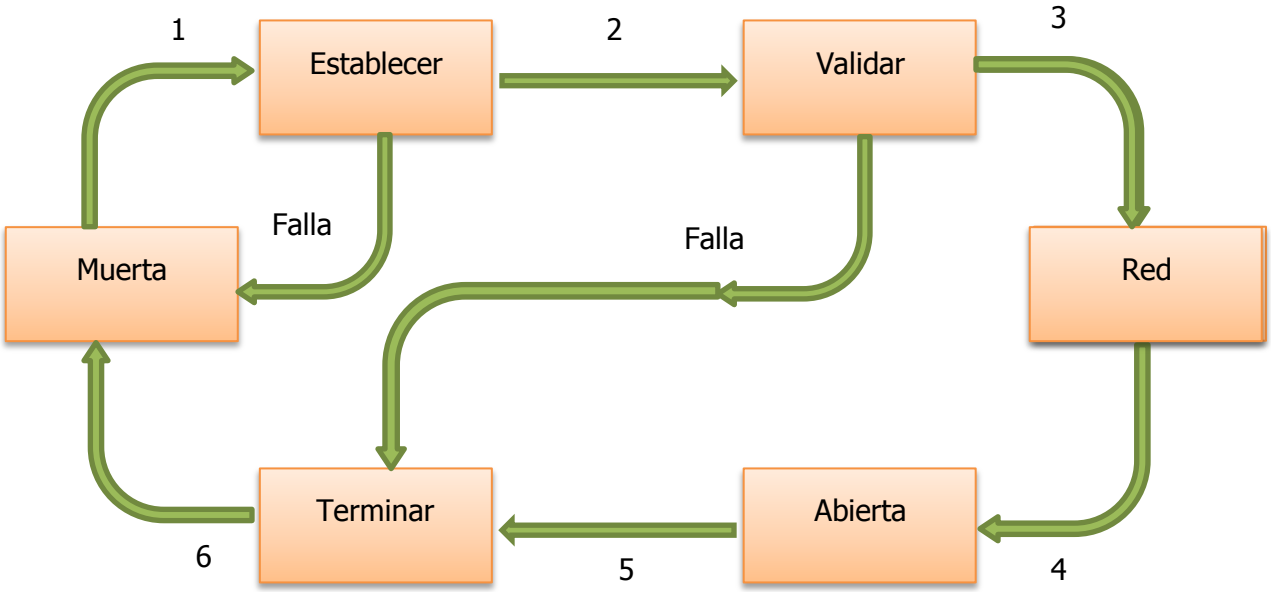
**Protocolo:** 1 ó 2 Bytes determina a qué tipo de protocolo pertenece el paquete recibido de la capa de red. Así, PPP permite establecer una comunicación multiprotocolo; es decir, puede utilizarse para transmitir paquetes pertenecientes a diferentes protocolos del nivel de red. Entre las posibilidades se encuentra **IP, IPX, Appletalk, DECNET, OSI** y otros.

**Datos:** De una longitud variable hasta un máximo que negocia LCP al establecer la conexión. Por defecto, el tamaño máximo del **frame** es de 1500 bytes.

**Checksum:** 2 Bytes, pero puede ser de 4 si se negocia.

PPP puede utilizarse sobre medios físicos muy diversos; por ejemplo, conexiones mediante módem, ISDN, líneas dedicadas, o incluso por conexiones SONET/SDH de alta velocidad.

Las fases de la conexión son las siguientes:




1. Cuando se detecta la portadora (forma de onda, que es modulada por una señal que se quiere transmitir) es porque se ha realizado una conexión a nivel de capa física y la conexión está en la fase "*establecer*". Hasta entonces la línea estaba en reposo o *"muerta"*, ya que no existía conexión.
2. Se negocian las opciones LPC (Link Control Protocol, protocolo de control de enlace) y si se llega a un acuerdo se pasa a la fase de *"validar"*, que consiste en la verificación de identidad del usuario.
3. Al entrar en la fase de "*red*" se invoca al protocolo NCP (**Network** Control Protocol, protocolo de control de red), el encargado de negociar los parámetros específicos para cada protocolo utilizado, apropiado para configurar la capa de red.
4. Una vez configurada se pasa a la fase *"abierta"*, y comienza el trasporte de datos.
5. Finalmente, la conexión pasa a fase de *"terminar"* cuando ya no existen más datos para transmitir y se desea liberar la conexión.
6. Una vez finalizada la conexión se pasa a la etapa de reposo o *"muerta"*.

### Protocolo de control de vínculo

El protocolo de control de vínculos (LCP, Link Control Protocol) establece y configura las tramas de PPP, las cuales definen la forma en que se encapsulan los datos para su transmisión, a través de la red de área extensa. El formato de trama estándar de PPP garantiza que el **software** de acceso remoto de cualquier proveedor pueda comunicarse y reconocer paquetes de datos de cualquier programa de acceso remoto que cumpla los estándares de PPP.

### Protocolos de autentificación

Los protocolos de autentificación se negocian inmediatamente después de determinar la calidad del vínculo y antes de negociar el nivel de red, para obtener más información acerca de los protocolos de autentificación disponibles.

### Protocolos de control de red

Los protocolos de control de red establecen y configuran distintos parámetros de los de TCP/**IP**, IPX y AppleTalk. La tabla siguiente los describe.

El protocolo IPX/SPX no está disponible en las versiones basadas en el procesador *Itanium* de los sistemas operativos Windows.

| Protocolo de control de red | Descripción |
|---|---|
| **Protocolo de control del protocolo Internet (IPCP,  Internet Protocol Control Protocol )** | IPCP se utiliza para configurar TCP/**IP** en el cliente de acceso remoto. Entre los parámetros de configuración se incluyen una dirección **IP** y las direcciones **IP** de los servidores DNS y WINS. |
| **Protocolo de control de intercambio de paquetes entre redes (IPXCP,  Internet Packet Exchance Control Protocol )** | IPXCP se utiliza para configurar IPX en el cliente de acceso remoto. Está muy extendido dentro de los proveedores de PPP. Entre los parámetros de configuración incluyen los números de red y nodo IPX. |
| **Protocolo de control AppleTalk (ATCP, AppleTalk Control Protocol)** | ATCP se utiliza para configurar AppleTalk en el cliente de acceso remoto. Entre los parámetros de configuración se incluye una dirección Apple Talk. |

### 2.1.4 IP V4

**IP**v4 es la versión 4 del Protocolo de Internet (**IP** o Internet Protocol) y constituye la primera versión de **IP** que es implementada de forma extensiva. **IP**v4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/**IP** para Internet.

**IP**v4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (**switches**) de paquetes (por ejemplo, a través de **Ethernet**). Tiene las siguientes características: es un protocolo de un servicio de **datagramas** no fiable (también referido como de mejor esfuerzo), no proporciona garantía en la entrega de datos, no proporciona ni garantías sobre la corrección de los datos, puede resultar en paquetes duplicados o en desorden.

Los problemas que se pueden presentar se resuelven en el nivel superior en el modelo TCP/**IP**; por ejemplo, a través de TCP o UDP. El propósito principal de **IP** es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

**IP**v4 utiliza direcciones de 32 **bits** (4 bytes), las cuales limitan el número de las posibles a utilizar a 4,294,967,295 únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión (**Multicast**), etc. Debido a esto se reduce el número de **IP**'s que realmente se pueden utilizar.

Cuando se escribe una dirección **IP**v4 en cadenas, la notación más común es la decimal con puntos. Hay otras notaciones basadas sobre los valores de los octetos de la dirección **IP**. Por ejemplo la IP 201.161.1.226 en la notación decimal con puntos:

| Notación | Valor | Conversión desde decimal con puntos |
|---|---|---|
| **Decimal con puntos** | 201.161.1.226 | ---------- |
| **Hexadecimal con puntos** | 0xC9.0xA1.0x01.0xE2 | Cada octeto de la dirección es convertido individualmente a hexadecimal. |
| **Octal con puntos** | 0311.0241.0001.0342 | Cada octeto es convertido individualmente en octal. |
| **Binario con** | 11001001.10100001.00000001.11100010 | Cada octeto es convertido |

| | | |
|---|---|---|
| **puntos** | | individualmente a binario. |
| **Hexadecimal** | 0xC9A101E2 | **Concatenación** de los octetos de hexadecimal con puntos. |
| **Decimal** | 3382772194 | La forma hexadecimal convertida a decimal. |
| **Octal** | 31150200742 | La forma hexadecimal convertida a octal. |
| **Binario** | 11001001101000010000000111100010 | La forma hexadecimal convertida a binario. |

Teóricamente, todos estos formatos mencionados deberían ser reconocidos por los navegantes (sin combinar). Además, en las formas con puntos, cada octeto pude ser representado en combinación de diferentes bases.

Desde 1993 rige el esquema CIDR (Classless Inter-Domain **Routing** o Encaminamiento Inter-Dominios sin Clases), cuya principal ventaja es permitir la subdivisión de redes y admitir las entidades sub-asignar direcciones **IP**, como haría un ISP (Internet Service Provider, proveedor de servicios de Internet). Éste conecta a sus usuarios a Internet, a través de diferentes tecnologías, con un cliente.

El principio fundamental de encaminamiento (**routing**) es que la dirección codifica información acerca de localización de un dispositivo dentro de la red. Esto implica que este equipo no funcionará en otra parte de la red al que no esté asignado.

Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el CIDR y hasta 1998 fue supervisada por la IANA (Internet Assigned Numbers Authority o Agencia de Asignación de Números Internet) y sus RIR (Regional Internet Registries o Registros Regionales de Internet). Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la ICANN (Internet Corporation for Assigned Names and Numbers o Corporación de Internet para los Nombres y Números Asignados). Cada RIR mantiene una base de datos WHOIS disponible al público y que permite hacer búsquedas que proveen información acerca de las asignaciones de **IP**. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas, las cuales se utilizan para localizar direcciones **IP** geográficamente.

Bloques de direcciones reservadas

| Bloques de direcciones CIDR | Descripción | Referencia |
|---|---|---|
| **0.0.0.0/8** | Red actual (sólo válido como dirección de origen) | RFC 1700 |
| **10.0.0.0/8** | Red privada | RFC 1918 |
| **14.0.0.0/8** | Red de datos públicos | RFC 1700 |
| **39.0.0.0/8** | Reservado | RFC 1797 |
| **127.0.0.0/8** | Anfitrión (local**host**) | RFC 1700 |
| **128.0.0.0/16** | Reservado | |
| **169.254.0.0/16** | Red privada (Zeroconf) | RFC 3927 |
| **172.16.0.0/12** | Red privada | RFC 1918 |
| **191.255.0.0/16** | | |
| **192.0.0.0/24** | | |
| **192.0.2.0/24** | Red de pruebas | RFC 3330 |
| **192.88.99.0/24** | Retransmisión desde **IP**v6 hacia **IP**v4 | RFC 3068 |
| **192.168.0.0/16** | Red privada | RFC 1918 |
| **198.18.0.0/15** | Pruebas de desempeño de red | RFC 2544 |
| **223.255.255.0/24** | Reservado | RFC 3330 |
| **224.0.0.0/4** | Multidifusión (**Multicast**, antes red Clase D) | RFC 3171 |
| **240.0.0.0/4** | Reservado (Antes red Clase E) | RFC 1700 |
| **255.255.255.255** | Difusiones (**Broadcast**) | |

De los más de cuatro millones de direcciones permitidas por **IP**v4, tres rangos están especialmente reservados para utilizarse solamente en redes privadas. Estos rangos no tienen encaminamiento fuera de una privada y las máquinas dentro de estas redes no pueden comunicarse –directamente- con las públicas, únicamente consiguen hacerlo a través de la Traducción de Direcciones de Red o **NAT** (**Network** Address Translation).

Bloques reservados para redes privadas

| Nombre | Rango de direcciones IP | Número de direcciones IP | Tipo de clase | Bloque CIDR mayor |
|---|---|---|---|---|
| **Bloque de 24 bits** | 10.0.0.0 – 10.255.255.255 | 16,777,215 | Única clase A | 10.0.0.0/8 |
| **Bloque de 20 bits** | 172.16.0.0 – 172.31.255.255 | 1,048,576 | 16 clases B contiguas | 172.16.0.0/12 |
| **Bloque de 16 bits** | 192.168.0.0 – 192.168.255.255 | 65,535 | 256 clases C contiguas | 192.168.0.0/16 |

Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255 ó 127.0.0.0/8 en la notación CIDR, está reservado para la comunicación del anfitrión local (local **host**). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada, y cualquier paquete enviado hacia alguna dirección de éste, deberá regresar como un paquete entrante hacia la misma máquina.

Algunos segmentos del espacio de direcciones de **IP**, disponibles para la versión 4, se especifican y asignan a través de documentos RFC (Request For Comments o Solicitud De Comentarios), que son conjuntos de notas técnicas y de organización elaborados desde 1969, donde se describen los estándares o recomendaciones de Internet, antes ARPANET. Ejemplos de esto son los usos del Retorno del sistema (loopback, RFC 1643), las redes privadas (RFC 1918) y Zeroconf (RFC 3927), que no están bajo el control de los RIR (Regional Internet Registries o Registros Regionales de Internet).

La máscara de sub-red es utilizada para separar los **bits** de un identificador de una red, a partir de los **bits** del identificador del anfitrión. Se escribe utilizando el mismo tipo de notación que para las direcciones **IP**.

| CIDR | MÁSCARA DE SUB-RED | ANFITRIONES | NOMBRE DE LA CLASE | USO TÍPICO |
|---|---|---|---|---|
| **/8** | 255.0.0.0 | 16777216 | Clase A | Bloque más grande definido por la IANA |
| **/9** | 255.128.0.0 | 8388608 | | |
| **/10** | 255.192.0.0 | 4194304 | | |
| **/11** | 255.224.0.0 | 2097152 | | |

| | | | | |
|---|---|---|---|---|
| **/12** | 255.240.0.0 | 1048576 | | |
| **/13** | 255.248.0.0 | 524288 | | |
| **/14** | 255.252.0.0 | 262144 | | |
| **/15** | 255.254.0.0 | 131072 | | |
| **/16** | 255.255.0.0 | 65536 | Clase B | |
| **/17** | 255.255.128.0 | 32768 | | ISP/negocios grandes. |
| **/18** | 255.255.192.0 | 16384 | | ISP/negocios grandes. |
| **/19** | 255.255.224.0 | 8192 | | ISP/negocios grandes. |
| **/20** | 255.255.240.0 | 4096 | | ISP pequeños/ negocios grandes. |
| **/21** | 255.255.248.0 | 2048 | | ISP pequeños/ negocios grandes. |
| **/22** | 255.255.252.0 | 1024 | | |
| **/23** | 255.255.254.0 | 512 | | |
| **/24** | 255.255.255.0 | 256 | Clase C | LAN grande. |
| **/25** | 255.255.255.128 | 128 | | LAN grande. |
| **/26** | 255.255.255.192 | 64 | | LAN pequeña. |
| **/27** | 255.255.255.224 | 32 | | LAN pequeña. |
| **/28** | 255.255.255.240 | 16 | | LAN pequeña. |
| **/29** | 255.255.255.248 | 8 | | |
| **/30** | 255.255.255.252 | 4 | | Redes de unión (enlaces punto a punto). |
| **/31** | 255.255.255.254 | 2 | | Red no utilizable, sugerida para enlaces punto a punto (RFC 3021). |
| **/32** | 255.255.255.255 | 1 | | Ruta del anfitrión. |

### 2.1.5 IP V6

Cuando hacemos uso de Internet, la comunicación entre nuestro dispositivo electrónico y los diferentes elementos de la red utilizan como vía un protocolo llamado Protocolo de Internet (**IP**, Internet Protocol).

Desde que Internet tuvo un uso comercial ha utilizado el protocolo **IP** V4. Cuando nació **IP** V4 tuvo una gran aceptación comercial; pero éste sólo dispone de 2^32 direcciones (con una longitud de 32 **bits**; es decir, 4.294.967.296 direcciones). Esto, aunado al crecimiento de usuarios y dispositivos, implica una inevitable carencia de direcciones.

Por tal motivo, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force) ha trabajado en una nueva versión del protocolo de éste, específicamente la versión 6 (**IP**v6). Ésta, a diferencia de la versión 4, posee direcciones con una longitud de 128 **bits**; es decir, 2^128 posibles direcciones

(340.282.366.920.938.463.463.374.607.431.768.211.456); dicho de otro modo, 340 sextillones.

La introducción de **IP**v6 se irá realizando gradualmente, en una coexistencia ordenada con **IP**v4, el objetivo de la versión 6 es el desplazamiento de su antecesor a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet. Debido a que el predominante en la actualidad es **IP**v4 no es posible su sustitución, tampoco es posible apagar la red, ni siquiera unos minutos y cambiar a **IP**v6.

Por tal motivo para evitar un impacto la IETF (Internet Engineering Task Force), que -como ya mencioné- es la organización encargada de la estandarización de protocolos, diseñó -a la par del **IP**v6- una serie de mecanismos de transición y coexistencia. En otras palabras, el cambio no consiste en una migración como erróneamente se cree, sino que ambos protocolos (**IP**v4 e **IP**v6) existirán durante algún tiempo; es decir, se producirá una coexistencia.

Las principales características del protocolo **IP**v6 son las siguientes:

- ✓ Mayor espacio de direccionamiento:
  Posee direcciones con una longitud de 128 **bits**, o sea 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456); dicho de otro modo, 340 sextillones.
  Esto hace que:
  - Desaparezcan los problemas de direccionamiento del **IP**v4.
  - No sean necesarias técnicas como el **NAT** para proporcionar conectividad a todas las computadoras/dispositivos de nuestra red.

- ✓ Seguridad:
  Uno de los grandes problemas de Internet es su falta de seguridad en su diseño base. Este es el motivo por el que han tenido que desarrollarse; por ejemplo, el **SSH** o **SSL**, protocolos a nivel de aplicación que añaden una capa de seguridad a las conexiones que pasan a través suyo.
  **IP**v6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

- ✓ Autoconfiguración:
  En el actual **IP**v4 han tenido que desarrollarse protocolos a nivel de aplicación que permitiesen a los equipos conectados a una red asignarles sus datos de conectividad al vuelo. Ejemplos son el **DHCP** o **BootP**.
  **IP**v6 incluye esta funcionalidad en el protocolo base, la propia pila intenta "autoconfigurarse" y descubrir el camino de conexión a Internet (*router discovery*).

- ✓ Movilidad:
  Con la movilidad (o ***roaming***) ocurre lo mismo que en los puntos anteriores, una de las características obligatorias de **IP**v6 es la posibilidad de conexión y desconexión de nuestro equipo de redes **IP**v6 y; por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.

## 2.2 PROTOCOLOS DE SEGURIDAD

### 2.2.1 WEP

El algoritmo WEP es el estándar opcional de seguridad utilizado en redes inalámbricas 802.11b y 802.11a, el cual está implementado en la capa de control de acceso al medio (**MAC**, Media Access Control). En general, dicha capa administra y mantiene la comunicación entre los nodos de una red, coordinando el acceso a un canal y utilizando protocolos que mejoren las conexiones sobre el medio inalámbrico.

El algoritmo WEP protege las comunicaciones inalámbricas contra ataques de intrusos y previene de acceso no autorizado a una red inalámbrica. Fue diseñado para proveer autenticación de usuarios, privacidad de datos e integridad de éstos, en una forma equivalente a una red cableada LAN.

El WEP consta de cuatro componentes esenciales para su funcionamiento: una llave secreta, un vector de inicialización, el algoritmo **RC4** y el **CRC-32** o Código de Redundancia Cíclica de 32 **bits**.

La mayoría de los puntos de acceso utilizados en redes **IEEE** 802.11 manejan llaves secretas estáticas, que comparten con los usuarios de la red para iniciar una transmisión de datos. Estas llaves se emplean para **encriptar** información con el algoritmo **RC4**. Generalmente una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Esta llave normalmente es de 40 **bits**; aunque existen implementaciones que usan llaves de 104 **bits** con el fin de ofrecer un nivel mayor de seguridad.

El WEP utiliza la llave compartida para generar una secuencia de llaves a través del **RC4**, que servirá para **encriptar** la información. Para evitar **encriptar** todos los paquetes con dicha secuencia, se utiliza un vector de inicialización (IV) de 24 **bits**, que minimiza la probabilidad de alimentar el **RC4** con las mismas entradas.

Así, la entrada que alimenta al **RC4** se compone de 64 ó 128 **bits** en total, conformados por 40 ó 104 **bits** -respectivamente- de la llave compartida y 24 **bits** de IV. Algunos sistemas asignan al vector de inicialización el valor de 0 al inicio de la transmisión y aumentan éste -unitariamente- por cada paquete transmitido. Después de que alcanzan los 16 millones de paquetes enviados, el valor del IV regresa a 0.

**RC4** es el algoritmo de cifrado de flujo más usado en la actualidad. Fue creado por Ron Rivest en 1987 y se mantuvo en secreto hasta que se hizo público en 1994. Los cifrados de flujo funcionan expandiendo una llave o cadena de **bits**, en una clave arbitrariamente larga de **bits** pseudo aleatorios.

En el caso del WEP, la llave se forma por el vector de inicialización y la llave secreta compartida. Éstas alimentan al algoritmo **RC4** para generar la secuencia de llaves utilizada para **encriptar** y **desencriptar** información.

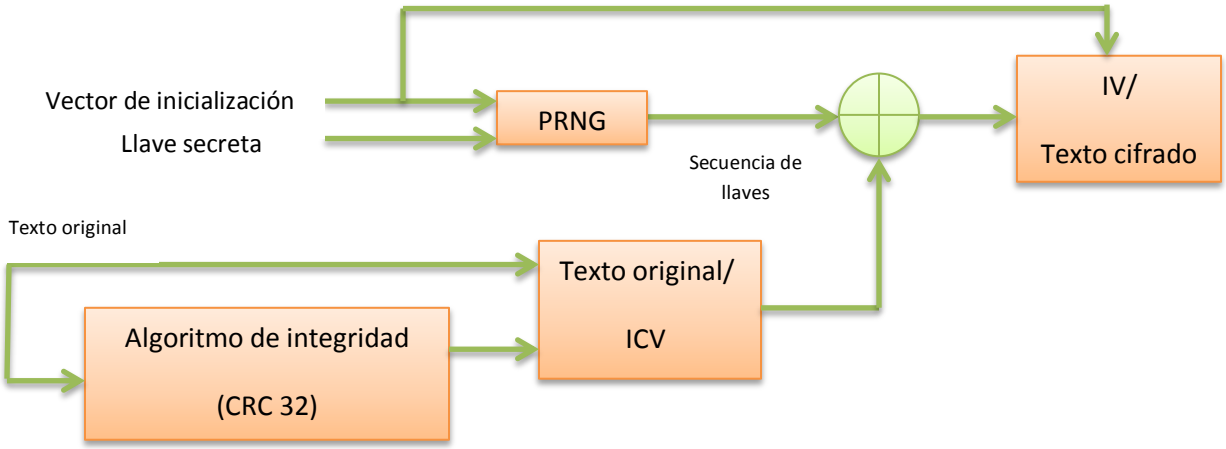
Una manera de asegurar que la información enviada en forma electrónica por una red no ha sido modificada, es utilizando las sumas de verificación (*checksums*); un procedimiento simple de éstas puede utilizarse para calcular el valor de un archivo y después compararlo con su valor previo. Si las sumas de verificación son iguales, el archivo no ha sufrido cambios; si no son iguales, el archivo habrá sido alterado.

En el caso de redes inalámbricas, en lugar de calcular el valor de un archivo, se calcula el de una cadena de **bits**, correspondiente a un mensaje transmitido.

Para calcular las sumas de verificaciones se utilizan códigos de redundancia cíclica (CRC), también llamados códigos polinómicos. Los CRC son muy usados en la práctica para la detección de errores en largas secuencias de datos.

Para llevar a cabo los procesos de encriptación y decriptación de información, el WEP utiliza cuatro componentes; el de encriptación lo realiza para cada paquete transmitido y se describe en los pasos siguientes:

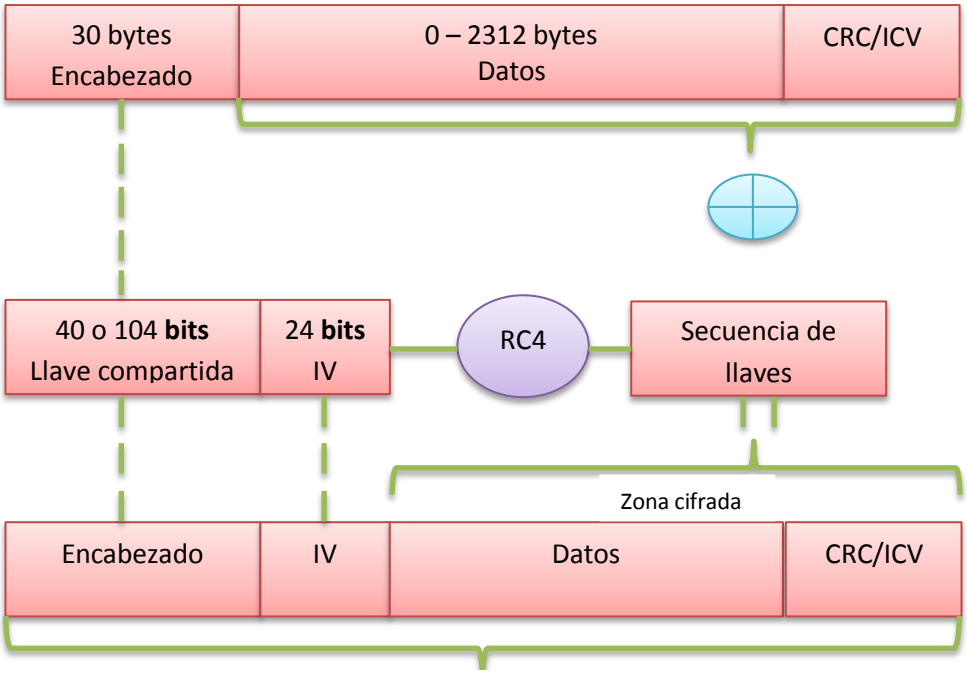
1. El transmisor calcula el **ICV** (valor de 4 **bits**) usando el **CRC-32** sobre el mensaje a transmitir y lo concatena al mismo.
2. El transmisor elige el **IV** y lo concatena a la llave compartida.
3. El **IV** y la llave secreta compartida alimentan al **RC4** que funciona como Generador de Números Pseudo Aleatorios (PRNG), para generar una secuencia de llaves.
4. El transmisor encripta el mensaje original haciendo la operación **XOR** entre éste y la secuencia generada en el paso anterior.
5. El transmisor envía el vector de inicialización seguido por el mensaje encriptado.




"Diagrama de bloques del proceso de encriptación del WEP"

El texto cifrado y el IV viajan por el enlace inalámbrico hacia el receptor, el cual deberá **desencriptar** la información. Es importante notar que el vector de inicialización se envía sin ningún tipo de encriptación, lo cual es una de las principales causas de las debilidades del WEP.

En la figura siguiente se muestra la trama completa enviada de transmisor a receptor, distinguiendo la parte encriptada que consiste de los datos y el ICV calculado por el CRC32, del encabezado **MAC** de la trama y el vector de inicialización que no están encriptados.




Encabezado, vector de inicialización y datos encriptados se envían al receptor

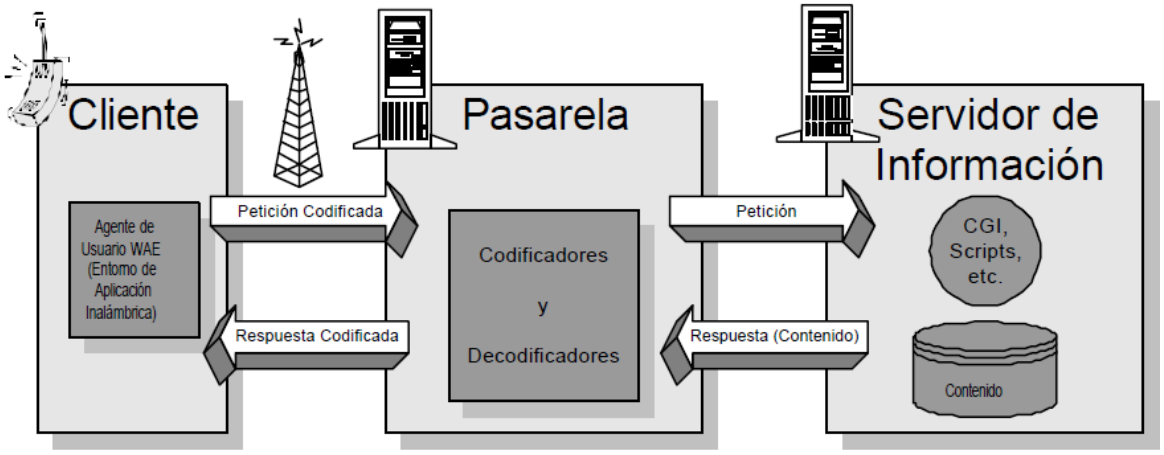
Al igual que en la encriptación, la decriptación en el receptor se realiza para cada trama 802.11, este proceso se describe en los pasos siguientes:

1) El receptor utiliza el IV enviado por el transmisor y la llave secreta compartida para generar una secuencia de llaves con el algoritmo **RC4**.
2) El receptor realiza la operación **XOR** entre la secuencia de llaves y el texto cifrado recibido para calcular el texto original y el ICV.
3) Con el **CRC-32** se calcula el valor ICV del texto original ya obtenido.
4) Si los valores ICV son iguales, acepta el mensaje; de otra forma lo rechaza.

### 2.2.2 WAP

El protocolo de Aplicaciones Inalámbricas surge como la combinación de dos tecnologías de amplio crecimiento y difusión durante los últimos años: las comunicaciones inalámbricas e Internet. Más allá de la posibilidad de acceder a los servicios de información contenidos en Internet, el protocolo pretende proveer de servicios avanzados adicionales.

Para ello, se parte de una arquitectura basada en la definida para el World Wide Web (WWW), pero adaptada a los nuevos requisitos del sistema. En la siguiente imagen se muestra el esquema de la arquitectura WAP.

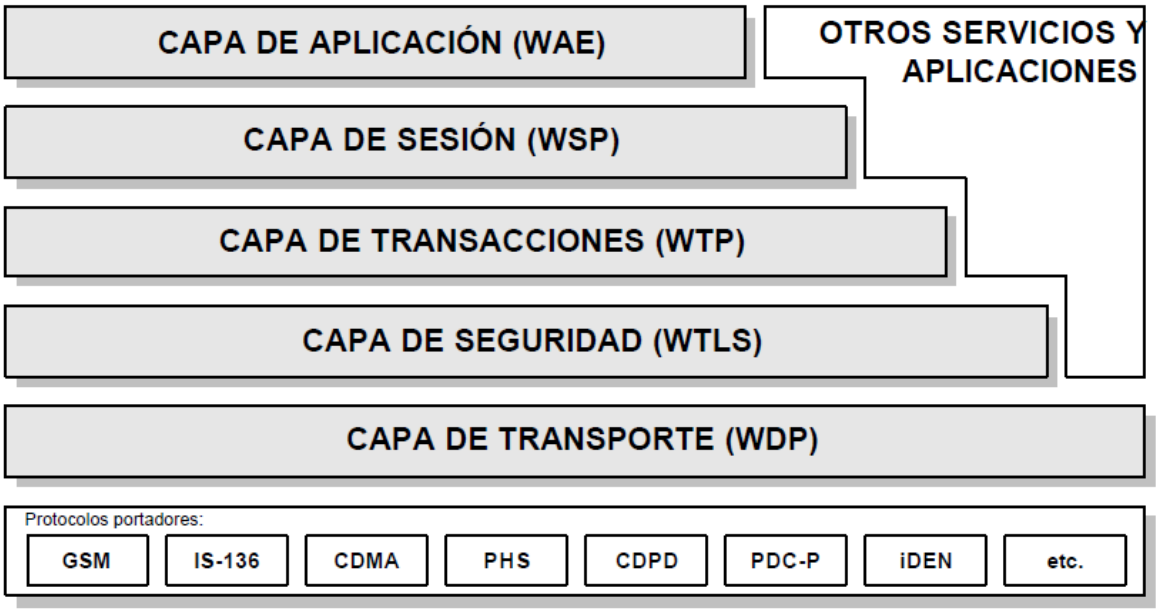


Podemos observar que en la terminal inalámbrica existiría un "micro navegador" encargado de la coordinación con la pasarela, a la cual realiza peticiones de información que son adecuadamente tratadas y redirigidas al servidor adecuado. Una vez procesada dicha petición en el servidor, se envían estos datos a la pasarela que de nuevo procesa adecuadamente para enviarlo a la terminal inalámbrica.

Para conseguir consistencia en la comunicación entre la terminal móvil y los servidores de red que proporcionan la información, WAP define un conjunto de componentes estándar:

1. Un modelo de nombres estándar. Se utilizan las URIs (Identificador Uniforme/Universal de Recurso) definidas en WWW para identificar los recursos locales del dispositivo (tales como funciones de control de llamada) y las URLs (Localización Universal/Uniforme de Recurso) también definidas en el WWW para reconocer el contenido WAP en los servidores de información.
2. Un formato de contenido estándar, basado en la tecnología WWW.
3. Unos protocolos de comunicación estándares, que permitan la interacción del micro navegador de la terminal móvil con el servidor Web en red.

La arquitectura WAP está pensada para proporcionar un entorno escalable y desplegable para el desarrollo de aplicaciones que funcionen en dispositivos de comunicación móvil. Con este propósito se define una estructura en capas, en la cual cada una de ellas es accesible por la capa superior, así como por otros servicios y aplicaciones, a través de un conjunto de interfaces muy bien definidas y especificadas. El siguiente esquema muestra la arquitectura WAP:



A continuación se explican, de una manera breve, las capas.

- **Capa de aplicación** (WAE/ Wireless Application Environment o Entorno Inalámbrico de Aplicación).

El Entorno Inalámbrico de Aplicación (WAE) tiene un propósito general basado en la combinación del World Wide Web y tecnologías de Comunicaciones Móviles.

Este entorno incluye un micro navegador, el cual posee las siguientes funcionalidades:

1) Un lenguaje denominado WML (Wireless Markup Language) similar al HTML, pero optimizado para su uso en terminales móviles.
2) Un lenguaje denominado WML Script, similar al JavaScript.
3) Un conjunto de formatos de contenido; es decir, datos bien definidos entre los que se encuentran imágenes, entradas en la agenda de teléfonos e información de calendario.

- **Capa de sesión** (WSP/ Wireless Session Protocol o Protocolo Inalámbrico de Sesión).

El Protocolo Inalámbrico de Sesión (WSP) proporciona a la Capa de Aplicación de WAP interfaz dos servicios de sesión: uno orientado a conexión que funciona por encima de la Capa de Transacciones y otro no orientado a conexión, que funciona por encima de la Capa de Transporte (y que proporciona servicio de **datagramas** seguro o no seguro).

Actualmente, esta capa consiste en servicios adaptados a aplicaciones basadas en la navegación Web, proporcionando las siguientes funcionalidades:

1) Semántica y funcionalidades del HTTP/1.1 en una codificación compacta.
2) Negociación de las características del protocolo.
3) Suspensión de la sesión y reanudación de la misma con cambio de sesión.

- **Capa de transacciones** (WTP/Wireless Transaction Protocol o Protocolo Inalámbrico de Transacción).

El Protocolo Inalámbrico de Transacción (WTP) funciona por encima de un servicio de **datagramas**, tanto seguros como no seguros, proporcionando las siguientes funcionalidades:

1) Tres clases de servicio de transacciones:

    - ✓ Peticiones inseguras de un solo camino.
    - ✓ Peticiones seguras de un solo camino.

- ✓ Transacciones seguras de dos caminos (petición-respuesta).

2) Seguridad usuario-a-usuario opcional.
3) Transacciones asíncronas.

- **Capa de seguridad** (WTLS/ Wireless **Transport Layer Security** o Capa Inalámbrica de Seguridad de Transporte).

La Capa Inalámbrica de Seguridad de Transporte (WTLS) es un protocolo basado en estándar **SSL**, utilizado en el entorno Web para la proporción de seguridad en la realización de transferencias de datos. Éste ha sido especialmente diseñado para los protocolos de transporte de WAP y optimizado con el fin de ser utilizado en canales de comunicación de banda estrecha. Por ello se han definido las siguientes características:

1) *Integridad de los datos.* Este protocolo asegura que los datos intercambiados entre la terminal y un servidor de aplicaciones no ha sido modificada y no es información corrupta.
2) *Privacidad de datos.* Este protocolo asegura que la información intercambiada entre la terminal y un servidor de aplicaciones no puede ser entendida por terceras partes, que puedan interceptar el flujo de datos.
3) *Autentificación.* Este protocolo contiene servicios para establecer la autenticidad de la terminal y del servidor de aplicaciones.

Adicionalmente, el WTLS puede ser utilizado para la realización de comunicación segura entre terminales.

- **Capa de transporte** (WDP/Wireless Datagram Protocol o Protocolo Inalámbrico de **Datagramas**).

El Protocolo Inalámbrico de **Datagramas** (WDP) proporciona un servicio fiable a los de las capas superiores de WAP y permite la comunicación, de forma transparente, sobre los protocolos portadores válidos.

Debido a que el WDP proporciona un interfaz común a los protocolos de las capas superiores, las capas de Seguridad, Sesión y Aplicación pueden trabajar independientemente de la red inalámbrica que dé soporte al sistema.

### 2.2.3 WAP2

La alianza WiFi lanzó en septiembre de 2004 el protocolo de seguridad WAP2, que suponía ser la versión certificada interoperable de la especificación completa del estándar **IEEE**

802.11i, el cual fue ratificado en junio de 2004. Para llevar a cabo la certificación se basa en las condiciones obligatorias de la última versión del estándar **IEEE** 802.11i. WAP2 es, por tanto, la implementación aprobada por la Wi-Fi Alliance interoperable con ésta.

Aunque los productos WAP siguen siendo seguros, muchas organizaciones han estado buscando una tecnología interoperable y certificada basada en el estándar **IEEE** 802.11i o han requerido del cifrado de **AES** por razones internas y reguladoras. WAP2 resuelve esas necesidades, basándose en su predecesor WAP (con el que es completamente compatible hacia atrás) y ha sido específicamente diseñado para cumplir los requisitos más exigentes de entornos empresariales.

**IEEE** 802.11i y WAP2 son virtualmente idénticos, pues las diferencias entre ambos son mínimas. Los dos emplean como código de cifrado **AES**/CCMP, en lugar de **RC4**/TKIP usado en WAP. A su vez existen dos desviaciones principales:

1) WAP2 permite funcionar en modo mixto con TKIP y CCMP para su compatibilidad hacia atrás con WAP.
2) WAP2 carece de ciertos aspectos definidos por **IEEE** 802.11i, en cuanto a servicios de voz inalámbricos, utilizados para prevenir la latencia de la señal o la pérdida de información durante el ***roaming***.

La principal de las diferencias de WAP2 respecto a WAP es que emplea, al igual que **IEEE** 802.11i, un mecanismo de cifrado más avanzado como **AES**. No obstante, WAP2 es compatible con WAP; por ello, algunos productos pueden ser utilizados en ambos por **software**. Otros, en cambio, requieren de una transformación en el **hardware**, debido a la naturaleza de cómputo intensiva del cifrado requerido para WAP2, **AES**.

Por otro lado, al igual que WAP, WAP2 permite dos modos de llevar a cabo la autenticación, dependiendo si el ámbito de aplicación es empresarial (**IEEE** 802.11X/EAP) o personal (PSK). Actualmente el **IEEE** y la Wi-Fi Alliance están intentando unificar WAP2 e **IEEE** 802.11i.

WAP2 utiliza los protocolos de autenticación definidos por el **IEEE** 802.11i y el de WAP.

El proceso de cifrado se realiza mediante lo establecido por el estándar **IEEE** 802.11i; el ya utilizado por WEP y WAP **RC4** es sustituido por **AES**, uno de bloques de clave simétrica que utiliza grupos de **bits** de una longitud fija. Un algoritmo de éstos significa que utiliza la misma clave maestra, tanto para cifrar como para descifrar los datos.

Mediante **AES**, las tramas de **bits** del texto plano son cifradas en bloques de 128 **bits**, calculados independientemente.

## 2.3 ESTÁNDAR IEEE 802.11 Y SUS VARIANTES

El protocolo **IEEE** (Institute of Electrical and Electronic Engineers) 802.11 es el estándar para comunicaciones de la **IEEE**, que define el uso de los dos niveles más bajos de la arquitectura **OSI** (Open Systems Interconnection) en la capa física y de enlace de datos, especificando sus normas de funcionamiento en una red inalámbrica. En general, los protocolos de la rama 802.X determinan la tecnología de redes de área local.

El estándar original de este protocolo data de 1997, era el **IEEE** 802.11, tenía velocidades de 1 hasta 2 **Mbps** y trabajaba en la banda de frecuencia de 2.4 GHz. La siguiente modificación apareció en 1999 y es designada como **IEEE** 802.11b, esta especificación alcanzaba de 5 hasta 11 **Mbps**, también trabajaba en la frecuencia de 2.4 GHz. Por otro lado, se realizó una especificación sobre una de 5 GHz. que conseguía los 54 **Mbps**, era la 802.11a y resultaba incompatible con los productos del 802.11b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11 g.

Como la tecnología avanza a pasos agigantados, a continuación se nombran las derivaciones del protocolo 802.11 para poder tener una idea de lo extenso que se ha vuelto.

- 802.11: Protocolo que proporciona de 1 a 2 **Mbps** en el rango de frecuencia de 2.4 GHz, usando: **FHSS** (Frequency Hopping Spread Spectrum) o DSSS (Direct Sequence Spread Spectrum).
- 802.11a: Revisión del protocolo 802.11 que proporciona 54 **Mbps** estandarizado y hasta 72 y 108 **Mbps**, con tecnologías de desdoblamiento no estandarizado en el rango de frecuencia 5 GHz. usando OFDM (Orthogonal Frequency Division Multiplexing) y DSSS.
- 802.11b: También llamado 802.11 High Rate o Wi-Fi, revisión del protocolo 802.11 que proporciona 11 **Mbps** con reducciones de 5.5, 2 y 1 **Mbps** en el rango de frecuencia 2.4 GHz., usando DSSS.
- 802.11d: Permite el uso de 802.11 en países restringidos por el uso de las frecuencias.
- 802.11e: Define el uso de QoS (Quality of Service).
- 802.11f: Define el enlace entre estaciones y Puntos de Acceso en modo viajero (***Roaming***).
- 802.11g: Protocolo que proporciona 54 **Mbps** en el rango de frecuencia 2.4 Ghz., manteniendo plena compatibilidad con el protocolo 802.11b. Puede trabajar con el protocolo 802.11a cambiando la configuración del dispositivo.

- 802.11h: Superior al 802.11a, permite asignación dinámica de canales (coexistencia con el HyperLAN). Regula la potencia en función de la distancia.
- 802.11i: Estándar que define el cifrado y la autentificación para complementar, mejorando el WEP. Mejorará la seguridad de las comunicaciones mediante el uso del WAP con su técnica llamada Temporal Key Integrity Protocol (TKIP), será aplicable a redes 802.11a (54 **Mbps**), 802.11b (11 **Mbps**) y 802.11g (22 **Mbps**). Lo desarrolla el comité formado por Cisco, VDG, Trapaza, Agere, **IBM**, Intersil y otros.
- 802.11j: Estándar que permitirá la armonización entre el **IEEE**, el ETSI HyperLAN2, ARIB (Association of Radio Industries and Businesses, Japan) e HISWAN (Hi Speed Wireless Access System).
- 802.11k: Trabajo en proceso; proporciona información para hacer las redes inalámbricas más eficientes.
    - ✓ Decisiones viajero (***roaming***).
    - ✓ Conocimiento del canal RF.
    - ✓ Nodos ocultos.
    - ✓ Estadísticas de clientes.
    - ✓ Transmisiones de control de energía (TCP).
- 802.11l: Saltado porque asimila al 802.11i.
- 802.11m: Trabajo en proceso. Propuesto para mantenimiento de redes inalámbricas.
- 802.11n:
    - ✓ Construido desde cero. (No chips en modo turbo).
    - ✓ Velocidad verdadera 100 **Mbps** (250 **Mbps** en el nivel físico).
    - ✓ Mejores distancias de operación.
- 802.11o: Trabajo en proceso. Exclusivo para voz en red inalámbrica (un cambio de código "handoff" más rápido, da la prioridad a tráfico de voz sobre datos).
- 802.11p: Trabajo en proceso. Usa la banda de 5.9 GHz para largo alcance.
- 802.11q: Trabajo en proceso. Ayuda para la VLAN (Virtual Lan).
- 802.11r: Trabajo en proceso. ("r" de ***roaming***), manejando un cambio de código "handoff" rápido cuando hay un viajero "**roaming**" entre Puntos de Acceso.
- 802.11s: Trabajo en proceso. Redes de autoayuda y de autoconfiguración.
- 802.11x: Se utiliza para resumir todos los estándares dentro del grupo de funcionamiento, pero no es un estándar.

### 2.3.1 Características del Estándar IEEE 802.11

La especificación original de 802.11 preveía conexiones a velocidades de 1 ó 2 MB/s en la banda de los 2.4 GHz, utilizando dos tipos de tecnología de espectro ensanchado (Spread Spectrum) por salto en frecuencia (**FHSS**) y secuencia directa (**DSSS**). El objetivo principal a la hora de utilizar el espectro ensanchado es transmitir ocupando una banda de frecuencias mayor de la requerida. Su creación se debe a investigaciones militares durante la Segunda Guerra Mundial, ya que de esta forma se evitaban ataques. **FHSS** se basa en que transmite en diferentes frecuencias, produciéndose saltos de una a otra, de una forma aleatoria que es imposible predecir. Por lo contrario, con DSSS (secuencia directa) se envían varios **bits** por cada bit de información real.

### 2.3.2 Operación del Estándar IEEE 802.11

La arquitectura 802.11 está integrada por varios componentes y servicios que interactúan para proporcionar la movilidad de la estación a las capas más altas del nivel de la red. El estándar **IEEE** 802.11 está orientado al desarrollo de Redes de Área Local inalámbricas con aplicación dentro de espacios interiores.

**Autentificación:** Dado que las redes inalámbricas han limitado seguridad física para prevenir el acceso desautorizado, 802.11 define de la autentificación para controlar el acceso a éstas. Su meta es proporcionar el control de acceso igual que en una red alámbrica (802.3). El servicio de la autentificación proporciona un mecanismo para una estación de identificar otra estación. Sin esta prueba de la identidad, la estación no permite utilizar la red inalámbrica para la entrega de los datos. Todas las estaciones 802.11, si son parte de un sistema de servicio básico **BSS** (Basic Service Set) independiente o de la red de un sistema de servicio extendido ESS (Extended Service Set), deben utilizar dicho servicio antes de comunicarse con otra estación. **IEEE** 802.11 define dos tipos de éste.

**Autentificación del sistema abierto:** Este es el método de la autentificación por defecto, que es un proceso muy simple, de dos etapas. Primero la estación que desea autenticar con otra envía una trama que contiene la identidad de la estación que envía. La de recepción -entonces- manda una trama que alerta cuando reconoce la identidad de la estación.

**La autentificación dominante compartida:** Este tipo de autentificación asume que cada estación ha recibido una llave compartida secreta con una independiente, segura del canal de la red 802.11. Las estaciones autentican con el conocimiento compartido de esta

llave. El uso de la autentificación dominante compartido requiere la puesta en práctica del cifrado vía WEP o el algoritmo de WEP.

**De-autentificación:** Su servicio se utiliza para eliminar a un usuario previamente autorizado para tener acceso al uso de la red en un futuro. Una vez que se "de-autentica" una estación, ésta no puede acceder a la red inalámbrica a menos que se ejecute nuevamente la autentificación.

La de-autentificación es una notificación y no puede ser rechazada. Por ejemplo, cuando una estación desee ser quitada de un **BSS**, puede enviar una trama de este servicio al punto de acceso asociado para notificar su retiro de la red. Un punto de acceso también puede bloquear una estación, enviando una trama de la de-autentificación a la estación.

**Privacidad:** El servicio de la privacidad del **IEEE** 802.11 está diseñado para proporcionar un nivel equivalente a la protección para los datos en la red inalámbrica, como es el suministrado por una red alámbrica con restricción de acceso físico. Este servicio protege los datos solamente, dado que ellos atraviesan este medio. No está diseñado para dar protección completa de datos entre las aplicaciones que corren sobre una red mezclada.

Con una red inalámbrica, todas las estaciones y otros dispositivos pueden "oír" los datos del tráfico tomando un lugar sin rango en la red, afectando seriamente el nivel de la seguridad de una conexión inalámbrica. **IEEE** 802.11 contrarresta este problema ofreciendo una opción de servicio de privacidad que levante la seguridad de la red 802.11a, la de una red alámbrica. Dicho servicio, aplicándose a todas las tramas de los datos y a algunas tramas de la autentificación, es un algoritmo de cifrado basado en el de WEP del 802.11.

**El servicio de entrega de datos:** Este servicio es similar al proporcionado por el resto del **IEEE** 802, ya que proporciona la entrega confiable de las tramas de los datos de la **MAC** (Medium Access Control) de una estación, al **MAC** en una u otras estaciones, con una mínima duplicación y reordenamiento de las tramas.

La trama del formato **MAC** se muestra en la figura que se visualiza a continuación, donde la dirección 2,3 y 4, control de la secuencia, y campos del cuerpo de la trama no se encuentran en cada una de las de transmisión. La de control es de 16 **bits** de longitud y contiene la información de control básica de ésta, incluyendo el tipo (datos, control del **MAC** o administración del **MAC**) y el subtipo, si la trama se origina o está limitada al DS (Distribution System) y si está encriptada. El campo de duración/ID indica la permanencia del resto de una secuencia del intercambio de la trama y se utiliza normalmente para controlar el mecanismo virtual del sentido de portador.

Los campos de dirección, si están presentes, contienen uno de los siguientes 48-**bits** de las direcciones de la capa de enlace de la **IEEE** 802:

- De destino.
- De la Fuente,
- Del Receptor,
- Del Transmisor,
- Identificación del Sistema Básico de Servicio (**BSSID**).

Para las redes de infraestructura, el **BSSID** es la dirección de la capa de enlace del Punto de Acceso; para las redes **ad-hoc**, es un número aleatorio generado cuando se forma la red **ad-hoc**. El receptor, el transmisor, y las direcciones de **BSSID** son las de **MAC** (de las estaciones unidas al **BSS**), que son transmitidas o recibidas de la trama sobre la red inalámbrica. El destino y las direcciones de la fuente son las de **MAC** de las estaciones inalámbricas, las cuales son el último destino y fuente de la trama.

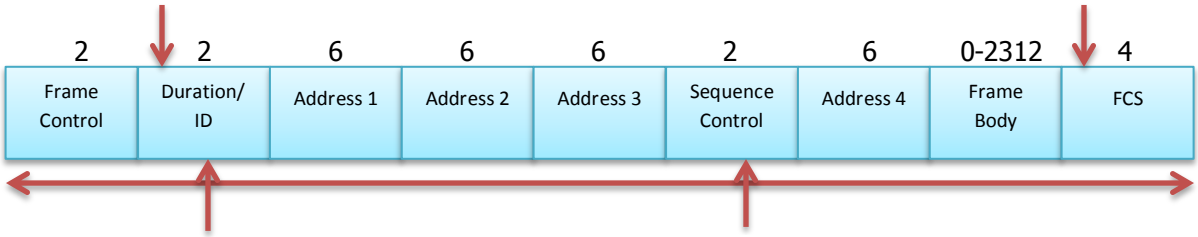
En casos como el anterior, donde están dos direcciones iguales (por ejemplo, la estación del receptor y la del destino son una); entonces se utiliza un solo campo. Cuatro de éstos están presentes únicamente en el caso infrecuente donde está el ***DS*** implementado con red de 802.11, y únicamente para las tramas que atraviesan el DS.

Un caso más típico implica una trama que se origina en una estación inalámbrica en una infraestructura **BSS** que esté limitada para una de red cableada como el 802.3. En este caso, el campo de la dirección 1 contiene el **BSSID,** el de la 2 contiene la de la estación de la fuente/transmisor, el de la 3 contiene la de destino, y el 4 no está presente. El **BSSID** y el destino (o la de la fuente para las tramas que fluyen al **BSS**) en la trama, evita requerir al Punto de Acceso y mantiene una lista de las direcciones **MAC** de las estaciones que no están en el **BSS**.

El campo de control de la secuencia es de 16 **bits** de longitud, y contiene el número de secuencia y los subcampos del número del fragmento. Las estaciones receptoras utilizan este campo para volver a reensamblar correctamente las tramas, para identificar y desechar fragmentos duplicados de la trama.

Este campo contiene un valor de duración de transmisión de trama y es necesario para implementar el mecanismo virtual de detección de portadora.

Frame Check Secuence




Los campos *address* definen el BSSID, dirección **MAC** del AP o identificador de punto de acceso, dirección fuente, destino, transmisor, receptor.

Secuencia de control de trama

Toda vez que una estación se asocie a un AP, puede comenzar a enviar y recibir las tramas de los datos hacia y desde el punto de acceso. Pero dado que múltiples estaciones pueden desear transmitir al mismo tiempo y en el mismo canal, un protocolo múltiple del acceso es necesario para coordinar estas emisiones.

Este protocolo es obligatorio para estaciones y puntos de acceso. El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar **IEEE** 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Access/Collision Advoidance), que significa que cada estación monitorea el canal antes de transmitir, y se detiene cuando detecta el canal ocupado. Aunque las redes 802.3 y 802.11 utilizan detección de portador de acceso aleatorio, los dos protocolos del **MAC** tienen diferencias importantes. Primero, en vez de usar la detección de la colisión, 802.11 usa técnicas para evitarla. En segundo lugar, debido a los índices relativamente altos del bit-error de los canales inalámbricos 802.11, utiliza un esquema de reconocimiento/retransmisión de la capa de enlace.

### 2.3.3 Tipos de codificación del Estándar IEEE 802.11

Cada protocolo maneja diferentes tipos de codificación, en el caso del 802.11a ocupa la codificación DSSS, en cambio el protocolo 802.11b y el 802.11g ocupan **FHSS** con lo cual pueden trabajar o compartirse cualquiera de éstos.

**Salto de Frecuencia (Frecuency Hopping Spread Spectrum Radio):** En el estándar **IEEE** 802.11 la portadora saltará sobre 2.4 GHz entre los límites 2.4 GHz y 2.483 GHz. Un patrón de salto determina las frecuencias en las que se transmitirá y en qué orden. Para recibir la señal adecuadamente, el receptor debe conocer ese patrón y escuchar la señal en el momento justo y frecuencia correcta.

**Secuencia Directa (Direct Sequence Spread Spectrum Radio):** El espectro ensanchado por ésta, combina una señal de datos con otra secuencia de tasa binaria elevada, a la cual se le denomina código chip (ganancia de procesado). Dicha ganancia incrementa la resistencia de la señal frente a las interferencias. El estándar 802.11 exige un mínimo de 11 **bits** para formar la secuencia (11 chips).

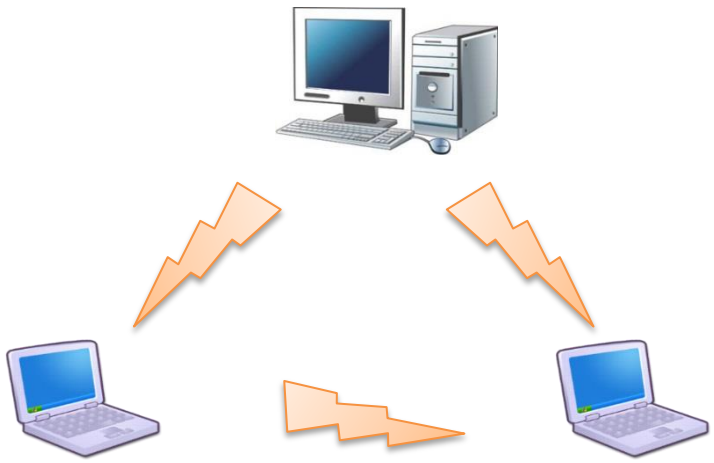
### 2.3.4 Modos de conexión

**Estación de red inalámbrica:** La estación (STA) es el componente más básico de la red inalámbrica. Una estación es cualquier dispositivo que contenga la funcionalidad del protocolo 802.11, la cual debe manejar **MAC** (Medium Access Control), PHY (Capa Física) y una conexión al medio inalámbrica. Las funciones del 802.11 se ponen en ejecución típicamente en el **hardware** y en el **software** de una tarjeta de red (NIC, **Network** Interface Card). Una estación podía ser una **PC** o computadora portátil, un dispositivo **PDA** o un punto de acceso. Éstas pueden ser móviles, portátiles o inmóviles y todas ellas deben soportar el 802.11, servicios de autentificación, de la de-autentificación, de privacidad y de entrega de los datos.

**El Servicio Básico Independiente Fijó (IBSS):** La topología más básica de la red inalámbrica es un sistema de las estaciones, que se han reconocido una de otra y están conectadas vía inalámbrica de una manera de uno a uno (**peer-to-peer**). Esta forma de topología de red se refiere a una **red ad-hoc**. En un IBSS, las estaciones móviles se comunican directamente entre ellas. Cada estación móvil puede no estar habilitada para comunicarse con otra estación debido a las limitaciones del rango.


IBSS Sistema Independiente del Servicio

**Sistema de Servicio Básico (BSS)**: Una infraestructura de Sistema de Servicio Básico es un componente llamado punto de acceso (AP). Éste proporciona una función local de la comunicación para el **BSS** y todas sus estaciones se comunican con el punto de acceso y ya no lo hacen directamente entre ellas. Todas las tramas son retransmitidas entre las estaciones por el punto de acceso (AP). Esta función local de la comunicación dobla con eficacia el rango del IBSS y puede -también- proporcionar la conexión a un sistema de distribución u otra red.



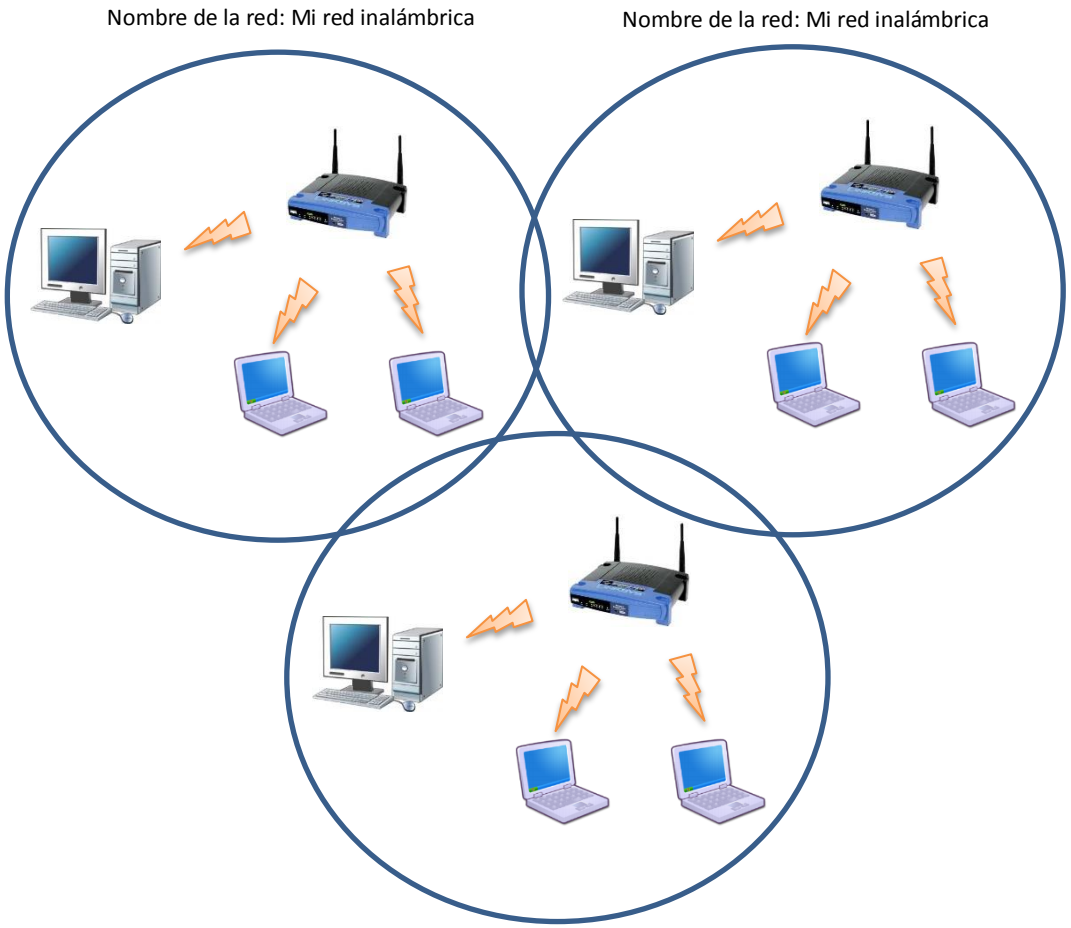
Infraestructura de Sistema de Servicio Básico (BSS)

**Sistema de Distribución (DS):** Es el medio por el cual un punto de acceso se comunica con otro, el fin es intercambiar tramas para las estaciones en su respectiva **BSS**. Estas tramas se utilizan para seguir estaciones móviles conforme se vayan moviendo de un **BSS** a otro y las intercambia por una red alámbrica. Como **IEEE** 802.11 lo describe, el sistema de distribución no es necesariamente una red, no es el lugar del estándar de alguna restricción en cómo es implementado el sistema de distribución, sólo en los servicios que debe proporcionar. Así el sistema de la distribución puede ser una red alámbrica como 802.3 o una de propósito especial que interconecta los puntos de acceso y proporciona los servicios de distribución requeridos.

**Sistema de Servicio Extendido (ESS):** La cobertura que extendía vía un Servicio Extendido (ESS) 802.11 prolonga el rango de la movilidad a uno arbitrario, a través del Sistema Extendido del Servicio (ESS), el cual pertenece a la infraestructura **BSS**, donde los puntos de acceso se comunican entre sí para remitir tráfico a partir de un **BSS** a otro, con el objetivo de facilitar el movimiento de estaciones entre **BSS**. El punto de acceso realiza esta comunicación a través del sistema de la distribución, que es la espina dorsal de la red inalámbrica y se puede construir de una red alámbrica o de la red inalámbrica.

El sistema de la distribución es típicamente una capa delgada en cada punto de acceso, que determina el destino para el tráfico recibido de un **BSS**; define si este tráfico se retransmite de nuevo a un destino en el mismo **BSS**, se remite a otro punto de acceso o se envía en la red alámbrica a un destino que no se encuentra en el sistema extendido del servicio. Las comunicaciones recibidas por un sistema de la distribución del punto de acceso se transmiten al **BSS**, mismas que serán recibidas por la estación móvil de destino.

El equipo de la red fuera del sistema extendido de servicio ve al ESS y a todas sus estaciones móviles como una sola red de la capa **MAC**, donde todas las estaciones están físicamente inmóviles. Así, el ESS oculta el desplazamiento de las estaciones de todo el exterior del ESS. Este nivel de dirección proporcionado por la arquitectura del 802.11 permite a los protocolos de red existentes, que no tienen ningún concepto de la movilidad, operar correctamente con una red inalámbrica donde sí la hay.




Sistema de Servicio Extendido (ESS)

# CAPÍTULO 3

# RED INALÁMBRICA UNIVERSITARIA (RIU)

# CAPÍTULO 3: RED INALÁMBRICA UNIVERSITARIA (RIU)

## 3.1 ¿QUÉ ES LA RIU?

La RIU es una red creada por y para la UNAM, que permite a los usuarios conectar dispositivos móviles para navegar por Internet, siempre y cuando los equipos posean las características y la tecnología suficiente para poder conectar con RIU.

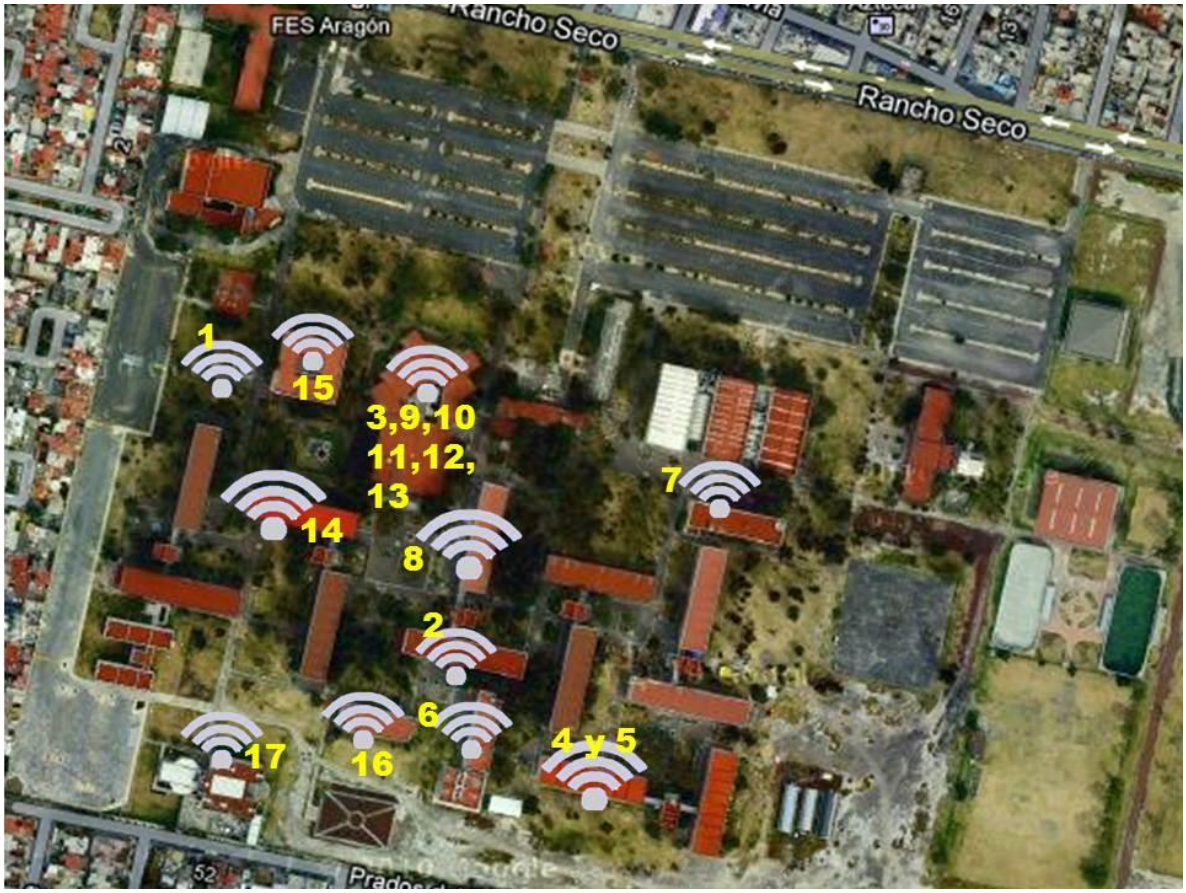
### 3.1.1 Objetivo

El objetivo de la RIU es satisfacer la necesidad que tiene la comunidad universitaria de estar conectada -constantemente- a Internet dentro del campus, con el fin de poder realizar diversas actividades académicas o administrativas en cualquier punto.

### 3.1.2 Cobertura dentro de la FES Aragón

Las antenas de RIU de la FES Aragón se trataron de colocar dentro de lugares con mayor afluencia de usuarios, con el propósito de dar cobertura a casi toda la Facultad. A continuación se puede observar un listado y un mapa en donde se encuentran estos puntos de acceso.

1. Explanada Edificio de Gobierno.
2. Explanada A1 Servicios Escolares.
3. Biblioteca Aula Magna Javier Barros.
4. Explanada de Posgrado A12.
5. Explanada de Derecho A12.
6. Explanada del Centro de Cómputo.
7. Explanada L3 Laboratorio Eléctrica.
8. Explanada Principal A4.
9. Biblioteca (Sala de Consulta).
10. Biblioteca (Sala de Estudios).
11. Biblioteca (Sala 7).
12. Biblioteca (primer piso, Sala de Estudio).
13. Biblioteca (primer piso, Sala 2).
14. Explanada A3.
15. Edificio de Gobierno.
16. Centro de Lenguas Extranjeras (CELE).
17. Centro Tecnológico.




### 3.2 Características de la RIU (software)

Como se puede observar en la imagen y la lista anterior, RIU se encuentra tanto en lugares cerrados como abiertos, con la finalidad de que los usuarios puedan moverse libremente sin perder la conexión a Internet. Como es lógico, no se pueden utilizar los mismos recursos para ambos espacios; ya que algunas antenas no pueden ser las adecuadas para cubrir ciertas zonas.

RIU es controlada por un **switch** central que se localiza en C.U. (Ciudad Universitaria), de allá llega la señal al **site** y posteriormente es repartida a los diferentes AP'S (Puntos de Acceso) que se encuentran dentro de la Institución. Posteriormente veremos las especificaciones de los equipos que se emplearon para dar vida a RIU dentro de la Facultad.

Para que RIU pueda funcionar de una manera óptima debe someterse a estándares de comunicación y protocolos de seguridad.

Los estándares de comunicación que utiliza RIU son el 802.11 a/b/g. A continuación se explicará cada uno de ellos.

**Características del 802.11a**:

Mientras se desarrollaba la 802.11b, la **IEEE** creaba una nueva extensión del estándar 802.11 denominada 802.11a. Debido a que la 802.11b ganó popularidad rápidamente, mucha gente cree que la 802.11a se creó después de ésta; aunque en realidad se desarrollaron a la vez.

Debido a su alto costo, la 802.11a suele utilizarse en redes de empresas, mientras que la 802.11b se usa más en redes domésticas. La 802.11a soporta velocidades de hasta 54 Mbits/s y trabaja a 5 GHz. Comparada con la 802.11b, a mayor frecuencia limita el rango de la 802.11a; además, el trabajar con una frecuencia superior significa que tiene más dificultades para atravesar muros y objetos. Por otro lado, como ambos estándares utilizan frecuencias distintas, sus tecnologías son incompatibles entre ellas. Algunos fabricantes ofrecen híbridos 802.11 a/b; aunque estos productos lo que tienen -realmente-son las dos extensiones implementadas.

**Características del 802.11b:**

La 802.11b utiliza la misma frecuencia de radio que el tradicional 802.11 (2.4 GHz); el problema es que al no tener regulación, se podían causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si sus instalaciones están a una distancia razonable de otros elementos, dichas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el costo de sus productos; a pesar de que esto suponga utilizar una frecuencia sin regulación.

**Características del 802.11g:**

Entre 2002 y 2003 apareció un nuevo estándar denominado 802.11g. Éste intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b, al mismo tiempo que permite velocidades de hasta 54 Mbs y utiliza la banda de frecuencia de 2.4 GHz. Además, al trabajar en la misma banda de frecuencia, el 802.11g es compatible con el 802.11b, por lo que puntos de acceso de uno pueden trabajar en redes del otro y viceversa.

Los protocolos de seguridad tienen el objetivo de evitar, o bien dificultar, ataques de carácter malicioso. Precisamente RIU adoptó como protocolo de seguridad a WAP; en el capítulo 2 se vio a fondo este protocolo, así es que daré un panorama amplio sobre el que resguarda la seguridad de la red.

WAP (Wireless Application Protocol / Protocolo de Aplicaciones Inalámbricas) surge como la combinación de dos tecnologías de amplio crecimiento y difusión durante los últimos años: las comunicaciones inalámbricas e Internet. Más allá de la posibilidad de acceder a los servicios de información contenidos en Internet, el protocolo pretende proveer de servicios avanzados adicionales.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA posee las siguientes tecnologías:

**IEEE 802.1:**

Estándar del **IEEE** de 2001 para proporcionar un control de acceso en redes basadas en "puertos"; este concepto que en un principio fue pensado para las ramas de un **switch**, ahora también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Éstas últimas tratarán -por lo tanto- de conectarse a un puerto del punto de acceso, el cual mantendrá dicho puerto bloqueado hasta que el usuario se autentifique. Con tal fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*), como puede ser RADIUS (*Remote Authentication Dial-In User Service*).

Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

**EAP**:

EAP, definido en la RFC 2284, es el *protocolo de autentificación extensible* que -como su nombre lo dice- lleva a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el PPP (*Point-to-Point Protocol*); aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X, bajo el nombre de EAPOL (*EAP over LAN*).

**TKIP (*Temporal Key Integrity Protocol*):**

Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

**MIC (*Message Integrity Code*):**

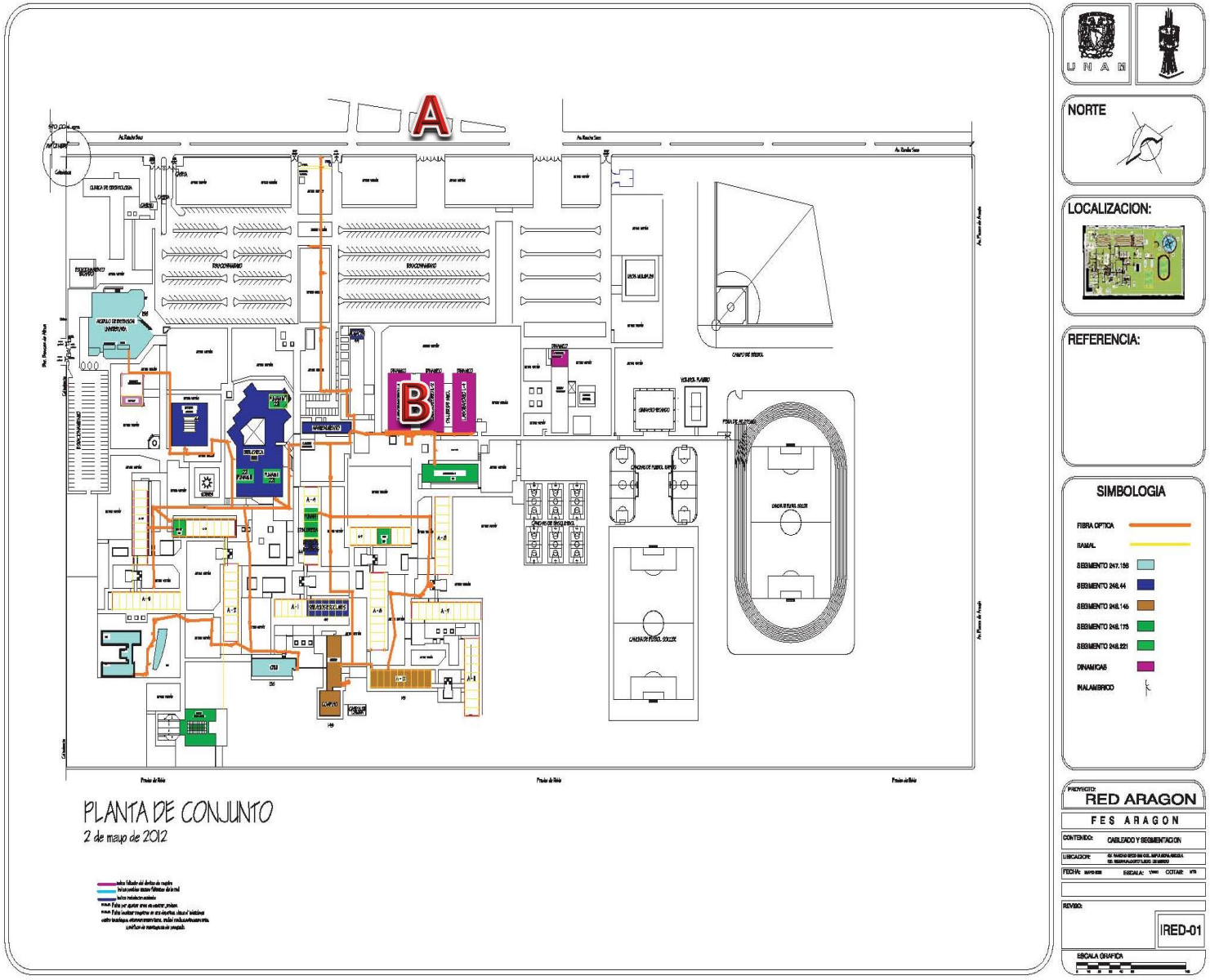
Código que verifica la integridad de los datos de las tramas.

### 3.3 Estructura física de la RIU dentro de la FES Aragón.

En el punto 3.1.2 se puede observan cómo se encuentran distribuidas las antenas de RIU en la FES Aragón; para poder llegar a todos esos espacios es necesario saber de dónde llega la señal que alimenta a los Puntos de Acceso (AP).

En el siguiente mapa se puede apreciar la estructura de la fibra óptica (resaltada en color naranja) dentro de la FES Aragón; es importante conocer cómo se encuentra ésta, ya que por este medio llega la señal desde C.U. y se dirige a las antenas asignadas a RIU.

En el mapa aparece una letra "A", ésta nos marca por dónde entra la señal a la Facultad y se desplaza hasta llegar al punto B, que es donde se localiza el **site** y aquí entra a los equipos necesarios para distribuir la señal.

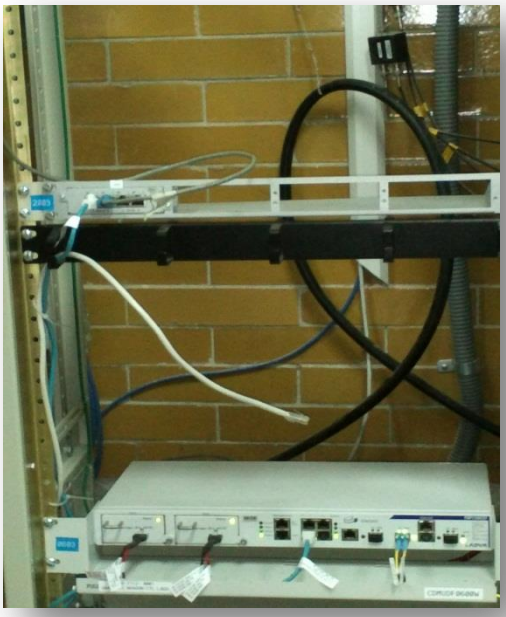

A
B
PLANTA DE CONJUNTO
2 de mayo de 2012
UNAM
NORTE
LOCALIZACION:
REFERENCIA:
SIMBOLOGIA
FIBRA OPTICA
RAMAL
SEGMENTO 247.156
SEGMENTO 248.44
SEGMENTO 248.145
SEGMENTO 248.175
SEGMENTO 248.221
DINAMICAS
INALAMBRICO
PROYECTO:
RED ARAGON
FES ARAGON
CONTENIDO:
CABLEADO Y SEGMENTACION
RED-01
ESCALA GRAFICA

Los equipos que intervienen en la distribución de señal a los diferentes Puntos de Acceso de RIU, que se encuentran dentro de la FES Aragón, son enumerados a continuación; van del primer equipo que recibe la señal, hasta el último que se encarga de llegar a los Puntos de Acceso:

1. En esta primera imagen se puede observar el cable de Telmex que viene de la calle. La señal que viaja por aquí procede de C.U.

2. Inmediatamente se conecta al **Rack** de Telmex, llamado RDA, que contiene las "acometidas de fibra óptica" para el ingreso de servicios digitales (voz y datos).

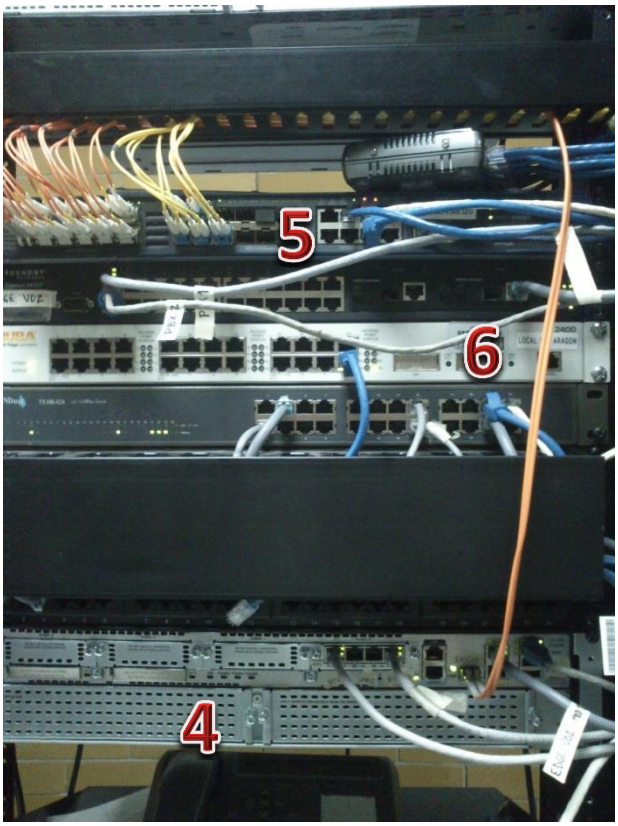
3. Después de llegar al Telmex RDA, pasa a un equipo llamado FSP150 CCf de la marca ADVA, el cual forma parte de la Plataforma para Servicios sobre Fibra (FSP) y presenta dispositivos para implementar la demarcación, extensión y agregación de servicios **Ethernet**, diseñados para soportar la entrega de los **Ethernet** inteligentes.



Los FSP 150 incorporan las más avanzadas capacidades de OAM (Operación, Administración y Gestión) y la demarcación Etherjak®, permitiendo a los operadores entregar servicios **Ethernet** inteligentes que puedan ser monitoreados y administrados remotamente, con un mínimo de visitas a los sitios. Asimismo, proveen la inteligencia necesaria para alentar a usuarios empresariales de datos a cambiar de **frame relay**, enlaces dedicados y servicios ATM al de **Ethernet** de grado operador ("**Carrier-Class**"); permiten al proveedor entregar **Ethernet** prácticamente en cualquier lugar, por medio de un amplio rango de opciones de transporte, para extender el **Ethernet** sobre facilidades de fibras ópticas, cobre, TDM/PDH y SONET/SDH.

4. Del FSP 150 la señal es llevada al **Router** de Cisco 2921, que es el principal, el cual nos llevará a distribuir los servicios (voz y datos). Este **router** posee las siguientes características técnicas:
   - 3 puertos 10/100/1000 integrados con un puerto capaz de conectar un RJ-45 o SFP.
   - Una ranura para el módulo de servicio.
   - 4 ranuras mejoradas de alta velocidad para tarjeta de interfaz WAN (EHWIC).
   - 3 ranuras para procesador de señal digital (DSP).
   - 1 servicio interno para la ranura de módulo de servicios de aplicaciones.
   - Energía totalmente integrada de distribución de los modelos de soporte 802.3 af Power over **Ethernet** (PoE) y Cisco PoF mejorada.
   - Integrado con aceleración por **hardware**, en encriptación **VPN**.

- Comunicaciones seguras en colaboración con el Grupo de **VPN** encriptado de transporte, Dynamic Multipoint **VPN** o el Easy **VPN**.
- Control de amenazas, integrado con Cisco IOS **Firewall**, Cisco IOS basada en zonas, IOS de Cisco **IPS** y Cisco **IOS Contente Fitering**.
- La administración de identidades: esta es de forma inteligente, protege los puntos finales que utilizan la autenticación, autorización y contabilidad (AAA) y la infraestructura de clave pública.




5. Después pasa la señal por el **router** CISCO 2921, llega al **Switch** de 3com (el principal) 3CRS48G-24S-91 (4800G), éste ofrece conmutación Gigabit, con enrutamiento **unicast** y **multicast** completo en una unidad de IU de altura. El modelo 3com 4800G cuenta con 24 conexiones frontales para puertos 10/100/1000 **Mbps**. de triple velocidad, de los cuales cuatro son combinados compartidos con puertos SFP de fibra de 100/1000 **Mbps**. Dos ranuras traseras admiten expansión de 10 GB de 1 ó 2 puertos, para conexiones locales unidad a unidad de gran ancho de banda y enlaces ascendentes. Todos los **switch** 4800G son totalmente compatibles con el enrutamiento y la gestión **IP**v4 e **IP**v6. Estos modelos **IP**v4/**IP**v6 de pila dual admiten los principales protocolos de enrutamiento de N3, protocolos **multicast** y mecanismos de enrutamiento de directivas, para garantizar una migración sin problemas de **IP**v4 a **IP**v6.

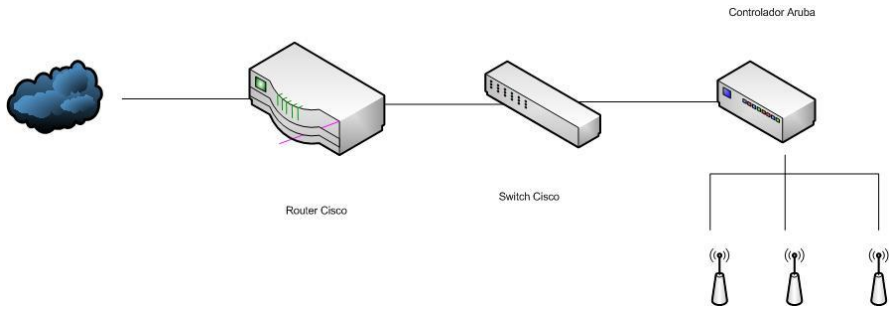
6. Para finalizar tenemos el control de Movilidad Aruba MC-2400 que se encarga de establecer el mando de las antenas o AP. Cuando se llega a caer el enlace en C.U. manda el control de las antenas y éste se encarga de la salida.

El controlador de Movilidad Aruba MC-2400 pertenece a la LAN inalámbrica que incorpora todas las funciones necesarias y permite agregar hasta 48 puntos de acceso o AP, manejados para proporcionar una seguridad y un mando centralizado en los despliegues inalámbricos. El MC-2400 permite una auténtica experiencia de red centrada en el usuario que ofrece una conectividad "**follow-me**", un acceso

basado en identidad y servicios de continuidad de aplicación, muy adecuados para despliegues inalámbricos en sedes regionales u oficinas densas. Se despliega fácilmente como una superposición sin interrumpir la red existente de cable y se puede gestionar de forma centralizada con ArubaOS o el sistema de gestión de movilidad Aruba. Actividades de convergencia avanzada, tales como el Control de Admisión de Llamadas (CAC, en inglés Call Admission Control), la gestión RF con reconocimiento de voz y la calidad de servicio estricta en el aire, permiten al MC-2400 proveer funcionalidades **VoIP** móviles.

Asimismo, el controlador MC-2400 se puede desplegar como un **gateway** de seguridad, basado en identidad para autentificar a los usuarios conectados por cable e inalámbricos, aplicar las políticas de control de acceso basadas en roles y poner en cuarentena a los clientes finales no seguros, para que no accedan a la red corporativa. Los usuarios invitados se soportan fácilmente y con seguridad mediante el servidor de portal cautivo incorporado y los servicios avanzados de red. El MC-2400 puede crear un entorno de red seguro sin necesidad de otros dispositivos **VPN**/cortafuegos, gracias a las funcionalidades **VPN** y **NAT** sitio a sitio integrados, túneles **split-tunneling** y un cortafuegos **stateful** (conforme a ICSA). El soporte de **VPN** sitio a sitio se puede integrar con los principales concentradores **VPN** para facilitar que la incorporación con las **VPN** existentes de la organización sea un éxito.

Por último, esta imagen muestra -de una manera más sencilla- cómo están conectados los equipos que le dan vida a RIU.



## 3.4 El entorno de RIU

### 3.4.1 Características de antenas Aruba

Para poder seleccionar el tipo de AP'S que serían usados en RIU DGSCA (ahora **DGTIC**), se buscó -en ese entonces- una empresa que lograra satisfacer los requerimientos que ésta necesitaba. Entre las empresas que presentaron sus productos estuvieron: Colubris **Networks**, Enterasys **Networks**, Foundry **Networks** y Aruba **Networks**.

Esta última empresa fue la que satisfacía los lineamientos necesarios para llevar a cabo el proyecto. Los modelos de antenas empleados fueron 3, ya que cada una de ellas cubre un área. En específico se usó la Aruba 70 para interiores amplios, misma que soporta alrededor de 300 personas; Aruba 61 para interiores reducidos, la cual tiene soporte para -aproximadamente- 50 personas y Aruba 60 para exteriores, ya que por la cantidad de usuarios eran necesarias antenas externas de alta ganancia.

A continuación se mostrarán las fichas técnicas de los AP'S utilizados para RIU, obtenidas de la página oficial de Aruba http://www.arubanetworks.com

**Aruba AP-70**

El Aruba AP-70 es un punto de acceso inalámbrico de interior, de alto rendimiento de doble radio (banda dual simultánea 802.11a más b/g), con numerosas funciones como entrada y monitorización de WLAN, detección y prevención de intrusiones inalámbricas y mallas seguras de empresa en los espectros RF de 2,4-2,5 GHz y 5 GHz. El AP-70 admite diversas opciones de instalación y ofrece servicios y aplicaciones de red basados en usuario para entornos de empresas, centros universitarios, sucursales y espacios de venta; así como ubicaciones remotas a través de redes públicas o privadas, gracias a su avanzada funcionalidad de punto de AP remoto.

El AP-70 se gestiona de forma centralizada desde un controlador de movilidad Aruba y ofrece al administrador de red un dominio sin precedentes sobre los servicios, la seguridad y los modelos de implementación. La flexibilidad de interfaces del AP-70 no tiene igual en un punto de acceso, ya que incorpora una interfaz **Ethernet** dual 10/100, PoE redundante 802.3af y una USB 2.0 para extensión de servicios. El AP-70 incorpora antenas duales integrales, omnidireccionales y multibanda de alto rendimiento y es compatible con las externas, mediante conexiones extraíbles cuádruples.

**APLICACIÓN**

- Aplicaciones de alto rendimiento en empresas y campus universitarios, sucursales y espacios de venta en los que se requiere flexibilidad de interfaces, también puede ser usado en interiores. Además funciona en aplicaciones de acceso remoto y de conector seguro.

**MODO DE FUNCIONAMIENTO**

- WLAN multiservicio 802.11a+b/g, Air Monitor 802.11a+b/g, combinación híbrida de punto de acceso remoto y Air Monitor de WLAN, todos ellos con conector seguro.

**RADIOS**

- Radio doble; configurables por **software** para 802.11a y 802.11b/g.

**GESTIÓN DE RF**

- Control automático de potencia de transmisión y gestión de canales con corrección automática de agujeros de cobertura, mediante Gestión de Radio Adaptativa (ARM, Adaptive Radio Management)

**SERVICIOS DE MOVILIDAD**

- Servicios de punto de acceso virtual:

- Admite hasta 32 SSID por punto de acceso.
- Múltiples portales cautivos por SSID.
- Admite cualquier combinación de tipos de cifrado/autenticación por SSID.
- QoS de nivel de sesión.
- Reparto de carga de VLAN.
- Creación y gestión de cuentas de invitados.

- Servicios de voz:

- QoS WMM (Wireless Multi-media).
- Etiquetado de 802.1p y DSCP a WMM.
- Asignación de prioridad de tráfico de subida.
- Control de admisión de llamadas (CAC, Call Admission Control).
- Clasificación de tráfico/reserva de ancho de banda de sesión (T-SPEC/TCLAS).
- Ahorro de energía automático no programado (U-APSD, Unscheduled Power Save Delivery).
- Control de sesión **stateful** (QoS de clientes de voz).
- SIP
- NOE
- Cisco Skinny.
- Vocera.

- SVP (Spectralink Voice Prioritization).
- Compatible con Proxy-ARP y filtrado de **multicast.**
  - Battery Boost.
  - Colas de prioridad.
  - ARM con escaneo consciente de la voz.

**ESPECIFICACIONES DE RADIO 802.11A**

● Frecuencia de funcionamiento: 5,150 GHz – 5,950 GHz.

● Canales disponibles: gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado.

● Modulación: multiplexado por división de frecuencias ortogonales (OFDM, Orthogonal Frequency Division Multiplexing).

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.):

- 54, 48, 36, 24, 18, 12, 9, 6 con ralentización automática.

**ESPECIFICACIONES DE RADIO 802.11B**

● Frecuencia de funcionamiento: 2,4 GHz – 2,5 GHz.

● Canales disponibles: gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado.

● Modulación: espectro disperso de secuencia directa (DSSS, Direct- Sequence Spread-Spectrum).

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.): 11, 5.5, 2, 1 con ralentización automática.

**ESPECIFICACIONES DE RADIO 802.11G**

● Frecuencia de funcionamiento: 2,4 GHz – 2,5 GHz.

● Canales disponibles: gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado.

● Modulación: multiplexado por división de frecuencias ortogonales (OFDM, Orthogonal Frequency Division Multiplexing).

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.): 54, 48, 36, 24, 18, 12, 9, 6 con ralentización automática.

**CANALES DISPONIBLES 802.11A/B/G**

● Gestionados de forma centralizada por el controlador de movilidad, en función del dominio regulatorio configurado.

● Gestionados por el controlador de movilidad, dependen del dominio regulatorio Configurado.

**ANTENA**

● Doble dipolo integral, omnidireccional, multibanda (soporta diversidad espacial).
- Ganancia:
- 2,4 GHz-2,5 GHz / 4,46 **dBi**.
- 5,150 GHz / 7,21 **dBi**.
- 5,350 GHz / 6,49 **dBi**.
- 5,850 GHz / 5,23 **dBi**.
● Cuatro interfaces RP-SMA (2 por radio) para antenas externas.

**Interfaces**
● Red:
- 2 x 10/100Base-T **Ethernet** (RJ45), autodetección de velocidad de enlace y MDI/MDX.
- Power-over-**Ethernet** (PoE) 48 V CC con soporte de **IEEE** 802.3af (carga compartida entre ambos puertos).
- Serie por **Ethernet** (SoE, Serial-over-**Ethernet**) (puerto principal).
● Alimentación:
- 1 x 5 V CC hasta 2,5 A (para adaptador de alimentación CA externo).
● Antena:
- 4 interfaces de antena RP-SMA (2 por radio).

**ALIMENTACIÓN**
● Power-over-**Ethernet** (PoE) 48 V CC con soporte de 802.3af.
● 5 V CC para alimentación CA externa (el adaptador se vende por separado).

**MONTAJE**
● Estándar:
- Sobremesa.
- Mural.
● Kit de montaje opcional:
- Mural seguro.
- Raíl para techo (15/16").
● Seguridad:
- Tornillo de seguridad.
- Anclaje de seguridad Kensington.

**CARACTERÍSTICAS FÍSICAS**
● Dimensiones/peso:
● Antena plegada:
- 7,4" x 6,8" x 1,4"
- 188 mm x 173 mm x 36 mm
- 0,52 kg.
● Antena extendida 180°:
- 7,4" x 11,7" x 1,4"

- 188 mm x 295 mm x 36 mm
● Dimensiones/peso (paquete enviado):
- 10,1" x 10,4" x 4,1"
- 257 mm x 264 mm x 104 mm

- 0,91 kg.

**CARACTERÍSTICAS MEDIOAMBIENTALES**

● En funcionamiento:
- Temperatura: de 0°C a 50°C (de 32°F a 122°F).
- Humedad: de 5 a 95% sin condensación.
● En almacenamiento:
- Temperatura: de 0°C a 70°C (de 32°F a 158°F).

**NORMATIVAS**

● FCC Parte 15.
● Industria de Canadá
● VCCI.
● MIC.
● PSE Mark: adaptadores/cables.
● Anatel.
● NOM/COFETEL.
● SRRC.
● GS Mark.
● CE Mark.
● Directiva R&TTE - 1995/5/CE.
● Directiva de baja tensión - 72/23/CEE.
● EN 300.328.
● EN 301.893.
● EN 301 489.
● UL/IEC/EN 60950-1:2001 CB, cULus.
● AS/NZS 4268, 4771.
● Medical EN 60601-1, -2
● UL2043 Listed.

**CERTIFICACIONES**

● Certificación Wi-Fi: 802.11a/b/g

## Aruba AP-60 y AP-61

Los dispositivos Aruba AP-60 y AP-61 son puntos de acceso inalámbricos de interior, de alto rendimiento de radio única (banda dual 802.11a o b/g) con numerosas funciones como entrada y supervisión de WLAN, detección y prevención de intrusiones inalámbricas y malla segura de empresa en los espectros RF de 2,4-2,5 GHz y 5 GHz. Los AP-60 y AP-61 de Aruba admiten diversas opciones de instalación y ofrecen aplicaciones y servicios seguros, enfocados al usuario en entornos de sedes centrales de empresas, sucursales o instituciones universitarias, así como de forma remota a través de redes públicas o privadas, actuando como puntos de acceso remotos o móviles. El AP-60 y el AP-61 se gestionan de forma centralizada desde un controlador de movilidad Aruba y ofrecen al administrador de red un manejo sin precedentes sobre los servicios, la seguridad y los modelos de implementación. El AP-60 puede equipar antenas externas a través de su doble interfaz para las desmontables; el AP-61 admite dos antenas integradas omnidireccionales multibanda de alto rendimiento.

**APLICACIÓN**

- Instalaciones de empresa de alta densidad y sucursales. Oficina remota, acceso a WLAN y monitorización del aire. Aplicaciones de interior.

**MODO DE FUNCIONAMIENTO**

- WLAN multiservicio 802.11a/b/g, Air Monitor 802.11a/b/g, combinación híbrida de punto de acceso WLAN, Air Monitor y punto de acceso remoto.

**RADIOS**

- Radio única, configurable por **software** para 802.11a o 802.11b/g

**GESTIÓN DE RF**

- Control de potencia de transmisión y gestión de canales automáticos con corrección automática de agujeros de cobertura, mediante Gestión de radio adaptativa (ARM, Adaptive Radio Management).

**SERVICIOS DE MOVILIDAD**

- Servicios de punto de acceso virtual:

- Admite hasta 16 SSID por punto de acceso.
- Portales cautivos múltiples por SSID.
- Admite cualquier combinación de tipo de cifrado/autenticación por SSID.
- QoS de nivel de sesión.
- Reparto de carga de VLAN.
- Creación y gestión de cuentas de invitados.

● Servicios de voz:

- QoS Wireless Multimedia (WMM).
- Etiquetado 802.1p y DSCP a WMM AC.
- Priorización del tráfico de subida.
- Control de admisión de llamadas (CAC).
- Clasificación de tráfico/reserva de ancho de banda de sesión (T-SPEC/TCLAS).
- Ahorro de energía automático no programado (U-APSD, Unscheduled Power Save Delivery).
- Seguimiento **stateful** de sesiones (QoS de cliente de voz **software**)
- SIP.
- NOE.
- Cisco *Skinny*.
- Vocera.
- Spectralink Voice Prioritization (SVP).
- Soporte de proxy ARP y filtrado de **multicast**.
- Battery Boost.
- Colas con prioridades.
- Soporte de escaneo con reconocimiento de voz en ARM.

**ESPECIFICACIONES DE RADIO 802.11A**

● Frecuencia de funcionamiento: 5,150 GHz – 5,950 GHz

● Canales disponibles: gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado.

● Modulación: multiplexado por división de frecuencia ortogonal (OFDM, Orthogonal Frequency Division Multiplexing).

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.): 54, 48, 36, 24, 18, 12, 9, 6 con fallback automático

**ESPECIFICACIONES DE RADIO 802.11B**

● Frecuencia de funcionamiento: 2,4 GHz – 2,5 GHz

● Canales disponibles: Gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado

● Modulación: Direct-Sequence Spread-Spectrum (DSSS)

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.): 11, 5.5, 2, 1 con fallback automático.

**ESPECIFICACIONES DE RADIO 802,11G**

● Frecuencia de funcionamiento: 2,4 GHz – 2,5 GHz.

● Canales disponibles: gestionados por el controlador de movilidad, dependen del dominio regulatorio configurado.

● Modulación: multiplexado por división de frecuencia ortogonal (OFDM, Orthogonal Frequency Division Multiplexing).

● Potencia de transmisión: configurable en intervalos de 0,5 dBm.

● Velocidades de asociación (**Mbps**.): 54, 48, 36, 24, 18, 12, 9, 6 con fallback automática.

**CANALES DISPONIBLES 802.11A/B/G**

● Gestionados de forma centralizada por el controlador de movilidad, en función del dominio regulatorio configurado,

**ANTENA**

● AP-60: doble interfaz RP-SMA para antenas externas (compatible con diversidad espacial).

● AP-61: doble dipolo integrado, omnidireccional, multibanda (compatible con diversidad espacial).

● Ganancia:

- 2,4 GHz-2,5 GHz / 2,8 **dBi**
- 5,150 GHz-5,350 GHz / 3,9 **dBi**
- 5,950 GHz / 4,0 **dBi**

**INTERFASES**

● Red:

- 1 x 10/100Base-T **Ethernet** (RJ45) con autodetección de velocidad de enlace y MDI/MDX.
- Power-over-**Ethernet** (PoE) 48 V CC compatible con **IEEE** 802.3af.
- Serie por **Ethernet** (SoE, Serial-over-**Ethernet**).

● Alimentación:

- 1 x 5 V CC hasta 1,5 A (para adaptador de alimentación CA externo).

● Antena: (sólo AP-60).

- 2 x interfaz RP-SMA de antena multibanda.

**ALIMENTACIÓN**

● Power-over-**Ethernet** (PoE) 48 V CC compatible con **IEEE** 802.3af.

● 5 V CC para alimentación CA externa (el adaptador se vende por separado).

**MONTAJE**

● Estándar:

- Sobremesa (soporte).
- Mural.

● Kit de montaje opcional:

- Mural seguro.
- Raíl para techo (15/16").

● Seguridad:

- Tornillo de seguridad.
- Anclaje de seguridad Kensington.

**CARACTERÍSTICAS FÍSICAS**

AP-60

● Dimensiones/peso:

- 6,25" x 3,9" x 1,1"
- 159 mm x 99 mm x 28 mm
- 0,23 kg.

● Dimensiones/peso (incluida la caja):

- 11,3" x 5,6" x 1,6"
- 287 mm x 142 mm x 41 mm
- 0,45 kg.

AP-61

● Dimensiones/peso:

- 8,5" x 3,9" x 1,1"
- 216 mm x 99 mm x 28 mm
- 0,27 kg.

● Dimensiones/peso (incluida la caja):

- 11,3" x 5,6" x 1,6"
- 287 mm x 142 mm x 41 mm
- 0.5 kg.

**CARACTERÍSTICAS MEDIOAMBIENTALES**

● En funcionamiento:

- Temperatura: de 0°C a 50°C (de 32°F a 122°F).
- Humedad: de 5 a 95% sin condensación.

● En almacenamiento:

- Temperatura: de 0°C a 70°C (de 32°F a 158°F).

**NORMATIVAS**

● FCC Parte 15.

● Industria de Canadá.

- VCCI.
- MIC.
- PSE Mark: adaptadores/cables.
- Anatel.
- NOM/COFETEL.
- SRRC.
- GS Mark.
- CE Mark.
- Directiva R&TTE - 1995/5/CE.
- Directiva de baja tensión - 72/23/CEE.
- EN 300.328
- EN 301.893
- EN 301 489
- UL/IEC/EN 60950-1:2001 CB, cULus.
- AS/NZS 4268, 4771
- Medical EN 60601-1, -2
- UL2043 Listed.

**CERTIFICACIONES**

- Certificación Wi-Fi: 802.11a/b/g

### 3.4.2 RIU ante las fallas de seguridad

Ante el incontenible avance tecnológico dentro de Internet, nos podemos encontrar con un sinfín de usuarios con características diferentes; por lo tanto, con actividades y necesidades diversas, las que al tratar de satisfacer pueden afectar a otros usuarios de la red.

Como bien sabemos, cualquier tipo de red puede presentar vulnerabilidad y ésta se da de acuerdo a sus características físicas; de tal manera, son posibles los problemas por interferencias electromagnéticas o por los límites físicos establecidos en una red cableada.

Desde que la UNAM concibió a RIU se planteó todas las posibilidades que conlleva una red inalámbrica de este tipo, ya que no sólo se concentraría en Ciudad Universitaria sino que llegaría a otras dependencias de la UNAM. Considerando la extensión de la red en automático, se pensó en contar con herramientas para asegurar la integridad de la red y de sus usuarios. Por tal motivo, la Dirección de Telecomunicaciones y el Departamento de Seguridad en Cómputo (DSC/UNAM-CERT) de la DGSCA desarrollaron el proyecto y los mecanismos para garantizar una operación eficiente y confiable de la red.

Los mecanismos utilizados para mitigar los riesgos identificados en las etapas iniciales de concepción de la RIU fueron: creación de políticas, control de acceso, integridad y confidencialidad.

#### 3.4.2.1 Tipos de ataques y fallas de seguridad WI-FI

Como sabemos la tecnología Wi-Fi es muy vulnerable, pues viaja a través del aire y es fácil que alguien con conocimientos y algunas herramientas puedan realizar diversos tipos de ataques.

Los ataques que se pueden realizar se dividen en 2 grupos: ataques pasivos y ataques activos. Los primeros son aquellos donde alguien "no autorizado" accede a la información sin modificarla y los segundos son aquellos en donde alguien -también- "no autorizado" modifica el contenido de la información o impide la utilización de la misma.

Dentro de los ataques pasivos podemos mencionar:

- ✓ Vigilancia/Espiar: el **hacker** monitorea el flujo de la información para descubrir el contenido.
- ✓ Análisis de Tráfico: El intruso captura la información transmitida y trata de descubrir datos sobre los parámetros de comunicación como son SSID, contraseñas o **direcciones MAC**.

Se consideran ataque activos los siguientes:

- Enmascaramiento (robo de identidad): El **hacker** se hace pasar por un usuario autorizado para poder tener acceso a la información.
- Retransmisión (Man-In-The-Middle): El atacante se coloca en medio del transmisor y el receptor, con la finalidad de recibir la información y una vez que tiene acceso a ella la retransmite para evitar ser descubierto.
- Alteración: El intruso modifica la información, esto quiere decir que puede quitar o adicionar el contenido de lo que se transmite.
- Denegación de Servicio (DoS): El **hacker** impide el uso normal de las transmisiones Wi-Fi, para quien es muy difícil evitar este tipo de ataques, ya que son muy sencillos de realizar.

Después de ver lo anterior, podríamos llegar a la conclusión de que algunos de estos ataques pueden ser inofensivos; pero no es así, ya que los riesgos a que se expone un particular o una empresa son enormes, si se considera que la utilización de recursos de Wi-Fi puede ser utilizada para realizar las siguientes acciones:

- ✓ Enviar **Spam** (por consecuencia estropear la reputación del dominio).
- ✓ Sembrar virus informáticos y troyanos en Internet.
- ✓ Distribuir **Spyware**.

- ✓ "**Hackear**" a otras organizaciones.
- ✓ Crear redes "zombies".

Anteriormente se mencionó, dentro de los ataques activos, a la Denegación de Servicio (DoS), lo cual es muy común en las redes inalámbricas, porque existe una gran cantidad de herramientas para poder llevarlos a cabo. Este tipo de ataques son muy difíciles de detectar y si se consigue hacerlo es complejo repelerlos; la duración de éstos puede ser por poco tiempo y sólo es posible descubrirlos en tiempo real.

A continuación se enlistan las formas de ataque Denegación de Servicio (DoS).

- ❖ Saturar el ambiente con ruido de radio-frecuencia:
  Las influencias negativas de las interferencias (el ruido) provocan pérdida de señales en Wi-Fi, si la calidad de transmisión es mala la red no funciona. Si alguien -deliberadamente- "produce" estos sonidos o interferencias en "nuestro espacio", la señal baja y por consecuencia el usuario se queda sin conexión.

  Este tipo de ataque es muy sencillo, se puede realizar con micro-ondas o con un generador de ruido. Si el administrador de red no cuenta con los elementos necesarios para detectar el problema, le será muy difícil darse cuenta del factor que está obstruyendo la red.

- ❖ Torrente de Autenticaciones:

  Cuando se trabaja con el estándar 802.11x y servidor RADIUS, es necesario que los usuarios se autentifiquen. Esto es complejo hablando criptográficamente, a su vez requiere un consumo considerable del procesador, esto es porque se deben tirar túneles y realizar búsquedas en las bases de datos. Si el usuario no es autenticado será rechazado, después de realizar todo el proceso.

  Cuando un **hacker** se dedica a enviar falsas peticiones de autentificación satura la red inalámbrica, ya que éstas resultan repetitivas o en gran cantidad; lógicamente por cada petición se lleva a cabo todo el proceso antes mencionado, provocando que los usuarios legítimos puedan autenticarse ante el servidor RADIUS, pues siempre estaría ocupado con el ataque del **hacker**.

- ❖ WAP-Modificación de paquetes:
  Un fallo importante que tiene el protocolo WEP es el de encriptación, el cual consiste en la falta de un método de chequeo de integridad. Esto quiere decir que los paquetes pueden ser alterados o sustraídos, pues WEP no verifica que lleguen bien cada uno de ellos. Precisamente para evitar este tipo de problemas se creó el protocolo WAP, el cual es un sistema de chequeo de integridad, cuyo mecanismo incluye TKIP-WPA que se encarga de verificar si los paquetes han sido modificados o manipulados. Si detecta que dos o más han sido cambiados en un minuto, el

sistema asume que alguien lo está atacando y -por precaución- desconecta a la cantidad de usuarios que se encuentren en la red inalámbrica. Cuando esto pasa, el **hacker** puede alterar o modificar un par de paquetes y logrará que el sistema desconecte a todos. Una vez que se vuelvan a reconectar podrá repetir la operación, manipulando dicho par y consiguiendo que la totalidad de usuarios sean rechazados otra vez. De esta forma nadie podrá trabajar en la red.

Otro tipo de ataque es la Imitación/Falsificación que se basa en el engaño y la suplantación de identidades y/o dispositivos pertenecientes a la red inalámbrica en cuestión. Generalmente se reemplaza un Access Point (AP), se hace creer a los usuarios que el AP pirata es legítimo o se suplanta a uno o varios clientes.

Dentro de este grupo de ataques existen los siguientes métodos de ataques:

- **MAC** Address Spoofing:
  Para poder comprender mejor este tipo de ataque es necesario recordar que la **dirección MAC**, también conocida como dirección física, es un identificador de 48 **bits** que nos permite ser reconocidos dentro de la red; en otras palabras, podríamos decir que es el nombre de nuestro equipo ante la red.

  Este ataque consiste -precisamente- en imitar o suplantar una **dirección MAC** legítima. Si la red inalámbrica está defendida mediante un sistema de filtrado de **direcciones MAC**, el **hacker** puede detectar alguna autorizada y utilizarla en su computadora, suplantando a la máquina acreditada. Esto se puede lograr de manera sencilla mediante el **software** Air Jack. El Access Point creerá que el equipo intruso (con la **dirección MAC** robada), es el usuario legítimo y permitirá la conexión a la Wi-Fi.

- Man-In-The-Middle/ MITM:
  Como su nombre lo dice "Hombre en el Medio", el objetivo del **hacker** es ubicarse entre el Access Point y el dispositivo Wi-Fi cliente; de esta forma puede controlar las comunicaciones del usuario. Una vez que logra su propósito, puede realizar 3 tipos de acciones:
  1. Modificar o alterar la información que se está transmitiendo a través suyo y de esta manera confundir o engañar al receptor.
  2. Transmitir la información sin ningún cambio. De esta forma logra enterarse del contenido.
  3. Bloquear la información transmitida y evitar que llegue a su destino.

  Para que este tipo de ataques se puedan lograr, el **hacker** debe localizar una red inalámbrica para actuar; posteriormente junta información sobre los SSID y demás parámetros del Access Point, tanto de la red inalámbrica como la del cliente; además necesitará un AP y una computadora cliente Wi-Fi. Actualmente existe un **software** que simula un Access Point en un equipo, con este programa

es suficiente una computadora para cumplir la función de Access Point y la del cliente Wi-Fi.

El Access Point del **hacker** deberá atraer al cliente o a los clientes para que se conecten a él y no al Access Point legítimo, a su vez su computadora tendrá la función de ser un usuario legítimo y enviará esta información al AP "verdadero".

En consecuencia, el **hacker** podrá participar de las actividades de la red inalámbrica y lanzar ataques de Denegación de Servicio-DoS.

- Session Hijacking:
  En español su nombre quiere decir "Secuestro de la Sesión". Este ataque consiste en "echar" a un usuario legítimo y reemplazarlo. Cuando consigue su objetivo el **hacker** participa de la red inalámbrica, en lugar del usuario "verdadero" que quedará desconectado.

  La manera en la que se realiza este ataque es la siguiente:

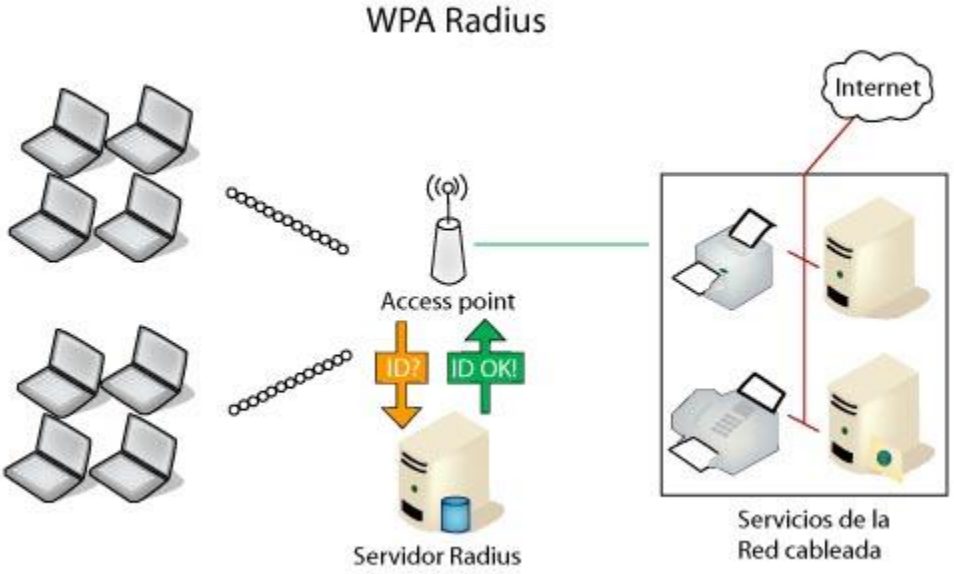
1. El **hacker** elige la red inalámbrica que va a atacar.
2. El atacante monitorea esa red Wi-Fi, analiza el tráfico y junta información como SSID, dirección **MAC**, etc.
3. El intruso lanza un ataque de Denegación de Servicio, contra el usuario que desea desconectar, hasta que consigue sacarlo de la red.
4. Con la información obtenida durante el monitoreo puede conectarse rápidamente a la red inalámbrica, ocupando el lugar del usuario legítimo, este último tratará de enlazarse pero no podrá, ya que el **hacker** lo suplantó.
5. Después de unos segundos el **hacker** se retira y permite conectarse al usuario legítimo.
6. El **hacker** podrá repetir sucesivamente su objetivo, ya sea con el mismo usuario o con uno diferente.

#### 3.4.2.2 Seguridad empleada por RIU

Como se mencionó con anterioridad, cuando RIU nació, una de las principales preocupaciones fue identificar los riesgos y por lo tanto darles una solución adecuada creando políticas, control de acceso, integridad y confidencialidad. Sin embargo, y definitivamente, la creación de políticas de uso y el monitoreo no eliminan los peligros en las redes 802.11; aunque el objetivo es visualizar las posibles amenazas y, una vez identificadas, poner a actuar a las herramientas asignadas para combatir efectivamente los ataques.

Otro punto que RIU decidió vigilar de una manera celosa, fue el control de acceso basado en el estándar WPA con el protocolo de autentificación PEAP de 802.1x. PEAP,

mismo que se encarga de implementar seguridad en la capa de transporte (**Transport Layer Security, TLS**) en la negociación; esto se logra gracias a un certificado digital firmado por una autoridad, el cual previene de un ataque de intercepción de información (**Man in the middle attack, MiTM**) donde un intruso capta la comunicación entre los usuarios de la red. Para poder evitar este tipo de inconveniente se requiere un usuario y una contraseña para poder acceder a RIU con seguridad.




Un aspecto más que se tomó en cuenta durante la implementación de RIU, fue cuidar la integridad de la infraestructura de la red al momento de un posible colapso a causa de la saturación del medio; por ello el **switch** central utiliza una asignación dinámica de frecuencias de operación, con esto se busca constantemente el canal menos saturado para transmitir. Por otro lado, este mismo **switch** permite monitorear el estado de los APs conectados a RIU, de esta forma se puede saber si un punto de acceso tiene amenaza de ataque.

Cabe destacar que la infraestructura de RIU es compatible con las mejores prácticas definidas por ITIL (Biblioteca de Infraestructura de Tecnología de Información); también es posible detectar geográficamente la ubicación de equipos que quieran atacar a RIU, ya sea por medio de un código malicioso o por negación de servicio.

A continuación se expondrán algunos puntos sobre lo que es la seguridad en ITIL, para poder tener una mejor comprensión del papel que juega en RIU. ITIL implica diferentes procesos para llevar a cabo una administración, entre los cuales se encuentra la seguridad de la información, aspecto por demás relevante en el ámbito de la interacción

a través de redes. Por otro lado, también se encarga de identificar los riesgos asociados al proceso para definir líneas de acción, con la finalidad de minimizarlos.

La manera en que ITIL aplica la seguridad determina, en primer lugar, los conceptos básicos de una adecuada protección de la información; posteriormente relaciona estos términos con los demás de la biblioteca, proveyendo de manera general las medidas de defensa adecuadas que deben ser aplicadas en cada uno de los procesos que lleve a cabo la administración; para finalizar, agrega una guía para suministrar tales medidas con referencia al Código de Prácticas de Administración de la Seguridad de la Información (BS7799), versión 1999, desarrollado por el Instituto de Estándares Británico (British Standards Institute). Este código cubre todos los tópicos conocidos del sitio de Internet del "Handbook Security" (Manual de Seguridad) de manera muy general. Contiene los siguientes 10 elementos del Código de Prácticas para la administración de la seguridad de la información:

1. **Políticas de seguridad.** Proporciona a la alta dirección apoyo para la seguridad de la información.
2. **Organización de la seguridad.** Ayuda a administrar la protección de la información dentro de la organización.
3. **Clasificación y control de activos.** Provee las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la organización.
4. **Seguridad del personal.** Necesaria para reducir los riesgos de errores humanos, robo, fraude o mal uso de las instalaciones y equipo.
5. **Seguridad física y ambiental.** Previene el acceso físico no autorizado a los sistemas de información, así como posibles daños a las instalaciones y a la información del negocio.
6. **Administración de comunicaciones y operaciones.** Permite garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.
7. **Control de acceso.** Previene el acceso lógico y cambio, no autorizado, a la información y a los sistemas de ésta, otorgando confidencialidad en los datos, para evitar interrupciones en los procesos normales de producción.
8. **Desarrollo y mantenimiento de los sistemas.** Permite incorporar la seguridad a los sistemas de información.
9. **Administración de la continuidad del negocio.** Contrarresta las interrupciones a las actividades del negocio y protege los procesos críticos de éste contra los efectos causados por fallas mayores o desastres.
10. **Conformidad.** Contribuye a evitar infracciones a las leyes civiles, jurídicas, obligaciones reguladoras o contractuales y cualquier otro requerimiento de seguridad.

Todos los puntos anteriores se combinan por medio del enfoque de procesos, otorgando controles, claves y medidas de protección que sirven para implementar un Sistema de Gestión de Seguridad.

Después de saber un poco más sobre lo que es la seguridad ITIL, regresaremos a tocar otro asunto que se consideró durante la implementación de la RIU, el de la disponibilidad de ésta. Para poder determinar dicho aspecto se consideraron dos puntos:

por un lado está la redundancia de enlaces; esto quiere decir que se dispone de dos equipos en ubicaciones geográficas distintas, lo cual ayuda a disminuir la probabilidad de que ambos fallen; el segundo punto es la "autosanación" que se aplica cuando alguno de estos dos equipos deja de funcionar. Las computadoras que se encuentran cerca de éstos aumentan su potencia de transmisión para poder cubrir el área sin servicio, lo cual se logra gracias a la administración centralizada del **switch** y de los algoritmos con los que cuenta para reducir este tipo de riesgos.

Todos los puntos antes mencionados son importantes, pero no lo es menos el tema de la confidencialidad de la información de los usuarios; para ello se consideraron varios aspectos que funcionan en distintas capas del **modelo OSI**.

El primero de ellos es el "aislamiento de usuarios", éste sirve para evitar la propagación de código malicioso, ya que los usuarios no pueden establecer conexiones directas con otros, en el mismo punto de acceso.

El segundo es la utilización de WAP TKIP, que permite establecer un canal cifrando individual para cada usuario; por el mismo motivo, un "usuario autenticado" no puede capturar información de otro.

El último aspecto es el transporte de la información del AP al **switch** central, para ello se utilizan túneles con encapsulado genérico de ruteo (Generic Routig Encapsulation), éstos se encargan de transportar el tráfico sin afectar los encabezados de los protocolos superiores. Dicho protocolo también se conoce como GRE y se emplea en combinación con otros "de túnel" para crear redes virtuales privadas. Fue diseñado para proporcionar mecanismos de propósito general, ligeros y simples, para encapsular datos sobre **redes IP**.

## 3.5 Relación Usuario-RIU

Ahora bien, regresando un poco al objetivo de RIU (Red Inalámbrica Universitaria), recordemos que ésta fue creada para satisfacer la necesidad de movilidad y conexión de la comunidad universitaria, en este caso de la FES Aragón. Así, después de ver todo el proceso por el cual RIU tiene que pasar para llegar al usuario final, salta una pregunta: ¿Cuál es la relación Usuario-RIU?

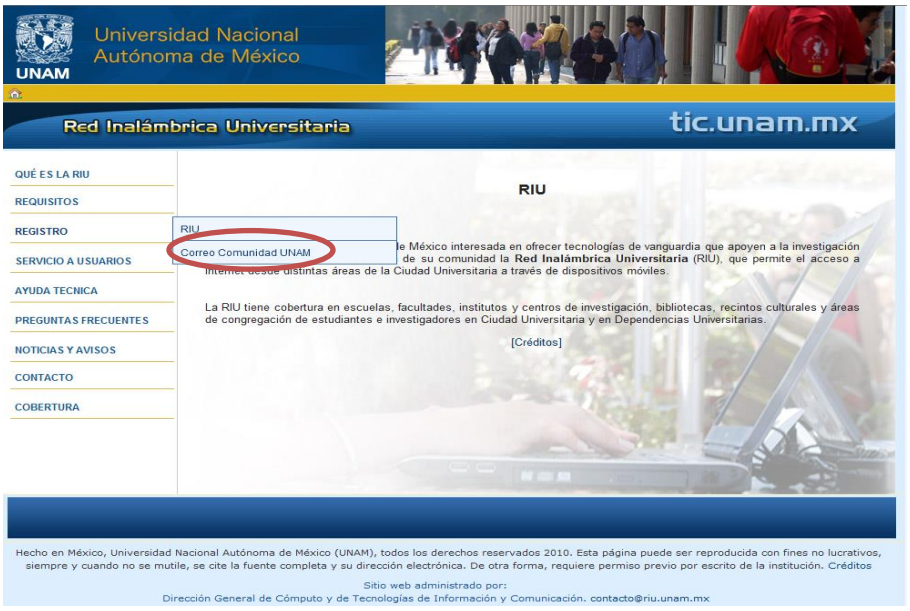
El usuario únicamente tiene contacto con RIU mediante su equipo cuando se configura con el fin de acceder a la red y, antes de esto, cuando hace su registro. Para poder obtener un usuario y una contraseña de RIU se deben realizar una serie de pasos antes de concretar su registro en línea.

A continuación se muestra cómo debe llevarse a cabo el proceso:

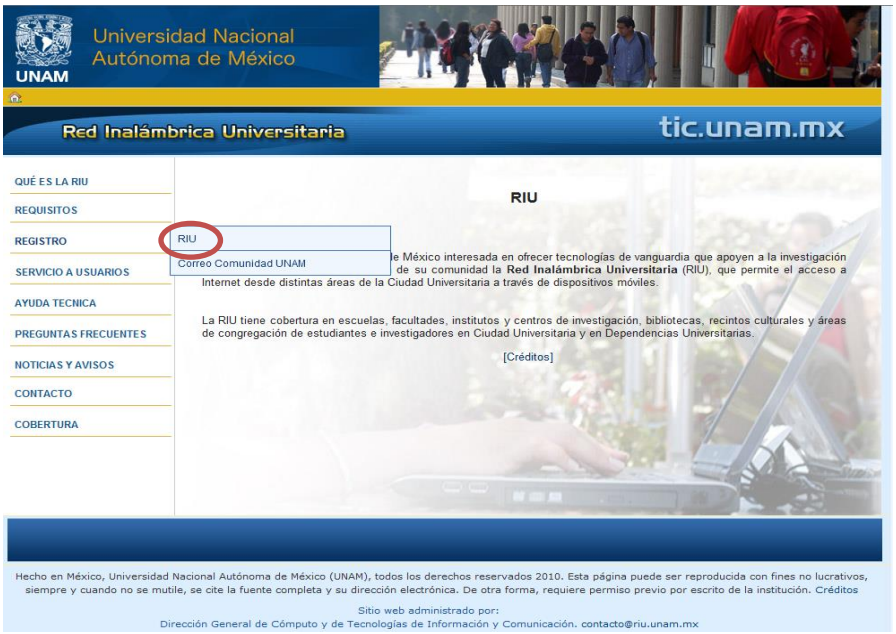
1. Entrar a la página RIU https://www.riu.unam.mx/


2. Dirigirse a la pestaña que dice REGISTRO.

3. Para poder realizar el registro de la cuenta de RIU, el usuario deberá tener una de Comunidad UNAM; si no la tiene, dentro de la página de RIU viene un botón que nos lleva a la de Comunidad UNAM, en la cual se encuentran los pasos a seguir para obtener una cuenta de correo.




4. Una vez que se obtuvo la cuenta de Comunidad UNAM se puede realizar el registro para obtener la de RIU.




5. Para seguir con este proceso es necesario dar de alta el Registro Institucional (http://www.servicios.unam.mx); o bien, la misma página de RIU te lleva al registro.

Después de dar *click* a la liga, se visualiza la siguiente ventana que es la que dará paso al Registro Institucional y se irán presentando las pantallas que se tienen que llenar para continuar este proceso.



Para confirmar tu solicitud, deberás ingresar a tu bandeja de entrada de tu correo electrónico registrado con dominio unam.mx y dar clic al primer vínculo (Liga de aceptación del servicio).

Esto permitirá corroborar tu deseo de realizar este Registro a Servicios TIC y validar tu dirección de correo electrónico.

**Importante**: De no realizar este paso en las siguientes **72 horas**, el sistema eliminará tu solicitud de registro y tendrás que seguir nuevamente el proceso desde el paso anterior.



Para concluir con tu proceso de registro, tras dar clic en el correo que te llegó a tu correo con dominio UNAM registrado, el sistema te llevará a una página Web que te señalará que el proceso ha sido exitoso.

Tras haber concluido los 4 pasos del proceso, ya puedes ingresar a http://www.servicios.unam.mx y entrar a tu sitio Web Personal, donde podrás ingresar a diversos servicios que la Universidad pone a tu disposición.

Entre ellos, el de la Red Inalámbrica Universitaria y Páginas Personales


Una vez que se tiene el Registro Institucional, hay que regresar a la página de inicio (http://www.servicios.unam.mx) y en el siguiente recuadro colocar los datos inscritos, para tener acceso al portal y así realizar el registro de RIU.


Al concluir el registro de RIU se obtendrá un usuario y contraseña, con los cuales se configura el equipo que se quiere conectar a la red, dependiendo del sistema operativo de éste. Los manuales de configuración se encuentra en la misma página de RIU; o bien, se puede asistir a la Unidad de Sistemas y Servicios de Computo de la FES Aragón, donde se proporciona el soporte técnico necesario.

# CAPÍTULO 4

## MEJORAS ESTRUCTURALES DE RIU

# CAPÍTULO 4: MEJORAS ESTRUCTURALES DE RIU

## 4.1 Antenas WI-FI que pueden optimizar el rendimiento de RIU

Al hablar de antenas WI-FI no sólo nos referimos a un tipo, pues existe una gran diversidad de ellas para satisfacer diferentes necesidades, ya que de acuerdo a la zona que deseemos cubrir con red inalámbrica, dependerán las especificaciones que buscaremos al momento de elegir una. Pero, antes de entrar a fondo en este tema, se dará una descripción de los tipos de antenas que podemos encontrar en el mercado.

- **Antenas direccionales (o directivas)**

Orientan la señal en una dirección muy determinada con un haz estrecho, pero de largo alcance. Una antena de este tipo actúa de forma parecida a un foco que emite un haz concreto y angosto; aunque de forma intensa (con mejor cobertura).

Las antenas direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor; sin embargo, fuera de esta zona no se "escucha" nada y -en consecuencia- no se puede establecer comunicación entre los interlocutores.

El alcance de una antena de este tipo viene determinado por una combinación de sus **dBi de ganancia**, la potencia de emisión del punto de acceso emisor y la sensibilidad con la que actúa el punto de acceso receptor.

Debido a que el haz de la antena direccional es estrecho, no siempre es fácil alinear (encarar) dos antenas de éstas, en un enlace inalámbrico entre dos puntos.

- **Antenas omnidireccionales**

Orientan la señal en todas direcciones con un haz amplio, pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz a todas partes, pero con una intensidad menor que la de un foco; es decir, con menos alcance.

Las antenas omnidireccionales "envían" la información -teóricamente- a los 360 grados, por lo que es posible establecer comunicación independientemente del punto en el que se esté; aunque, como ya se dijo, su alcance es menor que el de las antenas direccionales.

El tipo de alcance de una omnidireccional 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 del punto de acceso receptor. Con los mismos **dBi**, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

- **Antenas sectoriales**

Son la mezcla de los dos tipos anteriores. Las sectoriales emiten un haz más amplio que una direccional, pero no tanto como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional; aunque algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura; es decir, con un haz más ancho de lo normal.

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar dos o tres antenas sectoriales de 120º ó 4 de 80º. Éstas suelen ser más costosas que las antenas direccionales u omnidireccionales.

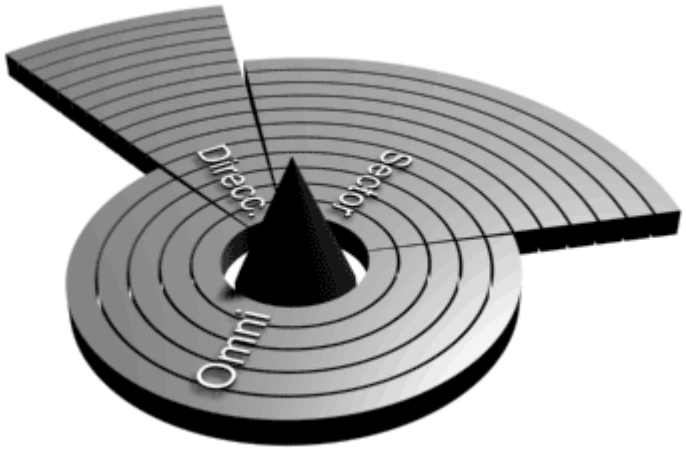
Hablando un poco más sobre el alcance de las antenas, debemos definir que la apertura de la señal es cuando se "abre" el haz de la antena. Éste, al ser emitido o recibido, tiene una abertura determinada verticalmente y otra horizontalmente.

Como su nombre lo indica, la apertura horizontal de una antena omnidireccional trabajará "horizontalmente" en todas direcciones; es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y los 40º y una sectorial entre los 90º y los 180º.

La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si la irregularidad geográfica es importante, la antena deberá tener gran abertura de este tipo. Por lo general las antenas, a más ganancia (potencia, por decirlo de algún modo) menos apertura vertical.

Por su parte, en las antenas direccionales -generalmente- se suele tener las mismas aperturas verticales y horizontales.

Entonces es aquí cuando llega la disyuntiva sobre qué tipo de antena debemos usar. Como he venido mencionando, debemos buscar una que cubra las necesidades del proyecto de vamos a realizar, tomando en cuenta las propiedades de la antena y el área que queremos abarcar. A continuación hago mención de algunas características de estos equipos.




Las antenas direccionales se pueden utilizar para unir dos puntos a larga distancia, mientras que las omnidireccionales se usan para dar señal extensa en los alrededores. Las antenas sectoriales se llegan a emplear cuando se necesita un balance de las dos cosas; es decir, llegar a largas distancias y -a la vez- a un área extensa.

En pocas palabras, si se necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque, por ejemplo) lo más recomendable es utilizar una antena omnidireccional. Si el área a cubrir es un punto muy concreto (como puede ser un **PC** que está bastante lejos), se aconseja el uso de una direccional. Por último, si la cobertura debe ser amplia y a la vez a larga distancia, la opción son las antenas sectoriales.

Una vez que se determinó el área que se va a abarcar, se debe tomar en cuenta la alineación de las antenas; sin olvidar que, mientras las omnidireccionales o sectoriales mandan la señal en un área muy amplia, las direccionales (o directivas) envían un haz de señal muy potente, pero estrecho. Es decir, si queremos hacer una unión inalámbrica entre dos dispositivos que llevan antenas direccionales y la distancia es larga, podemos

tener alguna dificultad en "encarar" a ambas con precisión. Esto es punto muy importante a considerar, pues en exteriores donde no se producen rebotes de la señal y ésta viaja de forma limpia de un punto a otro, la orientación correcta de las antenas es un elemento determinante para obtener una conexión rápida y libre de errores (reenvíos de paquetes/transmisiones).

Por otro lado, es importante mencionar la manera en que podemos aprovechar la tecnología para poder mejorar el servicio de la red inalámbrica. Para empezar, hay que tomar en cuenta la arquitectura de los edificios, porque -como sabemos- la señal se puede ver interferida por cualquier obstáculo que se le presente y debemos encontrar la mejor manera de adecuar la instalación, de acuerdo a las necesidades de las construcciones.

Como se puede apreciar en la imagen siguiente, sugiero un **site** por cada edificio en el que se piense instalar la red inalámbrica, el cual deberá estar equipado con los siguientes elementos:

- ✓ Rack

Un *rack* es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas, con el objetivo de que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, *cabinets* o armarios.

Externamente, los *racks* para montaje de servidores tienen una anchura estándar de 600 mm y un fondo de 600, 800, 900, 1000 y ahora incluso 1200mm. La de 600 mm para *racks* de servidores coincide con el tamaño estándar de las losetas en los centros de datos. De esta manera es muy sencillo hacer distribuciones de espacios en estos centros (CPD). Para el cableado de datos se utilizan también *racks* de 800 mm de ancho, cuando es necesario disponer de suficiente lugar lateral para el guiado de cables.

- ✓ Switch

Este elemento se utiliza para conectar múltiples dispositivos de la misma red dentro de un edificio o campus. Por ejemplo, puede enlazar computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuará como un controlador, permitiendo a los diferentes dispositivos distribuirse información y comunicarse entre sí. Mediante tales acciones y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

Existen dos tipos básicos de switches: gestionados y no gestionados.

-Los switches no gestionados funcionan de forma automática y no permiten realizar cambios. Los equipos de redes domésticas suelen utilizar de este tipo.

-Los switches gestionados permiten acceder a ellos para programarlos. Esto proporciona una gran flexibilidad porque el switch puede monitorizarse y ajustarse local o remotamente, para proporcionarle el control de cómo se transmite el tráfico en su red y quién tiene acceso a ésta.

✓ UPS

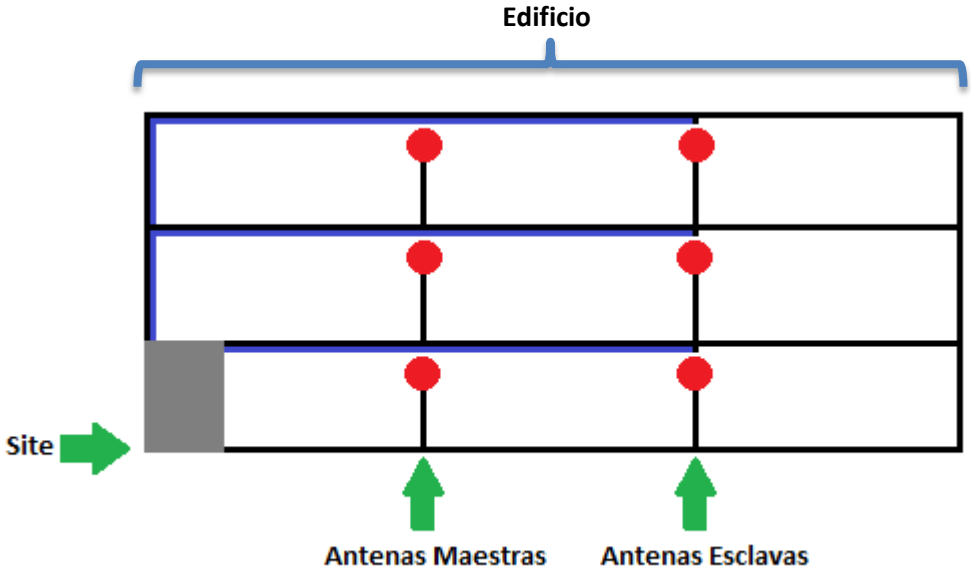
El UPS es una pieza importante en la seguridad de los sistemas de información. Su principal tarea es tomar el control cuando ocurre una interrupción de energía eléctrica, dando a los usuarios el tiempo necesario para guardar sus trabajos en proceso.

Los apagones no son los únicos incidentes que estos equipos manejan. La regulación y el filtrado de voltaje son otra función importante. Un buen UPS debe asegurar un suministro ininterrumpido de energía eléctrica para su equipo y -además- debe proporcionar energía de alta calidad.

Un UPS tiene tres partes:

-El rectificador, el cual transforma la corriente alterna en corriente directa que carga las baterías y da energía al UPS.
-Las baterías que almacenan la energía.
-El UPS que transforma la corriente directa proporcionada por el rectificador o las baterías a una corriente de 230 volts a 50 Hz, idéntica a la que suministra la red de electricidad.

El UPS también viene con un programa de desconexión automático: Cuando ocurre una suspensión de energía eléctrica, este programa (instalado en la computadora conectada al UPS) cerrará automáticamente todos los programas, después de haber realizado los respaldos requeridos.




Otro aspecto importante para tomar en cuenta es la tirada de los cables que deben estar bajo la Norma TIA-EIA 568A categoría 5e, que consiste en un sistema genérico de

alambrado de telecomunicaciones para edificios comerciales, los cuales puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones, contando con poca información acerca de este tipo de productos que posteriormente se implementaran. El montaje de los sistemas de cableado durante el proceso de instauración y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.
La norma ANSI/TIA/EIA-568-A, publicada en octubre de 1995, amplió el uso de Cable de Par Trenzado (UTP) y elementos de conexión para aplicaciones en Redes de Área Local (LAN) de alto rendimiento. La edición de la ANSI/TIA/EIA-568-A integra los Boletines Técnicos de Servicio TSB 36 y TSB 40ª, los cuales prolongan el uso de UTP en un ancho de banda de hasta 100 MHz. Esto permite el uso de Modo de Transferencia Asíncrona (ATM), Medio Físico Dependiente del Par Trenzado (TP-PMD), 100Base-Tx y otras 100 **Mbps**. o transmisiones superiores sobre UTP.

Esta norma guía la selección de sistemas de cableado al especificar los requisitos mínimos y componentes; asimismo, describe los métodos de pruebas de campo necesarios para satisfacer las reglamentaciones. Desde su implementación en 1992 Categoría 5 (CAT 5) sé a convertido en la predominante base instalada para el cableado horizontal de cobre. Se anticipaba que las especificaciones para el desempeño de Categoría 5 tendrían suficiente ancho de banda, para el manejo de las comunicaciones de alta velocidad de las redes locales LAN y el tráfico de datos en el futuro.

El estándar EIA/TIA 586-A específica:
-Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina.
-Topología y distancias recomendadas.
-Parámetros de medios de comunicación que determinan el rendimiento.
-La vida productiva de los sistemas de telecomunicaciones por cable, por más de 10 años.

La norma ANSI/TIA/EIA-568-A especifica los requisitos mínimos para cableado de telecomunicaciones dentro de edificios comerciales, incluyendo salidas y conectores, así como entre construcciones de conjuntos arquitectónicos. De acuerdo a dicha norma, un sistema de cableado estructurado consiste de 6 subsistemas funcionales:

1. Instalación de entrada, o acometida, es el punto donde la instalación exterior y dispositivos asociados entran al edificio. Éste puede estar utilizado por servicios de redes públicas, privadas del cliente, o ambas. Es el sitio de demarcación entre el portador y el cliente, y en donde están ubicados los dispositivos de protección para sobrecargas de voltaje.
2. El cuarto, local o sala de máquinas es un espacio centralizado para el equipo de telecomunicaciones (v.g., PBX, computadoras, conmutadores de imagen, etc.) que da servicio a los usuarios en el edificio.
3. El eje de cableado central proporciona interconexión entre los gabinetes de telecomunicaciones, locales de equipo, e instalaciones de entrada. Consiste de cables céntricos, interconexiones principales e intermedias, terminaciones mecánicas, y puentes de interconexión. Los cables centrales conectan gabinetes dentro de un edificio o entre varios de ellos.

4. Gabinete de telecomunicaciones, que es donde terminan en sus conectores compatibles los cables de distribución horizontal. Igualmente el eje de cableado central concluye en este gabinete, unido con puentes o cables de puenteo, a fin de proporcionar conectividad flexible, para extender los diversos servicios a los usuarios en las tomas o salidas de telecomunicaciones.
5. El cableado horizontal consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden utilizar varios tipos de cable para la distribución, ya que cada uno de ellos tiene sus propias limitaciones de desempeño, tamaño, costo, y facilidad de uso.
6. El área de trabajo, cuyos componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, hasta el equipo o estación de trabajo del usuario. Todos los adaptadores, filtros o acopladores utilizados para ajustar el equipo electrónico diverso al sistema de cableado estructurado, deben ser ajenos a la toma o salida de telecomunicaciones y están fuera del alcance de la norma 568-A.

Una vez que se tienen contempladas las necesidades y normas indispensables para poder hacer una instalación adecuada, se procede a elegir el tipo de antenas que cubran los requisitos de nuestro proyecto. Debemos recordar que los AP (Puntos de Acceso) pueden funcionar en tres tipos diferentes: maestro (*root*), repetidor (*repeater*) y puente (*bridge*). Los cuales funcionan de la siguiente forma:

- ✓ Maestro (*Root*): Este es el modo más común donde múltiples usuarios entran al punto de acceso al mismo tiempo, con portátiles y **PDA**'s pueden utilizar internet a través de un solo AP, compartiendo la conexión.
- ✓ Repetidor (*Repeater*): Se utiliza cuando se quiere extender la señal más allá de los límites actuales. Se necesita emplazar el punto de acceso en modo repetidor dentro del área de uno en modo Maestro (*Root*). Con esto, la señal AP Maestro se extenderá con igual fuerza por medio de este AP repetidor, mejorando el alcance.

Para los fines que perseguimos los AP's deberán ser tomados como Maestro y Repetidor, ya que la intensión de estos arreglos es poder tener una señal que abarque más distancia.

Como breviario cultural, a continuación menciono la última configuración del AP que es la de Puente (*Bridge*).

- ✓ Puente (*Bridge*): Como su nombre lo dice, se hace un puente inalámbrico entre dispositivos, dos AP's configurados de este modo sólo podrán hablar entre ellos. Este tipo de conexión es usada cuando se enlazan dos edificios separados en donde la instalación por cable no es viable. Para poder realizar este tipo de enlace se necesitan -además de- ambos AP's, dos antenas direccionales.

En la página 86 se puede ver un edificio, a cuyos pasillos -imaginariamente- segmenté en tres partes, en cada uno de ellos he colocado dos antenas: una funciona como maestra

y la otra como repetidora, esto con el fin de que la red cubra más distancia y llegue a todos los salones; ya que ése es uno de los grandes problemas de RIU, pues la recepción es óptima hasta la mitad, dejando a las instalaciones del fondo sin cobertura. Por ello, sugiero una antena repetidora para que la señal llegue a estos puntos, el frente de ésta deberá dirigirse hacia las aulas (dando la espalda a las explanadas), con toda la intensión de tener un mejor alcance en edificios y salones, gracias a este arreglo de colocación. Una vez que ya están debidamente configuradas e instaladas abarcaremos, sino en su totalidad, sí un 95% del edificio; de esta manera el usuario tendrá mayor cobertura y -por consiguiente- sus dispositivos móviles se verán beneficiados. Además, repartiendo la carga de usuarios a las antenas se evitará que se pierda la señal de los que ya están conectados, debido a las peticiones nuevas de quienes quieran conectarse.

## 4.2 Mejoras de seguridad ante los ataques a la Red

Existen diferentes procedimientos de seguridad para poder defender una red inalámbrica como RIU, a continuación se mencionan diferentes métodos que se pueden aplicar para dar confianza a esta red.

a) Sistemas dinámicos de seguridad:

-Actúan en tiempo real.
-Utilizan tecnología de camuflaje con la finalidad de infiltrar información falsa y de alterar los códigos del sistema de la red.
-También se ayudan por medio de una auto-actualización, con el objetivo de obtener los datos del **hacker** así como su ubicación. Además esto ayuda a comprender el modo de operación y de esa manera se puede prevenir otro ataque con el mismo método.

b) Certificados de clave pública:

-Consiste en un contrato digital, el cual ofrece una garantía en la legalidad de la utilización de la red inalámbrica y uso exclusivo del propietario de la red.
-Se manejan dos tipos de dichas claves:

* Clave pública: ésta consiste en que todos los usuarios tienen acceso a ella y generalmente se usa para que exista comunicación entre dos de ellos.
* Clave privada: en este tipo de claves el propietario es el único que la conoce, con esta misma se puede recuperar una clave pública y, lo más importante, evita que la red sea infringida.

Como sabemos, RIU posee sus propios certificados de seguridad, los cuales representan uno de tantos filtros que nos ayudan a conectarnos con protección a esta red.

No obstante, me gustaría destacar en este punto la necesidad imperiosa de renovar las contraseñas de los usuarios para poder llevar un mejor control, ya que muchos de éstos no son activos académica o laboralmente y aún tienen acceso a la red, entorpeciendo el acceso a quienes están en activo. Debemos tener en cuenta que esto es de suma importancia, si consideramos que por cada usuario activo se conectan dos equipos y por cada inactivo otros dos, provocando la saturación de los AP's.

A continuación explico la importancia de esta práctica (cambio de contraseñas), en la que deben considerarse los siguientes puntos para hacer más seguro el acceso del usuario y a su vez RIU evitará intromisiones.

Cuando se maneja un gran número de usuarios para una red se deben tomar todas las precauciones necesarias para llevar un control de los mismos, es muy importante que las contraseñas que se asignen sean de carácter "fuerte"; esto quiere decir que debe ser complicado poder descubrirlas. De esa manera, si las contraseñas son de calidad, el atacante tendrá dificultades para reconocerlas. En la actualidad existen herramientas que identifican los **password**, por eso la importancia de hacer una constante actualización de éstas y una depuración de usuarios.

En seguida, hago mención de algunos puntos a tomar en cuenta al momento de asignar contraseñas:

- Todos los usuarios deben estar asociados con una contraseña, sin excepción, ya que no se deben dejar "huecos" que permitan el paso a los intrusos.
- La longitud de las contraseñas no debe ser menor a 7 caracteres, pues -como se mencionó- el objetivo debe ser tener contraseñas "fuertes".
- Al elaborar una contraseña su estructura tiene que constar de caracteres alfabéticos (con minúsculas y mayúsculas), así como numéricos.
- En las contraseñas es necesaria una fecha de caducidad, esta característica es muy importante para no tener usuarios inactivos académicamente y que permitan el acceso a los activos.

Sabemos que, por la alta demanda que tiene RIU, sería casi imposible hacer esta práctica; así que podría sugerir que las fechas de caducidad sean generacionales y se den de baja los usuarios que vayan saliendo de la institución.

### 4.3 Mantenimiento Correctivo

Desde que se planea una red inalámbrica se toman en cuenta muchos factores físicos para poder implementar una red de esta naturaleza; pero aun cuando todo esté bien pensado siempre existen detalles que se salen de las manos. Al momento de ponerse en marcha comienzan a "saltar" algunos conflictos, y es aquí cuando se debe dar solución inmediata con un mantenimiento correctivo.

Muchos factores pueden hacer que los puntos de acceso no funcionen con normalidad o bien que la señal de RIU caiga, cuando esto ha llegado a suceder y no se encuentra una causa local, se reporta a **DGTIC** para que sea revisada desde sus instalaciones. Cabe mencionar que -en algunas ocasiones- el problema llega a ser el enlace con TELMEX. Una vez que se localiza la falla se trata de arreglar al instante para garantizar el servicio a los usuarios.

Si todo está funcionando correctamente afuera de la institución, el problema es interno y es cuando la Unidad de Sistemas y Servicios de Cómputo de la FES Aragón toma cartas en el asunto y debe aplicar -de inmediato- el mantenimiento correctivo que dé solución a la falla. A continuación enlisto algunas de las causas intrínsecas que pueden interferir con el buen funcionamiento de la RIU:

- Variación de voltaje: Esto afecta sobremanera a un equipo, desde una intermitencia en el servicio hasta provocar que éste se dañe en su totalidad. Para evitar tales fallas se pueden colocar supresores de picos o un **no-break**.

  La mayoría de los equipos electrónicos trabajan con niveles de voltaje estables para que puedan funcionar correctamente, si llega a existir una variación en la energía se pueden provocar deficiencias en el servicio. En este caso, es posible que el supresor de picos o el **no-break** estén fallando y -entonces- se hace una inmediata sustitución para garantizar la eficiencia de RIU.
- Ruptura de algún cable: Como sabemos, con el paso del tiempo el material de instalación suele deteriorarse o bien es provocado por algún factor físico; esto quiere decir que debido a algún incidente ajeno al servicio o al equipo puede existir cierto daño parcial en algún cable de la instalación. Por ello, en cuanto se detecta el tramo averiado, se hace la inmediata sustitución del mismo para poder restablecer el servicio de ese AP (punto de acceso).
- Obstrucción de la señal de la antena: Antes de ser colocadas las antenas en los puntos asignados, para cubrir las zonas especificadas, se estudia la geografía del área; de esa forma se evitan obstáculos que puedan interferir con el buen funcionamiento del equipo. Aunque no siempre las cosas salen como se planearon, ya que puede haber obstrucción de la rama de algún árbol que no estaba cuando se planeó colocar -en ese lugar- la antena; o bien, algún aparato que tampoco se encontraba en ese sitio. En tal caso se debe escanear la zona, se buscan las causas, se trata de limpiar el espacio o de mover la antena para que la señal de ésta no se vea bloqueada por ningún obstáculo.

### 4.4 Mantenimiento Preventivo

Como se mencionó en el punto anterior, al momento de implementar una red inalámbrica como la RIU, se realizó un estudio sobre el entorno en el que estaría trabajando, se tomaron en cuenta muchos factores, como por ejemplo: fuentes de interferencia, análisis de la cobertura y la fuerza de la señal de las antenas (tanto en lugares cerrados como abiertos). Ya en el punto anterior se habló sobre un mantenimiento correctivo de las posibles fallas durante el funcionamiento de la red, pero para tratar de evitar lo más que se pueda ese tipo de mantenimiento es preferible tomar medidas preventivas a nivel local; de esa forma se puede garantizar la calidad de servicio de la RIU.

El objetivo principal de un adecuado mantenimiento preventivo es la detección oportuna de degradaciones de la señal, saturaciones en los AP (punto de acceso) e incluso intrusiones dentro de la red.

Las principales áreas en donde se debe aplicar este tipo de mantenimiento son las siguientes:

- Equipamiento:
  En este punto nos referimos a la parte física de la estructura de la red inalámbrica, donde hay que poner constante atención a los AP'S (puntos de acceso), cableado (coaxial, estructurado, eléctrico), **networking**, etc., teniendo en cuenta que requieren un constante chequeo, además de actualizaciones de **firmware** o **drivers**, las cuales tendrán que ser realizadas cuando el experto lo aconseje. En el caso de instalaciones exteriores, se debe considerar la aceleración de la degradación de los equipos por las inclemencias del tiempo y los casos de robo y vandalismo (también presentes en instalaciones públicas), lo cual suele afectar sobre todo a antenas, cableado y puntos de acceso. Es importante una continua revisión a las partes físicas para tratar de evitar lo más que se puedan reparaciones de emergencia, como sería en el caso del mantenimiento correctivo.
- Entorno de radio:
  Este tipo de problema se puede encontrar tanto en el mantenimiento correctivo como preventivo, pues aunque durante este último se trate de localizar fuentes de interferencia y se les dé una solución para evitarlas, no se puede tener un control absoluto en el entorno en el que se va a desarrollar la red, ya que podrían colocar aparatos en donde antes no existían sin que se notifique a la Unidad de Sistemas y Servicios de Computo. Si se trata de ser previsor, en ese sentido es recomendable -como ya se indicó- hacer un chequeo de posibles fuentes de interferencia, las cuales en ocasiones suelen ser temporales, como pueden ser aparatos que no se ocupan constantemente (hornos de microondas o teléfonos inalámbricos), los que pueden generar un mal funcionamiento aleatorio y precisamente para evitar una interrupción en el servicio se puede prever una posible interferencia.

- Gestión de uso:
  Aunque este punto se va a ver detalladamente más adelante, hago mención de él, pues si se tiene cuidado en este aspecto es posible evitar conflictos a futuro. En esta área del mantenimiento podemos verificar el tráfico circulante, el número de usuarios y la distribución de los mismos en los AP (punto de acceso). Es importante realizar manutención periódica, ya que se pueden detectar posibles degradaciones, saturación o incluso intrusiones.

Como podemos ver, el mantenimiento preventivo puede evitar problemas futuros y -en ocasiones- los que deban atenderse de emergencia. Hay que tratar de evitar lo más que se pueda reparaciones urgentes, para que no se vea comprometido el buen funcionamiento de nuestra red y de esa forma hacer -con tiempo- las mejoras, ya sean de servicio o de una planificación de crecimiento de la red.

## 4.5 Monitoreo de Tráfico en la Red

Como es de suponerse **DGETIC** se encarga del constante monitoreo de RIU dentro de la FES Aragón. En lo personal, considero indispensable que dentro de las instalaciones -también-se deba monitorear la red, ya que si existe alguna anomalía se puede reportar inmediatamente a **DGETIC** para evitar un problema más grande o para que el tiempo de corrección sea menor. Llevar a cabo lo anterior requiere de diferentes herramientas que puedan ayudar a hacer esta supervisión, es importante mencionar que se necesitaría de un equipo externo en el cual se pueda instalar alguna de las herramientas que menciono a continuación:

- ✓ **AirMagnet WiFi Analyzer**

- Proporciona la causa u origen de los problemas informados de Wi-Fi.
- Maximiza las eficacias de 802.11n y la inversión.
- Visibilidad total del tráfico de Wi-Fi.
- No hay que pasar por alto un dispositivo vulnerable o amenaza de seguridad.
- Análisis independiente de la amortización de la inversión en las opciones de la infraestructura de WLAN.
- Estado de conformidad listo para auditoría.
- Herramienta de auditoría para verificar la conectividad de la red y el rendimiento de la aplicación.
- Solución de problemas en tiempo real.
- Resolver inmediatamente los problemas de la seguridad y del funcionamiento inducidos por **BYOD.**

AirMagnet WiFi Analyzer es la herramienta estándar del sector para realizar auditorías móviles y solucionar problemas de redes Wi-Fi de empresas, ayuda al personal de TI a resolver rápidamente las dificultades del usuario final, mientras que detecta de manera automática amenazas de seguridad y otras vulnerabilidades de la red inalámbrica. La solución permite a los encargados de ésta probar y diagnosticar docenas de fallas comunes de rendimiento de la red inalámbrica, incluyendo las que presente la capacidad de transmisión, problemas de conectividad, conflictos con dispositivos y con las trayectorias múltiples de señales. AirMagnet WiFi Analyzer incluye un completo motor de creación de informes de cumplimiento, que asigna automáticamente la información recogida de la red a los requisitos de cumplimiento de políticas y normativas.

- ✓ **NetSurveyor**

Herramienta diseñada para trabajar con redes Wi-Fi 802.11b/g. Proporciona información sobre la cercanía del punto de acceso (AP) en tiempo real y de manera gráfica; así permite determinar la presencia de los APs locales, intensidad de las señales de sus antenas y su ubicación óptima, realizar estudios de cobertura, identificar si existen interferencias de radiofrecuencias... Con este **software** se puede obtener: el SSID, la **MAC**, el tipo de cifrado, la fuerza (medida en dB/m), calidad de la señal (mW), etc. En definitiva, es una herramienta útil para ayudar a entender conceptos como puntos de acceso, estaciones-cliente, redes inalámbricas o SSIDs. Puede correr sobre Windows XP y VISTA.

- ✓ **InSSider**

Herramienta que permite controlar de modo gráfico la intensidad de señal de una WiFi. Al igual que la anterior detecta SSID, **MAC**, canal, intensidad y fuerza de radio recibida, seguridad, velocidad de la señal, etc. Funciona en Windows XP, VISTA y 7.

- ✓ **Ekahau Heatmapper**

Una divertida utilidad que permite dibujar un mapa de coberturas de una estancia y/o laboratorio, detectando las configuraciones de seguridad, simplemente desplazándose mediante un portátil con adaptador inalámbrico por el área de la estancia. Permite mostrar las conexiones ordenadas por potencia, seguridad, **MAC**, SSID o canal.

- ✓ **Vistumbler**

Esta dinámica herramienta permite escanear señales WiFi dentro del ámbito de cobertura, de modo que se puedan ubicar en una posición aproximada mediante Google Maps. Funciona en Windows VISTA y 7. La versión para Windows XP se denomina Netstumbler.

- ✓ **WiFi SiStr**

Es una pequeña utilidad bastante simple que permite determinar la intensidad de señal de una red inalámbrica.

- ✓ **Wireshark**

Para analizar tráfico de una red **Ethernet**, Wireshark requiere la librería Winpcap sobre Windows; si se desea examinar el de una red Wi-Fi en Windows, necesita de otra librería denominada Airpacap. No obstante, esta última no es de libre distribución.

En caso de que se quieran analizar tramas 802.11 con Wireshark sin disponer de la librería Airpacap, se obtendrán paquetes no interpretables encapsulados dentro de tramas 802.3 (**Ethernet**), cuando en realidad no son de este tipo. Para poder examinar la transmisión de datos en redes 802.11 sobre Windows, se requiere un analizador que soporte el **driver** del dispositivo inalámbrico que se vaya usar (hay gran diversidad de fabricantes y modelos). Por su gran variedad de **drivers** inalámbricos soportados, se recomienda el empleo de alguna de las siguientes herramientas en su versión trial o de evaluación:

- ✓ **Comview for WiFi**

Es una familia de monitores de red para diferentes necesidades. La versión Comview for WiFi permite analizar diferentes protocolos de redes WLAN. Funciona en XP, Vista y 7.

CommView for WiFi es la versión para conexiones inalámbricas de uno de los **sniffers** más completos y mejor valorados para Windows. Por definición, un **sniffer** es una utilidad diseñada para capturar el tráfico que viaja por redes de tipología **Ethernet**. CommView for WiFi es justo esto, pues cuenta con las funciones y herramientas necesarias para capturar los paquetes de conexiones inalámbricas. Concretamente, puede captar tramas **Ethernet** y analizar cada una de sus cabeceras y protocolos incluidos: paquetes **IP**, segmentos TCP, **datagramas** UDP, protocolos RTP o RTCP, entre otras posibilidades. Pero, sin duda, la razón por la que CommView for WiFi es muy popular entre los administradores de red es por su motor de descifrado; un sistema capaz de poner a prueba la seguridad de una red, descifrando las claves WEP y WPA definidos en sus puntos de acceso.

- ✓ **PRTG Network Monitor**

PRTG **Network** Monitor es un **software** de supervisión de redes completo, que ofrece una gran variedad de posibilidades para monitorear un **router.** Tiene la capacidad de inspeccionar el tráfico de éste y el uso de la red a todas horas. Si se detectan anomalías en el comportamiento de dicho tráfico, el **software** tiene la facultad de avisar en seguida; de esa forma se pueden resolver problemas antes de que afecten a otros.

También existen otros monitores de red no tan potentes y con menos dispositivos inalámbricos detectados, pero que pueden estar disponibles gratuitamente. Entre ellos se recomienda Kismet.

Kismet es un **sniffer** que sirve para la detección de intrusiones en redes inalámbricas 802.11, funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw y puede rastrear tráfico 802.11b, 802.11a, 802.11g y 802.11n. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. El cliente puede también actuar en

Windows; aunque la única fuente entrante de paquetes compatible es otra sonda. Este **software** se diferencia de otros **sniffers** inalámbricos por su funcionamiento pasivo, ya que lo hace sin enviar ningún paquete detectable, permitiendo localizar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros.

Igualmente, Kismet incluye características básicas de sistemas de detección de intrusos, como identificar programas de rastreo inalámbricos, incluyendo a NetStumbler o también ciertos ataques de red inalámbricas. Kismet tiene tres partes diferenciadas, las cuales son: una *sonda* que es utilizada para recoger paquetes; un servidor que recibe e interpreta dichos paquetes, puede ser usado en conjunción con dicha sonda o consigo mismo (extrapolando la información inalámbrica y organizándola); finalmente el *cliente*, quien se comunica con el servidor y muestra los datos que éste analizó.

# ANEXO

# ANEXO

## 1. Problemas y soluciones que presentan los usuarios con respecto a su equipo.

Aunque se tenga el equipo más potente del momento, siempre van a existir eventualidades que no nos permitan configurar adecuadamente nuestros equipos para poder conectarlos a las redes inalámbricas, así como a la RIU. Este anexo mencionará algunos de estos problemas y la manera de solucionarlos para poder tener una conexión adecuada.

A veces damos por hecho que nuestros equipos ya están preparados para poder ser conectados; quizá sí, pero cabe una remota posibilidad de que -por el más insignificante detalle- no sean capaces de ver la red. Si este es el caso, muy posiblemente no se tenga prendida la tarjeta inalámbrica; para poder corregir esto debemos fijarnos en el icono que se encuentra en la esquina inferior derecha de nuestro equipo. La imagen ilustra la forma en la que se vería este icono:

Para poderla reactivar se debe buscar en el teclado el icono de la inalámbrica, por lo regular casi siempre se encuentra en las teclas de la parte superior, que son las funciones; la podemos identificar fácilmente, ya que van desde F1 hasta F12. La forma de dicho icono puede ser la siguiente:

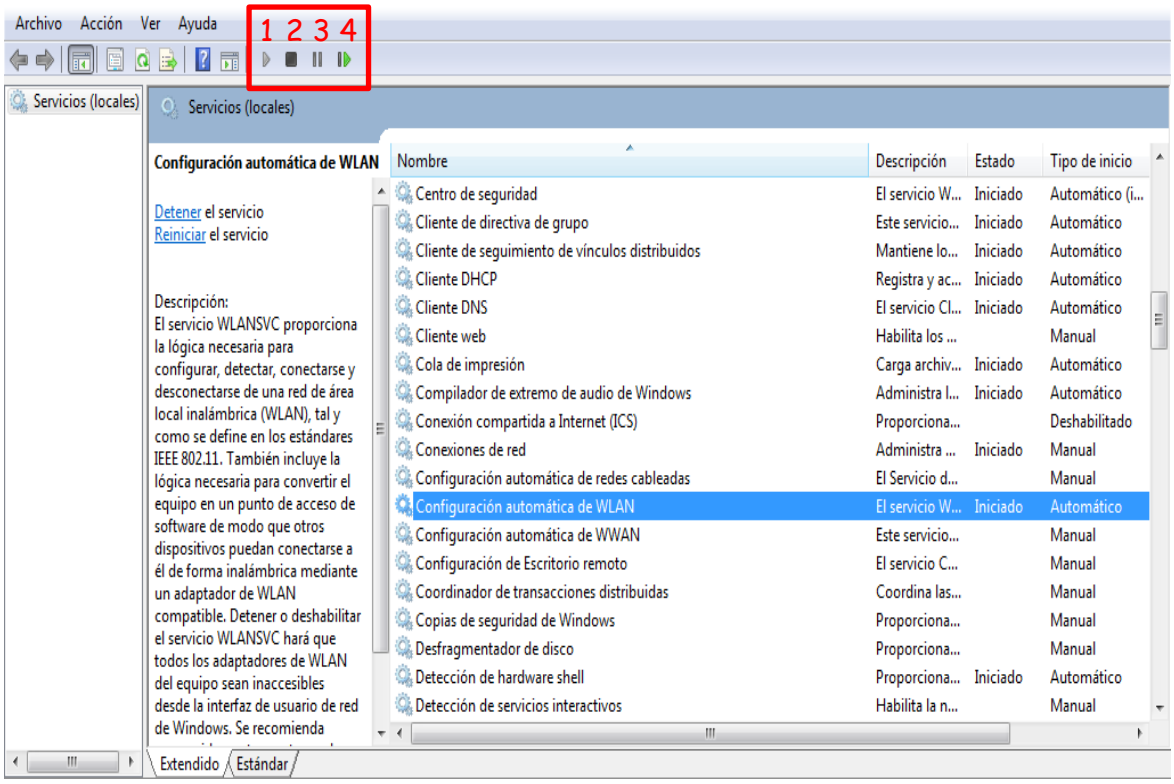
No todas las computadoras cuentan con estas teclas, ya que depende del modelo y de la marca; algunos equipos traen un solo botón, el cual no necesita otra combinación solamente se presiona y se activa la inalámbrica, éste puede encontrarse arriba o a un costado del teclado, o bien en alguno de los costados del equipo, como se puede apreciar en las siguientes imágenes.





Si después de esto aún no podemos conectar nuestro equipo a la red, otra posible solución es reiniciar el servicio. La ruta que se debe seguir es: Inicio / Panel de control / Herramientas administrativas / Servicios / Configuración automática de WLAN. Cuando lleguemos a esta última la seleccionamos y, con los controles que se encuentran encerrados en la siguiente imagen, podemos realizar estos servicios (menciono su función de izquierda a derecha):

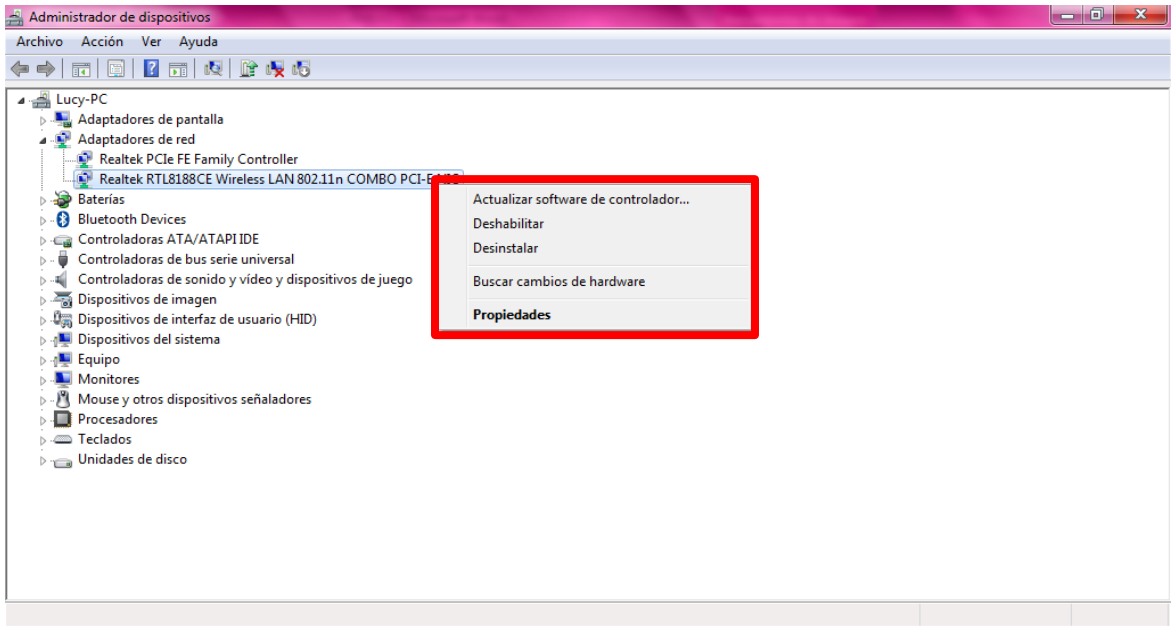
1. Iniciar servicio.
2. Detener servicio.
3. Hacer una pausa en el servicio.
4. Reiniciar servicio.



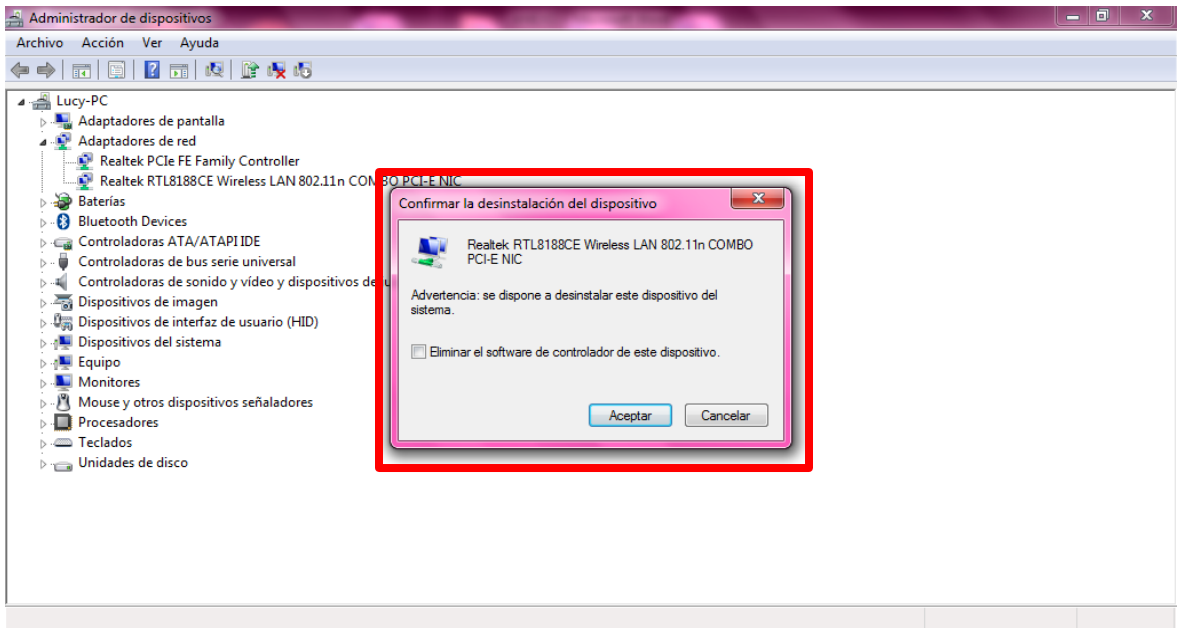

Una vez que reiniciamos el servicio -en teoría- podríamos configurar adecuadamente la red. En algunas ocasiones aún persiste el problema, en este caso podríamos dar otra solución que -en lo personal- no es lo idóneo pero sí lo mejor, ya que las tarjetas inalámbricas se pueden llegar a "viciar"; entonces para lograr su buen funcionamiento podemos "resetearlas", el inconveniente de esto es que todas las redes que tenemos configuradas con anterioridad serán eliminadas, obviamente tendremos que reconfigurar esas redes. Para poder lograr lo anterior se debe seguir la siguiente ruta: Inicio / Panel de control / Administrador de dispositivos/ Adaptadores de red. Cuando ya se está en este punto buscamos la tarjeta Wireless, la seleccionamos y -manteniendo el puntero sobre el nombre de la tarjeta- presionamos el botón derecho del mouse y se va a desplegar un menú, el cual nos da las siguientes opciones:

1. Actualizar **software** del controlador…
2. Deshabilitar.
3. Desinstalar.
4. Buscar cambios de **hardware**.
5. Propiedades.

La ventana lucirá de la siguiente manera:

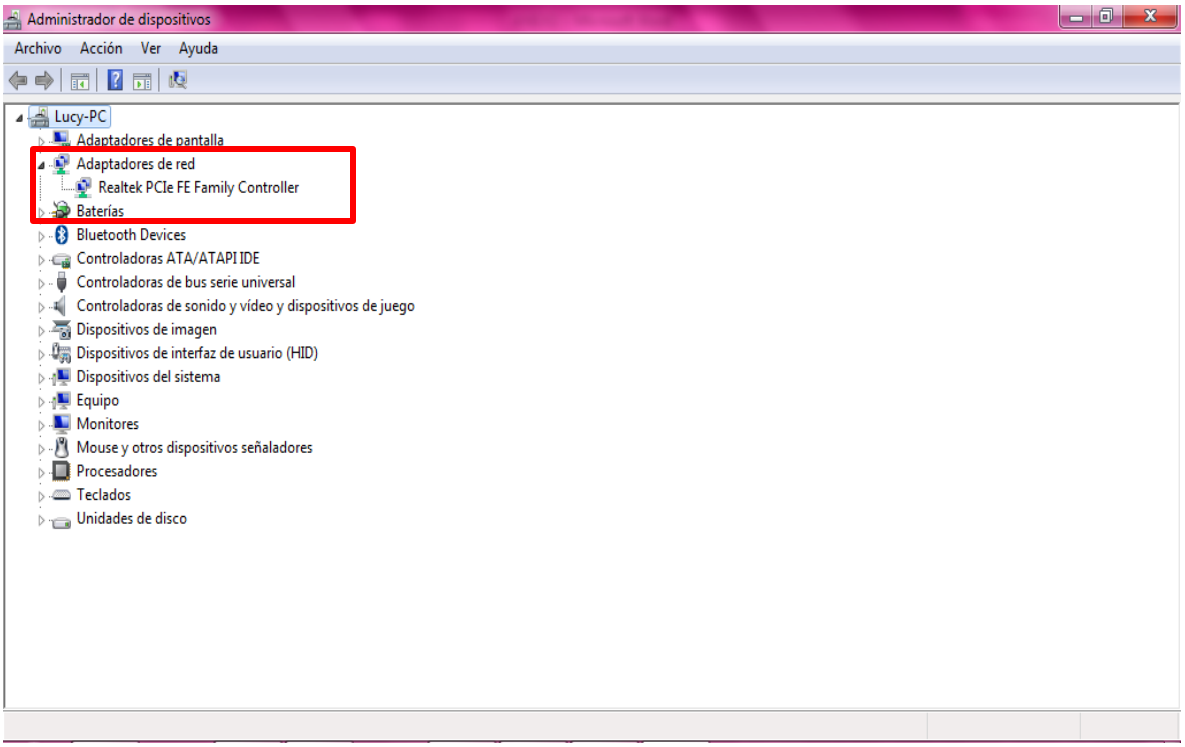



Cuando visualicemos el menú se deberá seleccionar la opción **Desinstalar**, inmediatamente saldrá un cuadro de diálogo, el cual se puede apreciar resaltado en un cuadro rojo en la siguiente imagen.

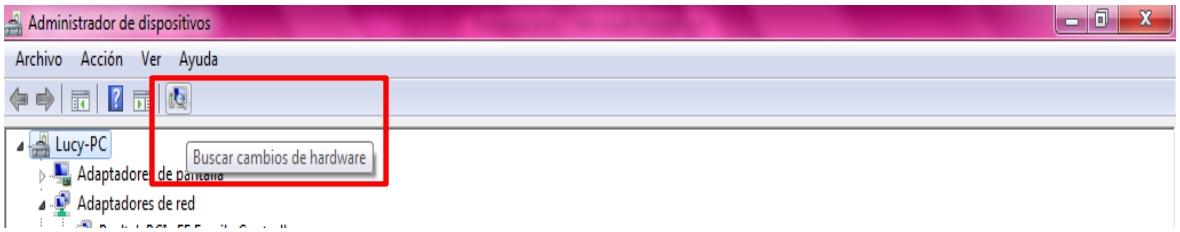


En este cuadro de diálogo sólo se debe seleccionar el botón **Aceptar**. Por ningún motivo se debe activar el cuadro que está junto a la opción "Eliminar el **software** de controlador de este dispositivo" , ya que si se selecciona se pierde el controlador (**software**) de la tarjeta de red y se tendrá que buscar en la página del fabricante del equipo. Lo único que nos interesa es formatear esta tarjeta.

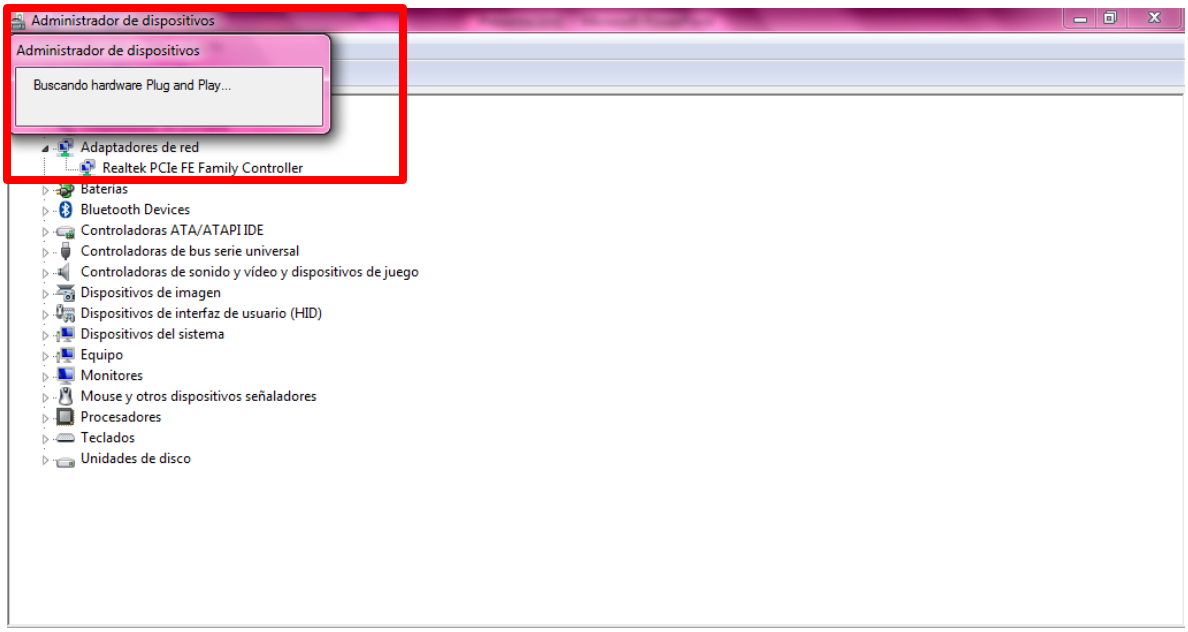
En la siguiente imagen se puede observar que ya no se encuentra la tarjeta inalámbrica.



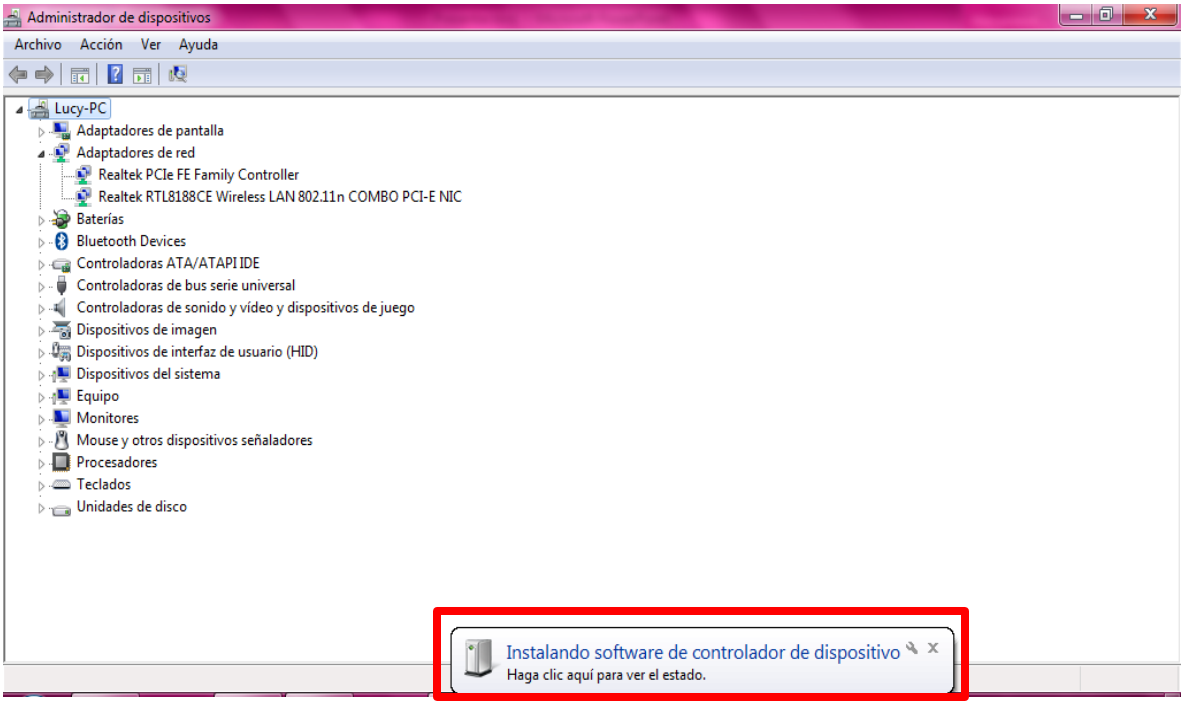

Para volver a activarla se tiene que presionar un botón en la parte superior, éste tiene la forma de una computadora con una lupa; es más, cuando el puntero pase por encima del icono saldrá un diálogo que dice "Buscar cambios de **hardware**" y se verá de la siguiente manera:



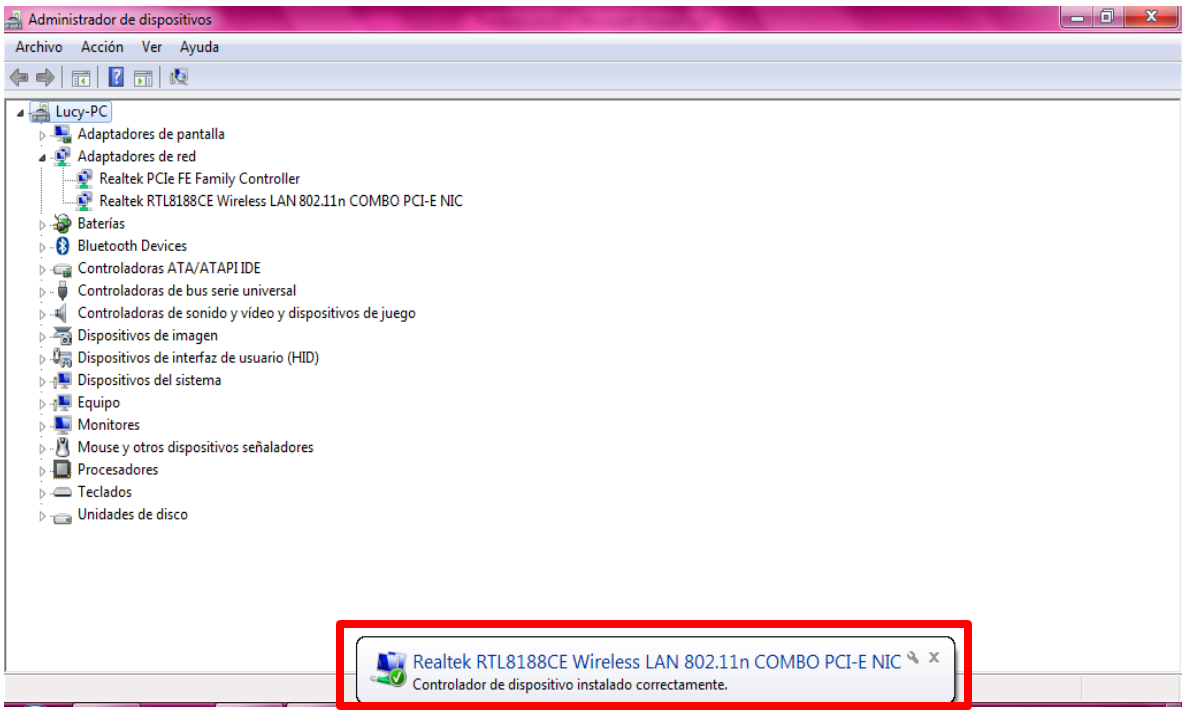
Una vez que se presionó el equipo, comenzará a buscar el dispositivo que se encuentra inactivo; porque -si bien recordamos- no se ha borrado el controlador, éste aún se encuentra almacenado en el equipo.




Cuando el equipo ya encontró la tarjeta manda un aviso que dice: "Instalando **software** de controlador de dispositivo", el cual se puede visualizar en la parte inferior derecha de la pantalla. Esto se ilustra en la siguiente imagen.



Ya que terminó de instalar la tarjeta el equipo envía un mensaje confirmatorio, el cual nos afirma que el dispositivo ha sido instalado correctamente; éste aparece en el mismo lugar del mensaje anterior que dice: "Instalando **software** de controlador de dispositivo". Pero ahora se pueden visualizar los datos técnicos de la tarjeta de red, la pantalla lucirá de la siguiente manera (cabe recordar que no va a decir lo mismo en todos los equipos, ya que depende del modelo y fabricante del equipo).




Una vez que se reinstaló la tarjeta de red, se puede configurar el equipo para conectarlo a la red inalámbrica.

Si después de hacer lo antes descrito no se puede conectar a la red inalámbrica cabe la posibilidad que el problema sea físico; eso quiere decir que la tarjeta inalámbrica puede estar dañada, en este caso sería complicado cambiarla internamente y se deberá adquirir una externa. En el mercado se pueden encontrar gran variedad de éstas y su instalación es fácil, ya que viene con su disco de instalación; algunas de ellas cuentan con su propio programa para la configuración de redes o bien podemos hacerlo con el mismo Windows.

Otra causa por la cual nuestro equipo no podría conectarse a red, radicaría en un problema de **software**; por ejemplo, puede ser que no se cuente con las actualizaciones necesarias. Si este es el problema la solución es fácil, con sólo bajar estas actualizaciones el equipo quedará listo. Por otro lado, los antivirus son otra posible dificultad; para resolver esto debemos irnos a los atributos de éste y cambiar algunos atributos para permitir la configuración de la red inalámbrica. Aquí no puedo dar los pasos a seguir, ya

que existen muchísimos antivirus en el mercado y cada uno tiene características diferentes.

Si el dispositivo que queremos conectar es diferente a una laptop y no podemos configurarlo, la página de RIU cuenta con diferentes manuales con las instrucciones necesarias para poder hacer la conexión, éstos se pueden consultar en el siguiente link:

http://www.riu.unam.mx/conecta.html

# CONCLUSIONES

# CONCLUSIONES

Al llegar al final de este trabajo he podido reafirmar la trascendencia que tienen en la actualidad las redes inalámbricas, pues debido al ritmo de vida actual no podemos estar -literalmente- estáticos; es decir, nuestra necesidad de desplazamiento nos ha llevado a crear herramientas que nos acompañen a donde quiera que nos movamos, las cuales -además- deben ser funcionales para poder realizar de manera exitosa nuestras tareas diarias.

Lo anterior implica, de manera especial, a la población universitaria, pues a causa del incremento de dispositivos móviles dentro de los campus, nació la implementación de redes inalámbricas; dado que hoy día es obsoleto un dispositivo móvil que no tenga acceso a Internet. En el caso de la UNAM, RIU (Red Inalámbrica Universitaria) ha sido una herramienta indispensable para toda la comunidad; aunque -debido al aumento de usuarios- ha corrido el riesgo de ser rebasada, aunado a que ahora en los campus se ha implementado Infinitum Móvil. Con todo y esto, no debemos olvidar que RIU es la primera red inalámbrica implementada, exclusivamente, para espacios universitarios y en ello radica su preponderancia.

Por lo ya expuesto y debido a la importancia de RIU, considero necesaria una reestructuración de ésta para poder brindar un mejor servicio. Quizá en una primera etapa las modificaciones deberían ser en los edificios, ya que en éstos existe una alta concentración de usuarios quienes, como resultado de la distribución de las antenas, han visto afectada la cobertura; pues en algunos lugares la señal es de mala calidad o simplemente no llega a ser percibida por los equipos.

Asimismo, me parece necesario que las Unidades de Sistemas de los campus en donde está implementada RIU deben tener una participación más activa en cuestión de mantenimiento preventivo; además de lo conveniente de hacer un monitoreo local, pues sería una manera más fácil de poder detectar fallas que deriven en problemas más graves, los cuales impidan el buen funcionamiento de la red. Una vez localizadas esas irregularidades puede llamarse directamente a los administradores de la red en C.U. De esta forma se tendría una vigilancia constante que facilitaría una pronta solución a cualquier eventualidad, evitando la interrupción de las actividades académicas en la institución.

Para finalizar, me gustaría resaltar los beneficios que RIU ha traído a la comunidad, ya que antes de que ésta se implementara sólo se podía tener acceso en centros de cómputo y era complicado llevar la red a todos los lugares. Aunque -en definitiva- ésta debe crecer más, porque considero que tiene la capacidad de dar un excelente servicio a los usuarios, elevando el desempeño de nuestra prestigiosa casa de estudios, si se sabe explotar al 100%.

# GLOSARIO

# GLOSARIO

**AES:** es un esquema de cifrado por bloques adoptado como un estándar.

**Bits:** es el acrónimo ***B****inary digi****t*** ('dígito binario'). Un bit es un dígito del sistema de numeración binario. El sistema binario usa solo dos dígitos, el 0 y el 1.

**BootP:** son las siglas de **Boot**strap **P**rotocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección **IP** automáticamente.

**Bridges:** dispositivo de interconexión de redes de computadoras, esto quiere decir que sirve para conectar redes separadas.

**Broadcast:** es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

**BSS:** También conocido como Sistema de Apoyo al Negocio, son los componentes que un proveedor de servicios de telecomunicaciones utiliza para ejecutar sus operaciones hacia los clientes.

**BSSID: (*B****asic S****ervice S****et Id****entifier)*** de una red de área local inalámbrica es un nombre de identificación único de todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

**Buses unidireccionales:** es un bus en el que la información fluye en una sola dirección, del CPU a la memoria o a los elementos de entrada y salida.

**BYOD: B**ring **y**our **O**wn **D**evice, en castellano «trae tu propio dispositivo», es una política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales.

**Carrier-Class:** es un sistema extremadamente confiable, probado y ampliamente capaz.

**Concatenación:** acto de unir o enlazar cosas.

**Concentrador (Hub):** dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

**Conmutador (Swith):** dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del **modelo OSI**. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red.

**CRC-32:** la comprobación de redundancia cíclica es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

**CSMA-CD:** del inglés **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection o en español **acceso múltiple con escucha de portadora y detección de colisiones**, es un protocolo de acceso al medio compartido. Su uso está especialmente extendido en redes **Ethernet** donde es empleado para mejorar sus prestaciones.

**Datagramas:** es un fragmento de paquete que es enviado con la suficiente información para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

**dBi:** es una unidad para medir la ganancia de una antena en referencia a una antena isótropa teórica. El valor de **dBi** corresponde a la ganancia de una antena ideal (teórica) que irradia la potencia recibida de un dispositivo al que está conectado, y al cual también transmite las señales recibidas desde el espacio, sin considerar ni pérdidas ni ganancias externas o adicionales de potencias.

**Desencriptar:** es el proceso contrario a la encriptación, mediante el cual un **criptograma** es transformado en el **texto plano** que le dio origen. En la mayoría de los métodos o algoritmos de encriptación para que la desencriptación sea exitosa es necesario poseer una **clave**, ya sea **pública** o **privada** que asegura que quién realiza el proceso está acreditado para tener acceso a la información original.

**DGTIC:** Dirección General de Cómputo y de Tecnologías de Información y Comunicación, identificada anteriormente como DGSCA (Dirección General de Servicios de Cómputo Académico) y antes de ella como PUC (Programa Universitario de Cómputo). Es la entidad líder en la UNAM en lo relacionado con las tecnologías de información y comunicación (TIC).

**DHCP:** siglas en inglés de *Dynamic **Host** Configuration Protocol*, en español «protocolo de configuración dinámica de **host** es un protocolo de red que permite a los clientes de una red **IP** obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones **IP** dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa **IP**, cuánto tiempo la ha tenido y a quién se la ha asignado después.

**Dirección MAC:** siglas en inglés de *Media Access Control*; en español "control de acceso al medio" es un identificador de 48 **bits** (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

**Drivers:** un **driver o controlador de dispositivo** para equipos, es un programa cuya finalidad es **relacionar el sistema operativo con los dispositivos hardware** (tarjeta gráfica, tarjeta de sonido, módem, tarjeta de Tv, wifi, lector mp3, etc.) y periféricos (impresora, escaner, cámara fotográfica, cámara de vídeo, etc.) de nuestro equipo.

**Encriptar:** es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.

**ESSID:** significa **Extended Service Set ID** y es el nombre identificable de una red.

**Ethernet:** es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD). Su nombre viene del concepto físico de *ether*. **Ethernet** define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del **modelo OSI**.

**FHSS:** del inglés *Frequency Hopping Spread Spectrum*, en español espectro ensanchado por salto de frecuencia es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos **bits**.

**Firewall:** es **software** o **hardware** que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo. También puede ayudar a impedir que **hackers** o **software** malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un **firewall** puede ayudar a impedir que el equipo envíe **software** malintencionado a otros equipos.

**Firmware:** es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura/escritura (ROM, EEPROM, flash, etc.), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

**Frame relay:** es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones. Frame Relay permite la transmisión de datos a altas velocidades basada

en protocolos de conmutación de paquetes. En Frame Relay los datos son divididos en paquetes de largo variable los cuales incluyen información de direccionamiento. Los paquetes son entregados a la Red Frame Relay, la cual los transporta hasta su destino específico sobre una conexión virtual asignada.

**Frame(s):** que es de tamaño fijo, estructura de datos que contiene una descripción particular de un objeto, que se deriva de conceptos avanzados y de la experiencia.

**Gateway:** es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

**Hackear:** se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina. El término hackear también significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.

**Hacker:** es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío.

**Half-duplex:** Cuando los datos circulan en una sola dirección por vez, la transmisión se denomina half-duplex. En la transmisión half-duplex el canal de comunicaciones permite alternar la transmisión en dos direcciones, pero no en ambas direcciones simultáneamente.

**Hardware:** se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

**Host (s):** también llamados anfitriones, se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar *anfitriones* para tener acceso a la red. En general, los *anfitriones* son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc.

**IBM:** International Business Machines, es una empresa multinacional estadounidense de tecnología y consultoría.

**IEEE:** corresponde a las siglas de ***The Institute of Electrical and Electronics Engineers***, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas

tecnologías, como ingenieros en eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación.

**IOS Contente Fitering:** es una solución de seguridad Web que ayuda a las organizaciones a proteger contra las amenazas de Internet conocidas y nuevas.

**IP:** es un acrónimo para Internet Protocol, un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP. Una dirección IP (o simplemente *IP* como a veces se les refiere) es un conjunto de cuatro números del 0 al 255 separados por puntos.

**IPS:** es un **software** que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

**ISO:** Organización Internacional de Normalización.

**MAC:** identificador de 48 **bits** que se corresponde de forma única con una interfaz de red.

**Man in the middle attack, MiTM:** es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

**Mbps:** megabit por segundo es una unidad que se usa para cuantificar un caudal de datos equivalente a 1024 kb/s.

**Modelo OSI:** en inglés, **O**pen **S**ystem **I**nterconnection "sistemas de interconexión abiertos" es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización.

**Modem:** acrónimo de **mo**dulator **dem**odulator, es el dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cable módem. Este aparato sirve para enviar la señal moduladora mediante otra señal llamada portadora.

**Multicast:** en español Multidifusión, es el envío de la información en múltiples redes a múltiples destinos simultáneamente.

**NAT:** en español Dirección de Red, es un mecanismo utilizado por **routers IP** para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

**Network (s):** también red a aquellas series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí, además de recursos y servicios, con el fin de generar una experiencia de trabajo compartida, y ahorrar tiempo y dinero.

**Networking:** es la integración de dos sistemas de redes completas.

**No-break:** es un dispositivo que se conecta al enchufe de la pared, integra una circuitería especial que permite alimentar un juego de baterías recargables internas mientras suministra energía eléctrica a la computadora. En caso de que se dé un corte de energía en el suministro de la red doméstica, las baterías automáticamente continúan alimentando a la computadora por un cierto periodo de tiempo, evitando pérdida de información.

**Ondas electromagnéticas:** son aquellas ondas que no necesitan un medio material para propagarse. Incluyen, entre otras, la luz visible y las ondas de radio, televisión y telefonía.

**OSI:** ***O****pen* ***S****ystem* ***I****nterconnection* "sistemas de interconexión abiertos" es el modelo de red descriptivo. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

**Password:** es una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

**PC:** son las siglas en inglés para denominar a una Computadora Personal.

**PDA:** un ordenador de bolsillo, organizador personal o una agenda electrónica de bolsillo, (PDA) (del inglés: *personal digital assistant* (asistente digital personal), es una computadora de mano originalmente diseñada como agenda electrónica (para tener uso de calendario, lista de contactos, bloc de notas, recordatorios, dibujar, etc.) con un sistema de reconocimiento de escritura.

**Peer-to-peer:** se traduce como par a par o punto a punto, y más conocida como P2P, se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red.

**Rack:** es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios.

**RC4:** es el sistema de cifrado de flujo *Stream cipher* más utilizado y se usa en algunos de los protocolos más populares como **Transport Layer Security** (TLS/**SSL**, para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP, para añadir seguridad en las redes inalámbricas).

**Red ad-hoc:** es un tipo de red inalámbrica descentralizada, porque no depende de una infraestructura pre-existente, como **routers** (en redes cableadas) o de puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.

**Roaming:** también conocido como Itinerancia utilizado en las redes Wi-Fi significa que el dispositivo Wi-Fi del cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.

**Routers:** (anglicismo) también conocido como enrutador o encaminador de paquetes, y españolizado como rúter es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el **modelo OSI**. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendase por subred un conjunto de máquinas **IP** que se pueden comunicar sin la intervención de un encaminador (mediante ***bridges****/puentes* ), y que por tanto tienen prefijos de red distintos.

**Routing:** recorrido.

**Sistemas ofimáticos:** son los utilizados para la realización mecanizada de las diversas tareas de la oficina, generalmente poco estructuradas. Podemos definir la ofimática como el conjunto eficiente de aplicaciones para la creación de documentos, comunicación y análisis de información de negocios. Ésta extiende la productividad a la Web, con la modernización de los procesos de trabajo y simplificando la compartición, acceso y análisis de ésta información.

**Site:** sitio.

**Sniffer:** es un programa de captura de las tramas de red (unidad de envió de datos).

**Software:** conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

**Spam:** correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*.

**Split-tunneling:** (división de túnel), es una red de computadora, permite que el usuario acceda a una red pública (internet) o bien una red LAN o WAN, al mismo tiempo, utilizando la misma conexión de red física. Este servicio de conexión generalmente se facilita a través de un programa como una aplicación de **software** de cliente **VPN**.

**Spyware:** (programa espía) es un **software** que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

**SSH:** **S**ecure **SH**ell, en español: intérprete de órdenes segura, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).

**SSL:** Secure Sockets Layer; en español «capa de conexión segura», es un protocolo criptográfico que proporcionan comunicaciones seguras por una red, comúnmente Internet.

**Stateful:** es un servidor de seguridad que realiza un seguimiento del estado de las conexiones de red que viajan a través de ella. El servidor de seguridad está programada para distinguir paquetes legítimos para diferentes tipos de conexiones. Sólo los paquetes que coincidan una conexión activa conocida será permitido por el firewall; otros serán rechazados.

**Token:** también llamado componente léxico es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación.

**Token passing:** (Paso de ficha) protocolo que se utiliza en redes Arcnet y Token Ring, y que se basa en un esquema libre de colisiones, dado que la señal (token) se pasa de un nodo o estación al siguiente nodo. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un sólo paquete viajará a la vez en la red.

**Transport Layer Security,TLS:** en español «seguridad de la capa de transporte» es un protocolo criptográficos que proporciona comunicaciones seguras por una red, comúnmente Internet.

**Unicast:** se basa en un proceso de envío de una información en una o más unidades de datos (**datagramas IP**) desde una máquina origen a una única máquina destinataria o receptor final. Por tanto, es una transmisión punto a punto con cada destinatario. Si se desea enviar la misma información y hay "n" destinatarios, habrá "n" comunicaciones punto a punto independientes o "n" copias de la misma información enviadas desde la máquina origen.

**VoIP:** Voz sobre Protocolo de Internet, también llamado Voz sobre **IP**, Voz **IP**, Voz**IP**, (Vo**IP** por sus siglas en inglés, *Voice over **IP***), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo **IP** (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de *Public Switched Telephone **Network***, Red Telefónica Pública Conmutada).

**VPN:** de las siglas en inglés de *Virtual Private* ***Network***, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

**XOR:** puerta lógica, o compuerta lógica, es un dispositivo electrónico con una función booleana. Suman, multiplican, niegan o afirman, incluyen o excluyen según sus propiedades lógicas. Se pueden aplicar a tecnología electrónica, eléctrica, mecánica, hidráulica y neumática. Son circuitos de conmutación integrados en un chip. La XOR representa la función de la desigualdad, es decir, la salida es verdadera si las entradas no son iguales, de otro modo el resultado es falso. Una manera de recordar XOR es "uno o el otro, pero no ambos".

# FUENTES DE CONSULTA

# FUENTES DE CONSULTA


- ✓ Black, Uyless,
  Redes de Computadores (Protocolos, normas e interfaces),
  2ª Edición,
  Ed. Alfaomega,
  México, 1997,
  pp. 585.

- ✓ Carballar, José Antonio,
  Wi-Fi (Cómo construir una red inalámbrica),
  2ª Edición,
  Ed. Alfaomega,
  México, Febrero 2005,
  pp. 257.

- ✓ Carballar, José Antonio,
  WiFi (Lo que necesitas saber),
  1ª Edición,
  Ed. Alfaomega,
  México, Julio 2010,
  pp. 211.

- ✓ Gallo, Michael A. / Hancock, William M.
  Comunicación entre computadoras y tecnologías de redes,
  Ed. Thomson,
  México, 2002,
  pp. 632.

- ✓ Gómez López, Julio,
  Guía de Campo Wi-Fi,
  1ª Edición,
  Ed. Alfaomega,
  México, Abril 2008,
  pp. 216.

- ✓ Halsall, Fred / Traducción Rafael Moreno Vozmediano,
  Redes de Computadoras e Internet,
  5ª Edición,
  Ed. Pearson Educación,
  Madrid, 2006,
  pp. 826.

- ✓ Huidobro Moya, José M.
  Comunicaciones en redes WLAN,
  1ª Edición,
  Ed. Limusa,
  México, 2006,
  pp. 356.

- ✓ Menascé, Daniel A. / Schwabe Daniel / Traducción: Obligado Guiñazu, Laura,
  Redes de Computadores (Aspectos Técnicos y Operacionales),
  Ed. Paraninfo,
  Madrid, 1988,
  pp. 168.

- ✓ Molina Robles, Francisco José,
  Instalación y mantenimiento de servicios de redes locales,
  1ª Edición,
  Ed. Alfaomega,
  México, Enero 2005,
  pp. 485.

- ✓ Rábago, J. Félix,
  Redes Locales,
  Ed. Anaya Multimedia,
  Madrid, 2008,
  pp. 400.

- ✓ Raya Cabrera, José Luis / Rayas Pérez, Cristina,
  Redes Locales y TCI/IP,
  Ed. Alfaomega,
  México, 1997,
  pp. 185.

- ✓ Raya, José Luis / Raya, Cristina,
  Redes Locales,
  Ed. Alfaomega,
  México, 2002,
  pp. 335.

- ✓ Roldán Martínez, David,
  Comunicaciones Inalámbricas (Un enfoque aplicado),
  Ed. Alfaomega,
  México, 2005,
  pp. 363.

- ✓ Satallings, William / Traducción López Soler, Juan Manuel,
  Comunicaciones y redes de Computadores,
  6ª Edición,
  Ed. Prentice Hall,
  Madrid, 2000,
  pp. 776.

- ✓ Tanenbaum, Andrew S.
  Redes de Computadoras,
  3ª Edición,
  Ed. Prentice Hall hispanoamericana,
  México, 1997,
  pp. 813.

- ✓ "Herramientas software para WIFI" [en línea], 2005, Disponible en: http://blogs.ua.es/redesitis/recursos-didacticos/herramientas-software-para-wifi/

- ✓ De la Rosa Ramos, J, "Seguridad en redes inalámbricas IEEE 802.11 (WLAN) con WEP mejorado" [en línea], 2006, Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/de_l_j/capitulo_3.html#

- ✓ "Definición de red WAN" [en línea], 2008-2014, Disponible en: http://definicion.de/red-wan/

- ✓ Fluke Corporation, "AirMagnet WiFi Analyzer" [en línea], 2006-2014, Disponible en: http://es.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-WiFi-Analyzer

- ✓ Mercado, Armando/Berríos, Figueroa/Chan Ye, Paul, "Redes Inalámbricas ad hoc" [en línea], Disponible en: http://facultad.bayamon.inter.edu/cgonzalezr/ELEN4618/Adhoc.pdf

- ✓ "Redes inalámbricas en modo infraestructura" [en línea], Disponible en: http://meshias.wordpress.com/2010/10/16/redes-inalambricas-en-modo- infraestructura/

- ✓ Blanco, Daniel / Castro, Rubén / Peñaranda, Edgardo / Zapata, Andrea, "Redes Inalámbricas: Modos de ataque y defensa" [en línea], 2012, Disponible en: http://prezi.com/j1corlkalxdw/redes-inalambricas-modos-de-ataque-y-defensa

- ✓ 34Telecom, "Antenas para redes inalámbricas WiFi" [en línea], Disponible en: http://www.34t.com/unique/WiFiAntenas.asp

- ✓ "Red inalámbrica WIFI mantenimiento preventivo" [en línea], 2013, Disponible en: http://www.academica.mx/blogs/red-inal%C3%A1mbrica-wifi-mantenimiento-preventivo

- ✓ "Wi-Fi Protected Access 2" [en línea], 2011, Disponible en: http://www.arg-wireless.com.ar/index.php?topic=249.0

- ✓ Aruba Networks, "Products" [en línea], 2014, Disponible en: http://www.arubanetworks.com

- ✓ Vergara, Kervin, "Topología de red: malla, estrella, árbol, bus y anillo" [en línea], 2007, Disponible en: http://www.bloginformatico.com/topologia-de-red.php

- ✓ Nieto Pérez, Iván, "Introducción a la tecnología WAP" [en línea], 1999-2008, Disponible en: http://www.elcodigo.com/tutoriales/wap/wap1.html

- ✓ Munditeractivos, "¿Qué es IPv6?" [en línea], 2002, Disponible en: http://www.elmundo.es/imasd/ipv6/queesipv6.html

- ✓ Falfán Jiménez, Betzabé, "Administración de la seguridad ITIL" [en línea], 2006 Disponible en: http://www.enterate.unam.mx/Articulos/2006/abril/itil.htm

- ✓ Espina García, Eduardo, "Seguridad en la Red Inalámbrica Universitaria" [en línea], 2007, Disponible en: http://www.enterate.unam.mx/Articulos/2007/agosto/art1.html

- ✓ Paessler, "PRTG" [en línea], Disponible en: http://www.es.paessler.com/prtg

- ✓ Pocalles, Josep, "La importancia de las contraseñas" [en línea], 2010, Disponible en: http://www.helpdesk-software.ws/es/it/2842004.htm

- ✓ Gobierno de España. Ministerio de Industria, Energía y Turismo, "IP.v6 Protocolo de Internet Versión 6" [en línea], Disponible en: http://www.ipv6.es/es-ES/Paginas/Index.aspx

- ✓ Linksys[en línea], Disponible en: http://www.linksysbycisco.com/LATAM/es/learningcenter/WPAyWPA2

- ✓ Rodríguez, Elisabet, "Evolución de la redes inalámbricas" [en línea], 2008 Disponible en: http://www.maestrosdelweb.com/principiantes/evolucion-de-las-redes-inalambricas/

- ✓ Dirección General de Cómputo y de Tecnologías de Información y Comunicación, "Guía para el Registro de Servicios TIC" [en línea], 2014 Disponible en: http://www.servicios.unam.mx/idUnamAI/guias/registro.pdf

- ✓ WiFi-online, "Modo de Punto de Acceso / Cliente-Root-Repetidor-Bridge" [en línea], 2012, Disponible en: http://www.wifi-online.es/blog_wifi-online/modo-de-punto-de-acceso-cliente-root- repetidor-bridge/

- ✓ "Cisco, lo que necesita saber sobre Routing y Switching" [en línea], Disponible en: https://www.cisco.com/web/ES/solutions/smb/products/routers_switches/routing_switching_primer.html