UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"Administración y Seguridad de una red wireless. Caso: Servicio para alumnos de la Facultad de Ingeniería"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

Ingeniero en Computación

P R E S E N T A

VERÓNICA MONROY ORTÍZ

DIRECTOR DE TESIS:

ING. NOÉ CRUZ MARÍN

2007

Dedicado a Migue, por todas las alegrías y
lecciones de vida que sin saber me ha dado

AGRADECIMIENTOS

Agradezco a Dios y a la Virgen por ayudarme en mi vida y darme todo lo necesario para estudiar y progresar.

A mi Mamy por todo el amor que me da, el esfuerzo que hizo conmigo día a día y el gran ejemplo para luchar y alcanzar todos mis sueños.

A mi Papá por el apoyo, ejemplo y cariño brindado siempre.

A Mis Abues (Nina y Rey) por ser tan lindos, quererme y cuidar siempre de mí.
A Bren y a Migue por todas las satisfacciones, apoyo y experiencias que compartieron conmigo.
A mis tíos Laura, Rocío y Dany por el animo, atenciones y cariño que me han dado desde niña.
A Eugenia Padilla (Mi Manis), por incluirme en su vida, por su amistad, lecciones, cariño y todo lo que compartimos durante tanto tiempo.

A las personas que hacen mi vida agradable y divertida, que me impulsan, acompañan y apoyan, mis amigos: X-tian Pineda (Mi hermanito), Alberto 83, Sergio Cuellar, Marian Aburto, Yezmin Flores, JuanCarlos Cedeño y Dana García.

A la UNAM, en especial a la Facultad de Ingeniería, por contar con todo lo necesario para mi formación. A mis maestros por enseñarme y compartir conmigo parte de su experiencia y conocimiento. Principalmente: al Ing. Noe Cruz Marín por todo el cariño, apoyo y amistad que me ha brindado. A la Ing. Jaquelina López por todas las enseñanzas y ejemplos, no solo profesionalmente, sino también en el aspecto personal. A Marco Vigueras por el modelo de profesionista que me enseñó y quiero seguir. A la Ing. Rosario Barragán, por sus atenciones y consejos.
A UNICA, y toda la gente ***especial*** que me ayudó ahí, por darme la oportunidad de dar mis primeros pasos en Administración y Seguridad y ser parte fundamental de esta tesis.

A Rafa Sandoval, por contagiarme de sus ganas para realizar las cosas y enseñarme el camino para llevarlas a cabo.

Al Ing. Francisco Miguel Pérez por todo el apoyo, oportunidades y compresión que me ha brindado durante el tiempo que he trabajado a su lado.

A todas las personas que por falta de memoria no incluyo, pero no dejan de ser importantes en mi vida.

Índice General

INTRODUCCIÓN

La palabra inalámbrico, evoca aquella emocionante época en que la radio dominaba el mundo del entretenimiento y las familias se reunían alrededor de un aparato de radio del tamaño de una mesa y se maravillaban ante una tecnología que emitía voces incorpóreas desde la lejanía. En el presente, un tipo de radio diferente está poniendo el mundo de la informática totalmente desconcertado. Ahora los radios son minúsculos chips encapsulados en dispositivos del tamaño de una tarjeta de crédito que se conectan en equipos que a su vez no son mucho más grandes que un cuaderno. Estos radios no transmiten ni reciben ásperas voces y efectos de sonido, sino pequeños paquetes de ceros y unos: datos informáticos. En el pasado, la radio conectó a la gente e hizo posible la primera cultura masiva; en la actualidad, la radio conecta las computadoras con redes inalámbricas y la inmensa red que es Internet.

El atractivo de las redes inalámbricas está en la combinación de flexibilidad, ubicuidad de la red y distancia entre nodos de red que hace que las redes inalámbricas superen al cableado. Conectando algunas piezas de equipo adecuado y activando una conexión podemos deambular por nuestra casa u oficina, salir al patio o tomar un café manteniendo el acceso a la red todo el tiempo. De repente estamos utilizando las redes de una forma que hace una década parecía ciencia ficción.

Comúnmente se escucha: ¿Quién puede imaginar la vida sin los servicios y facilidades que proporciona una computadora?, la computadora es un gran avance tecnológico y facilita muchas tareas, sin embargo, la comodidad no solo radica en la realización de dichas tareas, sino también en los servicios que se pueden adquirir estando la computadora en red. Es decir, servicios como intercambio de archivos, contacto con otras personas en tiempo real, hacer uso de los recursos compartidos; como pueden ser impresoras y el uso de algún software, el intercambio de datos a través del correo electrónico, las posibles transacciones que se realizan con los bancos y otros sitios de comercio electrónico, la consulta y hasta investigación de información en libros electrónicos, por mencionar algunos de los muchos servicios que se tienen al acceder a la superred. A medida que se van presentando las actualizaciones de tecnología, aparecen nuevas opciones para que el acceso a estos servicios para usuarios finales sea sencillo. Hoy en día la etapa de la evolución de tecnología ofrece un servicio sin cables, sin necesidad de tener al usuario en un lugar fijo, solo dentro de cierto perímetro, con gran flexibilidad para la expansión de usuarios, y muchas ventajas más, este tipo de tecnología es conocida como WIRELESS.

Hablando de una red wireless, se puede pensar que las ventajas aumentan considerablemente, por que se trata de equipos con acceso a Internet y con la ventaja de la movilidad. Lamentablemente, en realidad no es tan maravilloso, ya que no se cuenta con alto porcentaje de seguridad, si bien, para algunos ámbitos como los de un restaurante o algunos lugares públicos, la instalación de una red wireless, solo significa dar un servicio extra para sus clientes, pero este aspecto (el de la seguridad), no es tan cuidado. Sin embargo, si se trata de la implementación de una red wireless, de una empresa o una institución, es de suma importancia poder garantizar un alto nivel de seguridad, ya que se debe proteger ante todo la información que viaja por ella y la reputación de la institución.

En este trabajo de tesis el principal objetivo es proponer la implementación de la red Wireless en la Facultad de Ingeniería, que garantice una buena administración y nivel de seguridad adecuado, de manera que para las personas indicadas las tareas sean llevadas a cabo de manera sencilla y rápida y que los usuarios cuenten con un servicio de calidad.

Así en el capítulo uno, se hace un repaso de los conceptos básicos de redes convencionales. Principalmente los que son la base para el intercambio de datos, y muchos conceptos que se usan para ellas, también son usados para redes wireless. No solo se citan conceptos de redes convencionales sino de redes en general, es decir, términos como IP, MAC address, Duplex, velocidades, entre otros que serán usados en capítulos posteriores. Así mismo, se mencionan los primeros conceptos y definiciones de redes wireless, se citan los estándares, las frecuencias, los canales, algunas comparativas entre ellos, y también los conceptos más usados y mencionados en el uso de la tecnología. Se comienza a hacer la división que seguirá en toda la tesis, que es Administración y Seguridad.

Para el segundo capítulo, aborda el diseño de redes wireless, en general, se presentan los componentes tanto físicos como lógicos de una red. Se define la utilidad y las características de los componentes que se usarán en el desarrollo de la red. Se mencionan características de las antenas, los tipos más comunes y su área de cobertura según sus características, para así definir el comportamiento de la señal que emite la antena. Se explica la forma de trabajo de las redes, el protocolo y modelo de referencia 802.11, es necesario entender bien el estándar y la forma de trabajo de las tarjetas y el medio, el comportamiento del tráfico en la red y la transferencia de paquetes a través de ésta. Se hace una referencia a los tipos de topologías que existen en este ámbito, para clasificar la red que se propone y tener claros los demás tipos que se pueden configurar para el caso de Facultad. Finalmente, se

hace mención de algunos protocolos de seguridad y aspectos de administración.

En el tercer capítulo se hace mención de las diferentes técnicas de administración y seguridad. Es aquí, donde se marca la división entre los métodos de administración y seguridad. En cuanto a administración, se mencionan las diferentes soluciones que se pueden encontrar, así como los problemas que pueden surgir. Así mismo se mencionan los elementos que desde el punto de vista de este trabajo se puede dividir la administración y algunas de las soluciones que se han lanzado al mercado, o que se pueden implementar con los mismos sistemas operativos o que se pueden implementar en los mismos dispositivos de red. De igual forma se mencionan, las tareas en las que se puede dividir la implementación de la seguridad, sin embargo, se debe mencionar, que esta es una tarea que no se pueden encasillar en ciertas acciones, ya que como encargados de la seguridad, se debe actualizar, y afinar constantemente el esquema de seguridad, ya que no puede ser una tarea estática y llevada a cabo de igual forma por mucho tiempo. También se mencionan, algunos ataques que se presentan comúnmente, y se detallan los algoritmos y métodos más usados para el cifrado del tráfico en la red.

En el cuarto capítulo, se analiza específicamente el caso de la Facultad de Ingeniería. Es donde se analiza la problemática que se tiene para la implementación de la red Wireless. Se hace una división, entre los problemas que se tienen a nivel usuarios, a nivel de administración y a nivel de seguridad. Para cada aspecto se hace una descripción de cada problema que se presenta para prestar el servicio de red. Se hace la división de esta forma, ya que, son los aspectos que son más importantes, para lograr un servicio con calidad. Se considera un alto nivel de administración, el hecho de tener un buen monitoreo, distribución del ancho de banda, conocer perfectamente los servicios que se están prestando, las limitaciones y alcance de la red. También poder garantizar un alto nivel de seguridad, fundamentalmente los tres aspectos básicos: confiabilidad, integridad y disponibilidad. Se analiza también el contacto continuo con los usuarios, ya que hay que recordar que el mejor monitor de los servicios que se están prestando son los usuarios. Es aquí donde se plantea la posibilidad de hacer partícipes a los usuarios para que contribuyan con ciertas acciones de la seguridad y buen manejo de la red.

En el quinto capítulo, se presenta una solución específica al caso práctico y se da solución a los problemas que se analizaron en el capítulo cuatro. Aquí donde se propone la solución particular, los mecanismos y dispositivos que se usarán, según el análisis de la relación necesidades / recursos. Es decir, después del análisis de los problemas que se presentan para implementar la red de la Facultad de Ingeniería,

y analizar algunas las soluciones que existen en el mercado, se eligen las herramientas y combinación de estrategias de seguridad para lograr el objetivo: Una red wireless para la Facultad, que de servicio exclusivo para los alumnos del edificio principal, de manera eficaz, eficiente y segura.

En el sexto capítulo, se hacen algunas recomendaciones extras, para el mantenimiento de la red, las actualizaciones de los mecanismos implementados y el mantenimiento de los dispositivos utilizados para la puesta en marcha de dicha red. Se dan recomendaciones de las buenas prácticas de seguridad, lo que como administradores de red, se tiene que seguir o no se puede ignorar, y por la tendencia que se sigue en todo el trabajo, se mencionan algunas las recomendaciones que se tienen que hacer llegar a los usuarios de la red, para mantener el nivel de seguridad y dar a conocer las políticas de uso de la red y de la Facultad sobre el uso, derechos y obligaciones que tienen los usuarios y las sanciones a las que se harán acreedores los usuarios que violen dichas políticas.

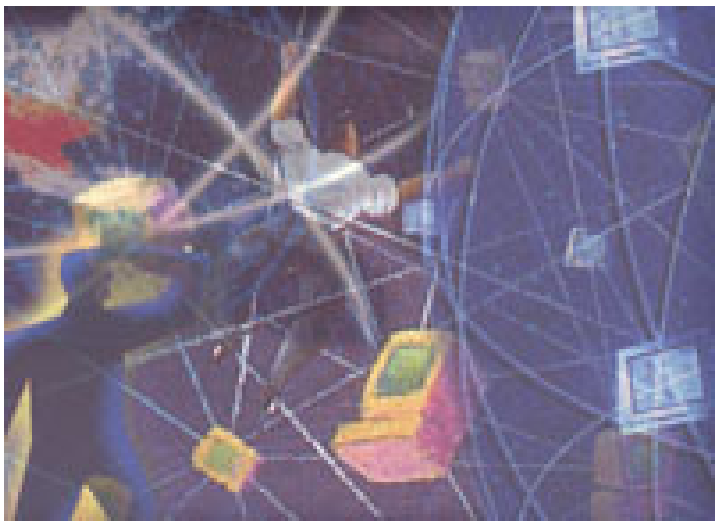
Finalmente vienen las conclusiones, que es donde se hace el análisis de los resultados que se proponen, además de mencionar aclaraciones del ¿Por qué?, de las soluciones propuestas y otras sugerencias que en el desarrollo del trabajo no se mencionan, como pueden ser las distribuciones en las que se recomienda el desarrollo de los dispositivos y herramientas que se usarán como parte de la solución. Además se mencionan las experiencias y lecciones que deja la investigación para el desarrollo de este trabajo.

Se debe mencionar que este trabajo se desarrolla en base al modelo OCTAVE (Operationally Critical Treta, Asset Vulnerability Evaluation), es un modelo desarrollado por el CERT/CC, y está establecido en el análisis de riesgos. Prácticamente en la estrategia de participación universal, es decir, la seguridad de la red, es responsabilidad de todos, no únicamente de las personas del departamento de Administración de redes y Seguridad.

Se divide en tres etapas:

1. Elaboración de perfiles activos / amenazas (Capítulo 3).
2. Identificación de vulnerabilidades en infraestructura (Capítulo 4).
3. Desarrollo de estrategias y planes (Capítulo 5).

CAPÍTULO 1



CONCEPTOS BÁSICOS

Para entender el funcionamiento de una red de datos, se deben conocer ciertos conceptos básicos que son generales para cualquier tipo de red. Términos y características que son obligatorias conocer, manejar y distinguir al hablar de redes. Considerando su importancia, este capítulo está dedicado a la definición de esos conceptos.

1.1 Redes de Computadoras

Red de datos
Conjunto de elementos que están conectados entre sí, para cumplir con un fin común.

Red de computadoras
Conjunto de terminales, nodos, servidores y elementos de propósito especial que interaccionan entre sí con la finalidad de compartir información y compartir recursos. Es un **sistema distribuido** donde la existencia de múltiples computadoras autónomas es transparente para el usuario, el cual puede teclear una orden para ejecutar un programa o tarea y ésta se ejecutará. La selección del mejor procesador y colocar los resultados en el lugar más apropiado es propia del Sistema Operativo y a la red en sí. Sin embargo el usuario no está conciente de que existen múltiples procesadores.
Existen redes que trabajan bajo la arquitectura **cliente-servidor** donde existe la posibilidad de utilizar diferentes servidores, que como su nombre lo indica proveen servicios a un conjunto de nodos denominados clientes, por lo que se considera que no existe limitante en cuanto al almacenamiento de la información, ya que se pueden ir instalando nuevos servidores, con la finalidad de expandir la red.
Algunas de las razones por las que considera trabajar bajo un concepto de red, es:

- Integridad, que se refiere a hacer de un sistema de varios elementos una sola herramienta, donde se usen de la mejor manera posible y se aprovechen al máximo.
- Y la rapidez y facilidad con la que se pueden compartir e intercambiar datos y recursos en cualquier momento.

Uno de los requerimientos básicos para establecer una red, es lograr una buena **conexión**.

Existen dos tipos de conexiones básicas:

- Punto a punto (peer to peer), cada elemento es conectado a otro por medio de un enlace físico (link).

- Multipunto (multipoint), todos los elementos estas conectados a un solo enlace físico.

Dirección IP
Por el hecho de que el intercambio de datos se da entre múltiples nodos, los nodos intermedios deben ser capaces de determinar el camino a seguir para llegar al nodo destino. Por lo que si se le asigna una dirección que ayude a la identificación de cada nodo. En Internet, se trabaja bajo el protocolo IP (Internet Protocol), cada nodo tiene una dirección denominada dirección IP.

Nodo
Término que se usa para referirse a cualquier dispositivo que forma parte de una red. Es decir: computadoras, de propósito general y propósito especial, switches, routers, bridges, etc.

Bandwidth
Velocidad de transmisión de bits por unidad de tiempo (por lo general por segundo).

Latency (Delay)
Tiempo que tarda un bit en propagarse de un nodo A a otro B.

Round Trip Time (RTT)
Tiempo que tarda un bit en ir de un nodo A a otro B y regresar. Es decir, RTT= 2 x Latency.

La diferencia que se establece para basarnos entre cual de los dos parámetros: Latency y Bandwidth, es el tamaño de la información que se envia, es decir, si la información transmitida es muy pequeña, el latency es quien define el tiempo de transmisión. Cuando la cantidad de información es grande, el Bandwidth, es el que define ese tiempo.

Comunicación Simplex
Comunicación entre dos puntos (nodos) en un solo sentido.

Comunicación Half Duplex
Comunicación entre dos puntos (nodos) en un solo sentido a la vez.

Comunicación Full Duplex
Comunicación entre dos puntos (nodos) en dos sentidos a la vez.

Modos de Transferencia

Difusión (Broadcast)

Comunicación a un conjunto de nodos. En este tipo de comunicación, se pude hacer una analogía a la televisión abierta, es decir, hay un equipo que da señal de estar vivo y a las máquinas que les interesan toman en cuenta dicha señal.

Conmutación (multicast)

Transmisión de información de un nodo a otro en específico. Aquí la analogía es con la televisión de paga, la "señal de vida", solo es emitida al que pide que se le informe, y cumple con determinados requisitos para que se le de la señal.

Modelos de Interconexión

Conetion oriented

Primero se establece un "camino", una conexión lógica y después se envían los datos, siguiendo la ruta ya establecida. Un ejemplo de esta conexión es el protocolo TCP (Transfer Control Protocol).

Conection less

La información se envía por paquetes, y cada uno puede seguir una ruta diferente, lo cual implica el desordenamiento de paquetes a la llegada. Un ejemplo de está conexión es el protocolo UDP (Unit Datagram Protocol).

Los conceptos presentados anteriormente, son básicos para las redes convencionales, y el motivo de citarlas en éste trabajo es por que son términos que serán usados a lo largo de este desarrollo.

1.2 Redes Wireless

Red Wireless

Estándar desarrollado por la **IEEE** (Institute of Electrical and Electronic Engineers) que permite conectar dispositivos mediante una frecuencia de 2,4 Ghz a 5 Ghz, con controladores que permiten comunicarse a través de los protocolos actuales de comunicación (TCP / IP), disponiendo cada dispositivo de una dirección única a nivel de Hardware (MAC address), y con una potencia de transmisión que va desde los 10-20 mW a los 100 mW (según la FCC / CEPT o la legislación de cada país).

IEEE (Institute of Electrical and Electronic Engineers), es la entidad encargada de crear estándares para casi todos los dispositivos

electrónicos. Para diferenciar las diferentes familias de estándares y los comités que se encargan de su certificación, utilizan valores numéricos, y es por esto que desde hace mucho tiempo se utiliza para los estándares de redes informáticas el valor numérico 802. Tras ese valor se van agrupando los diferentes estándares creados, por ejemplo para redes Ethernet es 802.3. Para redes wireless se determinó que fuese el 802.11 para las redes inalámbricas. En el caso del 802.11 se fueron creando subgrupos, que se han ido identificando mediante letras. Aunque existe un salto en las letras no queda espacio libre, existen muchísimas especificaciones que no ven la luz o simplemente son de transición. Es por eso que se comenzó a hablar de la 802.11b, siendo su fecha de aprobación en 1999. Y ésta fue la que la mayoría de los fabricantes aceptaron como la más estándar y la más completa. Al aceptarla los fabricantes se agruparon en otra asociación que simplemente certifica que los productos son compatibles entre sí dentro de la norma 802.11. Este grupo se denominó Wi-Fi (WirelessFidelity).

En la tabla 1.1, se explican resumidamente tres protocolos que actualmente se comercializan dentro del estándar 802.11. Estos son el 802.11b, 802.11a y 802.11g en orden de aprobación por el IEEE.

Estándar	802.11b	8.02.11a	802.11g
Aprobado IEEE	Julio 1999	Julio 1999	Junio 2003
Popularidad	Adoptado Masivamente	Nueva tecnología crecimiento bajo	Nueva tecnología con un rápido crecimiento
Velocidad	Hasta 8 Mbps	Hasta 54 Mbps	Hasta54 Mbps
Costo	Barato	Relativamente caro	Relativamente barato
Frecuencia	2.4 – 2.497 GHz	5.15 – 5.35 GHz 5.425–5.675GHz 5.725-5.875GHz	2.4– 2.497 GHz
Cobertura	Buena, cobertura de 300-400 a metros con buena conectividad con determinados obstáculos	Cobertura baja, unos 150 m, con mala conectividad con obstáculos	Buena cobertura, unos 300 -400 m con buena conectividad con determinados obstáculos
Acceso Público	El número de Hotspots crece exponencialmente	Ninguno en éste momento	Compatible con los Hotspots actuales de 802.11b. El paso a 8.02.11g no es dificil para los usuarios
Compatibilidad	Compatible con 802.11g, no es compatible con 802.11a	Incompatible con 802.11b, 8.02.11g	Compatible con 802.11b. No es compatible con 8.02.11a
Modos de Datos	1,2,5,5,11 Mbps	6, 9, 12, 24, 36, 48, 54 Mbps	1,2,5,5,11 Mbps
Modulación	CCK	OFDM	OFDM y CCK

Tabla 1.1 Estándares Wireless

En la imagen 1.1, se observa la relación entre la distancia (medida en pies, un pie = 0.3048 metros) y el ancho de banda que podemos usar en cada caso. Por supuesto las distancias pueden variar dependiendo de la potencia y los dBm irradiados por la antena de cada fabricante.

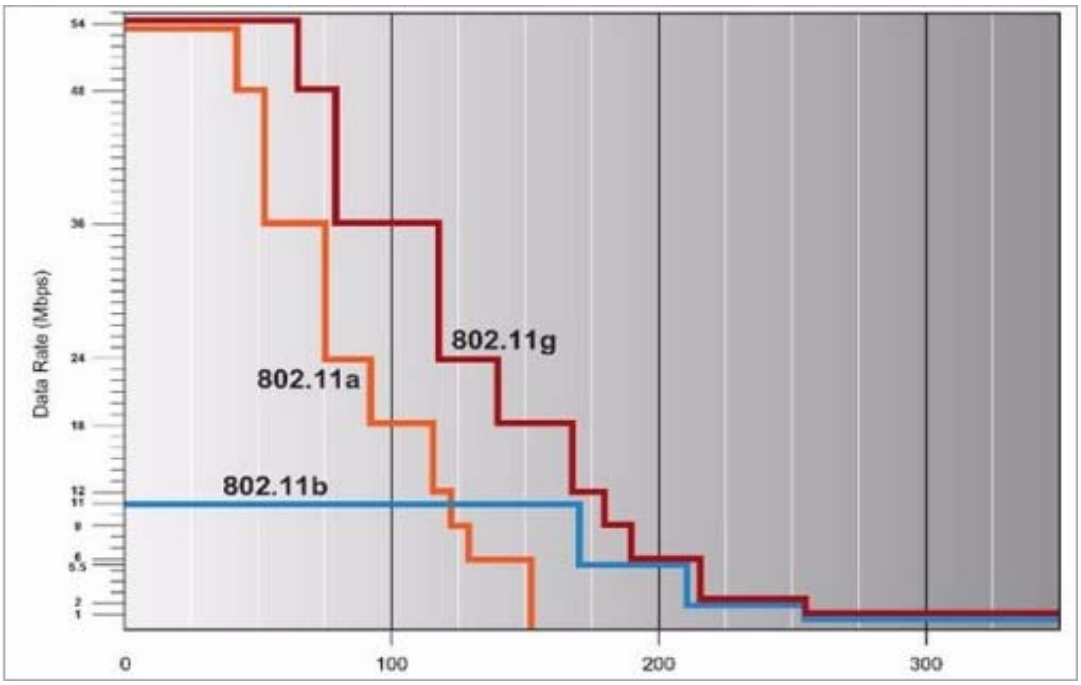


Imagen 1.1. Gráfica Distancia vs Ancho de banda de los estándares.

Como podemos observar la frecuencia más usada es la de 2.4Ghz. Dicha frecuencia es libre en prácticamente todos los países del mundo, ya que se trata de una frecuencia reservada para la investigación, educación o sanidad. Sin embargo en muchos países determinadas frecuencias dentro de los 2.4 Ghz están reservadas por el ejército o los gobiernos. En la tabla siguiente se observa la relación entre los canales y la frecuencia.

Canal	Frecuencia	Canal	Frecuencia
1	2.412 GHz	8	2.447 GHz
2	2.417 GHz	9	2.452 GHz
3	2.422 GHz	10	2.457 GHz
4	2.427 GHz	11	2.462 GHz
5	2.432 GHz	12	2.467 GHz
6	2.437 GHz	13	2.472 GHz
7	2.442 GHz	14	2.484 GHz

Tabla 1.2 Relación entre canal y frecuencia

De estos canales mencionados, generalmente los canales 5, 7 y 11 no son usados por ningún estándar.
En General el término Wireless es usado para cualquier tipo de comunicación sin alambres, sin embargo cualquiera de las siguientes palabras son usadas como sinónimo de wireless:

- PCS (Personal Communication Systems), es un estándar de comunicación celular.
- 802.11b, es uno de los estándares más conocidos, cuando menos, el que tuvo mayor aceptación y uso.
- Wi-Fi, asociación, certificadora para productos de la norma 802.11.
- Homero.
- Bluetooth, estándar de redes wireless opera en redes a pequeña escala como LAN, en general es referido a redes de Área personal (PAN, Personal).

Como se observa, todos estos términos son referidos a diferentes tecnologías.

Muchas son las cuestiones que se han dado, respecto a si conviene o no hacer un cambio de toda una estructurada red convencional a una inalámbrica, estas son algunas de las razones por las que se eligen dispositivos WLAN:

- Incrementa la productividad y debido al incremento de la movilidad.
- Infraestructura a bajo costo comparada con las redes alambradas.
- Rápido desarrollo de esquemas.
- No hay cableado, y si lo hay es mínimo o muy discreto.

SSID (Service Set Identification): ESSID (Extended Service Set Identification). Este identificador suele emplearse en las redes Wireless creadas con Infraestructura. Se trata de un conjunto de Servicios que agrupan todas las conexiones de los clientes en un sólo canal. Suele denominar de manera familiar el nombre de la red Wireless que da servicio un Punto de Acceso.

BSSID (Basic Service Set Identification)
Suele identificar una red creada a través del Punto a Punto.

Infraestructura
Opción de las redes Wireless que sólo puede ser activada por Access Point, y utilizada por tarjetas Wireless. Permite el enlace con más puntos

de acceso y la agrupación de clientes. Admite el Roaming entre Access Point.

Punto a Punto (Ad-hoc)

Opción que conecta dispositivos dotados de Wireless entre sí, sin necesidad de un Access Point. Podemos interconectar varios de dichos dispositivos entre sí, no sólo dos, tal y como ocurre en las redes Ethernet con cables cruzados (esta sería la similitud más cercana).

Canal
Un canal es una frecuencia de uso único y exclusivo dentro de su cobertura, por los mismos clientes.

dBi
Decibelios por encima (o por debajo) de la señal ideal de una antena.

Mw (Miliwatio)
Un milésimo de watt, es la base para medir los niveles de intensidad de la señal en los circuitos de telecomunicaciones.

1.3 Administración

Auditoria
Revisión cuyo único fin es detectar errores, fraudes, señalar fallas, se define claramente como **"es una actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas."**

"Se entiende por Auditoria Informática una serie de exámenes periódicos o esporádicos de un sistema informático. Tiene como objetivos evaluar los controles de la función informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente. El auditor informático debe velar por la correcta utilización de los recursos que la empresa dispone para lograr un eficiente y eficaz Sistema de Información.

Administrador
Es la persona o software, que ayudan a tener control sobre varios aspectos del sistema operativo. De ésta manera podemos referirnos al administrador de aplicaciones, archivos e incluso impresoras. En otras

palabras, un administrador es el responsable de facilitar el control de un entorno.

1.4 Seguridad

Seguridad informática

Es el conjunto de procedimientos y acciones durante la planeación, desarrollo, pruebas y tiempo de vida de un sistema, para garantizar que dicho sistema, está funcionando tal como fue planeado, exactamente para lo que fue desarrollado.

Habitualmente, al querer implantar la seguridad, se piensa que solo es abordar la seguridad como respuesta a un problema o situación específica, sin estudiar todos los elementos que puedan estar relacionados. Si se habla de una plataforma Web abierta a Internet, la seguridad no es responder si instalamos tal o cual firewall, es bastante más que eso: sistemas de alimentación ininterrumpida para máquinas críticas, duplicidad de almacenamiento, control físico, auditoria de conexiones internas y externas, blindaje de archivos de sistema, control de modificación de archivos, monitorización de tráfico de red, planes de contingencia y mucho más.

Un concepto global de seguridad informática sería aquel definido como el conjunto de procedimientos y acciones encaminados a conseguir la garantía de funcionamiento del sistema de información, obteniendo el cumplimiento de la finalidad para el que estaba establecido, manteniendo la integridad, entendida como la integridad del sistema por gente externa al mismo, y alertando la detección de actividad ajena, entendida como el control de la interacción de elementos externos al propio sistema. Si logramos esta tarea tan difícil podemos decir que disponemos de un sistema seguro, sin embargo nunca al 100%.

Conociendo al agresor

La potencial agresión sobre el sistema puede venir derivada de intervenciones de dos tipos.

Las intervenciones no maliciosas, ya sean por manipulaciones humanas o no, son imprevisibles y de resultado incierto. Las más habituales se refieren a cortes de corriente o alteraciones importantes en los niveles de voltaje en la alimentación eléctrica que pueden provocar daños irrecuperables en determinado hardware.

Las intervenciones maliciosas van ligadas a la manipulación humana. Las más peligrosas potencialmente, por el alcance del daño que se puede provocar y por la mayor dificultad en su detección, son las internas al propio sistema de información. El agresor lo enmarcaríamos dentro de los administradores del sistema, programadores o usuarios privilegiados, también incluiríamos a aquel que no teniendo acceso lógico al sistema sí lo tuviese físico a elementos críticos del mismo. Las grandes quiebras de seguridad han provenido siempre del interior de las estructuras atacadas y la mayor parte de las veces se han silenciado en un primer momento para no provocar reacciones incontroladas. La mayor peligrosidad de este tipo de actuaciones viene derivada del mayor conocimiento que el agresor dispone del medio sobre el que actúa. El otro tipo de intervención maliciosa es la de origen externo y que se produce casi siempre a través de línea de comunicaciones, como ejemplo más claro y actual podemos contemplar las intrusiones a través de Internet.

Procedimiento

Mediante la combinación de dos líneas de actuación muy claras.

En primer lugar, con el establecimiento de una política de seguridad que alcance a todo el sistema. Debe plasmarse en un documento escrito donde se contemple la asignación de responsabilidades y refrendado al más alto nivel de dirección posible, lo que implicará a toda la estructura en su cumplimiento. Se debe hacer un control riguroso de aplicación del mismo, pero también de su difusión para tener la certeza de que todos los afectados conocen su contenido. Para su implantación es necesaria una adecuada generación de medios humanos y materiales específicos. Y algo importantísimo, es fundamental la concienciar al personal afectado por las medidas a adoptar.

En segundo lugar, con la generación de auditorias periódicas internas y externas. Las internas provienen de la propia estructura de seguridad del sistema, mientras que las externas las realizarían personal de una empresa o contratados a tal efecto y no siempre los mismos. El objeto de las últimas es la revisión del sistema por parte de elementos que no se encuentren "viciados" por la rutina o el conocimiento del funcionamiento del sistema, extremo que se da con el personal propio.

Temporalidad

Los criterios implantados por la política de seguridad deben seguirse siempre, desde que el sistema es simple o sencillo hasta cuando su crecimiento lo transforma en uno complejo.

El mejor procedimiento es la escalabilidad, permitiendo de esta manera validar las políticas llevadas hasta el momento, afinando y optimizando las futuras.

Responsabilidades

De una manera genérica, la responsabilidad de implantación de la política de seguridad afecta a todos los usuarios del sistema de información, tanto los normales como los privilegiados, donde habría que englobar a administradores de sistemas, administradores de bases de datos y responsables de comunicaciones.

De manera específica, debe existir un responsable de seguridad, con dedicación exclusiva caso de tratarse de sistemas de información importantes. Para poder ejercer su labor debe contar con un equipo de seguridad que permita desarrollar la política determinada por escrito. Es positivo establecer un equipo de supervisión compuesto por los usuarios privilegiados señalados anteriormente y el equipo de seguridad.

Virus informático

El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de discos o de la red comunicación entre computadoras causando diversos tipos de daños a los sistemas.

También se define como: código ejecutable añadido a un programa legitimo con la intención de propagarlo a otros usuarios o sistemas. Puede eliminar o modificar información completa

Amenaza

Es la posibilidad de que ocurra un evento que pueda llevar al hecho de alterar el comportamiento de nuestro sistema, o peor aún, puede llevar a la suspensión total o parcial de los servicios que brinda nuestro sistema.

Ataque

Es el acto de llevar a cabo una amenaza, es decir, es hacer uso de herramientas y programas específicos que sean capaces de explotar vulnerabilidades existentes en nuestro sistema.

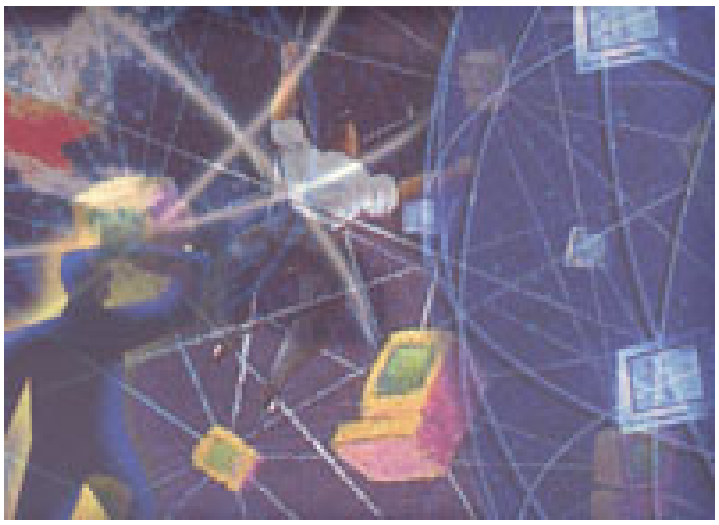
Política

Son normas que definen medidas para el comportamiento y forma de uso de los miembros de una organización respecto a los recursos de un sistema.

Prohibitiva: ***"Todo lo que no está explícitamente permitido está prohibido"***

Permisiva: ***"Todo lo que no está explícitamente prohibido está permitido"***

CAPÍTULO 2



DISEÑO DE REDES WIRELESS

2.1 Componentes básicos de una red Wireless

Se puede hablar de componentes lógicos y físicos de una red inalámbrica.

Físicamente, se tiene:

Access Point /Punto de Acceso (AP/PA)

Se trata de un dispositivo que ejerce básicamente funciones de Puente entre una red Ethernet cableada con una red Wireless sin cables. Su configuración permite interconectar en muchos casos varios Puntos de Acceso para cubrir una zona amplia, pudiendo por si sólo proporcionar la configuración TCP / IP mediante un servicio DHCP. Se suele configurar en un único canal y admite un nivel de cifrado, pudiendo enlazar un gran número de equipos entre ellos.

El AP actúa a modo de HUB una red convencional. Por el AP pasa toda la información de la red wireless como he dicho antes tiene la misma misión que un hub en una LAN cableada. El AP puede actuar tanto como bridge en este modo la red cableada es totalmente transparente con la wireless es como si físicamente fuera la misma red o como router con el cual se suelen hacer varias subredes para wireless, hay diferentes modelos de él , hay que son solo bridge o que son solo router o incluso que pueden hacer la función de Router y Bridge, para una pequeña red domestica en la que no hay que preocuparse mucho por la seguridad la mejor opción es un Bridge, mientras que el Router es mas indicado para instalaciones más grandes y con más riesgo en los datos.

Los AP son dispositivos fijos de la red. Por tanto:

- Sus antenas pueden situarse en lugares estratégicos, y pueden ser de alta ganancia.
- Se pueden dotar de antenas diversidad (para evitar los problemas de multitrayectoria)
- Tienen requerimientos de bajo consumo (no usan baterías)

Antenas

En los orígenes de la radio, las antenas se construían de forma empírica sin ninguna base científica. Un conductor de cualquier longitud funcionaba como antena, siempre que permitiera realizar el contacto. Además, las longitudes de onda eran enormes (se trabajaba casi siempre en onda larga o extralarga), resultaba muy complejo construir

antenas cuya longitud alcanzara algunas décimas de longitud de onda (se debe recordar que a 1 MHz, que actualmente es frecuencia de onda media, la longitud de onda es de 300 metros y esta frecuencia ya era muy elevada en los primeros tiempos).

A medida que se fue aumentando la frecuencia (y por tanto disminuyendo la longitud de onda), la longitud de las antenas prácticas empezó a ser una fracción importante de la longitud de onda. Gracias a las experiencias de los Radioaficionados en las longitudes de onda de 200 metros y menores, se pudo comprobar que algunas longitudes de hilo resultaban mucho más eficaces que otras, y que el hecho de aumentar a longitud del hilo no producía ningún beneficio si este aumento no se hacía de forma lógica. Veamos cuál es el principio de funcionamiento de una antena.

Principio del funcionamiento de las antenas

Para que una antena genere un campo electromagnético, se necesita que existan cargas eléctricas en movimiento. En el caso de los conductores paralelos, estas cargas son electrones que se mueven merced al impulso eléctrico de un generador (transmisor). Según las leyes de Maxweil toda carga eléctrica en movimiento acelerado, genera un campo eléctrico y otro magnético (campo electromagnético), que una vez creado se aleja indefinidamente del conductor.

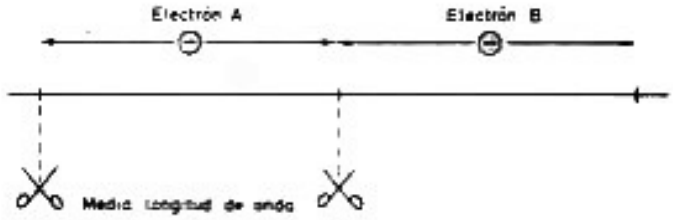


Imagen 2.1 Movimiento de electrones en un cable

Si a un hilo conductor se le aplica corriente alterna, todos los electrones libres se moverán siguiendo el ciclo de corriente alterna. A efectos prácticos es lo mismo considerar que los electrones se transmiten el movimiento de unos a otros, como considerar que un solo electrón realiza todo el trabajo.

Este electrón se mueve adelante y atrás siguiendo el ciclo de corriente alterna (imagen 2.1). Si el hilo conductor es infinito no hay problemas para el electrón y sus adyacentes, ya que siempre encuentran espacio

para moverse libremente. Pero en una antena real el hilo no es infinito, por tanto, si el corte se realiza el corte del hilo exactamente por los puntos marcados en la imagen 2.1, el electrón A no tiene problemas para moverse dentro del espacio que le queda.

¿Qué ocurre si se corta una medida distinta de la indicada? Si es más corta, el electrón tiene que rebotar en el extremo antes de haber llegado al final de su movimiento y lo invertirá de forma distinta (fuera de fase) a como lo hace el impulso de corriente alterna (figura 2.2 a).

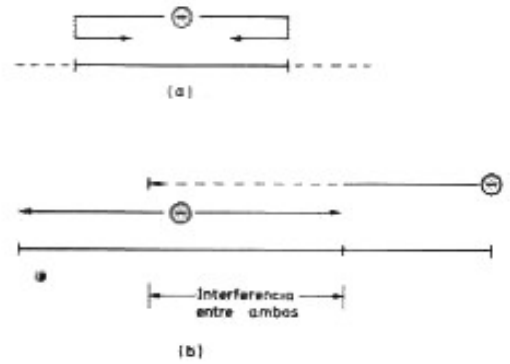


Imagen 2.1 **Efectos sobre los electrones si el cable no tiene la longitud adecuada.**

Si el hilo es más largo, el electrón A no tendrá problemas, pero el electrón B no podrá realizar el ciclo y, por tanto, intentará invadir el terreno del electrón A para conseguir completar su movimiento, interfiriéndose entre ellos. El resultado es el mismo, la corriente se interfiere y queda fuera de fase respecto al impulso de la corriente alterna que lo origina (imagen 2.2 b).

Estos son dos principios básicos del funcionamiento eléctrico de una antena:

1) La resonancia de una antena se relaciona directamente con el tamaño de la antena y la cantidad de corriente que puede fluir en ésta. La antena entra en resonancia cuando se tiene una reactancia cero y el flujo de corriente es máximo, en estas condiciones se dice que la antena es resonante a la frecuencia de diseño. El lector interesado en profundizar más acerca de este tema referirse a (Orr [1985] y Robert E. [1984]).

2) Impedancia, que depende del tipo de antena y de su construcción e instalación.

Pero la antena tiene por misión crear un campo electro-magnético que permita la comunicación, por lo tanto, cuanto más fuerte sea ese campo en la dirección deseada, más fácil será la comunicación; las características de ese campo dependen de la construcción física de la antena.

CARACTERISTICAS DE LAS ANTENAS

Polarización

Se define como polarización de una antena, la dirección que tiene el campo eléctrico de la onda electromagnética. Si el campo eléctrico es horizontal, la antena tiene polarización horizontal; si es vertical, tendrá polarización vertical. En general, la polarización coincide con la posición del hilo conductor de la antena. Si ésta tiene el conductor en posición horizontal, la antena tiene polarización horizontal; si está vertical, tendrá polarización vertical.

Angulo de radiación

Se llama ángulo de radiación al ángulo vertical (Por encima del horizonte) en que una antena emite (o recibe) la máxima intensidad de campo electromagnético.

Resulta evidente que todas las estaciones con las que podemos contactar se encuentran, o en línea horizontal o más allá del horizonte. Por el hecho de que las antenas se encuentran encima del suelo se produce una interacción entre el campo electromagnético que sale de la antena y la parte de éste que rebota en el suelo. La combinación de los dos hace que la energía se cancele para ciertos ángulos y que se refuerce para otros. El ángulo para el que el refuerzo es máximo se llama ángulo de radiación de una antena. Curiosamente ninguna antena real situada sobre el suelo tiene su máximo ángulo de radiación en dirección horizontal. La máxima radiación siempre ocurre con un cierto ángulo hacia arriba.

Directividad

Se denomina directividad a la dirección horizontal en la que se produce el máximo de radiación de una antena. Algunas antenas radian

igualmente hacia todas las direcciones horizontales, en cambio, otras tienen una o varias direcciones en las que la radiación se ve favorecido.

Ganancia

Se define como ganancia de una antena la diferencia que existe entre el campo electromagnético producido por una determinada antena en su dirección más favorable respecto al de otra antena que se toma como patrón. Científicamente se toma como referencia la antena ***isotrópica***.

Tipos de antenas

Antena Isotrópica

Es una antena ideal que radia uniformemente en todas direcciones. Evidentemente no existe tal antena pero, matemáticamente, es muy fácil calcular el campo electromagnético que produciría una antena de ese tipo. En la imagen 2.3 se puede observar el digrama de radiación de la antena isótrópica. Un diagrama de radiación sirve para determinar la energía radiada en cada dirección del espacio. Si analizamos esta antena veremos que en los planos verticales (x, z) e (y, z) la cantidad de energía radiada es exactamente la misma en todas las direcciones. Tenemos lo mismo para el plano horizontal (x, y). Esto nos indica que esta antena podrá enviar o recibir señal con las mismas condiciones esté en la posición que esté.

Si la ganancia de una antena está referida a la antena isotrópica se representa como **dBi**. Si está referida al dipolo se representa como **dBd**.

La ganancia de una antena siempre viene referida a otra, por tanto, no son de fiar las ganancias que no indiquen claramente cuál es la referencia (recordar que el decibelio es una medida comparativa).

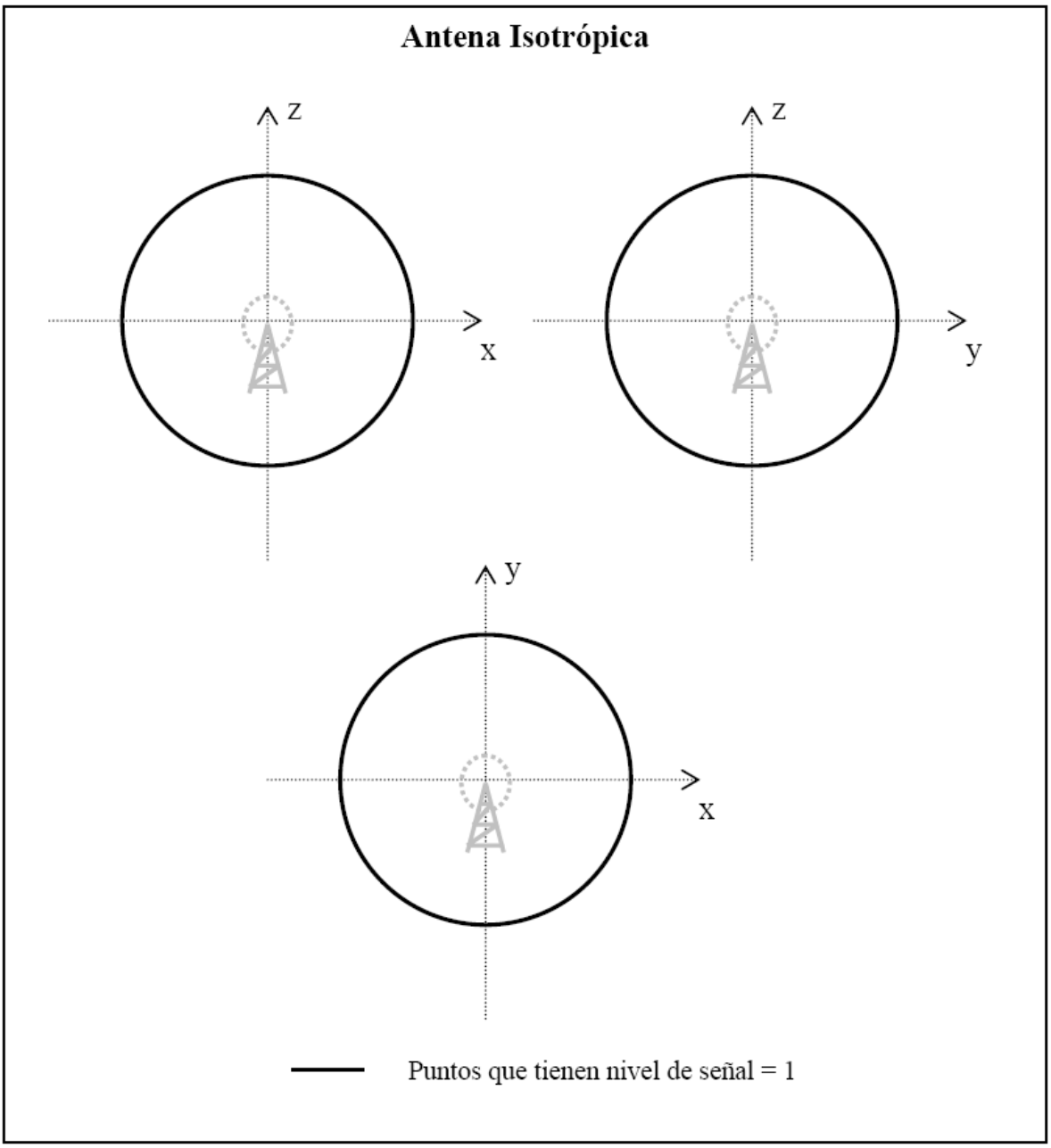


Imagen 2.3 Diagrama de radiación de la antena isotrópica

Antena direccional

Con las antenas direccionales viene el término de lóbulo principal, que se trata de la dirección donde se proyectará la mayor parte de la energía. Como es imposible hacer una antena que radie en una sola dirección nos interesará saber qué rango de direcciones (o abertura) recibirá el mayor porcentaje de energía. Nos interesará que el lóbulo principal sea lo más estrecho posible, así se gana en direccionalidad.

Por el simple hecho de trabajar en un medio físico no ideal, se cuenta con un número determinado de lóbulos secundarios. Estos lóbulos proyectarán energía en direcciones que no son la deseada, o en caso de recepción se captarán señales que no provienen directamente de nuestra fuente, captando ecos y reflexiones o interferencias de otras fuentes. Normalmente interesará una relación entre el lóbulo principal y los secundarios lo más grande posible.

Para entender como puede afectar eso usaremos el ejemplo de antena direccional de recepción de televisión. Esta antena se compone de una barra con unas espinas horizontales y detrás de todo tiene otras dos barras con espinas en una disposición de V. La disposición horizontal de esas espinas se debe a la polarización de la señal.

La barra central se encarga de recibir la señal, esta barra apunta directamente al repetidor de televisión más próximo, cuanto más alineada está la antena con el repetidor mejor es la calidad de la señal que se recibe, así el lóbulo principal apuntando directamente al repetidor. Las dos barras de la parte de atrás de la antena puesta en forma de V son reflectores, y se encargan de aprovechar mejor la señal que llega, es una manera de utilizar la forma de la antena a favor. La antena también puede recibir señal desde la parte de atrás, apunta al repetidor pero si se tiene un edificio que refleja la señal y la devuelve a la antena, como esta señal habrá recorrido una distancia mayor que la señal que llega directamente por la parte de delante de la antena.

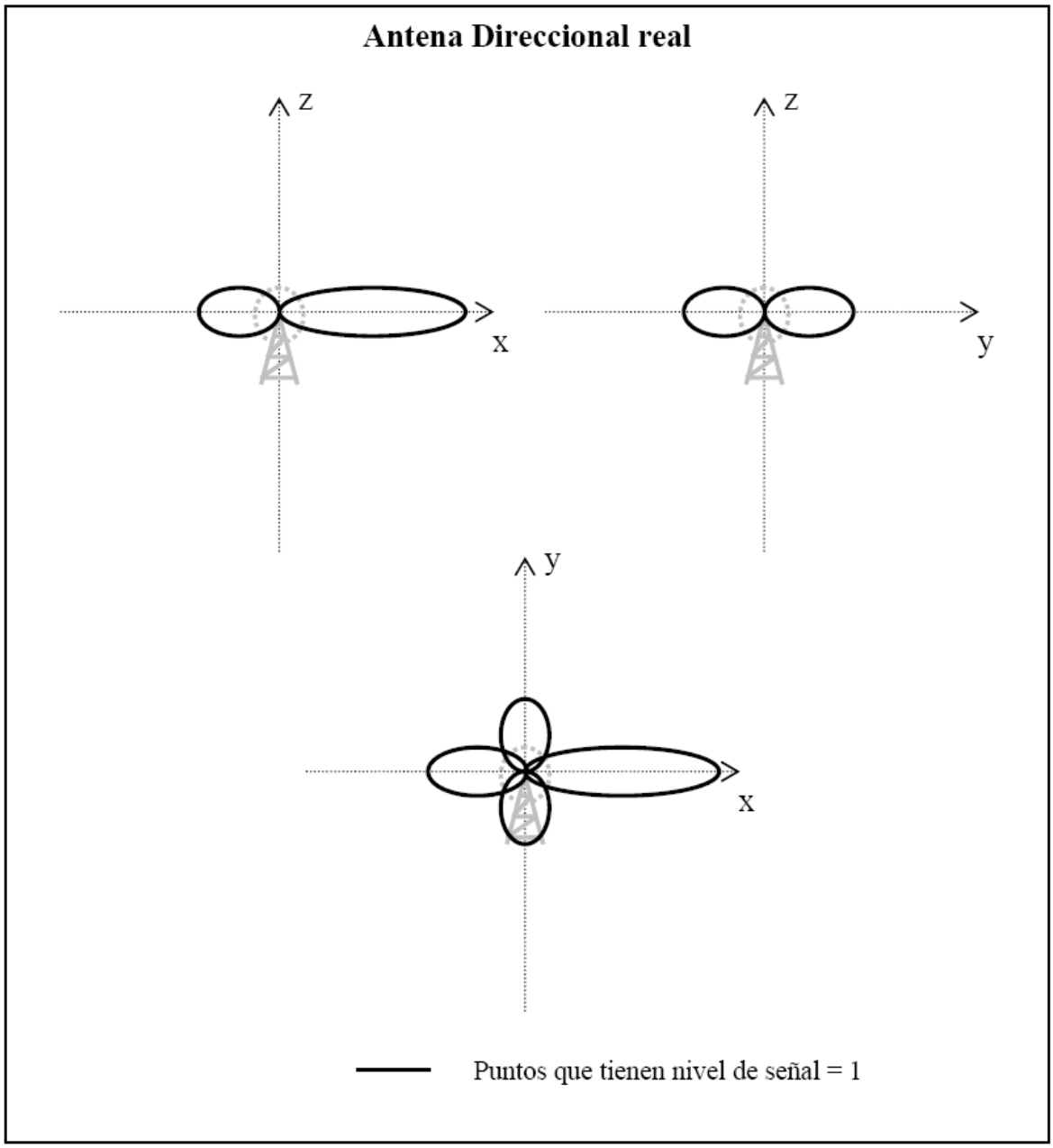


Imagen 2.4 Diagrama de radiación de la antena direccional

Antena de Dipolo

En la práctica la antena que se usa como referencia suele ser el dipolo, que ya tiene una ganancia de G=2.8 [dB] sobre la antena isotrópica. Esto se debe a que el dipolo es una antena muy simple y fácil de construir, por lo cual se pueden hacer comparaciones directas entre dos antenas sin tener que recurrir a la antena isotrópica que no existe y por tanto no es comparable directamente.

La antena de dipolo es una de las primeras antenas que se desarrollaron (por ejemplo este tipo de antena fue utilizada por Hertz y Marconi). Los dipolos y monopolos que generalmente se montan en una base plana, se usan a bajas frecuencias (HF,VHF y UHF) y se caracterizan por presentar una baja ganancia.

El costo de fabricación es bajo ya que su estructura geométrica es ligera y simple, además no presentan mayores problemas al acoplamiento con la línea de alimentación.

Antenas de abertura

En la mayoría de los casos son secciones abiertas de una guía de onda (conocidas comúnmente como antenas del tipo corneta), en otros casos pueden estar constituidas por extremos uniformes de guías de onda. Este tipo de antenas generalmente tienen una ganancia moderada y su empleo para recibir o transmitir señales es muy común en la banda de microondas.

Antenas Microcinta

Son relativamente un nuevo tipo de antenas, las cuales consisten de conductores impresos en cinta microstrip o de un tipo similar de substrato. Estas antenas son compatibles con tecnología plana para microondas. Estas antenas generalmente tienen su campo de aplicación en frecuencias para microondas, a un cuando se caracterizan por tener bajas ganancias.

Antenas de Reflector

Este tipo de antenas se caracterizan por tener alta ganancia, debido principalmente al diseño del plato el cual concentra la mayor parte de la radiación en el alimentador que se ubica en el punto focal del plato reflector, y en la mayoría de los casos es del tipo parabólico ó cilíndrico.

Su alta ganancia es una de las razones para emplear reflectores de gran tamaño para captar o transmitir en la región de microondas. Los platos reflectores son fáciles de fabricar, los cuales pueden ser muy grandes y robustos, por lo tanto su manejo es difícil.

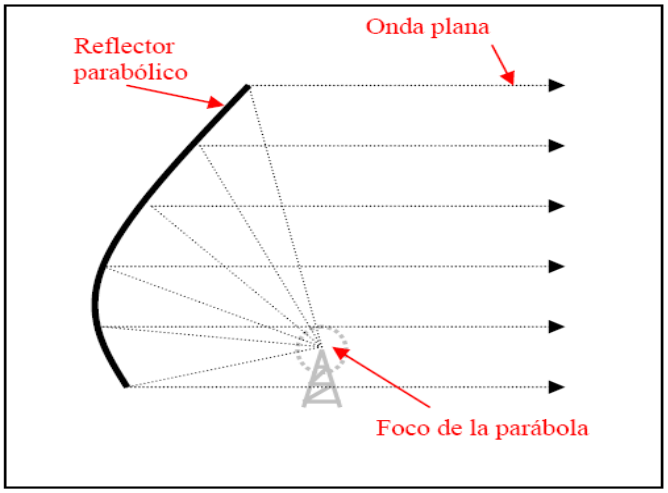


Imagen 2.5 Esquema de una antena de Reflector

Imagen 2.6 Algunos tipos de antenas

Antenas Omnidireccionales:

Una antena omnidireccional no emite exactamente en todas direcciones, sino que tiene una zona donde irradia energía por igual (por ejemplo el plano horizontal). Por ejemplo no puede interesar emitir o recibir señal de la parte que está exactamente encima de la antena, imaginémonos la antena de radio del coche. Se debe tener en cuenta también que en el plano horizontal sí que el comportamiento es totalmente omnidireccional. En el siguiente esquema (imagen 2.7) se puede observar este comportamiento, se observa la cantidad de señal enviada en dirección z es 0, en cambio la que se envía en las direcciones x e y es máxima, y entre los dos límites hay una graduación.

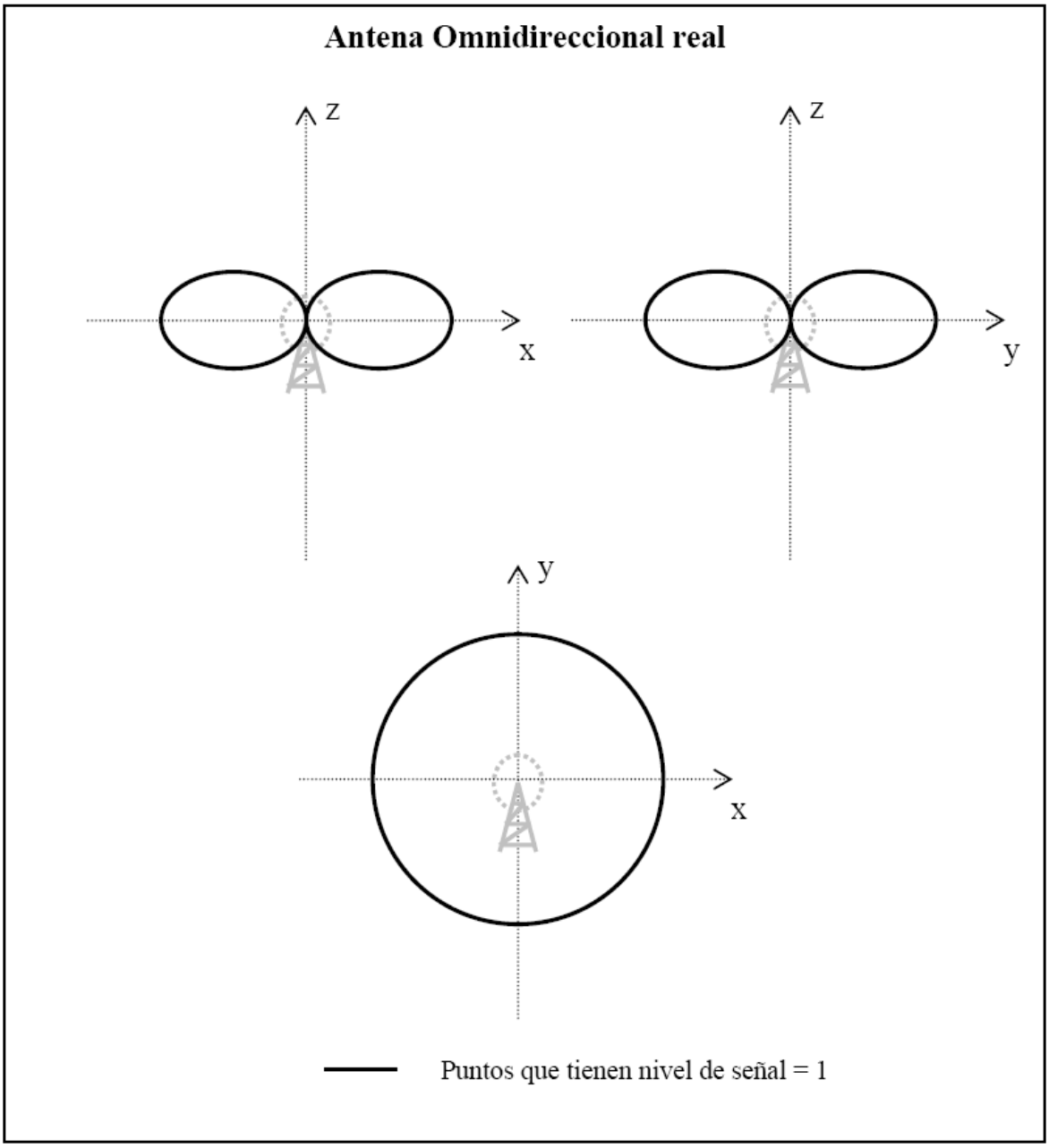


Imagen 2.7 Diagrama de radiación de la antena omnidireccional

- Lo más habitual es que no sobrepasen los 12-15dB de ganancia.
- También concentran la energía, pero en vez de hacerlo en una sola dirección, lo hacen horizontalmente. Cuanto mayor sea la ganancia de la antena, más energía se radia hacia el horizonte, y menos verticalmente.
- Una antena omnidireccional teórica de 0dB, radiaría en forma de esfera, es decir, igual en todas las direcciones.

- Una antena de tipo dipolo Ganancia (G)=2.2[dB] sería una esfera algo más aplanada, es decir, radia menos energía verticalmente (hacia arriba, y hacia abajo).
- Una antena omnidireccional de G=8[dBi] sería una esfera visiblemente plana, que concentra mucha energía en el horizonte, y radia poco verticalmente.
- Una omnidireccional de G=15[dBi] tendría poco aspecto de esfera de lo aplanada que sería. Apenas radia energía verticalmente. En el caso de ponerla en lo alto de un edificio, puede que las plantas bajas del mismo o plantas bajas de edificios cercanos ni siquiera tengan cobertura.
- Hay que imaginar una omnidireccional teórica de Ganancia (G)=100[dB]. No sería una esfera, sino un disco. Sólo radia hacia el horizonte: es capaz de llegar muy lejos, pero sólo en una fracción del horizonte, con lo cual apenas ofrece cobertura. No existe tal antena.
- Tipos más habituales de antenas omnidireccionales (ganancias orientadas)

  - Dipolo: G= 2.2 [dBi]
  - Colineales: G= 5-12 [dBi]
  - Guía-Ondas Ranuradas: G= 10-15 [dBi]

En el caso de las antenas internas de las tarjetas, su eficiencia y características empeoran considerablemente por estar colocadas muy cerca (de hecho, pegadas) a un aparato electrónico con partes de diversos materiales, especialmente relevantes las metálicas, por reflejar las microondas. Según las pruebas, resulta muy recomendable usar algún tipo de antena externa, aunque sea una sencilla omnidireccional de realización casera y ganancia moderada.

Tarjetas Inalámbricas

Los componentes básicos que se necesitan para crear una infraestructura wireless son los siguientes:

Tarjetas

Hay varios tipos de tarjetas disponibles en el mercado por su forma, las hay casi para cualquier dispositivo, las hay pcmcia para portátiles, pci para equipos de sobremesa y Compact Flash para dispositivos utraportatiles como PDAs o Tablet Pc, su misión principal es comunicar a los clientes con la red wireless aunque esto siempre no es así.

En el inicio del desarrollo de la tecnología, los chipsets mas extendidos para 802.11b, eran los ORINOCO, los prism y hermes, el chipset prism se puede usar en sistemas GNU/Linux y *BSD como AP. Para 802.11-DS+5.5+11 y 802.11+ se usaban un chipset de Texas Instruments.

Actualmente y gracias a los estándares internacionales que ahora existen, las marcas son muchas y de diferentes precios, soportan los diferentes estándares, y son soportadas en diferentes sistemas operativos, ya depende más del controlador que tenga instalado.

TarjetaPCI

Tarjeta PCMCIA

Imagen 2.8 Tipos de Tarjetas

En la siguiente imagen 2.9, se observa el alcance de las ondas de radio en función de la frecuencia:

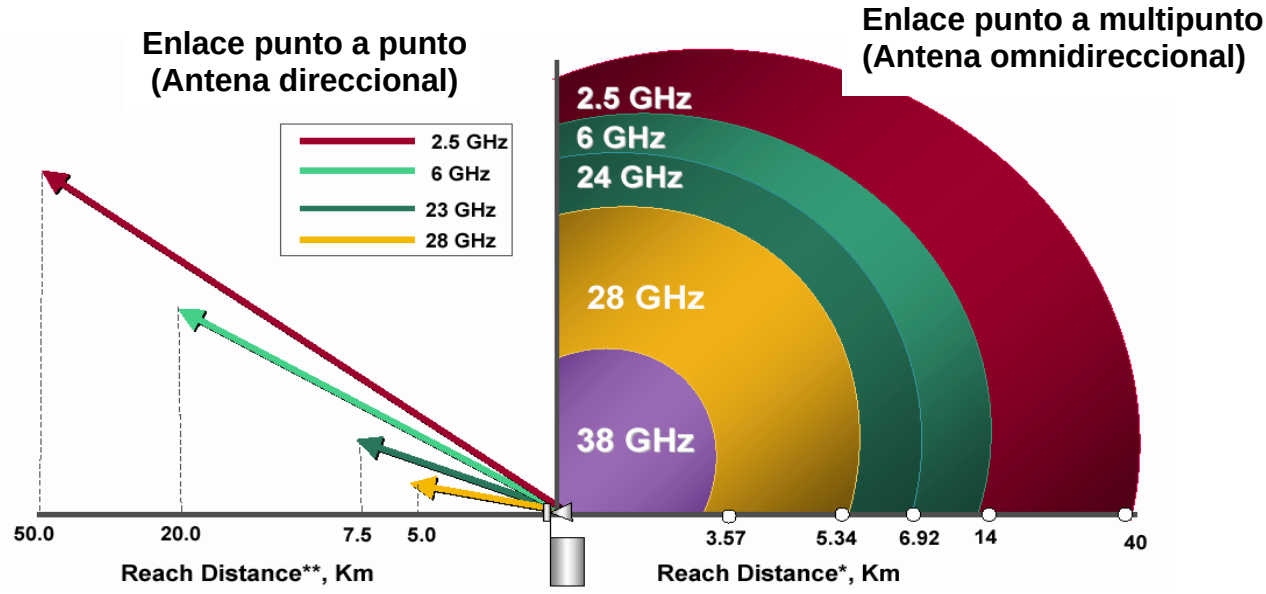


Imagen 2.9 Gráficas de distancia vs Frecuencia

Los dispositivos de red wireless, se pueden clasificar en diferentes generaciones según sus características, principalmente de su magnitud de frecuencia y de su velocidad. Básicamente se pueden distinguir tres generaciones, con la cuarta en pleno desarrollo.

Primera

Se habla de redes inalámbricas aisladas, con velocidad de 1Megabit y no existía Roaming ni compatibilidad entre marcas. La administración que se podía llevar a cabo es muy limitada y no existían estándares para la convivencia de dispositivos.

Segunda

En la segunda generación se comienza a administrar la seguridad en capas. Se comienza a hablar de roaming, por lo que aumentan considerablemente las zonas de cobertura. Comienzan los estándares y la compatibilidad entre las principales marcas de dispositivos. Comienzan las velocidades de 11 Mbps.

Tercera

En la tercera se habla de redes inalámbricas sin barreras, una convergencia entre redes públicas y privadas con mecanismos de seguridad avanzada. En cuanto a la velocidad, actualmente existen velocidades que van desde los 11Mbps (Megabits por segundo), 54 Mbps e incluso existen proveedores que ofrecen hasta 108Mbps.

Cuarta

Esta generación, está en pleno desarrollo, se considera el siguiente paso, los sistemas de 4ª generación deberán ser la red de acceso universal de los usuarios, con entera libertad de movimiento en cuanto a velocidad o cobertura, los de proveedores de servicios de telecomunicaciones buscan ser completamente compatibles con Internet; capaces de atender usuarios de diferentes servicios con necesidades diversas, servicio de calidad; y capaces de dar servicio a usuarios con movilidad irrestricta, proporcionándoles velocidades de transmisión más de 10 veces mayores que las ofrecidas por las redes inalámbricas de 3a generación. Sin embargo, no hay que perder de vista que de esta generación ya hay dispositivos, pero no funcionan al 100% cumpliendo con el objetivo del desarrollo de la generación.

2.2 Historia de las redes inalámbricas

Fecha	Evento
1986	Primeras WLANs. 900 MHz (860 Kbps). No disponible en Europa.
1993	WLANs de 1 y 2 Mbps en banda de 2,4 GHz. Primeras disponibles en Europa
7/1997	IEEE aprueba 802.11. 1 y 2 Mbps. Banda de 2,4 GHz e infrarrojos.
1998	Primeros sistemas de11 Mbps a 2,4 GHz. Preestándar 802.11b.
9/1999	IEEE aprueba 802.11b (hasta 11 Mbps, 2,4 GHz) y 802.11a (hasta 54 Mb/s, 5 GHz, no disponible en Europa)
12/2001	Primeros productos comerciales 802.11ª
12/2001	Borrador 802.11e (QoS en WLANs)
2003	IEEE aprueba 802.11g (hasta 54 Mbps, 2,4 GHz)

Tabla 2.1 Historia de la tecnología

2.3 Forma de trabajo de las redes inalámbricas

➢ Modelo de referencia de 802.11

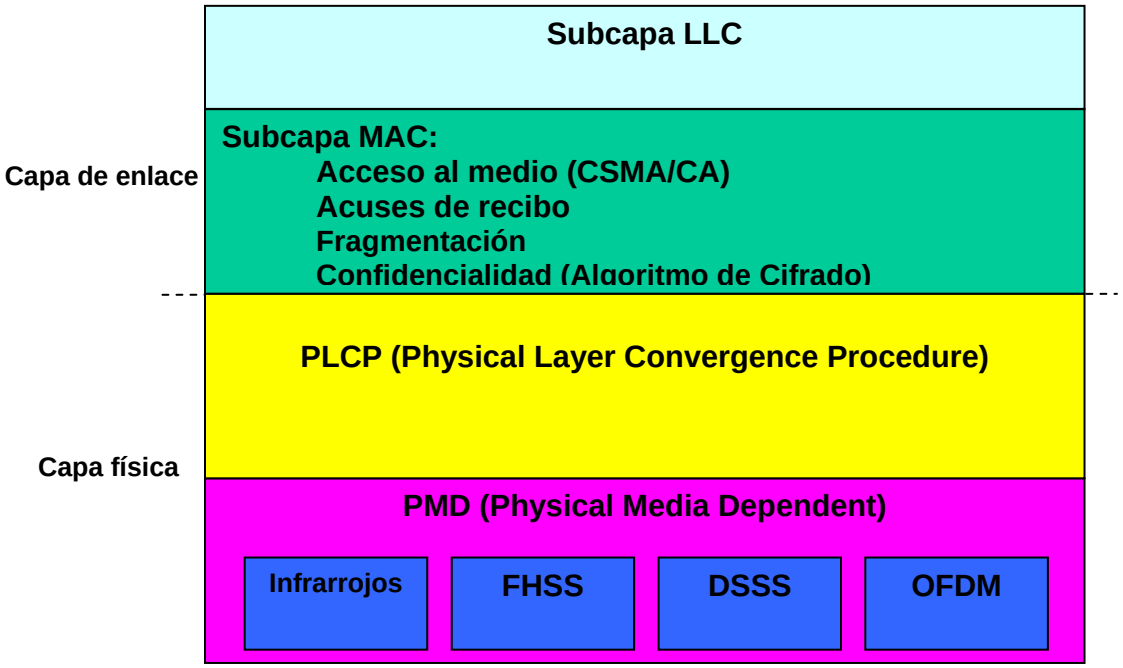
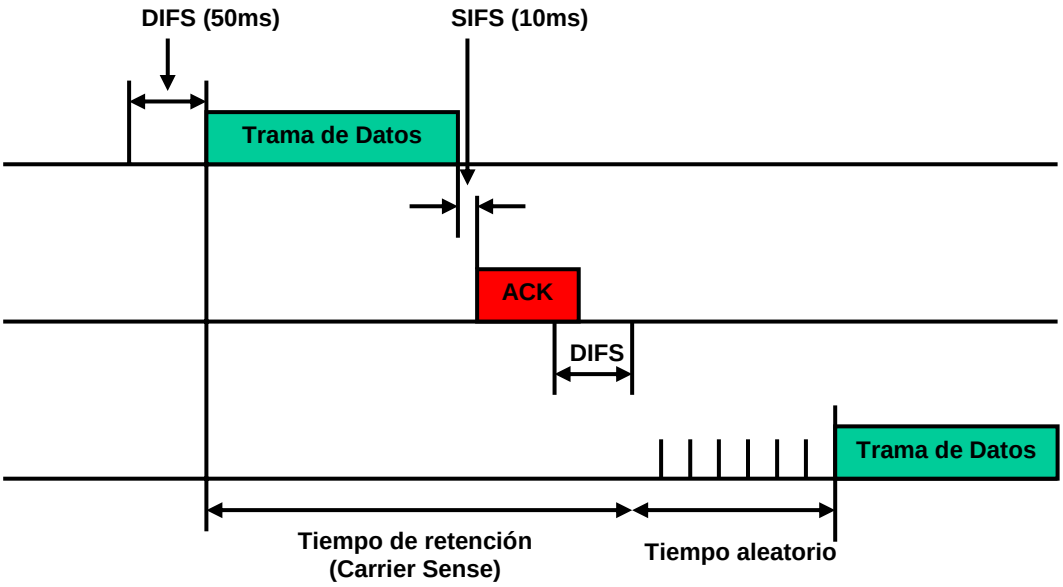


Imagen 2.9. Modelo de Capas

➢ Protocolo MAC de 802.11

El protocolo MAC utiliza una variante de Ethernet llamada CSMA/CA (Carrier Sense Multiple Access/Colision Avoidance). No puede usarse CSMA/CD porque el emisor de radio una vez empieza a transmitir no puede detectar si hay otras emisiones en marcha (no puede distinguir otras emisiones de la suya propia).

Cuando una estación quiere enviar una trama escucha primero para ver si alguien está transmitiendo. Si el canal está libre la estación transmite. Si está ocupado se espera a que el emisor termine y reciba su ACK, después se espera un tiempo aleatorio (siempre superior a un mínimo prefijado) y transmite. El tiempo en espera se mide por intervalos de duración constante. Al terminar espera a que el receptor le envíe una confirmación (ACK). Si ésta no se produce dentro de un tiempo prefijado considera que se ha producido una colisión, en cuyo caso repite el proceso desde el principio.



DIFS: DCF (Distributed Coordination Function) Inter Frame Space
SIFS: Short Inter Frame Space

Imagen 2.10. Secuencia de trabajo

Las colisiones se dan cuando dos estaciones a la espera elijan el mismo número de intervalos (mismo tiempo aleatorio) para transmitir después de la emisión en curso. En ese caso reintentan ampliando exponencialmente el rango de intervalos y vuelven a elegir. Es similar a Ethernet salvo que las estaciones no detectan la colisión, infieren que se ha producido cuando no reciben el ACK esperado. También se produce una colisión cuando dos estaciones deciden transmitir a la vez, o casi a la vez. Pero este riesgo es mínimo. Para una distancia entre estaciones de 70[m] el tiempo que tarda en llegar la señal es de 0,23 [μs].

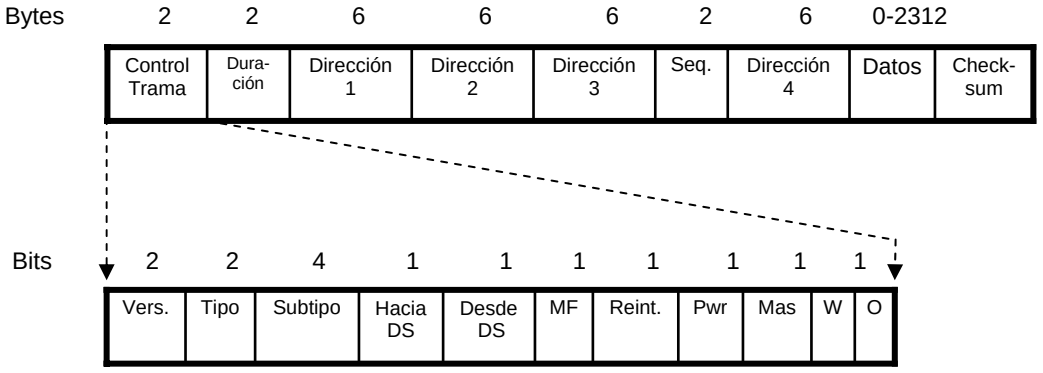
En el nivel MAC de 802.11 se prevé la posibilidad de que el emisor FRAGMENTE una trama para enviarla en tramas más pequeñas. Por cada fragmento se devuelve un ACK por lo que en caso necesario es retransmitido por separado.

Si el emisor ve que las tramas no están llegando bien puede decidir fragmentar las tramas grandes para que tengan más probabilidad de llegar al receptor.

La fragmentación permite enviar datos en entornos con mucho ruido, aun a costa de aumentar el overhead. Todas las estaciones están obligadas a soportar la fragmentación en recepción, pero no en transmisión.

El uso de mensajes RTS/CTS se denomina a veces *Virtual Carrier Sense*, permite a una estación reservar el medio durante una trama para su uso exclusivo. Si todas las estaciones se 'escuchan' directamente entre sí el uso de RTS/CTS no aporta nada y supone un overhead importante, sobre todo en tramas pequeñas. Se debe tomar en cuenta que no todos los equipos soportan el uso de RTS/CTS. Y los que lo soportan permiten indicar en un parámetro de configuración a partir de que tamaño de trama se quiere utilizar RTS/CTS. También se puede deshabilitar por completo su uso, cosa bastante habitual.

En la siguiente imagen se puede observar el formato de la trama 802.11:



MF: **Indica que siguen más fragmentos**
Reint.: **Indica que esta trama es un reenvío**
Pwr: **Para 'dormir' o 'despertar' a una estación**
Mas: **Advierte que el emisor tiene más tramas para enviar**
W: **La trama está cifrada con WEP (Wireless Equivalent Privacy)**
Duración: **Dice cuanto tiempo va a estar ocupado el canal por esta trama**
Dirección **Dirección de origen y destino. Dirección de base origen y destino.**

Imagen 2.11 Formato de trama

- **Forma de trabajo de las redes wireless**

El equipo (por lo general un AP) tiene dos antenas. El proceso es el siguiente:

a) El equipo recibe la señal por las dos antenas y compara, eligiendo la que le da mejor calidad de señal. El proceso se realiza de forma independiente para cada trama recibida, utilizando el preámbulo (128 bits en DSSS (Direct Sequence Spread Spectrum)) para hacer la medida.

b) Para emitir a esa estación se usa la antena que dio mejor señal en recepción la última vez

c) Si la emisión falla (no se recibe el ACK) cambia a la otra antena y reintenta

Las dos antenas cubren la misma zona.

Al resolver el problema de la interferencia multitrayectoria de DSSS el uso de FHSS ha caído en desuso.

Cuando una estación se enciende busca un AP en su celda. Si recibe respuesta de varios atiende al que le envía una señal más potente. La estación se registra con el AP elegido. Y como consecuencia de esto el AP le incluye en su tabla MAC.

El AP se comporta para las estaciones de su celda como un hub inalámbrico. En la conexión entre su celda y el sistema de distribución el AP actúa como un puente.

El servicio básico de área (BSA), es el área de radiofrecuencia cubierta por un access point, también referida como microcelula. Para el caso en el que se desee extender el área de servicio de una WLAN, es necesario adjuntar otro access point, de ésta manera se agrega otra microcelula a la región de cobertura. Sin embargo, para este caso se puede hablar de varios tipos de configuración, ya sea que los AP's estén conectados al mismo backbone o no.

Master
Es el modo en que se encuentra el AP para que pueda hacer de HUB.

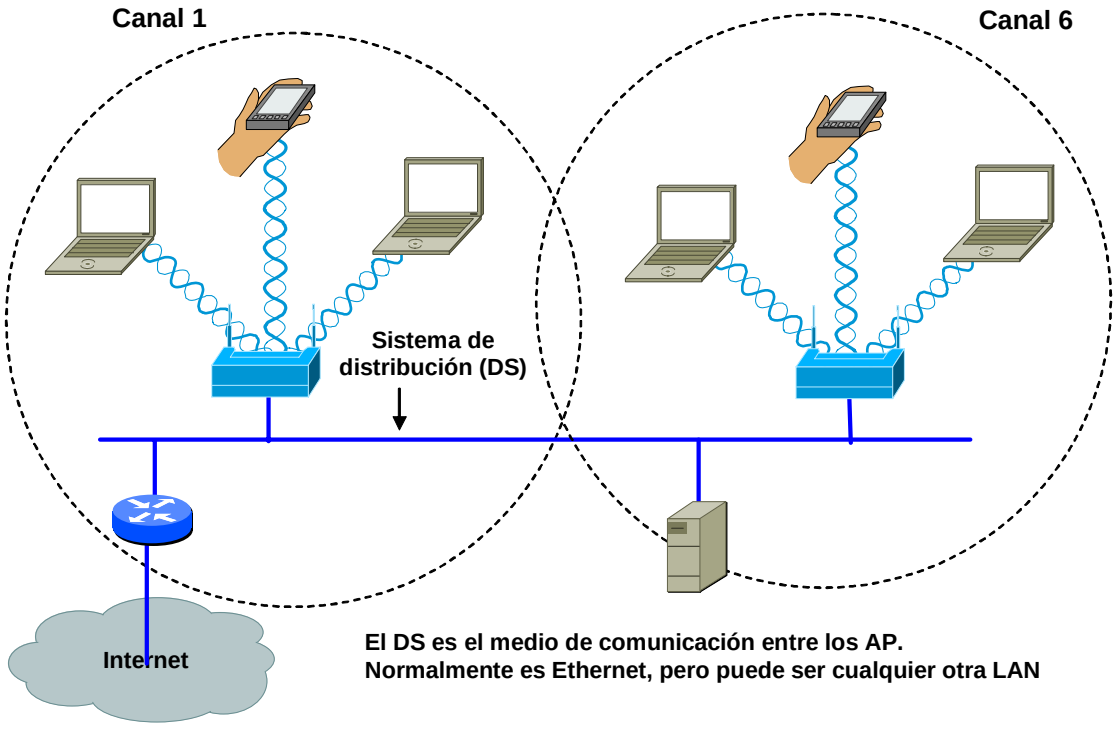
WDS
Es el modo que suele usar un AP para repetir la señal del AP Master cuando no existe cobertura suficiente.

2.4 Topologías Wireless

Infraestructuras posibles

a) **Configuración típica de una WLAN**, es referida a que cada access point este en diferente canal, y que los clientes los vean como puntos independientes (para mejor performance) y ellos elijan a que punto de acceso quieren conectarse. Así cada cliente solo puede comunicarse con otros clientes de la misma microcelula, y para hacerlo con los clientes de otras microcélulas, lo tienen que hacer con el uso del access point maestro (que es el primero que esta conectado en el backbone y es el que controla el flujo de tráfico de la red). Se pueden agregar el número de microcélulas que sean necesarias y así extender la zona de cobertura, a esto se le llama Servicio de Área Extendido (ESA). Es recomendable que entre las células extendidas se tenga en el 15 o 10 % de traslape para permitir el roamming entre los usuarios, sin que pierdan la conexión o la calidad de radiofrecuencia.

Imagen 2.12 Configuración típica de una WLAN



b) **Arquitectura microcelula.** Es una típica WLAN, puede incluir: PC's, Laptops, impresora, palm o cualquier dispositivo que se pueda conectar a una red convencional, sin embargo con varios

dispositivos, se puede experimentar una sobrecarga de dispositivos para el access point y el área de cobertura no es tan grande. Para resolver estos problemas, es recomendable agregar más access point, que puedan ayudar a balancear la carga de dispositivos. Para lograr el buen funcionamiento de ésta configuración, se recomienda que se tenga configurado el roaming (que los usuarios puedan tener movilidad entre cada célula).

Los AP envían regularmente (10 veces por segundo) mensajes de guía (beacon) para anunciar su presencia a las estaciones que se encuentran en su zona. Si una estación se mueve y cambia de celda detectará otro AP más potente y cambiará su registro. Esto permite la **ITINERANCIA ('HANDOVER')** sin que las conexiones se corten.

Los estándares 802.11 **no detallan** como debe realizarse la itinerancia, por lo que la interoperabilidad en este aspecto no siempre es posible. Sin embargo tratando de corregirlo varios fabricantes han desarrollado el IAPP (INTER-ACCESS POINT PROTOCOL).

c) Red Wireless con redundancia, es referido a la configuración que es necesaria cuando se habla de sistemas en los cuales la comunicación no puede ser interrumpida, y es necesario hacer una configuración de redundancia. Para ésta configuración si se debe tener cuidado en la compatibilidad de las marcas de los dispositivos, ya que hay muchas que no permiten la compatibilidad o estar en standby. El monitoreo es hecho para ambos vía radiofrecuencia y la conexión ethernet. La configuración del access point standby debe ser la misma que la del maestro, es decir, debe estar en el mismo canal de radiofrecuencia, y coincidir en todos los parámetros para que el servicio hacia los clientes sea transparente y no se note el cambio de access point.

d) Red Wireless con un access point cableado y un repetidor. En un desarrollo donde se extiende la cobertura es necesario, pero el acceso al backbone no es práctico, en el caso de hablar solo de extender la cobertura con el mismo número de clientes, entonces es más práctico usar un repetidor wireless. Que es simplemente un access point que no está conectado directamente al backbone cableado. Requiere del 50% de traslape con la señal del access

point maestro y se recomienda que éste repetidor se encuentre en el mismo canal.

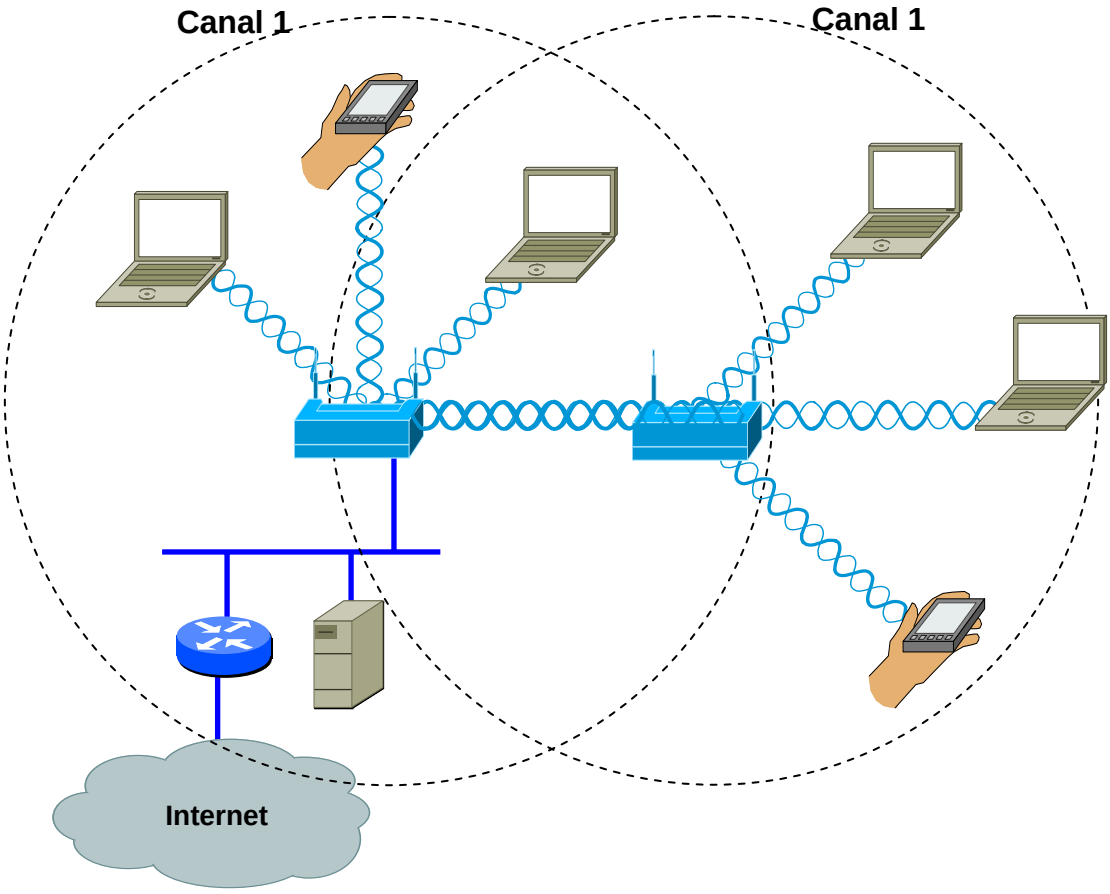


Imagen 2.13. Access Point cableado y repetidor.

Ad-hoc o BSS (Basic Service Set) Es un modo peer to peer es posible conectar muy pocos dispositivos en red por este método, se suele utilizar para enlaces punto a punto, por ejemplo para conectar dos PC's en un momento dado donde se encuentren solos sin otro tipo de red o para unir dos nodos wireless distantes.
En la imagen 2.8 se observa la posible arquitectura de una red wireless, para este caso se observa que se configuran 3 equipos en el mismo segmento de red. Se observa que este topología solo es usada para redes muy pequeñas y de preferencia de uso interno, o en una misma zona.

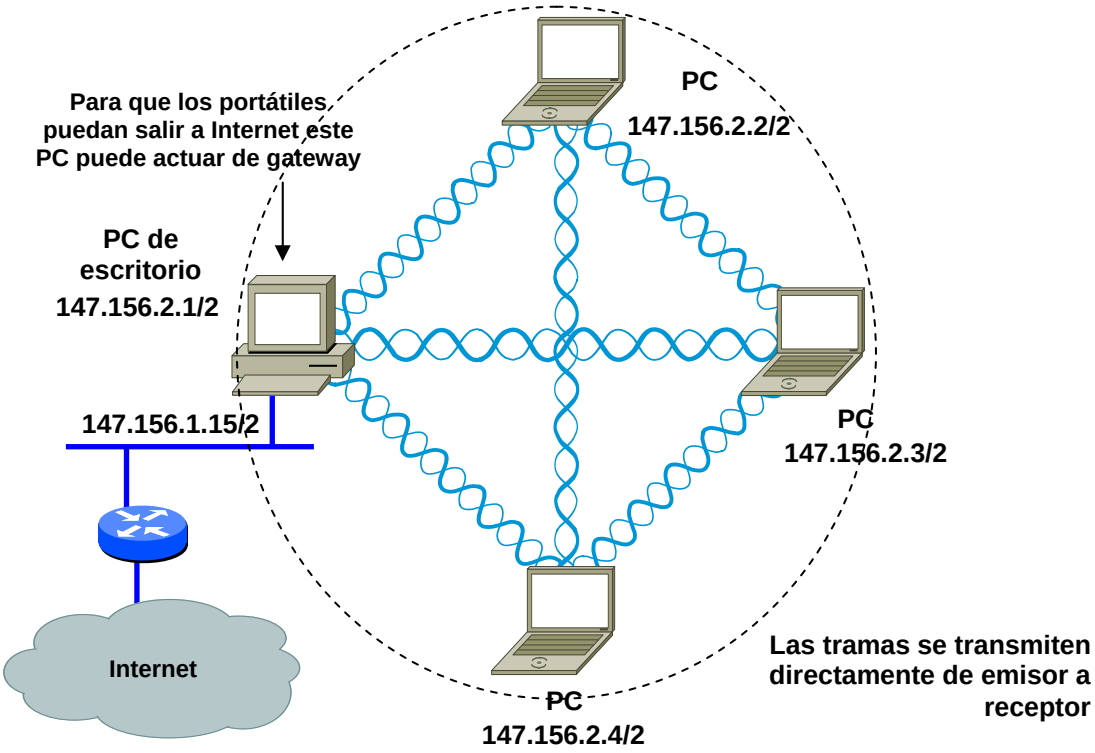


Imagen. 2.14 Topología Ad-hoc

f) Extensión de una red LAN convencional o cableada, la cual es de mucha utilidad para escalar nuestra red LAN, en alguna zona donde no sea tan fácil cablear, donde de un puerto del switch, se va a alimentar al AP y éste dará la conexión para los nuevos equipos que también podrán acceder a los recursos que se comparten con la red convencional.

g) Infraestructura o Managed: Se usa para conectar a un AP que hará el papel de HUB donde todos los paquetes de la red inalámbrica pasaran por ese AP.

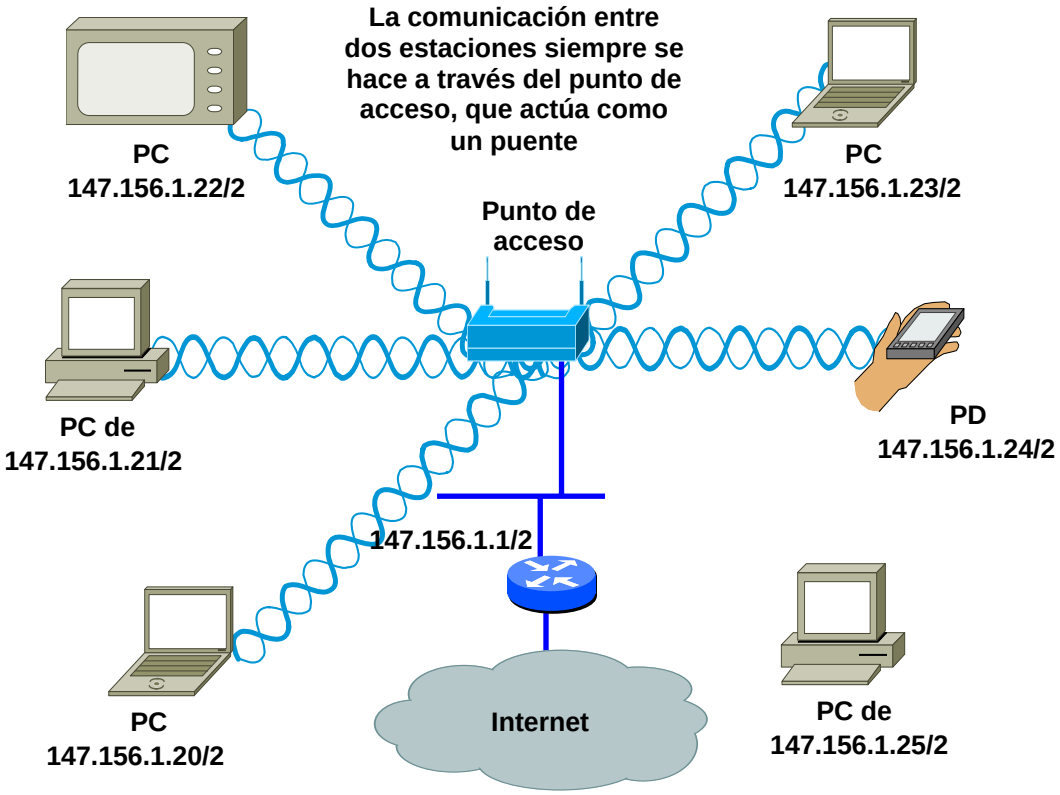


Imagen. 2.15 Topología de infraestructura

2.5 Administración de redes Wireless

Hablando del punto de vista de la administración, se tienen que contemplar varios aspectos. Desde la alimentación de energía de los dispositivos que conforman la red, hasta el uso de los recursos que se están compartiendo en dicha red.

Hablando del ahorro de energía, es importante en WLANs ya que muchos dispositivos funcionan con baterías. Muchos equipos contemplan un modo de funcionamiento latente o 'standby' de bajo consumo en el que no pueden recibir tramas. Y antes de 'irse a dormir' las estaciones deben avisar a su AP, para que retenga las tramas que se les envíen durante ese tiempo.

Periódicamente las estaciones dormidas han de 'despertarse' y escuchar si el AP tiene algo para ellos. El AP descarta las tramas retenidas cuando ha pasado un tiempo sin que sean solicitadas

Desde el punto de vista del rendimiento de los dispositivos, en cuanto al ancho de banda que manejan, El rendimiento real suele ser el 50-60% de la velocidad nominal. Por ejemplo con 11 Mb/s se pueden obtener 6 Mb/s en el mejor de los casos.

El overhead se debe a:

- Mensajes de ACK (uno por trama)
- Mensajes RTS/CTS (si se usan)
- Fragmentación (si se produce)
- Protocolo MAC (colisiones, esperas aleatorias, intervalos entre tramas)
- Transmisión del Preámbulo (sincronización, selección de antena, etc.) e información de control, que indica entre otras cosas la velocidad que se va a utilizar en el envío, por lo que se transmite a la velocidad mínima (1 Mb/s en FHSS y DSSS, 6 Mb/s en OFDM). Solo por esto el rendimiento de DSSS a 11 Mb/s nunca puede ser mayor del 85% (9,35 Mb/s)

Mucho se habla que las radiaciones de la señal no son buenas para la salud y es preocupante para muchas personas el hecho de que afecten a los seres humanos que las usan o que tienes que estar en una oficina donde se cuenta con una red inalámbrica, sin embargo se debe mencionar que:

- La radiación electromagnética de 2,4 GHz es absorbida por el agua y la calienta (hornos de microondas). Por tanto un emisor WLAN podría calentar el tejido humano. Sin embargo la potencia radiada es tan baja (100 mW máximo) que el efecto es despreciable. Es mayor la influencia de un horno de microondas en funcionamiento.
- Un Terminal GSM transmite con hasta 600 mW y se tiene mucho más cerca del cuerpo normalmente (aunque GSM no emite en la banda de 2,4 GHz).
- Los equipos WLAN solo emiten cuando transmiten datos. Un teléfono GSM emite mientras está encendido.

Desde el punto de vista de seguridad, la seguridad básica con la que cuentan éste tipo de redes es que los clientes y el punto de acceso se asocian mediante un **SSID (System Set Identifier)** común.

El SSID sirve para la identificación de los clientes ante el punto de acceso, y permite crear grupos 'lógicos' independientes en la misma zona (parecido a las VLANs). Esto no es en sí mismo una medida de

seguridad, sino un mecanismo para organizar y administrar una WLAN en zonas donde tengan que coexistir varias en el mismo canal.

Se dispone de mecanismos de autentificación y de cifrado los cuales se basan en diferentes protocolos que se verá más adelante.

2.6 Protocolos de Seguridad de redes Wireless

Hablando de redes Wireless, es muy importante el aspecto de seguridad ya que a diferencia de una red cableada en la cual para acceder a dicha red, se necesita la conexión física, en una red wireless alguien, puede acceder a la red solo estando ubicado en la zona de cobertura e incluso sin estar ubicado en la zona para cual fue definida la red.

Para una red wireless, es importante hablar de dos aspectos, la Autenticación y el cifrado. La autenticación es la que verifica que se pueda trabajar en una red, es el método que usan algunas aplicaciones para el control de acceso, lógicamente éste proceso requiere que el usuario presente sus credenciales de identificación y que el mecanismo las valide para permitir el acceso.

El cifrado es el que provee el cifrado de llaves después de la autenticación. Además es el mecanismo que es usado para proteger el flujo de control de datos.

El canal de las redes inalámbricas es totalmente inseguro, el medio es el aire y este medio es público a toda persona que se encuentre cerca. Además cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos).

Se puede mencionar la evolución de la seguridad de las WLAN en tres generaciones.

En la primera, se da el desarrollo del cifrado WEP, el cual no es fuerte en su autenticación. Su llave es estática y fácilmente vulnerable y no es escalable.

Las viejas formas de autenticación, consistían en solo algunas restricciones y dependían de métodos de seguridad como identificación de una WLAN por medio del SSID, control de

autenticación por medio de dirección MAC, llaves WEP estáticas y no había autenticación mutua.

El SSID, es el nombre del esquema de red y el cliente y el AP lo comparten. Si el cliente no tiene el SSID adecuado, entonces se deshabilita la asociación con el AP y ya no accede a la red.

El filtro de conexión por medio de dirección MAC, consiste en las tablas que se construyen manualmente en al access point para permitir o no permitir que los clientes se conecten dependiendo de la dirección física del equipo con el que desean conectarse.

WEP, era una buena opción, ha sido roto de distintas formas, lo que se ha convertido en una protección inservible. Como solución, el IEEE comenzó el desarrollo de la norma de seguridad, conocida como 802.11i.

WEP usa un algoritmo RC4 hay versiones de 64 a 256 bits pero la que actualmente mas se utiliza es la de 128 bits. Utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

En la segunda generación se tiene el desarrollo del Wi-Fi Protected Access (WPA). El cual provee cifrado, es fuerte y basa su autenticación en información del usuario.

En el presente, se tiene identificación y protección contra ataques de denegación de servicios. Los servicios de cifrado, ya cuentan con el algoritmo de cifrado AES, un manejo de llave dinámica, como puede ser el servicio provisto por WPA2.

Proceso de conexión a una Wireless LAN

El proceso de conexión a una red wireless tiene dos pasos envueltos en 3 estados:

1. No autentificado y No asociado
2. Autenticado y No asociado
3. Autenticado y Asociado

Durante el desarrollo de los estados anteriores el AP y el cliente intercambian los llamados "Magnament Frames" de ahí que a este tipo de red con AP se le llame Managed.

El Proceso que hace el cliente para poderse conectar al AP es el siguiente:

- Los AP emiten BACON Frames cada cierto tiempo.
- Estos frames contiene información sobre el AP (ESSID, si tiene WEP, etc.)
- Los clientes básicamente van en busca de BACON Frames para identificar posibles puntos de acceso.
- Una vez se topa con los BACON frames de un AP se asocia a él y se autentifica.
- Los clientes pueden emitir tramas "PROMOVE_REQUEST" para autentificarse en un AP con una ESSID en particular, en caso que en el área haya varios access point.

CAPÍTULO 3

ELEMENTOS DE ADMINISTRACIÓN Y SEGURIDAD EN REDES WIRELESS

3.- Elementos de seguridad y administración de redes wireless

Como administrador es importante tener un extenso conocimiento de las herramientas existentes y poder prevenir el funcionamiento inadecuado de la red. Es decir, que pueda garantizar que el servicio prestado es de alta calidad.
Como un asesor de seguridad en la red es necesario saber de herramientas que ayudan a prevenir un ataque o dar demasiada información sobre dicha red. Así como conocer los posibles ataques a los que se puede enfrentar.
En general se debe que garantizar una alta calidad de los servicios y garantizar que el usuario va contar totalmente con los 3 aspectos más importantes en la seguridad: Confiabilidad, Integridad y Disponibilidad.
A continuación se presentarán las herramientas principales que existen en el mercado, clasificadas desde 2 puntos de vista: la administración y seguridad.

3.1 Elementos de Administración

Para llevar a cabo una buena administración de la red, no es suficiente comprar los dispositivos de red y conectarlos, por que aunque la mayoría son plug and play, es decir, los conectas y comienzan a funcionar y generalmente funcionan como se necesita, esto no garantiza que sea la mejor y adecuada forma de trabajar de dichos componentes, ya que la mayoría de ellos cuentan con un software propietario (firmware), que tiene que configurarse a gusto y necesidades y no dejar la que traen de fábrica, ya que además de ser altamente inseguro, no es recomendable para obtener el mejor desempeño y aprovechar al máximo todas las características de dichos dispositivos.
Además de la buena configuración de los dispositivos de red, hay que configurar y apoyarse de otro tipo de dispositivos, complementarios que ayuden a las tareas de administración.

3.1.1 Sistemas de autenticación de acceso a la red

Es elemental poder llevar un control de a quién se le está prestando el servicio, y quién tiene derecho a tener ese servicio. O sea, llevar un control estricto de quienes están dentro de la red.
Se puede tener el caso de diferentes redes inalámbricas en un solo edificio, o redes que se sobreponen, una persona que pertenece a una red pero que este dentro del radio de 100 metros (por lo general es el alcance de un access point), es posible que no se cuente con las medidas de seguridad adecuadas, se pueda tener acceso a ella, lo que significa que aparte de consumir recursos, pone en riesgo la seguridad de los usuarios.

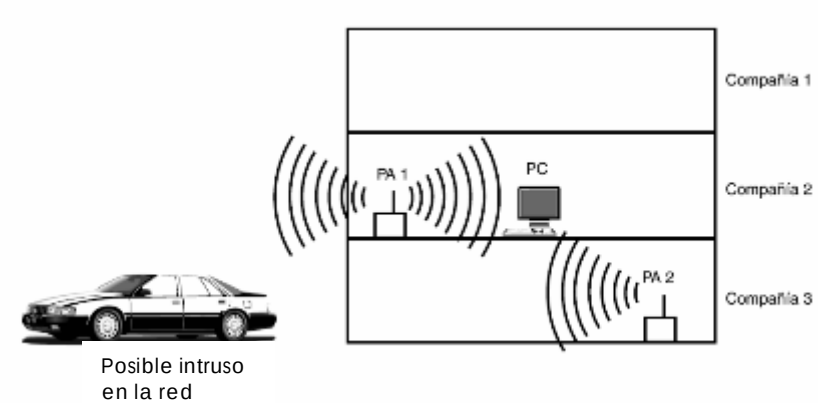


Imagen. 3.1 Posible Intrusión a una red Wireless

Para este aspecto, hay varias soluciones que se ofrecen ya, algunas con un alto costo, otras gratuitas, ya sea que se trate de software o hardware.

3.1.1.1 Sistema de filtrado de direcciones MAC en el Access Point.

Este es un método que consiste en la creación de una tabla de datos en cada Access point que forma parte de la red. Esta tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar a dicho access point. Es sabido que toda tarjeta de red posee una dirección MAC, que es asignada por el fabricante y se supone que por esto es única, y por esto es un dato útil para autenticar en la red.

Como se puede observar éste método es demasiado sencillo tomando en cuenta que la mayoría de los Access point de cualquier marca cuenta con ésta opción dentro de su firmware. Sin embargo, éste método es recomendable para redes pequeñas o caseras, ya que posee muchas desventajas para redes empresariales ya sean grandes o medianas.

⇒ Ya que si se cuenta con varios access point, cada vez que se desea autorizar o dar de alta o baja un equipo es necesario actualizar estas tablas de direcciones en todos los access point.

⇒ Como la edición de las tablas se lleva a cabo a “mano”, se debe tener extremo cuidado en dar los dígitos de la dirección MAC adecuadamente, ya que en caso de no darla adecuadamente el cliente deseado no se podrá autenticar.

⇒ Por lo general una dirección MAC, es fácil de obtener con algún sniffer en la red, ya que éstas viajan en claro, por lo que algún intruso pude obtener una dirección MAC de las máquinas autorizadas, y si bien ésta dirección es única si es posible cambiarla, empleando programas como **Air Jack** o **WellenReiter,** entre otros, también lo puede hacer por línea de comandos, así el atacante puede hacerse pasar por un usuario válido.

⇒ Lamentablemente, también se debe considerar el robo de uno de los equipos portátiles, por lo que en este caso el ladrón dispondrá de un equipo válido en la red.
⇒ Sin embargo no son sólo los equipos portátiles los que pueden ser robados, sino también los access point, lo que hace el problema de seguridad más serio, ya que un equipo de éstos, contiene la tabla de direcciones MAC de todos los equipos en validos en la red.

Igualmente se debe mencionar que si éste método no está combinado con un mecanismo de cifrado, no garantiza ninguna confidencialidad, y que debido a la facilidad para cambiar una dirección MAC, tampoco garantiza la autenticación. Aún peor, si se da el caso de un intruso que tenga el suficiente conocimiento para hacer un script o encuentre un programa para automatizar el cambio de direcciones MAC en poco tiempo y a su vez vaya pidiendo una dirección a los access point, de tal manera que cuando un cliente válido pida una IP para entrar en red, el access point ya no tenga IP, es decir, se da un ataque de denegación de servicios, entonces tampoco se puede garantizar la disponibilidad por éste método.

3.1.1.2 Uso de cifrado con llave WEP

El algoritmo WEP, es parte de la especificación 802.11. Este algoritmo se diseñó con el fin de proteger los datos de la conexión inalámbrica. Opera en la capa 2 del modelo OSI, y es soportado por la mayoría de los fabricantes.
Aparentemente este algoritmo resuelve el cifrado de datos en la red, sin embargo existen dos situaciones que hacen que no sea totalmente seguro en la manera que es empleado en la mayoría de las aplicaciones.
Casi todas las instalaciones emplean WEP con claves de cifrado estáticas, es decir es configurada una clave en el access point y nunca se cambia o muy extraña vez. Es decir un atacante que sniffee la red pueda acumular grandes cantidades de texto cifrado con la misma clave intente un ataque por fuerza bruta.
Además el vector de inicialización (IV) utilizado es una longitud muy corta, (24 bits) solamente es cuestión de tiempo para poder probar 2^{24} distintas posibles combinaciones. Así si el atacante logra conseguir dos tramas con vector de inicialización idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro e dichas tramas. Con el texto claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo, solo es necesario conocer el funcionamiento del algoritmo RC4, así entonces se puede obtener la clave secreta y descifrar toda la conversación.

Otra de las desventajas, es que no se ofrece el servicio de autenticación, es decir el cliente no puede autenticar a la red ni al contrario, solo es necesario que el equipo móvil y el access point compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Además en el mercado ya existen diferentes herramientas que pueden romper la llave secreta. Estas herramientas pueden ser gratuitas (la mayoría) y otras son con costo. El primer programa que hizo esto posible fue WEP Crack, que son una serie de scripts escritos en perl diseñados para analizar una serie de paquetes capturados por un sniffer.
AirSnort, es otra herramienta que hace lo mismo, rompe la clave WEP, pero también es un sniffer, además se debe mencionar que es muy fácil de usar, y contando, con que ella misma puede capturar el paquete que después analizará para romper la llave WEP.

3.1.1.3 Virtual Private Network VPN

Este tipo de redes emplea tecnología de cifrado para crear un canal virtual privado sobre una red de uso público. Son muy ideales para protección de redes inalámbricas ya que funcionan sobre cualquier dispositivo inalámbrico y superan muchas limitaciones que se presentan en el cifrado WEP. Para configurar una red wireless usando VPN's, se requiere que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, puede ser por el uso de la lista de control de acceso adecuada en un router, o agrupando todos los puertos de acceso inalámbrico en una VLAN, si es que son empleados dispositivos switchs. La lista de control de acceso o la VLAN, solo debe permitir el acceso del cliente inalámbrico a los servidores de autorización o autenticación de la VPN. También se debe permitir el acceso completo al cliente solo cuando haya sido debidamente autorizado y autenticado.

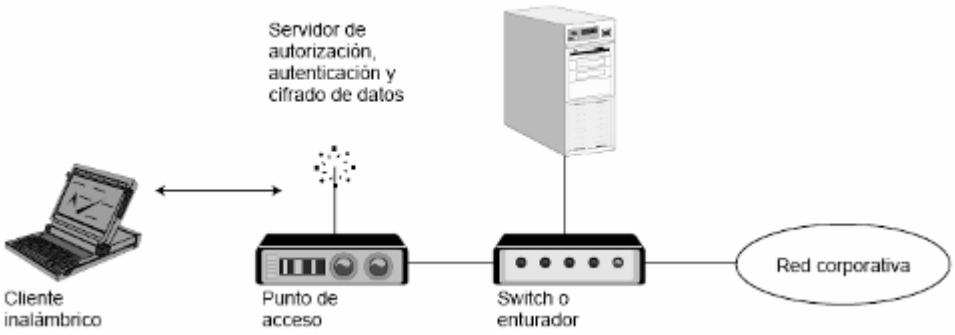


Imagen 3.2 Estructura de una VPN, para el acceso wireless seguro

En una VPN, existen servidores que se encargan de autenticar y autorizar a los clientes inalámbricos, de cifrar todo el tráfico que generen dichos clientes. Como los datos son cifrados en un nivel superior en la capa OSI, no es necesario ocupar WEP en este esquema.

3.1.1.4 Autenticación por medio del protocolo 802.1x

Este es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, el cual restringe la conexión de equipos no autorizados. Este protocolo fue creado por la IEEE para uso de redes convencionales. El problema es que este protocolo es compatible únicamente con los access point actuales, ya que los más antiguos no son compatibles.

Este protocolo involucra 3 participantes:

- El suplicante o equipo del cliente que desea conectarse a la red.
- El servidor de autorización/autenticación que contiene toda la información necesaria para saber cuales equipos y/o usuarios están autorizados para acceder a la red. Este protocolo fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación puede ser consultada en el RFC 2058. Inicialmente estos servidores fueron creados para autenticar usuarios de accesos remotos por conexión vía telefónica, sin embargo por su buen desempeño también comenzaron a ser usados para la autenticación de las redes LAN.
- El autenticador, que es el equipo de red (switch, router o servidor de acceso remoto), el cual recibe la conexión del suplicante y el servidor de autenticación y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

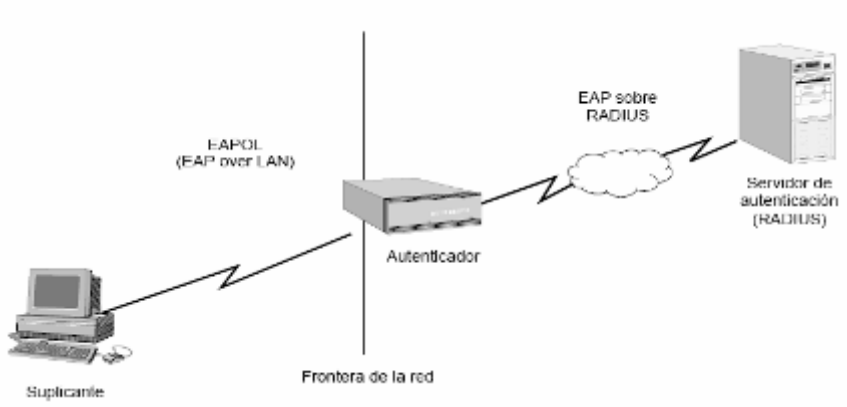


Imagen. 3.3 Sistema de autenticación 802.1x

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio de RADIUS de la siguiente manera:

1. El proceso inicia cuando el equipo se enciende y activa su interfaz de red y trata de hacer contacto con un access point, en ese momento la interfaz de red tiene el acceso bloqueado para tráfico normal y lo único que admite es el tráfico EAPOL (EAP or LAN), lo cual es requerido para llevar a cabo la autenticación.
2. La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea inicial el proceso de autenticación.
3. El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/Identity.
4. Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-ACCESS-Resquest al servidor de autenticación y le pasa los datos básicos de identificación del cliente.
5. El servidor de autenticación responde con un mensaje RADIUS-Access-Challenge, en le cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
6. El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.
7. Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión ala red.
8. El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

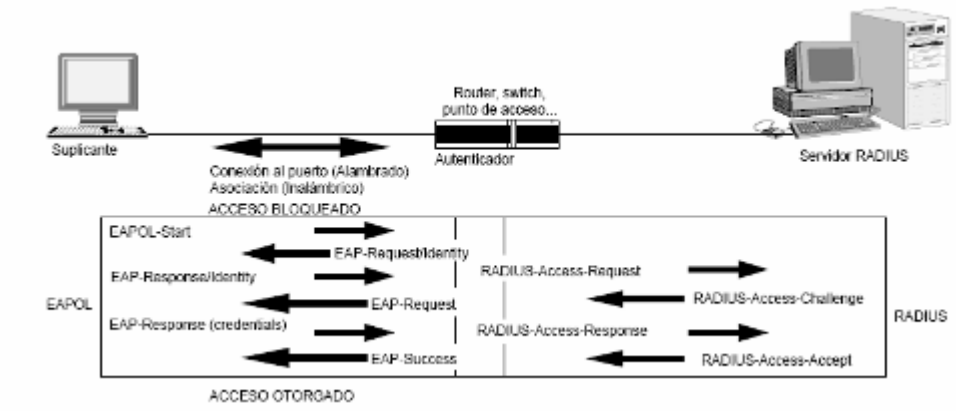


Imagen 3.4 Dialogo EAPOL-RADIUS

En el mensaje RADIUS-Access-Accept el servidor RADIUS, despacha también un juego de llaves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el access point. La ventaja de éste servicio, es que el servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo cada 5 min.), esto para evitar el ataque de rompimiento de llave mencionado anteriormente.

Existen varias variantes del protocolo EAP, básicamente se puede hablar de 2, las que emplean certificados de seguridad y las que utilizan contraseñas.
Las que emplean certificados de seguridad son:

a) 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 (transport Layer Substrate).
b) EAP-TTLS: Desarrollada por Funk software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente instalación de un certificado en el 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 como PAP, CHAP, MS-CHAP ó MS-CHAPv2.
c) PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos a EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

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

a) 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 certificadora (CA) conocida o montar una CA propia.
b) El diálogo de autenticación es largo lo que ocasiona que el proceso sea tardado, siendo especialmente molesto para los usuarios que tiene que autenticarse con mucha frecuencia (por ejemplo usuarios que constantemente cambien de access point)

c) La manipulación del certificado puede ser engorrosa para un usuario común. En muchos casos se elige instalar el certificado en la Terminal del usuario con lo cual, si la Terminal es robada 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, lo que obligaría a instalar el hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

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

b) LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de un nombre de usuario y contraseña, y soportar claves dinámicas WEP. Al ser una tecnología propietaria exige que todos los access point sean de marca Cisco y que el servidor RADIUS sea compatible con LEAP.
c) 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, aún con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servidor de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan pos ser un método de autenticación robusto y sencillo.

3.1.1.5 Autenticación por llaves WAP (WI-FI Protected Access)

Es un estándar propuesto por los miembros de la WI-FI Alliance (que reúne los grandes fabricantes de dispositivos WLAN) en colaboración con la IEEE. Con éste estándar se busca corregir los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporaly Key Integrity Protocol), el cual es el protocolo que se encarga de cambiar la clave compartida entre el Access point y el cliente cada cierto tiempo, para evitar ataques que permitan romper la clave. Igualmente, se mejoraron los algoritmos de cifrado de trama y de generación de los vectores de iniciación (IV's), con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP.
Dependiendo de la complejidad de la red, una access point puede operar con WPA en dos modalidades:

a) Modalidad de red empresarial: La cual requiere de la existencia de un servidor RADIUS en la red. El access point emplea el 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
b) Modalidad casera o PSK (Pre-Shared Key): En esta modalidad se trabaja cuando no se dispone de un servidor RADIUS en la red. Es entonces cuando es requerido introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al access point los dispositivos móviles cuya contraseña coincida con la del access point. 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), por que ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

La norma WPA data de abril de 2003 y desde entonces es obligatorio su uso para la alianza de WI-FI

3.1.1.6 Portal Captive (Portal cautivo)

Se trata de un mecanismo que proporciona autenticación, privacidad y cifrado. La autenticación que proporcionan es a través del WEB. Los usuarios deben contar con un nombre de usuario y contraseña, también se puede configurar para lograr la autenticación de dispositivos. La conexión entre el equipo y el servidor del portal cautivo es establecida de forma segura, se lleva a cabo usando el protocolo WEB seguro (HTTPS y SSL).
Su funcionamiento, es el siguiente:

a) El access point se comunica con el gateway

b) El gateway con el servidor de autenticación (Auth Server), que accede a la base de datos de usuarios.
c) Los mensajes de autorización se firman mediante PGP/GNUPGP
d) Una vez que está autenticado el gateway redirige el tráfico al exterior (LAN, Internet, etc)
e) Mantiene la sesión mientras el usuario está logueado

Este mecanismo, proporciona un mecanismo de QoS (Quality of Service), y a pesar de que el mecanismo ya era usado para redes alambradas, el uso tomó más importancia y utilidad para el caso de los "nodos libres", es decir, para las redes wireless.
Sin embargo, cuanta todavía con una serie de problemas, uno de ellos el más importante es que no resuelve el problema del spoofing

Dentro de las aplicaciones más conocidas y usadas se encuentran las siguientes:

Authpf OpenBSD

Es un sistema de autenticación proporcionado por el sistema operativo OpenBSD, el cual consiste en una serie de reglas que son usadas, dependiendo del perfil de cada usuario, si es que se establecen usuarios en la red. Esta basado en las credenciales que tiene que presentar cada usuario que desee tener acceso a la red.
Por las características del sistema operativo, se deduce que es gratuito, y de configuración variable, es decir, la configuración se puede adaptar a las necesidades, restricciones y criterio de cada administrador.
Las ventajas de usar este método de autenticación, es que aparte de ser un sistema de autenticación para el acceso a la red, también se pueden configurar reglas de uso de aplicaciones, puertos y servicios en la red, es decir es un firewall.
EL desarrollo, configuración e implantación de este sistema es relativamente sencillo cuando ya se tiene un poco de experiencia en el filtrado de paquetes del sistema operativo. Contrario a lo que pueda pensarse, esta sencillez no incluye un porcentaje bajo de seguridad, es decir, las fallas posibles en el uso de este sistema son bajas y no de alto riesgo.

Es una aplicación muy estable, gratuita, y va sobre un sistema operativo seguro, sin contar que es un sistema que soporta la mayoría de las aplicaciones que se proponen aquí.
Además Authpf, es un mecanismo de fácil implementación. Su forma de trabajo es la siguiente:

a) El cliente pide pasar por medio de la puerta de enlace, en este caso ese perfil lo tiene el servidor que tiene instalado el mecanismo.
b) El servidor solicita las credenciales del usuario, además de verificar algunos otros datos, como puede ser la MAC del usuario y si la petición es de un cliente válido. Esta validación se puede hacer en el AP, y de ahí se consulta al servidor que se tiene configurado, ya sea con éste mecanismo de seguridad o con otro como puede ser un servidor de RADIUS.
c) El cliente (en este caso el usuario), da las credenciales que tiene que obtener con anterioridad dando de alta a dicho usuario en la base de datos. Este servicio de alta de usuarios, se tiene que llevar a cabo de acuerdo con la base de datos de alumnos que maneja UNICA, ya que ellos tienen la base de datos de alumnos y profesores que tiene derecho al servicio y aquellos que lo han solicitado.

d) El servidor valida las credenciales del usuario y en caso de ser validas, le da acceso a su petición al DHCP discover, es decir pasa su solicitud de configuración de red al servidor DHCP.

NoCat Auth

Este es un sistema de validación de clientes para redes inalámbricas, que depende mucho del tipo de usuarios y del ancho de banda, así una vez que el usuario y el equipo se autentica, tendrá acceso a los servicios disponibles.

Es desarrollado por la comunidad Wireless de sonoma Country-Schuyler Erle, California (E.U.), con colaboración de de Seatle Wireless, Personal Telco, BAWUG, Houston WUG, además de grupos de todo el mundo.

Esta basado en autenticación segura con SSL (WEB). También es necesario un nombre de usuario y una contraseña para que el usuario pueda lograr la autenticación.
De las ventajas que se pueden encontrar, es que un mecanismo que informa de la salida y entrada del usuario en la red y añade implementación de QoS, por grupos o usuarios.
Otra ventaja muy impoprtante, es que puede ser usada como un Firewall entre el access point y el servidor de NoCat, el Firewall se lleva a cabo basado en el funcionamiento de IPtables, de hecho, este es uno de los requisitos que debe tener implementado el sistema donde sea instalada la aplicación.

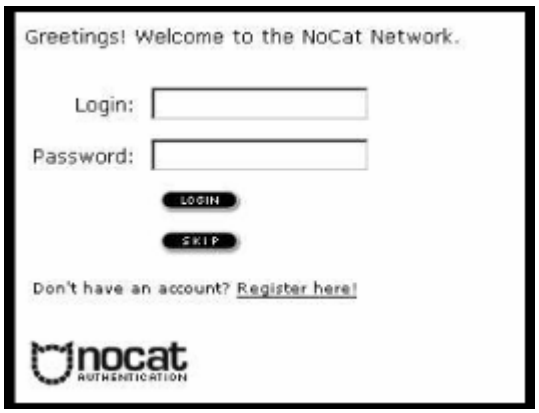


Imagen4.5. Pantalla de autenticación Web

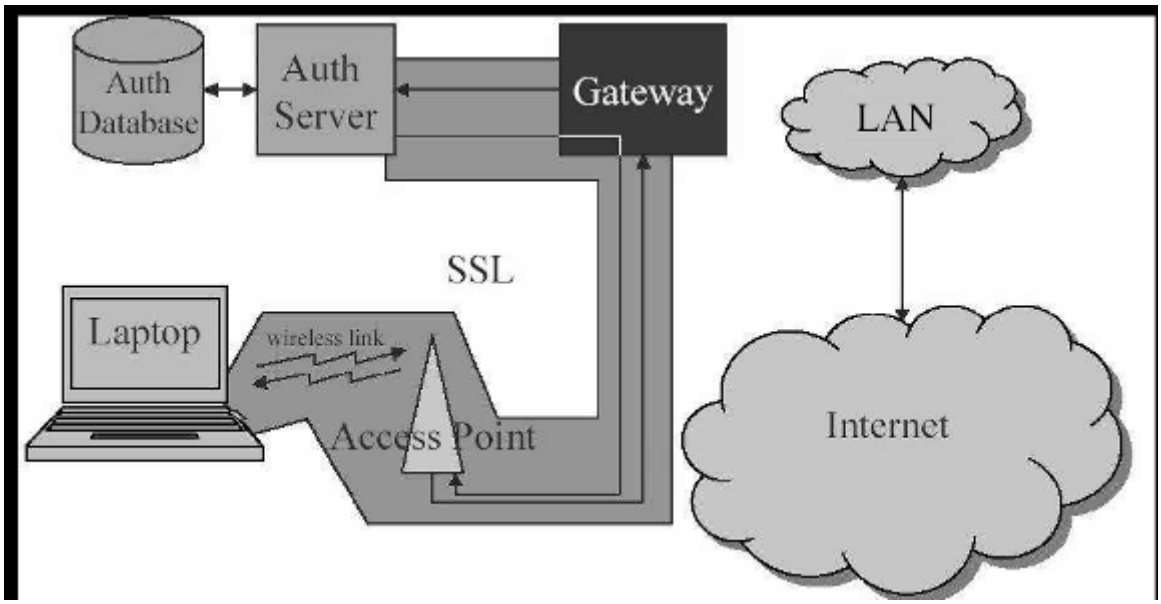


Imagen 3.6. Estructura de NoCat

Otra de sus ventajas es que la administración muy sencilla, el acceso para los usuarios es fácil y amigable, además que es de fácil uso, también es de fácil aprendizaje, es decir, basta con un solo uso, para que usuarios comunes, aprendan su funcionamiento. Y lo más importante, es que es una solución efectiva y a bajo costo, ya que se implementa sobre un sistema operativo libre, y además es accesible, por que se puede modificar según sus necesidades.

Entre las desventajas se puede encontrar, que sino está bien configurado, la comunicación es no cifrada por defecto, se tiene que implementar una VPN, por lo que el cliente necesita software específico, además como ya se mencionó no frena el problema de Spoofing.

De entre las necesidades que se presentan en los clientes son:

a) Contar con un navegador WEB (Mozilla, Netscape, Opera, Galeon, Internet Explorer, Konqueror).
b) El sistema operativo es independiente
c) No son necesario Plugins

d) Obviamente es necesaria su tarjeta wireless, y su cuenta de acceso al portal.

3.1.1.7 Sistema Abierto (OSA)

Open system authentication es el protocolo de autenticación por defecto para 802.11b. Como su nombre indica, este método autentica a cualquier cliente que pide ser autenticado. Es un proceso de autenticación NULO, las tramas se mandan en texto plano aunque esté activado el cifrado WEP.

3.1.2 Sistemas Detectores de Intrusos

Es fundamental contar con un dispositivo que ayude a controlar e identificar los posibles ataques o intrusiones que se presenten en la red. Aún es más importante poder llevar un control y estadísticas del tipo de tráfico que lleva nuestra red, ya que en un incidente de seguridad puede ser de mucha utilidad tener este tipo de información que ayude a cercar el área afectada. Es por esto que para un administrador es recomendable contar con un Sistema Detector de Intrusos (SID, por sus siglas en inglés), y de igual forma existen diferentes soluciones para este aspecto, ya sea gratuitas o con costo.

Es importante indicar que hay herramientas que son de doble uso, o como se les llama habitualmente, son un arma de dos filos, ya que son herramientas que como administrador te ayudan a conocer tu red y el nivel de seguridad que tienes en ella y por el otro lado son herramientas que mal usadas pueden dar un nivel alto de información sobre nuestra red, es decir son herramientas usadas normalmente por intrusos para el reconocimiento o incluso ataque a la red en cuestión. Sin embargo se debe considerar que siempre es mejor tener el conocimiento de dichas herramientas, ejecutarlas y usarlas en la red que se quiere administrar, ya que es mejor que seas tu a que sea cualquier intruso.

3.1.2.1 AirSnort

Es una herramienta gratuita y libre a la cual puede tener acceso descargándola de Internet. Es una herramienta fácil de configurar, y mucho más fácil de usar. **AirSnort,** que es muy conocido por que también cuenta con sistemas detectores de intrusos (SID) para redes convencionales. En especial esta herramienta para redes

inalámbricas es muy interesante, ya que cuenta con una herramienta para romper la llave de seguridad de la red (**AirCrack**)

En varios liveCD's (Distribuciones ligeras de Linux), ya viene configurado, así que solo es necesario acceder al conjunto de herramientas correspondiente a las redes inalámbricas, cuestión que hace más fácil la ejecución de las herramientas, lo verdaderamente preocupante, es que si se hace un mal uso de esta herramienta, se convierte en un excelente sniffer de la red, lo cual en manos de un intruso es peligroso.
Así también nos encontramos con una serie de herramientas UNIX, que por supuesto son de licencia libre y gratis. Muchas otras ya se encuentran incluidas y configuradas en liveCD's, lo que hace más fácil la ejecución de alguna herramienta que pueda vulnerar la red. Si bien para llevar a cabo la ejecución de éstas herramientas es necesario contar con una interfaz de red que sea reconocida en Linux, como son las interfaces de la marca ORINOCO, que son conocidas precisamente por ese aspecto, por que son las más útiles para correr este tipo de herramientas.

Imagen 3.7. Interfaz de LiveCD de Whoppix

En esta versión de live CD, viene una sección en las herramientas solo para redes wireless y para dispositivos bluetooth. Para acceder a estas herramientas, simplemente en el menú principal, en la sección Whoppix Tools, Wireless o bluetooth, dependiendo de lo que se desee. Pero para este caso lo que interesa es hacer una demostración de las diferentes herramientas con que cuenta.
Lo importante de estas herramientas es que como ya se había mencionado ya están configuradas, por lo que solo es necesario meter el CD, y bootear la máquina, y que tenga una tarjeta inalámbrica que sea reconocida por el sistema operativo.

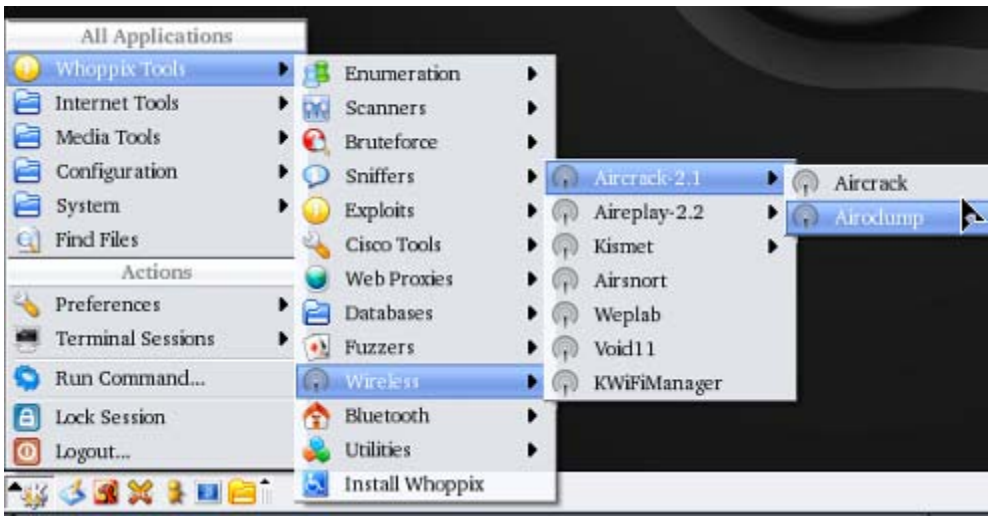


Imagen 3.8 Menú de herramientas Wireless en Whoppix

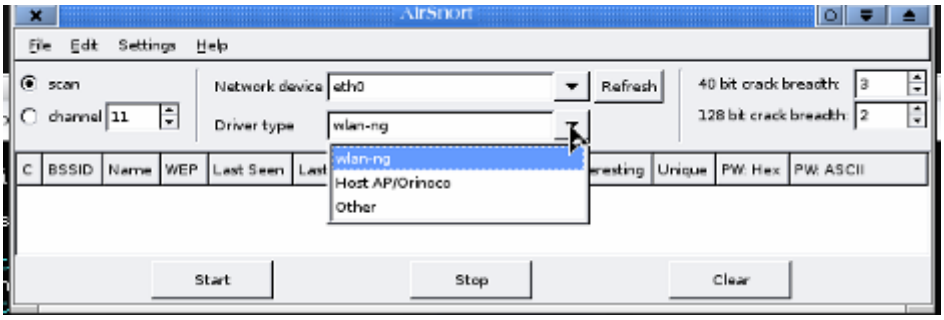


Imagen. 3.9 Interfaz de Airsnort

Para los sistemas operativos Windows, también existen varios programas que son SID's, lamentablemente la mayoría son de software propietario, y muy costoso, otros más se pueden implementar en los dispositivos de red ethernet (switches, routers) y algunos son parte del firmware de los access point, sin embargo no es recomendable configurar únicamente estos sistemas.

3.1.2.2 AirShang

Es un Sistema Detector de Intrusos, el cual funciona en sistemas operativos Linux, es desarrollado para el monitoreo de redes wireless principalmente, se basa en el monitoreo de direcciones MAC, lo cual no es muy bueno, ni da una seguridad de que el monitoreo que se lleva a cabo es el adecuado.

3.1.2.3 WIDZ

Es un IDS, que funciona bajo un sistema operativo Linux, y en sus ultimas versiones, ya es capaz de detectar access point falsos, Monkey-Jacks, Flouds entre otros e incorpora una "MAC Black-List" es uno de los más completos ya que no basa su funcionamiento solo en las direcciones MAC.

Existe otra herramienta muy parecida, llamada **WIDS,** la cual no implementa todas las opciones y facilidades que da WIDZ, sin embargo, respecto a otras herramientas, es muy fiable y realmente útil.

La herramienta comercial llamada **AIrDefense**, no es gratis, es una de las herramientas comerciales más conocidas, entre sus opciones más útiles se pueden encontrar dentro de las opciones de WIDZ.

3.1.3 Firewalls

Este es un dispositivo que se ha hecho fundamental en el control del tráfico permitido en una red. Para el caso de una red wireless, es uno de los dispositivos más importantes, ya que como no se puede controlar el acceso físico y las máquinas que forman parte de la red, no son máquinas que están a cargo del administrador así que no se tiene un estricto control del software y aplicaciones que se manejan en cada máquina.

De los diferentes firewalls que se pueden encontrar, son gratuitos, con costo, que se implantan mediante software o mediante hardware.

Gratuitos, son los que se implantan en sistemas operativos, gratuitos, como pueden ser:

- **IPtables**, de alguna distribución de Linux, este firewall está basado en reglas, que se activan en las diferentes tarjetas de red, es decir también está basado en el filtrado de paquetes.

- **Packet Filter, firewall** de openBSD, basado en el filtrado de paquetes, el cual tiene la característica de ser muy estable y eficiente, es de implementación sencilla y para actualizar o hacer una nueva configuración no es necesario un intervalo largo de tiempo.

En el caso de los firewall con costo, a nivel de software, se pude encontrar el **ISA Server,** de Windows Microsoft, por supuesto, se tiene que comprar licencia y su configuración no entra en la definición de sencillo. Es decir, es laboriosa y se tiene que cumplir con ciertos requisitos de hardware y software extra.

De los firewalls que se pueden encontrar a nivel de hardware, están los diferentes dispositivos o configuraciones que se realizan en los dispositivos de red. Estos servicios se presentan en switches, routers, o access point de las principales marcas de dispositivos de red, por

lo que su costo, configuración y eficiencia, depende de cada marca.

3.1.4 Sistemas de Monitoreo

Es necesario contar con un sistema que pueda informar del estado de la red, es decir, tener estadísticas e información real del comportamiento del tráfico a diferentes horas del día durante los diferentes días.
Es decir, es necesario contar con un sistema que ayude a monitorear, esto es útil en 2 diferentes puntos de vista, el primero es para obtener información sobre el desempeño de la red y el segundo es para obtener información sobre la seguridad de la red.

En cuanto al desempeño de la red, se puede hacer uso de diferentes herramientas, sin embargo la mayoría de ellas hacen uso del protocolo SNMP, que no es muy seguro, por eso al implantar un sistema basado en éste protocolo hay que tener mucho cuidado de configurarlo adecuadamente y no dejar el uso público que tiene por defecto. Muchas de estas herramientas se pueden configurar directamente en los dispositivos de red, por lo que dependen de cada fabricante y de cada modelo del dispositivo.

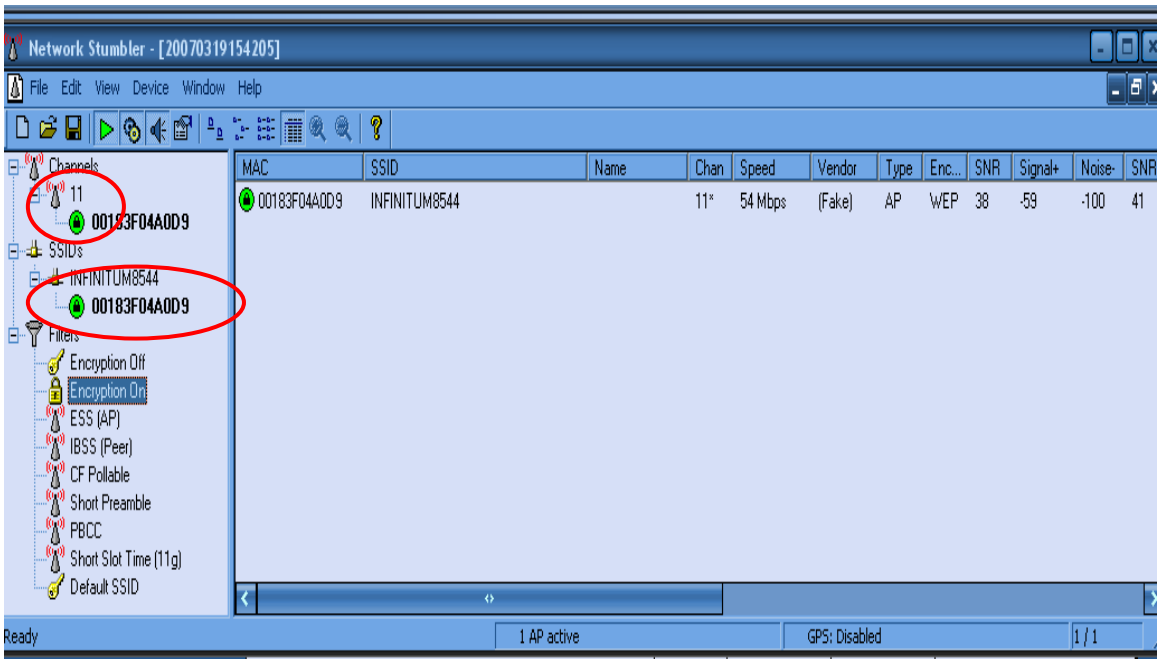
En el aspecto de la seguridad, se cuenta con herramientas, que del mismo modo que en el caso de los IDS se pueden obtener en LiveCD's, que son gratis e incluso, en caso de configurarlos en el sistema operativo, son sencillos de configurar.

- **Kismet.** El cual con ayuda de un dispositivo GPS (Global Position System), puede dar la información precisa de donde se localiza un access point, el SSID de la red y el alcance de dicha red. Su interfaz, es te texto, pero es amigable y de fácil entendimiento. Para su mejor funcionamiento, y obtener mejores resultados, es necesario contar con un GPS. La interfaz cuenta con muchas opciones. Hay aplicaciones extras que deben ser instaladas como **festival**, y el demonio de **GPS**d, por que este software trabaja en Linux. Una vez que se tengan estas aplicaciones instaladas, cualquier red que entre en nuestra cobertura lanzará un aviso hablado a través de kismet, indicando su nombre SSID, el canal en que opera y si esta abierto o cifrado. Unos segundos después de ser localizado, será visible en el mapa GPS

- **Airdump.** Es de la familia Snort, y es capaz de captura gran cantidad de tráfico, cuenta con una interfaz gráfica que hace su manejo más fácil. La herramienta más específica para esta tarea, es llamada AIRTRAF, ya que no solo permite

el monitoreo del tráfico, sino también permite la selección de un access point para su monitoreo específico.

Para el sistema operativo Windows, también existen herramientas para obtener la llave WEP y hacer un sniffeo de la red. A continuación se da un ejemplo del sniffer **Network Stumbler**:



3.10 Pantalla de Network Stumbler

Como se puede observar, esta herramienta da cosas tan básicas como el canal de frecuencia que tiene configurada la red inalámbrica, el SSID, y dependiendo de la información que nos interese específicamente de esa red que se va a monitorear son los filtros que se le pueden configurar.

- **Dsniff** demuestra lo inseguras que son algunas redes, sobretodo si nos empeñamos en enviar contraseñas en formato texto plano. Con este sniffer, nos daremos cuenta de los realmente importante que puede llegar a ser el uso del cifrado en nuestras comunicaciones diarias.

No sobra decir que un intruso con toda esta información, primeramente está atentando contra la confidencialidad de los usuarios.

Existen analizadores de tráfico como TCPDUM, IPTRAF, ETHEREAL, sin embargo, son analizadores que funcionan adecuadamente en redes alambradas, sin embargo, para este tipo de tráfico que se general en las redes wireless, solo ETHEREAL, es bastante práctico,

ya que si reconoce éste tráfico, y puede diferenciar entre diferentes protocolos como WEP y WAP.

3.1.5 Sistemas de cifrado

Con este servicio activado en una red, se busca que si la red es monitoreada o escuchada por intrusos de manera pasiva, los datos y la información que viajan por ella no sean vistos o cuando menos, no sea tan fácil obtener información que viaja por la red.
Este aspecto esta muy ligado con el sistema de autenticación que se use, ya que es necesario, por que los usuarios que entren en la red establezcan una comunicación cifrada con el Access point, y a su vez, el access point, poder establecer una comunicación segura con sus clientes.

Para lograr esta comunicación segura, se puede establecer un sistema de llaves con WEP, WPA, una VPN o intercambio de certificados, esta elección depende de las necesidades que se tengan en la red y del criterio del administrador.

Se debe tomar en cuenta también el nivel de seguridad que cada método puede proporcionar, ya que lamentablemente se puede hablar de una evolución rápida para romper llaves, y no se puede hablar de una evolución considerable del nivel de seguridad que se puede implementar en esta tecnología.
De igual manera, las herramientas que ayudan a obtener las llaves WEP, son libres y gratuitas, y en muchas distribuciones ya están configuradas, para que el usuario, solo las ejecute para obtenerlas, es el caso de WEP crack, la herramienta más popular y eficaz para lograrlo.

3.2 Elementos de Seguridad

Como administrador es importante tener un amplio conocimiento de los ataques existentes y de las herramientas tanto de administración como de ataques, o de las herramientas consideradas de doble filo. Hay que recordar que es mejor correr las herramientas en la red, y conocer la información que arrojan y las vulnerabilidades que se tienen, es importante, tener en cuenta que como administrador se tienen que tapar todos los hoyos de seguridad posibles, ya que los intrusos solo necesitan una puerta trasera para entrar.

3.2.1 Estrategias de seguridad

Para llevar a cabo un análisis profundo de los puntos vulnerables y hoyos de seguridad, se debe establecer una estrategia. Así en la

actualidad se conocen varios esquemas, que si bien, en los años anteriores se había usado por separado, en la actualidad, se propone el uso combinado y complementario de estos.

Defensa a fondo

Esta estrategia, trata de la redundancia en la seguridad. Se deben instalar varias herramientas, que a su vez sean complementarias entre sí, asegurando que alguien rompe una de las barreras de seguridad, exista otra que detenga al intruso, así la intrusión ser hará más difícil, tardada y hasta costosa para el intruso. Así de las herramientas ya mencionadas, podemos hablar no solo de sistemas detectores de intrusos a nivel de red, sino a de sistemas detectores de intrusos a nivel de host, de igual manera para los firewalls, se puede tener uno a nivel de red, y en diferentes instancias de toda la infraestructura de red, así también hacer la recomendación de que en cada equipo se instale un firewall personal, así también inculcar la cultura de la seguridad en los usuarios, con lo que el nivel del seguridad, ya no sería de red y de host, sino también a nivel de interfaz humana. Sin embargo por la implementación de este tipo de esquemas, no quiere decir que el sistema ya está seguro y no cuidar otros aspectos.
Se tiene que hacer notar la necesidad de bloquear todos los servicios y puertos que no se utilicen, establecer bien y específicamente los roes de cada equipo en la red, para que cerrar todos lo servicio que son exclusivos de ciertos servidores en la red, y no dejar esos servicios para equipos de usuarios.

Estrategia del menos privilegio

Este es un principio básico de la seguridad, no importa si es referente a la seguridad informática, es referente a la seguridad en general. Ya que en cualquier aspecto que se quiera resguardar, es importante mantener a los usuarios con el menos privilegio, y solo puedan hacer lo que estén destinados a hacer con el sistema. Ya en informática, es referente a permitir al usuario la ejecución de herramientas necesarias para realizar su trabajo y darle acceso a los programas y aplicaciones que necesita.

Cuando se instala un sistema operativo por defecto, es altamente inseguro, ya que dependiendo del sistema que se trate, tiene servicios y puertos abiertos que son innecesarios. Por ejemplo al instalar alguna distribución de Linux, y elegimos el escritorio de usuario con todas las aplicaciones que se pueden instalar por defecto, es entonces, cuando se abre el puerto de servicio de impresión, el servicio de archivos compartidos, así mismo se instala el software necesario para crear un servidor de correo, WEB o algún

otro, de tal forma que el usuario no sabe los servicios que tiene, así se dejan todas las puertas abiertas.
Del mismo modo en otros sistemas operativos, se instalan servicios innecesarios, como el servidor WEB de Windows, que es corregido hasta su versión Server 2003, pero todas las anteriores lo tienen activado. Si bien es cierto y algunos desarrolladores ya están trabajando para entregar una distribución cerrada y segura, sistemas como OpenBSD, en versiones anteriores ya no corren servicios innecesarios.
Para el caso de Windows es hasta la versión de servidor 2003 cuando podemos hablar de un sistema operativo con el menor privilegio.

Estrategia del Punto de ahogo

Se basa en tener un cuello de botella, en el cual se pude analizar todo lo que entra y sale de la red. Así es posible monitorear y bloquear todo aquello que no se desea que pase. Es decir, todo el tráfico de red tanto de entrada como de salida, pase por una máquina que haga la función de firewall, y que sea en ésta máquina donde se haga el filtrado de paquetes. Esta estrategia es muy efectiva cuando el administrador de la red conoce perfectamente toda la estructura de su red, y asegurar que no exista ningún otro acceso a Internet por el que el filtrado se haga inútil.
Este esquema puede variar y analizar dividiendo toda la infraestructura de la red en pequeñas redes para no saturar ni alentar el tráfico de la red.

Estrategia del eslabón más débil

Más que una estrategia, se trata de un principio fundamental en la seguridad, que es referente a que "*una cadena es tan fuerte como su eslabón más débil*". Como administradores, es necesario conocer cuales son los puntos débiles del sistema o red, para así tratar de eliminarlos y cuidar los puntos que se sabe son los más atractivos para los atacantes.
Así se pueden hacer simulacros de ataques y poder contar con un esquema o plan de contingencia en caso de presentarse una situación de emergencia de seguridad o de caída de servicios.

Estrategia de falla segura

Se trata de otra estrategia basada en un principio fundamental de seguridad, que es el pensar en la existencia de una falla, y las acciones a tomar cuando el sistema se encuentre en este estado, así también que acciones automáticas debe tomar el sistema. Esta

estrategia va de la mano con la estrategia anterior, ya que es recomendable primero localizar los puntos débiles, luego planear el plan de contingencia y finalmente aplicar las acciones correspondientes del plan de contingencia, se tienen que llevar a cabo simulacros para poner a prueba el plan y las acciones.
Es importante tener en cuenta que estos planes no son estáticos y que hay que estar actualizandolos, ya que así de rápido como cambian las cosas en el mundo informático, se debe tener actualizado el sistema operativo de los servidores y firmware de los dispositivos de red, también se debe tener actualizado el plan con respecto a los nuevos ataques, amenazas, gusanos, virus y todo tipo de malware que se presente.

Estrategia de Simplicidad

La premisa de que manteniendo las cosas simples son más fáciles de entender, en la seguridad es muy cierta e importante, ya que sino se entiende algo, no se puede considerar seguro, por que no se puede planear alguna reacción frente a determinada situación, por que simplemente no se entiende. Se debe tomar en cuenta que si algo es complejo, se puede encubrir u ocultar muchas situaciones, vulnerabilidades y amenazas del sistema, que por no entender o considerar existen y son constantemente los puntos que más atacan.
Existe una consideración de seguridad que dice que mientras más parchado esté un sistema es más seguro, sin embargo por deducción, es mejor tener algo robusto desde el principio, por que todo su comportamiento es homogéneo, y no tienes un parche que a su vez puede tener o esconder más amenazas y vulnerabilidades.

Estrategia de seguridad por oscuridad

Esta estrategia está basada en proteger las cosas ocultándolas. Para el caso de redes y sistemas de cómputo, a lo que se refiere, es contar con sistemas de seguridad que se guarden como secreto, y que las personas encargadas de estos sistemas tengan total discreción y no comenten si es posible la existencia de dichos sistemas de seguridad. Es decir suponer que los sistemas no serán atacados por el hecho de que la gente no sepa su existencia.

En mi particular punto de vista, esta estrategia no es útil ni buena, no creo que sea bueno suponer que no habrá intentos de ataques ni fallas, solo por que los demás, no sepan explícitamente que los dispositivos existen, ya que por las herramientas mencionadas anteriormente, y algunos ataques que es posible hacer, se puede identificar la existencia de ciertos dispositivos en la red. Ahora, no

digo que se tenga que publicar la estructura y los componentes de la red, sin embargo, si se debe considerar que por alguna manera personas ajenas al grupo de administradores y/o seguridad tengan conocimiento de la existencia de los dispositivos. Para mi es mejor, estar preparado para una posible emergencia de seguridad y considerar alguna falla en el dispositivo, para así tomar en cuenta las acciones necesarias en un plan de contingencia.

Estrategia de participación universal

Se basa en la participación de todos lo usuarios, es una parte sumamente importante en el aspecto de seguridad. Ya que son los usuarios el monitor más importante del sistema de seguridad que implemente, así, de que serviría una estructura altamente robusta y bien configurada cuando contamos con usuarios, que no tienen la cultura de seguridad informática. Es decir, se cuenta con usuarios, que no usan un password fuerte, que no tienen la precaución de guardarlo o memorizarlo, que prestan su password a personas no autorizadas o mal intencionadas.

Ahora, esta participación en el ámbito de la Facultad de Ingeniería, puede sonar difícil de controlar o de llevar a todos los usuarios de la red. Pero hay que tomar en cuenta que esta participación puede ser de forma obligada o voluntaria.

La forma voluntaria, incluye pláticas informativas, conferencias, cursos, carteles y acciones que sean necesarias para la información y capacitación de los usuarios, con el fin de crear una conciencia de la seguridad y la prevención que deben tomar con sus propios equipos e información que manejan a través de la red.

La forma obligatoria, tiene que ver con las políticas de seguridad que están establecidas y aprobadas por las autoridades de la Facultad, por lo que cualquier violación tiene su sanción correspondiente y que también es aprobada por las autoridades de la Facultad.

La recomendación es contar con una combinación balanceada de ambos casos, es decir, dar recomendaciones de las acciones que deben llevar a cabo y establecer los procedimientos necesarios para lograr al máximo el cumplimiento de las políticas y las sanciones adecuadas para cada falta que se presente.

Como administradores, es necesario tener en cuenta que lo más importante del trabajo llevado a cabo es la satisfacción de los usuarios, por los servicios que se están prestando, y que la mayor amenaza que puede existir es un usuario válido en la red, que no este de acuerdo con los servicios o con las políticas establecidas, así el usuario puede llevar a cabo acciones que evadan las políticas y que afecten a los demás usuarios en la red, la situación se puede volver aún peor considerando que ningún usuario reporte una anomalía o comportamiento extraño en la red como

consecuencia de las acciones del usuario en cuestión. Por eso es mejor considerar que los usuarios son informantes de ese tipo de situaciones y que están alertas y saben identificar una situación no común en el estado del sistema o red.

3.2.2 Posibles ataques

Las amenazas a las que puede estar expuesta una red son muchísimas, sin embargo para el caso de la tecnología inalámbrica, los ataques que se pueden presentar son muchos y muy diversos, sin embargo entre los más comunes y conocidos, se encuentran los mencionados abajo. No se puede dejar de mencionar que las herramientas de escaneo, mapeo, monitoreo y hasta el propio firewall puede ser un escalón o avance importante en las fases que un intruso lleva a cabo para atacar un sistema, así este tipo de software con una mala configuración puede establecer un reconocimiento muy completo del sistema. Una puerta trasera que sea explotable, un hoyo de seguridad por donde se pueda mantener el acceso al sistema.

3.2.2.1 Wardriving

El **wardriving,** propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en la Internet.

Imagen 3.11 Componentes necesarios para el Wardriving

Wardriving. A la izquierda puede observarse el equipo necesario (computadora, GPS y antena); a la derecha, los triángulos indican sobre el mapa la posición de redes inalámbricas.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que las computadoras que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichos equipos, instalarles software maligno o dañar la información.

3.2.2.2 Warchalking

El **warchalking,** que consiste en caminar por la calle con una computadora portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

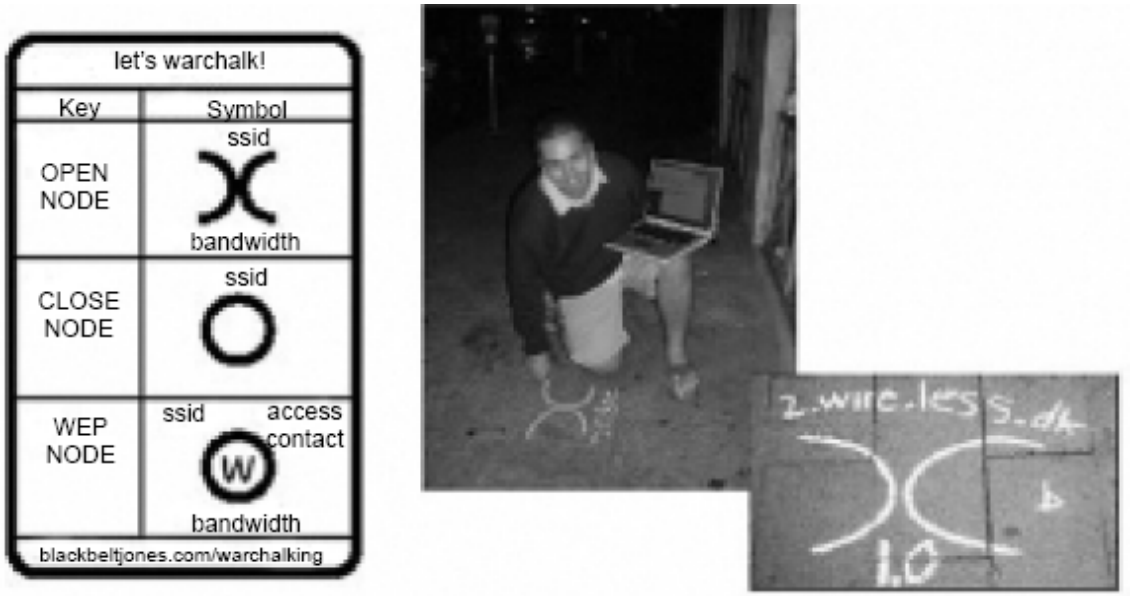


Imagen 4.12 Simbología usada en el warchalking

Ataques WAR. (Wardriving, Warchalking, Wardialing)

La palabra wardriving deriva de wardialing , el wardialing consiste en usar un módem para llamar a una lista de teléfonos para averiguar si poseen un módem , un PBX, o similar, esta técnica la podemos ver en la película Juegos de Guerra, wardriving vendría a ser lo mismo una técnica usada para encontrar puntos de acceso

wireless, pero en este caso en vez de usar una lista de teléfonos lo que usaremos será un coche o cualquier otro vehiculo para podernos mover buscando puntos de acceso, existen herramientas como Netstubler para Windows , Kismet para GNU/Linux *BSD, DSTUMBLER *BSD,KISMAC MacOS X, con las cuales podemos colocar nuestro interfaz de red en modo radio y escanear en busca de BACON Frames.

Warchalking es de dudosa legalidad, consiste en marcar con tiza la pared del edificio donde existe el AP, con las características del mismo (WEP,DHCP,Internet).

3.2.2.3 Denegación de Servicios y Ataques de spoofing o Suplantación de identidad

En la parte de suplantación de identidad, también se cuenta con herramientas que facilitan mucho éste tipo de ataque, ya que el access point, por lo general se ayuda para autenticar de la dirección MAC de las tarjetas de red. Las características de ésta dirección es que viene del fabricante, que son de 12 dígitos hexadecimales y que los primero seis son para identificar al fabricante y los otros seis son de las tarjetas de red, por lo que se supone es una dirección única de cada tarjeta y se creía que no es posible cambiarla. Sin embargo esto ha cambiado, ya que en la actualidad ya hay herramientas y una serie de comandos par llevar a cabo el cambio de ésta dirección. El ataque consiste en pedir una dirección IP por cada dirección MAC que puede adquirir, por lo que el access point da una IP a un mismo equipo, y cuando un cliente valido le pide una dirección IP, para entrar tomar todos los servicios que se ofrecen en la red, ya no tiene direcciones, es decir este ataque es de tipo de denegación de servicios.
En base a dejar al verdadero DHCP, sin disponibilidad para las peticiones válidas, es entonces cuando se presenta un equipo atacante con los servicios que se tenían, y engañan a los clientes haciéndolos pensar que es la red original, por lo que toda información que el cliente quiera enviar será verdaderamente enviada al atacante.

3.2.2.4 Malware

La palabra malware es la combinación de palabras malicious y software, por lo que al referirnos a este tipo de software se abarca desde virus, gusanos, exploits, caballos de Troya, en fin, todo tipo de código que es capaz de alterar el funcionamiento “normal” u ordinario de los sistemas.

Así en una red inalámbrica, es muy común encontrar este tipo de software, ya que lamentablemente, no es fácil llevar el control físico de las máquinas que se conectan a dicha red. Lamentablemente, es un hecho que muchos usuarios no tienen el cuidado necesario para conectar un equipo a Internet, es decir, no cuentan con software necesario como un Antivirus, un firewall personal y antiSpyware. Tampoco se tiene la educación para no ejecutar cualquier código que llega o abrir correos electrónicos con identidad desconocida y descargar los archivos adjuntos, por lo que es muy fácil encontrarse con un equipo infectado.
Así una computadora infectada y que ya tenga la configuración necesaria para conectarse a la red, puede tener acceso e infectar a más equipos en ella. Además, como en una red de éste tipo se habla de equipos portátiles, que tienen la facilidad de conectarse a distintas redes, donde también puede contaminarse.

3.2.2.5 Rompimiento de llave WEP

Ya es muy conocido que el uso del cifrado WEP, para una red wireless, no es suficiente, ya que este tipo de cifrado ya tiene tiempo que fue vulnerado, las fallas que han encontrado a grandes rasgos son:

Los CRC's son independientes de la llave utilizada

MIC Independiente de la llave, esto es ausencia de mecanismo de chequeo de integridad del mensaje. Esta debilidad en el cifrado da lugar a que conocido el texto plano de un solo paquete cifrado con WEP sea posible inyectar paquetes a la red.

Tamaño de IV demasiado corto, El IV (Vector de inicialización) tiene 24 bits de longitud y viaja como texto plano. Un AP que opere con grandes volúmenes de tráfico comenzará a repetir este IV a partir de aproximadamente 5 horas. Esta repetición hace que matemáticamente se pueda operar para poder obtener el texto plano de mensajes con IV repetido (sin gran nivel de dificultad). El estándar especifica que el cambio de IV es opcional, siendo un valor que empieza con cero y se va incrementando en uno.

Reutilización de IV, se pueden hacer ataques "Estadísticos", ya que el vector de inicialización se repite frecuentemente. En las nuevas correcciones que se usan en 802.11i está subsanado.

Deficiencias en el método de autenticación Shared Key, se pueden presentar ataques pasivos. Si un atacante captura el segundo y tercer mensaje de administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el

mensaje cifrado con la clave compartida. Con estos datos, posee todos los elementos para autenticarse con éxito sin conocer la clave secreta compartido (Con esto sólo logra autenticarse, luego queda el acceso a la red).

Debilidades en el algoritmo llave RC4

Esto es el funcionamiento de programas como airsnort o wepcrack, El funcionamiento, es realmente complicado, sin embargo, es una de las formas mas rápidas para obtener la WEP.

3.2.2.6 Falsificación de AP (Gemelo maligno)

Es muy simple colocar una AP que difunda el mismo SSID, para permitir acceso a cualquiera que se conecte, si sobre el mismo se emplean técnicas de "Phishing", se puede inducir a creer que se está conectando a una red en concreto. Existen varios productos ya diseñados par falsificar AP, en la terminología Wi-Fi se los suelen llamar "Rogue AP" o Fake AP", el más común es un conocido srcipt en Perl denominado justamente "FakeAP", que envía Beacons con diferentes SSID y diferentes direcciones MAC con o sin empleo de WEP.

Además hay que recordar que ciertos sistemas operativos, seleccionan el access point de mejor señal, de más alta calidad y de menor ruido, para conectarse a un AP, lo que hace más fácil este ataque, ya que solo es necesaria una colocación más cercana del AP maligno a los dispositivos a los que interesa engañar.

3.2.2.7 Debilidad en WPA

También existen vulnerabilidades para este protocolo, ya que resulta que si las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Esta debilidad se resuelve aparentemente fácil, ya que solo se necesita establecer claves más largas, sin embargo, no es lo más difícil, sino, hacer la conciencia a los administradores y usuarios, en usar claves que no sean palabras de diccionario, ni fáciles de adivinar, ni cortas, sin embargo, a veces, el reto se vuelve que las personas que las usan las recuerden.

3.2.2.8 Conciencia y cultura de los Administradores

Básicamente en este punto, se trata de señalar la dura tarea que se tiene al ser administrador de una red, ya sea la de este caso, o la de cualquiera, el administrador, debe contar con el conocimiento y con la cultura de no dejar la configuración de fábrica, esto solo lo hace la gente a nivel doméstico (y no siempre), pues no es serio, dado que de todos es sabido que direcciones IP usan determinadas marcas, por no decir contraseñas, SSID, etc. Son datos mínimos que se deben personalizar en un dispositivo de red, para no ser blancos de una mala broma o de un ataque más serio por el hecho de la mala configuración de los dispositivos.

3.2.2.9 Ataque de fuerza bruta

Este ataque, aunque funciona, dado a las limitaciones de WEP (indicadas anteriormente), no es tan común, dado que es tardado, aproximadamente 3 meses en obtener la clave con un equipo no muy potente.

Una variante de este ataque es el **Ataque de diccionario,** se lleva a cabo igual que el anterior, pero más rápido, gracias a la utilización de diccionarios, es decir, el ataque lo realiza con ayuda de archivos, donde se establecen las posibles contraseñas o claves, se basa en estos archivos para hacer todo los intentos de adivinar.

3.2.2.10 Ataque Inductivo Arbaugh

Se basa en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC. EL funcionamiento es el que sigue:

Para realizar el ataque hay que conocer parte del texto plano que viaja cifrado en una trama, que se puede obtener por ejemplo identificando mensajes “DHCPDISCOVER”, de los que conocemos que la cabecera IP tendrá como origen 0.0.0.0 y como destino 255.255.255.255 y tienen longitud fija. Una vez identificada la trama con el mensaje “DHCPDISCOVER” se realiza una XOR del texto plano conocido con el texto cifrado que se ha recibido, obteniendo así 24 bytes del de la cadena clave, para el IV concreto del paquete. Lo siguiente será modificar el paquete, pero de forma engañosa, es decir, se debe meter en un ARP o un ping, para así obtener respuesta. Una vez lanzado, se obtiene respuesta, era el último byte del vector, en caso contrario se tendrá que probar con los 255 posibilidades restantes, modificando el último

byte, por lo que también, es un ataque que se hace pocas veces por su posible complejidad.

El atacante tiene que volver a generar un paquete del cual se le devuelva una respuesta, (lo mejor es enviar broadcast pings, así se recibe múltiples respuestas por cada paquete que enviamos). El atacante conoce el texto plano de la respuesta y el que responde cada vez enviará el paquete con un IV diferente, así es posible construir una tabla de cadenas llave completas para cada IV que el atacante puede utilizar para descifrar el tráfico cifrado con WEP en tiempo real. Decir que tendría que capturar, teóricamente unos 24GB .

3.2.2.11 Ataques a ACL's basados en MAC

Para llevar a cabo el ataque basta con monitorear durante un momento el tráfico y fijarnos en la MAC de cualquiera de los clientes, sólo hace falta cambiar a la tarjeta de red de la máquina misma MAC y ya se salta la restricción. Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC se pueden presentar problemas, aunque generalmente en las redes wireless esto no suele ser un problema muy grave ya que el access point no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas forma, si se puede "anular" (sacar de red) a la máquina que le hemos "robado" la dirección MAC. Para hacer esto, se debe implementar un ataque de Denegación de Servicio.

Ataque de Denegación de Servicio (DoS)

Para realizar este ataque basta con monitorear durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez se conoce su MAC, y se le pone esa dirección a la tarjeta de red de la máquina y se hace que actúe como si fuera el AP. Lo único que tenemos que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (management frames) de no asociación o no autenticación. Si esto se quiere hacer a todos los clientes de la WLAN, se mandan estas tramas a la dirección MAC de broadcast. Para esto se cuenta con herramientas como wlan-jack o dassoc (desarrollada por @stake), ambas de linux.

3.2.2.12 SSID ocultos

Aunque no es exactamente un ataque, muchos administradores usan SSID, ocultos, sin embargo, en las siguientes líneas se verá como se puede descubrir los AP´s ocultos:

Al estar oculto, significa que el AP no emite beacom, por tanto no sabemos el SSID, en este caso, para descubrir el SSID deberíamos monitorear y esperar a que un cliente se conectara, y se ve el SSID en la trama PROVE REQUEST del cliente (en el caso de que no se manden BEACON FRAMES), o en la trama PROVE RESPONSE del AP. Pero también se puede "provocar" la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de no asociación o de no autentificación en lugar de mandarlas repetidamente, es decir, se le pone la dirección física del AP a la máquina y se manda una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autentificarse, con lo que se puede ver el SSID en los management frames. Para este fin se puede usar una herramienta muy popular como es essid-jack, también para linux.

3.2.2.13 Ataque Man in the middle

También conocido como "Mono en medio", consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.

Para realizar este ataque, primero se debe monitorear para obtener:

- El ESSID de la red (si esta oculto).
- La dirección MAC del AP.
- La dirección MAC de la victima.

Una vez que se conocen estos datos, se utiliza para no autentificar a la víctima del AP real, es decir, el atacante spoofea su MAC haciéndose pasar por el AP y manda tramas DEAUTH a la victima. La tarjeta wireless de la victima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante. Ya que el atacante hace creer a la victima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la victima estaba autenticada

anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wireless del atacante debe estar en modo master.

Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la víctima. De esta manera se ha conseguido insertar al atacante entre la victima y el AP, en la siguiente imagen se ve como quedaría la WLAN después de realizar el ataque.

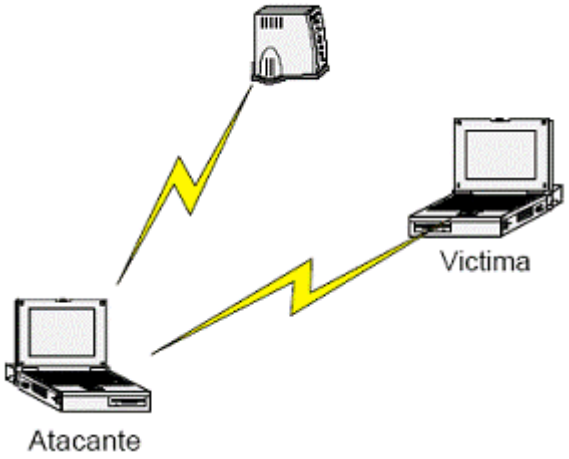


Imagen 3.13. Estructura del ataque Man in the middle

Es muy fácil implementar este tipo de ataques utilizando el driver air-jack con la herramienta monkey-jack.

3.2.2.14 Ataque ARP Poisoning

El ARP caché poisoning es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las victimas, limitando su efectividad a redes conectadas con switches (aunque curiosamente, no todos), hubs y bridges, pero no routers. La mayoría de los Puntos de Acceso 802.11b,g actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red wireless hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de ARP caché poisoning contra sistemas que están situados detrás del access point,por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN.

Ejemplo:

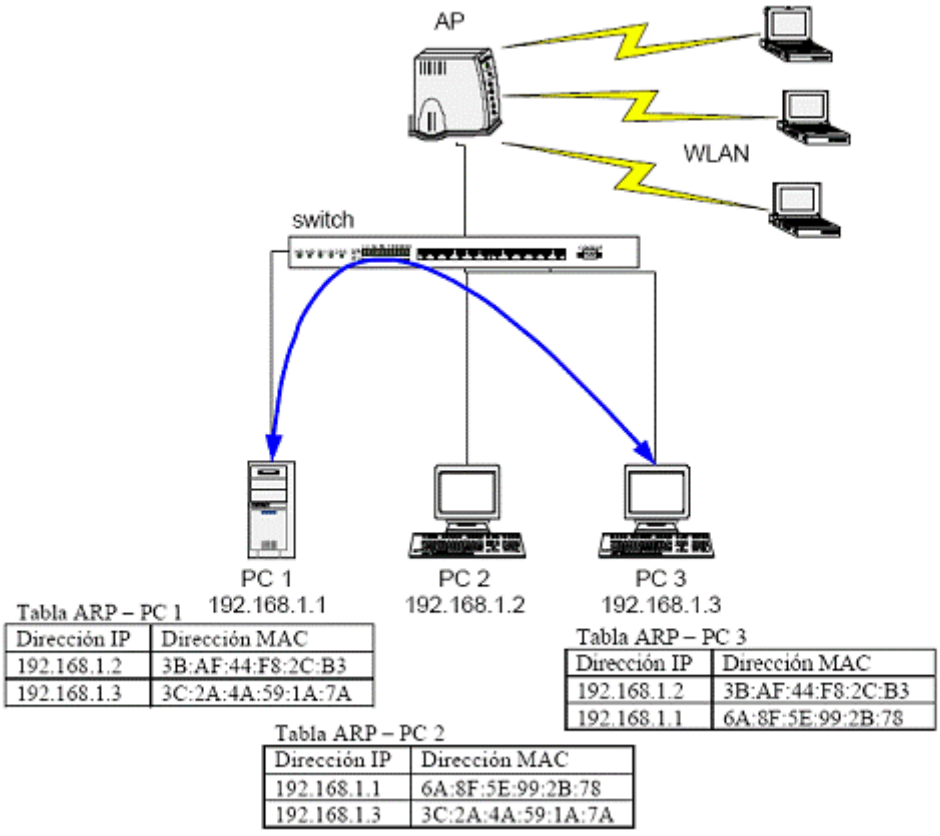


Imagen 3.14 Ejemplo de ARP Poisoning

El servidor PC 1 se comunica con PC 3 a través del switch, si un atacante desde la WLAN envenena la tabla de ARP's de PC 1 y de PC 3 podrá realizar un ataque del tipo "Man in the Middle" situándose entre los dos hosts de la red con cables.

Una vez realizado el ataque, se vería algo así:

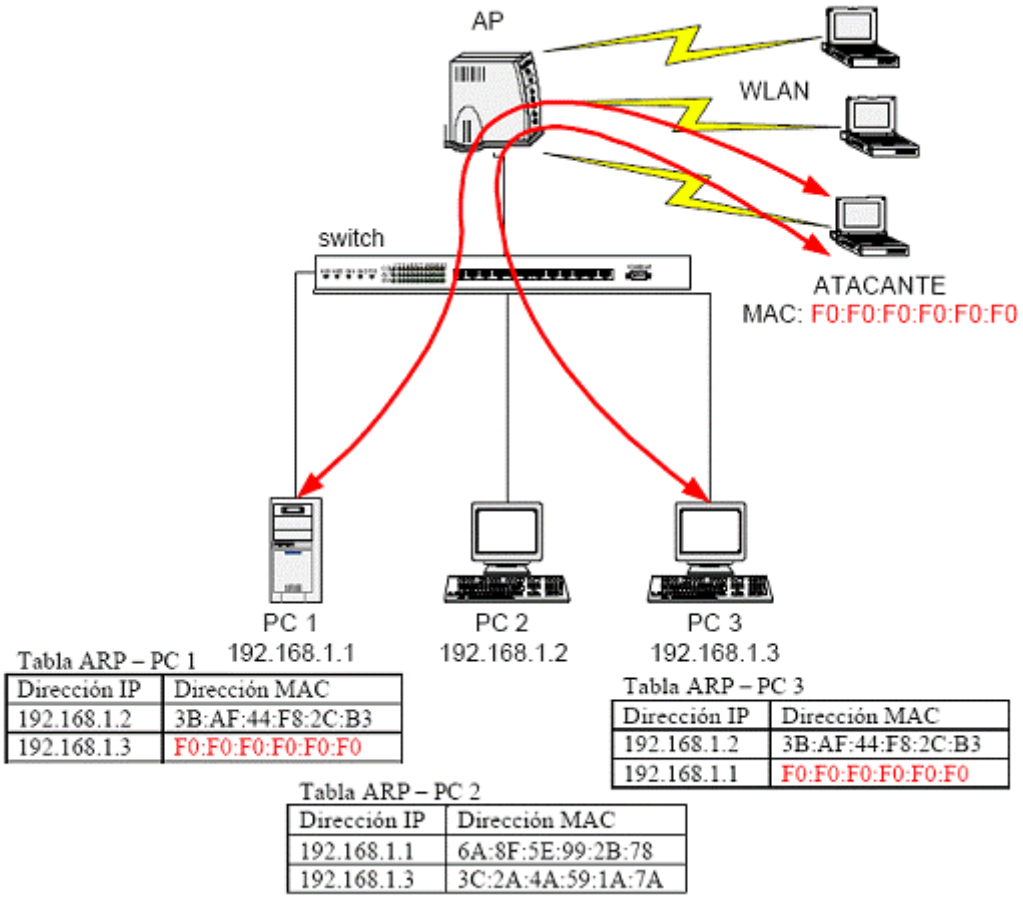


Imagen 3.15 Ejemplo de ARP Poisoning (2)

El atacante manda paquetes ARP REPLY a PC 2 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue "envenenar" la caché de ARP's de PC 2. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 2 la tiene también su propia MAC. Por como funciona el ARP, ambos pc´s actualizaran sus caches de acuerdo con la información inyectada, en este caso por el atacante. Como el switch y el AP forman parte del mismo dominio de broadcast, los paquetes ARP pasan de la red wireless a la red cableada sin ningún problema. Para realizar el ataque ARP Poisoning, existen múltiples herramientas, ya que este ataque no es específico de las redes wireless, la más famosa es el sniffer Ettercap (lo hace todo solo). Se puede frenar este ataque creando dos VLAN's en el switch, una para un puerto al que está conectado el AP y la otra para el resto de máquinas. Otra forma de frenarlo sería utilizando tablas de ARP estáticas (La solución mas rápida).

Existen más tipos de ataques que no se comentan aquí, dado que el principio de funcionamiento está basado en los detallados anteriormente.

CAPÍTULO 4

CASO:
RED WIRELESS EN LA FACULTAD DE INGENIERÍA

4. Caso: Propuesta de Red wireless en la Facultad de Ingeniería

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados y establecidos en un determinado lugar. Es decir, una red Wireless, permite montar toda una red con todas sus ventajas y ningún cable. Incluso hablando de una instalación temporal la tecnología wireless se vuelve una muy importante opción.

A continuación se observarán las necesidades y el por qué este trabajo de tesis, propone que se de un servicio de forma inalámbrica y para espacios abiertos de la Facultad de Ingeniería, es decir que se cuente con un servicio donde el usuario tenga solamente que darse de alta para indicar que va a usar el servicio y que pueda usarlo en cualquier lugar del edificio principal de la Facultad de Ingeniería. La problemática que representa llevar a cabo dar este servicio se dividirá en tres niveles: Nivel usuario, Nivel de administración de la red y Nivel de seguridad en la red.

4.1 Problemática a nivel de usuario

En la actualidad los alumnos en la Facultad de Ingeniería en el edificio principal, ya cuentan con un servicio de red inalámbrica, sin embargo, no es un servicio exclusivo de la Facultad, ya que se trata del servicio prestado por el proyecto RIU (Red Inalámbrica de la UNAM), el cual obviamente cubre bastantes necesidades de las que se tenían ya que antes los alumnos forzosamente tenían que acudir a las salas de cómputo donde se presta este servicio. A pesar de que el servicio prestado en estas salas es bueno, muchas veces no es suficiente y para aquellos que cuentan con una máquina portátil no hay servicio de red, ni siquiera convencional. La red inalámbrica propuesta es exclusiva para uso de los alumnos de la Facultad, ya sea para espacios abiertos, bibliotecas y auditorio. Claro el servicio propuesto debe contar con una interfaz para su fácil administración y por supuesto no dejar de lado el aspecto de la seguridad en la red, esto es asegurando que la red, va a ser disponible, integra y confiable. Además para la configuración de cada cliente considerando que la red es usada por todo tipo de usuarios, ya sean experimentados o no, la interfaz de usuario propuesta también debe ser de fácil manejo. También se debe recordar que los usuarios son la mejor forma de monitorear nuestros servicios, ya que son ellos los que nos dicen cuales son los servicios que les hace falta y esas son las necesidades que tiene que satisfacer la red.

4.1.1 Asignación de direcciones IP

Para tener acceso a la red y a Internet, los alumnos de la facultad de Ingeniería necesitan de una dirección IP. Sin embargo como es bien sabido la falta de direcciones IP, es el problema que se enfrenta hoy en día, a pesar de que existe la solución del protocolo IP versión 6 no todos los equipos tienen el software y/o hardware necesario para aguantar este protocolo por lo que se propone la solución de usar la traducción de direcciones IP para poder brindar el servicio a los alumnos de la Facultad.

Se está planteando el hecho de que los alumnos que cuenten con un equipo portátil puedan acceder a Internet, por lo que muy difícilmente se puede hablar de dar una dirección IP real a cada uno, además a nivel de administración de red se explicará como y por qué esta situación se debe y se puede evitar.

4.1.2 Prestación del servicio

Se debe contar con un estricto control de la asignación y tiempos de direcciones IP, ya que no se puede asignar una IP a un usuario y que cuente con el tiempo de acceso ilimitado, y consumir el ancho de banda que él desee, ya que no es una prestación justa del servicio, cuando en las salas de cómputo de la Facultad el control del servicio se lleva por tiempo, por lo que no se considera conveniente que los alumnos con equipo portátil deban contar con ésta conexión permanente, sin embargo, se debe mencionar que no se desea que cada que un usuario necesite conectarse, deba hacer toda la configuración, simplemente que se tenga que renovar la dirección IP cada cierto tiempo.
Debe considerarse si es necesaria la creación de perfiles de usuario ya que principalmente este servicio es para uso de los alumnos de la facultad, sin embargo como en las salas de cómputo, este servicio también es requerido por varios profesores y en estos casos el servicio es el mismo, sin ningún privilegio extra. Sin embargo para el caso en que los profesores usen su equipo portátil ya sea en una clase o en una conferencia, no es muy práctico que después de cierto tiempo pierdan la conexión o tengan que renovar la dirección que tienen asignada, además que hay alumnos que tiene que pasar un tiempo considerable realizando trabajos de las asignaturas, por lo que no se estaría prestando un servicio de calidad, ya que el proceso sería muy engorroso, además este proceso se puede llevar a cabo de forma automática, por lo que se debe considerar si vale la pena este proceso y la creación de perfiles de usuario.

Para el caso de la red wireless que se está proponiendo, se hace el análisis de cuales son los servicios que los alumnos de la Facultad de Ingeniería necesitan en una red.

Otro problema que se tiene que solucionar es dar servicio a las personas que se encuentran de visita, como pueden ser conferencistas o estudiantes de intercambio, etc. Se debe considerar la opción de tener visitantes y la manera en que se puede dar servicio a este tipo de personas, ya sea creando cuentas temporales que estén restringidas únicamente a los servicio de Internet y correo electrónico. Es importante llevar un control estricto de: ¿a quién se le presta el servicio?, ¿para qué?, ¿cuándo es hora pico?, ¿se genere gran tráfico en la red y se hace lenta?. En cuanto a los perfiles que se generen, se debe tener cuidado, se debe recordar que hay alumnos en toda Ciudad Universitaria y que no se puede dejar abierta la red.

4.1.3 Equipo de cada usuario

Se debemos mencionar la importancia de la cultura de la seguridad que tenga cada usuario. Por que si bien podemos hablar de un control de aplicaciones que pueden ser usadas por los alumnos, también se debe tener en cuenta que si se habla de un equipo propio de cada usuario, y que no es la única red a la que se conectan, por lo que si el equipo está infectado o comprometido, puede infectar o comprometer a otros equipos en ésta red que no cuenten con el software necesario para la protección de sus equipos, como pueden ser: un antivirus, antiSpyware y un firewall personal, así también, que no cuente con las actualizaciones correspondientes, ya sea del sistema operativo o del antivirus.

Otro problema a resolver es para brindar un servicio adecuado a aquellos alumnos que cuentan con un sistema operativo basado en la plataforma UNIX, sin embargo el servicio para este tipo de sistemas operativos muchas veces depende de la tarjeta de red inalámbrica con que cuente el equipo y la distribución que se tenga instalada.

4.2 Nivel de administración de la red

La falta de seguridad en las redes inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información.

Es importante destacar que uno de los objetivos de éste proyecto es ofrecer una red que esté sobre todo estable y controlada. Para evitar problemas como que la red deje de dar servicio, o se corten las

conexiones al paso de la información o saturación del canal. Es decir que se garantice que estará disponible y será rápida todo el tiempo.

Estos problemas pueden ser atribuidos a situaciones como mal diseño de la red, mala posición de antenas y access point, soporte de clientes en el access point, servicio de roaming en los access point, interfaz de administración de los usuarios.

4.2.1 Diseño de la red

En la Facultad ya se cuenta con el servicio de red inalámbrica de la RIU, así como también el servicio de cómputo que se ofrece en la sala de la Unidad de Cómputo Académico, sin embargo estos servicios no son suficientes, ya que el numero de alumnos atendidos en las sala de UNICA es muy bajo en comparación con el número de alumnos que toman clases en el edificio principal. Para el caso de la RIU, el problema desde este particular punto de vista es que no es un servicio administrado por gente de la Facultad, no existen perfiles de usuario, la cobertura no es la deseada en el edificio, ya que hay muchas zonas importantes (como salas de exámenes), donde la cobertura es nula, y no existe soporte para usuarios.
Para el adecuado funcionamiento de una red, es importante la estructura que deben tener los componentes y dispositivos que se ocupan en el diseño de una red, estamos hablando de componentes como un firewall a nivel de red, la colocación del access point. Es decir si el firewall no está colocado en la red adecuadamente, se puede tener como consecuencia un servicio de red muy lento.
En las salas de UNICA se cuenta con un firewall a nivel de red que ayuda a tener un control del tráfico y de los servicios que se prestan en ella.

4.2.2 Posición de antenas y access point

El edificio principal de la Facultad de Ingeniería, cuenta con 3 edificios principales, A, B y C, un edificio donde se encuentran los laboratorios y los salones conocidos como L, donde anexo al mismo edificio, se encuentra el que alberga la Biblioteca; así mismo existe con un auditorio que se encuentra en la planta baja de la facultad, así mismo se encuentra el edificio CETATI, donde se encuentra UNICA, la librería y otras oficinas, también cuenta con espacios abiertos, para este caso se consideran 3 principalmente(Fig. 4.2).

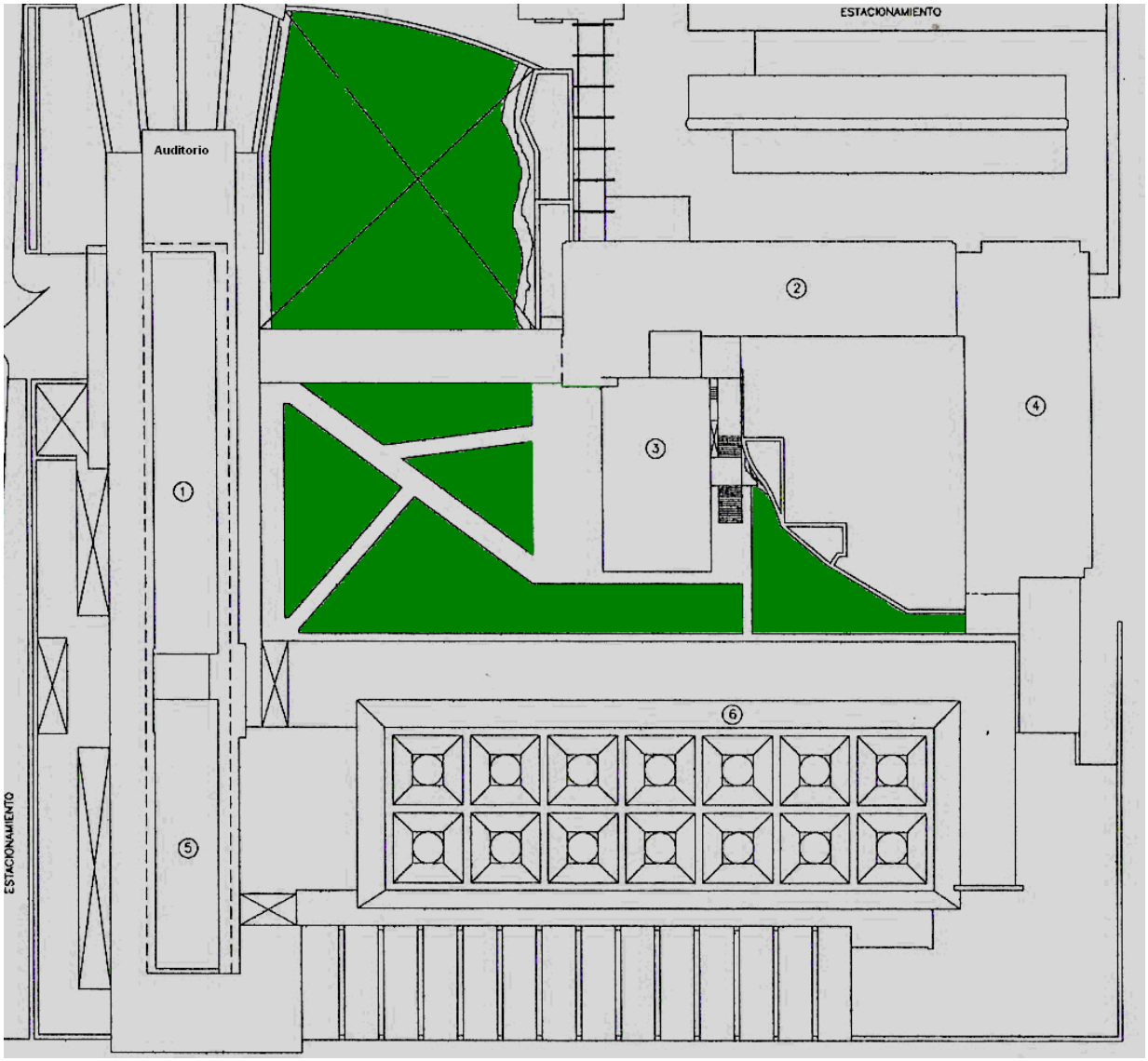


Imagen 4.1 Facultad de Ingeniería

1. Edificio A
2. Edificio B
3. Edificio CECAFI (salas de UNICA y librería)
4. Edificio C
5. Biblioteca
6. Edificio de laboratorios y salones L

Áreas Verdes

Es importante considerar la ubicación de cada una de las antenas y de los access point, ya que por el material de cada edificio no pasa la señal y podemos no encontrar el máximo rendimiento de las antenas.

Lo que se propone en este trabajo es dar el servicio para los espacios abiertos de la Facultad de Ingeniería, para la biblioteca y el

auditorio, por lo que para la colocación de los AP, se debe elegir un sitio estratégico.
Esta propuesta de redes en sitios abiertos es por que no existen lugares que no sean la biblioteca o las salas de UNICA para tomarlos como sitios de estudio, los cuales son lugares con muy poca capacidad a comparación del número de alumnos de la Facultad.

4.2.3 Número de clientes soportados en el access point

Es importante tomar en cuenta cuantos clientes soporta cada access point que conforme la red, ya que es fundamental el alcance que tenga, también es importante el número de usuarios que puedan soportar.
Este aspecto depende mucho de la marca y el modelo, y debe tomarse en cuenta ya que como se puede observar en la imagen 4.2 las áreas que se desean cubrir no son muy grandes y los puntos donde se pueden colocar los AP's no están muy alejados, sin embargo si es importante considerar que el número de alumnos que pueden conectarse si es alto, motivo por el cual hay que considerar este aspecto. Así como también, analizar detenidamente la relación Costo/Beneficio, es decir que los access point que se adquieran tengan el mejor resultado en esta relación. Y considerar ¿qué conviene más?

a) Invertir una antena que expanda el radio de alcance de la red, es decir se gane área de cobertura
b) O usar otro access point y entonces ganar número de usuarios posibles en un área de cobertura menor.

Imagen 4.2 Áreas donde se supone la concentración de alumnos

4.2.4 Servicio de roaming en los access point

El servicio de roaming se refiere para este caso, que independientemente del número de access point con que cuente la red, el servicio sea transparente para el usuario, es decir que si el usuario se desplaza entre el área de cobertura de cada access point no sean requeridas sus credenciales o alguna identificación para que el access point al que pertenece la nueva área de cobertura le de el servicio, es decir que no exista interrupción del servicio en todo lugar en donde se desea prestar el servicio, que sea constante y de calidad en cada punto del área.

Para lograr este objetivo se debe considerar que muchas marcas no son compatibles y que también unas no permiten llevar a cabo el roaming, ya que los dispositivos están configurados para trabajar de forma stand alone. Así mismo se debe considerar la distancia de cada access point para que no se coloquen tan lejanos que en la periferia de cada área de cobertura se pierda la señal, o colocarlos cercanos y se desaproveche la capacidad de los dispositivos.
En particular en el edificio de la Facultad de ingeniería, los muros son demasiado gruesos y el material no deja pasar la señal ya que rebota o simplemente la obstruye para dejar un área de acción bastante reducida.

4.2.5 Interfaz de administración de los usuarios.

Este aspecto no es visto por los usuarios directamente, sin embargo no deja de ser importante como los anteriores, por que si bien, los usuarios no lo "necesitan", es indispensable que dentro de la red que les de servicio se cuente con una administración adecuada, que le ayude a las personas indicadas a llevar un estricto control de las personas, servicios y equipos. Además que si desde la administración de la red es buena, seguramente para el usuario será más fácil darse de alta, y el servicio que recibirá será de alta calidad. Para el caso de la Facultad, el servicio de las salas de cómputo de UNICA, ya cuenta con una interfaz en la que es necesario que los alumnos se den de alta para que puedan tener acceso a las salas, este registro se hace en las salas de la Unidad, ya sea en la sala del edificio principal o en las salas del edificio anexo, donde también tiene salas, para llevar a cabo este registro el alumnos solamente necesita su comprobante de inscripción y una identificación, preferentemente la credencial de la Facultad resellada o actualizada. Para el caso de la red wireless, se necesitaría como dato extra a todos los datos identificación del servicio ya mencionado la dirección MAC del equipo portátil que se desea conectar, la marca y dar una clave de acceso para cada usuario así como una contraseña para el acceso a la red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante. Este es otro de los aspectos que se deben de tomar en cuenta a resolver para prestar el servicio de en la Facultad de Ingeniería. Para el caso de la interfaz de administración, desde la planeación es importante definir si se permite éste tipo de cuentas "visita", si el usuario tiene que darse de alta, o esta cuenta estará activada y se tendrá un monitoreo constante de su uso.

4.2.6 Sistema de autenticación de acceso a la red

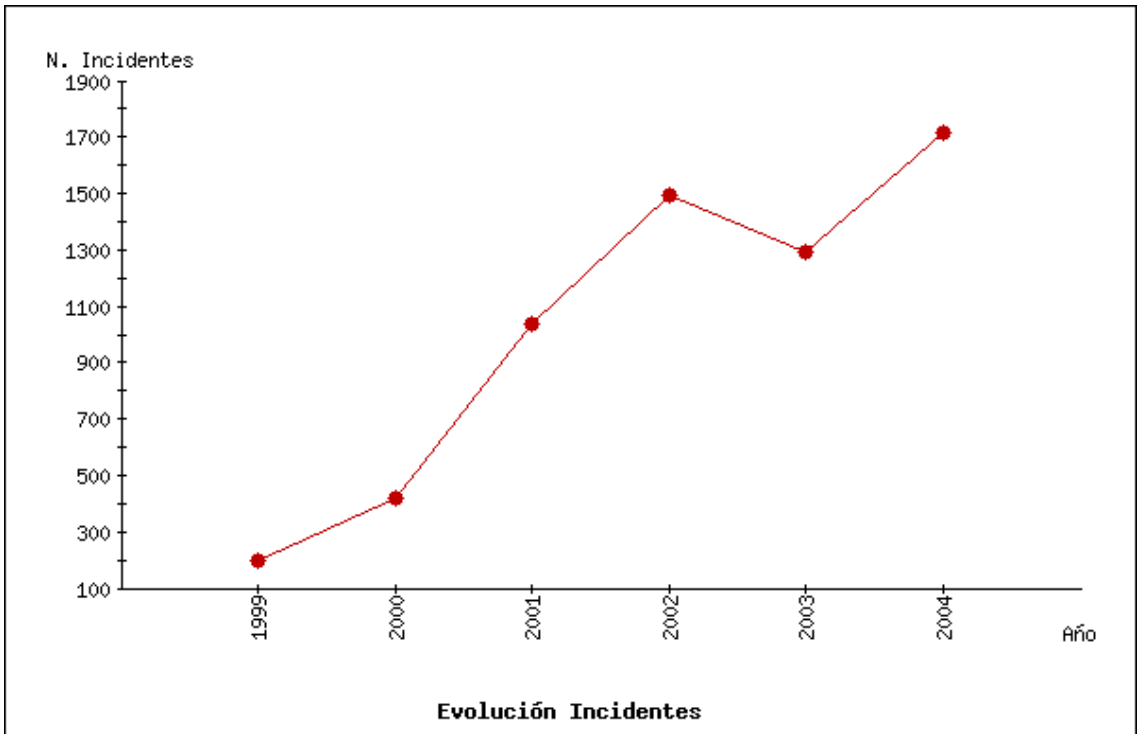
Para tener el control de quien esta autorizado para hacer uso de los recursos de la red se necesita contar con un control para autenticar a las máquinas y las personas que quieran ingresar a la red. Para esto, en el capítulo anterior se dio una serie de opciones que se

pueden implementar para lograr este control. Sin embargo la verdadera problemática está en que ninguna de las opciones tiene un porcentaje alto de seguridad.
Se pueden correr una serie de herramientas, que también se explicaron en el capitulo anterior, para obtener las diferentes llaves, y para romper la seguridad de algún sistema de autenticación explicado anteriormente.
Otro de los problemas, es que si encontramos una combinación realmente fuerte, los tramites para darse de alta y/o para iniciar sesión en la red, pueden llegar a ser muy engorrosos, lo que hace que el servicio no sea tan amigable para los usuarios comunes.
El hecho de que no se pueda garantizar un alto porcentaje en seguridad, hace que si algún intruso puede vulnerar alguna parte de nuestro sistema de autenticación, el sistema se vuelva totalmente inestable, esto puede llevar a dos situaciones; la primera es que cualquiera pueda entrar a la red, y ya no se garantice ninguno de los aspectos importantes de la seguridad, sobretodo la integridad. La segunda es que nadie pueda entrar en la red, por que no se autentica adecuadamente, lo que nos lleva a un ataque de denegación de servicios.

4.3 Nivel de Seguridad en la red

Sin duda este aspecto es de los más importantes, ya que es bien sabido que éste es el "talón de Aquiles" ésta tecnología y se encontraría con varios intentos de ataques y debe de estar preparada para soportar cuando menos, los ataques más conocidos, y otros que si bien son elaborados la infraestructura tanto lógica como física no se vea afectada en alto porcentaje o no por un largo intervalo de tiempo.
En este aspecto los problemas que se considera debemos enfrentar son la seguridad física de los dispositivos de la red, la seguridad lógica de los dispositivos de la red, la redefinición y ajuste de las políticas de seguridad, la aplicación adecuada de las políticas de seguridad.

Según cifras del CERT (Equipo de respuesta a incidentes), la cantidad de este tipo de software en a red crece de forma exponencial y existen más de 62000 virus, y el tiempo en el que se difunden y contaminan es extremadamente corto, además de existir muchas formas en las que se pueden contaminar la computadoras y con esto tener problemas de rendimiento en la red en los propios equipos.



Gráfica 4.1. Evolución de Incidentes, CERT/CC

La posible solución que se puede dar es contar con dispositivos a nivel de red como firewall y sistemas detectores de intrusos, donde se pueda hacer filtros por servicios o puertos. De esta forma es más práctica, ya que sabemos que los clientes solo deben hacer peticiones por puertos altos, es decir por puertos arriba del 1024 y que los servidores solo pueden recibir peticiones por puertos debajo del 1024 o establecer directamente el servicio que está prestando y el puerto correspondiente a su aplicación. Así mismo se debe establecer que la política de la red es totalmente restrictiva y que para ciertas aplicaciones que usen puertos no definidos o diferentes a los que se encuentran en los estándares se debe acudir con el administrador para abrir dicho puerto y se lleve un estricto control de los puertos y aplicaciones "especiales".

4.3.1 Seguridad Física de los dispositivos

Lamentablemente la posibilidad del robo de alguno de los componentes de la red es un aspecto que se debe de tomar en cuenta y pensar en alguna solución o método para evitarlo. Los casos en los que nos podemos enfrentar son, que roben los access point, las antenas o los equipos personales de los usuarios.

El hecho de que los access point se encuentren en partes externas de los edificios los hace puntos vulnerables al robo. Se puede pensar que una de las soluciones es que se coloquen en puntos extremadamente altos, sin embargo, se debe recordar que

dependiendo del tipo de antena, es el tipo de cobertura o expansión de la señal, es decir si se habla de una antena omnidireccional, con una ganancia de [dBi], no es una esfera perfecta, por lo que si es colocada en un punto muy alto hará zonas en los primeros pisos que no serán cubiertos.
Así también se tiene que hacer un análisis del material con que se va sostener, para no toparse con que el material afecta la expansión de la señal de las antenas o como administrador no poder obtener información del estado de cada access point por medio del encendido de los leds.

Ahora en cuanto al robo de los equipos portátiles, si bien, se puede pensar es cuestión de cada usuario, como administradores de la red debe interesar por que si se tiene acceso a la red de una máquina robada, se puede tratar de un usuario malicioso que no conozca y/o no respete las políticas establecidas en la red, o que trate de hacer algún tipo de ataque a partir de ese equipo, pero sobre todo lo más importante es que viola la seguridad en el aspecto de autenticación, por que si bien el control que se propone es por medio de la dirección MAC, (dispositivos), también se pide un nombre de usuario y una contraseña (interfaz de usuario).

4.3.2 Seguridad lógica de los dispositivos de red

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Sin embargo si es que en función del número de usuarios y las aplicaciones de cada uno la velocidad que cada usuario puede tener. Es decir, en una red de éste tipo si hablamos de un medio compartido.

La seguridad lógica probablemente sea la más difícil de controlar, ya que se puede encontrar desde un monitoreo no autorizado de la red, intrusiones en ella, consumo extremo de los recursos de la red y suplantación de identidad y de algunos usuarios o presencia de malware (virus, gusanos, spyware) en la red entre otro tipo de software que consuma el ancho de banda.

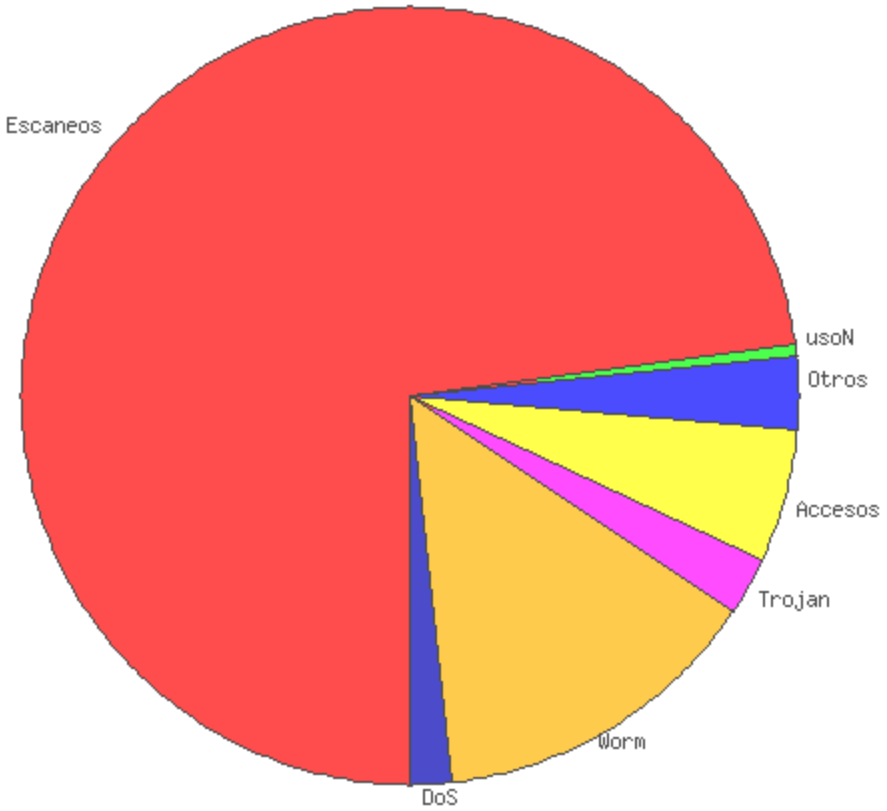
Monitoreo no autorizado

A pesar de que se trata de una red en un ambiente académico se trata del servicio para jóvenes que se están iniciando en la investigación y es común encontrarse con la situación de querer escuchar el tráfico de la red. Otro caso sería contar con usuarios experimentados que quieran hacer lo mismo. Si bien se puede pensar que en una red de este tipo no viaja información demasiado importante, si se debe garantizar la integridad y confidencialidad de dicha información, ya que es uno de los aspectos fundamentales de la red, y es de los aspectos que hacen que se pueda garantizar un servicio de calidad a los usuarios. El monitoreo no autorizado de la red, aparte de violar este aspecto, también pone en riesgo disponibilidad de los recursos de la red, ya que pueden consumirse demasiados haciendo esta actividad.
En el capítulo anterior se mencionaron los diferentes tipos de software con los que se puede contar para llevar a cabo esta actividad, y que es muy fácil conseguirlos, de nuevo se menciona que son armas de dos filos, si bien al administrador le sirve para hacer monitoreo del desempeño del servicio que está ofreciendo, para un usuario malicioso puede darle toda la información que pasa por la red y violar garantías importantes que se tiene que dar a los usuarios.

Mapeo y Enumeración de la red

Es importante verificar que tipo y que tanta información arroja la red cuando se le hace un mapeo y/o enumeración, ya que hay que considerar si en realidad es necesario que las personas se enteren de lo que hay en la red. Si bien como administradores de red ese tipo de herramientas sirve bastante, por que da información de que servicios y puertos se tienen y los equipos y tipo de configuración que se tiene en a red.
Si bien se comenta que del punto de vista del administrador es muy útil, del punto de vista del atacante es mucho más útil por que estos son los datos que pueden completar el paso de reconocimiento del sistema, por lo que es recomendable que ante este tipo de acciones se de la menos información posible. Se tiene que hacer una revisión constante de las bitácoras para que poder informarse de todos los eventos y lo que esta sucediendo con los usuarios y servicios.
En este caso el mapeo ayuda a dar información sobre los servicios, y puertos que se están prestando y dependiendo del tipo de mapeo es la información extra que se puede obtener.
Para el caso de una enumeración, lo que se puede obtener de información es el tipo de equipo y configuración que se está usando en la red. También se pueden obtener los recursos que se tienen compartidos, lo que hace más peligrosa esta acción, ya que la mayoría de los usuarios cuentan con archivos compartidos pero no lo

saben o no saben que se puede acceder a ellos por medio de la red.



Gráfica 4.2. Estadísticas por tipo de ataques

Como se puede observar, la mayor parte de ataques corresponden a los hechos por un escaneo, por lo menos, ese es el primer paso que dan los atacantes.

Suplantación de Identidad

Aquí se retoma lo mencionado en el punto de seguridad física, ya que si por algún motivo una máquina es robada, no es correcto que se sigan prestando los servicios de la red a dicho equipo, ya que no se habla de servicio a ciertas máquinas, sino el servicio a los alumnos, además el control de seguridad requiere también de una identificación del alumno, no sólo de la máquina.

Para el caso del robo de los access point, no significa solo la pérdida de un equipo primordial en la red, sino de la posibilidad que sea usado con fines malos, como hacerse pasar como parte de nuestra red para ciertos equipos que pueden interesar, como puede ser la computadora de algún profesor, o del personal que maneje documentos confidenciales o que simplemente no deben ver personas ajenas. Por lo que, se debe manejar un nivel de seguridad no únicamente donde el access point tenga que verificar si es el

cliente válido del que esta recibiendo peticiones, sino que también el cliente tiene que verificar que el access point al que le esta haciendo peticiones es válido y está autorizado para darle el servicio. Por este motivo se debe considerar una configuración en la que se pueda certificar la validez de ambas partes.

Presencia de Malware en la red

En el capítulo anterior, ya se mencionaba el origen de esta palabra MALWARE, ahora se tiene que considerar cuales son los riesgos que se corre al tener un equipo infectado dentro de la red.
La inconveniencia de un equipo portátil es que se puede conectar a cualquier red pública donde se tenga acceso, por lo que los equipos están abiertos a la posibilidad de infectarse, la desventaja, es que vienen a la red y pueden infectar a otros equipos conectados en ella. La principal desventaja de este aspecto es que se debe tener con una cultura en cada miembro de la red para hacerle conciencia de que su equipo debe contar con las actualizaciones correspondientes así como un constante monitoreo de su comportamiento, ya que en la mayoría de los casos estos problemas no son detectados hasta que ya infectaron a más equipos o cuando el equipo ya esta dañado, es decir si el equipos solo está comprometido para lanzar ataques desde él o consume los recursos, probablemente no sean detectados. Este tipo de software puede llegar por un archivo adjunto de un correo electrónico, algún archivo de un dispositivo externo como una memoria USB o CD-ROM o como ya se mencionó la conexión a una red ya contaminada.

Se debe tomar en cuenta la presencia de otro tipo de software que no precisamente es malware, pero que si consume ancho de banda y puede violar las políticas ya establecidas.

Software peer to peer

Este tipo de software es del que se puede descargar canciones, videos, libros o software. Lo peligroso de éste es que los usuarios pueden encontrarse con todo tipo de malware y ellos no saben en realidad lo que es, ya que son caballos de Troya, que simulan ser una cosa y resulta que son otra, es por esto que a pesar de que en las políticas actuales de la facultad ya está considerado y restringido, en esta red también hay que poner reglas específicas para este tipo de software.
Además del riesgo de la infección de los usuarios este tipo de software se apoderan de un gran porcentaje del ancho de banda así mismo se ponen en riesgo a la red de que le hagan algún monitoreo o escaneo donde se pueda obtener demasiada

información de la red, es decir se puede obtener acceso de usuarios no autorizados a la red.
Lo más importante en este aspecto, es que se violan los derechos de autor, ya que se puede descargar software, libros, canciones y videos de forma gratuita, que afectan y agreden a los autores y gente que tiene los derechos de esas obras.

Tráfico del protocolo ICMP

El protocolo ICMP, está diseñado para mandar mensajes en la red, si bien este protocolo fue diseñado par dar información sobre el estado en red de ciertos dispositivos, con el tiempo se ha descubierto toda la información que se puede obtener y hasta se han desarrollado ataques que se pueden hacer aprovechando el mismo protocolo, y se ha mal intencionado la información que con él se puede obtener.
Así mismo, el tráfico que se genera con este tipo de mensajes, es alto, es decir, ocupa mucho ancho de banda, y si se ve detenidamente, para un usuario normal es innecesario, ya que mucho no usan este protocolo para verificar el estado en la red, del dispositivo con el que quieren comunicarse.
Algunos de los comandos más comunes que se tienen que hagan uso del protocolo son:

PING
Da información sobre el estado en red del dispositivo al que se le aplique, lo único que se necesita para aplicarlo es el nombre canónico o la dirección IP del dispositivo. Puede informar, si el dispositivo es inalcanzable, si esta desconectado, si el problema es de tipo local, o si el estado del dispositivo es correcto.
Por medio de este comando se han desarrollado varios ataques, entre los más comunes, una denegación de servicios, también el ping de la muerte o inyección de código. El primero consiste en inundar al servidor con pings, de tal forma que se consuma todo su tiempo de procesamiento en contestar los mensajes de ping y cuando ya tenga que responder a una petición valida e importante no se encuentre disponible para hacerlo. El segundo, consta en enviar un paquete más grande de lo permitido, ya que con el comando ping, se puede manipular el tamaño del paquete enviado, así lo que se logra es una saturación en el ancho de banda. Finalmente la inyección de código es referente a aprovechar el campo de opciones en la cabecera ICMP, el cual por lo general no es revisado por ningún IDS o dispositivo, es ahí cuando se puede tener la oportunidad de inyectar código malicioso.

ARP

Este comando permite hacer una resolución de dirección IP a direcciones físicas (MAC), esto es importante considerarlo, ya que probablemente, una de las formas de autenticación en la red sea por medio de direcciones MAC, lo que hace que cualquiera que haga esta resolución obtenga una dirección MAC valida en la red. Con este comando también se puede hacer una modificación de la tabla de resoluciones MAC, cuestión es importante considerando que se llegue a tener acceso al AP.
Por ser un comando que hace uso del protocolo ICMP, hace que esté propenso al ataque de inyección de código.

RARP

En el caso de este comando, hace la conversión inversa que el comando ARP, muchos sistemas operativos, sobre todo los Windows, no cuentan con él, ya que el comando ARP, tiene opciones para llevar a cabo este procedimiento, es decir, resolver de dirección MAC a dirección IP. De igual manera, el uso de este comando debe considerarse por que da mucha información y por le uso del protocolo ICMP.

TRACEROUTE o TRACERT

Este comando, dice los diferentes "brincos", número de routers que tiene que pasar un paquete tiene que dar antes de llegar a su destino. Si bien, puede ser útil para saber la ruta que se sigue hacia cierto destino, también se puede tomar como una enumeración, ya que se ven todos los dispositivos que se tiene en la infraestructura, lo que puede ayudar para un ataque de evasión de IDS, manejando el TTL.

Como se puede observar este protocolo con sus diferentes comandos también son parte de las herramientas de doble filo, ya que del punto de vista del administrador son muy útiles, pero del punto de vista de un intruso, es demasiada información la que se puede obtener, y con un "adecuado" manejo se pueden llevar a cabo ataques de diferentes tipos. Por estos motivos, hay que considerar si se permite el uso de estos comandos en la red.

Tráfico de NETBIOS

Este es un protocolo propio del sistema operativo Windows de Microsoft, el cual fue diseñado par la comunicación entre dispositivos del mismo sistema operativo. Este protocolo originalmente fue desarrollado para la comunicación y compartir los recursos en la red. Sin embargo genera mucho tráfico y consumo del ancho de banda, por que hace un censo cada cierto tiempo, solamente para actualizar la información de si las máquinas vecinas siguen en red o si

su estado en la red ha cambiado, ya sea por la IP o por el nombre de red. Así mismo se debe volver a considerar que es una red escolar, y que difícilmente se puede llevar a cabo una estructura de recursos compartidos, y que muchos clientes no tienen el conocimiento de cómo acceder a los archivos compartidos, y no cuentan con la prevención adecuada para hacerlo.
Además se tiene que considerar que este protocolo usa puertos (137, 138, 139 y 445, para las nuevas versiones que usan SMB), que muchos gusanos y virus aprovechan para atacar, es más hay spyware que se aprovecha de estos puertos para instalar alguna puerta trasera que permita obtener información del equipo incluso después de ser desinstalado. Por lo que considerando esto, es recomendable no permitir este tipo de trafico en la red.

4.3.3 Ajuste de las políticas de seguridad

Actualmente, ya se cuenta con las Políticas de Seguridad de la Facultad de Ingeniería. Este documento, está muy completo, ya que abarca diferentes aspectos de prevención, uso, cuidados físicos y lógicos que se deben tener en la red convencional de la Facultad. También abarca una amplia consideración de derecho a uso que tiene los usuarios, como las sanciones que el usuario puede tener si falta a alguna de las normas mencionadas en este documento.
Para el caso de la red inalámbrica, hay que llevar a cabo el ajuste correspondiente del uso de ella, se debe establecer las situaciones completas y considerar aspectos como que el equipo en el que trabajan, es propio de los usuarios, y difícilmente se puede llevar un control de las páginas que visitan, del tiempo que tiene el servicio, o del uso de aplicaciones que puedan poner en riesgo a más usuarios en la red.

4.3.4 Aplicación adecuada de las políticas

En algunas redes de sitios públicos se maneja que cualquier persona pueda conectarse a Internet por medio de su infraestructura, sin embargo para este tipo de red no es recomendable ya que entonces no se garantiza la seguridad en ningún aspecto. Además se debe tomar en cuenta que es una red para una institución de educación que debe seguir ciertos reglamentos en los que se debe proteger para que los usuarios no instalen software de tipo peer to peer y respetar los derechos de autor, para evitar la descarga de música y software que violan estos derechos de autor, así como poder contaminarse y contaminar a otros equipos en la red

Para solucionar esto debemos tener políticas de red estrictas respecto a los archivos que se pueden manejar en cada

computadora. Aún así considerar aplicaciones que ayuden a tener control sobre los paquetes que transitan por la red. Como administradores de red, se tiene la responsabilidad de no hacer ningún a taque al exterior, y mucho más responsabilidad con los usuarios locales, que no sufran algún ataque o infección dentro de ella.
Se debe reflexionar sobre el uso de sistemas como Firewall en la periferia de la red, un Sistema Detector de intrusos (IDS), listas de control de acceso en dispositivos de red como routers o switches.
Se debe tomar en cuenta que los equipos son individuales, es decir, no es responsabilidad del administrador el software para la protección del equipo, es responsabilidad de cada usuario. El administrador tiene responsabilidad del tráfico que se permite en la red y la configuración adecuada de los dispositivos, tener un control de acceso y configuración adecuada de herramientas.

Otro problema que existe es el gran número de ataques se da a esta tecnología. Y aumenta más éste problema cuando hablamos de lo pocos métodos que hay para evitar los ataques como denegación de servicios o consumo excesivo del ancho de banda. Por ejemplo se habla de **wardriving** o de un **wartalking,** los cuales son ataques que descubren y reconocen la red. Se puede obtener la llave o llaves y lograr un acceso a la red, hasta con privilegios.
Así mismo se habla de un ataque de denegación de servicios, donde el atacante esté cambiando continuamente de dirección física o MAC, y haga demasiadas peticiones de direcciones IP, y dejar el DHCP inhabilitado para dar direcciones a usuarios válidos.

El monitoreo de servicios y puertos ocupados por los usuarios se convierten en un grave problema, por que las línea que distingue entre un monitoreo de administración y la violación de la privacidad e los usuarios es muy delgada, por lo que el personal encargado de dicha tarea debe contar con una firme ética profesional y las acciones que deben llevar a cabo en esta tarea, deben estar establecidas en detalladamente en las políticas.

La importancia y mención de ataques WAR, es por que se debe considerar el control de ciertos hechos y manejo de los dispositivos, como puede ser la detección de antenas de alta ganancia, y equipos trabajando dentro de un auto alrededor de la Facultad, se debe plantear si se tiene un política o acción que se pueda llevar a cabo en caso de detección de estos hechos.
De la misma forma, se debe considerar el hecho de estar alerta de las posibles señales pintadas en muros, referentes a Warchalking, se van a considerar acciones correspondientes a estos posibles ataques.

CAPÍTULO 5

PROPUESTA PARA LA IMPLEMENTACIÓN DE LA RED WIRELESS DE LA FI

5. Propuesta para la Implementación

Debido a la falta de recursos económicos para el desarrollo de éste proyecto, en este trabajo de tesis se hace una propuesta de la configuración e implementación de la red wireless de uso exclusivo de los alumnos de la Facultad de Ingeniería
Específicamente se proponen todas las herramientas y configuración para la implementación de la red wireless, tratando de resolver el mayor número de problemas que se analizaron en capítulo anterior.

5.1 Elementos físicos

Como elementos físicos tenemos los access point, las tarjetas de red, el enlace necesario para dar acceso a la red ethernet al access point y los posibles equipos que formarán la red.

5.1.1 Access Point

Tomando en cuenta las características de varias marcas de Access point, comparadas con las necesidades presentadas y analizadas, se recomienda el uso del Access point marca Cisco, modelo **Aironet 1200 Series**, el principal motivo de esta recomendación es que maneja un firmware o sistema operativo con el cual se pueden implantar diferentes niveles de seguridad.
Desde lo más básico como puede ser el ocultamiento del SSID de la red, la asociación y creación de la tabla de clientes con su dirección MAC.
Hasta configuraciones muy útiles de esquemas de red, que incluyen diferentes niveles de seguridad. Además de agregar que el IOS de Cisco es muy amigable, y la administración del dispositivo se realiza por WEB. Y es así también como se hace la actualización del IOS, y de la configuración actual del AP. Se cuenta con la posibilidad de una conexión a una base de datos externa, para realizar los respaldos de los clientes que tenga dados de alta, se puede realizar la replicación con otros access point existentes en la red.
Genera estadísticas que se pueden consultar por medio de la interfaz WEB. También cuenta con un puerto de consola, para ser administrado directamente conectado a la máquina del administrador, Así como la posibilidad de administración por medio de conexión Telnet o SSH.
Se puede tener el manejo de llaves WEP, WPA con TKIP activado, así como autenticación con RADIUS, y protocolos del estándar 802.1x
Para su mejor funcionamiento, requiere de una antena con módulo de 5GHz a 5dBi en modo omnidireccional. Es un dispositivo pequeño, fácil de manejar e instalar.

Su alcance es de un radio de 100 a 130 metros de radio, considerando a esa distancia una velocidad de 1Mbps y estando a 28 metros del access point, una velocidad de 54 Mbps, y es capaz de soportar los protocolos A, By G.
Así que considerando la estructura del edificio de la Facultad de Ingeniería, se propone el uso de 3 Access point, localizados en donde se indica en la siguiente imagen.

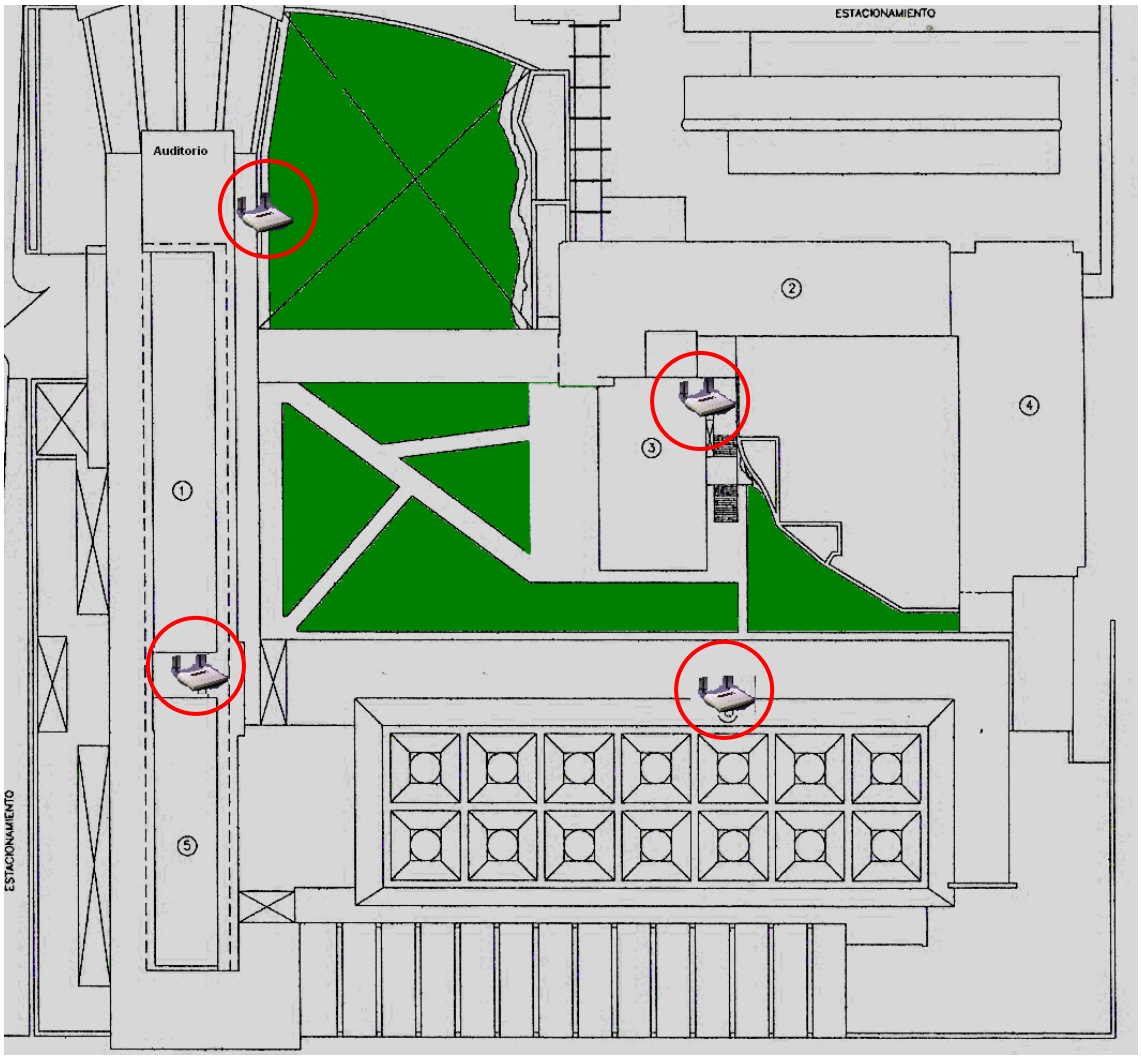


Imagen 5.1, Ubicación de AP's en la FI

La posición de cada access point, es considerando la distancia entre los edificios de la Facultad y puntos estratégicos para hacer una cobertura total de la biblioteca, del auditorio, la sala de cómputo de UNICA, los salones de los 3 edificios principales(A, B y C), también el edificios de laboratorios y salones L, con la cobertura que se tiene en los AP, también se da servicio en las oficinas que se encuentran en la parte baja del edificio de salones L, en la Dirección y oficinas anexas a ella y de las áreas verdes con que cuenta la Facultad, prácticamente, se cubren todos los espacios interesantes del edificio.

Los edificios elegidos, son altos y se consideran de difícil acceso en las áreas donde se desea colocar el access point.
De esta forma se puede hablar de un nivel adecuado de seguridad física de esos dispositivos, ya que por su desempeño, estos dispositivos se tienen que colocar en sitios abiertos.

5.1.2 Tarjetas de red

Hay que considerar la necesidad de la compatibilidad de varias marcas, estándares y modelos es decir que el Access point que se elija no este "casado", con tarjetas de su misma marca o de ciertas características que haga que los usuarios tengan que adquirir la tarjeta de cierta marca para poder contar con el servicio.
También se tiene que considerar, que hay equipos ya viejos, que no soportan el protocolo para la autenticación o no es compatible, esto como administradores de red, es importante tomarlo en cuenta, ya que siempre existirá el usuario que tiene ese tipo de problemas y hay que dar una explicación o posible solución del por qué tiene problemas para conectarse a la red.
El access point recomendado, no está casado con ningún tipo de tarjeta o marca en especial, los problemas que se pueden presentar con ciertas tarjetas de red, son de tipo de compatibilidad y soporte con el protocolo de autenticación, ya que como se mencionó en la breve descripción del dispositivo, es posible configurar los protocolos de autenticación más recientes, basados y establecidos en estándares internacionales de IEEE.

5.1.3 El enlace necesario para dar acceso a la red ethernet al access point

La mayoría de los Access point, necesitan una conexión de ethernet para dar el servicio inalámbrico a su LAN correspondiente.
Para este caso, se tiene que considerar la forma de cablear desde los switches que distribuyen la red ethernet de la facultad hasta los access point, es necesario recalcar que a pesar de que el cable está construido para soportar ciertas condiciones climáticas y trato rudo, se tiene que considerar el desgaste natural del material. Así como el hecho pasar los cables por rutas donde quede al alcance de los alumnos o cualquier persona que con solo unas tijeras o algún objeto corte o troce el cable, y ya sea intencional o no, hagan un ataque de denegación de servicios, al no llegar la conexión al AP, y no dar servicio. Se tiene que considerar también el no violar las recomendaciones del estándar ethernet 802.3, excediendo las distancias máximas permitidas.

5.1.4 Los equipos personales que formarán la red.

La seguridad física que se puede implementar depende de los usuarios que son lo dueños de los equipos, como administradores de la red se puede emitir un tríptico donde se den recomendaciones de seguridad física para cada equipo. En el que se puede incluir recomendaciones para la transportación del equipo así como los cuidados que se deben de tener en el uso del equipo en la estancia en la Facultad.

Realmente es difícil hablar de un control en este aspecto, ya que lamentablemente ningún sistema puede garantizar un alto nivel en seguridad física en ningún aspecto.
Para el modelo de Access point que se propone, se tiene una aplicación que es parte del conjunto de herramientas y aplicaciones Wireless LAN Solution Engine (WLSE) que son aplicaciones de administración que ofrece Cisco para sus equipos.
En especial esta herramienta se llama WLSE, Radio Management Tools. Lo que hace esta herramienta, es identificar los dispositivos que están siendo usados dentro del radio de los access point que la tengan instalada. Esta herramienta esta basada en java, y para el buen funcionamiento, se tiene que proporcionar una imagen del plano de la zona o edificios donde se encuentra la red, esta imagen es muy fácil de manejar, ya que se puede dar en formato, jpg, gif o png. De preferencia también debe proporcionar información sobre los nombres de los edificios y de preferencia una descripción que en su momento se considere sea útil, especificar la localización del Access point en cada piso.
La utilidad de esta herramienta, es para poder localizar un equipo que sea reportado como robado y usado en la misma red posteriormente, esta aplicación no solo es para equipos personales, sino también para access point, es decir en el caso de que sea robado, y después quiera ser usado para engañar a los usuarios para poder obtener su información, esta interfaz, manda avisos de donde está este equipo. Esta aplicación soporta 100 access point. Tienen una interfaz gráfica muy amigable, que es totalmente gráfica. Da también opciones para configurar a cada access point, los datos de sus vecinos, y de cuales, puede aceptar trabajar en equipo y aceptar como parte de la red. Dentro de su interfaz gráfica, da un reporte del alcance que está teniendo cada access point, también se puede tener un reporte de los equipos que están asociados a casa access point. Esta localización física la lleva a cabo por medio de la radiofrecuencia y dependiendo de la información que se haya proporcionado en la configuración de esta aplicación, por lo que es importante dar toda la información de nombres familiares u oficiales de los lugares de cobertura para hacer una buena triangulación de la señal que emite cada equipo. Esta aplicación no solo es

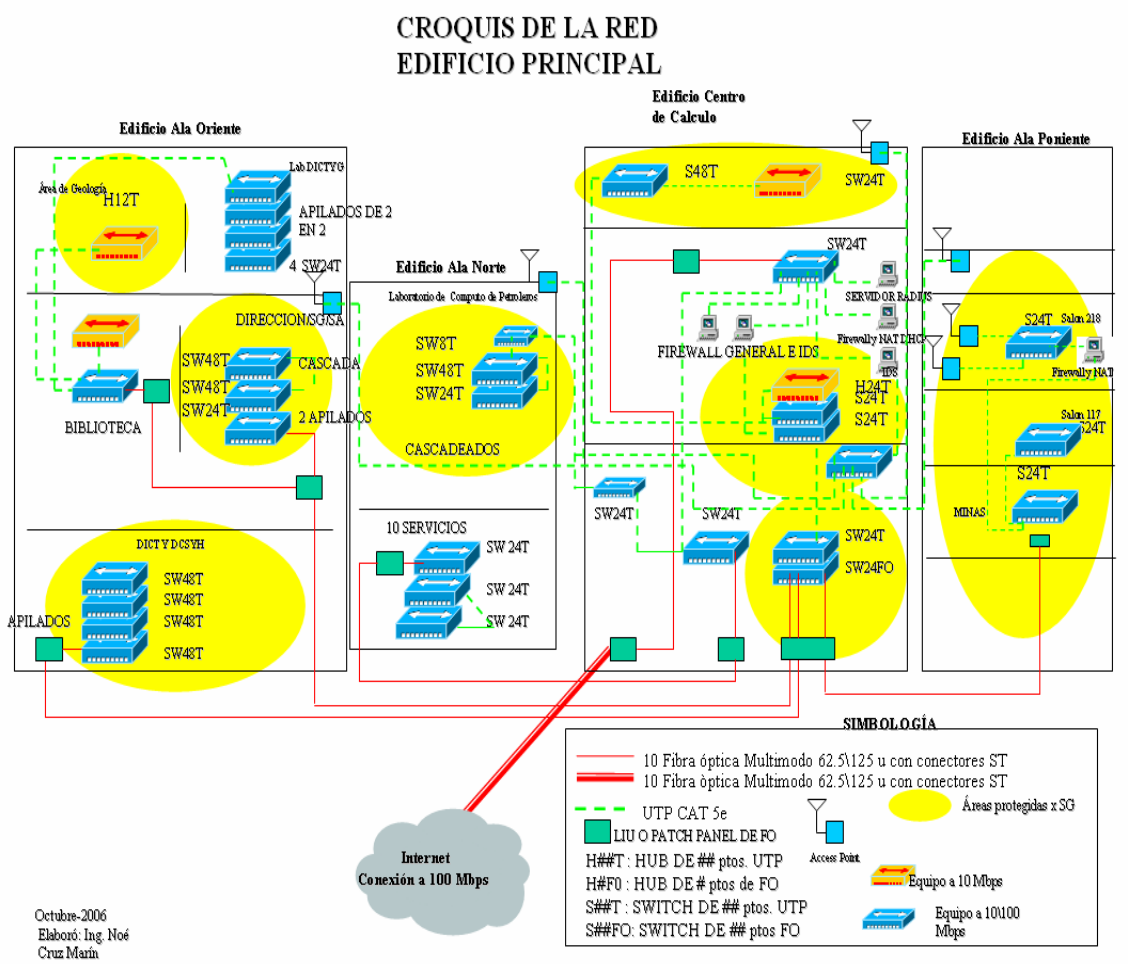
demasiado útil para la seguridad física, sino para la localización de un equipo infectado o de un equipo que sea victima de algún código malicioso y a partir de él se lleve a cabo algún ataque.

Además, se pueden obtener reportes de cuál es el access point con más solicitudes y desde qué lugares, por lo que desde el punto de vista de la administración simplifica demasiado el trabajo, para cuestiones de entrega de resultados o estadísticas del comportamiento de la red.

5.1.5 Ubicación de los servidores, firewalls e IDS

Así como las laptop y access point tienen el riesgo de ser robados, los equipos que tendrán el perfil de firewall, IDS, y el servidor de autenticación. Estás máquinas son de suma importancia, tanto para el adecuado funcionamiento de la red, como para tener un control y un nivel de seguridad adecuado, además que considerando la posición de éstos dispositivos en la red.

Por lo que se propone que éstas máquinas estén situadas en un lugar que no sea de fácil acceso, donde haya un control de acceso, solo para el personal autorizado, se cuente con un sistema eléctrico adecuado, para que en cualquier falla de energía se garantice que los equipos no se apagarán y se interrumpirá el servicio en la red. Así también debe contar con la temperatura adecuada, por este motivo, dicho lugar, debe contar con un sistema de aire acondicionado, para lograr el mejor funcionamiento de dichos equipos.
Se propone que estos equipos sean colocados en el cuarto de servidores con que cuenta la Unidad de Cómputo Académico de la Facultad de Ingeniería, ya que este es un espacio que cumple totalmente y que ya está acondicionado con los requisitos necesarios para alojar equipos críticos.



Esquema 5.1 Croquis de la red del Edificio principal

5.2 Elementos lógicos

Los elementos lógicos que se consideran más importantes la implementación de la red, los podemos dividir en los elementos lógicos para lograr una mejor administración y los que ayudan a lograr un nivel alto de seguridad en el servicio que se prestará.

Es muy importante indicar que esta red, es una infraestructura que ira sobre la red ethernet ya establecida en la Facultad, por lo que el enlace a Internet, no significará una red independiente totalmente, ni un gasto extra, ni la puesta en marcha de una estructura ethernet, para que dependa de ésta.

5.2.1 Administración

Para una buena administración, se tiene que considerar el mecanismo que se debe implementar para los siguientes aspectos: administración de usuarios, administración de access point, uso de ancho de banda, rendimiento de la red en general.

5.2.1.1 Administración de usuarios

En este aspecto, se considera un buen mecanismo de administración aquel que ayuda a cubrir la mayoría de los problemas que se analizaron, para este caso, el mecanismo es una combinación de varios sistemas.

Asignación de direcciones IP

Para la cobertura de este requisito, se propone el uso de un DHCP, si bien este protocolo puede ser implementado en el mismo access point, no es recomendable, dejar el control a un solo dispositivo de red. Así también este protocolo puede activarse en casi todos los sistemas operativos, o cuando menos, en los principales o más conocidos o basados en ellos, (Windows, Unix). Así la recomendación para la implementación del servidor DHCP, es que haga en el sistema operativo OpenBSD, ya que, además de ser de fácil configuración, se tiene la opción para una configuración avanzada, es decir, se puede llevar a cabo la autenticación de la dirección MAC para la asignación de la dirección IP. Así mismo se puede configurar un NAT (Network Address translation), el cual permite, hacer la traducción de un conjunto de direcciones privadas a una dirección real, lo que ayuda al ahorro de direcciones reales, y se asegura que ninguna máquina que tenga por extrañas razones un servicio que no deba tener, no va salir a Internet, o al público en general, ya que la dirección que tiene no es ruteable y no será vista desde afuera de la red.

Es importante mencionar que el manejo de este sistema operativo no es para usuarios comunes, y para lograr un buen funcionamiento de él se debe contar con experiencia en sistemas operativos basados en plataforma UNIX, y control y configuración desde la línea de comandos.

Considerando el tiempo que se tiene que prestar el servicio, en la configuración del servidor DHCP, se puede incluir el tiempo en el que se tiene que renovar la petición del cliente al servidor, sin embargo, no se considera que sea adecuado un tiempo de 2 a 4 horas, ya que el tiempo de trabajo de los alumnos, es más que ese tiempo. Además de considerar que por cada petición que se le hace al DHCP, se genera tráfico en la red, y que los alumnos que cuenten con el servicio, estarán trabajando en sus propios equipos, si bien se mencionaba que en las salas de cómputo de UNICA, se tiene un control de tiempo, la razón de éste es por la falta de quipos y la gran demanda que tienen, sin embargo en la temporada donde no se tiene mucha demanda (que es el tiempo en que casi terminan las clases), ese control se hace de lado, ya que no hay alumnos solicitando el lugar.

En conclusión se recomienda que el tiempo que se configure, sea de 8 a 12 horas, ya que no es el tiempo estimado que un alumno puede estar en la Facultad haciendo uso del servicio.
Y en cuanto a la clase de direcciones IP, que repartirá el DHCP, se considera que sean IP's de privadas de clase A, ya que son las que soportan el mayor número de máquinas. Es decir, como solo se habla de una red, y muchos clientes, la clase más conveniente, se considera la A. La Facultad cuenta con aproximadamente 8000 alumnos, de los cuales, la mitad toman clases en el edificio principal y se calcula que el 40% de los alumnos y personal que labora en este edifico harán uso de este servicio.

Control de acceso por medio de MAC address

Se puede tener un control de asignación por medio de MAC, sin embargo, en el access point que se propone se puede hacer un filtro o configurar el control de acceso por medio del mismo dato. En la interfaz de administración del access point, se configura la lista de usuarios que están autorizados para conectarse a él. Así se puede contar con un filtrado doble por medio de éste dato.
Es cierto que este dato se puede cambiar con ciertos comandos, sin embargo el cambio es temporal y no es sencillo llevarlo a cabo, además que se tendrán otros mecanismos de seguridad, antes de dejar que los clientes tengan acceso al DHCP para hacerle la petición.

Alcance de la zona de cobertura de los Access point

El access point que se propone tiene una cobertura promedio de 100 metros, las antenas que se proponen son omnidireccionales, lo que hace que la cobertura de la antena sea de tipo esférico, es decir, de donde sea colocado el access point, se cubrirá la zona de un ovoide con radio de 100 [m]. Esto significa que la cobertura también incluye los pasillos y algunos salones y oficinas que se encuentran en los pisos superiores o inferiores de los edificios donde serán colocados los access point.

En la imagen 5.1, se puede observar, que la ubicación propuesta para los AP, cubre la mayor parte de zonas de estudio o posibles zonas de ubicación y mayor afluencia de usuarios de la red, y adquiriendo las antenas ya mencionadas, con las que el AP es compatible, se observa que son de cobertura suficiente y capacidad suficiente de usuarios soportados. Y si hay zonas en donde se "enciman" las zonas de cobertura, en donde se ha observado hay más concentración de usuarios.
En cuanto al número de usuarios que soporta este modelo de access point, se manejan entre 128 a 200 usuarios, considerando el número

de alumnos con que cuenta la facultad y de ellos los que cuentan con un equipo portátil, la distribución de ubicación y los diferentes horarios en los que solicitan el servicio, se considera que el número de AP's y la capacidad de cada uno es adecuada, suficiente y capaz de soportar un crecimiento considerable de la población que pueda contar con su equipo.

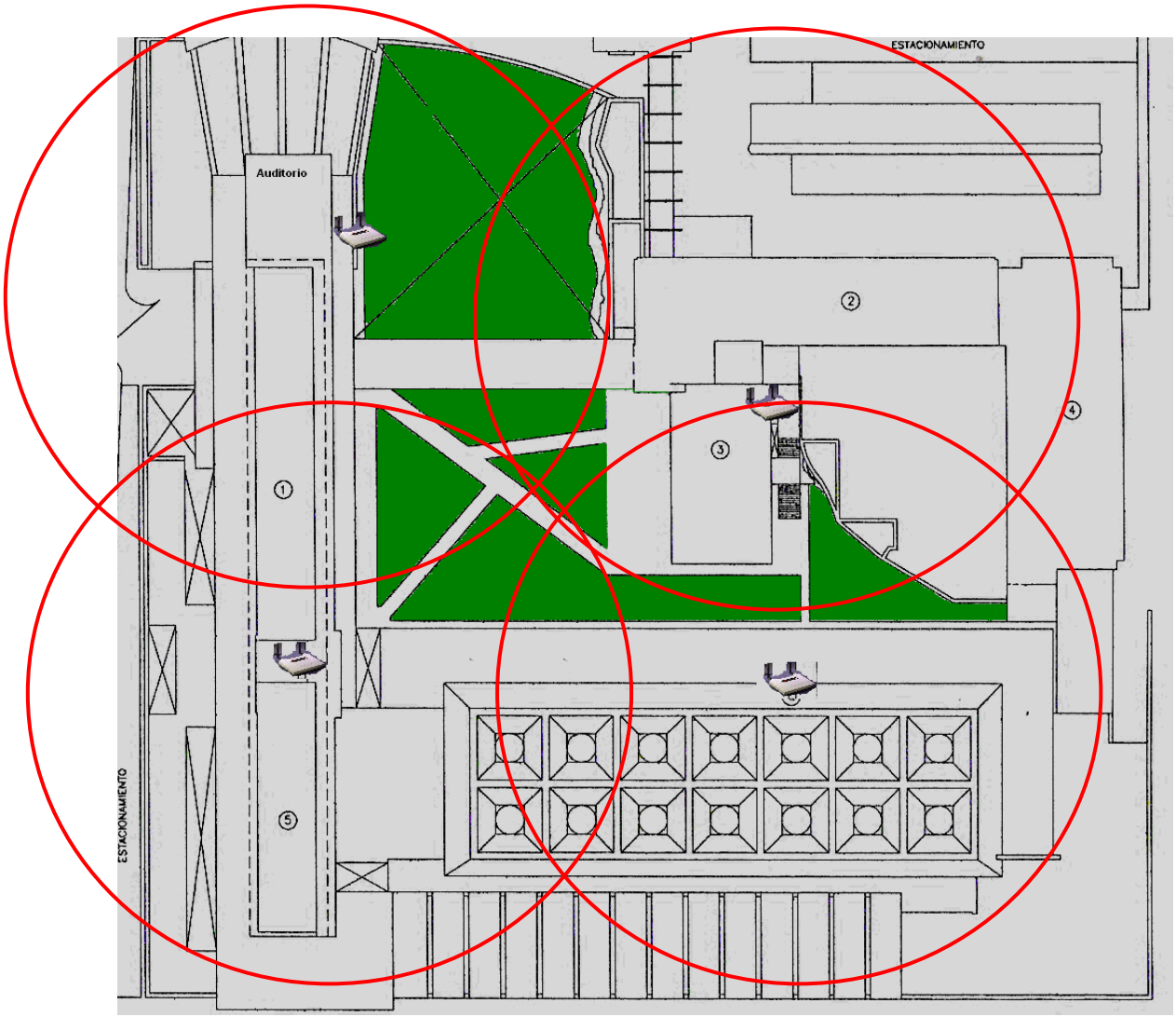


Imagen. 6.2 Alcance de AP y distribución de usuarios.

5.2.1.2 Administración de los access point

Es cierto que la mayoría de estos dispositivos son de tipo plug and play, es decir, se conectan y funcionan, sin embargo, es importante estar conciente que tiene un sistema operativo interno, y que por medio de él se administran y configuran. De igual manera se debe leer todos los manuales y especificaciones que vienen con el dispositivo, ya que en ellos se encontrarán los servicios que tiene activados por defectos, o lo servicios que se pueden activar.

Para el caso del access point **Aironet 1200 Series,** el dispositivo es capaz de trabajar en conjuntos con otros access point, haciendo

que para el usuario sea transparente el pasar de la zona de servicio de un AP a otro, cubriendo con esto el problema del roaming. Es decir si un usuario tiene necesidad de moverse de lugar, pasando de un área de cobertura a otra, el nuevo dispositivo que le de servicio, no le pedirá de nuevo su identificación, ni tendrá quehacer de nuevo la solicitud a los servidores para recibir la configuración de la red.

Así mismo, se puede asegurar, la configuración de los vecinos que cada access point tiene, estableciendo entre ellos relaciones de confianza, es decir, que para compartir sus tablas de configuración, así ante la presencia de un nuevo dispositivo no se va a hacer el intercambio de información y los usuarios que estén dentro de la red, no identificarán ese nuevo dispositivo como parte válida de la red, así se evita una suplantación de identidad de los dispositivos, de red.

Haciendo uso también del IOS del dispositivo, se puede obtener valiosa información que administrador de la red, es fundamental tener un estricto control sobre ella. Esta información puede ir desde las estadísticas de los usuarios, hasta listas de control de acceso que se configure.
Hay que hacer una observación que hay aspectos que se pueden monitorear por medio de herramientas externas, sin embargo el hecho de que el IOS del dispositivos permita llevar este tipo de control, es parte de la estrategia de seguridad que se elegirá más adelante.

5.2.1.3 Monitoreo del rendimiento de la red

Este es uno de los aspectos que se pueden monitorear por medio del IOS del dispositivo y también por medio de herramientas externas.
Llevar un monitoreo de administrador, por medio del IOS, permite que la configuración del propio software, pueda entregar reportes de los protocolos más usados en la red, de las horas de más tráfico en la red, del access point que más demanda tiene, es muy útil por que las estadísticas son totalmente gráficas y reportes.
Para el caso del monitoreo del rendimiento de la red, también existen herramientas que son independientes del IOS del AP, sin embargo los resultados que e pueden obtener de estas herramientas son totalmente dependientes de la estructura de red que se tenga. Así mismo, dichas herramientas dan excelentes resultados cuando se configuran en redes convencionales, por lo que hay que considerar el uso de estas herramientas en la parte ethernet de la red.

Herramientas como MRTG o NIKTO, son herramientas que en redes convencionales son totalmente útiles para el monitoreo del

desempeño de la red, ya que son herramientas que dan estadísticas, de acuerdo a diferentes aspectos. Que pueden ir desde el uso del ancho de banda, el porcentaje de uso de diferentes protocolos, y las posibles conexiones de los equipos. Sin embargo, para el caso de las redes wireless, puede ser útil solo en el monitoreo de la red en general, por que no cabe la posibilidad de monitorear equipo por equipo, así de esta forma solo se puede obtener información referente a la red en general.
En las redes convencionales existen herramientas para el monitoreo del desempeño de la red. Estas herramientas en general, se apoyan del protocolo SNMP, el cual, si no se configura de manera adecuada puede ser un importante agujero de seguridad. Entre las herramientas más conocidas y usadas están:

- MRTG
- NIKTO
- NTOP
- OSSIM

EL uso de cada una de ellas es totalmente dependiente del punto de vista y gusto del administrador, ya que cada una tiene su nivel de complejidad para la instalación, así mismo presentan ciertas ventajas una respecto de las otras, sin embargo, en general proporcionan información del desempeño de la red alambrada.

Considerando que se tiene una estructura de red como la siguiente, y las máquinas que servirá de sensores de monitoreo, en las posiciones donde se indica.

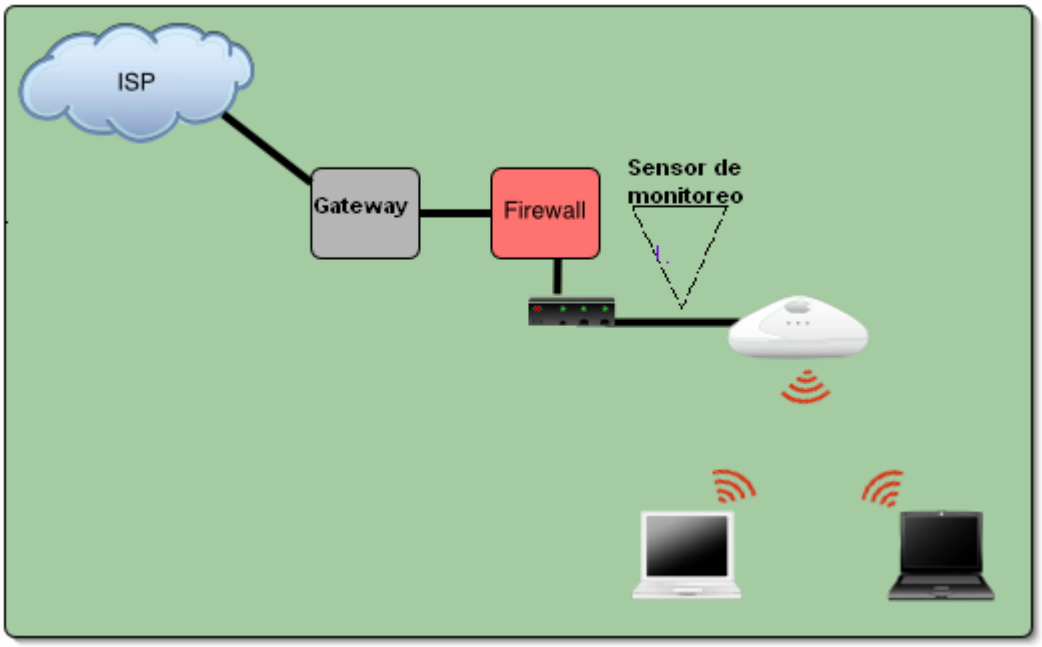


Imagen 5.3. Ubicación del sensor de monitoreo

5.2.2 Seguridad

Para lograr un nivel alto de seguridad, se tiene que considerar el aspecto del método de autenticación de los usuarios con los access point y la autenticación de los access point con los usuarios, el algoritmo y la estructura adecuada para el manejo de las llaves para controlar el tráfico de la red, elección y combinación de las estrategias de seguridad, consideraciones para el uso de dispositivos de seguridad en la red, acciones para evitar posibles ataques

5.2.2.1 Mecanismo de autenticación de acceso a la red

Durante la investigación que se llevó a cabo para el desarrollo de este trabajo, se instalaron y analizaron varias de las soluciones propuestas en el capítulo tres, sin embargo, al trabajar con ellas, se fueron descartando algunas definitivamente. Se analizaron también los sistemas de cifrado, de acuerdo a las características que se observan en la siguiente tabla.

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

Imagen 5.4 comparativa de métodos de cifrado

Basado en esto, la solución que se considera ideal, es la que lleva consigo cifrado de tipo WPA 2, o versión profesional, este es un método de cifrado que no se ha roto y que además como se puede trabajar con llaves dinámicas y no es necesario que el usuario instale aplicaciones específicas para su uso, pero si es necesaria una configuración especial para poder usarlo.

Sin embargo, considerando que para usuarios principiantes o con un nivel de manejo del sistema bajo, usan el sistema operativo Windows, para este tipo de usuarios, aparte de contar con un manual detallado, también se planea desarrollar una herramienta que haga

la configuración de manera automática, esta herramienta se proporcionaría a los usuarios en formato ejecutable y los requerimientos que necesitarían los equipos son básicos para seguridad de ellos, como son contar con las actualizaciones del dicho sistema operativo (Windows).

De las soluciones que mas convencieron fueron dos: EL portal cautivo y El servidor de RADIUS. Estas dos soluciones se pueden instalar y configurar juntas, es decir, no se excluye una de la otra, sin embargo desde este punto de vista, que sería un proceso muy engorroso la doble autenticación para el usuario, ya que sería una vez para el servidor de RADIUS, y una segunda vez en la interfaz del portal cautivo. Es cierto, se puede considerar que con la combinación de estas dos soluciones se puede aumentar el porcentaje del nivel de seguridad, también es cierto que ya se estaría cayendo en el nivel complejo y hostigante para los usuarios.

La versión del portal cautivo con la que se estuvo trabajando, fue con Authpf, la cual resultó ser una herramienta muy útil y práctica, ya que como anteriormente se explicó, la configuración no es muy sencilla, pero tampoco es imposible, pero los resultados obtenidos son muy buenos, ya que aparte de una interfaz de autenticación para el gateway, también es un firewall, y de los más recomendables. Además de estar sobre un sistema operativo estable y considerado dentro de los más seguros, además de ser un sistema con características cerradas, sin servicios que el administrador haya levantado, es sencillo.

El servidor RADIUS, que se analizó, es el software freeRADIUS. Es un servicio para autenticación remota estándar, además es compatible con SNMP. De las ventajas que se estudiaron y analizaron fueron las siguientes:

- Admite varios tipos de motores de bases de datos, esto para almacenar contraseñas, y usar diferentes tipos de esquemas de autenticación como PAP o CHAP (que son integrables con cualquier BD y Sistema operativo)
- Las nuevas versiones ya incorporan protección contra “sniffing” y algunos ataques activos que se vieron en el capítulo tres.
- Permite administración centralizada, lo que trae más sencillez en realizar sus tareas para el administrador y para los usuarios. Para el administrador, por que no necesita estar configurando repetidamente para diferentes puntos de la red. Y para los usuarios, por que solo bastará con darse de alta en la base de datos central, para ser usuario válido en la red.
- Es un software basado en estándares y tiene su respectiva configuración y descripción en el RFC 2865.

- Y cuenta con la definición, explicación y disponibilidad de sus servicios de Accounting en el RFC 2866.
- Es conocido como el software AAA, ya que permite y define los siguientes aspectos
  - **AUTENTICACIÓN:** Es capaz de verificar que una entidad, para este caso, el usuario, la máquina y el access point, es quien dice ser, generalmente este aspecto se cubre con uso de credenciales (nombre de usuario, contraseña, certificados, tokens, etc).
  - **AUTORIZACIÓN:** Es capaz de decidir si la entidad, una vez que ya está autenticada, tiene el nivel de permisos para tener acceso al recurso de la red.
  - **ACCESO, CONTROL DE:** Maneja ACL's (Listas de control de acceso), que le permiten definir, ¿a quién conceder que número de permisos?, y si el permiso es definitivo o solo temporal. Este aspecto ayuda al registro de usuarios, monitorización, contabilidad de recursos y generar informes.

Instalación y Configuración

- A continuación se presenta el esquema de red general:

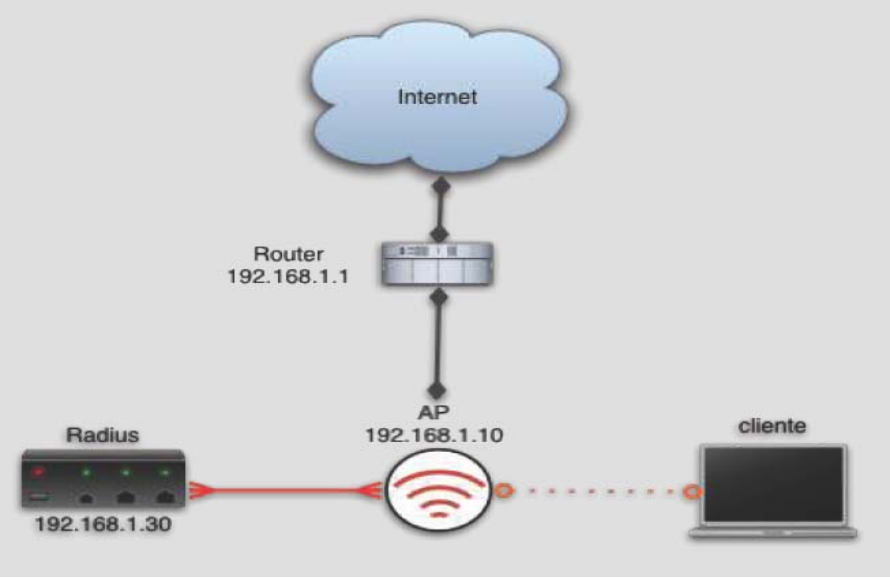


Imagen 5.5. Esquema de red con un servidor de RADIUS

El archivo de configuración general de FreeRADIUS es **RADIUS.CONF.** El cual es un archivo de configuración típico del sistema operativo Linux, es decir, cuenta con una pequeña explicación y manual de cada parámetro que se puede manejar en él.
Las directivas de configuración, están alojadas en el archivo **EAP.CONF,** es un include en el archivo radius.conf.
La descripción y credenciales de los diferentes dispositivos y credenciales que tienen que consultar al servidor antes de tener el acceso a la red son almacenados por defecto en **CLIENTS.CONF**

El archivo donde se especifican las credenciales de los usuarios con derecho a conexión a la red es **USERS.** Sin embargo, este archivo solo se usa si no existe otro backend para el almacenamiento de los usuarios.
SECRET, es usada para la comunicación entre el cliente RADIUS (AP) y el servidor de RADIUS.

Para el servidor RADIUS, son usados certificados de autenticidad, de los cuales debe haber un intercambio cuando se establece la comunicación. Por lo tanto, se debe contar con una entidad certificadora, así el archivo **CA.root**, es necesario para la creación de la CA (Certified Authority). En el servidor **CA.server,** se necesita para definir la creación de certificados en el servidor, y definir el nombre completo de dominio (fqdn), con el cual será conocida la entidad certificadora.
Es el archivo **CA.CLIENT,** es en donde se definen todos los certificados de los diferentes usuarios, se debe poner atención y no confundir con clients.conf, de RADIUS.

Xpextensions, es en donde se establece el OID para EAP-TLS.

También se deben copiar los archivos **root.der** (certificado de CA) y <usuario>.p12, que es la clave privada y certificado del cliente.

Para la configuración del Access point con el servidor de RADIUS, primero se debe mencionar que en el firmware del access point que se está recomendando, se puede establecer la conexión con el servidor RADIUS.
Pero el access point, cuenta con una opción para indicarle la dirección IP del correspondiente servidor de RADIUS, es decir un servidor externo, como es este caso.
En la interfaz donde se define el servidor RADIUS, se tiene que definir la dirección IP, el puerto por donde será establecida la comunicación, se establece también una llave secreta que es compartida entre ellos, esto para establecer la comunicación cifrada.

De entre las vulnerabilidades que se pueden encontrar, están:

- Una posible denegación de servicios (EAPOL-Start bombing)
- Se puede aplicar la ingeniería social para conseguir los certificados de los clientes, sin embargo, este es un riesgo que se corre siempre que se trabaja con usuarios, entonces, la cuestión es hacer conciencia en los usuarios.
- Se debe estar conciente que desde la zona cableada es posible atacar al servidor de certificados, por lo que ese

servidor sea parte de la red wireless, se debe proteger desde la red cableada, tanto física como lógicamente.

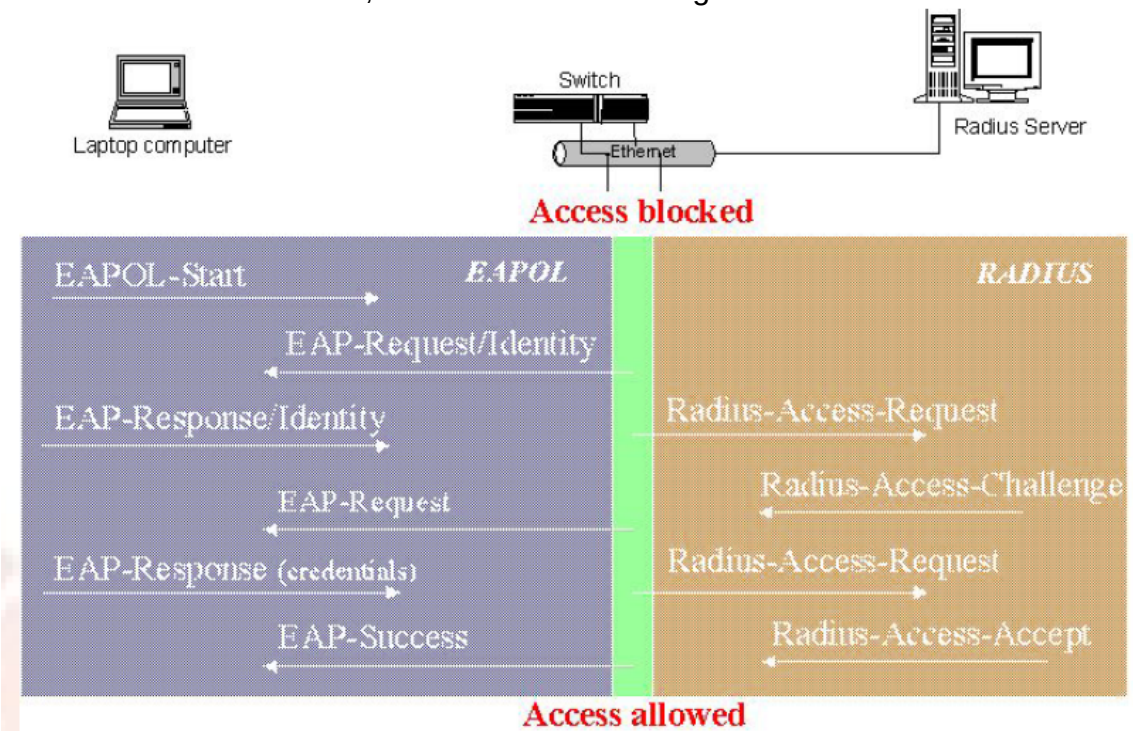


Imagen 5.6. Estructura lógica de la conexión con un servidor RADIUS.

Se usará cifrado WPA, con TKIP, ya que cuenta con bastantes ventajas, sigue con el empleo de RC4, pero ya no comparte la clave con todos los clientes. Cambia las claves cada 10000 paquetes aproximadamente. Y la mayoría de los dispositivos solo requieren una actualización de firmware para el soporte de su uso, sin embargo, hay tarjetas inalámbricas, de las más viejas, que no lo soportan.

En las nuevas versiones de TKIP, ya se habla de vectores de inicialización aumentados, el incremento de los vectores es en 32 bits, dejando un byte (dummybyte), con esto se busca evitar IV's débiles de 48 bits, pero estáticos.

También ya se menciona el IV, como un número de secuencia, y si uno ha sido recibido previamente, se descarta. Además en las nuevas versiones se evitan los reply-attacks.

5.2.2.2 Estrategia de Seguridad

De las estrategias descritas en el capitulo tres, y el análisis que se ha llevado a cabo para este caso, se ha concluido hacer una combinación entre varias de ellas.

Se pretende que la estrategia base sea la del punto de ahogo, se configurará un punto por el cual pase todo el tráfico de la red para analizarlo, es decir, se analiza por protocolo y no por contenido, por

que analizar el trafico de la red, no quiere decir que se va a atentar contra la confiabilidad de los usuarios. Para este caso el punto de ahogo será el punto donde será puesto el firewall, o sea, después del AP, sin embargo se tiene totalmente claro, que este punto solo servirá para el control de salida y entrada de la WLAN con Internet, y que el tráfico de las máquinas internas, no se puede controlar de esta manera, ya que no pasará por este punto.
La comunicación de los usuarios en la red, estará prohibida. En el IOS del AP, se tiene la opción de trabajar cada usuario en stand alone, o sea, indicarle que será como un swtich de una red convencional, sin embargo, en este caso y por todas las reglas del firewall, no se podrá tener contacto entre ellos, ni compartir archivos, ni siquiera hacer pings, por lo que cada una de las máquinas será independiente de la otra.

La implementación de la estrategia de participación universal, es totalmente fundamental, ya que, la responsabilidad de la seguridad de cada equipo depende de cada usuario, y como administrador de la red no es posible asignar o publicar algún software para el control de la seguridad. Por lo que será necesario dar platicas, conferencias y publicar trípticos para hacer conciencia de la importancia del uso del software indicado, la descarga e instalación de actualizaciones, cuidado físico del equipo son fundamentales para la seguridad de la red, y hacer conciencia de que una vez que su equipo se conecta a la red, ya es parte de ella y la seguridad de ella, es por lo tanto, responsabilidad de todos los usuarios.

5.2.2.3 Firewall

Este es uno de los dispositivos más importantes, de las redes en general. Desde su aparición y definición se ha hecho de suma importancia en la estructura de seguridad de una red. Su importancia radica en el conjunto de reglas que se configuran para el filtrado de paquetes en la red.

De las opciones que se analizaron, el firewall que se recomienda para la implementación de este caso, es el que se configura sobre el sistema operativo OpenBSD, es decir, con la configuración de la característica packet filter de dicho sistema.
La recomendación de esta aplicación va más sobre las características de seguridad del Sistema Operativo y la eficiencia probada del sistema de cifrado.
Algunas de las ventajas que se presentan al establecer este firewall, es que se trata de un dispositivo de tipo invisible. Lo que hace que en caso de un escaneo de red, de algún intruso, no se notará que existe el dispositivo, por que no cuenta con una dirección IP, y también es

transparente para el usuario. Lo único que hace es establecer un bridge entre dos interfaces de red, así cuando pasa el tráfico de dicha red, lo analiza y dependiendo de las reglas que tiene configuradas es lo que deja o no pasar.

Otra ventaja es que el usuario, no tiene que instalar ningún software o aplicación adicional, para lograr el control de los paquetes dentro de la red.

Los requisitos para su instalación son:

a) Una máquina con el sistema operativo openBSD, instalado, obviamente la recomendación, es que se instale la última versión del sistema, y si existen parches para dicha versión, instalarlos también.
b) Dicha máquina debe contar con dos interfaces de red, si se desea, se puede tener una tercera, esto para fines de administración, es decir, esta interfaz puede contar con una dirección IP, únicamente para el monitoreo del dispositivo. Con una configuración adecuada, esto no debe representar peligro alguno para la aplicación.

Los siguientes son los pasos que se deben seguir a grandes rasgos para la instalación

- Se debe verificar con el comando **ifconfig**, el reconocimiento de ambas interfaces y que no cuenten con direcciones IP asignadas.
- Las tarjetas tienen que ser configuradas en cada archivo de dispositivo correspondiente. Por lo general es en la siguiente ruta: /etc/hostname.nombre-tarjeta (ejemplo: **/etc/hostname.xl0**) En este archivo, solo se tiene que indicar que la tarjeta estará lista, o sea, que se tiene que activarr al encender el sistema.
- En el archivo **/etc/sysctl.conf,** se tiene que hacer una pequeña modificación para que se permita el forward y llevar a cabo el filtrado por paquetes o por direcciones MAC.
- Para crear el bridge entre las tarjetas de red, la utilería **brconfig,** es la que ayuda a verificar el estado del kernel sobre las interfaces de bridge, y es la que permite que se tenga el control de los bridges. Ese bridge, es el que permitirá filtrar las direcciones MAC. Así se contará con un control de todos los equipos de red que se conecten en. En general, el bridge, lo que hace es crear una liga lógica entre dos o más interfaces, el cual puede ser usado para separar el tráfico entre diferentes redes, y por supuesto filtrar los paquetes no deseados.

  Se debe crear el archivo **/etc/bridgename.bridge0.rules**, en el cual se debe indicar cuales son los dispositivos que se tienen que dejar pasar, es decir, se le tiene que indicar que los paquetes deben de pasar de una interfaz a la otra interfaz, y en el caso de querer bloquear cualquier otra interfaz también se debe indicar

con la siguiente línea: **block in on xl1,** con la cual se le indica que queda negada cualquier tarjeta que no se encuentre en la lista.

- Se tiene que activar el bridge, esto se hace con el comando brconfig, el nombre del bridge y el nombre de la tarjeta donde se quiere activar el bridge: **# brconfig bridge0 add xl1 up**
  Y para activar las reglas del bridge, se tiene que hacer con el mismo comando solo que se le tiene que indicar la ruta y el nombre del archivo que contiene las reglas del bridge:
  # brconfig bridge0 rulefile /etc/bridgename.bridge0.rules

- La herramienta packet filter, permite el filtrado de paquetes basados en el protocolo TCP/IP, que es el que se genera en la red en cuestión. Packet filter, es una herramienta que permite el bloqueo por protocolos, por puertos, paquetes, direcciones de origen o destino, y además genera bitácoras, para poder analizarlas y verificar su comportamiento en caso de existir algún comportamiento extraño o no esperado.
  Es en archivo /etc/pf.conf, donde predeterminadamente se pueden alojar las reglas de filtrado. De los aspectos importantes que se considera deben ser filtrados.
  Se debe usar la política prohibitiva, es decir, deberá estar todo bloqueado, y solo permitir paquetes de los protocolos que de acuerdo a las políticas de uso serán permitidos.

- El protocolo de correo (snmp puerto 25)

- De WEB y WEB seguro (puerto 80 y 443)

- No se recomienda permitir el tráfico del protocolo ICMP, ya que no es necesario, por que por la configuración que se hizo en el access point, la configuración de los usuarios, no permite ni siquiera este tipo de tráfico entre los usuarios de la red. Además que ya se explicaron las desventajas y vulnerabilidades que se pueden presentar en caso de permitir el uso de este protocolo.

- Se deben permitir los protocolos UDP y TCP, en el puerto 53 que va a permitir hacer consultas al DNS, lo cual es necesario para la salida a Internet.

- Permitir el puerto 67 y 68 de UDP, que es necesario para hacer la solicitud al servidor de DHCP. Sin embargo, como el servidor DHCP, estará perfectamente establecido, entonces, únicamente a la IP del servidor, hay que permitirle el puerto 67, que es el usa el servidor, todos los clientes usan el 68.

- El puerto 1812, que es el puerto que normalmente usa el servicio de RADIUS.

- Recordar que normalmente, se debe tener tráfico por puertos mayores a 1024, ya que ningún equipo será servidor, ni puede tener un rol que tenga que ver con un servicio dado por uno de los llamados puertos privilegiados. De igual forma el tráfico que sale de nuestra red, debe ir dirigido a puertos menores de 1024, los puertos privilegiados, claro, esto considerando la presencia de aplicaciones que se tengan que excluir específicamente de la regla.
- Otra de las consideraciones que se deben tener, es el protocolo de intercambio de archivos, es decir, considerar el hecho de que muchas páginas permiten la descarga de archivos o paquetes por medio de FTP. Sin embargo, este protocolo es inseguro, por definición, sin embargo, la recomendación no es bloquearlo completamente, sino, permitir conexiones activas, ya que la inseguridad del protocolo está basada en las sesiones pasivas que son permitidas.

- Las conexiones por el puerto 22, del protocolo SSH, son importantes, ya que muchos servicios de intercambio de archivos, también se llevan a cabo por medio de este protocolo, por lo que la única observación es que se cuente con la versión más reciente y la instalación de algunos parches de las aplicaciones o del mismo protocolo.

- Es importante mencionar que este archivo no es estático, es decir, las reglas pueden y deben cambiar, por que habrá aplicaciones que por definición de sus desarrolladores, usan puertos diferentes a los ya establecidos. Es por esta razón, que aparte de contar con una etapa de pruebas, para agregar y mejorar la configuración de las reglas, se debe estar al pendiente de las peticiones que algunos usuarios necesiten, y por supuesto la recomendación es contar con una buena bitácora y registro de todos los movimientos que se realicen en dicho archivo, y pedir una justificación válida al usuario que solicite el cambio o la nueva regla.

Se recomienda la colocación física del equipo donde sea configurado el firewall, en donde muestra la siguiente imagen:

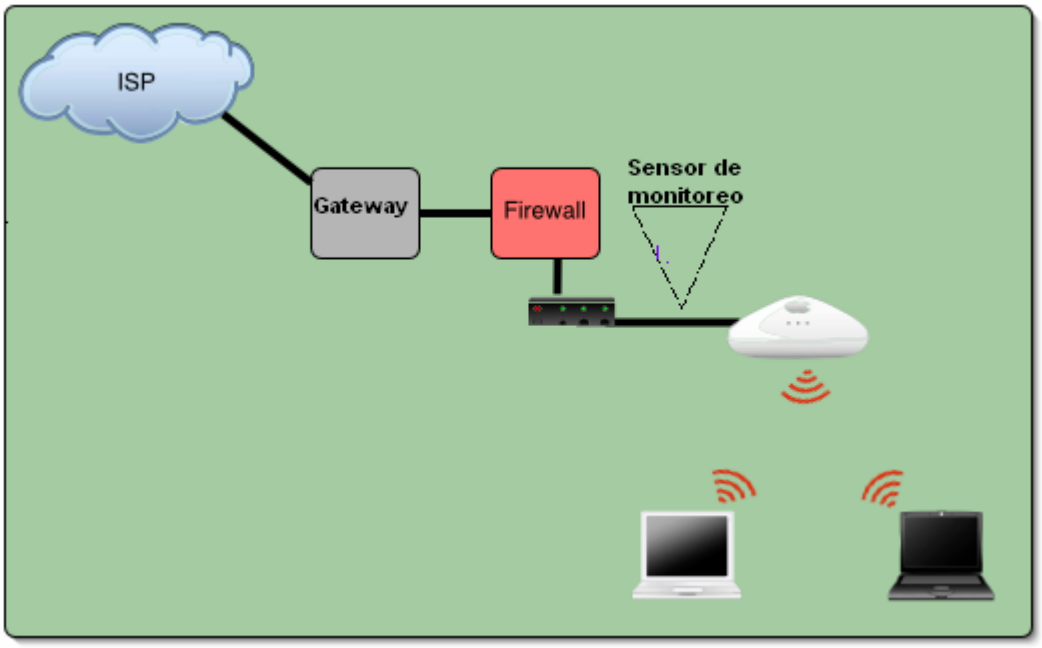


Imagen 5.7. Colocación del Firewall en la estructura de red

5.2.2.4 IDS (Sistema Detector de Intrusos)

Para la puesta en marcha de este mecanismo, se recomienda el uso de la familia de herramientas de SNORT, el ya conocido sistema para redes convencionales. En las redes ethernet, es muy usado, y se obtienen muy buenos resultados de él. Además de ser gratuito, y compatible con varias bases de datos para poder trabajar, es de configuración no tan sencilla, pero si cuenta con una interfaz muy amigable, entendible y que hace que el monitoreo del mismo se pueda llevar realizar de manera más sencilla.

Para el caso de las redes wireless, se cuenta con herramientas ya específicas para la tecnología. Las herramientas con las que cuenta, ya fueron mencionadas en este trabajo, sin embargo hay que mencionar que como administrador y/o encargado de la red, se deben configurar y aplicar en la red, ya que pueden dar información sobre las posibles, vulnerabilidades, amenazas, malas configuraciones o despistes que como administradores se puede no ver.

La configuración de este dispositivo, también es típicamente archivos de Linux, y se tienen que configurar las reglas para indicarle que tipo de alertas va a generar y a dónde las tiene que enviar, y en caso de presentarse un paquete con características no deseables, que hacer con él.

De entre las nuevas características que ya presenta esta herramienta en sus versiones más recientes, se encuentran:

- Es capaz de identificar un ataque de fragmentación de paquetes
- Detecta también la fragmentación de cadenas y el reensamblado de éstas.
- El porcentaje de shellcodes y código polimorfito que burlaban el mecanismo, ha bajado en gran porcentaje, lamentablemente, no se puede hablar de una solución al 100%.

Para la instalación de SNORT, es necesario descargarlo de http://www.snort.org/dowloads/snort-stable.tgz
Hacer la típica instalación de una aplicación de Linux, por medio de make y makefile. Realmente, lo tardado de su configuración, son las dependencias que puede tener de algunos paquetes en el equipo. Si se desea, también existe una versión que corre sobre sistemas BSD, sin embargo, se repite que no es recomendable tener estos mecanismos (firewall e IDS), corriendo en el mismo equipo, es mejor por separado.
No hay que olvidar que para llevar a cabo la detección de paquetes no deseados, tiene que monitorear o sniffear, por lo que La instalación de ls librería Libpcap es indispensable.

El equipo que se requiere, debe contar con:

- Sistema operativo instalado, basado en la plataforma UNIX, se recomienda usa la distribución DEBIAN.
- Que cuente con un procesador rápido y de alta capacidad.
- Memoria RAM, muy grande, se recomienda que sea la mayor cantidad posible.
- 2 Interfaces de red (NIC), rápida, de alto perfil, ya que se necesita que el análisis rápido para no detener el tráfico en este punto.
- Contar con espacio en disco, por el hecho del crecimiento y almacenamiento de las bitácoras.

Para correr SNORT, basado en su conjunto de reglas se hace con el siguiente comando:

```
snort -A full -c snort.conf
```

Las bitácoras están picadas por defecto en la siguiente ruta: /var/log/snort, sin embargo se puede personalizar esa ruta.

La recomendación de la mejor ubicación física en la red, es a un lado del firewall, ya que los dos tienen que trabajar en conjunto par lograr el mejor resultado. El problema es si viendo desde Internet, primero debe estar el firewall o el IDS, se recomienda que esta

decisión sea tomada dependiendo de si el switch de la red ethernet, permite el monitoreo o no de la red.

5.2.2.5 Políticas de Seguridad

En cuanto a la actualización de las políticas, se debe tomar en cuenta el desarrollo de políticas de uso y seguridad. Ya que aunque en el firewall se cuenta con reglas que se encargan de limitar y controlar las aplicaciones que se usan y el IDS, se encargará de los paquetes de tráfico que se permitirán o no, se debe contar con un documento que avale y respalde las acciones que se van a tomar.
Es decir, el documento donde se indican las reglas son las políticas y las acciones que se llevan a cabo para la aplicación de dichas políticas es la puesta en marcha y configuración de estos mecanismos.

Las políticas, además de indicar las medidas y normas, deben indicar también los derechos que los usuarios tienen, así como las sanciones a las que se harán acreedores en caso de incurrir en alguna falta.

Las políticas de la Facultad de Ingeniería, no son un documento hecho por que sí, es un documento, basado en estándares establecidos y con la aprobación de todo un consejo de profesionales en diferentes aspectos, que después de analizar las situaciones posibles, los riesgos, las consecuencias y las diferentes situaciones que se pueden presentar establecen una política, que cubre una norma, medida y/o acción. Por esta razón en esta sección únicamente se tocarán los puntos que a este punto de vista son muy importantes, o son de los puntos que no pueden dejar de tocarse en la reforma y actualización de las políticas.

A continuación se hará una propuesta de las políticas que se pueden considerar, tomando en cuenta los aspectos que se consideran necesarios en este proyecto.

- POLÍTICAS DE CUENTAS Y CONTRASEÑAS
  - → Las cuentas de usuario y las contraseñas e cada usuario, será proporcionada al activar la cuenta para hacer uso de las salas de cómputo de UNICA.
  - → Las cuentas son totalmente personales y no son transferibles.
  - → No se debe hacer mal uso de dicha cuenta, es decir, no se puede vender y no tiene costo alguno, bajo ninguna circunstancia.
  - → La cuenta caduca, cuando el usuario completó sus estudios y deje de ser alumnos inscritos de la Facultad de Ingeniería.

- POLÍTICAS DE CONTROL DE ACCESO

  → Los mecanismos y dispositivos que se implanten en la red son puestos en marcha y considerados por el administrador de la red y el personal de seguridad, por lo que ese equipo, es el encargado de la administración, monitoreo y mantenimiento de dichos mecanismos.

  → Se debe especificar que si bien es una red, los usuarios, hablando a nivel de equipos, no se pueden comunicar entre ellos, es decir, la red se denomina así por estar conectados a un solo dispositivo, sin embargo, no se va a compartir nada entre ellos, por cuestiones de seguridad de los mismo usuarios. Esto incluye servicio e impresión e intercambio de archivos entre otros.

- POLÍTICAS DE USO ADECUADO

  → Se debe recalcar que la finalidad y el principal objetivo del servicio de esta red, es de uso exclusivamente académico.

  → El uso adecuado de los recursos de la red, es decir, que por escrito se respalden todas las reglas con las que cuenta en firewall, para que no haya problema alguno sobre la claridad de éstas, se tienen que explicar lo más detalladamente posible.

  → Precisar el uso del software peer to peer, y de intercambio de archivos de música o software. Si bien se considera que en las reglas de firewall, se bloquea el posible uso de este tipo de software, también es cierto que la configuración de este tipo de software, cada vez se hace más fácil y engañosa, como para lograr un uso de estas herramientas.

  Si bien las desventajas de este software es la posible contaminación del equipo, descargando códigos maliciosos, virus, gusanos, spyware, etc, la principal razón por la cual no se deben usar en esta red, es la violación a la Ley Federal de Derechos de Autor, haciendo uso de archivos que no son de carácter gratuito o su uso no es el correcto indicado por el autor. Se tiene que recalcar que la importancia de este punto, radica en el hecho de que la violación es directamente de la UNAM como institución, no del usuario como persona.

  → Se prohibe cualquier actividad que represente un costo directo a la Facultad.

- POLÍTICAS DE RESPALDOS

  → Los respaldos de las bases de datos y de los servidores críticos de la red, como el servidor de RADIUS, es responsabilidad del administrador correspondiente de dicho servidor
  → Dichos respaldos deben ser almacenados, por las personas adecuadas, en lugares seguros y por supuesto alejados del cualquier riesgo de ser robados o riesgos naturales.
  Deben ser realizados en un periodo determinado de tiempo, no muy grande y no debe ser variable, es decir, se debe realizar, no importa si es día festivo o la hora de la comida.

- POLÍTICAS DE CORREO ELECTRÓNICO

  → Que da prohibido el envío de mensajes no solicitados (spam).
  → Atacar a usuarios, ya sea, enviando códigos maliciosos o contenido de amenazas.
  → Enviar copias de documentos y/o correos electrónicos como propios violando las leyes de autor.

- POLÍTICAS DE USO DE DIRECCIONES IP

  → Las direcciones IP, que serán proporcionadas por el DHCP, son exclusivas para los equipos que se den de alta en dicha red.
  → Queda prohibido extender el servicio de acceso a la red, por medio de una sola conexión inalámbrica.

- POLÍTICAS DE WEB

  → Las páginas WEB, que se permite visitar, este aspecto no es punidamente referente a las páginas de contenido pornográfico, también es referente a las páginas de donde se puede descargar software que caiga en la misma situación que el punto anterior.

  → Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en las políticas de uso aceptable.

5.3 Costo Estimado

El proyecto que en este trabajo se propone no está desarrollado aún, sin embargo como es una solución que se propone, también se tiene que aportar información sobre el posible costo que puede significar el proyecto. Se puede dar el caso de haber llegado a una solución tan ideal que en el costo represente su mayor desventaja. Es por esto, que a continuación se presenta una relación de los costos de mayor importancia para la puesta en marcha de este proyecto.

CONCEPTO	COSTO	Descripción
Access Point.	1 $899 USD 4 $2,597 USD	AIR-AP1231G-A-K9 802.11g IOS AP w/Avail CBus Slot, FCC Cnfg
Antenas Frecuencia 5 GHz	1 $209 USD 4 $841 USD	AIR-ANT5160V-R 5GHz 6dBi Omni Antenna w/RP-TNC connector
Antenas Frecuencia 2.4 GHz	1 $159 USD 4 $636 USD	2.4 GHz, 5.2 dBi Ceiling Omni Ant. w/RP-TNC Connector
Equipo para firewall	$ 10,440.29 MN	Marca Dell Dimension 5150 Procesador: Pentium Core duo Disco Duro: 80 GB RAM: 512 MB
Equipo para IDS	$ 11,744.09 MN	Marca Dell Dimension 5150 Procesador: Pentium Core duo Disco Duro: 80 GB RAM: 1 GB
Equipo para RADIUS Server	$ 10,440.29 MN	Marca Dell Dimension 5150 Procesador: Pentium Core duo Disco Duro: 80 GB RAM: 512 MB
Cableado hacia access point CABLE	Bobina de 505 mts. (1,300 pies) $ 2,358 MN	106836950 CABLE UTP CAT. 5, 4 Prs, 100 Mhz (Sólido) Color Gris
Cableado hacia access point Jacks AMP 406372-1	$13.50 MN c/u $ 67.50 MN	406372-1JACKS RJ45 CAT. 5 Color Marfil 5 Pzas.
Cableado access point Plugs AMP/TYCO 5-554720-3	$0.75 MN c/u $ 40.00 MN 50 pzas.	Conector modular macho (Plug) tipo RJ45, de 8 contactos. Con entrada para cable redondo
Cableado hacia access point CANALETA	$75.50 MN c/2m $ 9,815.50 MN. 130 pzas.	Canaleta de PVC rígido antiflama, con adhesivo de alta calidad, de 2 m de largo, diseñada para proteger cableado o alambrado en instalaciones eléctricas, de voz o datos, en color gris. Se utiliza para cables de hasta 40 vías o de 2 x 5 cm. @ 250 m

Cableado hacia access point Cinchos de Plástico LEGRAND LE-002	1000 cinchos $50.00 MN	Cincho sujetador de cable (Ty-rap) de nylon color natural de 2,5 mm de ancho y 96 mm de largo, con fuerza de tensión de amarre de 8 kg.
Interfaces de red extra	1 $300 MN 8 $2,400 MN	3com 10/100
Enlace	$0 MN	Se toma la infraestructura de Red UNAM
Misceláneos (táqueles, tornillos, abrazaderas, etc)	$ 2,000 MN	Accesorios necesarios para colocación y fijación de materiales y dispositivos
NO Break	$1,816.00 MN	Koblens. 2 horas de energía
Personal	$ 15,000 MN	Propinas, comidas, gastos personales

Tabla 5.1 Costos Estimados

SOFTWARE / TECNOLOGÍA	COSTO	DESCRIPCIÓN
DHCP	$0 MN	Protocolo que se configura sobre S.O. de distribución libre y gratuita OpenBSD
NAT	$0 MN	Servicio que se configura sobre S.O. de distribución libre y gratuita. OpenBSD
FREE RADIUS	$0 MN	Servicio que se configura sobre S.O. de distribución libre y gratuita. Debian
FIREWALL	$0 MN	Servicio que se configura sobre S.O. de distribución libre y gratuita. OpenBSD
IDS	$0 MN	Servicio que se configura sobre S.O. de distribución libre y gratuita. Debian
Sistema de Monitoreo	$0 MN	Servicio que se configura sobre S.O. de distribución libre y gratuita. Debian

Tabla 5.2 Costo de software/tecnologías

El número de equipos que se propone a usar son 3, esto por que los servicios de DHCP, NAT y el firewall, pueden ir sobre una sola máquina, esto, por que van instalados en el mismo sistema operativo. De contar con los recursos suficientes, es recomendable que se tenga una máquina dedicada exclusivamente para el firewall, sin embargo, aún sin ella se tiene un funcionamiento adecuado de la red.

En otro de los equipos, se recomienda la instalación del IDS en modo pacifico, esto es en el equipo que cuenta con mayor capacidad de

memoria RAM, por que es muy grande la cantidad de información que tiene que procesar. En el mismo equipo, se puede hacer la instalación de otro mecanismo de monitoreo del desempeño de la red, como complemento al trabajo que se llevará a cobo por el IOS de los AP's.

Ya en la tercera máquina, se tendrá únicamente el servidor de RADIUS, esto por que es una parte muy importante de la red, y además se debe recordar que es el equipo que tiene la información de los usuarios, tanto las credenciales como los certificados.

Se debe mencionar que los sistemas operativos que se recomiendan, no necesitan gran capacidad de máquina, de hecho, los equipos están sobrados en algunas propiedades como pueden ser disco duro, unidades de disco externo u otros atributos, sin embargo, el tamaño de la RAM, es el adecuado para realizar las tareas correspondientes.

En cuanto al número de las interfaces de red, es por que aparte de la que tiene el equipo, se recomienda que se tenga una tercera tarjeta para el monitoreo "remoto" de los equipos, esto no quiere decir, que ya el firewall deja de ser transparente, simplemente es un acceso por SSH, para lograr el monitoreo del equipo sin necesidad de estar físicamente en el cuarto de servidores.

Se comenta también que gastos como pueden ser el aire acondicionado, y la seguridad física de los equipos importantes, no se mencionan, por que UNICA, ya cuenta con al infraestructura necesaria que cubre estos aspectos. Incluso, el personal que lleve a cabo el trabajo de monitoreo y mantenimiento, ya es parte de UNICA, es decir, las tareas se dividirán entre los departamentos de Seguridad y Administración de Servidores respectivamente. Es por este motivo que no se considera un gasto extra de personas ajenas para la instalación y puesta en marcha de este proyecto.

TOTAL:	$ 135,664.67 MN

CAPÍTULO 6

RECOMENDACIONES DE BUENAS PRÁCTICAS DE SEGURIDAD.

Complementariamente a lo que se mencionó en los capítulos pasados, respecto a las acciones que se deben tomar para poder lograr un alto porcentaje de seguridad y adecuada administración de la red wireless de la Facultad de Ingeniería, se mencionarán algunas de las acciones e implementaciones que se pueden llevar a cabo, que si bien, algunas suenan bastante redundantes y básicas, si son necesarias o útiles, por que no entorpecen el uso de los usuarios y ayudan a llevar un adecuado control de las acciones.

BUENAS PRÁCTICAS DE SEGURIDAD A NIVEL DE RED

Es Necesario contar con un plan de mantenimiento de la red wireless, ya que hay que recordar que se está implantando con base en estándares internacionales, éstos cambian y se actualizan.
Además que recordar que el firmware de los dispositivos de red, se deben actualizar, ya que los IOS, pueden tener errores de programación y para resolverlos los fabricantes publican nuevas versiones. Estas nuevas versiones, también puede incluir, nuevas características y soporte para los protocolos de seguridad que van saliendo al mercado, cuentan con nuevas aplicaciones que ayudan a la mejor administración, como puede ser, una aplicación, para llevar un mejor control de los clientes, del monitoreo del tráfico, un Proxy, etc.

Para el caso de los dispositivos adicionales de red, como el firewall, es importante llevar un control sobre las reglas que se implementan en él, y un estricto control de las aplicaciones especiales, el nombre de la persona que hizo la petición para el uso de dicha aplicación y por supuesto, tener actualizado el sistema operativo sobre el que esté trabajando. Esta actualización, es referente tanto a la existencia de parches de sistema, como de las versiones de los sistemas operativos. De la misma manera, es fundamental llevar un control de las aplicaciones que están conviviendo en dicho equipo, ya que no serviría de nada tener un firewall totalmente controlado, un sistema operativo totalmente parchado y contar por ejemplo con una aplicación de base de datos que tenga vulnerabilidades y no contar con actualizaciones de dicha aplicación. En este mismo aspecto, se debe mencionar que si cabe la posibilidad de contar con un equipo dedicado a la tarea de ser firewall, no instalar aplicaciones donde los usuarios deban tener acceso como un servidor WEB o de base de datos, esto sería algo totalmente absurdo, ya que la tarea del firewall debe ser totalmente transparente y hasta es recomendable con cuente con un IP, para quedar exento de un posible ataque.

Para un Sistema Detector de Intrusos, la situación es muy parecida, de preferencia que sea un equipo dedicado solo a esa acción y también contar con las actualizaciones, en este caso, también

contar con las actualizaciones del software sobre el que está trabajando. Hay que recordar que las nuevas versiones, no solo representan un nueva interfaz, sino más ventajas en cuanto a las tareas que se pueden llevar a cabo, mejoras de seguridad en el propio software y convivencia con más aplicaciones, pero sobre todo para éste tipo de dispositivos, significa más capacidad de realizar bien su trabajo, es decir que sea un IDS, de nueva generación y que sea menos vulnerables a ataques o engaños que ya son conocidos.

De igual manera, para el conjunto de herramientas que se propone que se implemente hay que estar actualizando, y hacer pruebas de que su comportamiento es estable, que está dando los resultados que se esperan y sobre todo estar documentando y alerta sobre cualquier vulnerabilidad descubierta en dicha aplicación.

Servicios que serán usados como el DHCP o NAT, generan bitácoras, lo que nos lleva a recomendar que se tenga un control, revisión e interpretación de éstos archivos. Es decir, será necesario implementar un mecanismo que ayude a la revisión de bitácoras, incluso, ya existen mecanismos que hacen la revisión y generan y mandan alertas al correo del administrador para indicarle que se encontró algún comportamiento extraño o fuera de lo común.

Los servicios que serán usados, son configuraciones de archivos, como se ha mencionado, el equipo donde están alojados puede ser víctima de un ataque y alterar dichos archivos, o algunos otros archivos del sistema, para lograr crear un acceso permanente, ya sea al equipo o a la red, por esto, también se recomienda un mecanismo que ayude a verificar la integridad de los archivos, es decir, una vez que los servicios estén configurados y trabajando correctamente, se toma la "fotografía" del sistema, contra la que será comparado posteriormente, así en caso de algún cambio, también genera alertas y envía correos al administrador. Este tipo de mecanismo, tiene su eficacia basada en la configuración que haga el administrador, ya que como puede ser que mande un correo cada que ocurra un cambio, lo cual no es nada conveniente, ya que se llenará el correo del administrador, y éste dejará de ponerle atención, pensando que todas las alertas que envía son del mismo tipo, y sin importancia.

De igual forma la importancia de hace algo parecido con el tráfico de la red, la utilidad y los protocolos que más son usados, ya que como administrador siempre es importante contar con un parámetro real contra el cual comparar el estado actual del tráfico que presenta la red. Cuado se presenta una auditoria, este tipo de datos, y parámetros, es de mucha utilidad para los auditores, esto representaría un ahorro de trabajo para las dos partes. Este tipo de acciones es lo que se conoce de tipo Baseline.

A su vez, también se debe de implementar un mecanismo que force a los usuarios a cambiar su password cada determinado tiempo, preferentemente cada semestre, también que este password sea fuerte, es decir tenga una longitud mínima, que no sea una palabra de diccionario que sea fácilmente adivinable en un ataque de diccionario, y que el password no sea reutilizable mínimo durante 5 periodos de cambio.
Ya se hizo mención que la base de datos de usuarios con la que cuenta el sistema sea basado en la base de datos de usuarios de UNICA, esto es por que los administradores de esta sala ya tienen un mecanismo para la actualización de usuarios válidos en la Facultad con derecho de uso, así se puede asegurar que no se quedarán eternas cuentas que puedan significar una amenaza seria de seguridad. Así también se mencionó los access point que se recomiendan en el capítulo 6, puede tener una base de datos externa de los clientes de los que lleva el control por medio de dirección MAC, tomando en cuenta estas dos bases se debe crear una tercera donde se establezca la relación entre el usuario y su máquina, ya que de igual forma sino se actualizan esos datos, solo contaremos con cuentas inservibles de mucho tiempo.

Otro aspecto que es sumamente relevante es que como administrador, se debe tener la conciencia de que la tecnología inalámbrica, crece y cambia constantemente, es por esta razón que una vez que se asume la responsabilidad de administrarla, también se asume la responsabilidad de actualizarse constantemente, y estar dispuesto a hacer pruebas de los nuevos protocolos y evaluar la posibilidad de implementarlo, es decir, no por hecho de la implementación de ciertos mecanismos de seguridad ahora, quiere decir que esta implementación y configuración seguirá funcionando adecuadamente mucho tiempo, es decir, se debe estar conciente que se tiene una fecha de caducidad aproximadamente de 4 a 5 años.

Además como acciones complementarias, se debe tomar en cuenta las siguientes:

- Adquirir una comprensión en detalle de los riesgos potenciales del entorno (por ejemplo, malware, intrusos y desastres naturales)
- Realizar un análisis pro-activo de las consecuencias y mediciones de los posibles agujeros de seguridad en relación con los riesgos.
- La creación de una estrategia de implantación cuidadosamente planificada para integrar las medidas de seguridad dentro de todos los aspectos de una red corporativa, en base a esa comprensión y análisis.

Se tiene que recordar que una vez que todo está implementado, se tienen que llevar a cabo una serie de pruebas y aún después de abierta al público se tiene que llevar un monitoreo para verificar el nivel adecuado del firewall, así mismo es recomendable contar un mecanismo que ayude al análisis de los correos electrónicos, con esto no quiere decir que se tiene autorización para leer dichos correos, existen mecanismo, que a través de ciertos patrones ayudan a saber si el correo está infectado o es de tipo spam.

Si es posible, debe estar en contacto con otros administradores, o con personas autorizadas para llevar a cabo una auditoria y llevarla a cabo frecuentemente, para poder garantizar el buen funcionamiento y desempeño de la red.

Probablemente al inicio, en la puesta en marcha de la red, será necesario contar con personas que ayuden a la asesoría y configuración de algunos equipos, para que a los usuarios sea más fácil la introducción a la red, así mismo, estas personas, tendrán que estar correctamente capacitadas y de preferencia que exista un manual para la adecuada configuración de la red y las practicas de seguridad.

BUENAS PRÁCTICAS DE SEGURIDAD A NIVEL DE USUARIO

En cuanto a los usuarios, es necesario contar con su total participación, esto por que cada uno será administrador de su equipo, y no se tendrá un control de los programas y procesos que se tienen en cada equipo, por eso hay que hacer que los usuarios tengan un participación concienzuda. Para este aspecto se debe tener un cuidado especial, ya que hay usuarios que no son expertos, y el hecho de hablarles de ciertas actualizaciones y software y seguridad, puede hacer que se cree un pánico entre ellos, y que ellos mismos instalen software que sea dañino, haga lento a su equipo o se hagan una denegación de servicios ellos mismos.

Para un buen acercamiento con los usuarios será necesario dar una serie de pláticas y conferencias informativas de los servicios que se prestarán pero también de las acciones que serán necesarias que ellos lleven a cabo, estas acciones tendrán que ser publicadas y definidas en palabras sencillas y acciones de la misma forma. Todo lo publicado y dicho, aparte de sencillo debe ser concreto y haciendo conciencia de que las acciones son importantes de realizar pero no que son totalmente indispensables. Dentro de las acciones que se pueden sugerir:

1) **Antivirus:** Es necesario uno en su equipo y programarlo para que revise toda su máquina de forma periódica. No basta solo con la programación y no dejarlo actuar, ya que con frecuencia se programa en un horario donde la computadora no está encendida o son horas de trabajo y dicho análisis es cancelado. También es conveniente verificar periódicamente que está activado (muchos virus detienen los programas antivirus y dejan al equipo indefenso frente a otros ataques). Además, cada día aparecen virus nuevos y para poder protegerse de ellos, el antivirus necesita conocer la "firma", es decir, las características de esos virus. Por tanto, hay que actualizar el antivirus, ya sea manualmente, o bien de forma programada, frecuentemente o, si fuera posible, a diario.

2) **Firewall:** Un firewall o "cortafuegos" es recomendable la instalación de un software de este tipo si dispone de conexión a Internet, de cualquier tipo, ya sea por MODEM, ADSL, etc, pero sobretodo si la dirección IP es fija.

3) **Actualizar frecuentemente sus aplicaciones con los "parches de seguridad":** Las vulnerabilidades que se detectan en las aplicaciones más utilizadas (exploradores de Internet, procesadores de texto, hojas de cálculo, administradores de correo, etc.) suelen ser, un blanco habitual de los analistas de amenazas y vulnerabilidades, también de creadores de virus y código malicioso. Para evitarlo, una vez detectada una vulnerabilidad, las empresas fabricantes de 'software' ponen lo más rápidamente posible a disposición de sus clientes actualizaciones o "parches de seguridad" a través de Internet. Para que los usuarios estén protegidos, es necesaria la visita periódica al sitio de estas empresas e instalar dichas actualizaciones.

4) **Software o Aplicaciones Legales:** En necesario que todo el 'software' instalado en la máquina proviene de una fuente conocida y segura. No es conveniente instalar software pirata, ya que, además de transgredir la Ley, pueden contener virus, 'spyware' o archivos de sistema incompatibles con los del equipo, lo cual provocará inestabilidad en éste. Tampoco hay que confiar en los archivos gratuitos que se descargan de sitios WEB desconocidos, ya que son una potencial vía de propagación de virus. En cualquier caso, se debe analizar con el antivirus cualquier archivo que se descargue de Internet.

5) **Precaución con el correo electrónico:** Conviene analizar, antes de abrir, todos los correos electrónicos recibidos y sospeche de los mensajes no esperados o desconocido, incluso si provienen de

algún conocido. Los virus utilizan la libreta de direcciones de la máquina infectada para enviar sus réplicas y tratar de infectar a otros usuarios haciéndoles creer que están recibiendo un mensaje de un conocido.

6) **Reflexión con los archivos:** Se recomienda no descargar de Internet ni de adjuntos de correos electrónicos, ni distribuya o abra archivos ejecutables, documentos, etc. no solicitados. Para esto, se puede revisar con el antivirus cada nuevo elemento que se trate de incorporar a su máquina. No hay que abrir ningún archivo con doble extensión (como archivo.txt.vbs). En condiciones normales nunca se necesitan este tipo de archivos. Se puede configurar el sistema para que muestre las extensiones de todos los archivos.

7) **Copias de Seguridad:** Es importante realizar de forma periódica copias de seguridad de la información más valiosa. En caso de sufrir un ataque de un virus, algún gusano o una intrusión, las secuelas serán mucho menores si puede restaurar fácilmente los datos.

8) **Detención de Distribución:** No es bueno distribuir indiscriminadamente bromas de virus, alarmas, o cartas en cadena. Deben remitirse a los departamentos de informática o a centros especializados como el Centro de Alerta Antivirus. Debe comprobarse la veracidad de los mensajes recibidos y se puede ayudar a los demás colaborando en este aspecto. No se debe abrir ni contestar a los mensajes 'spam' (publicidad no deseada) ya que al hacerlo se reconfirma la existencia de la dirección.

9) **Mantenerse Informado:** Sobre todo de las novedades de seguridad informática, a través de los boletines de las empresas fabricantes de 'software', así como de los servicios de información y boletines del Centro de Alerta Antivirus, sobre las nuevas apariciones de virus informáticos. Si se sabe cómo actuar ante una situación de riesgo, se podrá minimizar al máximo las posibles pérdidas.

10) **Al regresar, utilizar la papelera:** Todos aquellos correos que resulten sospechosos, si no se conoce al remitente o presentan un 'Asunto' desconocido, deben ir a la papelera. Es importante vaciarla después.

CONCLUSIONES

El objetivo principal de este trabajo, es proponer la implementación de la red Wireless en la Facultad de Ingeniería, que garantice una buena administración y nivel de seguridad adecuado, de manera que para las personas indicadas las tareas sean llevadas a cabo de manera sencilla y rápida y que los usuarios cuenten con un servicio de calidad. Por lo que se puede señalar que el objetivo se cumplió.

El trabajo realizado para el alcance del objetivo se dividió en varias fases:

a) Investigación.
b) Evaluación de distintas soluciones que existen y/o aparecieron en el mercado
c) Implementación bajo un amiente virtual
d) Pruebas, tanto en el ambiente virtual como en el real
e) Realizar una documentación informal de la investigación y la implementación.

En la investigación se hizo el análisis de las necesidades de los usuarios de la Facultad, sus diferentes perfiles, el uso que le darían al servicio dependiendo de su perfil, cuales serían las principales ventajas de esta red sobre las soluciones ya existentes. En esta etapa se partió desde la investigación como tal, de qué es una red wireless, cuáles son sus componentes, sus características, la diferencia con las redes convencionales, tratando de que la respuesta fuera más allá de los cables.
Así se llegó al análisis de las posibles soluciones, tomando en cuenta lo existente en el mercado, sin embargo por tratarse de una nueva tecnología, se presentaron inconvenientes de la poca documentación a cerca de las soluciones o la aparición de nuevas versiones de software o hardware. En esta etapa, también apareció la evaluación en relación al costo / beneficio, es decir, en el mercado existen soluciones a un costo muy alto como son el firewall, el IDS o los mismo access point, por lo que se evaluaron las soluciones con las que se obtenían los resultados que cubrieran las necesidades anteriormente analizadas.

Por falta de recursos económicos, se llevó a cabo la implementación en un ambiente virtual. Se instalaron máquinas virtuales con los sistemas operativos correspondientes y ahí se realizó la configuración de dispositivos como el Firewall, el DHCP, NAT, RADIUS e IDS, las pruebas que se hicieron primero fue para una red convencional, y afortunadamente para ese ambiente, se obtuvieron los resultados esperados. Sin embargo para una red wireless se probó hasta la puesta en marcha de la red de ciencias de la tierra, sin embargo el AP, no es de la marca ni el modelo que aquí se propone, tampoco, se usa el protocolo de cifrado, únicamente de esta propuesta se usan los dispositivos de red ya mencionados, así se instalaron también las redes

de la sala de postgrado, de los laboratorio de ciencias de la tierra y de la dirección de la Facultad de Ingeniería.
Tiempo después se hizo la adquisición de los access point propuestos en esta tesis, con los cuales, se hicieron pruebas de cobertura y alcance de los access point y antenas, cabe mencionar que al inicio se consideraban 3 access point, y con estas pruebas se elevó el número de access point a 4, para lograr una cobertura adecuada y sobre todo el soporte del número de usuarios. Después de estas pruebas ya se hizo la implementación total de esta propuesta, ésta fue para un solo access point, y para pocas máquinas, luego de algunos ajustes en cuanto a la configuración de los equipos se llegó al resultado obtenido.

Finalmente, se realizó una documentación de la investigación, funcionamiento e implementación de los dispositivos de red que se instalaron, así como leer la documentación de los AP's y otros manuales de Cisco. Aparte del desarrollo de este trabajo, se cuenta con algunos manuales de las diferentes pruebas de herramientas, hasta que finalmente se llegó a esta solución, que desde el punto de vista de esta tesis es la mejor y la más viable.

- Firewall
- NAT
- DHCP, los 3 bajo sistema operativo OpenBSD
- IDS implementado con SNORT, bajo distribución Debian
- RADIUS, bajo la distribución Debian
- Access Point Cisco aironet 12000, series

Cabe mencionar que para la elección del access point, contó mucho la marca del dispositivo, por que se considera importante contar con el respaldo de una compañía seria, que para cuestiones de soporte o garantía responda adecuadamente, además de contar con actualizaciones para el IOS, aplicaciones y tecnología. Además después del análisis del funcionamiento y administración de dispositivos de diferentes marcas, se tiene que cubren diferentes aspectos, de seguridad, administración, cobertura y soporte de usuarios. Su firmware y las aplicaciones son sencillas para su manejo. El tiempo de vida aproximado para los dispositivos es de 4 a 5 años, sin embargo con una buena actualización y configuración la red puede cumplir su ciclo de vida funcionando de la manera más adecuada y sin llegar a conderarla obsoleta.

La seguridad informática, no es una moda, es una necesidad fundamental para el funcionamiento adecuado de los sistemas. La seguridad informática es una tarea que se debe llevar a cabo día con día, es un problema que va creciendo, se descubren nuevas vulnerabilidades, aparecen nuevos virus, gusanos, spyware, con nuevas características, por esto es necesaria la continua actualización.

En particular, para un servicio informático o tecnológico, como en este caso, el aspecto de la seguridad debe ser muy cuidado, ya que como prestadores del servicio, se debe poder garantizar la estabilidad del servicio, la privacidad de los usuarios de ésta, la disponibilidad de la red, en los horarios establecidos y una adecuada cobertura donde en realidad la necesitan.

El hecho de ser administrador de una red, trae consigo muchas responsabilidades, desde establecer una adecuada infraestructura, la administración de los dispositivos de red, estar al pendiente del adecuado funcionamiento de los equipos conectados en dicha red, en este caso el uso de tecnologías inalámbricas, se debe trabajar con los usuarios, para hacer conciencia de la responsabilidad en sus equipos, lo cual fuera de simplificar el trabajo, lo hace complejo, por que se debe cuidar el no caer en una paranoia de seguridad.

La implementación propuesta representa varias ventajas, como es la comodidad en los alumnos de ocupar su equipo portátil, la movilidad, tener acceso en cualquier lugar de la Facultad. Incluso para los alumnos que no cuentan con un equipo portátil, representa mayor oportunidad en el uso de las máquinas de la sala de Cómputo de UNICA, por que los alumnos con acceso a la Red Wireless ya no usarán dichas salas.

Otra ventaja, es la escalabilidad, respecto a una red convencional, se tiene que cada que se agrega un nuevo equipo a ella, se debe seguir un procedimiento, desde un puerto libre en el Switch, una IP asignada para el dispositivos, darla de alta con el administrador de la red, para que la registre en su control de máquinas, el lugar físico donde estará el equipo, ya que su acceso, tiene que ser estático por el cable; con el uso de la tecnología inalámbrica ya no es así, ya que cada que se quiera agregar un equipo a la red, únicamente se tiene que dar de alta en el sistema, y al conectarse usar su nombre de usuario y contraseña.

Con base en la profunda investigación que se llevó a cabo, se puede concluir que la tecnología inalámbrica, cubre adecuadamente la necesidad de una red de uso exclusivo de los alumnos de la Facultad de Ingeniería, y la adecuada implementación de ésta, junto con sus herramientas, hace que sea útil para los alumnos, y de fácil administración y control para el personal correspondiente encargado de estos aspectos.

La administración y la seguridad son dos aspectos diferentes, que tienen que trabajar en conjunto para llevar a cabo las tareas de cada uno de manera sencilla. Se debe tomar en cuenta que se trabaja en conjunto para lograr el bien de los usuarios.

Todas las recomendaciones y propuestas de este trabajo son para lograr un adecuado manejo de los dispositivos, usuarios, el mantenimiento y acciones constantes que se deben llevar a cabo, sean producidas de manera más simple.

Para el caso de la seguridad, que se pueda tener prevención y/o contención en el caso de un ataque o en presencia de tantas situaciones que resultan peligrosos para esta tecnología. Estos aspectos son importantes para dar el servicio y también representa la imagen de los Ingenieros en Computación de esta Facultad, y de la institución al no representar ningún peligro para otras redes vecinas o ajenas a ella.
De las aportaciones que se dan en este trabajo, se pueden encontrar:

- El diseño de la red, ya que se define la manera en que lógicamente funcionará y la localización física de los componentes de ella.
- La implementación de una firewall, el cual es transparente al usuario, no hace lento el tráfico y a bajo costo, significa la protección de los usuarios.
- Se considera el monitoreo de un IDS, para tener alertas sobre tráfico sospechoso e inusual de la red, ya que se pueden llevar a cabo acciones preventivas y correctivas antes de recibir las observaciones de los usuarios.
- El contar con políticas debidamente establecidas, que pueden informar y proteger tanto a usuarios como a administradores. Si bien ya se cuenta con un conjunto de políticas, las propuestas en este trabajo son para el caso puntual de la tecnología wireless.
- El análisis de las opciones que existen en el mercado para lograr la mejor solución para la red de la Facultad. Así mismo se establecen procedimientos para la implementación de cada una de las herramientas que forman parte de la solución.

APÉNDICE A

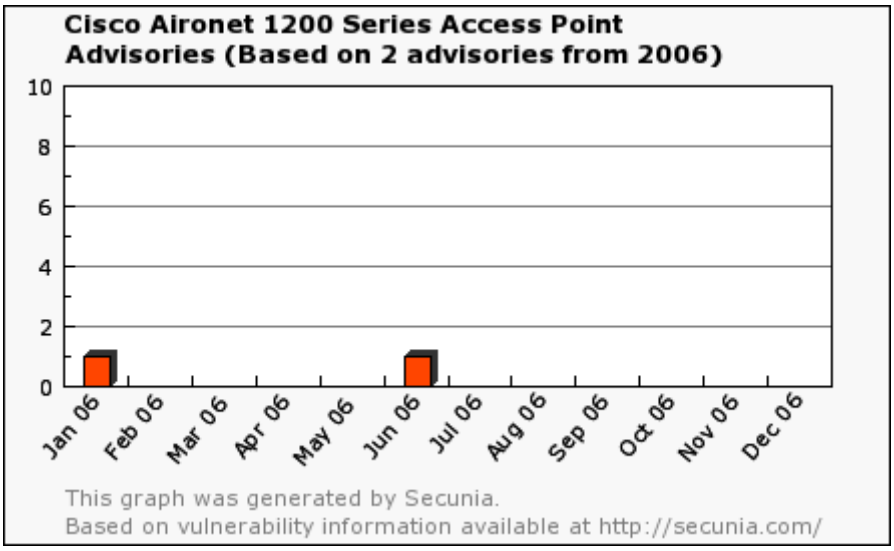
REPORTE DE VULNERABILIDADES DEL IOS DE LOS ACCESS POINT CISCO AIRONET 1200 SERIES

Como todos los sistemas operativos, el sistema operativo interno de los dispositivos Cisco, también tiene vulnerabilidades, que son descubiertas y reportadas en las principales páginas que reportan vulnerabilidades, amenazas y problemas de seguridad con diferentes aplicaciones o sistemas.
Por todo lo que se ha tratado sobre el tema de seguridad, es muy importante tener en cuenta, estos errores, y estar al pendiente del comportamiento estadístico. Con base en esta información y mucos otros aspectos que ya se mencionaron en su momento, fue como se recomendó e dispositivo, tanto por la marca, como por el modelo.

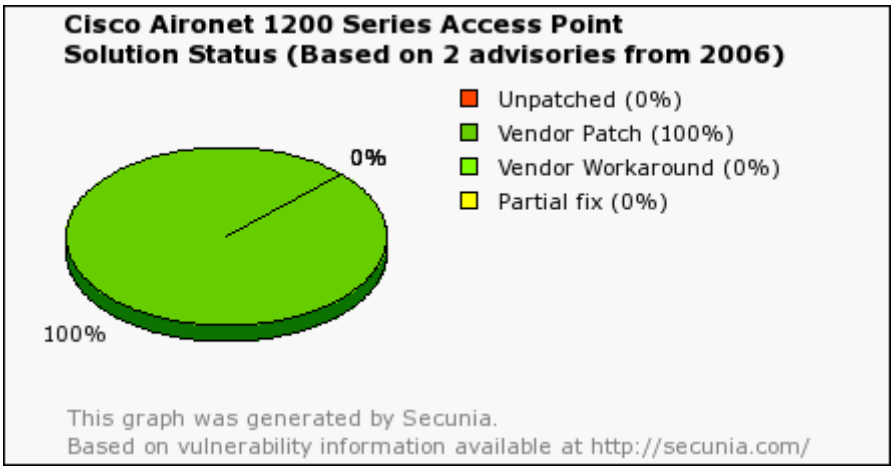
Uno de los sitios más serios y confiables en cuanto a la publicación de boletines de seguridad, alertas y reportes, es SECUNIA (www.secunia.com), es en este sitio donde se cuenta con un análisis sobre el comportamiento del IOS de este dispositivo.

La estadística que se analizó fue la del año en curso, así se puede observar lo siguiente:
En la página se hace la advertencia que el comportamiento del IOS, puede cambiar dependiendo de número de paquetes con que esté trabajando, la plataforma de los equipos y que hay situaciones fuera de lo común que puede alterar el comportamiento del IOS.

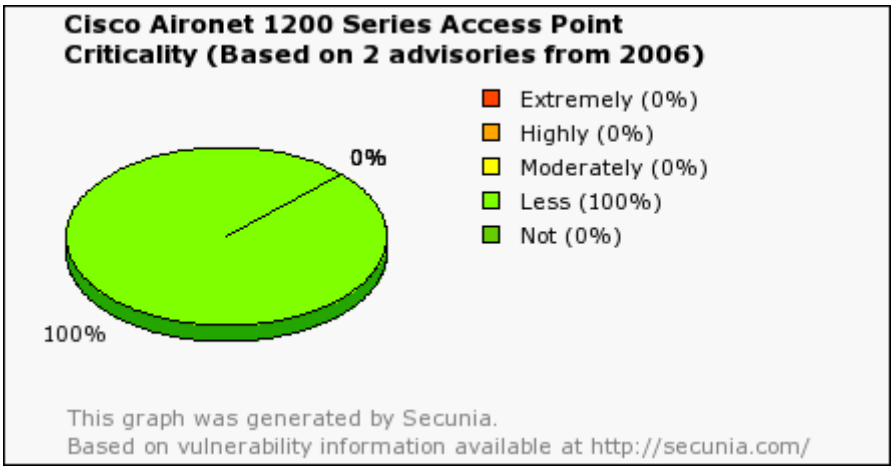
- Gráfica de Mes con Mes, esta gráfica, esta basada en le número de alertas que tuvo secunia con respecto al dispositivo.



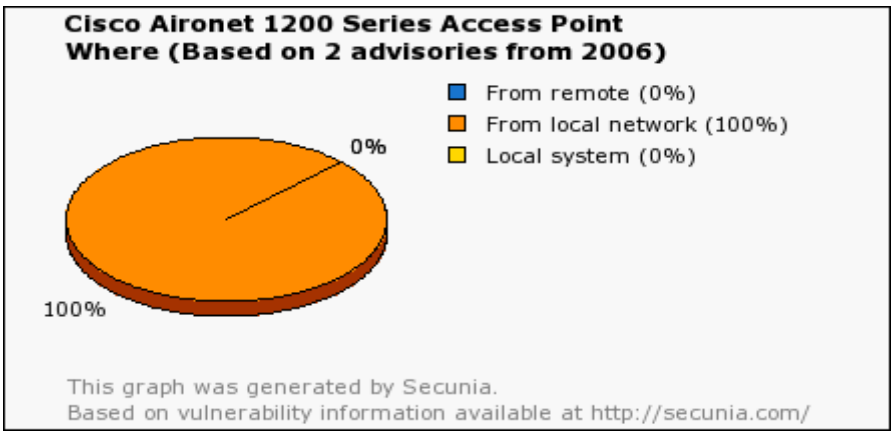
- Estado de solución. Es la gráfica que representa el número de soluciones que ofrece el fabricante respecto a los problemas del producto.



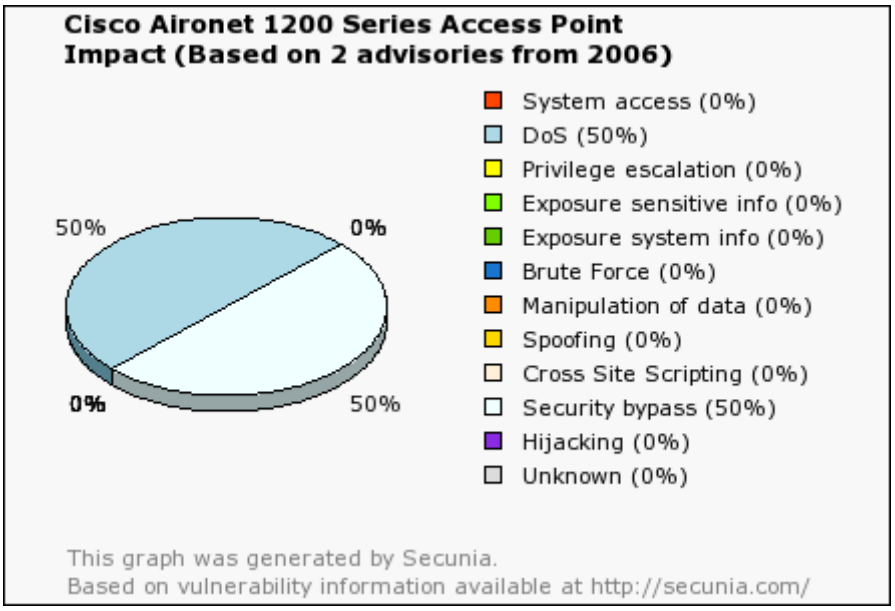
- Gráfica del porcentaje del nivel del problema: Clasifica los eventos reportados, dependiendo de su nivel de importancia.



- Gráfica de Dónde, es la gráfica que clasifica los eventos, dependiendo de la manera que se puedan llevar a cabo, remotamente o de forma local.



- Ya por último se presenta la gráfica del impacto, de acuerdo al alcance del evento, se clasifica de a cuerdo al impacto que puede alcanzar



Estos son los eventos reportados:
En Secunia, únicamente se han reportado 2 alertas sobre estos dipositivos, **Cisco Aironet 1200 Series Access Point,** durante el 2006.

Las dos ya fueron solucionadas como parches.

Cisco Wireless Access Point Web Management Vulnerability
Vendor Patch. Secunia Advisory 1 of 2 in 2006

Release Date:	**Secunia Advisory ID:**	**Solution Status:**
2006-06-29	SA20860	Vendor Patch
Criticality:	**Impact:**	**Where:**
	Security Bypass	From local network

Short Description:

Es una vulnerabilidad, la cual puede ser explotada por persosnas maliciosas, tiene que ver con la seguridad y restricciones del password.

Cisco Access Point ARP Memory Exhaustion Denial of Service
Vendor Patch. Secunia Advisory 2 of 2 in 2006

Release Date:	Secunia Advisory ID:	Solution Status:
2006-01-13	SA18430	Vendor Match
Criticality:	**Impact:**	**Where:**
	DoS	From local network

Short Description:

Es una vulnerabilidad reportada, la cual puede ser explotada por gente maliciosa y presentarse un DoS (Denial of Service).

En general, se pude comentar, que los eventos de seguridad que se presentaron para estos dispositivos, si son importantes, pero fueron resueltos rápidamente por la empresa, y su impacto no fue grande. Este hecho lejos de alejar la recomendación hecha, más bien acentúa la hecha a los administradores sobre estar informados y actualizados. Sin embargo hay que distinguir un aspecto muy importante. No se debe confundir ni pensar que el personal de seguridad únicamente se remite a la instalación de actualizaciones y parches, esta es solo una de las tareas que deben llevar a cabo, pero ni es la única ni la más importante, todas las acciones que tienen que llevar a cabo son complementarias unas de otras.

BIBLIOGRAFÍA Y MESOGRAFÍA

Capítulo 1

Bensky Alan, short range Wireless communication.

Capítulo 2

<Conceptos de redes>
Ing. Marco Antonio Vigueras Villaseñor. "Apuntes de clase de redes"

Gallo Michael and Hancock William. "Comunicación entre computadoras y tecnologías de redes". Ed. Thomson Learning. México, 2002

Capítulo 3

<Conceptos de Wireless>
Oullet Eric, Padjen Robert, Pfund Arthur, Building a Cisco Wireless LAN

http://cek.bitacoras.com/archivos/2004/06/03/wifi/

<Antenas>
Kraus. **Antenas Manual Book**. 3ª Edición. Mc.GrawHill.
http://www.canariaswireless.net/modules.php?name=News&file=article&sid=353
http://www.conceptronic.net/products.asp?p=C11iDTT
http://wireless.gumph.org/
http://www.aerialix.com/arlx-om2400.html

<Historia Wireless>
http://valenciawireless.net/weblog/vw/staticpages/index.php?page=20030624122328924

<Auditorias>
http://www.rociolopez.8m.com/

<Seguridad>
http://www.monografias.com/trabajos12/fichagr/fichagr.shtml
http://www.saulo.net/pub/inv/SegWiFi-art.htm

<Conceptos de Seguridad>
http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=7

<Articulo de redes inalámbricas y su problemática>
http://www.eghost.deusto.es/docs/WLAN_ArticuloRevistaESIDE_WLANyS uProblematica.pdf

Capítulo 4

Adam Engst; Glenn Fleishman. Introducción a las Redes Inalámbricas Ed. Anaya Multimedia

<Cuestiones de Salud por la frecuencia>
http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm

<Mecanismos de Seguridad>
www.wlana.org/learn/educate.htm
www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
www.intel.com/ebusiness/strategies/wireless/wlan/standards.htm
http://www.microsoft.com/spain/technet/seguridad/areas/administracion/clientes.asp

<Criptografía, Cifrado y Comunicaciones seguras>
http://www.microsoft.com/spain/seguridad/guidance/topics/cryptographyetc.mspx
http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF
http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf

<Portal Cautivo>
http://www.ciups.com
http://nocat.net

<Seguridad WEP>
http://www.cs.umd.edu/~waa/wireless.html
http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml/

<Ataques>
http://www.atc.uniovi.es/.../3iccp/2006/trabajos/wifi/
Warchalking. http://www.warchalking.org
WLAN Hacking.. http://www.wellenreiter.net/
AirJack. http://802.11ninja.net/airjack/
WEPCrack Project Info. http://sourceforge.net/projects/wepcrack
http://www.kismetwireless.net/
http://gpsdrive.kraftvoll.at/

<Seguridad WPA>
Authentication and Privacy. En ANSI / IEEE Standard 802.11, 1999 Edition.
http://standards.ieee.org/getieee802/download/802.11-1999.pdf
http://www.stargeek.com/item/20270.html
http://www.weca.net/OpenSection/pdf/WiFi_Protected_Access_Overview.pdf
http://www.open1x.org
Ponencias de :Toni de la Fuente [blyx.com], Ricardo Gallir, Diego Lendoiro (Inestable), Pau Oliva Fora
NoCatBOX HOWTO v1.4 : de Toni Diaz
http://nowired.com/madwifi/howto.pdf de Jorge R.

<Sniffer>
ftp://www6.software.ibm.com/software/developer/library/s−sniff.pdf
http://www.monkey.org/~dugsong/dsniff/
http://www.wi-fiplanet.com/tutorials/article.php/149207

Capítulo 5

Wheat Jeffrey, Hiser Randy, Tucker Jackie, Desing a Wireless Network

<Manual de WLAN>
http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp

<Administración WLAN>
http://www.maestrosdelweb.com/editorial/redeswlan/

Capítulo 6

<Listas e información de Seguridad>
http://www.cert.org
http://securityfocus.com

<Access Point, IOS, Aplicaciones>
Aironet Wireless LAN. Fundamentals and Site Survey. Student Guide. Volume 1 and 2
http://www.aironet.com
http://www.cisco.com

<Información de freeRADIUS>
RFC-2869: RADIUS Extensions
RFC- 2716: PPP EAP TLS Authentication Protocol
http://www.freeradius.org/doc/EAPTLS.pdf

http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO
http://blyx.com
http://www.open1x.org

<SNORT>
Manual FAQ SNORT. Descargado de www.snort.org
http://blyx.com

<Costos>
Parthner de Cisco
www.dell.com.mx

<Información Authpf>
http://www.openbsd.org
http://cvs.openbsd.org/es/
http://madridwireless.net
http://blyx.com
http://vklab.sinroot.net
http://www.geekspeed.net/wicap/

<Firewall>
http://openbsd.orf/faq/faq4.html
http://www.sorgonet.com/trashing/antenacd/

Capítulo 7

<Decálogo de Buenas prácticas>
http://www.securityfocus.com/seguridad/1062064166.html
http://www.seguridad.unam.mx/descarga.dsc?arch=424

<Recomendaciones de Seguridad>
http://www.microsoft.com/spain/technet/seguridad/recursos/masinfo/bpsegcorp.mspx
http://www.microsoft.com/spain/technet/seguridad/recursos/guias/recomendaciones.mspx

Apéndice A

<Estadísticas de Secunia>
http://secunia.com/product/1929/?task=statistics_2006