



FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES



TEMA

**Desarrollo de un manual interactivo como apoyo a la enseñanza aprendizaje en
instalación y configuración de Redes Inalámbricas para los estudiantes de la
Escuela de Informática**

Trabajo de Graduación presentado por:

Silvia Haydee Granillo Manzanarez

Karla María Martínez Rivas

Luis Ernesto Cardona Guadrón

Para optar al grado de:

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

Septiembre 2008

SAN SALVADOR, EL SALVADOR CENTROAMERICA

AUTORIDADES

LIC. JOSE MAURICIO LOUCEL

RECTOR

ING. NELSON ZARATE SANCHEZ

VICERRECTOR ACADEMICO

ING. LORENA DUQUE DE RODRIGUEZ

DECANO

JURADO EXAMINADOR

ING. RENE FABRICIO QUINTANILLA GOMEZ

PRESIDENTE

LIC. OMAR OSWALDO HERNANDEZ MARTIR

PRIMER VOCAL

ING. VICENTE ANTONIO ZARCEÑO JACO

SEGUNDO VOCAL

Septiembre, 2008

San Salvador, El Salvador, Centroamérica.

AGRADECIMIENTOS

A DIOS

Dedico el presente trabajo a mi Dios Todopoderoso, por haberme permitido llegar a culminar mi carrera, pues sin la ayuda de el nada de esto hubiera sido posible.

A MIS PADRES

Agradezco a mis padres Luz Evelia y Rene Granillo por su apoyo incondicional, su amor y su ternura, ya que son la única inspiración que me ayuda a seguir adelante, a mis hermanos, Alexander y Luís Alberto por todo su apoyo y su cariño que siempre me han brindado.

A MIS COMPAÑEROS DE TESIS

A mis compañeros de tesis, Karla y Luis ya que sin la ayuda de ellos este trabajo no hubiera sido posible.

A MI ASESOR

Así mismo le agradezco a nuestro asesor Ing. Vicente Antonio Zarceño Jaco, por sus constantes aportes en la realización de este.

Silvia Haydee Granillo Manzanarez.

AGRADECIMIENTOS

A DIOS: agradezco primeramente a Dios Por haberme permitido culminar mis estudios y haberme guardado y guiado a lo largo de mi vida.

A MI MADRE: María Carlota Rivas de Martínez aun que ya no este con vida este triunfo se lo dedico a ella; por haber estado apoyándome en momentos difíciles, ya que todo lo que soy se lo debo y siempre vivirá en mi corazón.

A MI PADRE: Ovidio Martínez Rodríguez por su apoyo incondicional por sus concejos, su paciencia, por su confianza y sobre todo por haberme permitido convertirme en una profesional.

A MI HERMANA: María jasmy Martínez Rivas por estar con migo en esos momentos difíciles por su apoyo incondicional por sus consejo y su paciencia.

A MI HERMANO: Leonel Martínez Rivas por la confianza y el apoyo brindado en estos años de mi vida.

A MI HIJA: Génesis Sucely Escobar Martínez ya que es uno los motivos mas grandes que me han permitido seguir luchando.

A MI ESPOSO: Juan Miguel Escobar por estar apoyándome en los momentos mas difíciles por apoyarme en lo largo de mi carrera.

A MI COMPAÑERO/A DE TESIS: Silvia y Luis por su confianza, paciencias por entenderme y el apoyo brindado a lo largo de la tesis.

KARLA MARIA MARTINEZ

AGRADECIMIENTOS

A DIOS: Doy gracias a Dios por haberme dado la oportunidad de poder seguir estudiando y ser mi ayuda y mi fortaleza mi soporte ante las adversidades.

A MIS PADRES: Que estuvieron al lado mío animándome, apoyándome con sus consejos sabios y haberme enseñado el temor a Dios instruyéndome en el camino recto.

A MI HERMANA: Que estuvo apoyándome en el desarrollo de la carrera, con su apoyo y consejos y haber estado a la par mía dándome ánimos para seguir adelante.

A MIS AMIGOS: Que estuvieron conmigo apoyándome y dando palabras de ánimo y dando sus consejos sabios y me daban ánimos para seguir adelante.

A MIS COMPAÑEROS DE TRABAJO: Que estuvieron conmigo en el desarrollo de mi carrera que fueron un pilar fundamental para la culminación de la carrera, que me daban consejos sabios.

A MIS MAESTROS DE LA UTEC: Que ayudaron a la formación en mi carrera que transmitieron sus conocimientos para hacerme un profesional.

A MI ASESOR: Que nos apoyo en el desarrollo de la tesis a darnos las observaciones necesarias para culminar con éxito la tesis y haber sido uno de los docentes que fueron parte de mi desarrollo profesional.

A MIS COMPAÑERAS DE TESIS: Que estuvieron a la par mía desarrollando la tesis que sin la ayuda de ellas no hubiera sido posible la culminación de la tesis

A LOS HERMANOS DE LA IGLESIA

Con su apoyo espiritual y oraciones que me sostuvieron a no desmayar.

Luís Ernesto Cardona Guadrón

INDICE

Introducción	i
--------------	---

CAPITULO I

GENERALIDADES DEL PROBLEMA

1.1	Situación Problemática	1
1.2	Enunciado Del Problema	2
1.3	Justificación	2
1.4	Objetivos	3
1.5	Alcances	4
1.6	Delimitación	4
1.7	Estudio de Factibilidad	5

CAPITULO II

MARCO TEORICO REFERENCIAL

2.1	Redes de Área Local (LAN)	8
2.2	Introducción a Las Redes de Área Local Inalámbrica (WLAN)	12
2.3	Principios De La Transmisión Inalámbrica	17

2.4	El Uso de Redes Inalámbricas (WLAN) En El Mundo	19
2.5	Tecnologías de Transmisión (Radio, Infrarrojo)	21
2.6	Radio	22
2.7	Métodos De Transmisión	24
2.8	Bandas De Frecuencia	27
2.9	Infrarrojo	28
2.10	Topologías	30
2.11	Tramas	32
2.12	Estándares WLAN	37
2.13	Mecanismos de Seguridad	44
2.14	Canales de Transmisión	47
2.15	Elementos que Integran una WLAN	55
2.16	Importancia de la Seguridad	61
2.16.1	Modo Ad-hoc y Modo Infraestructura	62
2.17	Principales Amenazas para la Seguridad de las WLAN	63
2.18	Políticas de Seguridad en las WLAN	64
2.19	Técnicas de Seguridad para Redes WLAN	68
2.19.1	Autenticación y Autorización de la Red	68
2.19.2	Protección de Datos de WLAN	70
2.19.3	Wpa y 802.11i	71
2.20	Instalación de las Tarjetas de Red	73
2.21	Nombres de las Redes Inalámbricas	85
2.22	Seguridad Inalámbrica	86

2.23	Redes de Área Personal Inalámbricas (Bluetooth)	93
2.23.1	Conceptos Actuales	95
2.23.2	Topología de Red Bluetooth	97
2.23.3	Seguridad Bluetooth.	101

CAPITULO III

PROYECTO TEMATICO

3.1	Planteamiento del Proyecto	105
3.2	Cronograma del Proyecto	109
3.3	Documentación Técnica	110
3.3.1	Software para crear Animaciones Flash	110
3.3.2	Software para Crear Cd-Dvds con Menús Autoejecutables	111
3.3.3	Software para Captura de Pantallas	114
3.4	Evaluación Técnica y Económica	115
3.5	Tecnología y Recursos Seleccionados	123
3.6	Presupuesto Proyecto	123
3.7	Oferta Técnica y Económica	125
3.7.1	Oferta Técnica	125
3.7.2	Oferta Económica	127

CAPITULO IV

PRESENTACION DE PROTOTIPO

4.1	Articulo de Socialización	129
4.2	Presentación del Prototipo (Power Point)	131
4.3	Evidencias del Proyecto	135
4.4	Conclusión	153
4.5	Recomendaciones	154
4.6	Anexos	155
4.7	Bibliografía	166

INTRODUCCIÓN

Hoy en día la Tecnología avanza a pasos agigantados con una rapidez indescriptible vivimos en un mundo automatizado, todo al alcance de nuestras manos con solo presionar un botón, estamos inmersos en un mundo lleno de retos y nuevas tecnologías, que hacen que estemos mejor comunicados donde quiera que estemos, con la introducción al mercado del internet vino a mejorar el medio por el cual nos comunicamos con todas las personas alrededor ya sea por e-mail o por paginas web informativas, negocios, deportes, turismo, estudios, etc._ Vino a mejorar los tiempos de respuesta de las compañías con sus clientes y así como la tecnología ha ido avanzando surgió una herramienta muy útil que liberaría el mundo de las redes informáticas cableadas, mejoraría la movilidad de los equipos, nos referimos a las redes inalámbricas el cual es el tema que desarrollaremos a continuación.

Como podemos ver las redes inalámbricas vinieron a apoyar a las oficinas que ya no estuvieran en un solo lugar encajonados a un espacio físico, sino que vino a liberar de ese confinamiento.

Ahora en día con el desarrollo de la tecnología y normas dictadas por la IEEE se crearon estándares para que pudieran funcionar las redes inalámbricas, y es así como han venido evolucionando las redes inalámbricas a tal grado que con una laptop nos podemos conectar a internet o a una red sin cables o también

utilizando teléfonos celulares con tecnología bluetooth que se utiliza en inalámbricas, así que el tema que nos lleva a estudio es la instalación y configuración de redes inalámbricas, como funcionan su instalación y configuración ponerlas en ejecución sirviendo al proceso enseñanza aprendizaje de las mismas.

CAPITULO I

GENERALIDADES DEL PROYECTO

1.1 SITUACION PROBLEMÁTICA

Las Redes Inalámbricas han tomado un papel muy importante en la industria de las Redes por lo cual es muy importante conocer sobre los diferentes elementos que interactúan en ella, sobre la tecnología, la instalación y la forma de operación de éstas; pero al tratar de profundizar sobre este tema se encuentra que no existe material didáctico y de fácil comprensión que contemple todo lo relacionado con la instalación y configuración de una red inalámbrica; ya que durante la carrera fue muy superficial lo adquirido en este campo tanto a nivel teórico como práctico.

Ampliando un poco mas sobre las practicas se encuentran grandes vacíos de tiempo, porque no hay disponibilidad en los laboratorios de redes, siendo a su vez un punto importante para el desarrollo del estudiante en el área de las redes inalámbricas ya que posteriormente se van a aplicar en el desarrollo laboral en cada una de las exigencias del diario vivir del profesional

1.2 ENUNCIADO DEL PROBLEMA

¿Como se puede apoyar al estudiante de Técnico en Ingeniería de Redes Computacionales a reforzar los conocimientos sobre la instalación y configuración de redes inalámbricas?

1.3 JUSTIFICACION

Considerando el problema de la enseñanza aprendizaje de redes inalámbricas surge la necesidad de crear un manual interactivo que tendrá como objetivo solucionar en gran parte los vacíos existentes del proceso enseñanza aprendizaje que vendrá a beneficiar en :

- Agilizar el aprendizaje del manejo de las redes inalámbricas a los estudiantes de la carrera de Técnico en Ingeniería de Redes Computacionales de la UTEC.
- Ayudar tanto al catedrático como al estudiante brindándole material de apoyo didáctico interactivo sobre redes inalámbricas
- Se tendrá un fácil acceso al manejo de la información de redes inalámbricas en un CD interactivo
- La investigación enriquecerá y fortalecerá los conocimientos que el estudiante necesita para incrementar su nivel académico

- El estudiante estará en la capacidad de implementar un buen sistema de seguridad sobre Redes Inalámbricas,

1.4 OBJETIVO GENERAL

Facilitar el aprendizaje de los alumnos de la carrera Técnico en Ingeniería de Redes Computacionales, en lo relacionado a la instalación y configuración de Redes Inalámbricas.

OBJETIVOS ESPECÍFICOS

- Investigar las diferentes herramientas aplicables para el diseño y desarrollo de materiales interactivos (CD'S interactivos)
- Crear un manual interactivo de estudio sistemático el cual contenga paso a paso procedimientos de fácil comprensión y aplicación en lo relacionado a la instalación y configuración de redes inalámbricas
- Proporcionar los mecanismos básicos de seguridad necesarios para implementar una red inalámbrica

1.5 ALCANCES

- Crear un CD interactivo de estudio sistemático que brinde un ambiente amigable y de fácil comprensión y que sea una herramienta útil para el docente y estudiante.
- La información teórica estará estrechamente relacionado con el material práctico
- Proporcionar material que muestre paso a paso todo el proceso de instalación y configuración de redes inalámbricas.
- Proporcionar los parámetros básicos de seguridad que se necesiten para configurar en una red inalámbrica.

1.6 DELIMITACION

GEOGRAFICO

El proyecto será llevado acabo para los estudiantes de la Escuela de Informática, Edificio Gabriela Mistral de la Universidad Tecnológica, ubicada en Calle Arce 1020

TEMPORAL

El proyecto se desarrollará en un periodo comprendido entre los meses de Febrero a Junio de 2008

ORGANIZACIONAL

Con el desarrollo del proyecto se beneficiaran los estudiantes y docentes de la carrera Técnico en Ingeniería de Redes Computacionales de la Facultad de Ciencias Aplicadas específicamente de la Escuela de Informática de la Universidad Tecnológica de El Salvador

ESPECIFICA

El CD interactivo se utilizará en el laboratorio de redes ubicado en la 5ª planta del edificio Francisco Morazán. Para que sea utilizado por los estudiantes que cursen alguna asignatura relacionada con las redes inalámbricas (diseño de redes, instalación de redes, mantenimiento de redes, nuevas tecnologías etc.

1.7 ESTUDIO DE FACTIBILIDAD

TECNICA

Para el estudio de factibilidad es necesario conocer los medios o los recursos que serán utilizados en el desarrollo del proyecto teniendo en consideración y estudio, que La Universidad Tecnológica cuenta con el equipo y las personas idóneas para poder dar a conocer el contenido del CD interactivo aplicarlo en la práctica.

Software	Papelería
Cámara de Video	Copias

Transporte	Impresiones
Acces Point	Gastos Generales
Computadora	

ECONOMICA

Para el desarrollo del CD interactivo será necesario contar con los siguientes recursos.

Recursos	Costo
Software	\$ 636.00
Papelería	\$ 100.00
Cámara de video	\$ 0.00
Copias	\$ 60.00
Transporte	\$ 100.00
Impresiones	\$ 50.00
Acces point	\$ 60.00
Gastos generales	\$ 80.00
Total	-----
	\$ 1,086.00

OPERATIVA

El objetivo fundamental de este proyecto es proporcionar una herramienta que proporcione nuevos conocimientos y a la vez refuerce lo concerniente a

instalación y configuración de redes inalámbricas en los estudiantes de Técnico en Ingeniería en Redes Computacionales.

CAPITULO II

MARCO TEORICO

2.1 REDES DE AREA LOCAL (LAN)

Una **red de área local**, o red local, es la interconexión de varias computadoras y periféricos. (*LAN* es la abreviatura inglesa de *Local Área Network*, red de área local'). Su extensión esta limitada físicamente a un edificio o a un entorno de pocos kilómetros. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta velocidad y topología.

Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.

Estaciones de Trabajo

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras. Esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun, etc.

Servidores

Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

Tarjeta de Interfaz de Red

Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. Las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes. A menudo se usan cajas externas para Mac's y para algunas computadoras portátiles. La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.

Son ocho las funciones de la NIC:

1. Comunicaciones de Host a Tarjeta
2. Buffering

3. Formación de Paquetes
4. Conversión Serial a Paralelo
5. Codificación y Decodificación
6. Acceso al Cable
7. Saludo
8. Transmisión y Recepción

Estos pasos hacen que los datos de la memoria de una computadora pasen a la memoria de otra.

Cableado

La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial.

Cable de par trenzado: Es con mucho, el tipo menos caro y más común de medio de red.

Cable coaxial: Es tan fácil de instalar y mantener como el cable de par trenzado, y es el medio que se prefiere para las LAN grandes.

Cable de fibra óptica: Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.

Equipo de conectividad

Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor.

Hubs o Concentradores: Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella.

Repetidores: Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.

Puentes: Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN.

Ruteadores: Los ruteadores son similares a los puentes, sólo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring.

Compuertas: Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Podrá tenerse, por ejemplo, una LAN que consista en computadoras compatibles con IBM y otra con Macintosh.

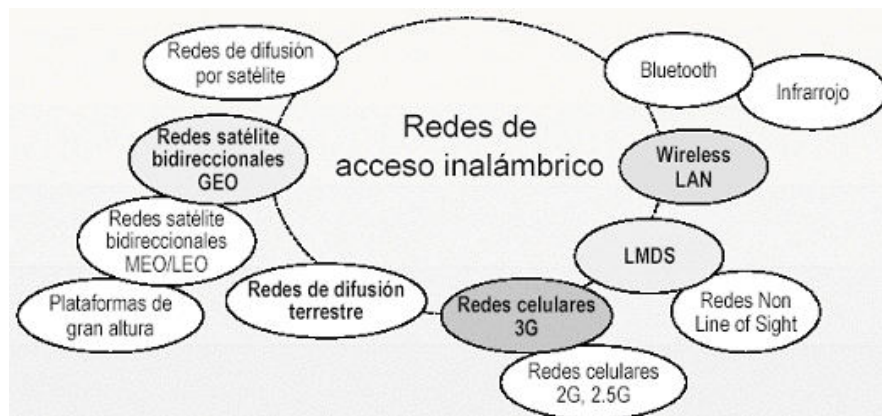
2.2 INTRODUCCION A LAS REDES DE AREA LOCAL INALAMBRICA (WLAN)

Una WLAN es un sistema de comunicaciones de datos que transmite y recibe datos utilizando ondas electromagnéticas (aunque también es posible con luz infraroja), en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (peer to peer), dentro de un edificio o en un área de cobertura. En EEUU han proliferado estas redes para acceso a Internet, en donde hay más de 4.000 zonas de acceso, y en Europa es previsible que pronto se extiendan. Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) para redes locales inalámbricas. Otras tecnologías como HyperLAN apoyada por el ETSI, y el nuevo estándar HomeRF para el hogar, también pretenden acercarnos a un mundo sin cables y, en algunos casos, son capaces de operar en conjunción y sin interferirse entre sí. Otro aspecto a destacar es la integración de las WLAN en entornos de redes móviles de 3G (UMTS) para cubrir las zonas de alta concentración de usuarios (los denominados hotspots), como solución de acceso público a la red de comunicaciones móviles.

Otra tecnología de acceso inalámbrico en áreas de pequeña extensión (PAN Personal Área Network) es Bluetooth, vista más como herramienta complementaria a WLAN. Bluetooth pretende la eliminación de cables, empleados en la conectividad del PC con sus periféricos, o proporcionar un medio de enlace entre dispositivos situados a muy pocos metros, sirviendo también como mando a distancia. Ambas tecnologías pueden coexistir en un mismo entorno sin interferirse gracias a los métodos de salto de frecuencia que emplean. Sus aplicaciones van en aumento y, conforme su precio se vaya reduciendo, serán más y más los usuarios que las utilicen, por las innegables

ventajas que supone su rápida implantación y la libertad de movimientos que permiten.

Las Redes Inalámbricas facilitan la operación en lugares donde los PC's no puede permanecer en un solo lugar, como en almacenes o en oficinas, así como en centro de difícil cableado interior. Actualmente no se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas, pero si pueden ser alternativa para el acceso en determinadas circunstancias. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica, pero tienen problemáticas asociadas a infraestructura, instalación y conservación. Las WLAN son un sistema de comunicación de datos flexible muy utilizado como una extensión de ésta, al ser posible combinar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo, pudiéndose desplazar con facilidad dentro del área deseada. Las LAN de corta distancia, son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, o centros para permitir acceso publico a Internet.



Las redes inalámbricas WLAN se diferencian de las convencionales Ethernet principalmente en la “Capa Física” y la “Capa de Enlace de Datos. Los dos métodos de implementación de la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja. Sin embargo esta última opción está en desuso y en la actualidad ya no se opera en este formato de transmisión. En la actualidad las redes WLAN se soportan exclusivamente en entornos de radio frecuencia en la banda ISM (2,45 GHz) y 5 GHz.

ORIGEN DE LAS WLAN.

El origen de las LAN inalámbricas o WLAN se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Posteriores investigaciones fueron realizadas tanto con infrarrojos como con microondas, bajo esquemas de transmisión de espectro ensanchado (SS, Spread Spectrum).

En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Commission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en SS, con las opciones DS (Direct Sequence) y FH (Frequency Hopping). La técnica de espectro ensanchado es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias

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

Más recientemente en los últimos 15 años, desde 1991, y de forma paralela al trabajo realizado por la IEEE en los Estados Unidos, la ETSI desarrolló sus propios sistemas inalámbricos, HIPERLAN e HIPERLAN2 dentro del Proyecto BRAN (Broadcast Radio Access Network). HIPERLAN fue desarrollado de 1991 a 1996, y HIPERLAN2, en el año 1999. Ambos han sido estandarizados tanto en su capa física como DLC (Data Link Control), permitiendo la coexistencia con cualquier tipo de tecnología de red y enlace existente en el mercado. Estos, son estándares inalámbricos de alta velocidad (hasta 20 Mbps y 54 Mbps) en la banda de 5GHz.

Gracias estos nuevos **estándares**, las redes inalámbricas evolucionan desde las prestaciones iniciales de 1 o 2 Mbps a las actuales que alcanzan 54 Mbps, con QoS e integración en nuevas redes como los son en las redes UMTS, GSM o IP. Un nuevo horizonte tecnológico y comercial se abre para estos sistemas, que han crecido de manera exponencial en los últimos 5 años.

Cómo trabajan las WLAN Red inalámbrica

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la

portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

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

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

Beneficios

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para conectar el computador, y los administradores de la red pueden poner a punto o aumentar la red sin instalar o mover cables. Veamos más ampliamente sus beneficios.

Visión general de los beneficios de una WLAN Frente a las redes tradicionales se tienen las siguientes ventajas en cuanto a productividad, comodidad y costos:

1. **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades. de servicio.
2. **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.
3. **Flexibilidad:** Permite llegar donde el cable no puede.
4. **Reducción de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
5. **Escalabilidad:** El cambio de topología de red es sencillo y trata de ser al igual pequeñas y grandes redes.

2.3 PRINCIPIOS DE LA TRANSMISION INALAMBRICA

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de

radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

- **De Larga Distancia.**- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Area Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.
- **De Corta Distancia.**- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: **Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares.** Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los

convencionales, ya que requieren circuitería especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

1. La carga de los teléfonos se termina fácilmente
2. La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
3. Las velocidades de transmisión son bajas.

Todas estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas, planos, etc. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas: **Red Pública De Conmutación De Paquetes Por Radio**. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencias restringidas por la propia organización de sus sistemas de cómputo.

2.4 EL USO DE REDES INALAMBRICAS (WLAN'S) EN EL MUNDO

El uso de las redes ha crecido y se está extendiendo por todo el mundo de forma notoria todo esto debido a que son eficaces ya que todos los usuarios

que están conectado a una red ya sea publica y privada pueden compartir los mismos datos, lo que ahorra dinero y mejora la productividad a mejores costos.

Anteriormente, los cables que conectaban a los equipos eran difíciles de colocar, resultaba antiestético, pero actualmente con las redes inalámbricas esto se ha vuelto mucho más sencillo y barato.

Las redes inalámbricas van ganado rápidamente adeptos como una tecnología y flexible, que permiten resolver los inconveniente derivados de la propia naturaleza del cable como medio físico de enlaces en las comunicaciones. Actualmente la mayor parte de las redes inalámbricas proporcionan un estándar de inconexión con redes cableadas en Ethernet o Token Ring.

El Espectro Electromagnético

Las ondas electromagnéticas cubren una amplia gama de frecuencias o de longitudes de ondas y pueden clasificarse según su principal fuente de producción. La clasificación no tiene límites precisos.

Región del espectro	Intervalo de frecuencias (Hz)
Radio-microondas	$0-3.0 \cdot 10^{12}$
Infrarrojo	$3.0 \cdot 10^{12}-4.6 \cdot 10^{14}$
Luz visible	$4.6 \cdot 10^{14}-7.5 \cdot 10^{14}$
Ultravioleta	$7.5 \cdot 10^{14}-6.0 \cdot 10^{16}$
Rayos X	$6.0 \cdot 10^{16}-1.0 \cdot 10^{20}$
Radiación gamma	$1.0 \cdot 10^{20}-....$

En la figura, se muestra las distintas regiones del espectro en escala logarítmica. En esta escala las ondas de radio y microondas ocupan un amplio espacio. En esta escala podemos ver todas las regiones del espectro, sin embargo, el tamaño relativo de las distintas regiones está muy distorsionado.

2.5 TECNOLOGIAS DE TRANSMISION (RADIO, INFRARROJO).

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

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

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

2.6 RADIO.

Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes:

- No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío.
- La velocidad es la misma que la de la luz, es decir 300.000 Km/seg.
- Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas.

No obstante las ondas electromagnéticas se atenúan con la distancia, de igual forma y en la misma proporción que las ondas sonoras. Pero esta desventaja es posible minimizarla empleando una potencia elevada en la generación de la onda, además que tenemos la ventaja de la elevada sensibilidad de los receptores.

Generación y propagación de las ondas

La antena es un conductor eléctrico de características especiales que debido a la acción de la señal aplicada genera campos magnéticos y eléctricos variables a su alrededor, produciendo la señal de radio en forma de ondas electromagnéticas.

Estas ondas se transmiten desde un punto central (la antena emisora) de forma radial y en todas direcciones, pero podemos diferenciar tres formas de transmisión:

- Onda de tierra: en principio las ondas de radio se desplazan en línea recta, atravesando la mayoría de los objetos que estén en su camino con

mayor o menor atenuación. Las pérdidas por dicha atenuación dependen de la frecuencia de la transmisión y de las características eléctricas de la tierra o el material atravesado. En términos generales a menor frecuencia mayor es el alcance de la onda y cuanto menor sea la densidad del material más fácil será atravesarlo.

Parte de esta onda es reflejada por la superficie terrestre.

- Onda visual o directa: es refractada en la baja atmósfera (refracción troposférica) debido a los cambios en la conductividad relativa en sus capas.
- Onda espacial: la atenuación en el aire es muy pequeña, lo que hace que la onda pueda alcanzar las capas altas de la atmósfera (ionosfera) y ser reflejada en su mayor parte de vuelta a tierra.

El mayor inconveniente que tendremos es que la transmisión de estos tres frentes no se hace a la misma velocidad, ya que las ondas reflejadas se retrasan con respecto a la onda directa, produciéndose un desfase que genera ruido (e incluso llegando a anular la onda si el desfase es de 180 grados). Para reducir este efecto hay que elevar la antena, ya que aumentando la altura se disminuye el ángulo de desfase.

Otro inconveniente es que en onda media la onda espacial no regresa a tierra durante el día pero sí durante la noche, debido a que la altura de la ionosfera se reduce. En cuanto a onda corta tenemos adicionalmente el inconveniente que a partir de una frecuencia crítica las ondas no son reflejadas a tierra y escapan al espacio.

2.7 Métodos de Transmisión

Hasta el momento hemos visto como se generan y propagan las ondas de radio, pero de nada sirve enviar una onda electromagnética si no lleva consigo el transporte de alguna información.

La modulación

Este sistema, que actualmente aún se emplea, parte de dos ondas:

- Onda portadora: es la encargada de fijar la frecuencia de transmisión y es la que alteraremos para que transporte la información que queremos.
- Onda moduladora: es la onda que queremos transmitir (voz, música, datos, etc.).

El proceso de modulación se basa alterar de una forma determinada la onda portadora en función de la onda moduladora, obteniéndose como resultado final la onda modulada que será radiada.

Para ello nos basaremos en los dos parámetros más importantes de una onda:

- La amplitud.
- La frecuencia.

En función del parámetro empleado vamos a tener dos posibles tipos modulación:

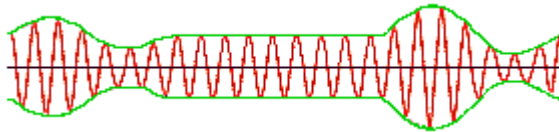
- Modulación en amplitud (AM).
- Modulación en frecuencia (FM).

Por supuesto existen más tipos de modulación, pero solamente tienen interés para transmisión radioeléctrica estas dos.

Modulación en amplitud (AM)

La modulación en amplitud fue el primer método de transmisión por radio.

Se basa en variar la amplitud de la onda portadora en función de la amplitud de la onda moduladora, obteniendo como resultado una onda modulada que contiene a la moduladora. Si unimos los extremos de la onda modulada obtendremos la señal moduladora y su simétrica (trazado en verde en el siguiente gráfico):



Un parámetro importante es el porcentaje de modulación, que indica la amplitud mínima o nivel cero de la onda modulada. Una modulación al 100% indica que la amplitud mínima será cero.

Optimización de la potencia

Como consecuencia de todo lo anterior vamos a obtener que en el mejor de los casos (porcentaje de modulación del 100%) la onda portadora consume el 50% de la potencia y cada banda lateral un 25%. Esto se resuelve filtrando la onda modulada antes de emitirla, con lo que nos situamos en uno de los siguientes sistemas:

- Modulación en doble banda lateral (DSB): se suprime la frecuencia central (portadora).

- Modulación en banda lateral única (BLU o SSB): suprime la portadora y una de las bandas laterales.
- Modulación en banda lateral vestigial (BLV): se suprime una parte de una de las bandas laterales. Este sistema se emplea en imagen de TV (vídeo).

Empleando uno de los sistemas anteriores obtendremos un mayor aprovechamiento de la potencia y ocuparemos un menor ancho de banda.

Modulación en Frecuencia (FM)

La modulación en Frecuencia es la técnica de transmisión por radio más popular actualmente. La FM es tan popular porque es capaz de transmitir más información del sonido que queremos transmitir, ya que en AM si se transmiten sonidos que están a frecuencias muy altas se consume un gran ancho de banda.

La modulación en frecuencia se basa en variar la frecuencia de la portadora con arreglo a la amplitud de la moduladora.

Supongamos que tenemos una señal moduladora cuya máxima amplitud es de 1V (valor de pico) y una onda portadora de 1000 KHz. Si suponemos que para este valor de amplitud la frecuencia de la portadora se desvía 15 KHz (simétricamente, es decir +15 KHz y -15 KHz), conforme oscile la señal moduladora la frecuencia de la portadora oscilará entre 985 KHz y 1015 KHz, ocupando un ancho de banda de 30 KHz.

En este sistema de modulación también tenemos un problema práctico, y es que rara vez el ancho de banda de la transmisión es inferior a diez veces el de la señal moduladora.

2.8 Bandas de Frecuencia

Internacionalmente se han dividido todo el espectro de frecuencia en las denominadas bandas de frecuencia. Esto se hace así para poder delimitar el acceso de los usuarios a estas bandas. Hay que mencionar que esta clasificación no es global y que algunos países difieren en su delimitación, pero en general podemos aceptarlas como generales

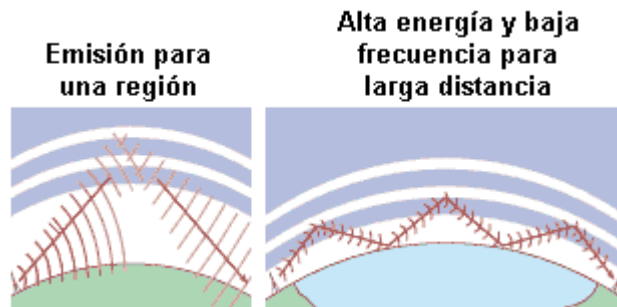
Conceptos básicos

Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes:

- No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío.
- La velocidad es la misma que la de la luz, es decir 300.000 Km/seg.
- Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas.

No obstante las ondas electromagnéticas se atenúan con la distancia, de igual forma y en la misma proporción que las ondas sonoras. Pero esta desventaja es posible minimizarla empleando una potencia elevada en la generación de la onda, además que tenemos la ventaja de la elevada sensibilidad de los receptores.

Transmisión a larga distancia



Basándonos en el efecto de refracción en la ionosfera y en la capa terrestre es posible transmitir a largas distancias. Para ello debemos emplear ondas de gran energía y de baja frecuencia.

2.9 INFRARROJO.

Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita “ver” al otro para realizar la comunicación por ello es escasa su utilización a gran escala.

Esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos (Bluetooth, Wireless, etc.).

Usos

Se utiliza principalmente para realizar intercambio de datos entre dispositivos móviles, como PDA's o móviles, ya que el rango de velocidad y el tamaño de los datos a enviar/recibir es pequeño. Adicionalmente, se puede usar para jugar juegos de dos jugadores.

Existen 3 Tipos

- Punto a punto
- Cuasidifuso A
- Difuso

En el modo punto-a-punto

Los patrones de radiación del emisor y del receptor deben de estar lo más cerca posible y que su alineación sea correcta. Como resultado, el modo punto-a-punto requiere una línea-de-visión entre las dos estaciones a comunicarse. Este modo, es usado para la implementación de redes Inalámbricas Infrarrojas Token-Ring. El “Ring” físico es construido por el enlace inalámbrico individual punto-a-punto conectado a cada estación.

Modo Cuasi-difuso

Son de emisión radial, es decir, que cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula. En el modo cuasi-difuso las estaciones se comunican entre si, por medio de superficies reflectantes. No es necesaria la línea-de-visión entre dos estaciones, pero sí deben de estarlo con la superficie de reflexión. Además es recomendable que las estaciones estén cerca de la superficie de reflexión, ésta puede ser pasiva ó activa. En las células basadas en reflexión pasiva, el reflector debe de tener altas propiedades reflectivas y dispersivas, mientras que en las basadas en reflexión activa se requiere de un dispositivo de salida reflexivo, conocido como satélite, que amplifica la señal óptica. La reflexión pasiva requiere más energía, por parte de las estaciones, pero es más flexible de usar.

Modo Difuso

El poder de salida de la señal óptica de una estación, debe ser suficiente para llenar completamente el total del cuarto, mediante múltiples reflexiones, en paredes y obstáculos del cuarto. Por lo tanto la línea-de-vista no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación, sin embargo esta flexibilidad esta a costa de excesivas emisiones ópticas. Por otro lado la transmisión punto-a-punto es el que menor poder óptico consume, pero no debe de haber obstáculos entre las dos estaciones. En la topología de Ethernet se puede usar el enlace punto-a-punto, pero el retardo producido por el acceso al punto óptico de cada estación es muy representativo en el rendimiento de la red. Es más recomendable y más fácil de implementar el modo de radiación cuasi-difuso. La tecnología infrarroja esta disponible para soportar el ancho de banda de Ethernet, ambas reflexiones son soportadas (por satélites y reflexiones pasivas).

2.10 TOPOLOGIAS

BSS, IBSS y ESS

IEEE 802.11b dispone de dos modos de radio posibles: **BSS e IBSS**, **INCOMPATIBLES** entre **BSS** es el modo de operación en el que un punto de acceso actúa como puerta de enlace entre una red inalámbrica y una red cableada, los nodos que pertenecen a la red inalámbrica, los

Clientes de *BSS*, establecen la comunicación con el punto de acceso y éste, actúa como un puente entre las dos tecnologías de red.

La segunda aplicación en importancia de las que se describen en el estándar IEEE 802.11 utiliza "puntos de acceso". Los puntos de acceso son componentes de red que controlan y gestionan toda la comunicación que se

produce dentro de una célula LAN inalámbrica, entre células LAN inalámbricas y, finalmente, entre células LAN inalámbricas y otras tecnologías LAN. Los puntos de acceso garantizan un empleo óptimo del tiempo de transmisión disponible en la red inalámbrica.

Ventajas:

- Incluso las estaciones que no pueden "verse" entre sí directamente se pueden comunicar
- Simple integración en estructuras de cable ya existentes

Inconvenientes:

- Coste más elevado del equipo
- Instalación y configuración más complejas

La instalación básica, compuesta por un solo punto de acceso y los sistemas inalámbricos conectados, se denomina Basic Service Set (BSS). Debido a que todavía no se ha estandarizado ningún protocolo de enrutamiento para la itinerancia, es importante que los puntos de acceso instalados sean de un único fabricante.

ESS es un conjunto extendido de **BSS**, es decir, los servicios que se ofrecen cuando existen más de un punto de acceso de tal forma que los clientes pueden unirse a cada punto de Acceso permitiendo la movilidad.

IBSS es un servicio básico entre iguales, en este modo dos clientes se pueden comunicar entre

Sí sin necesidad de que exista un punto de acceso, basta que ambos dispongan de tarjetas de red compatibles para lograr la comunicación, sería el equivalente a conectar dos *pc's* con

Tarjetas de red *Ethernet* mediante un cable cruzado, no se necesitan, *hubs*, *switches* ni otros dispositivos.

Además si uno de los clientes que operan en *IBSS* dispone de conexiones con otras redes,

Puede proporcionar acceso a las mismas actuando como reenviador o puente de conexión.

Es necesario configurar el protocolo *802.11b* para trabajar en *BSS* ó *IBSS*, pero no se puede trabajar en los dos modos de forma simultánea... o uno o el otro, pero no los dos a la vez.

Tanto *BSS* como *IBSS* admiten el cifrado y codificación **WEP** de clave compartida.

Lo más habitual es disponer de topologías con uno o varios *BSS* que brindan conectividad a sus respectivos clientes.

Una limitación de las comunicaciones *IBSS*, a parte de que sólo pueden comunicarse dos nodos entre sí, es que si usamos tarjetas de diferentes fabricantes, pueden existir

Incompatibilidades, si bien, con la expansión de las redes *802.11b*, cada fabricante han

Contribuido en la compatibilidad con el protocolo y podemos decir que hoy en día se certifica la conectividad de tarjetas que operan en *802.11b*.

Podrás encontrar también el modo *IBSS* como modo **Ad-Hoc o Ad-Hoc Demo**, son otras formas de llamar al modo de operación *IBSS*.

2.11 Tramas 802.11

El estándar 802.11 define varios tipos de tramas cada de las cuales tiene un objeto específico. Hemos visto anteriormente que tenemos que anunciar los puntos de acceso, asociar estaciones, autenticar clientes y otras funciones. Todas estas funciones normalmente se gestionan mediante unas tramas especiales, a parte de las tramas propias de transmisión de datos. Podemos

clasificar las tramas dependiendo de la función que desempeñan. Tenemos tramas de datos, las que transportan la información de capas superiores, tramas de gestión que permiten mantener las comunicaciones y tramas de control para, como su nombre indica, controlar el medio.

Cada trama contiene distintos campos de control, que incluyen por ejemplo el tipo de trama, si WEP está activo, si está activo el ahorro de energía, la versión del protocolo 802.11. Una trama 802.11 también incluye las direcciones MAC de origen y destino, un número de secuencia, un campo de control y el campo de datos.

Tramas de gestión

Las tramas 802.11 de gestión son las que permiten mantener comunicaciones a las estaciones inalámbricas y tenemos distintos tipos:

Trama de autenticación

Ya habíamos visto que la autenticación es el proceso para comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. El adaptador cliente inicia el proceso enviando al punto de acceso una trama de autenticación que contiene su identidad en el campo de datos.

El diálogo que se establece con las tramas de autenticación depende del sistema de autenticación que use el punto de acceso, si es abierto o con clave compartida. Cuando se trata de sistemas abiertos, el cliente sólo envía la trama de autenticación y el punto de acceso responde con otra trama de autenticación que indica si acepta o rechaza la conexión. En el caso de la autenticación de clave compartida, el punto de acceso tiene que comprobar que la estación tiene la llave correcta por lo que tenemos dos tramas de autenticación más en el diálogo, una que envía el punto de acceso con un texto para que lo cifre la

estación con su clave y otra de respuesta de la estación cliente con el desafío cifrado. Esto ya estaba descrito en la función de autenticación.

Trama de Desautenticación

Es una trama que envía una estación a otra cuando quiere terminar las comunicaciones.

Trama de Solicitud de Asociación

Este tipo de trama la utiliza la estación cliente para iniciar el proceso de asociación. Ya hemos visto que la asociación es un proceso por el cual el punto de acceso reserva recursos y sincroniza con una estación cliente. La asociación la inicia el cliente enviado al punto de acceso una trama de solicitud de asociación y el punto de acceso establece un ID de asociación para identificar al cliente y le reserva memoria.

Las tramas de asociación contienen los datos necesarios para esta función como son el SSID de la red, las tasas de transferencia, etc. En la función de asociación se define con más detalle el mecanismo de asociación.

Trama de Respuesta de Asociación

Este tipo de trama la utilizan los puntos de acceso para responder una solicitud de asociación. Esta trama puede contener si se acepta o rechaza la asociación. Si se acepta la asociación la trama también incluye el ID de asociación y las tasas de transferencia admitidas.

Trama de Solicitud de Reasociación

Cuando un cliente asociado con un punto de acceso se desplaza al radio de cobertura de otro punto de acceso de la misma red con mejor señal intenta

establecer una reasociación._ La reasociación implica que los puntos de acceso coordinen los buffer. Como era de esperar, para establecer una reasociación con un nuevo punto de acceso, el cliente le envía una trama de reasociación.

Trama de Respuesta de Reasociación

La trama de respuesta de reasociación es similar a la trama de respuesta de asociación, al fin y al cabo, lo que hacer es asociar con un nuevo punto de acceso.

Trama de Desasociación

Es una trama que puede enviar un estación cuando va a cerrar sus conexiones de red. Esta trama permite que el punto de acceso pueda liberar los recursos que tiene asignado a la estación durante el proceso de asociación.

Trama Beacon (baliza)

Un punto de acceso envía tramas beacon periódicamente para difundir su presencia y la información de la red, el SSID, etc, a las estaciones clientes en su radio de cobertura. Las estaciones pueden obtener lista de puntos de acceso disponibles buscando tramas beacon continuamente en todos canales 802.11. Las tramas beacon contienen la información necesaria para identificar las características de la red y poder conectar con el punto de acceso deseado.

Trama de Solicitud de Prueba

Las estaciones utilizan tramas de solicitud de prueba cuando necesitan obtener información de otra estación, por ejemplo obtener una lista de puntos de acceso disponibles.

Trama de Respuesta de Prueba

Esta trama es la respuesta de una estación a una solicitud. Esta trama contiene la información necesaria como por ejemplo las tasas de transmisión.

Tramas de Control

Las tramas 802.11 de control se utilizan para colaborar en la entrega de tramas de datos entre estaciones.

Trama Request to Send (RTS)

Se utilizan para reducir las colisiones en el caso de dos estaciones asociadas a un mismo punto de acceso pero mutuamente fuera de rango de cobertura. La estación envía una trama RTS para iniciar el diálogo de comienzo de transmisión de una trama.

Trama Clear to Send (CTS)

Las estaciones utilizan las tramas CTS para responder a una trama RTS para dejar el canal libre de transmisiones. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir el tiempo necesario para transmitir la trama.

Tramas Acknowledgement (ACK)

Las tramas ACK tienen como objetivo confirmar la recepción de una trama. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos.

Tramas de datos

Evidentemente existen tramas de datos que son las encargadas de transportar la información de las capas superiores.

2.12 ESTANDARES WLAN

¿Qué es un estándar?

Antes de comenzar a hablar de estándares inalámbricos, nos gustaría introducir el concepto de “estándar”. ¿Qué es un estándar por definición y por qué los estándares son importantes?

“Un sistema de reglas, condiciones o requerimientos que atañen a las definiciones de los términos; clasificación de los componentes; especificación de materiales, prestaciones u operaciones; delimitación de procedimientos; o medidas de la cantidad y calidad en la descripción de materiales, productos, sistemas, servicios o prácticas”

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

Los estándares WLAN principiaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original, incluyendo 802.11^a y 802.11b. La siguiente tabla contiene las variantes relacionadas al estándar 802.11.

Estándares para redes inalámbricas

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integrales –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

La especificación 802.11b fue ratificada por el IEEE en julio de 1999, y opera en un ancho de banda que abarca las frecuencias dentro del rango de 2.4 a 2.497 GHz del espectro de radio. El método de modulación seleccionado fue DSSS (Modulación de Secuencia Directa de Espectro Extendido) usando CCK (Modulación por Cambios de Código Complementarios), que permite una velocidad máxima de 11 Mbps. La especificación 802.11a también fue ratificada en esa fecha, pero los productos se hicieron disponibles en el mercado en el año 2001, de tal forma, que su despliegue no fue tan amplio como sucedió con 802.11b. 802.11a opera en frecuencias entre 5.15 y 5.875 GHz y utiliza el método de modulación OFDM (Multiplexación por División de Frecuencias Ortogonales), el cual hace posible velocidades de hasta 54 Mbps.

Han aparecido dos nuevos estándares para LAN inalámbricas que prometen ofrecer velocidades de hasta 54 Mbps a los usuarios de redes WLAN. Estos nuevos estándares están definidos en los grupos de trabajo 802.11a y 802.11g de IEEE.

Los productos IEEE 802.11g poseen un alto grado de compatibilidad con versiones anteriores (con productos ajustados a IEEE 802.11 e IEEE 802.11b) y todavía utilizan la banda de frecuencia ISM (2,4 GHz). Eso significa también que las distancias de transmisión de los productos 802.11b y 802.11g son más o menos las mismas.

Los productos IEEE 802.11a, por su parte, transmiten a 5 GHz. La tecnología 802.11a comporta células de RF más pequeñas (distancias efectivas más cortas) y un consumo de energía más alto. Los productos IEEE 802.11a, sin soluciones de chip de banda doble especiales, no ofrecen compatibilidad con versiones anteriores.

Al adoptar la banda de frecuencia de 5 GHz y utilizar la modulación OFDM, el estándar IEEE 802.11a goza de dos notables ventajas respecto al 802.11b. Incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento.

La banda de 5 GHz (banda UNII) está formada por tres sub-bandas, UNII1 (5,15 - 5,25 GHz), UNII2 (5,25 - 5,35 GHz) y UNII3 (5,725 - 5,825 GHz). Cuando se utilizan tanto UNII1 como UNII2, hay 8 canales sin solapamiento disponibles; mientras que con la banda de 2,4 GHz sólo hay 3. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2,4 GHz (300 MHz por 83,5 MHz). Así pues, una WLAN basada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos. Un inconveniente de utilizar la banda de 5 GHz es que las frecuencias utilizadas no están estandarizadas internacionalmente.

Asimismo, deben hacerse algunas transacciones en cuanto a compatibilidad y alcance. Como los estándares 802.11a y 802.11b operan en bandas de frecuencia distintas, los productos no son compatibles. El asunto de la compatibilidad se complica un poco más al no estar reflejados los requisitos europeos ETSI en el estándar IEEE 802.11a. Así pues, tecnologías como Dynamic-Frequency-Selection (DFS) y Transmit-Power-Protocol (TPC) están englobadas en el estándar IEEE 802.11h.

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales demuestran que los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

El estándar IEEE 802.11g alcanza velocidades más altas y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda de frecuencia de 2,4 GHz y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.

Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps_. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El borrador del estándar también especifica tipos de modulación opcionales (como OFDM/CCK) diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redundará en un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2,4 GHz no varía. El motivo es que el IEEE 802.11g todavía está restringido a tres canales en la banda de 2,4 GHz.

- Ofrece las mismas distancias de funcionamiento que el IEEE802.11b

La modulación OFDM se ha desarrollado para ser utilizada en sistemas 802.11a que ya operen en las bandas de 5 GHz. El mayor problema a la hora de

introducir la modulación OFDM en la banda de 2,4 GHz fue hacerla compatible con los productos 802.11b heredados.

El principal mecanismo para compartir canales en el sistema 802.11 es CSMA/CA. Para que este método funcione, cada radio debe ser capaz de detectar a todas las demás radios asociadas al mismo punto de acceso (incluido, obviamente, el propio PA). Pero con sistemas 802.11g que utilizaran OFDM, las radios 802.11b heredadas serían incapaces de detectar a los nuevos dispositivos.

El grupo de trabajo IEEE 802.11g solucionó este problema utilizando una función de solicitud de envío/preparado para enviar (RTS-CTS) que ya incorporan todos los dispositivos 802.11.

Para que una red IEEE 802.11 funcione correctamente, todos los nodos deben encontrarse dentro del radio de alcance del punto de acceso, aunque no suceda lo mismo entre ellos. Es lo que se conoce como problema del “nodo oculto”. En situaciones como ésta, se puede invocar el mecanismo de RTS-CTS para reducir la posibilidad de colisión. En IEEE 802.11g, la función RTS-CTS se puede utilizar para facilitar el funcionamiento de la red cuando hay una mezcla de clientes 802.11g y clientes 802.11b heredados operando en el mismo BSS (Basic Service Set).

Todos los clientes y puntos de acceso 802.11g deben ser capaces de retroceder y operar exactamente como un dispositivo 802.11b heredado. De esta forma, la migración a la tecnología 802.11g es fácil y dinámica. Mientras se van adquiriendo e instalando nuevos puntos de acceso 802.11g, los puntos de acceso 802.11b heredados pueden permanecer en servicio y ser totalmente compatibles con los clientes 802.11g más nuevos.

Aunque OFDM sea una tecnología excelente para las aplicaciones WLAN de interior, las leyes de la física indican que el alcance de la comunicación es proporcional a la longitud de onda. En otras palabras, los objetos dispersan y atenúan la energía de radiofrecuencia de un modo más eficaz cuanto más alta sea la frecuencia utilizada.

En un espacio abierto, las diferencias de propagación no deberían suponer ningún problema. Sin embargo, la mayoría de sistemas WLAN funcionan en interiores, donde los espacios abiertos son limitados y casi todas las señales de radio tiene que atravesar paredes, mobiliario y otros obstáculos.

Este ejemplo proviene de diversas pruebas publicadas y sólo pretende mostrar los resultados de los análisis comparativos. Obviamente, los resultados reales diferirán según el entorno de prueba real.

Los equipos IEEE 802.11a alcanzan velocidades de datos más altas en alcances cortos o, como en el ejemplo, en un vestíbulo donde es posible la propagación por un espacio abierto. No obstante, la velocidad de los datos disminuye rápidamente cuando la señal debe atravesar paredes y otros obstáculos.

Los productos IEEE 802.11g son capaces de conseguir velocidades de datos más elevadas y con mayor alcance que los productos con tecnología 802.11a. La combinación de OFDM y la mejor capacidad para atravesar paredes de sus 2,4 GHz confieren a los productos 802.11g una ventaja clara sobre otras tecnologías WLAN de alta velocidad. La capacidad para proporcionar una cobertura de gran rendimiento en un área comparativamente grande desde un único punto de acceso supone un factor importante de coste.

Un punto de acceso 802.11b de 2,4 GHz, por ejemplo, no podrá trabajar con una tarjeta de interfaz de red 802.11a de 5 GHz. No obstante, estos estándares pueden coexistir perfectamente.

2.13 Mecanismos de Seguridad

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

Existe el término “wardriving”, que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores

de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Mecanismos de seguridad para redes WLAN

Mecanismo de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). - Filtrado con dirección MAC (Control de Acceso al Medio): restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. - WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves,

	pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.1X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).
WPA (Wi-Fi Protected Access)	Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras– Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación. Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado.

2.14 Canales de Transmisión

Un *canal de transmisión* es una banda de frecuencia estrecha que se puede usar para comunicarse. El gobierno de cada país por lo general regula el uso del espectro radial ya que es su mayor usuario del espectro debido a usos militares.

Sin embargo, los gobiernos también permiten el uso de bandas de frecuencia sin licencias. Los grupos que se encargan de regular el uso de frecuencias radiales son:

- El ETSI (Instituto Europeo de Normas de Telecomunicaciones) en Europa
- La FCC (Comisión de Comunicaciones Federales) en Estados Unidos
- El MKK (Kensa-kentei Kyokai) en Japón

En 1985, Estados Unidos asignó tres bandas de frecuencia para uso industrial, científico y médico. Estas bandas de frecuencia que se denominan ISM son las bandas 902-928 MHz, 2.400-2.4835GHz y 5.725-5.850 GHz.

En Europa, las bandas de 890 a 915 MHz se utilizan para comunicaciones móviles (GSM) y sólo las bandas de 2.400 a 2.4835 GHz y de 5.725 a 5.850 GHz están disponibles para uso de radioaficionados.

Tecnologías de transmisión

Las redes de radio locales usan ondas radiales o infrarrojas para transmitir datos. La tecnología que se utiliza para enviar transmisiones de radio se denomina transmisión de banda estrecha y conecta distintas señales de comunicación a través de distintos canales. Sin embargo, las transmisiones

radiales habitualmente poseen numerosas limitaciones, lo cual hace que este tipo de transmisión sea insuficiente. Éstas son algunas de las limitaciones:

- Estaciones diferentes dentro de la misma célula que comparten banda estrecha de manera involuntaria.
- Propagación por **trayectoria múltiple de ondas radiales**. Una onda radial puede propagarse en distintas direcciones y posiblemente puede reflectarse o refractarse en objetos físicos. Es por ello que un receptor puede recibir la misma información varias veces. Esto sería el resultado de aquellas señales que van por caminos diferentes después de haberse reflectado varias veces.

Por tal motivo, y para minimizar problemas de interferencia, la capa física del estándar 802.11 define diversas técnicas de transmisión:

- Espectro ensanchado por saltos de frecuencia.
- Espectro ensanchado por secuencia directa.
- Tecnología infrarroja.

Banda estrecha

La técnica de *banda estrecha* consiste en el uso de una frecuencia de radio especificada para transmitir y recibir datos. La banda de frecuencia que se utilice debe ser lo más pequeña posible para no interferir con las bandas cercanas.

Espectro ensanchado

El estándar *IEEE 802.11* permite que dos técnicas de modulación de frecuencia desarrolladas para los militares transmitan datos. Estas técnicas, denominadas *espectro ensanchado*, consisten en utilizar una banda de frecuencia ancha para

transmitir datos de baja potencia. Existen dos tecnologías de espectro ensanchado:

- Espectro ensanchado por saltos de frecuencia.
- Espectro ensanchado por secuencia directa.

Salto de Frecuencia

La técnica de espectro ensanchado por saltos de frecuencia o **FHSS** consiste en dividir la frecuencia de banda ancha en al menos 75 canales distintos (con "saltos" de 1 MHz de distancia entre sí) y después transmitirla a través de una combinación de canales que todas las estaciones en la célula conocen. En el estándar 802.11 la banda de frecuencia de 2.4 a 2.4835 GHz acepta 79 canales discretos de 1 MHz. La transmisión se lleva a cabo de un canal hacia otro y sólo se usa cada canal durante un período de tiempo corto (aproximadamente 400 milésimas de segundo), lo que permite que una señal más fácil de reconocer se transmita en un determinado momento y en una determinada frecuencia.

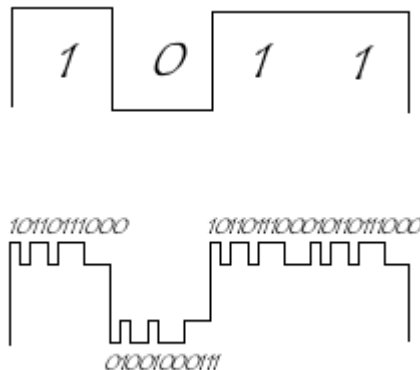
La técnica de espectro ensanchado por saltos de frecuencia se desarrolló originalmente para uso militar con el fin de prevenir que se escuchen las transmisiones radiales. La estación que no sabe qué combinación de frecuencia usar no puede escuchar la señal porque le sería imposible determinar la frecuencia en la que la señal fue transmitida y encontrar después la nueva frecuencia dentro de un período de tiempo corto.

Actualmente, las redes locales que usan esta tecnología son estándar. Debido a que la secuencia de frecuencias que se utiliza es conocida universalmente, esta técnica ya no es una forma segura de transmitir datos. Sin embargo, FHSS todavía se utiliza en el estándar 802.11 para reducir la interferencia entre las distintas estaciones de una célula.

Espectro ensanchado por secuencia directa

La técnica conocida como *espectro ensanchado por secuencia directa* (o DSSS) consiste en transmitir para cada bit enviado una secuencia de Barker de bits (a veces llamado *ruido pseudo aleatorio* o *PN*). En esta operación, cada bit establecido en 1 es reemplazado por una secuencia de bit y cada secuencia de bit establecida en 0 es reemplazada por su complemento.

La capa física del estándar 802.11 define una secuencia de 11 bits (10110111000) para representar el 1 y para codificar el 0 usa su complemento (01001000111). Cada bit que se codifica con esta secuencia se denomina *chip* o *código de chip*. Esta técnica (llamada *chipping* por "chip") modula cada bit que tenga la secuencia de Barker.



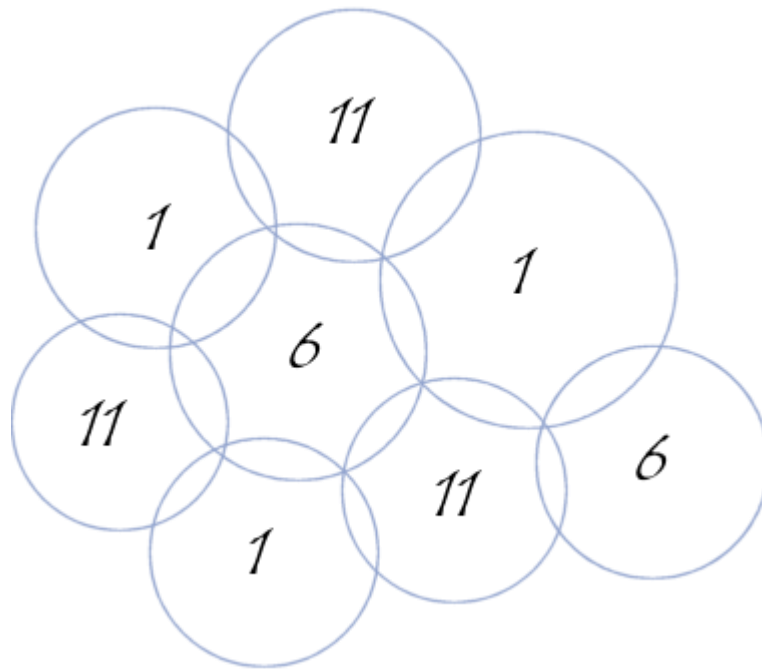
A través del chipping se envía información redundante y esto permite verificar errores e incluso corregirlos durante las transmisiones.

En el estándar 802.11, la banda de frecuencia 2.400-2.4835 GHz (83.5 MHz de ancho) se ha dividido en 14 canales distintos de 5 MHz cada uno. Sólo los primeros 11 se pueden usar en Estados Unidos y Canadá. En el Reino Unido se pueden usar los canales del 1 al 13 solamente. Éstas son las frecuencias que se asocian a los 14 canales:

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

Sin embargo, para una correcta transmisión de 11 Mbps se debe transmitir en una banda de 22 MHz porque, de acuerdo al teorema de Shannon, la frecuencia de muestreo debe ser al menos el doble de la señal para que se digitalice. Algunos canales se superponen con canales cercanos. Es por ello que generalmente se utilizan canales aislados (1, 6 y 11) que están a 25 MHz de distancia.

Por lo tanto, cuando dos puntos de acceso que usan los mismos canales tienen áreas de transmisión que se superponen, las distorsiones de señal pueden afectar las transmisiones. Para evitar cualquiera de estas interferencias, se recomienda distribuir los puntos de acceso y seleccionar canales de forma tal que dos puntos de acceso que usen el mismo canal nunca estén cerca.



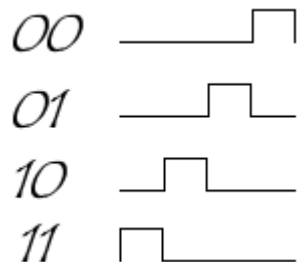
El estándar 802.11a utiliza las bandas de frecuencia de 5.15 a 5.35 Ghz y de 5.725 a 5.825 Ghz, lo que le permite definir 8 canales diferentes de 20 MHz de ancho cada uno, una banda lo suficientemente ancha como para evitar que los canales interfieran unos con otros.

Tecnología infrarroja

El estándar IEEE 802.11 también ofrece una alternativa a las ondas radiales: la luz infrarroja. La característica primordial de la tecnología infrarroja es el uso de una onda de luz para transmitir datos. Estas transmisiones viajan en una sola dirección, ya sea mediante una línea de visibilidad directa o al reflejarse en una superficie. Las ondas de luz ofrecen un alto nivel de seguridad debido a su naturaleza no difusa.

La tecnología infrarroja permite el envío de datos a una velocidad de 1 a 2 Mbits por segundo al usar una clase de modulación denominada **PPM** (*modulación de posición de pulso*).

La modulación *PPM* consiste en transmitir pulsos de amplitud constante y codificar información según la posición del pulso. Una velocidad de transferencia de 1 Mbps se alcanza con una modulación de 16 PPM y 2 Mbps se alcanzan con una modulación de 4 PPM, lo que permite que se codifiquen 2 bits de datos con cuatro posiciones posibles.



Técnicas de modulación

Mientras que la radio común utiliza una frecuencia modulada (FM) o una amplitud modulada (AM), el estándar 802.11b utiliza una técnica de modulación denominada *PSK* (Modulación por desplazamiento de fase). Durante este proceso cada bit sufre un desplazamiento de fase. Para transferir a velocidades bajas se usa un desplazamiento de 180 grados (es una técnica que se denomina *BPSK*, Modulación por desplazamiento de fase binaria), mientras que una serie de cuatro desplazamientos de 90 grados permiten transferencias dos veces más rápidas (técnica llamada *QPSK*, *Modulación por desplazamiento de fase en cuadratura*).

Optimización

El estándar 802.11b utiliza otro tipo de codificación para optimizar la capacidad de transmisión. Las dos secuencias de Barker usan dos palabras complementarias de 11 bits y pueden definir sólo dos estados (0 ó 1).

Existe un método alternativo llamado CCK (*modulación por código complementario*) que permite codificar directamente varios bits de datos en un

solo chip al utilizar ocho secuencias de 64 bits. Por lo tanto, el método CCK puede alcanzar una velocidad máxima de 5.5 Mbps al codificar 4 bits de una sola vez o hasta 11 Mbps al codificar 8 bits de datos.

La tecnología PBCC (*codificación convolucional binaria de paquetes*) hace que la señal sea más resistente a la distorsión de trayectoria múltiple. La empresa Texas Instruments ha desarrollado con éxito una secuencia que aprovecha esta mayor resistencia a la interferencia y que permite velocidades de 22 Mbps. Sin embargo, esta tecnología, denominada *802.11b+*, no cumple con los estándares *IEEE 802.11b*, con lo cual los periféricos que la admiten no son compatibles con los dispositivos 802.11b.

El estándar 802.11a opera en una banda de frecuencia de 5 GHz que tiene 8 canales diferentes. Por esta razón está disponible una técnica de transmisión alternativa que utiliza distintos canales. OFMD *multiplexación por división de frecuencia ortogonal* permite velocidades máximas de 54 Mbps al enviar datos de forma paralela en frecuencias diferentes. Además, OFDM utiliza el espectro en una forma más eficaz.

Tecnología	Codificación	Tipo de modulación	Velocidad
802.11b	11 bits (Secuencia de Barker)	PSK	1 Mbps
802.11b	11 bits (Secuencia de Barker)	QPSK	2 Mbps
802.11b	CCK (4 bits)	QPSK	5.5 Mbps
802.11b	CCK (8 bits)	QPSK	11 Mbps
802.11a	CCK (8 bits)	OFDM	54 Mbps
802.11g	CCK (8 bits)	OFDM	54 Mbps

2.15 ELEMENTOS QUE INTEGRAN UNA WLAN

Elementos de red WLAN

Los elementos fundamentales de las WLAN, basándonos en las posibles arquitecturas y estructuras de red descritas anteriormente, de menor a mayor jerarquía son:

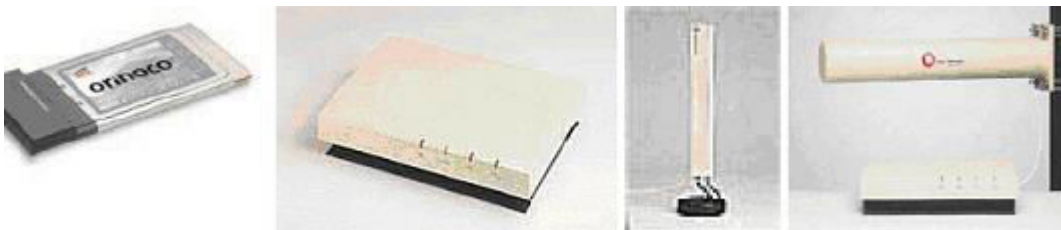


Figura. Ejemplo de equipos WLAN. a) Tarjeta PCMCIA, b) punto de acceso, c) antena omnidireccional para interior y d) antena direccional para exterior.

Antena

Se pone en el PC para permitir la recepción y transmisión de los datos en la red del PC.

Tarjeta inalámbrica

La Tarjeta realiza las funciones las tarjetas de red ethernet, adaptando las tramas ethernet que genera el PC, a las tramas del estándar inalámbrico y viceversa, posibilitando la transmisión transparente de la información. En muchas ocasiones estas integran la antena en la tarjeta. Son usados por los AP y por los portátiles.

Puntos de Acceso (AP)

Actúa como puente con dos tipos de interfaces, el inalámbrico hacia los nodos inalámbricos y el cableado hacia la red troncal (Ethernet). El AP es el encargado de coordinar la comunicación entre los entre nodos inalámbricos que están conectados a él. Además posee funcionalidades para la asignación de recursos, mediante el uso de tramas “baliza”, asignando un canal a las estaciones que se asocian al AP. Los AP deben además proporcionar autenticación y confidencialidad pues dan paso a la red cableada. Hay soluciones tipo RADIUS (login y password) para el acceso autenticado, que intentan proveer seguridad. Se gestionan con el protocolo SNMP.

Controlador de Acceso (AC)

El AC es un router IP que se encarga de asignar las direcciones IP a los terminales de la WLAN, mantener una lista de direcciones de los terminales correctamente autenticados y filtrar el tráfico, descartando los paquetes de terminales no autenticados. A su vez, los controladores de acceso se conectan a un elemento central encargado de la gestión de servicios. Así cumplen la función de ser pasarela a las redes IP externa permitiendo la conexión a Internet y a las aplicaciones que esta soporte.

Distribution System (DS)

Es la parte cableada de la red inalámbrica. Generalmente es una red Ethernet de la que cuelgan los AP y que está acabada en un AC, que gestiona la red. Pueden existir otro tipo de configuraciones del DS, ya que no hay un estándar que lo fije, quedando abierto a soluciones propietarias y particulares

Tipos de esquema de red

Las redes WLAN se integran en las redes privadas igual que las redes locales convencionales. Generalmente los puntos de acceso de la WLAN se conectan a un hub Ethernet y de éste a un router IP, o directamente a un equipo que integre ambas funcionalidades.

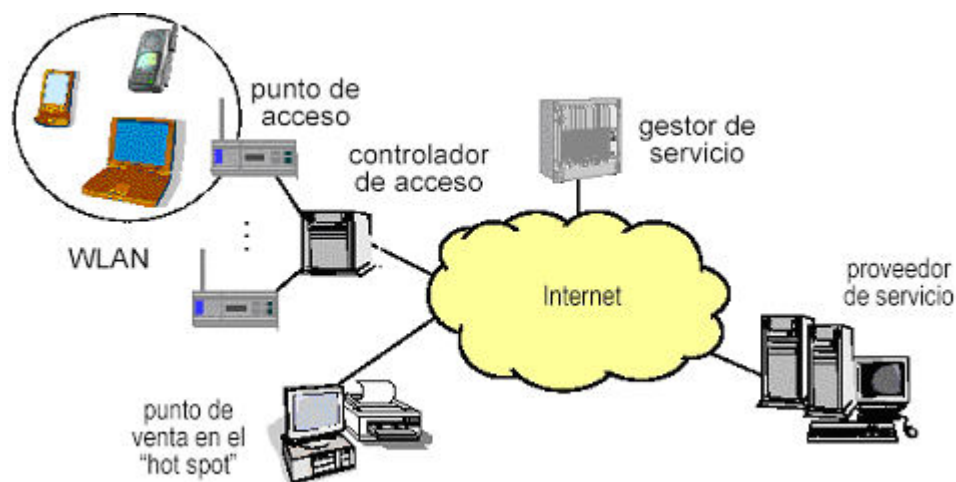


Figura. Estructura de red para acceso WLAN de los hot spots.

En el caso de prestación de servicios en un hot spot, la arquitectura general de red se representa en la Figura superior. Como muestra la figura, los puntos de acceso (AP) de la WLAN se conectan a un controlador de acceso (AC). El AC es un router IP que se encarga de asignar direcciones IP a los terminales de la WLAN, mantener una lista de direcciones de los terminales correctamente autenticados y filtrar el tráfico, descartando los paquetes de terminales no autenticados. Además el AC recoge la información necesaria para cobrar a los usuarios por el acceso. A su vez, los controladores de acceso se conectan a un elemento central encargado de la gestión de servicios. Este elemento, que

recibe diferentes nombres en las referencias consultadas, lo llamaremos aquí gestor de servicios (SM). El AC y el SM se comunican utilizando el protocolo Remote Authentication Dial-In User Service (RADIUS), que es el estándar de facto para funciones AAA (Authentication, Authorization, and Accounting) en las redes IP.

Ambos elementos dialogan cuando un usuario pide acceso al servicio, para que el SM diga al AC si debe permitir el acceso del usuario o no (la petición de acceso se comenta después con más detalle), y cuando el servicio termina, incluyendo el envío al SM de los datos que haya recogido el AC a efectos de tarificación. El SM contiene información local sobre los usuarios de la WLAN y actúa como pasarela hacia los sistemas de AAA de los proveedores de servicios. Además, el SM puede ofrecer una interfaz (por ejem. una página Web) al dueño del hot spot que hace funciones de intermediario entre los usuarios y los proveedores de servicio. Finalmente, el hotel carga el coste del acceso en la cuenta del huésped y comparte los ingresos con el proveedor del servicio. En el caso de un viajero no alojado en el hotel, se puede utilizar prepago: el usuario paga el cupón de acceso al recibirlo del recepcionista y posteriormente lo utiliza para acceder a la red. En otro escenario, un operador de móviles que por ejemplo quiere complementar sus servicios GPRS con acceso de mayor velocidad mediante WLAN puede utilizar una arquitectura similar a la descrita.

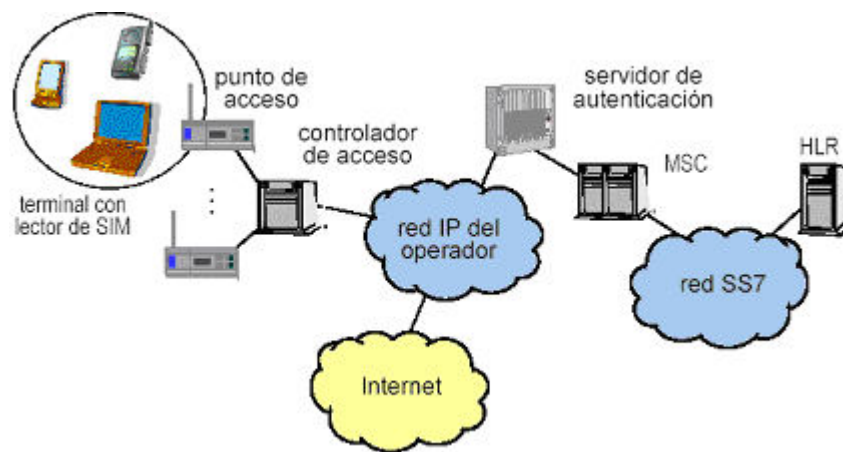


Figura. WLAN de un operador de móviles.

El controlador de acceso funciona como se ha descrito, mientras que el gestor de servicios (aquí se llama “pasarela de autenticación y tarificación” o “servidor de autenticación”) se comunica con un nodo MSC (Mobile Switching Center) del operador. Para obtener el permiso de acceso, el terminal WLAN debe poder leer la tarjeta SIM del usuario. En la arquitectura descrita, los mensajes del procedimiento normal de autenticación de GSM se encapsulan sobre IP entre el terminal y el servidor de autenticación (AS), que a su vez los pasa al MSC con un protocolo propietario. El MSC se comunica con el resto de elementos de la red, usando los protocolos de señalización normalizados de GSM, como MAP. Igualmente, el AS proporciona a la red GSM los datos de tarificación, de forma que el usuario reciba el correspondiente cargo por el uso de la WLAN en la factura de su operador. Este acceso permite itinerancia o roaming, es decir, el usuario puede acceder a través de una WLAN de otro operador GSM del cual no es cliente.

En las redes empresariales, se repiten las acciones del Hot Spots, salvo que ahora no hay que tener un control de la tarificación, sino que se controlan mas los aspectos relativos al acceso de la red. Generalmente las WLAN, se soportan

sobre la infraestructura cableada Ethernet. A esta, está conectado el AP, generalmente que cumple también funciones de router o switch, gestiona el acceso de los equipos a la red, y a Internet. Este mediante una tarjeta de red inalámbrica PCMCIA, da servicio a los equipos. Los receptores son generalmente PC fijos, con tarjetas de red Ethernet, a los que se conecta una antena que permite poder recibir y transmitir hacia el AP. Los PC portátiles, se les instala una tarjeta PCMCIA, para poder tener acceso a la red.



Figura.- Esquema red Oficina

2.16 IMPORTANCIA DE LA SEGURIDAD

MODO AHDOC Y MODO INFRAESTRUCTURA

Modos de funcionamiento

Una LAN inalámbrica puede configurarse para dos modos de funcionamiento: modo *infraestructura* y modo *ad hoc* (el modo ad hoc se conoce también como red punto-a-punto o red equipo-a-equipo). Cada modo tiene sus ventajas y desventajas y, según la ubicación y el tipo de conexión de red, un modo puede resultar más adecuado que otro.

Modo infraestructura

La diferencia principal entre una red de tipo infraestructura y una red de tipo ad hoc es que la primera incluye un equipo principal que tiene incorporado un adaptador de red inalámbrica y está conectado a un punto de acceso (AP) inalámbrico. De esta manera, los equipos que forman parte de la LAN inalámbrica de tipo infraestructura pueden acceder a los recursos y herramientas de la LAN cableada, incluyendo acceso a Internet y correo electrónico, intercambio de archivos y uso de la misma impresora.

Características

Los equipos de la red se comunican entre sí a través de un AP establecido. Todos los datos que se transmiten entre los equipos que conforman esta LAN inalámbrica pasan por el AP.

Ventajas

- Mayor alcance. El punto de acceso amplía el alcance de la LAN inalámbrica. Cada equipo se puede comunicar con los equipos que tengan una red inalámbrica y estén al alcance del punto de acceso.
- Itinerancia: Cuando el usuario se mueve en el hogar o la oficina, el equipo portátil con **TrueMobile** busca usar el mejor punto de acceso para asegurar que la comunicación con la red sea continua.
- Conectividad a la red. El punto de acceso puede servir de puente entre dos redes, con lo que la red LAN inalámbrica puede acceder a una red cableada existente. Los usuarios de la LAN inalámbrica pueden tener acceso a todas las funciones de la red cableada, desde acceso a los archivos del servidor hasta conexión a Internet y correo electrónico.

Desventajas

Como el modo infraestructura ofrece más características, requiere más componentes y más tiempo de configuración para desplegar la red.

2.16.1 Modo Ad-Hoc

La red ad-hoc es el tipo de red más fácil de instalar y es ideal para el hogar o las oficinas pequeñas. Este modo permite compartir archivos entre los empleados, imprimir documentos en una impresora compartida en la oficina y acceder a Internet por medio de un módem compartido. Sin embargo, en la red ad hoc, los equipos sólo se pueden comunicar con las redes inalámbricas que estén a determinado alcance y formen parte del mismo grupo de trabajo inalámbrico.

Características

Los equipos de la red se envían los datos directamente entre sí sin necesidad de pasar por un punto de acceso.

Ventajas

- Configuración sencilla
- Bajo costo

Desventajas

- La comunicación se limita a los equipos que están a determinado alcance.
- La seguridad IEEE 802.1x no está disponible.

2.17 Principales amenazas para la seguridad de las WLAN

Amenaza	Descripción de la amenaza
Interceptación (revelación de datos)	La interceptación de transmisiones de la red puede dar lugar a la revelación de datos confidenciales y de credenciales de usuario sin protección, además de a una posible usurpación de la identidad. Permite también que intrusos expertos recopilen información sobre los entornos de TI y la utilicen para atacar otros sistemas o datos que, de otra forma, no serían vulnerables.
Interceptación y modificación de los datos transmitidos	Si un atacante logra obtener acceso a la red, puede introducir un equipo falso que intercepte y modifique los datos comunicados entre dos usuarios autorizados.
Imitación	El acceso directo a la red interna permite que el intruso falsifique datos que parecen legítimos de manera que no sería posible desde fuera de la red, por ejemplo, un mensaje de correo electrónico de un usuario imitado. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red mucho más que en los que proceden del exterior de la red corporativa.
Denegación del servicio (DoS)	Un agresor determinado puede activar un ataque de DoS de diversas maneras. Por ejemplo, la interrupción de las señales de

Amenaza	Descripción de la amenaza
	radio se puede activar mediante algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de bajo nivel, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.
Carga libre (o robo de recursos)	Es posible que los intrusos sólo deseen utilizar su red como punto de libre acceso a Internet. Si bien esto no es tan grave como las demás amenazas, hará que, como mínimo, no sólo empeore el nivel de servicio prestado a los usuarios autorizados sino también que puedan introducirse virus y otras amenazas.
Amenazas accidentales	Algunas características de las WLAN facilitan la aparición de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar el equipo portátil sin la intención de conectarse a la red, pero se conecta a su WLAN automáticamente. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas.
WLAN no autorizadas	Si su empresa no dispone oficialmente de una WLAN, es posible que siga estando bajo la amenaza de las WLAN sin administrar que surjan en su red. El hardware de WLAN adquirido a bajo precio por parte de empleados entusiastas puede abrir vulnerabilidades no intencionadas en su red.

2.18 POLITICAS DE SEGURIDAD EN LAS WLAN

El término **política de seguridad** se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema.

Al tratarse de 'términos generales', aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en

cierta parte de la operación del sistema, lo que se denomina **política de aplicación específica**

Una política de seguridad puede ser **prohibitiva**, si todo lo que no está expresamente permitido está denegado, o **permisiva**, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto - las no contempladas - serían consideradas ilegales.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático

Disponibilidad

Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

Utilidad

Los recursos del sistema y la información manejada en el mismo a de ser útil para alguna función.

Integridad

La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

Autenticidad

El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

Confidencialidad

La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

Posesión

Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados **normativas** (aunque las definiciones concretas de cada documento que conforma la infraestructura de nuestra política de seguridad - política, normativa, estándar, procedimiento operativo...- es algo en lo que ni los propios expertos se ponen de acuerdo). El estándar ISO 17799 ([Sta00]) define las siguientes líneas de actuación:

Seguridad organizacional

Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, *outsourcing*, estructura del área de seguridad).

Clasificación y control de activos

Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

Seguridad del personal

Formación en materias de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitorización de personal...

Seguridad física y del entorno

Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos - incluyendo los humanos - de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

Gestión de comunicaciones y operaciones

Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la protección frente a *malware*, la gestión de copias de seguridad o el intercambio de *software* dentro de la organización.

Controles de acceso

Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos...

Desarrollo y mantenimiento de sistemas

Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de *software*.

Gestión de continuidad de negocio

Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.

Requisitos legales

Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de cifrado... junto a todos los aspectos relacionados con registros de eventos en los recursos (*logs*) y su mantenimiento.

2.19 TECNICAS DE SEGURIDAD PARA REDES WLAN

- La protección de una WLAN implica tres elementos fundamentales:
- Autenticación del usuario (o dispositivo) que se conecta a la red, de manera que se tenga un elevado grado de confianza en quién o qué está intentando conectarse.
- Autorización del usuario o dispositivo que va a utilizar la WLAN para poder controlar quien tiene acceso a ella
- Protección de los datos transmitidos en la red de manera que estén a salvo de interceptaciones y modificaciones no autorizadas

Es posible que precise también una función de auditoría junto con estas opciones, aunque la auditoría es principalmente una manera de comprobar y reforzar estos otros tres elementos.

2.19.1 Autenticación y Autorización de la red

La seguridad WEP estática se basa en un mero secreto compartido (clave o contraseña) para la autenticación en la WLAN. Todo el que posea esta clave secreta podrá contar con acceso a la WLAN. La WEP estándar original no proporciona ningún método para automatizar la actualización o distribución de

estas claves; por lo tanto, resulta extremadamente difícil cambiarlas con regularidad. Los defectos de cifrado en la WEP implican que un atacante puede descubrir las claves WEP estáticas mediante herramientas sencillas.

Con el fin de proporcionar un método más sólido de autenticación y autorización, Microsoft y una serie de proveedores han propuesto un marco de seguridad de WLAN mediante el protocolo 802.1X. 802.1X es un estándar del IEEE para realizar la autenticación del acceso a una red y, si se desea, administrar las claves utilizadas para proteger el tráfico. Su uso no se limita a las redes inalámbricas y, de hecho, también se implementan en muchos conmutadores de LAN de categoría superior.

El protocolo 802.1X implica al usuario de la red, un dispositivo de acceso a la red (o puerta de enlace) como un punto de acceso inalámbrico y un servicio de autenticación y autorización en forma de servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El servidor RADIUS desempeña la labor de autenticar las credenciales de los usuarios y de autorizar el acceso de éstos a la WLAN.

1X se basa en un protocolo IETF denominado "protocolo de autenticación extensible" (EAP) para llevar a cabo la comunicación de autenticación entre el cliente y el servidor RADIUS (transmitida por el punto de acceso). EAP es un protocolo general para la autenticación que admite diversos métodos de autenticación, basados en contraseñas, certificados digitales o bien otros tipos de credenciales.

Puesto que EAP es un método de autenticación conectable, no existe un único tipo de autenticación estándar EAP que se pueda utilizar. Distintos métodos de EAP, con distintos tipos de credenciales y protocolos de autenticación, pueden

resultar apropiados en distintas circunstancias. La utilización de métodos de EAP en la autenticación de WLAN se tratará en una sección más adelante.

2.19.2 Protección de datos de WLAN

La autenticación y el acceso a la red 1X constituyen sólo una parte de la solución. El otro componente significativo es la protección del tráfico de redes inalámbricas.

Los defectos del cifrado de datos WEP descritos con anterioridad se podrían haber mejorado si la WEP estática hubiera incluido un método para actualizar automáticamente las claves de cifrado con regularidad. Las herramientas para descifrar la WEP estática precisan recopilar entre uno y diez millones de paquetes cifrados con la misma clave. Dado que las claves WEP estáticas permanecen invariables a menudo durante semanas o meses, suele ser fácil para un atacante recopilar esa cantidad de datos. Puesto que todos los equipos de una WLAN comparten la misma clave estática, las transmisiones de datos desde todos los equipos de la WLAN pueden cosecharse para ayudarle a descubrir la clave.

Al utilizar una solución basada en 802.1X, se permite que las claves de cifrado se modifiquen con frecuencia. Como parte del proceso de autenticación segura 802.1X, el método de EAP genera una clave de cifrado que es exclusiva de cada cliente. Para evitar los ataques de descifrado WEP (descritos previamente), el servidor RADIUS fuerza con regularidad la generación de claves de cifrado nuevas. Esto permite que se empleen algoritmos de cifrado WEP (encontrados en la mayoría del hardware de WLAN actual) de una manera mucho más segura.

2.19.3 WPA y 802.11i

Aunque la WEP con el cambio dinámico de claves 802.1X resulta segura para la mayoría de los fines prácticos, existe un conjunto de problemas persistentes entre los que se incluyen:

- WEP utiliza una clave estática aparte para las transmisiones globales como los paquetes de difusión. A diferencia de las claves por usuario, la clave global no se renueva con regularidad. Pese a que es poco probable que los datos confidenciales se transmitan mediante difusión, al emplear una clave estática para la transmisión global se ofrece a los atacantes la oportunidad de descubrir información acerca de la red, como por ejemplo, direcciones IP y nombres de usuario y de equipo.
- Los marcos de redes protegidas por WEP poseen una protección de escasa integridad. Mediante las técnicas criptográficas, un atacante puede modificar la información del marco de WLAN y actualizar el valor de comprobación de la integridad del marco sin que el receptor lo detecte.
- A medida que se mejora la velocidad de transmisión de la WLAN y se mejora la capacidad informática y las técnicas criptoanalíticas, las claves WEP deberán renovarse con mayor frecuencia. De esta forma, se depositará una carga inaceptable en los servidores RADIUS.

Para afrontar estos problemas, el IEEE está trabajando en un nuevo estándar de seguridad para las WLAN denominado 802.11i; también conocido como "red de seguridad sólida" (RSN). La Alianza Wi-Fi, un consorcio formado por proveedores de fidelidad inalámbrica (Wi-Fi), ha publicado un estándar del sector denominado "Acceso protegido Wi-Fi" (WPA) lo que es, básicamente, una versión previa del 802.11i. WPA incluye un amplio subconjunto de funciones de 802.11i. Al publicar el WPA, la Alianza Wi-Fi ha podido exigir la

adherencia a la WPA de todos los equipos que lleven el logotipo Wi-Fi y ha permitido que los proveedores de hardware de redes de Wi-Fi ofrezcan una opción de alta seguridad estandarizada con anterioridad a la publicación del 802.11i. WPA reúne un conjunto de características de seguridad ampliamente aceptadas como las técnicas más seguras disponibles en la actualidad para proteger las WLAN.

WPA incluye dos modos: uno, que emplea 802.1X y la autenticación RADIUS (conocida simplemente como WPA) y otro esquema más sencillo para entornos SOHO que emplea una clave compartida previamente (conocida como WPA PSK). WPA asocia el cifrado seguro con la autenticación fuerte y el mecanismo de autorización de 802.1X. La protección de datos de WPA elimina las vulnerabilidades conocidas de WEP con los siguientes métodos:

Utilización de una clave de cifrado única para cada paquete

Utilización de un vector de inicialización mucho más largo, duplicando de forma eficaz el espacio de clave al agregar 128 bits adicionales de material para claves.

Adición de un valor de comprobación de integridad de mensaje firmado que no sea vulnerable a la alteración de datos o la suplantación

Incorporación de un contador de marcos cifrado para impedir los ataques de reproducción.

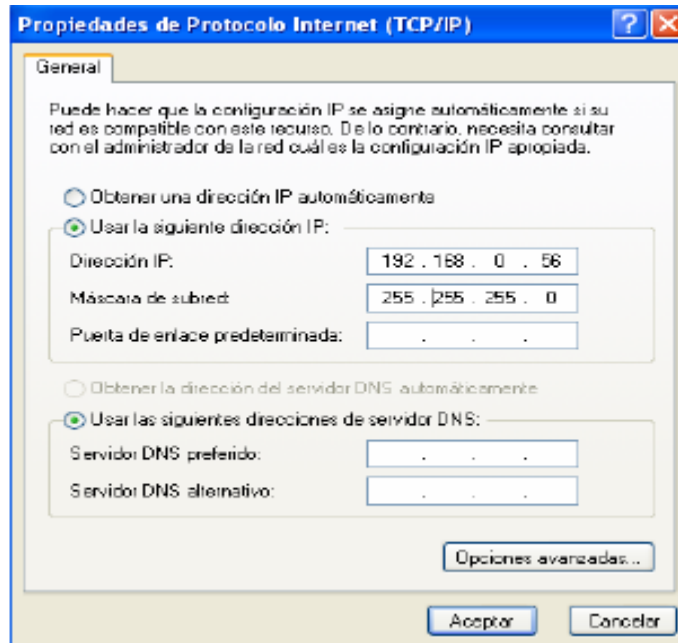
2.20 INSTALACION DE LAS TARJETAS DE RED

Access point DWL 2100AP

- Conectamos la Pc, mediante el cable de red, al Access Point
- En la Pc, ingresamos al Panel de Control y Luego a Conexiones de Red.
- En Conexiones de red, nos aseguramos que todas las redes estén desactivadas, con excepción de la red cableada (Conexión de Area Local).
- En conexión de Area Local hacemos clic derecho y se nos muestra la siguiente pantalla:

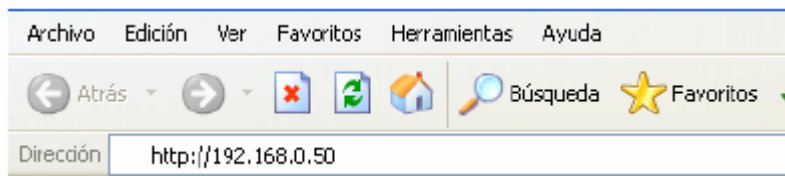


Luego Hacemos clic en el botón propiedades y colocamos como dirección IP de la PC lo siguiente

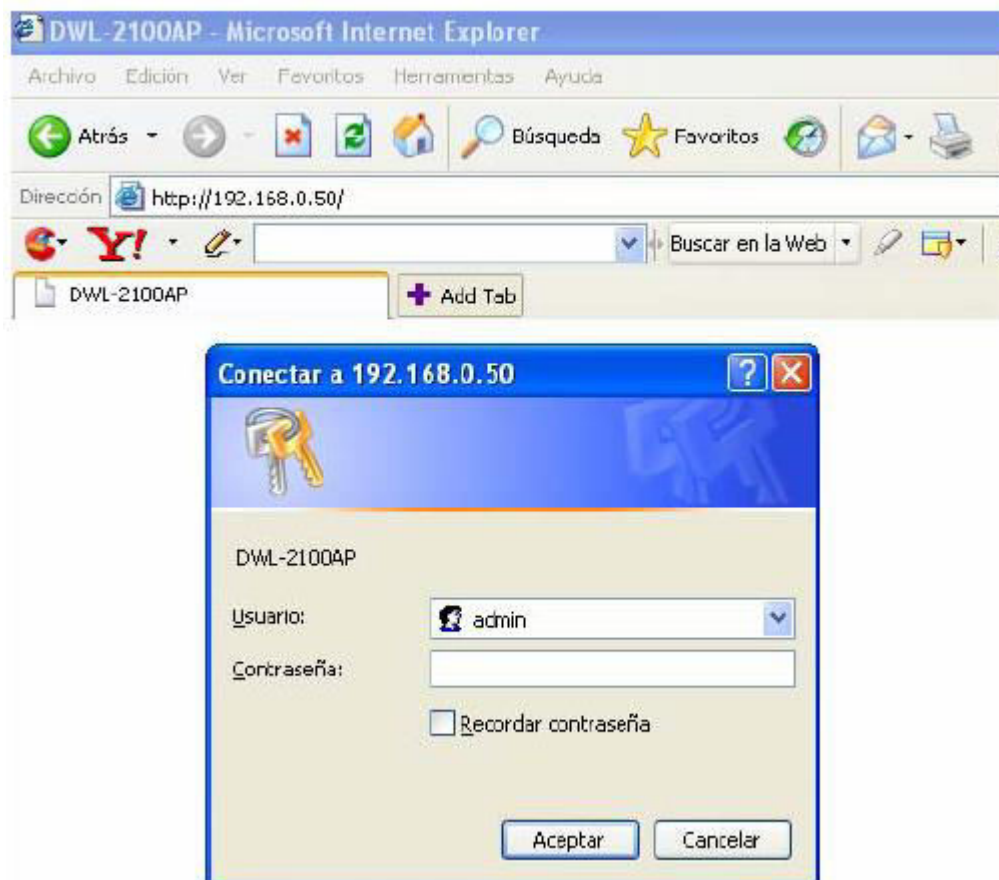


- Clic en aceptar, nuevamente aceptar

- Paso siguiente cargamos el navegador de Internet y en la barra de direcciones colocamos la siguiente dirección:



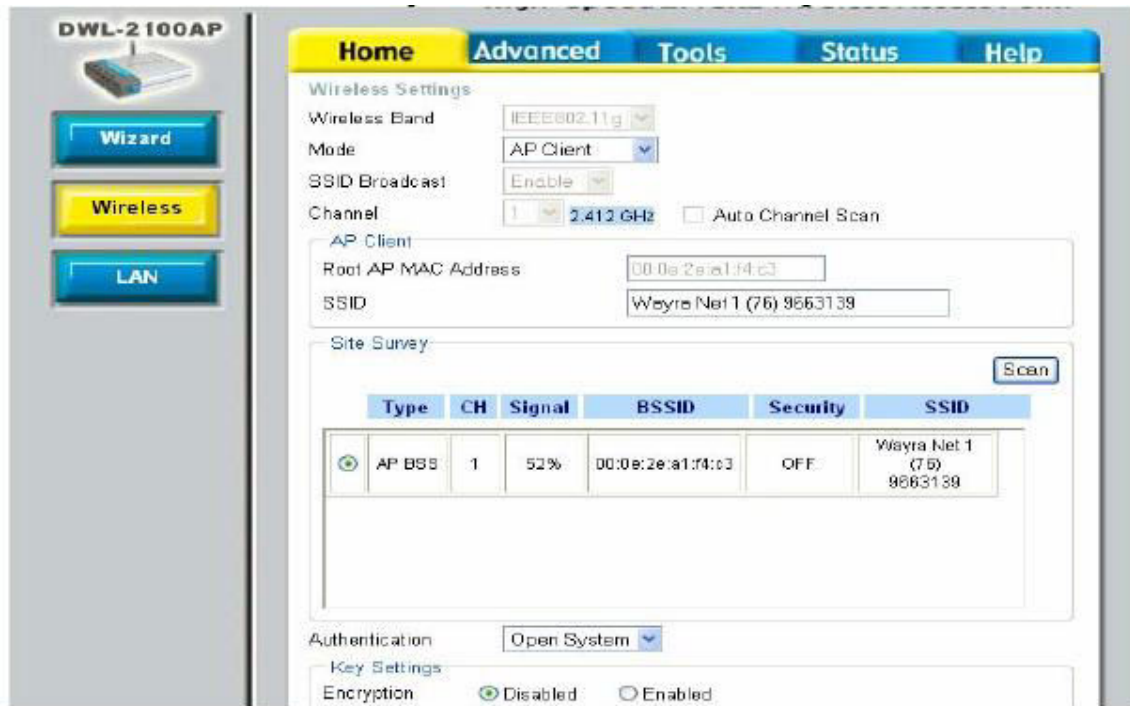
Presionamos Enter, y se nos muestra la siguiente pantalla para ingresar al Access Point, colocamos en el usuario admin., y el password lo dejamos en blanco



Seguidamente se nos muestra la siguiente pantalla en la que hacemos click en el botón wireless, se nos muestra la siguiente pantalla



En la opción modo, escogemos la opción AP Client, para configurar el Access Point como Clientes que nos permitirá comunicarnos a las antenas._ Dejemos todas las demás opciones por defecto._ Hacemos Clic en el botón SCAN, y dejamos que el equipo busque y reconozca todas las redes inalámbricas disponibles._ Como se muestra en la siguiente figura



Escogemos la antenna cuyo porcentaje esté sobre el 40%, el porcentaje mayor a 40% nos garantiza una conexión fiable para el buen servicio de Internet, de ser menor, puede causar problemas de conexión._ Hacemos clic en la option buton (circulo que se encuentra al lado izquierdo y que hace referencia a la antenna a la que deseamos conectarnos), En el ejemplo escogemos la antenna Wayra Net 1 como podemos ver que la opción SSID automáticamente se coloca el nombre de la antenna Wayra Net 1

Finalmente damos Clic en el botón Apply de la parte inferior de la pantalla y esperamos que el equipo reinicie por unos 30 segundos.

Authentication Open System ▾

Key Settings

Encryption ☒ Disabled ☐ Enabled

Key Type HEX ▾ Key Size 152 Bits ▾

Valid Key First ▾

First Key

Second Key

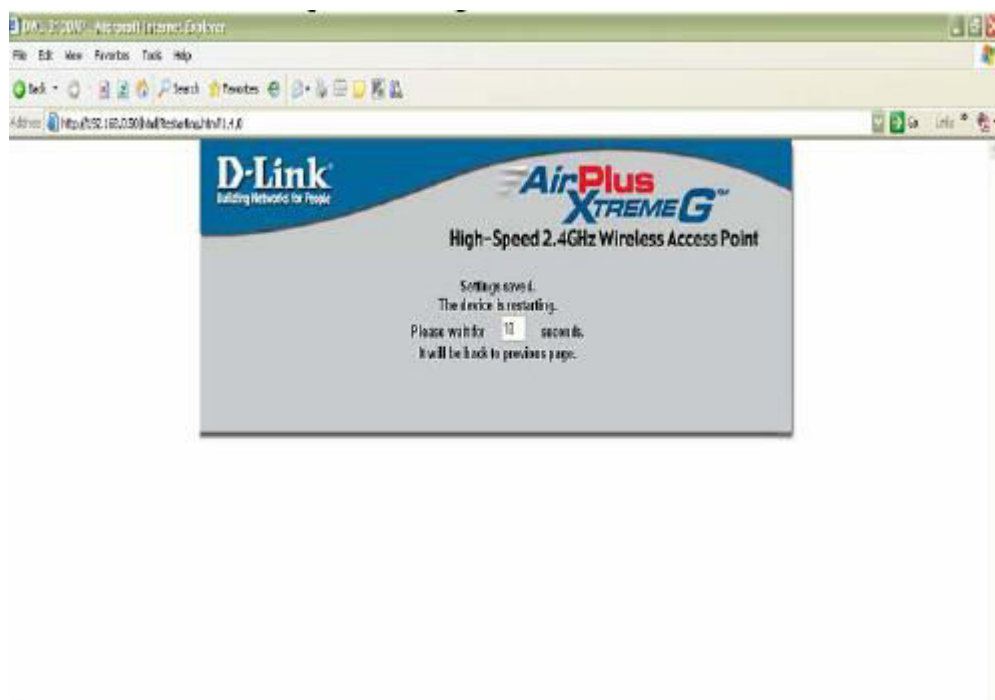
Third Key

Fourth Key

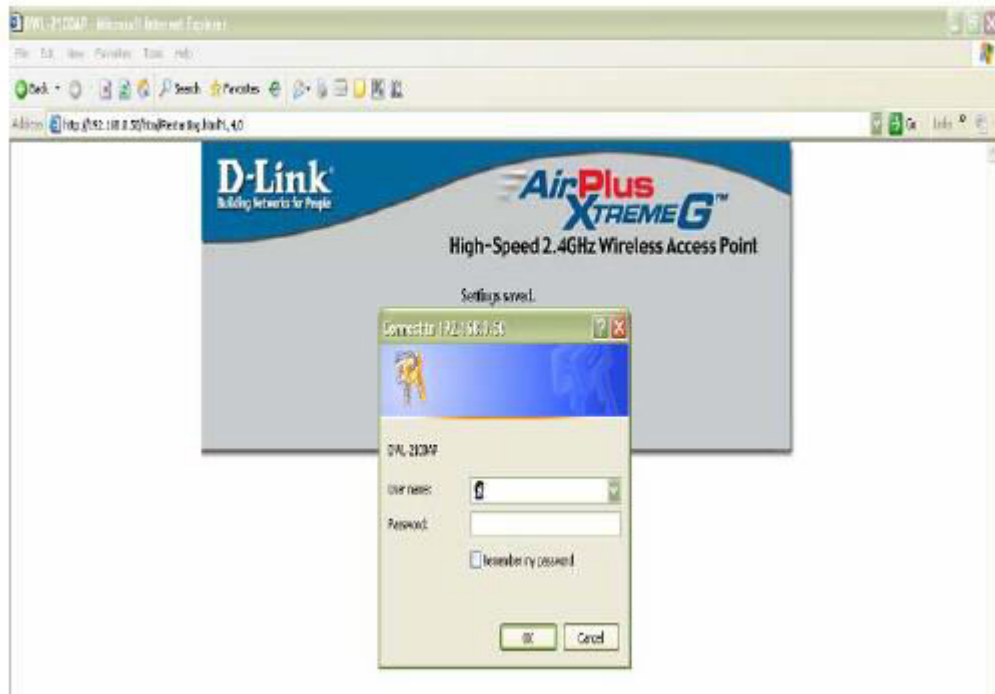
  

Apply Cancel Help

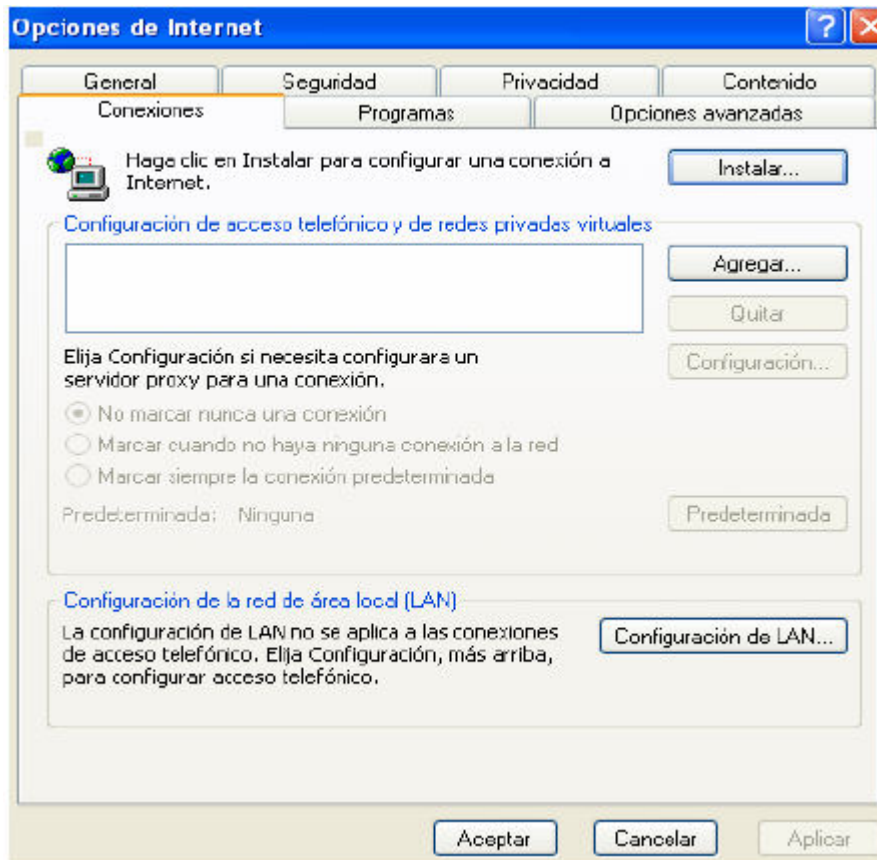
- Con esto finalizamos la configuración del Acces Point para que se conecte al servicio a través de la antena Wayra Net 1
- A continuación se mostrara la siguiente ventana



Y al término de los 30 segundos aparecerá una ventana de conexión, no coloque nada ni en el usuario ni en el Password



- Cerramos LA pantalla del navegador y nuevamente ingresamos a conexiones de red, para asignar el nuevo IP de la Pc que hará uso del servicio de Internet, El nuevo IP será automático al igual que el servidor DNS.
- Seguidamente abrimos el navegador web, ingresamos a la opción herramientas luego opciones de Internet, se nos muestra una pantalla, en la que hacemos clic en la pestaña conexiones



Hacemos clic en el botón de configuraciones de LAN, y activamos el check de utilizar Proxy para su LAN y la colocamos la dirección del Proxy 172.16.0.1, y el puerto 8080, tal como se muestra en la figura

Configuración de la red de área local (LAN)

Configuración automática

La configuración automática puede superponerse a la manual. Para evitar que esto ocurra, deshabilite la configuración automática.

☐ Detectar la configuración automáticamente

☐ Usar secuencia de comandos de configuración automática

Dirección:

Servidor proxy

Utilizar un servidor proxy para su LAN. Esta configuración no se aplicará a conexiones de acceso telefónico o de redes privadas virtuales (VPN).

☒ Dirección: Puerto: [Opciones avanzadas...](#)

☐ No usar servidor proxy para direcciones locales

[Aceptar](#) [Cancelar](#)

Hacemos clic en opciones avanzadas y nos aseguramos que la configuración este como se muestra a continuación

Configuración de los servidores proxy

Servidores

Tipo	Dirección del servidor proxy	Puerto
HTTP:	172.16.0.1	8080
Seguro:	172.16.0.1	8080
FTP:	172.16.0.1	8080
Gopher:	172.16.0.1	8080
Socks:		

☒ Usar el mismo servidor proxy para todos los protocolos

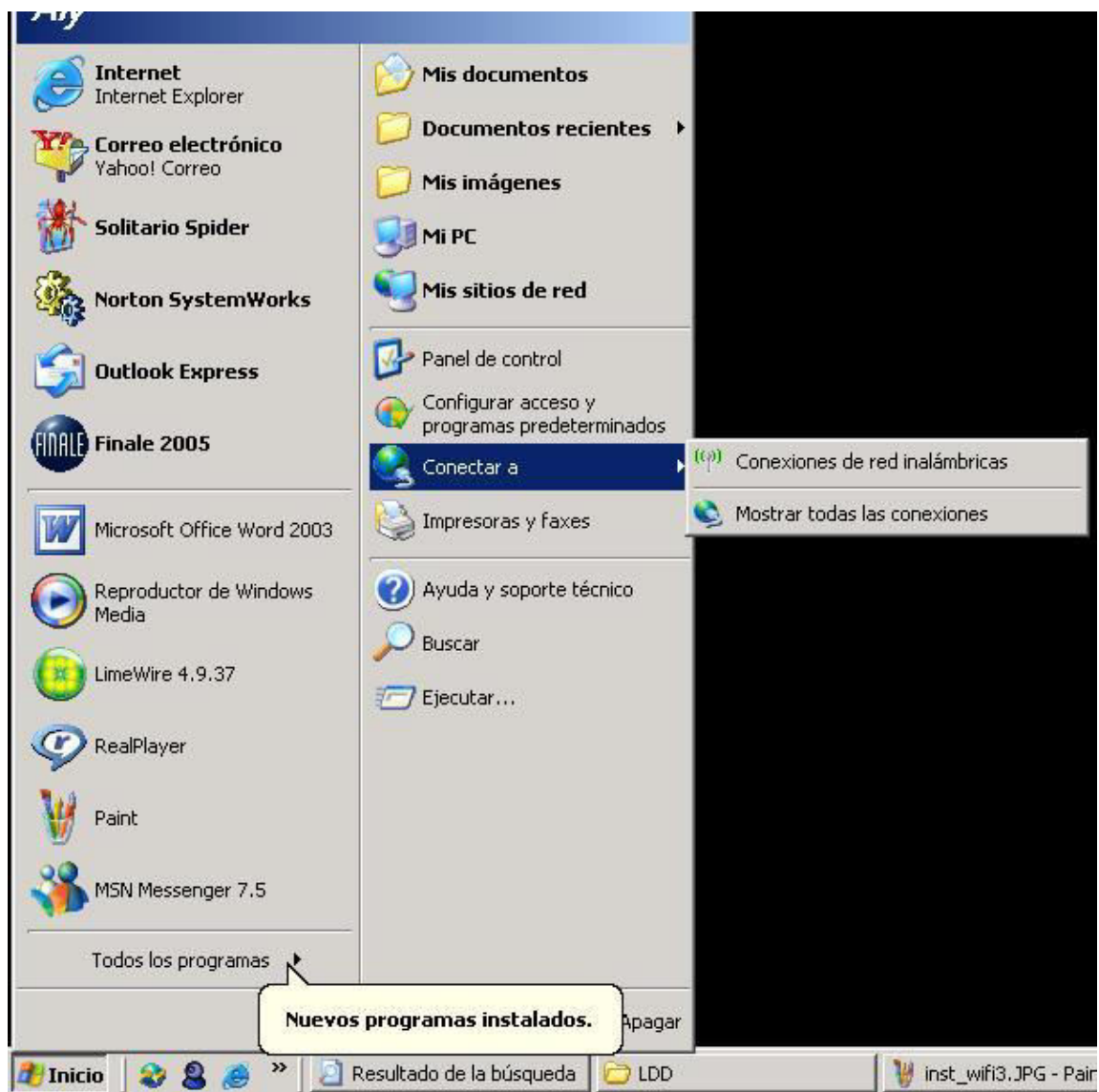
Excepciones

No usar proxy para las direcciones que comiencen por:

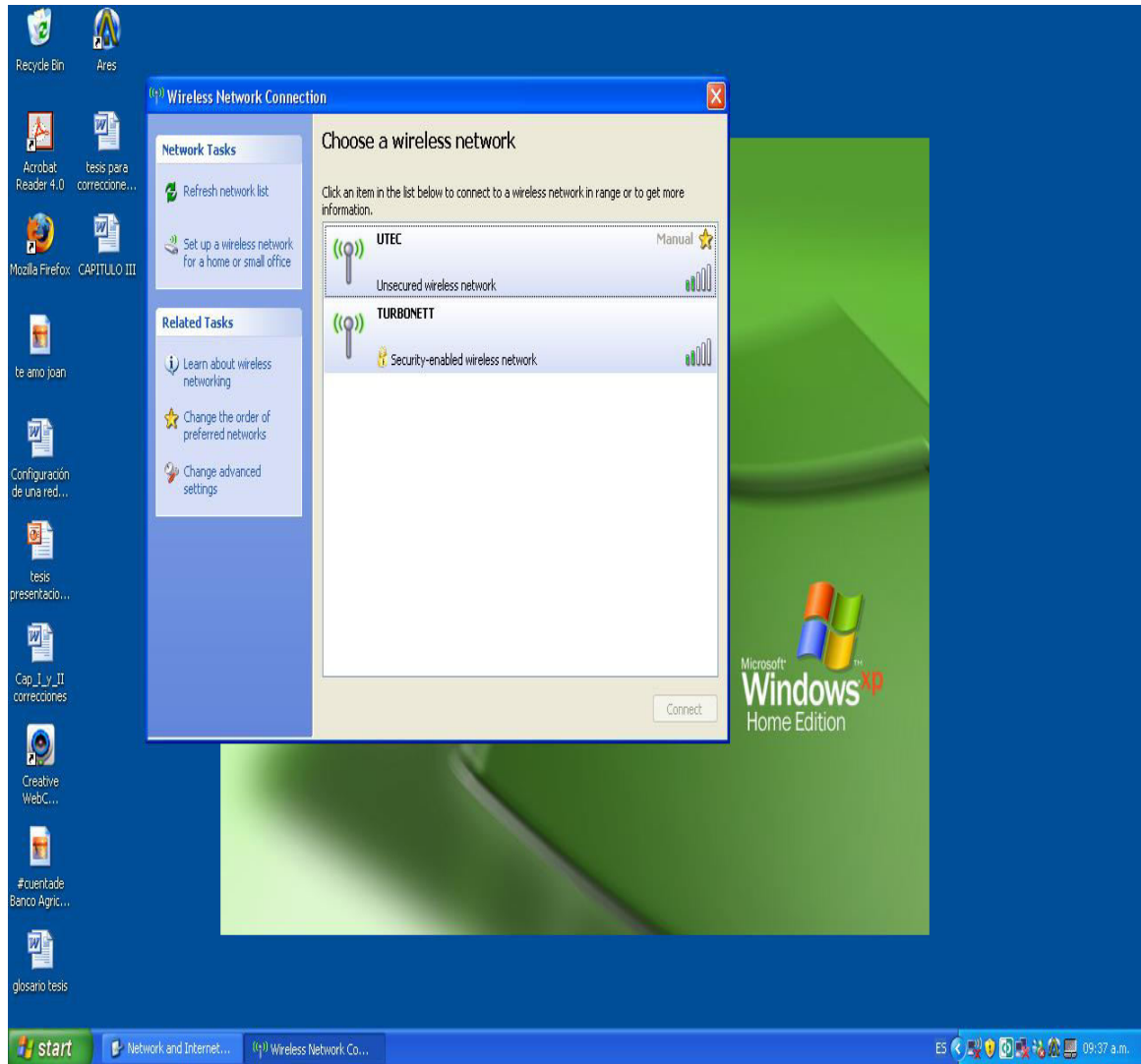
Utilizar punto y coma (;) para separar entradas.

[Aceptar](#) [Cancelar](#)

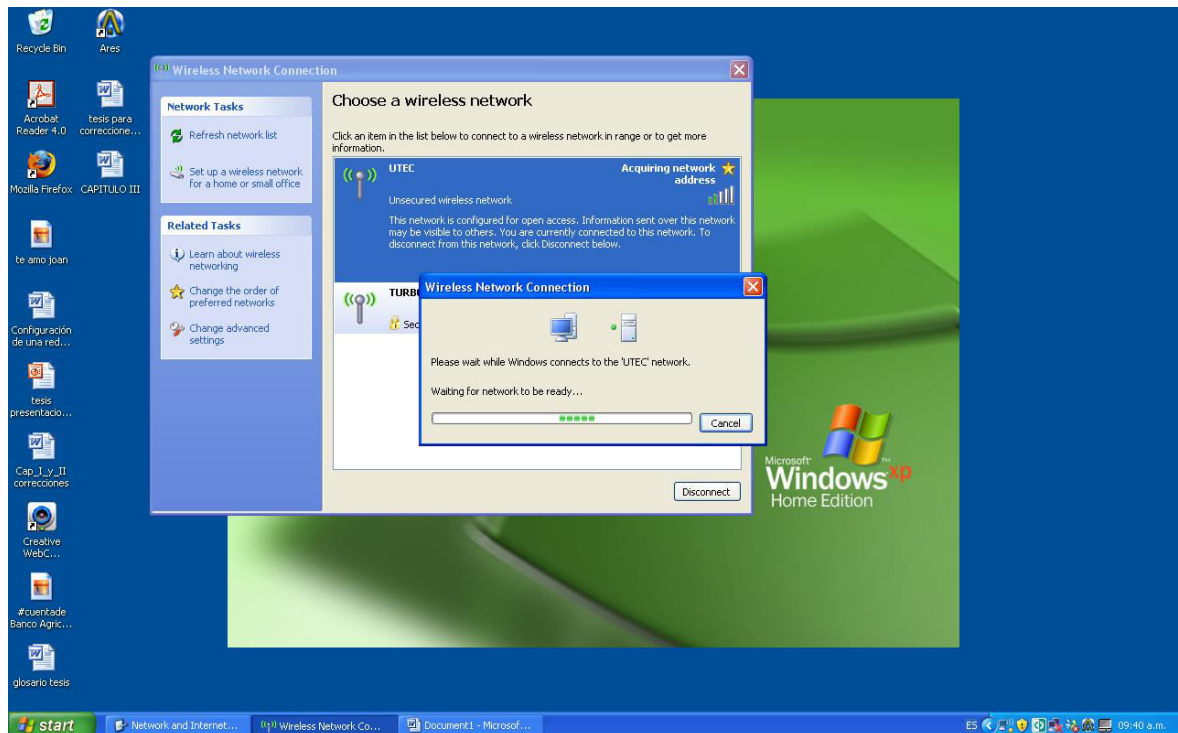
- Hacemos clic en aceptar, hasta cerrar todas las ventanas, incluso el navegador, Con eso hemos facilitado el acceso a Internet a través del Proxy.
- Para verificación ingresamos nuevamente al navegador y se nos mostrara una ventana donde se nos permita ingresar el usuario y la contraseña del cliente.



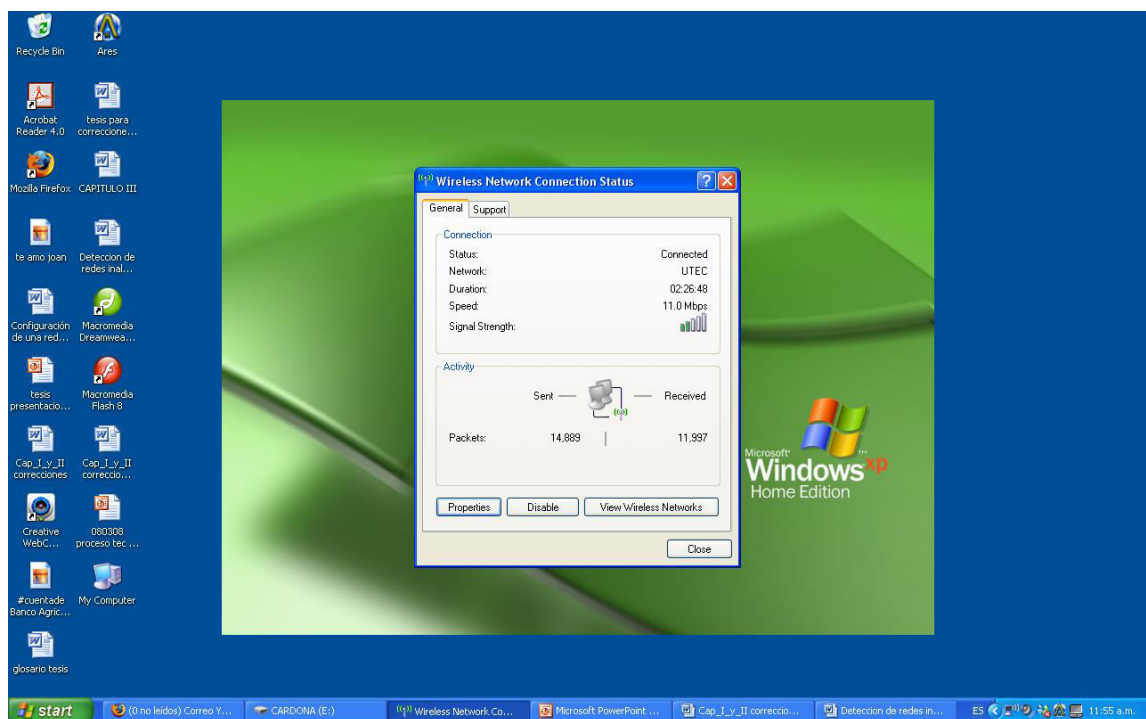
Se nos abrirá una nueva ventana llamada “Conexiones de red inalámbricas” y ro de esta ventana en el lado izquierdo haremos clic en “Configurar una red inalámbrica doméstica o de pequeña oficina:



Detección de redes inalámbricas



Conexión de a la red inalámbrica



2.21 Nombres de las Redes Inalámbricas

Las redes inalámbricas, tanto si funcionan en modo de infraestructura como en modo ad hoc, utilizan un nombre que se denomina identificador del conjunto de servicios (SSID) para identificar una red inalámbrica específica. Cuando los clientes inalámbricos se inician por primera vez, exploran la banda de frecuencias inalámbricas en busca de tramas de señalización especiales que envían los puntos de acceso inalámbricos o los clientes inalámbricos en modo ad hoc. Las tramas de señalización contienen el SSID, también denominado nombre de red inalámbrica. En la lista acumulada de nombres de red inalámbrica recopilados durante el proceso de exploración, el cliente inalámbrico puede determinar la red inalámbrica con la que se intentará establecer conexión. Uno de los elementos de la configuración de una red inalámbrica es seleccionar un nombre para la red inalámbrica. Si va a crear una nueva red inalámbrica, el nombre que elija debe ser distinto de los nombres de las demás redes dentro del intervalo de exploración. Por ejemplo, si va a crear una red inalámbrica en su casa y su vecino ya ha creado una que se llama HOGAR y es visible desde su casa, debe elegir otro nombre distinto de HOGAR.

Después de haber seleccionado un nombre de red inalámbrica y haberlo configurado para el punto de acceso inalámbrico (modo de infraestructura) o un cliente inalámbrico (modo ad hoc), dicho nombre será visible desde cualquier nodo inalámbrico IEEE. La búsqueda de redes inalámbricas ("war driving" en inglés) consiste en conducir por barrios de negocios o residenciales buscando nombres de redes inalámbricas. Cualquiera que condujera cerca de su red inalámbrica podría ver su nombre, pero que pudiera hacer algo más que ver el nombre de la red inalámbrica está determinado por el uso de la seguridad inalámbrica.

Con la seguridad inalámbrica habilitada y configurada correctamente, los buscadores de redes inalámbricas verían el nombre de la red y se unirían a ella, pero no podrían enviar datos, interpretar los datos enviados en la red inalámbrica, tener acceso a los recursos de la red inalámbrica o con cables (archivos compartidos, sitios Web privados, etc.) ni utilizar su conexión a Internet.

Sin la seguridad inalámbrica habilitada y configurada correctamente, los buscadores de redes inalámbricas podrían enviar datos, interpretar los datos enviados en la red inalámbrica, tener acceso a los recursos compartidos de la red inalámbrica o con cables (archivos compartidos, sitios Web privados, etc.), instalar virus, modificar o destruir información confidencial y utilizar su conexión a Internet sin su conocimiento o consentimiento. Por ejemplo, un usuario malintencionado podría utilizar su conexión a Internet para enviar correo electrónico o lanzar ataques contra otros equipos. El seguimiento del tráfico malintencionado llevaría a su casa o pequeña empresa.

Por estos motivos, Microsoft apremia a habilitar y configurar correctamente la seguridad inalámbrica.

2.22 Seguridad inalámbrica

La seguridad de IEEE 802.11 consta de cifrado y de autenticación. El cifrado se utiliza para cifrar o codificar, los datos de las tramas inalámbricas antes de que se envíen a la red inalámbrica. Con la autenticación se requiere que los clientes inalámbricos se autenticuen antes de que se les permita unirse a la red inalámbrica.

Cifrado

Están disponibles los siguientes tipos de cifrado para su uso con las redes 802.11:

WPA y WPA2

Cifrado WEP

Para el cifrado de los datos inalámbricos, el estándar 802.11 original definió la privacidad equivalente por cable (WEP). Debido a la naturaleza de las redes inalámbricas, la protección del acceso físico a la red resulta difícil. A diferencia de una red con cables donde se requiere una conexión física directa, cabe la posibilidad de que cualquier usuario dentro del alcance de un punto de acceso inalámbrico o un cliente inalámbrico pueda enviar y recibir tramas, así como escuchar otras tramas que se envían, con lo que la interceptación y el espionaje remoto de tramas de red inalámbrica resultan muy sencillos.

WEP utiliza una clave compartida y secreta para cifrar los datos del nodo emisor. El nodo receptor utiliza la misma clave WEP para descifrar los datos. Para el modo de infraestructura, la clave WEP debe estar configurada en el punto de acceso inalámbrico y en todos los clientes inalámbricos. Para el modo ad hoc, la clave WEP debe estar configurada en todos los clientes inalámbricos.

Tal como se especifica en los estándares de IEEE 802.11, WEP utiliza una clave secreta de 40 bits. La mayor parte del hardware inalámbrico para IEEE 802.11 también admite el uso de una clave WEP de 104 bits. Si su hardware admite ambas, utilice una clave de 104 bits.

Nota Algunos proveedores de productos inalámbricos anuncian el uso de una clave de cifrado inalámbrico de 128 bits. Es la suma de una clave WEP de 104 bits y otro número empleado durante el proceso de cifrado denominado vector

de inicialización (un número de 24 bits). Asimismo, algunos puntos de acceso inalámbricos recientes admiten el uso de una clave de cifrado inalámbrico de 152 bits. Se trata de una clave WEP de 128 bits sumada al vector de inicialización de 24 bits. Los cuadros de diálogo de configuración de Windows XP no admiten claves WEP de 128 bits. Si debe utilizar claves de cifrado inalámbrico de 152 bits, deshabilite la configuración automática desactivando la casilla de verificación **Usar Windows para establecer mi config. De red inalámbrica** en la ficha **Redes inalámbricas** de las propiedades de la conexión inalámbrica en Conexiones de red y emplee la utilidad de configuración incluida con el adaptador de red inalámbrico.

Elección de una clave WEP

La clave WEP debe ser una secuencia aleatoria de caracteres de teclado (letras mayúsculas y minúsculas, números y signos de puntuación) o dígitos hexadecimales (números del 0 al 9 y letras de la A a la F). Cuanto más aleatoria sea la clave WEP, más seguro será su uso.

Una clave WEP basada en una palabra (como un nombre de compañía en el caso de una pequeña empresa o el apellido si se trata de una red doméstica) o en una frase fácil de recordar se puede averiguar fácilmente. Después de que el usuario malintencionado haya determinado la clave WEP, puede descifrar las tramas cifradas con WEP, cifrar tramas WEP correctamente y comenzar a atacar la red.

Aunque la clave WEP sea aleatoria, todavía se puede averiguar si se recopila y analiza una gran cantidad de datos cifrados con la misma clave. Por lo tanto, se recomienda cambiar la clave WEP por una nueva secuencia aleatoria periódicamente, por ejemplo, cada tres meses.

Cifrado WPA

IEEE 802.11i es un nuevo estándar que especifica mejoras en la seguridad de las redes locales inalámbricas. El estándar 802.11i soluciona muchos de los problemas de seguridad del estándar 802.11 original. Mientras se ratifica el nuevo estándar IEEE 802.11i, los proveedores de productos inalámbricos han acordado un estándar intermedio ínter operable denominado WPA™ (acceso protegido Wi-Fi).

Con WPA, el cifrado se realiza mediante TKIP (Protocolo de integridad de claves temporales), que reemplaza WEP por un algoritmo de cifrado más seguro. A diferencia de WEP, TKIP proporciona la determinación de una única clave de cifrado de uní difusión de inicio para cada autenticación y el cambio sincronizado de la clave de cifrado de uní difusión para cada trama. Debido a que las claves TKIP se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA.

Microsoft proporciona compatibilidad con WPA para los equipos con Windows XP con Service Pack 2 (SP2). Para los equipos con Windows XP con Service Pack 1 (SP1), se debe obtener e instalar el [paquete de conjuntos de actualizaciones inalámbricas para Windows XP](#), una descarga gratuita de Microsoft.

Cifrado WPA2

WPA2™ es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar 802.11i. WPA2 admite las características de seguridad obligatorias adicionales del estándar 802.11i que no están incluidos para productos que admitan WPA. Con WPA2, el cifrado se realiza mediante AES (estándar de cifrado avanzado), que también

reemplaza WEP por un algoritmo de cifrado más seguro. Al igual que TKIP para WPA, AES proporciona la determinación de una clave de cifrado de uní difusión de inicio exclusiva para cada autenticación y el cambio sincronizado de la clave de cifrado de uní difusión para cada trama. Debido a que las claves AES se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA2. WPA2 es la forma más eficaz de seguridad inalámbrica.

Microsoft proporciona compatibilidad con WPA2 a los equipos con Windows XP con Service Pack 2 (SP2) mediante la actualización de WPA2 (acceso protegido Wi-Fi 2)/WPS IE (elemento de información de servicios de aprovisionamiento inalámbricos) para Windows XP con Service Pack 2, una descarga gratuita de Microsoft.

Autenticación

Están disponibles los siguientes tipos de autenticación para utilizarlos con las redes 802.11:

Sistema abierto

Clave compartida

IEEE 802.1X

WPA o WPA2 con clave previamente compartida

Sistema abierto

La autenticación de sistema abierto no es realmente una autenticación, porque todo lo que hace es identificar un nodo inalámbrico mediante su dirección de hardware de adaptador inalámbrico. Una dirección de hardware es una dirección asignada al adaptador de red durante su fabricación y se utiliza para identificar la dirección de origen y de destino de las tramas inalámbricas.

Para el modo de infraestructura, aunque algunos puntos de acceso inalámbricos permiten configurar una lista de direcciones de hardware permitidas para la autenticación de sistema abierto, resulta bastante sencillo para un usuario malintencionado capturar las tramas enviadas en la red inalámbrica para determinar la dirección de hardware de los nodos inalámbricos permitidos y, a continuación, utilizar la dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica.

Para el modo ad hoc, no existe equivalencia para la configuración de la lista de direcciones de hardware permitidas en Windows XP. Por lo tanto, se puede utilizar cualquier dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica basada en el modo ad hoc.

Clave compartida

La autenticación de clave compartida comprueba que el cliente inalámbrico que se va a unir a la red inalámbrica conoce una clave secreta. Durante el proceso de autenticación, el cliente inalámbrico demuestra que conoce la clave secreta sin realmente enviarla. Para el modo de infraestructura, todos los clientes inalámbricos y el punto de acceso inalámbrico utilizan la misma clave compartida. Para el modo ad hoc, todos los clientes inalámbricos de la red inalámbrica ad hoc utilizan la misma clave compartida.

IEEE 802.1X

El estándar IEEE 802.1X exige la autenticación de un nodo de red para que pueda comenzar a intercambiar datos con la red. Si se produce un error en el proceso de autenticación, se deniega el intercambio de tramas con la red. Aunque este estándar se diseñó para las redes Ethernet inalámbricas, se ha adaptado para su uso con 802.11. IEEE 802.1X utiliza EAP (Protocolo de

autenticación extensible) y métodos de autenticación específicos denominados tipos EAP para autenticar el nodo de red.

IEEE 802.1X proporciona una autenticación mucho más segura que el sistema abierto o la clave compartida y la solución recomendada para la autenticación inalámbrica de Windows XP es el uso de EAP-TLS (Transport Layer Security) y certificados digitales para la autenticación. Para utilizar la autenticación EAP-TLS para las conexiones inalámbricas, debe crear una infraestructura de autenticación que conste de un dominio de Active Directory, servidores RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) y entidades emisoras de certificados para emitir certificados a los servidores RADIUS y los clientes inalámbricos. Esta infraestructura de autenticación resulta más adecuada para grandes empresas y organizaciones empresariales, pero no es práctica para una oficina doméstica o de pequeña empresa.

La solución al uso de IEEE 802.1X y EAP-TLS para las pequeñas y medianas empresas es PEAP (EAP protegido) y el protocolo de autenticación por desafío mutuo de Microsoft, versión 2 (MS-CHAP v2) tipo EAP. Con PEAP-MS-CHAP v2, se puede lograr un acceso inalámbrico seguro mediante la instalación de un certificado adquirido en un servidor RADIUS y utilizando credenciales de nombre y contraseña para la autenticación. Windows XP con SP2, Windows XP con SP1, Windows Server 2003 y Windows 2000 con Service Pack 4 (SP4) admiten PEAP-MS-CHAP v2.

WPA o WPA2 con clave previamente compartida

Para una red doméstica o de pequeña empresa donde no se pueda realizar la autenticación 802.1X, WPA y WPA2 proporcionan un método de autenticación de clave previamente compartida para redes inalámbricas en modo de

infraestructura. La clave previamente compartida se configura en el punto de acceso inalámbrico y en cada cliente inalámbrico. La clave de cifrado WPA o WPA2 inicial se deriva del proceso de autenticación, que comprueba que tanto el cliente inalámbrico como el punto de acceso inalámbrico están configurados con la misma clave previamente compartida. Cada clave de cifrado WPA o WPA2 inicial es exclusiva.

La clave WPA o WPA2 previamente compartida debe ser una secuencia aleatoria de caracteres de teclado (letras mayúsculas y minúsculas, números y signos de puntuación) de una longitud mínima de 20 caracteres o dígitos hexadecimales (números del 0 al 9 y letras de la A a la F) de una longitud mínima de 24 dígitos hexadecimales. Cuanto más aleatoria sea la clave WPA o WPA2 previamente compartida, más seguro será su uso. A diferencia de la clave WEP, la clave WPA o WPA2 previamente compartida no está sujeta a la determinación mediante la recopilación de una gran cantidad de datos cifrados. Por lo tanto, no es necesario cambiar la clave WPA o WPA2 previamente compartida con tanta frecuencia.

2.23 REDES DE AREA PERSONAL INALAMBRICAS

(BLUETOOTH)

INTRODUCCION A LAS REDES DE AREA PERSONAL.

Wireless Personal Area Networks, Red Inalámbrica de Área Personal o Red de área personal o Personal área network es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras)

cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

Evolución

Las comunicaciones inalámbricas experimentaron un crecimiento muy importante dentro de la última década (GSM, IS-95, GPRS y EDGE, UMTS, y IMT-2000). Estas tecnologías permitieron una altísima transferencia de datos dentro de las soluciones de sistemas o redes inalámbricas. La ventaja de las comunicaciones inalámbricas es que con la Terminal, la persona se puede mover por toda el área de cobertura, lo que no ocurre con las redes de comunicaciones fijas; esto permitirá el desarrollo de diferentes soluciones PAN y cambiará el concepto de los espacios personales.

Las bases del concepto de red para espacio personal provinieron de ideas que surgieron en el año 1995 en el Massachusetts Institute of Technology (MIT) provienen para usar en señales eléctricas o impulsos eléctricos provenientes del cuerpo humano, y así poder comunicar el mismo con dispositivos adjuntos. Esto fue aceptado en primera instancia por los laboratorios de IBM Research y luego tuvo muchas variaciones desarrolladas por las diferentes instituciones y compañías de investigación. Las diferentes soluciones de PAN incluyen lo siguiente:

- Proyecto Oxygen (MIT);
- Pico-radio;
- Infrared Data Association (IrDA);
- Bluetooth;
- IEEE 802.15

El concepto de Bluetooth, originalmente desarrollado para reemplazar a los cables, está siendo aceptado mundialmente, y algunas de estas ideas son incorporadas en el estándar IEEE 802.15 relacionado a las PANs.

2.23.1 Conceptos Actuales

PAN es un Nuevo miembro de la familia GIMCV. El espacio personal abarca toda el área que puede cubrir la voz. Puede tener una capacidad en el rango de los 10 bps hasta los 10 Mbps. Existen soluciones (ejemplo, Bluetooth) que operan en la frecuencia libre para instrumentación, ciencia y medicina de sus siglas en ingles (instrumental, scientific, and medical ISM) en su respectiva banda de frecuencia de 2.4 GHz. Los sistemas PAN podrán operar en las bandas libres de 5 GHz o quizás mayores a éstas. PAN es un concepto de red dinámico que exigirá las soluciones técnicas apropiadas para esta arquitectura, protocolos, administración, y seguridad.

PAN representa el concepto de redes centradas a las personas, las cuales permite a las personas comunicarse con sus dispositivos personales (ejemplo, PDAs, tableros electrónicos de navegación, agendas electrónicas, computadoras portátiles) y así poder establecer una conexión inalámbrica con el mundo externo.

El Paradigma PAN

Las redes para espacios personales continúan desarrollándose hacia la tecnología del Bluetooth hacia el concepto de redes dinámicas, el cual nos permite una fácil comunicación con los dispositivos que van adheridos a nuestro cuerpo o a nuestra indumentaria, ya sea que estemos en movimiento o no, dentro del área de cobertura de nuestra red. PAN prevé el acercamiento de un paradigma de redes, la cual atrae el interés a los investigadores, y las industrias que quieren aprender más acerca de las soluciones avanzadas para redes,

tecnologías de radio, altas transferencias de bits, nuevos patrones para celulares, y un soporte de software más sofisticado.

El PAN debe proporcionar una conectividad usuario a usuario, comunicaciones seguras, y QoS que garanticen a los usuarios. El sistema tendrá que soportar diferentes aplicaciones y distintos escenarios de operación, y así poder abarcar una gran variedad de dispositivos.

Posibles equipos o dispositivos

Las diferentes demandas del servicio y los panoramas de uso hacen que PAN acumule distintos acercamientos hacia las funciones y capacidades que pueda tener. Algunos dispositivos, como un simple sensor pito, pueden ser muy baratos, y tener a su vez funciones limitadas. Otros pueden incorporar funciones avanzadas, tanto computacionales como de red, lo cual los harán más costosos. Deben preverse los siguientes puntos como importantes para su fácil escalabilidad:

- Funcionalidad y Complejidad;
- Precio;
- Consumo de energía;
- Tarifas para los datos;
- Garantía;
- Soporte para las interfaces.

Los dispositivos más capaces pueden incorporar funciones multimodo que permiten el acceso a múltiples redes.

Algunos de estos dispositivos pueden estar adheridos o usados como vestimenta para la persona, otros podrían ser fijos o establecidos

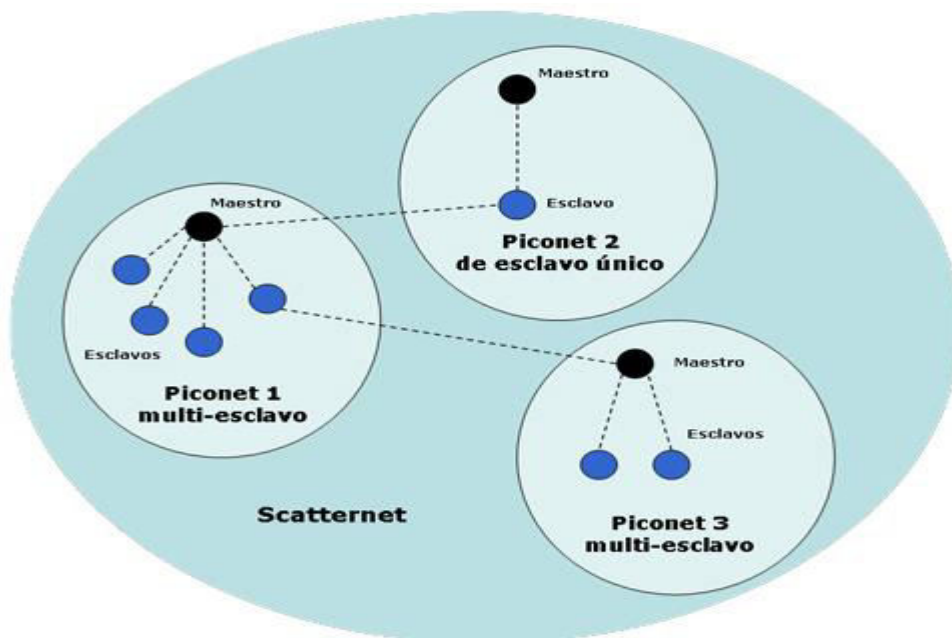
temporalmente con el espacio personal (ejemplo, sensores, impresoras y PDA's).

2.23.2 TOPOLOGIA DE RED BLUETOOTH

Bluetooth es un estándar que trabaja a una frecuencia de 2.4GHz disponible a nivel mundial, no requiere una licencia de operación y evita interferencias con otros dispositivos de comunicación. Los medios de comunicación bluetooth brindan el servicio de comunicación de forma estática y móvil siempre y cuando se encuentre dentro del radio de cobertura de la frecuencia o señal del dispositivo, también permite realizar sincronización de conexiones punto a punto y multipunto con sus respectivas normas.

El modelo de comunicación que se utiliza para sincronización de uno o varios dispositivos sobre comunicaciones bluetooth se basa en establecer un dispositivo maestro para realizar las conexión punto a punto o multipunto entre dispositivos de comunicación, en el cual el dispositivo maestro realiza la sincronización desde el punto de vista del reloj de tiempo y los saltos de frecuencia que realiza de canal en canal para sincronizar los dispositivos. Los dispositivos que se sincronizan con el maestro son llamados esclavos, los cuales pueden ser de 1 a 8 dispositivos esclavos, a este modelo de red se le denomina: Piconet .

La topología bluetooth se basa en la conformación de una o varias piconet, donde la unión de varias piconets se le denomina Scatternet, cabe mencionar que entre piconets cada uno de los dispositivos esclavos pueden ser participes en las distintas piconets mediante el enlace maestro de cada piconet, para este proceso se utiliza una Multiplexación por División de Tiempo (TDM) la cual permite que cada dispositivo esclavo de una piconet tendrá acceso de presencia en forma secuencial en una piconet a la vez. Observar el ejemplo



Topología Bluetooth.

Bluetooth es una tecnología que se incorpora y en la actualidad aún se sigue incorporando a distintos dispositivos móviles o estáticos, formando así una amplia gama de productos al alcance del usuario y de uso cotidiano. Los cuales brindan un servicio de comunicación e intercambio de información entre dispositivos bluetooth gracias al perfil OBEX FTP, el cual permite la transferencia de archivos entre móviles disponibles en el radio de cobertura disponible.

Los archivos que se pueden intercambiar entre dispositivos bluetooth utilizando el perfil OBEX FTP, va desde archivos de audio, texto, sincronización agendas, sincronización entre dispositivo y computadora, etc. Todo esto y más brindan los distintos productos existentes en el mercado que incorporan la tecnología bluetooth.

A continuación se listan en forma de categorías las distintas gamas de productos existentes:

Dispositivos de informática bluetooth.

Productos de hardware para sistemas de computo los cuales permitan la sincronización entre un ordenador y un sistema móvil que posea la tecnología bluetooth, estos van desde equipos portátiles que incorporan bluetooth integrado, pastillas USB para equipos de cómputo y pasarelas (gateways) de acceso a otras redes.



Dispositivos de Informática Bluetooth.

Dispositivos de entrada y salida Bluetooth.

Productos disponibles para equipos de cómputo los cuales permiten la comunicación de periféricos con una computadora y viceversa, estos pueden ser teclados, ratones, impresoras, etc.



Dispositivos de Entrada y Salida Bluetooth.

La amplia gama de productos ya mencionados por categoría pueden ser sincronizados entre sí para formar piconets en cualquier parte del mundo, también se pueden realizar sincronización entre piconets para conformar las scatternets, todo esto con un fin de comunicación para intercambio de información de cualquier tipo utilizando un dispositivo móvil o estático sin necesidad de cables, utilizando solamente un radio de cobertura y alguna frecuencia que este estandarizada. A continuación se visualiza una piconet entre dispositivos.



Modelo Visual de una Piconet.

2.23.3 SEGURIDAD BLUETOOTH.

Bluetooth es una de las tecnologías con una mayor utilización día a día que los demás medios de comunicación, ya que se encuentra presente en la mayoría de los dispositivos electrónicos móviles y estáticos, como son por lo general en celulares, palms, manos libres, módulos usb, periféricos para computadoras, entre otros. Teniendo un gran impacto por la facilidad de compartición de elementos entre usuarios mediante un celular (dispositivo móvil), ahorrando utilización de cables y evitando estar en una posición fija para transferir los datos, también brinda un gran apoyo para facilitar la utilización del celular en momentos que se está realizando otra tarea, este dispositivo es el manos libres que se conecta al celular para atender las llamadas por medio de una orden de voz.

El dispositivo Bluetooth fue realizado como una tecnología al alcance de los usuarios, estableciéndose como una tecnología flexible y barata, teniendo una especificación muy definida para su incorporación en equipos móviles y estáticos, formando un dispositivo con poco consumo de energía, brindando transferencia de información de forma punto a punto o multipunto y una pila de protocolos muy amplia para adaptarse en varias formas de uso: voz, archivos, audio, video, etc. Uno de los puntos más débiles de Bluetooth es su seguridad.

Logotipo Bluetooth.



ESTANDAR Y ESPECIFICACIONES DE BLUETOOTH

Bluetooth es el nuevo estándar para comunicación de dispositivos electrónicos, estos van desde dispositivos pequeños como son: celulares, palms, manos libres (audífonos), impresoras, ratones, teclados, pastillas USB, micrófonos, entre otros, que permiten la transmisión de voz y datos mediante un enlace radiofrecuencia a una distancia específica dependiendo del alcance del dispositivo bluetooth.

El proyecto Bluetooth surge en 1994 por la compañía Ericsson Mobile Communications sobre un dispositivo que funcionase como medio de comunicación entre dispositivos móviles, utilizando un enlace de radiofrecuencia y un bajo consumo de energía para dispositivos que utilizan baterías.

Bluetooth está conformado por dos símbolos que son:

* Las Ruinas Nordicas Hagalaz. 

* Berkana. 

La Figura 2.28 muestra la mezcla de los símbolos.

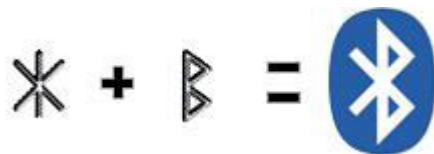


FIGURA 2.28: Formación del símbolo Bluetooth.

La especificación Bluetooth está sostenida por el grupo de trabajo IEEE 802.15.1 y se realizó con el fin de brindar un dispositivo electrónico de poco consumo eléctrico y para comunicar equipos de cómputo, celulares, dispositivos de hardware en entornos de comunicaciones móviles y estáticos. A continuación se presentan las especificaciones técnicas de bluetooth:

- Trabaja a una frecuencia de radio de 2.4GHz a 2.8GHz.
- Emplea la técnica de salto de frecuencia (FHSS, Frequency Hopping Spread Spectrum), que consiste en dividir la banda en 79 canales a una longitud de 1 Mhz y realizar 1,600 saltos.
- La potencia de transmisión varía según la versión del núcleo bluetooth:
 - Versión 1.1: 723.1 Kbps.
 - Versión 1.2: 1 Mbps. Versión 2.0+EDR: de 2.1 Mbps a 3 Mbps.
- La potencia de transmisión se divide en tres clases de productos:
 - Clase 1: 100 mW/20 dBm, con un rango de 100m.
 - Clase 2: 2.5 mW/4 dBm, con un rango de 10m.
 - Clase 3: 1 mW/0 dBm, con un rango de 1m.
- Utiliza protocolo de banda base para hacer una mejor transmisión de voz y datos.
- Los tipos de enlaces soportados para voz y datos son:
 - Enlace asíncrono sin conexión (ACL, Asynchronous Connectionless).
 - Enlace síncrono orientado a conexión (SCO, Synchronous Connection-Oriented).
- En 1999 se ratificó la versión 1.0 de bluetooth, de modo que las mejoras fueron las siguientes:
 - Versión 1.1: Soluciona errores de la versión 1.0. Añade indicadores de calidad de señal recibida (RSSI).
 - Versión 1.2:

- Implementa el salto de frecuencia (Adaptive Frequency Hopping).
 - Implementa tipo de enlace para aplicaciones de audio extended Synchronous Connections (eSCO) que mejora la calidad de voz.
 - Mejoras en el Host Controller Interface (HCI) para una sincronización más rápida.
- Versión 2.0:
 - Nueva versión compatible con anteriores 1.x.
 - Incorpora tecnología Enhanced Data Rate (EDR) que incrementa la velocidad de transmisión hasta 3 Mbps.
 - Reducción de consumo de energía.

CAPITULO III

PROYECTO TEMATICO

3.1 PLANTEAMIENTO DEL PROYECTO TEMATICO.

El proyecto se ha desarrollado para brindar una herramienta básica y sencilla de comprender para el área de redes inalámbricas, en apoyo a los estudiantes de la carrera Técnico .en Ingeniería de Redes computacionales por medio de un cd interactivo, el cual mostrara detalladamente los procesos para la instalación y configuración de los diferentes dispositivos para redes inalámbricas, como lo son tarjetas de redes inalámbricas, Acces Point y Router inalámbricos, por tanto es necesario recolectar información técnica documental que sirva como guía referencial para el proceso de enseñanza aprendizaje, detallando aspectos principales que conforman el cd interactivo denotando un perfil bastante amplio de las redes inalámbricas.

PRIMERA FASE

Tecnologías a utilizar, en la elaboración del cd interactivo.

Esta fase consiste en investigar detalladamente la documentación que se necesita para poder realizar, un manual interactivo, tomando aspectos indispensables, como contenido multimedia, digitalización de medios,

aplicaciones para la edición de video digital, de audio digital y texto, donde el usuario pueda interactuar con el material interactivo que se presenta en el cd.

Su contenido debe estar acorde a las necesidades del estudiante presentando documentación confiable, que sirva para desarrollar instalaciones y configuraciones inalámbricas de fácil acceso.

Actividades

1. Recopilar información sobre redes inalámbricas para la elaboración del cd interactivo
2. Seleccionar información adecuada y necesaria de cómo instalar y configurar los dispositivos que componen una red inalámbrica
3. Investigar que requerimientos necesitamos saber para elaborar el cd interactivo

SEGUNDA FASE.

Generalidades de cómo instalar y configurar una red inalámbrica.

La información recopilada necesaria para enseñar a instalar y configurar una red una red inalámbrica, así también como usar los diferentes dispositivos que se utilizan en la red, como lo son tarjetas inalámbricas, access point y routers inalámbricos, teniendo en cuenta la seguridad que debe de ir a la par de la configuración evitando el acceso no autorizado a personas ajenas a nuestra red inalámbrica.

Actividades

1. Investigar la información necesaria para interconectar Nodos Inalámbricos con Acces Point y muchos otros dispositivos
2. Desarrollar paso a paso la instalación y configuración de una red inalámbrica
3. Desarrollar mecanismos de seguridad en redes inalámbricas

TERCERA FASE

Conocimientos adquiridos en el trayecto de la elaboración del producto.

Con la finalización del proyecto, en el cual se proporciona la información tanto teórica como práctica para crear el cd interactivo donde se encontrara paso a paso como instalar y configurar una red inalámbrica.

De tal forma se dará por terminado el cd interactivo, siendo este una base para los estudiantes de la carrera Técnico .en Ingeniería de Redes Computacionales de la Universidad Tecnológica.

Las actividades a realizar son las siguientes:

- Desarrollo del cd interactivo.
- Instalación y configuración de redes inalámbricas.
- Captura de pantallas.

- Edición de video.
- Edición de contenido y.
- Finalización del producto.

3.2. CRONOGRAMA DEL PROYECTO

3.2 CRONOGRAMA DEL PROYECTO

					ABRIL 2008				MAYO 2008	
					Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6
ID	Nombre de Tarea	Duración (Días)	Comienzo	Fin	9-13 abr	14-20 abr	14-20 abr	21-27 abr	28 abr - 4 may	5 -10 may
	Capitulo IV									
1	Articulo	29	9-abr	8-may						
2	Recopilación de información para el Cd Interactivo	12	25-abr	9-may						
3	Elaboración del Prototipo	14	28-abr	9-may						
4	Presentación del Prototipo (Power Point)	2	5-may	6-may						
5	Evidencia del Avance del Proyecto	3	7-may	9-may						
6	Entrega del Proyecto	1	10-May	10-May						

3.3 DOCUMENTACION TECNICA

3.3.1 SOFTWARE PARA CREAR ANIMACIONES FLASH

- **Flash Saber 6.30 (VER ANEXO 1)**

Flash Saver es una utilidad para poder guardar las animaciones Flash que se encuentran en cualquier página Web.

Permite guardar los archivos Flash en diferentes categorías y aprovecha que ya han descargado los archivos simplemente al verlos y cuando decidas guardarlo lo hará directamente desde caché (a menos que especifiques lo contrario).

- **Selteco Alligátor Flash Designer 7.0.6 (VER ANEXO 2)**

Es una herramienta para todos, con muchas posibilidades, con un entorno intuitivo.

Desde menús o botones pasando por presentaciones de imágenes e introducciones en Flash, hasta formularios interactivos y animaciones con fotos y vídeos, cliparts y GIF animados, etc. Permite integrar vídeos y sonidos de fondo, incluso sacar provecho de la potencia brindada por ActionScript 2.0 para crear eventos y acciones Flash. Luego exportar la creación a SWF y a disfrutar de ella.

- **Macromedia Flash MX 2004 (VER ANEXO 3)**

Macromedia Flash es la herramienta de desarrollo Flash original, el programa mezcla gráficos vectoriales, bitmaps, sonido, animaciones y una interactividad avanzada para crear espectaculares webs que atraigan y entretengan a los visitantes.

Macromedia Flash MX ofrece un lenguaje de scripts (action script) para crear aplicaciones interactivas, juegos, efectos interfaces para web, etc.

3.3.2 SOFTWARE PARA CREAR CD-DVS CON MENÚS AUTOEJECUTABLES

- **CD Autorun creador 4.6 (VER ANEXO 4)**

CD Autorun Creator 4.6 es una herramienta mediante la cual podrás crear tanto CDs como DVDs autoejecutables con el contenido que se quiera almacenar en cada uno de ellos (música, fotografías, videos, documentos, etc), iniciándose así automáticamente cada vez que se introduzca en cualquier dispositivo de cd-drive.

Dispone de una serie de plantillas que sirven de guía y asistente para crear los CD/DVD lo más personalizados a tu gusto, así como poder incluir efectos de transición entre los distintos contenidos del CD/DVD.

- **CD Interface Studio 2.3.6.1 (VER ANEXO 5)**

CD Interface Studio permite crear muy fácilmente unos menús de carácter básico para tus CDs o DVDs de datos. El menú creado aparecerá automáticamente en cuanto se introduzca el disco en la bandeja. Esta utilidad es especialmente práctica para los discos en los que se graban cientos de programas o archivos distintos, que suelen ser extremadamente difíciles de manejar y de moverse por ellos.

A la hora de crear los menús, podremos incluir el nombre de cada archivo, programa o elemento del disco, junto con una pequeña descripción. Además, dispondremos de un buscador global para todo el disco.

- **Autoplay Express 4.2 (VER ANEXO 6)**

Con este programa podemos darle un toque personal e intransferible.

Por un lado, podemos crear nuestras propias carátulas y trabajos gráficos, etiquetas etc._ Para decorarlo y por otro, podemos diseñarle e incluir un menú de reproducción personalizado._Para esta segunda opción disponemos de este programa Autoplay Express.

Con Autoplay Express podemos crear fácilmente menús de autoarranque para nuestro disco CD o DVD, de forma que se abra automáticamente nada más

introducirlo en el lector. Además de darnos acceso a todas sus funciones y contenidos, también podremos visualizar algunos detalles sobre el mismo.

- **Autoption Graphic 8.0**

Autoption Graphic es un software que permite a los usuarios crear menús con botones de aspecto profesional para discos CD y DVD, sin necesidad de ser unos expertos en la materia, Invierte el menor tiempo y el mínimo esfuerzo posible, y sorpréndete con sus excepcionales resultados._ En pocos minutos conseguirás disponer de un vistoso menú de autoarranque para tu disco.

El programa te permite escoger entre diversas plantillas de diseño, y si lo deseas incluso utilizar tus propias fotos o imágenes digitales como fondo. Autoption Graphic incluye un total de 16 estilos diferentes, cada uno de ellos con total libertad a la hora de determinar sus tonos y colores.

Los botones incluidos en el menú podrán ejecutar aplicaciones o documentos, abrir sitios de Internet, enviar mensajes de correo electrónico, abrir carpetas, mostrar mensajes, o incluso enlazar a otros submenús para dar cabida a más opciones.

Otras características de Autoption Graphic son la posibilidad de incluir efectos de animación en los botones, el asistente de creación de botones, o los siempre vistosos efectos de sombreado. Entre sus mayores ventajas podemos citar la

facilidad de manejo (es bastante intuitivo), y los resultados de apariencia claramente profesional, conseguidos sin demasiado esfuerzo.

3.3.3 SOFTWARE PARA CAPTURA DE PANTALLAS

- **Screenshot Captor 2.36.03 (VER ANEXO 7)**

Esta aplicación me permite efectuar capturas de pantalla, ya sea de forma aislada, o como actividad habitual, con mayores o menores exigencias. Puedes realizar varias capturas consecutivas, asignar teclas rápidas para determinadas tareas, capturar ventanas completas, el área total del escritorio, el trozo que tú indiques, etc. Screenshot Captor es una herramienta muy completa que, además de su amplia funcionalidad en el ámbito de las capturas, también ofrece un paquete básico de utilidades gráficas para editar y mejorar el aspecto tus capturas en cuanto las realices, asegurándote así siempre la mayor calidad.

- **Camtasia Studio 5.0.1 (VER ANEXO 8)**

Esta aplicación es capaz de capturar a vídeo cualquier cosa que aparezca en la pantalla, editar el vídeo resultante, mejorarlo y, finalmente, compartirlo.

En cuanto a la grabación, Camtasia Studio permite capturar una ventana, una zona o la pantalla completa. Es capaz de capturar audio, recoger la imagen de

una cámara web e incluso se atreve con un PowerPoint. Lógicamente, las posibilidades son muchas.

Si hablamos de edición, Camtasia ofrece funciones para hacer zoom, añadir audio, crear efectos de transición e incluso limpiar el sonido de ruidos.

Por último, al exportar, encontrarás que puedes publicar tu creación en Flash, QuickTime, AVI, prepararlo para web, CD o incluso DVD.

- **Super Screen Recorder 3.0 (VER ANEXO 9)**

Captura toda la actividad que suceda en la pantalla de la computadora, para almacenarlo en un video de formato AVI._ Las opciones de captura de Súper Screen Recorder son similares a las que encontramos en un programa de captura en imagen estática. Se puede escoger entre capturar (grabar, en este caso) a pantalla completa o solamente en un área concreta definida por el usuario, incluir sonido en los vídeos, o elegir el formato y la calidad del vídeo final._ Realmente sencillo de utilizar, de configurar y con resultados de bastante calidad.

3.4 EVALUACION TECNICA Y ECONOMICA

En este apartado, se realiza una evaluación técnica a cada uno de los recursos requeridos para la elaboración del prototipo, los cuales deben de ser comparados con otros recursos similares. Entre alguno de los aspectos que se

toman en cuenta a la hora de evaluar cada uno de los recursos; tenemos los siguientes:

- ✓ Funcionalidad
- ✓ Manejabilidad
- ✓ Compatibilidad y
- ✓ Costos

El objetivo principal de este procedimiento, es seleccionar la aplicación que resulte más funcional, adaptable y conveniente en relación a las ventajas que ofrezca.

El procedimiento para realizar la evaluación es el siguiente:

1. listar las características específicas que se desean evaluar.
2. especificar cual es la función que se requiere de la aplicación a utilizar, en relación a cada una de las características.
3. establecer cual es el peso de dicha función en relación a las demás.
4. ponderación. Esta técnica permite determinar cuan funcional resulta el parámetro requerido. La leyenda de la ponderación es la siguiente:

“0” No cumple o no especifica.

“1” Cumple a medias pero es funcional.

“2” Cumple o excede.

5. La calificación resulta de multiplicar el peso por la ponderación determinada.
6. Luego se hace una suma de todas las calificaciones que obtuvo la aplicación evaluada. La cantidad resultante de esa suma, debe ser dividida entre 2, entonces esta será la nota que la aplicación obtuvo. Estos son todos los pasos del 1 al 6 que se deben realizar para evaluar cada una de las aplicaciones en comparación.
7. ahora que ya se tiene el resultado de evaluación de cada una de las aplicaciones que se han comparado se debe de seleccionar aquella que haya obtenido la mayor calificación, la cual debe de oscilar entre el 80% y el 100%. En caso de que la nota sea menor, se deben tomar las consideraciones necesarias, con el fin de realizar una buena elección.

CREACION DE ANIMACION FLASH

Nombre de la aplicación	Flash Saber 7	Setelco Aligator Flash Designer 7.06	Macromedia Flash MX 2004
--------------------------------	----------------------	---	---------------------------------

características a evaluar	función parametro requerido	Peso %	Ponderación	Calificación	Ponderación	Calificación	Ponderación	Calificación
creacion de animacion flash	animaciones interactivas avanzadas	30	0	0	2	60	2	60
operación de exportación	creacion de proyectores autoejecutables (.exe)	10	2	20	2	20	2	20
interfaz de usuario	herramientas simplificadas	25	2	50	2	50	2	50
incorporacion de video	soporte para el formato fslv	15	0	0	2	30	2	30
incorporación de efectos especiales	galerias de efectos especiales	15	2	30	2	30	2	30
utilñización de comandos scrips	personalizacion de comandos scrips	5	1	5	1	5	2	10
			Total	105		195		200
			Ponderacion final %	52.5		97.5		100
			Resultado obtenido	Reprobado		Aprobado		Aprobado

La aplicación seleccionada fue la que obtuvo el 100% de nota (Macromedia Flash MX 2004)

CREAR CD AUTO RUN

Nombre de la aplicación	AUTO RUN CREATOR 4.6	CD INTERFACE STUDIO 2.3	AUTO PLAY EXPRESS 4.2
--------------------------------	-----------------------------	------------------------------------	------------------------------

características a evaluar	función parámetro requerido	Peso %	Ponderación	Calificación	Ponderación	Calificación	Ponderación	Calificación
aparición grafica	permite total personalización de diseño	25	2	50	1	25	2	50
Plantillas	posee gran variedad de elementos prediseñados	15	2	30	1	15	1	15
facilidad de uso	herramientas simplificadas	20	1	20	1	20	2	40
efectos especiales	posee galería de efectos especiales	15	2	30	1	15	2	30

contenido multimedia	permite la incorporación de imagen video y sonido	25	2	50	1	25	1	25
			Total	180		100		160
			Ponderación final %	90		50		80
			Resultado obtenido	Aprobado		Reprobado		Aprobado

La Aplicación seleccionada fue la que obtuvo el 90% de nota (Autorun Creator 4.6)

Captura de Pantallas

Nombre de la aplicación	Screen Shet Captor	Camtasia Studio 5	Super Screen Recorder
-------------------------	--------------------	-------------------	-----------------------

características a evaluar	función parámetro requerido	Peso %	Ponderación	Calificación	Ponderación	Calificación	Ponderación	Calificación
Captura de video	Permite Capturar cualquier parte de la pantalla	30	2	60	2	60	2	60
Compresión de Video	Formato FLV	30	1	30	2	60	1	30
Permite la Captura de imágenes Estáticas	Extracción de cuadros específicos de un video	10	2	20	2	20	2	20
Creación de Menús para CDs/DVDs	Plantillas Prediseñadas	10	1	10	2	20	1	10
Permite la Edición de Video y Audio	Efectos Especiales	20	2	40	2	40	2	40

			Total	160		200	160
			Ponderación final %	80		100	80
			Resultado obtenido	Aprobado		Aprobado	Aprobado

La Aplicación seleccionada fue la que obtuvo el 100% de nota Camtasia Studio 5

3.5. TECNOLOGÍA Y RECURSOS SELECCIONADOS

Luego de haber realizado el análisis técnico y económico, se detalla cada uno de los recursos que se han seleccionado, justificando el porque de la elección de cada uno de ellos.

NOMBRE DE LA APLICACIÓN	JUSTIFICACIÓN
Camtasia Studio 5	Esta aplicación es la que posee mayor cantidad de herramientas, ya que no solo captura pantallas, si no que también permite crear efectos especiales.
CD Autorum creador 4.6	Es una herramienta la cual crea CDS como DVD autoejecutables además permite almacenar contenido multimedia (música, fotografías, video, etc.).
Macromedia Flash MX 2004	Es la mejor herramienta para crear animaciones flash, mezcla gráficos vectoriales, bitmaps, sonido, animaciones y una interactividad avanzada para crear espectaculares webs

3.6. PRESUPUESTO PROYECTADO

Este es el detalle de los recursos a utilizar para la elaboración del prototipo.

CANTIDAD	PRODUCTO	PRECIO
1	Camtasia Studio 5 (ver.Prueba)	\$239.00
1	CD Autorum creador 4.6	\$38.00
1	Macromedia Flash MX 2004	\$199.00
	Impresiones	\$90.00
	Fotocopias	\$40.00
	Video Cámara (compra/Alquiler)	\$ 0.00
	Gastos Varios : Pasajes, Alimentación	\$100.00
TOTAL		\$673.00

3.7 OFERTA TECNICA Y ECONOMICA

3.7.1 OFERTA TECNICA



S.S. 29 de marzo

de 2008

Señores

Facultad de Informática y Ciencias Aplicadas

Universidad Tecnológica de El Salvador

Presente.

Reciban cordiales saludos y éxitos en sus labores diarias, el objetivo de la presente es dar a conocer nuestra oferta técnica.

Daremos a conocer un nuevo servicio en la cual tenemos la creación de un cd interactivo, el cual consiste en una guía paso a paso de la instalación y configuración de redes inalámbricas, denotando una red Lan inalámbrica bajo la plataforma Windows, donde el estudiante podrá de forma sencilla y práctica interactuar con el cd obteniendo una mayor asimilación del contenido._ En sus aplicaciones multimedia audio y video, motivando así el proceso de enseñanza aprendizaje del estudiante.

Características del CD interactivo

- Interfaz interactiva con el Usuario
- Fácil entendimiento
- Fácil comprensión y asimilación
- Fácil acceso a la información
- Internet no necesaria
- Compatible en Ambiente Windows
- Windows 98, Windows 2000, Windows Xp (512 Mb de Ram recomendado), Windows Vista (1 GB de Ram minimo)
- Ambiente Linux (Distribuciones Red-Hat y Ubuntu (512 Mb de Ram recomendado))

Contenido del CD interactivo

- Construcción de una red inalámbrica
- Instalación y configuración de una red inalámbrica
- Instalación de Access Point
- Instalación de Routers Inalámbricos
- Métodos de seguridad
- Tecnologías Existentes

En lo anterior presentado estaremos abiertos a cualquier consulta

Atentamente

Luis Ernesto Cardona

Gerente de Mercadeo

3.7.2 OFERTA ECONOMICA



S.S. 29 de

marzo de 2008

Señores

Facultad de Informática y Ciencias Aplicadas

Universidad Tecnológica de El Salvador

Presente.

Reciban cordiales saludos y éxitos en sus labores diarias.

Para la creación del cd interactivo, fue necesaria la utilización de varios factores tanto técnicos como económicos los cuales aplicados todos, surgió dicho material con la finalidad de tener una herramienta útil para el proceso enseñanza aprendizaje del estudiante de la facultad de informática y ciencias aplicadas

Por lo tanto hacemos de su conocimiento el costo de cada manual interactivo a comercializar

Licencia de Uso

Cd interactivo	\$ 50.00
----------------	----------

Garantía	1 Año
----------	-------

La garantía cubre el mal funcionamiento del cd, excluyendo fallas de hardware, en espera que la información brindada sea de su agrado y satisfacción quedamos al pendiente de su respuesta.

Atentamente

Luis Ernesto Cardona

Gerente de Mercadeo

CAPITULO IV

4.1 ARTICULO DE SOCIALIZACION

En nuestro de venir diario y búsqueda de conocimientos teórico práctico que nos introduce al mundo de las redes inalámbricas en consideración a estos aspectos.

Es de mucha utilidad saber como se instalan y configuran dichas redes lo cual toma mayor relevancia, en el momento que debemos enfrentar el proceso de enseñanza aprendizaje encontraremos que al profundizar en el tema de las redes inalámbricas no se contaba con un material didáctico idóneo y de fácil comprensión para el estudiante en lo relacionado a la instalación y configuración de las mismas.

Así que para ir entrando en materia tendremos que apoyarnos en un CD interactivo que tuviera un estudio sistemático de asimilación y comprensión rápida aplicada tanto a docente como estudiante, relacionado a la instalación y configuración de redes inalámbricas dando a su vez una muestra de los mecanismos de seguridad que podría ser útil a la red.

Con el desarrollo de este instrumento estaríamos aportando un recurso valioso a los estudiantes de la Escuela de Informática, generando así un gran deseo por aprender por la manera en que se presenta la información de dicho CD.

Siendo a su vez sencilla, de forma tal que su acceso es dinámico el manejo de la información, la cual a sido ya recopilada y seleccionada, para que el estudiante este en la capacidad de implementar una red inalámbrica.

Dejando así una gran gama de conocimientos a todas las personas que utilizan el CD llevándolos de la mano con dicho manual interactivo

4.2 Presentación del Prototipo (PowerPoint)



Desarrollo de un manual interactivo como apoyo a la enseñanza aprendizaje en instalación y configuración de redes inalámbricas para los estudiantes de la escuela de informática

Presentado por
Silvia Haydee Granillo
Karla María Martínez
Luis Ernesto Cardona Guadrón

- La creación del proyecto inicia con un estudio previamente realizado sobre la poca documentación existente en la instalación y configuración de redes inalámbricas enfocandolo a la plataforma Windows



Estamos en la necesidad de proporcionar una herramienta de apoyo que viene dada, por un material interactivo que proporcione la suficiente información que facilite la enseñanza aprendizaje al estudiante

- Temas relacionados a las redes inalámbricas
- Instalación y configuración de una red inalámbrica
- Seguridad en la red Inalámbrica
- Nuevas Tecnologías



Para la creación del CD interactivo se ha investigado que se necesita para crear un manual interactivo tomando aspectos relevantes como contenido multimedia , digitalización de medios, aplicación para la edición de video audio digital y texto

Tecnología y Recursos Seleccionados

- Camtasia Studio 5
- CD Autorum Creator 4.6
- Macromedia Flash MX 2004

Instalar y configurar una red Inalámbrica en la plataforma Windows teniendo como objetivo interconectar nodos inalámbricos en una oficina



- Con la creación del Manual Interactivo se ayudo a solventar la poca información que se tenia sobre la instalación y configuración de una red Inalámbrica



Los conocimientos adquiridos en el desarrollo del proyecto fue enriquecernos de conocimientos y nuevas experiencias sobre el tema



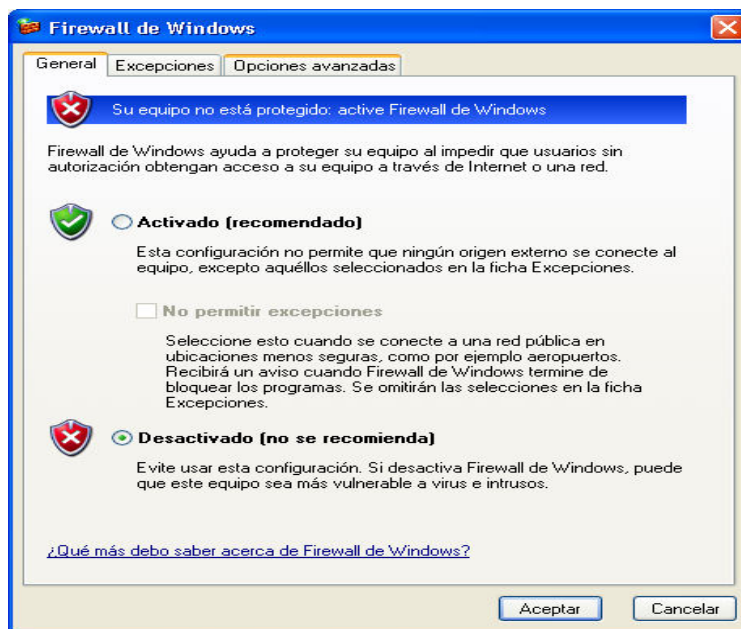
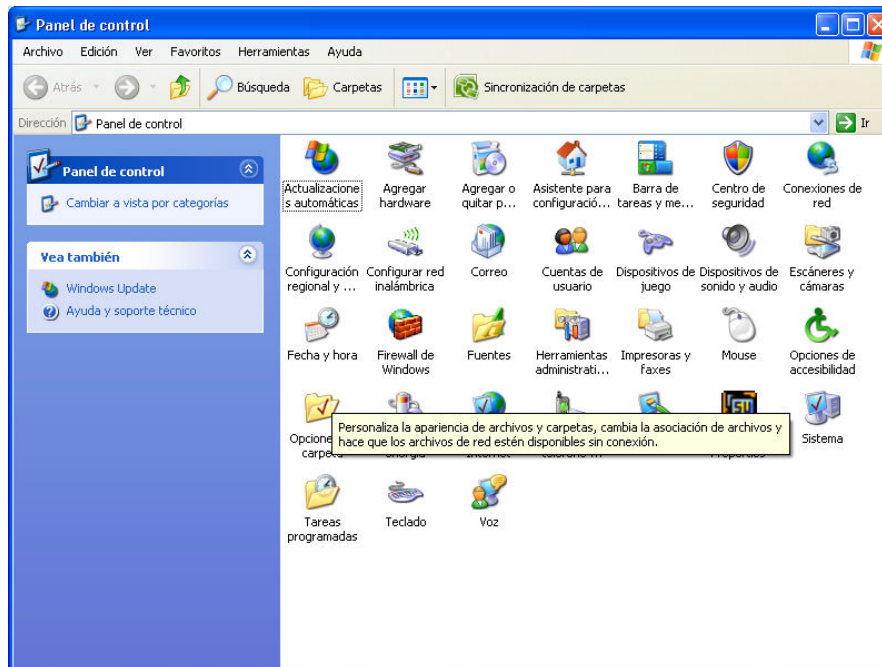
POR LO TANTO POR MEDIO DEL CD INTERACTIVO AYUDAMOS A SOLVENTAR OTRAS NECESIDADES EDUCATIVAS YA QUE ES LA FORMA MAS IDONEA E INTERACTIVA DE APRENDER



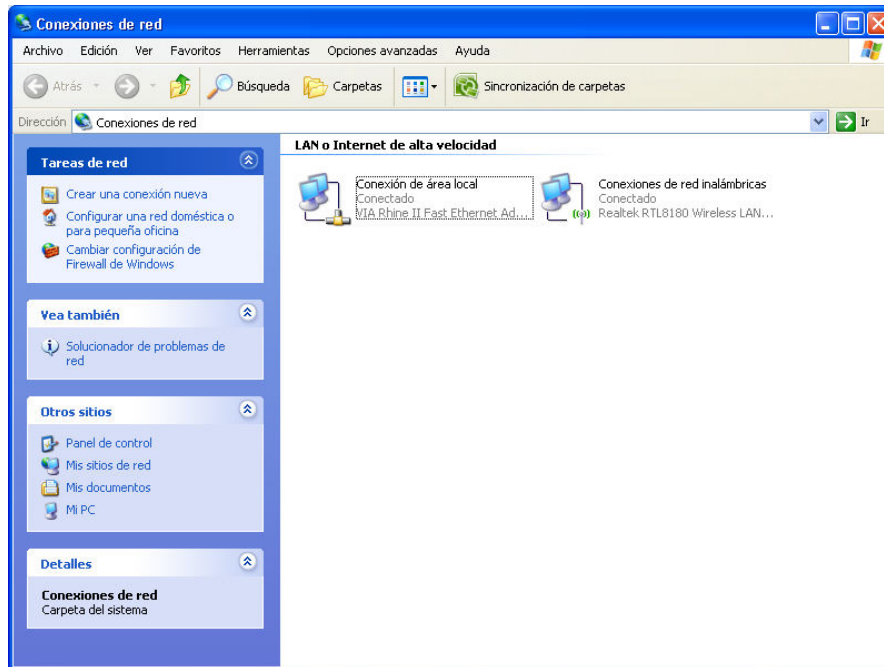
4.3 Evidencias del proyecto

Pasos para configurar una red inalámbrica

Desactivar el Firewall



Detección de red inalámbrica



Verificando estado de conexión



Verificando IP Inalámbrica

```
C:\> CMD

Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ADMIN>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local :

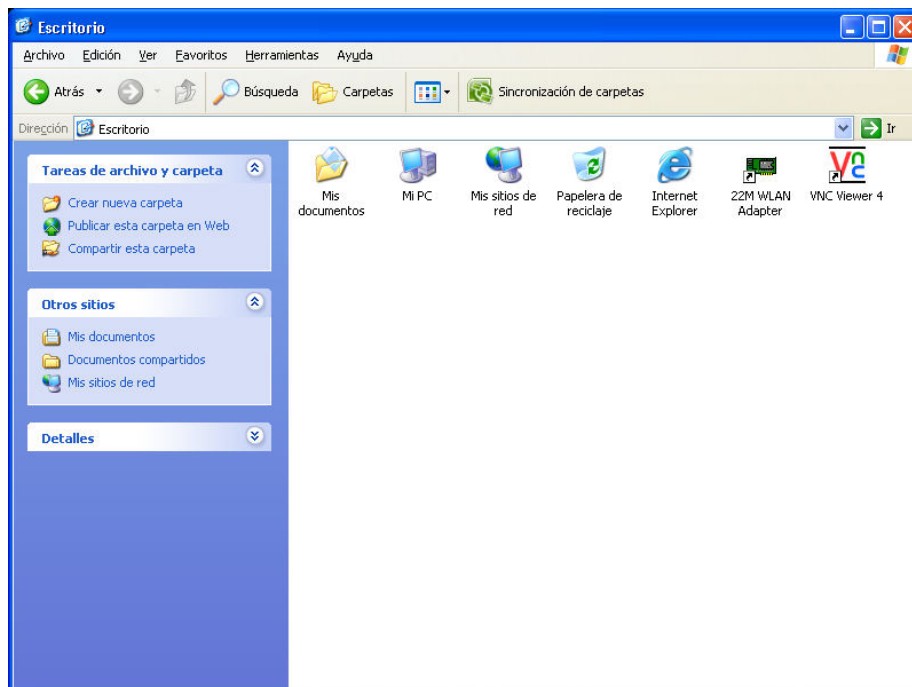
    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 10.10.7.25
    Máscara de subred . . . . . : 255.0.0.0
    Puerta de enlace predeterminada :

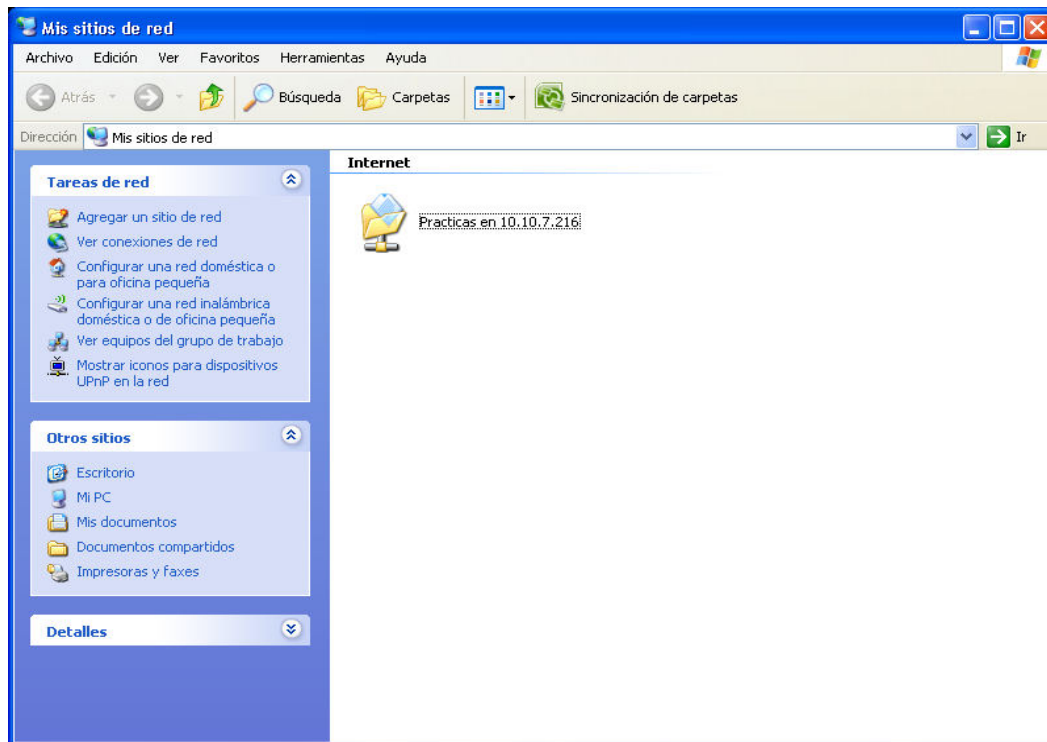
Adaptador Ethernet Conexiones de red inalámbricas :

    Sufijo de conexión específica DNS : adminwireless.utec.edu.sv
    Dirección IP. . . . . : 198.197.196.159
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada : 198.197.196.1

C:\Documents and Settings\ADMIN>_
```

Para configurar el Access point tenemos que escribir en el internet explorer la dirección IP asignada al Access Point inalámbrico por default





```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Redes>192.168.1.2
"192.168.1.2" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

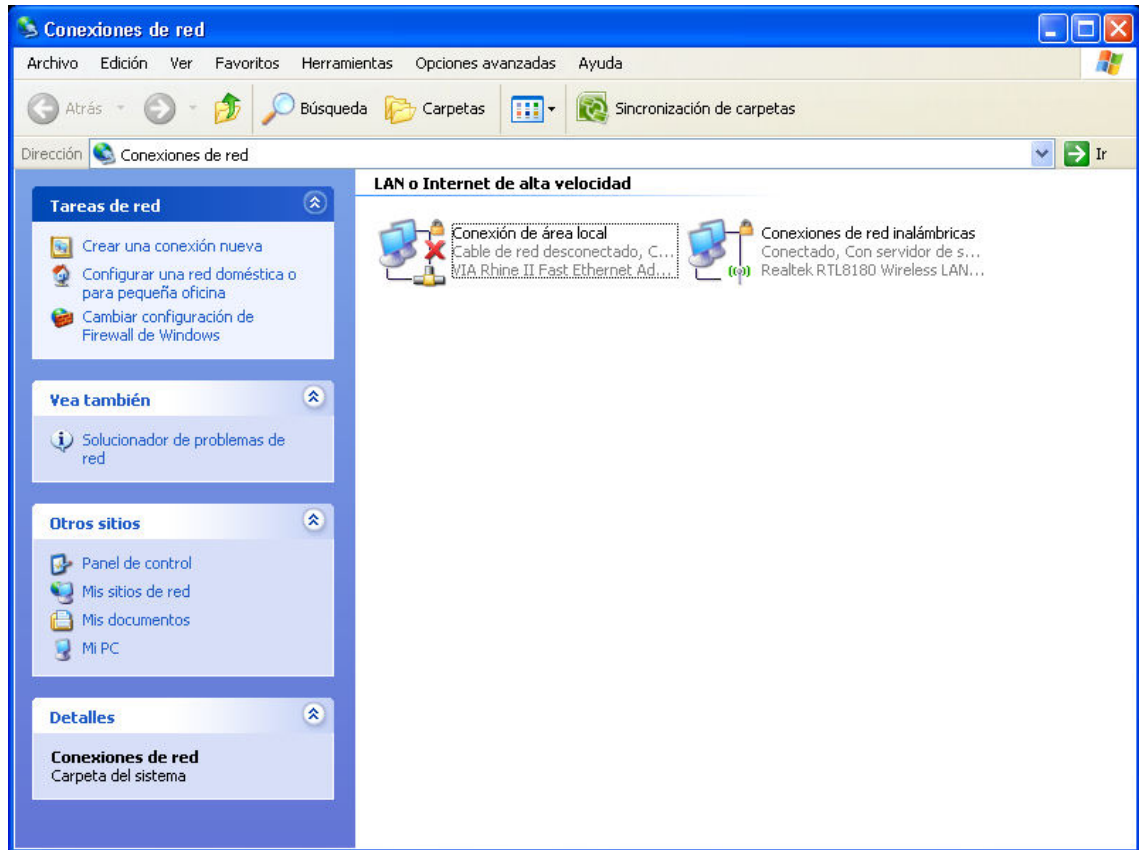
C:\Documents and Settings\Redes>ping 192.168.1.2

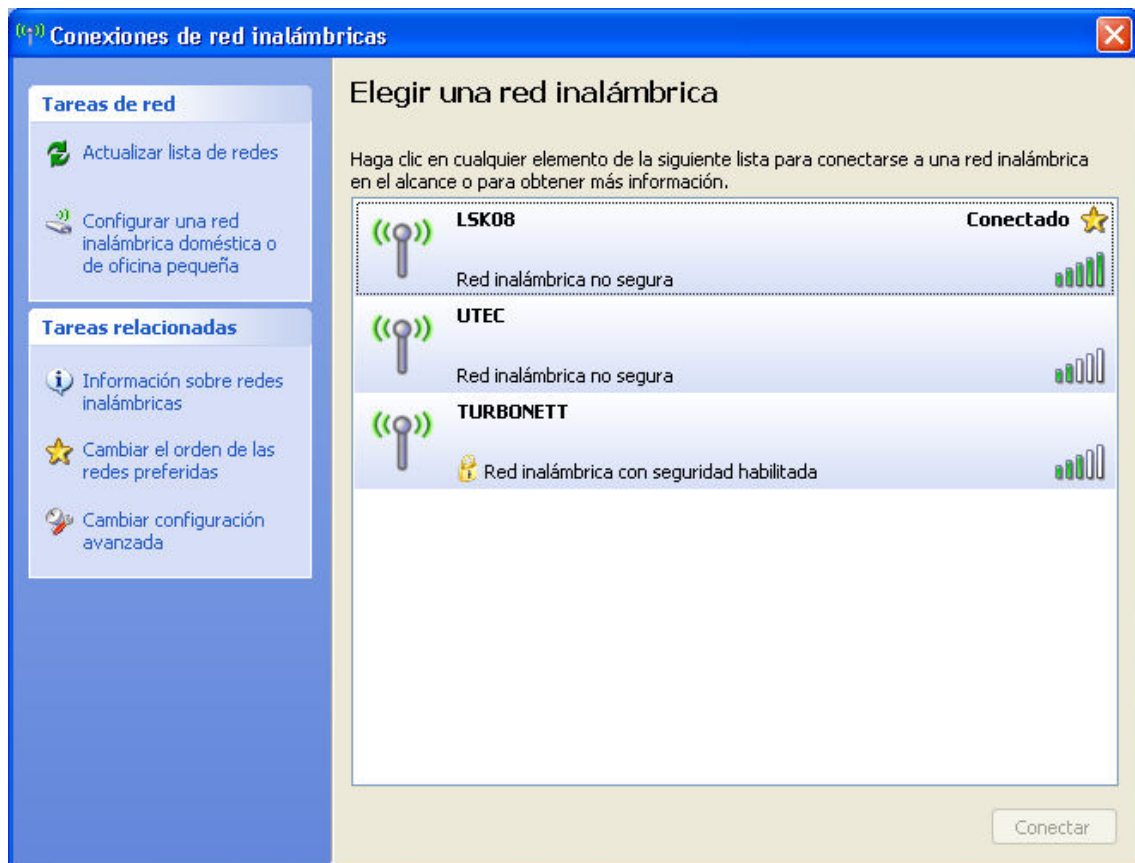
Haciendo ping a 192.168.1.2 con 32 bytes de datos:

Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Redes>
```





```

C:\WINDOWS\system32\cmd.exe
Adaptador Ethernet Conexión de área local :
    Sufijo de conexión específica DNS :
    Descripción . . . . . : VIA Rhine II Fast Ethernet Adapter
    Dirección física . . . . . : 00-0D-87-74-54-FE
    DHCP habilitado . . . . . : No
    Dirección IP . . . . . : 10.10.7.25
    Máscara de subred . . . . . : 255.0.0.0
    Puerta de enlace predeterminada :
    Servidores DNS . . . . . : 10.10.7.216

Adaptador Ethernet Conexiones de red inalámbricas :
    Sufijo de conexión específica DNS :
    Descripción . . . . . : Realtek RTL8180 Wireless LAN (Mini-)
PCI NIC
    Dirección física . . . . . : 00-40-F4-94-1A-3B
    DHCP habilitado . . . . . : No
    Autoconfiguración habilitada . . : Sí
    Dirección IP . . . . . : 192.168.1.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada :
    Servidor DHCP . . . . . : 192.168.1.1
    Concesión obtenida . . . . . : viernes, 16 de mayo de 2008 4:44:40
    Concesión expira . . . . . : sábado, 17 de mayo de 2008 4:44:40

C:\Documents and Settings\Redes>

```

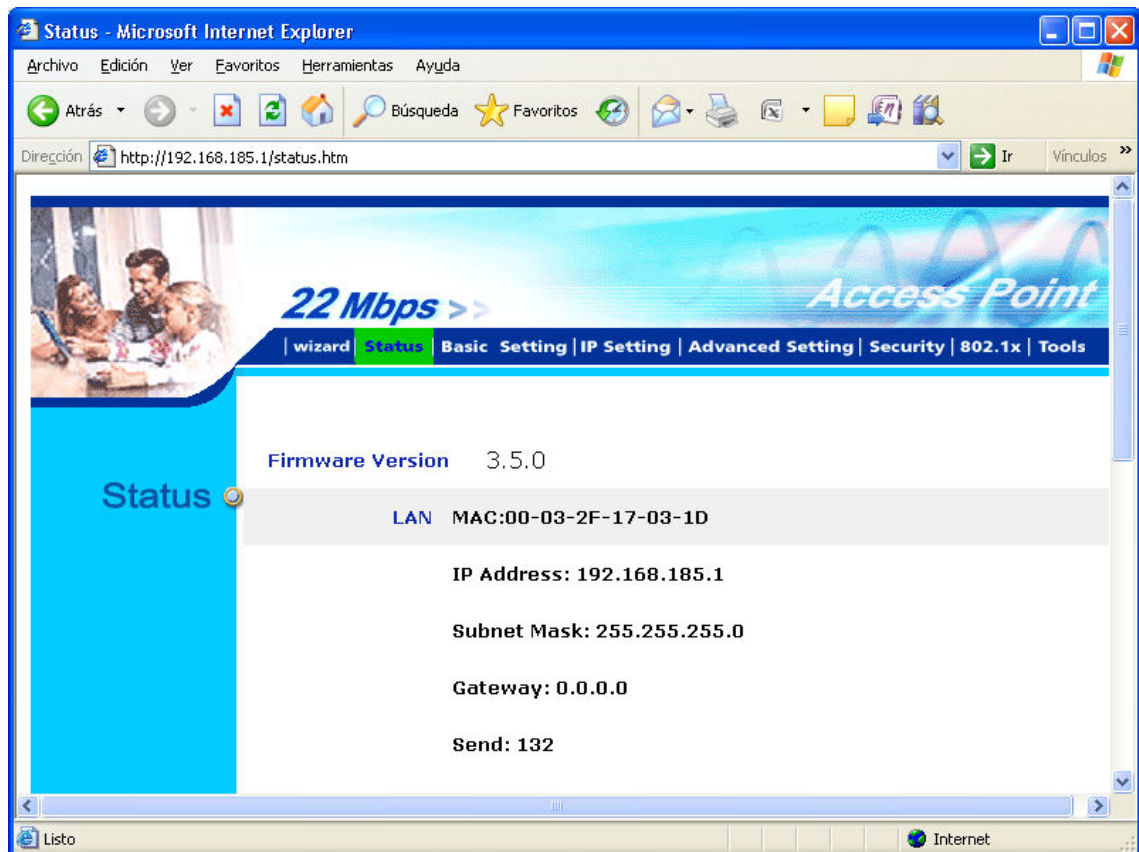
```

C:\WINDOWS\system32\cmd.exe
Configuración IP de Windows
    Nombre del host . . . . . : lab7-25
    Sufijo DNS principal . . . . . :
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado . . . . . : No
    Proxy WINS habilitado . . . . . : No

Adaptador Ethernet Conexiones de red inalámbricas :
    Sufijo de conexión específica DNS :
    Descripción . . . . . : Realtek RTL8180 Wireless LAN (Mini-)
PCI NIC
    Dirección física . . . . . : 00-40-F4-94-1A-3B
    DHCP habilitado . . . . . : No
    Autoconfiguración habilitada . . : Sí
    Dirección IP . . . . . : 192.168.1.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada :
    Servidor DHCP . . . . . : 192.168.1.1
    Concesión obtenida . . . . . : viernes, 16 de mayo de 2008 5:28:10
    Concesión expira . . . . . : sábado, 17 de mayo de 2008 5:28:10

C:\Documents and Settings\Redes>

```



En la figura anterior y siguiente se muestra ya el entorno de configuración del Access Point los pasos para configurarlo

Firmware Version 3.5.0

LAN **MAC:00-03-2F-17-03-1D**

IP Address: 192.168.1.1

Subset Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 1282

Receive: 1167

Wireless **MAC:00-03-2F-10-67-63**

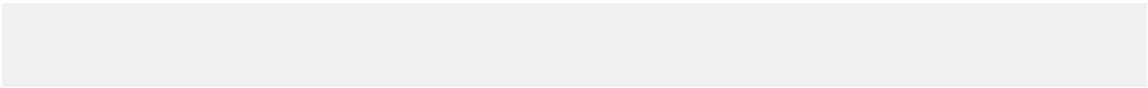
SSID: LSK08

Encryption Function : Disable

Channel: 6

Send: 271

Receive: 59



Connection Time	Wireless Station
Nov/07/2007 19:07:53	00:11:F5:15:7B:76
Nov/07/2007 19:27:43	00:18:DE:B4:53:11

Basic settings

AP Name

AP17031D

SSID

LSK08

Channel

6

(Domain: USA)

WEP Key ☒ **Disable** ☐ **64bits** ☐ **128bits** ☐ **256bits**

Mode ▼

☒ **1.**

☐ **2.**

☐ **3.**

☐ **4.**

Ip settings

LAN IP ☐ **Obtain IP Automatically**

☒ **Fixed IP**

Address

Subnet Mask

Gateway

DHCP Server ☒ **On**

☐ **Off**

IP Range From
to

DNS Server

Advanced settings

AP Mode ☒ **AP**

☐ **AP Client** **Remote AP BSS ID**

☐ **Wireless Bridge** **Remote Bridge MAC**

☐ **Multiple Bridge**

Beacon Interval (msec, range:1~1000, default:100)

DTIM Interval (range: 1~255, default:3)

Authentication Type ☐ **Open System** ☐ **Shared Key** ☒ **Both**

Preamble ☒ **Short Preamble** ☐ **Long Preamble**

Basic Rate ☐ **1-2(Mbps)** ☒ **1-2-5.5-11(Mbps)** ☐ **1-2-5.5-11-22(Mbps)**

Supported Rate ☐ **1-2(Mbps)** ☐ **1-2-5.5-11(Mbps)** ☒ **1-2-5.5-11-**

22(Mbps)

Antenna Selection ☐ Left Antenna ☐ Right Antenna ☒ Diversity Antenna

SSID broadcast ☒ Enable ☐ Disable

4X Mode ☒ Enable ☐ Disable

Apply

Cancel

Security

Password

Administrator id:

AP Password New:

Confirm:

Apply

Cancel

MAC Filter

☐ Enabled ☒ Disabled

☐ Only **deny** PCs with MAC listed below to access device

☒ Only **allow** PCs with MAC listed below to access device

1~10



MAC 1

	-		-		-		-		-	
----------------------	---	----------------------	---	----------------------	---	----------------------	---	----------------------	---	----------------------

MAC 2 - - - - -

MAC 3 - - - - -

MAC 4 - - - - -

MAC 5 - - - - -

MAC 6 - - - - -

MAC 7 - - - - -

MAC 8 - - - - -

MAC 9 - - - - -

MAC 10 - - - - -

802.1x	☒ Enabled
	☐ Disabled
Encryption Key	Length ☒ 64 bits ☐ 128 bits ☐ 256bits
	Lifetime 30 Minutes ▼
RADIUS Server 1	IP 0 0 0 0

Port

Shared Secret

**RADIUS Server
2 (optional)**

IP . . .

Port

Shared Secret

tools

Backup Settings

Restore Settings

**Restore to default
settings**

Firmware Upgrade

Backup Settings

Restore Settings

Restore

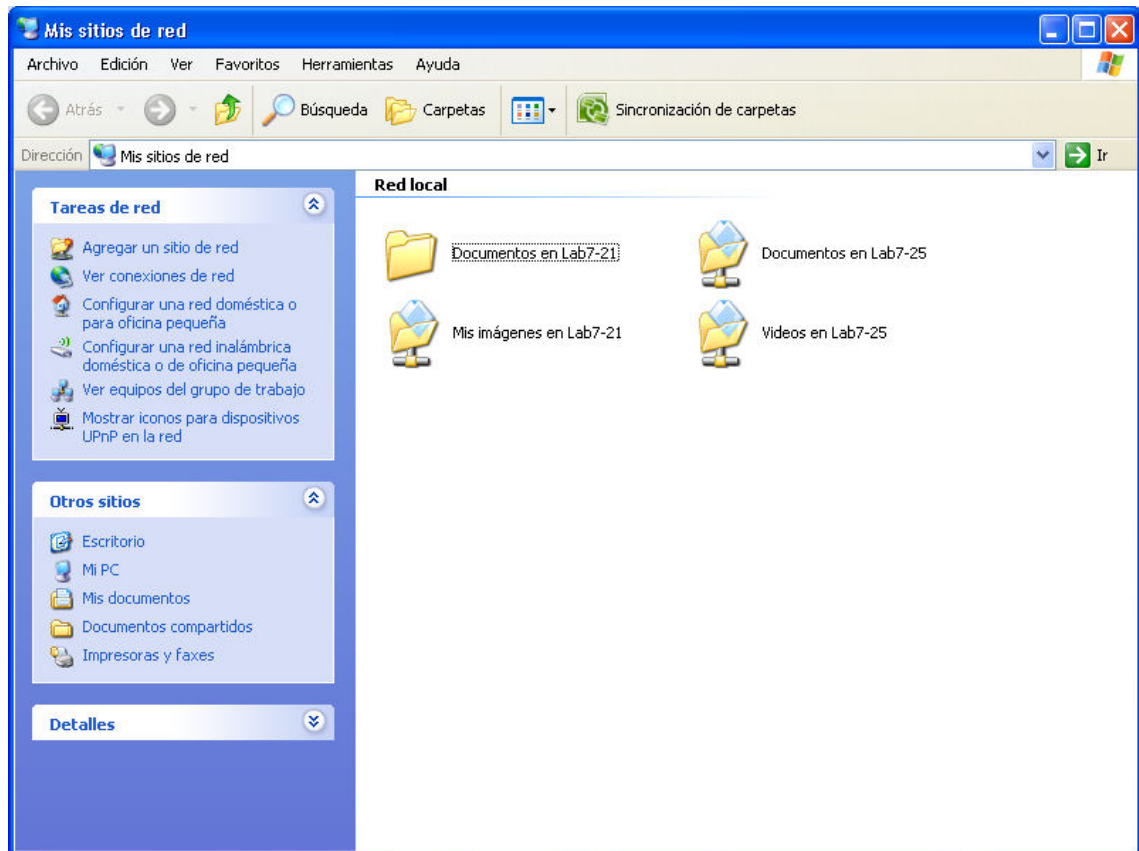
Restore to default settings

Default

Firmware Upgrade

Upgrade

Aquí se muestra la red compartida



FOTOS DE LOS INTEGRANTES DEL GRUPO EN LA ELABORACION DEL PROTOTIPO



Aquí se ensambla el access point

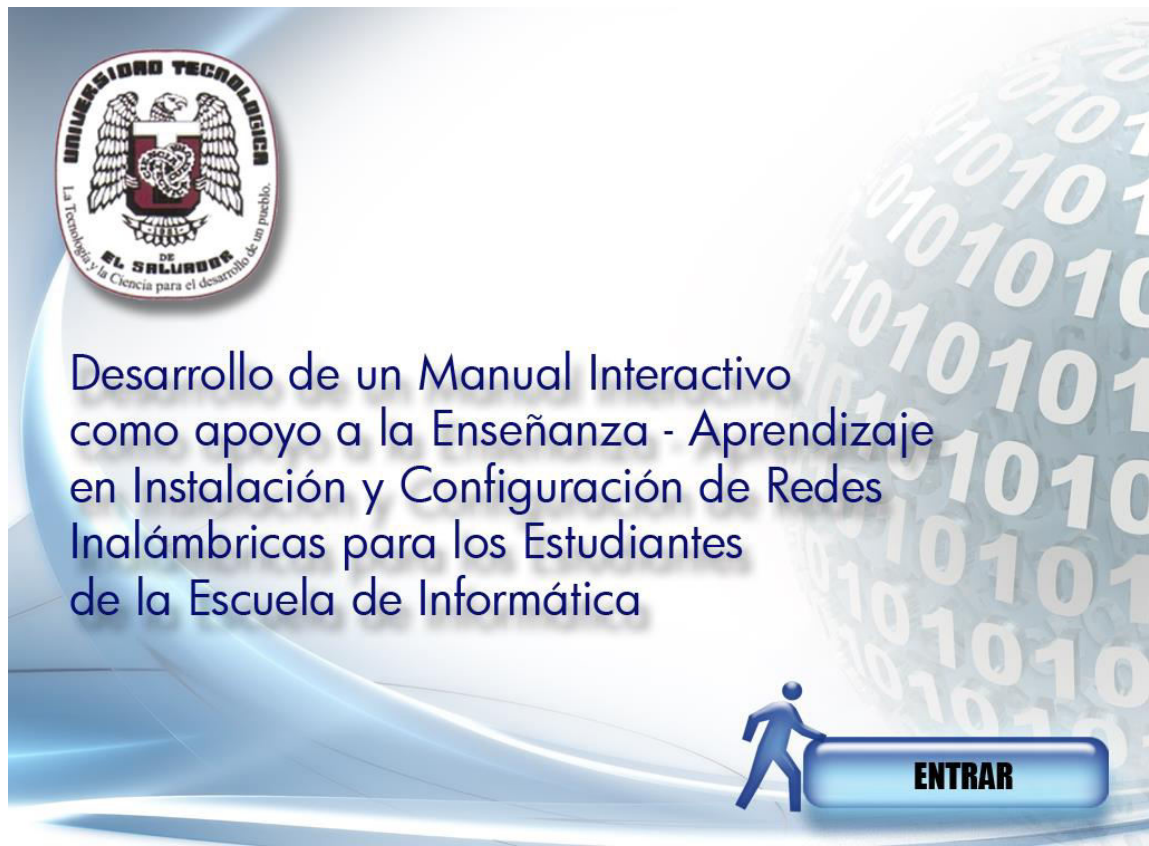


Aquí se conecta el cable que va del Access Point a la maquina



AQUÍ SE MUESTRA AL EQUIPO DE TRABAJO CONFIGURANDO LA RED INALAMBRICA

PANTALLA DE INICIO DEL CD INTERACTIVO



CONCLUSION

En la tesis desarrollada se hace un aporte a las necesidades de conocimiento de las nuevas tecnologías que se utilizan hoy en día en amplio espectro de redes inalámbricas, que es el medio en el que el mundo gira siendo así se crea la necesidad de dichas redes por su movilidad, flexibilidad, fácil instalación y su costo bajo.

Se desarrollaron de tal forma que los estudiantes pueden aprender o reafirmar sus conocimientos en el área inalámbrica, donde se da un material de apoyo que facilita el proceso enseñanza aprendizaje y puesta en marcha de la instalación y configuración de redes inalámbricas.

El estudiante que se guíe por el material interactivo que se ha proporcionado estará en la capacidad de instalar una red inalámbrica local, el estudiante a su vez puede profundizar más en los temas expuestos con solo entrar ya sea a una página web recomendada o archivos PDF contenidos en el cd interactivo.

Todo esto listo para que el conocimiento adquirido sea transmitido a nuevas generaciones que sigan ahondando más y más, se siembra la semilla del conocimiento la cual germinará y hará de las generaciones venideras mejores profesionales, eficientes.

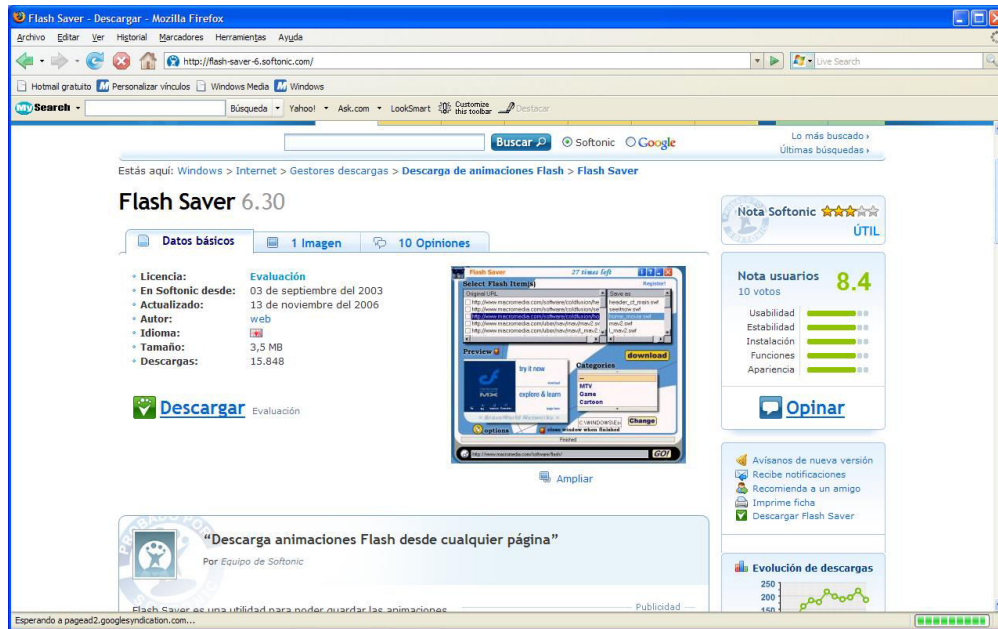
RECOMENDACIONES

- Se recomienda a la Universidad Tecnológica compre más equipo de redes inalámbricas, que vaya a la vanguardia de la tecnología tales como Access Point, Tarjetas de red Inalámbricas, antenas inalámbricas y usb inalámbricas.
- Desarrollar seminarios teóricos y prácticos con regularidad en temas específicos que sean de interés para las materias que estén íntimamente relacionadas con las redes inalámbricas.
- Aperturar nuevos laboratorios especializados, que cuenten con el equipo inalámbrico actualizado en redes inalámbricas, para poder desarrollar esta tecnología

ANEXOS

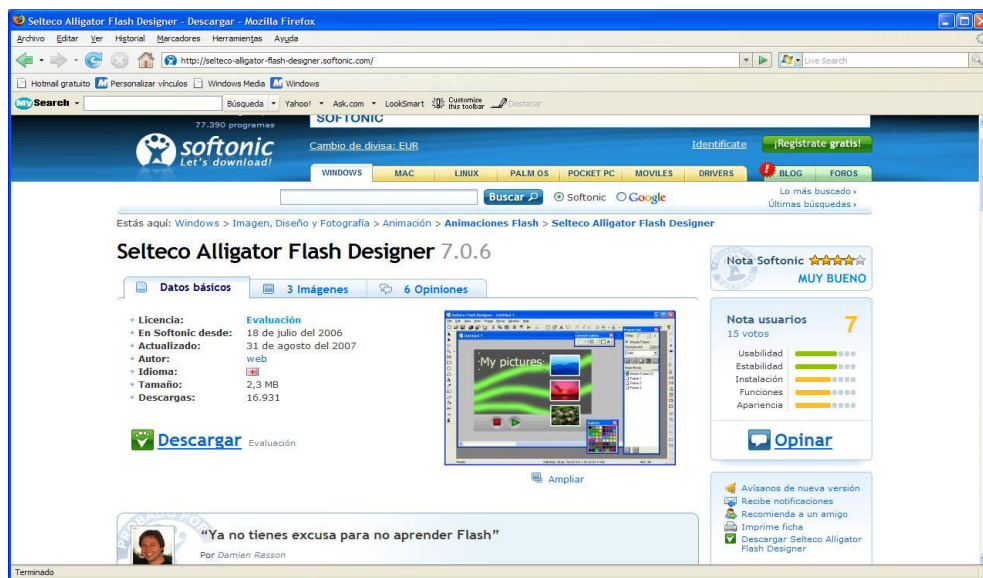
ANEXO 1

FLASH SABER 6.30



ANEXO 2

SELTECO ALLIGATOR DESIGNER 7.0.6



Selteco Alligator Flash Designer - Descargar - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://selteco-alligator-flash-designer.softonic.com/

Hotmail gratuito Personalizar vínculos Windows Media Windows

MySearch Búsqueda Yahoo! Ask.com LookSmart Customize this toolbar Destacar



"Ya no tienes excusa para no aprender Flash"

Por Damien Rasson

Si te quedas alucinado, con los ojos abiertos como platos siempre que visitas un blog o una página web creada con una buena carga de Flash, atrévete a usarla y deja de temer a esta tecnología, en realidad es mucho más fácil de lo que parece, ya lo verás.

Sobre todo si tienes a tu alcance una utilidad como este "alligator" de Selteco: Flash Designer, una herramienta para todos, con muchas posibilidades y encima, con un entorno intuitivo desde el que podrás crear toda suerte de elementos en Flash para tu web.

Desde menús o botones pasando por presentaciones de imágenes e introducciones en Flash, hasta formularios interactivos y animaciones con fotos y videos, cliparts y GIF animados, etc. No hay límite. Podrás usar formas, y convertirlas en zonas de enlace, integrar videos y sonidos de fondo, incluso sacar provecho de la potencia brindada por ActionScript 2.0 para crear eventos y acciones Flash. Luego exportas tu creación a SWF y a disfrutar de ella.

- Limitaciones de la versión de prueba:**
Funcional durante un periodo de 30 días
- Para utilizar Selteco Alligator Flash Designer necesitas:**
 - Sistema operativo: Win95/98/98SE/Me/2000/NT/XP

[Descargar Selteco Alligator Flash Designer](#)

Softonic informa que Selteco Alligator Flash Designer (54015) debe ser utilizado según la normativa de propiedad intelectual

Transfiriendo datos desde www.freelotto.com

Recomienda a un amigo
Imprime ficha
☒ Descargar Selteco Alligator Flash Designer

Evolución de descargas



Últimas 12 semanas

Publicidad

¡Felicidades!

Eres el visitante
2,982,283,600th

Flash Saver - Descargar - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://flash-saver-6.softonic.com/

Hotmail gratuito Personalizar vínculos Windows Media Windows

MySearch Búsqueda Yahoo! Ask.com LookSmart Customize this toolbar Destacar



"Descarga animaciones Flash desde cualquier página"

Por Equipo de Softonic

Flash Saver es una utilidad para poder guardar las animaciones Flash que encuentres en cualquier página Web.

Para ello basta por ejemplo con que realices una búsqueda con Flash Saver en la página en la que te encuentres y, tras analizarla entera, Flash Saver te mostrará el archivo en su visualizador interno, la URL del mismo y la posibilidad de descargarlo.

Permite guardar los archivos Flash en diferentes categorías y aprovecha que ya has descargado los archivos simplemente al verlos y cuando decidas guardarlo lo hará directamente desde caché (a menos que especifiques lo contrario).

Funciona con los navegadores: Internet Explorer, Netscape, Firefox, Opera...

- Para utilizar Flash Saver necesitas:**
 - Sistema operativo: Win95/98/98SE/Me/2000/NT/XP

[Descargar Flash Saver](#)

Softonic informa que Flash Saver (21185) debe ser utilizado según la normativa de propiedad intelectual y el vigente Código Penal. Softonic no permite la inserción de ningún crack, serial o keygen y se exime de cualquier responsabilidad derivada del uso inadecuado de Flash Saver.

Compartir Flash Saver en:  ¿Qué es esto?

Evolución de descargas



Últimas 12 semanas

Publicidad

IMVITE

TV en Vivo Videos Shows de TV A-Z

**6500 canales En Vivo de 110 países
100% Gratis!**

**TV Shows A-Z
Dibujos Animados A-Z
Musica A-Z**

imvite.com/es [Ads by Google](#)

Publicidad

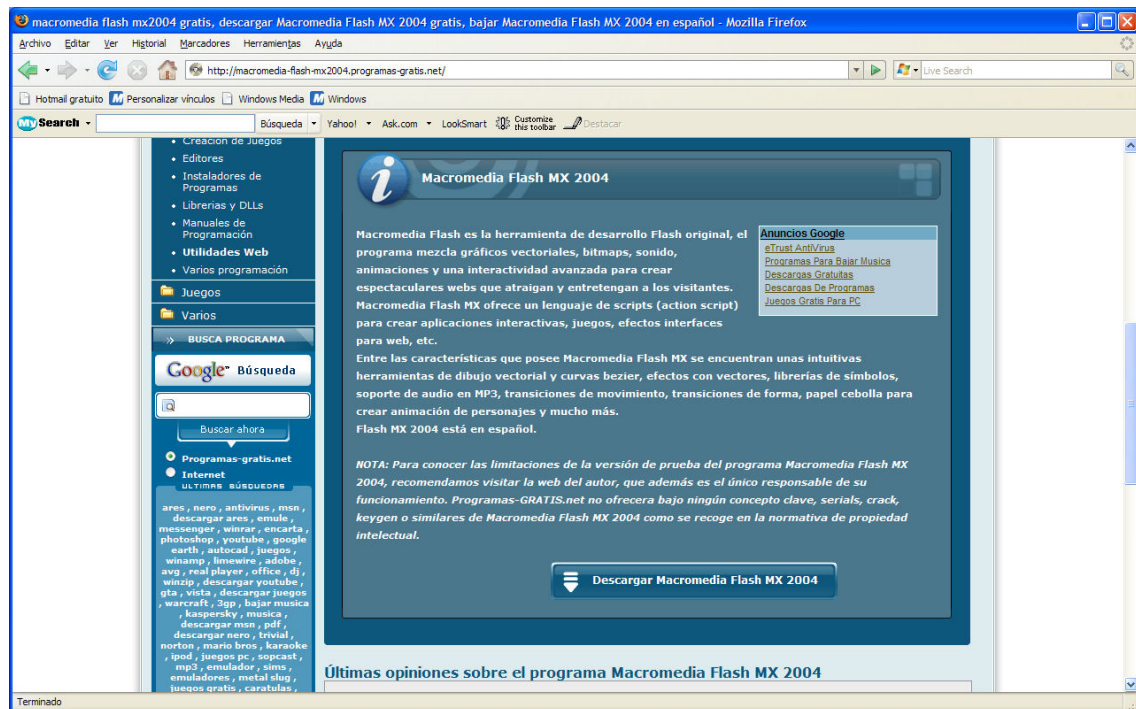
ASÍ CUALQUIERA
¡QUE FÁCIL!

[Descargar](#)

¡UAUHHH ES UN
DELUXE

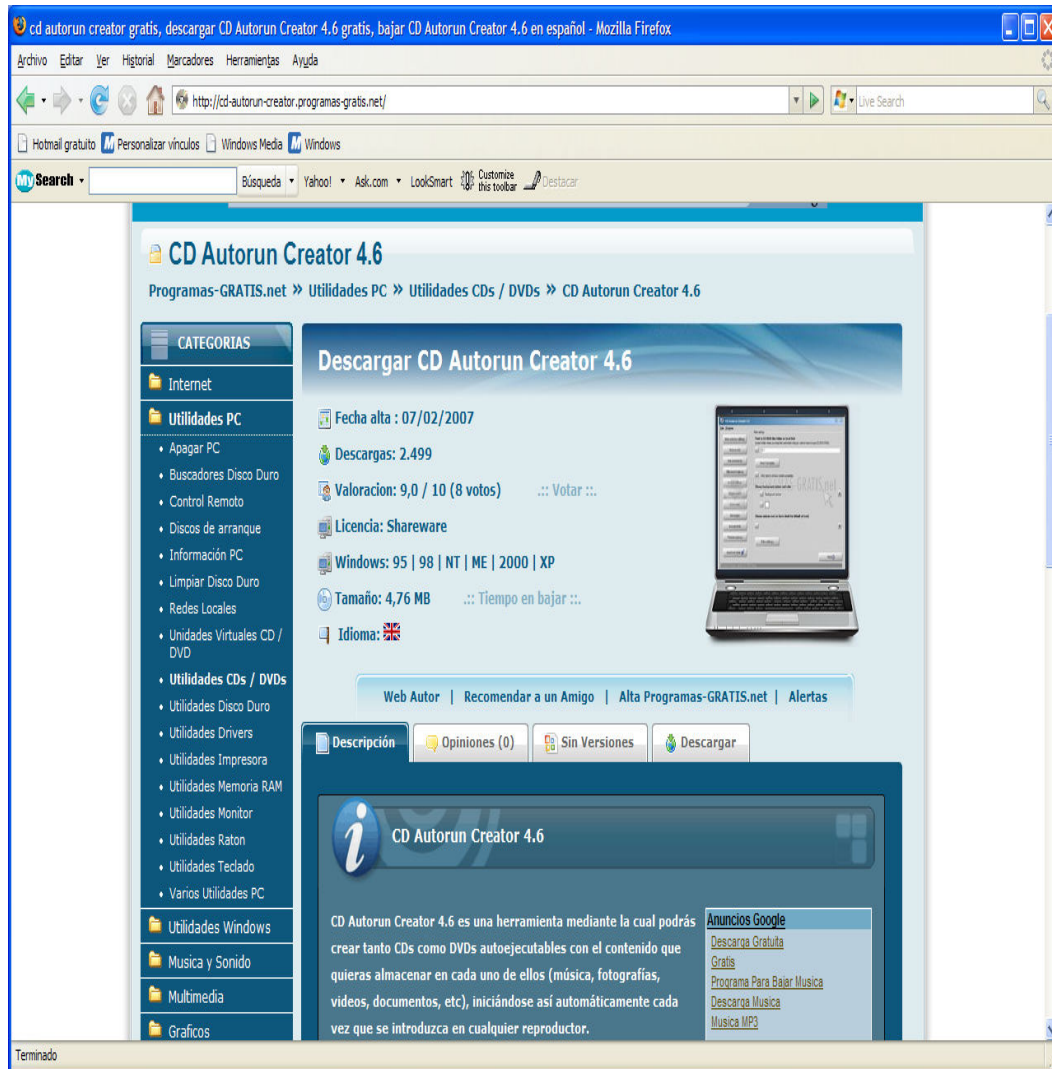
ANEXO 3

MACROMEDIA FLASH MX 2004



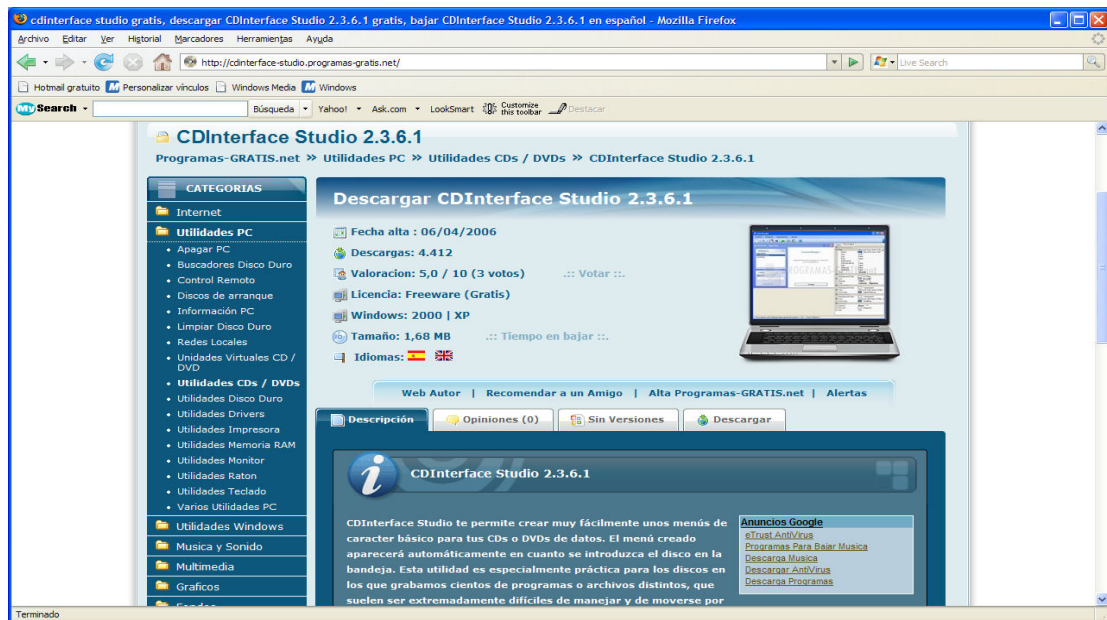
ANEXO 4

CD Autorun creador 4.6



ANEXO 5

CDINTERFACE STUDIO 2.3.6.1



ANEXO 6

Autoplay Express 4.2



ANEXO 7

SCREENSHOT CAPTOR 2.36.03



ANEXO 8

CAMTASIA STUDIO 5.0.1





SUPER SCREEN RECORDER 3.0



Matriz de Congruencia

Tema

Desarrollo de un manual interactivo como apoyo a la enseñanza aprendizaje en instalación y configuración de redes inalámbricas para los estudiantes de la escuela de informática

ENUNCIADO DEL PROBLEMA

¿Cómo se puede apoyar al estudiante de Técnico en Ingeniería de Redes Computacionales a reforzar los conocimientos sobre la instalación y configuración de redes inalámbricas?

OBJETIVO GENERAL

Facilitar el aprendizaje de los alumnos de la carrera Técnico en Ingeniería de Redes Computacionales, en lo relacionado a la instalación y configuración de Redes Inalámbricas.

OBJETIVO ESPECIFICO 1

1 Investigar las diferentes herramientas aplicables para el diseño y desarrollo de materiales

OBJETIVO ESPECIFICO 2

Crear un manual interactivo de estudio sistemático el cual contenga paso a paso procedimientos de fácil comprensión y aplicación en lo relacionado a la instalación y

OBJETIVO ESPECIFICO 3

Proporcionar los mecanismos básicos de seguridad necesarios para implementar una red

interactivos (CD'S interactivos)	configuración de redes inalámbricas	inalámbrica
Alcance 1 Crear un CD interactivo de estudio sistemático que brinde un ambiente amigable y de fácil comprensión y que sea una herramienta útil para el docente y estudiante.	Alcance 2 La información teórica estará estrechamente relacionado con el material práctico	Alcance Proporcionar material que muestre paso a paso todo el proceso de instalación y configuración de redes inalámbricas.
MARCO TEORICO En el proyecto se ha evaluado la necesidad de crear un instrumento útil y necesario para la comunidad estudiantil de la Escuela de Informática, dando a su vez grandes pasos para el mejoramiento de la enseñanza aprendizaje como se ve reflejado pues de la manera en la cual se han escogido los temas, relacionados íntimamente con las redes inalámbricas, dejando así un legajo de conocimientos a ;as generaciones venideras, se ha pensado que dicho material interactivo sea una herramienta para poder aprender y reforzar los conocimientos de cómo instalar y configurar una red inalámbrica.		
PRODUCTO 1 Cd interactivo	PRODUCTO 2 Recopilación de información Idónea para cd	PRODUCTO 3 Instalación y configuración de una red inalámbrica

PROYECTO TEMATICO

PRIMERA FASE

Tecnologías a utilizar, en la elaboración del cd interactivo.

Esta fase consiste en investigar detalladamente la documentación que se necesita para poder realizar, un manual interactivo, tomando aspectos indispensables, como contenido multimedia, digitalización de medios, aplicaciones para la edición de video digital, de audio digital y texto, donde el usuario pueda interactuar con el material interactivo que se presenta en el cd.

Su contenido debe estar acorde a las necesidades del estudiante presentando documentación confiable, que sirva para desarrollar instalaciones y configuraciones inalámbricas de fácil acceso.

Actividades

1. Recopilar información sobre redes inalámbricas para la elaboración del cd interactivo
2. Seleccionar información adecuada y necesaria de cómo instalar y configurar los dispositivos que componen una red inalámbrica
3. Investigar que requerimientos necesitamos saber para elaborar el cd interactivo

SEGUNDA FASE.

Generalidades de cómo instalar y configurar una red inalámbrica.

La información recopilada necesaria para enseñar a instalar y configurar una red una red inalámbrica, así también como usar los diferentes dispositivos que se utilizan en la red, como lo son tarjetas inalámbricas, access point y routers inalámbricos, teniendo en cuenta la seguridad que debe de ir a la par de la configuración evitando el acceso no autorizado a personas ajenas a nuestra red inalámbrica.

Actividades

1. Investigar la información necesaria para interconectar Nodos Inalámbricos con Acces Point y muchos otros dispositivos

2. Desarrollar paso a paso la instalación y configuración de una red inalámbrica
3. Desarrollar mecanismos de seguridad en redes inalámbricas

TERCERA FASE

Conocimientos adquiridos en el trayecto de la elaboración del producto.

Con la finalización del proyecto, en el cual se proporciona la información tanto teórica como práctica para crear el cd interactivo donde se encontrara paso a paso como instalar y configurar una red inalámbrica.

De tal forma se dará por terminado el cd interactivo, siendo este una base para los estudiantes de la carrera Técnico .en Ingeniería de Redes Computacionales de la Universidad Tecnológica.

Las actividades a realizar son las siguientes:

- Desarrollo del cd interactivo.
- Instalación y configuración de redes inalámbricas.
- Captura de pantallas.
- Edición de video.
- Edición de contenido y.
- Finalización del producto.

PRESUPUESTO PROYECTADO

\$673.00

OFERTA ECONOMICA

\$50.00

BIBLIOGRAFIA

APPLE, ¿Cómo acceder a una red inalámbrica encriptada? [En línea], [consulta: Abril 2008].

Disponible en: <http://docs.info-apple.com/article.html?artnum=106424-es>

ZONAGRATUITA, seguridad en redes inalámbricas II [en línea], [consulta: abril 2008]

Disponible en: <http://zonagratis.com/servicios/seguridad/wireles2.html>

PROGRAMAS-GRATIS, CD autorun creator4.6 [en línea], [consulta: abril 2008]

disponible en: <http://cd-autorun-creator.programas-gratis.net/>

PROGRAMAS-GRATIS, autoplay – Express [en línea], [consulta: abril 2008] disponible

en: <http://autoplay-express.programas-gratis.net/>

SOFTONIC, selteco Alligátor flash designer [en línea] [consulta: abril 2008] disponible:

en <http://selteco-alligator-flash-designer.softonic.com/>

SOFTONIC, camtasia estudio 5.0 [en línea] [consulta: abril 2008] disponible en:
<http://camtasia-studio.softonic.com/>

FREEWARE FILES, CD interface Studio [en línea], [consulta: abril 2008] disponible en:
http://freewarefile.com/cdinterface-studio-v-program_9520.html

WIKIPEDIA, red de área local [en línea] [consulta: abril 2008] disponible en:
<http://http.es.wikipedia.org/wiki/lan>

MONOGRAFIAS, protocolo de seguridad Web [en línea], [consulta: abril 2008]
<http://monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml>

ADSL FAQS, ¿Qué es wpa/wpa2? [En línea], [publicado: junio 3, 2007], [consulta: abril 2008]

Disponible en: <http://adslfaq.com.ar/que-es-wpa-wpa2/>

DNS. BDAT, seguridad en redes inalámbricas [en línea], Fabrega Martínez, Pedro Pablo, [consulta: abril 2008]

Disponible en: http://dns.debat.net/seguridad_en_redes_inalambricas/

ENTERATE EN LINEA, redes inalámbricas, estándares y mecanismos de seguridad [en línea], Cuellar Ruiz, Jaime, [publicado: 31, Agosto 2004], [consulta: abril 2008]

Disponible en: <http://enterate.unam.mx/articulos/2004/agosto/redes.html>

PROGRAMAS-GRATIS, utilidades CDS/DVDS [en línea], [consulta: abril 2008]

<http://programas-gratis.net/descargar-bajar/utilidades-cds-dvds/2-0-semanal/>

PROGRAMAS-GRATIS, capturadores de pantalla [en línea], [consulta: abril 2008]

<http://programas-gratis.net/descargar-bajar/capturar-pantalla/6-0-semanal>

WIKIPEDIA, bluetooth [en línea], [consulta: abril 2008]

Disponible en: <http://es.wikipedia.org/wiki/bluetooth>

TECNYO, ¿Qué es bluetooth? [En línea] [Publicado: octubre, 18 2007] [Consulta: abril 2008]

Disponible en: <http://tecnio.com/%c2%bfque-es-bluetooth/>

ALEGSA, definición, orígenes y usos de la tecnología inalámbrica bluetooth, [en línea],
[publicado: octubre, 25 2006], [consulta: abril 2008]

Disponible en: <http://alegsa.com.ar/notas/86.php>

MONOGRAFIAS, tecnología bluetooth [en línea], Mata Ramírez, Mario Pablo,
[consulta: abril 2008]

<http://monografias.com/trabajos43/tecnologia-bluetooth/tecnologia-bluetooth.shtml>

SPITZER, ¿Qué es el infrarrojo? [en línea], [consulta: abril 2008]

Disponible en: http://spitzer.caltech.edu/spanol/edu/learn_irl