UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE LA RED INALÁMBRICA PARA EL CAMPUS DE CIUDAD UNIVERSITARIA (RIU)

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

EUGENIA PADILLA MENDOZA

GABRIELA GONZÁLEZ IZQUIERDO

DIRECTOR DE TESIS:
ING. ALFREDO HERNÁNDEZ MENDOZA

CIUDAD UNIVERSITARIA MÉXICO, D.F. 2007

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería.

Por permitirnos ser parte de esta gran institución que nos ha dado las mejores herramientas para desarrollarnos profesionalmente y como personas, por todas las enseñanzas, satisfacciones y alegrías y porque en ella conocimos a nuestros mejores amigos.

A nuestros profesores por todo el aprendizaje trasmitido y porque nos enseñaron a amar a la UNAM.

A DGSCA.

Por ser una gran institución que tuvo la visión y la inquietud de desarrollar este proyecto que es de gran utilidad para la comunidad universitaria y en la cual aprendimos muchas cosas que nos permitieron crecer como profesionistas.

Al Ing. Roberto Rodríguez Hernández por toda la ayuda proporcionada y por compartirnos sus valiosos conocimientos y experiencias.

Al Departamento de Redes de DGSCA.

Por todas las facilidades proporcionadas durante realización de la RIU, a nuestros compañeros de trabajo por su apoyo, enseñanzas y orientación en temas que eran nuevos para nosotras.

A nuestro asesor el Ing. Alfredo Hernández Mendoza.

Por aceptarnos en este proyecto, por tus enseñanzas, paciencia, consejos y te agradecemos que a pesar de tu carga de trabajo nos dedicaste el tiempo necesario para la realización y revisión de estas páginas.

Gabriela y Eugenia.

A Marcos y Yolanda.
Mis padres, por ser ejemplo de lucha, esfuerzo y esperanza, por todo el amor, por brindarme la confianza y la libertad de escoger mí camino, por apoyarme y motivarme siempre para seguirlo.

A Ángeles.
Mi hermana mayor, por estar conmigo, por escucharme y apoyarme siempre y en todo momento, incondicionalmente, sin importar la distancia, por darme el ejemplo de valentía, porque has cuidado de Sus y de mi aún cuando no tenías que hacerlo.

A Susana.
Mi hermana menor, por contagiarme de tu entusiasmo y alegría, por enseñarme a ser tolerante, porque siempre me motivas para seguir adelante y por la infancia tan hermosa que pasamos juntas.

A mis Amigos,
Porque aún escogiendo caminos distintos podemos darnos tiempo de disfrutar lo que la vida nos, porque en los momentos difíciles siempre han estado conmigo y por todo lo que hemos vivido juntos: Maribel, Laura, Leonardo, Christian, Memo, Omar, Jose Luis, Victor Hugo. A mis amigos y compañeros de trabajo de DGSCA por todas sus enseñanzas y por hacer mi vida mas agradable.

Al Ing. Alejandro Rentaría,
Mi jefe y amigo, por darme la oportunidad de ser parte de tu equipo de trabajo, porque me has enseñado muchas cosas, por la gran paciencia que me has tenido, por tus consejos, y por tu infinita colaboración para la terminación de este trabajo.

A Eugenia,
Mi compañera de tesis, por la confianza para hacer algo desconocido, porque pudimos hacer a un lado nuestras diferencias para terminar este proyecto juntas.

Gabriela.

A Dios.
Por permitirme llegar hasta este momento, por todo lo que tengo y soy.

A mis padres Angela y Francisco.
Por su apoyo, preocupaciones, consejos, cariño, cuidados, enseñanzas, por los buenos ejemplos que me dieron y por todo el esfuerzo que pusieron para que concluyera todo lo que me he propuesto en la vida.

A mis hermanas Elena, Gabriela, Verónica y Adriana.
Por su cariño, cuidados, apoyo, por el tiempo que le dedicaron a enseñarme y explicarme tantas cosas, por estar siempre conmigo y por hacer que mi vida sea más sencilla.

A mis tías Martha y Mary y a mi abuelita Trini.
Por sus preocupaciones y consejos.

A Alejandro.
Por tus consejos, apoyo, paciencia, enseñanzas, por todo el tiempo que le dedicaste para que este trabajo resultara lo mejor posible y por hacerme tan feliz.

A Vero.
Por todo lo que hemos compartido, por estar siempre a mi lado, por tu apoyo dentro y fuera de los salones de clase, por lo agradable que hiciste nuestro paso por la universidad y por hacerme reír tanto.

A Gaby.
Por el empeño, preocupaciones y todo el tiempo dedicado para que realizáramos y concluyéramos este trabajo.

A mis amigos y compañeros en DGSCA.
Por todos lo momentos compartidos, por hacer que mi primer trabajo profesional fuera agradable y divertido.

Eugenia.

ÍNDICE

CAPÍTULO 3
DISEÑO DE LA RED INALÁMBRICA UNIVERSITARIA

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

OBJETIVOS

OBJETIVO GENERAL

Diseñar e implementar una red inalámbrica que cubra gran parte de Ciudad Universitaria.

OBJETIVOS PARTICULARES

- Cubrir lugares de gran afluencia para la comunidad universitaria, que sea gratuita y que esté disponible casi en todo momento los 365 días del año.

- Diseñar una red segura, lo que permitirá garantizar la confidencialidad de la información de los usuarios, utilizando el mecanismo de cifrado necesario y proporcionándole credenciales únicas a cada uno de ellos.

- Utilizar una tecnología inalámbrica que cuente con una administración centralizada, que permita un crecimiento a futuro y que sirva como modelo para implementarla en otras escuelas de la UNAM.

- Estandarizar las diversas redes inalámbricas ya existentes a lo largo del campus universitario.

INTRODUCCIÓN

El presente trabajo de tesis trata sobre la realización del diseño y la implementación de una red inalámbrica que cubra gran parte del campus de Ciudad Universitaria proporcionando servicio de red, como por ejemplo, navegación por web, consulta de correo electrónico y de acervos bibliotecológicos en línea.

La realización de dicho proyecto surgió debido a que una de las actividades importantes de la comunidad universitaria es el uso de Internet y como resulta difícil proporcionar servicio de red cableada a cada universitario porque es costosa y no se cuenta ni con el espacio ni con la infraestructura suficiente, se consideró proporcionar un servicio de red inalámbrico con el cual los universitarios pudieran hacer uso de sus equipos portátiles en cualquier lugar con cobertura del servicio, sin la necesidad de pedir prestado equipo a los laboratorios propios de su facultad o de esperar turno para hacer uso de un equipo de cómputo con red.

Los aspectos más importantes que se tomaron en cuenta para el diseño de la RIU (Red Inalámbrica Universitaria) fueron los siguientes:

- Que fuera de uso exclusivo para la comunidad universitaria, por lo que los usuarios deben ser personas activas dentro la UNAM, ya sea estudiantes, académicos o investigadores.

- El servicio será gratuito y disponible prácticamente todo el año.

- Las personas que cuenten con dispositivos de red inalámbricos podrán hacer uso de ella en lugares de gran afluencia universitaria, por ejemplo bibliotecas, auditorios, jardines, explanadas y cafeterías.

- Intentar estandarizar la seguridad de las redes inalámbricas existentes en ciudad universitaria, para lo cual se propone poco a poco ir cambiando las que son inseguras y hacerlas parte de la Red Inalámbrica Universitaria.

Después de la implementación se espera que esta propuesta sirva como prototipo para la instalación en otros campus fuera de Ciudad Universitaria o para su integración a la misma de ser posible, así como para aumentar y mejorar las actividades académicas en la UNAM lo cual contribuiría al fortalecimiento de la enseñanza superior en México y mantendría a la Universidad en la vanguardia de la tecnología.

En este proyecto de tesis se describen los aspectos importantes de las redes inalámbricas, así como el diseño y la implementación de la RIU. A continuación se mencionan brevemente las características principales de cada capítulo.

En el capítulo uno se describen los conceptos básicos de las redes inalámbricas, sus orígenes, los elementos que la componen, así como los beneficios y aplicaciones de las mismas.

En el segundo capítulo se describe la teoría del estándar de seguridad 802.11, sus principales tecnologías y las formas de seguridad que se utilizarán para el acceso a la RIU.

En el tercer capítulo se mencionan las necesidades del diseño, los problemas de implementación que se tuvieron, así como también la metodología, las políticas de seguridad y el direccionamiento.

Finalmente en el cuarto capítulo se describe las etapas de implementación, las configuraciones de equipo, el monitoreo y la puesta en operación.

CAPÍTULO 1

REDES INALÁMBRICAS

1.1 Orígenes de las redes inalámbricas.

La necesidad de comunicación siempre estará presente tanto en nuestras relaciones personales como en las laborales. Esta necesidad es la razón que ha promovido el desarrollo de nuevas tecnologías que permitan obtener una comunicación fiable, ágil, eficaz y rápida, permitiendo al mismo tiempo aprovechar estas ventajas en nuestro beneficio. De esta manera el desarrollo tecnológico al que nos enfrentamos nos ha llevado a crecer de una manera inmensa, nos ha facilitado, mejorado y agilizado muchas de las tareas que en el pasado eran lentas, complicadas y muchas veces costosas.

Tal ha sido el avance de la tecnología que se han desarrollado herramientas como la computadora que nos permiten realizar nuestras actividades cotidianas, así mismo es un medio de comunicación que permite que usuarios en sitios remotos puedan compartir su información por medio de Internet.

Por su parte Internet fue concebido a finales de los años 60, originalmente fue llamado ARPANET y su misión era conectar las computadoras de diferentes instituciones militares con el fin de que las comunicaciones no fueran

interrumpidas si alguna de estas instituciones era destruida. De esta manera día a día la comunicación ha ido aumentando, así como los medios con los que se propaga, dando oportunidad a todas las personas de mantenerse informadas de lo que pasa a su alrededor o en otras partes del mundo.

Buscando esta comunicación entre equipos de cómputo, fueron creados los protocolos que permitieron que la información pudiera viajar y ser interpretada por las computadoras, independientemente de su sistema operativo, fue así como nacieron los protocolos TCP/IP (Transmision Control Protocol/Internet Protocol). A los cuales desde su creación se les ha dado gran importancia por lo que los han mejorado enormemente.

Las redes han evolucionado de tal manera que permiten tener computadoras conectadas entre sí, lo cual genera una superautopista de la información que conecta a organismos oficiales, educativos, empresariales, etc. Así mismo han surgido nuevas tecnologías como lo son las redes inalámbricas las cuales han ido creciendo de tal manera que ahora ya son parte importante de nuestra vida laboral.

El origen de las redes inalámbricas WLAN (Wireless Local Area Network) se remonta a los años 70. Fue en una fábrica suiza donde se obtuvieron los primeros resultados satisfactorios de comunicación inalámbrica, lo cual se logró cuando ingenieros de IBM hicieron uso de enlaces infrarrojos para realizar una red de área local.

Posteriormente se siguieron realizando investigaciones en infrarrojos y en microondas, en esta última se utilizó a nivel laboratorio el esquema de espectro disperso (Spread Spectrum).

En 1985 la comisión federal de comunicaciones (FCC) y la agencia federal del gobierno de Estados Unidos, asignó las siguientes bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz al uso de redes inalámbricas que se basaban en el esquema de frecuencias altas. ISM se refiere a una banda reservada internacionalmente para uso no comercial de Radio Frecuencia electromagnética y para ser usada por las áreas: científica, médica e industrial (son utilizadas por los teléfonos

inalámbricos domésticos, las microondas, o los dispositivos BlueTooth). La banda es para uso comercial ya que la FCC no se involucra en quien debe de trasmitir dicha banda.

Una de las razones por las que las redes inalámbricas dejaron el laboratorio fue el hecho de que se les asignara una banda de frecuencias con lo cual se logró una mayor actividad en las industrias, y que se trabajara más en la fase de desarrollo. Fue hasta 1991 que se hicieron publicaciones de redes inalámbricas operativas con velocidad un poco mayor a 1 Mbps, que es el mínimo establecido por la IEEE 802 para que una red de área local sea considerada como tal.

En 1990, se forma el comité IEEE 802.11, el cual trató de generar la norma para las redes inalámbricas pero fue hasta 1994 cuando se llegó a algo más concreto.

En 1992 se creó Winforum, asociación formada por Apple y por empresas de telecomunicaciones e informática, con el objeto de conseguir bandas de frecuencia para los sistemas personales de comunicación (PCS).

En 1993 se asignaron las bandas de 5.2 y 17.1 GHz. Ese mismo año se forma la IRDA (Infrared Data Association), la cual buscaba promover el desarrollo de las redes inalámbricas hechas por enlaces infrarrojos.

En 1996 un grupo de empresas del sector de informática móvil (mobile computing) y de servicios, forman el Foro de interoperabilidad de redes inalámbricas (Wireless LAN Interoperability Forum, WLI Forum) con el fin de crear productos y servicios interoperativos. También se creo la alianza WECA (Wireless Ethernet Compatibility Alliance), la cual es una asociación internacional sin fines de lucro con el fin de certificar interoperabilidad entre productos WLAN basados en la especificación IEEE 802.11, y que en el 2002 cambio su nombre por Alianza Wi-Fi (Wireless Fidelity) por cuestiones de mercado.

En ese mismo año, el Instituto Europeo de Estándares en Telecomunicaciones (ETSI) aprobó el estándar HiperLAN (High Performance LAN), el cual

soportaba velocidades de hasta 10 Mbps.

La fuerza que a la fecha ha cobrado esta tecnología se debe, en gran medida, a la facilidad de instalación y conexión, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes cableadas convencionales, además de que se ha convertido en una excelente alternativa que ofrece conectividad en lugares donde resulta inconveniente o imposible brindar servicio de una red cableada.

1.2 Definición de una red inalámbrica.

Una red inalámbrica (WLAN) es una red local que conecta equipos terminales a la red de datos sin la necesidad de utilizar cables de comunicación para ello, utiliza la radio frecuencia y los infrarrojos para establecer una conexión a red.

Así mismo es un sistema de comunicación de datos flexible que puede llegar a reemplazar o extender una red de área local cableada o simplemente ofrecer funcionalidad adicional.

1.3 Elementos de una red inalámbrica (WLAN).

1.3.1 Puntos de acceso (AP).

El punto de acceso es un dispositivo que hace que haya una conexión de red transparente con dispositivos inalámbricos que se encuentren dentro de su radio de cobertura. Así mismo permite añadir de forma rápida y fácil otros dispositivos inalámbricos que amplían su cobertura y operabilidad, lo cual también permite que una red de área local pueda ser llevada a lugares inaccesibles evitando el cableado y brindando movilidad.

Algunas de las características de los puntos de acceso son:

- Recepción, amplificación y transmisión de señal.
- Interfaces Ethernet.
- Autenticación.
- Procesamiento IEEE 802.1x.
- Cifrado de datos.
- Múltiples SSID (Service Set IDentifier).

Figura 1.1 Puntos de acceso

La Figura 1.1 muestra algunos puntos de acceso existentes en el mercado.

En los últimos años se han ido realizando grandes cambios y mejoras en el diseño y la arquitectura de las redes inalámbricas y en los elementos que la conforman. La arquitectura del punto de acceso es un factor importante en la seguridad, la flexibilidad y la escalabilidad de las redes inalámbricas y éstos se han ido modificando a tal grado que han dado como resultado un nuevo concepto en la funcionalidad de puntos de acceso. En el lenguaje de la industria, se les conoce como “Fat APs” (puntos de acceso gordos) y “Thin APs” (puntos de acceso delgados).

1.3.1.1 Puntos de acceso “gordos”.

Los puntos de acceso gordos tienen la arquitectura tradicional de los puntos de acceso. Son dispositivos independientes que manejan toda la funcionalidad de la red inalámbrica, extendiendo las funcionalidades del radio 802.11 hasta la autenticación de usuarios 802.1x, así como también cifrado inalámbrico, movilidad segura y administración.

Ya que los puntos de acceso gordos funcionan como dispositivos independientes cada uno de ellos administra de forma autónoma todos los datos y funciones de control, es decir, cuentan con toda la inteligencia necesaria que les permite soportar transmisión de datos, seguridad y al mismo tiempo son robustos ya que administran diversas funciones como por ejemplo, mecanismos de cifrado, soporte para servidores de autenticación y de DHCP, traducción de direcciones de red (NAT) e incluso funciones de redes virtuales privadas (VPN).

Típicamente se concentran en un puerto de un switch con tecnología PoE (power over ethernet 802.3af) o como una aplicación separada de esta tecnología necesitando una fuente de poder externa para alimentar al punto de acceso.

Cuando los puntos de acceso gordos tienen fallas los administradores de éstos tienen que recolectar información de cada punto de acceso e investigar claramente de donde viene el problema y realizar los cambios necesarios en cada uno de ellos. Debido a que tienen un diseño autónomo son difíciles de administrar y se necesita estar actualizando el software o reiniciando parámetros de seguridad en cada uno de ellos, por lo que una red inalámbrica con este tipo de dispositivos resulta más costosa que el software y el hardware comprados inicialmente.

Muchos puntos de acceso de este tipo tienen dificultades manejando transmisiones porque no hay un monitoreo de conexiones central, estas limitaciones pueden ser problemáticas con aplicaciones como lo son voz sobre IP (VoIP), que requiere un ancho de banda estable mientras los usuarios

se muevan dentro de la cobertura, debido a su arquitectura autónoma, los puntos de acceso gordos no pueden manejar mejor estas dificultades y evitar los problemas que vienen cuando las conexiones se caen o son detenidas.

1.3.1.2 Puntos de acceso “delgados”.

Los puntos de acceso delgados son dispositivos con un controlador de administración centralizada por lo que no funcionan como unidades independientes y al mismo tiempo simplifican las responsabilidades de administración y tienen un menor costo, el controlador maneja los datos y las tramas que entran y salen de los puntos de acceso delgados.

Los puntos de acceso delgados pueden ser considerados como dispositivos transmisor-receptor con una interfaz Ethernet, su arquitectura es sencilla y son fáciles de configurar, por otro lado, intentan cumplir solamente con las funciones necesarias para ofrecer un rendimiento óptimo y valor financiero, mientras mueven todas las demás funciones de la WLAN al switch controlador. La Figura 1.2 muestra dos puntos de acceso delgados.

Algunas de las características de los puntos de acceso delgados son:

- Inservibles sin el switch controlador.
- No almacenan ninguna configuración.
- No almacenan llaves de cifrado.
- Rápido reemplazo.
- Administración y configuración centralizadas.
- Tolerantes a fallas.

Figura 1.2 Puntos de acceso delgados

1.3.2. Puntos de extensión (EP).

Los puntos de extensión son utilizados para aumentar el alcance de la cobertura de los puntos de acceso que se encuentran en la red inalámbrica, mucho más allá del alcance de éstos, de tal manera que van a funcionar como éstos últimos, pero sin la necesidad de estar cableados en la red local, lo que se puede observar en la Figura 1.3.

Los puntos de extensión vuelven a transmitir las señales que los dispositivos inalámbricos emiten al punto de acceso o a otro punto de extensión, por lo que los puntos de extensión pueden servir como puentes entre los puntos de acceso y los dispositivos inalámbricos lejanos ya que pueden encadenarse y pasar mensajes entre ellos.

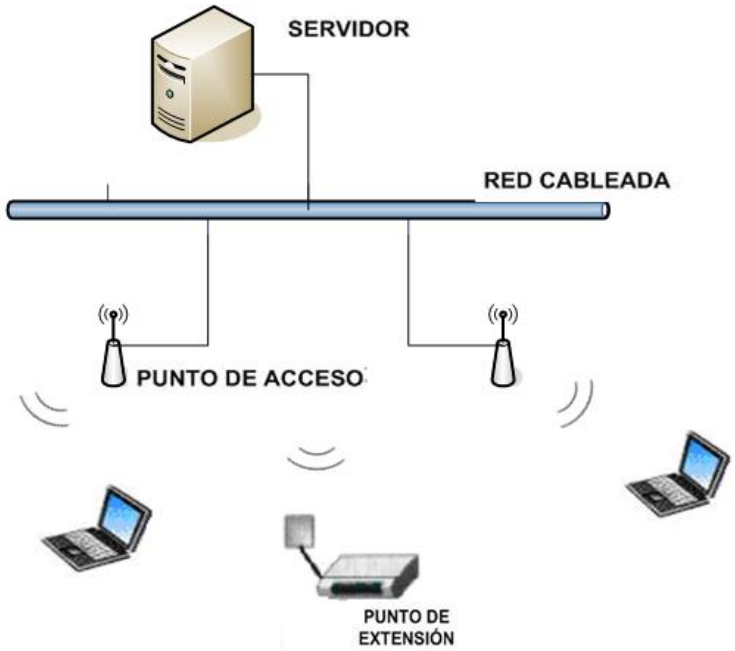


Figura 1.3 Conexión de un punto de extensión

1.3.3 Switch Controlador.

A medida que se agregan más estándares de redes inalámbricas y funciones de seguridad a un punto de acceso, los requerimientos de memoria, procesamiento y potencia aumentan. Esto hace que cada punto de acceso sea más “gordo” y más caro. Además, la administración de todas estas funciones en una red inalámbrica grande se podría convertir en algo complicado que consume mucho tiempo.

En la actualidad la tecnología se ha ido desarrollando, creando nuevos dispositivos con grandes beneficios, ahora en lugar de contar con puntos de acceso como dispositivo de intercambio entre las diferentes computadoras, surge un switch controlador el cual tiene la capacidad de crear túneles de seguridad IP para transportar los datos cifrados, utiliza el protocolo GRE (General Routing Encapsulation) entre éste y el punto de acceso, incluso si se encuentra en una ubicación remota, de esta manera los clientes inalámbricos se comunican directamente con los puntos de acceso, y se crea un túnel en el que se manda todo el tráfico a un switch controlador.

Esta jerarquía de punto de acceso, túnel y switch controlador, ofrece beneficios como seguridad, integridad, incrementa la escalabilidad y centraliza la administración, es decir, las funciones de administración y seguridad son manejadas por el switch controlador y ya no se necesitan en cada uno de los puntos de acceso. Lo anterior no solo baja el costo del punto de acceso, sino que además aumenta la velocidad de acceso a la red inalámbrica, ya que un switch está encargándose de lo que anteriormente se negociaba entre múltiples puntos de acceso. En vez de varios puntos de acceso gordos, una red inalámbrica consiste en muchos puntos de acceso delgados y un switch controlador debido a que éste último puede cumplir con funciones adicionales que a un punto de acceso gordo se le podrían hacer difíciles como por ejemplo:

• Protección contra intrusos: La administración centralizada es mucho más efectiva para defenderse de una amenaza de intrusión (un punto de acceso no autorizado que suplanta a un punto de acceso legítimo) que una implementación con puntos de acceso gordo.

• Auto asignación de canales: Si un punto de acceso gordo nuevo se conecta a la red, todos los puntos de acceso tienen que renegociar el canal que usará cada uno. Con un switch controlador, si se detecta un nuevo dispositivo primero alerta al administrador de red para verificar que sea un dispositivo legítimo, una vez verificado, el switch le permite el acceso a la red y automáticamente le reasigna otro canal a cada punto de acceso para evitar interferencias, ya que de otra manera no podrán mantener señales claras.

Un switch controlador tiene la capacidad de soportar los tipos de cifrado más avanzados y utilizar los estándares IEEE 802.11 a, b y g, así mismo dependiendo del tamaño del switch puede soportar una gran cantidad de puntos de acceso.

La Figura 1.4 muestra algunos switches controladores, el primero con mayor soporte de puntos de acceso que el segundo.

Figura 1.4 Switch controlador

Algunas desventajas que se pueden mencionar de estos equipos son:

- Cuando el switch controlador central llega a presentar una falla o apagarse completamente, toda la red inalámbrica dejará de dar servicio hasta que éste se encuentre en funcionamiento nuevamente.

- La cantidad de puntos de acceso que el swich controlador soporta depende de cada marca y por lo tanto el crecimiento de la misma puede llegar a ser limitado.

- En la mayoría de los casos una implementación con puntos de acceso gordos resulta más barata en una red pequeña que una solución con switches controladores, debido a que estos últimos son costosos.

1.3.4 Tarjetas de red.

Una tarjeta de red permite a un dispositivo electrónico acceder a la red y compartir recursos entre dos o más equipos (discos duros, cdrom, impresoras etc), o simplemente tener acceso a Internet.

Para las redes inalámbricas existen varios tipos de tarjetas, las que se usan para las computadoras portátiles se llaman PCMCIA (Personal Computer Memory Card International Association, asociación de la industria de fabricantes de hardware para computadoras portátiles) y para las PDA's (Personal Digital Assistant) y teléfonos celulares se llaman Compact Flash

(CF).

PC Card es la denominación que recibe la conexión PCMCIA de 16 bits de las computadoras portátiles. Para las PCMCIA de 32 bits se usa la denominación CARD BUS.

El tamaño de las tarjetas PCMCIA o PC Card es similar al de una tarjeta de crédito y tiene 68 conectores. Existen tres tipos de tarjetas:

- Tipo I, con un grosor de 3.3 mm la cual es utilizada para añadir memorias RAM o Flash RAM.
- Tipo II, con un grosor de 5 mm la cual es utilizada para adaptadores de red y fax módem, como la que se muestra en la Figura 1.5.
- Tipo III, con un grosor de 10.5 mm y es utilizada para conexiones de disco duro.

Características:

1. Tasa de transferencia de datos de hasta 11 ó 54 Mbps.

2. Compatible con la mayoría de los sistemas operativos.

3. Con características de Plug-and-Play para un fácil ajuste.

4. Interoperable con equipos compatibles con el estándar IEEE 802.11b y g.

5. Soporte para cifrado de datos con WEP, WPA y WPA2.

Figura 1.5 Tarjeta PCMCIA

Compact Flash fue originalmente un tipo de dispositivo de almacenamiento de datos, usado en dispositivos electrónicos portátiles. Principalmente existen dos tipos, CF I como la que se muestra en la Figura 1.6 y CF II, miden 43 mm y 36 mm y es ligeramente más grueso el segundo que el primero.

Hay tres velocidades de tarjetas: CF original, CF de Alta Velocidad y CF 3.0 más rápida que los anteriores. Las tarjetas CF pueden ser usadas directamente en una ranura PC Card con un adaptador enchufable y con un lector para cualquier número de puertos comunes como USB o FireWire.

Las tarjetas CF son mucho más compactas que las tarjetas de memoria PCMCIA de Tipo I, excepto por su grosor que es el mismo que las tarjetas PCMCIA Tipo I y Tipo II respectivamente.

Figura 1.6. Tarjeta CompactFlash de Tipo I de alta velocidad de 32MB

1.3.5. Antenas.

Una antena es un dispositivo que ayuda a difundir o recoger ondas radioeléctricas, ya que éstas convierten las señales eléctricas en ondas electromagnéticas y viceversa.

Las antenas sirven para aumentar la capacidad de transmisión y recepción de los dispositivos inalámbricos, además de que se utilizan para que la señal llegue hasta donde se tenga planeado con una buena calidad.

La comunicación puede ser bidireccional si se realiza en ambas direcciones, pero si la comunicación no se realiza simultáneamente en ambos sentidos se denomina comunicación semiduplex.

Las antenas tienen dos tipos de aperturas, la vertical y la horizontal. La apertura es cuando el haz de la antena se abre y el haz recibido o emitido se determina ya sea horizontalmente o verticalmente.

La apertura vertical se debe tomar en cuenta si existe mucho desnivel entre los puntos que se van a unir de forma inalámbrica, si el desnivel es demasiado la antena debe tener mucha apertura vertical, las antenas que tienen mucha ganancia tienen menos apertura vertical.

Las antenas se pueden dividir en tres: direccionales, omnidireccionales y sectoriales.

1.3.5.1 Antenas direccionales (directivas).

Este tipo de antenas enfocan toda la señal que aplica la tarjeta o punto de acceso a una dirección concreta, lo cual depende del modelo y de las características de la antena.

Así mismo envían la información a una parte de la zona de cobertura en un ángulo determinado, razón por la cual el alcance de éstas es mayor, la principal desventaja que tienen es que fuera del radio de cobertura de la

antena los dispositivos inalámbricos no escuchan ni envían nada y por lo tanto no pueden establecer comunicación.

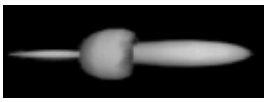
Con estas antenas se puede orientar la señal con un haz de largo alcance pero estrecho. Dicho alcance se determina por medio de los decibeles de ganancia que tengan las antenas, así como de la potencia de emisión del punto de acceso emisor y de la sensibilidad de receptor.

Su apertura oscila entre los 40˚ y 80˚, normalmente tienen las mismas aperturas horizontales que verticales.

Se utilizan para unir dos puntos que se encuentran a una distancia larga o para enlazar un punto que tenga una antena omnidireccional.

A

B



C

Figura 1.7 Antenas direccionales

La Figura 1.7 muestra antenas de tipo direccional. Las figuras A y B son de 2.4 GHz las cuales extienden la red inalámbrica para la conexión entre edificios, la figura C muestra el patrón de radiación de este tipo de antenas.

1.3.5.2 Antenas Omnidireccionales.

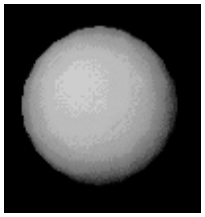
Este tipo de antenas de forma teórica envían la información en los 360˚, es decir, orientan la señal en un haz amplio y de corto alcance razón por la cual se puede tener comunicación no importando el punto en el que esté.

El alcance de este tipo de antenas es menor que el de las direccionales pero los factores que determinan su alcance son los mismos que para las antenas direccionales. Cabe mencionar que aunque una antena direccional y una omnidireccional tengan los mismos decibeles, la primera va a dar mucho más cobertura que la segunda.

Una antena de éstas trabaja horizontalmente en todas direcciones, ya que su apertura es de 360˚ y se utiliza para dar una señal extensa en los alrededores del punto de acceso.

A

B



C

Figura 1.8 Antenas Omnidireccionales.

La Figura 1.8 muestra dos antenas onmidireccionales. En la figura A se observa una de 5 dBi de ganancia, en la figura B se observa una de 4 dBi. El patrón de radiación se muestra en la figura C.

1.3.5.3 Antenas sectoriales.

Este tipo de antenas es una mezcla de las antenas direccionales y omnidireccionales y por lo tanto tiene un costo mayor que las dos. Su alcance se encuentra entre los dos tipos, es decir, su alcance es mayor que una antena omnidireccional pero menor que la direccional.

Para lograr tener un largo alcance y una cobertura de 360˚ se necesita tener tres antenas sectoriales de 120˚ o 4 sectoriales de 90˚, ya que su apertura es entre los 90˚ y 180˚, se utilizan cuando se quiere llegar a grandes distancias y tener una amplia cobertura.

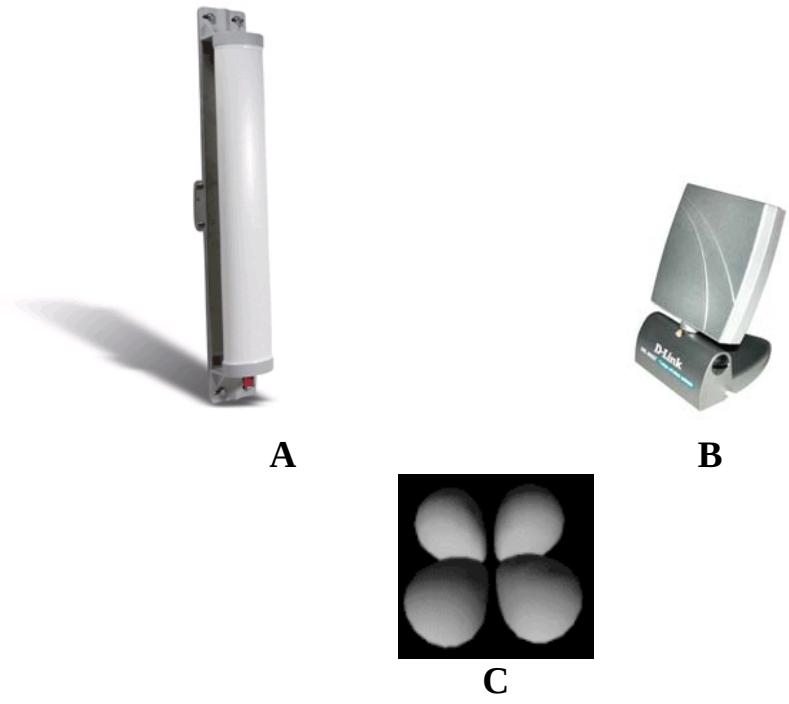


Figura 1.9 Antenas de tipo sectorial

En la Figura 1.9 se observan antenas sectoriales con diferente ganancia, la antena de la Figura A tiene una ganancia de 12 dBi y la antena de la Figura B de 6 dBi. La figura C muestra el patrón de radiación de este tipo de antenas.

1.4 Topologías de redes inalámbricas.

1.4.1 Punto a punto (ad-hoc).

Las redes inalámbricas se construyen utilizando dos topologías básicas, que son infraestructura y ad-hoc.

Las redes ad-hoc, es la topología más sencilla ya que en ella los propios dispositivos inalámbricos crean la red y no existe ningún controlador central ni puntos de acceso ya que cada dispositivo se comunica directamente con los demás dentro de la red como se muestra en la Figura 1.10. Muchas de las operaciones que controla el punto de acceso, como la señalización y la sincronización, en esta topología son manejadas por un equipo de cómputo. La red ad-hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

En este tipo de redes, el único requisito deriva del rango de la señal, ya que es necesario que las terminales móviles estén dentro de este rango para que la comunicación sea posible, además de que todos los equipos conectados deben estar configurados con el mismo BSSID (Basic Service Set Identifier).

Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Algunos ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad-hoc serían un domicilio sin red con cable o una sala de conferencias donde los usuarios utilicen sus computadoras con regularidad para intercambiar información entre ellas.

Figura 1.10 Imagen de una topología ad-hoc

1.4.2 Infraestructura.

En esta topología existe un nodo central llamado punto de acceso, el cual es el enlace para todos los demás nodos e incorpora dispositivos inalámbricos. Dicho punto de acceso une la red inalámbrica con la red LAN cableada, así mismo es el controlador central y tiene configurado el SSID o nombre de la red al que los clientes se asocian. Todos los nodos deben de estar dentro del radio de cobertura del punto de acceso para poder establecer comunicación.

El punto de acceso es el que coordina la transmisión y recepción de los diferentes dispositivos con tecnología inalámbrica dentro del rango que éste puede cubrir, como se observa en la Figura 1.11.

La extensión y la cantidad de dispositivos que puede aceptar dependen del estándar de conexión inalámbrica utilizado, además de las características del producto.

En este tipo de topología pueden existir varios puntos de acceso para incrementar la extensión de la cobertura o uno solo en áreas pequeñas.

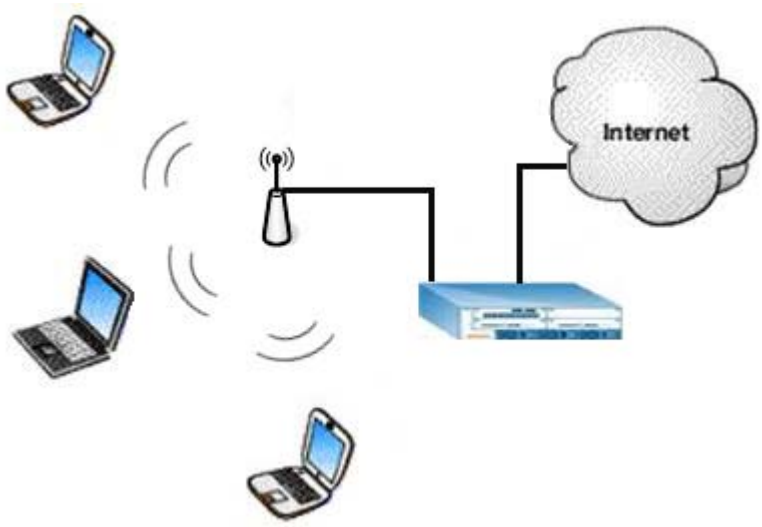


Figura 1.11 Imagen de una topología infraestructura

1.4.2.1 Funcionamiento de la topología Infraestructura.

El dispositivo inalámbrico identifica las redes inalámbricas disponibles para la conexión. Dicho proceso se lleva a cabo por medio del control de las tramas de señalización que vienen de los puntos de acceso, o por medio del sondeo activo de una red específica.

El dispositivo elige una red inalámbrica entre las que se encuentran disponibles y se asocia ante ésta. Después de que este proceso termina, comienza la autenticación que es cuando el dispositivo inalámbrico y el punto de acceso se aceptan mutuamente.

Con la asociación el punto de acceso y el dispositivo inalámbrico hacen un intercambio de información, el punto de acceso utiliza dicha información para enviar a los posibles puntos de acceso, que también pertenecen a la red inalámbrica, cuál es la ubicación actual del dispositivo inalámbrico que se quiere conectar. Hasta que haya finalizado la autenticación el dispositivo inalámbrico puede recibir o transmitir tramas en la red.

En este tipo de topología el tráfico de red procedente de los dispositivos inalámbricos pasa primero por un punto de acceso para poder llegar a otra red, ya sea cableada u otra inalámbrica. Así mismo el acceso a la red se da por medio de un protocolo que detecta las portadoras ya que los dispositivos inalámbricos están escuchando las transmisiones de otros por un tiempo especificado antes de transmitir ellos, con lo cual se evitan colisiones. En esta topología el transmisor o el receptor es siempre un punto de acceso.

Como es posible que dos estaciones que se encuentren dentro del alcance del punto de acceso no se escuchen y con ello puedan llegar a ocurrir colisiones, se incluye un intercambio de paquetes antes de comenzar la transmisión. Si un dispositivo no puede escuchar lo que otros dispositivos transmiten puede escuchar la transmisión que manda el punto de acceso y con ello evitar mandar algo.

Para que exista transmisión fluida entre el punto de acceso y los clientes debe existir una señal potente, un sondeo para buscar puntos de acceso y un proceso de reasociación para poder conectarse a un punto de acceso diferente en caso de perder la conexión.

Así mismo la sincronización entre los dispositivos inalámbricos se da por medio de las tramas de señalización que el punto de acceso manda periódicamente lo cual sirve para comprobar el estado del dispositivo receptor.

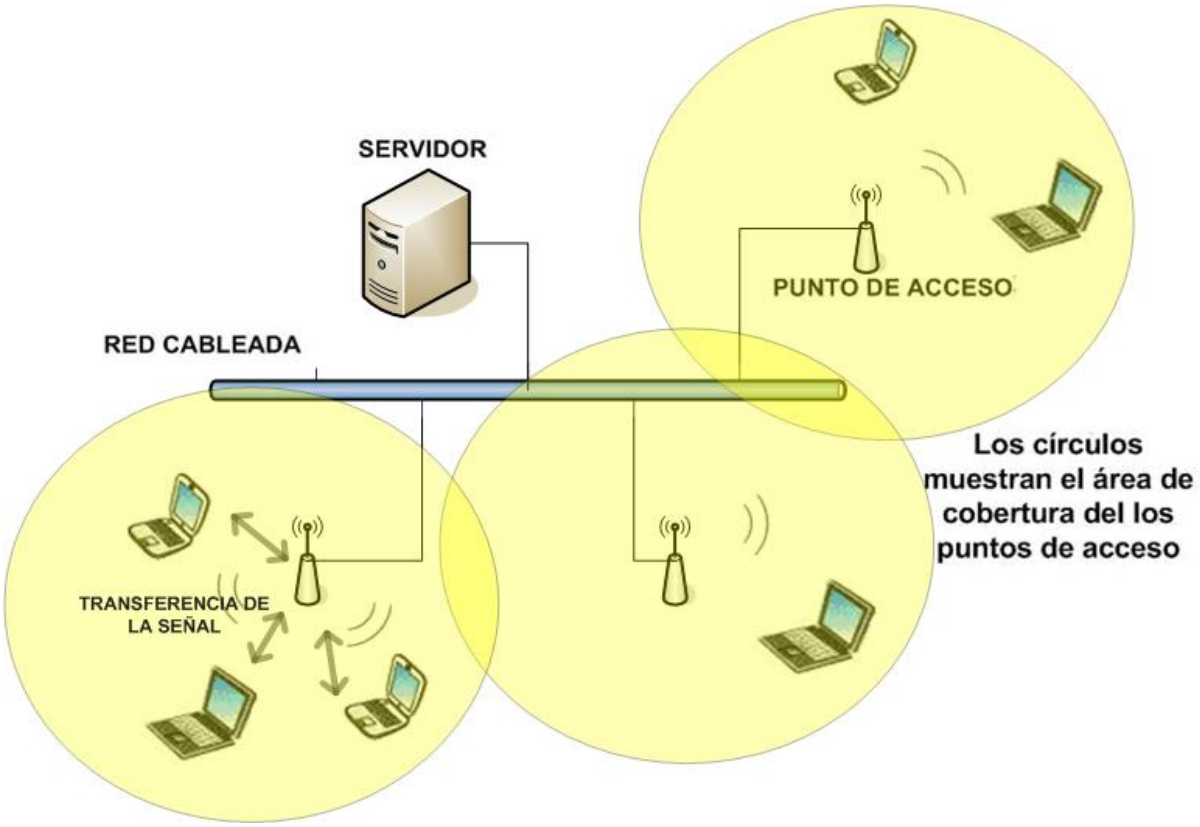


Figura 1.12 Funcionamiento Topología Infraestructura

En la figura 1.12 se muestra el funcionamiento de una red inalámbrica con topología infraestructura. Los dispositivos se comunican de forma inalámbrica con el punto de acceso el cual está conectado a la red cableada. Los dispositivos pueden mantener la conexión de red mientas se encuentren en el área de cobertura de los puntos de acceso.

1.5 Beneficios y aplicaciones de las redes inalámbricas.

Las redes locales inalámbricas dan ventajas de conectividad sin necesidad de usar cables, ya que en algunos lugares el cable resulta inadecuado como puede ser en los edificios históricos o en las naves industriales, en éstas últimas por cuestiones de seguridad ya que los cables pueden ocasionar accidentes o puede ser que se necesite espacio libre para el transporte interno.

Por otra parte con este tipo de redes se tiene mayor libertad de movimiento, la reubicación de terminales es más sencilla y su instalación es rápida.

Las redes inalámbricas se pueden ver como un complemento a las redes cableadas ya existentes y no como la sustitución de éstas. Cuando una infraestructura de red sea sólida, fija, difícil de movilizar y costosa de cambiar, se puede complementar con una red inalámbrica la cual puede moverse con el usuario y cambiar así como la empresa u organización lo haga.

Los usuarios móviles se han incrementado en los últimos años debido a la aparición en el mercado de dispositivos inalámbricos como lo son las tarjetas de red inalámbricas para las computadoras portátiles o los PDA's Además de que existe una gran necesidad de tener acceso a red la mayoría del tiempo, por lo que en los lugares públicos se están instalando redes inalámbricas para dar servicios a los visitantes.

Actualmente las redes locales inalámbricas se encuentran instaladas principalmente en lugares como restaurantes, bancos, fábricas, hospitales y estaciones de transporte, debido a las necesidades principalmente de sus trabajadores y usuarios.

Cuando las empresas, universidades y hoteles llegan a tener eventos o congresos y los participantes o visitantes necesitan una conexión a red, la mejor opción para ello es instalar una red inalámbrica que les proporcione el servicio y al mismo tiempo que sea independiente de su red cableada para evitar problemas de seguridad, además que la mayoría de los lugares no tienen suficientes puntos de red cableados para proporcionar todos los servicios necesarios.

CAPÍTULO 2

ESTÁNDAR IEEE 802.11

2.1 Introducción.

Este capítulo tratará de explicar el estándar IEEE 802.11, sus orígenes, su arquitectura, sus tres principales tecnologías que son 802.11a, 802.11b y 802.11g así como sus diversas especificaciones.

Se abarcarán también los tipos de seguridad básica que las redes inalámbricas pueden implementar para tratar de lograr un desempeño sin intrusiones.

Dichos esquemas de seguridad son WEP, WPA y WPA2, de los cuales se explicará la forma en la que realizan el cifrado, descifrado y la autenticación de usuarios.

El estándar 802.11 trata de normalizar el uso de la redes inalámbricas de área local, uno de sus principales objetivos es que exista una escalabilidad e interoperabilidad entre los productos inalámbricos, es decir, que la tecnología de los dispositivos inalámbricos que se encuentra en el mercado comercial y que es desarrollada por distintos fabricantes sea compatible entre sí, y con ello la implementación de una red inalámbrica sea más fácil.

2.2 Tecnología del estándar IEEE 802.11.

El estándar 802.11 es un grupo de especificaciones desarrolladas por el IEEE (Instituto de Ingeniería Eléctrica y Electrónica) para redes inalámbricas. Estas especificaciones definen una interfaz para que exista una comunicación entre un cliente inalámbrico y un punto de acceso o entre dos o más clientes inalámbricos a través del aire.

Los orígenes de este estándar se remontan al año de 1990 cuando se forma el comité IEEE 802.11 con el objetivo de tratar de realizar una norma para el funcionamiento de las redes inalámbricas. El 1994 se da a conocer el primer borrador pero es hasta 1999 que la norma fue ratificada.

La versión original fue dada a conocer en junio de 1997, la cual especifica dos velocidades teóricas de transmisión de 1 y 2 Mbps. Dichas velocidades se alcanzaban por medio de la transmisión de señales infrarrojas en la banda ISM de 2.4 GHz. El estándar 802.11 utiliza el rango de frecuencias de 2.4 GHz, y la divide en canales (11 para EE.UU. y 9 para Europa), definiendo unos anchos de banda de 11, 5, 2 y 1 Mbps por canal, como se observa en la Tabla 2.1.

Número de Canal	Frec. EE.UU.	Frec. Europa
1	2.412	No Disponible
2	2.417	No Disponible
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462
Frecuencia en GHz.		

Tabla 2.1 Bandas ISM

Una debilidad del estándar original fue que como se dejó mucha libertad de implementación a los proveedores de equipos se presentaron dificultades de interoperabilidad entre equipos de diferentes marcas. Lo anterior fue corregido en el estándar 802.11b, el cual fue el estándar que más aceptación logró.

El IEEE 802.11 ha estado en constante desarrollo, ya que es el encargado de realizar los estándares para las redes de área local inalámbricas, así como proponer y definir nuevas mejoras y apéndices al mismo.
La familia de especificaciones del estándar 802.11 para la tecnología WLAN se enlista a continuación:

- 802.11a Estándar para redes inalámbricas de alta velocidad para la banda de 5 GHz. soporta hasta 54 Mbps.

- 802.11b Estándar de redes inalámbricas para la banda de 2.4 GHz. soporta hasta 11 Mbps.

- 802.11c Procedimientos de operación de puentes y es parte del estándar 802.11d.

- 802.11d Procedimientos para configurar dispositivos automáticamente para que cumplan con las regulaciones de radiotransmisión locales.

- 802.11e Dirige la calidad de los requisitos de servicios para todas las interfaces de radio de redes inalámbricas IEEE.

- 802.11f Define comunicaciones del punto de acceso interno para facilitar redes inalámbricas múltiples distribuidas por proveedores.

- 802.11g Establece una técnica de modulación adicional para la banda de 2.4 GHz. Soporta velocidades de hasta 54 Mbps.

- 802.11h Define la gestión del espectro de la banda de 5 GHz.

- 802.11i Dirige las debilidades de la seguridad actual tanto para los protocolos de cifrado como de autenticación. El estándar abarca los protocolos 802.1x, TKIP y AES.

- 802.11j Extensión de estándar hecha para Japón.

- 802.11k Realces de las medidas de radio.

- 802.11m Mantenimiento del estándar.

- 802.11n Proporciona mejoras de mayor capacidad de proceso. Se pretende que proporcione velocidades de hasta 500 Mbps.

- 802.11p Acceso inalámbrico para los vehículos, básicamente ambulancias o autobuses.

- 802.11r Roaming rápido.

- 802.11s Tecnología de redes MESH.

- 802.11T WPP (Wíreless Performance Prediction) Método de prueba y métrica.

- 802.11u Relación con las redes que no son del 802.11 por ejemplo celulares.

- 802.11v Administración de redes inalámbricas.

- 802.11w Administración de tramas.

Actualmente este protocolo es conocido como Wi-Fi y es el resultado de lo que anteriormente se conocía como alianza para la compatibilidad Ethernet inalámbrica a la que más tarde se utilizó para describir a los equipos con el significado de "fidelidad inalámbrica".

Wi-Fi surgió como resultado de una decisión tomada en 1985 por la FCC para abrir varias bandas del espectro inalámbrico para su uso sin necesidad de una licencia gubernamental. Estas bandas, denominadas "bandas de basura" ya se habían asignado a equipos como los hornos de microondas. Para trabajar con ellas, los dispositivos necesitan utilizar la tecnología de "espectro disperso". Esta tecnología propaga una señal de radio en un amplio rango de frecuencias permitiendo que la señal sea menos susceptible de interferir y difícil de interceptar.

2.2.1 Arquitectura IEEE 802.11.

Una red de área local 802.11 está basada en una arquitectura celular, en la que el sistema está dividido en celdas llamadas BSS (Basic Service Set), dichas celdas son controladas por un punto de acceso.

Una red inalámbrica puede funcionar con una sola celda y un solo punto de acceso o sin éste último, pero la mayoría de las instalaciones de redes inalámbricas tienen varias celdas y los puntos de acceso están conectados a un backbone llamado DS (Distribution System) el cual es normalmente Ethernet.

La interconexión de redes inalámbricas incluyendo las diferentes celdas, sus respectivos puntos de acceso y sistemas de distribución se pueden ver como una sola red 802 y es llamada en el estándar como ESS (Extended Service Set).

El IEEE 802.11 define la operación de una red inalámbrica en las capas Física y Enlace de Datos del modelo OSI. La capa Física soporta: infrarrojo, modulación por saltos de frecuencia (FHSS), espectro disperso por secuencia directa (DSSS) y modulación por división ortogonal de frecuencia (OFDM), la capa de Enlace de Datos hace un manejo para control de enlace lógico y control de acceso al medio.

Así como la capa MAC desempeña la funcionalidad del estándar, también proporciona fragmentación, retransmisión de paquetes y reconocimiento. Define el método como método de acceso la función de coordinación

distribuida que es el método básico de acceso y es un mecanismo CSMA/CA (Carrier Sense Múltiple Access with Colission Avoidance).

Un protocolo CSMA trabaja de la siguiente forma: una estación quiere transmitir, si el medio está ocupado, la estación emisora deja su transmisión para otro momento, si el medio está libre entonces puede realizarla.

Este protocolo permite transmitir con una demora mínima, aunque puede llegar a ocurrir una colisión porque la estación puede ver que el medio está libre cuando no es cierto. Cuando ocurre lo anterior, la capa MAC puede retransmitir los paquetes por si misma, lo cual causa un retraso significativo.

CSMA por si solo no puede ser utilizado en una red inalámbrica debido a que se necesita una implementación radio Full Dúplex, que es capaz de transmitir y recibir al mismo tiempo, lo que incrementaría el precio de los dispositivos, además de que en una red inalámbrica no se puede asumir que todas las estaciones se están escuchando unas a otras.

Para corregir lo anterior el estándar 802.11 utiliza la Anulación de Colisiones (Collision Avoidance, CA) junto con un esquema de admisión positiva, el cual funciona de la siguiente manera:

Una estación que quiere transmitir analiza el medio, si éste está ocupado entonces retrasa la transmisión; si está libre en un tiempo específico entonces la estación puede transmitir.
La estación receptora checa el paquete de identificación de la estación emisora y si el medio está libre el receptor manda un paquete de aceptación ACK, este paquete le indica al emisor que no hay peligro de colisión. Si el emisor no recibe éste, el ACK volverá a mandar su paquete de identificación hasta que el receptor le mande su ACK o hasta que se de por vencido después de cierto número de retransmisiones.

2.2.2 Espectro disperso.

El espectro disperso forma parte del estándar IEEE 802.11, esta tecnología trabaja dividiendo las señales informativas en varias frecuencias, que pertenecen a la banda ISM.

Dentro de las aplicaciones que tiene el espectro disperso está: GPS (sistemas de posicionamiento satelital) telecomunicaciones móviles 3G, redes inalámbricas con los estándares 802.11a, 802.11b y 802.11g y Bluetooth.

Algunas de las ventajas para la transmisión en espectro disperso son las siguientes:

- Las señales en espectro disperso son altamente resistentes al ruido y a la interferencia.

- Las señales en espectro disperso son difíciles de interceptar.

- Una transmisión de este tipo suena como un ruido momentáneo, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.

- Las transmisiones en espectro disperso pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

Las tres técnicas más utilizadas de espectro disperso en este estándar son:

- Modulación por saltos de frecuencia (FHSS).

- Modulación de secuencia directa (DSSS).

- Multiplexación por división en frecuencias ortogonales (OFDM).

2.2.2.1 DSSS (Direct Sequence Spread Spectrum).

El espectro disperso por secuencia directa es una tecnología de transmisión utilizada principalmente en redes inalámbricas en donde una señal de datos en la estación trasmisora es combinada con una secuencia mayor de bits de datos, es decir, genera un patrón de bit redundante por cada bit que es transmitido. Este bit es llamado *chipping code*, su longitud tiene una probabilidad mayor de que los datos que se lleguen a perder puedan ser recuperados, ya que si durante la transmisión de datos uno o más bits en el *chipping code* son dañados se pueden aplicar técnicas estadísticas a las señales de radio que permiten la recuperación de los datos sin la necesidad de retrasmitir la información.

Esta técnica no envía la información por medio de varias frecuencias sino por medio de un transmisor, solamente el receptor puede descifrar la información porque conoce el algoritmo de dichos bits adicionales. Debido a lo anterior se puede alcanzar la velocidad de transmisión de datos de 10 Mbps y una distancia entre trasmisores de 150 m.

La secuencia de Barker (también llamado código de dispersión o PseudoNoise) es la utilizada para modular los bits, es rápida y está diseñada para que aparezca aproximadamente la misma cantidad de 1’s que de 0’s.
En DSSS se representa cada 0 y cada 1, respectivamente, por los símbolos -1 y +1. En la figura 2.1 se muestra dicha secuencia.

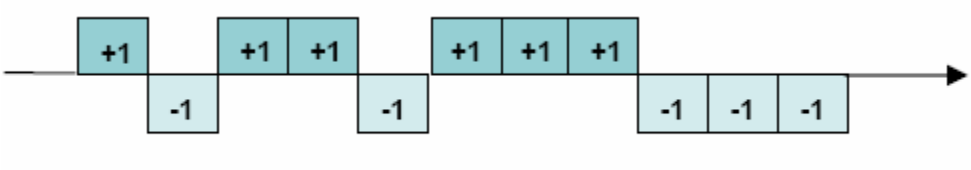


Figura 2.1 Secuencia de Berker.

Para los receptores que no conocen el algoritmo, esta tecnología la toman como una señal de ruido con un ancho de banda con bajo poder por lo cual es ignorada.

2.2.2.2 FHSS (Frequency Hopping Spread Spectrum).

El espectro disperso por salto de frecuencia es una técnica de modulación de señal que se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia en sincronía con el transmisor. Los receptores no autorizados escucharán una señal ininteligible equivalente a la recepción de ruido de corta duración, si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits.
Este método de transmisión de señales 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 de una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo.

El orden en los saltos en frecuencia que el emisor debe realizar se puede observar en la figura 2.2, y viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que son conocidas solamente por el transmisor y el receptor siempre dentro de la banda de los 2.4GHz.

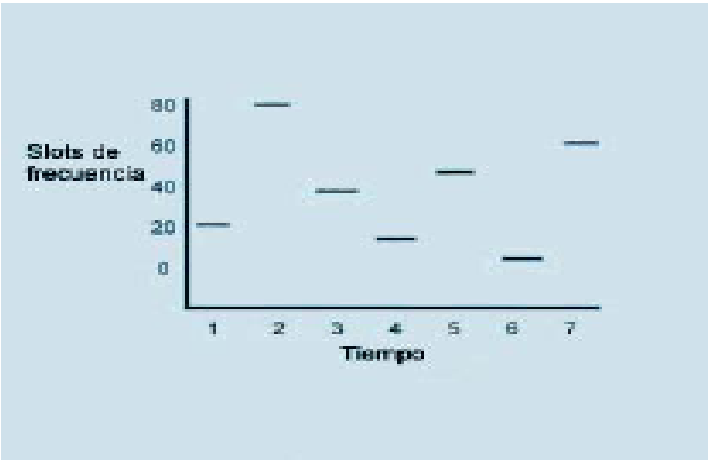


Figura. 2.2 Secuencia Pseudoaleatoria.

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

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.

FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tienen una cantidad de receptores diseminados en un área relativamente cercana al punto de acceso.

2.2.2.3 OFDM (Orthogonal Frequency Division Multiplexing).

La modulación por división ortogonal de frecuencia es también llamada modulación por multitono discreto, en inglés Discreet Multitone Modulation (DMT), es un método de modulación digital en el cual cada señal se separa en varios canales de banda angosta a diferentes frecuencias. La tecnología se concibió inicialmente en los años 60 y 70 durante investigaciones para minimizar la interferencia entre canales cercanos uno al otro en frecuencia.

En algunos aspectos, el OFDM es similar a la múltiplexación por división de frecuencia tradicional (FDM), que permite transmitir grandes cantidades de datos digitales sobre una onda de radio, con la diferencia básica de la forma en que las señales se modulan y demodulan. OFDM 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) hacia el receptor en diferentes frecuencias.

La tecnología es utilizada para el envío de señales de televisión digital, y también se considera como una forma de obtener transmisión de datos a alta velocidad sobre las líneas convencionales de teléfono.

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, lo cual proviene del inglés Coded OFDM.

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras equiespaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la transformada discreta de Fourier directa e inversa.

En la Figura 2.3 se puede observar 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.

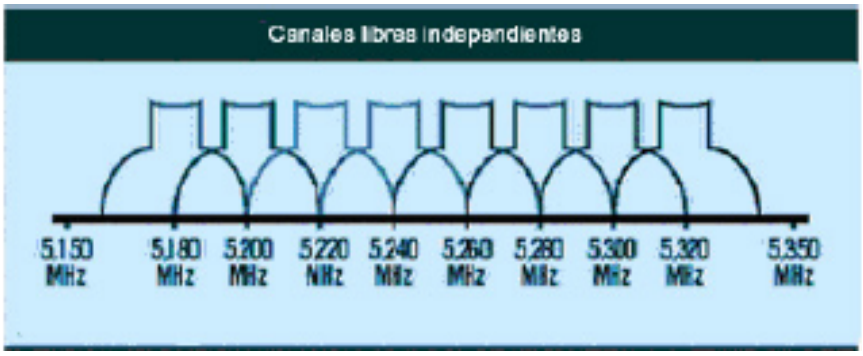


Figura 2.3 Canales del código OFDM

De estos canales, el COFDM 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 (Binary Phase Shift Keying) usado para la modulación a 125 Kbps de datos por canal, es decir, una tasa de datos de 6 Mbps.

- QPSK (Quadrature Phase Shift Keying) dobla la cantidad de datos

modulados produciendo una tasa de datos de 12 Mbps.

- 16-QAM (16 Level Quadrature Amplitude Modulation), logra una tasa de datos de 24 Mbps (modulando 4 bits por hertz).

- 64-QAM (64 Level Quadrature Amplitude Modulation) obtiene una tasa de datos de 54 Mbps (produce 8 bits por ciclo o 10 bits por ciclo).

OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal. 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.

Entre los sistemas que usan la modulación OFDM destacan:

- La televisión digital terrestre, también conocida como TDT.

- La radio digital.

- La radio digital de baja frecuencia.

- El protocolo de enlace ADSL.

- El protocolo de red de área local IEEE 802.11a/g.

- El sistema de transmisión inalámbrica de datos 802.16 ó WiMAX.

2.2.3 Estándar 802.11a.

El estándar 802.11a surgió en 1999, cuando la IEEE lo aprobó, pero fue hasta el 2001 que hizo su aparición en el mercado. Éste estándar transmite a una banda de frecuencia de 5 GHz y utiliza el esquema de modulación OFDM,

con lo que incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento.

La tecnología 802.11a utiliza células de RF más pequeñas (distancias efectivas más cortas) y un consumo de energía más alto. Los productos IEEE 802.11a sin soluciones de chip de banda doble, es decir, que soporten tecnología 802.11a/g, no ofrecen compatibilidad con versiones anteriores.

La banda de 5 GHz (banda UNII) está formada por tres sub-bandas, UNII1 (5.15 – 5.25 GHz), UNII2 (5.25 – 5.35 GHz) y UNII3 (5.725 – 5.825 GHz). Cuando se utilizan tanto UNII1 como UNII2, tiene 12 canales solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2.4 GHz (300 MHz por 83.5 MHz). Así pues, una red inalámbrica basada en el estándar 802.11a puede soportar aplicaciones importantes que implican vídeo, voz, y la transmisión de imágenes y archivos grandes, lo que hace que se pueda manejar una concentración más alta de los usuarios, a velocidades de datos más altas en alcances cortos ofreciendo mayor rendimiento de procesamiento total.

El sistema OFDM provee a las redes inalámbricas una transferencia de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Los productos IEEE 802.11a deben de ser capaces de transmitir y recibir datos de 6, 12 y 24 Mbps.

Las velocidades teóricas de transmisión del estándar 802.11a son las siguientes:

- Exteriores valor máximo **30 metros** a 54 Mbps
- Exteriores valor mínimo **300 metros** a 6 Mbps
- Interiores valor máximo **12 metros** a 54 Mbps
- Interiores valor mínimo **90 metros** a 6 Mbps

El uso de 802.11a también puede evitar la interferencia que existe en los dispositivos Bluetooth y los teléfonos que funcionan en la frecuencia de 2.4 GHz. Sin embargo, dado que utiliza la banda de 5 GHz, restringe el uso de los

equipos 802.11a únicamente a puntos de línea de vista, con lo que se hace necesaria la instalación de un mayor número de puntos de acceso. Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas

802.11a no es compatible con las redes 802.11b o 802.11g. Es decir un usuario equipado de una tarjeta 802.11b o 802.11g no podrá interconectar directamente a un punto de acceso 802.11a.

2.2.4 Estándar 802.11b.

EL 802.11b fue liberado en Septiembre de 1999 por el IEEE y tuvo una rápida aceptación como tecnología de redes inalámbricas debido a que hubo un incremento de velocidad de transmisión de datos con respecto al estándar original, así como también hubo una reducción considerable en los precios de los productos.

En sus inicios el estándar proponía que los equipos tuvieran una tarjeta de red con una dirección MAC única con el objeto de que el punto de acceso conociera esa dirección MAC y solo establecer la comunicación con las direcciones que tenía registradas. Lo anterior se modificó debido al incremento de usuarios de una red inalámbrica y al aumento de equipos que la conforman.

Este estándar define dos componentes; una estación inalámbrica que puede ser una PC o una computadora portátil que contengan una tarjeta de red inalámbrica y un punto de acceso, dicho punto actúa como un puente entre la estación inalámbrica y la red cableada.

802.11b trabaja en la banda de 2.4 GHz y puede ser implementada en cualquier país e incluye tanto redes ad-hoc como ESS (Extended Services Set). Esta banda es compartida con teléfonos inalámbricos, hornos de microondas, dispositivos Bluetooth, etc. La desventaja de utilizar este tipo de

bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión, dichos errores provocan que los paquetes de información sean reenviados una y otra vez.

Un error del 50% ocasiona que se reduzca en dos terceras partes la transmisión real de datos, por lo que la velocidad máxima teórica no es tal en realidad.

Tiene una velocidad de transmisión de 11 Mbps y el modo de transmisión de datos se realiza por medio de DSSS debido a que esta forma de modulación maneja bien las señales débiles y los datos no tienen que ser retransmitidos.
Para poder disminuir errores de interferencia el 802.11a y 802.11b reducen la velocidad de transmisión de la capa física, por lo que el 802.11b tiene las velocidades de transmisión de información 5.5, 2 y 1 Mbps. La velocidad teórica es alcanzable en un ambiente sin interferencia y a corta distancia. Si se tuviera una banda más ancha, más canales de radio pueden estar en ella sin tener interferencia.

Así mismo el estándar utiliza el método de acceso al medio CSMA/CA como en el estándar original. Debido a este protocolo la máxima velocidad que una aplicación puede tener es aproximadamente 5 Mbps.

Los dispositivos que utilizan este estándar aparecieron en el mercado de forma muy rápida debido a la técnica de modulación DSSS. Técnicamente 802.11b utiliza CCK (Complementary Code Keying) como técnica de modulación, ésta es una variación de CDMA.

La mayoría de las redes bajo el estándar 802.11b pueden alcanzar distancias de 100 metros en interiores y con una mayor potencia se puede extender esa longitud, aunque en interiores la potencia de transmisión, las paredes y otros objetos pueden interferir la señal.

2.2.5 Estándar 802.11g.

En Junio de 2003, se ratificó un tercer estándar, el 802.11g. Éste utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b, de modo que los dispositivos 802.11b y 802.11g puedan coexistir bajo la misma red) pero opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24.7 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a, lo que permite dar servicio a más la cantidad de usuarios y extender el uso de las redes 802.11 a servicios bastante demandados como la transmisión inalámbrica de video-multimedia y la difusión de MPEG.

Utiliza los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.
Gran parte del proceso del diseño de este estándar fue el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar b la presencia de nodos bajo el estándar g reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redunda en un menor número de usuarios inalámbricos de alta velocidad.

Una de las grandes ventajas de 802.11g es que gestiona mejor el nivel de reflexión de la señal, es decir, las señales de radio rebotan en diferentes entornos como suelos, metal, e incluso el aire, en diferentes ángulos y velocidades. Un receptor debe recuperar todos y cada uno de esos ‘rebotes’ de una misma señal que llegan en momentos diferentes, y recomponer ese ‘paquete’ de datos en uno único.

802.11g (al igual que 802.11a) divide el espectro de forma que permite a los

receptores manejar estos ‘rebotes’ de una forma muy simple pero mucho más efectiva que 802.11b.

2.3 Seguridad.

El problema de la seguridad en las redes es un tema importante debido al gran crecimiento tecnológico y a la necesidad de proteger la información. El futuro desarrollo de los sistemas de seguridad se ha tornado en un asunto necesario para las naciones del mundo.

Algunos aspectos que proporciona el desarrollo de sistemas de seguridad para redes inalámbricas son:

- Asegurar la invulnerabilidad de la información de las personas, de sus derechos y garantías.

- Otorgar seguridad a las redes que promueven el futuro desarrollo y evolución del comercio digital facilitando el desarrollo de la infraestructura de la información. Para el caso de RIU, asegurar la información de la comunidad universitaria.

En este sentido, para poder considerar una red inalámbrica como segura, debería de cumplir por lo menos con los siguientes requisitos:

- No debe ser abierta, es decir que no permita el libre acceso a todo el público en general, ya que clientes no autorizados pueden acceder a la red y causar daños serios como propagación de virus, instalación de sniffers y por lo tanto robo, modificación o falsificación de información.

- Utilizar algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.

Dentro de los esquemas de seguridad que pueden ser implementados en una red inalámbrica, se encuentran: filtrado por direcciones MAC, uso de VPN, WEP, WPA y WPA2.

A continuación de describe el filtrado por direcciones MAC y el acceso a una red inalámbrica por medio de VPN, dichos métodos no se consideraron para ser aplicados en la RIU por ser difíciles de implementar y por tener muchas desventajas.

Filtrado por Direcciones MAC.

El Filtrado de Direcciones MAC consiste en registrar en los puntos de acceso la dirección MAC de todas las máquinas que pueden acceder a una red inalámbrica y con ello lograr la autenticación de usuarios.

Dentro de las ventajas de utilizar este método se encuentra que es sencillo de implementar por lo que normalmente es utilizado en redes pequeñas o caseras.

Algunas de las desventajas de este método son:

- Cada vez que se da de baja o de alta a algún equipo dentro de la red inalámbrica se deben modificar las tablas de las direcciones MAC de cada uno de los puntos de acceso y si se tiene demasiados equipos esto puede volverse inmanejable, por lo que no es recomendable para redes muy grandes como es el caso de la RIU.

- La transmisión de las direcciones MAC se realiza sin cifrar, por lo que

se pueden capturar éstas con facilidad y algún intruso puede ocupar la dirección MAC obtenida y acceder a la red.

- No garantiza la confidencialidad de la información debido a que no provee ningún mecanismo de cifrado.

Uso de VPN.

Existe otro método que se utiliza en las redes inalámbricas que es la red privada virtual (Virtual Private Network, VPN), en éste se utilizan tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público.

Utilizar una VPN en una red inalámbrica nos permite aislar zonas y servicios de la red interna, agrupando todos los puertos de acceso inalámbrico en una VLAN. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN y una vez que el cliente ha sido debidamente autorizado y autenticado se le permite el acceso completo a la red inalámbrica y cifra todo el tráfico generado.

A pesar de no haber sido diseñada para su aplicación en redes inalámbricas este método funciona sobre cualquier tipo de hardware inalámbrico, el uso de una VPN es una solución excelente para tener conectividad dentro de una red insegura, como lo es Internet (aunque la calidad de las implementaciones de VPN varíe). Sin embargo, no es necesariamente la mejor solución para asegurar las redes inalámbricas internas. Para este tipo de aplicaciones, una VPN ofrece poca o ninguna seguridad adicional en comparación con las soluciones 802.1x; al mismo tiempo que incrementan de manera significativa la complejidad y los costos y reducen el aprovechamiento de la red, por lo que la administración de ésta se vuelve más compleja.

Esta tecnología puede considerarse como segura, aunque tiene el inconveniente de que existe una falta de interoperabilidad entre dispositivos de distintos fabricantes.

Comprobada la poca fiabilidad del filtrado por direcciones MAC y la dificultad para implementar VPN en una red inalámbrica, se desarrollaron nuevas tecnologías que han tratado de solventar estas deficiencias como lo son WEP, WPA y WPA2 que se describirán a continuación.

2.3.1 WEP (Wired Equivalent Privacy).

WEP es un esquema de seguridad para redes inalámbricas que es parte del estándar IEEE 802.11 original y fue publicado en 1999.

WEP intenta asegurar que las WLAN tengan un nivel de privacidad cifrando las señales de radio para ser equivalente en cuanto a seguridad a una red cableada.

El objetivo de este esquema es evitar que los mensajes de broadcast puedan ser captados por personas ajenas, ya que las redes inalámbricas utilizan radiofrecuencias y por lo tanto son susceptibles a que puedan ser escuchadas, para realizar lo anterior WEP intenta proveer confidencialidad, autenticación y control de acceso en redes inalámbricas, así como evitar una modificación no autorizada de datos.

El cifrado de los datos con WEP no se extiende a las transmisiones finales, protege solo los paquetes de información y no la cabecera de la capa física, por lo que otras estaciones en la red pueden escuchar los datos de control que se necesitan para administrarla (aunque supuestamente las estaciones de la red no pueden descifrar los datos de los paquetes).

2.3.1.1 Cifrado y descifrado WEP.

WEP utiliza una misma llave simétrica y estática entre los clientes y el punto de acceso, el algoritmo de cifrado es RC4 y utiliza 64 bits, de los cuales 24 corresponden al Vector de Inicialización (IV) y 40 a la llave secreta.

El Vector de Inicialización es generado dinámicamente y debería ser diferente

para cada trama, el objetivo de éste es cifrar con claves diferentes para evitar que un posible atacante pueda capturar suficiente tráfico cifrado con la misma llave y con ello determinar la llave secreta y descifrar el mensaje.

El estándar establece que una llave única se asocia con cada cliente pero en la práctica una sola llave es compartida entre todos ellos.

Dos procesos son aplicados a los datos con texto en claro, uno de ellos es el cifrado de datos y el otro es el que protege a los datos de modificaciones no autorizadas mientras éstos son trasmitidos, lo que se muestra en la Figura 2.4.

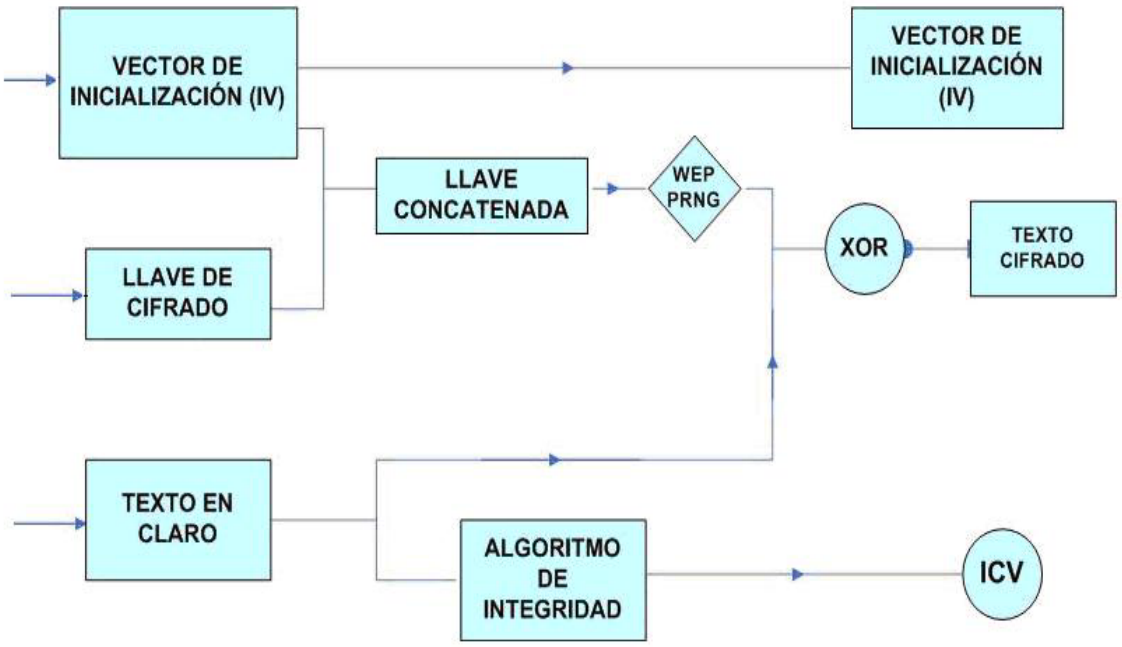


Figura 2.4 Cifrado de datos con WEP

El cifrado de datos comienza cuando la llave secreta es concatenada con el IV, la llave resultante es insertada en el PGNR (generador de números pseudoaleatorios), con lo cual se genera una llave larga y aleatoria. El emisor hace una función XOR entre el texto en claro y la última llave generada con lo cual se obtiene el texto cifrado. Al obtener el texto cifrado el emisor lo transmite junto con el IV.
El segundo proceso que tiene el objeto de proteger al texto cifrado de modificaciones no autorizadas, se realiza por medio del algoritmo CRC con

32 bits, dicho algoritmo verifica la integridad del texto en claro lo que produce un valor llamado ICV (Valor de integridad). El ICV se concatena con el texto en claro y es enviado al receptor.

Para el descifrado de datos también se utilizan dos procesos, uno es la obtención del texto en claro y el otro es la aceptación del mensaje por medio del algoritmo de integridad.

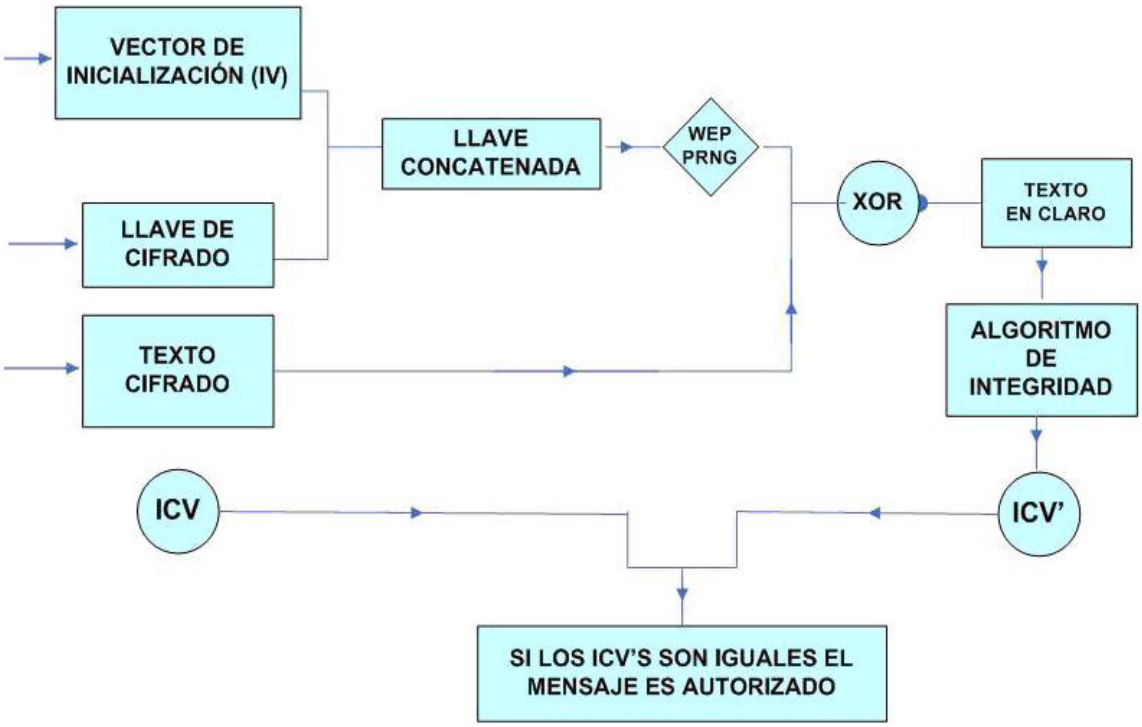


Figura 2.5 Descifrado de datos con WEP.

En la Figura 2.5 se muestran los dos procesos del descifrado, lo cual se realiza de la siguiente manera:

El descifrado de datos se realiza cuando el receptor obtiene el texto cifrado y el IV; para el proceso de descifrado usa su copia de la llave secreta y la concatena con el IV, después genera su llave larga aleatoria y también hace una función XOR pero ahora con el texto cifrado y la llave larga aleatoria, con lo cual obtiene el texto en claro.

El proceso de aceptación del mensaje se realiza después de que el receptor obtiene el texto en claro y éste le aplica el algoritmo de integridad y obtiene un nuevo ICV', después se hace una comparación entre éste y el ICV que fue enviado por el emisor, si los dos son iguales el mensaje es autorizado.

La distribución de llaves es un problema ya que la mayoría de las redes inalámbricas comparten una llave entre todos los clientes y puntos de acceso dentro de la red y por lo tanto es difícil mantener la llave verdaderamente secreta con tantos usuarios. Algunos administradores de red resuelven el problema configurando cada uno de los clientes con la llave secreta ellos mismos, pero esa no es la mejor solución ya que si un dispositivo móvil es comprometido los demás deberán reconfigurarse. Una mejor opción sería asignar a cada cliente su propia llave y cambiarla frecuentemente.

2.3.1.2 Autenticación de WEP.

WEP provee dos tipos de autenticación: el de default que es cuando el sistema está abierto, es decir, donde todos los usuarios tienen el acceso permitido, en el cual realmente no existe un esquema de seguridad como tal y, la autenticación de llave compartida que controla el acceso a la red inalámbrica, con lo que previene accesos no autorizados.

En el método de autenticación compartida cuando un cliente se trata de asociar con un punto de acceso éste le responde enviándole un texto aleatorio, el cliente debe cifrarlo con la llave compartida y enviárselo de regreso al punto de acceso para autenticarse, éste último lo descifra y lo compara con el texto original, si es igual el punto de acceso envía un mensaje de confirmación y acepta al cliente dentro de la red, si éste no tiene la llave para cifrar el texto o es erróneo el punto de acceso lo rechaza. Dicho procedimiento se describe en la Figura 2.6

El método descrito previamente solo funciona si se encuentra habilitado en el punto de acceso, de los contrario la autenticación será abierta.

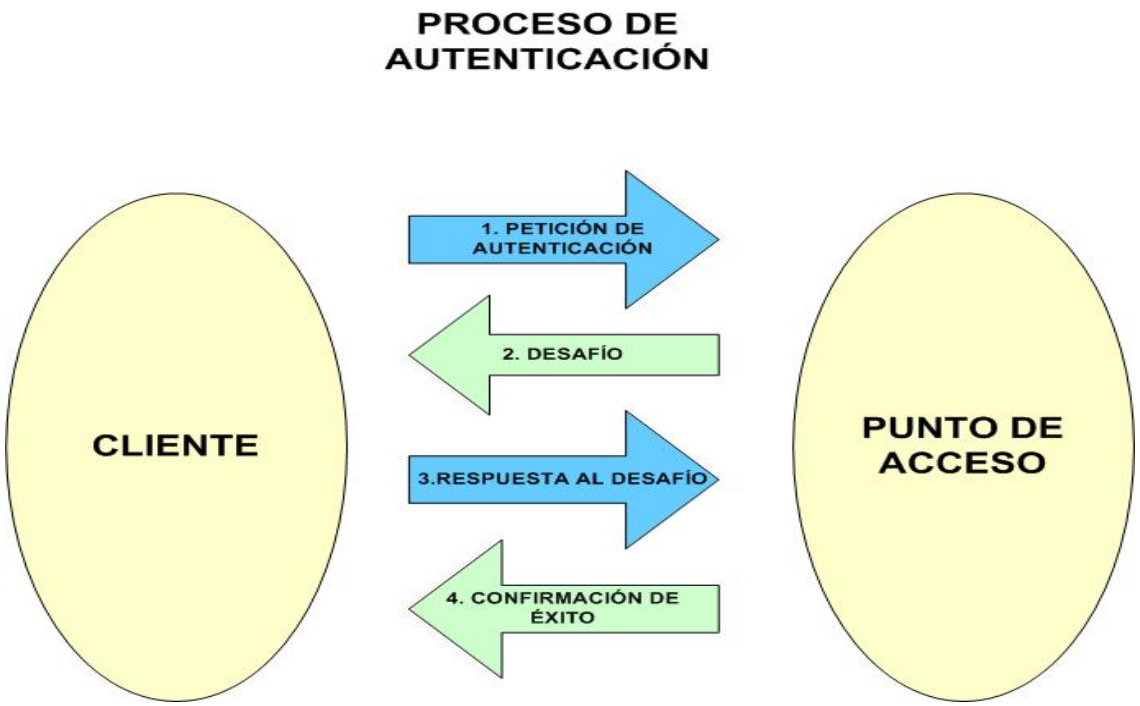


Figura 2.6 Autenticación con WEP.

2.3.1.3 Debilidades de WEP.

El estándar 802.11 no especifica como manejar el IV ya que dice que debe cambiarse en cada trama pero no obliga a ello, por lo que los fabricantes de equipo tienen que arreglárselas para ir variando dicho valor y éstos normalmente se van por la opción más sencilla, la cual es que cada vez que se arranca la tarjeta de red, se fija el IV en cero y se incrementa en uno para cada trama. Lo anterior ocasiona que las primeras combinaciones de llaves secretas e IV's se estén repitiendo frecuentemente, además de que si los clientes utilizan la misma llave de cifrado, las tramas con la misma llave se van a multiplicar por el medio.

El número de vectores de inicialización que puede existir no es muy elevado, su valor es 224 lo cual resulta en 16 millones aproximadamente por lo que éstas se van a estar repitiendo en cuestión de minutos u horas dependiendo de la carga de la red.

Una solución que se dio para evitar las vulnerabilidades de WEP fue aumentar la llave de cifrado a 128 bits, pero como lo único que cambia es la llave secreta a 104 bits, porque los 24 restantes son el IV, el cual no se puede cambiar porque así está definido en el estándar, las vulnerabilidades descritas del IV siguen siendo las mismas.

También se puede llegar a conocer la llave secreta, ya que se puede deducir si tenemos suficientes vectores de identificación conocidos y sus tramas con el mismo IV asociado.

Por otra parte también se ha encontrado que a pesar del algoritmo CRC de 32 bits se han podido hacer modificaciones a los datos y al mismo CRC, ya que si se llega a conocer la llave de cifrado, el atacante puede llegar a hacer un mensaje cifrado, trasmitirlo y con ello llegar a conocer el valor del ICV.

Con respecto a las debilidades de autenticación, WEP no incluye autenticación de usuarios sino que entran a la red los clientes que tengan configuradas la clave WEP, la cual es la misma tanto para el cifrado como para la autenticación.

Por otra parte no existen mecanismos de protección contra mensajes repetidos, lo que permite que se introduzca un mensaje y se capture en la red en un momento posterior.

Algunas de las vulnerabilidades descritas anteriormente se trataron de evitar utilizando WEP dinámico, el cual busca incorporar mecanismo de distribución automática tanto de claves como autenticación de usuarios por medio de 802.1x, EAP y un servidor RADIUS.

Otra opción fue implementar VPN’s junto con WEP, lo que permite establecer una conexión segura dentro de una red privada, la VPN permite crear un túnel que protege los datos de las redes inalámbricas de accesos no autorizados.
Debido a las serias debilidades que fueron identificadas en WEP se optó por utilizar otros mecanismos de seguridad como lo fue primero WPA y posteriormente WPA2. Dichos mecanismos serán explicados más adelante.

2.3.2 WPA (WI-FI PROTECTED ACCESS).

La alianza Wi-Fi ha intensificado sus investigaciones para sacar al mercado un estándar basado en la interoperabilidad de las especificaciones de seguridad que permitan incrementar el nivel de protección de los datos y el control de acceso para las redes inalámbricas. Tales especificaciones se concentran en un estándar denominado Wi-Fi Protected Access, WPA.

El procedimiento WPA fue anunciado por Wi-Fi Alliance en los primeros meses de 2003. Ésta solución pretende reemplazar el estándar WEP, ofreciendo un método robusto de cifrado de datos y un mecanismo de autenticación de red.

La Wi-Fi Alliance asegura que todo equipo de red inalámbrica que posea el sello "Wi-Fi Certified" podrá ser actualizado por software para que cumpla con la especificación WPA.

WPA presenta un fuerte método de autenticación a través del uso del estándar 802.1x y EAP (Extensible Authentication Protocol). También provee un cifrado robusto de 128 bits y para solucionar el problema de cifrado de datos, WPA propone un protocolo conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP. Para asegurar la integridad de los mensajes y prevenir la captura y falsificación de paquetes se integra MIC (Message Integrity Protocol).

WPA esta diseñado para operar en dos modalidades, dependiendo de la complejidad de la red y de las necesidades de los usuarios.

• Modalidad de red empresarial:

Se utiliza para operar con redes de gran tamaño para lo cual 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.

• Modalidad de red casera, o PSK (Pre-Shared Key):

Está diseñado para las redes caseras o de pequeñas oficinas, quienes no tienen servidores disponibles. Opera en un modo no administrado y utiliza una llave pre-compartida PSK que sirve para la autenticación en vez del 802.1x del modo anterior.

La autenticación se realiza al introducir el PSK manualmente en el punto de acceso y con ello generar la llave de cifrado.

Solamente podrán acceder a la red inalámbrica 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-PSK es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

En la Tabla 2.2 se muestra un cuadro de las propiedades de WPA.

Característica	Componente Tecnológico	Funciones
Autenticación y Llave maestra	802.1x	Intensifica el cifrado WEP a través de la autenticación por puerto, con una distribución de llaves por sesión.
	Extensible Authentication Protocol (EAP)	Permite gran variedad de métodos de autenticación a los clientes y el uso de certificados (en muchos casos) para proporcionar autenticación mutua (es decir, el servidor autentica al cliente y viceversa).
Autorización y cuentas	RADIUS (Remote Authentication Dial-In User Service)	Permite solo a los usuarios autorizados acceder a la red.
Confidencialidad	TKIP (Temporaly Key Integrity Protocol)	Provee un fuerte cifrado para la criptografía de los datos.
Integridad	MIC (Message Integrity Check)	Protección contra la falsificación de paquetes.

Tabla 2.2 Propiedades de WPA.

2.3.2.1 Cifrado WPA.

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.

TKIP esta compuesto por los siguientes elementos:

- **Código de integración de mensajes MICHAEL (MIC)**, el cual cifra el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Michael especifica un nuevo algoritmo que calcula un código de integridad de mensaje de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos existentes. El código MIC se coloca entre la parte de datos del marco IEEE 802.11 y el valor ICV de 4 bytes. El campo MIC se cifra junto con los datos del marco y los de ICV. También ayuda a proporcionar protección de reproducción, si un paquete sufre cualquier cambio, deberá ser rechazado y generar una alerta, que indica una posible falsificación del mismo.

- **Combinación de clave por paquete**. La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete, lo que reduce la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

- **Utilización de un IV** (vector de inicialización). Utiliza un IV de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques de repetición, descartando los paquetes recibidos fuera de orden. Esta duplicación de tamaño del IV implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones. Si se realiza un gran simplificación (pues el caso es más complejo) y se divide 280 billones sobre 16 millones, el resultado es: 17.500.000, por lo tanto si un IV de 24 bits se repite en el orden de 5 horas

en una red inalámbrica de una mediana empresa, entonces un IV de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años, es decir, se repetiría después de miles de años.

La Figura 2.7 muestra la estructura de cifrado TKIP propuesta en WPA.

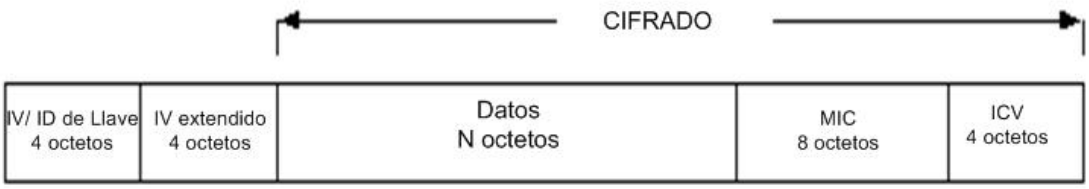


Figura 2.7 Estructura de cifrado TKIP.

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 248 paquetes utilizando una sola llave temporal antes de ser rehusada.

2.3.2.2 Autenticación WPA.

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 inalámbricas. La idea básica es que cuando un dispositivo intenta conectarse a un punto de acceso, éste le pide algún tipo de credenciales que reenvía a un servidor de autenticación para que se le indique si debe autorizar o no al dispositivo para acceder a la red inalámbrica.

El punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor RADIUS (Remote Authentication Dial-In-Use Service) para autenticar las credenciales del cliente. La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de

validar las credenciales y obtener claves para obtener acceso a la red. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

En sistemas con 802.1x se generan dos llaves, la llave de sesión (pairwise key) y la llave de grupo (groupwise key). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso, las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

Los pasos que se muestran en la Figura 2.8 describen el planteamiento que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red:

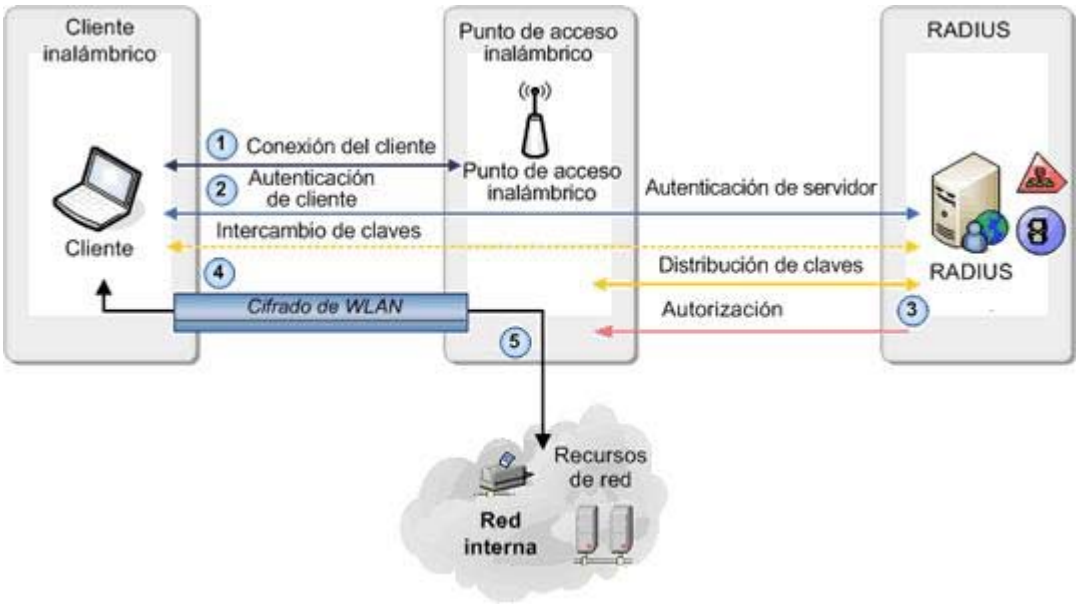


Figura 2.8 Autenticación WPA.

1. Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando un cliente inalámbrico entra en el alcance del punto de acceso, éste envía un desafío al cliente.

2. Cuando el cliente recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.

3. Posteriormente, el servidor RADIUS solicita las credenciales del cliente, especificando el tipo de credenciales necesarias para confirmar su identidad. El cliente las envía al servidor RADIUS (a través del "puerto no controlado" del punto de acceso). El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.

4. Si las credenciales son correctas, el servidor RADIUS autoriza el acceso al cliente y abre el puerto para establecer la comunicación.

5. El cliente tiene acceso a la red y puede transmitir datos cifrados y utilizar los recursos de la red. Para mantener un nivel de seguridad, se puede pedir al usuario que vuelva a autenticarse periódicamente.

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.

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

Existen variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos, 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**: 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**: Desarrollada por Funk Software y Certicom. 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**: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TTLS, 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, para lo cual requiere de un nombre de usuario y contraseña.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas, las cuales son:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

- El diálogo de autenticación es largo, esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen

que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en el equipo inalámbrico del usuario, con lo cual, si éste es robado y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- **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.

  Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada). Por estos problemas, EAP-MD5 ha caído en desuso.

- **LEAP**: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

- **EAP-SPEKE**: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

2.3.3 WPA2.

WPA es la versión certificada y operable del estándar IEEE 802.11i y proporciona seguridad a las redes inalámbricas de una forma más eficiente que sus predecesores.

Fue dado a conocer en Septiembre de 2004 por la alianza Wi-Fi e incluye el algoritmo de cifrado AES (Advanced Encryption Standar), utiliza cifrado por bloque con llaves simétricas de 128 bits, además requiere de un software potente para realizar sus algoritmos, por lo que dispositivos antiguos sin suficientes capacidades de proceso no pueden incorporar WPA2.

Para asegurar la integridad y la autenticidad de los mensajes, este estándar utiliza un mecanismo de cifrado avanzado, usa el protocolo CCMP (Counter-Mode/Cypher Block Chaining/Message Authentication Code Protocol).

En este esquema de seguridad al igual que en WPA también existen dos modos de certificación los cuales son los siguientes:

Modo empresarial.

Este modo opera de la misma manera que WPA, con la diferencia que utiliza AES que es más fuerte que TKIP y provee una seguridad adicional a la red.

Modo personal.

Este modo también funciona de la misma manera que WPA pero utiliza el algoritmo de cifrado AES.

WPA2 protege a la red de colisiones de llaves, repetición de mensajes, ataques de fuerza bruta, paquetes falsos, autenticación falsa, etc.

Llaves temporales

WPA2 utiliza un conjunto de cuatro diferentes llaves para cada pareja punto de acceso-cliente, estás llaves son conocidas como pares de llaves transitorias,

y también utiliza un conjunto de dos diferentes llaves para tráfico de multicast y de broadcast.

El conjunto de pares de llaves usadas para datos unicast y la llave EAP sobre la red LAN (EAPOL-Key por sus siglas en inglés EAP OVER LAN) son las siguientes:

- **Llave de cifrado de datos**. Es de 128 bits y es usada para cifrar tramas unicast.

- **Llave de integridad de datos**. Es de 128 bits y es usada para calcular el MIC para tramas unicast.

- **Llave de cifrado EAPOL**. Es de 128 bits y es usada para cifrar mensajes EAPOL.

- **Llave de integridad EAPOL**. Es de 128 bits y es usada para calcular el MIC de los mensajes EAPOL.

2.3.3.1 Cifrado y descifrado WPA2.

Con AES los bits son cifrados por bloques de un texto en claro que son calculados independientemente, después una llave actúa a través del texto en claro. AES tiene un tamaño de bloque de 128 bits con tres posibles longitudes, 128, 192 y 256 bits, para el IEEE 802.11i se usa la llave de 128 bits y también incluye 4 etapas en cada ronda. Cada ronda es iterada 10, 12 o 14 veces dependiendo del tamaño de la llave, para este estándar cada ronda es iterada 10 veces. Se utiliza la misma llave tanto para cifrar como para descifrar los datos.

Además hace uso de un vector de inicialización (IV) de 48 bits y toma 2128 operaciones romper la llave de AES lo que lo hace un algoritmo de cifrado muy seguro.

AES utiliza el protocolo CCMP que es un nuevo modo de operación para un cifrado de bloques que habilita el uso de una sola llave en el cifrado y la autenticación, dicha llave debe ser temporal y actual para cada sesión y un único número de paquete para cada trama protegida por la llave temporal dada.

Los dos modos de CCMP incluyen modo de conteo (CTR) que realiza el cifrado de datos y el código de autenticación de mensajes de cifrado por bloques CBC-MAC (Cypher Block Chaining / Message Authentication Code Protocol) que permite la integridad de los datos.

Con CCMP las falsificaciones pueden ser fácilmente detectadas mediante el mensaje de código de integridad CBC-MAC protegiendo tanto a la fuente como al destino.

Modo de conteo.

El modo de conteo CTR es un modo confidencial con las características de que un conjunto de bloques de entrada (contadores) produce una secuencia de bloques de salida. Estos bloques resultantes hacen una XOR con el texto en claro para producir el texto cifrado.

En el cifrado y descifrado CTR puede realizar la función de cifrado paralelo y puede recuperar bloques independientemente de los otros.

El algoritmo de cifrado se describe en la Figura 2.9 y funciona de la siguiente manera:

1. Cifra un contador inicial con AES y la llave de integridad de datos, lo que produce un resultado de 128 bits **Resultado1**.
2. Realiza una operación XOR entre **Resultado1** y el bloque inicial de datos o primer bloque de mensaje de 128 bits, lo que produce el primer bloque cifrado de 128 bits.
3. Incrementa el contador y lo cifra con AES y la llave de integridad de datos, lo que produce **Resultado2**.

4. Realiza una XOR entre **Resultado2** y los siguientes 128 bits de datos, lo que produce el segundo bloque cifrado.

Se repiten los pasos tres y cuatro hasta que se terminen los bloques de 128 bits. Para el bloque final se hace una XOR entre el contador cifrado y los bits restantes, produciendo datos cifrados de la misma longitud que el último bloque de datos.

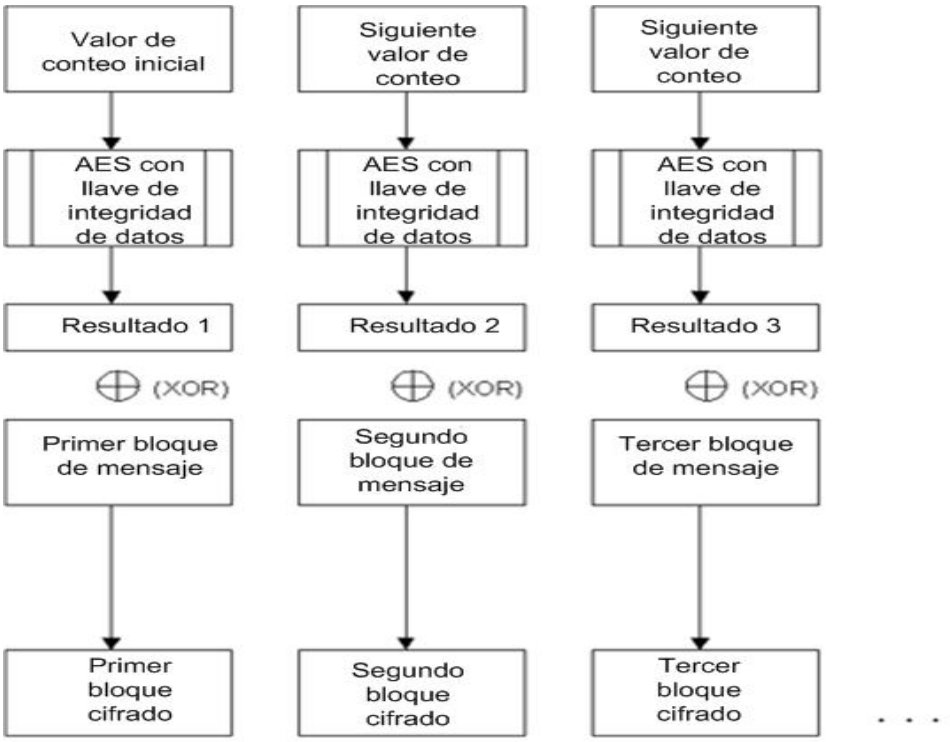


Figura 2.9 Cifrado en modo de conteo.

Modo CBC-MAC.

CBC-MAC es usado para generar una autenticación como resultado del proceso de cifrado, lo cual es diferente de las implementaciones MIC en las que un algoritmo de forma separada checa la integridad de los datos. Es un modo confidencial caracterizado por el encadenamiento del texto en claro con el texto cifrado, para lo cual requiere un vector de inicialización, lo que resulte del proceso anterior será el código de autenticación para el paquete.

El proceso de cifrado CBC-MAC se muestra en la Figura 2.10 y su modo de operación es el siguiente:

1. Cifra un bloque inicial de 128 bits con AES y la llave de integridad de datos esto produce el resultado de 128 bits, es el bloque llamado **Resultado1**.

2. Realiza una operación OR exclusiva (XOR) entre **Resultado1** y los siguientes 128 bits de datos, sobre el cual la MIC es calculada. Esto produce el bloque **XResultado1**.

3. Cifra **XResultado1** con AES y llave de integridad de datos, lo que produce **XResultado2**.

4. Realiza una XOR entre **Resultado2** y los siguientes 128 bits de datos, lo que produce **XResultado2**.

Los pasos 3 y 4 se repiten hasta terminar los bloques de 128 bits de datos. Los 64 bits de orden mayor del resultado final es el MIC de WPA2.

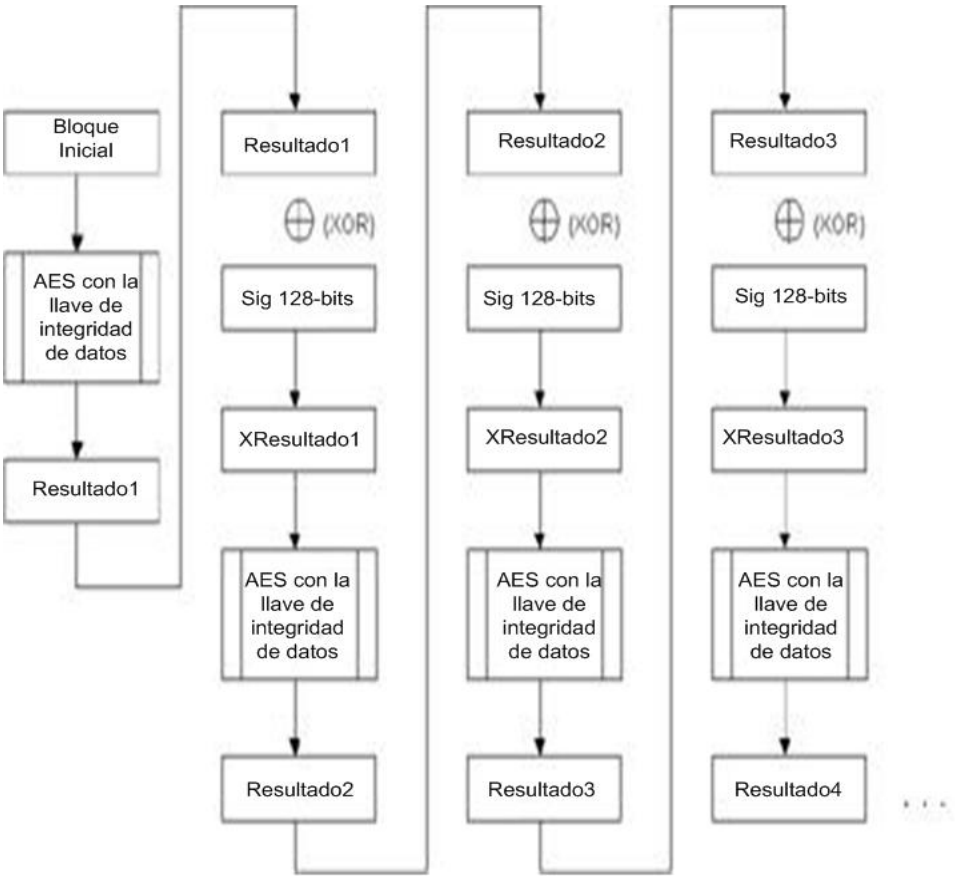


Figura 2.10 Cifrado WPA2.

El descifrado como ya se mencionó con anterioridad se realiza con la misma llave y sigue los mismos procesos que para el cifrado pero en vez de los datos en claro se inicia con los datos en forma cifrada.

2.3.3.2 Autenticación WPA2.

El modo de autenticación WPA2 utiliza los protocolos 802.1x y EAP los cuales crean un marco entre el cliente y el servidor de autenticación por medio del punto de acceso tal como funcionan para WPA, con la diferencia de que al completar el proceso de asociación, se instalan las llaves de cifrado de AES. Cuando un cliente empieza a comunicarse dentro de la red el cifrado con AES protege los datos intercambiados.

Existen 6 componentes para la autenticación en modo empresarial los cuales son:

- Dispositivos inalámbricos, para que los usuarios se puedan conectar a la red inalámbrica, los cuales deben de estar actualizados para soportar el esquema de cifrado WPA2.
- Cliente suplicante.
- Soportar tipos de EAP.
- Puntos de acceso que soporten WPA2.
- Servidores de autenticación.
- Servidores de bases de datos.

El servidor de autenticación ayuda a asegurar que sólo los usuarios autorizados accedan a la red inalámbrica y también que sólo puedan entrar a las áreas que tienen permitidas. Normalmente se utiliza un servidor de autenticación de tipo RADIUS.

Las credenciales de los usuarios normalmente se encuentran en una base de datos externa como SQL, LDAP, Active Directory, etc., la cual debe poder ser accedida por el servidor de autenticación. Lo anterior no tiene una configuración establecida en el estándar, por lo que se pueden utilizar implementaciones específicas.

AES hace muy difícil pero no imposible la intrusión a una red inalámbrica, así como también incrementa la complejidad del cifrado de los datos en la misma y junto con 802.1x y EAP hace a la red inalámbrica muy segura.

WPA2 incluye un modo de operación opcional que permite la coexistencia entre de WPA y WPA2 para lo clientes dentro de un mismo identificador de red, este modo se puede utilizar si es que hay una transición de WPA a WPA2, los clientes pueden escoger entre usar TKIP o AES.

2.3.3.3 Actualizaciones a WPA2.

Un punto de acceso que no tenga las facilidades computacionales para soportar los cálculos más complejos que tiene AES no puede ser actualizado a través de firmware y debe ser reemplazado. También hace falta reemplazar los adaptadores de red inalámbricos y el software del punto de acceso a una versión más reciente que soporte este esquema de seguridad, en todos los casos los fabricantes del equipo son los que venden las actualizaciones.

La Tabla 2.3 muestra los elementos de los tres esquemas de seguridad antes descritos.

Características	WEP	WPA	WPA2
Algoritmo de Cifrado	RC4	RC4 (TKIP)	AES
Llave de cifrado	40 bits	128 bits	128 bits
Vector de Inicialización	24 bits	48 bits	48 bits
Llave de autenticación	Ninguna	64 bits	64 bits
Comprobación de integridad	CRC-32	MICHAEL	CBC-MAC
Distribución de llaves	Manual	802.1x (EAP)	802.1x (EAP)
Llave única por	Red	Paquete, sesión, usuario	Paquete, sesión, usuario
Negociación por cifrado	No	Sí	Sí
Seguridad Ad-hoc (P2P)	No	No	Sí
Pre-Autenticación	No	No	Sí usando 802.1x EAPOL

Tabla 2.3 Comparación entre esquemas de seguridad.

CAPÍTULO 3

DISEÑO DE LA RED INALÁMBRICA UNIVERSITARIA

En este capítulo se desarrollará el tema del diseño, necesidades e importancia de implementar la red inalámbrica universitaria. Así como también mencionaremos los parámetros que se tomaron en cuenta para su diseño como lo fueron:

- Antecedentes.
- Descripción de la propuesta.
- Metodología.
- Definición de los lugares a cubrir.
- Estudios de cobertura.
- Evaluación de las tecnologías inalámbricas.
- Pruebas a los equipos inalámbricos.
- Resultados obtenidos en las pruebas.
- Prediseño de la red.
- Diseño propuesto para la red inalámbrica universitaria, el cual abarca metodología y políticas de uso.

3.1 Antecedentes.

Tomando en cuenta que el uso de Internet y de las redes de computadoras en general se ha convertido en una necesidad dentro de las actividades de la UNAM, que las dependencias han crecido en cuanto al número de usuarios y que el número de servicios de red ya no es suficiente, se han ido buscando soluciones a esta dificultad, para lo cual se consideró la utilización de redes inalámbricas cuya utilización se ha facilitado debido a que en los últimos años han salido al mercado una gran cantidad de tecnologías inalámbricas las cuales han mejorado los algoritmos de cifrado, lo que ha permitido implementaciones fáciles, rápidas y en algunos casos con un bajo costo. Esta facilidad de implementación de redes inalámbricas ha ido creando el interés en muchas facultades, institutos y centros de investigación para poner en marcha el funcionamiento de su propia red inalámbrica y así disminuir la falta de este servicio.

Sin embargo dichas implementaciones solo dan servicio exclusivamente a sus usuarios y tienen la desventaja de no ser seguras tanto en el acceso como en el transporte de la información, poniendo en riesgo la confidencialidad e integridad de los datos y la propia red local.

Debido a lo anterior se buscó implementar una red inalámbrica para la comunidad universitaria que cubra las necesidades de los usuarios.

3.2 Descripción de la propuesta.

La propuesta para este proyecto fue diseñar e implementar una red inalámbrica que de cobertura en gran parte del campus de Ciudad Universitaria, así mismo, que pueda ser utilizada por y de uso exclusivo de la comunidad universitaria, sin costo alguno y procurando ofrecer una disponibilidad del 99.9%.

Dicha red debe proporcionar principalmente los servicios de navegación por web y consulta de correo electrónico. Así mismo se busca estandarizar las redes inalámbricas que existen a lo largo del campus universitario cubriendo

zonas de mayor afluencia, en general espacios comunes para la comunidad en los cuales desarrollen sus actividades académicas, ofreciendo movilidad dentro del campus y que al mismo tiempo sea lo más segura posible.

Una de las características importantes fue considerar soluciones inalámbricas que contaran con los siguientes requerimientos, debido a que fueron las necesidades principales de la Red Inalámbrica Universitaria.

- Puntos de acceso que soporten el estándar 802.11a/b/g para que los distintos dispositivos inalámbricos (clientes) ya existentes puedan ser compatibles con esta red.

- Puntos de acceso a los que se les pudieran implementar mecanismos de seguridad como lo son: WEP y WPA con el objetivo de evitar o dificultar el acceso no autorizado a la red inalámbrica, así como ataques de intrusión y propagación de virus, procurando que nadie pudiera comprometer a la RedUNAM ni a las redes locales de las dependencias y de esta manera mantener la información de los usuarios segura.

- Equipos que cuenten con una administración centralizada (realizada por DGSCA), así mismo con un monitoreo efectivo que permita detectar fallas y con soporte para actualizaciones de software y firmware.

- Equipos que cuenten son soporte para los servicios: DHCP, NAT, firewall y detector de intrusos (IDS).

- Equipos que puedan dar un buen servicio de red a gran parte de la comunidad universitaria.

Por otra parte se espera que esta propuesta sirva como prototipo para la instalación de redes inalámbricas en otros campus fuera de Ciudad Universitaria y con ello aumentar y mejorar las actividades académicas en la

UNAM, lo anterior contribuiría al fortalecimiento de la enseñanza superior en México y mantendría a la Universidad en la vanguardia de la tecnología.

3.3 Metodología.

Parte importante en la creación de una red inalámbrica es definir y seguir una metodología que nos permita evitar errores costosos, para lo cual se deben planear con anticipación las actividades a realizar.

Como puntos importantes a tomar en cuenta en la realización del diseño de la red inalámbrica universitaria se encuentran los siguientes aspectos:

1. Conocer y analizar las necesidades de las facultades, institutos y centros de investigación interesados en ser parte del proyecto de la RIU e identificar las áreas de interés que se desean cubrir con la red inalámbrica.
2. Detección de señales de redes inalámbricas existentes mediante un recorrido por Ciudad Universitaria.
3. Realizar el estudio de cobertura en las áreas de interés de cada dependencia.
4. Definición de estándares a utilizar.
5. Estudio de mercado de las soluciones existentes.
6. Pruebas en laboratorio con los productos existentes en el mercado.
7. Resultados de las pruebas.
8. Definición del diseño de la RIU.
9. Implementación de políticas de uso.

3.4 Aspectos a tomar en cuenta en el diseño de la red inalámbrica.

A continuación se describirán los aspectos que se tomaron en cuenta antes de realizar el diseño de la red inalámbrica universitaria. Dentro de dichos aspectos se encuentran la definición de los lugares a cubrir dentro de las facultades, institutos, centros de investigación, coordinaciones, etc. Así mismo se describirá el estudio de cobertura y las herramientas necesarias que

se tomaron en cuenta para su realización. Además se hablará acerca de las tecnologías mas adecuadas para el diseño y la implementación de la RIU, se describirá el protocolo de pruebas aplicado a las tecnologías participantes y los resultados de las mismas.

3.4.1 Definición de los lugares a cubrir.

Como primera etapa de la definición de los lugares a cubrir, se enviaron oficios a cada una de las dependencias de Ciudad Universitaria, en dichos oficios se les informaba a los directores de cada dependencia acerca de la realización de éste proyecto y se les invitaba a participar en él.

Posteriormente se realizaron visitas a cada una de las dependencias que decidieron participar. En dichas visitas se les informaron las características de esta red inalámbrica. Así mismo en algunos casos los lugares que se iban a cubrir con la RIU se dejaban a juicio de los secretarios técnicos y de los administradores de red de cada dependencia. Para llevar a cabo el proceso anterior se les recomendaba que las áreas fueran lugares de uso común, donde existiera más concurrencia de universitarios y donde el cableado de las redes locales fuera inaccesible.

Los principales lugares que se planearon cubrir fueron: bibliotecas, auditorios, cafeterías, jardines, explanadas y espacios abiertos como son la explanada del Centro Cultural Universitario, la explanada principal de Ciudad Universitaria (islas), alberca, etc.

Las dependencias interesadas en ser parte de la RIU en esta primera etapa fueron 59 y se encuentran listadas en la Tabla 3.1.

No. Dependencia	Dependencia
1.	Torre de Rectoría
2.	Biblioteca Central
3.	Biblioteca Nacional
4.	Dirección General de Orientación y Servicios Educativos
5.	Dirección General de Servicios de Cómputo Académico
6.	Centro de Enseñanza Para Extranjeros
7.	Centro de Enseñanza de Lenguas Extranjeras
8.	Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas
9.	Alberca Olímpica
10.	Universum
11.	Explanada de la Sala Netzahualcóyotl
12.	Coordinación de Humanidades
13.	Facultad de Arquitectura
14.	Facultad de Derecho
15.	Facultad de Derecho (Posgrado)
16.	Facultad de Filosofía y Letras
17.	Facultad de Psicología
18.	Facultad de Ingeniería (Edificio principal)
19.	Facultad de Ingeniería (Anexo)
20.	Facultad de Ingeniería (Posgrado)
21.	Facultad de Química
22.	Facultad de Química (Edificios D y E)
23.	Facultad de Medicina
24.	Facultad de Economía
25.	Facultad de Veterinaria
26.	Facultad de Odontología

27.	Facultad de Odontología (Posgrado)
28.	Facultad de Contaduría
29.	Facultad de Contaduría (Posgrado)
30.	Facultad de Ciencias
31.	Facultad de Ciencias Políticas
32.	Escuela Nacional de Trabajo Social
33.	Instituto de Química
34.	Instituto de Fisiología Celular
35.	Instituto de Matemáticas
36.	Instituto de Geografía
37.	Instituto de Física
38.	Instituto de Geología
39.	Instituto de Geofísica
40.	Instituto de Investigaciones Biomédicas
41.	Instituto de Biología
42.	Instituto de Ecología
43.	Instituto de Investigaciones Antropológicas
44.	Instituto de Ciencias Nucleares
45.	Instituto de Materiales
46.	Instituto de Ciencias de la Atmósfera
47.	Instituto de Astronomía
48.	Instituto de Investigaciones Filológicas
49.	Instituto de Investigaciones Sociales
50.	Instituto de Investigaciones Históricas
51.	Instituto de Investigaciones Estéticas
52.	Instituto de Investigaciones Jurídicas
53.	Instituto de Investigaciones Filosóficas
54.	Instituto de Ciencias del Mar
55.	Instituto de Investigaciones Económicas

56.	Centro de Investigaciones Sobre América del Norte
57.	Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades
58.	Centro Universitario de Investigaciones Bibliotecológicas
59.	Coordinación de la Investigación Científica

Tabla 3.1 Dependencias participantes en la RIU.

3.4.2 Estudios de cobertura.

Una red inalámbrica ideal consiste en un cliente inalámbrico comunicándose con un punto de acceso a pocos metros de distancia, con línea de vista entre ellos y sin ningún obstáculo, ruido o interferencias en los canales de comunicación, sin embargo, en condiciones reales esto no es posible ya que por una parte los usuarios no saben en donde se encuentran físicamente los puntos de acceso y por otra, los canales de radio frecuencia se comparten con algunos otros aparatos electrónicos como hornos de microondas y teléfonos inalámbricos, además se interponen objetos que absorben la señal como paredes, ventanas, árboles, personas, libros y objetos que reflejan la señal como el metal y el agua.

Para minimizar el impacto que puedan causar las situaciones descritas es necesario realizar estudios de cobertura, con lo cual se logra mejorar la señal o ubicar en lugares óptimos los puntos de acceso para dar mejor servicio.

Como parte del estudio de cobertura para la RIU, se realizó un recorrido por toda ciudad universitaria para detectar las redes inalámbricas existentes, con el fin de determinar si estas redes podían causar alguna interferencia y también con el objetivo de realizar un censo para conocer la tendencia de mecanismos de seguridad utilizados, así como también la importancia que los administradores de red le daban tanto a la implementación de las redes inalámbricas como a la seguridad de éstas. Esta actividad se llevó a cabo con la ayuda del software Netstumbler.

El resultado fue que se detectó una gran cantidad de redes inalámbricas, aproximadamente 200 (en mayo del 2004), de las cuales la mayoría no contaba con algún tipo de seguridad, es decir, tenían autenticación abierta; menos de la tercera parte tenían seguridad WEP y solo 3 contaban con seguridad WPA.

En la Figura 3.1 se muestra una captura del software Netstumbler en la que se muestran cuatro redes, de las cuales solo una tiene seguridad WPA.

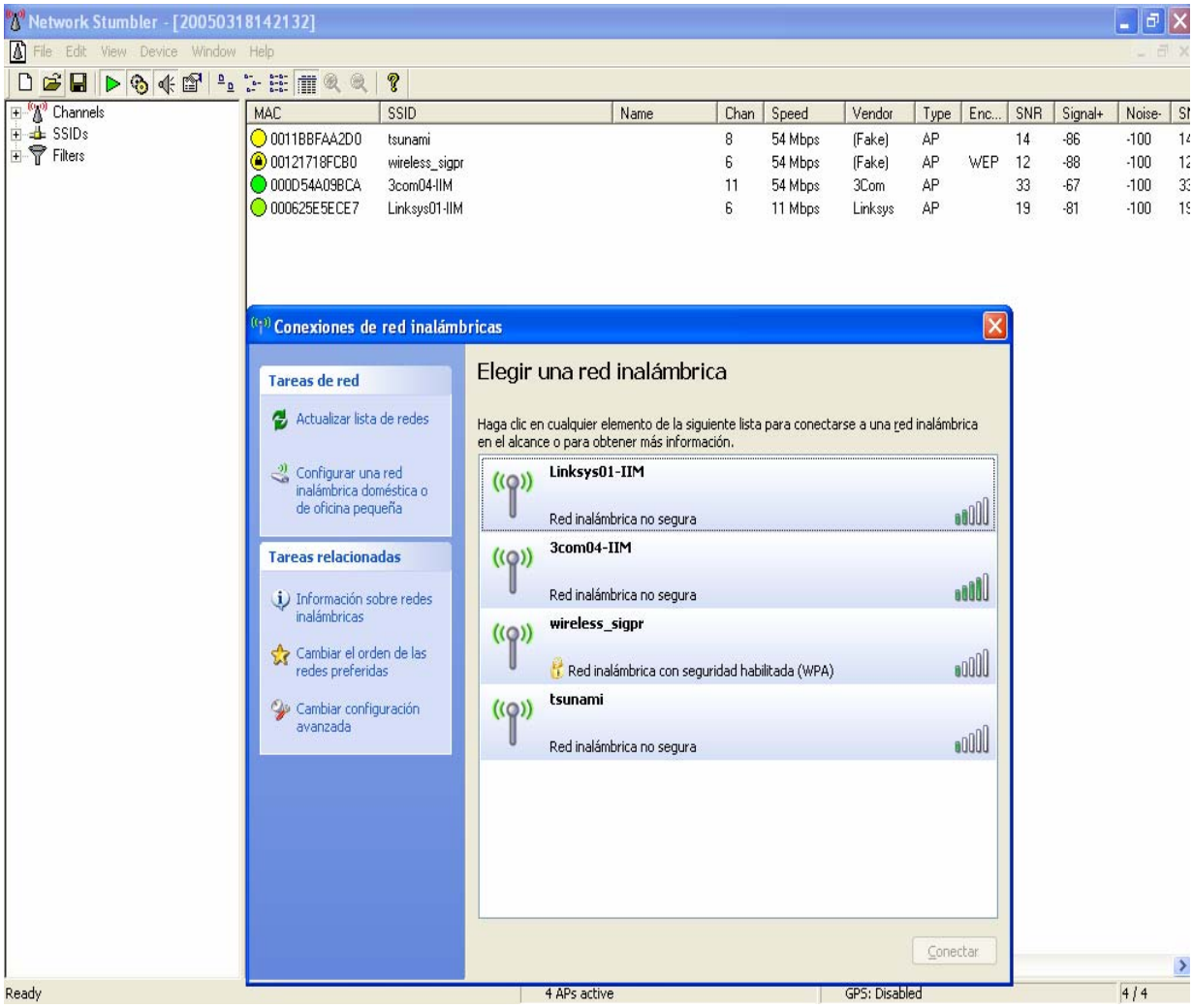


Figura 3.1 Captura de identificadores de red con Netstumbler.

Una vez que los responsables de red de las distintas dependencias sugirieron los lugares en donde requerían servicio de red inalámbrica, se realizaron las pruebas de cobertura, las cuales consistieron en configurar puntos de acceso y colocarlos en los lugares donde se requería dar servicio de red inalámbrica.

Para la realización de las pruebas se utilizaron las siguientes herramientas:

Software

- Netstumbler.
- Sistema operativo Windows XP.

Hardware

- Computadoras portátiles.
- Puntos de acceso.
- Antenas de mayor ganancia.

Este estudio consistió en utilizar laptop's con el software Netstumbler con el objeto de detectar la potencia de la señal emitida por el punto de acceso en varias zonas.

La Figura 3.2 muestra un ejemplo de la potencia de la señal emitida con un punto de acceso de prueba. En dicha figura se pueden observar los cambios de la potencia de la señal respecto al tiempo en minutos. La señal también era afectada por obstáculos que se encontraban entre el punto de acceso y la laptop. Por ejemplo en el minuto 45 la potencia de la señal fue de -67dBm, valor que cambió al minuto 46 a -83 dBm debido a que la laptop se encontraba más lejos del punto de acceso.

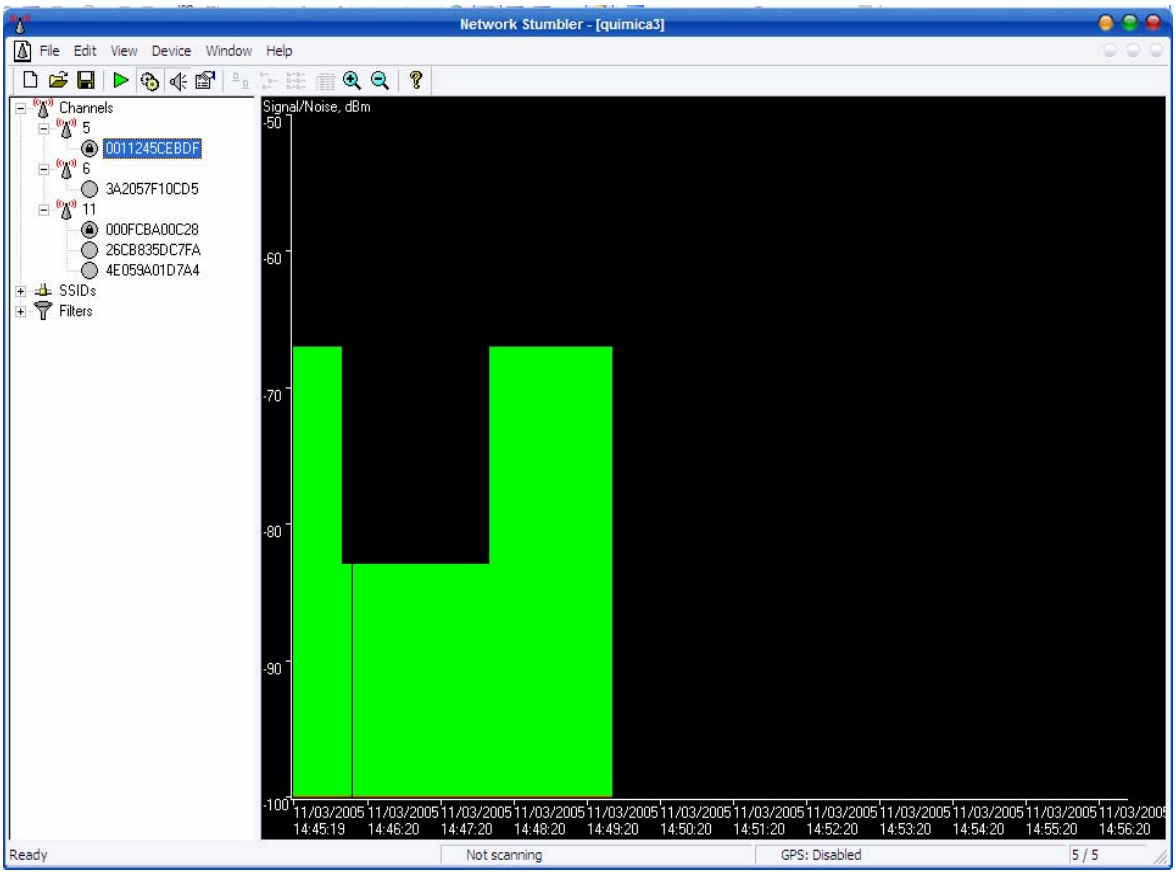


Figura 3.2 Captura de la potencia de la señal con Netstumbler.

Como parte del estudio de cobertura se realizaron transferencias de archivos así como envío de paquetes ICMP entre equipos portátiles, tratando de que éstos estuvieran lo más alejados posibles entre ellos, estas pruebas nos permitieron conocer hasta qué distancia se perdía la comunicación y si existía o no pérdida de paquetes en la transferencia de archivos. De ésta manera se pudo determinar el lugar más óptimo para la colocación tanto de los puntos de acceso como de las antenas tratando de librar los obstáculos, ya que al hacer las pruebas se observó que el papel de los libros, la madera y el concreto principalmente disminuían considerablemente la potencia de la señal.

Además de realizar los estudios de cobertura en sitio, también se realizaron simulaciones de cobertura con ayuda del software **Ekahau Site Survey,** un ejemplo de simulación de la señal emitida por los puntos de acceso en la Facultad de Derecho se muestra en la Figura 3.3.

En esta figura se observa que los colores van de anaranjado para una señal excelente, hasta el color azul rey que indica una señal muy débil, pasando por una gama de verdes que indican que la señal va perdiendo potencia gradualmente. En esta simulación se tomaron en cuenta los posibles obstáculos como muros, tabla roca, cristales o mobiliario.

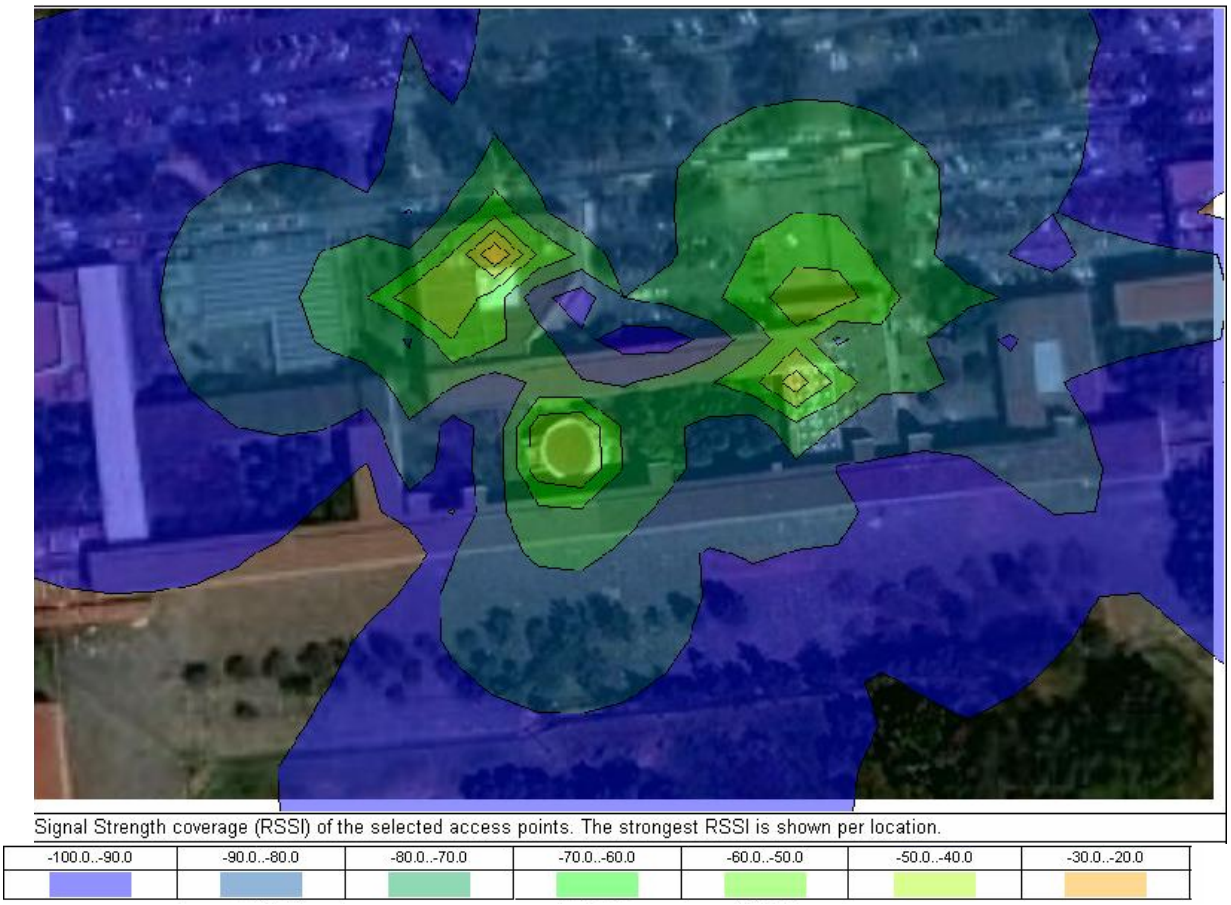


Figura 3.3 Simulación de cobertura a la Facultad de Derecho.

Con el análisis de las necesidades del proyecto y el estudio de cobertura se pudo obtener información que sirvió para la realización del protocolo de pruebas con el que participaron las diferentes empresas con el fin de evaluar

su tecnología, además de que se logró realizar un estimado de la cantidad de puntos de acceso y antenas que se llegarían a utilizar para dar servicio de red inalámbrica en las 59 facultades e institutos, los cuales fueron aproximadamente 270.

3.4.3 Selección de los equipos que se adecuen a las características y necesidades de la red inalámbrica.

De la gran cantidad de tecnologías inalámbricas existentes en el mercado hasta el momento de la selección de equipos se consideraron las siguientes empresas por ser las que contaban con la tecnología que mejor se adecuaba a las necesidades de esta implementación. Dichas empresas son:

- Colubris Networks.
- Enterasys Networks.
- Aruba Networks.
- Foundry Networks.

Estas empresas presentaron sus productos con pláticas informativas de las cuales pudimos recopilar la siguiente información que se presenta en la Tabla 3.2, en la cual se muestran las características principales que cada una de las empresas participantes ofrecía.

Característica	Colubris Networks	Aruba Networks	Foundry Networks	Enterasys Networks
802.11a, b, g	X	X	X	X
WEP	X	X	X	X
WPA	X	X	X	X
WPA2	X	X	X	X
PoE	X	X	X	X
802.1x	X	X	X	X
DHCP	X	X		X
NAT	X	X		X
QoS		X	X	X
Administración centralizada	X	X	X	X
Administración distribuida	X		X	
Detector de intrusos (IDS)	X	X	X	X
SNMP	X	X	X	X
Puntos de acceso de monitoreo	X	X		
Redundancia	X	X	X	
Roaming		X	X	
Detección Rogue AP	X	X	X	
DoS		X	X	X

Tabla 3.2 Características de las empresas participantes.

NOTA: La información presentada en la Tabla 3.2 es un resumen de las características principales de la tecnología de cada empresa. La **X** significa que la empresa cumple con la característica.

Después de analizar las soluciones presentadas por cada empresa, se realizaron pruebas a las mismas con el fin de evaluarlas y determinar cual era la que mejor cubría las necesidades en la red inalámbrica universitaria.

3.4.4 Protocolo de pruebas.

El protocolo de pruebas fue diseñado para la evaluación de las tecnologías inalámbricas y dentro de los aspectos que se consideraron importantes son:

- Cumplir con esquemas de seguridad como WEP, WPA y WPA2.
- Número máximo de usuarios con los cuales el punto de acceso provee un servicio adecuado a una velocidad de transmisión razonable.
- Tipos de administración de los equipos, si es centralizada o distribuida.
- Radio de cobertura, tanto en espacios abiertos como en interiores.
- Monitoreo de recursos, si los equipos inalámbricos incluyen alguna forma de ser monitoreados en cuanto a usuarios, rendimiento, estadísticas de servicio, etc.
- Evaluar si los equipos inalámbricos contaban con NAT y DHCP incluido.
- Soporte para servidor de autenticación.
- Soporte para protocolos de autenticación.
- Soporte para creación de grupos y cuentas de acceso a la red inalámbrica.

- Manejo de diferentes anchos de banda y velocidad de transmisión.

- Costo.

Los puntos anteriores son las características básicas dentro de las necesidades para la implementación de la Red Inalámbrica Universitaria, sin embargo, también se consideraron otras características importantes para mejorar dicho servicio como fueron:

- Redundacia, se refiere a que exista un respaldo del servicio en caso de que ocurra alguna falla en la red inalámbrica tanto en switches, puntos de acceso y fuentes de poder, y la forma en la que se solucionaría el problema.

- Servicios de Roaming. esto se refiere a que los usuarios cuenten con la movilidad que se pretende dar con una red inalámbrica a lo largo de todo el campus sin perder conectividad.

- Puntos de acceso de monitoreo, se refiere a que existan puntos de acceso dedicados a analizar el servicio de la red inalámbrica.

- Soporte para Detector de Intrusos (IDS).

- Soporte para PoE.

3.4.5 Pruebas y resultados de los equipos inalámbricos.

La aplicación de las pruebas se realizó a las empresas: Aruba Networks, Colubris Networks, Foundry Networks y Enterasys Networks y consistieron en armar una maqueta de pruebas de acuerdo con la Figura 3.4. Previo a la implementación de la maqueta se le proporcionó a cada empresa el protocolo de pruebas con el objetivo de que cada una de ellas presentara su equipo inalámbrico con el que pudieran cumplir cada uno de los puntos del protocolo.

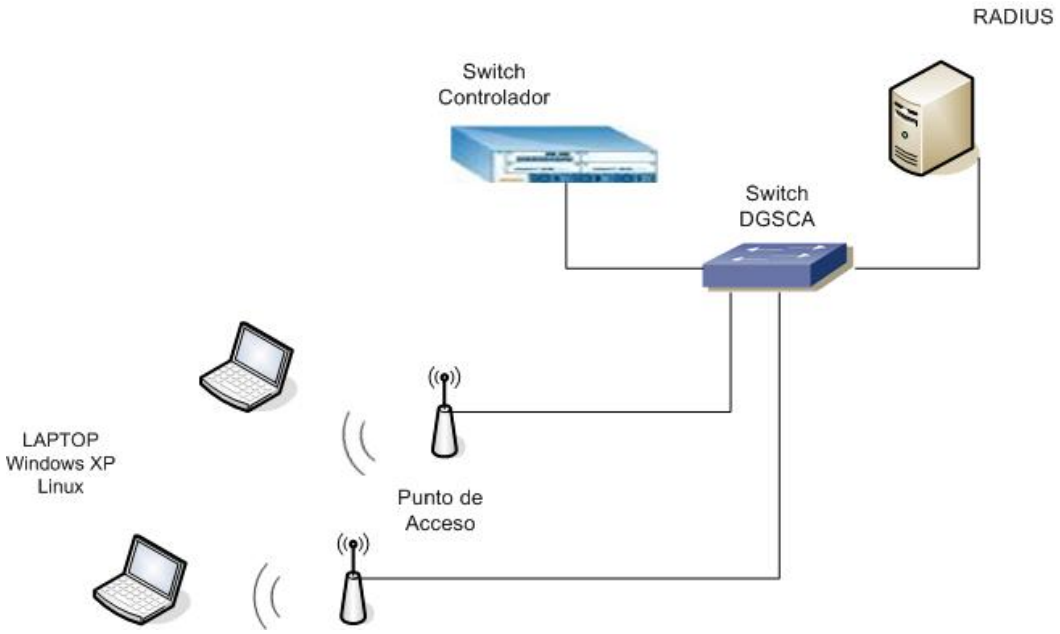


Figura 3.4 Maqueta de pruebas.

La maqueta de pruebas se formó con un switch que da servicio de red en DGSCA al cual se le conectó un servidor RADIUS configurado con los parámetros necesarios, un switch controlador y varios puntos de acceso los cuales eran controlados por el switch controlador.

3.4.5.1 Equipos presentados por las empresas.

El equipo que presentó cada una de las empresas fue:

Aruba Networks:

- Aruba 800 switch controlador.
- Un punto de acceso Aruba 70.
- Tres puntos de acceso Aruba 60.

Colubris Networks:

- Un punto de acceso controlador MSC-3200.
- Dos puntos de acceso MAP-320.

Enterasys Netwoks:

- Enterasys RoamAbout Wireless Switch RBT 8100.
- Plataforma de administracion RoamAbout Switch Manager.
- Dos puntos de acceso.

Foundry Networks:

- Switch controlador.
- Dos puntos de acceso IronPoint 200

3.4.5.2 Pruebas.

Para la realización de las pruebas cada empresa configuró su equipo de acuerdo al protocolo de pruebas y se evaluó punto por punto de éste.

La realización de cada una de las pruebas consistió en:

- Comprobar los esquemas de seguridad. En este punto se evaluó si los equipos inalámbricos soportaban los protocolos WEP, WPA, WPA2, así como el tipo autenticación de usuarios EAP-PEAP, TLS y TTLS. Lo anterior se logró configurando los switches con los diferentes esquemas de seguridad y autenticación.

- Radio de cobertura. Se comprobó el rango de cobertura de los equipos presentados por las empresas tanto en línea de vista como con obstáculos como lo fueron, paredes, muebles, etc.

- Tipos de administración de los equipos. En esta prueba se comprobaron las formas de administración que son soportadas, como por ejemplo la centralizada, así como las ventajas y desventajas de cada una de ellas, se comprobó la forma de administración, es decir, SSH, HTTP, HTTPS, telnet, y CLI, así como también que se pudieran realizar respaldos tanto de las configuraciones como del sistema operativo.

- Transferencia de archivos. Esta prueba consistió en bajar archivos y comprobar la velocidad a la que operaba la red y el tiempo de transmisión de los archivos. Las herramientas que se utilizaron para comprobar la velocidad de la red inalámbrica se encuentran en las páginas web http://www.speakeasy.net y http://www.adsl4ever.com. (Consultadas en Agosto de 2005).

- Monitoreo de recursos. En este punto se evaluó si la plataforma de administración mostraba gráficas en tiempo real de los recursos utilizados y si contaban con monitoreo de recursos mediante SNMP.

- Evaluación de servicios de red. En esta prueba se analizó si se requería de servidores externos de NAT y DHCP o si los switches controladores ya traían incluido el servicio. Así como también soporte para servidor de autenticación RADIUS y LDAP.

- Detección de puntos de acceso intrusos. Consistió en configurar un punto de acceso ajeno a la red con el mismo SSID, si la plataforma de administración no reportaba el suceso la prueba fallaba.

- Soporte para creación de grupos y cuentas. Se realizó con ayuda de un servidor RADIUS en el cual se generaban perfiles de usuario, se conectaron a la red y se verificó que se les asignaran los siguientes atributos:

  - Asignación de VLAN diferente a cada tipo de usuarios.
  - Permisos para uso de aplicaciones por tipo de usuario.
  - Manejo de diferentes anchos de banda para cada usuario.
  - Una sesión por usuario.

Al revisar la configuración del switch se verificó que cada usuario mantuviera sus privilegios y atributos asignados.

3.4.5.3 Resultados.

De las pruebas anteriormente realizadas se obtuvieron los siguientes resultados:

Los puntos de acceso de la empresa **Aruba Networks** cumplieron con:

- Monitoreo de recurso mediante SNMP.
- Administración centralizada.
- Detección de Rogue AP (punto de acceso intruso).
- Verificación de privilegios de usuarios.
- Autenticación con WEP-128, WEP-64, WPA-TKIP, WPA-TTLS, WPA-PEAP, WPA-TLS.
- Control de ancho de banda.
- DHCP.
- NAT.
- Soporte de más de 500 puntos de acceso por switch controlador.
- Soporte para servidor de autenticación.

Además los equipos **Aruba Networks** contaban con las características de:

- Monitoreo de Recursos en tiempo real.
- Administración mediante CLI, HTTPS, Conexión Remota.
- Redundancia en puntos de acceso, switches controladores y fuentes de poder.
- Detección de un ataque de Denegación de Servicios.
- Alarmas UP/DOWN y clasificación de eventos.
- Rate-limit por perfil.
- Roaming.
- Control de tráfico.

Para la empresa **Colubris Networks** estos fueron los resultados:

- Monitoreo de recurso mediante SNMP.
- Redundancia en puntos de acceso.
- Autenticación con WEP-128, WEP-64, WPA-TKIP, WPA-TTLS, WPA-PEAP, WPA-TLS.
- DHCP.
- NAT.
- Control de ancho de banda.
- Control de tráfico.
- Una sesión por usuario mediante RADIUS.
- Soporte para servidor de autenticación.

Foundry Networks cumplió con las siguientes pruebas:

- Monitoreo de recurso mediante SNMP.
- Detección de Rogue AP.
- Autenticación con WEP-128, WEP-64, WPA-TKIP, WPA-TTLS, WPA-PEAP, WPA-TLS.
- Soporte para servidor de autenticación.

Enterasys Netwoks cumplió con las siguientes características

- Monitoreo de recurso mediante SNMP.
- Detección de Rogue AP.
- Autenticación con WEP-128, WEP-64, WPA-TKIP, WPA-TTLS, WPA-PEAP, WPA-TLS.
- DHCP.
- Soporte para servidor de autenticación.

Después de analizar los resultados de la pruebas a los equipos se llegó a la conclusión de que la empresa que cubrió mejor las necesidades de la RIU fue **Aruba Netwoks**, ya que además de cumplir con la mayoría de los puntos del

protocolo de pruebas, tuvo características adicionales de gran ayuda para esta implementación. La más importante fue el soporte por parte del switch controlador que permitió la conexión de más de 500 puntos de acceso lo cual solucionó la conectividad entre la gran cantidad de puntos de acceso necesarios para dar servicio de red inalámbrica a lo largo de Ciudad Universitaria, así como también proporcionó una administración centralizada, un monitoreo eficaz y redundancia de equipo.

3.5 Diseño de la propuesta.

En este tema se explicará la forma en la que se fue diseñando la RIU, así como también se hablará del direccionamiento, la seguridad, la topología de la red inalámbrica y las políticas de uso.

Debido al tamaño de la red inalámbrica y en base a los resultados de los estudios de cobertura se determinó que la infraestructura necesaria fuera:

- Switches. Dos switches Aruba 6000 Modular Mobility Controller, las principales características por las cuales se eligió este equipo fueron:

    - Control de 512 puntos de acceso por switch los cuales cuentan con dos tarjetas modulares, cada una de ellas soporta 256 puntos de acceso.
    - Soporte para 8192 usuarios conectados a los diferentes puntos de acceso.
    - Manejo del protocolo VRRP.

- Puntos de acceso. Después de analizar los alcances de los diferentes puntos de acceso se decidió utilizar aproximadamente 270, los cuales fueron distribuidos de la siguiente manera:

    - Aruba 70 para espacios interiores muy extensos como bibliotecas concurridas, auditorios para más de 300 personas, explanadas,

jardines y cafeterías grandes donde el equipo se colocaba dentro de un edificio, etc.

- Aruba 61 para espacios interiores reducidos como fue el caso de salas de juntas, auditorios, jardines y cafeterías pequeñas para aproximadamente 50 personas, salas de becarios, etc.

- Aruba 60 para espacios exteriores muy extensos donde no fue posible colocar los puntos de acceso dentro de los edificios como la explanada principal de Ciudad Universitaria. Para este modelos se utilizaron antenas externas de alta ganancia y cajas NEMA para cubrir al punto de acceso de la intemperie.

3.5.1 Topología de la RIU.

Otro aspecto dentro del diseño de la RIU fue la incorporación de los switches centrales inalámbricos a la RedUNAM, es decir, se integraron al backbone de la UNAM, esto para que existiera conectividad entre los puntos de acceso conectados a los switches de cada dependencia y los switches controladores Aruba. El backbone de la RedUNAM está compuesto por cuatro switches principales colocados en Arquitectura, Zona Cultural, IIMAS y DGSCA, juntos forman una doble delta y se conectan entre sí por medio de enlaces de fibra a 10 GB.

La topología de la RIU está formada por los siguientes elementos:

- Dos switches controladores.
- Backbone de la RedUNAM.
- Servidores de AAA (Authentication, Authorization and Accounting).

Los dos switches controladores se conectaron entre sí por enlaces de fibra a 1GB lo que permite tener redundancia por medio del protocolo VRRP. Uno de los switches controladores y los servidores AAA se conectaron al nodo DGSCA y el otro switch controlador conectó al nodo IIMAS.

Entre los puntos de acceso y los switches controladores Aruba se forma una topología de estrella.

El esquema de la topología de los switches de la RIU se muestra en la Figura 3.5.

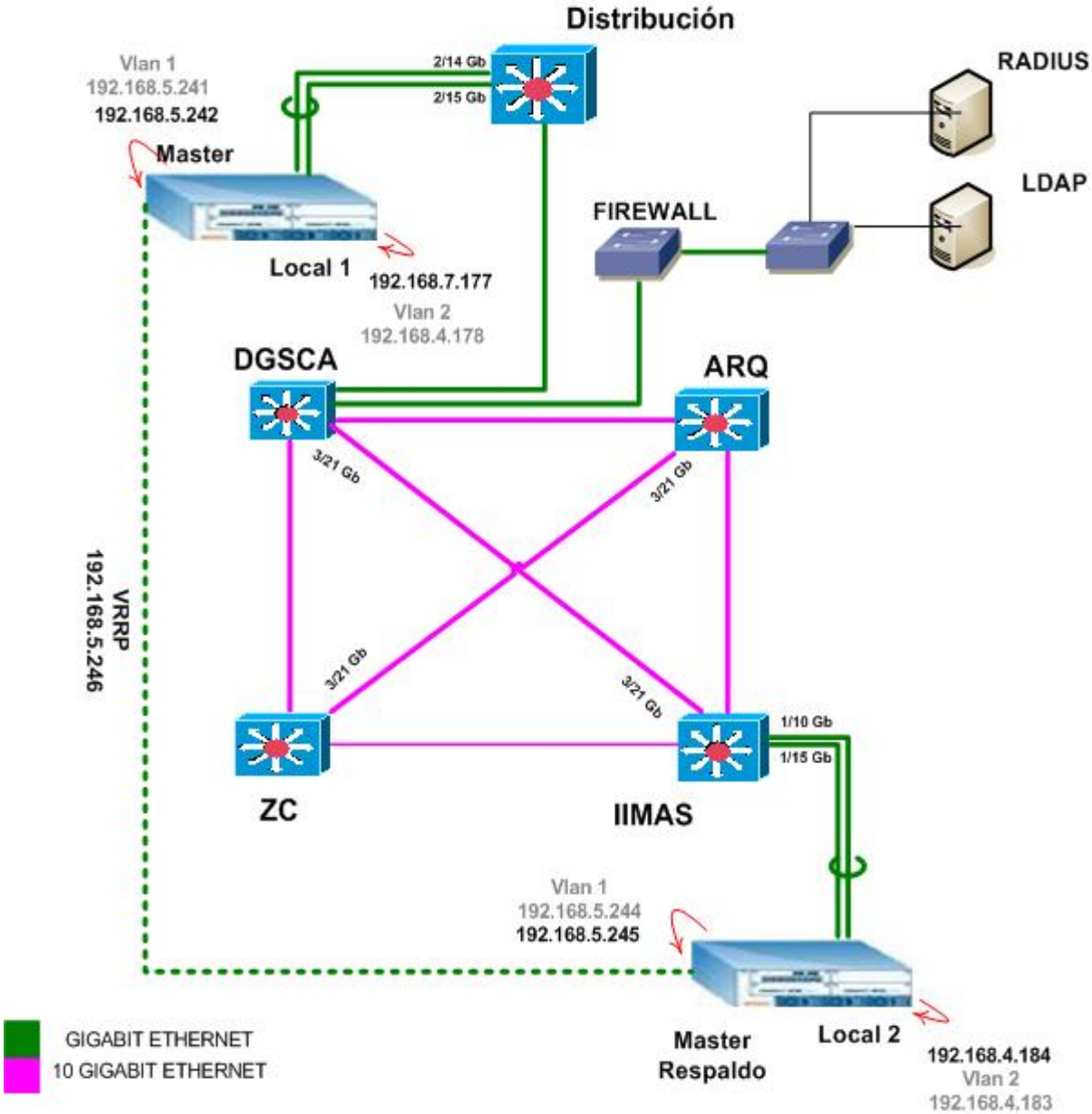


Figura 3.5 Topología de la RIU.

3.5.2 Modo de operación.

La topología de la RIU está formada por dos switches controladores los cuales cuentan con dos tarjetas modulares cada uno, lo que divide al switch lógicamente en dos. El primer switch lo forman el MASTER y el LOCAL1, el segundo switch lo forman el MASTER RESPALDO y el LOCAL2, lo que se observa en la Figura 3.6. Con este esquema se pretendió que se repartiera la carga de trabajo entre los switches y al mismo tiempo que funcionaran como respaldo uno del otro.

Figura 3.6 Diseño lógico de los switches principales de la RIU.

El MASTER está conectado al nodo DGSCA y el MASTER RESPALDO al nodo IIMAS, lo que permite disminuir los puntos de falla de la red inalámbrica, ya que si el MASTER falla, el MASTER RESPALDO entra en operación realizando las funciones de éste.

Así mismo, el LOCAL1 está configurado de tal manera que atiende las peticiones de conexión a los usuarios que pertenezcan a los nodos Arquitectura y DGSCA, al mismo tiempo el LOCAL2 realiza el mismo trabajo para los usuarios de los nodos de Zona Cultural e IIMAS.

Debido a que la administración es centralizada, cuando un punto de acceso es conectado a los switches de la red local de cada dependencia, éste le pide al MASTER su configuración inicial que es transmitida por medio de un tftp.

Entre la información que el MASTER proporciona, se encuentra la configuración de VLAN’s, de subredes y de tablas de ruteo, así como la dirección IP de loopback del switch LOCAL al que se debe conectar cada

punto de acceso, así como también les indica que en caso de que se caiga su switch LOCAL correspondiente, él será el respaldo.

El MASTER es el que proporciona la configuración global como por ejemplo; políticas del firewall, tipo de autenticación, configuración de radiofrecuencia, lo que facilita la configuración y mantenimiento de la red inalámbrica. También mantiene a la RIU actualizada de cualquier eventualidad, por ejemplo cuando un punto de acceso no está en funcionamiento.

Cuando el MASTER se cae la red continúa trabajando sin ninguna interrupción debido a que el switch llamado MASTER RESPALDO está configurado para que automáticamente todos los puntos de acceso se conecten a él sin perder el servicio de conectividad hasta que el switch principal esté arriba de nuevo (este proceso se realiza por medio del protocolo VRRP y por la conexión física que existe entre ellos).

Los switches LOCAL1 y LOCAL2 proporcionan los servicios de DHCP y NAT, éstos servicios son importantes debido a que el DHCP asigna automáticamente las direcciones IP que los usuarios van a utilizar para tener conectividad con la RIU, y que dependen de la zona en la que estén conectados. Para que la red inalámbrica tenga salida a Internet necesita de la traducción de direcciones IP que proporciona NAT. Así mismo operan independientemente del MASTER pero dependen de él para la configuración de la seguridad, políticas, autenticación y radiofrecuencia.

3.5.3 Direccionamiento.

Otro de los aspectos dentro del diseño de la RIU fue la realización del direccionamiento, lo cual fue importante debido a la gran cantidad de dependencias que formaron parte del proyecto y a que no era factible que cada una de ellas proporcionara las direcciones IP necesarias para cada punto de acceso, de esta manera surgió la necesidad de crear un direccionamiento de red propio para la RIU. Al mismo tiempo se trató de separarla de la red local de cada dependencia y así evitar que los usuarios hicieran uso de los recursos de red de las facultades, institutos y centros de investigación.

Los puntos que se tomaron en cuenta para la realización del direccionamiento fueron:

- La cantidad de puntos de acceso necesarios para cubrir las áreas de interés de cada dependencia.

- La cantidad de facultades, institutos y centros de investigación que se asignaron a cada nodo de acuerdo al backbone de la RedUNAM, es decir que todas las dependencias presentes en el proyecto de la RIU fueron distribuidas a uno de los cuatro nodos principales: Arquitectura, Zona Cultural, IIMAS y DGSCA.

- La necesidad de que los usuarios de la RIU pudieran acceder a bibliotecas digitales de la UNAM, ya que esto sólo se logra siendo parte de la RedUNAM.

- El crecimiento a futuro de la RIU.

Analizando los puntos anteriores y considerando el hecho de que se asignaron cinco segmentos de red /24, se comenzó a diseñar el direccionamiento de tal manera que cada dependencia permitiera tener 16 direcciones IP para poderlas asignar a los diferentes puntos de acceso.

Los cinco segmentos de red fueron subneteados /28 por lo que $2^n=16$, con n=4, de tal manera que resultaron 16 subredes por cada segmento de red y 16 host para cada subred.

La Tabla 3.3 hace referencia a una parte del nodo IIMAS (segmento 192.168.3.0) en la que se pueden observar algunos datos del direccionamiento, las cuales se describirán a continuación:

- La primera columna se refiere al número de dependencia.

- La segunda columna se refiere al nombre de la Facultad, Centro o Instituto.

- La tercera columna hace referencia a una red no homologada, dichas direcciones IP son las que serán asignadas por medio de los switches LOCAL a los usuarios que requieran conexión.

  Debido a que es un segmento no homologado, éstas direcciones IP requieren ser traducidas por medio del NAT para dar salida a Internet.

- La cuarta, quinta, sexta, séptima y novena columnas se refieren a la información de red de un segmento homologado para efectos de monitoreo y funcionamiento de los puntos de acceso, sin embargo, por motivos de seguridad en las siguiente figura se muestra su valor modificado.

- La octava columna hace referencia a las localidades de los puntos de acceso, las cuales tienen la funcionalidad de identificar la ubicación de cada uno de ellos en los diferentes edificios. Las localidades están formadas por tres valores que se refieren a edificio, piso y punto de acceso respectivamente.

No	Facultad	Red privada	ID RED	Broadcast	mascara	Ip's	Loc.	gateway
31	Facultad de Medicina	10.30.10.0	192.168.3.0	192.168.3.15	255.255.255.240	192.168.3.1	45.1.1	192.168.3.14
						192.168.3.2	45.1.2	
						192.168.3.3	45.2.1	
						192.168.3.4	45.1.3	
						192.168.3.5	45.1.4	
						192.168.3.6	46.2.2	
						192.168.3.7	46.1.5	
						192.168.3.8	46.1.1	
32	Facultad de Química	10.30.11.0	192.168.3.16	192.168.3.31	255.255.255.240	192.168.3.17	47.1.1	192.168.3.30
						192.168.3.18	47.1.2	
						192.168.3.19	47.1.3	
						192.168.3.20	48.1.1	
						192.168.3.21	48.2.1	
33	Instituto de Fisiología Celular	10.30.12.0	192.168.3.32	192.168.3.47	255.255.255.240	192.168.3.33	49.1.1	192.168.3.46
						192.168.3.34	49.1.2	
						192.168.3.35	49.2.1	
34	Instituto de Química	10.30.13.0	192.168.3.48	192.168.3.63	255.255.255.240	192.168.3.49	50.1.1	192.168.3.62
						192.168.3.50	50.1.2	
						192.168.3.51	51.1.1	
						192.168.3.52	51.2.1	
						192.168.3.53	52.1.1	
						192.168.3.54	52.1.2	
						192.168.3.55	52.2.1	
35	Facultad de Economía	10.30.14.0	192.168.3.64	192.168.3.79	255.255.255.240	192.168.3.65	53.1.1	192.168.3.78
						192.168.3.66	53.1.2	
						192.168.3.67	53.2.1	
						192.168.3.68	54.1.1	
						192.168.3.69	54.1.2	
						192.168.3.70	54.1.3	
						192.168.3.71	54.1.4	

Tabla 3.3 Algunas dependencias del direccionamiento del nodo IIMAS.

3.5.4 Diseño de la Seguridad.

Las redes inalámbricas han tenido un crecimiento notable en los últimos años debido a su facilidad de instalación y conexión, lo que permite facilitar el trabajo al usuario y mejorar las opciones de conexión. Sin embargo no todas son ventajas al hablar de las redes inalámbricas porque la implementación de éstas sin algún tipo de seguridad es riesgoso ya que alguna persona que capte desde el exterior un punto de acceso puede no solo entrar a la red de la compañía sino emplearla también como ataque hacia otras empresas sin ser detectado, navegar gratis en la Intranet, robar software e información o introducir virus y demás códigos maliciosos.

Como se vio en Capítulo 2 existen varios mecanismos de seguridad que se pueden implementar en una red inalámbrica con los cuales se busca tener medidas de seguridad que garanticen la integridad, confidencialidad, autenticidad y disponibilidad, es decir, conservación de la información que se maneja, por lo tanto se busca que sea lo menos vulnerable a ataques de denegación de servicios, instalación de sniffers, robo de contraseñas por medio de ataques de diccionario, ataques de fuerza bruta, etc.

En el diseño de la seguridad de la red inalámbrica universitaria se consideró que debido a la gran cantidad e importancia de la información que se maneja en la UNAM el acceso a la RIU no podía ser abierta, además de que el objetivo era tratar de evitar ataques y vulnerabilidades implementando un mecanismo de seguridad junto con la integración de las características del switch controlador Aruba en cuanto a seguridad, por ejemplo, éste evita ataques de Denegación de Servicos (DoS), detecta y deniega conexiones ad-hoc y puntos de acceso intrusos, etc.

Como parte del diseño de la seguridad se consideró utilizar un mecanismo de autenticación en doble vía, para lo cual en un principio se tomaron en cuenta los protocolos de seguridad WEP y WPA, debido a que se buscaba incluir la mayoría de los sistemas operativos tanto de laptop’s como de PDA’s (Windows 98, Windows Me, Windows XP, Windows 2000, Linux y Mac OS, Windows Mobile, Palm OS, etc). Sin embargo debido a las vulnerabilidades ya mencionadas de éste, se consideró solamente implementar un mecanismo

más robusto, el cual fue WPA, teniendo como opción de actualización a WPA2 intentando que en un futuro la transición fuera transparente a los usuarios.

La implementación de WPA en RIU está formada por el protocolo de autenticación 802.1x que integra tres elementos, los cuales son un cliente, un autenticador (que para este caso son los puntos de acceso) y un servidor de autenticación RADIUS. Para completar este mecanismo se utiliza PEAP, lo que permite el uso de credenciales de autenticación únicas para cada cliente, es decir, el usuario introduce su nombre de usuario y contraseña manualmente.

El servidor RADIUS está certificado digitalmente por medio de Thawte y le asegura al cliente que el servidor de autenticación al cual se está conectando es el verdadero.

Las credenciales de todos los usuarios de RIU se encuentran en un servidor LDAP. Así mismo la información intercambiada entre el servidor y sus clientes es cifrada con un túnel TLS.

3.5.5 Políticas de uso.

La creación de políticas de uso es importante porque los usuarios deben utilizar la RIU en forma responsable, ya que es un servicio de gran utilidad para toda la comunidad universitaria.

Las políticas de uso para la red inalámbrica universitaria fueron realizadas por la Dirección General de Servicios de Cómputo Académico y pueden ser consultadas en la página web www.riu.unam.mx/politicas.htm

CAPÍTULO 4

IMPLEMENTACIÓN DE LA RED INALÁMBRICA UNIVERSITARIA

Una vez concluida la etapa del diseño de RIU se realizó la implementación de la misma, siendo el último capítulo de este trabajo de tesis.

En este capítulo se hablara acerca de las etapas que formaron parte de la implementación, como lo fueron la configuración e instalación de los equipos requeridos en la red inalámbrica, se mencionarán los problemas que se presentaron durante la implementación, se hablará también acerca de la etapa de pruebas para la RIU y los resultados observados, así como de la forma en la que se estará monitoreando.

4.1 Etapas de Implementación.

Esta etapa fue la más importante porque en ella se materializaron cada una de las partes del diseño. Su realización permitió desarrollar todos los aspectos teóricos planteados durante el mismo y de esa manera poder cumplir con los objetivos principales del proyecto.

Las etapas de implementación fueron las siguientes:

- Realización del cableado para los puntos de acceso.
- Revisión del cableado.
- Configuración de puntos de acceso, switches controladores y servidores AAA.
- Instalación de puntos de acceso y switches controladores.
- Realización de manuales para los usuarios.
- Verificación de conectividad de los puntos de acceso con los switches controladores.
- Señalización de las zonas de cobertura RIU.
- Sistema de monitoreo para la RIU.
- Etapa de pruebas con usuarios reales.
- Puesta en operación, asesoría y configuración de equipos para los usuarios de la RIU.

4.2 Cableado de nodos.

Como primera parte en la implementación de la RIU se contrató a una empresa, que sería la responsable del cableado estructurado de los puntos de red necesarios para colocar los puntos de acceso en las 59 dependencias.

En esta etapa no fue necesario cablear los 270 puntos de red ya que en algunos casos solo se trataba de reubicaciones.

Esta empresa también se encargo de etiquetar y escanear todos los puntos de red donde se iba a colocar un punto de acceso, con el fin de verificar que éstos funcionaran e identificarlos en los equipos activos.

Los puntos de red que se cablearon quedaron rematados, del lado de los puntos de acceso en su mayoría en faceplates y algunos otros fueron rematados con conector RJ45 para los casos en los que se puso caja NEMA, en el otro extremo en el cuarto de telecomunicaciones quedaron en un panel separado y etiquetado.

Para optimizar los tiempos de finalización en el diseño, se dividió el cableado y la instalación en tres etapas. Durante la primera y la segunda etapa se cablearon 100 puntos de red, en la tercera se cablearon los últimos 70 puntos, todos ellos en los lugares que se decidieron durante la etapa de diseño.

En la Tabla 4.1 se muestran las etapas del cableado las cuales se agruparon por nodos del backbone de la RedUNAM.

Etapa	Puntos de acceso	Zona
Etapa 1	100	Arquitectura y Zona Cultural
Etapa 2	100	IIMAS
Etapa 3	70	DGSCA

Tabla 4.1 Etapas del cableado.

4.3 Configuración de equipo.

Durante el levantamiento del cableado se comenzó la configuración de los equipos controladores que permiten administrar la red inalámbrica, posteriormente se configuraron los puntos de acceso y los servidores AAA. A continuación se describirá cómo se realizó la configuración de éstos.

4.3.1 Configuración de switches controladores.

La configuración de los switches controladores Aruba se llevó a cabo con la ayuda de los ingenieros de la empresa Aruba Netwoks, de los ingenieros de la empresa ITNova, ya que es una de las representantes de Aruba Networks en México y de los ingenieros del departamento de Redes de la DGSCA.

La principal información configurada en el switch fue:

- Configuración del SSID, en este caso “RIU”.
- Establecer la función que tendrá cada switch, es decir, si será LOCAL o MASTER.
- Dirección IP de administración para cada uno de los switches.
- Dirección de los DNS.
- Protocolo de seguridad WPA y 802.1x.
- Habilitar el protocolo 802.3af.
- Establecer los radios 802.11a/b/g.
- Dirección IP del servidor RADIUS y su respaldo.
- Establecer VLAN’S para cada una de las subredes establecidas en el direccionamiento.
- Establecer los parámetros para la asignación de direcciones IP para cada VLAN por medio de DHCP.
- Habilitar el uso de NAT y establecer el rango de direcciones IP que utilizará.
- Habilitar el protocolo VRRP entre los switches MASTER y MASTER RESPALDO.
- Aplicación de políticas en el firewall y activación de IDS.
- Configuración de los parámetros del protocolo SNMP.

4.3.2 Configuración de puntos de acceso.

Una vez que la empresa encargada del cableado entregó los primeros 100 puntos, la empresa ITNova, comenzó la configuración de los puntos de acceso correspondientes basándose en la información del direccionamiento que fue definido con anterioridad y debido a que la administración es centralizada, es decir, que el switch controlador es el encargado de la administración de todos los puntos de acceso, seguridad, etc, se deben configurar los siguientes parámetros:

- La dirección IP del MASTER que les permita conectarse a éste y obtener su configuración inicial.
- Para fines de administración también se requiere configurarles una dirección IP válida, así como un gateway y una máscara.
- Una localidad que nos permita conocer la ubicación del punto de acceso dentro de Ciudad Universitaria, con el siguiente formato: *edificio.nivel.número*

4.3.3 Configuración de servidores AAA.

Para llevar a cabo el mecanismo de Autenticación, Autorización y Conteo de la RIU se implementó un servidor RADIUS con las herramientas openssl y freeradius y un servidor LDAP instalando la herramienta ldap, lo anterior bajo un sistema operativo Linux.

Para la configuración del servidor RADIUS se le habilitó el modo de autenticación utilizado PEAP y se le configuró las direcciones IP de los switches centrales y del servidor LDAP.

El servidor LDAP se configuró para almacenar la información de todos los usuarios de la RIU. Por su parte los servidores AAA están protegidos por el firewall de la RedUNAM.

4.4 Instalación de switches controladores y puntos de acceso.

Una vez configurados los switches controladores Aruba y siguiendo el diseño de la RIU, se instalaron de la siguiente manera, el equipo que forman el MASTER y el LOCAL1 se instaló en DGSCA y el equipo compuesto por MASTER RESPALDO y LOCAL2 se colocó en IIMAS.

Para la instalación de los puntos de acceso, la empresa ITNova comenzó con la colocación de los mismos en los primeros 100 nodos de red terminados junto con sus respectivos inyectores PoE. que son los que le proveen energía

eléctrica desde los cuartos de telecomunicaciones. Para proporcionarle alimentación de red y de corriente eléctrica al mismo tiempo se conectó un patchcord del faceplate al punto de acceso.

Así mismo como parte de la colocación, se consideró asegurar físicamente y en la medida de lo posible los puntos de acceso, manteniéndolos fuera del alcance de un atacante y también protegiéndolos de robo físico por lo que fueron sujetados por dos abrazaderas de metal.

El procedimiento anterior fue el mismo para las siguientes etapas del cableado e instalación, la única diferencia fue que durante la tercera etapa se colocaron las cajas NEMA con sus respectivas antenas.

Figura 4.1 Nodos y faceplate para los puntos de acceso de la RIU.

En la Figura 4.1 se muestra la instalación de patch panel para los nodos de los puntos de acceso de la RIU, así como un faceplate que quedó en el techo para la conexión del punto de acceso.

Figura 4.2 Colocación de un punto de acceso.

En la Figura 4.2 se muestra la colocación completa de puntos de acceso. En la figura izquierda se observa un caso para interiores en donde la instalación del punto de acceso fue en el techo, la antena forma 90˚ con respecto al techo con lo cual se logra dar cobertura de 360˚ a su alrededor.

En la figura derecha se observa un caso para exteriores, donde el punto de acceso esta dentro de una caja NEMA con una antena externa omnidireccional de 5dBi.

4.5 Etapa de pruebas.

La etapa de pruebas comenzó con los primeros 100 puntos de acceso instalados y tuvo como objetivo verificar la conectividad de cada uno de ellos hacia el switch controlador, así mismo sirvió para comprobar la compatibilidad de los dispositivos inalámbricos, tratando de resolver los problemas que se presentaban.

Durante esta etapa se levantó la conexión de todos los puntos de acceso hacia los switches controladores y se verificó que cada uno de ellos bajara correctamente su imagen del MASTER, posteriormente que se alojaran en su switch LOCAL correspondiente; en caso contrario se buscaba la razón por la cual no funcionaba correctamente, pudiendo ser dichas fallas debido a la configuración, cableado o defecto físico.

Antes de dar a conocer la RIU a los usuarios finales se realizaron pruebas en la que sólo personal de la Dirección de Telecomunicaciones de la DGSCA tenía acceso, para comprobar la conectividad de los equipos inalámbricos hacia los puntos de acceso desde diferentes lugares con cobertura, así mismo se realizaron manuales de ayuda para la configuración de los diferentes sistemas operativos capaces de conectarse a la RIU como: Windows XP, Windows 2000, Linux, Macintosh OS 10 y Windows Mobile.

Cuando se terminó de verificar la conectividad de la RIU se proporcionaron cuentas de prueba a los administradores de red de cada dependencia y manuales de configuración de RIU, con el objetivo de que algunos usuarios utilizaran la red inalámbrica y reportaran anomalías como por ejemplo: interferencias que se producían entre la RIU y sus redes inalámbricas locales, fallas en la asignación de direcciones IP por medio del DHCP, dificultades en la conexión debido a falta de soporte del protocolo de cifrado, entre otras cosas. Además de que estas pruebas ayudaron a realizar un listado de tarjetas inalámbricas de computadoras portátiles y PDA´s que soportaran el protocolo utilizado en RIU para darlo a conocer a los usuarios.

También durante esta etapa se comenzó la señalización de los lugares con cobertura de la RIU para que los usuarios pudieran identificar fácilmente las zonas adecuadas para poder contar con conexión a la RIU.

En la Figura 4.3 se muestra el símbolo de la señalización de la cobertura de la RIU. Este ejemplo se encuentra en la explanada de la Facultad de Derecho.

Figura 4.3 Señalización de la RIU.

4.6 Problemas de implementación.

La implementación de la red inalámbrica universitaria tuvo algunas dificultades debido a la gran cantidad de puntos de acceso que se colocaron y a las diferencias en la administración de las redes locales de cada dependencia.

Para resolver esto, fue importante analizar los inconvenientes que se presentaron para lograr un buen funcionamiento de la red inalámbrica y evitar que dichos problemas sucedieran en la menor medida de lo posible, ya que provocaron retrasos en la terminación del proyecto.

Dichos problemas se describen a continuación:

- Durante el levantamiento del cableado se presentaron dificultades debido a que el acceso a lugares como bibliotecas y auditorios no siempre era posible ya que interfería con las actividades de las dependencias y no se podía trabajar durante conferencias, talleres, eventos especiales, etc. Esto provocó retrasos en la entrega de los nodos y por lo tanto en la colocación de los puntos de acceso.

- En cuanto al cableado se tuvieron algunos errores de etiquetado y de escaneo de UTP, esto provocó que al momento de instalar los puntos de acceso no se encontraran los nodos correspondientes o que el equipo no encendiera.

- Algunos equipos de dónde dependían los puntos de acceso eran hubs (medios compartidos), esto provocó que los puntos de acceso no bajaran la configuración inicial correctamente, que perdieran conectividad más frecuentemente con el MASTER y que no proporcionaran un buen servicio a los usuarios, ya que dependía del tráfico que se generaba en los hubs.

- Algunas dependencias contaban con un firewall en su red local, lo cual no permitía la comunicación entre el punto de acceso y el MASTER. Esta situación se solucionó hasta que se establecieron las reglas correctas que permitieran establecer una comunicación adecuada.

- Falta de conectividad debido a errores en la configuración de los switches controladores, de los puntos de acceso o por defectos de fábrica de los equipos.

- Problemas de la red local de las dependencias ya que algunas veces contaban con equipo de cable coaxial o conector telco que no permitían conectar los puntos de acceso, en esos casos se tuvo que realizar la conexión en lo que la dependencia actualizaba sus equipos.

- Algunas dependencias no contaban con puntos de red disponibles en sus equipos activos para los puntos de acceso y la DGSCA les proporcionó switches para solucionar el problema.

- En cuanto a la configuración de los equipos inalámbricos, algunos usuarios no lograban conectar sus equipos debido a que no contaban, en el caso del sistema operativo Windows con el Service Pack correspondiente a la versión (XP con SP2 y 2000 con SP4), y además de que algunas tarjetas inalámbricas no contaban con la actualización para soportar el protocolo WPA.

4.7 Monitoreo de la red inalámbrica.

Uno de los aspectos importantes a tomar en cuenta dentro de la administración de una red, es monitorear los eventos que suceden en ella, es decir, conocer el uso que se le da a la red de acuerdo al ancho de banda utilizado, la disponibilidad de los equipos ya sea switches controladores o puntos de acceso, cuál es la utilización de la red inalámbrica por zonas, etc., así mismo tener conocimiento cuando un equipo no esta trabajando correctamente, es decir, si el equipo se encuentra apagado o inestable.

De esta manera un sistema de monitoreo ofrece la ventaja de administrar, prevenir y/o detectar los posibles problemas de la red inalámbrica a través de gráficas y datos.

Debido a la importancia de monitorear continuamente la red, la RIU cuenta con dos sistemas que realizan dicha tarea los cuales se complementan uno con otro, ya que se pueden obtener diferentes datos de cada uno de ellos. Uno es un sistema propietario de ARUBA llamado “The Aruba Mobility

Management System", el otro es un sistema implementado con software libre llamado Cacti.

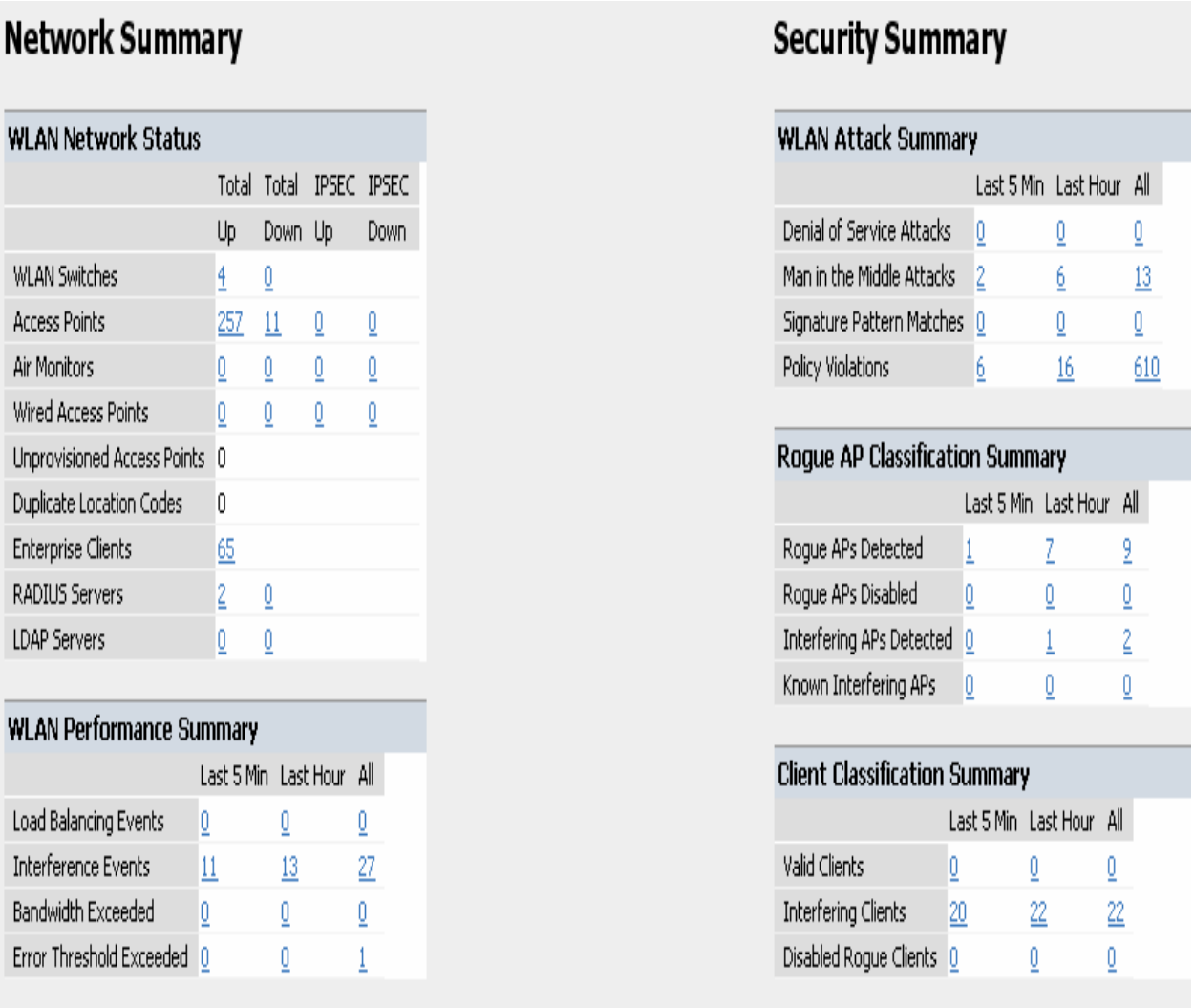
The Aruba Mobility Management System.

La consola de administración de los switches controladores de Aruba permite conocer entre otras cosas el estado de los dispositivos, es decir si los switches, servidores RADIUS y los puntos de acceso se encuentran funcionando o no, también permite realizar actualizaciones, respaldos a los equipos y conocer cuantos usuarios están conectados, la zona en la que se encuentran y el switch LOCAL al cual están asociados.

Otra de las herramientas que ofrece este sistema de monitoreo es que tiene integrado un Detector de Intrusos, el cual nos permite identificar los accesos no autorizados o el uso incorrecto de la red inalámbrica, algunas de las características de éste son las siguientes:

- Detección de Rogue AP (intrusos) o de interferencia.
- Denegación de Servicio (DoS).
- Detección de ataque hombre en medio.
- Detecta y desactiva redes ad-hoc.

En la Figura 4.4 se puede observar el menú principal del monitoreo Aruba, en el que se muestra el estado de los puntos de acceso, de los switches controladores, de los clientes y de los ataques presentados en la RIU.



Network Summary

WLAN Network Status

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Switches	4	0		
Access Points	257	11	0	0
Air Monitors	0	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate Location Codes	0			
Enterprise Clients	65			
RADIUS Servers	2	0		
LDAP Servers	0	0		

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	11	13	27
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	1

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	0	0	0
Man in the Middle Attacks	2	6	13
Signature Pattern Matches	0	0	0
Policy Violations	6	16	610

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	1	7	9
Rogue APs Disabled	0	0	0
Interfering APs Detected	0	1	2
Known Interfering APs	0	0	0

Client Classification Summary

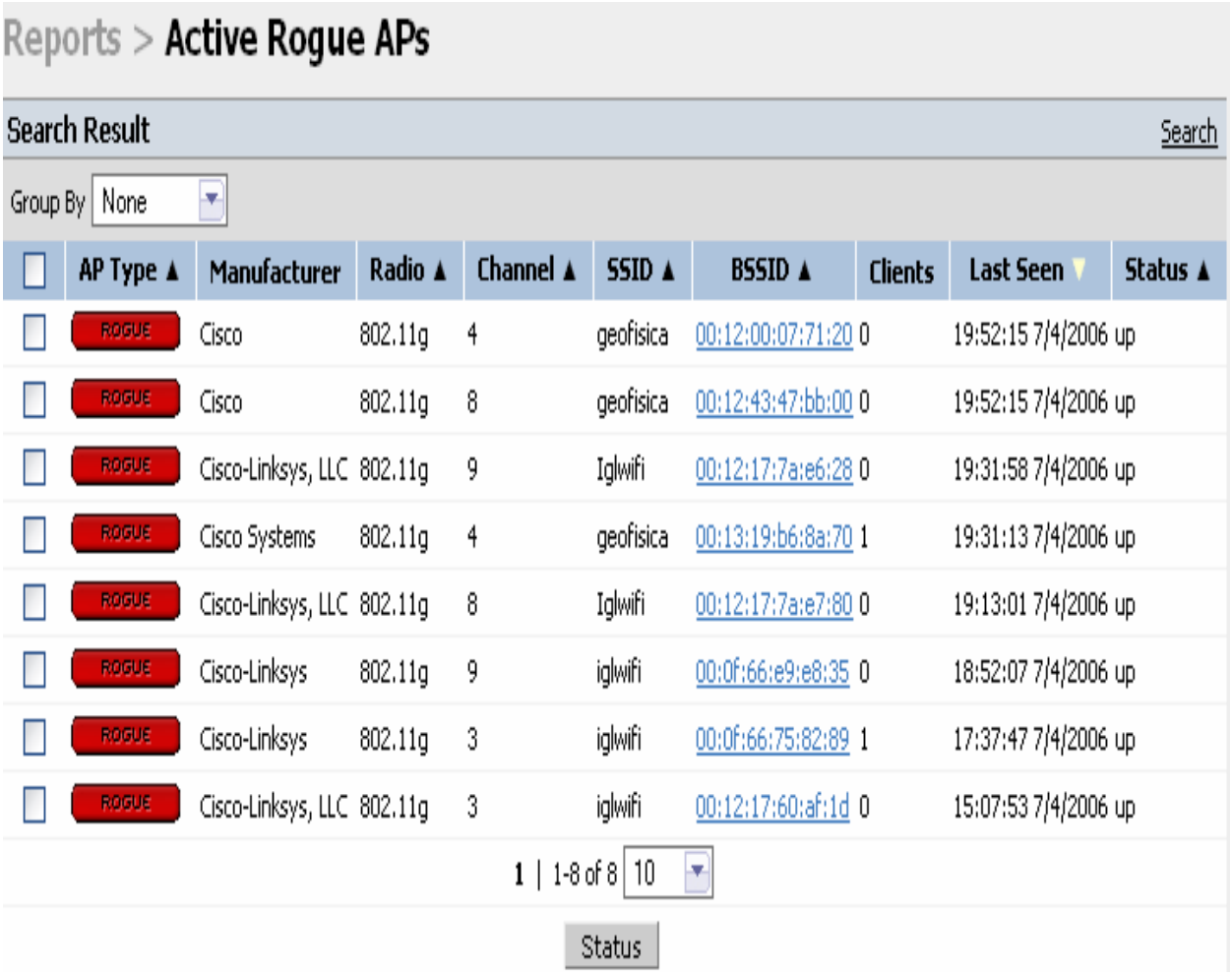
	Last 5 Min	Last Hour	All
Valid Clients	0	0	0
Interfering Clients	20	22	22
Disabled Rogue Clients	0	0	0

Figura 4.4 Información presentado por el sistema de monitoreo Aruba.

En la Figura 4.5 se muestra un ejemplo de un ROGUE AP, en la cual se observa la ubicación, marca del equipo y la dirección física (MAC address) del mismo, el SSID, el canal en el que esta operando y la fecha en que lo detectó.

Estos resultados son debido a que como ya se mencionó con anterioridad, en Ciudad Universitaria existen muchas redes inalámbricas que no son parte de la RIU, este sistema de monitoreo Aruba tiene la habilidad de detectar un punto de acceso que causa interferencia o intruso y los clasifica de acuerdo a

su comportamiento, al mismo tiempo que los bloquea y no los deja trabajar hasta que se verifica su identidad.



Reports > Active Rogue APs

Search Result — Search

Group By: None

	AP Type	Manufacturer	Radio	Channel	SSID	BSSID	Clients	Last Seen	Status
	ROGUE	Cisco	802.11g	4	geofisica	00:12:00:07:71:20	0	19:52:15 7/4/2006	up
	ROGUE	Cisco	802.11g	8	geofisica	00:12:43:47:bb:00	0	19:52:15 7/4/2006	up
	ROGUE	Cisco-Linksys, LLC	802.11g	9	Iglwifi	00:12:17:7a:e6:28	0	19:31:58 7/4/2006	up
	ROGUE	Cisco Systems	802.11g	4	geofisica	00:13:19:b6:8a:70	1	19:31:13 7/4/2006	up
	ROGUE	Cisco-Linksys, LLC	802.11g	8	Iglwifi	00:12:17:7a:e7:80	0	19:13:01 7/4/2006	up
	ROGUE	Cisco-Linksys	802.11g	9	iglwifi	00:0f:66:e9:e8:35	0	18:52:07 7/4/2006	up
	ROGUE	Cisco-Linksys	802.11g	3	iglwifi	00:0f:66:75:82:89	1	17:37:47 7/4/2006	up
	ROGUE	Cisco-Linksys, LLC	802.11g	3	iglwifi	00:12:17:60:af:1d	0	15:07:53 7/4/2006	up

1 | 1-8 of 8 | 10

Status

Figura 4.5 Reporte de Rogue AP.

Cacti

El segundo sistema de monitoreo consiste en la utilización del software llamado Cacti. Esta herramienta está instalada en un servidor con sistema operativo Linux y realiza gráficas de acuerdo a los datos enviados por los switches controladores por medio de peticiones SNMP.

Cacti permite cuantificar el uso de la RIU, al mismo tiempo ayuda a generar gráficas que muestran la cantidad de usuarios conectados, la cantidad de puntos de acceso asociados a los switches controladores y el tráfico generado en éstos.

En las siguientes figuras se muestran las gráficas que se pueden generar mediante Cacti, éstos datos fueron generados en un día.

En la Figura 4.6 se observa la cantidad de puntos de acceso asociados al switch LOCAL1, en promedio detecta 140 puntos de acceso.

En la Figura 4.7 se muestra la gráfica de los clientes asociados al switch LOCAL1, esto se refiere a los clientes inalámbricos que están utilizando el servicio de la RIU en las dependencias asociadas a los nodos DGSCA y Arquitectura.

En la Figura 4.8 se muestra la gráfica de la utilización de CPU del switch LOCAL1 se observa que el porcentaje es del 20% y su uso se mantiene constante a lo largo del día.

En la Figura 4.9 se muestra la gráfica del ancho de banda utilizado por el enlace del switch LOCAL1, se observa un máximo de entrada 6.66 Mbps y un máximo de salida de 6.84 Mbps, las horas en las que se hace mayor uso son de las 8 am a las 6 pm.

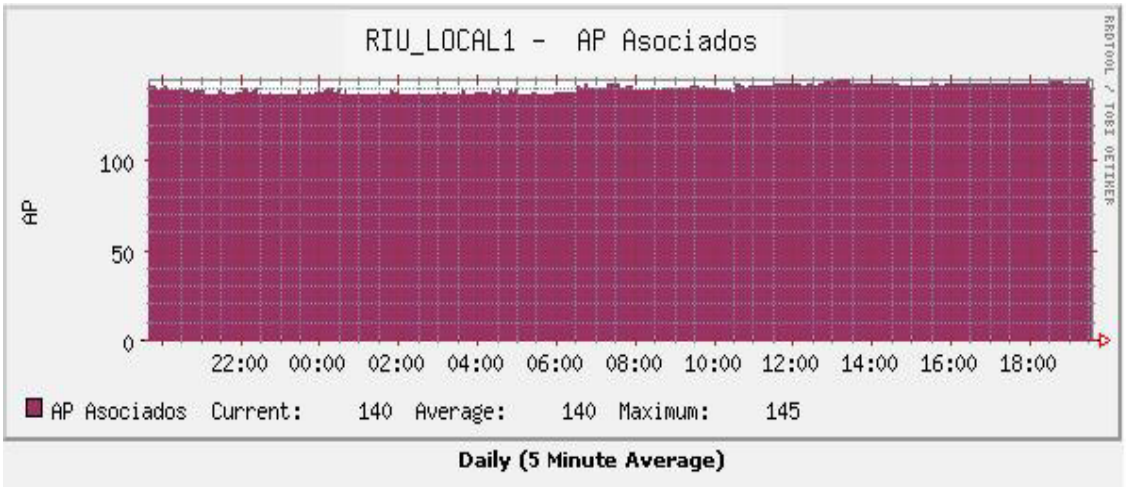


Figura 4.6 Gráfica de puntos de acceso asociados al switch LOCAL1.

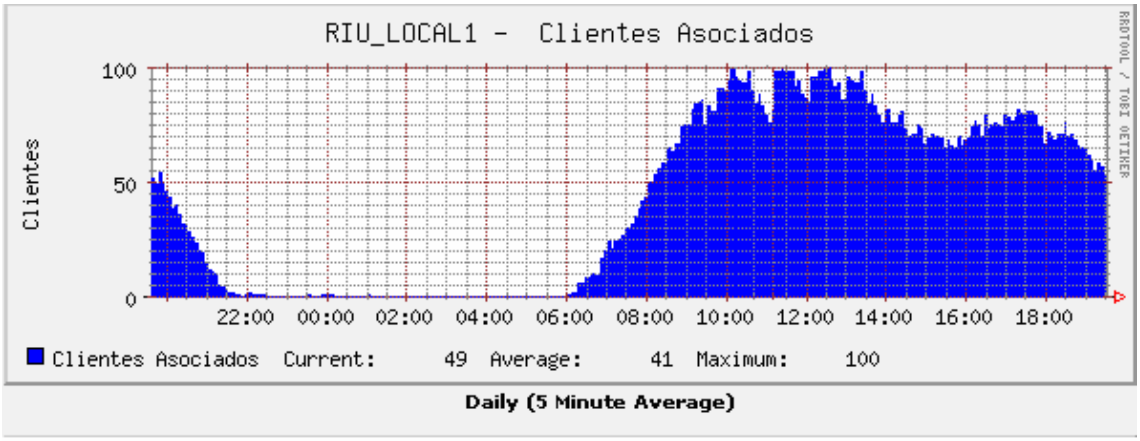


Figura 4.7 Gráfica de clientes asociados al switch LOCAL1.

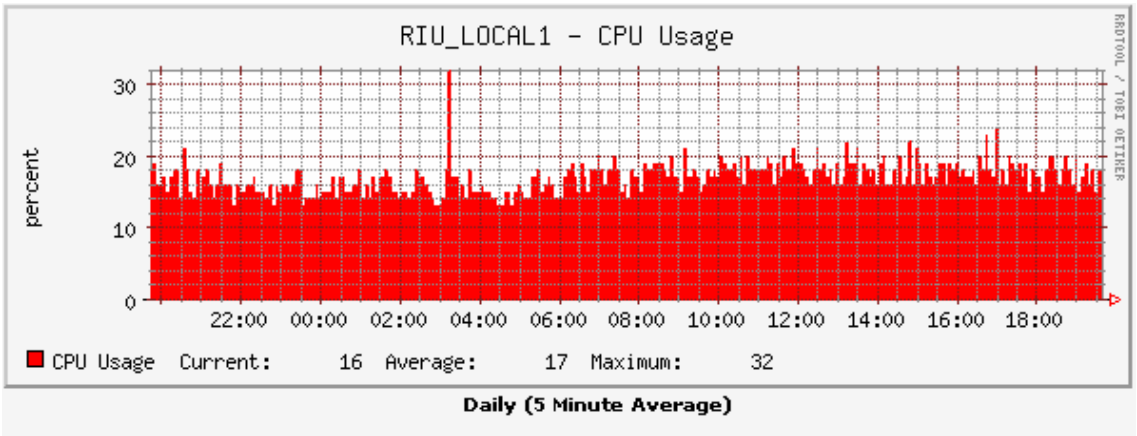


Figura 4.8 Gráfica de utilización de CPU del switch LOCAL1.

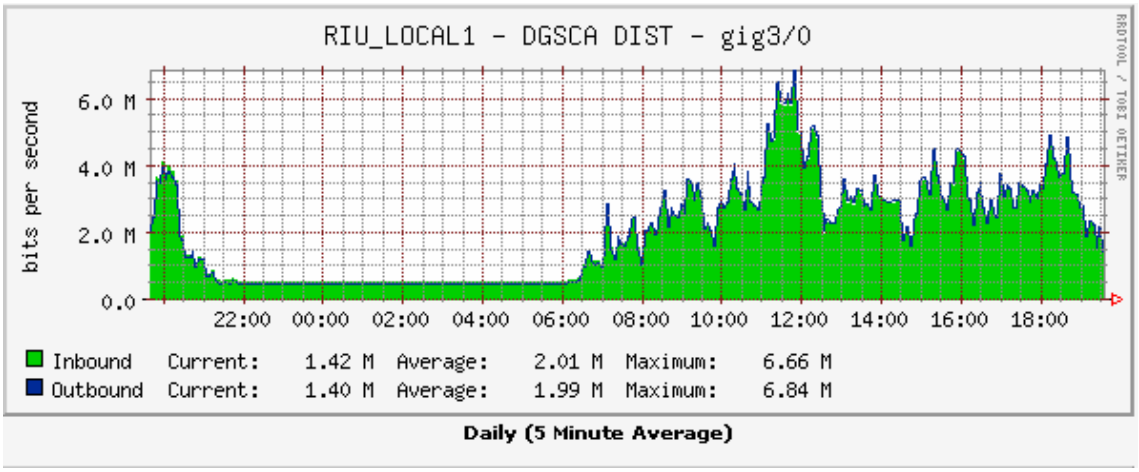


Figura 4.9 Gráfica del ancho de banda utilizado del switch LOCAL1.

4.8 Puesta en Operación.

Al solucionarse la mayoría de los problemas que se presentaron durante la etapa de pruebas y una vez implementados los sistemas de monitoreo, en el mes de mayo del 2006 entró en operación la RIU para la comunidad universitaria.

La creación de las cuentas de acceso para cada alumno, investigador y académico comienza realizando un registro en línea, posteriormente los usuarios deberán acudir al departamento de atención a usuarios de la DGSCA para acreditar que forman parte de la UNAM. De ésta manera obtendrán su cuenta personalizada, es decir, nombre de usuario y contraseña diferente para cada usuario; con lo que podrán hacer uso de la RIU en cualquier lugar de Ciudad Universitaria con cobertura de red inalámbrica.

En el caso de los alumnos, las cuentas se deben renovar cada vez que inicie un nuevo semestre y mientras sigan siendo estudiantes activos, en el caso de los académicos e investigadores tienen vigencia por un año.

Para los becarios de las distintas dependencias de la UNAM y que no sean estudiantes, es necesario llevar a DGSCA una carta de la institución en la que

se encuentra realizando algún proyecto, en la que se solicite una cuenta de la RIU.

Las cuentas de invitado se refieren a las personas que vienen a congresos, conferencias, etc y que no permanecen mucho tiempo en Ciudad Universitaria. Para obtener este tipo de cuentas se requiere una carta de invitado expedida por la facultad visitada.

Dado que la RIU permite trabajar con el estándar IEEE 802.11a/b/g al mismo tiempo, para que un cliente inalámbrico pueda conectarse a ella se requiere que los equipos funcionen con alguno de estos estándares y con el mecanismo de cifrado WPA.

La conexión de un dispositivo móvil hacia la RIU se describe a continuación.

Una vez que el dispositivo inalámbrico detecta la señal de la red inalámbrica (SSID), éste intenta conectarse a la RIU para lo cual el punto de acceso realiza un túnel GRE hacia el switch controlador. A través de ese túnel se manda la información del usuario, es decir, nombre de usuario y contraseña. El switch controlador envía las credenciales de usuario hacia el servidor RADIUS, éste a su vez busca las credenciales dentro del servidor LDAP para determinar si es un usuario válido o no, si el resultado es exitoso el cliente es aceptado y el servidor de DHCP le proporciona una dirección IP del segmento 10.x.x.x de acuerdo al direccionamiento y al lugar donde se encuentra el cliente, dicha dirección IP será traducida por NAT a una dirección válida para poder tener salida a Internet, si el proceso anterior resultó exitoso el usuario podrá utilizar el servicio de la red inalámbrica universitaria RIU.

En caso de que la autenticación falle las credenciales serán pedidas de nuevo y la auto-negociación se realizará otra vez.

La Figura 4.10 muestra la forma en la que un cliente inalámbrico establece la conexión a la RIU, se pueden observar también los dispositivos que cuentan con el protocolo para poder ingresar a la RIU.

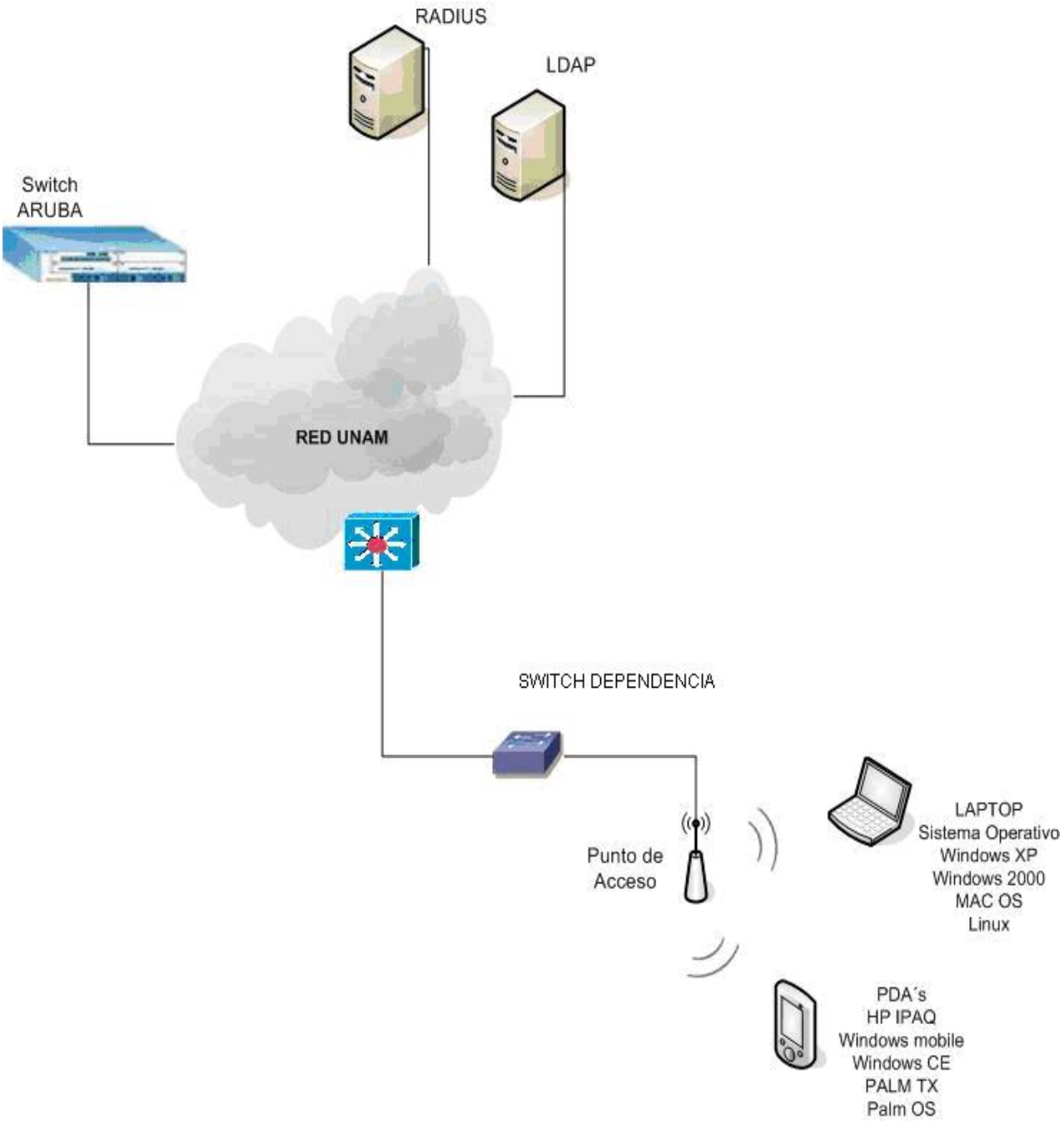


Figura 4.10 Conexión a la RIU.

CONCLUSIONES

Con la implementación de la RIU se cumplió con el objetivo de dar servicio de red inalámbrica de manera gratuita a la comunidad universitaria cubriendo gran parte de los lugares con mayor afluencia de universitarios.

Como resultado del análisis de las tecnologías inalámbricas presentadas por las empresas, se definió implementar Aruba, por ser la tecnología que más se adecuaba a las necesidades del proyecto.

Con el diseño propuesto se consiguió contar con una red lo más segura posible debido a que utiliza el protocolo de seguridad WPA, de esta manera los clientes son autenticados con servidores RADIUS por medio de usuario y contraseña, así mismo, la RIU cuenta con sistemas de monitoreo, uso de políticas de operación y la implementación de redundancia en el backbone, lo que permite mantener el servicio de red disponible el 99.9% del tiempo.

El servicio de red inalámbrica que proporciona RIU ha tenido gran aceptación por parte de la comunidad universitaria ya que los alumnos, académicos e investigadores se han interesado ampliamente en obtener sus cuentas de usuario, en configurar sus equipos portátiles buscando asesoría y soporte ya sea por medio de correo electrónico, vía telefónica o atención personalizada y con ello utilizar el servicio de red inalámbrica.

Hasta la fecha se han registrado aproximadamente 8000 usuarios, de los cuales en un día normal se llegan a conectar 500 simultáneamente. La cantidad aproximada de universitarios que se conectan en un día es de 2500 y no se han registrado aún incidentes de seguridad graves ni de mal uso de ésta.

Con la implementación de este proyecto se logra mantener a la UNAM a la vanguardia de la tecnología, así mismo la comunidad universitaria puede aprovechar mejor los recursos de sus equipos portátiles teniendo movilidad y de esta manera realizar sus actividades académicas de forma más eficiente.

Con la liberación formal del servicio se consiguió dar cobertura a 59 dependencias con más de 270 puntos de acceso y se considera que seguirá creciendo en los próximos años ya que con la infraestructura actual se puede llegar a tener un crecimiento del 40%, tan solo en Ciudad Universitaria y con ello cubrir los lugares sin cobertura o ampliar los que ya tienen.

Así mismo se tomó como base la experiencia del proyecto de la RIU para implementar el servicio de red inalámbrica en las FES Acatlán, Aragón, Cuautitlán, Iztacala y Zaragoza, con lo que la mayoría de las escuelas de estudios superiores de la UNAM contarían con este servicio.

Por otro lado se notó un decremento de redes inalámbricas inseguras debido a que la mayoría de los administradores de red preferían intercambiar sus puntos de acceso por los de la RIU y se espera que éstos sigan decreciendo hasta que sean integrados a ésta en su totalidad.

También se ha incorporado la Escuela Nacional de Enfermería y Obstetricia (ENEO), y algunas dependencias que actualmente no forman parte del proyecto se unirán a éste como lo es la Escuela Nacional de Música (ENM).

APÉNDICE A

En las siguientes figuras se muestra algunos lugares a los cuales se dio cobertura con la RIU ya que se consideraban con zonas en las cuales los universitarios realizan sus actividades académicas como lo son las áreas de estudio, bibliotecas, explanadas, cafeterías, auditorios, etc.

Figura A.1 Jardín Facultad de Medicina.

Figura A.2 Biblioteca Central, planta baja.

Figura A.3 Anexo de Ingeniería, biblioteca Enrique Rivero Borell.

Figura A.4 Auditorio de la Facultad de Veterinaria y Zootecnia.

Figura A.5 Explanada de la Escuela Nacional de Trabajo Social.

Figura A.6 Cafetería del Instituto de Ciencias del Mar y Limnología.

Figura A.7 IIMAS, biblioteca.

Fotos cortesía del Departamento de Diseño DGSCA, UNAM.

GLOSARIO

-A-

Active Directory

Es una implementación de servicios de directorio LDAP hecha por Microsoft para su uso en plataformas Windows.

Administración Centralizada

Proceso de crear, diseñar, mantener y controlar los dispositivos de la red inalámbrica en una sola consola de administración. De esta manera, un punto de acceso fuera de esta consola nunca podrá funcionar.

Administración Distribuida

Administración de los recursos de un dispositivo electrónico de forma que a cada uno de ellos se le gestiona por separado.

Ataque de diccionario

Es un ataque informático que consiste en recorrer con todas (o la mayoría) de las palabras conocidas en un idioma dado, un buen diccionario tiene entre 100

mil y 200 mil palabras. Este ataque intenta averiguar las contraseñas aprovechando la utilización de palabras comunes o previsibles.

Atenuación

La atenuación de una señal es la pérdida de potencia al transitar por cualquier medio de transmisión, se mide en decibeles y en porcentajes, la cantidad de atenuación varía en función de la frecuencia.

-B-

Bluetooth

Tecnología inalámbrica desarrollada por Ericsson en 1994 que hace factible la conectividad inalámbrica entre dispositivos a distancias que no excedan los 10 metros, y alcanzando velocidades del rango de 1Mbps. Trabaja en la frecuencia de 2.4 GHz y puede llegar a formar redes con diversos equipos de comunicación: computadoras móviles, radiolocalizadores, teléfonos celulares, PDAs, e, inclusive, electrodomésticos.

-C-

Captive Portal

Sistema que permite controlar los accesos a redes Wi-Fi, su arquitectura está formada por un gateway que encamina las conexiones, mientras que un Servidor de Autenticación define a qué perfil pertenece cada conexión y qué partes de la red podrá visitar en consecuencia.

CHAP

Challenge Handshake Authentication Protocol. Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, Una vez efectuado el enlace, el servidor envía un mensaje de desafío al solicitante de la conexión, el cual responde con un valor hash que será comparado por el servidor con sus

cálculos del valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario, finaliza.

Conexión PAPI

Conexiones de puntos de acceso a proveedores de información.

-D-

Denegación de Servicio (DoS).

Ataque DoS. Se trata de un ataque diseñado específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas por usuarios autorizados.

DHCP

Dynamic Host Configuration Protoco. Protocolo de Configuración Dinámica de Servidores. Es un protocolo de red estándar que permite que un servidor provea los parámetros de configuración de red (máscara de red, puerta de enlace, etc.) a las computadoras conectadas a la red y también incluye un mecanismo de asignación de direcciones IP.

Dirección IP

Es un número binario de 32 bits que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

DNS

Domain Name Server. Sistema de Nombres de Dominio. Es un sistema de base de datos distribuida que sirve para traducir nombres de computadoras a direcciones IP y viceversa.

-E-

Enlace PPP

El *Protocolo Punto a Punto* (PPP) proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto y permite establecer comunicación a nivel de enlace entre dos computadoras. Generalmente se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. También es utilizado sobre conexiones de banda ancha como PPPoE o PPPoA.

-F-

Faceplates

Caja modular de pared que cubre el conector hembra del RJ45, disponible en varios colores y configuraciones. Utilizado en cableado estructurado.

Firewall

Es un dispositivo ya sea hardware o software que funciona como barrera y controla el tráfico entre las redes, típicamente entre la red de una empresa e Internet, sin embargo, también puede ser una división entre redes de distintas compañías. El *firewall* necesita establecer ciertas reglas que le permita aceptar a los usuarios legítimos y bloquear a los usuarios no autorizados que puedan dañar su información.

Fireware

Puerto de alta velocidad diseñado por Apple, para la conexión de periféricos en una computadora.

Firmware

Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es una combinación de software y hardware. ROMs, PROMs y EPROMs que tienen datos o programas grabados dentro.

-G-

GPS

Sistema de Posicionamiento Global. Sistema de navegación por satélite, tiene cobertura global y continua que ofrece de forma rápida y temporalmente precisa una posición geográfica de un elemento.

-I-

IDP

Intrusión Detection Prevention, Identifican incidentes potenciales tratando de evitarlos. Guardan información relacionada con eventos observados, notifican a los administradores de seguridad de ataques y producen reportes.

IDS

Sistema de Detección de Intrusos (*Intrusion Detection System*) es un programa usado que se basa en el análisis del tráfico de la red, para detectar accesos no autorizados o ataques a un equipo de cómputo o a una red.

El IDS suele tener sensores virtuales con los que detecta anomalías en la red que pueden ser indicio de ataques o alarmas falsas.

IPS

Intrusion Protection System. Ayudar a mantener sistemas de red seguros, identificando y bloqueando tráfico sospechoso.

-L-

LDAP

Lightweight Directory Access Protocol implementa un servicio de directorio especializado para acceder a depósitos de información referente a usuarios, contraseñas y otras entidades en un entorno de red, ofreciendo una amplia capacidad de filtrado sobre la información que esta siendo solicitada.

-M-

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol, Protocolo de autenticación de cifrado de contraseñas por desafío mutuo de Microsoft que proporciona seguridad de alto nivel para las conexiones de acceso remoto.

MS-CHAP V2

Es la versión actualizada de MSCHAP, es un proceso unidireccional con contraseña cifrada y autenticación mutua, la clave de cifrado se basa siempre en la contraseña del usuario y en una cadena de desafío arbitraria.

-N-

NAT

Network Address Translation, Traducción de Dirección de Red. Una dirección IP privada se traduce a un grupo de direcciones públicas. Se utiliza para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

NEMA

Caja que cumple con las especificaciones de la *Nacional Electrical Manufacturers Association* (NEMA) para colocar en este caso puntos de acceso en exteriores, es un material que protege el contenido de los efectos

negativos del medio ambiente y cuenta con una placa de montaje para equipos inalámbricos y cableados.

-P-

PAP

Password Authentication Protocol. Es el método más básico de autenticación, en el cual el nombre de usuario y la contraseña se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión.

Patchcord

Cable de red (UTP, F.O., etc) que se usa en el gabinete de comunicaciones de una red para conectar algún equipo de red con equipos activos o al panel de parcheo dentro del gabinete de comunicaciones. No sobrepasa los 5 metros de longitud.

Patch panel

Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos concentrando un conjunto de cables en un solo dispositivo.

PoE

Power over Ethernet se rige según el estandar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad o puntos de acceso. Es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP/STP en una red Ethernet.

Protocolo GRE

Protocolo de encapsulación genérico. Permite la creación de redes virtuales sobre enlaces IP de protocolos distintos de IP como Novell, AppleTalk, NetBeui o SNA.
Es posible emplear el protocolo GRE para unir redes locales, no define ningún tipo de cifrado de datos, por lo que se debe emplear el estándar IPsec para asegurarlos.

-Q-

QoS

Quality of Service, Calidad de Servicio. Se refiere a la capacidad de la red de proporcionar un mejor servicio a un tráfico de red seleccionado, Una de sus metas es proporcionar prioridad incluyendo ancho de banda dedicado, latencia y mejorar pérdidas de características, así mismo que al dar prioridad a algunos flujos los demás no deben fallar.

-R-

RADIUS

Remote Access Dial-In Use Server. Es un servidor de autenticación y contabilidad de usuarios remotos. Puede ser usado dentro de una red en la que se requiera de un mecanismo de autenticación de usuarios centralizado. Soporta varios esquemas de autenticación como uso de nombre de usuario y contraseña.

Roaming

En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un punto de acceso a otro sin interrumpir el servicio o pérdida de conectividad

Rogue AP

Punto de acceso que se instala en una red sin autorización del administrador y con intensiones maliciosas, su objetivo es capturar información importante, como nombres de usuario y contraseñas que se obtienen en el momento que los clientes se autentican con el falso punto de acceso.

-S-

SNMP

Simple Network Management Protocol, Protocolo de Administración Simple para Redes, facilita el intercambio de la información de administración de los dispositivos de la red.

Gestiona todo lo relacionado a la administración y monitoreo de los dispositivos de redes así como también las funciones de éstos.

SQL

Structured Query Language, Lenguaje de Consulta Estructurado**.** Es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones sobre las mismas

Subneteo

Definido en el estándar RFC 950, en el que se explica el mecanismo para dividir una red en subredes.

El principal objetivo consiste en reducir el tamaño de un dominio de difusión, debido a que las difusiones se envían a todos los hosts de una red o una subred.

-T-

Thawte

Autoridad certificadora que proporciona certificados digitales con cifrado SSL de 128 bits.

-U-

USB

Universal Serial Bus. Bus serial estándar para conectar dispositivos electrónicos con un equipo de cómputo.

-V-

VRRP

*Virtual Routing Redundancy Protocol***.** Es un protocolo que provee la forma de tener uno o más respaldos de routers cuando se configura uno estáticamente dentro de una red de área local (LAN).

BIBLIOGRAFÍA

Hield Gilbert.
Building a wireless office
Auerbach publications, 2003

León-García Alberto e Wiidjaja Indra.
Redes de comunicaciones, conceptos, fundamentos y arquitecturas básicas.
McGraw Hill

Nichols Randall K., Lekkas Panos C.
Wireless Security: Models, Threats and solutions
McGraw Hill telecom, 2002

Flickenger Rob.
Building Wireless Community Networks
ED O'Reilly, Enero 2002

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

REVISTAS

"Seguridad en redes inalámbricas". Revista: e.Security latin American security. Articulista: Cecilia Villarubia, Editorial Mexicana de Impresos México D.F. Páginas 40-43, No. Volumen 5 Agosto-Septiembre 2006.

"Seguridad en redes inalámbricas 802.11". Revista: Sistemas y Telemática. Articulista: Juan Manuel Madrid Molina. Editorial Universidad Icesi, Colombia. Páginas 13-28. Fecha de aceptacion 20-04-2004

MESOGRAFÍA

Aruba Networks
www.arubanetworks.com/
Consultado en Mayo del 2005

Speakeasy speed test
www.speakeasy.net/
Consultado en Agosto del 2005

Test de Velocidad alojado en adsl4ever.com
www.adsl4ever.com/test/11
Consultado en Agosto del 2005

Modulación por división ortogonal de frecuencia
es.wikipedia.org/wiki/Modulaci%C3%B3n_por_divisi%C3%B3n_ortogonal_de_frecuencia
Consultado en Mayo del 2006

Frequency Hopping Spread Spectrum
www.redlibre.net/modules.php?name=Encyclopedia&op=content&tid=149
Consultado en Mayo del 2006

Wi-Fi Protected Access Data Encryption and Integrity.
www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx
Consultado en Junio del 2006

Seguridad Wi-Fi: WEP, WPA y WPA2
www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
Consultado en Junio del 2006

Wi-Fi
www.wi-fi.org
Consultado en Junio del 2006

Seguridad en LAN inalámbricas con PEAP y contraseñas.
www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.mspx
Consultado en Julio del 2006