UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

"PROPUESTA DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA EN EL DEPARTAMENTO DE REDES DE LA DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO, C. U."

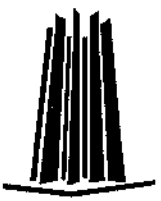
T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A :

ALEJANDRO RENTERÍA ESPINOSA

ASESOR DE TESIS:
M. en I. DAVID J. GONZÁLEZ MAXINEZ



MÉXICO, 2005.

D E D I C A T O R I A.

Este trabajo, culminación no solo de una vida académica, sino de un sueño de vida, se lo dedico a mi mamá, que es la persona que más admiro en este mundo, de la cual me siento muy orgulloso, porque ella es el mejor ejemplo de lucha y superación que he podido tener y por enseñarme que no hay imposibles.

Con mucho cariño y amor

Ale.

AGRADECIMIENTOS

A Dios

Por darme la familia que tengo, por otorgarme defectos y virtudes, por siempre estar a mi lado, por lo bueno y malo que he vivido y por brindarme la oportunidad de llegar a conseguir esta meta en mi vida, en compañía de mis seres queridos.

A mi Mamá y Abuelita

Por darme la oportunidad de estar donde estoy y que pusieron todo de su parte para hacerme un hombre de provecho y seguir estudiando hasta este punto de mi vida.

A mis Hermanos

Por su amor, cariño y apoyo incondicional.

A mi Papá y Abuelitos

Por el amor incondicional y por la huella que dejaron en mi (†).

A mi familia

Por aceptarme tal cual soy y por las muestras de cariño que he recibido de todos ustedes.

AGRADECIMIENTOS

A mis asesores

Por sus observaciones y consejos para la terminación de este trabajo.

A mis amigos, de la ENEP y DGSCA

Por su amistad, alegrías, experiencias vividas, motivaciones y todo el apoyo que me dieron para seguir adelante.

A la UNAM y DGSCA

Por darme los elementos y cualidades necesarias para poder desarrollarme como persona y como profesionista.

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA EN LA DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO C.U.

Introducción

Capítulo I Redes inalámbricas

Capítulo II El estándar IEEE 802.11

Capítulo III Seguridad en el estándar IEEE 802.11

Capítulo IV Propuesta de la red inalámbrica

INTRODUCCIÓN

El mundo de las comunicaciones tiene una serie de cambios muy importantes. En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo, necesidad y aceptación de las comunicaciones móviles y en concreto de las redes inalámbricas.

Una de las tecnologías más prometedoras y discutidas es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja, que actualmente está siendo ampliamente investigada. Las redes inalámbricas facilitan la operación en lugares donde las computadoras no pueden permanecer en un solo lugar, como dentro de edificios, entre edificios o en campus universitarios.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas, sino más bien complementarias, ya que las redes cableadas ofrecen velocidades de transmisión mayor que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, 11 Mbps y 54 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps, 100 Mbps y 1000 Mbps.

Se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "red híbrida" y así poder resolver los últimos metros hacia una estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y que el operador se pueda desplazar con facilidad dentro de un campus u oficina.

Hoy en día no es raro llegar a un hotel, aeropuerto, una conferencia o cualquier otro lugar público y encontrar que si disponemos de una tarjeta inalámbrica en nuestra laptop podemos conectarnos a una red inalámbrica.

Debido a la gran cantidad de información relacionada con las redes inalámbricas y puesto que es imposible abarcar todos los estándares y profundizar en cada uno de ellos, el objetivo de este trabajo es describir el funcionamiento básico de las redes inalámbricas y proponer la implementación de una red inalámbrica en el departamento de redes de la Dirección General de Servicios de Computo Académico, C.U.

La tesis comprende cinco capítulos, dos anexos y un glosario, los cuales se describen de manera breve a continuación:

El primer capítulo describe un panorama general de las redes inalámbricas historia, descripción, funcionamiento, elementos que la conforman, topologías, aplicaciones y beneficios, que fueron el punto de partida para algunas de las tecnologías de datos de hoy en día.

En el segundo capítulo se explora a detalle el protocolo 802.11, sus estándares, medios de acceso, tecnologías y protocolos de comunicación con los que se obtendrá una idea clara del comportamiento de éste.

El tercer capítulo describe el funcionamiento de los diferentes mecanismos de seguridad de las redes inalámbricas, vulnerabilidades y los nuevos mecanismos de seguridad.

Dentro del cuarto capítulo aplicare los conocimientos adquiridos durante el desarrollo de la tesis para la propuesta de implementación de la red inalámbrica en el departamento de redes de la DGSCA C.U

En el quinto capítulo, se hablara del futuro de las redes inalámbricas y de los diferentes grupos que trabajan para el desarrollo de nuevas tecnologías inalámbricas

En el anexo A se muestran las configuraciones de los equipos involucrados (punto de acceso, bridge, radius y switches) de la solución

En el anexo B se describe las características de equipos inalámbricos de tres diferentes compañías para la implementación de la red inalámbrica.

Por último un glosario que se desarrolló dentro de la elaboración de esta tesis como apoyo para la comprensión de la misma.

Capítulo 1

Redes Inalámbricas

1.1 Historia de las redes inalámbricas.

El origen de las redes inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Las investigaciones siguieron adelante tanto con infrarrojos como con radio frecuencias (RF), donde se utilizaba el esquema del spread spectrum (espectro ensanchado), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2.400-2.483,5 GHz, 5.725-5.850 GHz a las redes inalámbricas basadas en spread spectrum.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria, ese respaldo hizo que las redes inalámbricas empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a las redes inalámbricas operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

1.2 ¿Qué es una red inalámbrica?

Una red inalámbrica o WLAN (siglas en inglés de Wireless Local Area Network), es un sistema flexible de comunicación de datos realizado como una extensión o alternativa de una LAN cableada. Utiliza tecnología de radio frecuencia, las redes inalámbricas transmiten y reciben datos por el aire, reduciendo al mínimo la necesidad de conexiones cableadas.

Una red inalámbrica puede definirse como una red local (red de comunicación con una cobertura geográfica limitada, relativamente de alta velocidad de transmisión, baja tasa de errores y administrada de forma privada) que utiliza ondas electromagnéticas para enlazar los equipos conectados a la red en lugar de los cables de par trenzado o de fibra óptica que se utilizan en las redes convencionales cableadas. Estos enlaces se implementan básicamente a través de tecnología de radio frecuencia y en menor medida de infrarrojos.

Hoy en día, a las redes inalámbricas se les está reconociendo más como una necesidad de conexión de uso general para una gama amplia de clientes comerciales e instituciones educativas.

1.3 Tipos de tecnología.

Según el diseño requerido se tienen distintas tecnologías aplicables:

1.3.1 Banda estrecha.

Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

1.3.2 Banda ancha.

Es el usado por la mayor parte de los sistemas inalámbricos. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso de no estar en la correcta frecuencia el receptor, la señal aparece como ruido de fondo.

1.3.2.1 Tipos de tecnología en banda ancha:

a) Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda).

Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

b) Salto de frecuencia (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.

1.3.3 Infrarrojos.

No es una técnica muy usada. Se usan frecuencias muy altas ($3X10^{11}$Hz a $4x10^{14}$Hz) para el transporte de datos. Como la luz, los infrarrojos no pueden traspasar objetos opacos. Por lo que o bien se utiliza una comunicación con línea de visión directa o bien es una difusión.

No son prácticas para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales.

1.4 Como trabajan las redes inalámbricas.

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto.

En una configuración típica una red inalámbrica con un punto de acceso conectado a la red cableada, el punto de acceso recibe la información, la almacena y transmite entre la red inalámbrica y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red inalámbrica a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente y las ondas de radio, vía una antena.

Para poder identificar a las celdas inalámbricas se les asigna un nombre de red en una cadena con longitud máxima de 32 caracteres denominado Service Set Identifier (SSID). Para poder agregarse a una determinada celda es requisito indispensable que el equipo tenga en su configuración interna el mismo SSID.

1.5 Elementos de una red inalámbrica.

1.5.1 Puntos de Acceso (AP): Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto de equipos, reciben y transmiten información de forma similar a la tarjeta de red. Las señales emitidas por el punto de acceso son esféricas, por lo que son capaces de cubrir una área radial a su alrededor. En la figura 1.1 se muestran diferentes puntos de acceso que disponen comúnmente de una interfaz ethernet RJ-45 que le permite estar conectado a una red cableada (LAN), además de la interfaz inalámbrica por la cual se conectan los equipos de dicha naturaleza, actuando así como un HUB inalámbrico.

Entre sus principales características destacan: permitir la conexión a la red inalámbrica, coordinar el tráfico entre estaciones, controlar el acceso, mejorar la calidad de enlace y, por lo tanto, garantizar la calidad de servicio.

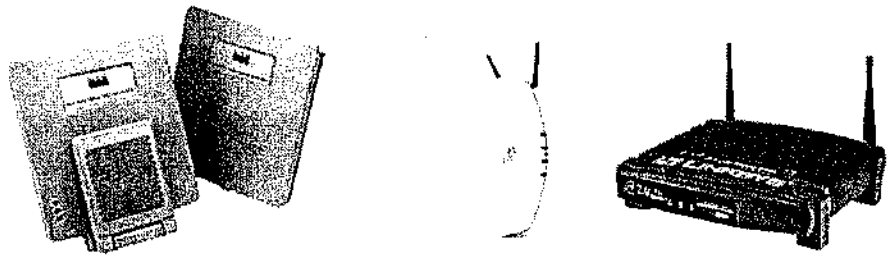


Figura 1.1 Puntos de Acceso (AP)

1.5.2 Puntos de Extensión (EP): Los puntos de extensión funcionan como su nombre lo indica: extienden el rango de la red inalámbrica retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión, proporcionando libertad y flexibilidad de la conectividad inalámbrica a los dispositivos con actividad ethernet.

En la figura 1.2 se muestran los puntos de extensión y gracias a ellos tendremos la oportunidad de conectar con la red inalámbrica cualquier dispositivo cableado de ethernet, independientemente del sistema operativo que utilice y despreocuparse así de su configuración.

Figura 1.2 Puntos de extensión (EP)

1.5.3 Tarjetas de red:

- **PCMCIA:** Reciben y transmiten información digital sobre una frecuencia de radio (2.4 Ghz o 5 Ghz) La tarjeta convierte la señal de radio en datos digitales (pequeños paquetes de información). La tarjeta de red establece la conexión entre el punto de acceso y el dispositivo de comunicación, dichas tarjetas se muestran en la figura 1.3.

Figura 1.3 Tarjetas PCMCIA (PC Cards)

- **Tarjetas PCI:** Se conectan a una computadora de escritorio, y funcionan de forma similar a las tarjetas de red pcmcia, que se muestran en la figura 1.4.

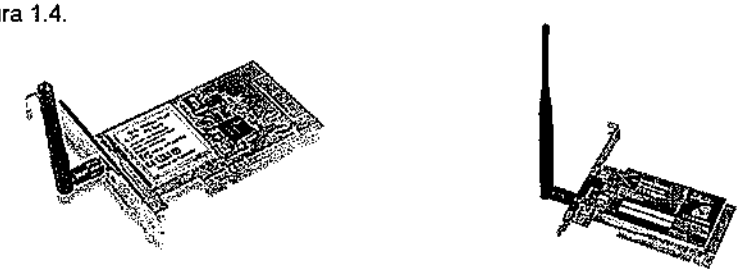


Figura 1.4 Tarjetas adaptadoras PCI

1.5.4 Antenas: Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas. Aumentan la zona de influencia/cobertura de nuestras tarjetas inalámbricas, de manera que en lugar de dar cobertura a unos cientos de metros, podemos alcanzar miles de metros sin problemas, en la figura 1.5 se observan dichas antenas.

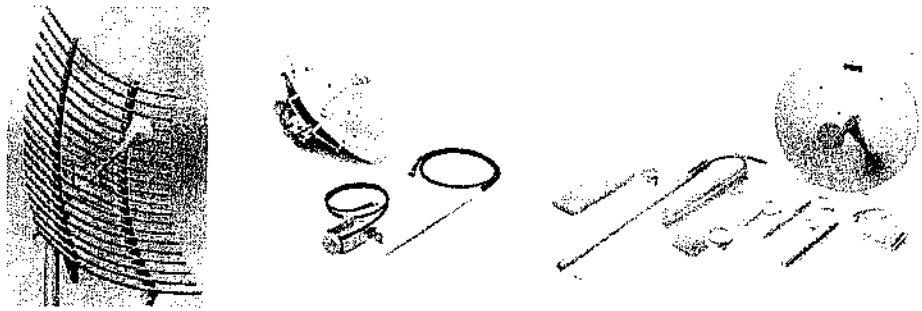


Figura 1.5 Antenas

Tipos de antena.

Básicamente disponemos de dos tipos:

- **Omnidireccionales:** las cuales dan cobertura con un diagrama de radiación circular (360º), como se ve en la figura 1.6. Se supone que dan servicio por igual independientemente de su colocación, pero debido a que las frecuencias en las que estamos trabajando son próximas a microondas, los diagramas no son circulares, son óvalos.

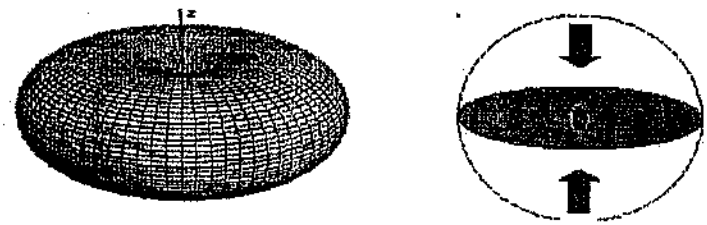


Figura 1.6 Radiación de una antena omnidireccional

- **Direccionales:** son directivas y solo emiten/reciben con un ancho de haz definido por la construcción de la antena como se ve en la figura 1.7.

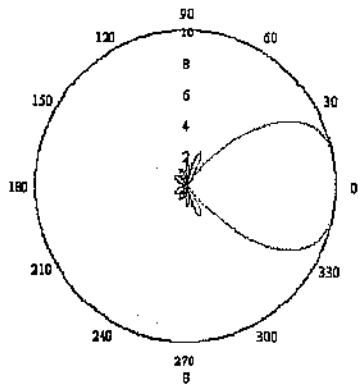


Figura 1.7 Radiación de una antena direccional

1.6 Topologías de las redes inalámbricas.

Las redes inalámbricas pueden ser simples o complejas.

1.6.1 Topología ad-hoc.

También llamadas IBSS, Independent Basic Service Set, es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.

En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

Para una red inalámbrica con topología ad-hoc, todos los equipos conectados deben de ser configurados con el mismo identificador de servicio básico (Basic Service Set, BSSID)

Un ejemplo sencillo de esta configuración se muestra en la figura 1.8.

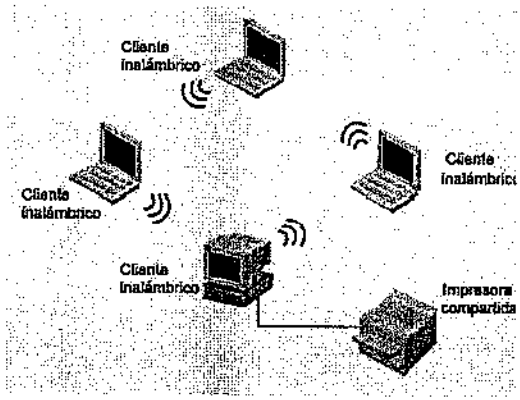


Figura 1.8. Topología ad-hoc.

1.6.2 Topología en modo infraestructura.

Del mismo modo, como en las redes ethernet, en las cuales se dispone de un hub o concentrador para unir todos los host, ahora disponemos de los puntos de acceso (AP), los cuales se encargan de crear esa conversación para que se puedan conectar el resto de host inalámbricos que están dentro de su área de cobertura, dicha configuración la podemos ver en la figura 1.9.

Los puntos de acceso (AP's) son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

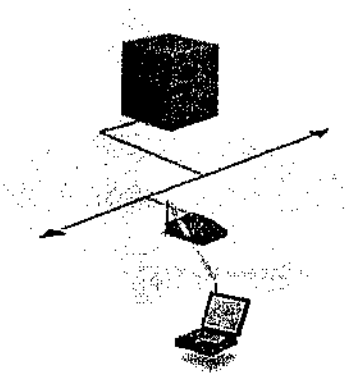


Figura 1.9. Cliente y punto de acceso

En la figura 1.10 podemos ver una de las utilidades más interesantes de esta tecnología inalámbrica, es la posibilidad de realizar roaming entre los AP's, con lo que al igual que la tecnología celular, no perdemos cobertura y podemos movernos desde el campo de cobertura de un AP a otro sin problemas, para ello debemos configurar los APs para que trabajen en distintos canales de frecuencia para que no se produzcan problemas de funcionamiento en las zonas donde existe cobertura de más de un AP.

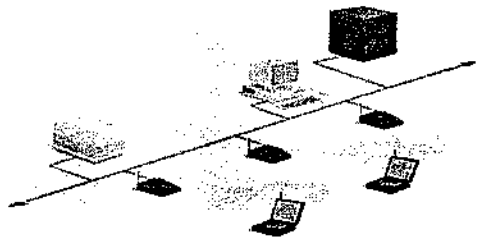


Figura 1.10 Múltiples puntos de acceso y "roaming".

1.6.2.1 Uso de un punto de extensión (EP).

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un punto de extensión (EP) para aumentar el número de puntos de acceso y cobertura de la red inalámbrica, como se muestra en la figura 1.11, de modo que funcionan como tales pero no están conectados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre lo indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden formarse como una hilera para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

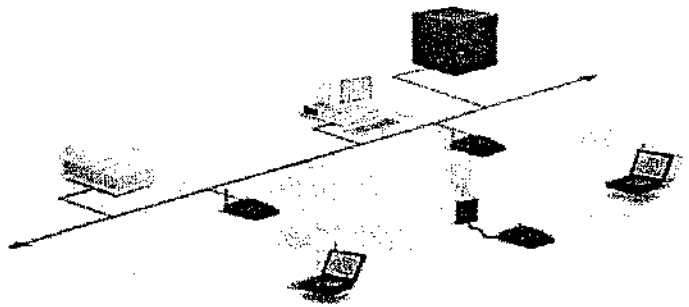


Figura 1.11 Uso de un punto de extensión.

1.6.2.2 Uso de antenas direccionales.

Uno de los últimos componentes a considerar en una red inalámbrica es la antena direccional. Por ejemplo: se quiere una red inalámbrica en un edificio y se necesita extender a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena direccional en cada edificio con línea de visión directa. En la figura 1.12 se muestra la configuración en la cual la antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión inalámbrica en este ejemplo.

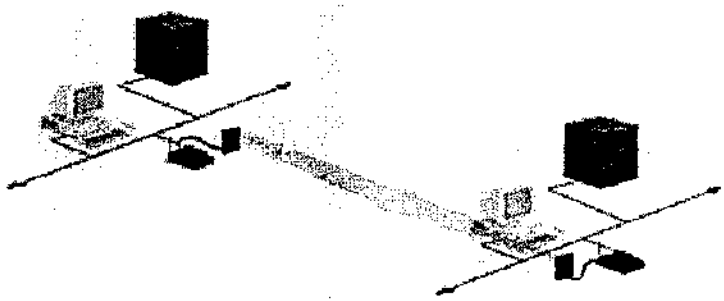


Figura 1.12 Uso de antenas direccionales.

1.7.- Beneficios y aplicaciones de las redes inalámbricas.

Con las redes inalámbricas, los usuarios pueden acceder a información compartida sin necesidad de tener que buscar un lugar donde poder conectar sus equipos, entre los beneficios que ofrecen están:

- **Movilidad:** Las redes inalámbricas ofrecen información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

- **Facilidad de instalación:** Evitan obras para tender cables a través de muros y techos.

- **Flexibilidad:** Las redes inalámbricas permite llegar a lugares donde una red cableada no puede.

- **Minimización de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el coste inicialmente más alto de la red inalámbrica es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

- **Escalabilidad:** El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes.

Entre las múltiples aplicaciones que en la actualidad se les está dando a las redes inalámbricas, destacan las siguientes:

- Entornos de difícil cableado, como edificios históricos, instalaciones con asbesto,...
- Entornos cambiantes, como bancos, pequeñas empresas,...
- En lugares o sedes temporales donde podría no compensar la instalación de una red cableada.
- Para interconectar dispositivos en ambientes industriales con severas condiciones ambientales.
- Para interconectar redes locales cableadas entre dos edificios.
- Etc.

Con este último punto finaliza el presente capítulo observando la historia de las redes inalámbricas, detalles, entendiendo su historia, componentes, topologías, funcionamiento y beneficios que nos ofrece este tipo de tecnología, para así abrirnos paso al segundo capítulo: El estándar IEEE 802.11

Capítulo 2

El estándar IEEE 802.11

2.1 Introducción.

El IEEE 802.11 es un estándar para redes inalámbricas definido por la organización IEEE (Institute of Electrical and Electronics Engineers), instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías.

El estándar IEEE 802.11 supone la apuesta del IEEE por las redes inalámbricas. Todas ellas se basan en una red tipo Ethernet y, aunque su filosofía es la misma, difieren en la banda de frecuencia utilizada, el ancho de banda que ofrecen, etc.

El estándar IEEE 802.11 es un estándar en continua evolución, debido a que existen cantidad de grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales.

La primera versión del estándar fue definida en 1997. Aunque el comité evaluador fue creado en 1990, muestra del gran desarrollo que ha sido la primera versión. Esta versión trata de ofrecer varias formas para poder interconectar computadores y otros dispositivos sin la necesidad de cables. Esta primera versión, visto hoy, está obsoleta, pero ha marcado un principio para una tecnología prometedora.

Se nos ofrece tres alternativas en cuanto a tecnología subyacente para poder realizar nuestra red. Ofrece entre otras cosas tres capas físicas, por la cual enviaríamos los datos, una por infrarrojos (IR), y dos por la banda ISM 2.4Ghz con técnicas de espectro ensanchado, ya sea con salto en frecuencias como por secuencia directa.

La especificación original de 802.11 preveía conexiones a velocidades de 1 ó 2 Mbps en la banda de los 2,4 GHz utilizando salto de frecuencias (FHSS) o secuencia directa (DSSS). FHSS y DSSS son dos tipos de espectro ensanchado (spread spectrum). 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 y escuchas. FHSS (salto de frecuencias) se basa en que transmite en diferentes bandas de frecuencias, produciéndose saltos de una otra de una forma aleatoria que es posible predecir. Por contra, con DSSS (secuencia directa) se envían varios bits por cada bit de información real.

En julio de 1999, los líderes de la industria inalámbrica se unieron para crear la Alianza para la Compatibilidad Ethernet Inalámbrica (WECA).

Dentro de la familia de las 802.11, el estándar más extendido a día de hoy es el 802.11b, también conocido como wi-fi (wireless fidelity). wi-fi es un término registrado auspiciado por la WECA, cuya finalidad es certificar productos de diferentes fabricantes basados en 802.11b y capaces de inter operar entre sí. Utiliza la banda de los 2,4 GHz y proporciona anchos de banda de hasta 11 Mbps. En espacios de interior es capaz de comunicar nodos separados 50 metros entre sí, mientras que llega a los 100 metros en el exterior

La siguiente generación de las 802.11 viene de mano de 802.11a, también denominada WLAN. Esta implementación utiliza la banda de los 5 GHz y puede llegar a ofrecer el nada despreciable ancho de banda de hasta 54 Mbps. Para evitar interferencias se transmite en OFDM (Multiplexación por División en Frecuencia Ortogonal), cabe mencionar que también existe el estándar 802.11g. Esta versión proporciona entre 20 y 54 Mbps usando DSSS y OFDM. La característica que lo hace especialmente interesante es su compatibilidad con el estándar 802.11b.

2.2 Tecnología del estándar IEEE 802.11.

Como ya se ha explicado, el estándar permite el uso de varios medios y técnicas para establecer conexiones.

El estándar original permite usar infrarrojos, espectro ensanchado tanto en salto en frecuencias como secuencia directa. Todo ello con la ventaja de usar una capa de acceso al medio (MAC) común. Ello da mucha flexibilidad a los desarrolladores e investigadores, que pueden olvidarse de ciertos aspectos ya que no existe dependencia directa entre ellos.

Los estándares de IEEE 802.11 son de libre distribución y cualquier persona puede ir a la página Web del IEEE y descargarlos. Estos estándares sólo definen especificaciones para las capas físicas y de acceso al medio y para nada tratan modos o tecnologías a usar para la implementación final de una red inalámbrica.

2.2.1 Capa física (PHY).

La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. En la figura 2.1 se muestran las diferentes tecnologías de capa física **(FHSS, DSSS, OFDM e IR)** que se definen para transmitir por el medio inalámbrico.

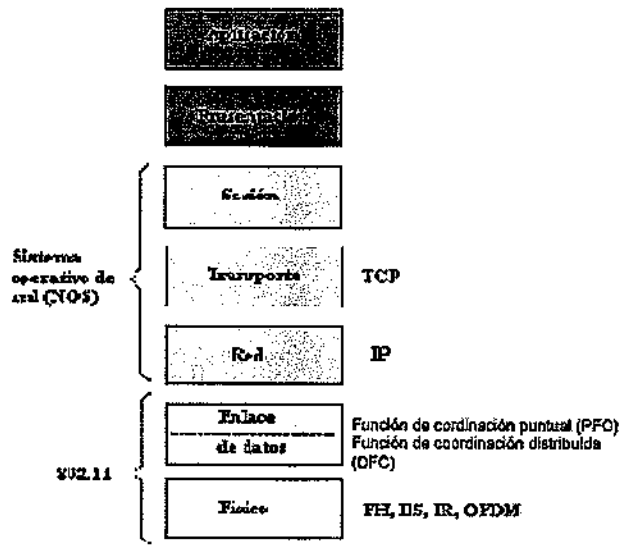


Figura 2.1. Tecnologías de capa física

La capa física se divide en dos subcapas que corresponden a dos funciones de protocolos:

EL **procedimiento de convergencia de la capa física, PLCP** (Physical Layer convergente Procedure), es la subcapa superior y proporciona una función de convergencia que transforma las PDU MAC a un formato adecuado para su transmisión y recepción a través de un medio físico dado.

La supcapa dependiente del medio físico, PDM (Physical Médium Dependent), hace referencia a las características y métodos de transmisión a través de medios inalámbricos

En la figura 2.2 se muestra que cada PDU MAC se transforma en una trama PLCP que consta de tres partes. La primera es un preámbulo que proporciona información de sincronización y de comienzo de trama. La segunda parte es una cabecera PLCP que contiene información sobre la velocidad de transmisión y otra información de inicialización, así como información de longitud de trama y un CRC. La tercera parte consta de la PDU MAC posiblemente modificada (entremezclada) para dar respuesta a las características del medio de transmisión. La estructura completa de cada PLCP depende de la definición de la capa física particular.

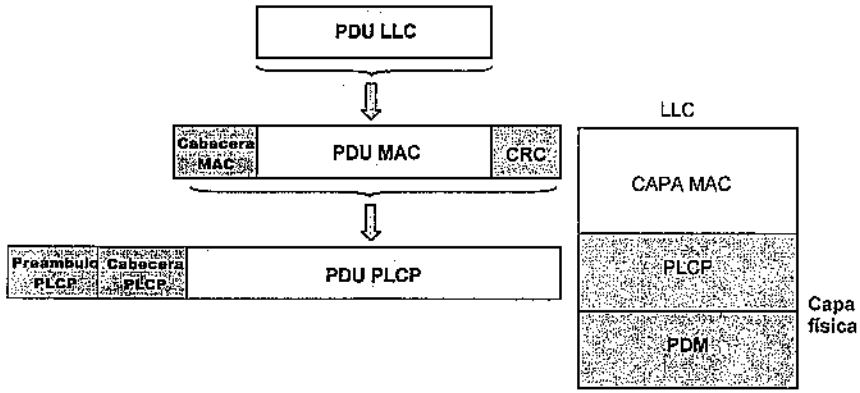


Figura 2.2.- Procedimiento de capa física

2.2.1.1 Radio frecuencia.

Como ya se ha comentado las definiciones para la transmisión por radiofrecuencia en los estándares son espectro ensanchado por salto en frecuencias (FHSS) y espectro ensanchado por secuencia directa (DSSS). Ambos están definidos para trabajar en la banda de 2.4Ghz.

2.2.1.2 Espectro ensanchado.

La tecnología de espectro ensanchado consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en lugar de concentrar la energía de las señales alrededor de una portadora concreta lo que se hace es repartirla por toda la banda disponible.

Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda frecuencial.

2.2.1.2.1 Tecnología de espectro ensanchado por secuencia directa (DSSS).

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

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o *PseudoNoise*). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. En DSSS se representa cada 0 y cada 1, respectivamente, por los símbolos -1 y +1.

Un ejemplo de esta secuencia se muestra en la figura 2.3:

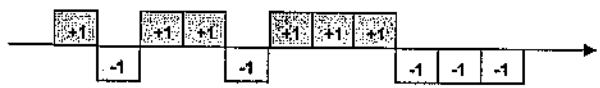


Figura 2.3 Secuencia de Barker.

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

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

A continuación podemos observar en la figura 2.4 como se utiliza la secuencia de *Barker* para modular la señal original a transmitir:

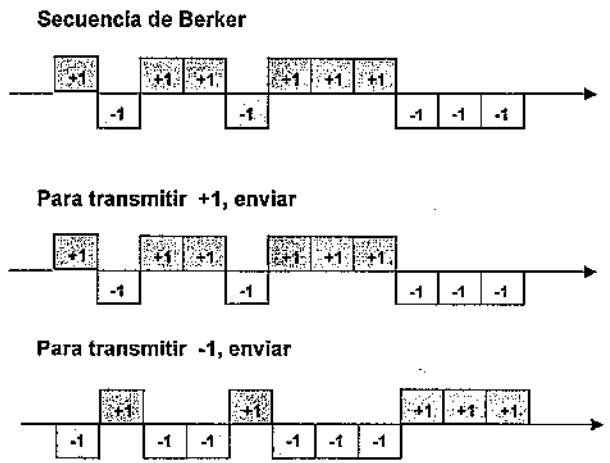


Figura 2.4 Codificación de la información mediante la secuencia de Barrer.

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

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

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

En la figura 2.5 se muestra el formato de las tramas PLCP. El preámbulo comienza con 128 bits de sincronismo entremezclados que el receptor utiliza para detectar la presencia de una señal. El preámbulo finaliza con un delimitador de comienzo de trama de 16 bits usado para la sincronización de bits. La cabecera PLCP consta de un campo de señal de 8 bits que indica a la capa física la modulación a utilizar en la transmisión y recepción de la MPDU, un campo de servicio de 8 bits reservado para uso futuro, un campo de 16 bits que indica el número de octetos en la MPDU, de 4 a 2^{16} y una secuencia CRC de 16 bits.

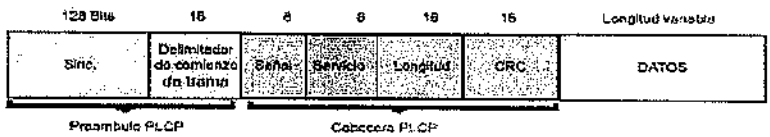


Figura 2.5 Formato de trama PLCP en DSSS

2.2.1.2.2 Tecnología de espectro ensanchado por salto en frecuencia (FHSS).

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

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal.

El orden en los saltos en frecuencia que el emisor debe realizar se puede observar en la figura 2.6, y viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer.

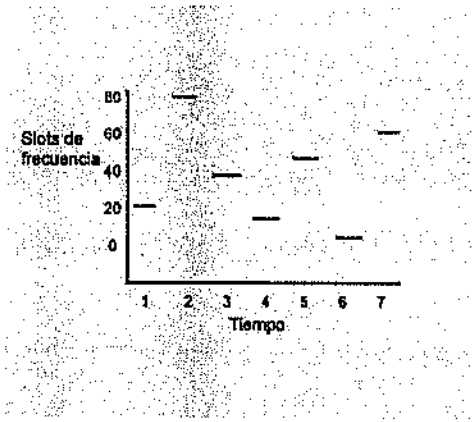


Figura 2.6 Secuencia Pseudoaleatoria

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación el efecto global es que aunque vamos cambiando de canal físico con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación.

Para un usuario externo a la comunicación la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK, Frequency Shift Keying, y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps bajo condiciones de operación óptimas.

La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo, además de que permite un diseño de radio simple, pero como desventaja la velocidad esta limitada a un máximo de 2Mbps. Esta limitación viene impuesta principalmente por regulaciones de la FCC, que restringe los canales a un ancho de banda máximo de 1 MHz. Estas regulaciones obligan al sistema FHSS a usar la banda 2.4GHz por completo, con lo que deben saltar a menudo, lo que conlleva una gran carga de overhead para los saltos.

En la figura 2.7 se muestra el formato de las tramas PLCP. El comienzo es un preámbulo de 80 bits donde se utiliza el patrón de sincronización 0101 que emplea el receptor para detectar la presencia de una señal y conseguir la temporizacion de los símbolos. El preámbulo finaliza con el delimitador de comienzo de trama de 16 bits 0000 1100 1011 1101. La cabecera PLCP consiste en un indicador de longitud de PDU_PLCP de 12 bits, lo que permite una longitud máxima de 4.095 bytes.

La cabecera PLCP consta también de un campo de cuatro bits, de los que los tres primeros están reservados y el último indica operación a 1 Mbps o a 2 Mbps. Los ultimos 16 bits de la cabecera PLCP corresponden a un CRC.

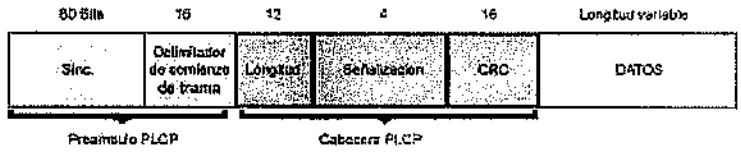


Figura 2.7 Formato de trama en FHSS.

2.2.1.2.3 OFDM (Wideband Orthogonal Frequency Division Multiplexing).

Esta es la técnica utilizada por el estándar 802.11a. Multiplexa la información en múltiples radio frecuencias simultáneamente, es decir, parte una señal (portadora) de alta velocidad en decenas o centenas de señales de menor velocidad que son transmitidas en paralelo (subportadoras).

En la figura 2.8 podemos ver que cada portadora tiene un ancho de banda de 20 MHz y es dividido en 52 subcanales siendo cada uno de 300 KHz aproximadamente de ancho.

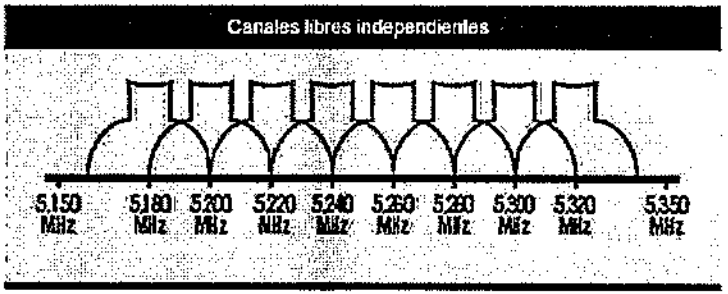


Figura 2.8 Canales del código OFDM

De estos canales, el COFDM (código OFDM) usa 48 para datos y los 4 restantes se usan para la corrección de errores.

En cuanto al tipo de modulación que se emplea es:

- **BPSK** es usado para la modulación a 125 Kbps de datos por canal, es decir, una tasa de datos de 6 Mbps.

- **Con QPSK** se dobla la cantidad de datos modulados produciendo una tasa de datos de 12 Mbps.

- **Usando 16-QAM** (16 level quadrature amplitude modulation) se logra una tasa de datos de 24 Mbps (modulando 4 bits por hetz).

- **Mediante 64-QAM** se obtiene una tasa de datos de 54 Mbps (produce 8 bits por ciclo o 10 bits por ciclo).

OFDM es tolerante al ruido y la señal que se transmite es difícil de descifrar. Los equipos con tecnología OFDM son una buena solución en distancias moderadas para redes de información punto a punto, multipunto, acceso de alta velocidad a Internet, videoconferencia, telefonía, etc.

2.2.2 La capa de acceso al medio (MAC).

Los diferentes métodos de acceso de IEEE 802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel de enlace de datos.

Además, la capa de gestión MAC controlará aspectos como sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura.

2.2.2.1 Descripción funcional MAC.

El protocolo MAC IEEE 802.11 se especifica en términos de función de coordinación que determinan cuando una estación en un BSS puede transmitir y cuando puede recibir unidades de datos de protocolo (PDU) a través del medio inalámbrico, se compone de dos funcionalidades básicas, las cuales se muestran en la figura 2.9.La función de coordinación distribuida, DFC (*Distributed Coordination Funcional*), permite la transmisión de datos asíncronos de PDU MAC de acuerdo con el método de mejor esfuerzo. Con DFC, el medio de transmisión opera exclusivamente en el modo de contención, lo que requiere que todas las estaciones luchen por conseguir el canal para cada paquete a transmitir. IEEE define también una función de coordinación puntual, PFC (*Point Coordination Funtion*), que se implementa mediante un punto de acceso, para permitir la transmisión orientada a conexión de PDU MAC dentro de un intervalo de tiempo máximo. Con PCF, el medio puede alternar entre el periodo de contención, CP (*Contention Period*), durante el cual el medio está en modo de contención, y un periodo libre de contención, CFP (*Contention Free Period*). Durante CFP la utilización del medio esta controlada por el punto de acceso, con lo que elimina la necesidad de que las estaciones luchen por conseguir el acceso al canal.

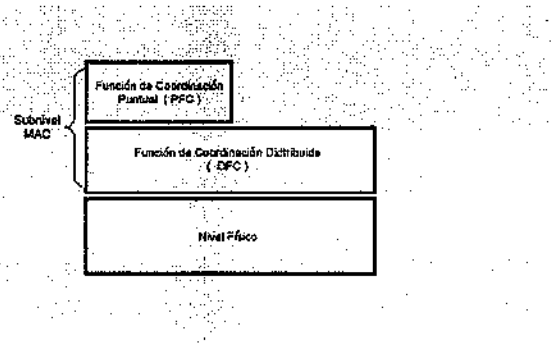


Figura 2.9 Subcapas PCF y DFC del subnivel MAC

2.2.2.1.1 Función de Coordinación Distribuida (DFC).

Definimos *función de coordinación* como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.

El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Las características de DFC las podemos resumir en estos puntos:

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio
- Necesario reconocimientos ACKs, provocando retransmisiones si no se recibe
- Usa campo Duration/ID que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre

- Implementa fragmentación de datos
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS)
- Soporta Broadcast y Multicast sin ACKs

Protocolo de acceso al medio CSMA/CA y MACA.

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es conocido como CSMA/CA (Carrier Sense Multiple Access with Collision Advoidance).

El protocolo CSMA/CA funciona de la siguiente manera:

1.- Cuando una estación desea transmitir información debe escuchar el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

2.- Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).

3.- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transmisión actual antes de realizar cualquier acción.

4.- Una vez finaliza esta espera la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado *ventana de contienda* (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5.- Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición. Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es 20μseg.

En la anterior figura 2.10 podemos ver un ejemplo del funcionamiento de acceso CSMA/CA.

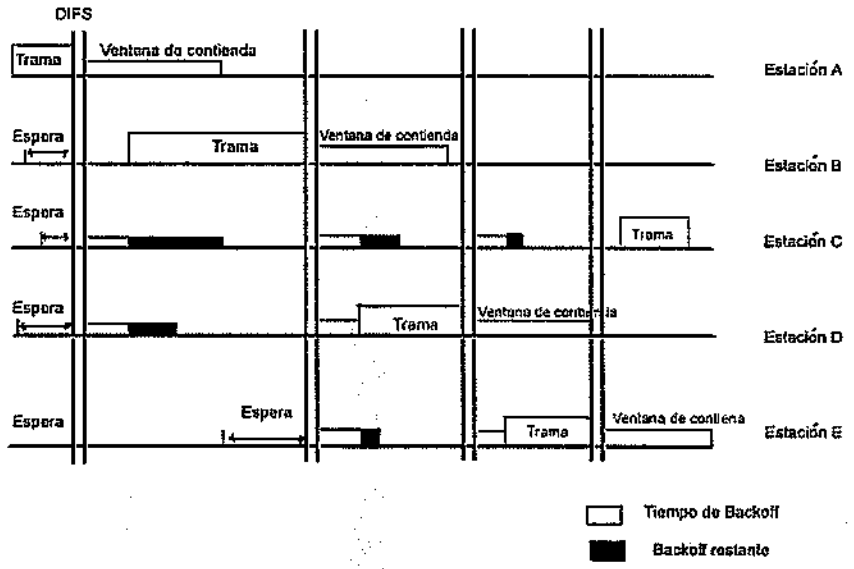


Figura 2.10 Acceso al Medio CSMA/CA

Sin embargo, CSMA/CA en un entorno inalámbrico presenta una serie de problemas. Los dos principales problemas son:

- Nodos ocultos. Una estación cree que el medio está libre, pero en realidad está ocupado por otro nodo que no oye.

- Nodos expuestos. Una estación cree que el medio está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone el estándar 802.11 es MACA o MultiAccess Collision Avoidance.

Según este protocolo, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS

- Al escuchar un CTS, hay que esperar según la longitud

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

Espaciado entre tramas IFS.

En la figura 2.11 se puede ver el tiempo de espacio entre tramas IFS. Durante este periodo mínimo, una estación estará escuchando el medio antes de transmitir. Se definen cuatro espacios para dar prioridad de acceso al medio inalámbrico.

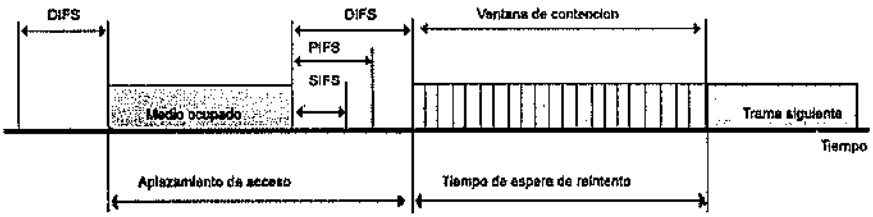


Figura 2.11 Espacio entre tramas IFS

• SIFS (Short IFS). Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama. Por último, es usado por el punto de coordinación o PC para enviar testigo a estaciones que quieran transmitir datos síncronos

• PIFS (PCF). Es utilizado por STAs para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.

• DIFS (DCF). Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza pues para el envío de tramas MAC MPDUs y tramas de gestión MMPDUs.

• EIFS (Extended IFS). Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

Conocimiento del medio.

Las estaciones tienen un conocimiento específico de cuando la estación, que en estos momentos tiene el control del medio porque está transmitiendo o recibiendo, va a finalizar su periodo de reserva del medio.

Esto se hace a través de una variable llamada NAV (Network Allocation Vector) que mantendrá una predicción de cuando el medio quedará liberado.

En la figura 2.12 se muestra el mecanismo de transmisión de MPDU mediante el mecanismo RTS/CTS. Tanto al enviar un RTS como al recibir un CTS, se envía el campo Duration/ID con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo Duration/ID. En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.

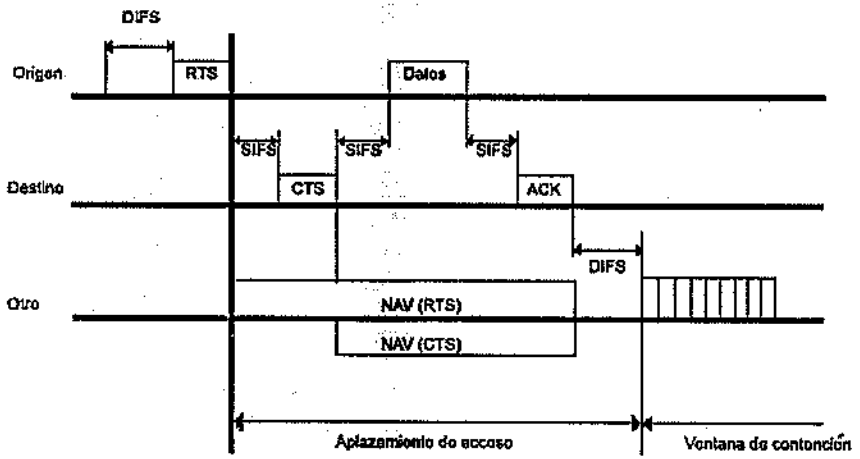


Figura 2.12 Transmisión de MPU con RTS/CTS

2.2.2.1.2 Función de Coordinación Puntual (PFC).

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual, PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, en concreto, define una técnica de interrogación circular desde el punto de acceso para este nivel. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio.

Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o en un conjunto básico de servicios dentro de una estructura llamada *supertrama*. Un parte de esta *supertrama* se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios.

Una vez finaliza este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.

Un aspecto previo a comentar el funcionamiento de PFC es que es totalmente compatible con el modo DFC, observándose que el funcionamiento es transparente para las estaciones. De esta manera, una estación se asociará (se dará de alta en un modo infraestrucutra) de modo que pueda actuar en el periodo CFP, declarándose como CFPollable, o por el contrario, se situará su NAV según las indicaciones del punto de coordinación.

Existe un nodo organizador o director, llamado punto de coordinación o PC. Este nodo tomará el control mediante el método PIFS, y enviará un CF-Poll a cada estación que pueda transmitir en CFP, concediéndole poder transmitir una trama MPDU. El PC mantendrá una lista Pollable donde tendrá todos los datos de las estaciones que se han asociado al modo CF-Pollable. La concesión de transmisiones será por riguroso listado y no permitirá que se envíen dos tramas hasta que la lista se haya completado.

El nodo utilizará una trama para la configuración de la supertrama, llamada Beacon, donde establecerá una CFRate o tasa de periodos de contienda. Pese a que el periodo de contienda se puede retrasar por estar el medio ocupado, la tasa se mantendrá en el siguiente periodo con medio libre.

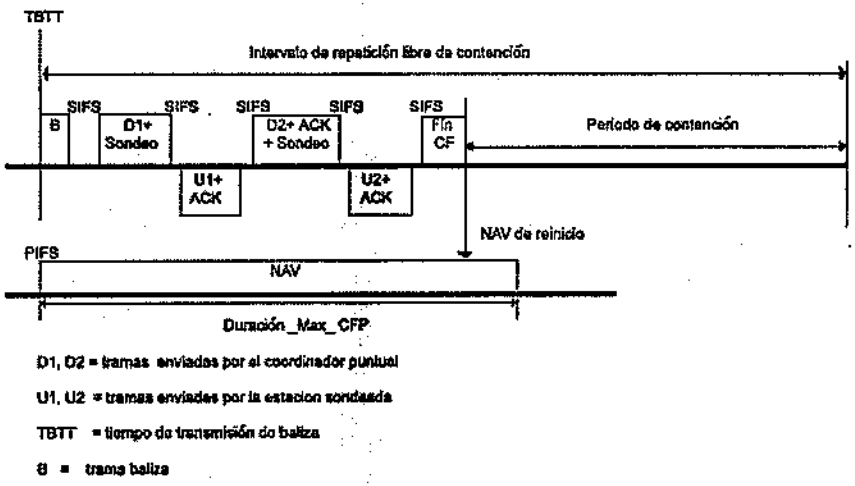


Figura 2.14 Transmisión de tramas mediante coordinación puntual.

Como podemos observar en al figura 2.14, la transmisión de CF-Polls espera un tiempo SIFS. También podemos ver que si una estación no aprovecha su CF-Poll se transmite a la siguiente en el listado Pollable.

Las estaciones que no usen el CF, situarán su NAV al valor del final del CF y luego lo resetearán para poder modificarlo en el periodo de contienda en igualdad de condiciones.

2.2.2.2 Formato de las tramas MAC.

Las tramas MAC contienen los siguientes componentes básicos:

• Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia

• Un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama

• Una secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits

Las tramas MAC se pueden clasificar según tres tipos:

1. Tramas de datos.

2. Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda

3. Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

El formato de la trama MAC genérica se muestra en la figura 2.15 y tiene el siguiente aspecto:

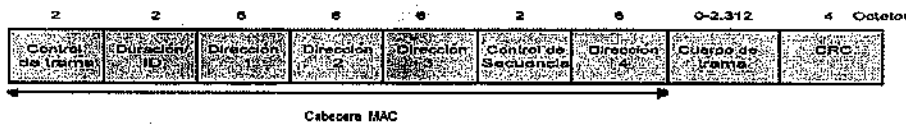


Figura 2.15 Formato de trama MAC

Los campos que componen esta trama son:

- **Campo de control**. El cual se examinará a detalle más adelante.

- **Duration/ID.** En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.

- **Campos address1-4.** Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- **Campo de control de secuencia.** Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.

- **Cuerpo de la trama.** Varía según el tipo de trama que se quiere enviar.

- **FCS.** Contiene el checksum.

Los campos de control de trama se muestran en la figura 2.16 y tienen el formato siguiente:

Figura 2.16 Campos de control de trama

Versión: La versión del protocolo 802.11 (La actual es la 0)

Tipo: El tipo de trama identifica si es de gestión (00), de control (01) o de datos (10).

Subtipo: El campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos; por ejemplo, tipo = gestión y subtipo solicitud de asociación o tipo = control y subtipo ACK

Hacia DS: El campo hacia DS se especifica a 1 para las tramas de datos dirigidas al sistema de distribución, incluso para aquellas procedentes de una estación asociada a un punto de acceso con dirección de difusión o multidestino.

De DS: El campo de DS toma el valor 1 en las tramas de datos que salen del sistema de distribución.

En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución.

Más fragmentos: Se activa si se usa fragmentación.

Retransmisión: Se activa si la trama es una retransmisión solo en tramas de tipo datos o gestión.

Control de potencia: Se activa si la estación utiliza el modo de economía de potencia.

Más datos: Se activa si la estación tiene tramas pendientes en un punto de acceso.

WEP. Se activa si se usa el mecanismo de autenticación y cifrado.

2.3 Tecnología de infrarrojos.

La verdad es que IEEE 802.11 no ha desarrollado todavía en profundidad esta área y solo se mencionara las características principales:

- Entornos muy localizados, un aula concreta, un laboratorio, un edificio.
- Modulaciones de16-PPM y 4-PPM que permiten 1 y 2 Mbps de transmisión.
- Longitudes de onda de 850 a 950 manómetros de rango.
- Frecuencias de emisión entre $3{,}15 \cdot 10e^{14}$ Hz y $3{,}52 \cdot 10e^{14}$ Hz.

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

Para describir esta capa física seguiremos las especificaciones del IrDA5 organismo que ha estado desarrollando estándares para conexiones basadas en infrarrojos.

2.3.1 Clasificación.

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

2.3.1.1 Sistemas de corta apertura.

Los sistemas infrarrojos de corta apertura, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los controles remotos de las televisiones: el emisor debe orientarse hacia el receptor antes de empezar a transferir información, limitando por tanto su funcionalidad. Resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que está más orientado a la portabilidad que a la movilidad.

2.3.1.2 Sistemas de corta apertura.

Los sistemas de gran apertura permiten recibir la información en un ángulo mucho más amplio por lo que el transmisor no tiene que estar directamente alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos. La dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor). Esta es una de las dificultades que han retrasado el desarrollo del sistema infrarrojo en la norma 802.11.

2.3.2 Capas y protocolos.

El principio de funcionamiento en la capa física es muy simple y proviene del ámbito de las comunicaciones ópticas por cable: un LED (Light Emitting Diode), que constituye el dispositivo emisor, emite luz que se propaga en el espacio libre en lugar de hacerlo en una fibra óptica, como ocurre en una red cableada. En el otro extremo, el receptor, un fotodiodo PIN recibe los pulsos de luz y los convierte en señales eléctricas que, tras su manipulación (amplificación, conversión a formato bit -mediante un comparador- y retemporización) pasan a la UART (Universal Asynchronous Receiver Transmitter) del ordenador, de forma que para la CPU todo el proceso luminoso es absolutamente transparente, como se muestra en la figura 2.17. En el proceso de transmisión los bits viajan mediante haces de pulsos, donde el cero lógico se representa por existencia de luz y el uno lógico por su ausencia. Debido a que el enlace es punto a punto, el cono de apertura visual es de 30° y la transmisión es half duplex, esto es, cada extremo del enlace emite por separado.

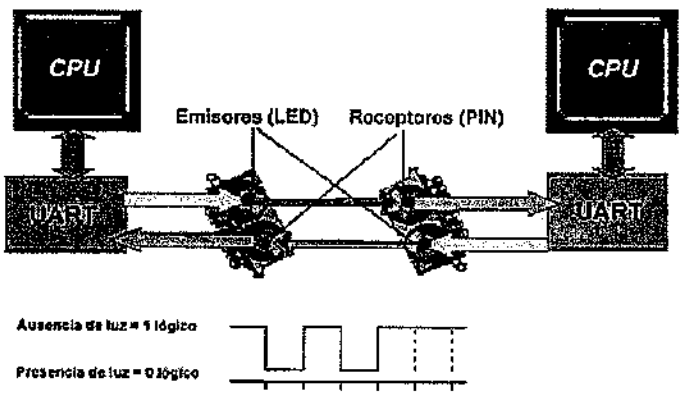


Figura 2.17 Dispositivos necesarios para una transmisión

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

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

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

En este capítulo se observaron las diferentes tecnologías de espectro ensanchado e infrarrojo, estándares que se utilizan en las redes inalámbricas actuales, así como la capa de acceso al medio MAC y la física las cuales que hacen posible la comunicación inalámbrica, dando pie al tercer capítulo: Seguridad en el estándar IEEE 802.11.

Capítulo 3

Seguridad en el estándar IEEE 802.11

3.1 Retos de seguridad.

Resulta evidente que las comunicaciones inalámbricas ofrecen un punto de vulnerabilidad en la transmisión de datos, puesto que las emisiones difícilmente pueden acotarse a la zona de cobertura, sino que habitualmente suelen alcanzar puntos fuera del área de transmisión deseada. Para evitar que otros receptores ajenos a la red inalámbrica puedan hacer un uso indebido de la información que viaje por el aire se ha adoptado un mecanismo de control de acceso al medio, lo cual evita en gran medida las escuchas indiscretas. No obstante, este sistema no es suficiente, por lo que opcionalmente se puede realizar un proceso de cifrado de los datos que se transmiten por la red inalámbrica.

A la hora de proteger la información que viaja por el espacio mediante sistemas de cifrado se puede hacer uso de las técnicas como WEP-40 y WEP-104. Estos dos sistemas son funciones opcionales de la especificación IEEE 802.11 que proporcionan una seguridad equivalente a la de una red LAN cableada.

3.2 Mecanismos de seguridad.

3.2.1 Protocolo equivalente al cableado WEP (Wired Equivalent Protocol).

Las redes inalámbricas (WLANs) son más inseguras que las redes cableadas, ya que el medio físico utilizado para la transmisión de datos son las ondas de radio. Para proteger los datos que se envían a través de las redes inalámbricas, el estándar 802.11b define el uso del protocolo WEP (Wired Equivalent Privacy). WEP intenta proveer de la seguridad de una red cableada a una red inalámbrica, cifrado los datos que viajan sobre las ondas de radio en la capa MAC.

3.2.1.1- Como funciona WEP.

WEP utiliza el algoritmo RC4 para el cifrado con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros 24 van en el paquete como Vector de Inicialización (IV).

3.2.1.2.- Llaves.

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática.

La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red inalámbrica que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

En la figura 3.1 se muestra el proceso que se realiza para generar las llaves:

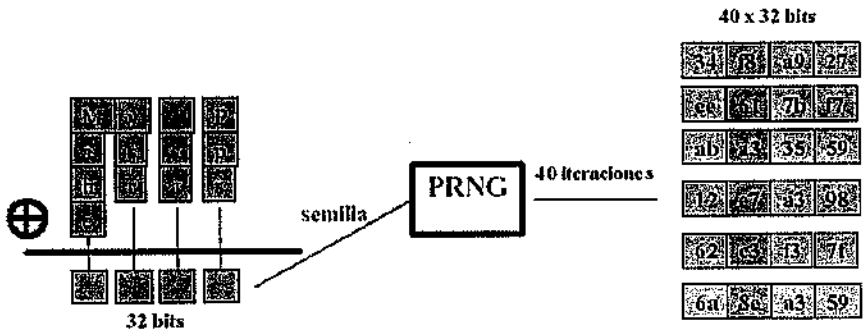


Figura 3.1 Proceso de generación de llaves

Se hace una operación XOR con la cadena ASCII (My Passphrase) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una.

Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits.

De estas 4 llaves sólo se utilizará una para realizar el cifrado WEP como veremos a continuación.

3.2.1.3 Cifrado.

Para generar una trama cifrada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como valor de chequeo de integridad (ICV: Integrity Check Value). Ver figura 3.2

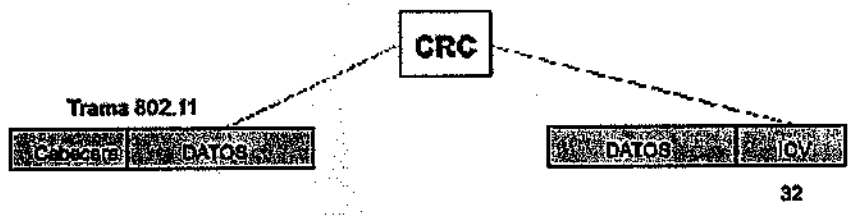


Figura 3.2 Trama 802.11 y calculo del CRC

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles, ver figura 3.3:

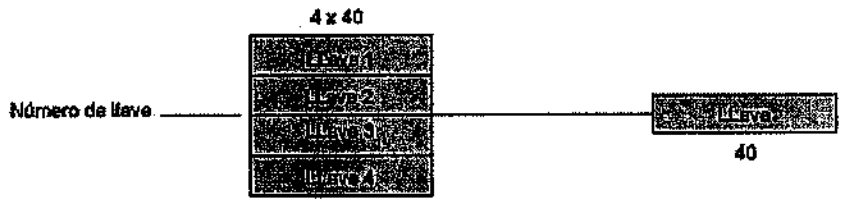


Figura 3.3 Selección de la llave de 40 bits

Y en la figura 3.4 podemos ver como añadimos el vector de inicialización (IV) de 24 bits al principio de la llave seleccionada:

Figura 3.4 Vector de inicialización + llave de 40 bits

El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para cifrar la trama. En el caso de utilizar cifrado de 128 bits tendríamos 24 bits de IV y 104 de llave.

Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el keystream o flujo de llave, como lo podemos observar en la figura 3.5. Realizando una operación XOR con este keystream y el Payload+ICV obtendremos el Payload+ICV cifrado.

Se utiliza el IV y la llave para cifrar el Payload + ICV:

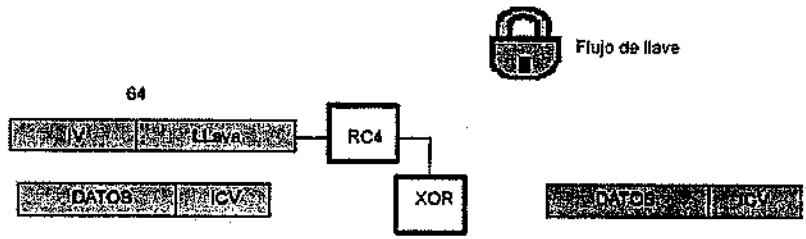


Figura 3.5 Aplicación del algoritmo RC4.

Después añadimos la cabecera y el IV+Keynumber sin cifrar. En la figura 3.6 se muestra como queda la trama definitiva lista para ser enviada:

Figura 3.6 Trama cifrada con WEP

3.2.1.4 Descifrado.

Ahora vamos a ver el proceso que se realiza para el descifrado de una trama cifrada con WEP:

Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama, ver figura 3.7:

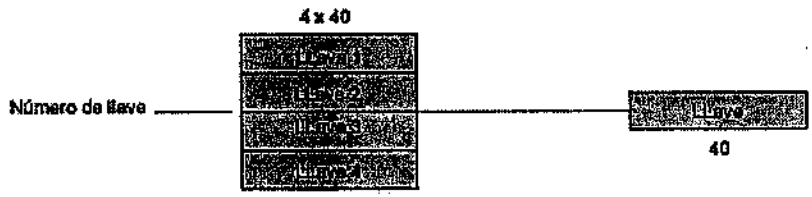


Figura 3.7 Selección de la llave de 40 bits

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación en la figura 3.8.

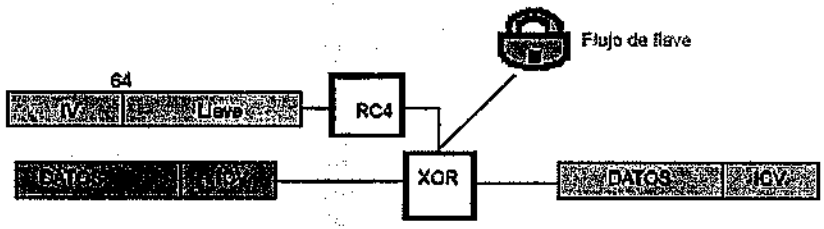


Figura 3.8 Proceso de descifrado.

Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original.

Esta es la forma de funcionamiento del sistema de seguridad de las redes inalámbricas, ampliamente criticado por muchos expertos. Entre sus principales puntos débiles frecuentemente se señalan los siguientes:

3.2.1.5 Vulnerabilidades.

- **Características lineales de CRC32**
- **MIC independiente de la llave**
- **Tamaño de IV demasiado cortó.**

3.2.1.5.1 Características lineales de CRC32

Esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Ian Goldberg y David Wagner (Universidad de Berkeley).

Como hemos visto anteriormente, el campo ICV (Integrity Check Value) de una trama cifrada con WEP contiene un valor utilizado para verificar la integridad del mensaje.

Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV.
- Los CRCs son lineares.

Debido a que los CRCs son lineales, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es lineal y esto permite hacer el 'bit flipping' como se describe en la figura 3.9.

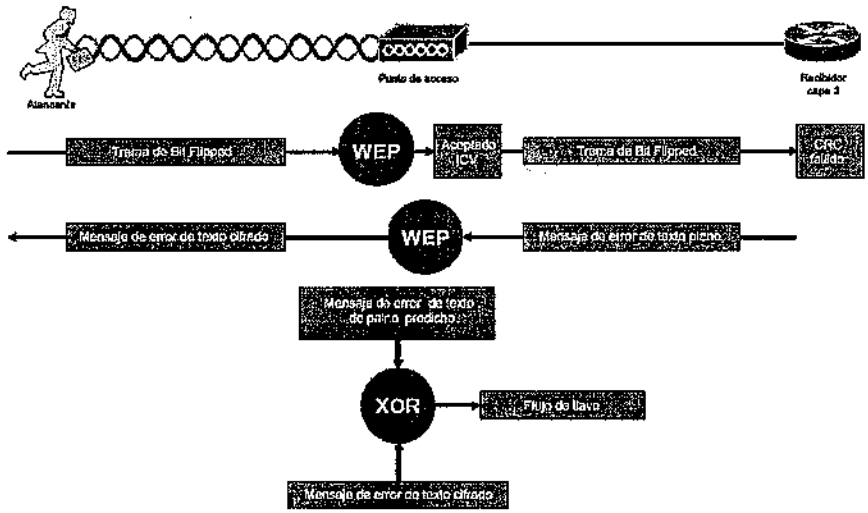


Figura 3.9 Vulnerabilidad del CRC

3.2.1.5.2 MIC independiente de la llave

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de Berkeley).

Esta vulnerabilidad en WEP es conocida en inglés como "Lack of keyed MIC" Ausencia de mecanismo de chequeo de integridad del mensaje (MIC) dependiente de la llave.

El MIC que utiliza WEP es un simple CRC-32 calculado a partir del payload, por lo tanto no depende de la llave ni del IV.

Esta debilidad en el cifrado da lugar a que conocido el plaintext de un solo paquete cifrado con WEP sea posible inyectar paquetes a la red.

3.2.1.5.3 Tamaño del vector de inicialización (IV) demasiado cortó.

Otra de las deficiencias del protocolo viene dada por la corta longitud del campo IV en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin cifrar).

La corta longitud del IV, hace que éste se repita frecuentemente y de lugar a la deficiencia del protocolo, basada en la posibilidad de realizar ataques estadísticos para recuperar el plaintext gracias a la reutilización del IV.

3.2.2 Autenticación abierta OSA (Open System Authentication).

Es el protocolo de autenticación por defecto definido para las redes 802.11. En la figura 3.10 se muestra el proceso de todos los clientes que inician la autenticación ante un punto de acceso son registrados en la red. Ambos, envían en texto plano todas las tramas (management frames), incluso cuando el WEP está activado.

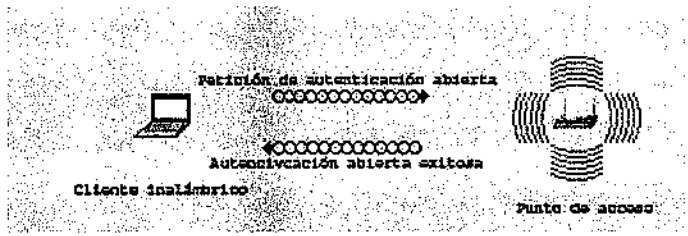


Figura 3.10 Proceso de autenticación abierta

Vulnerabilidades.

El propio sistema es una vulnerabilidad en sí mismo, absolutamente todos los clientes que piden ser autenticados en la red lo son.

3.2.3 Listas de control de acceso ACL (Access Control List).

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que estén en la lista de control de acceso del punto de acceso previamente configuradas.

Vulnerabilidades.

Las direcciones físicas viajan en texto plano y con un analizador de red, se pueden capturar las direcciones permitidas por dicho AP. Modificando la NIC (Network Interface Card), un intruso puede acceder a dicha red.

3.2.4 Control de acceso a la red cerrada CNAC (Closed Network Access Control).

En la figura 3.11 se muestra el mecanismo de control de acceso a la red cerrada que pretende controlar el acceso a la red inalámbrica y permitir solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

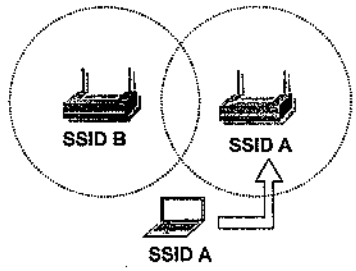


Figura 3.11 Proceso de control de acceso a la red cerrada.

Vulnerabilidades.

Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca
- No se proporciona ningún tipo de cifrado a través de este esquema
- Además cada fabricante establece valores por defecto que no son modificados por administradores inexpertos.

3.2.5 Autenticación de llave compartida SKA (Shared Key Authentication).

Se basa en un desafío cliente – punto de acceso, en donde ambos comparten una llave secreta para iniciar dicha autenticación, siendo el cliente el dispositivo móvil que desea ser autentificado y el punto de acceso el que recibirá dicha petición.

El proceso de autenticación de llave compartida se puede ver la figura 3.12, donde el cliente envía una trama (management frame) indicando que el método a usar es de llave compartida. Al recibir el punto de acceso esta trama, enviará una nueva con los 128 Bytes de texto para ser usado como desafío.

El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio.

Una vez recibida esta segunda trama por el cliente, se copia el contenido del desafío en el cuerpo de una nueva trama, que a su vez es cifrada con WEP usando la llave compartida más un nuevo vector de inicialización (esta vez es elegido por el cliente). Una vez realizado todo esto se envía al responder.

El punto de acceso al recibir esta trama procede a:

a. Descifrarla.
b. Comprobar si el CRC es válido.
c. Verificar la validez del desafío.

Si la comprobación es correcta, se produce la autenticación del cliente con el punto de acceso y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con la petición de autenticación es el punto de acceso. De esta manera se asegura una autenticación mutua.

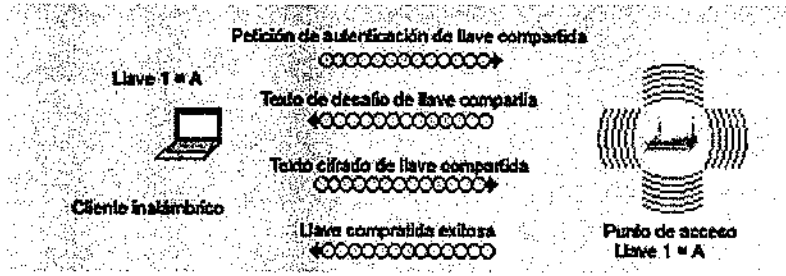


Figura 3.12 Proceso de autenticación de llave compartida

Vulnerabilidades.

Mediante un analizador de red, es fácil obtener los datos necesarios para recrear tramas válidas y engañar al punto de acceso al que se desea conectar. Capturando el segundo mensaje, obtendríamos el texto desafío aleatorio en texto plano y con el tercer mensaje el mismo texto pero ya cifrado y el vector de inicialización, como se muestra en la figura 3.13.

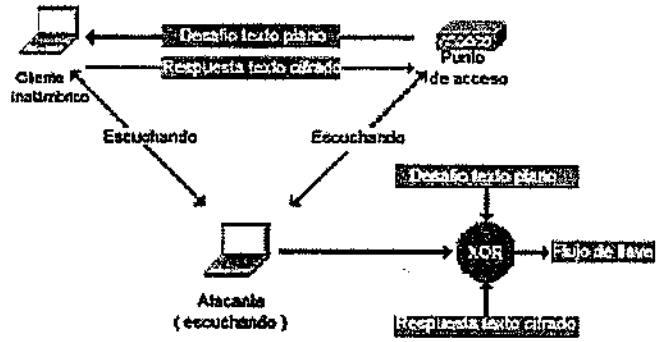


Figura 3.13 Vulnerabilidad de la llave compartida.

3.3 Nuevas tecnologías para seguridad de redes inalámbricas.

3.3.1 Wi-Fi Protected Access (WPA).

Wi-Fi Protected Access (WPA), una nueva solución para seguridad de red inalámbrica basada en estándares de la Wi-Fi Alliance. La nueva solución pretende reemplazar el estándar Wired Equivalent Privacy (WEP) y ofrece métodos robustos de cifrado de datos y autenticación de red.

El procedimiento "Wi-Fi Protected Access" o WPA ha sido anunciado por Wi-Fi Alliance para los primeros meses de 2003 con el fin de sustituir a WEP. WPA necesita una clave maestra por cada usuario. Esta clave maestra es una contraseña que WPA utiliza para generar una clave para cifrar el tráfico de la red y esta clave de cifrado es generada automáticamente usando la clave maestra cada vez que se produce una transmisión, lo que aumenta sensiblemente la seguridad. WPA ha sido diseñada como una mejora de WEP por lo que la mayoría de los dispositivos inalámbricos podrán ser actualizados a esta nueva tecnología.

La autenticación se basa en el estándar 802.1x que define un protocolo de autenticación por puerto, considerando cada frecuencia de radio como un puerto en el caso de las redes inalámbricas.

El salto de calidad que supone el WPA con respecto al WEP lo da el uso del protocolo TKIP (Temporal Key Integrity Protocol) para la criptografía de los datos y por el protocolo EAP (Extensible Authentication Protocol) para la autentificación del usuario, función totalmente ausente en el WEP.

El EAP permitirá el acceso a la red sólo a los usuarios autorizados, que tendrán que mostrar sus propias credenciales para acceder a la obtención de una clave que permita, a su vez, el acceso a la susodicha red. Una vez obtenido el acceso a la comunicación, el WPA prevé la posibilidad de "mezclar" las claves introducidas en cada paquete de datos con un control de la integridad del mensaje (MIC), así como un mecanismo para la reasignación de claves de autentificación.

El WPA está basado en un estándar futuro, todavía no disponible, denominado IEEE 802.11i que, en teoría, no tendrá las debilidades estructurales del actual 802.11b.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

3.3.1.1 WPA en modo empresarial.

Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

3.3.1.2 WPA PSK.

Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

En la tabla 3.1 se muestra una comparación de WEP contra WPA

	WEP	WPA
Cifrado	Vulnerable por hackers	Corrige todas las debilidades de WEP
	Llave de 40 y 104 bits	Llaves de 128 bits
	Utilización de la misma llave estática	Utilización de llaves dinamicas por usuario, sesión y por paquetes
	Distribución manual de la llave	Distribución automática de llaves
Autenticación	Debilidad, ya que WEP es usado como mecanismo de autenticación	Fuerte autenticación por usuario, utilización de 802.1x y EAP

Tabla 3.1 Diferencias WEP vs WPA

3.3.2 Protocolo de llaves integras seguras temporales TKIP (Temporal Key Integrity Protocol).

Con este protocolo se pretende resolver las deficiencias de WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del firmware.

El protocolo TKIP esta compuesto por los siguientes elementos:

Un código de integración de mensajes (MIC), cifrada el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11.

Contramedidas para reducir la posibilidad de que un atacante pueda aprender o utilizar una determinada llave.

Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación. Para hacer frente a este problema se creó específicamente el estándar 802.1x.

3.3.3 802.1x.

Este estándar inicialmente se pensó para proporcionar seguridad mediante el control de acceso a los puertos de una red tradicional, pero ha demostrado ser más útil en entornos de redes inalámbricos. La idea básica es que cuando un dispositivo intenta conectarse a un punto de acceso, este le pide algún tipo de credenciales que reenvía a un servidor de autenticación para que se le indique si debe autorizar o no a dicho dispositivo a acceder a la red inalámbrica.

3.3.3.1 Modo de operación.

El estándar IEEE 802.1X se basa en el concepto de puerto para proporcionar control de acceso. Estos puertos son los puntos a través de los cuales se puede acceder a los servicios proporcionados por el punto de acceso Un control de acceso basado en puertos permite que el uso de un puerto del sistema sea controlado para asegurar que únicamente los clientes autorizados puedan hacer uso de los servicios disponibles a través de dicho puerto.

El protocolo 802.1x involucra tres participantes ver figura3.14.

- **Una estación cliente.**
- **Un Punto de Acceso.**
- **Un servidor de autenticación (AS).**

En este nuevo elemento, el servidor de autenticación, es el que realiza la autenticación real de las credenciales proporcionadas por el cliente. El servidor de autenticación es una entidad separada situada en la zona cableada (red clásica), pero también implementable en un punto de acceso. El tipo de servidor utilizado podría ser RADIUS, u otro tipo de servidor.

El estándar 802.1x introduce un nuevo concepto, el concepto de puerto habilitado/inhabilitado en el cual hasta que el cliente no se valide en el servidor no tiene acceso a la red.

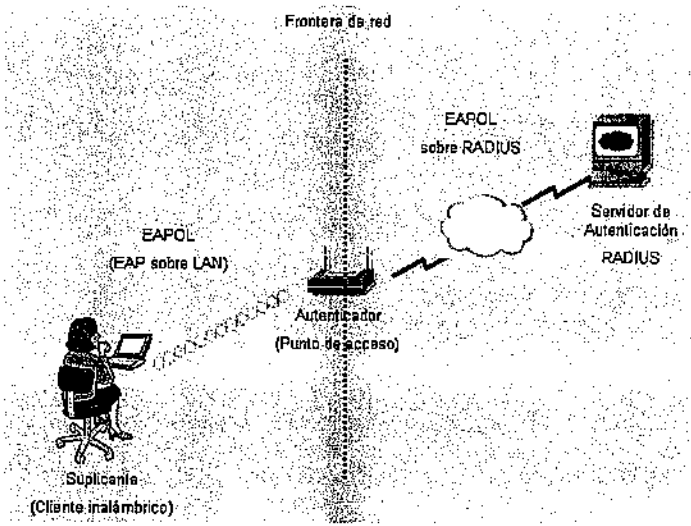


Figura 3.14 Arquitectura de un sistema de autenticación 802.1x.

3.3.3.2 Protocolo de autenticación extensible sobre una red de área local EAPOL (Extensible Authentication Protocol Over LAN).

EAPOL es un protocolo sencillo utilizado para transmitir paquetes entre el cliente y el punto de acceso en una red inalámbrica. Este protocolo, generalmente, es iniciado por el punto de acceso cuando detecta que un nuevo cliente se ha conectado, aunque también puede ser iniciado por el cliente.

Este protocolo define la forma en que los paquetes EAP (Extensible Authentication Protocol), se transmitan entre el cliente y el punto de acceso.

3.3.2.3 Protocolo de autenticación extensible EAP (Extensible Authentication Protocol).

El Protocolo de Autenticación Extensible (EAP) es un protocolo general originalmente creado para realizar autenticación sobre enlaces PPP, soportando varios mecanismos de autenticación en la figura 3.14 se puede ver el esquema de ubicación del protocolo. Este protocolo es una extensión del protocolo punto a punto (PPP).

EAP se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto mediante otros dispositivos de seguridad.

EAP se encuentra dentro del protocolo de autenticación PPP y proporciona un marco general compatible con diversos métodos de autenticación. EAP está diseñado para disuadir a los usuarios de la implementación de sistemas de autenticación propietarios y permitir desde las contraseñas hasta los certificados de clave pública. Con el estándar EAP, la interoperatividad y la compatibilidad de los métodos de autenticación pasa a ser una tarea de lo más simple.

El estándar IEEE 802.1x se trata de una norma para pasar EAP por una LAN cableada o inalámbrica. Con 802.1x, el usuario empaqueta los mensajes EAP en tramas Ethernet sin tener que recurrir a PPP. Se trata de autenticación y nada más.

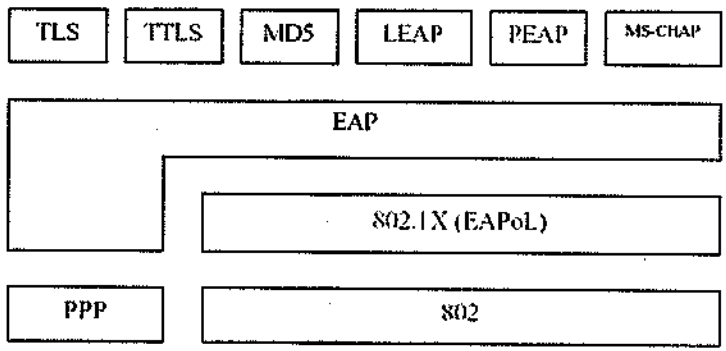


Figura 3.14 Esquema de ubicación del protocolo EAP.

El esquema básico de funcionamiento del protocolo es el siguiente:

1) Después de terminar la fase de establecimiento de enlace, el autenticador envía una o más solicitudes para autentificar al cliente. La solicitud tiene un campo de "tipo" para indicar qué se está solicitando. No siempre es necesario una solicitud inicial de identidad, en algunos casos se puede presuponer (e.g. Líneas dedicadas).

2) El cliente envía un paquete de respuesta para cada solicitud recibida. Como con el paquete de solicitud, el paquete de respuesta contiene un campo de "tipo" que se corresponde con el campo de "tipo" de la solicitud.

3) El autenticador termina la fase de autentificación con un paquete de éxito o fallo según el caso.

3.3.2.3.1 Protocolos de autenticación sobre EAP.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas. Las variantes de EAP que emplean certificados de seguridad son las siguientes:

EAP-TLS (EAP - Transport Level Security).

Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

EAP-TTLS (EAP - Tunneled TLS).

Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.

PEAP (Protected Extensible Authentication Protocol).

Protocolo desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador. El empleo de certificados permite una autenticación fuerte entre cliente y servidor.

Las variantes de EAP que utilizan contraseñas son las siguientes:

EAP-MD5.

EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

Es el más sencillo de implementar.

LEAP (Lightweight Extensible Authentication Protocol).

Implementación de EAP propietaria de CISCO. Emplea un esquema de nombre de usuario y contraseña. Con LEAP es necesaria una autenticación mutua tanto del cliente como del servidor (típicamente un servidor RADIUS). Se utiliza claves privadas compartidas para construir los mensajes intercambiados. También permite utilizar claves WEP dinámicas por usuario o sesión. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

MS-CHAP.

Protocolo de Microsoft de autenticación por desafío mutuo. Es conocido también como MSCHAPv1.

Proceso de desafío mutuo:

1.- El autenticador envía al cliente un identificador de sesión y una cadena de desafío arbitraria.

2.- El cliente envía como respuesta el nombre de usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.

3.- El autenticador comprueba la respuesta y, si es válida, se autentican las credenciales del usuario.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada.
- La llave de encriptación principal es única para cada estación, por lo tanto, el trafico de esta llave es reducido (no se repite en otros clientes).
- Existe una generación dinámica de llaves por parte del AS, sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

Con las mejoras a los mecanismos de seguridad en las redes inalámbricas termino este capítulo, entendiendo los diferentes mecanismos de seguridad y vulnerabilidades que en este tipo de redes se presentan, dando pie ahora al capítulo cuarto: Propuesta de la red inalámbrica.

Capítulo 4

Propuesta de la red inalámbrica

4.1 ANTECEDENTES.

La Dirección General de Servicios de Cómputo Académico de C.U. es la entidad universitaria encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la institución; brinda servicios educativos de redes, Internet, supercómputo, seguridad, telefonía, visualización, animación por computadora, diagnóstico, auditoria, diseño y programación de sistemas, que se basan en una infraestructura actualizada de cómputo.

La Dirección General de Servicios de Cómputo Académico actualmente cuenta con una infraestructura de red de comunicaciones cuyas principales características son:

- Forma parte del Backbone de GigabitEtherner de la RedUNAM.
- El protocolo de transporte empleado es GigabitEtherner y FastEthernet.
- El acceso y distribución al Backbone de la RedUNAM es en 1000BaseSX y 100BaseFX.
- El protocolo de red principalmente empleado es IP.

Los servicios que brinda la Dirección General Servicios de Cómputo Académico, en específico la Dirección de Telecomunicaciones conformada por los siguientes departamentos son:

Departamento de redes.

El departamento de redes, compuesto por cinco áreas que son NOC, TAC, NIC, administración de servidores y telefonía descritos a continuación:

Centro de Operación de la Red (NOC).

El NOC (Network Operation Center) o Centro de Operación de la RedUNAM, es el encargado de mantener funcionando de manera eficiente la interconexión de las redes locales, los enlaces de área amplia y la "Columna Vertebral" o Backbone de la RedUNAM.

Actualmente las actividades más importantes que desarrolla el Centro de Operación de RedUNAM son las siguientes:

- Monitoreo.
- Tarificación.
- Generación de estadísticas.
- Administración de equipos de ruteo.
- Seguimiento de reportes (Troubleshooting).

Centro de Asistencia Técnica (TAC).

El TAC (Tecnical Asistence Center) o Centro de Asistencia Técnica de la RedUNAM tiene como objetivo primordial garantizar el buen funcionamiento de los switches del backbone, switches periféricos y de acceso de la RedUNAM; proporcionando así el servicio a todas las redes LAN de las dependencias distribuidas en los campus Universitario.

De igual manera es el encargado de proporcionar a la comunidad universitaria y a usuarios en general el Servicio de Acceso Remoto también conocido como Servicio Dial-Up, permitiendo realizar una conexión confiable y segura a RedUNAM desde cualquier ubicación geográfica.

Actualmente las actividades más importantes que desarrolla el Centro de Asistencia Técnica de la RedUNAM son las siguientes:

- Monitoreo.
- Generación de estadísticas.
- Administración de equipos de switcheo y de acceso remoto.
- Seguimiento de reportes (Troubleshooting).

Centro de Información de la Red (NIC).

El **NIC** (Network Information Center) o Centro de Información de la RedUNAM se encarga de la administración y del mantenimiento de los servidores de nombres (DNS's) de la RedUNAM.

Actualmente las actividades más importantes que desarrolla el Centro de Información de la RedUNAM son las siguientes:

- Administración de servidores de nombres.
- Monitoreo.
- Asignación de Direcciones IP.
- Asignación y Solicitud de Dominios.

Administración Servidores.

El área de administración de servidores es el responsable de la administración, mantenimiento y actualización de los servidores centrales de la RedUNAM para brindar servicio a la comunidad universitaria.

Los servidores y servicios más importantes a su cargo son:

- Correo electrónico
- Hospedaje de sitios web
- FTP Anónimo.
- Servicio de aviso.

Telefonía.

El área de Telefónica es la encargada de brindar a la Comunidad Universitaria, independientemente de su ubicación geográfica, los servicios de comunicación telefónica y radio-localización personal, a través de los más modernos medios tecnológicos para garantizar la mayor confiabilidad y contribuir en el mejor desempeño de las actividades sustanciales de nuestra Institución.

Diagrama de conexión actual del departamento de redes, conmutación y servidores:

El diagrama muestra como están conectados las diferentes áreas del departamento de redes, en este esquema existe un nodo principal, el cual va conectado al backbone de la RedUNAM, del cual dependen 6 switches y un hub repartidos y ubicados en distintas áreas de la manera siguiente

- Dos switches apilados que dan servicio al área de servidores, uno de estos switches va conectado al switch principal con un enlace de fibra de 100 Mbps y los servicios hacia las pc's y estaciones de trabajo a 10 y 100 Mpbs.

- Un switch y un hub para proporcionar los servicios al área de telefonía. El switch funciona como convertidor de medios, ya que todos los enlaces del switch principal a los switches de distribución son en fibra óptica y el hub que proporciona los servicios, solamente tiene puertos en utp, estos mismos servicios estan a 10 Mbps.

- Tres switches apilados para el área de operación de la red, uno de estos switches va conectado al switch principal con un enlace de fibra de 100 Mbps y los servicios hacia las pc's y estaciones de trabajo a 10 y 100 Mpbs.

Este es el esquema de administración y monitoreo de la RedUNAM, que se puede ver en la figura 4.1.

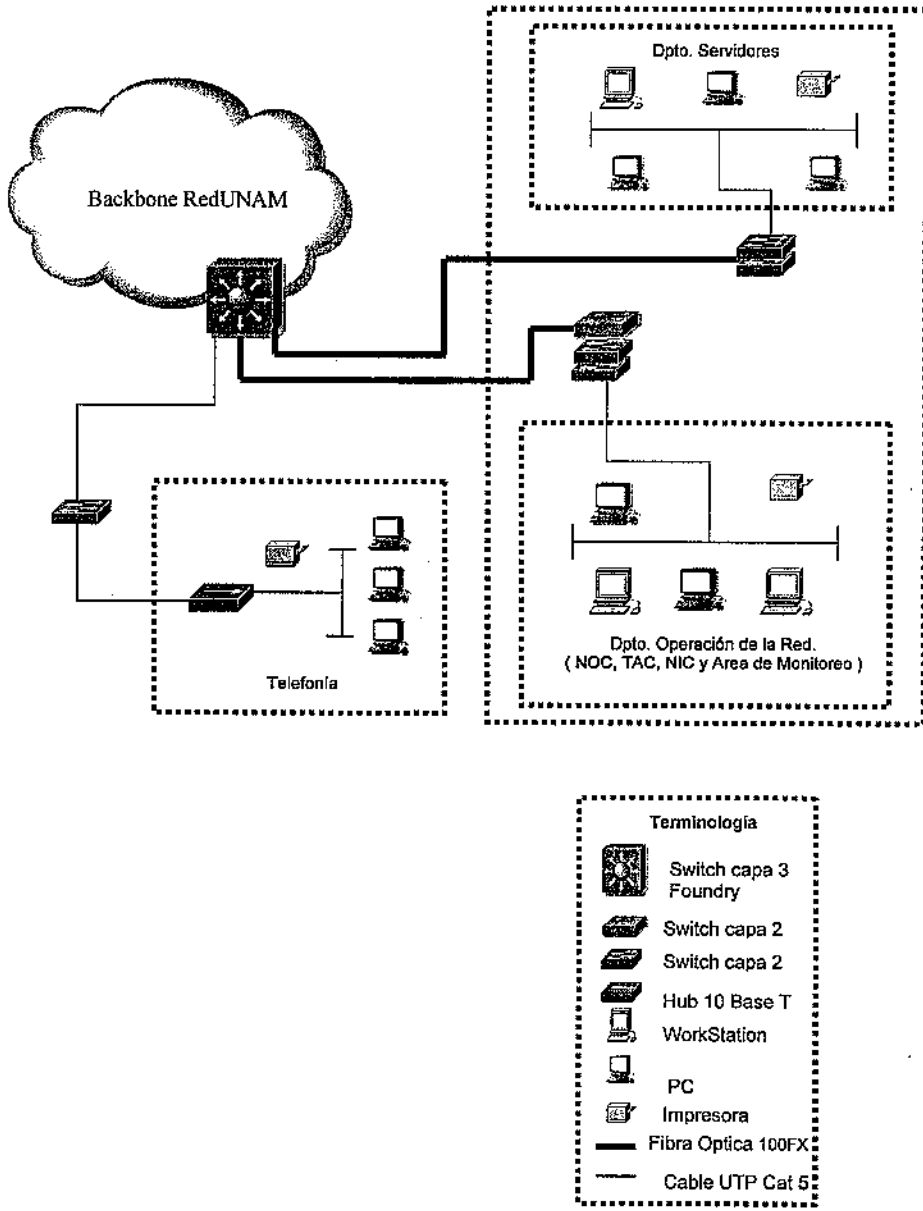


Figura 4.1 Diagrama de conexión actual

4.2 Descripción de la propuesta.

Los puntos más importantes a discutir en la propuesta de la red inalámbrica (WLAN) son:

- Necesidades del diseño de la red inalámbrica.
- Problemas de implementación
- Selección de la tecnología de red inalámbrica a implementar.
- La selección de la topología a utilizar.
- Estrategia para solucionar los problemas de seguridad de las redes inalámbricas.
- Selección de los equipos que se adecuen a las características y necesidades del Departamento de Operación de la Red
- Diseño de la red inalámbrica.
- Metodología.
- Políticas de seguridad.
- Costo de la red inalámbrica.
- Pruebas.

4.3 Necesidades del diseño de la red inalámbrica:

Debido a que se tiene que reubicar las áreas de NOC, TAC, NIC, administración de servidores y telefonía en una nueva área dentro de la DGSCA, una de las necesidades es encontrar una solución que permita cambios de infraestructura (para modificaciones posteriores, en la ubicación de puestos de trabajo o áreas) y a su vez permitir el ahorro de gastos de cableado y también aprovechar la movilidad típica de este tipo de redes.

4.4 Problemas de implementación.

La implementación de una red de estas características presenta algunos detalles relativos al ancho de banda que maneja un punto de acceso, que solo es de 11 Mbs y será compartido por todos los equipos dentro del rango de cobertura del punto de acceso o por la ***n*** cantidad de equipos que tengan configurado el mismo SSID.

Otro punto importante es relacionado a la seguridad, que es necesario cuidar puesto que el medio de transmisión físico es el aire, por lo tanto no se puede evitar que un tercero pueda recibir información muy importante. Pero con mecanismos adecuados de seguridad se evitará que un tercero pueda recibir dicha información, tales como passwords para acceder a los routers de la RedUNAM, etc.

Hago hincapié en la seguridad, ya que nos permitirá asegurar las transmisiones con la misma seguridad que ofrece la red local cableada y evitar que la información transmitida sea descifrada por personal no autorizado.

4.5 Selección de la tecnología de red inalámbrica a implementar.

En primer lugar descartamos la tecnología de FHSS, ya que con ella solo podemos transmitir un máximo de 2Mbs. Por lo tanto la tecnología que utilizaremos es DSSS ya que utiliza la técnica CDMA/CA con la que se puede lograr tasas de transmisión de 1 hasta 11Mbps, además de que nos va a permitir en un futuro un incremento de transmisión de bits de 11 Mbs a 54 Mbs en la banda de los 2.4 Ghz con el estándar 802.11g, además se encuentra más comercializada y estable.

Por este motivo ésta será la tecnología que se utilizará en la implementación de la red inalámbrica.

La selección de la topología a utilizar.

En cuanto a la topología a implementar será en modo infraestructura, debido a la gran cantidad de Works Stations, PC's y demás dispositivos, (para llevar a cabo la administración y monitoreo de la RedUNAM) que se encuentran dentro de los departamentos de operación de la red, conmutación y servidores.

4.6 Estrategia para solucionar los problemas de ancho de banda y de seguridad en las redes inalámbricas.

Debido a que un punto de acceso solo maneja un ancho de banda de 11 Mbps y a que es un medio compartido, se utilizara un nuevo segmento de red y este se subneteara /28, además de la utilización del protocolo 802.1q (VLAN's), todo esto para minimizar el dominio de broadcast, en tan solo 13 equipos por subred y así tener un mejor rendimiento en la red y evitar aun más las colisiones.

Con respecto a la poca seguridad proporcionada por el mecanismo de control de acceso, mediante el uso de un identificador de red (SSID), se evitará que el punto de acceso lo difunda, también se utilizaran claves wep de 104 bits y se ira cambiando la clave wep periódicamente

Por ultimo para reforzar aun más la seguridad, se utilizara un mecanismo de control de acceso (802.1X) a la red inalámbrica.

4.7 Selección de los equipos que se adecuen a las características y necesidades del Departamento de Operación de la Red.

En la elección de los equipos, debemos de tomar en cuenta que existen distintos fabricantes para distintas necesidades, además son varios los factores a considerar a la hora de comprar un sistema inalámbrico para la instalación de una red inalámbrica, por lo tanto, los fabricantes que he considerado por encontrarse entre las más representativas y competitivas en las soluciones para las redes inalámbricas son los siguientes:

- **3Com.**
- **Cisco.**
- **Orinoco (Proxim).**

Los aspectos a tener en cuenta en la selección de los equipos inalámbricos son los siguientes:

- Cobertura.
- Compatibilidad con redes existentes.
- Interoperatividad.
- Dualidad 802.11 a y b (upgrade para 802.11g).
- Simplicidad y facilidad de uso.
- Seguridad (Wep de 128 bits, 802.1x, WPA y WP2).
- Multiplataforma.

Dado que diversos fabricantes están promoviendo distintos equipos para las redes inalámbricas y en ocasiones soluciones que integran seguridad a los datos sobre la misma plataforma, se dará una breve explicación de estos equipos en el anexo de este trabajo.

4.8 Diseño de la propuesta.

Tras las necesidades previas, en la figura 4.2 se muestra el diseño de la propuesta de la red inalámbrica ideada, en la que se ha tenido en cuenta las necesidades y problemáticas comentadas anteriormente, en cuanto a la tecnología a utilizar y mecanismos a utilizar.

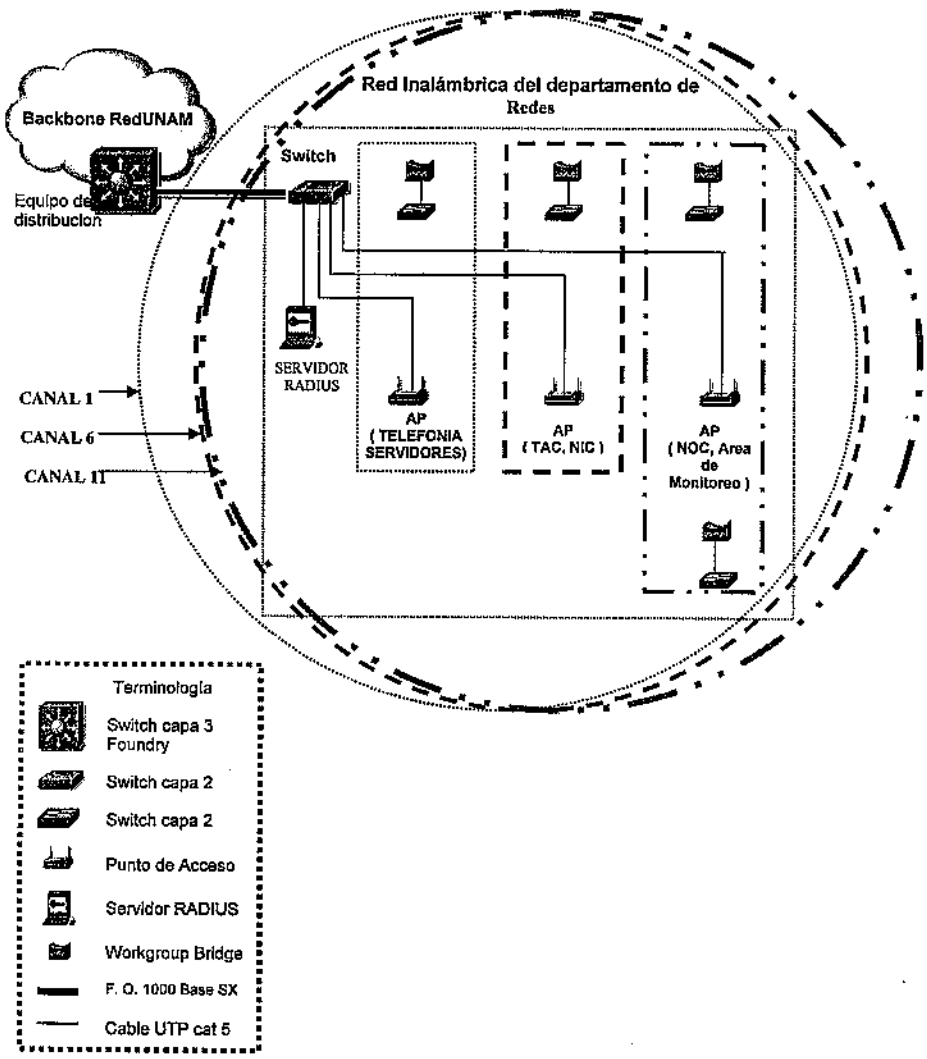


Figura 4.2 Diseño de la propuesta de la red inalámbrica.

Visión general de la propuesta.

Como ya se ha comentado anteriormente, la configuración de la red inalámbrica del departamento de redes que mejor se adecua a la hora de resolver los retos planteados en la propuesta es el modo infraestructura.

En dicha propuesta se tendrá un switch como nodo principal, en el cual se propone habilitar 802.1Q y configurar 3 Vlan's, las cuales proporcionaran la conexión a los diferentes puntos de acceso para las áreas (NOC, TAC, NIC, Servidores, Telefonía y la área de monitoreo), dicho switch estará conectado directamente a el quipo de distribución de DGSCA, en el cual también se habilitara 802.1Q y se configuraran las 3 Vlan's correspondientes, la conexión entre los switches involucrados propongo que sea en giga, ya que el switch de distribución cuenta con puertos disponibles y así mejorar la velocidad de entrada y salida hacia el backbone de la RedUNAM e Internet.

Como ya se ha comentado anteriormente, la implementación de las vlan's nos permitirán un mejor desempeño en la administración y monitoreo, al dividirse dominios de colisión y de broadcast, y así los usuarios pueden moverse a través de la red o cambiar de ubicación, manteniendo su pertenencia al grupo de trabajo lógico.

Las vlan's propuestas se pueden ver en la tabla 4.1:

Departamento	Vlan
Servidores	Vlan 1
Telefonía	Vlan 1
Centro de Asistencia Técnica (TAC)	Vlan 2
Centro de Información de la Red (NIC)	Vlan 2
Centro de Operación de la Red (NOC)	Vlan 3
Área de Monitoreo	Vlan 3

Tabla 4.1 Vlan,s del departamento

El nuevo direccionamiento para la asignación de los equipos (PC,s estaciones de trabajo e impresoras) del departamento se muestra en la tabla 4.2 y quedaría de la siguiente forma:

No	ID RED	BROADCAST	RANGO			UTILIZABLE	AREA
1	192.168.1.0	192.168.1.15	192.168.1.1	-	192.168.1.14	SI	NOC
2	192.168.1.16	192.168.1.31	192.168.1.17	-	192.168.1.30	SI	TAC
3	192.168.1.32	192.168.1.47	192.168.1.33	-	192.168.1.46	SI	NIC
4	192.168.1.48	192.168.1.63	192.168.1.49	-	192.168.1.62	SI	SER
5	192.168.1.64	192.168.1.79	192.168.1.65	-	192.168.1.78	SI	TEL
6	192.168.1.80	192.168.1.95	192.168.1.81	-	192.168.1.94	SI	MONITOREO

Tabla 4.2 Direccionamiento para la asignación de los equipos del departamento

En la tabla 4.3 se muestra el direccionamiento para la administración de los equipos inalámbricos (puntos de acceso y puntos de extensión) y seria el siguiente:

No	ID RED	BROADCAST	RANGO			UTILIZABLE	DISPOSITIVO (Access Point y Bridges)
1	192.168.1.232	192.168.1.239	192.168.1.233	-	192.168.1.238	SI	SERVIDORES Y TELEFONIA
2	192.168.1.240	192.168.1.247	192.168.1.241	-	192.168.1.246	SI	TAC y NIC
3	192.168.1.248	192.168.1.255	192.168.1.249	-	192.168.1.254	SI	NOC y MONITOREO

Tabla 4.3 Direccionamiento para la administración de los equipos inalámbricos del departamento

Como se puede observar en la propuesta, la colocación de los puntos de acceso cubre de manera total el área del departamento, por lo que dichos puntos de acceso se configuraran en canales distintos de radiofrecuencia para evitar el solapamiento de señales e interferencias de transmisión, como se muestra en la tabla 4.4.

Punto de Acceso	Canal
Noc, Monitoreo	1
Tac. Nic	6
Servidores, Telefonía	11

Tabla 4.4 Canales de radiofrecuencia.

Utilizaremos también puntos de extensión (bridges), los cuales pertenecerán a las áreas correspondiente, ya que dichos departamentos cuentan con equipos a los cuales no se les puede instalar tarjetas o adaptadores inalámbricos, tales como work stations, IP Phones e impresoras, además de habilitar el control de acceso en base a la dirección MAC.

Respecto a la seguridad se propone instalar un servidor de RADIUS el cual recibirá las peticiones de autenticación del personal que se conectara a la red por parte del punto de acceso.

Además de configurar en los puntos de acceso y bridges inalámbricos las medidas de seguridad necesarias, tales como wep y listas de acceso.

4.9 Metodología.

En el proceso de reubicación de los equipos de los departamentos engloba un conjunto de actividades las cuales son expuestas a continuación:

- Dar a conocer a los departamentos involucrados de este movimiento, la nueva estructuración de la red.
- Programación del movimiento de los equipos a su nueva ubicación.
- Preparación de los equipos para el nuevo esquema.
- Configuración y re-configuración de los equipos que se cambiaran de ubicación, así como los que se agregaran a nuevo diagrama.
- Asignación de un nuevo segmento de direcciones IP.
- Hacer una adecuada segmentación de la red para poder aislar el tráfico de la misma en dominios, lo cual redundara en el buen funcionamiento de la red.

4.10 Políticas de seguridad

A parte de las medidas tomadas en el diseño de la red inalámbrica, debemos de aplicar ciertas normas y políticas de seguridad que ayudaran a mantener la red más segura:

- Utilizar WEP (128) como una implementación mínima de seguridad, para cualquier usuario que se conecte a la red. Esto nos permite un cierto nivel de cifrado para la información.
- Deshabilitar DHCP para la red inalámbrica. Las IP's deben de ser fijas, para así tener también un control de las direcciones IP que se están conectando a la red.
- No emitir Beacon Frames, ya que estos anuncian el nombre de la red inalámbrica y cualquier dispositivo inalámbrico que este dentro del rango de cobertura de la red detectaría que hay una red inalámbrica disponible.

- Cambiar el SSID (Server Set ID) que viene por default en AP's, ya que son conocidos y esta puede ser una vulnerabilidad en la red inalámbrica.
- Todo el personal dentro de la red inalámbrica deben acceder a los equipos de administración utilizando SSH.

4.11 Costo de la red inalámbrica.

Como ya ha quedado ampliamente descrita la propuesta de la red inalámbrica, hay diferencias técnicas y económicas, que harán que la solución inalámbrica sea más económica que una solución cableada bajo ciertas condiciones.

El despliegue de la red inalámbrica implica dos tipos de costos: el generado para la infraestructura, por los puntos de acceso; y el derivado por los adaptadores inalámbricos para los usuarios.

Los precios de los puntos de acceso varían dentro del rango de 800 y 1000 dólares. Los bridges inalámbricos entre 200 y 400 dólares. Por su parte los adaptadores inalámbricos cuestan entre 200 y 700 dólares, y los hay disponibles para plataformas de computadoras estándar.

El costo de la instalación y mantenimiento de la red inalámbrica es menor al correspondiente a una LAN cableada, por dos razones:

- Elimina el costo generado por el tendido del cableado estructurado y las actividades asociadas a la instalación, mantenimiento y reparación.
- Simplifica movimientos de la infraestructura, crecimientos y cambios por consiguiente, disminuye los costos generados durante estas actividades.

En base a la propuesta de la red inalámbrica para el departamento de redes de la DGSCA, CU, los equipos que más se adecuan a ella, es toda la solución Cisco, ya que cumplen con todos los requisitos necesarios, como son: compatibilidad, interoperabilidad, seguridad, actualización para nuevos estándares, etc.

Además los puntos de acceso cisco soportan alimentación sobre ethernet, a diferencia de los 3com y Proxim que necesitan de un inyector de alimentación ethernet. Los bridges inalámbricos Cisco soportan 8 dispositivos ethernet, seguridad wep y EAP, los 3Com solo soporta 4 dispositivos ethernet y seguridad wep y proxim que no cuenta con este tipo de dispositivos.

4.12 Pruebas

Estas son las pruebas de conectividad y seguridad de la propuesta de la red inalámbrica:

Dado que no se emite el identificador de red como se puede ver en la figura 4.3, se tiene que configurar la red inalámbrica manualmente de la siguiente manera:

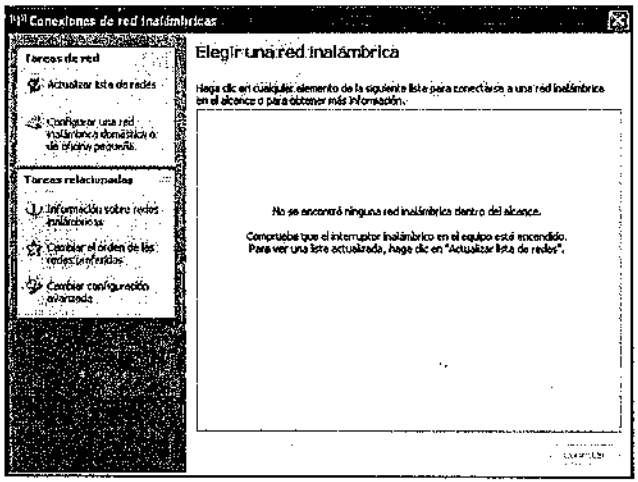


Figura 4.3 Conexión de red inalámbrica sin encontrar ninguna red disponible

Damos un clic con el mouse en **"Cambiar configuración avanzada"** del cuadro de dialogo de conexiones inalámbricas y nos muestra el siguiente menú, como se muestra en la figura 4.4.

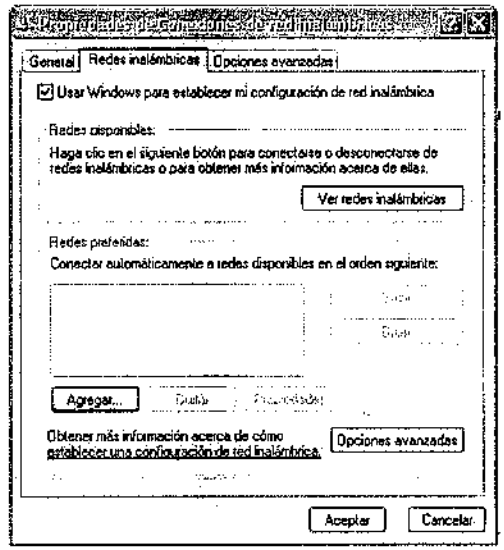


Figura 4.4 Menú "Propiedades de conexiones de red inalámbrica"

En este menú nos muestra las siguientes pestañas de configuración: General, Redes Inalámbricas y Opciones avanzadas.

- **General:** aquí es donde configuraremos la dirección ip asignada a nuestro adaptador de red inalámbrico.
- **Redes Inalámbricas:** aquí configuraremos el nombre de nuestra red inalámbrica y características de seguridad como: WEP
- **Opciones Avanzadas:** aquí es donde seleccionaremos la opción de utilizar o no el firewall de Windows.

Para configurar la red inalámbrica, seleccionamos el botón de Agregar, aquí nos muestra el siguiente menú, figura 4.5, en donde configuramos todos los parámetros como son el nombre de la red (SSID) y la clave WEP.

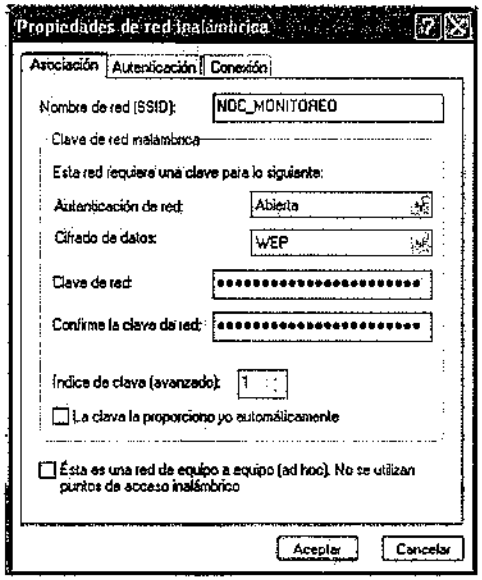


Figura 4.5 Configuración de la red inalámbrica y wep.

En la pestaña de autenticación seleccionamos la opción de "Autenticación", donde habilitamos 802.1x y seleccionamos la opción de EAP protegido por PEAP, como se ve en la figura 4.6.

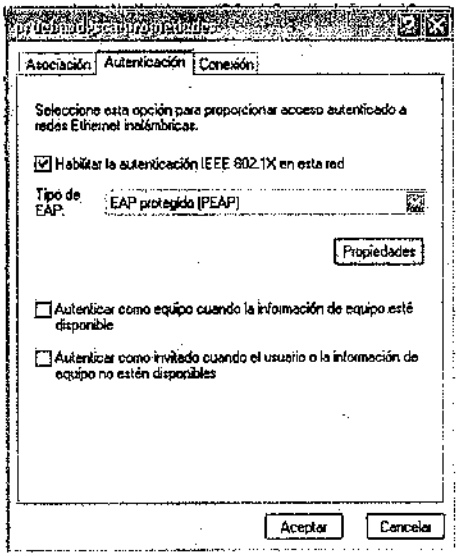


Figura 4.6 Selección del 802.1x y EAP

Ya que tenemos todos los parámetros configurados empieza el proceso de conexión y autenticación como se muestra en las siguientes figuras:

En la figura 4.7 se abre el cuadro de dialogo donde nos pide el nombre de usuario y contraseña para conectarnos a la red inalámbrica.

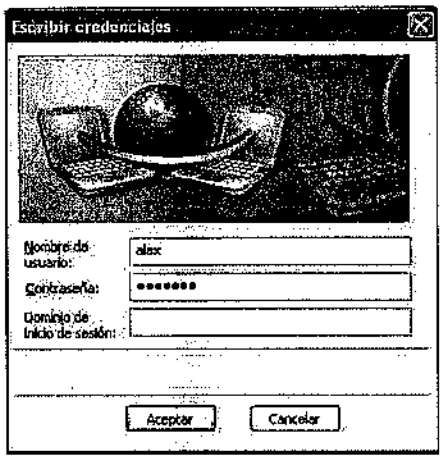


Figura 4.7 Ventana de nombre de usuario y contraseña

Ya que introducimos el nombre de usuario y contraseña, empieza el proceso de autenticación, como se muestra en la figura 4.8.

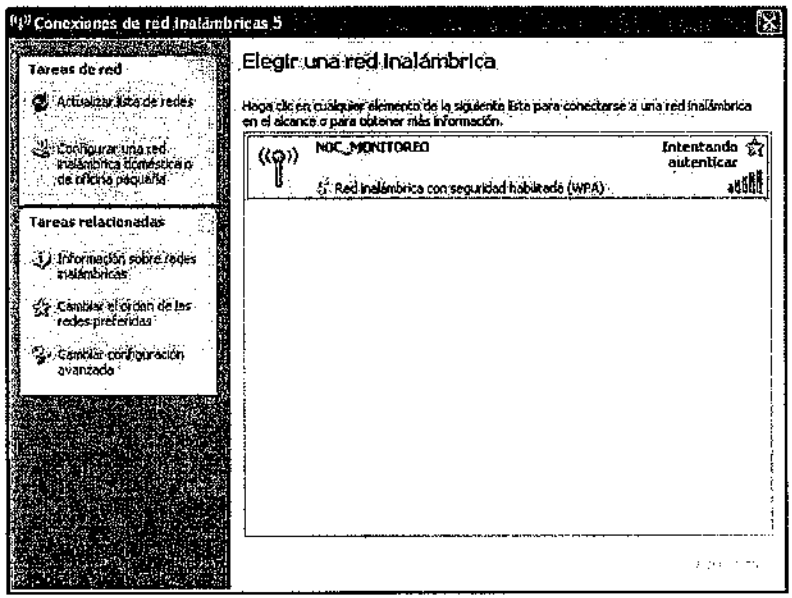


Figura 4.8 Proceso de autenticación.

En la figura 4.9 se muestra el proceso de comprobación del nombre de usuario y contraseña.

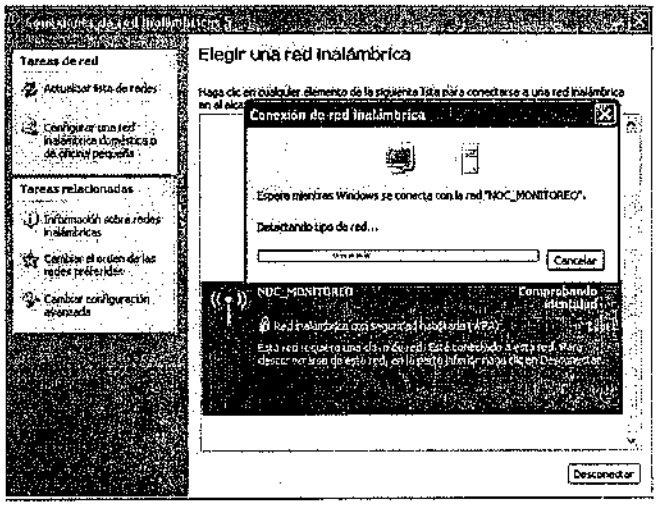


Figura 4.9 Comprobación del nombre de usuario y contraseña.

Y finalmente se logra la conexión como se muestra en la figura 4.10

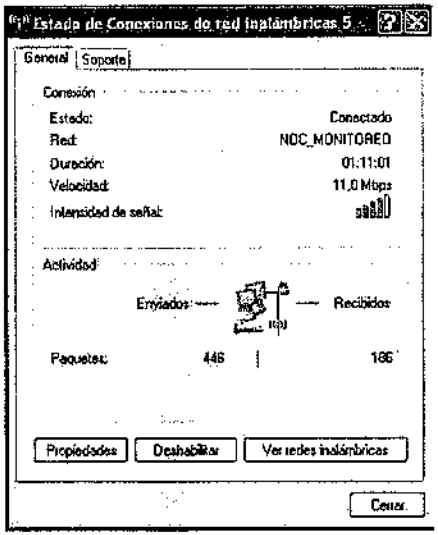


Figura 4.10 Conexión exitosa.

Capítulo 5

Futuro de las redes inalámbricas

Las redes inalámbricas poseen un futuro prometedor, debido a la gran aceptación que están recibiendo en escuelas, empresas o en el hogar. Esto es debido en gran parte a la presión que las grandes compañías que están detrás de los componentes están ejerciendo en el mercado de las telecomunicaciones inalámbricas.

El hecho de disponer de una red inalámbrica permite ofrecer servicios que de otra manera no estarían disponibles y, en el caso de estar, presentarían con soluciones alternativas unos costes superiores a los de esta red. Entre estos servicios se pueden destacar:

- Telefonía de VoIP e inalámbrica: Se pueden implementar servicios de telefonía a través de soluciones de voz sobre IP e inalámbrica, sistemas que se están utilizando en universidades, grandes empresas y organismos públicos para ahorrar costes en telefonía. En la figura 5.1 se muestra algunos de los modelos de teléfonos para este fin.

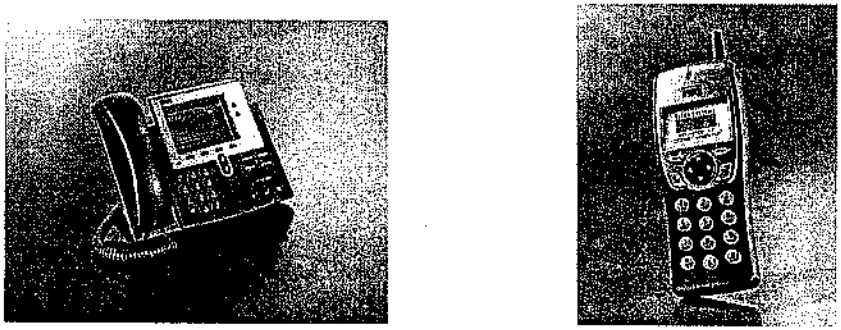


Figura 5.1 Teléfonos IP

- Video-Conferencia: Al disponer de un ancho de banda de hasta 11 Mbps se puede desarrollar servicios de video-conferencia, tanto en comunicaciones persona a persona como entre más de dos personas; de esta forma, los participantes pueden abaratar costes, al evitar la necesidad de desplazarse. En la figura 5.2 se muestran las cámaras de videoconferencia inalámbricas que se pueden utilizar.

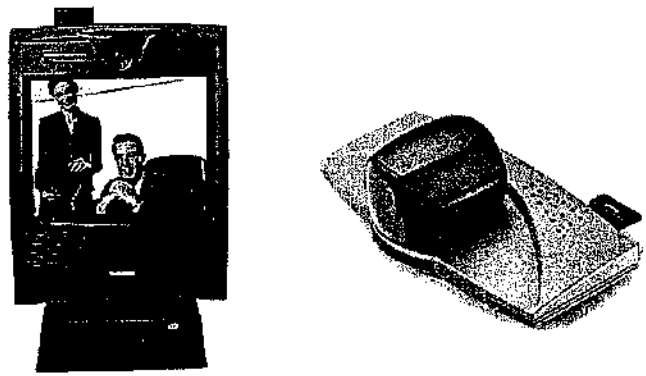


Figura 5.2 Video cámaras inalámbricas

- VPN (Virtual Private Network, Red Privada Virtual) bajo redes inalámbricas: servicio de comunicación entre diferentes edificios públicos o edificios de una misma universidad, que se encuentren en la misma ciudad o en ciudades distintas. Además en estas redes privadas se pueden incorporar políticas de cifrado de datos que las hacen más seguras que las redes tradicionales.

Por otra parte existen grupos de trabajo de la IEEE que han estado trabajando en los nuevos estándares que deben cubrir las necesidades de este tipo de redes, sacando a la luz numeras especificaciones dentro del marco del 802.11. Aunque actualmente no se han terminado muchas de estas especificaciones mencionare los diferentes trabajos y sus estados actuales ya que parece que la industria se está moviendo hacia compromisos y consensos que permitirán que muchos de los elementos de la próxima generación proporcionen mayor velocidad, fiabilidad, voz, audio y video y las bases de seguridad que permitan sustentar este tipo de redes.

- **802.11a:** Opera en la banda de 5GHz lo que da un ancho menos poblado proporcionando más canales y un ancho de banda mayor. De esta forma podemos tener más puntos de acceso con menos interferencias y señales más limpias. 802.11a cuenta simplemente con una posición aventajada especialmente cuando en entornos donde el rendimiento de la red en el lado servidor es importante y el cableado físico es costoso. Los fabricantes producirán tarjetas duales que permitirán a un cliente enlazarse con 802.11g/b y 802.11a, aunque no a la vez. El objetivo de IEEE ha sido asegurarse de que todo menos la parte de radio de los estándares a, b y g sea compatible. De esta forma un fabricante puede proporcionar dos tipos de radios sin duplicar el resto del equipo manteniendo, así, los costes muy bajos.

- **Grupo 11c:** Añadir soporte MAC en 802.1 para operaciones de puente para el estándar 802.11.

- **Grupo 11d:** Definir nuevos requerimientos para la capa física, como puede ser canales, secuencias de saltos y otros requerimientos para hacer funcionar 802.11 en otros países, dónde no es posible implementar 802.11, puesto que no tienen 2.4Ghz libre o es más corto.

- **Grupo 11e:** Mejorar el MAC del 802.11 para que pueda manejar de forma adecuada Calidad de servicio, poder tener clases de servicio y mejorar los mecanismos de seguridad y autentificación. Esta es una tarea compleja que involucra la coordinación entre las radios de los diferentes clientes, puntos de acceso y administradores de sistemas. QoS es necesario para la emisión de voz de calidad utilizando VOIP (voz sobre IP) y para multimedia. Inicialmente 802.11e cubría QoS y seguridad. Pero con los constantes informes de debilidad en el sistema de cifrado WEP (Wireless Equivalent Privacy) la parte de seguridad adquirió su propia identidad en el grupo 802.11i.

- **Grupo 11f:** Ayudar la interoperabilidad entre puntos de acceso.

- **Grupo 11g:** Conseguir mejorar la tasa de transmisión de hasta 22Mbit/seg en la banda de 2.4GHz de una forma totalmente compatible hacia atrás con 802.11b. El OFDM (Orthogonal Frequency División Multiplexing) desarrollado como codificador para 802.11a será adoptado por 802.11g como mecanismo de codificación. Texas Instruments está fabricando equipos con una codificación diferente llamada PBCC (Packet Binary Convolution Coding) que también será soportada por 802.11g.

- **Grupo 11h:** Al contrario que en Ethernet, las especificaciones de radio 802.11 no escuchan la red antes de transmitir para comprobar que la línea esta libre. Estas, en cambio, transmiten y sin esperar la respuesta apropiada, paran y retransmiten. Los dispositivos Ethernet escuchan, envían, y si encuentran algún problema, esperan una cantidad de tiempo determinada antes de retransmitir. 802.11h se basa en 802.11a para resolver los problemas de interferencias y uso, así como mejorar la coexistencia con otras especificaciones que trabajan en el mismo ancho de banda. La especificación h chequea si las frecuencias están en uso antes de la transmisión (Dynamic Frequency Selection o DFS) y de que transmitan con el nivel de energía mínimo (Transmit Power Control o TPC). Estas mejoras fueron formuladas para conseguir los requisitos de uso de la banda de 5GHz en la Unión Europea que denomina a su especificación equivalente como HiperLAN2.

- **Grupo 11i:** El grupo de esta especificación ha estado trabajando en la sustitución de WEP y afortunadamente se definirá con la suficiente compatibilidad como para no tener que revisar los sistemas ya creados. La propuesta actual es la de mejorar WEP por medio de la creación de un gran numero de vectores de inicialización para el cifrado WEP. Estos motivos hacen que la propuesta busque la modificación de WEP para conseguir que no sea crackeado en 100.000 o más años con la tecnología actual. WEP2 es el nombre del nuevo estándar que utiliza claves temporales (Temporal Key Integrity Protocol o TKIP), asegurando que una clave retiene su seguridad a lo largo del tiempo. Un paso más allá es el de rotar entre muchas claves en periodos cortos de tiempo.

Como he mencionado, hay grupos de trabajo, hoy día trabajando en paralelo, con el objetivo común de mejorar el estándar en diversos aspectos.

Con el tiempo se espera que el aumento de demanda de productos 802.11 incremente la competencia y hagan LAN inalámbricas más competitivas y baratas, para casi todas aplicaciones que requieren conectividad inalámbrica.

Conclusiones

En esta tesis he presentado la utilización de las redes inalámbricas como una alternativa de implementación fiable para la administración de la RedUNAM dentro del departamento de redes de la Dirección General de Servicios de Computo Académico C.U.

Además, tras detallar y presentar la propuesta de la red inalámbrica, se puede ver cómo se solucionan los problemas de ancho de banda y de seguridad que en la propuesta se comentaron:

- Al utilizar un nuevo segmento de red y subnetearlo /28, se redujeron los dominios de broadcast en solo 13 equipos por red, además de la utilización del estándar 802.1Q para crear vlan's para las diferentes áreas del departamento y así lograr grupos lógicos independientes.
- Al utilizar el 802.1X junto con el servidor de RADIUS, evitamos que cualquier persona ajena a los departamentos, puedan tener acceso a la red,

Por otra parte dentro del enorme horizonte de las comunicaciones inalámbricas y la computación móvil, las redes inalámbricas van ganando adeptos como una tecnología madura y robusta que permite resolver varios de los inconvenientes del uso del cable como medio físico, muchas de ellas de vital importancia en el trabajo cotidiano.

Obviamente, no se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, las prestaciones de unas y otras, a día de hoy, no pueden compararse. Sin embargo, la pacífica convivencia de las redes cableadas y de las inalámbricas, da lugar a una nueva generación de redes híbridas que cubren por completo, según su configuración y diseño, las necesidades de conectividad tanto fija como móvil, que toda empresa moderna y competitiva requiere.

Por ello puedo concluir que la en la realización de este trabajo incorporó el uso de diferentes tecnologías para cubrir las deficiencias de las redes inalámbricas para la implementación de dicha red, que el estándar 802.11 se trate de una especificación en continua evolución con posibilidad de adaptarse a nuevos requerimientos y demandas de usuarios en un futuro y que es una buena alternativa para la administración de la RedUNAM sin fisuras.

GLOSARIO

Acknowledge character (ACK): Es un carácter de control de transmisión, enviado por la estación receptora como una respuesta afirmativa a la estación que envía. En ocasiones es usado como carácter de control de corrección

CTS: Clear To Send: Libre para enviar: responde el receptor si se puede transmitir

DCF: Distributed Coordination Funcion: Función de coordinación distribuida

DSSS: Direct Sequence Spread Spectrum: Tecnología de espectro expandido de secuencia directa. Esta tecnica consiste en la generacion de un patron de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información. Este bit patron es llamado un chip (o chipping code). La longitud del chip, tiene una probabilidad mayor de que los datos puedan ser recuperados. Si uno o mas bits en el chip son dañados durante la transmisión, estos se pueden recuperar.

FCC: Agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones

FHSS: Frequency Hopping Spread Spectrum: Tecnología de espectro expandido con saltos de frecuencia. Esta técnica utiliza una señal portadora que cambia de frecuencia en un patrón que es conocido por el transmisor y el receptor. Apropiadamente sincronizada, la red efectúa este cambio para mantener un solo canal lógico de operación.

IEEE Institute of Electrical and Electronics Engineers: Instituto de Ingenieros Eléctricos y Electrónicos.

IEEE 802.11: Especificaciones para 1-2 Mbps en la banda de los 2.4 GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS).

IEEE 802.11b: Extensión de 802.11 para proporcionar 11 Mbps usando DSSS.

IEEE 802.11a: Extensión de 802.11 para proporcionar 54 Mbps usando OFDM.

IEEE 802.11g: Extensión de 802.11 para proporcionar 20-54 Mbps usando DSSS y OFDM. Es compatible hacia atrás con 802.11b. Tiene mayor alcance y menor consumo de potencia que 802.11a

ISM Bands Industrial, Scientific and Medical: Bandas de Aplicaciones Industriales, Cientificas y Medicas de libre uso.

IV (Vector de Inicialización): Es un vector binario no secreto usado como algoritmo de entrada para la encripcion de los datos.

LAN (Local Area Network, Red de Área Local): Normalmente no se suele extender más de uno o varios edificios.

MAC: Media Access Control: Control de acceso al medio (o a la capa física)

NIC: Network Interface Card: Tarjeta interfaz de red.

PCF: Point Coordination Funcion: Función de coordinación puntual.

PHY: Physical Layer (Capa física) es el medio en el cual se transmiten los datos.

Plain Text: Información sin encriptar

RF: La abreviación para la radiofrecuencia. De, o perteneciente a cualquier frecuencia dentro del espectro electromagnético normalmente asociado con la propagación de las ondas radio.

RTS: Ready To Send: Listo para enviar: es lo que dice el transmisor

SSH (Secure SHELL): SSH es un servicio de arquitectura cliente-servidor que permite conectarse desde una estación a otra a través de la red para ejecutar programas de forma remota. Dado que exista un servidor de SSH, los clientes pueden autenticarse en este e invocar comandos que se ejecutan en el servidor. SSH puede sustituir a programas como telnet, rsh, rlogin y rcp. Estos tienen como desventaja fundamental su gran vulnerabilidad debido a que la infomación intercambiada se trasmite de la misma forma en que se envía, pudiendo ser accedida por ``clientes" no autorizados. En cambio SSH provee varios mecanismos para encriptar lo trasmitido a través de canales inseguros. Con SSH también se pueden mover ficheros desde un extremo a otro de la conexión así como establecer conexiones gráficas *X* seguras.

SUBNETEO: Una máscara de red permite dividir la parte del HostID en dos partes por medio de la operación booleana AND bit por bit con lo que se obtiene:

La primera parte identifica al número de subred y la segunda parte identifica al host en esa subred.

Dirección IP regular

Identificador de Red	Identificador de Equipo

Dirección Subneteada

Identificador de Red	Identificador de Subred	Identificador de Equipo de la Subred

Mascara de Red *11111111 11111111 11111111 00000000*
255. 255. 255. 0

100000100 . 11111000 . 00000000 . 00000000 = 132.248.0.0 de manera binaria
111111111 . 11111111 . 11111111 . 00000000 = 255.255.255.0 de manera binaria

Para el mejor entendimiento del "subneteo" se ejemplifica un caso dentro de RedUNAM. La UNAM cuenta, entre otras redes, con una red clase B con dirección 132.248.0.0 y con mascara 255.255.255.0 que generan 2^{16} (65536) direcciones para asignar a equipos. Debido a las necesidades de asignar direcciones a las diferentes dependencias de la UNAM se optó por dividir la red en 256 subredes con 256 hosts en cada subred, entonces la mascara resultante es 255.255.255.0, la tabla 2-5 contiene el resultado de este subneteo.

a) Formato Hexadecimal:

Red :	**132.248.0.0**		
Clase :	**B**		
Máscara Natural :	**255.255.0.0**		
Máscara Aplicada :	**255.255.255.0**	**Máscara 24 bits**	
No. de subredes :	**256**	**Utilizables:**	**254**
No. de hosts por subred :	**256**	**Utilizables:**	**254**

b) Formato Binario:

FORMATO BINARIO	DECIMAL	SIGNIFICADO
Subred 0		
11111111 . 11111111 . 00000000 . 00000000	132.248.0.0	NetID de la subred 0
11111111 . 11111111 . 00000000 . 00000000	132.248.0.1	Primera dirección
11111111 . 11111111 . 00000000 . 00000010	132.248.0.2	Segunda dirección
.	.	.
.	.	.
11111111 . 11111111 . 00000000 . 11111101	132.248.0.253	Penúltima dirección
11111111 . 11111111 . 00000000 . 11111110	132.248.0.254	Última dirección
11111111 . 11111111 . 00000000 . 11111111	132.248.0.255	Dirección broadcast subred
Subred 1		
11111111 . 11111111 . 00000001 . 00000000	132.248.1.0	NetID de la subred 1
11111111 . 11111111 . 00000001 . 00000000	132.248.1.1	Primera dirección
11111111 . 11111111 . 00000001 . 00000010	132.248.1.2	Segunda dirección
.	.	.

.	.	.
111111111 . 11111111 . 00000001 . 11111101	132.248.1.253	Penúltima dirección
111111111 . 11111111 . 00000001 . 11111110	132.248.1.254	Última dirección
111111111 . 11111111 . 00000001 . 11111111	132.248.1.255	Dirección broadcast subred 1
.	.	.
.	.	.

De lo anterior resulta la siguiente tabla:

c)

No.	ID RED	BROADCAST	RANGO			UTILIZABLE
1	132.248.0.0	132.248.0.255	132.248.0.1	-	132.248.0.254	NO
2	132.248.1.0	132.248.1.255	132.248.1.1	-	132.248.1.254	SI
3	132.248.2.0	132.248.2.255	132.248.2.1	-	132.248.2.254	SI
4	132.248.3.0	132.248.3.255	132.248.3.1	-	132.248.3.254	SI
5	132.248.4.0	132.248.4.255	132.248.4.1	-	132.248.4.254	SI
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
252	132.248.251.0	132.248.251.255	132.248.251.1	-	132.248.251.254	SI
253	132.248.252.0	132.248.252.255	132.248.252.1	-	132.248.252.254	SI
254	132.248.253.0	132.248.253.255	132.248.253.1	-	132.248.253.254	SI
255	132.248.254.0	132.248.254.255	132.248.254.1	-	132.248.254.254	SI

Tabla 2-5 (a), (b) y (c), Subneteo de una red clase C.

Existe una fórmula que ayuda a calcular el valor de la máscara y determinar el número de hosts y subredes que más convenga a las necesidades de cada red:

N° de hosts o N° de subredes = $2^n - 2$, donde n = N° de bits.

Como consecuencia del explosivo crecimiento de Internet, uno de los mayores problemas que enfrenta la comunidad de Internet es el agotamiento de direcciones IP; esto nos lleva a la implementación de nuevas estrategias en el manejo de direcciones IP: Variable Length Subnet Masks (VLSM) y Classless Inter-Domain Routing (CIDR). A continuación se describen estas estrategias.

VLAN (Virtual Local Area Networks; Redes virtuales de área local): Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

Existen dos clases de VLAN: implícitas y explícitas. Las implícitas no necesitan cambios en el frame, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos. En esta clase de VLAN el usuario no modifica ni manipula el frame, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario.

Las VLAN explícitas si requieren modificaciones, adiciones y cambios (MAC) al frame, por lo que sacaron los estándares 802.1p y 802.1q, en donde se colocan ciertas etiquetas o banderas en el frame para manipularlo.

Las VLAN, se dividen en cuatro tipos principales: basadas en puertos, basadas en MAC, VLANs de capa 3 y basada en reglas (*policy based*).

VLANs Basadas en Puertos (*Membership by Port Group*)La VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un switch o también, en algunos casos, sobre varios switches. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

VLAN basadas en MAC (*Membership by MAC address*) Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.

VLANs de Capa 3 (*Layer 3-Based VLANs*). Las VLANs de capa 3 toman en cuenta el tipo de protocolo o direcciones de la capa de red, para determinar la pertenencia a una VLAN. Aunque estas VLANs están basadas en información de la capa 3, esto no constituye una función de enrutamiento y no debería ser confundido con el enrutamiento en la capa de red.

VLANs Basadas en Reglas (*Policy Based VLANs*).Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

VPN (Virtual Private Network, Red Privada Virtual): red que funciona sobre otra red ya establecida, siendo esta arquitectura transparente al usuario final.

WEP: Wired Equivalen Privacy: Privacidad equivalente a alambre.

Wi-Fi (Wireless Fidelity): Término registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de interoperar con los de otros fabricantes.

Wireless: Tecnología de comunicación inalámbrica.

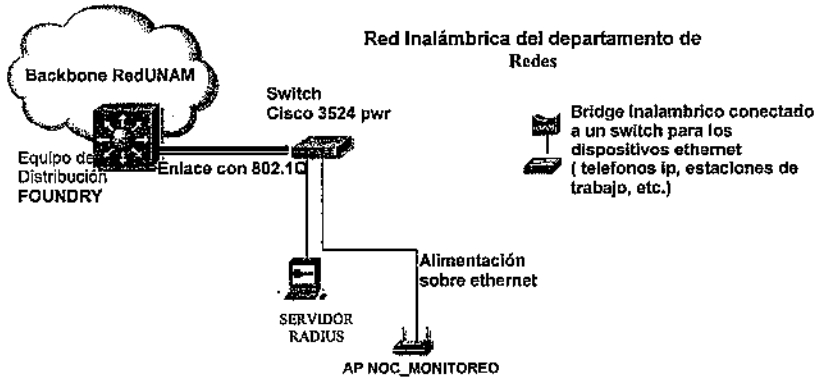
WLAN: Wireless Local Area Network: Red de Area Local Inalámbrica.

ANEXO A

CONFIGURACIONES DE LOS EQUIPOS

En dichas configuraciones solo se muestra los parámetros que se tienen que modificar en el caso de los switches, ya que hay líneas que no tienen nada que ver con el esquema de la red inalámbrica, a diferencia del ap y bridge inalámbrico, donde la configuración es completa .

El diagrama de la siguiente figura es para ilustrar las configuraciones de los equipos involucrados.



Configuración Foundry (Equipo de distribución)

```
!
vlan 1 name TEL_SERV by port
 tagged ethe 1/6
 router-interface ve 10
!
vlan 2 name TAC_NIC by port
 tagged ethe 1/6
 router-interface ve 20
!
vlan 3 name NOC_MONI by port
 tagged ethe 1/6
 router-interface ve 30
!!
interface ethernet 1/6
 port-name RED INALAMBRICA SEG 120
!
interface ve 10
 port-name AP SERVIDORES-TELEFONIA
 ip address 192.168.1.62 255.255.255.240 ospf-passive
 ip address 192.168.1.78 255.255.255.224 ospf-passive
 ip address 192.168.1.238 255.255.255.248 ospf-passive
 ip ospf area 0.0.0.4
!
interface ve 20
 port-name AP TAC-NIC
 ip address 192.168.1.30 255.255.255.240 ospf-passive
 ip address 192.168.1.46 255.255.255.240 ospf-passive
 ip address 192.168.1.246 255.255.255.248 ospf-passive
ip ospf area 0.0.0.4
!

interface ve 30
 port-name AP NOC-MONITOREO
 ip address 192.168.1.14 255.255.255.240 ospf-passive
 ip address 192.168.1.94 255.255.255.24 ospf-passive
 ip address 192.168.1.254 255.255.255.248 ospf-passive
ip ospf area 0.0.0.4
!
```

Configuración del switch cisco 3524 pwr

```
!
interface FastEthernet0/1
 description SERVIDORES-TELEFONIA
 switchport access vlan 1
 switchport mode dynamic desirable
 no ip address
!
interface FastEthernet0/2
 description TAC_NIC
 switchport access vlan 2
 switchport mode dynamic desirable
 no ip address
!
interface FastEthernet0/3
 description NOC_MONITOREO
 switchport access vlan 3
 switchport mode dynamic desirable
 no ip address
```

```
!
interface FastEthernet0/4
 description EQUIPO DE AUTENTICACION RADIUS
 switchport access vlan 3
 switchport mode dynamic desirable
 no ip address

interface GigabitEthernet0/1
 description Conexion al Foundry RED_INALAMBRICA
 switchport trunk encapsulation dot1q
 switchport mode trunk
no ip address
!
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan2
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan3
ip address 192.168.1.253 255.255.255.248
no ip route-cache

ip default-gateway 192.168.1.254
```

Configuración de los access point's

La configuración es la misma para los tres access point, a excepción de los nombres de la red inalámbrica (SSID) los cuales son :

- TAC_NIC
- SERVIDORES_TELEFONIA
- NOC_MONITOREO

Esta es la configuración del ap para las áreas de NOC y MONITOREO.

```
AP_NOC_MONITOREO#
!
Current configuration : 2161 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP_NOC_MONITOREO
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 132.248.120.51 auth-port 1812 acct-port 1813
```

```
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization lpmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
enable secret 5 $1$fife$lel8xCsilG368yxF9QxjN/
!
username Cisco password 7 106D000A0618
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 2 size 128bit 7 3823F25A0AB9783FA0A5E65A9502 transmit-key
 encryption mode ciphers tkip wep128
 !
 broadcast-key change 100000
 !
 !
 ssid NOC_MONITOREO
   authentication open
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
```

```
!
interface BVI1
 ip address 192.168.1.252 255.255.255.248
 no ip route-cache
!
ip default-gateway 192.168.1.254
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/ivory/1100
ip radius source-interface BVI1
radius-server host 192.168.1.250 auth-port 1812 acct-port 1813 key 7 0607032454
54
radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
End
```

Configuración de los Bridges inalámbricos.

La configuración de los bridges inalámbricos es la misma para los tres, a excepción de los nombres de la red inalámbrica (SSID) los cuales son :

- TAC_NIC
- SERVIDORES_TELEFONIA
- NOC_MONITOREO

Esta es la configuración de bridge inalámbrico para las áreas de NOC y MONITOREO

```
CONFIGURATION of Cisco WGB350 V8.80 Bridge NOC_MONITOREO


configuration radio ssid "NOC_MONITOREO"
configuration radio rates 1_11
configuration radio basic_rates 1
configuration radio world off
configuration radio i80211 rts 2048
configuration radio i80211 Privacy encryption on
configuration radio i80211 Privacy auth open
configuration radio extended parentid any
configuration radio extended parent_timeout off
configuration radio extended count_retry 64
configuration radio extended refresh 100
configuration radio extended power full
configuration radio extended fragment 2048
configuration security mode eap
configuration security username "alex"
configuration ethernet active on
```

```
configuration ethernet transparent off
configuration ethernet remove all
configuration ethernet add 080009f04250
configuration ethernet add 08006908f031
configuration ethernet add 0002b3e79833
configuration ethernet add 006008ab2ff3
configuration ethernet add 00096e04127f
configuration ethernet add 001111238a5e
configuration ethernet add 080020b94f2d
configuration ethernet add 001111395069
configuration ethernet staletime 700
configuration identity bootp_DHCP off
configuration identity name "Bridge NOC_MONITOREO"
configuration identity class "WGB350"
configuration identity inaddr 192.168.001.251
configuration identity inmask 255.255.255.248
configuration identity routing delete all
configuration identity routing net 000.000.000.000 192.168.1.254
000.000.000.000
configuration identity dns1 132.248.010.002
configuration identity dns2 132.248.204.001
configuration identity domain ""
configuration identity location ""
configuration identity contact ""
configuration console delete all
configuration console communities remote off
configuration console type ansi
configuration console linemode off
configuration time time_server 000.000.000.000
configuration time sntp_server 000.000.000.000
configuration time offset 0
configuration time dst off
configuration pspf off
statistics display_time 10
association niddisp numeric
filter multicast default forward
filter multicast remove all
filter node ethdst forward
filter node remove all
filter protocols default off
filter protocols unicast off
filter protocols remove all
filter direction to_radio
diagnostics load ftp dest 000.000.000.000
diagnostics load ftp username ""
diagnostics load ftp filename ""
diagnostics load distribute type firmware
diagnostics load distribute control newer
diagnostics load distribute remove all
logs printlevel severe
logs loglevel all
logs ledlevel error/severe
logs bnodelog off
```

```
logs snmp trapdest none
logs snmp trapcomm "public"
logs snmp loglevel off
logs snmp authtrap off
logs syslog 000.000.000.000
logs syslevel error/severe
logs facility 16
logs rcvsyslog on
```

Configuración de RADIUS en el servidor

Por *default* los archivos binarios que se tienen que editar se instalan en /etc/freeradius,.

Editar los archivo de configuración

En /usr/local/etc/raddb existen cuatro archivos:

- clients.conf
- users
- eap.conf

Se edita el archivo *clients.conf,* donde se configuran los que serán los clientes (puntos de acceso) de RADIUS. Para efectos prácticos se debe incluir lo siguiente:

```
client <IP_del_punto de acceso> {
      secret=<llave>
      shortname= AP
}
```

Donde *client* será la dirección IP que te fue asignada, *secret* es la llave que se usará para cifrar los paquetes de radius y también sirve para la autenticación.

Ejemplo:

```
client 192.168.1.252  {
     secret        = hola
     shortname     = AP_CISCO_AVAYA
}
```

En el archivo *users* se configuran los usuarios que serán autenticados por RADIUS.

```
#Autenticación local
usuario  Auth-Type := Local, User-Password == "passwd"
Service-Type=Login-User,
Login-Service=Telnet
```

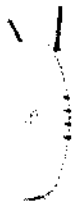
Ejemplo

```
alex  Auth-Type := local, User-Password == "alex"
      Service-Type=Login-User,
      Login-Service=Telnet
```

En el archivo eap.*conf* se configuran parámetros generales del tipo de autenticación EAP.

ANEXO B

El 3Com Wireless 8200 Access Point



Características y ventajas

- Se entrega como un punto de acceso monomodo 802.11b, que opera en la banda de 2,4 GHz con velocidad de conexión de 11 Mbps, y actualizable a modo dual 802.11b-802.11a con el kit de actualización
- Clear Channel Select y Dynamic Rate Shifting seleccionan el mejor canal y mantienen las conexiones de red constantemente disponibles al eligir la velocidad de conexión óptima.
- Se asigna a cada radio un ESSID (ID de Conjunto de Servicios Extendido) que identifica únicamente la red inalámbrica
- El inyector de alimentación en línea alimenta el punto de acceso sobre Ethernet,
- La autenticación de direcciones MAC basada en servidor RADIUS y local controla el acceso a la red inalámbrica
- El soporte de IP Estático y de DHCP permite la entrada manual de direcciones IP y la generación automática de direcciones IP, para una configuración y un setup flexibles

- Soporta encriptación WEP de 64 y 128 bits
- El soporte para SNMP, 3Com Network Supervisor, HP Open View, así como otros software de administración basados en estándares garantizan una integración sin discontinuidades con su red cableada

Especificaciones de producto

- **Compatibilidad con Normas Inalámbricas:** Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11a (con kit de actualización)
- **Velocidades de Datos Soportadas :** 802.11b: 1, 2, 5.5, 11 Mbps
- 802.11a: (con kit de actualización): 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **Banda de Frecuencias:** 802.11b: 2.4 GHz
  802.11a (con kit de actualización): 5 GHz
- **Medio Inalámbrico:** DSSS
- **Protocolo de Acceso a Medios:** CSMA/CA
- **Alcance Operativo:** 802.11b: hasta 100 metros (328 pies) en transmisión y recepción
  802.11a (con kit de actualización): hasta 115 metros (377 pies) en transmisión y recepción
- **Soporta**: 250 usuarios simultáneos
- **Antena:** 802.11b: opciones de antena disponibles, consulte la lista de "Opciones" para más información
  802.11a (con kit de actualización): sólo antena integrada
- **Seguridad:** Autenticación RADIUS; autenticación de direcciones MAC, protocolos EAP-MD5, EAP-TLS, EAP-TTLS, PEAP; encriptación WEP de 64 y 128 bits, encriptación WEP de 64, 128 y 154 bits en el kit de actualización 802.11; ESSID; protección de contraseña
- **Administración de Red:** Wireless Infrastructure Device Manager, Wireless LAN Discovery Tool, 3NS, SNMP (SNMP v1, SNMP v3, HP OpenView 6.2, 3NS)
- **Requisitos del sistema** para ejecutar la aplicacion una PC con CD-ROM, sistema operativo Windows Me/2000/98/95b+/NT 4.0+

3Com Wireless workgroup Bridge

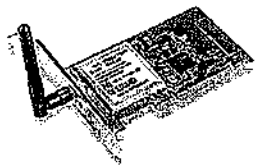
Características y ventajas

- Utiliza sistemas de comunicaciones NBX de 3Com, para la implementación rápida y eficaz de redes de voz y datos.
- Mediante la utilización de un hub o switch, podrá conectar hasta cuatro usuarios por bridge.
- Certificación Wi-Fi.
- En la mayoría de casos, no se requiere ninguna configuración, simplificándose así este proceso.
- Administración remota via Web, o bien mediante SNMP.

Especificaciones de producto

- **Velocidades de redes LAN inalámbrica:** 1, 2, 5'5 y 11 Mbps.
- **Gestión:** Servidor de gestión Web (el navegador debe tener soporte XML)
- **Tipos de soporte:** Interfaz Ethernet: RJ-45 10BASE-T, 802.11/Wi-Fi-compliant (2'4 GHz DSSS)
- **Estándares:** certificado Wi-Fi; IEEE 802.11b, IEEE 802.11, IEEE 802.3, IEEE 802.1d, HTTP
- **Requisitos del sistema** Para que funcionen las aplicaciones de administración, es necesario un PC con una unidad de CD-ROM y el sistema operativo Windows Me/2000/98/95b+/NT 4.0+

3Com 11 Mbps Wireless LAN PCI Adapter



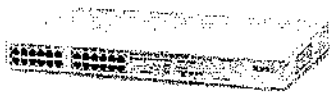
Características y ventajas

- El soporte 802.1x proporciona autenticación de usuario mediante servidor RADIUS
- Características similares a las de una red cableada con velocidades de hasta 11 Mbps y distancias de hasta 100 metros en interiores
- Sencilla instalación con funcionamiento plug-and-play y utilidad de configuración fácil de usar
- El cambio dinámico de velocidad garantiza la fiabilidad de las conexiones, incluso en condiciones de ruido
- Firmware actualizable a futuros estándares de seguridad y mejoras de funcionalidades
- La certificación Wi-Fi garantiza la interoperabilidad multiproveedor.

Especificaciones de producto

- **Bus :** PCI
- **Controladores:** Windows XP, Me, 2000, 98 SE, 98, 95 OSR2, and Windows NT 4.0 (Service Pack 6)
- **Seguridad:** 40- and 128-bit WEP encryption
- **Velocidades soportadas:** 1, 2, 5.5, and 11 Mbps
- **Distancia :** 100 metros (328 feet) en interiores
- **Sistema Operativo** Windows XP, Me, 2000, 98 SE, 98, 95 OSR2, or Windows NT 4.0 (service pack 6 or above)

SuperStack 3 Switch 4400 PWR



Características y ventajas

- Cumple con la especificación IEEE P802.3af
- Switch 4400 incluye clasificación y priorización avanzada de tráfico de capa 4, login de red de seguridad mediante RADIUS y control de contabilidad
- Solución ideal para instalaciones de telefonía de voz NBX, ya que el switch prioriza automáticamente el tráfico de voz
- El software 3Com Network Supervisor (con periodo de prueba de 60 días incluido) soporta la priorización automática de tráfico en tiempo real o crítico

Especificaciones de producto

- **Total de Puertos:** 24 puertos 10BASE-T/100BASE-TX con auto negociación y Potencia En Línea.
- **Interfaces con los Medios:** RJ-45
- **Características de switching Ethernet:** Autonegociación full/half-duplex y control de flujo; soporte para 802.1Q VLAN, priorización de tráfico 802.1p, DiffServ, Clasificación de Paquetes Multi-Layer; Marcaje de Paquetes DiffServ; Protocolo de Control de Agregación de Enlaces 802.3ad; Login de Red 802.1x mediante RADIUS
- **Administración:** Administración de interfaz de web, administración de interfaz de línea de comandos, 3Com Network Supervisor
- **Ranura de expansión para un modelo de Gigabit ethernet** (MT-RJ) 1000BASE-SX Module

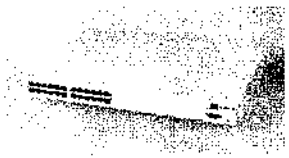
ORiNOCO AP-2000 Access Point

Características del AP-2000

- Arquitectura de doble slot que permite la fácil actualización hacia el estándar 802.11a a 54Mbps en 5GHz o el 802.11g a 54Mbps en 2.4GHz permitiendo un desempeño optimo en las aplicaciones.
- Velocidad de alto desempeño a 11Mbps o 54Mbps
- Amplio rango de cobertura de hasta 500 mts.
- Certificado de interoperabilidad WiFi
- Administración y gestión basada en web con soporte SNMP
- Características de contabilización vía RADIUS.
- IEEE 802.1x para mejorar la seguridad del sistema Wi-Fi con autenticación basada en usuario y distribución de clave WEP automática
- Admite Alimentación sobre Ethernet
- WEP y cifrado RC4 de 128 bits y tabla de control de direcciones MAC y autenticación Radius
- Selección de canal automática
- Admite redes LAN virtuales (hasta 16 VLANs)
- Reenvío de paquete
- Admite el modo 802.11a Turbo (108 Mbit/s), cuando se utiliza junto con el Kit AP-2000 5 GHz

NOTA : El radio debe ser adquirido por separado y no cuenta con bridges inalámbricos.

Proxim AE 3af DC Power Injectors



- Soportra el ORINOCO AP-2000
- Estandar IEEE 802.3af
- 12 puertos ethernet 10/100 BaseT RJ 45

ORINOCO PCI adapter

Características

Los adaptadores ORiNOCO PCI están diseñados para ampliar su red inalámbrica a escritorios, puntos de venta y otros dispositivos no portátiles.

El adaptador ORiNOCO PCI es compatibles con todas las tarjetas PC que cumplan con el estándar ORiNOCO IEEE 802.11b.

El PCI se entregan como adaptadores únicos. La tarjeta PC, que completa la solución, debe pedirse por separado.

ORINOCO PC Card

Características

Seguridad

La tarjeta PC Silver, dispone de privacidad alámbrica equivalente (WEP), con una clave de 64 bits.

La versión Gold proporciona mayor seguridad con una clave de 128 bits, utilizando un cifrado RC4 y 802.1x,

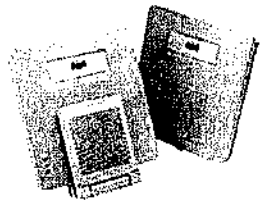
Certificado de Compatibilidad Wi-Fi de la WECA.

ORiNOCO PC Card: es compatible con Windows 95/98/2000/CE/NT/XP, Apple Mac OS 7.5.2, 8.6, 9.0 y 9.4, Novell Client 3.x y 4.x y Linux (versiones kernel 2.0.x hasta 2.2.x, 2.4) en procesadores Intel.

Protocolo de Acceso al Medio CSMA/CA (Collision Avoidance) con ACK

Se puede instalar en un ORiNOCO AP-2000 el adaptador PCI.

Cisco Aironet 1200 Series Access Point



Características

- Soporta 802.11b, 802.11a o los dos simultáneamente.
- Tiene Cisco IOS Software para futuras actualizaciones de IOS (firmware)
- Soporta Virtual LAN (VLAN) un máximo de 16 vlan's
- Soporta QoS prioritizando asi el trafico basado en el estandar 802.1p para servicios de voz y video
- Proxy Mobile IP provee sin diferenciar roaming entre subredes aumentando asi la movilidad de voz sobre 802.11
- Wireless Domain Services (WDS) es una caracteristica del Cisco IOS software la cual aumenta la movilidad de un cliente en la red inalámbrica.
- Fast Secure Roaming Permite que los dispositivos autenticados tengan movilidad con seguridad de un punto de acceso a otro sin ningún perceptible retrazo durante la reasociación.
- Contiene 8 MB de memoria flash para futuras actualizaciones de firmware y soporte para neuevos estandares 802.11 y caracteristicas avanzadas
- Soporta alimentacion sobre ethernet

Especificaciones

- Velocidades soportadas 802.11b: 1, 2, 5.5, 11 Mbps
- Cisco IOS Software
- Autosensing 802.3 10/100BASE-T Ethernet
- Mini-PCI (32-bit) modulo del radio
- Medio Inalámbrico DSSS
- Protocolo de acceso al Medio CSMA/CA
- Modulación DBPSK 1 Mbps, DQPSK 2 Mbps, CCK 5.5 and 11 Mbps
- Seguridad 802.1X y TKIP, WPA y AES lista (802.11g version)
- Protocolos de Autentificacion : 802.1X, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, Wi-Fi Protected Access (WPA) y lista de Acceso por MAC address
- Configuracion remota via BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP
- Configuracion local: CLI
- Encrpcion WEP de 64 y 128
- Certificación Wi-Fi

Cisco Aironet 350 *Series* Workgroup Bridge

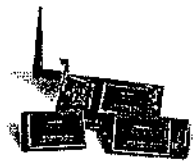
Caracteristicas

- Soporta un máximo de ocho dispositivos con activación Ethernet. a través del uso de un hub o switch por brida.
- Soporta el estandar IEEE 802.1x que utiliza el protocolo EAP (Extensible Authentication Protocol), para la autenticación de los dispositivos conectados al bridge.
- El bridge soporta seguridad WEP (Wired Equivalent Privacy) y proporciona un cifrado de 64 y 128 bits.
- Configuración y administración vía web, Telnet, FTP, TFTP o SNMP.

Especificaciones del puente para trabajo en grupo de la Serie Cisco Aironet 350

Velocidades de datos admitidas: 1, 2, 5,5 y 11 Mbps
Interfaz del cliente: Ethernet 10BaseT
Clientes compatibles: Directa: uno y a través de hub: o switch ocho
Medio inalámbrico: DSSS
Protocolo de acceso a los medios: CSMA/CA
Modulación: DBPSK a 1 Mbps, DQPSK a 2 Mbps, CCK a 5,5 y 11 Mbps

Cisco Aironet 350 Series Client Adapters



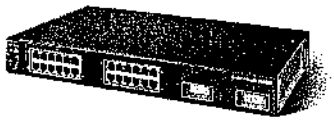
Caracteristicas

- Comunicaciones seguras en la red. basada en el estándar IEEE 802.1x mediante el protocolo EAP (Extensible Authentication Protocol)
- Utilidades con gran número de prestaciones para facilitar la configuración y la administración. Cisco Aironet Client Utility (ACU)
- Compatibilidad con los sistemas operativos más utilizados. Windows 95, 98, NT 4.0, Windows 2000, Windows ME, Windows CE, Mac OS versión 9.x y Linux.

Especificaciones

- **Velocidades de datos admitidas** 1, 2, 5,5 y 11 Mbps
- Estándar de la red IEEE 802.11b
- Interfaz del sistema PCI
- **Banda de la frecuencia** De 2,4 a 2,4897 GHz
- **Medio inalámbrico** DSSS
- **Protocolo de acceso a los medios** CSMA/CA
- **Modulación** DBPSK,DQPSK y CCK
- **Tipo de autenticación** LEAP
- **Certificación:** Wi-Fi

Catalyst 3524-PWR XL Stackable 10/100 Ethernet Switch



Especificaciones técnicas

- Dúplex completo IEEE 802.3x en puertos 10Base-T, 100Base-TX y 1000Base-X
- Protocolo de árbol de conmutación IEEE 802.1D
- Priorización CoS IEEE 802.1p
- VLAN IEEE 802.1Q
- Especificación IEEE 802.3ab 1000Base-T
- Especificación IEEE 802.3z 1000Base-X
- 1000Base-X (GBIC)
    - 1000Base-T
    - 1000Base-SX
    - 1000Base-LX/LH
    - 1000Base-ZX
- Especificación IEEE 802.3u 100Base-TX
- Especificación IEEE 802.3 10Base-T
- Administración vía web integrada, telnet, ssh, y CLI

BIBLIOGRAFÍA

LIBROS

Manual de referencia, Redes
McGraw Hill
Craig Zacker
Traducción: Manuel Cariacedo Cadierno.

Building a wireless office
Auerbach publications
Gilbert Held

Wireless security , models threats and solutions
McGraw Hill
Randall K. Nichiols y Panos C. Lekkas

Redes de comunicaciones, conceptos, fundamentos y arquitecturas básicas
McGraw Hill
Alberto Leon-García e Indra Widjaja

Comunicaciones y redes de computadoras.
Prentice may
William Stallings

A field guide to wireless LAN's for administrators and power users
Prentice Hall
Thomas Maufer

REVISTAS

PACKET
Cisco System magazine
Second quarter 2002

iQ
The fastest way to increase your internet quotient
November / December 2002

PACKET
Cisco System magazine
First Quarter 2003

PACKET
Cisco System magazine
Second quarter 2003

Referencias de Internet

Fabricantes de los equipos

http://www.3com.com
http://www.cisco.com
http://www.proxim.com

Otros sitios de interés.

http://www.utdallas.edu/ir/wlans/whitepapers/whatwlan.pdf
http://www.utdallas.edu/ir/wlans/whitepapers/802.11primer.pdf
http://www.utdallas.edu/ir/wlans/whitepapers/wlan_wp.pdf
http://www.blackhat.com/presentations/bh-usa-01/TimNewsham/bh-usa-01-TimNewsham.ppt
http://www.utdallas.edu/ir/wlans/whitepapers/WirelessUseInEducation.doc
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
http://lcd.efn.unc.edu.ar/frames/archivos/fernets.pdf
http://www.icesi.edu.co/es/publicaciones/contenidos/sistemas_telematica/3/jamdrid-seguridad_redes_inalambricas.pef
http://videos.aimme.es:3001/videos/CursoCE2003/04lecisa.pdf
http://www.monografias.com